UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE

Maestro(a) en Seguridad y Gestión de Riesgos Informáticos

PROYECTO

Técnicas y Aplicaciones de la Informática Forense en procesos de peritaje informático.

PRESENTADO POR

José Carlos Barrera Barahona

Erickson Yasir Elías Pineda

Leysi Abigail Tejada Sandoval

ASESOR

Mg. Leonel Antonio Maye

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

Junio 2022

Contenido

Resumen

En el presente documento se proporciona una perspectiva real de la labor del investigador forense en casos de investigación y análisis forense digital.

La investigación forense conlleva una continua formación acompañada por la experiencia práctica en casos de investigación reales.

A medida que surgen nuevas tecnologías y entornos, la labor del perito informático se vuelve de vital importancia ya que el perito es el que dictamina las vías de investigación apoyándose en las diferentes técnicas y aplicaciones de la investigación forense como tal. Por lo tanto, el ámbito multidisciplinar de la informática forense digital la convierte en una ciencia con tendencia a la especialización como ocurre por ejemplo en medicina.

La elección del tipo de peritaje forense para el desarrollo de un caso de investigación dependerá de la experiencia y de las herramientas con las que el investigador forense cuente.

El caso práctico presentado en este documento se compone de varias guías con la finalidad de poder abarcar el mayor espectro de líneas de investigación posible.

Las guías incluidas en el presente documento son:

1. Análisis en Casos de Robo de Información Personal.
2. Phishing.
3. Metodología Forense en sistemas Windows.
4. Técnicas de Recuperación de Información.
5. Metodología Forense en sistemas Linux.

Es importante seguir un protocolo de actuación adecuado que esté bien documentado y apegado a derecho, así mismo, se debe determinar claramente los objetivos de la investigación en curso, esto debe realizarse en base al requerimiento inicial, adicionalmente, se deben describir las herramientas y utilidades forenses utilizadas durante el caso de investigación. El perito se centrará en investigar aquello que se le encomiende y para ello, deberá recabar toda la información que considere relevante para el caso. El investigador forense tiene la responsabilidad de conocer que evidencias son las que se deben de adquirir.

Guía 1: Análisis en Casos de Robo de Información Personal

Proceso

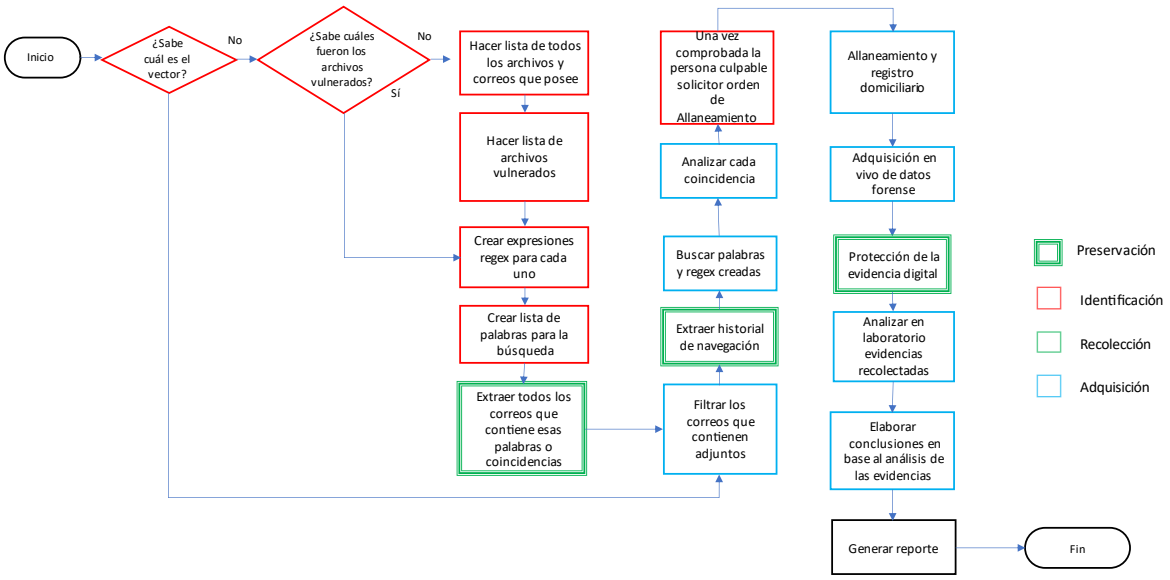


Figura 1: Diagrama del proceso

Detalle

Paso	Propósito	Técnica	Descripción	Herramientas
¿Sabe cuál es el vector de ataque?	Descubrir si se tiene conocimientos que puedan asegurar que sabemos la causa del ataque	Entrevista Evidencias previas	Se consulta al interesado si tiene conocimiento sobre un vector de ataque que considere que es probable que sea el causante del ataque	✓ Editor de texto ✓ Grabadora ✓ Notepad++
¿Sabe cuál correo fue vulnerado?	Saber si se tiene conocimiento del correo que fue víctima del ataque	Entrevista	Se consulta al interesado si sabe que correo fue vulnerado en el ataque de phishing	✓ Editor de texto ✓ Grabadora ✓ Notepad++
Hacer lista de todos los correos	Determinar cuál es el posible correo que sirvió como vector.	Entrevista.	Se consulta al interesado sobre los correos que posee o ha poseído.	✓ Editor de texto ✓ Notepad++
Hacer lista de todos los usuarios que posee	Determinar cuáles cuentas o servicios pueden solicitar información de interés o facilitan la recuperación de cuentas	Entrevista.	Consultar al interesado que servicios posee tales como FB, Twitter, cuentas e-banca, otros portales empresariales, etc.	✓ Editor de texto ✓ Notepad++
Crear expresiones regex para cada uno	Crear expresiones que hagan coincidencias visuales con los servicios analizados	Búsqueda de texto	Crear un listado de regex que faciliten la búsqueda. Estas expresiones deben contener las frases más significativas utilizadas por las interfaces de los servicios utilizados.	✓ Regex Generator (w) ✓ RegexR(w) ✓ Browserling(w)
Crear lista de palabras para la búsqueda	Crear lista de palabras empleadas por esos servicios. Agregar palabras propias de ingeniería social.	Análisis.	Agregar palabras con los nombres de bancos, nombre de la persona, nombres de documentos, nombres de compañeros de trabajo, etc.	✓ Editor de texto ✓ Notepad++
Extraer todos los correos que contiene esas palabras o coincidencias	Crear una copia para facilitar su análisis. Crear una copia de respaldo.	Backup	Crear una copia local de los correos del servidor. Usar si ya existe una. Todos los gestores que correo crean una copia local de los correos recibidos. Ver tiempo para el borrado automático.	✓ Gestor de correo ✓ Thunderbird ✓ WinRAR
Filtrar los correos que contienen Urls	Analizar los que contienen potenciales vectores.	Carving	Buscar todos los correos que contienen https, http, etc. (Tag href) Especial atención a los que tienen dos correos como coincidencias.	✓ Gestor de Correo ✓ Visor EML ✓ EML Viewer Tool ✓ Forensic EML Viewer ✓ Notepad++
Analizar cada uno	Verificar HTTP[S]	Carving	Buscar y analizar las Url´s que no están cifradas.	✓ Visor EML ✓ EML Viewer Tool ✓ Forensic EML Viewer ✓ Notepad++ ✓ FileScan.io (w) ✓ Virus Total (w) ✓ Hybrid Analisys(w)
Filtrar los correos que contienen adjuntos	Analizar si los adjuntos poder ser vectores	Carving	Analizar si en los correos hay ejecutables o archivos que pueden servir para ello como	✓ Visor EML ✓ EML Viewer Tool ✓ Forensic EML Viewer ✓ Notepad++

			vectores (ej. PDF, JPG, SVG)	
Extraer historial de navegación	Listar los sitios a los que se ha navegado que fueron recibidos como parte de los correos.	Carving	Analizar si alguno de los sitios enviados fue usado.	✓ Browser ✓ BrowsingHistoryView ✓ IEHistoryView
Buscar palabras y regex creadas	Buscar en los correos coincidencias de potenciales vectores.	Carving	Buscar en las partes del correo, textos o indicaciones a proporcionar información. Analizar imágenes.	✓ Thunderbird ✓ Visor EML ✓ EML Viewer Tool ✓ Forensic EML Viewer ✓ Notepad++
Analizar cada coincidencia	Verificar cada uno de los sitios visitados.	Análisis.	Determinar cuál es el vector de compromiso.	✓ FileScan.io (w) ✓ Virus Total (w) ✓ Hybrid Analisys(w) ✓ Cuckoo
Creación de imagen forense de las pruebas	Respalda la información para su posterior análisis	Clonación	Obtener insumos iniciales para la investigación	✓ AccessData FTK Imager
Analizar Metadatos de los archivos de prueba originales	Analizar metadatos de los archivos originales para obtener pruebas del culpable	Análisis.	Encontrar información de las fotografías, como el día y hora que se realizaron, la marca y modelo del dispositivo / móvil cámara con que se hicieron y el software utilizado.	✓ AccessData FTK Imager ✓ ExifDataView
Allanamiento y registró domiciliario	Recolectar la evidencia física utilizara para el ataque	Recolección	Obtener evidencia física, ordenadores entre otros para su posterior análisis	✓ Bolsas Faraday ✓ Rotuladores, Cámaras
Adquisición en vivo de datos forenses	Recolectar información de portátil y otros dispositivos utilizados	Recolección y preservación	Obtener fotos de la pantalla del dispositivo utilizado, fotos de la escena para tener evidencias de la correcta recolección de evidencias	✓ Bolsas Faraday ✓ Rotuladores, Cámaras
Adquisición de la información almacenada en la memoria RAM	Recoletar evidencia de memoria ram para su análisis	Recolección y preservación	Obtener información forense contenida en la memoria RAM obtener contraseñas de discos o archivos cifrados, procesos en ejecución, conexiones establecidas, contraseñas de correo electrónico u otros accesos web autenticados	✓ AccessData FTK Imager
Análisis en laboratorio de las evidencias recopiladas	Analizar las evidencias recolectadas para elaborar conclusiones	Análisis	Analizar evidencias para determinar el vector de ataque y si las acusaciones contra Javier son ciertas para presentar informe posteriormente a la corte	✓ AccessData FTK Imager ✓ Bulk Extractor Viewer ✓ Autopsy
Elaborar informe final	Redactar un informe final en base al análisis de las evidencias	Análisis.	Brindar un informe final de lo ocurrido en el caso forense	✓ Word, PDF

Tabla 1: Detalles del proceso

Aspectos relacionados

Proceso	Caso de empleo
Auditorías regulares	Realizar múltiples validaciones a la configuración del sistema de manera diaria, semanal, mensual o de acuerdo con las necesidades del negocio.
Eliminación de cuentas no utilizadas.	Eliminar las cuentas asociadas a personas que ya no estén vinculadas a la organización, realización de pruebas.
Sitios confiables	Navegar por sitios que cuenten con mecanismo de seguridad, así como evitar descargar archivos, programas ejecutabes de sitios sospechosos.

Tabla 2: Aspectos relacionados

Ejemplo

La autoridad judicial solicita los servicios del perito informático judicial JNC para dar apoyo a la investigación tecnológica en un caso de delito informático.

Se facilita el expediente del procedimiento judicial con el fin de aportar al perito toda la información del caso.

Caso "AMPARO CONTRA JAVIER"

En primer lugar, se detalla la denuncia interpuesta por la victima Amparo ante la policía nacional contra Javier, quien es dueño de una empresa de servicio técnico informático.

Trascripción de la declaración de Amparo:

Amparo deposita su ordenador portátil para su reparación en la empresa YoReparoTuPC -servicio técnico informático - de San Salvador (El Salvador).

Le atiende Javier dueño de la empresa y único técnico y empleado de la misma.

Ese mismo día Amparo recoge el portátil ya reparado. Desde su móvil marca LG realiza un video y varias fotos personales e íntimas. Las descarga a su ordenador y las envía por correo electrónico (amparo.xiva@gmail.com) a su novio Jorge (jorge.chiva@gmail.com).

Al día siguiente, Juan un amigo de Javier informa a Amparo que Javier le ha enseñado unas fotografías y un video de ella en los que aparece semidesnuda. Esto ocurrió en la oficina de la empresa de Javier desde su portátil y cree que estaban almacenadas en un pendrive negro con lados plateados. Juan también afirma que Javier le dijo que podía acceder al correo de Amparo pero que iba a borrar todo rastro por seguridad.

A la vista de la denuncia el Juez declara a Javier como presunto acusado de los delitos que se citan a continuación y ordena el registro de la empresa de Javier para recabar las pruebas.

Presuntos delitos cometidos por Javier:

Intromisión informática.

El artículo 30 Ley Especial Contra Los Delitos Informáticos y Conexos:

Art. 30.- El que adquiera para sí o para un tercero a través de cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación, o posea material pornográfico en el que se haya utilizado a una niña, niño, adolescente o persona con discapacidad o su imagen para su producción, será sancionado con prisión de dos a cinco años. Igual sanción se aplicará al que posea en dispositivos de almacenamiento de datos informáticos o a través de cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación, material pornográfico en el que se haya utilizado a una niña, niño, adolescente o persona con discapacidad o su imagen para su producción.

Revelación de secretos laborales o profesionales.

El Código penal establece en su artículo 23:

Art. 23.- El que sin autorización obtenga o dé a conocer por medio de las Tecnologías de la Información o Comunicación, un código, contraseña de acceso o cualquier otro medio de acceder a un programa o datos almacenados en un equipo o dispositivo tecnológico, con el fin de lucrarse así mismo, a un tercero o para cometer un delito, será sancionado con prisión de cinco a ocho años. (1) Igual sanción tendrá el que sin autorización revele o difunda los datos o información, contenidos en un sistema informático que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, con el fin de obtener algún tipo de beneficio para sí o para otro. (1)

Manipulación de datos reservados registrados en ficheros o soportes informáticos.

Establece el artículo 26 del código penal:

Art. 26-A. Quien por cualquier medio telemático accediere a sistemas de programas, o dispositivos electrónicos o datos informáticos de una persona natural o jurídica, restringiendo el acceso a ellos y a los datos informáticos almacenados, con el propósito de exigir u obtener un provecho a cambio de la liberación de estos, será sancionado con prisión de cuatro a seis años. (1) Si la conducta del inciso anterior afectare a sistemas, programas o datos informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión y transporte de energía, de medios de transporte u otros de servicio público, o destinados a la prestación de servicios financieros, o la realización de transacciones en Bitcoin u otras criptomonedas, así como que permitan su convertibilidad automática e instantánea a moneda de curso legal, la sanción de prisión será de seis a ocho años. (1)

Requerimiento 01

Recopilar las fotografías y video originales realizados por Amparo y enviados por correo desde su portátil. Aportar las pruebas del envió del correo de Amparo a Jorge y su contenido según declarado por Amparo.

Requerimiento 02

Identificar, requisar y preservar el dispositivo almacenamiento extraíble

usb negro –p*endrive*- para su posterior análisis en laboratorio.

Buscar y extraer los archivos que contienen las fotografías y video deAmparo (pruebas originales).

Requerimiento 03

Determinar si el portátil Toshiba propiedad de Javier sito en la oficina de su empresa contiene indicios que incriminen o no a éste de los delitos que se le acusa.

Acceso a la cuenta de amparo.xiva@gmail.com - contraseña robada.

Rastro digital de las fotografías y video de Amparo (prueba original).

Determinar si el *pendrive* citado ha sido conectado a dicho portátil.

Una vez se tiene claro el tipo de pericia que se va a realizar, se debe planificar las actuaciones y documentar la línea de investigación con los métodos y herramientas a emplear.

En caso de cualquier duda, antes de comenzar la investigación, es necesario realizar todas preguntas pertinentes a fin de solventarlas.

Identificación y preservación de las pruebas originales

En primer lugar, se van a identificar y custodiar las fotografías y videos almacenados en el portátil propiedad de Amparo –pruebas originales-, y enviadas como adjunto en el mensaje de correo electrónico. Se incluirán como prueba original en la investigación.

Obtener información del mensaje de correo electrónico enviado

Se realiza un respaldo digital de contenido original de la cabecera, cuerpo y adjuntos del mensaje enviado con el nombre "Gmail - Fotos y video enviadas por Amparo.pdf" se protege contra escritura para evitar su manipulación y se realiza una captura de pantalla (figura 2), todo esto se realiza ante el secretario judicial que da fe del proceso.

El contenido del mensaje es:

MIME-Version: 1.0
Received: by 10.31.234.197 with HTTP; Mon, 14 Mar 2016 08:52:55 -0700 (PDT)
Date: Mon, 14 Mar 2016 16:52:55 +0100
Delivered-To: amparo.xiva@gmail.com
Message-ID: CAKCdkKMsKF+8n302M2zCqAu3sOf_Lb1Y4k7QbGn2=nEax6ebUg@mail.gmail.com
Subject: Fotos y video
From: =?UTF-8?Q?Amparo_S=C3=A1nchez?= amparo.xiva@gmail.com
To: Jorge Navarro jorge.chiva@gmail.com
Content-Type: multipart/mixed; boundary=001a1140ffd6254820052e0446c7
--001a1140ffd6254820052e0446c7
Content-Type: multipart/alternative; boundary=001a1140ffd6254819052e0446c5
--001a1140ffd6254819052e0446c5
Content-Type: text/plain; charset=UTF-8--001a1140ffd6254819052e0446c5Content-Type: text/html; charset=UTF-8

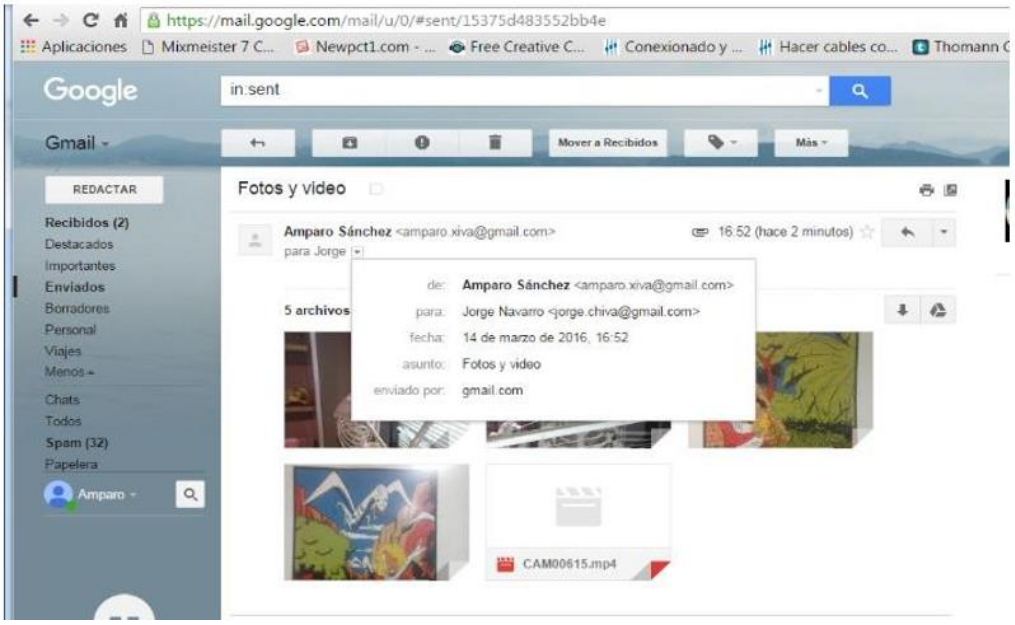


Figura 2: Captura de pantalla del mensaje de correo electrónico.

Es importante especificar el servidor de correo electrónico por si esta prueba fuera requerida en caso de procedimiento judicial.

Servidor: GMAIL.COM /empresa Google/

Crear imagen forense de las pruebas

En el laboratorio con la aplicación portable AccessData FTK Imager v3.1.18 se crea la imagen de los ficheros originales en "pruebaoriginal.ad1" y sus correspondientes *hashes*. Se copian por duplicado finalmente en CD para su custodia y preservación (figura 3).

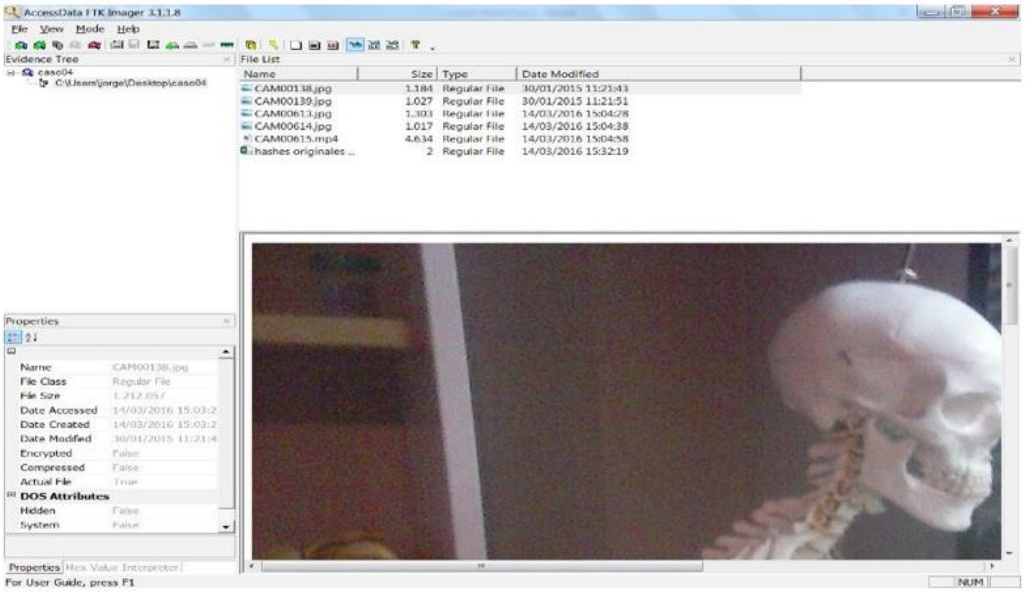


Figura 3: Creación de copia forense de las pruebas originales con FTK Imager.

Hash de la imagen creada pruebaoriginal.ad1 y ficheros originales con sus *hashes* (figura 4).

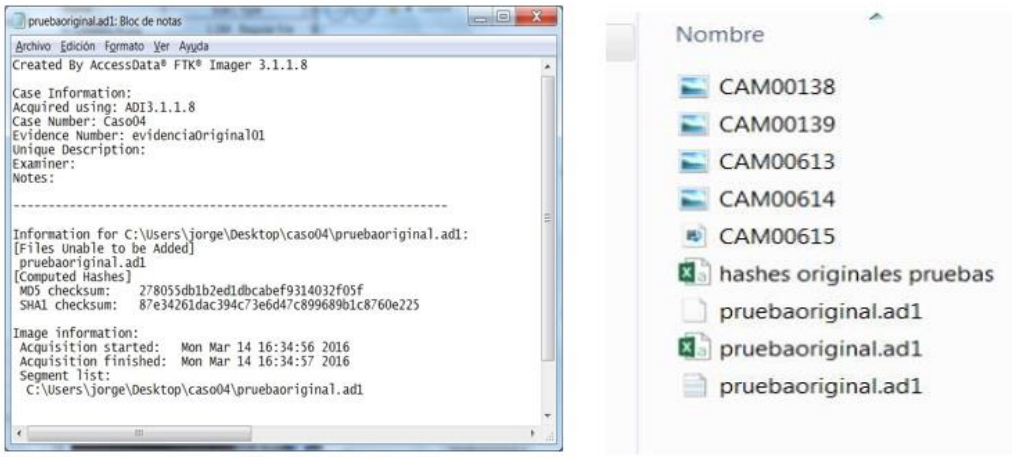


Figura 4: Hash de la imagen creada y pruebas originales.

Se comprueban los *hashes* de las dos copias para asegurar su integridad y se comprueba que coinciden.

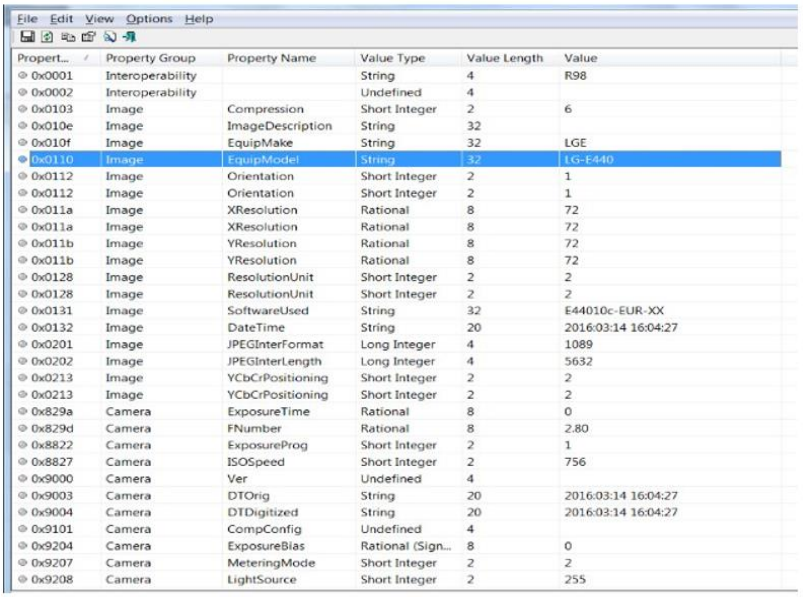
Se etiquetan con el nombre EVI01 y número de identificación de cada soporte.

Se entrega una copia - CD EVI01-01- al funcionario encargado de la custodia de evidencias y se documenta. Se anota en el documento de custodia que la copia -CD EVI01-02 - se traslada al laboratorio para la investigación.

Metadatos de los archivos de prueba originales

Los metadatos nos proporcionan una valiosa información de las fotografías, como el día y la hora en que se realizaron, la marca y modelo del dispositivo / móvil cámara con que se hicieron y el software utilizado.

Para realizar la tarea se utiliza la herramienta portable **ExifDataView 1.2** (figura 5).



Propert...	Property Group	Property Name	Value Type	Value Length	Value
0x0001	Interoperability		String	4	R98
0x0002	Interoperability		Undefined	4	
0x0103	Image	Compression	Short Integer	2	6
0x010e	Image	ImageDescription	String	32	
0x010f	Image	EquipMake	String	32	LGE
0x0110	Image	EquipModel	String	32	LG-E440
0x0112	Image	Orientation	Short Integer	2	1
0x0112	Image	Orientation	Short Integer	2	1
0x011a	Image	XResolution	Rational	8	72
0x011a	Image	XResolution	Rational	8	72
0x011b	Image	YResolution	Rational	8	72
0x011b	Image	YResolution	Rational	8	72
0x0128	Image	ResolutionUnit	Short Integer	2	2
0x0128	Image	ResolutionUnit	Short Integer	2	2
0x0131	Image	SoftwareUsed	String	32	E44010c-EUR-XX
0x0132	Image	DateTime	String	20	2016:03:14 16:04:27
0x0201	Image	JPEGInterFormat	Long Integer	4	1089
0x0202	Image	JPEGInterLength	Long Integer	4	5632
0x0213	Image	YCbCrPositioning	Short Integer	2	2
0x0213	Image	YCbCrPositioning	Short Integer	2	2
0x829a	Camera	ExposureTime	Rational	8	0
0x829d	Camera	FNumber	Rational	8	2.80
0x8822	Camera	ExposureProg	Short Integer	2	1
0x8827	Camera	ISOSpeed	Short Integer	2	756
0x9000	Camera	Ver	Undefined	4	
0x9003	Camera	DTOrig	String	20	2016:03:14 16:04:27
0x9004	Camera	DTDigitized	String	20	2016:03:14 16:04:27
0x9101	Camera	CompConfig	Undefined	4	
0x9204	Camera	ExposureBias	Rational (Sign...	8	0
0x9207	Camera	MeteringMode	Short Integer	2	2
0x9208	Camera	LightSource	Short Integer	2	255

Figura 5: Metadatos de las fotografías originales.

Destacar que dichas fotografías se realizaron con la cámara de una móvil marca LG modelo E400 y con el software descrito en el campo *SoftwareUsed*, en la fecha y hora mostrada en la fila *DateTime*.

Resumen de las tareas realizadas en este procedimiento

En esta tarea se han recopilado, preservado y custodiado las pruebas originales.

Donde se obtienen: cuatro archivos JPG de fotografías, un archivo de video MP4 (ver más arriba) y la prueba del envío del mensaje por correo electrónico con los citados archivosadjuntos.

Se obtiene además información de cuándo y con que marca y modelo de dispositivo se realizaron dichas fotografías y video. Se hace copia duplicada de todo en CD. Y se generan y anotan en el documento de cadena de custodia los hashes correspondientes a los archivos.

Herramientas forenses utilizadas en la investigación

AccessData FTK Imager v 3.1.2: para crear la copia forense de las evidenciasoriginales y generación de *hashes*.

ExifDataView v 1.2: para obtener los metadatos de las fotografías.

Allanamiento y registro domiciliario

Se acompaña a los funcionarios, policía y secretario judicial al domicilio de la empresa de Javier para el registro e incautación de los dispositivos digitales y demás pruebas relevantes para el caso, sobre todo el dispositivo *usb pendrive* y el portátil Toshiba.

Una vez en la escena se realizarán fotografías y vídeos (figura 6) de los equipos e instalaciones asociados al procedimiento. Un funcionario requisará el *pendrive,* considerado como elemento de prueba, hallado sobre la mesa del escritorio. Se almacena en una bolsa especial aislado de campos electromagnéticos que lo puedan dañar y se identifica como EVI02. Se inicia la cadena de custodia y su traslado posterioral laboratorio forense para su análisis.

Figura 6: Fotografías de la investigación de campo.

Una vez identificadas las pruebas que se van a investigar y documentada la escena completa, se debe, dependiendo del escenario, actuar de una manera u otra. En este caso, en primer lugar, se investigará el portátil encendido por considerarlo una prueba volátil con riesgo de pérdida de información relevante, en caso de bloqueo o corte de suministro eléctrico. Se identificará como **EVI03** en el documento de campo y en la cadena de custodia.

Adquisición en vivo de datos forenses

Este tipo de investigación forense denominada –*live forensics*- requiere herramientas software portables poco intrusivas (recordar que no se dispone de equipos hardware forense, que sería lo ideal) para la recolección de evidencias en la información volátil del sistema Windows del portátil Toshiba.

Se realizará en primer lugar una fotografía del contenido de la pantalla (figura 7), a ser posible que se vea la fecha y hora del sistema. Es recomendable realizar un vídeo y/o fotografías y capturas de pantalla de todo el procedimiento de investigación y documentar cada acción realizada. Indicar que la investigación de un sistema encendido "vivo" es irrepetible por esto cuanto más documentada más fácil será su exposición y defensa.

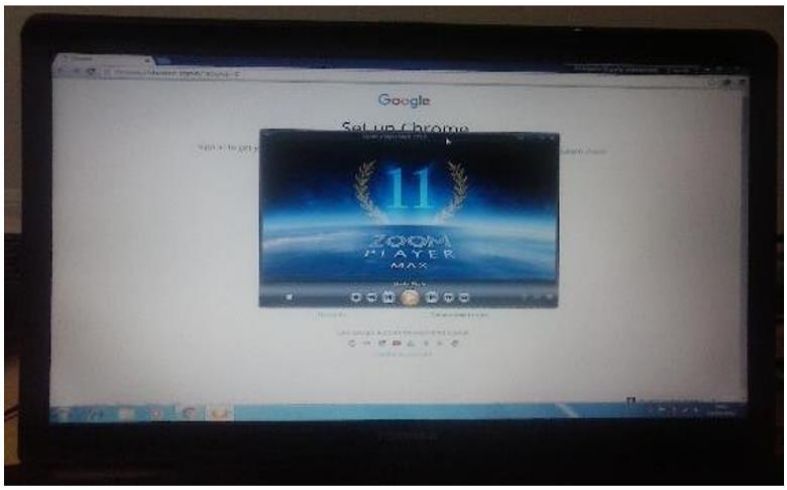


Figura 7: Fotografía de la pantalla del portátil.

Para realizar la adquisición y análisis de los datos forenses volátiles se utilizan las herramientas portables forenses contenidas en el *pendrive* de trabajo de campo. Se protege contra escritura y se conecta al portátil Toshiba donde el sistema Windows le asigna la unidad de disco E:\.

Se chequea todo el sistema Windows en de busca virus, *malwares* y *rootkits* que puedan perjudicar la investigación o dañar el contenido del pendrive de trabajo. Desde la Shell de Windows como administrador se ejecutan los programas SuperAntiSpyware (SAS) y ClamWin desde la carpeta E:\VIRUS Y MALWARE. En ambos casos el resultado ha sido: "NO SE HAN ENCONTRADO AMENAZAS".

Determinar la fecha y hora del sistema Windows

Para comprobar la diferencia horaria con respecto a la proporcionada por UTC se ejecuta desde la Shell de Windows el siguiente comando:

date /t > fechayhoradeportatilEv03.txt & time /t >> fechayhoradeportatilEv03.txt

El archivo de salida "fechayhoradeportatilEv03.txt" se almacena en la carpeta de recopilación de datos forenses (E:\DATOS CASO).

La hora del portátil tiene un adelanto de 5 minutos respecto a UTC. Es posible que durante la investigación está información sea relevante por ejemplo si es necesario un "*time line*" o para determinar la fecha y hora exacta de sucesos.

Seguidamente, se obtiene el *hash* del fichero de salida y se anota en el documento de cadena de custodia.

Para obtener los *hashes*, si no se indica lo contrario, se utilizará durante todo el desarrollo del caso el software **HashMyFiles.** Este programa genera los hashes MD-5, SHA1, SHA-256, SHA-384 y SHA-512 proporcionando mayor validez a las pruebas recopiladas (figura 8).

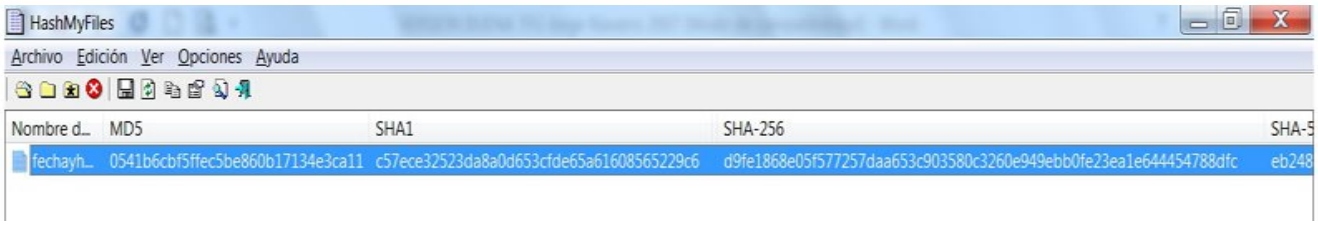


Figura 8: Hashes generados con el software HashMyFiles.

Seguidamente, se procede a adquirir la información forense volátil en orden de más a menos volatilidad, de acuerdo a la recomendación de las normas aplicadas en la investigación.

Apuntar que, la información de la memoria de un sistema Windows se encuentra en la propia RAM -memoria física- y en el fichero de intercambio "*pagefile.sys*" -memoria virtual-. En nuestro caso se adquiere solamente la memoria física –RAM- puesto que el fichero "*pagefile*" está almacenado en el disco duro y puede ser analizado posteriormente en el laboratorio.

Adquisición de la información almacenada en la memoria RAM

La información forense contenida en la memoria RAM es importante, sobre todo, para obtener contraseñas de discos o archivos cifrados, procesos en ejecución, conexiones establecidas, contraseñas de correo electrónico u otros accesos web autenticados.

Mediante la versión portable del programa **AccessData FTK Imager** se realiza la captura de la memoria RAM a fichero, se crea la imagen forense y se calculan los *hashes*, todo ello en el mismo proceso. En la ventana siguiente se elige la carpeta de destino, el nombre del fichero de volcado ".mem", la opción incluir *pagefile* (desmarcar) y crear la imagen (marcar) según se muestra en la figura 9.

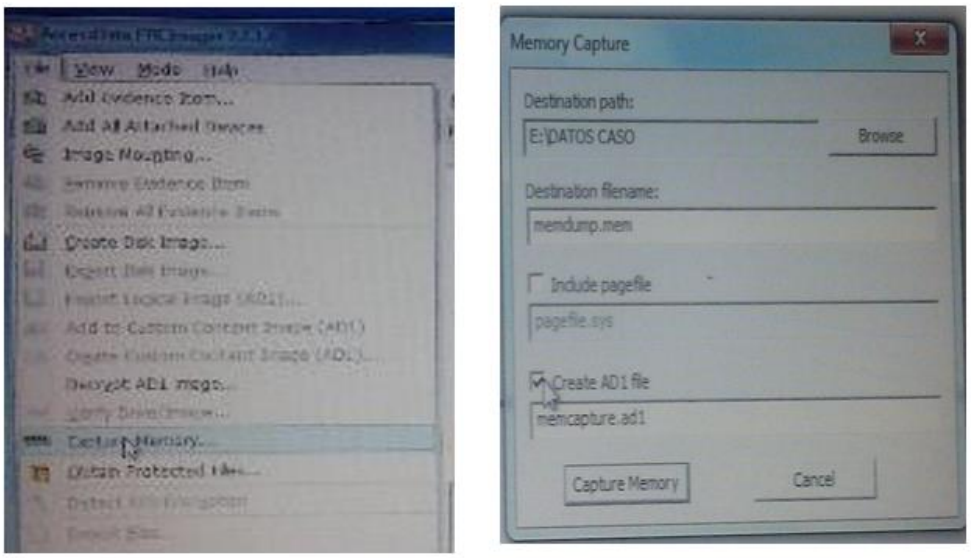


Figura 9: Volcado de memoria RAM con AccessData FTK Imager.

Una vez obtenida la imagen correspondiente al volcado de memoria física se genera su *hash* correspondiente y se anota en el documento de cadena de custodia.

Hash

Nombre de archivo: **memcapture.ad1**

Ruta completa : E:\DATOS CASO\memcapture.ad1
MD5 :
8a42eeb99be91ec88bbf02a55fee991c
SHA1 :
8c016a8eb6ec600e79058330155f62c0a3e8c43cCRC32 :
1cbf12e5
SHA-256 :
65e5ee3b78e5b703729cbc040902bd1998c2a2ae0a7258987ee7b7e9e76075f3SHA-512 :
5dc1784a2b23571923c059c8f029634ded8999f7f1c6e5b19e991d4d7ec3f3a975a1402ee1b3a5d340f5a690534ecbd79f
57baecc7eac7f7a1766695d7ef0a6d
SHA-384 :
b0c456f339d59854ca025a017a628f450538fab749ae070190fd044db619a946a2af2343f0144efeffe1e461f665ca
b5 Extensión : ad1
Atributos del archivo: R

Adquisición del resto de información volátil del portátil

Una manera de realizar esta tarea de forma rápida, eficaz, segura y poco intrusiva es mediante una utilidad que ejecute un proceso *batch* con todas las herramientas forenses de adquisición que consideremos apropiadas para el tipo de investigación.

Se ha decidido escoger la herramienta **Investigador 2.0**, idónea para la recolección automática de evidencias digitales en sistemas Windows encendidos.

Desarrollada por ingeniero del Laboratorio Pericial Informático - Neuquen - Argentina.

Este software utiliza aplicaciones gratuitas para realizar la recolección de información digital forense asociada a un equipo informático (figura 10).

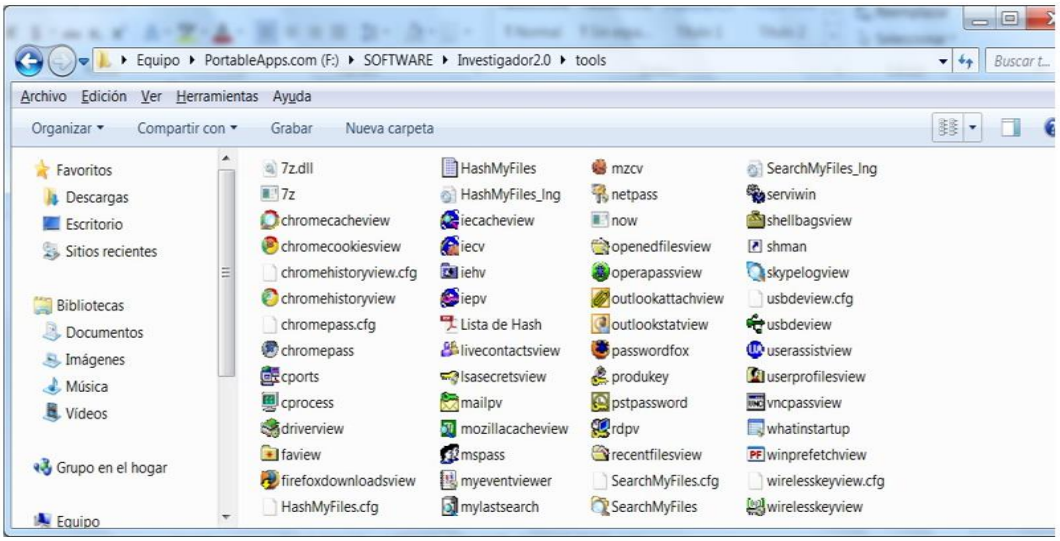


Figura 10: Herramientas y utilidades incluidas en el software Investigador 2.0

Para lanzar el proceso como administrador, desde la Shell de Windows, ir al directorio E:\SOFTWARE\Investigador2.0 y ejecutar la aplicación INVESTIGADOR.

Puede demorar varios minutos. No se debe cancelar ni cerrar las ventanas emergentes que la aplicación vaya desplegando.

Los resultados son guardados dentro del mismo dispositivo y carpeta desde el que se ejecuta el software. Asimismo, el software Investigador crea una carpeta comprimida con todos los archivos resultantes de la inspección digital automatizada y un fichero de texto con los *hashes*.

Al lanzar la aplicación aparece una ventana con varios menús de pestañas con casillas de verificación para seleccionar la información a recopilar según el tipo de caso ainvestigar (figura 11).

Es aconsejable marcar la casilla “Abrir el reporte” para que nos muestre los resultados una vez terminados el proceso. Finalmente pulsamos el botón EJECUTAR.

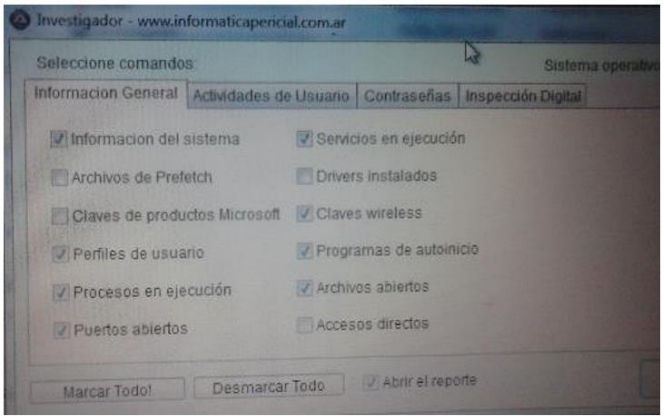


Figura 11: Configuración de aplicación Investigador 2.0

La aplicación genera una estructura (figura 12) de carpetas y archivos con la intención de crear posteriormente un DVD *Autorun* para navegar por los resultados obtenidos. Destacar el archivo de resultados comprimido y el fichero *hashes* generado. En la figura 13 se muestran los archivos que contienen la información forense a analizar en busca de las evidencias requeridas.

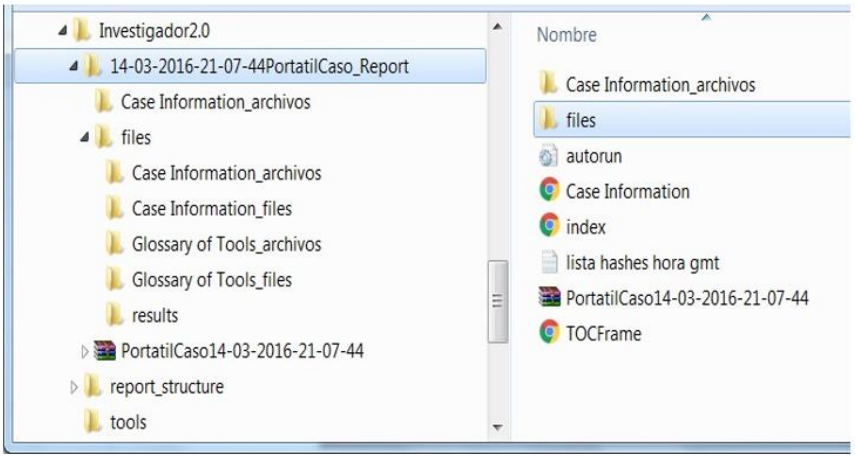


Figura 12: Estructura de carpetas de resultado de análisis de la aplicación Investigador 2.0

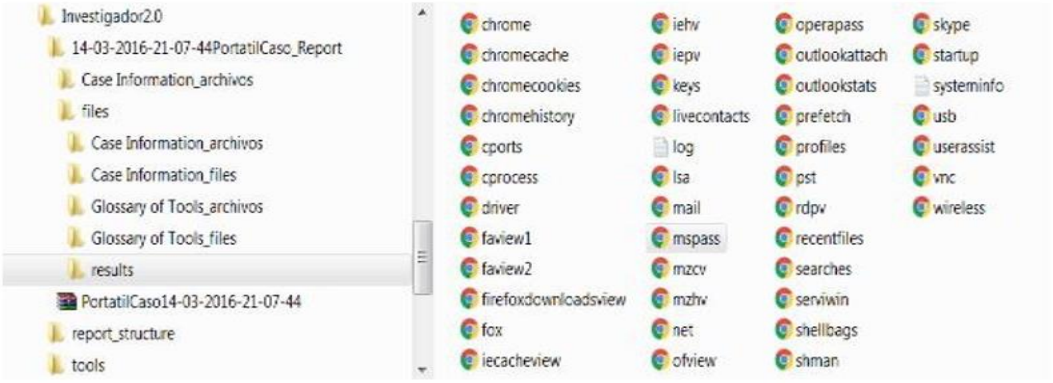


Figura 13: Archivos forenses generados por la aplicación Investigador 2.0

Una vez finalizado el proceso de adquisición de datos forenses, y antes de navegar por los resultados obtenidos, se realizarán dos copias en *DVD* con el contenido de la carpeta de salida generada en este apartado (ver figura 12) y la imagen de captura de memoria RAM "**memcapture.ad1** …" del aparado anterior. Se identifican los *DVDs* como **EVI03-1 / EVI03-2** y se preparan para su traslado. Junto con los hashes generados se anotan las evidencias en el documento de cadena de custodia donde se especifica que una copia debe ir al laboratorio forense para ser analizada. Y finalmente, se documenta la investigación con los pasos realizados y la secuencia fotográfica / video realizada.

Resumen de las tareas realizadas en este procedimiento

En primer lugar, se analiza el sistema en busca de amenazas (virus, *malware*, *rootkits*, etc).

Posteriormente, se comprueba el desfase horario de Windows respecto a UTC y se realiza la imagen forense del volcado de la memoria RAM.

Para finalizar con la recopilación y adquisición del resto de información volátil de Windows (logs, procesos, información del sistema, caches de navegación, contraseñas, datos de red, etc).

Copia en DVD por duplicado de los datos adquiridos. Documentación del proceso añadiendo fotografías y videos, así como cumplementar la información en las hojas de cadena de custodia.

Herramientas forenses utilizadas

Análisis en busca de posibles amenazas: **SAS** y **WinClam**

Imagen de volcado de la memoria RAM: **AccessData FTK Imager**

Adquisición de información volátil de Windows: **Investigador 2.0** (conjunto de utilidades forenses).

En la fase de análisis se detalla cada herramienta ejecutada y su cometido en la investigación.

Generación de hashes: **HashMyFile**

Una vez adquirida toda la información volátil del portátil se debe desconectar del suministro eléctrico de forma "brusca", tirando del cable, o sea, no apagar de manera ordenada. Así nos aseguramos de que durante el proceso de apagado no se ejecute ningún programa oculto que pueda alterar la información de los dispositivos de almacenamiento. Una vez apagado el portátil se precintará, identificará y se preservará para

su traslado al laboratorio por si fuera necesario y a requerimiento judicial realizar el análisis forense de sus discos duros.

Análisis en laboratorio de las evidencias recopiladas

Una vez en el laboratorio forense se procede con la fase de análisis en busca de las evidencias requeridas en el expediente judicial.

Pruebas recopiladas en la fase de adquisición:

- EVI01 pruebas originales (fotografías, vídeo y mensaje de correo).
- EVI02 pendrive *usb* requisado en el registro domiciliario.
- EVI03 información volátil del portátil Toshiba (volcado de la memoriaRAM y resto de datos del sistema Windows).

A continuación, se solicitan las pruebas –evidencias a analizar- al funcionario encargado, se actualiza la información en el documento de cadena de custodia, se planifica el proceso de investigación y se prepara el entorno de trabajo.

Se comenzará realizando la adquisición y preservación de la información forense del

pendrive EVI02 para su posterior análisis en búsqueda de evidencias.

Posteriormente, se analizará la información volátil del sistema operativo Windows del portátil Toshiba adquirida durante el registro domiciliario y preservada en el DVD EVI03.

Adquisición de datos y análisis forense del pendrive - EVI02

Para realizar la investigación de un dispositivo usb de almacenamiento es necesario utilizar un sistema que no altere ni contamine la información del mismo cuando se conecta a la estación forense. Para ello, se utiliza la distribución Live GNU/LinuxUbuntu de Caine 7.0, que monta sus dispositivos automáticamente en modo lectura.

En primer lugar, se ejecuta VirtualBox y se arranca la máquina virtual Caine 7. Una vez aparece el escritorio de Caine se introduce al pendrive EVI02 y se monta el dispositivo (doble clic). El sistema le asigna el nombre USB 2.0 Flash Drive 2,1 Gb Volume en /dev/sdb (figura 14). Se comprueba que realmente solo tiene permisos de lectura.

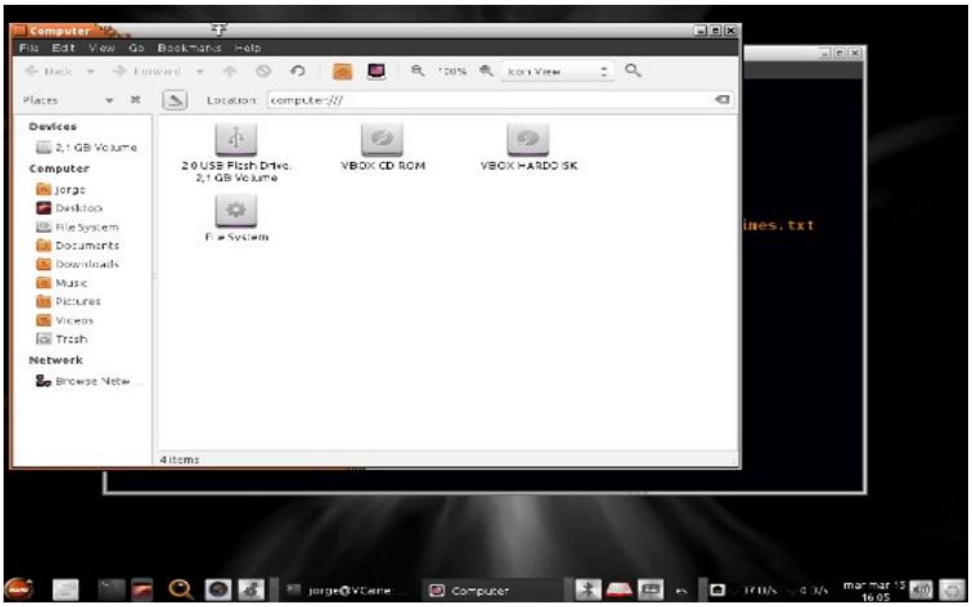


Figura 14: Pendrive EVI02 listo para la creación de copia forense.

Lo primero que se debe hacer es crear la imagen forense del dispositivo requisado comoEVI02, utilizando la herramienta GUYMAGER (figura 15) para adquisición de imágenes forenses. Esta herramienta gráfica permite crear en un solo proceso dos copias de imágenes forenses en distintos formatos –dd, raw, ev, ad..- del mismo dispositivo, una para trabajar y la otra como *backup*.

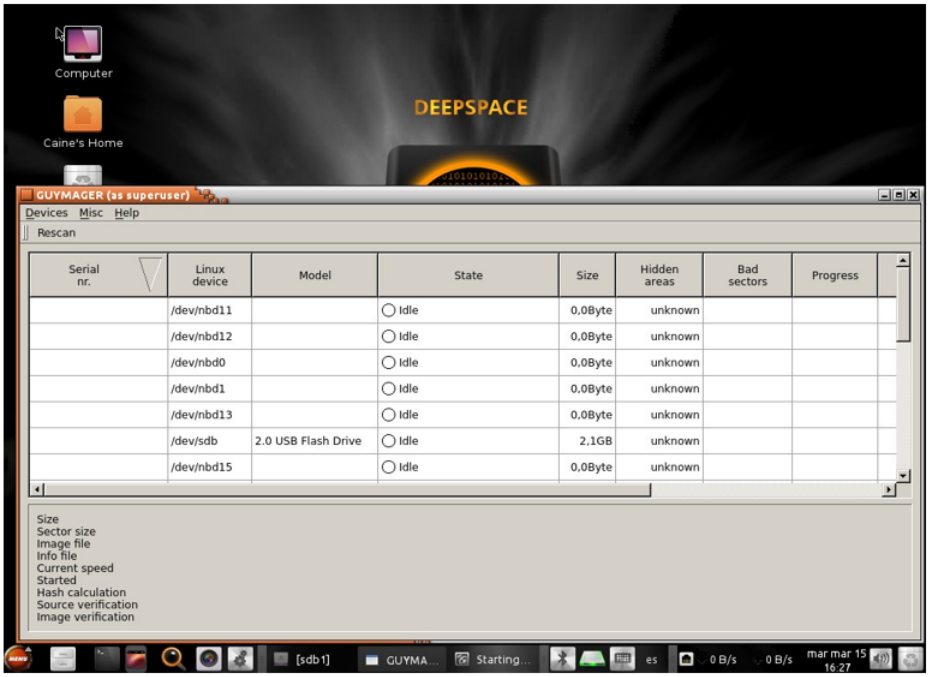


Figura 15: Software Guymager con el cual se creará doble copia de imagen forense del pendrive.

Las imágenes se crearán con el nombre **evidencia02** en los directorios (figura 16):

/home/jorge/Documents/Caso/Copia/CopiaTrabajar

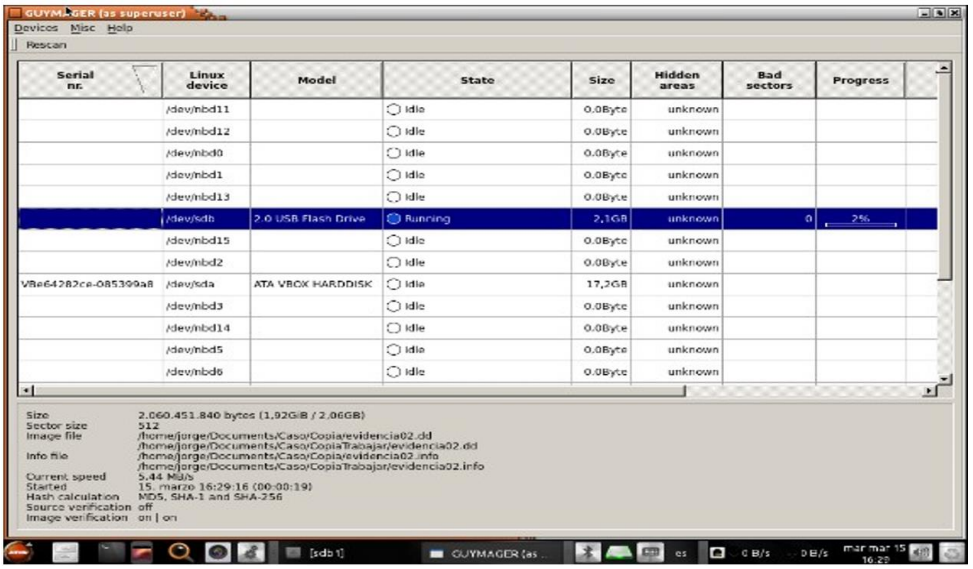


Figura 16: Software Guymager ejecutando la copia forense del pendrive.

Una vez creada la imagen forense del pendrive se debe comprobar los *hashes* correspondientes antes de continuar con la investigación. Si no coincidieran se deberá repetir el proceso.

Se utiliza la herramienta QuickHash que tienen la facilidad de comparar los *hashes* de los archivos y mostrar el resultado obtenido (figura 17). Se observa que el resultado obtenido el CORRECTO.

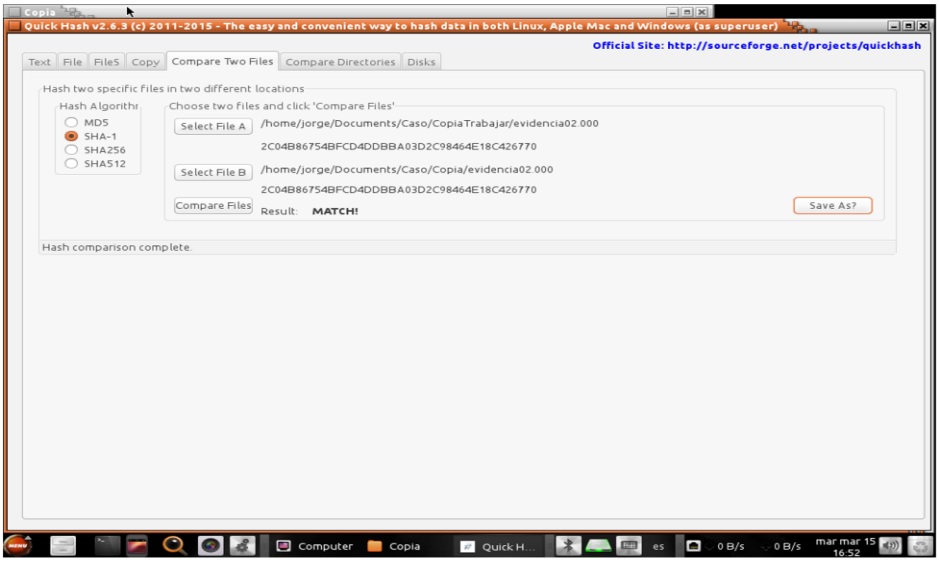


Figura 17: QuickHash utilizado para comparar los hashes de las imágenes creadas.

Ahora se procede a desmontar el pendrive para preservar su información y devolver al almacén actualizando el documento de la cadena de custodia. Posteriormente, se copia el resultado de los *hashes* al documento de investigación junto con el nombre de las imágenes creadas.

Luego, se cambia los permisos a modo solo lectura –*AccessData*- los directorios …/Copia y … /CopiaTrabajar para asegurar que durante la investigación no se alteren las imágenes forenses.

Para asegurar todavía más la imagen forense –evidencia02.000- se realiza una copia a DVD utilizando la herramienta de Linux Ubuntu **Brasero** (figura 18). Para poder utilizar el DVD en el sistema operativo Windows debe estar activada la opción *Joliet.* Se etiqueta con identificador **DVD EVI02** y se realiza el *hash* para anotarlo en el documento de la cadena de custodia.

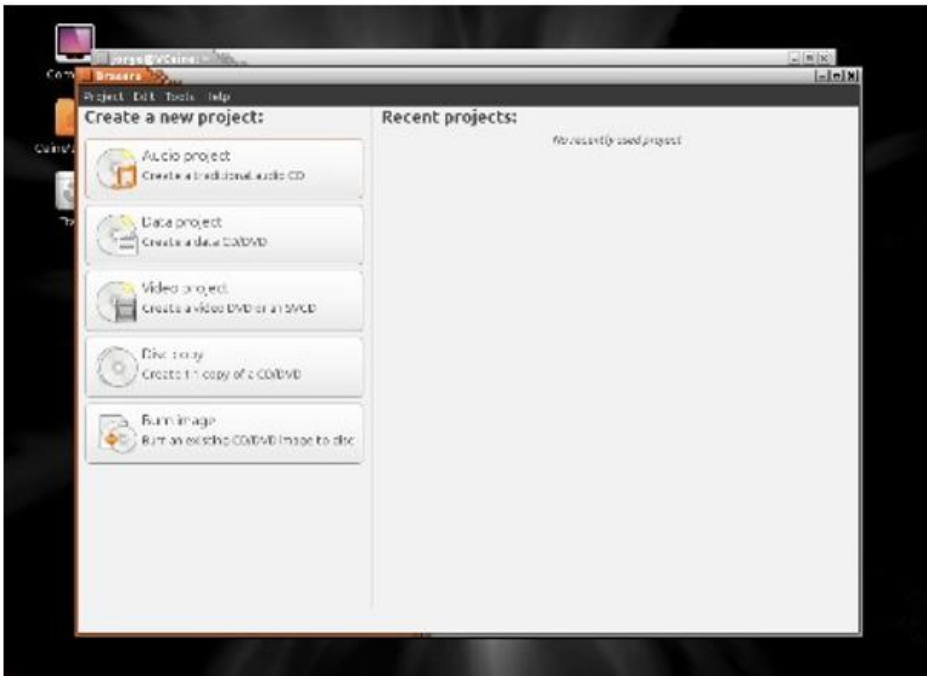


Figura 18: Software Brasero para crear DVD con la imagen evidencia02.

A partir de este momento ya estamos listos para comenzar el análisis forense de la imagen "evidencia02.000" del directorio …/CopiaTrabajar.

En primer lugar, con la herramienta **Autopsy** creamos un nuevo caso (figura 19) para realizar el análisis en busca de evidencias, archivos de fotografías y vídeo aportados como prueba original a la investigación.

Se añade un host y se crea la imagen forense a partir de la imagen "evidencia02.000", se observa como Autopsy ha reconocido que se trata de un disco con formato de sistema de ficheros FAT32 (figura 20).

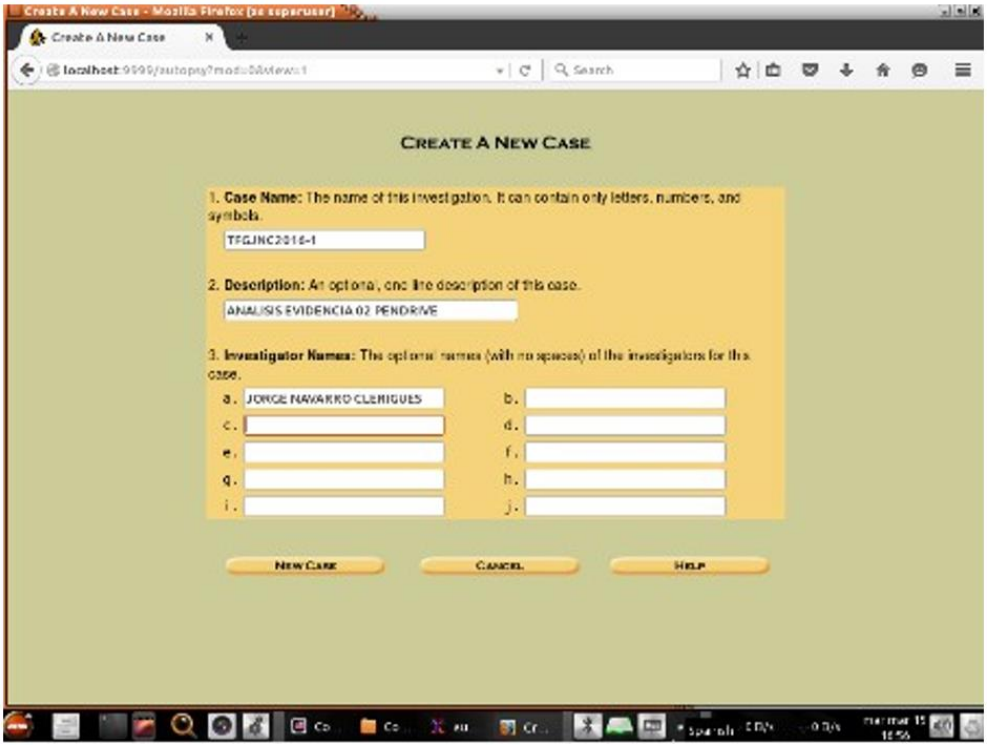


Figura 19: Creación de nuevo caso con Autopsy en Caine.

En la figura 20 se muestran los detalles de la imagen forense realizada del pendrive. Seguidamente pulsar ADD para elegir el volumen y comenzar el análisis pulsando el botón ANALYZE (figura 21).

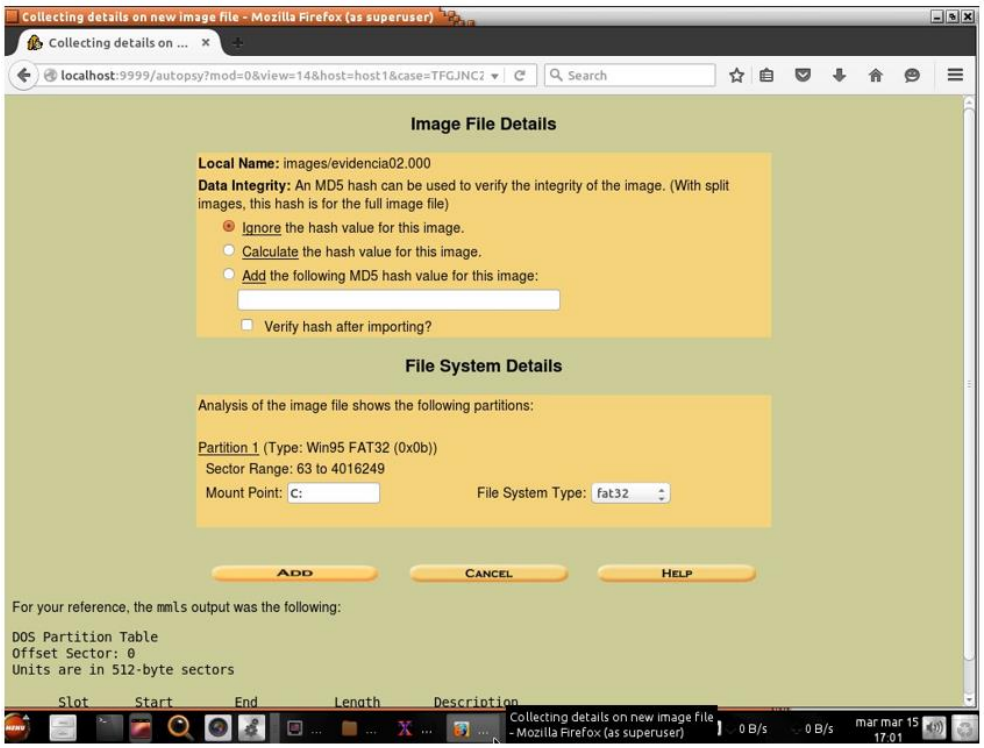


Figura 20: Añadir nueva imagen en Autopsy.

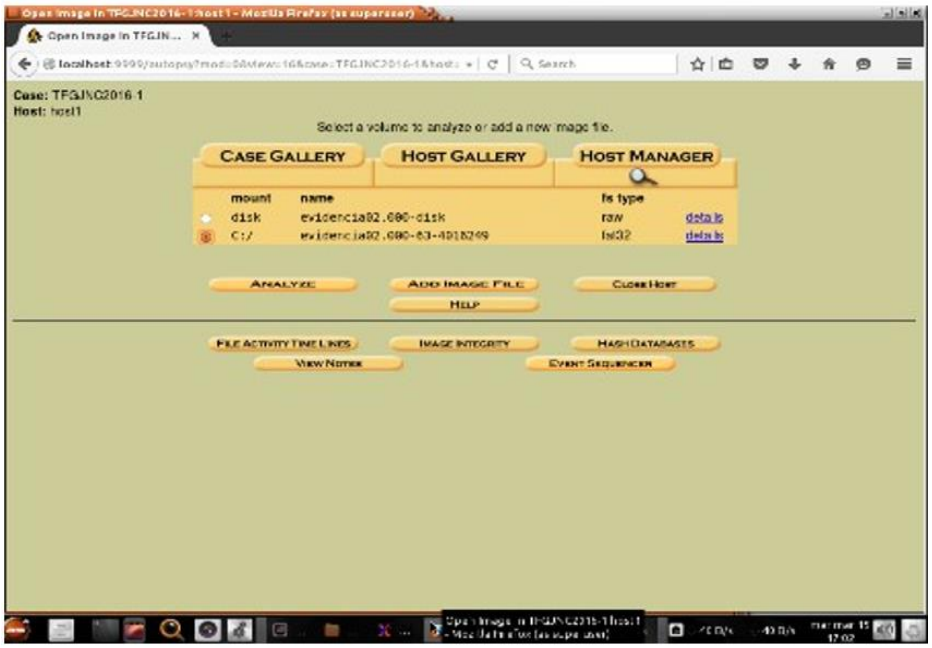


Figura 21: Seleccionar volumen a analizar en Autopsy.

El análisis con Autopsy nos revela que el pendrive no contiene ningún archivo. Se muestran las carpetas ocultas del sistema de archivos y la carpeta de archivos borrados

$OrphanFiles/. La columna META nos proporciona información de los metadatos de cada directorio así como sus hashes correspondientes (figura 22)

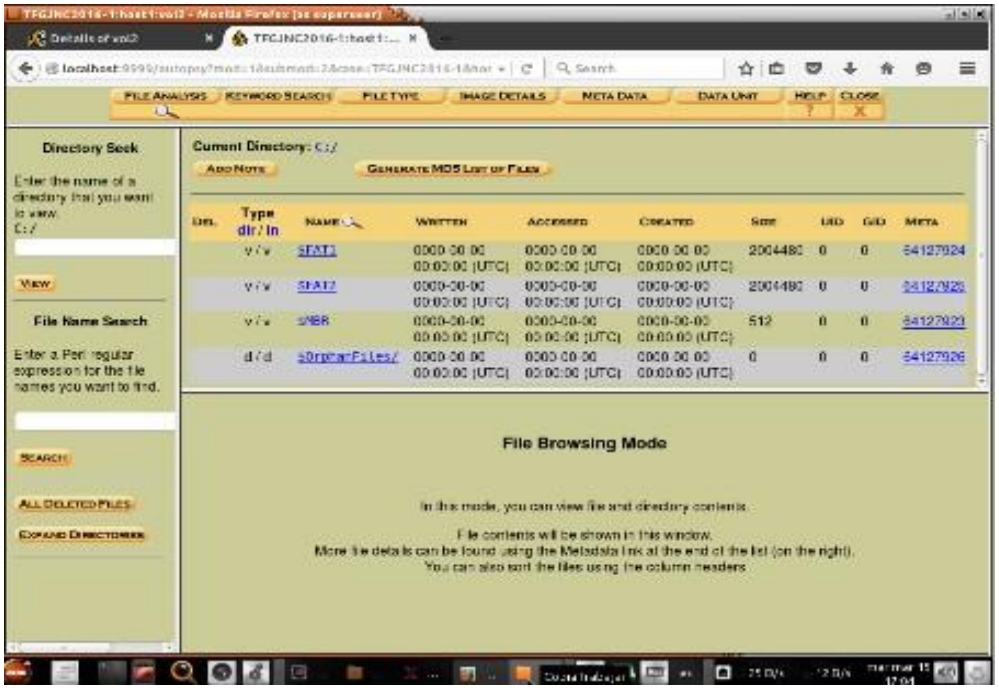


Figura 22: Resultado del análisis de ficheros en Autopsy.

Para la búsqueda evidencias, en File Name Search escribimos el nombre de algún archivo de fotografía, por ejemplo: “CAM” y pulsamos el botón SEARCH. No encuentra ningún archivo. Intentamos con otra expresión, por ejemplo: “JPG” y nos devuelve una lista de archivos borrados extensión JPG (figura 23). Lo mismo ocurre al pulsar el botón “ALL DELETED FILES”, nos devuelve la lista completa de archivos eliminados.

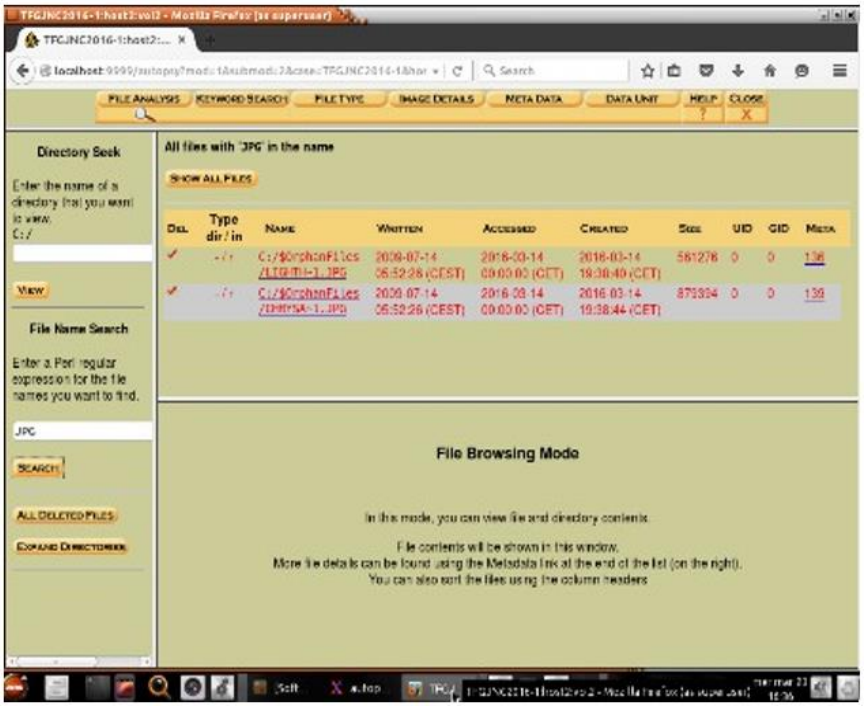


Figura 23: Archivos borrados del pendrive en Autopsy.

Ni el nombre, ni contenido, ni hash de los archivos hallados corresponden con las fotografías y video que se buscan.

Autopsy no aporta evidencias probatorias que demuestren que las pruebas originales –fotografías y vídeo- han sido almacenadas o eliminadas del pendrive alguna vez.

Se determina que el pendrive no contiene archivos visibles porque ha sido formateado o borrado mediante otra técnica. Los archivos hallados (figura 23) fueron borrados antes de formatear el dispositivo *usb* pero no corresponden con los buscados en la investigación.

En estos casos, se debe documentar todo el proceso realizado y utilizar otras herramientas de análisis de datos en “bruto” –que no tengan en cuenta el tipo de sistema de ficheros del volumen a analizar- como, por ejemplo, **Bulk Extractor Viewer** que posee, entre otros, un módulo para técnicas *caring en archivos JPG.*

Posteriormente, se realiza el análisis forense de la imagen “evidencia02.000” con la herramienta **Bulk Extractor Viewer** 1.5.5 como muestra la figura 24.

Ir a menú Tools -> Run Bulk Extractor … aparece una ventana donde seleccionamos la imagen a analizar, dejar por defecto los módulos que van ejecutarse durante el análisis (mails, jpg, urls, zip, hiberfile, etc) e introducir los nombres de las imágenes Copia y CopiaTrabajar para comprobar los *hashes* automáticamente después del análisis de datos.

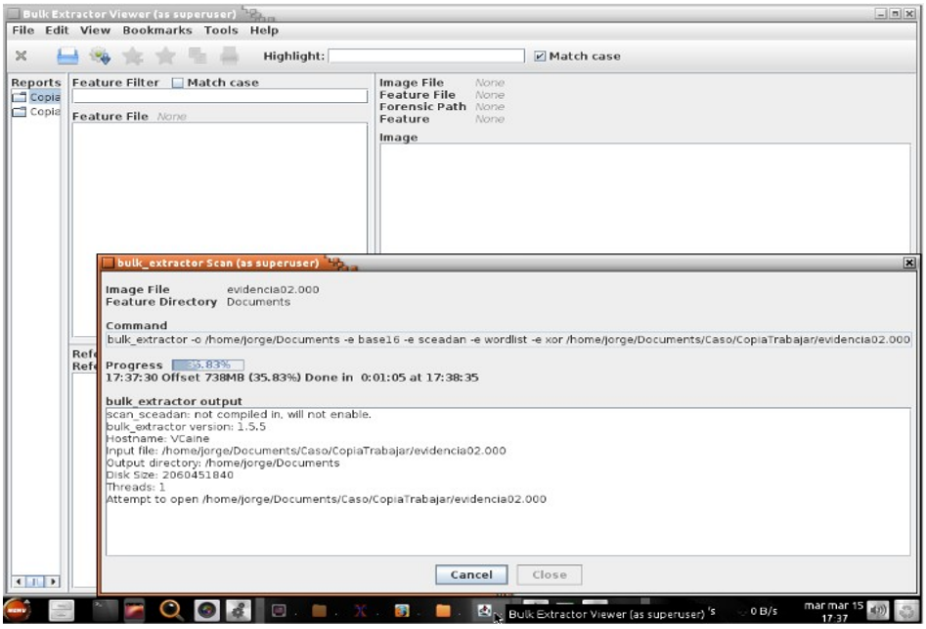


Figura 24: Bulk Extractor Viewer para análisis en bruto.

Bulk Extractor Viewer genera varios reportes de texto con los resultados obtenidos en el directorio /home/jorge/Documents y un directorio con los archivos jpg hallados.

exif.txt

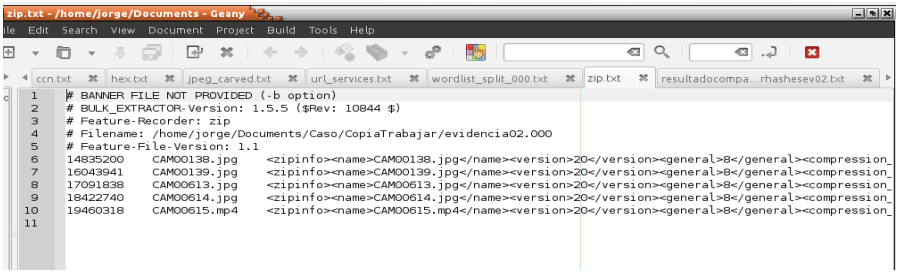


Figura 25: Bulk Extractor Viewer. Resultado de Exif - Metadatos.

Zip.txt

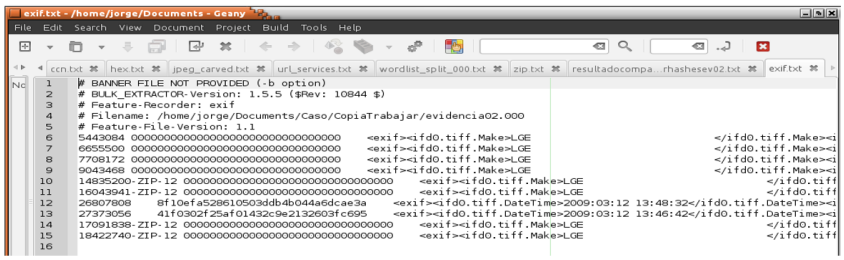


Figura 26: Bulk Extractor Viewer. Resultado de archivos zip encontrados.

resultadocompararhashesev02.txt

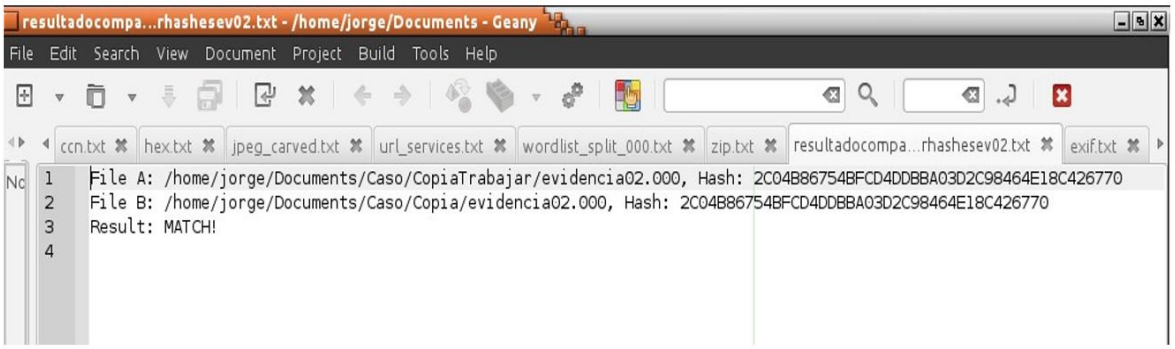


Figura 27: Bulk Extractor Viewer. Resultado de comparativa de hashes de imágenes forenses.

En la figura 28 se muestra el contenido del archivo ZIP recuperado, con las cuatro fotografías y el vídeo.

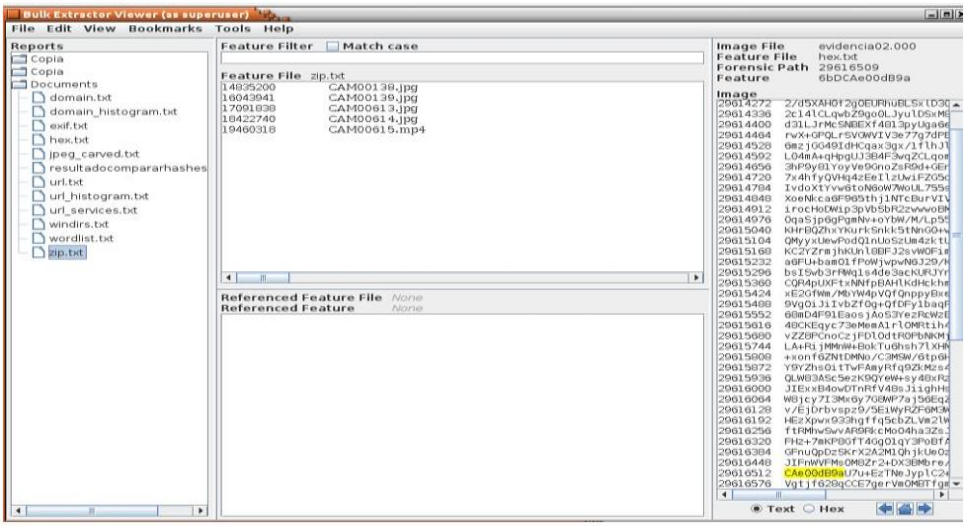


Figura 28: Bulk Extractor Viewer. Contenido de archivo zip recuperado.

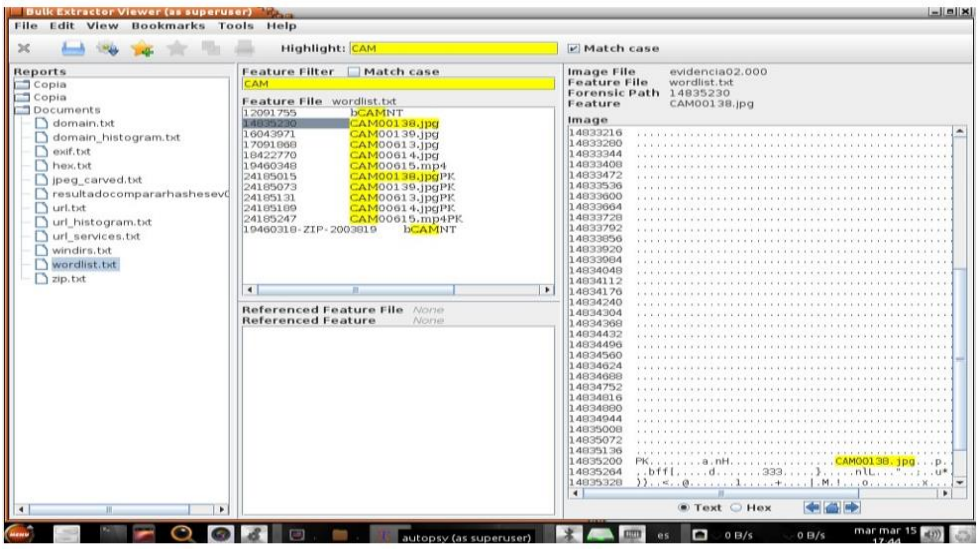


Figura 29: Bulk Extractor Viewer. Ficheros recuperados - wordlist.

En la figura 29 se muestra el contenido del directorio "…/jpeg_carved/000" con las fotografías recuperadas.

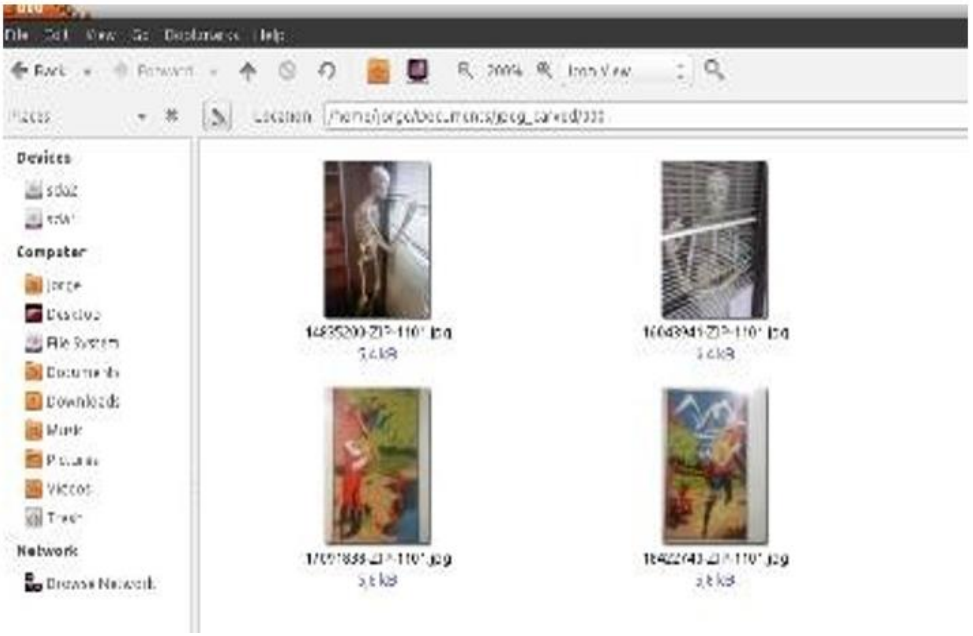


Figura 30: Bulk Extractor Viewer. Fotografías recuperadas mediante Carving.

Los resultados obtenidos se copian a DVD para reportarlos al caso, entre otra información, los archivos con las imágenes fotográficas recuperadas del pendrive.

Dichas fotografías corresponden con las pruebas originales al poder ser visionadas y comprobar que son idénticas, el vídeo ha sido imposible recuperarlo, pero si se tiene la información de sus metadatos con su nombre, tamaño, fecha creación, etc.

El módulo *Exif* (figura 25) ha proporcionado los metadatos de los archivos CAMxxx.JPG en los que se observa la marca y modelo del móvil/cámara fotográfica utilizada, móvil LG modelo E400.

Además, se han obtenido al final del análisis los hashes de las imágenes forenses de trabajo y copia preservada comprobando que son idénticos, de esta forma se asegura la validez de la investigación.

El análisis forense digital de la evidencia02 (contenido del pendrive) con la herramienta Bulk Extractor Viewer si nos proporciona información suficiente para afirmar que las fotografías y vídeo aportados como prueba original al caso han sido almacenados y, posteriormente mediante formateo u otra técnica anti-forense, eliminados del pendrive. Además, se creó un archivo comprimido zip con dichos archivos.

Análisis forense digital de la información volátil del portátil - EVI03

Se solicita al funcionario responsable de la custodia de evidencias uno de los dos DVD EVI03 para proceder a su análisis en laboratorio. Se actualiza el documento de cadena de custodia y se planifica la investigación.

Como la información proporcionada está almacenada en DVD -protegido contra escritura- no es obligado trabajar en Linux con Caine 7.0. Con fines didácticos, se van a utilizar en este apartado herramientas y utilidades forenses digitales desarrolladas para Windows. Apuntar que la información adquirida con Investigador 2.0 resultado de la investigación está en ficheros *html* y de texto, solamente se debe realizar la búsqueda de texto / palabras / *strings* relevantes en la investigación. Se deben buscar indicios probatorios que demuestren el intento de acceso a la cuenta de correo electrónico de Amparo –amparo.xiva@gmail.com- desde el portátil Toshiba, así como cualquier otra información relacionada con la investigación, como por ejemplo, si el pendrive ha sido utilizado en el portátil, si se han descargado las fotografías y video, si se ha ocultado información intencionadamente, si conoce la contraseña de la cuenta de correo, si se han utilizado herramientas anti-forense, etc.

Análisis del volcado de la memoria RAM

La figura 31 muestra los archivos adquiridos en la captura de la información en memoria RAM del portátil y copiados por duplicado en DVD para su preservación.

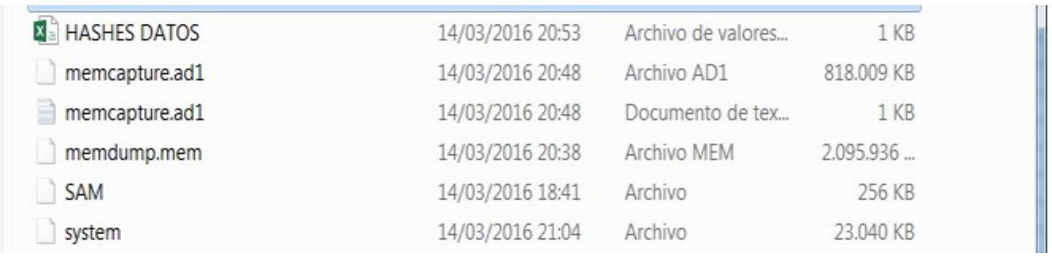


Figura 31: Datos forenses de EVI03 en DVD.

Con la herramienta AccessData FTK Imager, en primer lugar, se añaden los archivos con datos forenses y se crea la imagen (figura 32).

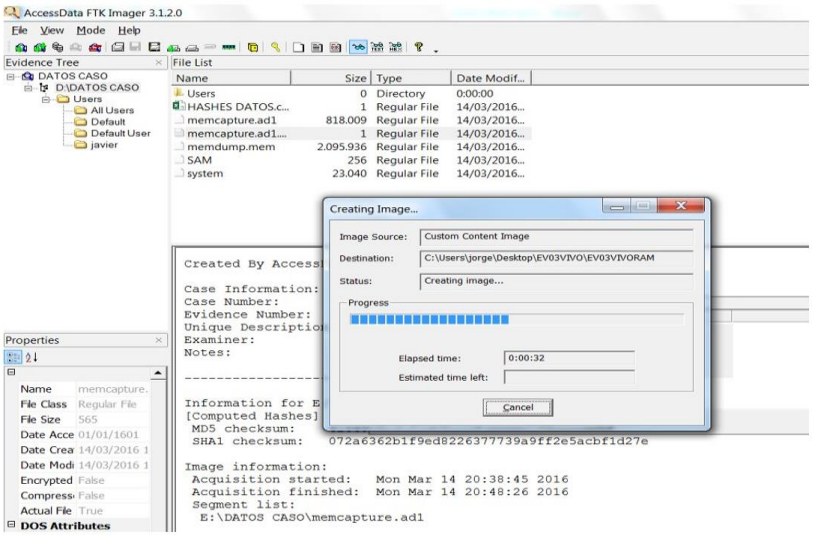


Figura 32: FTK Imager para añadir datos forenses de EVI03 y crear la imagen.

Sumario del proceso

Case Number: EV03FTKVOLATILAMPARO
Evidence Number: 03 Examiner:
JORGE NAVARRO
Notes: DATOS VIVO PORTATIL EVIDENCIA 03 RAM
Information for C:\Users\jorge\Desktop\EV03VIVO\EV03VIVORAM.ad1:[Custom Content Sources]
DATOS CASO:D:\DATOS CASO|memcapture.ad1(Exact) DATOS CASO:D:\DATOS CASO|memdump.mem(Exact) DATOS CASO:D:\DATOS CASO|SAM(Exact)
DATOS CASO:D:\DATOS CASO|system(Exact)
DATOS CASO:D:\DATOS CASO|memcapture.ad1.txt(Exact)
[Computed Hashes]
MD5 checksum: bc39fb76b06e04b0a78b88b63a719a07
SHA1 checksum: 0bb02c73299136ced8c182ed831c66aa7dca4766Image information:
Acquisition started: Tue Mar 15 14:26:29 2016
Acquisition finished: Tue Mar 15 14:30:58 2016
Segment list:
C:\Users\jorge\Desktop\EV03VIVO\EV03VIVORAM.ad1
C:\Users\jorge\Desktop\EV03VIVO\EV03VIVORAM.ad2

A continuación, se marca la opción “Show text only” y se ejecuta”Find …” para buscar lacadena “amparo.xiva” en el volcado de memoria RAM. El resultado ha sido positivo, la cadena se ha encontrado varias veces. Extracto del resultado:

> *.].7.E*
>
> *https://accounts.google.com/**ServiceLoginEmailamparo.xiva@gmail.comPass wd**https://accounts.google.com/*

También se encuentran evidencias de que se ha introducido la contraseña de la cuentade Amparo –amparo.xiva@gmail.com- como demuestra la figura 33.

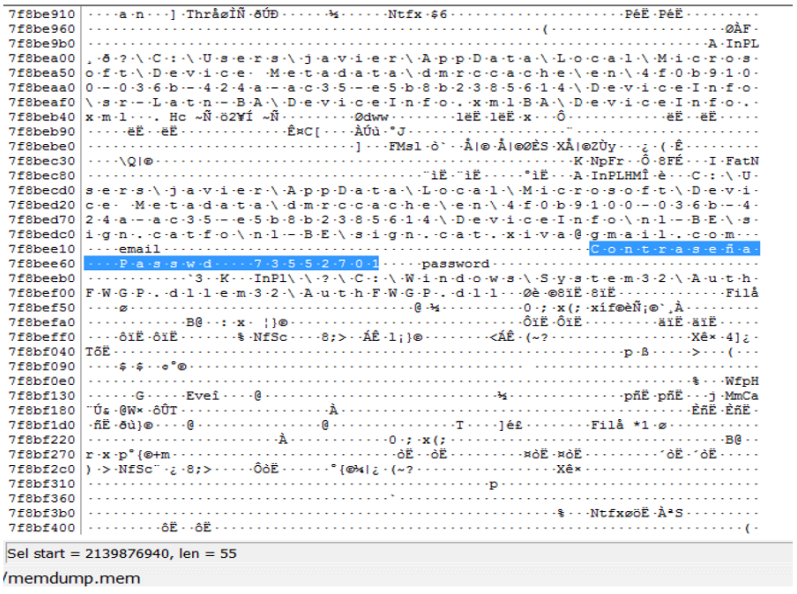


Figura 33: FTK Imager. Contraseña del correo en la RAM.

También se busca por nombre o extensión de archivo, por ejemplo, “CAM” o “JPG” y se observa que bajo *library folder* - unidad E:\ existen los nombres de los archivos que son similares a las fotografías y vídeo de la prueba original. Y además, el fichero ZIP con los archivos comprimidos “FOTOSYVIDEO.ZIP” (figura 34).

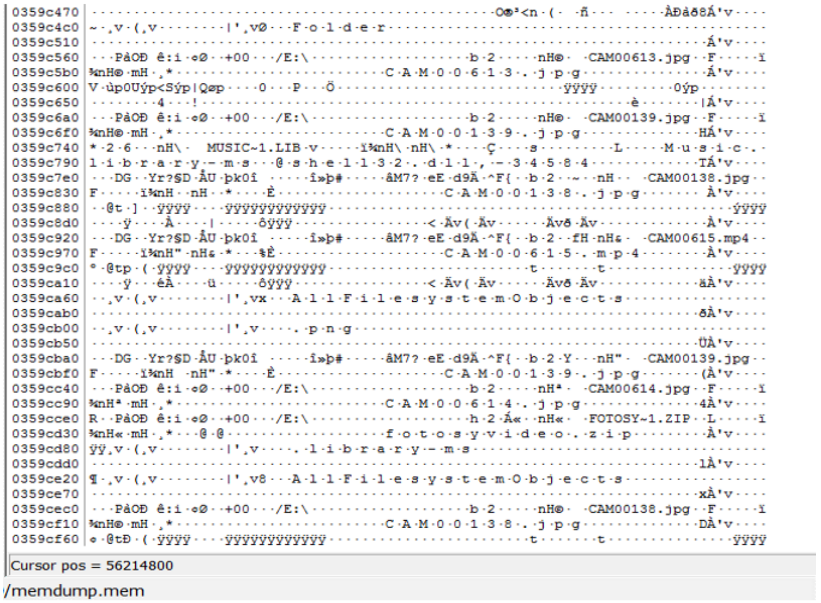


Figura 34: Unidad E:\ y nombre de las fotografías, video y zip.

Se encuentran evidencias que demuestran que el pendrive requisado se ha introducido en el portátil Toshiba como se observa en la figura 35, USb 2.0 … y número de serie.

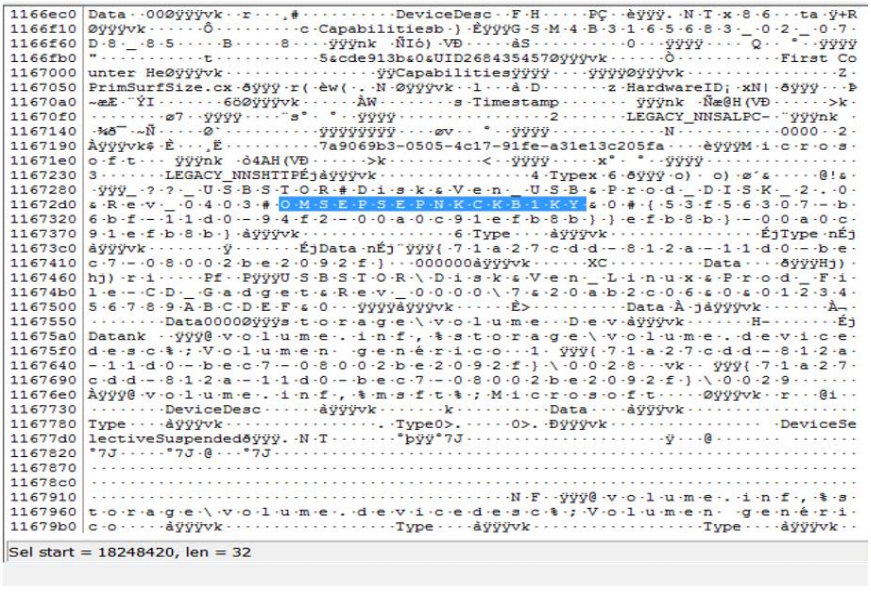


Figura 35: Número de serie del pendrive EVI02 introducido en el portátil.

Se buscan evidencias del uso de técnicas anti-forense, y se observa que se han realizado búsquedas en internet sobre “esteganografía” y se ha accedido a la web de descarga de *softonic* con la intención de descargar el programa “Camouflage” utilizado para ocultar información mediante técnicas de esteganografía[30] (figura 36).

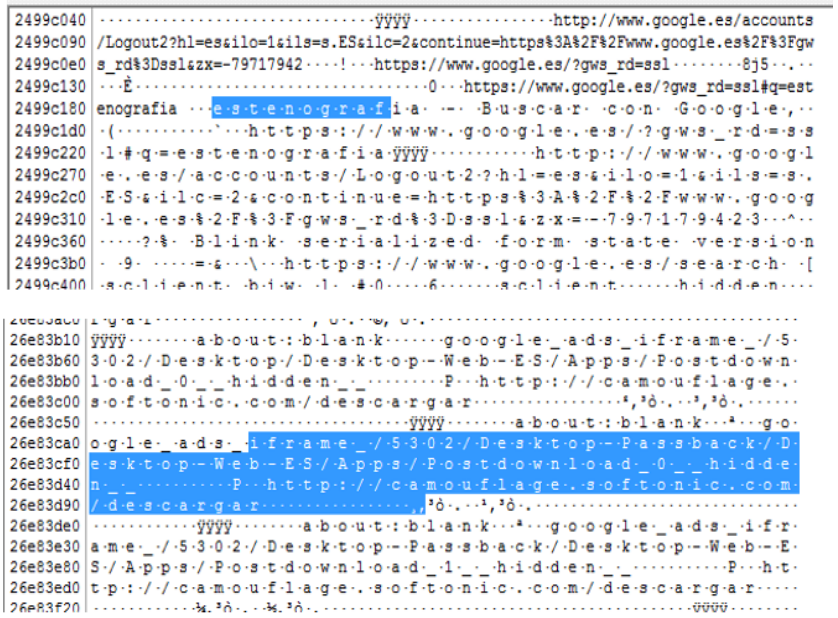


Figura 36: Búsqueda y descarga de programas de esteganografía - Camouflage.

Esta información resulta muy útil para el equipo forense encargado del análisis de los discos duros del portátil Toshiba, además, evidencian el interés por estas técnicas de ocultación de información, utilizada, entre otros, por pederastas para camuflar contenido de pornografía infantil, por redes criminales, en ciberespionaje, etc.

Análisis de la información de Windows del portátil

Para finalizar con el análisis de la información volátil del portátil vamos a localizar evidencias referentes al caso en los ficheros reportados con la herramienta Investigador 2.0. Recordar que éstos se encuentran almacenados en la carpeta RESULTS del DVD EVI03.

De toda la información investigada se extrae la que es relevante para el caso. A continuación, se detalla el resultado del análisis.

En primer lugar, se realiza el hash de todos los documentos reportados con el fin de garantizar lavalidez de las pruebas en el juicio. Para ello con la herramienta HashMyFiles elegiremos la carpeta Results y automáticamente se realiza el hash de todos los archivos de prueba.

Ejemplo de un fichero de salida proporcionado por HashMyFiles:

Nombre de archivo: mspass.html
Ruta completa : D:\results\mspass.html
MD5 : ec6bdbe0fafcdaca1f0927cb8bad7418
SHA1 : 6947a6c4cfbc48c2566d0e4bacf0fa34d76c13e2
CRC32 : b5f01e1b
SHA-256 : 2e9a49fb497aa8c3951fed9a93728ebe1a751f8d117ac49dc69a79e41053b728SHA-
512 :
c9654bb68edae2f044ca723180c6a594f0ff703bd331aff30dcf4879fa4835c16322a3bb2ddc1b08271
6557f0b121656599ad82c063b44bda1b9385bb241ee6b
SHA-384 :
4d339d8683b6c11c0020e6930d0160fc4cb9faa674ac9aea2b2a1cd81cf08bf5405bf026e44d353b7f b242480c2a8a1a
Fecha de modificación: 14/03/2016 21:11:02
Fecha de creación: 14/03/2016 21:11:02
Tamaño 432
Versión del archivo:
Versión del producto:
Idéntico :
Extensión : html
Atributos del archivo: R

A continuación, se estudia el contenido de los ficheros de datos forenses adquiridos:

systeminfo.txt

Información del portátil
Nombre de host: LAPTOP-TOSHIBA
Nombre del sistema operativo: Microsoft Windows 7 Ultimate
Versión del sistema operativo: 6 1.7600 N/D Compilación 7600
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Estación de trabajo independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
Propiedad de: Javier
Organización registrada: YoReparoTuPC
Id. del producto: 00426-OEM-8992662-00400
Fecha de instalación original: 30/07/2013,
21:36:54
Tiempo de arranque del sistema: 14/03/2016,
18:41:06Fabricante del sistema: TOSHIBA
Modelo el sistema: Satellite Pro P200
Tipo de sistema: X86-based PC

Procesador(es): 1 Procesadores instalados.
[01] : x64 Family 6 Model 15 Stepping 11 GenuineIntel ~2201 Mhz
Versión del BIOS: TOSHIBA V2.70, 13/12/2010
Directorio de Windows: C:\Windows
Directorio de sistema:
C:\Windows\system32
Dispositivo de arranque: \Device\HarddiskVolume3
Configuración regional del sistema: es; Español (internacional)
Idioma de entrada: es; Español (tradicional)
Zona horaria: (UTC+01:00) Bruselas, Copenhague, Madrid, París
Cantidad total de memoria física: 2.046 MB
Memoria física disponible: 1.369 MB
Memoria virtual: tamaño máximo: 4.093 MB
Memoria virtual: disponible: 3.078 MB
Memoria virtual: en uso: 1.015 MB
Ubicación(es) de archivo de paginación: C:\pagefile.sys
Dominio: YOREPAROTUPC
Servidor de inicio de sesión: \\LAPTOP-TOSHIBA
Revisión(es): 1 revisión(es) instaladas. [01]: KB958488
Tarjeta(s) de red: 3 Tarjetas de interfaz de red instaladas.
[01] : Intel(R) Wireless WiFi Link 4965AGN
Nombre de conexión: Conexión de red inalámbricaDHCP habilitado: Sí
Servidor DHCP: 192.168.1.1
Direcciones IP [01]: 192.168.1.133
[02]: Realtek PCIe FE Family Controller
Nombre de conexión: Conexión de rea local
Estado: Hardware ausente
[03]: VirtualBox Host-Only Ethernet Adapter
Nombre de conexión: VirtualBox Host-Only Network
Estado: Hardware ausente

UsbDview: Obtiene evidencias de que el pendrive USB 2.0.. con número de serie mostrado en la figura 37 corresponde con el investigado y ha sidoutilizado en el portátil Toshiba.

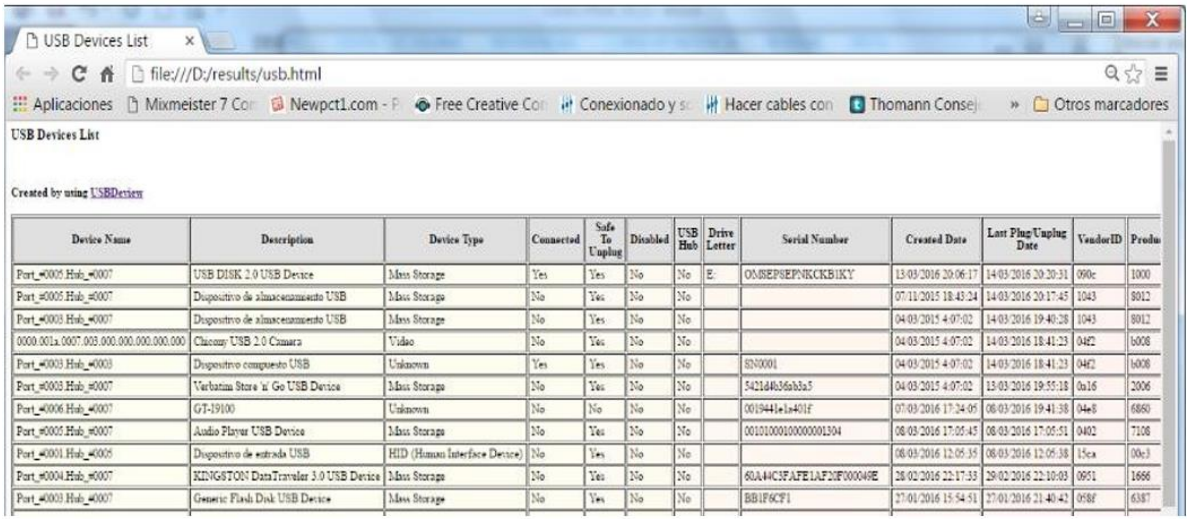


Figura 37: Resultado de la aplicación UsbDview.

ChromePass: Obtiene las contraseñas almacenadas en Chrome. Se evidencia que desde este portátil se ha accedido a la cuenta de amparo y que se conocía evidentemente la contraseña (figura 38).

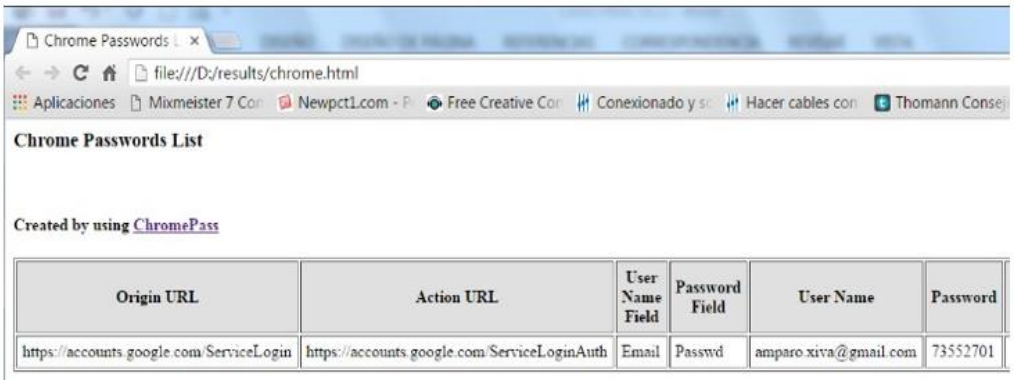
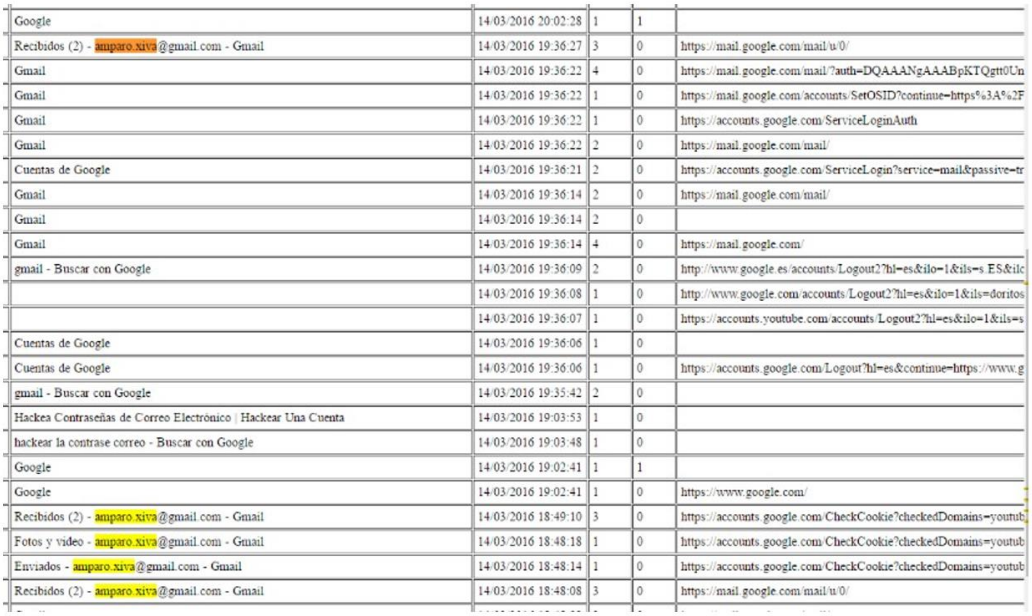


Figura 38: Resultado de la aplicación ChromePass. Contraseña del correo.

ChromeHistory: Se observa en la figura 39 como desde este portátil se ha accedido a la carpeta de correos Enviados y abierto el mensaje de asunto Fotos y vídeo.



Google	14/03/2016 20:02:28	1	1	
Recibidos (2) - amparo.xiva@gmail.com - Gmail	14/03/2016 19:36:27	3	0	https://mail.google.com/mail/u/0/
Gmail	14/03/2016 19:36:22	4	0	https://mail.google.com/mail/?auth=DQAAANgAAABpKTQgtt0Un
Gmail	14/03/2016 19:36:22	1	0	https://mail.google.com/accounts/SetOSID?continue=https%3A%2F
Gmail	14/03/2016 19:36:22	1	0	https://accounts.google.com/ServiceLoginAuth
Gmail	14/03/2016 19:36:22	2	0	https://mail.google.com/mail/
Cuentas de Google	14/03/2016 19:36:21	2	0	https://accounts.google.com/ServiceLogin?service=mail&passive=tr
Gmail	14/03/2016 19:36:14	2	0	https://mail.google.com/mail/
Gmail	14/03/2016 19:36:14	2	0	
Gmail	14/03/2016 19:36:14	4	0	https://mail.google.com/
gmail - Buscar con Google	14/03/2016 19:36:09	2	0	http://www.google.es/accounts/Logout2?hl=es&ilo=1&ils=s.ES&ilc
	14/03/2016 19:36:08	1	0	http://www.google.com/accounts/Logout2?hl=es&ilo=1&ils=doritos
	14/03/2016 19:36:07	1	0	https://accounts.youtube.com/accounts/Logout2?hl=es&ilo=1&ils=s
Cuentas de Google	14/03/2016 19:36:06	1	0	
Cuentas de Google	14/03/2016 19:36:06	1	0	https://accounts.google.com/Logout?hl=es&continue=https://www.g
gmail - Buscar con Google	14/03/2016 19:35:42	2	0	
Hackea Contraseñas de Correo Electrónico | Hackear Una Cuenta	14/03/2016 19:03:53	1	0	
hackear la contrase correo - Buscar con Google	14/03/2016 19:03:48	1	0	
Google	14/03/2016 19:02:41	1	1	
Google	14/03/2016 19:02:41	1	0	https://www.google.com/
Recibidos (2) - amparo.xiva@gmail.com - Gmail	14/03/2016 18:49:10	3	0	https://accounts.google.com/CheckCookie?checkedDomains=youtub
Fotos y video - amparo.xiva@gmail.com - Gmail	14/03/2016 18:48:18	1	0	https://accounts.google.com/CheckCookie?checkedDomains=youtub
Enviados - amparo.xiva@gmail.com - Gmail	14/03/2016 18:48:14	1	0	https://accounts.google.com/CheckCookie?checkedDomains=youtub
Recibidos (2) - amparo.xiva@gmail.com - Gmail	14/03/2016 18:48:08	3	0	https://mail.google.com/mail/u/0/

Figura 39: Resultado de la aplicación ChromeHistory. Acceso del correo.

Otra información forense de interés obtenida durante la adquisición de evidencias:

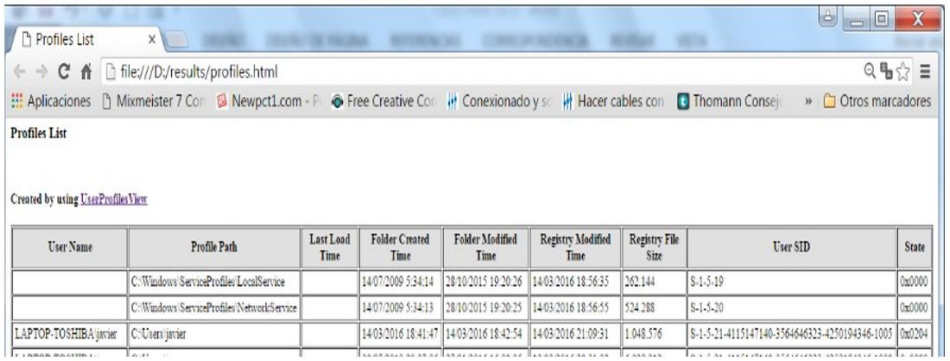


Figura 40: Usuarios de Windows en UserProfileView.

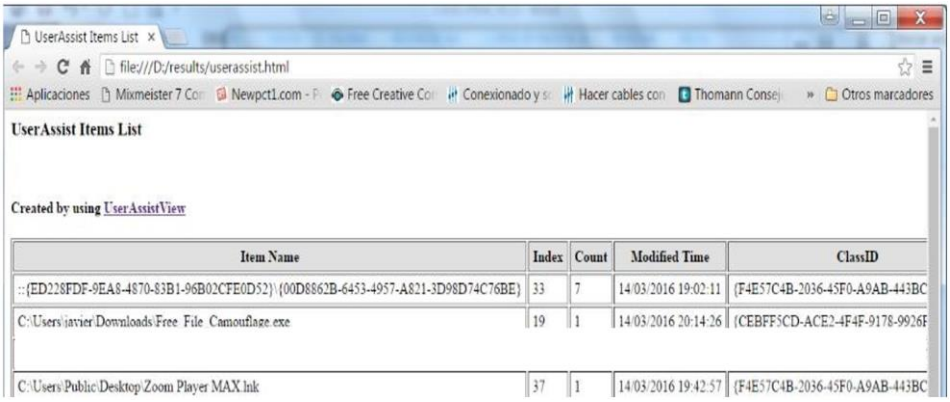


Figura 41: Programas ejecutados por usuario activo con UserAssistView.

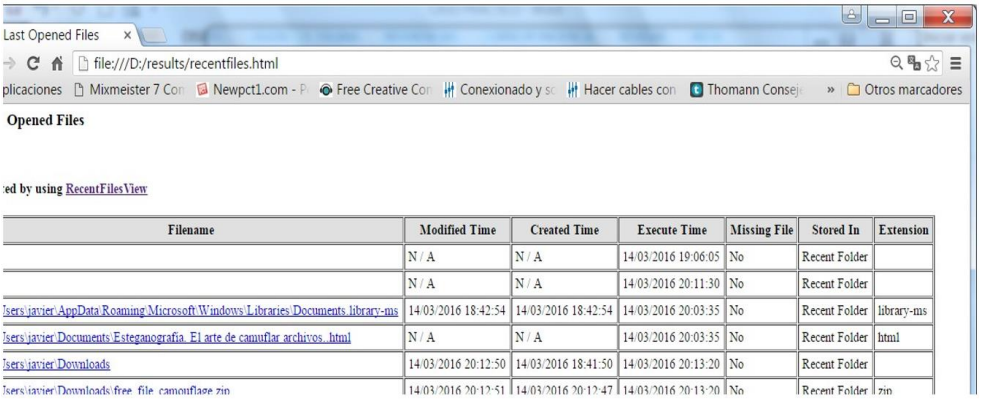


Figura 42: Ficheros abiertos recientemente – RecentFilesView.

Se observa que el usuario de Windows "javier" ha ejecutado el programa "Camouflage", entre otros, recientemente en el portátil, ver figuras 41, 42 y 43.

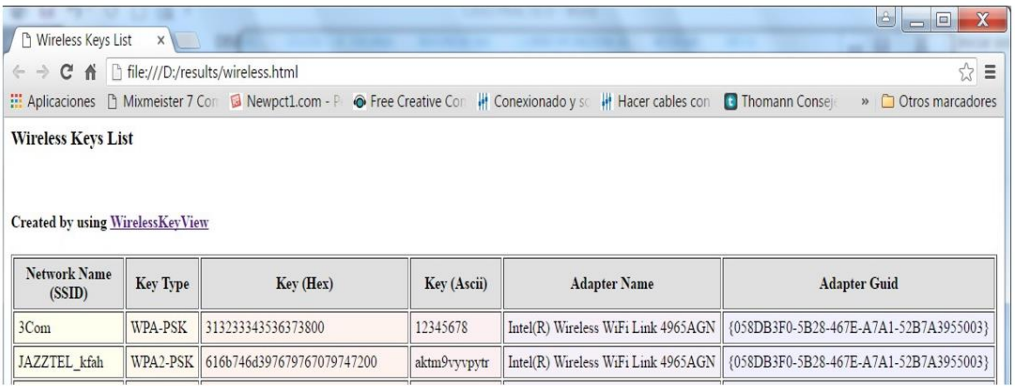


Figura 43: Resultado de la aplicación WirelessKeyView.

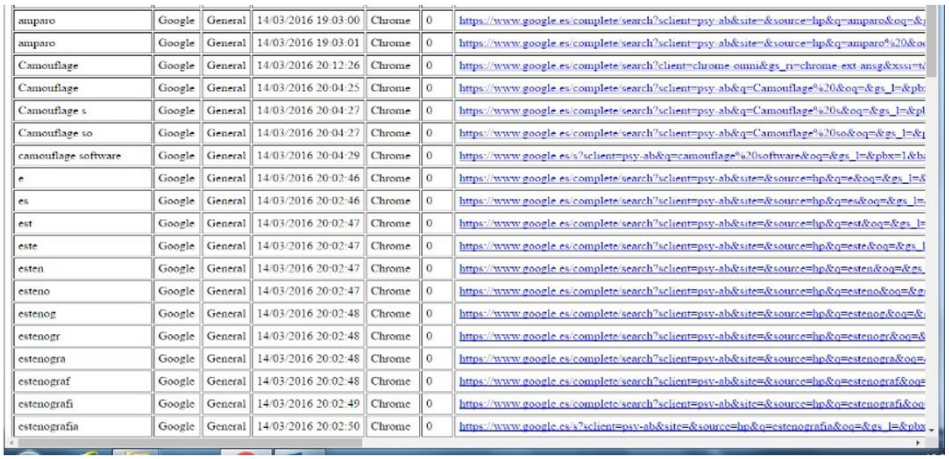


Figura 44: Resultado de búsquedas realizadas - MyLastSearch.

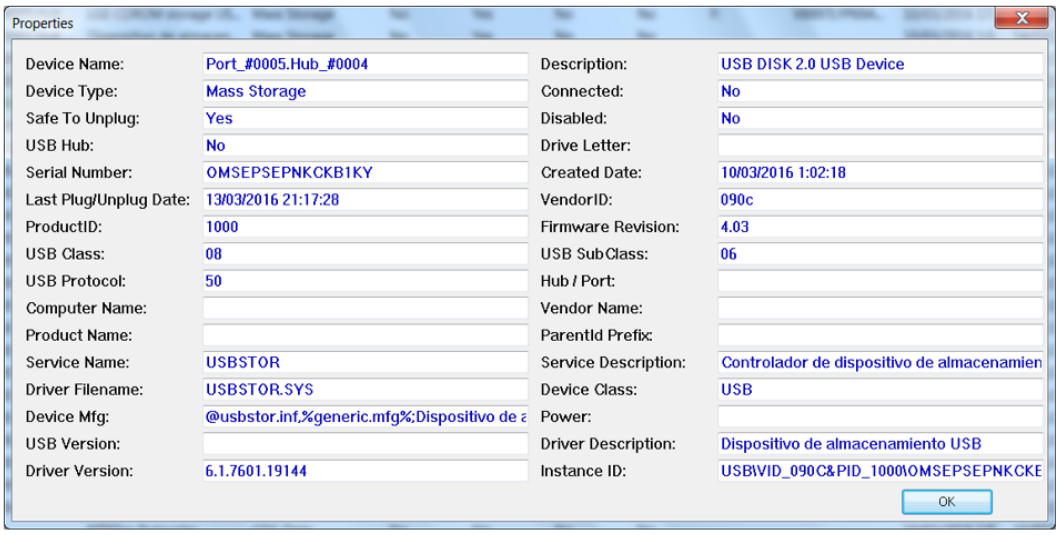


Figura 45: Número de serie del pendrive investigado - UsbDView.

Conclusiones de la investigación forense de la información volátil evi03

El resultado de la investigación forense realizada en laboratorio de la información volátil recopilada –EVI03- en el portátil Toshiba con nombre LAPTOP-TOSHIBA\\ determina que:

1. El usuario de Windows con nombre "javier" e identificador "S-1-5-21-4115147140- 3564646323-4250194346-1005" ha accedido con el navegador Chrome a la cuenta de correo "amparo.xiva@gmail.com" y que evidentemente conoce la contraseña de acceso a dicha cuenta y ésta ha sido además tecleada, registrada y mostrada en los resultados "735527…".

2. Se ha accedido a la carpeta Enviados de dicha cuenta, se ha abierto el mensaje con Asunto "Fotos y vídeo" y se han descargado los adjuntos en formato ZIP conel nombre "Fotos y video.zip" y además cada uno por separado:

   Archivos en formato JPG con nombre CAM00138, CAM00139, CAM00613, CAM00614.
   Archivo formato vídeo MP4 con nombre CAM00615.

3. El pendrive requisado como prueba Ev02 con número de serie OMSEPSEP… ha sido utilizado en el portátil Toshiba.

4. Se han realizado búsquedas en internet referentes a técnicas de esteganografía –ocultar información- y se ha descargado, instalado y utilizado el programa Camouflage (utilizado para camuflar ficheros en otros, por ejemplo, fotografías en imágenes de fondo de Windows, un texto en una imagen o para cifrar archivos, etc).

Consideraciones de la investigación forense del pendrive – evi02

En este punto se podría dar por satisfactoria la investigación forense puesto que se ha evidenciado lo requerido en el expediente del procedimiento judicial. No obstante, a la vista de los resultados obtenidos del análisis del pendrive -evi02-, en los que se ha localizado un vídeo que no ha podido ser recuperado y además se ha descargado e instalado el programa Camouflage utilizado para ocultar información, según ofrecen los resultados de la investigación de la evi03, es necesario ampliar la investigación forense con otras herramientas desarrolladas principalmente para este tipo de casos.

A continuación, se realiza el análisis forense de la imagen adquirida del pendrive y almacenada en DVD –evi02-. El objetivo es localizar evidencias de ocultación deinformación e intentar recuperar el vídeo u otros archivos relevantes utilizando herramientas forenses desarrolladas para entornos Windows como Autopsy 4.0, OsForensics 3.3 x64 y Xteg.

Ampliación del análisis forense del pendrive - EVI02 con Autopsy

Autopsy 4.0 funciona en entornos Windows y es muy útil para el tipo de investigación que se va a realizar: localizar y extraer archivos eliminados o dañados de un dispositivo *usb* y localizar archivos ocultos con técnicas estenográficas, entre otras.

El modo de trabajar en Autopsy es:

Crear el caso a investigar.

Añadir la imagen forense con la información a analizar:

Imagen almacenada en DVD “evidencia02”.

Ejecutar los módulos de investigación *–Ingest Módules-. Nada más cargar la imagen –fuente de datos- automáticamente se lanzan los módulos deinvestigación.*

Localizar en el árbol de resultados aquellas evidencias relevantes para el caso.

Crear informe de resultados.

Una vez cargada la imagen forense “evidencia02” y finalizada la ejecución de los módulos analíticos, procedemos a estudiar los resultados obtenidos (figura 46).

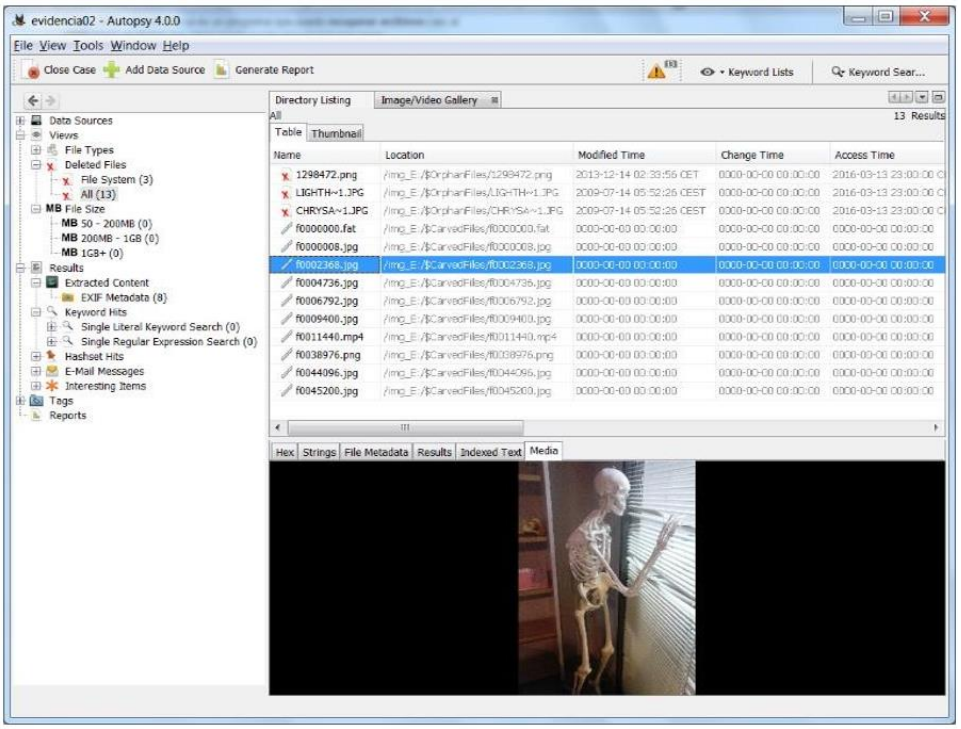


Figura 46: Análisis forense del pendrive con Autopsy.

En principio, la información encontrada por Autopsy 4.0 es similar a la obtenida anteriormente, las tres imágenes borradas, las cuatro fotografías, el vídeo … (figura 47).

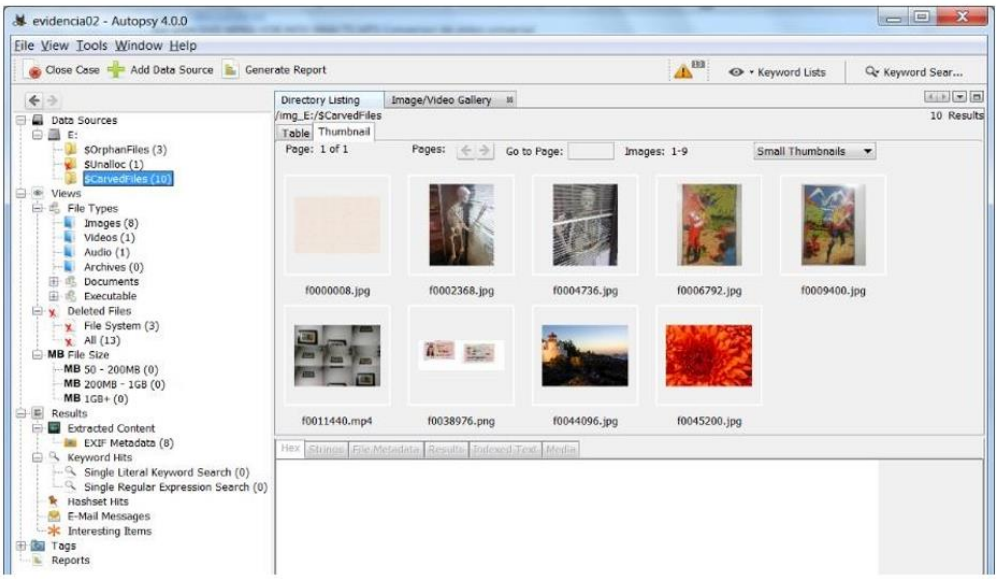


Figura 47: Archivos encontrados con Autopsy.

Utilizamos la función exportar para intentar recuperar los archivos encontrados. Se han exportado todos los archivos (figura 48) y éstos se abren correctamente. Se comprueba que hasta el vídeo se visiona correctamente y su contenido es similar al vídeo de la prueba original.

Vemos que además se han exportado otros archivos como “README”.

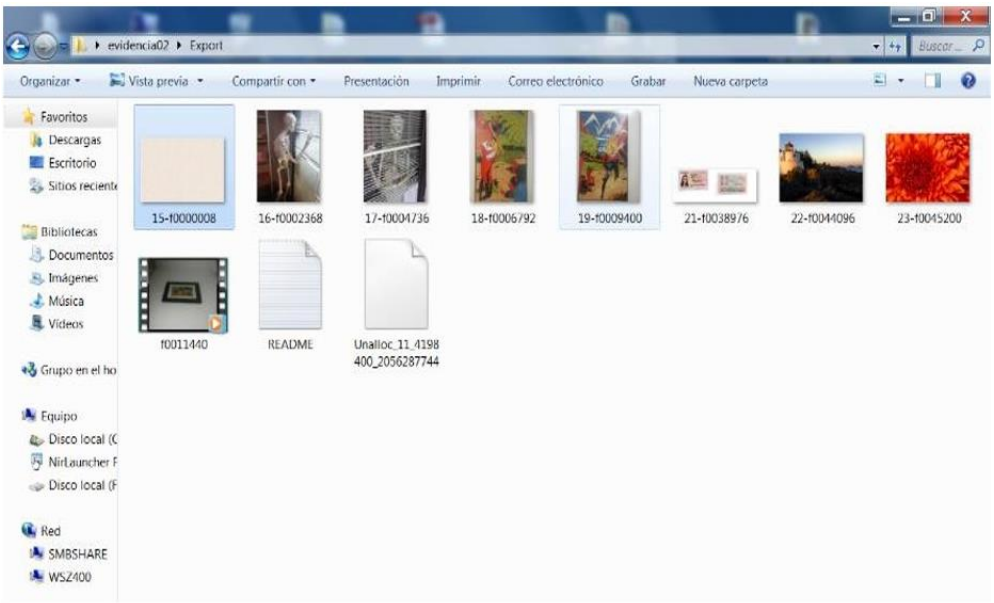


Figura 48: Archivos contenidos en el pendrive exportados con Autopsy.

Una vez recuperados los archivos con Autopsy se realizan los hash (figura 49) de todos ellos con la utilidad HashMyFiles, se documenta y se realiza imagen para su custodia.

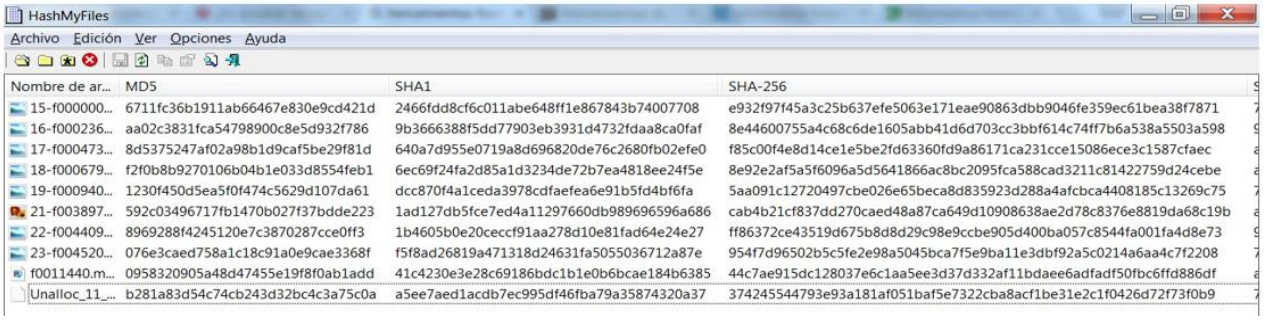


Figura 49: Hash de los archivos exportados con Autopsy.

OsForensics. Análisis de ocultación de información de los archivos exportados

Con OSForensics se van a analizar todos los archivos exportados en búsqueda de técnicas de ocultación. Como se puede observar en la figura 50, el módulo "*Mismatch Files"* alerta de la existencia de un fichero que oculta su identidad real, sustituyendo su nombre y extensión por otro.

En concreto el archivo "README.LOG" no es lo que parece. En realidad, es una fotografía –archivo JPG- de Amparo oculta bajo una extensión log (figura 51).

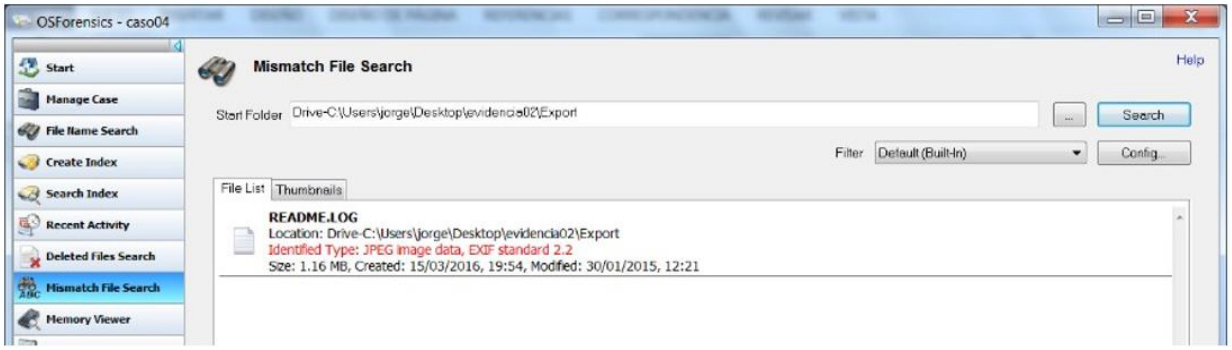


Figura 50: Mismatch File con OSForensics.

Figura 51: Fotografía camuflada en fichero README.LOG

Xteg. Localizar archivos con esteganografía.

A la vista de los resultados en los que se observaba la instalación del programa Camouflage, es necesario realizar la investigación en los archivos exportados con Autopsy 4.0 para ver si contienen muestras de técnicas estenográficas. El programa Xteg nos indica que en estos archivos no se encuentran evidencias de ocultación de información mediante esteganografía (figura 52).

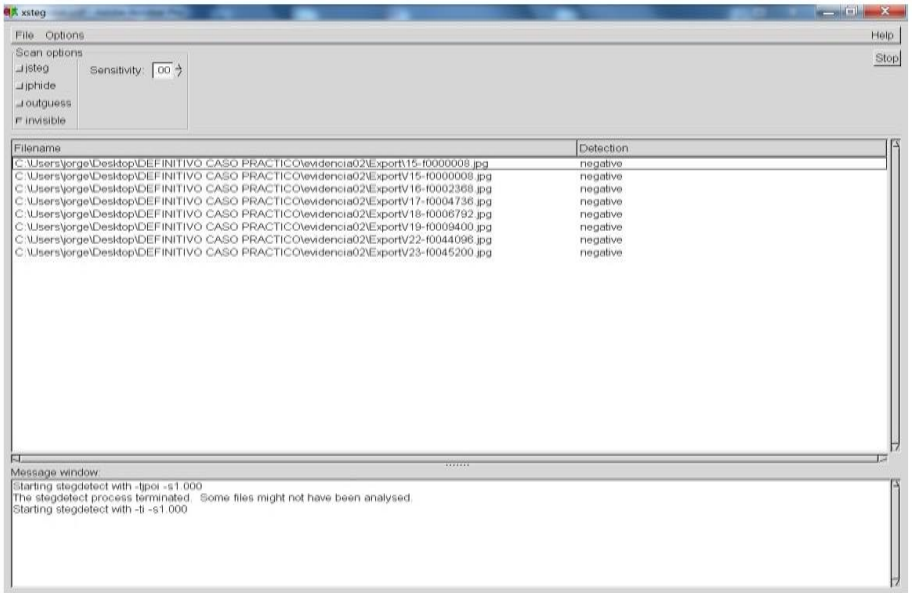


Figura 52: Resultado negativo en la búsqueda de esteganografía con Xteg.

Conclusión del análisis realizado al pendrive "evi02" con Autopsy , OSForensics y Xteg.

Con Autopsy se ha conseguido exportar el vídeo y otros archivos que antes no había sido posible recuperar. Además, con OSForensics se ha descubierto que el archivoREADME.LOG oculta su información real, una fotografía de Amparo. También, se ha utilizado la herramienta Xteg para localizar evidencias de esteganografía en los archivos exportados, siendo el resultado negativo.

Informe de resultados en la investigación del caso

Existen evidencias de que, en el *pendrive usb* -evi02- investigado se han copiado y posteriormente eliminado -mediante formateo u otra técnica- las fotografías y vídeo presentados como pruebas al caso. Además, se demuestra que el usuario de Windows con nombre "javier" del portátil Toshiba investigado, ha accedido a la cuenta de correo electrónico "amparo.xiva@gmail.com, abierto la carpeta enviados, leído el mensaje con asunto "FOTOS y VIDEO" y descargado el archivo ZIP con sus adjuntos -pruebas originales- lo que evidencia que se conoce la contraseña. Además, se consigue averiguarcon la utilidad ChromePass y de la información de la RAM con FTK Imager, siendo ésta"73552…". Por otro lado, se obtienen pruebas que afirman que el pendrive con número de serie "OMSEPSEP…" es el pendrive a investigar –evi02- y éste se ha conectado al portátil Toshiba, tal y como se declara en la denuncia. Y por último, se ha averiguado que el pendrive contiene un archivo eliminado README.LOG que en realidad es una fotografía de Amparo.

Guía 2: Phishing

Proceso

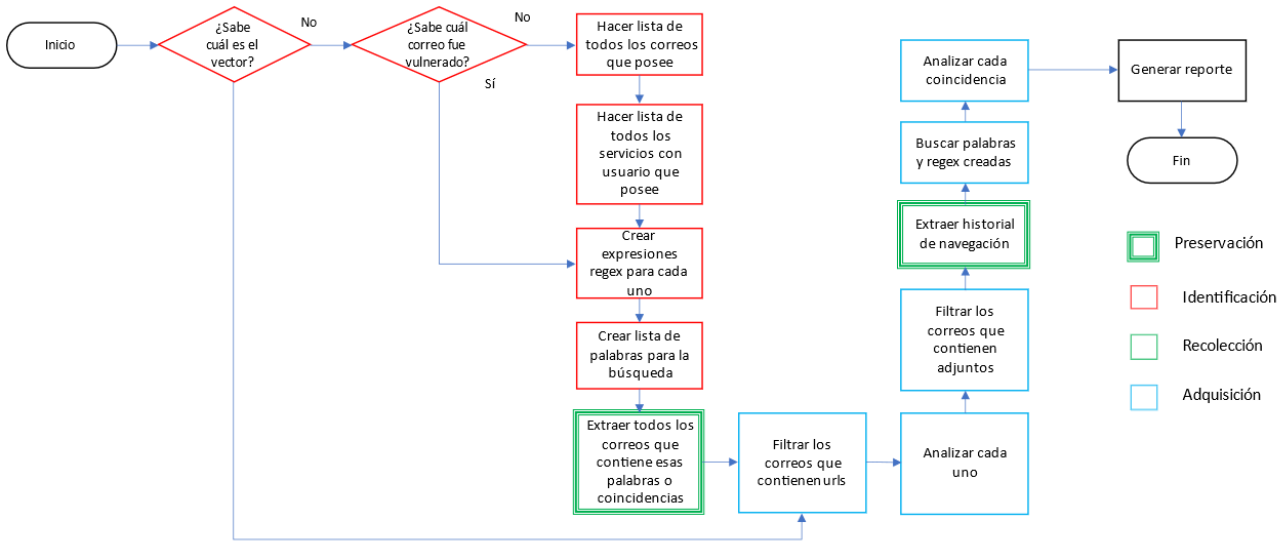


Figura 1: Diagrama del proceso

Detalle

Paso	Propósito	Técnica	Descripción	Herramientas
¿Sabe cuál es el vector de ataque?	Descubrir si se tiene conocimientos que puedan asegurar que sabemos la causa del ataque	Entrevista Evidencias previas	Se consulta al interesado si tiene conocimiento sobre un vector de ataque que considere que es probable que sea el causante del ataque	Editor de texto Grabadora Notepad++
¿Sabe cuál correo fue vulnerado?	Saber si se tiene conocimiento del correo que fue víctima del ataque	Entrevista	Se consulta al interesado si sabe que correo fue vulnerado en el ataque de phishing	Editor de texto Grabadora Notepad++
Hacer lista de todos los correos	Determinar cuál es el posible correo que sirvió como vector.	Entrevista.	Se consulta al interesado sobre los correos que posee o ha poseído.	Editor de texto Notepad++ Grabadora
Hacer lista de todos los usuarios que posee	Determinar cuáles cuentas o servicios pueden solicitar información de interés o facilitan la recuperación de cuentas	Entrevista.	Consultar al interesado que servicios posee tales como FB, Twitter, cuentas e-banca, otros portales empresariales, etc.	Editor de texto Notepad++ Grabadora
Crear expresiones regex para cada uno	Crear expresiones que hagan coincidencias visuales con los servicios analizados	Búsqueda de texto	Crear un listado de regex que faciliten la búsqueda. Estas expresiones deben contener las frases más significativas utilizadas por las interfaces de los servicios utilizados.	Regex Generator (w) RegexR(w) Browserling(w)
Crear lista de palabras para la búsqueda	Crear lista de palabras empleadas por esos servicios. Agregar palabras propias de ingeniería social.	Análisis.	Agregar palabras con los nombres de bancos, nombre de la persona, nombres de documentos, nombres de compañeros de trabajo, etc.	Editor de texto Notepad++
Extraer todos los correos que contiene esas palabras o coincidencias	Crear una copia para facilitar su análisis. Crear una copia de respaldo.	Backup	Crear una copia local de los correos del servidor. Usar si ya existe una. Todos los gestores que correo crean una copia local de los correos recibidos. Ver tiempo para el borrado automático.	Gestor de correo Thunderbird WinRAR
Filtrar los correos que contienen Urls	Analizar los que contienen potenciales vectores.	Carving	Buscar todos los correos que contienen https, http, etc. (Tag href) Especial atención a los que tienen dos correos como coincidencias.	Gestor de Correo Visor EML EML Viewer Tool Forensic EML Viewer Notepad++
Analizar cada uno	Verificar HTTP[S]	Carving	Buscar y analizar las Url´s que no están cifradas.	Visor EML EML Viewer Tool Forensic EML Viewer Notepad++ FileScan.io (w) Virus Total (w) Hybrid 46nalysis(w)
Filtrar los correos que contienen adjuntos	Analizar si los adjuntos poder ser vectores	Carving	Analizar si en los correos hay ejecutables o archivos que pueden servir para ello como vectores (ej. PDF, JPG, SVG)	Visor EML EML Viewer Tool Forensic EML Viewer Notepad++
Extraer historial de navegación	Listar los sitios a los que se ha navegado que fueron recibidos como parte de los correos.	Carving	Analizar si alguno de los sitios enviados fue usado.	Browser BrowsingHistoryView IEHistoryView

Buscar palabras y regex creadas	Buscar en los correos coincidencias de potenciales vectores.	Carving	Buscar en las partes del correo, textos o indicaciones a proporcionar información. Analizar imágenes.	Thunderbird Visor EML EML Viewer Tool Forensic EML Viewer Notepad++
Analizar cada coincidencia	Verificar cada uno de los sitios visitados.	Análisis.	Determinar cual es el vector de compromiso.	FileScan.io (w) Virus Total (w) Hybrid 47nalysis(w) Cuckoo
Generar reporte	Redactar un informe final en base al análisis de las evidencias	Análisis.	Brindar un informe final de lo ocurrido en el caso forense	Word, PDF

Tabla 1: Detalles del proceso

Aspectos relacionados

Proceso	Caso de empleo
Auditorías regulares	Realizar múltiples validaciones a la configuración del sistema de manera diaria, semanal, mensual o de acuerdo con las necesidades del negocio.
Eliminación de cuentas no utilizadas.	Eliminar las cuentas asociadas a personas que ya no estén vinculadas a la organización, realización de pruebas.
Sitios confiables	Navegar por sitios que cuenten con mecanismo de seguridad, así como evitar descargar archivos, programas ejecutabes de sitios sospechosos.

Tabla 2: Aspectos relacionados

Ejemplo

El objetivo primordial de este ejemplo es analizar la copia forense byte a byte que se generó de la computadora portátil del director financiero Jean de la empresa M57 dotbiz y así determinar de qué manera se presentó la filtración de datos.

El caso M57 Jean (2009), busca dar a conocer un problema de fuga de datos empresariales, lo que se clasifica como "Alta Confidencialidad". Los hechos sucedieron a partir de una filtración de un documento tipo hoja de cálculo de Excel, encontrada en la computadora de dicho directivo.

Cabe aclarar que dicha información no debería ser suministrada a ningún funcionario de la empresa, ya que esta contenía información personal de sus empleados, como lo son sus nombres, apellidos, salario y números de identificación personal. Todo esto se logra evidenciar a través de un análisis forense realizado a la imagen Encase.

Para el desarrollo de la investigación, se usó el software forense "Autopsy" el cual suministró un informe detallado de los sucesos que se llevaron a cabo en la computadora; también se encontraron mensajes enviados a través de la plataforma de Microsoft Outlook 2000, donde se observan conversaciones entre la presidente y el director financiero; en donde le solicita generar dicha hoja de cálculo.

Caso: Exfiltración corporativa

M57.biz es una nueva empresa web que desarrolla un catálogo de arte corporal.

Hechos del caso:

$ 3 millones en financiación inicial; ahora cerrando ronda de $ 10M

2 fundadores / propietarios

10 empleados contratados el primer año

Personal actual

Presidenta: Alison Smith

Director financiero: Jean

Programadores: Bob, Carole, David, Emmy

Comercialización: Gina, Harris

BizDev: Indy

M57.biz es una corporación virtual

Programadores:

Trabajan fuera de sus casas

Sesión diaria de chat en línea; Parque de oficinas para reuniones presenciales semanales

Marketing y BizDev:

Trabajan en habitaciones de hotel o Starbucks (principalmente en la carretera)

Reuniones en persona una vez cada dos semanas.

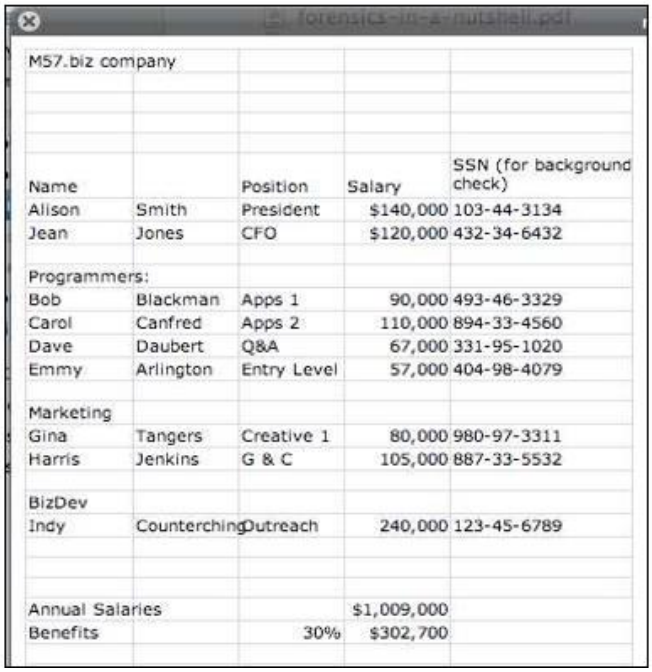
La mayoría de los documentos se intercambian por correo electrónico.

El caso: exfiltración de documentos

Se publicó una hoja de cálculo que contenía información confidencial como archivo adjunto en el foro de "soporte técnico" del sitio web de un competidor.

La hoja de cálculo provino de la computadora del Oficial Principal de Finanzas Jean.

A continuación, se muestra la hoja de cálculo:



M57.biz company

Name		Position	Salary	SSN (for background check)
Alison	Smith	President	$140,000	103-44-3134
Jean	Jones	CFO	$120,000	432-34-6432
Programmers:				
Bob	Blackman	Apps 1	90,000	493-46-3329
Carol	Canfred	Apps 2	110,000	894-33-4560
Dave	Daubert	Q&A	67,000	331-95-1020
Emmy	Arlington	Entry Level	57,000	404-98-4079
Marketing				
Gina	Tangers	Creative 1	80,000	980-97-3311
Harris	Jenkins	G & C	105,000	887-33-5532
BizDev				
Indy	Counterching	Outreach	240,000	123-45-6789
Annual Salaries			$1,009,000	
Benefits		30%	$302,700	

Figura 2: Hoja de cálculo filtrada

Resúmenes de entrevistas

Alison (presidenta):

No sé de qué está hablando Jean.

Nunca le pedí a Jean la hoja de cálculo.

Nunca recibí la hoja de cálculo por correo electrónico.

Jean (director financiero):

Alison me pidió que preparara la hoja de cálculo como parte de la nueva ronda definanciación.

Alison me pidió que le enviara la hoja de cálculo por correo electrónico.

Eso es todo lo que sé.

Identidades electrónicas

Alison (President): alison@m57.biz ; password: "ab=8989

Jean (CFO): jean@m57.biz ; password: gick*1212

La investigación

Se ha obtenido una copia del disco duro de la computadora de Jean.

Puntos de pericia Solicitados

El cliente, uno de los financiadores de la empresa solicita los siguientes puntos de pericia:

¿Cuándo creó Jean esta hoja de cálculo?

¿Cómo llegó desde su computadora al sitio web de la competencia?

¿Quién más de la empresa está involucrado?

MARCO METODOLOGICO

Adquisición

En este paso es importante que toda la información que se tome sea por medio de una copia forense al disco original, es decir, que se realice una copia de seguridad de manera completa de toda la información que se almacene en el disco, dentro de la copia se debe incluir el espacio no asignado por los sistemas de archivos, los archivos borrados e incluso datos que pudieran haber existido antes de que el soporte fuese formateado para que esto se lleve a cabo, es necesario disponer de herramientas y/o aplicaciones que nos permitan realizar este tipo de toma de información, dentro de las posibles aplicaciones a utilizar se encuentran dd, EnCase, FTK, Air, entre muchas más herramientas, las cuales serán capaces de obtener dichos resultados.

Para el escenario de ejemplo: M57-Jean 2009 se tiene como evidencia desde la página web "Digital Corpora" una imagen forense del tipo Encase (E01) de la cual contiene toda la información del disco de almacenamiento de la computadora portátil del CFO de M57 dotbiz el cual es Jean.

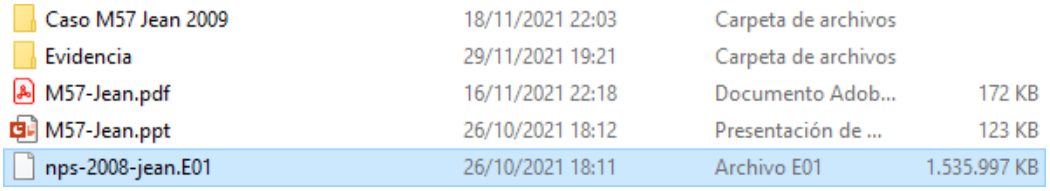


Figura 3: Imagen forense Encase descargada para el análisis del caso.

Las especificaciones de la primera imagen forense son las siguientes:

En esta tabla se da a conocer las especificaciones técnicas que tiene la imagen forense tipo Encase para este escenario de la empresa M57 dotbiz a través del software libre Autopsy		
No.	Nombre	Descripción
1	Nombre	nps-2008-jean.E01
2	Tipo	Imagen Encase (.E01)
3	Tamaño (bytes)	10737418240
4	Tamaño del Sector	512 Bytes
5	Cantidad Volúmenes	Volumen 1, 2 y 3.
6	MD5	78a52b5bac78f4e711607707ac0e3f93
7	SHA1	Not calculated
8	SHA-256	Not calculated
9	Device ID	12e99ae4-b15a-496b-94f5-4693edb95a1e

Tabla 3: Especificaciones imagen Encase (E01)

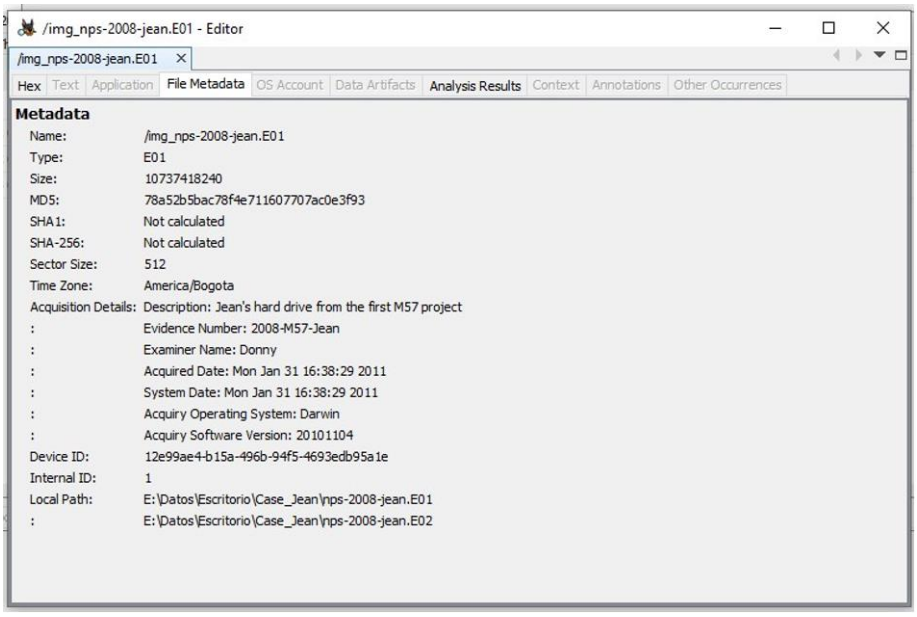


Figura 4: Especificaciones de volumen 2 obtenidos en la copia forense.

No.	Nombre	Descripción
1	Nombre	vol2 (NTFS / exFAT (0x07): 63-20948759)
2	Sector de inicio	63
3	Longitud en sectores	20948697
4	Descripción	NTFS / exFAT (0x07)
5	Tipo de Sistema de Archivos	NTFS
6	Desplazamiento de imagen	32256
7	Tamaño de bloque	4096 Bytes
8	Recuento de bloques	2618587
9	Última entrada de metadatos	32848

Tabla 4: Propiedades de volumen 2 obtenidos en la copia forense.

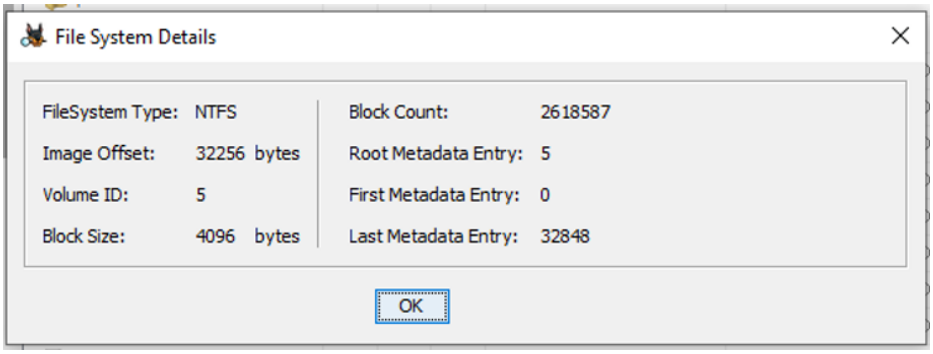


Figura 5: Detalle de sistema de archivos de volumen 2.

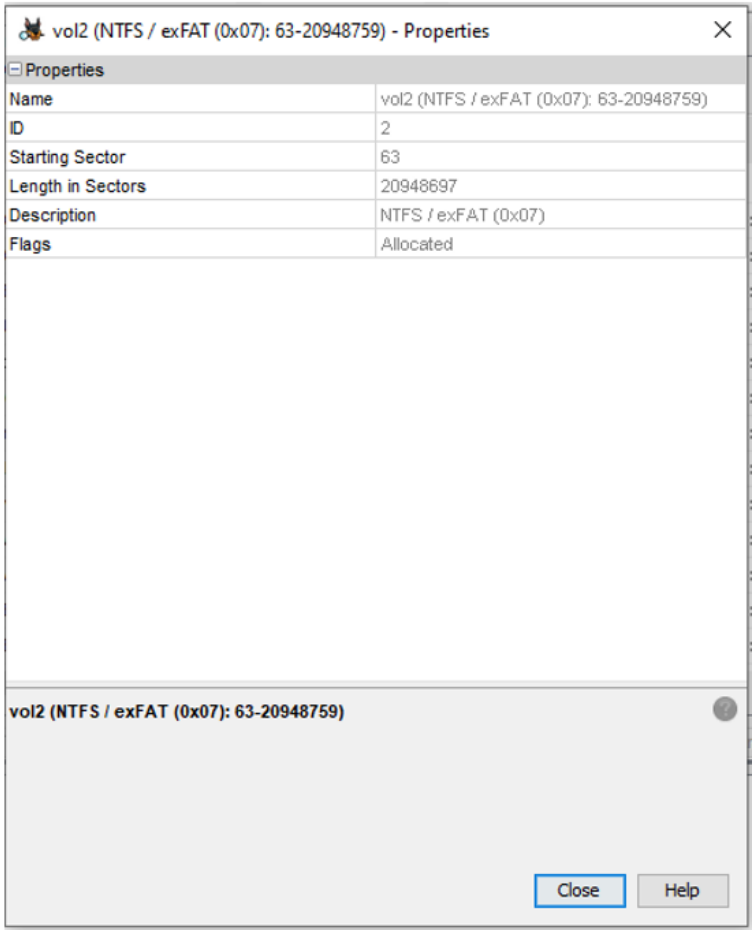


Figura 6: Propiedades de sistema de archivos de volumen 2.

Análisis

El análisis consiste en la identificación, el estudio y en la interpretación de los elementos de evidencia existentes en el soporte de datos

Es importante que el investigador forense evalúe cada uno de los datos obtenidos, para que así mismo determine que archivosse consideran sospechosos y conozca detalladamente el contenido de estos; de manera que cuando evalué y analice cada uno de los archivos este puede dar una conclusión o un veredicto de lo que sucedió.

Resumen de entrevistas a las dos personas involucradas.

Alison (Presidenta)

No sé de qué está hablando Jean.

Nunca le pedí a Jean la hoja de cálculo.

Nunca recibí la hoja de cálculo por correo electrónico.

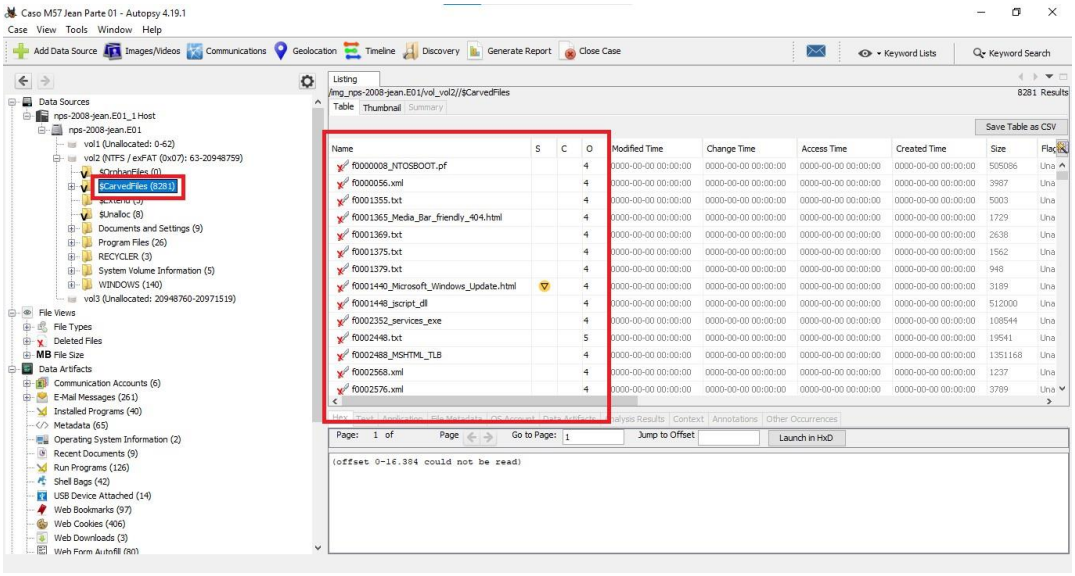
Jean (director financiero)

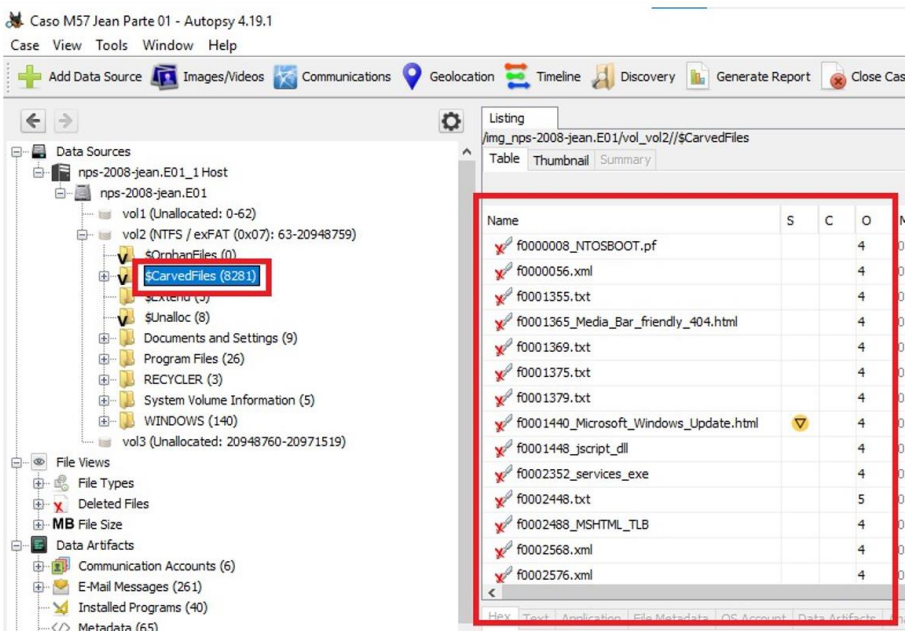
Alison me pidió que preparara la hoja de cálculo como parte de la nuevaronda de financiación.

Alison me pidió que le enviara la hoja de cálculo por correo electrónico.

Eso es todo lo que sé.

En el volumen 2 de la imagen forense de nombre “nps-2008-jean.E01” se halla un total de 8281 archivos que fueron borrados del sistema de archivos de disco de almacenamiento de la computadora portátil del CFO Jean.





Figuras 7 y 8: Archivos encontrados en la imagen Encase E01.

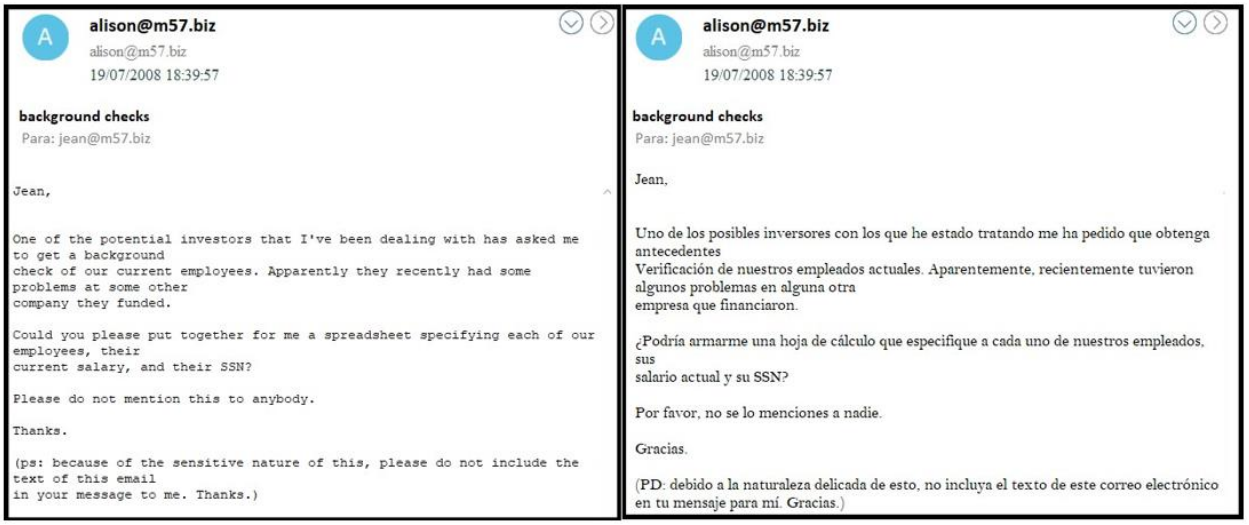
En esta imagen forense respecto al disco de almacenamiento de la computadora portátil de Jean de la empresa M57 dotbiz, se encuentran los siguientes volúmenes:

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-62)	1	0	63	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 63-20948759)	2	63	20948697	NTFS / exFAT (0x07)	Allocated
vol3 (Unallocated: 20948760-20971519)	3	20948760	22760	Unallocated	Unallocated

Figura 9: Volúmenes encontrados en la imagen Encase E01.

Como se observa en la figuras 7 y 8 se encuentran 8,281 archivos que fueron formateados del disco duro de la computadora de Jean, pero solamente en la siguiente ruta "vol2/Documentos and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst" se encuentra un archivo Outlook.pst el cual contiene conversaciones que mantuvo el director financiero Jean con la presidenta Alison y otros compañeros de la empresa mencionada en este caso, a través de la plataforma de Microsoft Outlook 2000.

A continuación, se muestran los mensajes enviados a través de la plataforma Microsoft Outlook 2000 entre el director Financiero Jean y la presidenta Alison de la empresa M57 dotbiz



alison@m57.biz
alison@m57.biz
19/07/2008 18:39:57

background checks
Para: jean@m57.biz

Jean,

One of the potential investors that I've been dealing with has asked me to get a background
check of our current employees. Apparently they recently had some problems at some other
company they funded.

Could you please put together for me a spreadsheet specifying each of our employees, their
current salary, and their SSN?

Please do not mention this to anybody.

Thanks.

(ps: because of the sensitive nature of this, please do not include the text of this email
in your message to me. Thanks.)

alison@m57.biz
alison@m57.biz
19/07/2008 18:39:57

background checks
Para: jean@m57.biz

Jean,

Uno de los posibles inversores con los que he estado tratando me ha pedido que obtenga antecedentes
Verificación de nuestros empleados actuales. Aparentemente, recientemente tuvieron algunos problemas en alguna otra
empresa que financiaron.

¿Podría armarme una hoja de cálculo que especifique a cada uno de nuestros empleados, sus
salario actual y su SSN?

Por favor, no se lo menciones a nadie.

Gracias.

(PD: debido a la naturaleza delicada de esto, no incluya el texto de este correo electrónico en tu mensaje para mí. Gracias.)

Figura 10: Mensaje enviado por Alison a Jean.

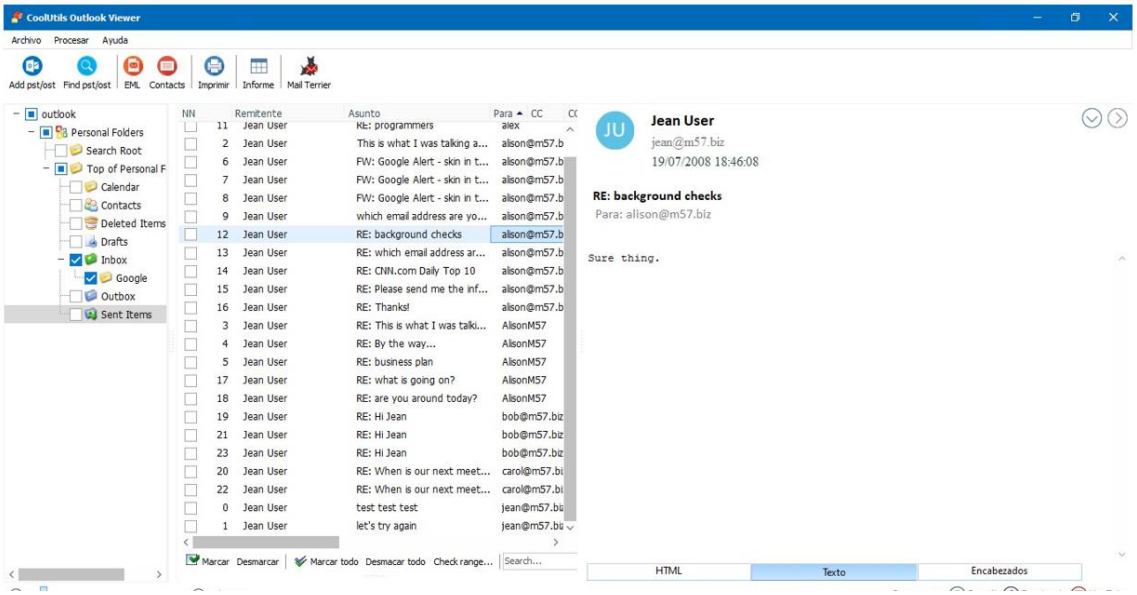


Figura 11: Respuesta por parte de Jean a Alison.

Figura 12: Mensaje de Alison a Jean.

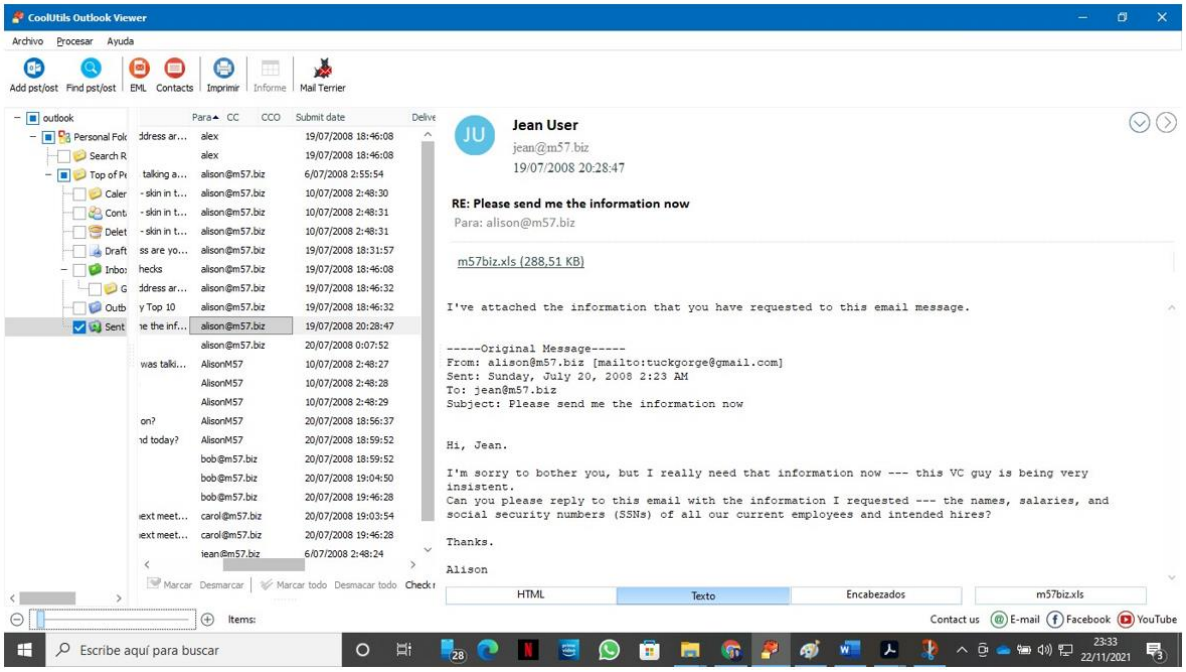


Figura 13: Hoja de Cálculo enviada al correo tuckgeorge@gmail.com.

Custodia y Presentación

En este paso, el investigador forense recopila toda la información encontrada y la transforma en un informe de fácil entendimiento para alguien que no es conocedor de informática, por otro lado, es importante que el investigador forense deje en constancia todos los pasos que realizó, toda la información que recopiló, para que así mismo esta información sea utilizada como prueba ante un caso en concreto.

En el volumen 2 de la imagen forense de nombre “nps-2008-jean.E01” se halla un total de 8281 archivos que fueron borrados del sistema de archivos del disco de almacenamiento de la computadora portátil del CFO Jean.

Entre los archivos borrados se encuentran imágenes en formato jpg, png, gif. Archivos tipo de acceso directo y de aplicaciones. Documento de texto tipo Word,txt, hojas de cálculo xls y archivos dll.

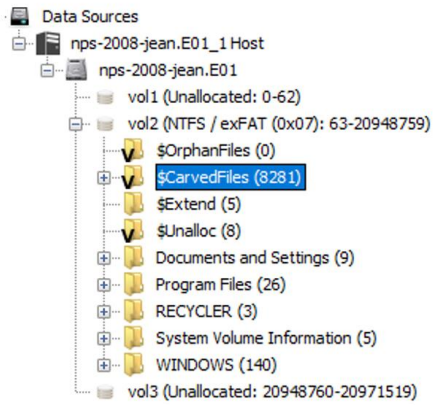


Figura 14: Archivos encontrados en la imagen forense nps-2008-jean.E01 .

En la Figura 10 con el asunto de “verificaciones de antecedentes o background checks” la presidenta Alison le está pidiendo a Jean que arme una hoja de cálculo en donde especifique a cada uno de los empleados de M57 dotbiz, su salario actual y sus números de seguridad social, ya que uno de los posibles inversores que han tratado con Alison le está pidiendo antecedentes de la empresa, la verificación de los empleados actuales de la empresa. Y de igual manera le pide a Jean que no se lo mencione a nadie y que tampoco en el asunto del mensaje incluya el texto de este correo electrónico. En pocas palabras que sea lo más discreto posible con la información que le está solicitando Alison.

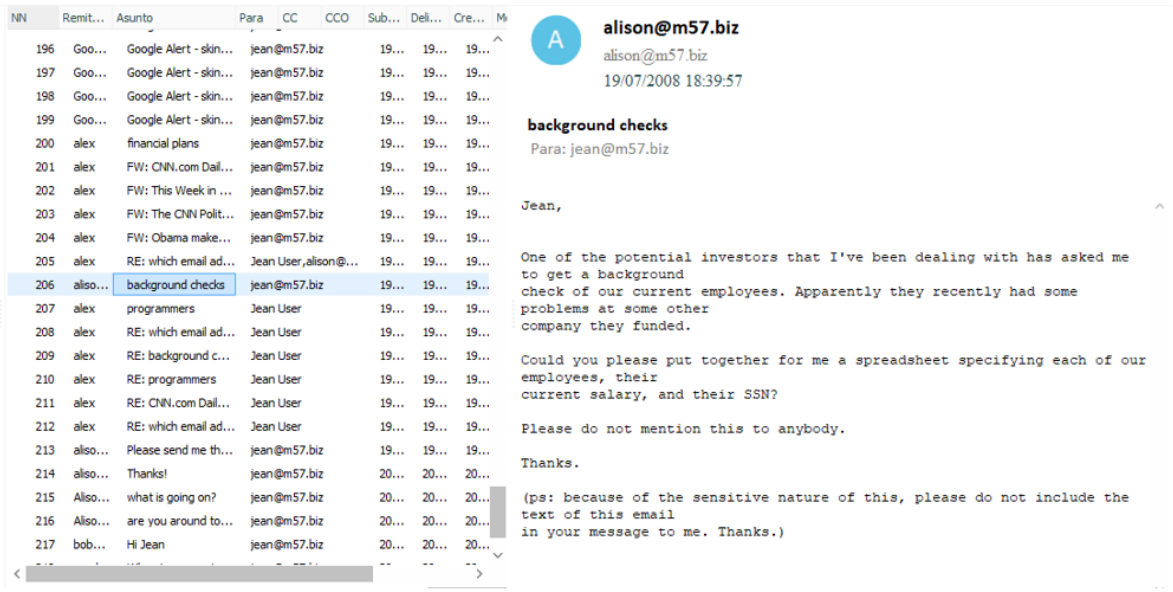


Figura 15: Correo con asunto “background checks” de Alison .

En la Figura 11 le responde Jean a la presidenta Alison, si estásegura en cuanto a que le envíe esa información delicada de la empresa M57dotbiz.

En la Figura 12 se logra visualizar un cambio significativo en el mensaje que recibió Jean el día 19 de julio de 2008 a las 20:22:45, debido a que el correo del que fue enviado este mensaje, pasa de ser un correo corporativo de la empresa M57 a ser un correo personal, tal cual como se logra evidenciar en la Figura 16. Nos dice que este mensaje lo ha enviado una persona con el nombre de usuario del correo de la presidenta Alison el cual es “alison@m57.biz” a través del correo electrónico personal “tuckgorge@gmail.com” de la plataforma de Gmail.

Figura 16: Visualización del encabezado del mensaje enviado desde el correo personal del infiltrado en la empresa a través del software CoolUtils Outlook Viewer .

Línea de Tiempo

Este paso es importante, ya que, por medio de herramientas informáticas, el investigador forense puede obtener una lista de los procesos que ocurrieron, la fecha en que ocurrieron y los cambios que se dieron allí; la línea de tiempo se utiliza para ayudar al investigador a comprender la evolución de los hechos y las relaciones decausa y efecto existentes en los mismos.

El orden cronológico del ataque de phishing se presenta en la siguiente tabla:

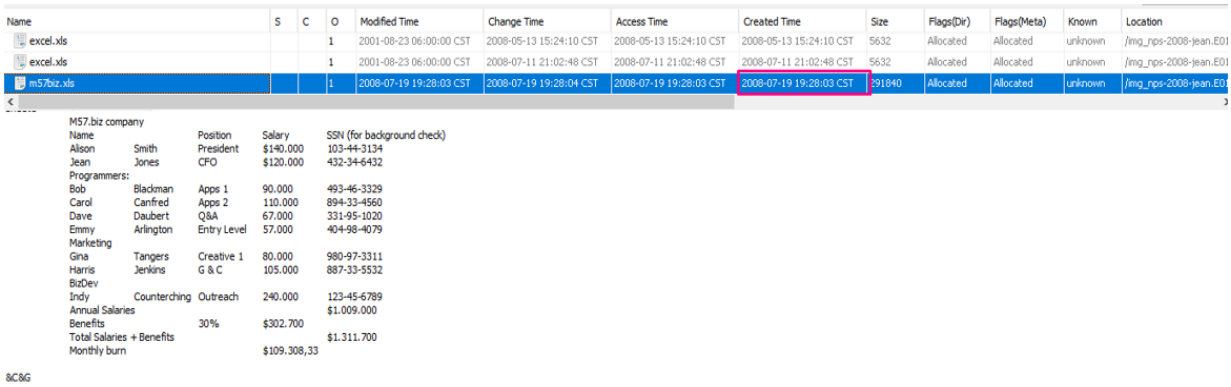
Fecha	Actividad
19/07/2008	Se crea el documento de Excel llamado m57biz.xls
19/07/2008	Un Email de una persona externa a la compañía envía un mensaje a Jean con el archivo de Excel creado pidiendo los salarios, lista de empleados ente otros fingiendo ser Alison: From tuckgorgo.com (alison@m57.biz)
19/07/2008	Jean abre el archivo y lo llena con los datos y lo envía a tuckgorgo.com pensando que es Alison(alison@m57.biz)
19/07/2008	La Alison falsa responde muchas gracias
19/07/2008	Jean responde con gracias también al atacante
20/07/2008	Alison sospecha que algo raro ha pasado (un posible hackeo) y pregunta a Jean si todo está bien
20/07/2008	Jean responde que no sabe nada de un evento sospechoso
20/07/2008	Bob notó el cartel de SSN en un sitio web, le envió un correo electrónico a Jean para verificar si lo sabía.
20/07/2008	Jean le responde a Bob que no sabe nada acerca de ese post
20/07/2008	Bob siguió una pregunta por correo electrónico preguntándole a Jean si el SSN y el salario eran suyos.
20/07/2008	Jean respondió afirmativamente, lo que confirma un incidente de infracción, pero no sabía cómo sucedió.

Tabla 5: Cronología gráfica del escenario M57 Jean.

Presentación de informe

¿Cuándo creó Jean esta hoja de cálculo?

Luego de analizar la evidencia recolectada con FTK Imager en Autopsy se descubrió que la fecha de creación del Excel es la siguiente **2008/07/19 a las 19:28:03** como se muestra en la siguiente imagen:



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
excel.xls			1	2001-08-23 06:00:00 CST	2008-05-13 15:24:10 CST	2008-05-13 15:24:10 CST	2008-05-13 15:24:10 CST	5632	Allocated	Allocated	unknown	/img_nps-2008-jean.E01
excel.xls			1	2001-08-23 06:00:00 CST	2008-07-11 21:02:48 CST	2008-07-11 21:02:48 CST	2008-07-11 21:02:48 CST	5632	Allocated	Allocated	unknown	/img_nps-2008-jean.E01
m57biz.xls			1	2008-07-19 19:28:03 CST	2008-07-19 19:28:04 CST	2008-07-19 19:28:03 CST	2008-07-19 19:28:03 CST	291840	Allocated	Allocated	unknown	/img_nps-2008-jean.E01

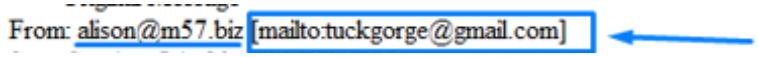
M57.biz company				
Name		Position	Salary	SSN (for background check)
Alison	Smith	President	$140.000	103-44-3134
Jean	Jones	CFO	$120.000	432-34-6432
Programmers:				
Bob	Blackman	Apps 1	90.000	493-46-3329
Carol	Canfred	Apps 2	110.000	894-33-4560
Dave	Daubert	Q&A	67.000	331-95-1020
Emmy	Arlington	Entry Level	57.000	404-98-4079
Marketing				
Gina	Tangers	Creative 1	80.000	980-97-3311
Harris	Jenkins	G & C	105.000	887-33-5532
BizDev				
Indy	Counterching	Outreach	240.000	123-45-6789
Annual Salaries				$1.009.000
Benefits		30%	$302.700	
Total Salaries + Benefits				$1.311.700
Monthly burn			$109.308,33	

&C&G

Figura 17: Evidencia de fecha de creación de la hoja de cálculo.

¿Cómo llegó desde su computadora al sitio web de la competencia?

Se realizo un ataque de phishing(spear phishing) usando una técnica bastante común que consiste en hacerse pasar por un miembro de una empresa para solicitar a los empleados el envió de información como se puede ver en la parte del encabezado del correo:



el atacante con correo tuckgorge@gmail.com fingió ser la la presidenta(alison@m57.biz) para hacer uso de su autoridad en la organización, presentando también urgencia en la petición para lograr que los datos fueran enviados con la mayor prioridad posible.

Adicionalmente, se encontró el primer mensaje enviado por el atacante donde solicitaba que se enviara el documento y además que no se mencionara a nadie de ello (algo que de por sí ya es sospechoso y que debió alertar a Jean) además al final le pide por favor que en la respuesta cuando se le envié el archivo no poner el texto del mensaje original (otra razón más para sospechar).

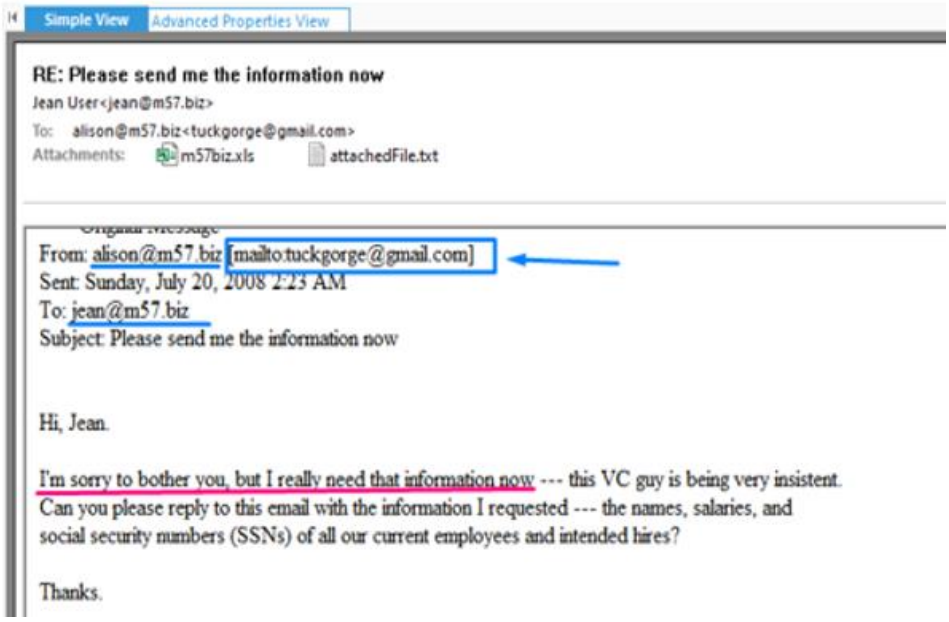


Figura 18: Evidencia 1 de spear phishing.

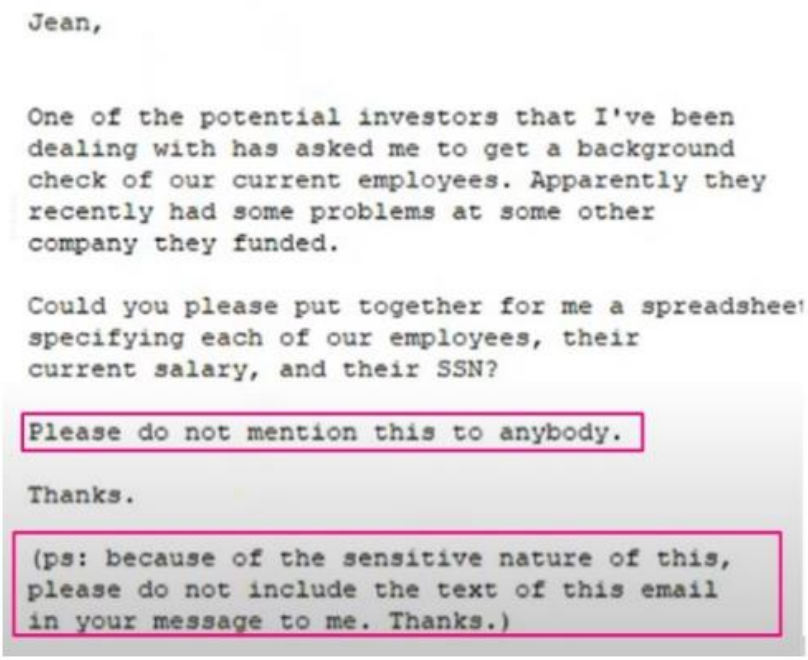


Figura 19: Evidencia 2 de spear phishing.

¿Quién más de la empresa está involucrado?

Nadie más de la empresa está involucrado se trató de un ataque de spear phishing dirigido para Jean y ella cayó en la trampa y envió la información al atacante **tuckgorge@gmail.com** como se mostró en el punto de pericia número dos, Alison fue el único objetivo del ataque.

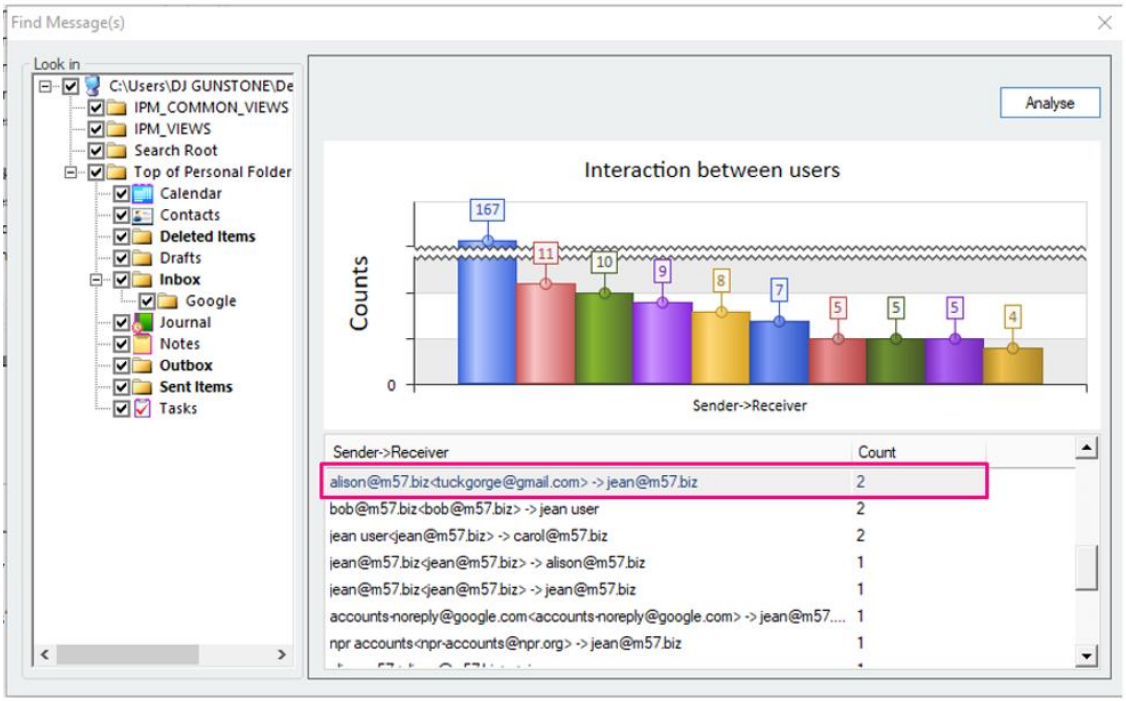


Figura 20: Evidencia de personas involucradas en la empresa.

Guía 3: Metodología Forense en Sistemas Windows

Proceso

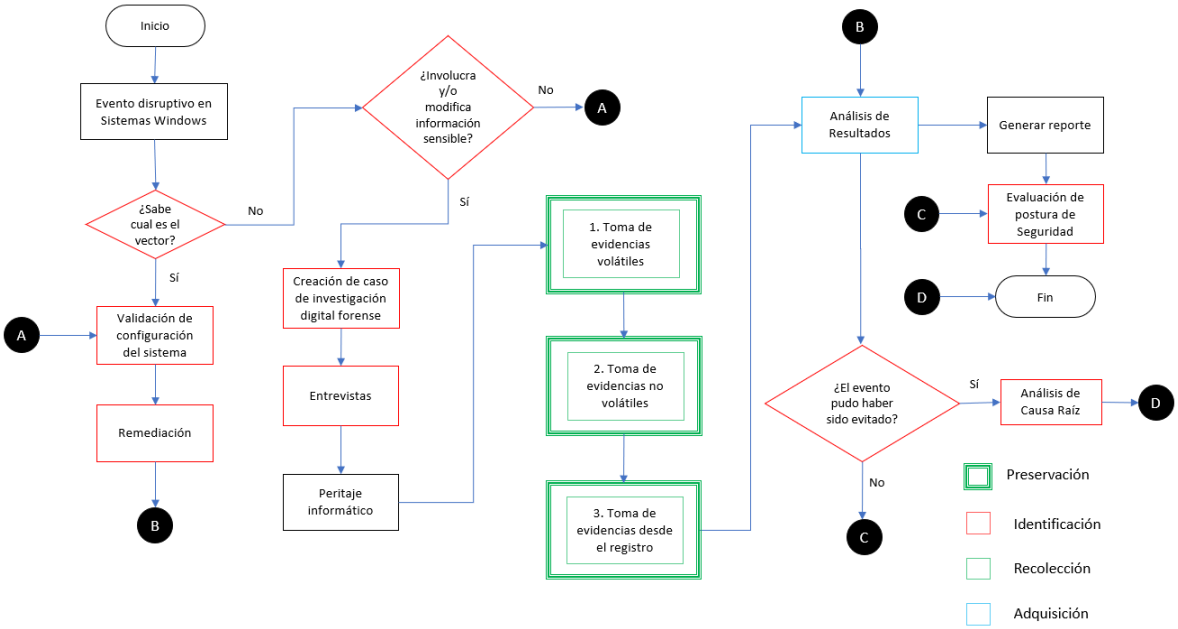


Figura 1: Diagrama del proceso

Detalle

	Paso	Propósito	Técnica	Descripción	Herramientas
Peritaje Informático	**Toma de evidencias volátiles.**	Recopilación de información crucial para la investigación	Software especializado / Análisis de información.	Toma de evidencias volátiles.	cmd, dumpit, shadow copy, PsService, PsList, PsLoggedon, promiscdetect, NETVIEWX.
	Toma de evidencias no volátiles (Unidades de Almacenamiento).	Recopilación de información crucial para la investigación	Software especializado / Análisis de información.	Toma de evidencias no volátiles (Unidades de Almacenamiento).	NortonGhost, MBRUtil, ntsinfo, FreeUndelete.
	Toma de evidencias no volátiles (Hardware, Logs y Ficheros del sistema).	Recopilación de información crucial para la investigación	Software especializado / Análisis de información.	Toma de evidencias no volátiles (Hardware, Logs y Ficheros del sistema).	Psinfo, Total Commander, psloglist, rifiuti-vista.
	Toma de evidencias no volátiles (Variables, tareas y enlaces).	Recopilación de información crucial para la investigación	Software especializado / Análisis de información.	Toma de evidencias no volátiles (Variables, tareas y enlaces).	pfirewall, lnk_parser_cmd , EDD.
	Toma de evidencias no volátiles (Historiales, portapapeles y estructura MAC).	Recopilación de información crucial para la investigación	Software especializado / Análisis de información.	Toma de evidencias no volátiles (Historiales, portapapeles y estructura MAC).	mylastsearch, BrowsingHistoryView, insideclipboard.
	Toma de evidencias no volátiles (Contraseñas).	Recopilación de información crucial para la investigación	Software especializado / Análisis de información.	Toma de evidencias no volátiles (Contraseñas).	netpass, webbrowserpasswview, mailpv.
	Toma de evidencias desde el Registro.	Recopilación de información crucial para la investigación	Software especializado / Análisis de información.	Toma de evidencias desde el Registro.	wirelessnetconsole, WhatInStartup, setupapi.dev, usbHistory.
	Asegurar el reingreso del forense al sistema.	Establecer un perímerto digital de investigación.	Software especializado / Análisis de información.	Asegurar el reingreso del forense al sistema.	Utilman.
	Análisis de Logs y procesos adicionales.	Validar la información plasmada en los logs para la búsqueda de parámetros que lleven a la resolución del caso,	Software especializado / Análisis de información.	Análisis de Logs y procesos adicionales.	HackersUtility

Tabla 1: Detalles del proceso

Aspectos relacionados

Proceso	Caso de empleo
Auditorías regulares	Realizar múltiples validaciones a la configuración del sistema de manera diaria, semanal, mensual o de acuerdo con las necesidades del negocio.
Eliminación de cuentas no utilizadas.	Eliminar las cuentas asociadas a personas que ya no estén vinculadas a la organización, realización de pruebas.
Sitios confiables	Navegar por sitios que cuenten con mecanismo de seguridad, así como evitar descargar archivos, programas ejecutabes de sitios sospechosos.

Tabla 2: Aspectos relacionados

Ejemplo

Metodología Forense Windows

Sección 1: Toma de evidencias volátiles

Etiquetado y toma de evidencias volátiles.

Se debe fotografiar minuciosamente con cámaras digitales de alta resolución cada una de las evidencias físicas, por ejemplo: pendrive, CDs, ordenadores, teléfonos, etc.

Posteriormente se debe realizar un inventario completo indicando: marca, modelo, sistemas operativos, donde fue encontrada la evidencia física, así como su posible relación con las otras evidencias.

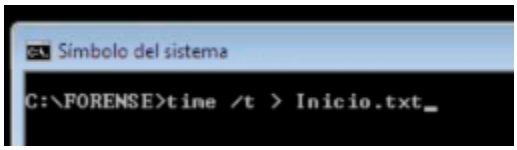
También se debe definir quién se hará cargo de la cadena de custodia de la evidencia.

Posteriormente, se inicia el trabajo de volcado de evidencias volátiles para asentar una base de línea de tiempo, es decir, tomando un punto de partida para cronometrar los tiempos de trabajo e ir tomando referencias cruzadas con la toma de cada una de las evidencias se debe obtener la fecha y la hora dada por el sistema del momento en el que se va a iniciar la investigación forense.

Se debe realizar la primera impresión de toma de evidencia digital, para ello, el investigador forense debe ejecutar copias seguras de cada herramienta, para el ejemplo, se utilizará el cmd.exe desde un pendrive forense.

El pendrive tiene que contar con las herramientas, posteriormente debe haber otro pendrive o otra partición si se trata de un disco rígido en donde se vayan dejando cada uno de los archivos que se van a generar.

Lo primero que hay que hacer es realizar la toma de fecha y hora, para dicho propósito, se debe ejecutar el comando: time /t > Inicio.txt.



En el ejemplo, se indica que el resultado del comando lo guarde en el archivo Inicio.txt

Posteriormente se ejecuta este comando:

Date /t >> Inicio.txt

El símbolo >> significa que sume el valor de la fecha a la hora, de tal manera que esté tanto la fecha como la hora.

Para ver el contenido del archivo .txt, se ejecuta el siguiente comando:

Type Inicio.txt

El proceso descrito anteriormente es el primer paso de toma de evidencia volátil.

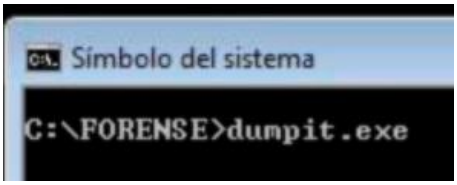
Captura y análisis de la memoria volátil RAM en tiempo de ejecución

El investigador forense debe tomar una instantánea de lo más volátil, en este caso de la memoria.

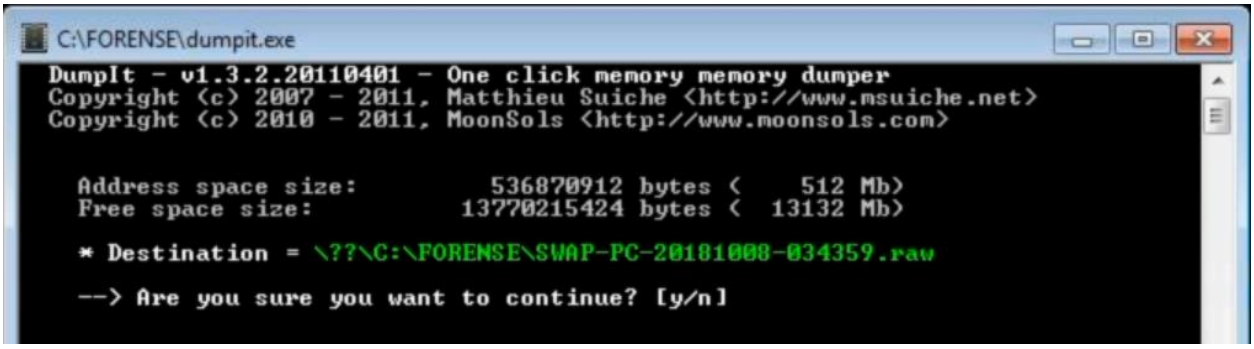
Existe la memoria RAM física como la SODIMM, y, en segundo lugar, la toma de muestra volátil hace referencia al archivo de paginación que se denomina WindowsPageFile.cis o archivo de intercambio Swap.

El objeto con orden de volatilidad más alto es la memoria RAM, para el ejemplo se utilizará la aplicación Dumpit.exe, el cual es un archivo portable que al ejecutarlo realiza un volcado de la memoria RAM en el lugar en donde se ejecute.

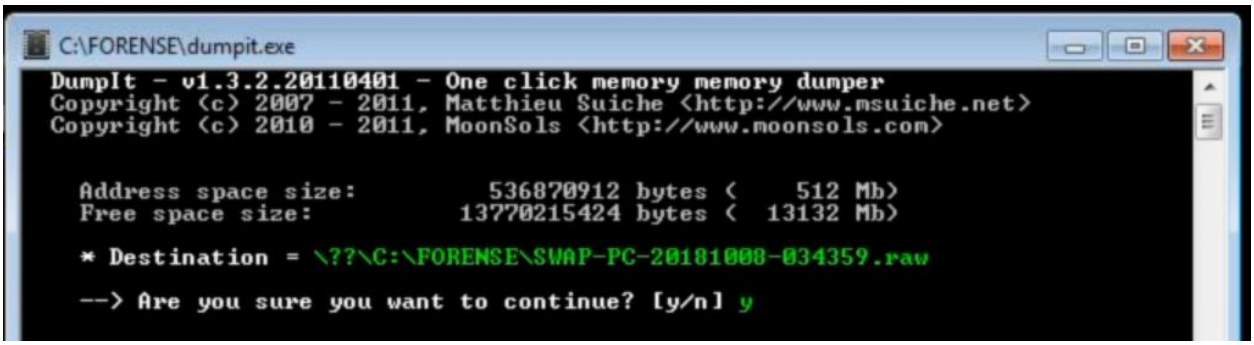
Se ejecuta el siguiente comando: dumpit.exe



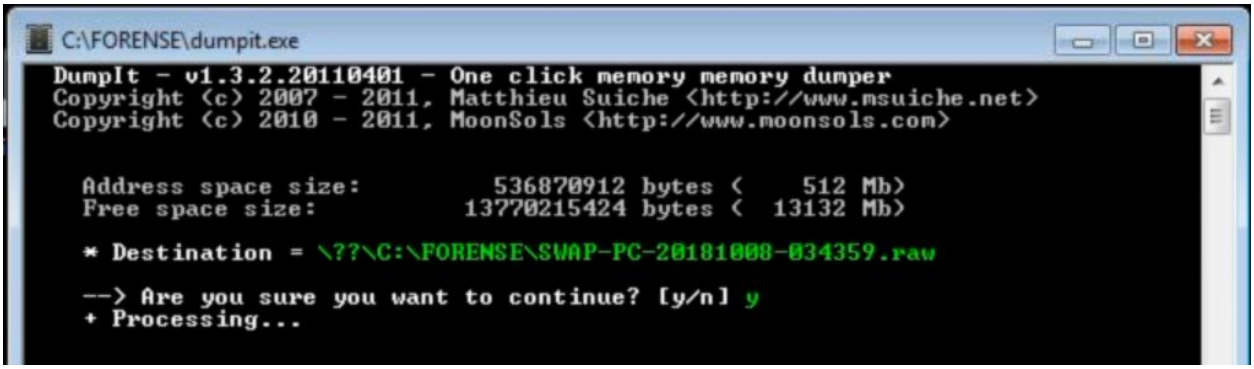
Al ejecutarlo, mostrará lo siguiente:



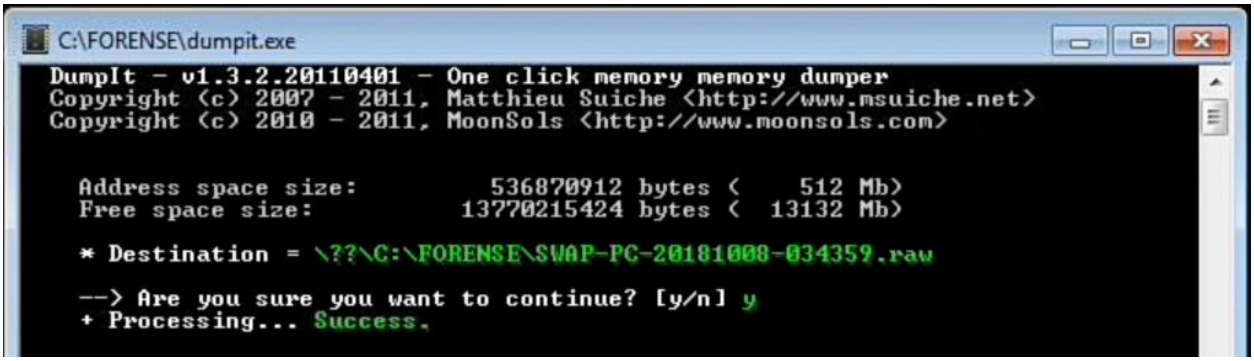
Para el ejemplo, la herramienta indica que realizará un volcado de 512 MB.



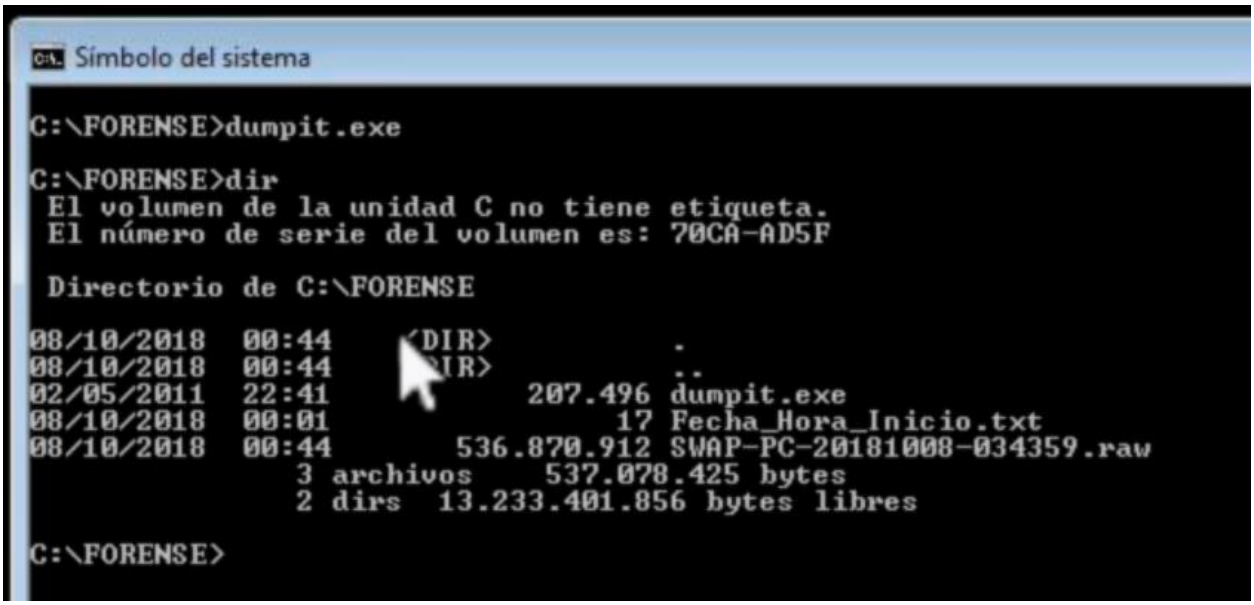
Se coloco la letra y para iniciar con el volcado.



Es importante aclarar que esta aplicación logra realizar volcado de memoria de todas las versiones de Windows, ya sea de 32 bit, 64 bits, Windows XP, 7, 8, 8.1, 10. Dumpit utiliza sus propias API y no pasa por el sistema operativo, lo anterior resulta útil en el caso que el sistema operativo haya sido comprometido con un rootkit.



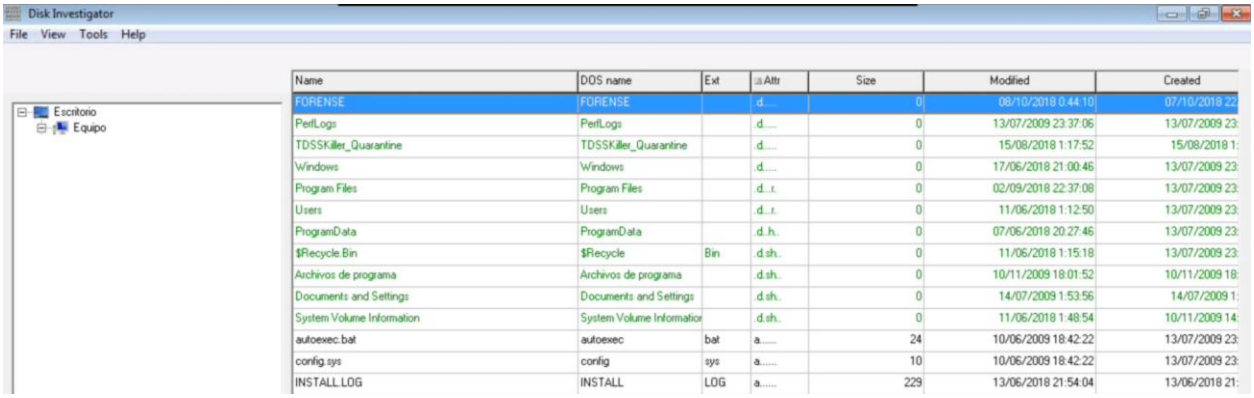
Posteriormente, al ejecutar el comando dir mostrará lo siguiente:



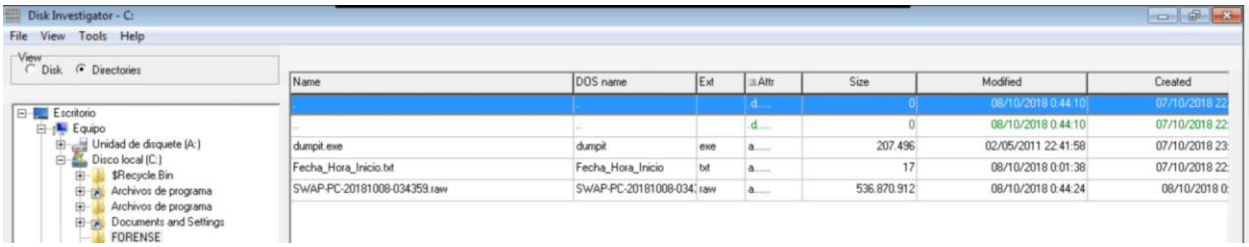
Tenemos un archivo denominado SWAP-PC (es el nombre de la PC utilizada en el ejemplo), fecha, día, hora con un formato .raw.

Luego, se debe obtener el archivo con formato .raw y analizarlo en una ubicación segura.

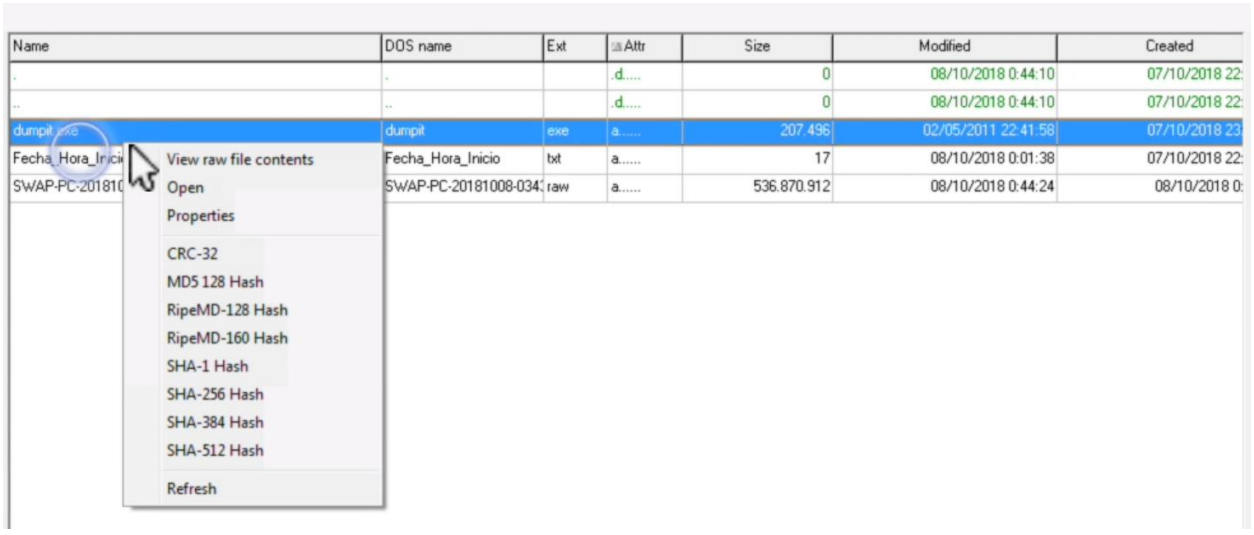
Continuando con el ejemplo, se utilizará la herramienta Disk Investigator.



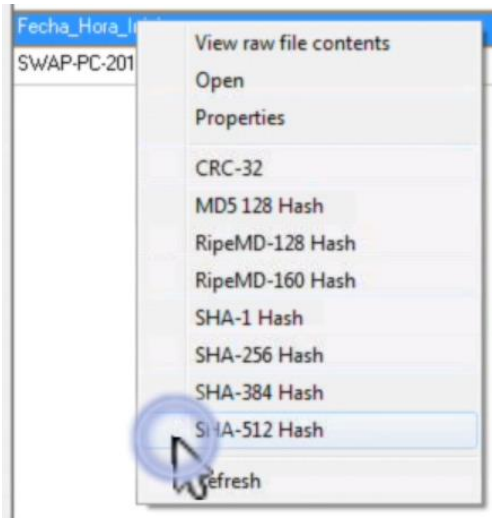
Nota: Para el ejemplo se realiza el análisis en la misma PC, sin embargo, en una investigación forense, este procedimiento deberá ser realizado en una ubicación segura.



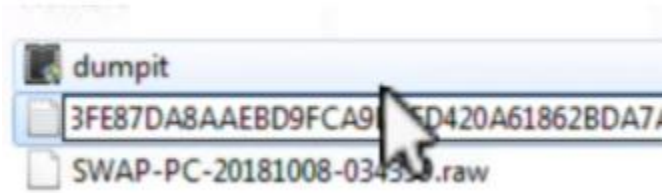
Al hacer click derecho sobre los archivos, se muestra los siguiente:

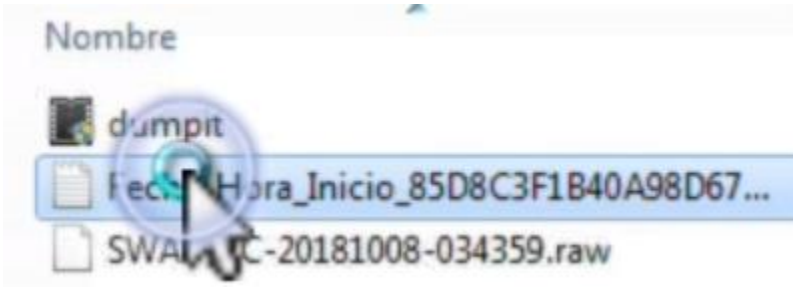


Se recomienda utilizar SHA-256, 384 o 512 Hash, para el ejemplo se utilizará SHA-512 Hash.



Al realizar esto, la herramienta Disk Investigator lee el archivo y genera un Hash, el cual se debe de copiar y añadir al nombre del archivo tal como se muestra a continuación.



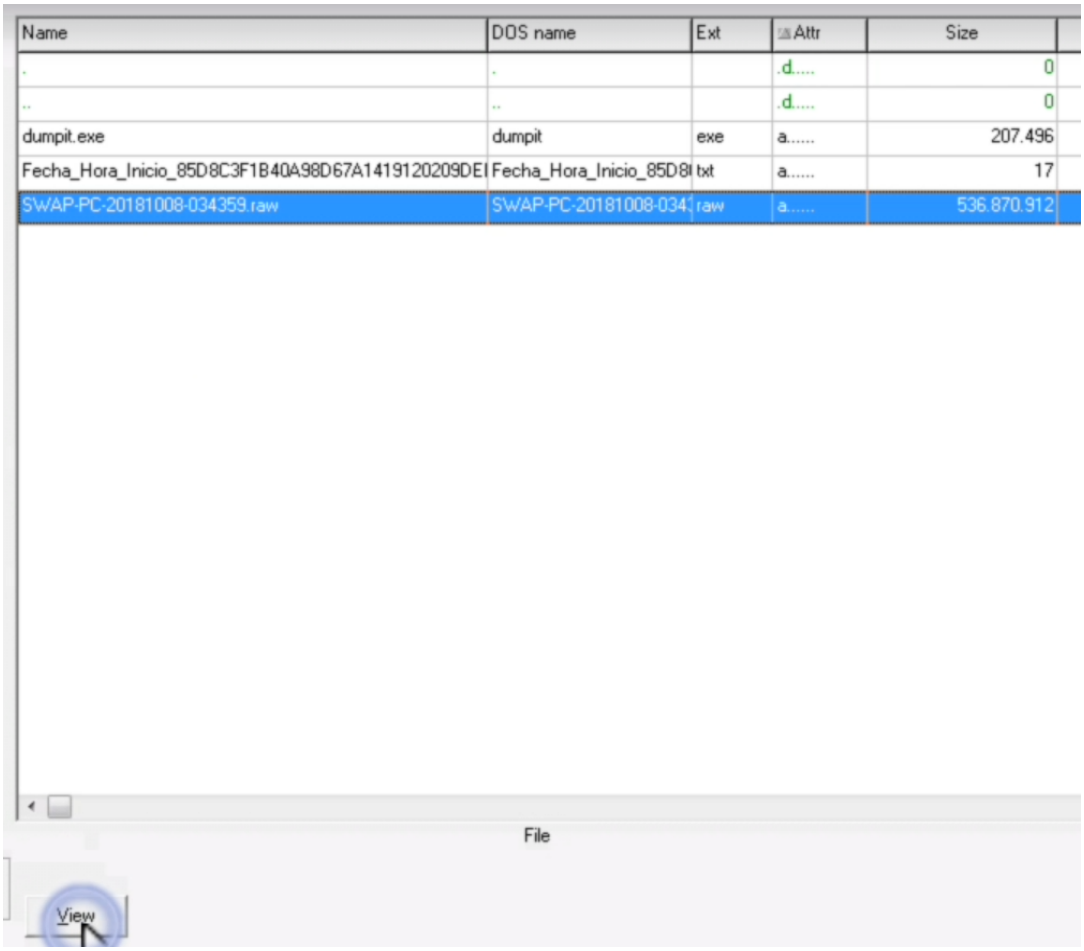


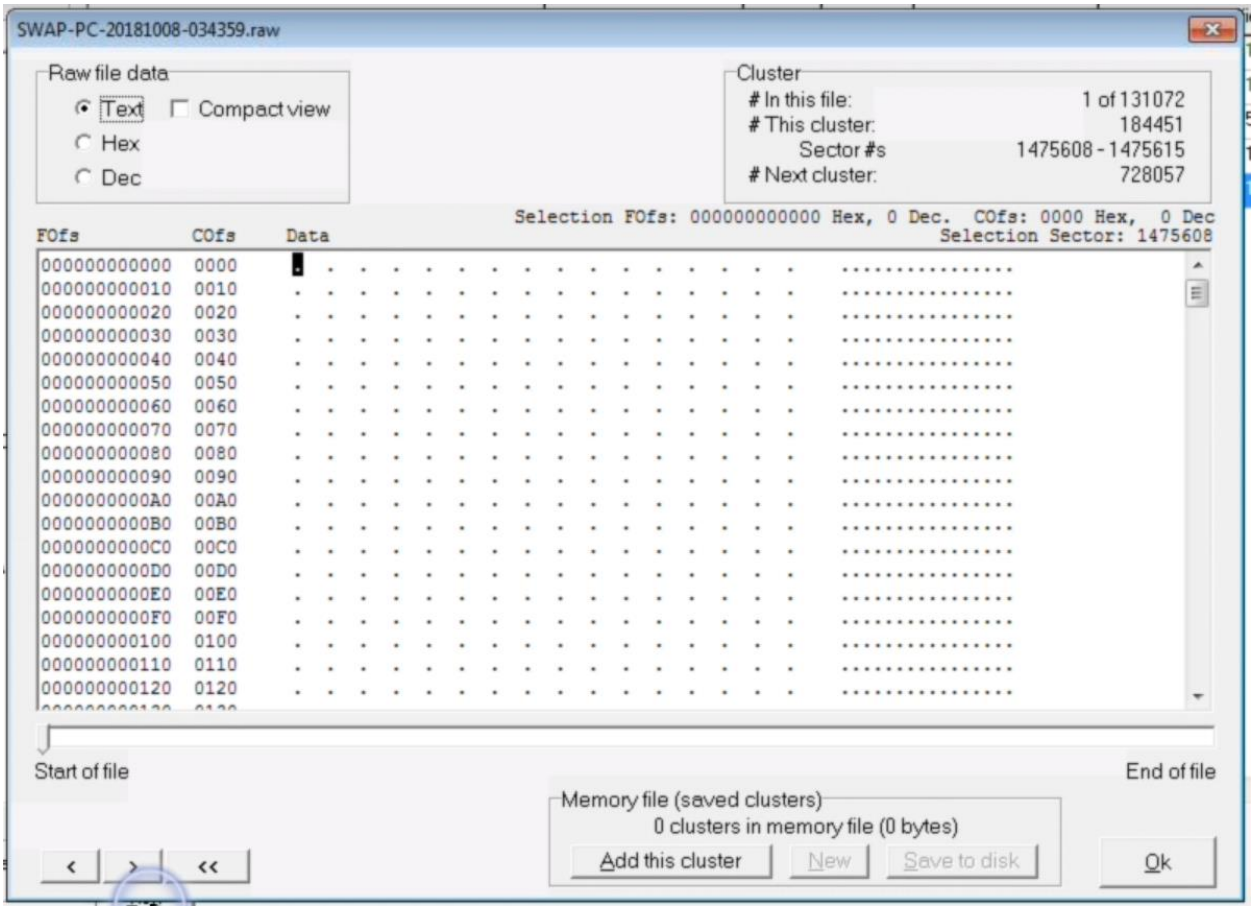
A partir de este momento, a cada toma de evidencia se le debe realizar cálculo de hash, para el ejemplo se utilizó la herramienta Disk Investigator, posteriormente se debe colocar el hash en el nombre del archivo.

De tal manera que, si alguien abriera el archivo y cambiara un 0 por un 1, cuando se vuelve a calcular el hash da un número completamente diferente.

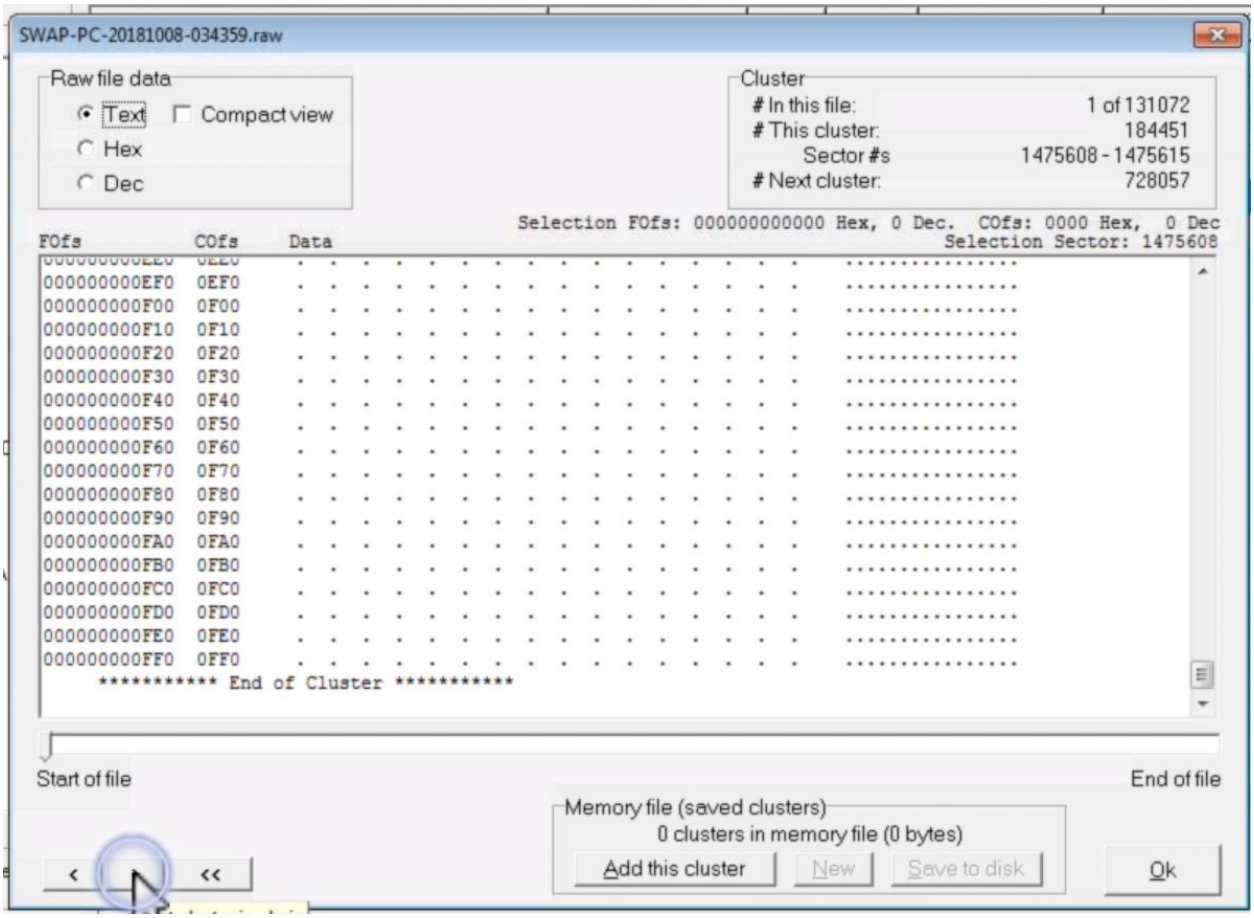
El proceso anterior asegura que la evidencia no sea modificada.

En la herramienta Disk Investigator se puede leer un archivo que tenga medio Giga (para el ejemplo) y que lo cargue inmediatamente, ya que la herramienta lo va cargando por clusters.

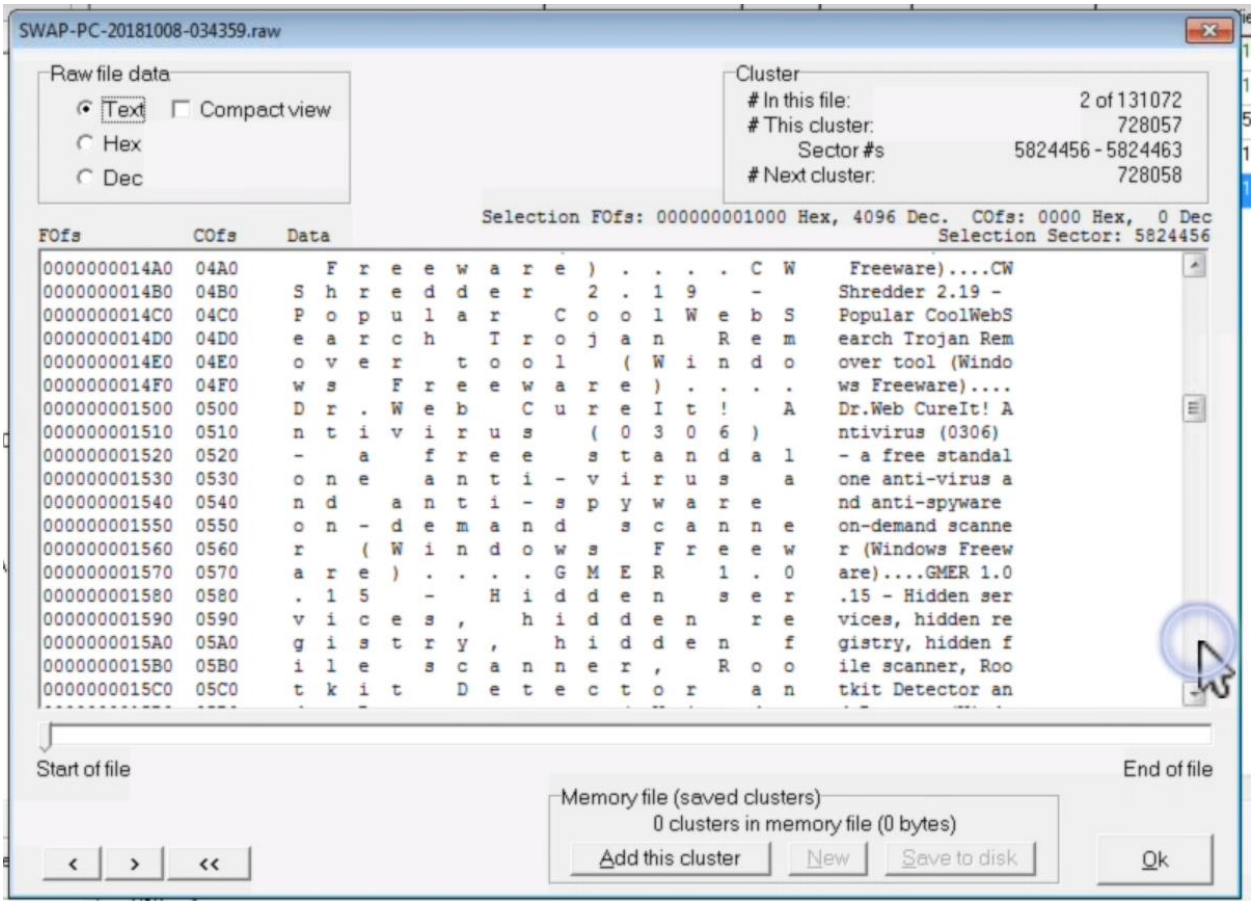



SWAP-PC-20181008-034359.raw
Raw file data
Text
Compact view
Hex
Dec
Cluster
In this file: 1 of 131072
This cluster: 184451
Sector #s 1475608 - 1475615
Next cluster: 728057
Selection FOfs: 000000000000 Hex, 0 Dec. COfs: 0000 Hex, 0 Dec
Selection Sector: 1475608
FOfs COfs Data
Start of file
End of file
Memory file (saved clusters)
0 clusters in memory file (0 bytes)
Add this cluster
New
Save to disk
Ok

Para visualizar el segundo cluster, se da click en el ícono > tal como se muestra a continuación:



Para el ejemplo, se muestra lo siguiente:



Captura de la memoria volátil de paginación en tiempo de ejecución

El archivo de paginación de memoria RAM o memoria virtual de intercambio (swap) se denomina PageFile.sys, un volcado y análisis de dicho archivo puede revelar nombres, contraseñas y recursos de red que hayan sido utilizados por el intruso.

El archivo PageFile.sys generalmente está ubicado en la unidad C, sin embargo, se recomienda realizar una búsqueda de este archivo por si se ha cambiado la ubicación o si la máquina tiene más de una partición de disco duro.

Después de haber volcado la memoria RAM en una PC encendida se debe realizar inmediatamente el volcado del archivo de paginación.

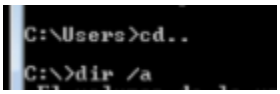
Importante. Existe una opción de borrar el archivo de paginación cuando se apague el sistema, de tal manera que si se realiza un clonado del disco duro se tendrá que apagar la máquina, lo cual borrará el archivo de paginación.

Windows protege el archivo de paginación en tiempo de ejecución.

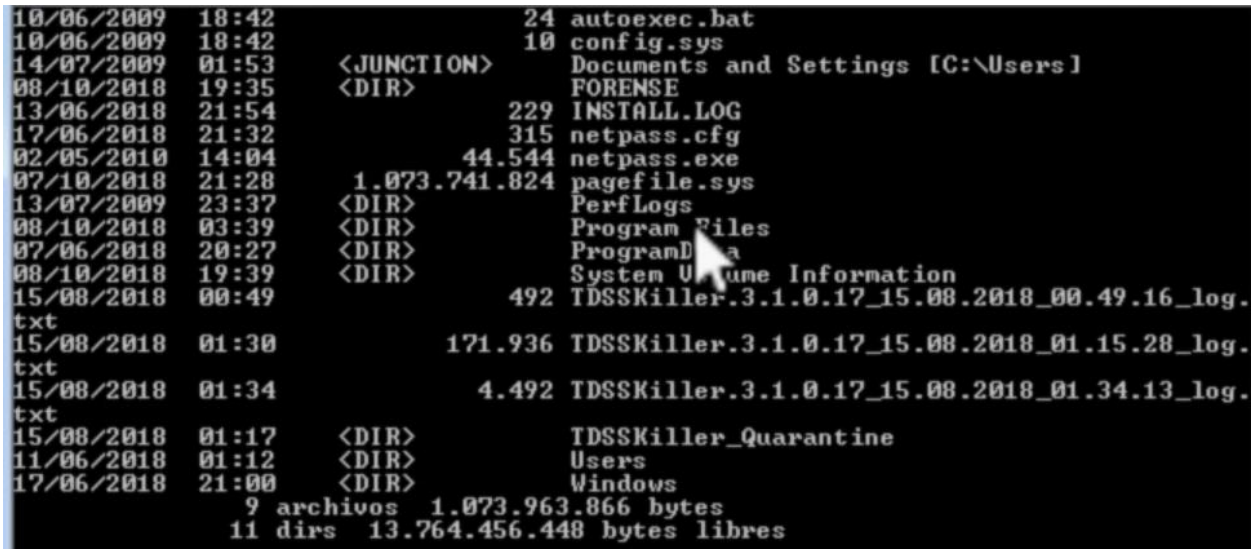
Para el ejemplo se irá a la carpeta raíz que es en donde se encuentra el archivo de paginación, se ejecutan los siguientes comandos en el cmd:

Cd..

Dir /a



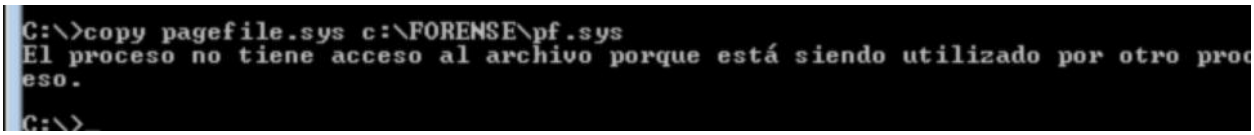
A continuación, se muestran todos los archivos, incluyendo el archivo de paginación pagefile.sys:



Se copiará el archivo de paginación, para realizarlo se ejecutará el siguiente comando:

Copy pagefile.sys c: \Forense\pf.sys

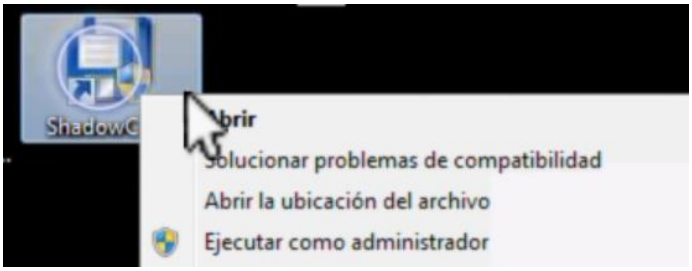
Importante: Para el ejemplo se copia el archivo de paginación en el disco C, sin embargo, en la práctica debe de copiarse en una ubicación segura.



Aunque se ejecute cmd como admin no será posible realizar este comando.

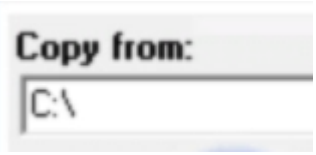
Continuando con el ejemplo, para poder copiar el archivo de paginación en tiempo de ejecución se utiliza la herramienta Shadow copy.

Una vez instalada la herramienta Shadow copy, debe ser ejecutada como admin.

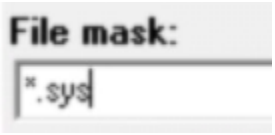


Este software utiliza pss o servicio de copia sombra de Windows, lo cual permite tomar copias de cualquier archivo, aunque esté siendo protegido.

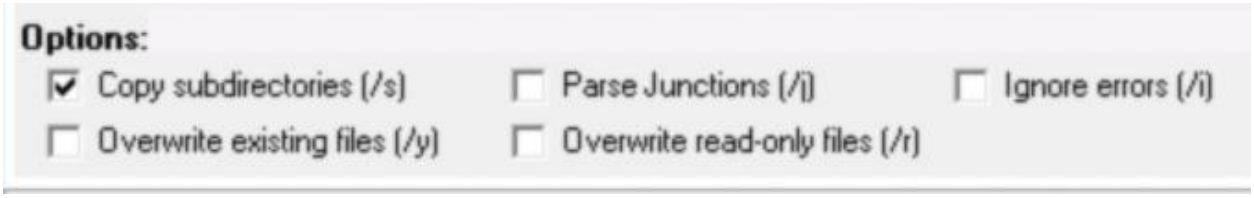
En la sección Copy from se indica desde donde, para el ejemplo se indicará que lo haga desde el disco C que es en donde está ubicado el archivo de paginación

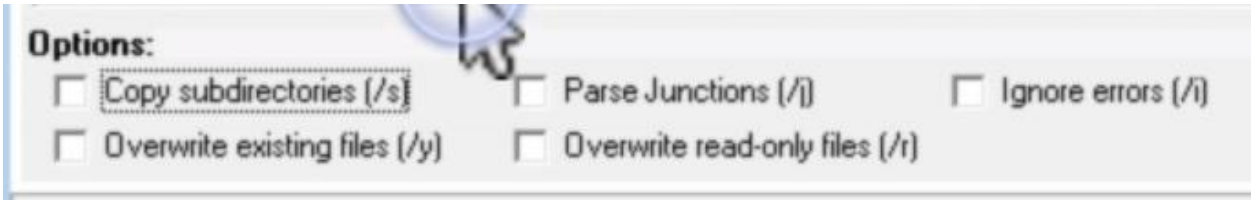


En la sección File mask, se indicará lo siguiente, es decir, todo lo que termine con extensión .sys:

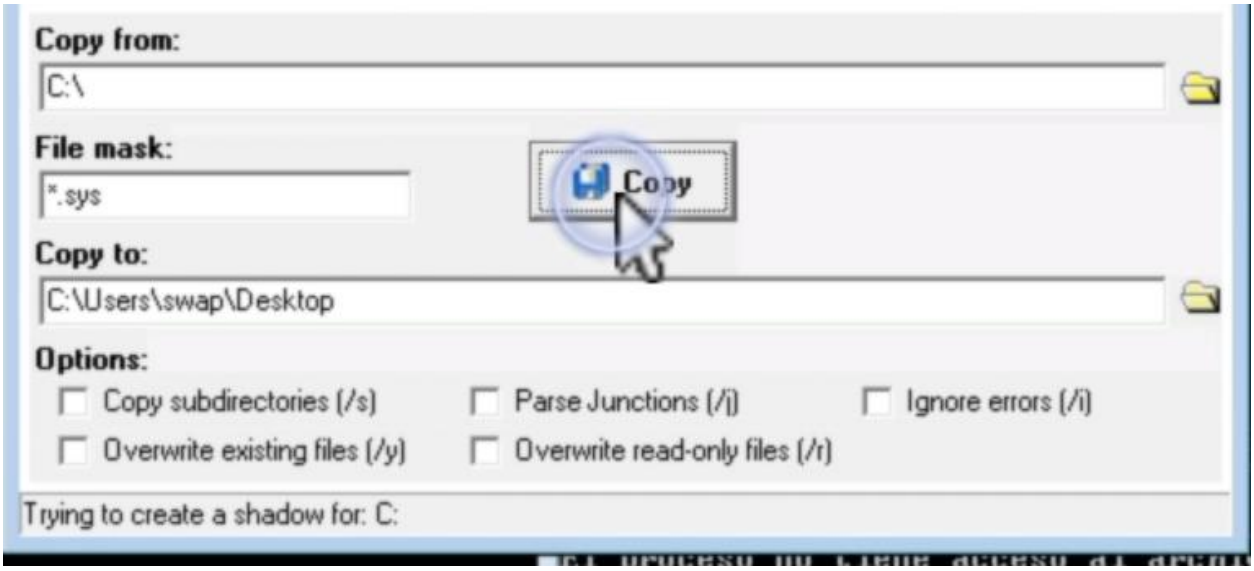


Para el ejemplo, se desmarca la opción Copy subdirectories (/s), ya que si se marca copiaría todo el disco duro.

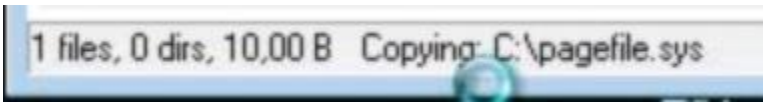




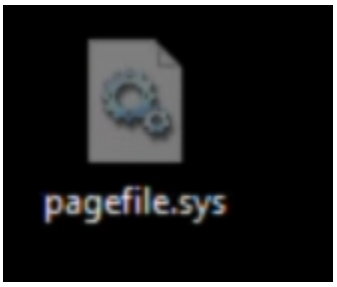
Posteriormente, dar click en Copy.



Al finalizar se mostrará lo siguiente:



Para este ejemplo se indicó que el archivo se guardará en el Desktop:



De esta manera se vence la protección de archivos por uso del sistema operativo.

Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Captura de los Servicios en ejecución

Un servicio es un programa que funciona en segundo plano, transparente al usuario, permite acciones como compartir pantalla, carpetas, archivos, anunciarse en la red, DHCP, cifrados, etc.

Es muy importante obtener la lista de todos los servicios que estén ejecutándose en la máquina afectada para verificar los servicios que se encuentren detenidos, así como validar si han plantado servicios de acceso remoto o servicios que posibilitan compartir carpetas o escritorio.

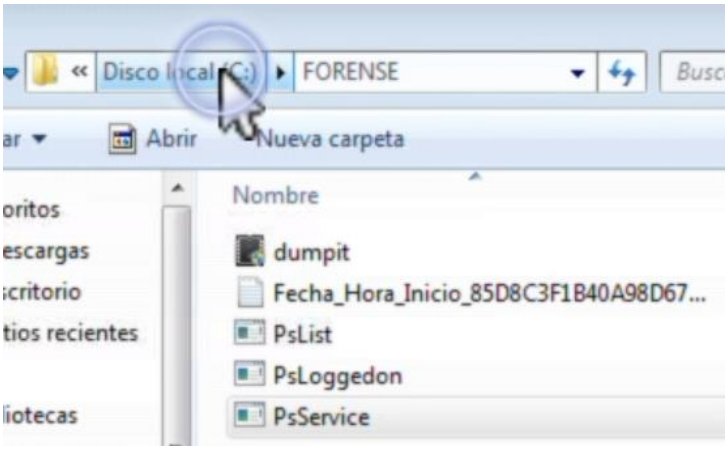
Se debe tomar una instantánea de todos los servicios que se estén ejecutando en la máquina afectada, es recomendable utilizar aplicaciones que no sean del sistema operativo, ya que podrían estar comprometidos con un rootkit lo cual afectaría la toma de evidencias.

Para realizar la captura de los servicios en ejecución se utiliza la herramienta PsService.exe con el siguiente comando:

PsServide.exe > servicios.txt

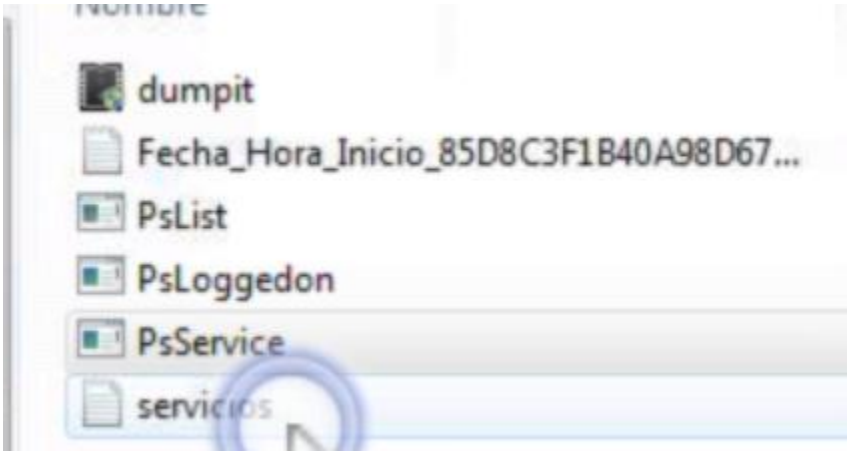
```
C:\FORENSE>PsService.exe > servicios.txt
```

Importante: Las carpetas mostradas en el ejemplo estarían en un pendrive protegido contra escritura solamente read only en una investigación forense y en el segundo pendrive se volcaría la evidencia..



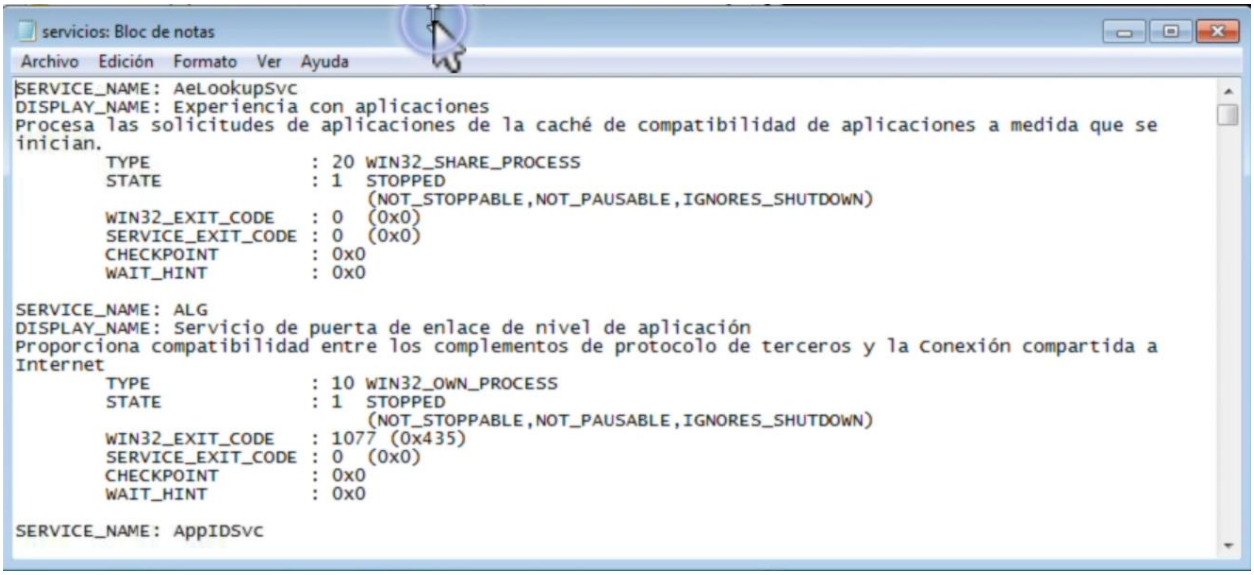
Al presionar enter, se muestra el banner de la herramienta:

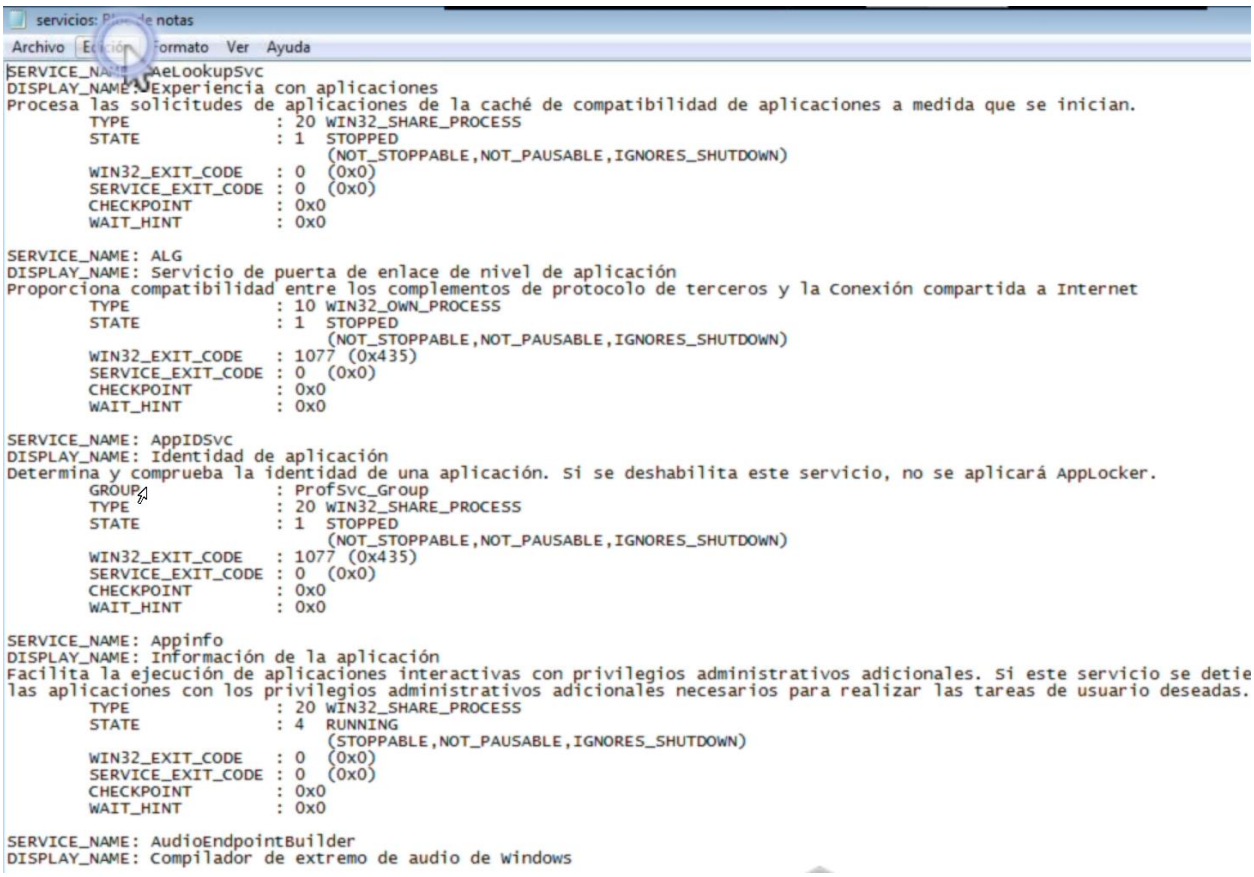
Como se aprecia en la siguiente imagen, se generó el archivo servicios.txt:



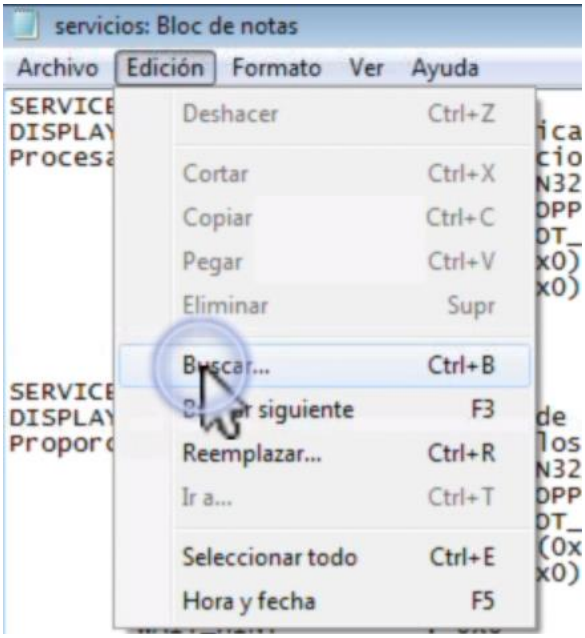
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

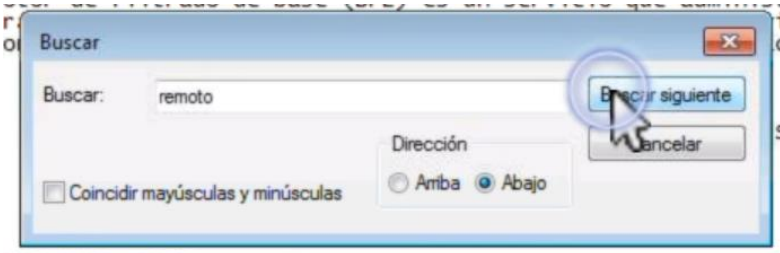
Al abrir el archivo muestra lo siguiente:





Se pueden establecer filtros con palabras clave tal como se muestra a continuación:






```
ICE_NAME: BITS
LAY_NAME: Servicio de transferencia inteligente en segundo plano (BITS)
sfiere archivos en segundo plano mediante el uso de ancho de banda de red inactivo. Si
, como Windows Update o MSN Explorer, no podrán descargar programas ni otra información
    TYPE               : 20 WIN32_SHARE_PROCESS
    STATE              : 1  STOPPED
                            (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 1077 (0x435)
    SERVICE_EXIT_CODE  : 0  (0x0)
    CHECKPOINT         : 0x0
    WAIT_HINT          : 0x0

ICE_NAME: Browser
LAY_NAME: Examinador de equipos
iene una lista actualizada de equipos en la red y proporciona esta lista a los equipos
a no se actualizará o mantendrá. Si se deshabilita el servicio, no se podrá iniciar ning
    GROUP              : NetworkProvider
    TYPE               : 20 WIN32_SHARE_PROCESS
    STATE              : 1  STOPPED
                            (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 1077 (0x435)
    SERVICE_EXIT_CODE  : 0  (0x0)
    CHECKPOINT         : 0x0
    WAIT_HINT          : 0x0

ICE_NAME: bthserv
LAY_NAME: Servicio de compatibilidad con Bluetooth
ervicio Bluetooth admite la detección y asociación de dispositivos Bluetooth remotos. S
```

Captura de los Procesos en ejecución

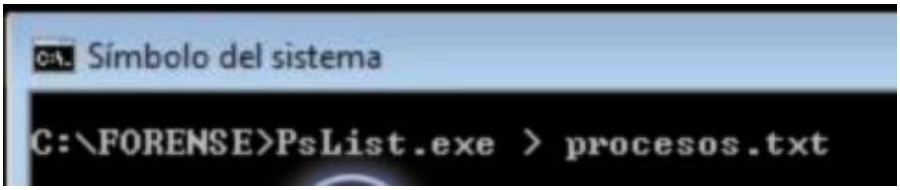
Un proceso es una secuencia de instrucciones, registros, variables y recursos asignados, es el acto necesario para la ejecución de una aplicación por parte del sistema operativo.

Se debe tomar una instantánea de todos los procesos que estén ejecutándose en la máquina comprometida.

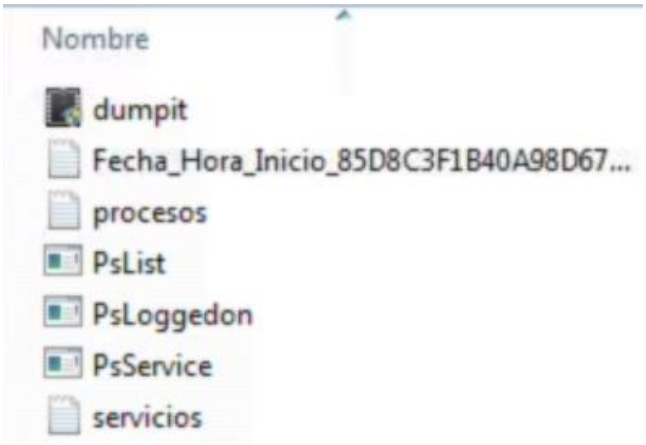
Lo que se busca son procesos de alguna aplicación que por ejemplo pueda realizar buffer overflow, un cambio de espacio de memoria para ganar privilegios de admin, escalación de privilegios, procesos que traten de matar antivirus, que traten de agregar usuarios, que traten de agregar excepciones al firewall de Windows, etc.

Para el ejemplo, se utilizará la herramienta PsList.exe, para ello, se ejecuta el siguiente comando:

PsList.exe > procesos.txt

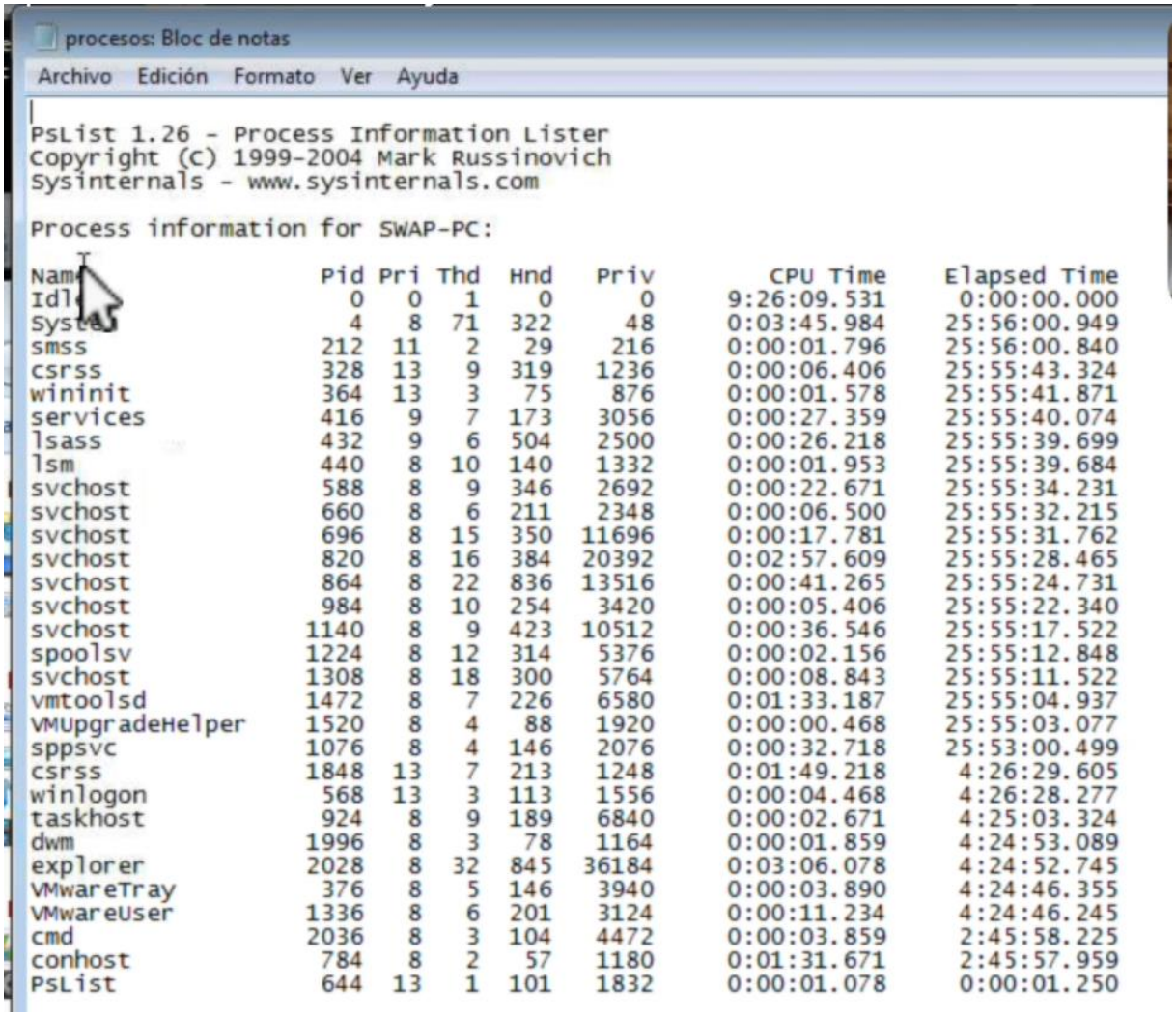


Posteriormente, se genera el archivo procesos.txt tal como se muestra en la siguiente imagen:



Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Al abrirlo, muestra lo siguiente:



Importante: siempre se debe verificar que el proceso con nombre Idle tenga PID = 0, el número de proceso se va incrementando a medida que se van dando los pasos naturales de procesos. Si el Idle tiene un valor diferente de 0, indicaría un rootkit, llamada de acceso remoto, etc.

Captura de la lista de usuarios e inicios de sesión

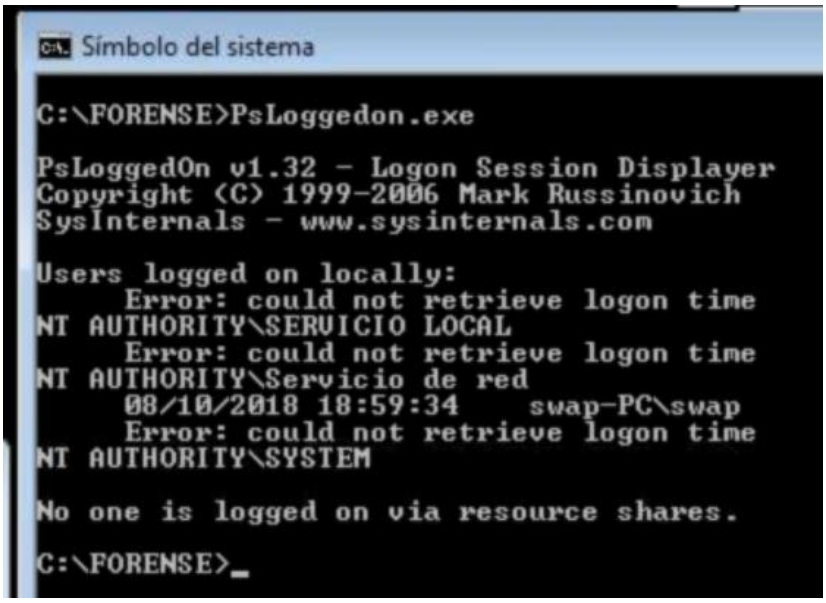
Existen usuarios humanos y usuarios máquina.

El inicio de sesión se da cuando un usuario o proceso gana acceso a un sistema cerrado.

Se debe tomar una instantánea de los usuarios del sistema.

Se debe realizar una captura del estado de los usuarios y en donde ha iniciado sesión.

Para el ejemplo se utilizará la herramienta PsLoggedon.exe:

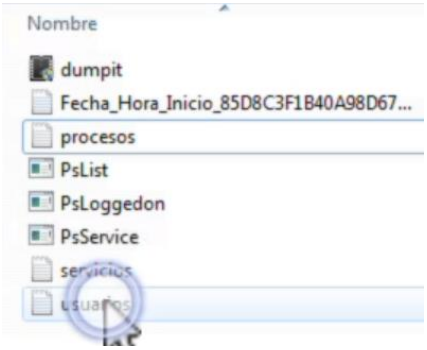


Al ejecutar la herramienta, muestra información de usuarios y fechas de inicio de sesión, sin embargo, es necesario guardar dicha información en un archivo, motivo por el se ejecuta el siguiente comando:

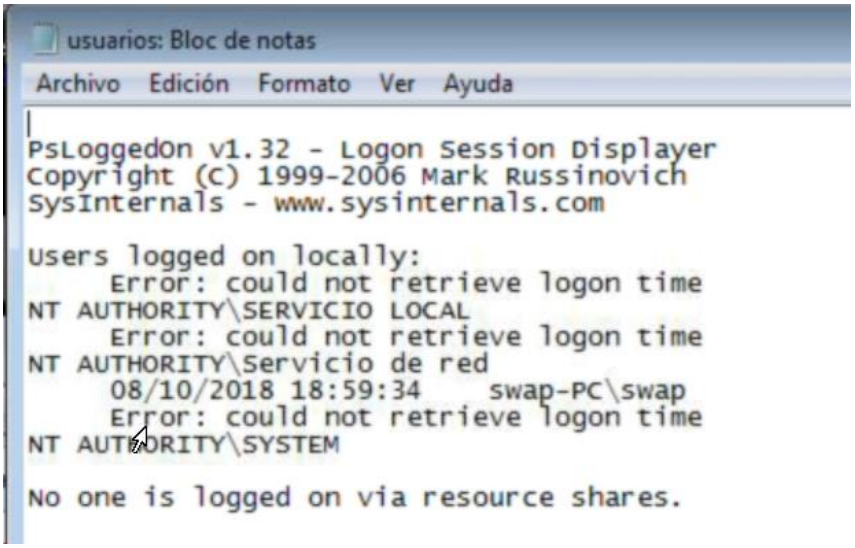
Psloggedon.exe > usuarios.txt

Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Posteriormente, el archivo es generado y al ingresar se valida que la información mostrada en el cmd se muestre en el archivo generado.



Al abrir el archivo, se muestra la siguiente información:

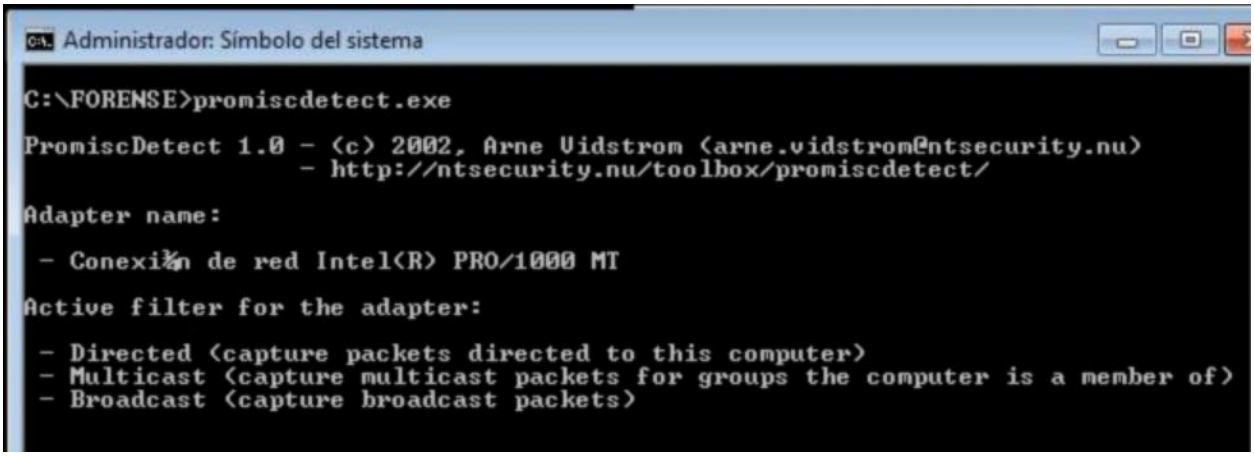


Nota: No se recomienda utilizar comandos del sistema operativo en la máquina comprometida.

Captura del estado de la red

Es muy importante saber si no existen tarjetas de red o NIC en modo promiscuo.

Para el ejemplo, se utilizará la herramienta promiscdetect.exe:



Al ejecutar la herramienta, se indica que la conexión de red se está efectuando a través de una única tarjeta de red, para el ejemplo se muestra una placa con chipset Intel a 1 GB, los roles de esa tarjeta son:

- Directo o Unicast.
- Multicast, que significa que puede enviar un paquete desde su dirección de red hacia un grupo determinado.
- Broadcast, es decir, que puede enviar un mensaje desde esta placa hacia toda la red.

Entre los roles no se muestra promisc, lo cual indica que no tiene el modo promiscuo entre sus roles.

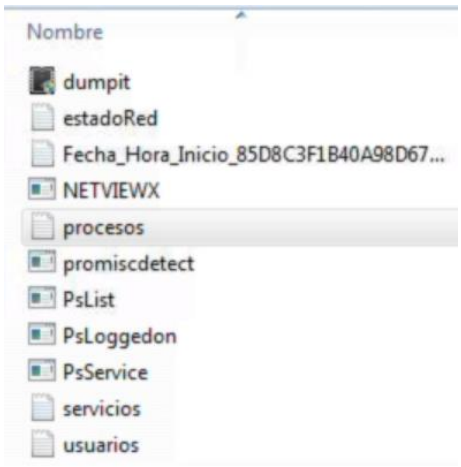
Continuando con el ejemplo, se utilizará la herramienta NETVIEWX.EXE

Al ejecutar la herramienta NETVIEWX a secas nos dará como resultado los roles que tiene esa máquina, un rol es una capacidad, tal como se muestra a continuación:

Se ejecutará el siguiente comando con el propósito de guardar en aun archivo la información proporcionada por la herramienta promiscdetect.exe:

```
C:\FORENSE>promiscdetect.exe > estadoRed.txt
```

Posteriormente, el archivo es generado:



Se ejecutará el siguiente comando para añadir al archivo estadoRed.txt la información proporcionada por la herramienta NETVIEWX

```
C:\FORENSE>NETVIEWX.EXE >> estadoRed.txt
```

Se podría utilizar las herramientas nativas del sistema operativo sacándolas de otro sistema operativo en el que se tenga la certeza de que esta limpio o recién instalado y luego colocándolas en el pendrive forense, para luego ejecutar las herramientas nativas de Windows desde el pendrive forense.

Para el ejemplo, se realizan las siguientes validaciones:

```
C:\FORENSE>arp -a

Interfaz: 192.168.43.77 --- 0xb
  Dirección de Internet          Dirección física      Tipo
  192.168.43.20          00-0c-29-40-55-53     dinámico
  192.168.43.40          00-0c-29-a7-9c-32     dinámico
  192.168.43.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.22             01-00-5e-00-00-16     estático
  224.0.0.252            01-00-5e-00-00-fc     estático
  239.255.255.250        01-00-5e-7f-ff-fa     estático
  255.255.255.255        ff-ff-ff-ff-ff-ff     estático
```

El protoclo arp vincula todas las direcciones IP a las que se haya conectado esa máquina y por ende el intruso, con las direcciones MAC.

La información proporcionada por el protocolo arp puede ser añadida al archivo estadoRed mediante el siguiente comando:

```
C:\FORENSE>arp -a >> estadoRed.txt
```

Otra validación a realizar es el estado de las tablas de Net BIOS, para lo cual, se ejecuta el siguiente comando, el cual mostrará una tabla de Net BIOS con todo lo que conoce:

```
C:\FORENSE>nbtstat -c

Conexión de área local:
Dirección IP del nodo: [192.168.43.77] Id. de ámbito : []

                Tabla caché remota de NetBIOS

    Nombre             Tipo       Dir de Host     Vida [s]
    ------------------------------------------------------------
    WINDOZE2KADV   <00>  Único            192.168.43.20       142
```

De acuerdo con la salida, se puede determinar que la máquina comprometida ha tenido comunicación con la máquina con nombre WINDOZE2KADV con IP 192.168.43.20.

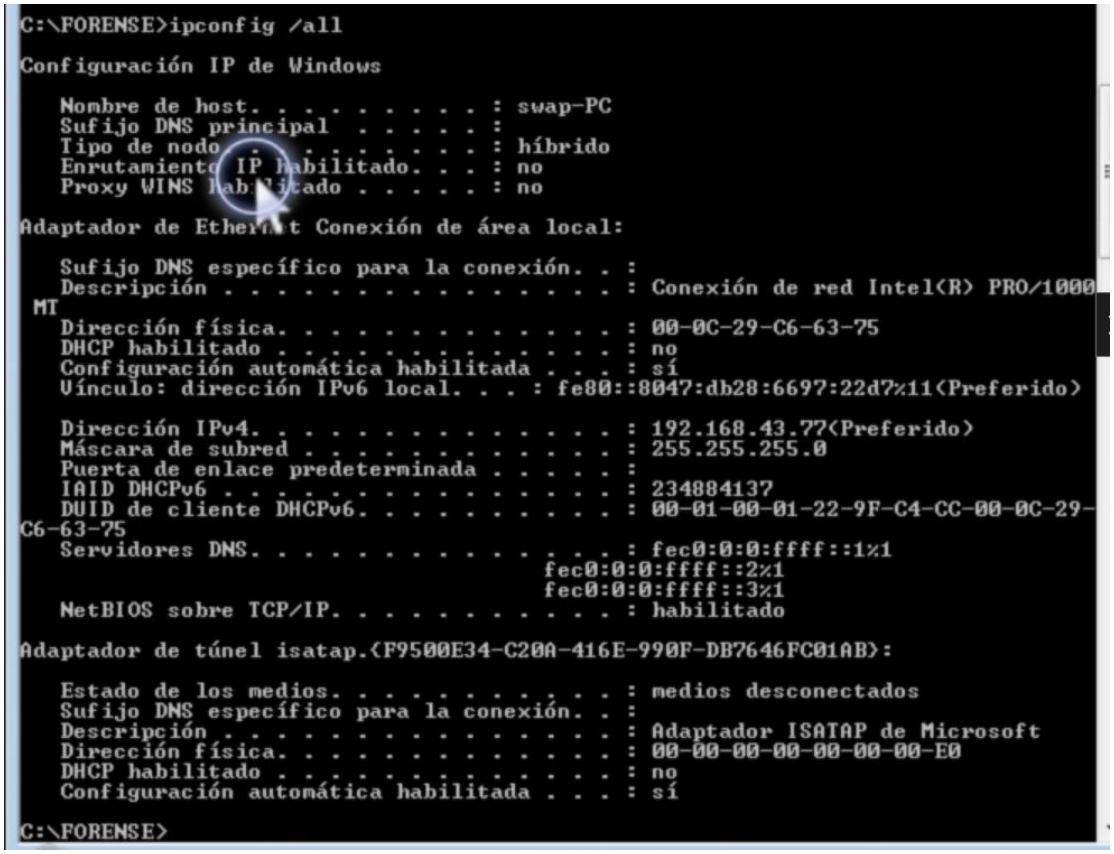
Se añade esta información al archivo de evidencias mediante el siguiente comando:

```
C:\FORENSE>nbtstat -c >> estadoRed.txt
```

Para obtener información sobre los adaptadores, se ejecuta el siguiente comando:

```
C:\FORENSE>ipconfig /all
```

Para el ejemplo, muestra lo siguiente:



Se añade esta información al archivo de evidencias mediante el siguiente comando:

```
C:\FORENSE>ipconfig /all >> estadoRed.txt
```

Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Es necesario validar a que sitios se ha podido conectar el intruso, por lo tanto, se ejecuta el siguiente comando:

```
C:\FORENSE>ipconfig /displaydns
```

Para validar el estado de las conexiones de todos los puertos de la máquina comprometida se ejecuta el siguiente comando:

```
C:\FORENSE>netstat -an
```

```
C:\FORENSE>netstat -an

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    192.168.43.77:139      0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
  TCP    [::]:49154             [::]:0                 LISTENING
  TCP    [::]:49155             [::]:0                 LISTENING
  TCP    [::]:49156             [::]:0                 LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:52207          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:52204        *:*
  UDP    192.168.43.77:137      *:*
  UDP    192.168.43.77:138      *:*
  UDP    192.168.43.77:1900     *:*
  UDP    192.168.43.77:52203    *:*
```

Sección 2: Toma de evidencias no volátiles (Unidades de Almacenamiento)

Captura BitStream o clonado del disco duro

Existen 3 tipos de toma de evidencias desde discos duros:

1. Copia Clon o BitStream
2. Copia a imagen.
3. Por árbol de carpetas.

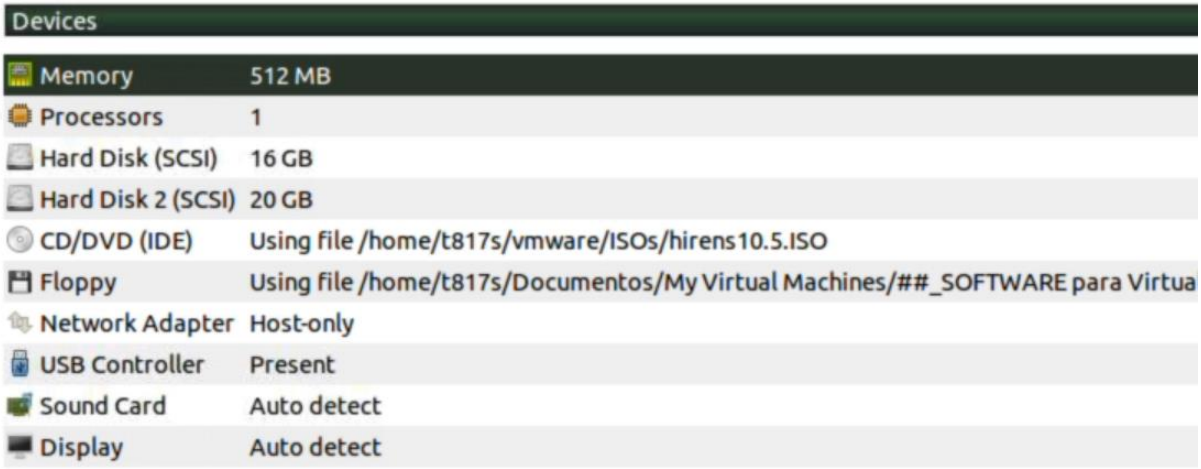
La copia a imagen permite recrear varias veces la evidencia y es menos costosa.

Para los ejemplos de esta sección se utilizará una imagen en live CD del Norton Ghost, Norton Ghost es un software que permite hacer clon de discos o de particiones a otro disco a imágenes con la característica de que cuando lo hace a imágenes permite hacer a imagen formato .gho que es propia del software o a imágenes. vmdk que son imágenes de disco duro listas para utilizar en el ejemplo.

Desconectar bruscamente la toma de energía es útil para evitar ciertos borrados reprogramados por el intruso o por el sistema operativo.

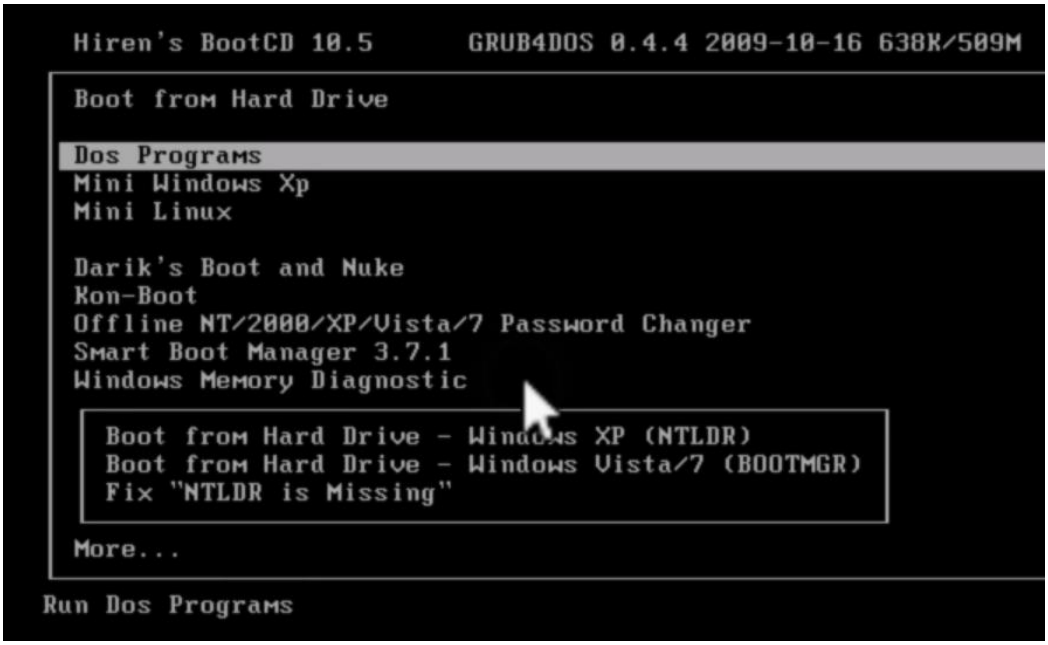
En el caso de tratarse de un equipo portátil tal como una laptop, primero es necesario remover la batería, posteriormente se debe de desconectar el cargador del tomacorriente, lo anterior se realiza para no dar lugar a que se borren ciertos archivos.

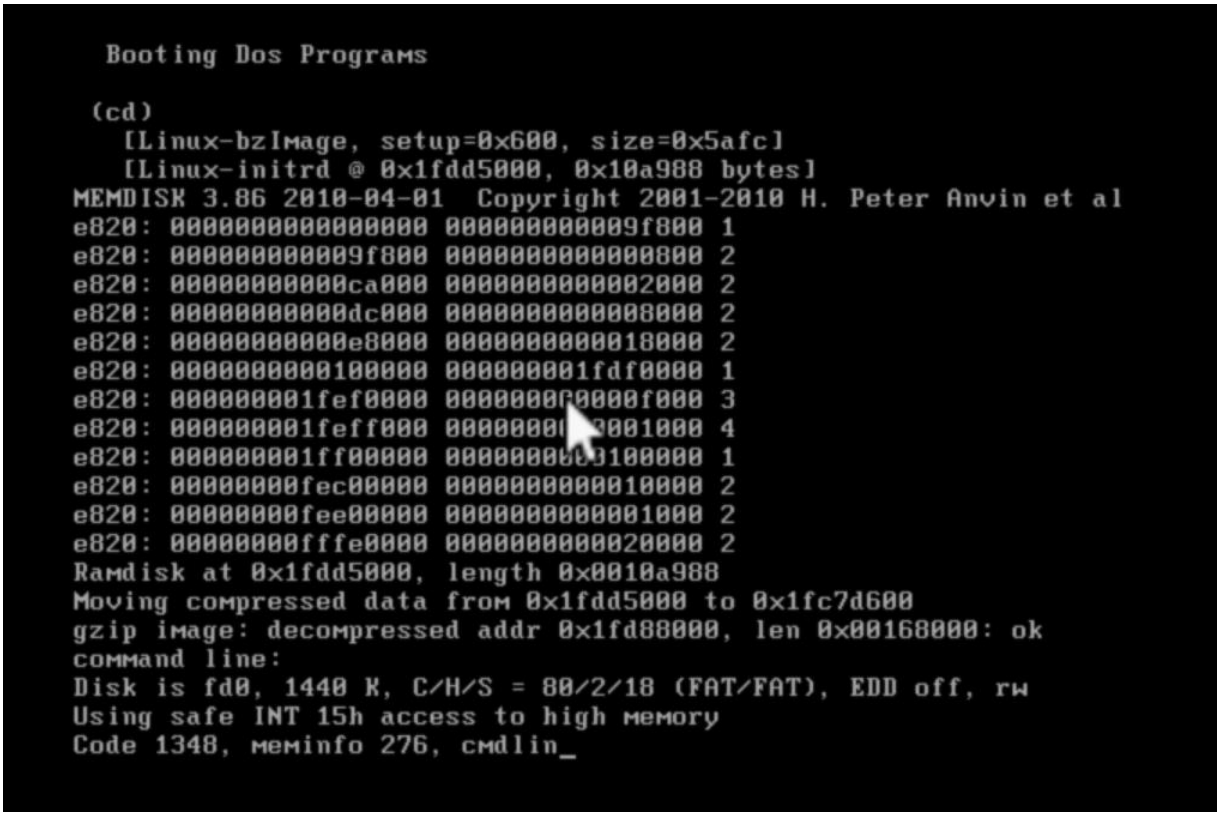
Continuando con el ejemplo, se utilizará una máquina virtual con Windows 7, el disco 2 de 20 GB se tomaría como el disco real del investigador forense.



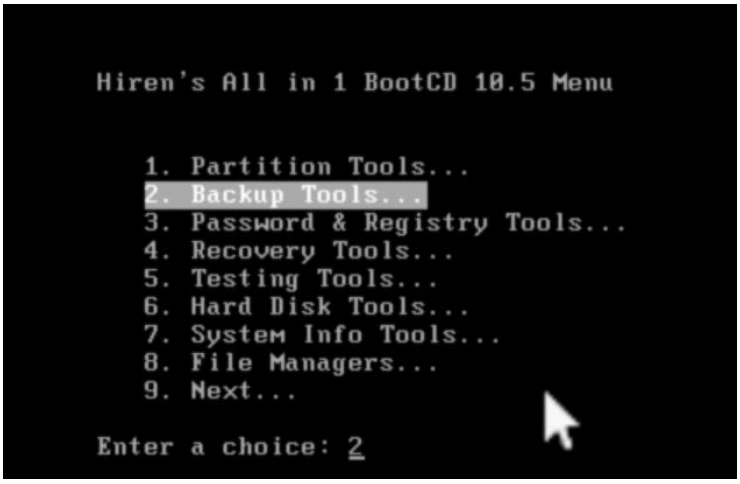
A continuación, se muestra el procedimiento a realizar con el software Norton Ghost:

Al iniciar la máquina virtual se elige la opción Dos Programs, tal como se muestra en la siguiente imagen:

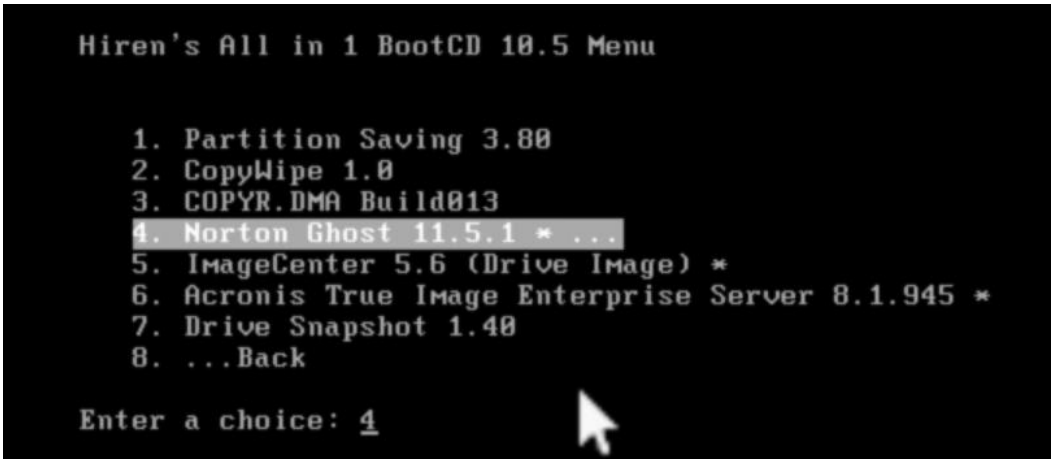




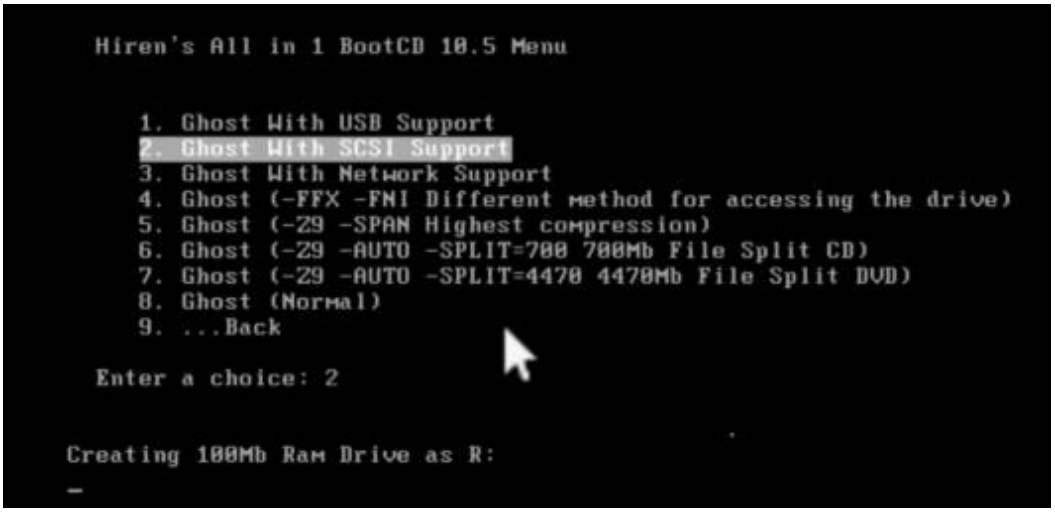
Luego se elígela opción Backup Tools.



Posteriormente, se debe elegir la opción 4 que es la de Norton ghost.

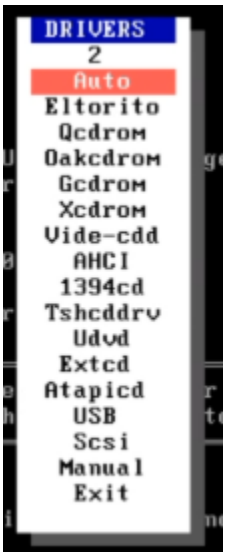


Se elige la opción 2.

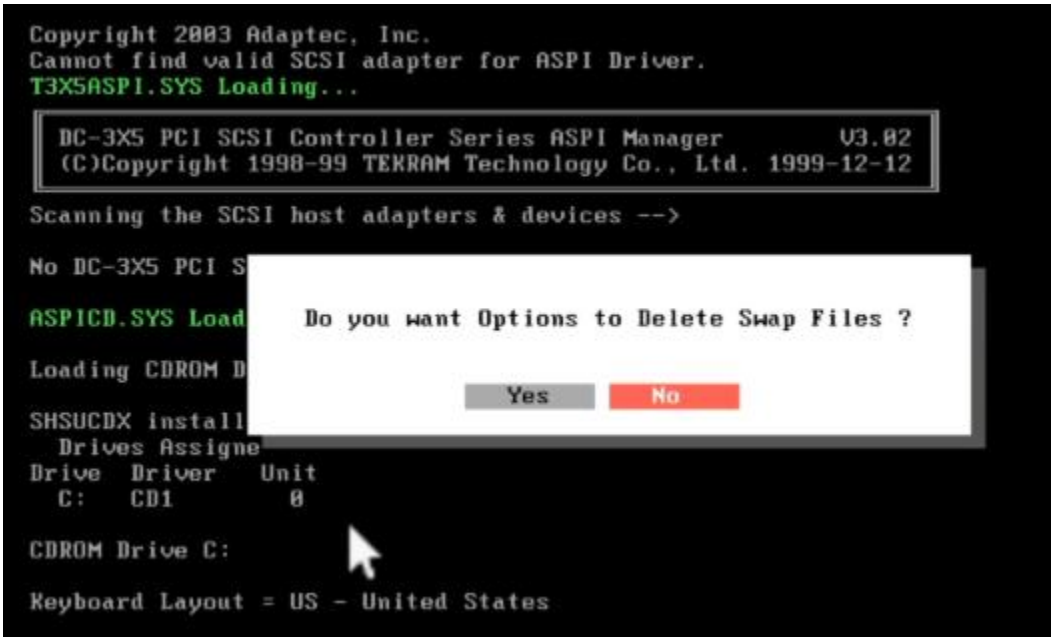


Se elige la opción Si:

Se elige la opción Auto:

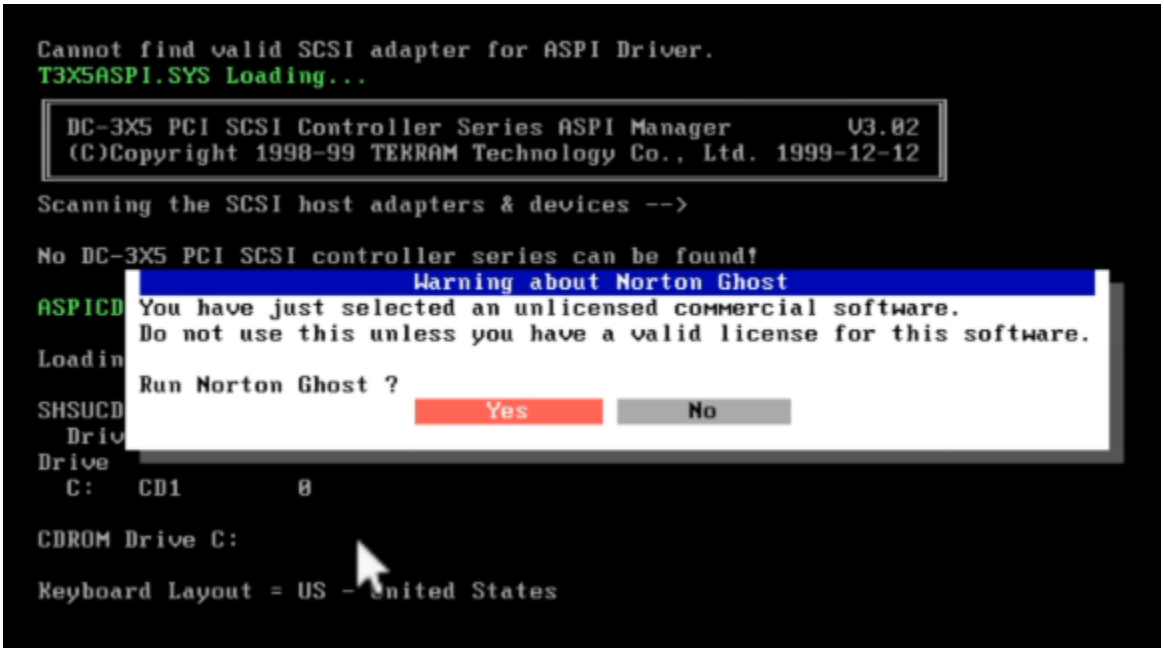


Se elige la opción No:

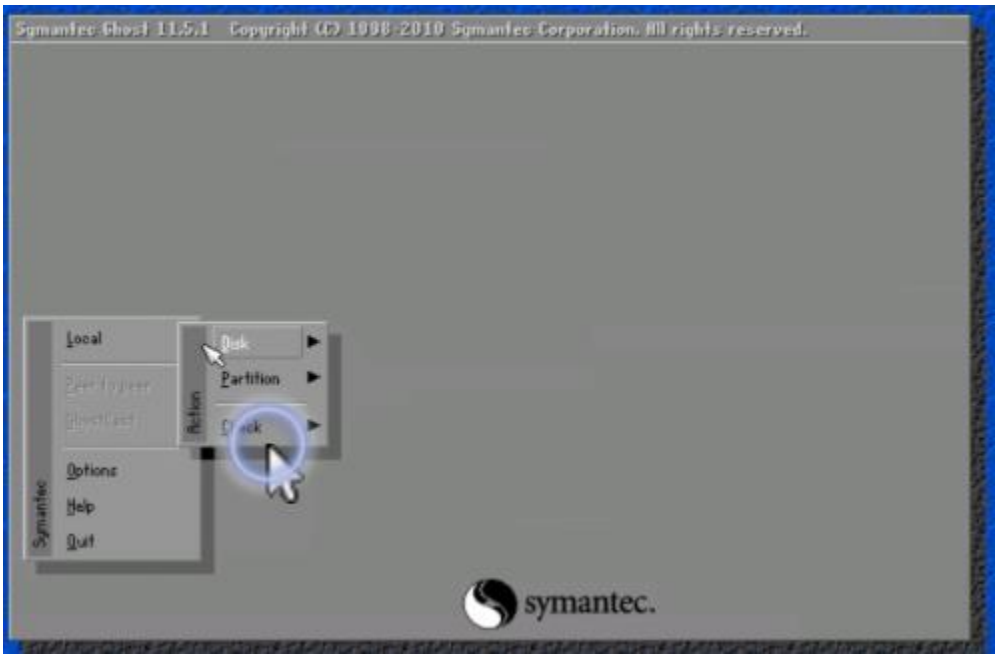


Se elige la opción No:

Se elige la opción Si:

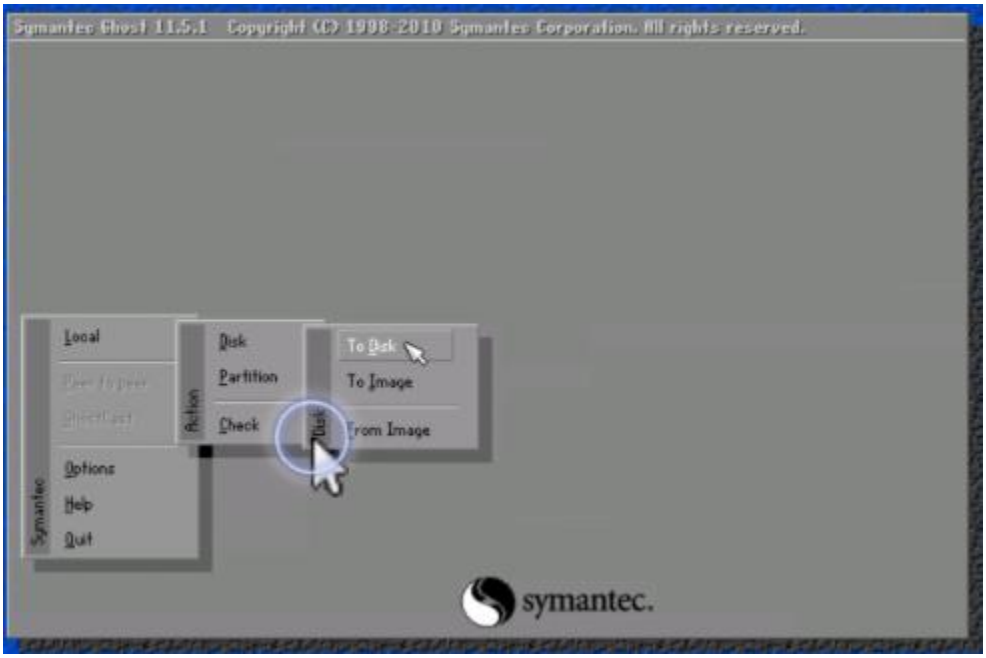


Al cargar, Norton Ghost da la opción de copiar Discos o Particiones.

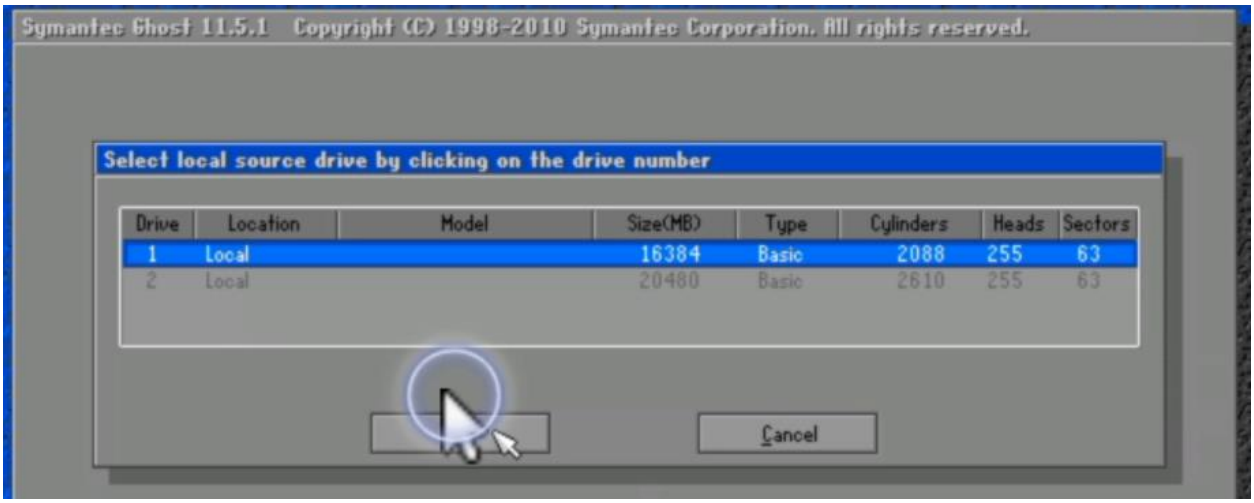


Para el ejemplo, se realizará un clonado BitStream de todo el disco duro.

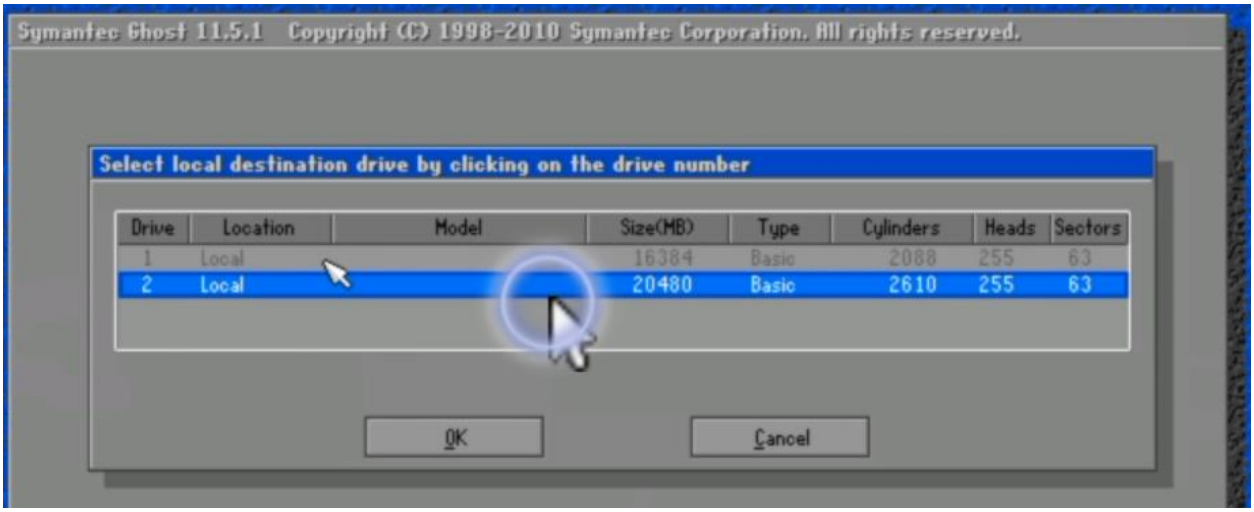
Por lo tanto, se elige la opción Disk > To Disk.



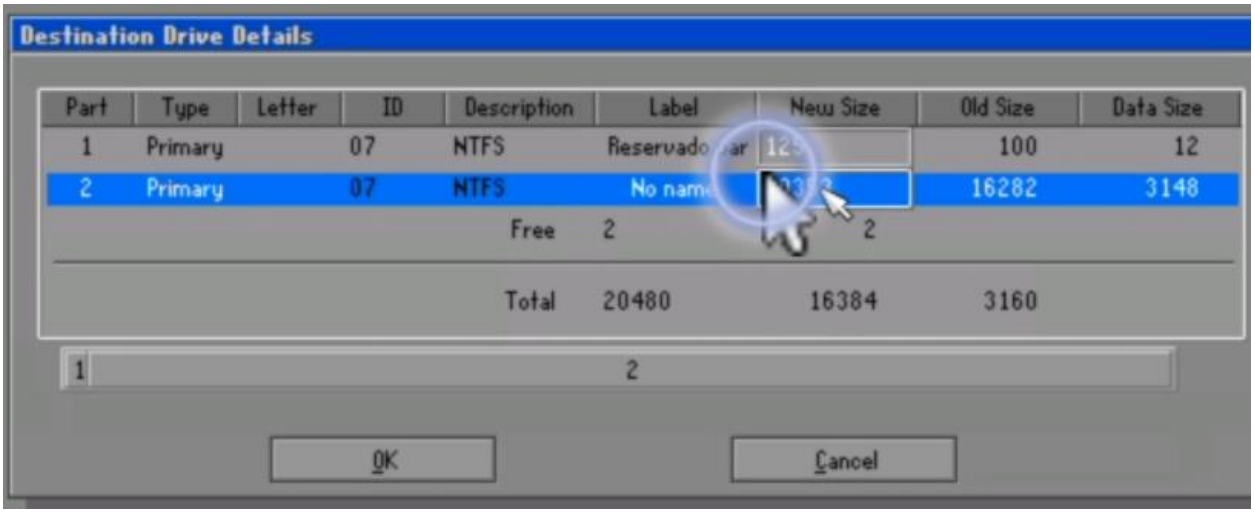
Se selecciona el disco de 16 GB como la fuente.



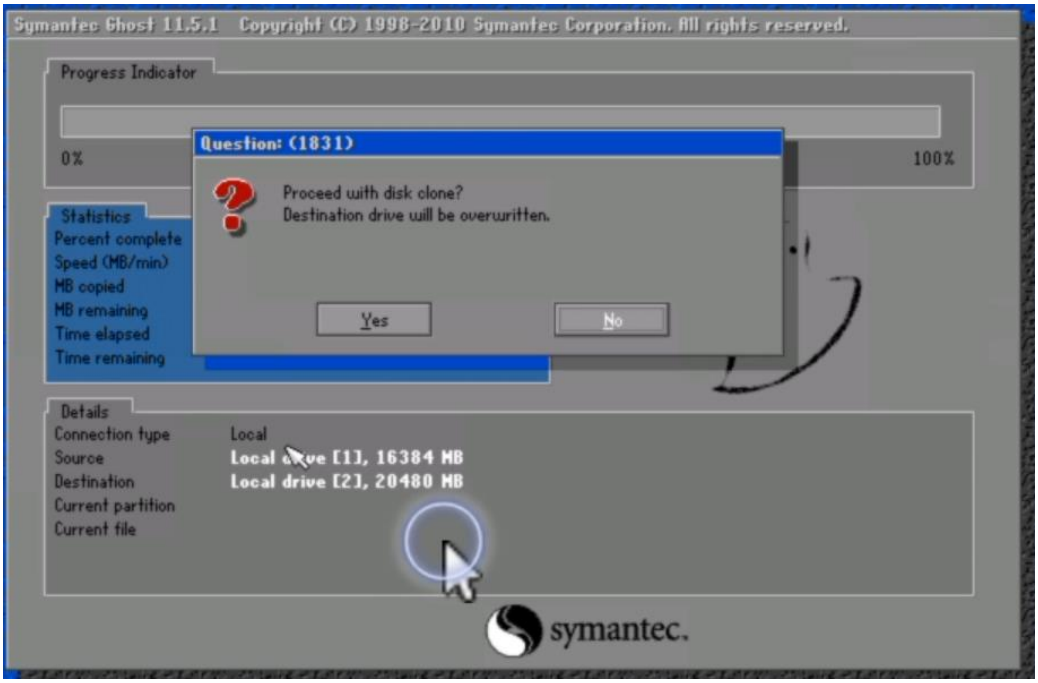
Luego se selecciona el otro disco (de 20 GB) como destino.

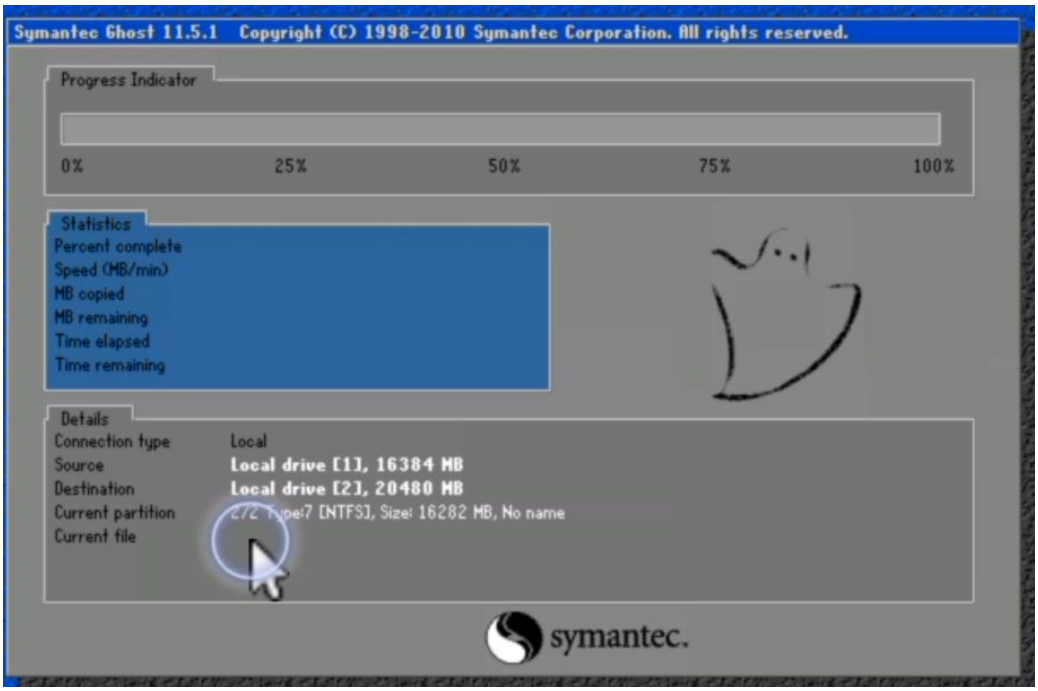


Al dar click en OK se muestran las particiones del disco de destino, se selecciona la partición 2 y click en OK.



Se elige la opción Si:





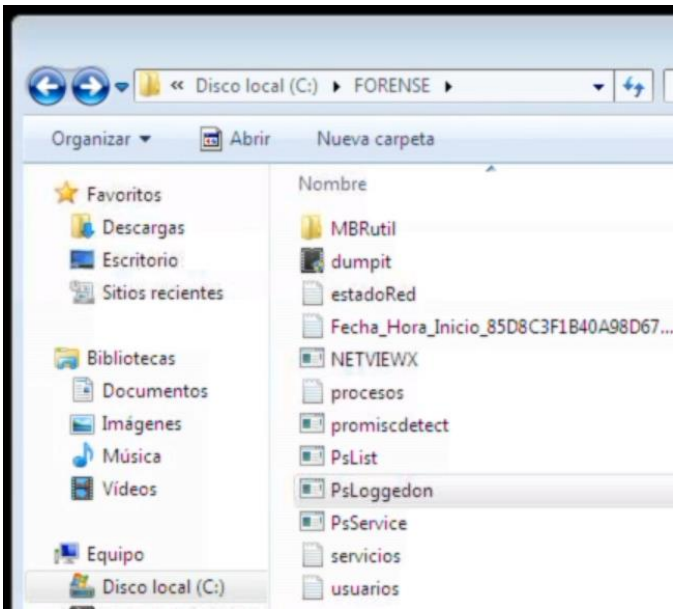
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Captura del sector de Inicio Maestro MBR

El MBR o Master Boot Record posee 512 bytes y es lo primero que se lee en un disco duro, el MBR contiene el número de particiones, desde que sector se inicia y en qué sector termina cada una de las particiones, también almacena cual es la partición activa que es la que arranca el sistema operativo al encender un equipo.

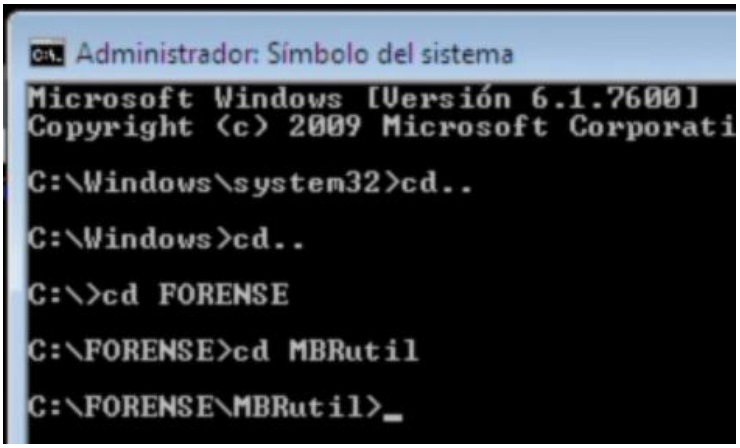
Una partición en un disco duro es una forma lógica de dividir un disco físico, de tal manera que el sistema operativo identifica cada partición como un disco diferente.

Para ejemplificar la copia del MBR, se utilizará la herramienta MBRutil.

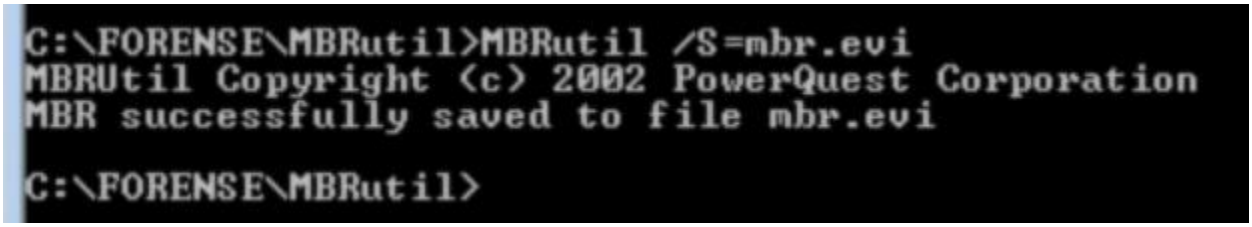


Se ejecuta el cmd como admin.

Es necesario ir a la ubicación en donde está colocada la herramienta, posteriormente se ingresa a la carpeta tal como se muestra a continuación:

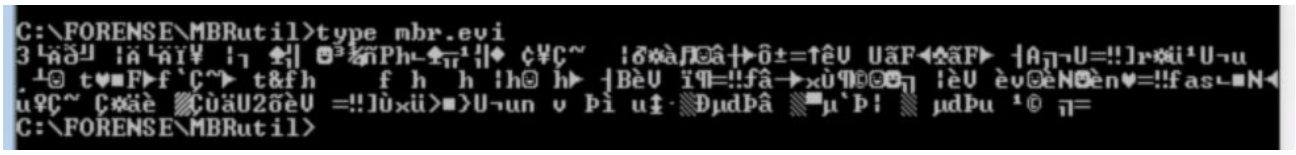


Una vez en la carpeta, se ejecuta el siguiente comando: MBRUtil /S=mbr.evi



Se indica que el MBR fue guardado en el archivo mbr.evi

Al ejecutar el comando type mbr.evi se valida que el contenido no es comprensible, sin embargo, el archivo mbr.evi se puede subir a sitios como Virus total o al sitio de Symantec, Karspesky o MacAfee en donde se realizan análisis de MBR e indican si existe algún tipo de amenaza que afecte al sector de inicio maestro o MBR, por lo que es muy importante realizar una copia de este archivo y guardarlo.



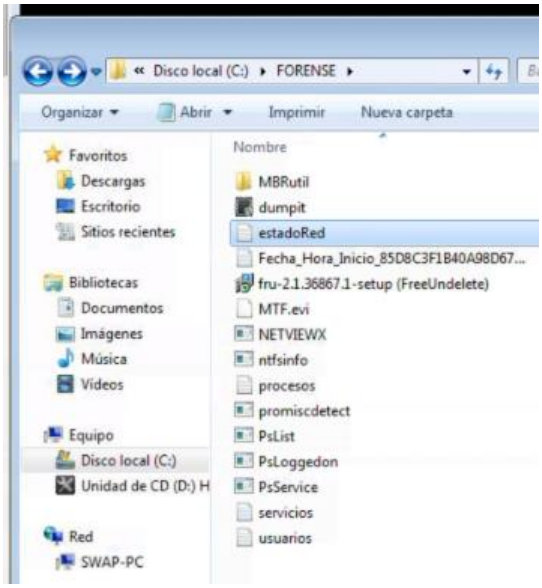
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Captura de la Tabla Maestra de Archivos MFT

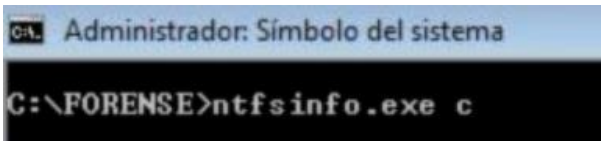
La MFT o tabla maestra de archivos almacena permisos, fechas, nombres, tamaño, etc, de todos los archivos y directorios del disco duro, incluso de los archivos eliminados siempre y cuando no hayan sido sobrescritos.

Cuando se obtiene la copia del disco duro, por ende, también se ha obtenido la MFT, sin embargo, es recomendable extraerla por separado para poder analizar ciertos ficheros.

Para el ejemplo, se utilizará la herramienta ntsinfo



Se ejecuta cmd como admin, posteriormente se ingresa la ruta en donde está ubicada la herramienta y se ejecuta el siguiente comando: ntfsinfo.exe c, c es la unidad en donde se realizará.



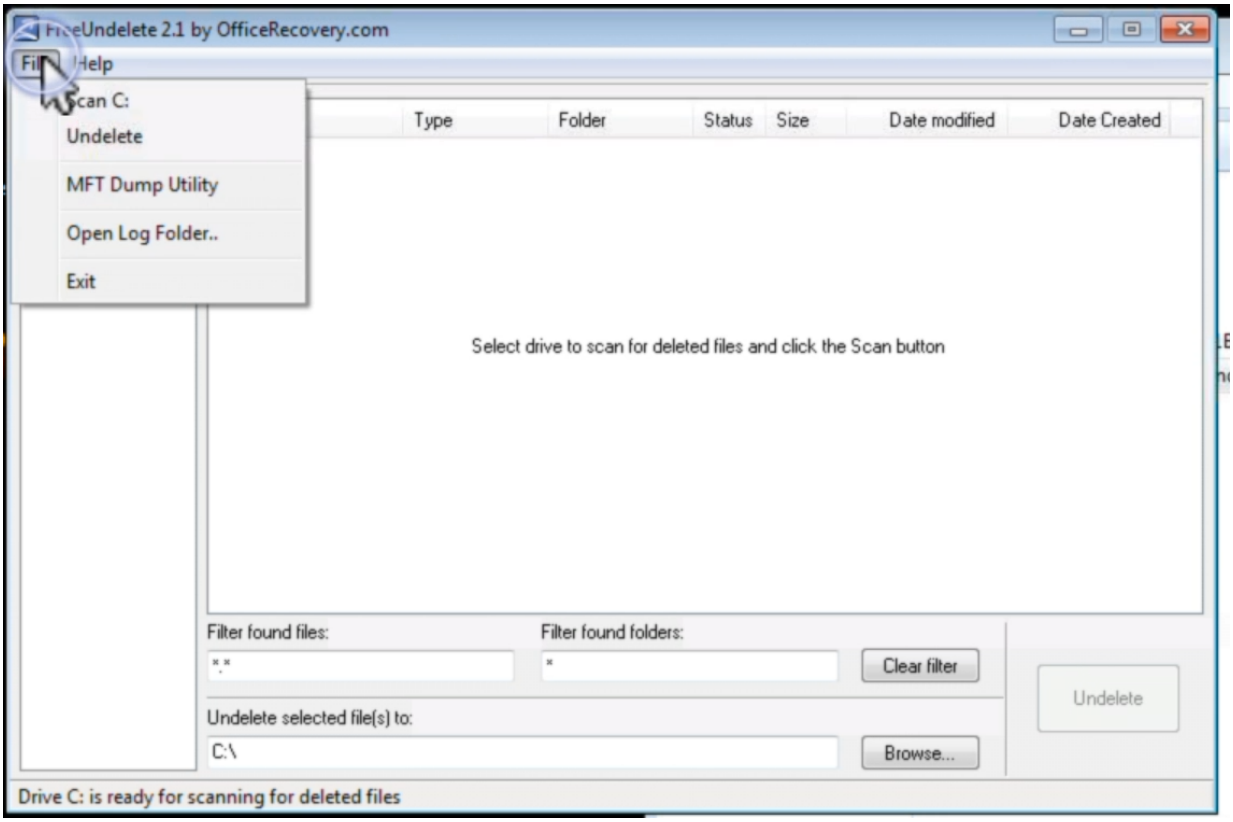
Para el ejemplo, al ejecutar el comando, se devuelve la siguiente información:

Entre la información proporcionada por el comando se puede determinar que la tabla tiene un tamaño de 23 MB, también se muestra el clúster de inicio de la tabla.

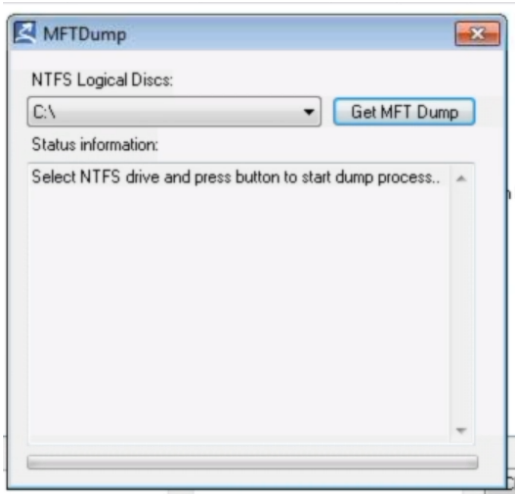
Posteriormente, debe realizarse un volcado, para el ejemplo, se utilizará la herramienta FreeUndelete.

Una vez instalada la herramienta, se ejecuta, y se va a la siguiente ruta:

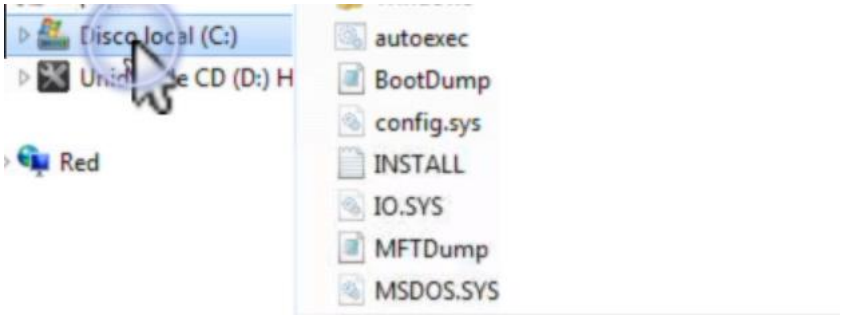
File > MFT Dump Utility.



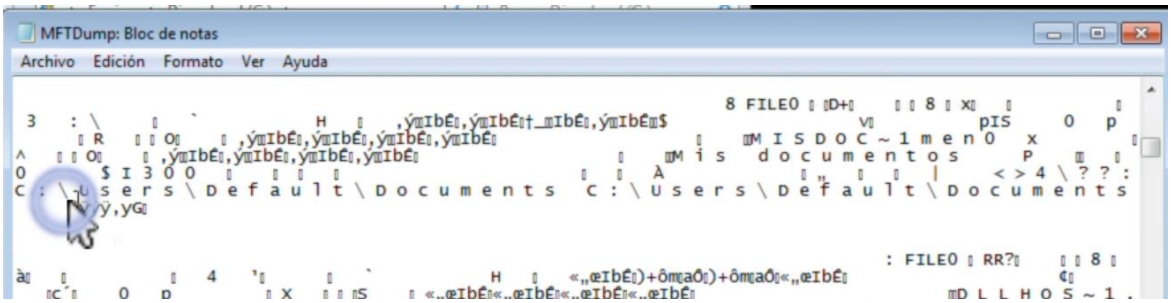
La herramienta consultará en que disco se desea realizar.



Al dar click en Get MFT Dump generara dos archivos: BootDump y MFTDump en el disco C: para el ejemplo.



Al abrir el archivo MFTDump en el bloc de notas mostrará información similar a la que se muestra a continuación:



El archivo MFTDump también podría abrirse utilizando la herramienta Disk Investigator, Notepad++, etc.

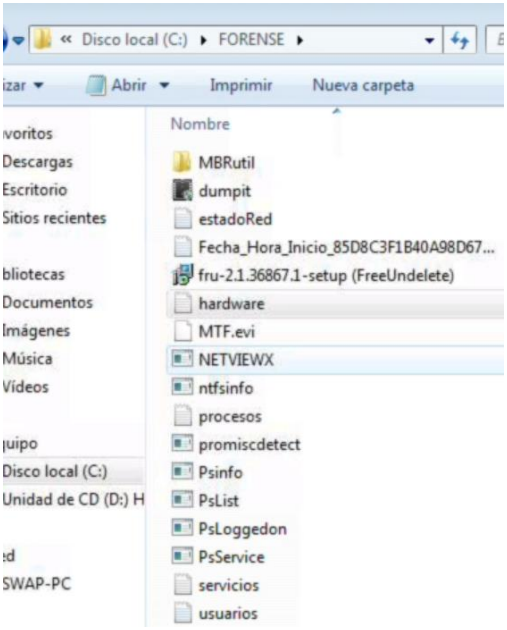
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Sección 3: Toma de evidencias no volátiles (Hardware, Logs y Ficheros del sistema)

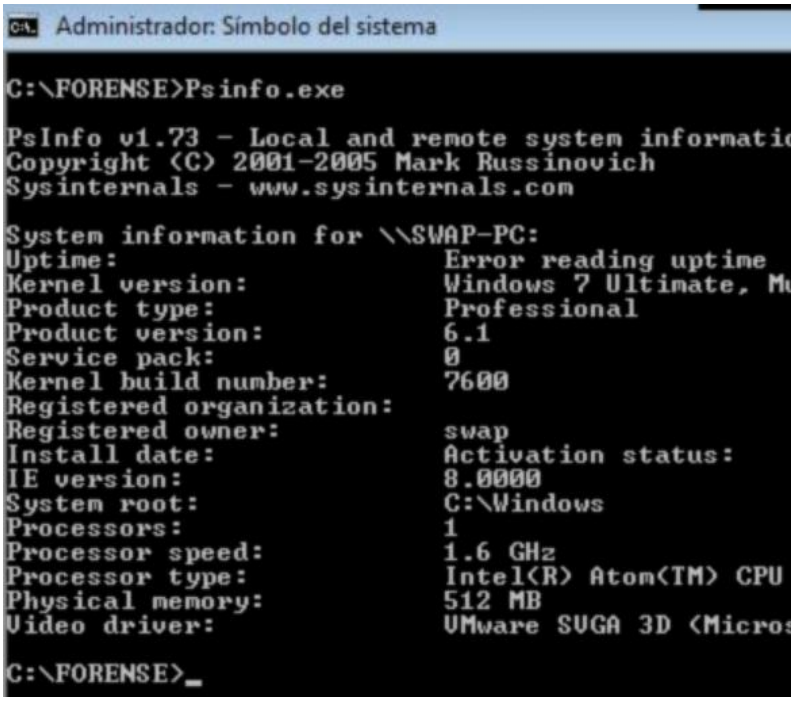
Capturar las características del Hardware

Es imperativo capturar la información del estado del hardware de la computadora comprometida, ya que contar con dicha información ayuda a determinar si el atacante pudo haber retirado o modificado algún componente de hardware.

Para el ejemplo, se utilizará la herramienta Psinfo.



Al ejecutar el comando Psinfo.exe, se muestra la siguiente información:

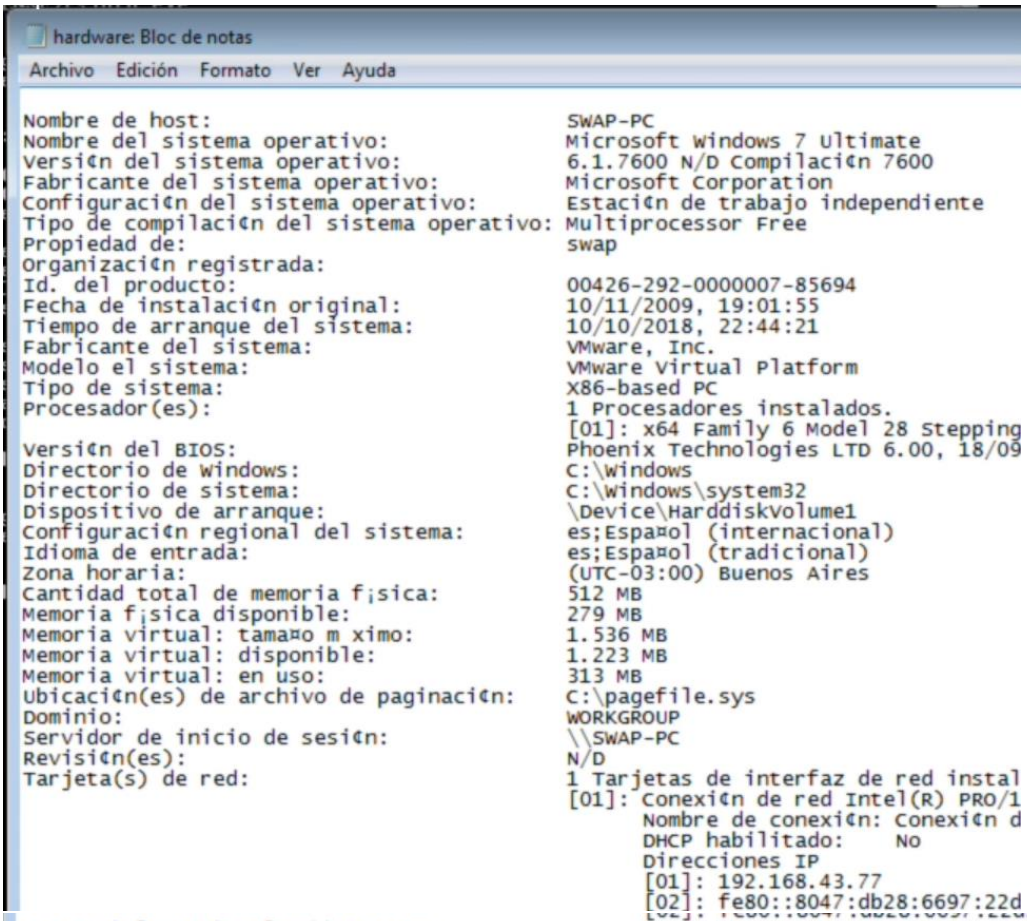


Posteriormente, se ejecuta el siguiente comando:

Al ejecutar dicho comando, la información generada por el comando systeminfo será guardada en el archivo hardware.txt.

Luego, se ejecuta el siguiente comando para añadir la información proporcionada por el comando Psinfo.exe al archivo hardware.txt.

Al abrir el archivo hardware.txt, se mostrará la información proporcionada por los comandos previamente ejecutados:

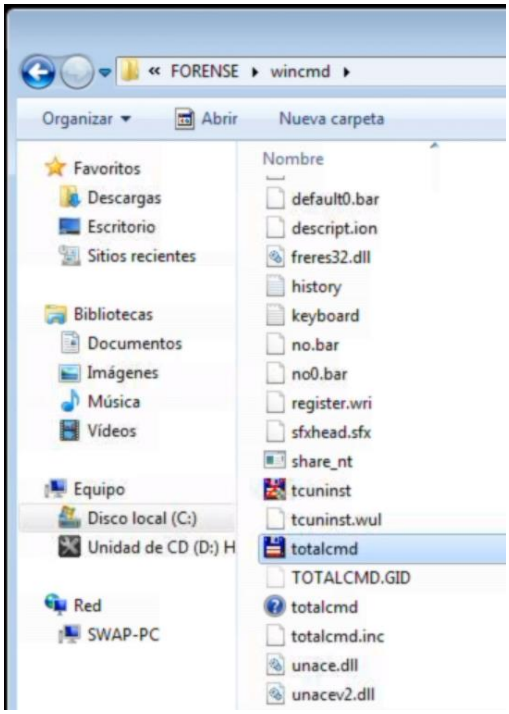


Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

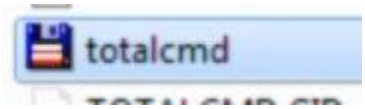
Captura de ficheros y directorios específicos con CRC

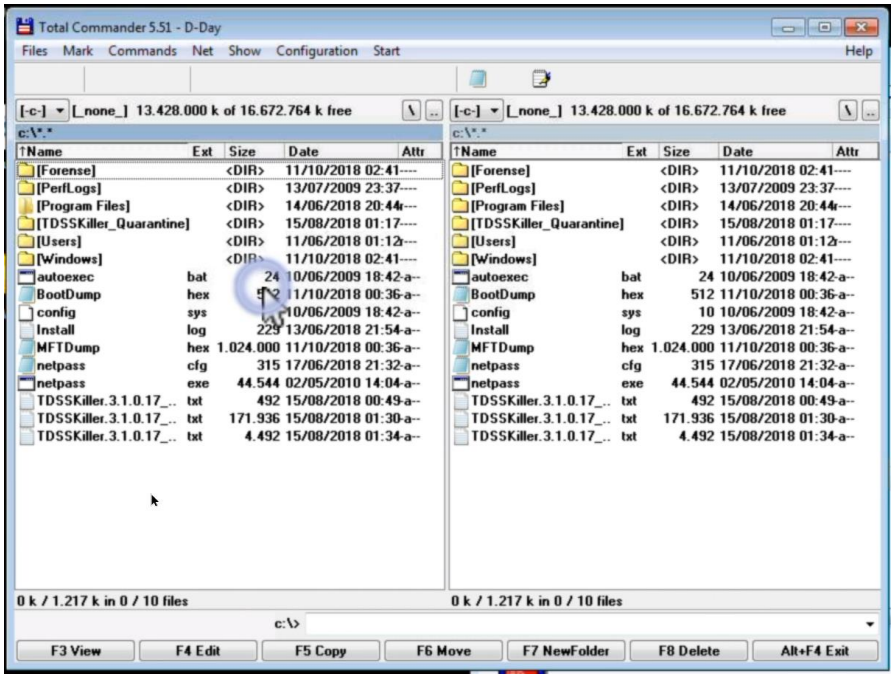
La adquisición de archivos y carpetas aisladas debe contar con un sistema de comprobación.

Para el ejemplo, se utilizará la aplicación total commander.

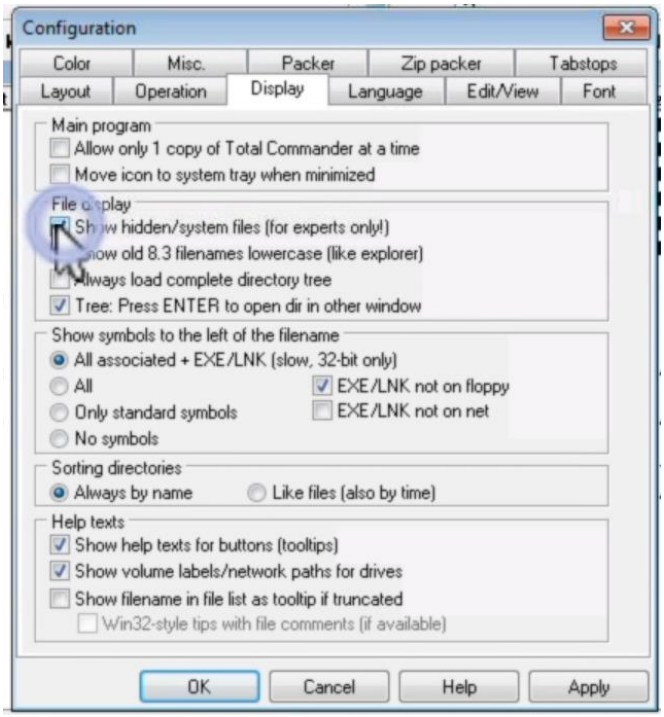


Se debe ejecutar la aplicación total commander como administrador.

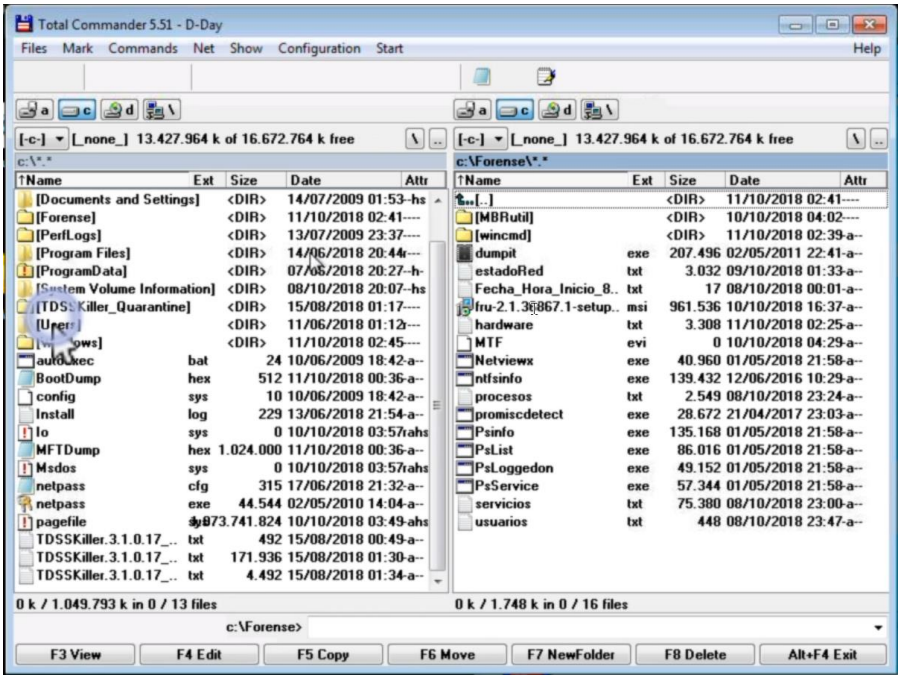




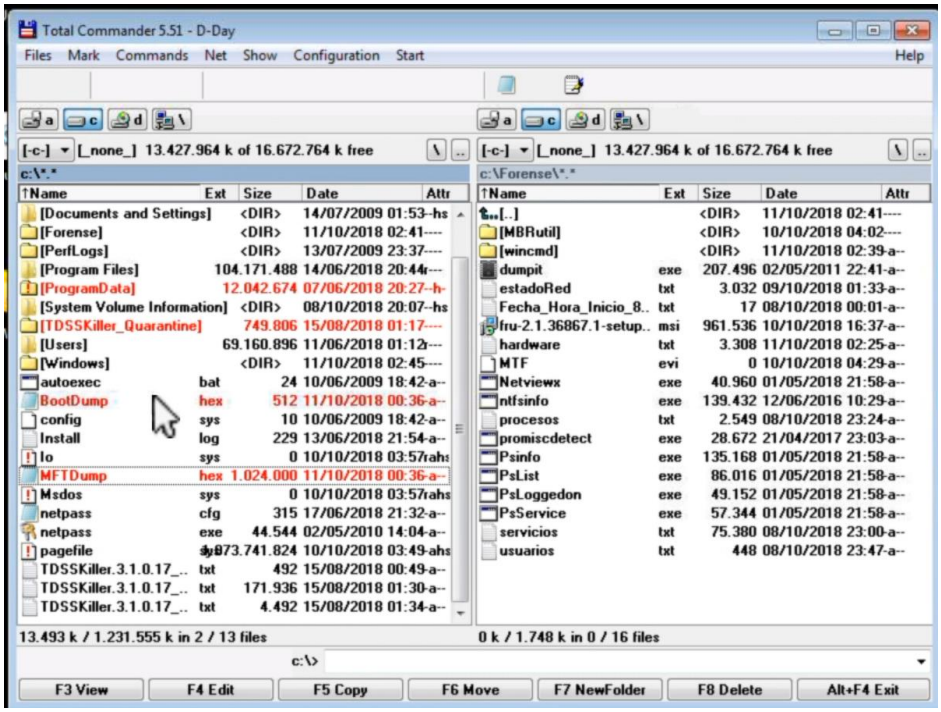
La aplicación total commander se puede configurar para que muestre los archivos ocultos del sistema al ir a Configuration > Options y marcar el cuadro Show hidden/system files tal como se muestra a continuación.



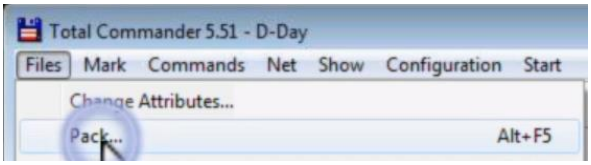
La sección izquierda muestra las carpetas a copiar, la sección derecha muestra el destino en donde se copiarían dichas carpetas.



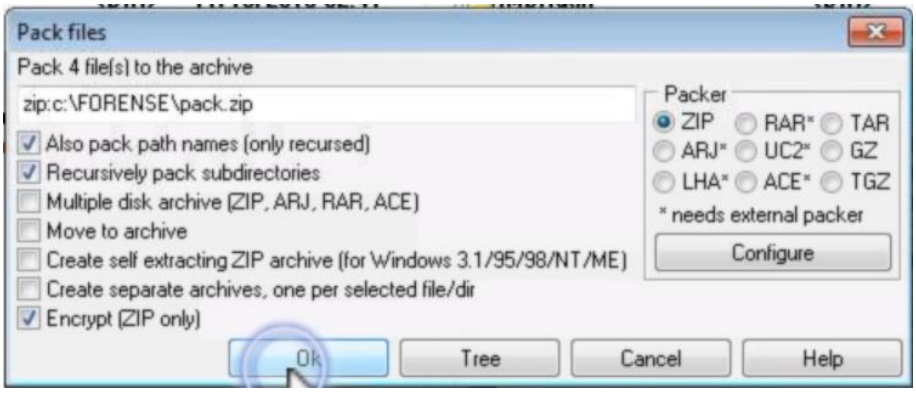
Con la barra espaciadora se pueden seleccionar las carpetas a copiar, al hacerlo, las carpetas se podrán en color rojo y mostrarán el tamaño tal como se muestra a continuación:



Para realizarlo, se debe ir a Files > Pack

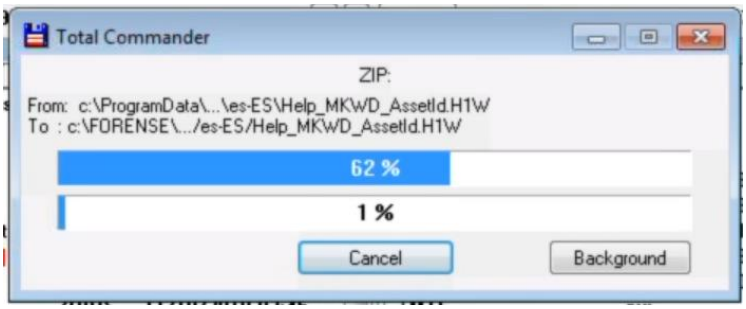


Se mostrará lo siguiente, lo cual significa que empaquetará y copiará las carpetas previamente seleccionadas en el destino mostrado en el sector derecho:

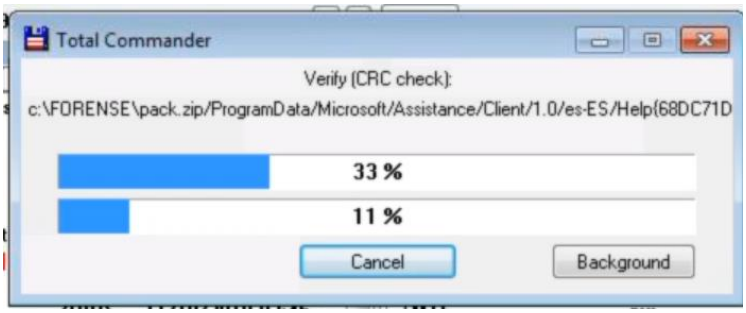


Si se selecciona la casilla Encrypt (ZIP only), pedirá que se asigne una contraseña.

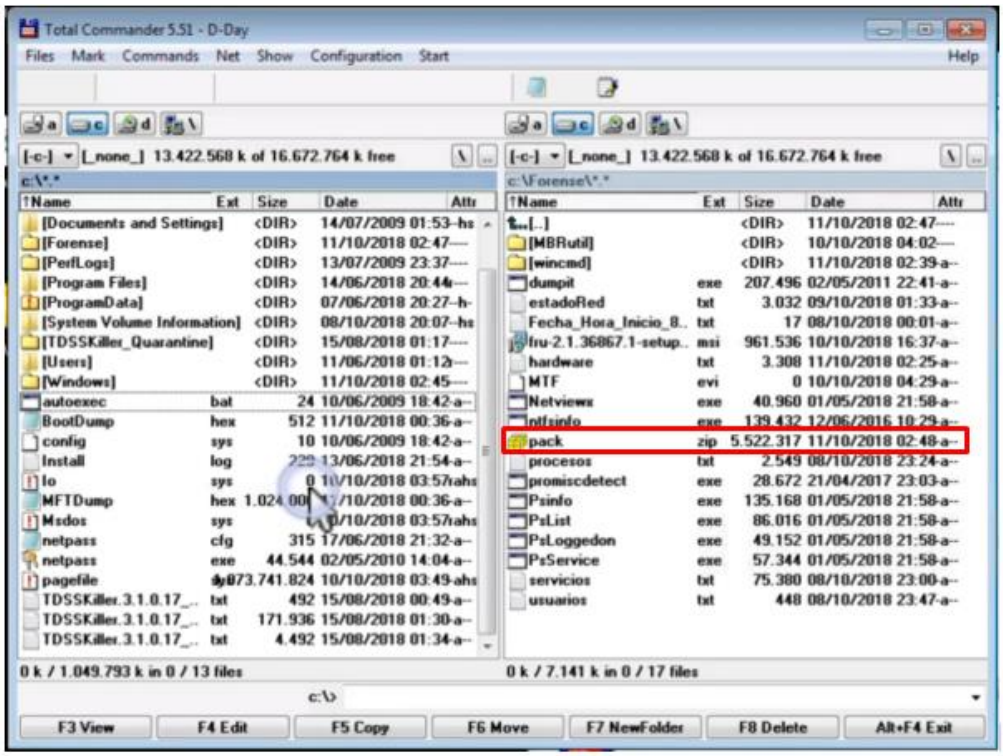
Luego pedirá que se ingrese la contraseña asignada para verificación.



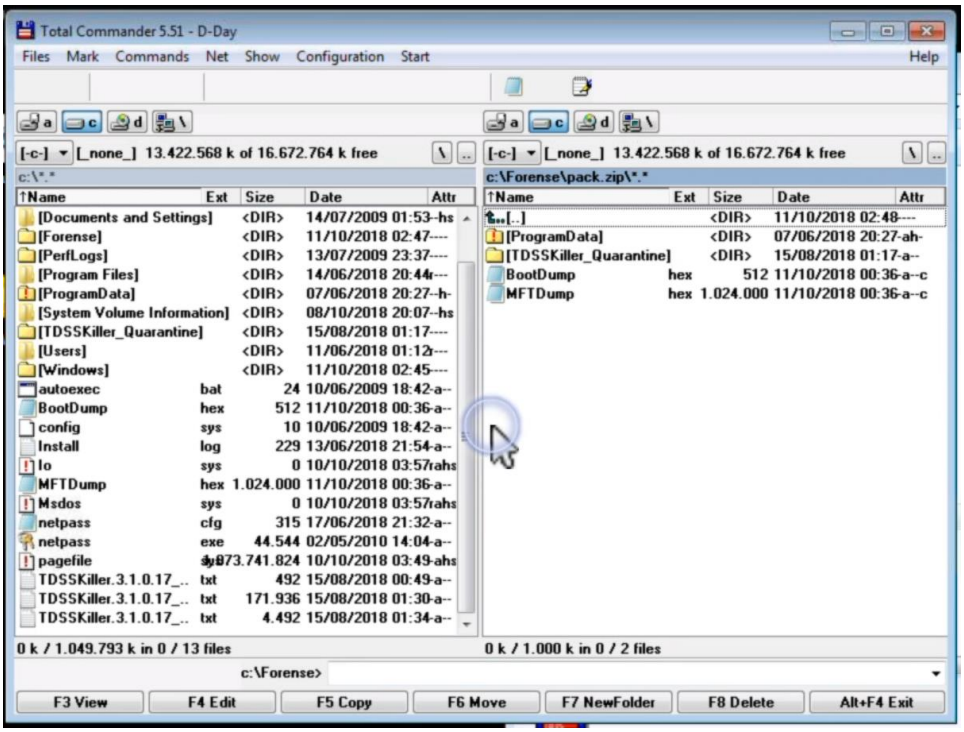
Al terminar de copiar, realizará una comprobación de CRC para cada uno de los archivos tal como se muestra a continuación.



Al finalizar, se mostrará el archivo pack del lado derecho:



Al abrir dicho archivo, se puede validar que contiene todo el árbol de carpetas y subcarpetas que fueron seleccionadas previamente.



Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

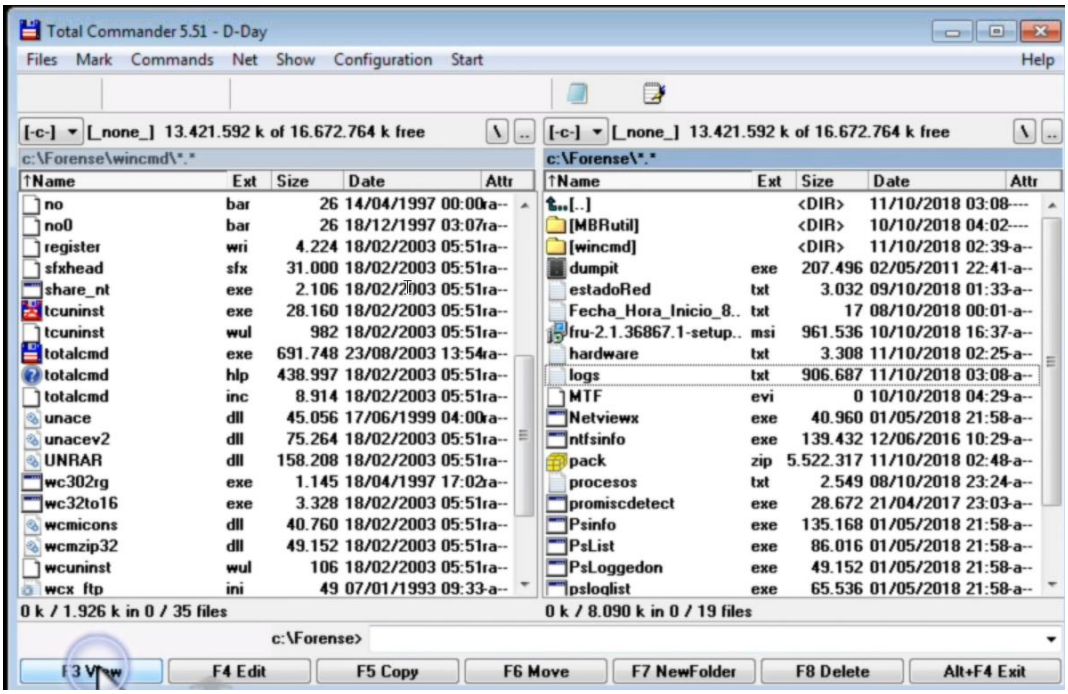
Captura de los Logs del Sistema

Los logs son archivos de texto que almacenan información relevante en un sistema informático.

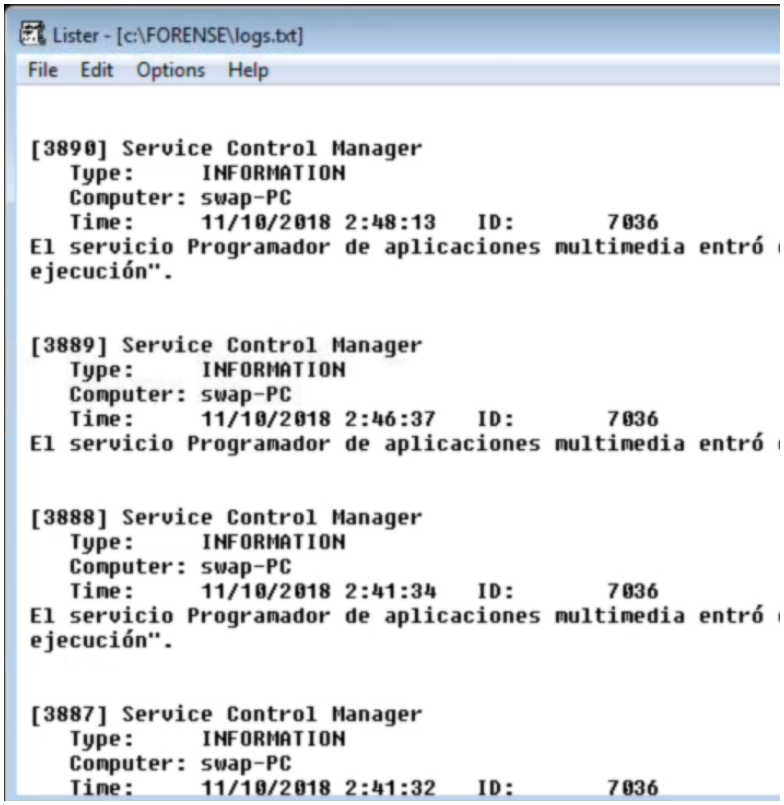
Para el ejemplo se utilizará la herramienta psloglist.exe.

Al ejecutar el siguiente comando se almacenará la información generada por la herramienta en el archivo logs.txt.

Para los ejemplos de manejo de archivos se utilizará la herramienta total commander.



Al abrir el archivo logs.txt se mostrará la siguiente información:

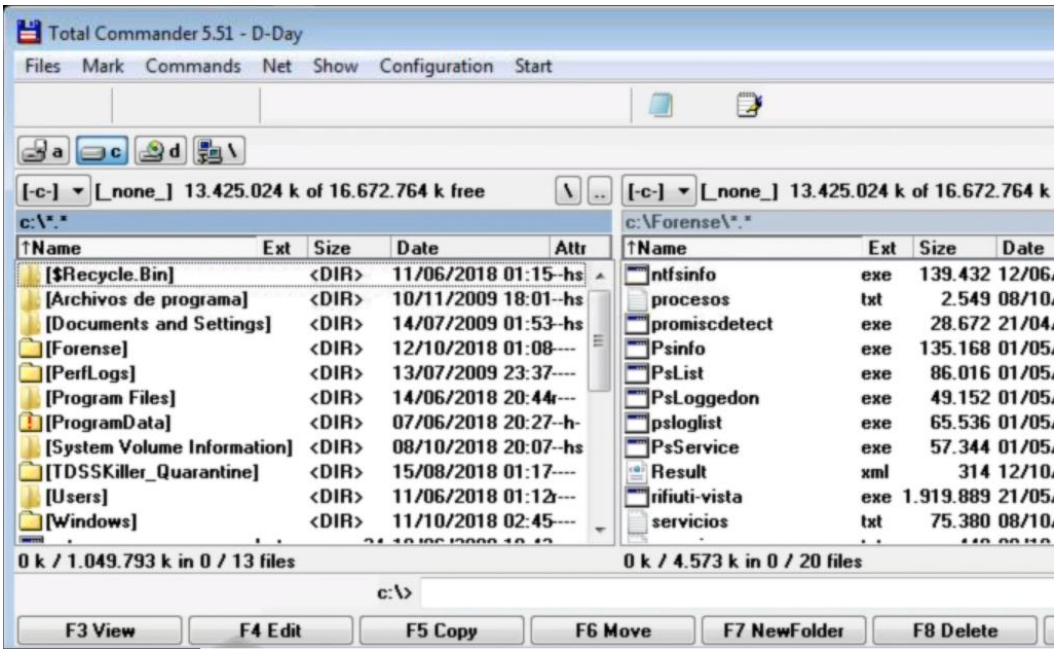


Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

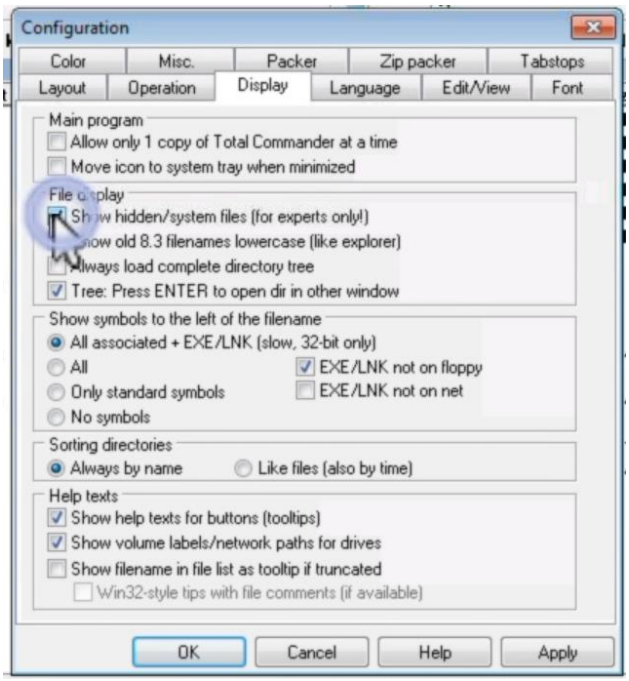
Captura de la papelera de reciclaje

Se deben obtener la lista de todos los ficheros y carpetas que hayan sido enviados a la papelera de reciclaje.

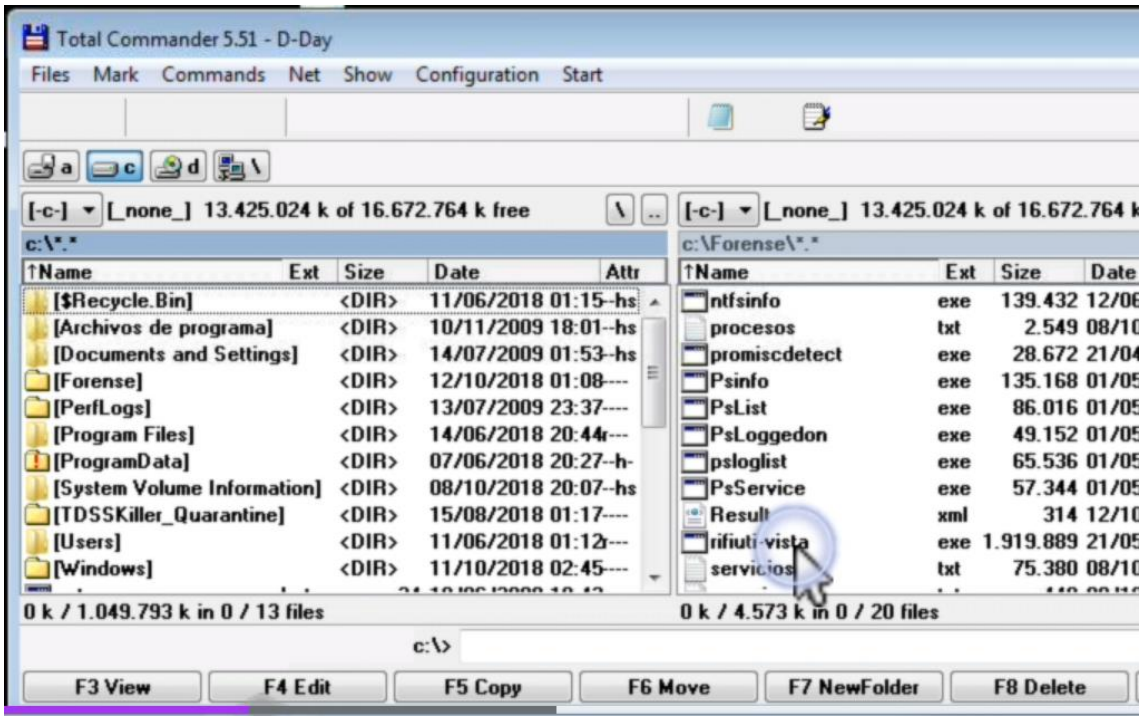
En Windows 7, 8, 10, en el disco C está ubicada la carpeta $Recycle.bin tal como se muestra en la siguiente imagen:



Es necesario recordar que la aplicación total commander fue configurada para mostrar archivos ocultos.

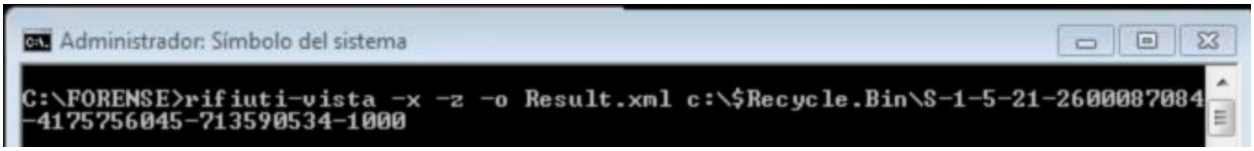


Para el ejemplo, se utilizará la herramienta rifiuti-vista, la cual se utiliza para Windows y vista y versiones posteriores.

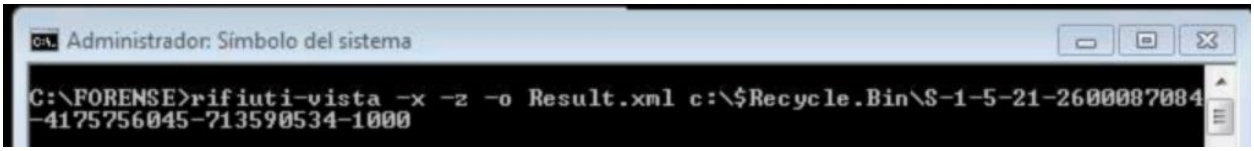


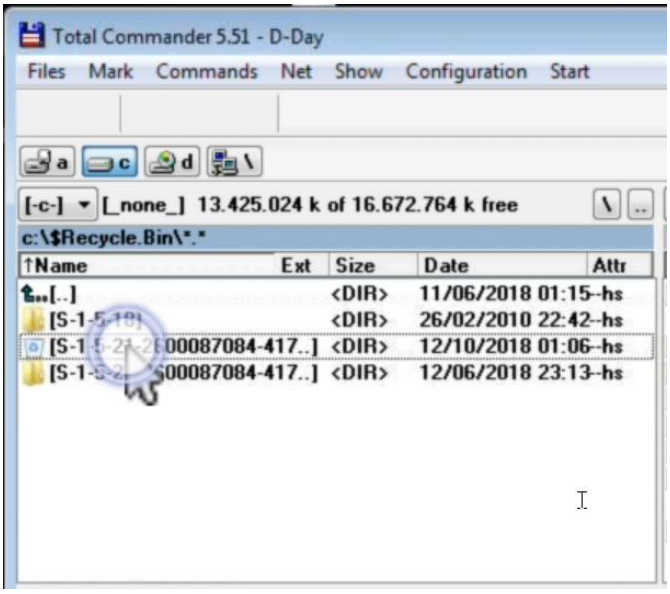
Se ejecuta cmd como admin y se coloca el siguiente comando:

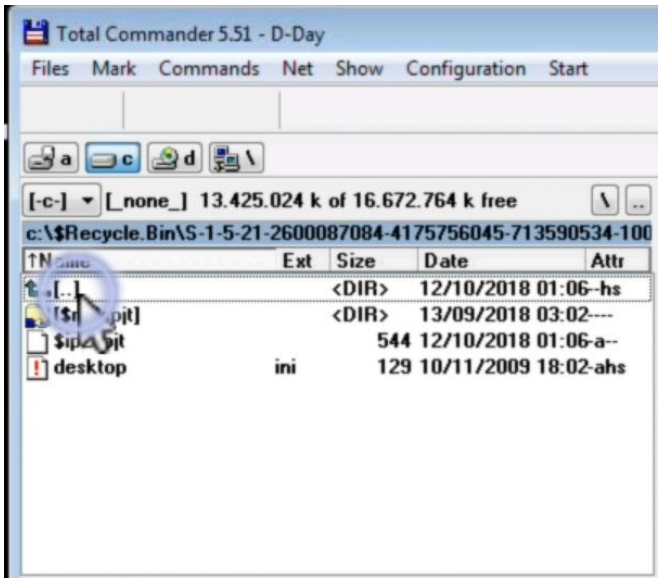
Rifiuti-vista -x -z -o Result.xml c:\$Recycle.Bin\ (ruta de la carpeta en la que se pudo accesar en este caso mediante la herramienta total commander)



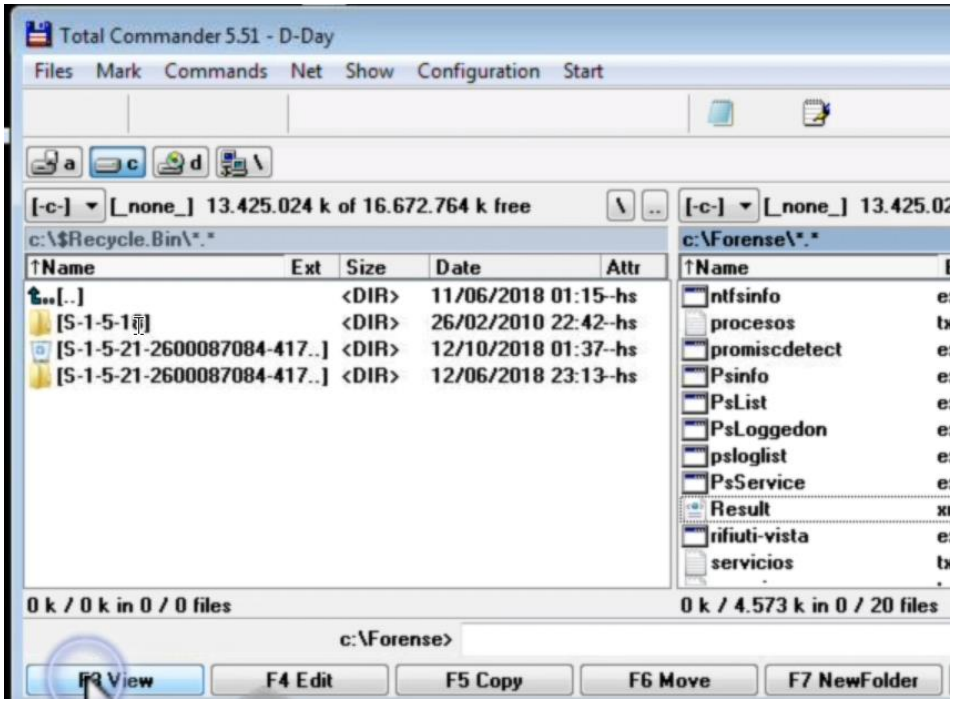
A continuación, se muestra el nombre la carpeta en la que se pudo acceder, por ende, fue la que se colocó en el cmd.







Al ejecutar el comando en el cmd, tuvo que haber generado el archivo Result.xml en la ruta C:\Forense tal como se muestra en la siguiente imagen, para validar el contenido de dicho archivo, se debe seleccionar el archivo y hacer click en F3 View en total commander.



La información del archivo indica el tamaño del archivo que se envío a la papelera, la fecha y hora en la que se borró, también indica el usuario que lo borró y la carpeta en la que el archivo se encontraba.

```
<Filename>c:\$Recycle.Bin\S-1-5-21-2600087084-4175756045-713590534-1000</Filename
>
  <record index="$IP2SPJT" time="2018-10-12T01:06:34-0300" size="6256951">
    <path>C:\Users\swap\Desktop\exiftoolgui</path>
  </record>
  <record index="$I2QUB9E.xml" time="2018-10-12T01:37:21-0300" size="314">
    <path>C:\FORENSE\Result.xml</path>
  </record>
</recyclebin>
```

Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Sección 4: Toma de evidencias no volátiles (Variables, tareas y enlaces)

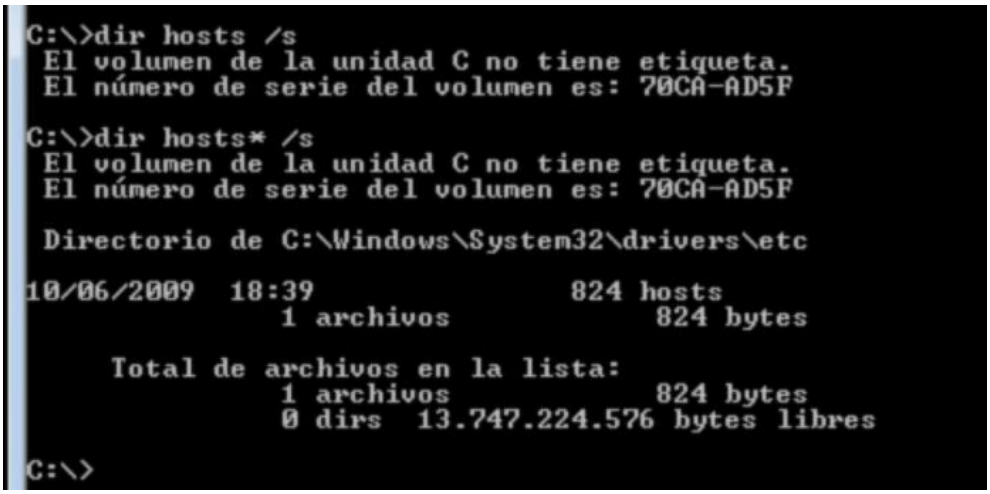
Captura del archivo de resolución local de direcciones

El archivo de resolución local de direcciones es la presa preferida de los intrusos, por lo tanto, debe ser copiado como evidencia.

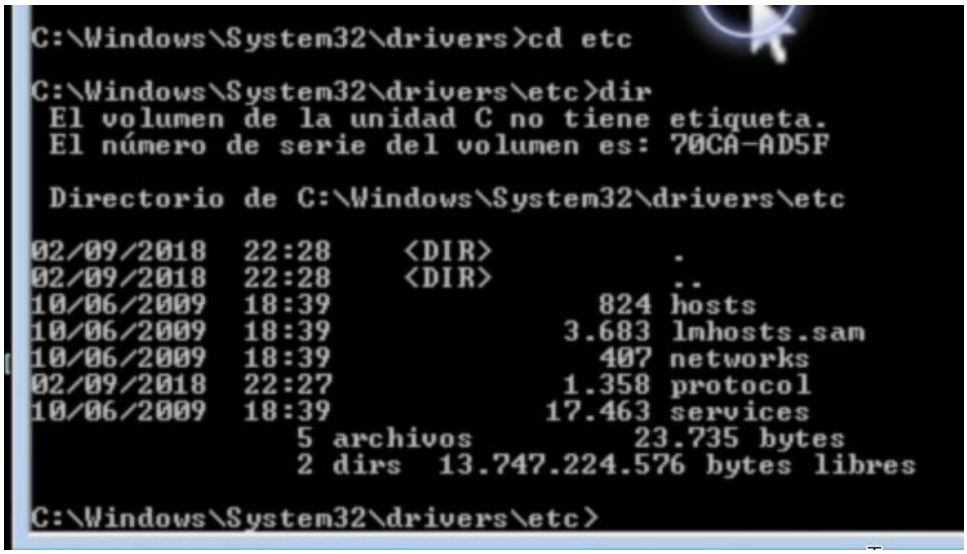
Es imperativo analizar y capturar la evidencia del archivo host, lo anterior se debe a que la mayoría de los delitos graves, tales como robo de tarjeta de crédito, fraude bancario, suplantación de identidad, etc, hacen uso y modificación del archivo host.

Para el ejemplo, se ejecuta el cmd como admin, luego se ejecuta el siguiente comando:

Dir hosts /s o dir hosts* /s



Al ingresar a la ruta indicada C:\Windows\System32\drivers\etc y al ejecutar el comando dir, se determina que el archivo hosts se encuentra allí.



Para copiar el archivo, se ejecuta el siguiente comando: copy host C:\Forense

Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Captura de las variables de entorno

Es necesario tomar una muestra de las variables de entorno de la máquina comprometida.

Las variables del entorno son un artificio que le dice al sistema operativo cuales son las carpetas del sistema, por lo tanto, cualquier aplicación que se encuentre dentro de esas carpetas va a ser ejecutada directamente sin necesidad de escribir toda la ruta, las variables de entorno fuera del estándar son indicios de manipulación.

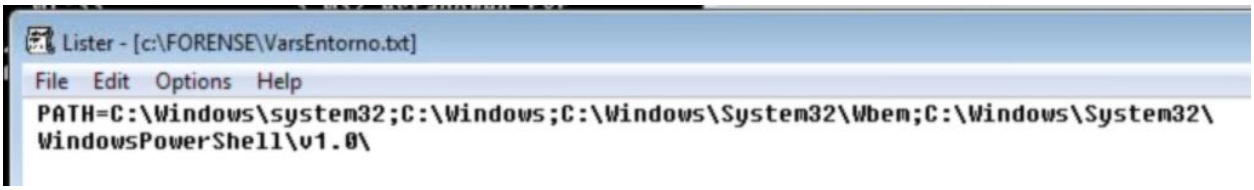
Al ejecutar cmd como admin y ejecutar el comando path, se mostrarán todas las variables de entorno

```
C:\FORENSE>path
PATH=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32
\WindowsPowerShell\v1.0\
```

Para capturar las variables de entorno en un archivo de texto, se ejecuta el siguiente comando:

```
C:\FORENSE>path > VarsEntorno.txt
```

Al abrirlo se muestra lo siguiente:

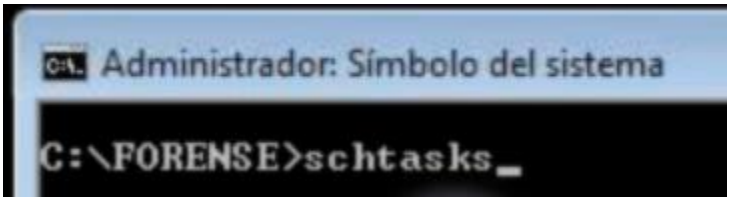


Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Captura de las tareas programadas

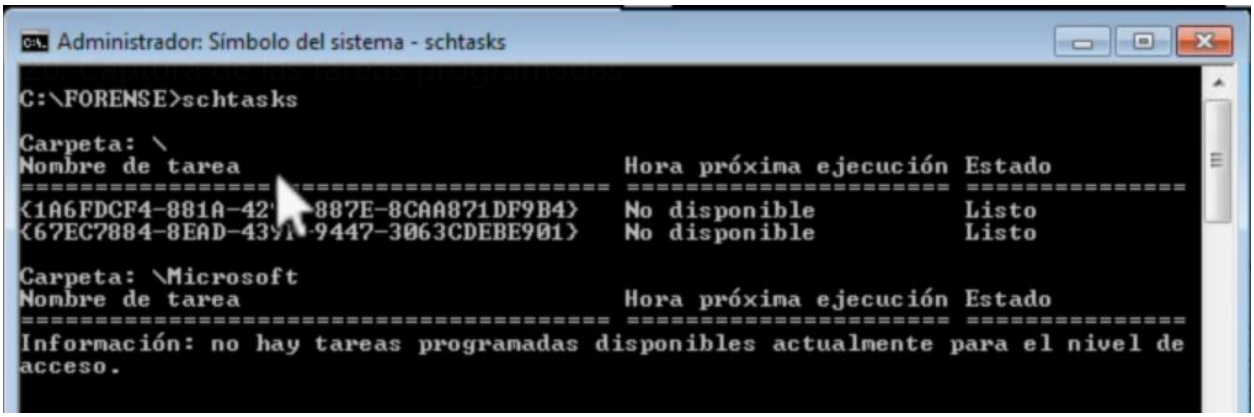
Las tareas programadas pueden ser utilizadas para ejecutar procesos no deseados en el sistema comprometido.

Para validar las tareas programadas, se ejecuta el siguiente comando.



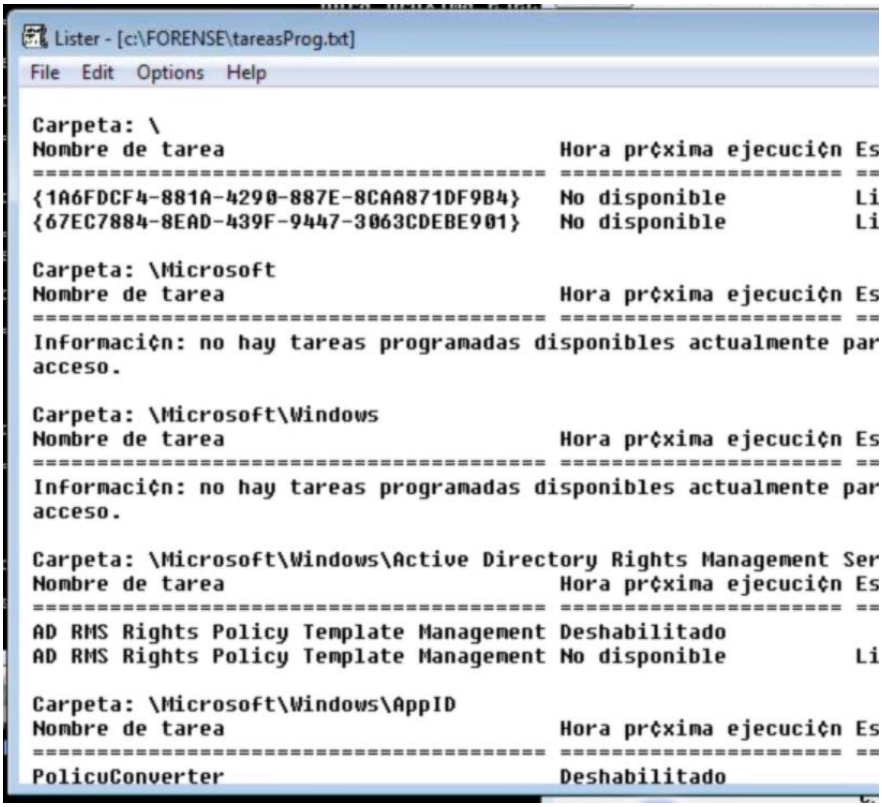
El comando anterior forma parte del sistema operativo, pero se puede aislar el binario y tenerlo en un pendrive forense para ejecutarse en la máquina comprometida.

Al ejecutar el comando empezará a listar todas las tareas programadas.



Para capturar las tareas programadas en un archivo de texto, se ejecuta el siguiente comando:

Al abrirlo se muestra lo siguiente:



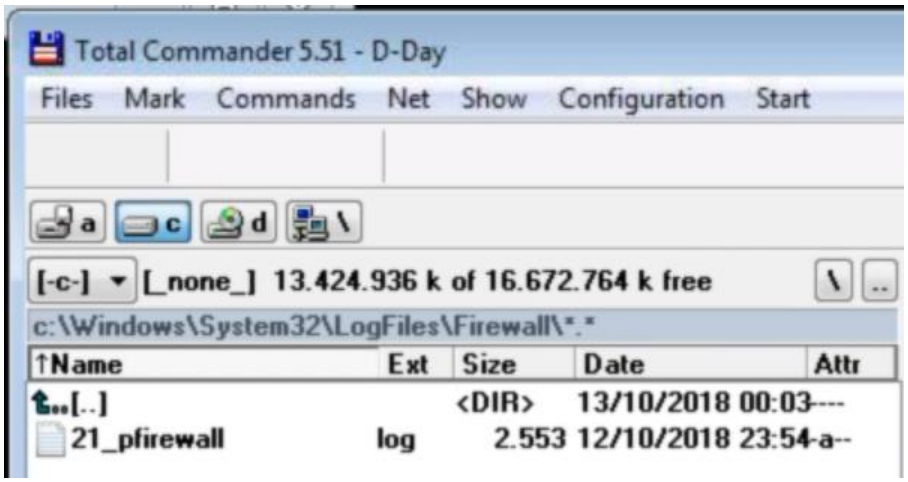
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Captura de la actividad del Firewall

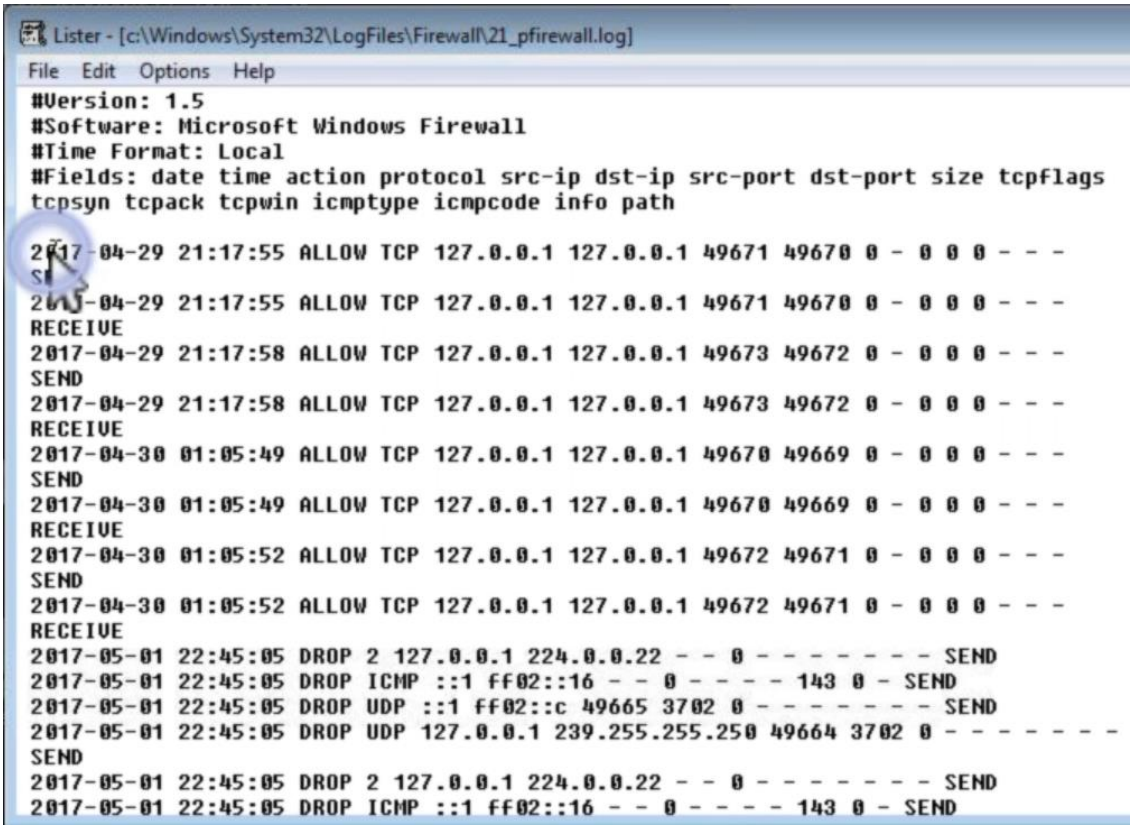
Se debe auditar las conexiones y paquetes del firewall.

Para tal propósito, es necesario ir a la ruta C:\Windows\System32\LogFiles\Firewall\, en dicha ruta se encuentra ubicado el archivo pfirewall.log.

Para el ejemplo, se utilizará la herramienta total commander:



Al abrir dicho archivo, se muestra la siguiente información:



Para capturar el archivo pfirewall.log mediante total commander, se debe realizar el proceso descrito en la sección 3.2

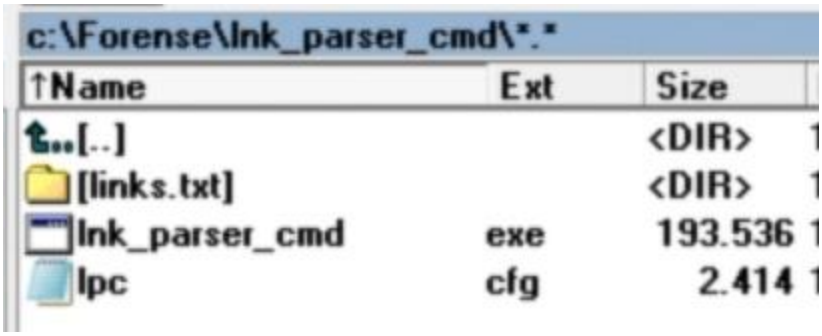
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Captura de archivos lnk

Los archivos con extensión .lnk o link son muy utilizados para acortar la ubicación ya sea de archivos o de carpetas, sin embargo, tienen funcionalidades extra que permiten a ciertos rootkit y malware realizar escalación de privilegios en el sistema.

Para realizar para realizar parsing en todo el disco y buscar los archivos .lnk y extraer la información se utilizará la herramienta lnk_parser_cmd.

El paquete lnk_parser_cmd cuenta con un archivo de configuración y la herramienta.



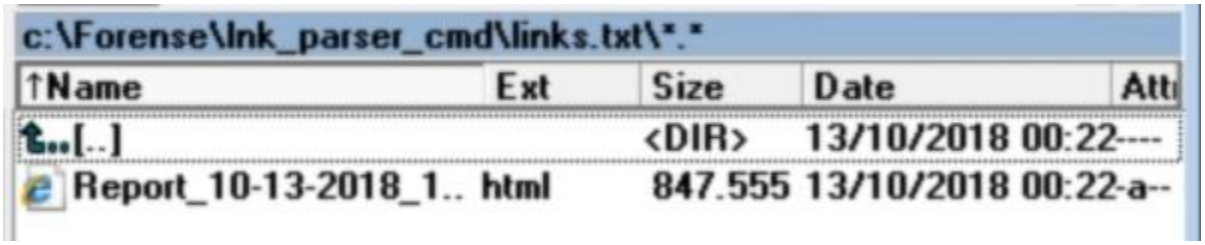
Para ejecutarla, es necesario ejecutar el cmd como administrador, posteriormente, es necesario colocarse en la carpeta de la herramienta y ejecutar el siguiente comando:

Lnk_parser_cmd.exe -o links.txt -w -s c:

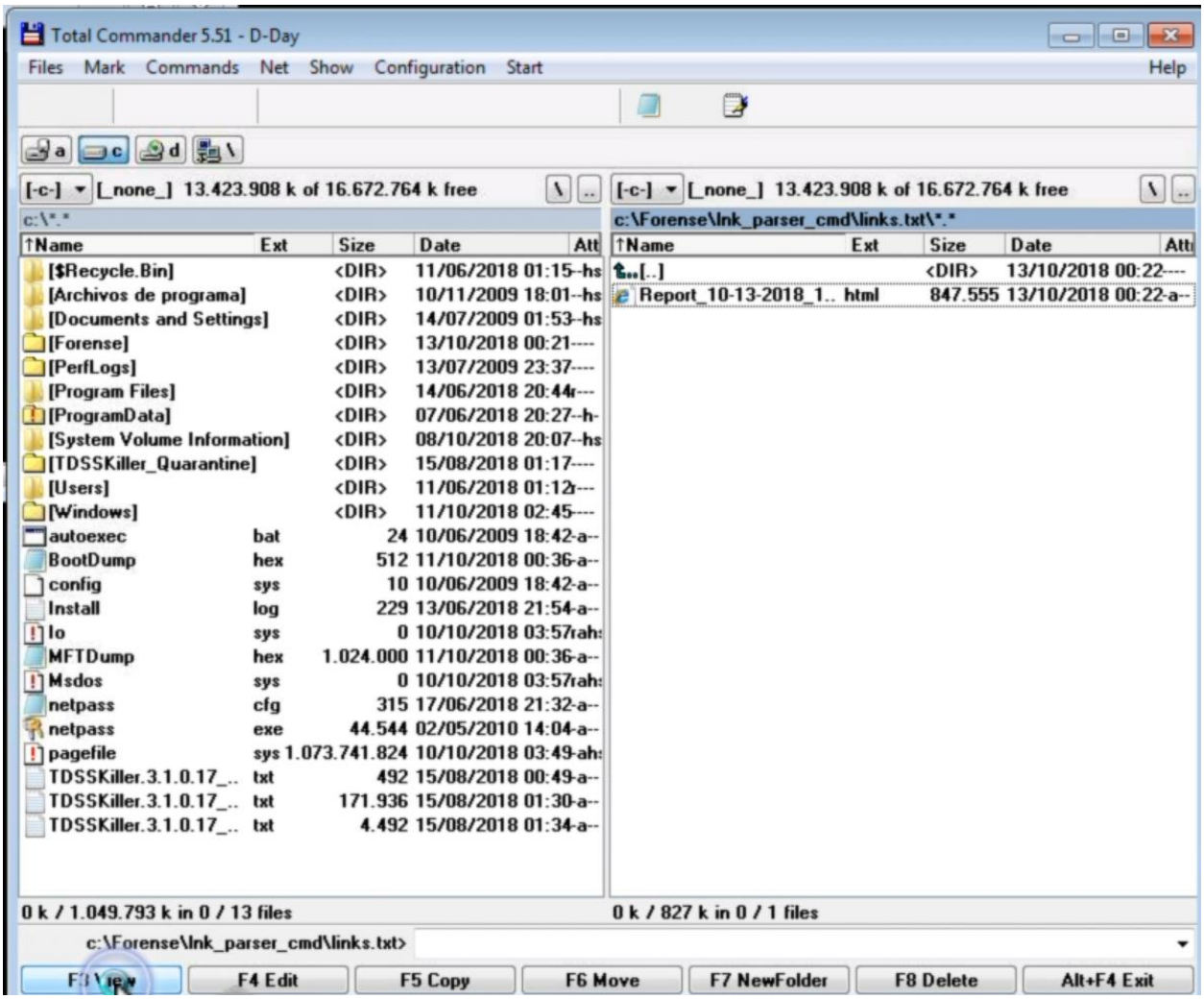
El comando significa que se ejecutará una búsqueda en el disco C:, que sea silencioso -s, -w indica que el informe que genere lo presente en html y el output -o que lo coloque en el archivo links.txt.

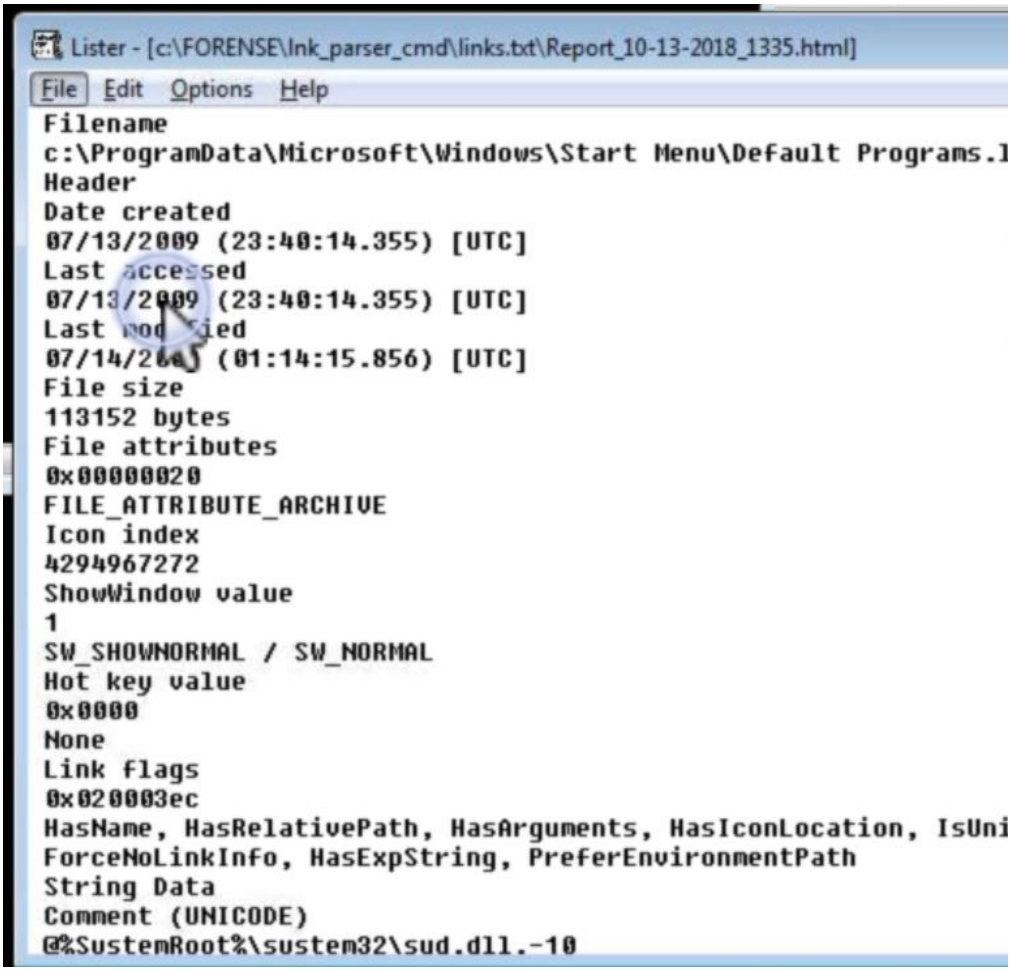
Al ejecutar el comando, se generará esta carpeta:

Al ingresar a dicha carpeta, se mostrará lo siguiente:



Al abrir el archivo, total commander automáticamente lo mostrará en el formato que corresponde, en este caso HTML.





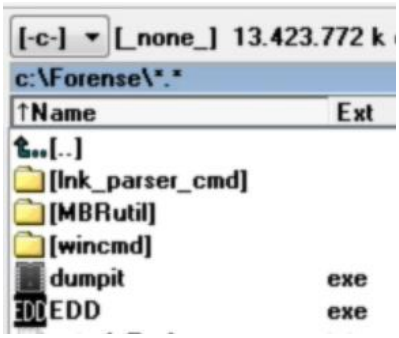
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Mapeo de Unidades encriptadas

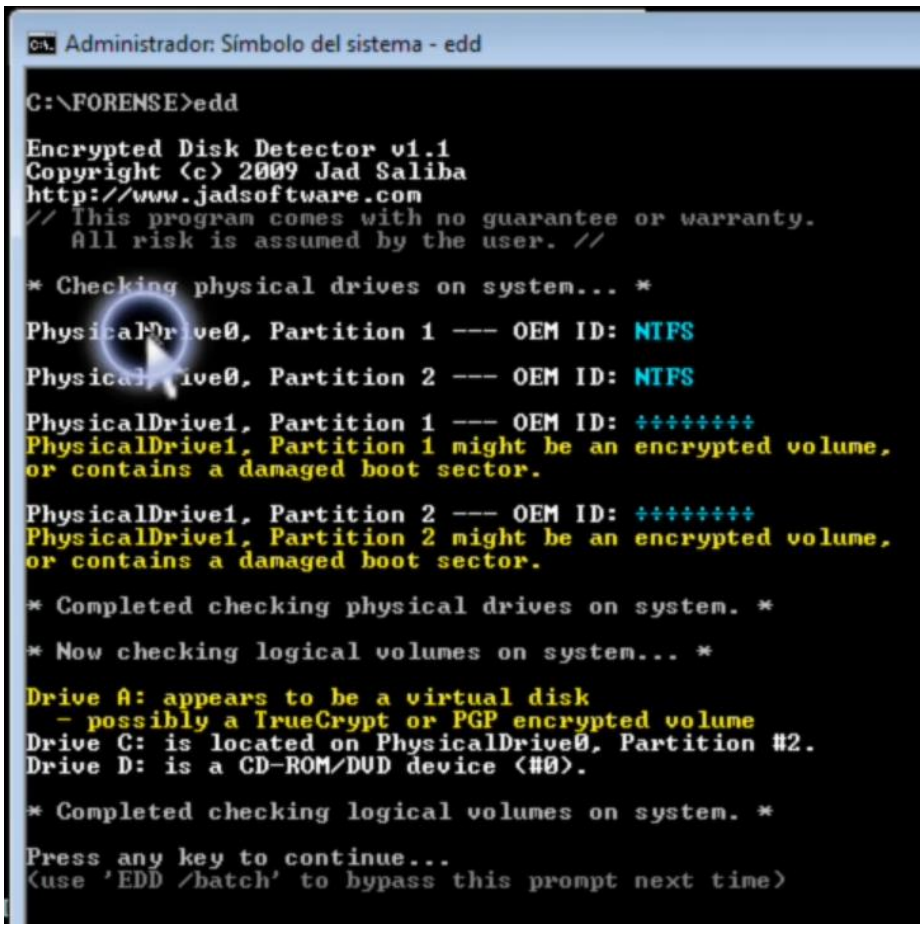
Un volumen encriptado o cifrado, puede ser un archivo que represente una partición o puede ser una partición completa que esté cifrada, lo anterior significa que, aunque tenga un sistema de archivos estándar por ejemplo NTFS de estar cifrado no se podría ver.

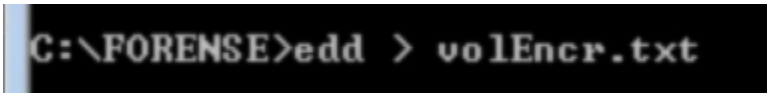
Es necesario detectar la presencia de unidades cifradas (bitlocker, PGP, safeboot, truecrypt,etc)

Para la detección de volúmenes cifrados o encriptados, se utilizará la herramienta EDD.



Para ejecutar la herramienta, se ejecuta el siguiente comando en el cmd: edd





Se realiza lo siguiente en dado caso el pendrive utilizado esté protegido contra escritura que en este caso es el C: por lo cual se guarda en un pendrive que no cuente con protección contra escritura que para el ejemplo sería el J:

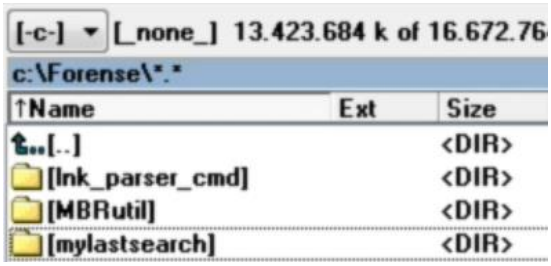
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Sección 5: Toma de evidencias no volátiles (Historiales, portapapeles y estructura MAC)

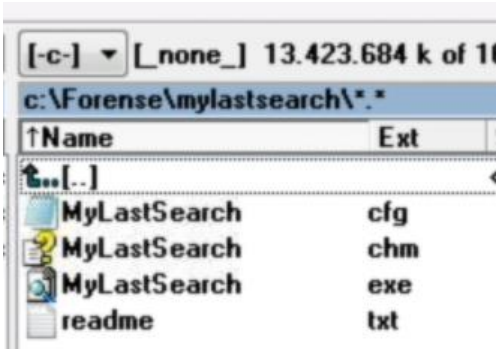
Capturar el historial de búsquedas

Se debe de capturar las búsquedas realizadas en los navegadore web y/o redes sociales para averiguar las fechas y sitios utilizados en las consultas.

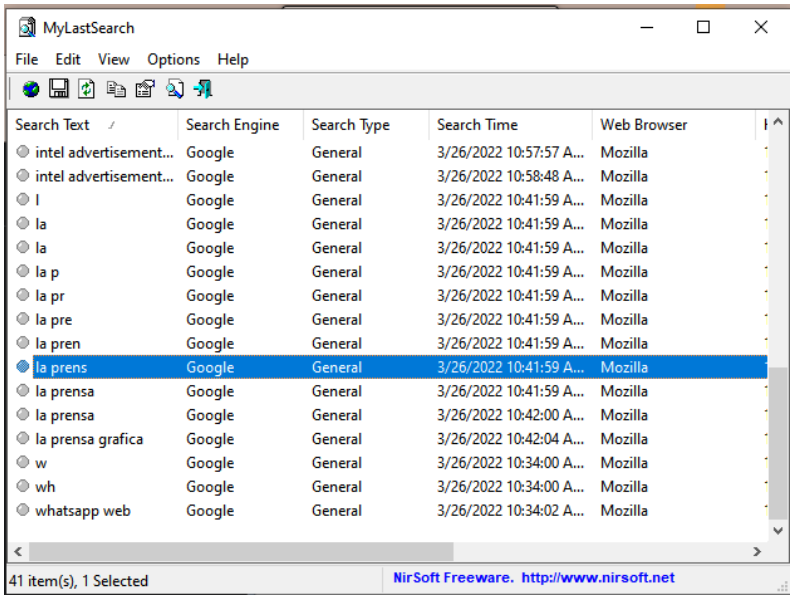
Para el ejemplo, se utilizará la herramienta mylastsearch.



Se ejecuta el archivo MyLastSearch.exe



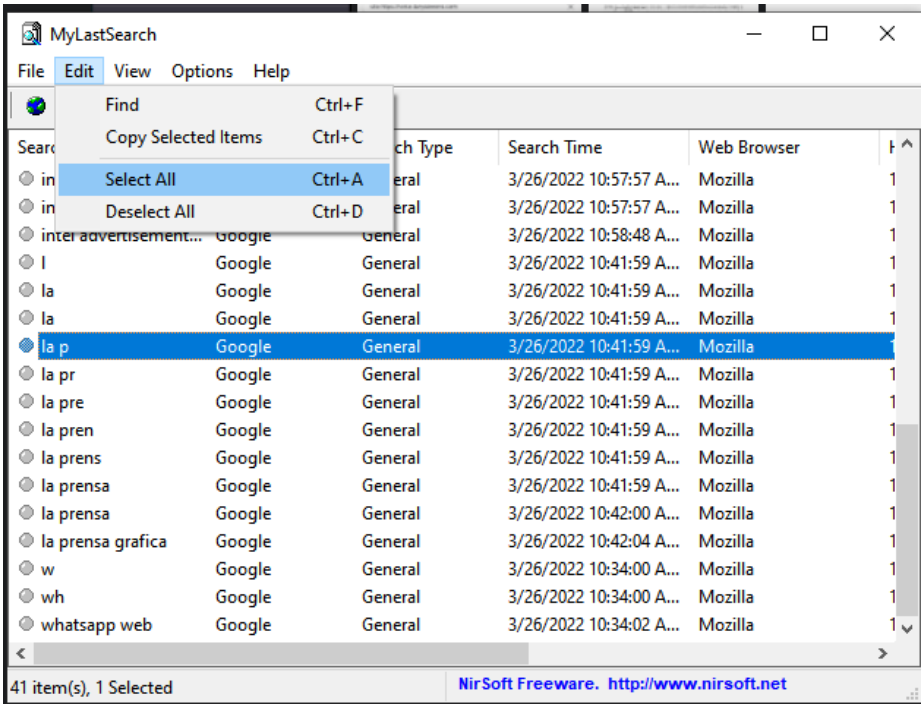
Al abrir la herramienta, inmediatamente realiza un escaneo.



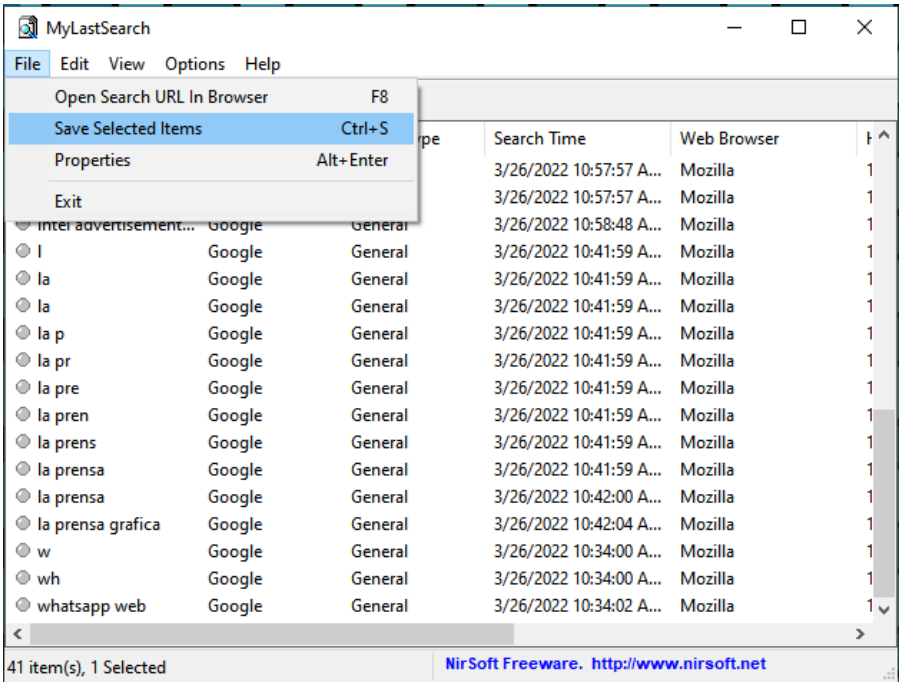
Nirsoft Freeware es excelente para aplicaciones de investigación forense.

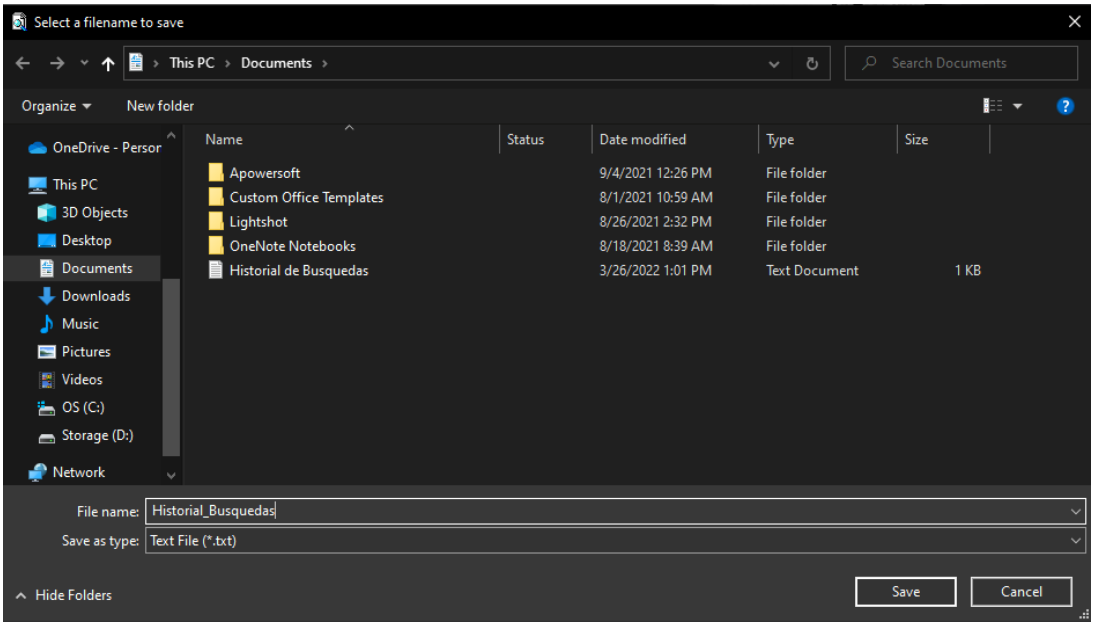
Para guardar la información proporcionada por la herramienta, se realiza lo siguiente:

Edit > Select All



File > Save Selected Items





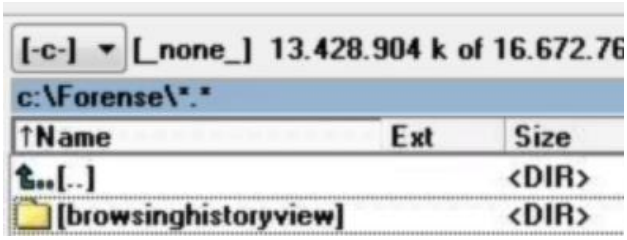
Al abrir el archivo .txt se muestra la siguiente información.

Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

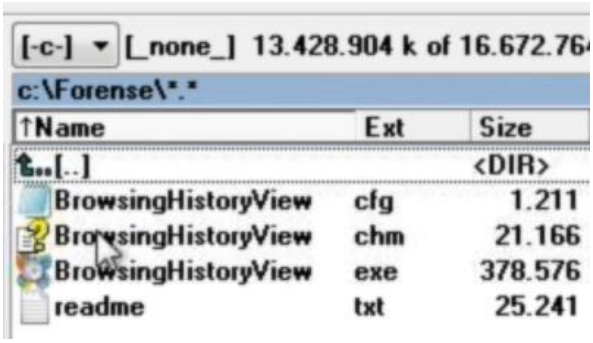
Capturar historial de navegación

El historial de navegación resulta útil para analizar infección por virus y troyanos.

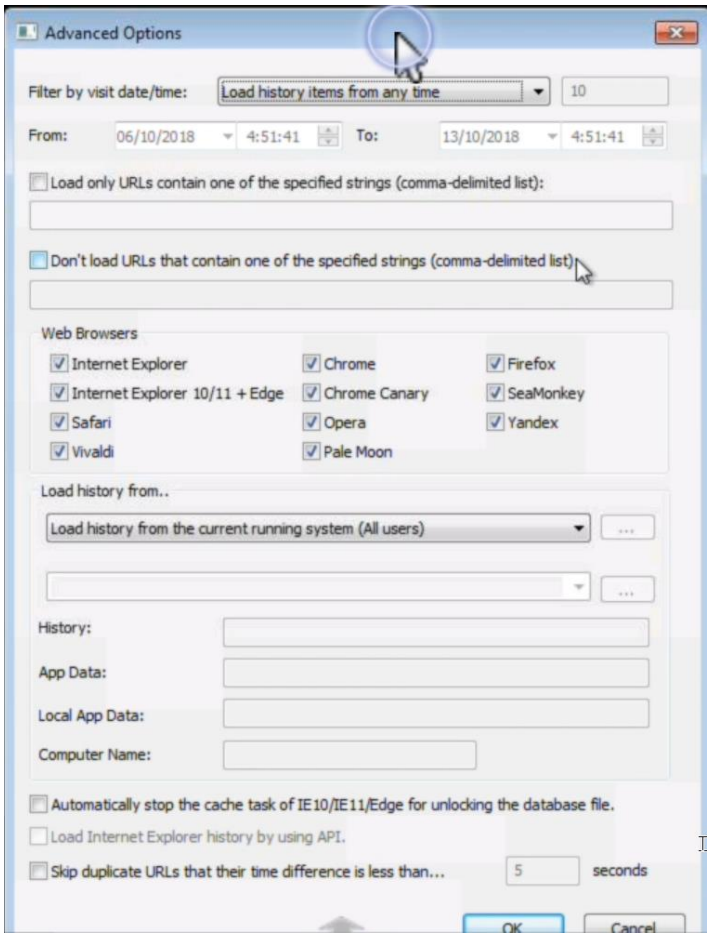
Para el ejemplo, se utilizará la herramienta BrowsingHistoryView.



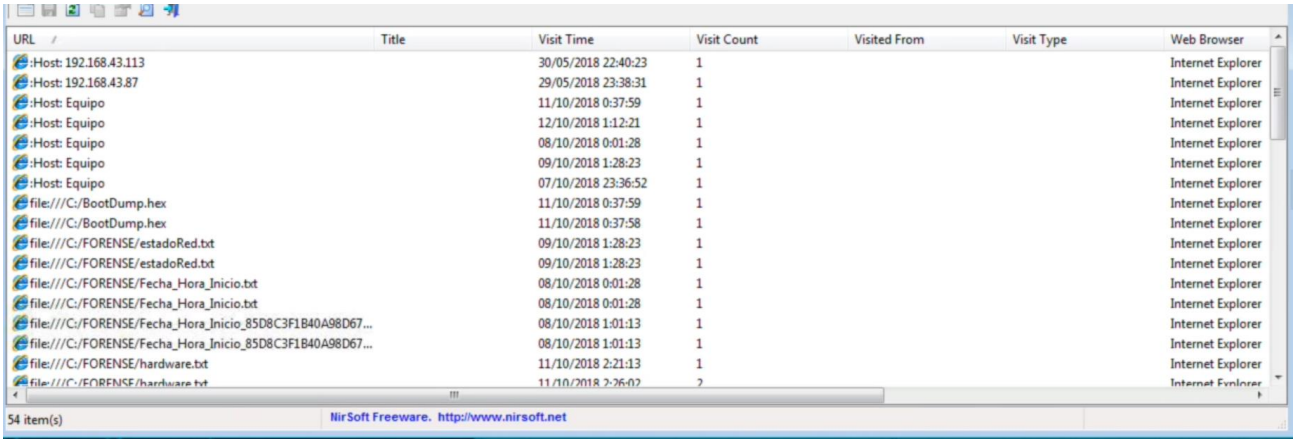
Se debe ejecutar el archivo .exe como administrador.



Al ingresar a la herramienta, lo primero que se muestra son los diferentes filtros con los cuales se puede realizar una configuración custom, para el ejemplo se da click en OK.



Al hacerlo, se muestra lo siguiente:

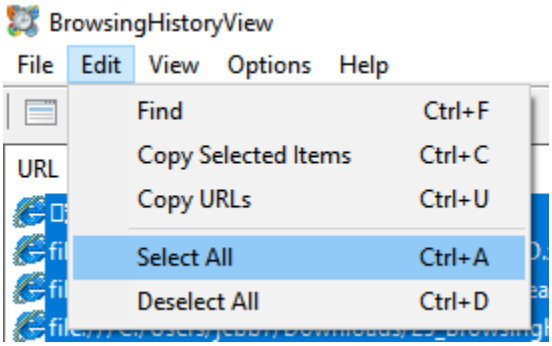


URL	Title	Visit Time	Visit Count	Visited From	Visit Type	Web Browser
:Host: 192.168.43.113		30/05/2018 22:40:23	1			Internet Explorer
:Host: 192.168.43.87		29/05/2018 23:38:31	1			Internet Explorer
:Host: Equipo		11/10/2018 0:37:59	1			Internet Explorer
:Host: Equipo		12/10/2018 1:12:21	1			Internet Explorer
:Host: Equipo		08/10/2018 0:01:28	1			Internet Explorer
:Host: Equipo		09/10/2018 1:28:23	1			Internet Explorer
:Host: Equipo		07/10/2018 23:36:52	1			Internet Explorer
file:///C:/BootDump.hex		11/10/2018 0:37:59	1			Internet Explorer
file:///C:/BootDump.hex		11/10/2018 0:37:58	1			Internet Explorer
file:///C:/FORENSE/estadoRed.txt		09/10/2018 1:28:23	1			Internet Explorer
file:///C:/FORENSE/estadoRed.txt		09/10/2018 1:28:23	1			Internet Explorer
file:///C:/FORENSE/Fecha_Hora_Inicio.txt		08/10/2018 0:01:28	1			Internet Explorer
file:///C:/FORENSE/Fecha_Hora_Inicio.txt		08/10/2018 0:01:28	1			Internet Explorer
file:///C:/FORENSE/Fecha_Hora_Inicio_85D8C3F1B40A98D67...		08/10/2018 1:01:13	1			Internet Explorer
file:///C:/FORENSE/Fecha_Hora_Inicio_85D8C3F1B40A98D67...		08/10/2018 1:01:13	1			Internet Explorer
file:///C:/FORENSE/hardware.txt		11/10/2018 2:21:13	1			Internet Explorer
file:///C:/FORENSE/hardware.txt		11/10/2018 2:26:02	2			Internet Explorer

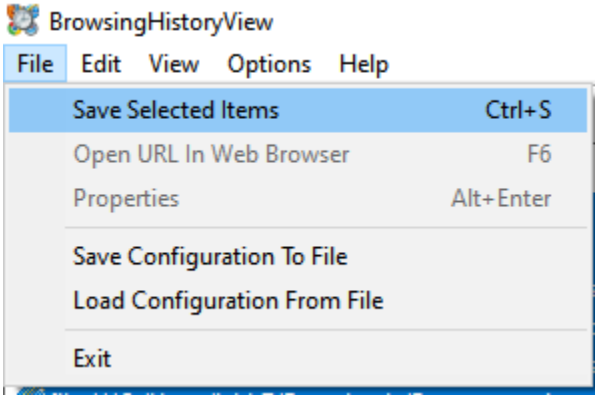
54 item(s) NirSoft Freeware. http://www.nirsoft.net

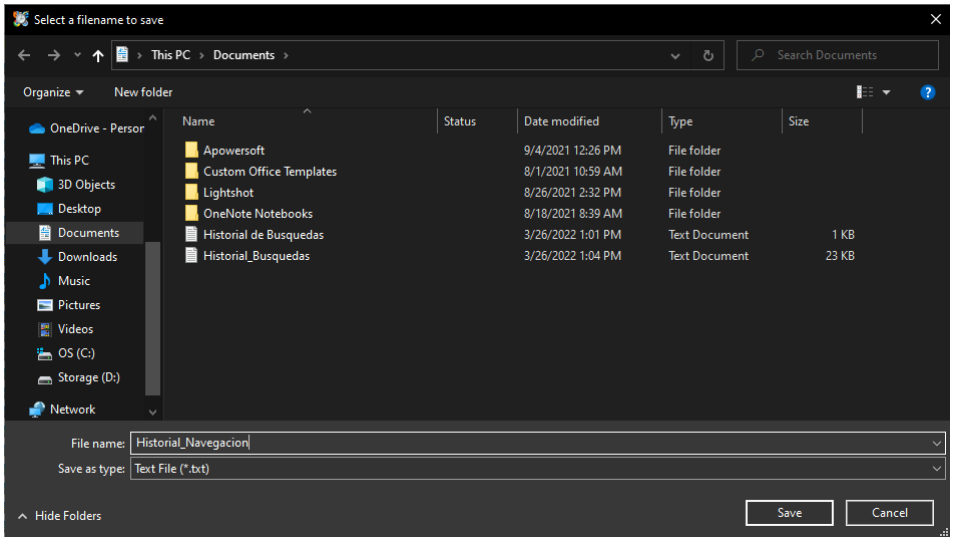
Para guardar la información obtenida por la herramienta, se realizar lo siguiente:

Edit > Select All



File > Save Selected Items





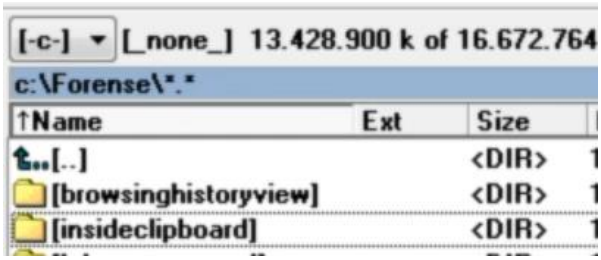
Al abrir el archivo .txt se muestra la siguiente información.

Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

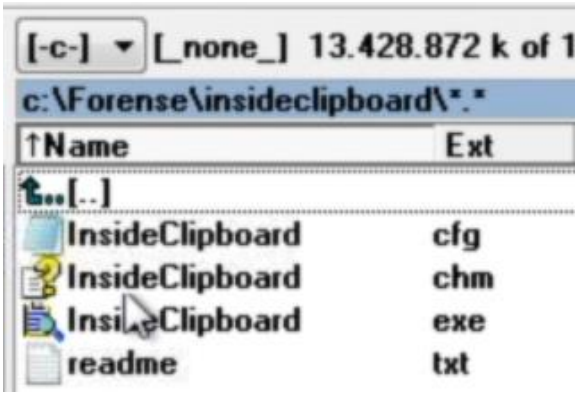
Captura del portapapeles

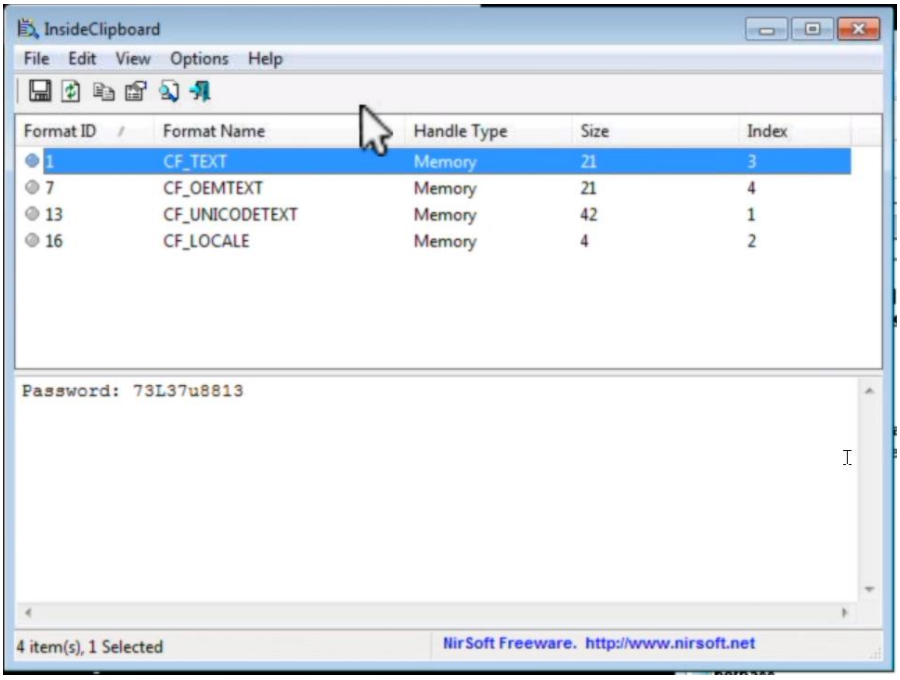
El portapapeles contiene URLs, contraseñas, información de carácter recurrente, etc.

Para el ejemplo, se utilizará la herramienta insideclipboard.

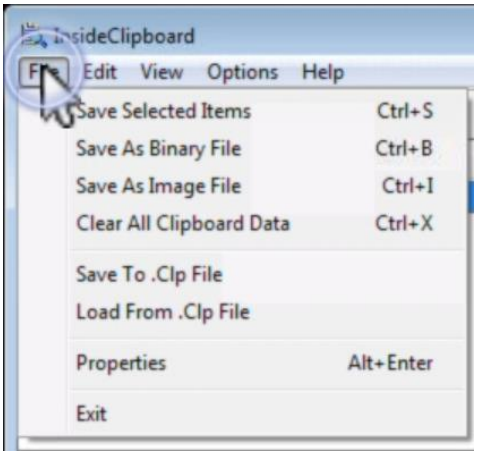


Se debe ejecutar el archivo .exe como administrador.





La herramienta permite guardar la información en diversos formatos.

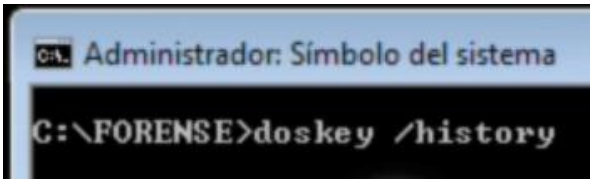


Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

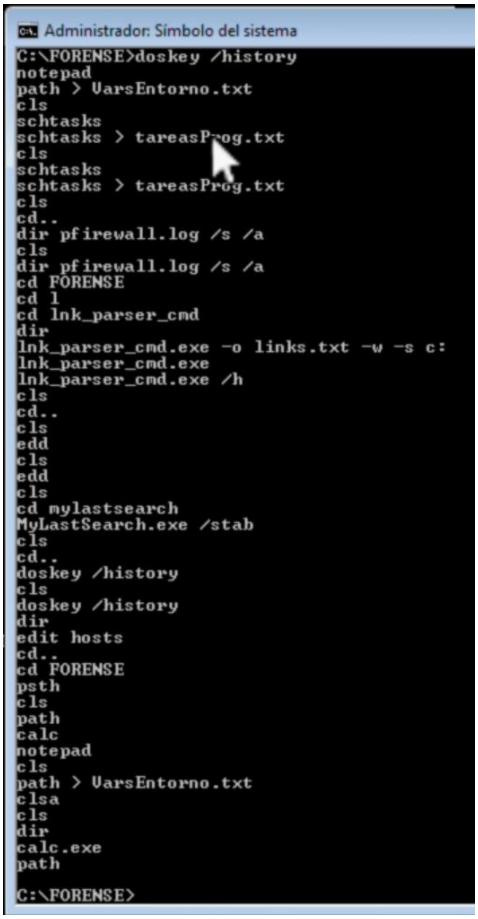
Capturar historial de consola

El historial de comandos de la consola puede proporcionar indicios de los conocimientos del atacante.

Para visualizar el historial de consola, se debe ejecutar el comando doskey /history



Para el ejemplo, devuelve la siguiente información:



Para guardar los resultados se ejecuta el siguiente comando:

Doskey /history > Historial_consola.txt

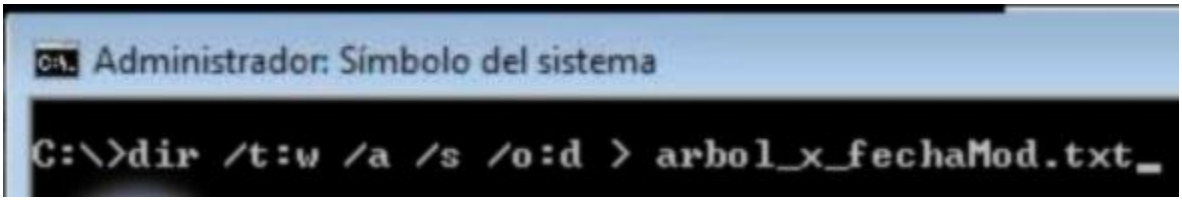
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Capturar estructura MAC de carpetas y archivos

Es necesario obtener los listados MAC (Modificación, Acceso, Creación) de los archivos y carpetas del disco duro.

Para obtener el listado por Modificación y posteriormente guardarlo en un archivo .txt se ejecuta el siguiente comando:

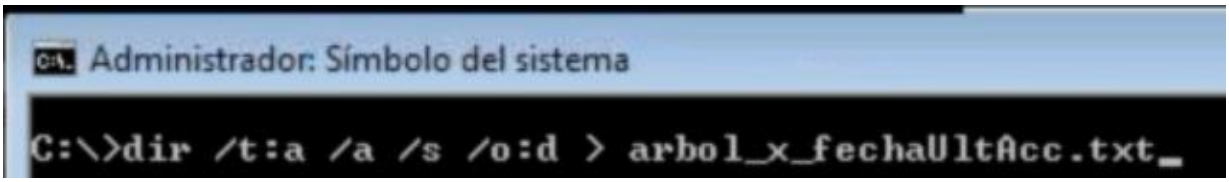
Dir /t:w /a /s /o:d > arbol_x_fechaMod.txt



/t significa tipo, :w significa por fecha de modificación, /a que liste todas las carpetas inclusive las ocultas, /s significa subdirectory, es decir que realice anidado de todas las carpetas que van conteniendo carpetas hasta la última, /o significa orden, :d significa que lo orden por fecha y hora desde la más antigua hasta la más reciente y finalmente que guarde esa información en el archivo .txt indicado.

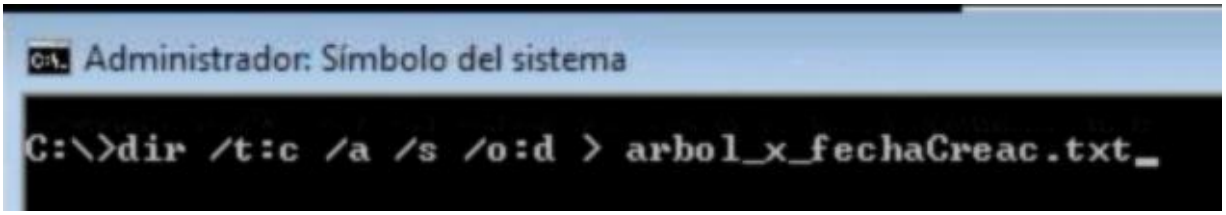
Posteriormente, se ejecutan los siguientes comandos para obtener los listados de Acceso y Creación:

Dir /t:a /a /s /o:d > arbol_x_fechaUltAcc.txt



:a significa por fecha de acceso.

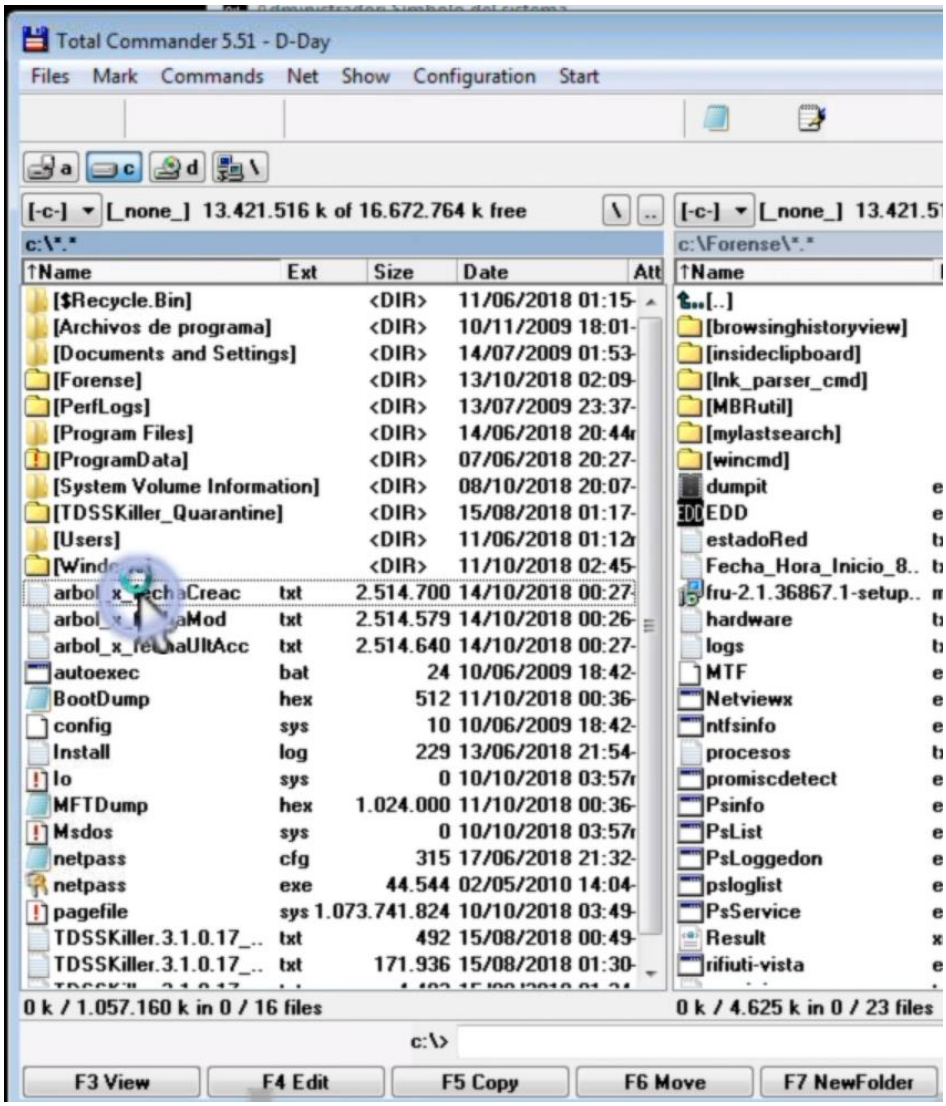
Dir /t:c /a /s /o:d > arbol_x_fechaCreac.txt



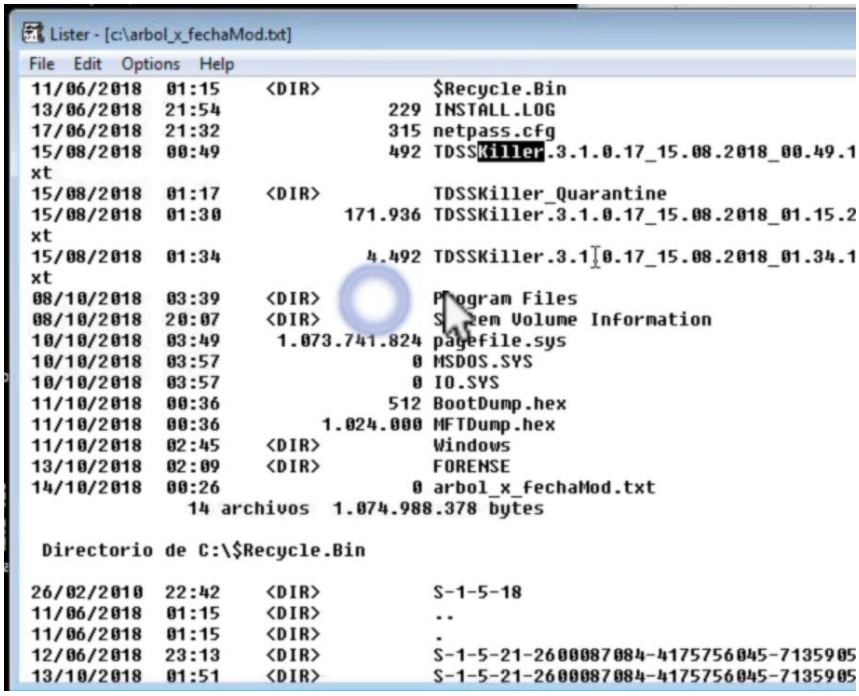
:c significa por fecha de creación.

Importante: los comandos deben ser ejecutados desde el directorio raíz, para el ejemplo, se ejecutaron desde el disco C:

Una vez generados los archivos, se debe validar su contenido, para el ejemplo, desde la aplicación total commander se hace click en F3 View para validar el contenido de los archivos seleccionados.



Al abrir los archivos, se muestra la siguiente información:



Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Sección 6: Toma de evidencias no volátiles (Contraseñas)

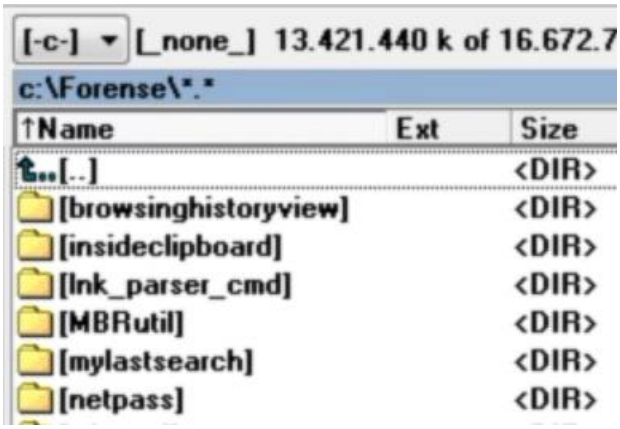
Capturar las contraseñas a recursos de red

Es necesario capturar las credenciales de acceso a los recursos de la red, ya sea un disco duro compartido, para formar parte de un dominio, para conectarse a un servidor de correo electrónico interno o de base de datos de administración interna que requiera usuario y contraseña.

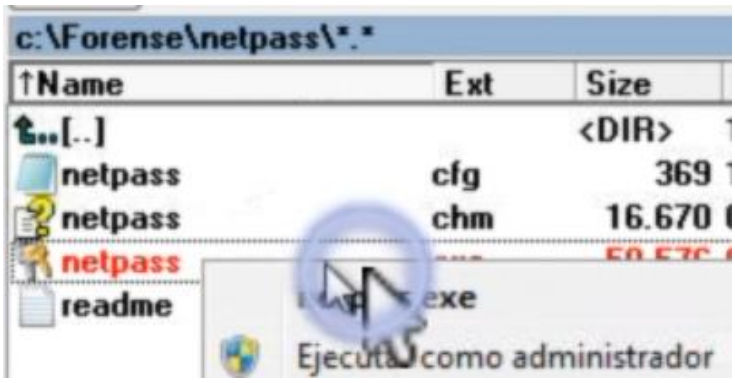
Esto permite trazar un perfil de actividades del intruso e indican por donde se debe de buscar.

Importante: Existe una serie de condiciones para que el software que será utilizado en los ejemplos funcione, ya que depende de cómo estén configurados los master password, de cómo esté configurado cierto nivel de seguridad en el registro de Windows, si la PC está o no integrada a un dominio, etc.

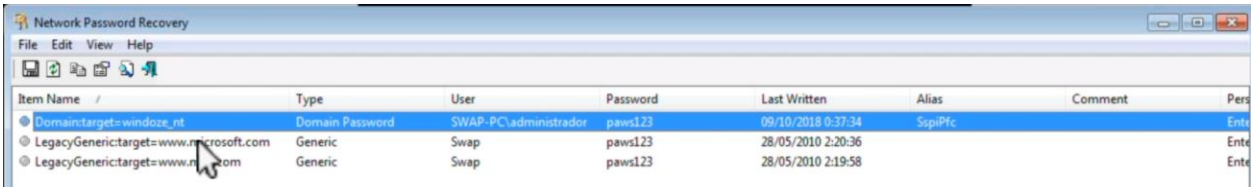
Para el ejemplo, se utilizará la herramienta netpass.

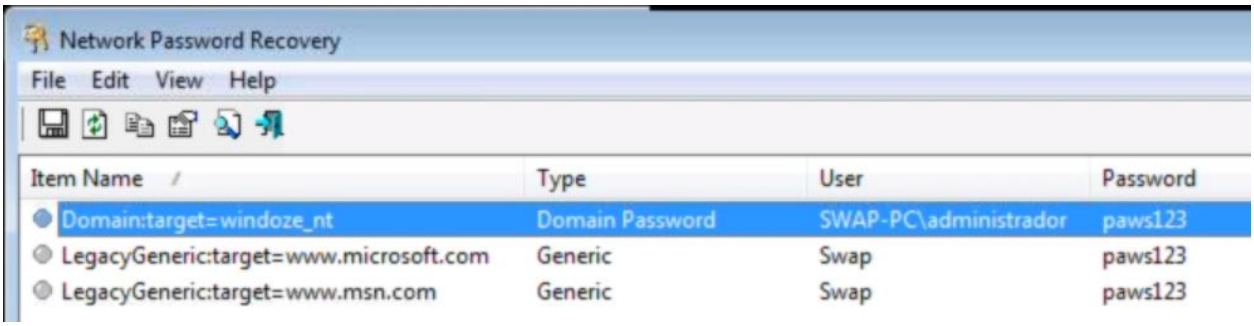


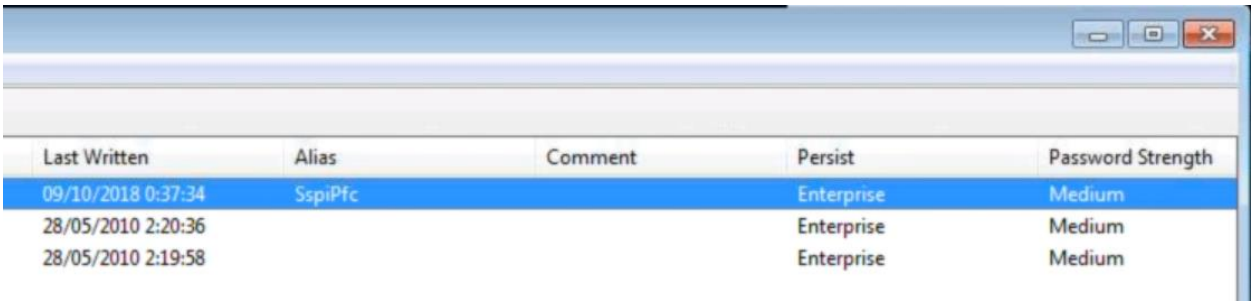
Se debe ejecutar el archivo .exe. como administrador.



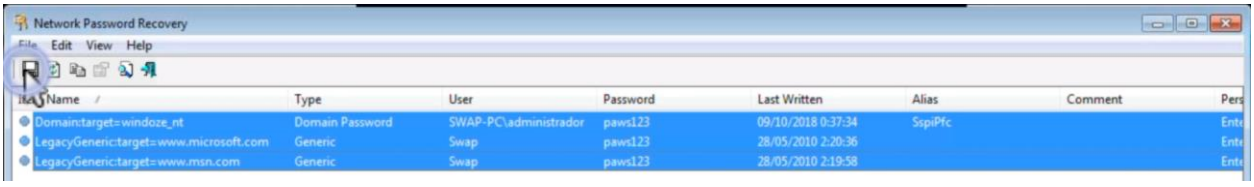
Para el ejemplo, se muestra lo siguiente:

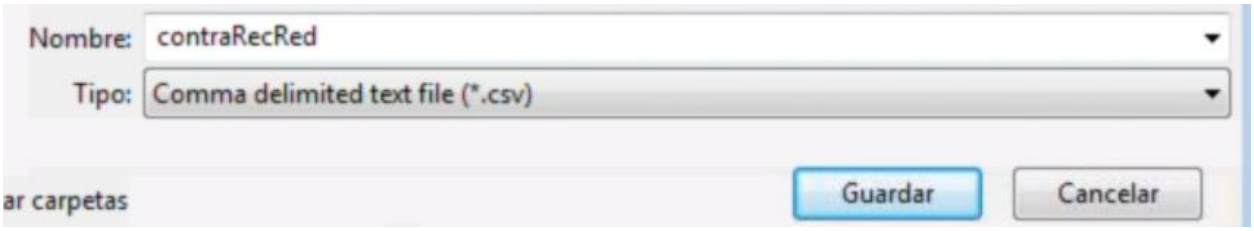




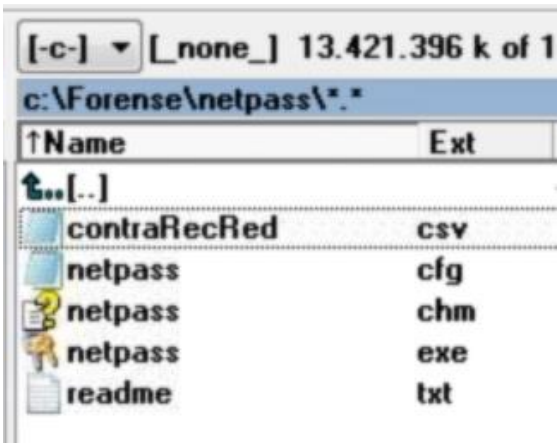


Para guardar la información proporcionada por la herramienta, se deben de seleccionar todos los campos y posteriormente dar click en el ícono del disket.

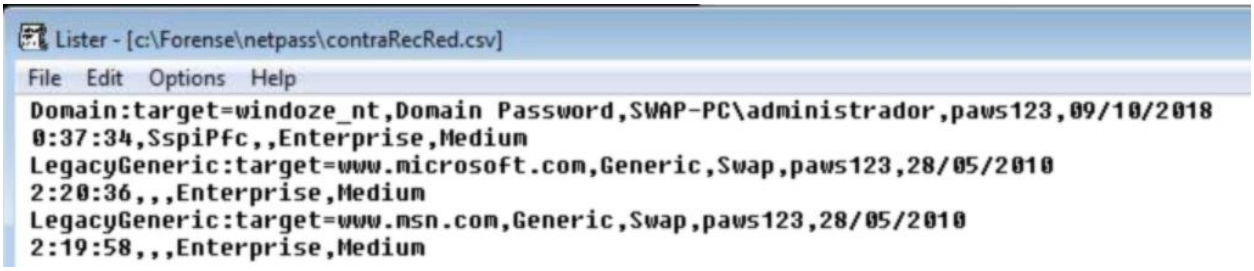




El archivo fue generado en la ruta indicada.



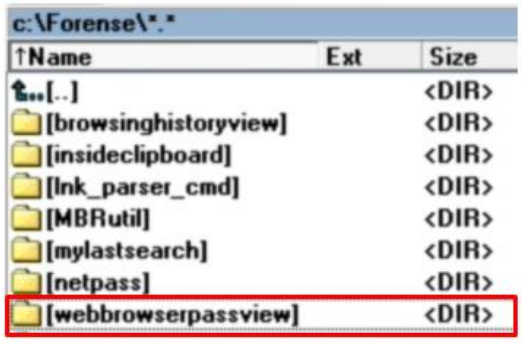
Al abrirlo, mostrará la información en el formato elegido, en este caso se eligió el formato csv:



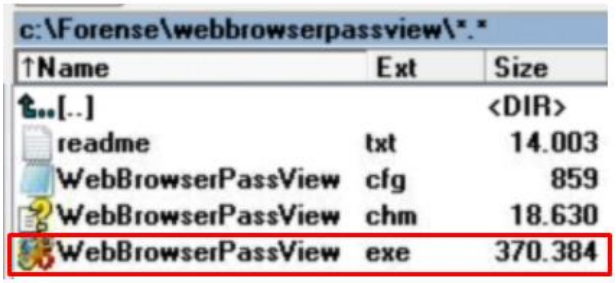
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Capturar Usuarios y Contraseñas desde los navegadores

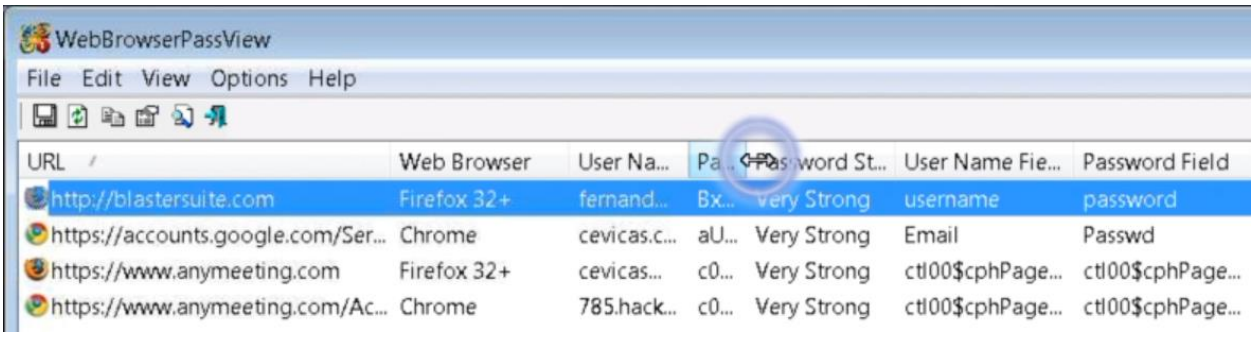
Para ejemplificar la captura de usuarios y contraseñas desde los navegadores, se utilizará la herramienta webbrowserpasswview de Nirsoft.



Se debe ejecutar el archivo .exe como administrador.



Al listar la información, se incluirá la URL adonde se conectó, con que navegador web lo realizó, el nombre de usuario y la contraseña que utilizó, la longitud de la contraseña, así como la fecha de creación y modificación de la contraseña.



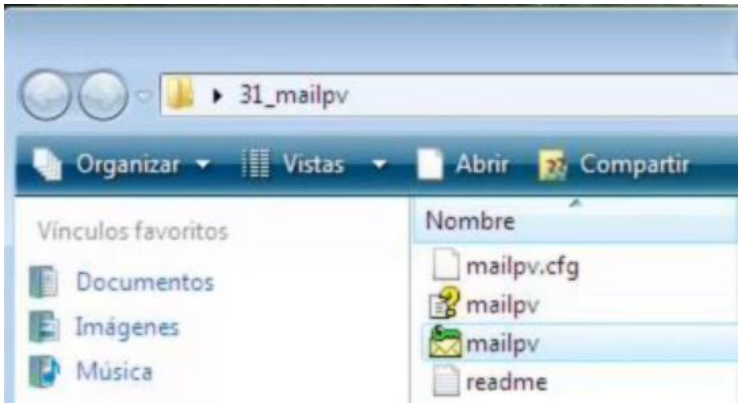
Para guardar la información proporcionada por la herramienta, se deben de seleccionar todos los campos y posteriormente dar click en el ícono del disket.

Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Capturar las contraseñas del correo electrónico

Se deben de capturar las contraseñas de los gestores de correo electrónico por si el intruso las modificó como parte del ataque.

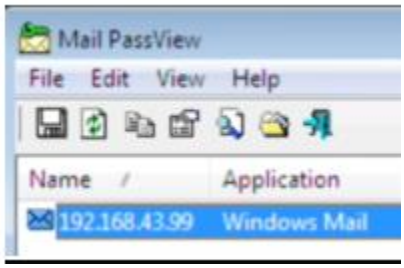
Para ejemplificar la captura de contraseñas del correo electrónico, se utilizará la herramienta mailpv.

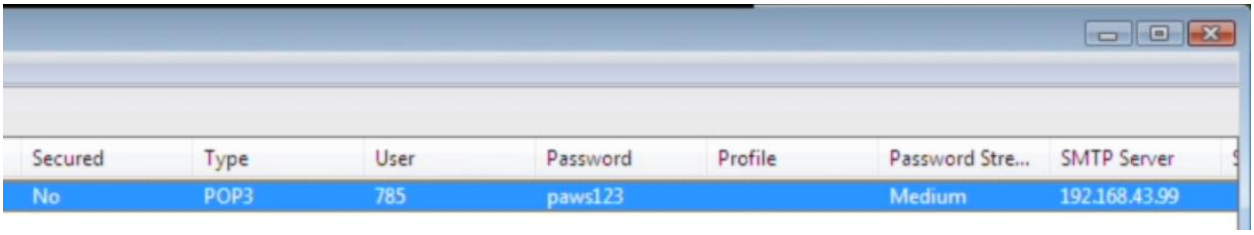


El archivo mailpv debe ejecutarse como administrador.

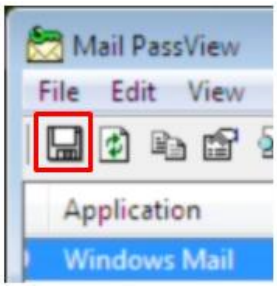
La herramienta automáticamente busca en todos los archivos de configuración y desencripta las contraseñas.

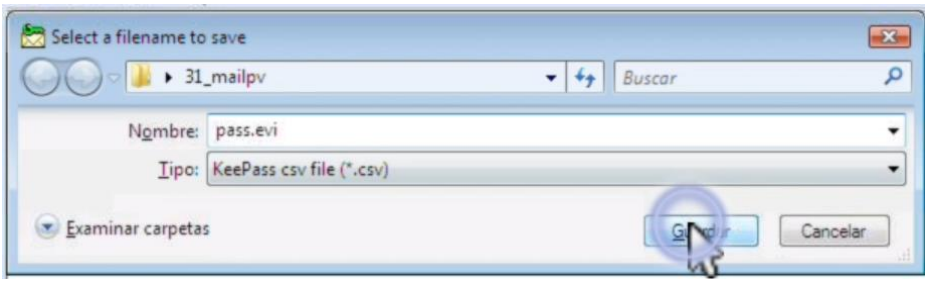
Para el ejemplo, se muestra la siguiente información:

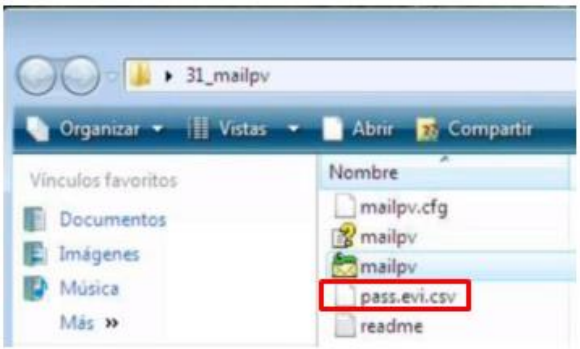


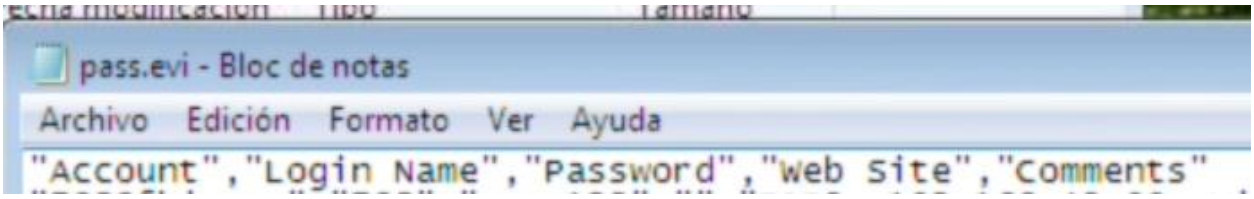


Para guardar la información proporcionada por la herramienta, se deben de seleccionar todos los campos y posteriormente dar click en el ícono del disket.









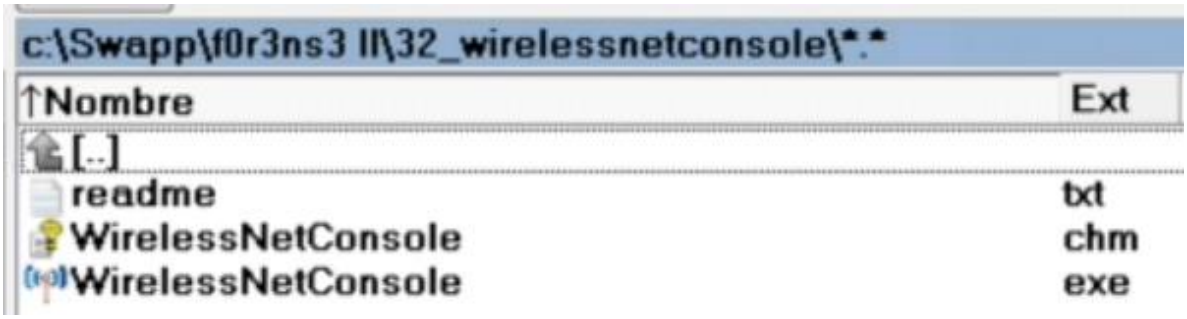
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Sección 7: Toma de evidencias desde el Registro

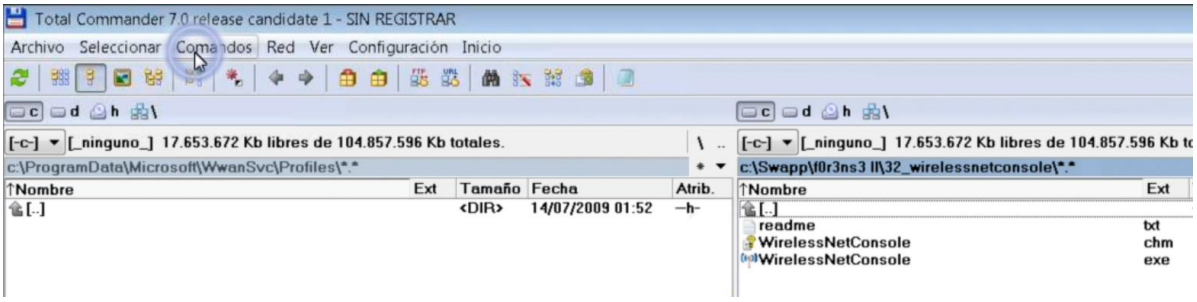
Capturar las redes WiFi a las que se han conectado

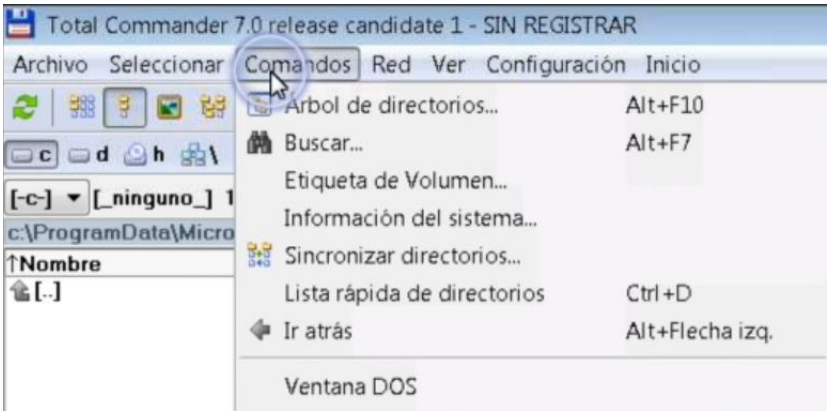
Verificar las redes WiFi a las que se han conectado resulta útil para descubrir aplicaciones.

Para ejemplificar la captura de las redes WiFi a las que se han conectado, se utilizará la herramienta wirelessnetconsole.

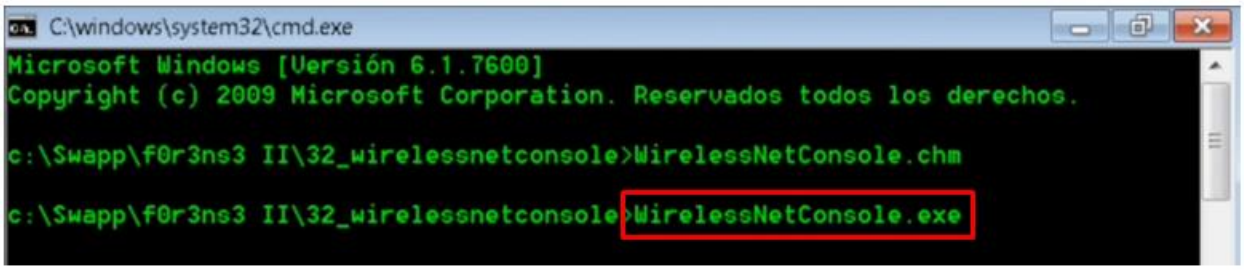


Mediante la aplicación total commander, es posible abrir la consola dando click del lado derecho de la aplicación que es en donde se encuentra la carpeta wirelessnetconsole, posteriormente ir a Comandos > Ventana DOS

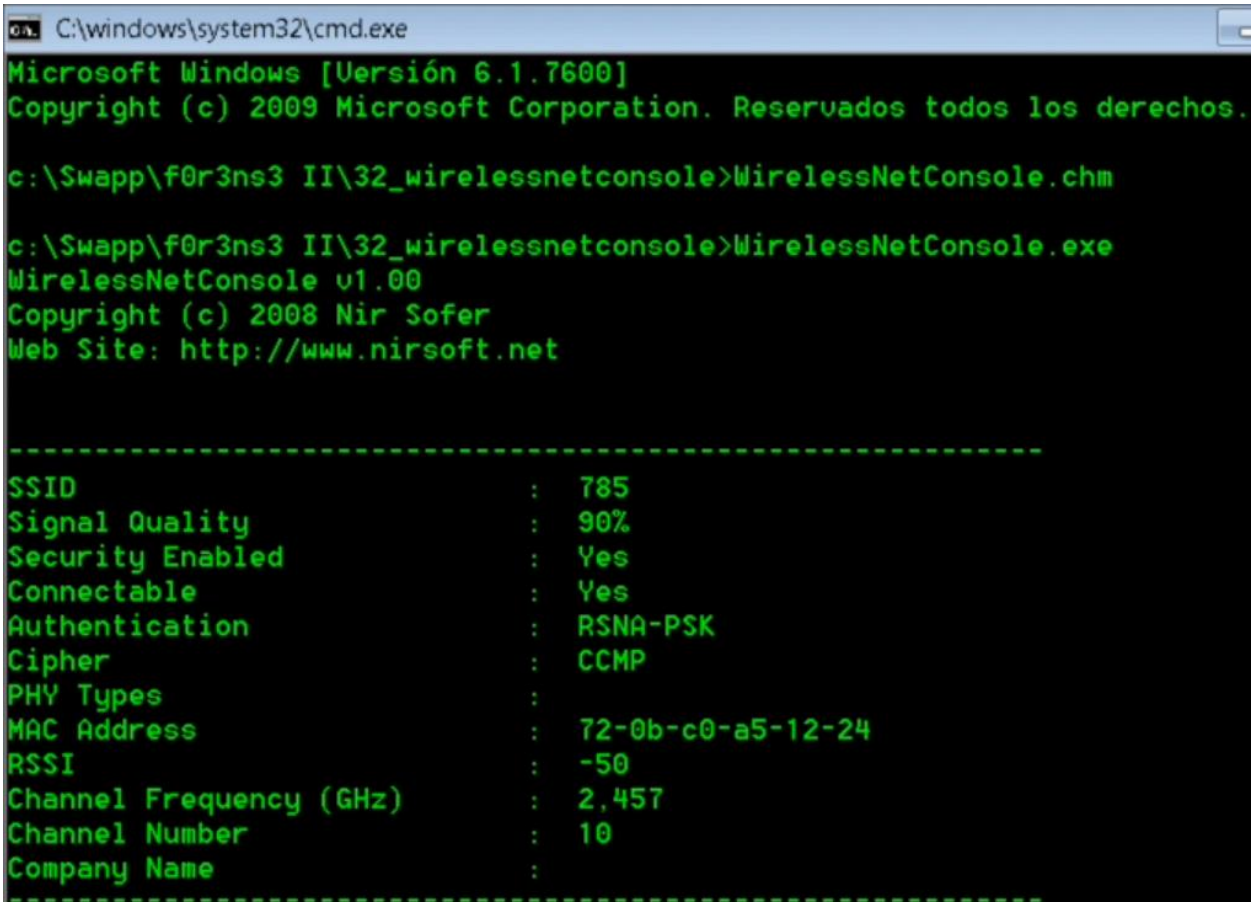




En la consola, se debe escribir el comando WirelessNetConsole.exe



Se muestra la siguiente información:



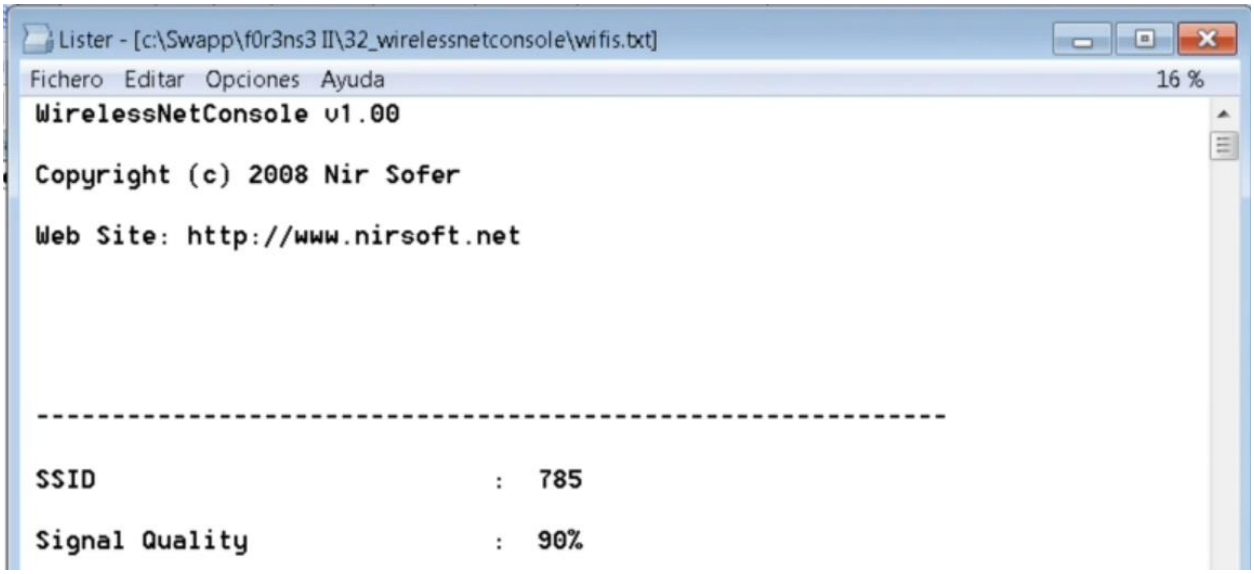
El parámetro Signal Quality podría brindar indicios de la presencia de redes WiFi sospechosas, por ejemplo, si se valida que existe una red con Calidad de la señal a 40 % y la señal del router verdadero es de 100 %, lo anterior puede ser una importante evidencia a tomar en cuenta.

Para capturar la información en un archivo de texto, se ejecuta el siguiente comando:

WirelessNetConsole.exe > wifis.txt

```
c:\Swapp\f0r3ns3 II\32_wirelessnetconsole>WirelessNetConsole.exe > wifis.txt
```

Al abrirlo se muestra la siguiente información:



Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Aplicaciones autoejecutadas en el inicio del sistema

El autoinicio es el lugar predilecto para perpetrar virus y troyanos en el sistema.

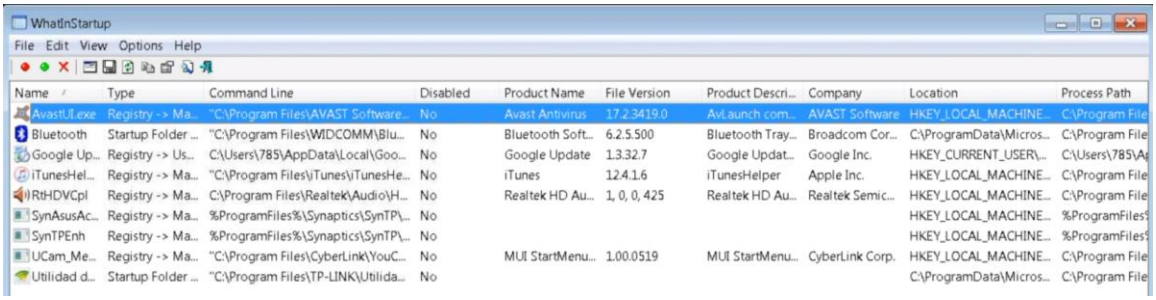
Es imperativo realizar una captura de todo el software que se ejecuta en forma automática con el inicio del sistema.

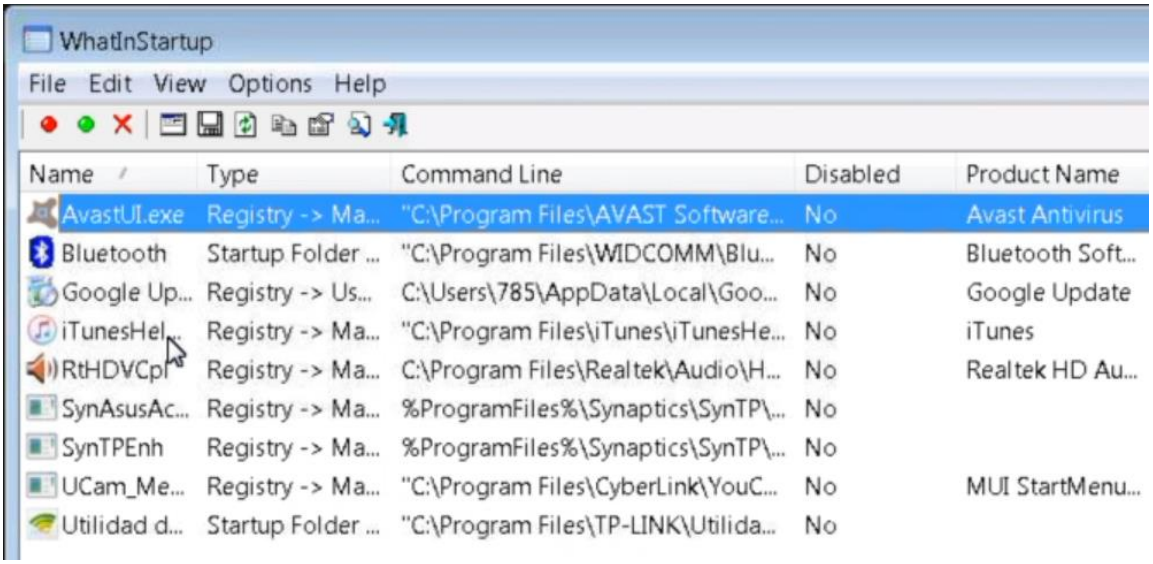
Para ejemplificar, se utilizará la herramienta WhatInStartup de Nirsoft, dicha herramienta proporciona información tal como el nombre de la aplicación, ruta completa en el disco duro, el nombre verdadero de la aplicación lo cual ayuda a validar si la aplicación es realmente la que está instalada en el sistema.

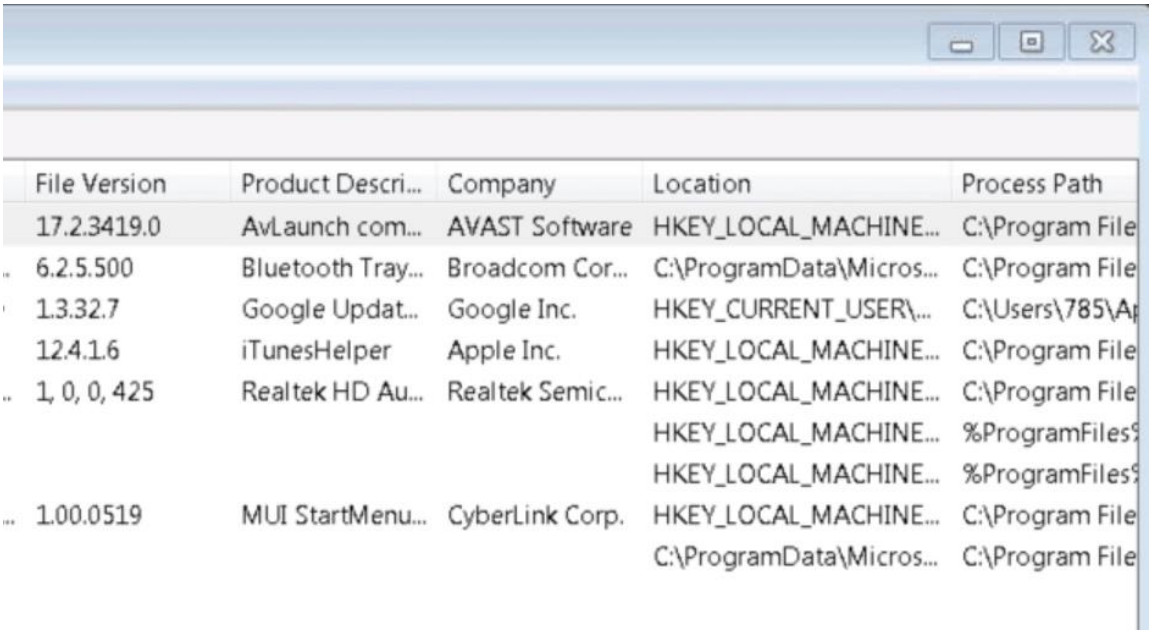
Es importante auditar todas las entradas de programas que se autoejecuten en el sistema.

Se debe ejecutar la herramienta como administrador.

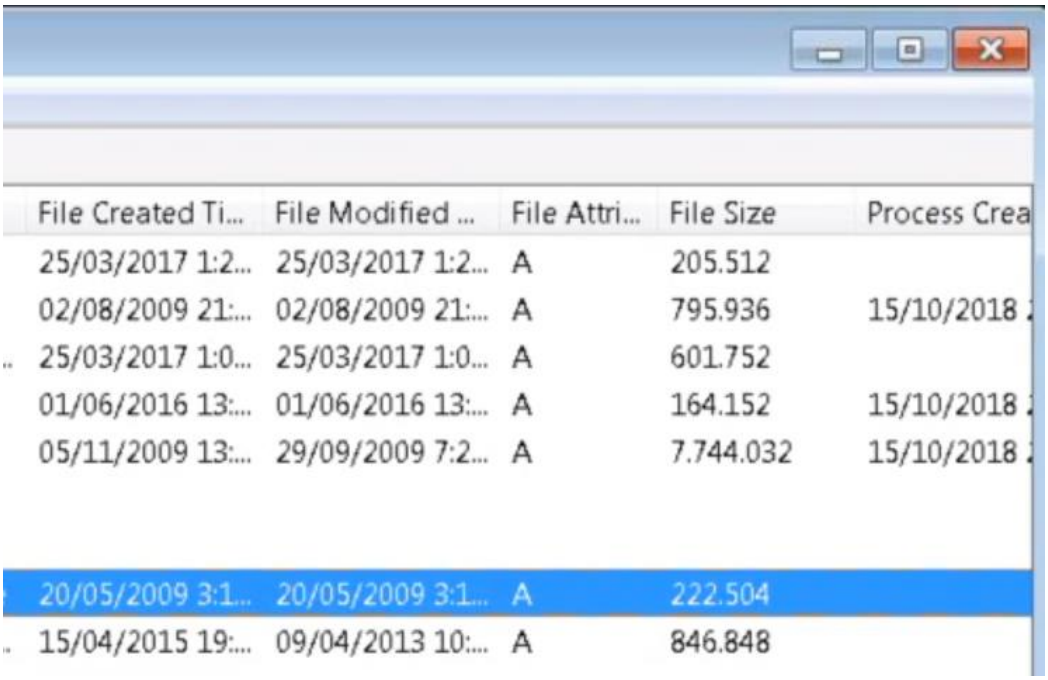
Al ejecutar la herramienta, se mostrarán los siguientes campos:





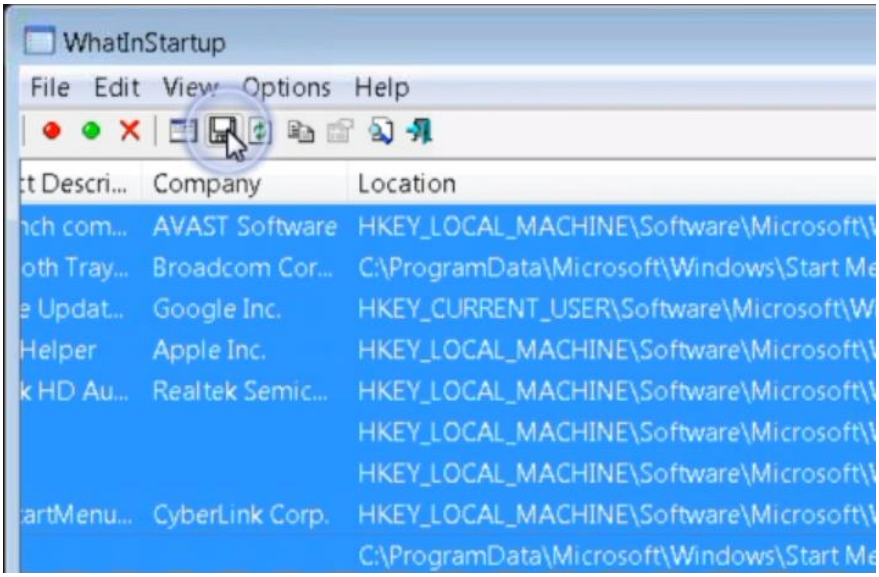


File Version	Product Descri...	Company	Location	Process Path
17.2.3419.0	AvLaunch com...	AVAST Software	HKEY_LOCAL_MACHINE...	C:\Program File
6.2.5.500	Bluetooth Tray...	Broadcom Cor...	C:\ProgramData\Micros...	C:\Program File
1.3.32.7	Google Updat...	Google Inc.	HKEY_CURRENT_USER\...	C:\Users\785\Ap
12.4.1.6	iTunesHelper	Apple Inc.	HKEY_LOCAL_MACHINE...	C:\Program File
1, 0, 0, 425	Realtek HD Au...	Realtek Semic...	HKEY_LOCAL_MACHINE...	C:\Program File
			HKEY_LOCAL_MACHINE...	%ProgramFiles%
			HKEY_LOCAL_MACHINE...	%ProgramFiles%
1.00.0519	MUI StartMenu...	CyberLink Corp.	HKEY_LOCAL_MACHINE...	C:\Program File
			C:\ProgramData\Micros...	C:\Program File



File Created Ti...	File Modified ...	File Attri...	File Size	Process Crea
25/03/2017 1:2...	25/03/2017 1:2...	A	205.512	
02/08/2009 21:...	02/08/2009 21:...	A	795.936	15/10/2018
25/03/2017 1:0...	25/03/2017 1:0...	A	601.752	
01/06/2016 13:...	01/06/2016 13:...	A	164.152	15/10/2018
05/11/2009 13:...	29/09/2009 7:2...	A	7.744.032	15/10/2018
20/05/2009 3:1...	20/05/2009 3:1...	A	222.504	
15/04/2015 19:...	09/04/2013 10:...	A	846.848	

Para guardar la información, se seleccionan todos los registros, luego click en el ícono de disket.

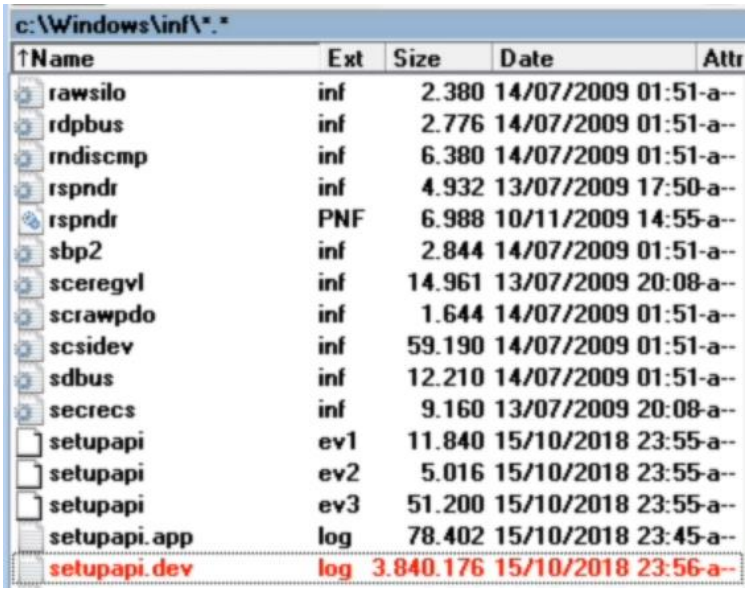


Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

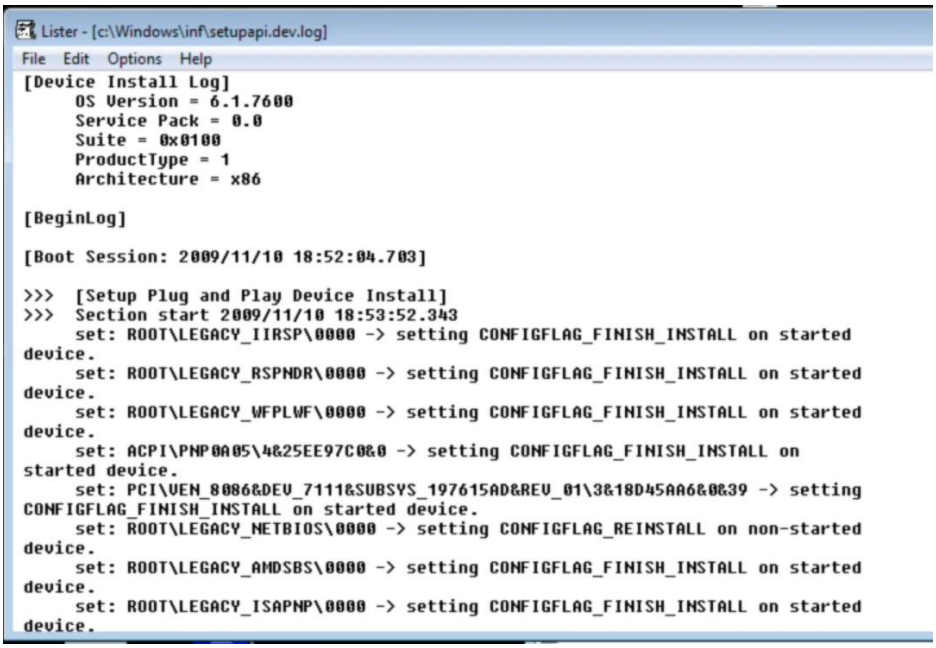
Capturar los dispositivos USB que se hayan conectado

Se debe recrear la base de datos de dispositivos USB conectados en el sistema.

En el archivo setupapi.view localizado en la ruta C:\Windows\inf\,

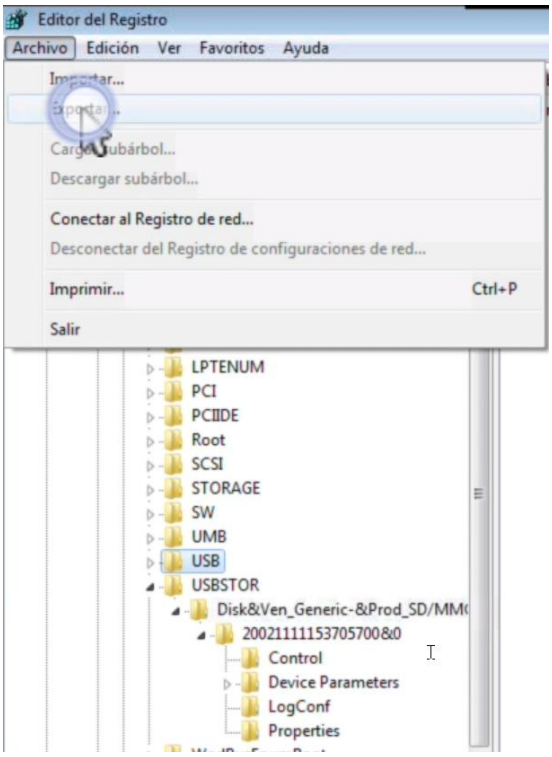


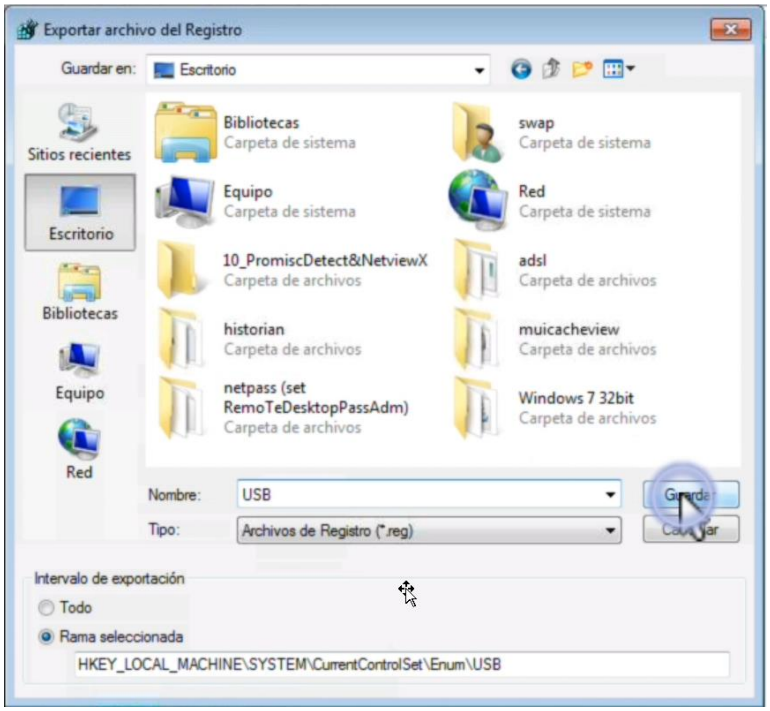
Al abrirlo, muestra la siguiente información:



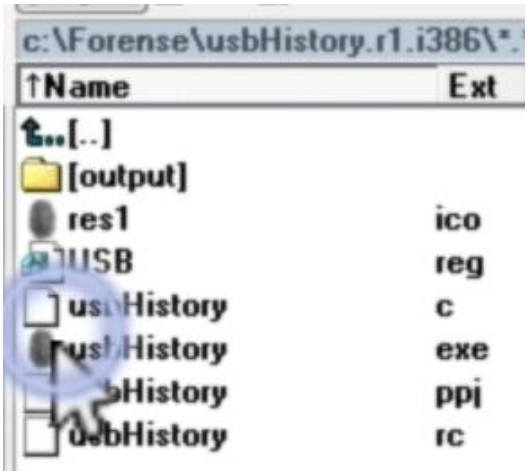
Importante: se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

También es posible realizar la captura de la información en las claves de registro de Windows, para realizarlo, se debe seleccionar la carpeta, luego ir a Archivo > Exportar.

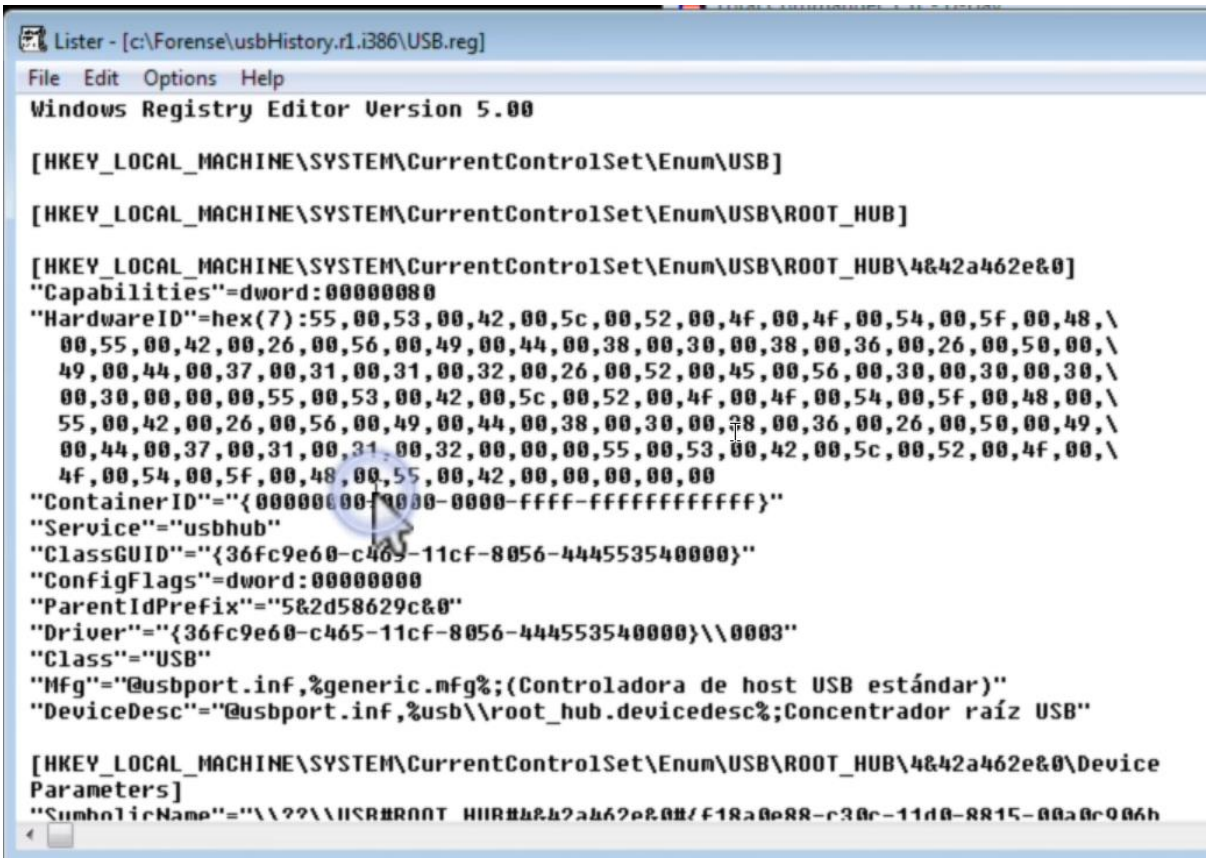




Continuando con el ejemplo, se abrirá el archivo desde la aplicación total commander.



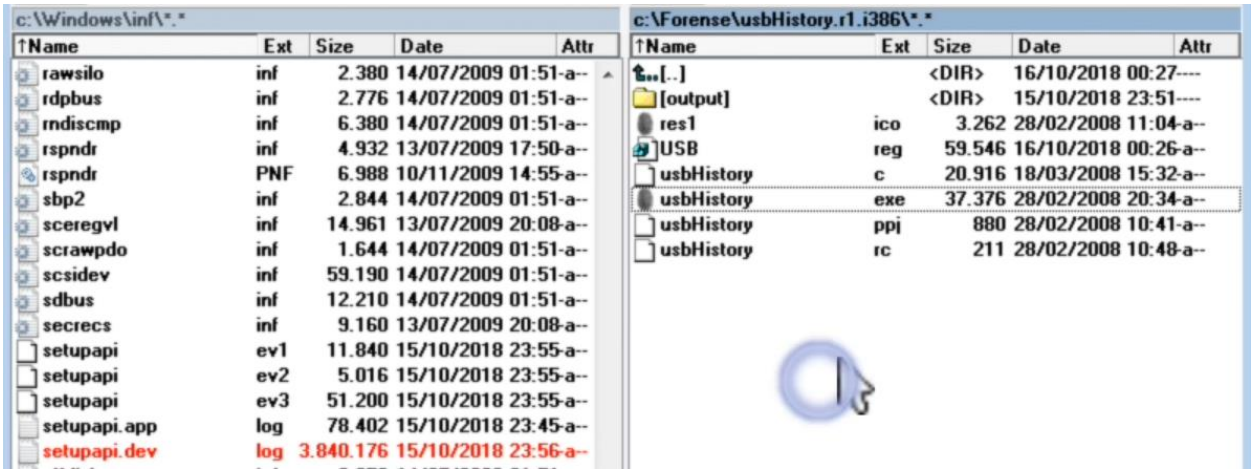
Se muestra la siguiente información:



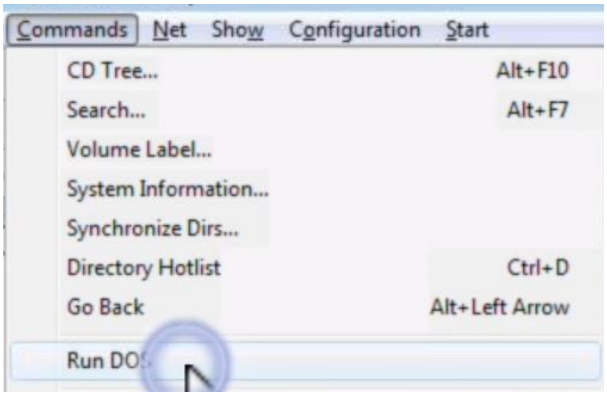
Importante: se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Lo anterior también puede capturarse mediante otras herramientas, para el ejemplo, se utilizará la herramienta usbHistory.

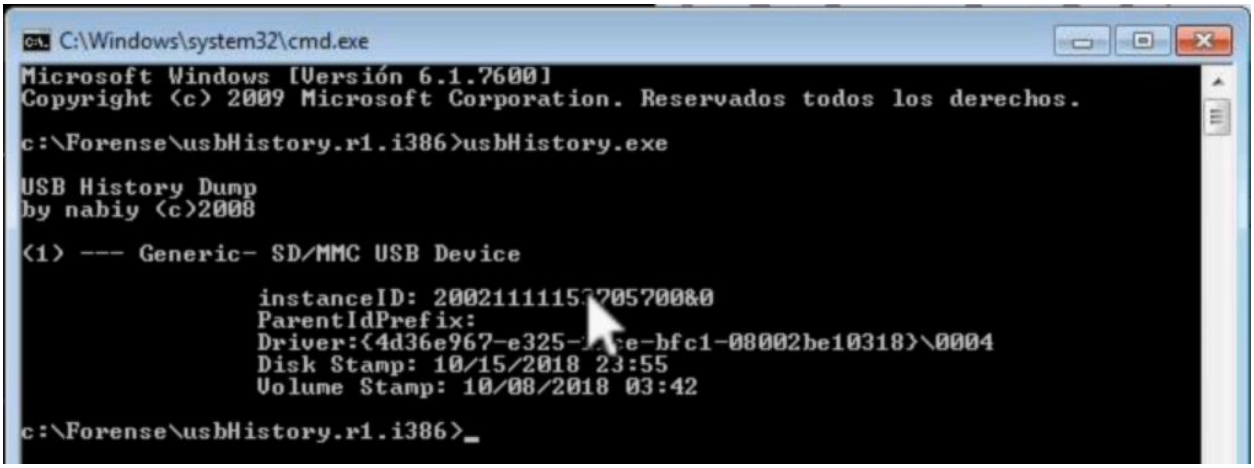
En la aplicación total commander, se da click a la parte derecha de la pantalla que es en donde está la carpeta usbHistory.



Luego ir a Commands > Run DOS



En la consola, se ejecuta el comando usbHistory.exe, al realizar esto, se muestra la siguiente información:



Para guardar la información en un archivo de texto, se ejecuta el siguiente comando:

usbHistory.exe > HistorialUSB.txt

Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

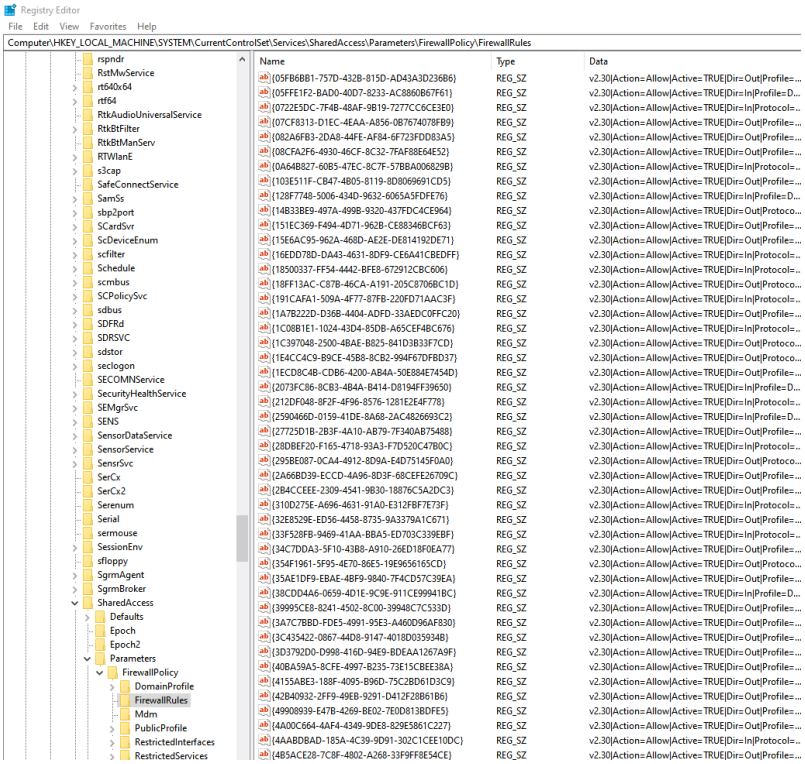
Capturar la configuración del Firewall

Se deben capturar las posibles excepciones del firewall.

Lo más importante al momento de auditar las reglas del firewall, es validar que no existan excepciones que permitan conectar troyanos o aplicaciones de control remoto desde la red pública o privada.

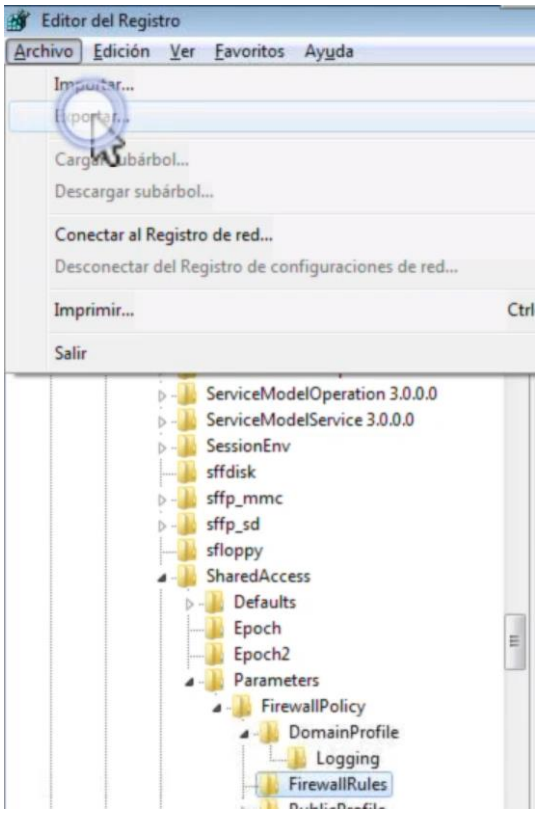
Para realizar lo anterior es necesario navegar a las claves de registro en regedit en la siguiente ruta

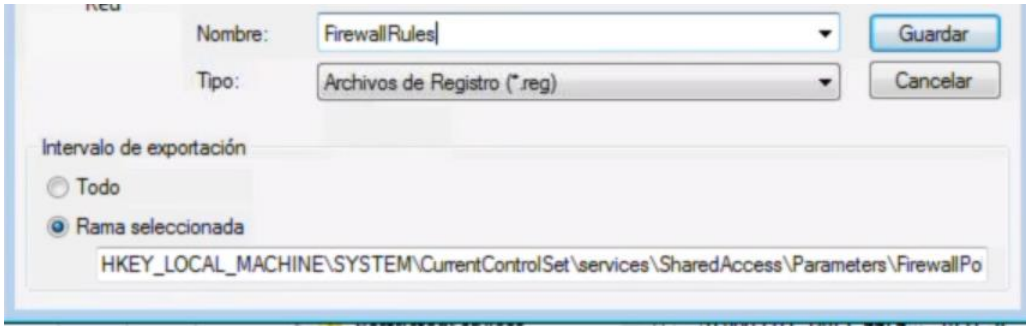
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules



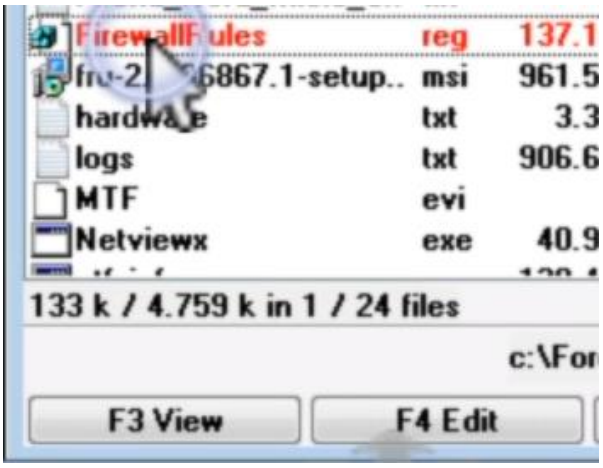
Para obtener la información, es necesario seleccionar la carpeta FirewallRules, luego ir a:

Archivo > Exportar.





En la aplicación total commander se selecciona el archivo y click en F3 View.



Se muestra la siguiente información:

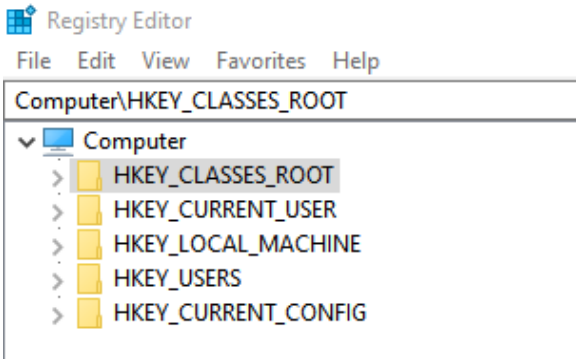
Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Capturar posibles Registry Spawnings

Windows almacena en el registro ciertas entradas que tienen que ver con la asociación de extensiones y programas.

Existe una técnica utilizada por los troyanos y los virus que se denomina Registry Spawner, un Registry Spawner es una modificación a cierta entrada del registro que tenga que ver con las extensiones para ejecutar otro archivo u otra extensión de archivo, etc.

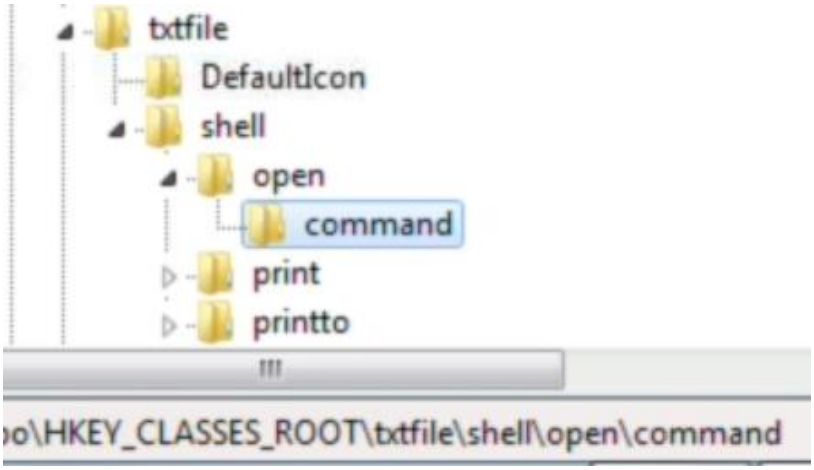
En regedit, se extiende a carpeta la carpeta HKEY_CLASSES_ROOT.



Dentro de dicha carpeta existe una rama de registro para cada tipo de extensión de archivo.

Para validar el contenido, se debe desplegar lo siguiente:

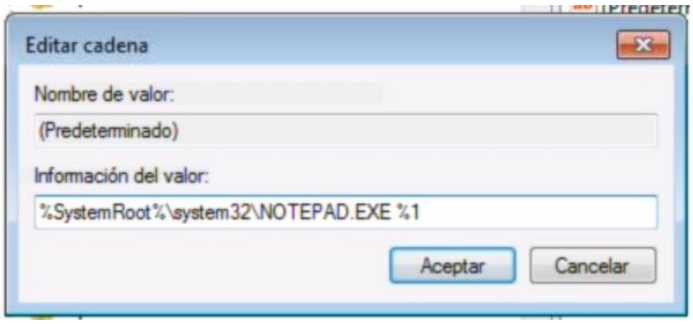
Shell > open >command.



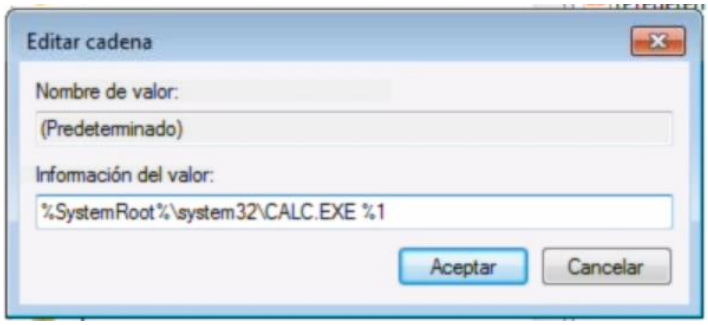
Al realizar lo anterior, se mostrará lo siguiente:

Significa que al abrir un archivo .txt, se abrirá el Notepad.

Un virus podría tener acceso al registro y reemplazar el programa original, que para el ejemplo es el Notepad.



Para el ejemplo, se modificará de la siguiente manera:



De tal manera que cuando se abra un archivo .txt, se abrirá la calculadora.

Para obtener la información, es necesario seleccionar la carpeta HKEY_CLASSES_ROOT, luego ir a: Archivo > Exportar.

Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Capturar listado de aplicaciones instaladas

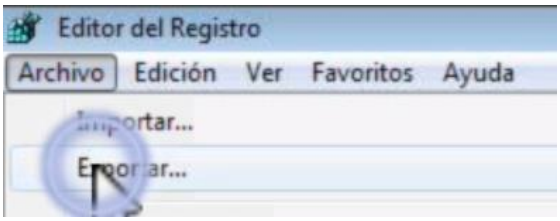
La lista de aplicaciones instaladas brindará información de posibles manipulaciones.

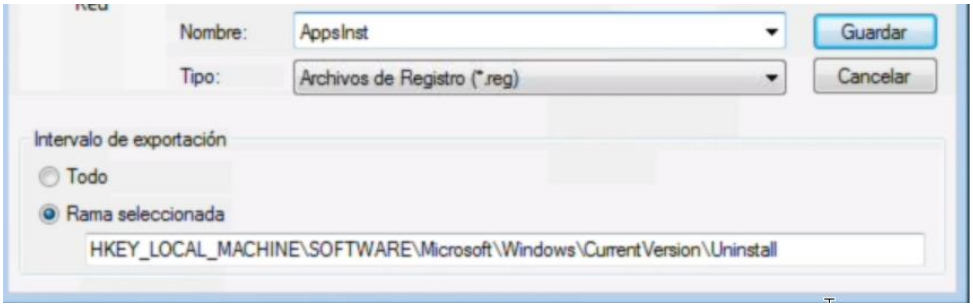
Se debe realizar la copia de la rama del registro encargada de las aplicaciones instaladas.

Por lo tanto, es necesario ir a la siguiente ruta:

Equipo\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

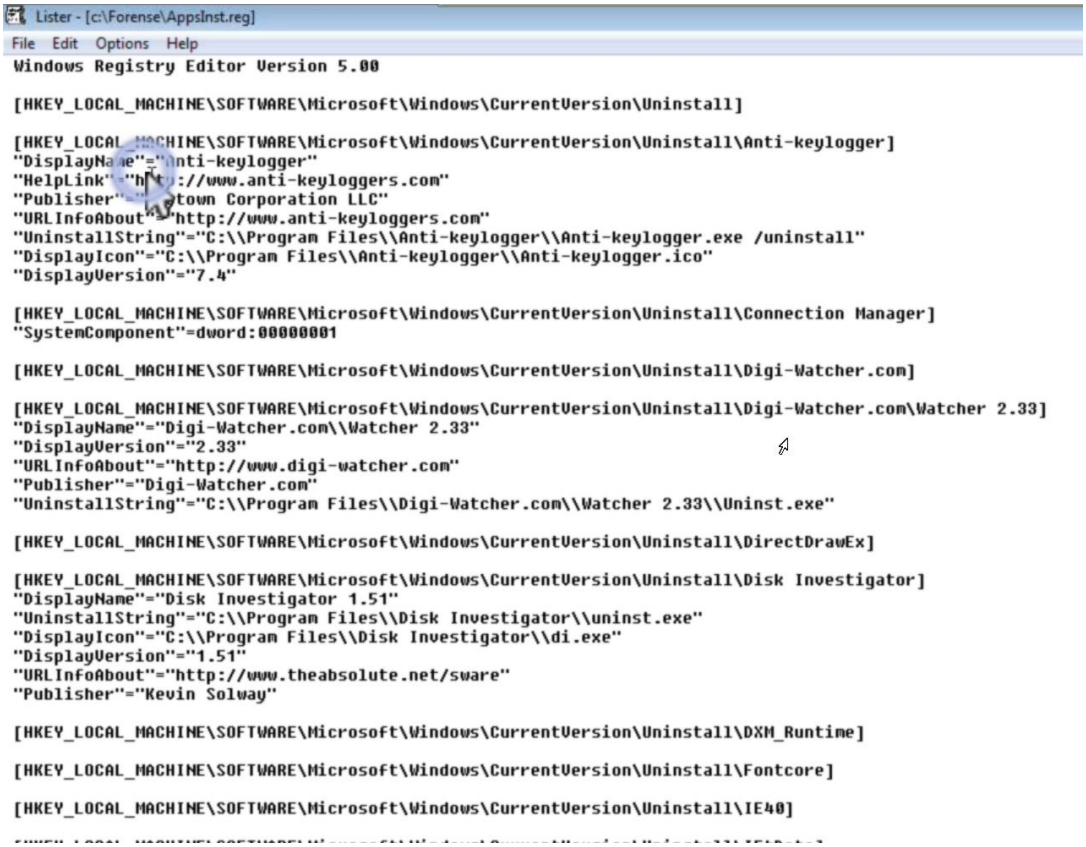
Una vez seleccionada la carpeta Uninstall, ir a: Archivo > Exportar.





Para el ejemplo, se abre el archivo desde la aplicación total commander haciendo click en F3 View.

Se muestra la siguiente información:



Importante: Al finalizar, se debe realizar la toma de la fecha y de la hora, así como el cálculo de Hash de 512 tal como se realizó en la sección 1.1, lo anterior es un mecanismo que permite asegurar la evidencia.

Sección 8: Asegurar el reingreso del forense al sistema

Que es un HOUSEKEEPER y porqué es necesario

Un House Keeper es una forma de retorno a una máquina por otro lado aún si se le ha bloqueado la cuenta de usuario normal o administrador.

Se deben crear House Keepers en todas las máquinas que van a estar bajo auditoría para que, en el caso de algún incidente, el trabajo forense se pueda concretar de mejor forma.

Plantando el Housekeeper forense

Existe una cuenta más poderosa que la del administrador, es la cuenta máquina o system.

Si se asegura un house keeper con privilegios de system, será posible pasar por encima de los rootkit que podría haber instalado el intruso.

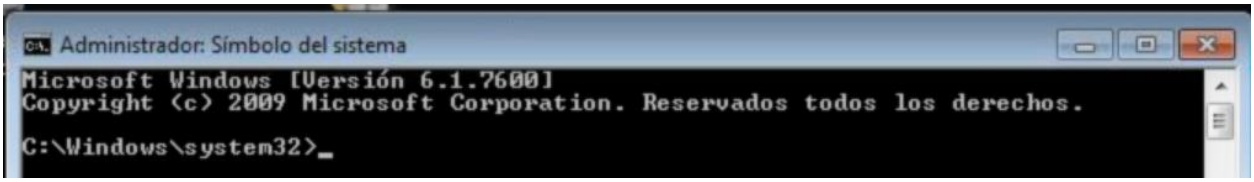
Uno de los house keepers más fácil de instrumentar y de los más efectivos ya que proporciona una Shell con privilegios system es el house keeper de las sticky key, las sticky key son un artificio de accesibilidad en casos de movilidad reducida, por ejemplo, en donde se repite la movilización de una tecla 5 veces y se abre una aplicación que tiene varias opciones de accesibilidad.

En Windows 7, 8 y 10, la aplicación se llama Utilman.exe y se encuentra localizada en la carpeta Windows/System32.

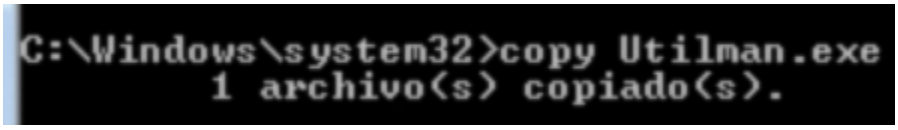
El truco está en reemplazar ese archivo cmd.exe que corresponde a la consola de DOS.

Para el ejemplo, se realiza lo siguiente:

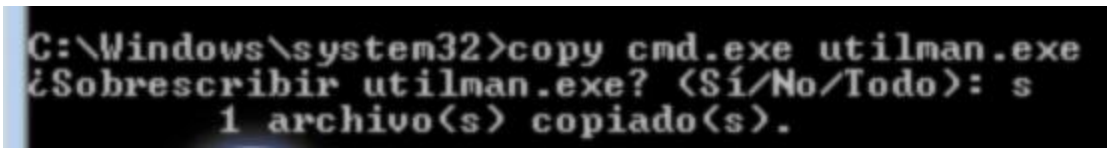
Se ejecuta como admin el cmd, posteriormente ubicarse en la ruta \Windows\System32



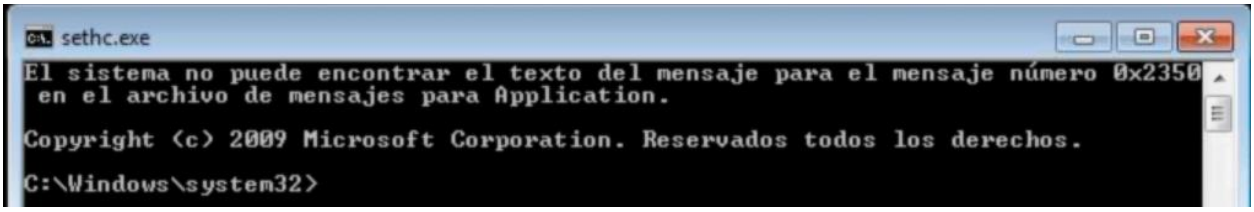
Ejecutar el siguiente comando: copy Utilman.exe



Luego, ejecutar el siguiente comando: copy cmd.exe utilman.exe



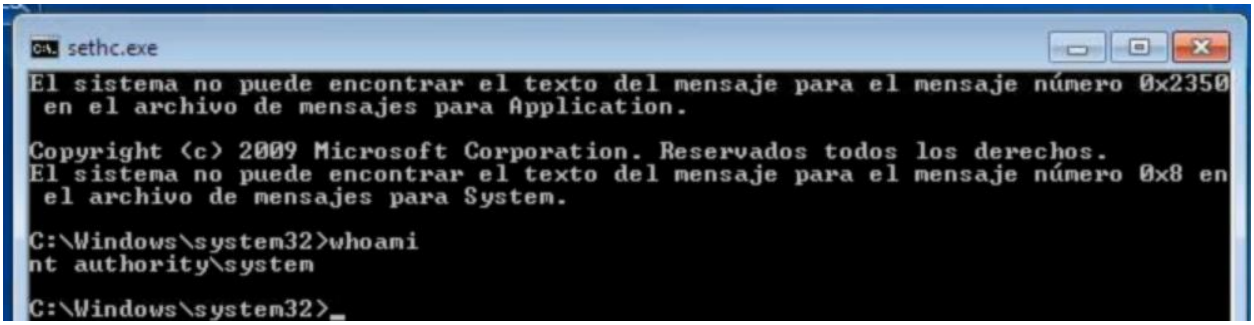
Al presionar 5 veces la tecla Shift, abrirá la consola.



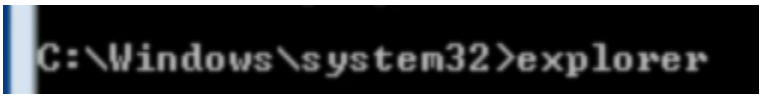
Para el ejemplo se asume que se ha troyanizado Windows y que no se tiene acceso para poder realizar la toma de evidencias.

La ventana que se muestra a continuación funciona con privilegios system.

Al presionar 5 veces la tecla Shift, se abrirá la consola, por lo tanto, se ejecuta el comando whoami y se indica que el usuario system es el actual.

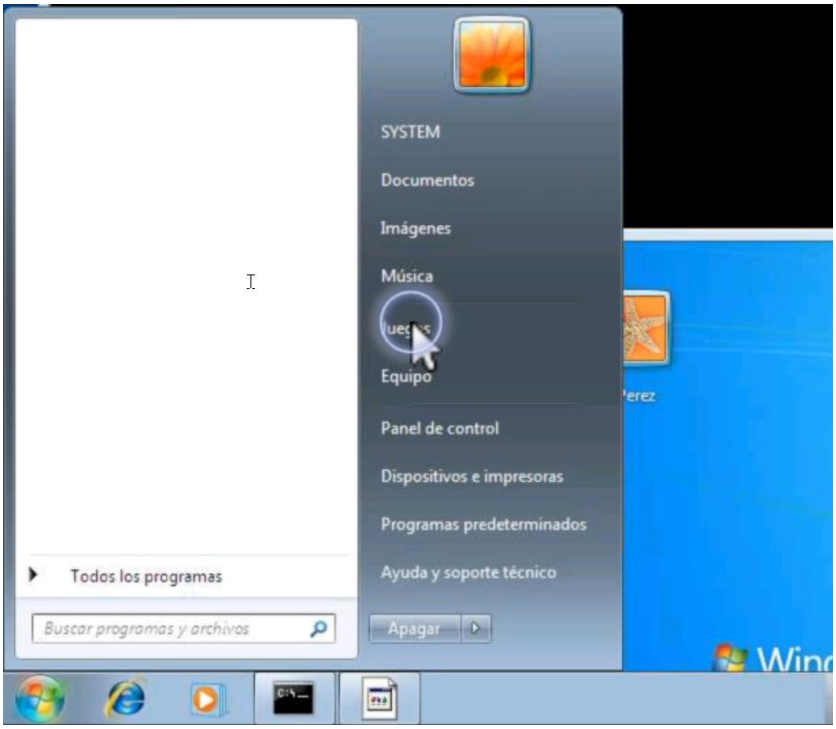


Luego, se ejecuta el comando explorer.



Tardará un poco en dar acceso, lo anterior se debe a que el usuario system no es un usuario humano, por lo tanto, nunca tuvo un perfil creado, así que tarda un poco hasta que genera el perfil como si fuese un usuario real.

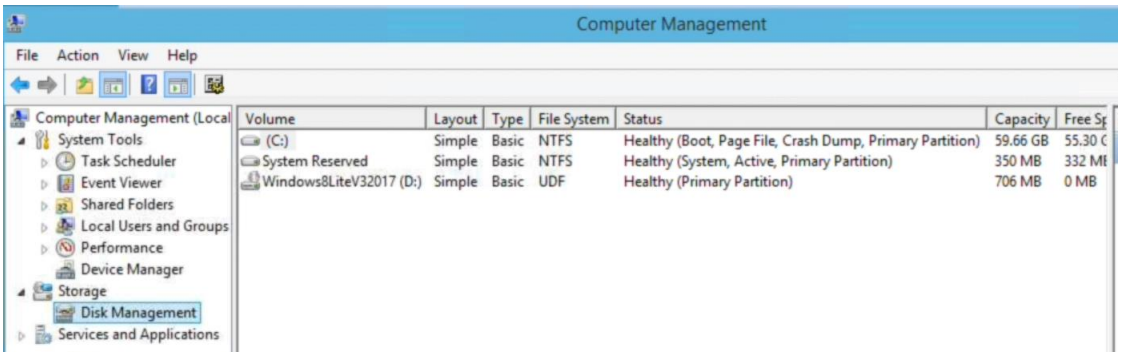
Luego de eso, ya se tendría acceso al sistema tal como se muestra en la siguiente imagen.



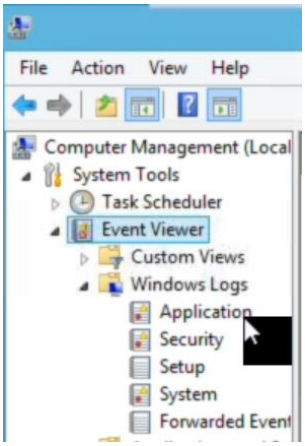
Sección 9: Análisis de Logs y procesos adicionales

Análisis de Logs – Descubrir usuarios nuevos o sospechosos

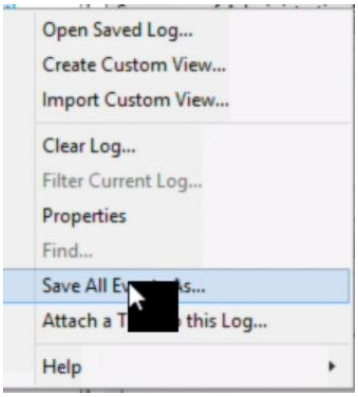
Es necesario ir a Computer Management.



Posteriormente ir a Event Viewer y desplegar Windows logs.



Para el ejemplo, se dio click derecho en Application, Security, Setup & System y luego click derecho para ir a la opción Save all Events as.



Se Guardan los archivos como .txt.

Luego se deben generar archivos desde la consola.

Se ejecuta el siguiente comando:

Find /I “Account Name” Seclog.txt > SecLog1.txt

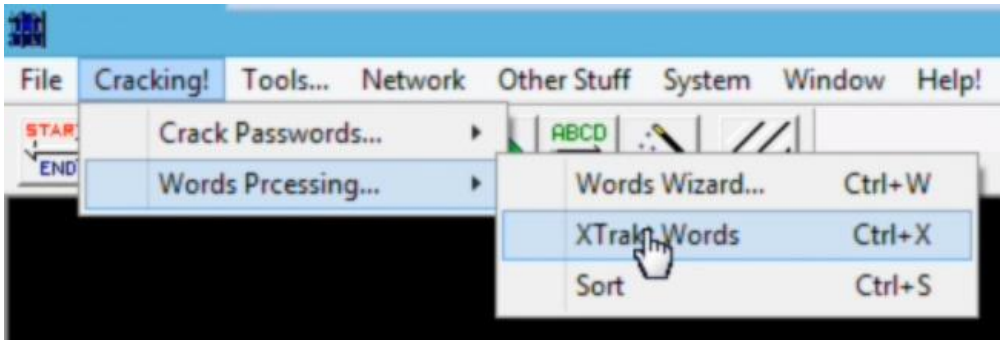
Lo que hace el comando es buscar el parámetro Account Name en el archivo SecLog,txt para luego colocar esa información en un nuevo archivo de texto.

/I significa que ignore si las palabras son mayúsculas o minúsculas.

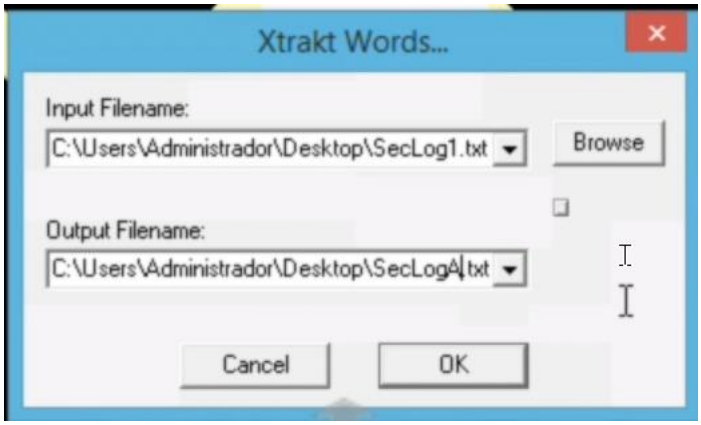
Continuando con el ejemplo, se utilizará la herramienta HackersUtility.

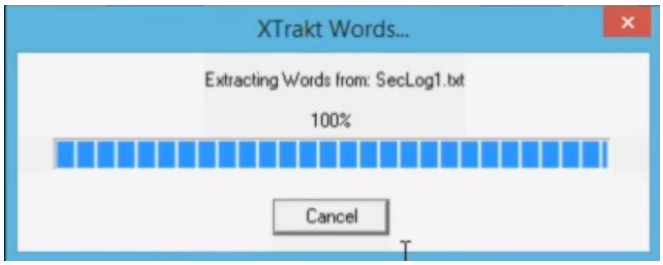
En HackersUtility ir a:

Cracking! > Words Processing > Xtrak Words.

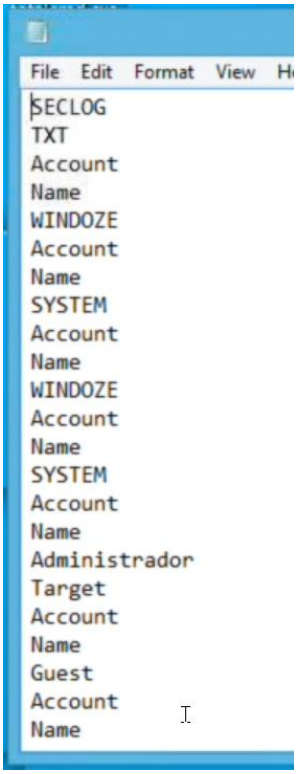


Como entrada, se coloca el archivo de texto que contiene los Account Name, en este caso es el archivo SecLog1,y como salida se coloca el nombre del nuevo archivo que se desea generar, para el ejemplo se nombró SecLogA.



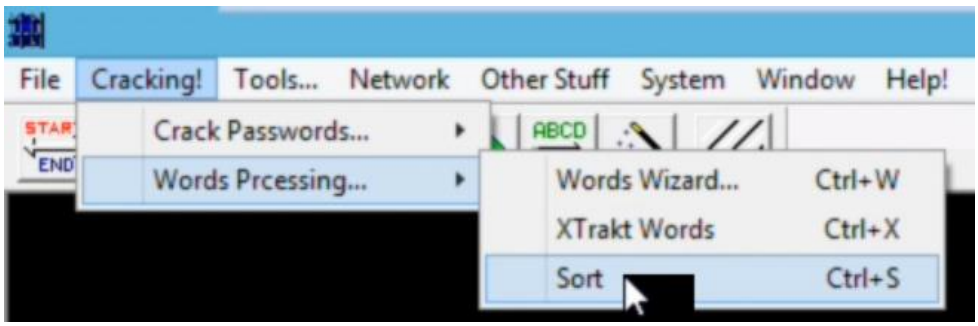


Al abrir el archivo generado, se muestra lo siguiente:



Sin embargo, se aprecia que existen parámetros repetidos, para quitar los parámetros repetidos para efectos de optimizar el análisis ir a HackersUtility, a la opción:

Cracking! > Words Processing > Sort



La entrada, en este caso sería el archivo SecLogA y la salida sería el nuevo archivo .txt a generar.

Al abrir el archivo, se muestran sin repetición todos los nombres de los usuarios que han intervenido en todos los logs.

Importante: Se recomienda comparar la información contenida en el archivo que fue procesado en HackersUtility con la información contenida en el archivo original, para los ejemplos el archivo original es SecLog.txt, ya que, al efectuar dicha comparación, se obtendrá un mejor análisis de la situación en la investigación forense.

Análisis de Logs – Descubrir intentos de ingreso sin contraseña

En esta sección se utilizan los siguientes parámetros de búsqueda:

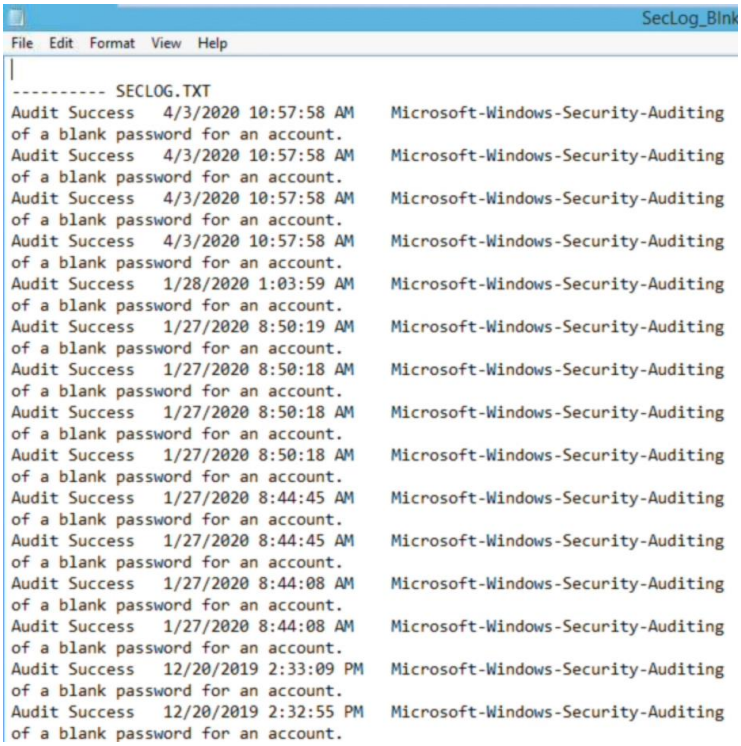
Find /I “Blank Password” Seclog.txt > SecLog_BlnkPass.txt.

```
C:\Users\Administrador\Desktop>find /I "Blank Password" SecLog.txt > SecLog_Blnk
Pass.txt_
```

Lo que hace el comando es buscar el parámetro Blank Password en el archivo SecLog,txt para luego colocar esa información en un nuevo archivo de texto.

/I significa que ignore si las palabras son mayúsculas o minúsculas.

Al abrir el archivo, se mostrará las fechas y horas en que se ha intentado descubrir la existencia de una contraseña en blanco para una cuenta.



Importante: Se recomienda comparar la información contenida en el archivo con la información contenida en el archivo original, para los ejemplos el archivo original es SecLog.txt, ya que, al efectuar dicha comparación, se obtendrá un mejor análisis de la situación en la investigación forense.

Análisis de Logs – Descubrir cambios de dominio y nombre de PC

En esta sección se utilizan los siguientes parámetros de búsqueda:

Find /I “Account Domain” Seclog.txt > SecLog_Domains.txt

```
C:\Users\Administrador\Desktop>find /I "Account Domain" SecLog.txt > SecLog_D.tx
t
```

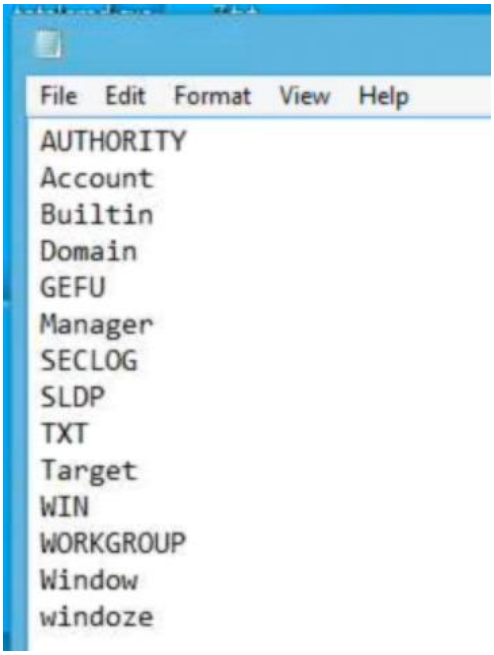
Para ver el contenido de dicho archivo, se ejecuta el siguiente comando:

```
C:\Users\Administrador\Desktop>type SecLog_D.txt
```

Al ver el contenido del archivo, se determina que hay muchas repeticiones:

Por lo cual, se utiliza la herramienta HackersUtility utilizando primero Xtract Words y luego Sort tal como se realizó en la sección 9.1

Una vez que el archivo ya haya sido procesado, se mostrará la siguiente información con lo cual ya será posible proceder con el análisis:



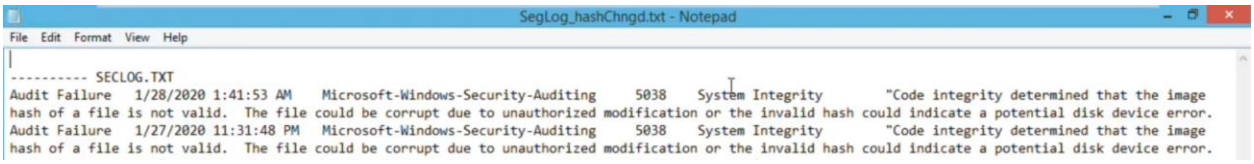
Importante: Se recomienda comparar la información contenida en el archivo que fue procesado en HackersUtility con la información contenida en el archivo original, para los ejemplos el archivo original es SecLog.txt, ya que, al efectuar dicha comparación, se obtendrá un mejor análisis de la situación en la investigación forense.

Análisis de Logs – Descubrir manipulación en aplicaciones

En esta sección se utilizan los siguientes parámetros de búsqueda:

Find /I “hash” Seclog.txt > SecLog_hashChngd.txt

Al abrir el archivo, se muestra la siguiente información:

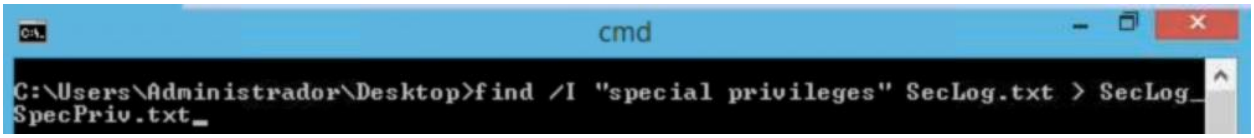


Importante: Se recomienda comparar la información contenida en el archivo con la información contenida en el archivo original, para los ejemplos el archivo original es SecLog.txt, ya que, al efectuar dicha comparación, se obtendrá un mejor análisis de la situación en la investigación forense.

Análisis de Logs - Descubrir elevación de privilegios

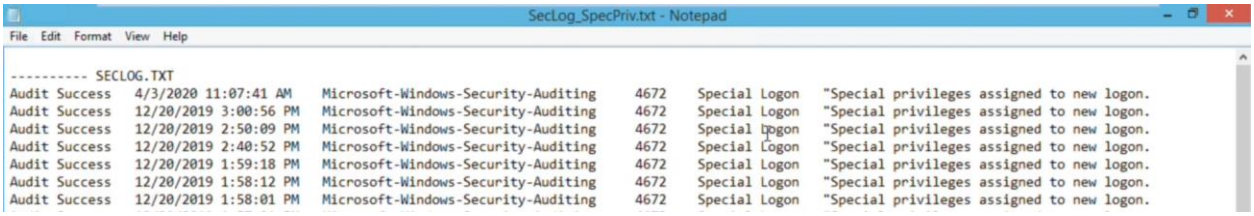
En esta sección se utilizan los siguientes parámetros de búsqueda:

Find /I “special privileges” Seclog.txt > SecLog_SpecPriv.txt



El comando filtrará todos los eventos por donde algún proceso o cuenta de usuario haya escalado privilegios.

Al abrir el archivo, se muestra la siguiente información:



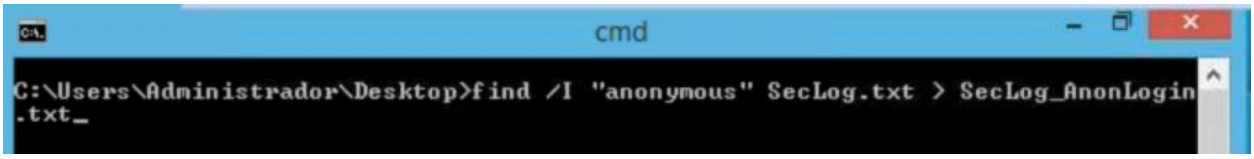
Se recomienda filtrar la hora y fecha en las que se produjo la intrusión.

Importante: Se recomienda comparar la información contenida en el archivo con la información contenida en el archivo original, para los ejemplos el archivo original es SecLog.txt, ya que, al efectuar dicha comparación, se obtendrá un mejor análisis de la situación en la investigación forense.

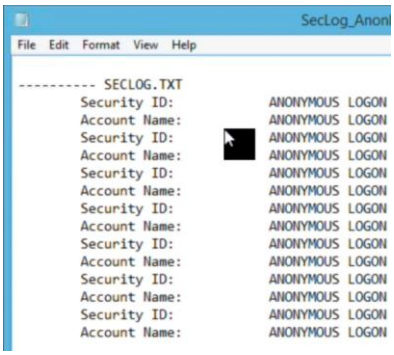
Análisis de Logs – Descubrir ingresos remotos anónimos

En esta sección se utilizan los siguientes parámetros de búsqueda:

Find /I “anonymous” Seclog.txt > SecLog_AnonLogin.txt

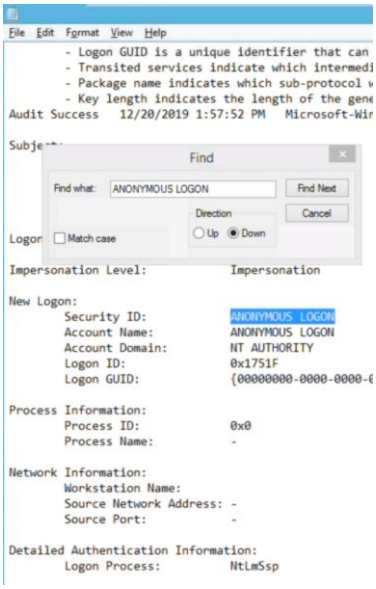


Al abrir el archivo, se muestra la siguiente información:



Importante: Se recomienda comparar la información contenida en el archivo con la información contenida en el archivo original, para los ejemplos el archivo original es SecLog.txt, ya que, al efectuar dicha comparación, se obtendrá un mejor análisis de la situación en la investigación forense.

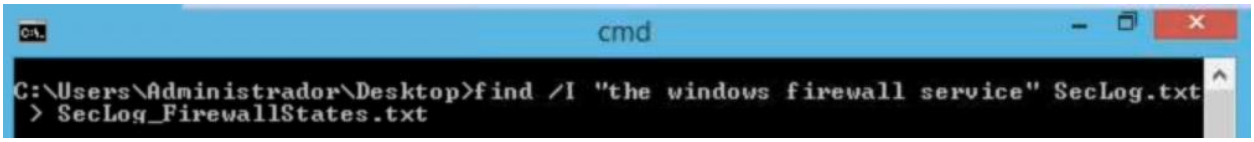
Por ejemplo, al buscar ANONYMOUS LOGON en el archivo original (SecLog.txt) se puede visualizar la siguiente información:



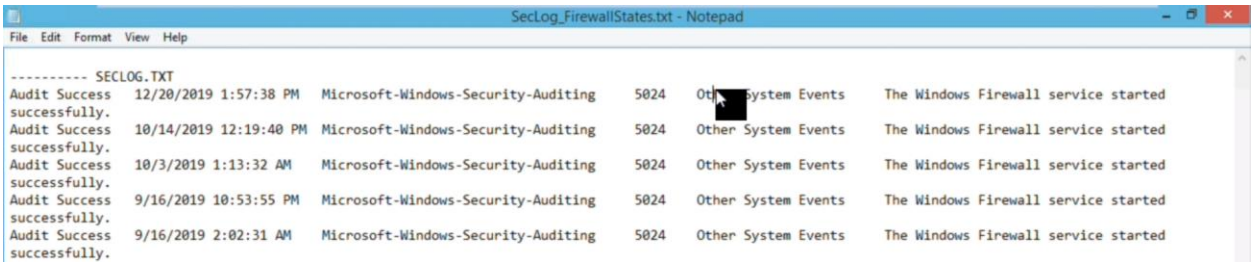
Análisis de Logs – Buscar inicios y detención del Firewall

En esta sección se utilizan los siguientes parámetros de búsqueda:

Find /I “the windows firewall service” Seclog.txt > SecLog_FirewallStates.txt



Al abrir el archivo, se muestra la siguiente información:



Importante: Se recomienda comparar la información contenida en el archivo con la información contenida en el archivo original, para los ejemplos el archivo original es SecLog.txt, ya que, al efectuar dicha comparación, se obtendrá un mejor análisis de la situación en la investigación forense.

Guía 4: Técnicas de Recuperación de Información

Proceso

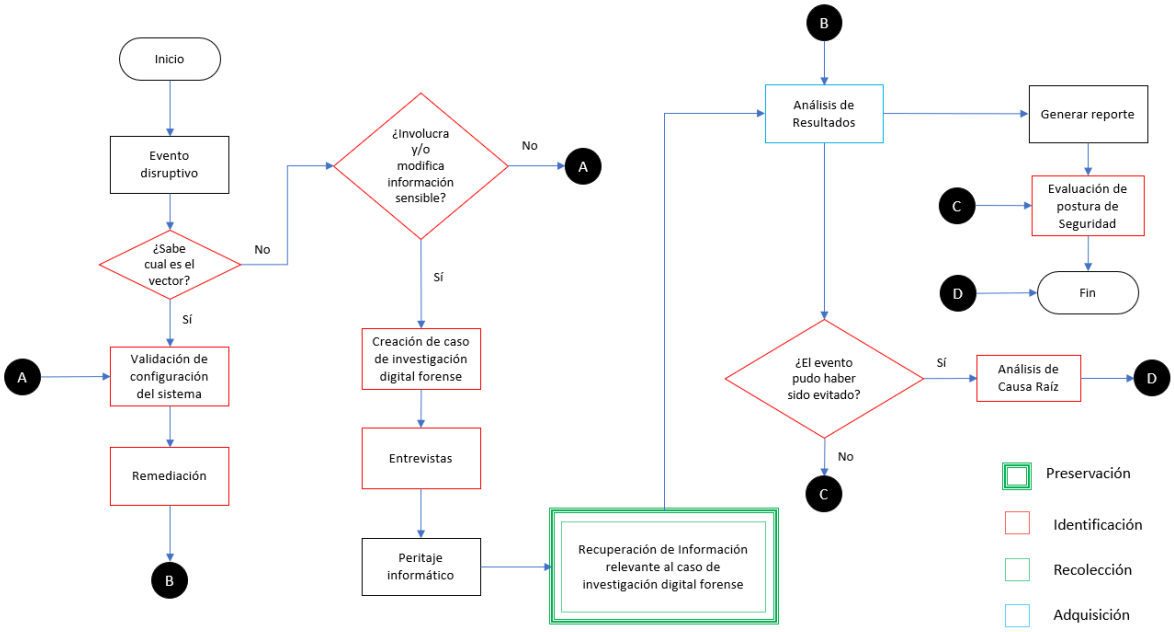


Figura 1: Diagrama del proceso

Detalle

Paso	Propósito	Técnica	Descripción	Herramientas
Evento Disruptivo	Evento producido de forma maliciosa con el objetivo de obtener información sensible y/o dañar el honor de el objetivo	Ingeniería social, hacking no ético, etc.	Vulneración de equipos informáticos, cuentas privilegiadas, etc.	Software y hardware especializado.
Creación de caso de investigación digital forense	Da inicio a la investigación en torno al evento disruptivo.	Recopilación de información. Análisis sistemático.	Investigación de los actores involucrados en el evento disruptivo	Software y hardware especializado.
Entrevistas	Recopilación de información testimonial.	Entrevistas orales sustentadas por grabaciones y otros factores.	Recopilación de información que podría dar indicios acerca de la causa raíz del evento.	Grabadoras, cámaras, etc.
Peritaje Informático	Recopilación de información digital.	Herramientas de hardware y software.	Recopilación de información digital que podría hacer posible la reconstrucción de los hechos.	Software y hardware especializado.
Análisis de resultados	Comprensión y reconstrucción del evento disruptivo a través de le videncia recabada.	Ciencias aplicadas de informática forense.	Formulación de hipótesis y validación de evidencias técnicas recabadas.	Software y hardware especializado.
Elaboración de reporte	Comunicar los hallazgos de manera sistemática haciendo énfasis en aquellos puntos que brinden pistas de lo ocurrido.	Explicación a nivel ténico y ejecutivo de lo realizado durante la investigación.	Documentación técnica en la cual se verá plasmada los resultados de la investigación.	Ofimática.
Evaluación de postura de seguridad	Determinar si los mecanismos de seguridad adoptados o la falta de estos fueron decisivos en la generación del evento.	Auditoría, pruebas de hardware y software, replicación de eventos, etc.	Conjunto de pruebas técnicas y testimoniales que determinarán la eficacia o resiliencia ante un evento disruptivo.	Software y hardware especializado.
Identificación y análisis de causa raíz	Determinar el vector con el objetivo de establecer mecanismos que puedan anular su efecto ante el escenario de un evento igual o similar.	Reconocimiento	Identificación de la causa raíz, así como del impacto ocasionado.	Software y hardware especializado.

Tabla 1: Detalles del proceso

Aspectos relacionados

Proceso	Caso de empleo
Eliminación de cuentas no utilizadas.	Eliminar las cuentas asociadas a personas que ya no estén vinculadas a la organización, realización de pruebas.
Validación de Información	Cotejar la información provista en correos, chats, etc con la información oficial empresarial
Sitios confiables	Navegar por sitios que cuenten con mecanismo de seguridad, así como evitar descargar archivos, programas ejecutabes de sitios sospechosos.

Tabla 2: Aspectos relacionados

Ejemplo

Autopsy: Guía completa para Análisis Forense (Windows)

Autopsy es una herramienta de código abierto que se utiliza para realizar operaciones forenses en la imagen de disco de las evidencias.

Para el ejemplo, se muestra la investigación forense que se realiza sobre la imagen de disco.

Los resultados obtenidos en este ejemplo proveen líneas base para investigar y localizar información relevante. Autopsy es utilizada por las fuerzas del orden, la policía local y también se puede utilizar en las empresas para investigar las pruebas encontradas en un delito informático. Adicionalmente, se puede utilizar para recuperar información que ha sido borrada.

Autopsy puede ser descargada del siguiente link:https://www.autopsy.com/download/

Creación de un nuevo caso

Se debe ejecutar la herramienta Autopsy en el sistema operativo Windows y elegir la opción "`New Case`" ("*Nuevo Caso*") para crear un nuevo caso.

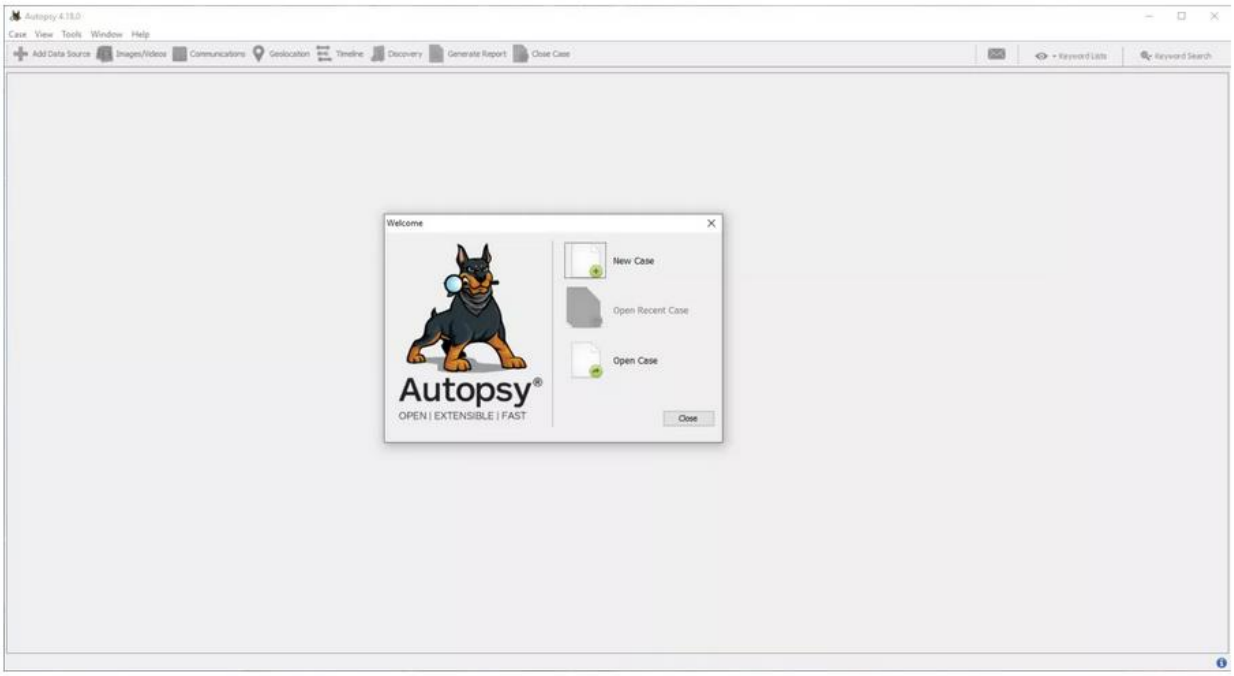


Figura 1: Crear nuevo caso en Autopsy.

A continuación, se debe rellenar toda la información necesaria del caso, como el nombre de este, y se debe elegir un directorio base para guardar todos los datos del caso en un solo lugar.

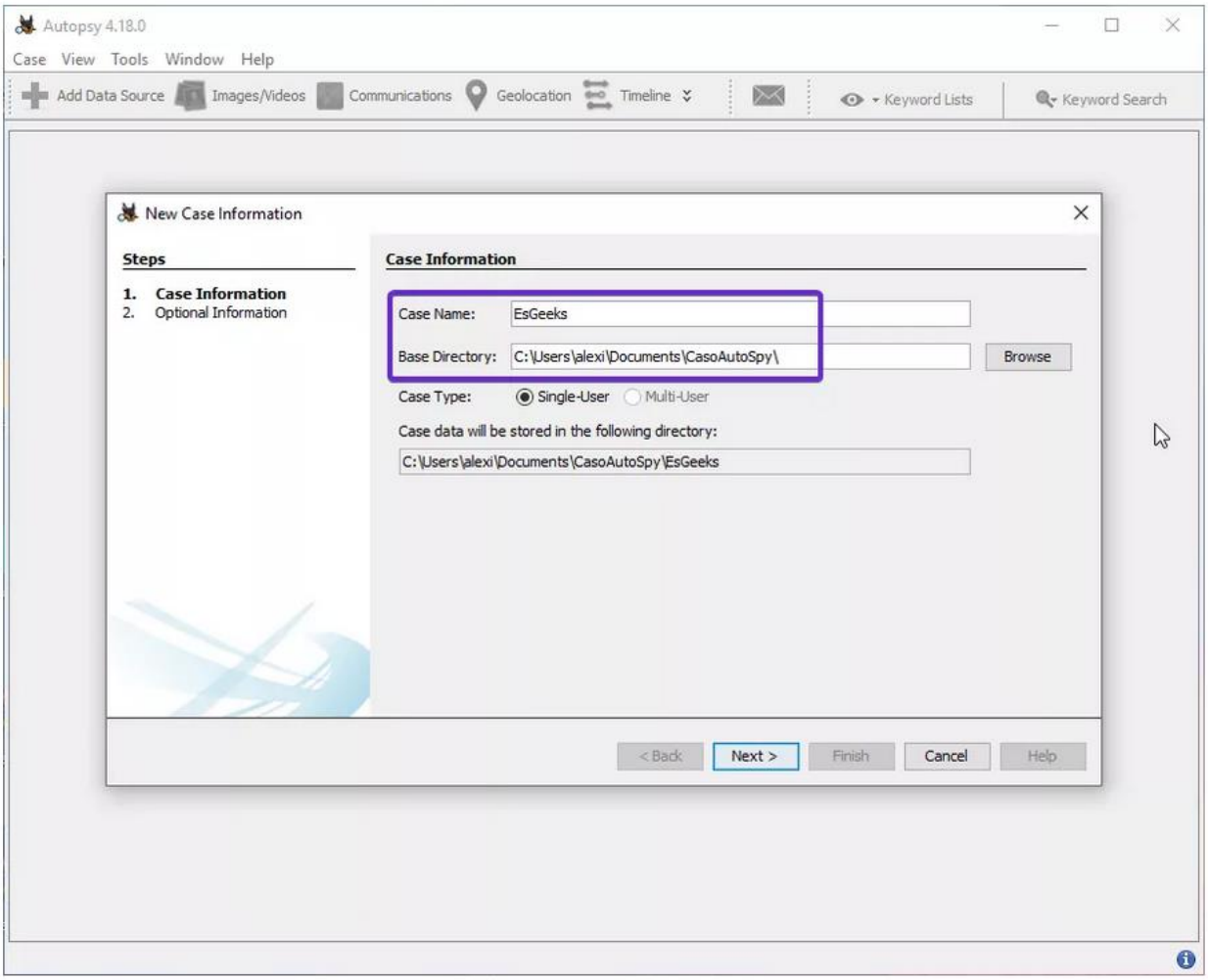


Figura 2: Información del caso.

También es posible añadir información adicional opcional sobre el caso si es necesario.

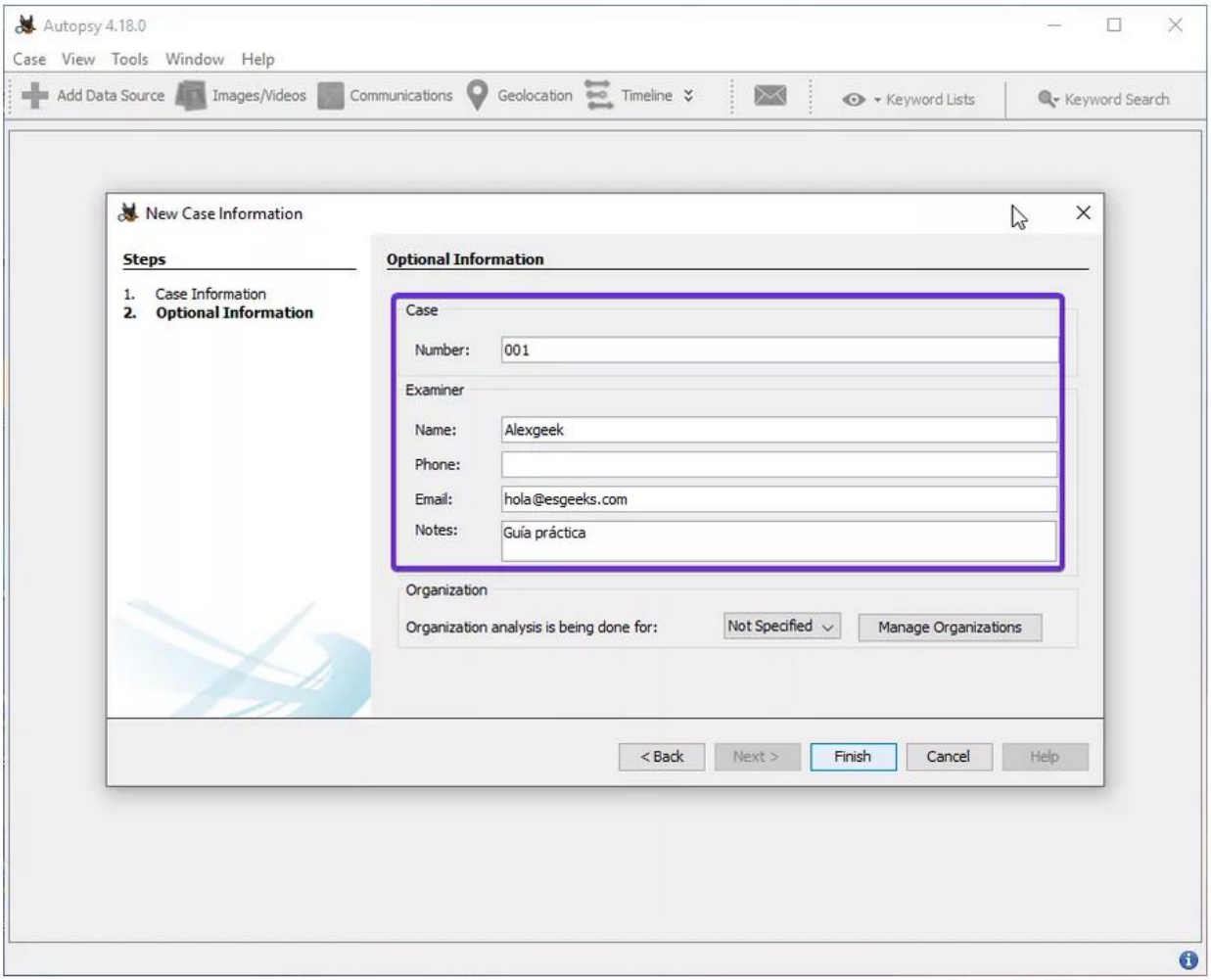


Figura 3: Información opcional adicional.

Es necesario elegir el tipo de fuente de datos. Hay varios tipos para elegir.

- **Disk Image or VM file**: Esto incluye el archivo de imagen que puede ser una copia exacta de un disco duro, una tarjeta multimedia o incluso una máquina virtual.
- **Local Disk**: Esta opción incluye dispositivos como discos duros, pen drives, tarjetas de memoria, etc.
- **Logical Files**: Incluye la imagen de cualquier carpeta o archivo local.
- **Unallocated Space Image File**: Incluyen archivos que no contienen ningún sistema de archivos y se ejecutan con la ayuda del módulo *Ingest*.
- **Autopsy Logical Imager Results**: Incluyen la fuente de datos de la ejecución del generador de imágenes lógicas.
- **XRY Text Export**: Incluyen la fuente de datos de la exportación de archivos de texto desde XRY.

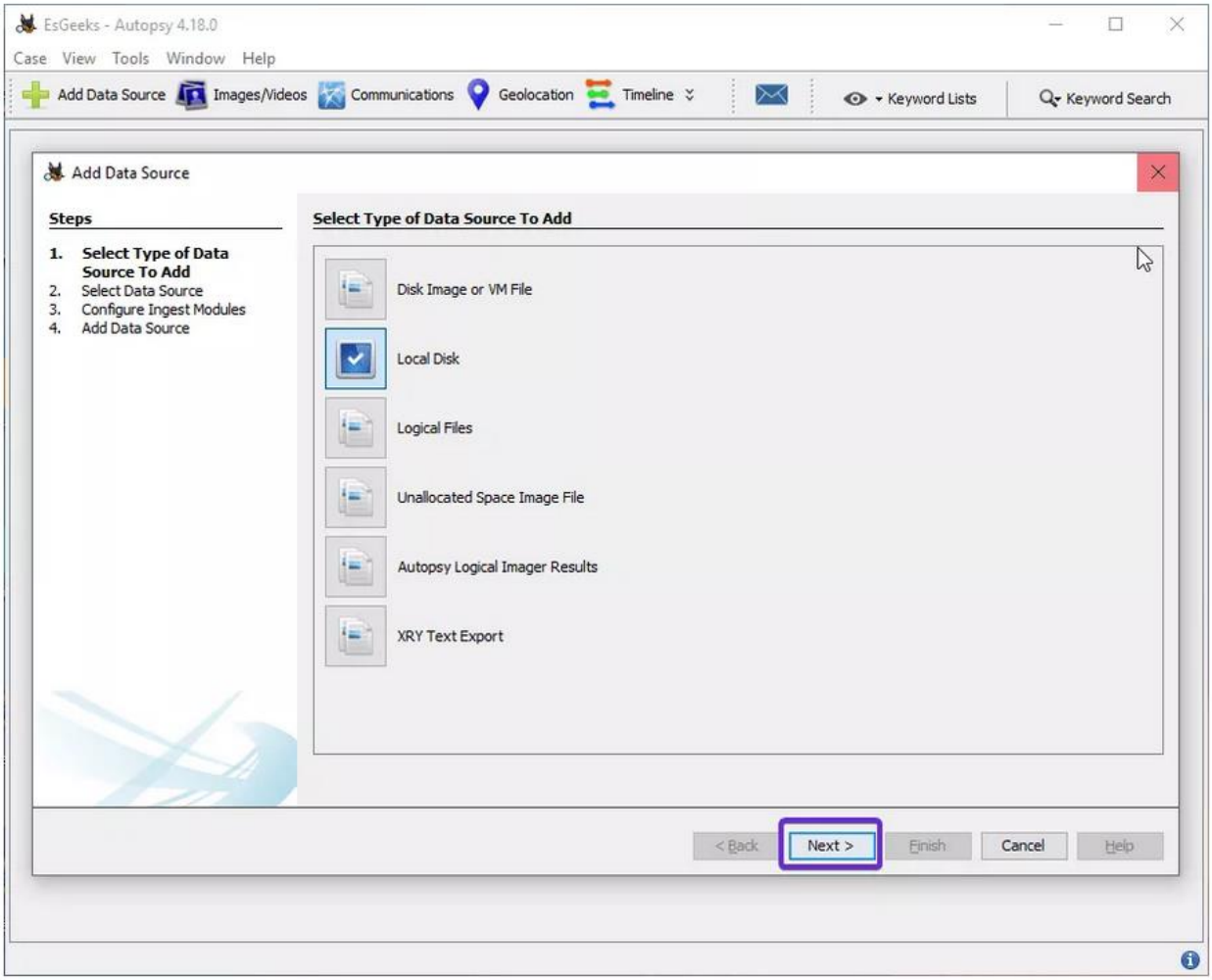


Figura 4: Tipos de fuentes de datos.

Debe de añadirse la fuente de datos. Para el ejemplo, se elegirá una fuente externa dispositivo USB), así que se añadirá la ubicación de ese dispositivo.

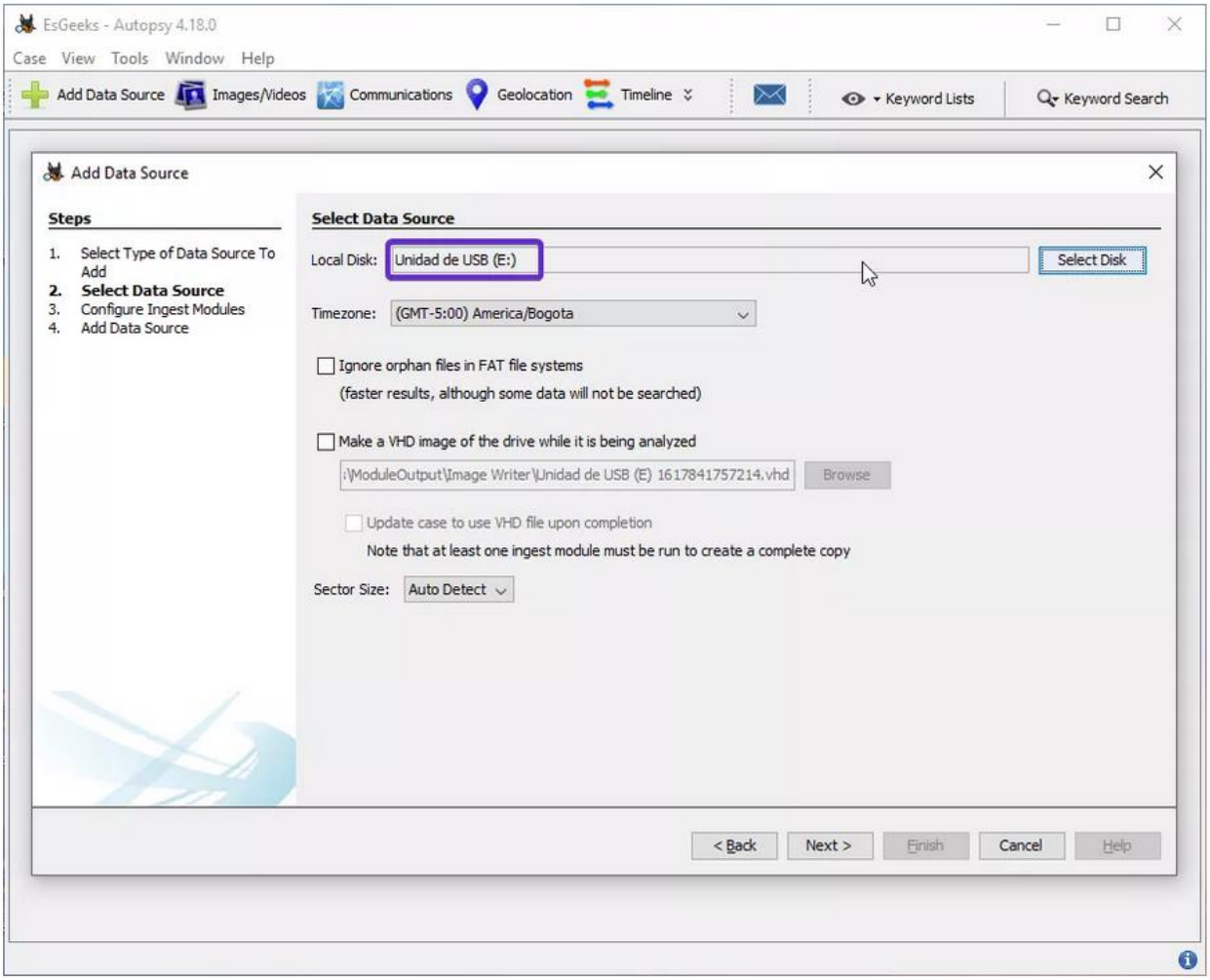


Figura 5: Analizar unidad USB.

A continuación, se solicitará la configuración del módulo **Ingest**.

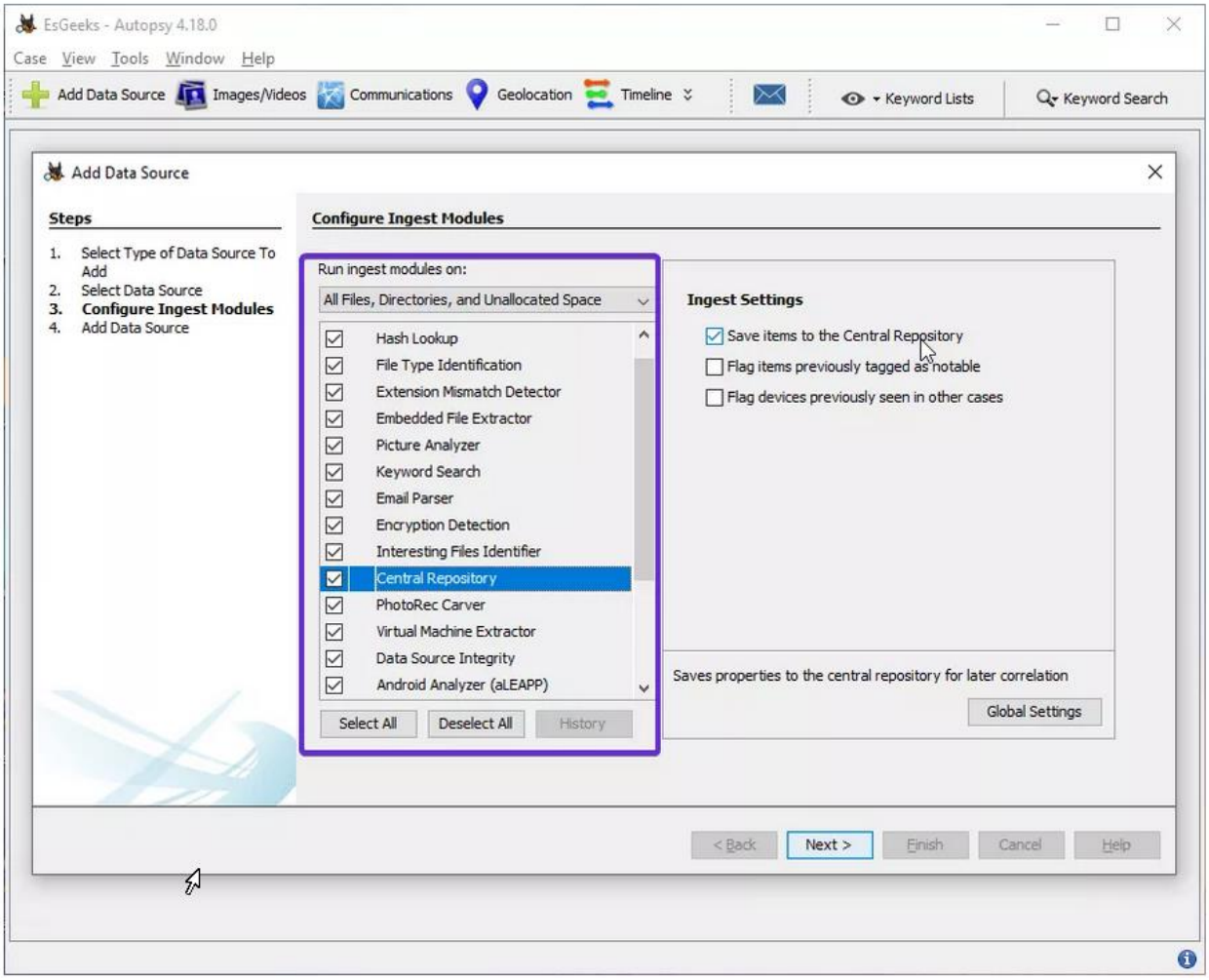


Figura 6: Configuración módulo Ingest.

El contenido del módulo **Ingest** se encuentra en la siguiente tabla:

Módulo Ingest	Descripción
Recent Activity	Se utiliza para descubrir las operaciones recientes que se realizaron en el disco, como los archivos que se vieron recientemente.
Hash Lookup	Se utiliza para identificar un archivo concreto mediante su valor hash.
File Type Identification	Se utiliza para identificar los archivos basándose en sus firmas internas y no sólo en las extensiones de los archivos.
Extension Mismatch Detector	Se utiliza para identificar los archivos cuyas extensiones han sido manipuladas o han sido modificadas para ocultar las pruebas.
Embedded File Extractor	Se utiliza para extraer archivos incrustados como .zip, .rar, etc. y utilizar esos archivos para su análisis.
Keyword Search	Se utiliza para buscar una palabra clave concreta o un patrón en el archivo de imagen.
Email Parser	Se utiliza para extraer información de los archivos de correo electrónico si el disco contiene alguna información de la base de datos de correo electrónico.
Encryption Detection	Esto ayuda a detectar e identificar los archivos encriptados protegidos por contraseña.
Interesting File Identifier	Mediante esta función, el examinador recibe una notificación cuando los resultados corresponden al conjunto de reglas definidas para identificar un tipo de archivo concreto.
Central Repository	Guarda las propiedades en el repositorio central para su posterior correlación.
PhotoRec Carver	Esto ayuda al examinador a recuperar archivos, fotos, etc. del espacio no asignado en el disco de imagen.
Virtual Machine Extractor	Ayuda a extraer y analizar si se encuentra alguna máquina virtual en la imagen de disco.
Data Source Integrity	Ayuda a calcular el valor hash y a almacenarlo en la base de datos.

Tabla 3: Contenido de módulo Ingest.

Detalles del Módulo Ingest

La información de la fuente de datos (***Data Source***) muestra los metadatos básicos.

Su análisis detallado se muestra en la parte inferior. Se puede extraer uno tras otro.

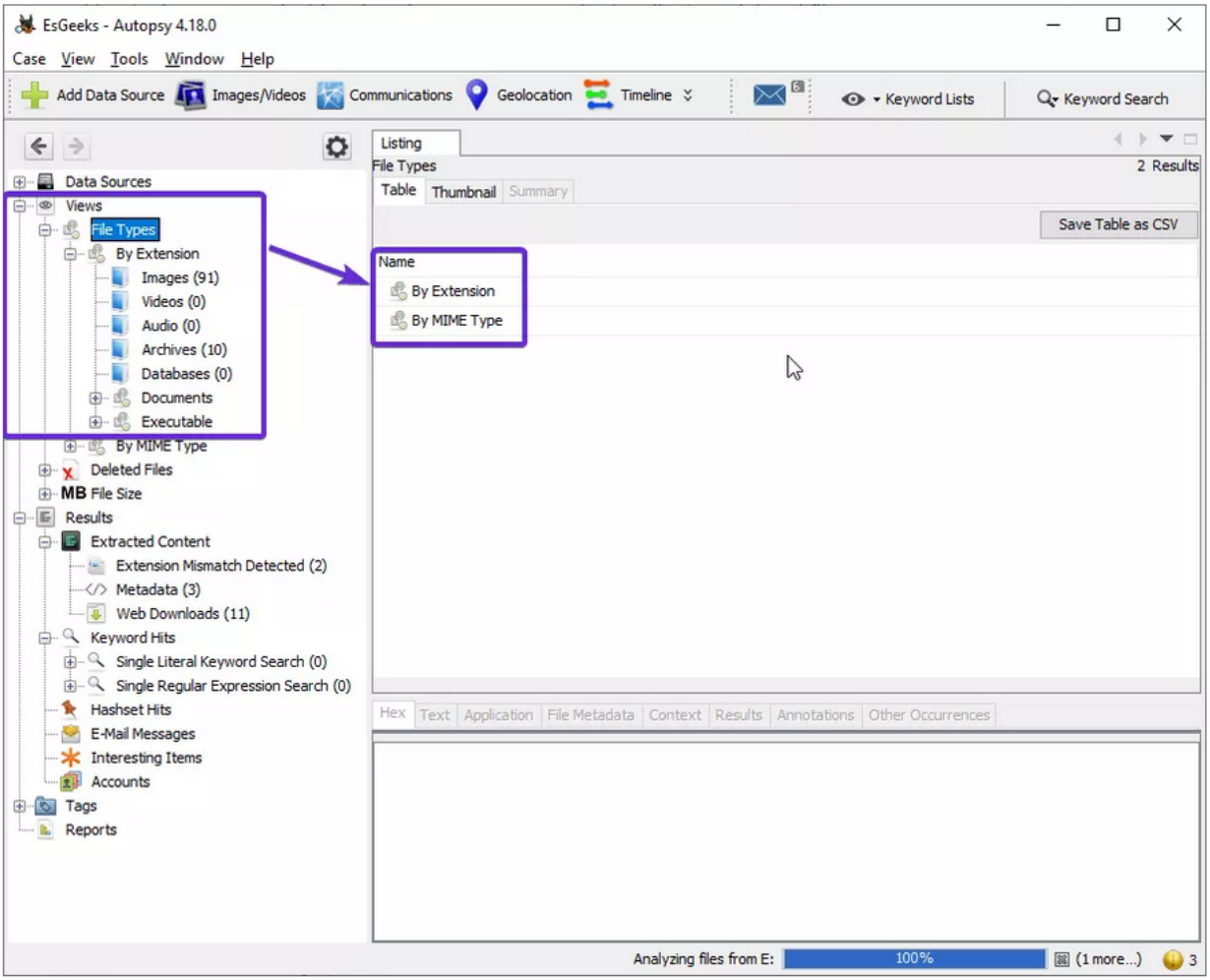


Figura 7: Información de Data Source.

Vistas

File Type (Tipo de archivo): Se puede clasificar en forma de extensión de archivo o tipo MIME.

Proporciona información sobre las extensiones de archivo que suelen ser utilizadas por el sistema operativo, mientras que los tipos MIME son utilizados por el navegador para decidir qué datos representar. También muestra los archivos eliminados.

Importante: Estos tipos de archivo se pueden clasificar en función de la extensión (*Extension*), los documentos (*Documents*) y los ejecutables (*Executables*).

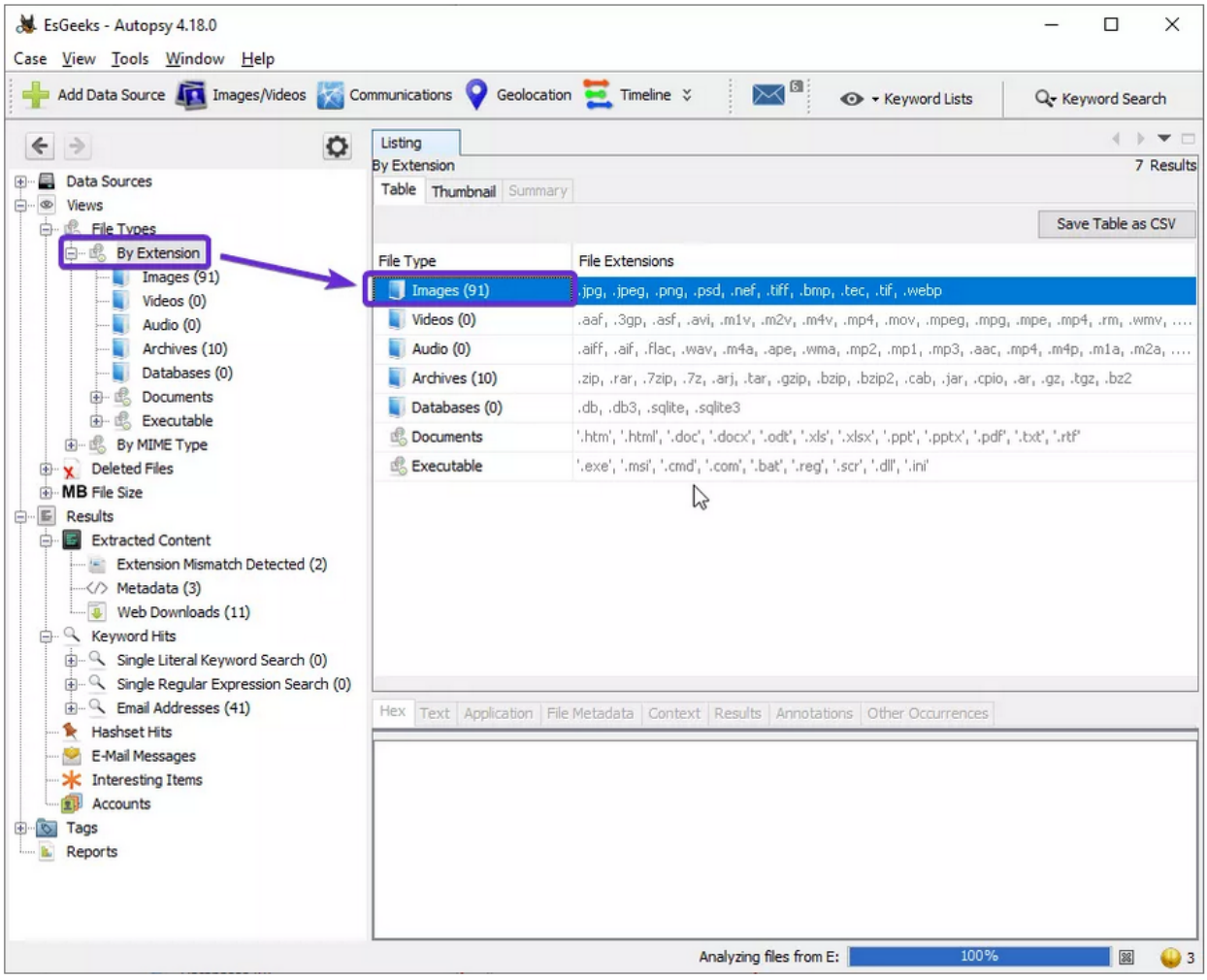


Figura 8: Sección File Types.

Por extensión

En la categoría Tipos de archivo por extensión (*By Extension*), se puede observar que se ha subdividido en tipos de archivo como imágenes, vídeo, audio, archivos, bases de datos, etc.

Al hacer clic en las imágenes, se puede explorar las imágenes que se han recuperado.

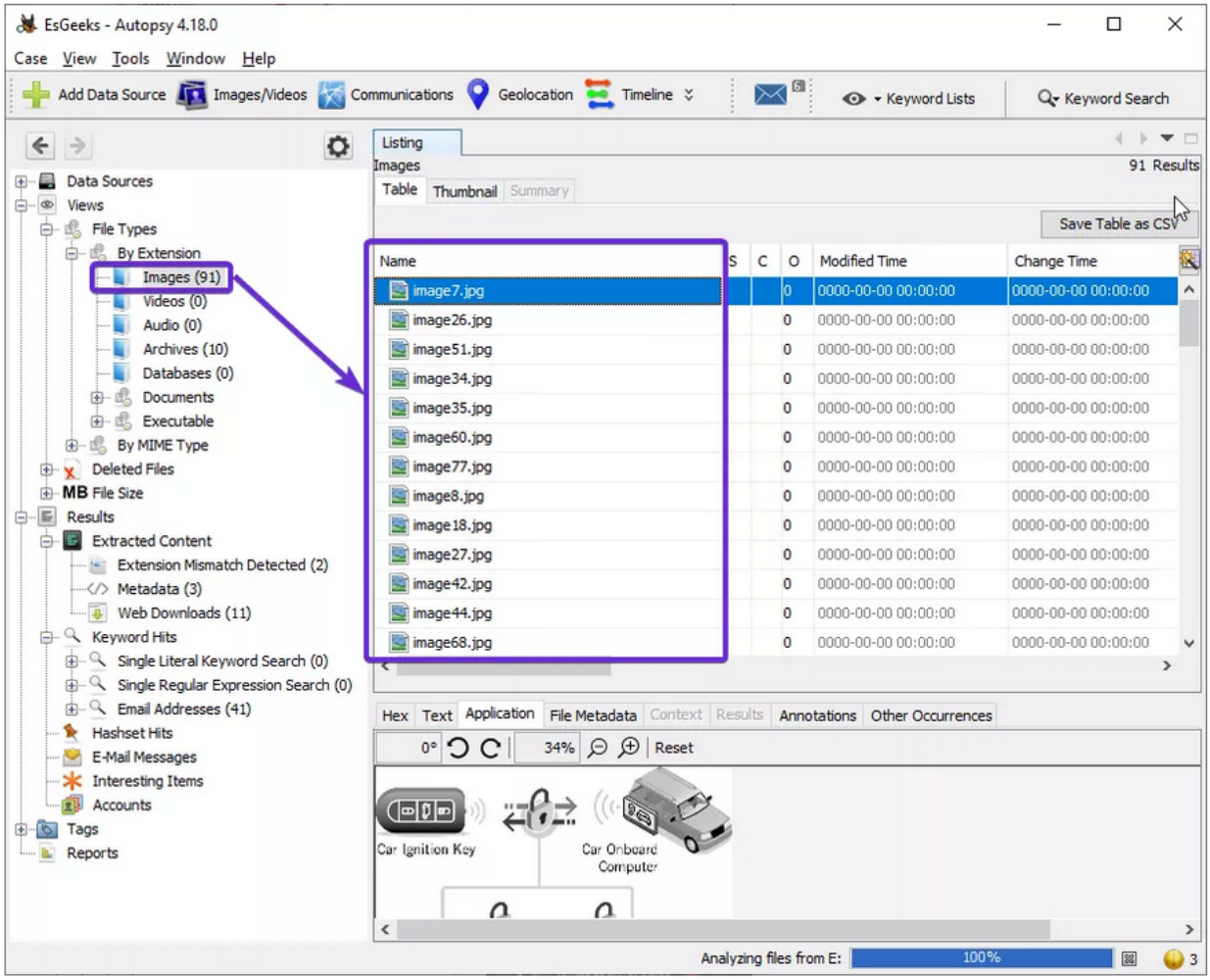


Figura 9: Filtros By Extension.

También es posible visualizar la miniatura de las imágenes.

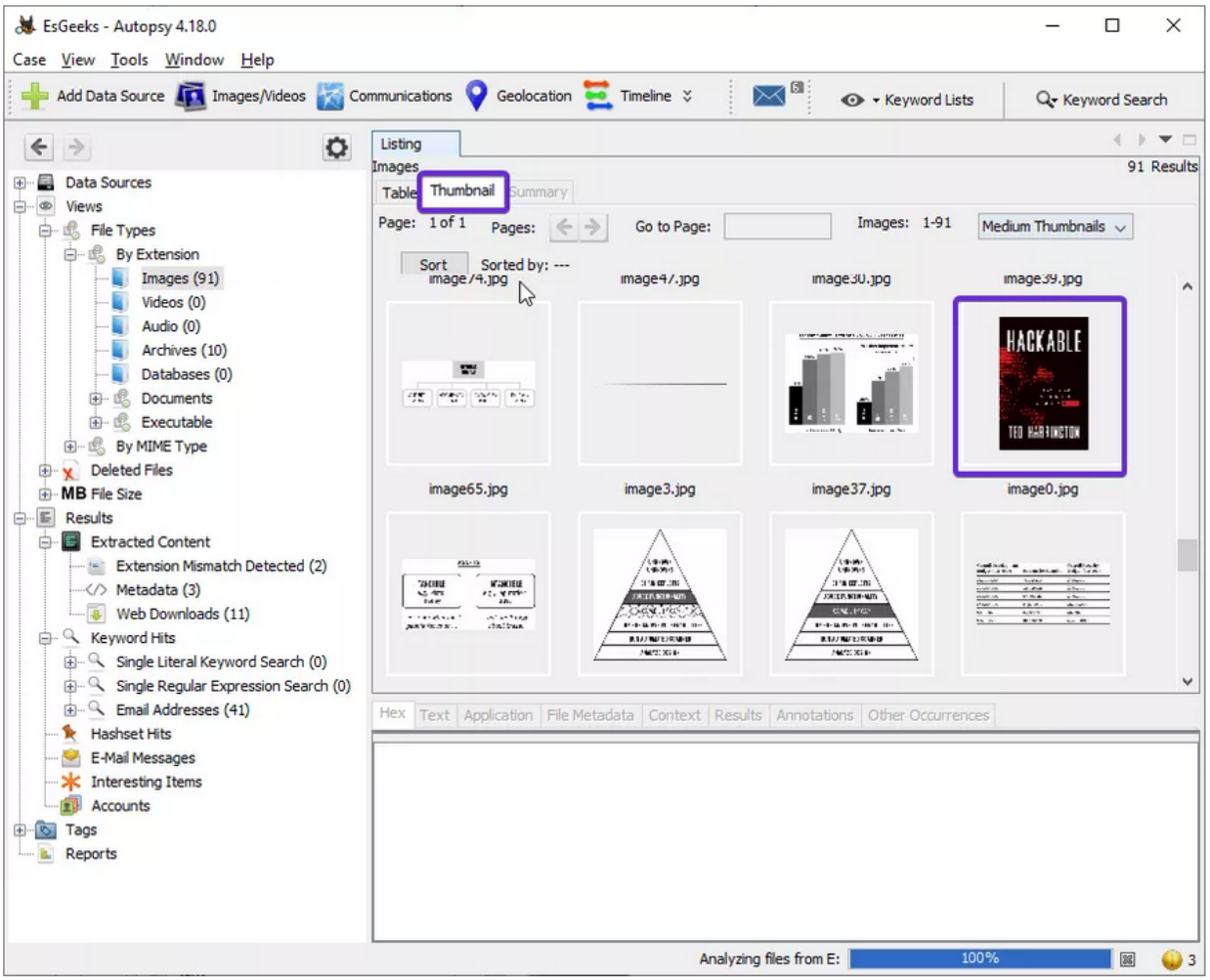


Figura 10: Ver miniatura de imágenes.

En la miniatura, se pueden ver los metadatos del archivo y los detalles de la imagen.

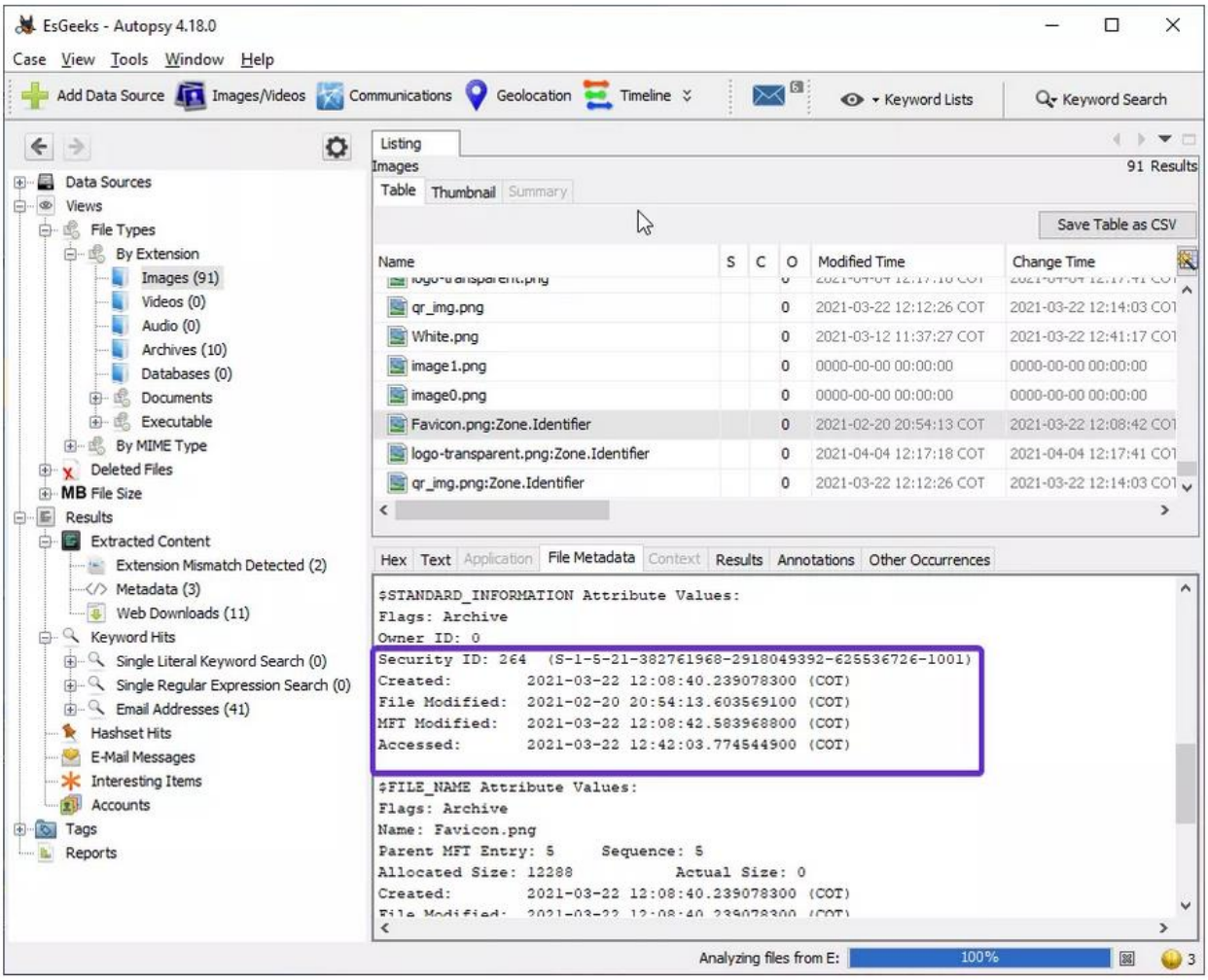


Figura 11: Metadatos y detalles de Imagen.

Aquí también es posible visualizar algunos archivos del tipo "*Archives*" que se han recuperado.

Se pueden extraer estos archivos del sistema y además es posible visualizarlos utilizando varios programas.

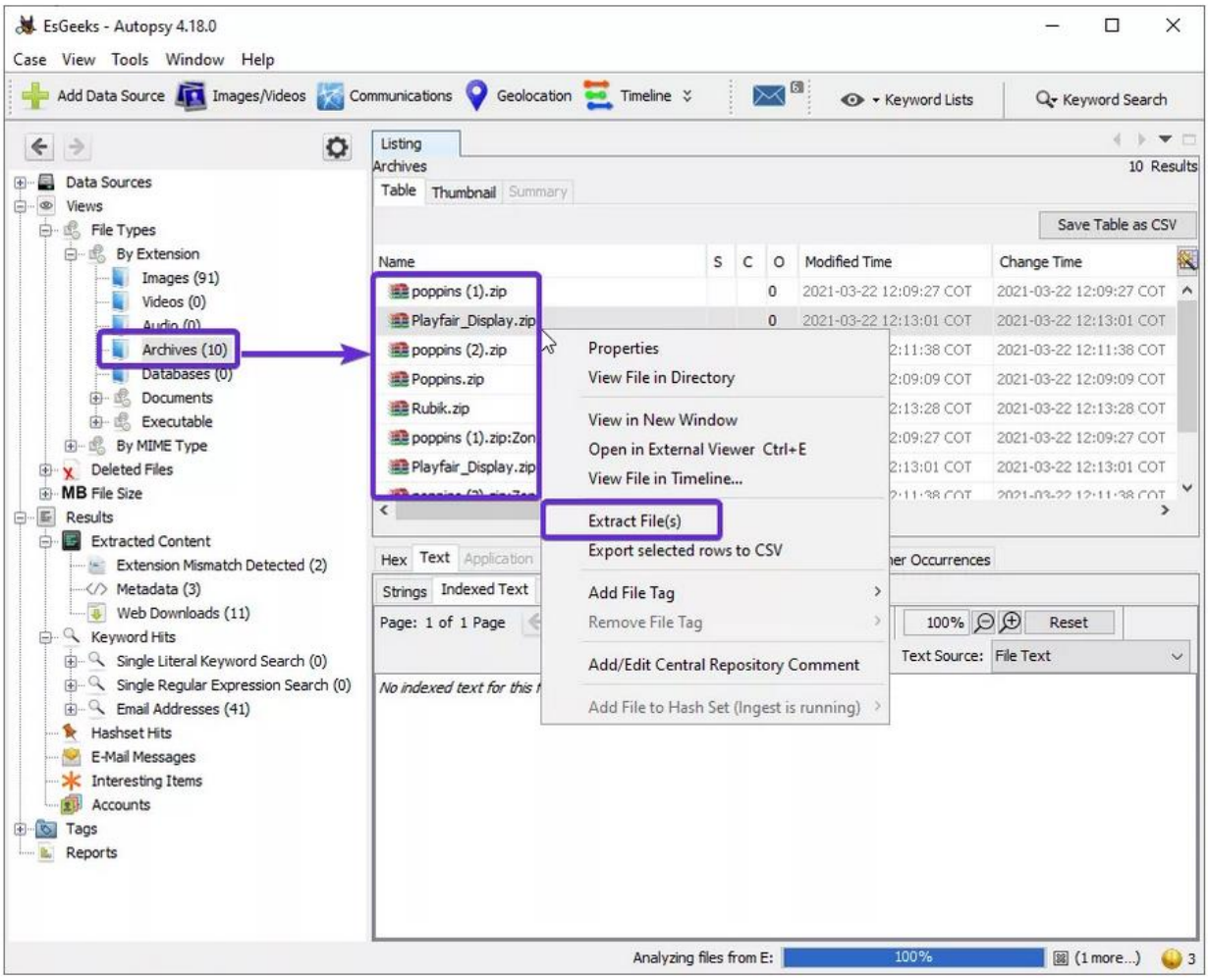


Figura 12: Extraer archivos recuperados.

Documentos

Los documentos se clasifican en 5 tipos: HTML, Office, PDF, Texto sin formato (Plain Text) y Texto enriquecido (Rich Text).

Al explorar la opción de documentos, se pueden observar todos los documentos PDF presentes, puedes hacer clic en los importantes para verlos.

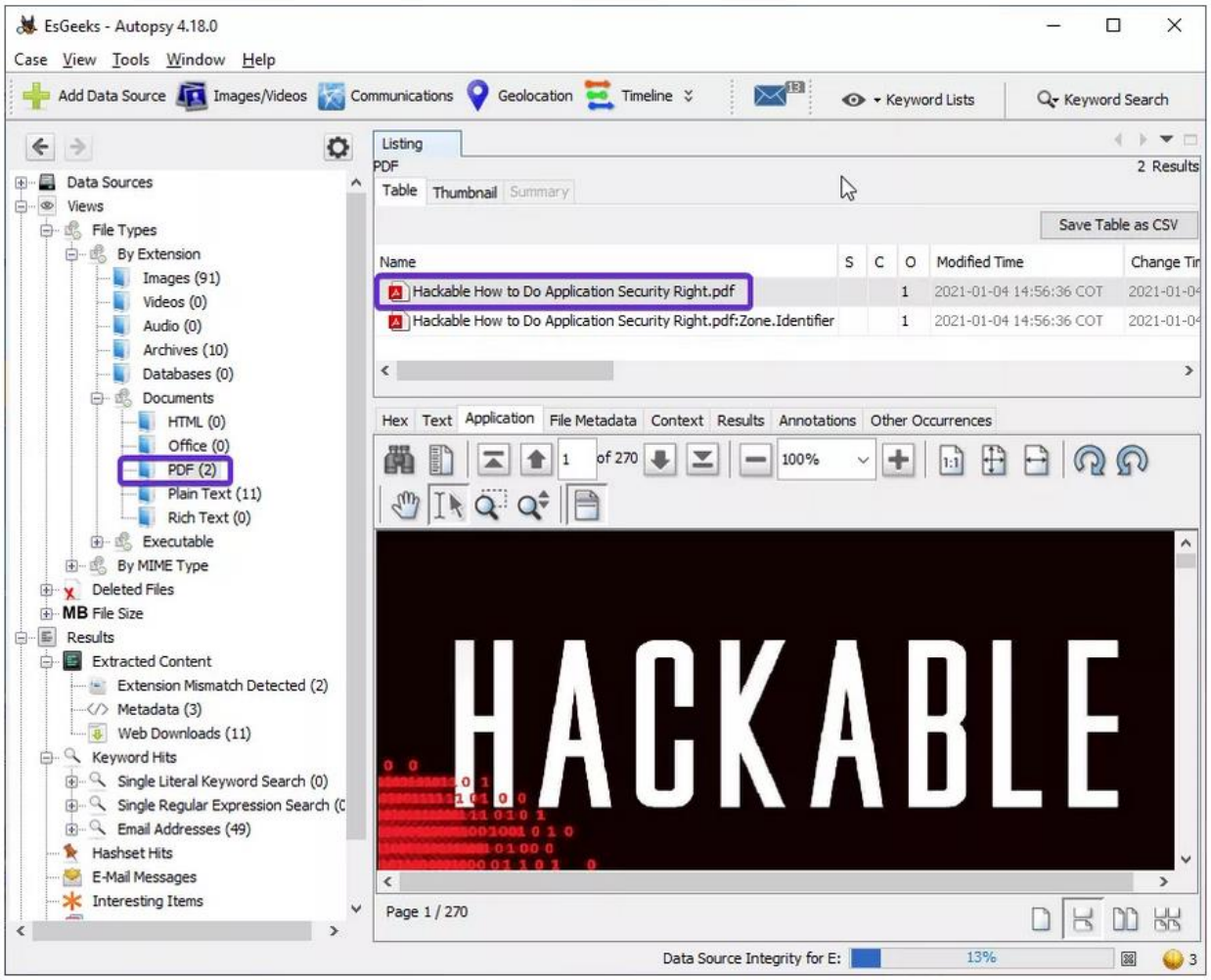


Figura 13: Tipos de documentos.

Del mismo modo, es posible visualizar los diversos archivos de texto plano, adicionalmente, también es posible recuperar los archivos de texto plano eliminados.

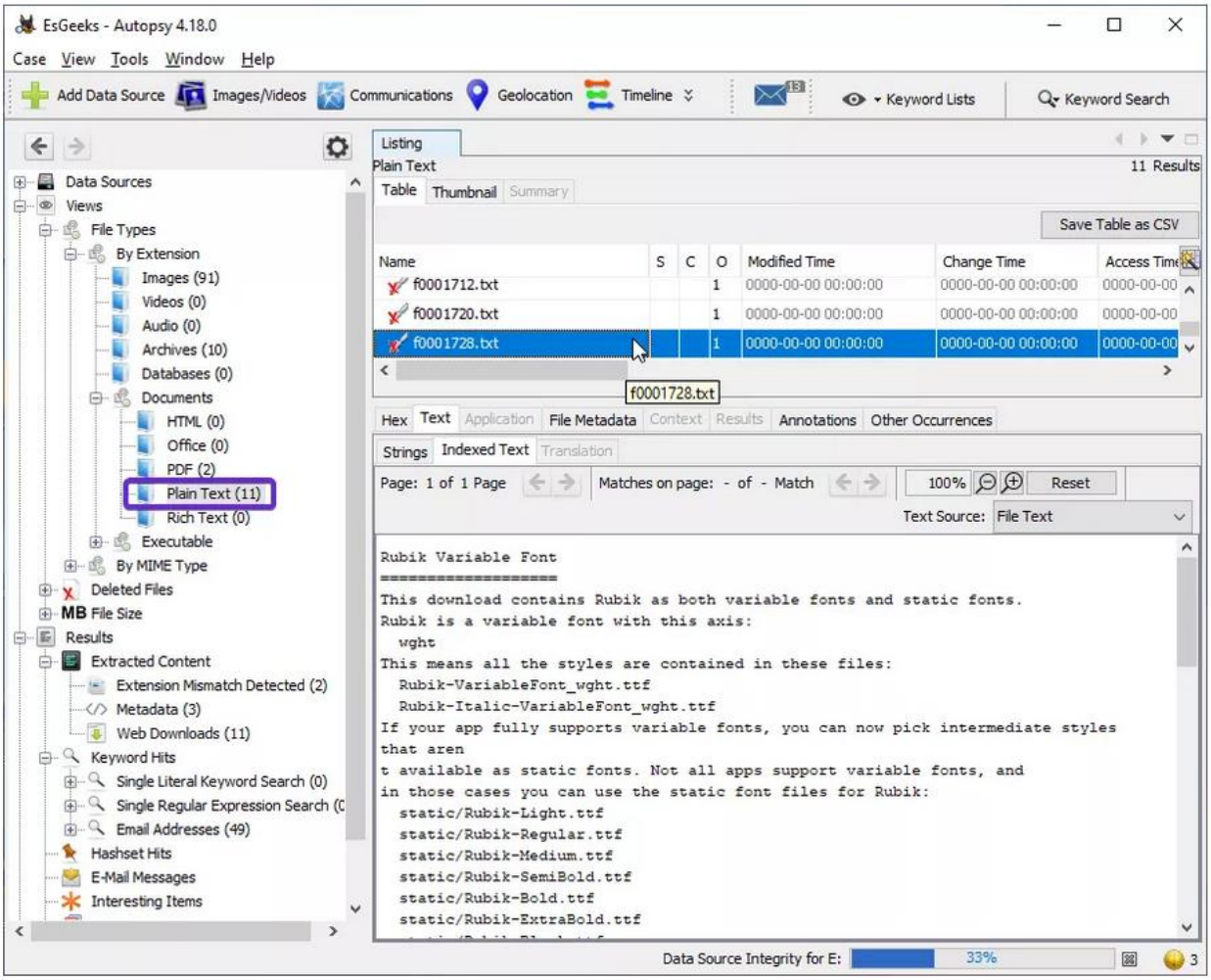


Figura 14: Recuperar archivos en texto plano.

Ejecutables

Estos tipos de archivos se subdividen en .exe, .dll, .bat, .cmd y .com.

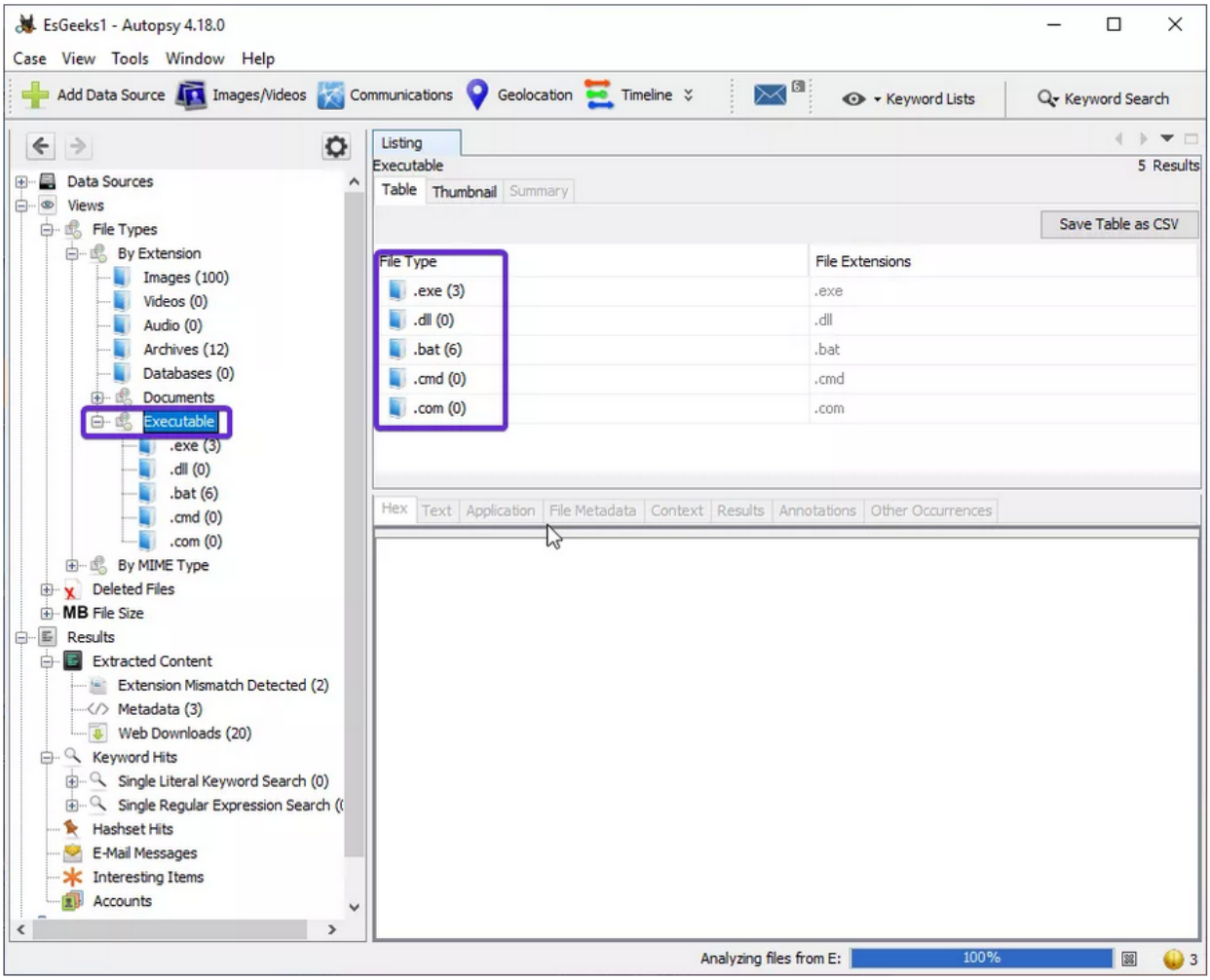


Figura 15: Tipos de archivos ejecutables.

Por tipo MIME

En este tipo de categoría, hay cuatro subcategorías como aplicación, audio, imagen y texto. Estas se dividen a su vez en más secciones y tipos de archivo.

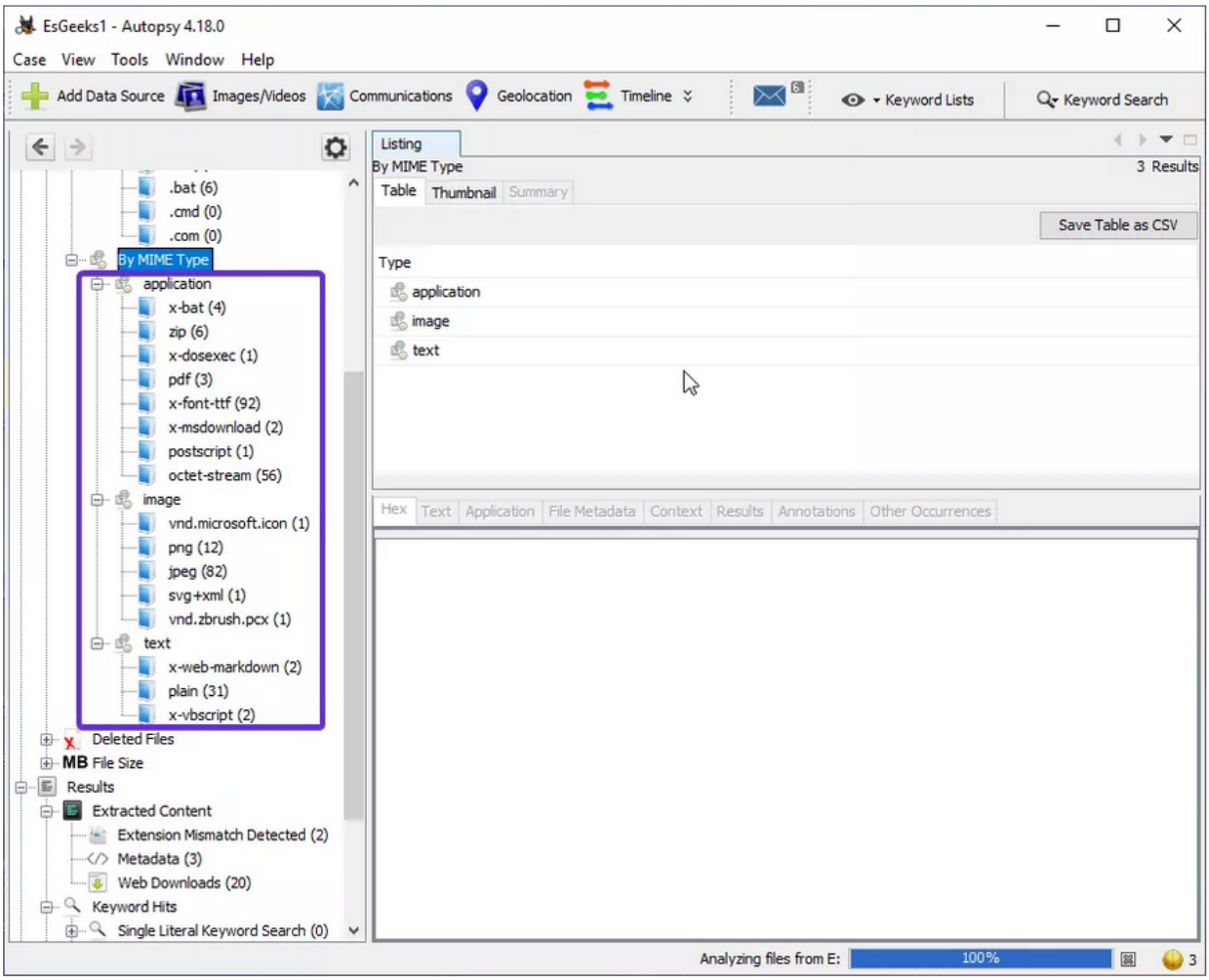


Figura 16: Tipos de archivos MIME.

Archivos eliminados

(Deleted Files) Muestra información sobre el archivo eliminado que luego se puede recuperar.

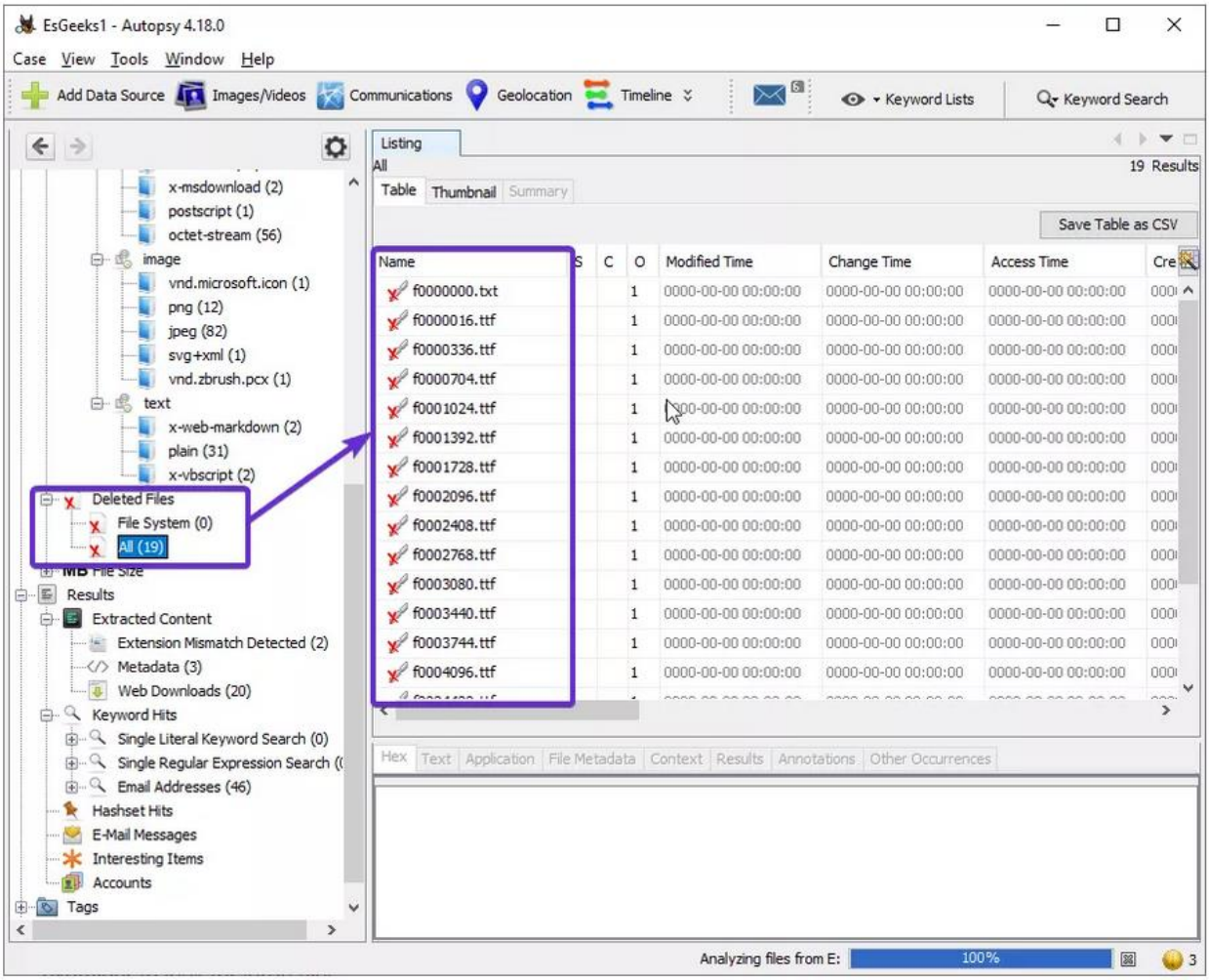


Figura 17: Recuperar archivos eliminados.

Archivos de tamaño MB

(MB Size Files) En esta sección, los archivos se clasifican en función de su tamaño, a partir de 50 MB.

Esto permite al examinador buscar archivos de gran tamaño.

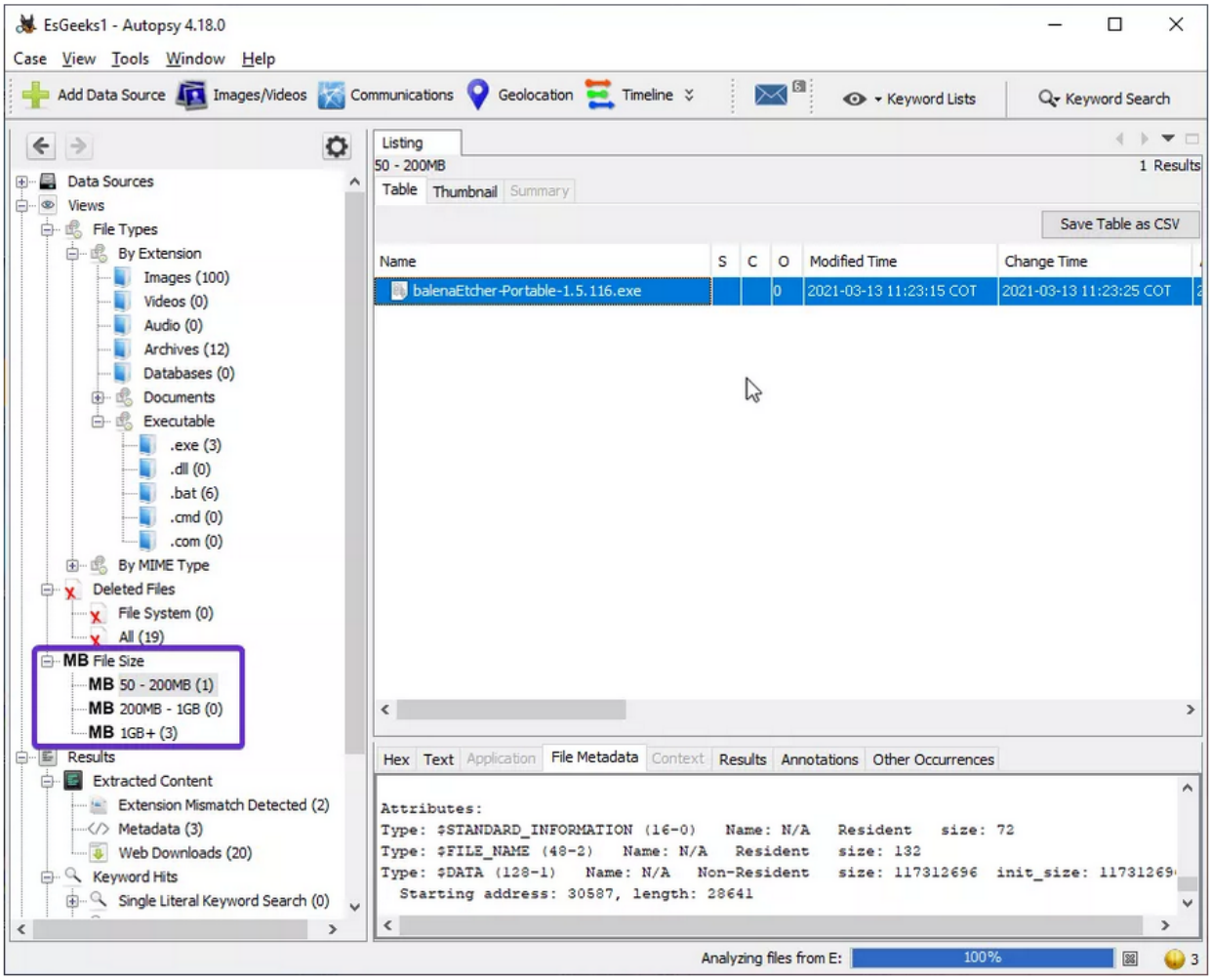


Figura 18: Clasificar archivos por tamaño.

Resultados

En esta sección, se obtiene la información sobre el contenido que fue extraído.

Contenido extraído

(Extracted Content) Todo el contenido que fue extraído es segregado en detalle.

En esta sección es posible encontrar metadatos, papelera de reciclaje y descargas web.

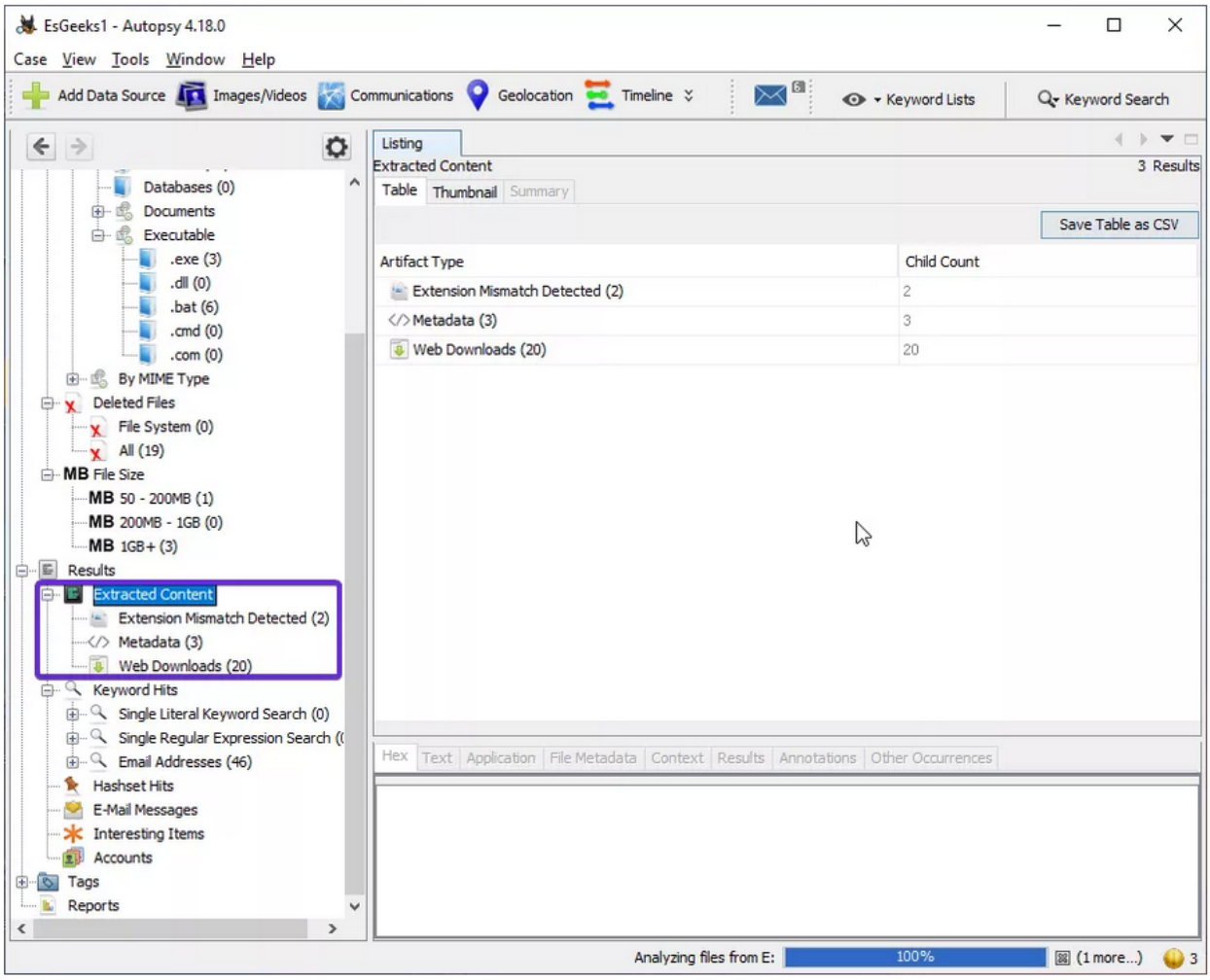


Figura 19: Sección Extracted Content.

Metadatos (Metadata): Es posible ver toda la información sobre los archivos como la fecha de creación, de modificación, el propietario del archivo, etc.

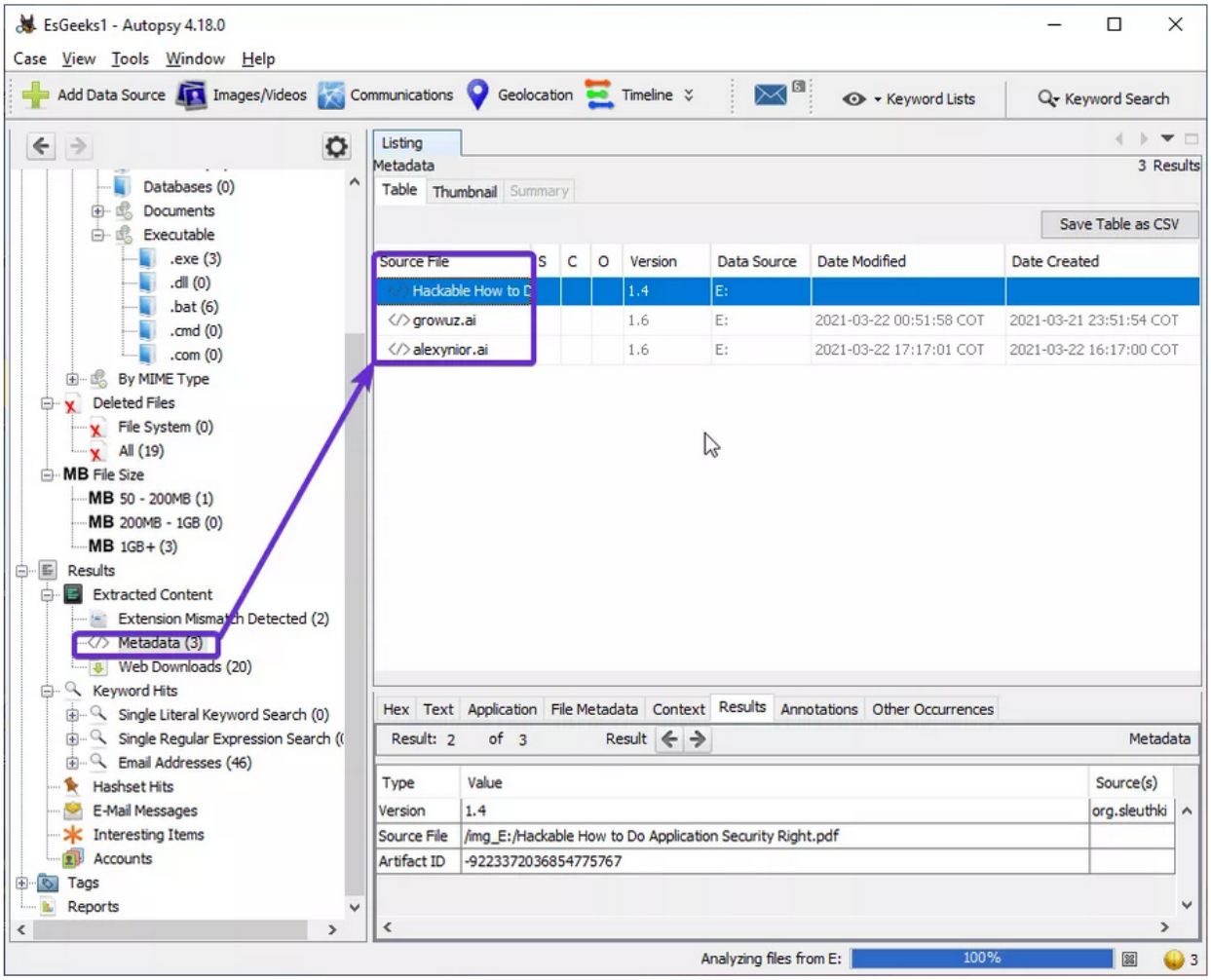


Figura 20: Sección Metadata.

Descargas Web (Web Downloads): Aquí se pueden ver los archivos que fueron descargados de internet.

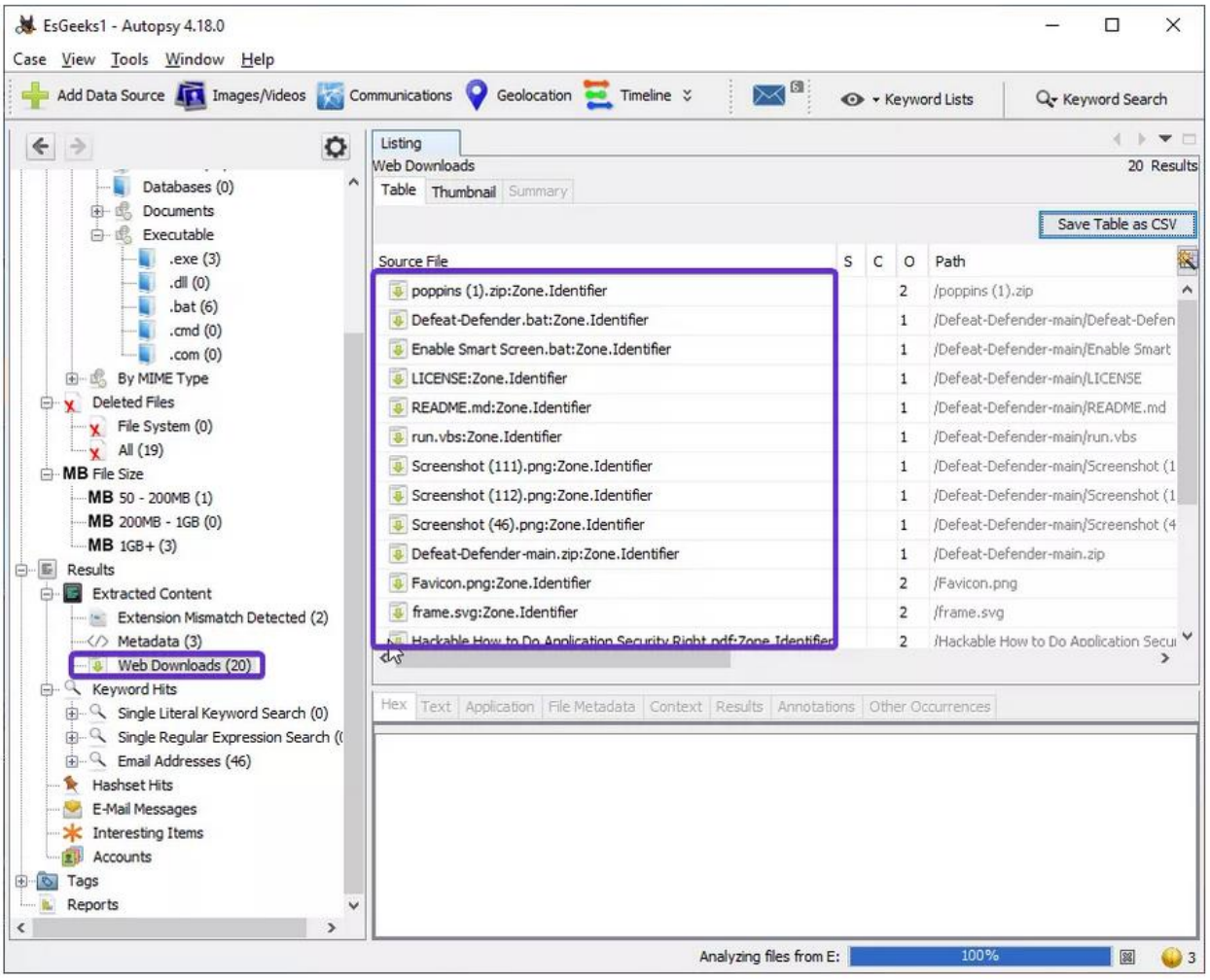


Figura 21: Sección Web Downloads.

Palabras clave

(Keyword Hits) Aquí se puede buscar cualquier palabra clave específica en la imagen de disco. La búsqueda se puede realizar con respecto a la coincidencia exacta, coincidencias de subcadena, correos electrónicos, palabras literales, expresiones regulares, etc.

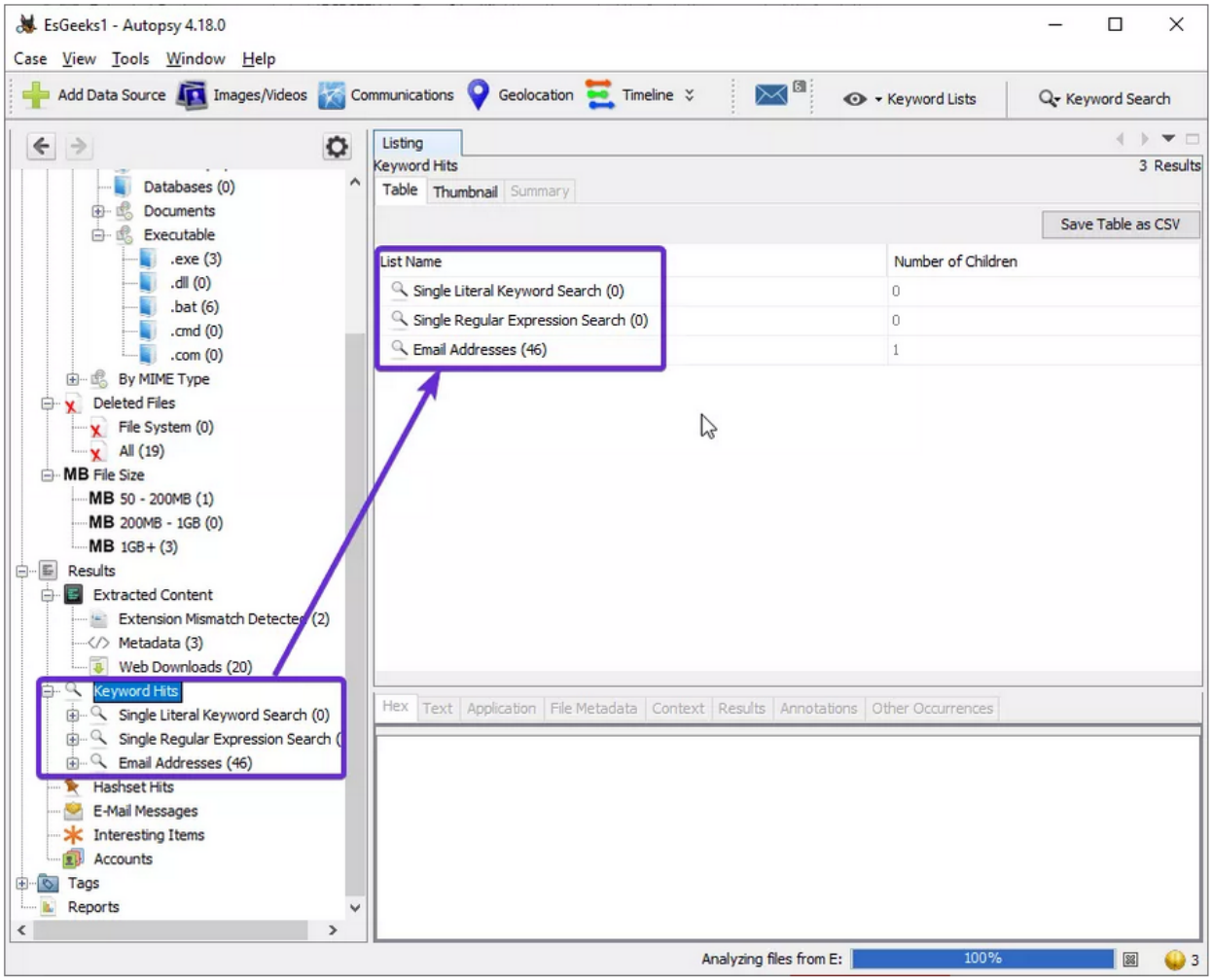


Figura 22: Sección Keyword Hits.

Se pueden ver las direcciones de correo electrónico disponibles.

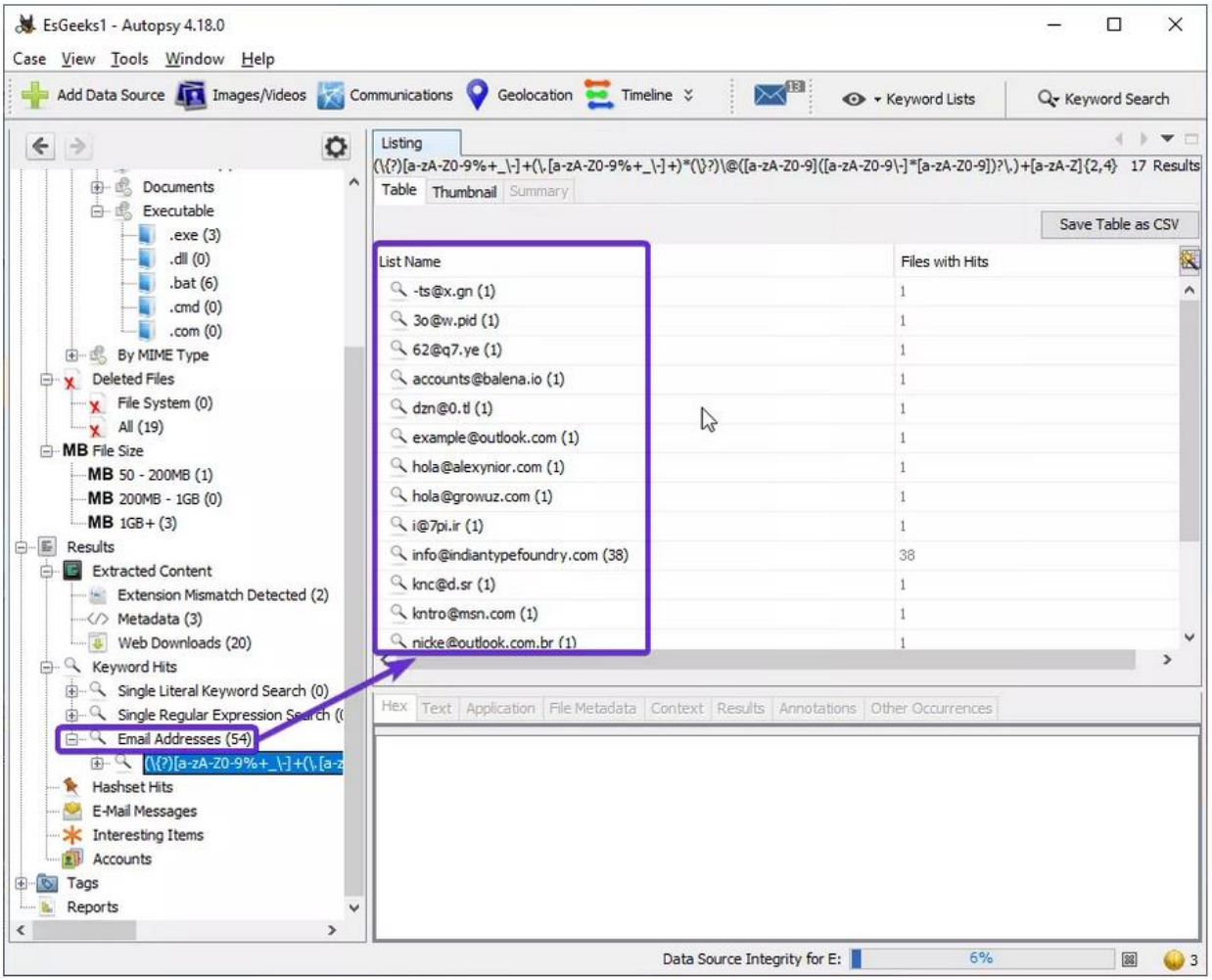


Figura 23: Filtro por correo electrónico.

Se puede optar por exportar a un formato CSV.

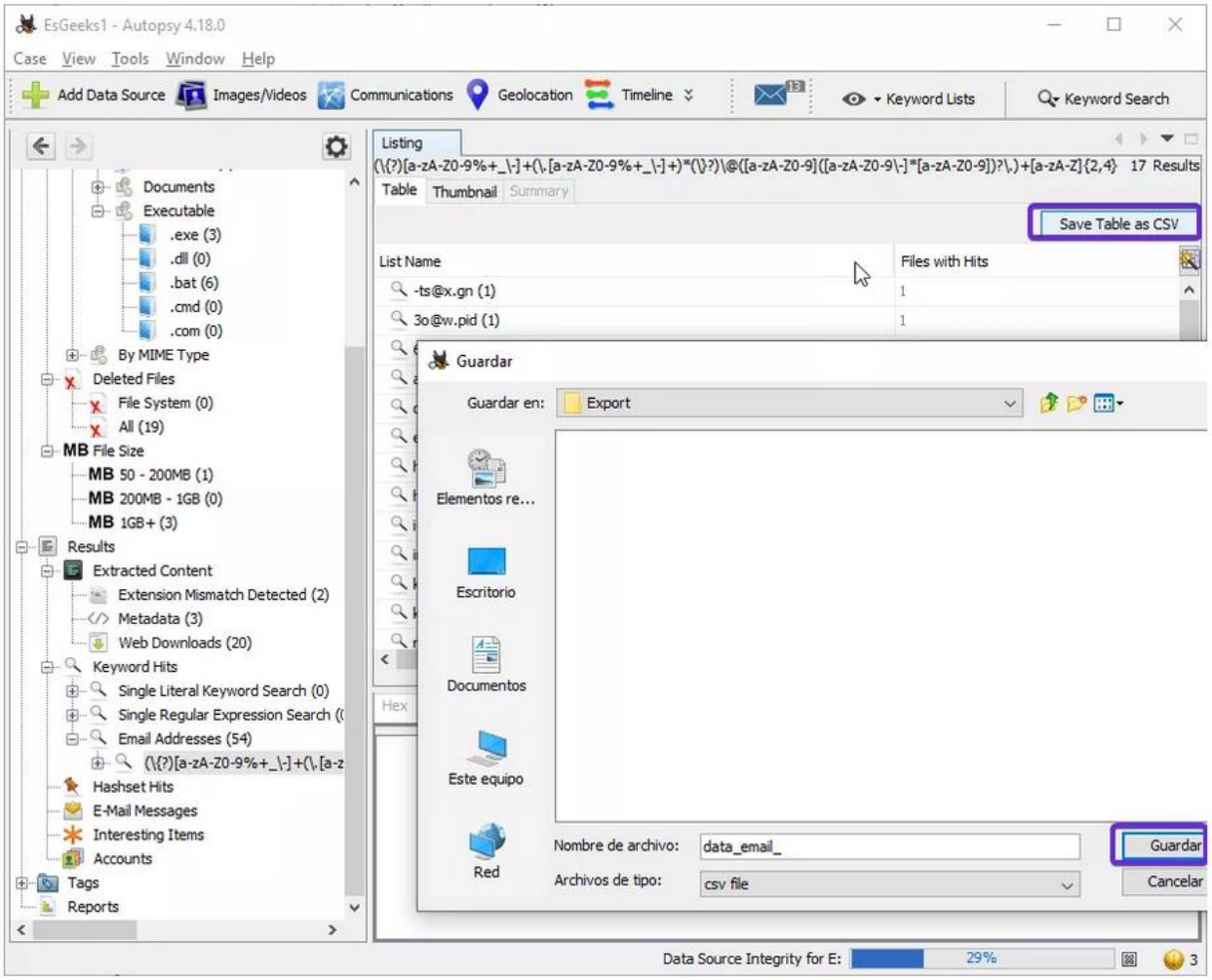


Figura 24: Exportar en formato CSV.

Línea de tiempo (Timeline)

Mediante esta función es posible obtener información sobre el uso del sistema en forma de estadística (statistical), detallado (detailed) o lista (list).

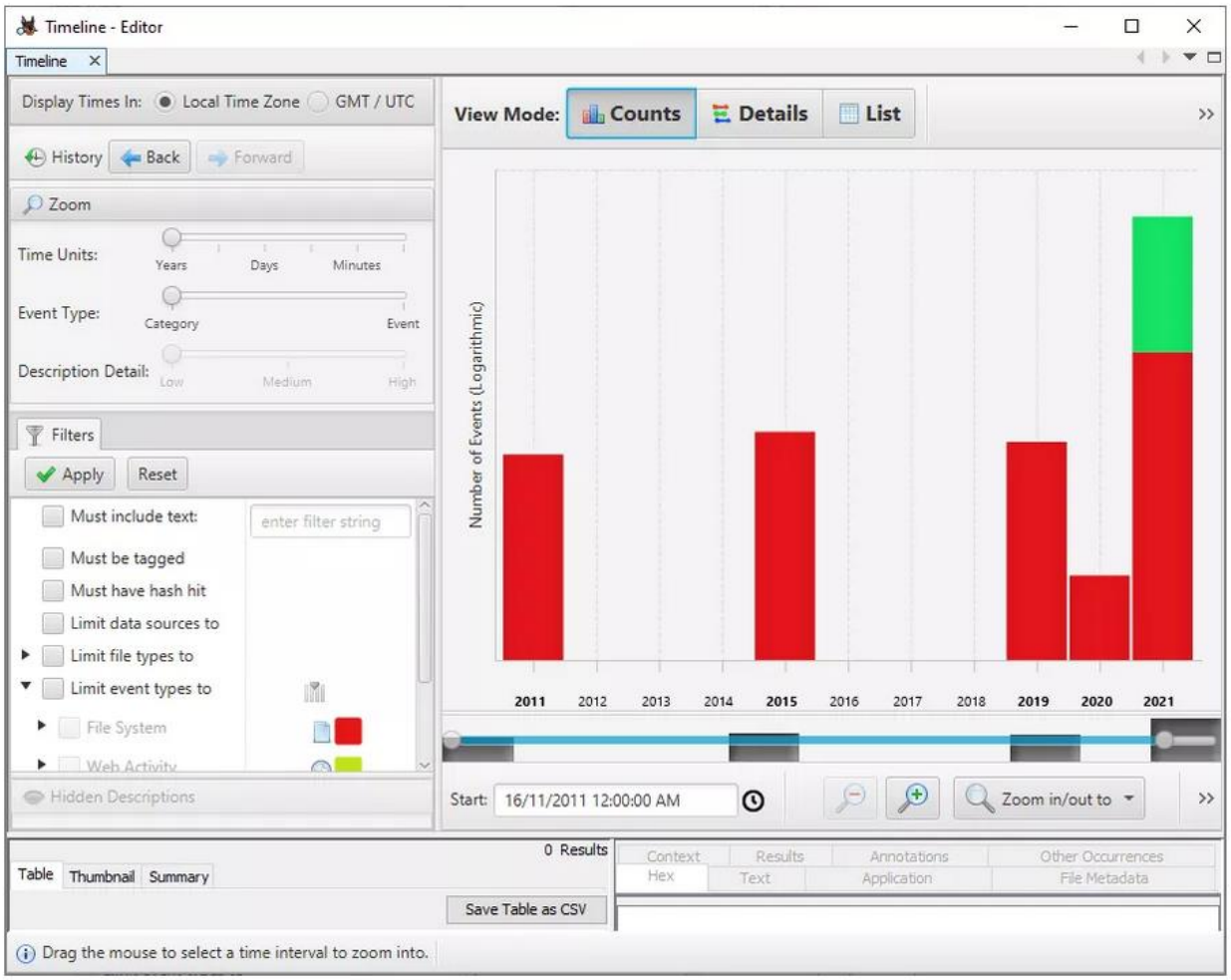


Figura 25: Timeline en formato estadística.

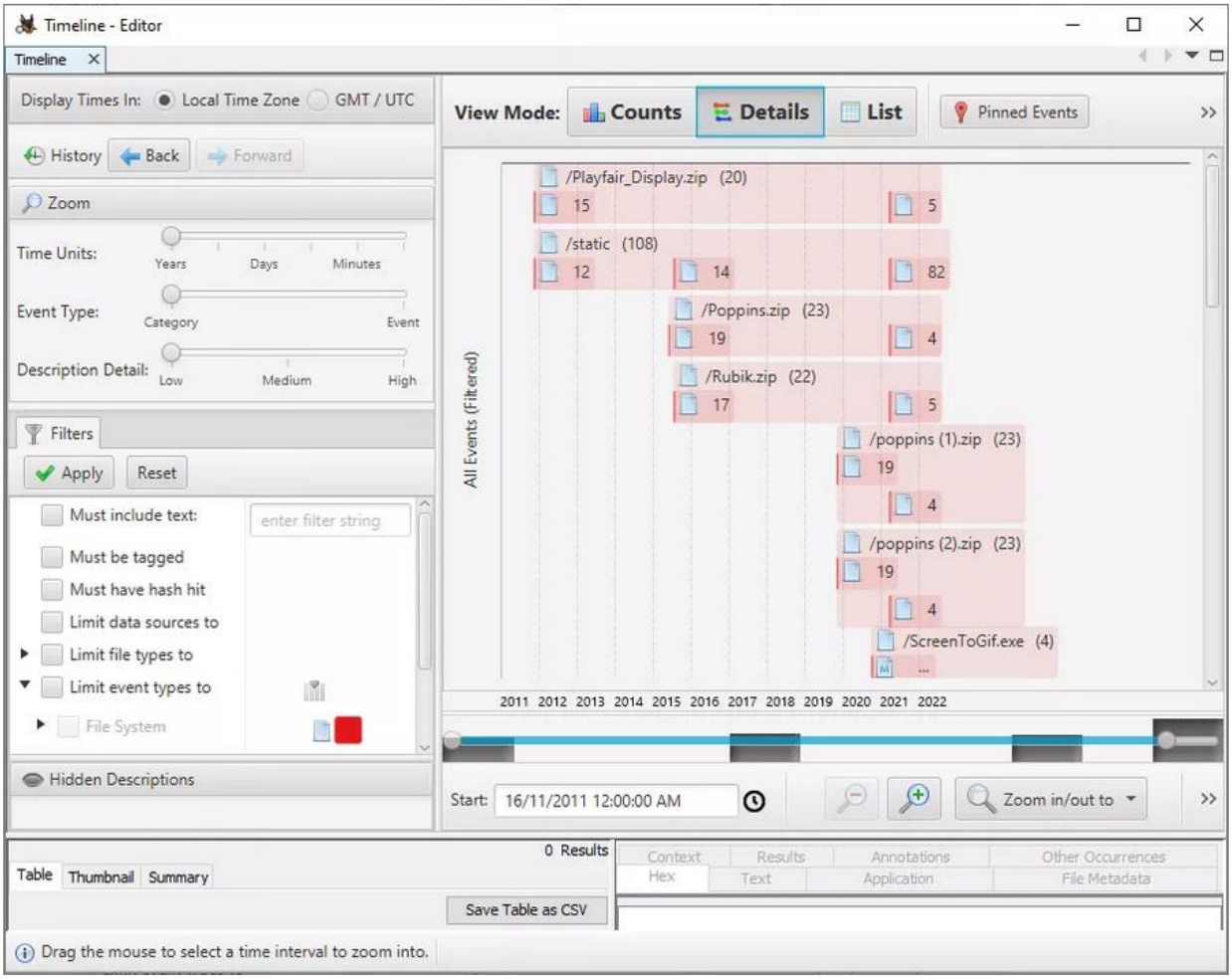


Figura 26: Timeline en formato detallado.

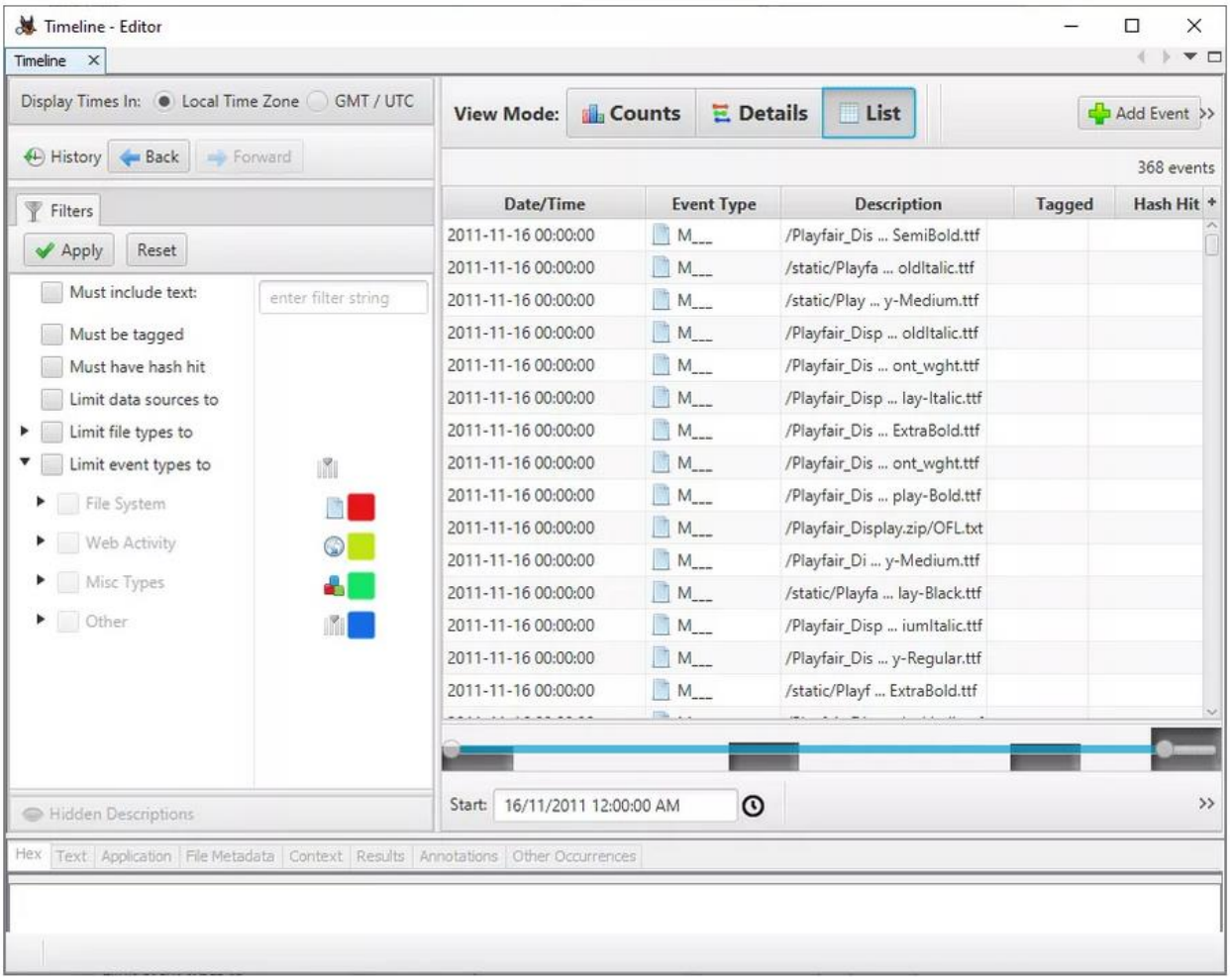


Figura 27: Timeline en formato lista.

Descubrimiento (Discovery)

Esta opción permite encontrar medios utilizando diferentes filtros que están presentes en la imagen de disco.

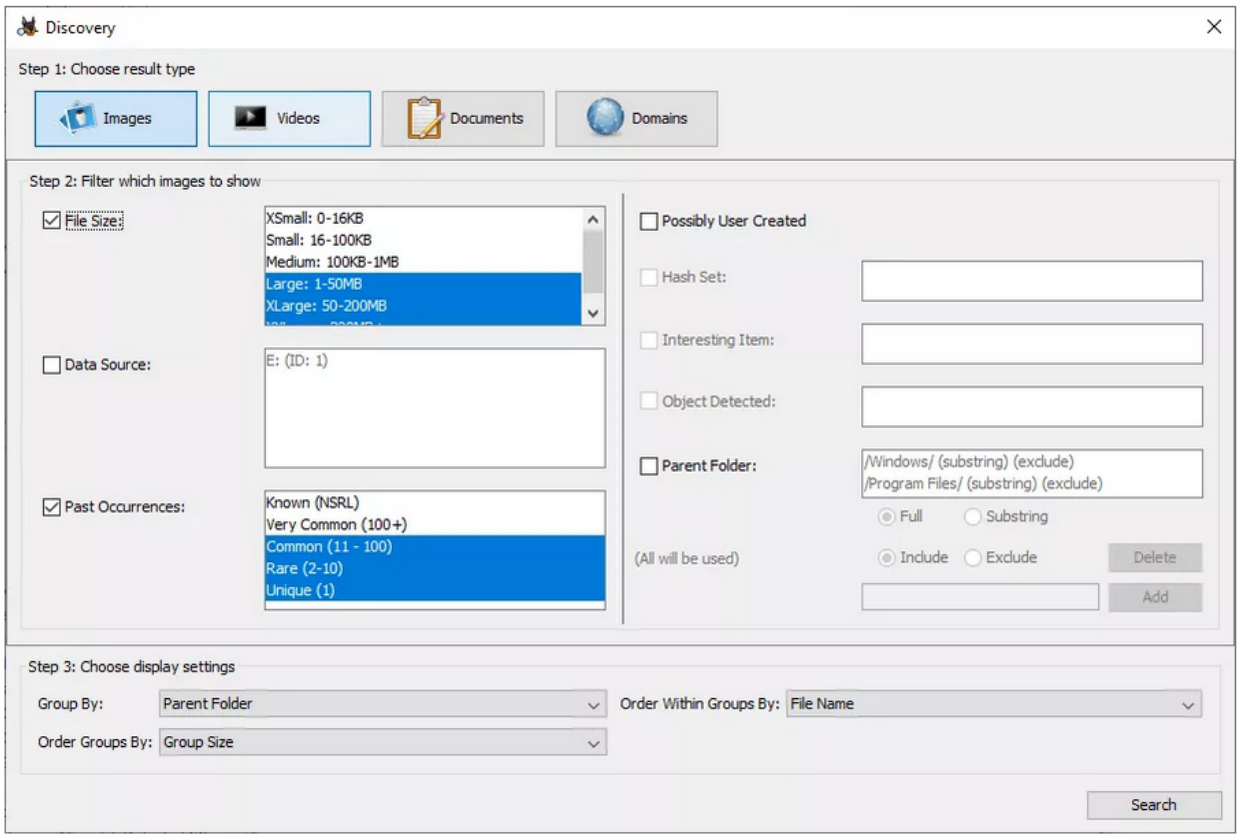


Figura 28: Descubrir medios por filtro.

Según las opciones seleccionadas, se pueden obtener los resultados deseados.

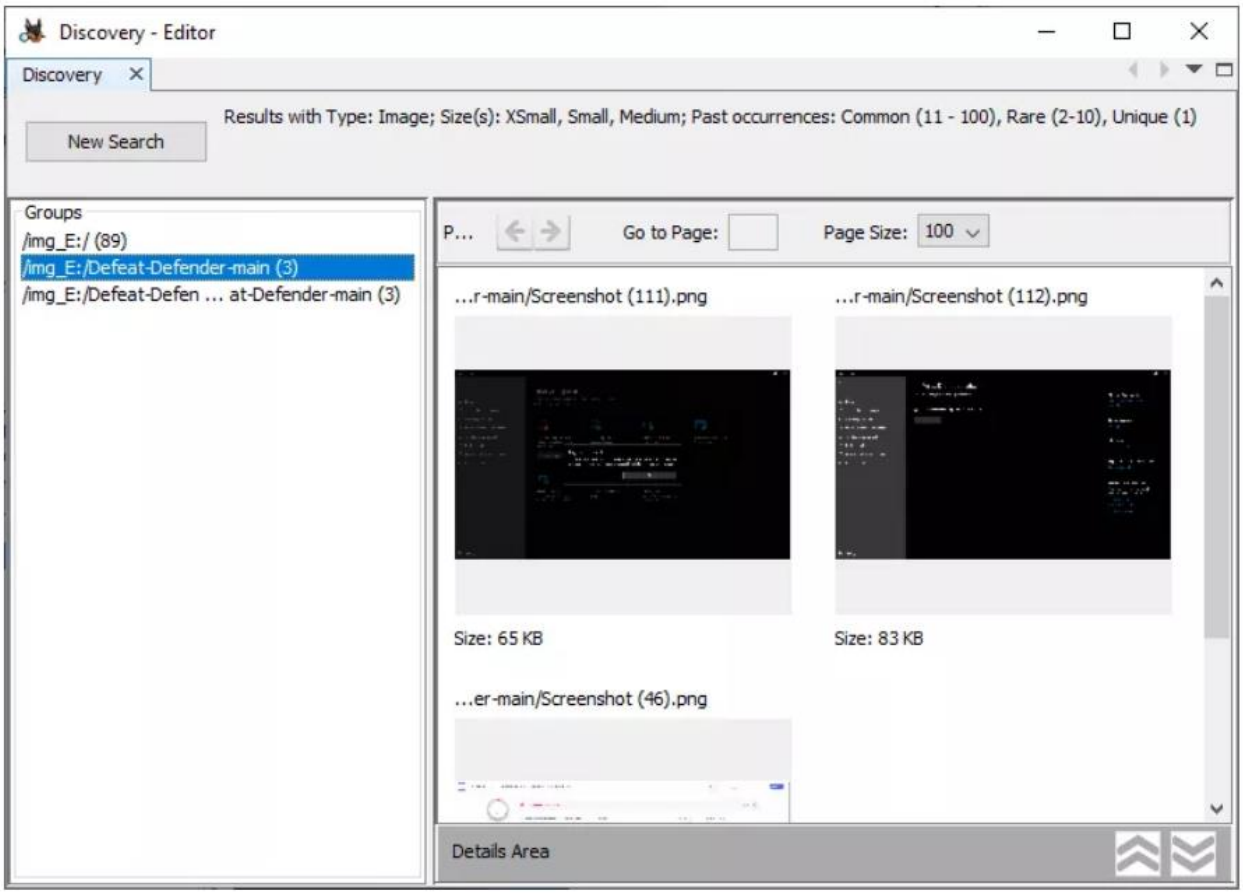


Figura 29: Resultados de filtros.

Imágenes/Vídeos

Esta opción permite encontrar imágenes y vídeos a través de varias opciones y múltiples categorías.

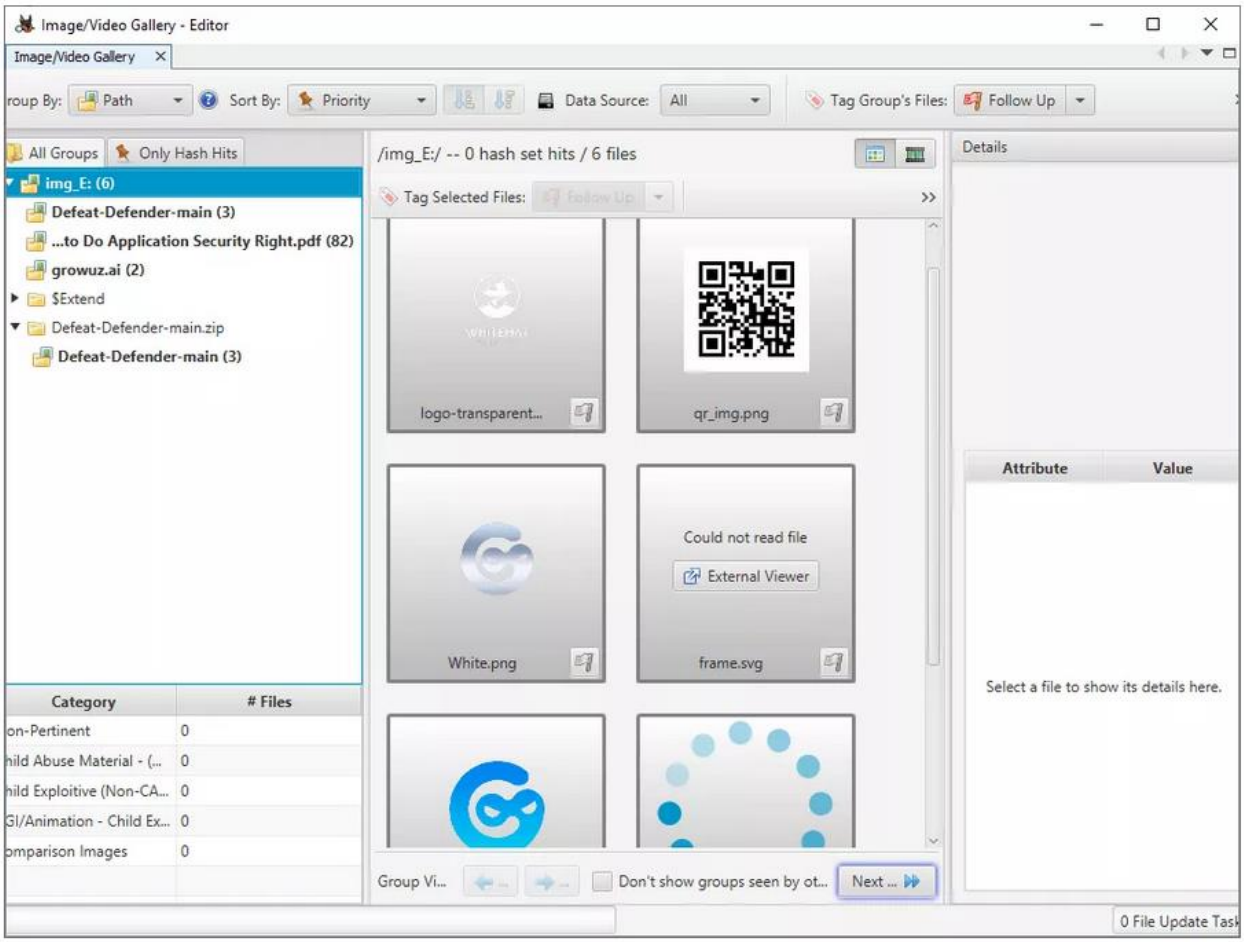


Figura 30: Resultados de imágenes y videos.

Añadir etiqueta de archivo

El etiquetado se puede utilizar para crear marcadores, seguimiento, marcar como cualquier elemento notable, etc.

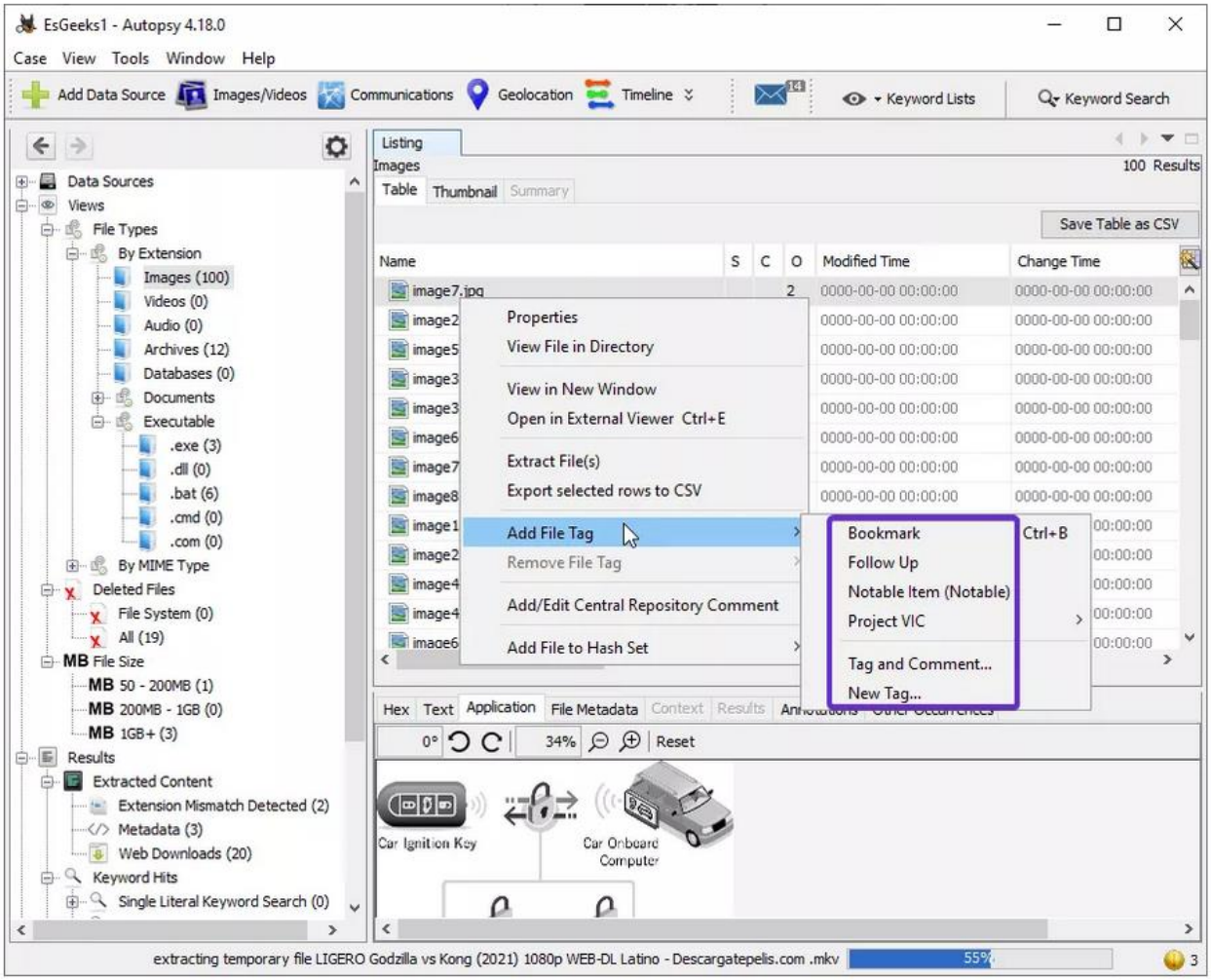


Figura 31: Etiquetado de archivos.

Al observar las opciones de etiquetas, se puede determinar que los archivos fueron etiquetados de acuerdo con varias categorías.

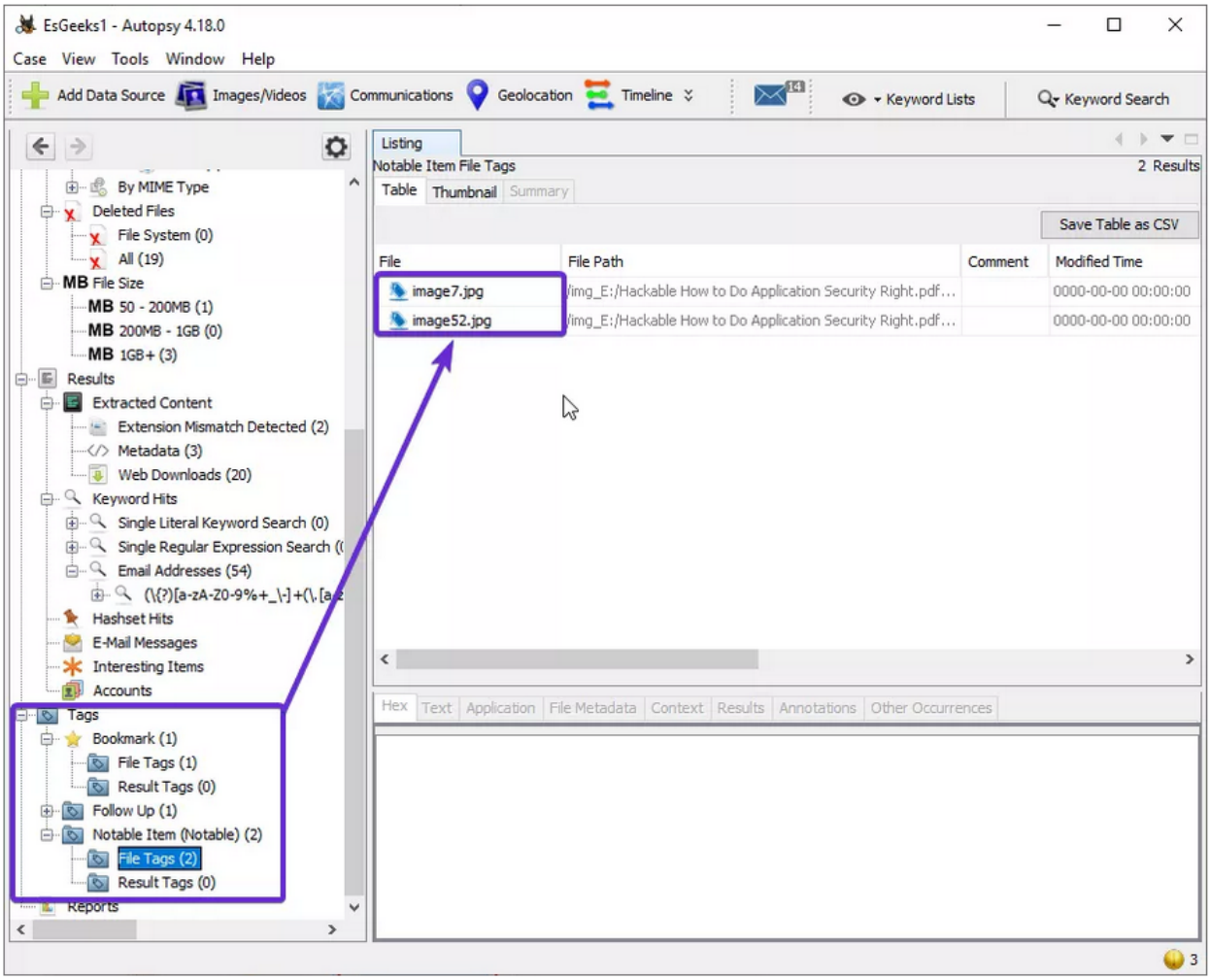


Figura 32: Filtros por etiquetas.

Generar Informe

Una vez terminada la investigación, el examinador puede generar el informe en varios formatos según su preferencia.

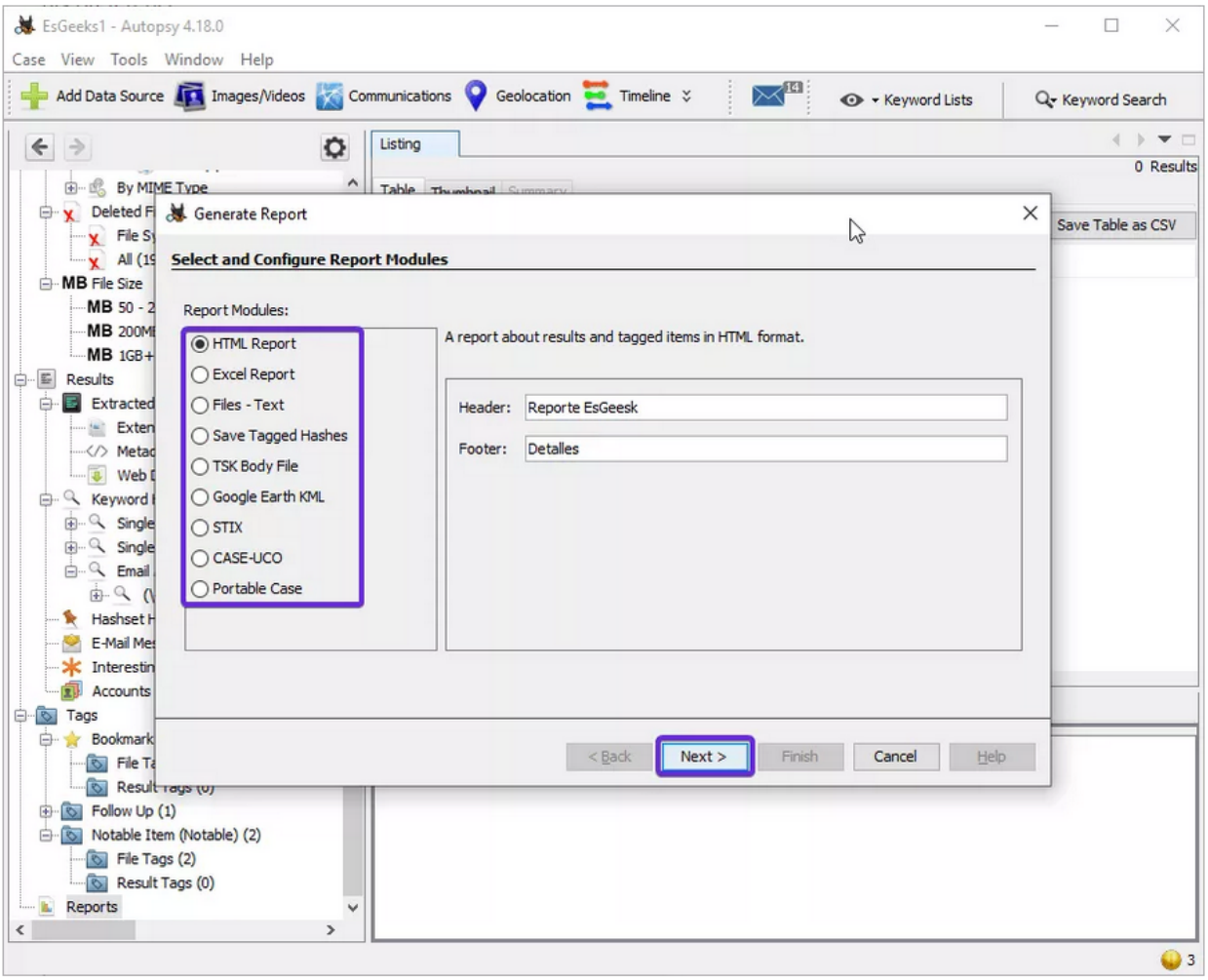


Figura 33: Generar informe.

Se debe comprobar la fuente de datos del informe a generar.

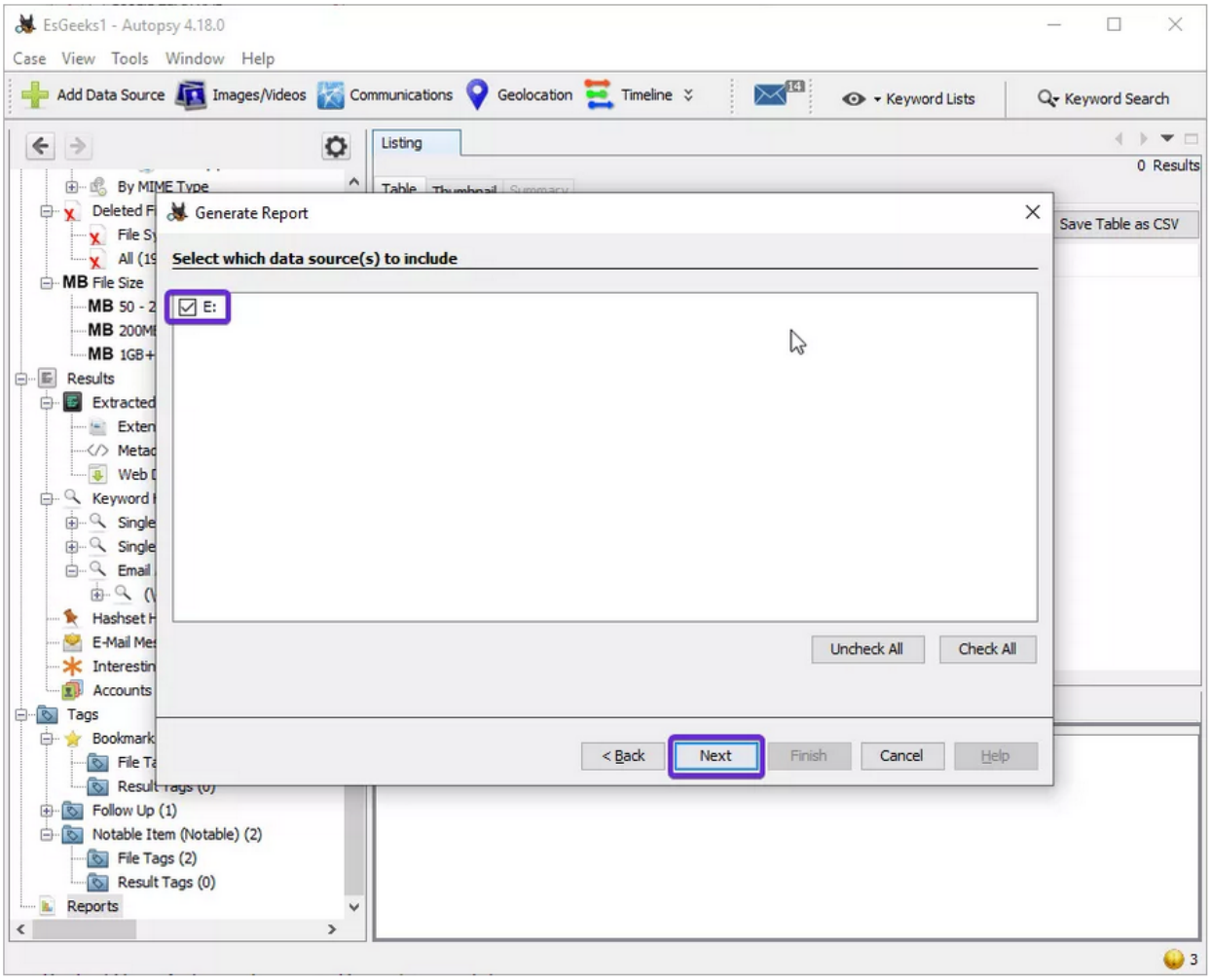


Figura 34: Informe de fuente de datos.

Para el ejemplo, se genera el informe en formato HTML.

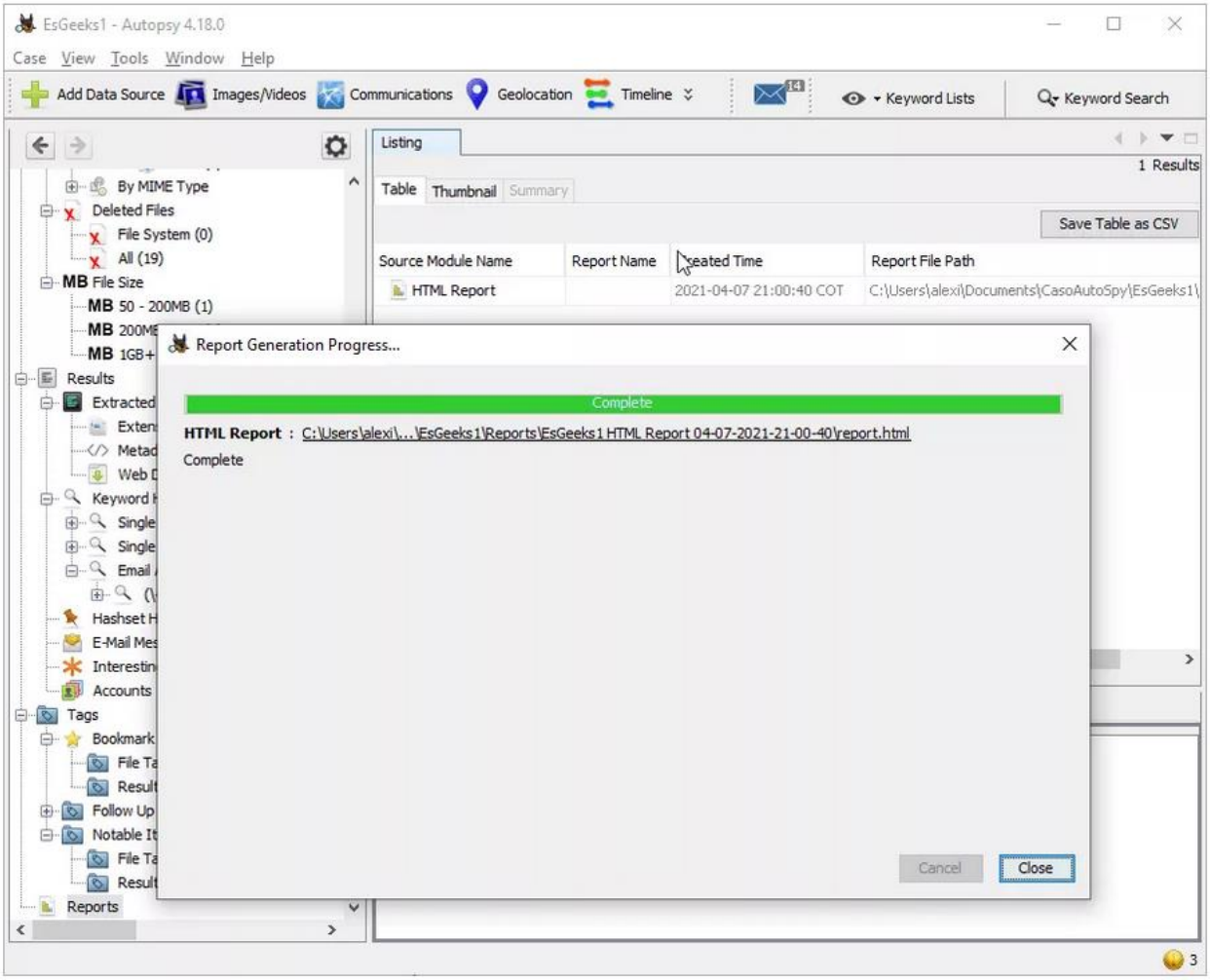


Figura 35: Informe generado en HTML.

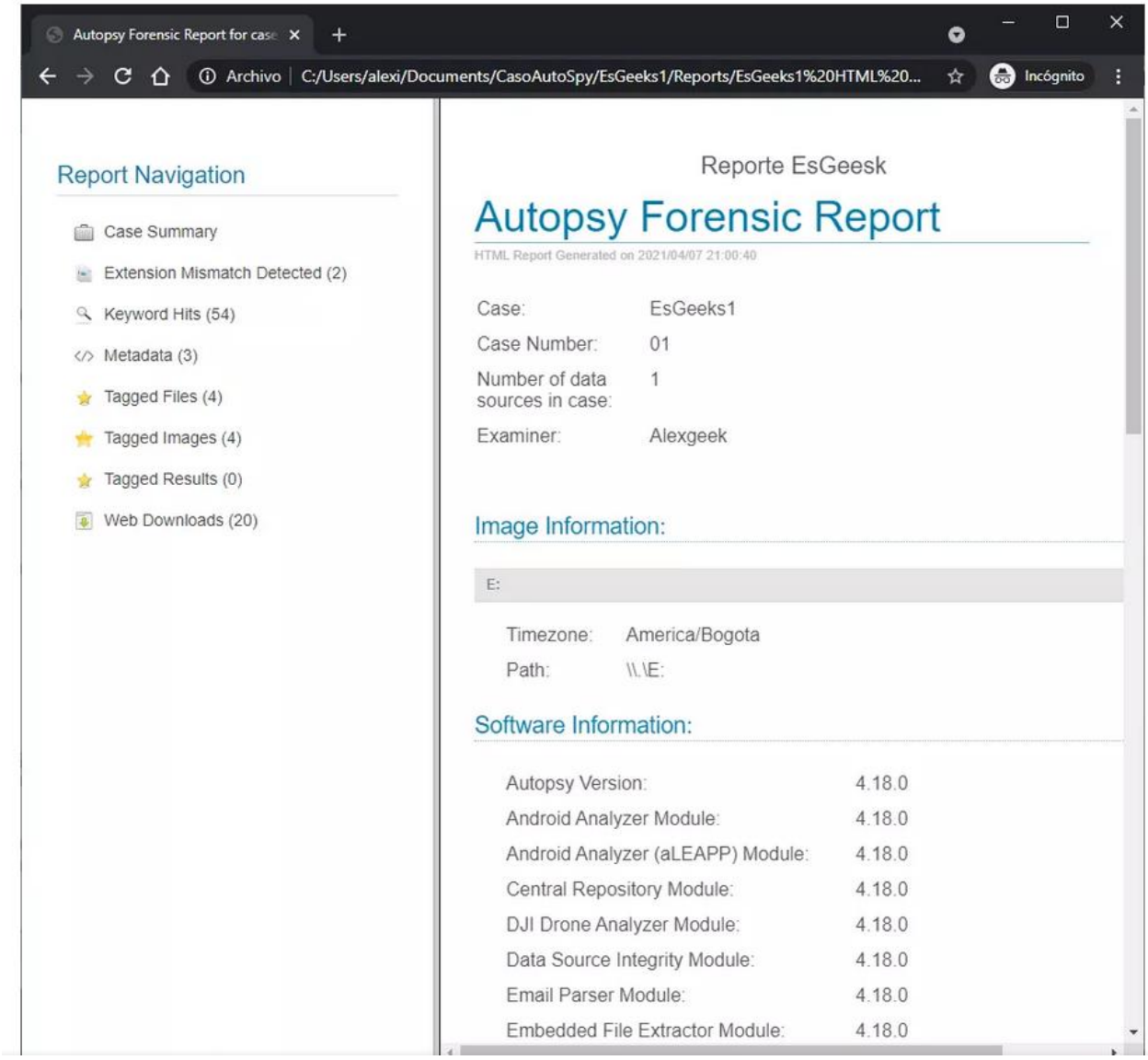


Figura 36: Informe forense de Autopsy generado en HTML.

Guía 5: Metodología Forense Linux

Proceso

El presente documento provee procesos y aspectos relacionados a una investigación digital forense, haciendo especial énfasis en sistemas Linux.

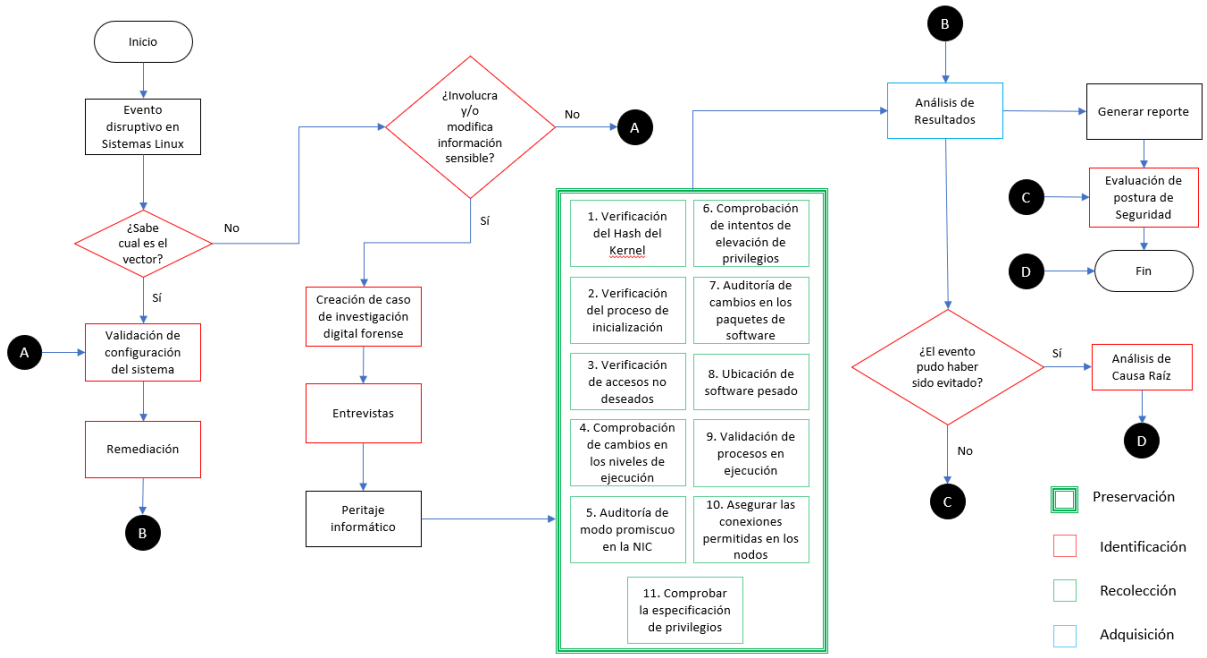


Figura 1: Diagrama del proceso

Detalles

En este apartado, se describen los procesos recomendados en el peritaje informático aplicado a sistemas Linux.

	Paso	Propósito	Técnica	Descripción	Herramientas
Peritaje Informático	**Verificación del Hash del Kernel**	Ayuda a determinar si el kernel ha sido modificado de alguna forma.	Comprobación md5 del hash.	Suma de comprobación a cada bit del archivo, digestión de hash y comparación de resultado del kernel.	Shell
	Verificación del proceso de inicialización	Determinar si en la inicialización del sistema existe algo fuera de lo común.	Comparación de mensajes de inicialización del sistema.	Validar que la inicialización no contenga procesos ajenos al funcionamiento normal.	Shell
	Verificación de accesos no deseados	Determinar si ha habido algún acceso no autorizado en el sistema.	Auditoría de accesos al sistema.	Validación de las cuentas de accceso.	Shell
	Comprobación de cambios en los niveles de ejecución	Validar la existencia de patrones anómalos en los niveles de ejecución del sistema.	Análisis de logs de niveles de ejecución.	Auditoría de los niveles de ejecución utilizados.	Shell
	Auditoría de modo promiscuo en la NIC.	Comprobar si en la NIC hay presencia de sniffer o de algún mecanismo de red no deseado en el sistema.	Validación de configuración de puertos.	Auditoría de logs en interfaces de red.	Shell
	Encontrar intentos de elevación de privilegios	Validar la existencia de intentos de elevación de privilegios.	Análisis de logs de autenticación.	Auditoría de privilegios de cuentas de usuario.	Shell
	Auditoría de cambios en los paquetes de software	Comprobar la existencia de cambios, instalación y ejecución de software anómalo en el sistema.	Análisis de logs.	Auditoría de cambios en paquetes de software.	Shell
	Ubicación de software pesado	Comprobar la existencia de logs o sniffers en el sistema.	Análisis de espacio en memoria y disco.	Validación de software anómalo.	Shell
	Validación de procesos en ejecución	Determinar la existencia anómala de procesos en ejecución el sistema.	Análisis de los procesos en ejecución del sistema.	Validación de procesos del sistema.	Shell
	Asegurar las conexiones permitidas en los nodos.	Validar que solamente existan las conexiones permitidas en el sistema.	Mapeo de red.	Auditoría de conexiones de red.	Shell
	Comprobar la especificación de privilegios	Determinar la existencia de usuarios root no permitidos en el sistema.	Análisis de archivo sudoers.	Auditoría de usuarios root.	Shell

Tabla 1: Detalles del proceso

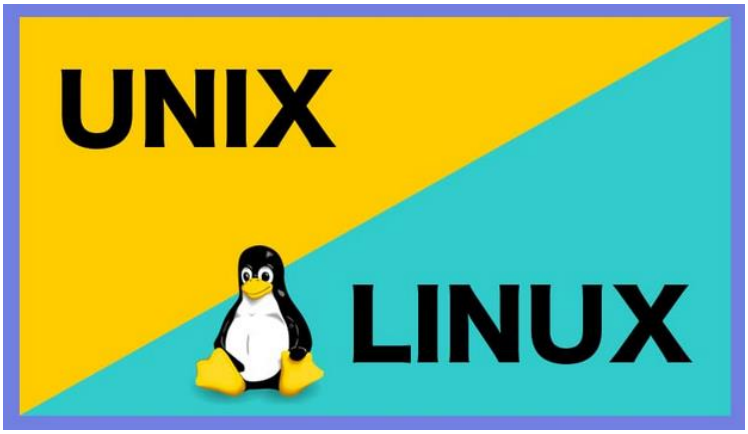
Aspectos relacionados

Proceso	Caso de empleo
Auditorías regulares	Realizar múltiples validaciones a la configuración del sistema de manera diaria, semanal, mensual o de acuerdo con las necesidades del negocio.
Eliminación de cuentas no utilizadas.	Eliminar las cuentas asociadas a personas que ya no estén vinculadas a la organización, realización de pruebas.
Sitios confiables	Navegar por sitios que cuenten con mecanismo de seguridad, así como evitar descargar archivos, programas ejecutabes de sitios sospechosos.

Tabla 2: Aspectos relacionados

Ejemplo

Metodología Forense Rutinaria (Unix & GNU Linux)



Verificación del Hash del Kernel. (Verificación de hash de los archivos que contiene el kernel)

El hash es una forma segura de representar una contraseña o valor de comprobación de una cosa.

El Kernel o núcleo es la parte más sofisticada de un sistema, consiste en un núcleo que realiza las tareas más complejas tales como el manejo y administración de la memoria de acceso aleatorio (RAM), prioridad de los procesos, manejo de aplicaciones, etc.

Para el ejemplo, se requiere conocer si un atacante ha comprometido el kernel con un rootkit, un rootkit es un paquete de software diseñado para permanecer oculto en un equipo mientras proporciona acceso y control remotos. Los hackers utilizan los **rootkits** para manipular un equipo sin el conocimiento ni el consentimiento del propietario.

Es muy importante que inmediatamente después de ser instalado un sistema Unix o GNU Linux se genere un hash de los archivos principales, en este caso el kernel y posteriormente se verifique la suma de comprobación ante cualquier tipo de duda de intrusión.

La generación de una suma de comprobación en MD5 del hash de los archivos del núcleo se realiza de la siguiente manera:

Sha512sum /boot/vmlinuz

Ejemplo de respuesta:

```
5f345151794b6fad56061fcec30ae97d  /boot/vmlinuz
```

Lo que hace es realizar una suma de comprobación a cada bit del archivo y digerir el hash.

```
5f345151794b6fad56061fcec30ae97d  /boot/vmlinuz
```

El siguiente paso es copiar la cadena de caracteres y guardarla en un pendrive encriptado, posteriormente cuando se empiece a realizar la rutina de comprobación se compara si los caracteres con el kernel son idénticos.

Tienen que ser idénticos a menos que se actualice el kernel del sistema operativo.

Verificación del proceso de inicialización

Es necesario verificar que en el proceso de inicialización del sistema no se indique nada fuera de lo común, como, por ejemplo, la carga de algún servicio extra o alguna operación extraña con las placas de red, etc.

Para ello, se procede a generar una instantánea de los mensajes de inicialización del sistema y posteriormente se guarda en un lugar seguro como podría ser un pendrive encriptado o un CD/DVD no regrabable.

Lo que se pretende es ejecutar el comando en un sistema limpio (sistema recién instalado), posteriormente guardar el resultado de esta comprobación y ante la menor duda de una intrusión bastará con volver a ejecutar el comando en el sistema sospechoso, retirar ese archivo y en una máquina limpia, por ejemplo, la máquina del auditor la cual podría ser un back track 5 en modo forense o Kali, revisar la comprobación del archivo original con el archivo de inicialización de la máquina con sospechas de intrusión.

Para realizar esto, es necesario utilizar los siguientes comandos:

Para auditar el proceso de inicialización del sistema se debe llamar la orden:

dmesg

Si se ejecuta esta orden, se enlistará todo lo que sea digno de destacar en un sistema, sin embargo, es necesario colocar en un archivo la información que se muestra en la terminal, para tal propósito ejecutamos lo siguiente en un sistema limpio, es decir en un sistema recién instalado:

dmesg > original.log

Si nos encontramos en la PC con sospechas de intrusión., ejecutamos lo siguiente:

dmesg > sospecha.log

Luego ejecutamos lo siguiente;

ls – lash sospecha.log

La salida anterior indica que el archivo tiene un tamaño de 32K.

Para realizar la comprobación, se comparan los archivos original.log y sospecha.log, para ello, se introduce el siguiente comando:

cmp original.log sospecha.log

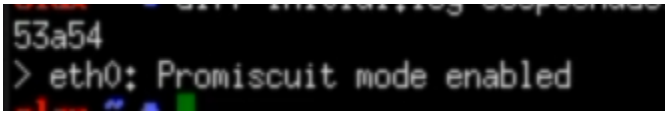
Para el ejemplo, devolvió lo siguiente:

Indica que existe una diferencia, lo cual significa que el archivo original.log comparado con el archivo sospecha.log difiere en 2270 caracteres en la línea 54.

Si se desea saber exactamente cuál es la diferencia, se debe ejecutar el siguiente comando:

diff original.log sospecha.log

Para el ejemplo, devolvió lo siguiente:



Lo cual indica que de la línea 53 a la 54 existe esta diferencia: en el sistema comprometido eth0 anunció que fue habilitado en modo promiscuo.

Lo anterior es una clara evidencia de intrusión.

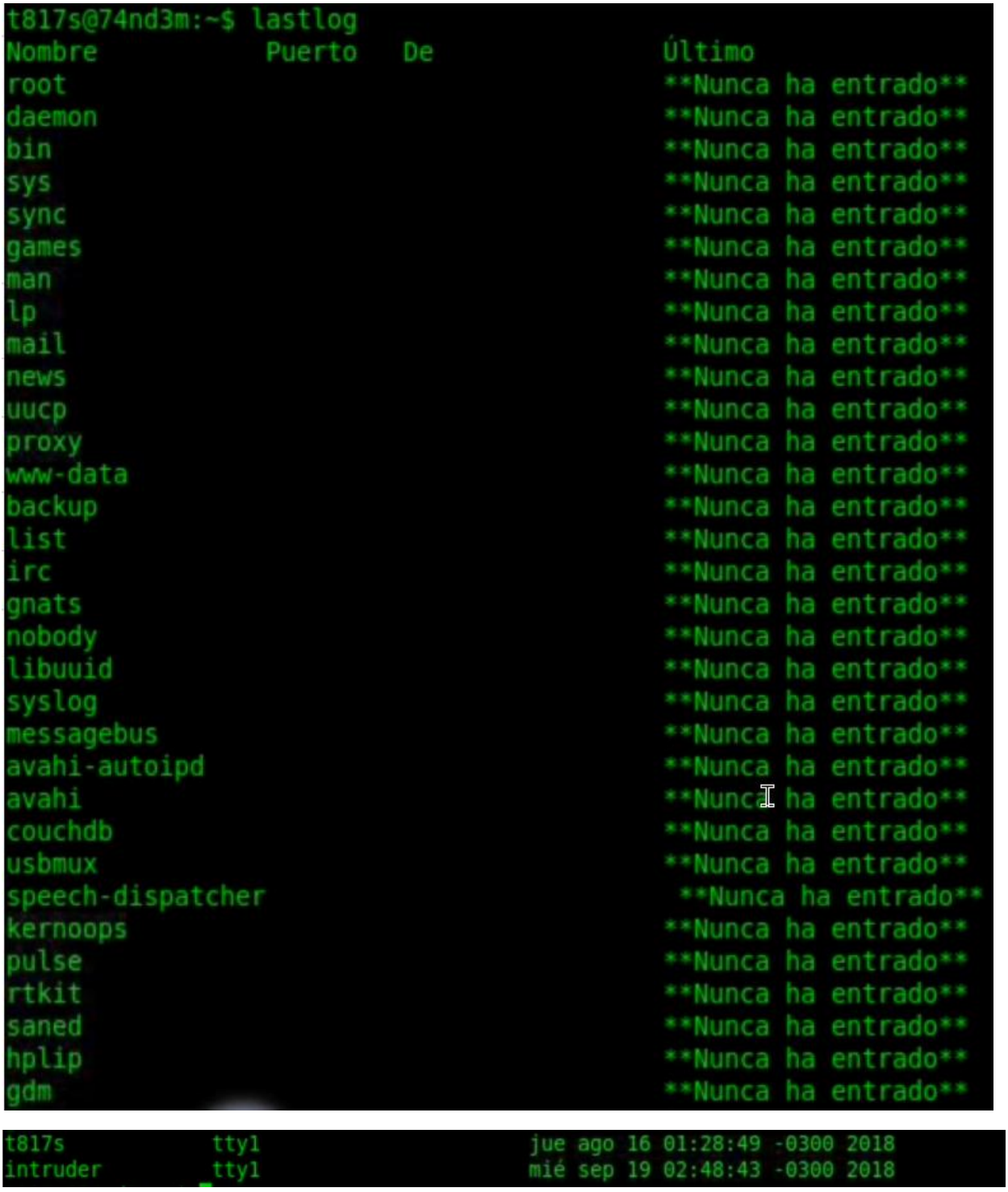
Verificación de accesos no deseados

Es necesario verificar cuando fue la última vez que los usuarios ingresaron al sistema, sobre todo si el sistema estuvo funcionando durante la noche, lo cual sirve para verificar accesos no deseado mediante cuentas de usuarios reales.

La forma de verificar los accesos al sistema, los horarios y desde que cuentas, se logra ejecutando una consola de comandos e ingresando la orden:

Lastlog

Para el ejemplo, devolvió lo siguiente:



Si se desea inhabilitar al usuario “intruder” , se debe ingresar al archivo passwd ubicado en etc, para acceder al archivo passwd se debe ejecutar el siguiente comando:

Nano /etc/passwd

Al bajar se observa la cuenta “intruder”

Al colocarle el símbolo # al inicio de la cuenta y al grabar el archivo, la cuenta quedará inhabilitada, recordar que al colocar el símbolo # al inicio de la línea equivale a comentarear dicha línea lo cual inhabilita el comando.

Por lo tanto, al realizar la modificación anterior, la persona que utilizaba el usuario “intruder” ya no podrá ingresar al sistema.

Comprobación de cambios en los niveles de ejecución

Los niveles de ejecución o Runlevels son formas determinadas de funcionar de un sistema UNIX o GNU Linux permitiendo un control más seguro del sistema operativo, por ejemplo, los Runlevel 0 indicarían el apagado de la PC.

Importante: Un Run Level del tipo mono usuario sin soporte de red (nivel de ejecución 1), puede ser una clara señal de un ataque de hacking físico.

Nivel de ejecución	Modo	Descripción
0	Alto	Indica halt o apagado de la máquina.
1	Monousuario	No configura la interfaz de red o los demonios de inicio, ni permite que ingresen otros usuarios que no sean el usuario root, sin contraseña. Este nivel de ejecución permite reparar problemas, o hacer pruebas en el sistema.
2	Multiusuario	Multiusuario sin soporte de red.
3	Multiusuario con soporte de red.	Inicia el sistema normalmente sin GUI.
4	Multiusuario con soporte de red.	No usado, con esta opción el administrador puede personalizar el inicio para cargar algún servicio.
5	Multiusuario gráfico (X11)	Indica multiusuario completo con inicio gráfico (X11)
6	Reinicio	Se reinicia el sistema.

Tabla 3: Niveles de ejecución de Linux.

Es muy importante auditar los cambios en los niveles de ejecución, para lograrlo, es necesario ejecutar el siguiente commando:

Cat /var/log/messages I grep runlevel

```
cat /var/log/messages | grep runlevel
```

Para el ejemplo, devolvió lo siguiente:

```
Sep 24 00:29:56 (none) init: Switching to runlevel: 0
Sep 24 00:35:14 (none) init: Switching to runlevel: 0
Sep 24 00:48:38 (none) init: Switching to runlevel: 0
Sep 24 04:26:41 (none) init: Switching to runlevel: 0
Oct 21 20:06:56 (none) init: Switching to runlevel: 6
Feb  6 16:20:09 (none) init: Switching to runlevel: 6
Jul 26 21:09:07 (none) init: Switching to runlevel: 6
Aug  8 03:30:24 (none) init: Switching to runlevel: 6
Oct 27 08:45:00 (none) init: Switching to runlevel: 6
Feb 18 14:59:04 (none) init: Switching to runlevel: 6
Feb 19 21:30:04 (none) init: Switching to runlevel: 0
May 10 09:29:14 (none) init: Switching to runlevel: 0
```

Se muestra la fecha y hora de los cambios de nivel de ejecución.

Auditoría de modo promiscuo en la NIC

Una tarjeta de red o NIC que se encuentre operando en modo promiscuo, podría indicar la presencia de un sniffer en el sistema comprometido.

En este punto, se pretende verificar cuando se conectaron o desconectaron las diferentes tarjetas de red o NIC del sistema que está siendo auditado, así como determinar si las NICs se establecieron en modo promiscuo.

Primero, es necesario averiguar cuantas placas de red tiene el sistema, por lo tanto, se ejecuta el siguiente commando:

ifconfig

```
# ifconfig
```

Para el ejemplo, devolvió lo siguiente:

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Para activar la interfaz ethernet se realiza lo siguiente:

```
# ifconfig eth0 up
```

Luego se Vuelve a ejecutar el commando ifconfig

```
# ifconfig
```

Para el ejemplo, devolvió lo siguiente:

```
eth0      Link encap:Ethernet  HWaddr 00:0C:29:87:E2:53
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:18 Base address:0x1080

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Para auditar los cambios en la interfaz ethenet 0, se ejecuta el siguiente comando:

```
# cat /var/log/messages | grep eth0
```

Los resultados que se muestran indican todos los cambios que ha tenido la interfaz:

```
Sep 24 00:08:10 (none) kernel: eth0: registered as PCnet/PCI II 79C970A
Sep 24 00:26:51 (none) kernel: eth0: registered as PCnet/PCI II 79C970A
Sep 24 00:32:31 (none) kernel: eth0: registered as PCnet/PCI II 79C970A
Sep 24 00:40:20 (none) kernel: eth0: registered as PCnet/PCI II 79C970A
Sep 24 00:57:41 (none) kernel: eth0: registered as PCnet/PCI II 79C970A
Sep 28 01:59:42 (none) kernel: eth0: registered as PCnet/PCI II 79C970A
Oct 20 17:53:27 (none) kernel: eth0: registered as PCnet/PCI II 79C970A
Oct 20 20:52:12 (none) kernel: device eth0 entered promiscuous mode
Oct 20 20:52:53 (none) kernel: device eth0 left promiscuous mode
Oct 20 20:57:29 (none) kernel: device eth0 entered promiscuous mode
Oct 20 20:58:10 (none) kernel: device eth0 left promiscuous mode
Oct 20 20:59:32 (none) kernel: device eth0 entered promiscuous mode
Oct 20 21:00:25 (none) kernel: device eth0 left promiscuous mode
Oct 20 21:01:06 (none) kernel: device eth0 entered promiscuous mode
Oct 20 21:01:30 (none) kernel: device eth0 left promiscuous mode
Oct 20 21:07:29 (none) kernel: device eth0 entered promiscuous mode
Oct 20 21:07:30 (none) kernel: device eth0 left promiscuous mode
Oct 20 21:07:30 (none) kernel: device eth0 left promiscuous mode
Oct 21 07:57:04 (none) kernel: device eth0 entered promiscuous mode
Oct 21 07:57:22 (none) kernel: device eth0 left promiscuous mode
Oct 21 07:59:50 (none) kernel: device eth0 entered promiscuous mode
Oct 21 08:01:17 (none) kernel: device eth0 left promiscuous mode
Oct 21 08:02:08 (none) kernel: device eth0 entered promiscuous mode
```

Se muestra que para determinadas fechas y horas la interfaz se estableció en modo promiscuo, luego casi de inmediato se salió del modo promiscuo, dicho comportamiento correspondería a sniffing de red.

Esta información se puede correlacionar con los cambios en los niveles de ejecución de la sección anterior, por ejemplo, si para esas fechas y horas se valida que se encontraba en el nivel de ejecución 1, podría indicar que el usuario tuvo acceso físico a la PC comprometida.

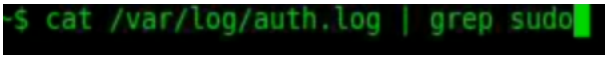
Encontrar intentos de elevación de privilegios

Las técnicas de elevación de privilegios se utilizan para ganar accesos administrativos a un determinado sistema.

Es necesario verificar los logs para cada servicio de nuestro sistema, con esto se tendrá la capacidad de saber cuándo se ingresaron comandos sudo; el comando sudo se utiliza para ejecutar acciones con los privilegios del usuario root.

El comando a ejecutar es el siguiente:

Cat / var/log/auth.log I grep sudo



Para el ejemplo, devolvió lo siguiente:

Se indican las fechas, horas, desde que máquina, con que cuenta de usuario, desde donde se ingresó, así como el comando que se ejecutó.

Auditoría de cambios en los paquetes de software

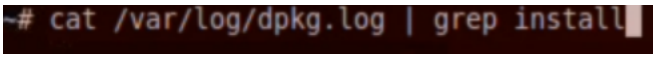
Los paquetes de software son todas las aplicaciones que pueden estar instaladas en los sistemas de tipo UNIX & GNU Linux.

Los cambios pueden ser:

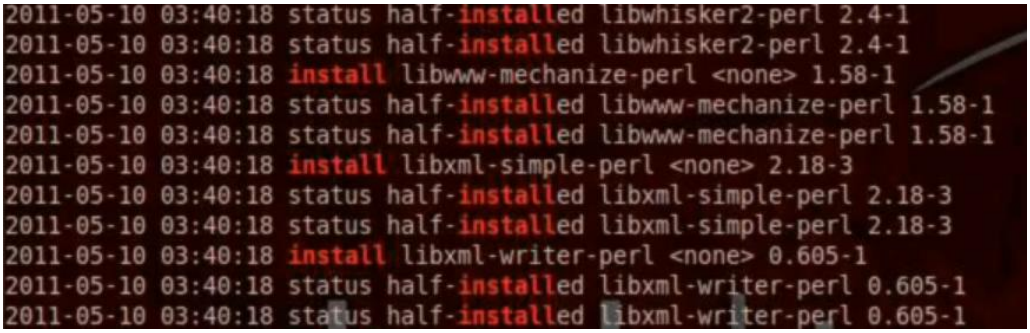
- Instalación de software.
- Actualización de software
- Eliminación de software.

Para validar las instalaciones realizadas en el sistema, se puede utilizar el siguiente comando:

Cat /var/log/dpkg.log I grep install

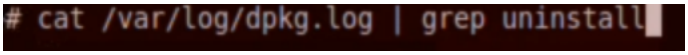


Para el ejemplo, devolvió lo siguiente:



Para validar las desinstalaciones realizadas en el sistema, se puede utilizar el siguiente comando:

Cat /var/log/dpkg.log I grep uninstall



Para el ejemplo, no devolvió nada, lo cual significa que no se ha desinstalado nada.

Para validar las actualizaciones realizadas en el sistema, se puede utilizar el siguiente comando:

Cat /var/log/dpkg.log I grep upgrade

Para el ejemplo, devolvió lo siguiente:

Adicionalmente, se puede ejecutar lo siguiente para almacenar la salida de los comandos en un archivo .txt para posteriormente almacenar dichos archivos en un pendrive encriptado y ante la sospecha de modificación, se podría realizar la comparativa de los archivos para determinar si en efecto hubo alguna modificación.

Comandos utilizados:

Cat /var/log/dpkg.log I grep install > muestrainstalados.txt

Cat /var/log/dpkg.log I grep uninstall > muestradesinstalados.txt

Cat /var/log/dpkg.log I grep upgrade > muestraactualizados.txt

Ubicación de software pesado

La presencia de aplicaciones o archivos de gran tamaño puede deberse a actividades ocultas como logs o sniffers.

Se utilizará el comando df y el comando free, el comando df muestra el tamaño total de cada unidad de almacenamiento y los espacios ocupados y restantes para cada una de ellas.

El comando free proporciona una salida en pantalla en la que se puede visualizar el tamaño total, el tamaño ocupado y el tamaño restante, pero en esta ocasión también de la memoria RAM y de la memoria virtual, la memoria virtual es una porción del disco duro que puede ser utilizada como si fuera memoria RAM en caso de agotarse la memoria RAM real lo cual ralentizaría el sistema.

Auditar el espacio libre en las unidades de almacenamiento es una buena política para encontrar software pesado.

Al ejecutar el comando df, proveerá una salida inentendible.

```
slax ~ # df
Filesystem           1K-blocks      Used Available Use% Mounted on
tmpfs                  4008380   2386372   1418388  63% /
/dev/sda1              4008380   2386372   1418388  63% /mnt/sda1
```

Por lo tanto, es necesario agregar -h, que significa human readable.

Para el ejemplo, devolvió lo siguiente:

```
slax ~ # df -h
Filesystem           Size  Used Avail Use% Mounted on
tmpfs                3.9G  2.3G  1.4G  63% /
/dev/sda1            3.9G  2.3G  1.4G  63% /mnt/sda1
```

Para el ejemplo, nos indica que tiene una unidad de disco sda1 de 3.9 GB que está utilizando 2.3 GB (63%) y que está disponible 1.4 GB.

El comando free proporciona el estado de la memoria RAM, que para el ejemplo tiene un total de 123 MB, de los cuales han sido utilizados 120 MB y que aún tiene disponible 2.8 MB, por lo que de la memoria Swap del disco duro sda1 que tiene un total de 120 MB no ha utilizado nada.

```
slax ~ # free
             total       used       free     shared    buffers     cached
Mem:        123044     120228       2816          0      10240      96860
-/+ buffers/cache:      13128     109916
Swap:       120476          0     120476
```

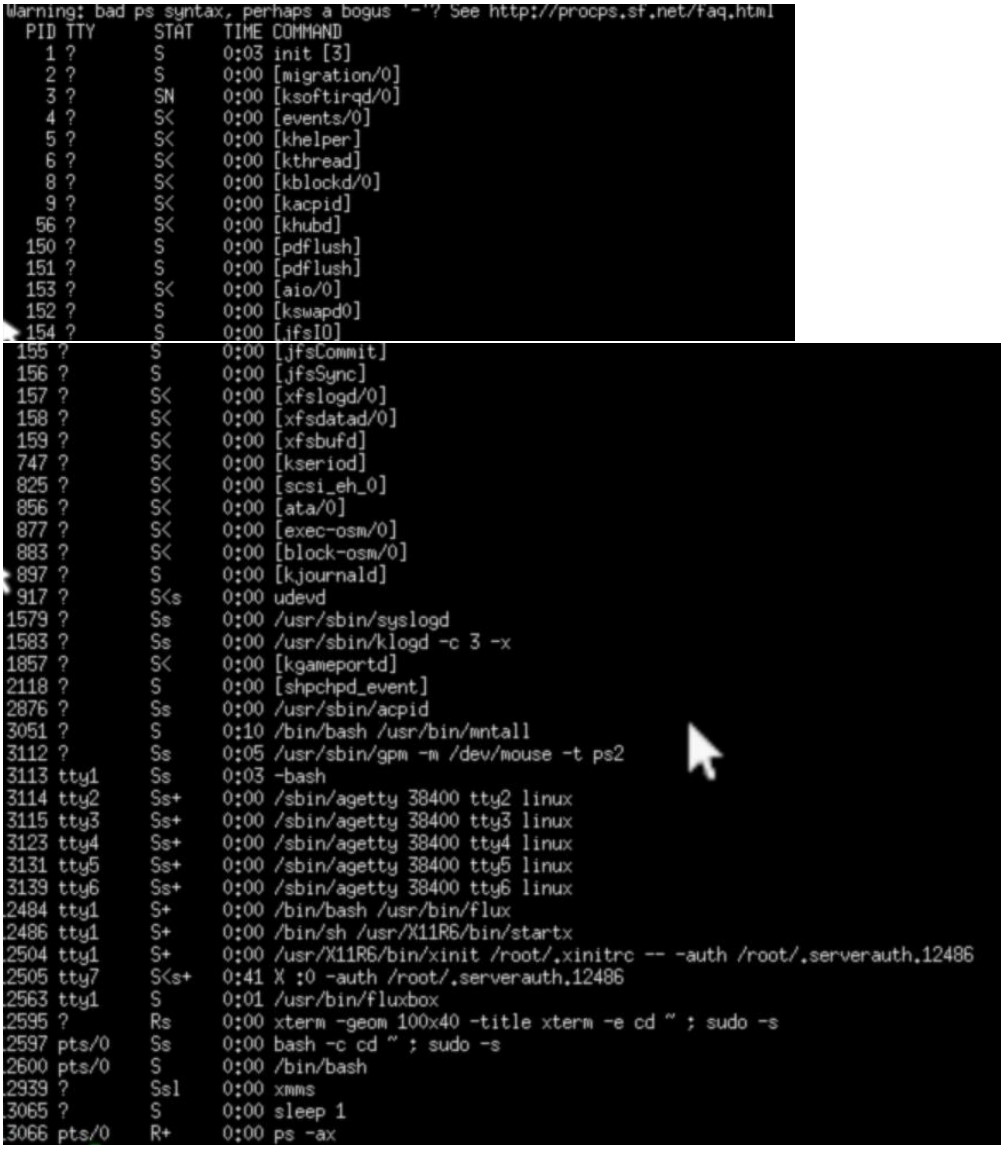
Validación de procesos en ejecución

Se debe de auditar los procesos en ejecución, indicando sus archivos de operaciones.

Un proceso es una aplicación que puede estar funcionando en segundo plano y que no necesariamente debe tener interfaz gráfica (GUI).

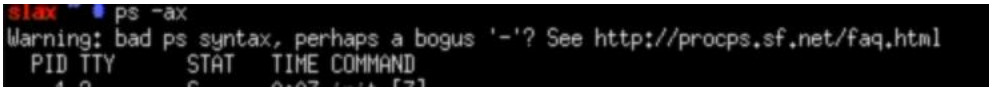
Para verificar los procesos en ejecución se debe ejecutar el siguiente comando:

Ps -ax



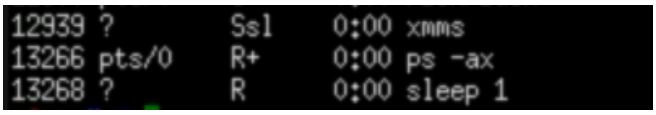
Para el ejemplo, se muestran todos los procesos y de donde se ejecutan las aplicaciones.

Al ejecutar el comando ps -ax, se muestran tres columnas:



La primera columna es el ProcessID (**PID TTY**), cada proceso, programa o aplicación que corre con interfaz gráfica o sin ella, ya sea en primer plano o en segundo plano tiene asignado un número de ProcessID, lo cual le permite realizar operaciones tales como pasarla a primer plano, dejarla en segundo plano, ponerla a dormir, volver a ejecutarla y eliminarla. Por ejemplo, si se hace referencia al ProcessID con la orden kill es posible matar el proceso.

Para el ejemplo, se asume que la aplicación xms podría ser un troyano, su ProcessID es 12939



Siguiendo con el ejemplo, se ejecutará el siguiente comando: kill -9 12939, -9 que equivale a darle la orden de callarse y apagarse.

Se recomienda llevar a cabo el proceso anterior en el caso de encontrar un proceso no deseado.

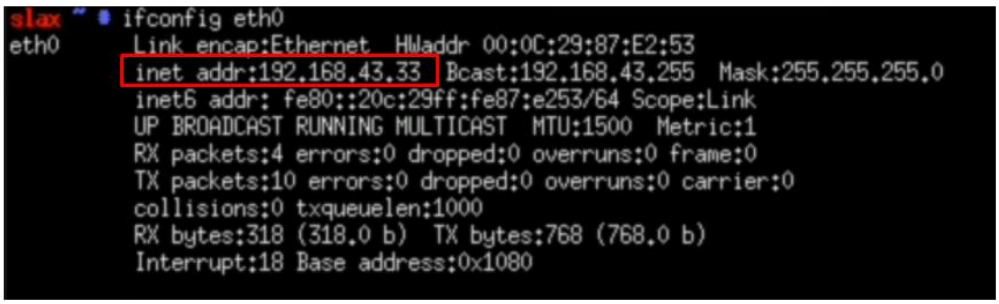
Asegurar las conexiones permitidas en los nodos

Debe de asegurarse que las PCs de los usuarios realicen solo las acciones permitidas, para ello se hace uso de un escáner llamado NMAP, al ejecutarlo nos estaría indicando los puertos de comunicación abiertos en el sistema objetivo.

Un intruso no puede estar presente, pero puede haber plantado alguna herramienta que haga mal uso de datos o que abra un puerto de comunicación del protocolo TCP o UDP para poder conectarse o para poder conectar algún tipo de servicio no deseado, por ello es recomendable realizar un escaneo con NMAP.

Lo primero que hay que hacer es conocer la dirección IP de la máquina a escanear, no es recomendable instalarlo en la propia PC y escanearlo desde adentro ya que podría contener un rootkit.

Si es un sistema GNU Linux, se debe ejecutar el siguiente comando: ifconfig eth0



En inet address aparece la dirección IP.

Posteriormente, desde otra PC, se ejecuta el comando nmap junto con la dirección IP de la PC objetivo:

Nmap 192.168.43.33

Siguiendo el ejemplo, al ejecutar el comando, se indica que se encontró un Puerto TCP con estado abierto el cual corresponde a un servicio X11, un servicio relacionado con el movimiento de imágenes.

Es importante recordar que un puerto abierto en una PC significaría que dicha máquina está prestando un servicio al exterior, por ende, es una vulnerabilidad que debe ser solucionada.

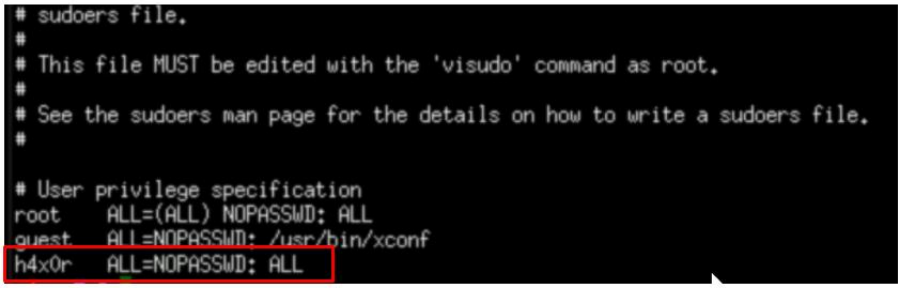
Comprobar la especificación de privilegios

Se debe de verificar que no existan usuarios con control total, es decir que no haya usuarios que puedan ejecutar el comando sudo desde sus cuentas a través de la consola y posteriormente abrir a nombre del usuario admin o del root cualquier aplicación que se desee.

Para realizar la validación se debe ejecutar el siguiente comando:

Cat /etc/sudoers

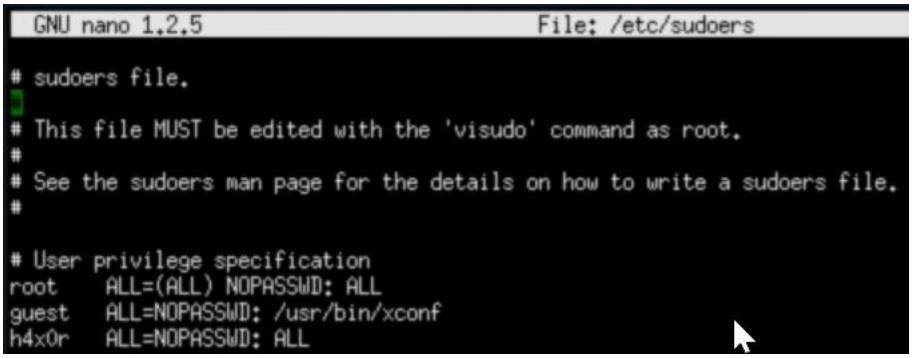
Para el ejemplo, devolvió lo siguiente:



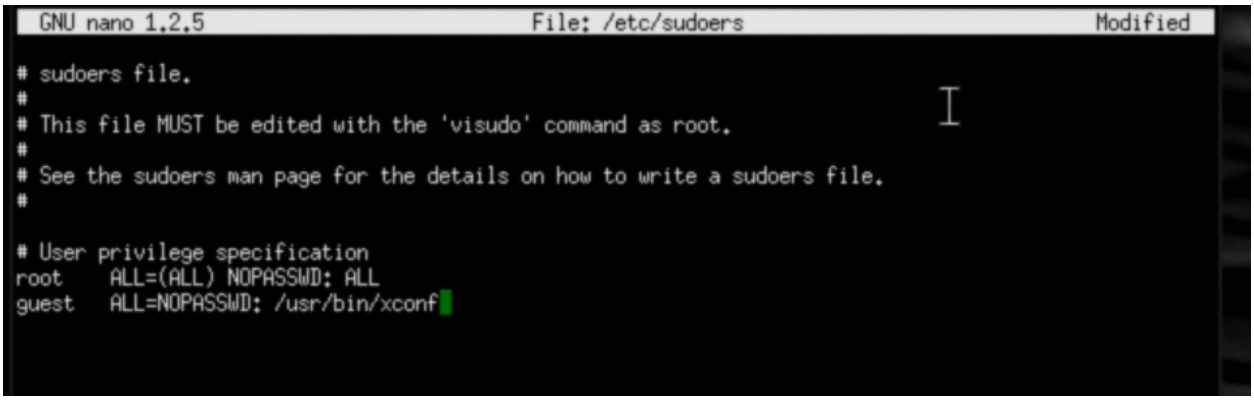
La salida indica que el usuario h4x0r no va a pedir contraseña para cualquier acción que se realice y va a poder utilizar el comando sudo para abrir cualquier aplicación del sistema.

Por lo tanto, para editar el archivo se ejecuta el siguiente comando:

Nano /etc/sudoers



Se debe de eliminar toda la línea del usuario h4x0r.



Luego presionar Ctrl + X, elegir Y, presionar enter.

Posteriormente, comprobar que los cambios fueron realizados, ejecutando el comando

Cat /etc/sudoers