

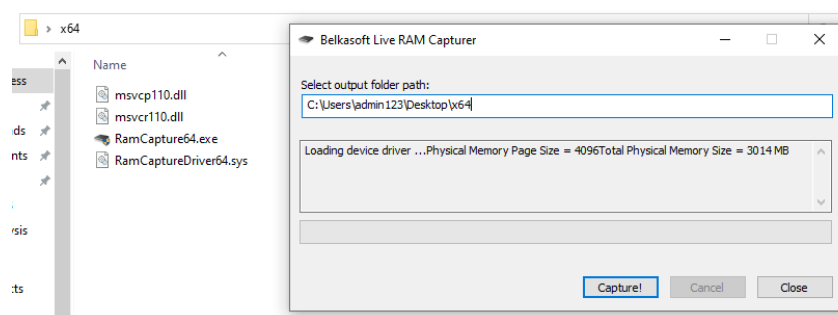
Forencia en equipos Windows	2
Realizar un volcado de la memoria volatil (RAM) en sistemas Windows	2
Belkasoft Live RAM Capturer	3
Realizar una imagen del sistema	5
Kroll Artifact Parser And Extractor (KAPE)	5
Informacion General y descarga.....	6
Uso	8
Target options	9
Module options	14
Registros de windows	18
ftk imager	19
Instalación en una USB	19
Datos importantes.....	20
Recopilación de registros y datos	20
Registry Explorer de Eric Zimmerman	28
Registros SAM.....	29
Registros SOFTWARE y SYSTEM.....	32

Análisis Forense de 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” más adelante se explica cómo descargar la herramienta, por ahora destaco que la misma es portable (no requiere instalación), 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”.

 20240127.mem	1/27/2024 10:27 AM	MEM File	3,087,296 KB
--	--------------------	----------	--------------

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 página 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 página 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 día laborable si aceptan su solicitud le enviarán el link de descarga al correo electrónico registrado.

Un usuario subió una versión 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.

Información 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 información 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.

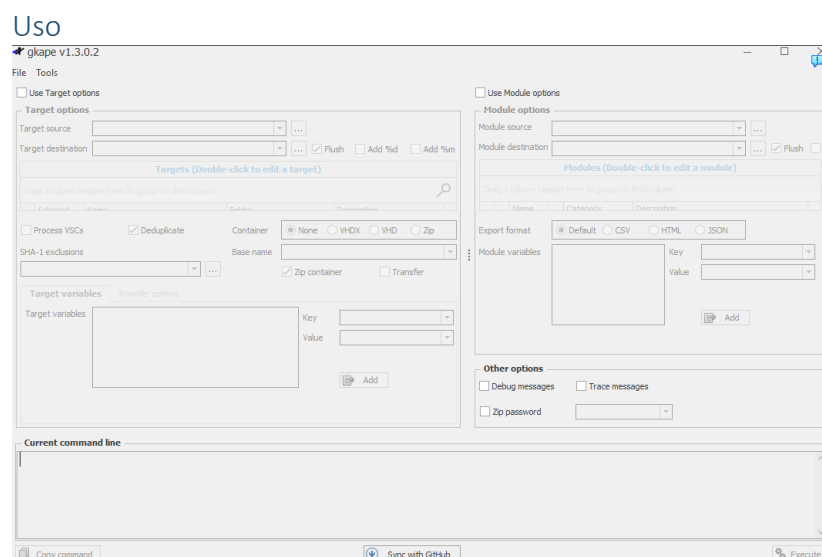
La segunda etapa (opcional) del procesamiento es ejecutar uno o más programas con los datos recopilados. Esto funciona apuntando a nombres de archivos o directorios específicos. Se ejecutan varios programas en los archivos y el resultado de los programas luego se guarda en directorios nombrados según 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 gráfica, esto es realmente útil si deseamos simplemente ejecutar un

script en la maquina en la cual realizaremos la investigación.

Target opciones

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

☒ Use Target options

Target options

Target source: Required

Target destination: Required

☒ Flush ☐ Add %d ☐ Add %m

Targets (Double-click to edit a target)

Drag a column header here to group by that column

Selected	Name	Folder	Description
----------	------	--------	-------------

☐ Process VSCs ☒ Deduplicate

Container: ☒ None ☐ VHDX ☐ VHD ☐ Zip

SHA-1 exclusions:

Base name:

☒ Zip container ☐ Transfer

Target variables **Transfer options**

Target variables:

Key:

Value:

Add

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

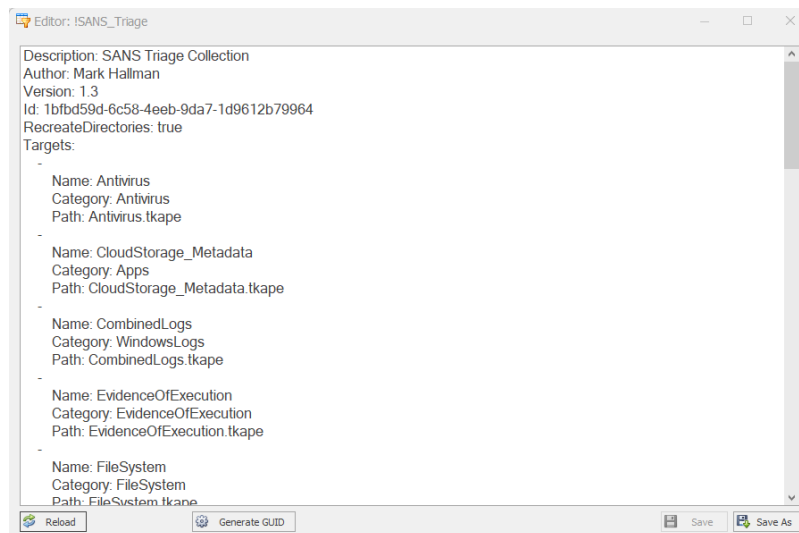
directorio de origen al de destino.

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 almacenará todo lo recopilado.

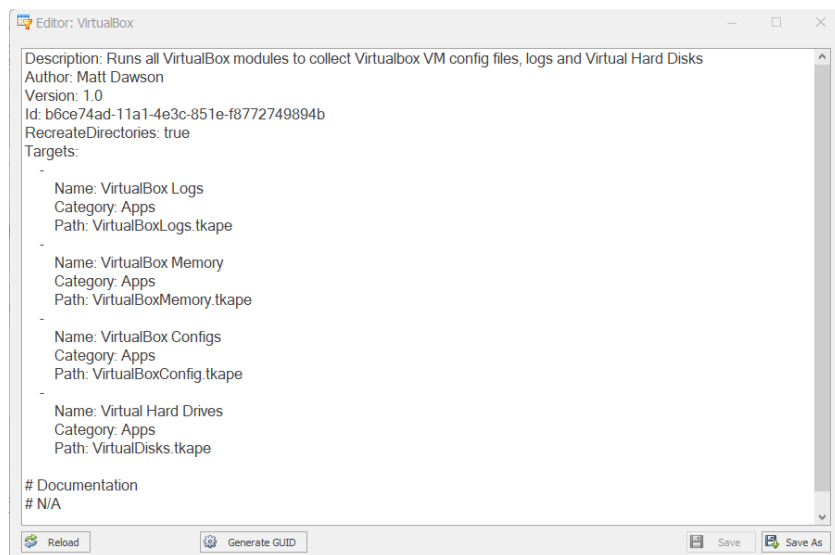
Targets (Double-click to edit a target)				
Drag a column header here to group by that column				
	Selected	Name	Folder	Description
▼	<input checked="" type="checkbox"/>	c	c	c
▶	<input type="checkbox"/>	!BasicCollection	Compound	Basic Collection
	<input type="checkbox"/>	!SANS_Triage	Compound	SANS Triage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

Ahora pasamos a la selección del Target

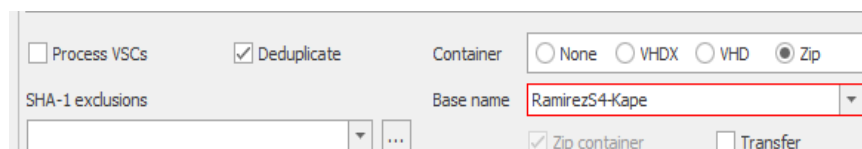


Como mencione antes tenemos varias opciones interesantes las cuales agrupan varios artefactos, por defecto recomiendo usar “SANS Triage Collection”, haciendo doble clic sobre cualquiera obtendremos lo

que recopila, además de poder modificarlo.



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

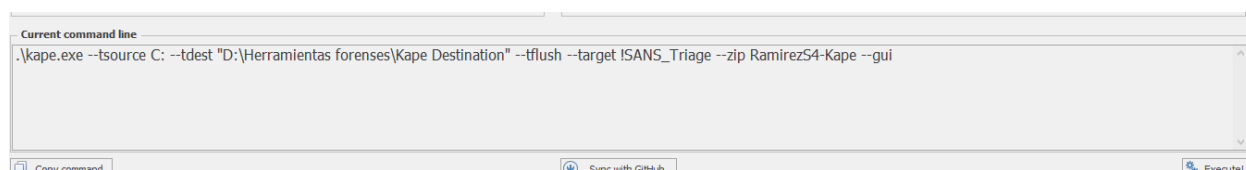


Las opciones que se presentan abajo son

Elias Ramirez – RamirezS4

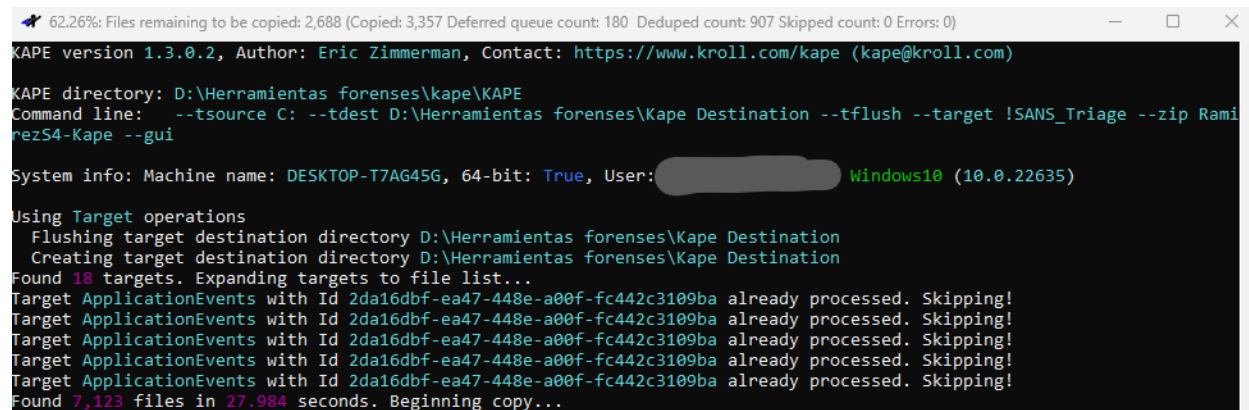
explicadas en el documento de información, pero recomendamos que el resultado este comprimido usando Zip para su mejor transferencia.

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 recopilación 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 in 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 descomprimida pesa 4.3 GB los artefactos recopilados, todo obtenido de forma automática.

	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 opciones

Ahora mostrare el uso del apartado “Module opciones”.

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 ip config, 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 módulos tenemos varios interesantes entre ellos:

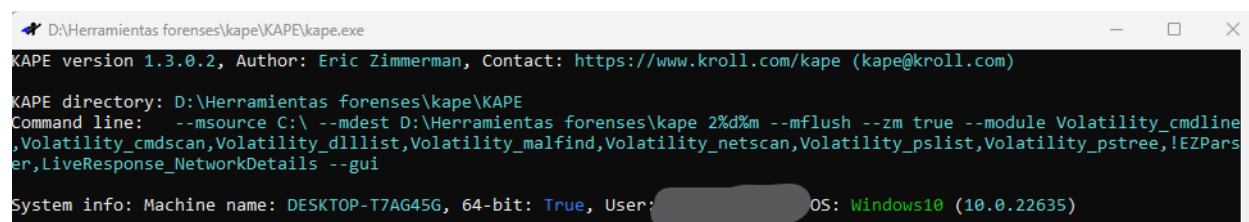
“Eric Zimmerman Parsers” el cual utiliza las herramientas de Eric Z. las cuales se pueden adquirir en el siguiente enlace <https://www.sans.org/tools/ez-tools/> Son una increíble colección de herramientas que procesan y analizan casi todos los artefactos de Windows.

Elias Ramirez – RamirezS4

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

También un conjunto de herramientas y comandos para obtener información sobre la red y conexiones.

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

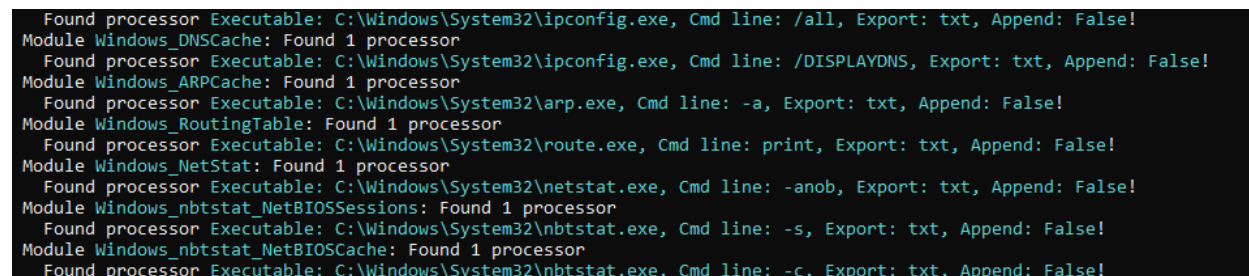


```
D:\Herramientas forenses\kape\KAPE\kape.exe
KAPE version 1.3.0.2, Author: Eric Zimmerman, Contact: https://www.kroll.com/kape (kape@kroll.com)

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,!EZParse
r,LiveResponse_NetworkDetails --gui

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

Mediante la línea de comandos podemos ver la ejecución de las herramientas



```
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

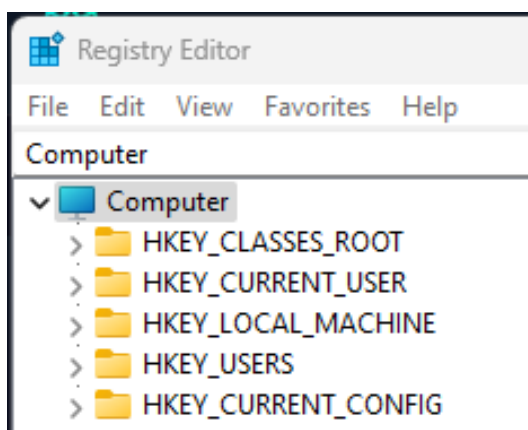
Entre los resultados podemos ver el resultado de los comandos

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, también podemos ver los archivos en la papelera de reciclaje junto con su tamaño y fecha de borrado.

SourceName	File Type	FileName	File Size	Deleted On
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HIE84XB.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento1.asd	35840	1/8/2024 23:10
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\H43X24Q	\$I	C:\Users\Elias.Ramirez\Desktop\Prueba1	17187091	1/8/2023 14:8
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\H7NDASA.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento2.asd	23040	1/14/2024 16:55
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\H8PFLAI.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento1.asd	23552	1/6/2024 13:47
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HIB1NEVO.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento1.asd	23552	1/9/2024 22:50
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HIC7IR7E.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento1.asd	33792	1/12/2024 13:46
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HJL7LOW.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento2.asd	43008	*****
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HIM60A47.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento1.asd	31744	1/12/2024 13:46
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HIN53C0S.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento1.asd	418304	1/14/2024 16:55
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HJPY242O.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento1.asd	313856	*****
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HIRU79Z.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\HIN60D03.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento1.asd	23552	*****
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HIV24SFG.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento2.asd	98816	1/12/2024 0:58
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HVK41TX.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento1.asd	24064	1/13/2024 14:45
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HXGATIL.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento2.asd	23552	1/13/2024 14:45
C:\Recycle.Bin\S-1-5-21-1355104075-3981333728-3372849789-1001\HMT1M.asd	\$I	C:\Users\Elias.Ramirez\AppData\Roaming\Microsoft\Word\Guardado con Autorrecuperaci3n de Documento1.asd	24064	*****

Registros de Windows



El sistema de registros de Windows es una interfaz operativa que provee Windows como un recurso muy 3til para guardar las configuraciones del usuario, guardar rutas de acceso para archivos o carpetas y mantener un respaldo de los drivers utilizados para el hardware del equipo,

as3 como ajustes b3sicos del equipo, Datos sobre qu3 aplicaciones est3n instaladas, sus configuraciones, los archivos que pueden crear y con qu3 programa abrir cada tipo, entre otras funciones. Fijarse en la imagen la cual muestra las 5 principales clases que tenemos en un sistema.

El registro est3 organizado en una serie de claves, cada una de las cuales representa un aspecto diferente de la configuraci3n del sistema. Las claves est3n organizadas en una estructura jer3rquica, y las claves principales contienen claves y valores secundarios.

ftk imager

Esta es una herramienta muy potente que recopila datos de cualquier dispositivo o sistema digital que produzca, transmita o almacene datos; y realiza el análisis forense de los mismos, también pudo ser usada en los módulos anteriores pero la preferí reservar para este apartado el enlace de la fuente oficial de la misma es <https://www.exterro.com/digital-forensics-software/ftk-imager>. Posee una gran desventaja la cual es que requiere instalación y esto afecta la integridad del dispositivo.

Instalación en una USB

Aunque existe un método para instalar el mismo en una unidad USB, deben Insertar el dispositivo USB formateado con ya sea sistema de archivos FAT32 o NTFS en un equipo que tendrá instalado FTK Imager. Copiar toda la carpeta de instalación de nombre “FTK Imager”, el cual generalmente se ubica en la ruta “C: \Program Files\AccessData\FTK Imager” o “C:\Program Files (x86) \AccessData\FTK Imager”, hacia el dispositivo USB. Insertar el dispositivo USB en el sistema donde se requiere realizar un Triage o generar imágenes forenses. Navegar el directorio creado en el dispositivo USB, para luego ejecutar el archivo de nombre “FTK Imager.exe”, con los privilegios del usuario Administrador.

Datos importantes

Las claves "HKEY_LOCAL_MACHINE(HKLC)" y "HKEY_CURRENT_USER(HKCU)" son las claves de registro más importantes, ya que la mayoría de los datos de valor forense se almacenan en estas claves.

Windows realiza automáticamente una copia de seguridad de toda la estructura del registro en caso de falla. Esto se almacena en "C:\Windows\System32\Config\RegBack". Es fundamental analizar esto, ya que el registro de respaldo puede tener valores que no están en el registro más reciente. Esto puede ayudarnos a encontrar claves de registro manipuladas comparando la copia de seguridad y los valores de registro actuales.

Recopilación de registros y datos

Cuando Abrimos FTK Imager nos pedirá seleccionar el disco donde tenemos la información, luego iremos recorriendo la ruta hasta llegar a "C:\Windows\System32\Config".



C:\NONAME [NTFS]/[root]/Windows/System32/config

En su caso podría variar el disco principal lo demás debería ser igual. Una vez en esta ruta verán un conjunto grande de archivos. Buscaremos los archivos "SAM, SECURITY, SOFTWARE, SISTEMA y sus registros logs".

Veremos que cada uno de estos registros que buscaremos tiene un formato similar al siguiente:

SYSTEM	10,752	Regular File	1/12/2024 2:53:18 PM
SYSTEM.FileSlack	128	File Slack	
SYSTEM.LOG1	0	Regular File	12/7/2019 9:03:44 AM
SYSTEM.LOG1		\$I30 INDX Entry	
SYSTEM.LOG2	2,685	Regular File	12/7/2019 9:03:44 AM
SYSTEM.LOG2		\$I30 INDX Entry	
SYSTEM.LOG2.FileSlack	520	File Slack	

No tomaremos los archivos “. FileSlack” entonces en este caso solo tomaría los archivos: “SYSTEM”, “SYSTEM.LOG1” Y “SYSTEM.LOG2”, y así sería con todos los casos al final deberíamos tener mínimo 12 archivos

Comenzamos

Al encontrar todos los archivos que buscamos le damos a “Add to Custom Content image (AD1)”

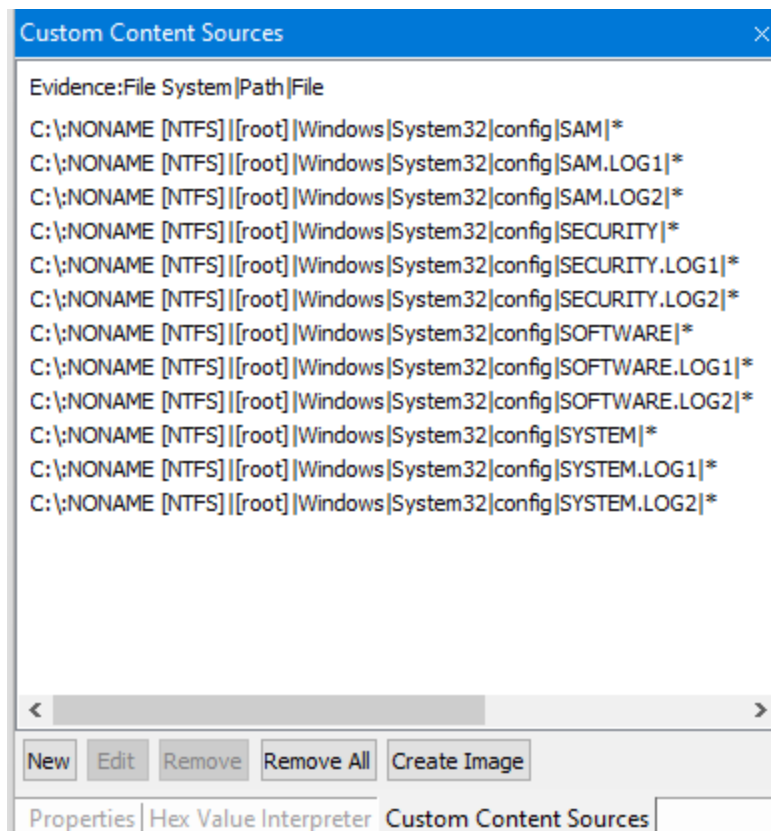
SAM	64	Regular File	1/12/2024 2:53:18 PM
SAM.FileSlack		File Slack	
SAM.LOG1		Regular File	12/7/2019 9:03:44 AM
SAM.LOG1		File Slack	
SAM.LOG2		Regular File	12/7/2019 9:03:44 AM

Export Files...

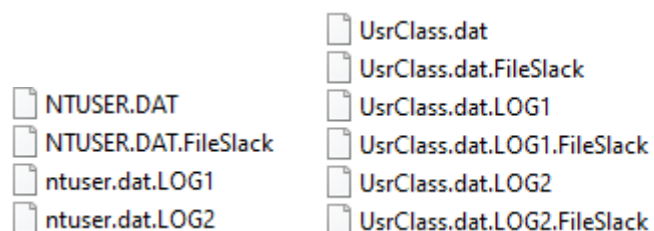
Export File Hash List...

Add to Custom Content Image (AD1)

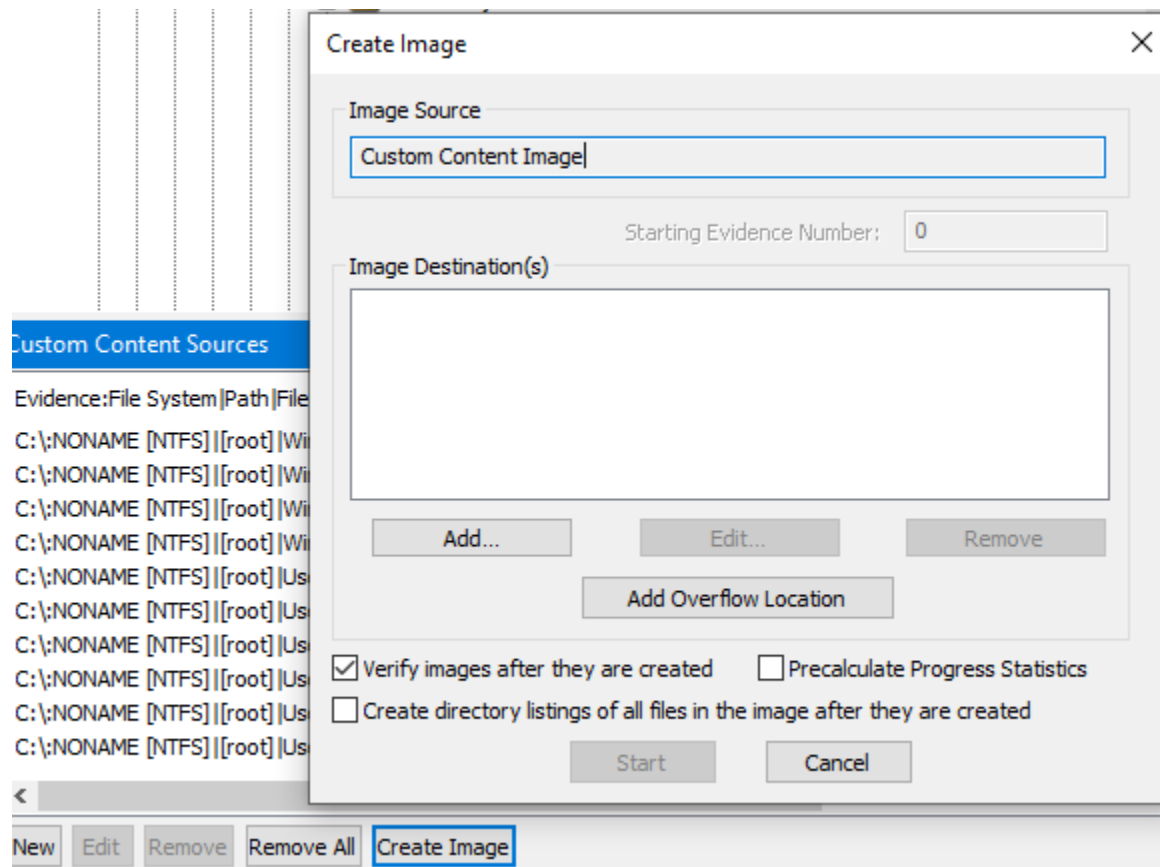
Al final lo veríamos así:



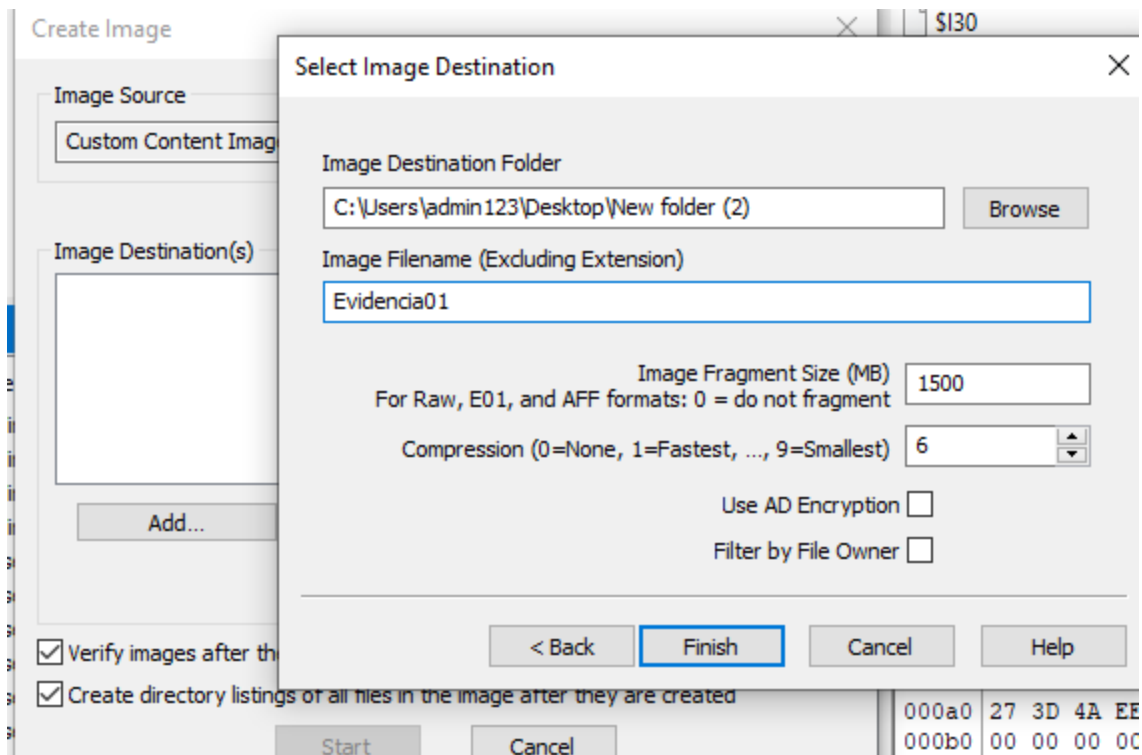
También agregamos los archivos NTUSER.DAT en la ruta “C:\Users\ [nombre de usuario]” y UsrClass.dat en la ruta “User\AppData\Local\Microsoft\Windows\”.



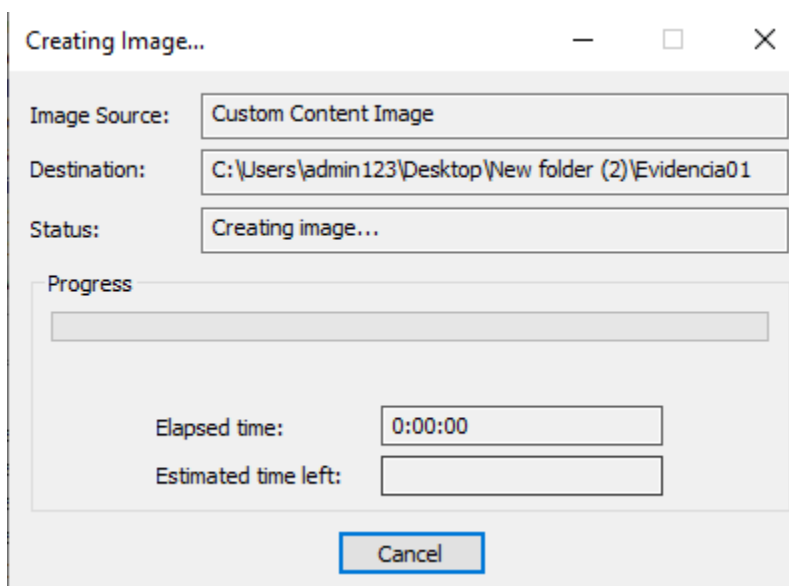
Presionamos crear imagen personalizada y luego le damos a añadir



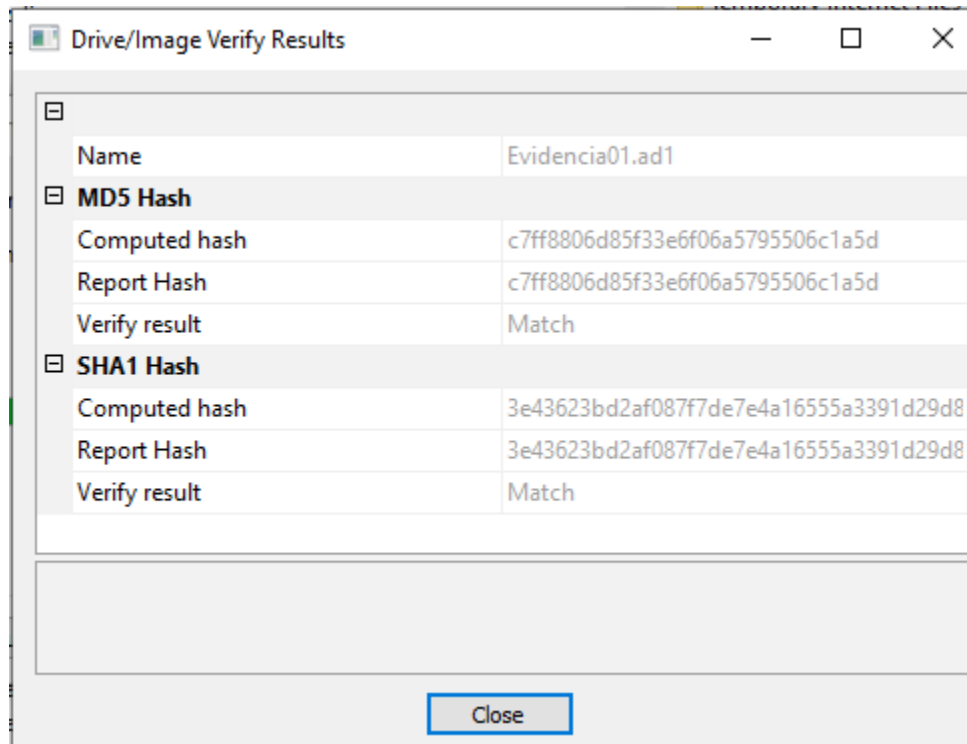
Se abrirá esta ventana, rellenamos los datos



Ahora solo debemos esperar que se complete



Al finalizar nos dará el hash md5 y sha1 del archivo ad1 recién generado



Viendo el resultado vemos los archivos recopilados

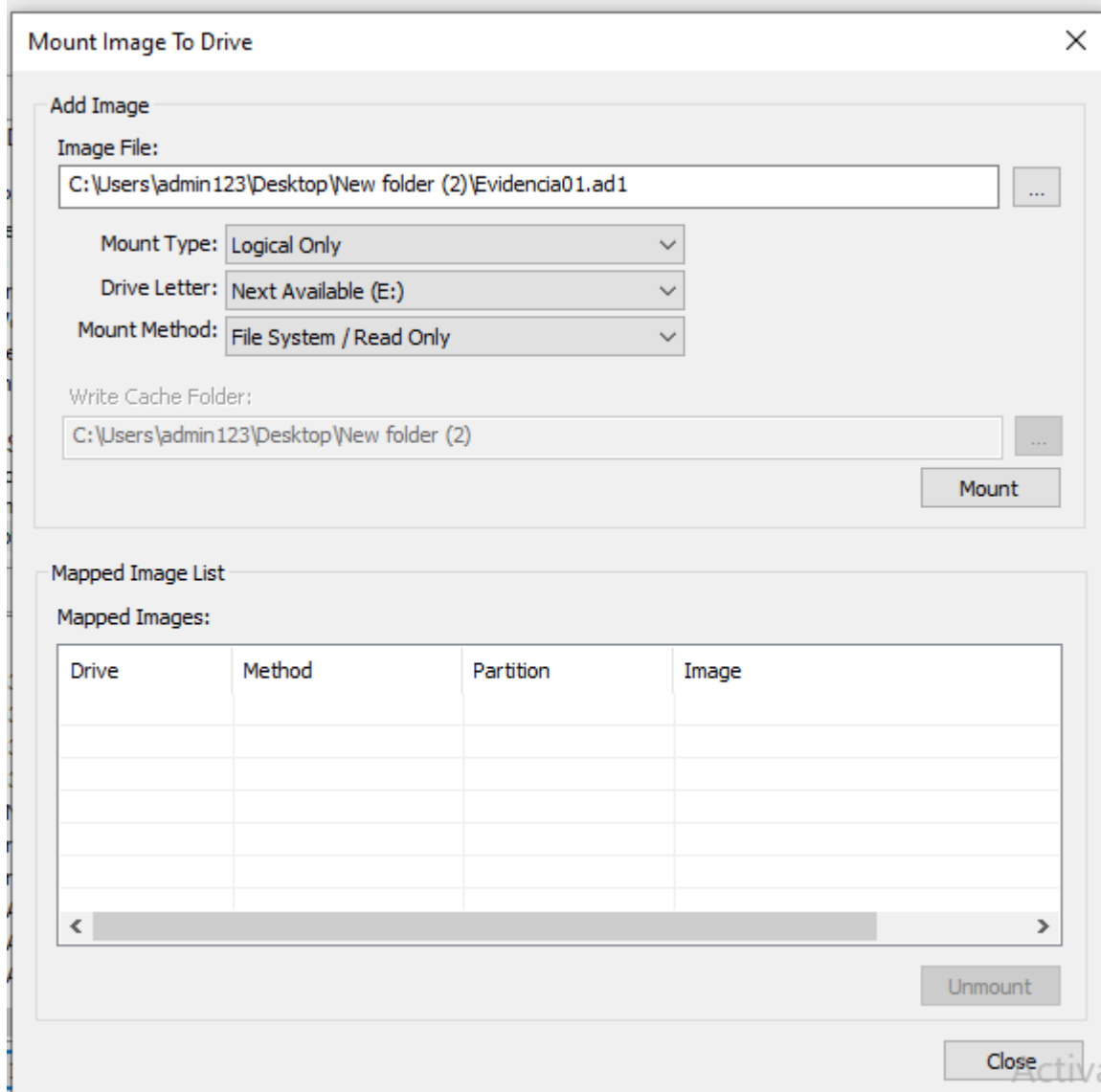
```
Evidencia01.ad1.txt - Notepad
File Edit Format View Help

-----
Information for C:\Users\admin123\Desktop\New folder (2)\Evidencia01.ad1:
[Custom Content Sources]
C:\:NONAME [NTFS][root]Windows\System32\config\SAM*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Windows\System32\config\SAM.LOG1*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Windows\System32\config\SAM.LOG2*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Windows\System32\config\SECURITY*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Windows\System32\config\SECURITY.LOG1*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Windows\System32\config\SECURITY.LOG2*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Windows\System32\config\SOFTWARE*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Windows\System32\config\SOFTWARE.LOG1*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Windows\System32\config\SOFTWARE.LOG2*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Windows\System32\config\SYSTEM*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Windows\System32\config\SYSTEM.LOG1*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Windows\System32\config\SYSTEM.LOG2*(Wildcard,Consider Case,Include Subdirectories)
C:\:NONAME [NTFS][root]Users\admin123\NTUSER.DAT(Exact)
C:\:NONAME [NTFS][root]Users\admin123\ntuser.dat.LOG1(Exact)
C:\:NONAME [NTFS][root]Users\admin123\ntuser.dat.LOG2(Exact)
C:\:NONAME [NTFS][root]Users\admin123\AppData\Local\Microsoft\Windows\UsrClass.dat(Exact)
C:\:NONAME [NTFS][root]Users\admin123\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1(Exact)
C:\:NONAME [NTFS][root]Users\admin123\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2(Exact)
[Computed Hashes]
MD5 checksum: c7ff8806d85f33e6f06a5795506c1a5d
SHA1 checksum: 3e43623bd2af087f7de7e4a16555a3391d29d8b4

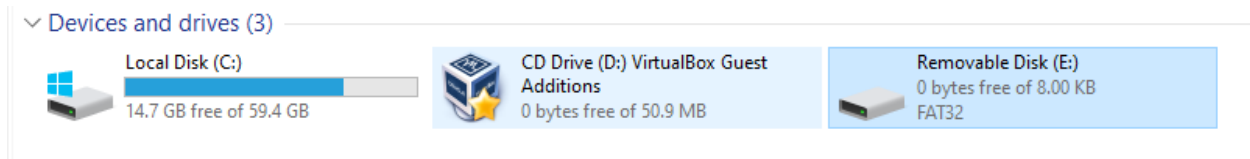
Image information:
Acquisition started: Sun Jan 28 05:28:46 2024
Acquisition finished: Sun Jan 28 05:29:25 2024
Segment list:
C:\Users\admin123\Desktop\New folder (2)\Evidencia01.ad1

Activate Windows
Go to Settings to activate Windows.
```

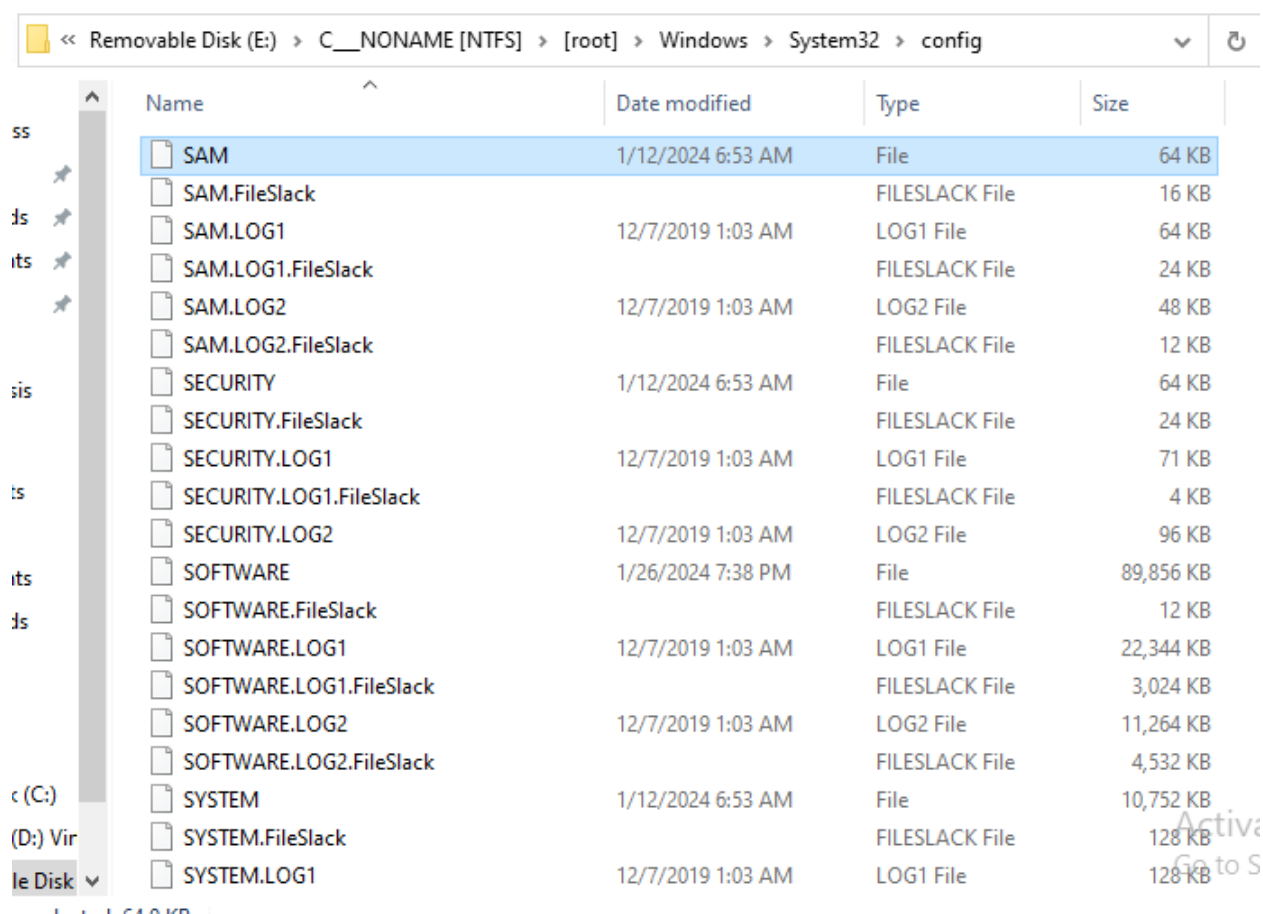
En el mismo FTK vamos al montaje de imagen y seleccionamos la imagen recién creada.



Vemos como se agregó la imagen



Navegamos en las carpetas y veremos los archivos recopilados en sus respectivas rutas, pueden tomar esta imagen como referencia para ver los archivos que deben tener, es bueno aclarar que los archivos “. FileSlack” que ven no es que los seleccionemos en pasos anteriores, sino que este se genera al momento de montar la imagen.



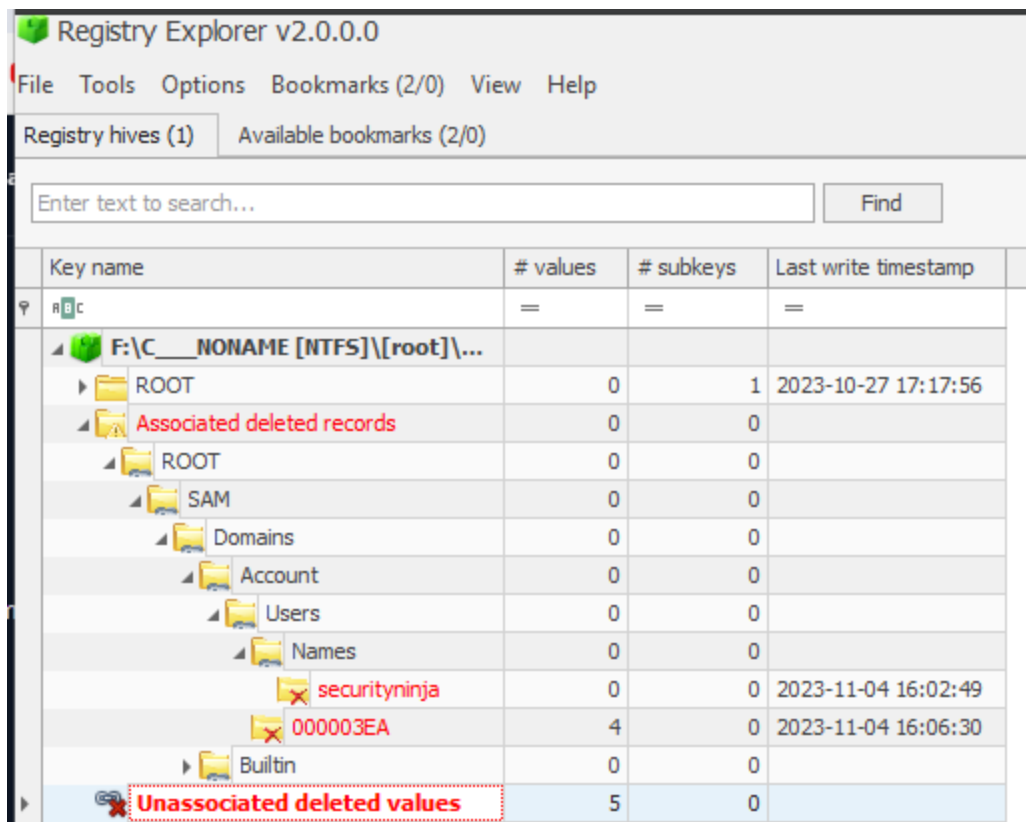
Name	Date modified	Type	Size
SAM	1/12/2024 6:53 AM	File	64 KB
SAM.FileSlack		FILESLACK File	16 KB
SAM.LOG1	12/7/2019 1:03 AM	LOG1 File	64 KB
SAM.LOG1.FileSlack		FILESLACK File	24 KB
SAM.LOG2	12/7/2019 1:03 AM	LOG2 File	48 KB
SAM.LOG2.FileSlack		FILESLACK File	12 KB
SECURITY	1/12/2024 6:53 AM	File	64 KB
SECURITY.FileSlack		FILESLACK File	24 KB
SECURITY.LOG1	12/7/2019 1:03 AM	LOG1 File	71 KB
SECURITY.LOG1.FileSlack		FILESLACK File	4 KB
SECURITY.LOG2	12/7/2019 1:03 AM	LOG2 File	96 KB
SOFTWARE	1/26/2024 7:38 PM	File	89,856 KB
SOFTWARE.FileSlack		FILESLACK File	12 KB
SOFTWARE.LOG1	12/7/2019 1:03 AM	LOG1 File	22,344 KB
SOFTWARE.LOG1.FileSlack		FILESLACK File	3,024 KB
SOFTWARE.LOG2	12/7/2019 1:03 AM	LOG2 File	11,264 KB
SOFTWARE.LOG2.FileSlack		FILESLACK File	4,532 KB
SYSTEM	1/12/2024 6:53 AM	File	10,752 KB
SYSTEM.FileSlack		FILESLACK File	128 KB
SYSTEM.LOG1	12/7/2019 1:03 AM	LOG1 File	128 KB

Para explorar los registros usaremos la herramienta Registry Explorer de Eric Zimmerman Para descargar todas las herramientas de Eric Zimmerman pueden utilizar el siguiente script <https://f001.backblazeb2.com/file/EricZimmermanTools/Get-ZimmermanTools.zip>, si solo quieren descargar algunas pueden ir al enlace <https://ericzimmerman.github.io/#!index.md> y si quieren descargar de forma directa registry Explorer ir al enlace <https://www.sans.org/tools/registry-explorer/>.

Abrimos la herramienta con permisos de administrador, vamos al lado izquierdo en “file” y veremos que tenemos dos opciones, tenemos la opción de abrir los registros del sistema en tiempo real o cargar la copia que realizamos en este caso, por motivos de mantener la integridad del equipo investigado usaremos la copia que acabamos de crear y montamos con FTK, lo seleccionamos todos y abrimos

Registros SAM

Para este primer ejemplo abriremos los registros SAM previamente obtenidos:



Key name	# values	# subkeys	Last write timestamp
F:\C__\NONAME [NTFS]\[root]\...	=	=	=
ROOT	0	1	2023-10-27 17:17:56
Associated deleted records	0	0	
ROOT	0	0	
SAM	0	0	
Domains	0	0	
Account	0	0	
Users	0	0	
Names	0	0	
securityninja	0	0	2023-11-04 16:02:49
000003EA	4	0	2023-11-04 16:06:30
Builtin	0	0	
Unassociated deleted values	5	0	

Mientras me desplazo por los mismos veo algunos registros fueron eliminados veo que se trata de un usuario borrado llamado “securityNinja” y me dice la fecha en que se eliminó.

Ahora vamos a ir a la ruta “Users” y la seleccionamos veremos que en la parte derecha nos dará información:

The screenshot shows the Windows Registry Editor. The left pane displays the tree structure of the registry, with the 'Users' subkey under the 'SAM' hive selected. The right pane shows the 'Values' tab, displaying a list of user accounts. The 'Users' value is highlighted, showing a 'RegDword' type with a value of 0. The 'Users' value is a RegDword with a value of 0.

Key name	# values	# subkeys	Last write timestamp
F:\C:\NONAME [NTFS]\[root]\...	=	=	=
ROOT	0	1	2023-10-27 17:17:56
SAM	2	3	2023-10-27 17:32:33
Domains	1	2	2023-10-27 17:17:56
Account	2	3	2023-11-06 16:57:02
Aliases	1	2	2023-10-27 17:17:56
Groups	1	2	2023-10-27 17:17:56
Users	1	7	2023-11-04 16:06:30
Builtin	3	3	2023-12-25 16:57:56
LastSkuUpgrade	1	0	2023-10-27 17:32:33
RXACT	1	0	2023-10-27 17:17:56
Associated deleted records	0	0	
Unassociated deleted values	5	0	

Value name	Value type	Value
(default)	RegDword	0

Entre la información que podemos encontrar en este apartado se encuentra:

- Intentos fallidos de inicio de sección
- Intentos exitosos de inicio de sección
- Fecha de creación de la cuenta
- Ultima fecha de ingreso al sistema
- Ultima vez que se cambió la clave de los usuarios
- Fecha del último intento de sección fallido.
- Grupos en los que se encuentra el usuario
- En caso de que se tenga configurado podemos ver las preguntas de seguridad.
- Si la cuenta esta deshabilitada o no

Ya vemos toda la información que podemos obtener de los registros sin necesidad de realizar algún comando o modificación en el equipo, solamente extraemos los registros y los analizamos en un entorno aislado.

También podemos observar los miembros de cada grupo y una breve descripción del grupo

Enter text to search...Find

Key name# values

F:\C_\NONAME [NTFS]\[root]\Windows\System32\co...

ROOT

SAM

Domains

Account

Aliases

Groups

Users

Builtin

Aliases

Groups

Users

LastSkuUpgrade

RXACT

Associated deleted records

Unassociated deleted values

Drag a column header here to group by that column

Group NameCommentUsers

Administrators

Administrators have complete and unrestricted access to the computer/domain

S-1-5-21-2964515817-89810237-1856536195-500,
S-1-5-21-2964515817-89810237-1856536195-1001

Users

Users are prevented from making accidental or intentional system-wide changes and can run most applications

S-1-5-4, S-1-5-11

Guests

Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted

S-1-5-21-2964515817-89810237-1856536195-501

Power Users

Power Users are included for backwards compatibility and possess limited administrative powers

Backup Operators

Backup Operators can override security restrictions for the sole purpose of backing up or restoring files

Replicator

Supports file replication in a domain

Remote Desktop Users

Members in this group are granted the right to logon remotely

Network Configuration Operators

Members in this group can have some administrative privileges to manage configuration of networking features

Performance Monitor Users

Members of this group can access performance counter data locally and remotely

Performance Log Users

Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces

S-1-5-4

Total rows: 19

Export

Registros SOFTWARE y SYSTEM

Ahora mostrare que información útil puede obtenerse de estos registros, los usaremos en conjunto ya que de una forma u otra se complementan, entre la información que podemos encontrar aquí se encuentra:

- configuración del sistema

- Servicios que inician con el sistema e información sobre estos
- información del sistema operativo
- información de red
- información de zona horaria

Sobre los servicios podremos ver la información que mencionamos y cada uno tendrá su respectivo archivo con información adicional

The screenshot displays the Windows Services console. On the left, a tree view shows the hierarchy of services, with 'Services' expanded under 'ControlSet001'. The main pane shows a list of services with columns: Name, Description, Display Name, Start Mode, Service Type, Name Key, Parameters, Group, Image Path, Service DLL, and Required Privileges. The services listed include .NET CLR Data, .NET CLR Networking, .NET CLR Networking 4.0.0.0, .NET Data Provider for Oracle, .NET Data Provider for SqlServer, .NET Memory Cache 4.0, .NETFramework, ADOVMPackage, adsi, CoreUI, crypt32, DGLocator, ESENT, and HomeGroupProvider. The bottom status bar shows 'Selected hive: SYSTEM_clean', 'Last write: 2024-01-28 01:42:54', 'Key contains no values', 'Load complete', 'Value: None', 'Collapse all hives', and 'Hidden keys: 0'.

Name	Description	Display Name	Start Mode	Service Type	Name Key	Parameters	Group	Image Path	Service DLL	Required Privi...
.NET CLR Data			Disabled	Adapter	2023-10-27 ...					
.NET CLR Networking			Disabled	Adapter	2023-10-27 ...					
.NET CLR Networking 4.0.0.0			Disabled	Adapter	2019-12-07 ...					
.NET Data Provider for Oracle			Disabled	Adapter	2019-12-07 ...					
.NET Data Provider for SqlServer			Disabled	Adapter	2019-12-07 ...					
.NET Memory Cache 4.0			Disabled	Adapter	2019-12-07 ...					
.NETFramework			Disabled	Adapter	2019-12-07 ...					
ADOVMPackage										
adsi										
CoreUI										
crypt32										
DGLocator										
ESENT										
HomeGroupProvider										

También podemos ver la información sobre la versión del sistema que tenemos

Drag a column header here to group by that column						
Value Name	Value Type	Data	Data Record Reallocated	
...
EditionID	RegSz	Enterprise
EditionSubManufacturer	RegSz	
EditionSubstring	RegSz	
EditionSubVersion	RegSz	
InstallationType	RegSz	Client
InstallDate	RegDword	0
ProductName	RegSz	Windows 10 Enterprise
ReleaseId	RegSz	2009
SoftwareType	RegSz	System
SystemRoot	RegSz	C:\Windows
UBR	RegDword	2965
DisplayVersion	RegSz	22H2
RegisteredOwner	RegSz	admin 123
RegisteredOrganization	RegSz	
PathName	RegSz	C:\Windows

Esta información por lo general se encuentra en la ruta “SOFTWARE\Microsoft\Windows NT\CurrentVersion” en mi caso se encuentra en la

WOW6432Node\Microsoft\Windows NT\CurrentVersion

La máquina que utilizo es un Windows 10 con VM-Flare instalado, la cual es perfecta para realizar análisis de malware.

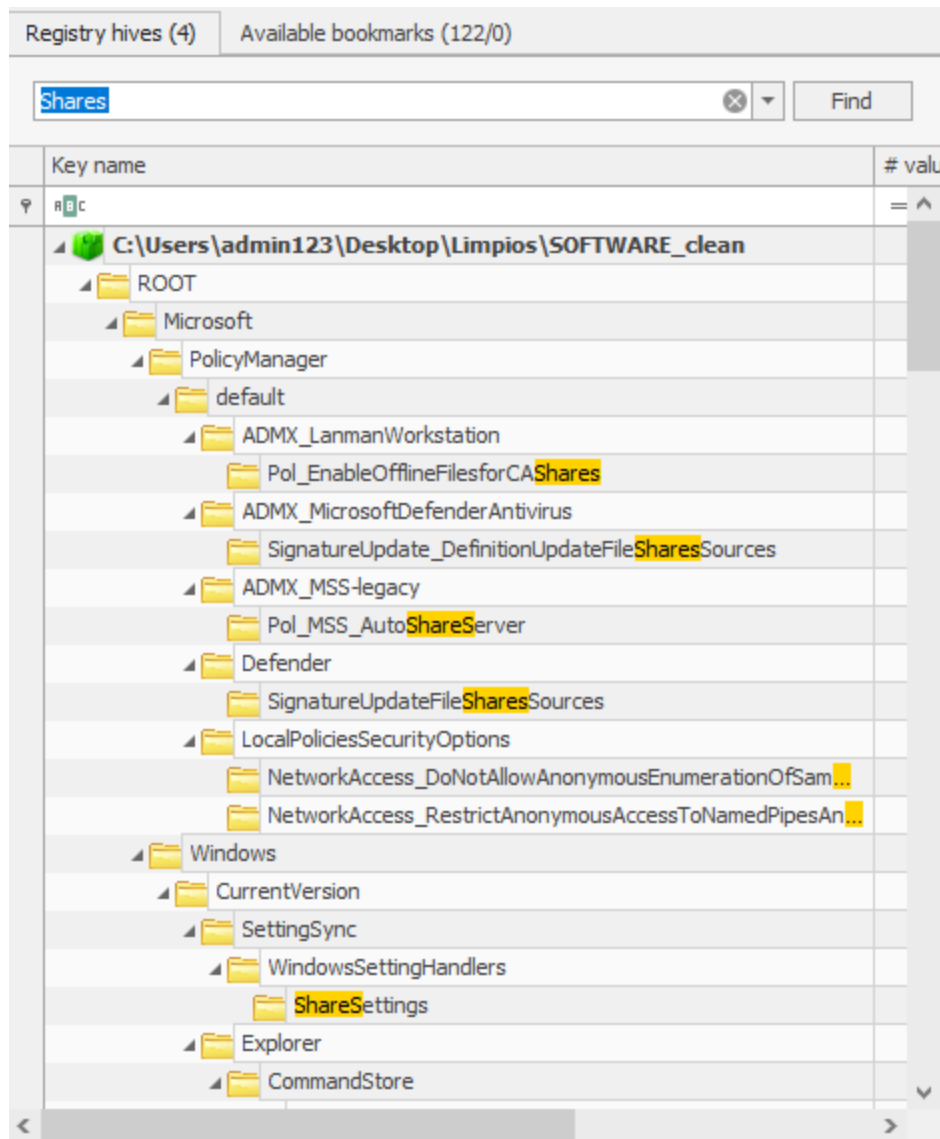
En estos registros también encontraremos sobre las conexiones de la maquina “- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList”

The screenshot displays the NetworkList application interface. On the left, a tree view shows the file system structure, with 'NetworkList' highlighted under 'CurrentVersion'. The main pane on the right shows a table of network data. The table has columns: First Network, Network Name, Name Type, First Connect L..., Last Connected ..., Managed, DNS Suffix, Gateway Mac A..., and Profile GUID. The first row of data shows 'Network' as the First Network, 'Network' as the Network Name, 'Wired' as the Name Type, and '2023-10-27 10:...' as the First Connect L... The table also shows '2024-01-27 17:...' as the Last Connected ..., 'Managed' as 'false', '<none>' as the DNS Suffix, '52-54-00-12-35-02' as the Gateway Mac A..., and '(8801E099-9718-47E0-A9F9-54A54087836F)' as the Profile GUID. Below the table, there is a 'Total rows: 1' indicator and an 'Export' button. A 'Status messages' dialog box is open, displaying 'Displays information related to program usage and actions'. At the bottom, a status bar shows 'Selected hive: SOFTWARE', 'Last write: 2024-01-28 01:40:30', '3 of 3 values shown (100.00%)', 'Copied path to clipboard', 'Value: (default)', 'Collapse all hives', and 'Hidden keys: 0 18'.

First Network	Network Name	Name Type	First Connect L...	Last Connected ...	Managed	DNS Suffix	Gateway Mac A...	Profile GUID
Network	Network	Wired	2023-10-27 10:...	2024-01-27 17:...	<input type="checkbox"/>	<none>	52-54-00-12-35-02	(8801E099-9718-47E0-A9F9-54A54087836F)

Podemos ver de forma rápida el SSID de la red, la primera y última vez que se conectó y la MAC del AP o router.

Otro apartado útil es el de búsqueda de la parte superior izquierda en la cual podemos buscar por palabras o ruta clave. Por ejemplo, sabemos o pensamos que el atacante pudo acceder a algún recurso compartido buscamos la palabra clave “shares” y tenemos los siguientes resultados



Aquí podemos buscar si el equipo tenía algún recurso compartido al momento de tomar los registros, también podemos ver a que recursos compartidos se tenía acceso desde la máquina.

