práctica 3. adquisición y análisis de triaje

Hecho por: izan Navarro

índice

1-introducción:

Como se ha visto anteriormente, en nuestra labor como analista forense es posible que tengamos problemas o reticencias a la hora de realizar un clonado completo del disco del equipo a analizar.

Para esos casos aparece la figura del triaje de sistema de archivos.

Un triaje es una selección de archivos y/o artefactos de gran valor forense para la investigación. Es útil en situaciones en las que realizar una imagen forense no es viable o el tiempo es un factor importante.

2-Realización del triaje:

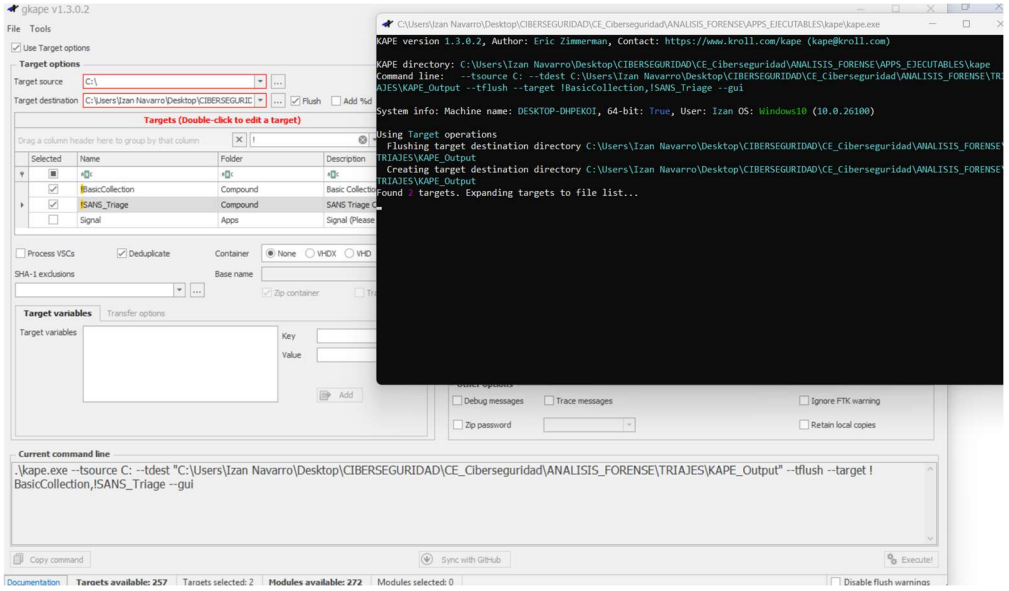
En este ejercicio deberás realizar un triaje de tu equipo de trabajo, pero con diferentes herramientas. Ten en cuenta que es posible que cada triaje ocupe 2Gb.

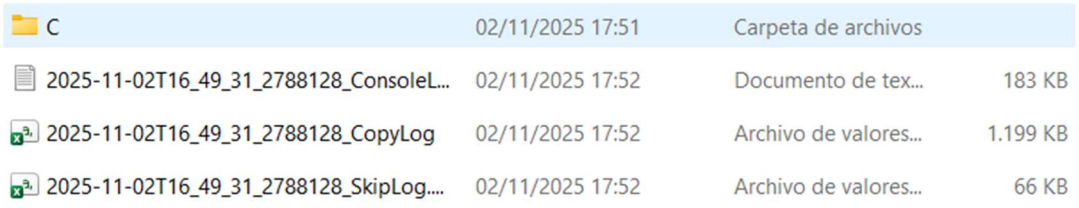
1. Realiza y guarda el triaje con la herramienta Wintriage (deja las opciones por defecto).

Entramos dentro del ejecutable “wintriage.exe” y seleccionamos el archivo destino donde guardar la información del triaje y después le damos al botón “Triage!”.

2. Realiza y guarda el triaje con la herramienta KAPE (selecciona únicamente el Target KapeTriage).

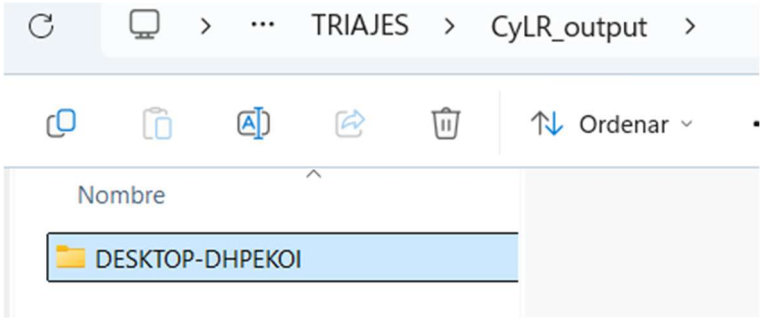
Le damos al ejecutable “kape.exe” y nos saldrá una pantalla donde seleccionar un “Target Source” donde seleccionaremos nuestro disco “C:\” y un target destination donde guardar la información extraída del triaje.





3. Realiza y guarda el triaje con una nueva herramienta propuesta (CyLR). Únicamente funciona en modo comando y devuelve el resultado en un archivo .zip. Descarga la última versión estable y consulta su funcionamiento en https://github.com/orlikoski/CyLR

Ejecutamos el programa “CyLR” y de manera autónoma se nos abrirá un terminal donde se cogerá por defecto nuestro Disco Duro principal como punto de partida para el triaje y después se nos creará en la misma carpeta de descarga, una carpeta con el nombre de nuestra maquina HOST y dentro, su información.



3-Análisis del triaje:

Responde a las siguientes cuestiones analizando los resultados del triaje. Indica también el triaje que has utilizado (el de que aplicación) para obtener la información y con qué herramienta has conseguido la evidencia (si es que has utilizado alguna).

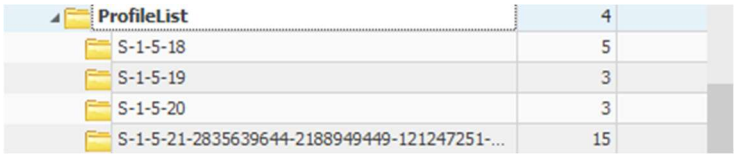
Para la realización de la actividad utilizaré la herramienta “Registry Explorer” de Eric Zimmerman y utilizaré el triaje de KAPE. Esta herramienta se descarga desde un repositorio de GitHub de Eric Zimmerman.

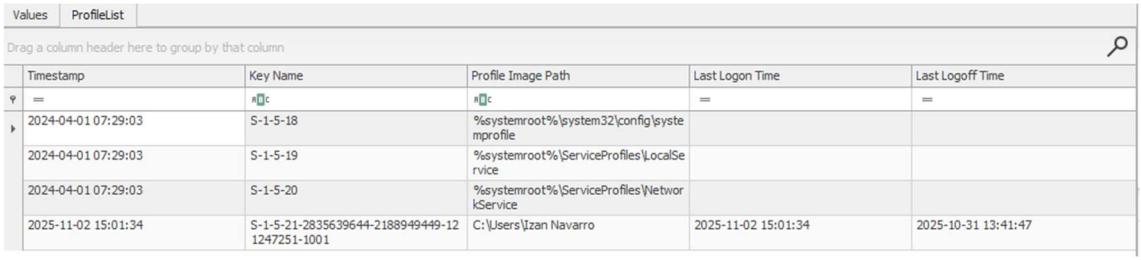
Enlace del repositorio de descarga:

https://ericzimmerman.github.io/#!index.md

1. Indica los perfiles de usuario que se han iniciado sesión en el equipo

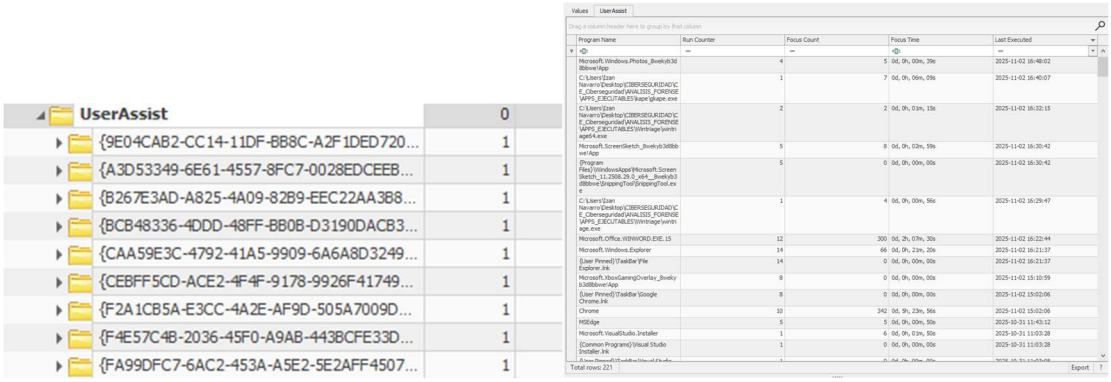
Ruta: “Microsoft/Windows NT/CurrentVersion/ProfileList





2. Las últimas aplicaciones abiertas por el usuario del pc (el que tú utilizas)

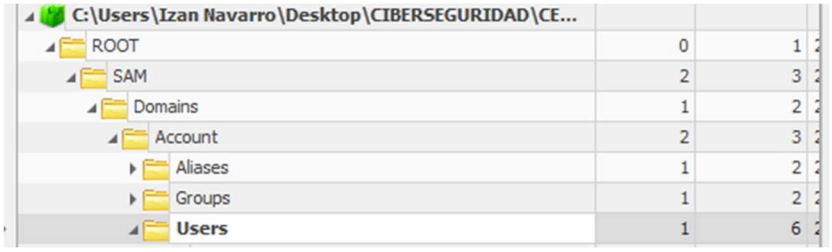
Ruta: “Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist”



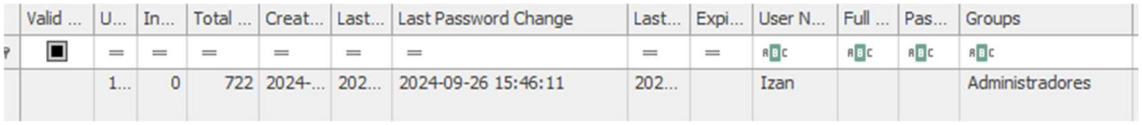
UserAssist	0
{9E04CAB2-CC14-11DF-BB8C-A2F1DED720...	1
{A3D53349-6E61-4557-8FC7-0028EDCEEB...	1
{B267E3AD-A825-4A09-82B9-EEC22AA3B8...	1
{BCB48336-4DDD-48FF-BB0B-D3190DACB3...	1
{CAA59E3C-4792-41A5-9909-6A6A8D3249...	1
{CEBFF5CD-ACE2-4F4F-9178-9926F41749...	1
{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D...	1
{F4E57C4B-2036-45F0-A9AB-443BCFE33D...	1
{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507...	1

3. El último instante en el que se cambió la contraseña de tu usuario

La Ruta: “HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users”



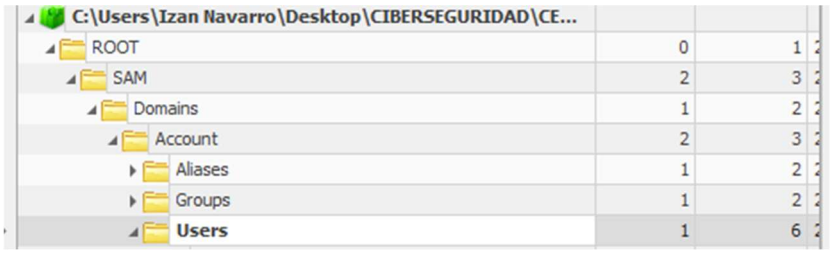
C:\Users\Izan Navarro\Desktop\CIBERSEGURIDAD\CE...		
ROOT	0	1
SAM	2	3
Domains	1	2
Account	2	3
Aliases	1	2
Groups	1	2
Users	1	6



Valid ...	U...	In...	Total ...	Creat...	Last...	Last Password Change	Last...	Expi...	User N...	Full ...	Pas...	Groups
	1...	0	722	2024-...	202...	2024-09-26 15:46:11	202...		Izan			Administradores

4. La última vez que hubo un intento fallido de inicio de sesión

La Ruta: “HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users”

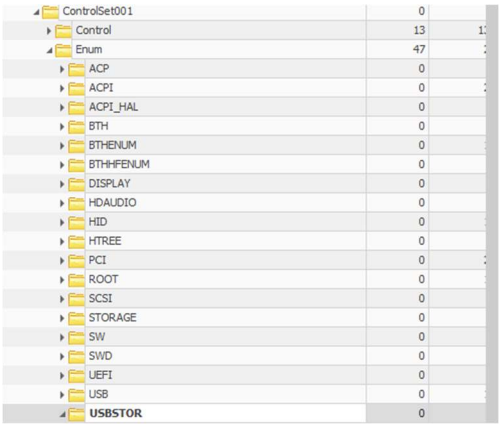


C:\Users\Izan Navarro\Desktop\CIBERSEGURIDAD\CE...		
ROOT	0	1
SAM	2	3
Domains	1	2
Account	2	3
Aliases	1	2
Groups	1	2
Users	1	6

Vali...	User Id	Invalid Login Count	Tot...	Cre...	Last Login Time	Las...	Las...	Ex...	User ...	Ful...	Pa...	Groups
	1001	0	722	202...	2025-11-02 15:01:59	20...	20...		Izan			Administradores

5. El último dispositivo USB que se conectó

La Ruta es: “SYSTEM/ControlSet001/Enum/USBSTOR”



Timestamp	Manufacturer	Title	Version	Serial Number	Device Name
2025-10-24 14:41:58	Ven_	Prod_PHILIPS	Rev_1100	7&325b708c&0	PHILIPS USB Device
2025-10-06 11:59:20	Ven_ASolid	Prod_USB	Rev_	021220238&0	ASolid USB USB Device
2025-10-07 16:53:29	Ven_Generic	Prod_Flash_Disk	Rev_8.01	13988EDD&0	Generic Flash Disk USB Device
2025-10-07 15:15:05	Ven_Kingston	Prod_DataTraveler_3.0	Rev_PMAP	60A44C413E29BE81AB4C645D&0	Kingston DataTraveler 3.0 USB Device
2025-10-30 18:17:39	Ven_VendorCo	Prod_ProductCode	Rev_2.00	7777054D893220440548&0	VendorCo ProductCode USB Device
2025-10-30 18:17:39	Ven_VendorCo	Prod_ProductCode	Rev_2.00	9207117B2626081097 6&0	VendorCo ProductCode USB Device

6. La fecha y en la que obtuvo su última IP. Identifica que interfaz es (Wifi o cableada)

La Ruta es: “SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces”

IP Address	Subnet Mask	DHCP Subnet Mask	DHCP Server	DHCP Name Server	DHCPIP Address	DHCP Default Gateway	Lease Obtained Time	Lease Terminates Time	Enabled DHCP
192.168.56.1	255.255.255.0								☐
									☐
									☑
									☑
									☐
									☑
		255.255.255.0	192.168.1.1	100.100.1.1 100.90.1.1	192.168.1.243	192.168.1.1	2025-11-02 15:01:42	2025-11-03 15:01:42	☑

7. La lista de software que se arranca al inicio del sistema

La Ruta para ver el software de arranque del sistema es: “SOFTWARE\Microsoft\Windows\CurrentVersion\Run”

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
SecurityHealth	RegExpandSz	%windir%\system32\SecurityHealthSystray.exe	00-00-00-00	☐	☐

4-Conclusiones:

Redacta un informe argumentado tus conclusiones en el que se responda a las siguientes cuestiones:

• ¿Qué herramienta de triaje es más completa?

Si miro cómo se ordena el sitio y cómo se reparte la información, creo que KAPE (Kroll Artifact Parser and Extractor) es la mejor opción. Es la herramienta de sacar datos de triaje más completa y sirve para muchas cosas. Su mejor punto es el orden en que muestra lo que saca. Esto ayuda a entender mejor el contenido. También hace fácil hallar piezas clave en una revisión forense. Su diseño con módulos y la opción de ajustarla con objetivos y partes la hace flexible. Sirve para retos y gustos distintos. KAPE no solo saca datos bien. También los clasifica de forma clara y ordenada. Esto ayuda mucho al hacer el estudio.

• ¿Cuál de ellas es más sencilla de utilizar?

Para usarla fácil, pienso que CyLR es la más simple y directa. Funciona casi sola. Por defecto, elige todo el equipo como lugar para sacar datos. Crea una carpeta al momento con todo lo extraído. Esta carpeta queda cerca del programa que se usa. No pide ajustes difíciles ni saber mucho. Esto es muy bueno si hay que tomar datos rápido. O si la gente no sabe mucho de esto. CyLR también es muy rápida al correr. Saca la información del sistema con gran eficiencia. Así asegura que lo que saca es total y seguro.

• ¿Cuál ofrece mejores resultados?

Al hablar de lo que sacan, la cuenta es buena. KAPE ordena y pone en grupos los datos que toma. Esto hace el estudio de después mucho más fácil. Su forma clara y con detalle ayuda a ver las piezas forenses rápido. Pero, CyLR es mejor en cuánto saca. Hace una toma más grande de todo el equipo. Pienso que KAPE da mejores resultados en orden, claridad y cuánto sirve para el estudio. CyLR brilla por lo mucho que toma y lo rápido que junta datos. Por eso, elegir una u otra depende de lo que se busque. Si se quiere orden y estudio, KAPE es mejor. Si se necesita tomar rápido y mucho sin cambiar nada, CyLR es más útil.

5-Evidencias:

Por último, sube los triajes a tu onedrive, compártelos e indica aquí los enlaces compartidos

Aquí comparto el enlace a un ZIP con los triajes guardados en mi GoogleDrive

https://drive.google.com/file/d/1-q3qsCFmZ0qHeQTSCIW_MkQsLjirPo1v/view?usp=sharing