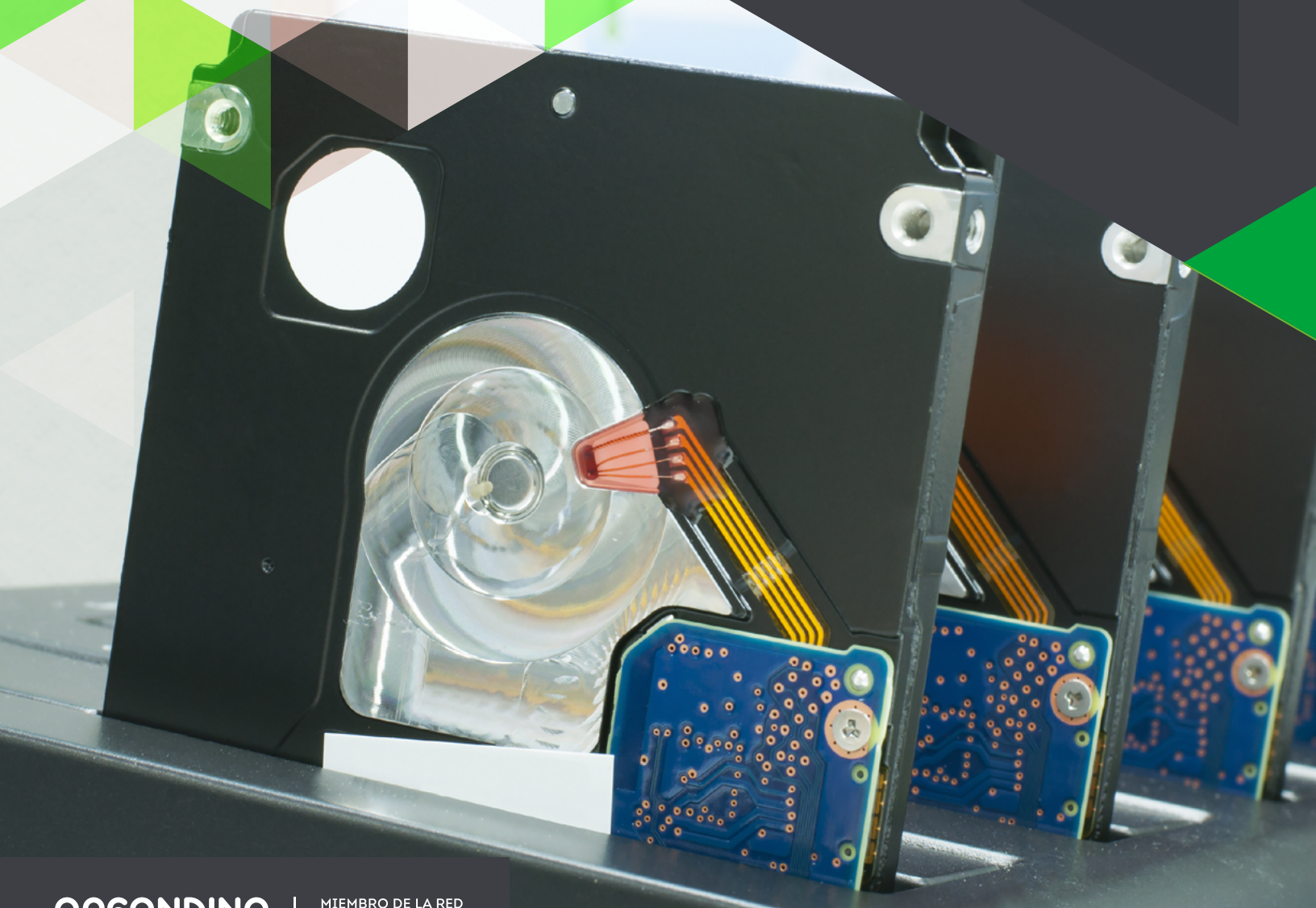
INFORMÁTICA FORENSE

Luis Francisco Lopez Urrea

EJE 4

Propongamos



AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED ILUMNO

Fuente: Shutterstock/392319763

ÍNDICE

INTRODUCCIÓN

Apreciado investigador, hasta este punto hemos revisado los conceptos, técnicas, leyes, procedimientos y herramientas que nos pueden ayudar a desarrollar una investigación de carácter digital forense. En el desarrollo del eje crítico social, dejamos enunciada una investigación relacionada con una extorsión que realiza un individuo a su expareja a través de correo electrónico, existe un alto número de investigaciones de carácter digital forense que podríamos desarrollar y son innumerables las herramientas que podemos emplear. Para una exploración más amplia de los múltiples casos relacionados con la investigación digital forense que pueden encontrarse aún pendientes de resolver, le recomiendo visitar el sitio http://honeynet.org/challenges allí podrá conocer muchas situaciones de la vida real que involucran la investigación digital forense. De igual forma le invito a realizar la lectura La dimensión internacional de la prueba digital.

En el desarrollo del presente módulo, vamos a abordar tres investigaciones relacionadas con la informática forense. Lo invitamos a observar la vídeo cápsula: Así trabajamos contra el cibercrimen en el Centro Cibernético Policial – Policía de Colombia, en la página principal del eje.

Como investigadores digitales forenses recibimos un medio extraíble obtenido en la escena de la captura de un "presunto extorsionista" por los agentes de la Fiscalía, quienes nos solicitan hacer el análisis del medio y entregar las evidencias que pueda contener junto al análisis respectivo.

Vamos a desarrollar la investigación, en la que un individuo extorsiona a su expareja sentimental con publicar algunas fotos íntimas si ella no regresa con él.

En una entidad gubernamental que administra recursos de la salud, se denuncia la perdida de una elevada suma de dinero a través de transacciones electrónicas, quien realiza la denuncia es un ingeniero informático que trabaja para la empresa. Usted hace parte de un equipo de investigación asignado por el ente encargado

Resultado de una investigación digital forense

Clonado y análisis de un disco duro o medios extraíbles (escenario 1)

Una nueva investigación forense que nos encomiendan consiste en adquirir la imagen bit a bit de una memoria USB que se encontró en la escena de un delito, en el que el presunto responsable realizaba llamadas extorsivas a personas que tenía registradas en alguna especie de lista, al llegar los investigadores no encontraron ningún listado de personas en el computador de escritorio ni listados físicos, lo único que encontraron fue una memoria USB, que se pone en cadena de custodia y es entregada para su análisis al investigador forense. Así, apreciado investigador, vamos a proceder a efectuar el análisis de la "posible evidencia" recibida:

Adquirir la imagen del disco duro o medio a analizar: como se ha reiterado en el desarrollo del módulo TENEMOS PROHIBIDO trabajar sobre los medios originales. Por ello, el primer paso luego de cumplir con los registros correspondientes en los formatos de cadena de custodia es obtener la imagen de la evidencia a través de alguna de las herramientas de las que hemos hablado; en este escenario usamos el programa Access Data FTK Imager. Ya hemos hablado en este curso de otros programas que permiten hacer el mismo trabajo, pero uno de los propósitos del curso es presentarle a usted la mayor cantidad de herramientas posibles para que pueda hacer uso de las que más se ajusten a sus necesidades. Adquirimos una réplica exacta del disco, no se trata de una imagen ISO. En este caso con el programa FTK Imager tenemos dos opciones; la versión lite que se puede montar en el medio forense (estéril) que llevó al computador víctima y que se ejecuta desde la memoria o disco en el que voy a obtener la imagen, con esta versión evitó instalar software de cualquier tipo en el equipo víctima. La versión completa se instala en la estación de trabajo forense.

En el análisis que nos ocupa, voy a trabajar desde la estación forense, así que instalo en ella el programa FTK Imager, este es un programa de pago, en un formulario de registro usted puede indicar que se trata de una descarga con fines educativos y a su correo llegará el enlace de descarga. www.marketing.accessdata.com/ftkimager3.4.2. Para este caso (copia de memoria USB) voy a desarrollar las dos tareas desde la estación forense.

Para obtener la réplica exacta de la memoria seleccionó la opción.

File (abro el menú archivo)

Create Disk (Selecciono la opción crear un nuevo disco)

Image (Escojo crear una nueva Figura de disco)

Physical Drive (Selecciono el tipo de medio del que deseo obtener la imagen).

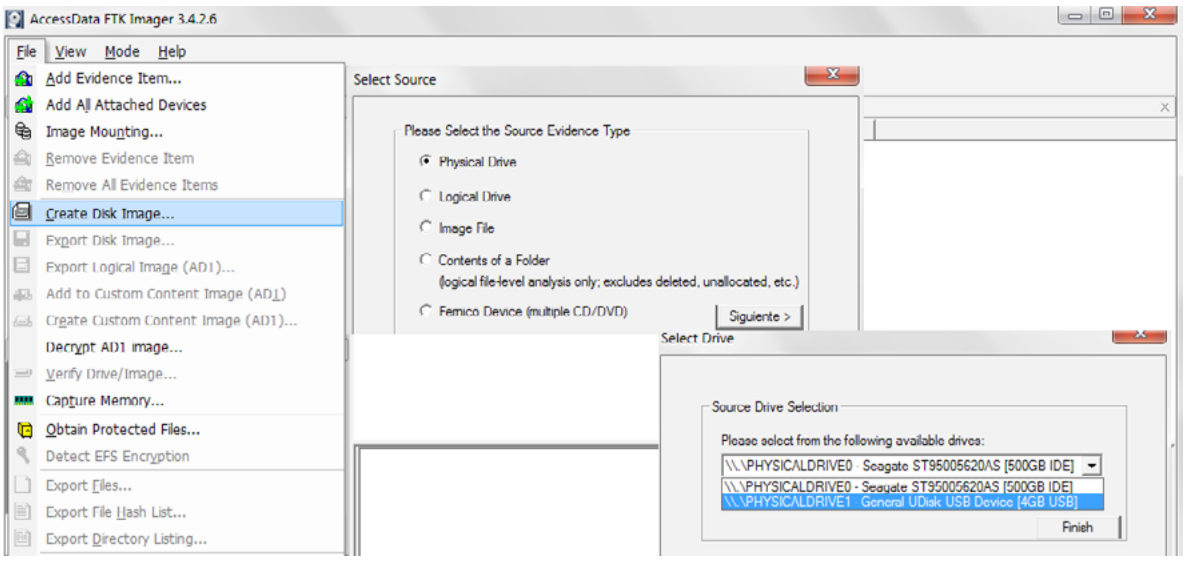


Figura 1. FTK Imager disco duroFuente: propia

Al hacer click en la opción "Finish" el programa solicita información relacionada con el destino de la copia, la opción add, pide confirmar el formato bajo el que se va a hacer la réplica, recomiendo hacer la imagen con formato RAW (copia bit a bit), en el cuadro que corresponde a la información del ITEM de la evidencia puede agregar los datos relacionados con la cadena de custodia. En este caso guardaré la copia en una carpeta que he creado en la estación forense con el número del caso (Caso1).

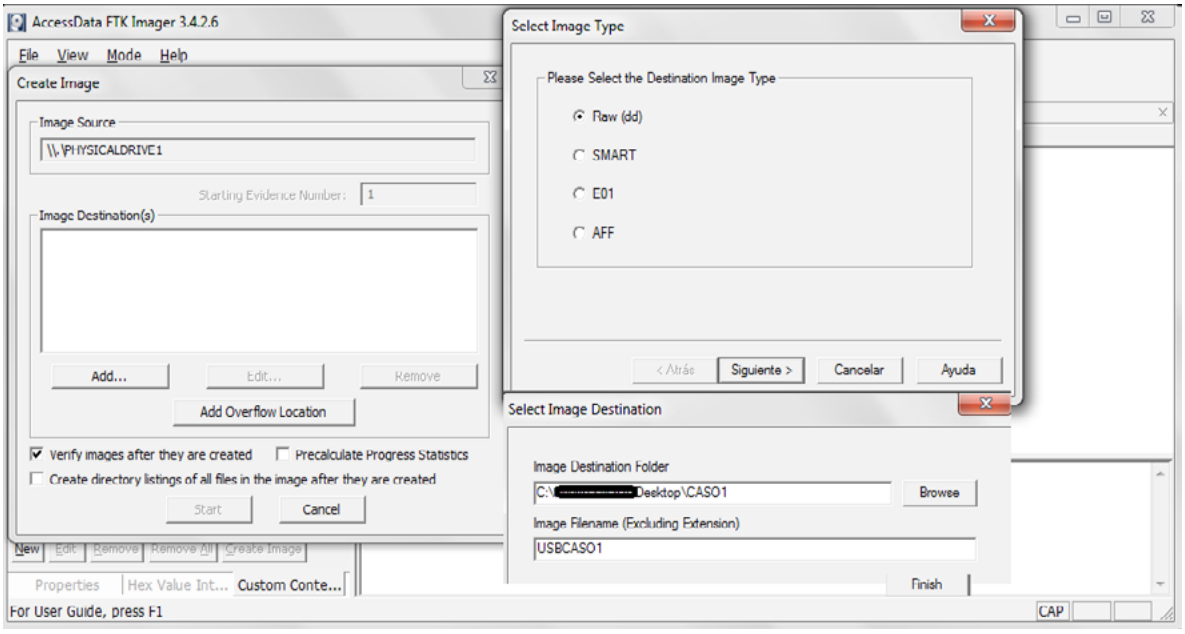


Figura 2. FTK Imager tipo de copia
Fuente: propia

Una vez que finaliza el procedimiento para obtener la imagen el programa genera el resumen SSH del archivo obtenido usando los algoritmos SHA-1 y MD5 se recomienda hacer una captura de pantalla del valor generado, además en la carpeta del caso el programa genera un archivo txt con esta información.

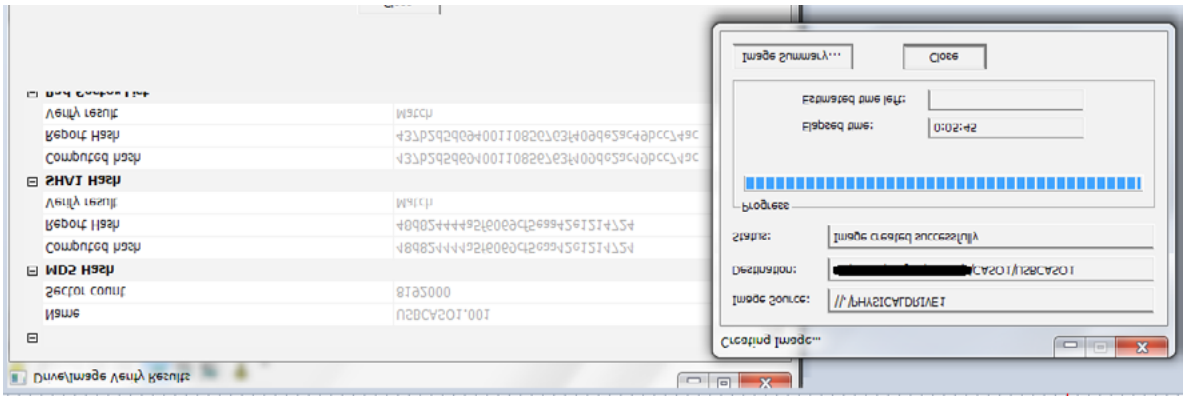


Figura 3. FTK Imager creación
Fuente: propia

Ya hemos adquirido la réplica de la memoria USB a analizar y tenemos sus valores SSH, es momento de iniciar el análisis.

Analizar el archivo de imagen adquirida.

En nuestra máquina de investigación forense procedemos a abrir el programa FTK Imager y cargar el archivo que contiene la imagen del medio obtenido para efectuar el análisis.

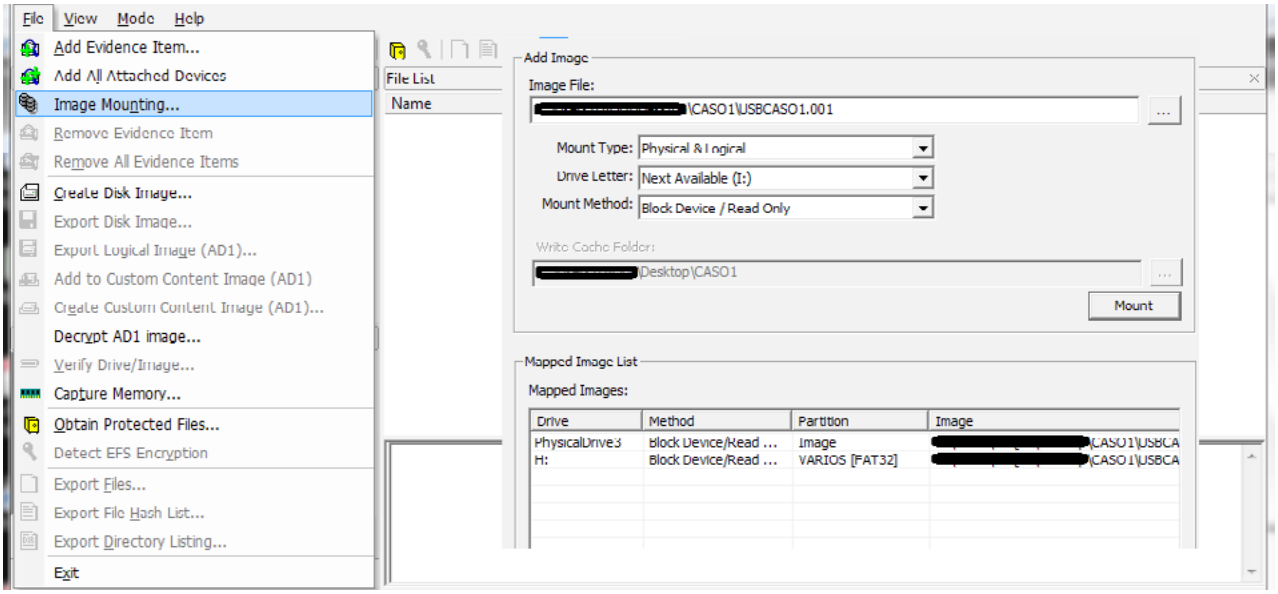


Figura 4. Montar imagen
Fuente: propia

Como se puede observar, el programa ha montado la imagen del disco que se ha adquirido, pero una vez que hemos montado la imagen, ¿qué información podemos encontrar? Esta es la pregunta que usted como investigador forense puede estar haciéndose en este momento, pues bien, con FTK no podremos analizar el contenido del medio.

Para acceder al contenido del medio que hemos capturado y proceder a buscar información relacionada con nuestra investigación, vamos a utilizar el programa WinHex, esta utilidad es un potente editor Hexadecimal que permite leer casi cualquier tipo de sistema de archivos y acceder a la información que contiene; permite acceder a archivos borrados e inclusive algunos archivos eliminados a través de un formato del medio, puede editar la memoria RAM, y procesos de memoria virtual entre muchas otras características y funcionalidades. Así, apreciado investigador, le recomiendo usar este programa una vez haya montado la imagen del medio a analizar para hacer un análisis exhaustivo.

Ya hemos montado la imagen del archivo USBCASO1 con el FTK imager, procedemos a cargar la imagen con el programa WINHEX http://www.winhex.com/winhex/hex-editor.html (ya está instalado en mi estación forense) siempre que ejecutemos el programa debemos tener en cuenta ejecutarlo en modo administrador, además, en las opciones de lectura y escritura en el medio debemos dejar marcada la opción como solo lectura (no quisiéramos que por algún error o accidente se borre información valiosa que se encuentra en el medio que estamos analizando.

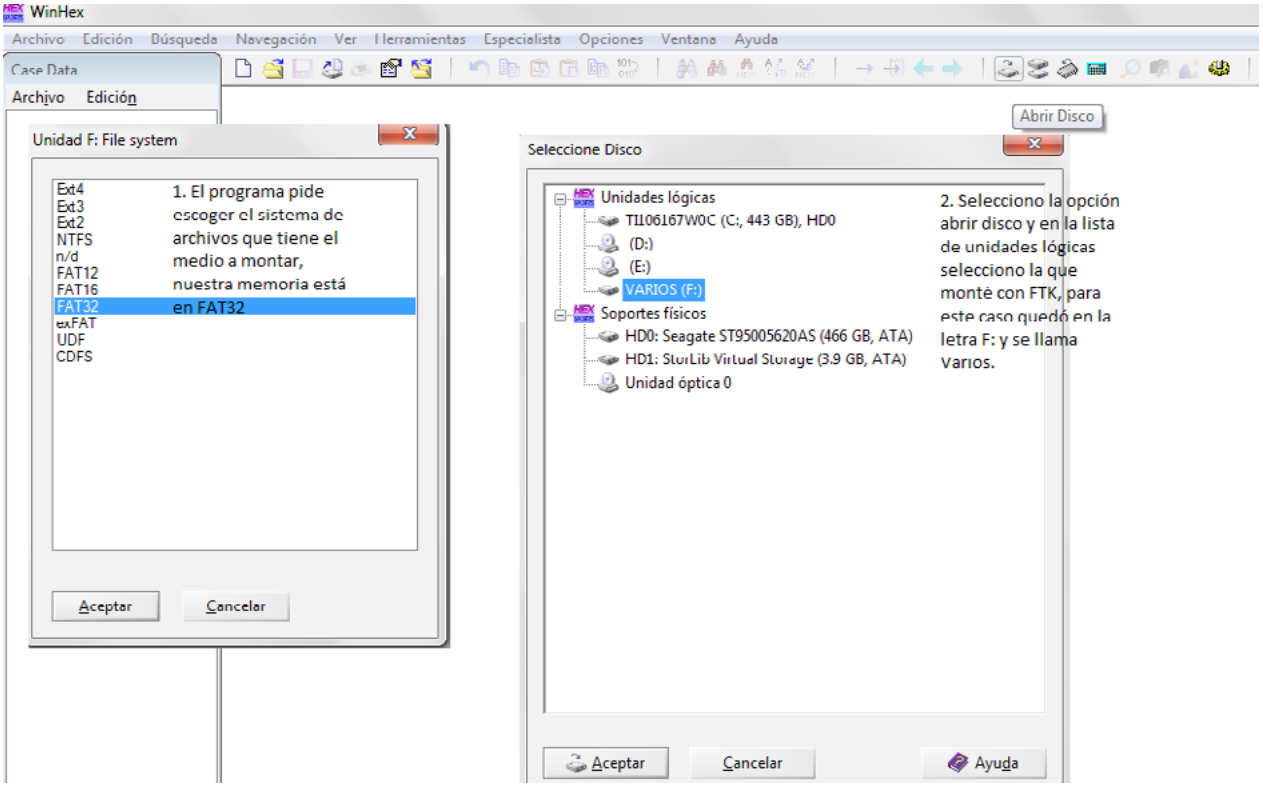


Figura 5. Seleccionar imagen a montar
Fuente: propia

El programa solicita determinar el sistema de archivos que contiene el medio a analizar, nos presenta la lista de unidades disponibles para su análisis, en nuestro caso, la unidad es lógica puesto que estamos trabajando sobre la réplica obtenida.

En mi estación forense cargué la imagen con el programa FTK Imager y quedó marcada con la letra F: el nombre de la unidad es el nombre que tenía el medio original (varios). Una vez se carga la imagen con el Winhex tendremos una vista de nuestro medio ajustada al sistema de archivos seleccionado y con las posiciones marcadas en formato hexadecimal. Seleccionamos la opción "Root Directory", el programa muestra el listado de archivos existentes en el medio, así como los archivos que han sido eliminados (aparecen con un signo de interrogación e iconos más tenues). Debemos destacar que en este análisis el proceso ha sido muy sencillo, no en todos los casos vamos a tener tantas ventajas, además el medio del que obtuve la imagen tiene un tamaño de 4GB, y hacer un análisis sector a sector sería una tarea muy compleja. Si los medios son pequeños y la imagen no se encuentra en muy buen estado será necesario calcular el offset inicial, sumar el tamaño del archivo para obtener el offset final e indicarle al programa estos valores para exportar esa área a un archivo.

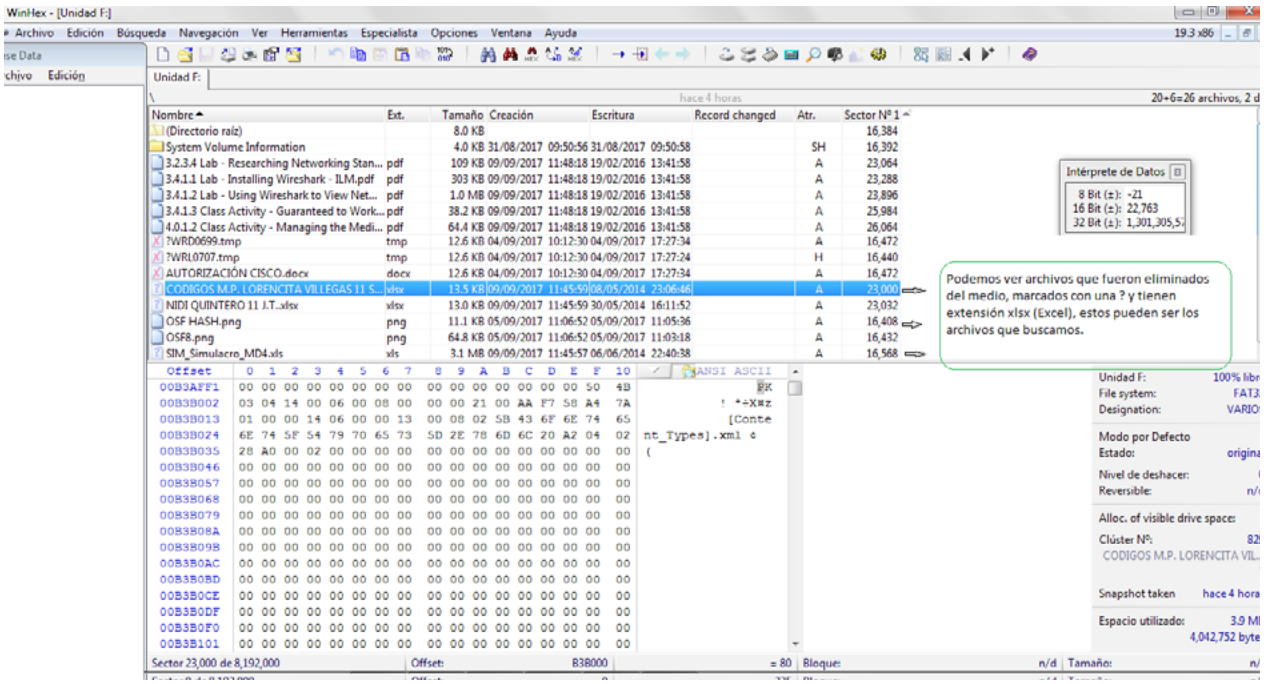


Figura 6. Win Hex captura de estructura
Fuente: propia

En la lista se observan archivos eliminados con extensión .xlsx, estas hojas de cálculo podrían contener los listados que estamos buscando, el programa señala además el sector en que se encuentra el archivo y la posición hexadecimal de su ubicación. Intento recuperar el primer archivo de extensión .xlsx. Hago click derecho en el archivo que deseo recuperar, señalo la ruta en la que deseo guardar el archivo, en mi caso lo guardo en la carpeta CASO1/ARCHIVOS y hago click en aceptar. El archivo recuperado debe aparecer en la carpeta seleccionada.

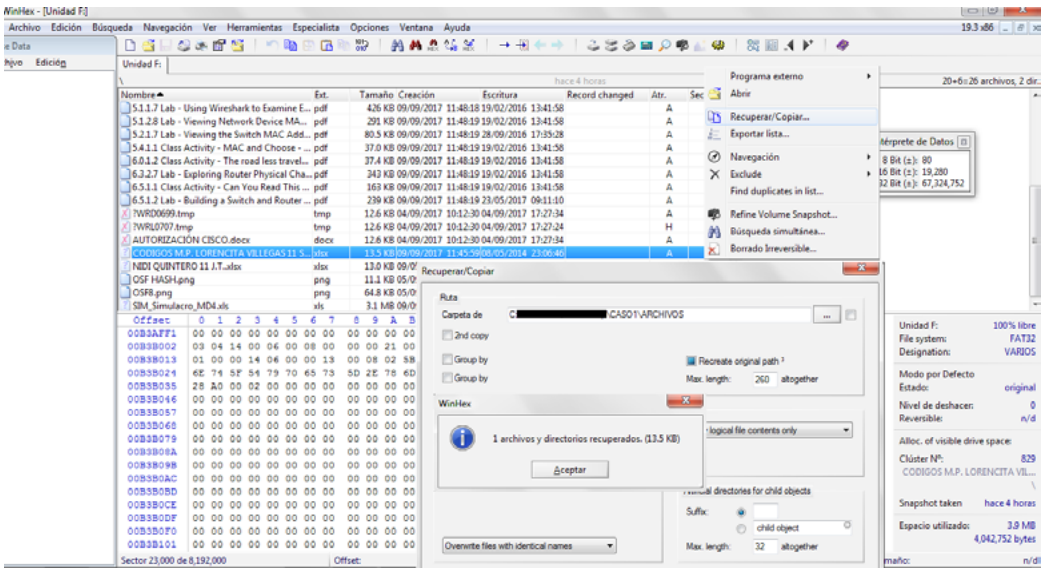


Figura 7. WinHex recuperar archivos borrados
Fuente: propia

Verifico en la ruta seleccionada que allí aparezca el archivo que he recuperado.

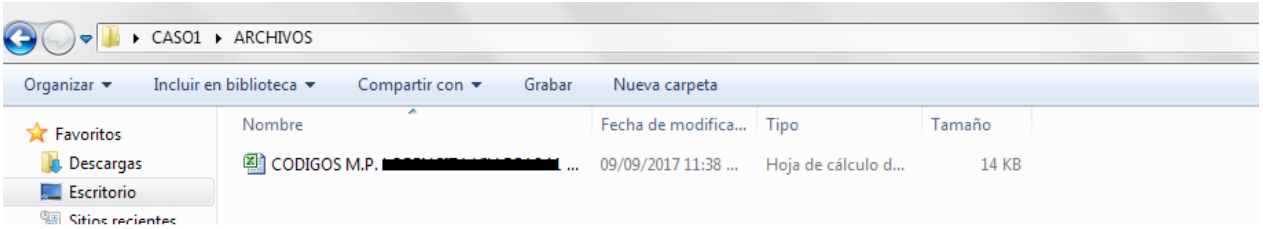


Figura 8. Verificar archivo
Fuente: propia

Abro el archivo recuperado para analizar su contenido.

	A	B	C	D	E
4	11	1	414711102	AYALA ZULETA BIBIANA ANDREA	4161
5	11	1	414711103	DIAZ LEYVA VERONICA	4161
6	11	1	414711104	FAJARDO MAZA LAURA YOLANDA	4161
7	11	1	414711105	JAIMES MARTINEZ LAURA DANIELA	4161
8	11	1	414711106	LEGUIZAMON MARTIN PAULA ANDREA	4161
9	11	1	414711107	LESMES SALDAÑA YESICA PAOLA	4161
10	11	1	414711108	LONDOÑO GALLEGO MARIA CAMILA	4161
11	11	1	414711109	MARTINEZ DIAZ LAURA VALENTINA	4161
12	11	1	414711110	MELO JESSICA ALEJANDRA	4161
13	11	1	414711111	MENDOZA AYA DAYANNA FERNANDA	4161
14	11	1	414711112	MORA SANDOVAL PAOLA ANDREA	4161
15	11	1	414711113	MORERA MONTAÑA MARIA CAMILA	4161
16	11	1	414711114	MUÑOZ PINILLA MARIA ANGELA	4161
17	11	1	414711115	MURCIA SUAREZ ANGIE STEFFANY	4161
18	11	1	414711116	ORTEGA MARTINEZ XIMENA ALEXANDRA	4161

Figura 9. Contenido del archivo
Fuente: propia

Podemos observar que el archivo obtenido contiene un listado de nombres en Excel junto a algunos códigos. Se buscaba algún listado de personas con números o datos de contacto, ¿podría ser este el archivo que buscamos?

Instrucciones

Para finalizar el análisis es necesario obtener los metadatos del archivo analizado, pero esta tarea se debe hacer, ¿antes de abrir el archivo, o la puedo hacer después? Al respecto lo invito a revisar el caso en la página principal del eje.

El programa que más opciones nos entrega cuando se trata de analizar los metadatos de algún archivo, y el de más amplio uso por los analistas forenses se llama "La Foca" (Fingerprint Organizations With Collected Archivos), desde este enlace puede descargar el programa https://www.elevenpaths.com/es/labstools/foca-2/index.html# .

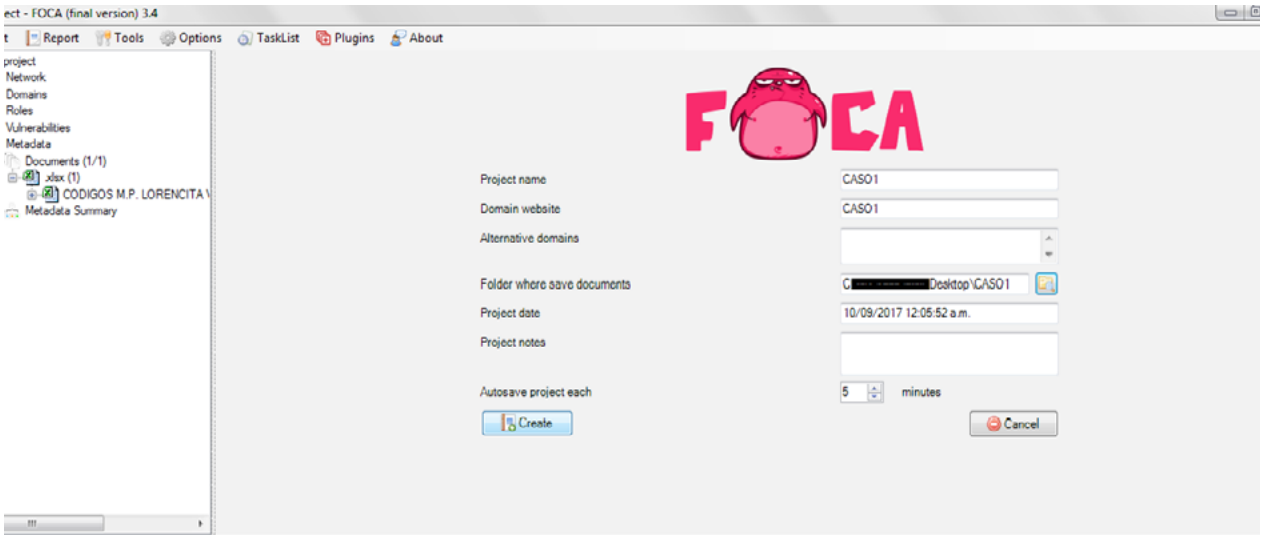


Figura 10. La Foca general
Fuente: propia

El programa solicita iniciar un nuevo proyecto, para asegurar el orden del análisis en nuestra investigación registro el nombre de nuestro proyecto "CASO1" señalo la carpeta que contiene los archivos a analizar y creo el proyecto. Una vez se crea el proyecto debo marcar el archivo a analizar. Hacemos click con el botón secundario del mouse en el área para agregar archivos y seleccionamos "add archive" agregar archivo, marco el archivo del que deseo obtener los metadatos.

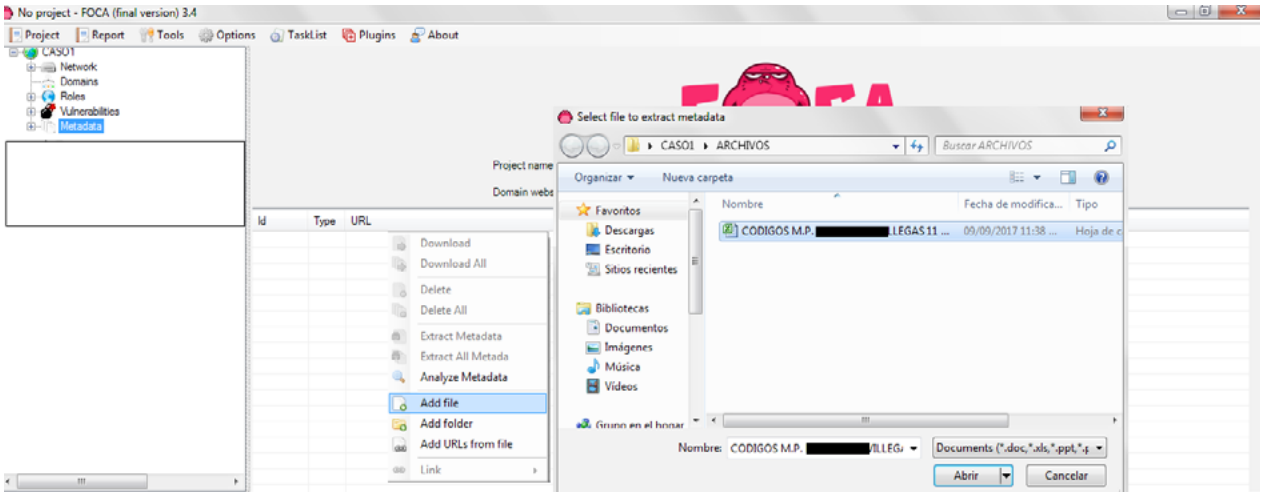


Figura 11. La Foca edición
Fuente: propia

Luego de seleccionar el archivo, hacemos click derecho sobre él y encontramos la opción "mostrar todos los metadatos" seleccionamos la opción y encontramos información que puede ser valiosa para nuestra investigación forense. Repetimos el mismo procedimiento con los otros archivos borrados que encontramos y procedemos a elaborar el informe. El cual, de acuerdo con lo propuesto por López, (2007) debe contener:

• Antecedentes de la situación (bajo qué circunstancias se está desarrollando el proceso), si la evidencia le fue entregada para su análisis, el número del caso, el código de evidencia, las características, fecha y hora de su recepción, funcionario que la entrega.

•¿Cómo se obtuvo la evidencia? Descripción de las condiciones bajo las cuales los investigadores accedieron al dispositivo o elementos entregados para su análisis.

• Descripción de la evidencia.

• Entorno del análisis (descripción de las herramientas a emplear).

• Análisis de la evidencia (descripción física y lógica de los elementos analizados, en este caso la memoria USB).

• Descripción de los hallazgos. Hash, de la imagen obtenida, hash de los archivos encontrados, metadatos de los archivos contenidos en el medio, archivos borrados, estructura.

• Conclusiones del análisis.

En los elementos que se listaron el investigador olvidó desarrollar algunos procedimientos de control relacionados con la cadena de custodia y el registro de los eventos, por favor en la bitácora que debe realizar descríbalos y realícelos. Los invito a realizar la actividad de repaso.

Instrucción

Un elemento fundamental en cualquier investigación es la elaboración del informe, de su detalle, claridad y la forma como los resultados sean expuestos depende en gran medida que la autoridad judicial, o los destinatarios del informe validen los resultados que entregamos, así durante todo el proceso de investigación se hace necesario elaborar una bitácora que se constituye en el insumo central del informe.

1. Elaborar la bitácora de eventos relacionados con las actividades que desarrolla el investigador en el caso de análisis 1 (memoria USB – llamadas extorsivas) que se expone en el desarrollo del módulo.

Bitácora

La palabra bitácora deriva del francés (bitacle) y su traducción se asemejaría a compartimento. Para ser considerado como bitácora, los datos se deben estructurar en forma cronológica y ordenada, en forma muy similar a la de un dialogo, iniciando generalmente con la fecha y la hora.

2. Tenga en cuenta los elementos que componen un informe de carácter técnico judicial para presentar como resultado de una investigación digital forense:

a. Antecedentes del incidente.
b. Recolección de los datos.
c. Descripción de la evidencia.
d. Entorno del análisis.
   • Descripción de las herramientas.
e. Análisis de la evidencia.
   • Información del sistema analizado.
      - Características del SO.
      - Aplicaciones.
      - Servicios.
      - Vulnerabilidades.
      - Metodología.
f. Descripción de los hallazgos.
      - Huellas de la intrusión.
      - Herramientas usadas por el atacante.
      - Alcance de la intrusión.
      - El origen del ataque
g. Cronología de la intrusión.
h. Conclusiones.
i. Recomendaciones específicas.
j. Referencias.

Elabore el informe técnico judicial que corresponde a la investigación del caso 2 (hombre que extorsiona a su ex pareja con algunas fotografías de carácter íntimo).

Tracking de correo electrónico (escenario 2)

Uno de los casos que se abordan en el eje sociocrítico, hace referencia a una mujer que está siendo extorsionada a través del correo electrónico por su expareja, la amenaza se materializa a través de un correo electrónico que el hombre le envía a quien fue su compañera sentimental indicando que, si no vuelve con él, hará públicas algunas fotografías íntimas de ella (adjuntas al correo). El agresor borra el correo de su buzón y las fotos de su computadora.

Desarrollo de la investigación

Para este análisis se realizan dos tareas de análisis forense:

1. Rastreo o tracking y el respectivo análisis forense de correos electrónicos.

¡Lectura complementaria!

Como apoyo nos servirá la lectura complementaria ***Interceptación de comunicaciones telemáticas***, en la página principal del eje.

2. Obtener y analizar los metadatos de archivos (en ese caso las fotografías adjuntas al correo).

Tipo de análisis: el análisis forense que se efectúa es post-mortem, como usted ya lo sabe apreciado investigador el correo electrónico es una herramienta de comunicación asíncrona, y la situación que vamos a analizar se presenta después de (es decir, ya se produjo el correo y se generó la amenaza).

Herramientas a emplear: para este análisis usaremos las siguientes utilidades:

1. Programa Foca (Fingerprint Organizations With Collected Archivos). Algo así como las huellas dactilares de las organizaciones en archivos recolectados: se usa este programa para encontrar TODOS los metadatos y la información que se encuentre oculta en cualquier archivo, que puede estar ubicado en los medios locales (equipo) o en algún sitio de Internet, muestra un amplio volumen de información que será muy útil en nuestra labor de análisis forense.

2. Programa ExifToools: utilidad que obtiene metadatos desde línea de comandos, permite obtener detalles específicos relacionados con modelo de cámara, profundidad de color y otros elementos propios de las imágenes (https://www.sno.phy.queensu.ca/~phil/exiftool/).

3. Google Maps: permite localizar un sitio en el mapa conocida su ubicación o coordenadas.

4. GeoIP en línea: utilidad que permite conocer las coordenadas exactas en relación con una dirección IP.

El caso es puesto en nuestro conocimiento por el abogado que representa a la mujer víctima de la extorsión. Usted como investigador no puede abrir el correo, debe solicitar a la víctima que abra su correo en su presencia (y si está de acuerdo) proceder con el inicio de la investigación. La mujer abre el correo y muestra al investigador su contenido:

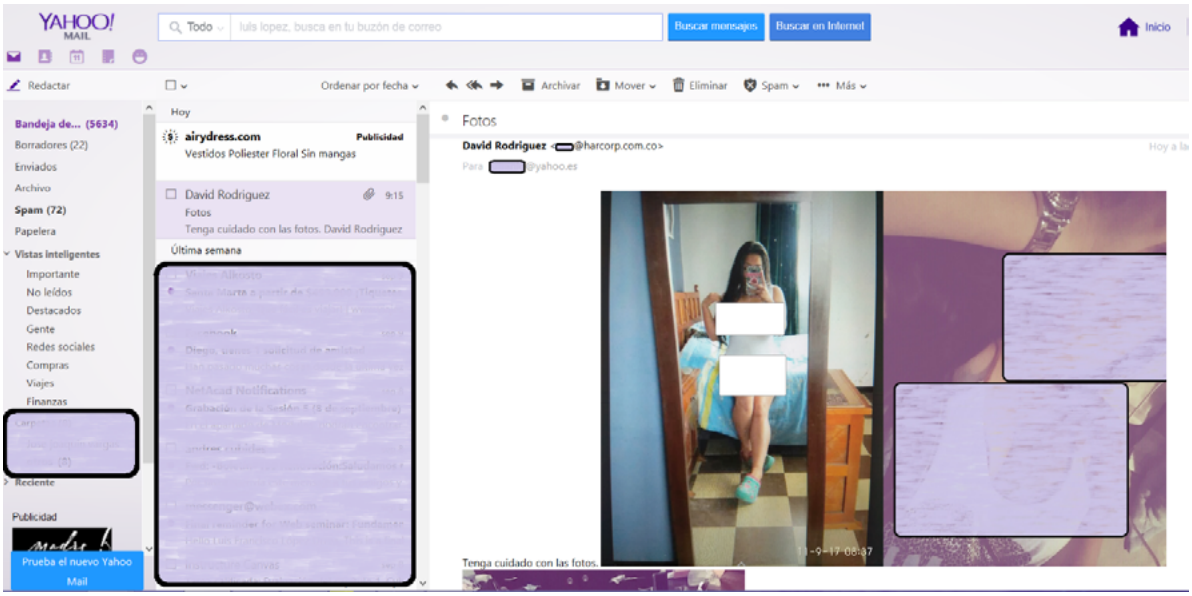


Figura 12. Correo electrónico entrada
Fuente: propia

En el cliente de correo de la afectada, en este caso Yahoo! desplegó la opción más, ver mensaje sin formato (cada cliente de correo tiene una opción para ver el mensaje original).

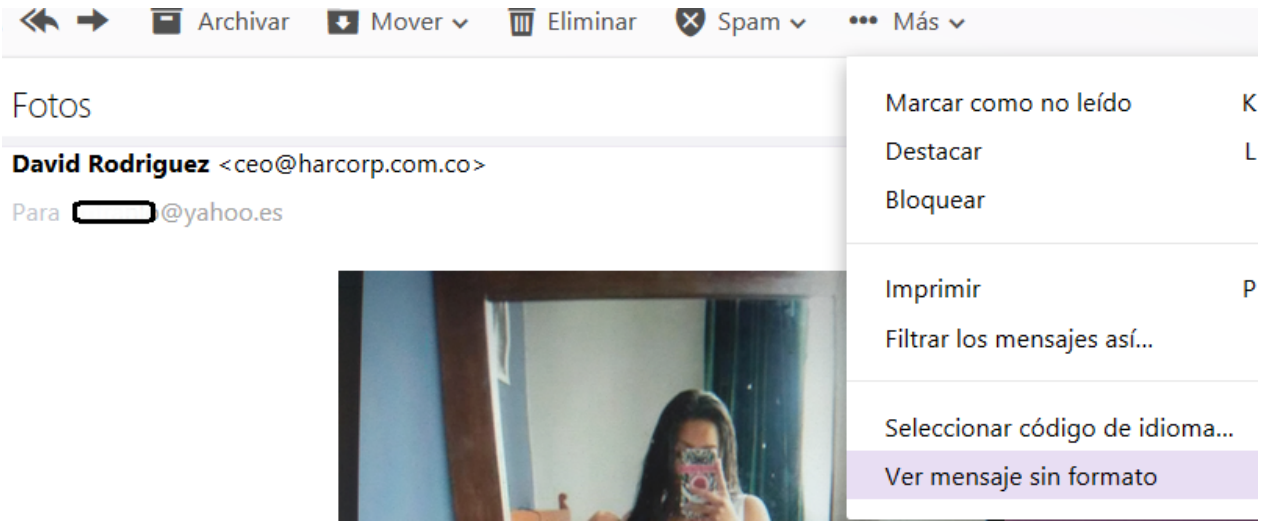


Figura 13. Correo sin formato
Fuente: propia.

Aparece una ventana con la codificación original del mensaje de correo electrónico, recomiendo guardar copia del archivo, puede copiar todo el contenido y guardarlo en un archivo de texto (no olvide la comprobación de integridad del archivo obtenido). En este caso extraje las partes con la información más útil para nuestra investigación (fecha y hora de recibido y dirección IP de origen del correo).

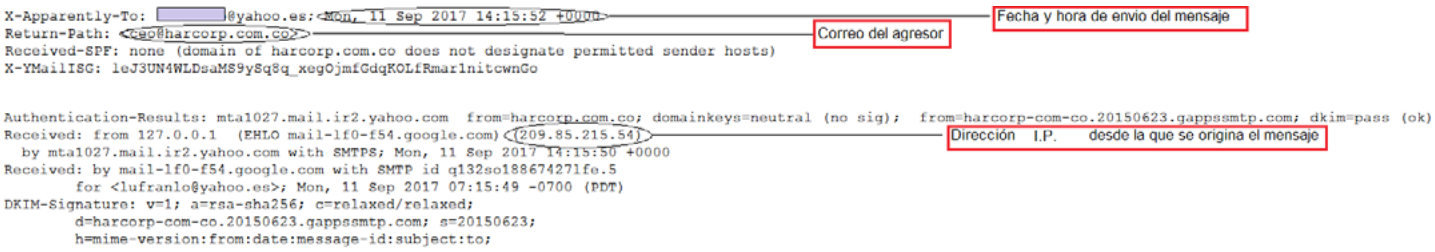


Figura 14. Direcciones en correo
Fuente: propia

Con la utilidad en línea Geoip, procedo a ubicar la localización de la dirección IP desde la cual fue enviado el correo electrónico, es posible que está información no ayude dentro de la investigación, debemos tener en cuenta que el agresor en el afán de "no dejar rastros" envío el correo desde un "Café Internet" o una red pública de un centro comercial, por ejemplo, sin embargo, ingresó en el programa la dirección IP de la que proviene el mensaje.

GeoIP2 resultados de Ciudad

Dirección IP	Código de país	Ubicación	Código postal	Coordenadas aproximadas*	Radio de exactitud	ISP	Organización	Do
209.85.215.54	US	Estados Unidos, Norteamérica		37.751, -97.822	1000	Google	Google	go

Figura 15. Geoip
Fuente: propia

Como podemos observar, el cliente de correo nos muestra la dirección IP del servidor donde se genera el correo y no la del cliente en el que se origina, así que esta información no sirve de mucho en la investigación. Ahora procedemos a descargar los archivos adjuntos del correo electrónico y vamos a analizar sus metadatos con el programa Exiftool. Descargo los adjuntos, los copio en la misma carpeta donde está el programa y ejecuto el programa desde línea de comandos.

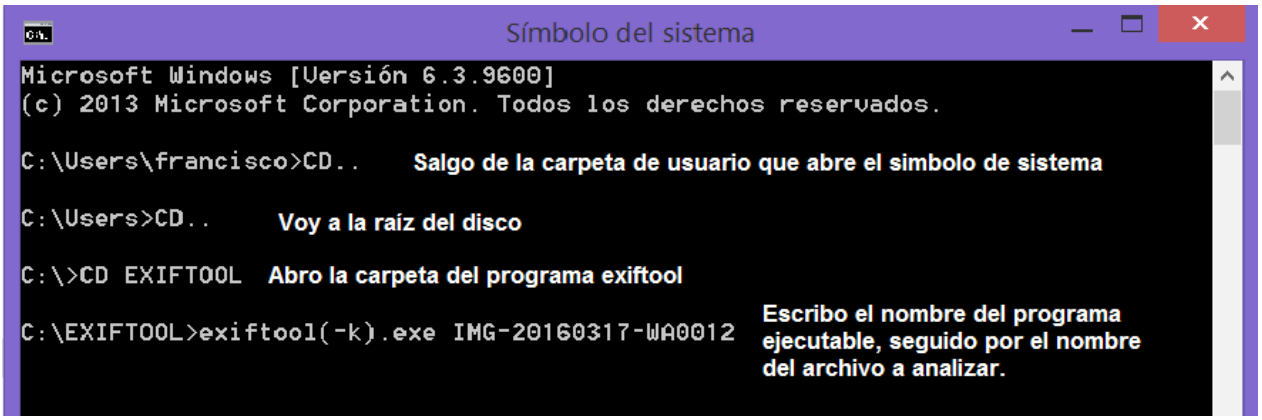


Figura 16. EXIFTool
Fuente: propia

Una vez el programa extrae y muestra los metadatos del archivo procedo a efectuar su análisis, para identificar posible información que pueda contribuir en la investigación.

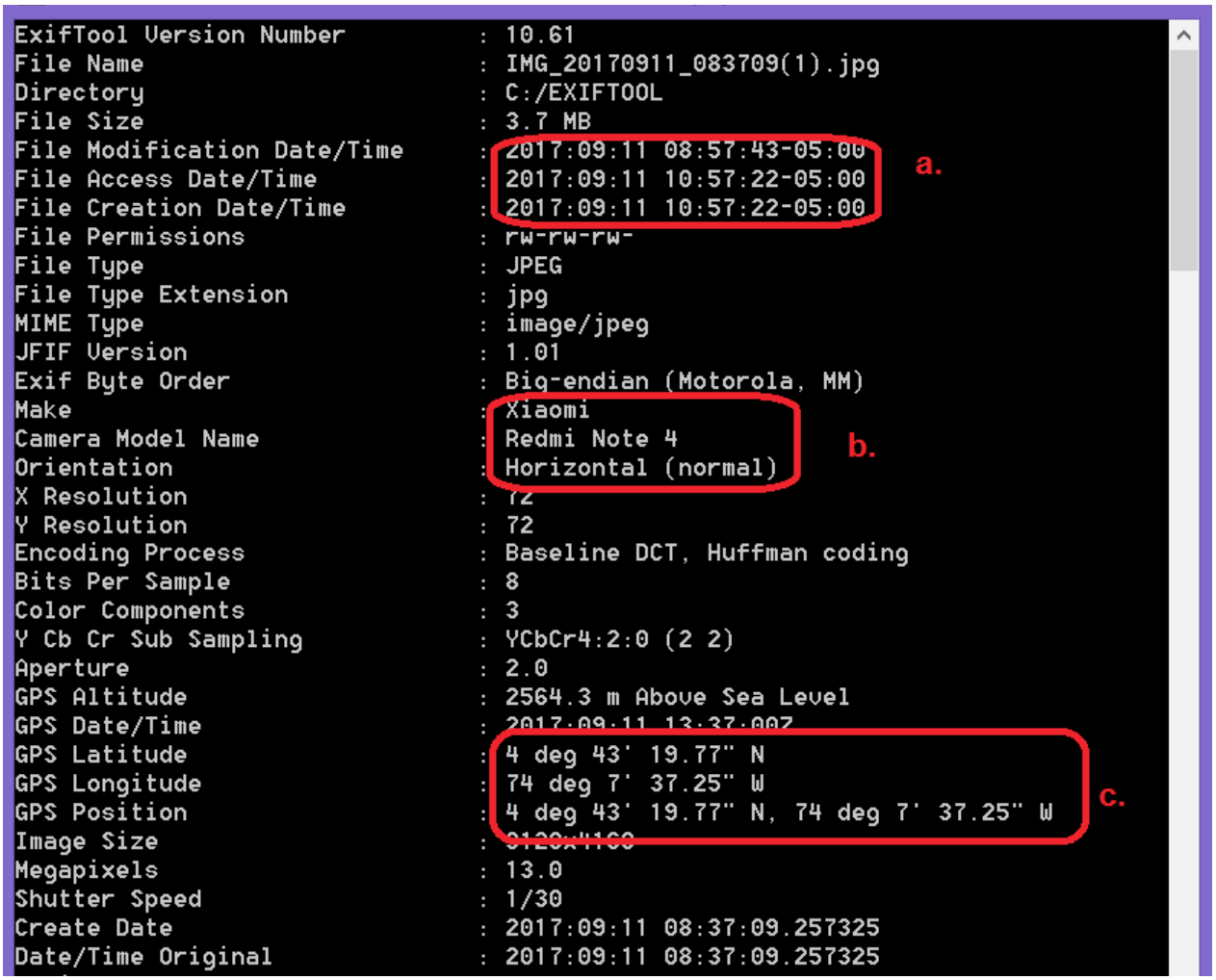


Figura 17. ExifTool coordenadas
Fuente: propia

La figura nos muestra una parte de la información que el programa Exiftool obtiene como análisis de metadatos, es muy amplio el rango de resultados que este análisis ofrece para nuestra investigación, sin embargo, en la información de esta imagen me voy a centrar en tres elementos clave (marcados en rectángulos de color rojo) que pueden servir para que el abogado contratado por la afectada inicie un proceso judicial en contra del agresor.

a. Las fechas de captura de la imagen. Si la relación entre los dos terminó hace bastante tiempo, ¿por qué la fecha de las imágenes es tan reciente? El agresor no obtuvo estas imágenes con el consentimiento de la afectada. ¿Tomo las fotografías de su computadora u otro dispositivo electrónico de ella al que accedió a través de una contraseña que conocía? ¿Se trata entonces de un abuso de confianza con fines extorsivos?

b. El modelo del celular y la cámara con que tomo las fotografías: el agresor accedió a las imágenes íntimas de la afectada y tomó desde su celular las fotografías de las imágenes, en los metadatos se puede apreciar la marca del dispositivo y su modelo. Así, en una eventual denuncia se puede solicitar al juez que use el celular del agresor como prueba válida, casi con absoluta certeza vamos a encontrar que el celular que presenta coincide con el dispositivo con el que fueron tomadas las fotografías.

c. Los datos del GPS asociados a la captura de las imágenes: para este caso las coordenadas que corresponden a la captura de las imágenes nos pueden proporcionar información respecto del lugar exacto en donde se encontraba el agresor en el momento de tomar las fotografías, es decir podemos conocer si lo hizo directamente en su domicilio, en su trabajo, en la casa de la afectada. Para esta información vamos a emplear una utilidad en línea asociada a Google Maps, llamada www.coordenadasgps.com, allí ingresamos las coordenadas obtenidas en grados. Latitud: 4° 43′ 19.77″ Longitud: 74° 7′ 37.25″. Cuando hemos introducido los datos hacemos click en obtener dirección y esperamos los resultados. La imagen de Google Maps nos devuelve la información requerida:

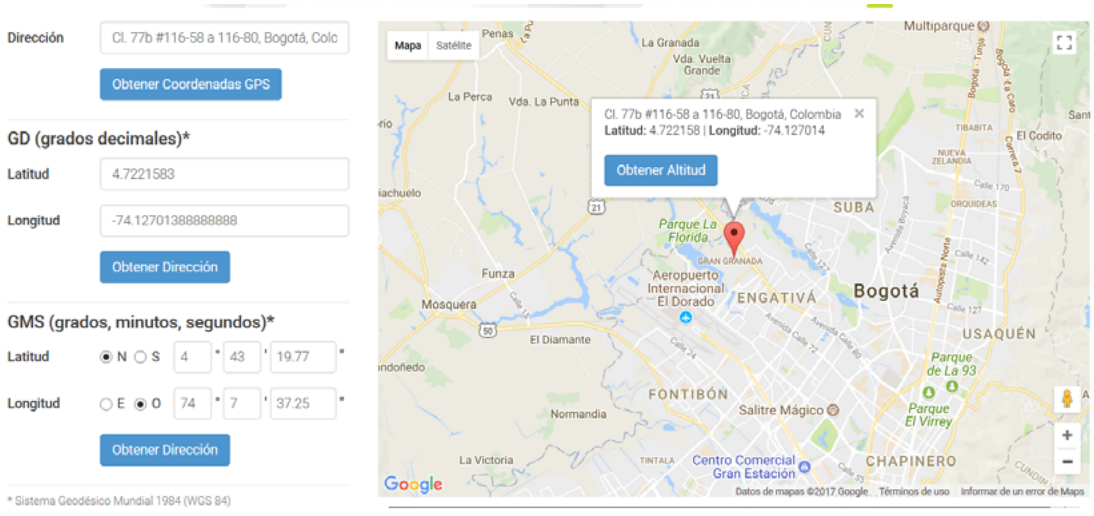


Figura 18. Google Maps coordenadas
Fuente: propia

En el escenario que he planteado, la dirección del presunto agresor, es entregada con un margen de error máximo de 50 metros por el programa Google Maps a través de la utilidad de ubicación de coordenadas; así y a partir del conocimiento que tiene la víctima de la información personal de su expareja ella nos informa que se trata del lugar en el que vive su expareja, información que puede ser cotejada en un eventual proceso judicial a través del recibo de un servicio público o la información de arraigo que debe suministrar el agresor en caso de ser notificado del inicio de una investigación.

La información que recabamos en este pequeño ejercicio servirá entonces para que el representante de la víctima demuestre ante un juez que ¿en efecto el ex compañero sentimental de la afectada es el responsable de las amenazas que ella está recibiendo a través de su correo electrónico? Recuerde apreciado investigador que en el desarrollo del eje sociocrítico hablamos de la Ley de Protección de Datos Personales, Ley 1581 de 2012, que en su artículo 5° establece los datos sensibles, dentro de ellos se encuentra la vida "sexual e íntima" de las personas, y prohíbe su publicación sin la autorización del titular de los derechos (la persona que aparece en la fotografía). Así, el Código Penal sanciona este tipo de publicaciones sin el consentimiento expreso del titular de los derechos, con penas privativas de la libertad de hasta doce (12) años. El caso que investigamos puede tipificar dos delitos, la presión que ejerce la expareja de la mujer para que regrese con él (extorsión) y la publicación de datos sensibles sin la autorización del titular de los derechos. Al respecto le invito a realizar la actividad de repaso 2:

Instrucción

El trabajo del investigador digital forense cuando se trata de analizar un delito cometido por un atacante experto en informática puede suponer un reto muy importante para el investigador digital forense, y no siempre los resultados serán satisfactorios.

1. Elaborar la bitácora de eventos relacionados con las actividades que desarrolla el investigador en Análisis de lavado de activos o robo de información por un agresor experto en informática y técnicas antiforenses (escenario 3).

2. El informe ejecutivo.

Este informe consiste en un resumen del análisis efectuado, pero empleando una explicación no técnica, con lenguaje común, en el que se expondrá los hechos más destacables de lo ocurrido en el sistema analizado. Constará de pocas páginas, entre tres y cinco, y será de especial interés para exponer lo sucedido a personal no especializado en sistemas informáticos, como pueda ser el departamento de Recursos Humanos, Administración, e incluso algunos directivos. En este informe deberá, donde se describir, al menos, lo siguiente:

- Motivos de la intrusión.
- Desarrollo de la intrusión
- Resultados del análisis.
- Recomendaciones.

Elabore el informe ejecutivo (máximo tres hojas) en el que explique el desarrollo de las actividades de investigación que corresponden al escenario 3 (agresor experto en informática).

Análisis de lavado de activos o robo de información por un agresor experto en informática y técnicas antiforenses (escenario 3)

Video

Para comenzar observe la videocápsula ***Bienvenidos a "Hackerville", la capital mundial del cibercrimen | Sinfiltros.com***, en la página principal del eje.

Como parte del equipo de investigación forense, debemos adelantar varias tareas:

a. Obtener la información relacionada con la fecha, hora y condiciones de las transacciones que se relacionan con la "pérdida" de dinero de la entidad; previa orden judicial el banco entregó los detalles relacionados con transacciones que en apariencia no tenían un destino que coincide con el patrón habitual de la entidad, se puede comprobar que la suma total de dinero que se "perdió" corresponde a transacciones electrónicas "transferencias a otras cuentas". No se conocen los destinatarios de las cuentas a las que fue transferido el dinero. Se realizaron veinte transacciones en total, el banco entrega las fechas y horas de las transacciones. ¿Qué tipo de investigación forense se realiza?

b. Identificar dentro de la red corporativa; efectuar una auditoría para obtener todos los logs de equipos, actividades y otras situaciones que puedan implicar que la red haya sido objeto de un atacante externo que haya suplantado un equipo del dominio, y haya realizado la transacción. La revisión del registro de los firewalls no muestra un intento de escaneo o reenvío de puertos, situaciones comunes cuando algún agresor externo intenta ingresar a nuestra red corporativa.

¡Lectura complementaria!

Antes de continuar le invito a realizar, en la página principal del eje, la lectura Registro de dispositivos y registros remotos desde la página 361 a la 400.

Escaneo de puertos lanzado desde la aplicación NMAP, el registro de todas estas actividades queda guardado en el firewall de la red.

```
Starting Nmap 5.21 ( http://nmap.org ) at 2012-10-24 15:29 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0072s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0F:CB:9F:F6:E1 (3Com)

Nmap scan report for repetidor.mshome.net (192.168.1.2)
Host is up (0.0023s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  unknown
3389/tcp open  ms-term-serv
5800/tcp open  vnc-http
5900/tcp open  vnc
```

Figura 19. NMAP
Fuente: propia

La anterior imagen corresponde al scan de los puertos de un host en una red, los puertos que se muestran abiertos pueden ser redireccionados para obtener acceso al host. Cuando una actividad de este tipo se desarrolla el registro de eventos del firewall conserva la evidencia.

all log entries.Max(2000)

	If	Rule	Source	Destination
16:17:46	LAN	lan address (1491712150)	192.168.80.250:49168	192.168.80.50:2
16:17:46	LAN	Default allow LAN to any rule (100000101)	192.168.80.250:49167	192.168.80.50:2
16:17:46	LAN	Default allow LAN to any rule (100000101)	192.168.80.250:49166	192.168.80.50:2
16:17:46	LAN	Default allow LAN to any rule (100000101)	192.168.80.250:49165	192.168.80.50:5
16:17:46	LAN	Default allow LAN to any rule (100000101)	192.168.80.250:49164	192.168.80.50:3
16:17:46	LAN	lan address (1491712150)	192.168.80.250:49163	192.168.80.50:8
16:17:46	LAN	Default allow LAN to any rule (100000101)	192.168.80.250:49162	192.168.80.50:1
16:17:46	LAN	lan address (1491712150)	192.168.80.250:49161	192.168.80.50:4

Figura 20. Firewall
Fuente: propia

En este caso se detectan múltiples intentos de escaneo de puerto desde el equipo 192.168.80.250/24 al equipo 192.168.80.50/24, ¿tiene sentido el resultado de esta captura? ¿Por qué razón un equipo dentro de mi propia red hace un scan de puertos a otro dispositivo dentro de la misma red? Usted procede a investigar el equipo identificado con la IP 192.168.80.50 y no encuentra ningún software instalado o eliminado de forma reciente que desarrolle esta actividad. Este puede ser considerado un primer hallazgo. Pero no lo olvide apreciado investigador, de lo primero que debe desconfiar es de lo evidente. Sin embargo, una tarea sencilla que usted puede realizar es comparar las fechas y horas de las transacciones fraudulentas con las fechas y horas de los registros del Firewall, tal vez pueda encontrar coincidencias.

a. Analizar las políticas de la red corporativa y establecer si existen reglas y restricciones para el acceso a transacciones financieras desde las estaciones; ¿Qué tipo de análisis se efectúa sobre las estaciones? ¿De qué elementos se hace necesario capturar imágenes? Una vez que se analizan los datos no se encuentra evidencia de software extraño o actividades sospechosas o ilícitas efectuadas a través de las estaciones, aunque como es obvio se encuentran rastros de transacciones en línea como pago a proveedores, servicios públicos, transferencias a regiones.

¡Lectura complementaria!

Para profundizar lo invitamos a realizar la lectura de las páginas 455-494 de ***Otros medios de investigación tecnológica en el proceso penal***, en la página principal del eje.

b. Se hace verificación del correo electrónico corporativo de todos los trabajadores de la entidad; no es necesario solicitar autorización de los trabajadores, puesto que el correo electrónico corporativo es una herramienta de propiedad de la empresa puesta a disposición del trabajador; por tal razón, los funcionarios no pueden argumentar alguna violación de la privacidad o intimidad. De todas formas, se notifica a todo el personal de las actividades que se van a desarrollar, algunos trabajadores proceden a eliminar correos de carácter personal o que ellos consideran sensible de sus buzones de correo. Sin embargo, la auditoría no se efectúa buzón por buzón, sino que se hace de forma directa sobre el servidor de correo, así a pesar de haberse eliminado correos de las bandejas de entrada o enviados de los buzones personales, en el servidor se conservan por política copia de todos los correos enviados y recibidos. Como resultado de la auditoría del correo electrónico en el servidor no se encuentra en apariencia ninguna información relacionada con la "pérdida" del dinero, no obstante, llama nuestra atención como investigadores forenses un mensaje de correo electrónico que contiene la imagen de una mascota que en varias ocasiones ha sido enviado sin que el correo haya recibido algún tipo de respuesta.

c. Análisis de los archivos sospechosos obtenidos: Como investigadores forenses descargamos la imagen para efectuar su análisis, esta es la imagen que descargamos del servidor:

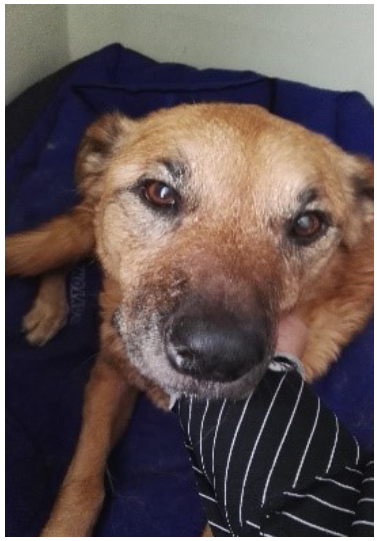


Figura 21. Luna
Fuente: propia

A simple vista, aparece una mascota con una mano en su parte inferior, pero aparece la primera pregunta que debe orientar nuestro análisis: ¿la imagen contiene algo?, como investigadores procedemos a analizar los metadatos con el programa "La Foca" a continuación un resumen de los resultados.

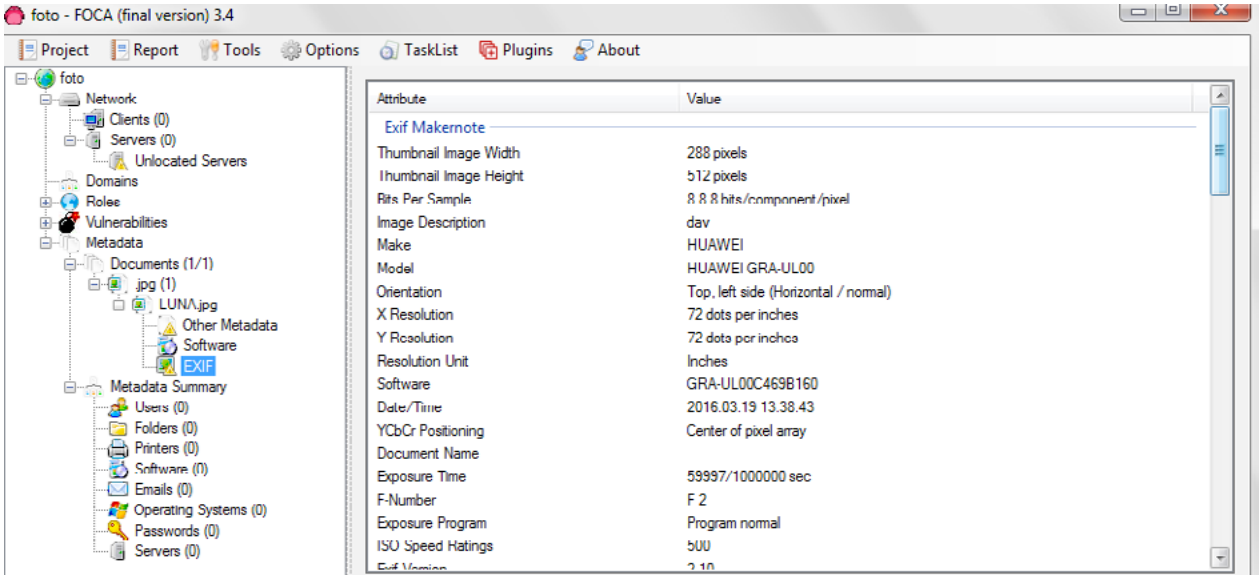


Figura 22. Metadatos luna
Fuente: propia

A simple vista no encontramos nada extraño en el archivo, sin embargo por las características del mensaje procedemos a efectuar un nuevo análisis con otra utilidad, en este caso el programa StegSecret http://stegsecret.sourceforge.net/.

¿Y qué hace este programa? Desde tiempos inmemoriales el hombre ha buscado técnicas para hacer llegar información valiosa a otras personas en otros lugares sin que esta sea detectada, la técnica se conoce bajo el nombre de esteganografía. Miles de años antes de los computadores el hombre ya usaba esta técnica que consiste en ocultar algo dentro de un objeto al que se denomina "portador", con la llegada de los computadores, miles de aplicaciones gratuitas y de pago nos ofrecen la posibilidad de ocultar un mensaje o archivo que queremos ocultar dentro de otro llamado "portador", así el programa StegSecret aplica diversos algoritmos para tratar de identificar la existencia de información oculta dentro de un archivo "portador", una de las técnicas esteganográficas más usada es la "EOF", ocultar información al final del archivo portador o LSB, reemplazar el bit menos significativo de cada patrón de bits para poner allí parte del archivo o mensaje a ocultar. Para obtener mayor información al respecto consulte la lectura recomendada (Lectura recomendada esteganografia).

El programa StegScan se basa en un archivo autoejecutable que se encuentra compilado en lenguaje JAVA y puede ser usado en ordenadores tipo Linux o Mac sin ningún inconveniente.

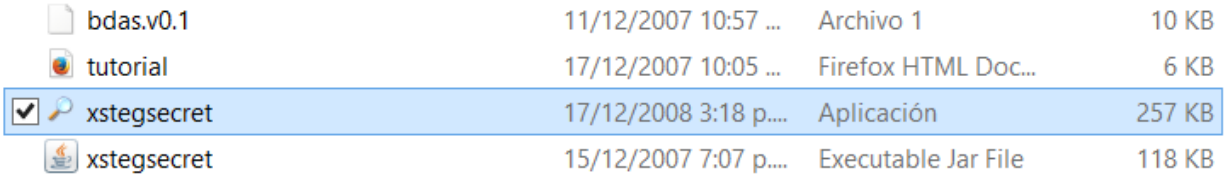


Figura 23. Esteganografia StegSecret
Fuente: propia

Seleccionamos el archivo a analizar, para esto primero debemos seleccionar el archivo de la carpeta, el programa pone la carpeta completa en la lista una vez allí, se vuelve a seleccionar el archivo y se da click en la lupa para iniciar la búsqueda.

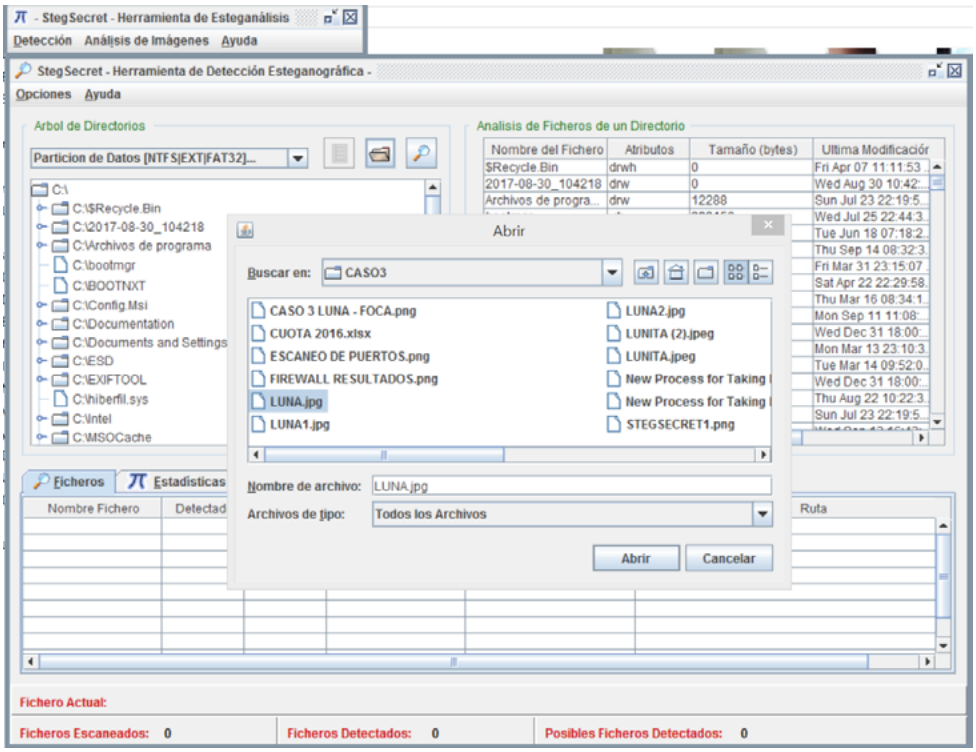


Figura 24. Resultados análisis esteganográfico
Fuente: propia

Una vez hecha la búsqueda el programa arroja los resultados.

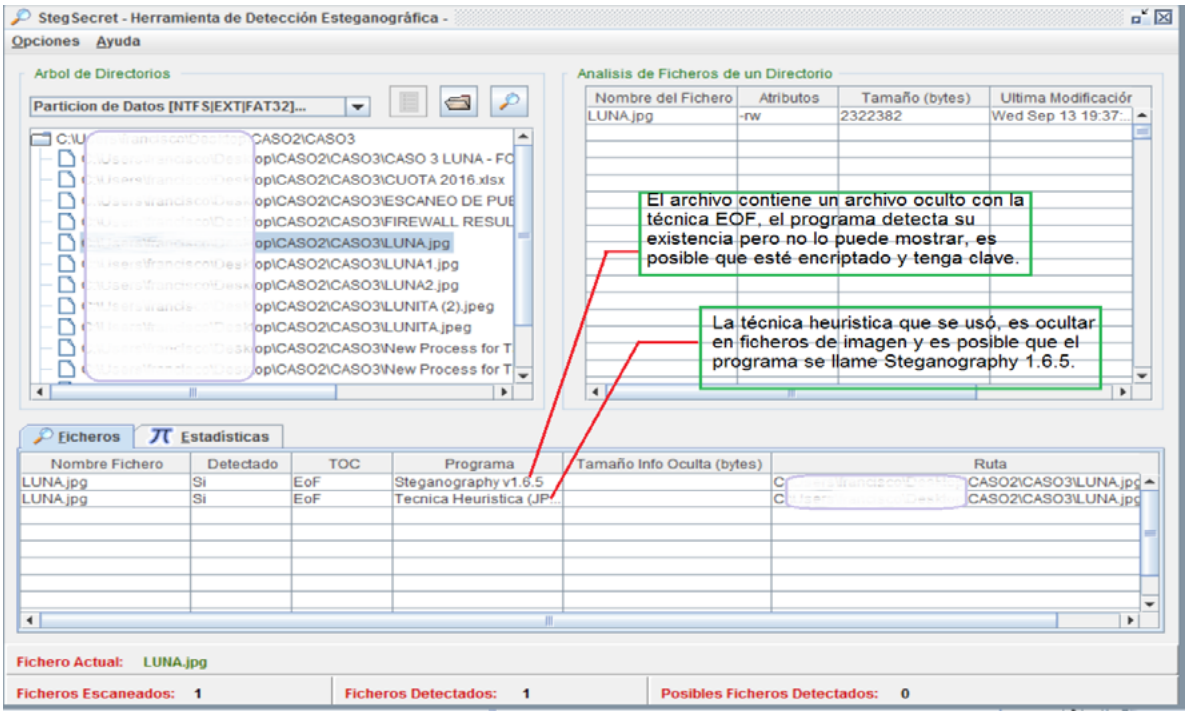


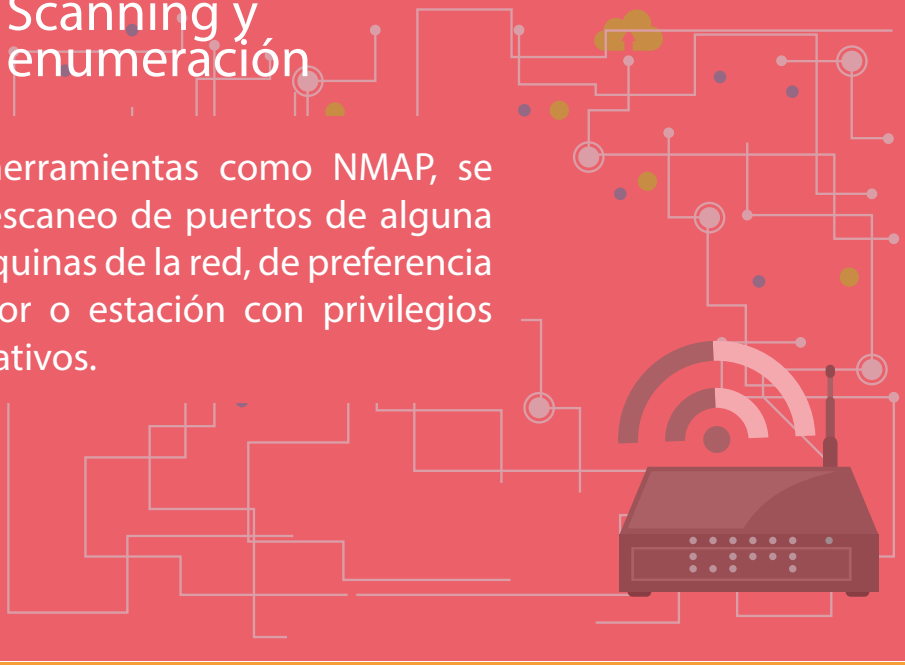
Figura 25. Análisis resultados esteganográfico
Fuente: propia

Hemos encontrado la respuesta a nuestra primera y segunda preguntas: ¡El archivo ESCONDE ALGO! Y es posible que el programa con el que se ocultó la información se llame Steganography versión 1.6.5; será parte de nuestro trabajo como investigadores digitales forenses buscar alguna herramienta que nos ayude a determinar, al menos, qué fue lo que se ocultó en este archivo.

Por un momento quiero mostrarle desde el extremo del atacante experto en informática, cuál fue el procedimiento que empleó para cometer el ilícito sin dejar en apariencia rastros que conduzcan a los investigadores a obtener las evidencias que lo relacionen con el delito. A continuación, observemos la siguiente infografía.

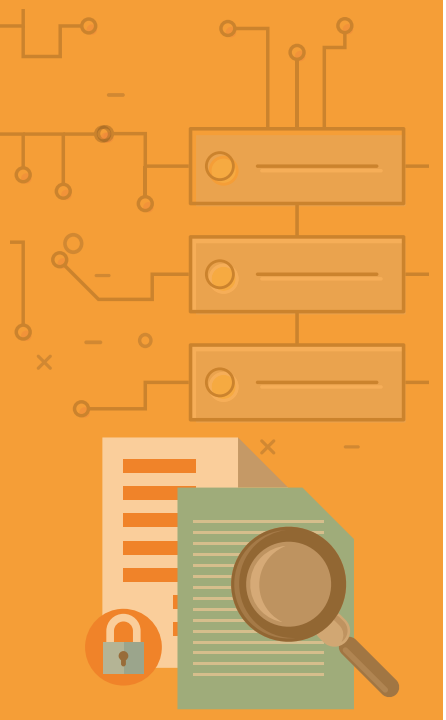
.2 Scanning y enumeración

Usando herramientas como NMAP, se hace un escaneo de puertos de alguna de las máquinas de la red, de preferencia un servidor o estación con privilegios administrativos.



.3 Análisis de vulnerabilidades

Puede ser mediante el mismo programa Meta Sploit puede intentar ingresar al puerto de llamado de procedimientos remoto abierto para intentar acceder al servidor como usuario.



.4 Ejecutar instrucciones desde mi equipo

Con programas como Meterpreter, puedo ejecutar instrucciones desde mi equipo atacante en el servidor para mostrar bases de datos entre otras.

.5 Post explotación

El atacante puede usar las mismas herramientas usadas en el ataque para tratar de eliminar del registro las entradas que dan cuenta del ingreso de un equipo desde una red externa.

Figura 26. Cronología de un ataque a una red de datos
Fuente: propia

1. Es un atacante experto en informática que simuló un ataque externo a un servidor dentro de la empresa, por tal razón los registros en el firewall que muestran el escaneo de puertos desde un equipo dentro de la red a otro equipo que hace parte de la misma red esta técnica se conoce como Port Forwarding y se usa para hacer un proceso llamado Pivoting (esto puede confundir al analista). Para este fin existen múltiples herramientas que se pueden ejecutar desde versiones LIVE CD o máquinas virtuales. Una de las suites que más utilidades reúne para atacar redes desde afuera y obtener acceder a equipos que están dentro de la red para robar información o hacer transacciones fraudulentas se llama Kali Linux. Aquí una simulación de un ataque realizado con Kali Linux a una red.

Port Forwarding

Reenvío de puertos, se usa esta técnica para acceder a un equipo dentro de una red a la que no tengo acceso, desde el exterior para redirigir un puerto abierto en un equipo a otro equipo "víctima" sin que el equipo víctima lo detecte.

Pivoting

Técnica de hackers que permite que una vez acceda a una máquina dentro de una red pueda moverme a otro equipo dentro de la red para acceder a los sistemas que necesite intervenir, por lo general se acompaña del port forwarding.

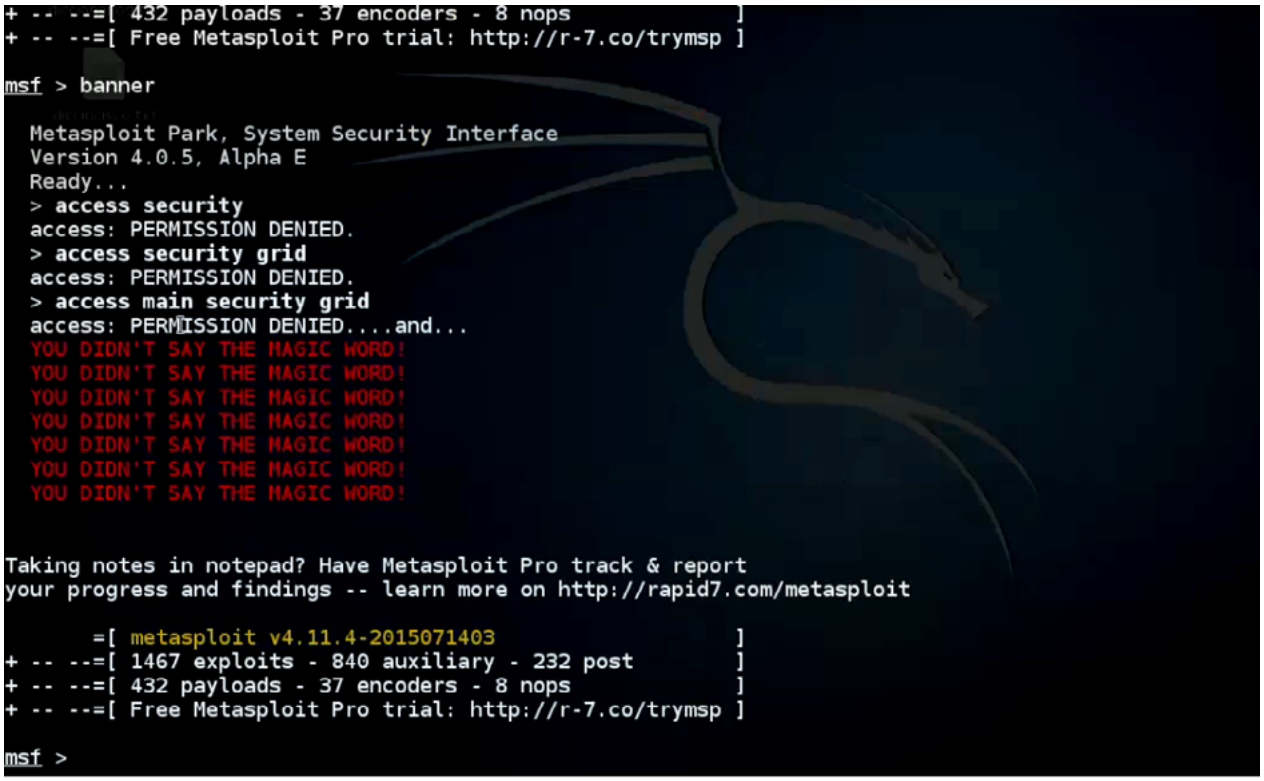


Figura 27. Metasploit
Fuente: propia

En esta imagen a través de una utilidad llamada metasploit se intenta acceder a un servidor con Windows server ubicado en una red a la que no tengo permiso de acceso. Uno de los programas incluidos en la suite y que en apariencia el atacante empleo para acceder a la red de la empresa víctima se llama "meter preter".

1. ¿Pudo nuestro agresor "interno" simular un ataque desde el exterior de la red para despistar a los investigadores? No olvide que los equipos de la red del área financiera no son accesibles por los demás empleados de la empresa, es posible que alguien desde adentro haya simulado un ataque externo pero en efecto haya desarrollado un ataque desde dentro para acceder a los equipos del área financiera que son los únicos que cuentan con los permisos de acceso a las transacciones financieras.

Video

Ahora veamos en la página principal del eje, la videocápsula *Documental sobre internet oculta*.

2. Instaló varias máquinas virtuales en su ordenador para correr todas las utilidades de explotación y acceso, y luego las borró del ordenador de forma segura. Las suites de esteganografia y encriptación moderna incorporan utilidades como el programa "ERASER" (https://eraser.heidi.ie/download/) que borra de forma segura cualquier archivo del disco e inclusive del archivo de paginación de la memoria sin que ninguna herramienta forense pueda descubrir que se encontraba allí.

3. Para comunicarse con la persona que desde fuera de la red recibía la información de las transacciones y retiraba el dinero una vez depositado en las cuentas destino, ocultaba un archivo de Excel en una imagen; el destinatario del correo (cómplice) conoce la contraseña para abrir el archivo y el programa bajo el cual se desarrollaba la tarea. "Our Secret". Aquí una vista del procedimiento:

a. Ocultar el archivo en la imagen, para esto primero seleccionamos el archivo que hará las veces de portador, puede ser un documento, una imagen, un audio, o un video. Aquí escojo las fotos de una mascota.

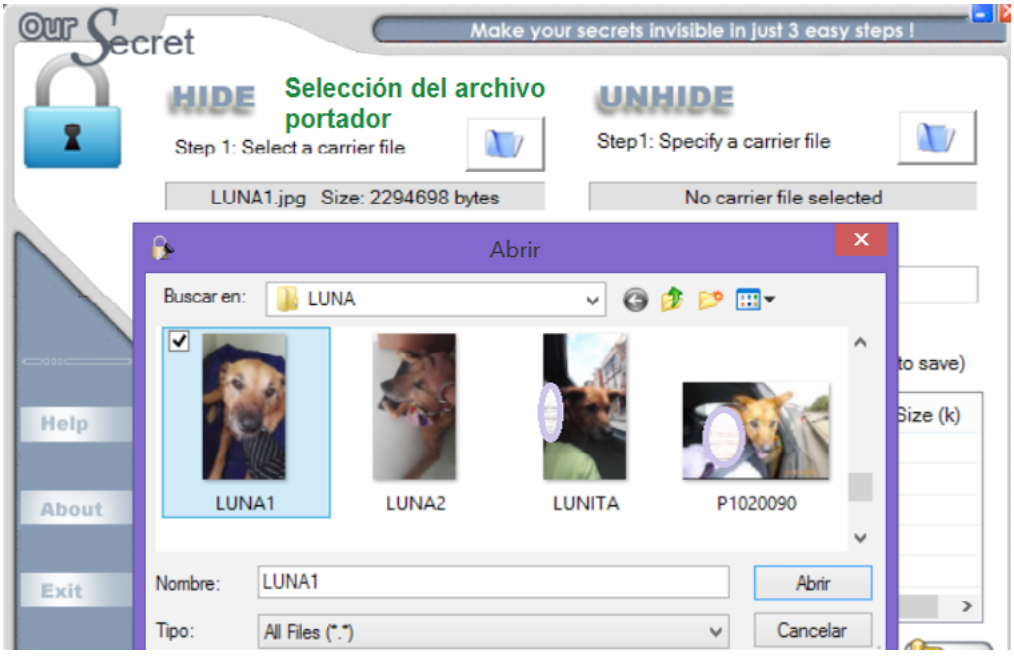


Figura 28. Our Secret elección de portador
Fuente: propia

Una vez que se ha seleccionado el "portador" procedo a seleccionar el archivo y/o mensaje que quiero ocultar. En este caso es un archivo de Excel que se llama cuota. Allí quien comete el ilícito registra los detalles de las transacciones para que su cómplice pueda acceder al dinero.

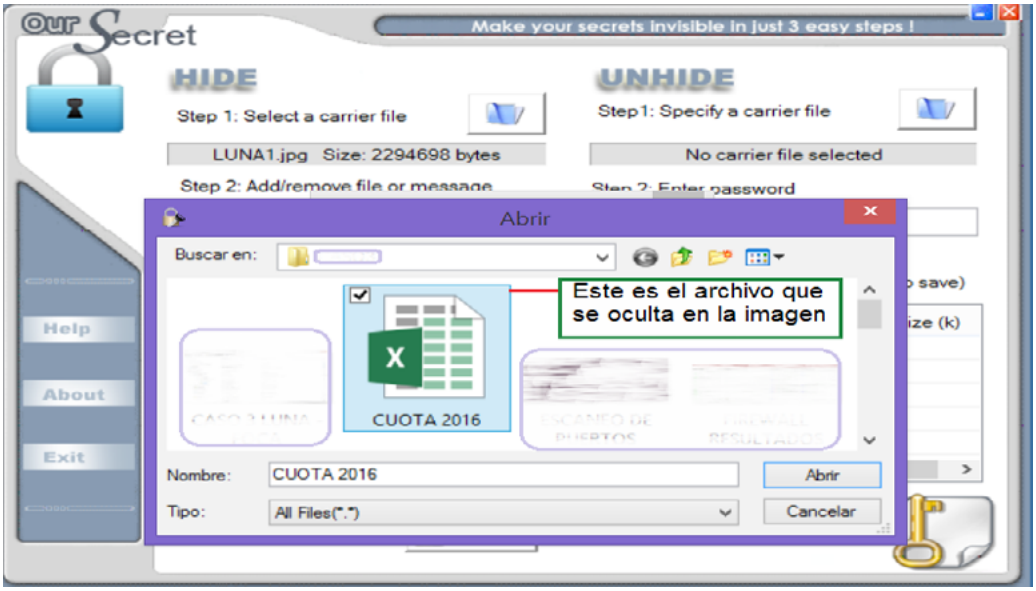


Figura 29. Our Secret archivo oculto
Fuente: propia

En el menú que aparece puedo seleccionar la opción de ocultar un mensaje de texto que escribo dentro del espacio que el programa abre para este fin, únicamente anexo el archivo cuota 2016. Escribo una contraseña, de nuevo la reingreso y escojo la opción HIDE (ocultar), sin la contraseña es imposible acceder a contenido del fichero oculto o el mensaje. Escojo el nombre y la ubicación del nuevo archivo y click en guardar. La imagen queda lista para ser enviada.

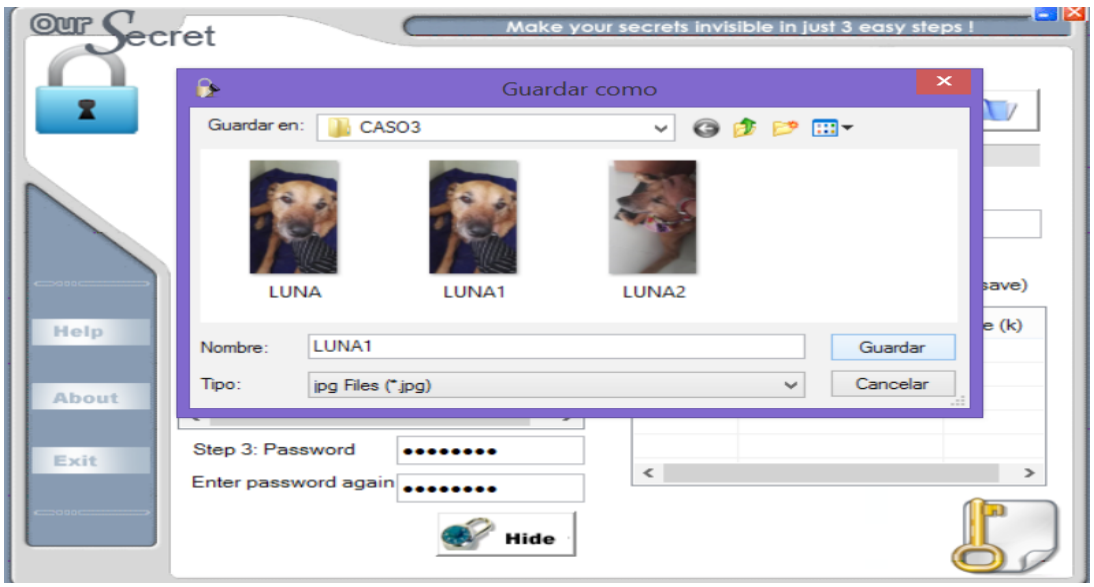


Figura 30. Our Secret ocultar y encriptar
Fuente: propia

Voy a mostrar la imagen original y la "portadora" para que usted trate de identificar cambios entre las dos, además voy a exponer los metadatos obtenidos con Exiftool. El nombre del archivo original es Luna1 y el archivo portador es Luna4.

Figura 31. Metadatos original y portador
Fuente: propia

Como podemos observar los programas que extraen metadatos, especializados en imágenes como Exiftool no detectan algo sospechoso. Así, la persona que adelantó las acciones delictivas y conocedora experta de las técnicas antiforenses ha puesto en aprietos al equipo forense.

Cuando el "cómplice" externo de la persona que está desarrollando la actividad ilícita recibe el archivo LUNA4 por correo, lo único que hace es abrirlo con el programa OURSECRET, introduce la contraseña y listo. Tiene el mensaje oculto y el archivo de Excel enviado.

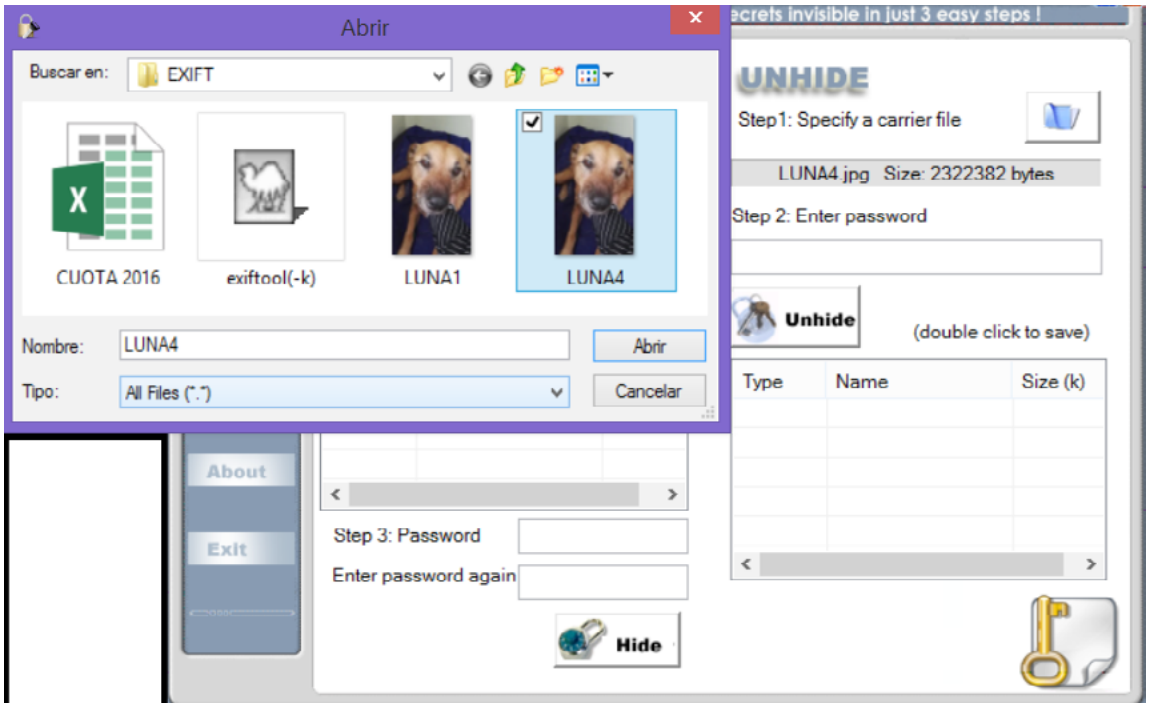


Figura 32. Our Secret extraer oculto
Fuente: propia

Cuando el destinatario introduce la contraseña puede acceder a la información. El programa Our-Secret no solo oculta el archivo, además aplica un procedimiento que se conoce con el nombre de Encriptación, así, en el eventual escenario de que logremos llegar a la información que se encuentra oculta en el portador, los algoritmos de cifrado que aplica el programa hacen casi que imposible que podamos identificar el contenido del archivo o del mensaje. La imagen muestra como accede el "cómplice" externo al archivo oculto.

Encriptación

Es una técnica que consiste en implementar uno o varios algoritmos matemáticos que van transformando las cadenas de bits en códigos que se vuelven indescifrables para la persona que logre acceder a ellos sin tener la clave correspondiente. Windows incluye una utilidad de encriptación llamada Bitlocker, en el mercado hay varias utilidades como vera crypt o best crypt.

Figura 33. Our Secret archivo oculto en destino
Fuente: propia.

A modo de conclusión para este caso:

A pesar de contar con algunos indicios que pueden dar pistas respecto al responsable de la pérdida de dinero al interior de la organización, con el análisis de las posibles "evidencias" que tenemos aún no podemos obtener una prueba irrefutable que permita hacer una imputación de responsabilidad sobre un empleado específico.

Una actividad adicional que usted como investigador forense podría desarrollar consiste en recuperar cada uno de los correos enviados por la persona a la que consideramos sospechosa "el que ha enviado las imágenes" con la información oculta, comparar las fechas y horas de los correos y envío de las imágenes con las fechas y horas de las transacciones fraudulentas, y tratar de establecer un patrón o concordancia de tiempo entre uno y otro suceso, así tal vez logren convencer al sospechoso haciéndole creer que se encuentra descubierto y pueda informar la contraseña y el programa que uso para encriptar y ocultar los archivos.

BIBLIOGRAFÍA

Bbrezinski, D. y Killalea, T. (2002). RFC 3227: *Guidelines for Evidence Collection and Archiving*. *Network Working Group*. Recuperado de http://www.rfceditor.org/rfc/rfc3227.txt

Cano, J. (2009). Computación forense. *Descubriendo los rastros informáticos*. Ciudad de México, México: Editorial Alfaomega.

Ministerio de las Tecnologías de la Información y las Comunicaciones. (2016). *Serie seguridad y privacidad de la información*. *Guía 13*. Evidencia digital. Bogotá, Colombia: Ministerio de las Tecnologías de la Información y las Comunicaciones.