DLA Piper Martínez Beltran
Carrera 7 No. 71-21 Torre B Of. 602
Bogotá, Colombia
www.dlapipermb.com

Bogotá, D.C., octubre de 2022

Señora,
JUEZ 19 CIVIL DEL CIRCUITO DE BOGOTÁ
ATN. DRA. ALBA LUCÍA GOYENECHE GUEVARA
E. S. D.

REF.	**Solicitantes:**	INTEGRAL S.A. y OTRO
	Solicitado:	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.
	Radicado:	**2020-00339**
	Asunto:	**Recurso de reposición y en subsidio de apelación contra el auto del 13 de octubre de 2022**

El suscrito, **SERGIO ROJAS QUIÑONES**, mayor de edad, con domicilio en la ciudad de Bogotá D.C., identificado como aparece al pie de mi firma, actuando en mi condición de apoderado de **INTEGRAL S.A.** y del **CONSORCIO GENERACIÓN ITUANGO**, acudo respetuosamente ante el Despacho con el fin de interponer los recursos de **REPOSICIÓN** y, en subsidio, de **APELACIÓN**, contra el auto del 13 de octubre de 2022, notificado por anotación en el estado del día siguiente, por medio del cual el H. Despacho resolvió decretar la terminación del trámite por desistimiento tácito, con fundamento en las siguientes consideraciones:

I. OPORTUNIDAD Y PROCEDENCIA

1.1 El auto del 13 de octubre de 2022 fue notificado por anotación en el estado del día siguiente, con lo cual, los 3 días del término de ejecutoria empezaron a correr desde el 18 de octubre hasta el **20 de octubre de 2022** (incluyéndolo), razón por la cual este recurso ha sido formulado en término.

1.2 Como no existe norma que indique que el recurso de reposición no procede contra el auto que decreta la terminación del proceso, el mismo es procedente en los términos de los artículos 318 y 319 del Código General del Proceso (CGP).

1.3 En cuanto a la procedencia del recurso de apelación se refiere, tenemos que el auto que le pone fin al proceso por cualquier causa es apelable, en los términos del numeral 7 del artículo 321 del CGP.

1.4 Como el auto recurrido decretó la terminación del trámite por desistimiento tácito, el recurso de apelación también es, entonces, procedente.

II. CONSIDERACIONES DEL RECURSO

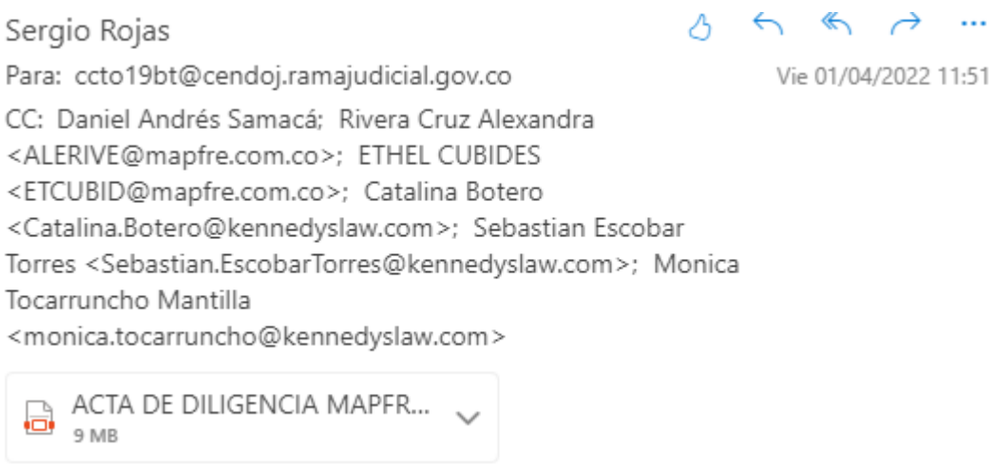
2.1 Mediante auto del 2 de febrero de 2022, notificado por anotación en el estado del día siguiente, el H. Despacho otorgó un plazo de 40 días para que se allegara al presente trámite la experticia que fue encomendada, en los siguiente términos:

"*Finalmente, se otorga un plazo de 40 días para que se presente la experticia que le fue encomendada*".

2.2 Así, el término concedido corrió desde el 4 de febrero y hasta el **1 de abril de 2022**, incluyéndolo.

2.3 Mediante correo electrónico del 1 de abril de 2022 enviado a las 11:51 a.m. (que se adjunta), el suscrito radicó el dictamen informático dentro del plazo de 40 días concedido por el H. Despacho.

2.4 Dicho correo se remitió a la dirección electrónica del Despacho y con copia a la parte contraria:


Sergio Rojas

Para: ccto19bt@cendoj.ramajudicial.gov.co Vie 01/04/2022 11:51

CC: Daniel Andrés Samacá; Rivera Cruz Alexandra <ALERIVE@mapfre.com.co>; ETHEL CUBIDES <ETCUBID@mapfre.com.co>; Catalina Botero <Catalina.Botero@kennedyslaw.com>; Sebastian Escobar Torres <Sebastian.EscobarTorres@kennedyslaw.com>; Monica Tocarruncho Mantilla <monica.tocarruncho@kennedyslaw.com>

ACTA DE DILIGENCIA MAPFR...
9 MB

2.5 De lo cual, solo puede concluirse que la experticia fue presentada dentro del plazo otorgado por el Despacho.

2.6 Seguramente por un error involuntario, el H. Despacho omitió el anterior correo y, por ello, profirió el auto aquí recurrido que decretó el desistimiento tácito.

2.7 Esto explicaría también la constancia secretarial del 13 de octubre de 2022 que precedió al auto recurrido, según la cual "*EN LA FECHA Y AL DESPACHO HOY 13 DE OCTUBRE DE 2022, INFORMANDO QUE VENCIDOS LOS TERMINOS DE 40 DIAS NO DIERON CUMPLIMIENTO A LO ORDENADO*".

2.8 No obstante, lo cierto es que mis representadas sí dieron cumplimiento a lo ordenado, allegando la experticia dentro del plazo concedido para el efecto.

2.9 Por lo anterior, respetuosamente solicito se revoque el auto aquí recurrido y, en su lugar, se tenga por presentada la experticia dentro del plazo concedido por el H. Despacho.

2.10 Por lo demás, en el dictamen pericial correspondiente puede leerse que el señor Perito indicó que "La totalidad de las imágenes forenses contenedoras de la totalidad de la evidencia digital asegurada queda en bóveda de seguridad en las instalaciones de ADALID CORP a disposición del **JUZGADO** y cualquier decisión sobre las mismas será atendida en el menor tiempo posible". No obstante esta manifestación, el lugar en el que deben reposar los anexos del dictamen (imágenes forenses y evidencia digital) es con el dictamen mismo, como manda el artículo 226 del Código General del Proceso, razón por la cual se solicitará al Despacho que requiera a la firma ADALID para que remita tales anexos con destino al expediente.

III. SOLICITUD

Con fundamento en las anteriores consideraciones, respetuosamente solicito al Despacho que:

3.1 Se sirva **REVOCAR** el auto del 13 de octubre de 2022 que decretó la terminación del trámite por desistimiento tácito y, en su lugar, se tenga por presentada la experticia dentro del plazo otorgado por el H. Despacho.

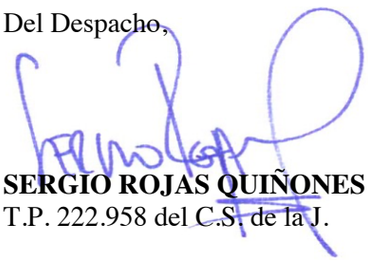
3.2 Se sirva **REQUERIR** a la firma ADALID CORP para que acompañe, con destino al expediente, los anexos digitales que sirvieron de base al dictamen oportunamente radicado, como prescribe el artículo 226 del Código General del Proceso.

DLA Piper Martínez Beltran
Carrera 7 No. 71-21 Torre B Of. 602
Bogotá, Colombia
www.dlapipermb.com

IV. ANEXOS

4.1 Correo electrónico del 1 de abril de 2022, por medio del cual se radicó la experticia dentro del plazo otorgado por el H. Despacho, junto con su anexo.

Del Despacho,



SERGIO ROJAS QUIÑONES
T.P. 222.958 del C.S. de la J.

ADALID
Security, Legal & Forensic Corporation

ACTA DE DILIGENCIA TÉCNICA DE ASEGURAMIENTO DE INFORMACIÓN DIGITAL

FECHA:	16 de noviembre del año 2021
HORA INICIO:	14:00 horas
QUIEN ATIENDE LA DILIGENCIA:	Sebastián ESCOBAR TORRES C.C. No. 1.018.466.417 Willigton Leandro TORRES MORALES C.C. No. 79.708.420 Alexandra RIVERA CRUZ C.C. No. 51.849.114 Bayrón PRIETO CASTELLANOS C.C. No. 80.075.270
CARGO:	-APODERADO ESPECIAL -PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN -JEFE JURIDICO -ASESOR
LUGAR:	MAPFRE Colombia, Carrera 14 No. 96 – 34, Edificio MAPFRE SEGUROS, Auditorio sala 1, en la ciudad de Bogotá, D.C.
OBJETIVO:	Realizar la inspección, aseguramiento y análisis de información contenida en los buzones de correos electrónicos de funcionarios y exfuncionarios de MAPFRE SEGUROS GENERALES DE COLOMBIA S.A, Sebastián ESCOBAR TORRES atendiendo a lo ordenado en el auto de fecha 8 de noviembre de 2021 por el juzgado 19 civil del circuito de Bogotá, dentro del proceso de prueba extraprocesal bajo el radicado número 11001310301920200033900, el cual se asegura en imagen forense para posterior procesamiento y aplicación de protocolo de gestión de evidencias aportado por MAPFRE para este proceso (palabras de inclusión y exclusión).

DESARROLLO

En la ciudad de Bogotá D.C., Colombia el día 16 de noviembre del año 2021, siendo las 14:00 horas, en cumplimiento a lo requerido por **INTEGRAL S.A y CONSORCIO GENERACION ITUANGO**, se reúnen en la Carrera 14 No. 96 – 34, Edificio MAPFRE SEGUROS, Auditorio sala 1, en la ciudad de Bogotá, D.C. - Colombia., los funcionarios de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**, **Sebastián ESCOBAR TORRES,** identificado con cédula de ciudadanía **No. 1.018.466.417** de Bogotá quien funge como **APODERADO ESPECIAL**, **Willigton Leandro TORRES MORALES,** identificado con cédula de ciudadanía **No. 79.708.420** de Bogotá, quien funge como **PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN, Alexandra RIVERA CRUZ,** identificado con cédula de ciudadanía **No. 51.849.114** de Bogotá, quien funge como **JEFE JURIDICO, Bayrón PRIETO CASTELLANOS,** identificado con cédula de ciudadanía **No. 80.075.270** de Bogotá, quien funge como **ASESOR** y los peritos en informática forense asignados por ADALID CORP S.A.S., **Endrick Dann Axel DÍAZ ORTEGA** identificado con cédula de ciudadanía **No. 1.016.036.658** y **Héctor Alberto DUSSAN MONTOYA** identificado con cédula de ciudadanía **No. 1.026.260.827** lo anterior, con el fin de realizar la inspección, aseguramiento y análisis de información contenida en los correos electrónicos de funcionarios y exfuncionarios de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A,** atendiendo a lo ordenado en el auto de fecha 8 de noviembre de 2021 por el juzgado 19 civil del circuito de Bogotá, dentro del proceso de prueba extraprocesal bajo el radicado número 11001310301920200033900, el cual se asegura en imágenes forenses para su posterior procesamiento y aplicación de protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**. para este proceso (palabras de inclusión y exclusión).

A continuación, se presentan los buzones de correo objeto de análisis:

- avictor@mapfre.com.co
- dagomez@mapfre.com.co
- mmalago@mapfre.com.co
- jmriano@mapfre.com.co
- aclemen@mapfre.com.co
- etcubid@mapfre.com.co
- jalbertos@mapfre.com
- anferam@mapfre.com.co
- jlcube@mapfre.com
- aquerol@mapfre.com
- csalina@mapfre.com.co
- jmerine@mapfre.com.co

- ctorres@mapfre.com.co
- anrinco@mapfre.com.co
- gueveca@mapfre.com.co
- mvivian@mapfre.com
- acparra@mapfre.com.co
- jctorr2@mapfre.com.co
- lsuarez@mapfre.com.co
- cruzj@mapfre.com.co
- rocarre@mapfre.com.co
- jospaga@mapfre.com.co

La sesión inicio a las 14:20 en donde por parte de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** se puso en conocimiento a los peritos de ADALID CORP. sobre el contenido del acuerdo de confidencialidad propuesto por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** para efectos de la practica probatoria.

Luego de leer el contenido del acuerdo de confidencialidad propuesto por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** el equipo de ADALID CORP. procede a realizar la firma del documento por medio de la página de internet https://app.mifirma.co/ .

Una vez revisado y firmado el Acuerdo de confidencialidad, el señor **Willigton Leandro TORRES MORALES** hace entrega a los peritos de ADALID CORP. de (1) Un disco duro color blanco, con capacidad de almacenamiento de **1000GB,** el cual, a través del software **CrystalDiskInfo** en su versión **8.12.12** se logra identificar su número serial "**WN911W3Z",** en su parte superior se encuentra marcado como **"prueba extraprocesal".** La información contenida en el disco duro, así como sus características y de más información se puede visualizar en las siguientes imágenes:

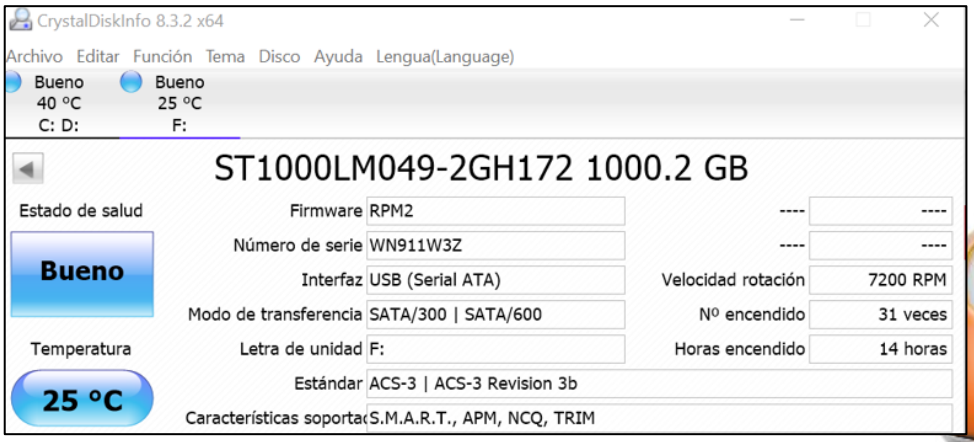


Ilustración 1 Características del Disco Duro entregado por MAPFRE SEGUROS GENERALES DE COLOMBIA S. Desde el aplicativo CrystalDiskInfo.

	
Fotografía Disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista superior)	Fotografía disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista posterior)

Dentro del Disco Duro se encuentran los archivos en formato .PST de las cuentas de correo electrónico asignadas a los funcionarios que se encuentran retirados de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**, los cuales serán mencionados a continuación:

Nombre	Fecha de modificación	Tipo
ACLEMEN	3/11/2021 4:19 p. m.	Carpeta de archivos
ANFERAM	28/10/2021 10:52 a. m.	Carpeta de archivos
AVICTOR	28/10/2021 9:14 a. m.	Carpeta de archivos
CTORRES	16/11/2021 11:28 a. m.	Carpeta de archivos
DAGOMEZ	28/10/2021 11:13 a. m.	Carpeta de archivos
JCTORR2	28/10/2021 9:42 a. m.	Carpeta de archivos
JMERINE	28/10/2021 9:32 a. m.	Carpeta de archivos
JMRIANO	16/11/2021 8:25 a. m.	Carpeta de archivos
JOSPAGA	28/10/2021 11:03 a. m.	Carpeta de archivos
LSUAREZ	28/10/2021 11:18 a. m.	Carpeta de archivos
MVIVIAN	28/10/2021 9:52 a. m.	Carpeta de archivos

Ilustración 2 Visualización contenido del Disco Duro entregado por MAPFRE SEGUROS GENERALES DE COLOMBIA S.A

ID	CORREOS FUNCIONARIOS RETIRADOS	REALIZACIÓN IMAGEN FORENSES	TAMAÑO GB
1	avictor@mapfre.com.co	1 – 17NOV2021	380 MB
2	aclemen@mapfre.com.co	2 – 17NOV2021	42.6 GB
3	jospaga@mapfre.com.co	3 – 18NOV2021	4.49 GB
4	ctorres@mapfre.com.co	4 – 18NOV2021	17.7 GB
5	dagomez@mapfre.com.co	5 – 19NOV2021	28.8 GB
6	lsuarez@mapfre.com.co	6 – 19NOV2021	45.8 GB
7	anferam@mapfre.com.co	7 – 19NOV2021	52.3 GB
8	mvivian@mapfre.com	8 – 19NOV2021	57 GB
9	jctorr2@mapfre.com.co	9 – 22NOV2021	59.3 GB
10	jmriano@mapfre.com.co	10 – 22NOV2021	115 GB
11	jmerine@mapfre.com.co	11 – 22NOV2021	118 GB

Tabla 1 Correos electrónicos de funcionarios retirados MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.

Todo esto con el fin de realizar una revisión preliminar de los archivos contenidos en el disco duro entregado por el señor **Willigton Leandro TORRES MORALES** en formato .PST los cuales se identifican en la **ilustración 2** anteriormente mostrada. Al realizar la revisión de la información contenida en el disco duro, el personal de **MAPFRE SEGUROS GENERALES DE COLOMBIA S. A** informa al equipo de **ADALID CORP**. que los buzones de correo en formato .PST contenidos en el disco duro pertenecen a funcionarios retirados de la empresa **MAPFRE SEGUROS GENERALES DE COLOMBIA S. A**.

De igual manera, el personal de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** le indica al equipo de **ADALID CORP.** que los correos electrónicos faltantes de los trabajadores de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** que aún se encuentran activos dentro de la compañía serán exportados y entregados en el orden que se solicite uno a uno luego de finalizar con la realización de las imágenes forense de los correos del personal retirado, los cuales fueron entregados en el disco duro antes mencionado. Una vez finalizados los anteriores procedimientos, los peritos de ADALID CORP. S.A.S. proceden de manera final a regresar el disco duro al señor **Willigton Leandro TORRES MORALES** el día 16 de noviembre de 2021.

El día 17 de noviembre de 2021 se inicia la diligencia siendo las 9:00 a.m., para este objeto, el señor **Willigton Leandro TORRES MORALES** encargado de la presente diligencia y quien funge como **Profesional De Seguridad De La Información**, hace entrega a los peritos designados por ADALID CORP. S.A.S. de (1) Un Disco Duro color **BLANCO**, identificado su número serial **WN911W3Z,** con capacidad de almacenamiento de **1000GB**, el cual se encentra marcado con en su parte superior con las palabras **"prueba extraprocesal HTGO"** con el propósito de que el equipo de ADALID CORP realice la preservación y aseguramiento para cada una de los buzones de correo electrónico allí contenidos:

De conformidad con lo mencionado anteriormente se explican los procedimientos y procesos que se realizaran para cada uno de los buzones de correo suministrados por **MAPFRE SEGUROS GENERALES DE COLOMBIA S. A.:**

1. Se realiza una imagen forense contentiva del buzón de correo electrónico.
2. Se procesa la información en la herramienta FTK 7.2.
3. Se realizan los siguientes filtros de información en la opción de búsqueda indexada de la herramienta FTK 7.2, tomando como referencia el protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Tabla 2 *Filtros aplicados al procesamiento de los buzones de correo.*

4. Tras la aplicación de cada uno de los filtros de información a través de la opción de búsqueda indexada en el software de Informática Forense FTK, si este genera resultados asociados a la búsqueda de las palabras clave previamente establecidas, se le aplicarán el siguiente comando de exclusión de información, solicitado por **MAPFRE** como se presenta a continuación, en garantía de su información y lo autorizado por el Juzgado 19 Civil del Circuito de Bogotá:

<?xml version="1.0" encoding="UTF-8"?>
<exportedFilter xmlns="http://www.accessdata.com/ftk2/filters"><filter name="PALABRAS DE EXCLUSIÓN MAPFRE" matchCriterion="any" id="f_1000001" read_only="false" description=""><rule position="0" enabled="true" id="a_9429" operator="is"><one_string value="@kennedyslaw.com"/></rule><rule position="1" enabled="true" id="a_9429" operator="is"><one_string value="catalina.botero@kennedyslaw.com"/></rule><rule position="2" enabled="true" id="a_9429" operator="is"><one_string value="nick.thomas@kennedyslaw.com"/></rule><rule position="3" enabled="true" id="a_9429" operator="is"><one_string value="louis.foscolo@kennedyslaw.com"/></rule><rule position="4" enabled="true" id="a_9429" operator="is"><one_string value="caitlin.gallagher@kennedyslaw.com"/></rule><rule position="5" enabled="true" id="a_9429" operator="is"><one_string value="sebastian.escobartorres@kennedyslaw.com"/></rule><rule position="6" enabled="true" id="a_9429" operator="is"><one_string value="Monica.Tocarruncho@kennedyslaw.com"/></rule><rule position="7" enabled="true" id="a_9429" operator="is"><one_string value="Kennedys"/></rule><rule position="8" enabled="true" id="a_9429" operator="is"><one_string value="Kennedys Colombia"/></rule><rule position="9" enabled="true" id="a_9429" operator="is"><one_string value="Kennedys Londres"/></rule><rule position="10" enabled="true"

id="a_9429" operator="is"><one_string value="Nick Thomas"/></rule><rule position="11" enabled="true" id="a_9429" operator="is"><one_string value="Caitlin Gallagher"/></rule><rule position="12" enabled="true" id="a_9429" operator="is"><one_string value="Louis Foscolo"/></rule><rule position="13" enabled="true" id="a_9429" operator="is"><one_string value="Catalina Botero Arango"/></rule><rule position="14" enabled="true" id="a_9429" operator="is"><one_string value="Sebastián Escobar Torres"/></rule><rule position="15" enabled="true" id="a_9429" operator="is"><one_string value="Monica Tocarruncho"/></rule><rule position="16" enabled="true" id="a_9429" operator="is"><one_string value="Responsabilidad Civil"/></rule><rule position="17" enabled="true" id="a_9429" operator="is"><one_string value="Póliza No. 2901311000164"/></rule><rule position="18" enabled="true" id="a_9429" operator="is"><one_string value="2901311000164"/></rule><rule position="19" enabled="true" id="a_9429" operator="is"><one_string value="Subjetividad"/></rule><rule position="20" enabled="true" id="a_9429" operator="is"><one_string value="RC"/></rule><rule position="21" enabled="true" id="a_9429" operator="is"><one_string value="RCE"/></rule><rule position="22" enabled="true" id="a_9429" operator="is"><one_string value="Maquinaria"/></rule><rule position="23" enabled="true" id="a_9429" operator="is"><one_string value="Equipo"/></rule><rule position="24" enabled="true" id="a_9429" operator="is"><one_string value="M&E"/></rule><rule position="25" enabled="true" id="a_9429" operator="is"><one_string value="EyM"/></rule><rule position="26" enabled="true" id="a_9429" operator="is"><one_string value="Terrorismo"/></rule><rule position="27" enabled="true" id="a_9429" operator="is"><one_string value="Sabotaje"/></rule><rule position="28" enabled="true" id="a_9429" operator="is"><one_string value="S&T"/></rule><rule position="29" enabled="true" id="a_9429" operator="is"><one_string value="Transporte"/></rule><rule position="30" enabled="true" id="a_9429" operator="is"><one_string value="Cargo"/></rule><rule position="31" enabled="true" id="a_9429" operator="is"><one_string value="Market Meeting"/></rule><rule position="32" enabled="true" id="a_9429" operator="is"><one_string value="Reunión de Mercado"/></rule></filter><attribute id="a_9429" type="string"><table>cmn_ObjectDeviceSearchedItems</table><column>Value</column></attribute></exportedFilter>

PALABRAS DE EXCLUSIÓN MAPFRE

5. Los resultados obtenidos luego de realizar los 14 filtros de información y aplicar los comandos de exclusión sobre cada correo electrónico y que sean satisfactorios para el proceso, serán exportados en un

documento .HTML para cada buzón de correo analizado y por separado en marcadores para una fácil interpretación de este.

Tras explicar los procedimientos y procesos a realizar, se procede a iniciar la labor pericial en Informática Forense de la siguiente manera:

1. **Buzón de correo electrónico avictor@mapfre.com.co.**

El día 17 de noviembre de 2021 el equipo de ADALID CORP. ingresa a la carpeta **AVICTOR**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

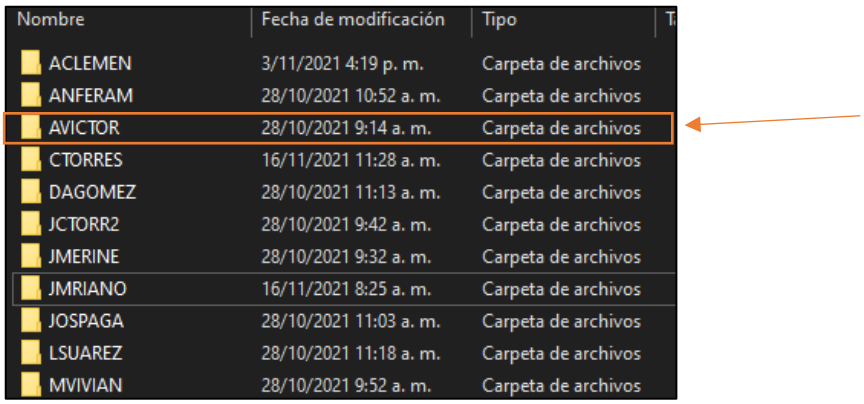


Ilustración 3 Visualización carpeta AVICTOR.

Posteriormente, procede a validar la información contenida al interior de la carpeta **AVICTOR** identificada al interior del disco duro como se observa en las siguientes imágenes:

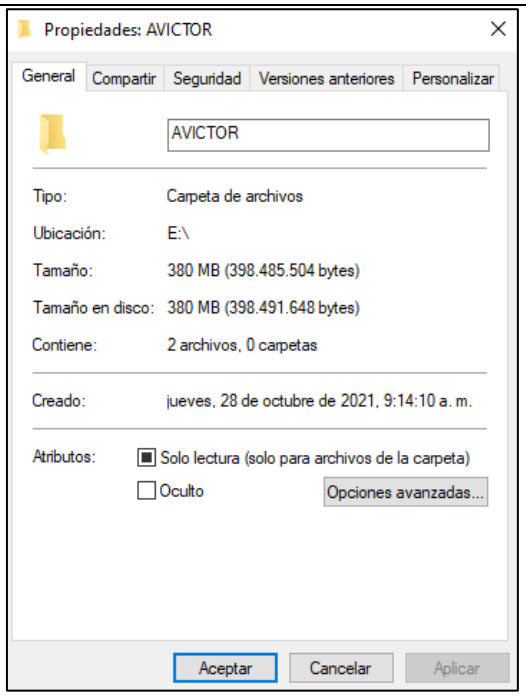


Ilustración 4 Propiedades de la carpeta AVICTOR visto desde el Disco Duro.

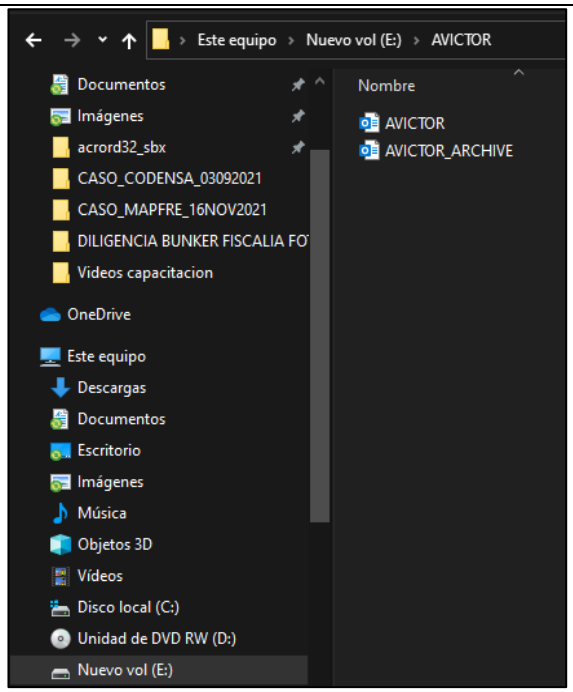


Ilustración 5 Contenido de la carpeta AVICTOR visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**avictor@mapfre.com.co.**" asignado a **Víctor Jonathan ARELLANO CARDONA** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **10:42:03** y culminando el mismo de forma satisfactoria a las **10:42:56**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_17NOV2021
Número de prueba: 001_AVICTOR
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO AVICTOR@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO

DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP S.A.S. - Endrick Dann Axel DÍAZ ORTEGA
Notas:

Information for F:\1. AVICTOR\IMAGENFORENSE_PST_AVICTOR_MAPFRE_17NOV2021.ad1:
[Custom Content Sources]
AVICTOR:G:\AVICTOR | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 7d7787982808d7be0d6baf4f87b9505a
SHA1 checksum: 1818a0e2013e2215acf8130a1f35002f72fc48de

Image information:
Acquisition started: Wed Nov 17 10:42:03 2021
Acquisition finished: Wed Nov 17 10:42:55 2021
Segment list:
F:\1. AVICTOR\IMAGENFORENSE_PST_AVICTOR_MAPFRE_17NOV2021.ad1

Image Verification Results:
Verification started: Wed Nov 17 10:42:55 2021
Verification finished: Wed Nov 17 10:42:56 2021
MD5 checksum: 7d7787982808d7be0d6baf4f87b9505a : verified
SHA1 checksum: 1818a0e2013e2215acf8130a1f35002f72fc48de : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **HITACHI**, identificado con número de serie **JP2930HQ2N6YLH**, con capacidad de almacenamiento de **1000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Luego, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**avictor@mapfre.com.co.**" asignado a **Víctor Jonathan ARELLANO CARDONA** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 6 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO AVICTOR@MAPFRE.COM.CO.

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico **avictor@mapfre.com.co** asignada **Víctor Jonathan ARELLANO CARDONA** para el desarrollo de sus funciones:

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
1	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Víctor Jonathan ARELLANO CARDONA → avictor@mapfre.com.co	ad1	0.38 GB
TOTAL					**0.38 GB**

Tabla 3 Detalle del buzón de correo electrónico asignado avictor@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico **avictor@mapfre.com.co** asignado a **Víctor Jonathan ARELLANO CARDONA** para el desarrollo de sus funciones aloja un total de **0.38 GB** dentro de este espacio el laboratorio de informática forense logró hallar un total de **Siete mil ochocientos seis (7.806)** archivos (incluyendo carpetas), como se observa a continuación.

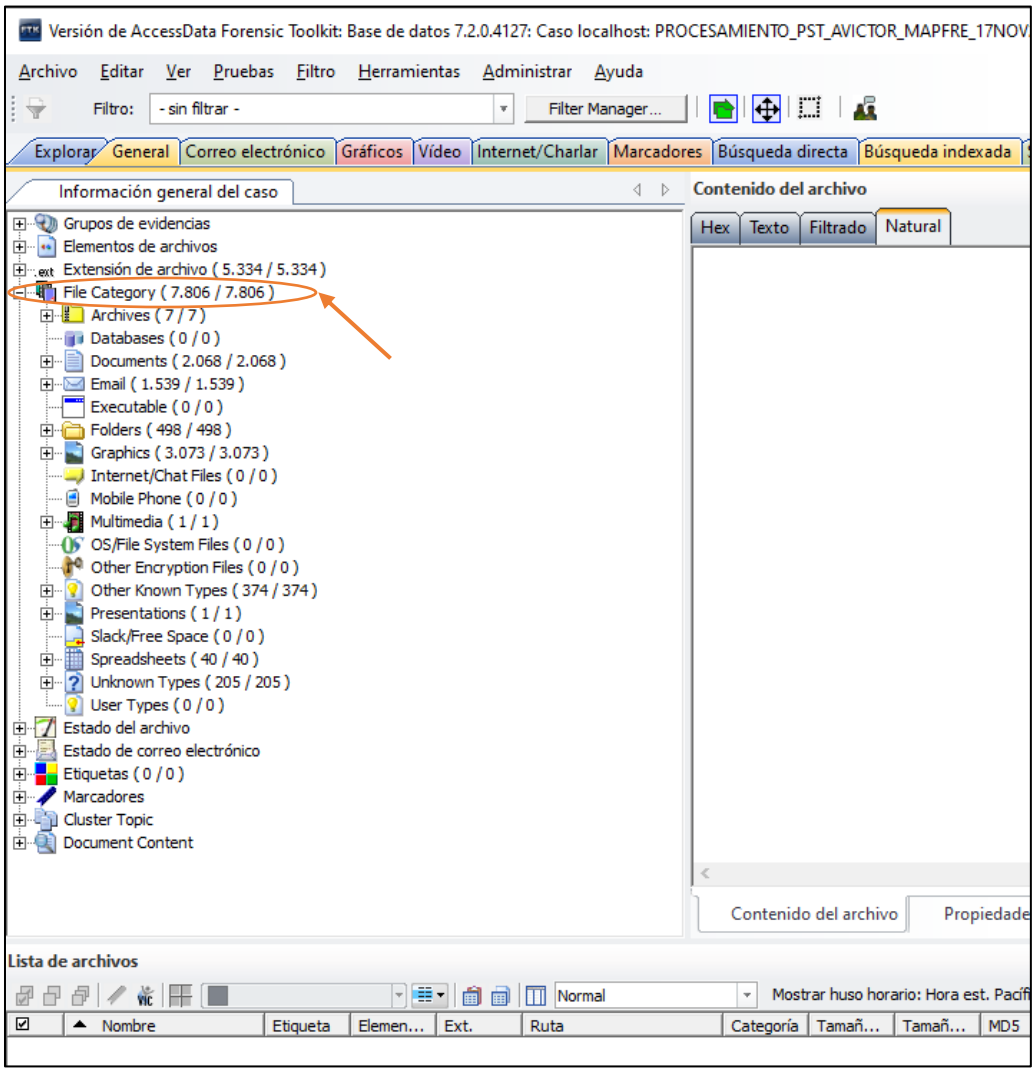


Ilustración 7 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico avictor@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO VÍCTOR JONATHAN ARELLANO CARDONA → AVICTOR@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información

eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico a victor@mapfre.com.co asignado a Víctor Jonathan ARELLANO CARDONA, iniciando el día el **17** de noviembre del presente año con una duración aproximada de Un (1) días calendario, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Mil ochocientos cincuenta (1.850)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

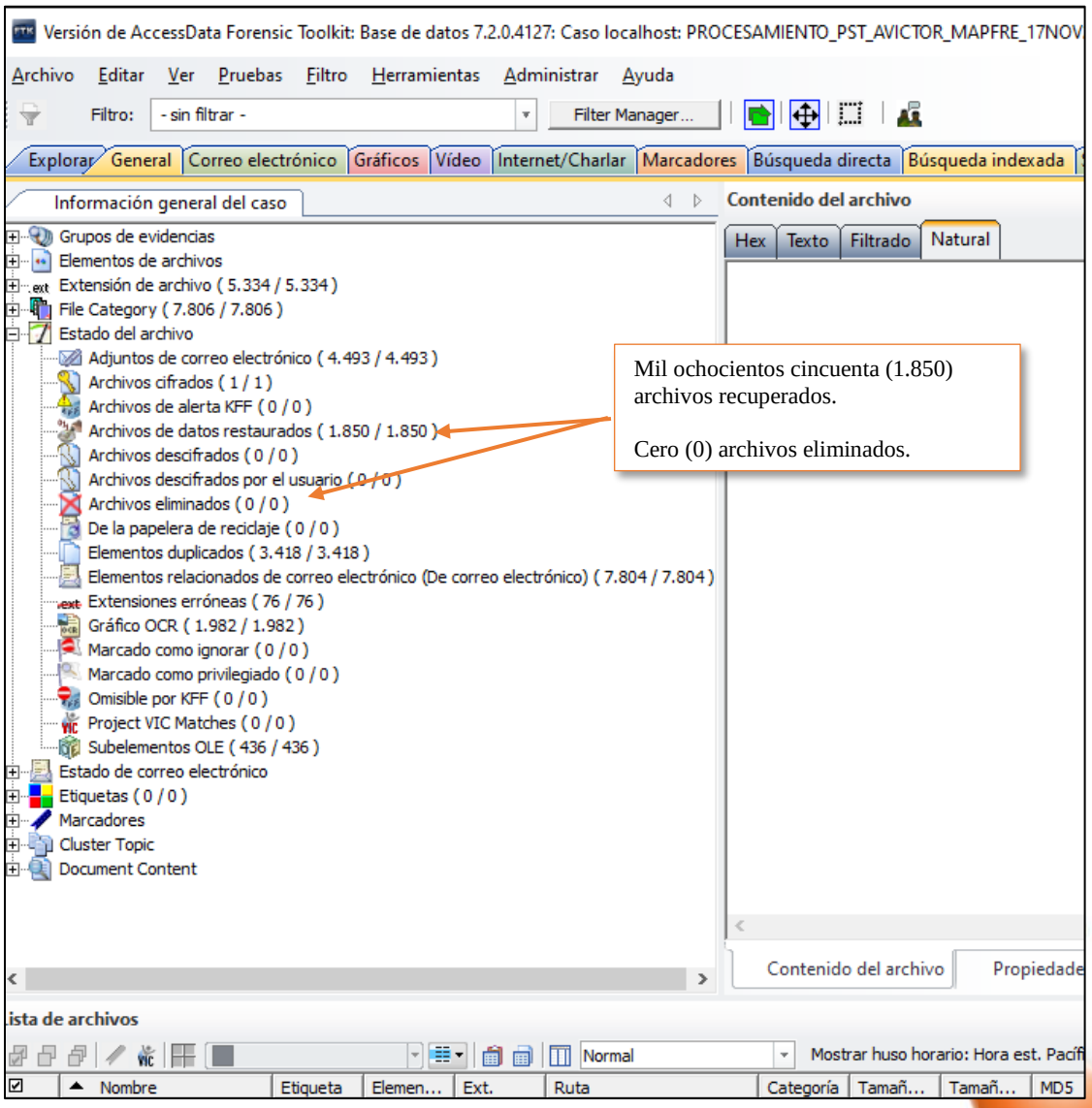


ilustración 8 Total de archivos recuperados en la cuenta de correo electrónico avictor@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Siete mil ochocientos seis (7.806)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

- **RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO AVICTOR@MAPFRE.COM.CO.**

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico avictor@mapfre.com.co asignada a **Víctor Jonathan ARELLANO CARDONA** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	7
2	Documentos	2.068
3	Correo Electrónico	1.539
4	Carpetas	498
5	Gráficos	3.073
6	Multimedia	1
7	Otro tipo de Archivos	374
8	Presentaciones	1
9	Hojas de cálculo	40
10	Tipos de archivos desconocidos	205
TOTAL		**7.806**

Tabla 4 Información buscada evidencia 001_AVICTOR, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior **tabla**, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Siete mil ochocientos seis (7.806).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean

legibles, archivos **duplicados**[1], falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Cuatro mil cuatrocientos noventa y tres (4.493) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Un (1) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Mil ochocientos cincuenta (1.850) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Tres mil cuatrocientos dieciocho (3.418) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico
- **Siete mil ochocientos cuatro (7.804) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Setenta y seis (76) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Mil novecientos ochenta y dos (1.982) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Cuatrocientos treinta y seis (436) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico avictor@mapfre.com.co asignada a **Víctor Jonathan ARELLANO CARDONA** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

[1] Se eliminan del filtro resultado archivos duplicados, entendiendo como duplicidad, que tengan igual tamaño e igual huella digital HASH MD5 y SHA1.

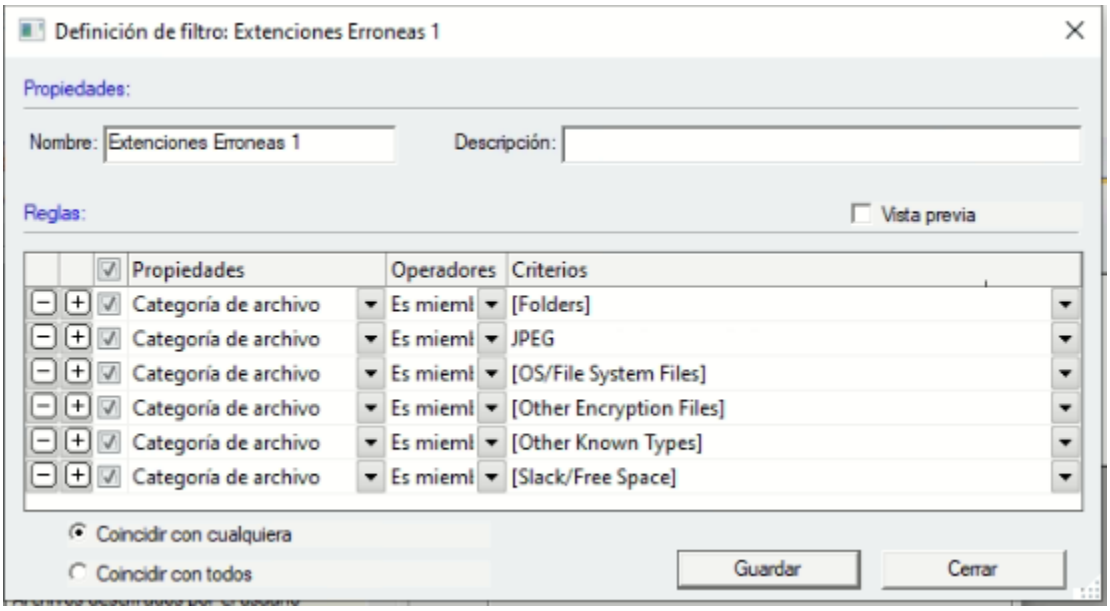


Ilustración 9 Filtro para excluir las extensiones erróneas.

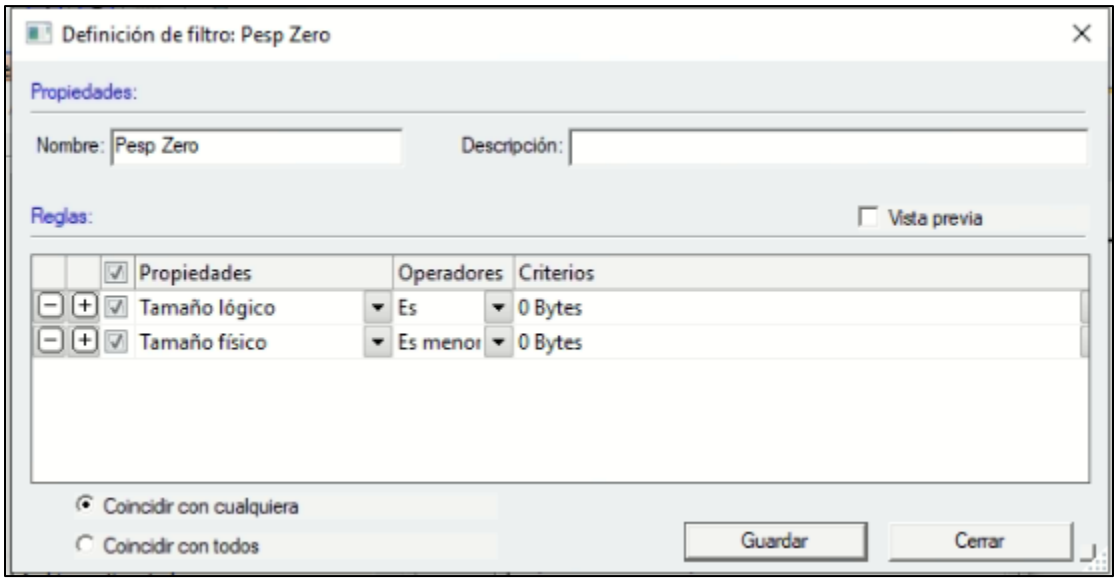


Ilustración 10 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

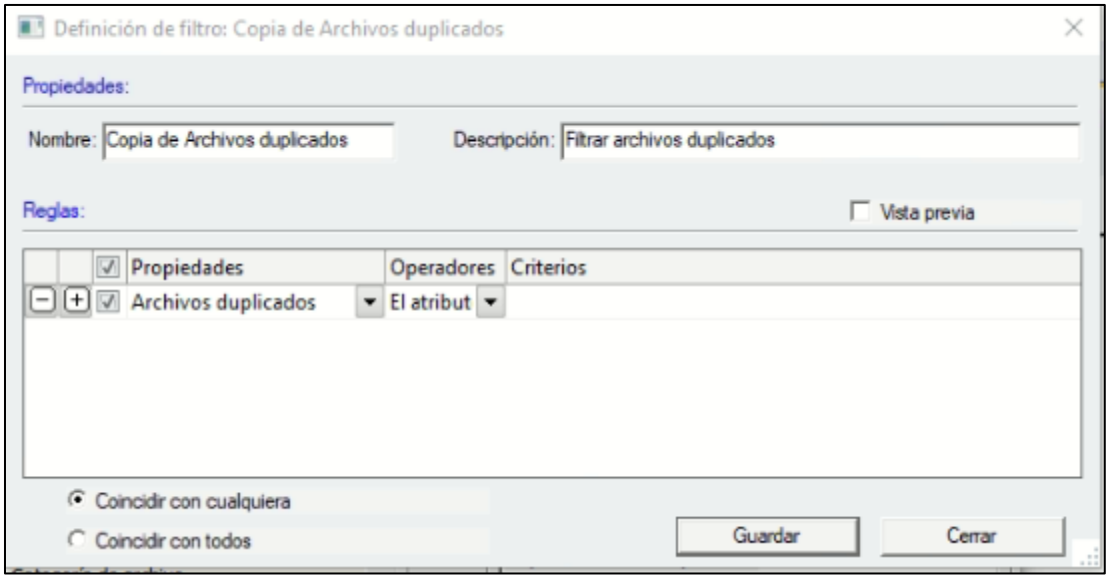


Ilustración 11 Filtro para excluir los archivos duplicados.

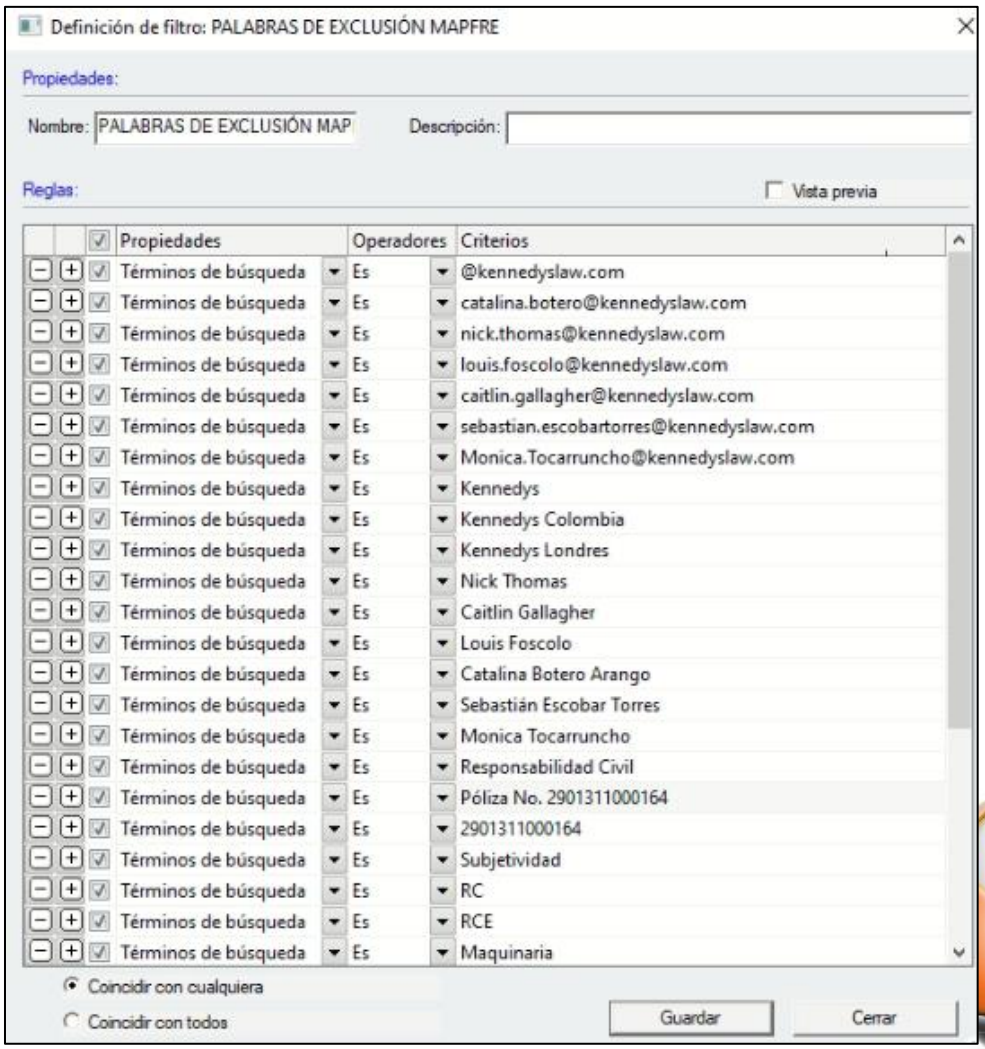


Ilustración 12 Filtro para excluir los archivos suministrado por MAPFRE - 1.

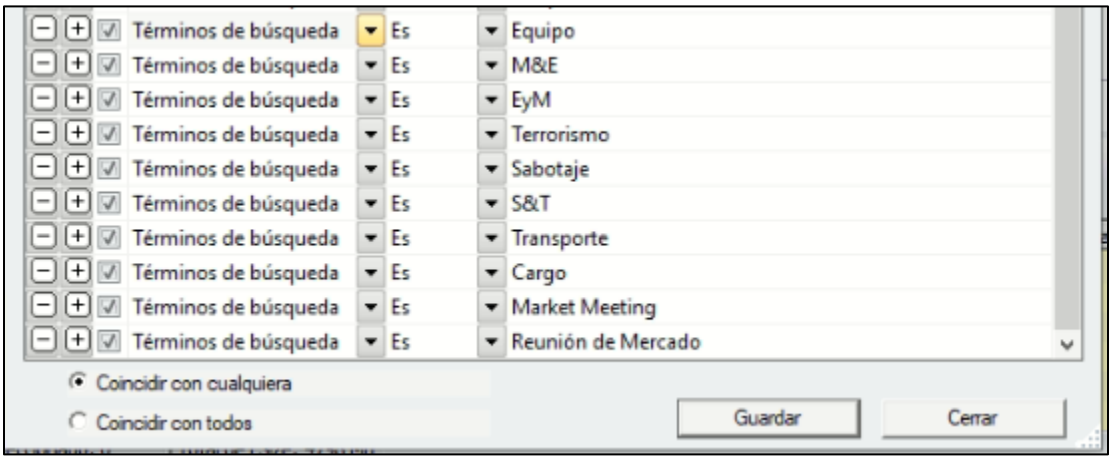
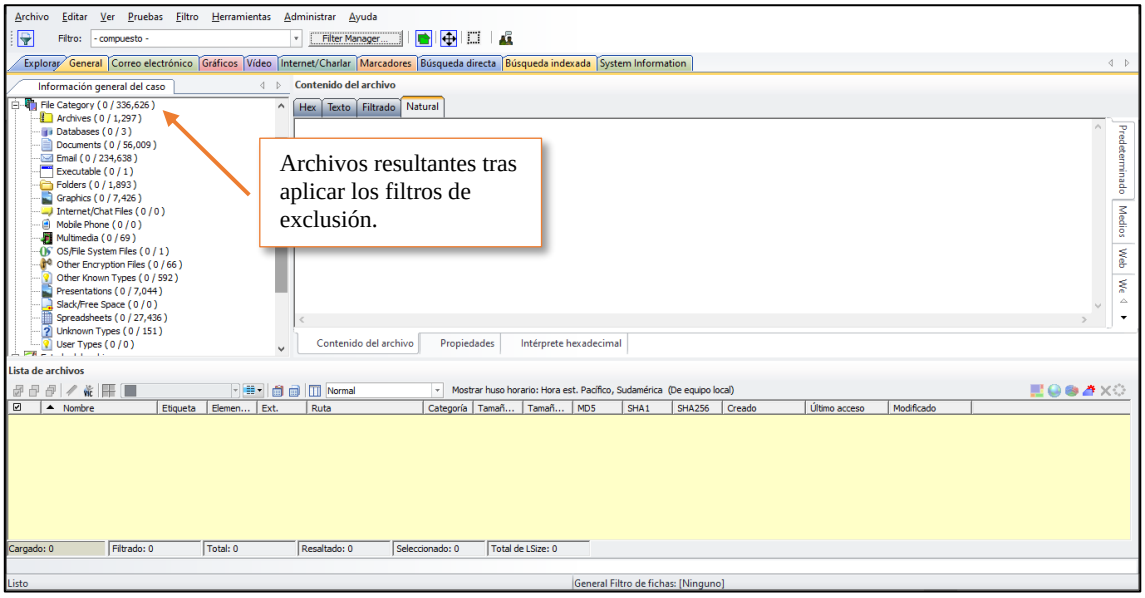


Ilustración 13 Filtro para excluir los archivos suministrado por MAPFRE - 2.

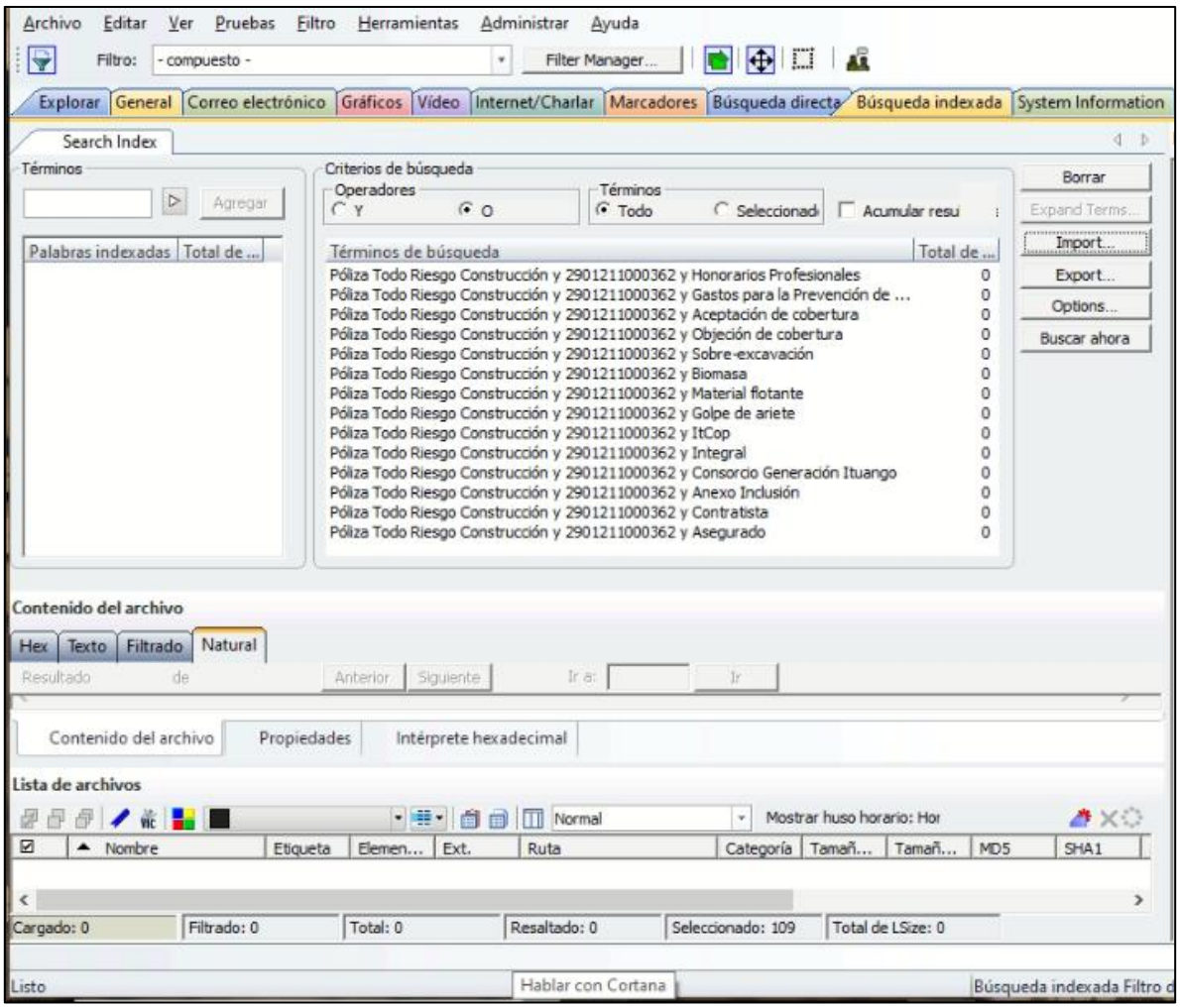
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Cero (0)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo avictor@mapfre.com.co asignada a **Víctor Jonathan ARELLANO CARDONA** para el desarrollo de sus funciones.

2. Buzón de correo electrónico aclemen@mapfre.com.co.

El día 17 de noviembre de 2021 el equipo de ADALID CORP ingresa a la carpeta **ACLEMEN**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

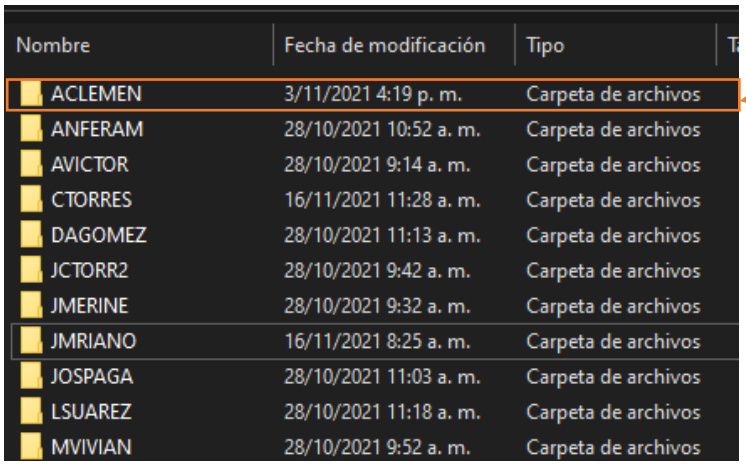


Ilustración 14 Visualización carpeta ACLEMEN

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **ACLEMEN** identificada dentro del disco duro como se observa en las siguientes imágenes:

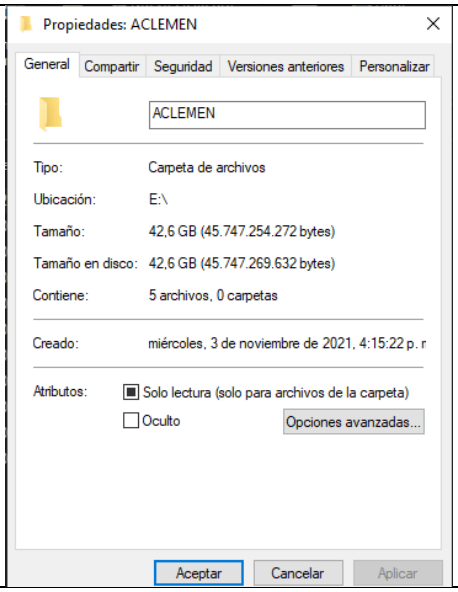


Ilustración 15 Propiedades de la carpeta ACLEMEN visto desde el Disco Duro.

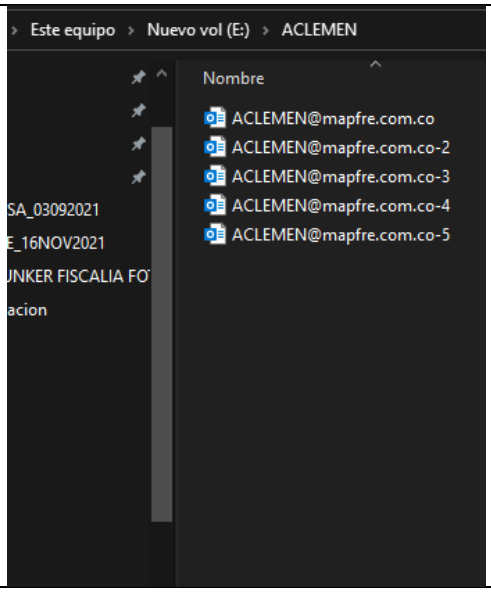


Ilustración 16 Contenido de la carpeta ACLEMEN visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**aclemen@mapfre.com.co**" asignado a **Antonio CLEMENTE CAMPANARIO** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **12:36:57** y culminando el mismo de forma satisfactoria a las **14:27:43**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_17NOV2021
Número de prueba: 002_ACLEMEN
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ACLEMEN@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP S.A.S. - Endrick Dann Axel DÍAZ ORTEGA
Notas:

Information for F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad1:
[Custom Content Sources]
ACLEMEN: G:\ACLEMEN|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 5b6abdd3129e2330f3a46cc583d004a7
SHA1 checksum: 70e7587e2b2fac10f3c58a029e552844a8aabf49

Image information:
Acquisition started: Wed Nov 17 12:36:57 2021
Acquisition finished: Wed Nov 17 14:20:40 2021
Segment list:
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad1
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad2
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad3
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad4

F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad5
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad6
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad7
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad8
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad9
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad10
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad11
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad12
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad13
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad14
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad15
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad16
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad17
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad18
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad19
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad20
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad21
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad22
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad23
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad24
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad25
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad26

F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad27
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad28
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad29
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad30

Image Verification Results:
Verification started: Wed Nov 17 14:20:40 2021
Verification finished: Wed Nov 17 14:27:43 2021
MD5 checksum: 5b6abdd3129e2330f3a46cc583d004a7 : verified
SHA1 checksum: 70e7587e2b2fac10f3c58a029e552844a8aabf49 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **HITACHI**, identificado con número de serie **JP2930HQ2N6YLH**, con capacidad de almacenamiento de **1000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:



	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**aclemen@mapfre.com.co**" asignado a **Antonio CLEMENTE CAMPANARIO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 17 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ACLEMEN@MAPFRE.COM.CO.**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico aclemen@mapfre.com.co asignada **Antonio CLEMENTE CAMPANARIO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño
2	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Antonio CLEMENTE CAMPANARIO → aclemen@mapfre.com.co	ad1	42.6 GB
TOTAL					**42.6 GB**

Tabla 5 Detalle del buzón de correo electrónico asignado aclemen@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico aclemen@mapfre.com.co asignado a **Antonio CLEMENTE**

CAMPANARIO para el desarrollo de sus funciones **aloja** un total de **42.6 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Un millón ochocientos treinta y cinco mil seiscientos ochenta y dos (1.835.682)** archivos (incluyendo carpetas), como se observa a continuación:

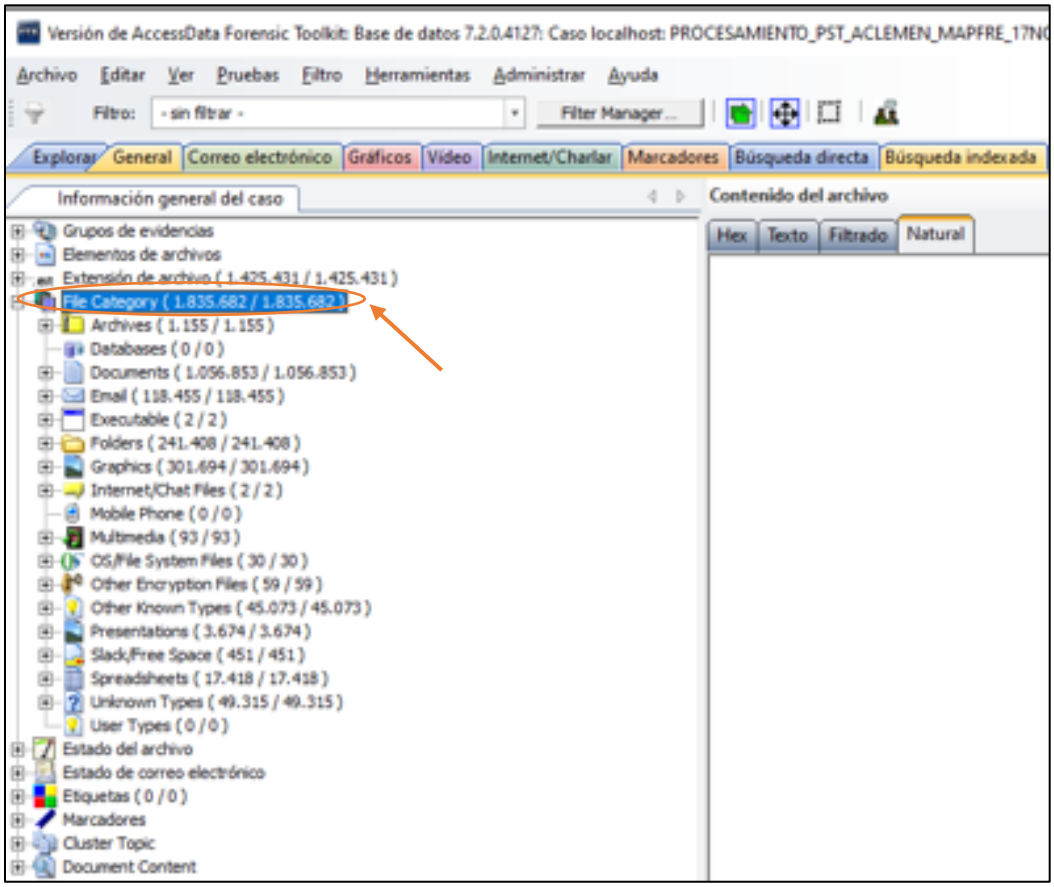


Ilustración 18 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico aclemen@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO ANTONIO CLEMENTE CAMPANARIO → ACLEMEN@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico aclemen@mapfre.com.co asignado a **Antonio CLEMENTE CAMPANARIO**, iniciando el día el **17** de noviembre del presente año con una duración aproximada de Ocho (8) días calendario el resultado a dicho proceso arrojó que existen **cero (0)** ítems en condición de "eliminados" y se reconstruyeron **Ciento cuatro mil**

setecientos sesenta y dos (104.762) archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

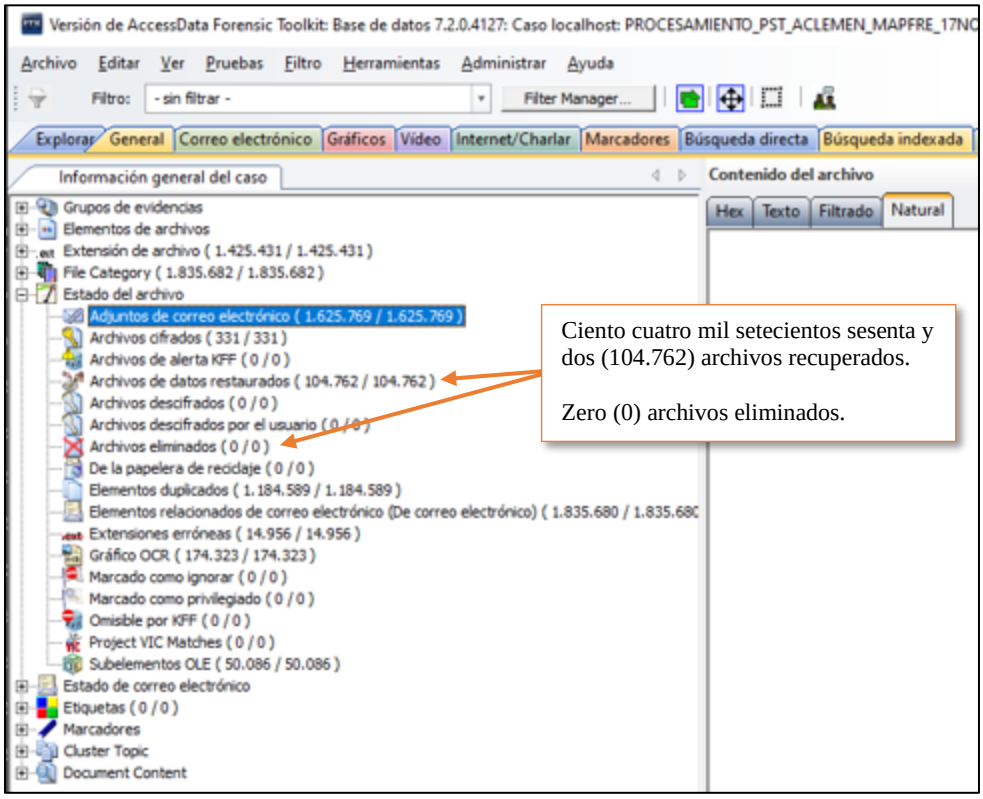


ilustración 19 Total de archivos recuperados en la cuenta de correo electrónico aclemen@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Un millón ochocientos treinta y cinco mil seiscientos ochenta y dos (1.835.682)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

- **RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ACLEMEN@MAPFRE.COM.CO.**

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico

aclemen@mapfre.com.co asignada a **Antonio CLEMENTE CAMPANARIO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1.155
2	Documentos	1.056.853
3	Correo Electrónico	118.455
4	Ejecutables	2
5	Carpetas	241.408
6	Archivo de chat	2
7	Gráficos	301.694
8	Multimedia	93
9	Archivos del sistema	30
10	Otros archivos encriptados	59
11	Otros archivos desconocidos	45.073
12	Presentaciones	3.674
13	Espacio libre	451
14	Hojas de cálculo	17.418
15	Tipos de archivos desconocidos	49.315
TOTAL		**1.835.682**

Tabla 6 Información buscada evidencia 002_ACLEMEN, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Un millón ochocientos treinta y cinco mil seiscientos ochenta y dos (1.835.682).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Un millón seiscientos veinticinco mil setecientos sesenta y nueve (1.625.769) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Trecientos Treinta y Un (331) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Ciento cuatro mil setecientos sesenta y dos (104762) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Un millón ciento ochenta y cuatro mil quinientos ochenta y nueve (1.184.589) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Un millón ochocientos treinta y cinco mil seiscientos ochenta (1.835.680) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Catorce mil novecientos cincuenta y seis (14.956) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Ciento setenta y cuatro mil trescientos veintitrés (174.323) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Cincuenta mil ochenta y seis (50.086) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico aclemen@mapfre.com.co asignada a **Antonio CLEMENTE CAMPANARIO** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



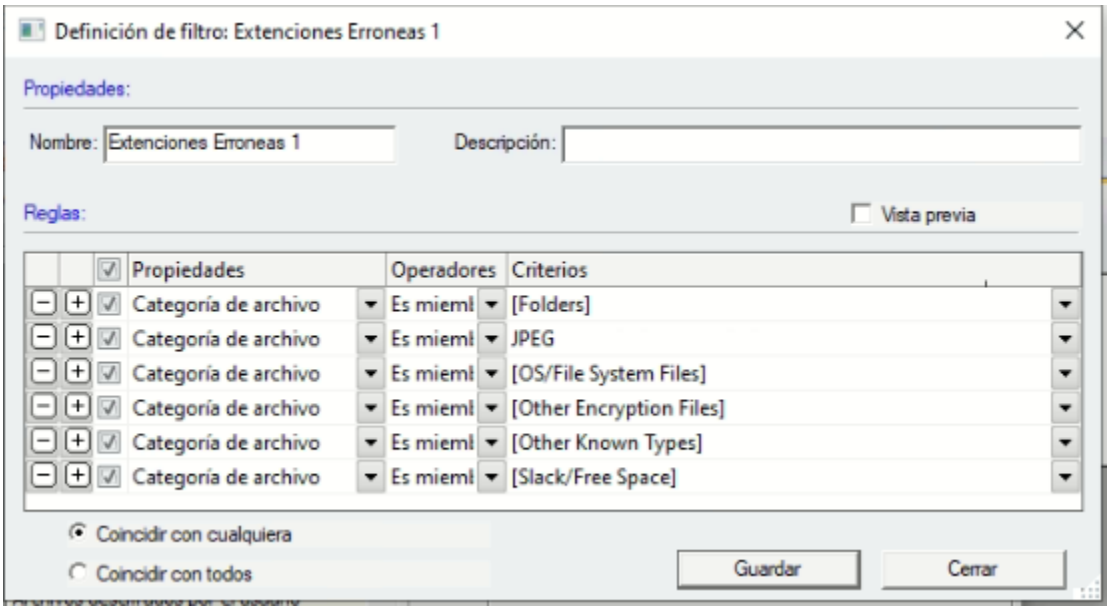


Ilustración 20 Filtro para excluir las extensiones erróneas.

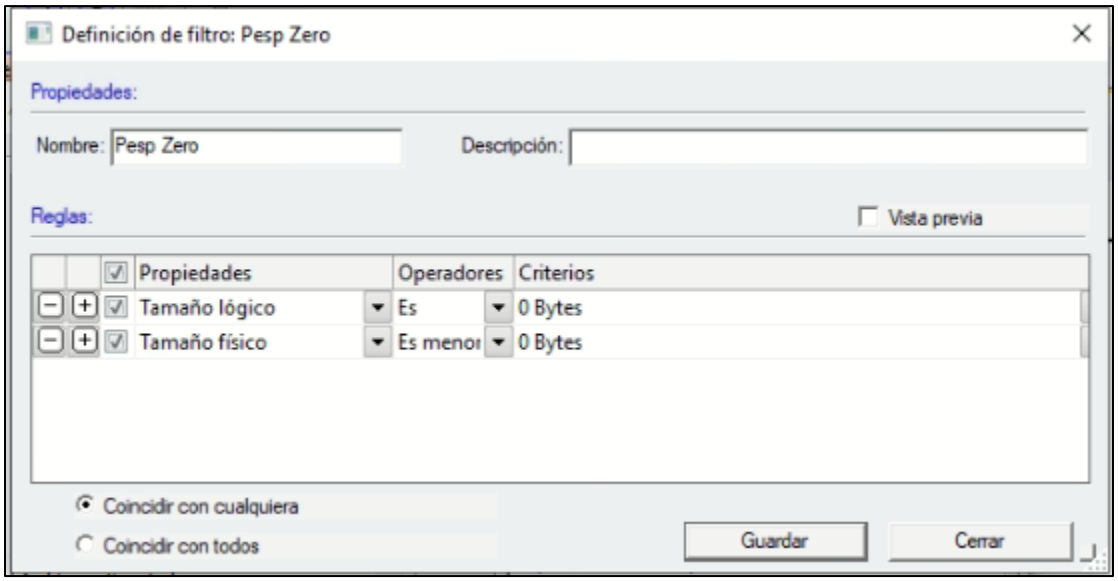


Ilustración 21 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

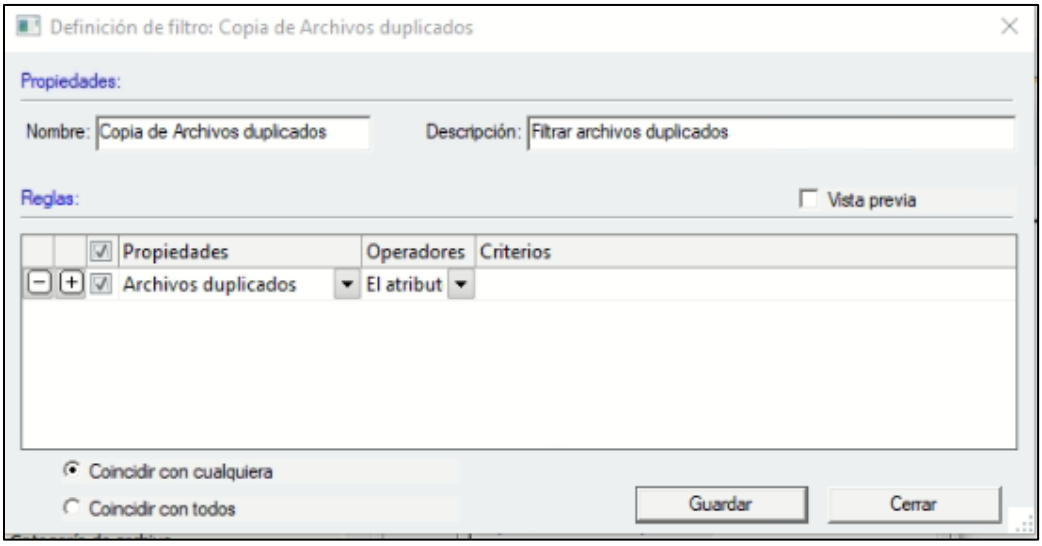
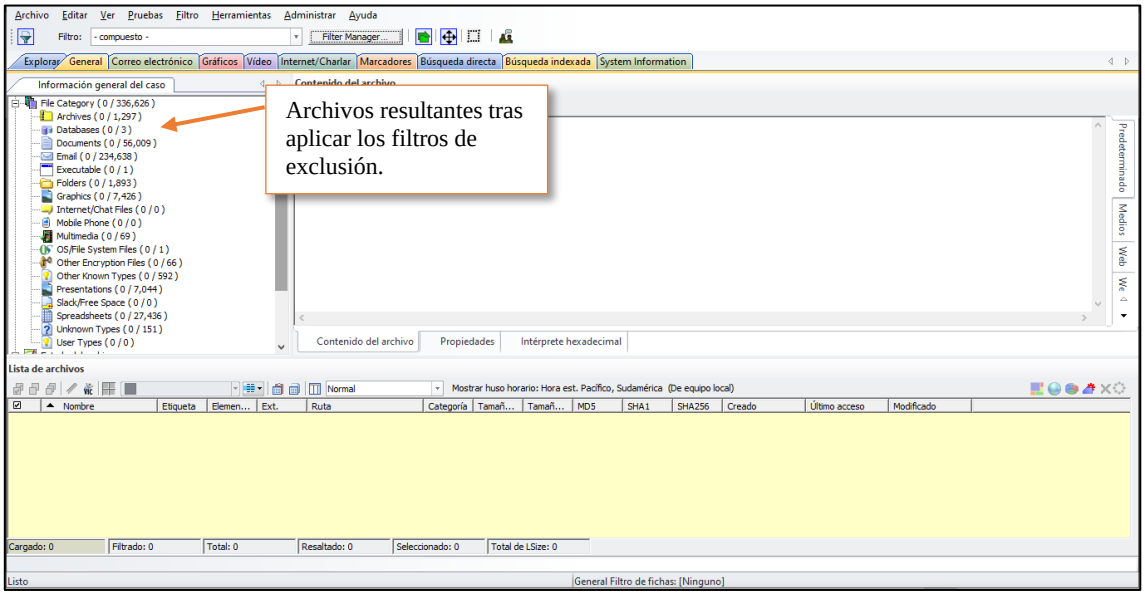


Ilustración 22 Filtro para excluir los archivos duplicados.

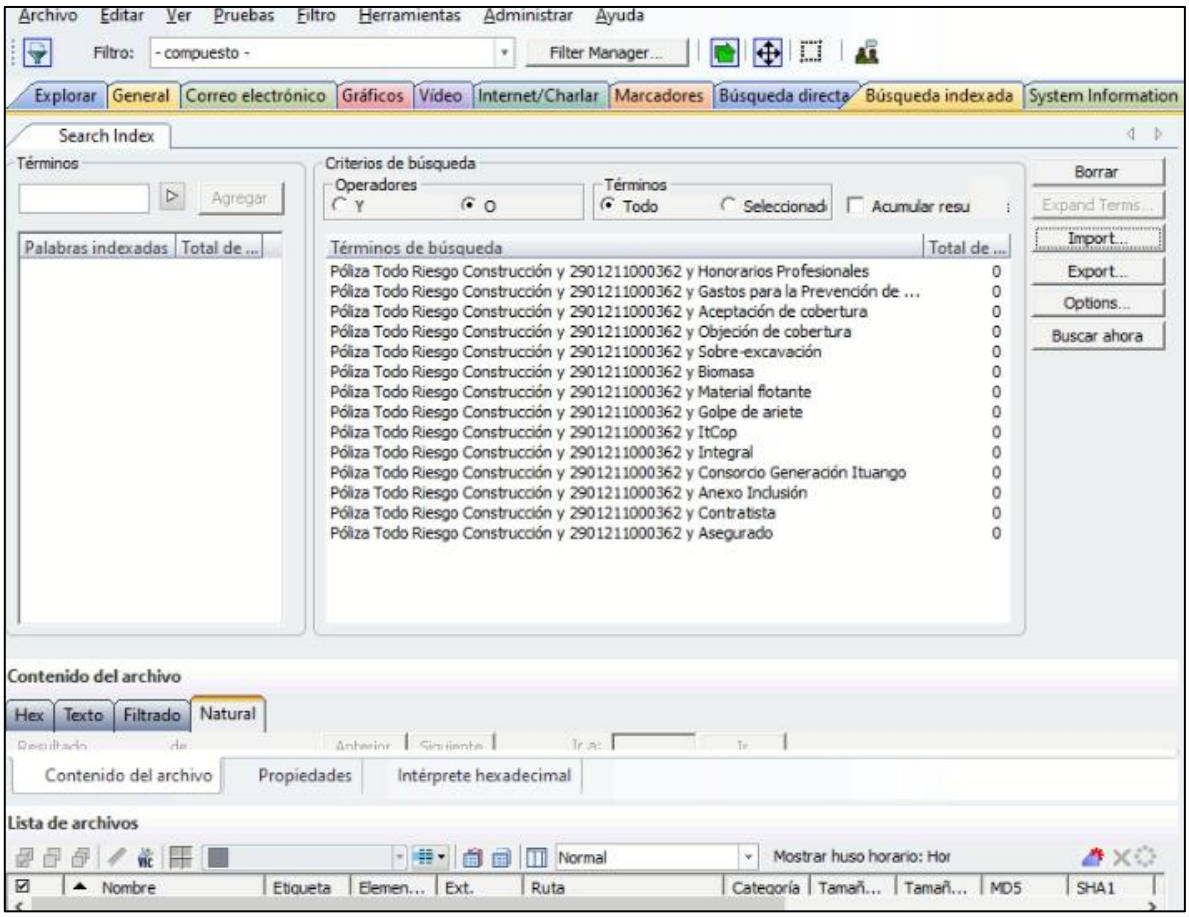
Tras aplicar los filtros anteriormente mencionados, se logra reducir muestra de información a **Cero (0)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo aclemen@mapfre.com.co asignada a **Antonio CLEMENTE CAMPANARIO** para el desarrollo de sus funciones.

3. Buzón de correo electrónico jospaga@mapfre.com.co.

El día 18 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **JOSPAGA**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

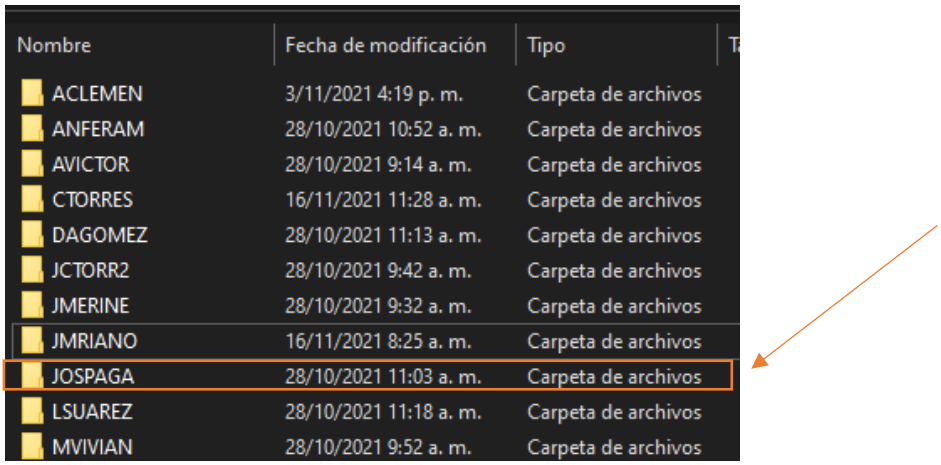


Ilustración 23 Visualización carpeta JOSPAGA

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **JOSPAGA** identificada dentro del disco duro como se observa en las siguientes imágenes:

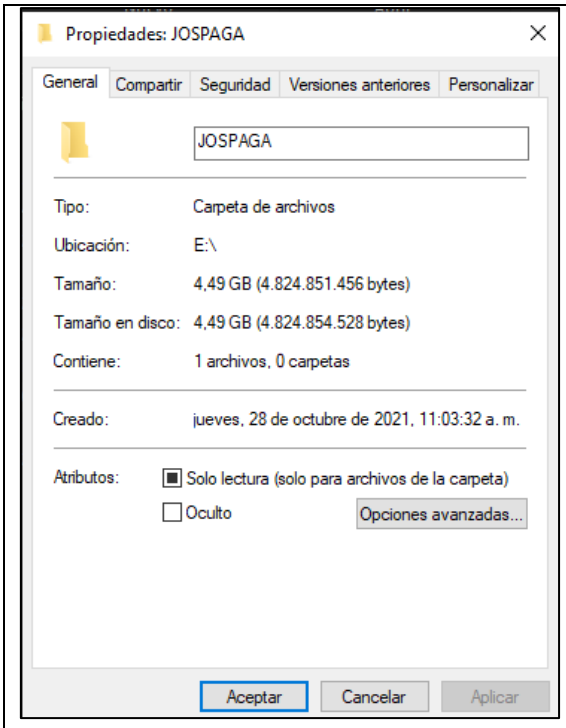


Ilustración 24 Propiedades de la carpeta JOSPAGA visto desde el Disco Duro.

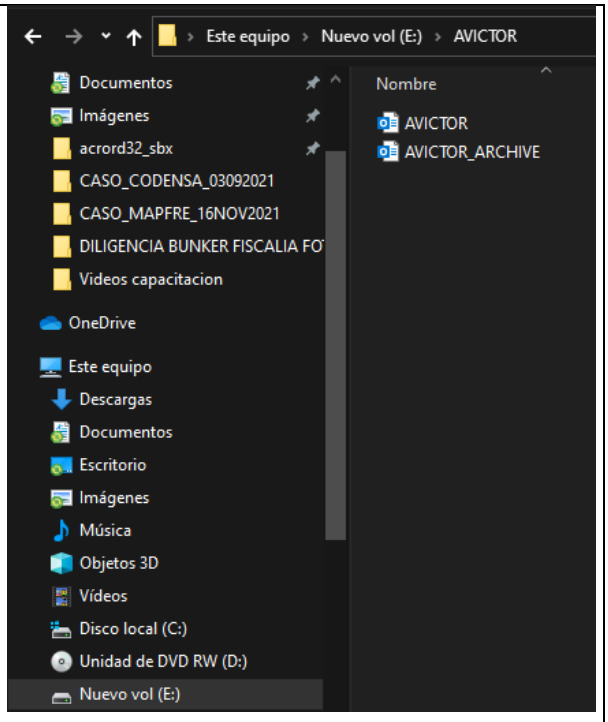


Ilustración 25 Contenido de la carpeta JOSPAGA visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**jospaga@mapfre.com.co.**" asignado a

José Fernando PALACIO GALLÓN para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **10:35:09** y culminando el mismo de forma satisfactoria a las **10:51:17**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_18NOV2021
Número de prueba: 003_JOSPAGA
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO JOSPAGA@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for F:\EVIDENCIA_MAPFRE_2\3. JOSPAGA\IMAGENFORENSE_PST_JOSPAGA_MAPFRE_18NOV2021.ad1:
[Custom Content Sources]
E::E:\ | JOSPAGA | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 326f16dbe95b854b5fdd979f1828ab88
SHA1 checksum: 090832e206bf6c9540fcfdad2d7d1aa1a25b74a3

Image information:
Acquisition started: Thu Nov 18 10:35:09 2021
Acquisition finished: Thu Nov 18 10:50:38 2021
Segment list:
F:\EVIDENCIA_MAPFRE_2\3. JOSPAGA\IMAGENFORENSE_PST_JOSPAGA_MAPFRE_18NOV2021.ad1

F:\EVIDENCIA_MAPFRE_2\3. JOSPAGA\IMAGENFORENSE_PST_JOSPAGA_MAPFRE_18NOV2021.ad2 F:\EVIDENCIA_MAPFRE_2\3. JOSPAGA\IMAGENFORENSE_PST_JOSPAGA_MAPFRE_18NOV2021.ad3 F:\EVIDENCIA_MAPFRE_2\3. JOSPAGA\IMAGENFORENSE_PST_JOSPAGA_MAPFRE_18NOV2021.ad4 Image Verification Results: Verification started: Thu Nov 18 10:50:38 2021 Verification finished: Thu Nov 18 10:51:17 2021 MD5 checksum: 326f16dbe95b854b5fdd979f1828ab88 : verified SHA1 checksum: 090832e206bf6c9540fcfdad2d7d1aa1a25b74a3 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de 2000GB, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico **jospaga@mapfre.com.co"** asignado a **José Fernando PALACIO GALLÓN** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 26 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO JOSPAGA@MAPFRE.COM.CO."**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**. para la cuenta de correo electrónico **jospaga@mapfre.com.co"** asignado a **José Fernando PALACIO GALLÓN** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
3	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	José Fernando PALACIO GALLÓN → jospaga@mapfre.com.co	ad1	4.49 GB
TOTAL					**4.49 GB**

Tabla 7 Detalle del buzón de correo electrónico asignado jospaga@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico **jospaga@mapfre.com.co"** asignado a **José Fernando PALACIO GALLÓN** para el desarrollo de sus funciones **aloja** un total de **4.49 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento noventa y seis mil ciento ochenta y nueve (196.189)** archivos (incluyendo carpetas), como se observa a continuación.

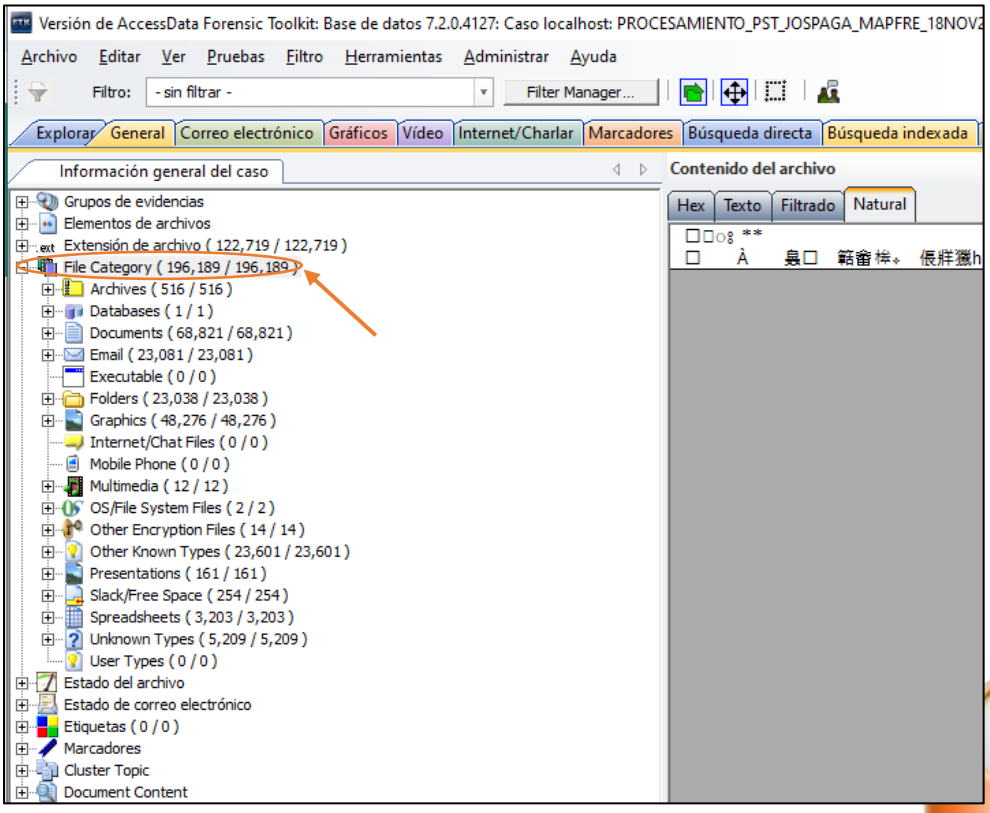


Ilustración 27 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico jospaga@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JOSÉ FERNANDO PALACIO GALLÓN → JOSPAGA@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico **jospaga@mapfre.com.co"** asignado a **José Fernando PALACIO GALLÓN** iniciando el día el **18** de noviembre del presente año con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **cero (0)** ítems en condición de "eliminados" y se reconstruyeron **Veintisiete mil ochocientos once (27.811)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

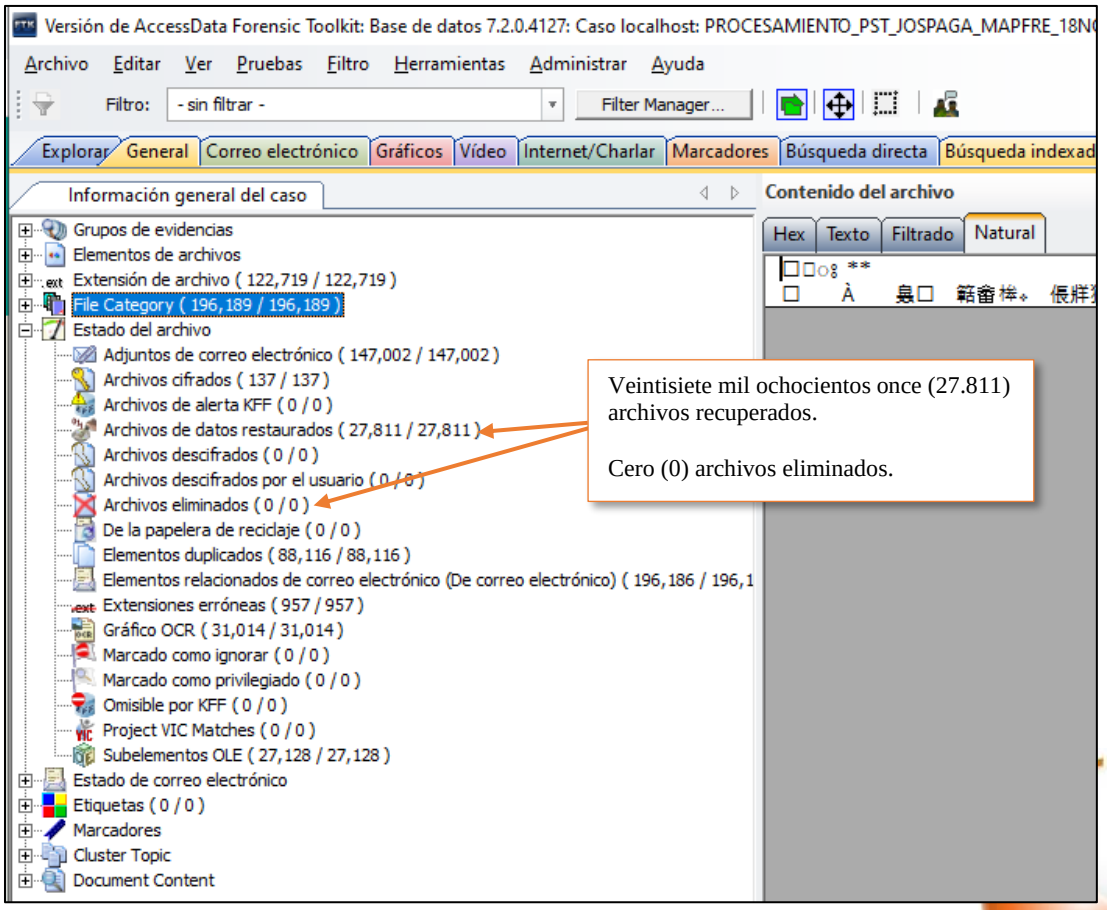


ilustración 28 Total de archivos recuperados en la cuenta de correo electrónico jospaga@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento noventa y seis mil ciento ochenta y nueve (196.189)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

- **RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO JOSPAGA@MAPFRE.COM.CO.**

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico **jospaga@mapfre.com.co** asignado a **José Fernando PALACIO GALLÓN** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	516
2	Bases de Datos	1
3	Documentos	68.821
4	Correo Electrónico	23.081
5	Carpetas	23.038
6	Gráficos	48.276
7	Multimedia	12
8	Archivos del sistema	2
9	Otros archivos encriptados	14
10	Otros archivos desconocidos	23.601
11	Presentaciones	161
12	Espacio libre	254
13	Hojas de cálculo	3.203
14	Tipos de archivos desconocidos	5.209
TOTAL		**196.189**

Tabla 8 Información buscada evidencia 003_JOSPAGA, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento noventa y seis mil ciento ochenta y nueve (196.189).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **ciento cuarenta y siete mil dos (147.002) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **ciento treinta y siete (137) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Veintisiete mil ochocientos once (27.811) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Ochenta y ocho mil ciento dieciséis (88.116) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento noventa y seis mil ciento ochenta y seis (196.186) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **novecientos cincuenta y siete (957) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Treinta y un mil catorce (31.014) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Veintisiete mil ciento veintiocho (27.128) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico jospaga@mapfre.com.co asignado a **José Fernando PALACIO GALLÓN** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

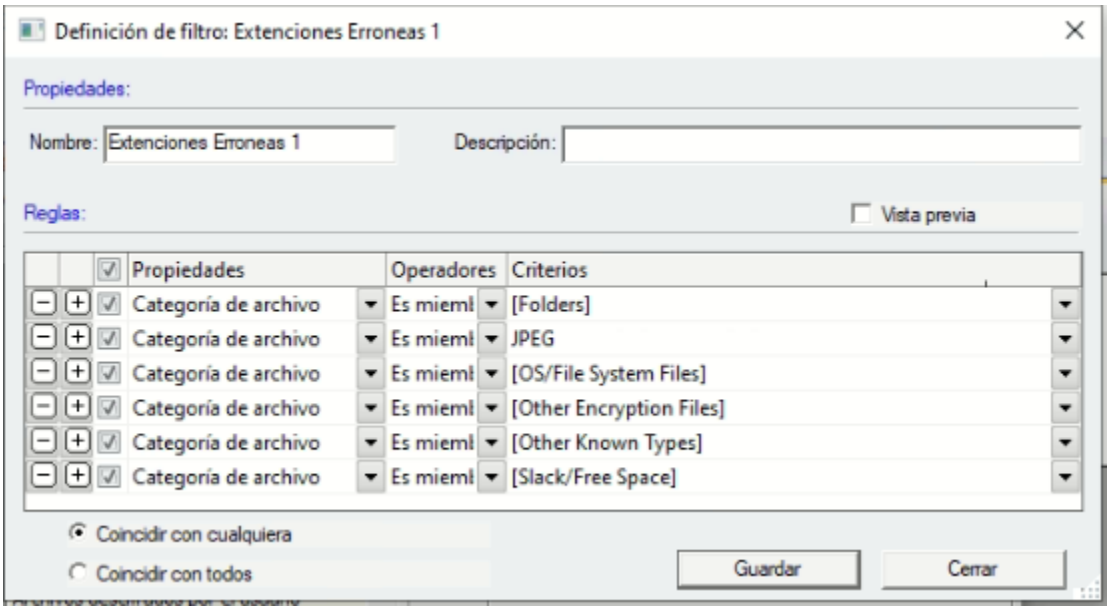


Ilustración 29 Filtro para excluir las extensiones erróneas.

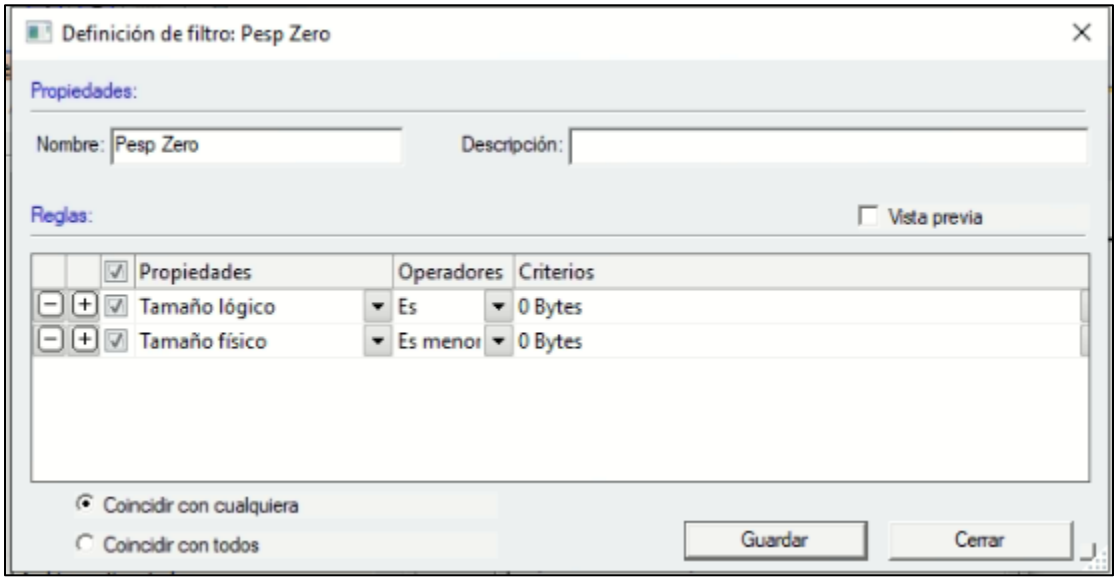


Ilustración 30 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

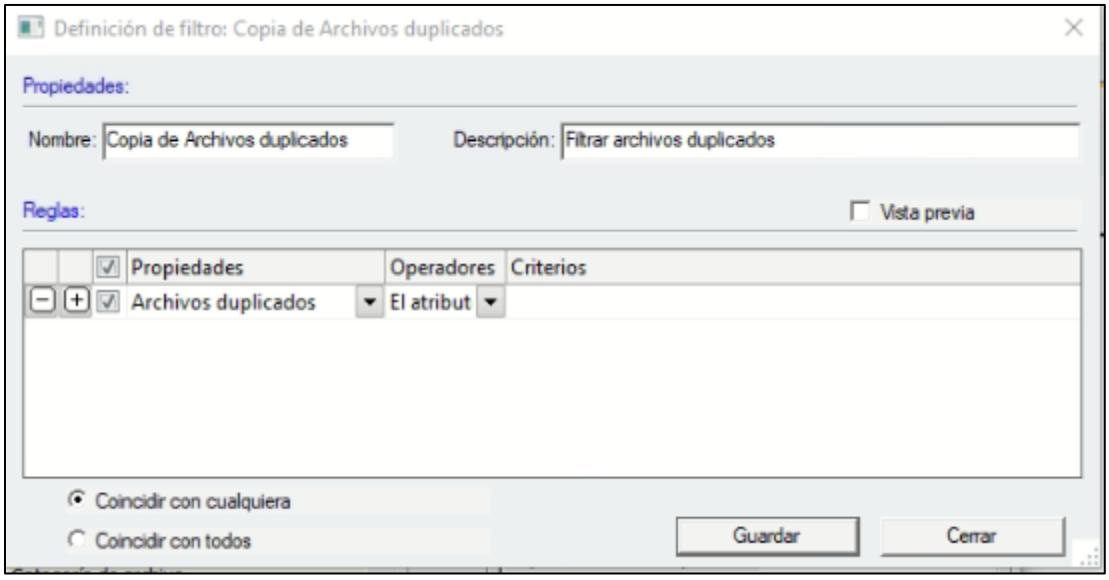


Ilustración 31 Filtro para excluir los archivos duplicados.

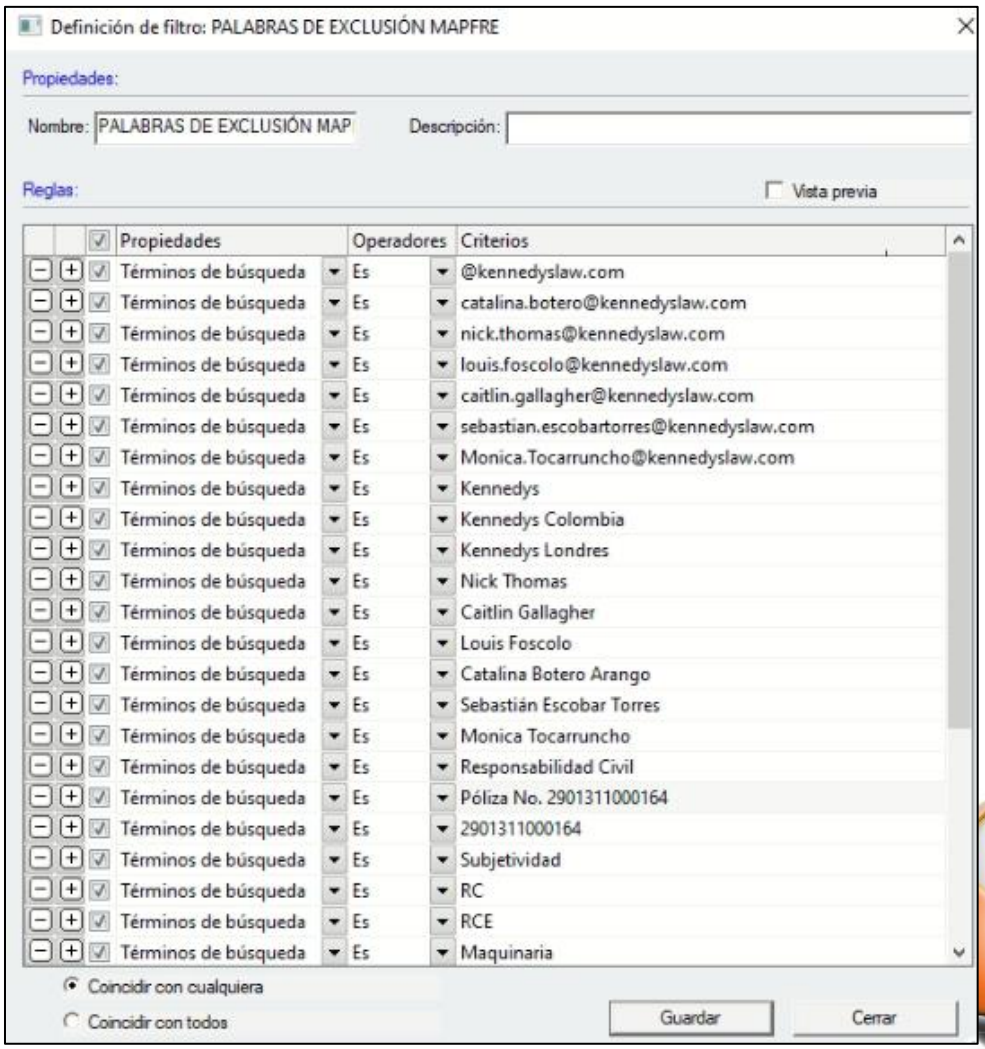


Ilustración 32 Filtro para excluir los archivos suministrado por MAPFRE - 1.

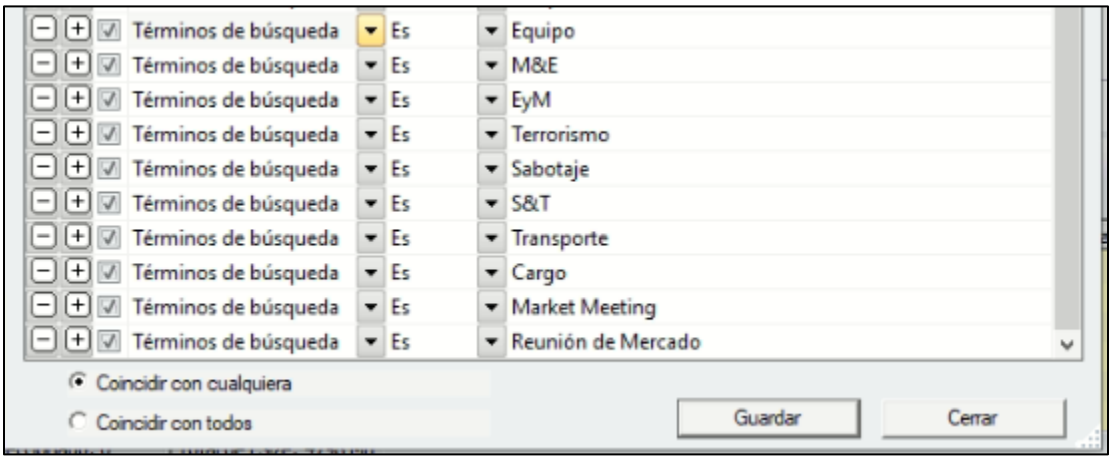
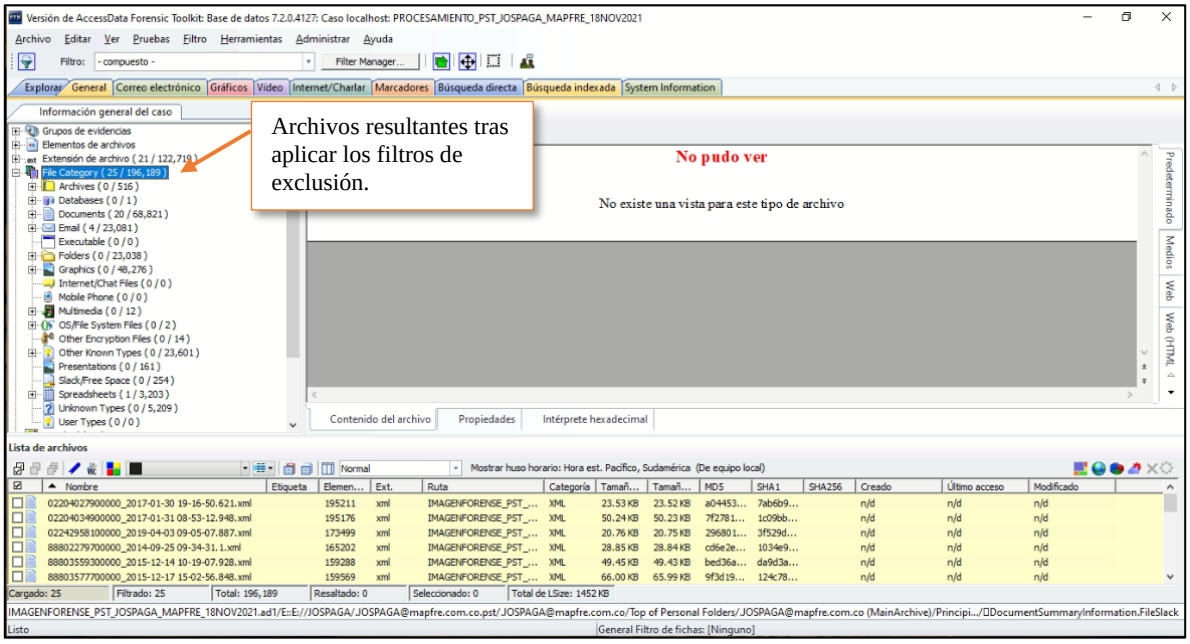


Ilustración 33 Filtro para excluir los archivos suministrado por MAPFRE - 2.

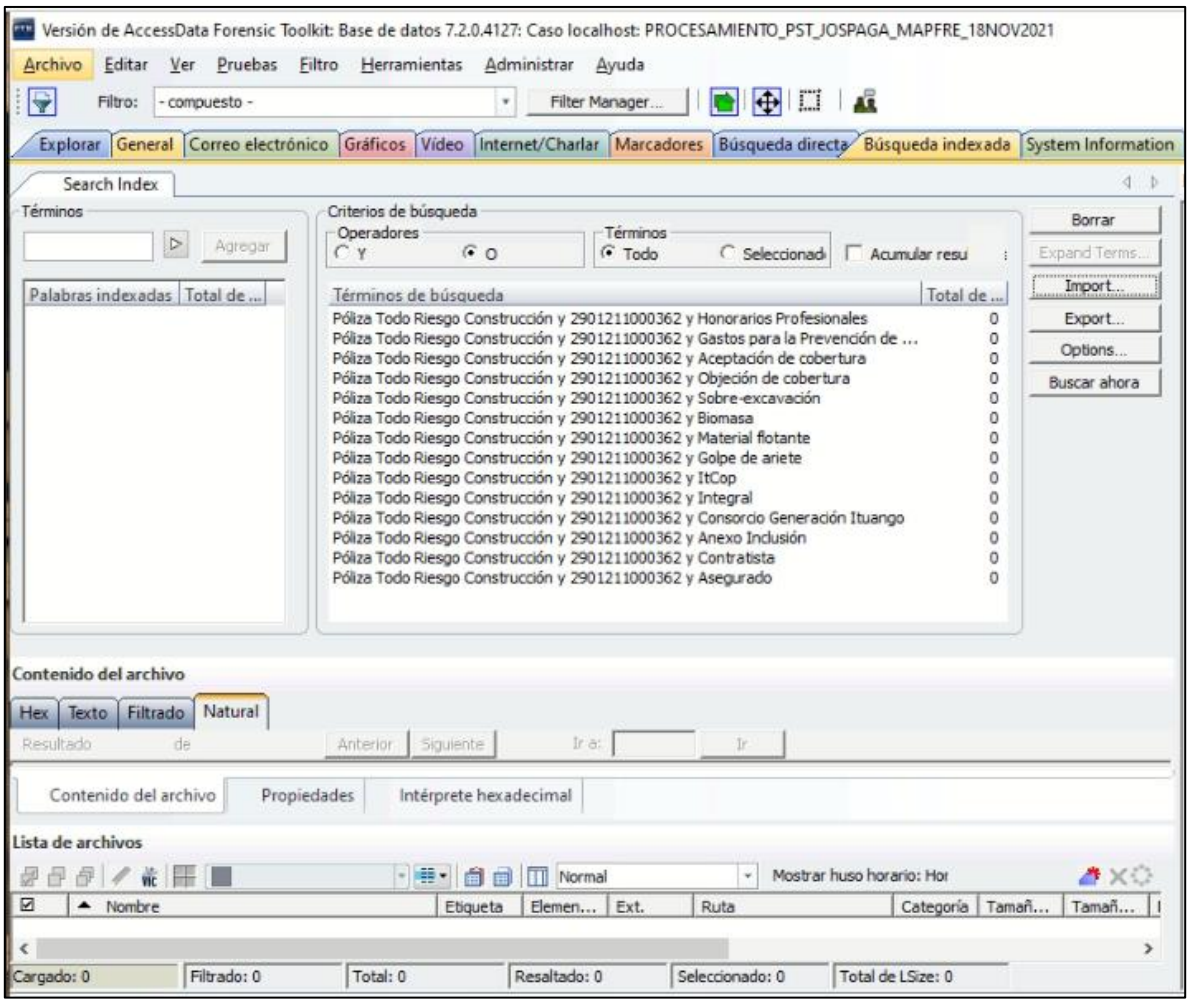
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Veinticinco (25)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo jospaga@mapfre.com.co asignado a **José Fernando PALACIO GALLÓN** para el desarrollo de sus funciones.

4. Buzón de correo electrónico ctorres@mapfre.com.co.

El día 18 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **CTORRES**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

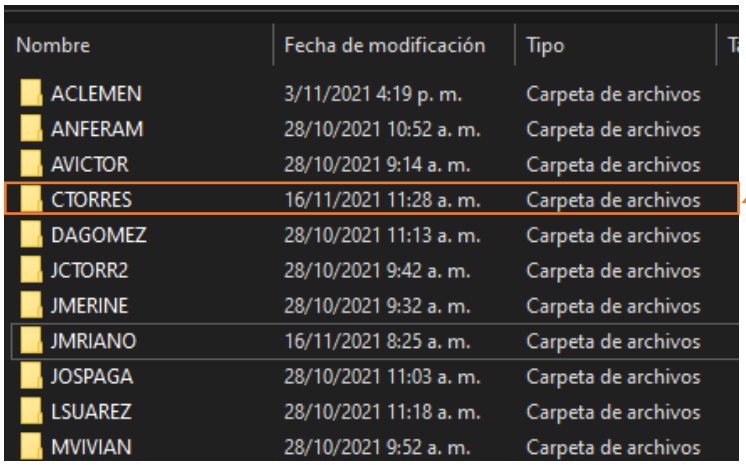


Ilustración 34 Visualización carpeta CTORRES.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **CTORRES** identificada dentro del disco duro como se observa en las siguientes imágenes:

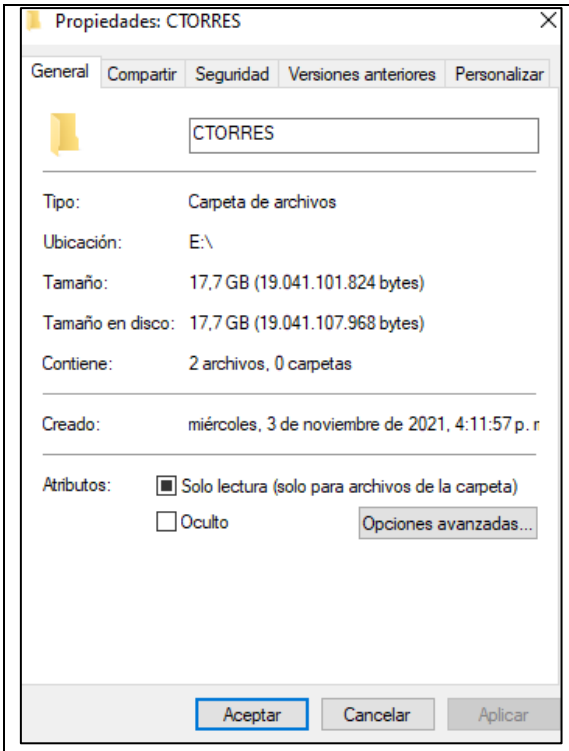


Ilustración 35 Propiedades de la carpeta CTORRES visto desde el Disco Duro.

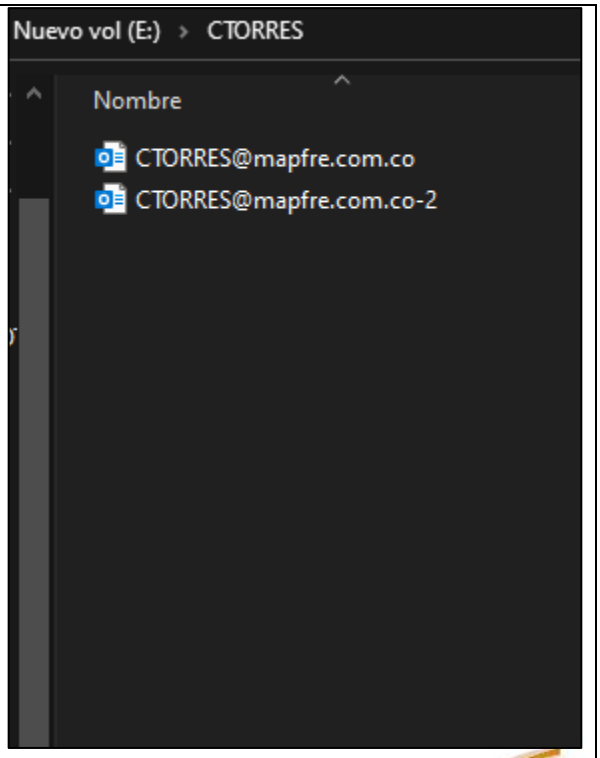


Ilustración 36 Contenido de la carpeta CTORRES visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**ctorres@mapfre.com.co**" asignado a

Carmenza GUATAVITA TORRES para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **12:37:10** y culminando el mismo de forma satisfactoria a las **13:44:09**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_18NOV2021
Número de prueba: 004_CTORRES
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO CTORRES@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad1:
[Custom Content Sources]
E::E:\|CTORRES|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 25137b08f6c1fc4b57519ff976b5d139
SHA1 checksum: d20019fe0ad8526bbac422c7b8dd475f7225e8e0

Image information:
Acquisition started: Thu Nov 18 12:37:10 2021
Acquisition finished: Thu Nov 18 13:41:31 2021
Segment list:

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad1

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad2

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad3

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad4

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad5

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad6

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad7

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad8

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad9

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad10

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad11

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad12

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad13

Image Verification Results:
Verification started: Thu Nov 18 13:41:31 2021
Verification finished: Thu Nov 18 13:44:09 2021
MD5 checksum: 25137b08f6c1fc4b57519ff976b5d139 : verified

SHA1 checksum: d20019fe0ad8526bbac422c7b8dd475f7225e8e0 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**ctorres@mapfre.com.co**" asignado a **Carmenza GUATAVITA TORRES** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados,

esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 37 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO CTORRES@MAPFRE.COM.CO.**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico ctorres@mapfre.com.co asignada **Carmenza GUATAVITA TORRES** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño
4	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Carmenza GUATAVITA TORRES → ctorres@mapfre.com.co	ad1	**17,7 GB**
TOTAL					**17,7 GB**

Tabla 9 Detalle del buzón de correo electrónico asignado ctorres@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico **ctorres@mapfre.com.co** asignado a **Carmenza GUATAVITA TORRES** para el desarrollo de sus funciones **aloja** un total de **17,7 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Un millón ciento cincuenta y siete mil novecientos doce (1.157.912)** archivos (incluyendo carpetas), como se observa a continuación.

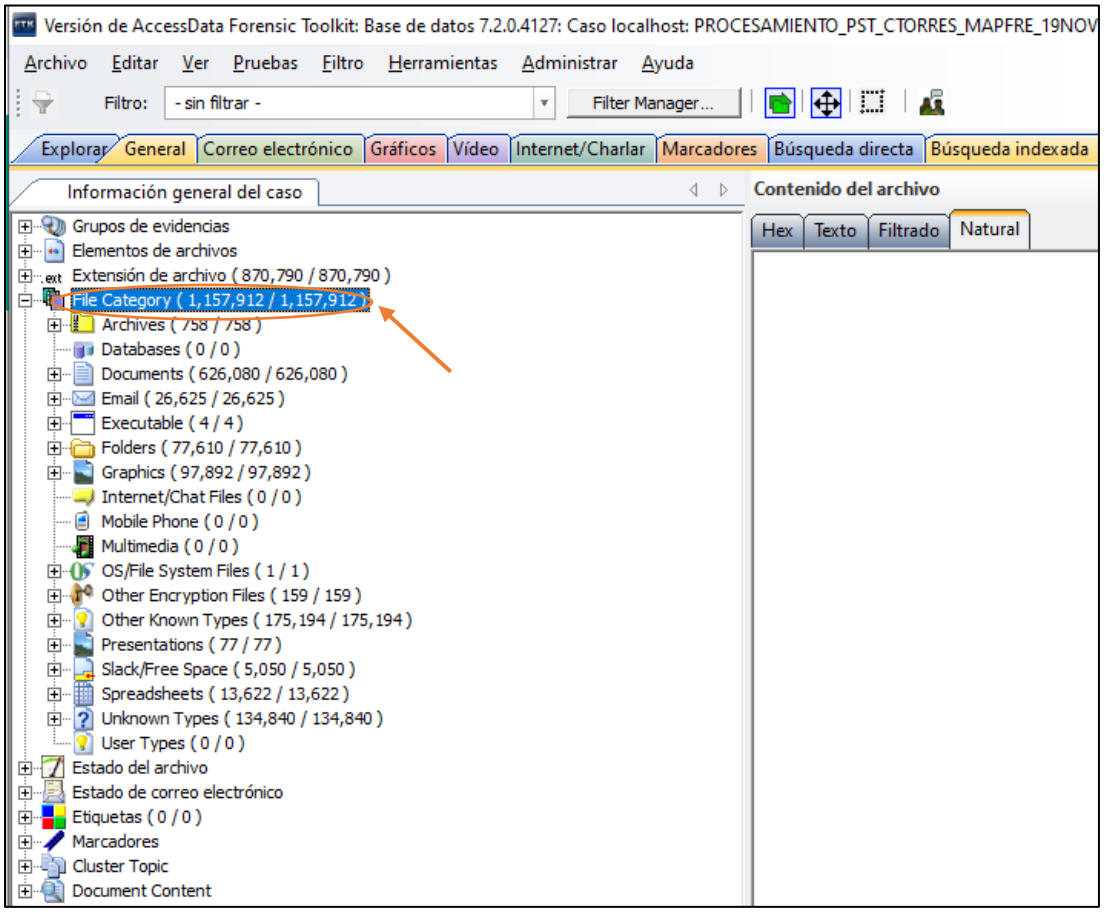


Ilustración 38 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico ctorres@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO CARMENZA GUATAVITA TORRES → CTORRES@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos,

en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico ctorres@mapfre.com.co asignada a Carmenza GUATAVITA TORRES para el desarrollo de sus funciones, iniciando el día el **23** de noviembre del presente año con una duración aproximada de Un (1) día calendario, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Diez mil setecientos ochenta y ocho (10.788)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

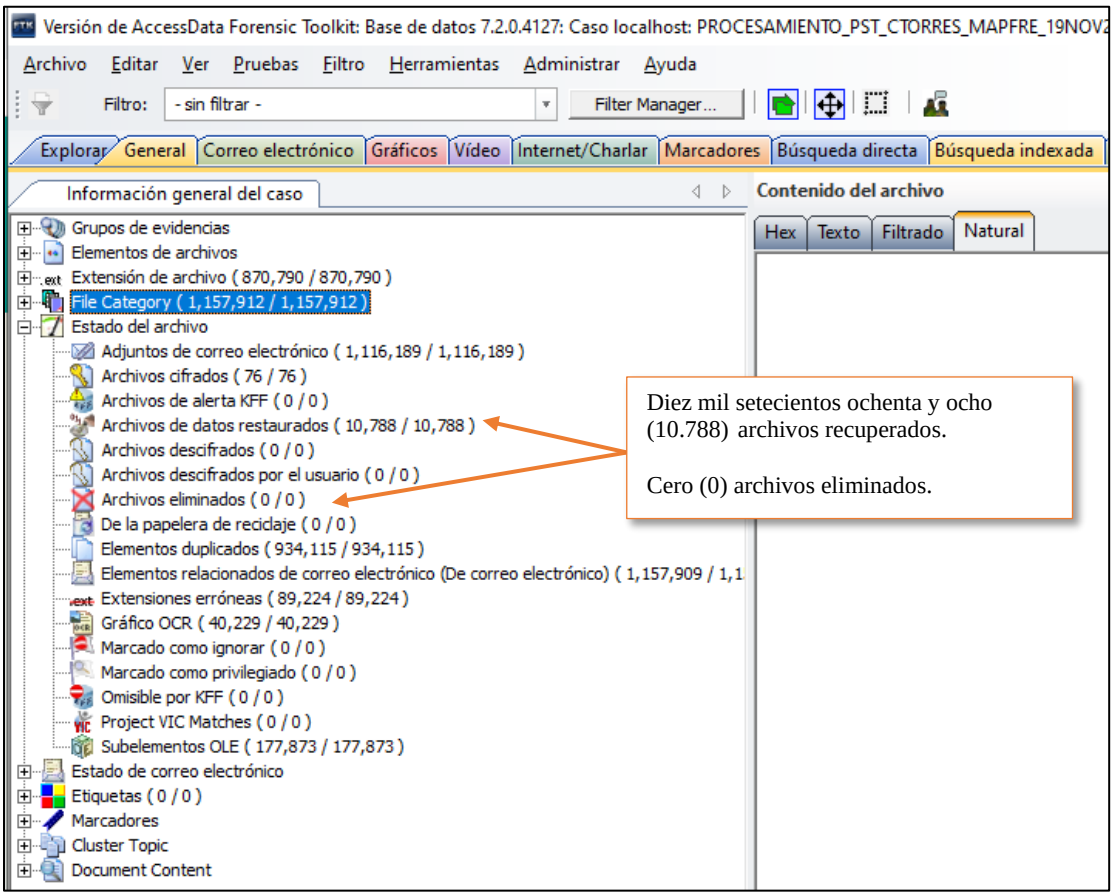


ilustración 39 Total de archivos recuperados en la cuenta de correo electrónico ctorres@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Un millón ciento cincuenta y siete mil novecientos doce**

(1.157.912) archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

- **RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO CTORRES@MAPFRE.COM.CO.**

Luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico ctorres@mapfre.com.co asignada a **Carmenza GUATAVITA TORRES** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	758
2	Documentos	626.080
3	Correo Electrónico	26.625
4	Ejecutables	4
5	Carpetas	77.610
6	Gráficos	97.892
7	Archivos del sistema	1
8	Otros archivos encriptados	159
9	Otros archivos desconocidos	175.194
10	Presentaciones	77
11	Espacio libre	5.050
12	Hojas de cálculo	13.622
13	Tipos de archivos desconocidos	134.840
TOTAL		**1.157.912**

Tabla 10 Información buscada evidencia 004_CTORRES, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Un millón ciento cincuenta y siete mil novecientos doce (1.157.912).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Un millón ciento dieciséis mil ciento ochenta y nueve (1.116.189) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Setenta y seis (76) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Diez mil setecientos ochenta y ocho (10.788) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Novecientos treinta y cuatro mil ciento quince (934.115) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **n millón ciento cincuenta y siete mil novecientos nueve (1.157.909) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Ochenta y nueve mil doscientos veinticuatro (89.224) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Cuarenta mil doscientos veintinueve (40.229) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Ciento setenta y siete mil ciento ochenta y tres (177.183) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico ctorres@mapfre.com.co asignada a **Carmenza GUATAVITA** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

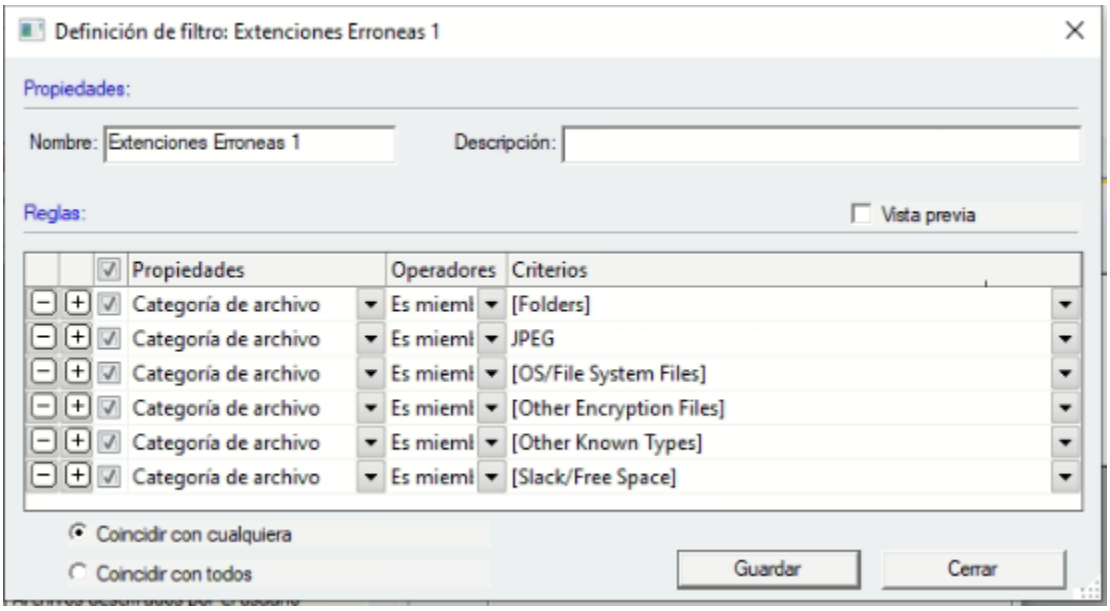


Ilustración 40 Filtro para excluir las extensiones erróneas.

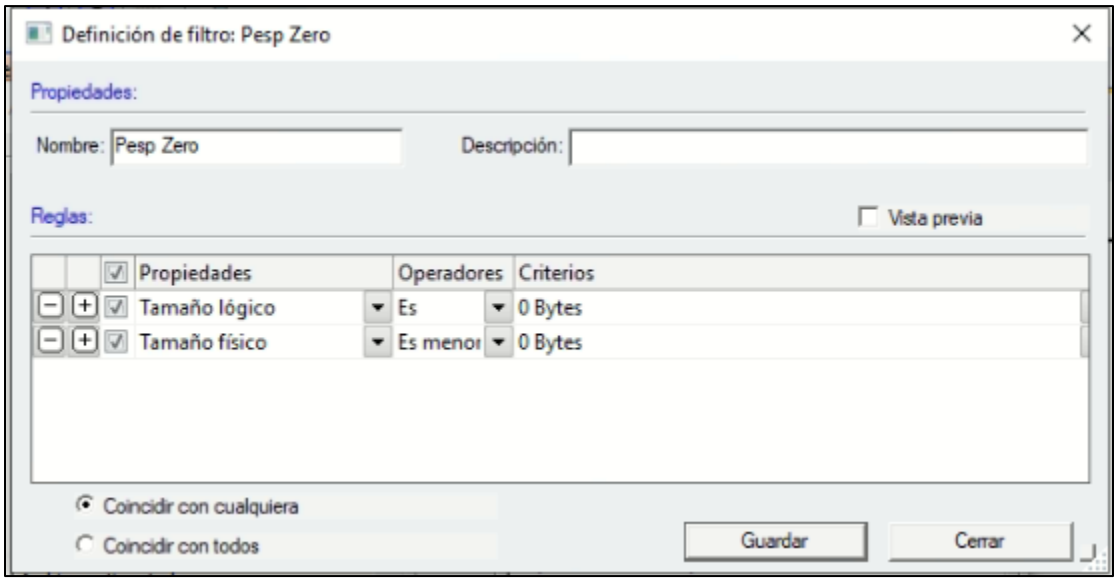


Ilustración 41 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

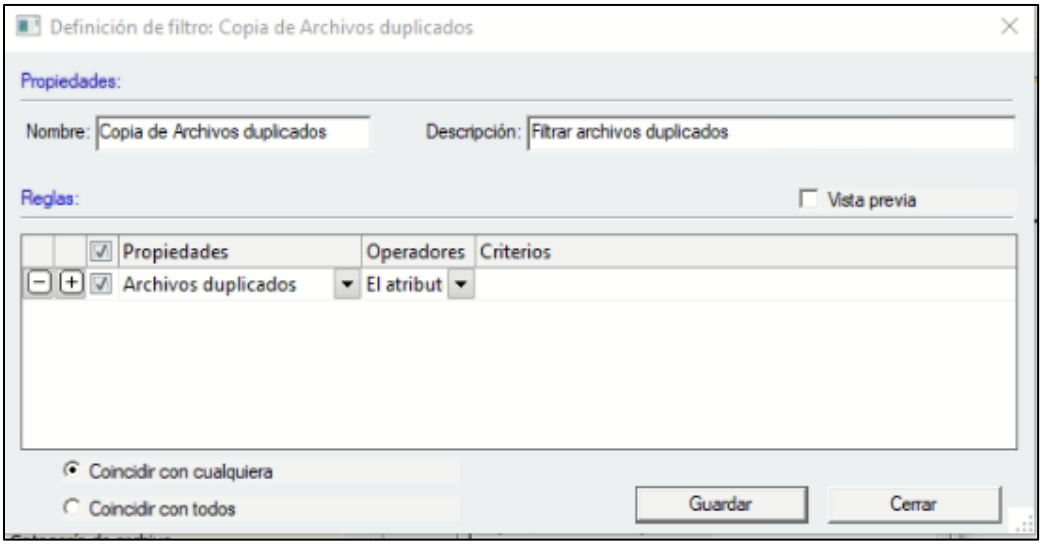
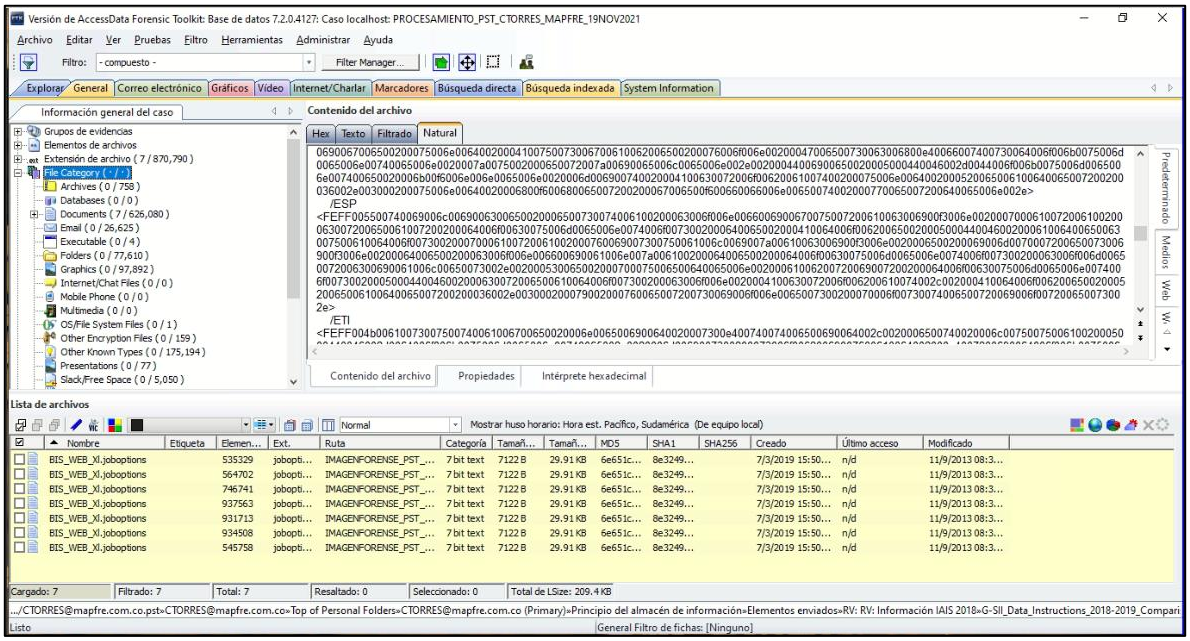


Ilustración 42 Filtro para excluir los archivos duplicados.

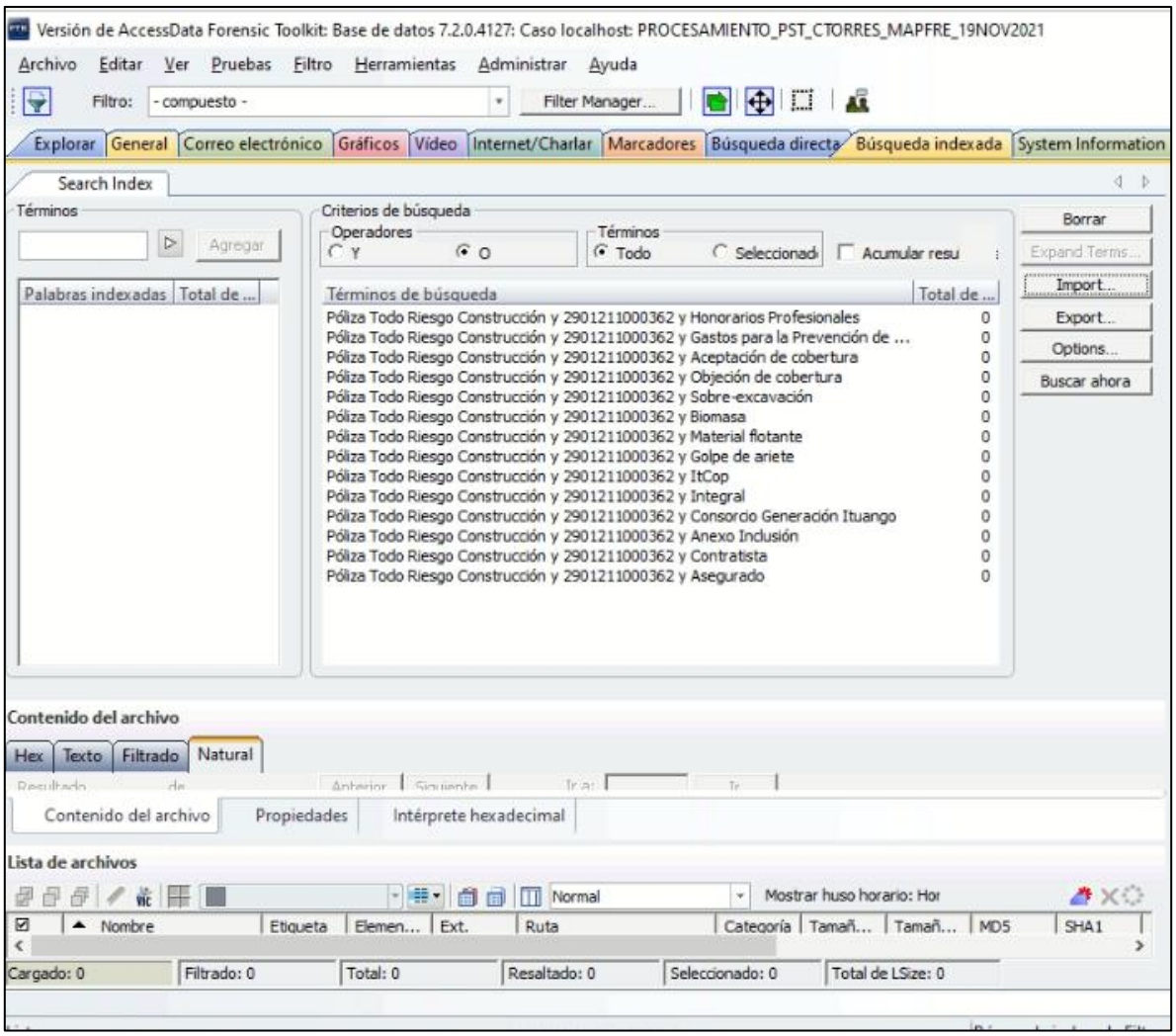
Tras aplicar los filtros anteriormente mencionados, se logra reducir muestra de información a **Siete (7)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo **ctorres@mapfre.com.co** asignada a **Carmenza GUATAVITA TORRES** para el desarrollo de sus funciones.

5. **Buzón de correo electrónico dagomez@mapfre.com.co.**

El día 19 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **DAGOMEZ**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

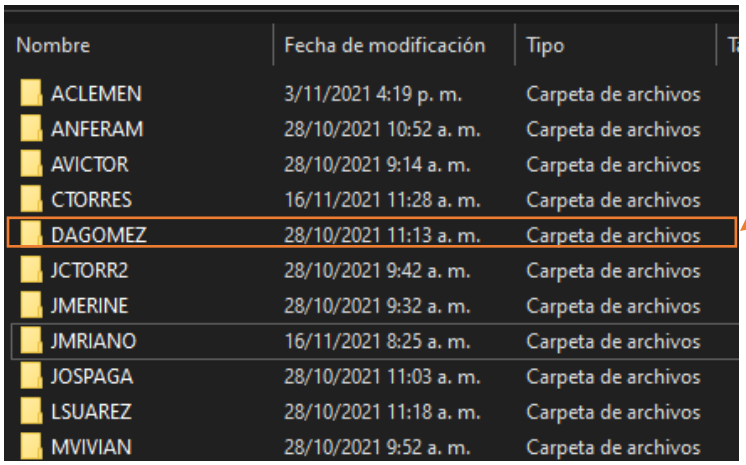


Ilustración 43 Visualización carpeta DAGOMEZ

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **DAGOMEZ** identificada dentro del disco duro como se observa en las siguientes imágenes:

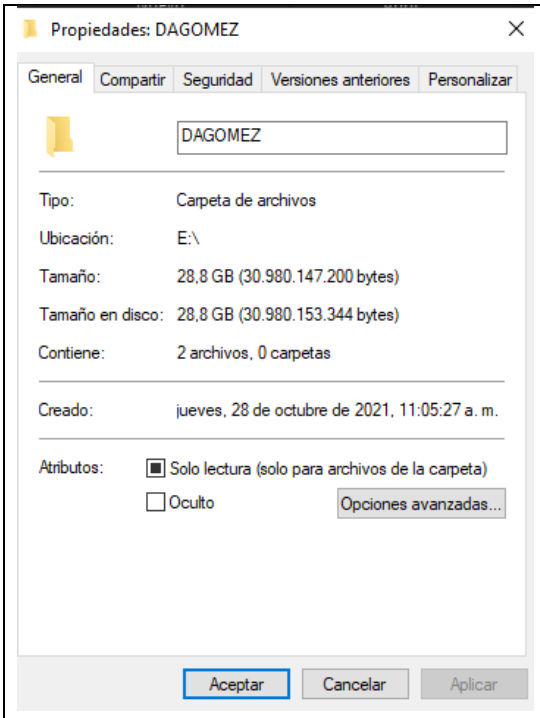


Ilustración 44 Propiedades de la carpeta DAGOMEZ visto desde el Disco Duro.

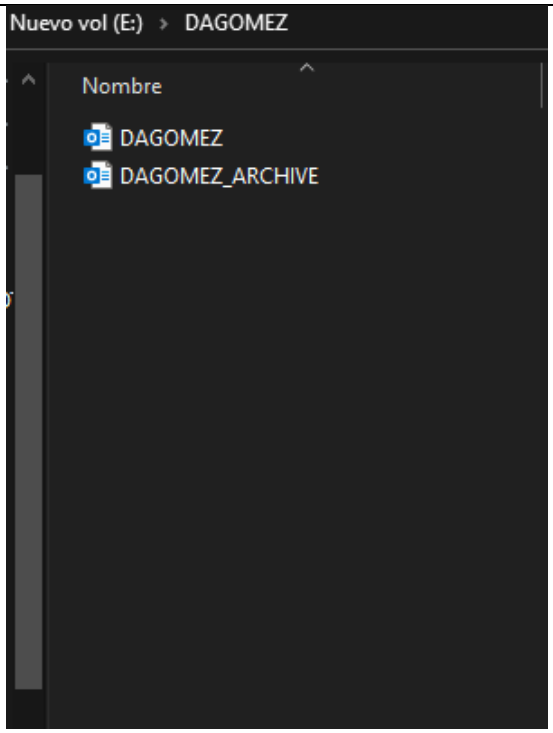


Ilustración 45 Contenido de la carpeta DAGOMEZ visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**dagomez@mapfre.com.co.**" asignado a

David GÓMEZ JIMÉNEZ para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **14:55:13** y culminando el mismo de forma satisfactoria a las **15:05:30**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_19NOV2021
Número de prueba: 005_DAGOMEZ
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO DAGOMEZ@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad1:
[Custom Content Sources]
K::K:\|DAGOMEZ|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 334e31abcf31639ee1a251289be3ac33
SHA1 checksum: b906341ba507626503910b9f85783c073d48a96d

Image information:
Acquisition started: Fri Nov 19 14:55:13 2021
Acquisition finished: Fri Nov 19 15:01:59 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad20

Image Verification Results:
Verification started: Fri Nov 19 15:01:59 2021
Verification finished: Fri Nov 19 15:05:30 2021
MD5 checksum: 334e31abcf31639ee1a251289be3ac33 : verified
SHA1 checksum: b906341ba507626503910b9f85783c073d48a96d : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB,** el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**dagomez@mapfre.com.co.**" asignado a **David GÓMEZ JIMÉNEZ** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 46 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO DAGOMEZ@MAPFRE.COM.CO."**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas MAPFRE SEGUROS GENERALES DE COLOMBIA S.A. para la cuenta de correo electrónico dagomez@mapfre.com.co asignada David GÓMEZ JIMÉNEZ para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
5	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	David GÓMEZ JIMÉNEZ → dagomez@mapfre.com.co	ad1	28.8 GB
TOTAL					**28.8 GB**

Tabla 11 Detalle del buzón de correo electrónico asignado dagomez@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico dagomez@mapfre.com.co asignado a David GÓMEZ JIMÉNEZ para el desarrollo de sus funciones **aloja** un total de **28.8 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Cuatrocientos ochenta y cinco mil setecientos diecinueve (485.719)** archivos (incluyendo carpetas), como se observa a continuación.

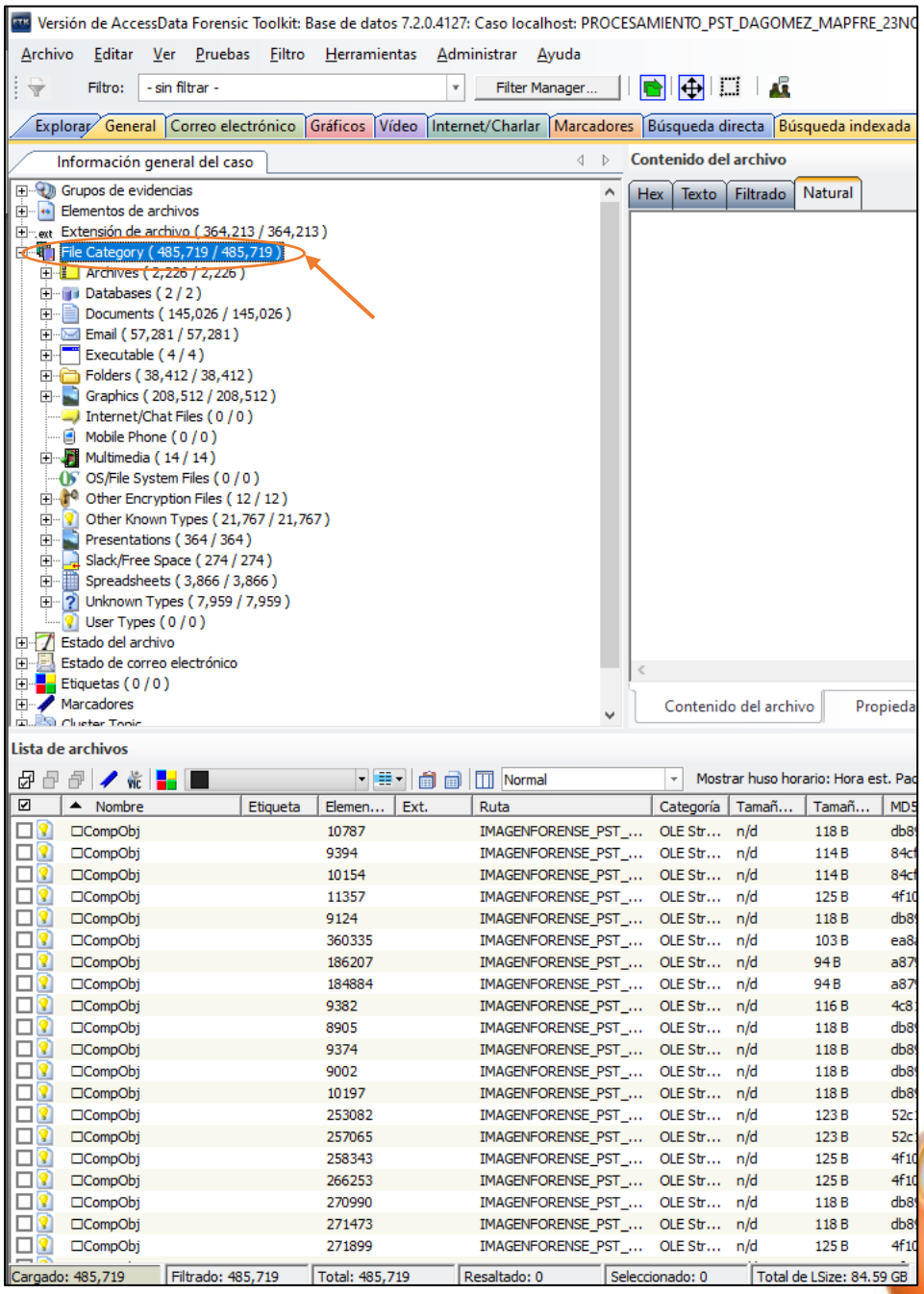


Ilustración 47 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico dagomez@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JOSÉ FERNANDO PALACIO GALLÓN → DAGOMEZ@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico dagomez@mapfre.com.co asignado a **David GÓMEZ JIMÉNEZ,** iniciando el día el **23** de noviembre del presente año con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Ciento diecinueve mil setecientos cuarenta y seis (119.746)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:



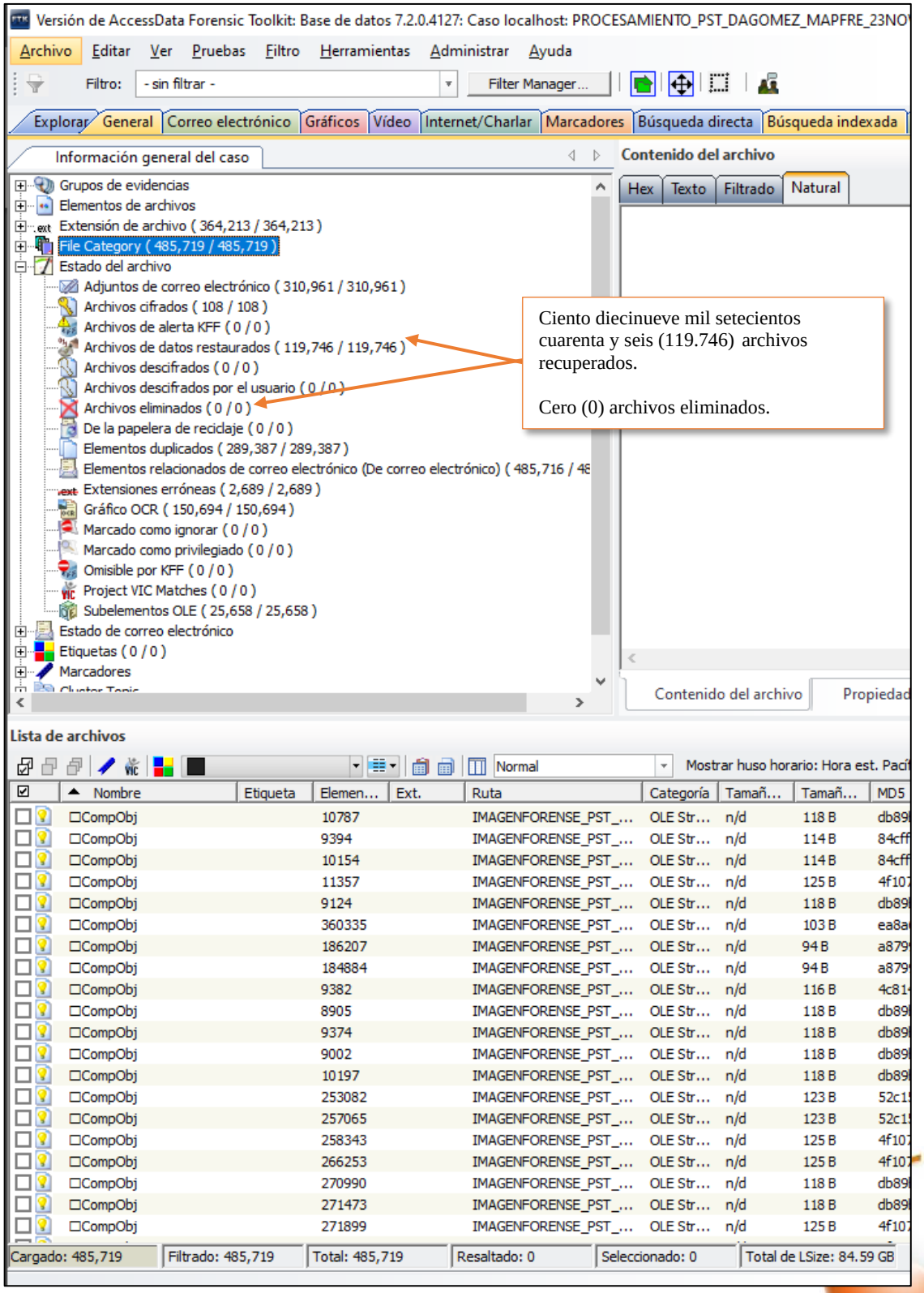


ilustración 48 Total de archivos recuperados en la cuenta de correo electrónico dagomez@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Cuatrocientos ochenta y cinco mil setecientos diecinueve (485.719)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO DAGOMEZ@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico dagomez@mapfre.com.co asignado a David GÓMEZ JIMÉNEZ para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	2.226
2	Bases de Datos	2
3	Documentos	145.026
4	Correo Electrónico	57.281
5	Ejecutables	4
6	Carpetas	38.412
7	Gráficos	208.512
8	Multimedia	14
9	Otros archivos encriptados	12
10	Otros archivos desconocidos	21.767
11	Presentaciones	364
12	Espacio libre	274
13	Hojas de cálculo	3.866
14	Tipos de archivos desconocidos	7.959
TOTAL		**485.719**

Tabla 12 Información buscada evidencia 005_DAGOMEZ, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Cuatrocientos ochenta y cinco mil setecientos diecinueve (485.719)**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Trescientos diez mil novecientos sesenta y un (310.961) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **ciento ocho (108) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Ciento diecinueve mil setecientos cuarenta y seis (119.746) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Doscientos ochenta y nueve mil trescientos ochenta y siete (289.387) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Cuatrocientos ochenta y cinco mil setecientos dieciséis (485.716) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Dos mil seiscientos ochenta y nueve (2.689) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Ciento cincuenta mil seiscientos noventa y cuatro (150.694) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Veinticinco mil seiscientos cincuenta y ocho (25.658) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico dagomez@mapfre.com.co asignado a **David GÓMEZ JIMÉNEZ** para el desarrollo de sus funciones el equipo de ADALID CORP

procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

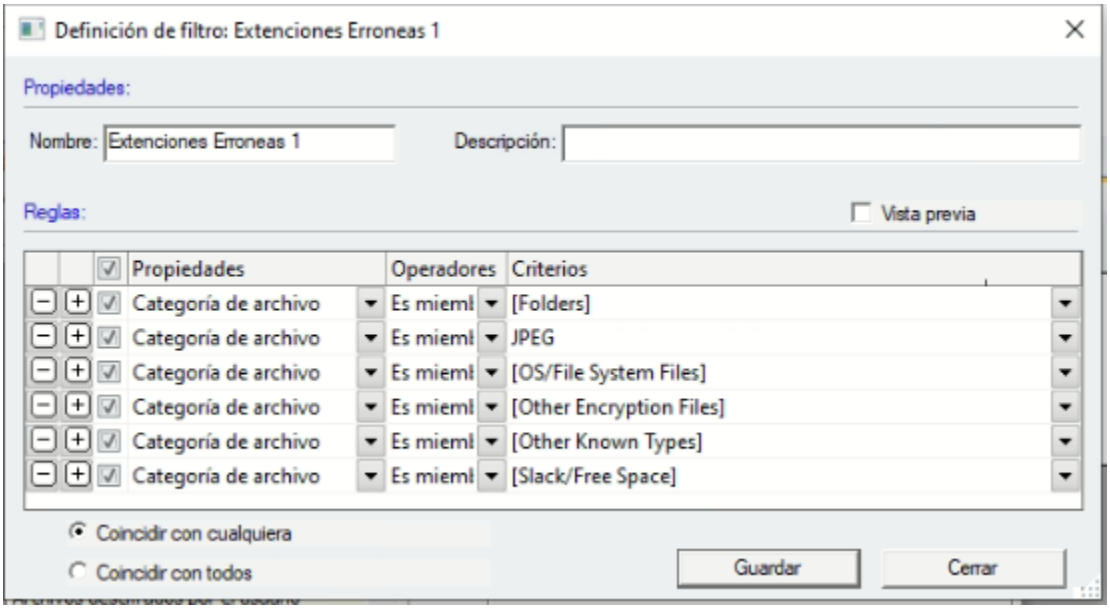


Ilustración 49 Filtro para excluir las extensiones erróneas.

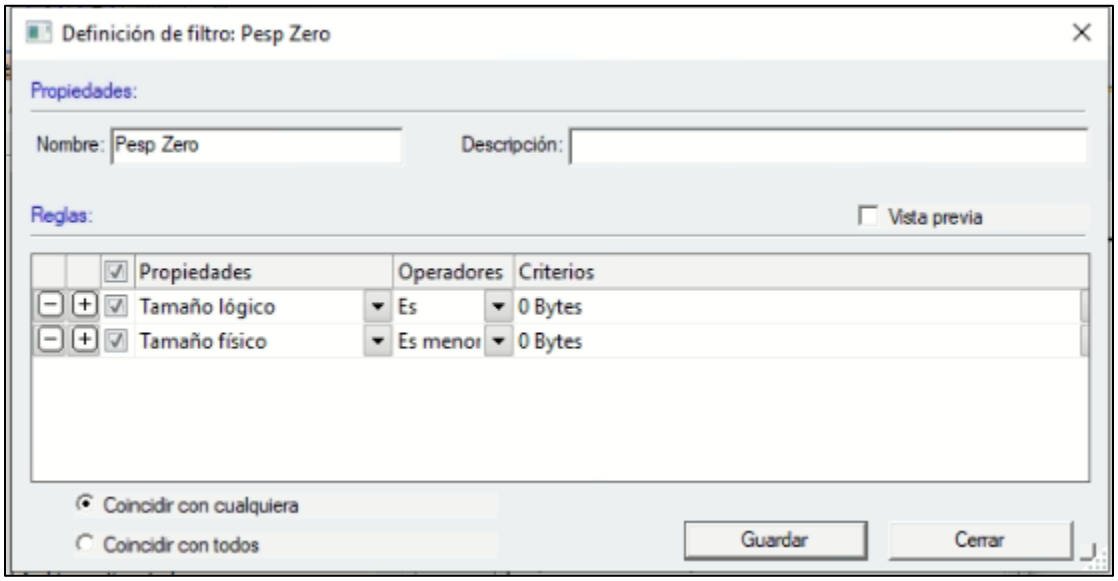


Ilustración 50 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

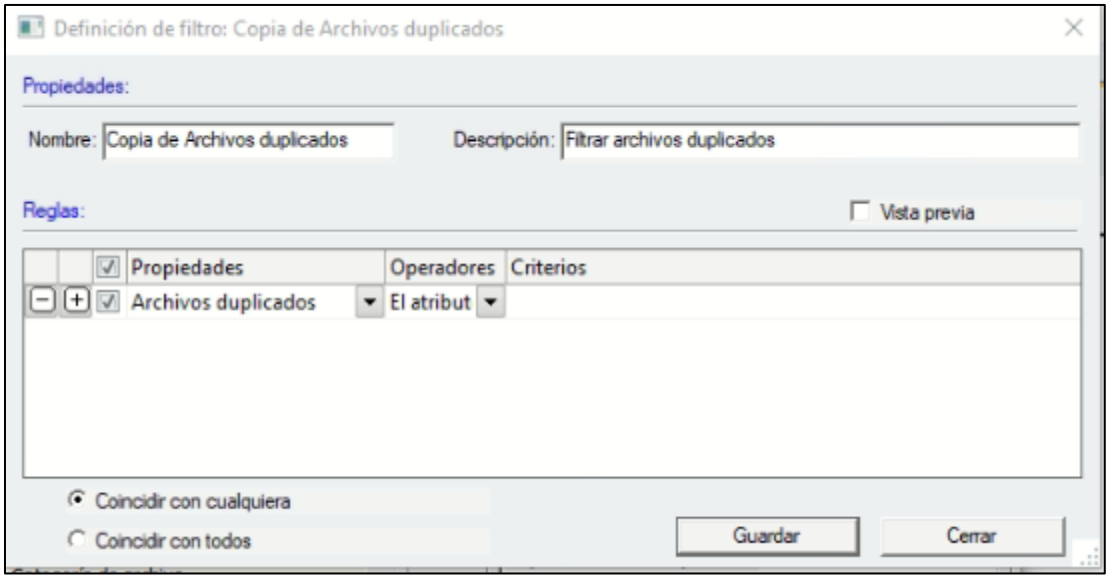


Ilustración 51 Filtro para excluir los archivos duplicados.

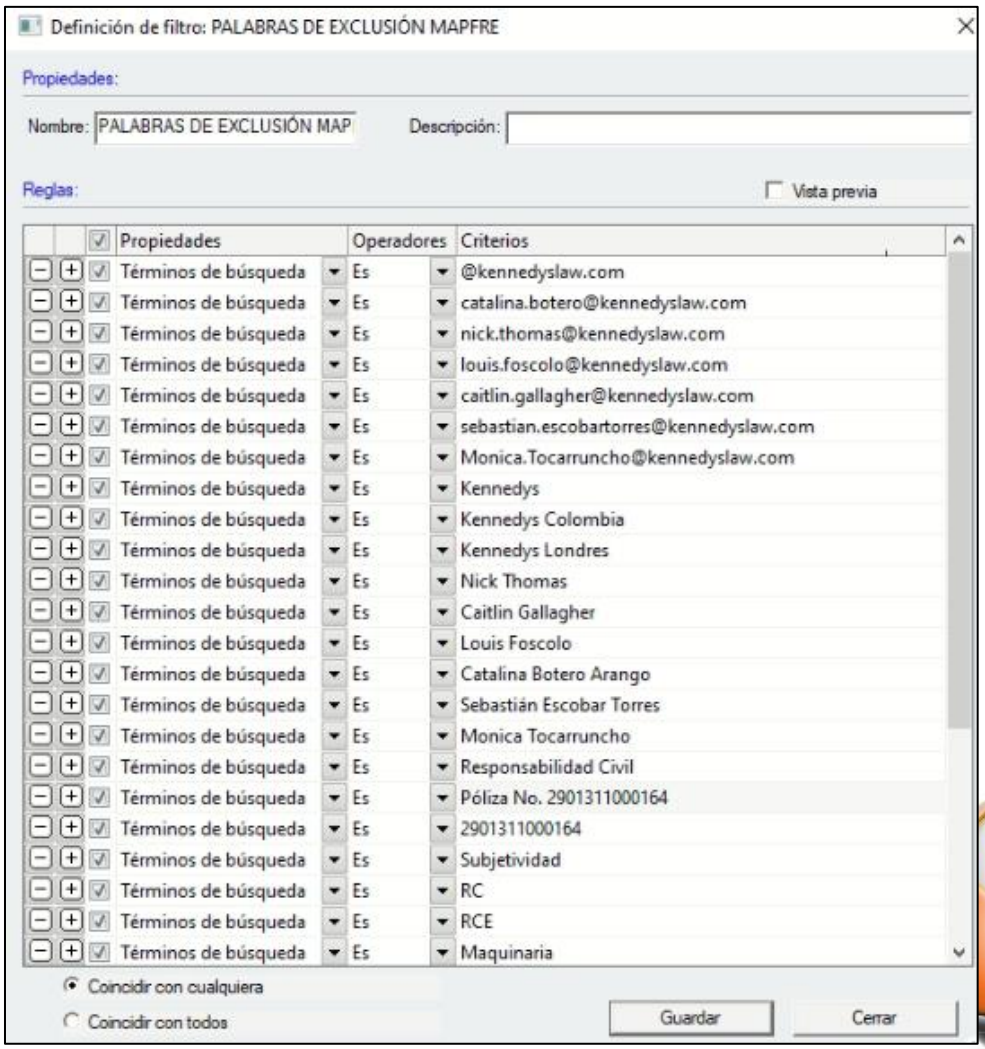


Ilustración 52 Filtro para excluir los archivos suministrado por MAPFRE - 1.

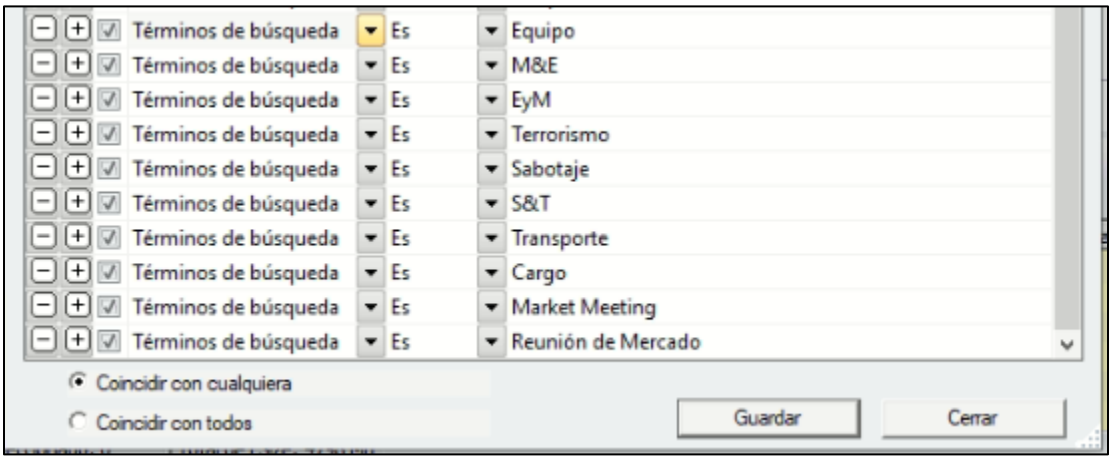
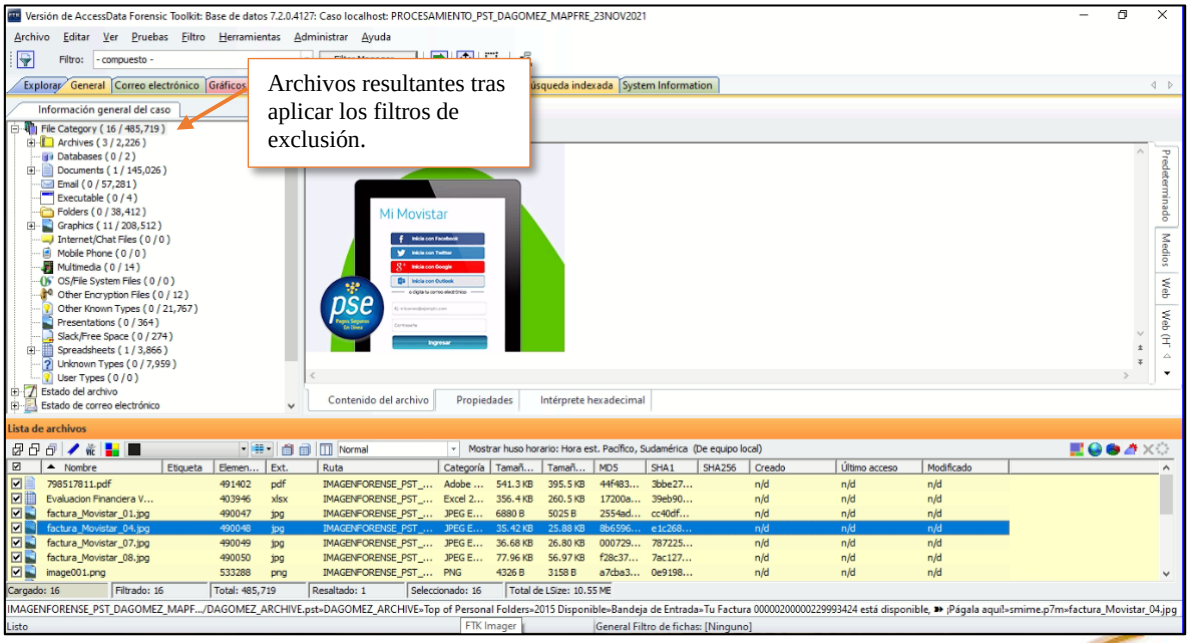


Ilustración 53 Filtro para excluir los archivos suministrado por MAPFRE - 2.

Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Dieciséis (16)** registros como se observa en la siguiente imagen:

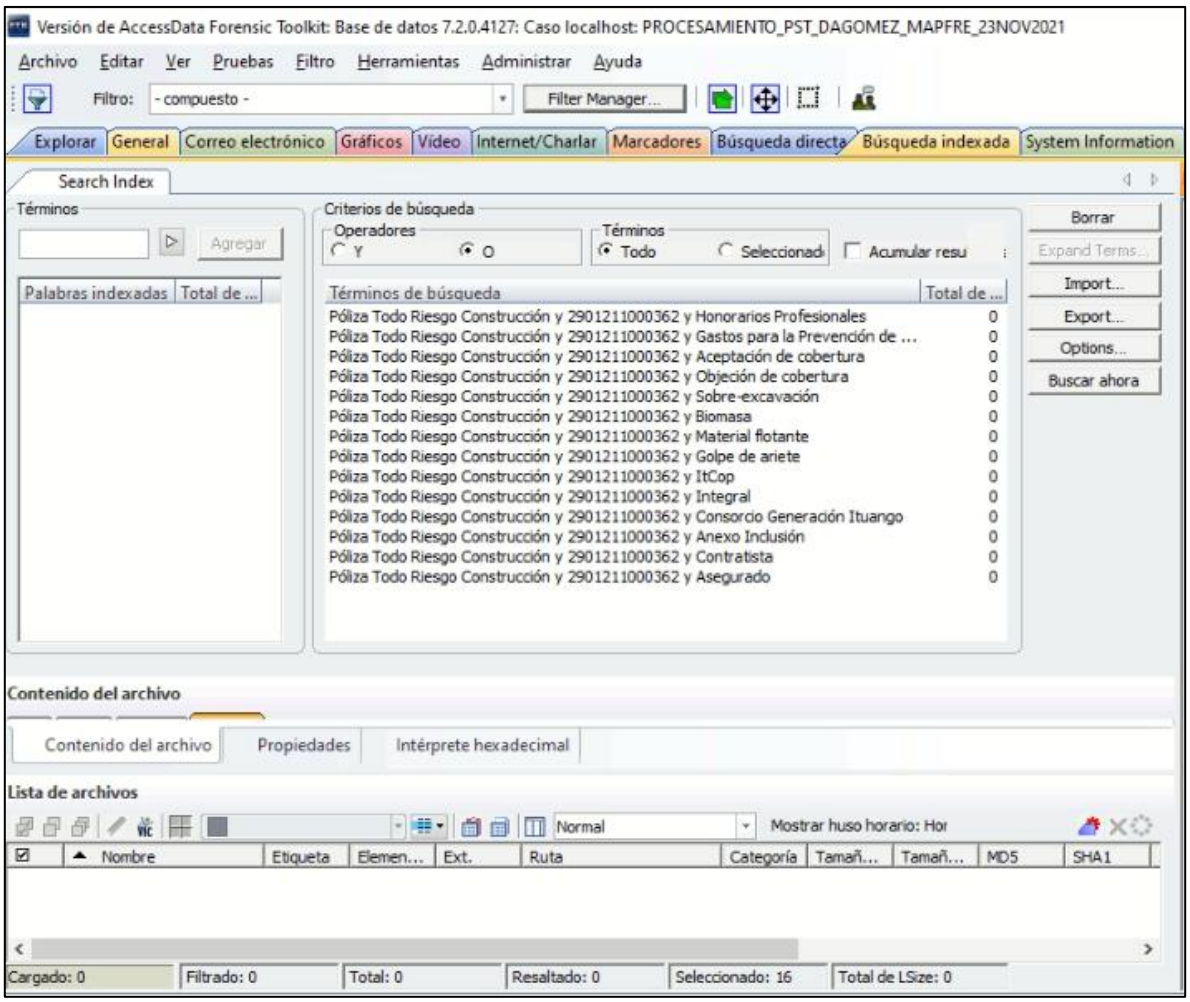


Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión

7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo dagomez@mapfre.com.co asignado a **David GÓMEZ JIMÉNEZ** para el desarrollo de sus funciones.

6. Buzón de correo electrónico lsuarez@mapfre.com.co.

El día 19 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **LSUAREZ**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

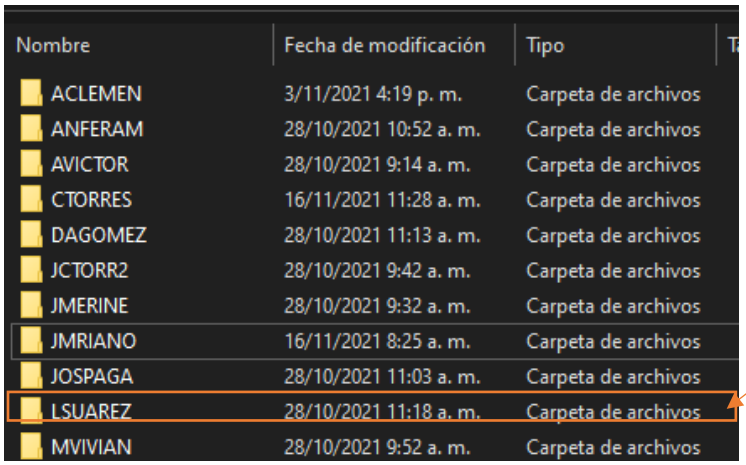


Ilustración 54 Visualización carpeta LSUAREZ

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **LSUAREZ** identificada dentro del disco duro como se observa en las siguientes imágenes:

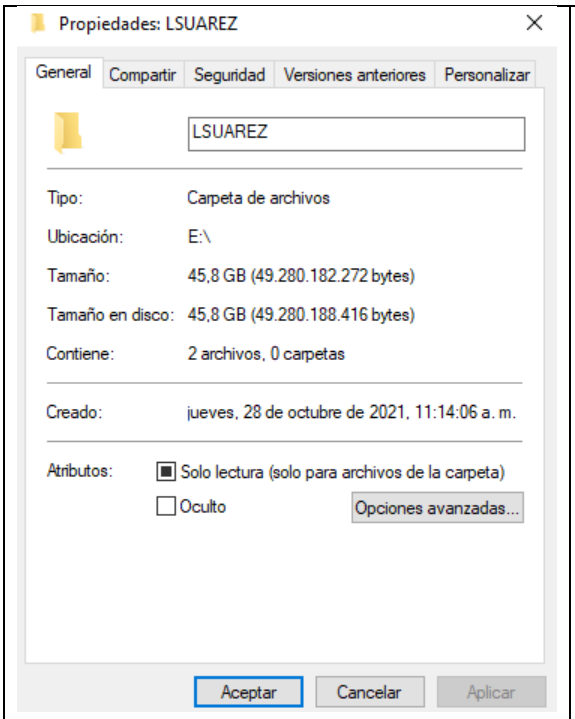


Ilustración 55 Propiedades de la carpeta LSUAREZ visto desde el Disco Duro.

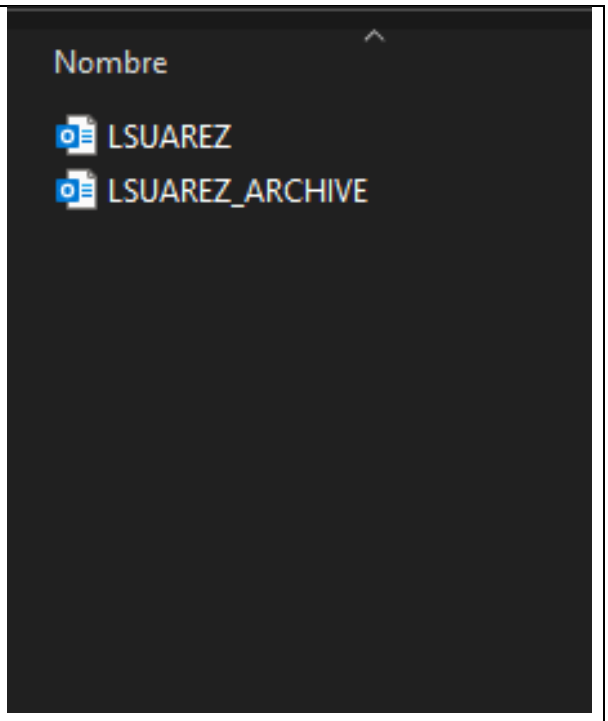


Ilustración 56 Contenido de la carpeta LSUAREZ visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**lsuarez@mapfre.com.co.**" asignado a **Luis Alberto SUÁREZ URREGO** para el cumplimiento de sus funciones los peritos

informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **15:08:28** y culminando el mismo de forma satisfactoria a las **15:24:51**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_19NOV2021
Número de prueba: 006_LSUAREZ
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO LSUAREZ@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad1:
[Custom Content Sources]
K::K:\|LSUAREZ|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 36a5dc50b305d9a816109d85d035ede9
SHA1 checksum: 8734e3612bd6e58f70e833fd1a991fe5b9178b4d

Image information:
Acquisition started: Fri Nov 19 15:08:28 2021
Acquisition finished: Fri Nov 19 15:19:44 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad29

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad30

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad31

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad32

Image Verification Results:
Verification started: Fri Nov 19 15:19:50 2021
Verification finished: Fri Nov 19 15:24:51 2021
MD5 checksum: 36a5dc50b305d9a816109d85d035ede9 : verified
SHA1 checksum: 8734e3612bd6e58f70e833fd1a991fe5b9178b4d : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:





Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**lsuarez@mapfre.com.co.**" asignado a **Luis Alberto SUÁREZ URREGO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 57 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO LSUAREZ@MAPFRE.COM.CO."**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo

electrónico lsuarez@mapfre.com.co asignada **Luis Alberto SUÁREZ URREGO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
6	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Luis Alberto SUÁREZ URREGO → lsuarez@mapfre.com.co	ad1	45.8 GB
TOTAL					**45.8 GB**

Tabla 13 Detalle del buzón de correo electrónico asignado lsuarez@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico lsuarez@mapfre.com.co asignado a **Luis Alberto SUÁREZ URREGO** para el desarrollo de sus funciones **aloja** un total de **45.8 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Setecientos treinta y ocho mil doscientos setenta y cuatro (738.274)** archivos (incluyendo carpetas), como se observa a continuación.

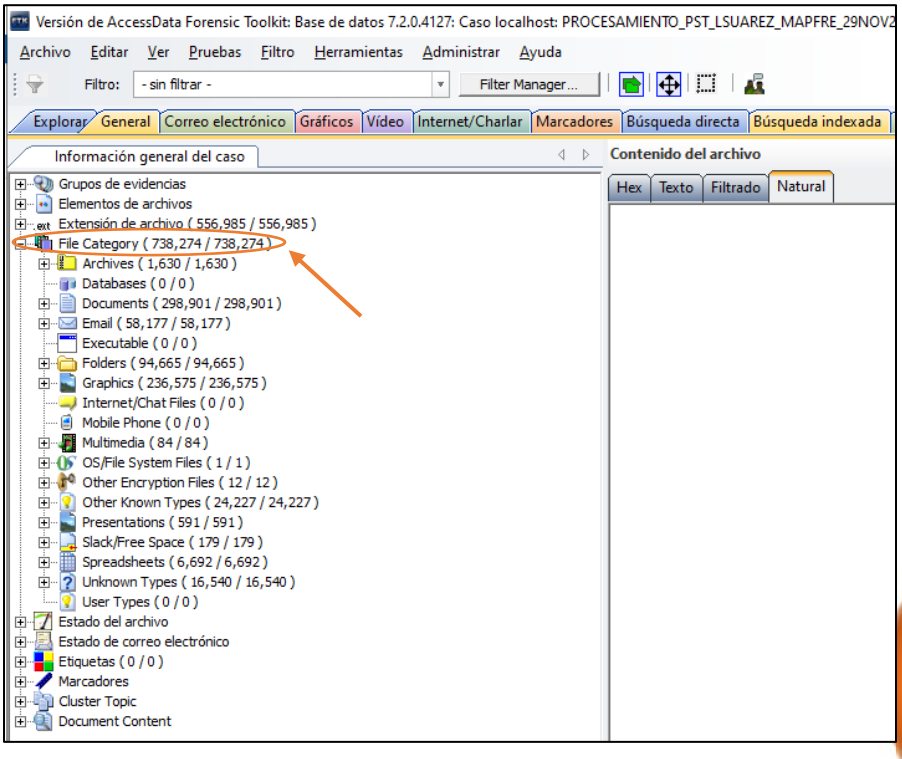


Ilustración 58 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico lsuarez@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO LUIS ALBERTO SUÁREZ URREGO → LSUAREZ@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico lsuarez@mapfre.com.co asignado a **Luis Alberto SUÁREZ URREGO**, iniciando el día el **29** de noviembre del presente año con una duración aproximada de Un (7) día calendario, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Ciento treinta y nueve mil ciento cincuenta y ocho (139.158)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

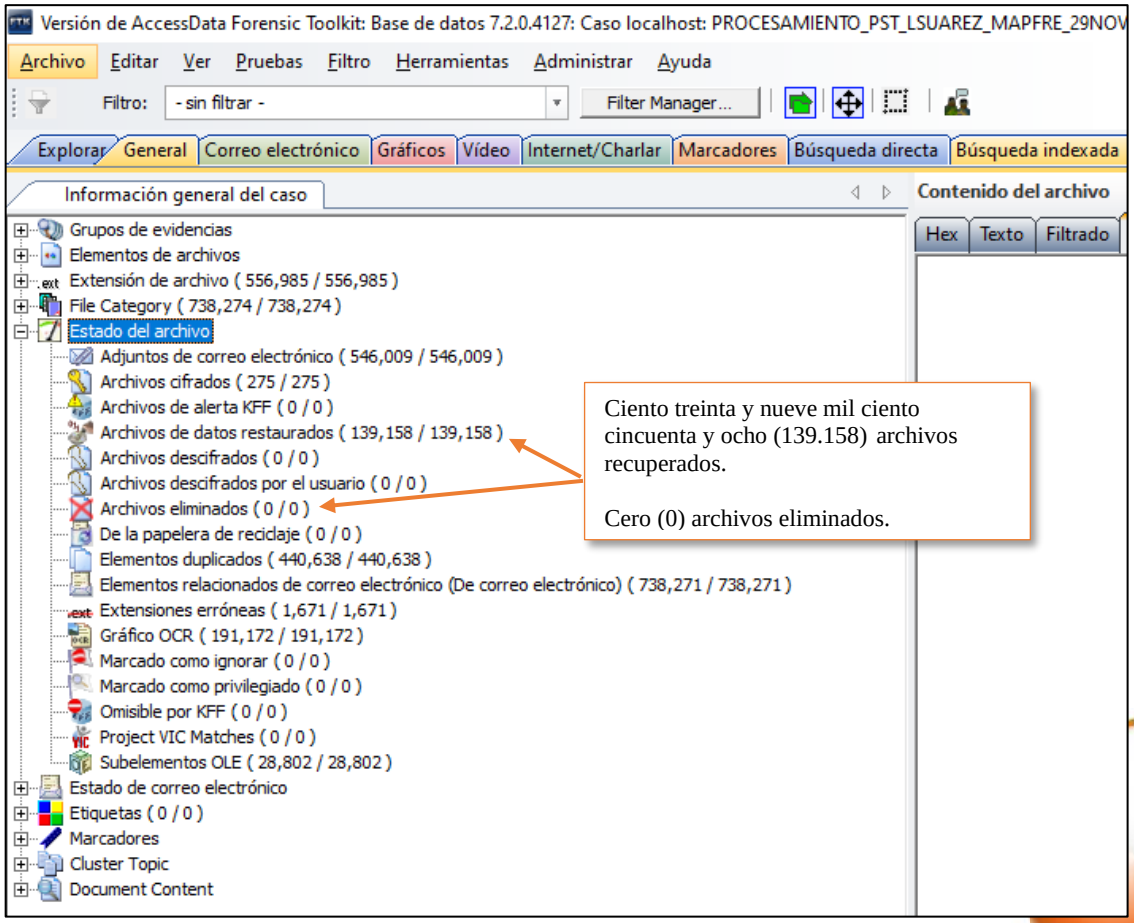


ilustración 59 Total de archivos recuperados en la cuenta de correo electrónico lsuarez@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Setecientos treinta y ocho mil doscientos setenta y cuatro (738.274)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO LSUAREZ@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico lsuarez@mapfre.com.co asignado a **Luis Alberto SUÁREZ URREGO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1.630
2	Documentos	298.901
3	Correo Electrónico	58.177
4	Carpetas	94.665
5	Gráficos	236.575
6	Multimedia	84
7	Archivos del sistema	1
8	Otros archivos encriptados	12
9	Otros archivos desconocidos	24.227
10	Presentaciones	591
11	Espacio libre	179
12	Hojas de cálculo	6.692
13	Tipos de archivos desconocidos	16.540
TOTAL		**738.274**

Tabla 14 Información buscada evidencia 006_LSUAREZ, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Setecientos treinta y ocho mil doscientos setenta y cuatro (738.274).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Quinientos cuarenta y seis mil nueve (546.009) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Doscientos setenta y cinco (275) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Ciento treinta y nueve mil ciento cincuenta y ocho (139.158) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Cuatrocientos cuarenta mil seiscientos treinta y ocho (440.638) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Setecientos treinta y ocho mil doscientos setenta y un (738.271) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Mil seiscientos setenta y un (1.671) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Ciento noventa y un mil ciento setenta y dos (191.172) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Veintiocho mil ochocientos dos (28.802) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo lsuarez@mapfre.com.co asignado **a Luis Alberto SUÁREZ URREGO** para el desarrollo de sus funciones el equipo de ADALID CORP procede a

aplicar filtros para excluir la información que no se requiere de la siguiente manera:

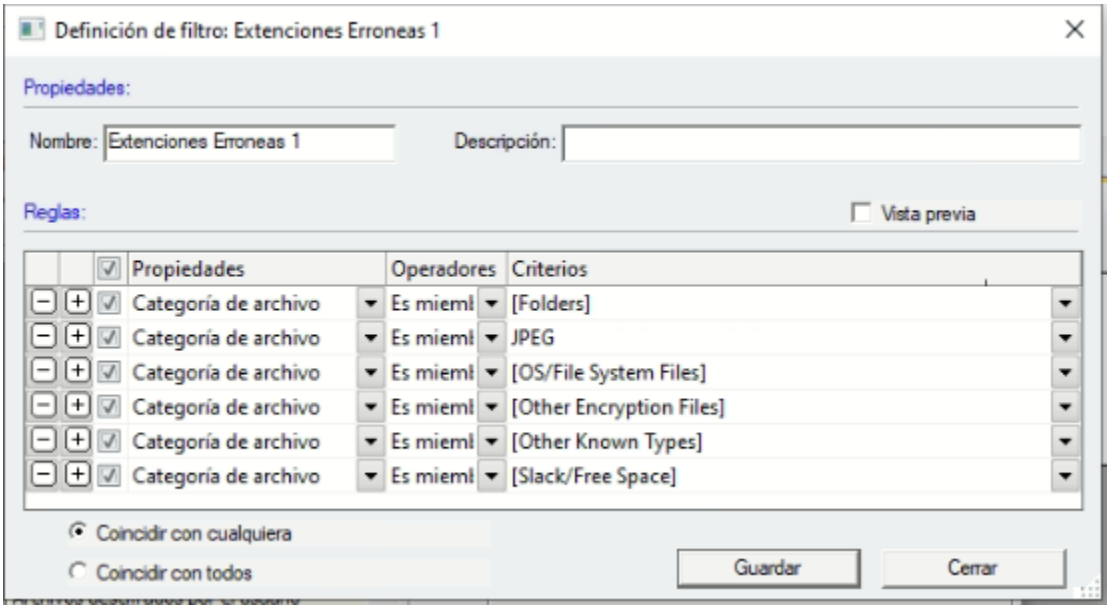


Ilustración 60 Filtro para excluir las extensiones erróneas.

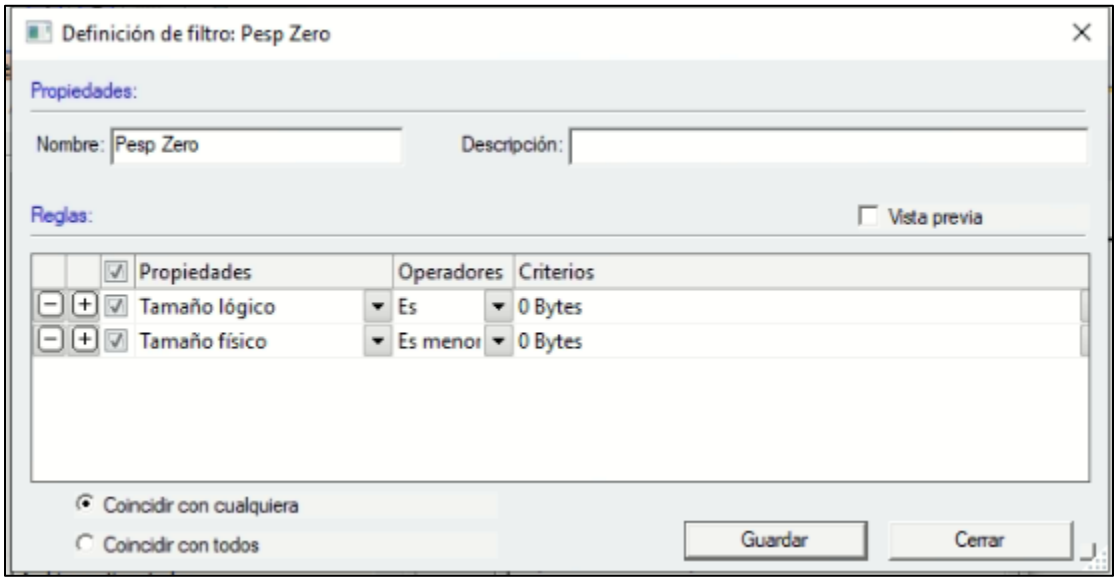


Ilustración 61 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

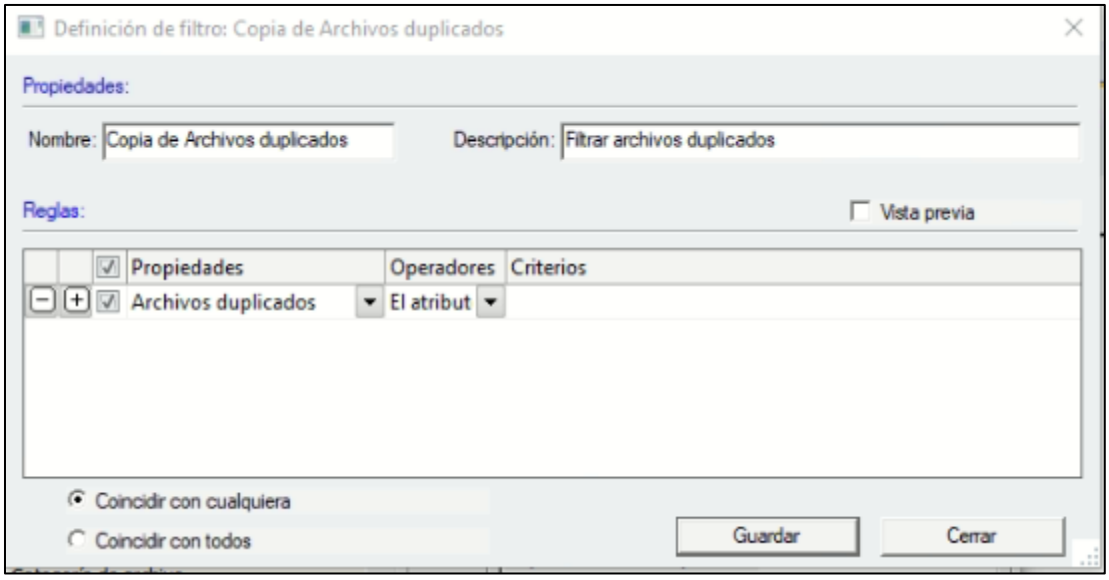


Ilustración 62 Filtro para excluir los archivos duplicados.

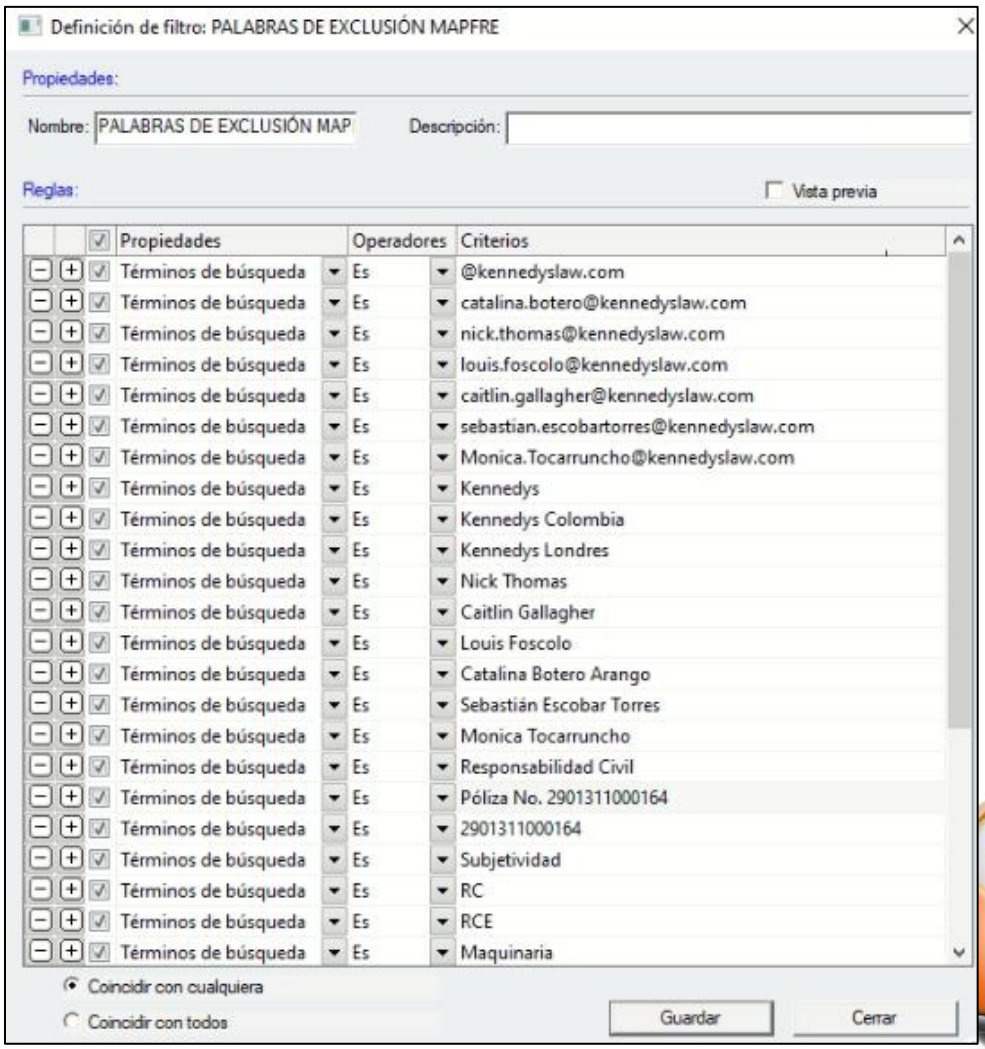


Ilustración 63 Filtro para excluir los archivos suministrado por MAPFRE - 1.

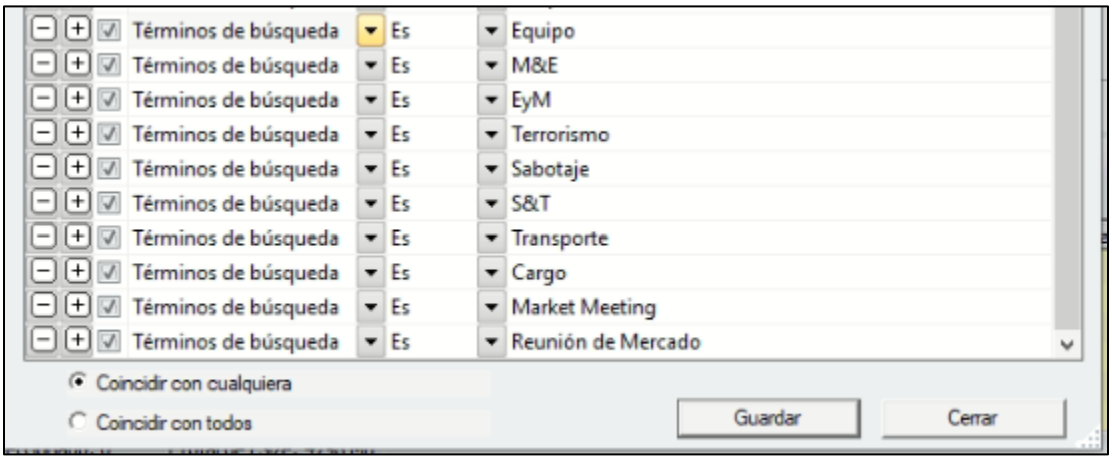
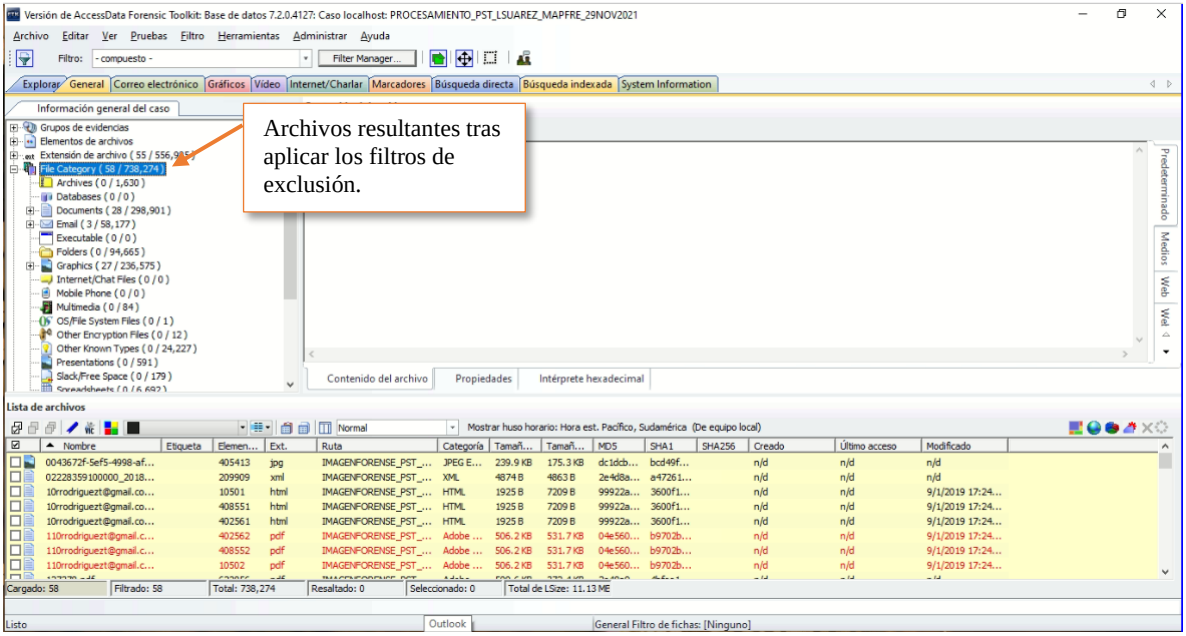


Ilustración 64 Filtro para excluir los archivos suministrado por MAPFRE - 2.

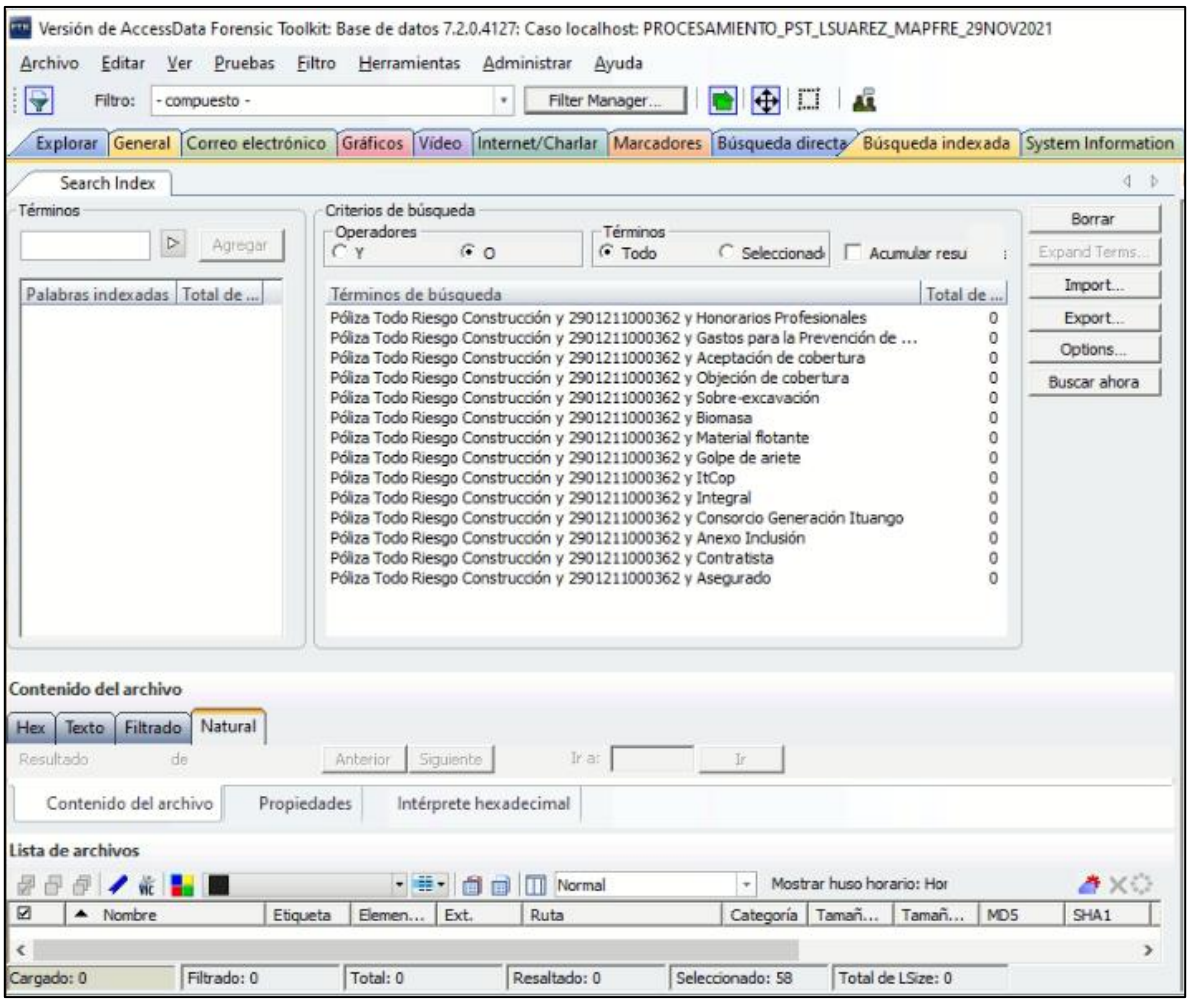
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Cincuenta y ocho (58)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo lsuarez@mapfre.com.co asignado a **Luis Alberto SUÁREZ URREGO** para el desarrollo de sus funciones.

7. Buzón de correo electrónico anferam@mapfre.com.co.

El día 19 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **ANFERAM**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

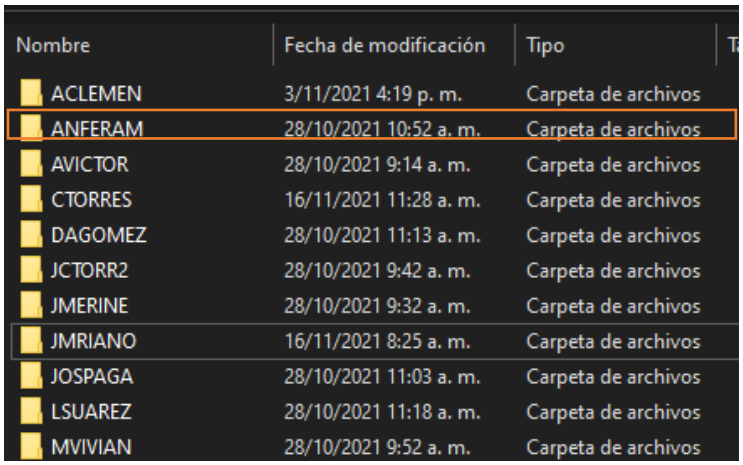


Ilustración 65 Visualización carpeta ANFERAM.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **ANFERAM** identificada dentro del disco duro como se observa en las siguientes imágenes:

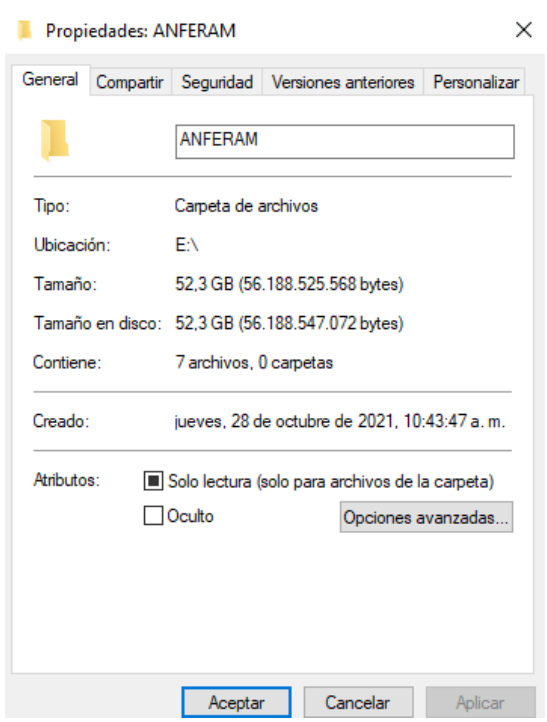


Ilustración 66 Propiedades de la carpeta ANFERAM visto desde el Disco Duro.

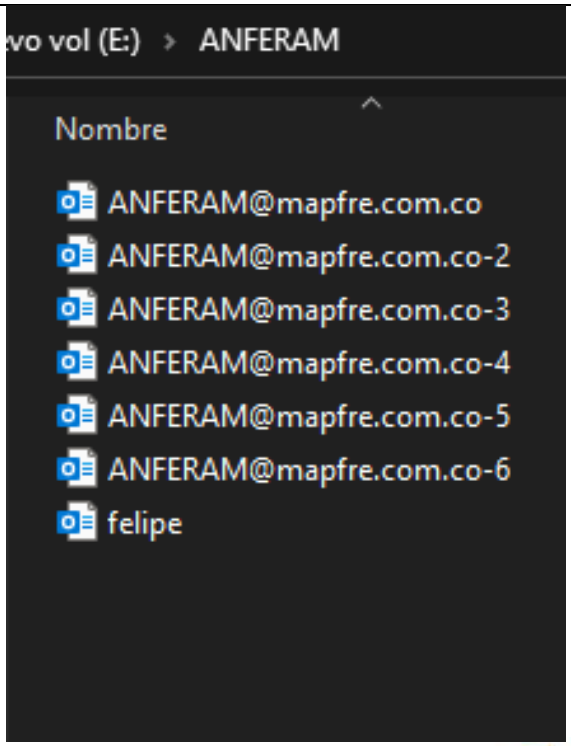


Ilustración 67 Contenido de la carpeta ANFERAM visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**anferam@mapfre.com.co.**" asignado a

Andrés Felipe RAMÍREZ para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **15:34:32** y culminando el mismo de forma satisfactoria a las **15:54:44**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_19NOV2021
Número de prueba: 007_ANFERAM
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ANFERAM@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad1:
[Custom Content Sources]
K::K:\ | ANFERAM | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: d534e4492f211de5338af83951c38c46
SHA1 checksum: 9d747d52eabeadd3571ddf2033cba1cc4c2c6bd7

Image information:
Acquisition started: Fri Nov 19 15:34:32 2021
Acquisition finished: Fri Nov 19 15:49:39 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad29 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad30 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad31 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad32 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad33 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad34 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad35 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad36 Image Verification Results: Verification started: Fri Nov 19 15:49:39 2021 Verification finished: Fri Nov 19 15:54:44 2021 MD5 checksum: d534e4492f211de5338af83951c38c46 : verified SHA1 checksum: 9d747d52eabeadd3571ddf2033cba1cc4c2c6bd7 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**anferam@mapfre.com.co.**" asignado a **Andrés Felipe RAMÍREZ** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 68 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ANFERAM@MAPFRE.COM.CO.**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico anferam@mapfre.com.co asignada a **Andrés Felipe RAMÍREZ** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
7	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Andrés Felipe RAMÍREZ → anferam@mapfre.com.co	ad1	52.3 GB
TOTAL					**52.3 GB**

Tabla 15 Detalle del buzón de correo electrónico asignado anferam@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico anferam@mapfre.com.co asignado a Andrés Felipe RAMÍREZ

para el desarrollo de sus funciones **aloja** un total de **52.3 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Novecientos ocho mil cuatrocientos veintitrés (908.423)** archivos (incluyendo carpetas), como se observa a continuación.

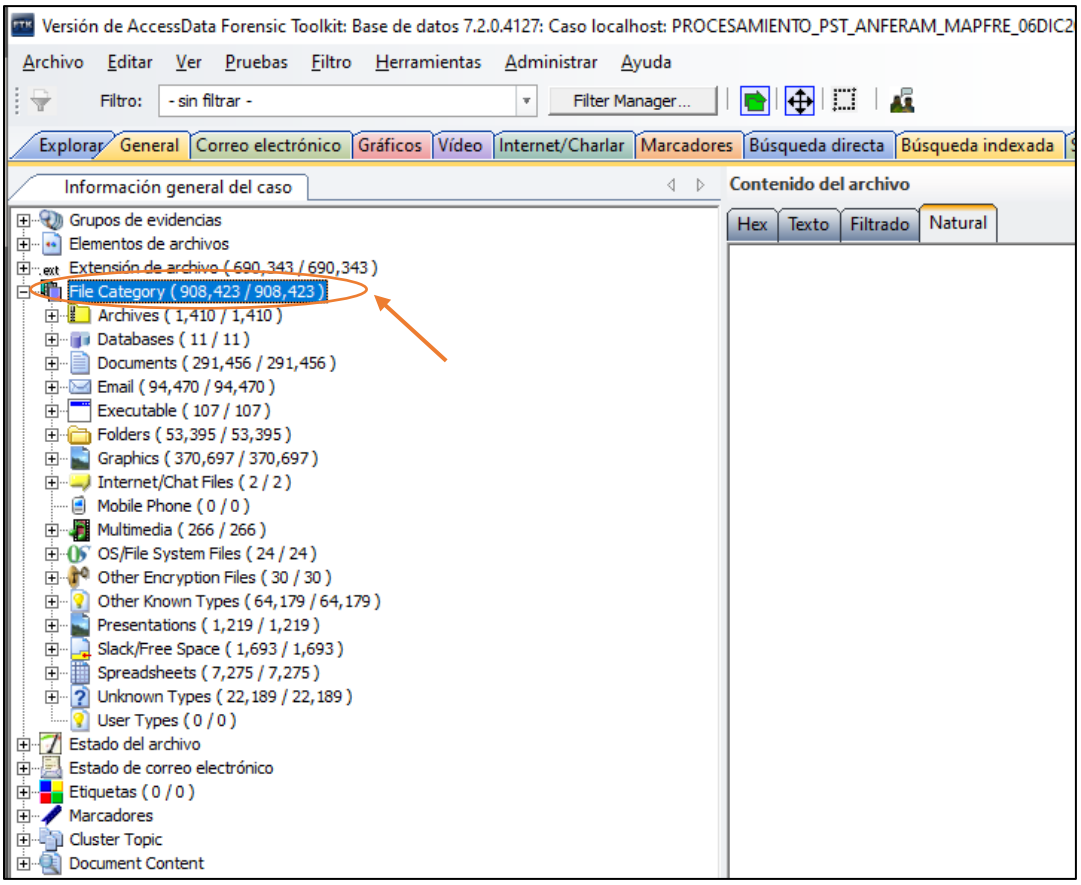


Ilustración 69 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico anferam@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO ANDRÉS FELIPE RAMÍREZ → ANFERAM@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico anferam@mapfre.com.co asignado a **Andrés Felipe RAMÍREZ**, iniciando el día el 06 de diciembre del presente año con una duración aproximada de **cinco (5)** día calendario, el resultado a dicho proceso arrojó que existen **Novecientos ochenta y un (981)** ítems en condición de "eliminados" y se reconstruyeron **Doscientos treinta y seis mil doscientos noventa y un (236.291)** archivos de datos restaurados,

que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

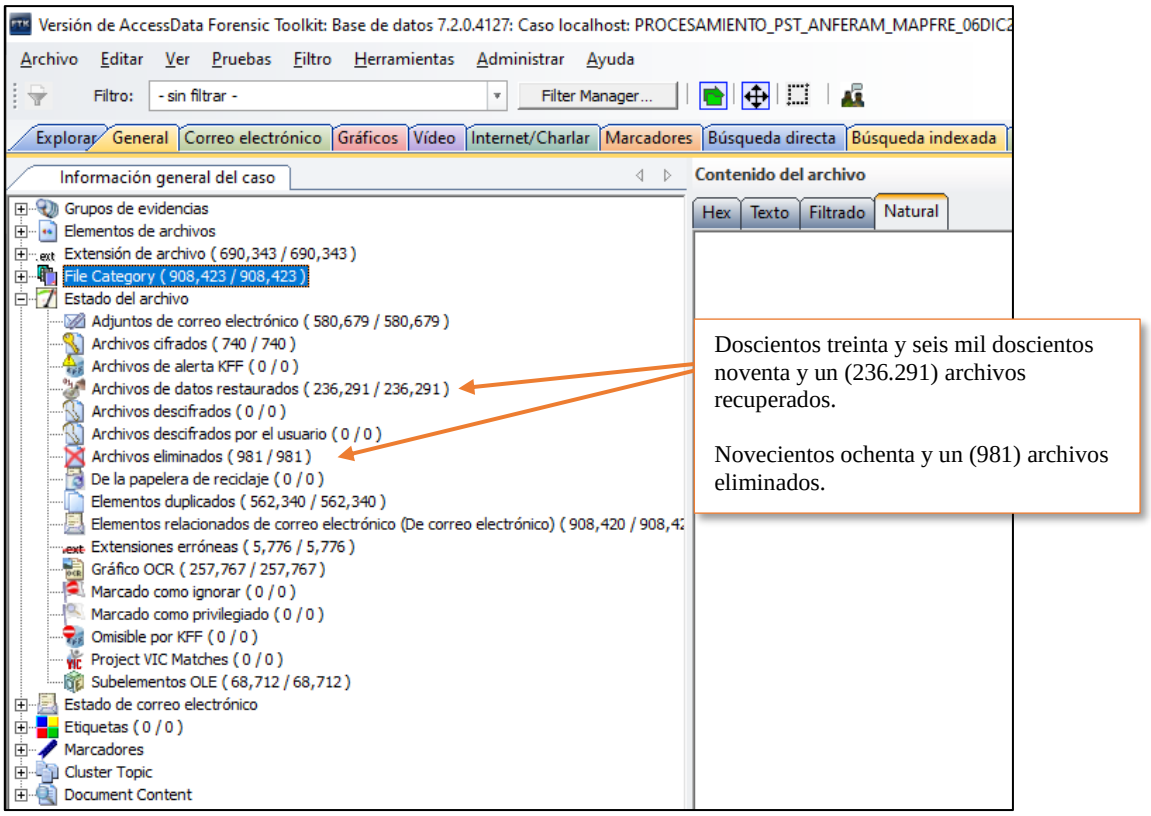


ilustración 70 Total de archivos recuperados en la cuenta de correo electrónico anferam@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Novecientos ocho mil cuatrocientos veintitrés (908.423)** (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ANFERAM@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico

anferam@mapfre.com.co asignado a **Andrés Felipe RAMÍREZ** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1.410
2	Bases de Datos	11
3	Documentos	291.456
4	Correo Electrónico	94.470
5	Ejecutables	107
6	Carpetas	53.395
7	Gráficos	370.697
8	Archivos de Internet/Chat	2
9	Multimedia	266
10	Archivos del sistema	24
11	Otros archivos encriptados	30
12	Otros archivos desconocidos	64.179
13	Presentaciones	1.219
14	Espacio libre	1.693
15	Hojas de cálculo	7.275
16	Tipos de archivos desconocidos	22.189
TOTAL		**908.423**

Tabla 16 Información buscada evidencia 007_ANFERAM, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Novecientos ocho mil cuatrocientos veintitrés (908.423).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Quinientos ochenta mil seiscientos setenta y nueve (580.679) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Los archivos cifrados recuperados **Setecientos cuarenta (740) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Doscientos treinta y seis mil doscientos noventa y un (236.291) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos Eliminados **Novecientos ochenta y un (981) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Quinientos sesenta y dos mil trescientos cuarenta (562.340) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Novecientos ocho mil cuatrocientos veinte (908.420) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Cinco mil setecientos setenta y seis (5.776) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Doscientos cincuenta y siete mil setecientos sesenta y siete (257.767) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Sesenta y ocho mil setecientos doce (68.712) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico anferam@mapfre.com.co asignado a **Andrés Felipe RAMÍREZ** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

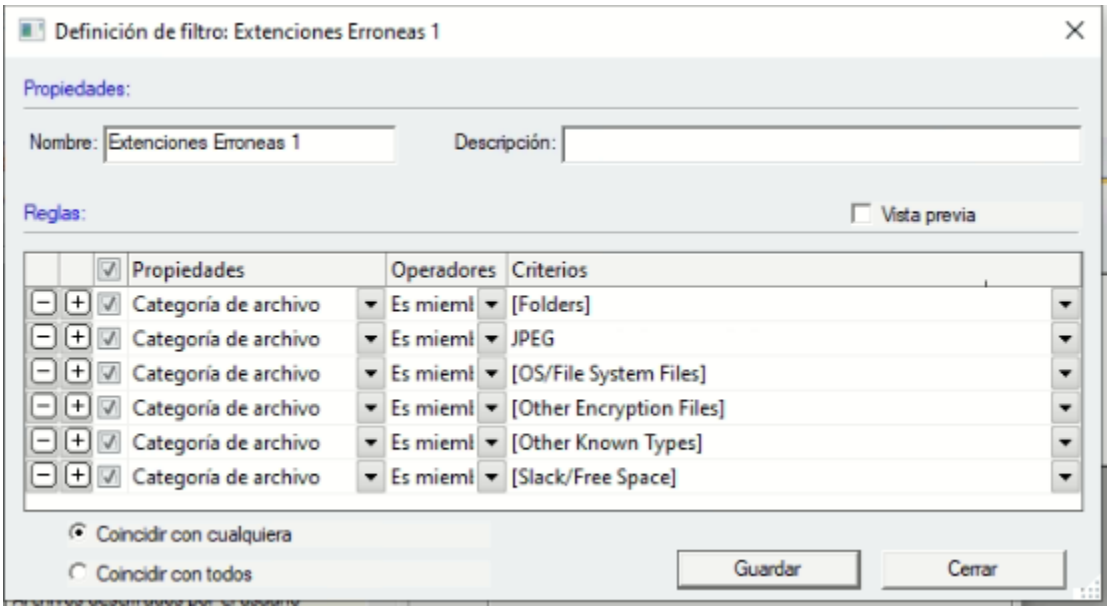


Ilustración 71 Filtro para excluir las extensiones erróneas.

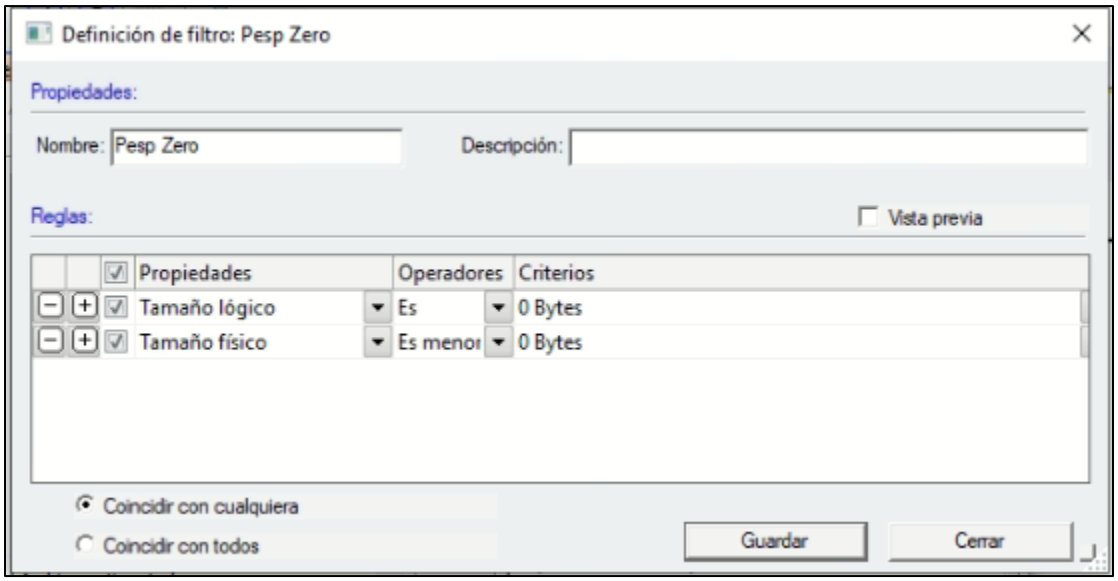


Ilustración 72 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

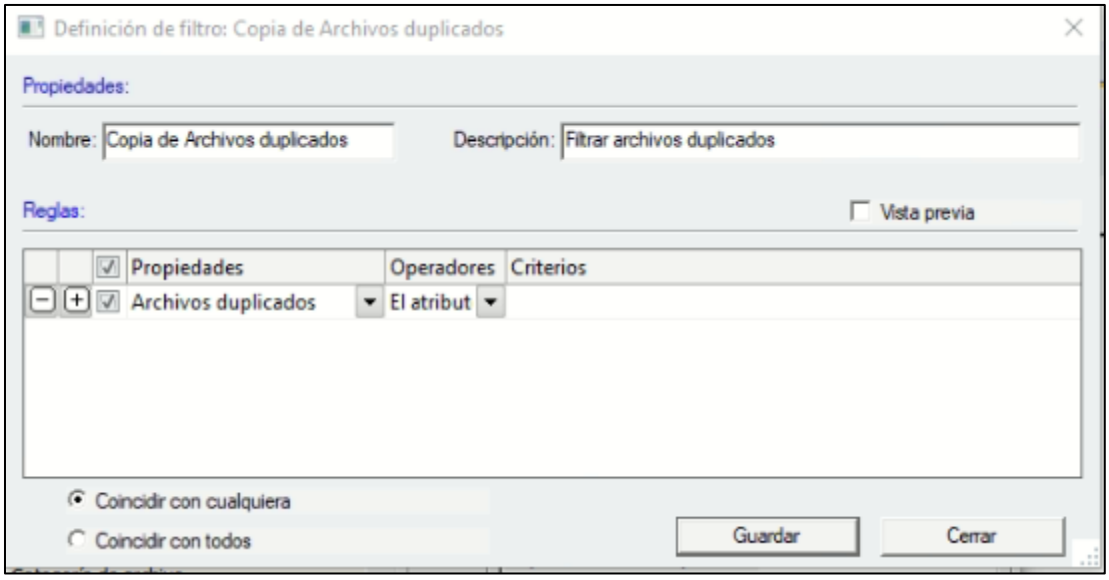


Ilustración 73 Filtro para excluir los archivos duplicados.

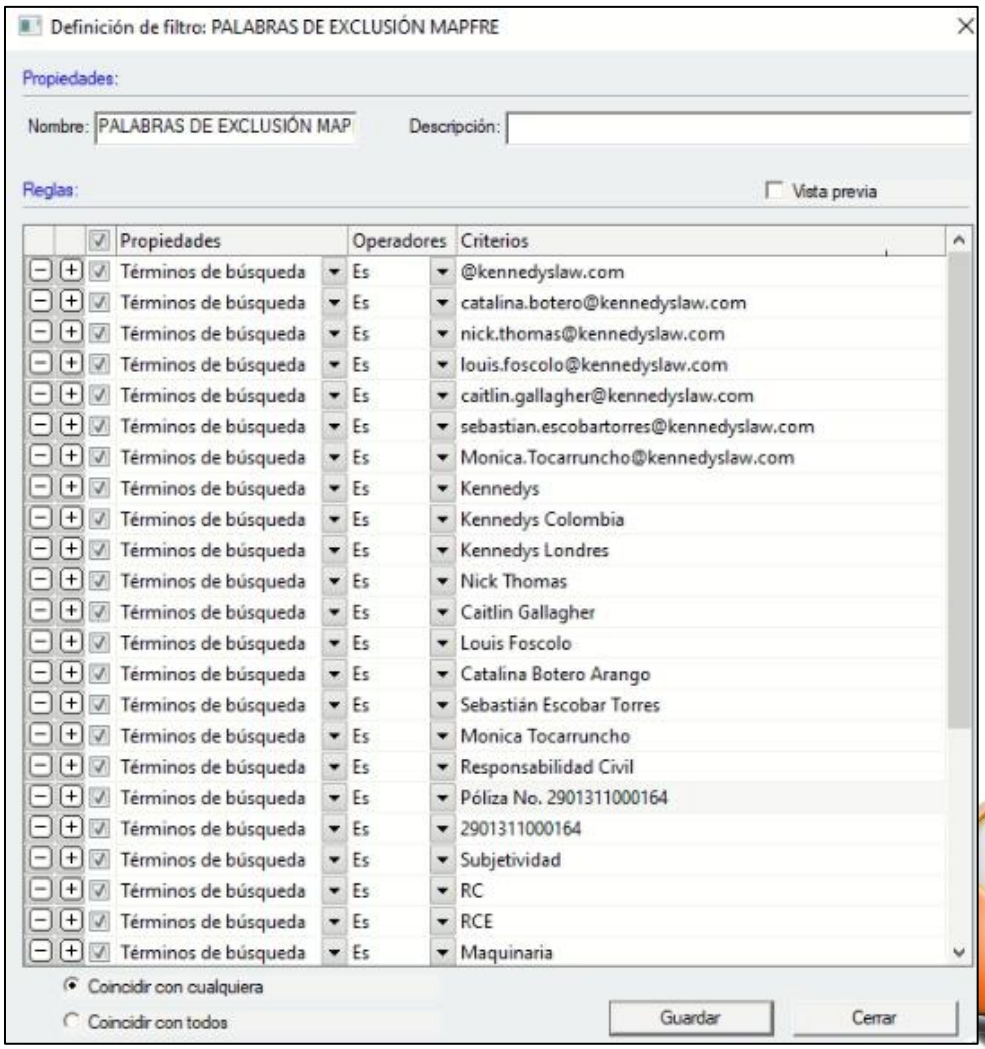


Ilustración 74 Filtro para excluir los archivos suministrado por MAPFRE - 1.

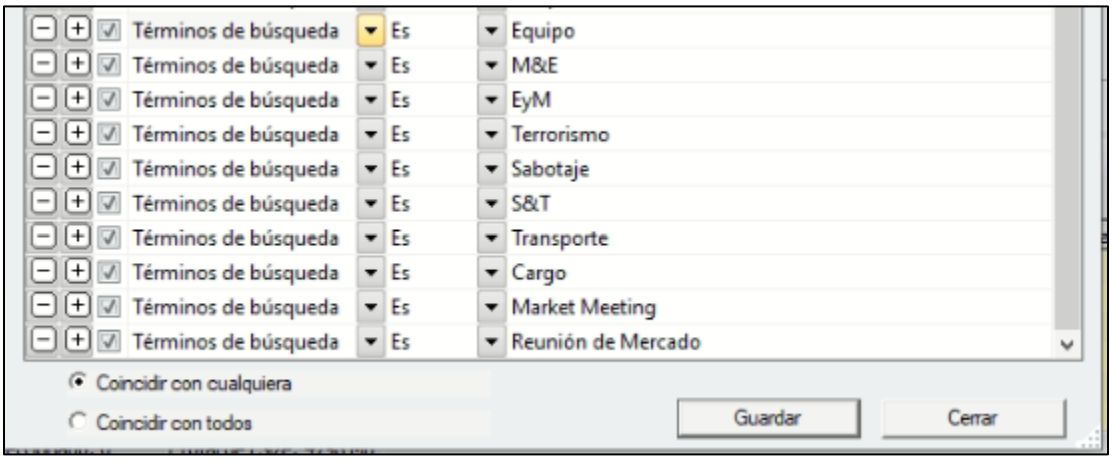
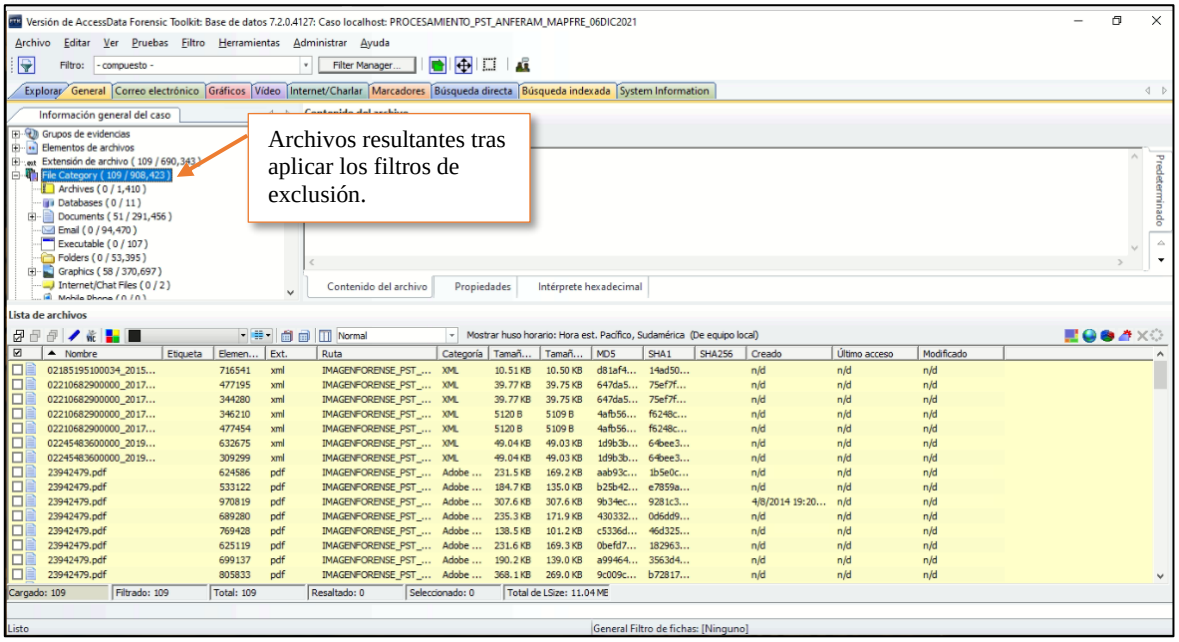


Ilustración 75 Filtro para excluir los archivos suministrado por MAPFRE - 2.

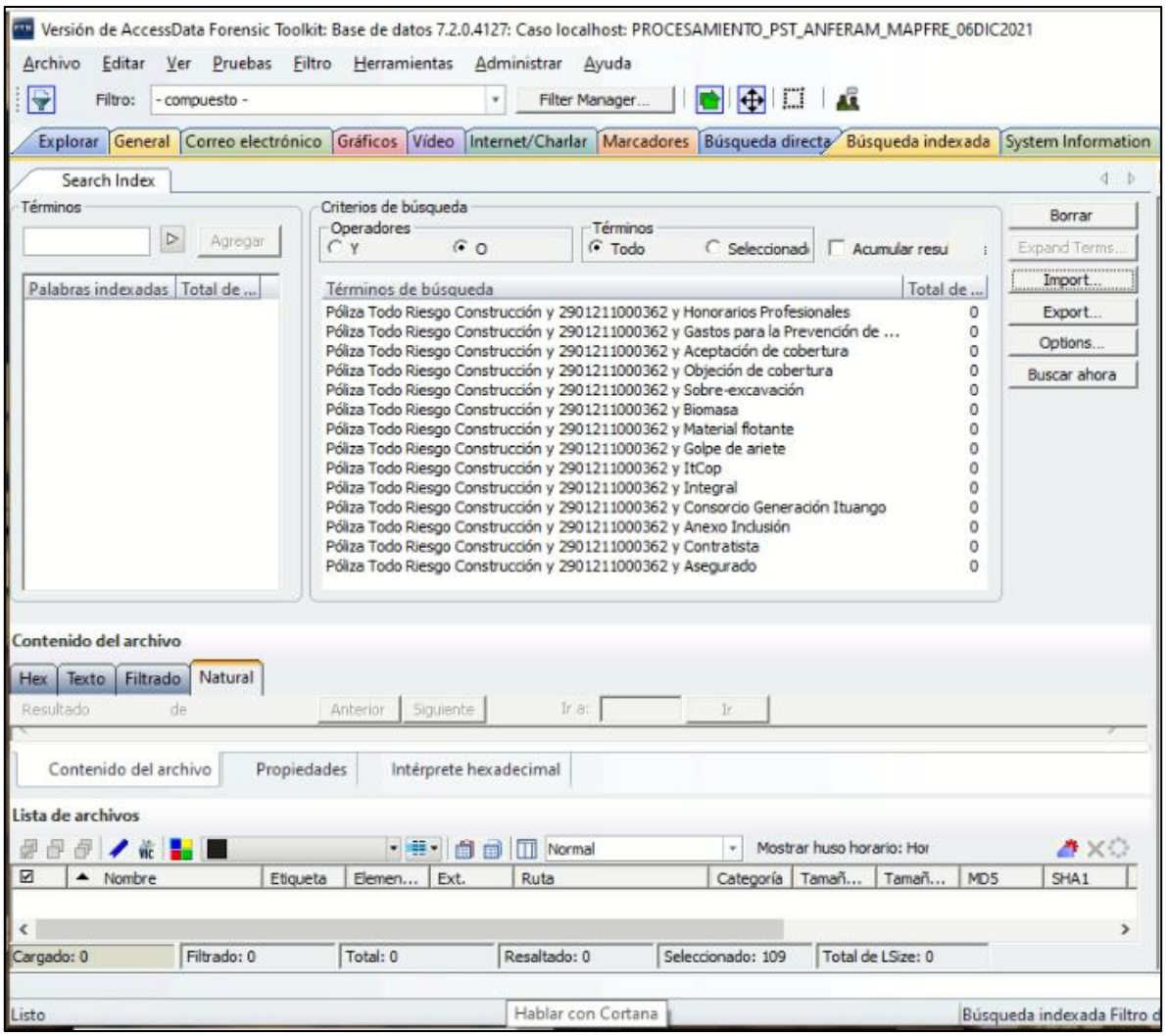
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Ciento nueve (109)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo anferam@mapfre.com.co asignado a **Andrés Felipe RAMÍREZ** para el desarrollo de sus funciones.

8. Buzón de correo electrónico mvivian@mapfre.com.

El día 19 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **MVIVIAN**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

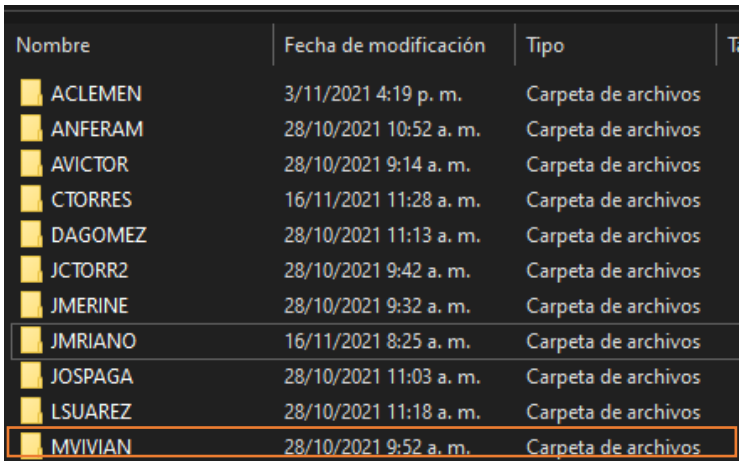


Ilustración 76 Visualización carpeta MVIVIAN

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **MVIVIAN** identificada dentro del disco duro como se observa en las siguientes imágenes:

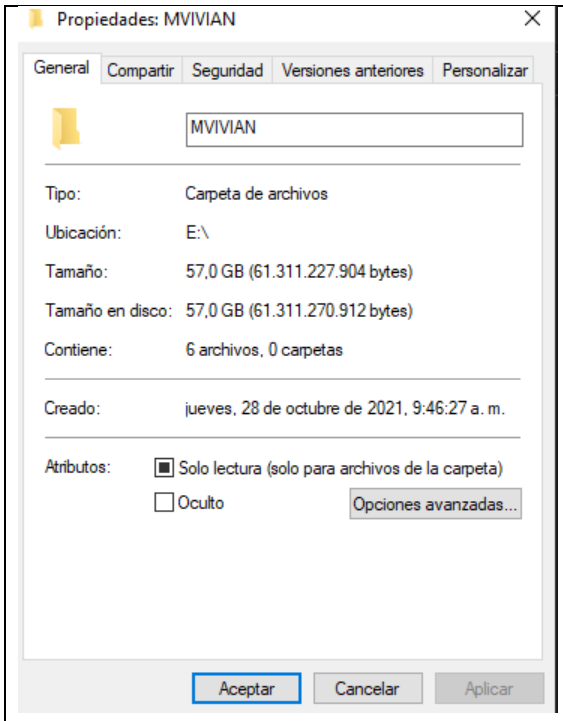


Ilustración 77 Propiedades de la carpeta MVIVIAN visto desde el Disco Duro.

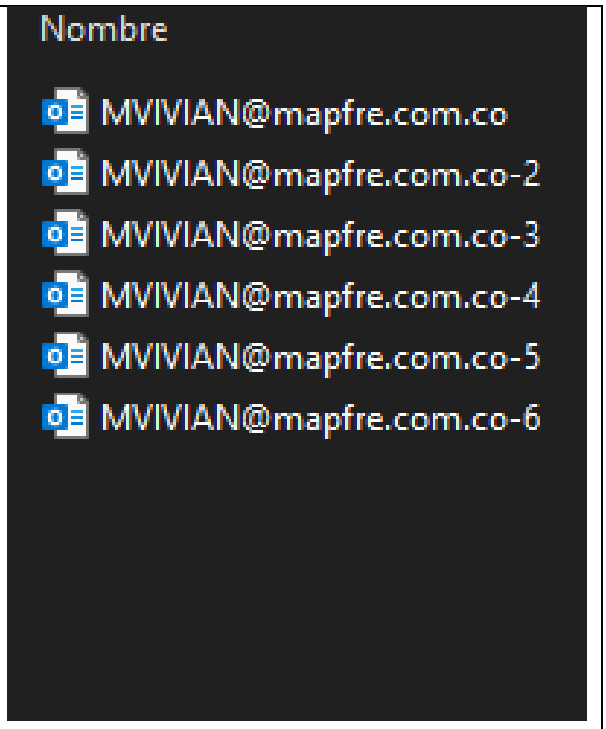


Ilustración 78 Contenido de la carpeta MVIVIAN visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**mvivian@mapfre.com.**" asignado a

Viviana Rocío MOYANO para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **15:59:28** y culminando el mismo de forma satisfactoria a las **16:22:11**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_19NOV2021
Número de prueba: 008_MVIVIAN
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO MVIVIAN@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad1:
[Custom Content Sources]
K::K:\|MVIVIAN|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: f2b048976f511d39e5985af537222dea
SHA1 checksum: 493d58bf1f54dcc30314162538921cf1b8ac853d

Image information:
Acquisition started: Fri Nov 19 15:59:28 2021
Acquisition finished: Fri Nov 19 16:16:02 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad29

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad30

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad31

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad32

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad33

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad34

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad35

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad36

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad37

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad38

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad39

Image Verification Results:
Verification started: Fri Nov 19 16:16:02 2021
Verification finished: Fri Nov 19 16:22:11 2021
MD5 checksum: f2b048976f511d39e5985af537222dea: verified
SHA1 checksum: 493d58bf1f54dcc30314162538921cf1b8ac853d: verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con

capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**mvivian@mapfre.com.**" asignado a **Viviana Rocío MOYANO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 79 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO MVIVIAN@MAPFRE.COM."**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico mvivian@mapfre.com asignada **Viviana Rocío MOYANO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
8	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Viviana Rocío MOYANO → mvivian@mapfre.com	ad1	57.0 GB
TOTAL					**57.0 GB**

Tabla 17 Detalle del buzón de correo electrónico asignado mvivian@mapfre.com
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico mvivian@mapfre.com asignado a **Viviana Rocío MOYANO** para

el desarrollo de sus funciones **aloja** un total de **57.0 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Setecientos treinta mil doscientos dieciocho (730.218)** archivos (incluyendo carpetas), como se observa a continuación.

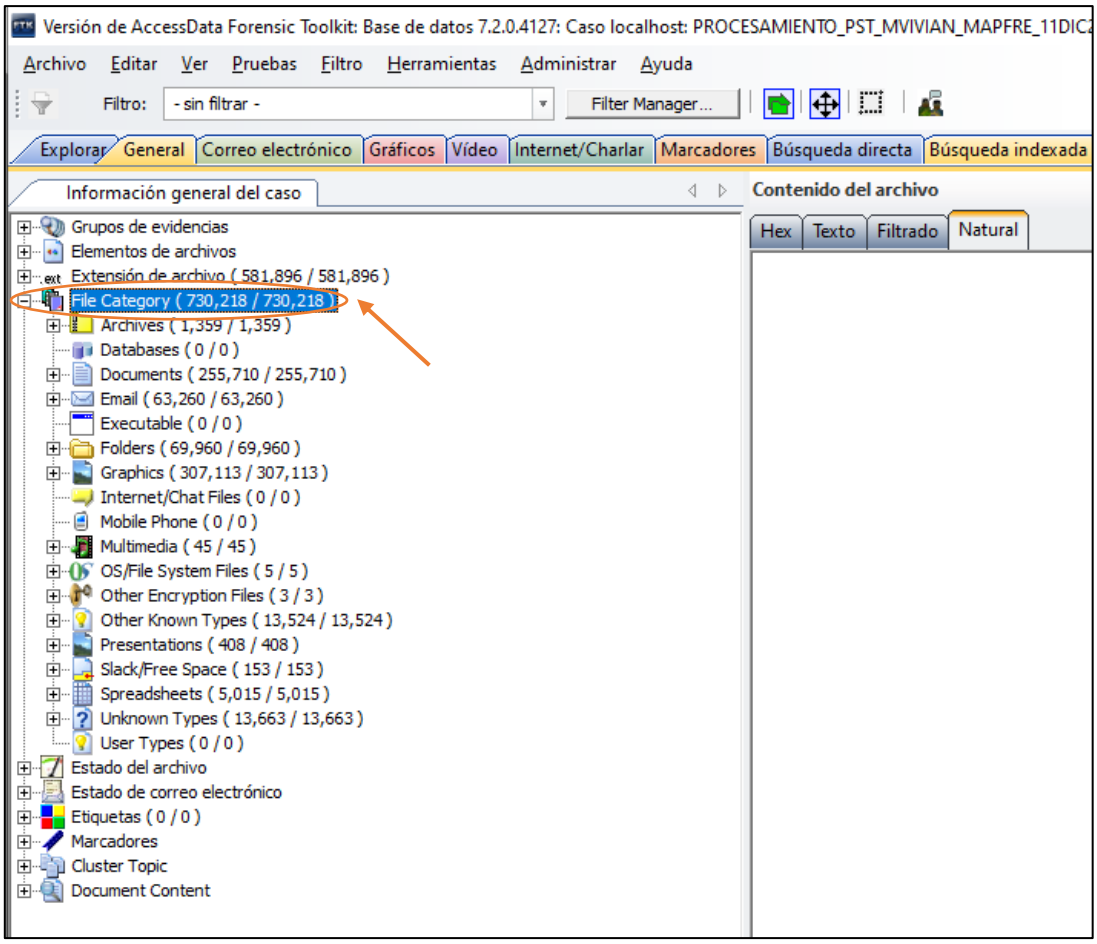


Ilustración 80 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico mvivian@mapfre.com.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO VIVIANA ROCÍO MOYANO → MVIVIAN@MAPFRE.COM.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico mvivian@mapfre.com asignado a **Viviana Rocío MOYANO**, iniciando el día el **11** de diciembre del presente año con una duración aproximada de **Diez (10)** días calendarios, el resultado a dicho proceso arrojó que existen **cero (0)** ítems en condición de "eliminados" y se reconstruyeron **Ciento noventa y cuatro mil cuatrocientos**

treinta y un (194.431) archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

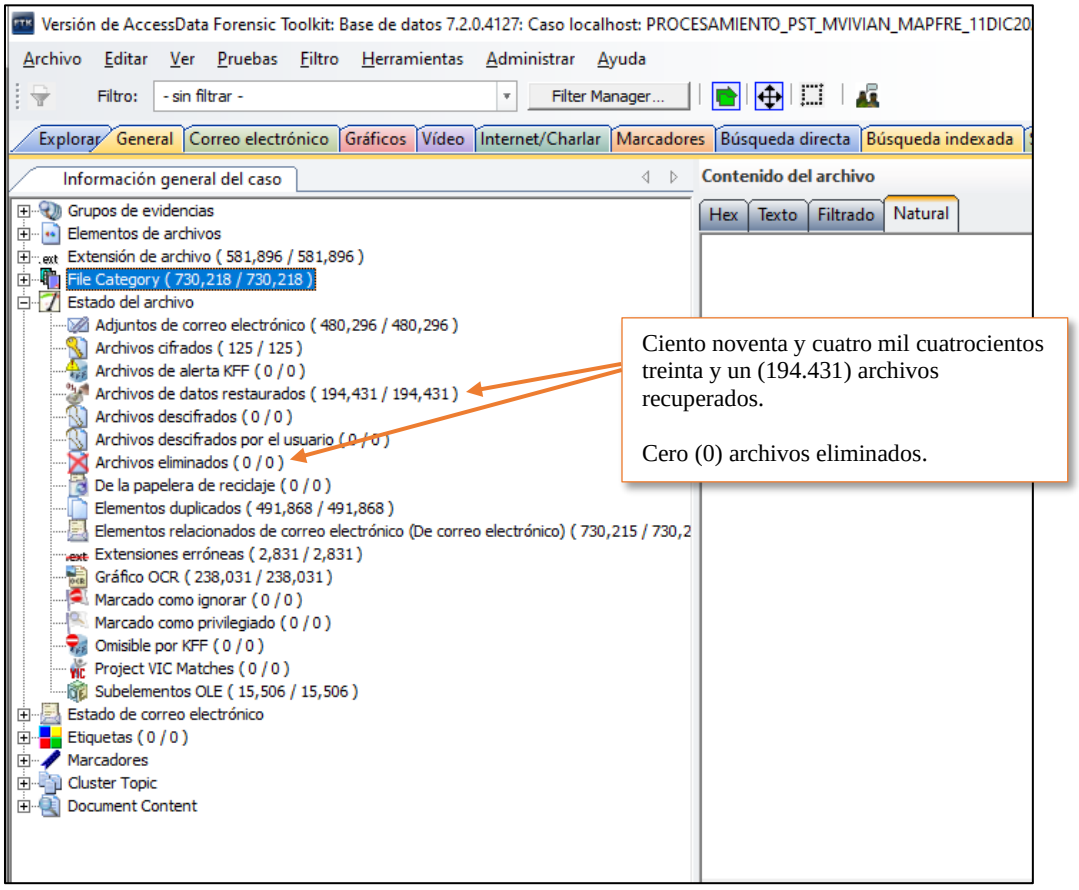


ilustración 81 Total de archivos recuperados en la cuenta de correo electrónico mvivian@mapfre.com.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Setecientos treinta mil doscientos dieciocho (730.218)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

- **RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO MVIVIAN@MAPFRE.COM.CO.**

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico mvivian@mapfre.com asignado a **Viviana Rocío MOYANO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1.359
2	Documentos	255.710
3	Correo Electrónico	63.260
4	Carpetas	69.960
5	Gráficos	307.113
6	Multimedia	45
7	Archivos del sistema	5
8	Otros archivos encriptados	3
9	Otros archivos desconocidos	13.524
10	Presentaciones	408
11	Espacio libre	153
12	Hojas de cálculo	5.015
13	Tipos de archivos desconocidos	13.663
TOTAL		**730.218**

Tabla 18 Información buscada evidencia 008_MVIVIAN, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Setecientos treinta mil doscientos dieciocho (730.218).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Cuatrocientos ochenta mil doscientos noventa y seis (480.296) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Ciento veinticinco (125) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Ciento noventa y cuatro mil cuatrocientos treinta y un (194.431) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Cuatrocientos noventa y un mil ochocientos sesenta y ocho (491.868) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Setecientos treinta mil doscientos quince (730.215) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Dos mil ochocientos treinta y un (2.831) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Doscientos treinta y ocho mil treinta y un (238.031) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Quince mil quinientos seis (15.506) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico mvivian@mapfre.com asignado a **Viviana Rocío MOYANO** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

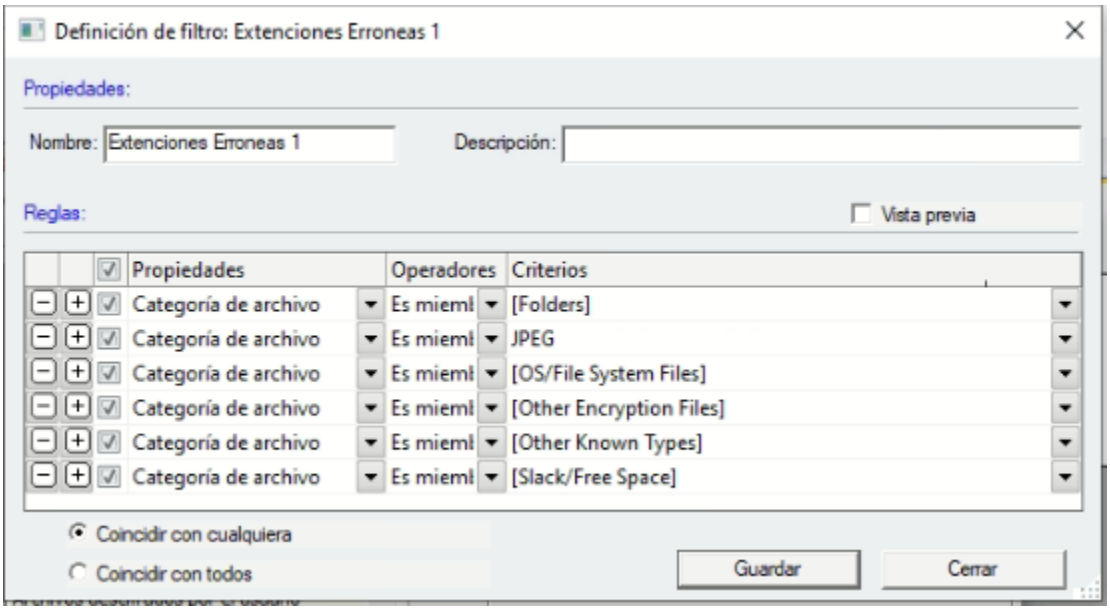


Ilustración 82 Filtro para excluir las extensiones erróneas.

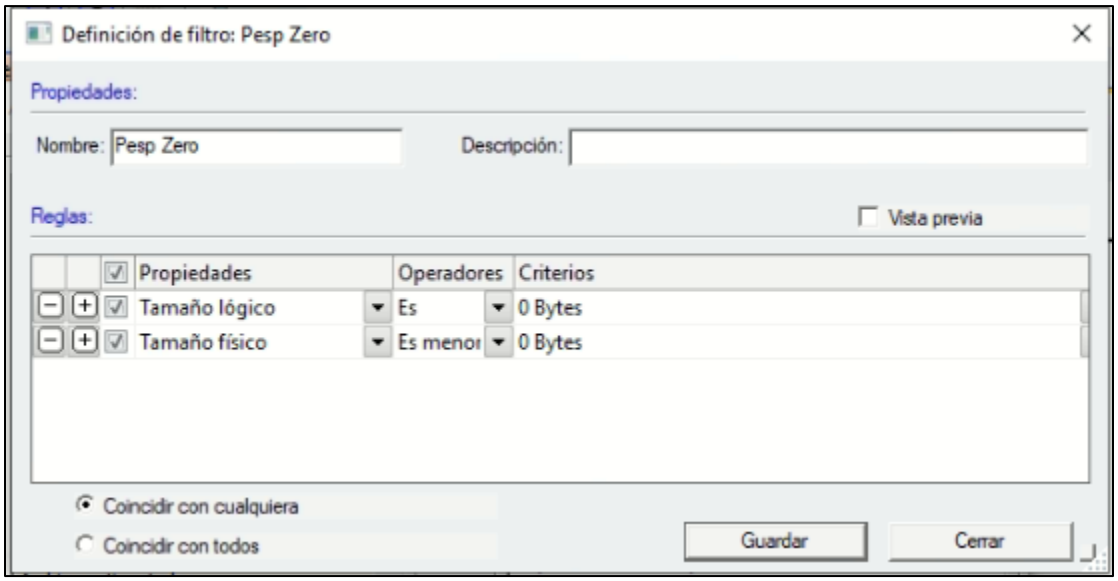


Ilustración 83 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

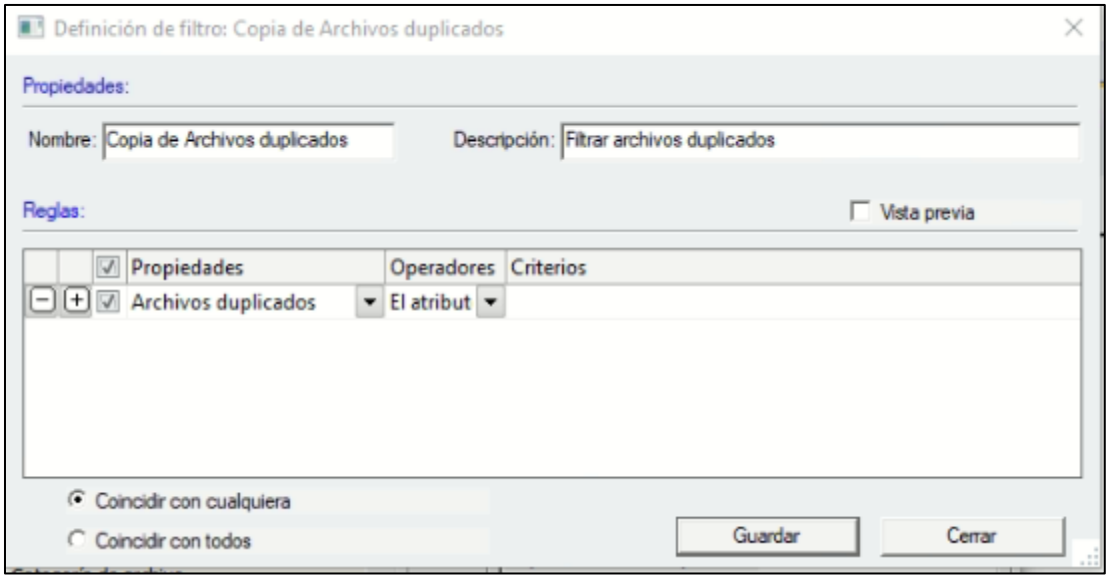


Ilustración 84 Filtro para excluir los archivos duplicados.

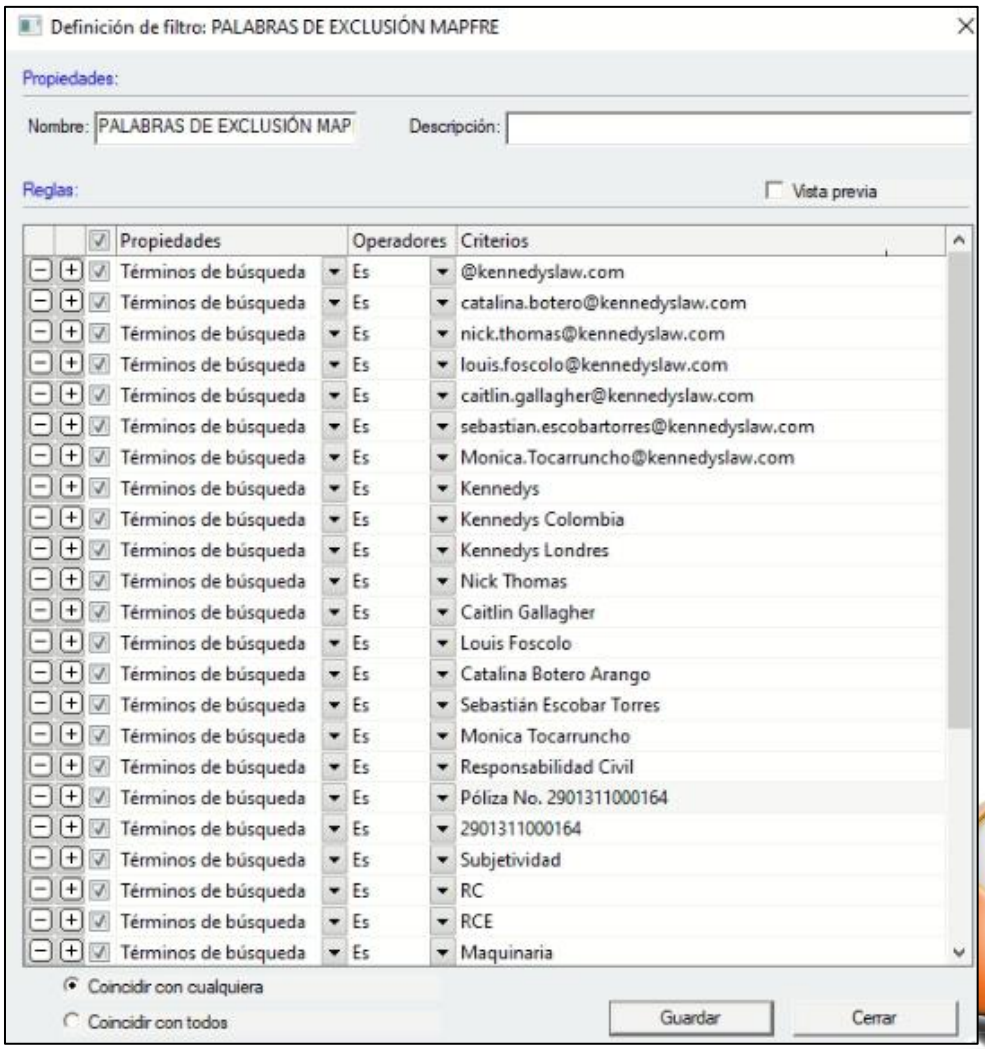


Ilustración 85 Filtro para excluir los archivos suministrado por MAPFRE - 1.

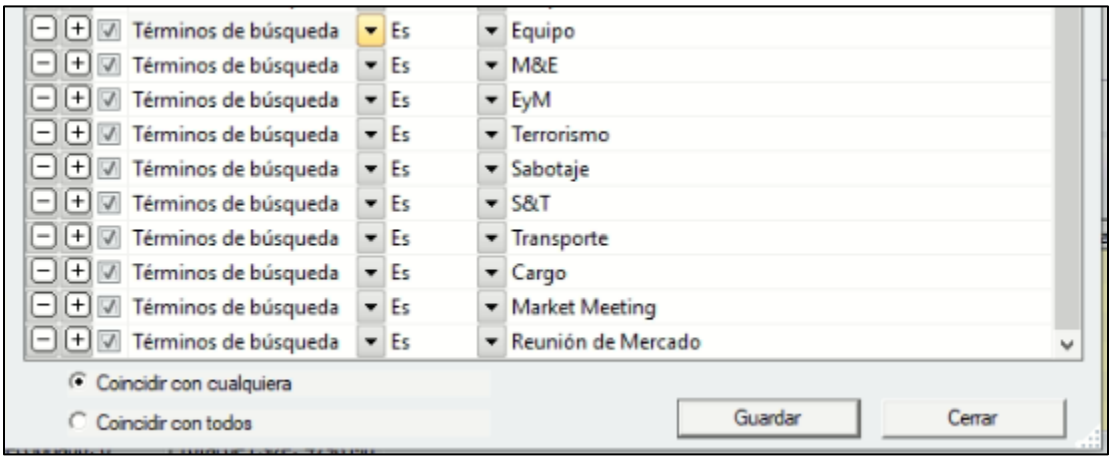
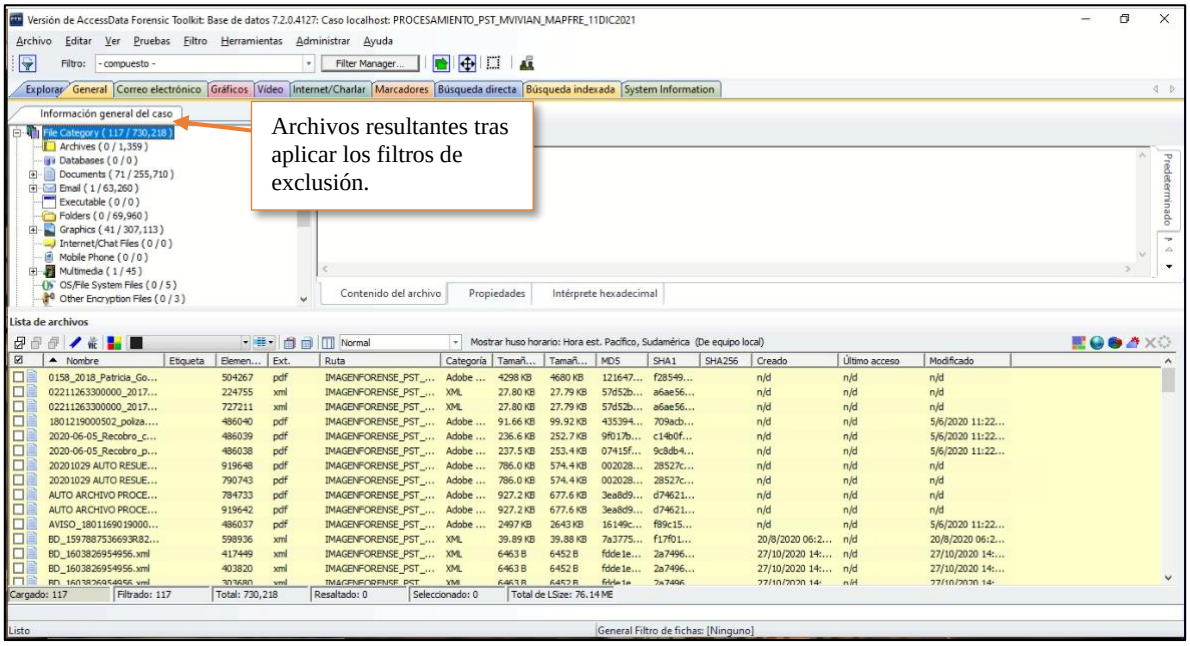


Ilustración 86 Filtro para excluir los archivos suministrado por MAPFRE - 2.

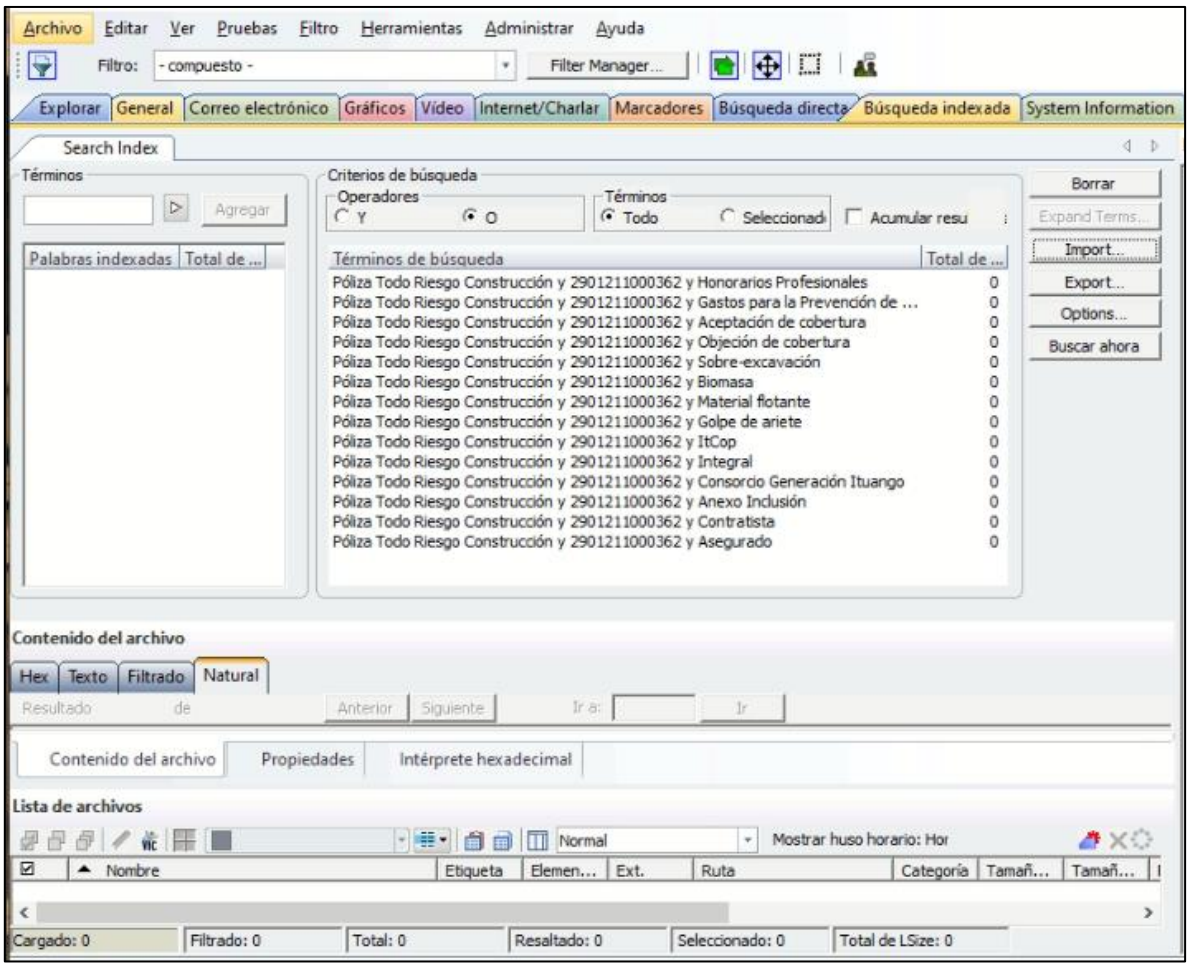
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Veinticinco (117)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo mvivian@mapfre.com asignado a **Viviana Rocío MOYANO** para el desarrollo de sus funciones.

9. Buzón de correo electrónico jctorr2@mapfre.com.co

El día 22 de noviembre del 2021, el equipo de ADALID CORP ingresa a la carpeta **JCTORR2**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

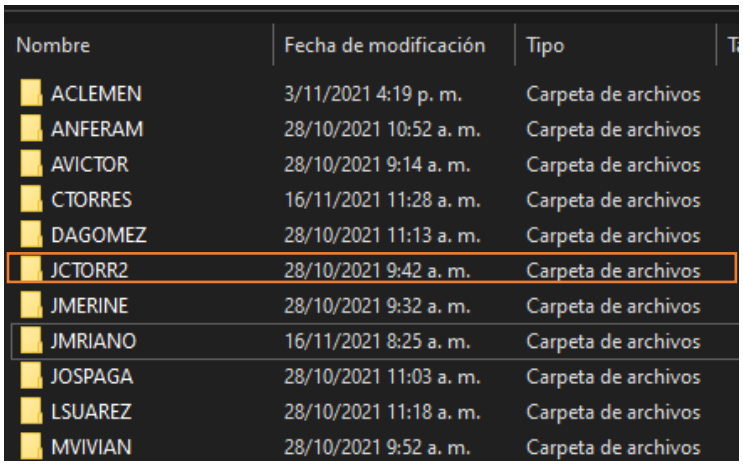


Ilustración 87 Visualización carpeta JCTORR2.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **JCTORR2** identificada dentro del disco duro como se observa en las siguientes imágenes:

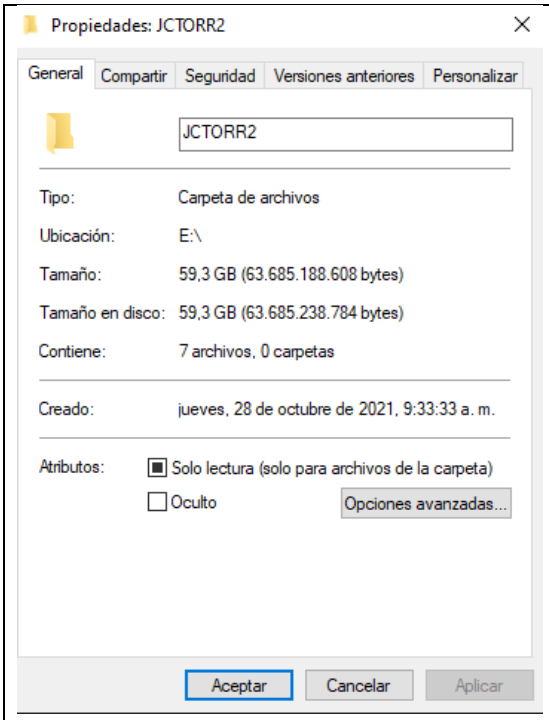


Ilustración 88 Propiedades de la carpeta JCTORR2 visto desde el Disco Duro.

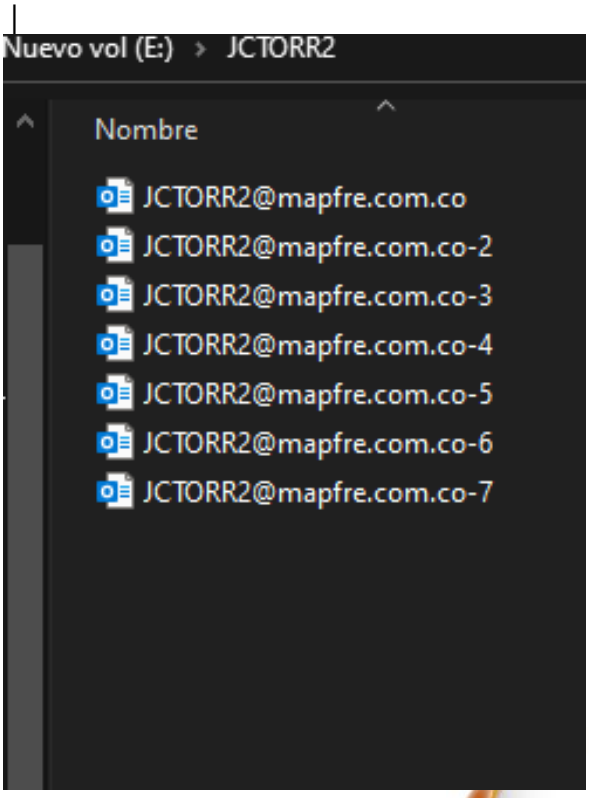


Ilustración 89 Contenido de la carpeta JCTORR2 visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**jctorr2@mapfre.com.co.**" asignado a **Juan Camilo TORRES LOZANO** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **10:00:06** y culminando el mismo de forma satisfactoria a las **10:17:22**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_22NOV2021
Número de prueba: 009_JCTORR2
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO JCTORR2@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for
I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad1:
[Custom Content Sources]
K::K:\|JCTORR2|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 82febeb311661f24839ced114ce64e7b
SHA1 checksum: 47c4c084826f4119210640aa34aae4b32068e556

Image information:
Acquisition started: Mon Nov 22 10:00:06 2021
Acquisition finished: Mon Nov 22 10:12:52 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad29

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad30

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad31

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad32

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad33

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad34

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad35

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad36

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad37

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad38

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad39

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad40

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad41

Image Verification Results:
Verification started: Mon Nov 22 10:12:54 2021
Verification finished: Mon Nov 22 10:17:22 2021
MD5 checksum: 82febeb311661f24839ced114ce64e7b : verified

SHA1 checksum: 47c4c084826f4119210640aa34aae4b32068e556 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**jctorr2@mapfre.com.co.**" asignado a **Juan Camilo TORRES LOZANO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 90 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO JCTORR2@MAPFRE.COM.CO.

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico jctorr2@mapfre.com.co asignada **Juan Camilo TORRES LOZANO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
9	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Juan Camilo TORRES LOZANO → jctorr2@mapfre.com.co	ad1	59.3 GB
TOTAL					**59.3 GB**

Tabla 19 Detalle del buzón de correo electrónico asignado jctorr2@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico jctorr2@mapfre.com.co asignada a **Juan Camilo TORRES LOZANO** para el desarrollo de sus funciones **aloja** un total de **59.3 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Un millón noventa y un mil setecientos sesenta y ocho (1.091.768)** archivos (incluyendo carpetas), como se observa a continuación.

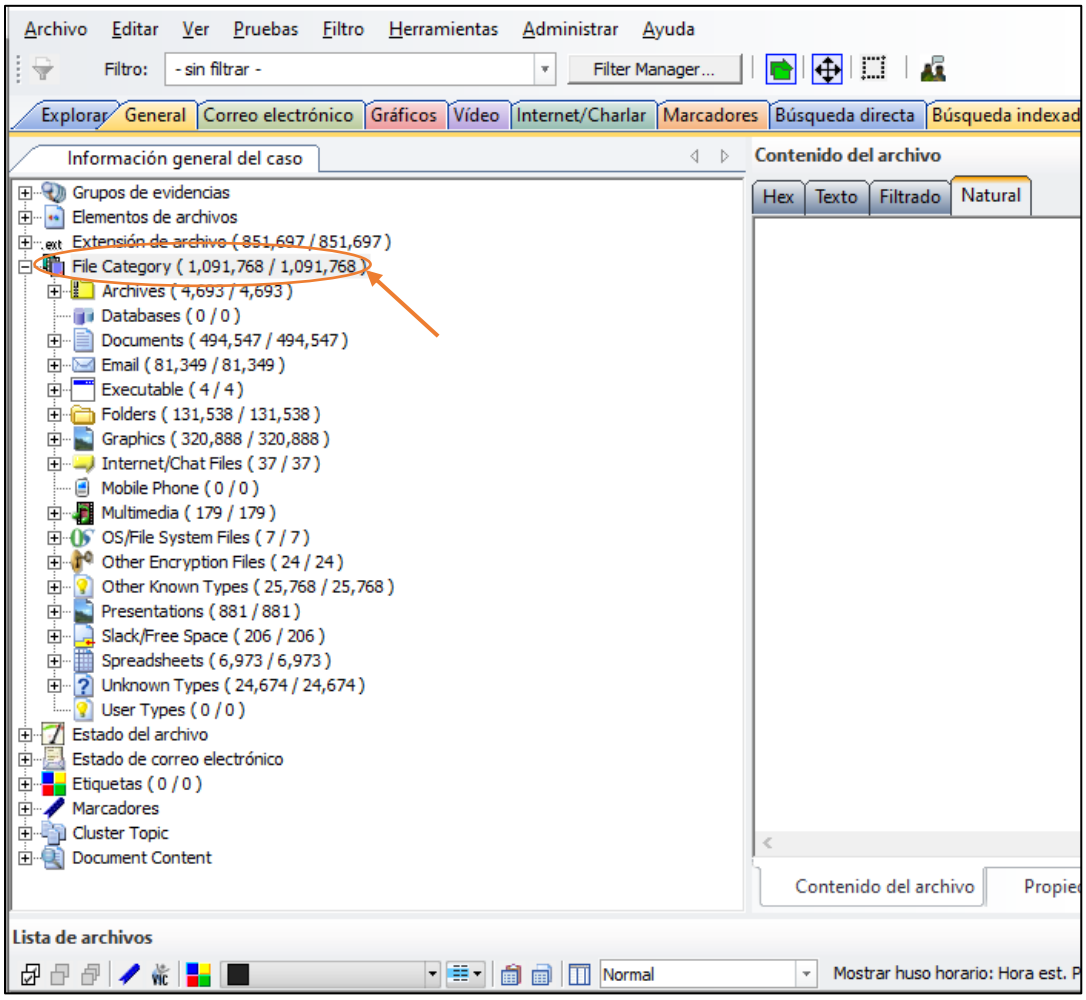


Ilustración 91 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico jctorr2@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JUAN CAMILO TORRES LOZANO → JCTORR2@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos,

en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico jctorr2@mapfre.com.co asignada a **Juan Camilo TORRES LOZANO**, iniciando el día el **27** de diciembre del año 2021 con una duración aproximada de diez (10) días calendarios y finalizando el día 07 de enero de 2022, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Ciento ochenta y dos mil ochocientos cincuenta y dos (182.852)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

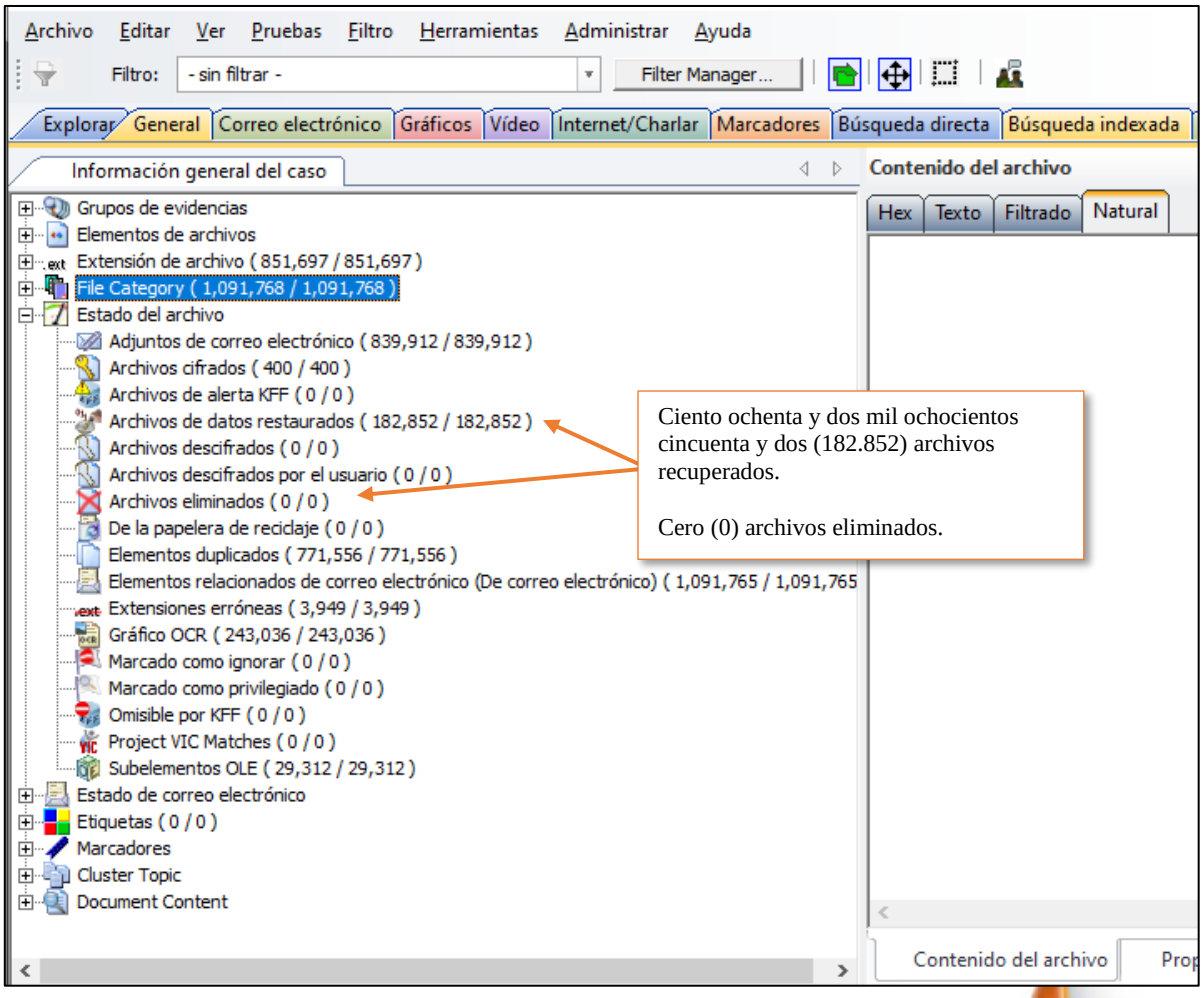


ilustración 92 Total de archivos recuperados en la cuenta de correo electrónico jctorr2@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Un millón noventa y un mil setecientos sesenta y ocho (1.091.768)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO JCTORR2@MAPFRE.COM.CO.

Luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico jctorr2@mapfre.com.co asignada a **Juan Camilo TORRES LOZANO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	4693
2	Documentos	494.547
3	Correo Electrónico	81.349
4	Ejecutables	4
5	Carpetas	131.538
6	Gráficos	320.888
7	Archivos Internet/Chats	37
8	Multimedia	179
9	Archivos del sistema	7
10	Otros archivos encriptados	24
11	Otros archivos desconocidos	25.768
12	Presentaciones	881
13	Espacio libre	206
14	Hojas de cálculo	6.973
15	Tipos de archivos desconocidos	24.674
TOTAL		**1.091.768**

Tabla 20 Información buscada evidencia 009_ JCTORR2, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Un millón noventa y un mil setecientos sesenta y ocho (1.091.768).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Ochocientos treinta y nueve mil novecientos doce (839.912)** archivos de datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Cuatrocientos (400) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Diez mil setecientos ochenta y ocho (10.788) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Setecientos setenta y un mil quinientos cincuenta y seis (771.556) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Un millón noventa y un mil setecientos sesenta y cinco (1.091.765) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Tres mil novecientos cuarenta y nueve (3.949) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Doscientos cuarenta y tres mil treinta y seis (243.036) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Veintinueve mil trescientos doce (29.312) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico jctorr2@mapfre.com.co asignada a **Juan Camilo TORRES LOZANO** para el desarrollo de sus funciones el equipo de ADALID

CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

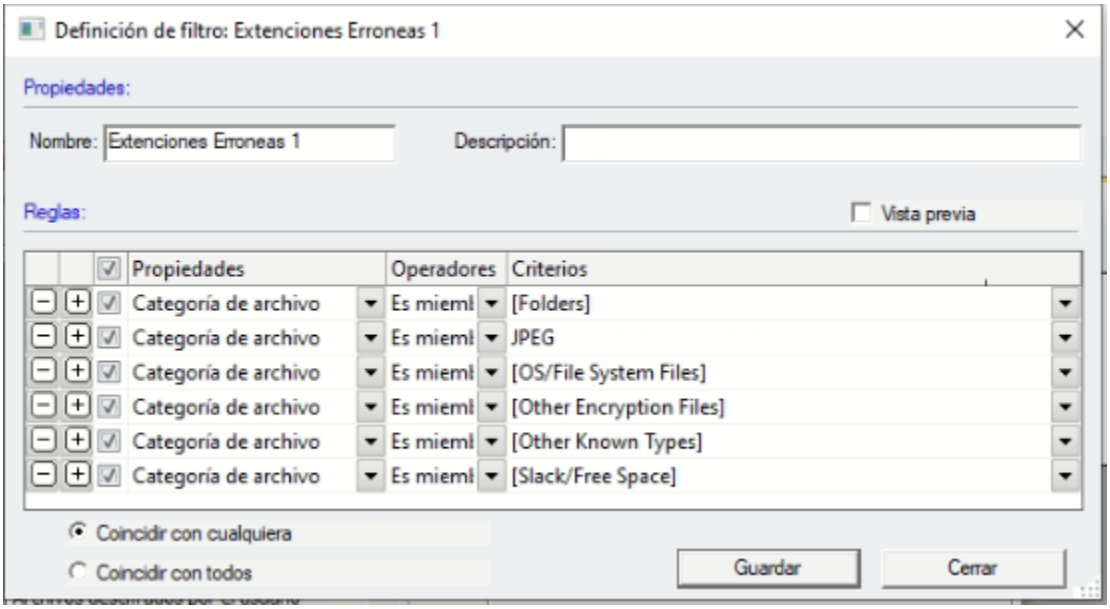


Ilustración 93 Filtro para excluir las extensiones erróneas.

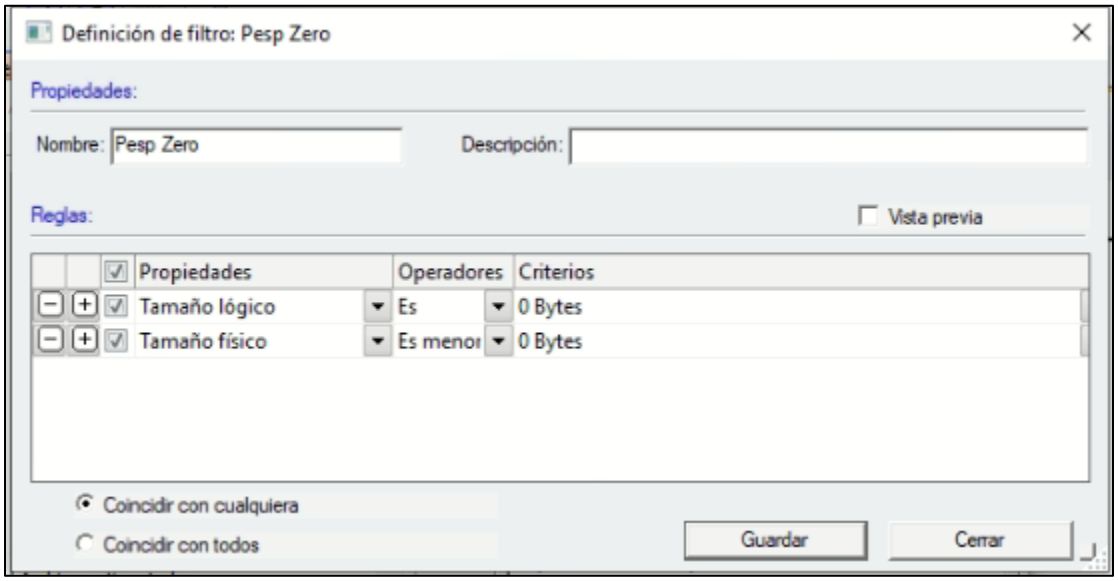


Ilustración 94 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

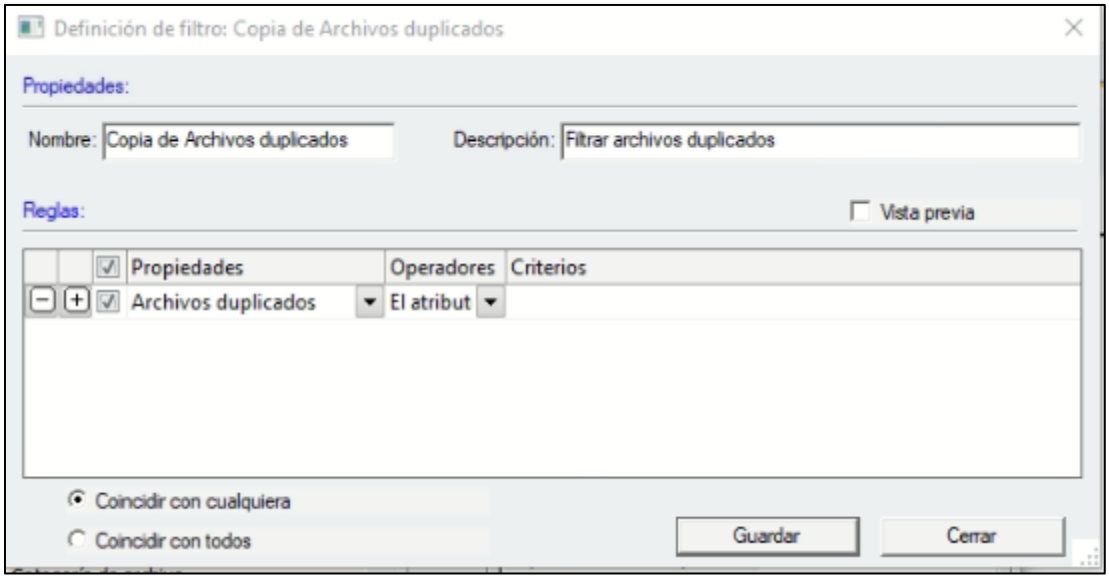


Ilustración 95 Filtro para excluir los archivos duplicados.

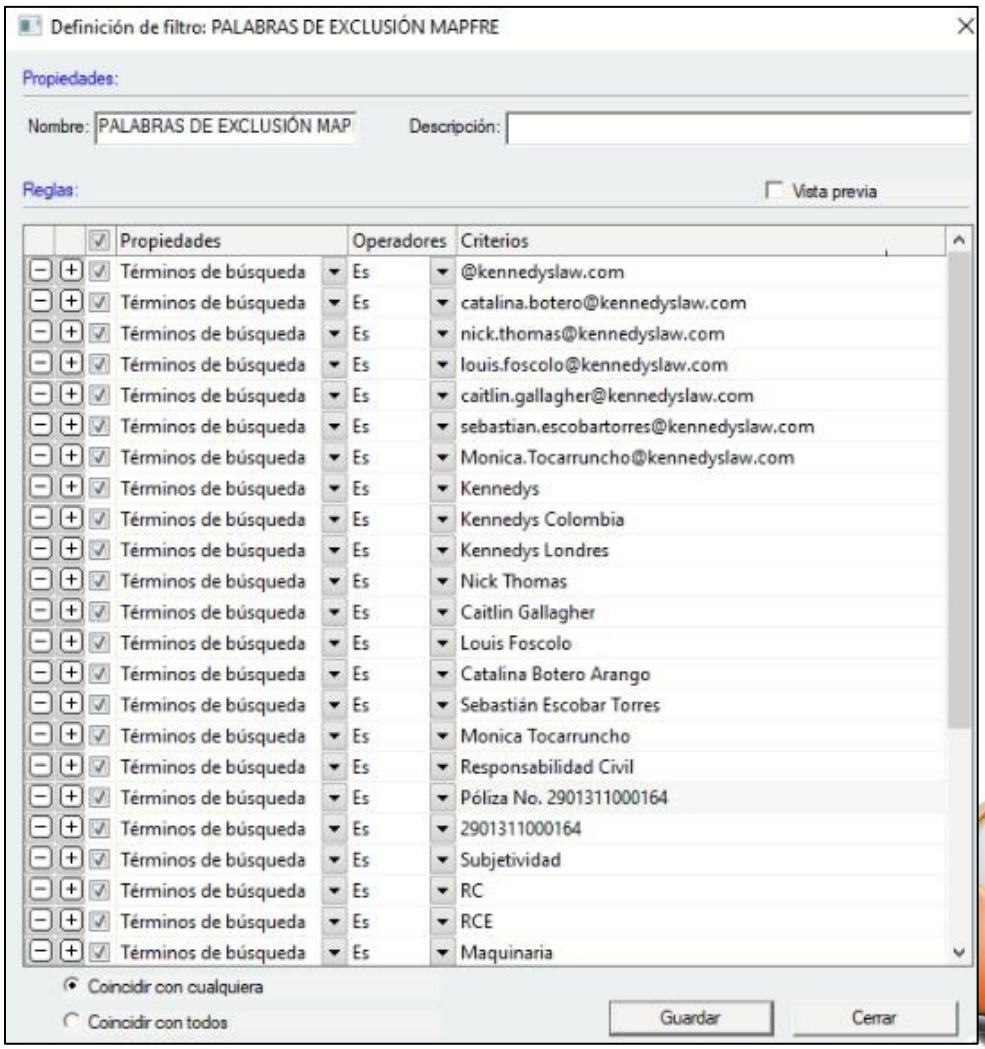


Ilustración 96 Filtro para excluir los archivos suministrado por MAPFRE - 1.

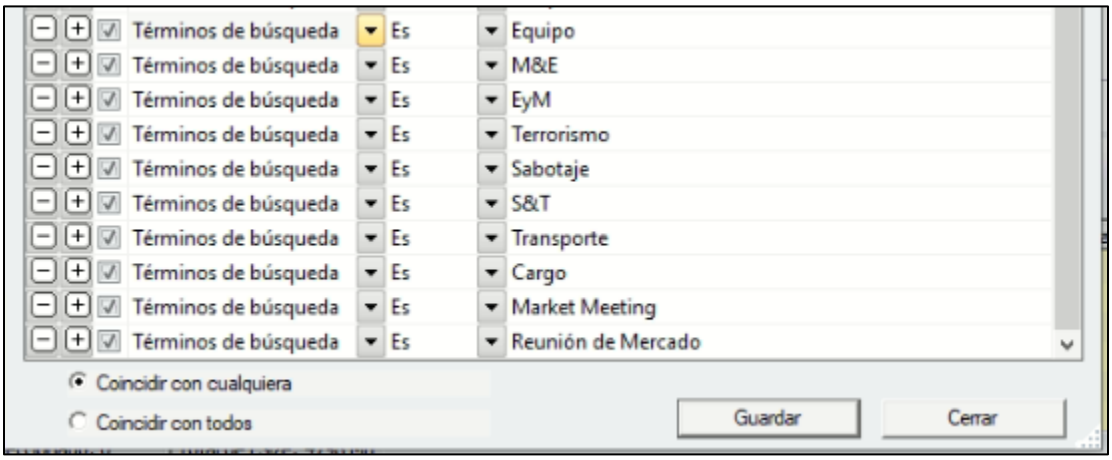
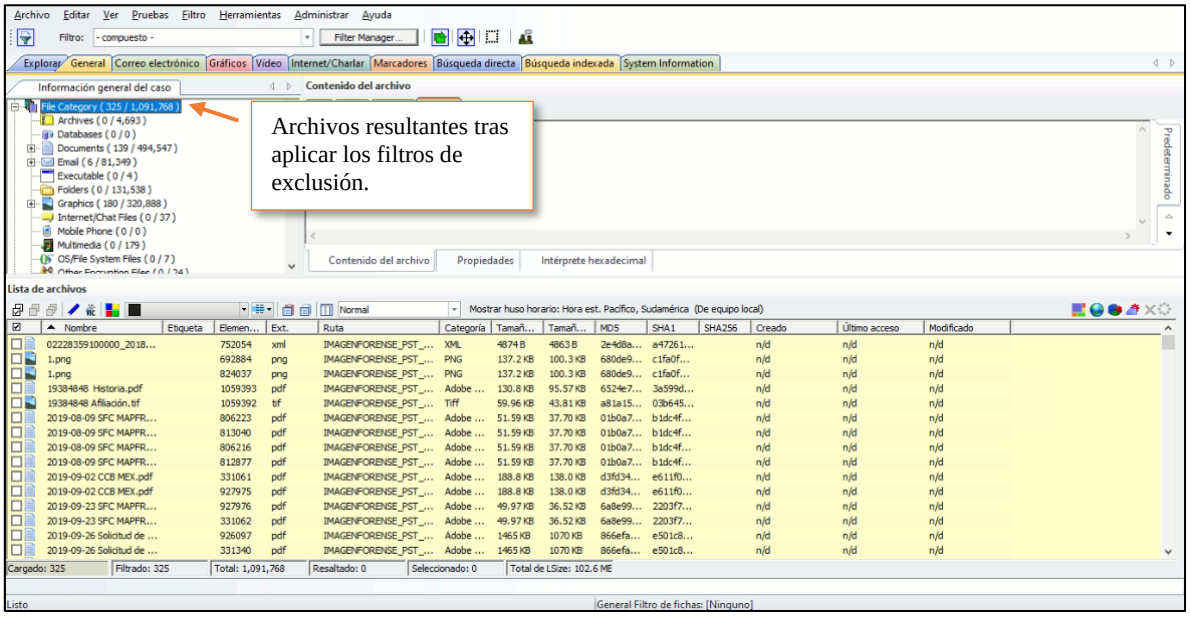


Ilustración 97 Filtro para excluir los archivos suministrado por MAPFRE - 2.

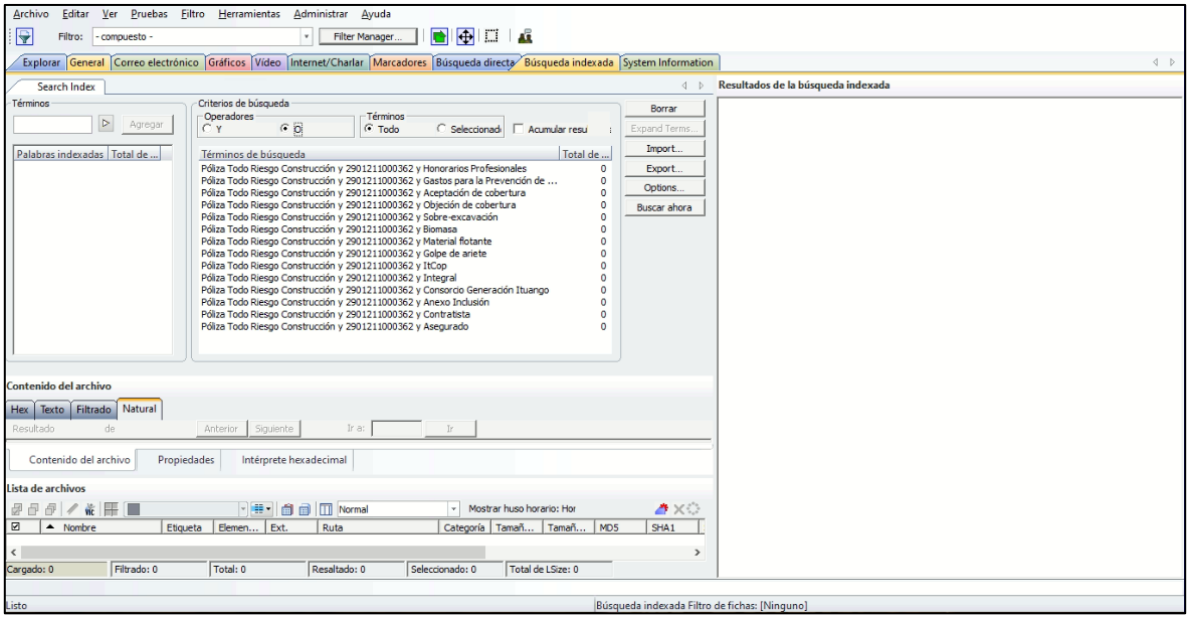
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Trecientos Veinticinco (325)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo jctorr2@mapfre.com.co asignada a **Juan Camilo TORRES LOZANO** para el desarrollo de sus funciones.

10. Buzón de correo electrónico jmriano@mapfre.com.co.

El día 22 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **JMRIANO**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

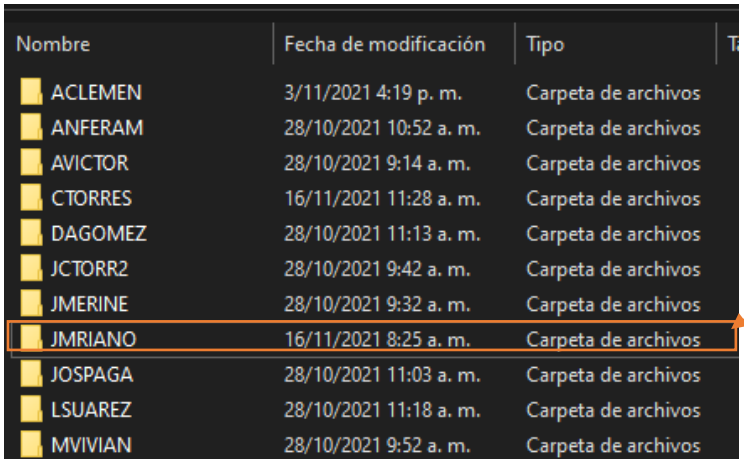


Ilustración 98 Visualización carpeta JMRIANO

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **JMRIANO** identificada dentro del disco duro como se observa en las siguientes imágenes:

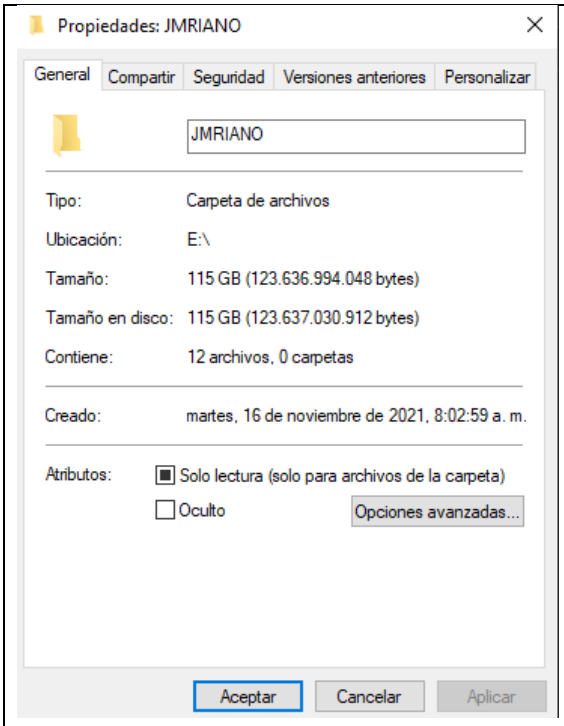


Ilustración 99 Propiedades de la carpeta JMRIANO visto desde el Disco Duro.

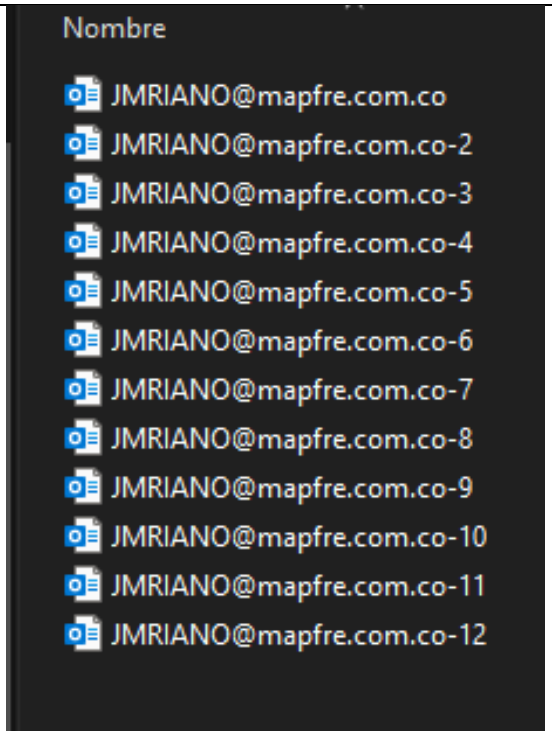


Ilustración 100 Contenido de la carpeta JMRIANO visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**jmriano@mapfre.com.co.**" asignado a **José Manuel RIAÑO** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **10:25:29** y culminando el mismo de forma satisfactoria a las **10:58:24,** tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_22NOV2021
Número de prueba: 10_JMRIANO
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO JMRIANO@MAPFRE.COM.CO, ENTREGADOS POR

MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for
I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad1:
[Custom Content Sources]
K::K:\ | JMRIANO | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: de6744c8bb0c6717f072120e5caaa982
SHA1 checksum: a37b029f544c9f91919cd44368238523600bb645

Image information:
Acquisition started: Mon Nov 22 10:25:29 2021
Acquisition finished: Mon Nov 22 10:49:47 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad29

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad30

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad31

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad32

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad33

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad34

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad35

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad36

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad37

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad38

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad39

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad40

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad41

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad42

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad43

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad44

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad45

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad46

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad47

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad48

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad49

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad50

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad51

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad52

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad53

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad54

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad55

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad56

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad57

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad58

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad59

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad60

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad61

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad62

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad63

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad64

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad65

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad66

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad67

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad68

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad69

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad70

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad71

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad72

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad73

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad74

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad75

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad76

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad77 I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad78 I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad79 Image Verification Results: Verification started: Mon Nov 22 10:49:48 2021 Verification finished: Mon Nov 22 10:58:24 2021 MD5 checksum: de6744c8bb0c6717f072120e5caaa982 : verified SHA1 checksum: a37b029f544c9f91919cd44368238523600bb645 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB,** el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:





Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**jmriano@mapfre.com.co.**" asignado a **José Manuel RIAÑO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 101 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO JMRIANO@MAPFRE.COM.CO."**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo

electrónico **jmriano@mapfre.com.co** asignada **José Manuel RIAÑO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
10	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	José Manuel RIAÑO → jmriano@mapfre.com.co	ad1	115 GB
TOTAL					**115 GB**

Tabla 21 Detalle del buzón de correo electrónico asignado jmriano@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico jmriano@mapfre.com.co asignado a **José Manuel RIAÑO** para el desarrollo de sus funciones **aloja** un total de **115GB,** dentro de este espacio el laboratorio de informática forense logró hallar un total de **Tres millones veinticinco mil ciento dieciocho (3.025.118)** archivos (incluyendo carpetas), como se observa a continuación.



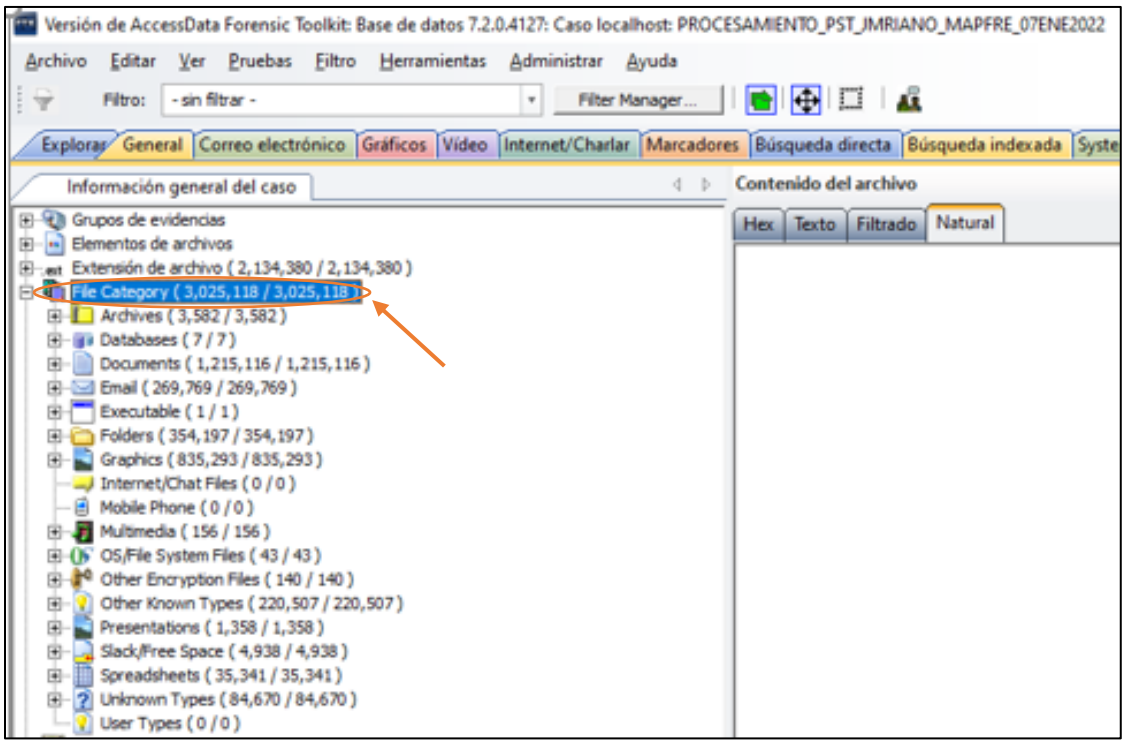


Ilustración 102 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico jmriano@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JOSÉ MANUEL RIAÑO → JMRIANO@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico jmriano@mapfre.com.co asignado a José Manuel RIAÑO , iniciando el día el **07** de enero de 2022 con una duración aproximada de dieciocho (18) días calendario, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Cuatrocientos ochenta y siete mil ciento cincuenta y siete (487.157)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

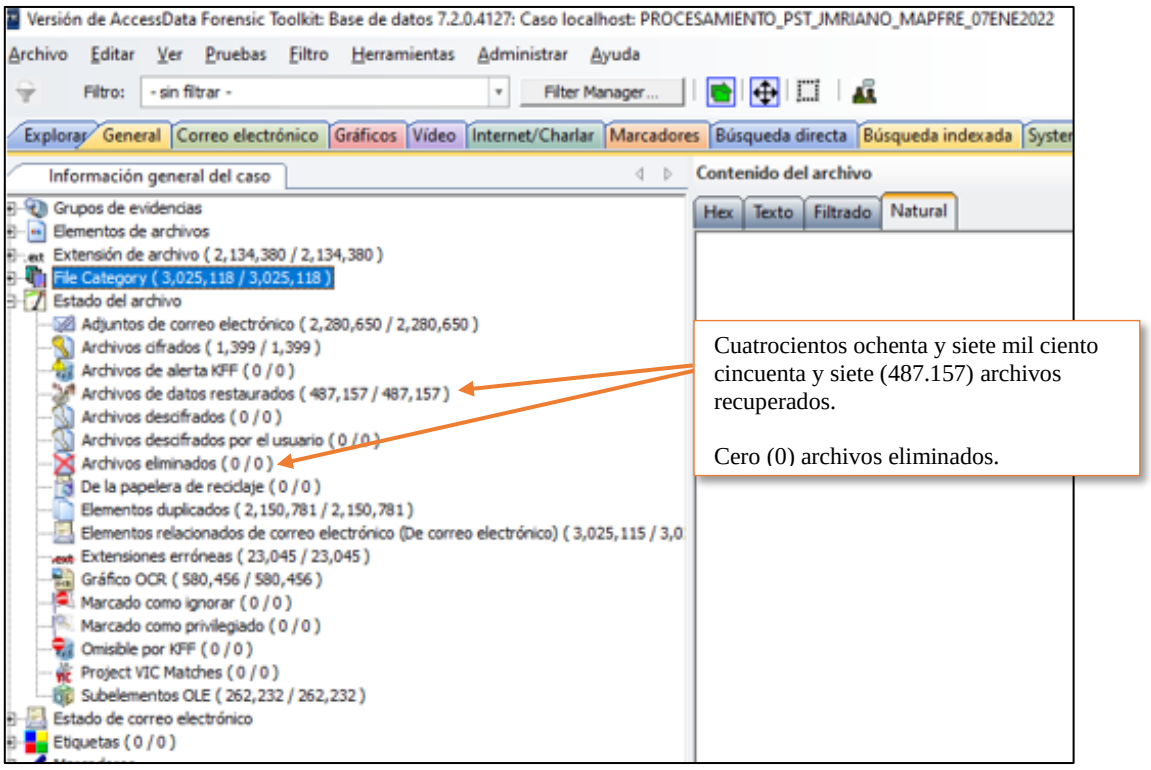


ilustración 103 Total de archivos recuperados en la cuenta de correo electrónico jmriano@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Tres millones veinticinco mil ciento dieciocho (3.025.118)** de archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO JMRIANO@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico jmriano@mapfre.com.co asignado a **José Manuel RIAÑO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	3.582
2	Bases de Datos	7
3	Documentos	1.215.116
4	Correo Electrónico	269.769
5	Ejecutables	1
6	Carpetas	354.197
7	Gráficos	835.293
8	Multimedia	156
9	Archivos del sistema	43
10	Otros archivos encriptados	140
11	Otros archivos desconocidos	220.507
12	Presentaciones	1.358
13	Espacio libre	4.938
14	Hojas de cálculo	35.341
15	Tipos de archivos desconocidos	84.670
TOTAL		**3.025.118**

Tabla 22 Información buscada evidencia 10_JMRIANO, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Tres millones veinticinco mil ciento dieciocho (3.025.118).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Dos millones doscientos ochenta mil seiscientos cincuenta (2.280.650) archivos de**

datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Los archivos cifrados recuperados **Mil trescientos noventa y nueve (1.399) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Cuatrocientos ochenta y siete mil ciento cincuenta y siete (487.157) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Dos millones ciento cincuenta mil setecientos ochenta y un (2.150.781) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Tres millones veinticinco mil ciento quince (3.025.115) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Veintitrés mil cuarenta y cinco (23.045) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Quinientos ochenta mil cuatrocientos cincuenta y seis (580.456) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Doscientos sesenta y dos mil doscientos treinta y dos (262.232) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico jmriano@mapfre.com.co asignado a **José Manuel RIAÑO** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



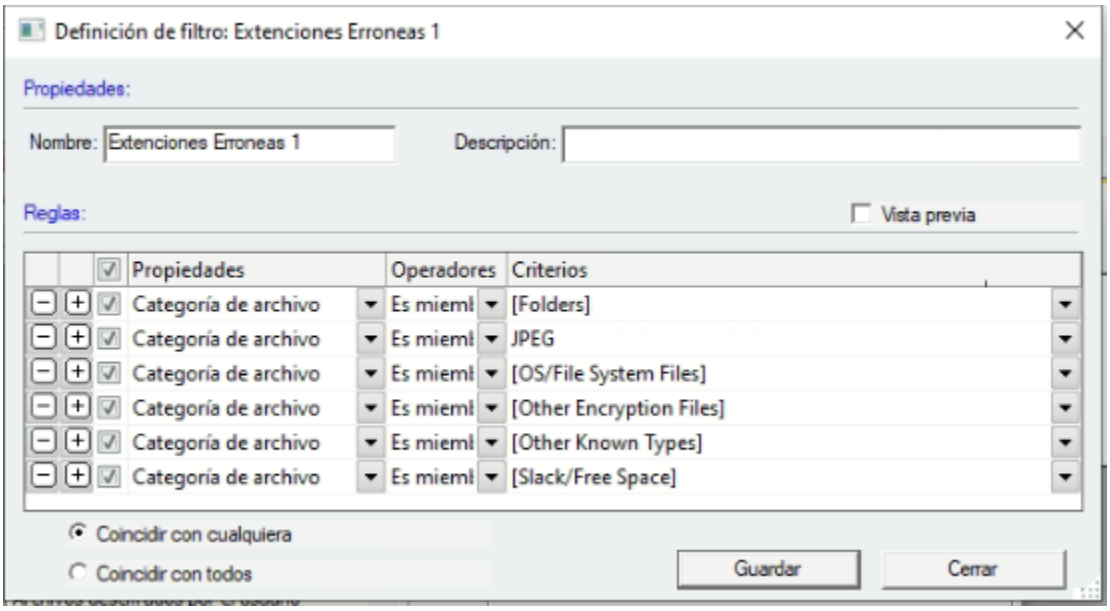


Ilustración 104 Filtro para excluir las extensiones erróneas.

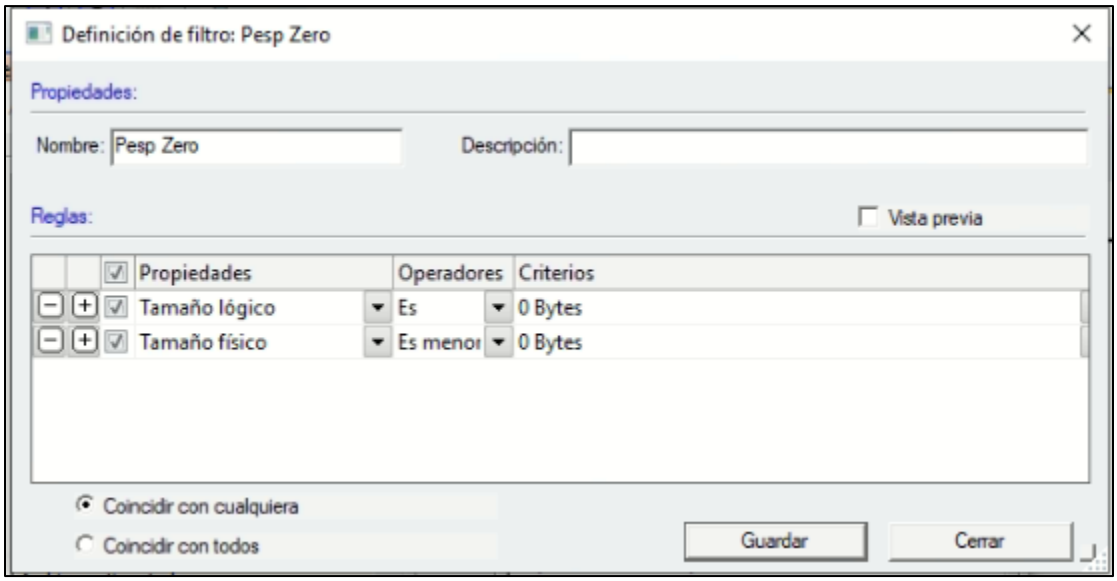


Ilustración 105 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

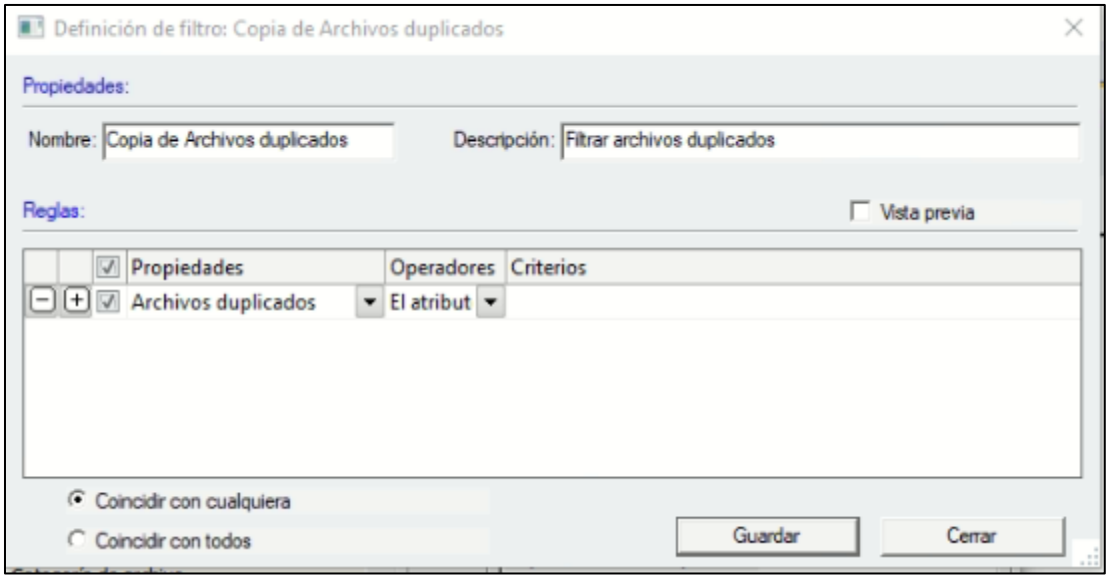


Ilustración 106 Filtro para excluir los archivos duplicados.

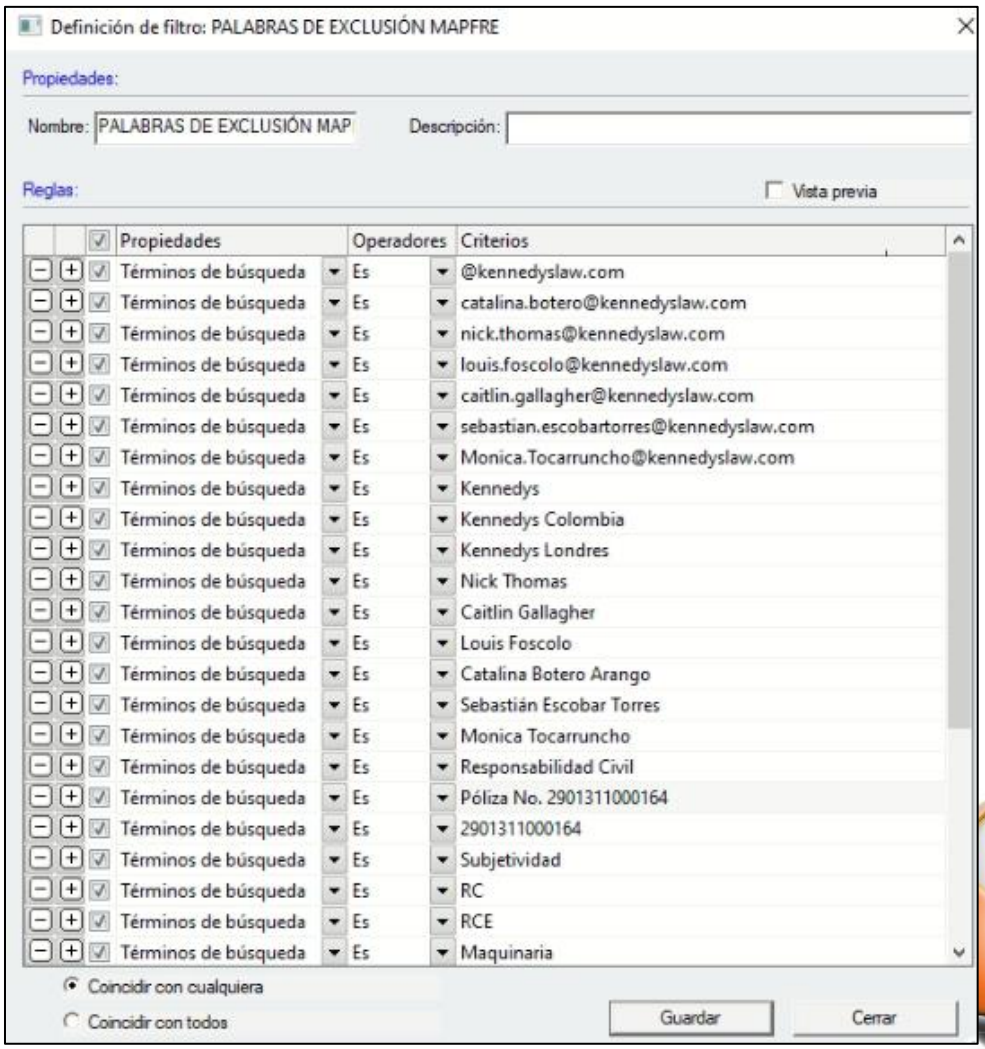


Ilustración 107 Filtro para excluir los archivos suministrado por MAPFRE - 1.

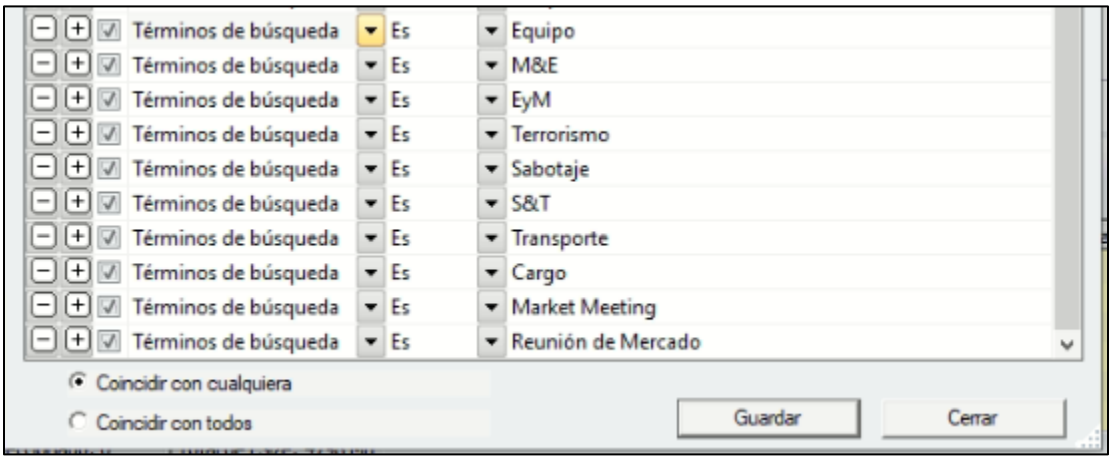
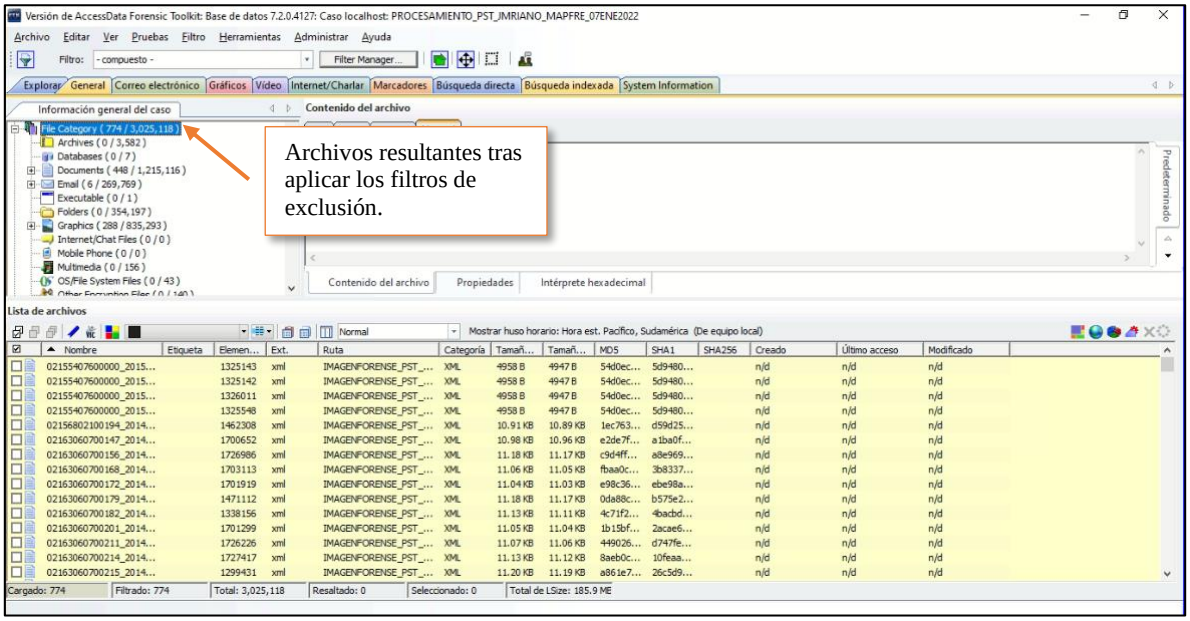


Ilustración 108 Filtro para excluir los archivos suministrado por MAPFRE - 2.

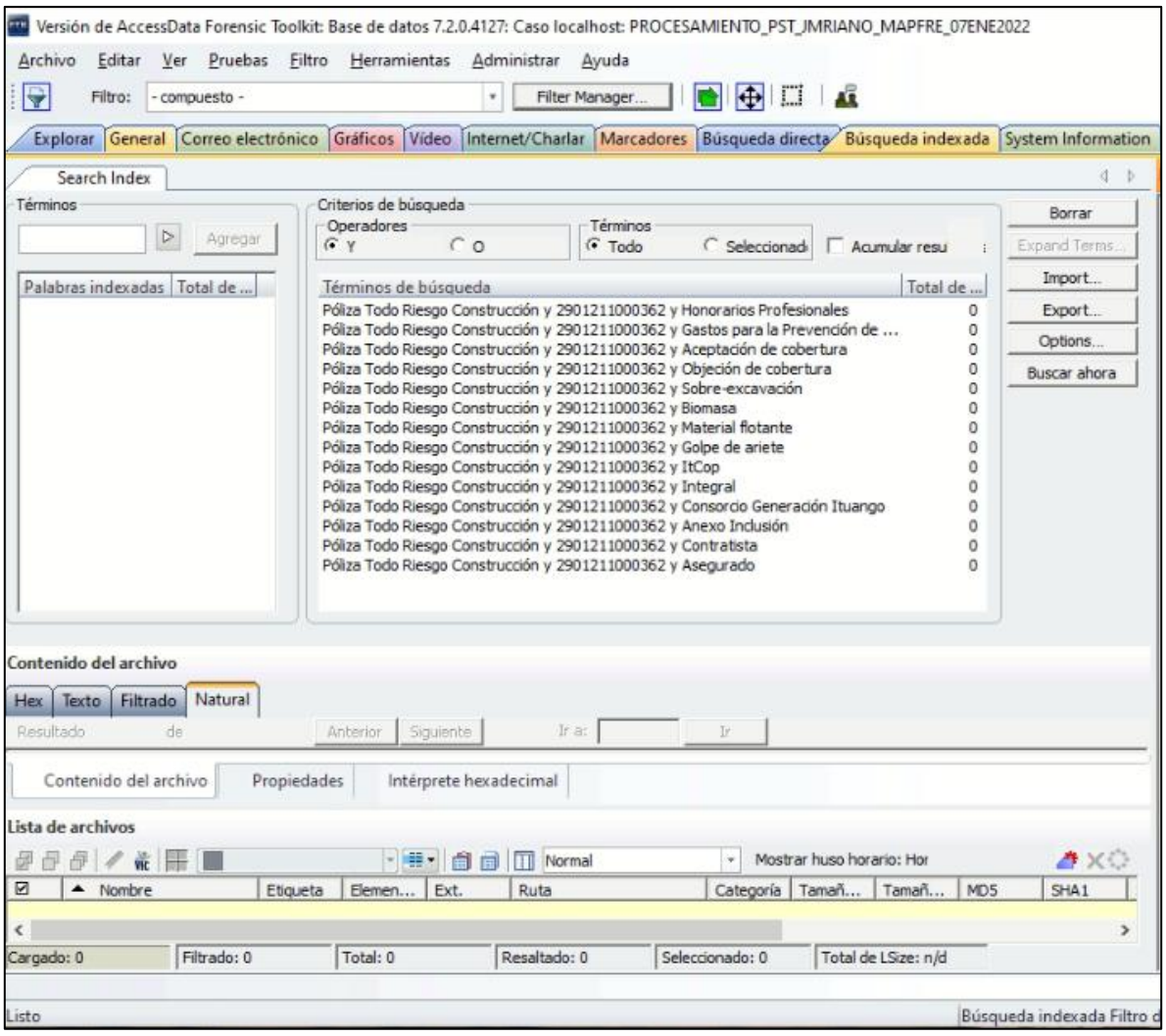
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Setecientos setenta y cuatro (774)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo jmriano@mapfre.com.co asignado a **José Manuel RIAÑO** para el desarrollo de sus funciones.

11. Buzón de correo electrónico jmerine@mapfre.com.co.

El día 22 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **JMERINE**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

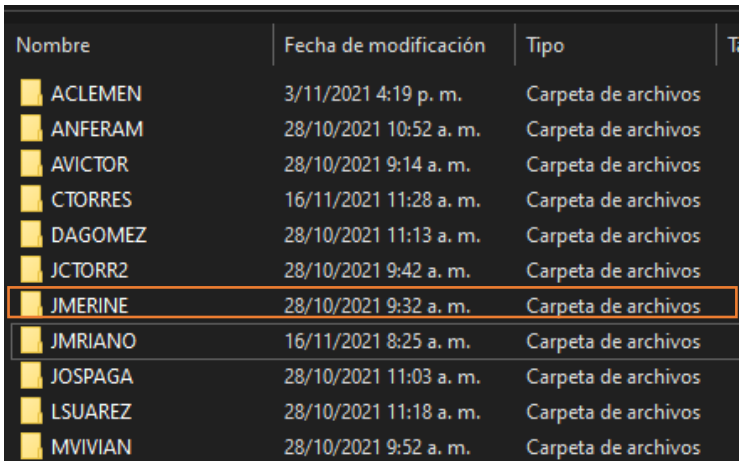


Ilustración 109 Visualización carpeta JMERINE.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **JMERINE** identificada dentro del disco duro como se observa en las siguientes imágenes:

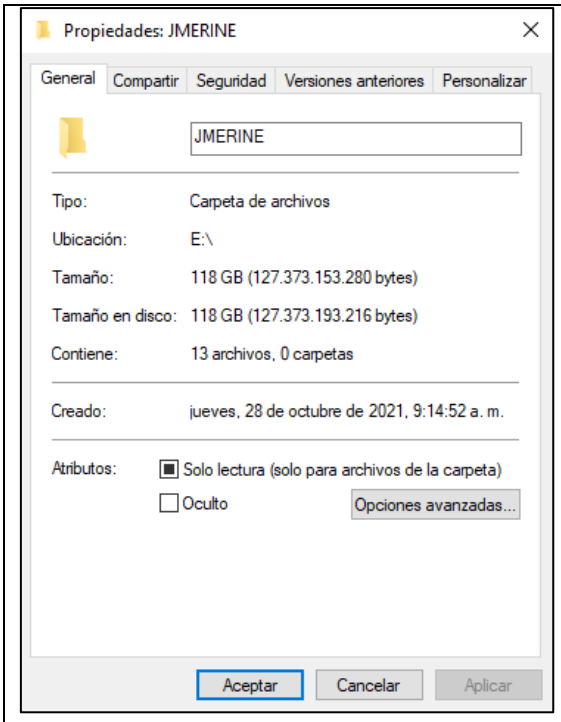


Ilustración 110 Propiedades de la carpeta JMERINE visto desde el Disco Duro.

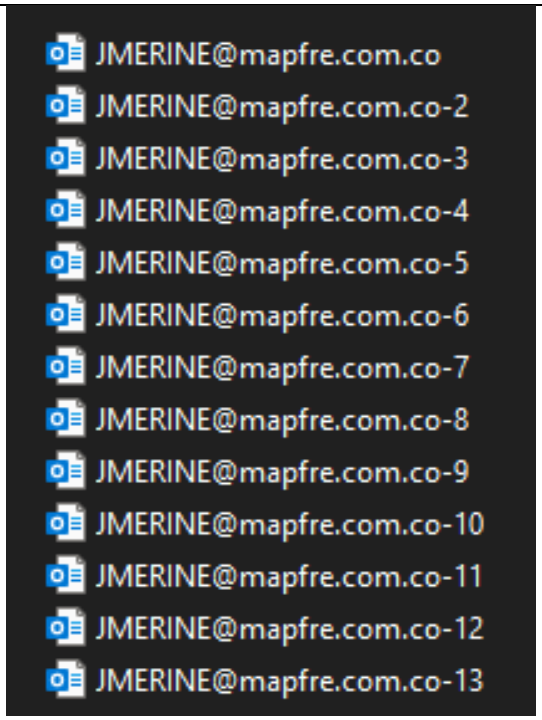


Ilustración 111 Contenido de la carpeta JMERINE visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**jmerine@mapfre.com.co.**" asignado a

José Manuel MERINERO MARTIN para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **11:13:27** y culminando el mismo de forma satisfactoria a las **11:47:50,** tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_22NOV2021
Número de prueba: 11_JMERINE
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO JMERINE@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for
I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad1:
[Custom Content Sources]
K::K:\ | JMERINE | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 4ca2ff21652b030e18792d53572fc81a
SHA1 checksum: fdf3b09289d272e99375b5a141b0617ae789e477

Image information:
Acquisition started: Mon Nov 22 11:13:27 2021
Acquisition finished: Mon Nov 22 11:38:20 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad29

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad30

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad31

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad32

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad33

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad34

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad35

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad36

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad37

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad38

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad39

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad40

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad41

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad42

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad43

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad44

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad45

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad46

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad47

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad48

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad49

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad50

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad51

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad52

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad53

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad54

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad55

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad56

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad57

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad58

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad59

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad60

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad61

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad62

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad63

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad64

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad65

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad66

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad67

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad68

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad69

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad70

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad71

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad72

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad73

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad74

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad75

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad76

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad77

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad78

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad79

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad80

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad81

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad82

Image Verification Results:
Verification started: Mon Nov 22 11:38:23 2021
Verification finished: Mon Nov 22 11:47:50 2021
MD5 checksum: 4ca2ff21652b030e18792d53572fc81a : verified
SHA1 checksum: fdf3b09289d272e99375b5a141b0617ae789e477 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**jmerine@mapfre.com.co.**" asignado a **José Manuel MERINERO MARTIN** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 112 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO JMERINE@MAPFRE.COM.CO.

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**. para la cuenta de correo electrónico jmerine@mapfre.com.co asignada a **José Manuel MERINERO MARTIN** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
11	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	José Manuel MERINERO MARTIN → jmerine@mapfre.com.co	ad1	118 GB
TOTAL					**118 GB**

Tabla 23 Detalle del buzón de correo electrónico asignado jmerine@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico jmerine@mapfre.com.co asignado a **José Manuel MERINERO**

MARTIN para el desarrollo de sus funciones **aloja** un total de **118 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Trescientos treinta y seis mil seiscientos veintiséis (336.626)** archivos (incluyendo carpetas), como se observa a continuación.

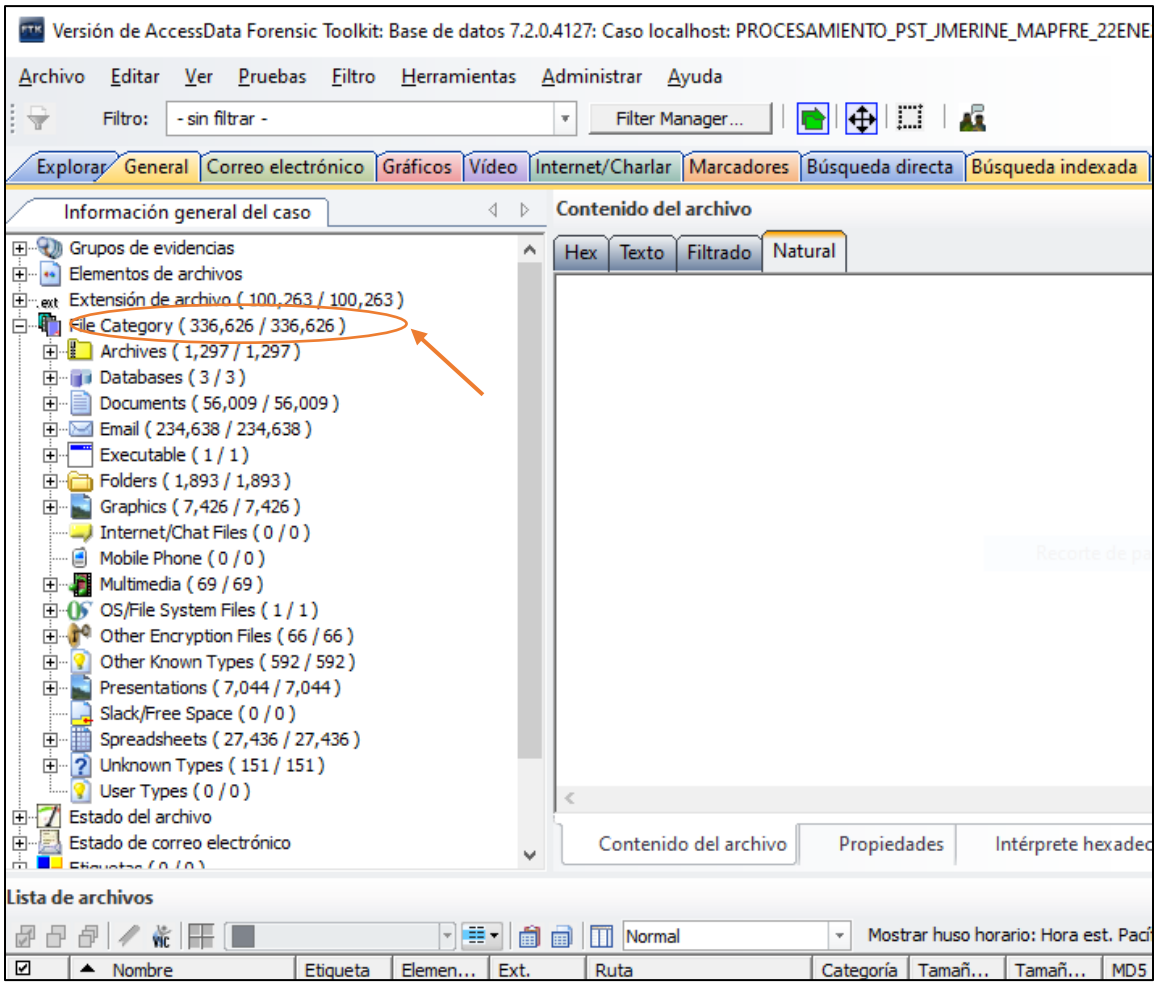


Ilustración 113 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico jmerine@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JOSÉ MANUEL MERINERO MARTIN → JMERINE@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico jmerine@mapfre.com.co asignado a **José Manuel MERINERO MARTIN**, iniciando el día el **22** de enero

del 2022 con una duración aproximada de Siete (7) día calendario, el resultado a dicho proceso arrojó que existen **cero (0)** ítems en condición de "eliminados" y se reconstruyeron **cero (0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

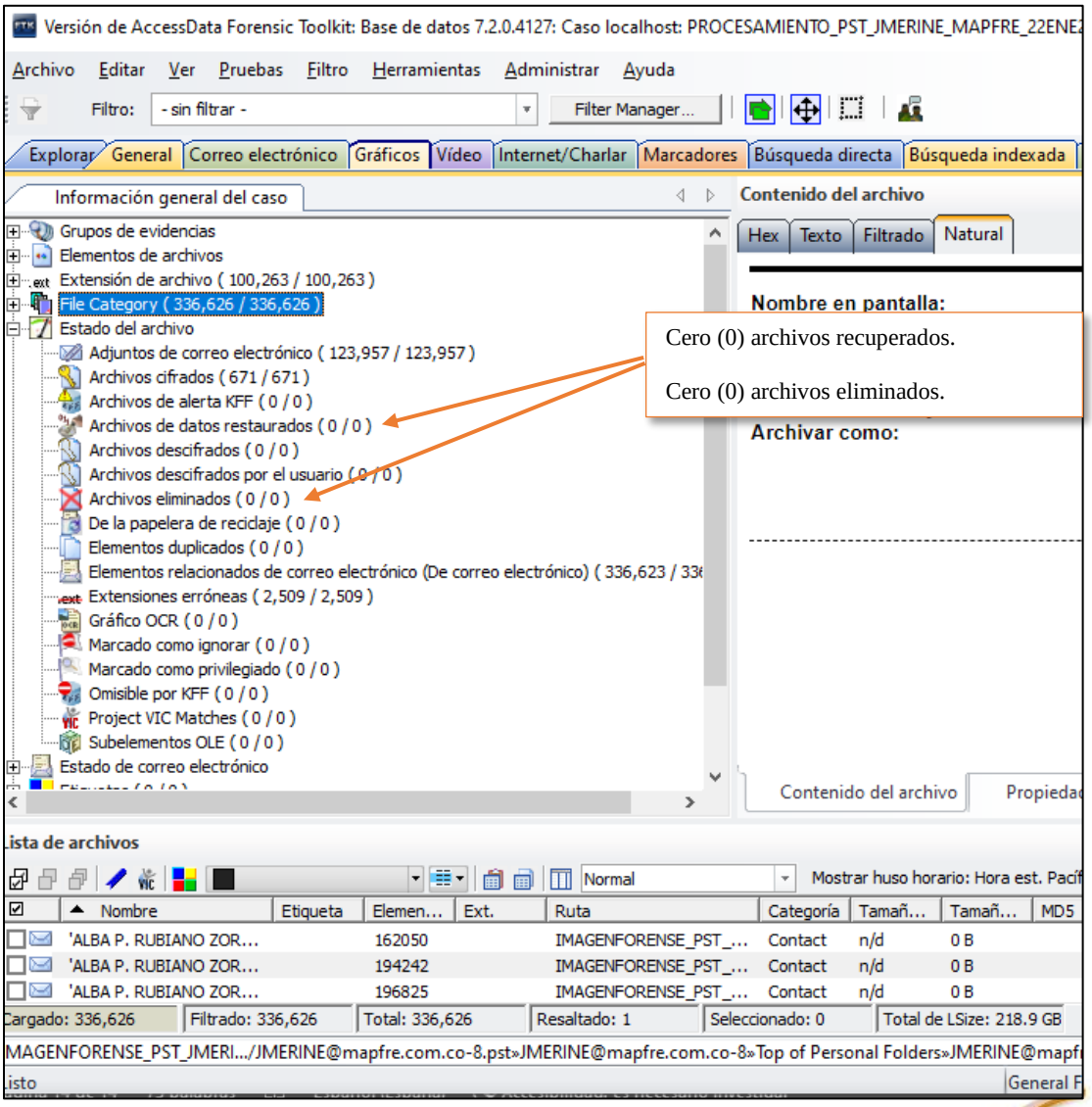


ilustración 114 Total de archivos recuperados en la cuenta de correo electrónico jmerine@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS**

GENERALES DE COLOMBIA S.A., es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Trescientos treinta y seis mil seiscientos veintiséis (336.626)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO JMERINE@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico jmerine@mapfre.com.co asignado a **José Manuel MERINERO MARTIN** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1.297
2	Bases de Datos	3
3	Documentos	56.009
4	Correo Electrónico	234.638
5	Ejecutables	1
6	Carpetas	1.893
7	Gráficos	7.426
8	Multimedia	69
9	Archivos del sistema	1
10	Otros archivos encriptados	66
11	Otros archivos desconocidos	592
12	Presentaciones	7.044
13	Hojas de cálculo	27.436
14	Tipos de archivos desconocidos	151
TOTAL		**336.626**

Tabla 24 Información buscada evidencia 011_JMERINE, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Trescientos treinta y seis mil seiscientos veintiséis (336.626).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Ciento veintitrés mil novecientos cincuenta y siete (123.957) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Seiscientos setenta y un (671) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Trescientos treinta y seis mil seiscientos veintitrés (336.623) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Dos mil quinientos nueve (2.509) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico jmerine@mapfre.com.co asignado a **José Manuel MERINERO MARTIN** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

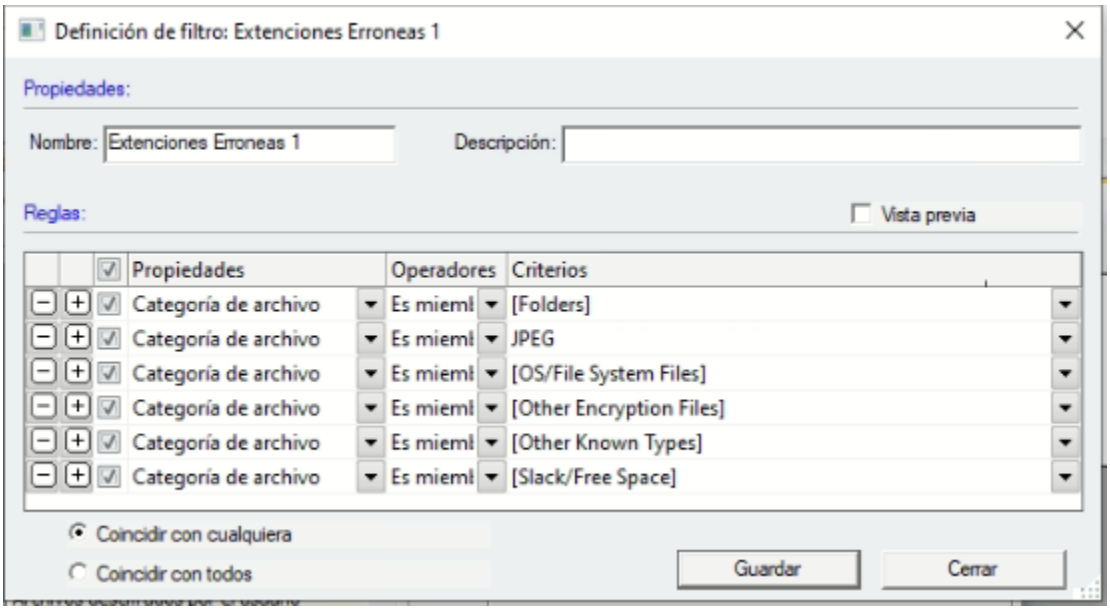


Ilustración 115 Filtro para excluir las extensiones erróneas.

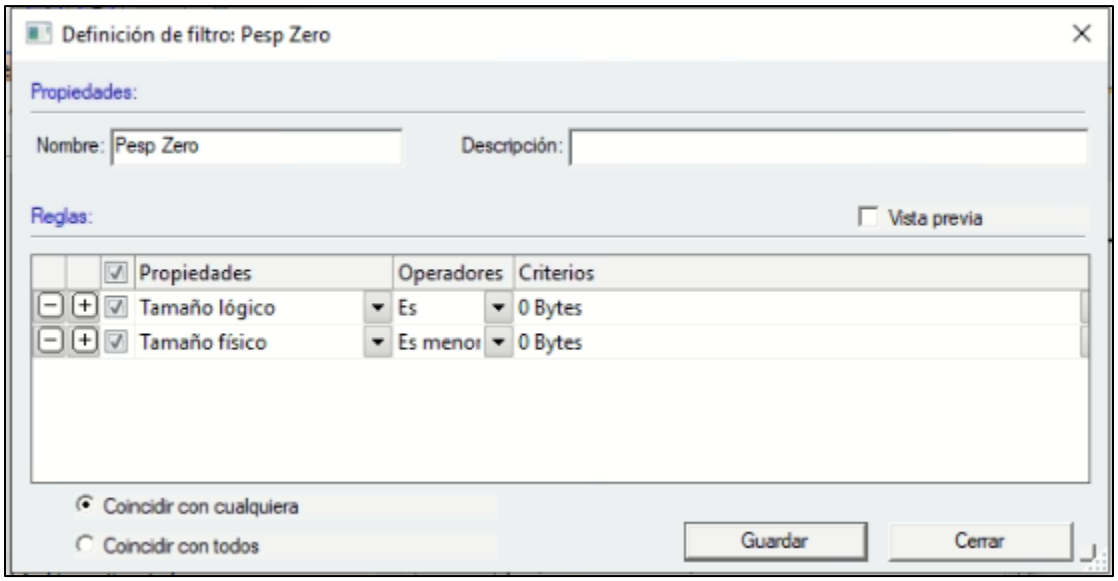


Ilustración 116 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

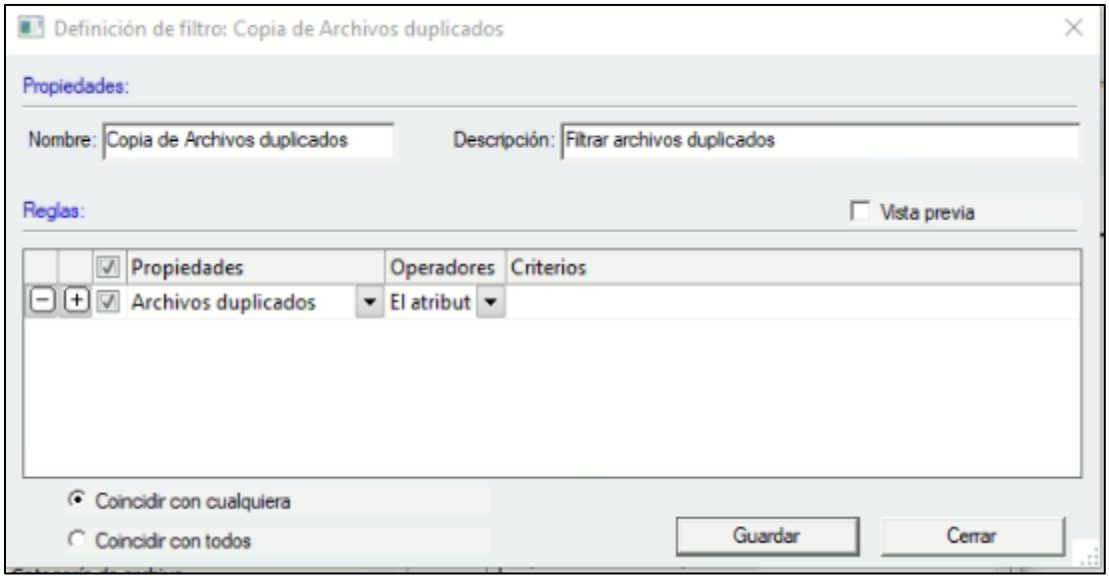


Ilustración 117 Filtro para excluir los archivos duplicados.

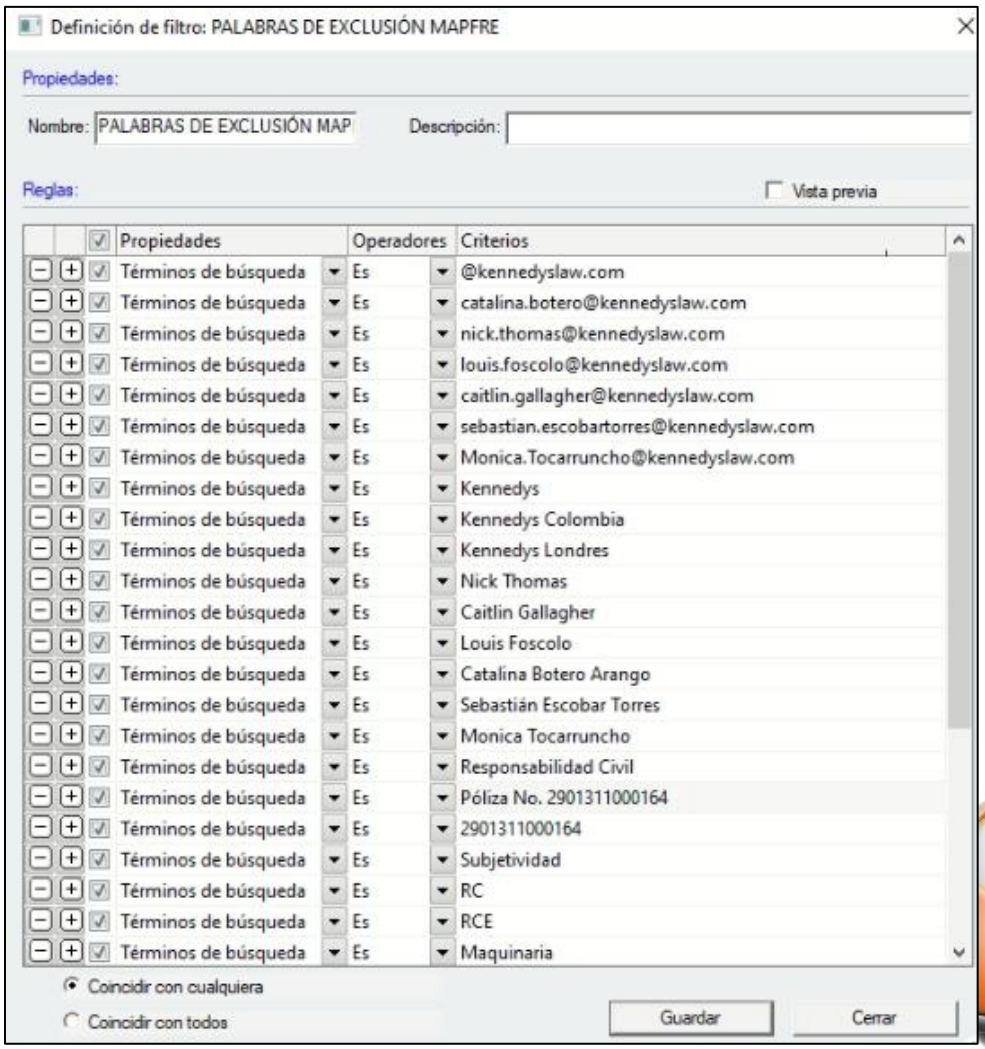


Ilustración 118 Filtro para excluir los archivos suministrado por MAPFRE - 1.

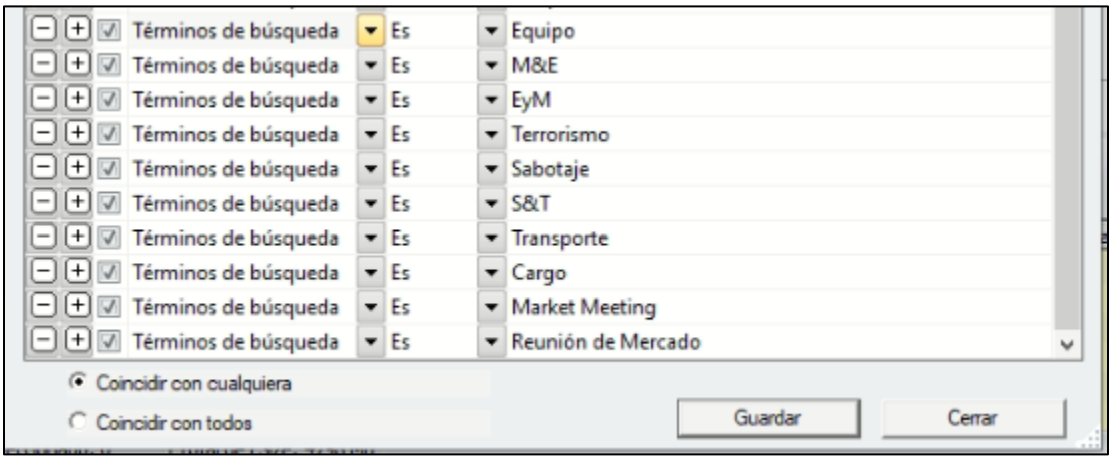
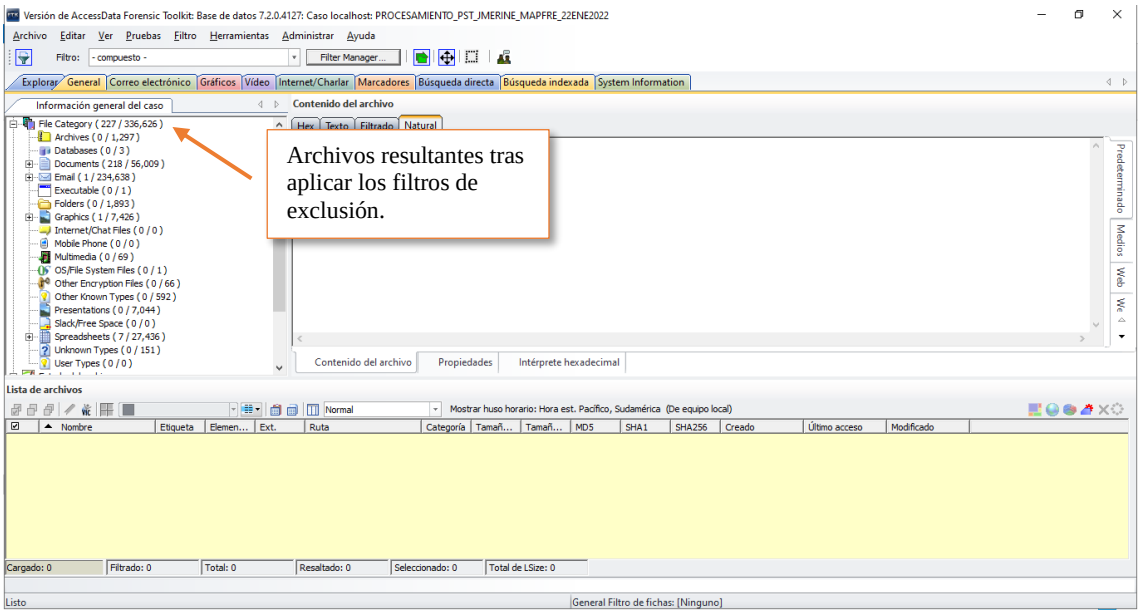


Ilustración 119 Filtro para excluir los archivos suministrado por MAPFRE - 2.

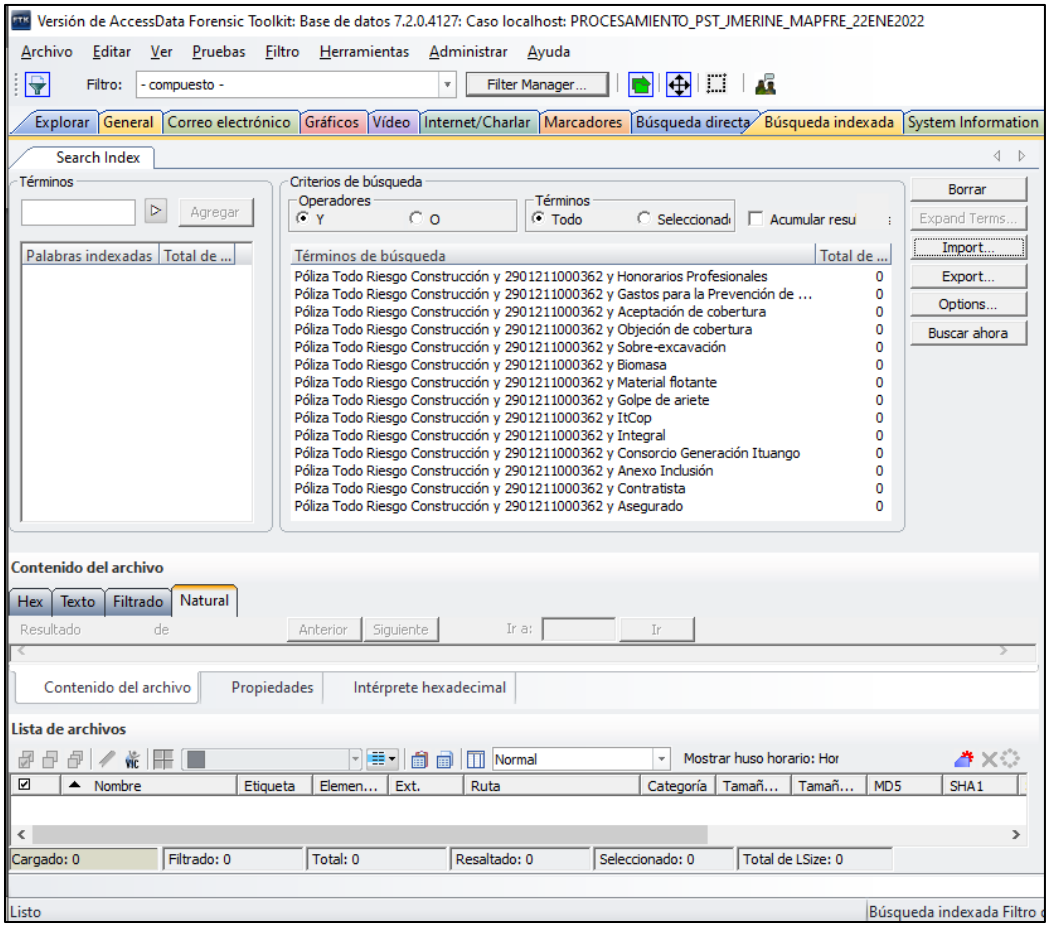
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Doscientos veintisiete (227)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo jmerine@mapfre.com.co asignado a **José Manuel MERINERO MARTIN** para el desarrollo de sus funciones.

Una vez realizadas las imágenes forenses para los buzones de correo electrónico pertenecientes a exfuncionarios de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** los cuales se encuentran identificados con las siguientes direcciones de correo (aclemen@mapfre.com.co, anferam@mapfre.com.co, avictor@mapfre.com.co, ctorres@mapfre.com.co, dagomez@mapfre.com.co, jctorr2@mapfre.com.co, jmerine@mapfre.com.co, jmriano@mapfre.com.co, jospaga@mapfre.com.co, lsuarez@mapfre.com.co, mvivian@mapfre.com) el equipo de ADALID CORP hace entrega de (1) Un disco duro color blanco, con capacidad de almacenamiento de **1000GB** al señor **Willigton Leandro TORRES MORALES,** identificado con cédula de ciudadanía **No. 79.708.420** de Bogotá, quien funge como **PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN** el día 30 de noviembre a las 11:50 horas.

El día 01 de diciembre de 2021, el señor **Willigton Leandro TORRES MORALES** hace entrega a los peritos de ADALID CORP. de (1) Un disco duro color blanco, con capacidad de almacenamiento de **1000GB,** el cual en su parte superior se encuentra marcado como **"prueba extraprocesal"** como se presenta a continuación**:**

	
Fotografía Disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista superior)	Fotografía disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista posterior)

Dentro del Disco Duro se encuentran los archivos en formato .PST de las cuentas de correo electrónico asignadas a Once (11) funcionarios que se encuentran retirados y Cuatro (4) cuentas de correo electrónico de funcionarios activos dentro de la empresa **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A,** los cuales serán mencionados a continuación:

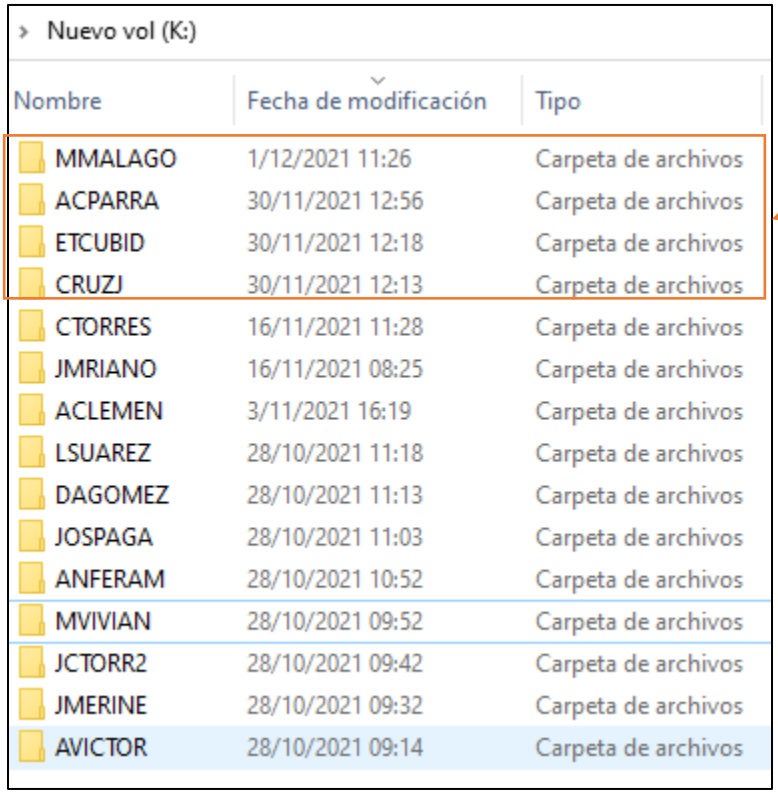


Ilustración 120 Visualización contenido completo del Disco Duro entregado por MAPFRE SEGUROS GENERALES DE COLOMBIA S.A a 01 de diciembre de 2021.

Los correos electrónicos suministrados el 01 de diciembre de 2021 serán presentados a continuación:

Correos funcionarios retirados	ORDEN ENVIO IMÁGENES fecha en la que se realizo	Tamaño GB
mmalago@mapfre.com.co	15 - 01-diciembre-2021	58.3 GB
acparra@mapfre.com.co	12 - 01-diciembre-2021	43.0 GB
etcubid@mapfre.com.co	14 - 01-diciembre-2021	55.9 GB
cruzj@mapfre.com.co	13 - 01-diciembre-2021	50.1 GB

Tabla 25 *Buzones de correo suministrados el 01 de diciembre de 2021.*

12. Buzón de correo electrónico acparra@mapfre.com.co.

El día 01 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta **ACPARRA**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

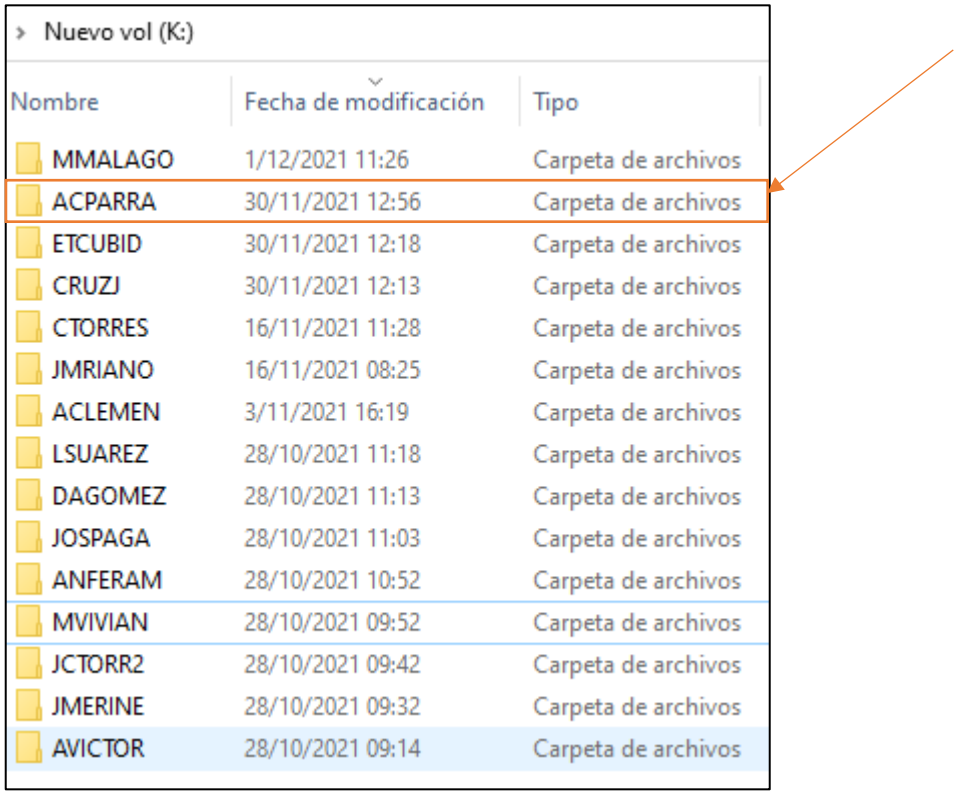


Ilustración 121 Visualización carpeta ACPARRA.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **ACPARRA** identificada dentro del disco duro como se observa en las siguientes imágenes:

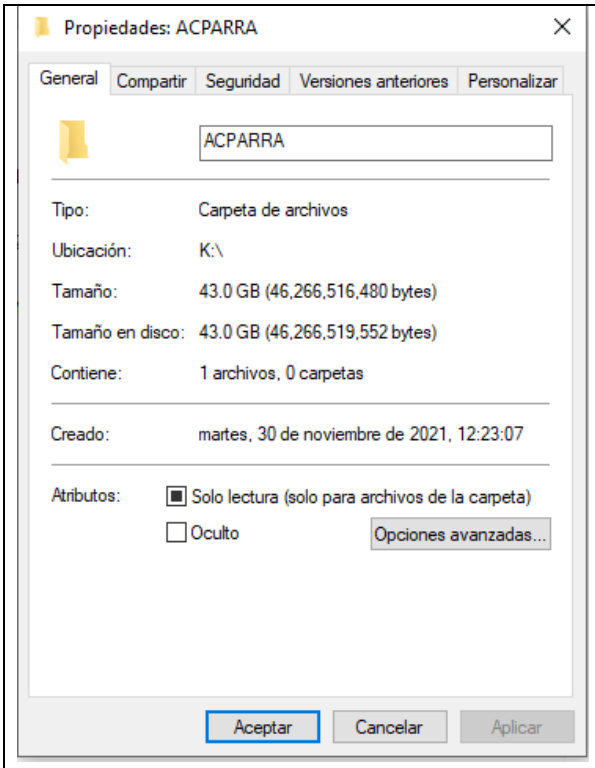


Ilustración 122 Propiedades de la carpeta ACPARRA visto desde el Disco Duro.

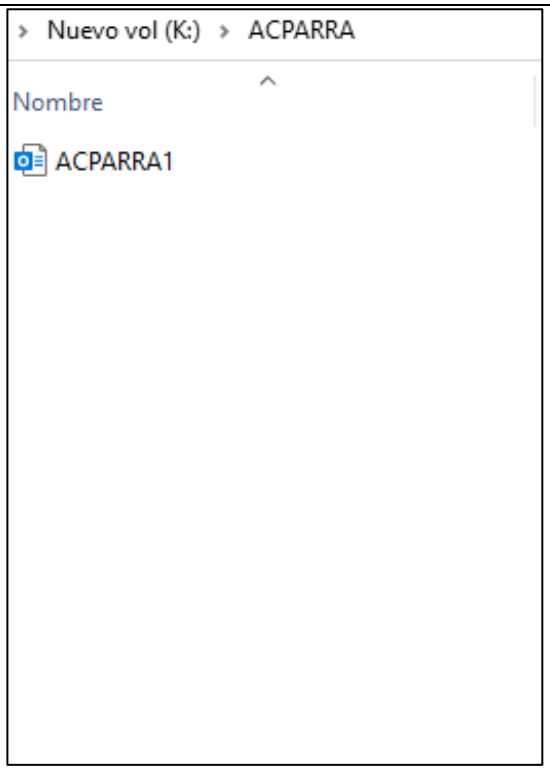


Ilustración 123 Contenido de la carpeta ACPARRA visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**acparra@mapfre.com.co.**" asignado a **Andrés Camilo PARRA BALAGUERO** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **14:12:31** y culminando el mismo de forma satisfactoria a las **15:14:07**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_01DIC2021
Número de prueba: 012_ACPARRA
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ACPARRA@MAPFRE.COM.CO, ENTREGADOS POR

MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP S.A.S. - Hector Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad1:
[Computed Hashes]
MD5 checksum: 31383bb73ba2962329cfe4057918b2ff
SHA1 checksum: d937640697a74fe39a1dabfcfeb857c096bd6b16

Image information:
Acquisition started: Wed Dec 1 14:12:31 2021
Acquisition finished: Wed Dec 1 15:02:34 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad22 I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad23 Image Verification Results: Verification started: Wed Dec 1 15:02:34 2021 Verification finished: Wed Dec 1 15:14:07 2021 MD5 checksum: 31383bb73ba2962329cfe4057918b2ff : verified SHA1 checksum: d937640697a74fe39a1dabfcfeb857c096bd6b16 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**acparra@mapfre.com.co.**" asignado a **Andrés Camilo PARRA BALAGUERO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 124 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ACPARRA@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico acparra@mapfre.com.co asignada **Andrés Camilo PARRA BALAGUERO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
12	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Andrés Camilo PARRA BALAGUERO → acparra@mapfre.com.co	ad1	43.0 GB
TOTAL					**43.0 GB**

Tabla 26 Detalle del buzón de correo electrónico asignado acparra@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico acparra@mapfre.com.co asignado a **Andrés Camilo PARRA BALAGUERO** para el desarrollo de sus funciones **aloja** un total de **43.0 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Seiscientos noventa y dos mil doscientos ochenta y nueve (692.289)** archivos (incluyendo carpetas), como se observa a continuación.

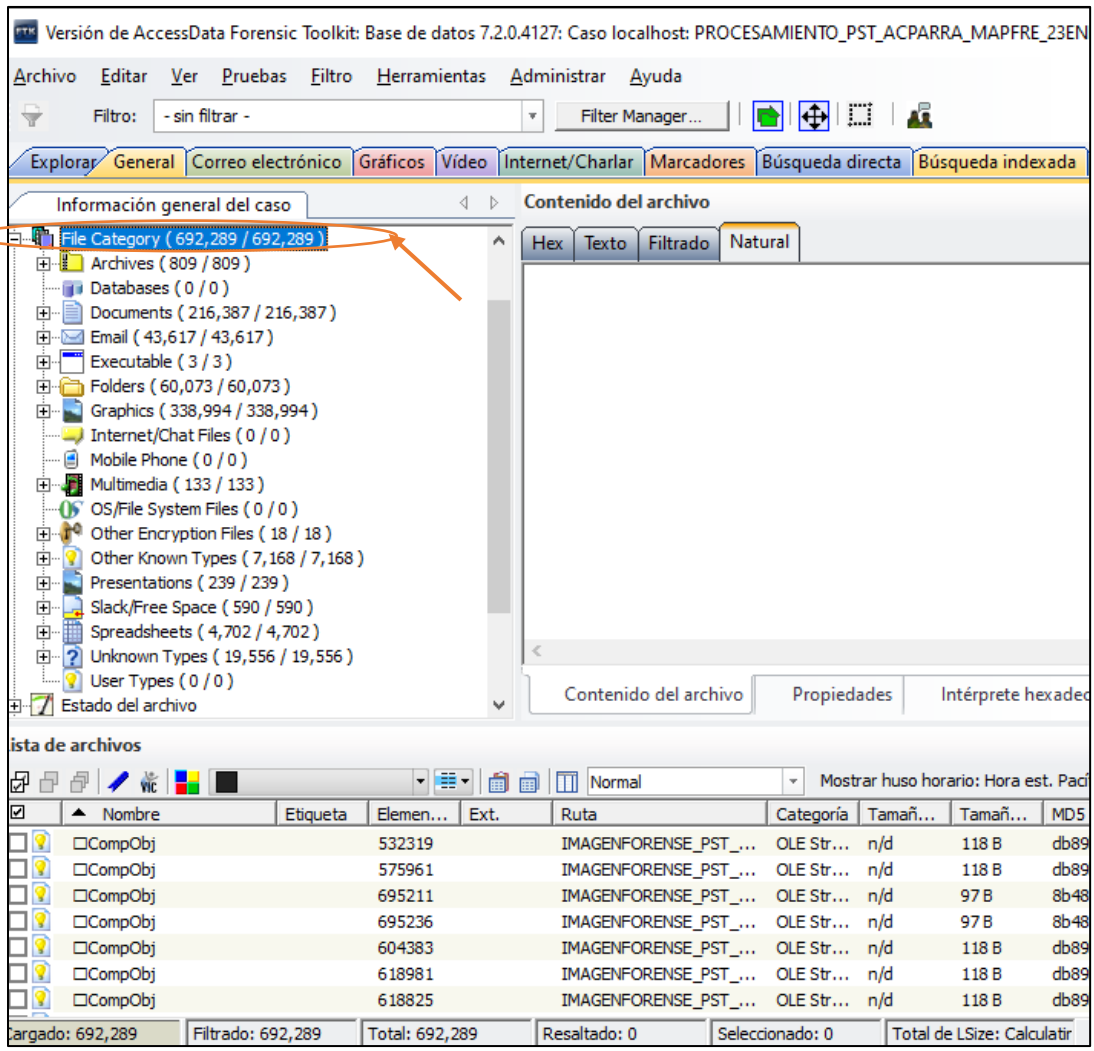


Ilustración 125 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico acparra@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO ANDRÉS CAMILO PARRA BALAGUERO → ACPARRA@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico acparra@mapfre.com.co asignado a **Andrés Camilo PARRA BALAGUERO**, iniciando el día el **23** de enero del 2022 con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **Dos (2)** ítems en condición de "eliminados" y se reconstruyeron **Ciento noventa y siete mil ochocientos veintiocho (197.828)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron

recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

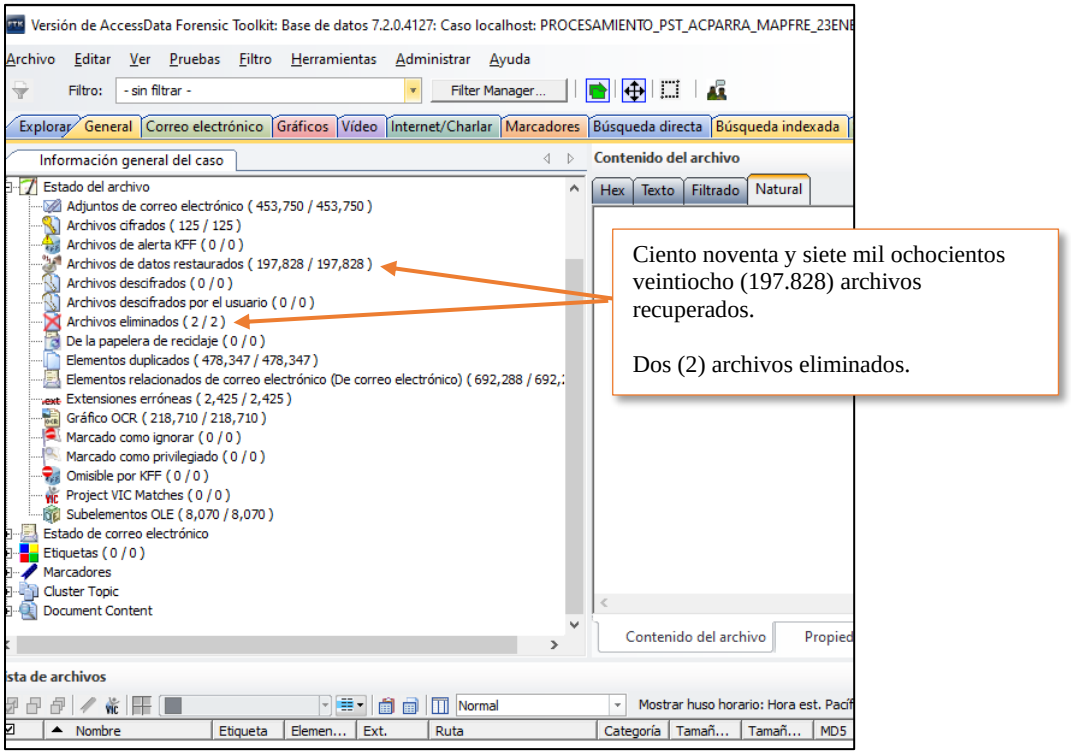


ilustración 126 Total de archivos recuperados en la cuenta de correo electrónico acparra@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Seiscientos noventa y dos mil doscientos ochenta y nueve (692.289)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ACPARRA@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico acparra@mapfre.com.co asignado a **Andrés Camilo PARRA BALAGUERO para** el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	809
2	Documentos	216.387
3	Correo Electrónico	43.617
4	Ejecutables	3
5	Carpetas	60.073
6	Gráficos	338.994
7	Multimedia	133
8	Otros archivos encriptados	18
9	Otros archivos desconocidos	7.168
10	Presentaciones	239
11	Espacio libre del sistema	590
12	Hojas de cálculo	47.02
13	Tipos de archivos desconocidos	19.556
TOTAL		**692.289**

Tabla 27 Información buscada evidencia 012_ACPARRA, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Seiscientos noventa y dos mil doscientos ochenta y nueve (692.289)**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Cuatrocientos cincuenta y tres mil setecientos (453.750) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Ciento veinticinco (125) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Ciento noventa y siete mil ochocientos veintiocho (197.828) archivos de datos obtenidos** por el

proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Archivos de datos Eliminados **Dos (2) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Cuatrocientos setenta y ocho mil trescientos cuarenta y siete (478.347) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Seiscientos noventa y dos mil doscientos ochenta y ocho (692.288) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Dos mil cuatrocientos veinticinco (2.425) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Doscientos dieciocho mil setecientos diez (218.710) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Ocho mil setenta (8.070) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico acparra@mapfre.com.co asignado a **Andrés Camilo PARRA BALAGUERO** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



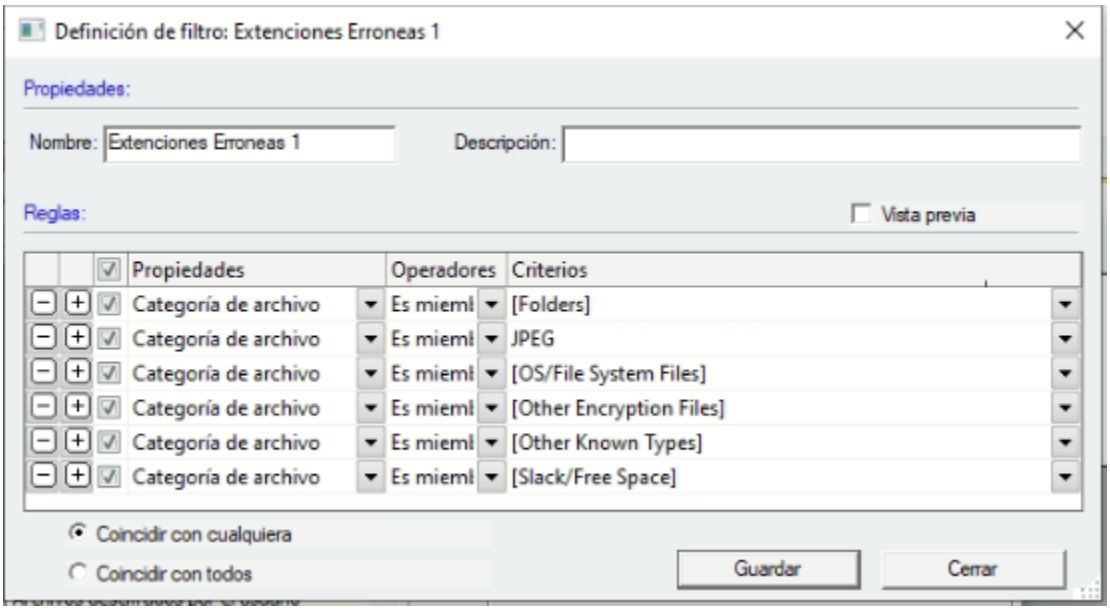


Ilustración 127 Filtro para excluir las extensiones erróneas.

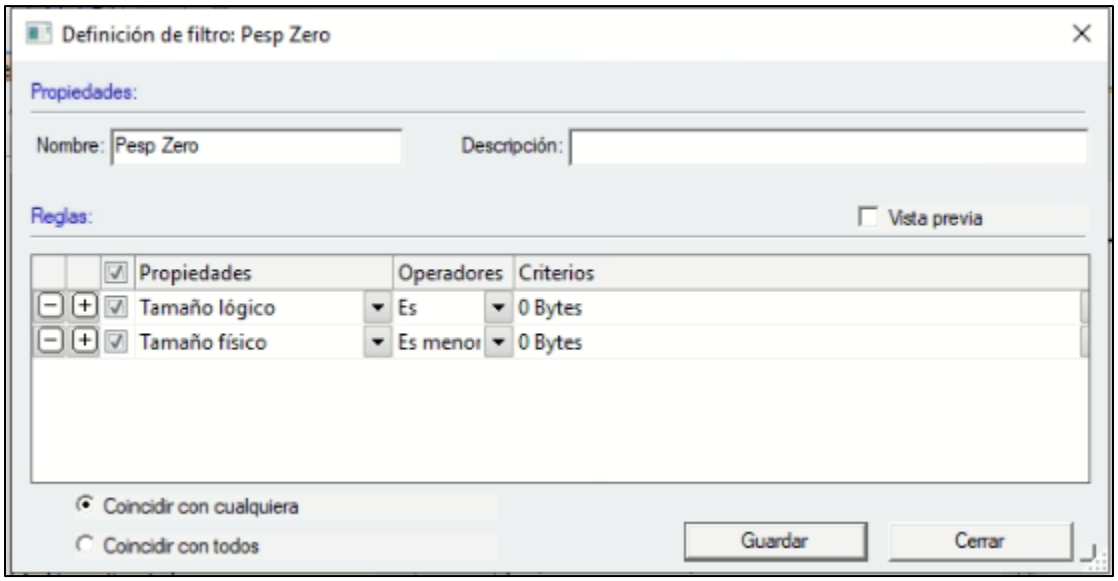


Ilustración 128 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

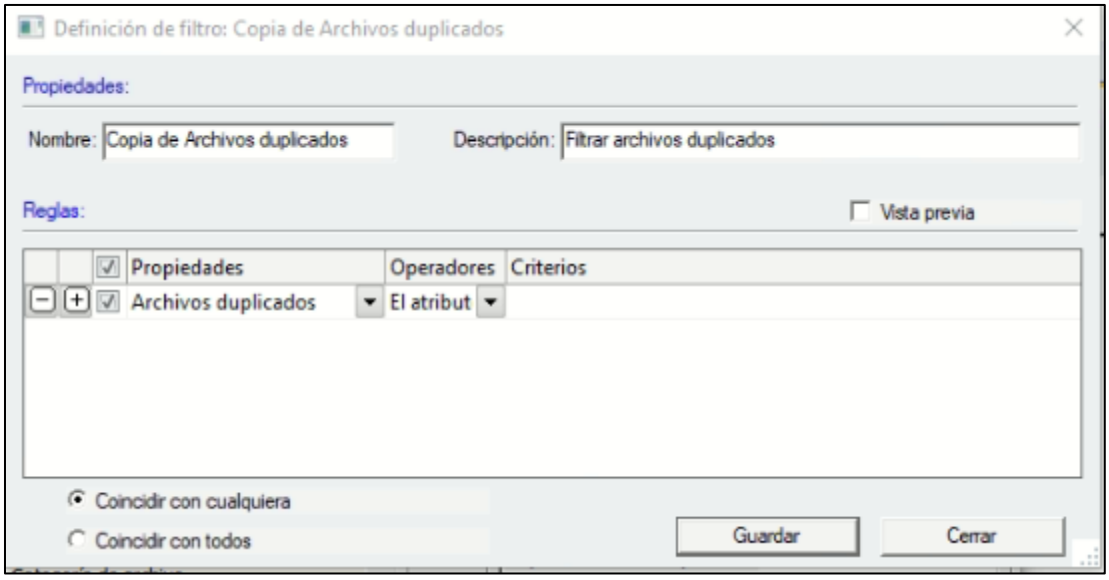


Ilustración 129 Filtro para excluir los archivos duplicados.

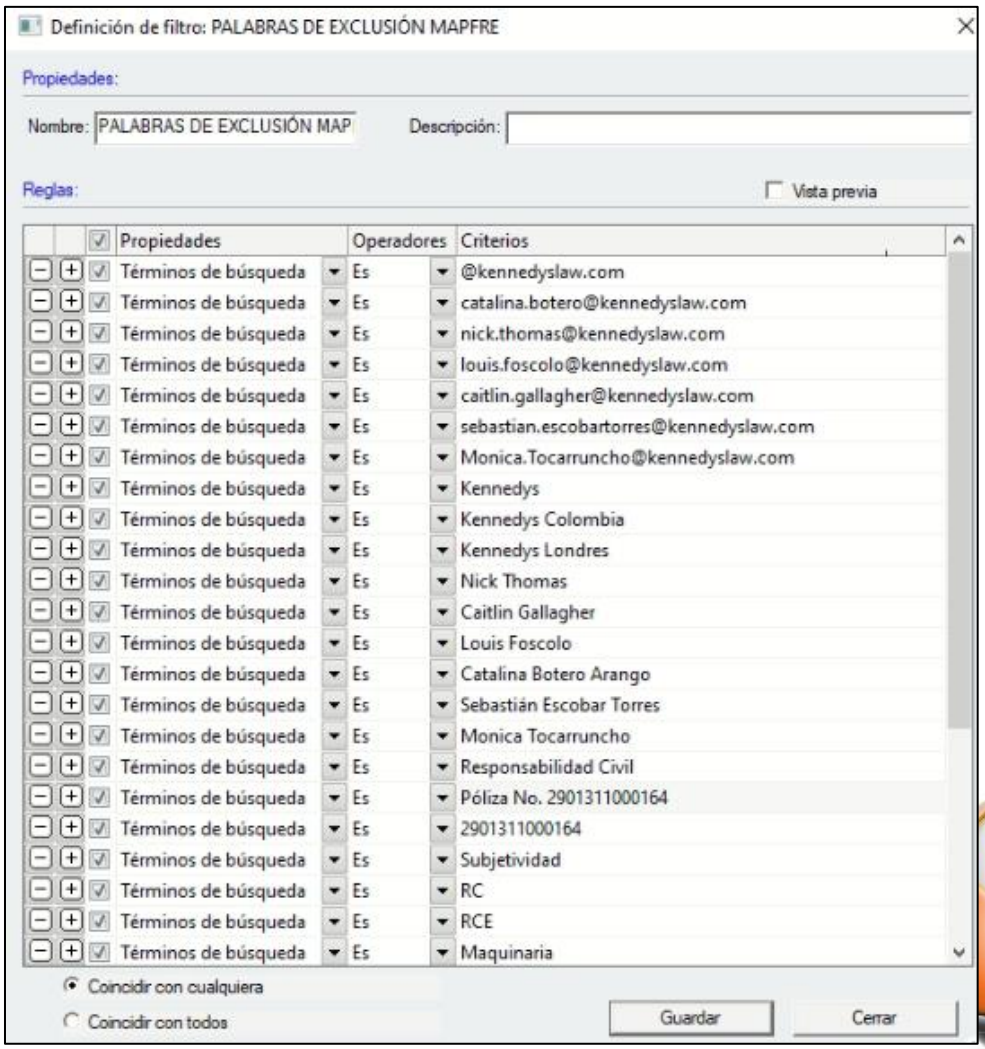


Ilustración 130 Filtro para excluir los archivos suministrado por MAPFRE - 1.

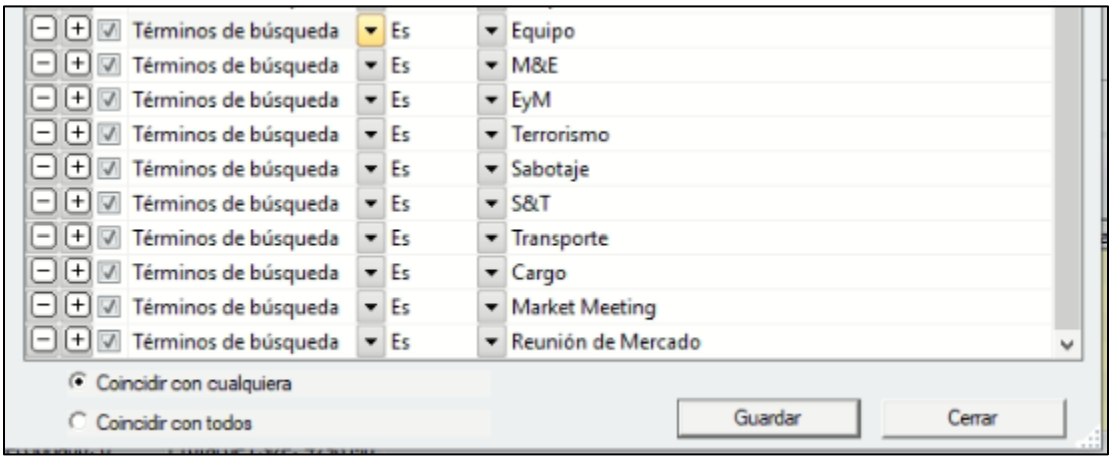
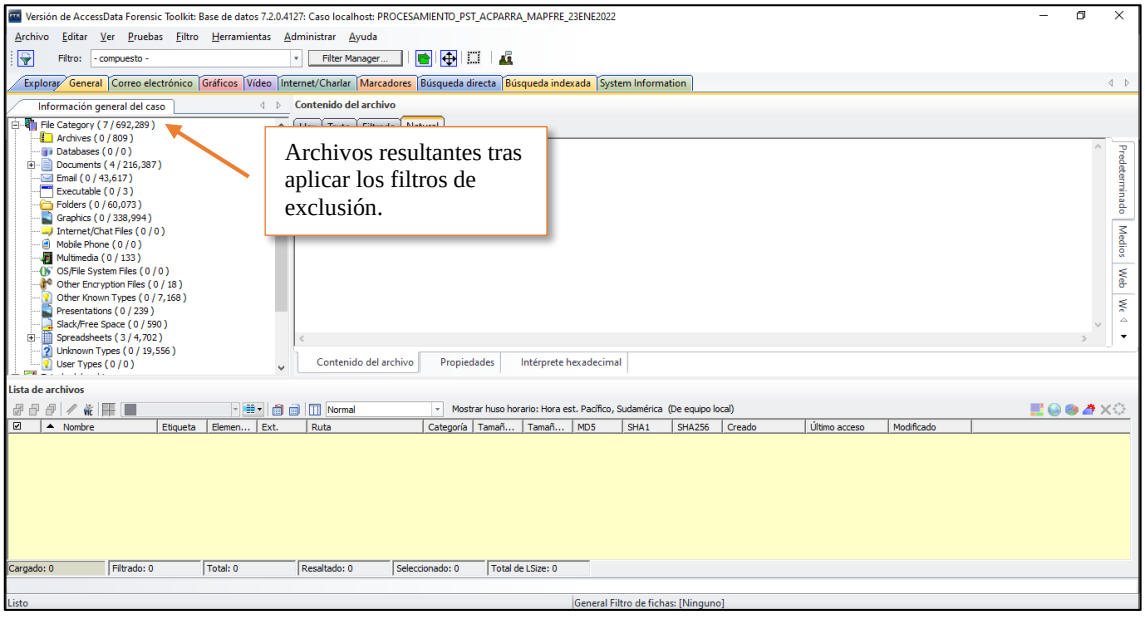


Ilustración 131 Filtro para excluir los archivos suministrado por MAPFRE - 2.

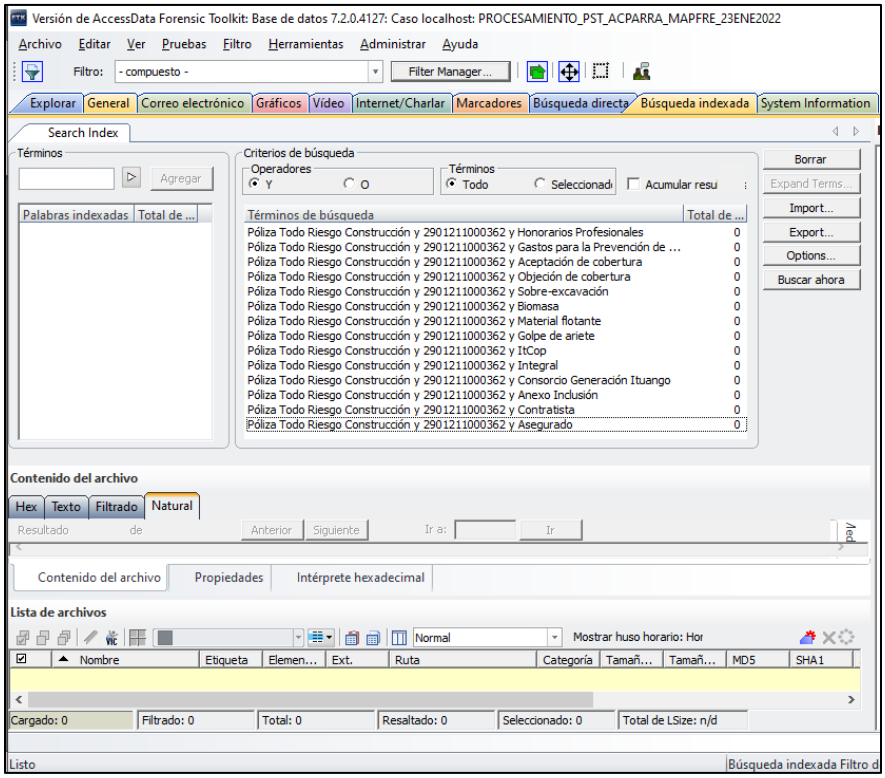
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Siete (7)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo acparra@mapfre.com.co asignado a **Andrés Camilo PARRA BALAGUERO** para el desarrollo de sus funciones.

13. Buzón de correo electrónico cruzj@mapfre.com.co.

El día 01 de diciembre de 2021, el equipo de ADALID CORP ingresa a la carpeta **CRUZJ**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

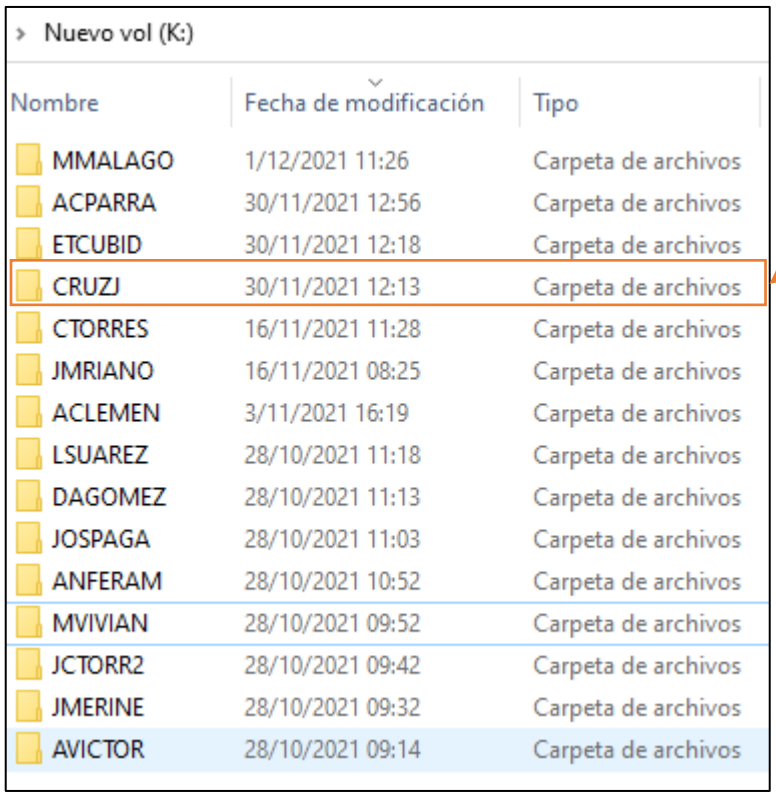


Ilustración 132 Visualización carpeta CRUZJ

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **CRUZJ** identificada dentro del disco duro como se observa en las siguientes imágenes:

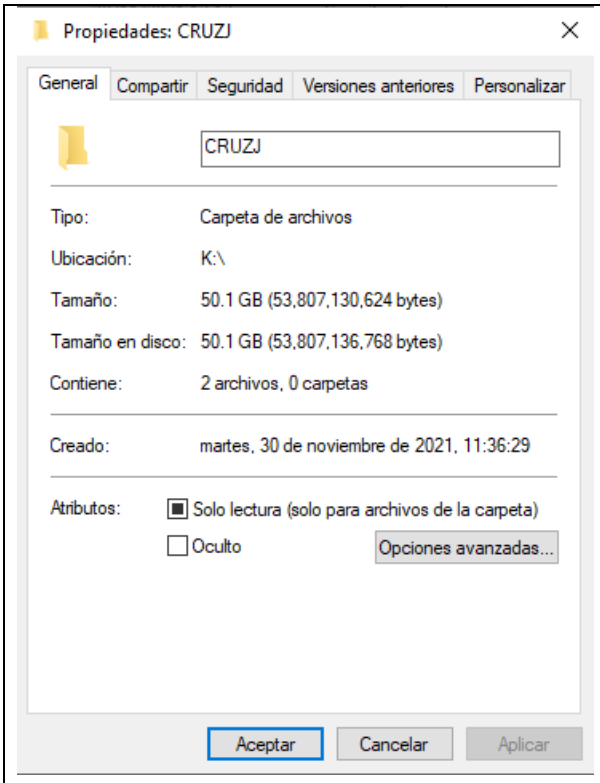


Ilustración 133 Propiedades de la carpeta CRUZJ visto desde el Disco Duro.

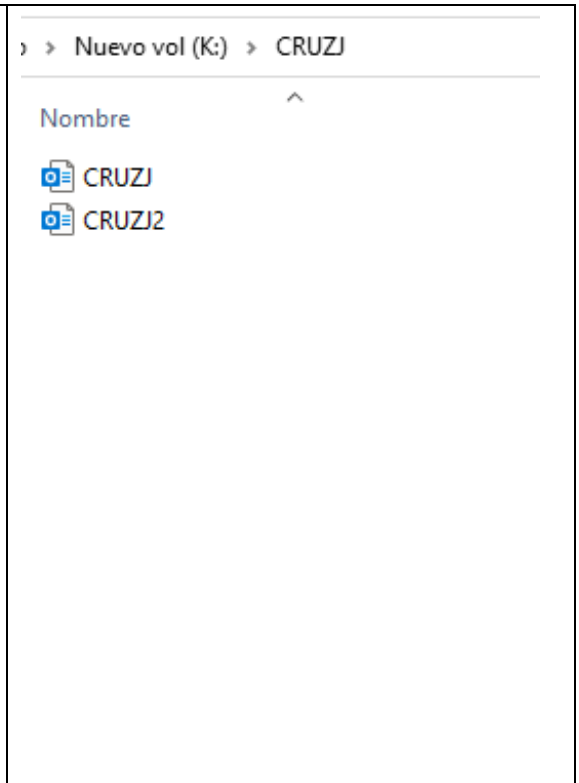


Ilustración 134 Contenido de la carpeta CRUZJ visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**cruzj@mapfre.com.co.**" asignado a **Jorge Cruz AGUADO** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las 15:18:42 y culminando el mismo de forma satisfactoria a las 16:29:17, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_01DIC2021
Número de prueba: 13_CRUZJ
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO CRUZJ@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A

ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad1:
[Computed Hashes]
MD5 checksum: ed3b9410edd6de02fe5e441ea43ddea2
SHA1 checksum: 91fad8664b30c42450ea5e3d4eadc83dd516faa4

Image information:
Acquisition started: Wed Dec 1 15:18:42 2021
Acquisition finished: Wed Dec 1 16:15:53 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad22

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad23

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad24

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad25

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad26

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad27

Image Verification Results:
Verification started: Wed Dec 1 16:15:53 2021
Verification finished: Wed Dec 1 16:29:17 2021
MD5 checksum: ed3b9410edd6de02fe5e441ea43ddea2 : verified
SHA1 checksum: 91fad8664b30c42450ea5e3d4eadc83dd516faa4 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**cruzj@mapfre.com.co.**" asignado a **Jorge Cruz AGUADO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 135 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO CRUZJ@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico cruzj@mapfre.com.co asignada **Jorge Cruz AGUADO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
13	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Jorge Cruz AGUADO → cruzj@mapfre.com.co	ad1	50.1 GB
TOTAL					**50.1 GB**

Tabla 28 Detalle del buzón de correo electrónico asignado cruzj@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico cruzj@mapfre.com.co asignado a Jorge Cruz AGUADO para el desarrollo de sus funciones **aloja** un total de **50.1 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Noventa y un**

mil seiscientos ochenta y siete (91.687) archivos (incluyendo carpetas), como se observa a continuación.

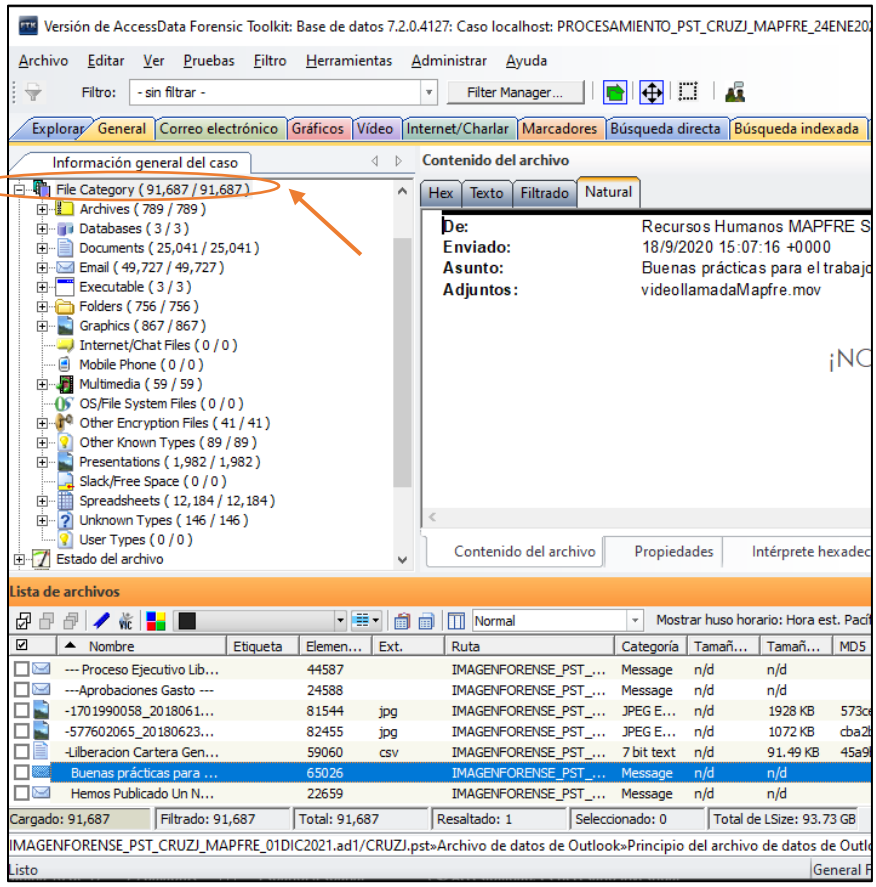


Ilustración 136 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico cruzj@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JORGE CRUZ AGUADO → CRUZJ@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico cruzj@mapfre.com.co asignado a Jorge Cruz AGUADO, iniciando el día el **24** de enero de 2022 con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **Cuarenta (40)** ítems en condición de "eliminados" y se reconstruyeron **Cero (0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como

"Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

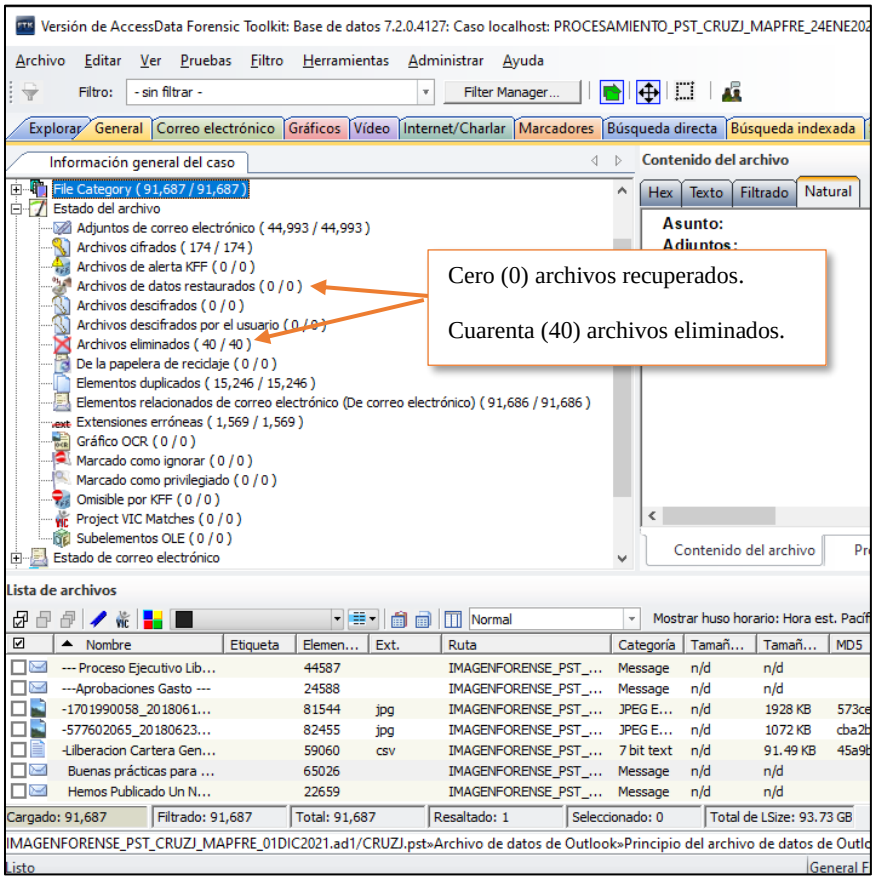


ilustración 137 Total de archivos recuperados en la cuenta de correo electrónico cruzj@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Noventa y un mil seiscientos ochenta y siete (91.687)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO CRUZJ@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico

cruzj@mapfre.com.co asignado a **Jorge Cruz AGUADO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	789
2	Bases de Datos	3
3	Documentos	25.041
4	Correo Electrónico	49.727
5	Ejecutable	3
6	Carpetas	756
7	Gráficos	867
8	Multimedia	59
9	Otros archivos encriptados	41
10	Otros archivos desconocidos	89
11	Presentaciones	1982
12	Hojas de cálculo	12.184
13	Tipos de archivos desconocidos	146
TOTAL		**91.687**

Tabla 29 Información buscada evidencia 013_CRUZJ, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Noventa y un mil seiscientos ochenta y siete (91.687).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Cuarenta y cuatro mil novecientos noventa y tres (44.993) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Ciento setenta y cuatro (174) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Los archivos de datos restaurados **Cero (0)** archivos de datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos eliminados **Cuarenta (40)** archivos de datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Quince mil doscientos cuarenta y seis (15.246)** archivos de datos recuperados por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Noventa y un mil seiscientos ochenta y seis (91.686)** archivos de datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Mil quinientos sesenta y nueve (1.569) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico mvivian@mapfre.com asignado a cruzj@mapfre.com.co asignado a **Jorge CRUZ** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

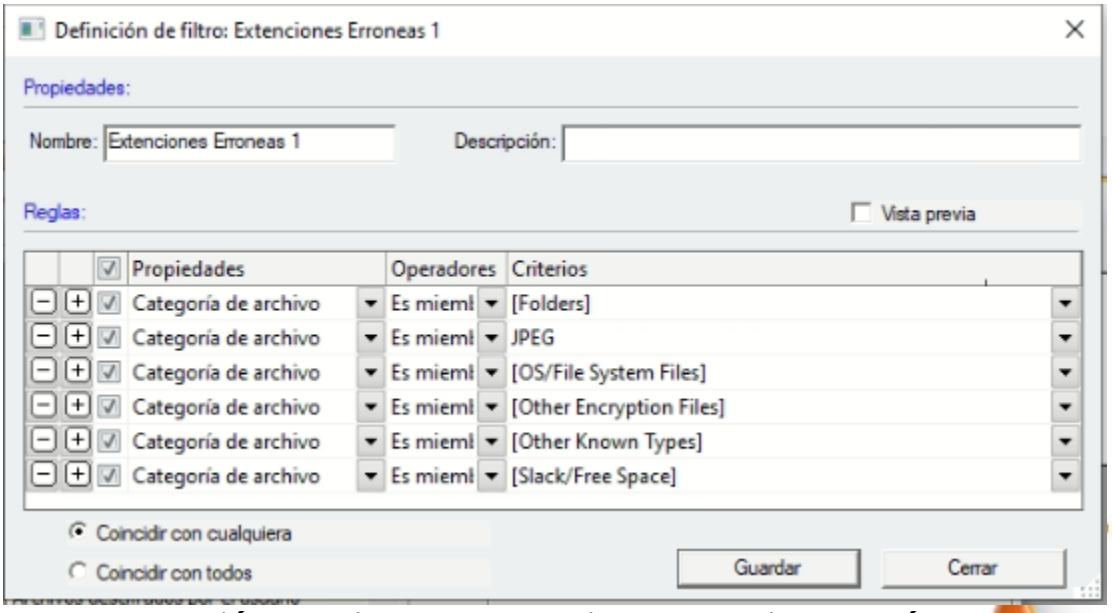


Ilustración 138 Filtro para excluir las extensiones erróneas.

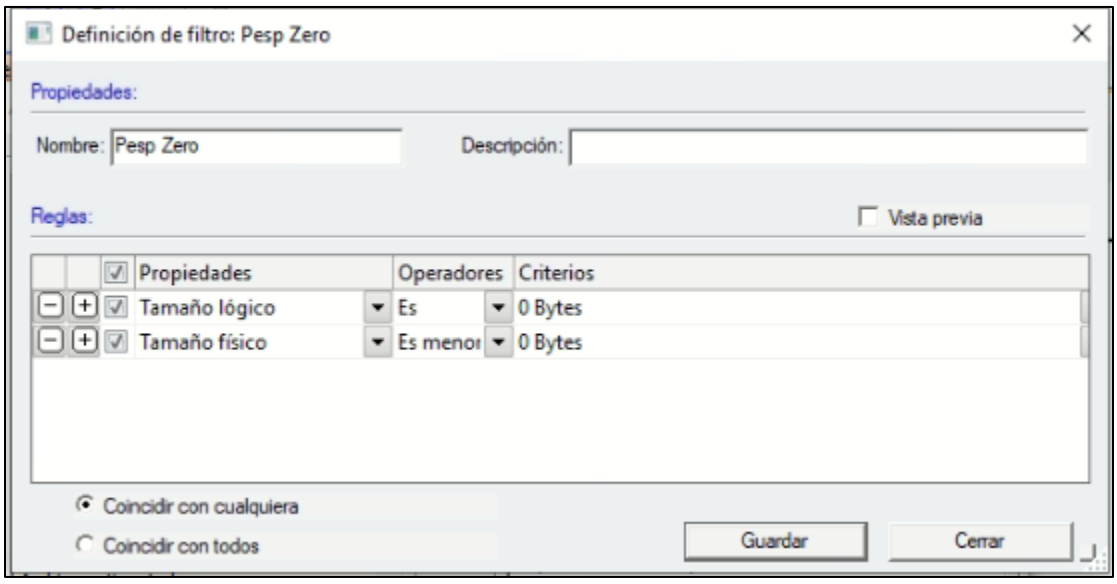


Ilustración 139 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

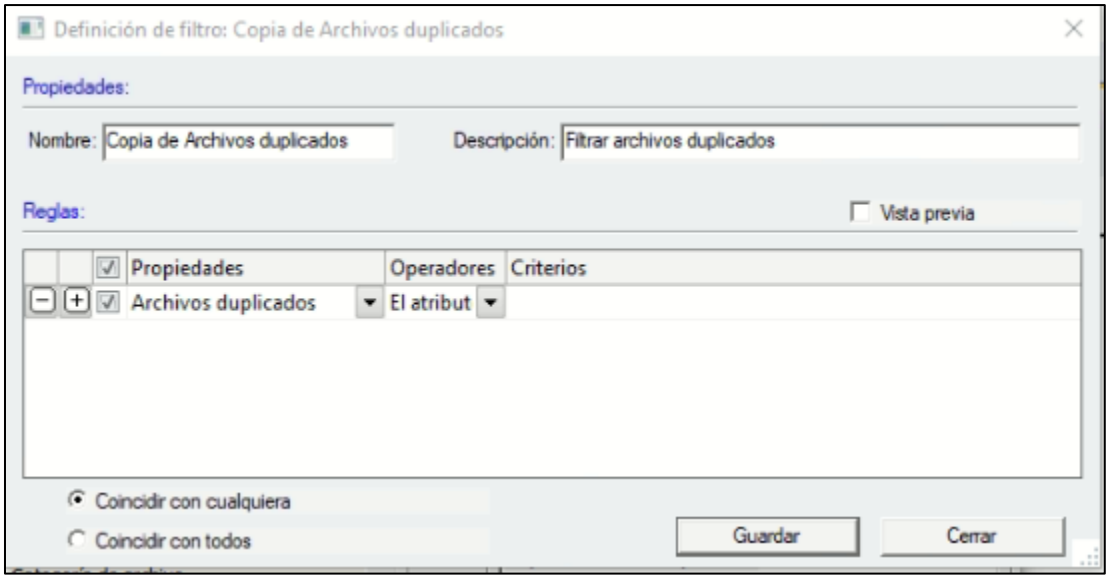


Ilustración 140 Filtro para excluir los archivos duplicados.

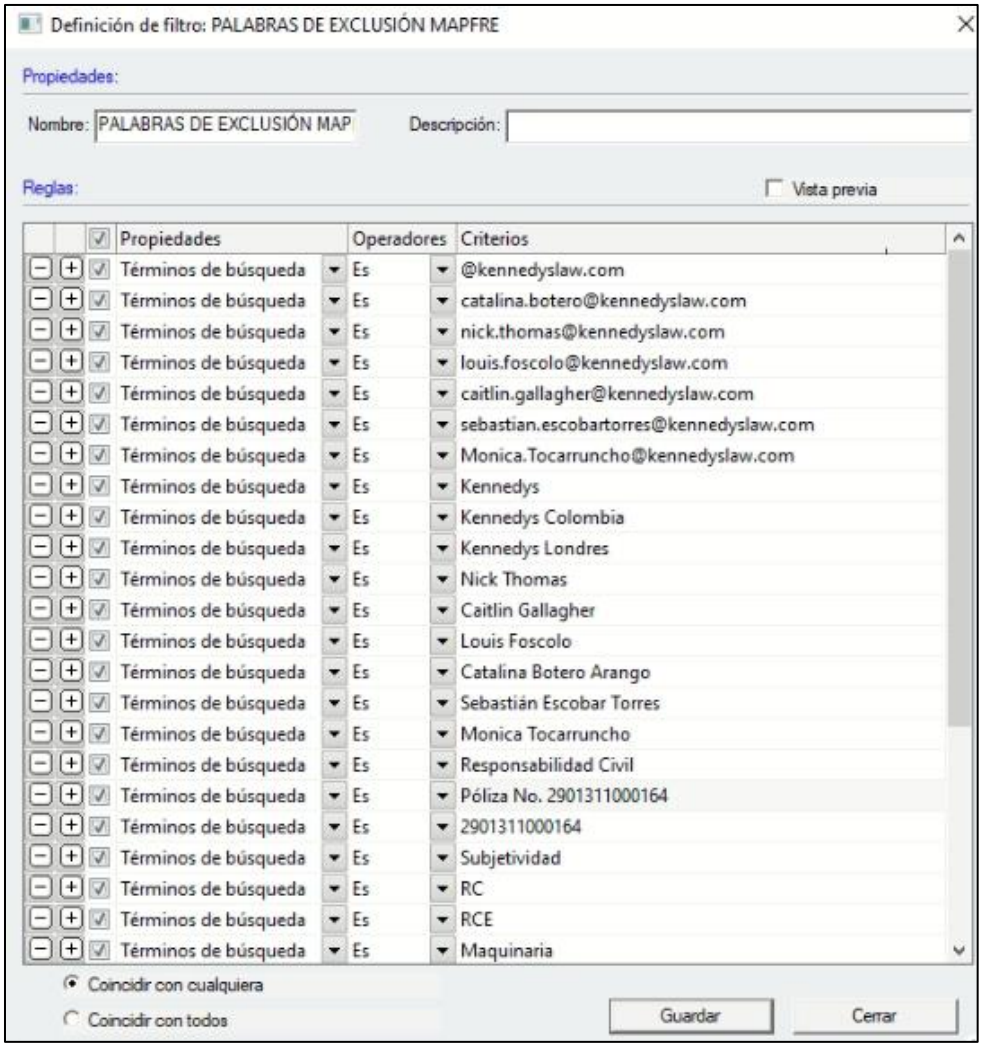


Ilustración 141 Filtro para excluir los archivos suministrado por MAPFRE - 1.

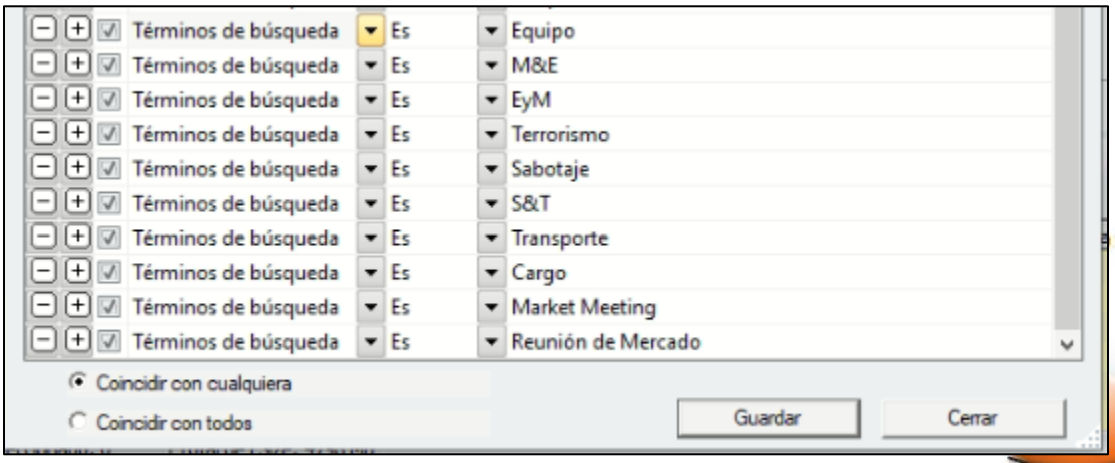
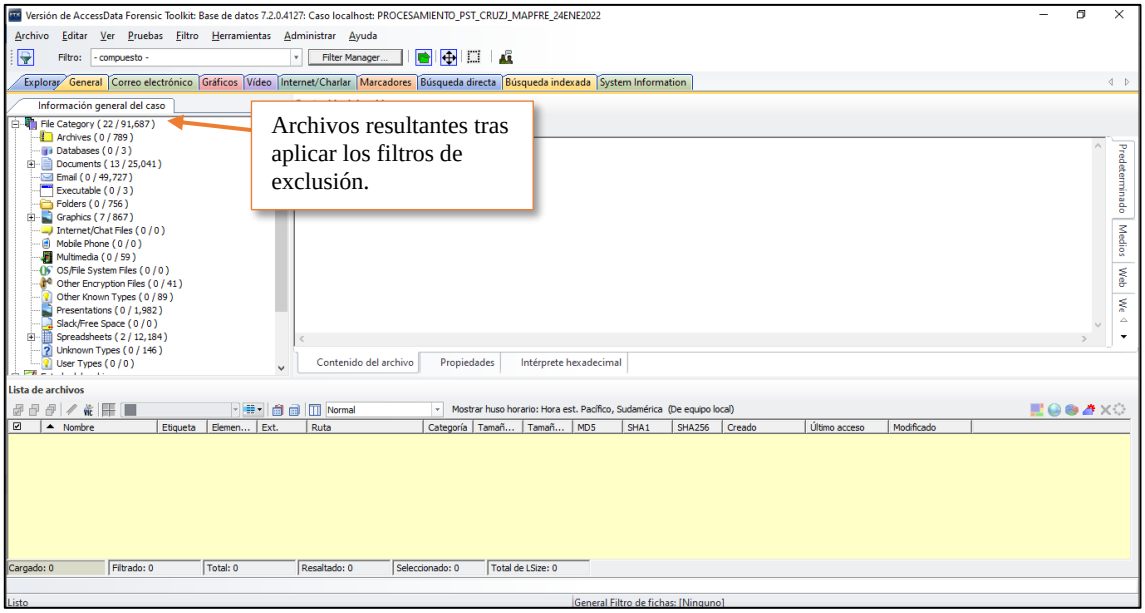


Ilustración 142 Filtro para excluir los archivos suministrado por MAPFRE - 2.

Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **veintidós (22)** registros como se observa en la siguiente imagen:

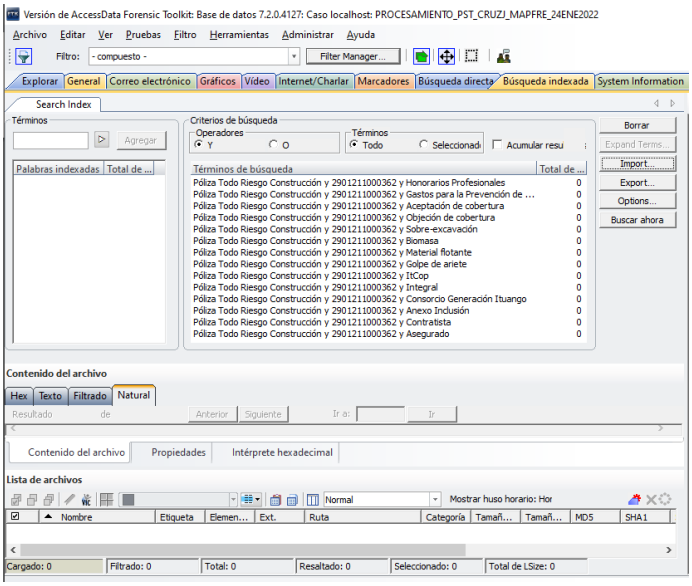


Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo cruzj@mapfre.com.co asignado a **Jorge CRUZ** para el desarrollo de sus funciones.

14. Buzón de correo electrónico etcubid@mapfre.com.co.

El día 01 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta **ETCUBID**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

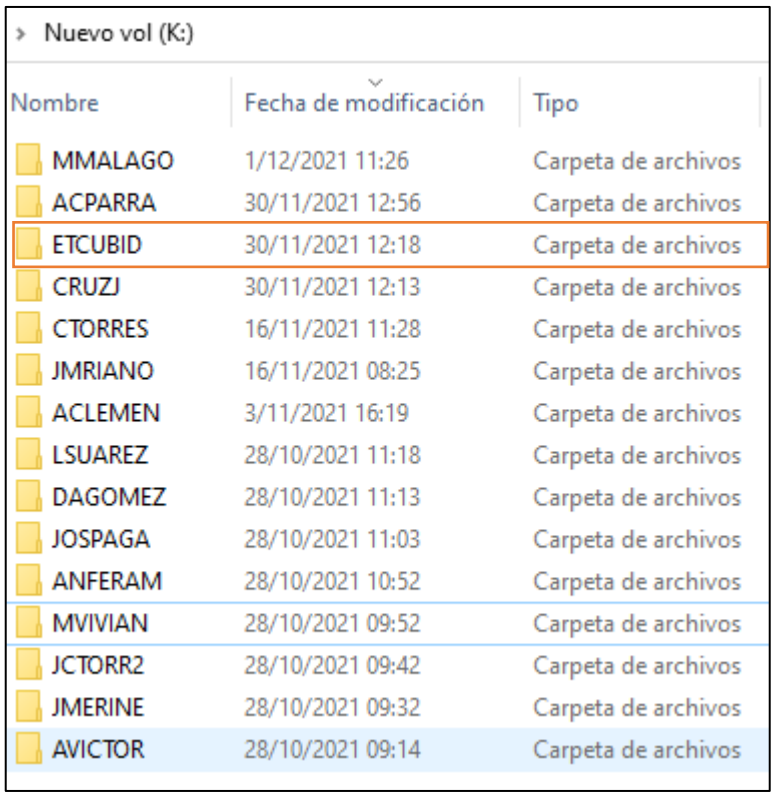


Ilustración 143 Visualización carpeta ETCUBID.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **ETCUBID** identificada dentro del disco duro como se observa en las siguientes imágenes:

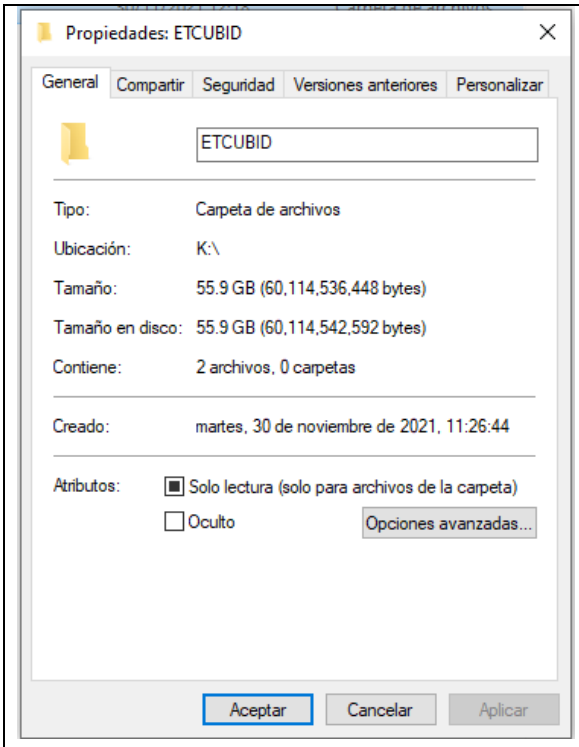


Ilustración 144 Propiedades de la carpeta ETCUBID visto desde el Disco Duro.

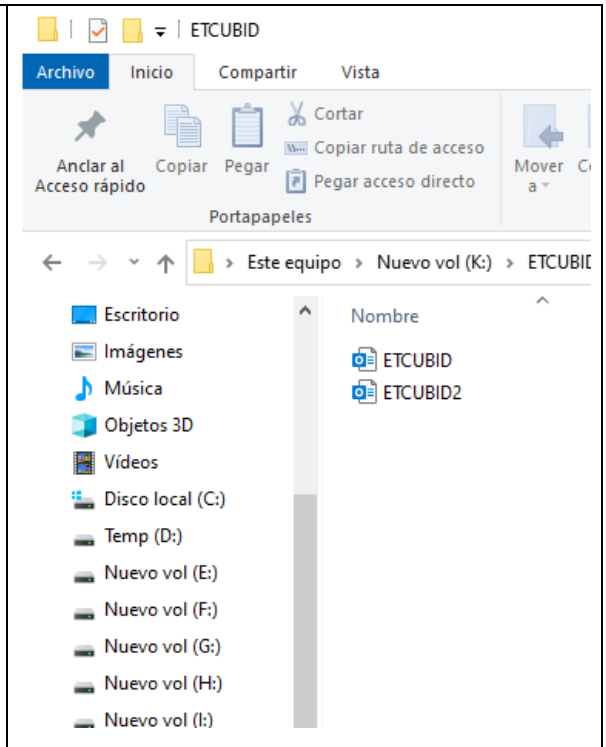


Ilustración 145 Contenido de la carpeta ETCUBID visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**etcubid@mapfre.com.co.**" asignado a **Ethel CUBIDES** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **16:32:53** y culminando el mismo de forma satisfactoria a las **17:53:04**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_01DIC2021
Número de prueba: 14_ETCUBID
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ETCUBID@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8

DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad1:
[Computed Hashes]
MD5 checksum: a6426ce7f6ca0217569271fe149bf3d7
SHA1 checksum: 3753a9577aa74a1f04b65a301238b025bf4fd805

Image information:
Acquisition started: Wed Dec 1 16:32:53 2021
Acquisition finished: Wed Dec 1 17:38:33 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad22

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad23

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad24

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad25

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad26

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad27

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad28

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad29

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad30

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad31

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad32

Image Verification Results:
Verification started: Wed Dec 1 17:38:33 2021
Verification finished: Wed Dec 1 17:53:04 2021
MD5 checksum: a6426ce7f6ca0217569271fe149bf3d7 : verified
SHA1 checksum: 3753a9577aa74a1f04b65a301238b025bf4fd805 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con

capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**etcubid@mapfre.com.co.**" asignado a **Ethel CUBIDES** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 146 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ETCUBID@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico etcubid@mapfre.com.co asignada Ethel CUBIDES para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
14	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Ethel CUBIDES → etcubid@mapfre.com.co	ad1	55.9 GB
TOTAL					**55.9GB**

Tabla 30 Detalle del buzón de correo electrónico asignado etcubid@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico etcubid@mapfre.com.co asignado a Ethel CUBIDES para el desarrollo de sus funciones **aloja** un total de **55.9 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento veintitrés**

mil trescientos veinticuatro (123.324) archivos (incluyendo carpetas), como se observa a continuación.

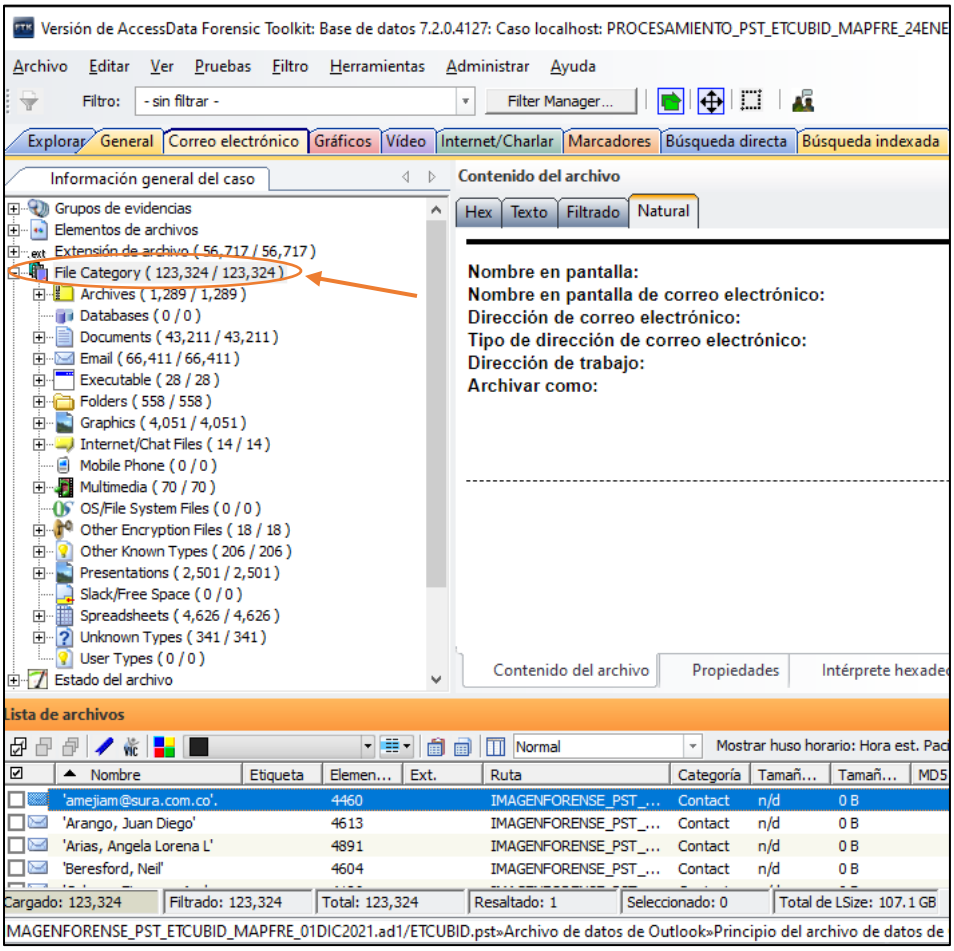


Ilustración 147 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico etcubid@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO ETHEL CUBIDES → ETCUBID@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico etcubid@mapfre.com.co asignado a Ethel CUBIDES, iniciando el día el **24** de enero del 2022, con una duración aproximada de Siete (7) día calendario, el resultado a dicho proceso arrojó que existen **Mil setenta y ocho (1.078**) ítems en condición de "eliminados" y se reconstruyeron **Cero (0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato

que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

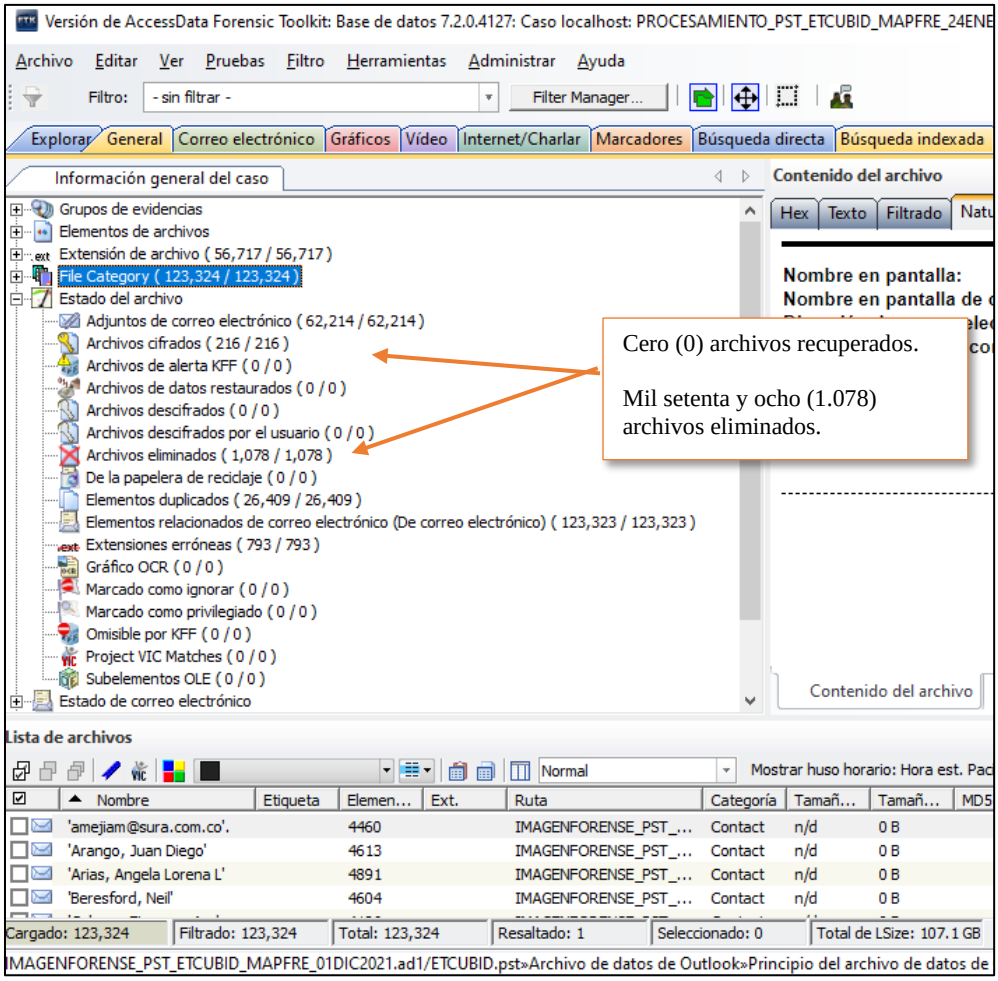


ilustración 148 Total de archivos recuperados en la cuenta de correo electrónico etcubid@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento veintitrés mil trescientos veinticuatro (123.324)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ETCUBID@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico etcubid@mapfre.com.co asignado a **Ethel CUBIDES** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1289
2	Documentos	43.211
3	Correo Electrónico	66.411
4	Ejecutable	28
5	Carpetas	558
6	Archivos de internet / chats	14
7	Gráficos	4.051
8	Multimedia	70
9	Otros archivos encriptados	18
10	Otros archivos desconocidos	206
11	Presentaciones	2501
12	Hojas de cálculo	4.626
13	Tipos de archivos desconocidos	341
TOTAL		**123.324**

Tabla 31 Información buscada evidencia 014_ETCUBID, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento veintitrés mil trescientos veinticuatro (123.324).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Sesenta y dos mil doscientos catorce (62.214) archivos de datos obtenidos** por el

proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Los archivos cifrados recuperados **Doscientos dieciséis (216) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos eliminados **Mil setenta y ocho (1.078) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Veintiséis mil cuatrocientos nueve (26.409) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento veintitrés mil trescientos veintitrés (123.323) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Setecientos noventa (793) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico etcubid@mapfre.com.co asignado a **Ethel CUBIDES para** el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

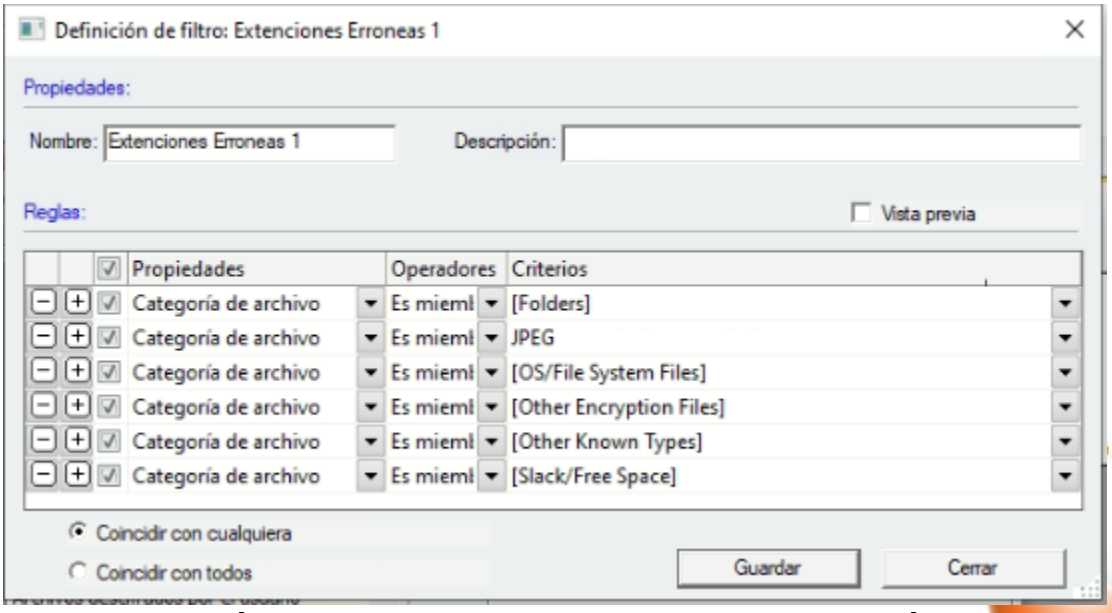


Ilustración 149 Filtro para excluir las extensiones erróneas.

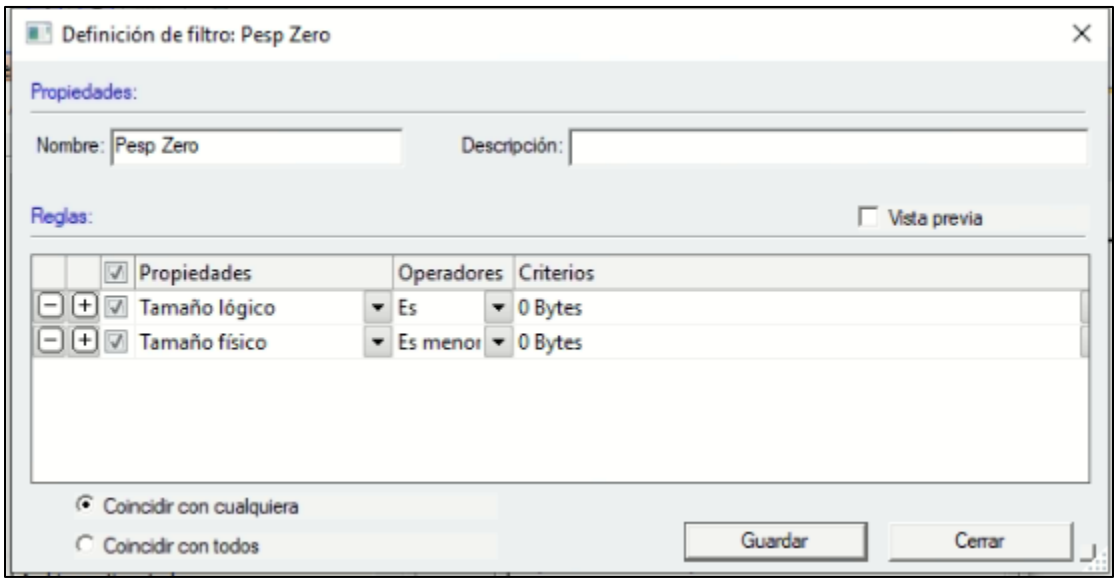


Ilustración 150 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

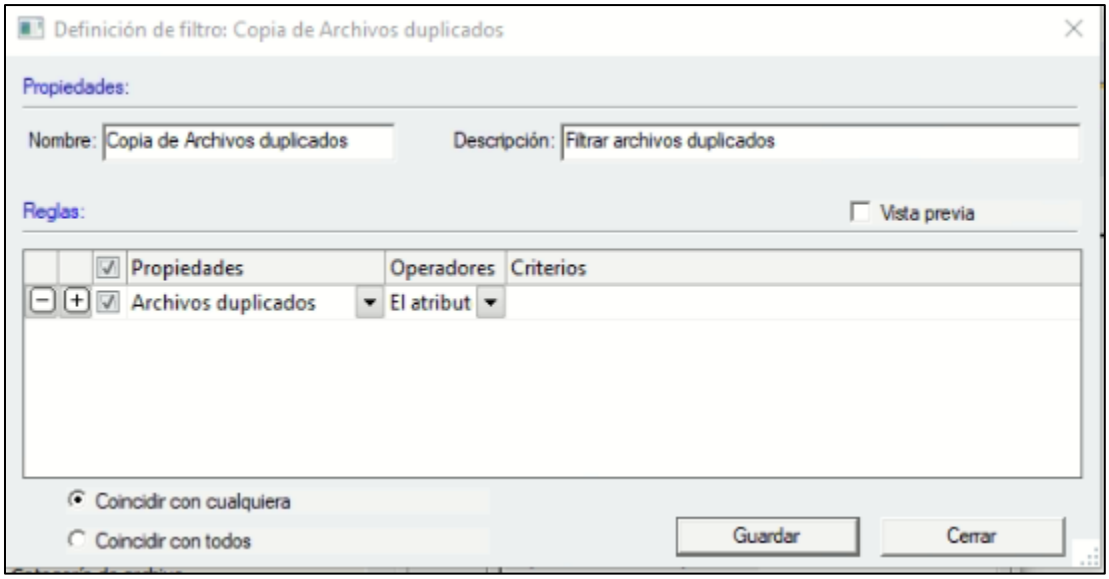


Ilustración 151 Filtro para excluir los archivos duplicados.

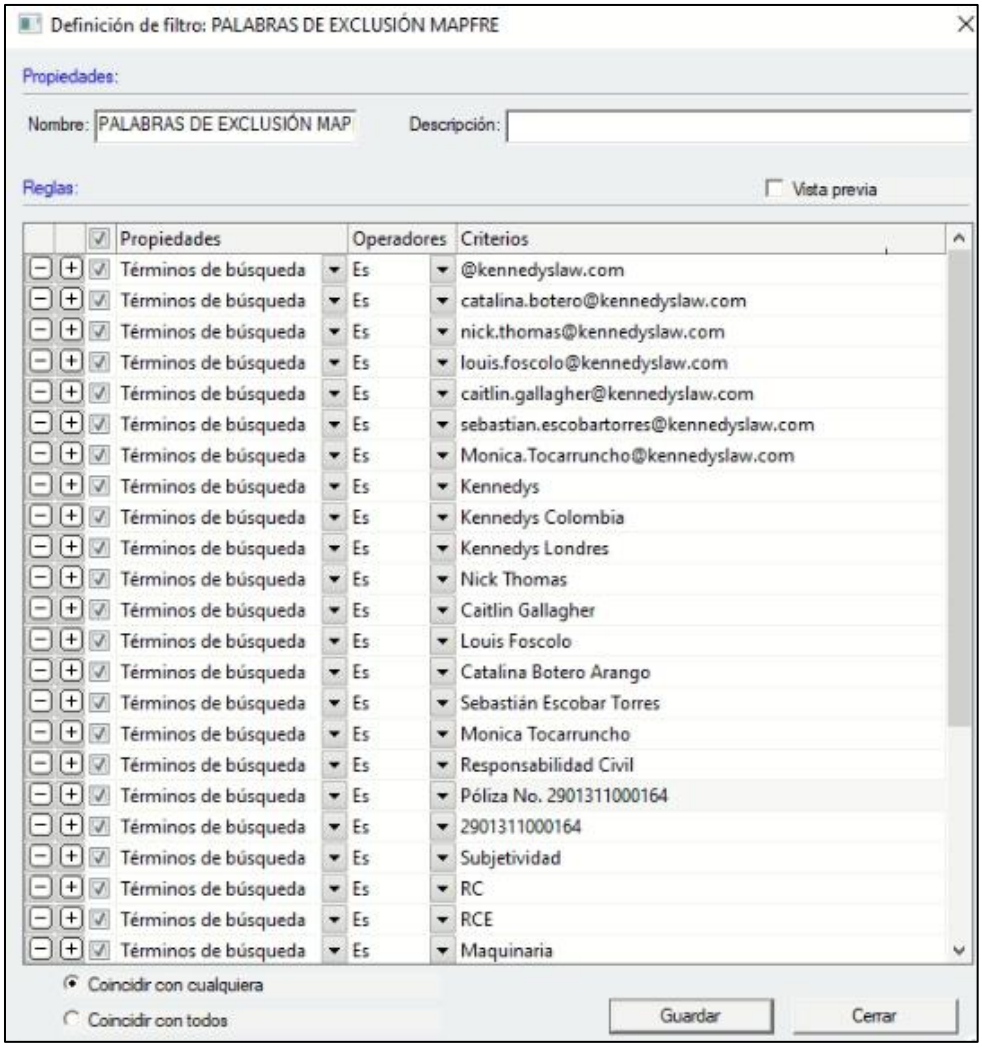


Ilustración 152 Filtro para excluir los archivos suministrado por MAPFRE - 1.

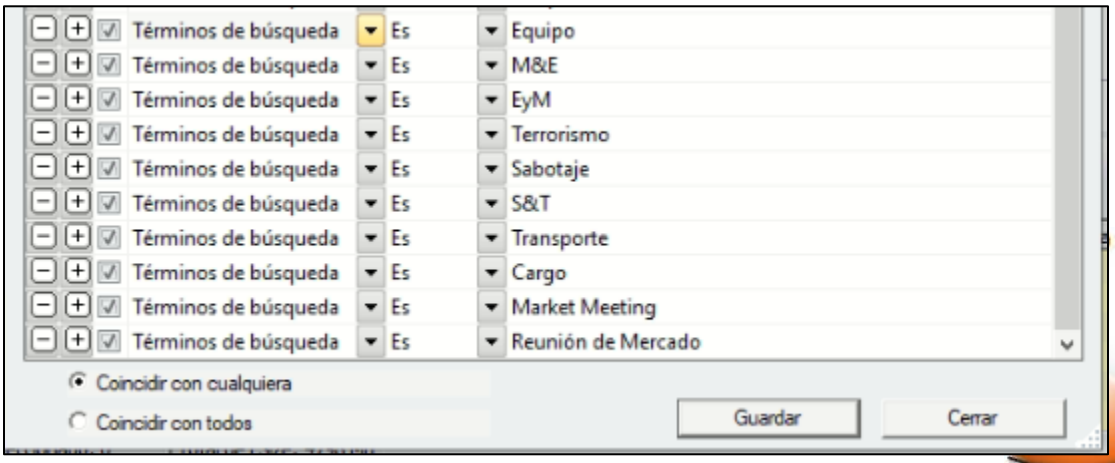
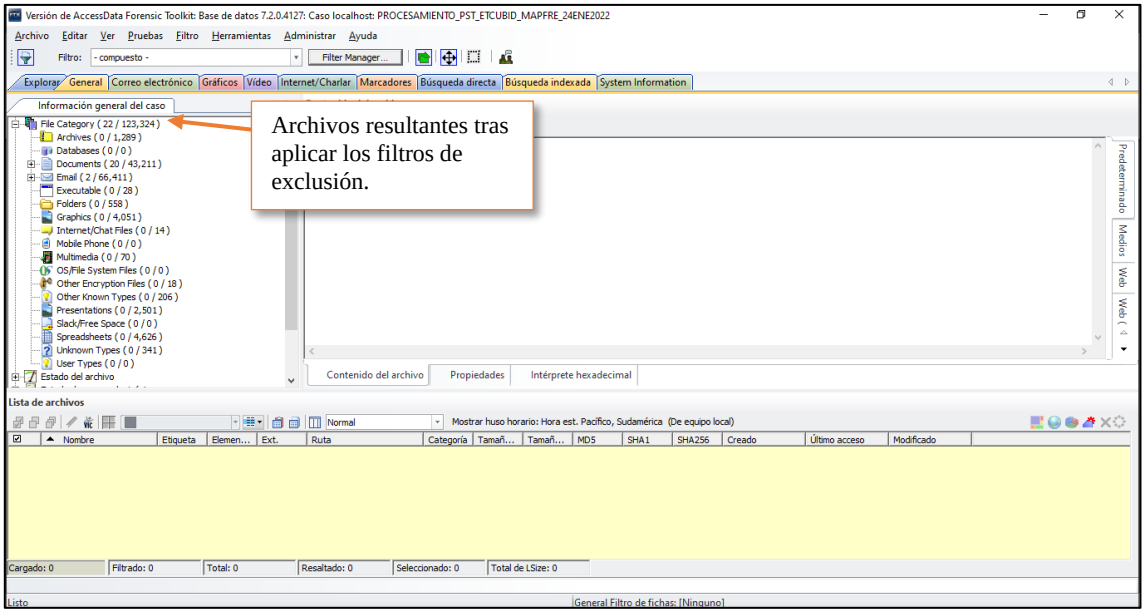


Ilustración 153 Filtro para excluir los archivos suministrado por MAPFRE - 2.

Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **veintidós (22)** registros como se observa en la siguiente imagen:

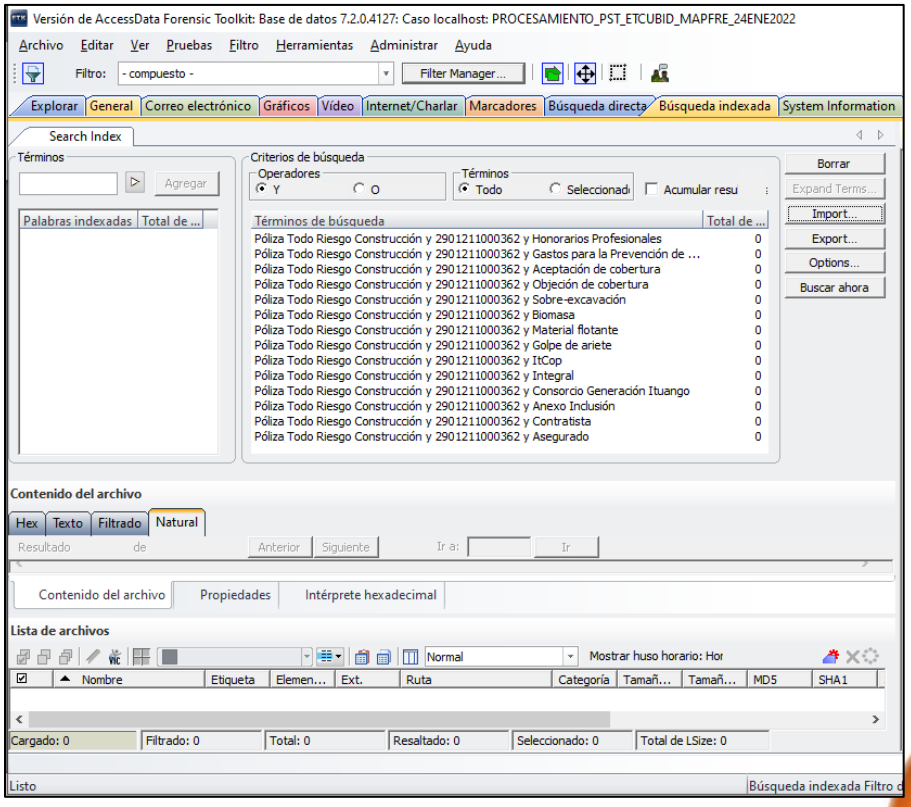


Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo etcubid@mapfre.com.co asignado a **Ethel CUBIDES** para el desarrollo de sus funciones.

15. Buzón de correo electrónico mmalago@mapfre.com.co.

El día 02 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta **MMALAGO**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

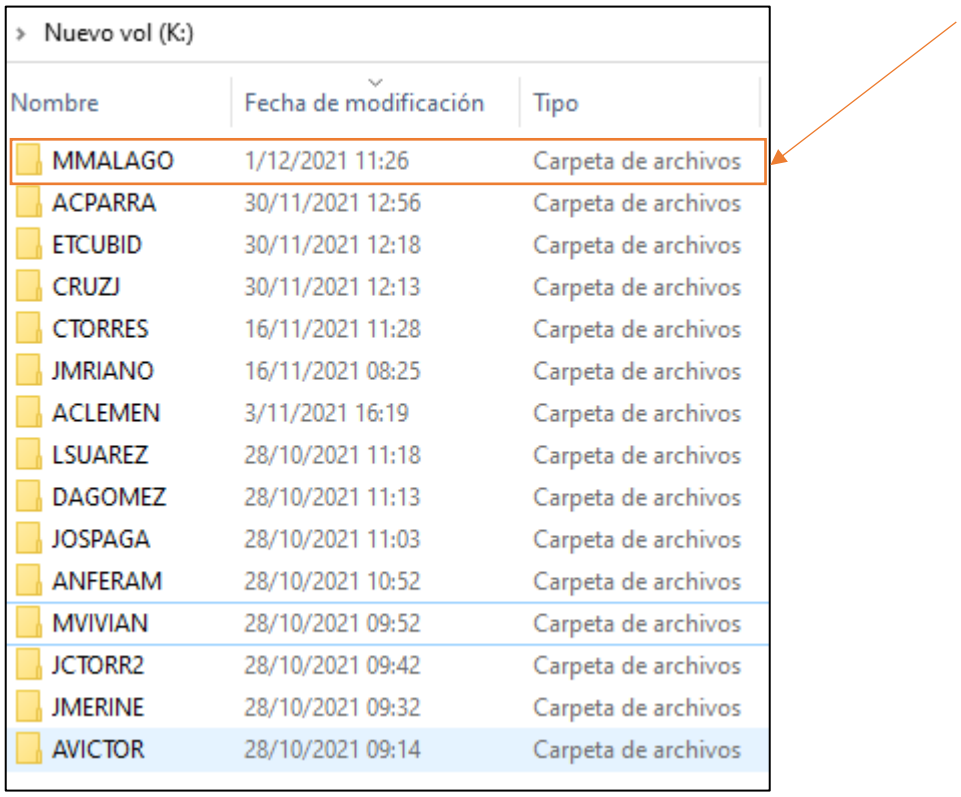


Ilustración 154 Visualización carpeta MMALAGO.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **MMALAGO** identificada dentro del disco duro como se observa en las siguientes imágenes:

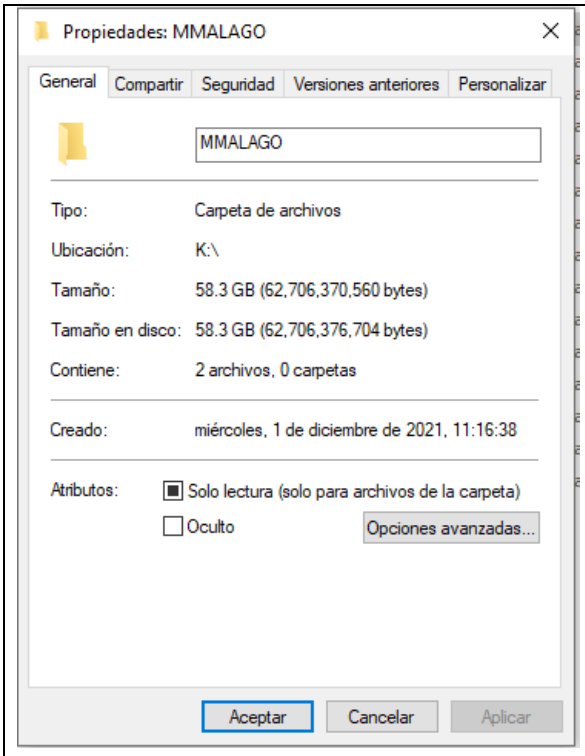


Ilustración 155 Propiedades de la carpeta MMALAGO visto desde el Disco Duro.

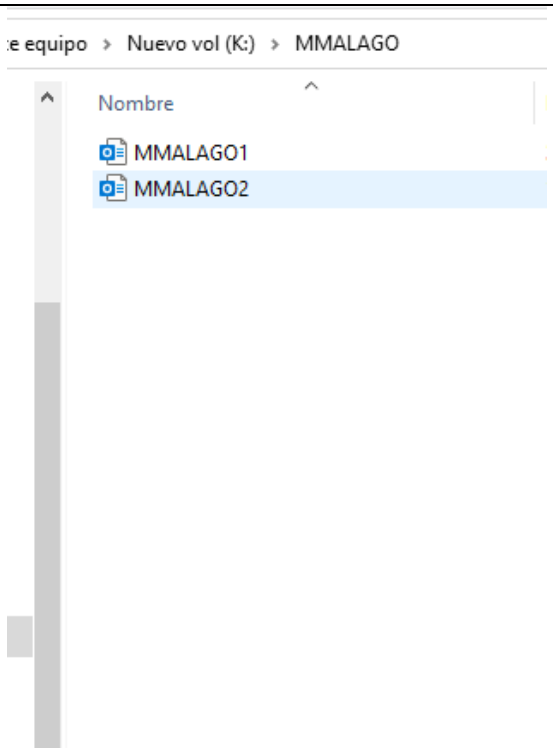


Ilustración 156 Contenido de la carpeta MMALAGO visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**mmalago@mapfre.com.co.**" asignado a **José Mauricio MALAGÓN ACOSTA** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **07:46:38** y culminando el mismo de forma satisfactoria a las **09:01:58**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_02DIC2021
Número de prueba: 15_MMALAGO
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO MMALAGO@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE

FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad1:
[Computed Hashes]
MD5 checksum: 73f2e7b307c8cbe24e68fd2cd5bec944
SHA1 checksum: 515cd0f6c475cc973c9af008a7ea79b87126ef69

Image information:
Acquisition started: Thu Dec 2 07:46:38 2021
Acquisition finished: Thu Dec 2 08:47:29 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad22

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad23

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad24

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad25

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad26

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad27

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad28

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad29

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad30

Image Verification Results:
Verification started: Thu Dec 2 08:47:29 2021
Verification finished: Thu Dec 2 09:01:58 2021
MD5 checksum: 73f2e7b307c8cbe24e68fd2cd5bec944 : verified
SHA1 checksum: 515cd0f6c475cc973c9af008a7ea79b87126ef69 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**mmalago@mapfre.com.co.**" asignado a **José Mauricio MALAGÓN ACOSTA** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 157 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO MMALAGO@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico mmalago@mapfre.com.co asignada **José Mauricio MALAGÓN ACOSTA** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
15	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	José Mauricio MALAGÓN ACOSTA → mmalago@mapfre.com.co	ad1	58.3 GB
TOTAL					**58.3 GB**

Tabla 32 Detalle del buzón de correo electrónico asignado mmalago@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico mmalago@mapfre.com.co asignado a **José Mauricio MALAGÓN ACOSTA** para el desarrollo de sus funciones **aloja** un total de **58.3 GB**, dentro de este espacio el laboratorio de informática forense logró hallar

un total de **Ciento cuarenta y siete mil doscientos dieciocho (147.218)** archivos (incluyendo carpetas), como se observa a continuación.

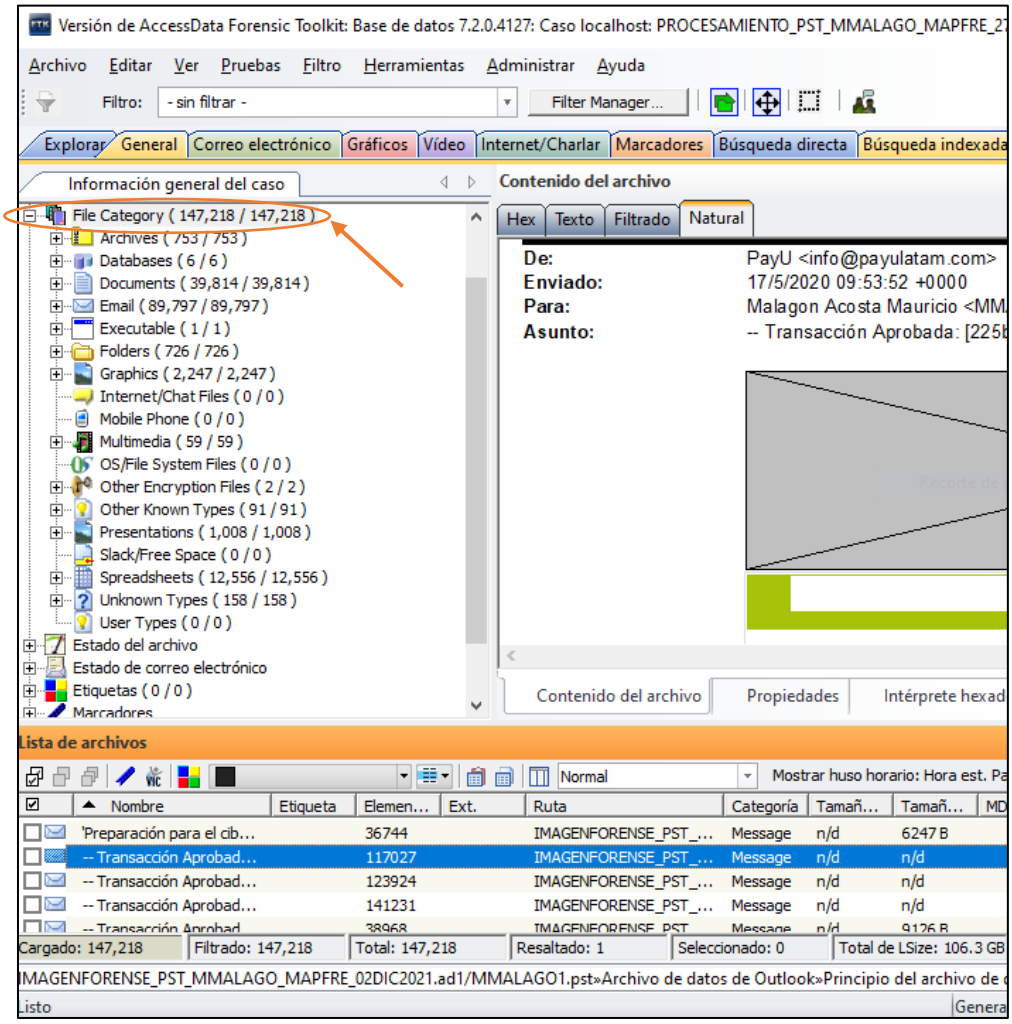


Ilustración 158 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico mmalago@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JOSÉ MAURICIO MALAGÓN ACOSTA → MMALAGO@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico mmalago@mapfre.com.co asignado a **José Mauricio MALAGÓN ACOSTA**, iniciando el día el **27** de enero del 2022, con una duración aproximada de Ocho (8) día calendario, el resultado a dicho proceso arrojó que existen **Doscientas ochenta y siete (287)** ítems en condición de "eliminados" y se reconstruyeron **cero (0)**

archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

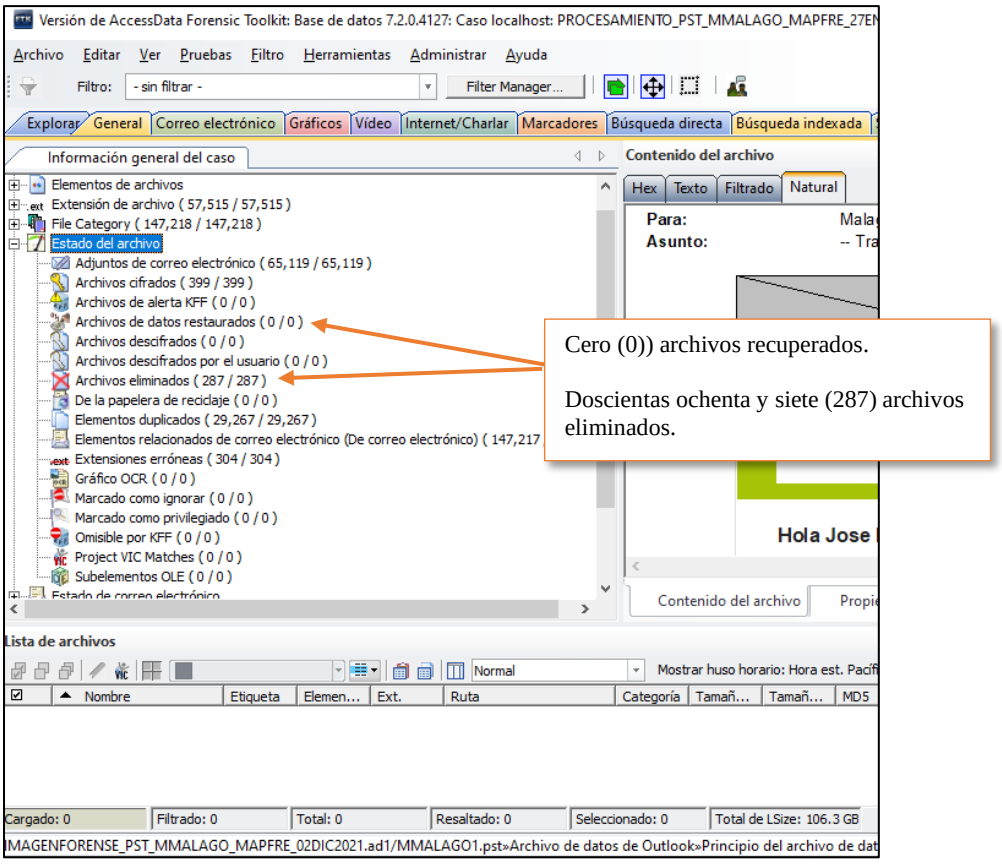


ilustración 159 Total de archivos recuperados en la cuenta de correo electrónico mmalago@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento cuarenta y siete mil doscientos dieciocho (147.218)** (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO MMALAGO@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico mmalago@mapfre.com.co asignado a **José Mauricio MALAGÓN ACOSTA** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	753
2	Bases de Datos	6
3	Documentos	39.814
4	Correo Electrónico	89.797
5	Ejecutables	1
6	Carpetas	726
7	Gráficos	2.247
8	Multimedia	59
9	Otros archivos encriptados	2
10	Otros archivos desconocidos	91
11	Presentaciones	1008
12	Hojas de cálculo	12.556
13	Tipos de archivos desconocidos	158
TOTAL		**147.218**

Tabla 33 Información buscada evidencia 015_MMALAGO, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento cuarenta y siete mil doscientos dieciocho (147.218).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Sesenta y cinco mil ciento diecinueve (65.119) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Trescientas noventa y nueve (399) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos eliminados **Veintisiete mil ochocientos once (287) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Ochenta y ocho mil ciento dieciséis (88.116) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento noventa y seis mil ciento ochenta y seis (196.186) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **novecientos cincuenta y siete (957) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Treinta y un mil catorce (31.014) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Veintisiete mil ciento veintiocho (27.128) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico mmalago@mapfre.com.co asignado a **José Mauricio MALAGÓN ACOSTA** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



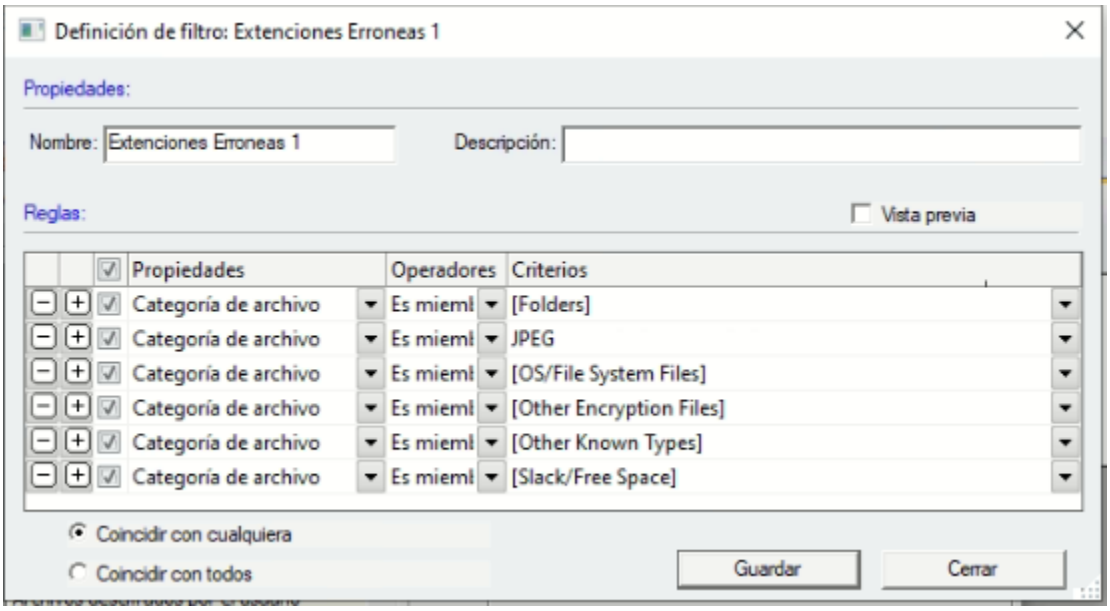


Ilustración 160 Filtro para excluir las extensiones erróneas.

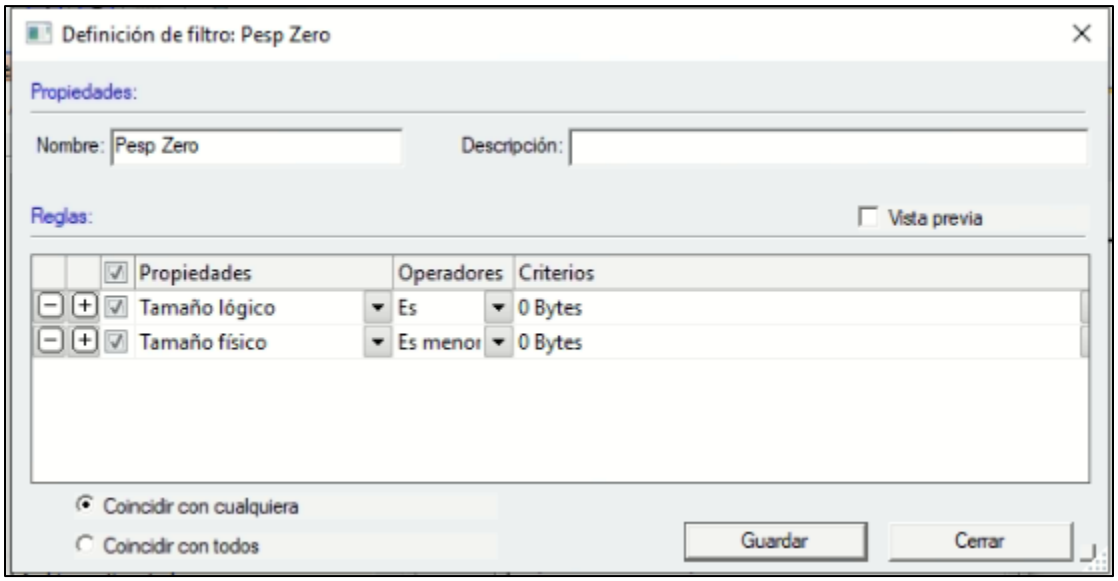


Ilustración 161 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

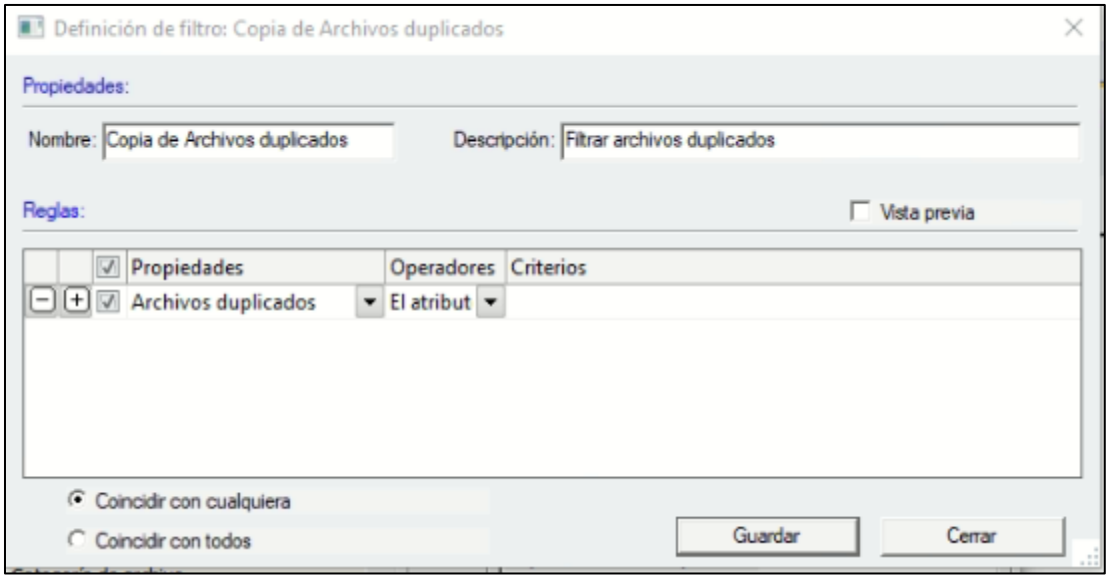


Ilustración 162 Filtro para excluir los archivos duplicados.

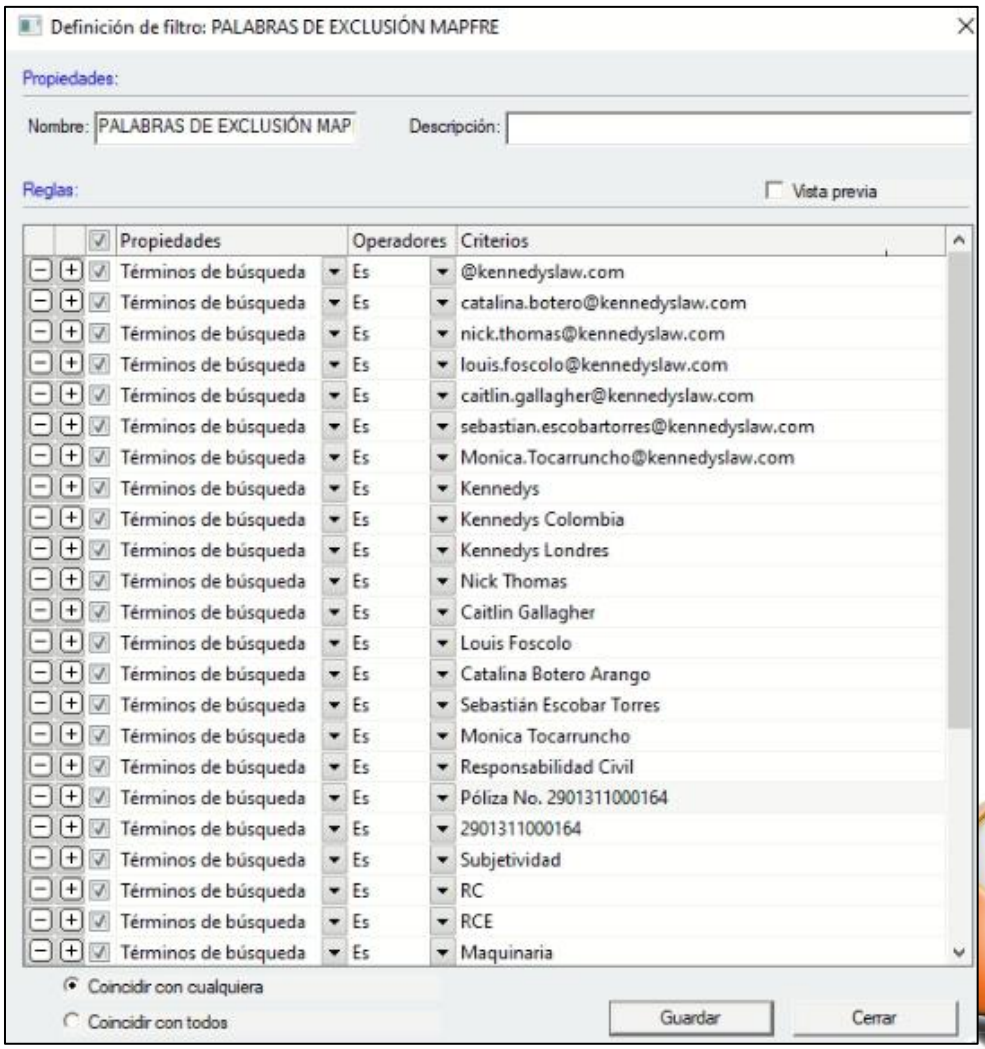


Ilustración 163 Filtro para excluir los archivos suministrado por MAPFRE - 1.

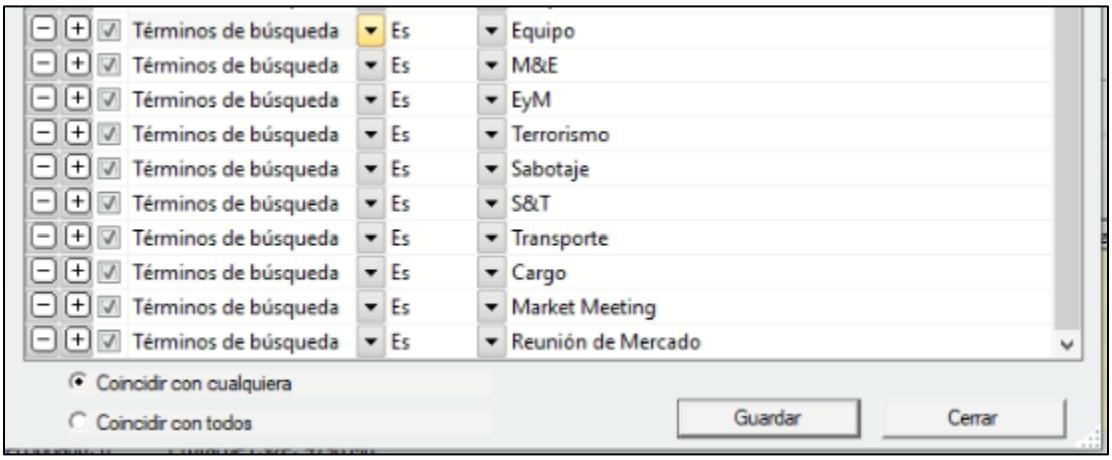
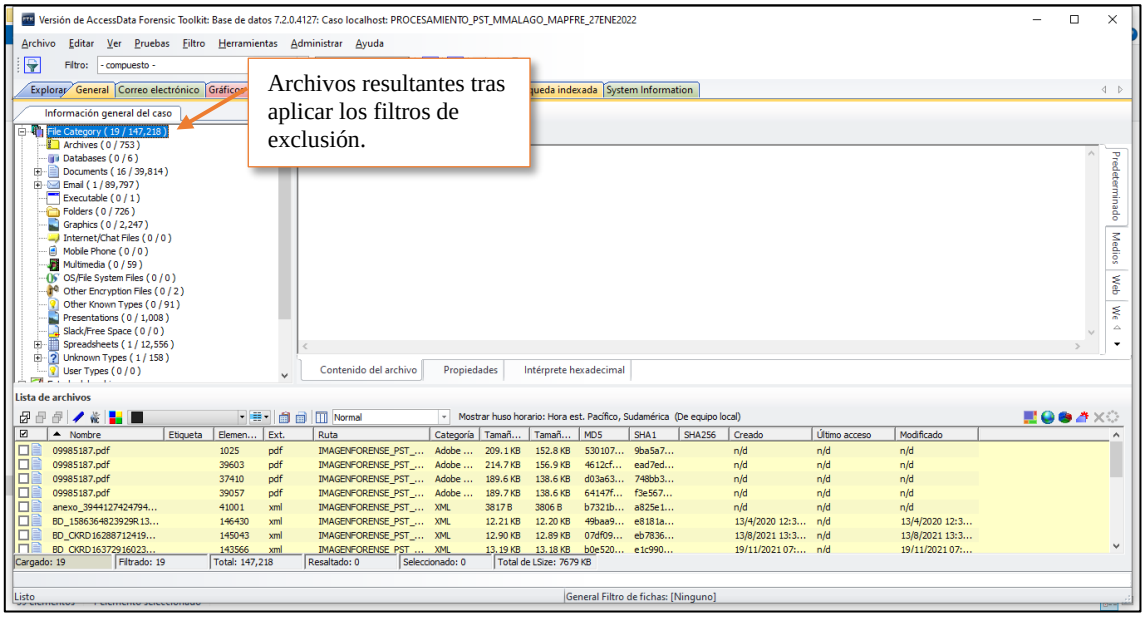


Ilustración 164 Filtro para excluir los archivos suministrado por MAPFRE - 2.

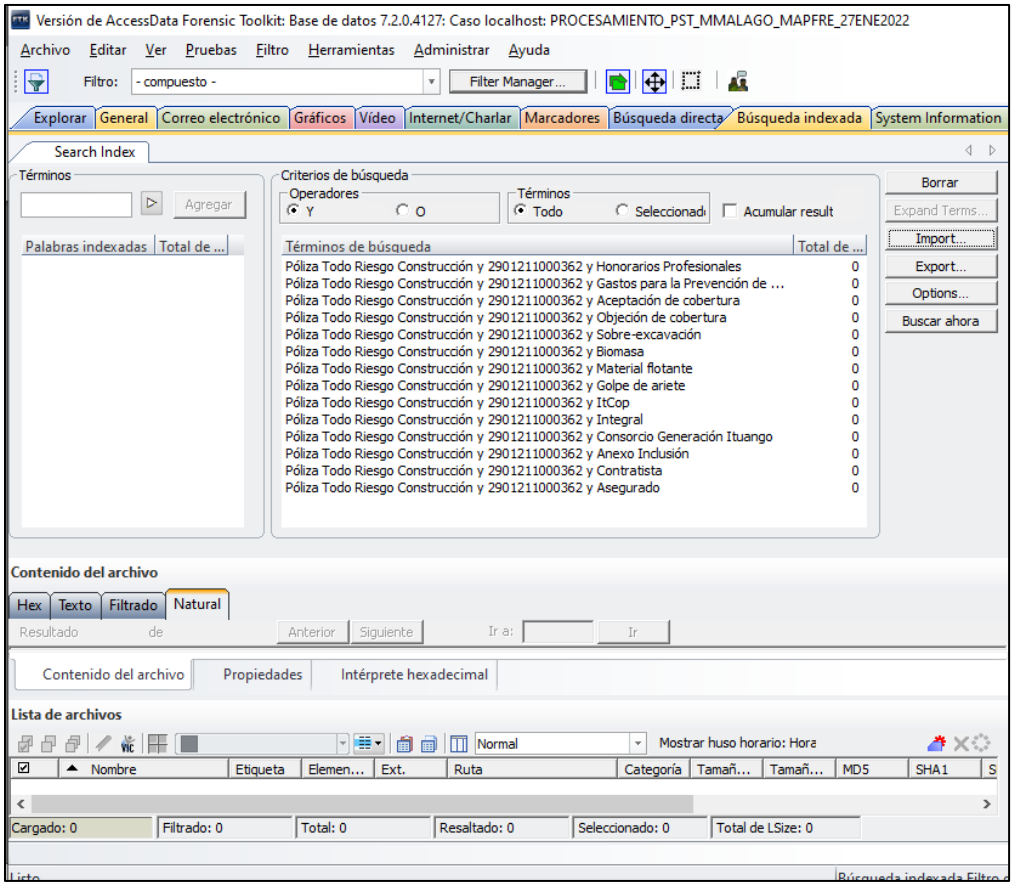
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Diecinueve (19)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo mmalago@mapfre.com.co asignado a **José Mauricio MALAGÓN ACOSTA** para el desarrollo de sus funciones.

Una vez realizadas las imágenes forenses para los buzones de correo electrónico pertenecientes a (4) funcionarios de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** los cuales se encuentran identificados con las siguientes direcciones de correo (mmalago@mapfre.com.co, acparra@mapfre.com.co, etcubid@mapfre.com.co, cruzj@mapfre.com.co), el equipo de ADALID CORP hace entrega de (1) Un disco duro color blanco, con capacidad de almacenamiento de **1000GB** al señor **Willigton Leandro TORRES MORALES,** identificado con cédula de ciudadanía **No. 79.708.420** de Bogotá, quien funge como **PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN** el día 07 de diciembre a las 15:03 horas.

De igual manera, el día 07 diciembre de 2021, el señor **Willigton Leandro TORRES MORALES** nuevamente hace entrega a los peritos de ADALID CORP. de (1) Un disco duro color **blanco**, con capacidad de almacenamiento de

1000GB, el cual en su parte superior se encuentra marcado como **"prueba extraprocesal"** como se presenta a continuación**:**

	
Fotografía Disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista superior)	Fotografía disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista posterior)

Al interior del Disco Duro se encuentran los archivos en formato .PST de las cuentas de correo electrónico asignadas a Once (11) funcionarios que se encuentran retirados y Seis (6) cuentas de correo electrónico de funcionarios activos dentro de la empresa **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**, de los cuales Dos (2) buzones de correo adicionales fueron suministrados el día 07 de diciembre y serán mencionados a continuación:

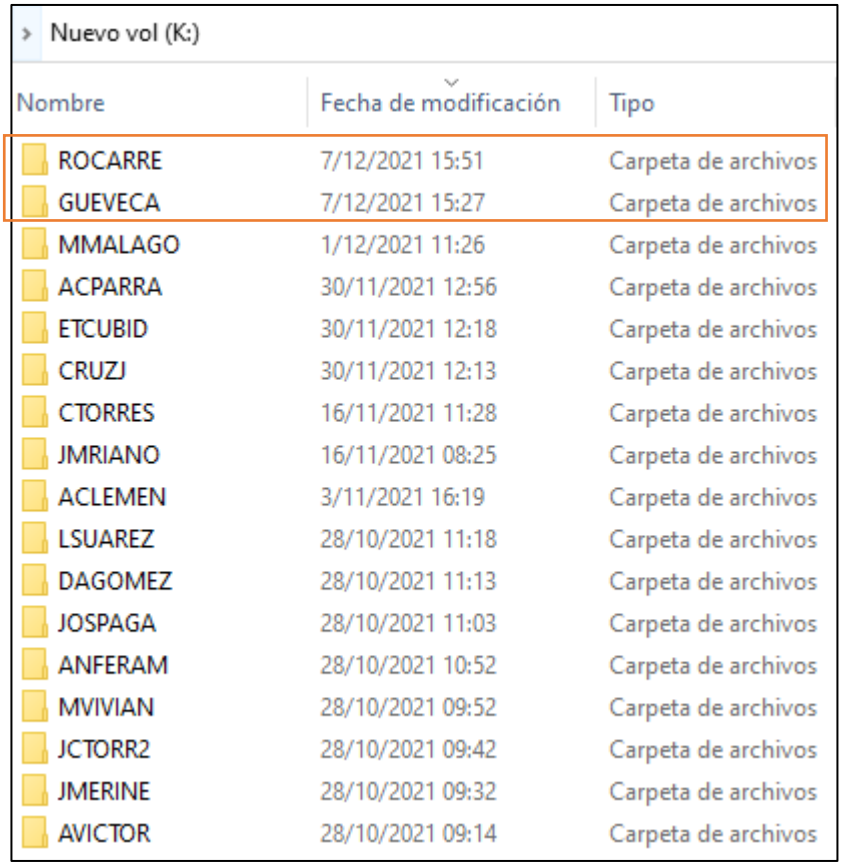


Ilustración 165 *Visualización contenido completo del Disco Duro entregado por MAPFRE SEGUROS GENERALES DE COLOMBIA S.A a 07 de diciembre de 2021.*

Adicionalmente, el señor **Willigton Leandro TORRES MORALES** indica al equipo de ADALID CORP. que no se entregaran los siguientes buzones de correo electrónico, en vista de que no se encuentran laborando en Colombia (jlcube@mapfre.com asignado a **José Luis CUBERO RIVERA** para el desarrollo de sus funciones, jalbertos@mapfre.com asignado a **Joaquín Alberto SOLERA** y aquerol@mapfre.com asignado a Luis Enrique **GIRALDO DURÁN**.

Los correos electrónicos suministrados el 07 de diciembre de 2021 serán presentados a continuación:

Correos funcionarios retirados	ORDEN ENVIO IMÁGENES fecha en la que se realizo	Tamaño GB
Carlos Alberto Guevara Mora	16 – 7 DIC -2021	**50.7 GB**
rocarre@mapfre.com.co	17 – 8 DIC -2021	**85.7 GB**

16. Buzón de correo electrónico gueveca@mapfre.com.co.

El día 01 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta GUEVECA, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:



Ilustración 166 Visualización carpeta GUEVECA

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **GUEVECA** identificada dentro del disco duro como se observa en las siguientes imágenes:

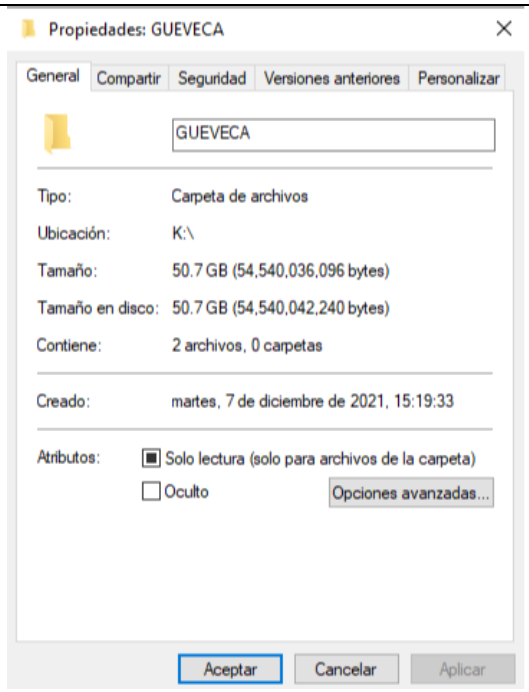


Ilustración 167 Propiedades de la carpeta GUEVECA visto desde el Disco Duro.

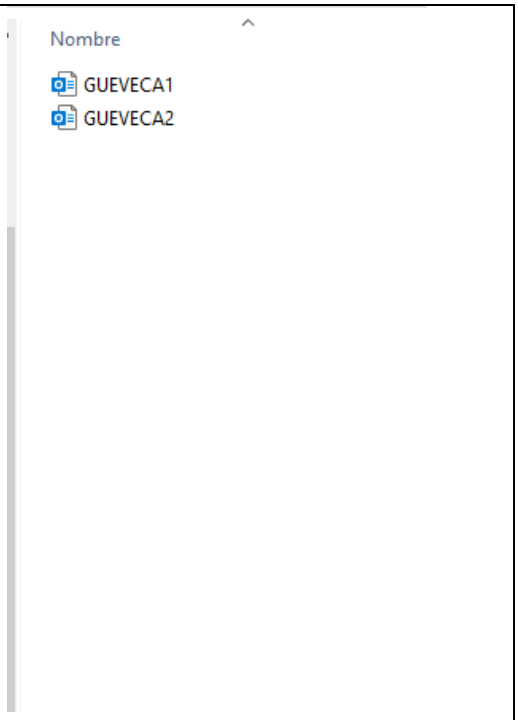


Ilustración 168 Contenido de la carpeta GUEVECA visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**gueveca@mapfre.com.co.**" asignado a **Carlos Alberto GUEVARA MORA** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **16:38:19** y culminando el mismo de forma satisfactoria a las **18:07:28,** tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_07DIC2021
Número de prueba: 016_GUEVECA
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO GUEVECA@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO

DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for
I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad1:
[Computed Hashes]
MD5 checksum: e1f945f3d80c3fc34ba37d6f39a9f07b
SHA1 checksum: a5f3f5fb0bb551475a8aa9e6b136d16d0f6c28e4

Image information:
Acquisition started: Tue Dec 7 16:38:19 2021
Acquisition finished: Tue Dec 7 17:50:18 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad22

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad23

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad24

Image Verification Results:
Verification started: Tue Dec 7 17:50:18 2021
Verification finished: Tue Dec 7 18:07:28 2021
MD5 checksum: e1f945f3d80c3fc34ba37d6f39a9f07b : verified
SHA1 checksum: a5f3f5fb0bb551475a8aa9e6b136d16d0f6c28e4 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie ***WD-WCAZA4915847***, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:





Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**gueveca@mapfre.com.co.**" asignado a **Carlos Alberto GUEVARA MORA** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 169 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO GUEVECA@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico gueveca@mapfre.com.co asignada **Carlos Alberto GUEVARA MORA** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
16	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Carlos Alberto GUEVARA MORA → gueveca@mapfre.com.co	ad1	50.7 GB
TOTAL					**50.7 GB**

Tabla 34 Detalle del buzón de correo electrónico asignado gueveca@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico gueveca@mapfre.com.co asignado a Carlos Alberto GUEVARA MORA para el desarrollo de sus funciones **aloja** un total de **50.7 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento noventa mil quinientas trece (190.513)** archivos (incluyendo carpetas), como se observa a continuación.

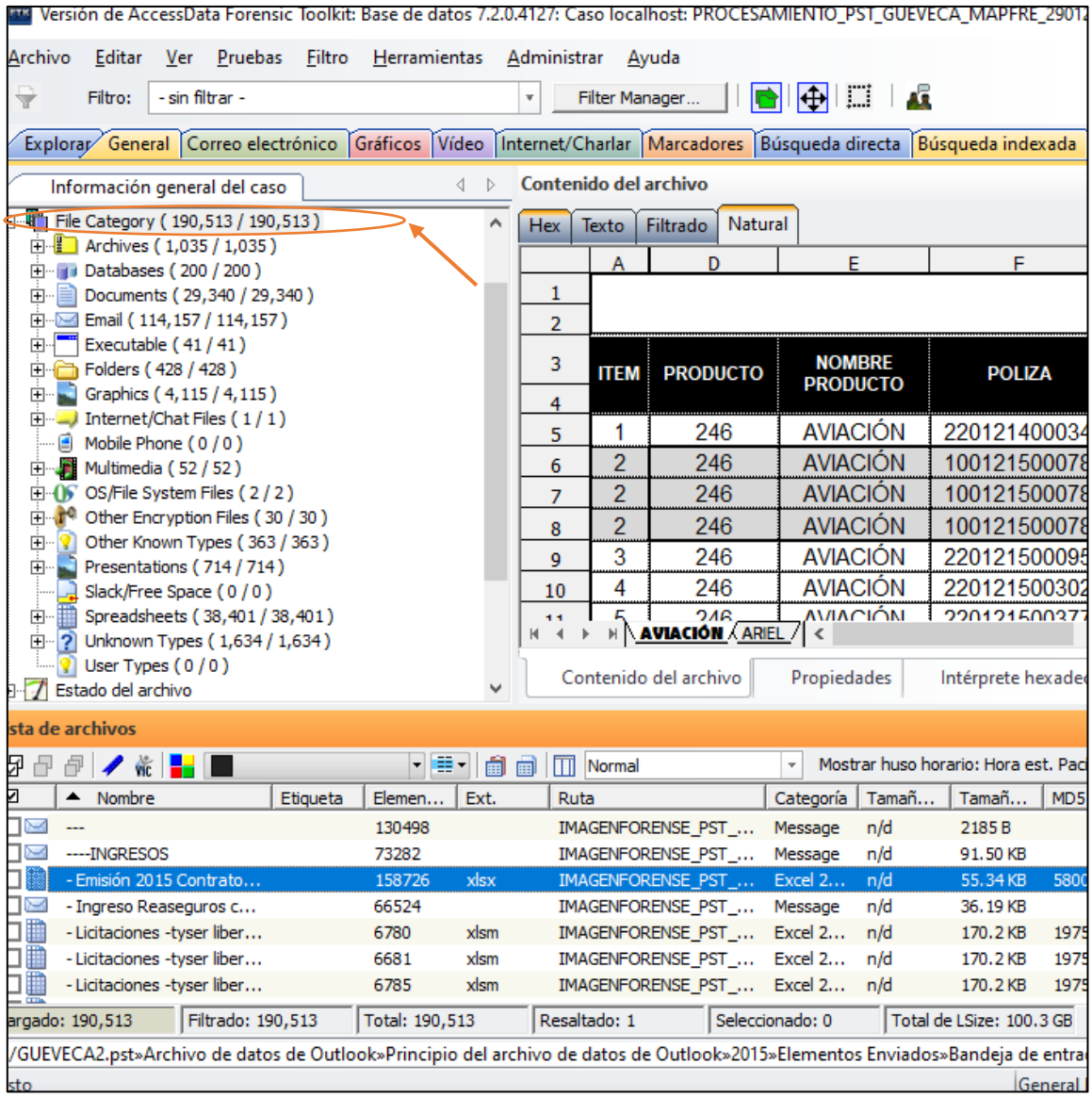


Ilustración 170 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico gueveca@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO CARLOS ALBERTO GUEVARA MORA → GUEVECA@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico gueveca@mapfre.com.co asignado a **Carlos Alberto GUEVARA MORA**, iniciando el día el **29** de enero del 2022, con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **Mil ochocientas sesenta y**

nueve (1.869) ítems en condición de "eliminados" y se reconstruyeron **Cero(0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

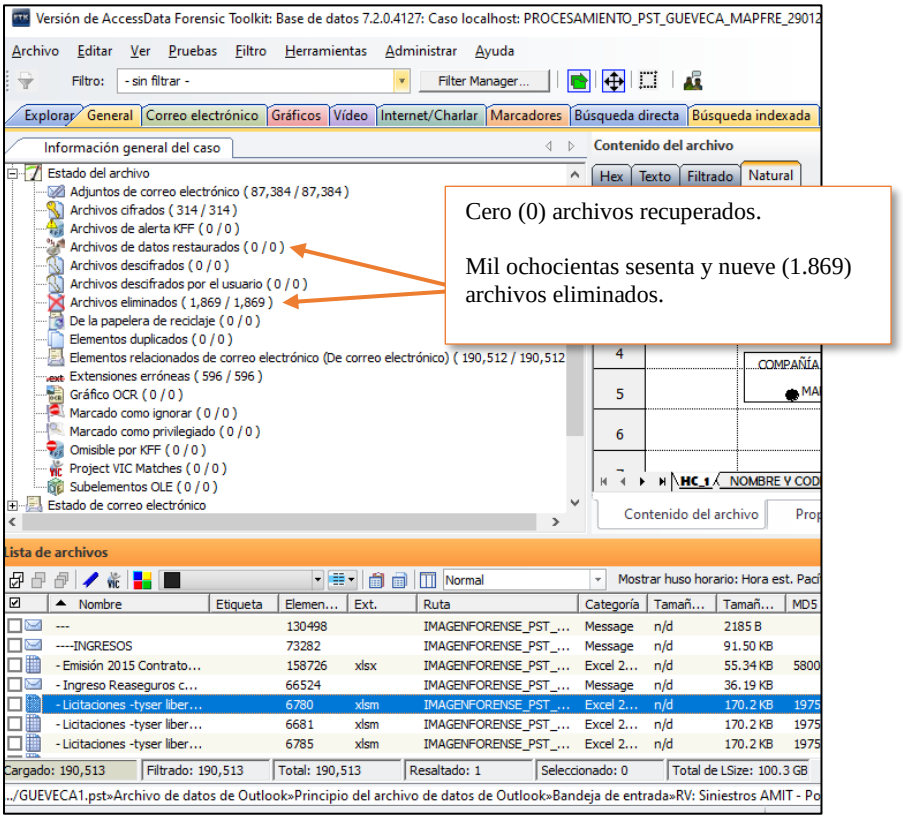


ilustración 171 Total de archivos recuperados en la cuenta de correo electrónico gueveca@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento noventa mil quinientas trece (190.513)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO GUEVECA@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico gueveca@mapfre.com.co asignado a **Carlos Alberto GUEVARA MORA** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1035
2	Bases de Datos	200
3	Documentos	29.340
4	Correo Electrónico	114.157
5	Ejecutables	41
6	Carpetas	428
7	Gráficos	4.115
8	Archivos de internet /chats	1
9	Multimedia	52
10	Archivos del sistema	2
11	Otros archivos encriptados	30
12	Otros archivos desconocidos	363
13	Presentaciones	714
14	Hojas de cálculo	38.401
15	Tipos de archivos desconocidos	1.634
TOTAL		**190.513**

Tabla 35 Información buscada evidencia 016_GUEVECA, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento noventa mil quinientas trece (190.513).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Ochenta y siete mil trescientas ochenta y cuatro (87384)** archivos de datos obtenidos por

el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Los archivos cifrados recuperados **Trescientas catorce (314) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos eliminados **Mil ochocientas sesenta y nueve (1.869) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento noventa mil quinientas doce (190.512)** archivos de datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Quinientas noventa y seis (596) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo gueveca@mapfre.com.co asignado a **Carlos Alberto GUEVARA MORA** para para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

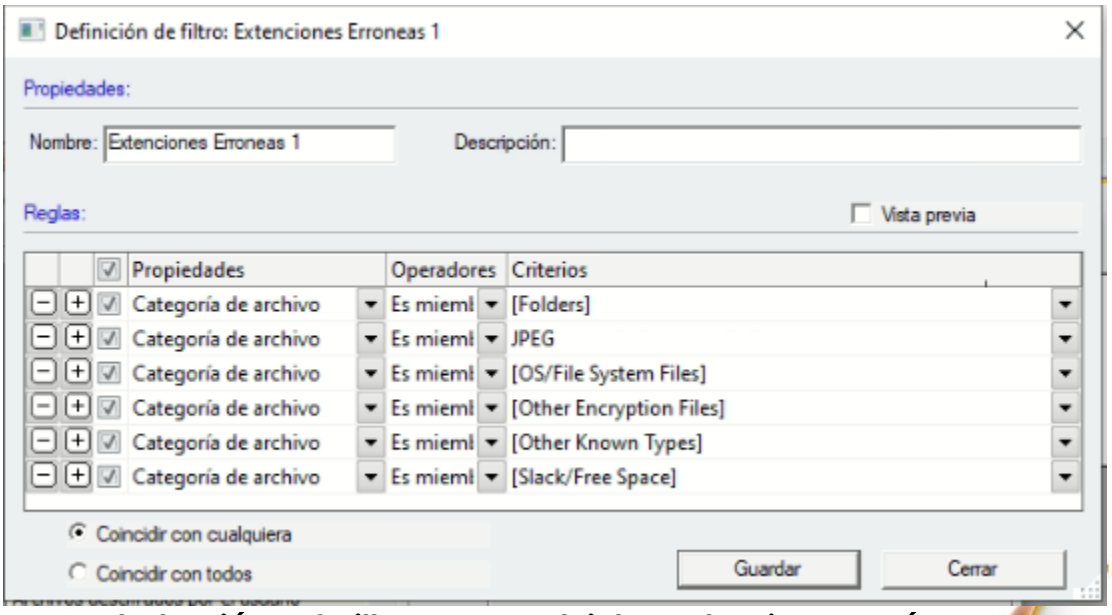


Ilustración 172 Filtro para excluir las extensiones erróneas.

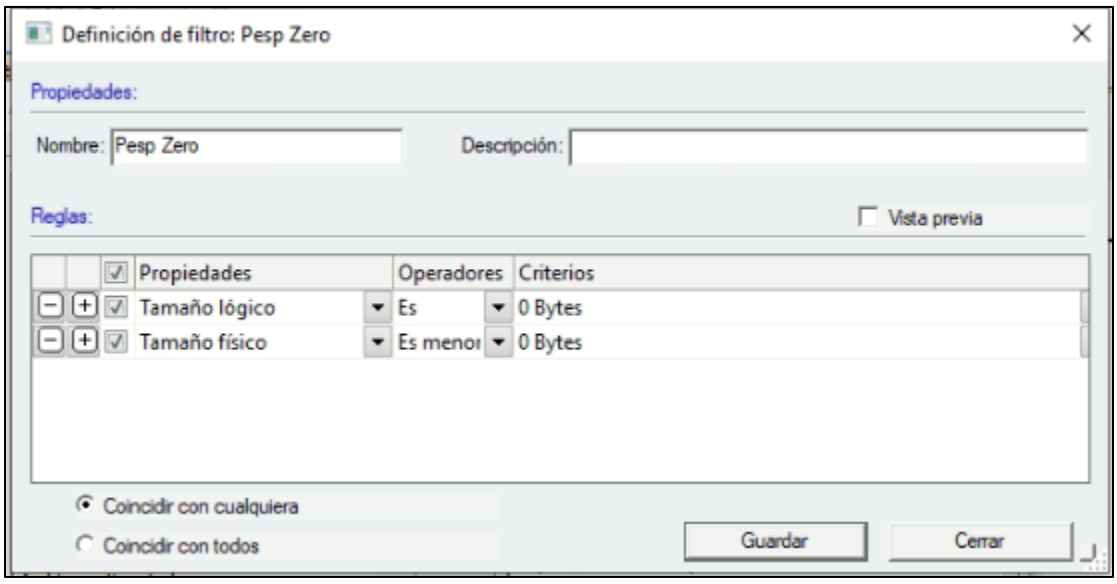


Ilustración 173 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

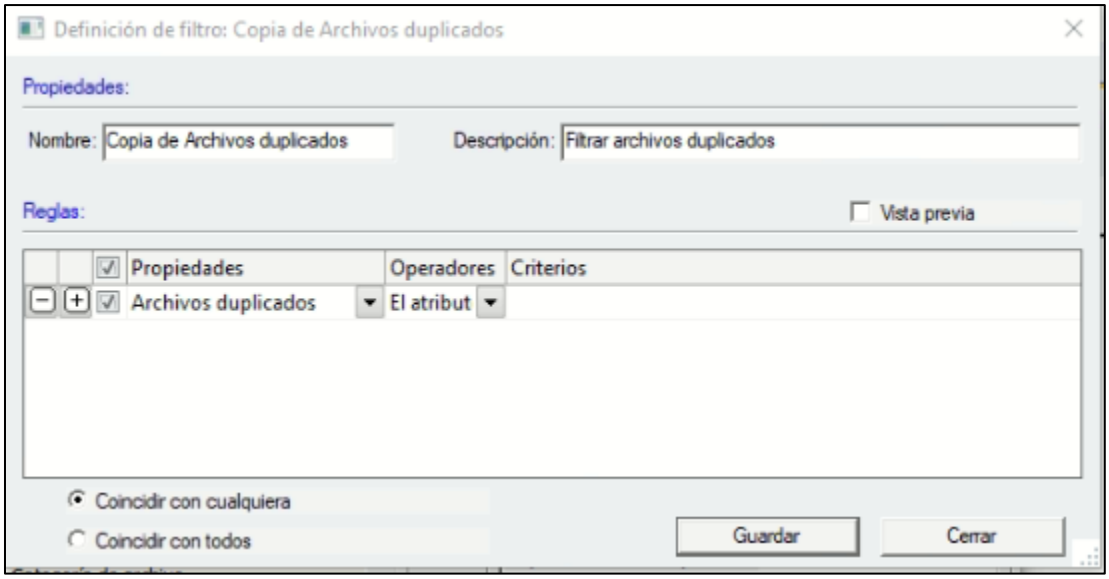


Ilustración 174 Filtro para excluir los archivos duplicados.

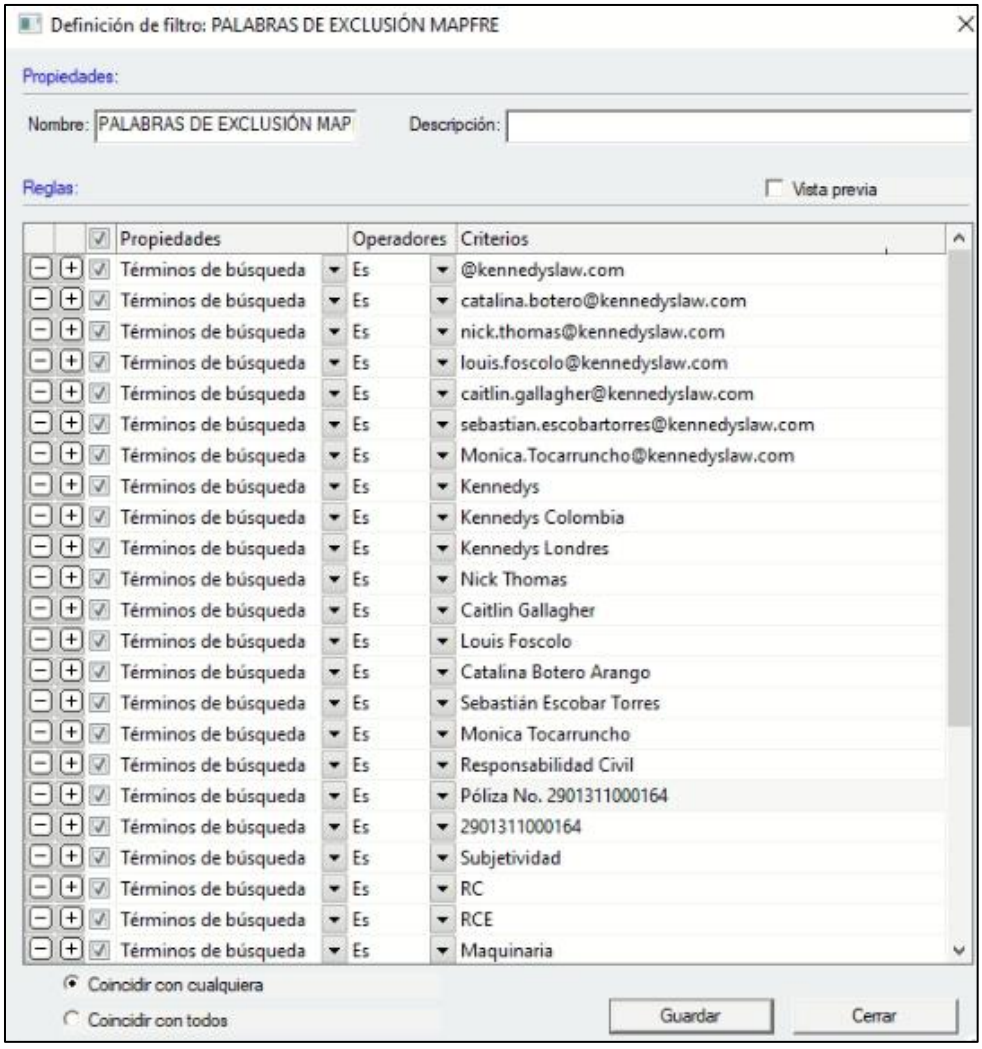


Ilustración 175 Filtro para excluir los archivos suministrado por MAPFRE - 1.

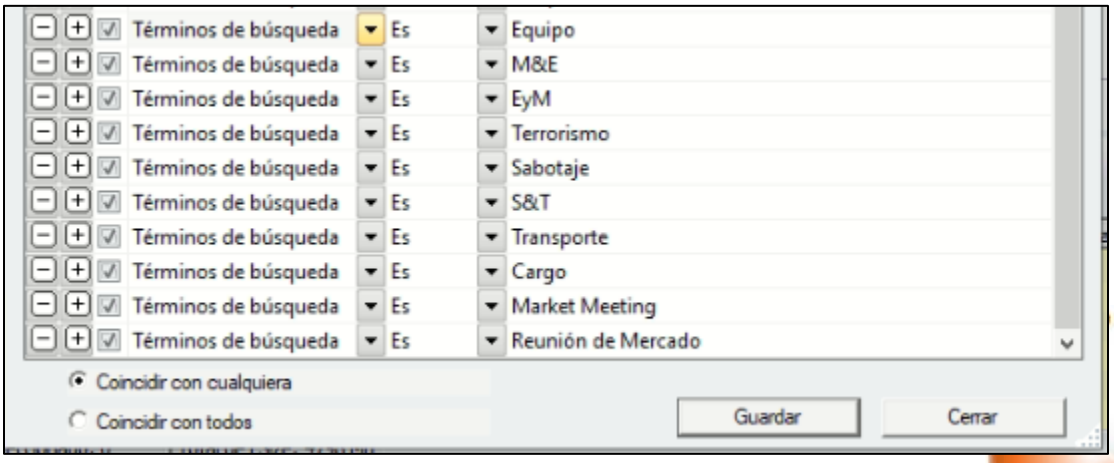
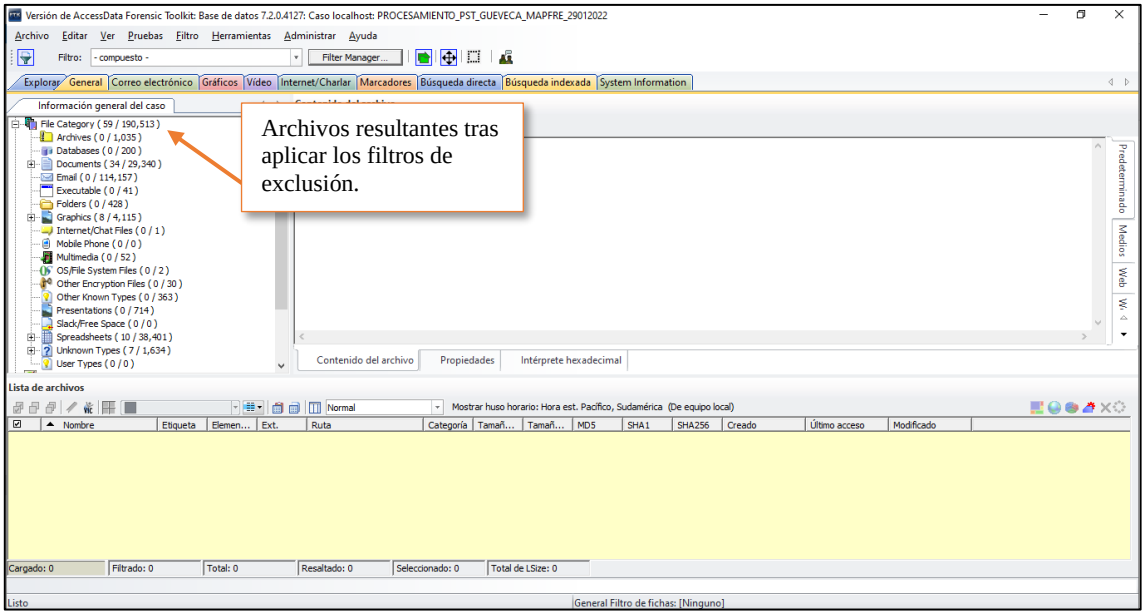


Ilustración 176 Filtro para excluir los archivos suministrado por MAPFRE - 2.

Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Cincuenta y nueve (59)** registros como se observa en la siguiente imagen:

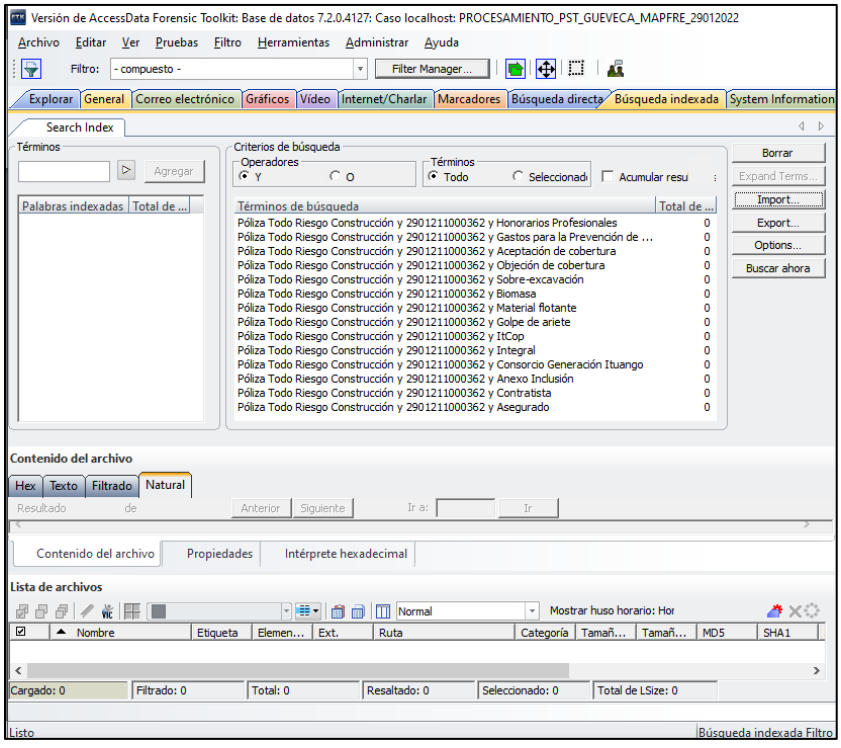


Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo gueveca@mapfre.com.co asignado a **Carlos Alberto GUEVARA MORA** para para el desarrollo de sus funciones.

17. Buzón de correo electrónico rocarre@mapfre.com.co.

El día 01 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta ROCARRE, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:



Ilustración 177 Visualización carpeta ROCARRE

Posteriormente, se procede a validar la información del contenido al interior de la carpeta ROCARRE identificada dentro del disco duro como se observa en las siguientes imágenes:

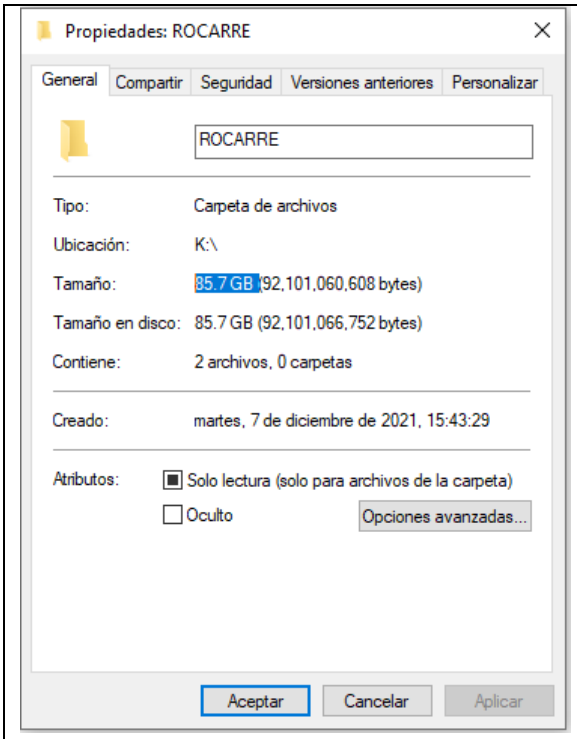


Ilustración 178 Propiedades de la carpeta ROCARRE visto desde el Disco Duro.

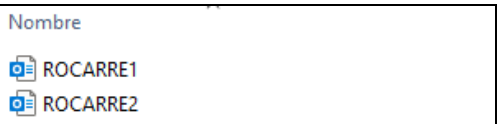


Ilustración 179 Contenido de la carpeta ROCARRE visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**rocarre@mapfre.com.co.**" asignado a ROCARRE para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las 23:07:00 y culminando el mismo de forma satisfactoria a las 02:13:30, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_08DIC2021
Número de prueba: 017_ROCARRE
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ROCARRE@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE

FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for
I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad1:
[Computed Hashes]
MD5 checksum: 775edcc80edc04552a83d75e90da2aac
SHA1 checksum: fab4be9073e47a100aaedfcbec42de7fffa2443f

Image information:
Acquisition started: Wed Dec 8 23:07:00 2021
Acquisition finished: Thu Dec 9 01:38:21 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad22

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad23

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad24

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad25

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad26

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad27

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad28

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad29

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad30

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad31

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad32

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad33

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad34

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad35

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad36

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad37

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad38

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad39

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad40

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad41

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad42

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad43

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad44

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad45

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad46

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad47

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad48

Image Verification Results:
Verification started: Thu Dec 9 01:38:21 2021
Verification finished: Thu Dec 9 02:13:30 2021
MD5 checksum: 775edcc80edc04552a83d75e90da2aac : verified

SHA1 checksum: fab4be9073e47a100aaedfcbec42de7fffa2443f : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca WESTERN DIGITAL, identificado con número de serie WD-WCAZA4915847, con capacidad de almacenamiento de 2000GB, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**rocarre@mapfre.com.co.**" asignado a **Rodrigo CARREÑO HERNÁNDEZ** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o

requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 180 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ROCARRE@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas MAPFRE SEGUROS GENERALES DE COLOMBIA S.A. para la cuenta de correo electrónico rocarre@mapfre.com.co asignada Rodrigo CARREÑO HERNÁNDEZ para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
17	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Rodrigo CARREÑO HERNÁNDEZ → rocarre@mapfre.com.co	ad1	85.7 GB
TOTAL					**85.7 GB**

Tabla 36 Detalle del buzón de correo electrónico asignado rocarre@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico rocarre@mapfre.com.co asignado a Rodrigo **CARREÑO HERNÁNDEZ** para el desarrollo de sus funciones **aloja** un total de **85.7 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento setenta y cuatro mil seiscientas cincuenta y dos (174.652)** archivos (incluyendo carpetas), como se observa a continuación.

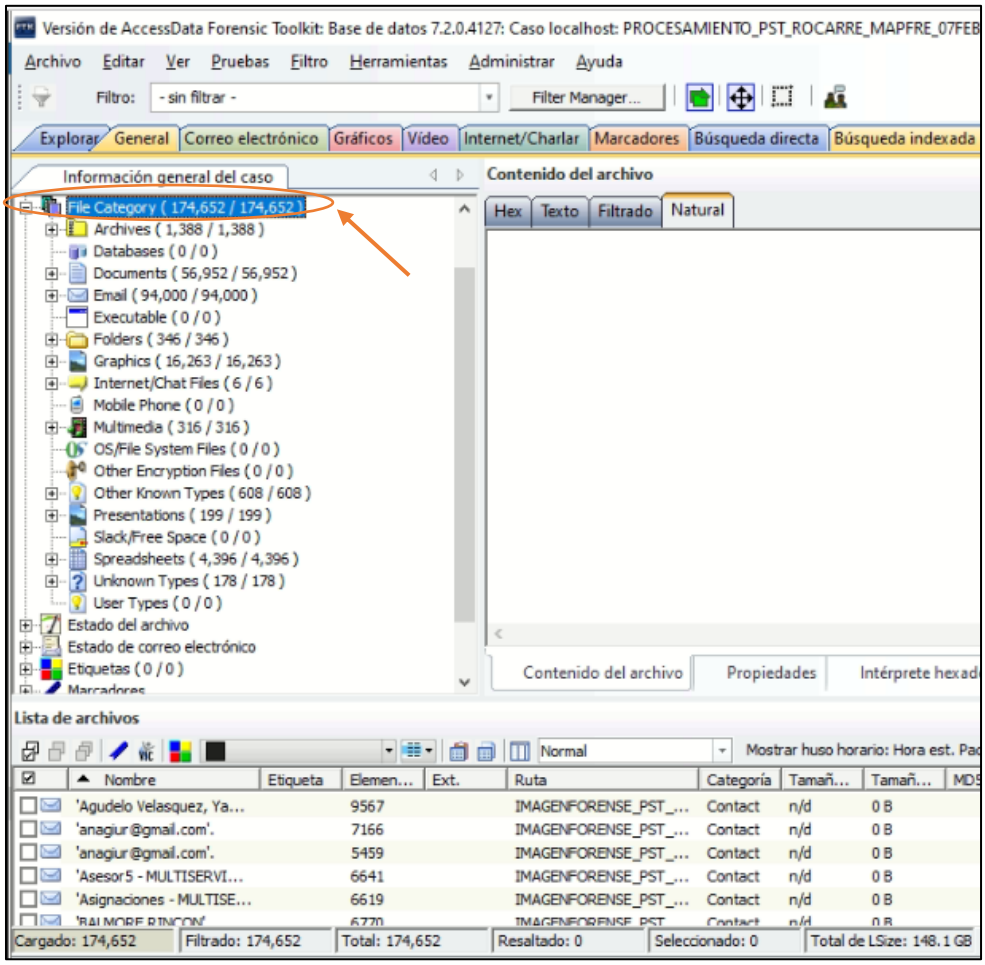


Ilustración 181 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico rocarre@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO RODRIGO CARREÑO HERNÁNDEZ → ROCARRE@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico rocarre@mapfre.com.co

asignado a Rodrigo CARREÑO HERNÁNDEZ, iniciando el día el **07** de febrero del 2022, con una duración aproximada de Cuatro (4) día calendario, el resultado a dicho proceso arrojó que existen **Mil doscientas setenta y una (1.271)** ítems en condición de "eliminados" y se reconstruyeron **Cero (0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

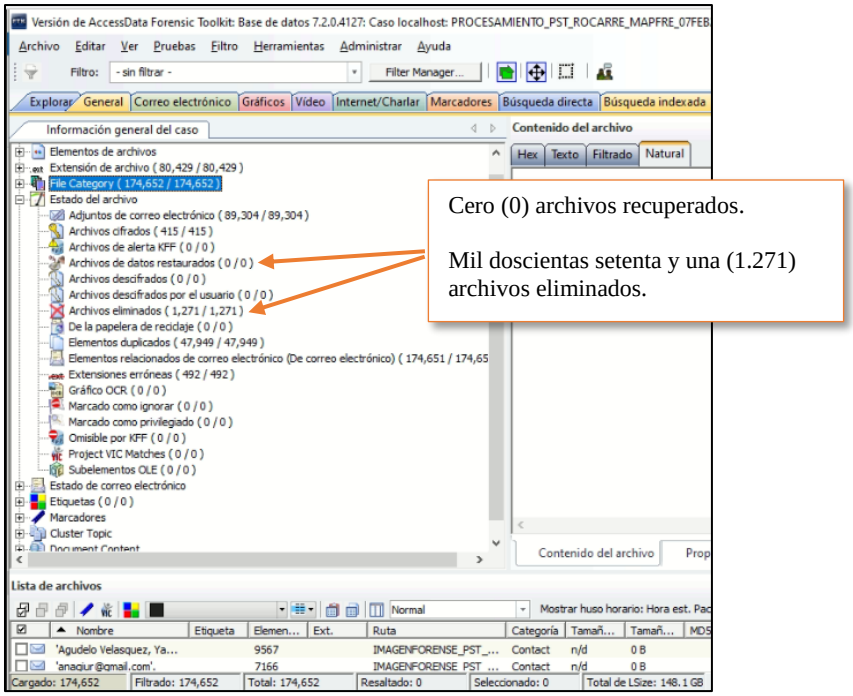


ilustración 182 Total de archivos recuperados en la cuenta de correo electrónico rocarre@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento setenta y cuatro mil seiscientas cincuenta y dos (174.652)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ROCARRE@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico rocarre@mapfre.com.co asignado a Rodrigo **CARREÑO HERNÁNDEZ** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1388
2	Documentos	56.952
3	Correo Electrónico	94.000
4	Carpetas	346
5	Gráficos	16.263
6	Archivos de internet/chats	6
7	Multimedia	316
8	Otros archivos desconocidos	608
9	Presentaciones	199
10	Hojas de cálculo	4.396
11	Tipos de archivos desconocidos	178
TOTAL		**174.652**

Tabla 37 Información buscada evidencia 017_ROCARRE, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento setenta y cuatro mil seiscientas cincuenta y dos (174.652).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Ochenta y nueve mil trescientas cuatro (89.304) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Cuatrocientas quince (415) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos eliminados **Mil doscientas setenta y una (1.271) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Cuarenta y siete mil novecientas cuarenta y nueve (47949) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento setenta y cuatro mil seiscientas cincuenta y una (174651) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Cuatrocientas noventa y dos (492) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico rocarre@mapfre.com.co asignado a Rodrigo **CARREÑO HERNÁNDEZ** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

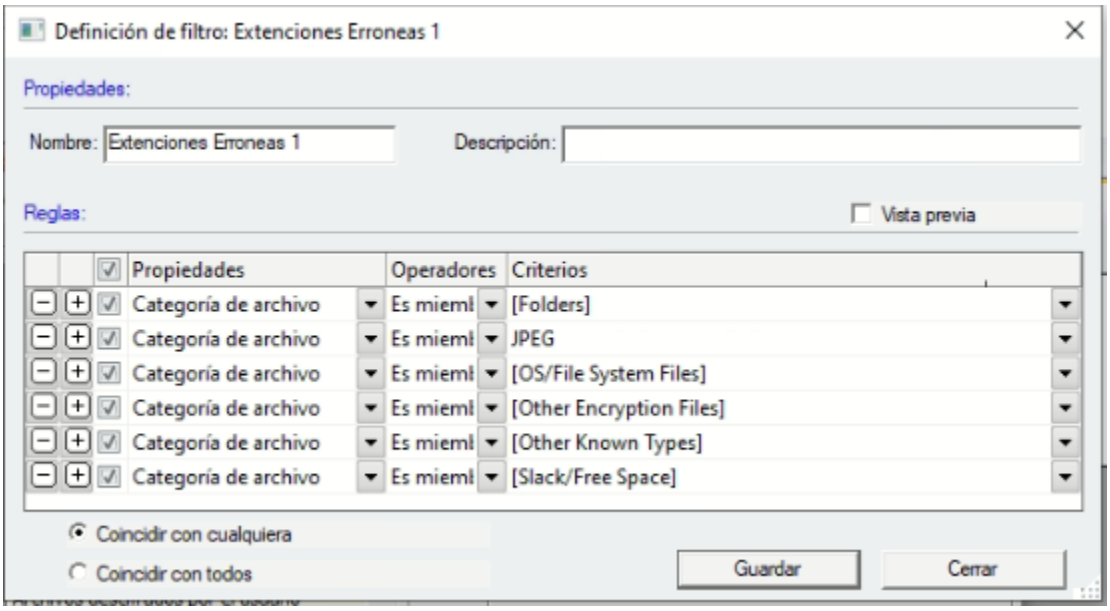


Ilustración 183 Filtro para excluir las extensiones erróneas.

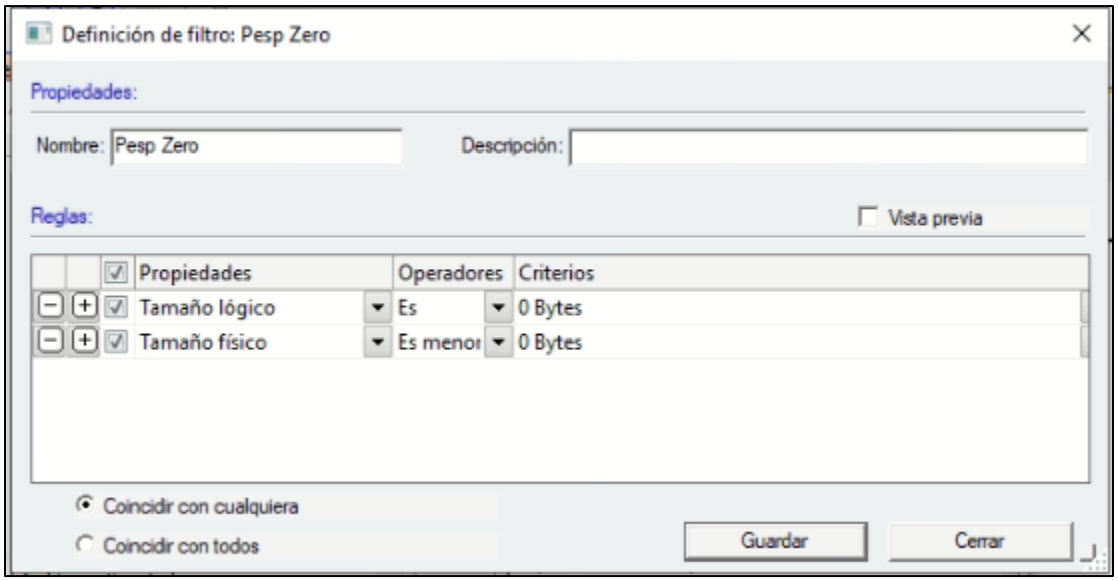


Ilustración 184 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

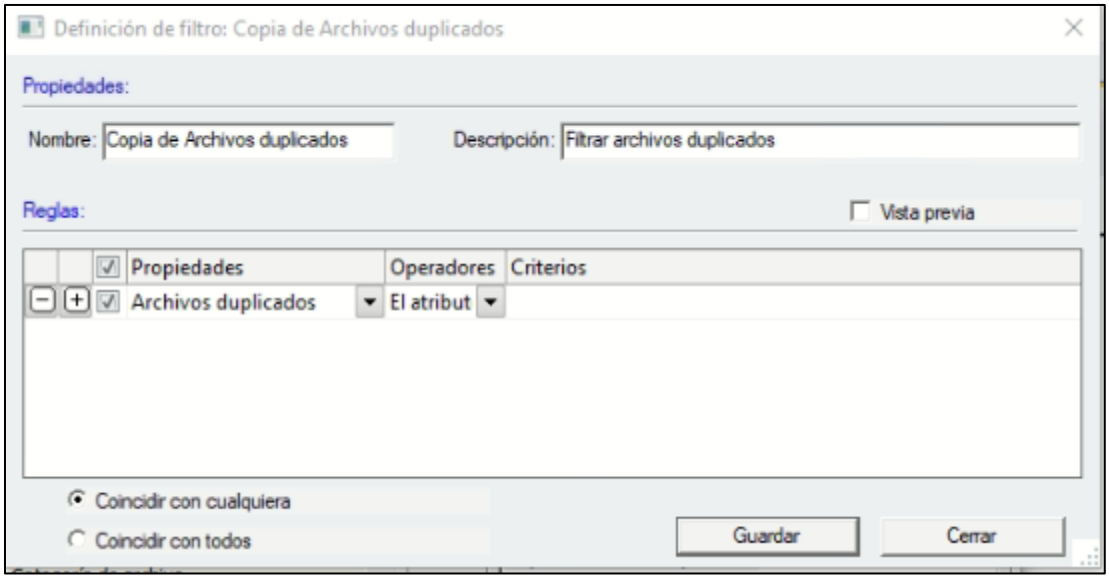


Ilustración 185 Filtro para excluir los archivos duplicados.

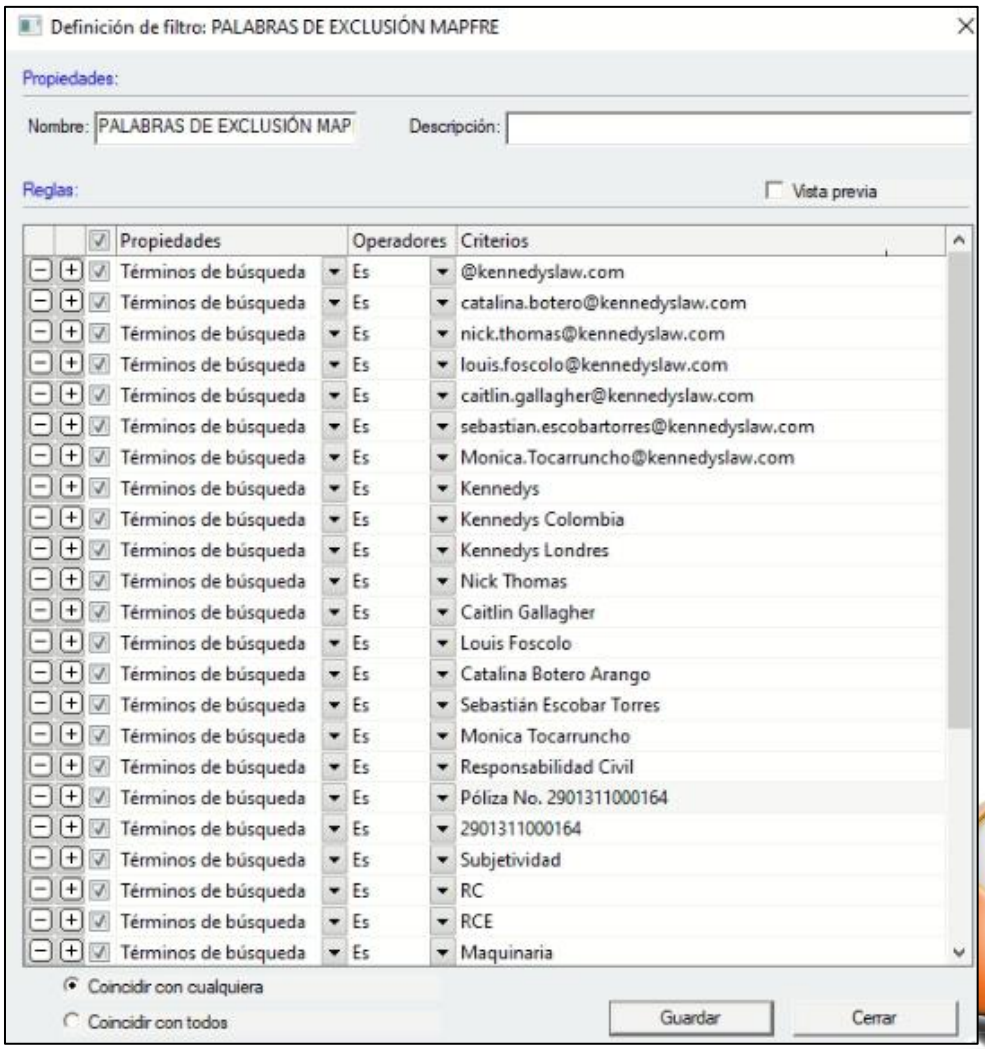


Ilustración 186 Filtro para excluir los archivos suministrado por MAPFRE - 1.

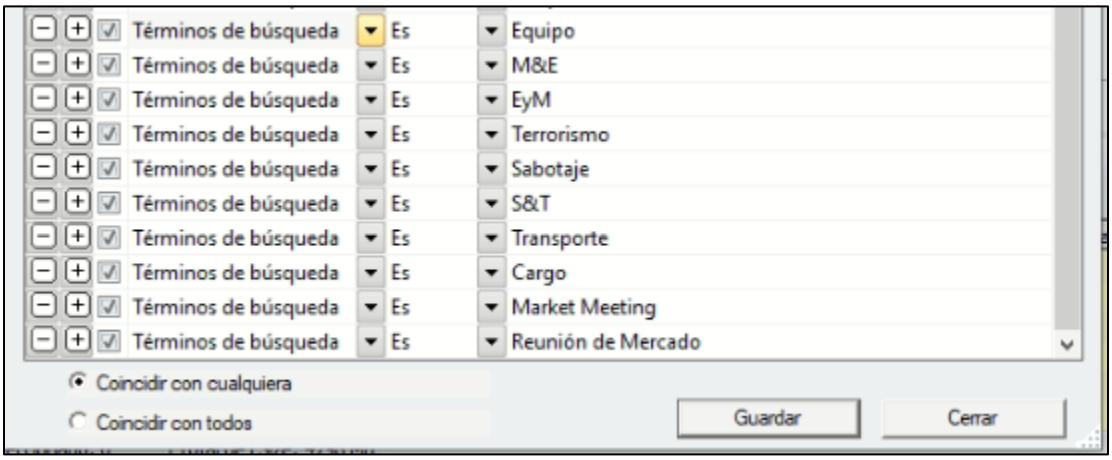
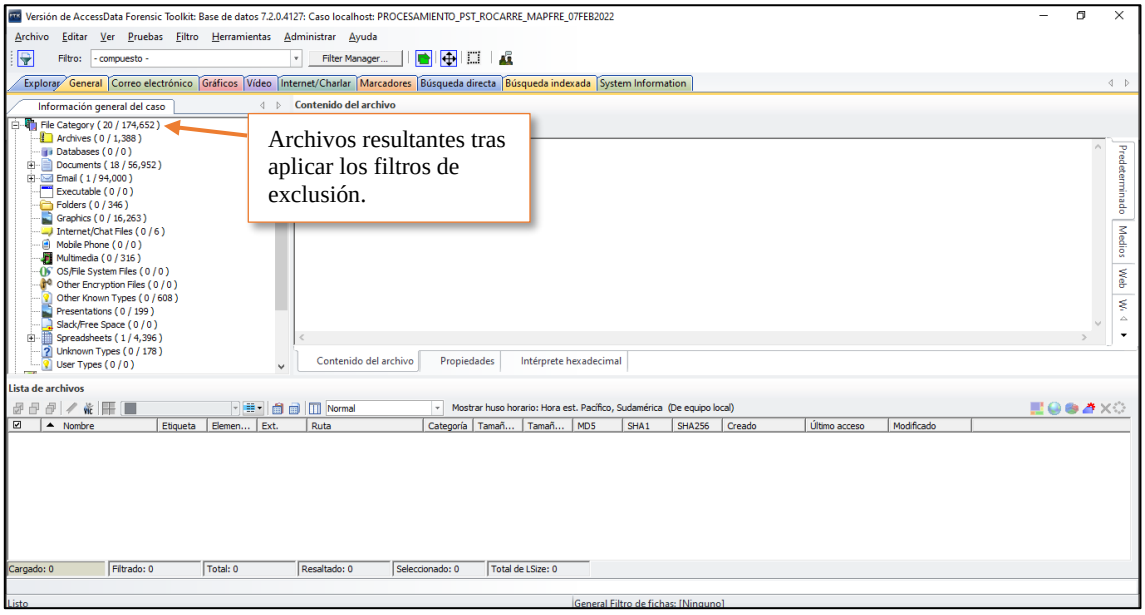


Ilustración 187 Filtro para excluir los archivos suministrado por MAPFRE - 2.

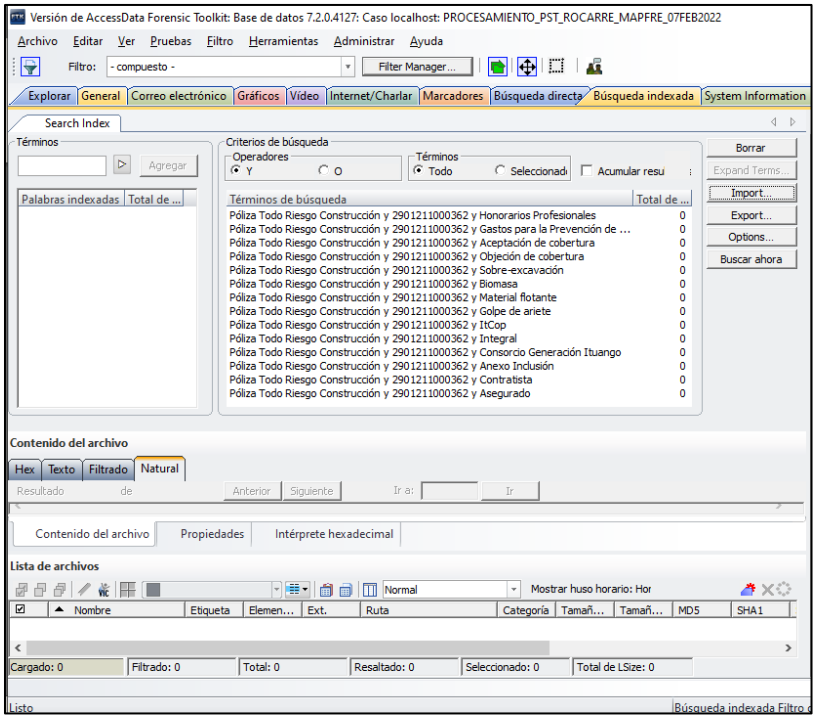
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Veinte (20)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo rocarre@mapfre.com.co asignado a Rodrigo **CARREÑO HERNÁNDEZ** para el desarrollo de sus funciones.

Una vez realizadas las imágenes forenses para los buzones de correo electrónico pertenecientes a (2) funcionarios de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** los cuales se encuentran identificados con las siguientes direcciones de correo (gueveca@mapfre.com.co, rocarre@mapfre.com.co) el equipo de ADALID CORP hace entrega de (1) Un disco duro color blanco, con capacidad de almacenamiento de **1000GB** al señor **Willigton Leandro TORRES MORALES,** identificado con cédula de ciudadanía **No. 79.708.420** de Bogotá, quien funge como **PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN** el día 14 de diciembre a las 16:00 horas.

De igual manera, el día 16 diciembre de 2021, el señor **Willigton Leandro TORRES MORALES** nuevamente hace entrega a los peritos de ADALID CORP. de (1) Un disco duro color **blanco**, con capacidad de almacenamiento de **1000GB**, el cual en su parte superior se encuentra marcado como **"prueba extraprocesal"** como se presenta a continuación**:**

	
Fotografía Disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista superior)	Fotografía disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista posterior)

Al interior del Disco Duro se identifican Dos (2) buzones de correo en formato .PST como se muestra en la siguiente imagen:

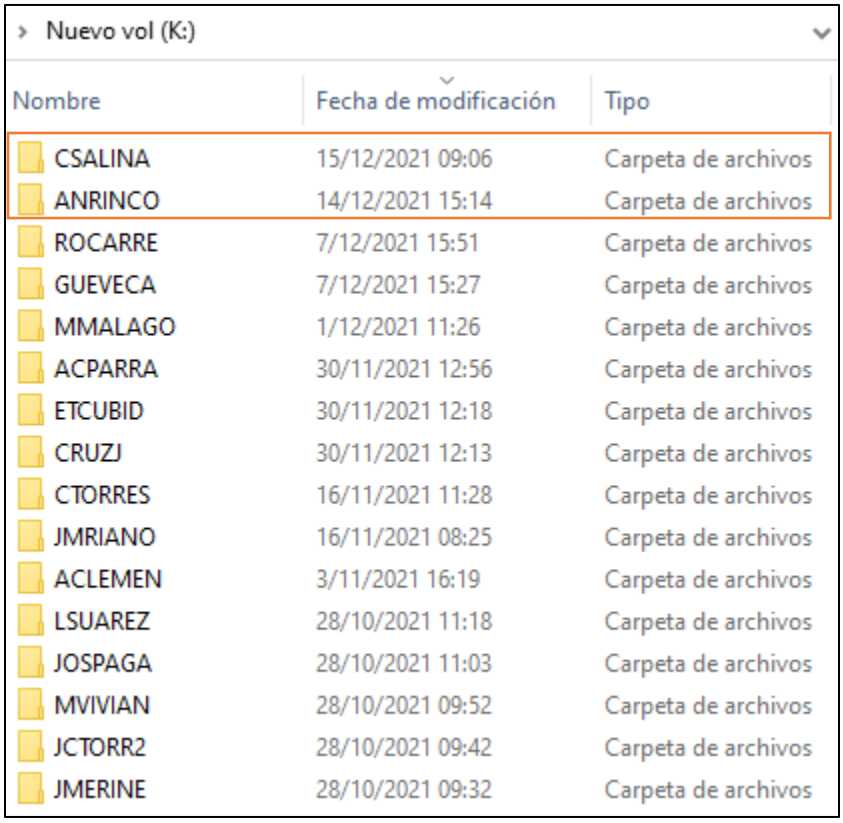


Ilustración 188 *Visualización contenido completo del Disco Duro entregado por MAPFRE SEGUROS GENERALES DE COLOMBIA S.A a 17 de diciembre de 2021.*

Los correos electrónicos suministrados el 16 de diciembre de 2021 serán presentados a continuación:

Correos funcionarios retirados	ORDEN ENVIO IMÁGENES fecha en la que se realizo	Tamaño GB
Claudia Rocio SALINASI	**18 – 17 DIC -2021**	**40.4 GB**
Andrés Alfonso RINCON	**19 – 17 DIC -2021**	**55.6 GB**

18. Buzón de correo electrónico csalina@mapfre.com.co.

El día 17 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta **CSALINA**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

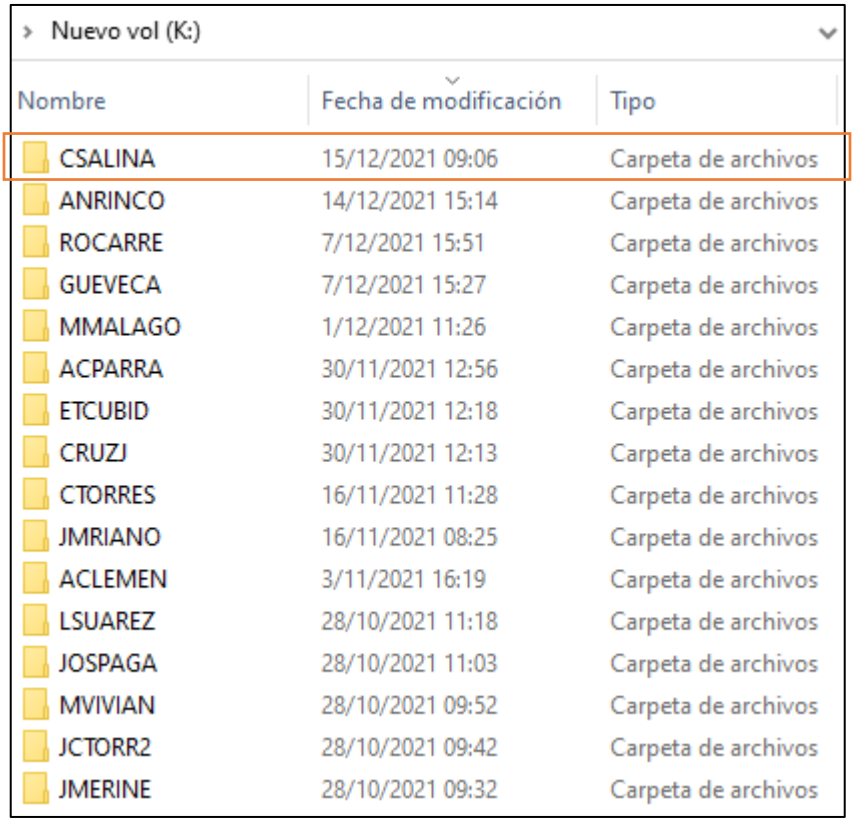


Ilustración 189 Visualización carpeta CSALINA

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **CSALINA** identificada dentro del disco duro como se observa en las siguientes imágenes:

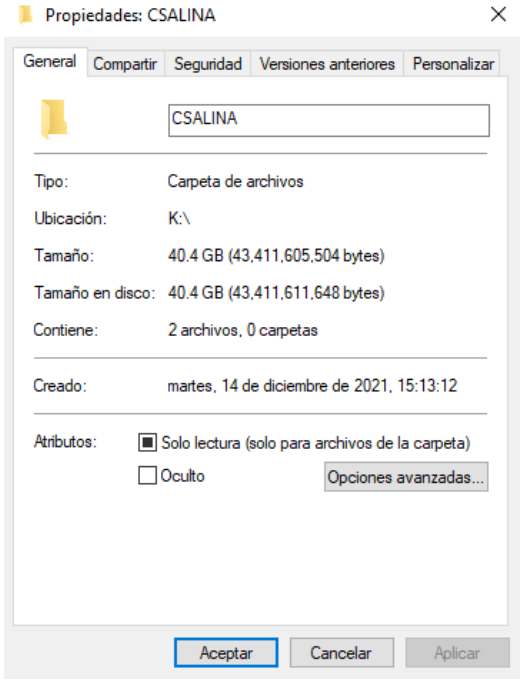


Ilustración 190 Propiedades de la carpeta CSALINA visto desde el Disco Duro.

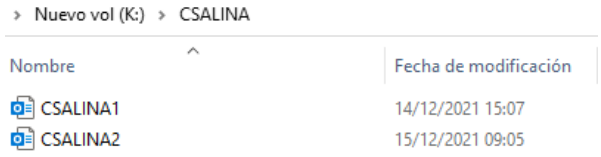


Ilustración 191 Contenido de la carpeta CSALINA visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**csalina@mapfre.com.co**" asignado a **Claudia ROCIO SALINASI** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **09:28:43** y culminando el mismo de forma satisfactoria a las **10:17:32**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_17DIC2021
Número de prueba: 18_CSALINA
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO CSALINA@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO

DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad1:
[Custom Content Sources]
K::K:\ | CSALINA | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: ec0267c1a3ffa7b40f2a9d9b6c1bbcc0
SHA1 checksum: b5e7ea4b96117e879d13928e2dc3da51aa6c4089

Image information:
Acquisition started: Fri Dec 17 09:28:43 2021
Acquisition finished: Fri Dec 17 10:07:33 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad20

Image Verification Results:

Verification started: Fri Dec 17 10:07:34 2021 Verification finished: Fri Dec 17 10:17:32 2021 MD5 checksum: ec0267c1a3ffa7b40f2a9d9b6c1bbcc0 : verified SHA1 checksum: b5e7ea4b96117e879d13928e2dc3da51aa6c4089 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**csalina@mapfre.com.co.**" asignado a **Claudia ROCIO SALINASI** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**

Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 192 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO CSALINA@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico csalina@mapfre.com.co asignada Claudia ROCIO SALINASI para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
18	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Claudia ROCIO SALINASI → csalina@mapfre.com.co	ad1	40.4 GB
TOTAL					**40.4 GB**

Tabla 38 Detalle del buzón de correo electrónico asignado csalina@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico csalina@mapfre.com.co asignado a Claudia ROCIO SALINASI para el desarrollo de sus funciones **aloja** un total de **40.4 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento veinticinco mil seiscientos dieciocho (125.618)** archivos (incluyendo carpetas), como se observa a continuación.

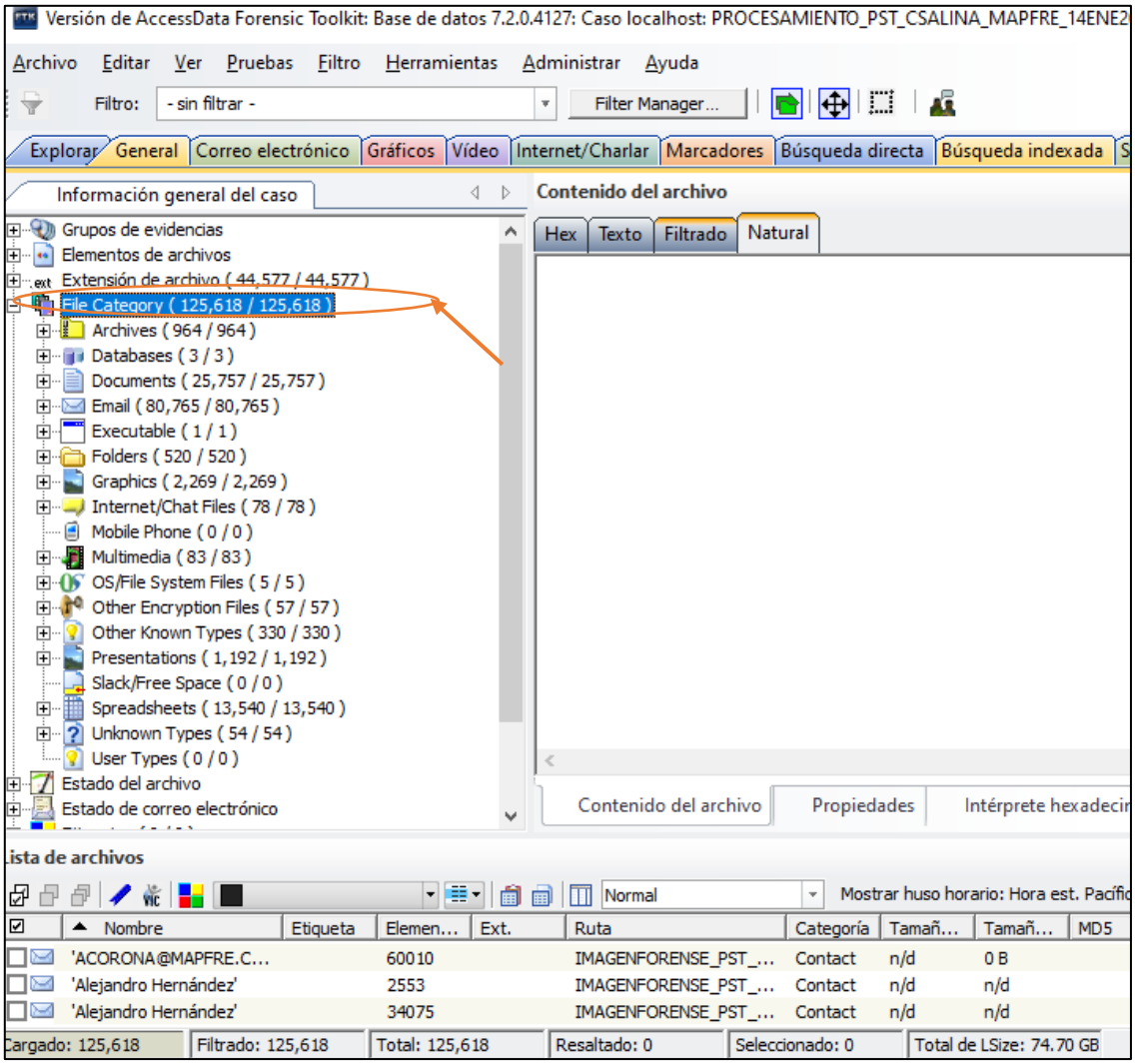


Ilustración 193 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico csalina@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO CLAUDIA ROCIO SALINASI → CSALINA@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos,

en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico csalina@mapfre.com.co asignado a Claudia ROCIO SALINASI, iniciando el día el **14** de enero del 2022, con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **Cuatrocientos treinta y cuatro (434)** ítems en condición de "eliminados" y se reconstruyeron **Cero (0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

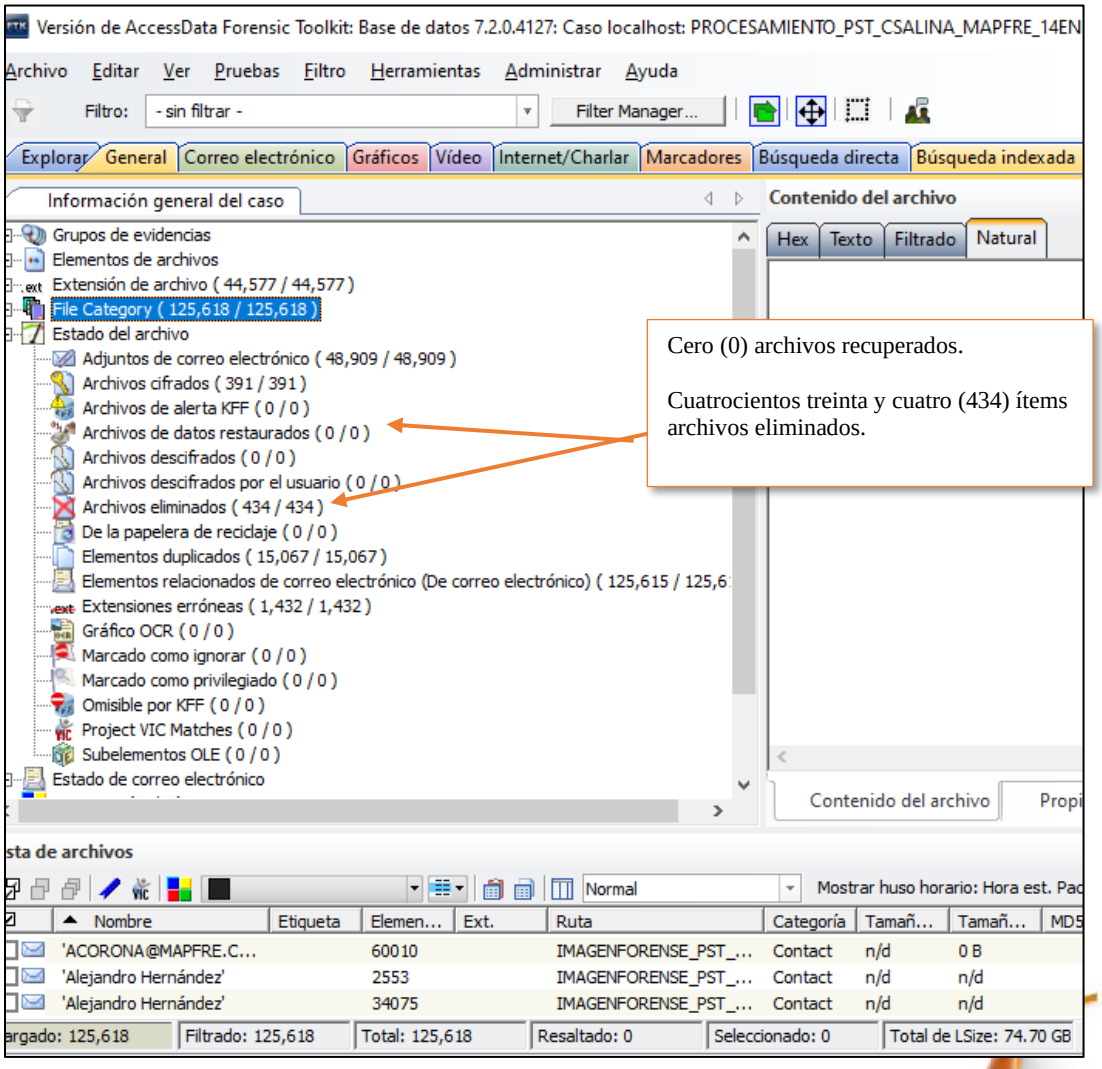


ilustración 194 Total de archivos recuperados en la cuenta de correo electrónico csalina@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS**

GENERALES DE COLOMBIA S.A., es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento veinticinco mil seiscientos dieciocho (125.618)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO CSALINA@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico csalina@mapfre.com.co asignado a **Claudia ROCIO SALINASI** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	964
2	Bases de Datos	3
3	Documentos	25.757
4	Correo Electrónico	80.765
5	Ejecutables	1
6	Carpetas	520
7	Gráficos	2.269
8	archivos de internet/chat	78
9	Multimedia	83
10	Archivos del sistema	5
11	Otros archivos encriptados	57
12	Otros archivos desconocidos	330
13	Presentaciones	1192
14	Hojas de cálculo	13.540
15	Tipos de archivos desconocidos	54
TOTAL		**125.618**

Tabla 39 Información buscada evidencia 018_CSALINA, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento veinticinco mil seiscientos dieciocho (125.618)**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de

depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Cuarenta y ocho mil novecientos nueve (48.909) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Trescientos noventa y un (391) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos Eliminados **Cuatrocientos treinta y cuatro (434) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Quince mil sesenta y siete (15.067) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento veinticinco mil seiscientos quince (125.615) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Mil cuatrocientos treinta y dos (1432) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico csalina@mapfre.com.co asignado a **Claudia ROCIO SALINASI** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



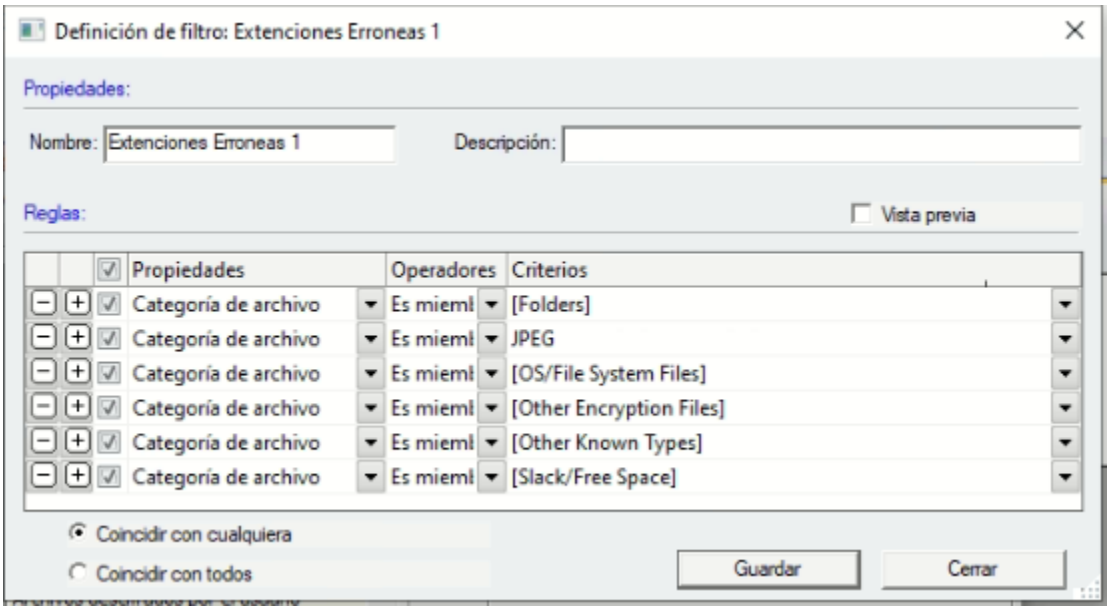


Ilustración 195 Filtro para excluir las extensiones erróneas.

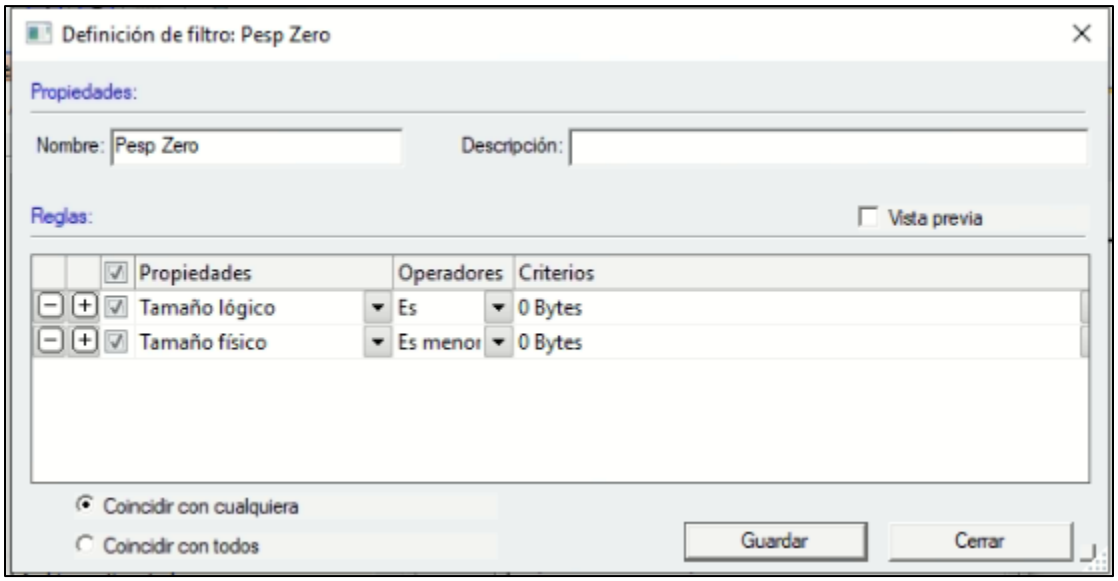


Ilustración 196 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

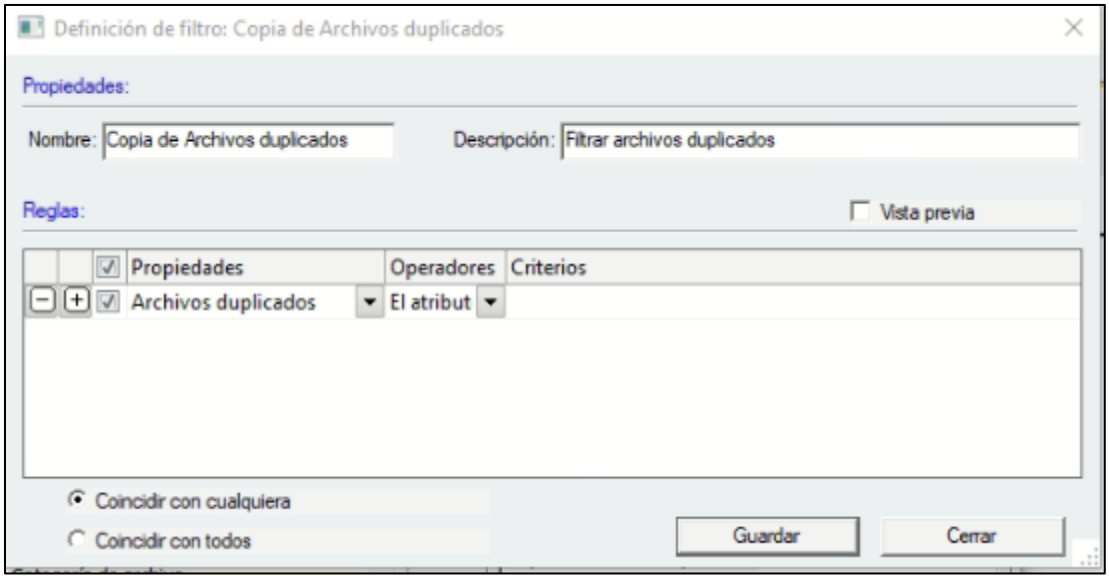


Ilustración 197 Filtro para excluir los archivos duplicados.

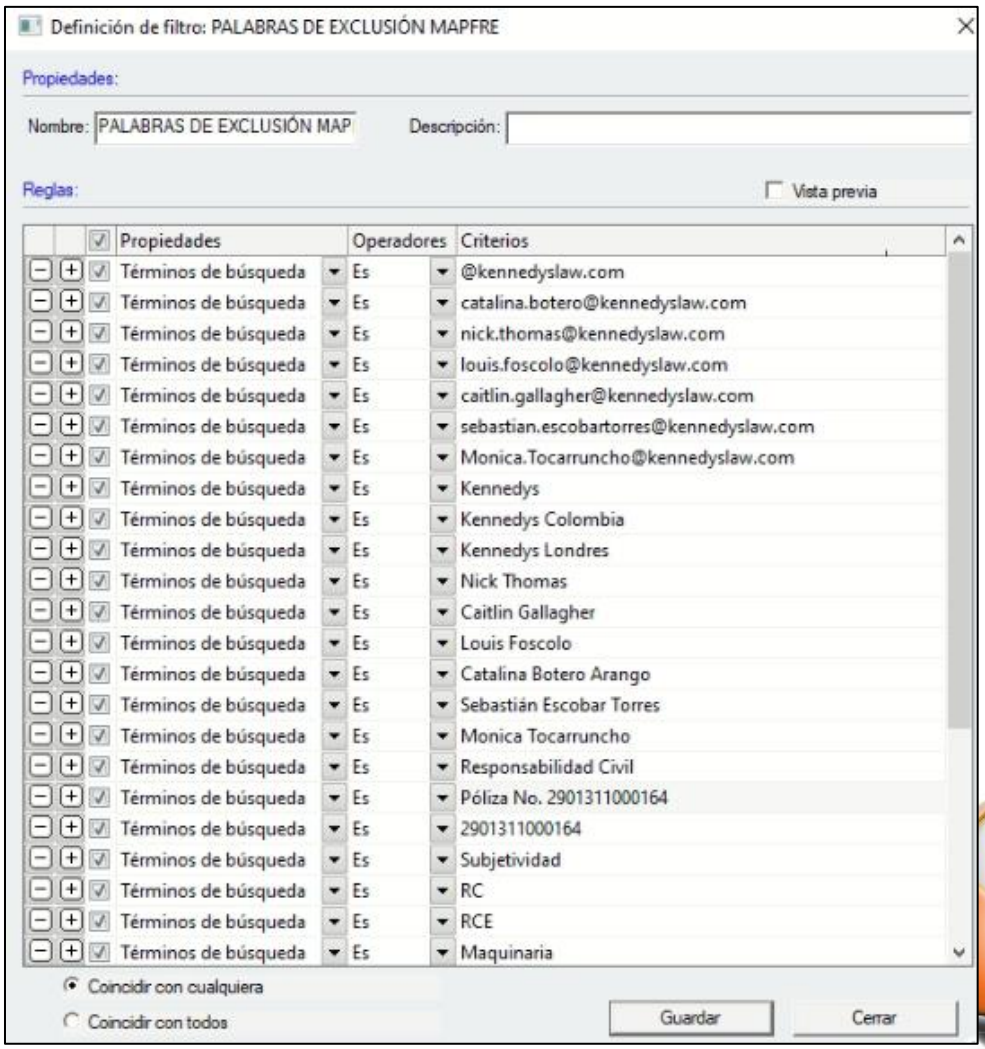


Ilustración 198 Filtro para excluir los archivos suministrado por MAPFRE - 1.

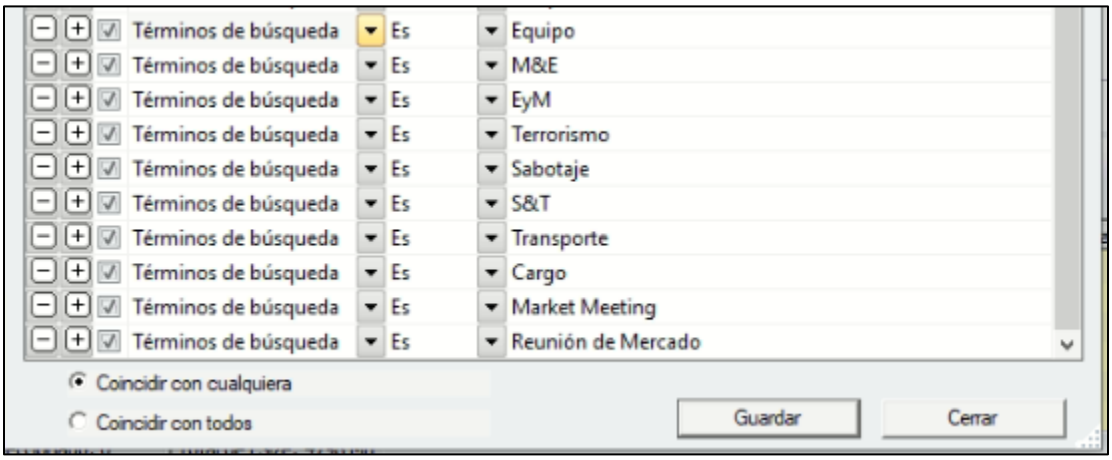
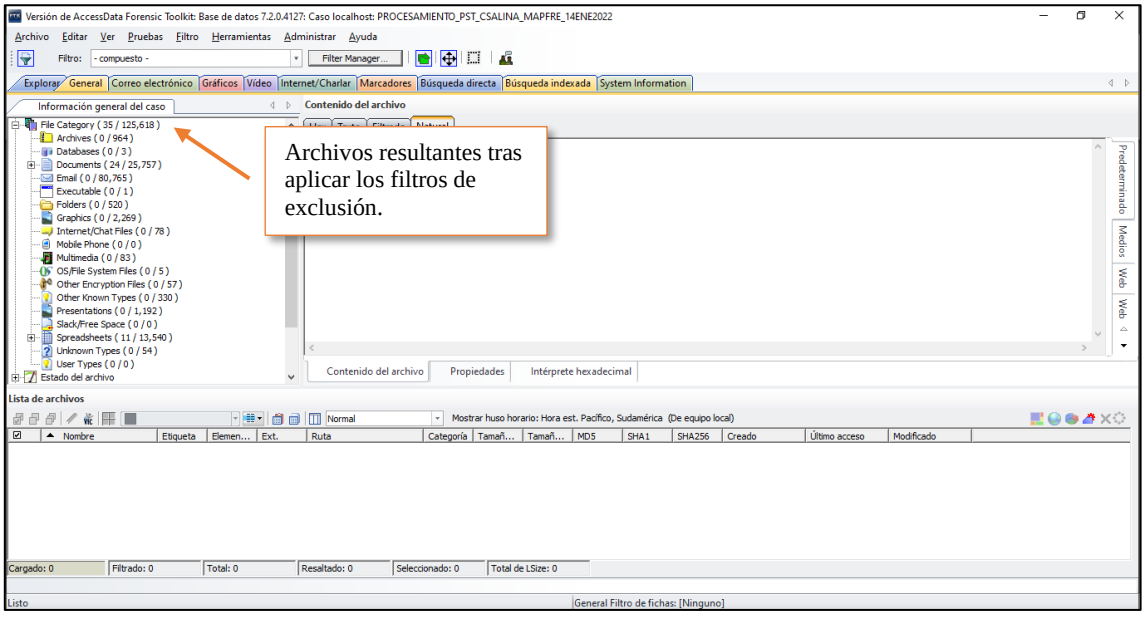


Ilustración 199 Filtro para excluir los archivos suministrado por MAPFRE - 2.

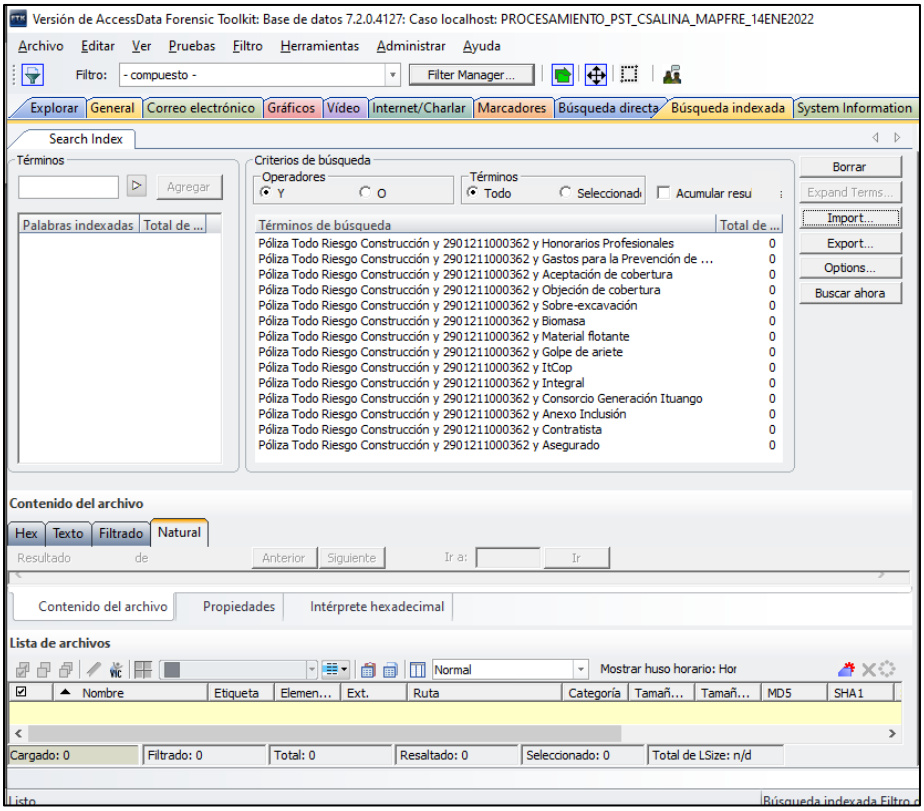
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Treinta y cinco (35)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo csalina@mapfre.com.co asignado a **Claudia ROCIO SALINASI** para el desarrollo de sus funciones.

19. Buzón de correo electrónico anrinco@mapfre.com.co.

El día 17 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta **ANRINCO**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

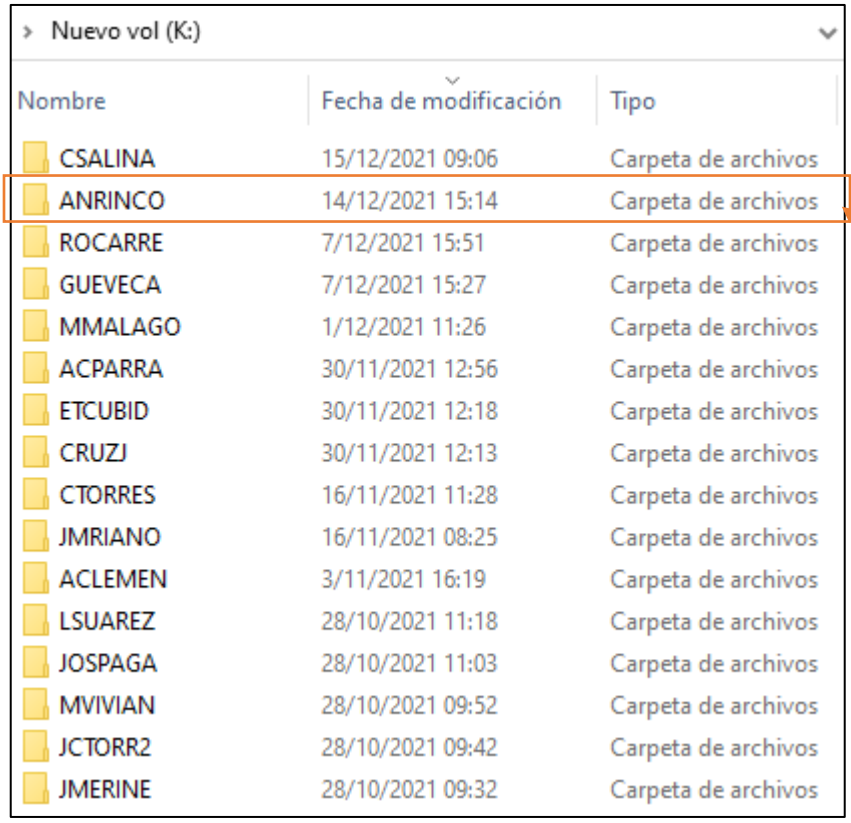


Ilustración 200 Visualización carpeta ANRINCO

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **ANRINCO** identificada dentro del disco duro como se observa en las siguientes imágenes:

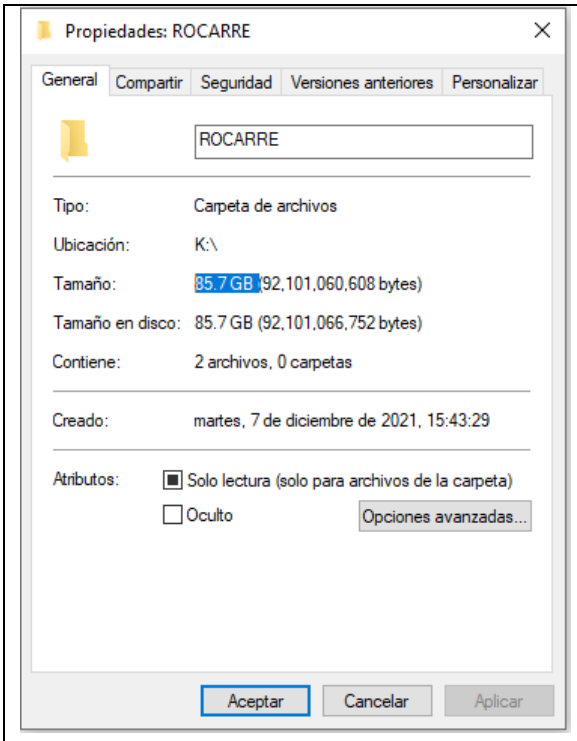


Ilustración 201 Propiedades de la carpeta ANRINCO visto desde el Disco Duro.

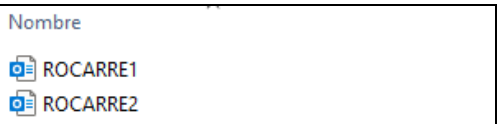


Ilustración 202 Contenido de la carpeta ANRINCO visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**anrinco@mapfre.com.co**" asignado a **Andrés Alfonso RINCON** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **10:24:34** y culminando el mismo de forma satisfactoria a las **11:28:33**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_17DIC2021
Número de prueba: 19_ANRINCO
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ANRINCO@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE

FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad1:
[Custom Content Sources]
K::K:\ | ANRINCO | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: b579effd896fb4f8c349e6490dc95a5f
SHA1 checksum: d608596c5fd7c32134969a1d9903f3a1ea837d62

Image information:
Acquisition started: Fri Dec 17 10:24:34 2021
Acquisition finished: Fri Dec 17 11:14:57 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad1

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad2

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad3

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad4

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad5

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad6

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad7

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad8

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad9

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad10

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad11

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad12

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad13

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad14

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad15

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad16

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad17

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad18

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad19

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad20

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad21

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad22

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad23

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad24

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad25

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad26

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad27

Image Verification Results:
Verification started: Fri Dec 17 11:14:57 2021
Verification finished: Fri Dec 17 11:28:33 2021
MD5 checksum: b579effd896fb4f8c349e6490dc95a5f : verified
SHA1 checksum: d608596c5fd7c32134969a1d9903f3a1ea837d62 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:



	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**anrinco@mapfre.com.co.**" asignado a **Andrés Alfonso RINCON** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 203 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ANRINCO@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas MAPFRE SEGUROS GENERALES DE COLOMBIA S.A. para la cuenta de correo electrónico anrinco@mapfre.com.co asignada Andrés Alfonso RINCON para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
19	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Andrés Alfonso RINCON → anrinco@mapfre.com.co	ad1	55.6 GB
TOTAL					**55.6 GB**

Tabla 40 Detalle del buzón de correo electrónico asignado anrinco@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico anrinco@mapfre.com.co asignado a Andrés Alfonso RINCON para el desarrollo de sus funciones **aloja** un total de **55.6 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento**

treinta y nueve mil cuatrocientos sesenta y siete (139.467) archivos (incluyendo carpetas), como se observa a continuación.

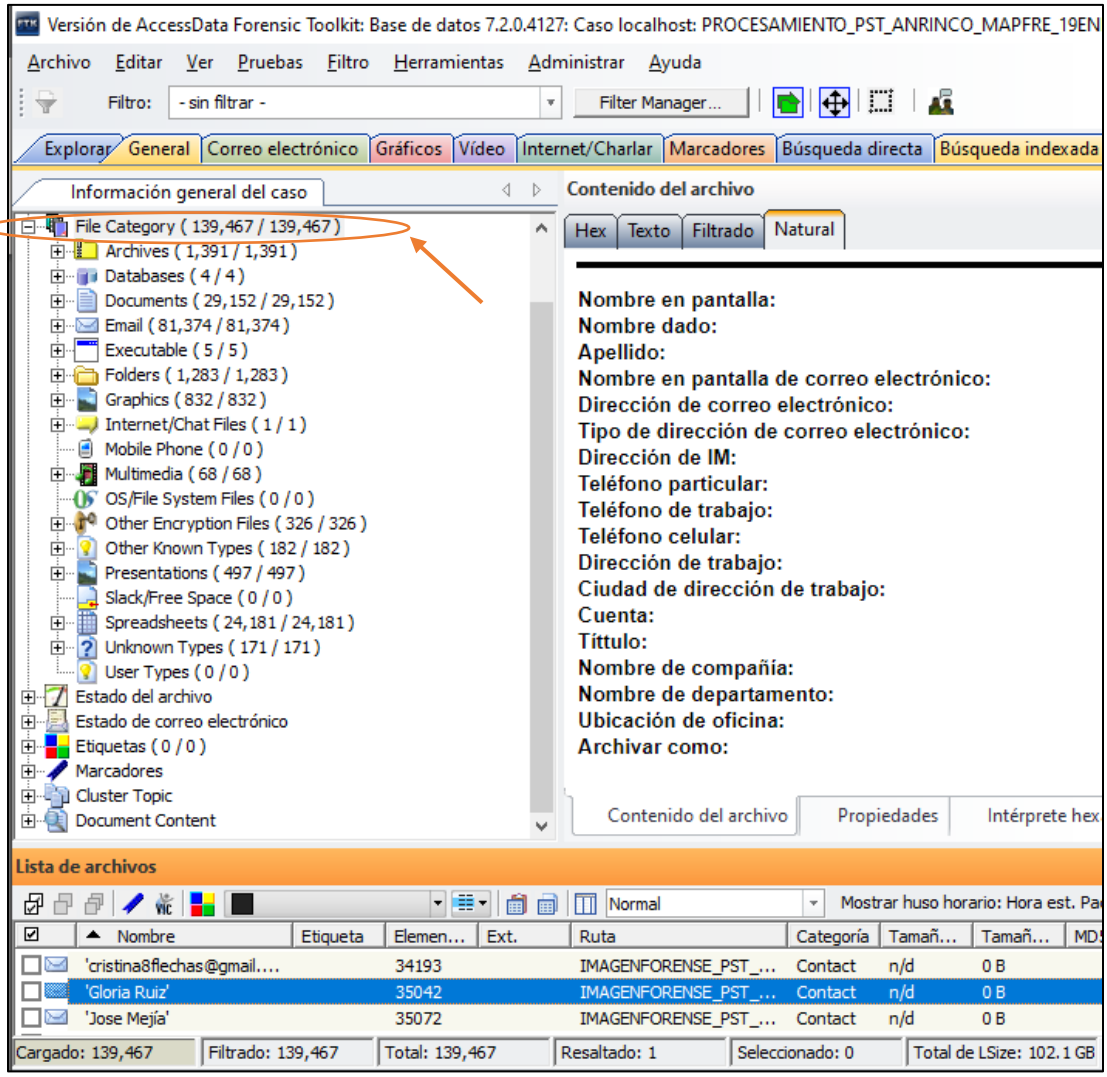


Ilustración 204 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico anrinco@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO ANDRÉS ALFONSO RINCON → ANRINCO@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico anrinco@mapfre.com.co asignado a Andrés Alfonso RINCON, iniciando el día el **19** de enero del 2022.

con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **Ciento sesenta y cinco (165)** ítems en condición de "eliminados" y se reconstruyeron **cero (0)** de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

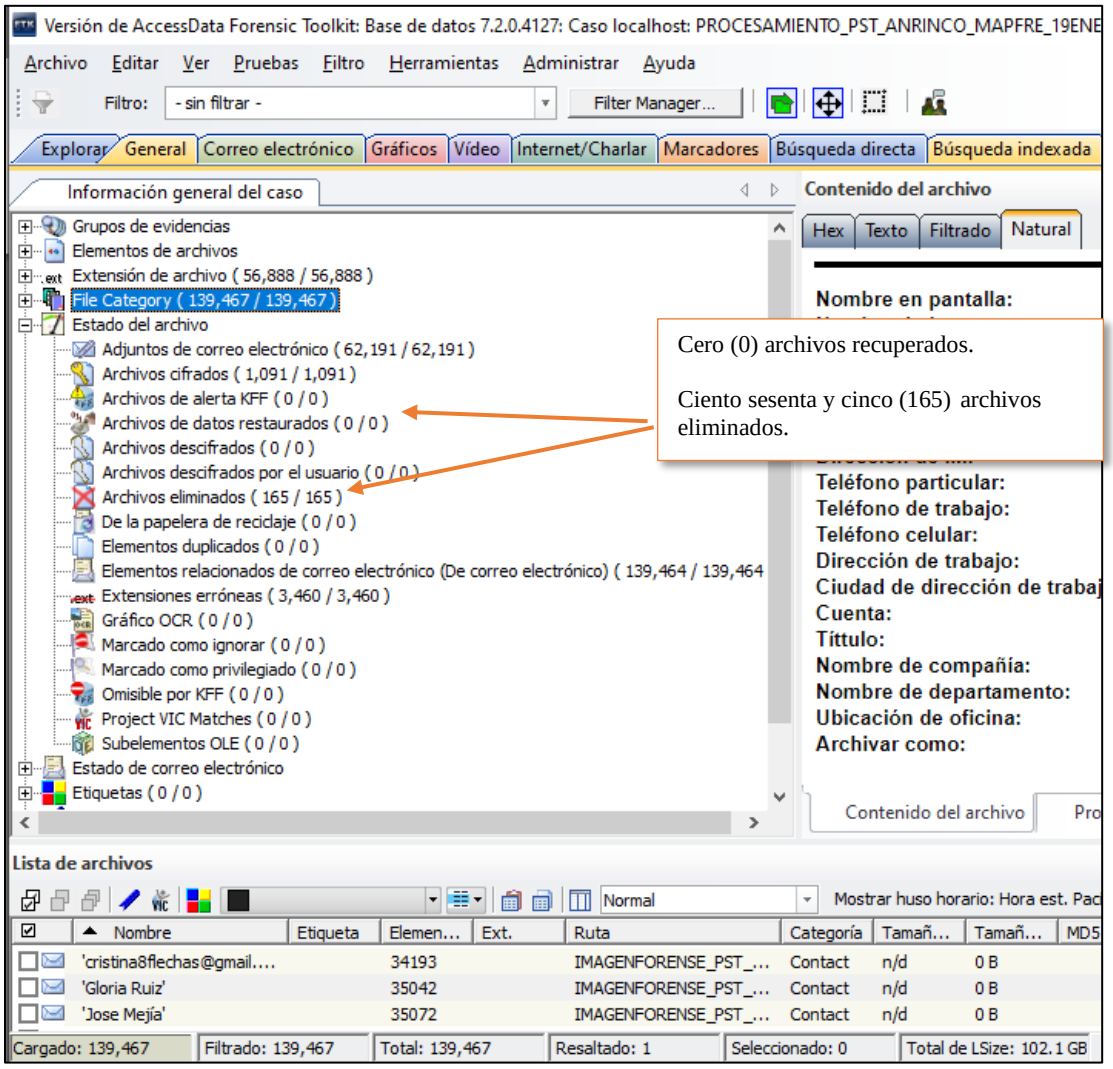


ilustración 205 Total de archivos recuperados en la cuenta de correo electrónico anrinco@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento treinta y nueve mil cuatrocientos sesenta y siete (139.467)**

archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ANRINCO@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico anrinco@mapfre.com.co asignado a **Andrés Alfonso RINCON** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1391
2	Bases de Datos	4
3	Documentos	29.152
4	Correo Electrónico	81.374
5	Ejecutables	5
6	Carpetas	1.283
7	Gráficos	832
8	archivos de internet/chat	1
9	Multimedia	68
10	Otros archivos encriptados	326
11	Otros archivos desconocidos	182
12	Presentaciones	497
13	Hojas de cálculo	24.181
14	Tipos de archivos desconocidos	171
TOTAL		**139.467**

Tabla 41 Información buscada evidencia 019_ANRINCO, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento treinta y nueve mil cuatrocientos sesenta y siete (139.467).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean

legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Sesenta y dos mil ciento noventa y un (62.191) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Mil noventa y un (1.091) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos Eliminados **Ciento sesenta y cinco (165) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento treinta y nueve mil cuatrocientos sesenta y cuatro (139.464) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Tres mil cuatrocientos sesenta (3.460) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico anrinco@mapfre.com.co asignado a **Andrés Alfonso RINCON** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



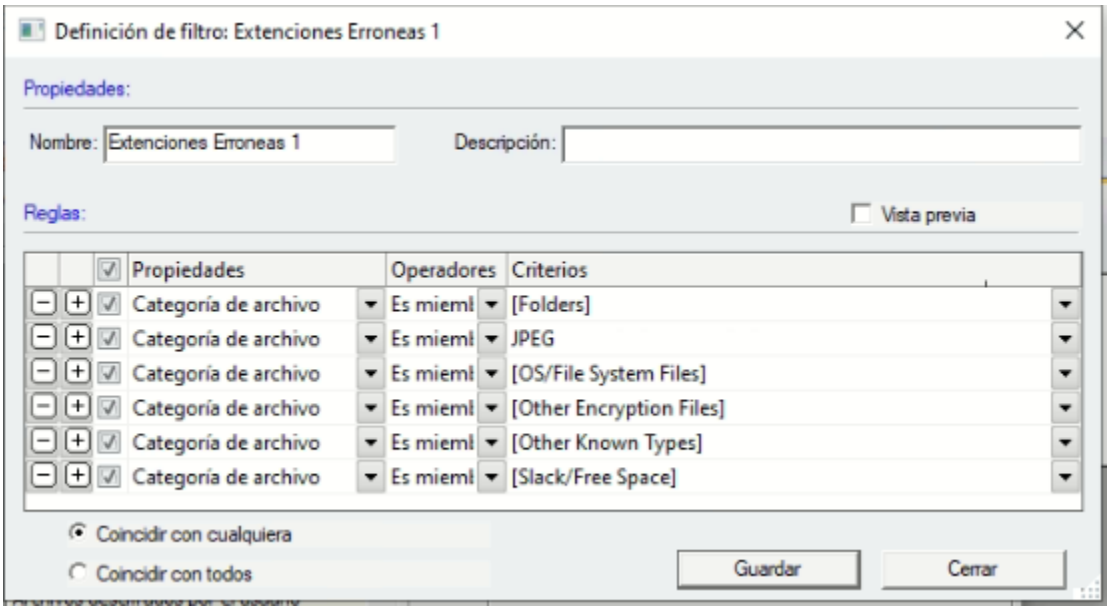


Ilustración 206 Filtro para excluir las extensiones erróneas.

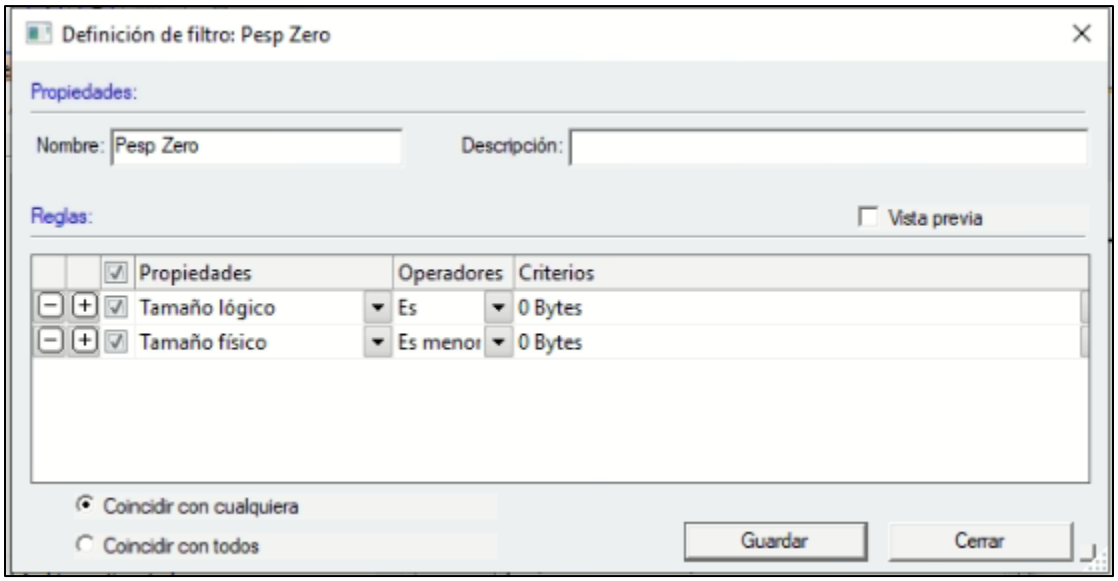


Ilustración 207 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

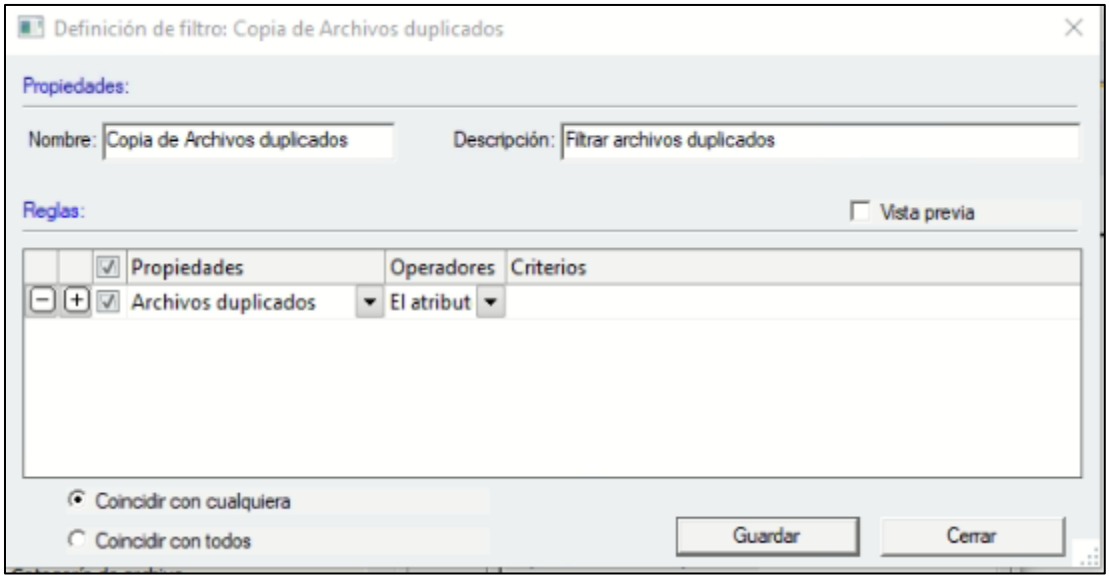


Ilustración 208 Filtro para excluir los archivos duplicados.

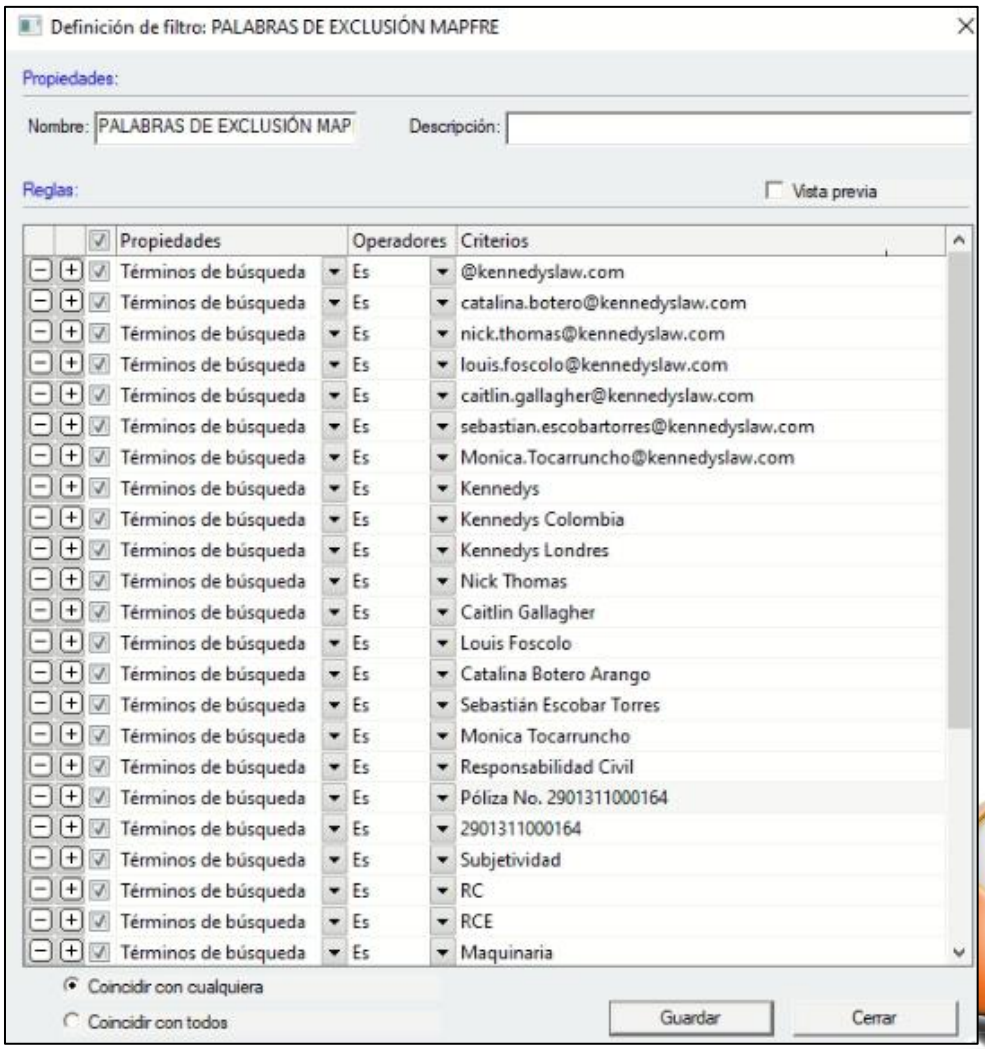


Ilustración 209 Filtro para excluir los archivos suministrado por MAPFRE - 1.

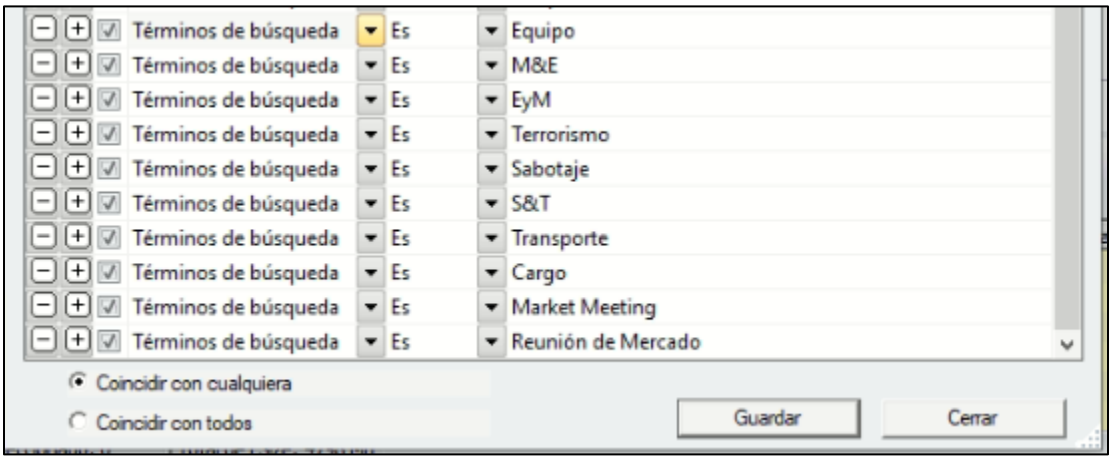
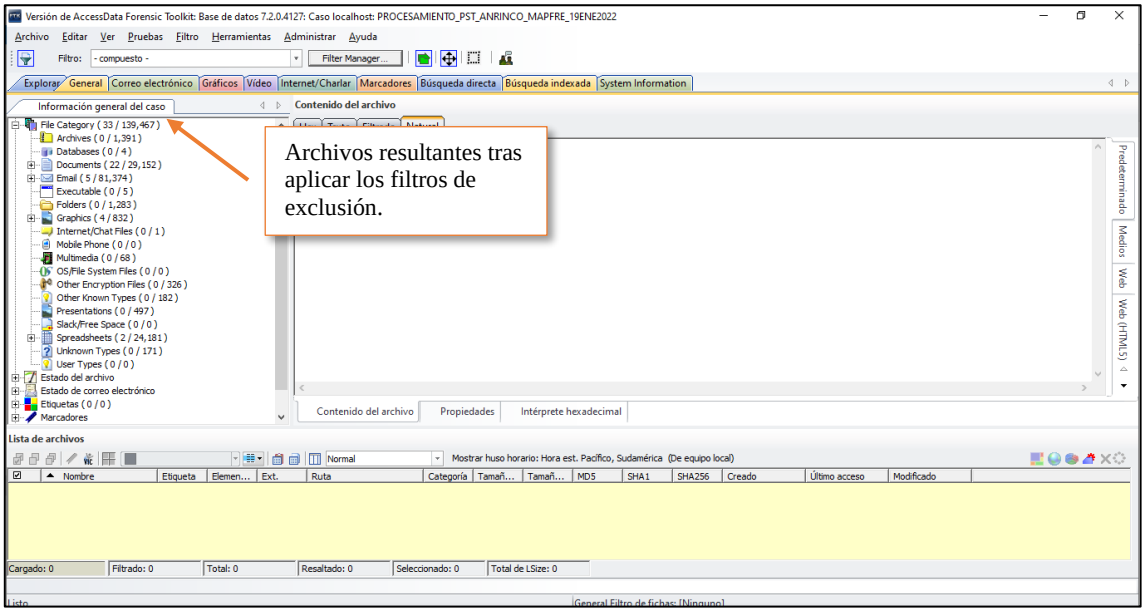


Ilustración 210 Filtro para excluir los archivos suministrado por MAPFRE - 2.

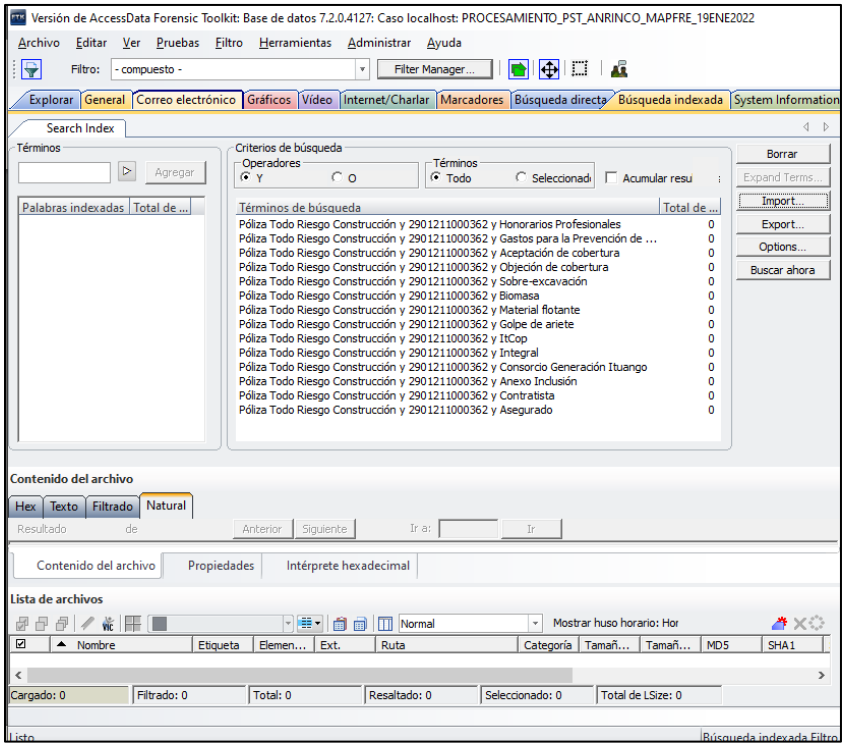
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Treinta y tres (33)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de anrinco@mapfre.com.co asignado a **Andrés Alfonso RINCON** para el desarrollo de sus funciones.

CONCLUSIONES.

- Se identificaron, adquirieron, recolectaron, preservaron y analizaron satisfactoriamente diez y nueve (19) imágenes forenses adquiridas dentro de las instalaciones de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**,., atendiendo a lo ordenado en el auto de fecha 8 de noviembre de 2021 por el juzgado 19 civil del circuito de Bogotá, dentro del proceso de prueba extraprocesal bajo el radicado número 11001310301920200033900, el cual se asegura en imagen forense para posterior procesamiento y aplicación de protocolo de gestión de evidencias aportado por MAPFRE para este proceso (palabras de inclusión y exclusión)., información toda puesta a disposición de los peritos designados por ADALID CORP, que fungieron como apoyo técnico-pericial a la diligencia ordenada por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**

- Tras realizar el filtrado de información para cada uno de los Diez y Nueve (19) buzones de correo entregados en las instalaciones de

MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., el equipo de ADALID CORP no identifico datos asociados posteriores.

- No se halló evidencia de fallas en la integridad de datos que impidan acceder a la información contenida en los dispositivos celulares ni a ninguno de sus archivos de registros de conversaciones.

- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **7d7787982808d7be0d6baf4f87b9505a** y SHA1 **1818a0e2013e2215acf8130a1f35002f72fc48de** para el buzón de correo de AVICTOR@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **5b6abdd3129e2330f3a46cc583d004a7** y SHA1 **70e7587e2b2fac10f3c58a029e552844a8aabf49** para el buzón de correo de ACLEMEN@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **326f16dbe95b854b5fdd979f1828ab88** y SHA1 **090832e206bf6c9540fcfdad2d7d1aa1a25b74a3** para el buzón de correo de JOSPAGA@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **25137b08f6c1fc4b57519ff976b5d139** y SHA1 **d20019fe0ad8526bbac422c7b8dd475f7225e8e0** para el buzón de correo de CTORRES@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **334e31abcf31639ee1a251289be3ac33** y SHA1 **b906341ba507626503910b9f85783c073d48a96d** para el buzón de correo de DAGOMEZ@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **36a5dc50b305d9a816109d85d035ede9** y SHA1 **8734e3612bd6e58f70e833fd1a991fe5b9178b4d** para el buzón de correo de LSUAREZ@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.

- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **d534e4492f211de5338af83951c38c46** y SHA1 **9d747d52eabeadd3571ddf2033cba1cc4c2c6bd7** para el buzón de correo de ANFERAM@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **f2b048976f511d39e5985af537222dea** y SHA1 **493d58bf1f54dcc30314162538921cf1b8ac853d** para el buzón de correo de MVIVIAN@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **82febeb311661f24839ced114ce64e7b** y SHA1 **47c4c084826f4119210640aa34aae4b32068e556** para el buzón de correo de JCTORR2@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **de6744c8bb0c6717f072120e5caaa982** y SHA1 **a37b029f544c9f91919cd44368238523600bb645** para el buzón de correo de JMRIANO@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **4ca2ff21652b030e18792d53572fc81a** y SHA1 **fdf3b09289d272e99375b5a141b0617ae789e477** para el buzón de correo de JMERINE@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **31383bb73ba2962329cfe4057918b2ff** y SHA1 **d937640697a74fe39a1dabfcfeb857c096bd6b16** para el buzón de correo de ACPARRA@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **ed3b9410edd6de02fe5e441ea43ddea2** y SHA1 **91fad8664b30c42450ea5e3d4eadc83dd516faa4** para el buzón de correo de CRUZJ@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5

a6426ce7f6ca0217569271fe149bf3d7 y SHA1 **3753a9577aa74a1f04b65a301238b025bf4fd805** para el buzón de correo de ETCUBID@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.

- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **73f2e7b307c8cbe24e68fd2cd5bec944** y SHA1 **515cd0f6c475cc973c9af008a7ea79b87126ef69** para el buzón de correo de MMALAGO@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **e1f945f3d80c3fc34ba37d6f39a9f07b** y SHA1 **a5f3f5fb0bb551475a8aa9e6b136d16d0f6c28e4** para el buzón de correo de GUEVECA@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **775edcc80edc04552a83d75e90da2aac** y SHA1 **fab4be9073e47a100aaedfcbec42de7fffa2443f** para el buzón de correo de ROCARRE@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **ec0267c1a3ffa7b40f2a9d9b6c1bbcc0** y SHA1 **b5e7ea4b96117e879d13928e2dc3da51aa6c4089** para el buzón de correo de CSALINA@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **b579effd896fb4f8c349e6490dc95a5f** y SHA1 **d608596c5fd7c32134969a1d9903f3a1ea837d62** para el buzón de correo de ANRINCO@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** A ADALID CORP.
- Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para los (19) Diez y nueve buzones de correo analizados.
- No se realizo la entrega de los siguientes buzones de correo indicando que estos no se encontraban en **COLOMBIA**.

BUZONES DE CORREO QUE NO VAN A SER ENTREGADOS DE PARTE DE MAPFRE (NO ESTÁN EN COLOMBIA)	
Nombre	**Correo electrónico**

BUZONES DE CORREO QUE NO VAN A SER ENTREGADOS DE PARTE DE MAPFRE (NO ESTÁN EN COLOMBIA)	
Luis Enrique Giraldo Durán	aquerol@mapfre.com
José Luis Cubero Rivera	jlcube@mapfre.com
Joaquín Alberto Solera	jalbertos@mapfre.com

- Se realizo el procesamiento, análisis, filtros de información y aplicación de palabras clave para los siguientes buzones de correo, lo anterior según el protocolo establecido por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** con los filtros y vectores allí establecidos.

BUZONES DE CORREO ENTREGADOS POR PARTE DE MAPFRE (PROCESADOS)		
No.	**NOMBRE**	**Correo electrónico**
1	VÍCTOR JONATHAN ARELLANO CARDONA	avictor@mapfre.com.co
2	DAVID GÓMEZ JIMÉNEZ	dagomez@mapfre.com.co
3	JOSÉ MAURICIO MALAGÓN ACOSTA	mmalago@mapfre.com.co
4	JOSÉ MANUEL RIAÑO	jmriano@mapfre.com.co
5	ANTONIO CLEMENTE CAMPANARIO	aclemen@mapfre.com.co
6	ETHEL CUBIDES	etcubid@mapfre.com.co
7	ANDRÉS FELIPE RAMÍREZ	anferam@mapfre.com.co
8	CLAUDIA ROCIO SALINASI	csalina@mapfre.com.co
9	JOSÉ MANUEL MERINERO MARTIN	jmerine@mapfre.com.co
10	CARMENZA GUATAVITA TORRES	ctorres@mapfre.com.co
11	ANDRÉS ALFONSO	anrinco@mapfre.com.co
12	CARLOS ALBERTO GUEVARA MORA	gueveca@mapfre.com.co
13	VIVIANA ROCÍO MOYANO	mvivian@mapfre.com
14	ANDRÉS CAMILO PARRA BALAGUERO	acparra@mapfre.com.co
15	JUAN CAMILO TORRES LOZANO	jctorr2@mapfre.com.co
16	LUIS ALBERTO SUÁREZ URREGO	lsuarez@mapfre.com.co
17	JORGE CRUZ AGUADO	cruzj@mapfre.com.co
18	RODRIGO CARREÑO HERNÁNDEZ	rocarre@mapfre.com.co
19	JOSÉ FERNANDO PALACIO GALLÓN	jospaga@mapfre.com.co

La totalidad de las imágenes forenses contenedoras de la totalidad de la evidencia digital asegurada queda en bóveda de seguridad en las instalaciones de ADALID CORP a disposición del **JUZGADO** y cualquier decisión sobre las mismas será atendida en el menor tiempo posible.

De esa forma se rinde el presente informe de laboratorio quedando atento a cualquier inquietud o duda al mismo.

Atentamente,

rma: 526d8ec8-5255-477b-941f-49d135918194

ID Firma: b250cada-49b2-4bcd-9f64-d3b494a6e1a3

Andrés GUZMÁN CABALLERO
CEO
ADALID Corp. S.A.S.
andres@adalid.com

Endrick Dann Axel DÍAZ ORTEGA
Abogado Perito en Informática Forense
ADALID Corp. S.A.S.
axel.diaz@adalid.com

Hector Dussan

ID Firma: 5bc72cbe-4c08-4f5d-b0ac-01de6993ee8d

Héctor Alberto DUSSAN MONTOYA
Ingeniero de Laboratorio
ADALID Corp. S.A.S.
hector.dussan@adalid.com

PERFILES PROFESIONALES

ADALID CORP S.A.S.

ADALID CORP S.A.S. es la única empresa de América Latina con un equipo forense de más de 200 profesionales de todo el mundo quienes son expertos en todas las ramas de la ciencia, cuenta con dos laboratorios propios completamente dotados y especializados en el análisis de acústica e informática forenses, útiles para la extracción segura de información, toma, certificación y análisis de evidencias digitales. ADALID Corp®. no es una agencia de contacto con peritos, es un equipo que da un gran valor agregado a cualquier prueba presentada en un proceso judicial. A través de la experiencia y amplia trayectoria de más de 10 años, ADALID ha sido reconocido por haber participado en tribunales arbitrales, procesos legales civiles, laborales, administrativos, penales, comerciales, de familia y policivos, asesorando a varias firmas de abogados, reconocidas empresas y clientes, tales como: Empresa de Licores de Cundinamarca, Legislación Económica S.A.S. Legis S.A.S, Tu Boleta, Busca pé Colombia, Mcr Entertainment, Comunicaciones Regionales de Colombia, Centro Comercial Plaza de las Américas, Teleone Colombia, Comregcol, Asociación Colombiana de Ingenieros de Sistemas, Seltika, Digiware, Grupo Porcelamika Inc, Universidad Libre de Colombia, Ministerio de Hacienda y Crédito Público, Dirección Nacional de Planeación, Ministerio de Comunicaciones, Certicamara, Procuraduría General de la Nación, Roldan, Y&R, entre otros.

HOJA DE VIDA ADALID CORP S.A.S:
https://adalid-my.sharepoint.com/:f:/p/comercial/Es-PpkL8y1JAqb9xYlVKSo0BtklTnc4CHyKoZI9sypRE6Q?e=RA9NBc

Andrés GUZMÁN CABALLERO
CEO

Abogado Experto en Nuevas Tecnologías Aplicadas al Derecho. Magister Executive en Administración de Empresas y Liderazgo Estratégico, Cybercrime and Electronic Evidence, Perito and honorem en evidencias digitales, Perito en casos de E-evidence y crimen informático, Especialización en Derecho Administrativo, Diplomado en Internet, Comercio electrónico y su regulación, Docente de Postgrados, director de la Maestría de Protección de Datos de la Universidad Sergio Arboleda.

Endrick Dann Axel DÍAZ ORTEGA
Perito en Informática Forense

Abogado con Major en Economía de la Universidad Sergio Arboleda, Especialista en Seguridad de la Información e Informática de la misma Universidad, AccessData Certified Examiner v6 y cursos en: Técnicas Antiforenses del Centro Internacional de Excelencia Sergio Arboleda (España), Computer Hacking Forensics Investigator V9 del EC-Council, Introduction to Cyber Security de Cisco Networking Academy, Blockchain – Creación de Contratos Inteligentes de la Universidad Nacional de Colombia y Lean Six Sigma (Yellow, Green y Black Belt) de la Universidad Sergio Arboleda, entre otros.

Cuenta con más de siete años de experiencia en asuntos de Pericias en Informática Forense, Protección de Datos Personales, Derecho al olvido, Derecho Informático, Propiedad Intelectual y Seguridad de la Información e Informática.

Héctor Alberto DUSSAN MONTOYA (ingeniero de laboratorio)

Perito en Informática Forense.

Ingeniero de sistemas de la UNIVERSIDAD FRANCISCO JOSÉ DE CALDAS, con más de (2) años de experiencia en Seguridad de Informática y asuntos relacionados con Informática Forense en el sector privado, cuenta con una certificación AccessData Certified Examiner v6 y cursos en: Introduction to Cyber Security de Cisco Networking Academy, Cybersecurity Essentials de Cisco Networking Academy.



GLOSARIO

Archivo:

Una colección de datos almacenados en un disco bajo un formato específico e identificado con un nombre y una extensión.

Asegurar:

Es el proceso en el que se preserva la integridad de las Pruebas Electrónicas. En esta etapa nos aseguramos de que no se rompa la cadena de custodia de las pruebas.

A partir de los medios originales se crea la imagen forense, es decir, una copia exacta bit a bit del medio original.

Desde este momento el examinador trabajará única y exclusivamente sobre la imagen forense.

Bit:

Unidad mínima de información cuyo valor puede ser cero o uno.

Byte:

Conjunto de 8 bits que suele representar el valor asignado a un carácter. Puede tomar valores entre 0 y 255.



Búsqueda por palabra clave:

Es una búsqueda de documentos que contienen una o más palabras que vienen especificadas por el usuario y cuyo objetivo es limitar el número de documentos que se deben revisar en busca de información relevante para un caso.

Cadena de custodia:

Es el conjunto de acciones, medidas logísticas y los actores partícipes que, fehacientemente registrados en un informe, garantizan la salvaguarda de la identidad e integridad de los medios digitales que van a ser analizados.

Computer Forensic:

El Computer Forensic es el proceso de identificar, asegurar, extraer y presentar pruebas que hayan sido generadas electrónicamente y guardadas en medios de almacenamiento digital con el objetivo de que sean aceptadas en un proceso judicial.

Datos activos:

Son los archivos y carpetas que residen en las unidades de almacenamiento de los sistemas informáticos y que son accesibles y visibles para los usuarios de una forma inmediata y directa a través de las herramientas propias del sistema operativo.

Datos borrados:

Los datos borrados son archivos o carpetas que existieron en el ordenador en el pasado como datos activos y que, posteriormente, han sido borrados por el sistema operativo o el usuario final. Los datos borrados permanecerán en la unidad de almacenamiento hasta que sean sobrescritos por otro archivo.

Datos recuperados:

Es el término que identifica las carpetas y/o archivos recuperados o reconstruidos que habían sido eliminados de la zona de datos activos. Estos archivos pueden ser recuperados con su formato y tamaño original o en pequeños fragmentos, que necesitarán una labor de reconstrucción forense.

Datos en zonas sin usar / sin asignar:

Datos que en la actualidad residen en zonas del disco que no pertenecen a ningún fichero. Son restos digitales de documentos que fueron eliminados.

Datos en zonas slack:

Debido a la necesidad del ordenador de asignar el espacio de disco en bloques de tamaño fijo, hay una zona al final de cada fichero que, a pesar de estar asignada al fichero en sí, contiene información que no pertenece al mismo. Esta zona se llama "slack" y contiene información del contenido

que hubo en ese bloque del disco antes de que se asignase al nuevo fichero.

Digitalizar:

Almacenar información electrónica como una cadena de "unos" y "ceros".

Debido a que tanto "ceros" como "unos" pueden ser fácilmente representados por dos niveles voltaicos en un medio electrónico, el sistema de numeración binario es ampliamente utilizado en el mundo informático digital.

Dirección IP:

Cadena de cuatro números separados por puntos que se utilizan para representar e identificar a un ordenador en Internet.
Los ISP asignan estas IP's automáticamente cuando nos conectamos a Internet.

Disco duro:

Disco de metal cubierto con una superficie de grabación ferro magnética. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.

DVD:

Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

Entorno virtual:

Es la simulación computacional de un entorno de trabajo formado por la interconexión de múltiples ordenadores, el cual permite el acceso a información digitalizada independientemente de la ubicación física donde ésta se encuentre.

Extensión de un archivo:

Etiqueta habitualmente de longitud 3, precedida por un punto que identifica el formato del archivo de datos o la aplicación utilizada para modificarlo.

Extraer:

Es el proceso en el que se revisa y analiza la información con el objetivo de extraer las pruebas. Al trabajar sobre la imagen forense y no directamente sobre el medio original, nos aseguramos de que se conserva la integridad de las pruebas mientras éstas son examinadas.

Hash:

Es un código calculado matemáticamente basándose en el contenido de un mensaje o archivo. Este código tiene la propiedad que se trata de un

valor específico para un mensaje o archivo, para así demostrar que no ha sido modificado. Si un mensaje u archivo se modificará, entonces su hash habría cambiado, y ya no coincidiría con el valor hash original.

HTML (Hypertext Markup Language):

Lenguaje usado para escribir documentos para servidores World Wide Web. Es una aplicación de la ISO Standard 8879:1986.

HTTP (Hypertext Transfer Protocol):

HTTP es un protocolo con la agilidad y velocidad necesaria para distribuir y manejar sistemas de información multimedia sobre Internet. Una característica de HTTP es la independencia en la visualización y representación de los datos, permitiendo a los sistemas ser construidos independientemente del desarrollo de nuevos avances en la representación de los datos.

HTTPS:

Protocolo http seguro. Sus dos principales características son el cifrado y la autenticación.

Mediante el cifrado, ocultamos el contenido de las comunicaciones con el servidor a la vista de terceros. La autenticación permite a los usuarios saber que el servidor es quien dice ser a través del uso de certificados firmados por Autoridades de Certificación.
Identificar:



El proceso de identificación implica analizar dónde y cómo han sido creadas y almacenadas las pruebas y en qué sistema o sistemas residen.

A partir de esta información el investigador será capaz de seleccionar los métodos de recuperación más adecuados y qué herramientas deberán ser utilizadas para capturar los medios involucrados de una forma segura.

Imagen forense:

Es una copia exacta (bit a bit) de la unidad de almacenamiento de un sistema informático utilizada en una investigación forense.

Ingeniería Inversa:

Consiste en el análisis del código binario de un programa o aplicación para determinar su comportamiento real.

Internet:

Red global de datos basada en los protocolos TCP/IP que se utiliza para interconectar ordenadores y como medio de transporte de diversos servicios, siendo los más populares los servicios de e-mail, www y ftp.

ISP (Internet Service Provider):

Organización que provee la conexión de ordenadores a Internet, ya sea por líneas dedicadas o por líneas conmutadas. Es una entidad, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas físicas y/o jurídicas, puede ofrecerles una serie de servicios

(hospedaje de páginas web, consultoría de diseño, implantación de webs e Intranets, etc.).

Log:

Registro de determinados eventos generados por el sistema operativo, o por una aplicación, sobre un período de tiempo dado. Pueden ser utilizados por auditores externos para registrar/reconstruir el uso de un ordenador o aplicación.

Malware:

Término genérico usado para abarcar al software malicioso incluyendo: adware, troyanos, browser hijackers, keyloggers, dialers, tracking cookies, entre otros.

MD5:

Es un tipo de Hash que sirve para dar seguridad de que un archivo no se ha alterado, La codificación del MD5 es de 128 bits y es representada como un número de 32 dígitos hexadecimales.

Metadatos:

Los metadatos son información sobre un conjunto de archivos y/o carpetas que pueden describir, por ejemplo, cómo, cuándo y por quién ha sido creado, recibido, accedido y/o modificado. Estos datos se utilizan en Computer Forensic para reconstruir la cadena de acontecimientos asociada al fichero analizado.

Dependiendo del contexto en el que se emplee el término, se hace referencia a unos o a otros datos.

Presentar:

Es la etapa final del proceso en la que se presentan las pruebas de forma comprensible a interlocutores que no necesariamente tengan conocimientos de informática.

Durante esta etapa, se vinculan las pruebas digitales con el resto de las pruebas que componen el caso para reforzar al máximo la estrategia legal planteada.

Prueba Electrónica:

Información almacenada o transmitida en formato digital aceptada en un proceso judicial. Es necesario obtener la información siguiendo unos procedimientos muy concretos con personal especializado y operando dentro de un marco legal adecuado para garantizar que las pruebas sean aceptadas en juicio.

Rastros digitales:

Los rastros digitales son huellas electrónicas que vamos dejando al utilizar servicios informáticos o de comunicaciones.



RAW:

El formato RAW, cuya traducción literal del inglés al español significa: crudo, es un formato de archivos digitales, que contiene la totalidad de los datos desde el primer bit hasta el último bit del medio de almacenamiento al cual se le hace la copia, este formato no es compreso.

Router:

Elemento que determina la trayectoria o transferencia más eficiente de datos entre dos segmentos de la red. Opera mediante el uso de tablas y protocolos de enrutamiento.

Screenshot:

Es una captura de pantalla o también llamado: "pantallazo", es una imagen capturada por un equipo de cómputo, para registrar o documentar, los elementos visibles en el monitor u otro dispositivo de salida visual.

SHA1:

Es un tipo de Hash que sirve para dar seguridad de que un archivo no se ha alterado, La codificación del SHA1 es de 160 bits y es representada como un número de 40 dígitos hexadecimales.

Spam:



Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico.

Spoofing:

Procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente con el fin de engañar a un firewall.

TCP / IP Transmission Control Protocol / Internet Protocol:

Conjunto de protocolos que definen las reglas básicas de comunicación entre ordenadores dentro de Internet.

Troyano:

Es un tipo de software malicioso o spyware (también son conocidos como caballos de Troya) pueden ingresar al sistema, instalarse y ejecutarse sin el conocimiento del usuario, son capaces de realizar una gran variedad de tareas, entre las más conocidas: abrir puertos para futuros ingresos sin autorización, robar datos sensibles financieros, bancarios o personales; una particularidad y diferencia con otros tipos de Malware, es que no pueden replicarse ellos mismos.

Virus:

Programa que puede infectar otros programas, modificándolos para incluir una copia de sí mismo. Los virus tienen básicamente la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta

realizar daños importantes en los sistemas. Este tipo de programas pueden actuar de diversas maneras:

a) Solamente advertir al usuario de su presencia, sin causar daño aparente.
b) Tratar de pasar desapercibidos para causar el mayor daño posible.
c) Adueñarse de las funciones principales (infectar los archivos de sistema).

Virus de Macro:

Es la última presentación de los virus. Viajan en archivos de aplicación (Word, Excel, etc.) y no en archivos binarios (como lo hacen los virus tradicionales). Se ejecutan al abrir el fichero de datos que los contiene.

Virus en correo electrónico:

Los virus no pueden viajar en mensajes de correo electrónico, ya que únicamente utilizan el formato de 7 bits para transferir texto. La única manera en que pueden viajar es por archivos binarios que se envían mediante un anexo (attachment) al mensaje de texto. Es recomendable revisar estos archivos con un antivirus antes de su lectura.

Warez:

Copias piratas de los programas. Versiones de software protegido a las que se ha retirado fraudulentamente la protección.

WWW (World Wide Web):



Es el conjunto de todos los ordenadores que están conectados en red y que forman lo que se conoce como Internet.



EN CUMPLIMIENTO AL ARTÍCULO 226 Y SS DEL CGP

1. **La identidad de quien rinde el dictamen y de quien participó en su elaboración.**

ADALID CORP S.A.S. Nit. 900.095.522-5, en su nombre Endrick Dann Axel DÍAZ ORTEGA identificado con cédula de ciudadanía No. 1.016.036.658 y Héctor Alberto DUSSAN MONTOYA identificado con cédula de ciudadanía 1.026.260.827 de Bogotá.

2. **La dirección, el número de teléfono, número de identificación y los demás datos que faciliten la localización del perito.**

Dirección: Calle 70A # 11 – 28 Barrio Quinta Camacho, Bogotá D.C., Colombia
Teléfonos: +57 (1) 7432015, +57 3173677051.
Contacto: info@adalid.com
Web: www.adalid.com

3. **La profesión, oficio, arte o actividad especial ejercida por quien rinde el dictamen y de quien participó en su elaboración. Deberán anexarse los documentos idóneos que lo habilitan para su ejercicio, los títulos académicos y los documentos que certifiquen la respectiva experiencia profesional, técnica o artística.**



ADALID CORP S.A.S.

ADALID CORP S.A.S. es la única empresa de América Latina con un equipo forense de más de 200 profesionales de todo el mundo quienes son expertos en todas las ramas de la ciencia, cuenta con dos laboratorios propios completamente dotados y especializados en el análisis de acústica e informática forenses, útiles para la extracción segura de información, toma, certificación y análisis de evidencias digitales. ADALID Corp®. no es una agencia de contacto con peritos, es un equipo que da un gran valor agregado a cualquier prueba presentada en un proceso judicial. A través de la experiencia y amplia trayectoria de más de 10 años, ADALID ha sido reconocido por haber participado en tribunales arbitrales, procesos legales civiles, laborales, administrativos, penales, comerciales, de familia y policivos, asesorando a varias firmas de abogados, reconocidas empresas y clientes, tales como: Empresa de Licores de Cundinamarca, Legislación Económica S.A.S. Legis S.A.S, Tu Boleta, Busca pé Colombia, Mcr Entertainment, Comunicaciones Regionales de Colombia, Centro Comercial Plaza de las Américas, Teleone Colombia, Comregcol, Asociación Colombiana de Ingenieros de Sistemas, Seltika, Digiware, Grupo Porcelamika Inc, Universidad Libre de Colombia, Ministerio de Hacienda y Crédito Público, Dirección Nacional de Planeación, Ministerio de Comunicaciones, Certicamara, Procuraduría General de la Nación, Roldan, Y&R, entre otros.

Andrés GUZMÁN CABALLERO
CEO

Abogado Experto en Nuevas Tecnologías Aplicadas al Derecho. Magister Executive en Administración de Empresas y Liderazgo Estratégico, Cybercrime and Electronic Evidence, Perito ad honorem en evidencias digitales, Perito en casos de E-evidence y crimen informático, Especialización en Derecho Administrativo, Diplomado en Internet, Comercio electrónico y su regulación, Docente de Postgrados, director de la Maestría de Protección de Datos de la Universidad Sergio Arboleda.

Endrick Dann Axel DÍAZ ORTEGA
Perito en Informática Forense

Abogado con Major en Economía de la Universidad Sergio Arboleda, Especialista en Seguridad de la Información e Informática de la misma Universidad, AccessData Certified Examiner v6 y cursos en: Técnicas Antiforenses del Centro Internacional de Excelencia Sergio Arboleda (España), Computer Hacking Forensics Investigator V9 del EC-Council, Introduction to Cyber Security de Cisco Networking Academy, Blockchain – Creación de Contratos Inteligentes de la Universidad Nacional de Colombia y Lean Six Sigma (Yellow, Green y Black Belt) de la Universidad Sergio Arboleda, entre otros.

Cuenta con más de siete años de experiencia en asuntos de Pericias en Informática Forense, Protección de Datos Personales, Derecho al olvido, Derecho Informático, Propiedad Intelectual y Seguridad de la Información e Informática.

Héctor Alberto DUSSAN MONTOYA (ingeniero de laboratorio)

Perito en Informática Forense.

Ingeniero de sistemas de la Universidad Francisco José de Caldas, con más de (1) año de experiencia en Seguridad de Informática y asuntos relacionados con Informática Forense en el sector privado, cuenta con una certificación AccessData Certified Examiner v6 y cursos en: Introduction to Cyber Security de Cisco Networking Academy, Cybersecurity Essentials de Cisco Networking Academy.

4. **La lista de publicaciones, relacionadas con la materia del peritaje, que el perito haya realizado en los últimos diez (10) años, si las hubiere.**

   ADALID CORP S.A.S., al encontrarse legalmente constituida como persona jurídica no ha escrito bajo su autoría ningún tipo de publicación relacionada a los peritajes realizados por la misma en los últimos diez (10) años.

5. **Lista de casos en los que haya sido designado como perito o en los que haya participado en la elaboración de un dictamen pericial en los últimos cuatro (4) años.**

   ADALID CORP S.A.S., relaciona mediante Registro Único de Proponentes su experiencia en los procesos en los que ha sido designado como perito informático para la elaboración de dictámenes periciales.

REGISTRO ÚNICO DE PROPONENTES: https://adalid-my.sharepoint.com/:f:/p/comercial/EpTNFqPs5mRPj5f-SZ8sF3oBRpdreXDUaW4UDaita9fK9w?e=culY3u

6. **Si ha sido designado en procesos anteriores o en curso por la misma parte o por el mismo apoderado de la parte, indicando el objeto del dictamen.**

ADALID CORP. S.A.S. ha sido designada como perito en procesos anteriores por el apoderado DR. Sergio ROJAS para el dictamen informático del tribunal de arbitramento de **C.I. IBLU V. EPK KIDS SMART** para el año 2020**;** a su vez la firma **DLA PIPER MARTÍNEZ BELTRÁN** designó a ADALID CORP. S.A.S. para el proceso de **EDEMSA V. EDEMCO** para el año 2020**.**

El objeto del dictamen, en ambos casos, es una pericia informática sobre diferentes piezas digitales.

7. **Si se encuentra incurso en las causales contenidas en el artículo 50, en lo pertinente.**

Manifiesto con las solemnidades pertinentes que no me encuentro incurso en ninguna de las once (11) causales descritas y numeradas en el artículo 50 de la Ley 1564 de 2012, relacionadas con la exclusión de la lista de los auxiliares de la justicia; que aplican en mi oficio como perito particular.

8. **Declarar si los exámenes, métodos, experimentos e investigaciones efectuados son diferentes respecto de los que ha utilizado en peritajes rendidos en anteriores procesos que versen sobre las mismas materias. En caso de que sea diferente, deberá explicar la justificación de la variación.**

Declaro con las solemnidades necesarias que todos los métodos y/o procedimientos, inequívocamente adelantados, en el desarrollo de esta pericia obedecen a aquellos que regularmente se aplican y que aconsejan los más altos estándares nacionales e internacionales en la materia (particularmente los estándar ISO/IEC 27037:2012 e ISO/IEC 27042:2015), en consecuencia, no existe variación alguna que deba ser justificada.

9. **Declarar si los exámenes, métodos, experimentos e investigaciones efectuados son diferentes respecto de aquellos que utiliza en el ejercicio regular de su profesión u oficio. En caso de que sea diferente, deberá explicar la justificación de la variación.**

Declaro con las solemnidades necesarias que todos los métodos y/o procedimientos, inequívocamente adelantados, en el desarrollo de esta pericia obedecen a aquellos que regularmente aplico en el ejercicio de mi profesión como experto en informática forense, de acuerdo con los estándares ISO/IEC 27037:2012 e ISO/IEC 27042:2015, en consecuencia, no existe variación alguna que deba ser justificada.

10. **Relacionar y adjuntar los documentos e información utilizados para la elaboración del dictamen.**

El informe que relaciona las herramientas lógicas y físicas empleadas en la pericia, así como cualquier activo de información que deba hacer parte de este proceso técnico, se encuentra debidamente referenciado y/o adjunto al interior del informe final número **F-22-11306-ADO** de fecha 28 de febrero de 2022, atendiendo a una secuencia y metodología pertinentes debidamente explicadas y enuncia.

Trámite 2020-00339-00 / Integral S.A. y otro v. Mapfre Seguros Generales de Colombia S.A. [KEN-Legal.FID3044319]

Sergio Rojas <srojas@dlapipermb.com>

Vie 01/04/2022 11:51

Para: Juzgado 19 Civil Circuito - Bogota - Bogota D.C. <ccto19bt@cendoj.ramajudicial.gov.co>

CC: Daniel Andrés Samacá <dasamaca@dlapipermb.com>;alerive@mapfre.com.co <alerive@mapfre.com.co>;ETHEL CUBIDES <ETCUBID@mapfre.com.co>;Catalina Botero <Catalina.Botero@kennedyslaw.com>;Sebastian Escobar Torres <sebastian.escobartorres@kennedyslaw.com>;monica.tocarruncho <monica.tocarruncho@kennedyslaw.com>

Bogotá, D.C., marzo de 2022

Señora,
JUEZ 19 CIVIL DEL CIRCUITO DE BOGOTÁ
ATN. DRA. ALBA LUCÍA GOYENECHE GUEVARA
E. S. D.

REF.	**Solicitantes:**	INTEGRAL S.A. y OTRO
	Solicitado:	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.
	Radicado:	**2020-00339**
	Asunto:	**Aporta dictamen informático**

El suscrito, **SERGIO ROJAS QUIÑONES**, mayor de edad, con domicilio en la ciudad de Bogotá D.C., identificado como aparece al pie de mi firma, actuando en mi condición de apoderado de **INTEGRAL S.A.** y del **CONSORCIO GENERACIÓN ITUANGO**, acudo respetuosamente ante el Despacho a fin de aportar el dictamen pericial informático dentro del trámite de la referencia.

Atentamente,

SERGIO ROJAS QUIÑONES

ADALID
Security, Legal & Forensic Corporation

ACTA DE DILIGENCIA TÉCNICA DE ASEGURAMIENTO DE INFORMACIÓN DIGITAL

FECHA:	16 de noviembre del año 2021
HORA INICIO:	14:00 horas
QUIEN ATIENDE LA DILIGENCIA:	Sebastián ESCOBAR TORRES C.C. No. 1.018.466.417 Willigton Leandro TORRES MORALES C.C. No. 79.708.420 Alexandra RIVERA CRUZ C.C. No. 51.849.114 Bayrón PRIETO CASTELLANOS C.C. No. 80.075.270
CARGO:	-APODERADO ESPECIAL -PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN -JEFE JURIDICO -ASESOR
LUGAR:	MAPFRE Colombia, Carrera 14 No. 96 – 34, Edificio MAPFRE SEGUROS, Auditorio sala 1, en la ciudad de Bogotá, D.C.
OBJETIVO:	Realizar la inspección, aseguramiento y análisis de información contenida en los buzones de correos electrónicos de funcionarios y exfuncionarios de MAPFRE SEGUROS GENERALES DE COLOMBIA S.A, Sebastián ESCOBAR TORRES atendiendo a lo ordenado en el auto de fecha 8 de noviembre de 2021 por el juzgado 19 civil del circuito de Bogotá, dentro del proceso de prueba extraprocesal bajo el radicado número 11001310301920200033900, el cual se asegura en imagen forense para posterior procesamiento y aplicación de protocolo de gestión de evidencias aportado por MAPFRE para este proceso (palabras de inclusión y exclusión).

DESARROLLO

En la ciudad de Bogotá D.C., Colombia el día 16 de noviembre del año 2021, siendo las 14:00 horas, en cumplimiento a lo requerido por **INTEGRAL S.A y CONSORCIO GENERACION ITUANGO**, se reúnen en la Carrera 14 No. 96 – 34, Edificio MAPFRE SEGUROS, Auditorio sala 1, en la ciudad de Bogotá, D.C. - Colombia., los funcionarios de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**, **Sebastián ESCOBAR TORRES,** identificado con cédula de ciudadanía **No. 1.018.466.417** de Bogotá quien funge como **APODERADO ESPECIAL**, **Willigton Leandro TORRES MORALES,** identificado con cédula de ciudadanía **No. 79.708.420** de Bogotá, quien funge como **PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN, Alexandra RIVERA CRUZ,** identificado con cédula de ciudadanía **No. 51.849.114** de Bogotá, quien funge como **JEFE JURIDICO, Bayrón PRIETO CASTELLANOS,** identificado con cédula de ciudadanía **No. 80.075.270** de Bogotá, quien funge como **ASESOR** y los peritos en informática forense asignados por ADALID CORP S.A.S., **Endrick Dann Axel DÍAZ ORTEGA** identificado con cédula de ciudadanía **No. 1.016.036.658** y **Héctor Alberto DUSSAN MONTOYA** identificado con cédula de ciudadanía **No. 1.026.260.827** lo anterior, con el fin de realizar la inspección, aseguramiento y análisis de información contenida en los correos electrónicos de funcionarios y exfuncionarios de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A,** atendiendo a lo ordenado en el auto de fecha 8 de noviembre de 2021 por el juzgado 19 civil del circuito de Bogotá, dentro del proceso de prueba extraprocesal bajo el radicado número 11001310301920200033900, el cual se asegura en imágenes forenses para su posterior procesamiento y aplicación de protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**. para este proceso (palabras de inclusión y exclusión).

A continuación, se presentan los buzones de correo objeto de análisis:

- avictor@mapfre.com.co
- dagomez@mapfre.com.co
- mmalago@mapfre.com.co
- jmriano@mapfre.com.co
- aclemen@mapfre.com.co
- etcubid@mapfre.com.co
- jalbertos@mapfre.com
- anferam@mapfre.com.co
- jlcube@mapfre.com
- aquerol@mapfre.com
- csalina@mapfre.com.co
- jmerine@mapfre.com.co

- ctorres@mapfre.com.co
- anrinco@mapfre.com.co
- gueveca@mapfre.com.co
- mvivian@mapfre.com
- acparra@mapfre.com.co
- jctorr2@mapfre.com.co
- lsuarez@mapfre.com.co
- cruzj@mapfre.com.co
- rocarre@mapfre.com.co
- jospaga@mapfre.com.co

La sesión inicio a las 14:20 en donde por parte de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** se puso en conocimiento a los peritos de ADALID CORP. sobre el contenido del acuerdo de confidencialidad propuesto por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** para efectos de la practica probatoria.

Luego de leer el contenido del acuerdo de confidencialidad propuesto por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** el equipo de ADALID CORP. procede a realizar la firma del documento por medio de la página de internet https://app.mifirma.co/ .

Una vez revisado y firmado el Acuerdo de confidencialidad, el señor **Willigton Leandro TORRES MORALES** hace entrega a los peritos de ADALID CORP. de (1) Un disco duro color blanco, con capacidad de almacenamiento de **1000GB,** el cual, a través del software **CrystalDiskInfo** en su versión **8.12.12** se logra identificar su número serial "**WN911W3Z",** en su parte superior se encuentra marcado como **"prueba extraprocesal".** La información contenida en el disco duro, así como sus características y de más información se puede visualizar en las siguientes imágenes:

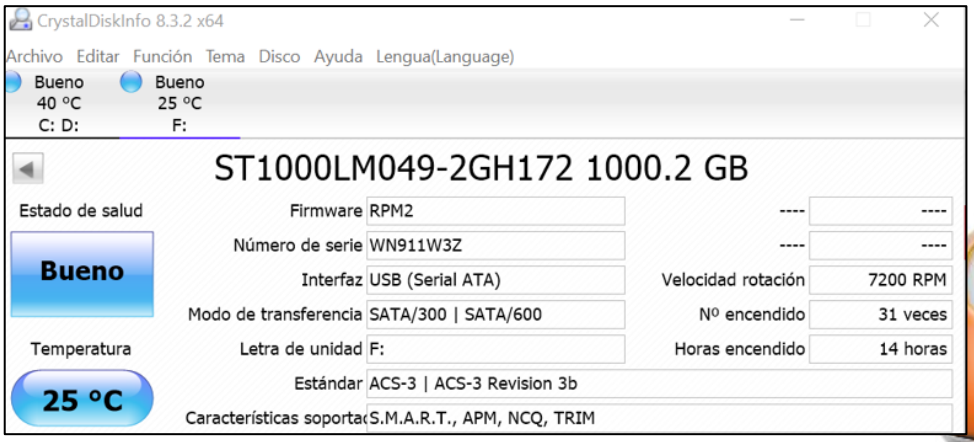


Ilustración 1 Características del Disco Duro entregado por MAPFRE SEGUROS GENERALES DE COLOMBIA S. Desde el aplicativo CrystalDiskInfo.

	
Fotografía Disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista superior)	Fotografía disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista posterior)

Dentro del Disco Duro se encuentran los archivos en formato .PST de las cuentas de correo electrónico asignadas a los funcionarios que se encuentran retirados de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**, los cuales serán mencionados a continuación:

Nombre	Fecha de modificación	Tipo
ACLEMEN	3/11/2021 4:19 p. m.	Carpeta de archivos
ANFERAM	28/10/2021 10:52 a. m.	Carpeta de archivos
AVICTOR	28/10/2021 9:14 a. m.	Carpeta de archivos
CTORRES	16/11/2021 11:28 a. m.	Carpeta de archivos
DAGOMEZ	28/10/2021 11:13 a. m.	Carpeta de archivos
JCTORR2	28/10/2021 9:42 a. m.	Carpeta de archivos
JMERINE	28/10/2021 9:32 a. m.	Carpeta de archivos
JMRIANO	16/11/2021 8:25 a. m.	Carpeta de archivos
JOSPAGA	28/10/2021 11:03 a. m.	Carpeta de archivos
LSUAREZ	28/10/2021 11:18 a. m.	Carpeta de archivos
MVIVIAN	28/10/2021 9:52 a. m.	Carpeta de archivos

Ilustración 2 Visualización contenido del Disco Duro entregado por MAPFRE SEGUROS GENERALES DE COLOMBIA S.A

ID	CORREOS FUNCIONARIOS RETIRADOS	REALIZACIÓN IMAGEN FORENSES	TAMAÑO GB
1	avictor@mapfre.com.co	1 – 17NOV2021	380 MB
2	aclemen@mapfre.com.co	2 – 17NOV2021	42.6 GB
3	jospaga@mapfre.com.co	3 – 18NOV2021	4.49 GB
4	ctorres@mapfre.com.co	4 – 18NOV2021	17.7 GB
5	dagomez@mapfre.com.co	5 – 19NOV2021	28.8 GB
6	lsuarez@mapfre.com.co	6 – 19NOV2021	45.8 GB
7	anferam@mapfre.com.co	7 – 19NOV2021	52.3 GB
8	mvivian@mapfre.com	8 – 19NOV2021	57 GB
9	jctorr2@mapfre.com.co	9 – 22NOV2021	59.3 GB
10	jmriano@mapfre.com.co	10 – 22NOV2021	115 GB
11	jmerine@mapfre.com.co	11 – 22NOV2021	118 GB

Tabla 1 Correos electrónicos de funcionarios retirados MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.

Todo esto con el fin de realizar una revisión preliminar de los archivos contenidos en el disco duro entregado por el señor **Willigton Leandro TORRES MORALES** en formato .PST los cuales se identifican en la **ilustración 2** anteriormente mostrada. Al realizar la revisión de la información contenida en el disco duro, el personal de **MAPFRE SEGUROS GENERALES DE COLOMBIA S. A** informa al equipo de **ADALID CORP**. que los buzones de correo en formato .PST contenidos en el disco duro pertenecen a funcionarios retirados de la empresa **MAPFRE SEGUROS GENERALES DE COLOMBIA S. A**.

De igual manera, el personal de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** le indica al equipo de **ADALID CORP.** que los correos electrónicos faltantes de los trabajadores de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** que aún se encuentran activos dentro de la compañía serán exportados y entregados en el orden que se solicite uno a uno luego de finalizar con la realización de las imágenes forense de los correos del personal retirado, los cuales fueron entregados en el disco duro antes mencionado. Una vez finalizados los anteriores procedimientos, los peritos de ADALID CORP. S.A.S. proceden de manera final a regresar el disco duro al señor **Willigton Leandro TORRES MORALES** el día 16 de noviembre de 2021.

El día 17 de noviembre de 2021 se inicia la diligencia siendo las 9:00 a.m., para este objeto, el señor **Willigton Leandro TORRES MORALES** encargado de la presente diligencia y quien funge como **Profesional De Seguridad De La Información**, hace entrega a los peritos designados por ADALID CORP. S.A.S. de (1) Un Disco Duro color **BLANCO**, identificado su número serial **WN911W3Z,** con capacidad de almacenamiento de **1000GB**, el cual se encentra marcado con en su parte superior con las palabras **"prueba extraprocesal HTGO"** con el propósito de que el equipo de ADALID CORP realice la preservación y aseguramiento para cada una de los buzones de correo electrónico allí contenidos:

De conformidad con lo mencionado anteriormente se explican los procedimientos y procesos que se realizaran para cada uno de los buzones de correo suministrados por **MAPFRE SEGUROS GENERALES DE COLOMBIA S. A.:**

1. Se realiza una imagen forense contentiva del buzón de correo electrónico.
2. Se procesa la información en la herramienta FTK 7.2.
3. Se realizan los siguientes filtros de información en la opción de búsqueda indexada de la herramienta FTK 7.2, tomando como referencia el protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Tabla 2 *Filtros aplicados al procesamiento de los buzones de correo.*

4. Tras la aplicación de cada uno de los filtros de información a través de la opción de búsqueda indexada en el software de Informática Forense FTK, si este genera resultados asociados a la búsqueda de las palabras clave previamente establecidas, se le aplicarán el siguiente comando de exclusión de información, solicitado por **MAPFRE** como se presenta a continuación, en garantía de su información y lo autorizado por el Juzgado 19 Civil del Circuito de Bogotá:

<?xml version="1.0" encoding="UTF-8"?>
<exportedFilter xmlns="http://www.accessdata.com/ftk2/filters"><filter name="PALABRAS DE EXCLUSIÓN MAPFRE" matchCriterion="any" id="f_1000001" read_only="false" description=""><rule position="0" enabled="true" id="a_9429" operator="is"><one_string value="@kennedyslaw.com"/></rule><rule position="1" enabled="true" id="a_9429" operator="is"><one_string value="catalina.botero@kennedyslaw.com"/></rule><rule position="2" enabled="true" id="a_9429" operator="is"><one_string value="nick.thomas@kennedyslaw.com"/></rule><rule position="3" enabled="true" id="a_9429" operator="is"><one_string value="louis.foscolo@kennedyslaw.com"/></rule><rule position="4" enabled="true" id="a_9429" operator="is"><one_string value="caitlin.gallagher@kennedyslaw.com"/></rule><rule position="5" enabled="true" id="a_9429" operator="is"><one_string value="sebastian.escobartorres@kennedyslaw.com"/></rule><rule position="6" enabled="true" id="a_9429" operator="is"><one_string value="Monica.Tocarruncho@kennedyslaw.com"/></rule><rule position="7" enabled="true" id="a_9429" operator="is"><one_string value="Kennedys"/></rule><rule position="8" enabled="true" id="a_9429" operator="is"><one_string value="Kennedys Colombia"/></rule><rule position="9" enabled="true" id="a_9429" operator="is"><one_string value="Kennedys Londres"/></rule><rule position="10" enabled="true"

id="a_9429" operator="is"><one_string value="Nick Thomas"/></rule><rule position="11" enabled="true" id="a_9429" operator="is"><one_string value="Caitlin Gallagher"/></rule><rule position="12" enabled="true" id="a_9429" operator="is"><one_string value="Louis Foscolo"/></rule><rule position="13" enabled="true" id="a_9429" operator="is"><one_string value="Catalina Botero Arango"/></rule><rule position="14" enabled="true" id="a_9429" operator="is"><one_string value="Sebastián Escobar Torres"/></rule><rule position="15" enabled="true" id="a_9429" operator="is"><one_string value="Monica Tocarruncho"/></rule><rule position="16" enabled="true" id="a_9429" operator="is"><one_string value="Responsabilidad Civil"/></rule><rule position="17" enabled="true" id="a_9429" operator="is"><one_string value="Póliza No. 2901311000164"/></rule><rule position="18" enabled="true" id="a_9429" operator="is"><one_string value="2901311000164"/></rule><rule position="19" enabled="true" id="a_9429" operator="is"><one_string value="Subjetividad"/></rule><rule position="20" enabled="true" id="a_9429" operator="is"><one_string value="RC"/></rule><rule position="21" enabled="true" id="a_9429" operator="is"><one_string value="RCE"/></rule><rule position="22" enabled="true" id="a_9429" operator="is"><one_string value="Maquinaria"/></rule><rule position="23" enabled="true" id="a_9429" operator="is"><one_string value="Equipo"/></rule><rule position="24" enabled="true" id="a_9429" operator="is"><one_string value="M&E"/></rule><rule position="25" enabled="true" id="a_9429" operator="is"><one_string value="EyM"/></rule><rule position="26" enabled="true" id="a_9429" operator="is"><one_string value="Terrorismo"/></rule><rule position="27" enabled="true" id="a_9429" operator="is"><one_string value="Sabotaje"/></rule><rule position="28" enabled="true" id="a_9429" operator="is"><one_string value="S&T"/></rule><rule position="29" enabled="true" id="a_9429" operator="is"><one_string value="Transporte"/></rule><rule position="30" enabled="true" id="a_9429" operator="is"><one_string value="Cargo"/></rule><rule position="31" enabled="true" id="a_9429" operator="is"><one_string value="Market Meeting"/></rule><rule position="32" enabled="true" id="a_9429" operator="is"><one_string value="Reunión de Mercado"/></rule></filter><attribute id="a_9429" type="string"><table>cmn_ObjectDeviceSearchedItems</table><column>Value</column></attribute></exportedFilter>

PALABRAS DE EXCLUSIÓN MAPFRE

5. Los resultados obtenidos luego de realizar los 14 filtros de información y aplicar los comandos de exclusión sobre cada correo electrónico y que sean satisfactorios para el proceso, serán exportados en un

documento .HTML para cada buzón de correo analizado y por separado en marcadores para una fácil interpretación de este.

Tras explicar los procedimientos y procesos a realizar, se procede a iniciar la labor pericial en Informática Forense de la siguiente manera:

1. **Buzón de correo electrónico avictor@mapfre.com.co.**

El día 17 de noviembre de 2021 el equipo de ADALID CORP. ingresa a la carpeta **AVICTOR**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

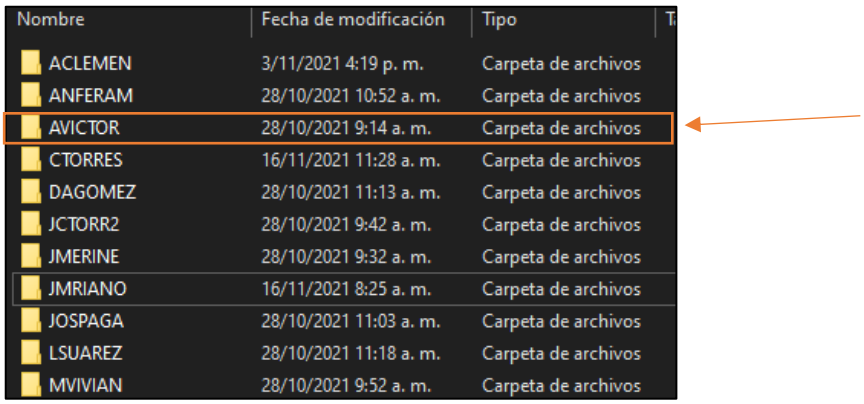


Ilustración 3 Visualización carpeta AVICTOR.

Posteriormente, procede a validar la información contenida al interior de la carpeta **AVICTOR** identificada al interior del disco duro como se observa en las siguientes imágenes:

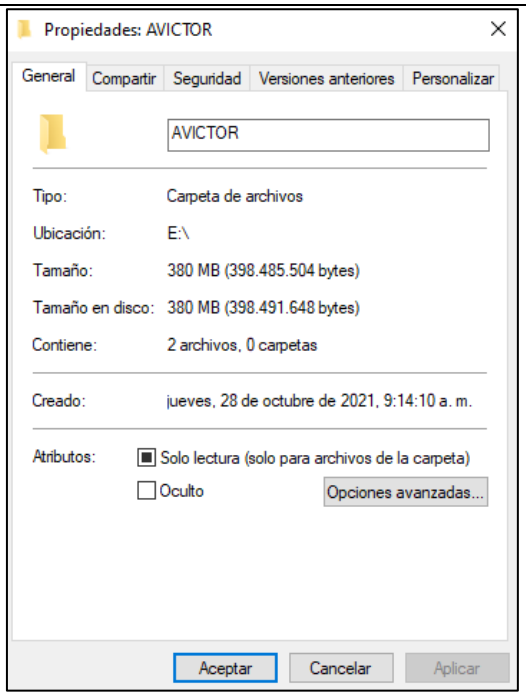


Ilustración 4 Propiedades de la carpeta AVICTOR visto desde el Disco Duro.

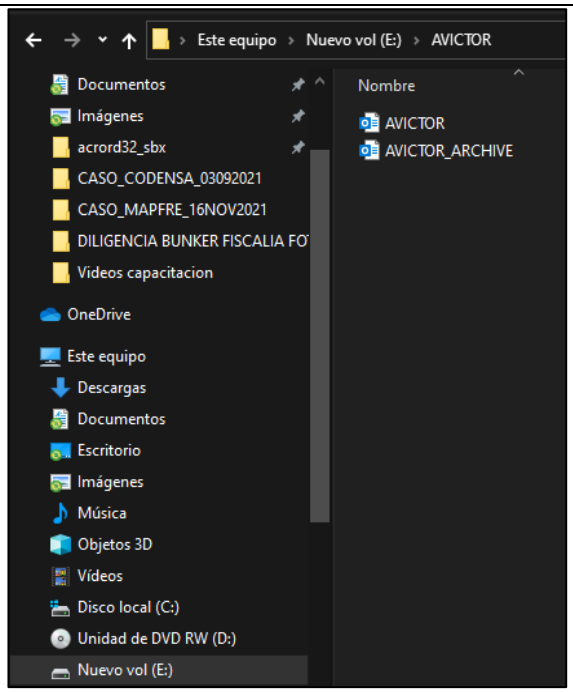


Ilustración 5 Contenido de la carpeta AVICTOR visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**avictor@mapfre.com.co.**" asignado a **Víctor Jonathan ARELLANO CARDONA** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **10:42:03** y culminando el mismo de forma satisfactoria a las **10:42:56**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_17NOV2021
Número de prueba: 001_AVICTOR
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO AVICTOR@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO

DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP S.A.S. - Endrick Dann Axel DÍAZ ORTEGA
Notas:

Information for F:\1. AVICTOR\IMAGENFORENSE_PST_AVICTOR_MAPFRE_17NOV2021.ad1:
[Custom Content Sources]
AVICTOR:G:\AVICTOR | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 7d7787982808d7be0d6baf4f87b9505a
SHA1 checksum: 1818a0e2013e2215acf8130a1f35002f72fc48de

Image information:
Acquisition started: Wed Nov 17 10:42:03 2021
Acquisition finished: Wed Nov 17 10:42:55 2021
Segment list:
F:\1. AVICTOR\IMAGENFORENSE_PST_AVICTOR_MAPFRE_17NOV2021.ad1

Image Verification Results:
Verification started: Wed Nov 17 10:42:55 2021
Verification finished: Wed Nov 17 10:42:56 2021
MD5 checksum: 7d7787982808d7be0d6baf4f87b9505a : verified
SHA1 checksum: 1818a0e2013e2215acf8130a1f35002f72fc48de : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **HITACHI**, identificado con número de serie **JP2930HQ2N6YLH**, con capacidad de almacenamiento de **1000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Luego, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**avictor@mapfre.com.co.**" asignado a **Víctor Jonathan ARELLANO CARDONA** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 6 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO AVICTOR@MAPFRE.COM.CO.

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico **avictor@mapfre.com.co** asignada **Víctor Jonathan ARELLANO CARDONA** para el desarrollo de sus funciones:

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
1	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Víctor Jonathan ARELLANO CARDONA → avictor@mapfre.com.co	ad1	0.38 GB
TOTAL					**0.38 GB**

Tabla 3 Detalle del buzón de correo electrónico asignado avictor@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico **avictor@mapfre.com.co** asignado a **Víctor Jonathan ARELLANO CARDONA** para el desarrollo de sus funciones aloja un total de **0.38 GB** dentro de este espacio el laboratorio de informática forense logró hallar un total de **Siete mil ochocientos seis (7.806)** archivos (incluyendo carpetas), como se observa a continuación.

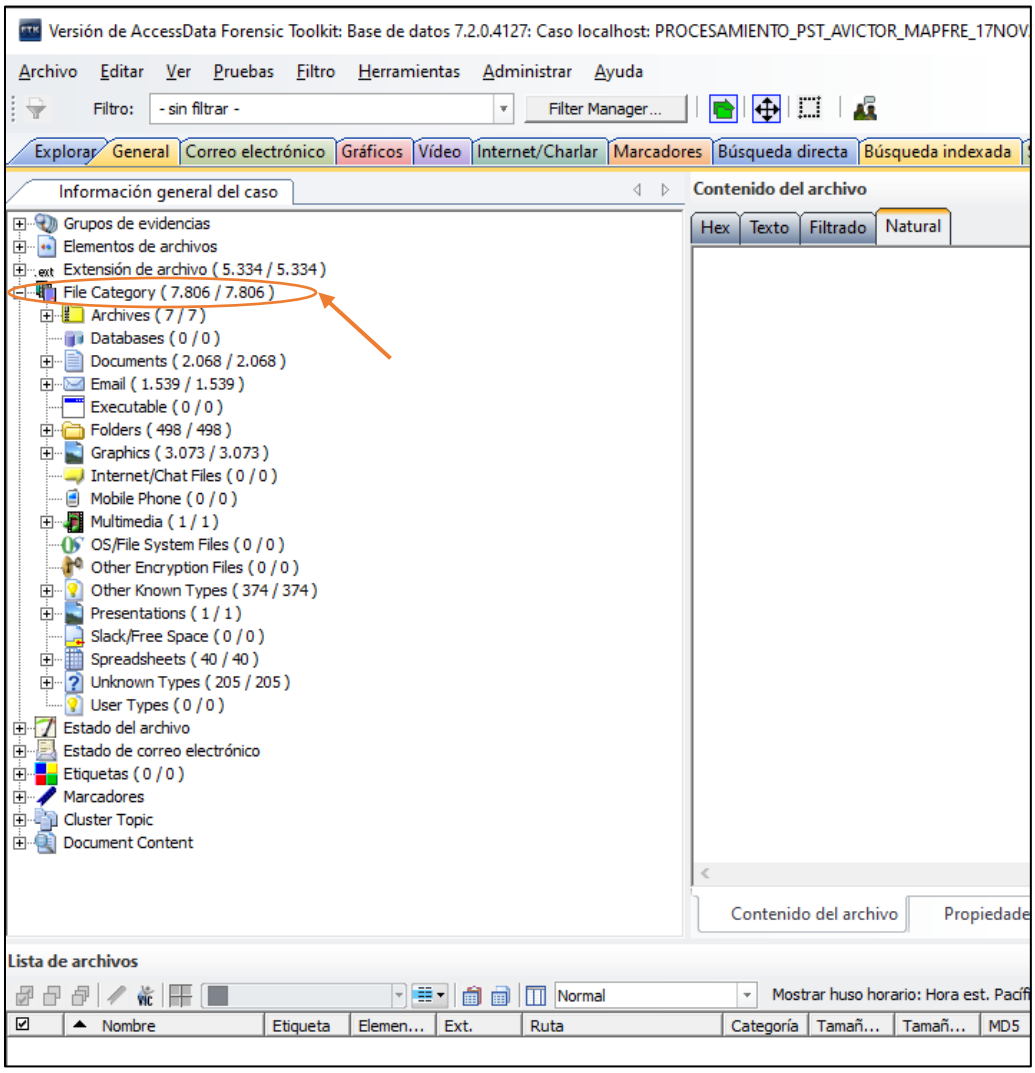


Ilustración 7 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico avictor@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO VÍCTOR JONATHAN ARELLANO CARDONA → AVICTOR@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información

eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico a victor@mapfre.com.co asignado a Víctor Jonathan ARELLANO CARDONA, iniciando el día el **17** de noviembre del presente año con una duración aproximada de Un (1) días calendario, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Mil ochocientos cincuenta (1.850)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

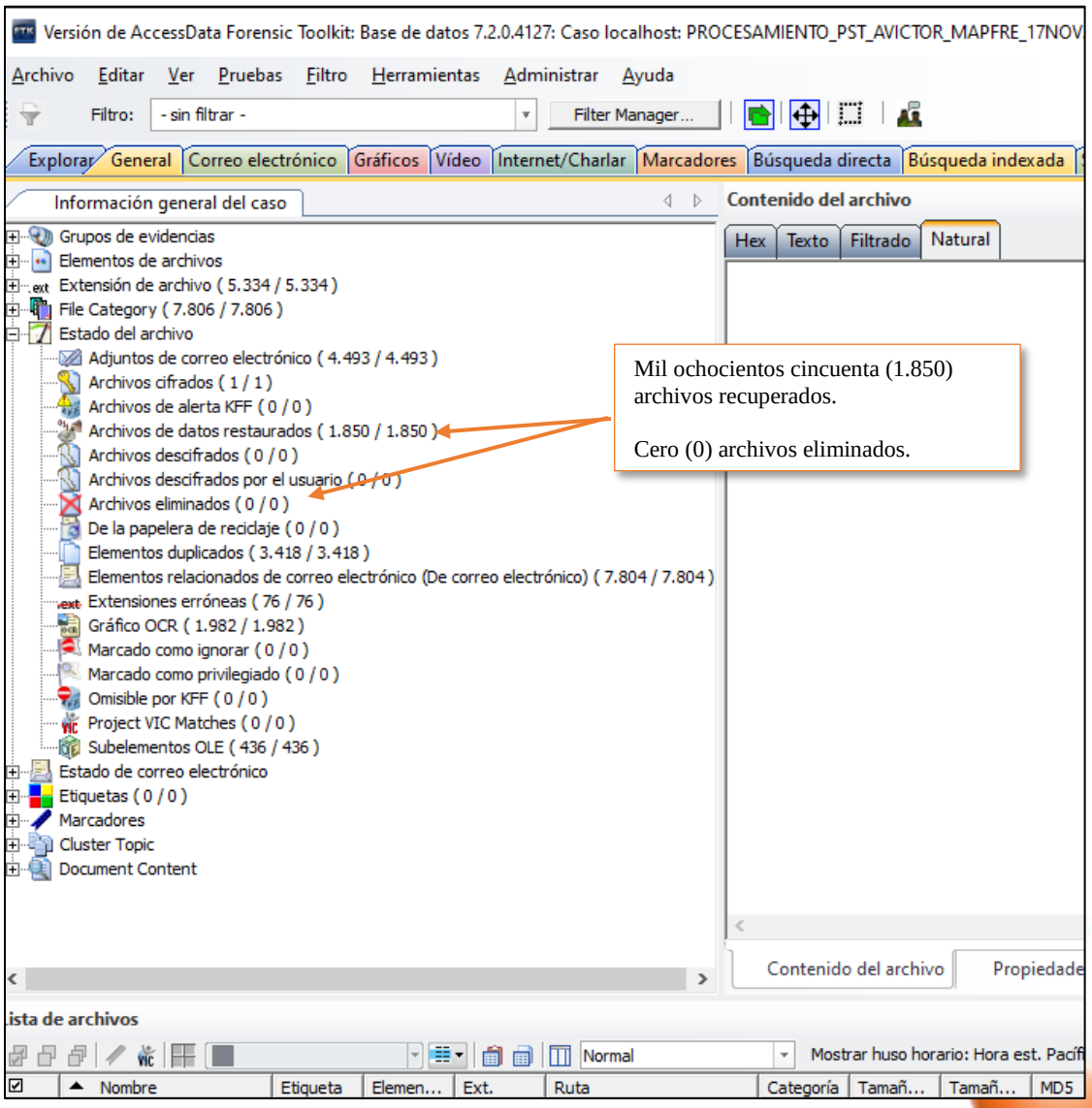


ilustración 8 Total de archivos recuperados en la cuenta de correo electrónico avictor@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Siete mil ochocientos seis (7.806)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

- **RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO AVICTOR@MAPFRE.COM.CO.**

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico avictor@mapfre.com.co asignada a **Víctor Jonathan ARELLANO CARDONA** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	7
2	Documentos	2.068
3	Correo Electrónico	1.539
4	Carpetas	498
5	Gráficos	3.073
6	Multimedia	1
7	Otro tipo de Archivos	374
8	Presentaciones	1
9	Hojas de cálculo	40
10	Tipos de archivos desconocidos	205
TOTAL		**7.806**

Tabla 4 Información buscada evidencia 001_AVICTOR, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior **tabla**, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Siete mil ochocientos seis (7.806).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean

legibles, archivos **duplicados**[1], falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Cuatro mil cuatrocientos noventa y tres (4.493) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Un (1) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Mil ochocientos cincuenta (1.850) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Tres mil cuatrocientos dieciocho (3.418) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico
- **Siete mil ochocientos cuatro (7.804) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Setenta y seis (76) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Mil novecientos ochenta y dos (1.982) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Cuatrocientos treinta y seis (436) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico avictor@mapfre.com.co asignada a **Víctor Jonathan ARELLANO CARDONA** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

[1] Se eliminan del filtro resultado archivos duplicados, entendiendo como duplicidad, que tengan igual tamaño e igual huella digital HASH MD5 y SHA1.

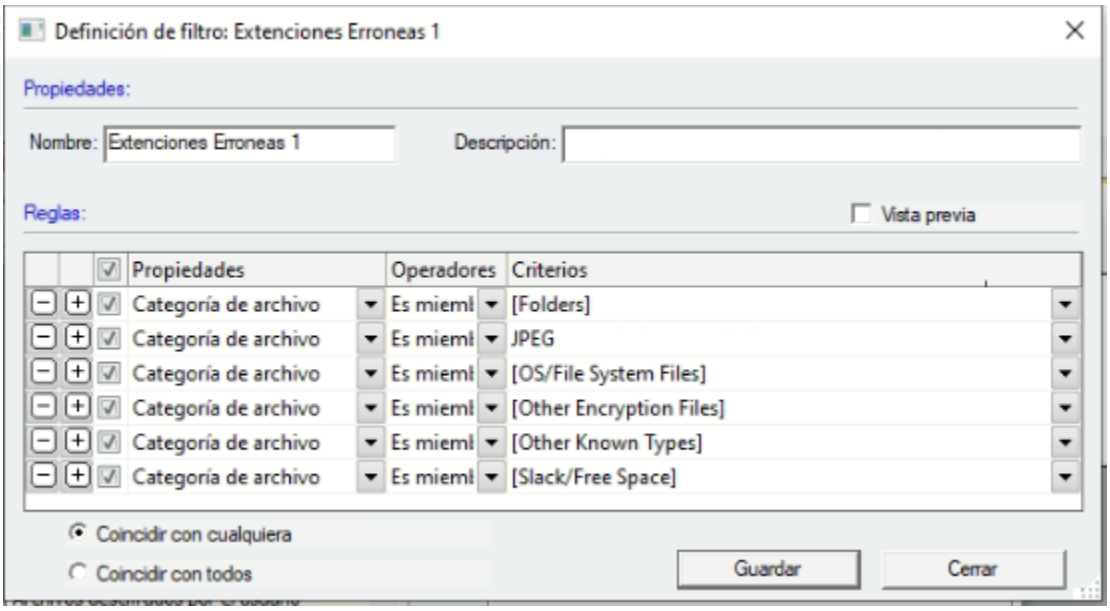


Ilustración 9 Filtro para excluir las extensiones erróneas.

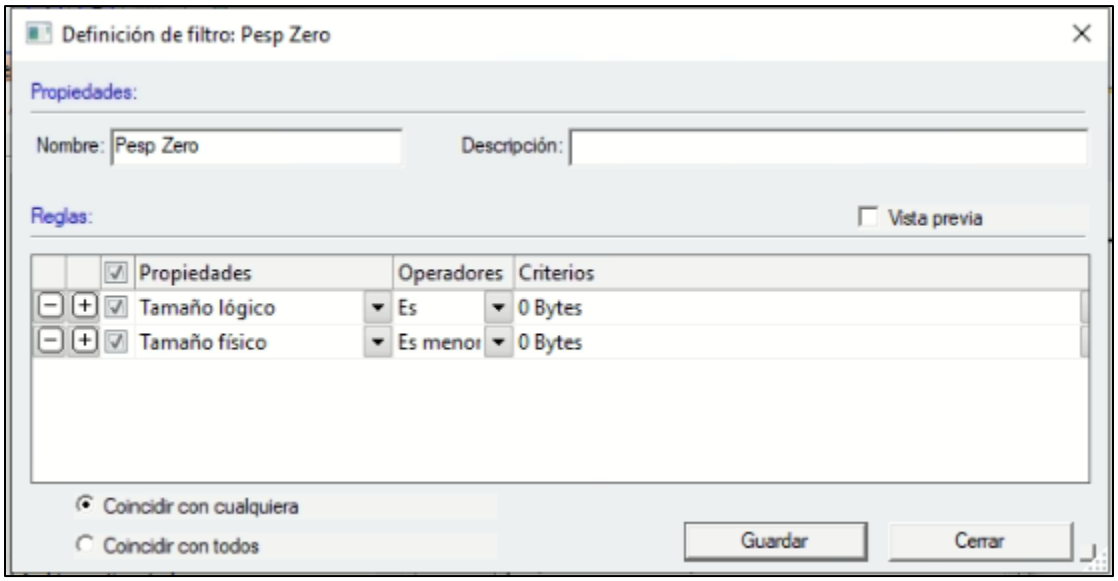


Ilustración 10 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

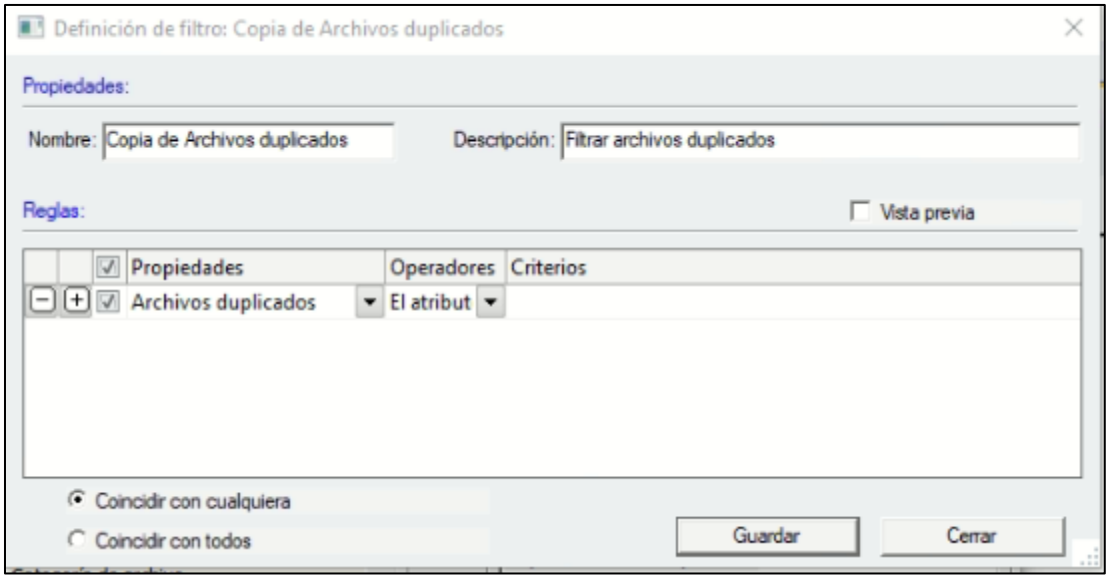


Ilustración 11 Filtro para excluir los archivos duplicados.

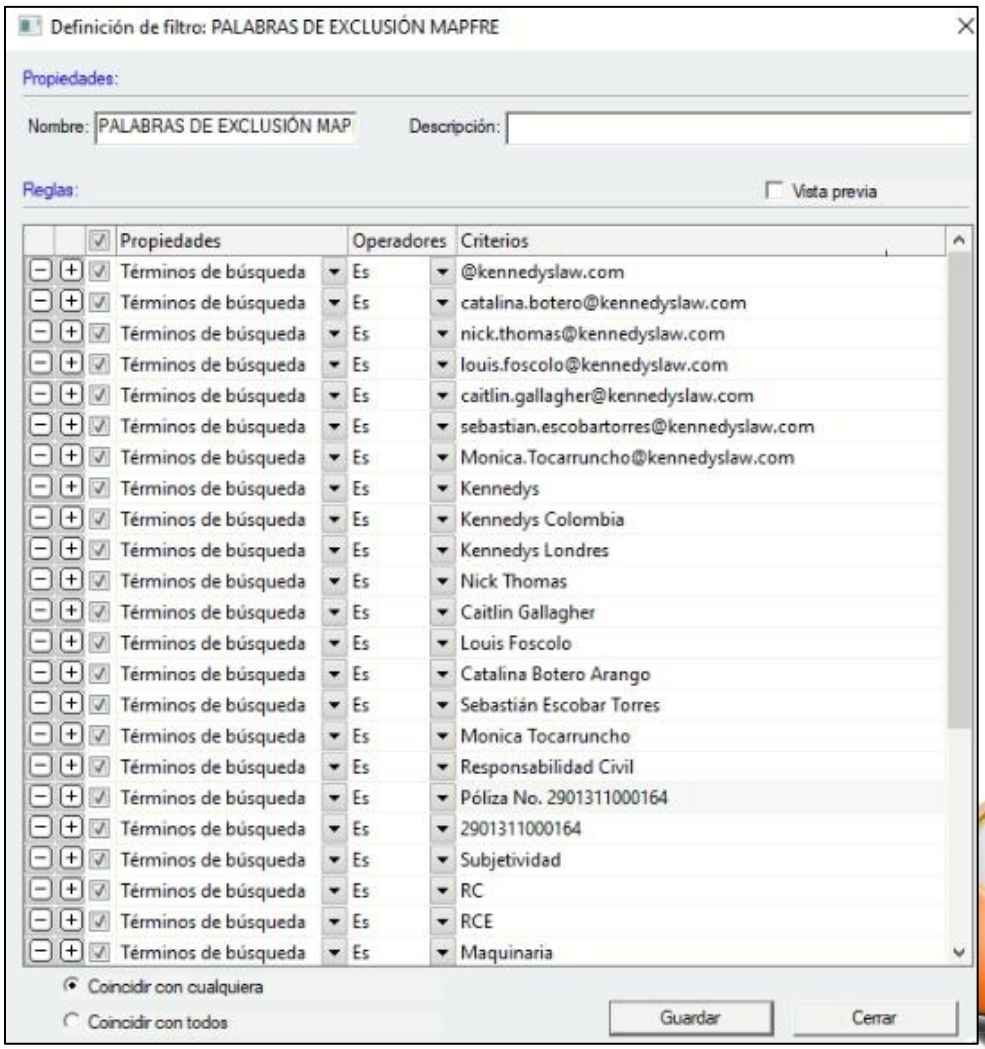


Ilustración 12 Filtro para excluir los archivos suministrado por MAPFRE - 1.

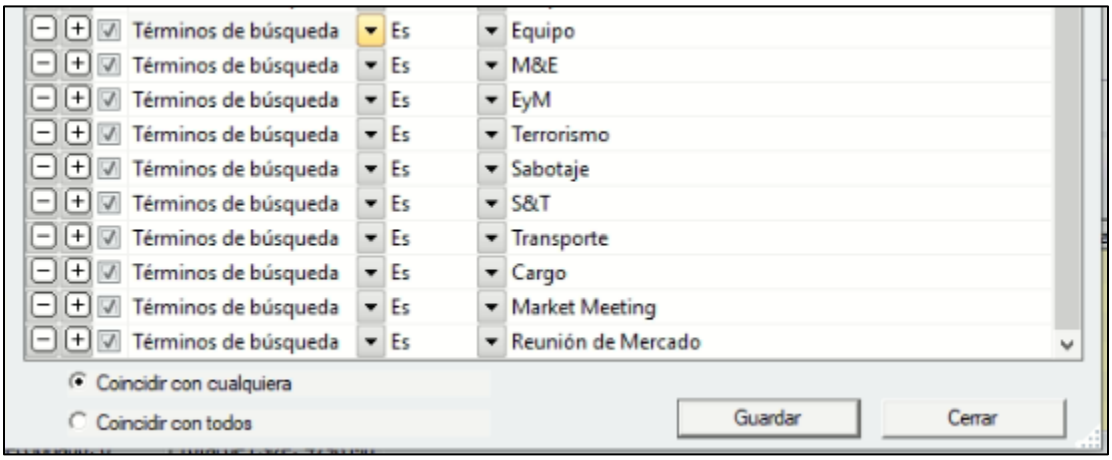
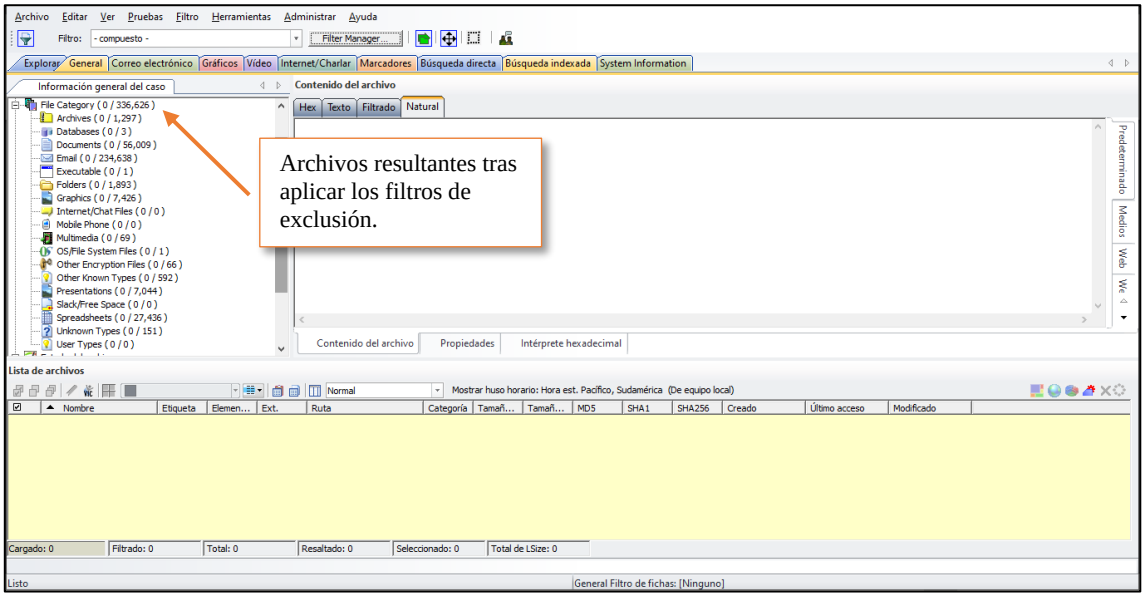


Ilustración 13 Filtro para excluir los archivos suministrado por MAPFRE - 2.

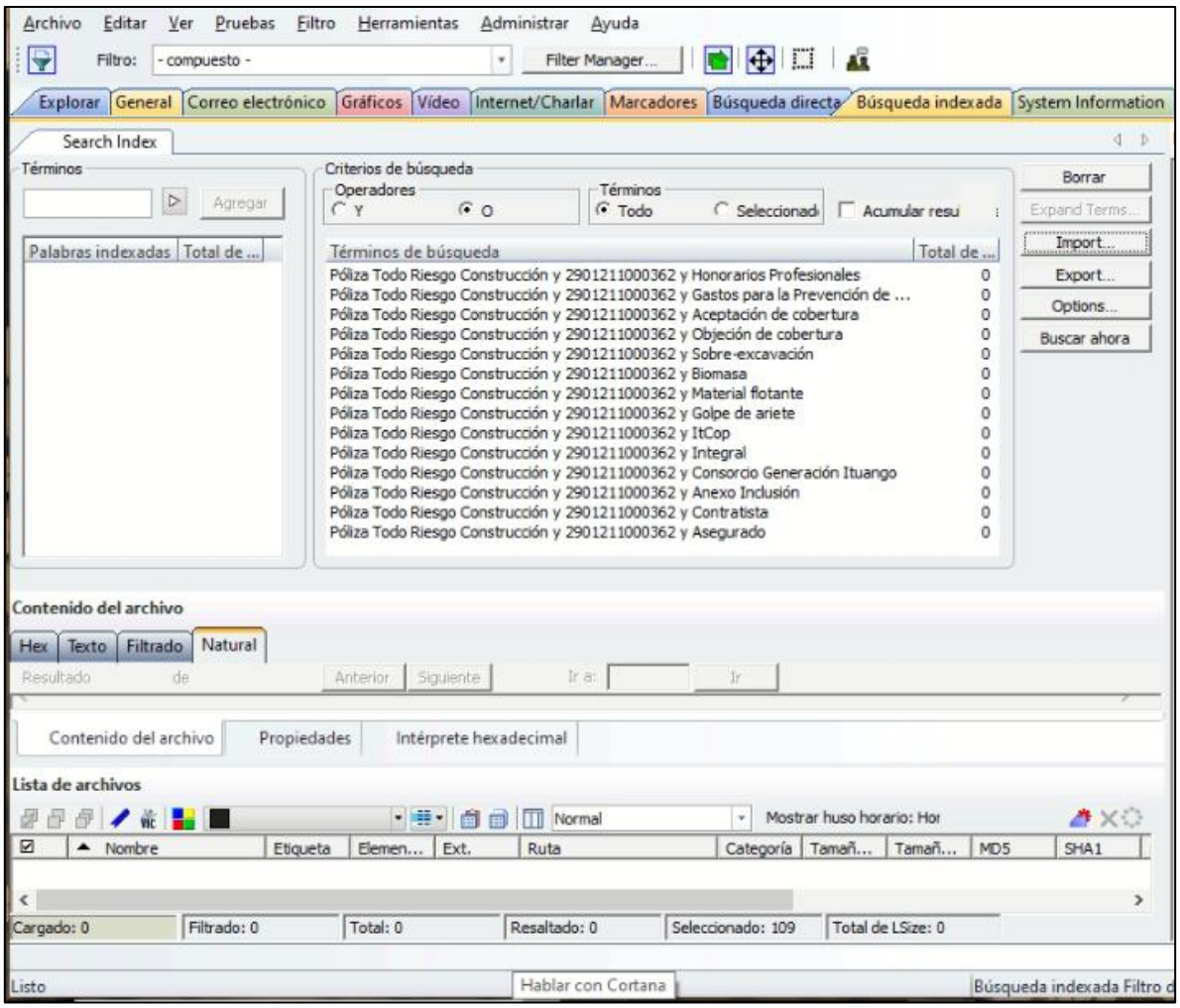
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Cero (0)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo avictor@mapfre.com.co asignada a **Víctor Jonathan ARELLANO CARDONA** para el desarrollo de sus funciones.

2. Buzón de correo electrónico aclemen@mapfre.com.co.

El día 17 de noviembre de 2021 el equipo de ADALID CORP ingresa a la carpeta **ACLEMEN**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

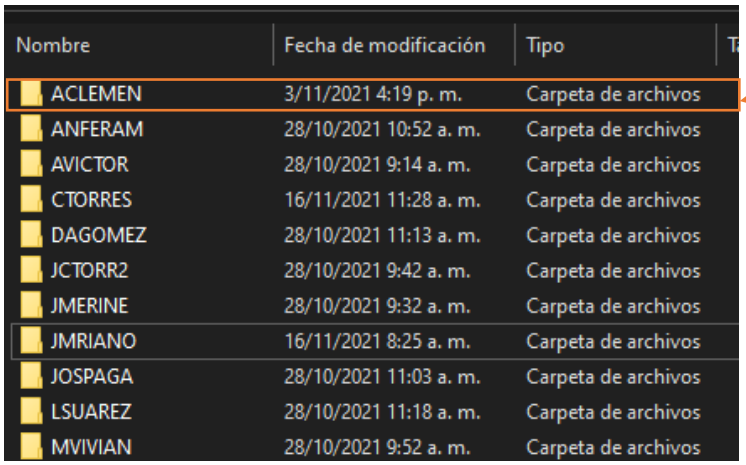


Ilustración 14 Visualización carpeta ACLEMEN

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **ACLEMEN** identificada dentro del disco duro como se observa en las siguientes imágenes:

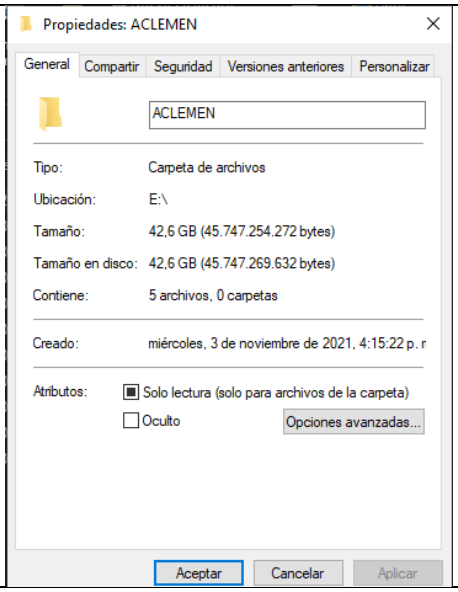


Ilustración 15 Propiedades de la carpeta ACLEMEN visto desde el Disco Duro.

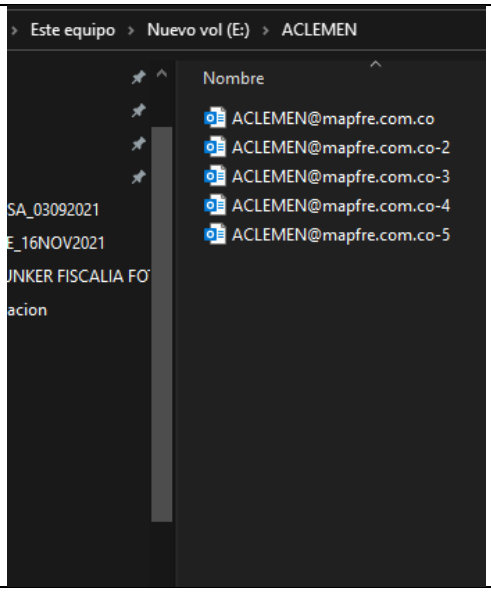


Ilustración 16 Contenido de la carpeta ACLEMEN visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**aclemen@mapfre.com.co**" asignado a **Antonio CLEMENTE CAMPANARIO** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **12:36:57** y culminando el mismo de forma satisfactoria a las **14:27:43**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_17NOV2021
Número de prueba: 002_ACLEMEN
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ACLEMEN@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP S.A.S. - Endrick Dann Axel DÍAZ ORTEGA
Notas:

Information for F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad1:
[Custom Content Sources]
ACLEMEN: G:\ACLEMEN|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 5b6abdd3129e2330f3a46cc583d004a7
SHA1 checksum: 70e7587e2b2fac10f3c58a029e552844a8aabf49

Image information:
Acquisition started: Wed Nov 17 12:36:57 2021
Acquisition finished: Wed Nov 17 14:20:40 2021
Segment list:
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad1
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad2
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad3
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad4

F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad5
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad6
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad7
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad8
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad9
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad10
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad11
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad12
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad13
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad14
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad15
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad16
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad17
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad18
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad19
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad20
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad21
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad22
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad23
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad24
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad25
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad26

F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad27
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad28
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad29
F:\2. ACLEMEN\IMAGENFORENSE_PST_ACLEMEN_MAPFRE_17NOV2021.ad30

Image Verification Results:
Verification started: Wed Nov 17 14:20:40 2021
Verification finished: Wed Nov 17 14:27:43 2021
MD5 checksum: 5b6abdd3129e2330f3a46cc583d004a7 : verified
SHA1 checksum: 70e7587e2b2fac10f3c58a029e552844a8aabf49 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **HITACHI**, identificado con número de serie **JP2930HQ2N6YLH**, con capacidad de almacenamiento de **1000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:



	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**aclemen@mapfre.com.co**" asignado a **Antonio CLEMENTE CAMPANARIO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 17 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ACLEMEN@MAPFRE.COM.CO.**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico aclemen@mapfre.com.co asignada **Antonio CLEMENTE CAMPANARIO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño
2	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Antonio CLEMENTE CAMPANARIO → aclemen@mapfre.com.co	ad1	42.6 GB
TOTAL					**42.6 GB**

Tabla 5 Detalle del buzón de correo electrónico asignado aclemen@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico aclemen@mapfre.com.co asignado a **Antonio CLEMENTE**

CAMPANARIO para el desarrollo de sus funciones **aloja** un total de **42.6 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Un millón ochocientos treinta y cinco mil seiscientos ochenta y dos (1.835.682)** archivos (incluyendo carpetas), como se observa a continuación:

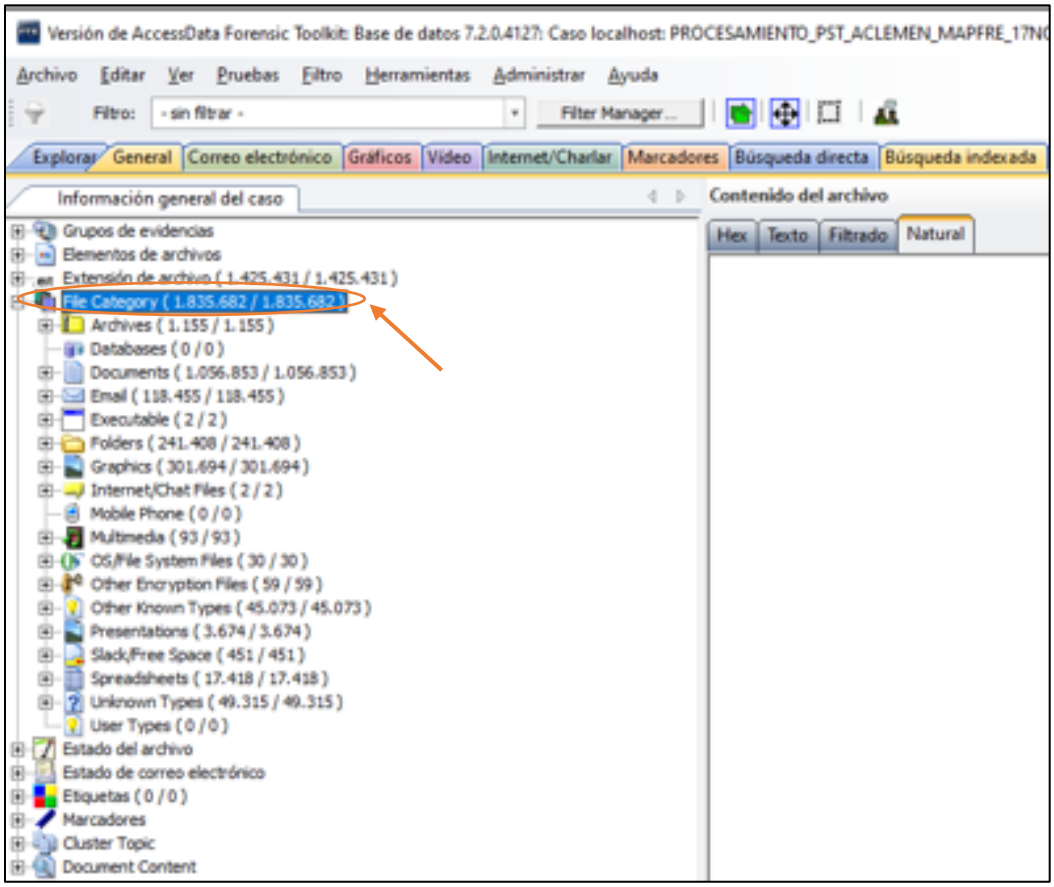


Ilustración 18 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico aclemen@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO ANTONIO CLEMENTE CAMPANARIO → ACLEMEN@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico aclemen@mapfre.com.co asignado a **Antonio CLEMENTE CAMPANARIO**, iniciando el día el **17** de noviembre del presente año con una duración aproximada de Ocho (8) días calendario el resultado a dicho proceso arrojó que existen **cero (0)** ítems en condición de "eliminados" y se reconstruyeron **Ciento cuatro mil**

setecientos sesenta y dos (104.762) archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

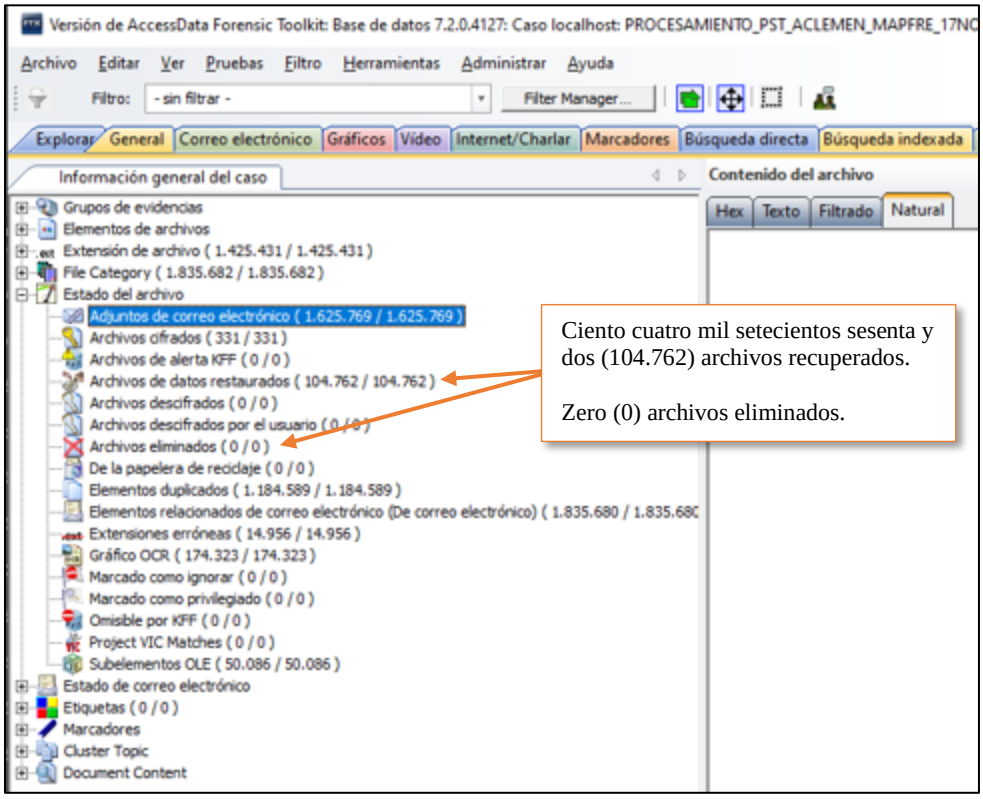


ilustración 19 Total de archivos recuperados en la cuenta de correo electrónico aclemen@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Un millón ochocientos treinta y cinco mil seiscientos ochenta y dos (1.835.682)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

- **RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ACLEMEN@MAPFRE.COM.CO.**

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico

aclemen@mapfre.com.co asignada a **Antonio CLEMENTE CAMPANARIO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1.155
2	Documentos	1.056.853
3	Correo Electrónico	118.455
4	Ejecutables	2
5	Carpetas	241.408
6	Archivo de chat	2
7	Gráficos	301.694
8	Multimedia	93
9	Archivos del sistema	30
10	Otros archivos encriptados	59
11	Otros archivos desconocidos	45.073
12	Presentaciones	3.674
13	Espacio libre	451
14	Hojas de cálculo	17.418
15	Tipos de archivos desconocidos	49.315
TOTAL		**1.835.682**

Tabla 6 Información buscada evidencia 002_ACLEMEN, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Un millón ochocientos treinta y cinco mil seiscientos ochenta y dos (1.835.682).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Un millón seiscientos veinticinco mil setecientos sesenta y nueve (1.625.769) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Trecientos Treinta y Un (331) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Ciento cuatro mil setecientos sesenta y dos (104762) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Un millón ciento ochenta y cuatro mil quinientos ochenta y nueve (1.184.589) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Un millón ochocientos treinta y cinco mil seiscientos ochenta (1.835.680) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Catorce mil novecientos cincuenta y seis (14.956) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Ciento setenta y cuatro mil trescientos veintitrés (174.323) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Cincuenta mil ochenta y seis (50.086) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico aclemen@mapfre.com.co asignada a **Antonio CLEMENTE CAMPANARIO** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



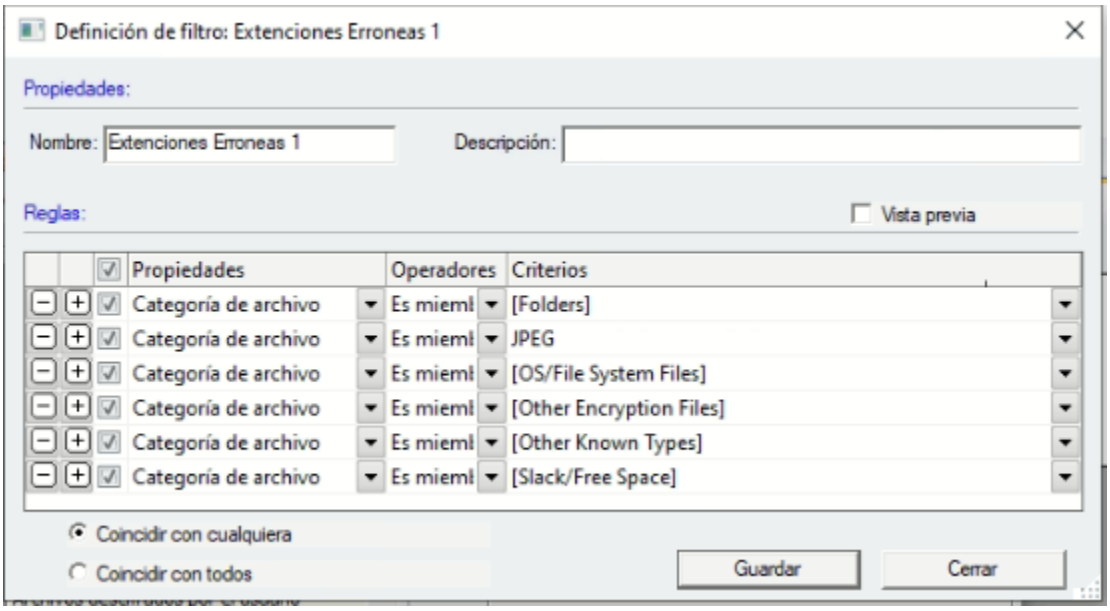


Ilustración 20 Filtro para excluir las extensiones erróneas.

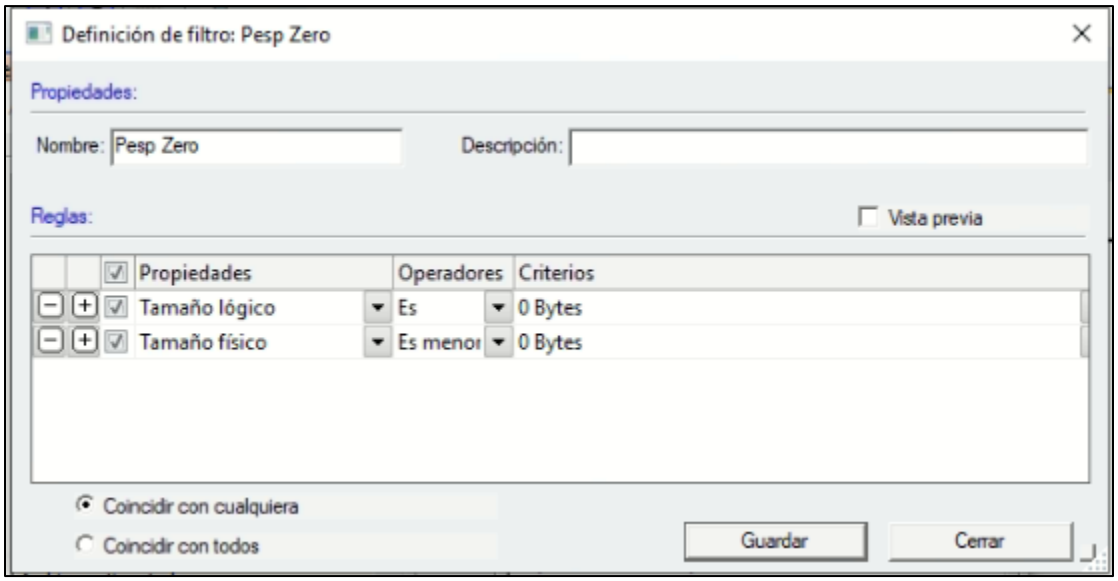


Ilustración 21 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

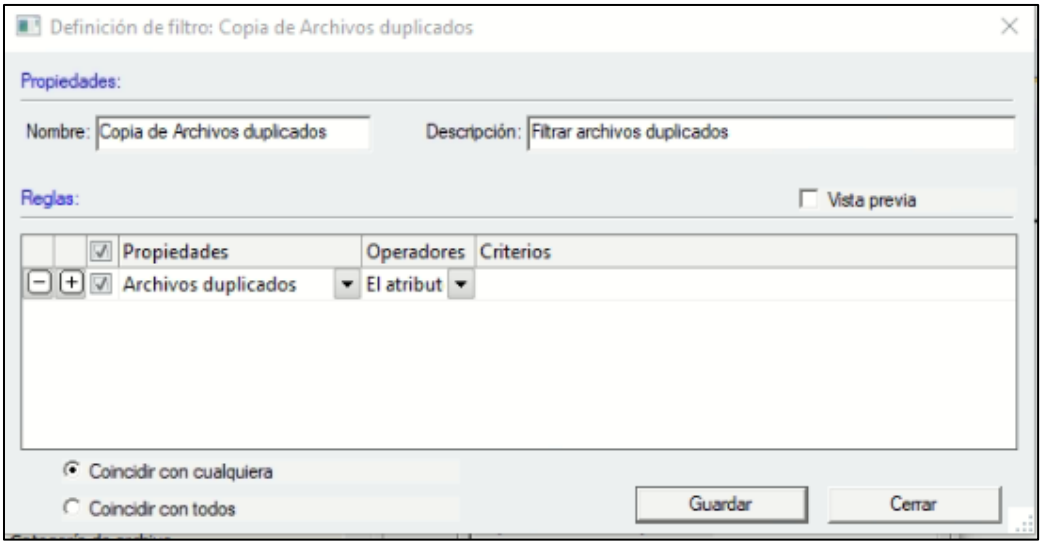
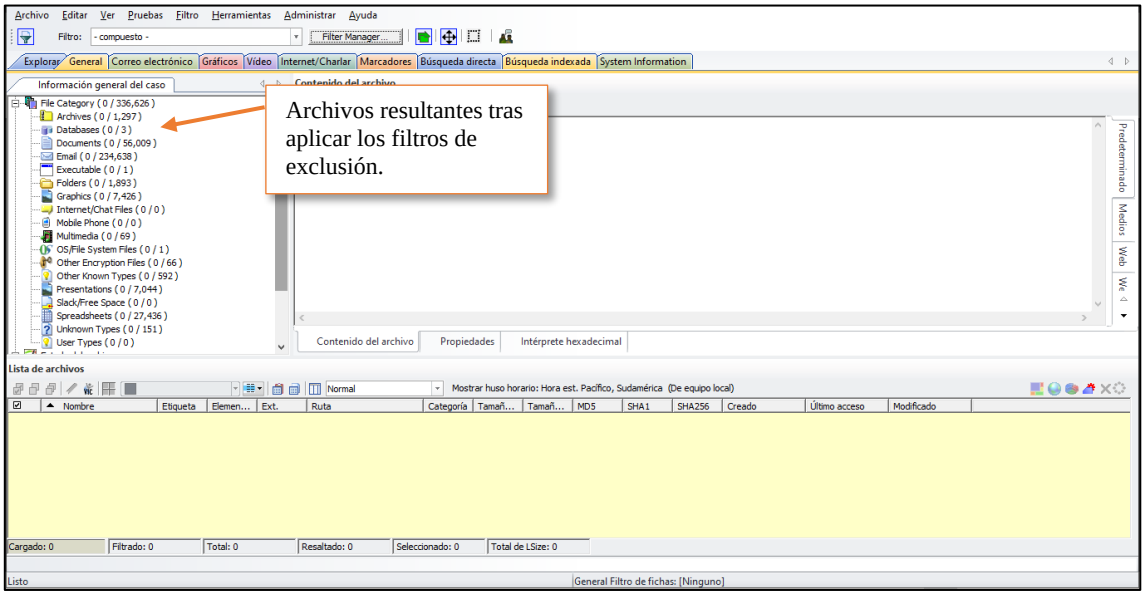


Ilustración 22 Filtro para excluir los archivos duplicados.

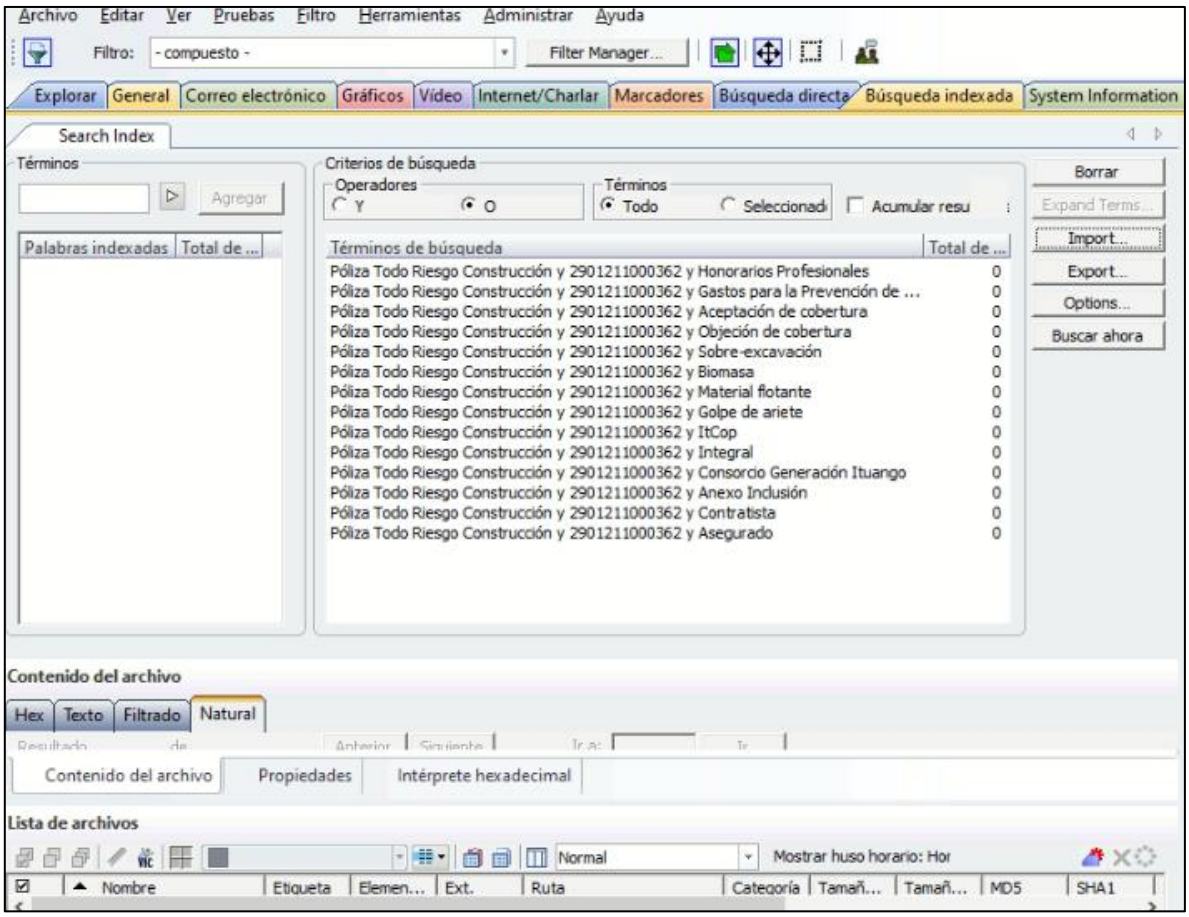
Tras aplicar los filtros anteriormente mencionados, se logra reducir muestra de información a **Cero (0)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo aclemen@mapfre.com.co asignada a **Antonio CLEMENTE CAMPANARIO** para el desarrollo de sus funciones.

3. Buzón de correo electrónico jospaga@mapfre.com.co.

El día 18 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **JOSPAGA**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

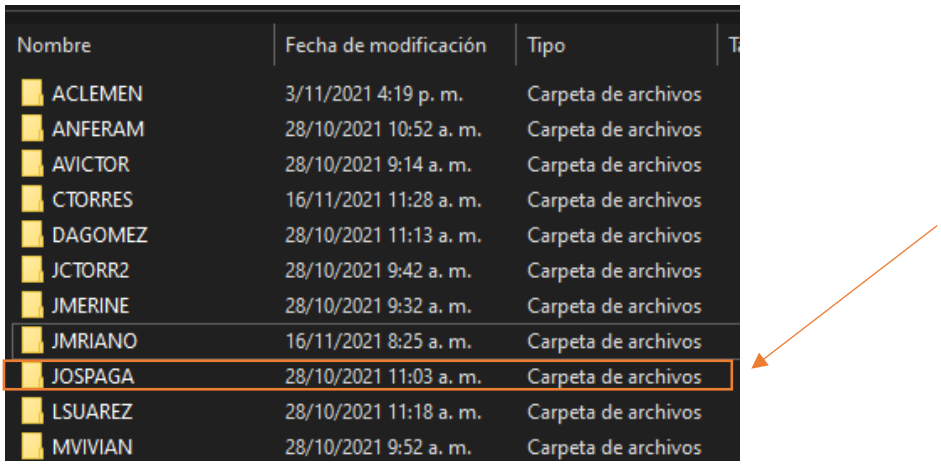


Ilustración 23 Visualización carpeta JOSPAGA

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **JOSPAGA** identificada dentro del disco duro como se observa en las siguientes imágenes:

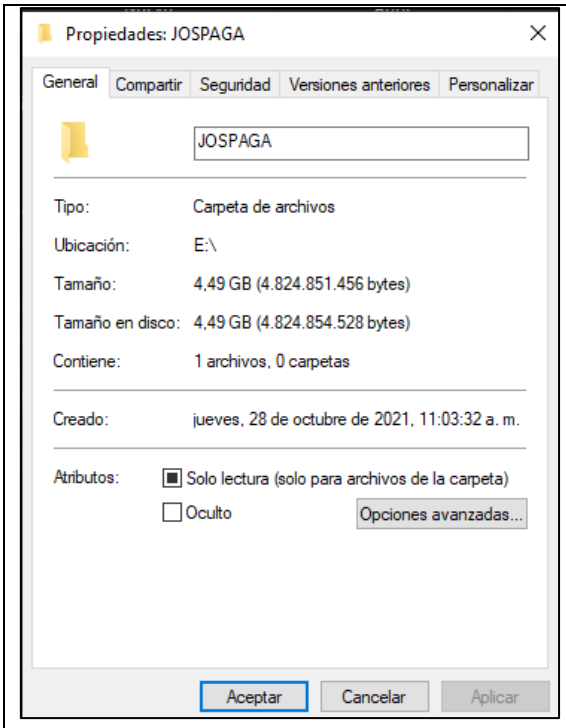


Ilustración 24 Propiedades de la carpeta JOSPAGA visto desde el Disco Duro.

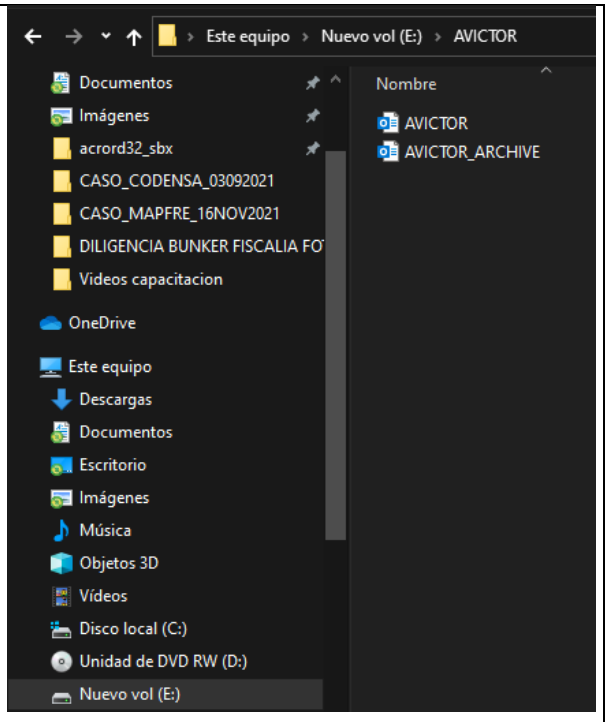


Ilustración 25 Contenido de la carpeta JOSPAGA visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**jospaga@mapfre.com.co.**" asignado a

José Fernando PALACIO GALLÓN para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **10:35:09** y culminando el mismo de forma satisfactoria a las **10:51:17**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_18NOV2021
Número de prueba: 003_JOSPAGA
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO JOSPAGA@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for F:\EVIDENCIA_MAPFRE_2\3. JOSPAGA\IMAGENFORENSE_PST_JOSPAGA_MAPFRE_18NOV2021.ad1:
[Custom Content Sources]
E::E:\ | JOSPAGA | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 326f16dbe95b854b5fdd979f1828ab88
SHA1 checksum: 090832e206bf6c9540fcfdad2d7d1aa1a25b74a3

Image information:
Acquisition started: Thu Nov 18 10:35:09 2021
Acquisition finished: Thu Nov 18 10:50:38 2021
Segment list:
F:\EVIDENCIA_MAPFRE_2\3. JOSPAGA\IMAGENFORENSE_PST_JOSPAGA_MAPFRE_18NOV2021.ad1

F:\EVIDENCIA_MAPFRE_2\3. JOSPAGA\IMAGENFORENSE_PST_JOSPAGA_MAPFRE_18NOV2021.ad2 F:\EVIDENCIA_MAPFRE_2\3. JOSPAGA\IMAGENFORENSE_PST_JOSPAGA_MAPFRE_18NOV2021.ad3 F:\EVIDENCIA_MAPFRE_2\3. JOSPAGA\IMAGENFORENSE_PST_JOSPAGA_MAPFRE_18NOV2021.ad4 Image Verification Results: Verification started: Thu Nov 18 10:50:38 2021 Verification finished: Thu Nov 18 10:51:17 2021 MD5 checksum: 326f16dbe95b854b5fdd979f1828ab88 : verified SHA1 checksum: 090832e206bf6c9540fcfdad2d7d1aa1a25b74a3 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de 2000GB, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico **jospaga@mapfre.com.co"** asignado a **José Fernando PALACIO GALLÓN** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 26 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO JOSPAGA@MAPFRE.COM.CO."**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**. para la cuenta de correo electrónico **jospaga@mapfre.com.co"** asignado a **José Fernando PALACIO GALLÓN** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
3	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	José Fernando PALACIO GALLÓN → jospaga@mapfre.com.co	ad1	4.49 GB
TOTAL					**4.49 GB**

Tabla 7 Detalle del buzón de correo electrónico asignado jospaga@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico **jospaga@mapfre.com.co"** asignado a **José Fernando PALACIO GALLÓN** para el desarrollo de sus funciones **aloja** un total de **4.49 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento noventa y seis mil ciento ochenta y nueve (196.189)** archivos (incluyendo carpetas), como se observa a continuación.

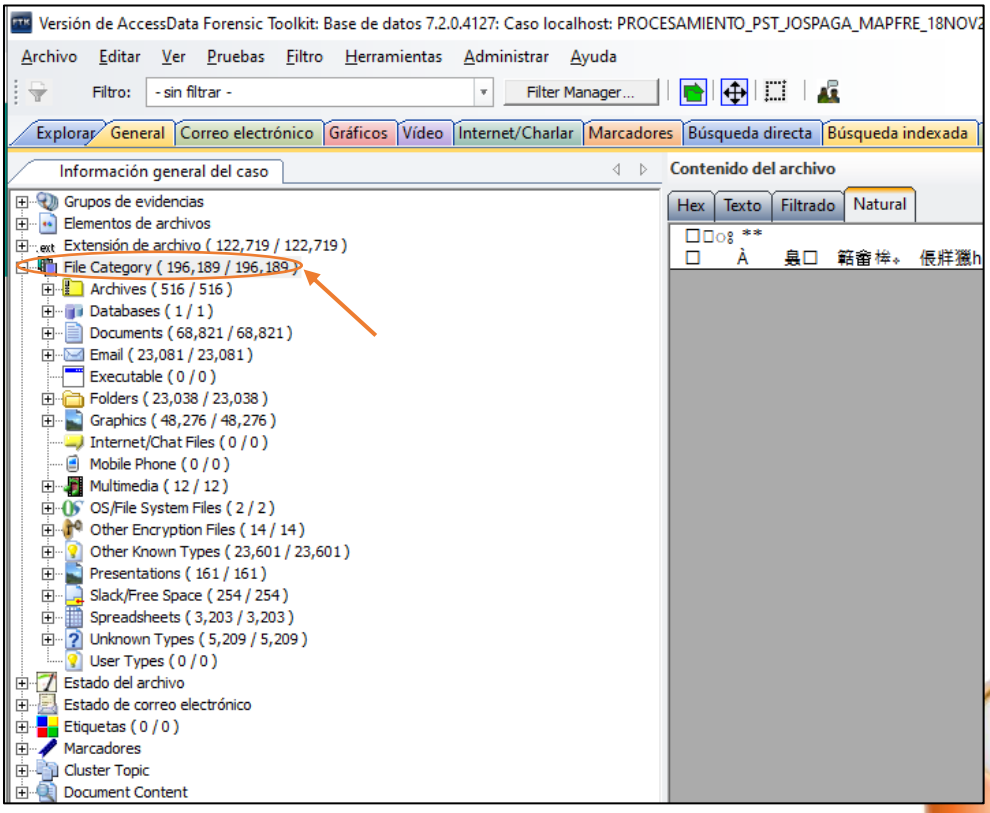


Ilustración 27 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico jospaga@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JOSÉ FERNANDO PALACIO GALLÓN → JOSPAGA@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico **jospaga@mapfre.com.co"** asignado a **José Fernando PALACIO GALLÓN** iniciando el día el **18** de noviembre del presente año con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **cero (0)** ítems en condición de "eliminados" y se reconstruyeron **Veintisiete mil ochocientos once (27.811)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

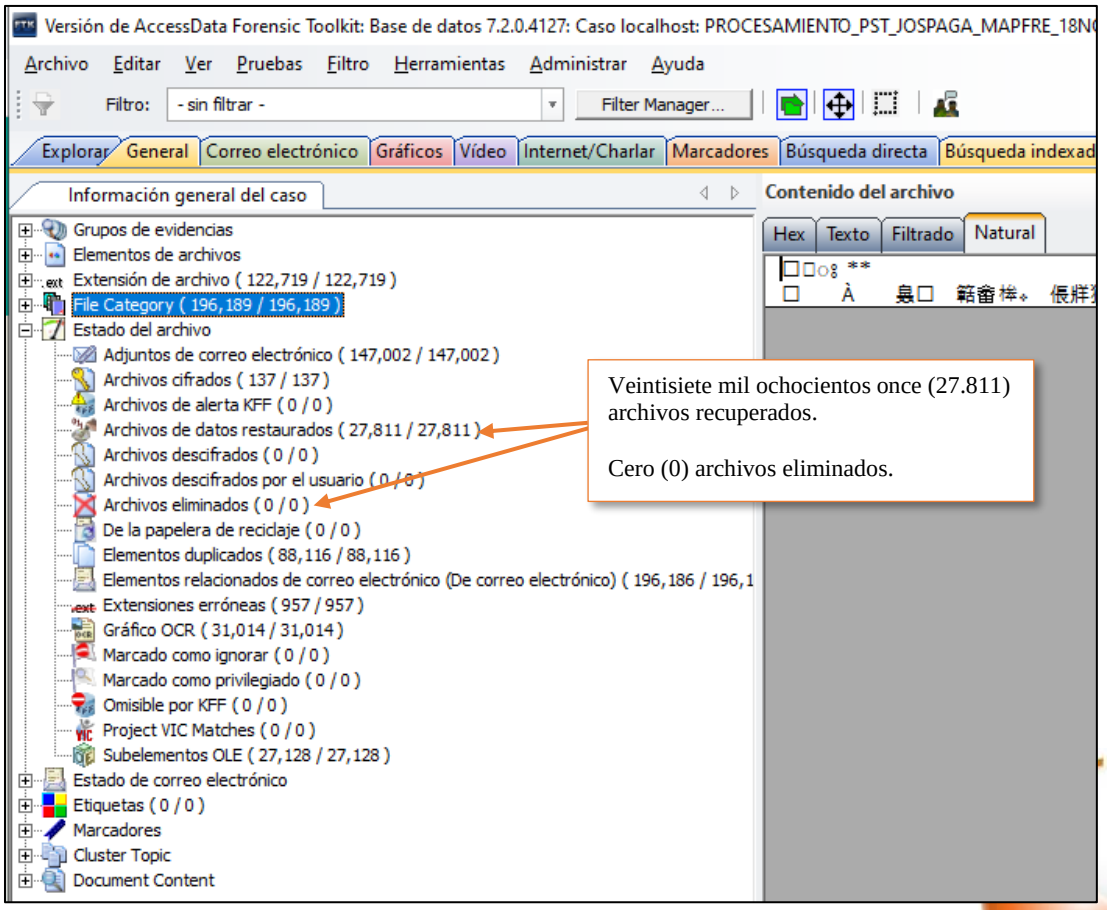


ilustración 28 Total de archivos recuperados en la cuenta de correo electrónico jospaga@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento noventa y seis mil ciento ochenta y nueve (196.189)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

- **RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO JOSPAGA@MAPFRE.COM.CO.**

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico **jospaga@mapfre.com.co** asignado a **José Fernando PALACIO GALLÓN** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	516
2	Bases de Datos	1
3	Documentos	68.821
4	Correo Electrónico	23.081
5	Carpetas	23.038
6	Gráficos	48.276
7	Multimedia	12
8	Archivos del sistema	2
9	Otros archivos encriptados	14
10	Otros archivos desconocidos	23.601
11	Presentaciones	161
12	Espacio libre	254
13	Hojas de cálculo	3.203
14	Tipos de archivos desconocidos	5.209
TOTAL		**196.189**

Tabla 8 Información buscada evidencia 003_JOSPAGA, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento noventa y seis mil ciento ochenta y nueve (196.189).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **ciento cuarenta y siete mil dos (147.002) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **ciento treinta y siete (137) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Veintisiete mil ochocientos once (27.811) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Ochenta y ocho mil ciento dieciséis (88.116) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento noventa y seis mil ciento ochenta y seis (196.186) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **novecientos cincuenta y siete (957) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Treinta y un mil catorce (31.014) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Veintisiete mil ciento veintiocho (27.128) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico jospaga@mapfre.com.co asignado a **José Fernando PALACIO GALLÓN** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

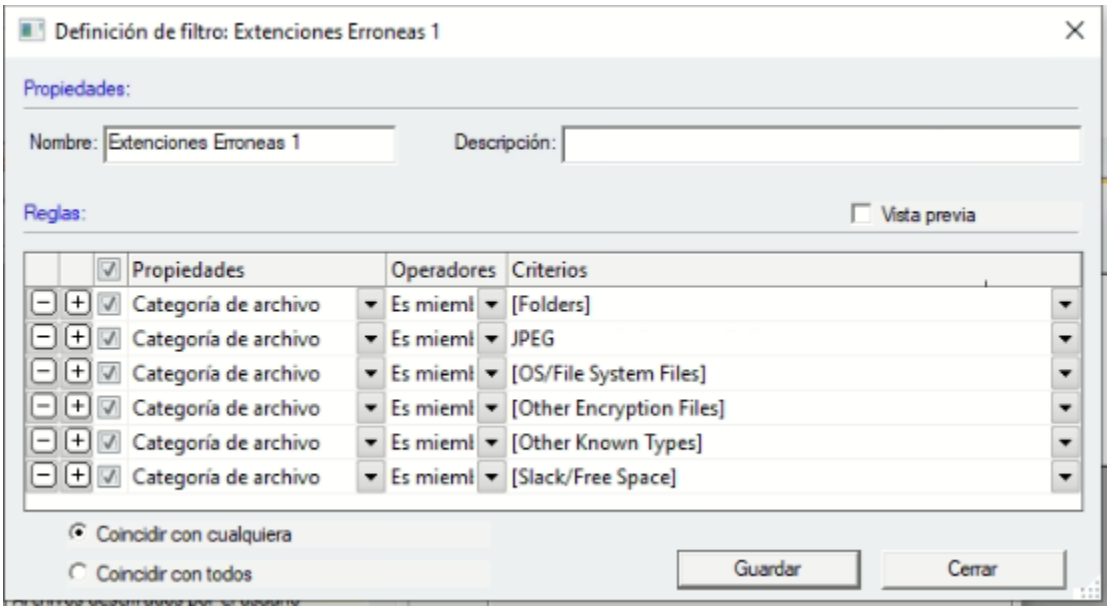


Ilustración 29 Filtro para excluir las extensiones erróneas.

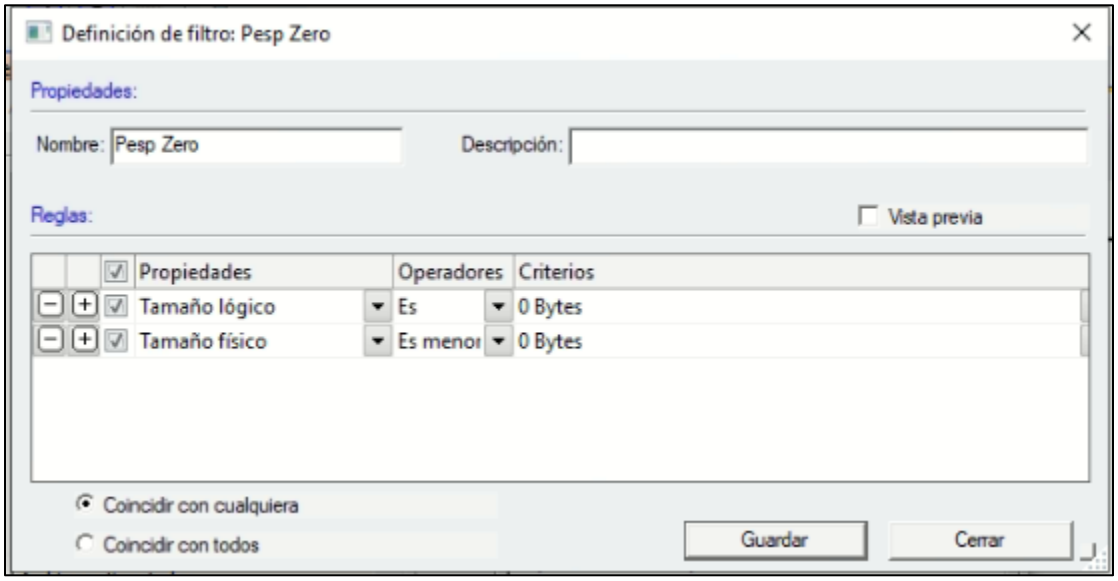


Ilustración 30 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

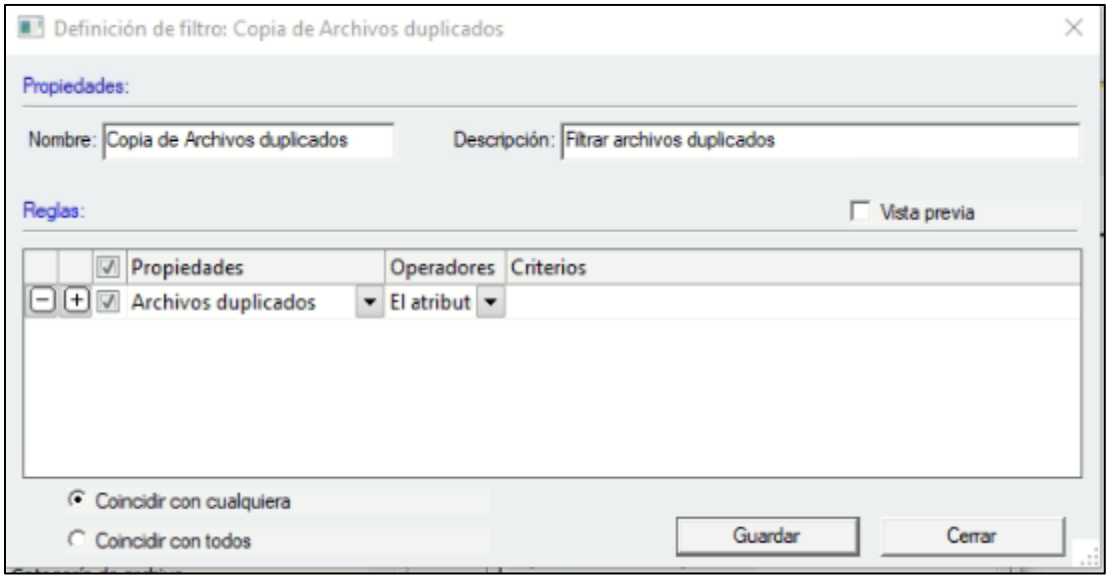


Ilustración 31 Filtro para excluir los archivos duplicados.

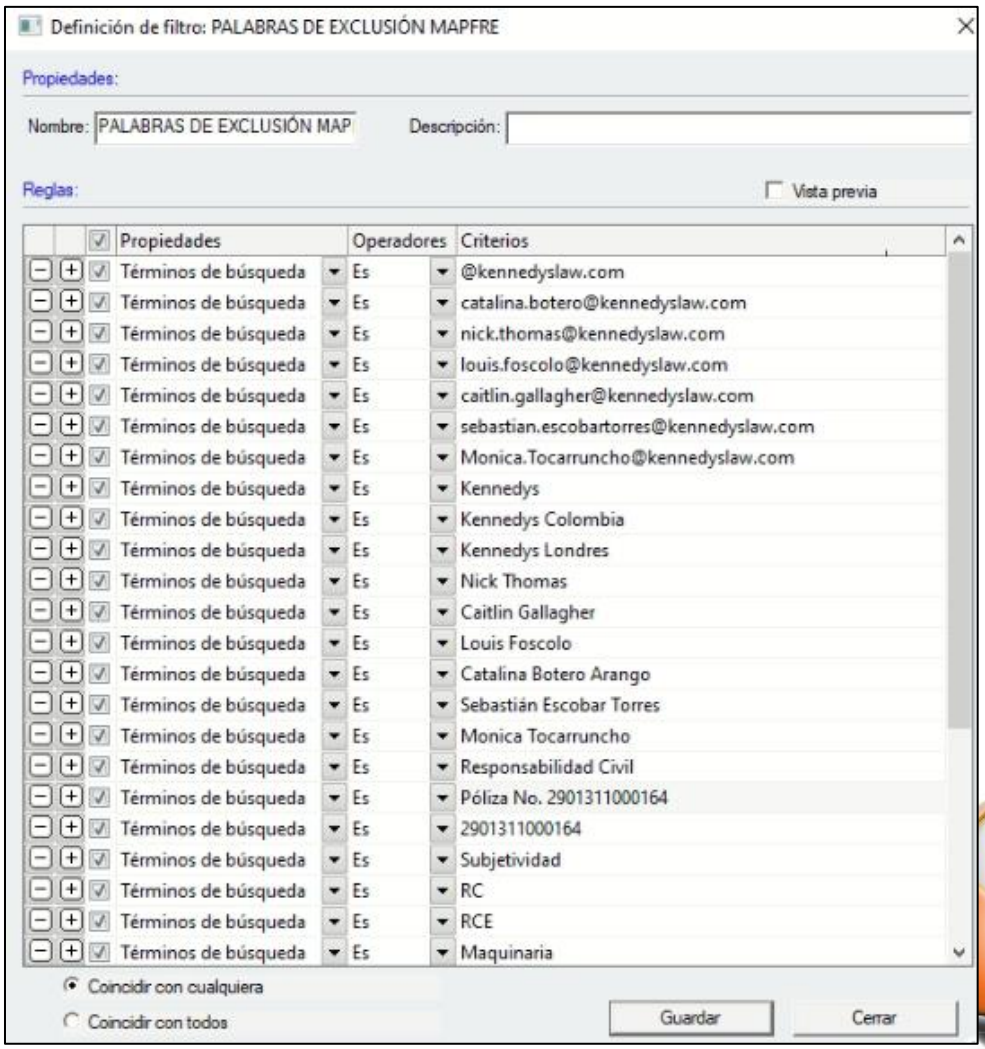


Ilustración 32 Filtro para excluir los archivos suministrado por MAPFRE - 1.

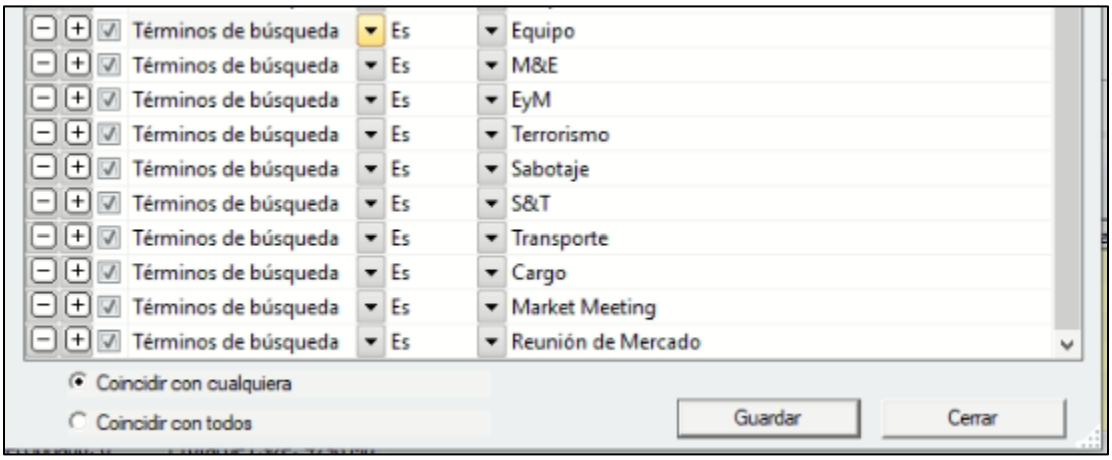
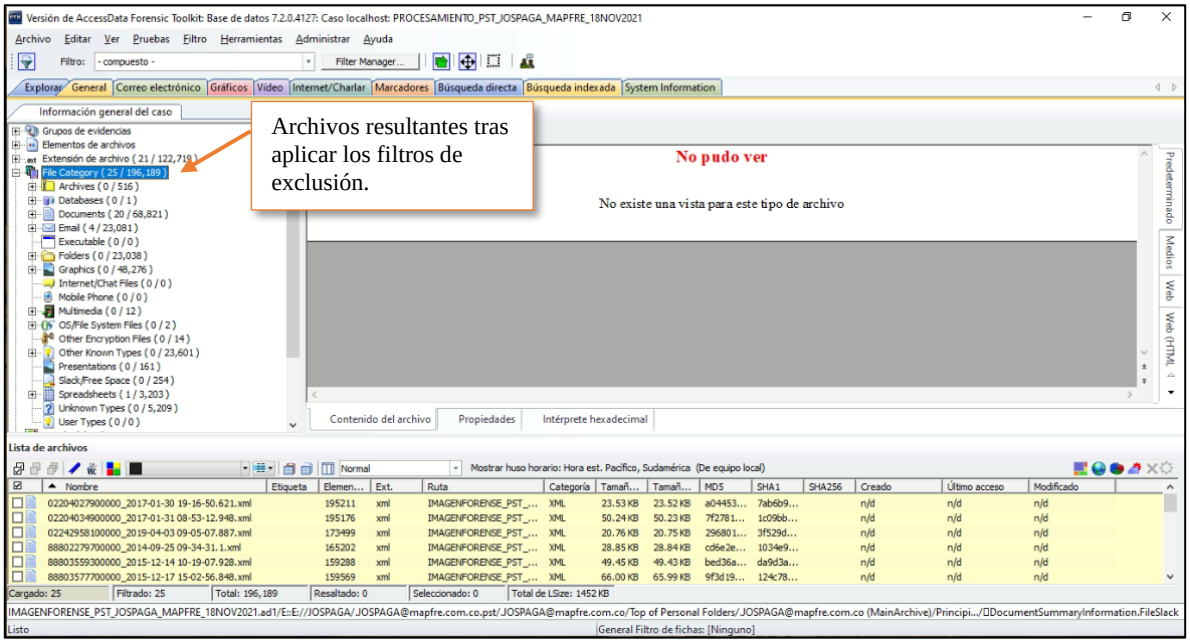


Ilustración 33 Filtro para excluir los archivos suministrado por MAPFRE - 2.

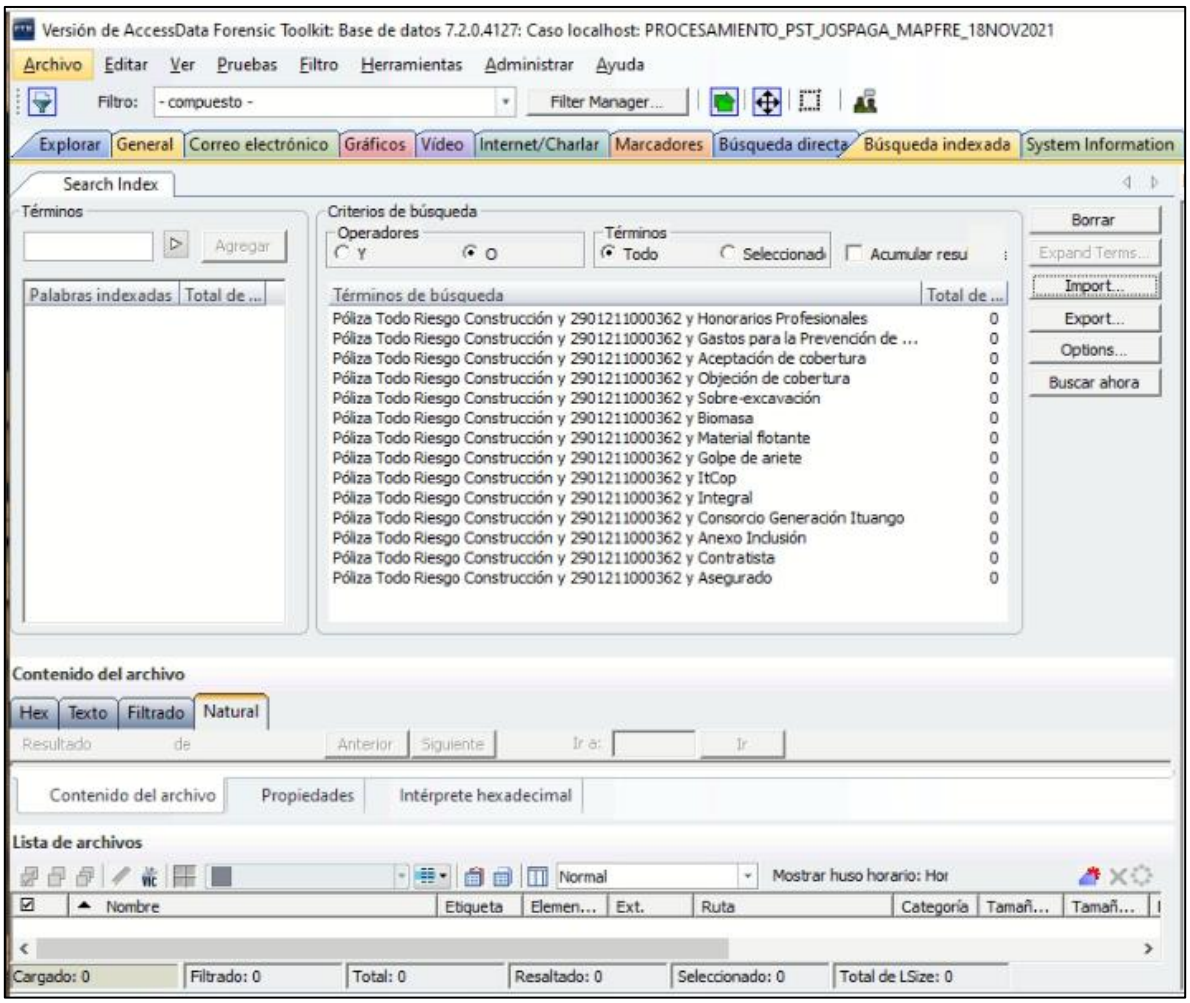
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Veinticinco (25)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo jospaga@mapfre.com.co asignado a **José Fernando PALACIO GALLÓN** para el desarrollo de sus funciones.

4. Buzón de correo electrónico ctorres@mapfre.com.co.

El día 18 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **CTORRES**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

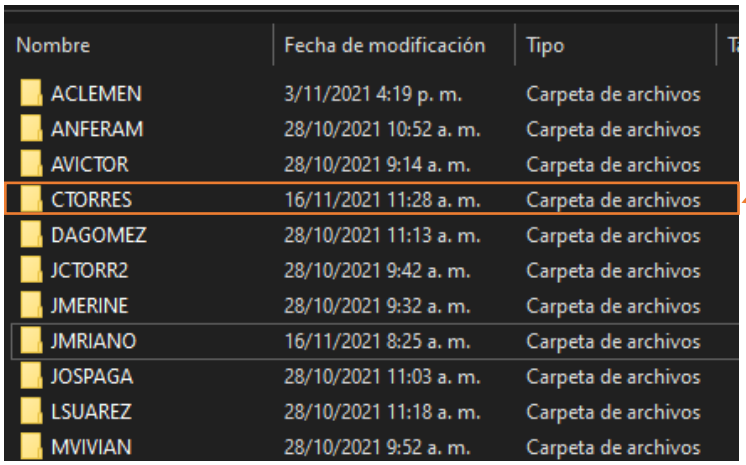


Ilustración 34 Visualización carpeta CTORRES.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **CTORRES** identificada dentro del disco duro como se observa en las siguientes imágenes:

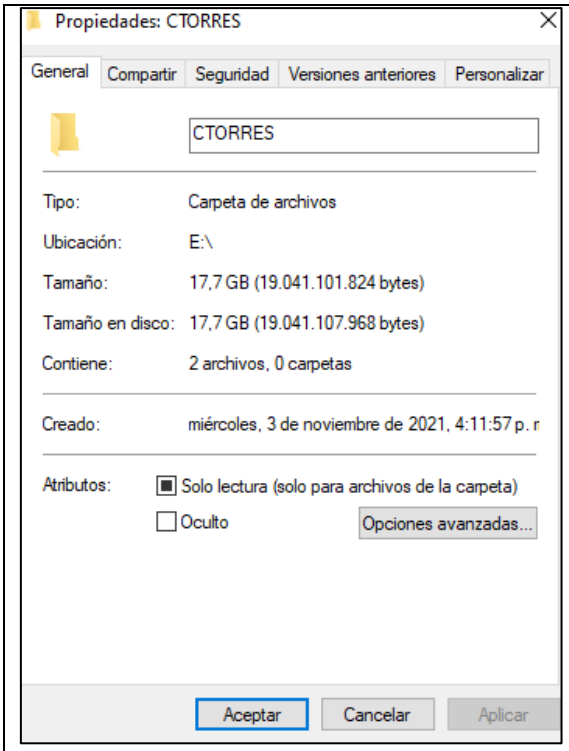


Ilustración 35 Propiedades de la carpeta CTORRES visto desde el Disco Duro.

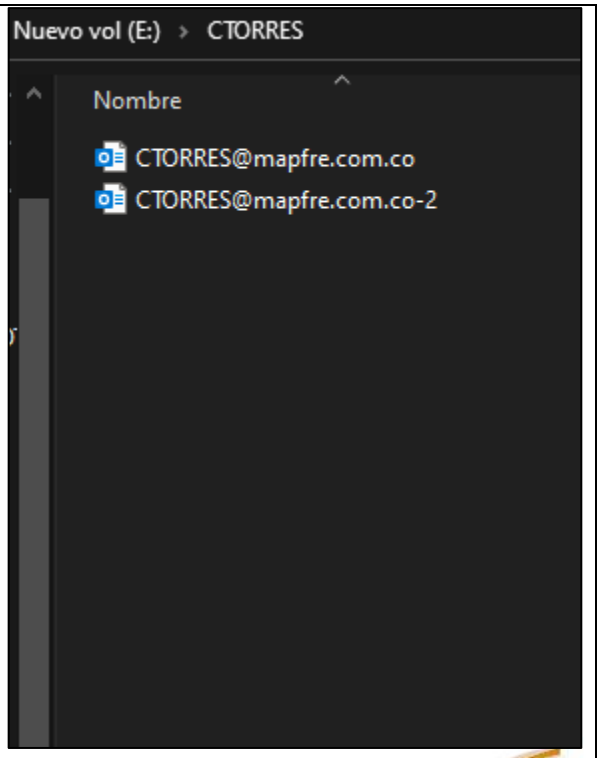


Ilustración 36 Contenido de la carpeta CTORRES visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**ctorres@mapfre.com.co**" asignado a

Carmenza GUATAVITA TORRES para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **12:37:10** y culminando el mismo de forma satisfactoria a las **13:44:09**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_18NOV2021
Número de prueba: 004_CTORRES
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO CTORRES@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad1:
[Custom Content Sources]
E::E:\|CTORRES|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 25137b08f6c1fc4b57519ff976b5d139
SHA1 checksum: d20019fe0ad8526bbac422c7b8dd475f7225e8e0

Image information:
Acquisition started: Thu Nov 18 12:37:10 2021
Acquisition finished: Thu Nov 18 13:41:31 2021
Segment list:

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad1

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad2

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad3

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad4

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad5

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad6

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad7

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad8

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad9

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad10

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad11

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad12

F:\EVIDENCIA_MAPFRE_2\4.CTORRES\IMAGENFORENSE_PST_CTORRES_MAPFRE_18NOV2021.ad13

Image Verification Results:
Verification started: Thu Nov 18 13:41:31 2021
Verification finished: Thu Nov 18 13:44:09 2021
MD5 checksum: 25137b08f6c1fc4b57519ff976b5d139 : verified

SHA1 checksum: d20019fe0ad8526bbac422c7b8dd475f7225e8e0 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**ctorres@mapfre.com.co**" asignado a **Carmenza GUATAVITA TORRES** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados,

esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 37 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO CTORRES@MAPFRE.COM.CO.**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico ctorres@mapfre.com.co asignada **Carmenza GUATAVITA TORRES** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño
4	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Carmenza GUATAVITA TORRES → ctorres@mapfre.com.co	ad1	**17,7 GB**
TOTAL					**17,7 GB**

Tabla 9 Detalle del buzón de correo electrónico asignado ctorres@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico **ctorres@mapfre.com.co** asignado a **Carmenza GUATAVITA TORRES** para el desarrollo de sus funciones **aloja** un total de **17,7 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Un millón ciento cincuenta y siete mil novecientos doce (1.157.912)** archivos (incluyendo carpetas), como se observa a continuación.

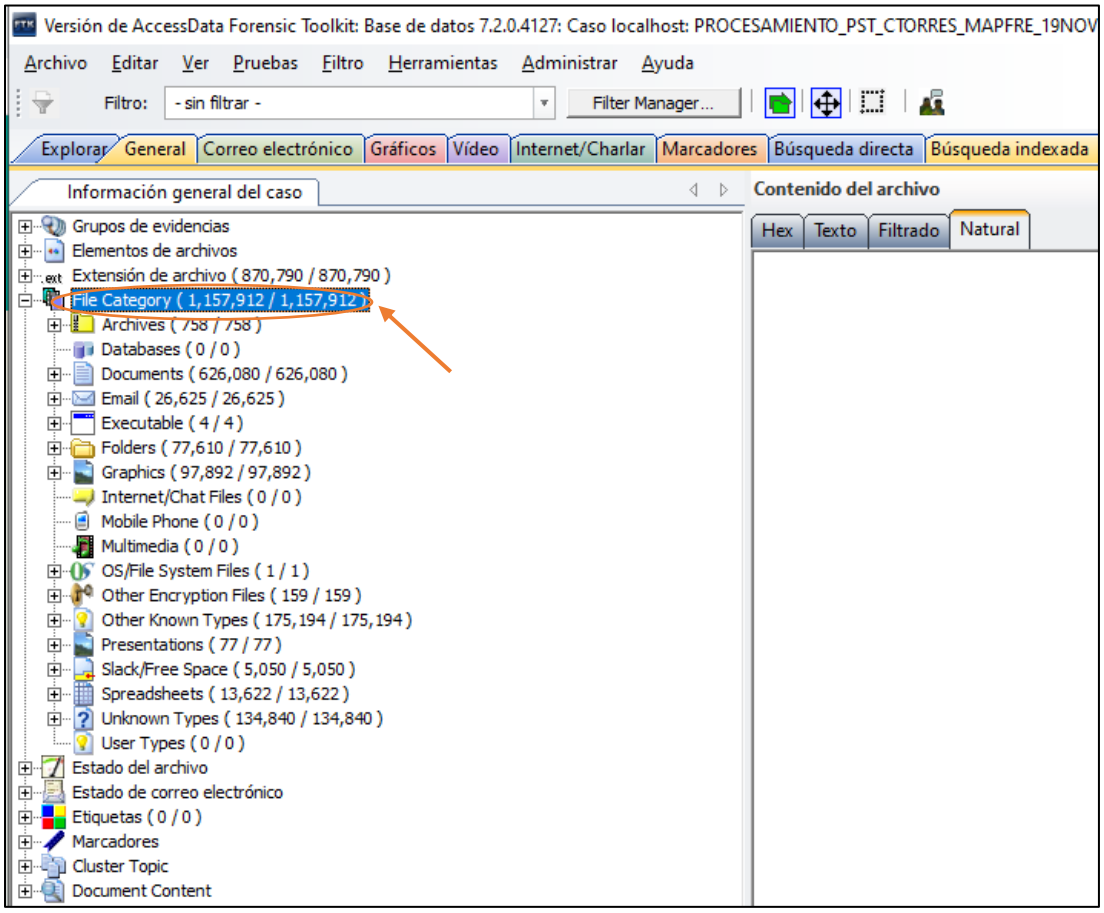


Ilustración 38 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico ctorres@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO CARMENZA GUATAVITA TORRES → CTORRES@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos,

en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico ctorres@mapfre.com.co asignada a Carmenza GUATAVITA TORRES para el desarrollo de sus funciones, iniciando el día el **23** de noviembre del presente año con una duración aproximada de Un (1) día calendario, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Diez mil setecientos ochenta y ocho (10.788)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

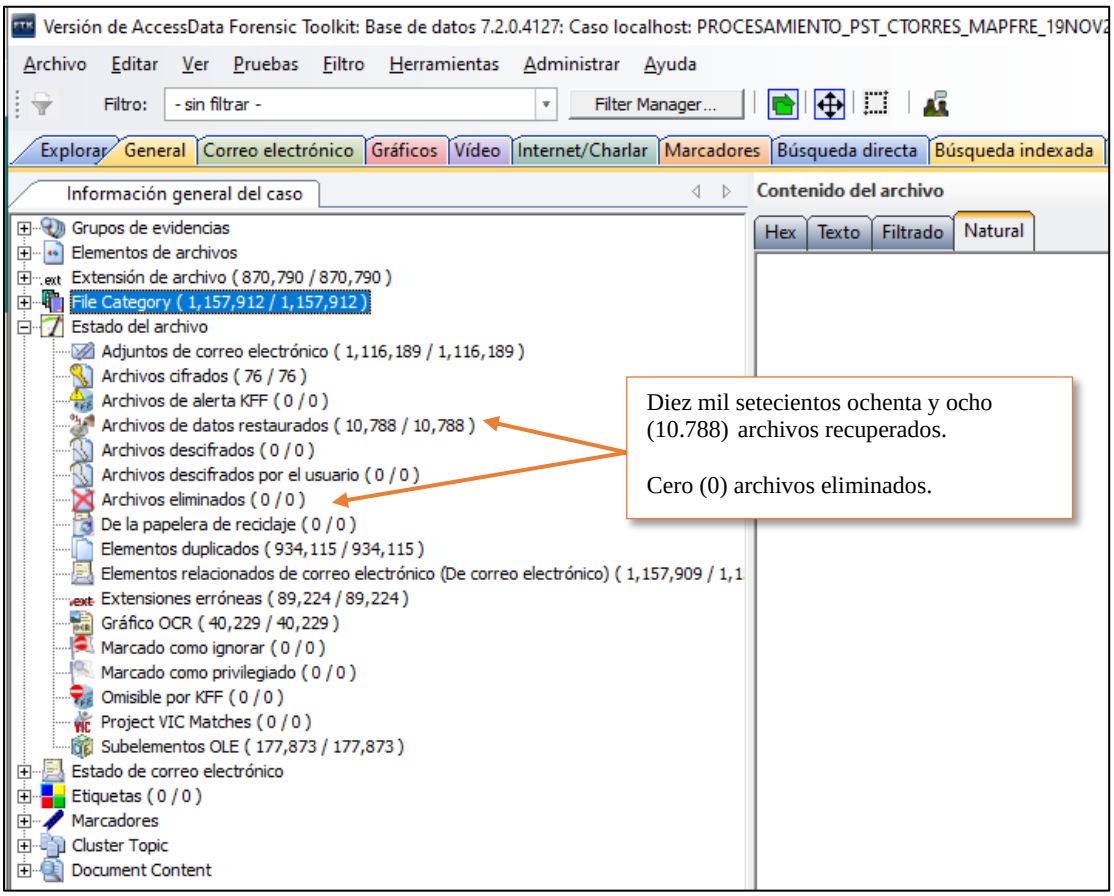


ilustración 39 Total de archivos recuperados en la cuenta de correo electrónico ctorres@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Un millón ciento cincuenta y siete mil novecientos doce**

(1.157.912) archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

- **RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO CTORRES@MAPFRE.COM.CO.**

Luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico ctorres@mapfre.com.co asignada a **Carmenza GUATAVITA TORRES** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	758
2	Documentos	626.080
3	Correo Electrónico	26.625
4	Ejecutables	4
5	Carpetas	77.610
6	Gráficos	97.892
7	Archivos del sistema	1
8	Otros archivos encriptados	159
9	Otros archivos desconocidos	175.194
10	Presentaciones	77
11	Espacio libre	5.050
12	Hojas de cálculo	13.622
13	Tipos de archivos desconocidos	134.840
TOTAL		**1.157.912**

Tabla 10 Información buscada evidencia 004_CTORRES, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Un millón ciento cincuenta y siete mil novecientos doce (1.157.912).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Un millón ciento dieciséis mil ciento ochenta y nueve (1.116.189) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Setenta y seis (76) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Diez mil setecientos ochenta y ocho (10.788) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Novecientos treinta y cuatro mil ciento quince (934.115) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **n millón ciento cincuenta y siete mil novecientos nueve (1.157.909) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Ochenta y nueve mil doscientos veinticuatro (89.224) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Cuarenta mil doscientos veintinueve (40.229) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Ciento setenta y siete mil ciento ochenta y tres (177.183) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico ctorres@mapfre.com.co asignada a **Carmenza GUATAVITA** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

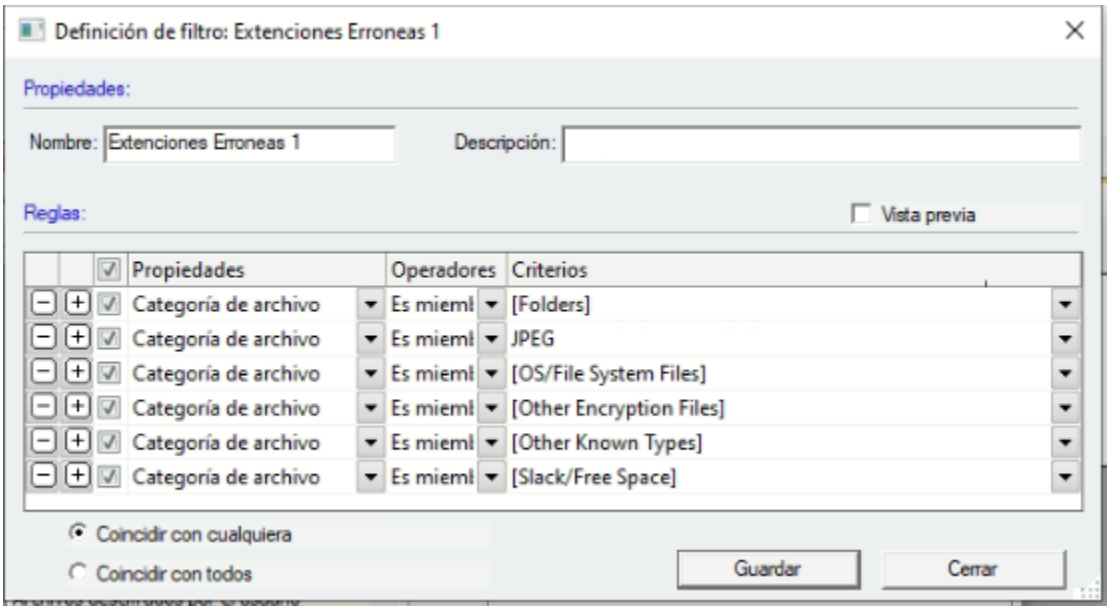


Ilustración 40 Filtro para excluir las extensiones erróneas.

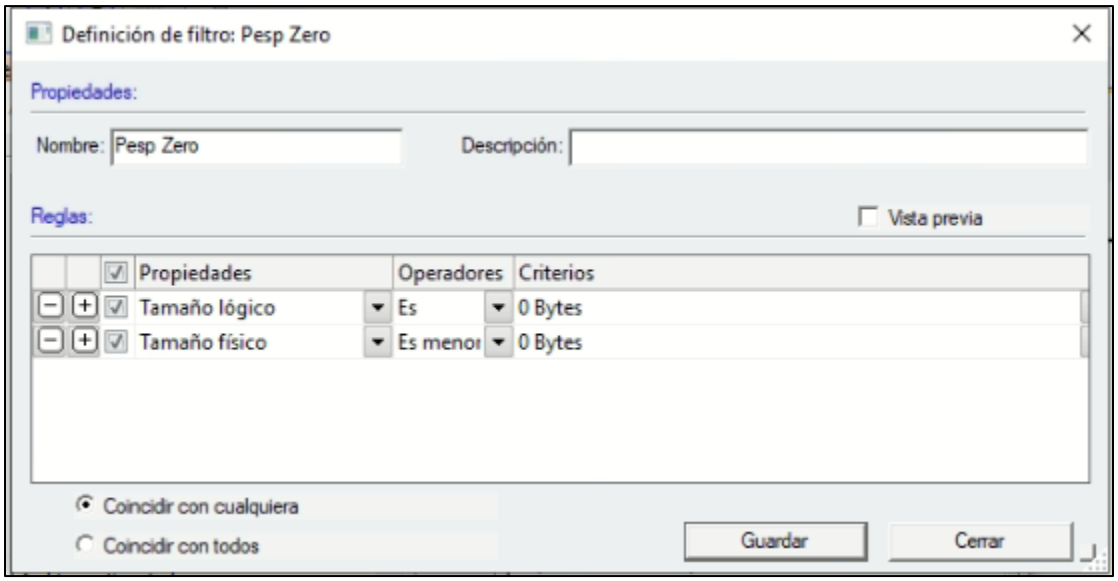


Ilustración 41 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

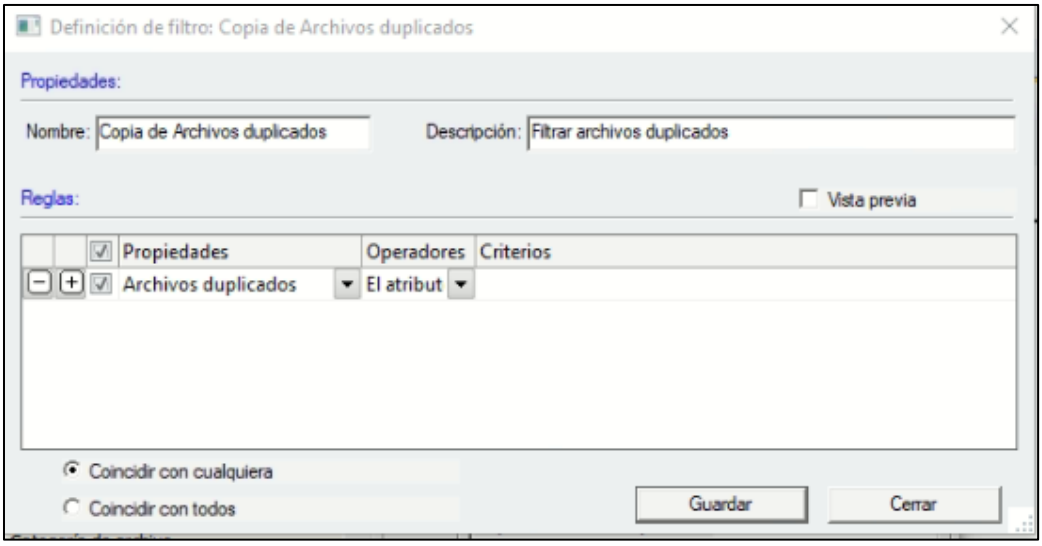
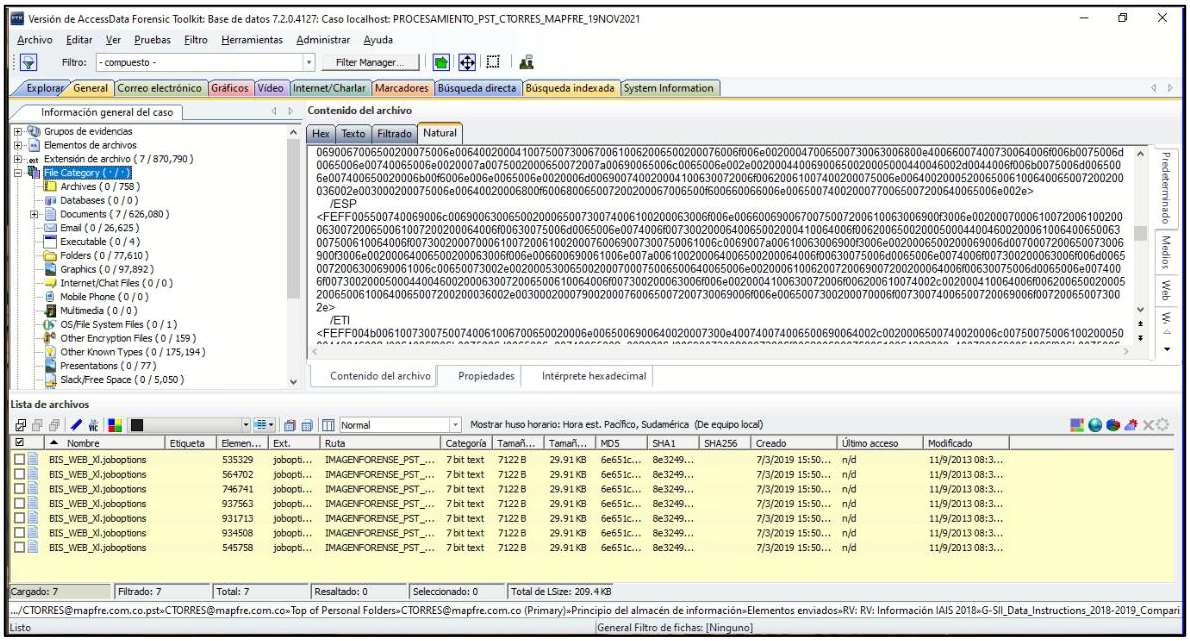


Ilustración 42 Filtro para excluir los archivos duplicados.

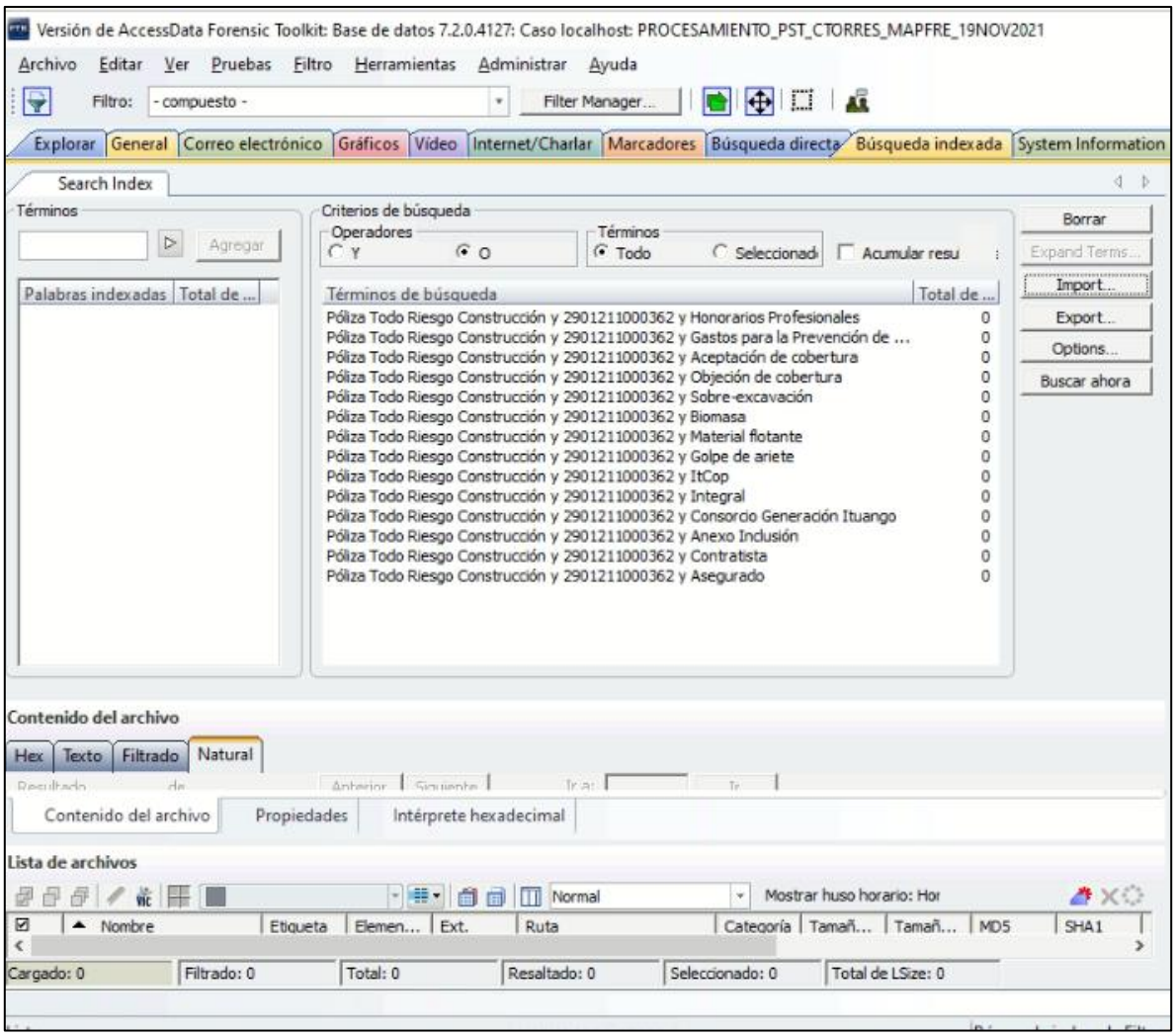
Tras aplicar los filtros anteriormente mencionados, se logra reducir muestra de información a **Siete (7)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo **ctorres@mapfre.com.co** asignada a **Carmenza GUATAVITA TORRES** para el desarrollo de sus funciones.

5. **Buzón de correo electrónico dagomez@mapfre.com.co.**

El día 19 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **DAGOMEZ**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

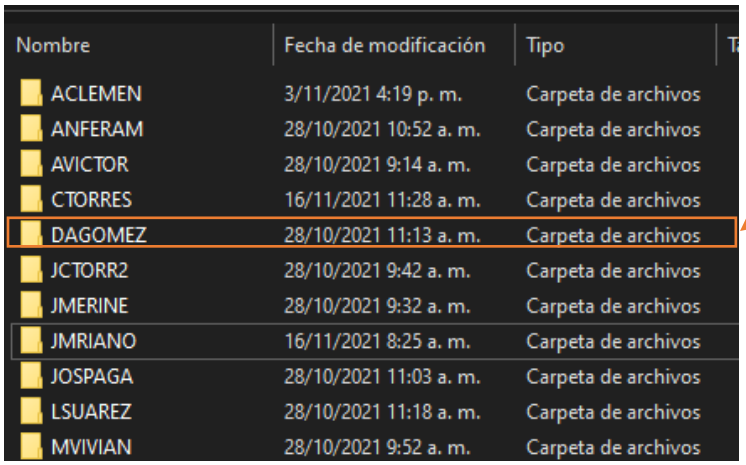


Ilustración 43 Visualización carpeta DAGOMEZ

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **DAGOMEZ** identificada dentro del disco duro como se observa en las siguientes imágenes:

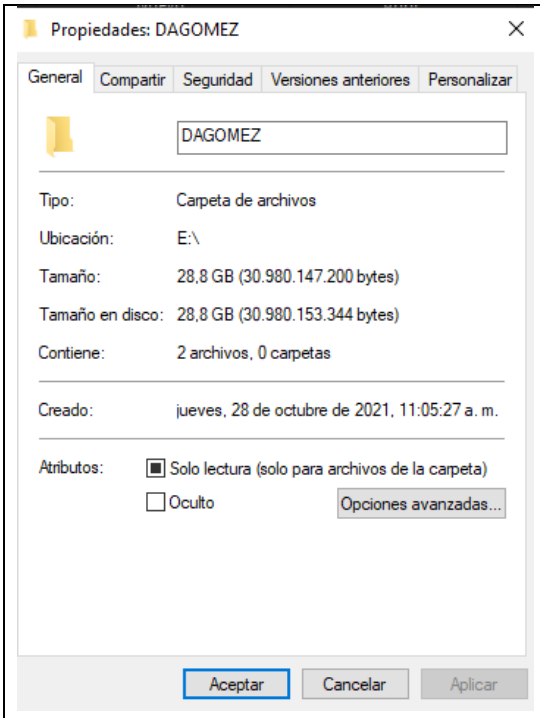


Ilustración 44 Propiedades de la carpeta DAGOMEZ visto desde el Disco Duro.

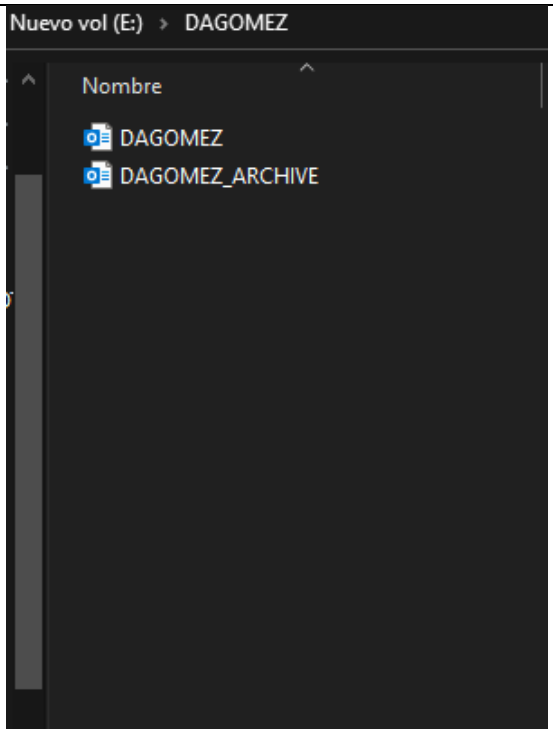


Ilustración 45 Contenido de la carpeta DAGOMEZ visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**dagomez@mapfre.com.co.**" asignado a

David GÓMEZ JIMÉNEZ para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **14:55:13** y culminando el mismo de forma satisfactoria a las **15:05:30**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_19NOV2021
Número de prueba: 005_DAGOMEZ
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO DAGOMEZ@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad1:
[Custom Content Sources]
K::K:\|DAGOMEZ|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 334e31abcf31639ee1a251289be3ac33
SHA1 checksum: b906341ba507626503910b9f85783c073d48a96d

Image information:
Acquisition started: Fri Nov 19 14:55:13 2021
Acquisition finished: Fri Nov 19 15:01:59 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\5.DAGOMEZ\IMAGENFORENSE_PST_DAGOMEZ_MAPFRE_19NOV2021.ad20

Image Verification Results:
Verification started: Fri Nov 19 15:01:59 2021
Verification finished: Fri Nov 19 15:05:30 2021
MD5 checksum: 334e31abcf31639ee1a251289be3ac33 : verified
SHA1 checksum: b906341ba507626503910b9f85783c073d48a96d : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB,** el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**dagomez@mapfre.com.co.**" asignado a **David GÓMEZ JIMÉNEZ** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 46 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO DAGOMEZ@MAPFRE.COM.CO."**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas MAPFRE SEGUROS GENERALES DE COLOMBIA S.A. para la cuenta de correo electrónico dagomez@mapfre.com.co asignada David GÓMEZ JIMÉNEZ para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
5	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	David GÓMEZ JIMÉNEZ → dagomez@mapfre.com.co	ad1	28.8 GB
TOTAL					**28.8 GB**

Tabla 11 Detalle del buzón de correo electrónico asignado dagomez@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico dagomez@mapfre.com.co asignado a David GÓMEZ JIMÉNEZ para el desarrollo de sus funciones **aloja** un total de **28.8 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Cuatrocientos ochenta y cinco mil setecientos diecinueve (485.719)** archivos (incluyendo carpetas), como se observa a continuación.

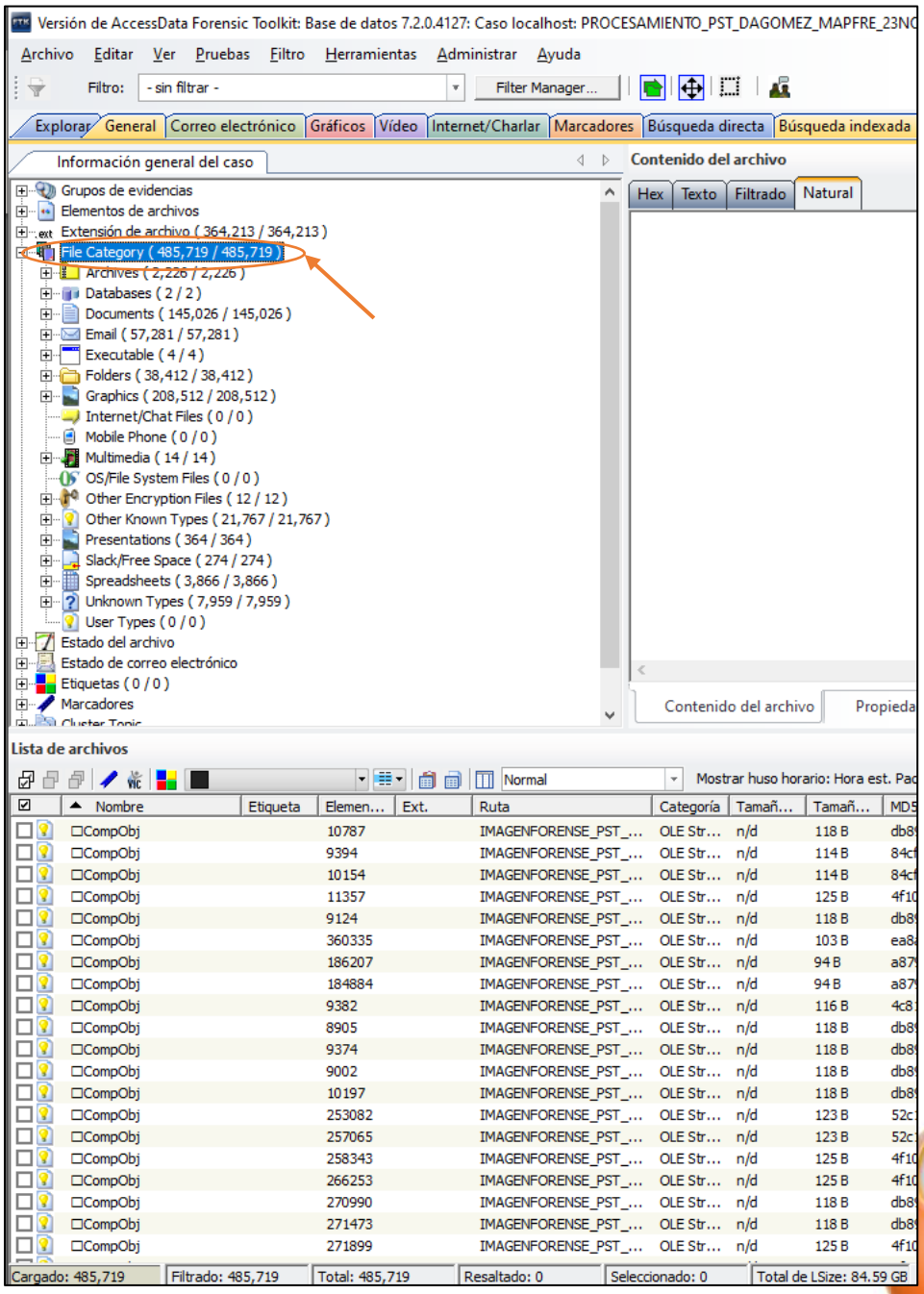


Ilustración 47 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico dagomez@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JOSÉ FERNANDO PALACIO GALLÓN → DAGOMEZ@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico dagomez@mapfre.com.co asignado a **David GÓMEZ JIMÉNEZ,** iniciando el día el **23** de noviembre del presente año con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Ciento diecinueve mil setecientos cuarenta y seis (119.746)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:



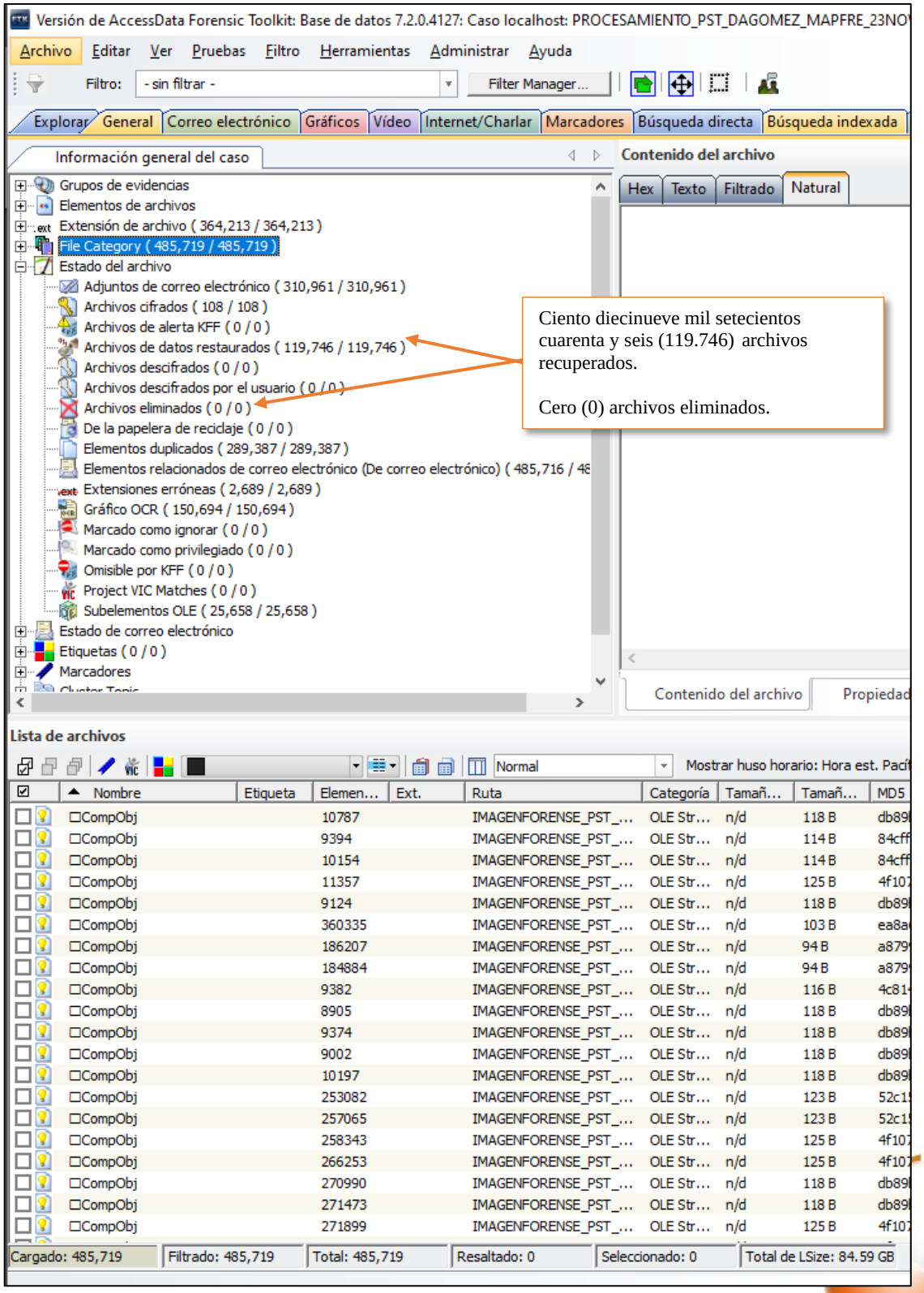


ilustración 48 Total de archivos recuperados en la cuenta de correo electrónico dagomez@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Cuatrocientos ochenta y cinco mil setecientos diecinueve (485.719)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO DAGOMEZ@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico dagomez@mapfre.com.co asignado a David GÓMEZ JIMÉNEZ para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	2.226
2	Bases de Datos	2
3	Documentos	145.026
4	Correo Electrónico	57.281
5	Ejecutables	4
6	Carpetas	38.412
7	Gráficos	208.512
8	Multimedia	14
9	Otros archivos encriptados	12
10	Otros archivos desconocidos	21.767
11	Presentaciones	364
12	Espacio libre	274
13	Hojas de cálculo	3.866
14	Tipos de archivos desconocidos	7.959
TOTAL		**485.719**

Tabla 12 Información buscada evidencia 005_DAGOMEZ, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Cuatrocientos ochenta y cinco mil setecientos diecinueve (485.719)**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Trescientos diez mil novecientos sesenta y un (310.961) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **ciento ocho (108) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Ciento diecinueve mil setecientos cuarenta y seis (119.746) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Doscientos ochenta y nueve mil trescientos ochenta y siete (289.387) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Cuatrocientos ochenta y cinco mil setecientos dieciséis (485.716) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Dos mil seiscientos ochenta y nueve (2.689) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Ciento cincuenta mil seiscientos noventa y cuatro (150.694) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Veinticinco mil seiscientos cincuenta y ocho (25.658) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico dagomez@mapfre.com.co asignado a **David GÓMEZ JIMÉNEZ** para el desarrollo de sus funciones el equipo de ADALID CORP

procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

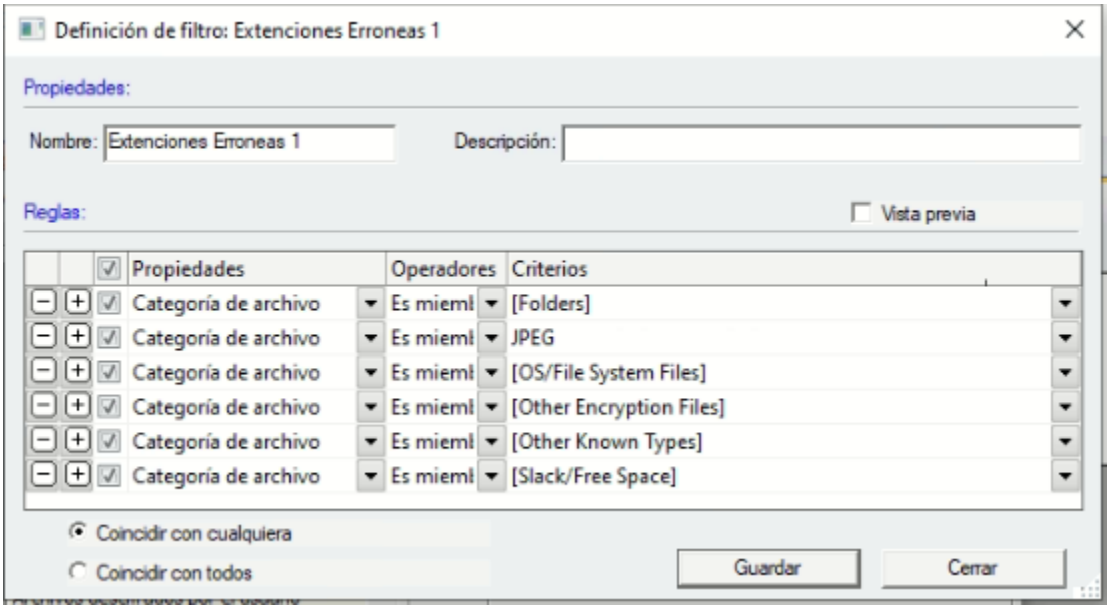


Ilustración 49 Filtro para excluir las extensiones erróneas.

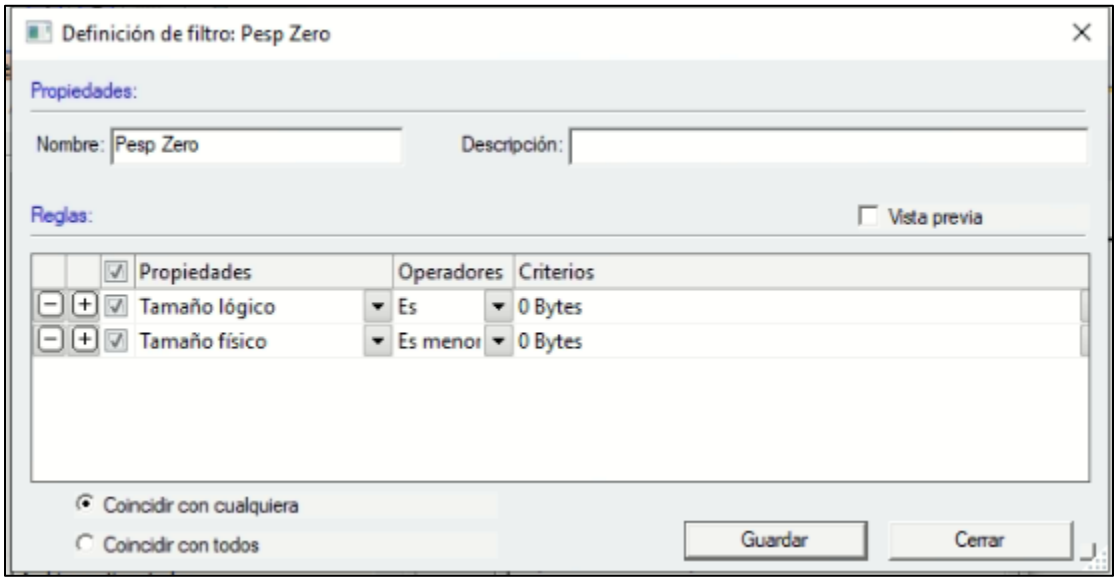


Ilustración 50 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

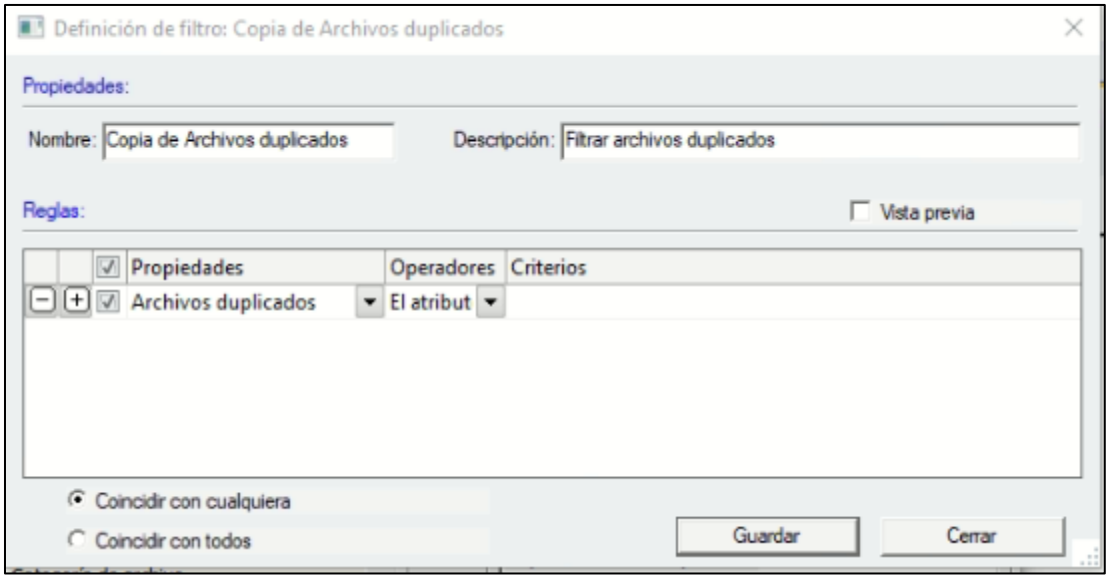


Ilustración 51 Filtro para excluir los archivos duplicados.

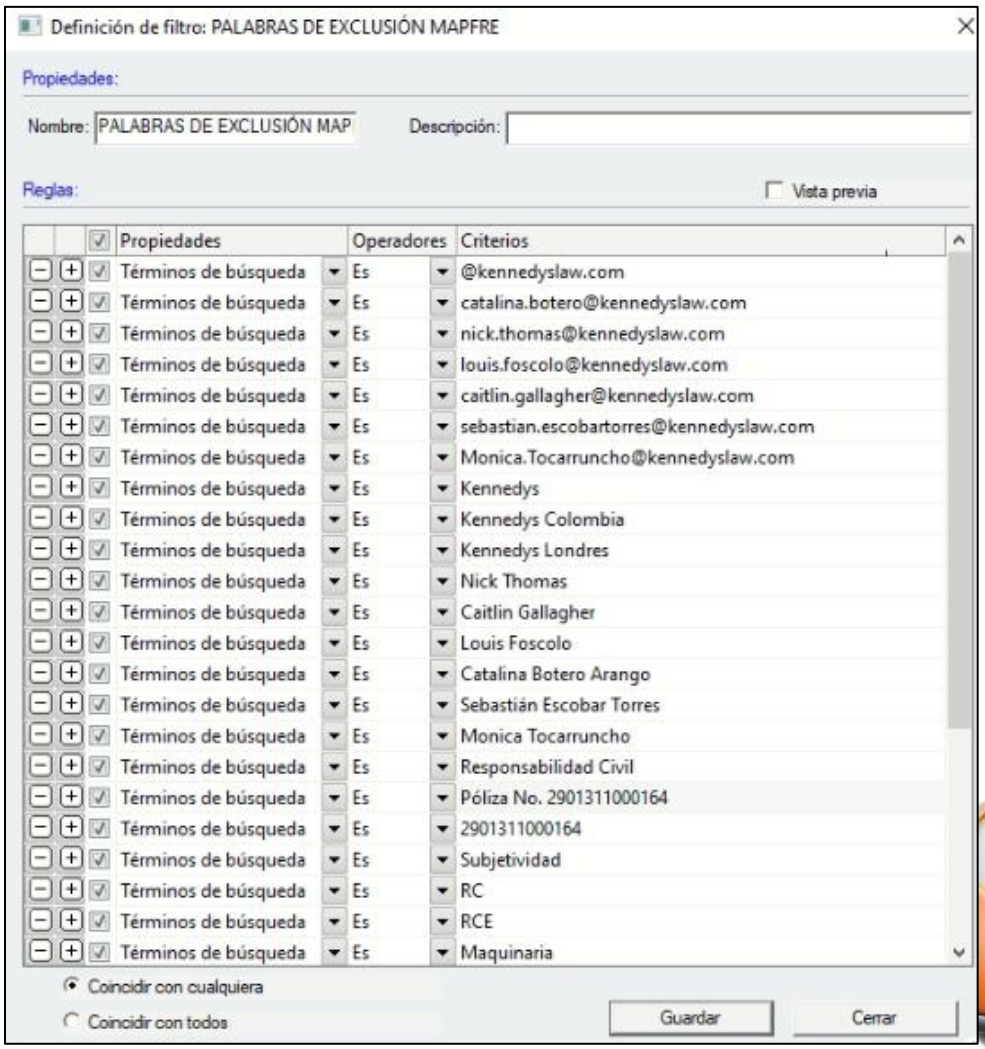


Ilustración 52 Filtro para excluir los archivos suministrado por MAPFRE - 1.

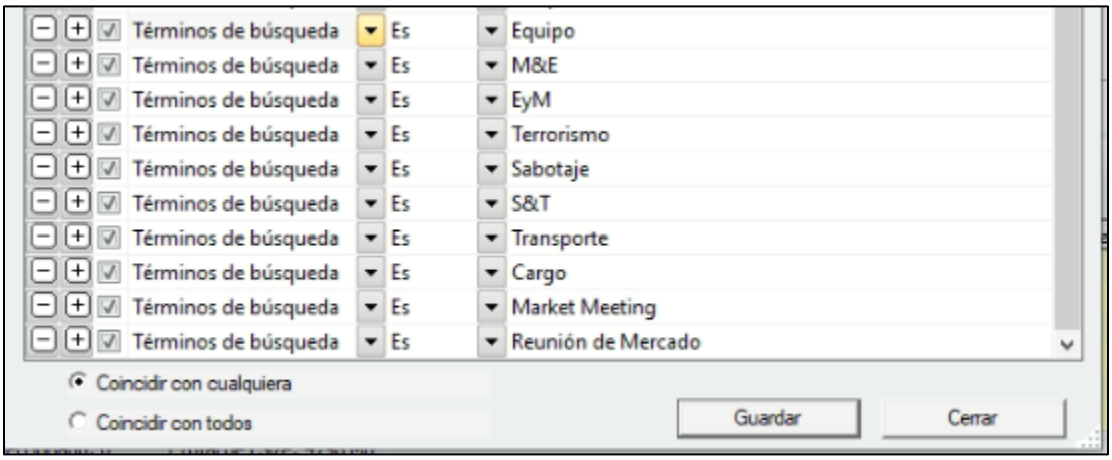
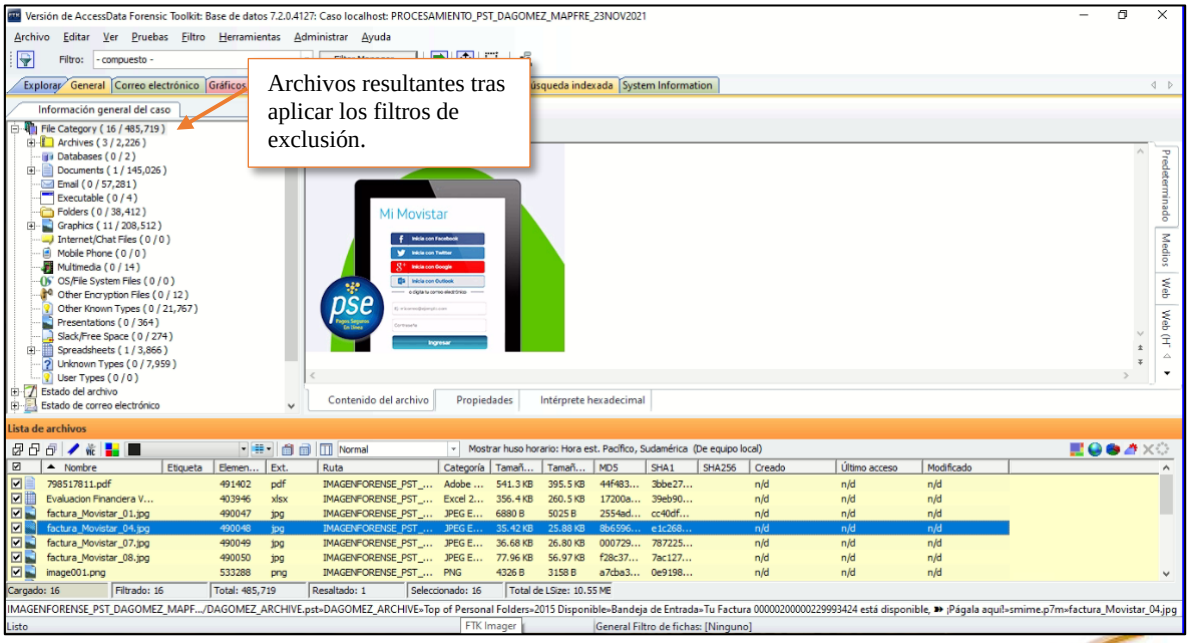


Ilustración 53 Filtro para excluir los archivos suministrado por MAPFRE - 2.

Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Dieciséis (16)** registros como se observa en la siguiente imagen:

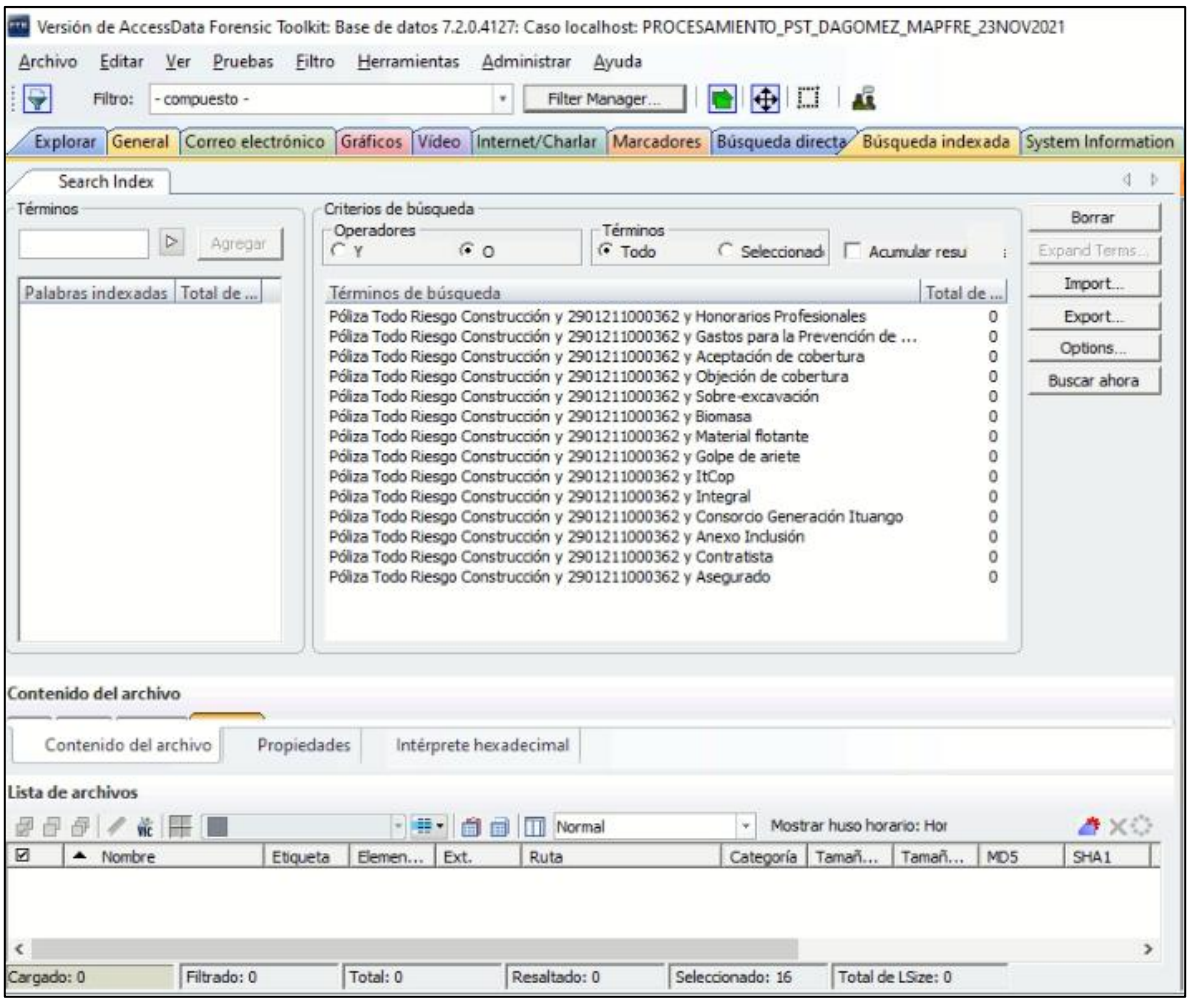


Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión

7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo dagomez@mapfre.com.co asignado a **David GÓMEZ JIMÉNEZ** para el desarrollo de sus funciones.

6. Buzón de correo electrónico lsuarez@mapfre.com.co.

El día 19 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **LSUAREZ**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

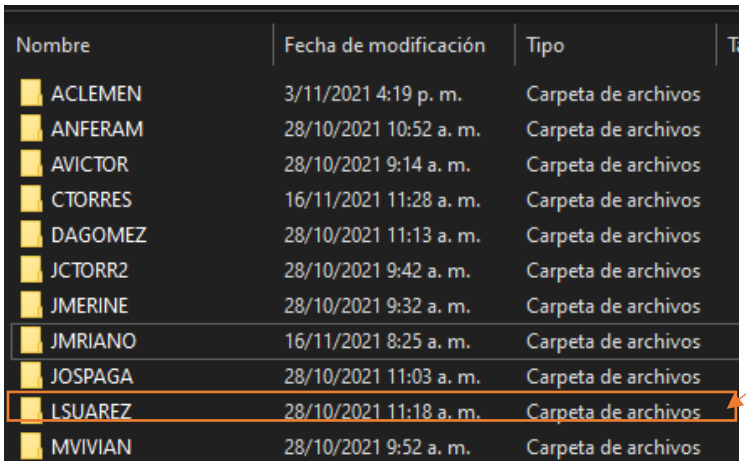


Ilustración 54 Visualización carpeta LSUAREZ

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **LSUAREZ** identificada dentro del disco duro como se observa en las siguientes imágenes:

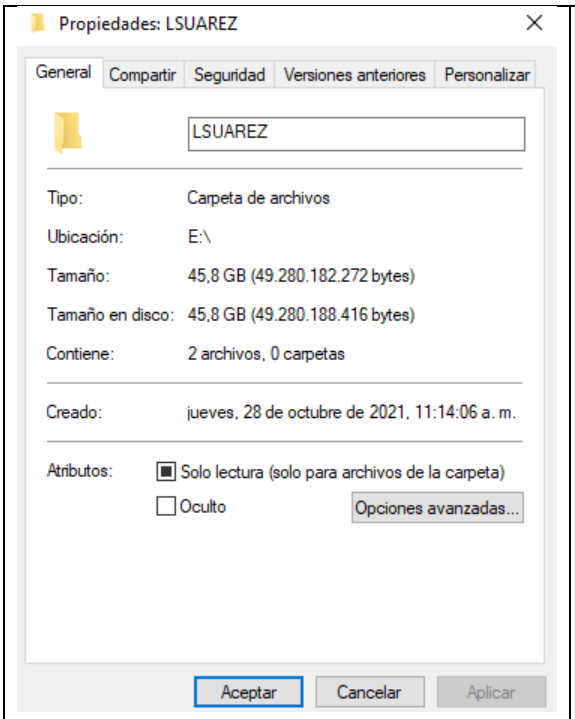


Ilustración 55 Propiedades de la carpeta LSUAREZ visto desde el Disco Duro.

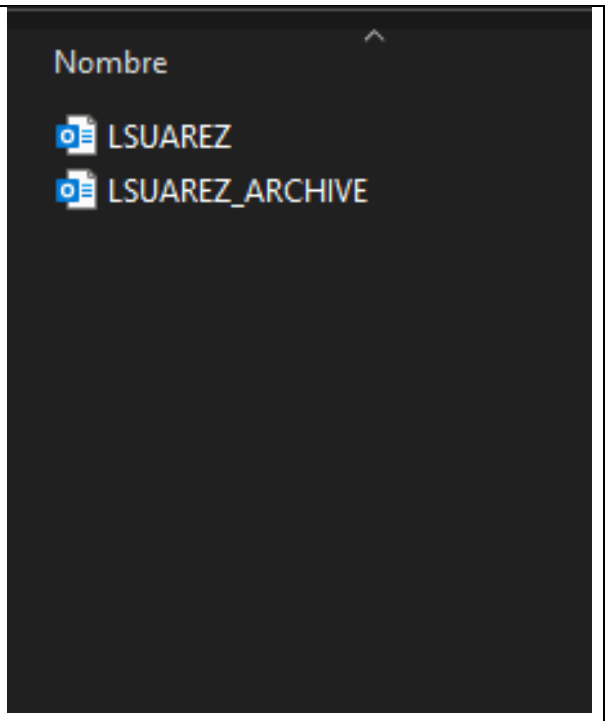


Ilustración 56 Contenido de la carpeta LSUAREZ visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**lsuarez@mapfre.com.co.**" asignado a **Luis Alberto SUÁREZ URREGO** para el cumplimiento de sus funciones los peritos

informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **15:08:28** y culminando el mismo de forma satisfactoria a las **15:24:51**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_19NOV2021
Número de prueba: 006_LSUAREZ
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO LSUAREZ@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad1:
[Custom Content Sources]
K::K:\|LSUAREZ|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 36a5dc50b305d9a816109d85d035ede9
SHA1 checksum: 8734e3612bd6e58f70e833fd1a991fe5b9178b4d

Image information:
Acquisition started: Fri Nov 19 15:08:28 2021
Acquisition finished: Fri Nov 19 15:19:44 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad29

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad30

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad31

I:\EVIDENCIA_MAPFRE_2\6.LSUAREZ\IMAGENFORENSE_PST_LSUAREZ_MAPFRE_19NOV2021.ad32

Image Verification Results:
Verification started: Fri Nov 19 15:19:50 2021
Verification finished: Fri Nov 19 15:24:51 2021
MD5 checksum: 36a5dc50b305d9a816109d85d035ede9 : verified
SHA1 checksum: 8734e3612bd6e58f70e833fd1a991fe5b9178b4d : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:





Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**lsuarez@mapfre.com.co.**" asignado a **Luis Alberto SUÁREZ URREGO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 57 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO LSUAREZ@MAPFRE.COM.CO."**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo

electrónico lsuarez@mapfre.com.co asignada **Luis Alberto SUÁREZ URREGO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
6	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Luis Alberto SUÁREZ URREGO → lsuarez@mapfre.com.co	ad1	45.8 GB
TOTAL					**45.8 GB**

Tabla 13 Detalle del buzón de correo electrónico asignado lsuarez@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico lsuarez@mapfre.com.co asignado a **Luis Alberto SUÁREZ URREGO** para el desarrollo de sus funciones **aloja** un total de **45.8 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Setecientos treinta y ocho mil doscientos setenta y cuatro (738.274)** archivos (incluyendo carpetas), como se observa a continuación.

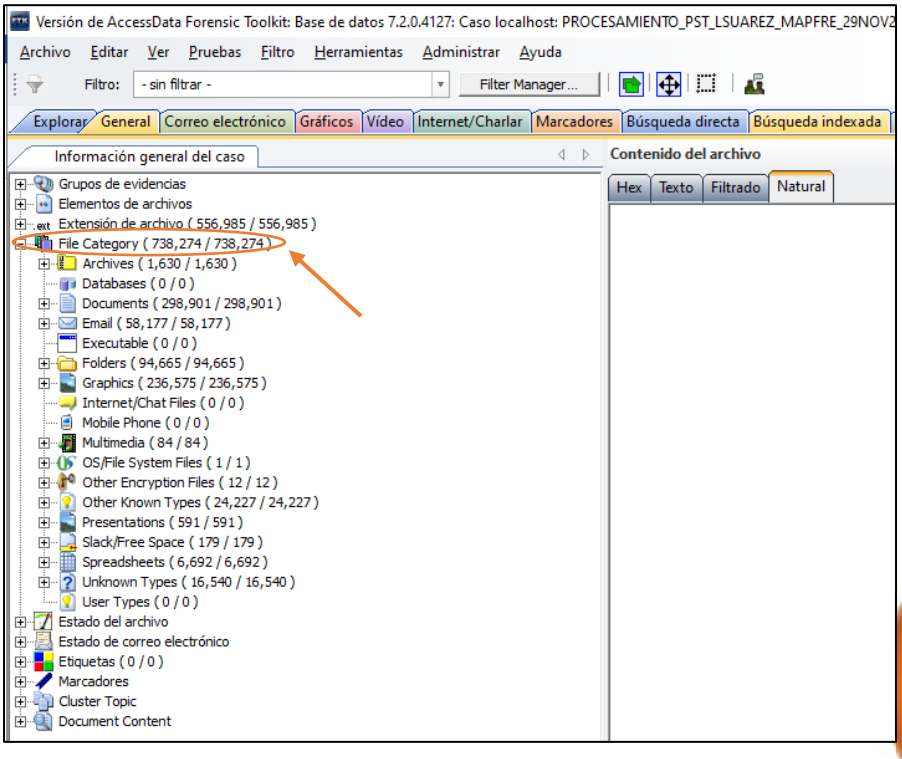


Ilustración 58 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico lsuarez@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO LUIS ALBERTO SUÁREZ URREGO → LSUAREZ@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico lsuarez@mapfre.com.co asignado a **Luis Alberto SUÁREZ URREGO**, iniciando el día el **29** de noviembre del presente año con una duración aproximada de Un (7) día calendario, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Ciento treinta y nueve mil ciento cincuenta y ocho (139.158)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

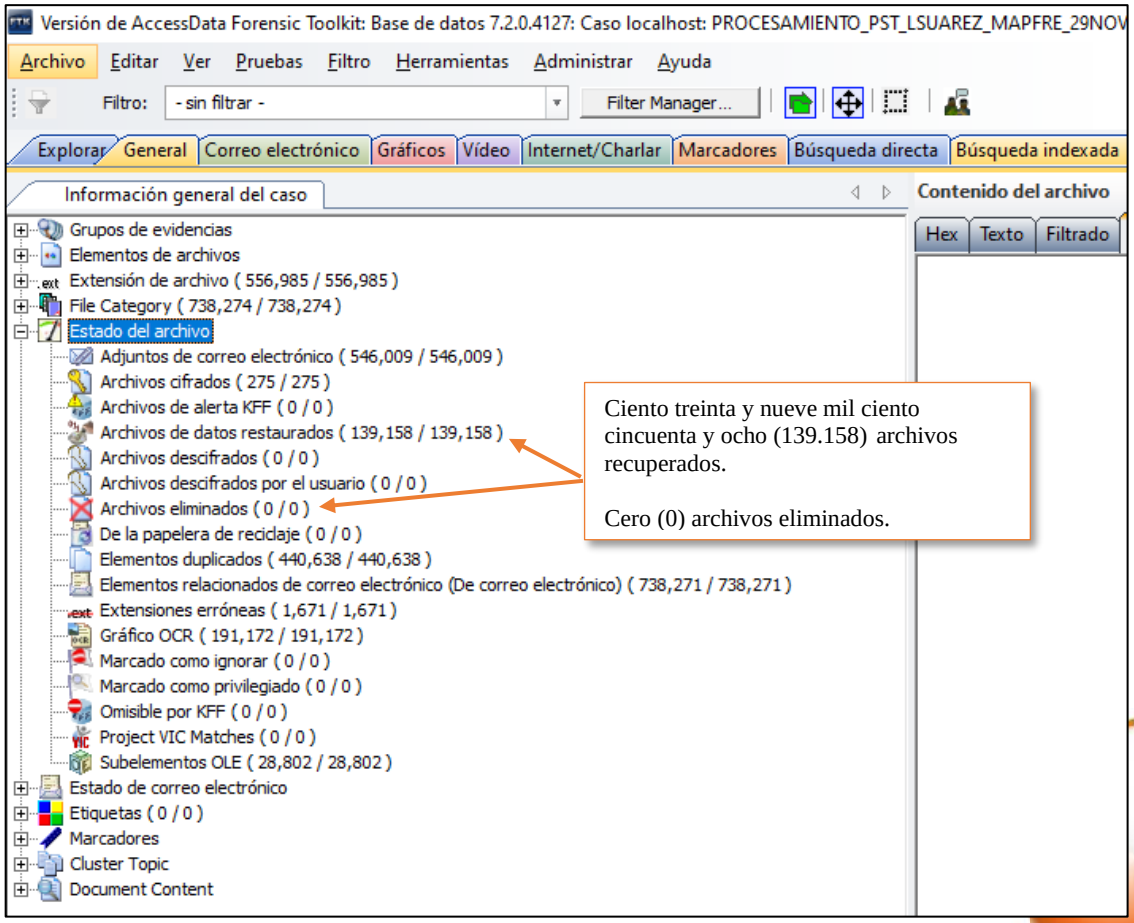


ilustración 59 Total de archivos recuperados en la cuenta de correo electrónico lsuarez@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Setecientos treinta y ocho mil doscientos setenta y cuatro (738.274)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO LSUAREZ@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico lsuarez@mapfre.com.co asignado a **Luis Alberto SUÁREZ URREGO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1.630
2	Documentos	298.901
3	Correo Electrónico	58.177
4	Carpetas	94.665
5	Gráficos	236.575
6	Multimedia	84
7	Archivos del sistema	1
8	Otros archivos encriptados	12
9	Otros archivos desconocidos	24.227
10	Presentaciones	591
11	Espacio libre	179
12	Hojas de cálculo	6.692
13	Tipos de archivos desconocidos	16.540
TOTAL		**738.274**

Tabla 14 Información buscada evidencia 006_LSUAREZ, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Setecientos treinta y ocho mil doscientos setenta y cuatro (738.274).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Quinientos cuarenta y seis mil nueve (546.009) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Doscientos setenta y cinco (275) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Ciento treinta y nueve mil ciento cincuenta y ocho (139.158) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Cuatrocientos cuarenta mil seiscientos treinta y ocho (440.638) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Setecientos treinta y ocho mil doscientos setenta y un (738.271) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Mil seiscientos setenta y un (1.671) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Ciento noventa y un mil ciento setenta y dos (191.172) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Veintiocho mil ochocientos dos (28.802) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo lsuarez@mapfre.com.co asignado **a Luis Alberto SUÁREZ URREGO** para el desarrollo de sus funciones el equipo de ADALID CORP procede a

aplicar filtros para excluir la información que no se requiere de la siguiente manera:

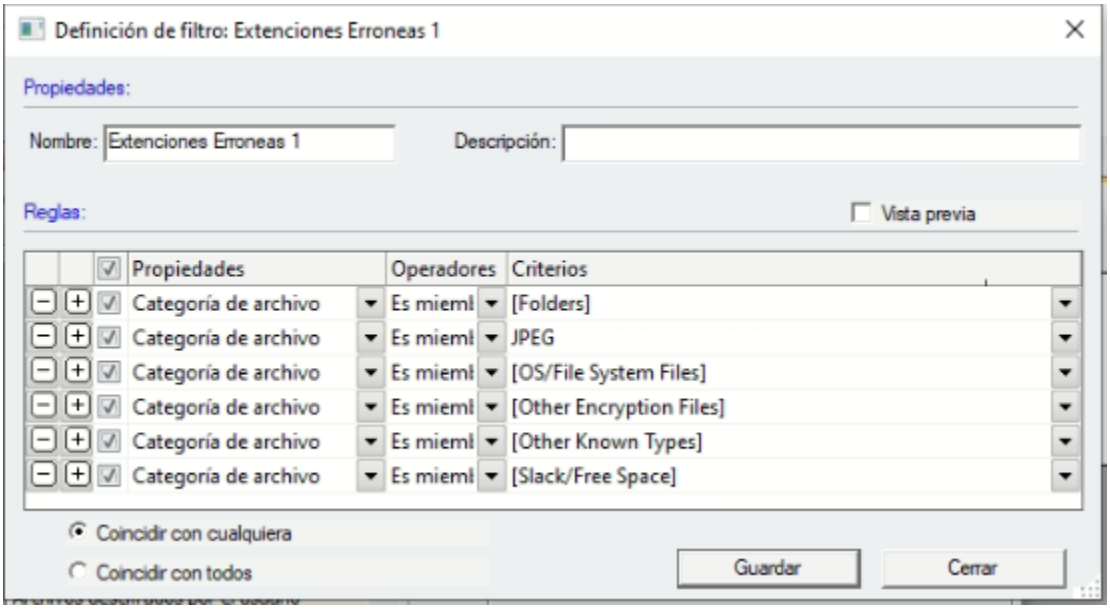


Ilustración 60 Filtro para excluir las extensiones erróneas.

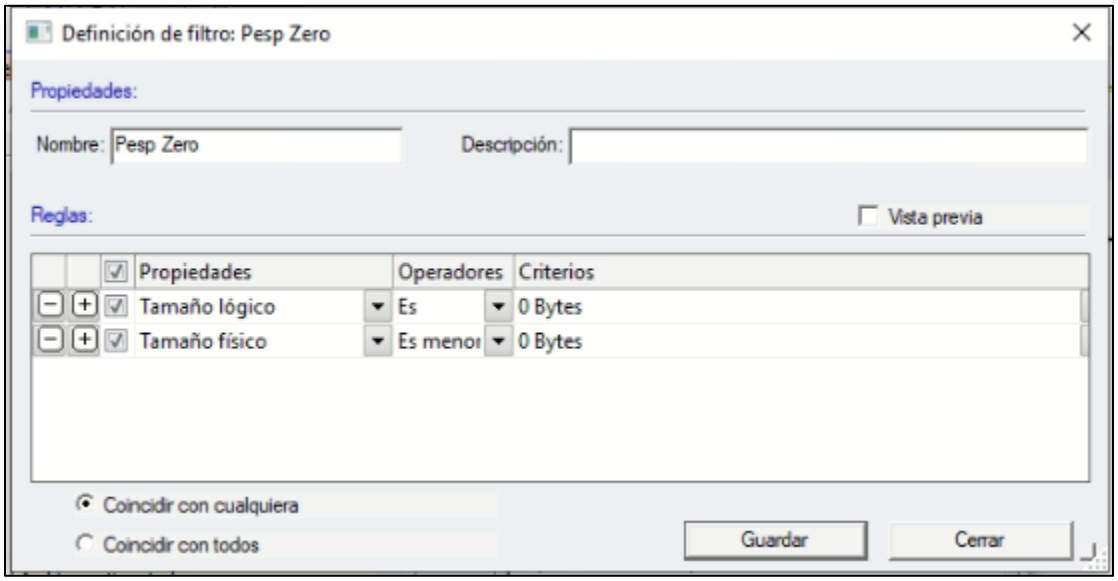


Ilustración 61 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

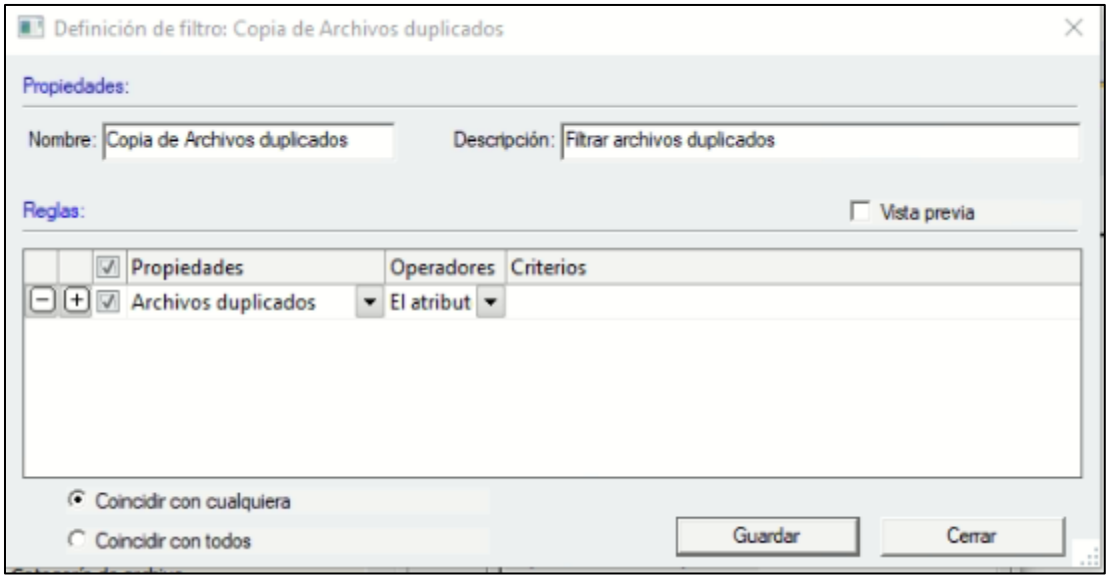


Ilustración 62 Filtro para excluir los archivos duplicados.

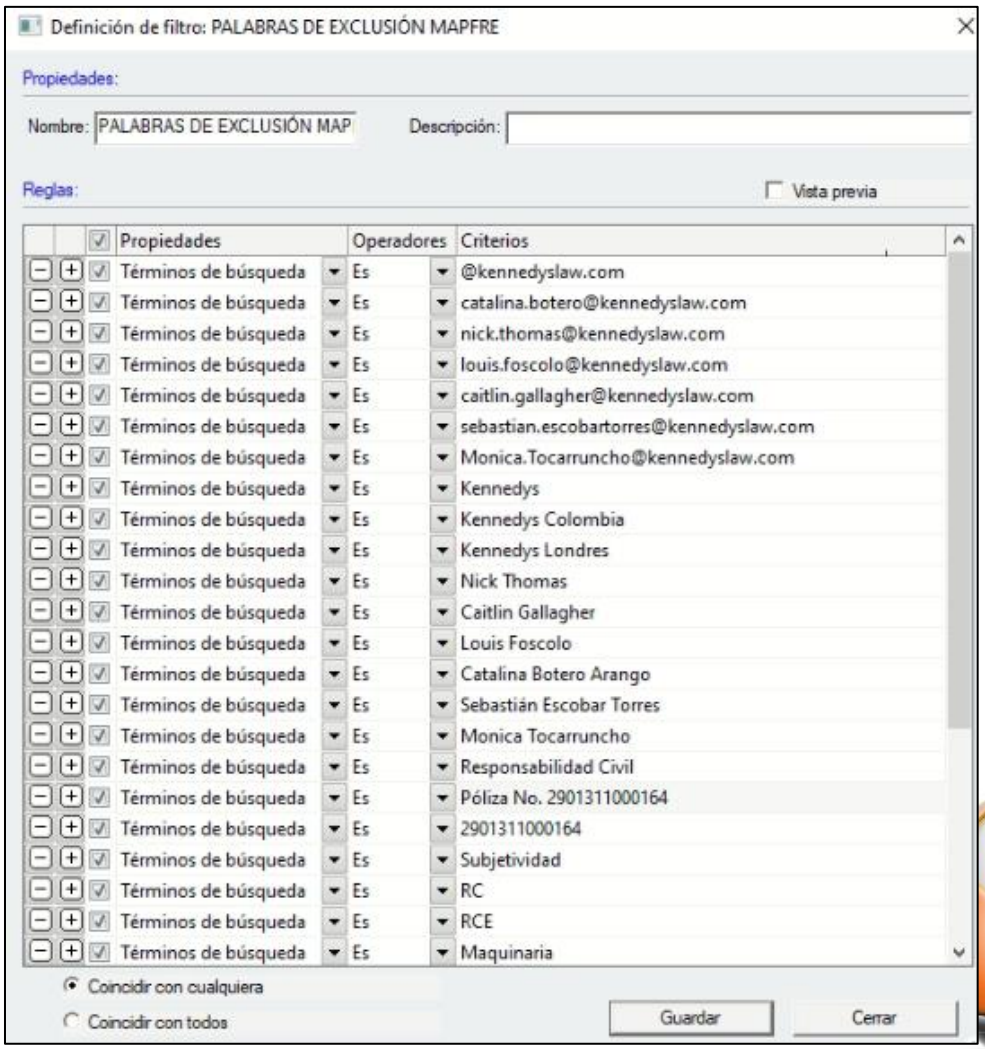


Ilustración 63 Filtro para excluir los archivos suministrado por MAPFRE - 1.

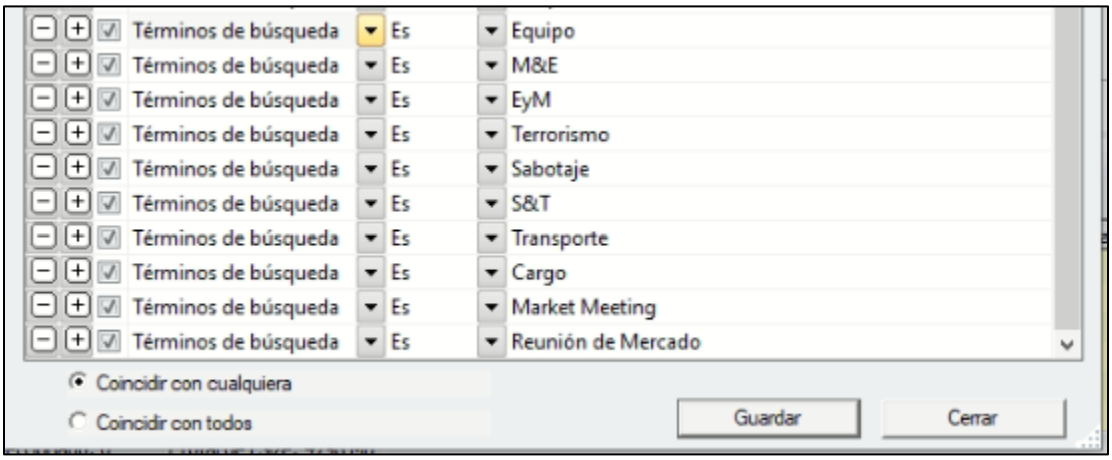
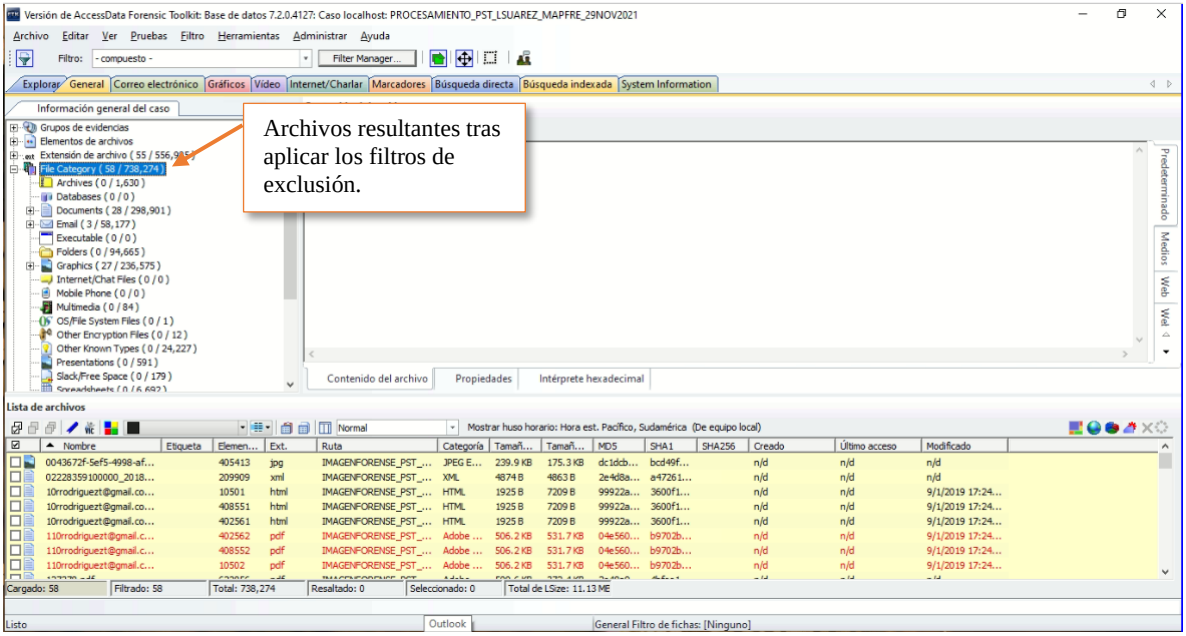


Ilustración 64 Filtro para excluir los archivos suministrado por MAPFRE - 2.

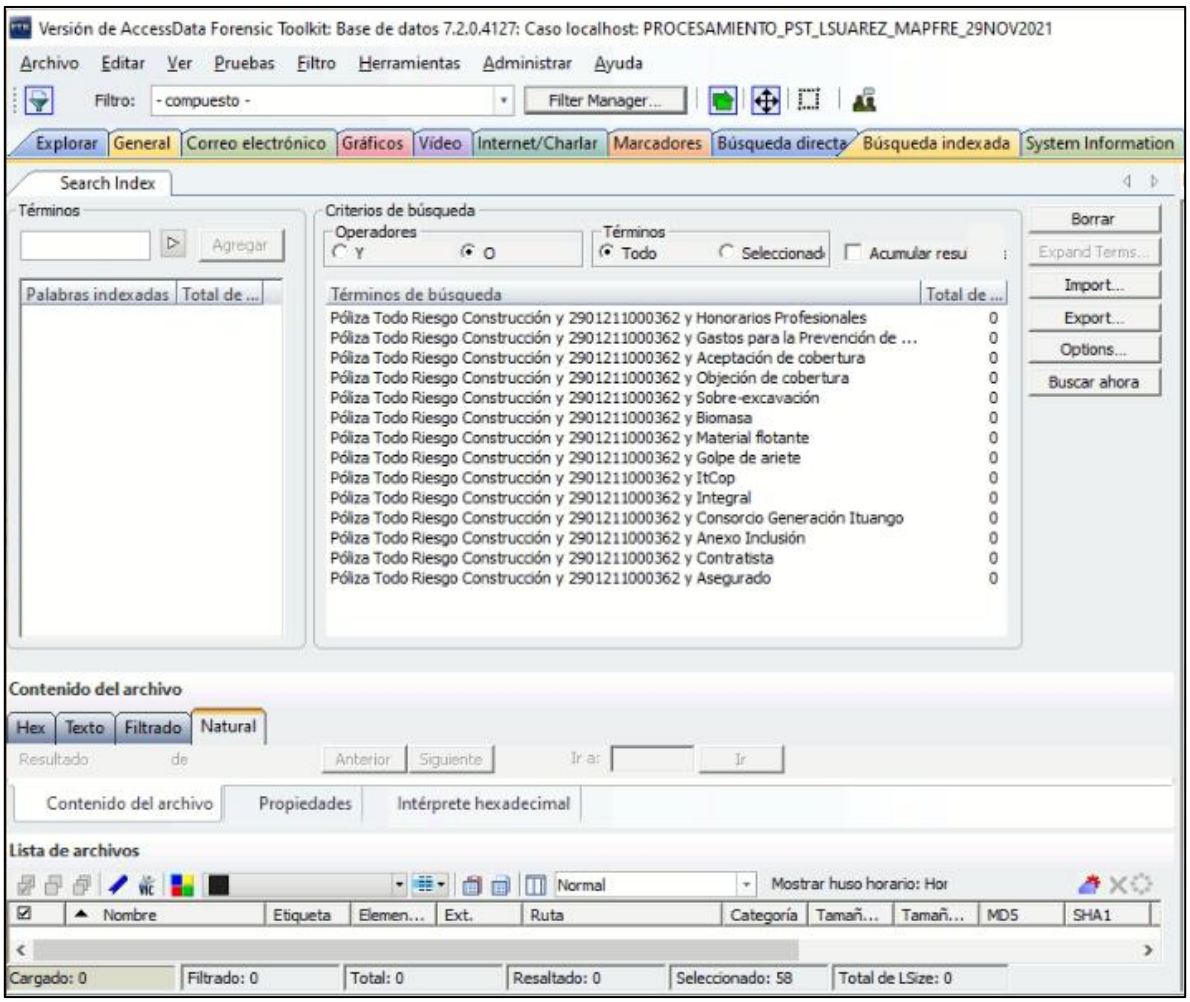
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Cincuenta y ocho (58)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo lsuarez@mapfre.com.co asignado a **Luis Alberto SUÁREZ URREGO** para el desarrollo de sus funciones.

7. Buzón de correo electrónico anferam@mapfre.com.co.

El día 19 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **ANFERAM**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

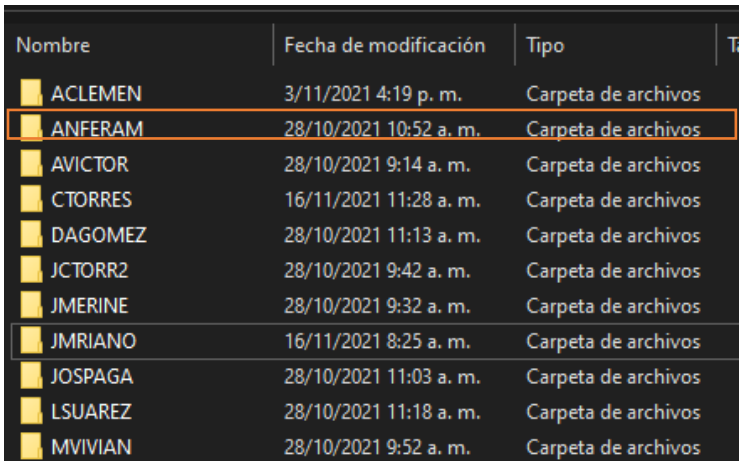


Ilustración 65 Visualización carpeta ANFERAM.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **ANFERAM** identificada dentro del disco duro como se observa en las siguientes imágenes:

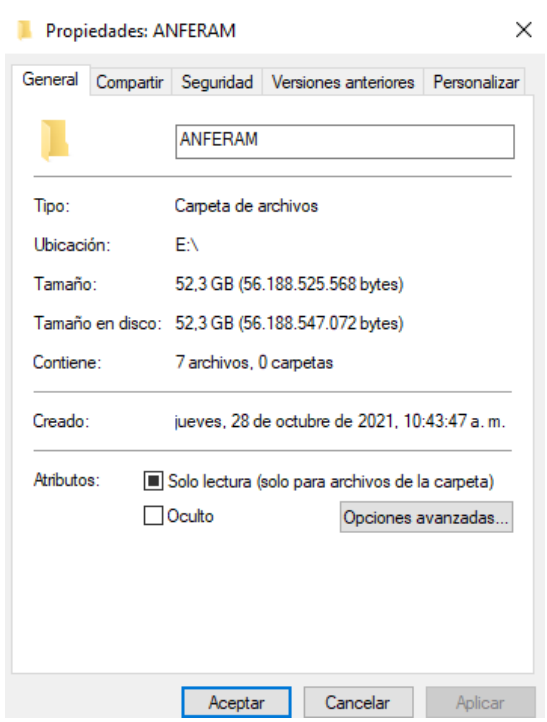


Ilustración 66 Propiedades de la carpeta ANFERAM visto desde el Disco Duro.

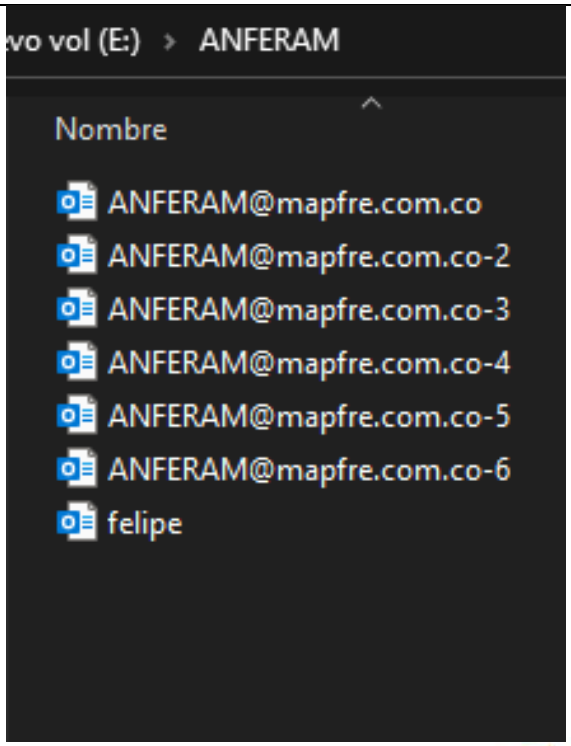


Ilustración 67 Contenido de la carpeta ANFERAM visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**anferam@mapfre.com.co.**" asignado a

Andrés Felipe RAMÍREZ para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **15:34:32** y culminando el mismo de forma satisfactoria a las **15:54:44**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_19NOV2021
Número de prueba: 007_ANFERAM
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ANFERAM@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad1:
[Custom Content Sources]
K::K:\ | ANFERAM | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: d534e4492f211de5338af83951c38c46
SHA1 checksum: 9d747d52eabeadd3571ddf2033cba1cc4c2c6bd7

Image information:
Acquisition started: Fri Nov 19 15:34:32 2021
Acquisition finished: Fri Nov 19 15:49:39 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad29 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad30 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad31 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad32 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad33 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad34 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad35 I:\EVIDENCIA_MAPFRE_2\7.ANFERAM\IMAGENFORENSE_PST_ANFERAM_MAPFRE_19NOV2021.ad36 Image Verification Results: Verification started: Fri Nov 19 15:49:39 2021 Verification finished: Fri Nov 19 15:54:44 2021 MD5 checksum: d534e4492f211de5338af83951c38c46 : verified SHA1 checksum: 9d747d52eabeadd3571ddf2033cba1cc4c2c6bd7 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**anferam@mapfre.com.co.**" asignado a **Andrés Felipe RAMÍREZ** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 68 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ANFERAM@MAPFRE.COM.CO.**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico anferam@mapfre.com.co asignada a **Andrés Felipe RAMÍREZ** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
7	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Andrés Felipe RAMÍREZ → anferam@mapfre.com.co	ad1	52.3 GB
TOTAL					**52.3 GB**

Tabla 15 Detalle del buzón de correo electrónico asignado anferam@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico anferam@mapfre.com.co asignado a Andrés Felipe RAMÍREZ

para el desarrollo de sus funciones **aloja** un total de **52.3 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Novecientos ocho mil cuatrocientos veintitrés (908.423)** archivos (incluyendo carpetas), como se observa a continuación.

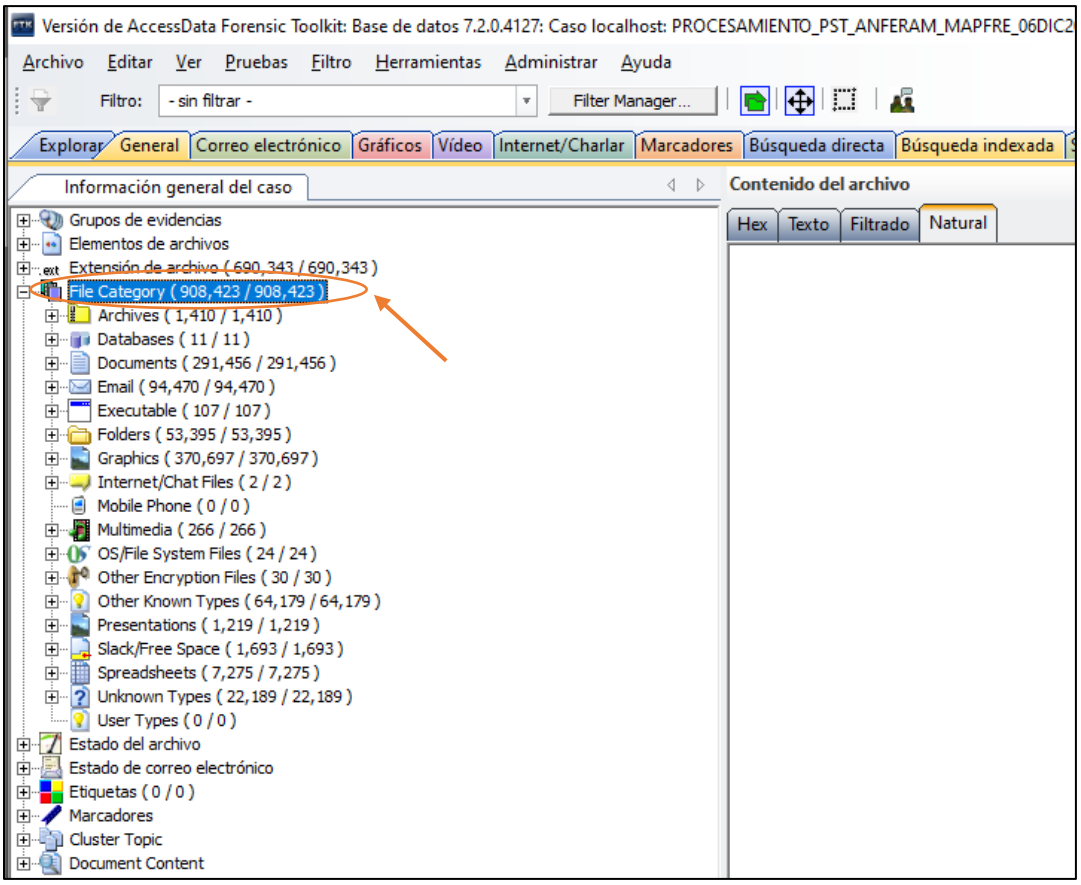


Ilustración 69 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico anferam@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO ANDRÉS FELIPE RAMÍREZ → ANFERAM@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico anferam@mapfre.com.co asignado a **Andrés Felipe RAMÍREZ**, iniciando el día el 06 de diciembre del presente año con una duración aproximada de **cinco (5)** día calendario, el resultado a dicho proceso arrojó que existen **Novecientos ochenta y un (981)** ítems en condición de "eliminados" y se reconstruyeron **Doscientos treinta y seis mil doscientos noventa y un (236.291)** archivos de datos restaurados,

que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

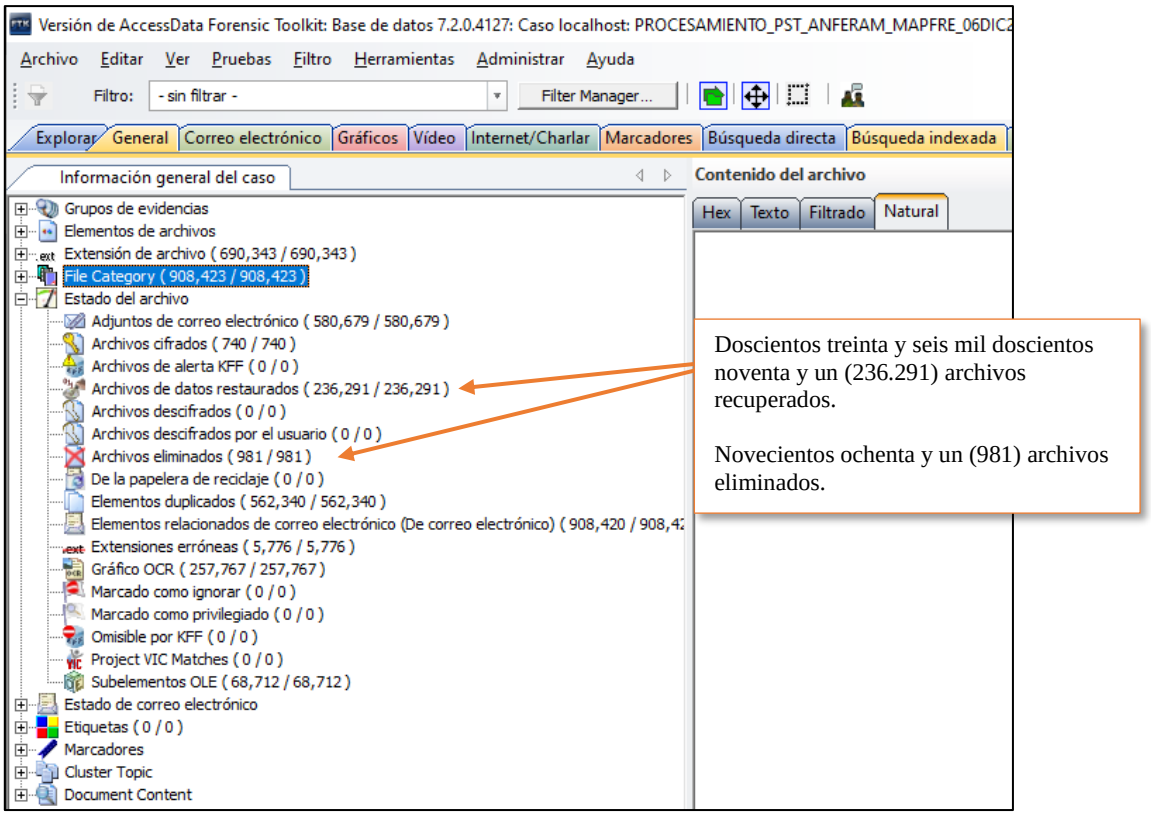


ilustración 70 Total de archivos recuperados en la cuenta de correo electrónico anferam@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Novecientos ocho mil cuatrocientos veintitrés (908.423)** (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ANFERAM@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico

anferam@mapfre.com.co asignado a **Andrés Felipe RAMÍREZ** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1.410
2	Bases de Datos	11
3	Documentos	291.456
4	Correo Electrónico	94.470
5	Ejecutables	107
6	Carpetas	53.395
7	Gráficos	370.697
8	Archivos de Internet/Chat	2
9	Multimedia	266
10	Archivos del sistema	24
11	Otros archivos encriptados	30
12	Otros archivos desconocidos	64.179
13	Presentaciones	1.219
14	Espacio libre	1.693
15	Hojas de cálculo	7.275
16	Tipos de archivos desconocidos	22.189
TOTAL		**908.423**

Tabla 16 Información buscada evidencia 007_ANFERAM, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Novecientos ocho mil cuatrocientos veintitrés (908.423).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Quinientos ochenta mil seiscientos setenta y nueve (580.679) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Los archivos cifrados recuperados **Setecientos cuarenta (740) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Doscientos treinta y seis mil doscientos noventa y un (236.291) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos Eliminados **Novecientos ochenta y un (981) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Quinientos sesenta y dos mil trescientos cuarenta (562.340) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Novecientos ocho mil cuatrocientos veinte (908.420) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Cinco mil setecientos setenta y seis (5.776) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Doscientos cincuenta y siete mil setecientos sesenta y siete (257.767) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Sesenta y ocho mil setecientos doce (68.712) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico anferam@mapfre.com.co asignado a **Andrés Felipe RAMÍREZ** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

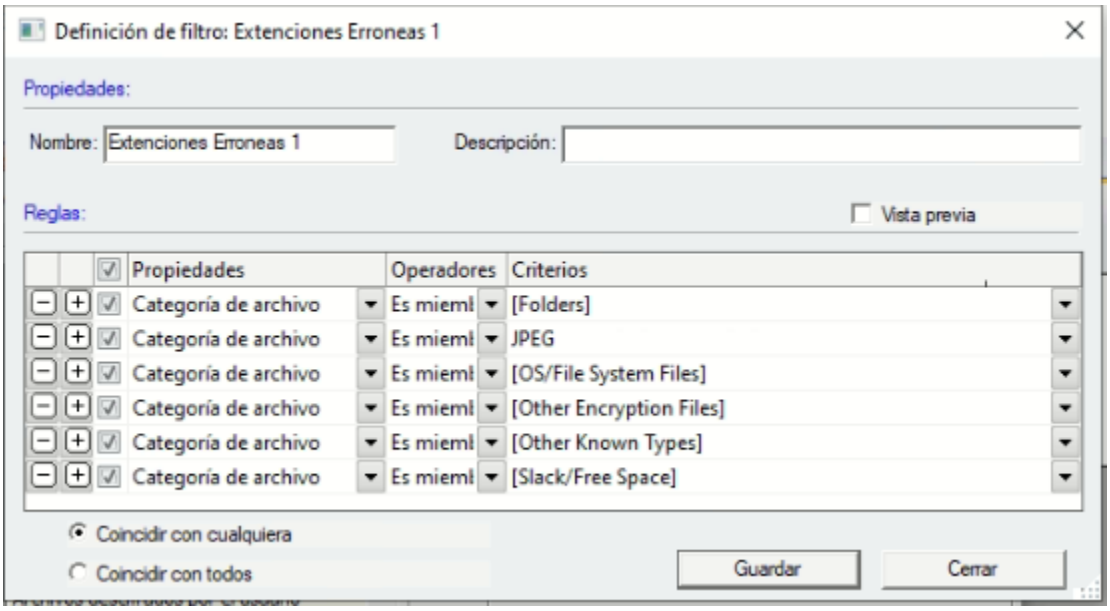


Ilustración 71 Filtro para excluir las extensiones erróneas.

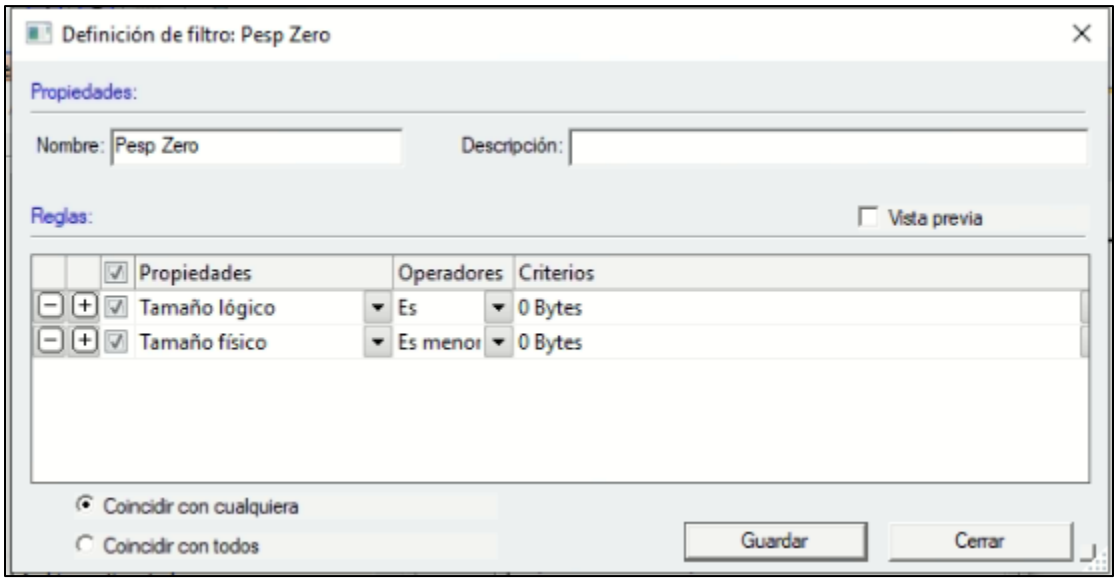


Ilustración 72 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

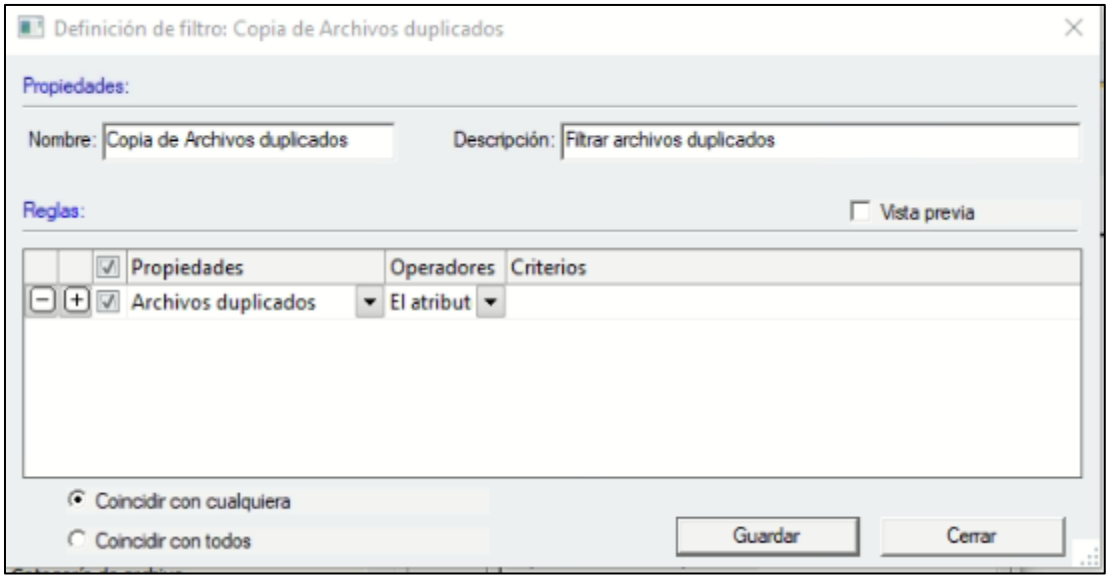


Ilustración 73 Filtro para excluir los archivos duplicados.

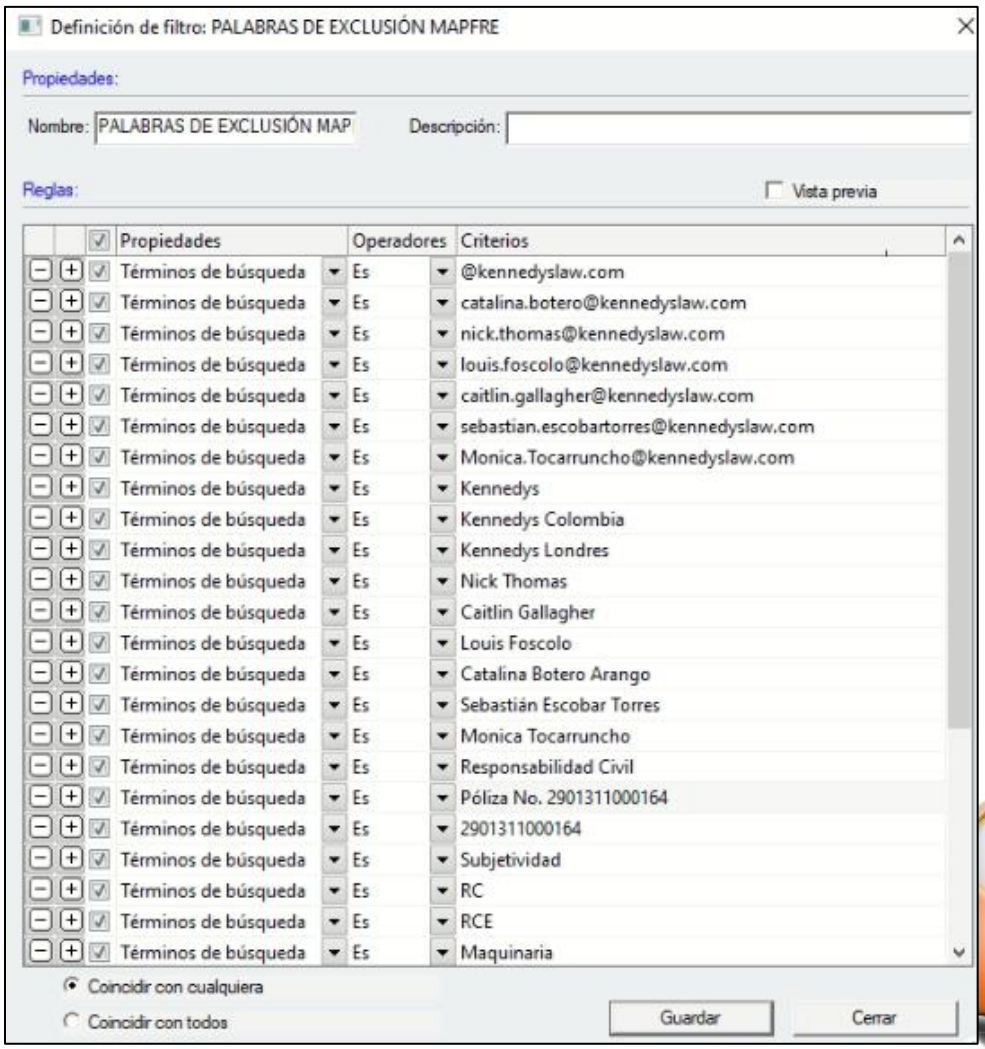


Ilustración 74 Filtro para excluir los archivos suministrado por MAPFRE - 1.

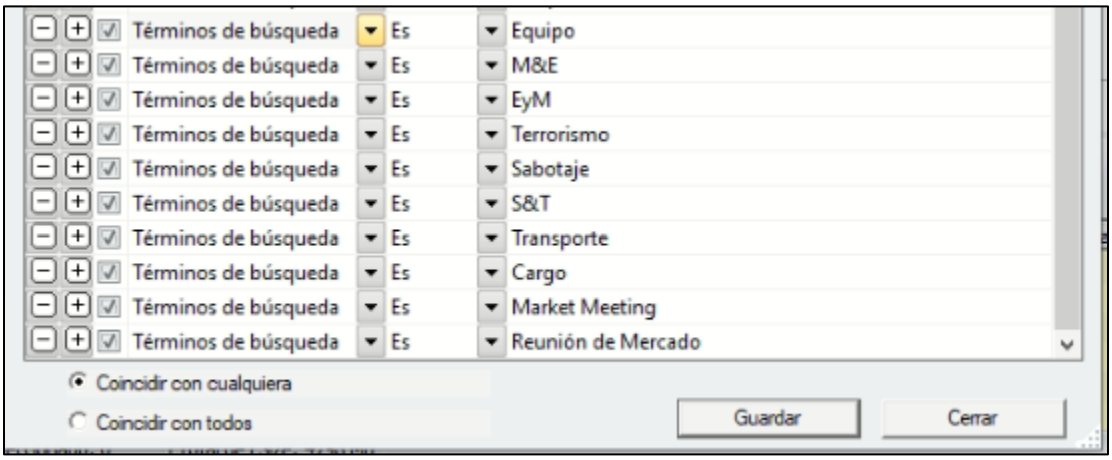
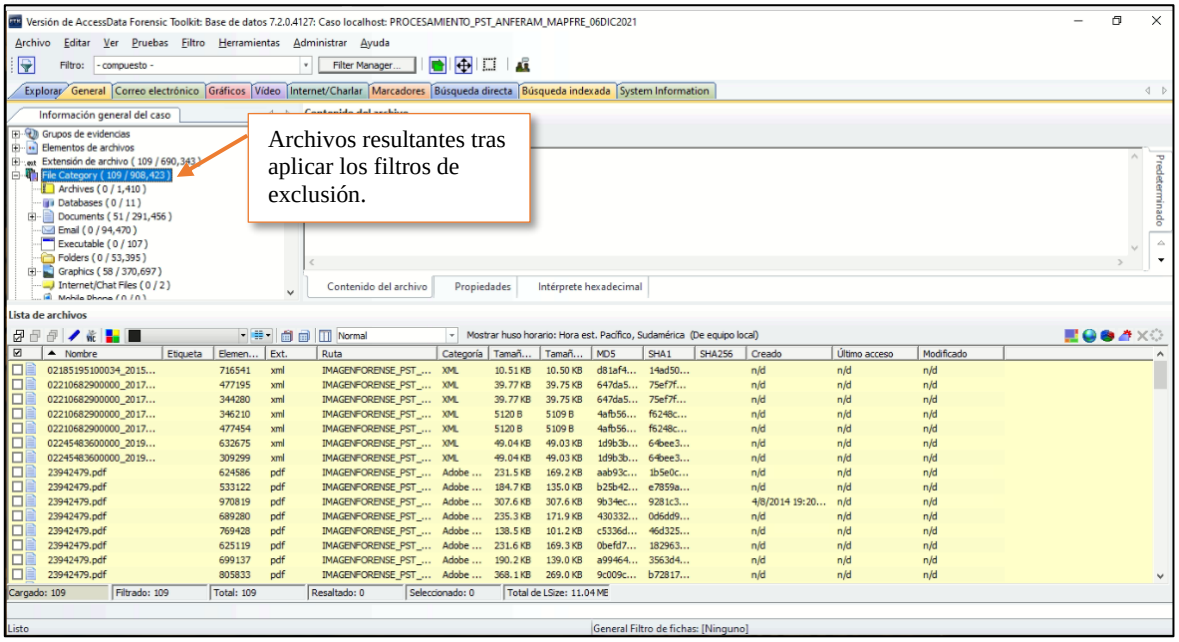


Ilustración 75 Filtro para excluir los archivos suministrado por MAPFRE - 2.

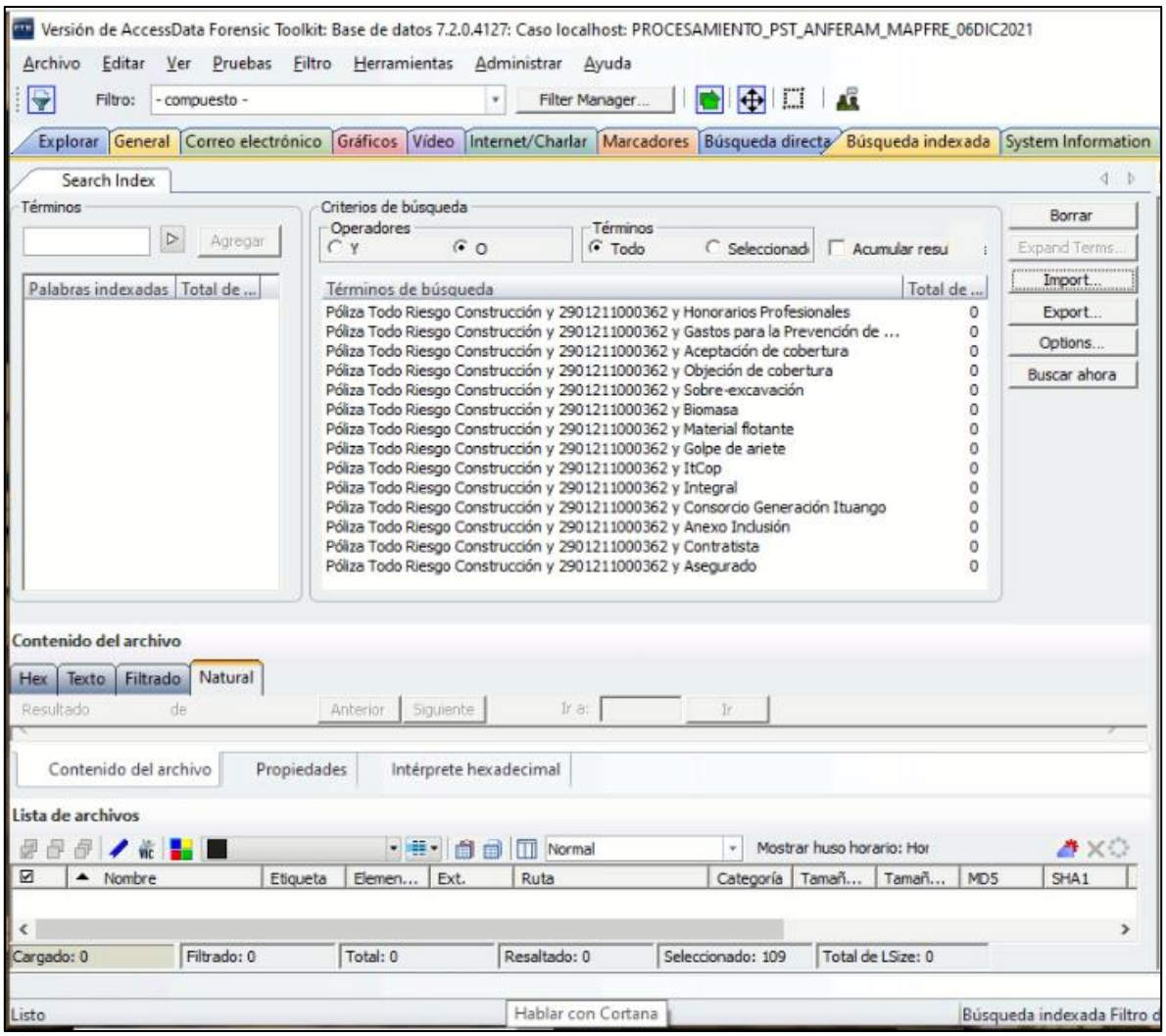
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Ciento nueve (109)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo anferam@mapfre.com.co asignado a **Andrés Felipe RAMÍREZ** para el desarrollo de sus funciones.

8. Buzón de correo electrónico mvivian@mapfre.com.

El día 19 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **MVIVIAN**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

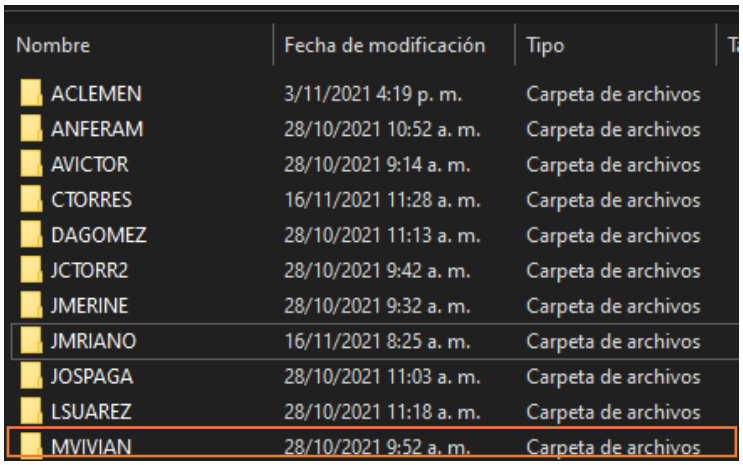


Ilustración 76 Visualización carpeta MVIVIAN

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **MVIVIAN** identificada dentro del disco duro como se observa en las siguientes imágenes:

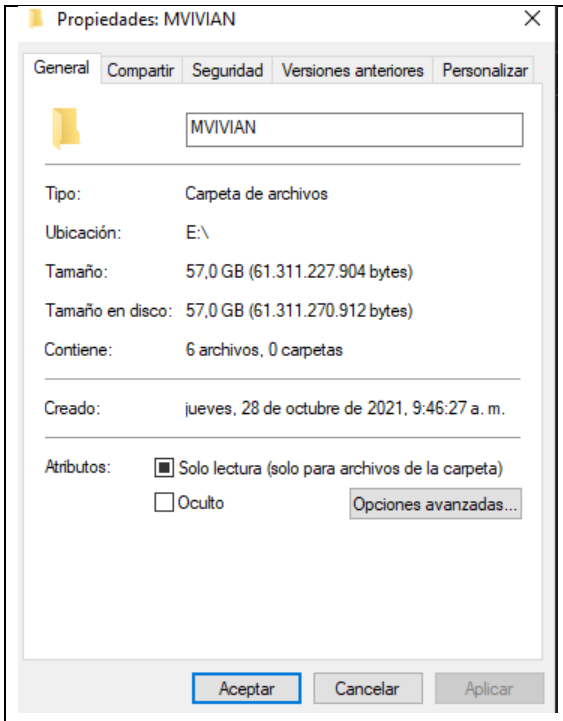


Ilustración 77 Propiedades de la carpeta MVIVIAN visto desde el Disco Duro.

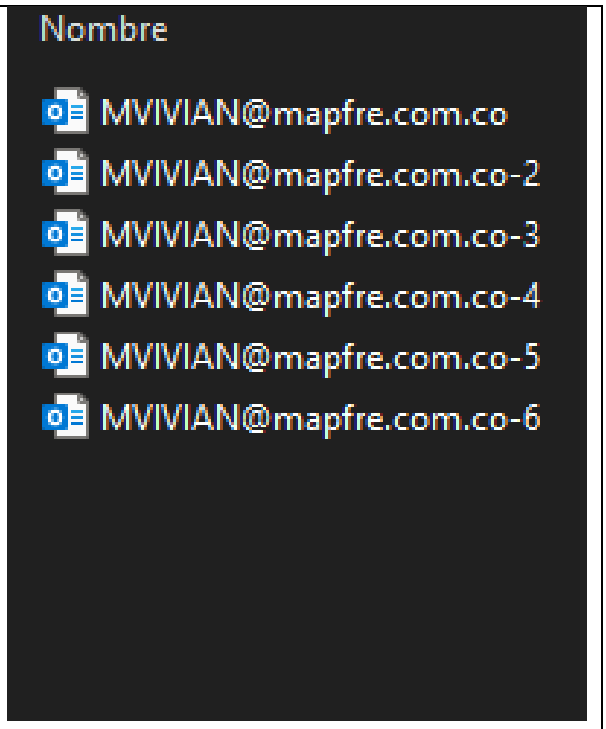


Ilustración 78 Contenido de la carpeta MVIVIAN visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**mvivian@mapfre.com.**" asignado a

Viviana Rocío MOYANO para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **15:59:28** y culminando el mismo de forma satisfactoria a las **16:22:11**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_19NOV2021
Número de prueba: 008_MVIVIAN
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO MVIVIAN@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad1:
[Custom Content Sources]
K::K:\|MVIVIAN|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: f2b048976f511d39e5985af537222dea
SHA1 checksum: 493d58bf1f54dcc30314162538921cf1b8ac853d

Image information:
Acquisition started: Fri Nov 19 15:59:28 2021
Acquisition finished: Fri Nov 19 16:16:02 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad29

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad30

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad31

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad32

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad33

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad34

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad35

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad36

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad37

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad38

I:\EVIDENCIA_MAPFRE_2\8.MVIVIAN\IMAGENFORENSE_PST_MVIVIAN_MAPFRE_19NOV2021.ad39

Image Verification Results:
Verification started: Fri Nov 19 16:16:02 2021
Verification finished: Fri Nov 19 16:22:11 2021
MD5 checksum: f2b048976f511d39e5985af537222dea: verified
SHA1 checksum: 493d58bf1f54dcc30314162538921cf1b8ac853d: verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con

capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**mvivian@mapfre.com.**" asignado a **Viviana Rocío MOYANO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 79 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO MVIVIAN@MAPFRE.COM."**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico mvivian@mapfre.com asignada **Viviana Rocío MOYANO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
8	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Viviana Rocío MOYANO → mvivian@mapfre.com	ad1	57.0 GB
TOTAL					**57.0 GB**

Tabla 17 Detalle del buzón de correo electrónico asignado mvivian@mapfre.com
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico mvivian@mapfre.com asignado a **Viviana Rocío MOYANO** para

el desarrollo de sus funciones **aloja** un total de **57.0 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Setecientos treinta mil doscientos dieciocho (730.218)** archivos (incluyendo carpetas), como se observa a continuación.

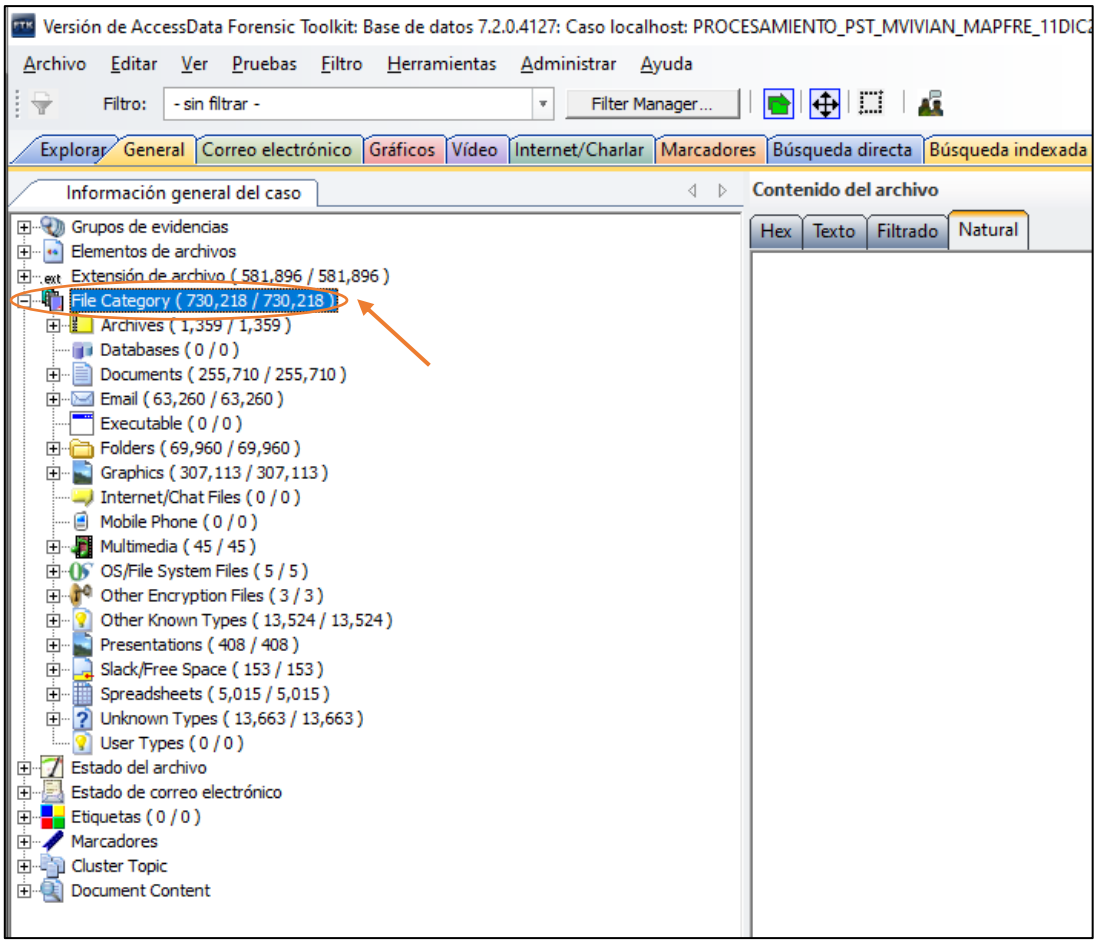


Ilustración 80 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico mvivian@mapfre.com.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO VIVIANA ROCÍO MOYANO → MVIVIAN@MAPFRE.COM.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico mvivian@mapfre.com asignado a **Viviana Rocío MOYANO**, iniciando el día el **11** de diciembre del presente año con una duración aproximada de **Diez (10)** días calendarios, el resultado a dicho proceso arrojó que existen **cero (0)** ítems en condición de "eliminados" y se reconstruyeron **Ciento noventa y cuatro mil cuatrocientos**

treinta y un (194.431) archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

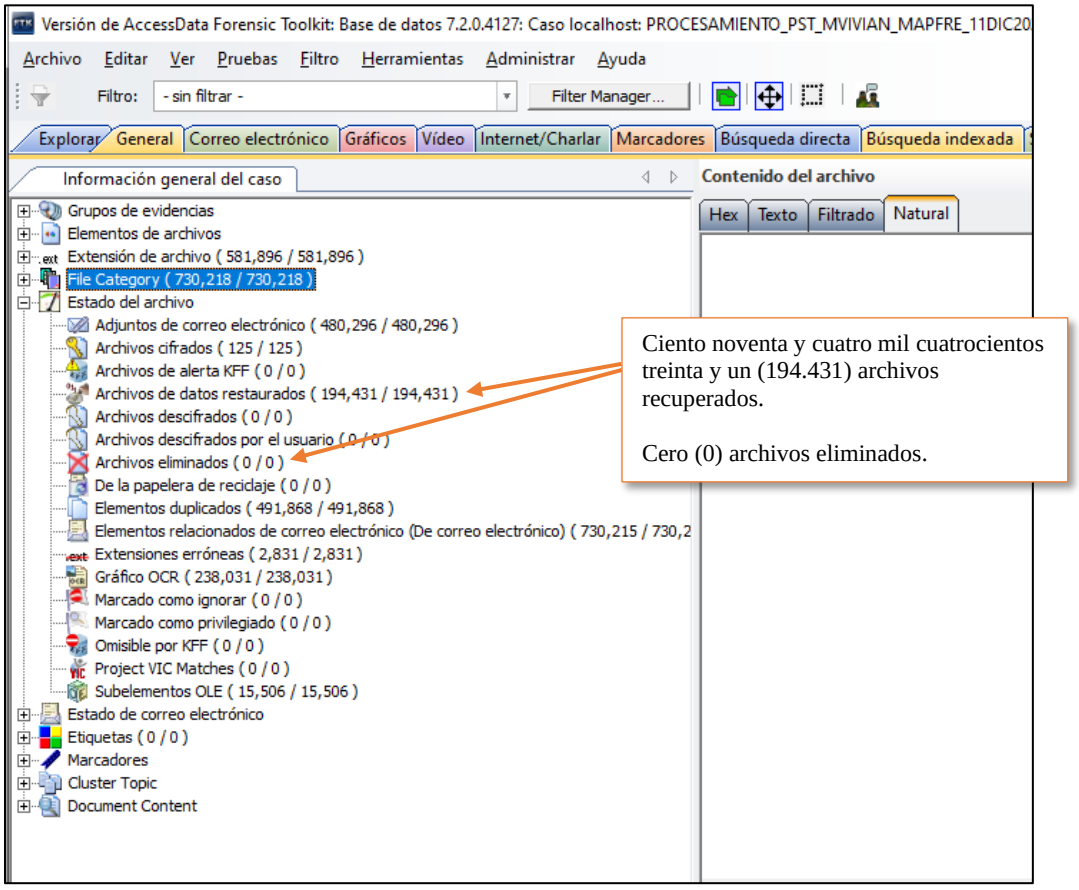


ilustración 81 Total de archivos recuperados en la cuenta de correo electrónico mvivian@mapfre.com.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Setecientos treinta mil doscientos dieciocho (730.218)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

- **RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO MVIVIAN@MAPFRE.COM.CO.**

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico mvivian@mapfre.com asignado a **Viviana Rocío MOYANO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1.359
2	Documentos	255.710
3	Correo Electrónico	63.260
4	Carpetas	69.960
5	Gráficos	307.113
6	Multimedia	45
7	Archivos del sistema	5
8	Otros archivos encriptados	3
9	Otros archivos desconocidos	13.524
10	Presentaciones	408
11	Espacio libre	153
12	Hojas de cálculo	5.015
13	Tipos de archivos desconocidos	13.663
TOTAL		**730.218**

Tabla 18 Información buscada evidencia 008_MVIVIAN, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Setecientos treinta mil doscientos dieciocho (730.218).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Cuatrocientos ochenta mil doscientos noventa y seis (480.296) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Ciento veinticinco (125) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Ciento noventa y cuatro mil cuatrocientos treinta y un (194.431) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Cuatrocientos noventa y un mil ochocientos sesenta y ocho (491.868) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Setecientos treinta mil doscientos quince (730.215) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Dos mil ochocientos treinta y un (2.831) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Doscientos treinta y ocho mil treinta y un (238.031) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Quince mil quinientos seis (15.506) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico mvivian@mapfre.com asignado a **Viviana Rocío MOYANO** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

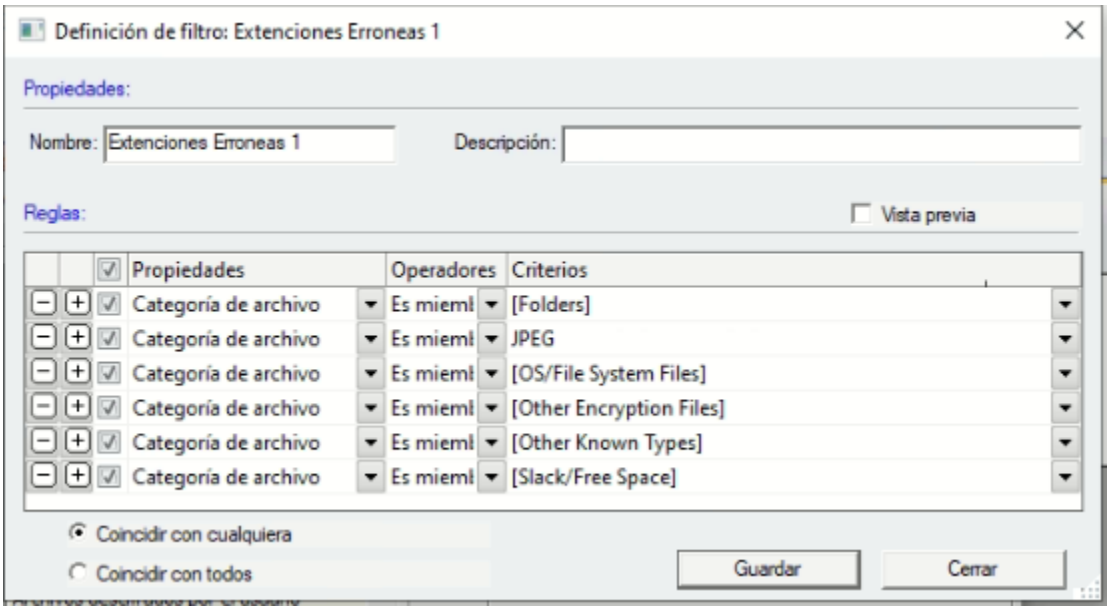


Ilustración 82 Filtro para excluir las extensiones erróneas.

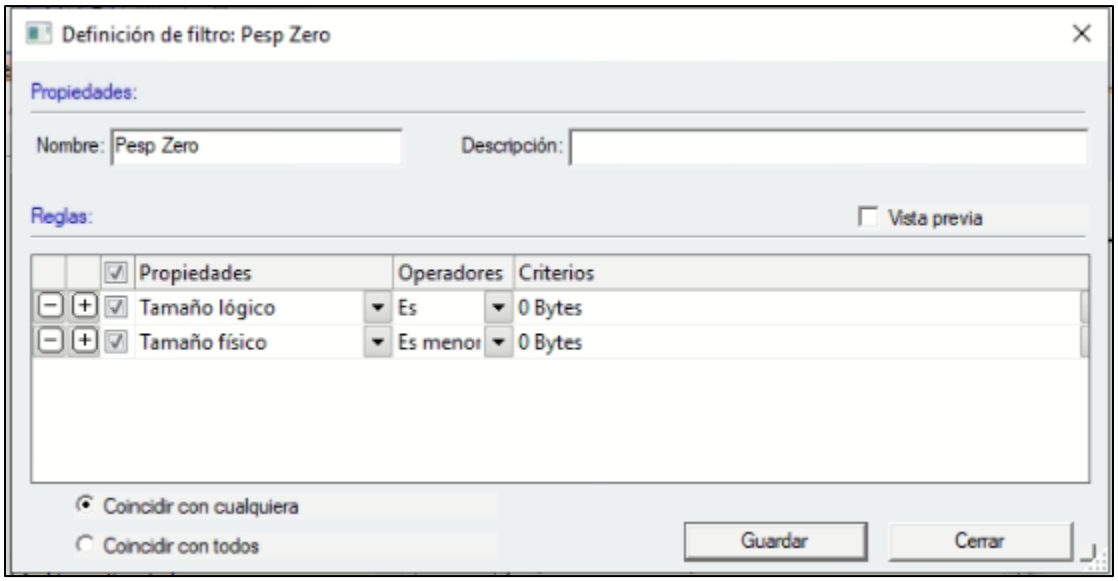


Ilustración 83 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

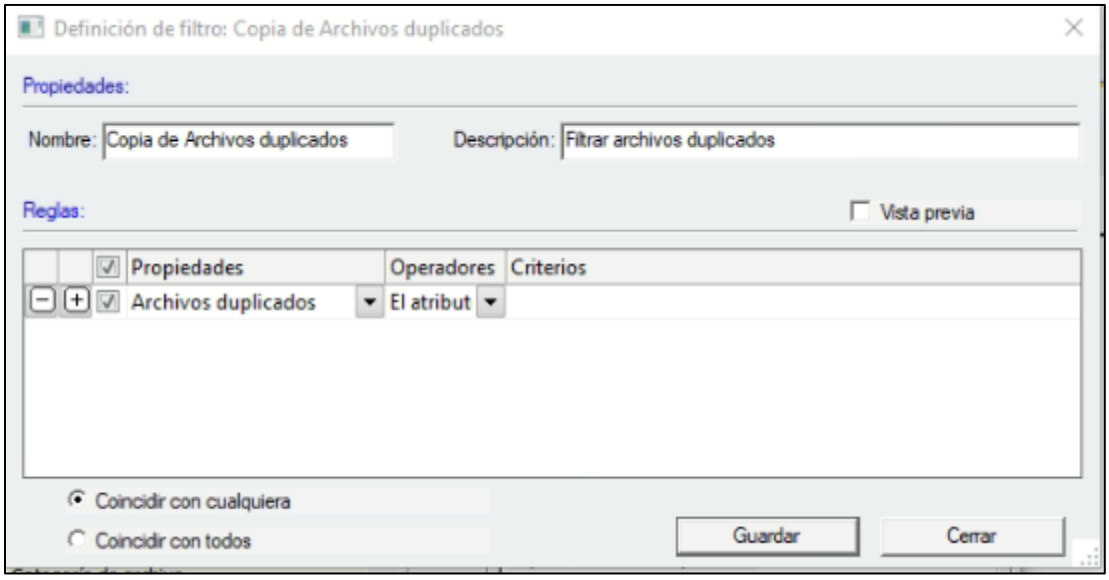


Ilustración 84 Filtro para excluir los archivos duplicados.

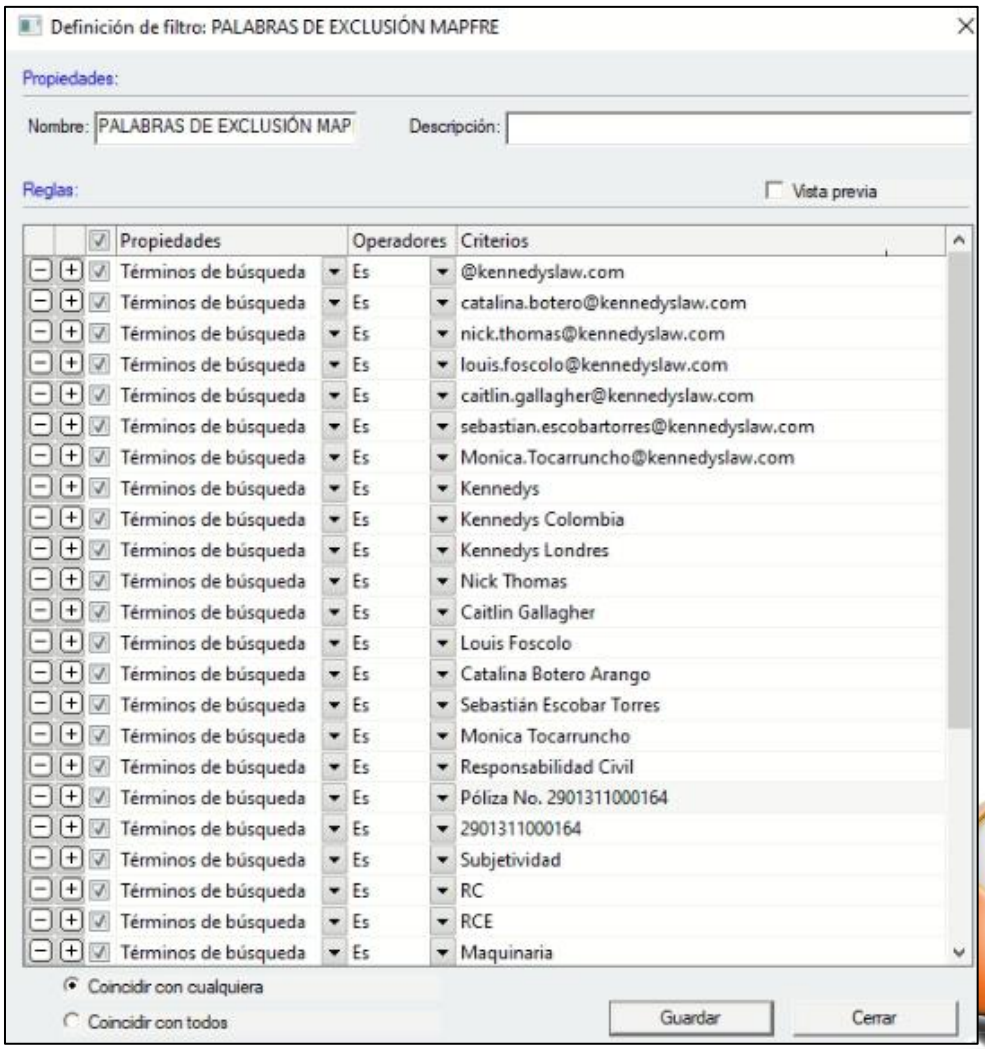


Ilustración 85 Filtro para excluir los archivos suministrado por MAPFRE - 1.

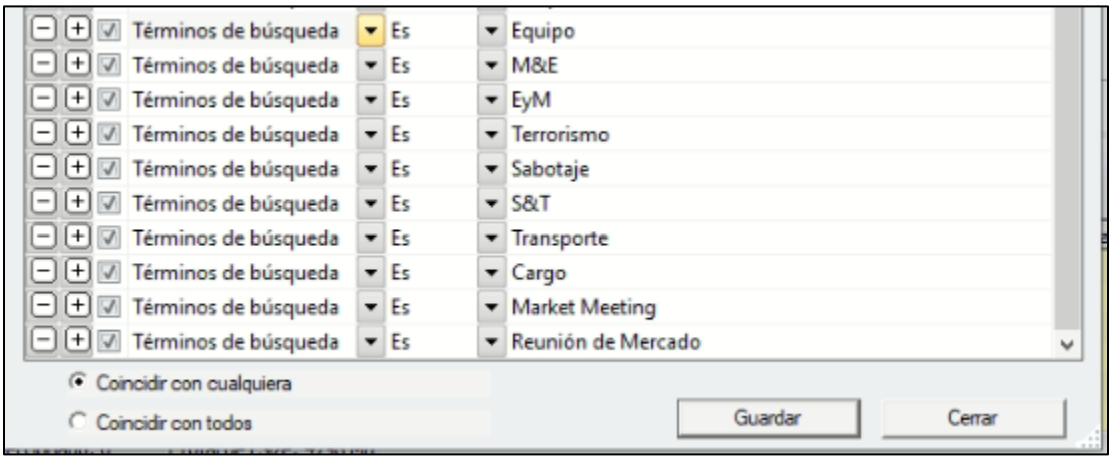
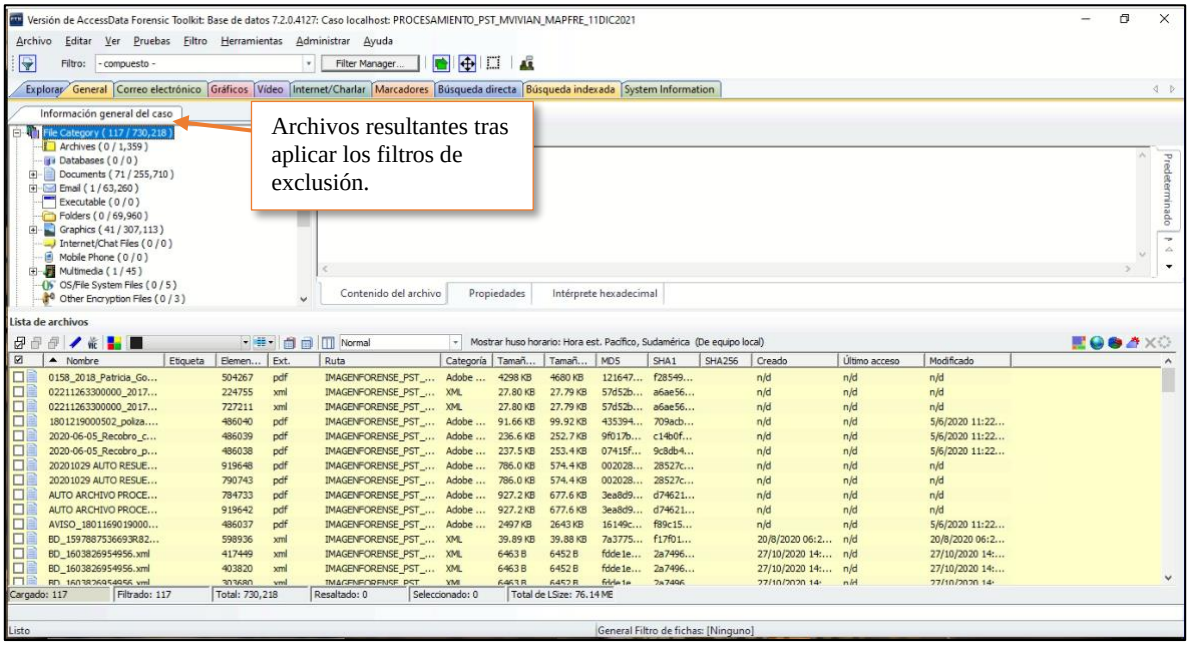


Ilustración 86 Filtro para excluir los archivos suministrado por MAPFRE - 2.

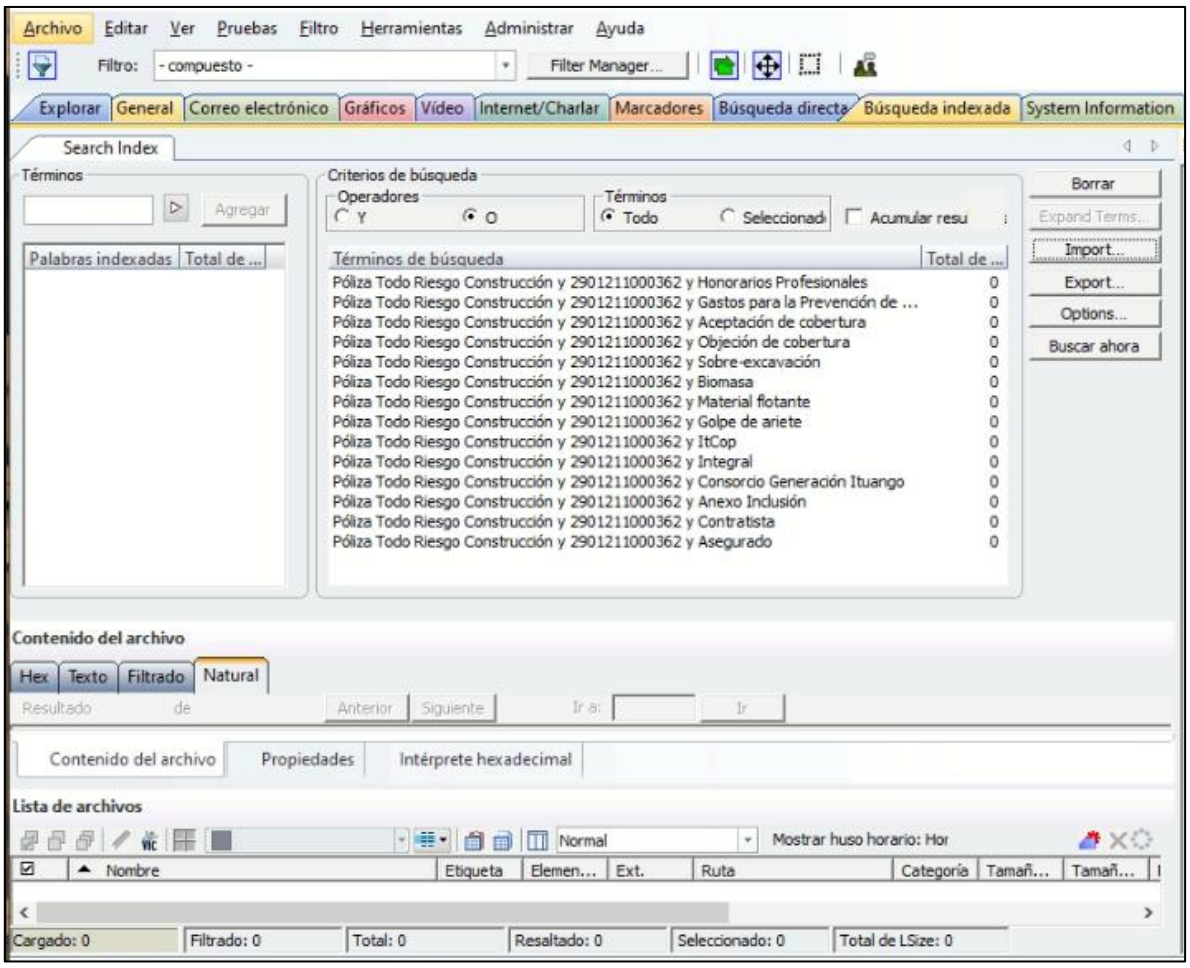
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Veinticinco (117)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo mvivian@mapfre.com asignado a **Viviana Rocío MOYANO** para el desarrollo de sus funciones.

9. Buzón de correo electrónico jctorr2@mapfre.com.co

El día 22 de noviembre del 2021, el equipo de ADALID CORP ingresa a la carpeta **JCTORR2**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

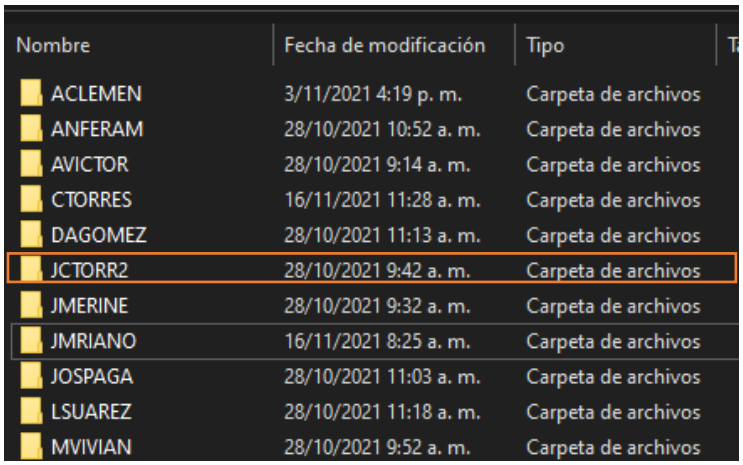


Ilustración 87 Visualización carpeta JCTORR2.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **JCTORR2** identificada dentro del disco duro como se observa en las siguientes imágenes:

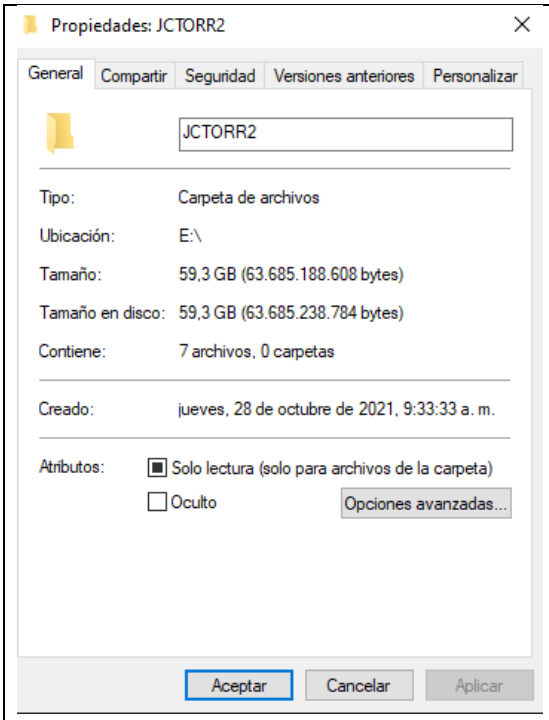


Ilustración 88 Propiedades de la carpeta JCTORR2 visto desde el Disco Duro.

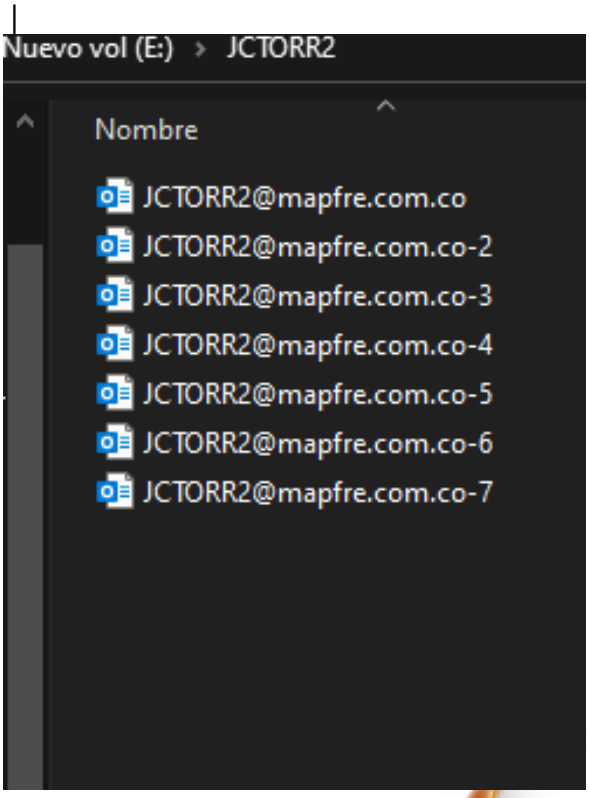


Ilustración 89 Contenido de la carpeta JCTORR2 visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**jctorr2@mapfre.com.co.**" asignado a **Juan Camilo TORRES LOZANO** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **10:00:06** y culminando el mismo de forma satisfactoria a las **10:17:22**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_22NOV2021
Número de prueba: 009_JCTORR2
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO JCTORR2@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for
I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad1:
[Custom Content Sources]
K::K:\|JCTORR2|*(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 82febeb311661f24839ced114ce64e7b
SHA1 checksum: 47c4c084826f4119210640aa34aae4b32068e556

Image information:
Acquisition started: Mon Nov 22 10:00:06 2021
Acquisition finished: Mon Nov 22 10:12:52 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad29

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad30

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad31

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad32

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad33

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad34

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad35

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad36

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad37

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad38

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad39

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad40

I:\EVIDENCIA_MAPFRE_2\9.JCTORR2\IMAGENFORENSE_PST_JCTORR2_MAPFRE_22NOV2021.ad41

Image Verification Results:
Verification started: Mon Nov 22 10:12:54 2021
Verification finished: Mon Nov 22 10:17:22 2021
MD5 checksum: 82febeb311661f24839ced114ce64e7b : verified

SHA1 checksum: 47c4c084826f4119210640aa34aae4b32068e556 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**jctorr2@mapfre.com.co.**" asignado a **Juan Camilo TORRES LOZANO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 90 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO JCTORR2@MAPFRE.COM.CO.

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico jctorr2@mapfre.com.co asignada **Juan Camilo TORRES LOZANO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
9	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Juan Camilo TORRES LOZANO → jctorr2@mapfre.com.co	ad1	59.3 GB
TOTAL					**59.3 GB**

Tabla 19 Detalle del buzón de correo electrónico asignado jctorr2@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico jctorr2@mapfre.com.co asignada a **Juan Camilo TORRES LOZANO** para el desarrollo de sus funciones **aloja** un total de **59.3 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Un millón noventa y un mil setecientos sesenta y ocho (1.091.768)** archivos (incluyendo carpetas), como se observa a continuación.

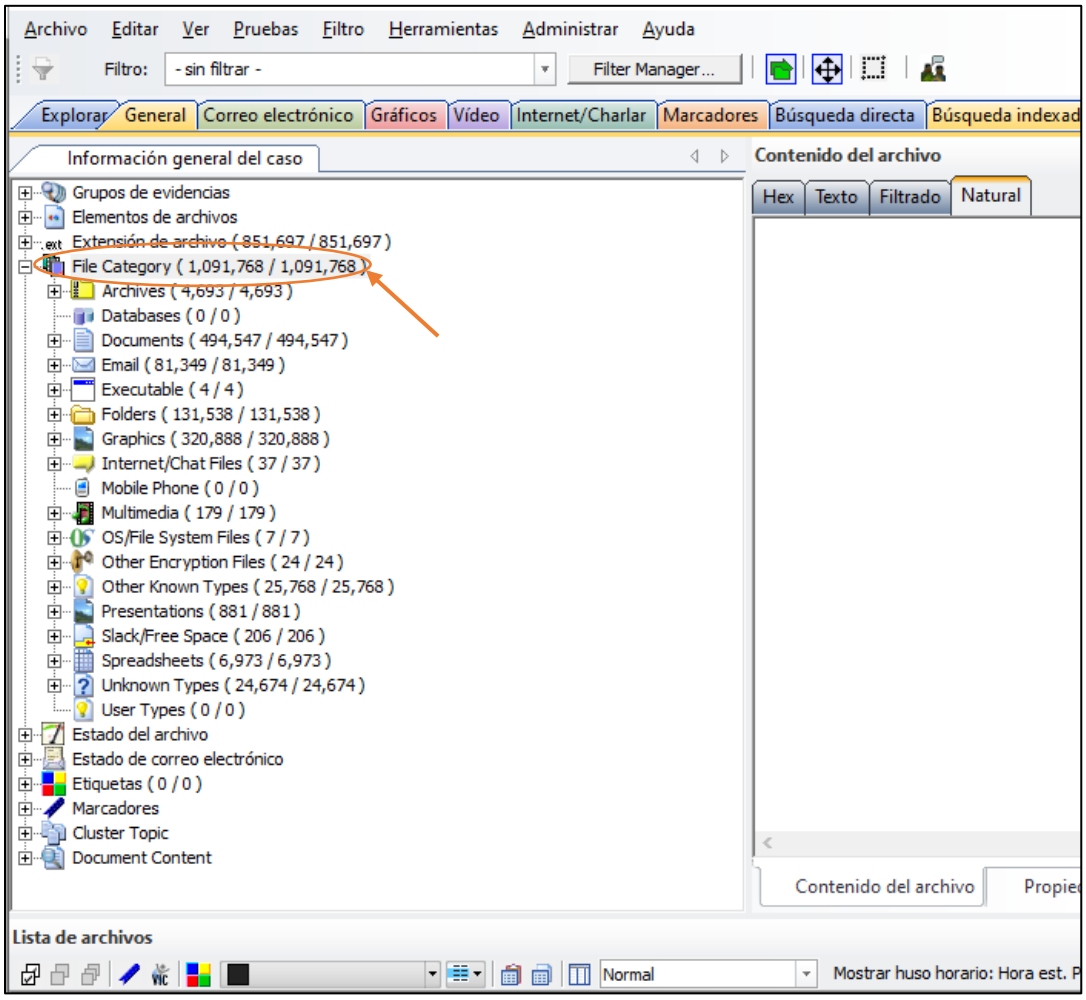


Ilustración 91 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico jctorr2@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JUAN CAMILO TORRES LOZANO → JCTORR2@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos,

en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico jctorr2@mapfre.com.co asignada a **Juan Camilo TORRES LOZANO**, iniciando el día el **27** de diciembre del año 2021 con una duración aproximada de diez (10) días calendarios y finalizando el día 07 de enero de 2022, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Ciento ochenta y dos mil ochocientos cincuenta y dos (182.852)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

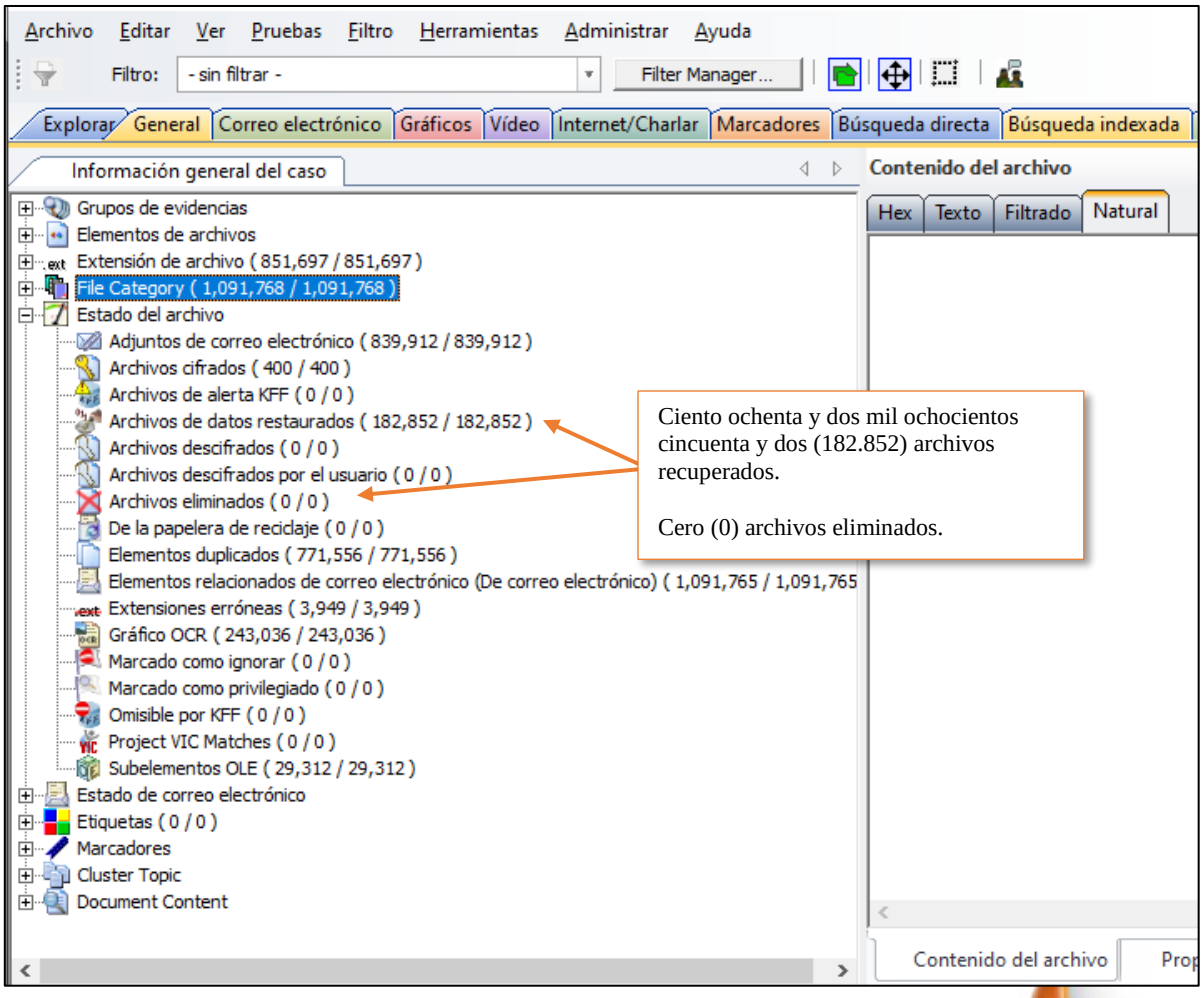


ilustración 92 Total de archivos recuperados en la cuenta de correo electrónico jctorr2@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Un millón noventa y un mil setecientos sesenta y ocho (1.091.768)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO JCTORR2@MAPFRE.COM.CO.

Luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico jctorr2@mapfre.com.co asignada a **Juan Camilo TORRES LOZANO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	4693
2	Documentos	494.547
3	Correo Electrónico	81.349
4	Ejecutables	4
5	Carpetas	131.538
6	Gráficos	320.888
7	Archivos Internet/Chats	37
8	Multimedia	179
9	Archivos del sistema	7
10	Otros archivos encriptados	24
11	Otros archivos desconocidos	25.768
12	Presentaciones	881
13	Espacio libre	206
14	Hojas de cálculo	6.973
15	Tipos de archivos desconocidos	24.674
TOTAL		**1.091.768**

Tabla 20 Información buscada evidencia 009_ JCTORR2, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Un millón noventa y un mil setecientos sesenta y ocho (1.091.768).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Ochocientos treinta y nueve mil novecientos doce (839.912)** archivos de datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Cuatrocientos (400) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Diez mil setecientos ochenta y ocho (10.788) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Setecientos setenta y un mil quinientos cincuenta y seis (771.556) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Un millón noventa y un mil setecientos sesenta y cinco (1.091.765) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Tres mil novecientos cuarenta y nueve (3.949) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Doscientos cuarenta y tres mil treinta y seis (243.036) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Veintinueve mil trescientos doce (29.312) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico jctorr2@mapfre.com.co asignada a **Juan Camilo TORRES LOZANO** para el desarrollo de sus funciones el equipo de ADALID

CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

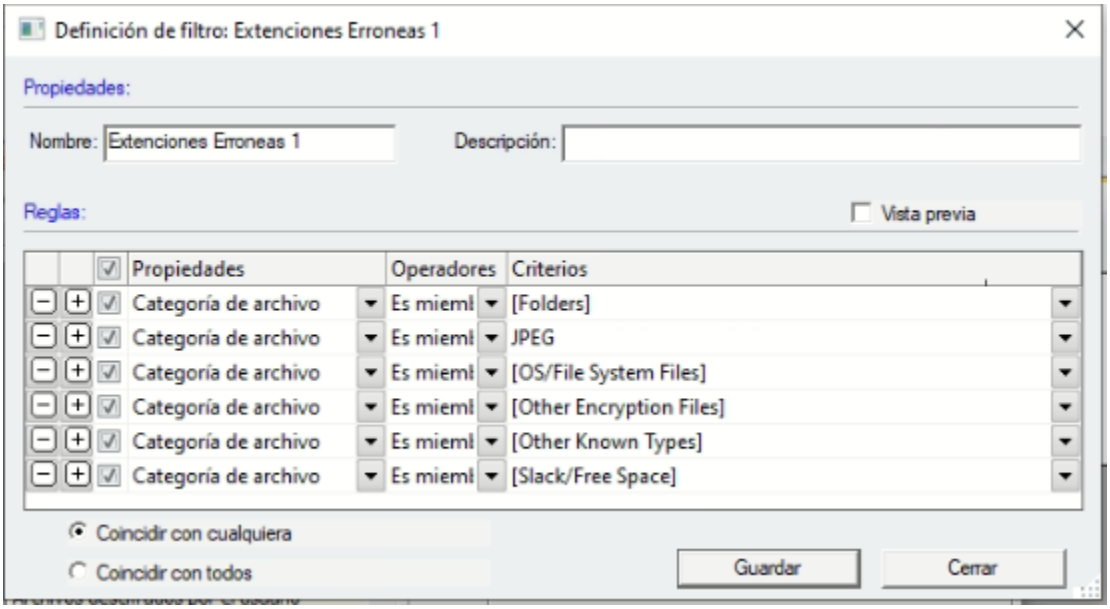


Ilustración 93 Filtro para excluir las extensiones erróneas.

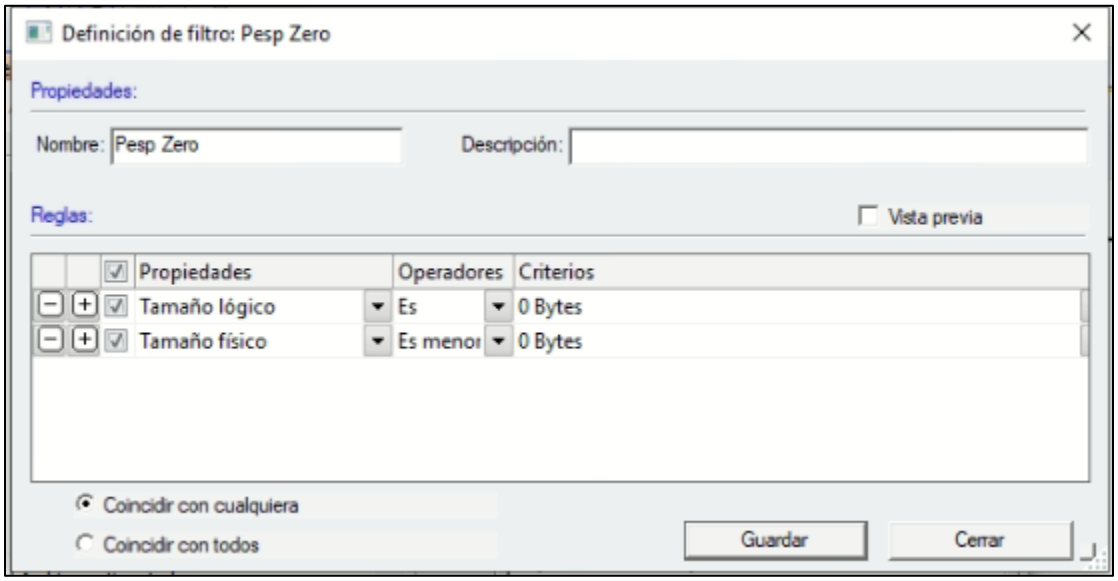


Ilustración 94 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

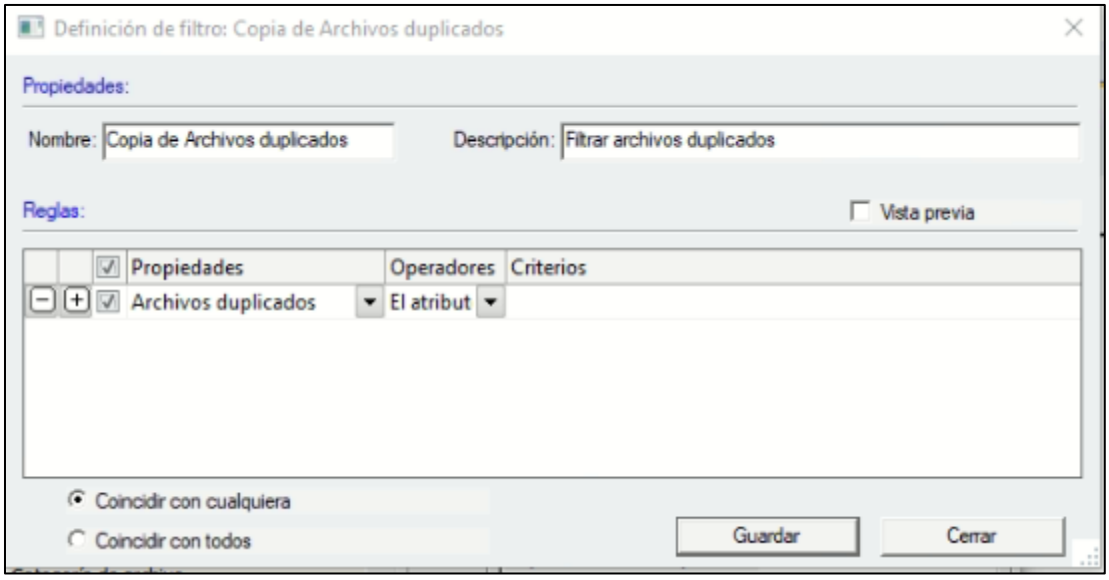


Ilustración 95 Filtro para excluir los archivos duplicados.

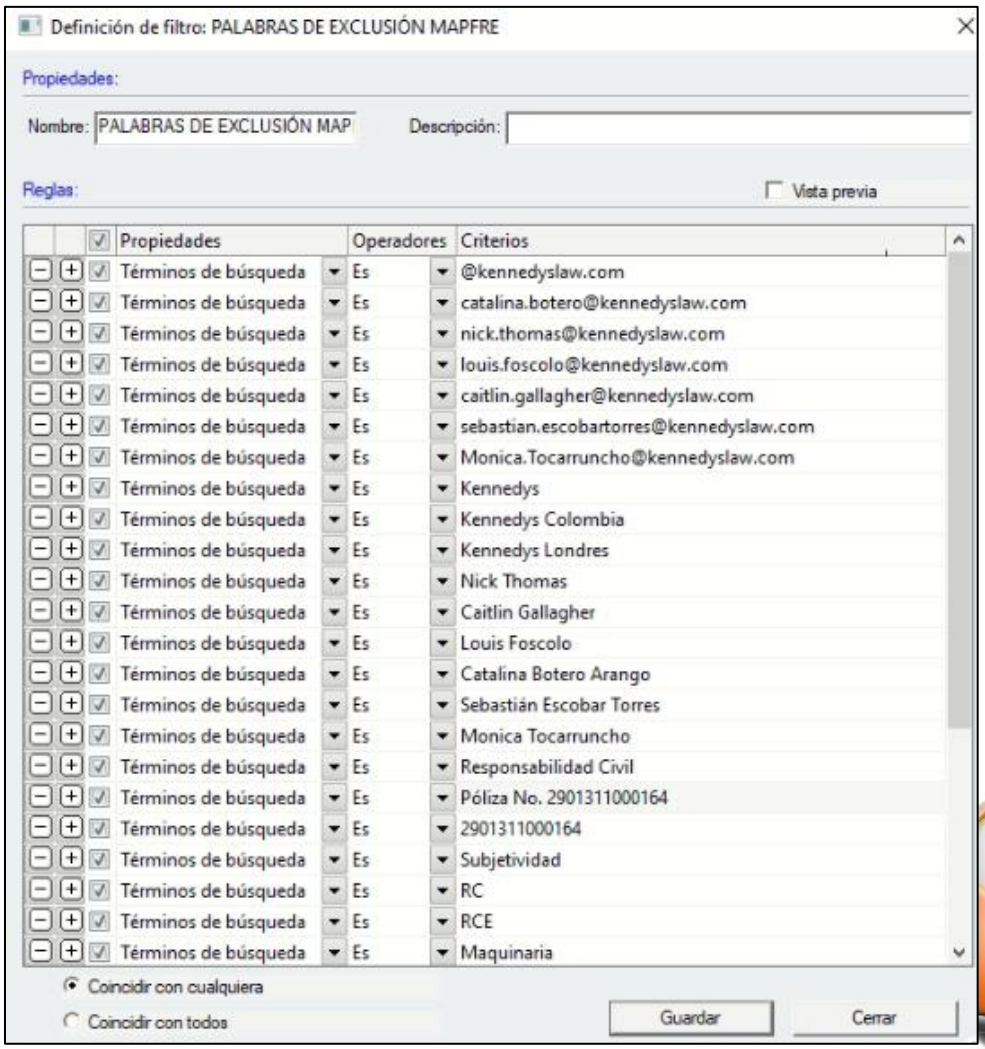


Ilustración 96 Filtro para excluir los archivos suministrado por MAPFRE - 1.

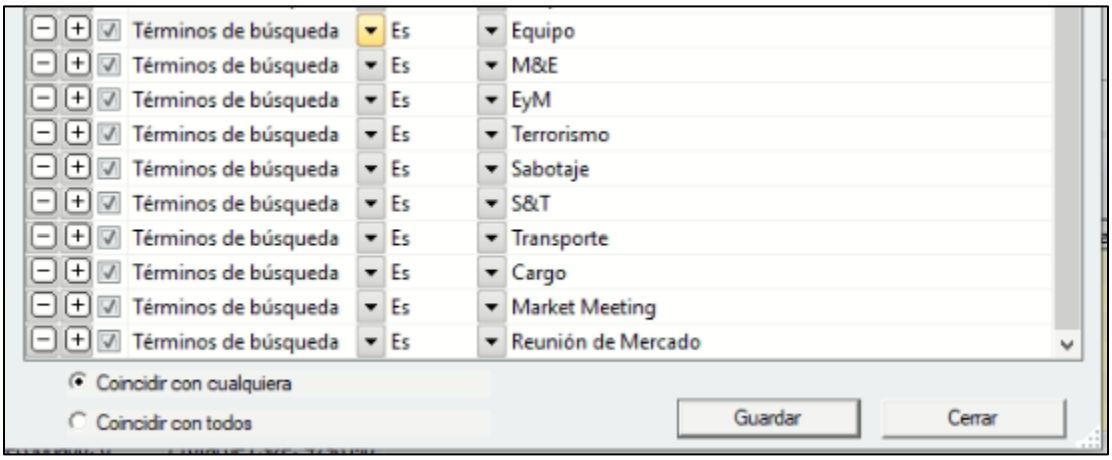
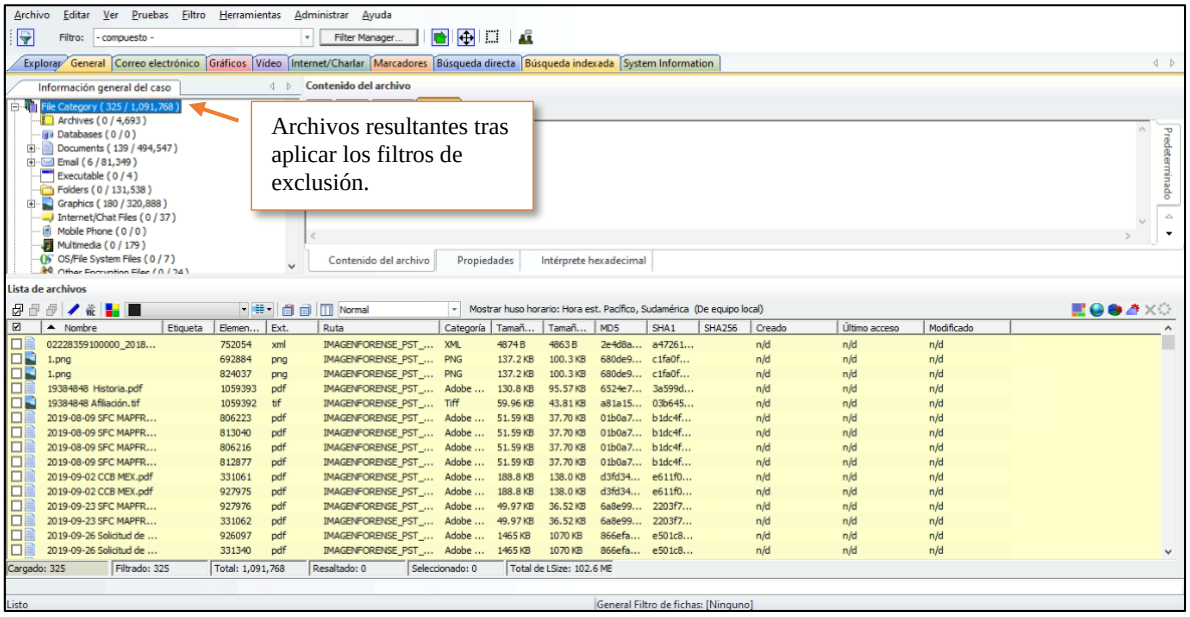


Ilustración 97 Filtro para excluir los archivos suministrado por MAPFRE - 2.

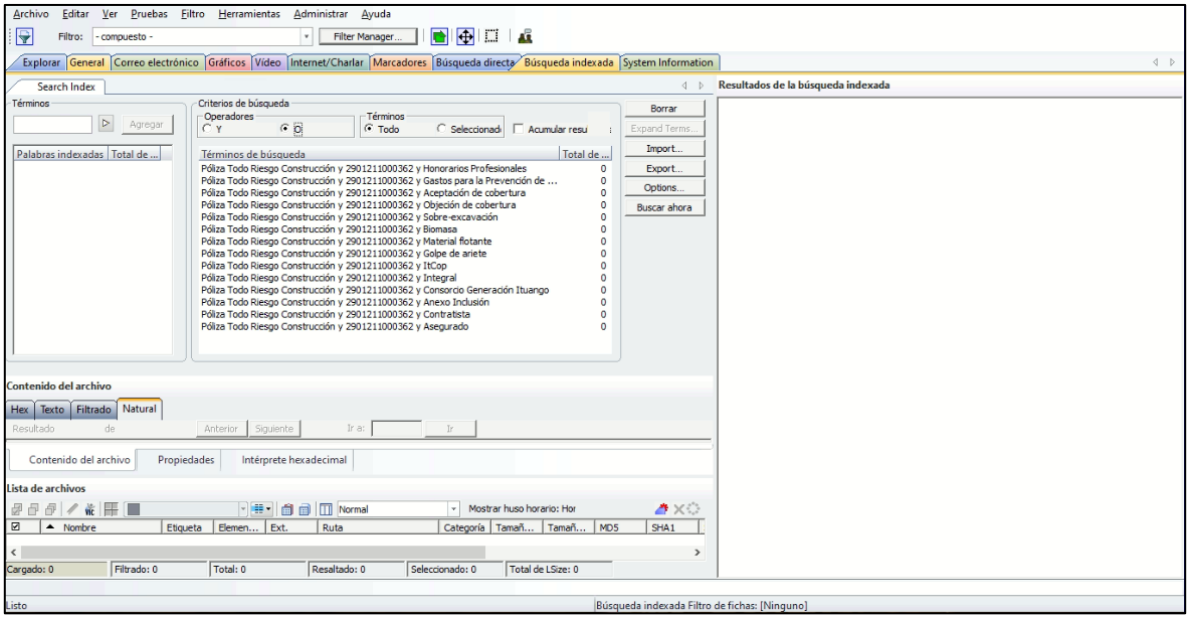
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Trecientos Veinticinco (325)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo jctorr2@mapfre.com.co asignada a **Juan Camilo TORRES LOZANO** para el desarrollo de sus funciones.

10. Buzón de correo electrónico jmriano@mapfre.com.co.

El día 22 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **JMRIANO**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

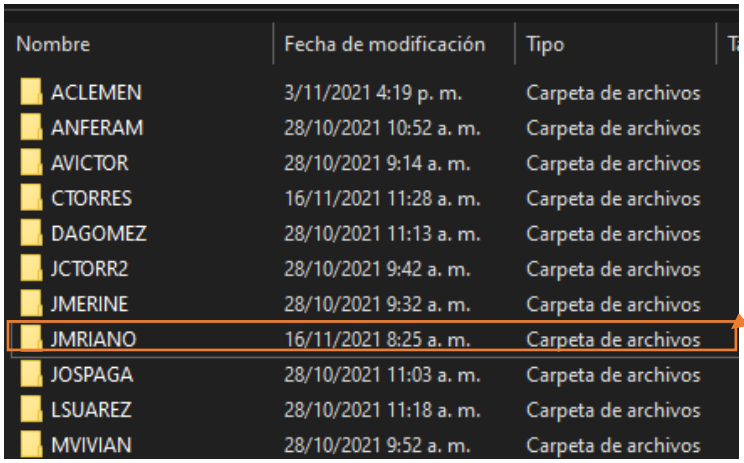


Ilustración 98 Visualización carpeta JMRIANO

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **JMRIANO** identificada dentro del disco duro como se observa en las siguientes imágenes:

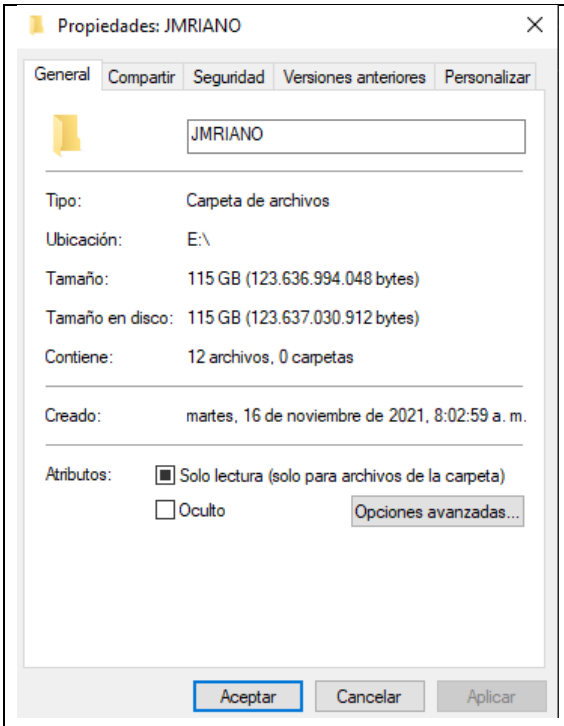


Ilustración 99 Propiedades de la carpeta JMRIANO visto desde el Disco Duro.

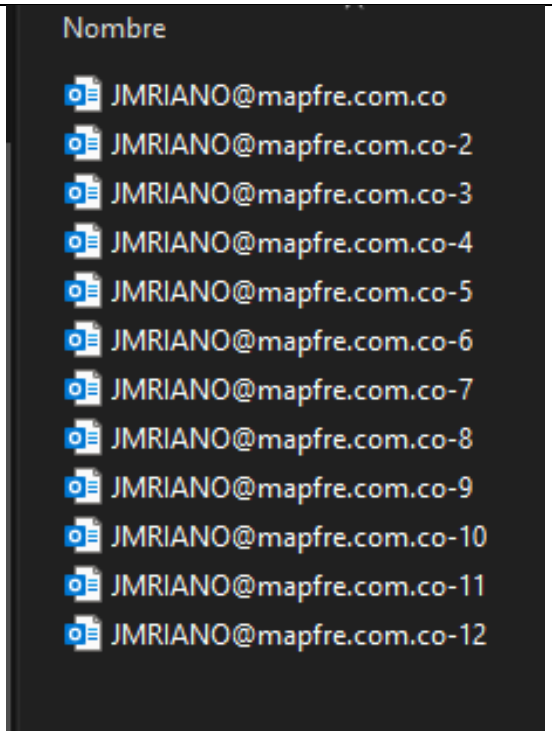


Ilustración 100 Contenido de la carpeta JMRIANO visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**jmriano@mapfre.com.co.**" asignado a **José Manuel RIAÑO** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **10:25:29** y culminando el mismo de forma satisfactoria a las **10:58:24,** tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_22NOV2021
Número de prueba: 10_JMRIANO
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO JMRIANO@MAPFRE.COM.CO, ENTREGADOS POR

MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for
I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad1:
[Custom Content Sources]
K::K:\ | JMRIANO | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: de6744c8bb0c6717f072120e5caaa982
SHA1 checksum: a37b029f544c9f91919cd44368238523600bb645

Image information:
Acquisition started: Mon Nov 22 10:25:29 2021
Acquisition finished: Mon Nov 22 10:49:47 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad29

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad30

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad31

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad32

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad33

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad34

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad35

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad36

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad37

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad38

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad39

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad40

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad41

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad42

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad43

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad44

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad45

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad46

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad47

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad48

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad49

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad50

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad51

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad52

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad53

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad54

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad55

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad56

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad57

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad58

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad59

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad60

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad61

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad62

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad63

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad64

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad65

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad66

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad67

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad68

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad69

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad70

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad71

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad72

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad73

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad74

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad75

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad76

I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad77 I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad78 I:\EVIDENCIA_MAPFRE_2\10.JMRIANO\IMAGENFORENSE_PST_JMRIANO_MAPFRE_22NOV2021.ad79 Image Verification Results: Verification started: Mon Nov 22 10:49:48 2021 Verification finished: Mon Nov 22 10:58:24 2021 MD5 checksum: de6744c8bb0c6717f072120e5caaa982 : verified SHA1 checksum: a37b029f544c9f91919cd44368238523600bb645 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB,** el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:





Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**jmriano@mapfre.com.co.**" asignado a **José Manuel RIAÑO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 101 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

- **ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO JMRIANO@MAPFRE.COM.CO."**

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo

electrónico **jmriano@mapfre.com.co** asignada **José Manuel RIAÑO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
10	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	José Manuel RIAÑO → jmriano@mapfre.com.co	ad1	115 GB
TOTAL					**115 GB**

Tabla 21 Detalle del buzón de correo electrónico asignado jmriano@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico jmriano@mapfre.com.co asignado a **José Manuel RIAÑO** para el desarrollo de sus funciones **aloja** un total de **115GB,** dentro de este espacio el laboratorio de informática forense logró hallar un total de **Tres millones veinticinco mil ciento dieciocho (3.025.118)** archivos (incluyendo carpetas), como se observa a continuación.



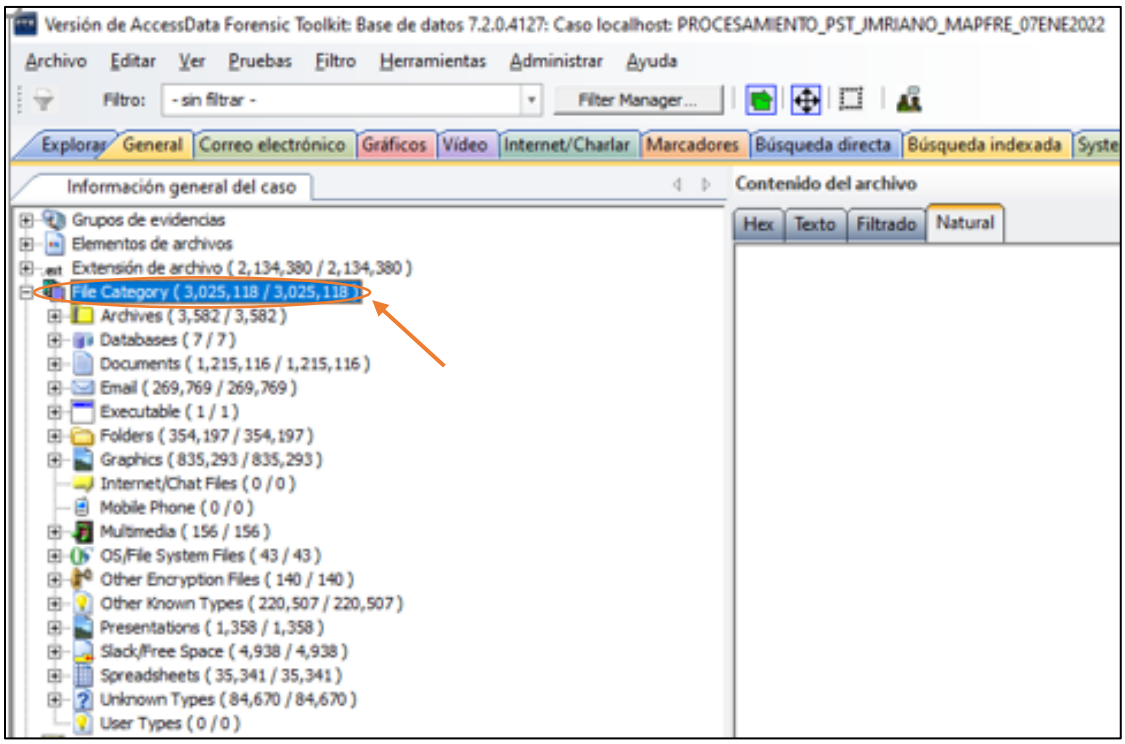


Ilustración 102 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico jmriano@mapfre.com.co.

- **RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JOSÉ MANUEL RIAÑO → JMRIANO@MAPFRE.COM.CO.**

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico jmriano@mapfre.com.co asignado a José Manuel RIAÑO , iniciando el día el **07** de enero de 2022 con una duración aproximada de dieciocho (18) días calendario, el resultado a dicho proceso arrojó que existen **cero (0**) ítems en condición de "eliminados" y se reconstruyeron **Cuatrocientos ochenta y siete mil ciento cincuenta y siete (487.157)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

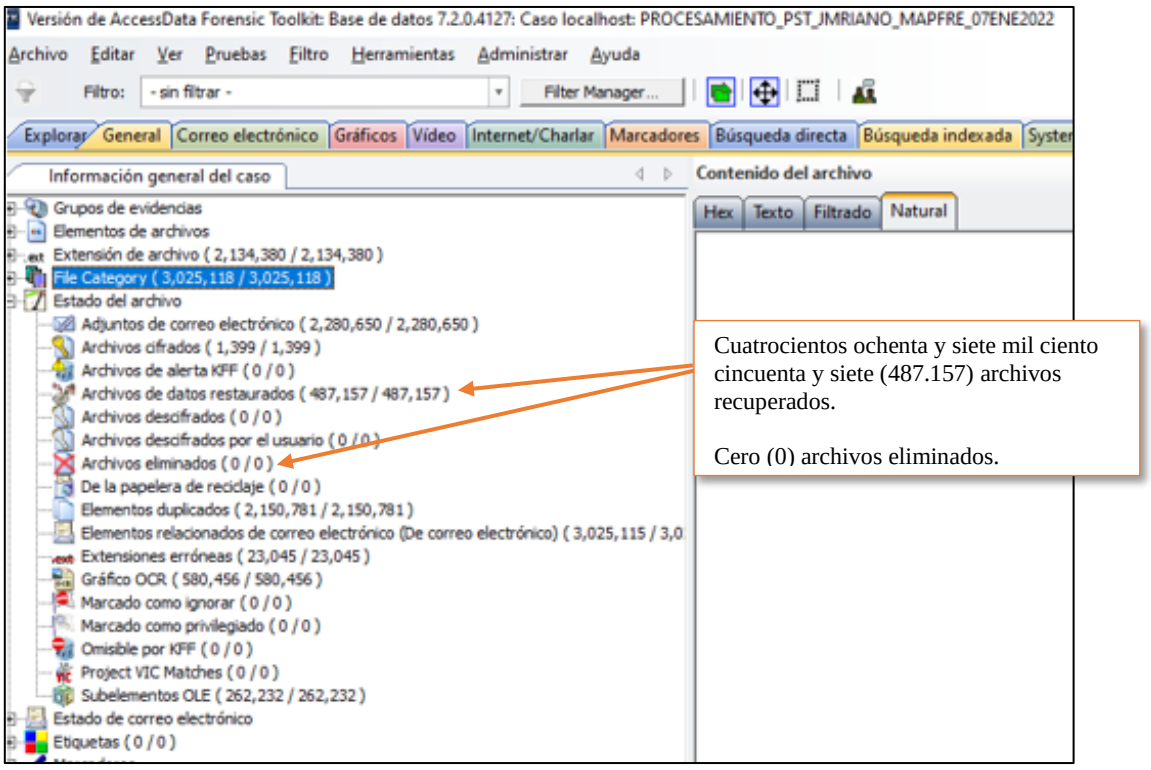


ilustración 103 Total de archivos recuperados en la cuenta de correo electrónico jmriano@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Tres millones veinticinco mil ciento dieciocho (3.025.118)** de archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO JMRIANO@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico jmriano@mapfre.com.co asignado a **José Manuel RIAÑO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	3.582
2	Bases de Datos	7
3	Documentos	1.215.116
4	Correo Electrónico	269.769
5	Ejecutables	1
6	Carpetas	354.197
7	Gráficos	835.293
8	Multimedia	156
9	Archivos del sistema	43
10	Otros archivos encriptados	140
11	Otros archivos desconocidos	220.507
12	Presentaciones	1.358
13	Espacio libre	4.938
14	Hojas de cálculo	35.341
15	Tipos de archivos desconocidos	84.670
TOTAL		**3.025.118**

Tabla 22 Información buscada evidencia 10_JMRIANO, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Tres millones veinticinco mil ciento dieciocho (3.025.118).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Dos millones doscientos ochenta mil seiscientos cincuenta (2.280.650) archivos de**

datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Los archivos cifrados recuperados **Mil trescientos noventa y nueve (1.399) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Cuatrocientos ochenta y siete mil ciento cincuenta y siete (487.157) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Dos millones ciento cincuenta mil setecientos ochenta y un (2.150.781) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Tres millones veinticinco mil ciento quince (3.025.115) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Veintitrés mil cuarenta y cinco (23.045) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Quinientos ochenta mil cuatrocientos cincuenta y seis (580.456) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Doscientos sesenta y dos mil doscientos treinta y dos (262.232) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico jmriano@mapfre.com.co asignado a **José Manuel RIAÑO** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



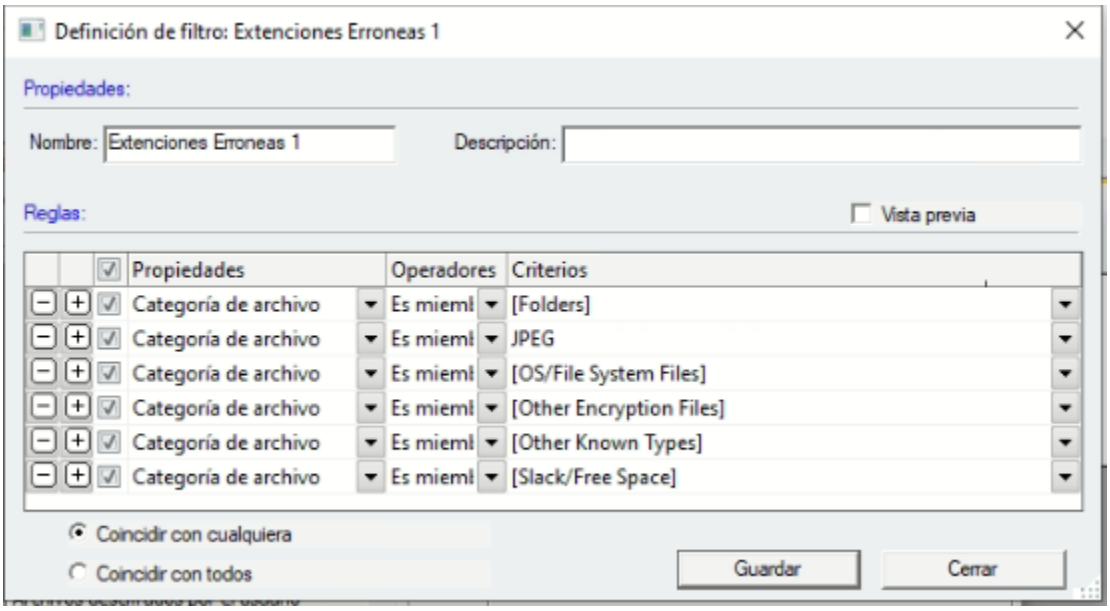


Ilustración 104 Filtro para excluir las extensiones erróneas.

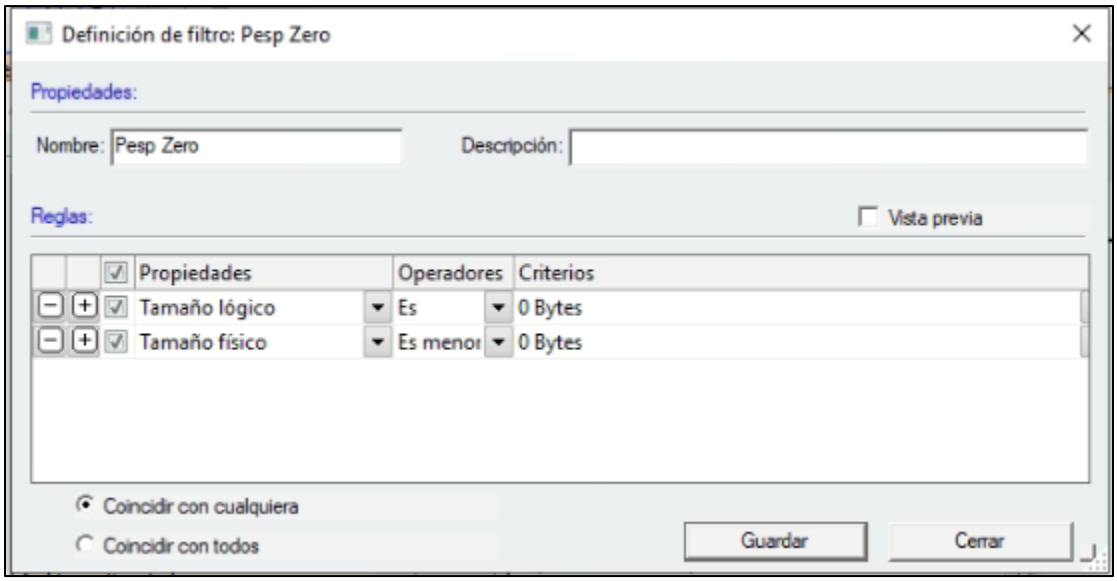


Ilustración 105 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

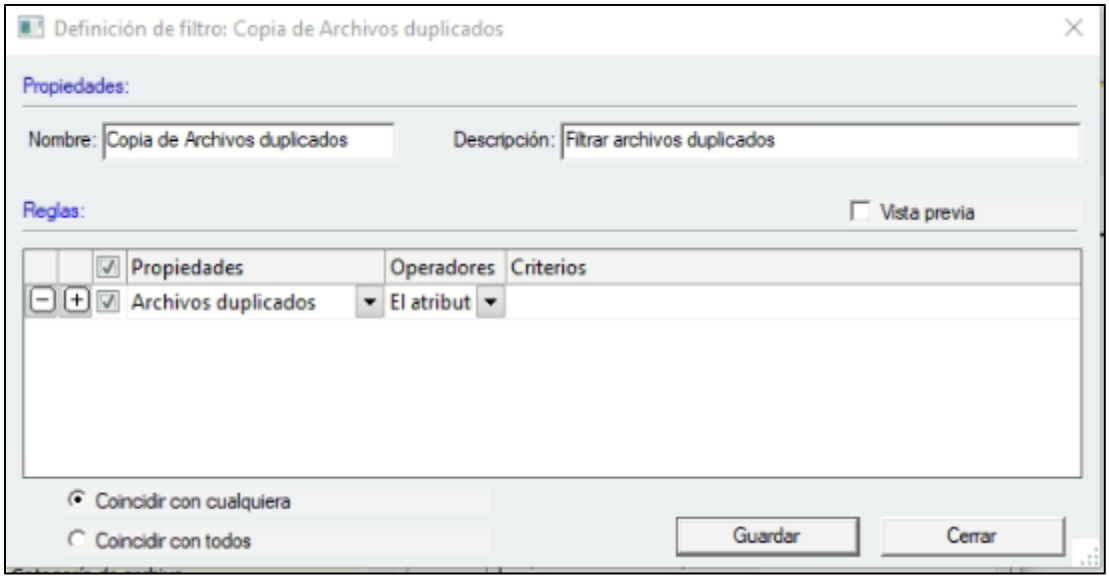


Ilustración 106 Filtro para excluir los archivos duplicados.

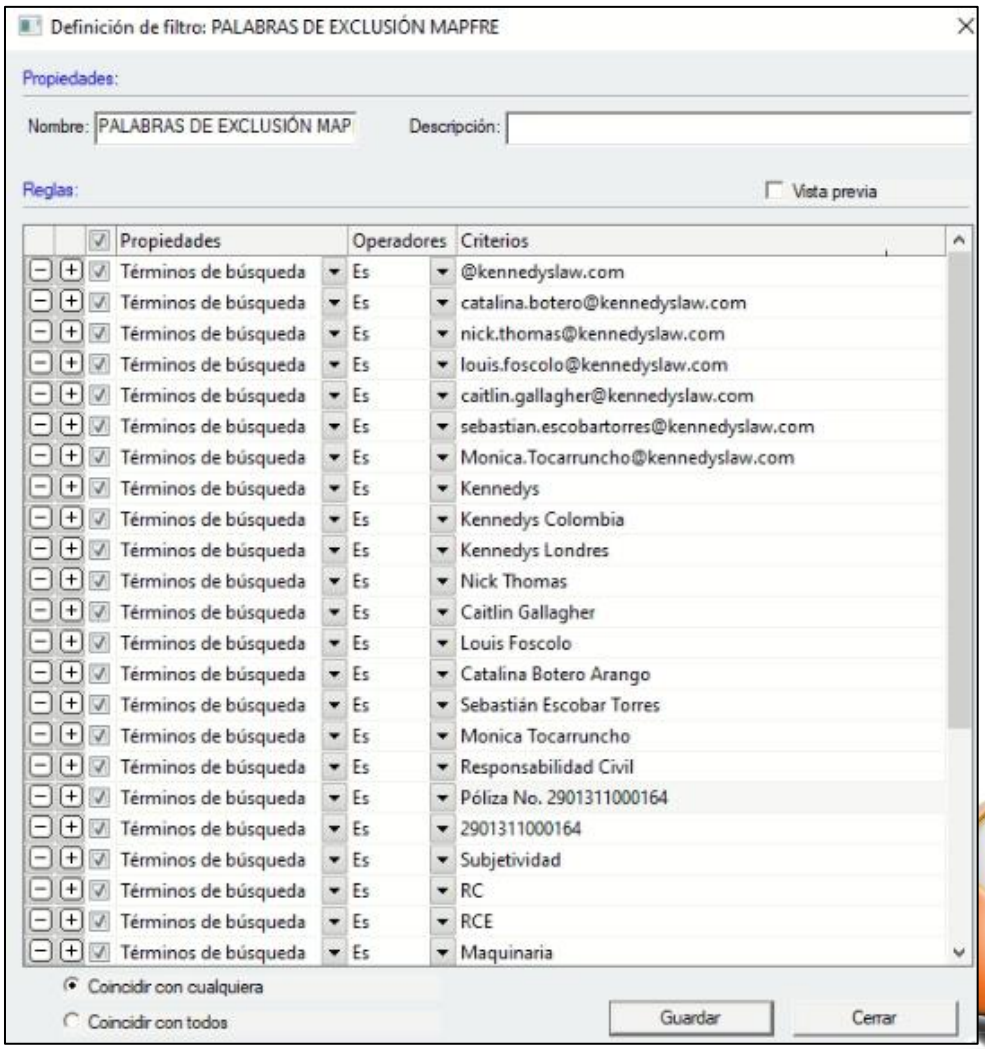


Ilustración 107 Filtro para excluir los archivos suministrado por MAPFRE - 1.

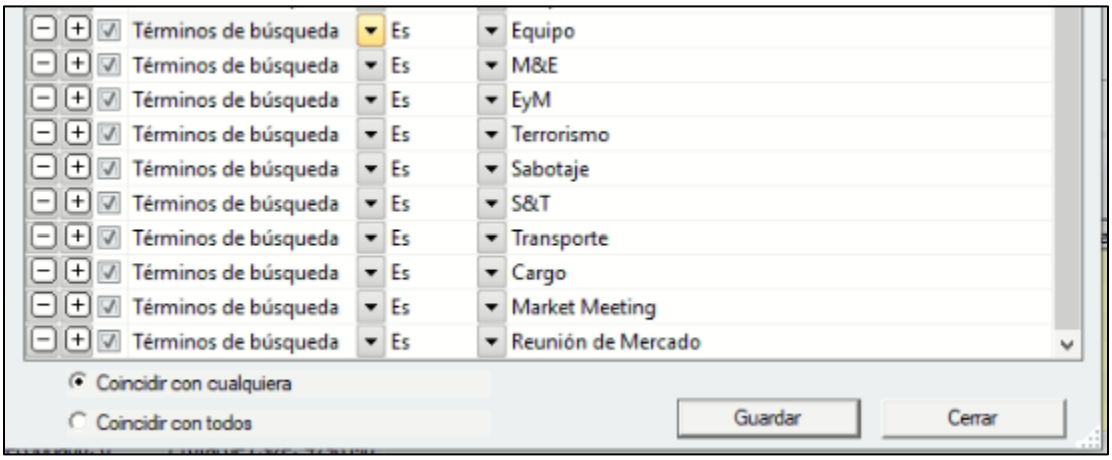
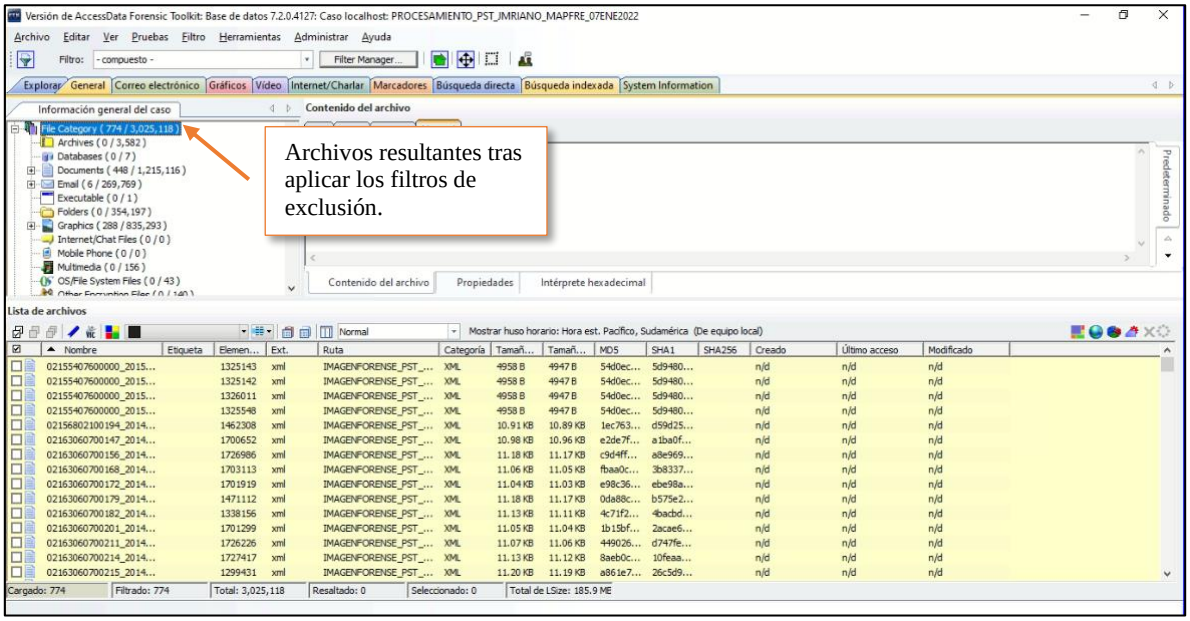


Ilustración 108 Filtro para excluir los archivos suministrado por MAPFRE - 2.

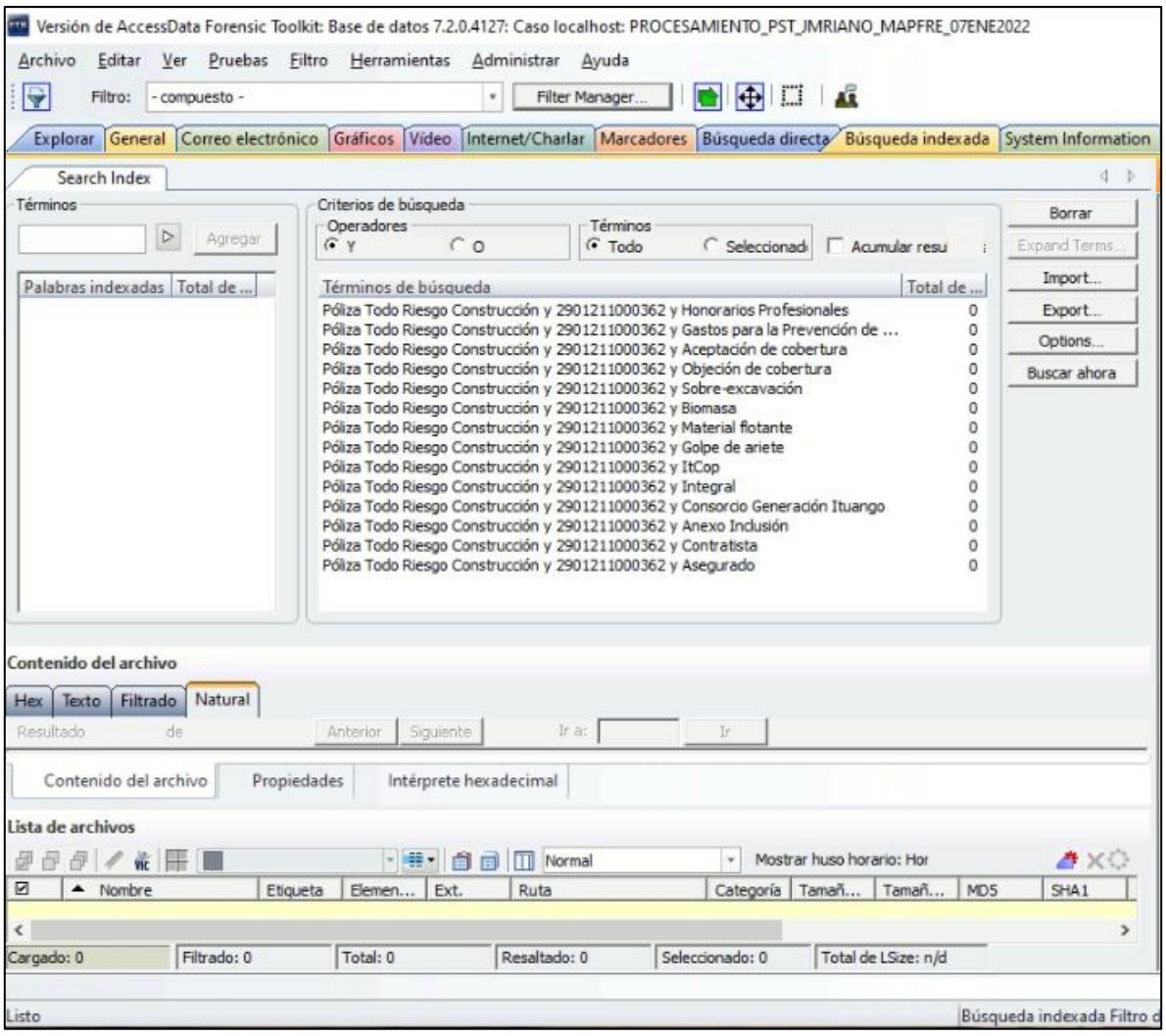
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Setecientos setenta y cuatro (774)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo jmriano@mapfre.com.co asignado a **José Manuel RIAÑO** para el desarrollo de sus funciones.

11. Buzón de correo electrónico jmerine@mapfre.com.co.

El día 22 de noviembre 2021, el equipo de ADALID CORP ingresa a la carpeta **JMERINE**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

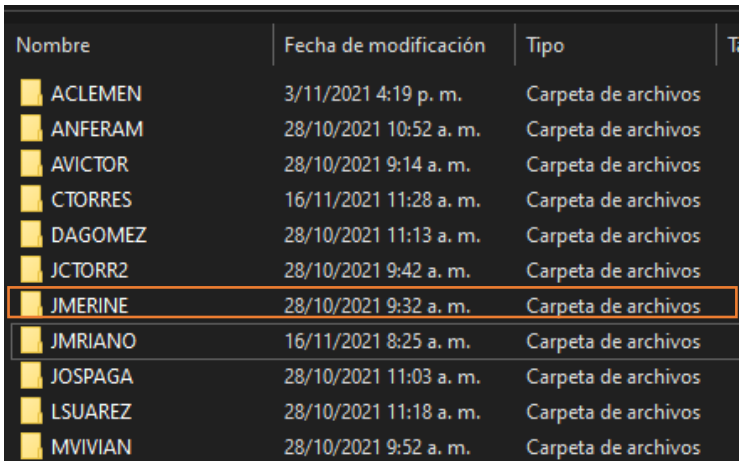


Ilustración 109 Visualización carpeta JMERINE.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **JMERINE** identificada dentro del disco duro como se observa en las siguientes imágenes:

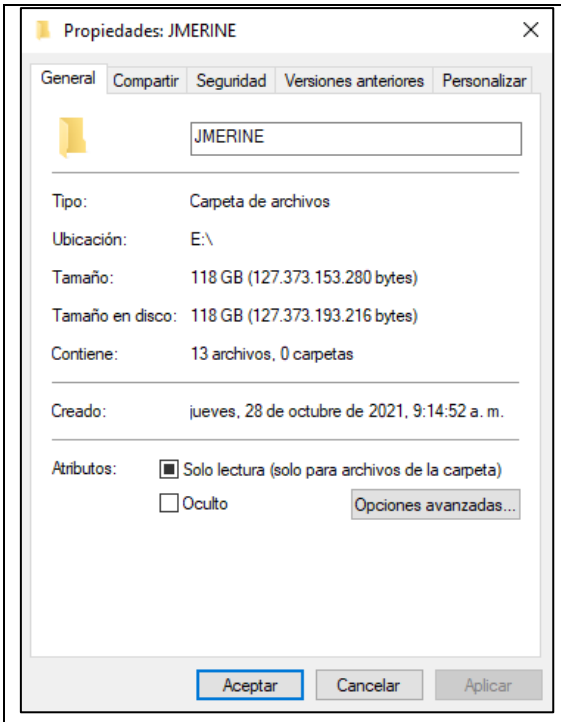


Ilustración 110 Propiedades de la carpeta JMERINE visto desde el Disco Duro.

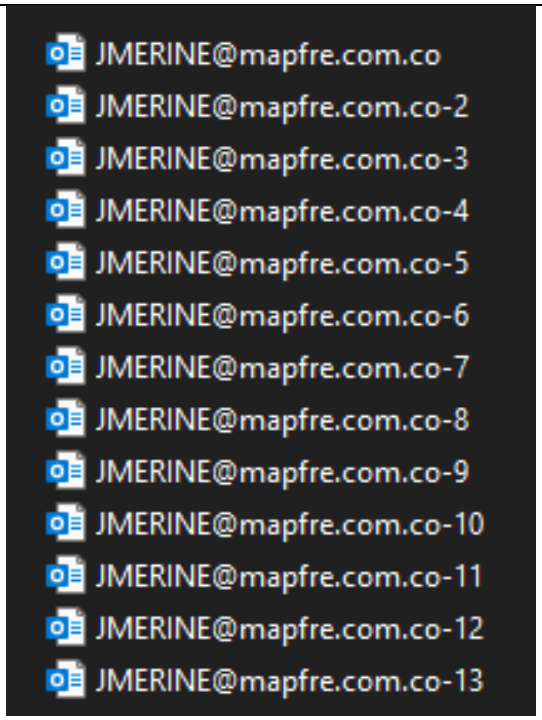


Ilustración 111 Contenido de la carpeta JMERINE visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**jmerine@mapfre.com.co.**" asignado a

José Manuel MERINERO MARTIN para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **11:13:27** y culminando el mismo de forma satisfactoria a las **11:47:50,** tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_22NOV2021
Número de prueba: 11_JMERINE
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO JMERINE@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for
I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad1:
[Custom Content Sources]
K::K:\ | JMERINE | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: 4ca2ff21652b030e18792d53572fc81a
SHA1 checksum: fdf3b09289d272e99375b5a141b0617ae789e477

Image information:
Acquisition started: Mon Nov 22 11:13:27 2021
Acquisition finished: Mon Nov 22 11:38:20 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad1

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad2

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad3

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad4

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad5

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad6

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad7

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad8

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad9

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad10

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad11

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad12

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad13

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad14

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad15

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad16

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad17

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad18

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad19

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad20

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad21

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad22

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad23

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad24

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad25

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad26

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad27

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad28

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad29

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad30

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad31

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad32

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad33

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad34

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad35

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad36

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad37

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad38

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad39

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad40

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad41

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad42

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad43

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad44

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad45

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad46

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad47

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad48

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad49

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad50

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad51

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad52

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad53

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad54

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad55

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad56

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad57

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad58

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad59

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad60

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad61

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad62

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad63

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad64

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad65

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad66

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad67

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad68

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad69

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad70

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad71

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad72

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad73

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad74

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad75

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad76

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad77

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad78

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad79

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad80

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad81

I:\EVIDENCIA_MAPFRE_2\11.JMERINE\IMAGENFORENSE_PST_JMERINE_MAPFRE_22NOV2021.ad82

Image Verification Results:
Verification started: Mon Nov 22 11:38:23 2021
Verification finished: Mon Nov 22 11:47:50 2021
MD5 checksum: 4ca2ff21652b030e18792d53572fc81a : verified
SHA1 checksum: fdf3b09289d272e99375b5a141b0617ae789e477 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**jmerine@mapfre.com.co.**" asignado a **José Manuel MERINERO MARTIN** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 112 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO JMERINE@MAPFRE.COM.CO.

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**. para la cuenta de correo electrónico jmerine@mapfre.com.co asignada a **José Manuel MERINERO MARTIN** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
11	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	José Manuel MERINERO MARTIN → jmerine@mapfre.com.co	ad1	118 GB
TOTAL					**118 GB**

Tabla 23 Detalle del buzón de correo electrónico asignado jmerine@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico jmerine@mapfre.com.co asignado a **José Manuel MERINERO**

MARTIN para el desarrollo de sus funciones **aloja** un total de **118 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Trescientos treinta y seis mil seiscientos veintiséis (336.626)** archivos (incluyendo carpetas), como se observa a continuación.

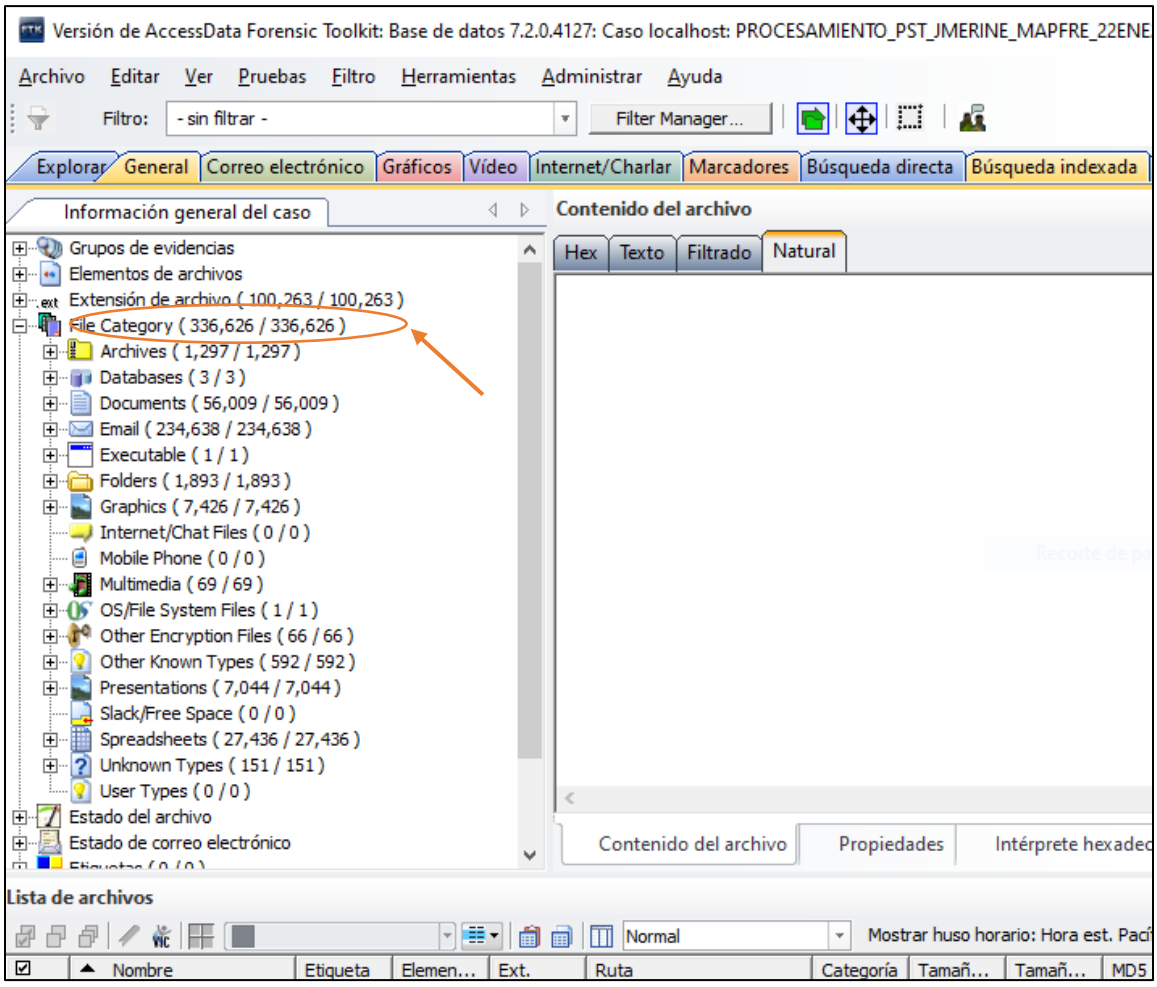


Ilustración 113 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico jmerine@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JOSÉ MANUEL MERINERO MARTIN → JMERINE@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico jmerine@mapfre.com.co asignado a **José Manuel MERINERO MARTIN**, iniciando el día el **22** de enero

del 2022 con una duración aproximada de Siete (7) día calendario, el resultado a dicho proceso arrojó que existen **cero (0)** ítems en condición de "eliminados" y se reconstruyeron **cero (0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

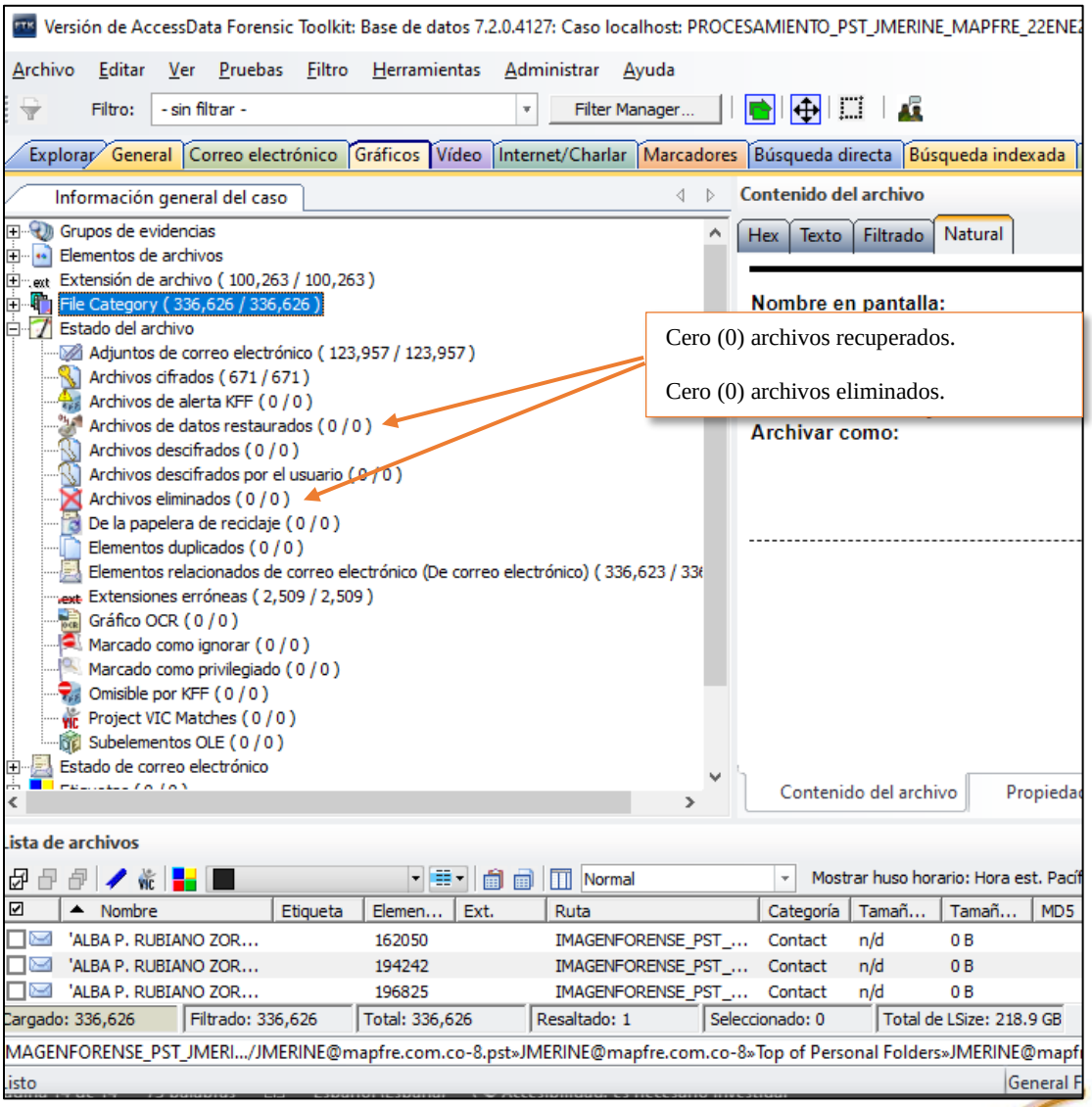


ilustración 114 Total de archivos recuperados en la cuenta de correo electrónico jmerine@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS**

GENERALES DE COLOMBIA S.A., es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Trescientos treinta y seis mil seiscientos veintiséis (336.626)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO JMERINE@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico jmerine@mapfre.com.co asignado a **José Manuel MERINERO MARTIN** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1.297
2	Bases de Datos	3
3	Documentos	56.009
4	Correo Electrónico	234.638
5	Ejecutables	1
6	Carpetas	1.893
7	Gráficos	7.426
8	Multimedia	69
9	Archivos del sistema	1
10	Otros archivos encriptados	66
11	Otros archivos desconocidos	592
12	Presentaciones	7.044
13	Hojas de cálculo	27.436
14	Tipos de archivos desconocidos	151
TOTAL		**336.626**

Tabla 24 Información buscada evidencia 011_JMERINE, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Trescientos treinta y seis mil seiscientos veintiséis (336.626).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Ciento veintitrés mil novecientos cincuenta y siete (123.957) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Seiscientos setenta y un (671) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Trescientos treinta y seis mil seiscientos veintitrés (336.623) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Dos mil quinientos nueve (2.509) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico jmerine@mapfre.com.co asignado a **José Manuel MERINERO MARTIN** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

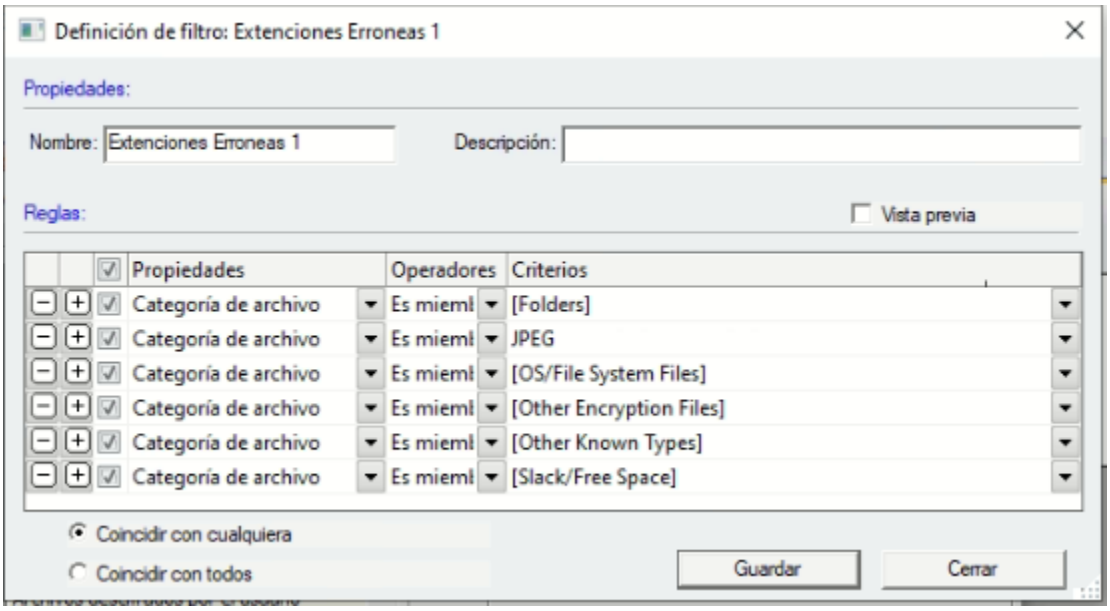


Ilustración 115 Filtro para excluir las extensiones erróneas.

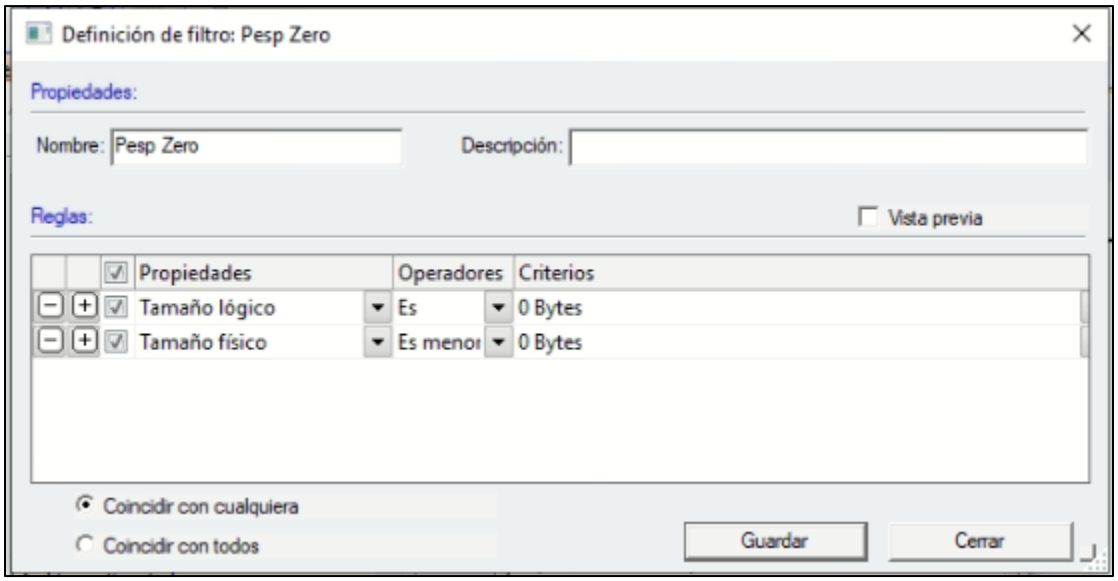


Ilustración 116 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

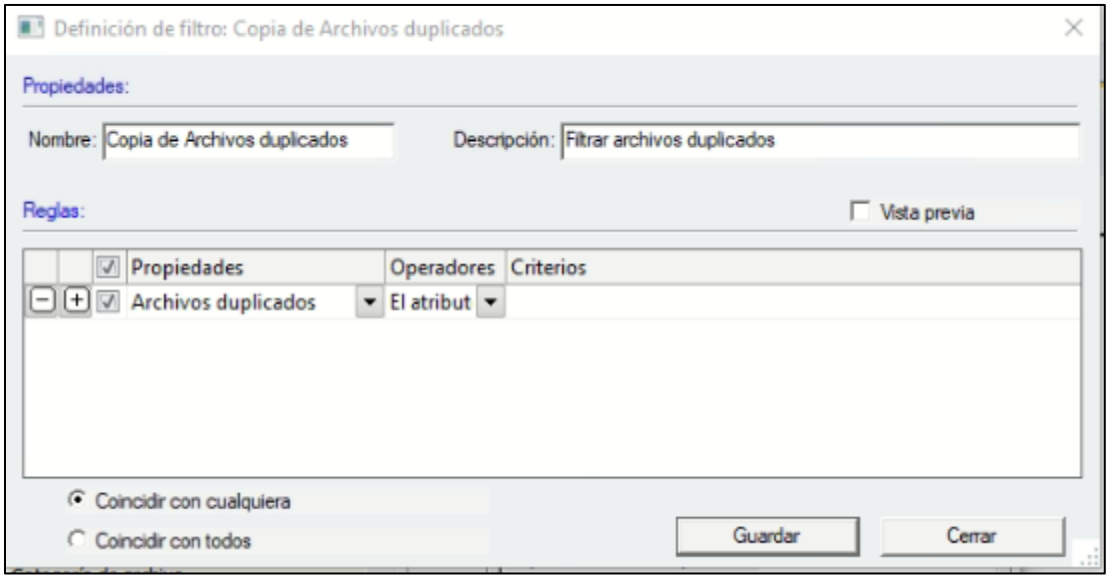


Ilustración 117 Filtro para excluir los archivos duplicados.

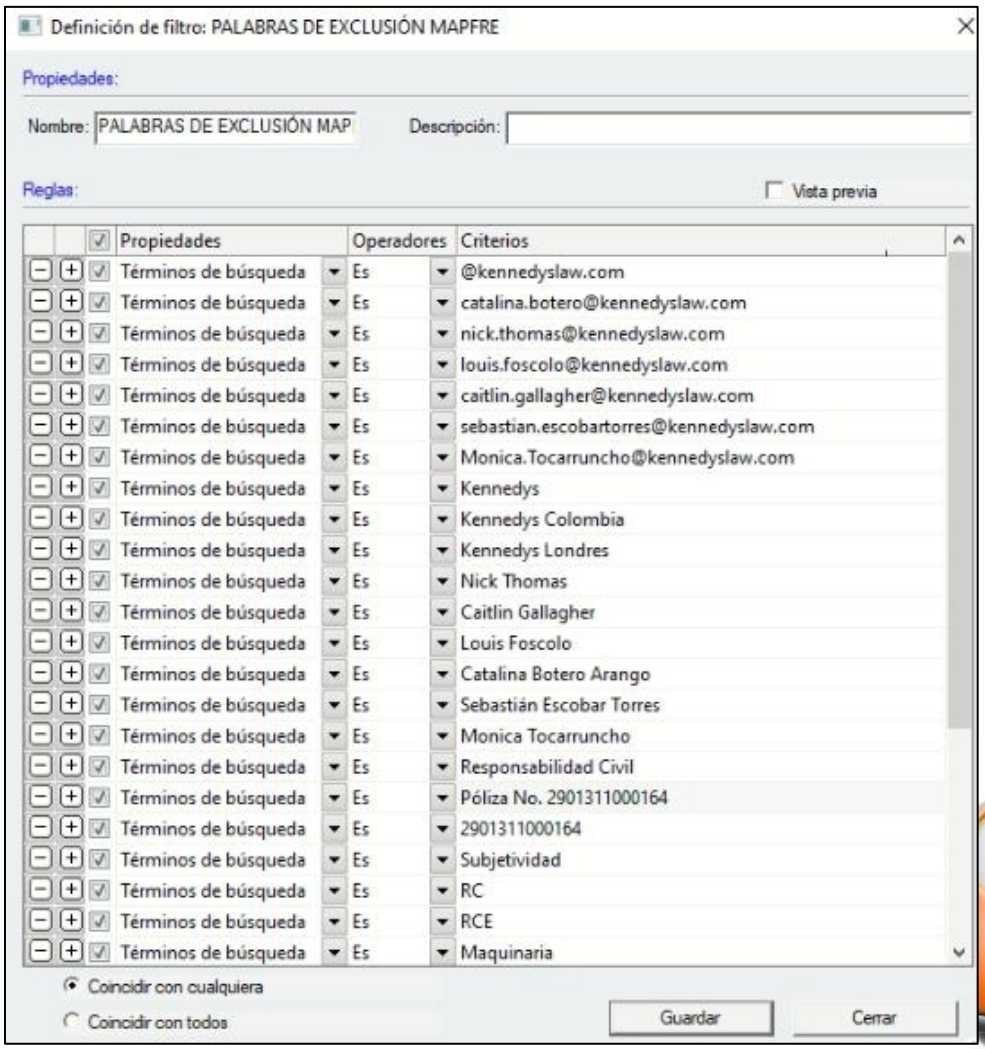


Ilustración 118 Filtro para excluir los archivos suministrado por MAPFRE - 1.

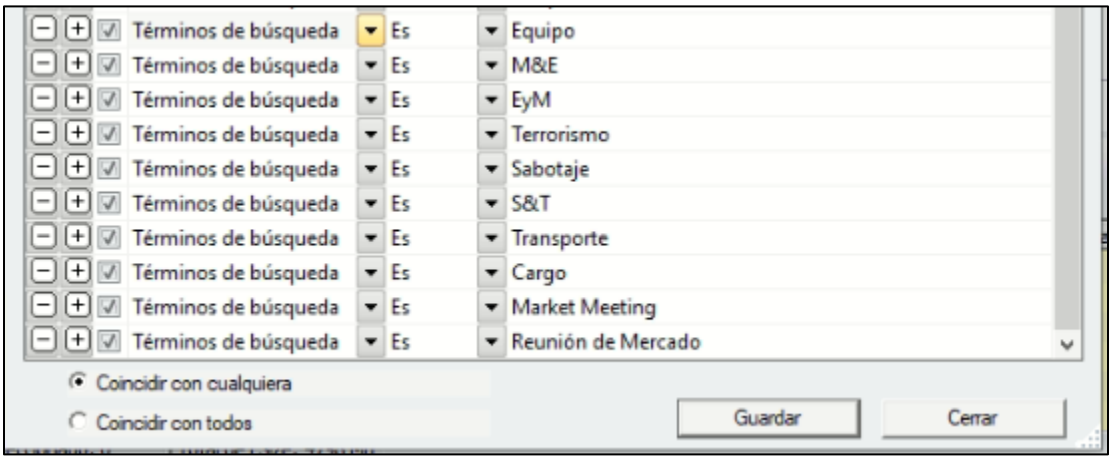
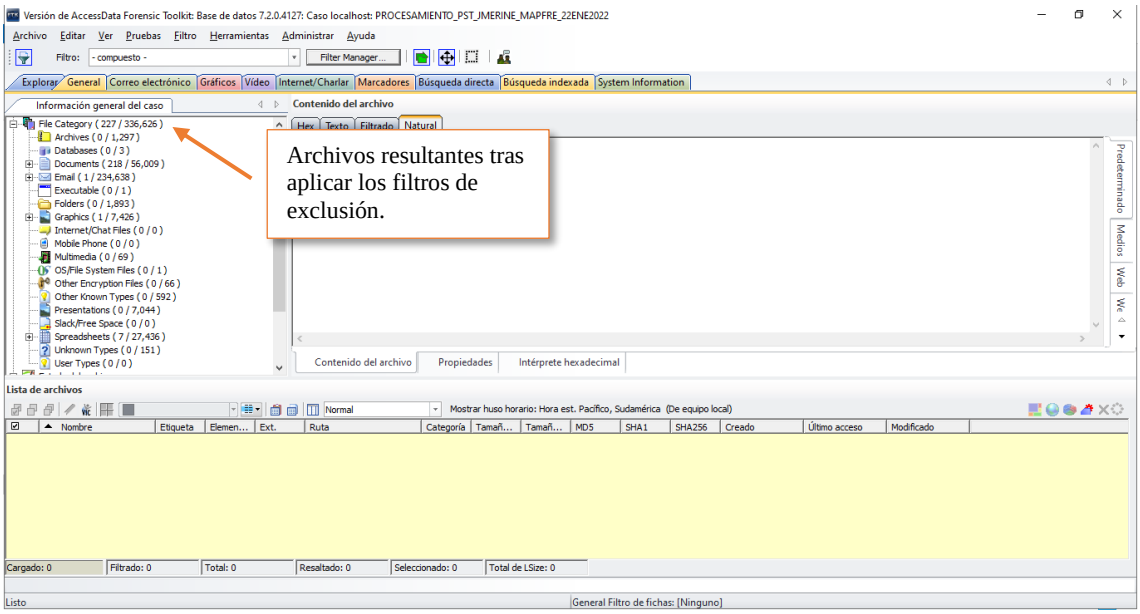


Ilustración 119 Filtro para excluir los archivos suministrado por MAPFRE - 2.

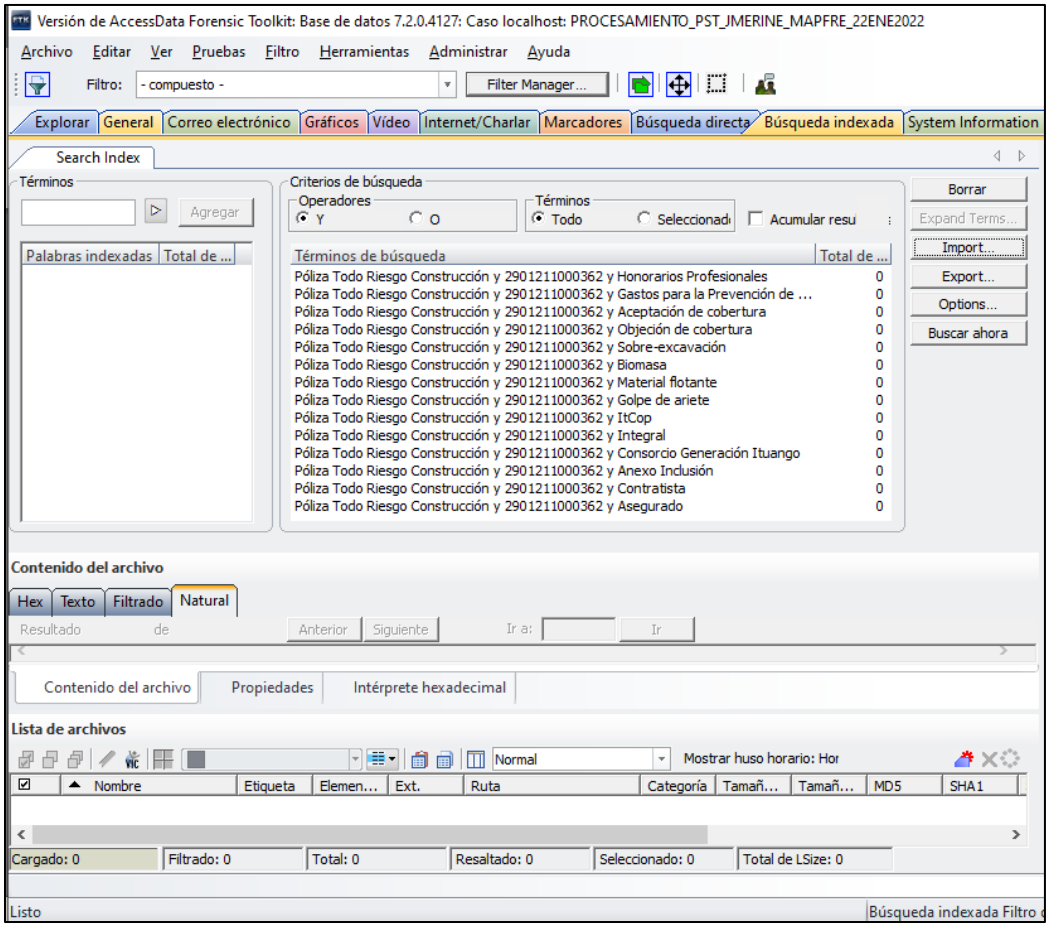
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Doscientos veintisiete (227)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo jmerine@mapfre.com.co asignado a **José Manuel MERINERO MARTIN** para el desarrollo de sus funciones.

Una vez realizadas las imágenes forenses para los buzones de correo electrónico pertenecientes a exfuncionarios de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** los cuales se encuentran identificados con las siguientes direcciones de correo (aclemen@mapfre.com.co, anferam@mapfre.com.co, avictor@mapfre.com.co, ctorres@mapfre.com.co, dagomez@mapfre.com.co, jctorr2@mapfre.com.co, jmerine@mapfre.com.co, jmriano@mapfre.com.co, jospaga@mapfre.com.co, lsuarez@mapfre.com.co, mvivian@mapfre.com) el equipo de ADALID CORP hace entrega de (1) Un disco duro color blanco, con capacidad de almacenamiento de **1000GB** al señor **Willigton Leandro TORRES MORALES,** identificado con cédula de ciudadanía **No. 79.708.420** de Bogotá, quien funge como **PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN** el día 30 de noviembre a las 11:50 horas.

El día 01 de diciembre de 2021, el señor **Willigton Leandro TORRES MORALES** hace entrega a los peritos de ADALID CORP. de (1) Un disco duro color blanco, con capacidad de almacenamiento de **1000GB,** el cual en su parte superior se encuentra marcado como **"prueba extraprocesal"** como se presenta a continuación**:**

	
Fotografía Disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista superior)	Fotografía disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista posterior)

Dentro del Disco Duro se encuentran los archivos en formato .PST de las cuentas de correo electrónico asignadas a Once (11) funcionarios que se encuentran retirados y Cuatro (4) cuentas de correo electrónico de funcionarios activos dentro de la empresa **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A,** los cuales serán mencionados a continuación:

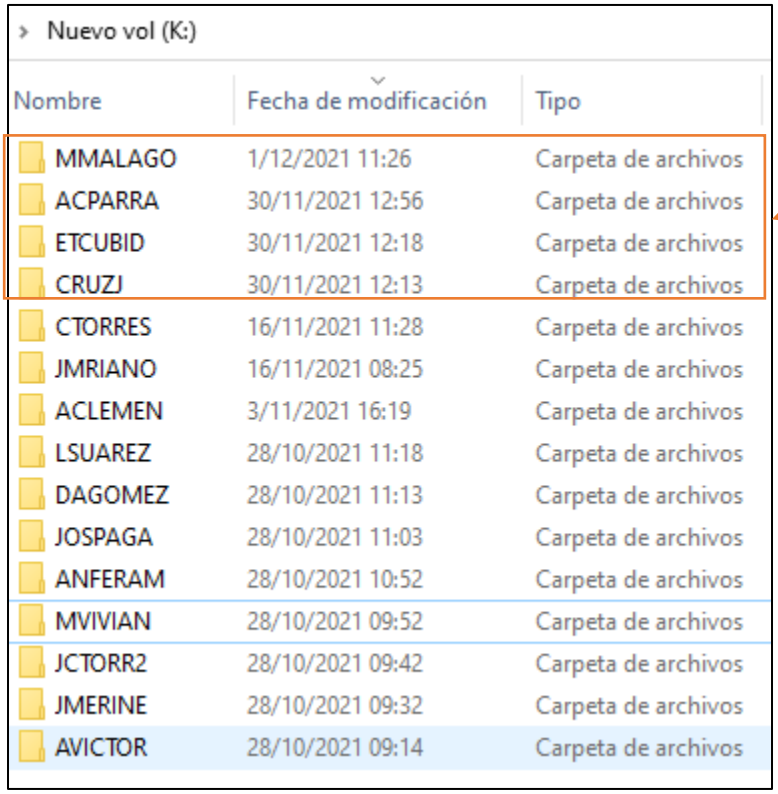


Ilustración 120 Visualización contenido completo del Disco Duro entregado por MAPFRE SEGUROS GENERALES DE COLOMBIA S.A a 01 de diciembre de 2021.

Los correos electrónicos suministrados el 01 de diciembre de 2021 serán presentados a continuación:

Correos funcionarios retirados	ORDEN ENVIO IMÁGENES fecha en la que se realizo	Tamaño GB
mmalago@mapfre.com.co	15 - 01-diciembre-2021	58.3 GB
acparra@mapfre.com.co	12 - 01-diciembre-2021	43.0 GB
etcubid@mapfre.com.co	14 - 01-diciembre-2021	55.9 GB
cruzj@mapfre.com.co	13 - 01-diciembre-2021	50.1 GB

Tabla 25 *Buzones de correo suministrados el 01 de diciembre de 2021.*

12. Buzón de correo electrónico acparra@mapfre.com.co.

El día 01 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta **ACPARRA**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

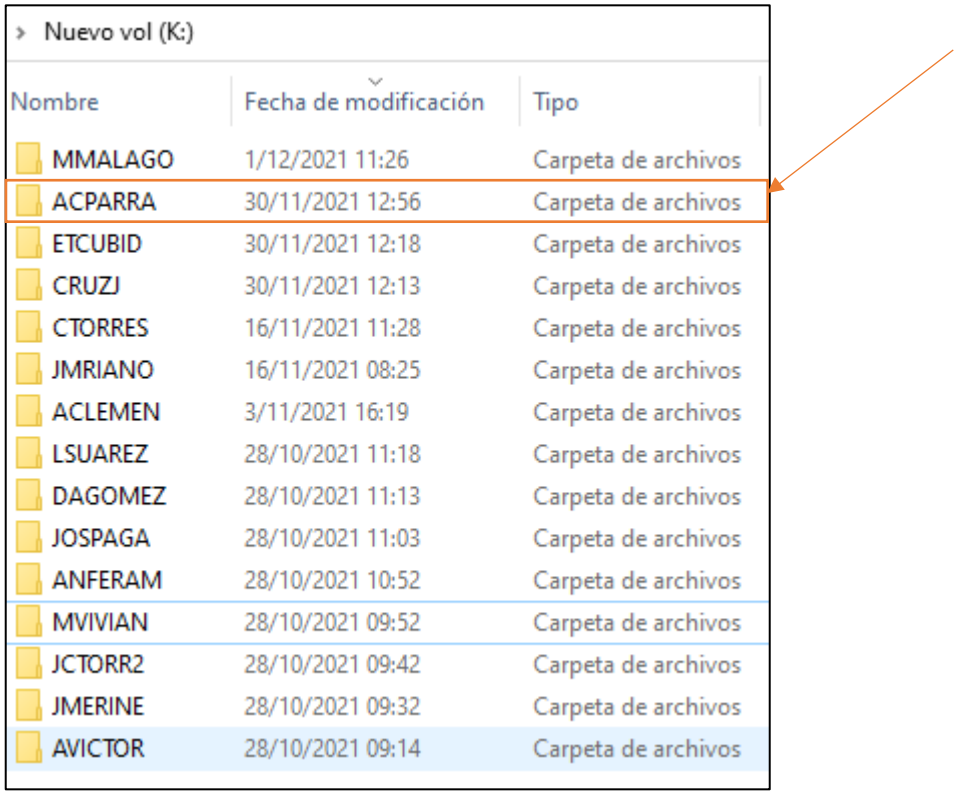


Ilustración 121 Visualización carpeta ACPARRA.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **ACPARRA** identificada dentro del disco duro como se observa en las siguientes imágenes:

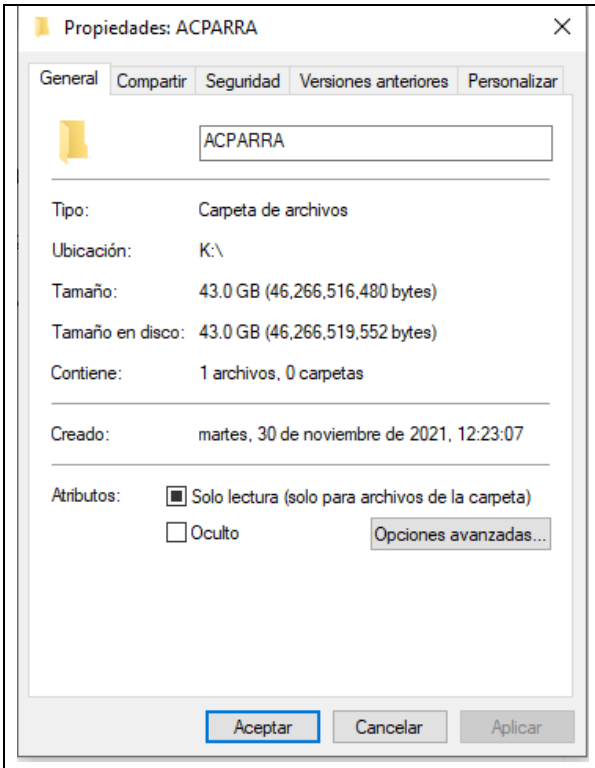


Ilustración 122 Propiedades de la carpeta ACPARRA visto desde el Disco Duro.

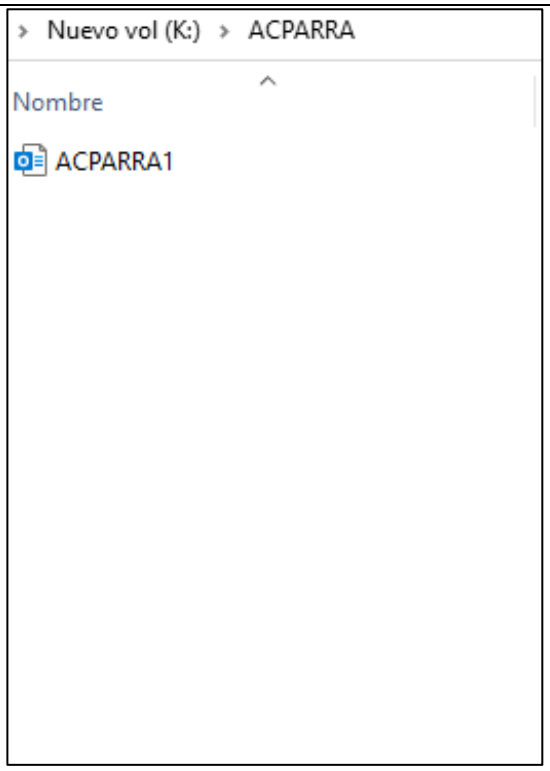


Ilustración 123 Contenido de la carpeta ACPARRA visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**acparra@mapfre.com.co.**" asignado a **Andrés Camilo PARRA BALAGUERO** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **14:12:31** y culminando el mismo de forma satisfactoria a las **15:14:07**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_01DIC2021
Número de prueba: 012_ACPARRA
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ACPARRA@MAPFRE.COM.CO, ENTREGADOS POR

MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP S.A.S. - Hector Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad1:
[Computed Hashes]
MD5 checksum: 31383bb73ba2962329cfe4057918b2ff
SHA1 checksum: d937640697a74fe39a1dabfcfeb857c096bd6b16

Image information:
Acquisition started: Wed Dec 1 14:12:31 2021
Acquisition finished: Wed Dec 1 15:02:34 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad22 I:\EVIDENCIA_MAPFRE_2\12.ACPARRA\IMAGENFORENSE_PST_ACPARRA_MAPFRE_01DIC2021.ad23 Image Verification Results: Verification started: Wed Dec 1 15:02:34 2021 Verification finished: Wed Dec 1 15:14:07 2021 MD5 checksum: 31383bb73ba2962329cfe4057918b2ff : verified SHA1 checksum: d937640697a74fe39a1dabfcfeb857c096bd6b16 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**acparra@mapfre.com.co.**" asignado a **Andrés Camilo PARRA BALAGUERO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 124 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ACPARRA@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico acparra@mapfre.com.co asignada **Andrés Camilo PARRA BALAGUERO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
12	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Andrés Camilo PARRA BALAGUERO → acparra@mapfre.com.co	ad1	43.0 GB
TOTAL					**43.0 GB**

Tabla 26 Detalle del buzón de correo electrónico asignado acparra@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico acparra@mapfre.com.co asignado a **Andrés Camilo PARRA BALAGUERO** para el desarrollo de sus funciones **aloja** un total de **43.0 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Seiscientos noventa y dos mil doscientos ochenta y nueve (692.289)** archivos (incluyendo carpetas), como se observa a continuación.

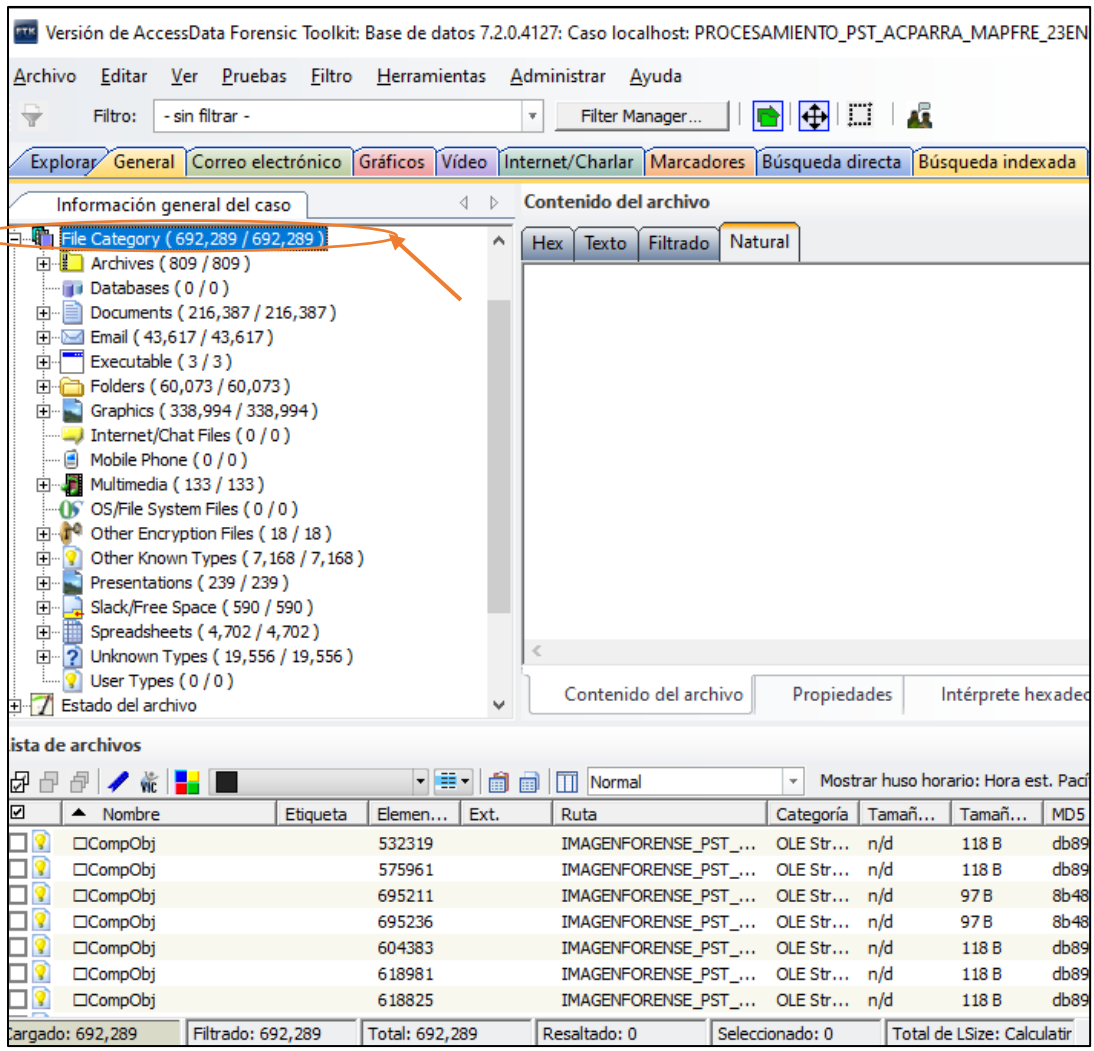


Ilustración 125 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico acparra@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO ANDRÉS CAMILO PARRA BALAGUERO → ACPARRA@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico acparra@mapfre.com.co asignado a **Andrés Camilo PARRA BALAGUERO**, iniciando el día el **23** de enero del 2022 con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **Dos (2)** ítems en condición de "eliminados" y se reconstruyeron **Ciento noventa y siete mil ochocientos veintiocho (197.828)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron

recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

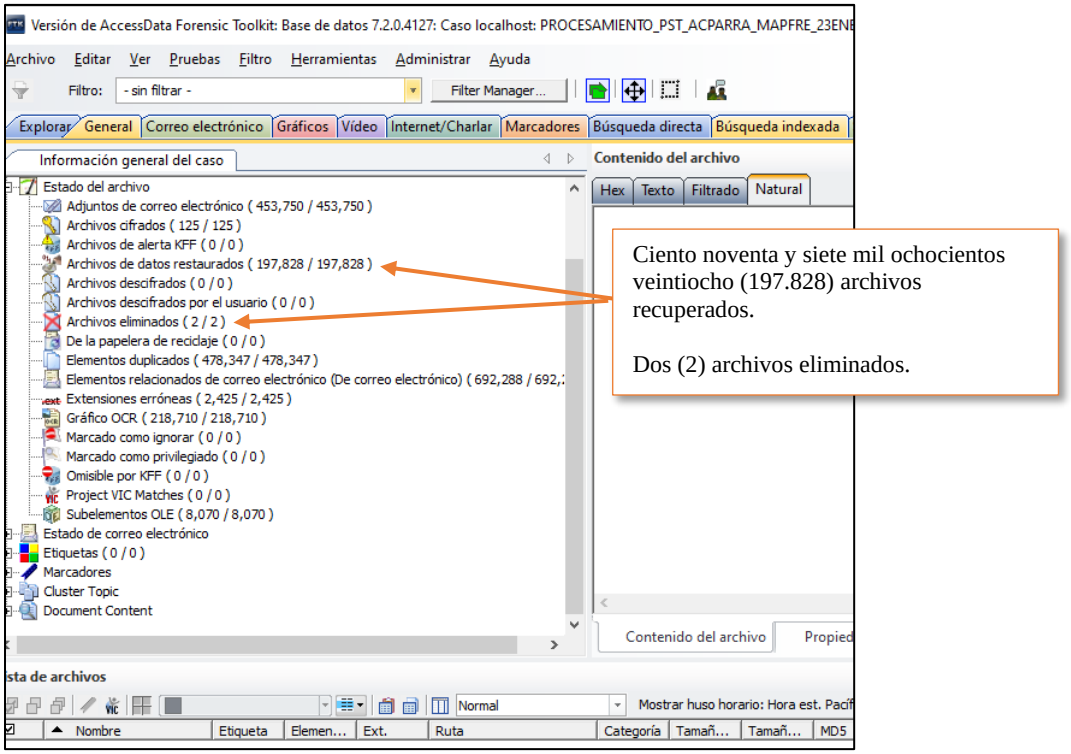


ilustración 126 Total de archivos recuperados en la cuenta de correo electrónico acparra@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Seiscientos noventa y dos mil doscientos ochenta y nueve (692.289)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ACPARRA@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico acparra@mapfre.com.co asignado a **Andrés Camilo PARRA BALAGUERO para** el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	809
2	Documentos	216.387
3	Correo Electrónico	43.617
4	Ejecutables	3
5	Carpetas	60.073
6	Gráficos	338.994
7	Multimedia	133
8	Otros archivos encriptados	18
9	Otros archivos desconocidos	7.168
10	Presentaciones	239
11	Espacio libre del sistema	590
12	Hojas de cálculo	47.02
13	Tipos de archivos desconocidos	19.556
TOTAL		**692.289**

Tabla 27 Información buscada evidencia 012_ACPARRA, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Seiscientos noventa y dos mil doscientos ochenta y nueve (692.289)**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Cuatrocientos cincuenta y tres mil setecientos (453.750) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Ciento veinticinco (125) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos restaurados **Ciento noventa y siete mil ochocientos veintiocho (197.828) archivos de datos obtenidos** por el

proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Archivos de datos Eliminados **Dos (2) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Cuatrocientos setenta y ocho mil trescientos cuarenta y siete (478.347) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Seiscientos noventa y dos mil doscientos ochenta y ocho (692.288) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Dos mil cuatrocientos veinticinco (2.425) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Doscientos dieciocho mil setecientos diez (218.710) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Ocho mil setenta (8.070) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico acparra@mapfre.com.co asignado a **Andrés Camilo PARRA BALAGUERO** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



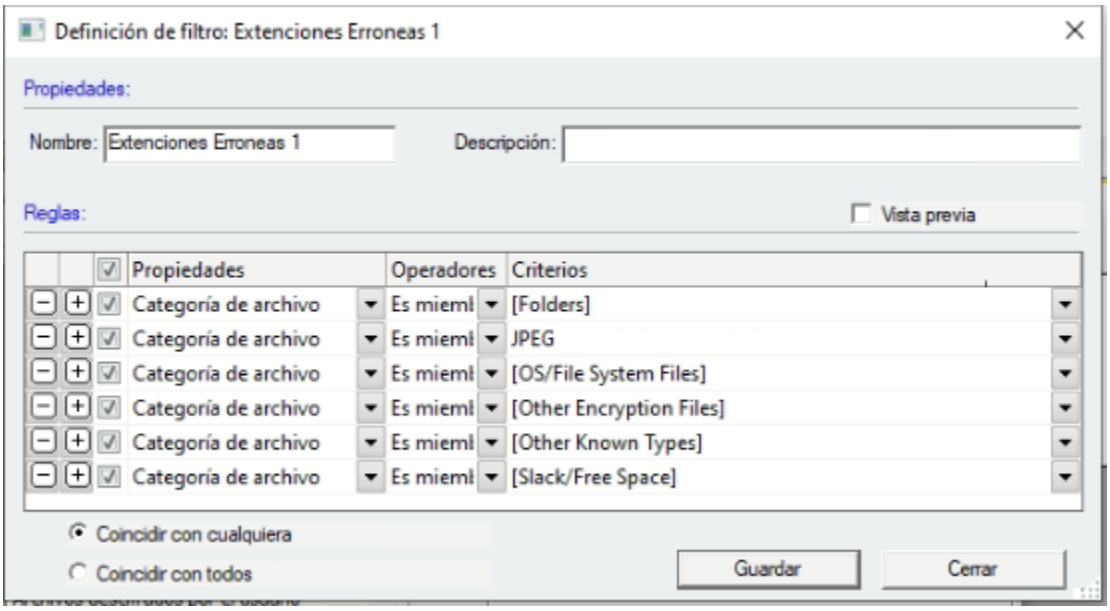


Ilustración 127 Filtro para excluir las extensiones erróneas.

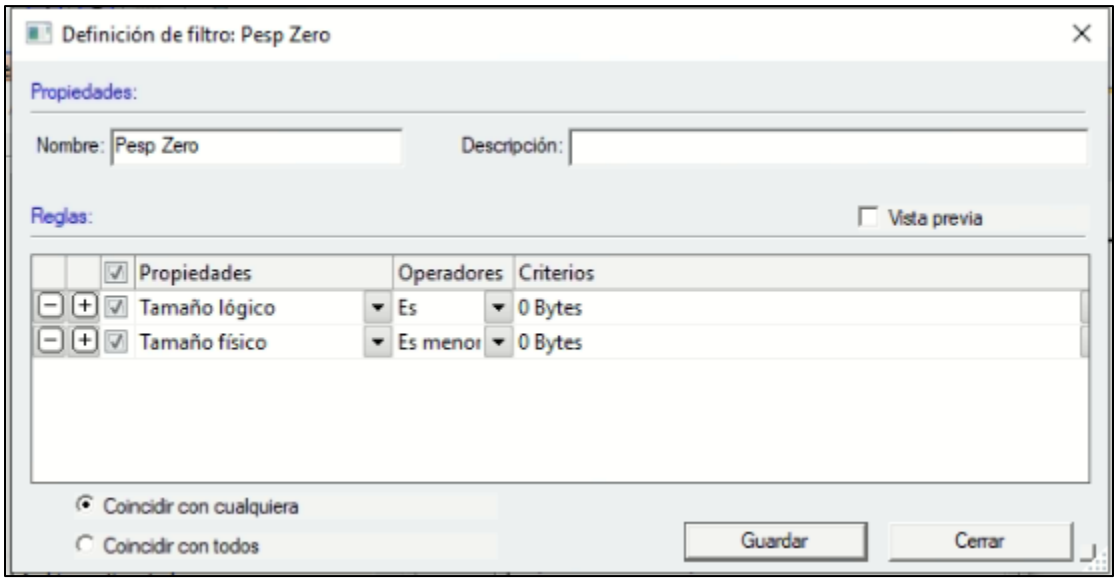


Ilustración 128 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

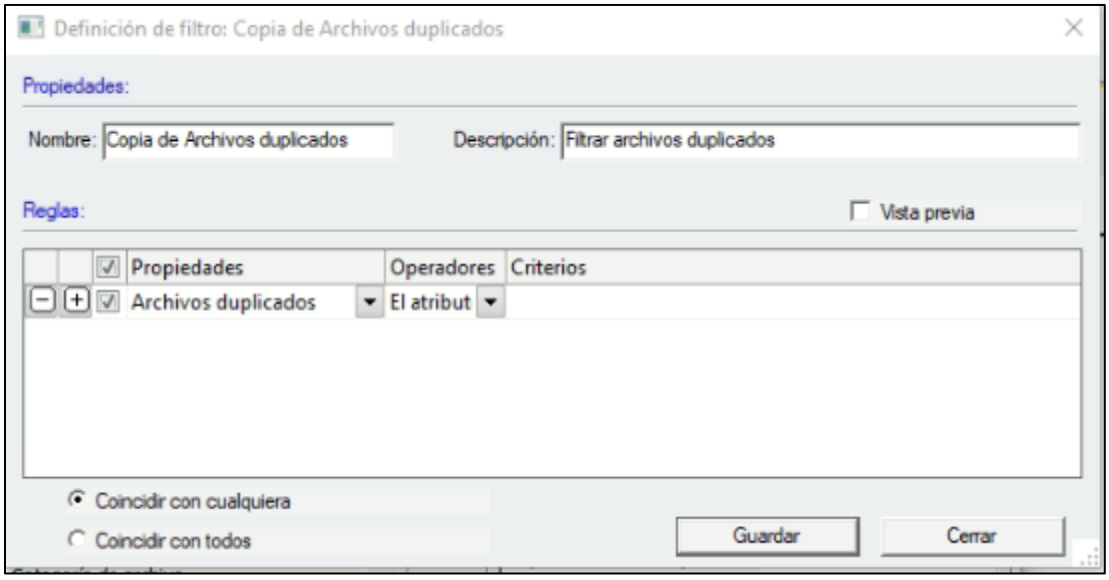


Ilustración 129 Filtro para excluir los archivos duplicados.

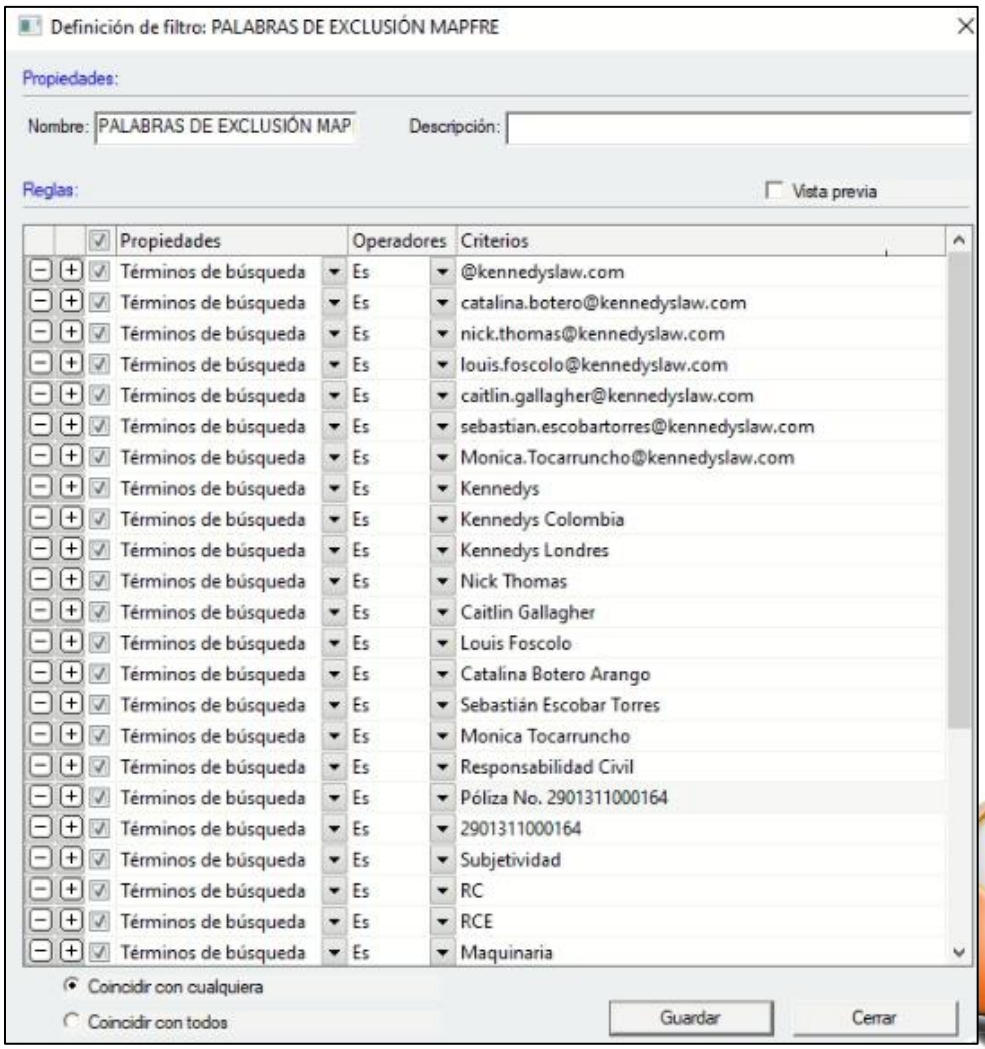


Ilustración 130 Filtro para excluir los archivos suministrado por MAPFRE - 1.

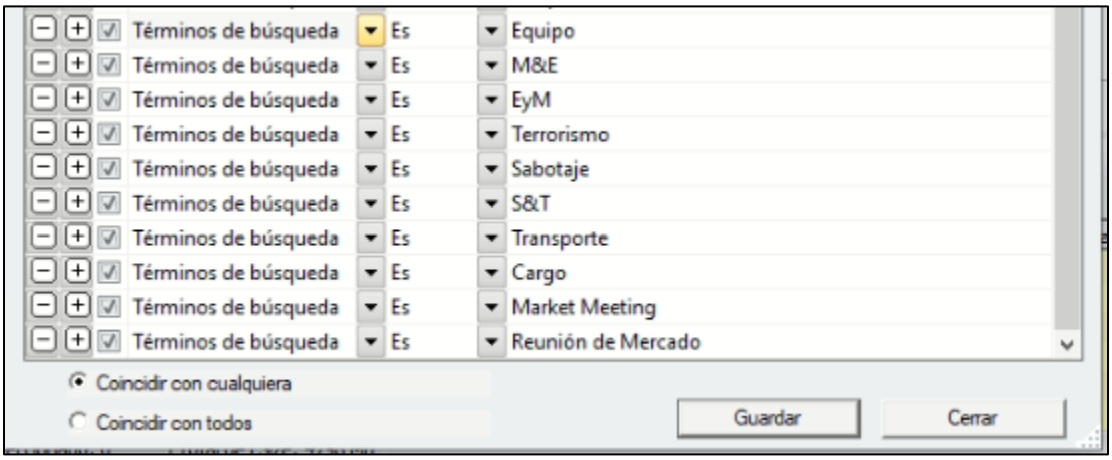
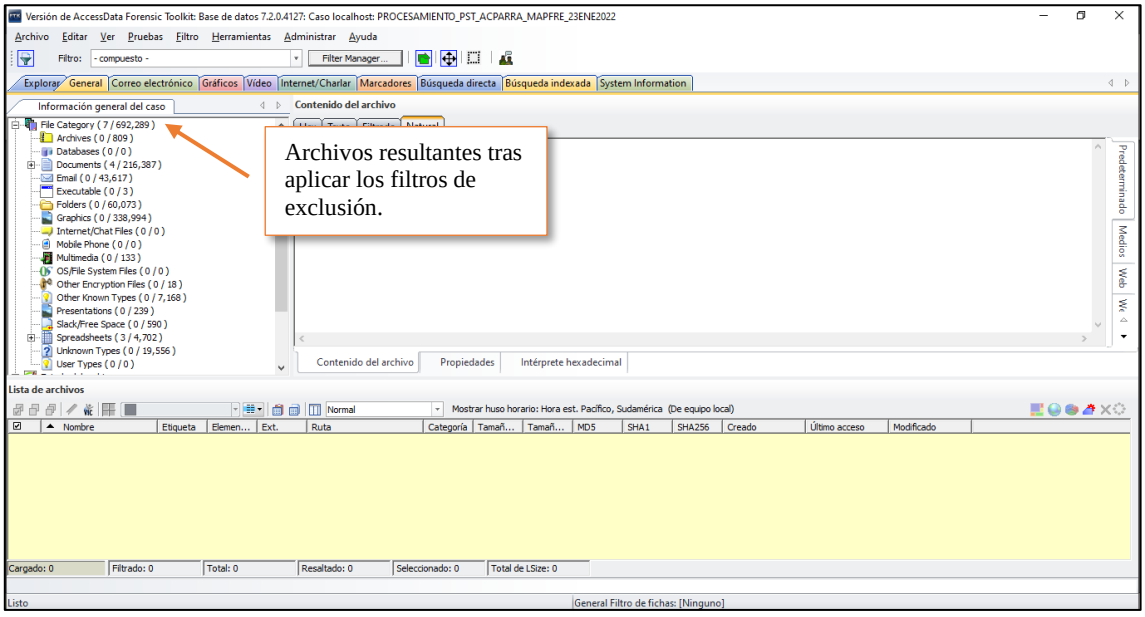


Ilustración 131 Filtro para excluir los archivos suministrado por MAPFRE - 2.

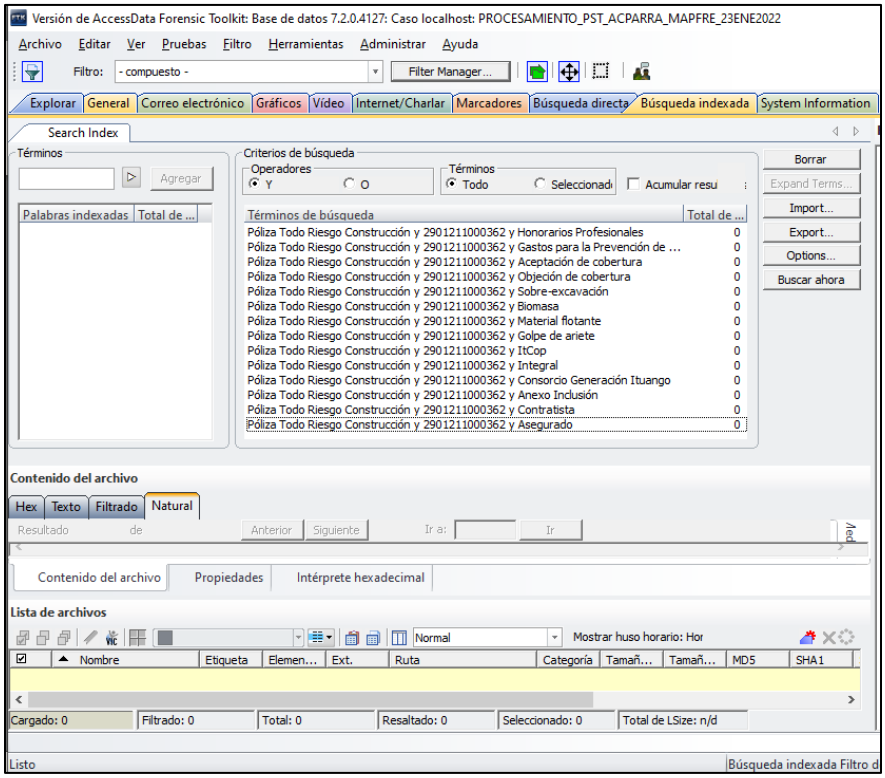
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Siete (7)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo acparra@mapfre.com.co asignado a **Andrés Camilo PARRA BALAGUERO** para el desarrollo de sus funciones.

13. Buzón de correo electrónico cruzj@mapfre.com.co.

El día 01 de diciembre de 2021, el equipo de ADALID CORP ingresa a la carpeta **CRUZJ**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

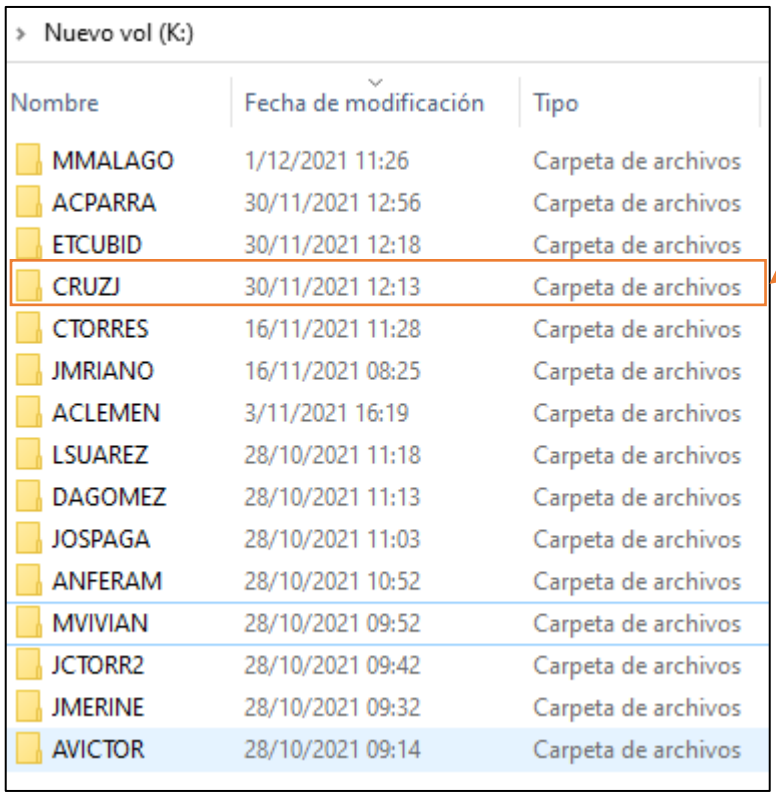


Ilustración 132 Visualización carpeta CRUZJ

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **CRUZJ** identificada dentro del disco duro como se observa en las siguientes imágenes:

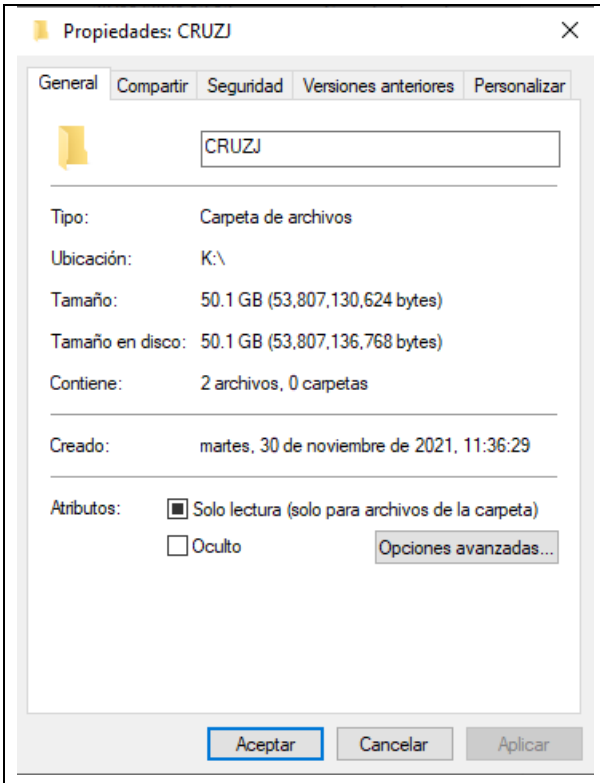


Ilustración 133 Propiedades de la carpeta CRUZJ visto desde el Disco Duro.

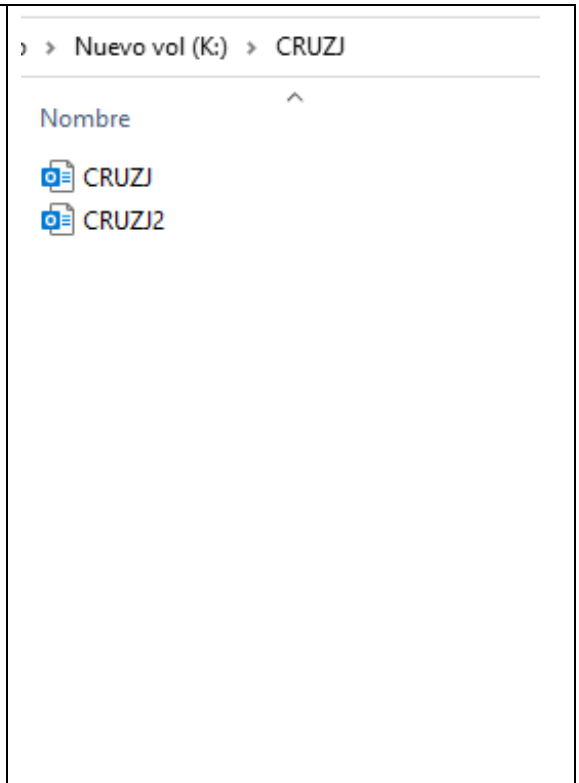


Ilustración 134 Contenido de la carpeta CRUZJ visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**cruzj@mapfre.com.co.**" asignado a **Jorge Cruz AGUADO** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las 15:18:42 y culminando el mismo de forma satisfactoria a las 16:29:17, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_01DIC2021
Número de prueba: 13_CRUZJ
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO CRUZJ@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A

ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad1:
[Computed Hashes]
MD5 checksum: ed3b9410edd6de02fe5e441ea43ddea2
SHA1 checksum: 91fad8664b30c42450ea5e3d4eadc83dd516faa4

Image information:
Acquisition started: Wed Dec 1 15:18:42 2021
Acquisition finished: Wed Dec 1 16:15:53 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad22

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad23

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad24

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad25

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad26

I:\EVIDENCIA_MAPFRE_2\13.CRUZJ\IMAGENFORENSE_PST_CRUZJ_MAPFRE_01DIC2021.ad27

Image Verification Results:
Verification started: Wed Dec 1 16:15:53 2021
Verification finished: Wed Dec 1 16:29:17 2021
MD5 checksum: ed3b9410edd6de02fe5e441ea43ddea2 : verified
SHA1 checksum: 91fad8664b30c42450ea5e3d4eadc83dd516faa4 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**cruzj@mapfre.com.co.**" asignado a **Jorge Cruz AGUADO** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 135 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO CRUZJ@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico cruzj@mapfre.com.co asignada **Jorge Cruz AGUADO** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
13	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Jorge Cruz AGUADO → cruzj@mapfre.com.co	ad1	50.1 GB
TOTAL					**50.1 GB**

Tabla 28 Detalle del buzón de correo electrónico asignado cruzj@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico cruzj@mapfre.com.co asignado a Jorge Cruz AGUADO para el desarrollo de sus funciones **aloja** un total de **50.1 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Noventa y un**

mil seiscientos ochenta y siete (91.687) archivos (incluyendo carpetas), como se observa a continuación.

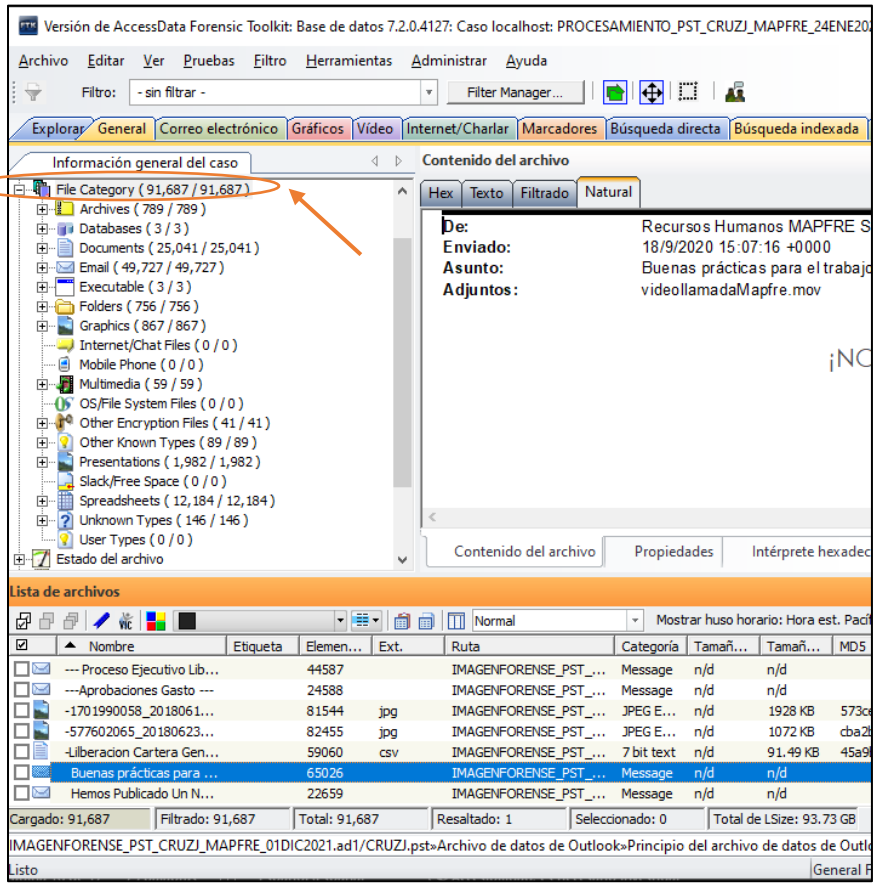


Ilustración 136 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico cruzj@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JORGE CRUZ AGUADO → CRUZJ@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico cruzj@mapfre.com.co asignado a Jorge Cruz AGUADO, iniciando el día el **24** de enero de 2022 con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **Cuarenta (40)** ítems en condición de "eliminados" y se reconstruyeron **Cero (0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como

"Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

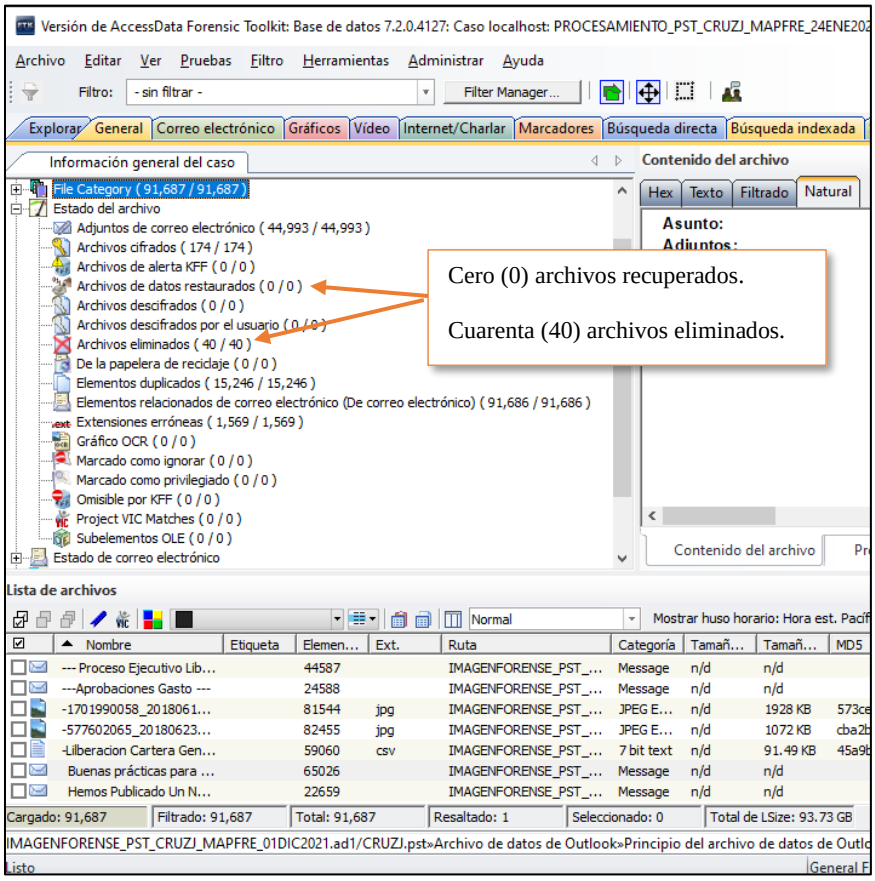


ilustración 137 Total de archivos recuperados en la cuenta de correo electrónico cruzj@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Noventa y un mil seiscientos ochenta y siete (91.687)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO CRUZJ@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico

cruzj@mapfre.com.co asignado a **Jorge Cruz AGUADO** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	789
2	Bases de Datos	3
3	Documentos	25.041
4	Correo Electrónico	49.727
5	Ejecutable	3
6	Carpetas	756
7	Gráficos	867
8	Multimedia	59
9	Otros archivos encriptados	41
10	Otros archivos desconocidos	89
11	Presentaciones	1982
12	Hojas de cálculo	12.184
13	Tipos de archivos desconocidos	146
TOTAL		**91.687**

Tabla 29 Información buscada evidencia 013_CRUZJ, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Noventa y un mil seiscientos ochenta y siete (91.687).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Cuarenta y cuatro mil novecientos noventa y tres (44.993) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Ciento setenta y cuatro (174) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Los archivos de datos restaurados **Cero (0)** archivos de datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos eliminados **Cuarenta (40)** archivos de datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Quince mil doscientos cuarenta y seis (15.246)** archivos de datos recuperados por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Noventa y un mil seiscientos ochenta y seis (91.686)** archivos de datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Mil quinientos sesenta y nueve (1.569) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico mvivian@mapfre.com asignado a cruzj@mapfre.com.co asignado a **Jorge CRUZ** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

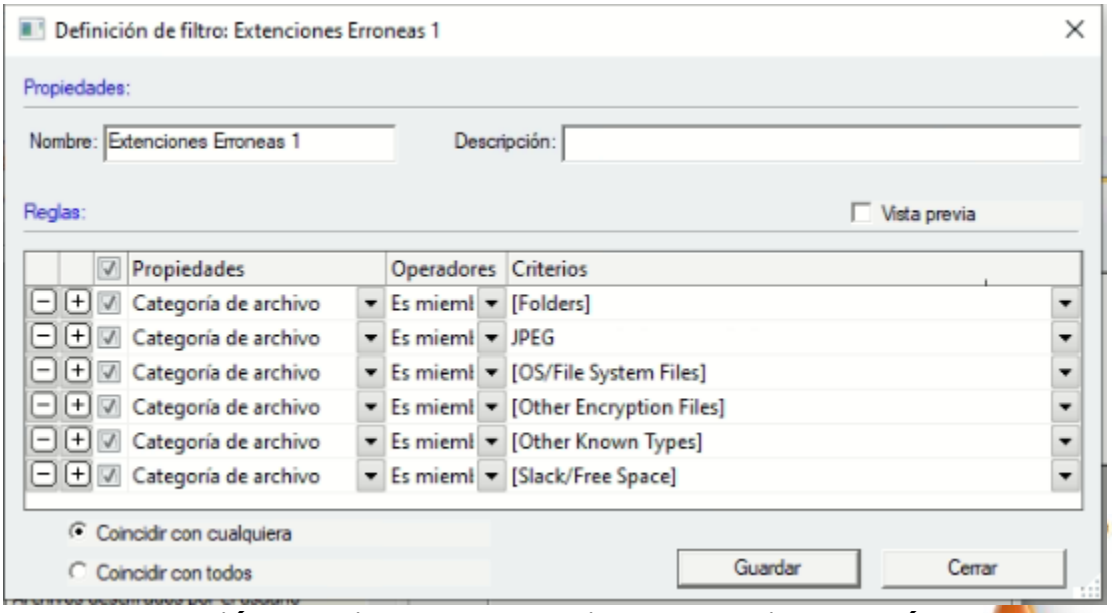


Ilustración 138 Filtro para excluir las extensiones erróneas.

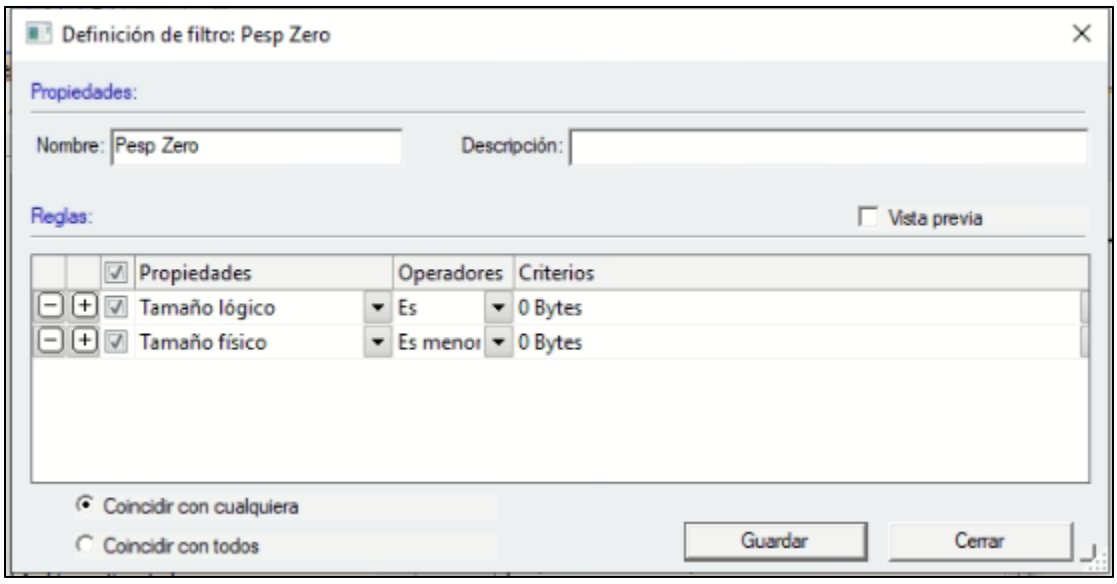


Ilustración 139 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

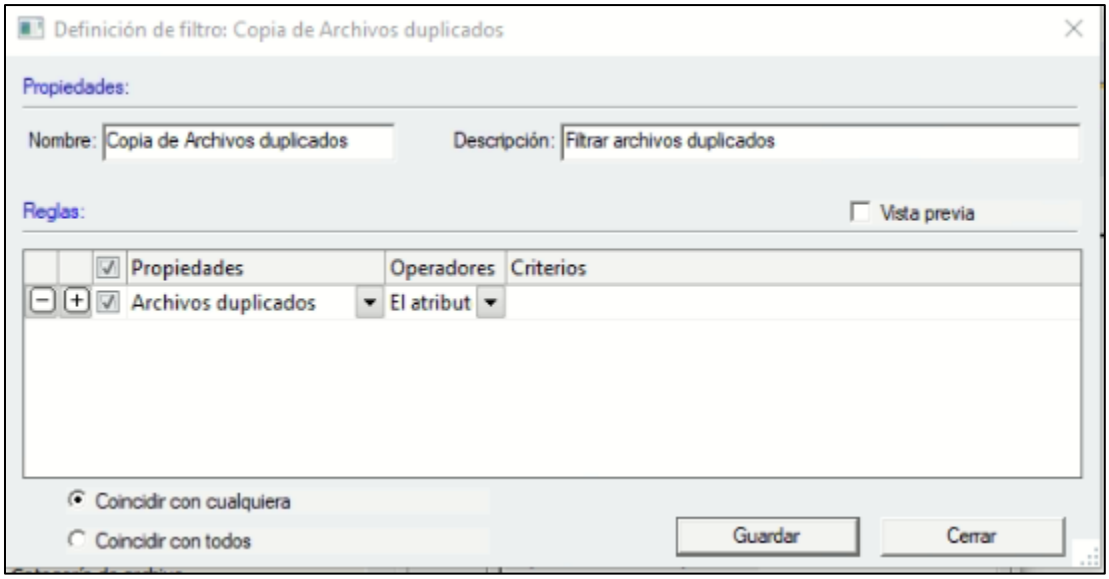


Ilustración 140 Filtro para excluir los archivos duplicados.

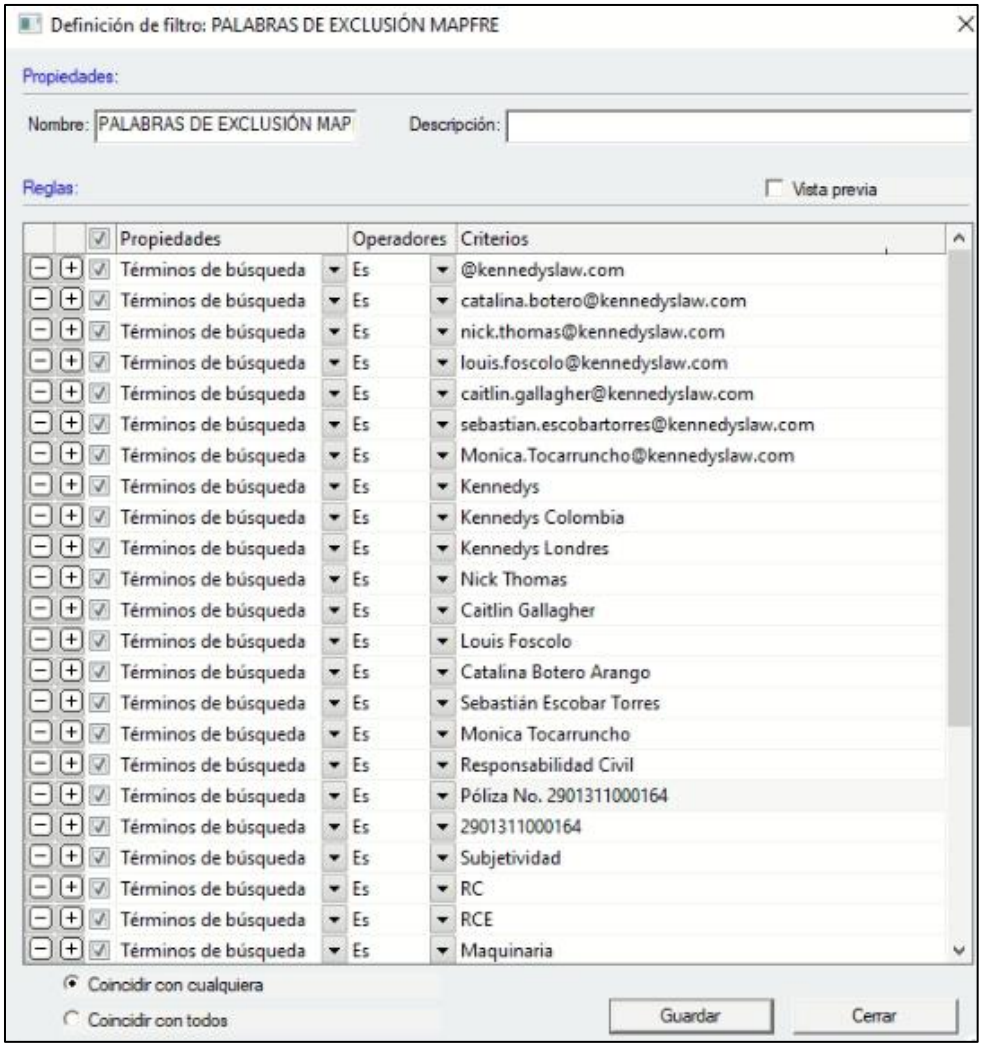


Ilustración 141 Filtro para excluir los archivos suministrado por MAPFRE - 1.

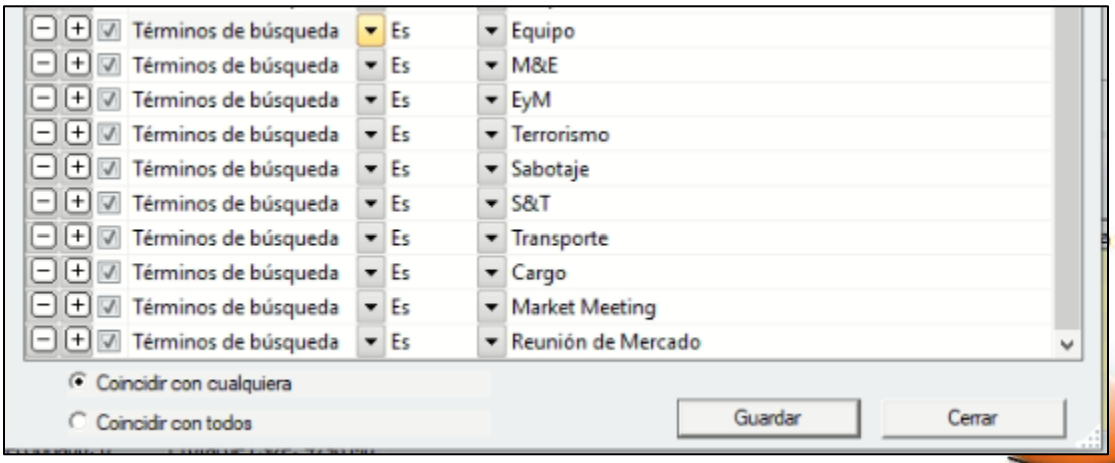
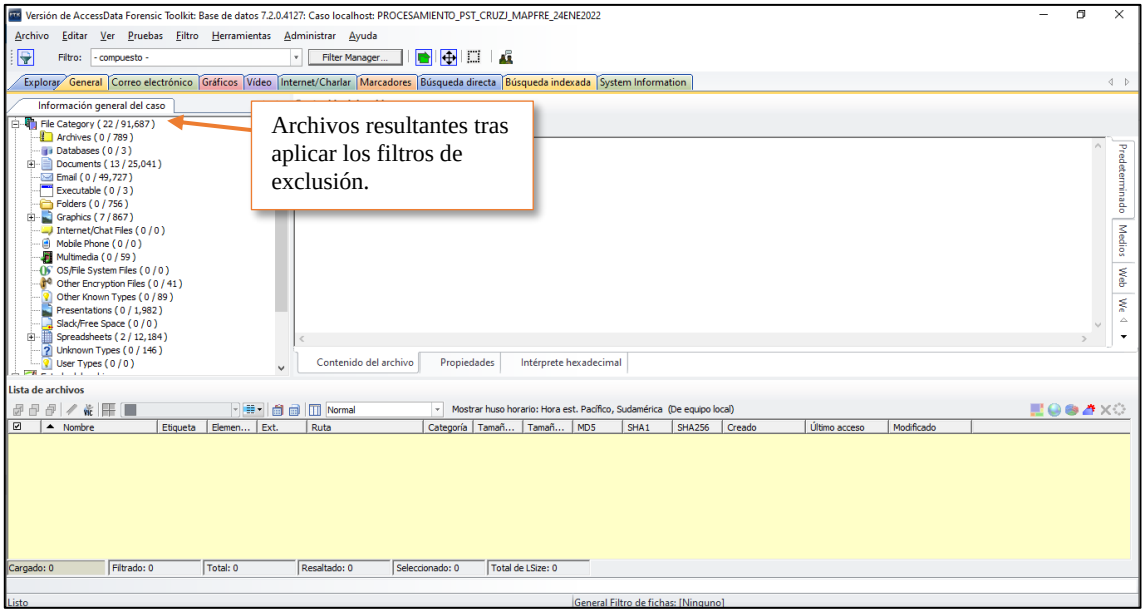


Ilustración 142 Filtro para excluir los archivos suministrado por MAPFRE - 2.

Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **veintidós (22)** registros como se observa en la siguiente imagen:

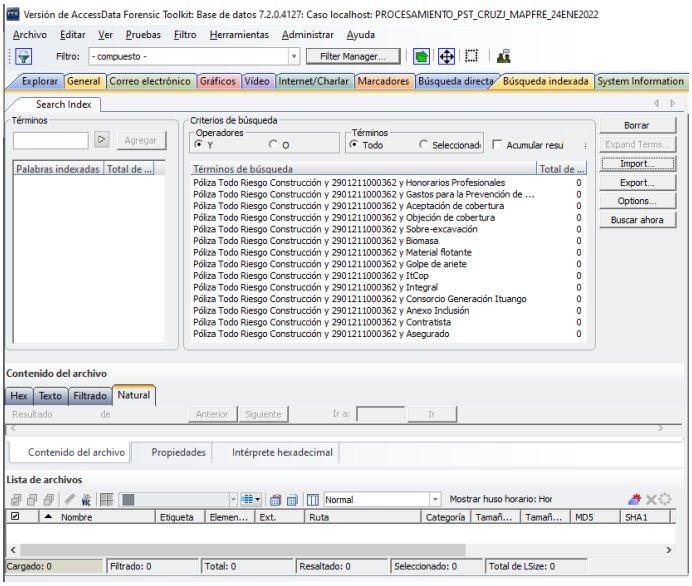


Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo cruzj@mapfre.com.co asignado a **Jorge CRUZ** para el desarrollo de sus funciones.

14. Buzón de correo electrónico etcubid@mapfre.com.co.

El día 01 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta **ETCUBID**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

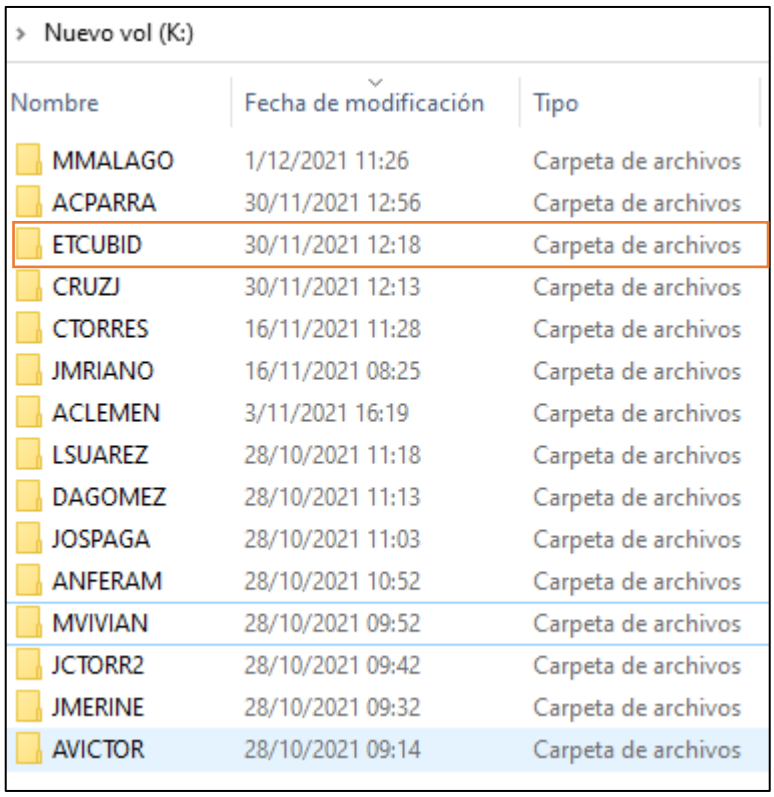


Ilustración 143 Visualización carpeta ETCUBID.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **ETCUBID** identificada dentro del disco duro como se observa en las siguientes imágenes:

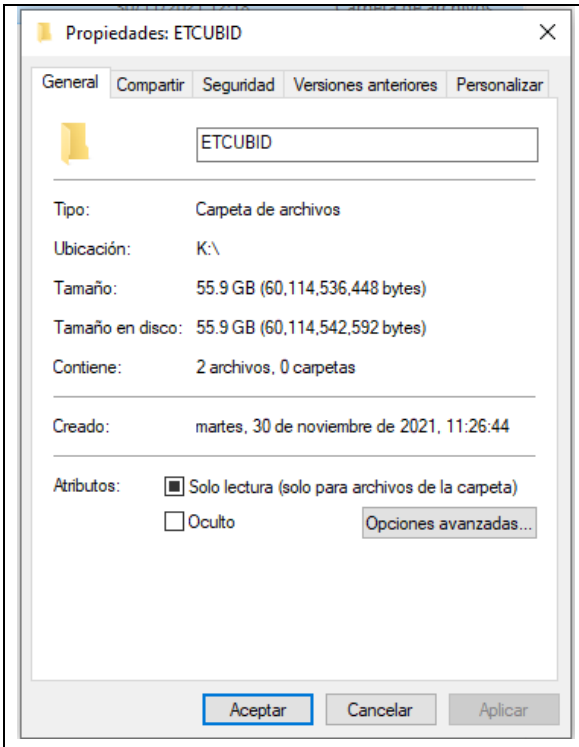


Ilustración 144 Propiedades de la carpeta ETCUBID visto desde el Disco Duro.

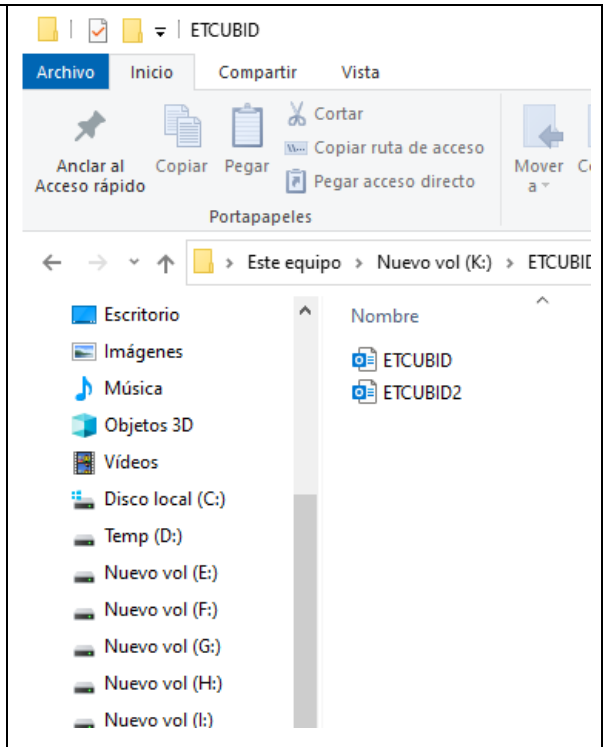


Ilustración 145 Contenido de la carpeta ETCUBID visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**etcubid@mapfre.com.co.**" asignado a **Ethel CUBIDES** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **16:32:53** y culminando el mismo de forma satisfactoria a las **17:53:04**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_01DIC2021
Número de prueba: 14_ETCUBID
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ETCUBID@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8

DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad1:
[Computed Hashes]
MD5 checksum: a6426ce7f6ca0217569271fe149bf3d7
SHA1 checksum: 3753a9577aa74a1f04b65a301238b025bf4fd805

Image information:
Acquisition started: Wed Dec 1 16:32:53 2021
Acquisition finished: Wed Dec 1 17:38:33 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad22

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad23

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad24

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad25

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad26

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad27

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad28

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad29

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad30

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad31

I:\EVIDENCIA_MAPFRE_2\14.ETCUBID\IMAGENFORENSE_PST_ETCUBID_MAPFRE_01DIC2021.ad32

Image Verification Results:
Verification started: Wed Dec 1 17:38:33 2021
Verification finished: Wed Dec 1 17:53:04 2021
MD5 checksum: a6426ce7f6ca0217569271fe149bf3d7 : verified
SHA1 checksum: 3753a9577aa74a1f04b65a301238b025bf4fd805 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con

capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**etcubid@mapfre.com.co.**" asignado a **Ethel CUBIDES** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 146 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ETCUBID@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico etcubid@mapfre.com.co asignada Ethel CUBIDES para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
14	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Ethel CUBIDES → etcubid@mapfre.com.co	ad1	55.9 GB
TOTAL					**55.9GB**

Tabla 30 Detalle del buzón de correo electrónico asignado etcubid@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico etcubid@mapfre.com.co asignado a Ethel CUBIDES para el desarrollo de sus funciones **aloja** un total de **55.9 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento veintitrés**

mil trescientos veinticuatro (123.324) archivos (incluyendo carpetas), como se observa a continuación.

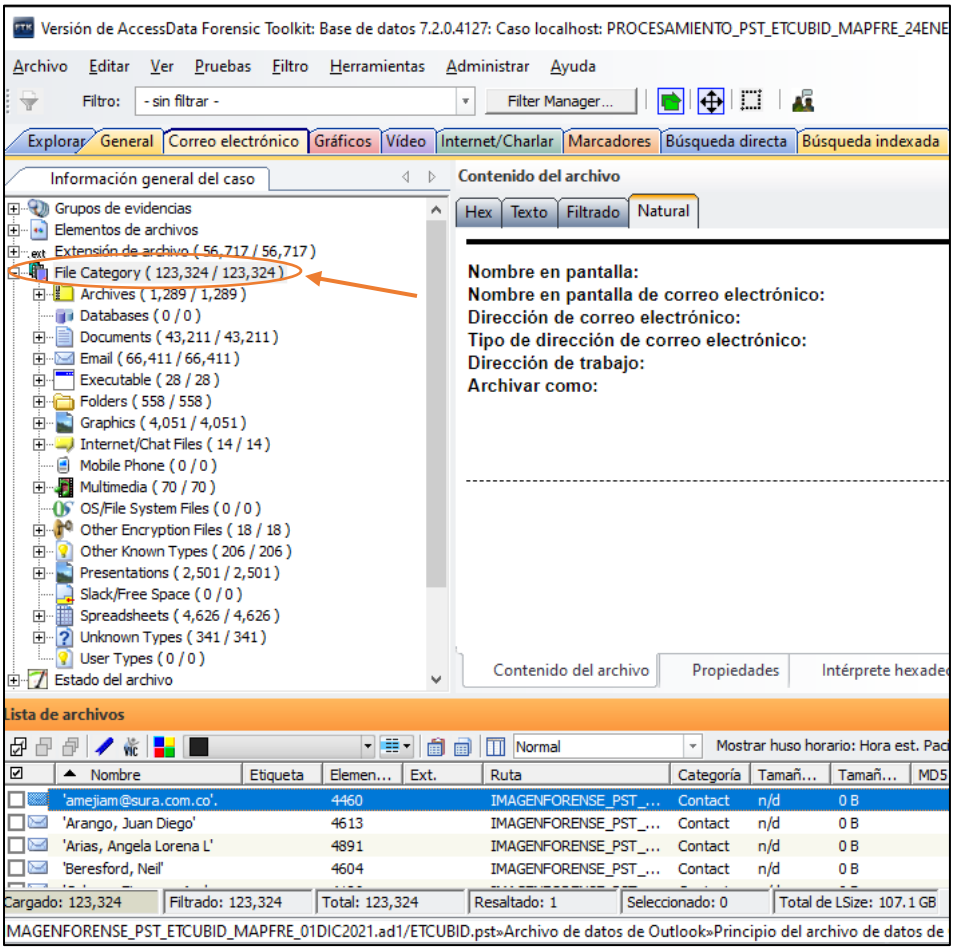


Ilustración 147 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico etcubid@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO ETHEL CUBIDES → ETCUBID@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico etcubid@mapfre.com.co asignado a Ethel CUBIDES, iniciando el día el **24** de enero del 2022, con una duración aproximada de Siete (7) día calendario, el resultado a dicho proceso arrojó que existen **Mil setenta y ocho (1.078**) ítems en condición de "eliminados" y se reconstruyeron **Cero (0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato

que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

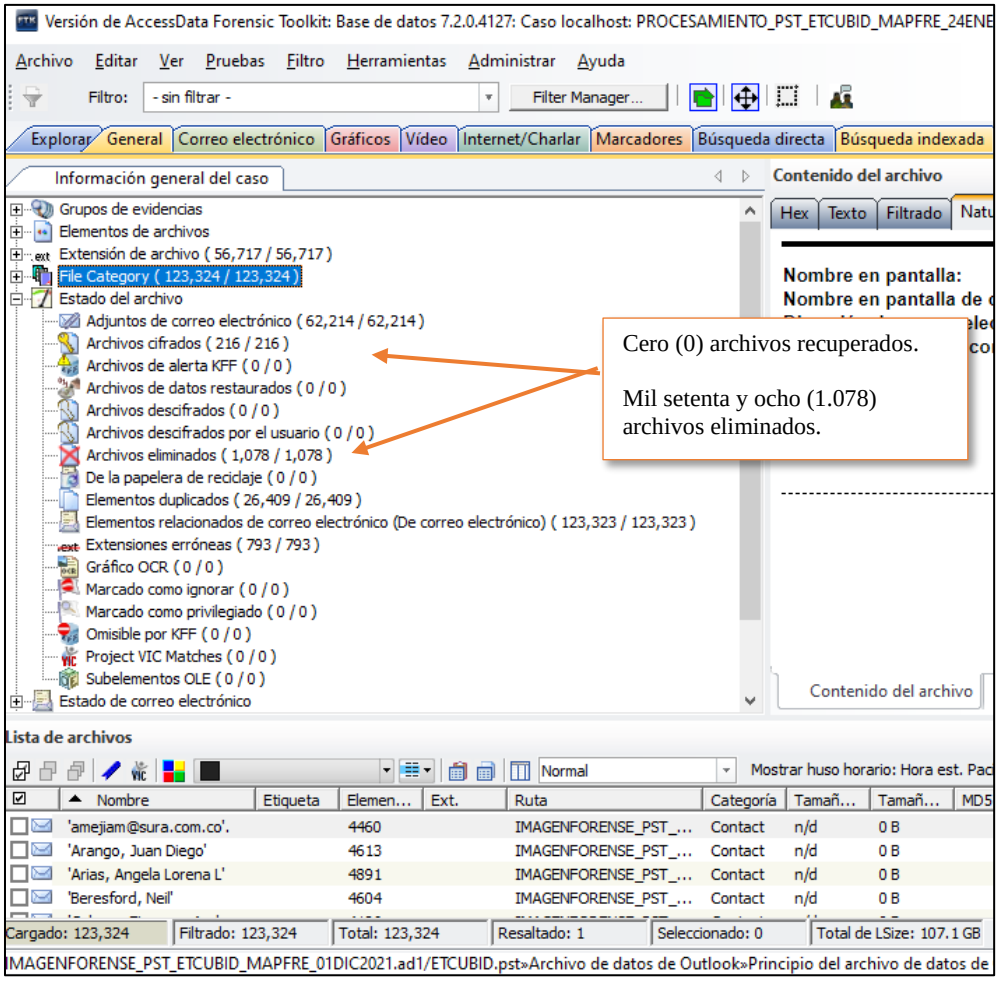


ilustración 148 Total de archivos recuperados en la cuenta de correo electrónico etcubid@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento veintitrés mil trescientos veinticuatro (123.324)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ETCUBID@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico etcubid@mapfre.com.co asignado a **Ethel CUBIDES** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1289
2	Documentos	43.211
3	Correo Electrónico	66.411
4	Ejecutable	28
5	Carpetas	558
6	Archivos de internet / chats	14
7	Gráficos	4.051
8	Multimedia	70
9	Otros archivos encriptados	18
10	Otros archivos desconocidos	206
11	Presentaciones	2501
12	Hojas de cálculo	4.626
13	Tipos de archivos desconocidos	341
TOTAL		**123.324**

Tabla 31 Información buscada evidencia 014_ETCUBID, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento veintitrés mil trescientos veinticuatro (123.324).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Sesenta y dos mil doscientos catorce (62.214) archivos de datos obtenidos** por el

proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Los archivos cifrados recuperados **Doscientos dieciséis (216) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos eliminados **Mil setenta y ocho (1.078) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Veintiséis mil cuatrocientos nueve (26.409) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento veintitrés mil trescientos veintitrés (123.323) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Setecientos noventa (793) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico etcubid@mapfre.com.co asignado a **Ethel CUBIDES para** el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

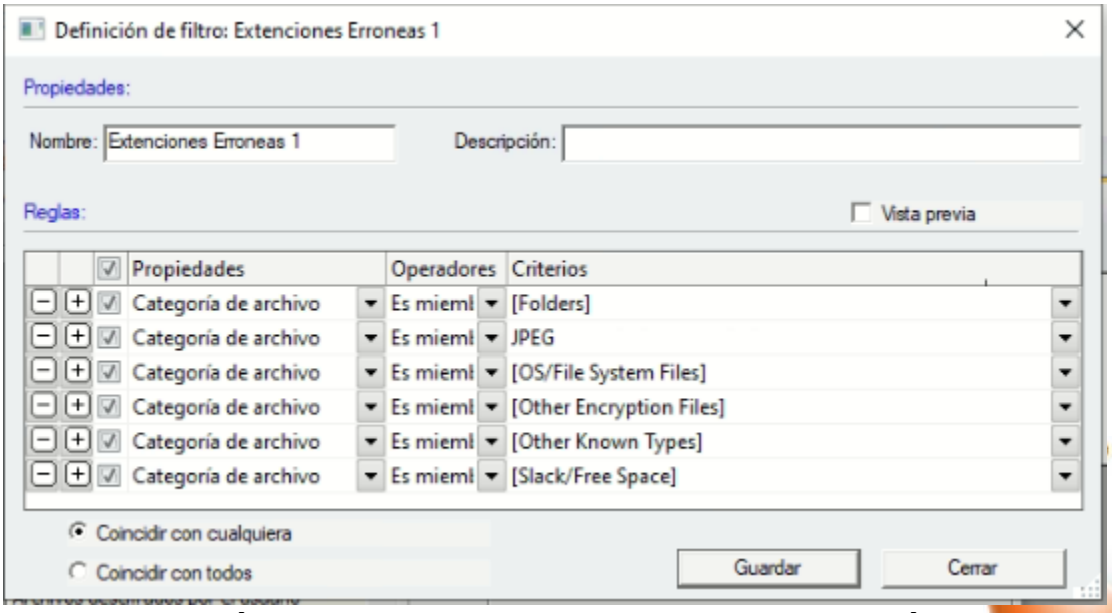


Ilustración 149 Filtro para excluir las extensiones erróneas.

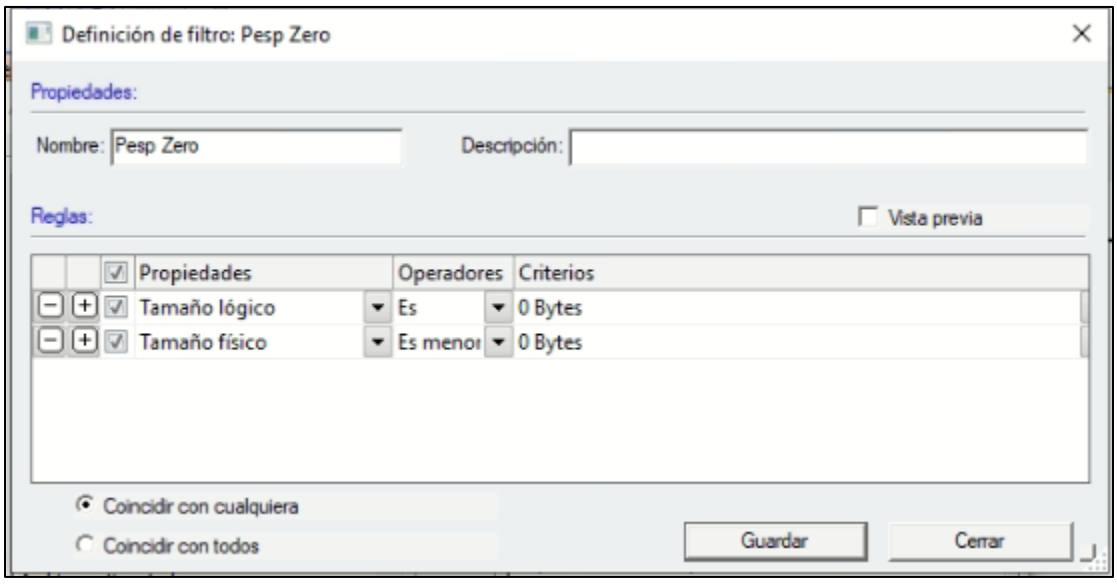


Ilustración 150 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

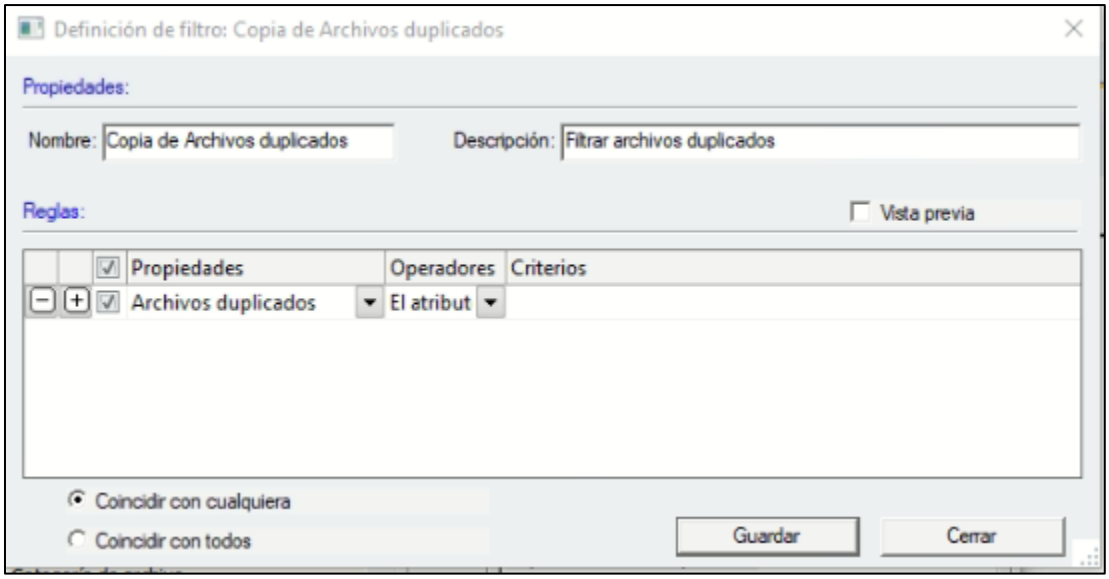


Ilustración 151 Filtro para excluir los archivos duplicados.

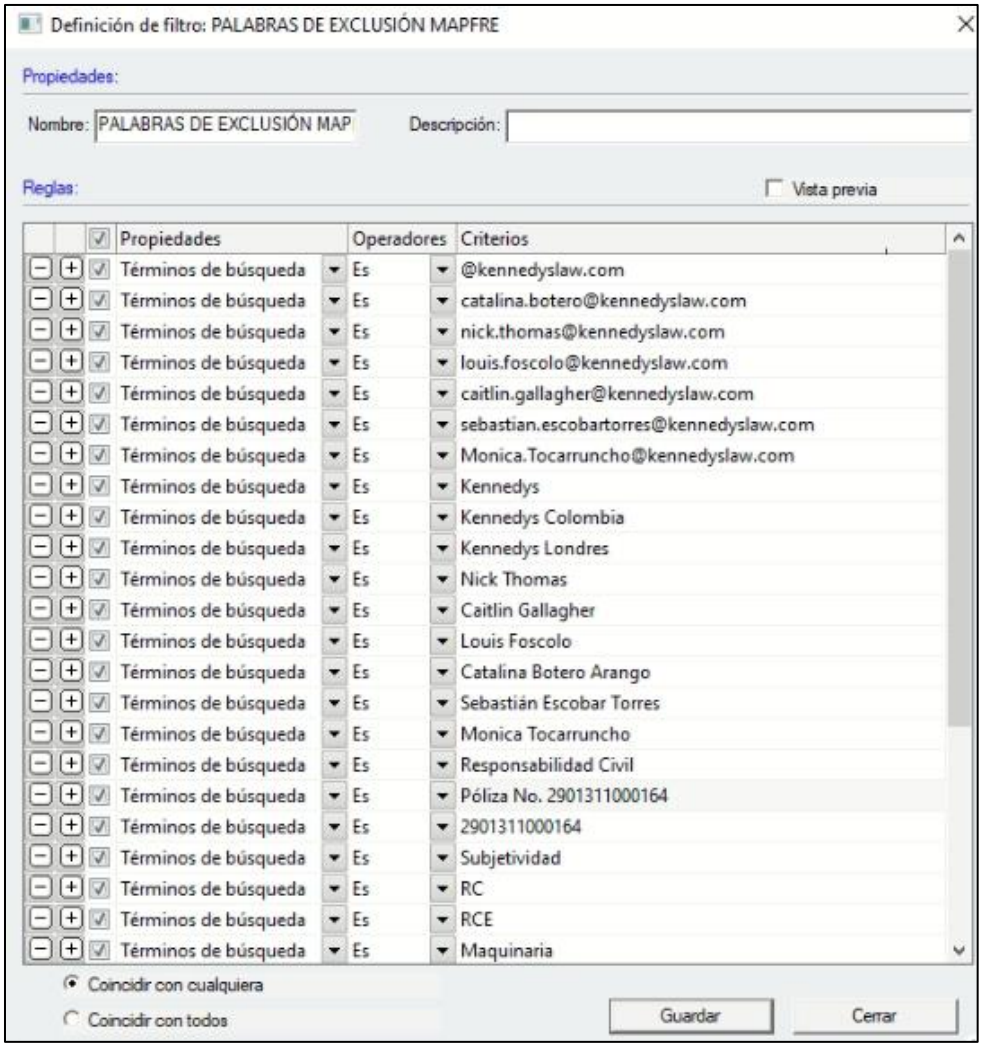


Ilustración 152 Filtro para excluir los archivos suministrado por MAPFRE - 1.

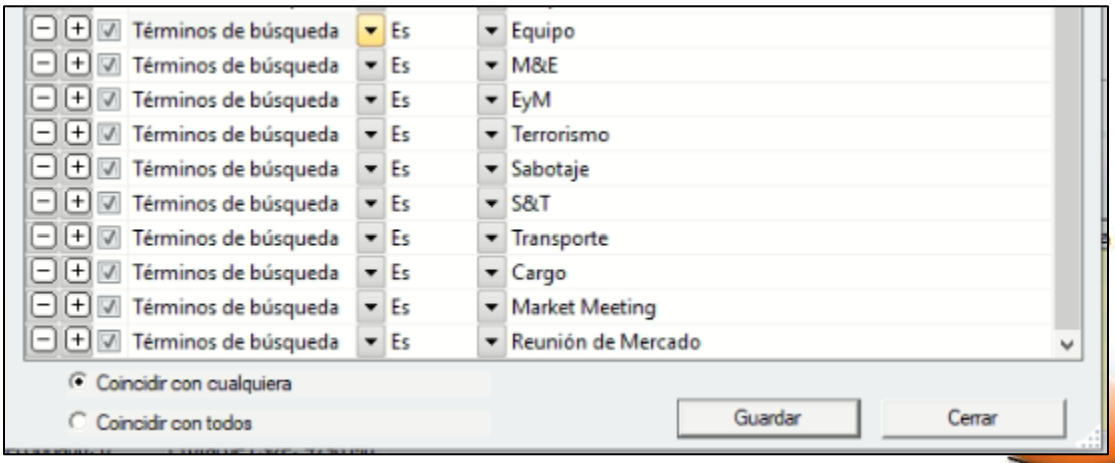
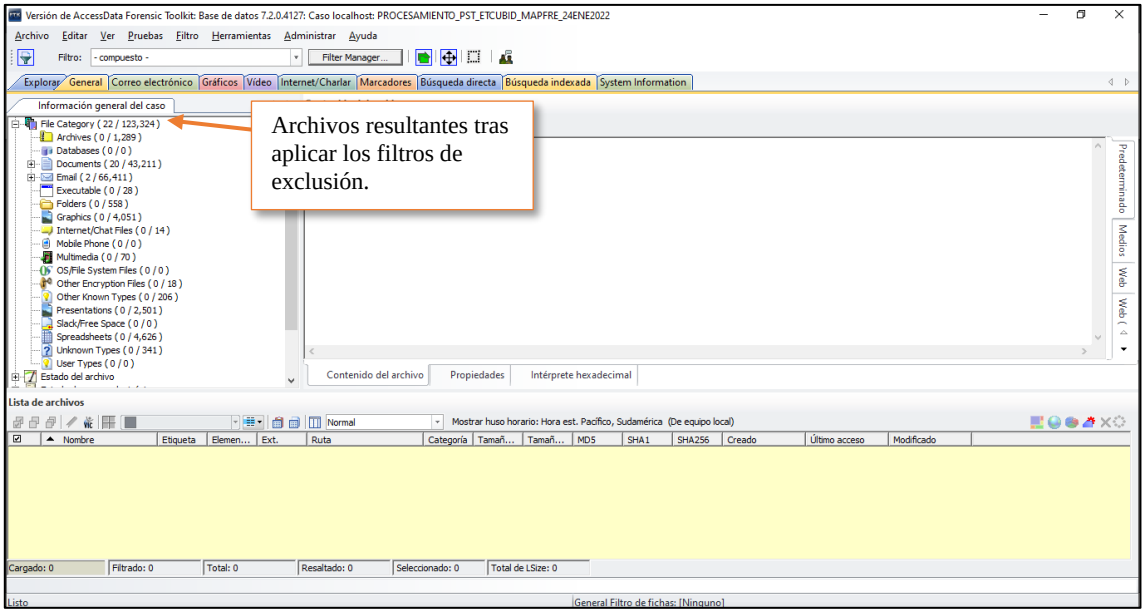


Ilustración 153 Filtro para excluir los archivos suministrado por MAPFRE - 2.

Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **veintidós (22)** registros como se observa en la siguiente imagen:

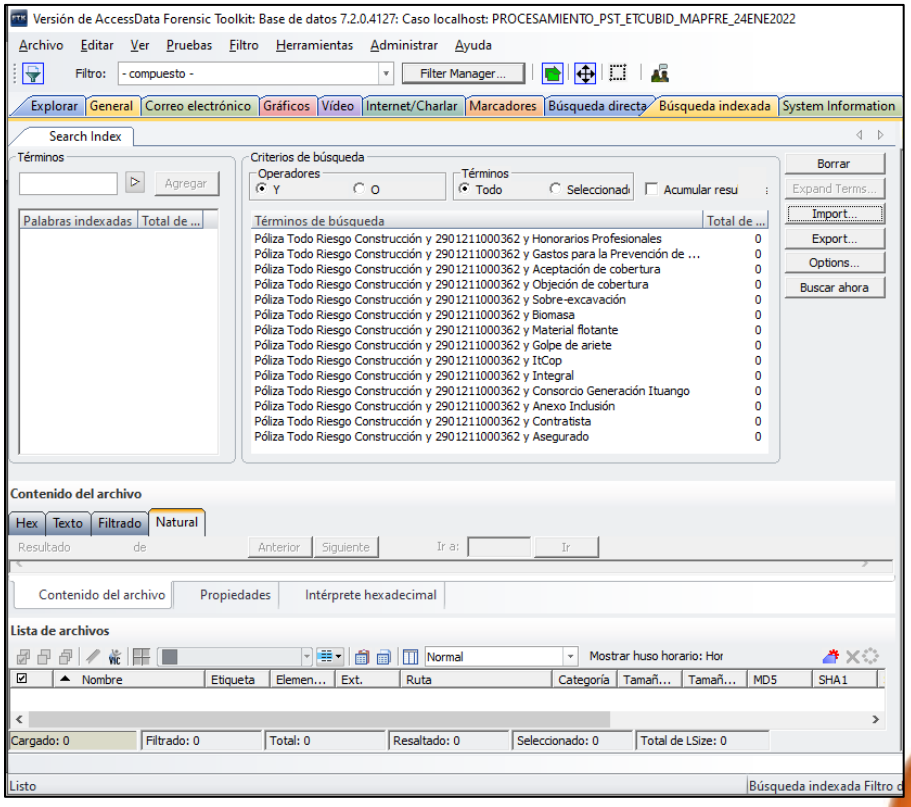


Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identificó resultados asociados para el buzón de correo etcubid@mapfre.com.co asignado a **Ethel CUBIDES** para el desarrollo de sus funciones.

15. Buzón de correo electrónico mmalago@mapfre.com.co.

El día 02 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta **MMALAGO**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

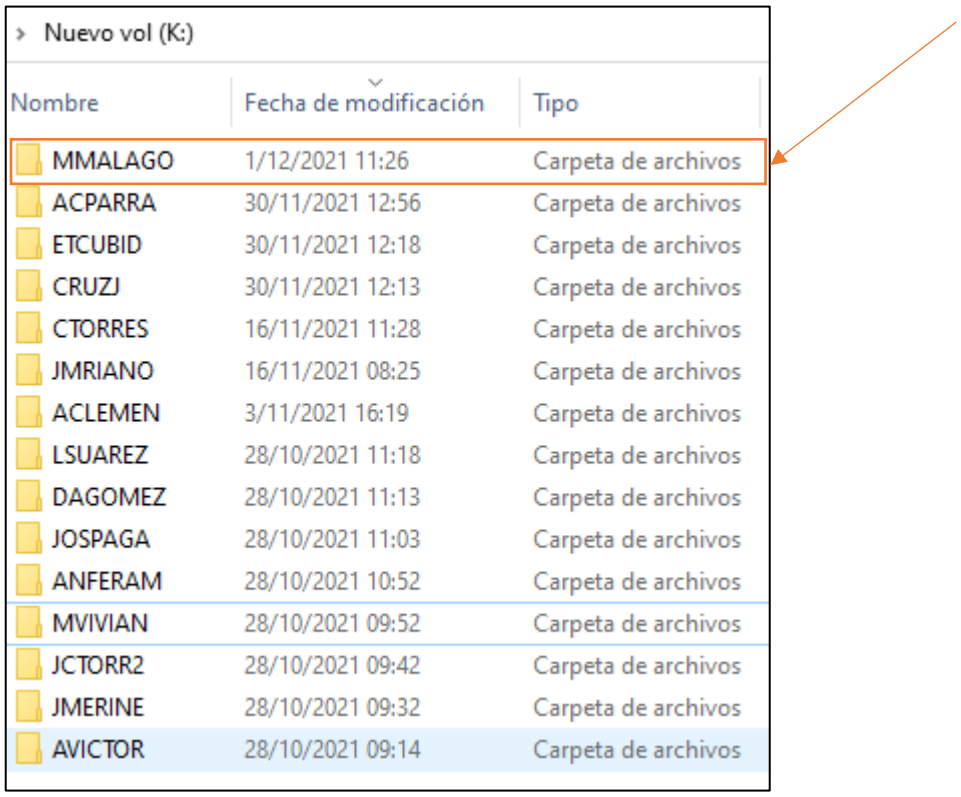


Ilustración 154 Visualización carpeta MMALAGO.

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **MMALAGO** identificada dentro del disco duro como se observa en las siguientes imágenes:

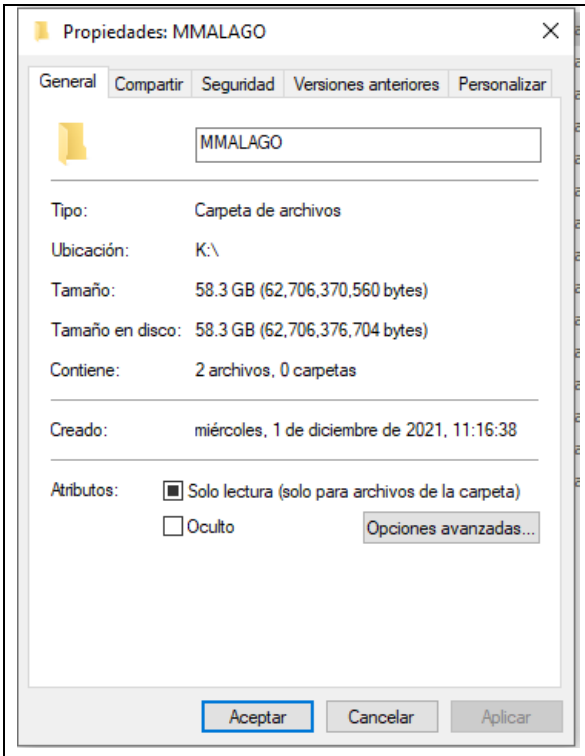


Ilustración 155 Propiedades de la carpeta MMALAGO visto desde el Disco Duro.

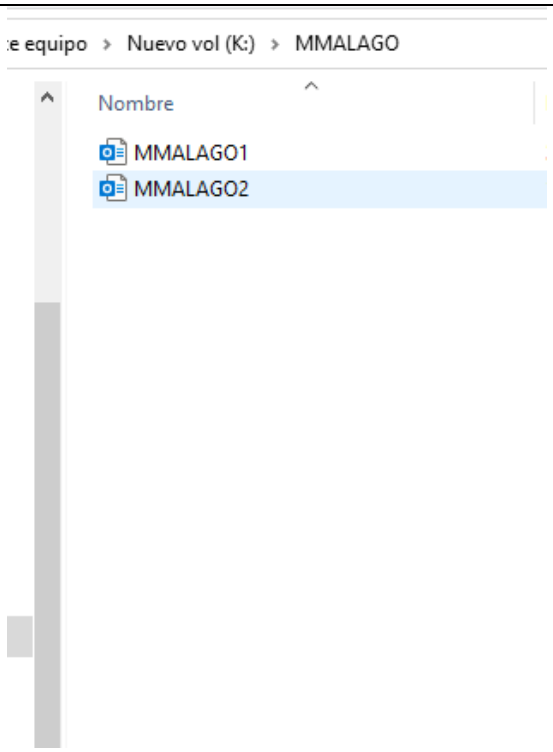


Ilustración 156 Contenido de la carpeta MMALAGO visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**mmalago@mapfre.com.co.**" asignado a **José Mauricio MALAGÓN ACOSTA** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **07:46:38** y culminando el mismo de forma satisfactoria a las **09:01:58**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_02DIC2021
Número de prueba: 15_MMALAGO
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO MMALAGO@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE

FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad1:
[Computed Hashes]
MD5 checksum: 73f2e7b307c8cbe24e68fd2cd5bec944
SHA1 checksum: 515cd0f6c475cc973c9af008a7ea79b87126ef69

Image information:
Acquisition started: Thu Dec 2 07:46:38 2021
Acquisition finished: Thu Dec 2 08:47:29 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad22

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad23

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad24

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad25

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad26

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad27

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad28

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad29

I:\EVIDENCIA_MAPFRE_2\15.MMALAGO\IMAGENFORENSE_PST_MMALAGO_MAPFRE_02DIC2021.ad30

Image Verification Results:
Verification started: Thu Dec 2 08:47:29 2021
Verification finished: Thu Dec 2 09:01:58 2021
MD5 checksum: 73f2e7b307c8cbe24e68fd2cd5bec944 : verified
SHA1 checksum: 515cd0f6c475cc973c9af008a7ea79b87126ef69 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**mmalago@mapfre.com.co.**" asignado a **José Mauricio MALAGÓN ACOSTA** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 157 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO MMALAGO@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico mmalago@mapfre.com.co asignada **José Mauricio MALAGÓN ACOSTA** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
15	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	José Mauricio MALAGÓN ACOSTA → mmalago@mapfre.com.co	ad1	58.3 GB
TOTAL					**58.3 GB**

Tabla 32 Detalle del buzón de correo electrónico asignado mmalago@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico mmalago@mapfre.com.co asignado a **José Mauricio MALAGÓN ACOSTA** para el desarrollo de sus funciones **aloja** un total de **58.3 GB**, dentro de este espacio el laboratorio de informática forense logró hallar

un total de **Ciento cuarenta y siete mil doscientos dieciocho (147.218)** archivos (incluyendo carpetas), como se observa a continuación.

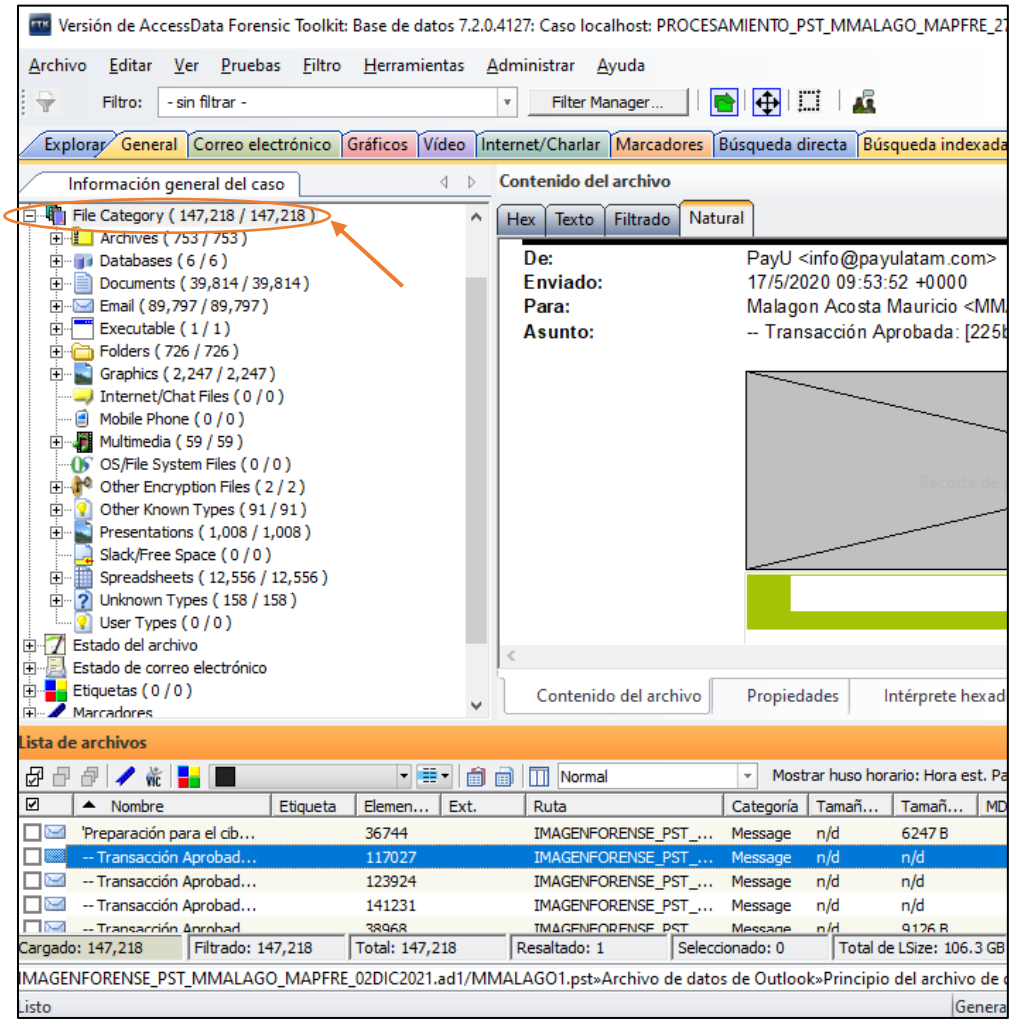


Ilustración 158 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico mmalago@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO JOSÉ MAURICIO MALAGÓN ACOSTA → MMALAGO@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico mmalago@mapfre.com.co asignado a **José Mauricio MALAGÓN ACOSTA**, iniciando el día el **27** de enero del 2022, con una duración aproximada de Ocho (8) día calendario, el resultado a dicho proceso arrojó que existen **Doscientas ochenta y siete (287)** ítems en condición de "eliminados" y se reconstruyeron **cero (0)**

archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

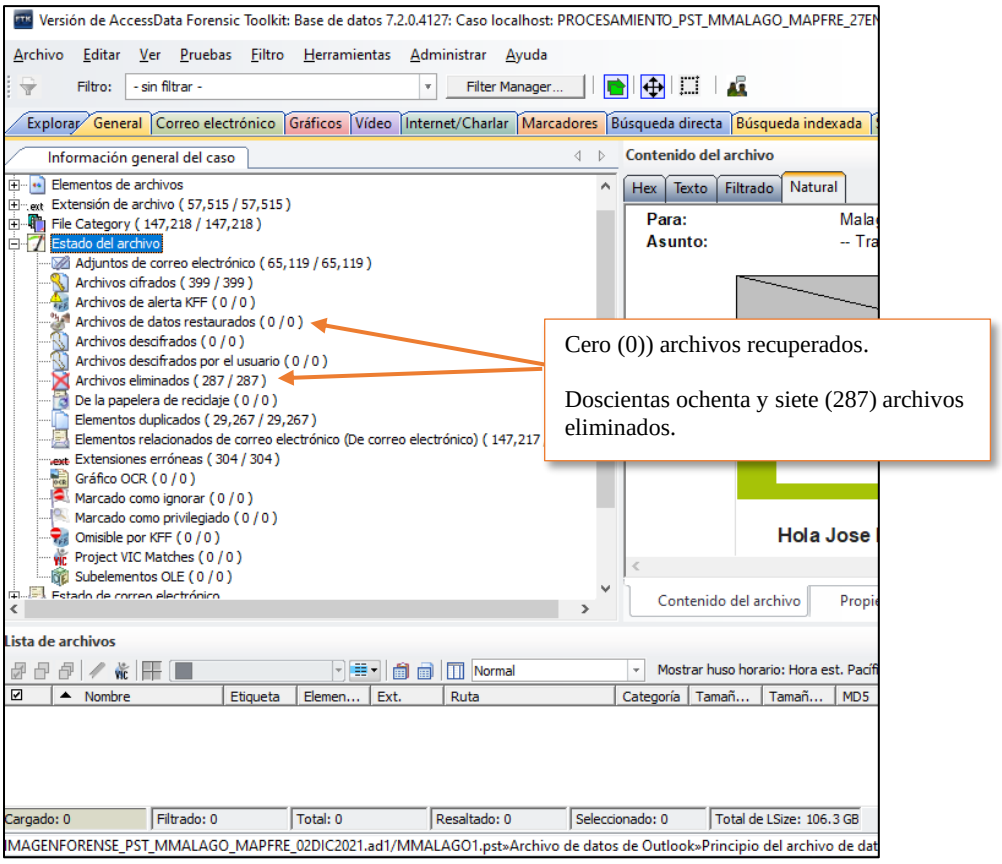


ilustración 159 Total de archivos recuperados en la cuenta de correo electrónico mmalago@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento cuarenta y siete mil doscientos dieciocho (147.218)** (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO MMALAGO@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico mmalago@mapfre.com.co asignado a **José Mauricio MALAGÓN ACOSTA** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	753
2	Bases de Datos	6
3	Documentos	39.814
4	Correo Electrónico	89.797
5	Ejecutables	1
6	Carpetas	726
7	Gráficos	2.247
8	Multimedia	59
9	Otros archivos encriptados	2
10	Otros archivos desconocidos	91
11	Presentaciones	1008
12	Hojas de cálculo	12.556
13	Tipos de archivos desconocidos	158
TOTAL		**147.218**

Tabla 33 Información buscada evidencia 015_MMALAGO, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento cuarenta y siete mil doscientos dieciocho (147.218).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Sesenta y cinco mil ciento diecinueve (65.119) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Trescientas noventa y nueve (399) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos eliminados **Veintisiete mil ochocientos once (287) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Ochenta y ocho mil ciento dieciséis (88.116) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento noventa y seis mil ciento ochenta y seis (196.186) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **novecientos cincuenta y siete (957) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo grafico OCR (Reconocimiento óptico de caracteres) **Treinta y un mil catorce (31.014) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo subelemento **Veintisiete mil ciento veintiocho (27.128) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico mmalago@mapfre.com.co asignado a **José Mauricio MALAGÓN ACOSTA** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



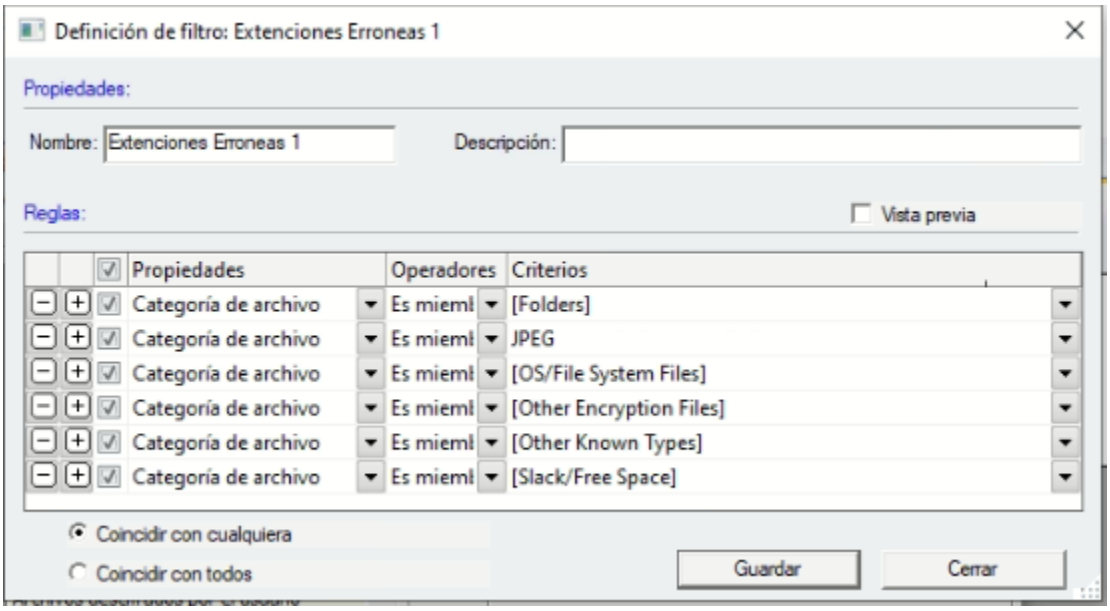


Ilustración 160 Filtro para excluir las extensiones erróneas.

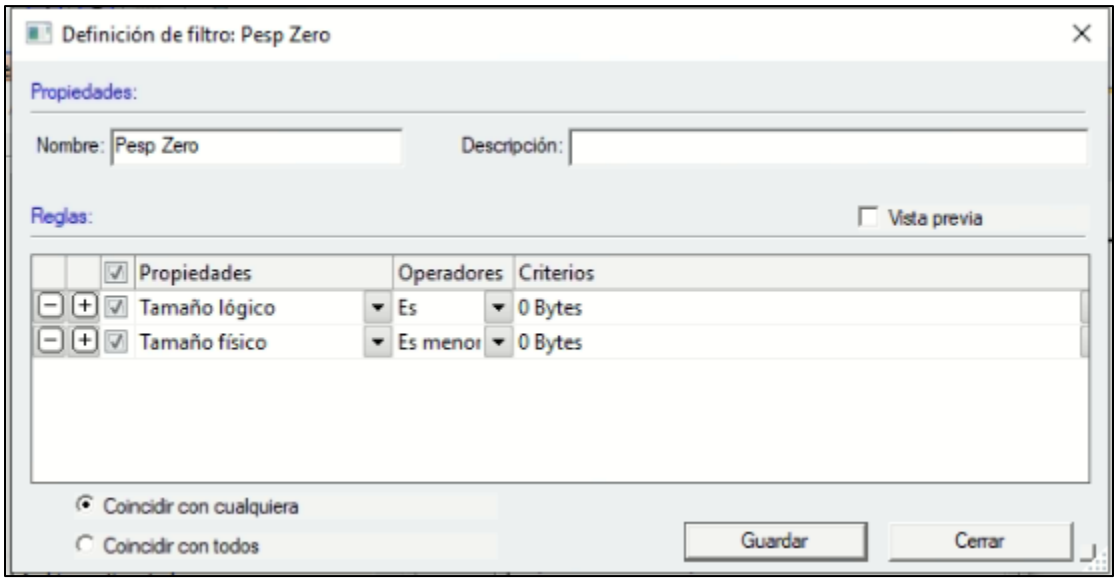


Ilustración 161 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

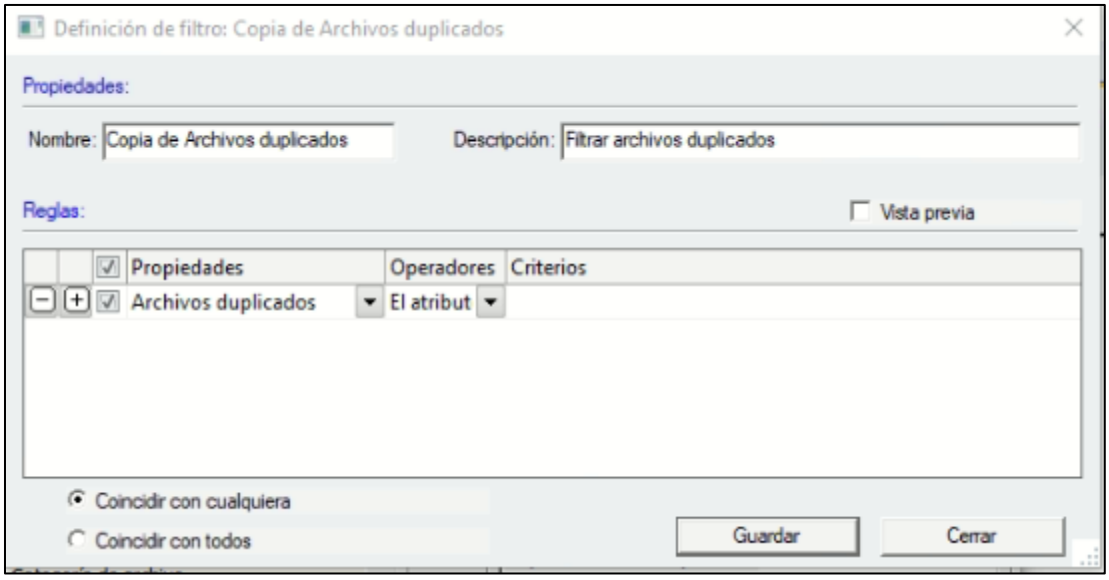


Ilustración 162 Filtro para excluir los archivos duplicados.

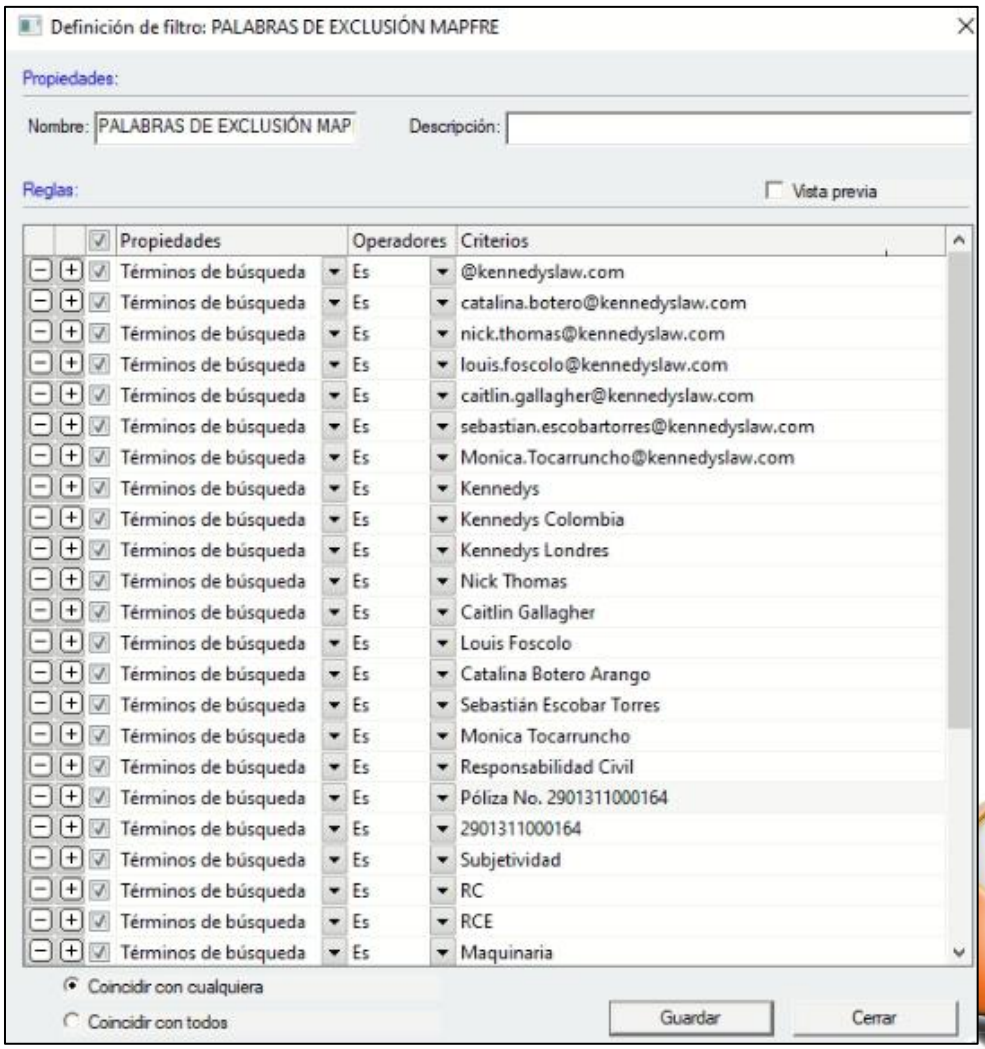


Ilustración 163 Filtro para excluir los archivos suministrado por MAPFRE - 1.

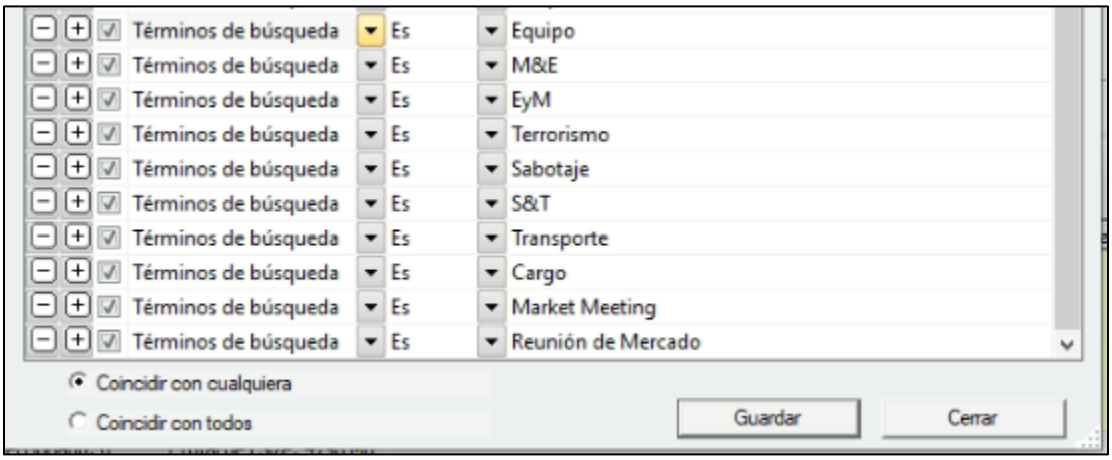
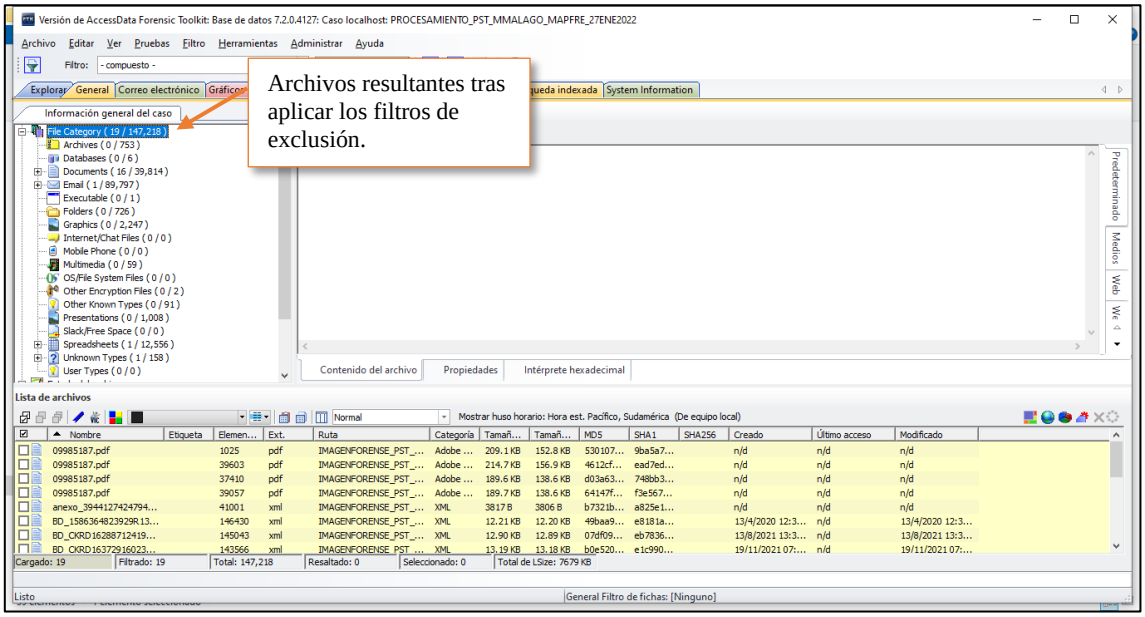


Ilustración 164 Filtro para excluir los archivos suministrado por MAPFRE - 2.

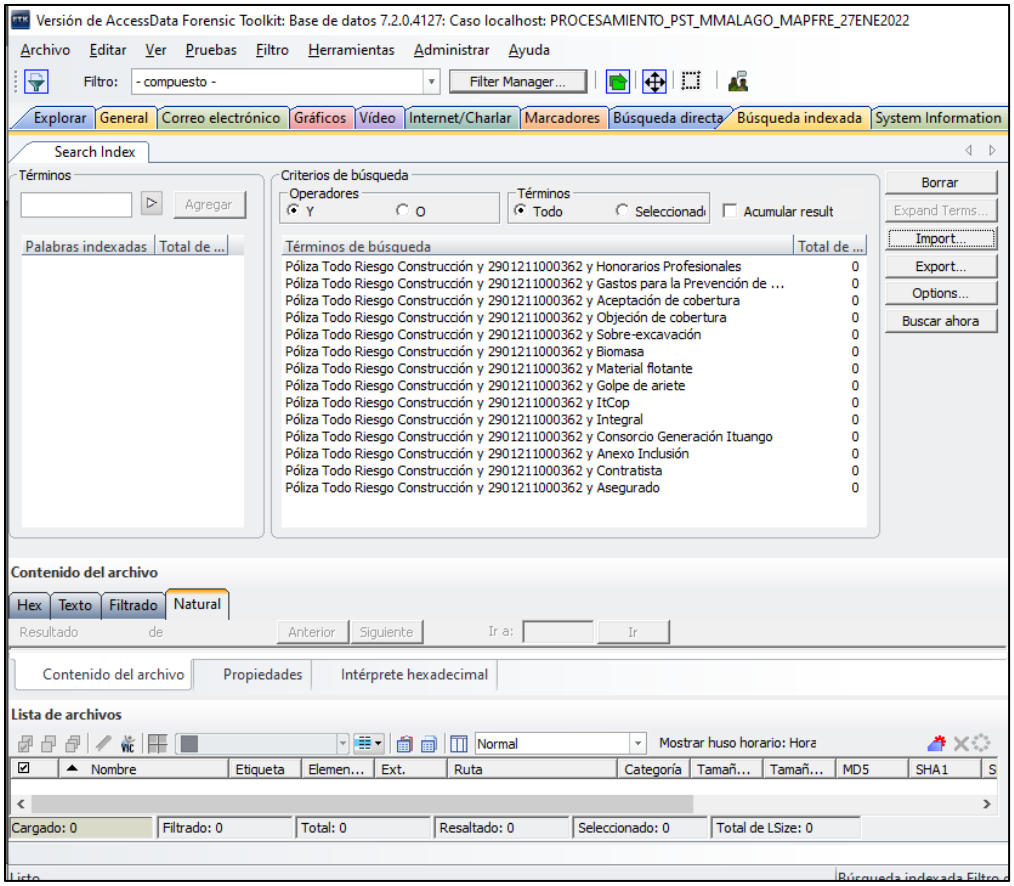
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Diecinueve (19)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo mmalago@mapfre.com.co asignado a **José Mauricio MALAGÓN ACOSTA** para el desarrollo de sus funciones.

Una vez realizadas las imágenes forenses para los buzones de correo electrónico pertenecientes a (4) funcionarios de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** los cuales se encuentran identificados con las siguientes direcciones de correo (mmalago@mapfre.com.co, acparra@mapfre.com.co, etcubid@mapfre.com.co, cruzj@mapfre.com.co), el equipo de ADALID CORP hace entrega de (1) Un disco duro color blanco, con capacidad de almacenamiento de **1000GB** al señor **Willigton Leandro TORRES MORALES,** identificado con cédula de ciudadanía **No. 79.708.420** de Bogotá, quien funge como **PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN** el día 07 de diciembre a las 15:03 horas.

De igual manera, el día 07 diciembre de 2021, el señor **Willigton Leandro TORRES MORALES** nuevamente hace entrega a los peritos de ADALID CORP. de (1) Un disco duro color **blanco**, con capacidad de almacenamiento de

1000GB, el cual en su parte superior se encuentra marcado como **"prueba extraprocesal"** como se presenta a continuación**:**

	
Fotografía Disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista superior)	Fotografía disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista posterior)

Al interior del Disco Duro se encuentran los archivos en formato .PST de las cuentas de correo electrónico asignadas a Once (11) funcionarios que se encuentran retirados y Seis (6) cuentas de correo electrónico de funcionarios activos dentro de la empresa **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**, de los cuales Dos (2) buzones de correo adicionales fueron suministrados el día 07 de diciembre y serán mencionados a continuación:

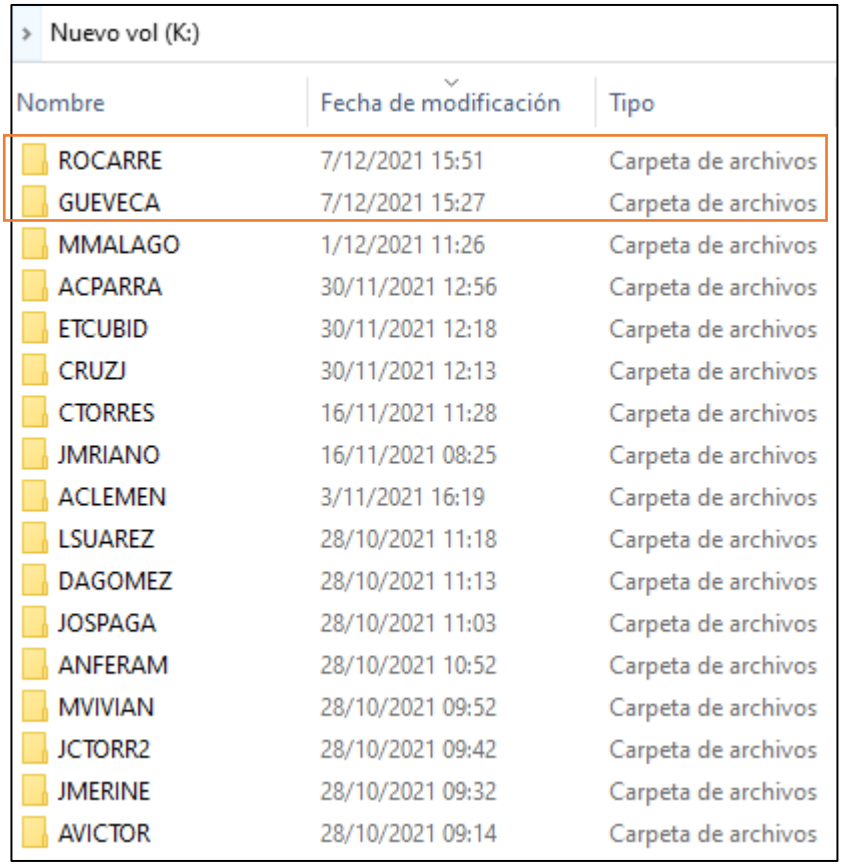


Ilustración 165 *Visualización contenido completo del Disco Duro entregado por MAPFRE SEGUROS GENERALES DE COLOMBIA S.A a 07 de diciembre de 2021.*

Adicionalmente, el señor **Willigton Leandro TORRES MORALES** indica al equipo de ADALID CORP. que no se entregaran los siguientes buzones de correo electrónico, en vista de que no se encuentran laborando en Colombia (jlcube@mapfre.com asignado a **José Luis CUBERO RIVERA** para el desarrollo de sus funciones, jalbertos@mapfre.com asignado a **Joaquín Alberto SOLERA** y aquerol@mapfre.com asignado a Luis Enrique **GIRALDO DURÁN**.

Los correos electrónicos suministrados el 07 de diciembre de 2021 serán presentados a continuación:

Correos funcionarios retirados	ORDEN ENVIO IMÁGENES fecha en la que se realizo	Tamaño GB
Carlos Alberto Guevara Mora	16 – 7 DIC -2021	**50.7 GB**
rocarre@mapfre.com.co	17 – 8 DIC -2021	**85.7 GB**

16. Buzón de correo electrónico gueveca@mapfre.com.co.

El día 01 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta GUEVECA, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:



Ilustración 166 Visualización carpeta GUEVECA

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **GUEVECA** identificada dentro del disco duro como se observa en las siguientes imágenes:

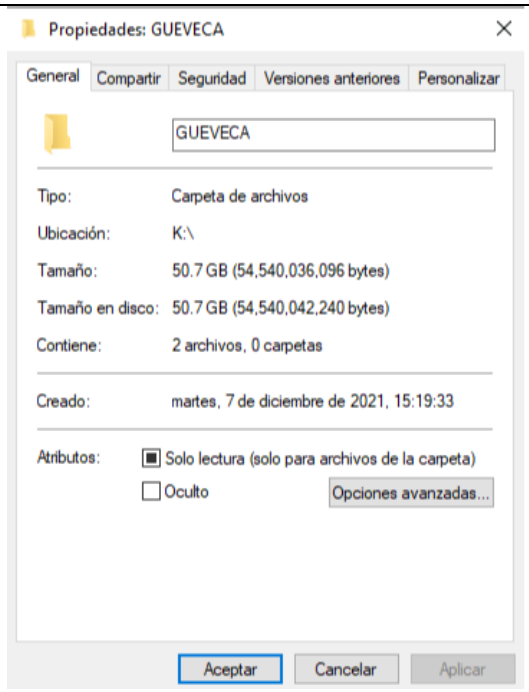


Ilustración 167 Propiedades de la carpeta GUEVECA visto desde el Disco Duro.

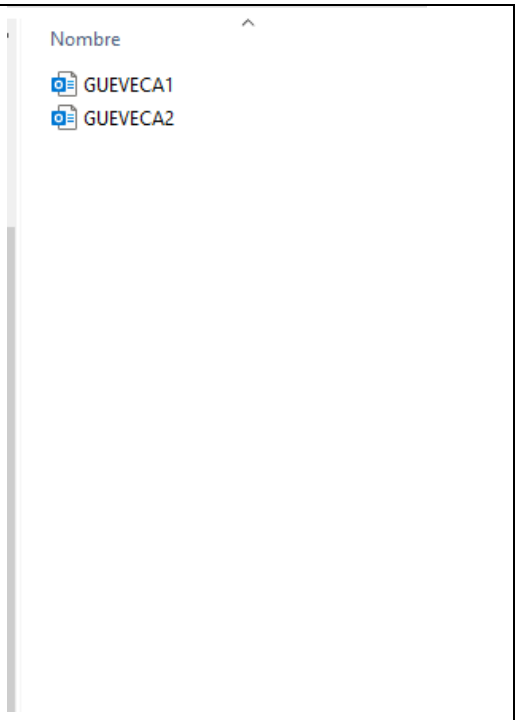


Ilustración 168 Contenido de la carpeta GUEVECA visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**gueveca@mapfre.com.co.**" asignado a **Carlos Alberto GUEVARA MORA** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **16:38:19** y culminando el mismo de forma satisfactoria a las **18:07:28,** tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_07DIC2021
Número de prueba: 016_GUEVECA
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO GUEVECA@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO

DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for
I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad1:
[Computed Hashes]
MD5 checksum: e1f945f3d80c3fc34ba37d6f39a9f07b
SHA1 checksum: a5f3f5fb0bb551475a8aa9e6b136d16d0f6c28e4

Image information:
Acquisition started: Tue Dec 7 16:38:19 2021
Acquisition finished: Tue Dec 7 17:50:18 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad22

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad23

I:\EVIDENCIA_MAPFRE_2\16.GUEVECA\IMAGENFORENSE_PST_GUEVECA_MAPFRE_07DIC2021.ad24

Image Verification Results:
Verification started: Tue Dec 7 17:50:18 2021
Verification finished: Tue Dec 7 18:07:28 2021
MD5 checksum: e1f945f3d80c3fc34ba37d6f39a9f07b : verified
SHA1 checksum: a5f3f5fb0bb551475a8aa9e6b136d16d0f6c28e4 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie ***WD-WCAZA4915847***, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:





Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**gueveca@mapfre.com.co.**" asignado a **Carlos Alberto GUEVARA MORA** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 169 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO GUEVECA@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico gueveca@mapfre.com.co asignada **Carlos Alberto GUEVARA MORA** para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
16	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Carlos Alberto GUEVARA MORA → gueveca@mapfre.com.co	ad1	50.7 GB
TOTAL					**50.7 GB**

Tabla 34 Detalle del buzón de correo electrónico asignado gueveca@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico gueveca@mapfre.com.co asignado a Carlos Alberto GUEVARA MORA para el desarrollo de sus funciones **aloja** un total de **50.7 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento noventa mil quinientas trece (190.513)** archivos (incluyendo carpetas), como se observa a continuación.

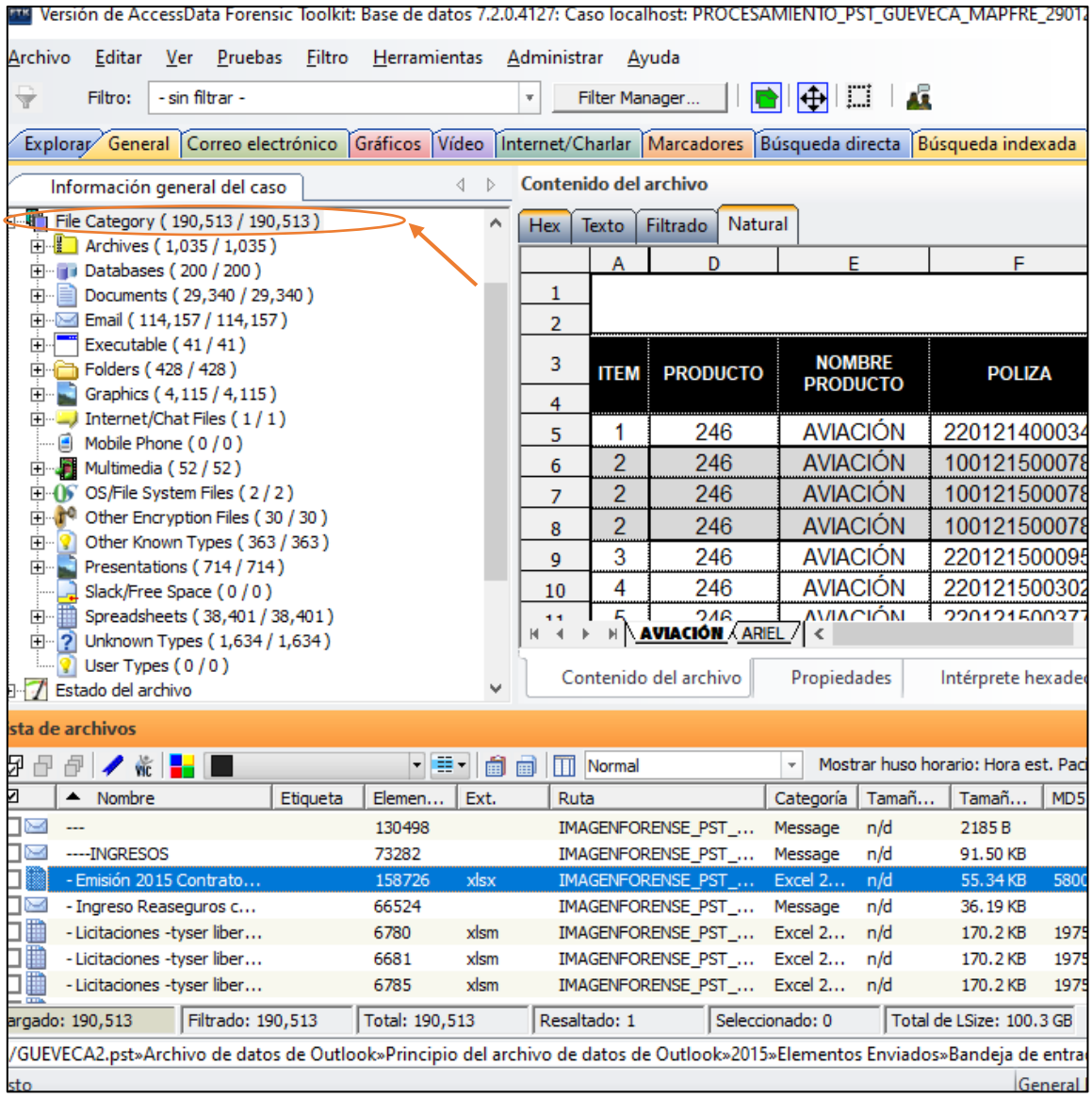


Ilustración 170 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico gueveca@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO CARLOS ALBERTO GUEVARA MORA → GUEVECA@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico gueveca@mapfre.com.co asignado a **Carlos Alberto GUEVARA MORA**, iniciando el día el **29** de enero del 2022, con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **Mil ochocientas sesenta y**

nueve (1.869) ítems en condición de "eliminados" y se reconstruyeron **Cero(0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

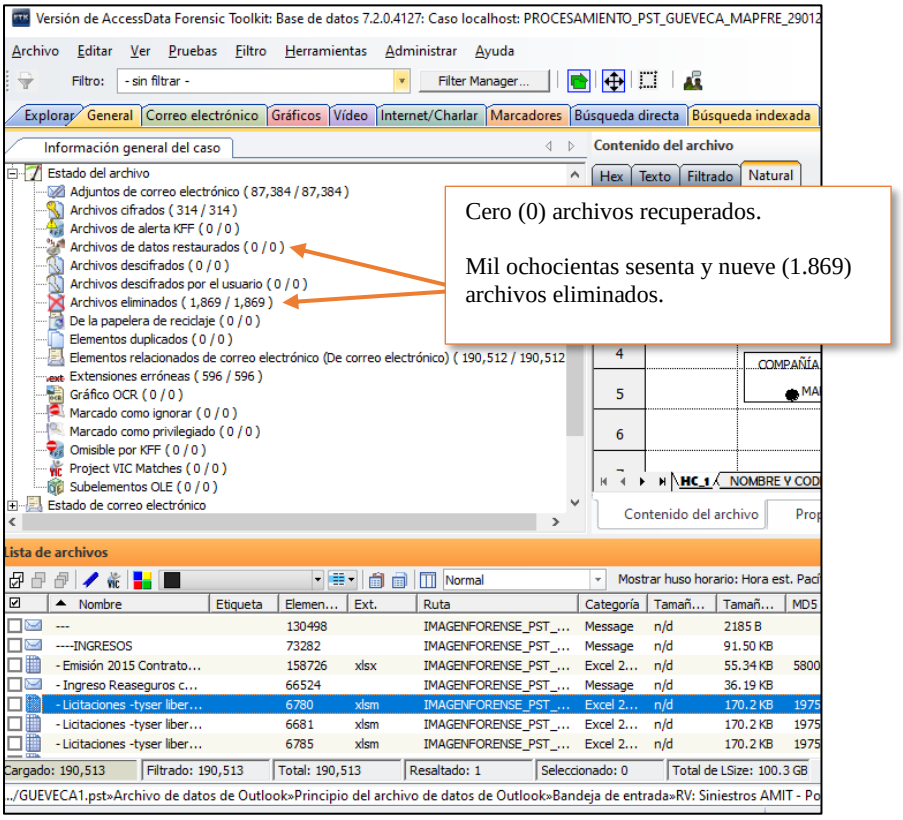


ilustración 171 Total de archivos recuperados en la cuenta de correo electrónico gueveca@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento noventa mil quinientas trece (190.513)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO GUEVECA@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico gueveca@mapfre.com.co asignado a **Carlos Alberto GUEVARA MORA** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1035
2	Bases de Datos	200
3	Documentos	29.340
4	Correo Electrónico	114.157
5	Ejecutables	41
6	Carpetas	428
7	Gráficos	4.115
8	Archivos de internet /chats	1
9	Multimedia	52
10	Archivos del sistema	2
11	Otros archivos encriptados	30
12	Otros archivos desconocidos	363
13	Presentaciones	714
14	Hojas de cálculo	38.401
15	Tipos de archivos desconocidos	1.634
TOTAL		**190.513**

Tabla 35 Información buscada evidencia 016_GUEVECA, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento noventa mil quinientas trece (190.513).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Ochenta y siete mil trescientas ochenta y cuatro (87384)** archivos de datos obtenidos por

el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

- Los archivos cifrados recuperados **Trescientas catorce (314) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos eliminados **Mil ochocientas sesenta y nueve (1.869) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento noventa mil quinientas doce (190.512)** archivos de datos obtenidos por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Quinientas noventa y seis (596) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo gueveca@mapfre.com.co asignado a **Carlos Alberto GUEVARA MORA** para para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

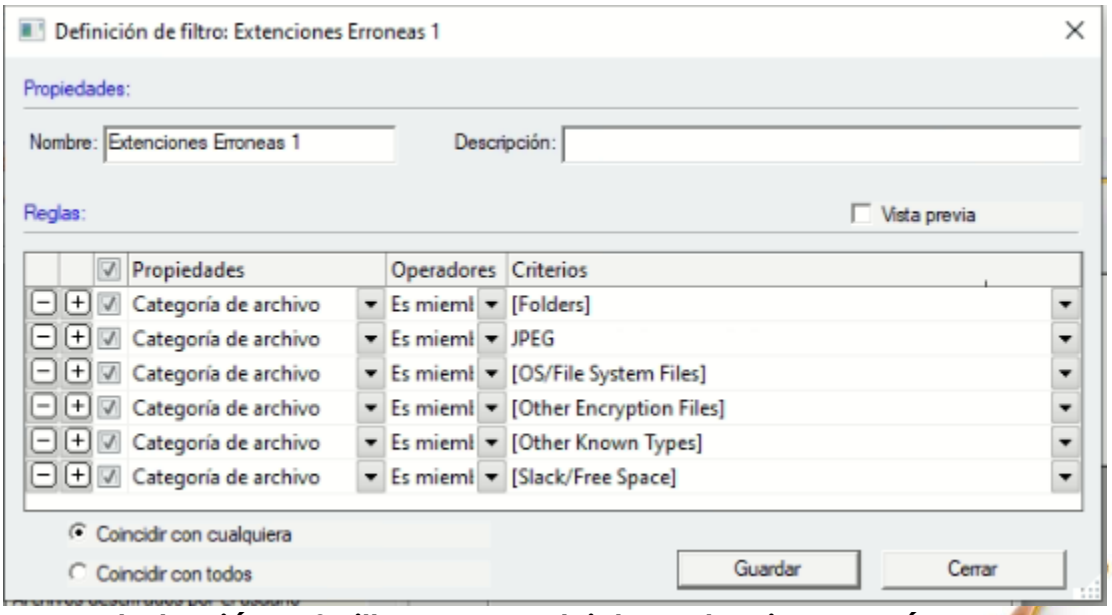


Ilustración 172 Filtro para excluir las extensiones erróneas.

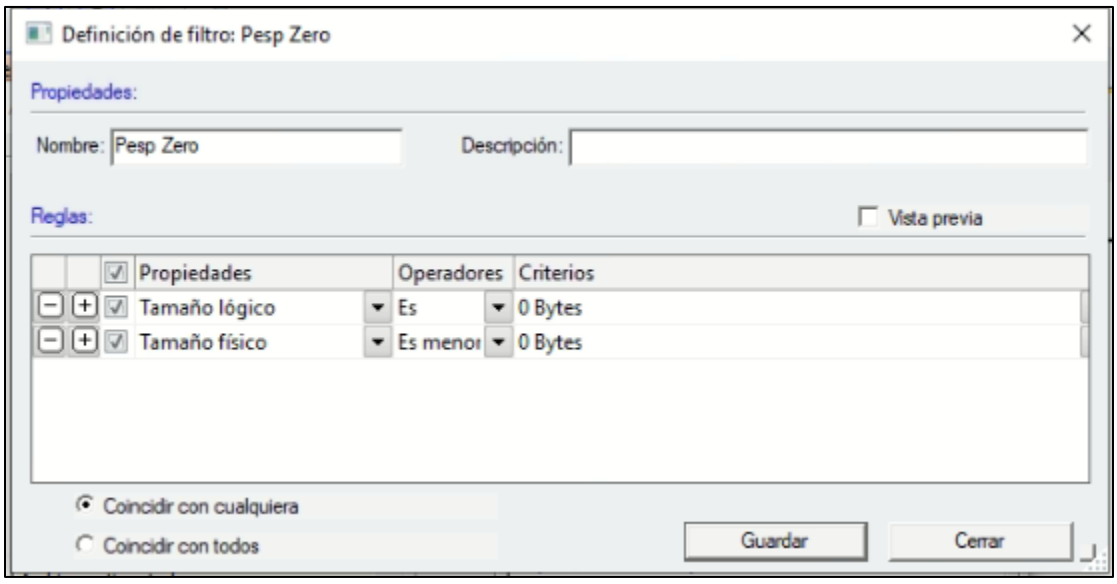


Ilustración 173 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

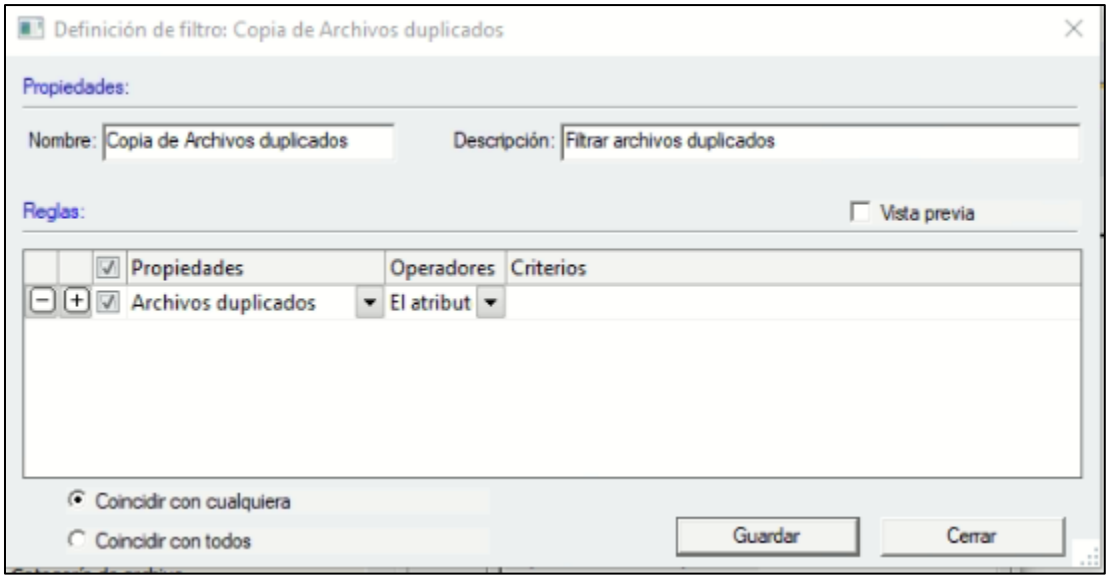


Ilustración 174 Filtro para excluir los archivos duplicados.

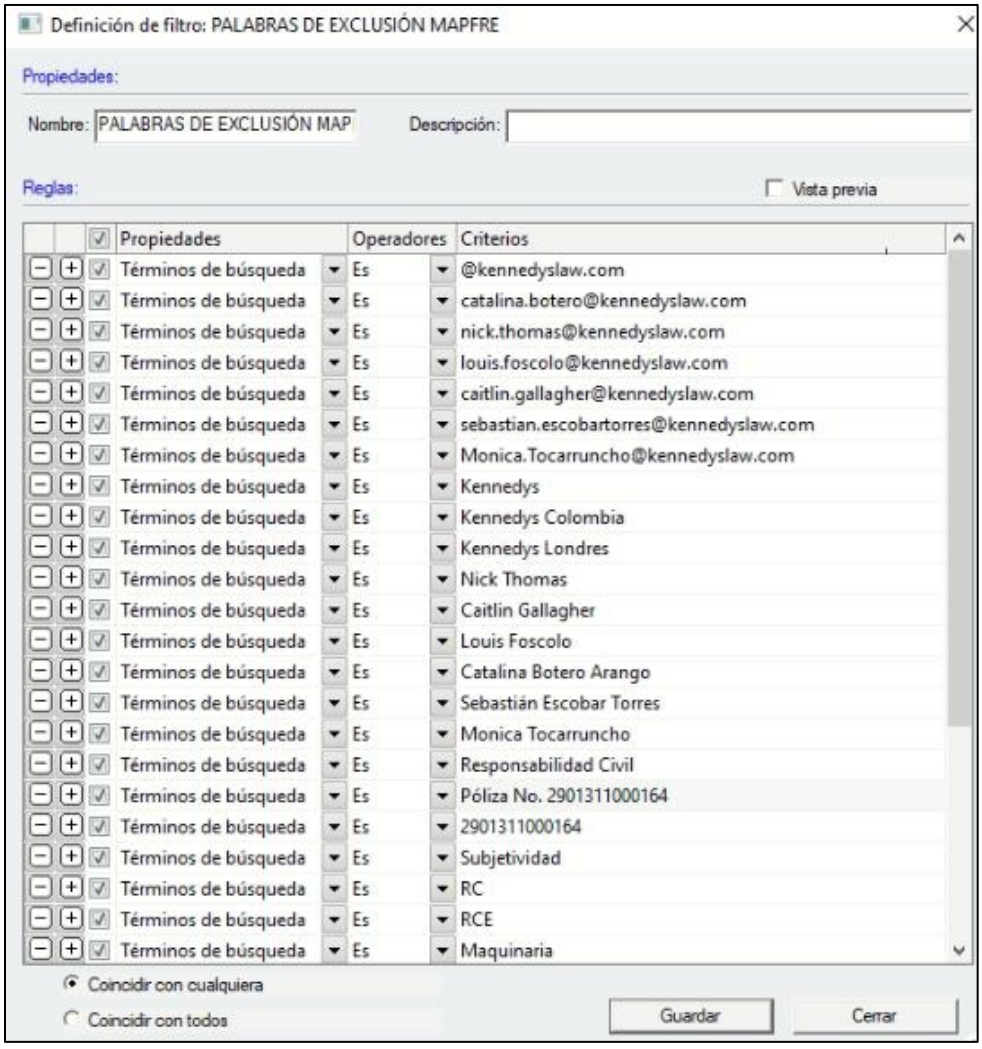


Ilustración 175 Filtro para excluir los archivos suministrado por MAPFRE - 1.

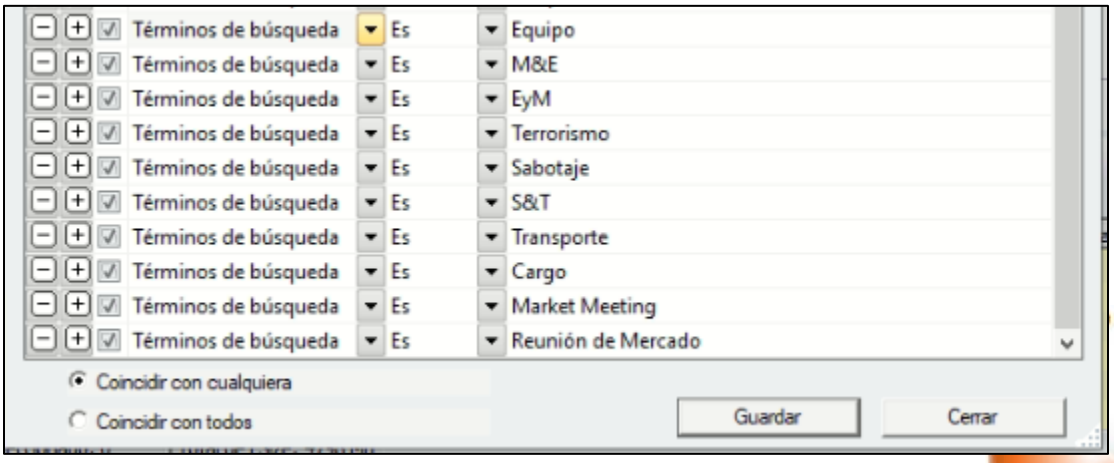
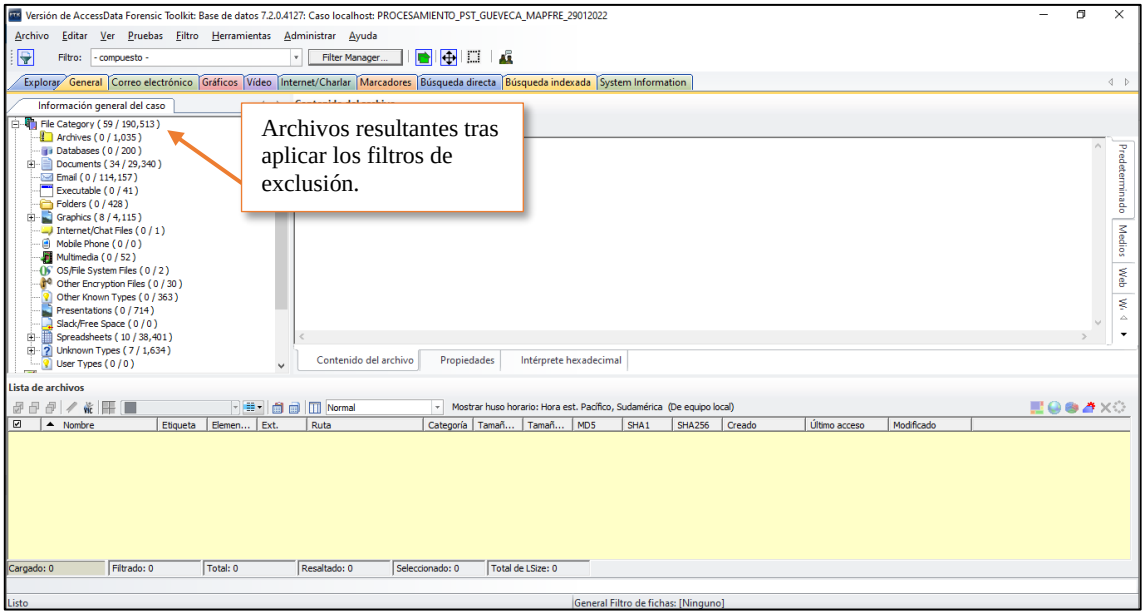


Ilustración 176 Filtro para excluir los archivos suministrado por MAPFRE - 2.

Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Cincuenta y nueve (59)** registros como se observa en la siguiente imagen:

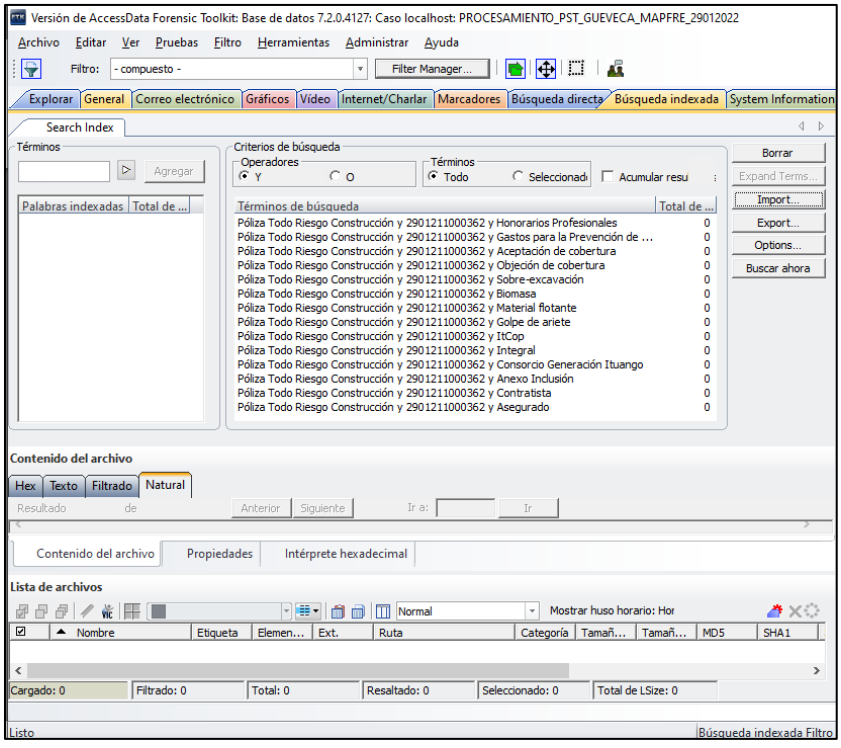


Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo gueveca@mapfre.com.co asignado a **Carlos Alberto GUEVARA MORA** para para el desarrollo de sus funciones.

17. Buzón de correo electrónico rocarre@mapfre.com.co.

El día 01 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta ROCARRE, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:



Ilustración 177 Visualización carpeta ROCARRE

Posteriormente, se procede a validar la información del contenido al interior de la carpeta ROCARRE identificada dentro del disco duro como se observa en las siguientes imágenes:

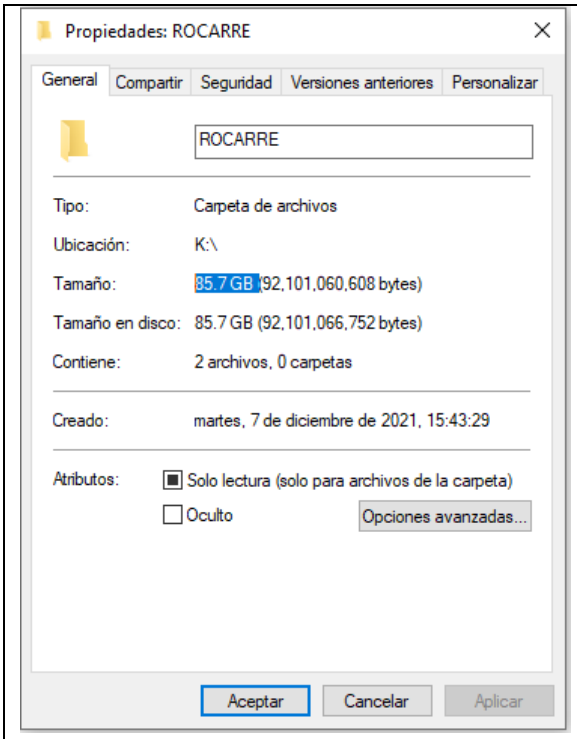


Ilustración 178 Propiedades de la carpeta ROCARRE visto desde el Disco Duro.

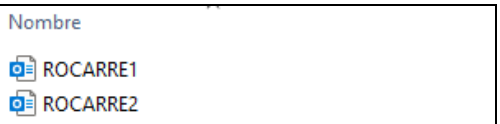


Ilustración 179 Contenido de la carpeta ROCARRE visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**rocarre@mapfre.com.co.**" asignado a ROCARRE para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las 23:07:00 y culminando el mismo de forma satisfactoria a las 02:13:30, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_08DIC2021
Número de prueba: 017_ROCARRE
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ROCARRE@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE

FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas:

Information for
I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad1:
[Computed Hashes]
MD5 checksum: 775edcc80edc04552a83d75e90da2aac
SHA1 checksum: fab4be9073e47a100aaedfcbec42de7fffa2443f

Image information:
Acquisition started: Wed Dec 8 23:07:00 2021
Acquisition finished: Thu Dec 9 01:38:21 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad20

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad21

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad22

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad23

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad24

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad25

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad26

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad27

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad28

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad29

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad30

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad31

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad32

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad33

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad34

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad35

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad36

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad37

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad38

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad39

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad40

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad41

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad42

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad43

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad44

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad45

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad46

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad47

I:\EVIDENCIA_MAPFRE_2\17.ROCARRE\IMAGENFORENSE_PST_ROCARRE_MAPFRE_08DIC2021.ad48

Image Verification Results:
Verification started: Thu Dec 9 01:38:21 2021
Verification finished: Thu Dec 9 02:13:30 2021
MD5 checksum: 775edcc80edc04552a83d75e90da2aac : verified

SHA1 checksum: fab4be9073e47a100aaedfcbec42de7fffa2443f : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca WESTERN DIGITAL, identificado con número de serie WD-WCAZA4915847, con capacidad de almacenamiento de 2000GB, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**rocarre@mapfre.com.co.**" asignado a **Rodrigo CARREÑO HERNÁNDEZ** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o

requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 180 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ROCARRE@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas MAPFRE SEGUROS GENERALES DE COLOMBIA S.A. para la cuenta de correo electrónico rocarre@mapfre.com.co asignada Rodrigo CARREÑO HERNÁNDEZ para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
17	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Rodrigo CARREÑO HERNÁNDEZ → rocarre@mapfre.com.co	ad1	85.7 GB
TOTAL					**85.7 GB**

Tabla 36 Detalle del buzón de correo electrónico asignado rocarre@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico rocarre@mapfre.com.co asignado a Rodrigo **CARREÑO HERNÁNDEZ** para el desarrollo de sus funciones **aloja** un total de **85.7 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento setenta y cuatro mil seiscientas cincuenta y dos (174.652)** archivos (incluyendo carpetas), como se observa a continuación.

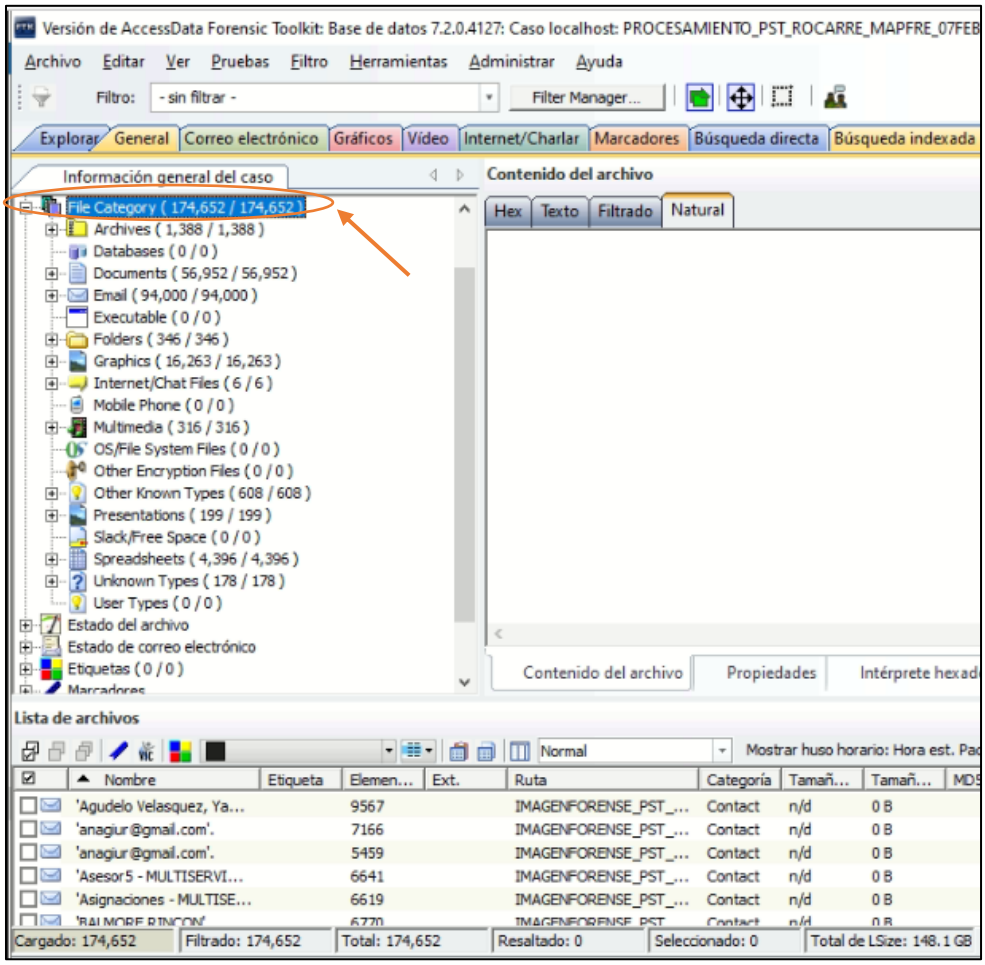


Ilustración 181 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico rocarre@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO RODRIGO CARREÑO HERNÁNDEZ → ROCARRE@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico rocarre@mapfre.com.co

asignado a Rodrigo CARREÑO HERNÁNDEZ, iniciando el día el **07** de febrero del 2022, con una duración aproximada de Cuatro (4) día calendario, el resultado a dicho proceso arrojó que existen **Mil doscientas setenta y una (1.271)** ítems en condición de "eliminados" y se reconstruyeron **Cero (0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

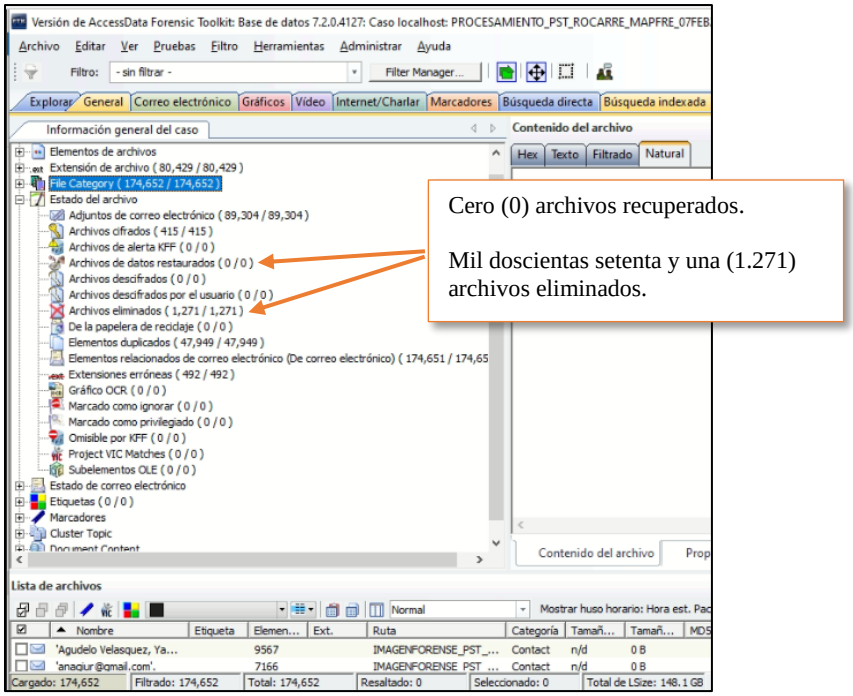


ilustración 182 Total de archivos recuperados en la cuenta de correo electrónico rocarre@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento setenta y cuatro mil seiscientas cincuenta y dos (174.652)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ROCARRE@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico rocarre@mapfre.com.co asignado a Rodrigo **CARREÑO HERNÁNDEZ** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1388
2	Documentos	56.952
3	Correo Electrónico	94.000
4	Carpetas	346
5	Gráficos	16.263
6	Archivos de internet/chats	6
7	Multimedia	316
8	Otros archivos desconocidos	608
9	Presentaciones	199
10	Hojas de cálculo	4.396
11	Tipos de archivos desconocidos	178
TOTAL		**174.652**

Tabla 37 Información buscada evidencia 017_ROCARRE, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento setenta y cuatro mil seiscientas cincuenta y dos (174.652).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Ochenta y nueve mil trescientas cuatro (89.304) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Cuatrocientas quince (415) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos eliminados **Mil doscientas setenta y una (1.271) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Cuarenta y siete mil novecientas cuarenta y nueve (47949) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento setenta y cuatro mil seiscientas cincuenta y una (174651) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Cuatrocientas noventa y dos (492) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico rocarre@mapfre.com.co asignado a Rodrigo **CARREÑO HERNÁNDEZ** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:

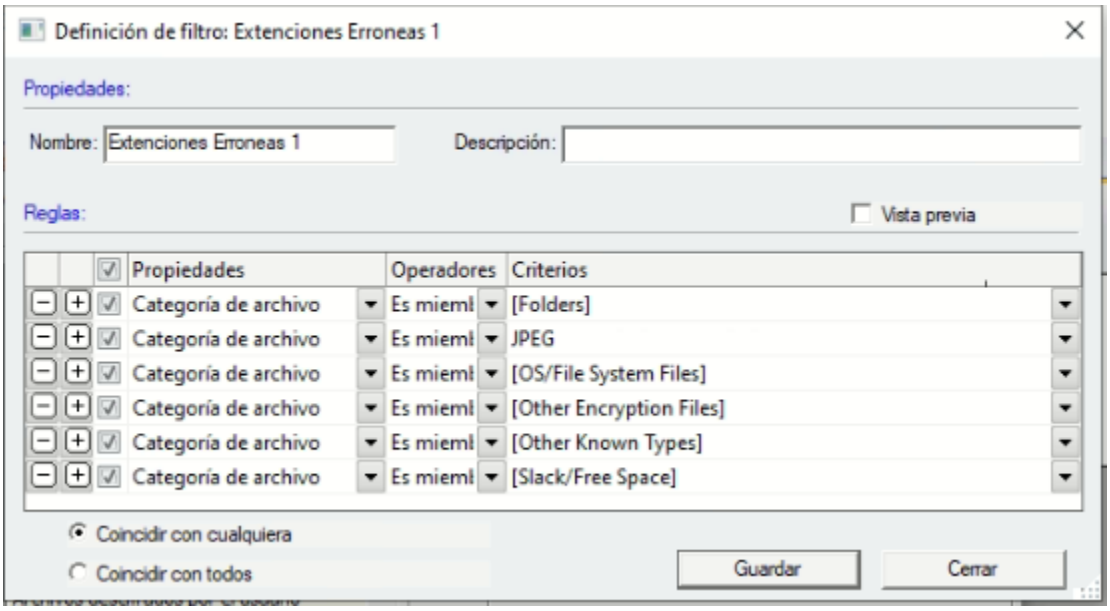


Ilustración 183 Filtro para excluir las extensiones erróneas.

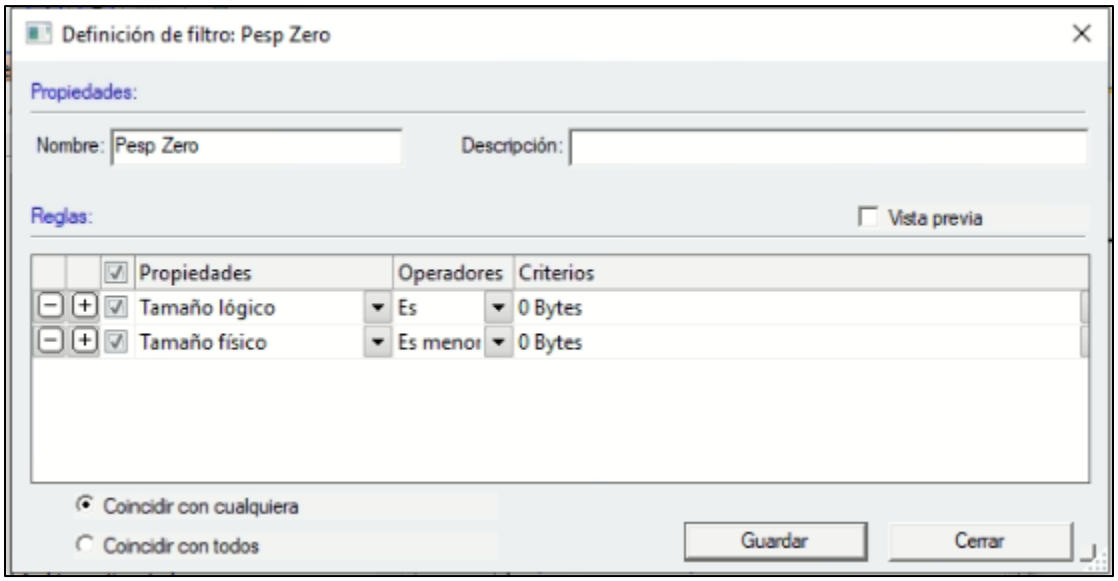


Ilustración 184 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

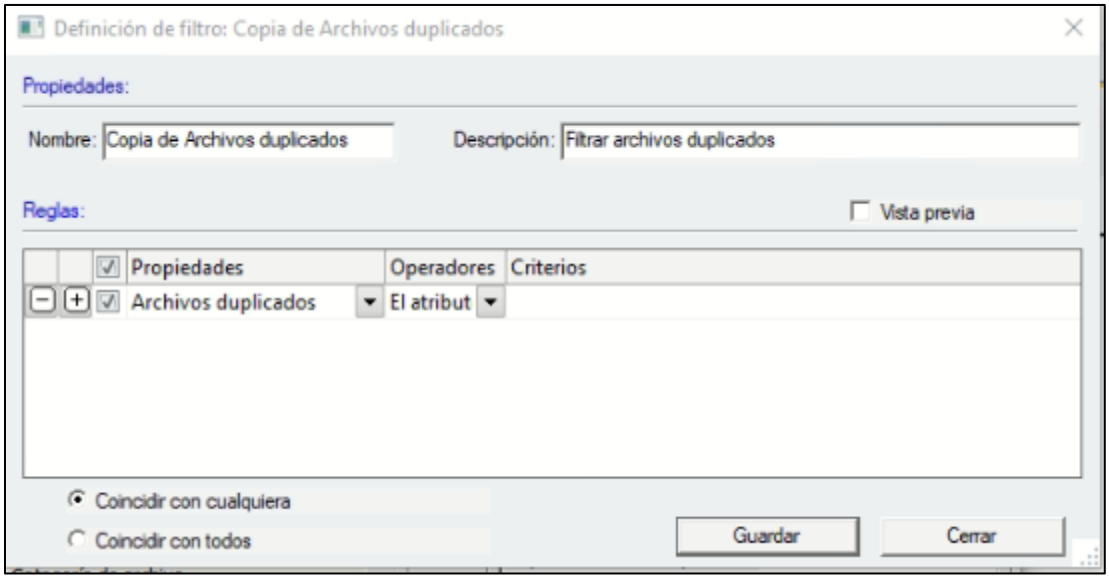


Ilustración 185 Filtro para excluir los archivos duplicados.

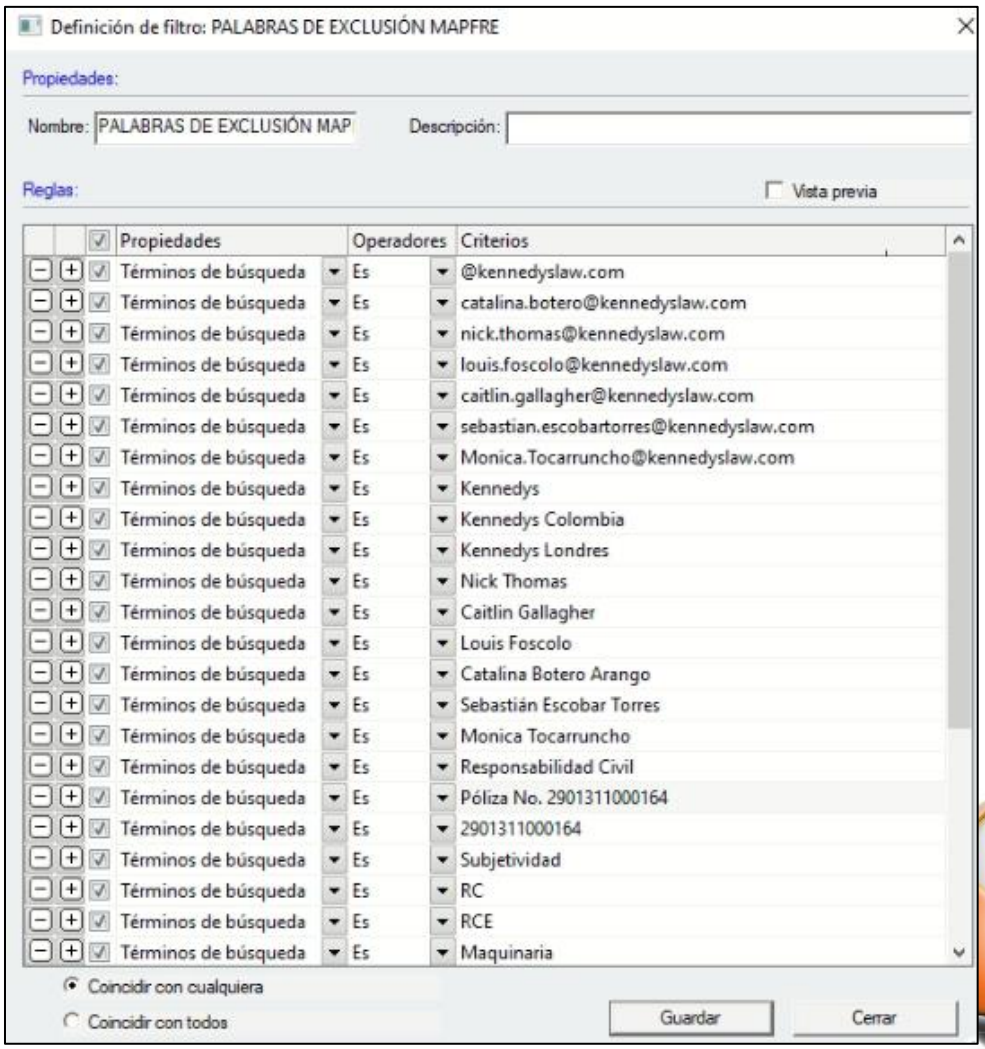


Ilustración 186 Filtro para excluir los archivos suministrado por MAPFRE - 1.

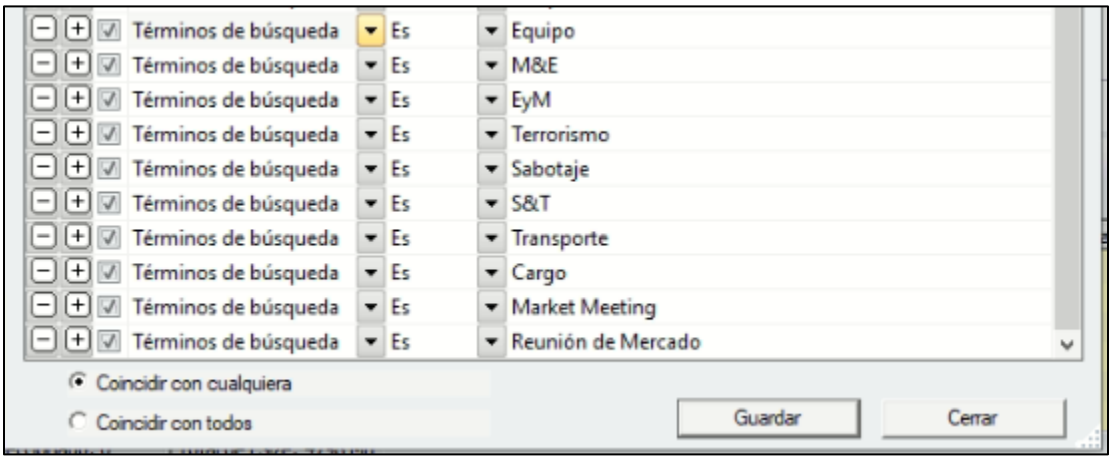
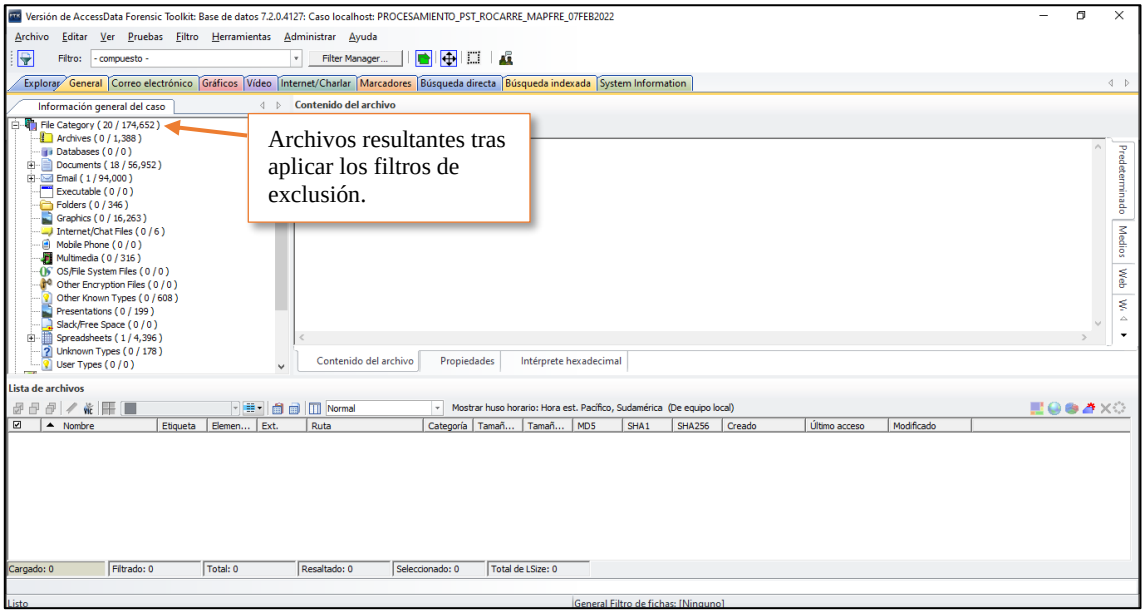


Ilustración 187 Filtro para excluir los archivos suministrado por MAPFRE - 2.

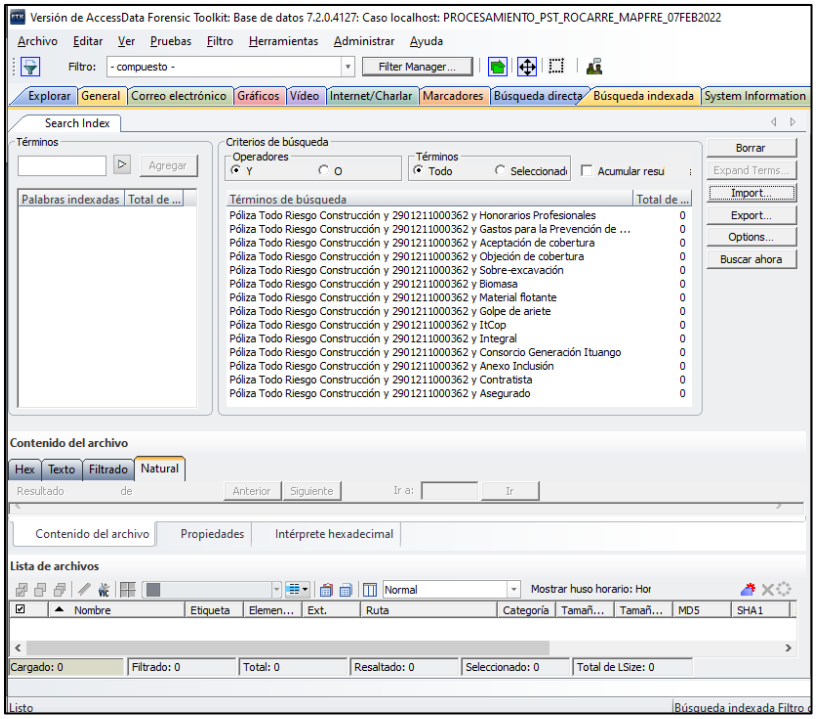
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Veinte (20)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo rocarre@mapfre.com.co asignado a Rodrigo **CARREÑO HERNÁNDEZ** para el desarrollo de sus funciones.

Una vez realizadas las imágenes forenses para los buzones de correo electrónico pertenecientes a (2) funcionarios de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** los cuales se encuentran identificados con las siguientes direcciones de correo (gueveca@mapfre.com.co, rocarre@mapfre.com.co) el equipo de ADALID CORP hace entrega de (1) Un disco duro color blanco, con capacidad de almacenamiento de **1000GB** al señor **Willigton Leandro TORRES MORALES,** identificado con cédula de ciudadanía **No. 79.708.420** de Bogotá, quien funge como **PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN** el día 14 de diciembre a las 16:00 horas.

De igual manera, el día 16 diciembre de 2021, el señor **Willigton Leandro TORRES MORALES** nuevamente hace entrega a los peritos de ADALID CORP. de (1) Un disco duro color **blanco**, con capacidad de almacenamiento de **1000GB**, el cual en su parte superior se encuentra marcado como **"prueba extraprocesal"** como se presenta a continuación**:**

	
Fotografía Disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista superior)	Fotografía disco duro entregado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A** (Vista posterior)

Al interior del Disco Duro se identifican Dos (2) buzones de correo en formato .PST como se muestra en la siguiente imagen:

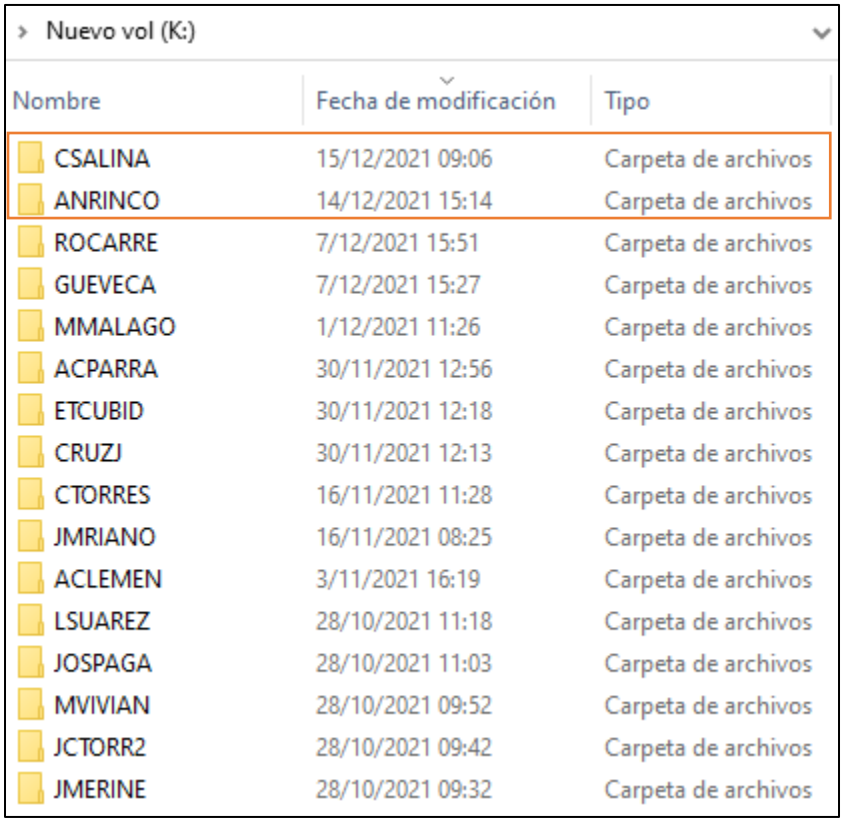


Ilustración 188 *Visualización contenido completo del Disco Duro entregado por MAPFRE SEGUROS GENERALES DE COLOMBIA S.A a 17 de diciembre de 2021.*

Los correos electrónicos suministrados el 16 de diciembre de 2021 serán presentados a continuación:

Correos funcionarios retirados	ORDEN ENVIO IMÁGENES fecha en la que se realizo	Tamaño GB
Claudia Rocio SALINASI	**18 – 17 DIC -2021**	**40.4 GB**
Andrés Alfonso RINCON	**19 – 17 DIC -2021**	**55.6 GB**

18. Buzón de correo electrónico csalina@mapfre.com.co.

El día 17 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta **CSALINA**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

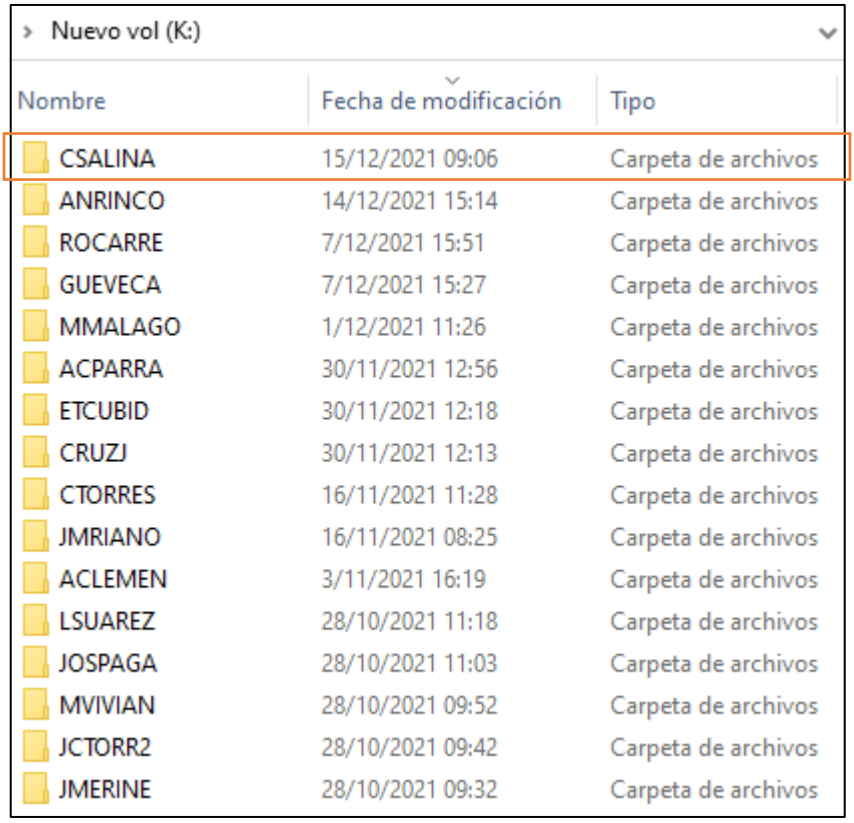


Ilustración 189 Visualización carpeta CSALINA

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **CSALINA** identificada dentro del disco duro como se observa en las siguientes imágenes:

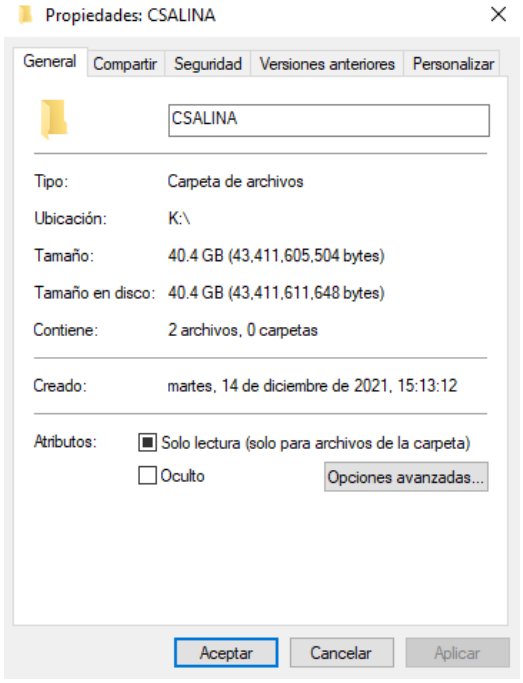


Ilustración 190 Propiedades de la carpeta CSALINA visto desde el Disco Duro.

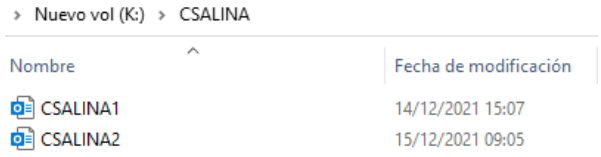


Ilustración 191 Contenido de la carpeta CSALINA visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**csalina@mapfre.com.co**" asignado a **Claudia ROCIO SALINASI** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **09:28:43** y culminando el mismo de forma satisfactoria a las **10:17:32**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_17DIC2021
Número de prueba: 18_CSALINA
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO CSALINA@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO

DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad1:
[Custom Content Sources]
K::K:\ | CSALINA | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: ec0267c1a3ffa7b40f2a9d9b6c1bbcc0
SHA1 checksum: b5e7ea4b96117e879d13928e2dc3da51aa6c4089

Image information:
Acquisition started: Fri Dec 17 09:28:43 2021
Acquisition finished: Fri Dec 17 10:07:33 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad1

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad2

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad3

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad4

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad5

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad6

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad7

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad8

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad9

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad10

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad11

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad12

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad13

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad14

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad15

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad16

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad17

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad18

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad19

I:\EVIDENCIA_MAPFRE_2\18.CSALINA\IMAGENFORENSE_PST_CSALINA_MAPFRE_17DIC2021.ad20

Image Verification Results:

Verification started: Fri Dec 17 10:07:34 2021 Verification finished: Fri Dec 17 10:17:32 2021 MD5 checksum: ec0267c1a3ffa7b40f2a9d9b6c1bbcc0 : verified SHA1 checksum: b5e7ea4b96117e879d13928e2dc3da51aa6c4089 : verified
Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL**, identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:

	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**csalina@mapfre.com.co.**" asignado a **Claudia ROCIO SALINASI** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**

Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 192 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO CSALINA@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** para la cuenta de correo electrónico csalina@mapfre.com.co asignada Claudia ROCIO SALINASI para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
18	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Claudia ROCIO SALINASI → csalina@mapfre.com.co	ad1	40.4 GB
TOTAL					**40.4 GB**

Tabla 38 Detalle del buzón de correo electrónico asignado csalina@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico csalina@mapfre.com.co asignado a Claudia ROCIO SALINASI para el desarrollo de sus funciones **aloja** un total de **40.4 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento veinticinco mil seiscientos dieciocho (125.618)** archivos (incluyendo carpetas), como se observa a continuación.

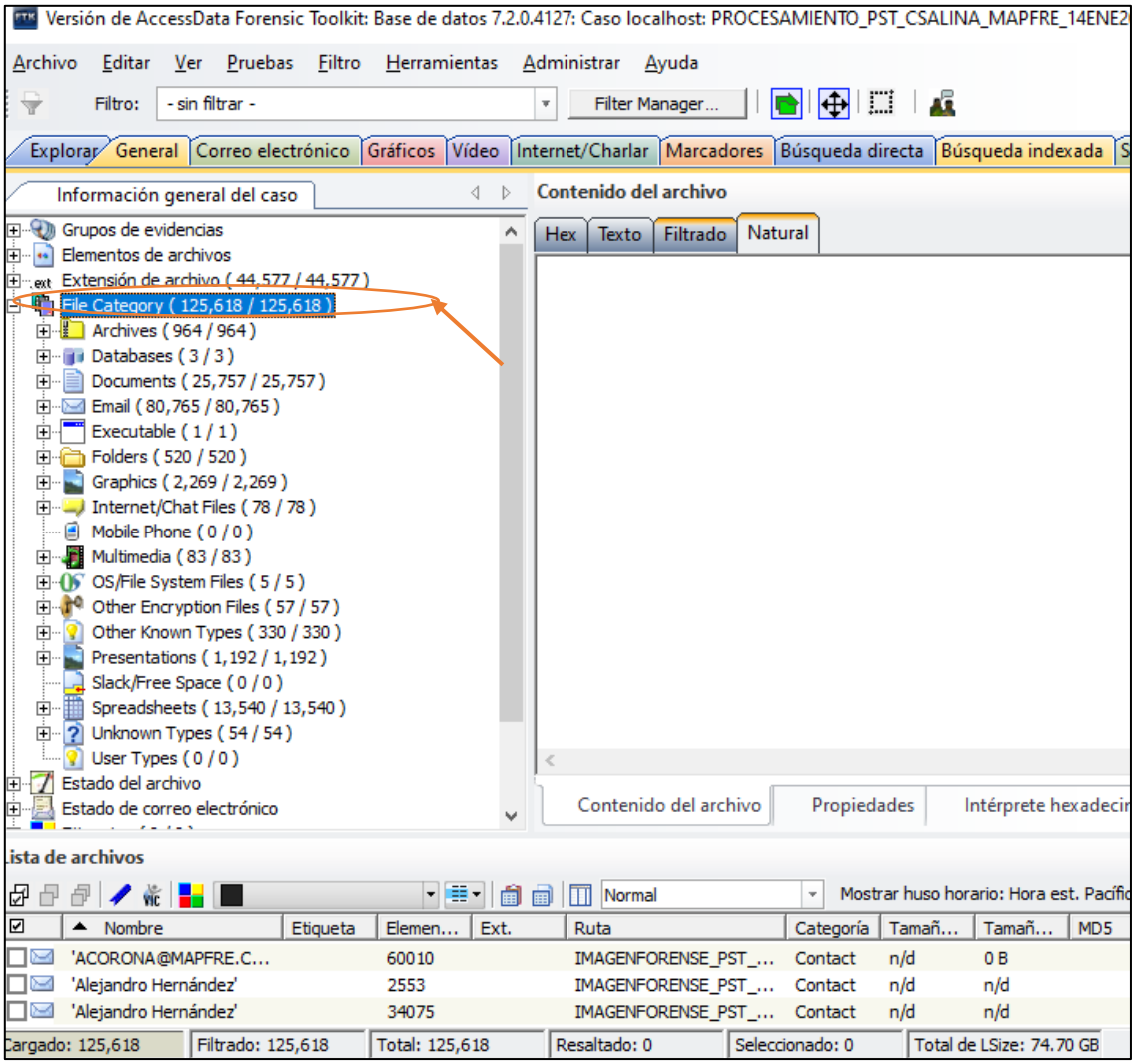


Ilustración 193 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico csalina@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO CLAUDIA ROCIO SALINASI → CSALINA@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos,

en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico csalina@mapfre.com.co asignado a Claudia ROCIO SALINASI, iniciando el día el **14** de enero del 2022, con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **Cuatrocientos treinta y cuatro (434)** ítems en condición de "eliminados" y se reconstruyeron **Cero (0)** archivos de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

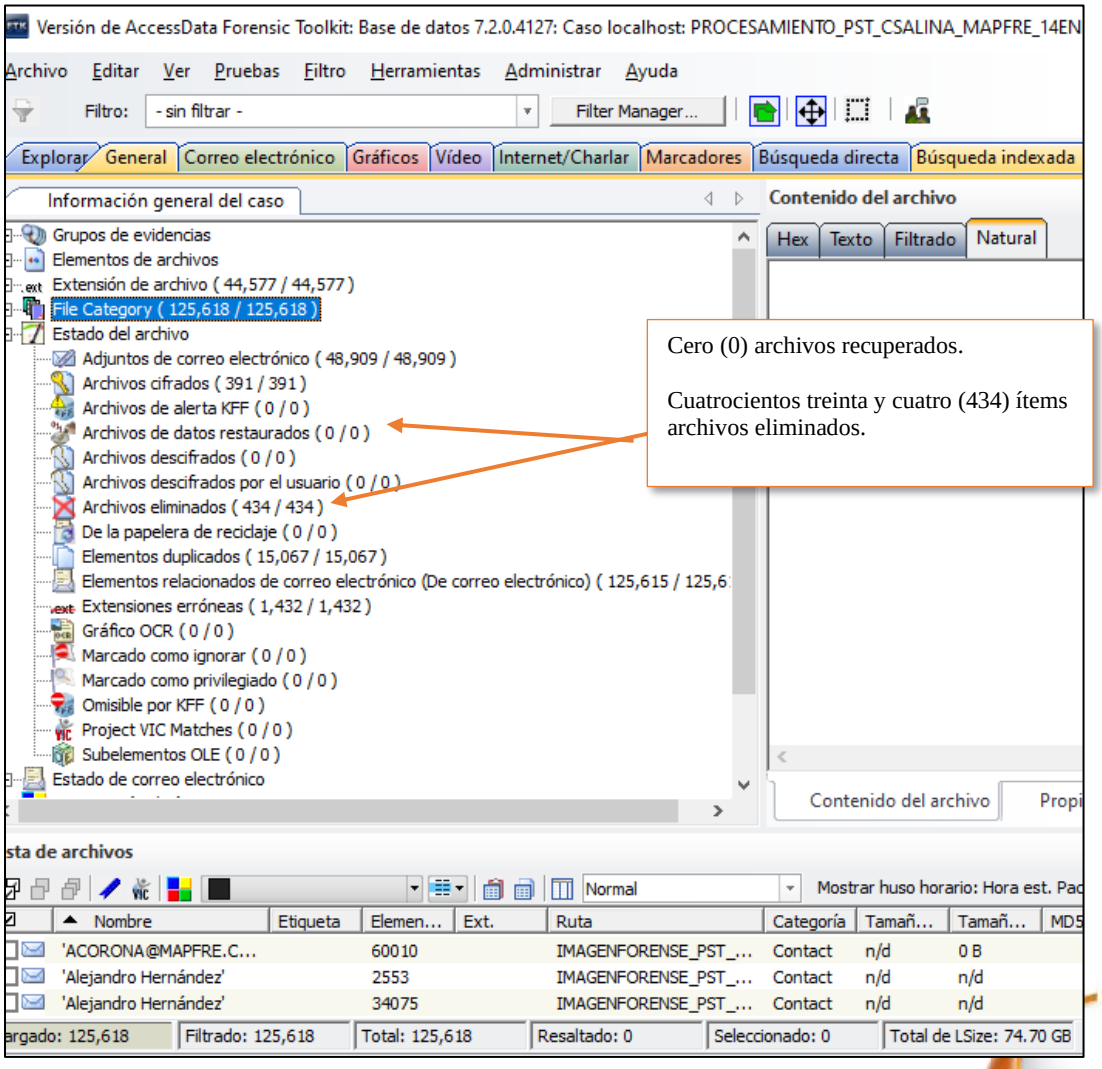


ilustración 194 Total de archivos recuperados en la cuenta de correo electrónico csalina@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS**

GENERALES DE COLOMBIA S.A., es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento veinticinco mil seiscientos dieciocho (125.618)** archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO CSALINA@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico csalina@mapfre.com.co asignado a **Claudia ROCIO SALINASI** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	964
2	Bases de Datos	3
3	Documentos	25.757
4	Correo Electrónico	80.765
5	Ejecutables	1
6	Carpetas	520
7	Gráficos	2.269
8	archivos de internet/chat	78
9	Multimedia	83
10	Archivos del sistema	5
11	Otros archivos encriptados	57
12	Otros archivos desconocidos	330
13	Presentaciones	1192
14	Hojas de cálculo	13.540
15	Tipos de archivos desconocidos	54
TOTAL		**125.618**

Tabla 39 Información buscada evidencia 018_CSALINA, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento veinticinco mil seiscientos dieciocho (125.618)**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de

depuración de datos a fin de eliminar archivos corruptos o que no sean legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Cuarenta y ocho mil novecientos nueve (48.909) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Trescientos noventa y un (391) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos Eliminados **Cuatrocientos treinta y cuatro (434) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos duplicados **Quince mil sesenta y siete (15.067) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento veinticinco mil seiscientos quince (125.615) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Mil cuatrocientos treinta y dos (1432) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico csalina@mapfre.com.co asignado a **Claudia ROCIO SALINASI** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



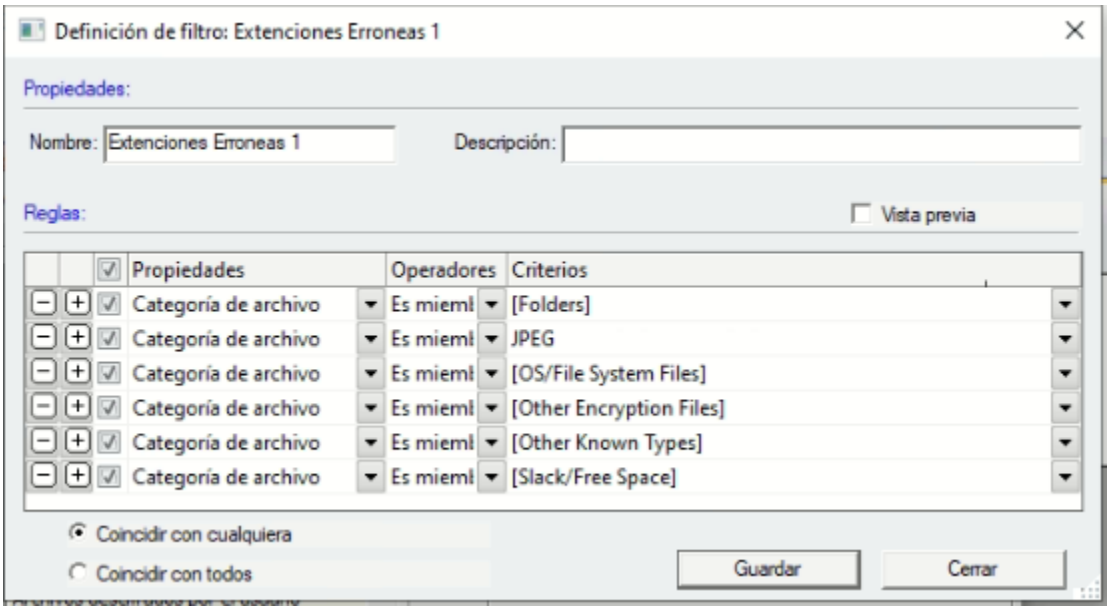


Ilustración 195 Filtro para excluir las extensiones erróneas.

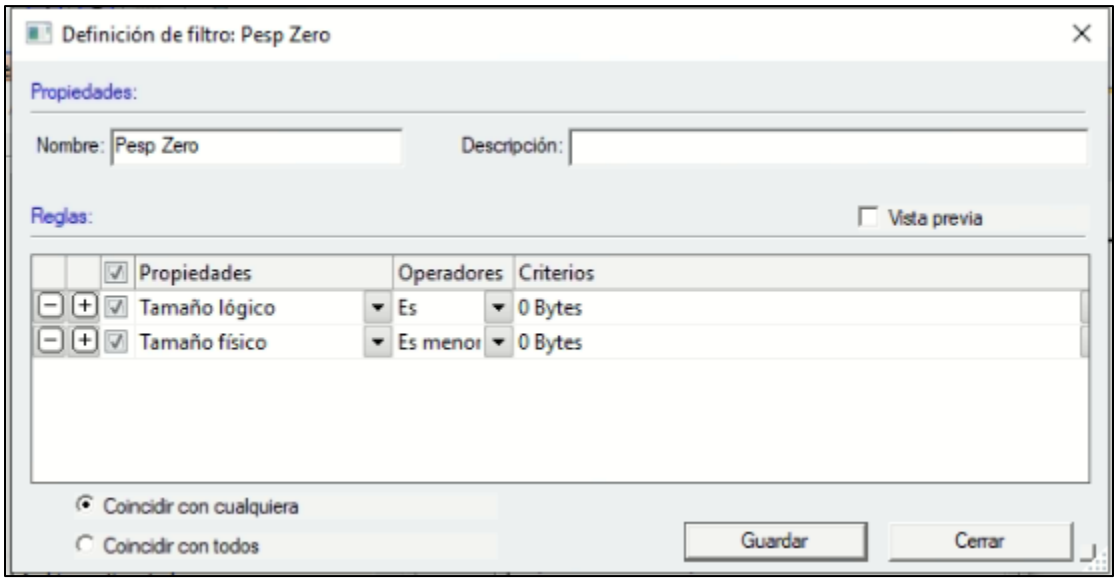


Ilustración 196 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

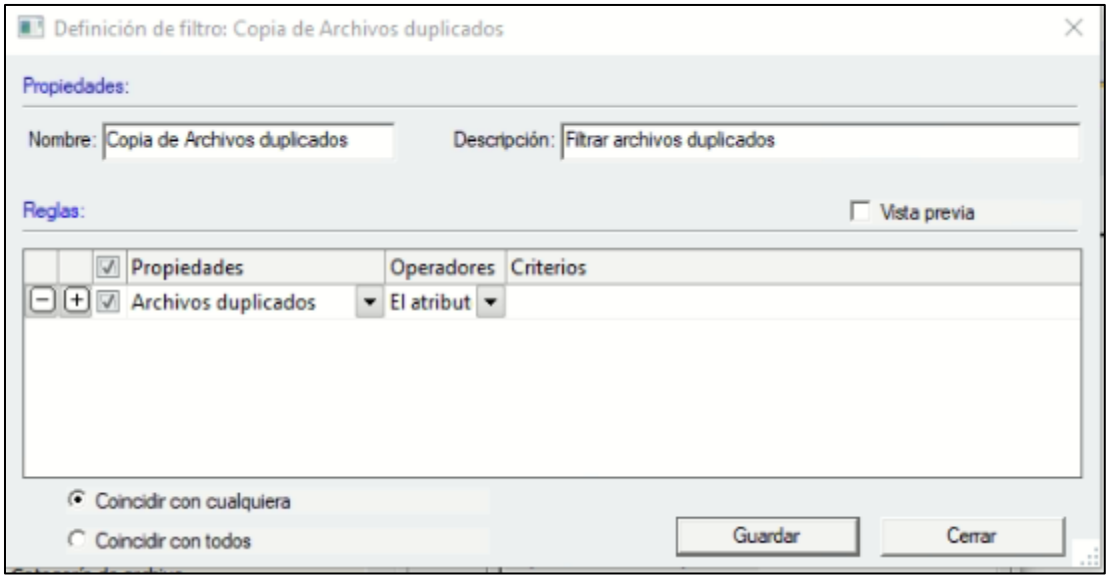


Ilustración 197 Filtro para excluir los archivos duplicados.

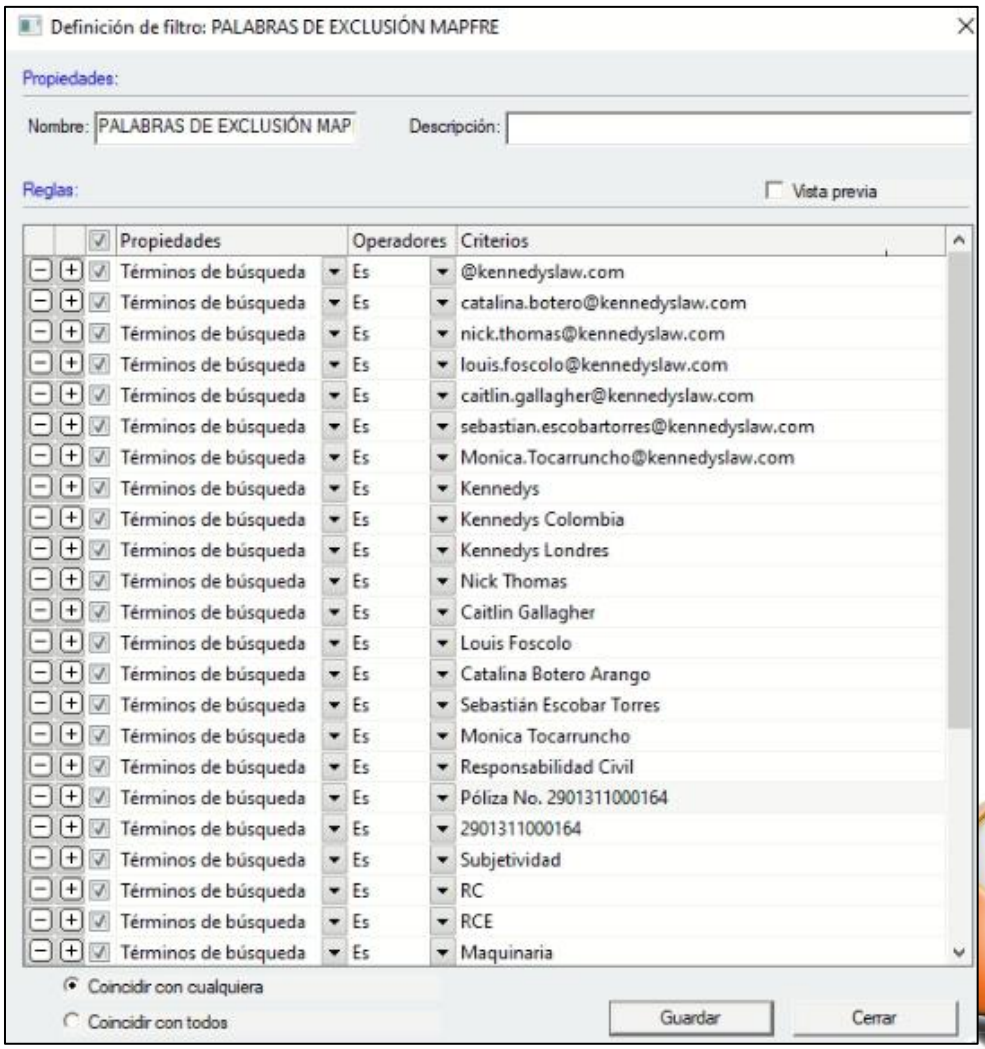


Ilustración 198 Filtro para excluir los archivos suministrado por MAPFRE - 1.

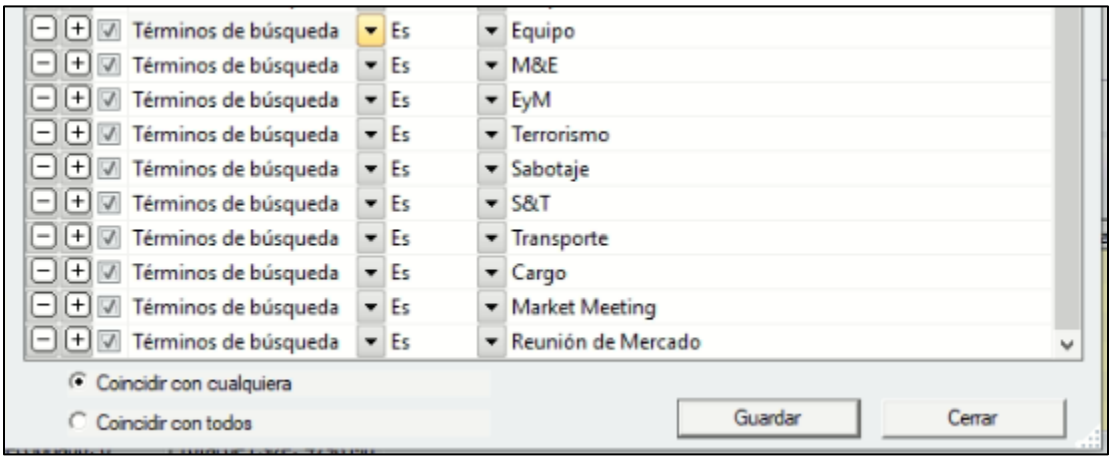
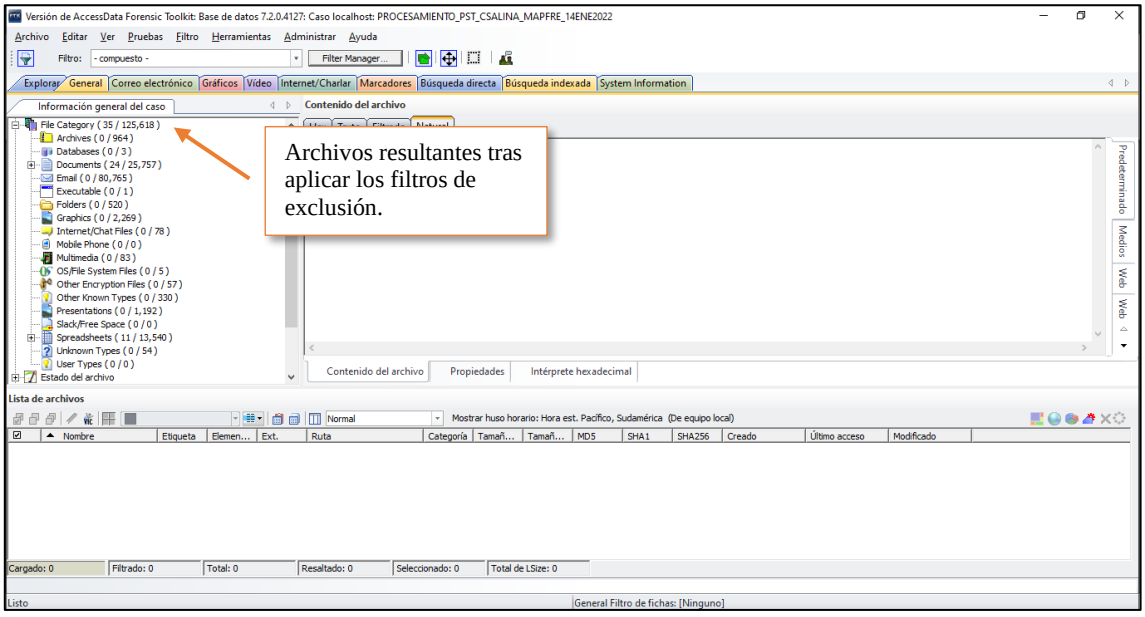


Ilustración 199 Filtro para excluir los archivos suministrado por MAPFRE - 2.

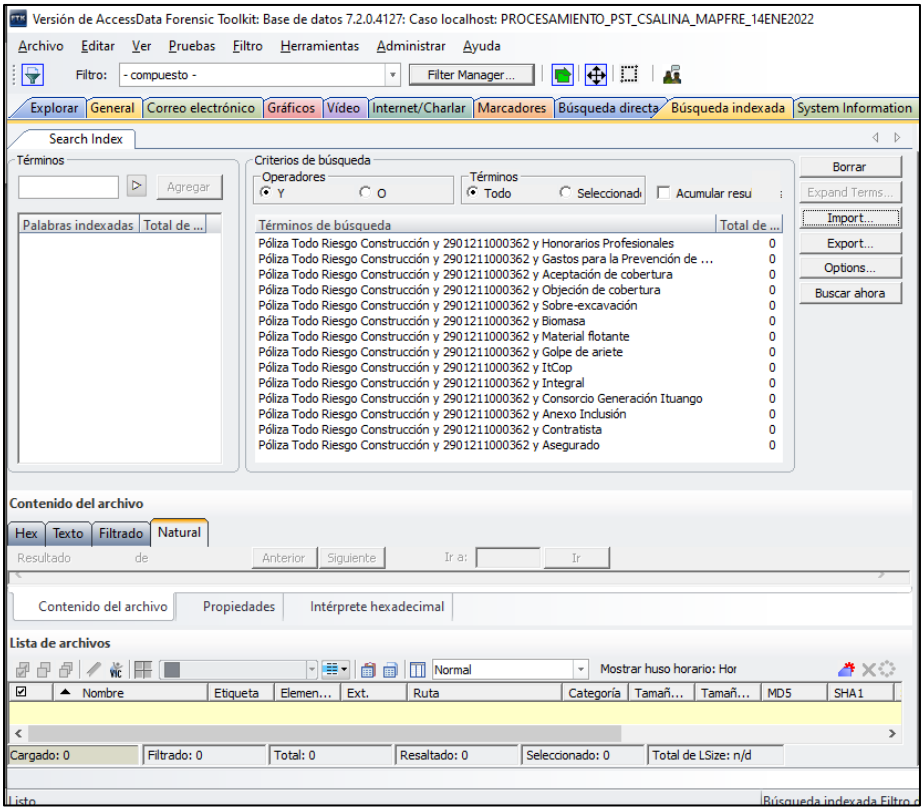
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Treinta y cinco (35)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de correo csalina@mapfre.com.co asignado a **Claudia ROCIO SALINASI** para el desarrollo de sus funciones.

19. Buzón de correo electrónico anrinco@mapfre.com.co.

El día 17 de diciembre 2021, el equipo de ADALID CORP ingresa a la carpeta **ANRINCO**, la cual se encuentra almacenada en el interior del disco duro como se observa a continuación:

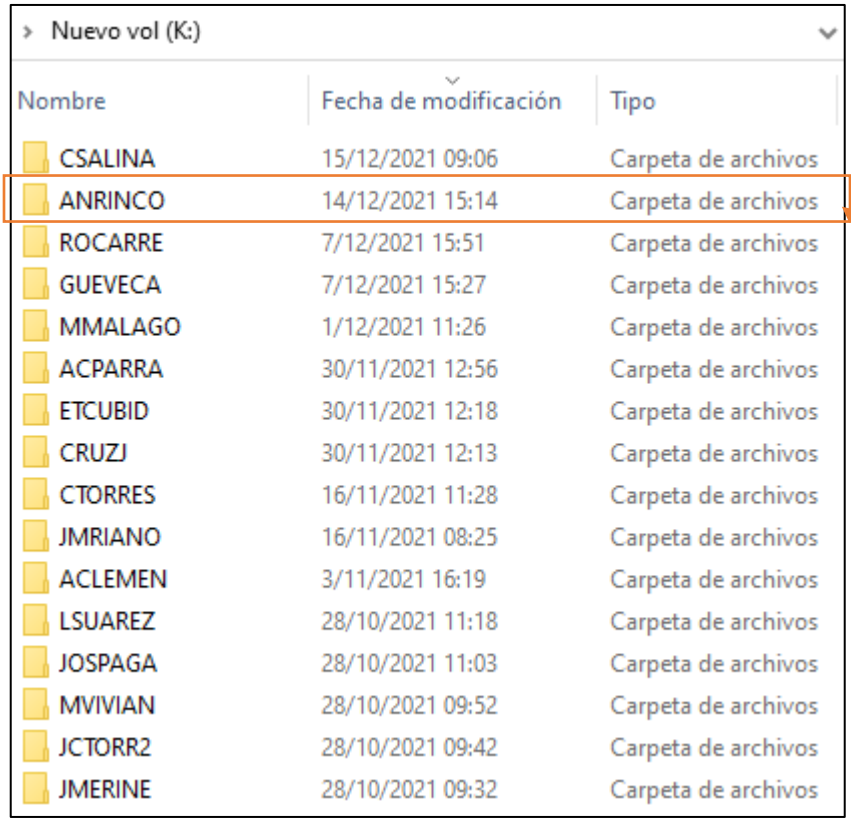


Ilustración 200 Visualización carpeta ANRINCO

Posteriormente, se procede a validar la información del contenido al interior de la carpeta **ANRINCO** identificada dentro del disco duro como se observa en las siguientes imágenes:

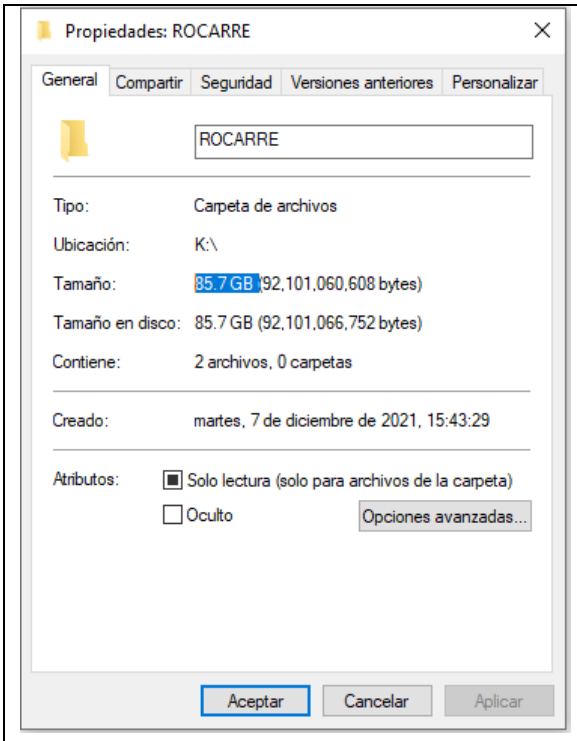


Ilustración 201 Propiedades de la carpeta ANRINCO visto desde el Disco Duro.

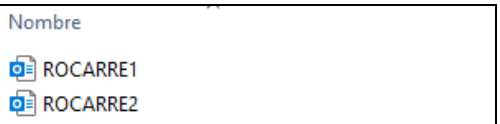


Ilustración 202 Contenido de la carpeta ANRINCO visto desde el Disco Duro.

Finalizado el proceso de identificación de las propiedades y el contenido del buzón de correo electrónico "**anrinco@mapfre.com.co**" asignado a **Andrés Alfonso RINCON** para el cumplimiento de sus funciones los peritos informáticos de ADALID CORP., inician el proceso de creación de imagen forense lógica utilizando el software FTK Imager en su versión 4.5.0.3, iniciando el proceso a las **10:24:34** y culminando el mismo de forma satisfactoria a las **11:28:33**, tal como se evidencia a continuación:

Creado por AccessData® FTK® Imager 4.5.0.3

Información del caso:
Se Adquirió usando: ADI4.5.0.3
Número de caso:
CASO_PRUEBAEXTRAPROCESAL_JUZGADO19CIVILCIRCUITOBOGOTÁ_MAPFRE_17DIC2021
Número de prueba: 19_ANRINCO
Descripción única: CARPETA CONTENEDORA DE ARCHIVOS EN FORMATO .PST DEL USUARIO ANRINCO@MAPFRE.COM.CO, ENTREGADOS POR MAPFRE A ADALID CORP. ATENDIENDO A LO ORDENADO EN EL AUTO DE

FECHA 8 DE NOVIEMBRE DE 2021 POR EL JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ, DENTRO DEL PROCESO DE PRUEBA EXTRAPROCESAL BAJO EL RADICADO NÚMERO 11001310301920200033900, EL CUAL SE ASEGURA EN IMAGEN FORENSE PARA POSTERIOR PROCESAMIENTO Y APLICACIÓN DE PROTOCOLO DE GESTIÓN DE EVIDENCIAS APORTADO POR MAPFRE PARA ESTE PROCESO (PALABRAS DE INCLUSIÓN Y EXCLUSIÓN)
Investigador: ADALID CORP. S.A.S. - Héctor Alberto DUSSAN MONTOYA
Notas: NA

Information for
I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad1:
[Custom Content Sources]
K::K:\ | ANRINCO | *(Comodín,Tener en cuenta el uso de mayúsculas/minúsculas,Incluir subdirectorios)
[Computed Hashes]
MD5 checksum: b579effd896fb4f8c349e6490dc95a5f
SHA1 checksum: d608596c5fd7c32134969a1d9903f3a1ea837d62

Image information:
Acquisition started: Fri Dec 17 10:24:34 2021
Acquisition finished: Fri Dec 17 11:14:57 2021
Segment list:

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad1

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad2

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad3

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad4

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad5

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad6

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad7

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad8

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad9

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad10

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad11

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad12

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad13

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad14

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad15

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad16

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad17

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad18

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad19

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad20

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad21

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad22

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad23

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad24

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad25

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad26

I:\EVIDENCIA_MAPFRE_2\19.ANRINCO\IMAGENFORENSE_PST_ANRINCO_MAPFRE_17DIC2021.ad1.ad27

Image Verification Results:
Verification started: Fri Dec 17 11:14:57 2021
Verification finished: Fri Dec 17 11:28:33 2021
MD5 checksum: b579effd896fb4f8c349e6490dc95a5f : verified
SHA1 checksum: d608596c5fd7c32134969a1d9903f3a1ea837d62 : verified

Registro de Imagen Forense de tipo lógico con resultado satisfactorio

Esta imagen forense es almacenada en un disco duro marca **WESTERN DIGITAL,** identificado con número de serie **WD-WCAZA4915847**, con capacidad de almacenamiento de **2000GB**, el cual se encuentra debidamente sanitizado, tal como se muestra a continuación:



	
Fotografía Disco duro de para almacenamiento de Imagen forense (Vista superior)	Fotografía disco duro utilizado (Vista posterior)

Posteriormente, con la ayuda de una de las herramientas forenses automatizadas más reconocidas a nivel mundial - FTK (Forensic Tool Kit) Versión 7.2, se analizó la totalidad de la evidencia digital del buzón de correo electrónico "**anrinco@mapfre.com.co.**" asignado a **Andrés Alfonso RINCON** para el cumplimiento de sus funciones, prestando mayor atención a la información suministrada a través del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** Con este software forense se logra recuperar, identificar, asegurar, indexar y presentar los datos basados en las solicitudes o requerimientos realizados, esto por medio de la búsqueda avanzada de palabras claves y por el filtro de datos hecho por ADALID.



Ilustración 203 Impresión de pantalla de la ejecución de software forense FTK Versión 7.2
Fuente: El presente estudio.

ANÁLISIS BUZÓN DE CORREO ELECTRÓNICO ANRINCO@MAPFRE.COM.CO."

A continuación, se detalla la capacidad del medio de almacenamiento y /o contenedor de evidencia digital suministrado en las oficinas MAPFRE SEGUROS GENERALES DE COLOMBIA S.A. para la cuenta de correo electrónico anrinco@mapfre.com.co asignada Andrés Alfonso RINCON para el desarrollo de sus funciones.

ID	Propietario del contenido	Tipo de medio de origen	Asignado a	Formato	Tamaño GB
19	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.	Buzón de correo electrónico	Andrés Alfonso RINCON → anrinco@mapfre.com.co	ad1	55.6 GB
TOTAL					**55.6 GB**

Tabla 40 Detalle del buzón de correo electrónico asignado anrinco@mapfre.com.co
Fuente: El presente estudio

La evidencia objeto de estudio contenida en el del buzón de correo electrónico anrinco@mapfre.com.co asignado a Andrés Alfonso RINCON para el desarrollo de sus funciones **aloja** un total de **55.6 GB**, dentro de este espacio el laboratorio de informática forense logró hallar un total de **Ciento**

treinta y nueve mil cuatrocientos sesenta y siete (139.467) archivos (incluyendo carpetas), como se observa a continuación.

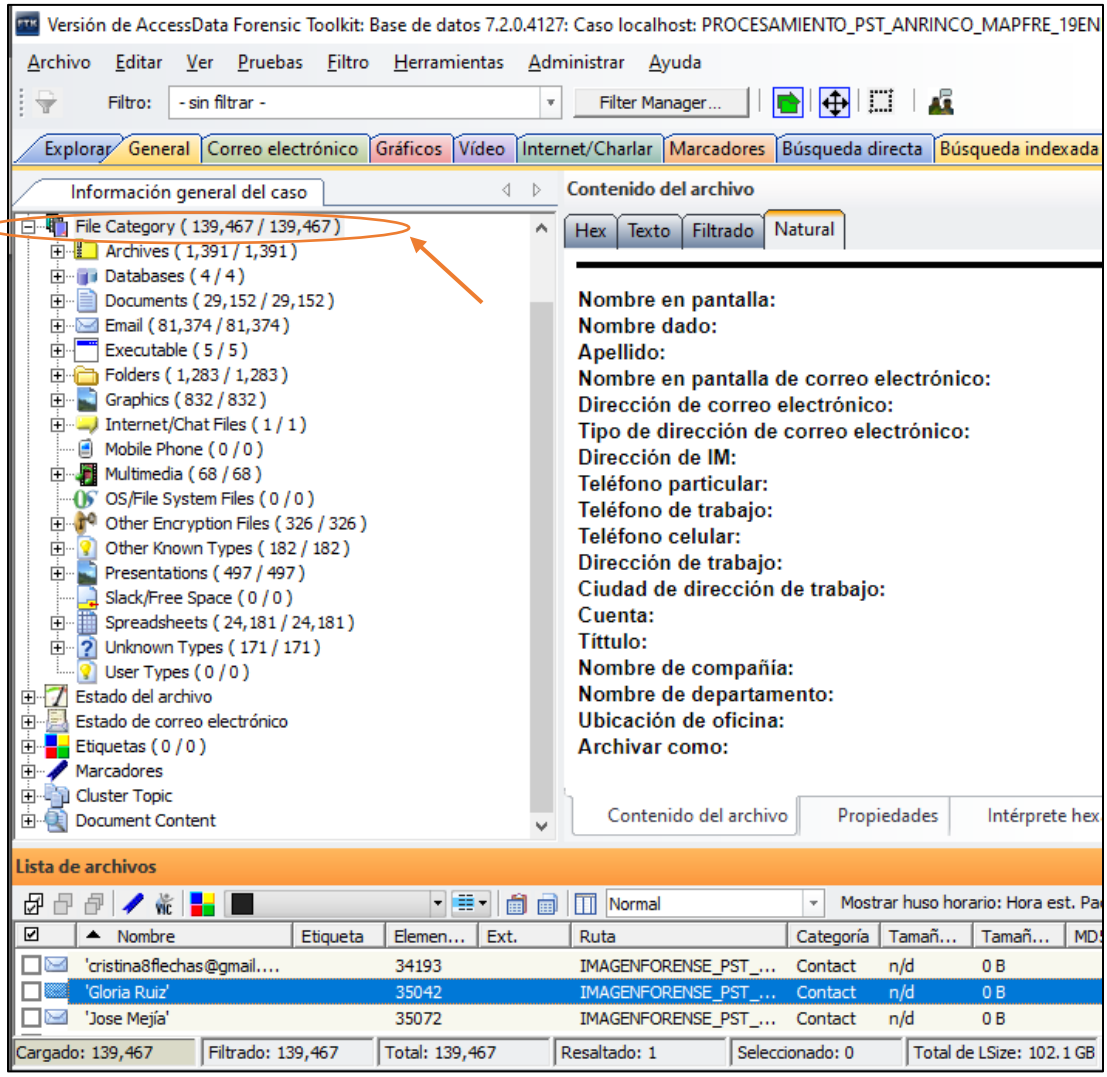


Ilustración 204 Total de archivos de la evidencia recolectado en la cuenta de correo electrónico anrinco@mapfre.com.co.

RECUPERACIÓN DE DATOS EN EL BUZÓN DE CORREO ELECTRÓNICO ANDRÉS ALFONSO RINCON → ANRINCO@MAPFRE.COM.CO.

El proceso de recuperación de datos es un proceso avanzado de un laboratorio de informática forense donde se reconstruye información eliminada y/o perdida dentro de medios de almacenamientos electrónicos, en este caso se realizó para la imagen forense realizada al contenido completo del buzón de correo electrónico anrinco@mapfre.com.co asignado a Andrés Alfonso RINCON, iniciando el día el **19** de enero del 2022.

con una duración aproximada de Cinco (5) día calendario, el resultado a dicho proceso arrojó que existen **Ciento sesenta y cinco (165)** ítems en condición de "eliminados" y se reconstruyeron **cero (0)** de datos restaurados, que responden efectivamente a posibles documentos incompletos o sin formato que fueron recuperados y reconstruidos mediante la actividad conocida como "Datacarving" dentro de la totalidad de las evidencias recolectadas en el presente caso:

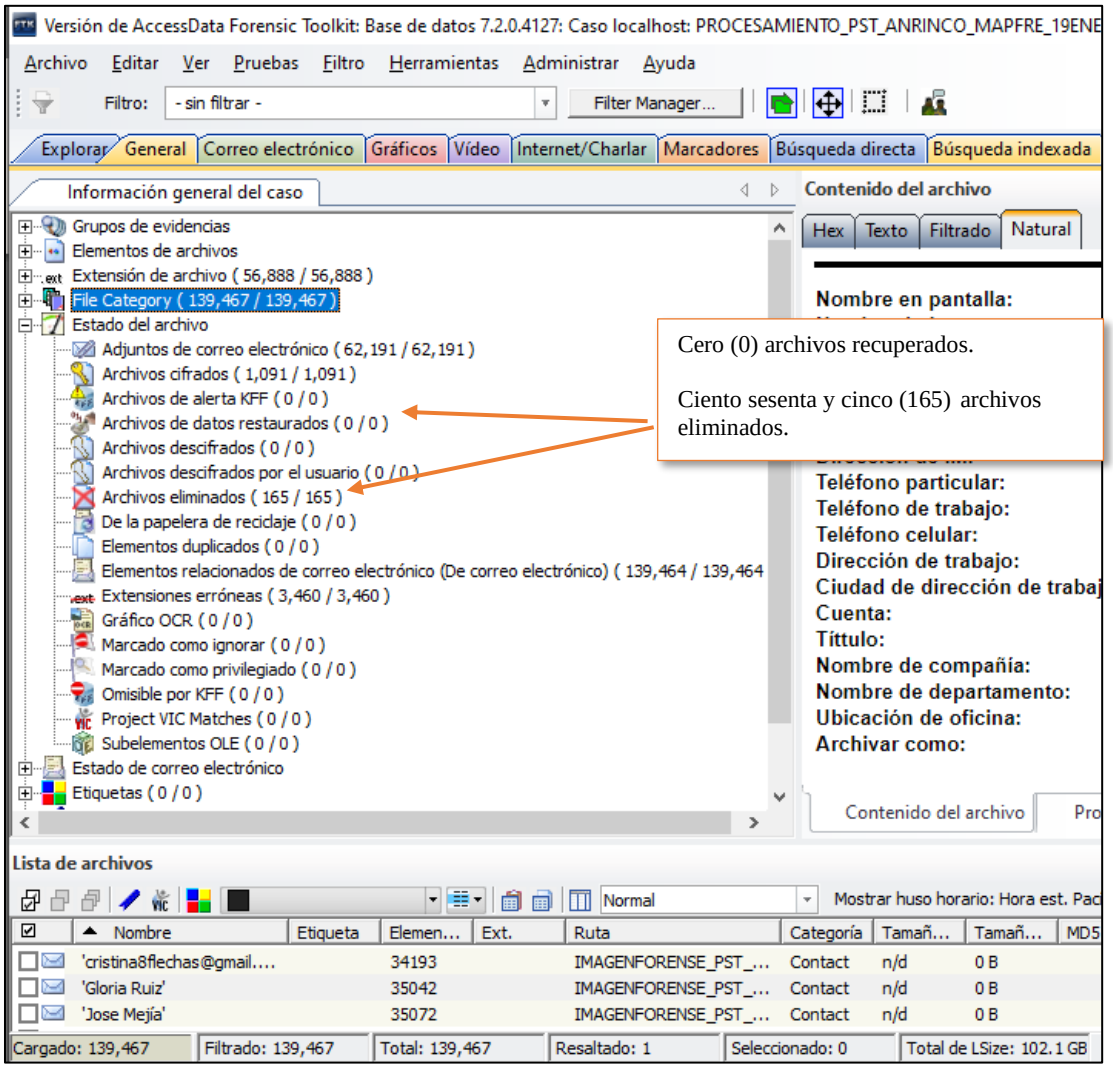


ilustración 205 Total de archivos recuperados en la cuenta de correo electrónico anrinco@mapfre.com.co.

Después de terminar con el proceso de recuperación se procedió con la identificación de todos y cada uno de los archivos contenidos en la evidencia recolectada en las instalaciones de oficinas **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**, es decir, se obtuvo la huella digital HASH MD5 y SHA1 para **Ciento treinta y nueve mil cuatrocientos sesenta y siete (139.467)**

archivos (entre activos y recuperados), este dato acompañará al archivo digital cuando este se requiera.

RESULTADOS A LAS BÚSQUEDAS EN EVIDENCIA RECOLECTADA EN LAS OFICINAS DE MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., CUENTA DE CORREO ELECTRÓNICO ANRINCO@MAPFRE.COM.CO.

luego de realizar un proceso detallado de búsqueda y filtrado de información digital sobre la cuenta de correo electrónico anrinco@mapfre.com.co asignado a **Andrés Alfonso RINCON** para el desarrollo de sus funciones, se obtienen los siguientes resultados:

#	Categoría del archivo	# de hallazgos
1	Archivos Comprimidos	1391
2	Bases de Datos	4
3	Documentos	29.152
4	Correo Electrónico	81.374
5	Ejecutables	5
6	Carpetas	1.283
7	Gráficos	832
8	archivos de internet/chat	1
9	Multimedia	68
10	Otros archivos encriptados	326
11	Otros archivos desconocidos	182
12	Presentaciones	497
13	Hojas de cálculo	24.181
14	Tipos de archivos desconocidos	171
TOTAL		**139.467**

Tabla 41 Información buscada evidencia 019_ANRINCO, hallada y filtrada conforme a lo ordenado.

Como se observa en la anterior tabla, el número de hallazgos es considerablemente alto al número de archivos originalmente recaudados, es decir el resultado a las búsquedas ejecutadas es de **Ciento treinta y nueve mil cuatrocientos sesenta y siete (139.467).**

Cabe resaltar que fueron encontrados más archivos teniendo en cuenta los procesos de recuperación y análisis previamente indicados, sin embargo y de manera posterior ADALID CORP gracias a las herramientas especializadas propias de un Laboratorio de Informática Forense, realizó un proceso de depuración de datos a fin de eliminar archivos corruptos o que no sean

legibles, archivos **duplicados**, falsos positivos (como archivos de tipo desconocido), archivos con tamaño cero, entre otros.

Los resultados a las búsquedas realizadas son:

- Los archivos de correo electrónico recuperados **Sesenta y dos mil ciento noventa y un (62.191) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos cifrados recuperados **Mil noventa y un (1.091) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Los archivos de datos Eliminados **Ciento sesenta y cinco (165) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Tipo elementos relacionados de correo electrónico **Ciento treinta y nueve mil cuatrocientos sesenta y cuatro (139.464) archivos de datos obtenidos** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.
- Archivos de datos tipo extensión errónea **Tres mil cuatrocientos sesenta (3.460) archivos de datos recuperados** por el proceso forense realizado en el Laboratorio de Informática Forense de ADALID CORP.

Una vez terminada la identificación de los datos procesados para el buzón de correo electrónico anrinco@mapfre.com.co asignado a **Andrés Alfonso RINCON** para el desarrollo de sus funciones el equipo de ADALID CORP procede a aplicar filtros para excluir la información que no se requiere de la siguiente manera:



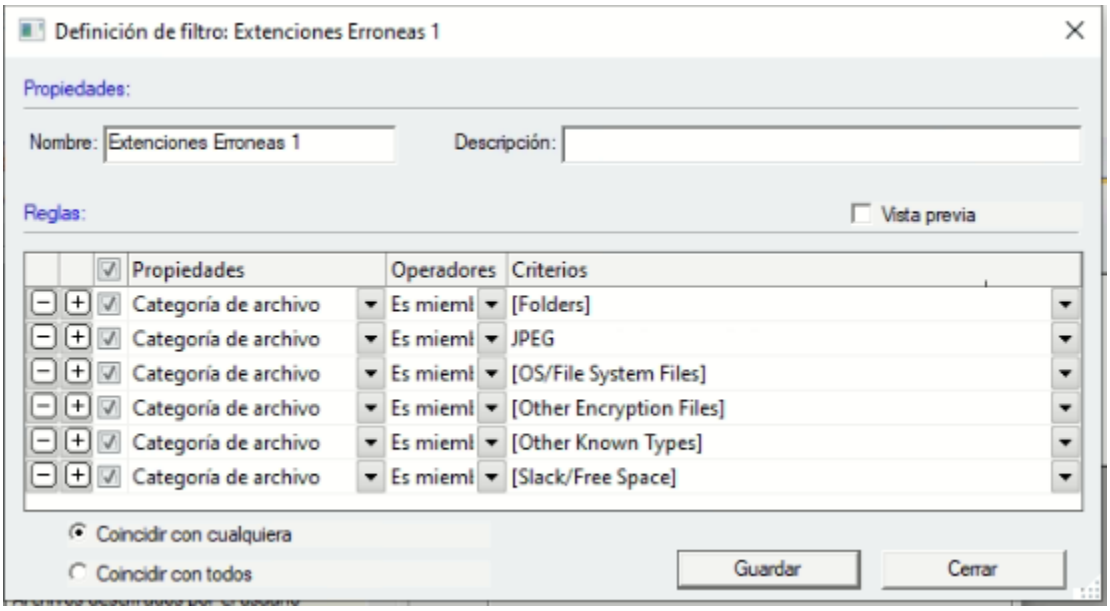


Ilustración 206 Filtro para excluir las extensiones erróneas.

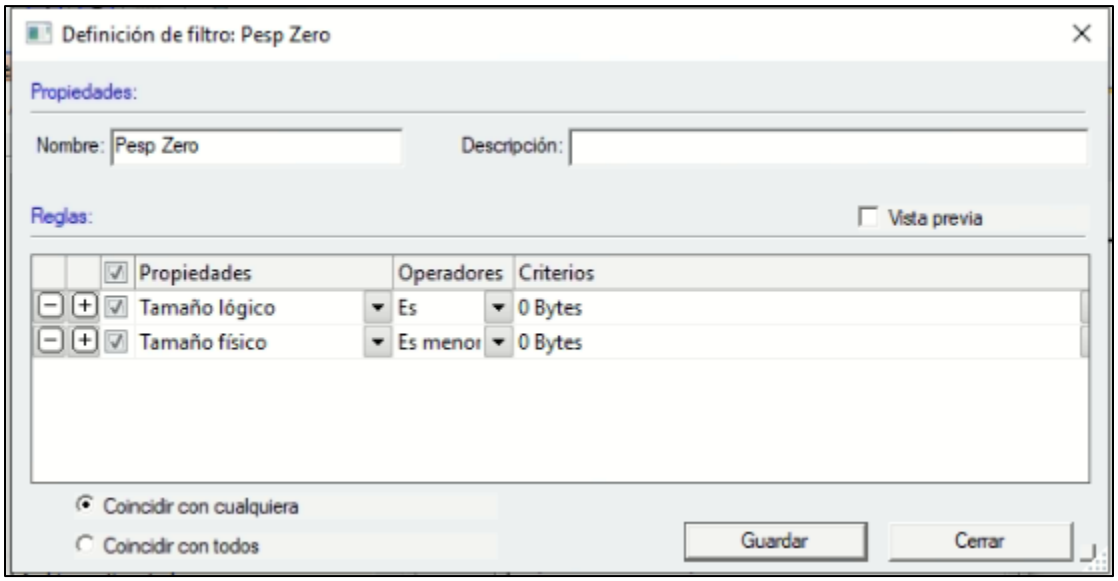


Ilustración 207 filtro para excluir los archivos de tamaño físico o lógico igual a 0.

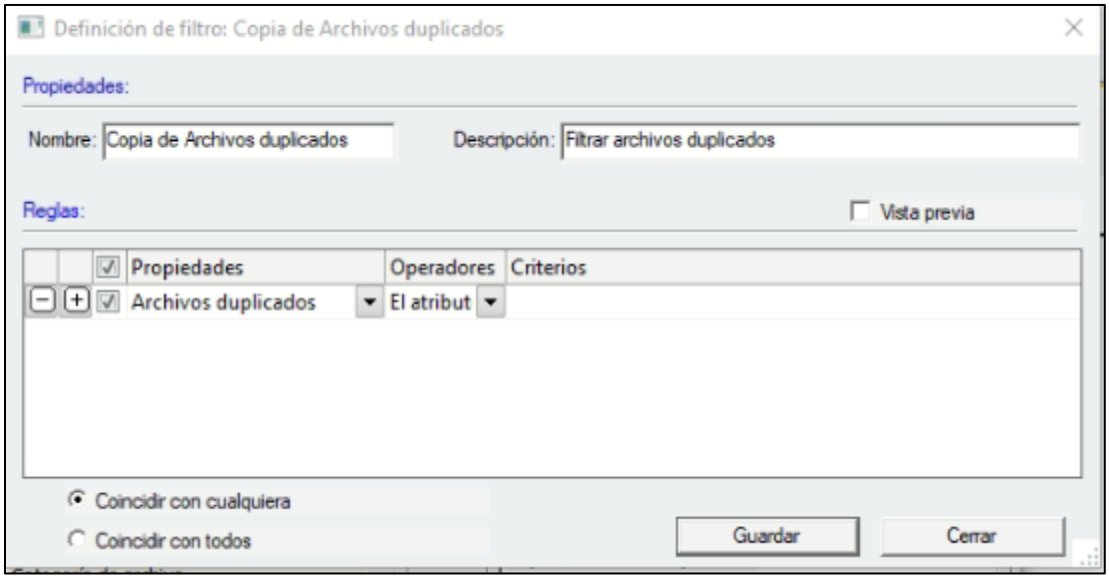


Ilustración 208 Filtro para excluir los archivos duplicados.

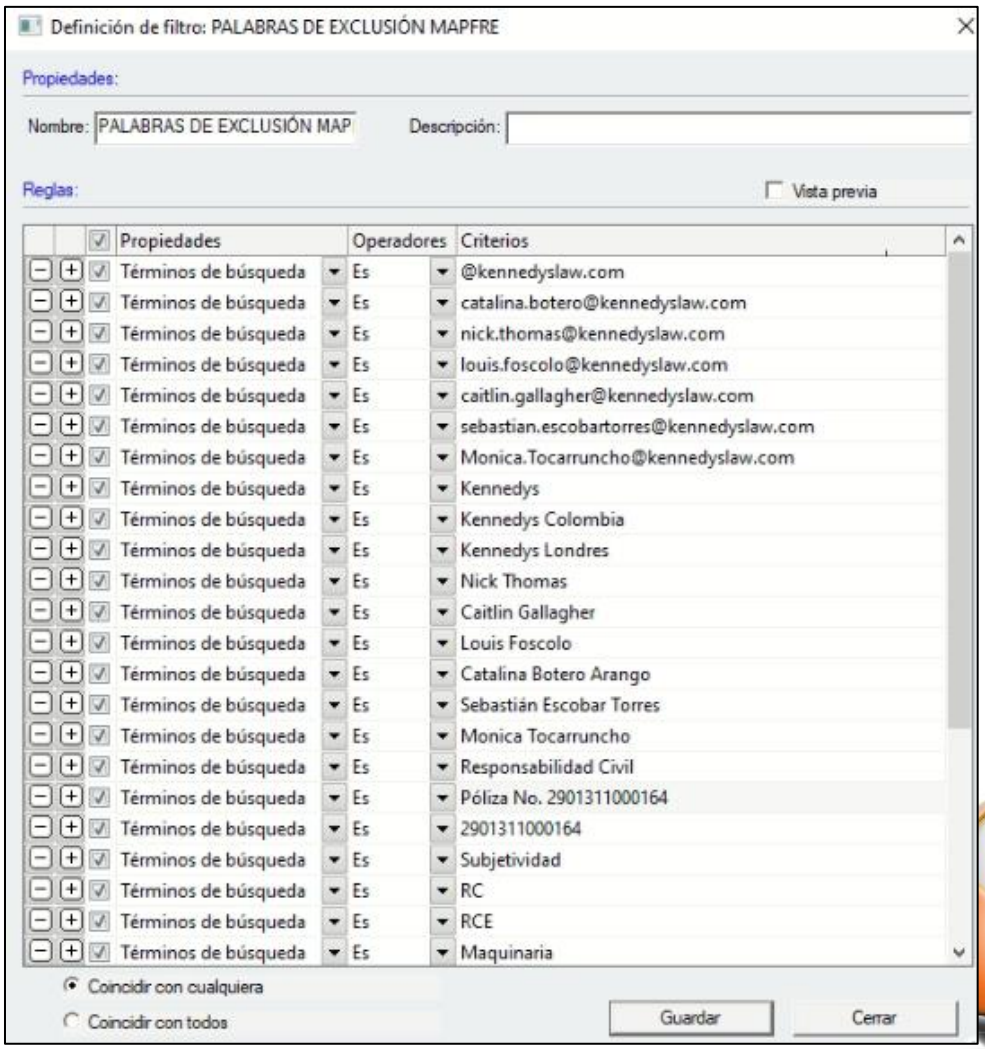


Ilustración 209 Filtro para excluir los archivos suministrado por MAPFRE - 1.

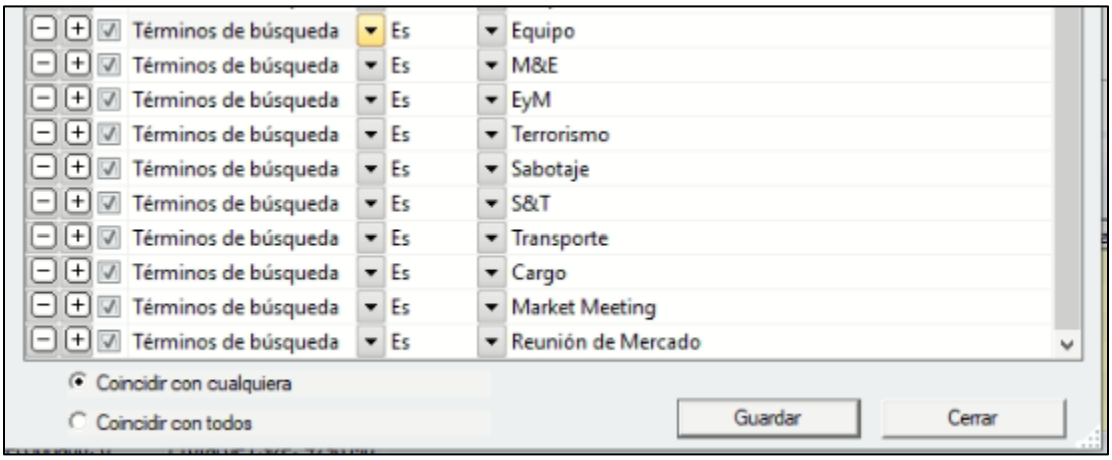
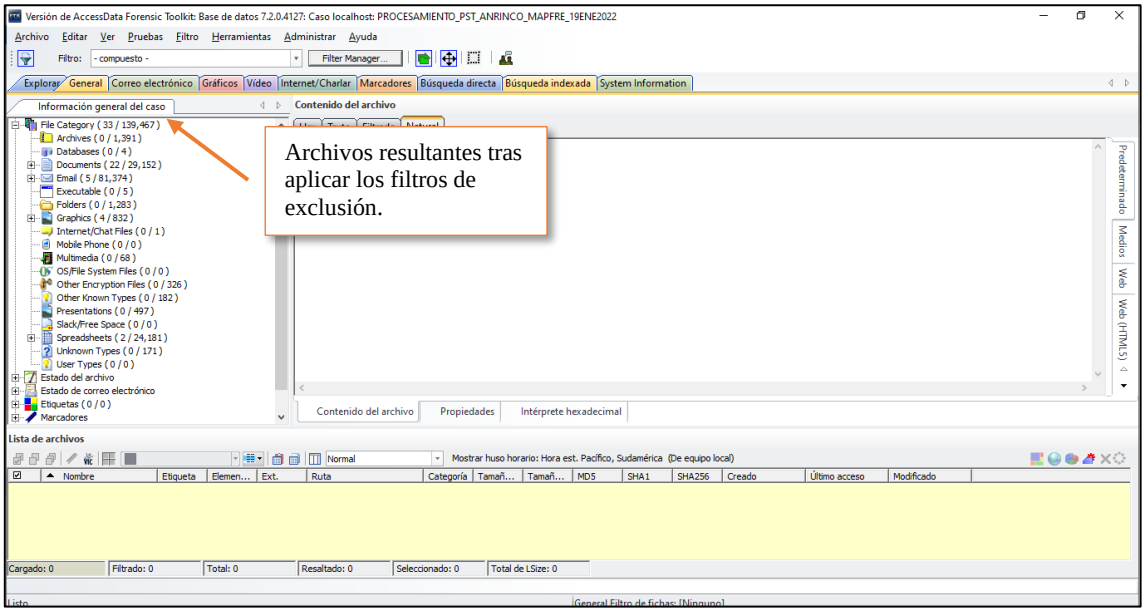


Ilustración 210 Filtro para excluir los archivos suministrado por MAPFRE - 2.

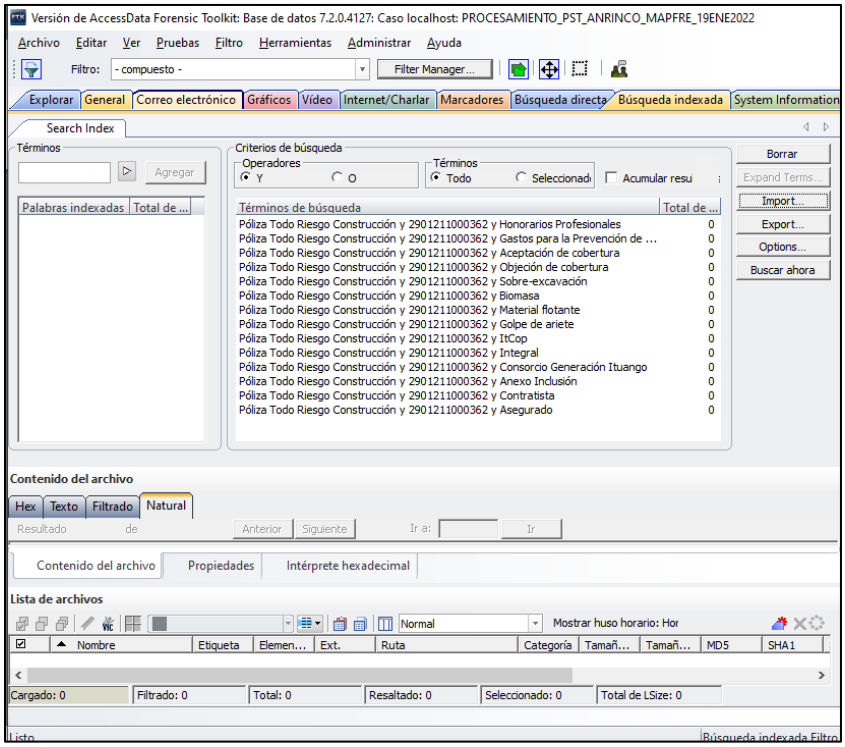
Tras aplicar los filtros de exclusión de información anteriormente mencionados, se logra reducir muestra de información a **Treinta y tres (33)** registros como se observa en la siguiente imagen:



Después, el equipo de ADALID CORP. aplica las palabras clave sobre la evidencia las cuales fueron tomadas del protocolo de gestión de evidencias aportado por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** las cuales fueron aplicadas y cargadas en la herramienta en la herramienta FTK Versión 7.2 a través de la pestaña de búsqueda del aplicativo, los filtros de información realizados en el aplicativo fueron los siguientes:

IDENTIFICADOR	FILTROS APLICADOS
FILTRO 1	Póliza Todo Riesgo Construcción y 2901211000362 y Honorarios Profesionales
FILTRO 2	Póliza Todo Riesgo Construcción y 2901211000362 y Gastos para la Prevención de Pérdidas
FILTRO 3	Póliza Todo Riesgo Construcción y 2901211000362 y Aceptación de cobertura
FILTRO 4	Póliza Todo Riesgo Construcción y 2901211000362 y Objeción de cobertura
FILTRO 5	Póliza Todo Riesgo Construcción y 2901211000362 y Sobre-excavación
FILTRO 6	Póliza Todo Riesgo Construcción y 2901211000362 y Biomasa
FILTRO 7	Póliza Todo Riesgo Construcción y 2901211000362 y Material flotante
FILTRO 8	Póliza Todo Riesgo Construcción y 2901211000362 y Golpe de ariete
FILTRO 9	Póliza Todo Riesgo Construcción y 2901211000362 y ItCop
FILTRO 10	Póliza Todo Riesgo Construcción y 2901211000362 y Integral
FILTRO 11	Póliza Todo Riesgo Construcción y 2901211000362 y Consorcio Generación Ituango
FILTRO 12	Póliza Todo Riesgo Construcción y 2901211000362 y Anexo Inclusión
FILTRO 13	Póliza Todo Riesgo Construcción y 2901211000362 y Contratista
FILTRO 14	Póliza Todo Riesgo Construcción y 2901211000362 y Asegurado

Los resultados de la aplicación de los filtros se observan en la siguiente imagen:



Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para el buzón de anrinco@mapfre.com.co asignado a **Andrés Alfonso RINCON** para el desarrollo de sus funciones.

CONCLUSIONES.

- Se identificaron, adquirieron, recolectaron, preservaron y analizaron satisfactoriamente diez y nueve (19) imágenes forenses adquiridas dentro de las instalaciones de **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A**,., atendiendo a lo ordenado en el auto de fecha 8 de noviembre de 2021 por el juzgado 19 civil del circuito de Bogotá, dentro del proceso de prueba extraprocesal bajo el radicado número 11001310301920200033900, el cual se asegura en imagen forense para posterior procesamiento y aplicación de protocolo de gestión de evidencias aportado por MAPFRE para este proceso (palabras de inclusión y exclusión)., información toda puesta a disposición de los peritos designados por ADALID CORP, que fungieron como apoyo técnico-pericial a la diligencia ordenada por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**

- Tras realizar el filtrado de información para cada uno de los Diez y Nueve (19) buzones de correo entregados en las instalaciones de

MAPFRE SEGUROS GENERALES DE COLOMBIA S.A., el equipo de ADALID CORP no identifico datos asociados posteriores.

- No se halló evidencia de fallas en la integridad de datos que impidan acceder a la información contenida en los dispositivos celulares ni a ninguno de sus archivos de registros de conversaciones.

- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **7d7787982808d7be0d6baf4f87b9505a** y SHA1 **1818a0e2013e2215acf8130a1f35002f72fc48de** para el buzón de correo de AVICTOR@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **5b6abdd3129e2330f3a46cc583d004a7** y SHA1 **70e7587e2b2fac10f3c58a029e552844a8aabf49** para el buzón de correo de ACLEMEN@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **326f16dbe95b854b5fdd979f1828ab88** y SHA1 **090832e206bf6c9540fcfdad2d7d1aa1a25b74a3** para el buzón de correo de JOSPAGA@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **25137b08f6c1fc4b57519ff976b5d139** y SHA1 **d20019fe0ad8526bbac422c7b8dd475f7225e8e0** para el buzón de correo de CTORRES@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **334e31abcf31639ee1a251289be3ac33** y SHA1 **b906341ba507626503910b9f85783c073d48a96d** para el buzón de correo de DAGOMEZ@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **36a5dc50b305d9a816109d85d035ede9** y SHA1 **8734e3612bd6e58f70e833fd1a991fe5b9178b4d** para el buzón de correo de LSUAREZ@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.

- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **d534e4492f211de5338af83951c38c46** y SHA1 **9d747d52eabeadd3571ddf2033cba1cc4c2c6bd7** para el buzón de correo de ANFERAM@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **f2b048976f511d39e5985af537222dea** y SHA1 **493d58bf1f54dcc30314162538921cf1b8ac853d** para el buzón de correo de MVIVIAN@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **82febeb311661f24839ced114ce64e7b** y SHA1 **47c4c084826f4119210640aa34aae4b32068e556** para el buzón de correo de JCTORR2@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **de6744c8bb0c6717f072120e5caaa982** y SHA1 **a37b029f544c9f91919cd44368238523600bb645** para el buzón de correo de JMRIANO@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **4ca2ff21652b030e18792d53572fc81a** y SHA1 **fdf3b09289d272e99375b5a141b0617ae789e477** para el buzón de correo de JMERINE@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **31383bb73ba2962329cfe4057918b2ff** y SHA1 **d937640697a74fe39a1dabfcfeb857c096bd6b16** para el buzón de correo de ACPARRA@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **ed3b9410edd6de02fe5e441ea43ddea2** y SHA1 **91fad8664b30c42450ea5e3d4eadc83dd516faa4** para el buzón de correo de CRUZJ@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5

a6426ce7f6ca0217569271fe149bf3d7 y SHA1 **3753a9577aa74a1f04b65a301238b025bf4fd805** para el buzón de correo de ETCUBID@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.

- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **73f2e7b307c8cbe24e68fd2cd5bec944** y SHA1 **515cd0f6c475cc973c9af008a7ea79b87126ef69** para el buzón de correo de MMALAGO@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **e1f945f3d80c3fc34ba37d6f39a9f07b** y SHA1 **a5f3f5fb0bb551475a8aa9e6b136d16d0f6c28e4** para el buzón de correo de GUEVECA@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **775edcc80edc04552a83d75e90da2aac** y SHA1 **fab4be9073e47a100aaedfcbec42de7fffa2443f** para el buzón de correo de ROCARRE@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **ec0267c1a3ffa7b40f2a9d9b6c1bbcc0** y SHA1 **b5e7ea4b96117e879d13928e2dc3da51aa6c4089** para el buzón de correo de CSALINA@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.**A ADALID CORP.
- De esta información se obtuvo una imagen forense en formato AD1, *que se identifica con el* HASH MD5 **b579effd896fb4f8c349e6490dc95a5f** y SHA1 **d608596c5fd7c32134969a1d9903f3a1ea837d62** para el buzón de correo de ANRINCO@MAPFRE.COM.CO, Entregados Por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** A ADALID CORP.
- Tras la aplicación de los filtros de exclusión de información y las palabras clave, el equipo de ADALID CORP no identifico resultados asociados para los (19) Diez y nueve buzones de correo analizados.
- No se realizo la entrega de los siguientes buzones de correo indicando que estos no se encontraban en **COLOMBIA**.

BUZONES DE CORREO QUE NO VAN A SER ENTREGADOS DE PARTE DE MAPFRE (NO ESTÁN EN COLOMBIA)	
Nombre	**Correo electrónico**

BUZONES DE CORREO QUE NO VAN A SER ENTREGADOS DE PARTE DE MAPFRE (NO ESTÁN EN COLOMBIA)	
Luis Enrique Giraldo Durán	aquerol@mapfre.com
José Luis Cubero Rivera	jlcube@mapfre.com
Joaquín Alberto Solera	jalbertos@mapfre.com

- Se realizo el procesamiento, análisis, filtros de información y aplicación de palabras clave para los siguientes buzones de correo, lo anterior según el protocolo establecido por **MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.** con los filtros y vectores allí establecidos.

BUZONES DE CORREO ENTREGADOS POR PARTE DE MAPFRE (PROCESADOS)		
No.	**NOMBRE**	**Correo electrónico**
1	VÍCTOR JONATHAN ARELLANO CARDONA	avictor@mapfre.com.co
2	DAVID GÓMEZ JIMÉNEZ	dagomez@mapfre.com.co
3	JOSÉ MAURICIO MALAGÓN ACOSTA	mmalago@mapfre.com.co
4	JOSÉ MANUEL RIAÑO	jmriano@mapfre.com.co
5	ANTONIO CLEMENTE CAMPANARIO	aclemen@mapfre.com.co
6	ETHEL CUBIDES	etcubid@mapfre.com.co
7	ANDRÉS FELIPE RAMÍREZ	anferam@mapfre.com.co
8	CLAUDIA ROCIO SALINASI	csalina@mapfre.com.co
9	JOSÉ MANUEL MERINERO MARTIN	jmerine@mapfre.com.co
10	CARMENZA GUATAVITA TORRES	ctorres@mapfre.com.co
11	ANDRÉS ALFONSO	anrinco@mapfre.com.co
12	CARLOS ALBERTO GUEVARA MORA	gueveca@mapfre.com.co
13	VIVIANA ROCÍO MOYANO	mvivian@mapfre.com
14	ANDRÉS CAMILO PARRA BALAGUERO	acparra@mapfre.com.co
15	JUAN CAMILO TORRES LOZANO	jctorr2@mapfre.com.co
16	LUIS ALBERTO SUÁREZ URREGO	lsuarez@mapfre.com.co
17	JORGE CRUZ AGUADO	cruzj@mapfre.com.co
18	RODRIGO CARREÑO HERNÁNDEZ	rocarre@mapfre.com.co
19	JOSÉ FERNANDO PALACIO GALLÓN	jospaga@mapfre.com.co

La totalidad de las imágenes forenses contenedoras de la totalidad de la evidencia digital asegurada queda en bóveda de seguridad en las instalaciones de ADALID CORP a disposición del **JUZGADO** y cualquier decisión sobre las mismas será atendida en el menor tiempo posible.

De esa forma se rinde el presente informe de laboratorio quedando atento a cualquier inquietud o duda al mismo.

Atentamente,

rma: 526d8ec8-5255-477b-941f-49d135918194

ID Firma: b250cada-49b2-4bcd-9f64-d3b494a6e1a3

Andrés GUZMÁN CABALLERO
CEO
ADALID Corp. S.A.S.
andres@adalid.com

Endrick Dann Axel DÍAZ ORTEGA
Abogado Perito en Informática Forense
ADALID Corp. S.A.S.
axel.diaz@adalid.com

Hector Dussan

ID Firma: 5bc72cbe-4c08-4f5d-b0ac-01de6993ee8d

Héctor Alberto DUSSAN MONTOYA
Ingeniero de Laboratorio
ADALID Corp. S.A.S.
hector.dussan@adalid.com

PERFILES PROFESIONALES

ADALID CORP S.A.S.

ADALID CORP S.A.S. es la única empresa de América Latina con un equipo forense de más de 200 profesionales de todo el mundo quienes son expertos en todas las ramas de la ciencia, cuenta con dos laboratorios propios completamente dotados y especializados en el análisis de acústica e informática forenses, útiles para la extracción segura de información, toma, certificación y análisis de evidencias digitales. ADALID Corp®. no es una agencia de contacto con peritos, es un equipo que da un gran valor agregado a cualquier prueba presentada en un proceso judicial. A través de la experiencia y amplia trayectoria de más de 10 años, ADALID ha sido reconocido por haber participado en tribunales arbitrales, procesos legales civiles, laborales, administrativos, penales, comerciales, de familia y policivos, asesorando a varias firmas de abogados, reconocidas empresas y clientes, tales como: Empresa de Licores de Cundinamarca, Legislación Económica S.A.S. Legis S.A.S, Tu Boleta, Busca pé Colombia, Mcr Entertainment, Comunicaciones Regionales de Colombia, Centro Comercial Plaza de las Américas, Teleone Colombia, Comregcol, Asociación Colombiana de Ingenieros de Sistemas, Seltika, Digiware, Grupo Porcelamika Inc, Universidad Libre de Colombia, Ministerio de Hacienda y Crédito Público, Dirección Nacional de Planeación, Ministerio de Comunicaciones, Certicamara, Procuraduría General de la Nación, Roldan, Y&R, entre otros.

HOJA DE VIDA ADALID CORP S.A.S:
https://adalid-my.sharepoint.com/:f:/p/comercial/Es-PpkL8y1JAqb9xYlVKSo0BtklTnc4CHyKoZI9sypRE6Q?e=RA9NBc

Andrés GUZMÁN CABALLERO
CEO

Abogado Experto en Nuevas Tecnologías Aplicadas al Derecho. Magister Executive en Administración de Empresas y Liderazgo Estratégico, Cybercrime and Electronic Evidence, Perito and honorem en evidencias digitales, Perito en casos de E-evidence y crimen informático, Especialización en Derecho Administrativo, Diplomado en Internet, Comercio electrónico y su regulación, Docente de Postgrados, director de la Maestría de Protección de Datos de la Universidad Sergio Arboleda.

Endrick Dann Axel DÍAZ ORTEGA
Perito en Informática Forense

Abogado con Major en Economía de la Universidad Sergio Arboleda, Especialista en Seguridad de la Información e Informática de la misma Universidad, AccessData Certified Examiner v6 y cursos en: Técnicas Antiforenses del Centro Internacional de Excelencia Sergio Arboleda (España), Computer Hacking Forensics Investigator V9 del EC-Council, Introduction to Cyber Security de Cisco Networking Academy, Blockchain – Creación de Contratos Inteligentes de la Universidad Nacional de Colombia y Lean Six Sigma (Yellow, Green y Black Belt) de la Universidad Sergio Arboleda, entre otros.

Cuenta con más de siete años de experiencia en asuntos de Pericias en Informática Forense, Protección de Datos Personales, Derecho al olvido, Derecho Informático, Propiedad Intelectual y Seguridad de la Información e Informática.

Héctor Alberto DUSSAN MONTOYA (ingeniero de laboratorio)

Perito en Informática Forense.

Ingeniero de sistemas de la UNIVERSIDAD FRANCISCO JOSÉ DE CALDAS, con más de (2) años de experiencia en Seguridad de Informática y asuntos relacionados con Informática Forense en el sector privado, cuenta con una certificación AccessData Certified Examiner v6 y cursos en: Introduction to Cyber Security de Cisco Networking Academy, Cybersecurity Essentials de Cisco Networking Academy.



GLOSARIO

Archivo:

Una colección de datos almacenados en un disco bajo un formato específico e identificado con un nombre y una extensión.

Asegurar:

Es el proceso en el que se preserva la integridad de las Pruebas Electrónicas. En esta etapa nos aseguramos de que no se rompa la cadena de custodia de las pruebas.

A partir de los medios originales se crea la imagen forense, es decir, una copia exacta bit a bit del medio original.

Desde este momento el examinador trabajará única y exclusivamente sobre la imagen forense.

Bit:

Unidad mínima de información cuyo valor puede ser cero o uno.

Byte:

Conjunto de 8 bits que suele representar el valor asignado a un carácter. Puede tomar valores entre 0 y 255.



Búsqueda por palabra clave:

Es una búsqueda de documentos que contienen una o más palabras que vienen especificadas por el usuario y cuyo objetivo es limitar el número de documentos que se deben revisar en busca de información relevante para un caso.

Cadena de custodia:

Es el conjunto de acciones, medidas logísticas y los actores partícipes que, fehacientemente registrados en un informe, garantizan la salvaguarda de la identidad e integridad de los medios digitales que van a ser analizados.

Computer Forensic:

El Computer Forensic es el proceso de identificar, asegurar, extraer y presentar pruebas que hayan sido generadas electrónicamente y guardadas en medios de almacenamiento digital con el objetivo de que sean aceptadas en un proceso judicial.

Datos activos:

Son los archivos y carpetas que residen en las unidades de almacenamiento de los sistemas informáticos y que son accesibles y visibles para los usuarios de una forma inmediata y directa a través de las herramientas propias del sistema operativo.

Datos borrados:

Los datos borrados son archivos o carpetas que existieron en el ordenador en el pasado como datos activos y que, posteriormente, han sido borrados por el sistema operativo o el usuario final. Los datos borrados permanecerán en la unidad de almacenamiento hasta que sean sobrescritos por otro archivo.

Datos recuperados:

Es el término que identifica las carpetas y/o archivos recuperados o reconstruidos que habían sido eliminados de la zona de datos activos. Estos archivos pueden ser recuperados con su formato y tamaño original o en pequeños fragmentos, que necesitarán una labor de reconstrucción forense.

Datos en zonas sin usar / sin asignar:

Datos que en la actualidad residen en zonas del disco que no pertenecen a ningún fichero. Son restos digitales de documentos que fueron eliminados.

Datos en zonas slack:

Debido a la necesidad del ordenador de asignar el espacio de disco en bloques de tamaño fijo, hay una zona al final de cada fichero que, a pesar de estar asignada al fichero en sí, contiene información que no pertenece al mismo. Esta zona se llama "slack" y contiene información del contenido

que hubo en ese bloque del disco antes de que se asignase al nuevo fichero.

Digitalizar:

Almacenar información electrónica como una cadena de "unos" y "ceros".

Debido a que tanto "ceros" como "unos" pueden ser fácilmente representados por dos niveles voltaicos en un medio electrónico, el sistema de numeración binario es ampliamente utilizado en el mundo informático digital.

Dirección IP:

Cadena de cuatro números separados por puntos que se utilizan para representar e identificar a un ordenador en Internet.
Los ISP asignan estas IP's automáticamente cuando nos conectamos a Internet.

Disco duro:

Disco de metal cubierto con una superficie de grabación ferro magnética. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.

DVD:

Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

Entorno virtual:

Es la simulación computacional de un entorno de trabajo formado por la interconexión de múltiples ordenadores, el cual permite el acceso a información digitalizada independientemente de la ubicación física donde ésta se encuentre.

Extensión de un archivo:

Etiqueta habitualmente de longitud 3, precedida por un punto que identifica el formato del archivo de datos o la aplicación utilizada para modificarlo.

Extraer:

Es el proceso en el que se revisa y analiza la información con el objetivo de extraer las pruebas. Al trabajar sobre la imagen forense y no directamente sobre el medio original, nos aseguramos de que se conserva la integridad de las pruebas mientras éstas son examinadas.

Hash:

Es un código calculado matemáticamente basándose en el contenido de un mensaje o archivo. Este código tiene la propiedad que se trata de un

valor específico para un mensaje o archivo, para así demostrar que no ha sido modificado. Si un mensaje u archivo se modificará, entonces su hash habría cambiado, y ya no coincidiría con el valor hash original.

HTML (Hypertext Markup Language):

Lenguaje usado para escribir documentos para servidores World Wide Web. Es una aplicación de la ISO Standard 8879:1986.

HTTP (Hypertext Transfer Protocol):

HTTP es un protocolo con la agilidad y velocidad necesaria para distribuir y manejar sistemas de información multimedia sobre Internet. Una característica de HTTP es la independencia en la visualización y representación de los datos, permitiendo a los sistemas ser construidos independientemente del desarrollo de nuevos avances en la representación de los datos.

HTTPS:

Protocolo http seguro. Sus dos principales características son el cifrado y la autenticación.

Mediante el cifrado, ocultamos el contenido de las comunicaciones con el servidor a la vista de terceros. La autenticación permite a los usuarios saber que el servidor es quien dice ser a través del uso de certificados firmados por Autoridades de Certificación.
Identificar:



El proceso de identificación implica analizar dónde y cómo han sido creadas y almacenadas las pruebas y en qué sistema o sistemas residen.

A partir de esta información el investigador será capaz de seleccionar los métodos de recuperación más adecuados y qué herramientas deberán ser utilizadas para capturar los medios involucrados de una forma segura.

Imagen forense:

Es una copia exacta (bit a bit) de la unidad de almacenamiento de un sistema informático utilizada en una investigación forense.

Ingeniería Inversa:

Consiste en el análisis del código binario de un programa o aplicación para determinar su comportamiento real.

Internet:

Red global de datos basada en los protocolos TCP/IP que se utiliza para interconectar ordenadores y como medio de transporte de diversos servicios, siendo los más populares los servicios de e-mail, www y ftp.

ISP (Internet Service Provider):

Organización que provee la conexión de ordenadores a Internet, ya sea por líneas dedicadas o por líneas conmutadas. Es una entidad, habitualmente con ánimo de lucro, que además de dar acceso a Internet a personas físicas y/o jurídicas, puede ofrecerles una serie de servicios

(hospedaje de páginas web, consultoría de diseño, implantación de webs e Intranets, etc.).

Log:

Registro de determinados eventos generados por el sistema operativo, o por una aplicación, sobre un período de tiempo dado. Pueden ser utilizados por auditores externos para registrar/reconstruir el uso de un ordenador o aplicación.

Malware:

Término genérico usado para abarcar al software malicioso incluyendo: adware, troyanos, browser hijackers, keyloggers, dialers, tracking cookies, entre otros.

MD5:

Es un tipo de Hash que sirve para dar seguridad de que un archivo no se ha alterado, La codificación del MD5 es de 128 bits y es representada como un número de 32 dígitos hexadecimales.

Metadatos:

Los metadatos son información sobre un conjunto de archivos y/o carpetas que pueden describir, por ejemplo, cómo, cuándo y por quién ha sido creado, recibido, accedido y/o modificado. Estos datos se utilizan en Computer Forensic para reconstruir la cadena de acontecimientos asociada al fichero analizado.

Dependiendo del contexto en el que se emplee el término, se hace referencia a unos o a otros datos.

Presentar:

Es la etapa final del proceso en la que se presentan las pruebas de forma comprensible a interlocutores que no necesariamente tengan conocimientos de informática.

Durante esta etapa, se vinculan las pruebas digitales con el resto de las pruebas que componen el caso para reforzar al máximo la estrategia legal planteada.

Prueba Electrónica:

Información almacenada o transmitida en formato digital aceptada en un proceso judicial. Es necesario obtener la información siguiendo unos procedimientos muy concretos con personal especializado y operando dentro de un marco legal adecuado para garantizar que las pruebas sean aceptadas en juicio.

Rastros digitales:

Los rastros digitales son huellas electrónicas que vamos dejando al utilizar servicios informáticos o de comunicaciones.



RAW:

El formato RAW, cuya traducción literal del inglés al español significa: crudo, es un formato de archivos digitales, que contiene la totalidad de los datos desde el primer bit hasta el último bit del medio de almacenamiento al cual se le hace la copia, este formato no es compreso.

Router:

Elemento que determina la trayectoria o transferencia más eficiente de datos entre dos segmentos de la red. Opera mediante el uso de tablas y protocolos de enrutamiento.

Screenshot:

Es una captura de pantalla o también llamado: "pantallazo", es una imagen capturada por un equipo de cómputo, para registrar o documentar, los elementos visibles en el monitor u otro dispositivo de salida visual.

SHA1:

Es un tipo de Hash que sirve para dar seguridad de que un archivo no se ha alterado, La codificación del SHA1 es de 160 bits y es representada como un número de 40 dígitos hexadecimales.

Spam:



Envío masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico.

Spoofing:

Procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente con el fin de engañar a un firewall.

TCP / IP Transmission Control Protocol / Internet Protocol:

Conjunto de protocolos que definen las reglas básicas de comunicación entre ordenadores dentro de Internet.

Troyano:

Es un tipo de software malicioso o spyware (también son conocidos como caballos de Troya) pueden ingresar al sistema, instalarse y ejecutarse sin el conocimiento del usuario, son capaces de realizar una gran variedad de tareas, entre las más conocidas: abrir puertos para futuros ingresos sin autorización, robar datos sensibles financieros, bancarios o personales; una particularidad y diferencia con otros tipos de Malware, es que no pueden replicarse ellos mismos.

Virus:

Programa que puede infectar otros programas, modificándolos para incluir una copia de sí mismo. Los virus tienen básicamente la función de propagarse, replicándose, pero algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta

realizar daños importantes en los sistemas. Este tipo de programas pueden actuar de diversas maneras:

a) Solamente advertir al usuario de su presencia, sin causar daño aparente.
b) Tratar de pasar desapercibidos para causar el mayor daño posible.
c) Adueñarse de las funciones principales (infectar los archivos de sistema).

Virus de Macro:

Es la última presentación de los virus. Viajan en archivos de aplicación (Word, Excel, etc.) y no en archivos binarios (como lo hacen los virus tradicionales). Se ejecutan al abrir el fichero de datos que los contiene.

Virus en correo electrónico:

Los virus no pueden viajar en mensajes de correo electrónico, ya que únicamente utilizan el formato de 7 bits para transferir texto. La única manera en que pueden viajar es por archivos binarios que se envían mediante un anexo (attachment) al mensaje de texto. Es recomendable revisar estos archivos con un antivirus antes de su lectura.

Warez:

Copias piratas de los programas. Versiones de software protegido a las que se ha retirado fraudulentamente la protección.

WWW (World Wide Web):



Es el conjunto de todos los ordenadores que están conectados en red y que forman lo que se conoce como Internet.



EN CUMPLIMIENTO AL ARTÍCULO 226 Y SS DEL CGP

1. **La identidad de quien rinde el dictamen y de quien participó en su elaboración.**

ADALID CORP S.A.S. Nit. 900.095.522-5, en su nombre Endrick Dann Axel DÍAZ ORTEGA identificado con cédula de ciudadanía No. 1.016.036.658 y Héctor Alberto DUSSAN MONTOYA identificado con cédula de ciudadanía 1.026.260.827 de Bogotá.

2. **La dirección, el número de teléfono, número de identificación y los demás datos que faciliten la localización del perito.**

Dirección: Calle 70A # 11 – 28 Barrio Quinta Camacho, Bogotá D.C., Colombia
Teléfonos: +57 (1) 7432015, +57 3173677051.
Contacto: info@adalid.com
Web: www.adalid.com

3. **La profesión, oficio, arte o actividad especial ejercida por quien rinde el dictamen y de quien participó en su elaboración. Deberán anexarse los documentos idóneos que lo habilitan para su ejercicio, los títulos académicos y los documentos que certifiquen la respectiva experiencia profesional, técnica o artística.**



ADALID CORP S.A.S.

ADALID CORP S.A.S. es la única empresa de América Latina con un equipo forense de más de 200 profesionales de todo el mundo quienes son expertos en todas las ramas de la ciencia, cuenta con dos laboratorios propios completamente dotados y especializados en el análisis de acústica e informática forenses, útiles para la extracción segura de información, toma, certificación y análisis de evidencias digitales. ADALID Corp®. no es una agencia de contacto con peritos, es un equipo que da un gran valor agregado a cualquier prueba presentada en un proceso judicial. A través de la experiencia y amplia trayectoria de más de 10 años, ADALID ha sido reconocido por haber participado en tribunales arbitrales, procesos legales civiles, laborales, administrativos, penales, comerciales, de familia y policivos, asesorando a varias firmas de abogados, reconocidas empresas y clientes, tales como: Empresa de Licores de Cundinamarca, Legislación Económica S.A.S. Legis S.A.S, Tu Boleta, Busca pé Colombia, Mcr Entertainment, Comunicaciones Regionales de Colombia, Centro Comercial Plaza de las Américas, Teleone Colombia, Comregcol, Asociación Colombiana de Ingenieros de Sistemas, Seltika, Digiware, Grupo Porcelamika Inc, Universidad Libre de Colombia, Ministerio de Hacienda y Crédito Público, Dirección Nacional de Planeación, Ministerio de Comunicaciones, Certicamara, Procuraduría General de la Nación, Roldan, Y&R, entre otros.

Andrés GUZMÁN CABALLERO
CEO

Abogado Experto en Nuevas Tecnologías Aplicadas al Derecho. Magister Executive en Administración de Empresas y Liderazgo Estratégico, Cybercrime and Electronic Evidence, Perito ad honorem en evidencias digitales, Perito en casos de E-evidence y crimen informático, Especialización en Derecho Administrativo, Diplomado en Internet, Comercio electrónico y su regulación, Docente de Postgrados, director de la Maestría de Protección de Datos de la Universidad Sergio Arboleda.

Endrick Dann Axel DÍAZ ORTEGA
Perito en Informática Forense

Abogado con Major en Economía de la Universidad Sergio Arboleda, Especialista en Seguridad de la Información e Informática de la misma Universidad, AccessData Certified Examiner v6 y cursos en: Técnicas Antiforenses del Centro Internacional de Excelencia Sergio Arboleda (España), Computer Hacking Forensics Investigator V9 del EC-Council, Introduction to Cyber Security de Cisco Networking Academy, Blockchain – Creación de Contratos Inteligentes de la Universidad Nacional de Colombia y Lean Six Sigma (Yellow, Green y Black Belt) de la Universidad Sergio Arboleda, entre otros.

Cuenta con más de siete años de experiencia en asuntos de Pericias en Informática Forense, Protección de Datos Personales, Derecho al olvido, Derecho Informático, Propiedad Intelectual y Seguridad de la Información e Informática.

Héctor Alberto DUSSAN MONTOYA (ingeniero de laboratorio)

Perito en Informática Forense.

Ingeniero de sistemas de la Universidad Francisco José de Caldas, con más de (1) año de experiencia en Seguridad de Informática y asuntos relacionados con Informática Forense en el sector privado, cuenta con una certificación AccessData Certified Examiner v6 y cursos en: Introduction to Cyber Security de Cisco Networking Academy, Cybersecurity Essentials de Cisco Networking Academy.

4. **La lista de publicaciones, relacionadas con la materia del peritaje, que el perito haya realizado en los últimos diez (10) años, si las hubiere.**

   ADALID CORP S.A.S., al encontrarse legalmente constituida como persona jurídica no ha escrito bajo su autoría ningún tipo de publicación relacionada a los peritajes realizados por la misma en los últimos diez (10) años.

5. **Lista de casos en los que haya sido designado como perito o en los que haya participado en la elaboración de un dictamen pericial en los últimos cuatro (4) años.**

   ADALID CORP S.A.S., relaciona mediante Registro Único de Proponentes su experiencia en los procesos en los que ha sido designado como perito informático para la elaboración de dictámenes periciales.

REGISTRO ÚNICO DE PROPONENTES: https://adalid-my.sharepoint.com/:f:/p/comercial/EpTNFqPs5mRPj5f-SZ8sF3oBRpdreXDUaW4UDaita9fK9w?e=culY3u

6. **Si ha sido designado en procesos anteriores o en curso por la misma parte o por el mismo apoderado de la parte, indicando el objeto del dictamen.**

ADALID CORP. S.A.S. ha sido designada como perito en procesos anteriores por el apoderado DR. Sergio ROJAS para el dictamen informático del tribunal de arbitramento de **C.I. IBLU V. EPK KIDS SMART** para el año 2020**;** a su vez la firma **DLA PIPER MARTÍNEZ BELTRÁN** designó a ADALID CORP. S.A.S. para el proceso de **EDEMSA V. EDEMCO** para el año 2020**.**

El objeto del dictamen, en ambos casos, es una pericia informática sobre diferentes piezas digitales.

7. **Si se encuentra incurso en las causales contenidas en el artículo 50, en lo pertinente.**

Manifiesto con las solemnidades pertinentes que no me encuentro incurso en ninguna de las once (11) causales descritas y numeradas en el artículo 50 de la Ley 1564 de 2012, relacionadas con la exclusión de la lista de los auxiliares de la justicia; que aplican en mi oficio como perito particular.

8. **Declarar si los exámenes, métodos, experimentos e investigaciones efectuados son diferentes respecto de los que ha utilizado en peritajes rendidos en anteriores procesos que versen sobre las mismas materias. En caso de que sea diferente, deberá explicar la justificación de la variación.**

Declaro con las solemnidades necesarias que todos los métodos y/o procedimientos, inequívocamente adelantados, en el desarrollo de esta pericia obedecen a aquellos que regularmente se aplican y que aconsejan los más altos estándares nacionales e internacionales en la materia (particularmente los estándar ISO/IEC 27037:2012 e ISO/IEC 27042:2015), en consecuencia, no existe variación alguna que deba ser justificada.

9. **Declarar si los exámenes, métodos, experimentos e investigaciones efectuados son diferentes respecto de aquellos que utiliza en el ejercicio regular de su profesión u oficio. En caso de que sea diferente, deberá explicar la justificación de la variación.**

Declaro con las solemnidades necesarias que todos los métodos y/o procedimientos, inequívocamente adelantados, en el desarrollo de esta pericia obedecen a aquellos que regularmente aplico en el ejercicio de mi profesión como experto en informática forense, de acuerdo con los estándares ISO/IEC 27037:2012 e ISO/IEC 27042:2015, en consecuencia, no existe variación alguna que deba ser justificada.

10. **Relacionar y adjuntar los documentos e información utilizados para la elaboración del dictamen.**

El informe que relaciona las herramientas lógicas y físicas empleadas en la pericia, así como cualquier activo de información que deba hacer parte de este proceso técnico, se encuentra debidamente referenciado y/o adjunto al interior del informe final número **F-22-11306-ADO** de fecha 28 de febrero de 2022, atendiendo a una secuencia y metodología pertinentes debidamente explicadas y enuncia.

RV: JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ/TRÁMITE DE PRUEBAS EXTRAPROCESALES/RAD 2020-00339/ RECURSO DE REPOSICIÓN Y EN SUBSIDIO DE APELACIÓN

Juzgado 19 Civil Circuito - Bogota - Bogota D.C. <ccto19bt@cendoj.ramajudicial.gov.co>
Jue 20/10/2022 8:12
Para: Arley Eduardo Espinosa <aespino@cendoj.ramajudicial.gov.co>

De: Sergio Rojas <srojas@dlapipermb.com>
Enviado: jueves, 20 de octubre de 2022 8:05 a. m.
Para: Juzgado 19 Civil Circuito - Bogota - Bogota D.C. <ccto19bt@cendoj.ramajudicial.gov.co>
Cc: monica.tocarruncho <monica.tocarruncho@kennedyslaw.com>; Sebastian Escobar Torres <sebastian.escobartorres@kennedyslaw.com>; Catalina.Botero@kennedyslaw.com <Catalina.Botero@kennedyslaw.com>; Daniel Andrés Samacá <dasamaca@dlapipermb.com>
Asunto: JUZGADO 19 CIVIL DEL CIRCUITO DE BOGOTÁ/TRÁMITE DE PRUEBAS EXTRAPROCESALES/RAD 2020-00339/ RECURSO DE REPOSICIÓN Y EN SUBSIDIO DE APELACIÓN

Bogotá, D.C., octubre de 2022

Señora,
JUEZ 19 CIVIL DEL CIRCUITO DE BOGOTÁ
ATN. DRA. ALBA LUCÍA GOYENECHE GUEVARA
E. S. D.

REF.	**Solicitantes:**	INTEGRAL S.A. y OTRO
	Solicitado:	MAPFRE SEGUROS GENERALES DE COLOMBIA S.A.
	Radicado:	**2020-00339**
	Asunto:	**Recurso de reposición y en subsidio de apelación contra el auto del 13 de octubre de 2022**

El suscrito, **SERGIO ROJAS QUIÑONES**, mayor de edad, con domicilio en la ciudad de Bogotá D.C., identificado como aparece al pie de mi firma, actuando en mi condición de apoderado de **INTEGRAL S.A.** y del **CONSORCIO GENERACIÓN ITUANGO**, acudo respetuosamente ante el Despacho con el fin de interponer los recursos de **REPOSICIÓN** y en subsidio de **APELACIÓN**, contra el auto del 13 de octubre de 2022, notificado por anotación en el estado del día siguiente, por medio del cual el H. Despacho resolvió decretar la terminación del trámite por desistimiento tácito.

Me permito adjuntar el recurso en formato PDF, junto con sus anexos.

En copia se encuentran los apoderados de la parte contraria.

Del Despacho,

SERGIO ROJAS QUIÑONES

JUZGADO DIECINUEVE CIVIL DEL CIRCUITO DE BOGOTÁ

PROCESO: 11001310301920200033900

Hoy 25 de octubre de 2022 siendo las ocho (8:00) de la mañana, SE FIJA EN TRASLADO EL RECURSO DE REPOSICIÓN por el término de TRES (3) días, en cumplimiento al artículo 319 y 108 del C.G.P.

Inicia:	26 de OCTUBRE de 2022 a las 8:00 A.M.
Finaliza:	28 de OCTUBRE de 2022 a las 5:00 P.M.

GLORIA STELLA MUÑOZ RODRIGUEZ