

Incident investigation



1. Recolección y almacenamiento de evidencias

En esta práctica se documentará el proceso de adquisición y análisis forense de una máquina comprometida, siguiendo la metodología de nuestra empresa para asegurar la integridad y autenticidad de las evidencias. La recolección incluirá información clave como la **tabla de enrutamiento**, el **caché ARP**, los **procesos**, la **memoria**, el contenido del **disco**, los **logs del sistema** y la **topología de red**.

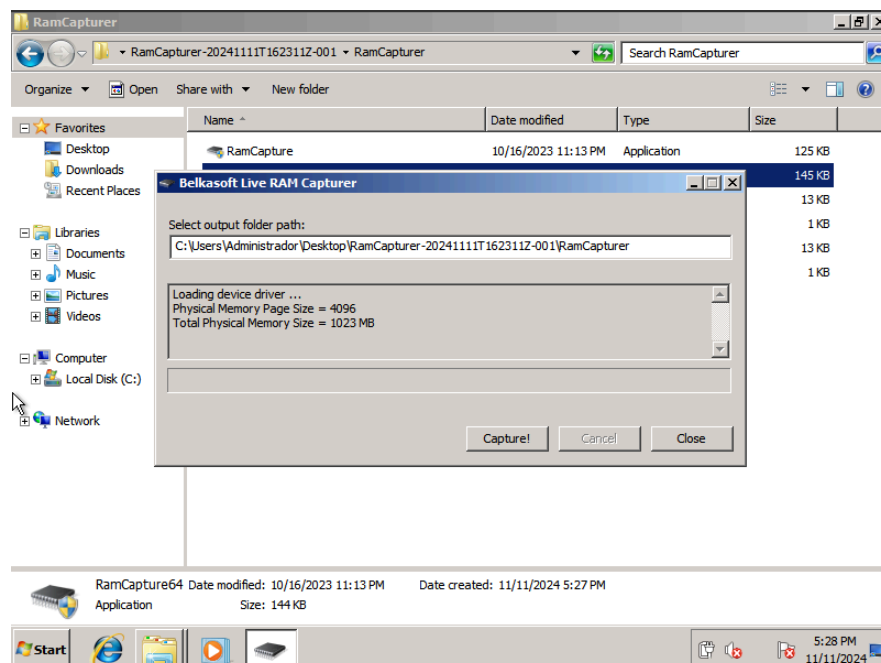
La investigación se estructura en cinco etapas: **recolección de evidencias**, **descripción de la evidencia**, **cadena de custodia**, **almacenamiento** y **metodología aplicada**. En cada fase, se implementan protocolos rigurosos para que la información refleje con precisión el estado del sistema en el momento de su adquisición.

Este informe detalla cada uno de estos pasos, desde la obtención de datos críticos en la máquina comprometida hasta su conservación en un entorno seguro, asegurando su idoneidad para análisis detallados y posibles fines legales.

- RAM

Para la adquisición de la memoria RAM, se utilizó **RAM Capturer** siguiendo estos pasos:

1. **Captura:** RAM Capturer se utilizó para volcar el contenido completo de la memoria, incluyendo procesos activos y datos en caché.



2. **Integridad:** Se generó un hash del volcado para futuras verificaciones.

```
vant@pop-os:~/Escritorio/CompartidaAdquisicion/RAM$ md5sum 20241111.mem
295129c42a4287004456df38a157045d  20241111.mem
vant@pop-os:~/Escritorio/CompartidaAdquisicion/RAM$ sha1sum 20241111.mem
5c1f399b6d1194e934dd4afe8ff05993a385f897  20241111.mem
vant@pop-os:~/Escritorio/CompartidaAdquisicion/RAM$
```

3. **Cadena de custodia**

Fecha y Hora de Recolección	12/11/2024 11:30
Persona Responsable de la Recolección	Gonzalo Pulido Sánchez
Transferencias de Custodia	13/11/2024 08:30 Manuel Rivas Firma
Método de Adquisición	RAM Capturer
Verificación de Integridad	MD5: 295129c42a4287004456df38a157045d SHA1: 5c1f399b6d1194e934dd4afe8ff05993a385f897

Este proceso asegura la captura íntegra y segura de la memoria para su análisis.

- Tabla de enrutamiento

Para obtener la tabla de enrutamiento, se utilizó el comando **route print** siguiendo estos pasos:

1. **Ejecución del comando:** Se ejecutó **route print** en el sistema comprometido, generando una salida detallada de la tabla de enrutamiento actual.

```

C:\Windows\system32\cmd.exe
=====
Interface List
=====
20...08 00 27 b8 9a 49 .....Intel(R) PRO/1000 MT Network Connection #3
1....00 00 00 00 00 00 .....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Microsoft ISM10P Adapter
13...00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
14...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway             Interface           Metric
0.0.0.0                    0.0.0.0          192.168.1.1         192.168.1.154       10
127.0.0.0                  255.0.0.0        On-link             127.0.0.1           306
127.0.0.1                  255.255.255.255  On-link             127.0.0.1           306
127.255.255.255            255.255.255.255  On-link             127.0.0.1           306
192.168.1.0                 255.255.255.0    On-link             192.168.1.154       266
192.168.1.154              255.255.255.255  On-link             192.168.1.154       266
192.168.1.255              255.255.255.255  On-link             192.168.1.154       266
224.0.0.0                  240.0.0.0        On-link             127.0.0.1           306
224.0.0.0                  240.0.0.0        On-link             192.168.1.154       266
255.255.255.255            255.255.255.255  On-link             127.0.0.1           306
255.255.255.255            255.255.255.255  On-link             192.168.1.154       266
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
20      266 ::0                          fe80::1
1       306 ::1/128                      On-link
20      18 2a0c:5a83:3101:e400::/64    On-link
20      266 2a0c:5a83:3101:e400:4ae:aff5:c70f:bbb0/128
20      266 2a0c:5a83:3101:e400:705a:a906:cdb9:d3d3/128
20      266 fe80::/64                      On-link
20      266 fe80::4ae:aff5:c70f:bbb0/128 On-link
1       306 ff00::/8                      On-link
  
```

2. **Registro de resultados:** La salida se guardó en un archivo para preservar el estado de las rutas y conexiones en el momento de la adquisición.

<https://drive.google.com/file/d/1i8ww0CksXIUu61j3yag0hPmsxcp0P0n/view?usp=sharing>

3. Cadena de custodia

Fecha y Hora de Recolección	12/11/2024 11:45
Persona Responsable de la Recolección	Gonzalo Pulido Sánchez
Transferencias de Custodia	13/11/2024 08:45 Manuel Rivas Firma
Método de Adquisición	route print
Verificación de Integridad	MD5: 0c104e7466ba30a2b346f21d928434a3 SHA1: 58acfbcb88f5a8f46c74ab5f6efdf0e9edf1 eecd4

Este procedimiento asegura que la configuración de enrutamiento se preserve para su análisis sin alteraciones.

- **Caché ARP**

Para obtener la caché ARP, se ejecutó el comando **arp -a** y se realizó una captura de pantalla con el siguiente procedimiento:

1. **Ejecución del comando:** Se utilizó **arp -a** en la máquina comprometida para mostrar las relaciones IP-MAC almacenadas en la caché ARP.
2. **Captura de pantalla:** Se tomó una captura de pantalla de la salida del comando, preservando el estado exacto de la caché en ese momento.

```
C:\Users\Administrador>arp -a

Interface: 192.168.1.154 --- 0x14
Internet Address      Physical Address      Type
192.168.1.1           2c-70-4f-2f-d0-af     dynamic
192.168.1.130         44-5c-e9-b3-aa-6e     dynamic
192.168.1.144         00-42-38-be-50-ff     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

3. Cadena de custodia

Fecha y Hora de Recolección	12/11/2024 12:00
Persona Responsable de la Recolección	Gonzalo Pulido Sánchez
Transferencias de Custodia	13/11/2024 09:00 Manuel Rivas Firma
Método de Adquisición	arp -a
Verificación de Integridad	

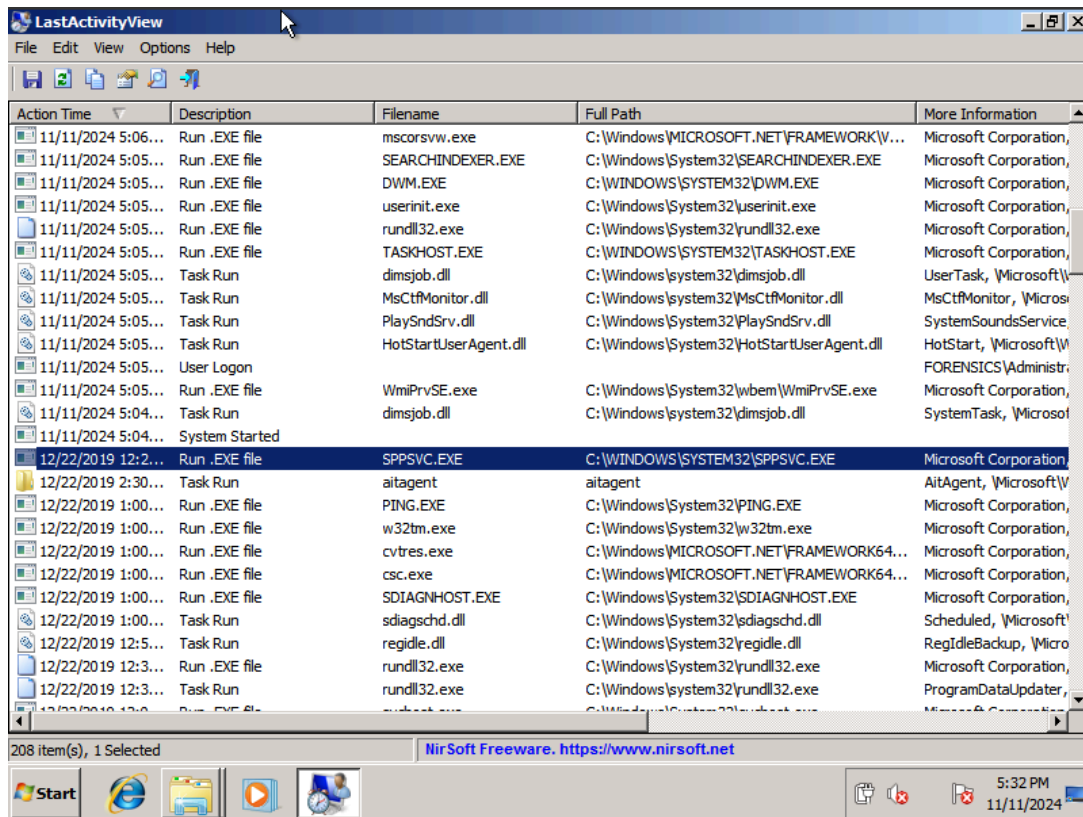
Este método permite conservar la información de la caché ARP de forma visual para su análisis.

- Procesos

Para la adquisición de información sobre los procesos, se utilizó **LastActivityView** siguiendo este procedimiento:

1. **Ejecución de LastActivityView:** La herramienta se ejecutó para capturar información detallada sobre todos los procesos en la máquina comprometida, incluyendo eventos y actividades sospechosas.

2. **Selección de actividad relevante:** Se identificaron y seleccionaron en pantalla aquellos procesos que parecían estar involucrados en la vulneración del sistema, realizando una captura de pantalla de estos para referencia inmediata.



The screenshot shows the LastActivityView application window. The title bar reads 'LastActivityView'. The menu bar includes 'File', 'Edit', 'View', 'Options', and 'Help'. Below the menu bar is a toolbar with icons for file operations. The main area is a table with the following columns: 'Action Time', 'Description', 'Filename', 'Full Path', and 'More Information'. The table contains a list of system activities, including file runs and task executions. The status bar at the bottom indicates '208 item(s), 1 Selected' and provides a link to 'NirSoft Freeware. https://www.nirsoft.net'.

Action Time	Description	Filename	Full Path	More Information
11/11/2024 5:06...	Run .EXE file	mscorsvw.exe	C:\Windows\MICROSOFT.NET\FRAMEWORK\...	Microsoft Corporation,
11/11/2024 5:05...	Run .EXE file	SEARCHINDEXER.EXE	C:\Windows\System32\SEARCHINDEXER.EXE	Microsoft Corporation,
11/11/2024 5:05...	Run .EXE file	DWM.EXE	C:\WINDOWS\SYSTEM32\DWM.EXE	Microsoft Corporation,
11/11/2024 5:05...	Run .EXE file	userinit.exe	C:\Windows\System32\userinit.exe	Microsoft Corporation,
11/11/2024 5:05...	Run .EXE file	rundll32.exe	C:\Windows\System32\rundll32.exe	Microsoft Corporation,
11/11/2024 5:05...	Run .EXE file	TASKHOST.EXE	C:\WINDOWS\SYSTEM32\TASKHOST.EXE	Microsoft Corporation,
11/11/2024 5:05...	Task Run	dimsjob.dll	C:\Windows\system32\dimsjob.dll	UserTask, \Microsof
11/11/2024 5:05...	Task Run	MsCtfMonitor.dll	C:\Windows\system32\MsCtfMonitor.dll	MsCtfMonitor, \Micro
11/11/2024 5:05...	Task Run	PlaySndSrv.dll	C:\Windows\System32\PlaySndSrv.dll	SystemSoundsService
11/11/2024 5:05...	Task Run	HotStartUserAgent.dll	C:\Windows\System32\HotStartUserAgent.dll	HotStart, \Microsof
11/11/2024 5:05...	User Logon			FORENSICS\Administr
11/11/2024 5:05...	Run .EXE file	WmiPrvSE.exe	C:\Windows\System32\wbem\WmiPrvSE.exe	Microsoft Corporation,
11/11/2024 5:04...	Task Run	dimsjob.dll	C:\Windows\system32\dimsjob.dll	SystemTask, \Microso
11/11/2024 5:04...	System Started			
12/22/2019 12:2...	Run .EXE file	SPPSVC.EXE	C:\WINDOWS\SYSTEM32\SPPSVC.EXE	Microsoft Corporation,
12/22/2019 2:30...	Task Run	aitagent	aitagent	AitAgent, \Microsof
12/22/2019 1:00...	Run .EXE file	PING.EXE	C:\Windows\System32\PING.EXE	Microsoft Corporation,
12/22/2019 1:00...	Run .EXE file	w32tm.exe	C:\Windows\System32\w32tm.exe	Microsoft Corporation,
12/22/2019 1:00...	Run .EXE file	cvtres.exe	C:\Windows\MICROSOFT.NET\FRAMEWORK64...	Microsoft Corporation,
12/22/2019 1:00...	Run .EXE file	csc.exe	C:\Windows\MICROSOFT.NET\FRAMEWORK64...	Microsoft Corporation,
12/22/2019 1:00...	Run .EXE file	SDIAGNHOST.EXE	C:\Windows\System32\SDIAGNHOST.EXE	Microsoft Corporation,
12/22/2019 1:00...	Task Run	sdiagschd.dll	C:\Windows\System32\sdiagschd.dll	Scheduled, \Microsof
12/22/2019 12:5...	Task Run	regidle.dll	C:\Windows\System32\regidle.dll	RegIdleBackup, \Micro
12/22/2019 12:3...	Run .EXE file	rundll32.exe	C:\Windows\System32\rundll32.exe	Microsoft Corporation,
12/22/2019 12:3...	Task Run	rundll32.exe	C:\Windows\system32\rundll32.exe	ProgramDataUpdater,
12/22/2019 12:3...	Task Run	rundll32.exe	C:\Windows\system32\rundll32.exe	Microsoft Corporation,

3. **Exportación de datos:** LastActivityView generó un archivo con un registro completo de todos los procesos activos, que se guardó para análisis forense.

https://drive.google.com/file/d/1vhRUIMAah_-UNirsQfxds7sIQ3rjVpT9/view?usp=sharing

4. Cadena de custodia

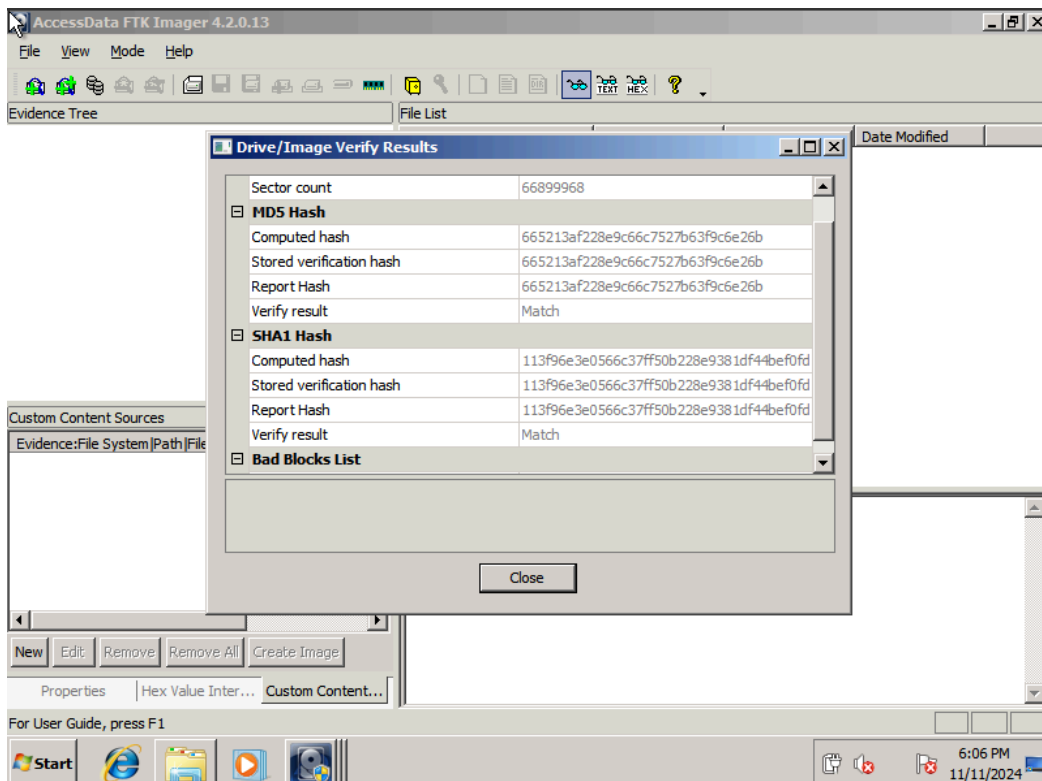
Fecha y Hora de Recolección	12/11/2024 12:15
Persona Responsable de la Recolección	Gonzalo Pulido Sánchez
Transferencias de Custodia	13/11/2024 09:15 Manuel Rivas Firma
Método de Adquisición	LastActivityView
Verificación de Integridad	MD5: dbf10b90147f57fa7741751b95b36e6b SHA1: f96eaf5f8f3eac70e401cd4a98b858d570 3a2bc6

Este procedimiento asegura que los procesos activos y las actividades sospechosas queden registrados y preservados.

- Disco

Para la adquisición del disco, se empleó **FTK Imager** con el siguiente procedimiento:

- Configuración de FTK Imager:** La herramienta se configuró para realizar una copia forense completa del disco, garantizando la integridad de los datos durante la adquisición.



2. **Captura de la imagen del disco:** FTK Imager generó varios archivos que contienen la imagen forense del disco comprometido, preservando todos los sectores y datos relevantes.

<https://drive.google.com/drive/folders/1YziS6VRfwXallrraOnKxGJ0qNU7D1n0m?usp=sharing>

3. **Verificación de integridad:** La herramienta generó un archivo **.txt** que incluye los hashes de los archivos de imagen y otra información relevante para futuras comprobaciones de integridad.

https://drive.google.com/file/d/1KrIf-088yHBRM9rk4o1dYg37ecNIBDs-/view?usp=drive_link

4. Cadena de custodia

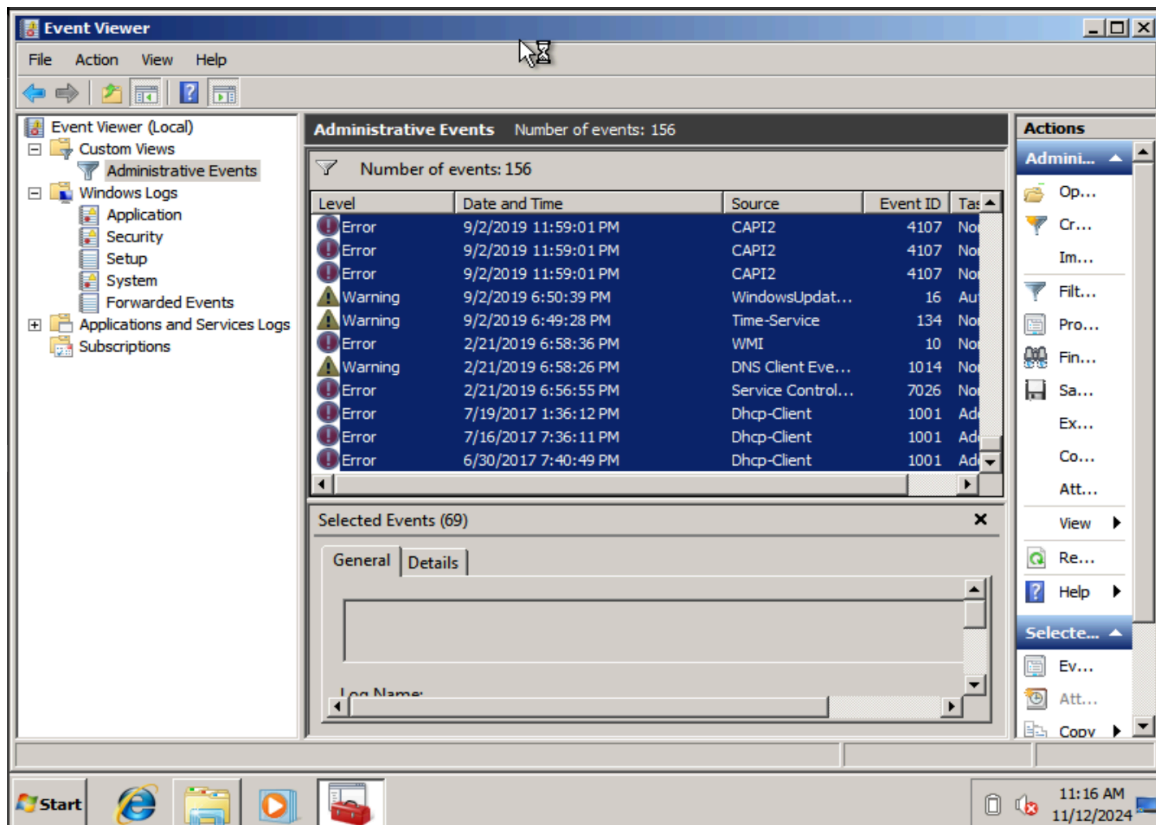
Fecha y Hora de Recolección	12/11/2024 12:30
Persona Responsable de la Recolección	Gonzalo Pulido Sánchez
Transferencias de Custodia	13/11/2024 09:30 Manuel Rivas Firma
Método de Adquisición	FTKImager
Verificación de Integridad	MD5: 665213af228e9c66c7527b63f9c6e26b SHA1: 113f96e3e0566c37ff50b228e9381df44b ef0fda

Este proceso asegura la copia exacta del disco para análisis sin riesgo de alteraciones en los datos originales.

- Logs del sistema

Para la adquisición de los logs del sistema, se utilizó la herramienta integrada de Windows, **Event Viewer**, siguiendo estos pasos:

1. **Acceso a Event Viewer:** Se utilizó Event Viewer para acceder a los registros del sistema, específicamente a las **Custom Views** (vistas personalizadas) que contienen eventos relevantes.



2. **Exportación de logs:** Se realizó la exportación de los Custom Views, guardando los eventos seleccionados en archivos de registro para conservar los detalles de actividad.

https://drive.google.com/file/d/1qXheZASfz_WwkWdFSHMLojOh2NBQVtC4/view?usp=sharing

3. Cadena de custodia

Fecha y Hora de Recolección	12/11/2024 12:45
Persona Responsable de la Recolección	Gonzalo Pulido Sánchez
Transferencias de Custodia	13/11/2024 09:45 Manuel Rivas Firma
Método de Adquisición	Event Viewer
Verificación de Integridad	MD5: 7f3ab325046ed146638c690a64fc1b3c SHA1: 7dbbf4ca695ddc0bd577debc73bd3cd8c 73dfd40

Este procedimiento garantiza la preservación de los eventos críticos del sistema para su análisis forense.

- Topología

Para la adquisición de la topología de red, se utilizó el comando **ipconfig** con el siguiente procedimiento:

1. **Ejecución del comando:** Se ejecutó **ipconfig** en la máquina comprometida para obtener información detallada sobre las interfaces de red, direcciones IP, subredes y puertas de enlace.
2. **Guardado de los resultados:** Los datos obtenidos del comando se guardaron en un archivo de texto (.txt) para su conservación y análisis.

https://drive.google.com/file/d/1Frg_Ty_av2ayonYi1nQBKQym2B6mV9Qt/view?usp=drive_link

3. Cadena de custodia

Fecha y Hora de Recolección	12/11/2024 13:00
Persona Responsable de la Recolección	Gonzalo Pulido Sánchez
Transferencias de Custodia	13/11/2024 10:00 Manuel Rivas Firma
Método de Adquisición	ipconfig
Verificación de Integridad	MD5: 1215b0cf10cea0be14c2193a9f7ba5f4 SHA1: 574f77b6b2949f0ddd01a89f1d5917ebd bc41d60

Este proceso asegura que la configuración de la red quede registrada de forma precisa para su posterior análisis forense.

[Enlace a carpeta compartida de adquisición](#)