

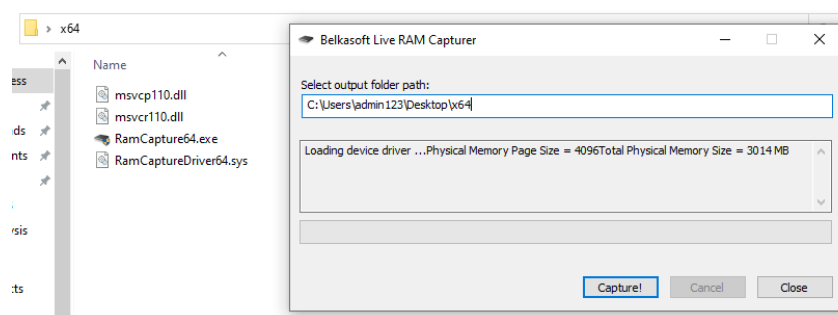
Forencia en equipos Windows	2
Realizar un volcado de la memoria volatil (RAM) en sistemas Windows	2
Belkasoft Live RAM Capturer	3
Realizar una imagen del sistema	5
Kroll Artifact Parser And Extractor (KAPE)	5
Informacion General y descarga.....	6
Uso	8
Target options	9
Module options	14

Forencia en equipos Windows

La adquisición forense, también conocida como imágenes forenses o adquisición de datos, es el proceso de crear un duplicado exacto (o "imagen") de datos de un dispositivo o medio de almacenamiento específico con el fin de preservar los datos originales para fines legales o de investigación. Luego, la imagen se puede analizar y examinar en busca de evidencia sin alterar los datos originales.

Realizar un volcado de la memoria volátil (RAM) en sistemas Windows

Necesitaremos “Belkasoft Live RAM Capturer” mas adelante se explica como descargar la herramienta, por ahora destaco que la misma es portable (no requiere instalacion), solo la ejecutamos como administrador.



Está diseñado para funcionar correctamente incluso si se está ejecutando un sistema agresivo anti-depuración o

anti-volcado de memoria. Al operar en modo kernel, Belkasoft Live RAM Capturer juega al mismo nivel que estos sistemas de protección, pudiendo adquirir correctamente el espacio de direcciones de las aplicaciones protegidas.

Lo abrimos como administrador, luego seleccionamos donde queremos guardar la captura de salida y presionamos capturar. El archivo resultante es de tipo “.mem”.



Belkasoft Live RAM Capturer

Está diseñado para funcionar correctamente incluso si se está ejecutando un sistema agresivo anti-depuración o anti-volcado de memoria. Al operar en modo kernel, Belkasoft Live RAM Capturer juega al mismo nivel que estos sistemas de protección, pudiendo adquirir correctamente el espacio de direcciones de las aplicaciones protegidas con los sistemas más sofisticados como nProtect GameGuard.

En su pagina oficial mencionan que: Belkasoft Live RAM Capturer es una diminuta herramienta forense gratuita que permite extraer de manera segura el contenido completo de la memoria volátil de una computadora, incluso si está protegido por un sistema anti-depuración o anti-dumping activo. Están disponibles las compilaciones de 32 y de 64 bits para minimizar la huella de la herramienta lo más posible. Los volcados de memoria capturados con Belkasoft Live RAM Capturer se pueden analizar con la opción Análisis de la memoria RAM en Belkasoft Evidence Center. Belkasoft Live RAM

Elias Ramirez – RamirezS4

Capturer es compatible con todas las versiones y ediciones de Windows, XP, Vista, Windows 7, 8 y 10, 2003 y 2008 Server incluidos.

Descarga

Van a la pagina oficial <https://belkasoft.com/ram-capturer>.

O directamente al link <https://belkasoft.com/get>, seleccionan “ Belkasoft Live RAM Capturer” y rellenan los datos que solicitan, luego de un dia laborable si aceptan su solicitud le enviarian el link de descarga al correo electronico registrado.

Un usuario subio una version un poco desactualizada a github
<https://github.com/mikebdp2/ram-capturer>

Realizar una imagen del sistema

La imagen del sistema puede ser completa o personalizada. Podemos especificar archivos o carpetas/rutas específicas que nos interesen para su adquisición en lugar de la adquisición del disco completo. Esto es realmente importante ya que las imágenes de disco completas pueden tardar horas o incluso días en adquirirse debido a su tamaño. La imagen personalizada puede permitirnos adquirir datos relevantes para una clasificación rápida e iniciar la investigación hasta que se adquiera el disco lleno. Entonces es necesario un análisis completo de la imagen del disco para un análisis en profundidad.

Kroll Artifact Parser And Extractor (KAPE)

Con KAPE, puede encontrar y priorizar los sistemas más críticos para su caso y recopilar artefactos clave antes de obtener imágenes. Esto significa ya no tener que esperar hasta que se recopilen imágenes completas del sistema y luego revisar datos donde normalmente menos del 10% tendrá algún valor forense, esto ahorra mucho tiempo y esfuerzo de cara a la respuesta rápida y precisa ante un incidente.

KAPE tiene soporte para una amplia variedad de artefactos digitales, incluidos registros del sistema, archivos de eventos, registros de aplicaciones y más. Permite a los

investigadores recopilar datos específicos de interés durante una investigación. KAPE utiliza perfiles que definen qué artefactos se deben recopilar y analizar. Estos perfiles son personalizables para adaptarse a las necesidades específicas de la investigación.

[Informacion General y descarga](#)

KAPE se centra en recopilar y procesar datos relevantes rápidamente, agrupando artefactos en directorios categorizados como EvidenceOfExecution, BrowserHistory y AccountUsage. Agrupar cosas por categoría significa que un examinador ya no necesita saber cómo procesar prefetch, shimcache, amcache, userassist, entre otros, ya que se relacionan con evidencia de artefactos de ejecución.

La informacion aquí presentada fue obtenida de <https://ericzimmerman.github.io/KapeDocs/#!/index.md>

KAPE cumple dos funciones principales: 1) recopilar archivos y 2) procesar archivos recopilados con uno o más programas.

En un nivel alto, KAPE funciona agregando máscaras de archivos a una cola. Luego, esta cola se utiliza para buscar y copiar archivos desde una ubicación de origen. Para los archivos bloqueados por el sistema operativo, se realiza una segunda pasada que

evita el bloqueo. Al final del proceso, KAPE hará una copia y preservará los metadatos de todos los archivos disponibles desde una ubicación de origen en un directorio determinado.

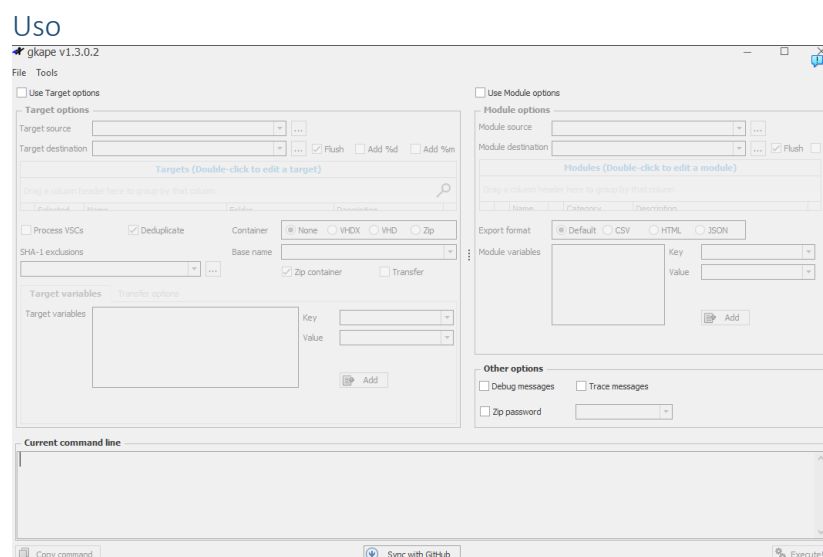
La segunda etapa (opcional) del procesamiento es ejecutar uno o más programas con los datos recopilados. Esto funciona apuntando a nombres de archivos o directorios específicos. Se ejecutan varios programas en los archivos y el resultado de los programas luego se guarda en directorios nombrados según una categoría, como EvidenceOfExecution, BrowserHistory, AccountUsage, etc.

Al agrupar cosas por categoría, los examinadores de todos los niveles tienen un medio para descubrir información relevante independientemente del artefacto individual del que proviene la información. En otras palabras, ya no es necesario que un examinador sepa cómo procesar Prefetch , ShimCache , Amcache , UserAssist , etc. en lo que se refiere a evidencia de artefactos de ejecución. Al pensar categóricamente y agrupar los resultados de la misma manera, se puede aprovechar una gama más amplia de artefactos para cualquier requisito determinado.

Para **descargar** vamos al enlace e ingresamos nuestros datos, nos llegaría el link de descarga mediante el correo electrónico.

<https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape#form716>

En resumen, KAPE tiene varios archivos de configuración en su directorio "destino". Estos contienen rutas, metadatos e información sobre diferentes artefactos forenses importantes que se pueden encontrar en los sistemas Windows. Podemos utilizar cualquiera de los objetivos junto con sus parámetros para recopilar el tipo de adquisición que queremos. Por ejemplo, existe un objetivo para adquirir datos relacionados con el "navegador" que recopilará los datos relevantes para el análisis del navegador. Hay un módulo de destino creado por el instituto SANS, que adquiere los artefactos y datos recomendados por SANS. KAPE tiene su propio objetivo patentado creado por los ingenieros de KAPE, que también adquiere artefactos buenos y relevantes para una clasificación rápida.



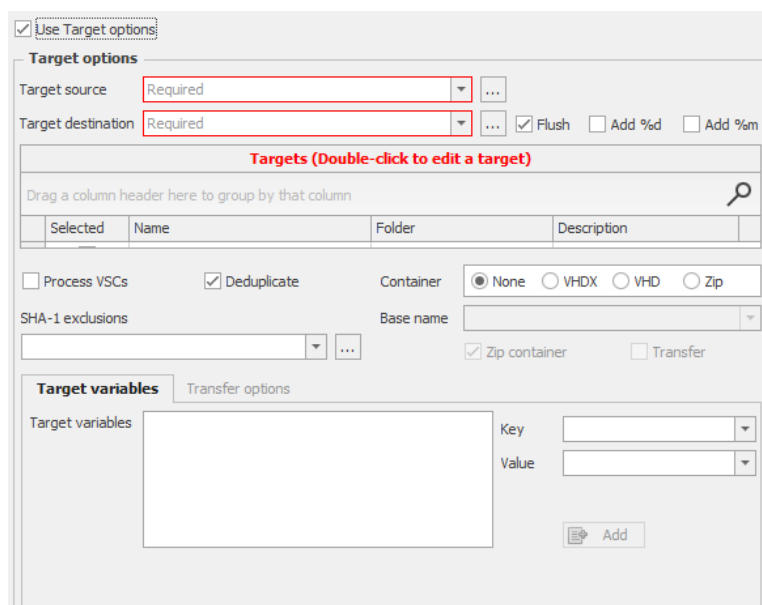
Extraemos los archivos.

Podemos ejecutar kape mediante comandos o con interfaz grafica, esto es realmente util si deseamos simplemente ejecutar un

script en la maquina en la cual realizaremos la investigacion.

Target options

Comenzare mostrando el uso del apartado “target options”. Los objetivos son esencialmente colecciones de especificaciones de archivos y directorios. KAPE sabe



The screenshot shows the 'Target options' window in KAPE. At the top, there is a checkbox labeled 'Use Target options' which is checked. Below this, the 'Target options' section contains two dropdown menus for 'Target source' and 'Target destination', both marked as 'Required'. To the right of these are checkboxes for 'Flush', 'Add %d', and 'Add %m'. Below these fields is a table titled 'Targets (Double-click to edit a target)' with columns 'Selected', 'Name', 'Folder', and 'Description'. Below the table are checkboxes for 'Process VSCs' and 'Deduplicate', and a 'Container' dropdown menu with options 'None', 'VHDX', 'VHD', and 'Zip'. There is also a 'Base name' dropdown menu and checkboxes for 'Zip container' and 'Transfer'. At the bottom, there is a 'Target variables' section with a large text area for 'Target variables', a 'Key' dropdown menu, a 'Value' dropdown menu, and an 'Add' button.

cómo leer estas especificaciones y expandirlas a archivos y directorios que existen en una ubicación de destino. Una vez que KAPE ha procesado todos los destinos y ha creado una lista de archivos, la lista se procesa y cada archivo se copia desde el

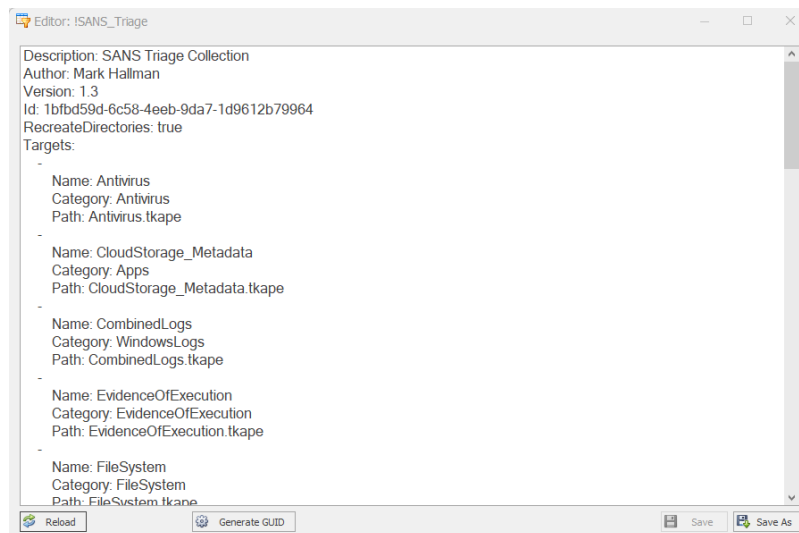
directorio de origen al de destino.

Los primeros dos campos que nos piden son:

- “Target source” el cual hace referencia a la ruta principal del sistema de windows o archivos por lo general “c:/”
- “Target destination” es la ruta de salida o donde se almacenara todo lo recopilado.

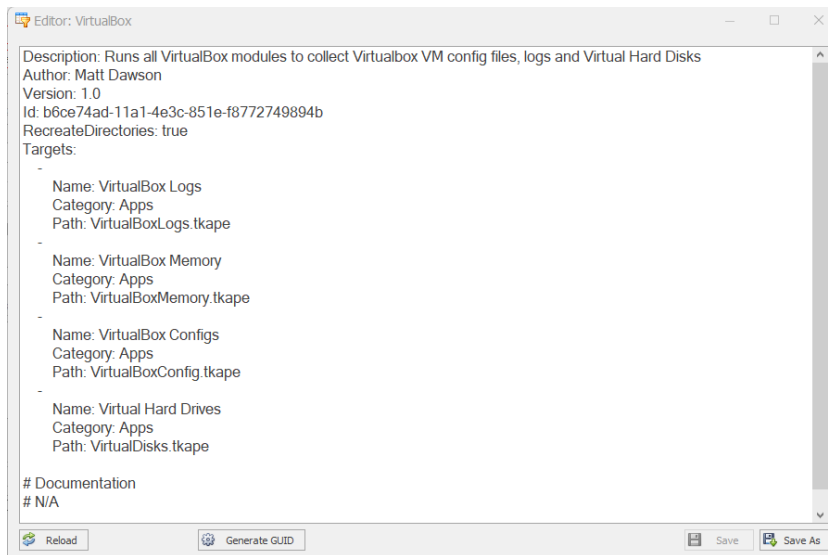
Targets (Double-click to edit a target)				
Drag a column header here to group by that column				
	Selected	Name	Folder	Description
▼	<input checked="" type="checkbox"/>	c	c	c
▶	<input type="checkbox"/>	!BasicCollection	Compound	Basic Collection
	<input type="checkbox"/>	!SANS_Triage	Compound	SANS Triage Collection

Ahora pasamos a la selección del Target

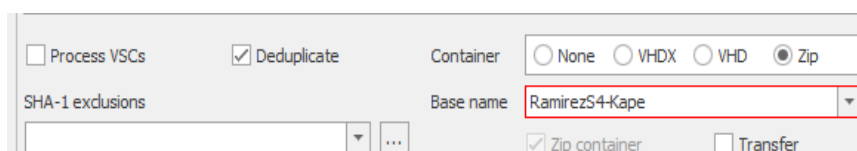


Como mencione antes tenemos varias opciones interesantes las cuales agrupan varios artefactos, por defecto recomiendo usar “SANS Triage Collection”, haciendo doble click sobre cualquiera obtendremos lo

que recopila, ademas de poder modificarlo.



Por ejemplo tambien tenemos otro de Virtual box, el cual colecta Virtualbox VM config files, logs and Virtual Hard Disks.

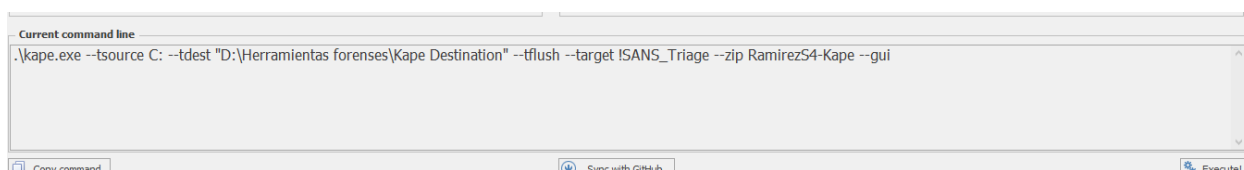


Las opciones que se presentan abajo son

Elias Ramirez – RamirezS4

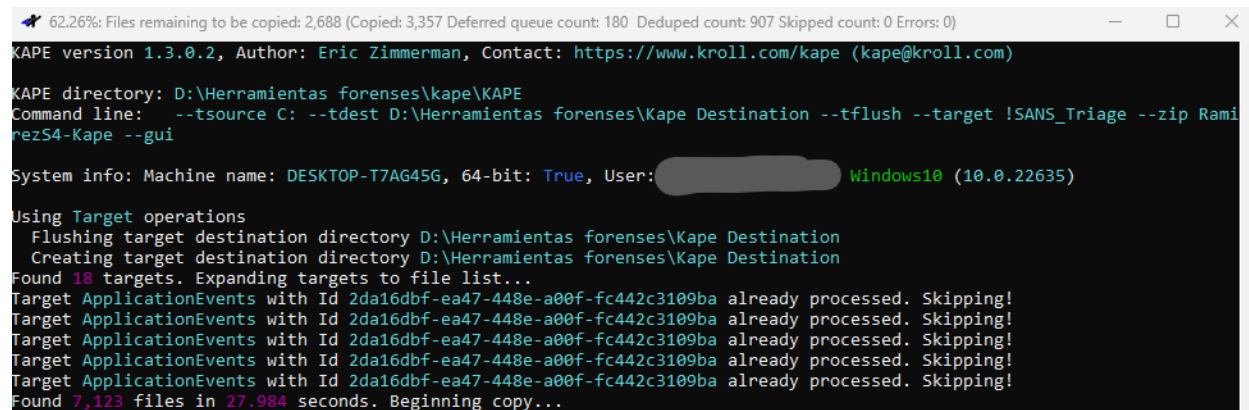
explicadas en el documento de informacion pero recomendamos que el resultado este comprimido usando zip para su mejor transferencia.

Podemos ver que se nos generan unos comandos los cuales se utilizan en el cmd, esto es lo que necesitamos copiar si queremos personalizar la recopilacion para luego ejecutarla en una maquina externa.



```
.\kape.exe --tsource C: --tdest "D:\Herramientas forenses\Kape Destination" --tflush --target ISANS_Triage --zip RamirezS4-Kape --gui
```

Una vez le demos a ejecutar se nos abre una cmd.



Una vez finalizado


```
Copied 5,473 (Deduplicated: 1,650) out of 7,123 files in 303.4144 seconds. See 2024-01-27T21_02_57_7360436_CopyLog.csv i
n the VHD(X)/Zip located in D:\Herramientas forenses\Kape Destination for copy details

Compressing files to D:\Herramientas forenses\Kape Destination\2024-01-27T210257_RamirezS4-Kape.zip...
Cleaning up files in D:\Herramientas forenses\Kape Destination...












Total execution time: 520.8700 seconds

Press any key to exit
```

Vamos a la carpeta de destino, extraemos los datos. Veo que descomprimido pesa 4.3 GB los artefactos recopilados, todo obtenido de forma automatica.

	2024-01-27T21_02_57_7360436_ConsoleLog.txt	1/27/2024 5:11 PM	Text Document	123 KB
	2024-01-27T210257_RamirezS4-Kape.zip	1/27/2024 5:11 PM	Compressed (zipp...	1,188,159 KB

Vemos los archivos recopilados

 \$Extend	1/27/2024 5:13 PM	File folder	
 \$Recycle.Bin	1/27/2024 5:05 PM	File folder	
 Program Files	1/27/2024 5:06 PM	File folder	
 ProgramData	1/27/2024 5:05 PM	File folder	
 RECYCLER	1/27/2024 5:05 PM	File folder	
 Users	1/27/2024 5:04 PM	File folder	
 Windows	1/27/2024 5:06 PM	File folder	
 \$Boot	1/27/2024 5:07 PM	File	8 KB
 \$LogFile	1/27/2024 5:07 PM	File	65,536 KB
 \$MFT	5/24/2021 12:47 AM	File	967,680 KB
 \$Secure_\$\$DS	5/24/2021 12:47 AM	File	13,066 KB

Module options

Ahora mostrare el uso del apartado “Module options”.

Al igual que los objetivos, los módulos se definen mediante propiedades simples y se utilizan para ejecutar programas. Estos programas pueden apuntar a cualquier cosa, incluidos archivos recopilados a través de las capacidades de destino, así como cualquier otro tipo de programa que desee ejecutar en un sistema desde una perspectiva de respuesta en vivo.

Por ejemplo si también desea recopilar el resultado de netstat o ipconfig , puede hacerlo. Cada una de estas opciones estaría contenida en su propio Módulo y luego agrupada

Elias Ramirez – RamirezS4

según los puntos en común entre los Módulos, como "NetworkLiveResponse", por ejemplo.

Activamos la opción y vemos los apartados

☒ Use Module options

Module options

Module source: ...

Module destination: ... ☒ Flush ☒ Add %d ☒ Add %m ☒ Zip

Modules (Double-click to edit a module)

Drag a column header here to group by that column

	Sel...	Name	Folder	Category	Description
▼	<input checked="" type="checkbox"/>	*c	*c	*c	*c
▶	<input type="checkbox"/>	!!ToolSync	Compound	Sync	Sync for new Maps, Batch Files, Targets and Modules
	<input checked="" type="checkbox"/>	!EZParser	Compound	Modules	Eric Zimmerman Parsers

Export format: ☒ Default ☐ CSV ☐ HTML ☐ JSON

Module variables:

Key:
Value:

Add

Other options

☐ Debug messages ☐ Trace messages ☐ Ignore FTK warning

☐ Zip password: ☐ Retain local copies

Entre los modulos tenemos varios interesantes entre ellos:

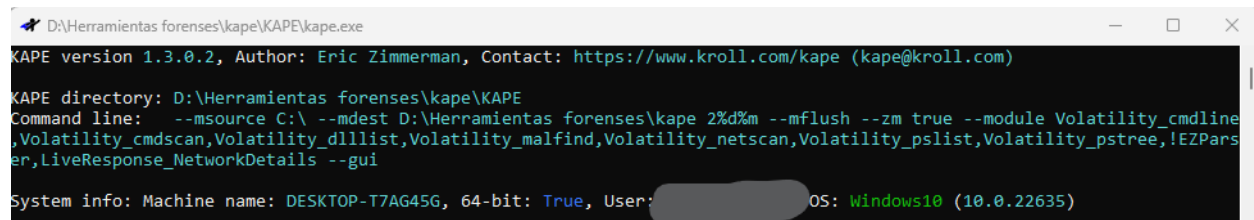
“Eric Zimmerman Parsers” el cual utiliza las herramientas de Eric Z. las cuales se pueden adquirir en el siguiente enlace <https://www.sans.org/tools/ez-tools/> Son una increíble colección de herramientas que procesan y analizan casi todos los artefactos de Windows.

Elias Ramirez – RamirezS4

Podemos llegar a ejecutar volatily en tiempo real en el equipo para obtener datos y/o otras herramientas.

Tambien un conjunto de herramientas y comandos para obtener informacion sobre la red y conexiones.

Luego de seleccionar varios de estos continuamos y seleccionamos ejecutar. La consola nuevamente se volvera a abrir.

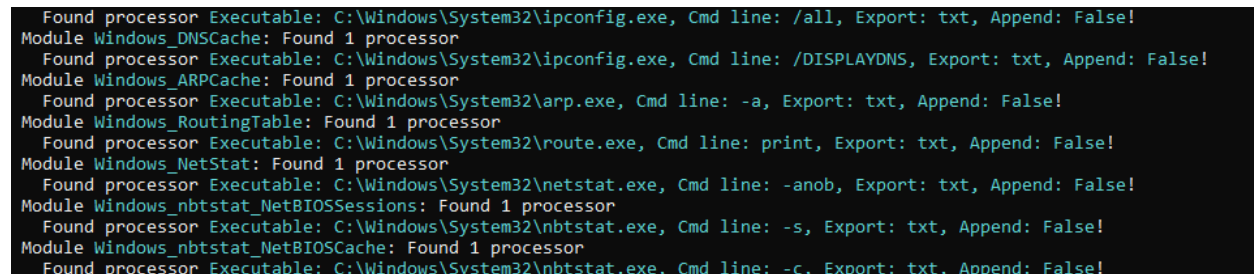
A screenshot of a Windows application window titled "D:\Herramientas forenses\kape\KAPE\kape.exe". The window contains a black terminal area with white text. The text displays the KAPE version (1.3.0.2), author (Eric Zimmerman), and contact information. It also shows the KAPE directory path, a detailed command line with various modules like Volatility and EZParser, and system information including machine name (DESKTOP-T7AG45G), 64-bit status (True), user (redacted), and OS (Windows10 10.0.22635).

```
D:\Herramientas forenses\kape\KAPE\kape.exe
KAPE version 1.3.0.2, Author: Eric Zimmerman, Contact: https://www.kroll.com/kape (kape@kroll.com)

KAPE directory: D:\Herramientas forenses\kape\KAPE
Command line: --msource C:\ --mdest D:\Herramientas forenses\kape 2%d%m --mflush --zm true --module Volatility_cmdline
,Volatility_cmdscan,Volatility_dlllist,Volatility_malfind,Volatility_netscan,Volatility_pslist,Volatility_pstree,!EZParser,LiveResponse_NetworkDetails --gui

System info: Machine name: DESKTOP-T7AG45G, 64-bit: True, User: [redacted] OS: Windows10 (10.0.22635)
```

Mediante la linea de comandos podemos ver la ejecucion de las herramientas

A screenshot of a terminal window showing the output of KAPE. It lists several Windows system components and the specific commands executed for each, such as ipconfig, netstat, and nbtstat. Each entry indicates that a processor was found and the command was executed successfully.

```
Found processor Executable: C:\Windows\System32\ipconfig.exe, Cmd line: /all, Export: txt, Append: False!
Module Windows_DNSCache: Found 1 processor
Found processor Executable: C:\Windows\System32\ipconfig.exe, Cmd line: /DISPLAYDNS, Export: txt, Append: False!
Module Windows_ARPCache: Found 1 processor
Found processor Executable: C:\Windows\System32\arp.exe, Cmd line: -a, Export: txt, Append: False!
Module Windows_RoutingTable: Found 1 processor
Found processor Executable: C:\Windows\System32\route.exe, Cmd line: print, Export: txt, Append: False!
Module Windows_NetStat: Found 1 processor
Found processor Executable: C:\Windows\System32\netstat.exe, Cmd line: -anob, Export: txt, Append: False!
Module Windows_nbtstat_NetBIOSSessions: Found 1 processor
Found processor Executable: C:\Windows\System32\nbtstat.exe, Cmd line: -s, Export: txt, Append: False!
Module Windows_nbtstat_NetBIOSCache: Found 1 processor
Found processor Executable: C:\Windows\System32\nbtstat.exe, Cmd line: -c, Export: txt, Append: False!
```


Al ver el resultado podemos notar que Los datos se clasifican según el tipo de información que almacenan.

EventLogs	1/27/2024 5:58 PM	File folder	
FileDeletion	1/27/2024 5:58 PM	File folder	
FileFolderAccess	1/27/2024 5:58 PM	File folder	
LiveResponse	1/27/2024 5:58 PM	File folder	
ProgramExecution	1/27/2024 5:58 PM	File folder	
Registry	1/27/2024 5:58 PM	File folder	
SQLDatabases	1/27/2024 5:57 PM	File folder	
SRUMDatabase	1/27/2024 5:58 PM	File folder	
SUMDatabase	1/27/2024 5:58 PM	File folder	
2024-01-27T21_40_42_3282567_Consol...	1/27/2024 5:57 PM	Text Document	17 KB
2024-01-27T214042_ModulesOutput.zip	1/27/2024 5:57 PM	Compressed (zipp...	24,534 KB

Entre los resultados podemos ver el resultado de los comandos

arp_cache.txt	1/27/2024 5:57 PM	Text Document	14 KB
dns_cache.txt	1/27/2024 5:57 PM	Text Document	61 KB
ipconfig.txt	1/27/2024 5:57 PM	Text Document	19 KB
netbios_cache.txt	1/27/2024 5:57 PM	Text Document	3 KB
netbios_sessions.txt	1/27/2024 5:57 PM	Text Document	3 KB
network_connections.txt	1/27/2024 5:57 PM	Text Document	47 KB
routing_table.txt	1/27/2024 5:57 PM	Text Document	18 KB

Por ejemplo tambien podemos ver los archivos en la papelera de reciclaje junto con su tamaño y fecha de borrado.

Elias Ramirez – RamirezS4

SourceName	File Type	FileName	File Size	Deleted On
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\1E84XB.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento1.asd	35840	1/8/2024 23:10
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\443X24Q	\$I	C:\Users\Elias Ramirez\Desktop\Prueba1	17187091	1/8/2023 14:8
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\7NDASA.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento2.asd	23040	1/14/2024 16:55
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\8PFLAI.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento1.asd	23552	1/6/2024 13:47
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\8PFLAI.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento1.asd	23552	1/9/2024 22:50
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\IC7IR7E.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento1.asd	33792	1/12/2024 13:46
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\JUL7LOW.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento2.asd	43008	#####
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\IM60A47.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Cambio la clave del usuario root a 12345.	31744	1/12/2024 13:46
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\IN53C0S.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento1.asd	418304	1/14/2024 16:55
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\IPY242O.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de estatus.asd	313856	#####
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\IRU79Z.rar	\$I	C:\Users\Elias Ramirez\Desktop\Prueba1.rar	776403	1/16/2023 0:41
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\IRN6Q0S.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento1.asd	23552	#####
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\IV24SFG.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento2.asd	98816	1/12/2024 0:58
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\Wk41TX.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento1.asd	24064	1/13/2024 14:45
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\XGATIL.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento2.asd	23552	1/13/2024 14:45
C:\\$Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\XGATIL.asd	\$I	C:\Users\Elias Ramirez\AppData\Roaming\Microsoft\Word\Guardado con AutorrecuperaciÃn de Documento1.asd	24064	#####

Hasta aquÃ este apartado por ahora, el documento seguira siendo actualizado.