INFORMÁTICA FORENSE

Luis Francisco López Urrea

EJE 3

Pongamos en práctica

AREANDINA
Fundación Universitaria del Área Andina
MIEMBRO DE LA RED
ILUMNO

Fuente: Shutterstock/684663283

ÍNDICE

"DUMP" de memoria RAM 19
El programa OSForensics. 20
Los discos duros 26
Clases de discos duros. 27
Estructura físico-lógica de los discos duros 28
Bibliografía 35

Los elementos propios de la informática forense y los relacionados de forma directa con la investigación digital forense, abren un nuevo campo de acción de los ingenieros de sistemas, pues tal como se detalló en los referentes epistemológicos y de carácter crítico social, se pone de manifiesto que el investigador digital forense debe reunir un conjunto de competencias, habilidades y conocimientos que contribuyan a adelantar con éxito el trabajo de investigación.

Así pues, no se trata únicamente del conocimiento de orden técnico, relacionado con el hardware y la arquitectura de los dispositivos que se emplean para el procesamiento automático de información. Además, exige conocer a fondo el funcionamiento de los sistemas operativos de más amplio uso en los sistemas informáticos (Windows, OS, Linux), la forma como se almacena la información en los dispositivos de almacenamiento (en los que en la mayor parte de casos se almacena la información de los hechos relacionados con la investigación), las estructuras bajo las cuales se almacenan los archivos en los discos duros y unidades extraíbles; la forma como se comunican los dispositivos a través de una red de comunicaciones y la forma de acceder a ella, las vulnerabilidades que pueda presentar un sistema de procesamiento electrónico de información, y muchos otros temas y habilidades que debe reunir el investigador digital forense.

Video

Al respecto, veamos la vídeo cápsula Tecnología forense: CTI en la página principal del eje.

https://www.youtube.com/watch?v=5CmM9K_FCqc&t=133s

Los elementos que se describen, por nombrar solo algunos hacen que la tarea de la investigación digital forense recaiga sobre personas con una formación básica en ingeniería de sistemas o áreas afines, ingeniería informática o de telecomunicaciones, por mencionar solo algunas.

Así pues, el conocimiento básico de muchos elementos que vamos a mencionar como parte de los elementos propios del presente eje se constituyen en una herramienta fundamental para el éxito de nuestra investigación.

Análisis digital forense

Video

Antes de indicar y desarrollar los elementos que hacen parte del presente eje, es necesario recordar que durante el desarrollo del eje epistemológico mencionamos la existencia de la RFC 3227, directrices para recolectar, adquirir y archivar evidencias, aquí puede acceder a la RFC.
https://www.youtube.com/watch?v=5CmM9K_FCqc&t=133s

El punto dos de la norma que refiero destaca los principios que debemos tener en cuenta para la recolección de evidencia, y es aquí donde reside el inicio del análisis digital forense. Uno de los aspectos que se destacan en esta sección de la RFC es acotar de forma inicial el trabajo sobre la evidencia más volátil para al final proceder sobre la menos volátil, así cuando usted como investigador digital forense responda ante un incidente debe observar la siguiente secuencia para ir de lo más a lo menos volátil.

Figura 1. RFC3227
Fuente: propia

Se destaca, además, la recomendación que se hace en referencia a la firma criptográfica de las evidencias recolectadas y la posibilidad de verificación a través de hash, no olvide que la cadena de custodia inicia desde el primer momento en que se ingresa a la escena. Así, es necesario recordarle los pasos que debe seguir al llegar a la escena en la que se ha cometido un delito y en la que su presencia sea requerida (Mintic, 2016).

¡Lectura recomendada!

En primera instancia recuerde el procedimiento general para la evidencia digital, pero antes realicemos la lectura Análisis Forense – Técnicas y Procedimientos, en la página principal del eje.
https://goo.gl/1gBukb

Figura 2. Procedimiento evidencia digital
Fuente: Mintic (2016)

De acuerdo con los lineamientos establecidos por múltiples autores, y con base en los protocolos reconocidos por las autoridades, tanto en el ámbito de la investigación como en lo judicial, la primera etapa reconocida tal vez como una de las más importantes en la investigación digital forense es el aislamiento de la escena, así (Mintic, 2016) recomienda lo siguiente para esta etapa.

Antes de adelantar cualquier procedimiento verificar si autoridades como el Centro Cibernético de la Policía Nacional (CCP), o el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert) pueden actuar como primeros respondientes ante el incidente. Si por los trámites requeridos y la urgencia de la acción, usted encuentra que no puede contar con la ayuda de ninguno de los dos organismos, es necesario contactar al responsable de administración de la infraestructura tecnológica afectada para que con su apoyo se pueda certificar el procedimiento realizado, la observación de todos los protocolos y el inicio de la cadena de custodia bajo las formalidades requeridas, de ser necesario acuda al personal de seguridad de la organización para desarrollar la actividad o solicite acompañamiento de la Policía Nacional.

- Aislamiento de la escena: (no olvide usar guantes especiales durante todo el tiempo desde antes del ingreso a la escena) antes de iniciar el procedimiento formal de investigación digital forense, es necesario que todas las personas que puedan estar presentes u operando los equipos se retiren de sus puestos de trabajo y dejen todos los dispositivos en la misma condición en que se encuentran al ingresar el investigador a la escena. Se recomienda antes de iniciar el procedimiento tomar una o varias fotografías de la escena.

- Perímetro de seguridad: aislar con cintas adecuadas la escena para evitar que personas ajenas a la investigación se acerquen a la zona o zonas en las que debe adelantar la investigación.

- Si el equipo o equipos de procesamiento de información ubicados en el área están encendidos NO LOS APAGUE, DEBE SEGUIR EL SIGUIENTE PROCEDIMIENTO.

- Selle con cintas de seguridad todos los puertos (USB, Lector de Memorias, etc.) unidades y conexiones externas de los laptops, servidores, estaciones de trabajo o computadores personales para evitar que alguna persona pueda encender o acceder a cualquier dispositivo y alterar su contenido.

    a. Tome fotografías de las computadoras encendidas, programas que se ejecutan, procesos, entre otros. Evite hacerlo con teléfonos celulares u otros dispositivos de uso personal, tenga en cuenta que todas las fotografías registren la fecha y hora del sistema en el momento de la captura.

    b. Ponga bajo seguro cada uno de los equipos, si hay computadores portátiles procure mantenerlos encendidos y llévelos con su respectivo cargador, hasta que se efectúe su análisis o haga entrega de él a la dependencia responsable de su análisis.

    c. En el caso de los computadores encendidos, capture la información descrita en la RFC 3227, antes de apagarlos, no olvide que para hacerlo debe seguir las instrucciones previstas en el desarrollo del eje epistemológico; es decir, usar las herramientas de investigación forense adecuadas y evitar instalar programas en el equipo pues altera su integridad y hace que la evidencia obtenida pueda ser declarada inválida.

- Si el equipo o equipos están apagados no los encienda, pueden existir programas instalados para afectar la integridad del equipo luego de ser encendido o se pueden borrar rastros importantes, a los que se puede acceder de forma posterior a través de diferentes procedimientos.

- Disponga en la escena de los equipos forenses necesarios para recolectar y adquirir la información, estaciones de trabajo forenses, medios externos (estériles – de preferencia nuevos) para capturar la copia de los discos, bolsa para evidencias,

bolsas antiestáticas, rótulos, etiquetas entre otros. (no olvide que no debe usar dispositivos de uso personal, para ninguna actividad relacionada con la investigación).

- La información original que se recolecta debe ser almacenada en un sitio protegido con las condiciones de almacenamiento necesarias, control de acceso, y siguiendo los protocolos de la cadena de custodia en cada etapa del proceso.

- Acceda a todos los dispositivos intermediarios de red que estuvieron en contacto con los computadores (routers, firewall, switch, acces point entre otros) intenté obtener la información que resida en estos dispositivos, por ejemplo, tablas de enrutamiento de los enrutadores, tabla ARP de los switch, reglas de los cortafuegos)

Video

Con base en esta información podemos iniciar ahora con nuestra primera etapa de intervención, la recolección de información digital, para esto nos servirá la videocápsula 2: Unidad de Delitos Informáticos, que encontrará en la página principal del eje.

Debe tener en cuenta, investigador, que el programa o programas que piensa utilizar para efectuar el análisis no debe ser instalado en el equipo que se va a investigar; así recomiendo descargar el programa en su estación de trabajo de investigación forense y generar una copia en un medio extraíble (memoria USB), desarrolle el procedimiento de recolección a partir de este medio. NO OLVIDE QUE LAS COPIAS ADQUIRIDAS DEBEN SER GENERADAS EN UN MEDIO LIBRE – (DE PREFERENCIA NUEVO).

Herramientas de recolección y adquisición de evidencias

Uno de los programas de fácil uso y reconocida eficacia en la recolección de evidencias en primera respuesta ante un incidente de seguridad es el programa conocido como FastIR_Collector. Programa de código abierto patrocinado por la empresa Sekoia, dentro de las características a destacar del programa se encuentra la posibilidad de uso bajo plataformas Windows y Linux.

FastIR_Collector

Por ser software de código abierto no necesita licencia para su uso, la descarga se puede hacer desde el siguiente enlace descargar FastIR_Collector en el enlace de descarga debe seleccionar las dos versiones, la que corresponde a sistemas de 64 bits X64 y la que corresponde a sistemas de 32 bits X86. Una vez descargadas las versiones que correspondan debe copiarlas en un medio extraíble, de preferencia estéril.

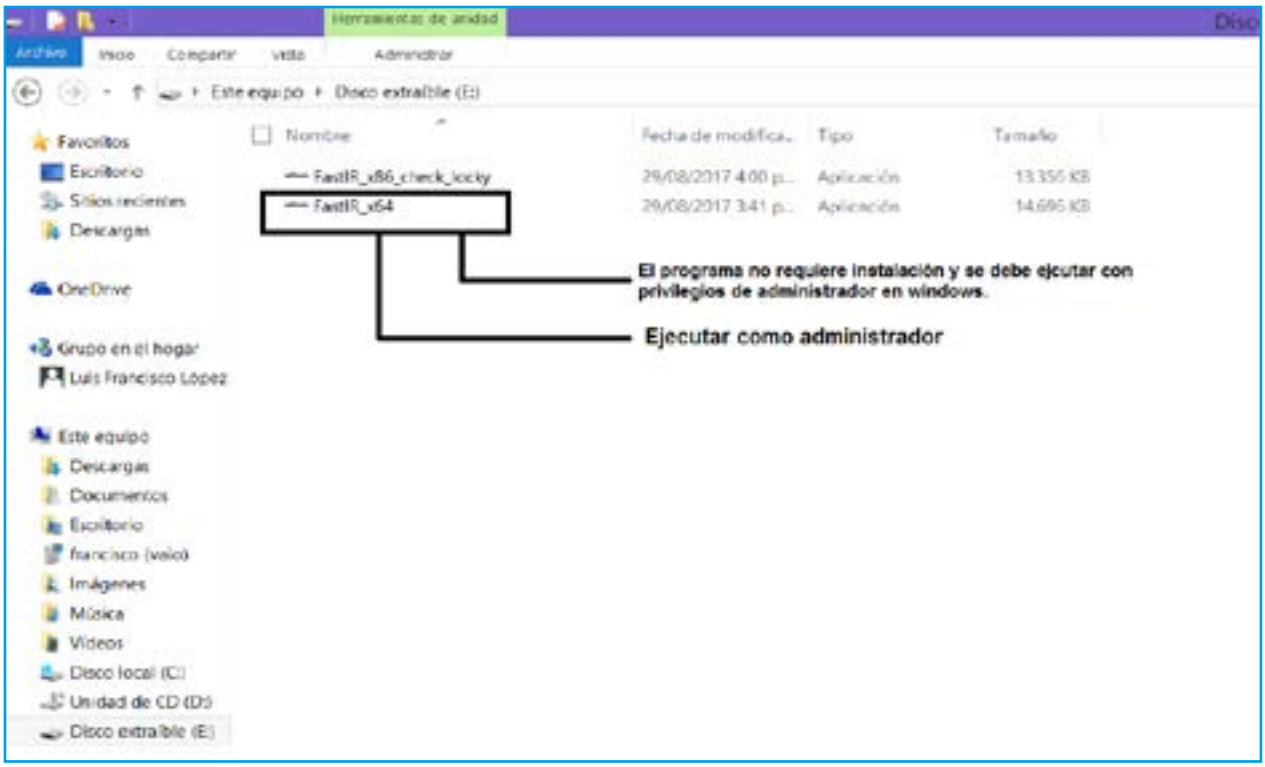


Figura 3. FASTIR Collector
Fuente: propia

Una vez hecha la copia en el medio extraíble, este será el dispositivo que va a insertar en la máquina a analizar.

En la máquina a analizar debe atender la siguiente recomendación: Los sistemas tipo Windows no garantizan seguridad, el medio extraíble que inserte puede ser escrito con algún malware u otro tipo de amenaza, así que asegúrese de que el puerto en que inserta el medio con los programas forenses quede registrado como de solo lectura. Para marcar el puerto como de solo lectura debe modificar la siguiente clave en el editor de registro de Windows:

"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies"

Para hacer esta tarea, por favor ejecute el editor de registro de Windows, puede usar la instrucción regedit, desde la línea ejecutar de Windows 7 o ejecutar con las Teclas Windows W en Windows 8.

Una vez se encuentre dentro del registro de Windows por favor busque la clave señalada.

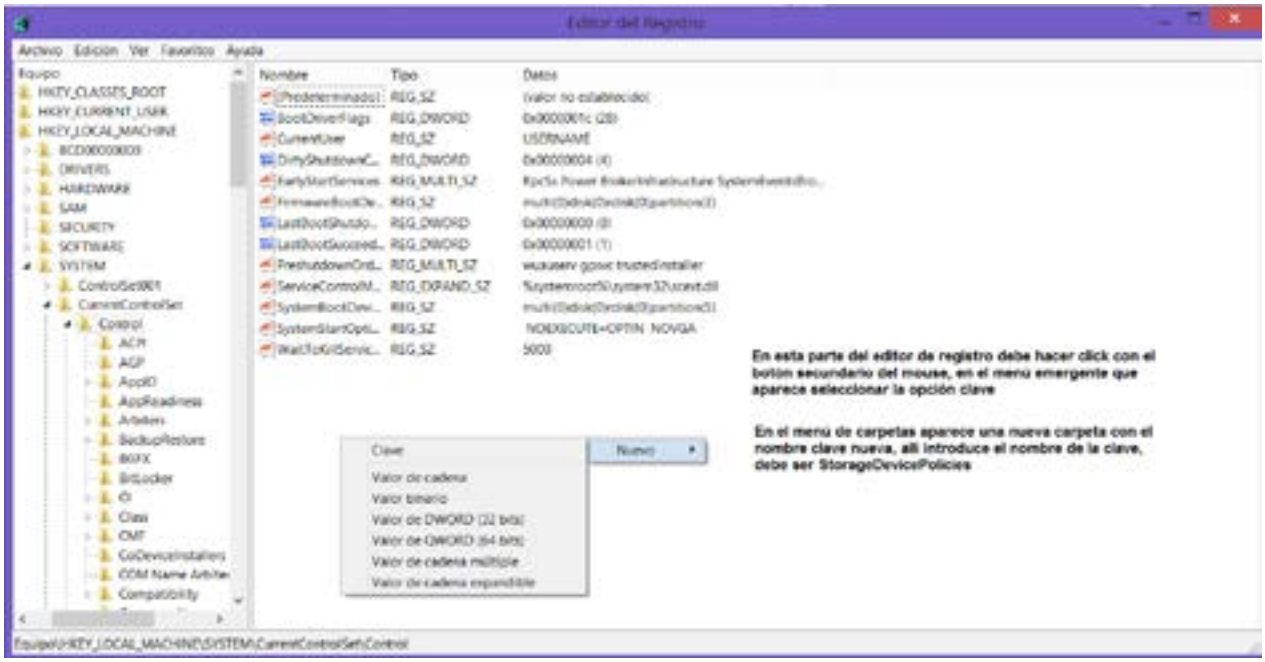


Figura 4. Editor de registro
Fuente: propia

Para continuar el proceso debe introducir un valor en la clave que ha creado.

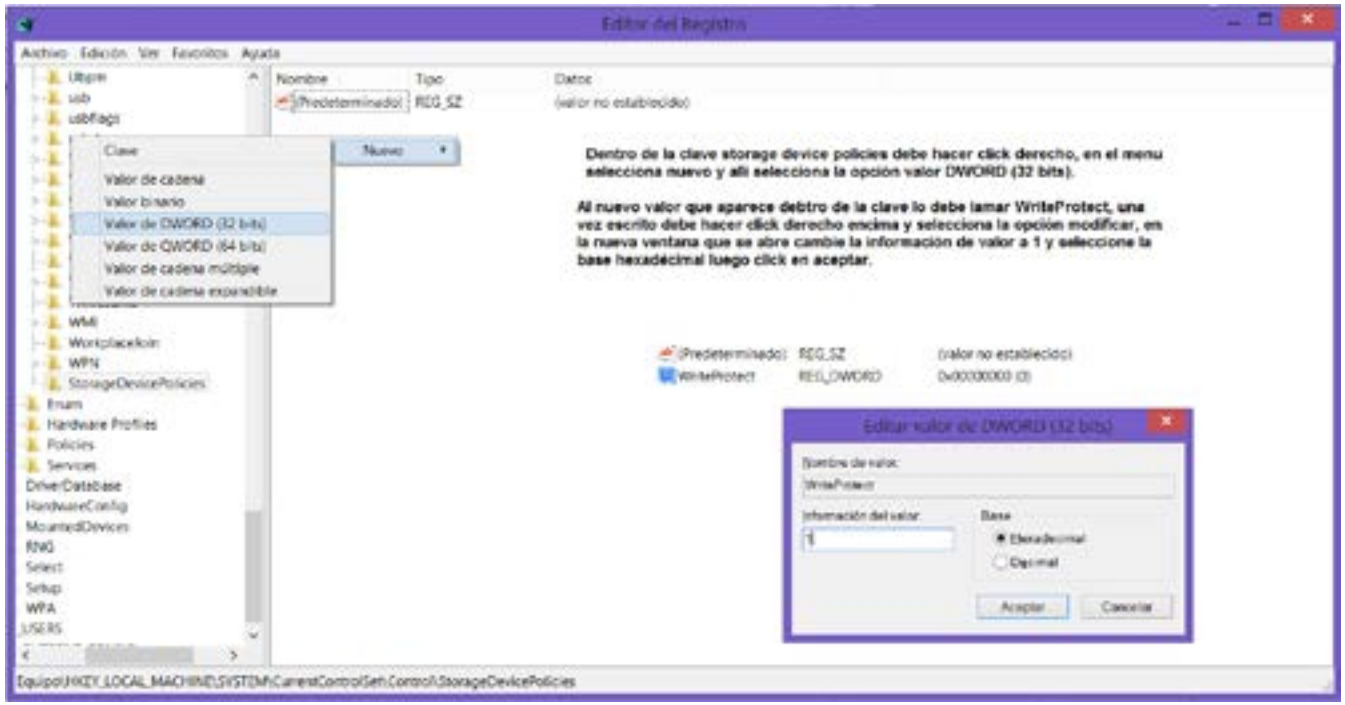


Figura 5. Clave registro
Fuente: propia

El resultado final debe ser el siguiente.

Figura 6. Protección escritura
Fuente: propia

Cuando termine este procedimiento, debe cerrar el editor de registro, así cuando intente copiar un archivo en el dispositivo extraíble e resultado será el siguiente.

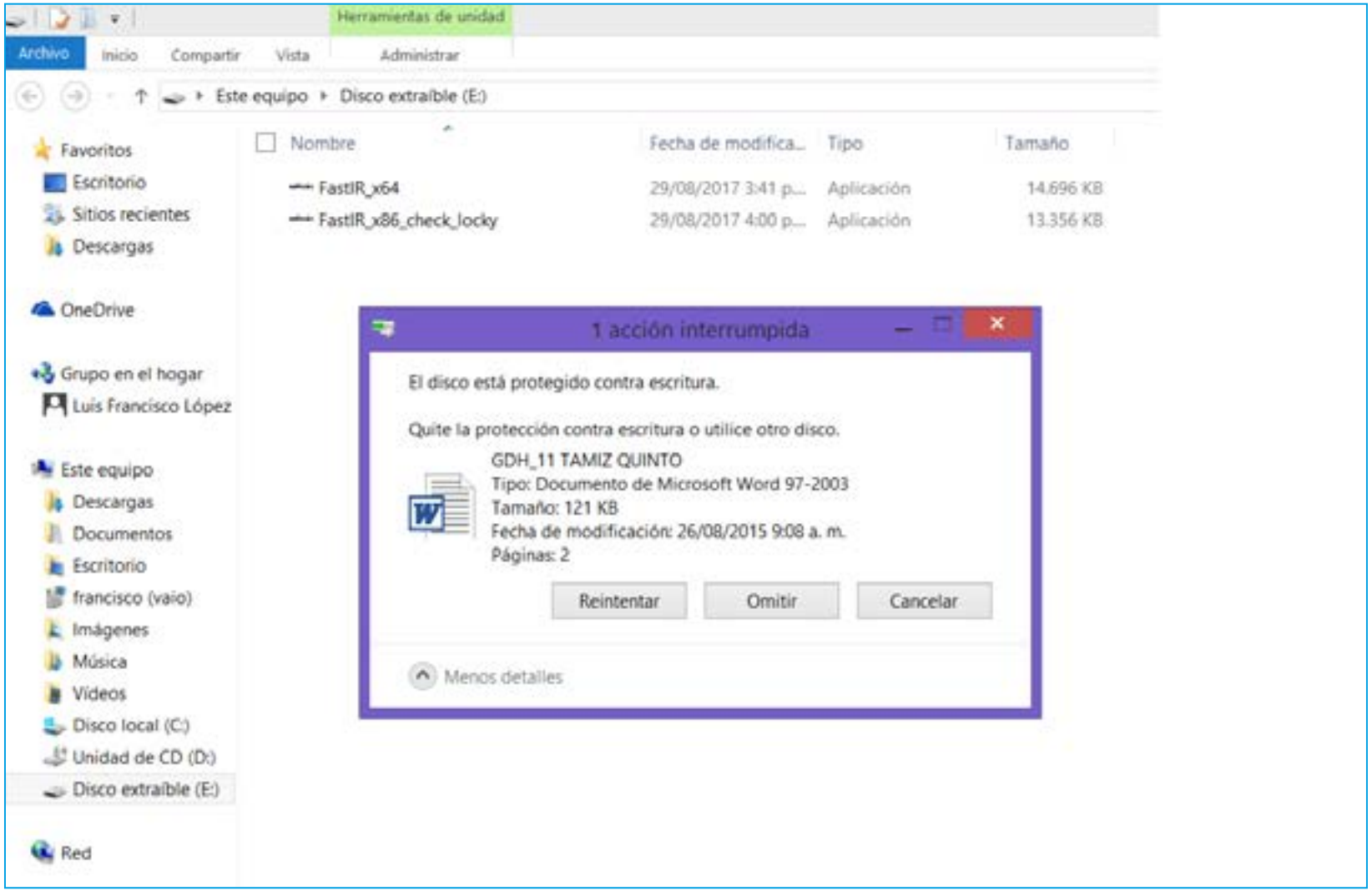


Figura 7. Prohibido escribir
Fuente: propia

Con este procedimiento no se podrá escribir ningún archivo en la memoria, así que si existe algún malware o virus en el sistema a investigar este no se copiará a nuestro medio en el que tenemos el programa para hacer el análisis. ¿Y cómo obtenemos las copias? Para hacerlo, sin retirar el medio con el que va a ejecutar los programas para hacer el análisis, debe regresar al registro y modificar el valor de la misma clave, ahora lo ponemos en cero. Así, un medio estará protegido contra escritura (el medio desde el que ejecutamos los programas de análisis) y el medio estéril para obtener la copia estará disponible para lectura y escritura. Este procedimiento nos asegura que usted apreciado investigador no escriba la información adquirida en el mismo medio en el que se encuentran los programas de análisis.

Una vez cumplidos los pasos descritos en relación con la protección de los medios, podemos continuar con la obtención de la información del sistema a través del programa FastIR_Collector; cuando accedemos al equipo víctima o atacante sin que haya sido apagado, podemos recolectar la siguiente información:

- Navegadores, historial y descargas.
- Carpeta Prefetch.
- Papelera de reiclaje.
- Directorios de inicio.
- Salud del sistema: Tabla ARP, lista de unidades, unidades de red, tarjetas de red, procesos, tabla de enrutamiento, tareas, trabajos programados, servicios, sesiones, zócalos.
- Registro: Carpetas de instalación, archivos MRU (Most Recently Used) abiertos y usados, servicios, claves de registro, archivos autiejecutables, historial de USB, lista de redes.
- Memoria: Portapapeles, DLL cargados, archivos abiertos.
- Recursos en uso: Tabla maestra de archivos, master boot record, RAM, Disco, Registro, SAM (administrador de cuentas de seguridad)

Toda la información anterior junto a algunos registros adicionales que no hemos mencionado, se pueden obtener cuando hacemos el análisis forense en vivo, por esta razón hemos recomendado de forma reiterada evitar apagar los equipos siempre que sea posible. La captura que efectúa el programa se exporta a un archivo CSV.

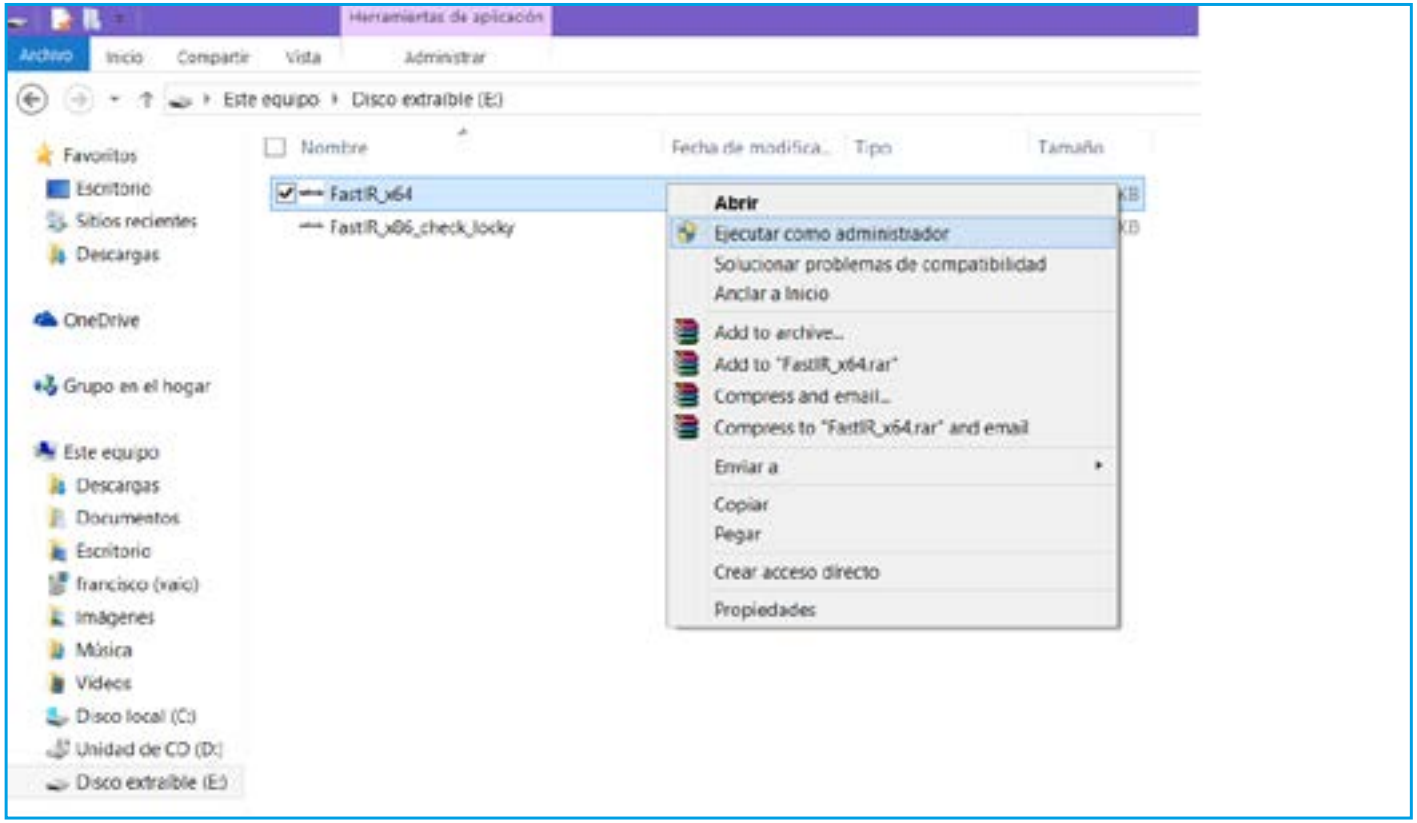
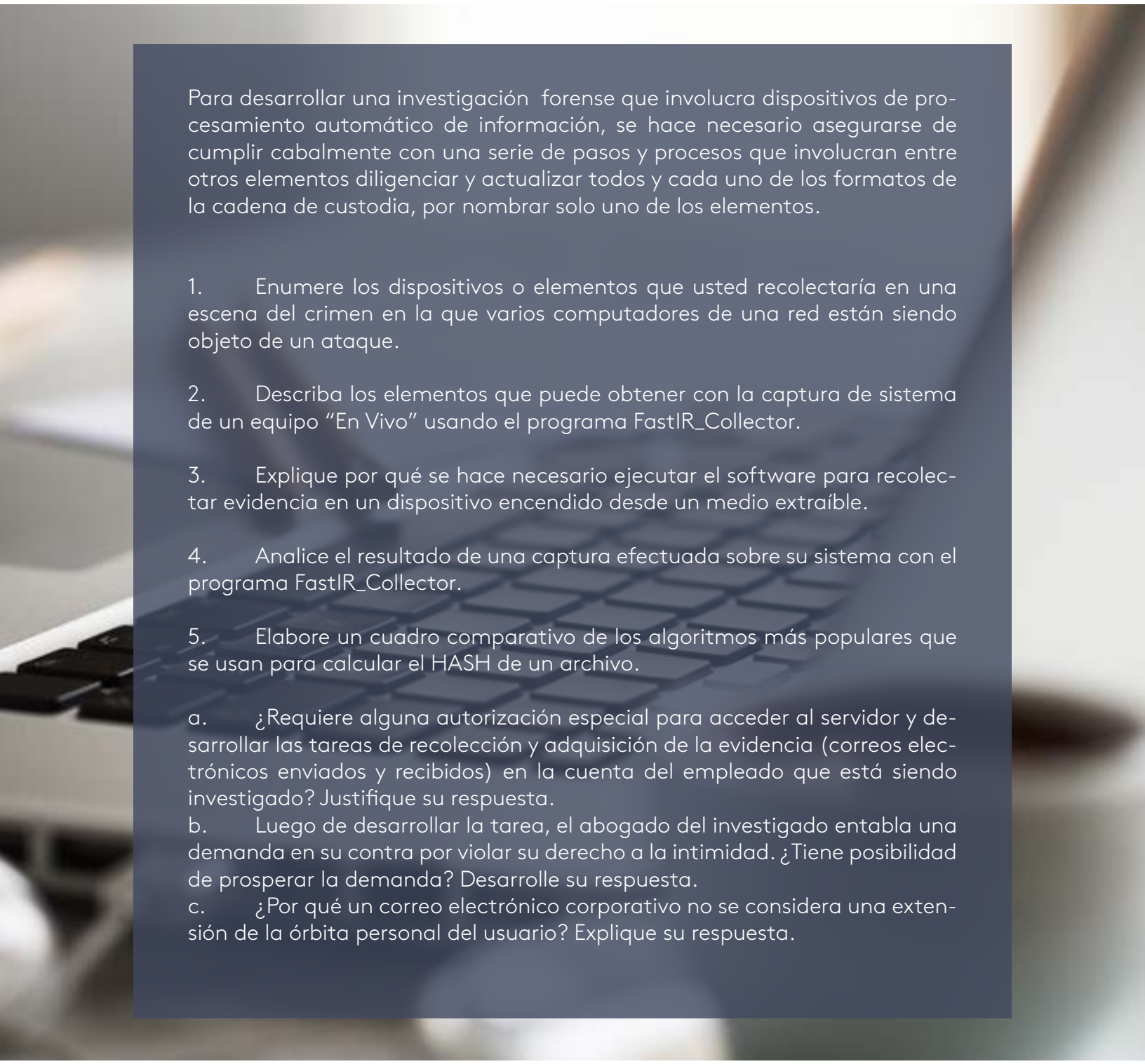


Figura 8. Ejecutar FASTIR
Fuente: propia

Así, ejecute el IR_Collector desde su medio forense (USB extraíble).

Seleccione la opción ejecutar como administrador para asegurar que tendrá acceso a todos los recursos del sistema durante la recolección de la información. En el equipo sobre el cual se hace la demostración se ejecuta el programa para sistemas de 64 bits; en su investigación seleccione la opción que se ajuste al sistema a analizar.

Recomiendo de forma especial ejecutar el programa desde el símbolo de sistema en modo ejecutar como administrador, pues muchas de las utilidades que el programa nos ofrece en el modo de línea de comandos no las podemos usar si ejecutamos el programa desde Windows. Ahora lo invitamos a realizar la actividad de repaso 1:



Para desarrollar una investigación forense que involucra dispositivos de procesamiento automático de información, se hace necesario asegurarse de cumplir cabalmente con una serie de pasos y procesos que involucran entre otros elementos diligenciar y actualizar todos y cada uno de los formatos de la cadena de custodia, por nombrar solo uno de los elementos.

1. Enumere los dispositivos o elementos que usted recolectaría en una escena del crimen en la que varios computadores de una red están siendo objeto de un ataque.

2. Describa los elementos que puede obtener con la captura de sistema de un equipo "En Vivo" usando el programa FastIR_Collector.

3. Explique por qué se hace necesario ejecutar el software para recolectar evidencia en un dispositivo encendido desde un medio extraíble.

4. Analice el resultado de una captura efectuada sobre su sistema con el programa FastIR_Collector.

5. Elabore un cuadro comparativo de los algoritmos más populares que se usan para calcular el HASH de un archivo.

a. ¿Requiere alguna autorización especial para acceder al servidor y desarrollar las tareas de recolección y adquisición de la evidencia (correos electrónicos enviados y recibidos) en la cuenta del empleado que está siendo investigado? Justifique su respuesta.
b. Luego de desarrollar la tarea, el abogado del investigado entabla una demanda en su contra por violar su derecho a la intimidad. ¿Tiene posibilidad de prosperar la demanda? Desarrolle su respuesta.
c. ¿Por qué un correo electrónico corporativo no se considera una extensión de la órbita personal del usuario? Explique su respuesta.

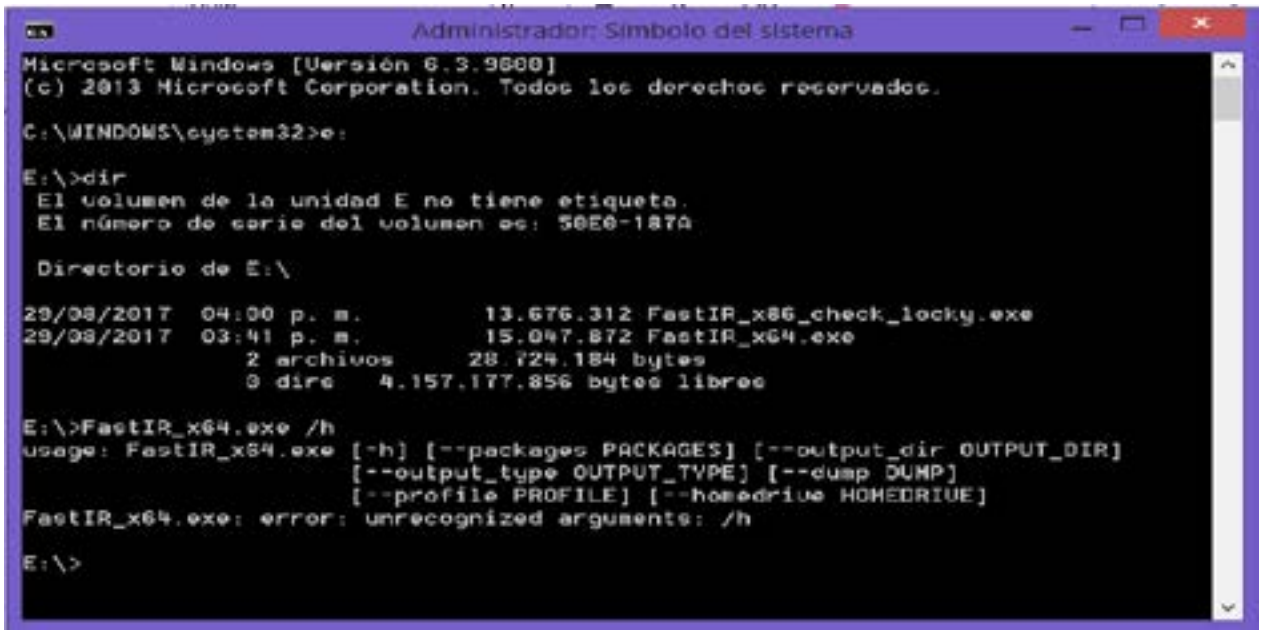


Figura 9. Línea de Comandos FASTIR
Fuente: propia

Como puede observar apreciado investigador, una de las herramientas que nos ofrece el programa es la de hacer DUMP de la memoria sin embargo recomiendo usar una herramienta específica para cada tarea. El FastIR lo usaremos para capturar el estado de la máquina en el momento de nuestra intervención, de otra parte y si tenemos en cuenta que no podemos escribir los resultados en el medio desde el que ejecutamos el programa seleccionaré entonces el modificador –output_dir desde línea de comandos para indicarle que debe generar el archivo de salida en la unidad estéril (unidad en la que obtendremos las copias de la información recolectada) en este ejemplo, la unidad en la que guardaré los archivos se encuentra marcada con la letra F.

Así, la instrucción que se ejecutará desde línea de comandos debe ser la siguiente:

FastIR_x64.exe –output_dir F:/. (No olvide que desde línea de comandos el sistema es sensible a mayúsculas o minúsculas). Esta instrucción generará el archivo de salida con los resultados en la unidad estéril F:/

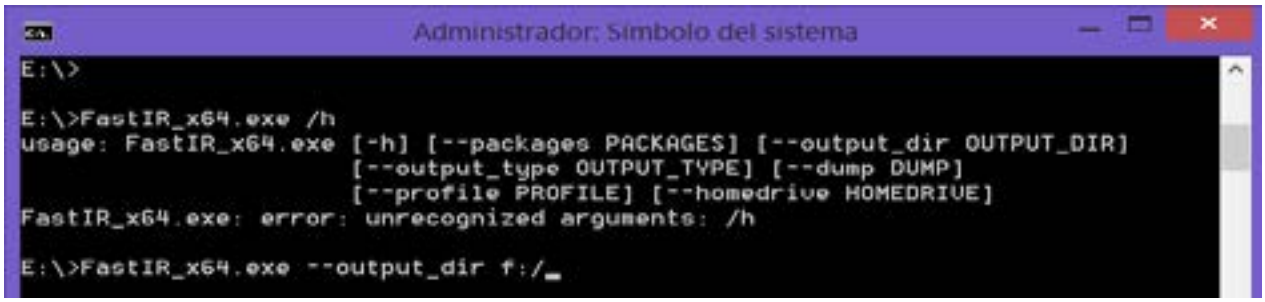


Figura 10. Estado máquina FASTIR
Fuente: propia

Debe esperar un tiempo, que puede ser elevado o no, depende de los procesos que se ejecuten en el equipo.

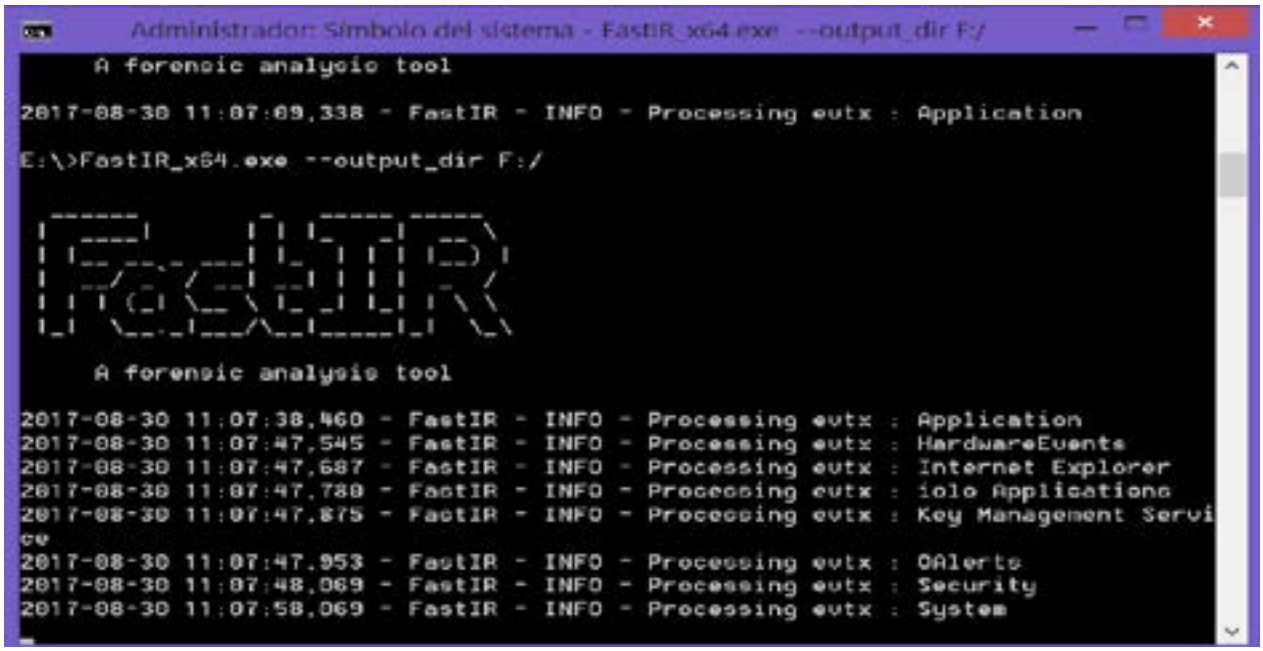


Figura 11. Captura de procesos FASTIR
Fuente: propia

Una vez concluya el proceso usted tendrá un archivo CSV en el medio estéril con toda la información relacionada con el estado de la máquina en el momento de la intervención.

Aquí una vista de las capturas realizadas alojadas en el medio extraíble estéril.

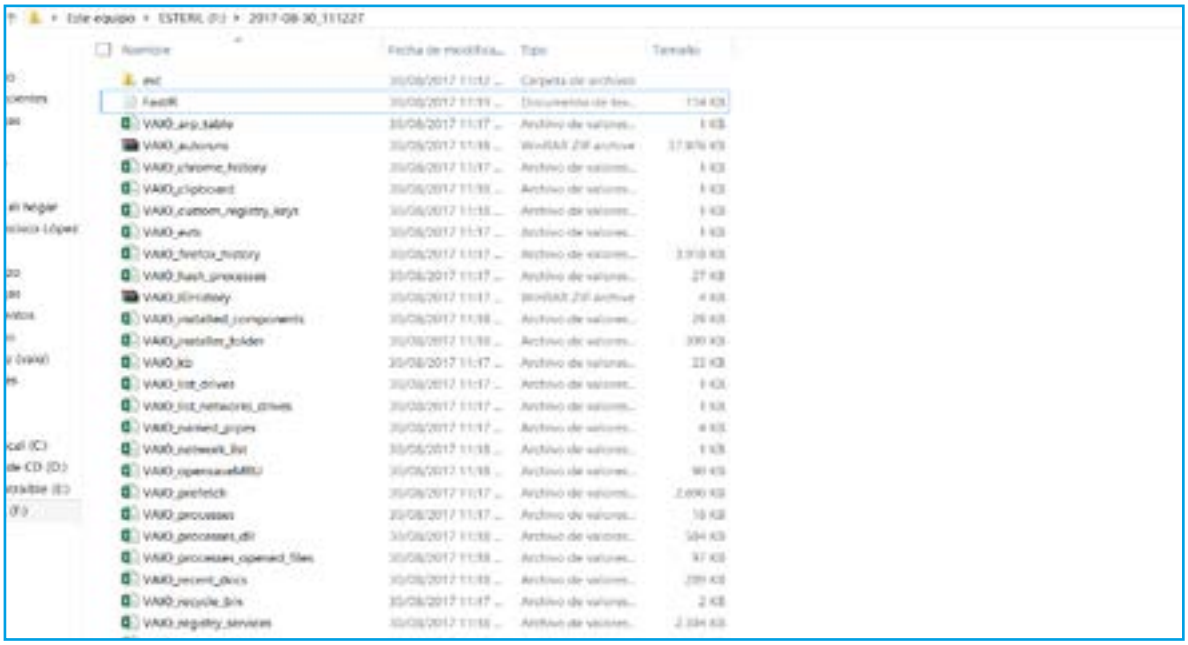


Figura 11. Captura de procesos FASTIR
Fuente: propia

Es su trabajo, como investigador digital forense, en primera instancia generar la firma digital de los archivos generados y obtener una nueva copia de los mismos en otro medio para realizar la investigación. Al abrir por ejemplo el archivo Firefox history podría encontrar información relevante.

Figura 13. Análisis de captura FASTIR
Fuente: propia

¡Lectura recomendada!

El análisis de toda esta información recolectada y adquirida es su labor como investigador digital forense. Al respecto le recomendamos realizar la lectura Análisis de Evidencias Digitales en la página principal del eje.

"DUMP" de memoria RAM

El siguiente paso que debe seguir al intervenir en un escenario de investigación digital forense es adquirir la información que se estaba procesando en el momento en que usted como investigador entra en escena, por esta razón reitero la recomendación de no apagar los equipos y luego de recolectar toda la información del equipo en el momento de la intervención (IR_Collector) obtener un volcado de memoria RAM.

Así, para adquirir la información relacionada con la investigación recomiendo por su interfaz y facilidad de uso el programa OSForensics lo puede descargar haciendo click sobre el enlace OSforensics, cuenta con una versión de pago y una versión gratuita, para esta actividad usaremos la versión libre del programa. De igual forma le invitamos a realizar la lectura Herramientas de análisis forense en la página principal del eje.

El programa OSForensics

- Instalación, puede correr en sistemas operativos Windows o Linux, en este caso descargo la versión para Windows por estar trabajando en una estación de trabajo con sistema Windows 8 de 64 bits. El procedimiento de instalación es simple e intuitivo, la única observación al respecto es escoger la opción marcada como Continue Using Free Versión (continuar usando la versión gratuita).

- A diferencia de IR_Collector este programa requiere de instalación, se recomienda instalar en su estación de trabajo de análisis forense. Luego de hacer la instalación el programa permite crear un ejecutable que se debe instalar en un medio extraíble desde el que se realizará el análisis en la máquina a investigar.

La figura muestra la interfaz del programa OSForensics instalado en la estación de trabajo forense.

Figura 14. OSForensics estación forense
Fuente: propia

¡Lectura recomendada!

Según la recomendación realizada en el desarrollo de cada uno de los ejes, siempre debemos evitar instalar cualquier aplicación o hacer cambios en el equipo o dispositivo a investigar, así seleccionamos en el programa OSForensics la opción install to USB para montar en el medio extraíble de investigación forense una copia ejecutable del programa. Ahora bien, realicemos la lectura Preservación de la evidencia digital en la página principal del eje.

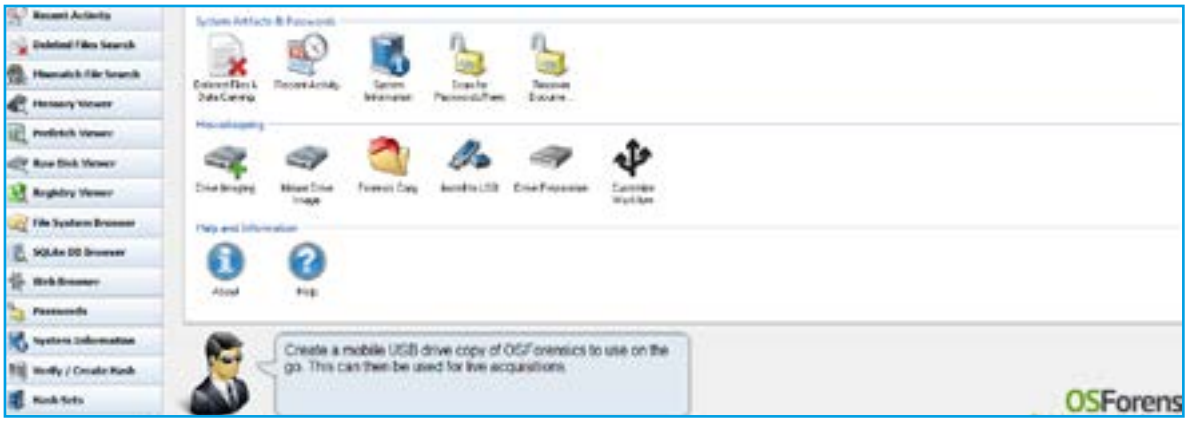


Figura 15. OSForensics exportar a USB
Fuente: propia

Para hacer la instalación del programa en su medio forense USB debe introducir en el puerto el medio extraíble en el que tendrá montadas las utilidades para efectuar el análisis, debe seleccionar en destino la ruta de la memoria y seleccionar la opción versión de evaluación. Ahora veamos la siguiente infografía:

Figura 16. Precauciones que debe tomar el investigador.
Fuente: propia

Figura 17. OSForensics proceso de exportación
Fuente: propia

Una vez que hayamos verificado que se instaló correctamente el programa en la memoria podemos insertar nuestro medio con las herramientas forenses en el equipo a investigar. No olvide marcar como de solo lectura el medio desde el que ejecuta las utilidades forenses. En otro puerto USB inserte la unidad estéril y cambie el valor de la clave de registro a cero para poder escribir en ella, en el medio estéril realizará el volcado de memoria.

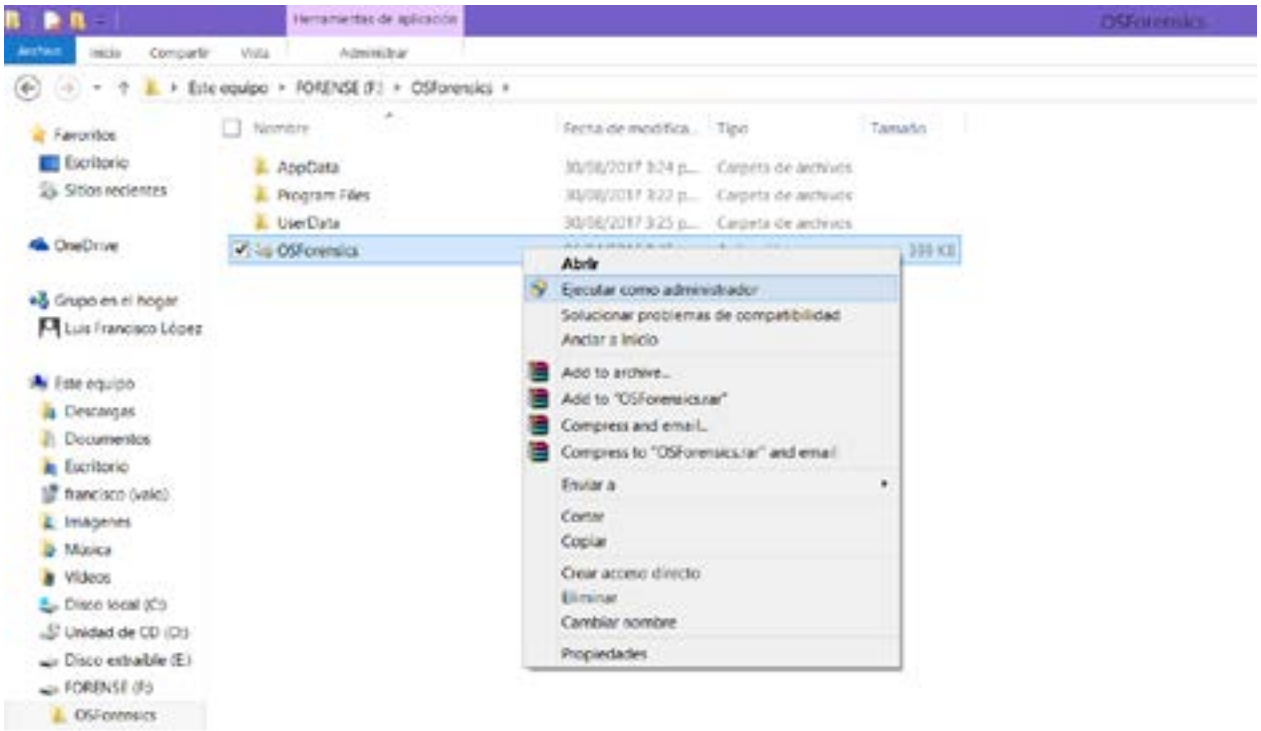


Figura 18. Abrir OSForensics desde equipo víctima
Fuente: propia

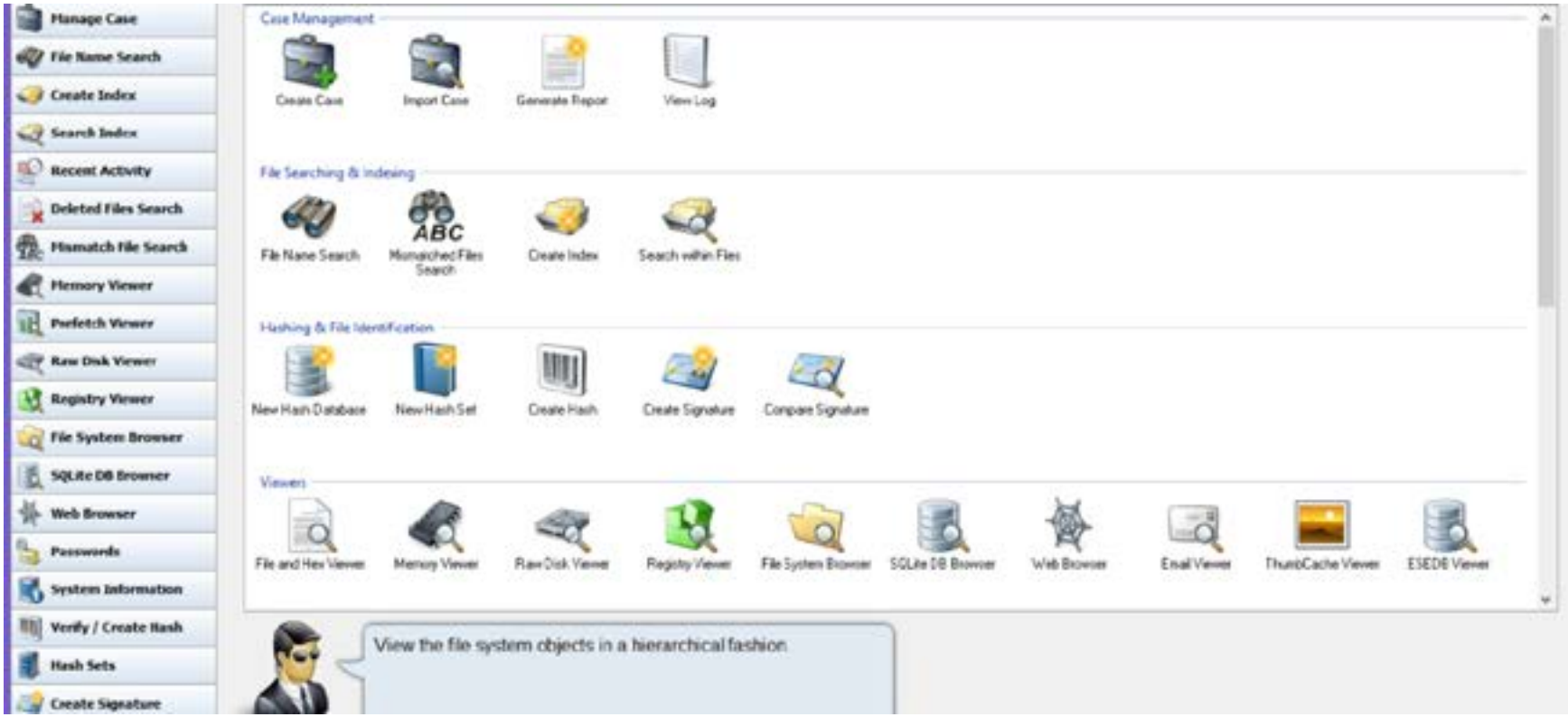


Figura 19. OSForensics desde USB
Fuente: propia

Para hacer el análisis y generar el archivo de volcado de la memoria física del equipo objeto del análisis, seleccionamos la opción memory viewer y entre las opciones que se despliegan elegimos la opción Dump Physycal Memory, al hacer click en la opción se abre un cuadro del navegador para seleccionar el lugar donde deseamos guardar la copia de la memoria física, para este caso selecciono la opción de guardar en el medio estéril. El procedimiento puede tardar un poco depende del contenido de la memoria, no olvide que esta es la primera copia (original), así que a través del mismo programa podemos crear el HASH del archivo que contiene la captura de la memoria.

El cálculo del HASH del archivo que se obtiene al volcar la memoria física se aplica al seleccionar la opción Verify/Create hash; seleccionamos la opción, en el archivo de entrada escogemos el archivo creado, escogemos el algoritmo de codificación que consideremos necesario, el programa nos permite escoger el algoritmo SHA1, MD5, CRC 32, SHA-256. Una vez escogemos el algoritmo aplicamos la función sobre el archivo y obtenemos el valor del HASH.

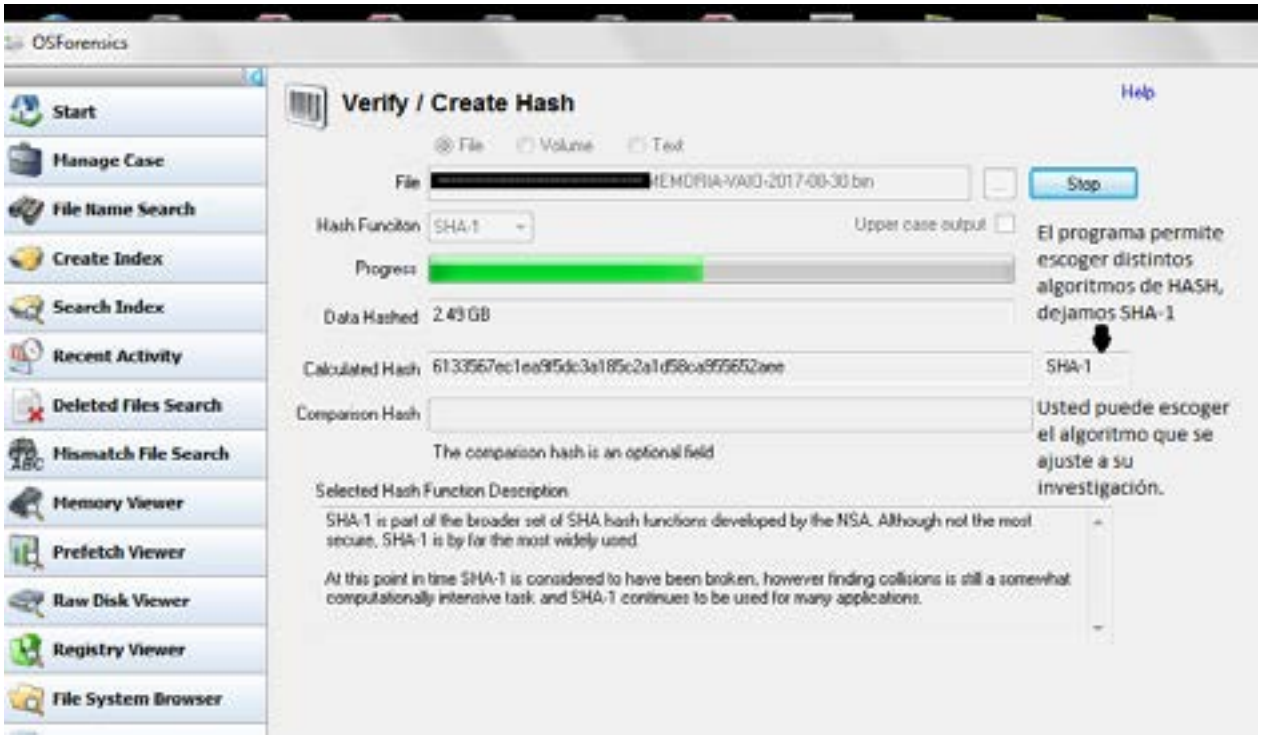


Figura 21. HASH de figura memoria OSForensics
Fuente: propia

Una vez finaliza el proceso, obtenemos un valor de hash con el algoritmo SHA-1 (en este caso para el archivo) copiamos este valor en un archivo de texto, y capturamos una imagen con el valor obtenido. Cuando se hacen los distintos análisis y cuando se presenta como posible evidencia el archivo, se debe aplicar un nuevo cálculo de hash y los valores obtenidos en las diferentes etapas del proceso debe ser idéntico. De esta forma se garantiza la integridad del archivo que se está analizando y que puede ser usado como evidencia.

Figura 22. Valor HASH SHA-1
Fuente: propia

Apreciado investigador, el formato del archivo que usted obtiene con la captura de memoria es .bin, así para poder analizar el contenido del archivo obtenido del volcado de memoria recomiendo usar la utilidad volatily, de forma inicial se desarrolló para usar en sistemas LINUX, pero con el paso del tiempo se ha habilitado para sistemas tipo WINDOWS a través de la ejecución de un SCRIPT que entre otras opciones descarga un instalador de PHYTON que es el lenguaje original bajo el que está escrita. Le recomiendo descargar la utilidad y hacer simulaciones de volcado de memoria. En el enlace puede obtener el script que permite descargar la utilidad volatily para Windows.

Es necesario recordarle que el análisis del volcado de memoria no trae las imágenes o documentos que se ejecutaban en el momento de la captura, volatily le mostrará entre otros los siguientes objetos que pueden contribuir de forma significativa en su labor de investigación:

- Fecha, hora y características del sistema.
- Procesos en ejecución.
- Puertos conectados y abiertos.
- Valores de registro usados por los procesos.
- Las DLL que cada proceso ejecuta.
- Módulos del núcleo del sistema operativo.
- Direcciones de memoria usadas por cada proceso.
- Ejecutables que se encuentran en memoria.
- Mapeo de direcciones y correspondencia en memoria virtual.

El listado anterior destaca algunos de los datos más importantes que usted puede obtener a través de la utilidad volatily en el análisis del archivo obtenido con el volcado de memoria RAM.

Los discos duros

Uno de los elementos de un sistema de procesamiento de información que puede aportar la mayor parte de información en relación con nuestra investigación de carácter forense es el disco duro. Por ser el medio de almacenamiento (permanente) por excelencia en cualquier computador, a través de un cuidadoso análisis podemos recabar información valiosa para nuestro trabajo forense. Antes de entrar en detalles en relación con su adquisición y análisis es necesario recordar algunos conceptos básicos en relación con este medio de almacenamiento y realizar la actividad de repaso 2:

El proceso de adquisición de las imágenes de los medios o elementos que pueden contribuir para responder preguntas clave de la investigación como: ¿Quién realizó el ataque? ¿Cómo lo hizo? ¿Por qué lo hizo? ¿Qué medios utilizó? Se puede desarrollar a través de variadas herramientas que se encuentran disponibles en el mercado, así que una de las primeras decisiones que afronta el investigador digital es qué herramienta empleo para pal investigación?

1. Al frente de cada uno de los términos explique en qué consiste cuando se hace una investigación digital forense:

- Asegurar la escena.
- Recolectar.
- Adquirir.
- Analizar.
- Preservar.
- Presentar.

2. Usted como investigador digital forense recibe una computadora que fue hallada en la escena de un crimen, una mujer fue hallada muerta, por causa indeterminada. Responda las preguntas que se presentan, argumente su respuesta:

a. Tipo de análisis.

b. De qué elementos adquiere sus imágenes para análisis.

c. Cómo asegura la integridad de la imagen.

d. Sobre qué copia de la imagen realiza el análisis.

e. Sobre qué elementos de la imagen obtenida efectúa el análisis.

3. Un compañero de trabajo le solicita recomendar una aplicación que le permita recuperar una gran cantidad de información que se borró luego de un formateo del disco duro, ¿qué información adicional necesita antes de recomendar alguna utilidad?, ¿qué utilidad recomienda?, ¿por qué?

4. Un investigador digital forense recibió un laptop para que efectuara un análisis en él, para acelerar el proceso instaló en el equipo la utilidad OSForensics. Evalúe la acción del investigador y explique por qué esta acción puede invalidar la evidencia.

a. ¿Requiere alguna autorización especial para acceder al servidor y desarrollar las tareas de recolección y adquisición de la evidencia (correos electrónicos enviados y recibidos) en la cuenta del empleado que está siendo investigado? Justifique su respuesta.

b. Luego de desarrollar la tarea, el abogado del investigado entabla una demanda en su contra por violar su derecho a la intimidad. ¿Tiene posibilidad de prosperar la demanda? Desarrolle su respuesta.

c. ¿Por qué un correo electrónico corporativo no se considera una extensión de la órbita personal del usuario? Explique su respuesta.

Clases de discos duros

En la actualidad los tipos de discos que se comercializan o distribuyen con computadores nuevos son:

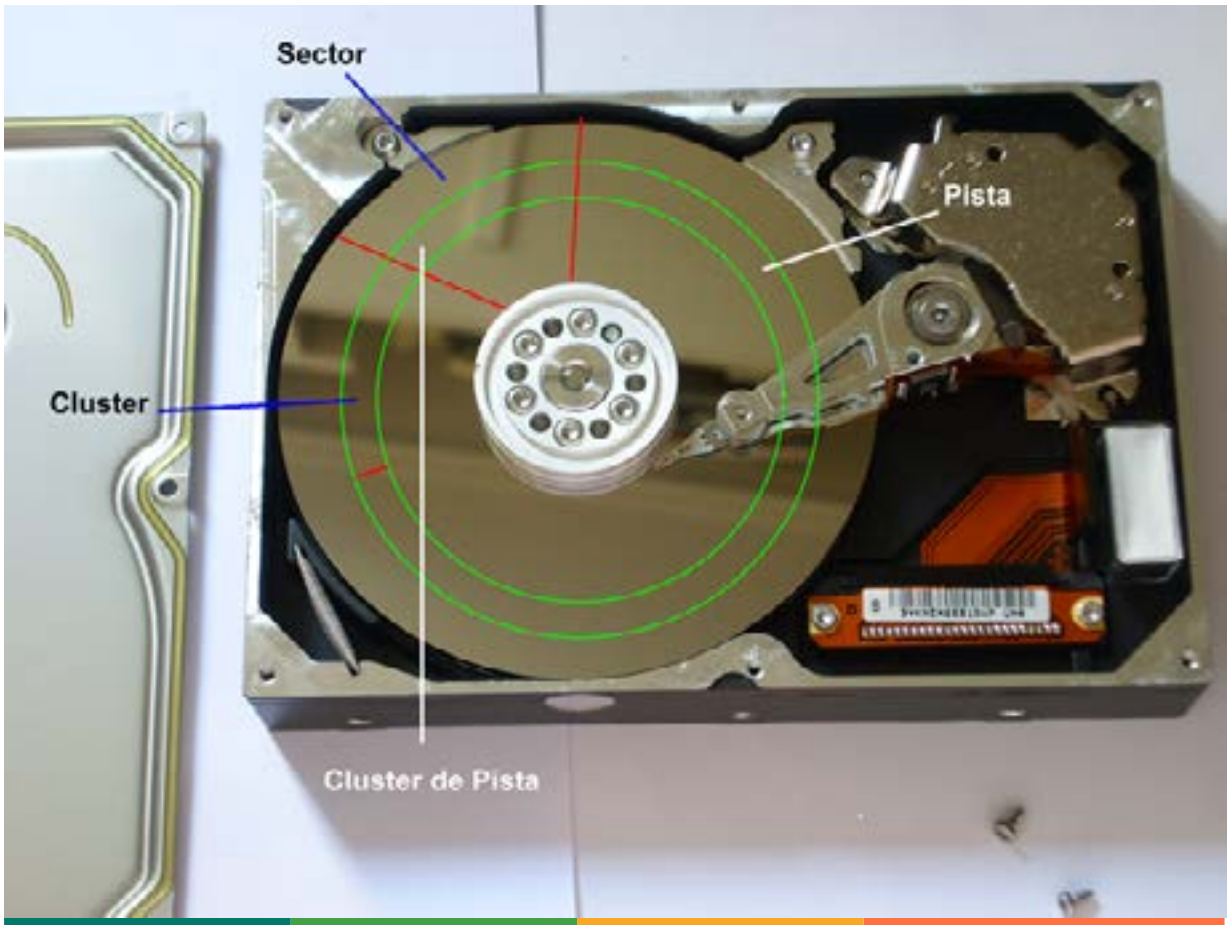
- Discos de Estado Sólido (SSD): este tipo de disco se destaca por su eficiencia energética y velocidad, su modo de funcionamiento es semejante al de las memorias USB. Su tecnología implica una baja latencia y alta velocidad de acceso por lo que, en la actualidad y a futuro, están llamado a convertirse en el estándar de almacenamiento de información.

- Discos Duros SATA: la evolución en la historia de los discos duros, ha estado marcada por el mismo principio de funcionamiento que se mantiene inclusive hasta esta clase de disco, es decir en efecto se trata de uno o varios discos o platos rígidos recubiertos por una capa de material magnetizable sobre el cual a través de un cabezal se escriben y leen los datos. El término SATA (Serial Advanced Technology Atachment) hace referencia a la tecnología bajo la cual se conecta el disco con la tarjeta madre y el resto del sistema, es la evolución de la tecnología anterior de conexión que se conoce bajo el nombre PATA o IDE. La cantidad de información que procesa un sistema y el tamaño cada vez mayor de los archivos implicó un cambio de tecnología, ya que la tecnología PATA alcanzaba una velocidad de hasta 150 Mb/s, mientras que un disco SATA transfiere a velocidades de hasta 600 Mb/s, además, reduce el consumo de energía y elimina la necesidad que existía en la tecnología IDE de configurar los discos a través de un puente para marcarlos como maestro o esclavo.

- Discos Duros SAS: son la evolución tecnológica de los discos SCSI, una de sus ventajas es su alta velocidad y las elevadas tasas de transferencia de información, algunas pruebas muestran tasas de hasta 6 GB/s. Se usan de forma predominante en servidores de almacenamiento como los IBM System Storage, Servidores de discos duros de HP, entre otros. Si tenemos en cuenta sus características, un factor que limita su uso en equipos de oficina u hogar es su costo elevado, se estima que pueden costar cuatro veces el valor de un disco SATA.

Estructura físico-lógica de los discos duros

Para comenzar observemos esta infografía:



Sector	Pista	Clúster de Pista	Clúster
Un sector de un disco duro es la sección de la superficie del mismo que corresponde al área encerrada entre dos líneas radiales de una pista.	Una pista de unidad de disco es un camino circular en la superficie del disco magnético (disco duro o disquete) donde la información es grabada magnéti-camente y de la cual también se lee la información registrada.	Porción de sector que se encuentra ubicada en una pista específica y delimitada por los límites del sector.	Es un conjunto de sectores contiguos que componen la unidad más pequeña de almacena-miento de un disco. Los archivos se almacenan en uno o varios clústers, dependiendo de su tamaño de unidad de asignación. Sin embargo, si el tamaño de archivo es menor que el tamaño de un clúster, este lo ocupa completo.

Figura 23. Estructura lógica del disco duro
Fuente: propia

Según la forma como se construyen los discos duros y la necesidad de organizar la información en su interior, los dos elementos fundamentales que se emplean para organizar los archivos en él son:

- Clústeres: también se le conoce como unidad de asignación, es la menor cantidad de espacio que se puede asignar en el disco para almacenar un archivo, la estructura de los discos se organiza a partir del tamaño del clúster. En sistemas tipo NTFS los clústeres se encuentran numerados de forma secuencial en números de clúster lógicos.

- Sectores: se conoce bajo ese nombre a las unidades de almacenamiento que contiene el disco duro y que se agrupan en el clúster; así, si un disco tiene sectores de 512 bytes y el tamaño del clúster es 512 entonces el clúster contiene un sector, si en cambio el clúster es de 8 kilobytes entonces contendrá 8 sectores. En el momento del inicio del sistema operativo el computador accede a sectores específicos del disco duro en os que se encuentra información clave en referencia al sistema operativo que se va a iniciar y dónde están ubicadas las particiones, esta información puede variar según el sistema operativo instalado en el sistema.

- Sistemas de archivos en los discos duros: la información de un sistema de procesamiento de información que se guarda o almacena en un disco duro, se encuentra en forma de bits (colecciones de unos y ceros), estos bits se escriben sobre la superficie de los platos que conforman el disco duro. Los grupos o cadenas de bits se almacenan de acuerdo a un orden que viene determinado por el sistema operativo, a través de complejos algoritmos se toma la decisión respecto al lugar o lugares en los que serán almacenados los unos y ceros que conforman un archivo, la forma como se podrá acceder a él, los datos adicionales (metadatos) que serán añadidos al archivo para etiquetarlo y facilitar su búsqueda entre otras tareas. Así el sistema de archivos gestiona la estructura física del disco duro y la organiza de tal forma que se puedan escribir y acceder los archivos guardados en el medio. Los sistemas de archivos más comunes de acuerdo a los sistemas operativos que se usan en la mayoría de computadores en la actualidad son:

1. NTFS: Es el sistema de archivos de los sistemas operativos de la familia Windows, es el acrónimo de New Tecnology File System, y es una evolución del sistema de archivos de los sistemas IBM OS/2 HPFS. Se caracteriza porque permite cifrar los archivos, agregar metadatos, y su tolerancia a fallos. La base para este sistema de archivos es la Tabla Maestra de Archivos o MFT, que se encuentra al interior del volumen (en una investigación forense esta es la primera misión, encontrar la MFT) en ella existe un registro que corresponde a cada archivo y carpeta que se crean dentro del volumen. Los metadatos que se usan para crear y mantener la estructura del sistema de archivos se encuentran en los primeros bytes de la tabla. La estructura del sistema de archivos NTFS se detalla en la siguiente tabla.

N°	Entrada del sistema	Descripción
1	$AttrDef	Esta lista contiene los atributos de los archivos
2	$BadClus	Registra una lista de clúster o sectores que tienen errores irrecuperables
3	$Bitmap	Muestra la disponibilidad y uso de los clúster
4	$Boot	Se utiliza para montar el volumen NTFS durante el proceso de "bootstrap"
5	$I30	Papelera, índice de elementos borrados
6	$LogFile	Listada las transacciones previas y almacenadas para futuras posibles restauraciones
7	$MFT	Archivo de registro base para un volumen NTFS, fundamental para nuestro análisis forense
8	$MftMirr	Almacena Los primeros cuatro registros del MFT para posibles restauraciones en caso de fallo o corrupción de la MFT primaria
9	$Secure	Esta lista de control de acceso, contiene los descriptores de seguridad únicos para los archivos sobre el volumen
10	$Volumen	Esta tabla almacena la información relacionada con el volumen.
11	$Upcase	Convierte todos los caracteres en mayúscula a caracteres Unicode minúscula
12	$	Esta es la carpeta Raíz
13	$Extend	Contiene la lista de las extensiones opcionales como cuotas e identificadores de objetivos

Tabla 1.
Fuente: https://support.microsoft.com/es-es

La figura nos permite identificar la arquitectura de NTFS.

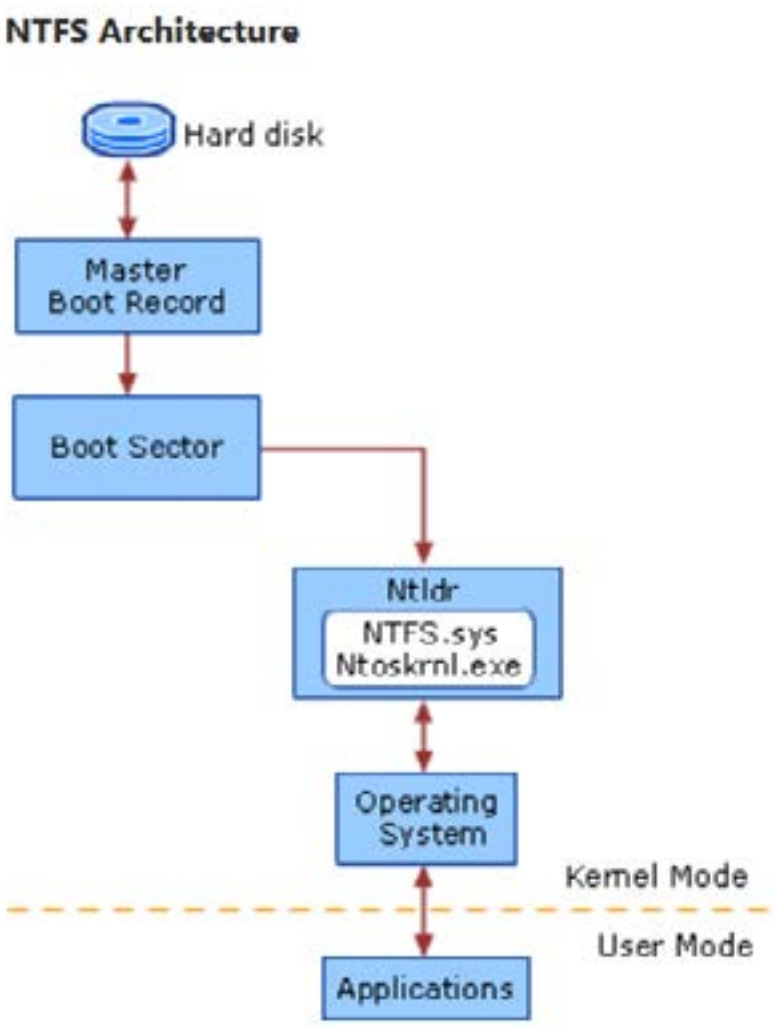


Figura 24. Estructura NTFS
Fuente: Microsoft.com Biblioteca Technet, How NTFS Work

Para información complementaria acerca del funcionamiento del sistema de archivos NTFS por favor consulte https://technet.microsoft.com/es-es/library/cc781134(v=ws.10). Es claro que por ser el sistema de archivos que usan los sistemas operativos Windows y por ser estos equipos lo de uso más frecuente en los escenarios a analizar, usted como investigador forense debe profundizar en este tipo de sistemas. El sistema NTFS no puede ser escrito desde sistemas tipo OS (MAC) o Linux.

Para el caso de las unidades removibles, memorias USB o flash, por el tamaño de los medios y su condición de medio de almacenamiento extraíble, se usa casi que en su totalidad el sistema de archivos FAT; se recomienda consultar la información relacionada con el sistema de archivos FAT a la que puede acceder en el enlace: https://technet.microsoft.com/es-es/library/cc776720(v=ws.10).

- Apple Mac OS X: HFS+ o Hierarchical File System: el sistema de archivos jerárquico se usa en los sistemas operativos tipo OS para los computadores de la familia Macintosh, se emplea desde la versión OS/X. Funciona de una forma en apariencia simple, crea un solo directorio que se expande cuando se agregan archivos y carpetas al disco duro. Este sistema emplea una tabla de asignación de archivos de 32 bits y permite la bifurcación de archivos, además se basa en una estructura denominada árbol-B para almacenar los metadatos.

- Es necesario informar que la empresa Apple, propietaria de todos los productos de la línea Macintosh (Appletv, iPhone, Mac Book, iMac) busca unificar los sistemas de archivos en todos sus dispositivos por lo que ya está listo el desarrollo del nuevo sistema de archivos para los equipos de la familia Mac, conocido bajo el nombre de APFS (Apple File System). Se espera que para el año 2018 todos los equipos de la familia Macintosh hayan migrado al nuevo sistema de archivos, los equipos nuevos que se venden en la actualidad ya vienen con el sistema de archivos APFS pre instalado. Un volumen HFS+ está compuesto por nueve estructuras que se presentan en la siguiente tabla:

N°	Nombre entrada	Descripción
1	Bloques de arranque	Se encuentran en los sectores 0 y 1 y son idénticos a los bloques de arranque encontrados en HFS.
2	Volume Header	Se encuentra en el sector 2 y es el equivalente al Master Directory Block en un volumen HFS. Almacena datos sobre el volumen, incluyendo el tamaño de los bloques de asignación, las marcas de tiempo y las ubicaciones de otras estructuras de volumen, como el archivo de catálogo o el archivo de exceso de extensión. Siempre se encuentra en el mismo lugar.
3	Archivo de Asignación	Hace un seguimiento de los blocks que están libres y de los que están en uso. Al igual que en el mapa de bits de volumen en HFS, cada bloque de asignación está representado por un bit. Un bit cero significa que el bloque está libre, mientras que un bit indica hacia un bloque en uso. El archivo de asignación difiere del mapa de bits de volumen de HFS al ser almacenado como un archivo normal, no ocupando un espacio especial reservado al principio del volumen. También puede cambiar de tamaño y no tiene que ser almacenado contiguamente dentro de un volumen.

4	Archivo de catálogo	Es un árbol B que contiene registros para todos los archivos y directorios almacenados en el volumen, comparable al archivo de catálogo HFS. Su diferencia principal es que los registros con HFS + son más grandes para permitir más campos y permitir que estos campos sean más grandes. Esto se ve en el tamaño del archivo de catálogo HFS + que es de 4 KB en Mac OS y 8 KB en Mac OS X, en contraposición al archivo de catálogo HFS, con sólo 512 bytes de tamaño. Los campos en HFS + también varían dependiendo de los datos que almacenan, a diferencia de HFS donde los campos son fijos.
5	Extents Overflow File	Es un árbol B que registra los bloques de asignación que se asignan a cada archivo como extents. Cada archivo en el registro de archivo de catálogo puede grabar hasta ocho extensiones para cada bifurcación de un archivo; se registran extensiones adicionales en el archivo Extents Overflow. Bloques malos también se registran como extensiones aquí. Los tamaños predeterminados para este archivo son 1 KB en Mac OS y 4 KB en Mac OS X.
6	Atributos Archivo	Es un árbol B que solo se encuentra en HFS +. Puede almacenar tres tipos de registros de 4 KB: registros de Atributos de Datos en Línea, registros de Atributos de Datos de Horquillas y registros de Atributos de Extensión. Sus propósitos se enumeran en la tabla a continuación.
7	Startup File	Está diseñado para sistemas que no son de Mac OS sin soporte HFS o HFS +; comparable a los bloques de arranque de volumen HFS.
8	Encabezado de volumen alternativo	Se encuentra en el segundo último sector de un volumen HFS + y es el equivalente del bloque de directorio maestro alternativo HFS.
9	Último sector	Está reservado para su uso por Apple durante el proceso de fabricación del equipo.

Tabla 2.
Fuente: http://ntfs.com/hfs.htm

Le recomiendo una lectura más completa del análisis en el sistema de asignación de archivos HFS+ en el siguiente enlace: mac.forensics.craiger-burke.IFIP.06.

Linux: EXT o Extended Filesystem: es el sistema de archivos de los sistemas operativos Linux, dentro de sus evoluciones se encuentra el EXT2, EXT3, EXT4; se caracteriza por que se basa en el sistema original de archivos de UNIX, soporta nombres de archivos desde 255 a 1012 caracteres y el tamaño de un archivo puede superar 1 exbibyte (ext4). En su versión más avanzada, permite crear un número infinito de subdirectorios. A su vez permite crear extensiones (rango de bloques físicos que se encuentran uno a continuación del otro) de hasta 128 MB. Al igual que en los sistemas tipo UNIX introduce el concepto de INODOS. Retrasa la asignación de bloques hasta tanto los datos sean depositados en el disco, esta característica hace más eficiente el uso del espacio pues reduce la fragmentación dado que se asigna el bloque una vez conocida su ubicación en el disco. Recomiendo consultar la información relacionada con el sistema de archivos EXT que encuentra en la página principal del eje.

INODO

Representa la estructura de datos en sistemas tipo UNIX, describe un objeto del sistema de archivos puede ser un archivo o un directorio. Cada inodo debe almacenar no solo la ubicación del bloque en el que se encuentra el archivo, además conserva os metadatos relacionados con el archivo u objeto, fecha de creación, último acceso, propietario entre otros datos.

BIBLIOGRAFÍA

Bbrezinski, D. y Killalea, T. (2002). RFC 3227: *Guidelines for Evidence Collection and Archiving. Network Working Group. February.* Recuperado de http://www.rfc-editor.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). *Guía 13. Evidencia digital. Serie seguridad y privacidad de la información*. Bogotá: Ministerio de las Tecnologías de la Información y las Comunicaciones.

Watson, D. y Jones, A. (2013). *Digital Forensics Processing and Procedures*. Londres, Reino Unido: Ed. Syngress.

Microsoft (2017). *How NTFS Works. Technet*. Biblioteca. Recuperado de: https://technet.microsoft.com/es-es/library/cc781134(v=ws.10)