Lab 2.2 - Triage Imaging with KAPE

Triage Acquisition

Triage Acquisition es una metodología en el campo de la Informática Forense y la Respuesta a Incidentes (DFIR, por sus siglas en inglés) **que se utiliza para adquirir rápidamente datos forenses relevantes de un sistema o dispositivo digital.** Esta técnica se emplea para obtener una visión inicial de la situación y recopilar información crítica de manera rápida y eficiente, sin la necesidad de realizar un proceso exhaustivo de adquisición forense.

Triage Acquisition se utiliza principalmente en situaciones donde el tiempo es un factor crítico, como en la respuesta a incidentes de seguridad, investigaciones de delitos cibernéticos, evaluación de amenazas y ataques, o en casos de emergencia donde se requiere una acción inmediata para preservar la integridad de los datos.

El objetivo principal de la Triage Acquisition **es recopilar datos esenciales de manera rápida para permitir a los investigadores tomar decisiones informadas sobre el curso de la investigación o para implementar medidas de respuesta adecuadas.**

Esto puede incluir la extracción de registros de eventos, la identificación de archivos y procesos sospechosos, la recopilación de información sobre la red y el sistema, entre otros.

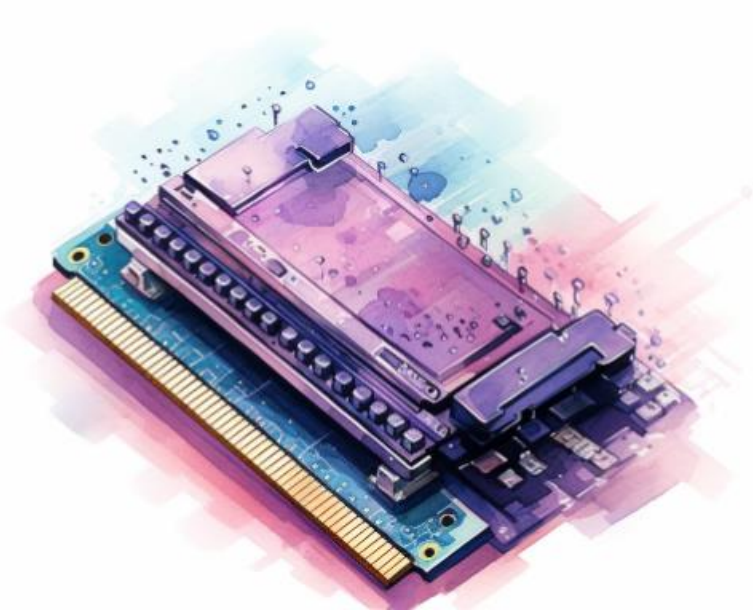
Es importante destacar que la **Triage Acquisition no reemplaza la adquisición forense completa y exhaustiva, sino que complementa este proceso al proporcionar una visión inicial de la situación y permitir una acción rápida.** Los datos adquiridos durante la Triage Acquisition pueden ser utilizados para iniciar investigaciones más detalladas y procesos forenses posteriores.

Step by Step Triage acquisition

En el paso a paso sobre un triage acquisition tenemos :

1. **Image RAM**: Es decir, capturar la memory
2. **Check Disk Encryption**: Nos apoyamos de herramientas como EDD.EXE
3. **Create Quick Triage Image**: Nos apoyamos de herramientas como KAPE
4. **Análisis del Triage image**: Usamos la misma herramienta de KAPE para el análisis
5. **Image Entire Hard Drive**: Solamente si es necesario, se crea una imagen del disco

Paso 1: Image RAM



La adquisición de memoria se ha convertido en uno de los cambios más importantes en el campo de la informática forense. La adquisición de memoria no es algo nuevo; ha estado presente durante más de 15 años.

Con la creciente popularidad de los programas de cifrado, **desconectar el enchufe de corriente ya ha resultado en que las agencias de investigación no tengan nada que examinar**. Además, una afirmación cada vez más popular de los abogados defensores es que el sistema estaba siendo controlado por una utilidad/Troyano administrativa remota o que un virus estaba causando toda la

actividad. Sin la recopilación de datos volátiles, esta posición se vuelve mucho más difícil de defender o refutar.

Al responder a un incidente que involucra evidencia digital, **la regla general para los primeros incident responder debe ser preservar la mayor cantidad de datos posible de la manera en que se encontraron cuando llegaron. La prioridad más inmediata debe ser capturar datos volátiles.**

Los datos volátiles se refieren a los datos que desaparecerán o serán destruidos una vez que el sistema informático se apague. Típicamente, esto incluye la RAM, pero va más allá. Los datos volátiles también incluyen las conexiones de red activas actuales, las aplicaciones en ejecución, las conexiones de red abiertas/escuchando, etc.

Gran parte de estos datos son extremadamente valiosos para determinar o refutar la afirmación de que alguien estaba conectado remotamente al ordenador controlando su actividad y, por lo tanto, el sospechoso/acusado es inocente. Se vuelve extremadamente difícil (no imposible) refutar estas afirmaciones si no se recopilan datos volátiles.

Cambiará la evidencia: Muchos argumentan que la recopilación de datos volátiles cambiará/alterará el estado actual de la evidencia tal como la encontró el investigador y, por lo tanto, la volverá inadmisible como evidencia. **Esto simplemente NO es cierto.**

¿Qué hay en la memoria y por qué debe ser adquirida?

En la memoria podemos encontrar lo siguiente:

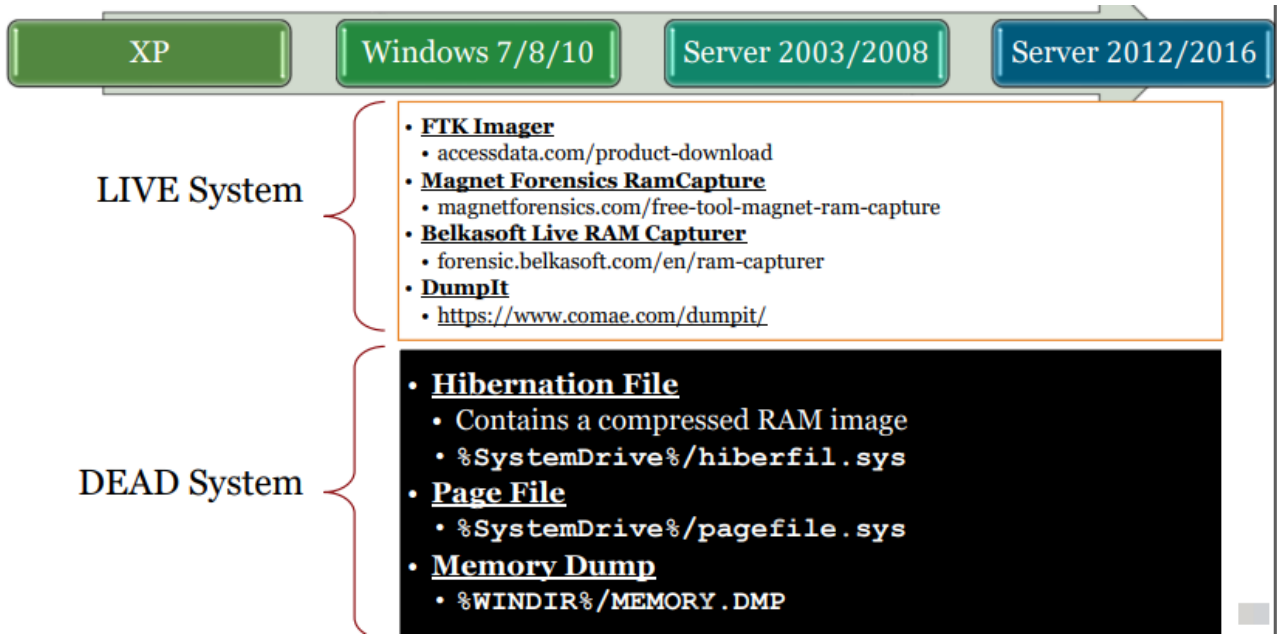
1. Procesos
2. Archivos abiertos y llaves de registros
3. Conexiones de Red
4. Configuración de parámetros
5. Encryption keys and passwords
6. Memory – only exploits / rootkit

Tienes todos los procesos, archivos, directorios y cualquier otra información que podría estar presente en la memoria residual. Se Puede usar esta información para reconstruir antiguos historiales y comandos que un usuario anterior podría haber escrito en el sistema.

Se puede descubrir antiguos correos electrónicos o sitios web que el usuario visitó, por otra parte, encontrar residuos de procesos que han finalizado. **Y probablemente lo más importante, es probable que**

tengas contraseñas tanto para el cifrado como para otros programas en texto claro aún presentes en la memoria.

Con el aumento del uso del cifrado, especialmente de utilidades de cifrado de disco completo como Windows BitLocker, PGP y TrueCrypt, es más importante ahora que nunca para los respondedores a incidentes crear una imagen de la RAM y recopilar datos volátiles en cualquier sistema encendido al que respondan. Si bien es la evidencia más volátil, también es una de las más valiosas.



Para crear una imagen de la RAM podemos usar **DumpIT** (está en nuestra máquina virtual)

Paso 2: Check Disk Encryption

Entonces, hasta ahora hemos creado una imagen de la RAM, y lo mas probable pensemos que, dado que se han recopilado los datos volátiles, es hora de desconectar el enchufe de corriente.

Hay dos cosas que debes considerar antes de desconectar el enchufe. Primero, **¿hay algo que sugiera que el dispositivo podría estar utilizando algún tipo de cifrado? ¿Hay tal vez una carpeta/volumen cifrado que esté actualmente montado, y una vez que desconectes la corriente, es posible que no tengas acceso al contenido de esa carpeta/volumen? ¿Qué pasa si el disco está cifrado completamente?**

Una de las cosas más importantes que debes hacer antes de apagar un sistema para quitar un disco duro es verificar si el disco está cifrado o no. Demostramos este paso en un esfuerzo por asegurar que los discos conectados no estén actualmente cifrados.

Si hubiera indicios de que el disco está cifrado, sería recomendable crear una imagen del disco mientras está encendido y en funcionamiento. Si lo apagas, es probable que no puedas recuperar las claves.

Si realizas una imagen en vivo de un disco debido al cifrado, siempre debes crear una imagen del disco lógico en lugar del físico. El disco lógico se ve como no cifrado por la

máquina local, mientras que el disco físico todavía está cifrado a nivel de disco.

¿Qué contiene un Triage Image?

Un triage image contiene los siguientes artefactos:

1. Registry hives y backups
2. LNK Files
3. Jump Lists
4. Prefetch
5. Event Logs y PnP Logs
6. Data del browser
7. Recycle Bin
8. Master File Table (MFT)
9. NTFS journal files
10. Pagefile y Hibernation files

Casi cualquier imagen de triaje de contenido personalizado, tomaríamos los siguientes archivos/artefactos listados. Usando la creación de imágenes de triaje de **KAPE**,

- **$MFT**: La tabla maestra de archivos, que es el índice de cada archivo y carpeta en el sistema.

- $Logfile y $USN $J (Journal): El archivo que registra la actividad de los archivos (apertura, cierre, creación, eliminación).

- Todos los archivos de registro y tal vez los archivos de registro de respaldo:

- SAM
- SYSTEM
- SOFTWARE
- DEFAULT
- NTUSER.DAT
- USRCLASS.DAT

- *.evtx: Estos son registros de eventos por su extensión de archivo, ubicados en la carpeta **%WinDir%\System32\winevt\Logs**.

- Otros archivos de registro: Estos incluyen setupapi.dev.log (registro de plug-and-play), registros de firewall, registros de IIS, etc., [root]\Windows\System32\LogFiles y [root]\inetpub\logs\LogFiles (para los registros de IIS si IIS está activado).

- *.lnk files: Estos son todos los archivos de enlace con extensión .lnk.

- ***.pf**: Estos son todos los archivos de prefetch con extensión .pf.

- **Pagefile.sys:** El archivo de paginación de Windows (una extensión de la RAM).

- hiberfile.sys: El archivo de hibernación es una imagen comprimida de la RAM la última vez que el sistema se colocó en hibernación.

• **La carpeta RECENT y sus subcarpetas**: Estas incluyen listas de acceso rápido (**jumplist**) (para Windows Vista/7/8).

• La carpeta principal del usuario de "**APPDATA**": Esto debería extraerse, ya que contiene la caché, historial, archivos de cookies y más.

Con los datos capturados anteriormente, más del 80% del tiempo se dedica a examinar los artefactos.

KAPE

KAPE (Kroll Artifact Parser and Extractor). KAPE es una herramienta desarrollada por **Eric Zimmerman** que se utiliza en el campo de la informática forense para la recopilación, análisis y extracción de artefactos digitales de sistemas informáticos.

KAPE es una herramienta extremadamente versátil y potente que permite a los investigadores forenses automatizar una amplia gama de tareas, desde la recopilación de datos volátiles hasta la extracción de artefactos de sistemas de archivos, registros y otros lugares relevantes en un sistema informático.

Algunas de las características clave de KAPE incluyen:

1. **Flexibilidad en la recopilación de datos**: **KAPE permite a los usuarios crear y personalizar paquetes de recopilación de datos para adaptarse a las necesidades específicas de cada investigación**. Esto significa que los investigadores pueden recopilar solo los artefactos relevantes para su caso particular.

2.**Automatización de tareas repetitivas**: KAPE automatiza muchas tareas que de otro modo serían tediosas y propensas a errores, lo que ahorra tiempo y recursos al investigador forense.

3. **Soporte para múltiples plataformas**: KAPE es compatible con una amplia gama de sistemas operativos, incluidos Windows, Linux y macOS, lo que lo hace útil para una variedad de escenarios de investigación.

4. **Extracción de artefactos forenses**: KAPE puede extraer una amplia variedad de artefactos forenses, incluidos registros de eventos, archivos de registro, archivos temporales, cookies de navegador, historiales de navegación, listas de acceso rápido, entre otros.

¿Por qué usar KAPE?

KAPE es principalmente un programa de triaje que apuntará a un dispositivo, encontrará los artefactos más relevantes desde el punto de vista forense y los analizará en cuestión de minutos.

Además, KAPE se puede utilizar para recopilar los artefactos más críticos al inicio del proceso de imagen tradicional. Mientras la imagen se completa, los datos generados por KAPE pueden ser revisados en busca de pistas, para construir líneas temporales, etc.

KAPE está impulsado por Target y Modules.

Tanto los Target como los Modules se definen utilizando YAML

Target: Collecta archivos/ folders

Modules: Procesa archivos /folders, también puede correr programas para colectar la memoria

Estas operaciones pueden ser usadas en conjunto o separadas.

Laboratorio: Triage imaging con KAPE

Objetivos

La recopilación de evidencia es posiblemente el paso más importante en el ciclo de vida de la evidencia digital. Generalmente, solo tienes una oportunidad para hacerlo bien, y los errores en la recopilación pueden destruir la evidencia.

Cuando respondes a un sistema en vivo, necesitarás actuar rápidamente para capturar la RAM, determinar si la unidad está cifrada y tomar una decisión informada sobre si crear una imagen en vivo o desconectar la energía del sistema. Retrasos o errores por parte del respondiente al incidente pueden resultar en una serie de resultados, incluida la modificación del sistema de archivos, el bloqueo de la pantalla o otros cambios significativos en el sistema.

Realizar una imagen de toda una unidad lleva horas. En investigaciones de alta prioridad, es posible que necesites que uno o más examinadores revisen los datos de una unidad de inmediato.

Realizar imágenes solo de porciones seleccionadas y artefactos de una unidad, aquellas áreas que sabemos tienen el mayor potencial para la información que estamos buscando, y luego proporcionar copias de esa imagen a varios examinadores puede marcar la diferencia en una investigación de rápida evolución. La imagen de

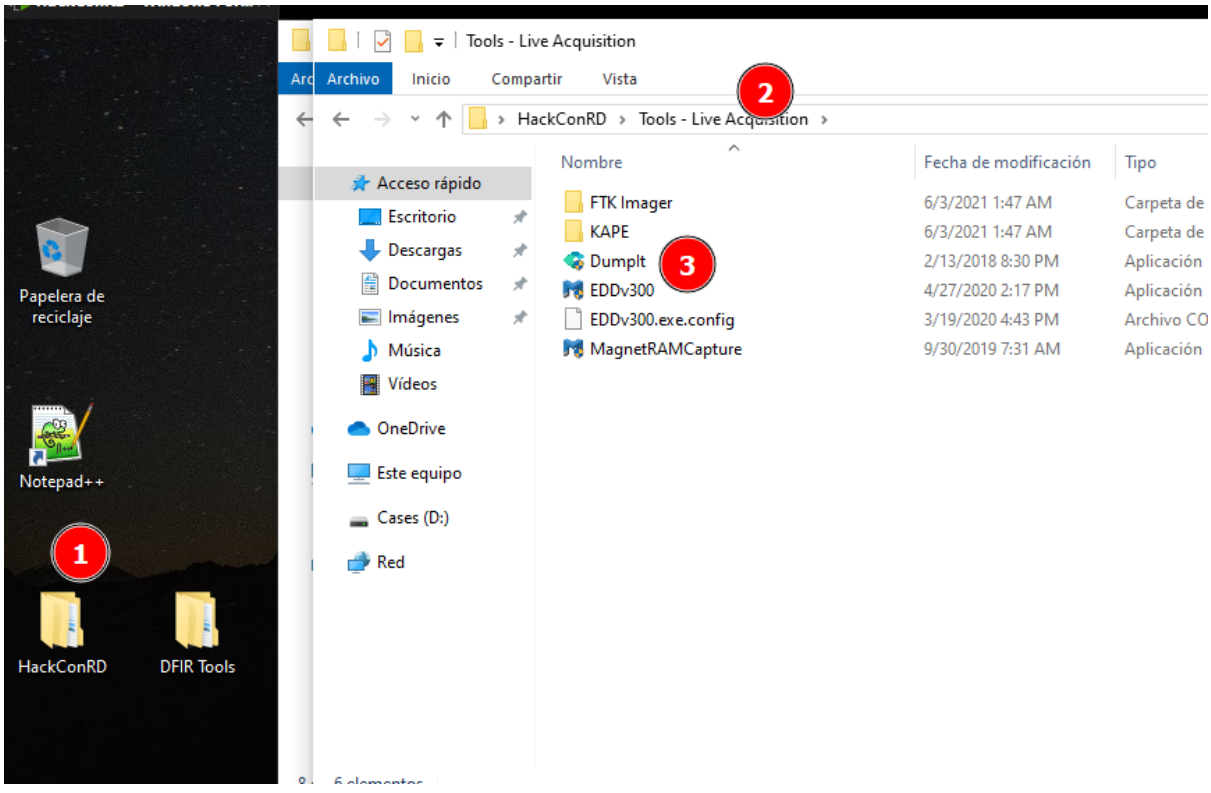
triage puede ser seguida por una imagen completa del disco si es posible.

KAPE es una herramienta gratuita que se puede utilizar para dirigirse a archivos específicos, carpetas y artefactos forenses para crear imágenes de triaje. KAPE también puede preprocesar los datos de triaje recopilados mediante la ejecución de herramientas forenses contra los datos recopilados.

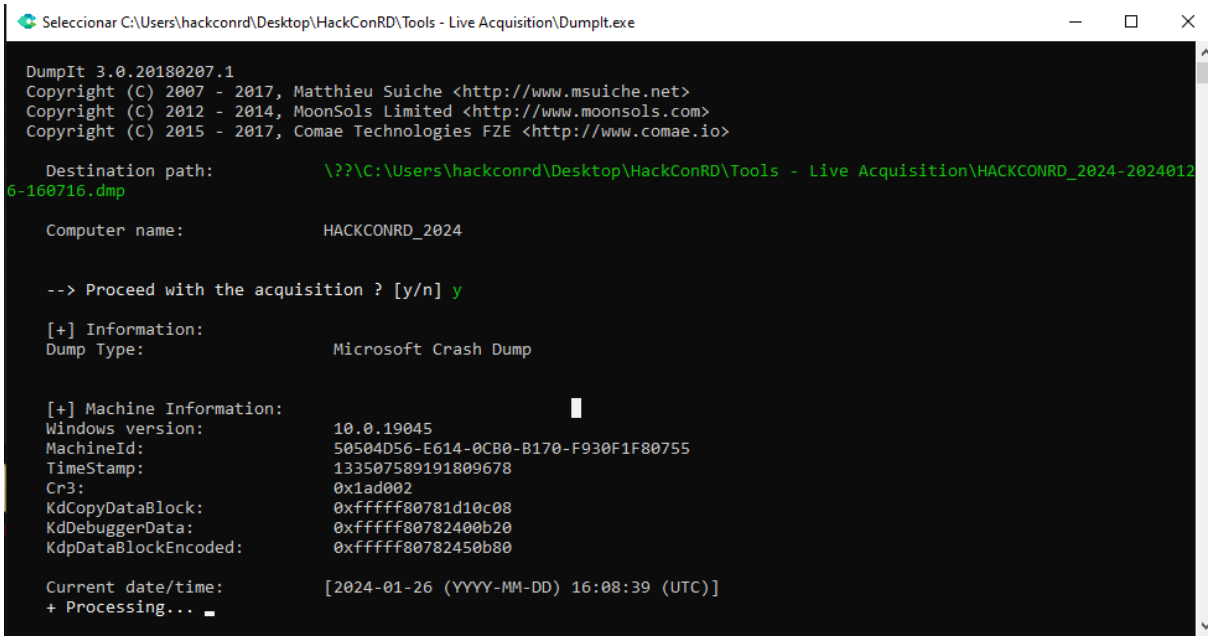
En este ejercicio, usaremos varias herramientas para practicar la recopilación de RAM, verificar signos de cifrado en un sistema en vivo y recopilar un conjunto de artefactos forenses de triaje que podamos usar rápidamente para análisis forense.

Parte I: Memory Acquisition

Nos ubicamos en nuestra máquina virtual, en nuestro Desktop tenemos una carpeta llamada HackConRD dentro una carpeta llamada Live Acquisition, vemos **DumpIT.exe**

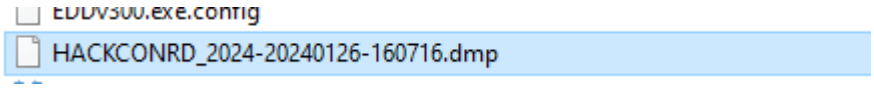


Lo abrimos y seleccionamos “Y”



Nota: Esto puede durar entre 5 a 20 minutos, seguiremos con las demas partes del ejercicio. DumpIT es portable, se puede tener en una USB y recolectar la info, el dump de memoria se guarda en la misma carpeta donde este el programa.

El resultado final será un archivo .dmp ubicado en la misma ubicación desde donde ejecutaste Dumpit.exe. El archivo de salida se nombrará según el nombre del host y la fecha.



Nota 2: El fichero resultante no será necesario en el workshop.

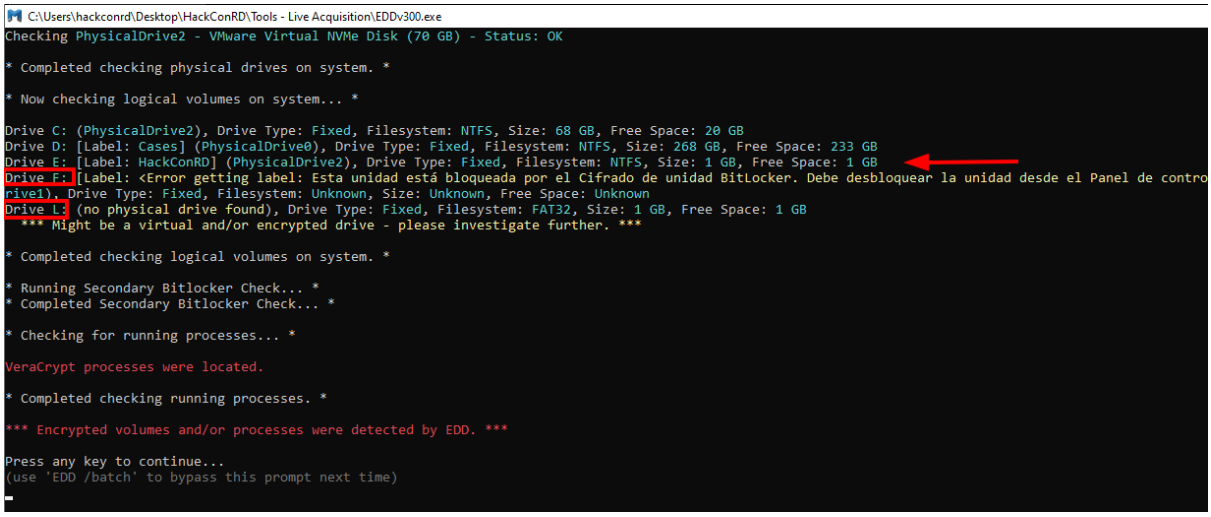
Parte II: Checking for Encryption

Después de crear una imagen de la RAM, el próximo paso, antes de considerar siquiera apagar el sistema, debería ser verificar signos de encriptación.

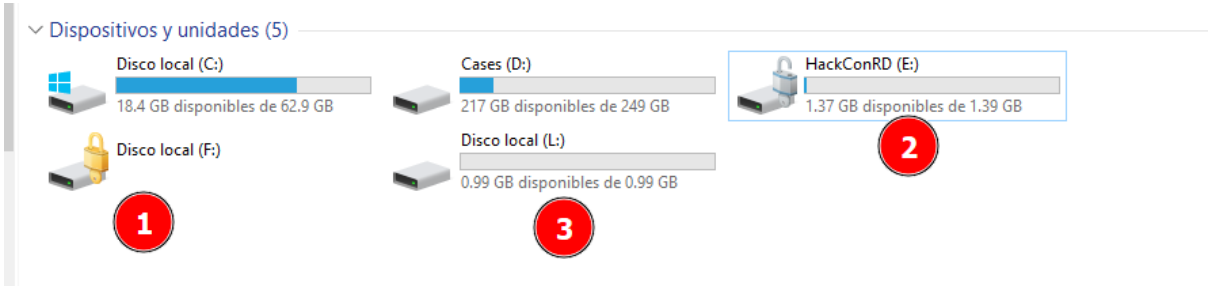
Si la encriptación de disco o archivos está activa, a menudo tu mejor oportunidad para recopilar evidencia **es con una imagen lógica en vivo**. Para verificar la presencia de encriptación, utilizaremos **Magnet Forensics Encrypted Disk Detector (EDD)**. **Normalmente ejecutaríamos esto mediante medios externos, pero para fines de**

clase, lanzaremos Encrypted Disk Detector desde nuestra Estación de Trabajo es decir nuestra maquina virtual.

Abrimos EDDv300 en nuestra carpeta donde esta DumpIT



Tenemos un disco cifrado con bitlocker y uno posiblemente con veracrypt (ha detectado el proceso y una unidad sospechosa)



1. **Bitlocker**
2. **Bitlocker pero esta desprotegido (abierto)**
3. **Contenedor de Veracrypt abierto**

En esto radica la importancia de EDD.exe y la rapidez en que detecta las diferentes unidades.

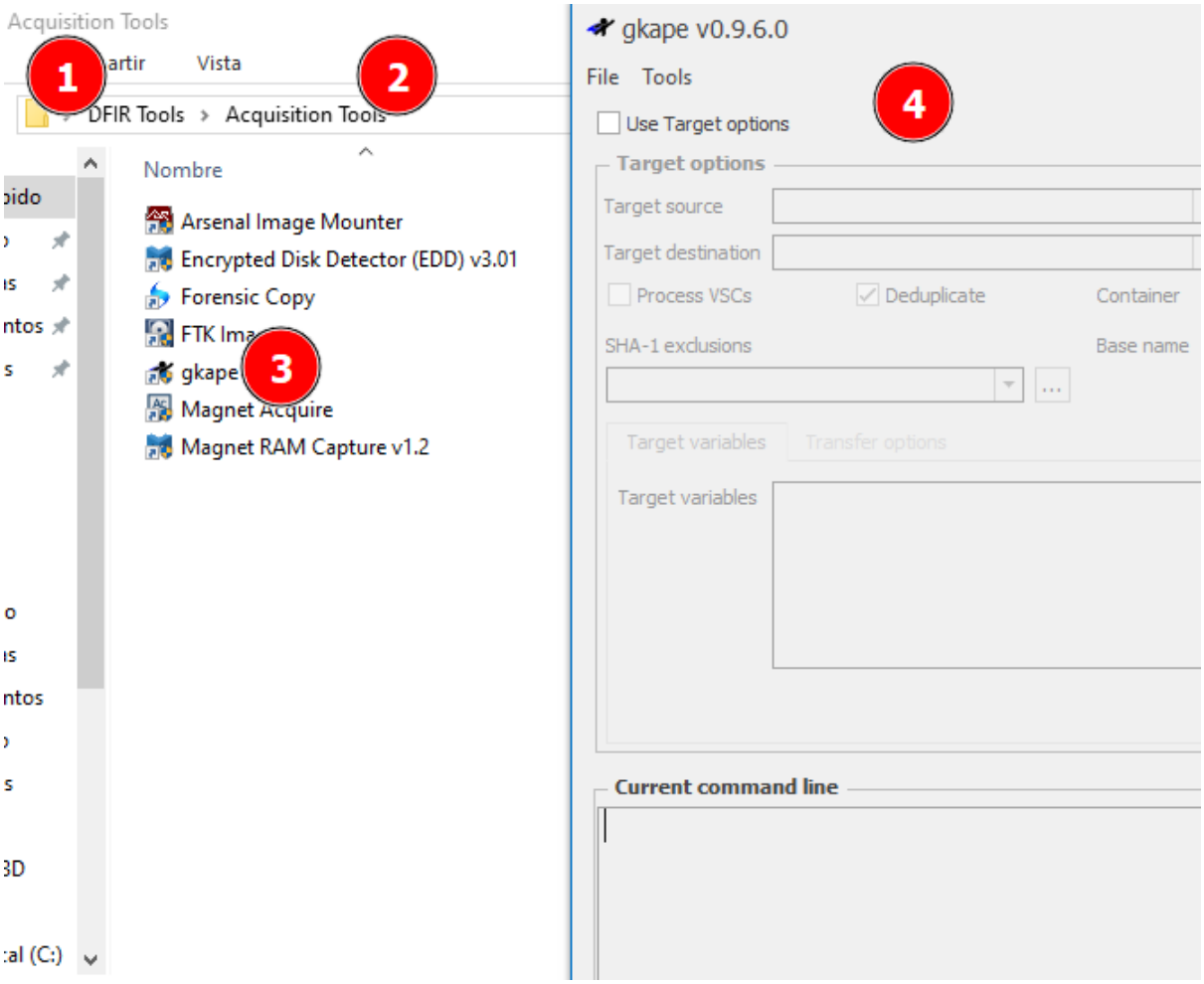
Parte III: Triage Collection with KAPE

Después de crear una imagen de la RAM y no encontrar signos de encriptación es típico que los Incident Response en casos no urgentes apaguen el sistema, retiren los device media del dispositivo (si es posible), apliquen un bloqueador de escritura de hardware y luego previsualicen el disco, recopilen datos de triaje o adquieran una imagen física completa.

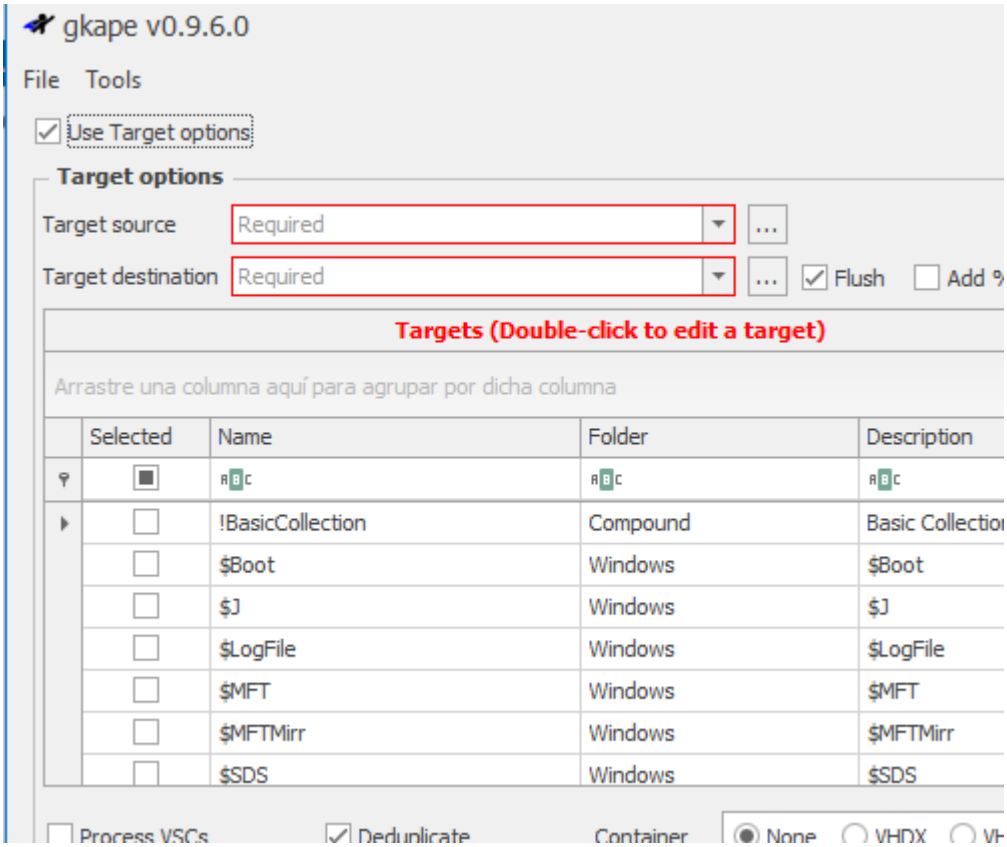
Sin embargo, en circunstancias donde la encriptación pueda estar presente o en casos de respuesta urgente de alta prioridad, existe otra opción: el triaje en vivo para identificar archivos, carpetas y artefactos clave, y recopilar datos de triaje del sistema en vivo. Para este ejercicio, simularemos la urgencia de recopilar datos de triaje de un sistema en vivo antes de apagarlo o retirar cualquier unidad.

Nota: Para este ejercicio, estaremos recopilando datos de triaje de una imagen de disco que capturamos del sistema en lugar del equipo real (por razones obvias, no tenemos acceso al equipo original en funcionamiento).

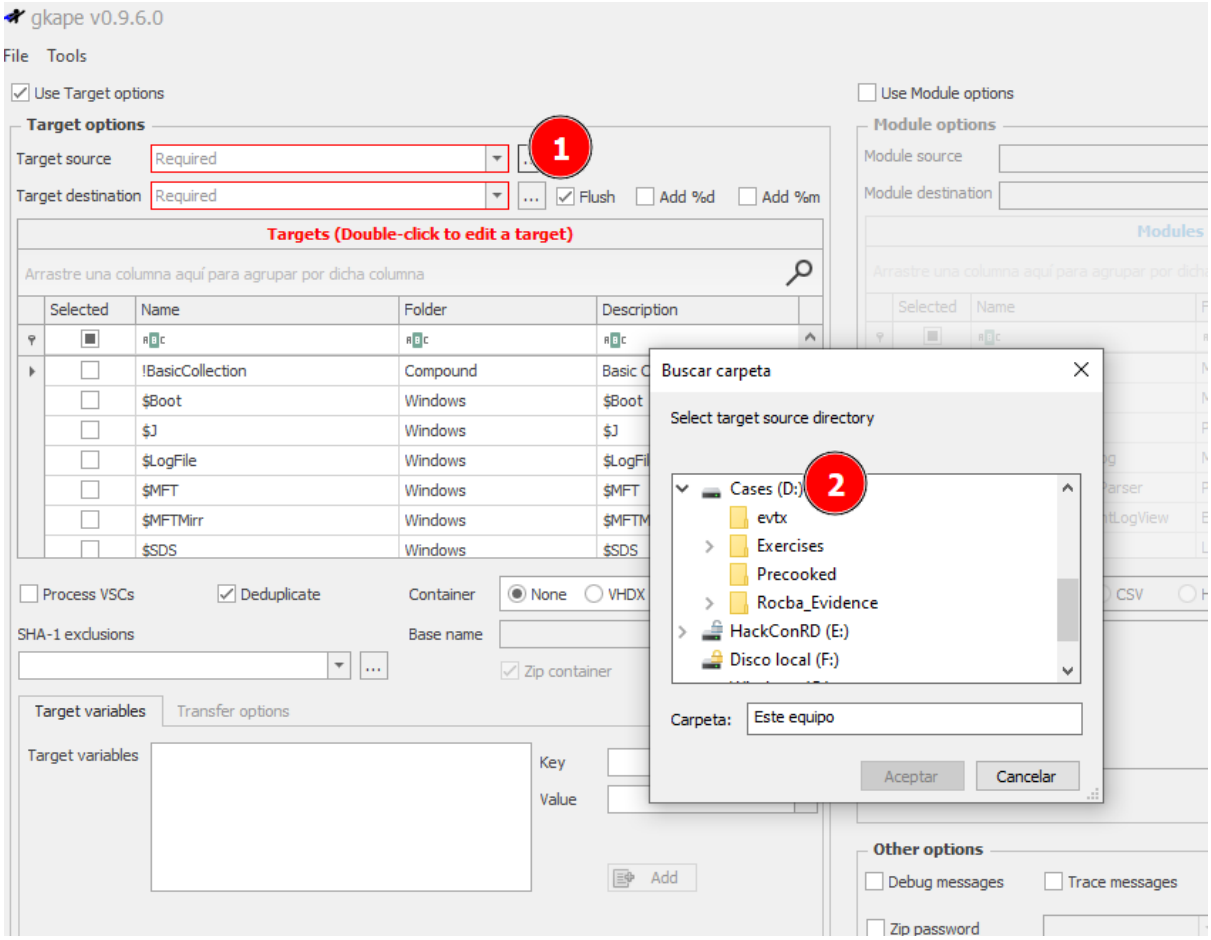
Encontramos KAPE en la ruta **\DFIR Tools\Acquisition Tools\gkape.exe**



Inicialmente, KAPE tendrá un aspecto claro y grisáceo. Una vez que haga clic en la casilla de verificación "**Use Target Options**", las opciones a continuación estarán disponibles. La captura de pantalla a continuación está recortada para mostrar solo el lado del Destino (colección) de la ventana de KAPE. La sección de destino es el lado izquierdo de la pantalla.

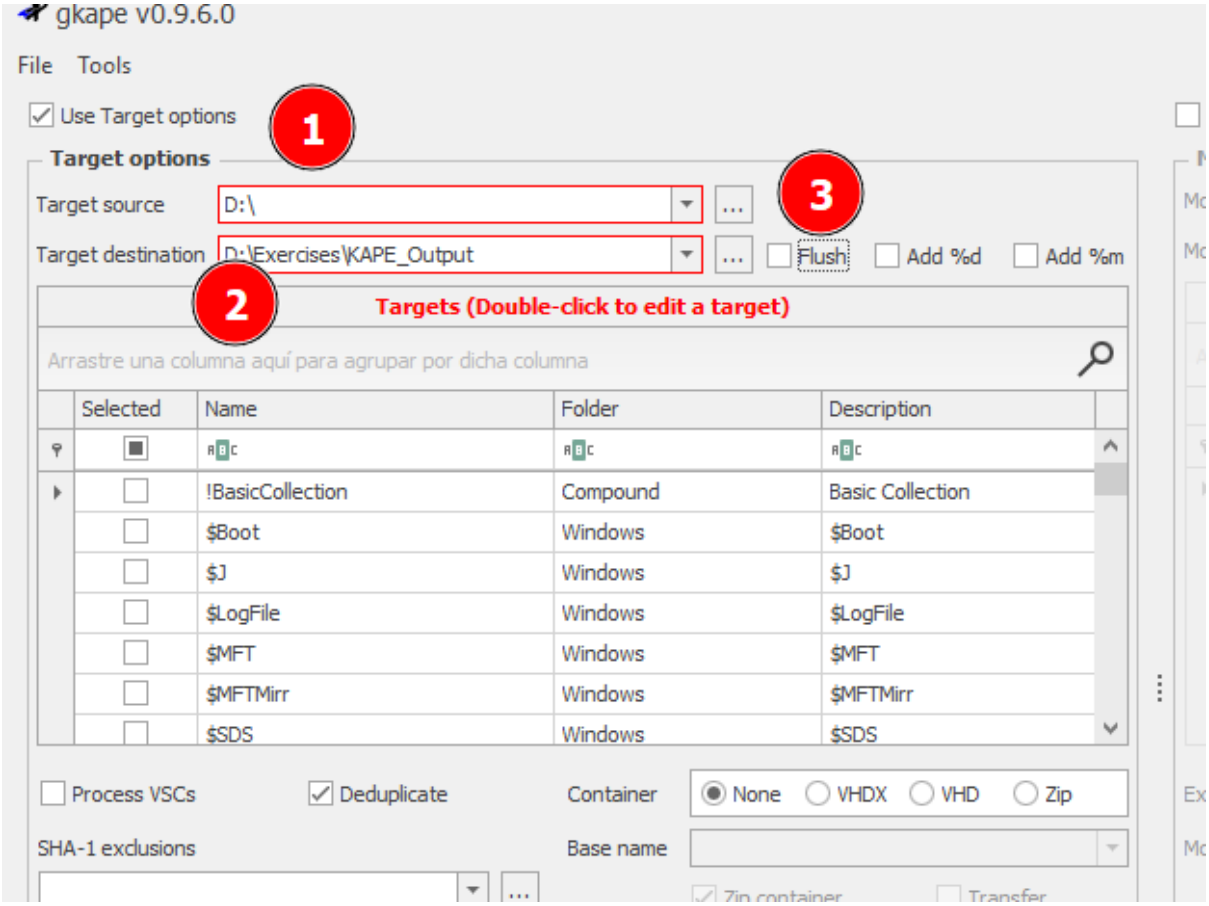


Debemos seleccionar Target source de la cual se desea recopilar. En este caso, debería seleccionar la letra de unidad correspondiente al archivo de imagen que se montó previamente con **Arsenal Image Mounter.**



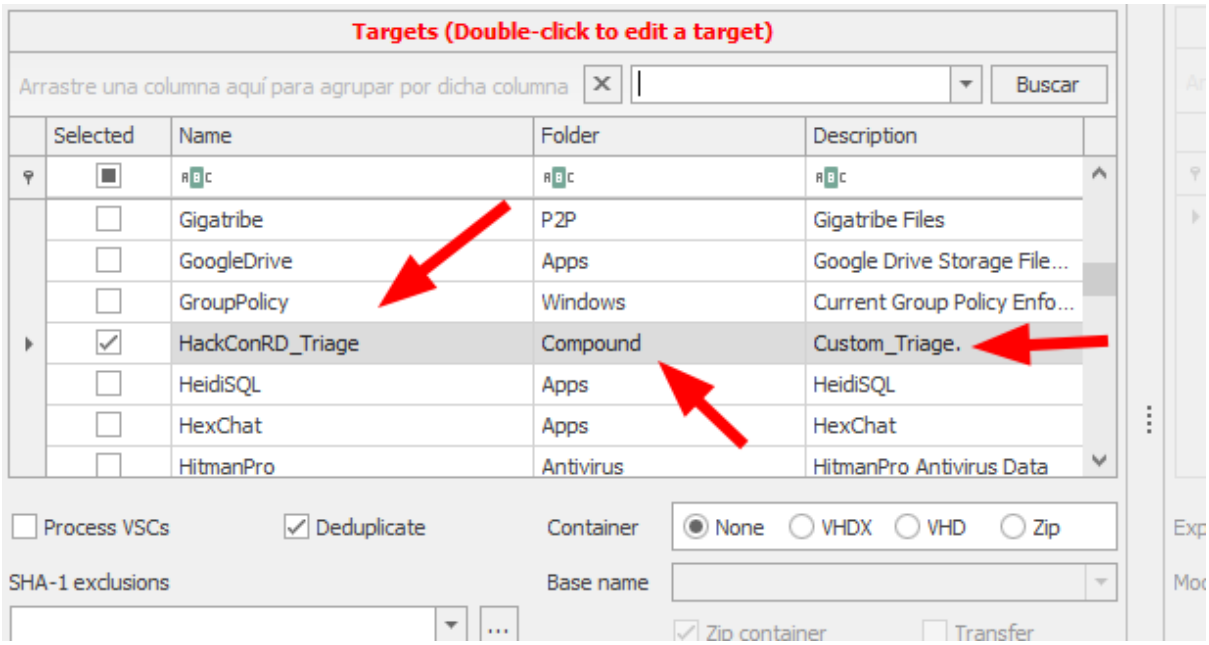
Debemos ahora selecionar la carpeta de destino. Utilice la carpeta **D:\Exercises\KAPE_Output** como destino. KAPE nombrará el archivo contenedor por nosotros

Desmarque la casilla "Flush". Flush indica a KAPE que elimine la carpeta de destino y la vuelva a crear antes de escribir nuevos datos en esa carpeta. Flush es una excelente característica cuando se realiza una prueba. En nuestro caso, con este ejercicio, no queremos eliminar nada antes de escribir nuevos datos en nuestra carpeta de salida.



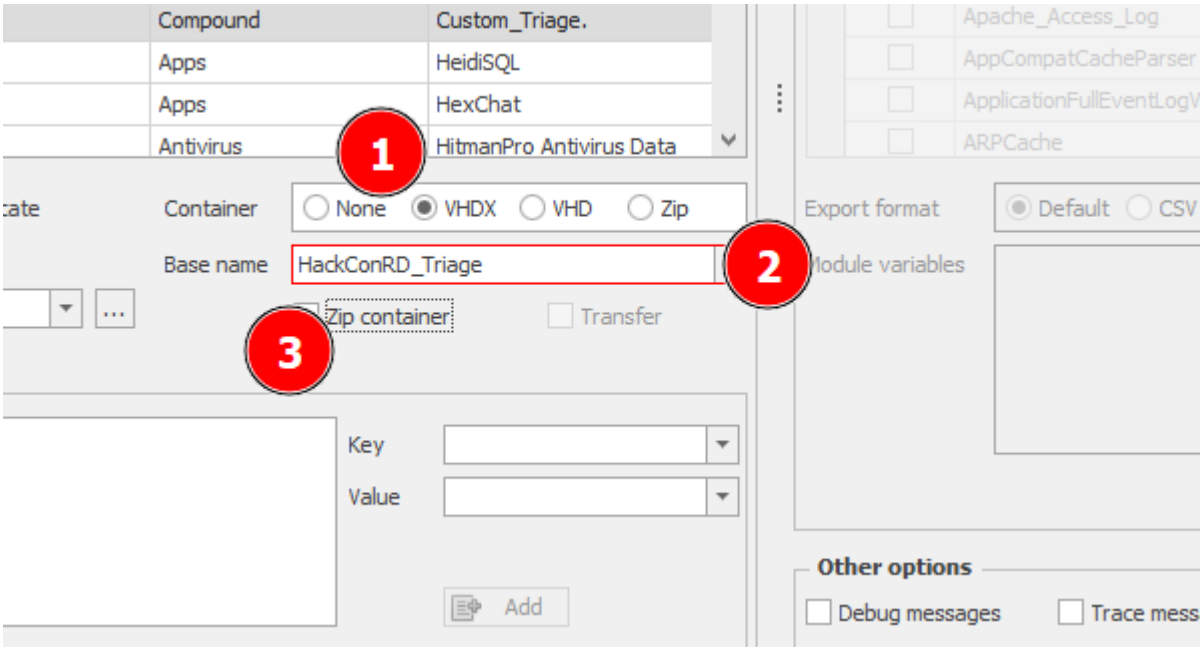
Selecciona el target (o los target) que deseas ejecutar en el source (en este caso, el source es la imagen montada en D:\).

Seleccionamos el **Target HackConRD_triage** haciendo clic en la casilla a la izquierda del nombre de este. **HackConRD_Triage**, es un target compuesto, lo que significa que está compuesto por otro target, específicamente creado para recopilar artefactos que probablemente contengan evidencia relevante en un sistema Windows. Un enlace a los artefactos recopilados por el target **HackConRD_Triage** está disponible al final de este ejercicio.

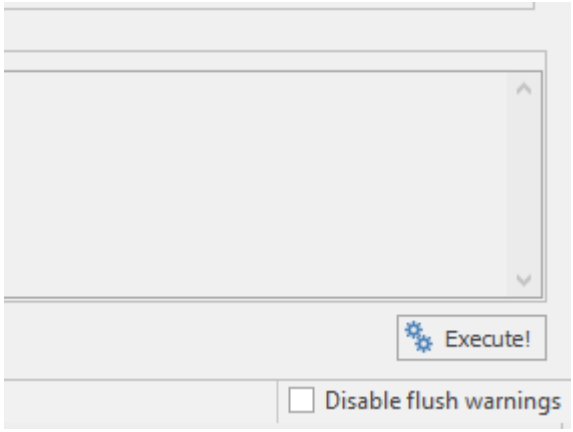


Ahora seleccionamos la opción de Container y escogemos VHDX como formato de contenedor

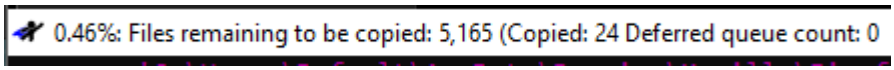
Nota: Le quitamos el check de Zip

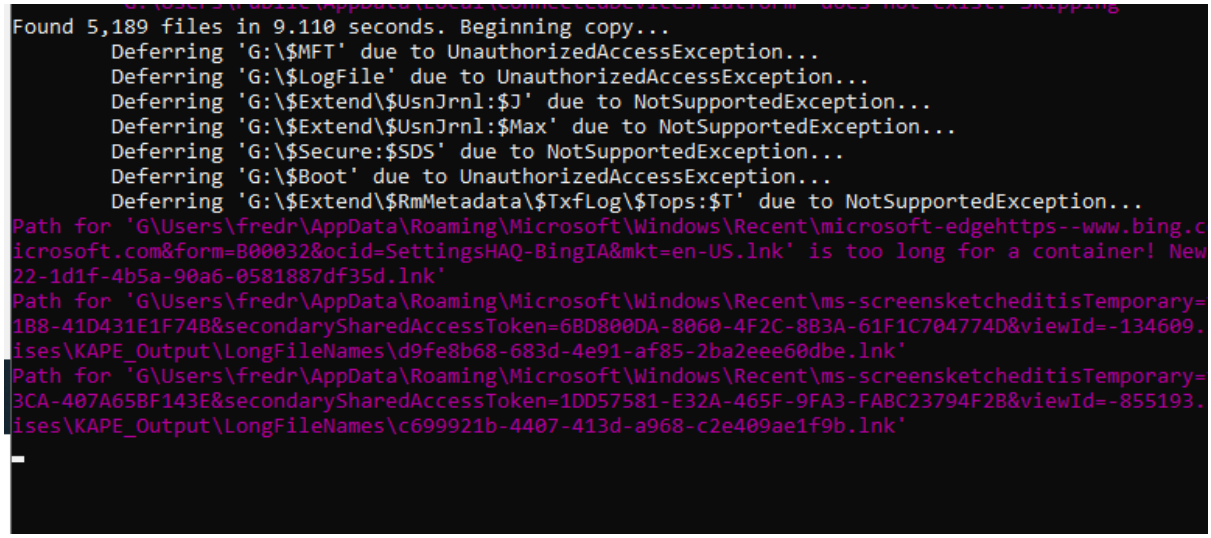


y… lanzamos!

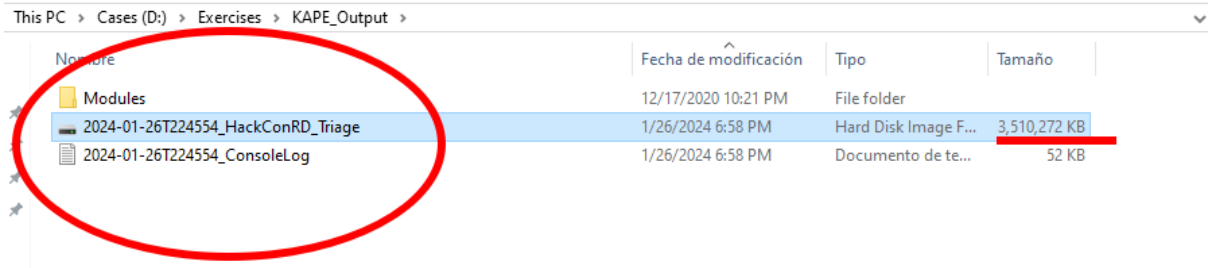


Observamos como va 😊

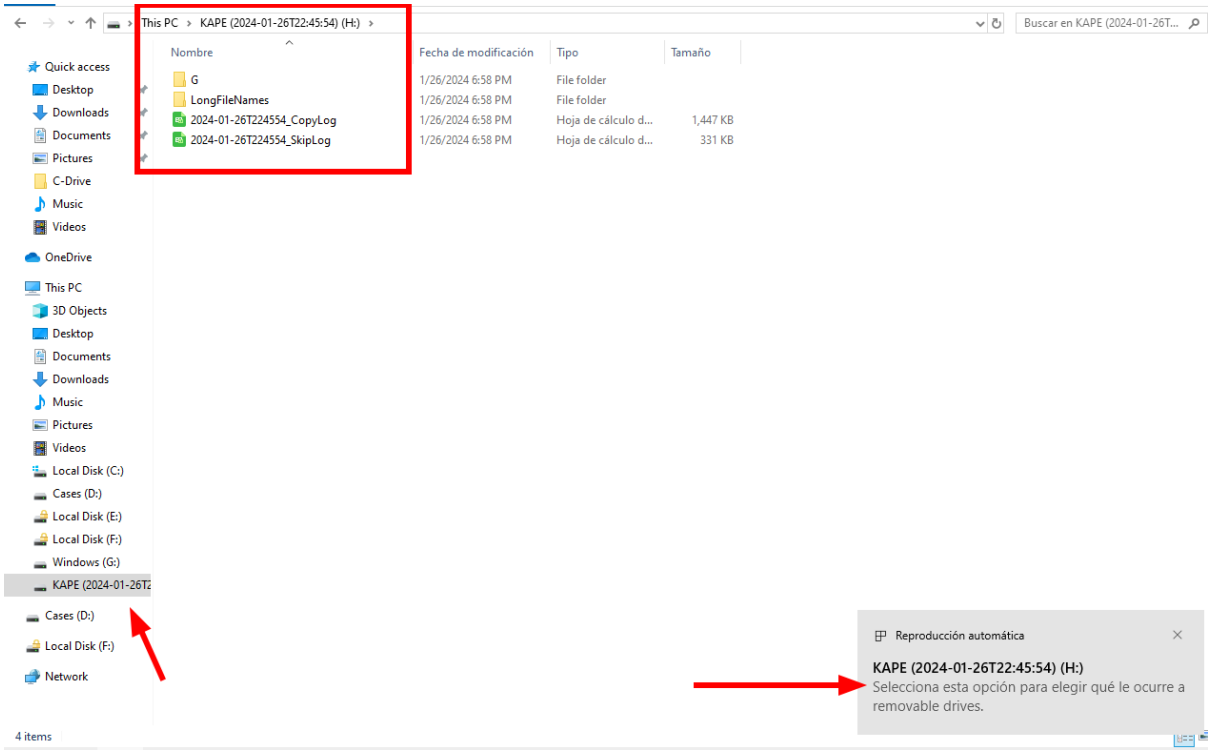




Tenemos nuestra imagen lista.



Si le damos doble click, montamos la imagen.



Consideraciones finales.

Los Incident response tienen solo una oportunidad para capturar la RAM. El uso de herramientas como DumpIt o Magnet RAM Capture puede hacer que la tarea sea sencilla.

Después de capturar la RAM, el siguiente paso debería ser verificar signos de encriptación. El uso de Encrypted Disk Detector puede identificar rápidamente varios tipos de encriptación. ¡Sin embargo, no incluye todas las formas posibles de encriptación disponibles!

También deberías realizar tu propia revisión superficial del sistema. Este conocimiento guiará tu decisión de realizar una imagen del sistema en vivo o de desconectar el sistema de alimentación. Apagar un sistema con cifrado completo de disco puede ser una medida que limite tu carrera, ya que a menudo impedirá cualquier acceso adicional a los archivos dentro de los contenedores encriptados.

Hacer una imagen completa de una unidad puede ser una tarea que consume mucho tiempo y que retrase la investigación. En situaciones donde se necesita un análisis inmediato para identificar información accionable, se debe considerar la creación de una imagen de triaje

utilizando una herramienta como KAPE y luego seguir con una imagen completa de disco.

Crear una pequeña imagen de triaje de archivos, carpetas y artefactos forenses seleccionados permite un análisis rápido e incluso la duplicación/distribución a un equipo de respuesta rápida de varios analistas que trabajan colaborativamente para identificar evidencia crítica y sensible al tiempo.

Copiar un archivo individual no capturará todos los metadatos asociados con ese archivo. Crear adecuadamente una imagen de triaje con una herramienta comprobada como KAPE te permitirá capturar y preservar toda la información asociada con un archivo específico de manera forense, al tiempo que permite completar un análisis rápido.