

Informe de Recolección y Almacenamiento de Evidencias

Investigador:

Yeray Almoguera Gonzalez

Fecha:

11 del Octubre de 2024

Número de Caso:

001

Índice

| | |
|---|-----------|
| 1. Recolección de evidencias..... | 3 |
| 1.1 Preparación del entorno de adquisición..... | 3 |
| 1.2 Aseguramiento de la escena..... | 4 |
| 1.3 Recolección de datos volátiles..... | 5 |
| Memoria RAM..... | 5 |
| Disco duro..... | 7 |
| Procesos en ejecución..... | 10 |
| Información del sistema..... | 12 |
| Tabla de enrutamiento..... | 14 |
| Caché DNS..... | 16 |
| Tabla ARP..... | 18 |
| Topología de red..... | 20 |
| 2. Cadena de custodia..... | 22 |
| 3. Almacenamiento de la evidencia..... | 23 |
| 4. Metodología aplicada..... | 24 |

1. Recolección de evidencias

Siguiendo la metodología establecida por nuestra empresa, se procedió a la adquisición completa de la máquina comprometida del departamento de IT. A continuación, se detallan los pasos seguidos para cada evidencia recolectada

1.1 Preparación del entorno de adquisición

Para garantizar la integridad de las evidencias y evitar cualquier contaminación, se ha establecido un entorno de adquisición controlado y seguro. Este proceso incluyó los siguientes pasos:

Se adquirió un disco duro nuevo, sin uso previo, con capacidad suficiente para almacenar todas las evidencias recolectadas. Se preparó un ordenador dedicado exclusivamente a la realización de la adquisición, asegurándose de que no tuviera conexión a internet ni software no esencial instalado.

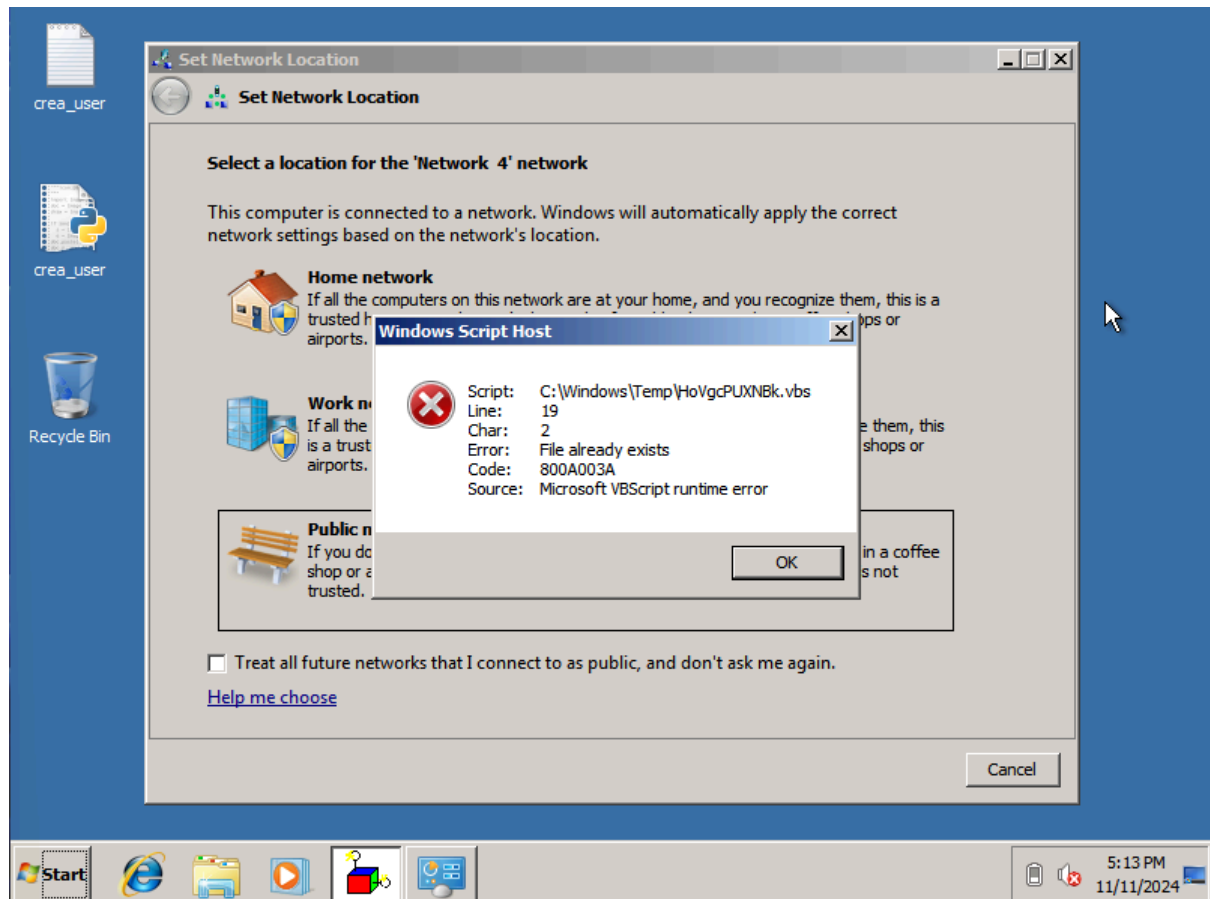
En cuanto a la sanitización del hardware, el disco duro nuevo fue sometido a un proceso de sanitización completa mediante herramientas forenses certificadas para eliminar cualquier dato residual que pudiera estar presente de fábrica. Además, el ordenador dedicado fue formateado e instalado con un sistema operativo limpio, configurado específicamente para llevar a cabo tareas forenses.

La configuración del entorno incluyó la creación de una carpeta compartida en el disco duro previamente sanitizado. Los permisos de acceso a esta carpeta se establecieron de manera que solo los investigadores autorizados pudieran acceder a ella, garantizando la seguridad de la información. Además, se habilitó un registro de auditoría para todas las operaciones realizadas en la carpeta compartida.

Por último, se llevaron a cabo verificaciones para asegurar que la carpeta compartida funcionara correctamente y que los permisos de acceso estuvieran configurados de forma adecuada. También se comprobó que el entorno estuviera completamente aislado de cualquier red externa, garantizando la integridad y seguridad del proceso.

1.2 Aseguramiento de la escena

Antes de iniciar la recolección, se aseguró la escena del incidente. Se tomaron fotografías del entorno del equipo y se documentó la hora y fecha del sistema. Se decidió no desconectar el equipo de la red ni de la alimentación eléctrica para preservar datos volátiles cruciales para la investigación.



Fotografía de cómo se encontró el ordenador antes de la intervención.

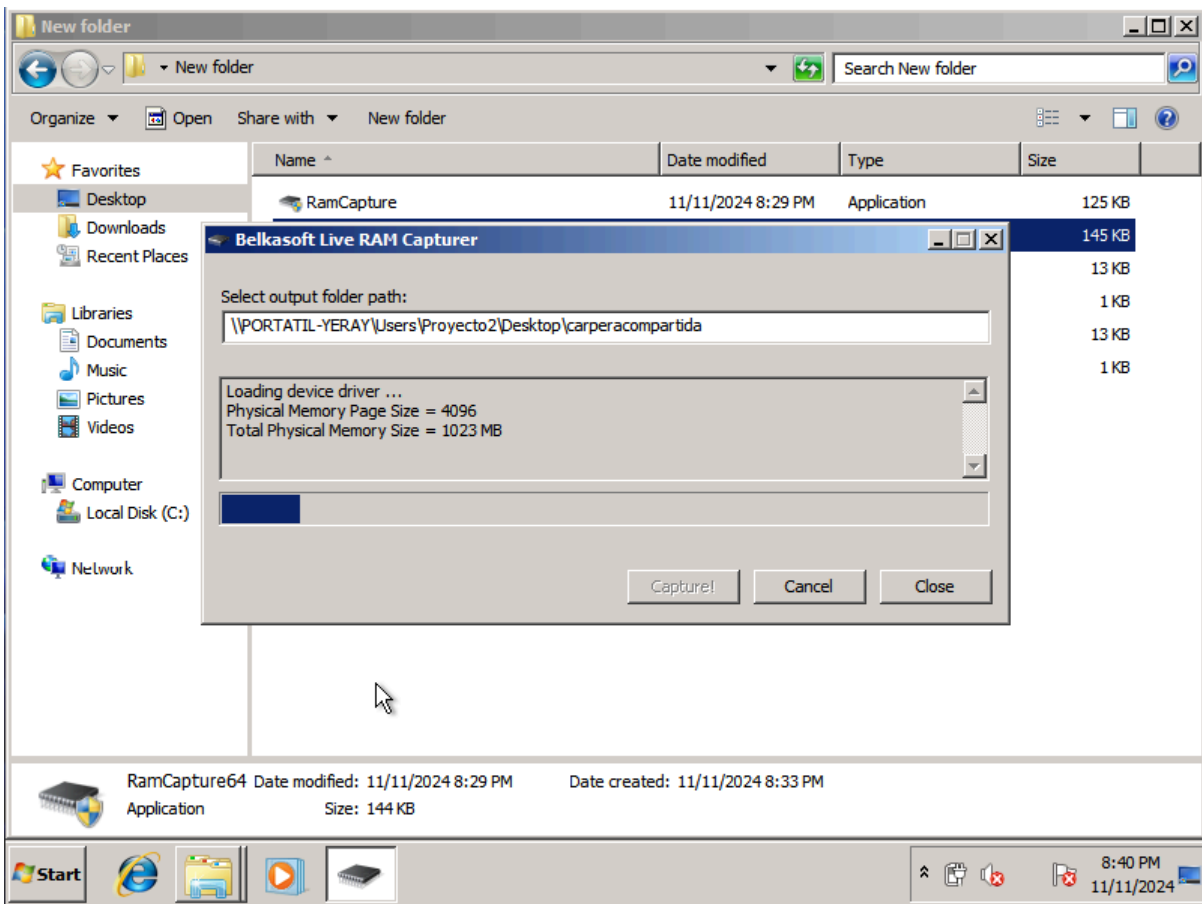
1.3 Recolección de datos volátiles

Memoria RAM

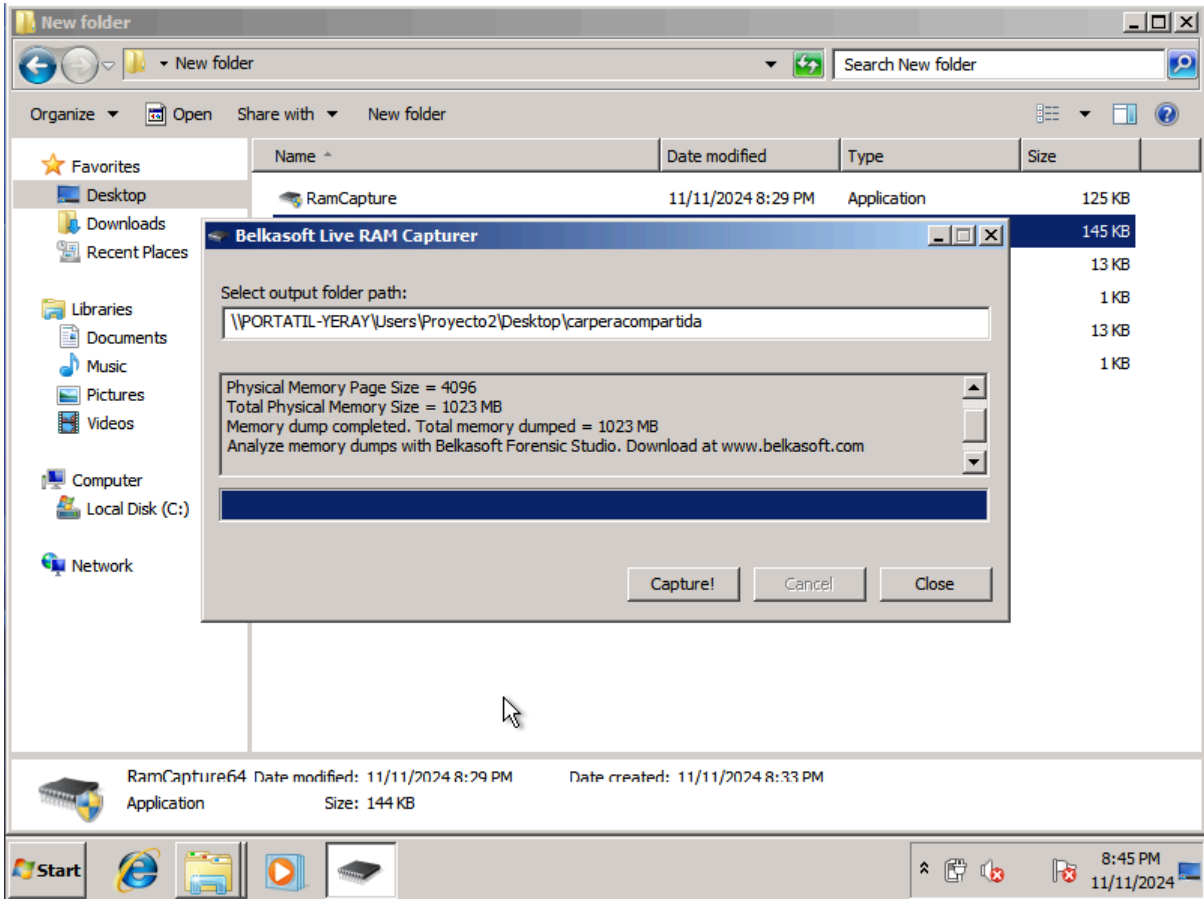
| | |
|-------------------------|---|
| Herramienta usada | Belkasoft Live RAM Capturer |
| Enlace a la Herramienta | https://belkasoft.com/ram-capturer |

Proceso de adquisición:

Se realizó la adquisición de la memoria RAM utilizando el programa Belkasoft Live RAM Capturer, ejecutando con privilegios de administrador desde la máquina afectada. Para garantizar la integridad de los datos, se accedió a la carpeta compartida previamente configurada en el disco duro forense limpio, estableciendo esta carpeta como destino para almacenar la captura de la memoria.



Tras completar el proceso de adquisición de la memoria RAM, se verificó el éxito de la operación. Para garantizar la integridad de los datos capturados, se procedió a calcular el valor hash del archivo generado por la aplicación Belkasoft Live RAM Capturer. Este procedimiento de verificación es crucial para establecer una línea base de autenticidad de la evidencia digital, permitiendo detectar cualquier alteración posterior en los datos adquiridos.



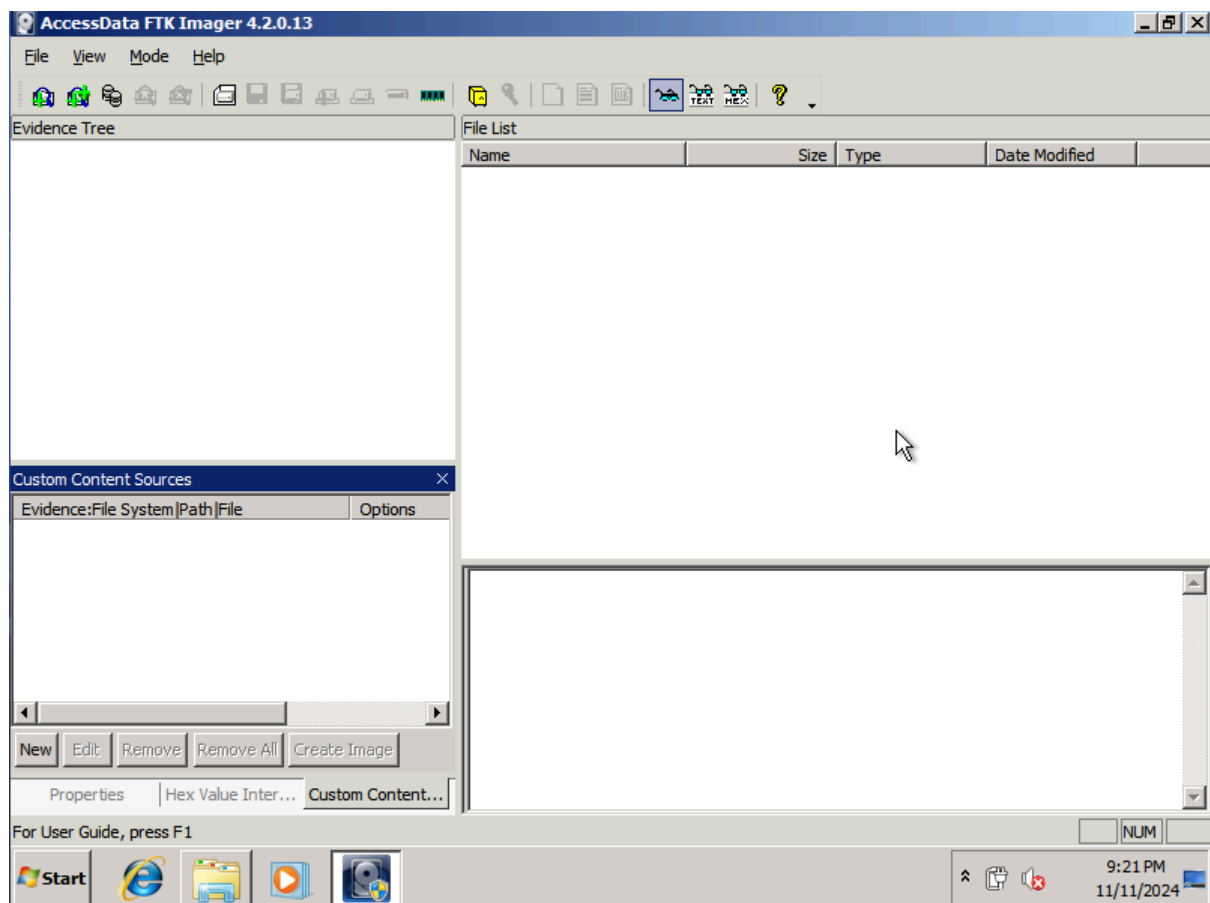
| | |
|----------------------------|--|
| Técnico Responsable | Yeray Almoguera González |
| Ubicación física | Disco Duro #05 |
| Algoritmos hash utilizados | SHA-256 |
| Valores hash generados | 1A35257B0774DA1DFA8B1288ED91F0A8B1569 86793FD3624F42D7AECA6466C6E |
| Fecha de adquisición | 11/11/2024 |
| Hora de adquisición | 8:45 PM |

Disco duro

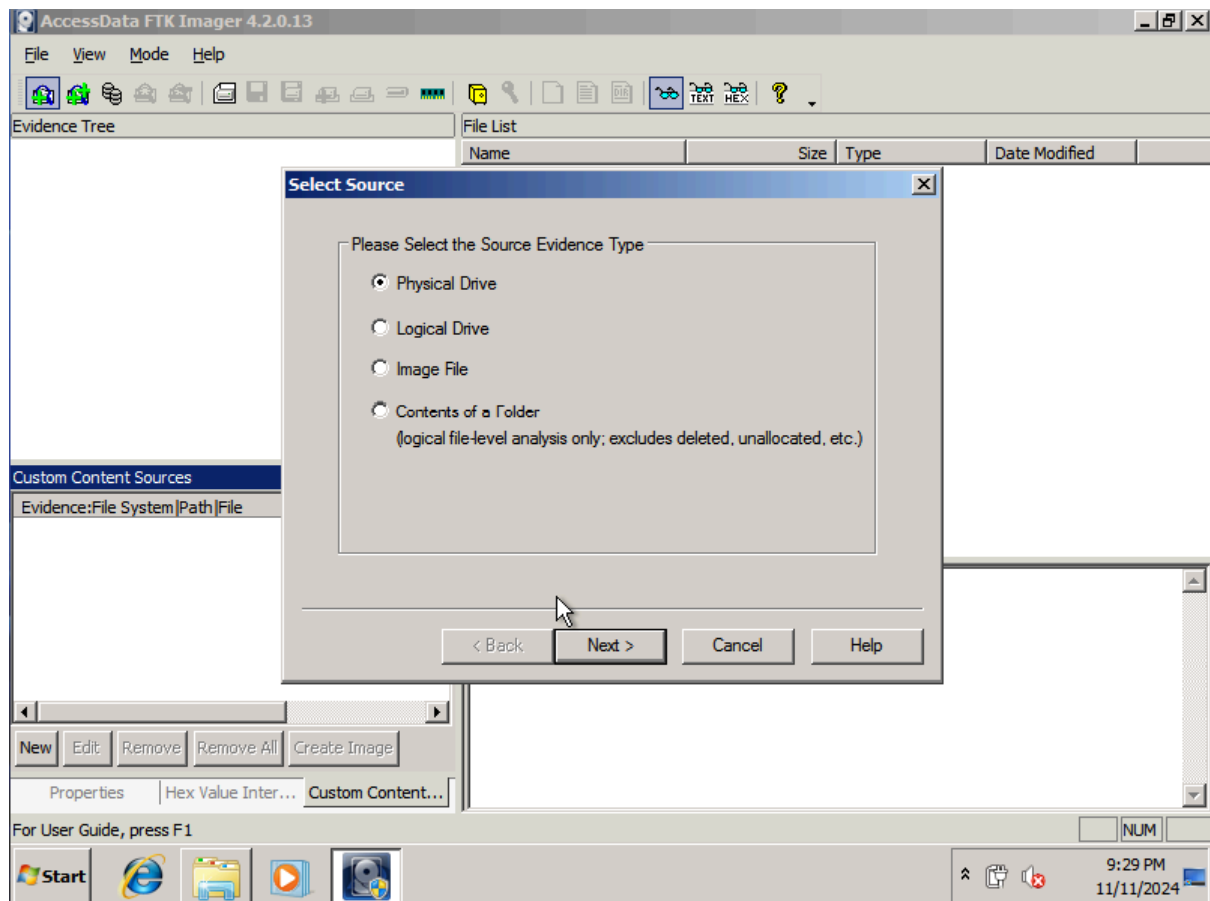
| | |
|-------------------------|---|
| Herramienta usada | AccessData FTK Imager |
| Enlace a la Herramienta | https://www.exterro.com/ |

Proceso de adquisición:

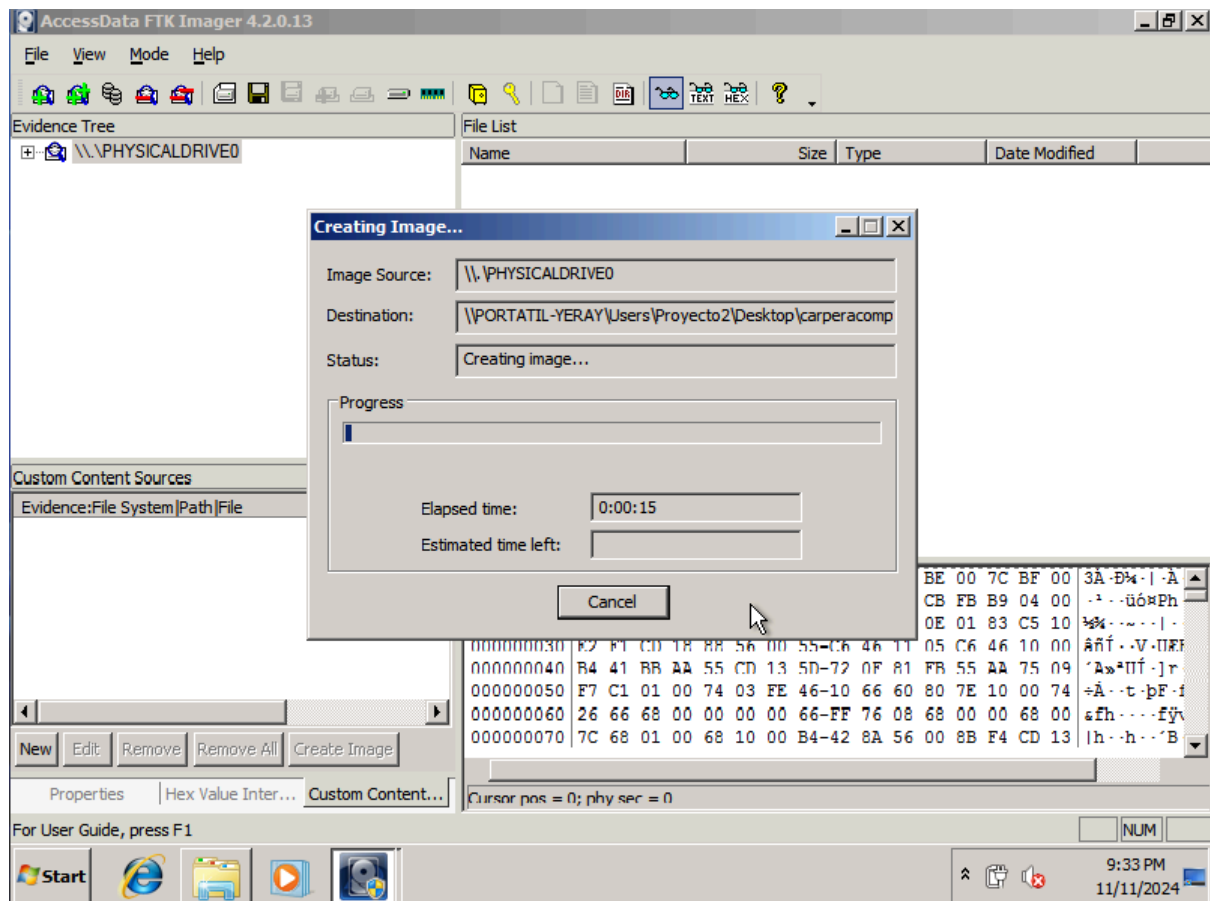
Siguiendo el protocolo establecido, se procedió a ejecutar nuevamente el programa de adquisición FTK desde la carpeta compartida, utilizando credenciales con privilegios de administrador. Esta acción se realizó para garantizar el acceso completo a todos los recursos del sistema necesarios para una captura exhaustiva de datos.



Para llevar a cabo la adquisición forense del disco duro, se utilizó la herramienta FTK Imager, siguiendo un protocolo riguroso para garantizar la integridad de los datos. El proceso se inició seleccionando la opción "Physical Drive" en la interfaz del software, lo cual permite realizar una captura bit a bit completa del disco. Esta metodología asegura que se obtenga una imagen forense exacta de todo el contenido del dispositivo, incluyendo particiones, espacio no asignado y metadatos del sistema de archivos.



Una vez identificado el disco duro objetivo, se procedió a seleccionar la totalidad del dispositivo para realizar una adquisición forense completa. Este enfoque garantiza la captura íntegra de todos los datos almacenados, incluyendo particiones visibles y ocultas, espacio no asignado, y metadatos del sistema de archivos. La adquisición del disco completo es crucial para asegurar que no se omita ninguna información potencialmente relevante para la investigación, permitiendo un análisis exhaustivo y preservando la integridad de la evidencia digital.



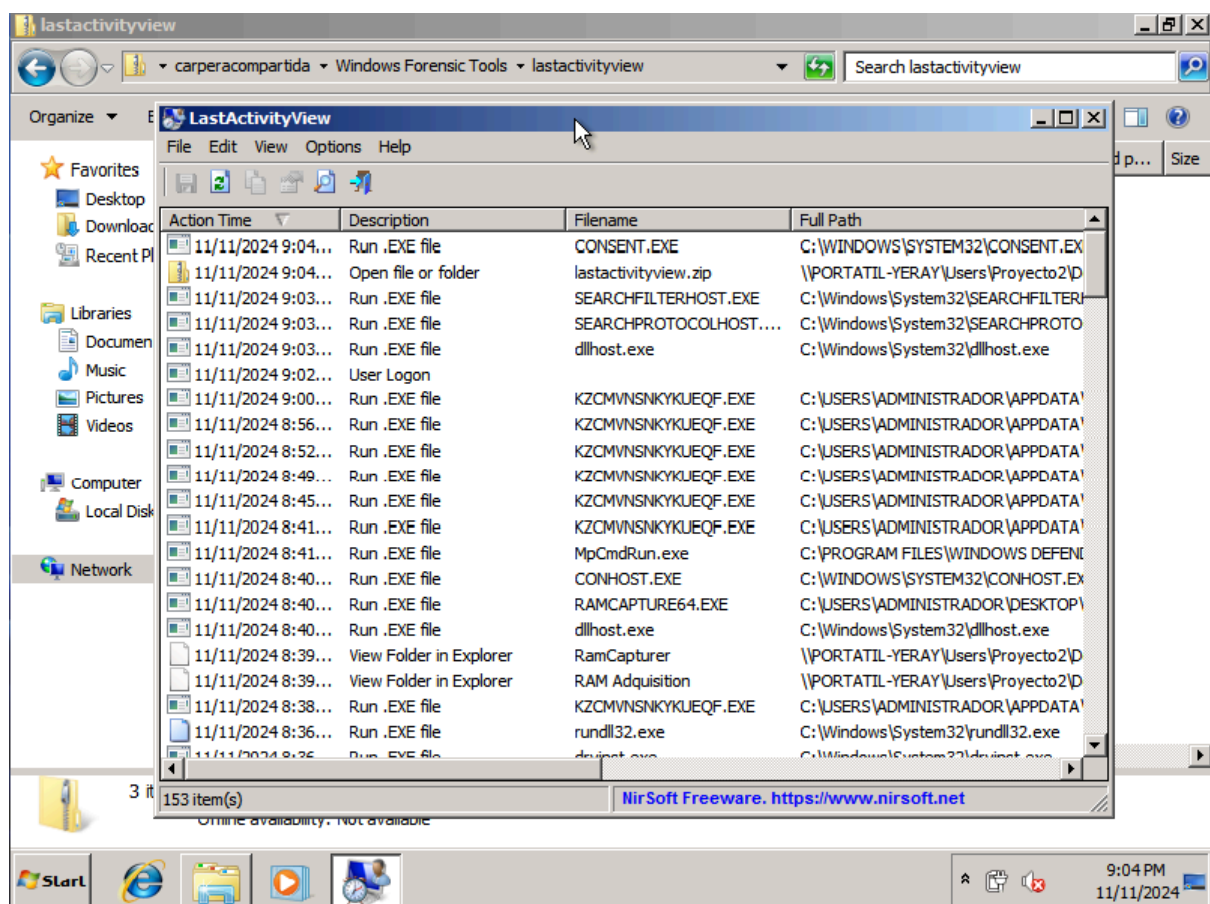
| | |
|-----------------------------------|---|
| Técnico Responsable | Yeray Almoguera González |
| Ubicación física | Disco Duro #05 |
| Algoritmos hash utilizados | MD5, SHA-1 |
| Valores hash generados | MD5 checksum: 24827b0922742e01633ae49c7c1ff3f6 |
| Valores hash generados | SHA-1 checksum: 1c2ca8d6d4a2d82f0bf2fba5f3bbe84c766015a6 |
| Fecha de adquisición | 11/11/2024 |
| Hora de adquisición | 9:33 PM |

Procesos en ejecución

| | |
|-------------------------|---|
| Herramienta usada | Last Activity View |
| Enlace a la Herramienta | https://www.nirsoft.net/ |

Proceso de adquisición:

Para la adquisición de los procesos que se ejecutaron en el ordenador, usamos la aplicación Last Activity View. Para este proceso, también ejecutamos la aplicación desde la carpeta compartida.



| | |
|-----------------------------------|--|
| Técnico Responsable | Yeray Almoguera González |
| Ubicación física | Disco Duro #05 |
| Algoritmos hash utilizados | SHA-256 |
| Valores hash generados | 521F4D9470B855ED351536A2C090BDB6712621 BD318FDCE9AB112EBAD15CAE04 |
| Fecha de adquisición | 11/11/2024 |
| Hora de adquisición | 09:44 PM |

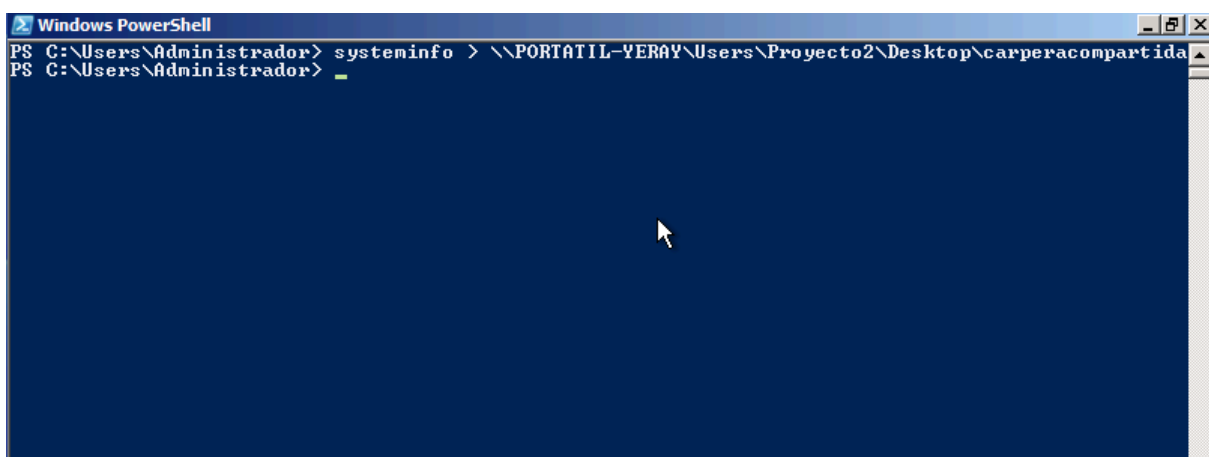
Información del sistema

| | |
|--------------------------|--------------------------------------|
| Herramienta usada | PowerShell |
| Comando Usado | systeminfo > ruta_carpera_compartida |

Para obtener la información del sistema comprometido, se siguió un protocolo riguroso que garantiza la integridad de los datos. Se abrió una sesión de PowerShell con privilegios elevados de administrador en el equipo afectado. Este paso es crucial para asegurar el acceso completo a la información del sistema operativo y hardware.

Se ejecutó el comando `systeminfo > \\ruta_de_la_carpeta_compartida`, redirigiendo la salida a un archivo en la carpeta de evidencias previamente establecida. Este comando captura una amplia gama de datos sobre el sistema, incluyendo la versión del sistema operativo, arquitectura del procesador, memoria instalada, parches de seguridad aplicados y otra información relevante sobre la configuración del hardware y software.

Inmediatamente después de la captura, se verificó la integridad del archivo generado calculando su valor hash. Este proceso de verificación es esencial para establecer una línea base de autenticidad de la evidencia digital, permitiendo detectar cualquier alteración posterior en los datos adquiridos.



```
Windows PowerShell
PS C:\Users\Administrador> systeminfo > \\PORTÁTIL-YERÁY\Users\Proyecto2\Desktop\carperacompartida
PS C:\Users\Administrador>
```

| | |
|-----------------------------------|--|
| Técnico Responsable | Yeray Almoguera González |
| Ubicación física | Disco Duro #05 |
| Algoritmos hash utilizados | SHA-256 |
| Valores hash generados | 0F1A4792ADA24068A75957C5A48899771145E3 AC95D6B0C5AACF8DE28C9F7B35 |
| Fecha de adquisición | 11/11/2024 |
| Hora de adquisición | 11:13 PM |

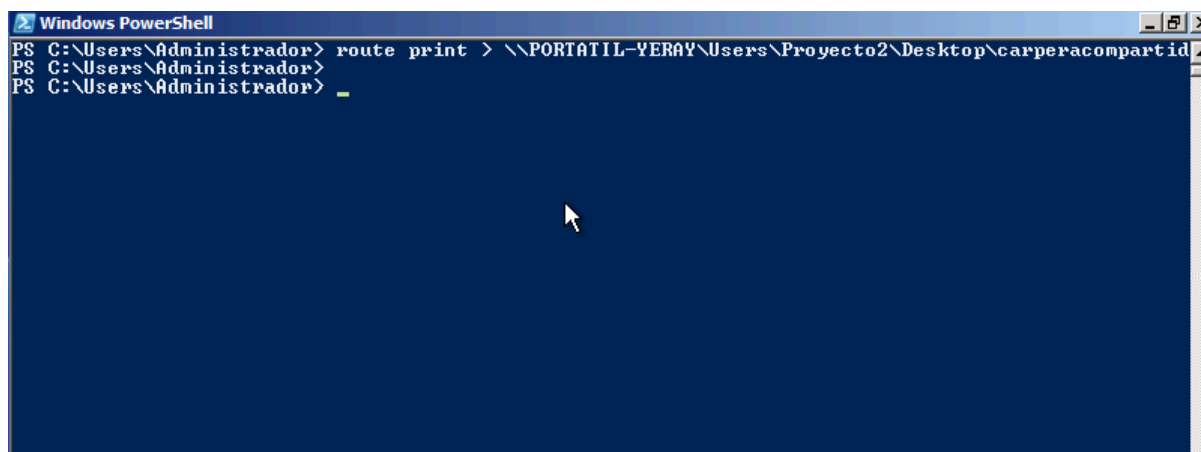
Tabla de enrutamiento

| | |
|--------------------------|---|
| Herramienta usada | PowerShell |
| Comando Usado | route print > ruta_de_la_carpeta_compartida |

Continuando con el proceso de adquisición de evidencias volátiles, el siguiente paso fue obtener la información del sistema comprometido. Utilizando la sesión de PowerShell con privilegios elevados de administrador previamente abierta, se procedió a ejecutar el comando `systeminfo > \\ruta_de_la_carpeta_compartida`.

Este comando captura una amplia gama de datos sobre el sistema, incluyendo la versión del sistema operativo, arquitectura del procesador, memoria instalada, parches de seguridad aplicados y otra información relevante sobre la configuración del hardware y software. Toda esta información se redirigió a un archivo en la carpeta de evidencias establecida.

Como en los casos anteriores, se realizó la verificación de integridad del archivo generado mediante el cálculo de su valor hash. Esta información del sistema es crucial para proporcionar un contexto completo del entorno en el que se produjo el incidente, lo que puede ayudar a identificar posibles vulnerabilidades o configuraciones que pudieran haber sido explotadas.



```
Windows PowerShell
PS C:\Users\Administrador> route print > \\PORTATIL-YERAY\Users\Proyecto2\Desktop\carperacompartida
PS C:\Users\Administrador>
PS C:\Users\Administrador> _
```

| | |
|-----------------------------------|--|
| Técnico Responsable | Yeray Almoguera González |
| Ubicación física | Disco Duro #05 |
| Algoritmos hash utilizados | SHA-256 |
| Valores hash generados | D553186CAE29A433DAFAC69F78B3A4CA3AC0 CD455E783DF0DDA63D71E24E42D5 |
| Fecha de adquisición | 11/11/2024 |
| Hora de adquisición | 11:15 PM |

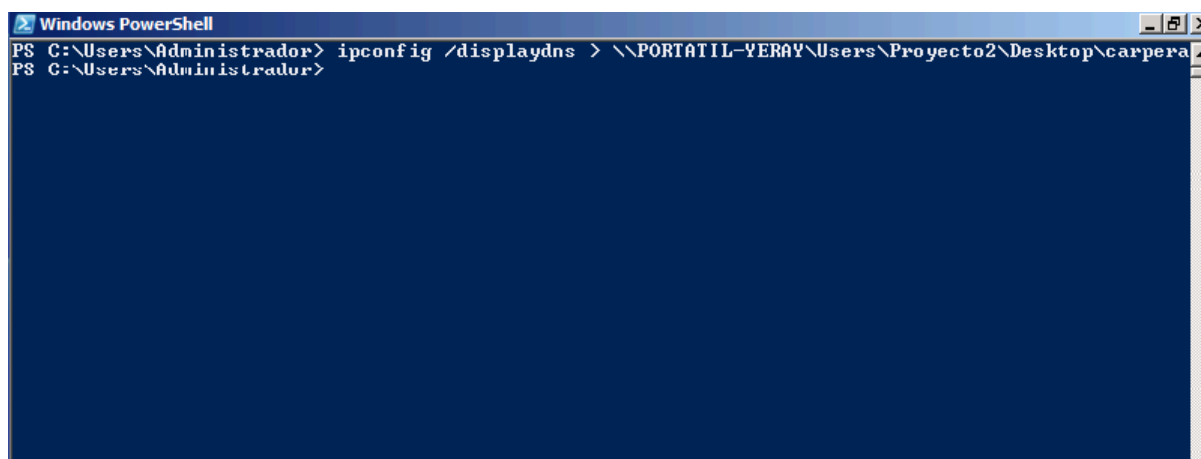
Caché DNS

| | |
|--------------------------|--|
| Herramienta usada | PowerShell |
| Comando Usado | ipconfig /displaydns > ruta_carpera_compartida |

Siguiendo con el proceso de adquisición de evidencias volátiles, el siguiente paso fue obtener la caché DNS del sistema comprometido. Utilizando la misma sesión de PowerShell con privilegios elevados, se procedió a ejecutar el comando `ipconfig /displaydns > \\ruta_de_la_carpeta_compartida`.

Este comando captura el contenido íntegro de la caché DNS, incluyendo todas las resoluciones de nombres de dominio recientes almacenadas en el sistema en el momento de la adquisición. La información obtenida se redirigió a un archivo en la carpeta de evidencias establecida.

Como en los pasos anteriores, se realizó la verificación de integridad del archivo generado mediante el cálculo de su valor hash. La caché DNS es particularmente valiosa en la investigación forense, ya que puede revelar conexiones recientes a dominios potencialmente maliciosos, ayudando a identificar posibles comunicaciones con servidores de comando y control o intentos de exfiltración de datos.



```
Windows PowerShell
PS C:\Users\Administrador> ipconfig /displaydns > \\PORTATIL-YERAY\Users\Proyecto2\Desktop\carpera
PS C:\Users\Administrador>
```


| | |
|-----------------------------------|--|
| Técnico Responsable | Yeray Almoguera González |
| Ubicación física | Disco Duro #05 |
| Algoritmos hash utilizados | SHA-256 |
| Valores hash generados | 715E2ABD18EE2D75710E89CC82D5B3900B331 54E92DE28E514970303839B775C |
| Fecha de adquisición | 11/11/2024 |
| Hora de adquisición | 11:19 PM |

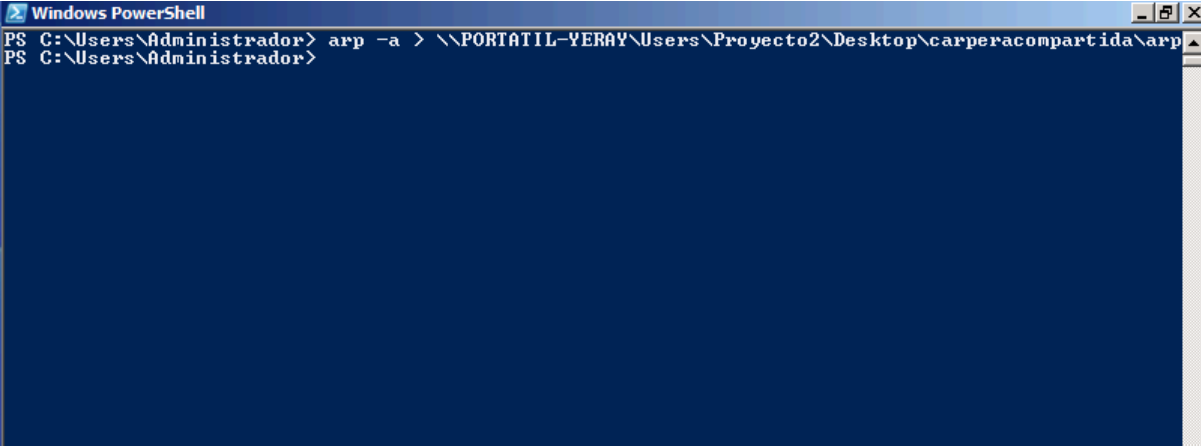
Tabla ARP

| | |
|--------------------------|----------------------------------|
| Herramienta usada | PowerShell |
| Comando Usado | arp -a > ruta_carpera_compartida |

Continuando con el proceso de adquisición de evidencias volátiles, se procedió a capturar la tabla ARP del sistema comprometido. Para ello, se utilizó la misma sesión de PowerShell con privilegios elevados de administrador previamente abierta.

Se ejecutó el comando `arp -a > \\ruta_de_la_carpeta_compartida`, redirigiendo la salida a un archivo en la carpeta de evidencias designada. Este comando captura la tabla ARP completa, incluyendo todas las asociaciones entre direcciones IP y direcciones MAC conocidas por el sistema en el momento de la adquisición.

Al igual que con las evidencias anteriores, inmediatamente después de la captura, se verificó la integridad del archivo generado calculando su valor hash. La adquisición de la tabla ARP es crucial en la investigación forense, ya que puede revelar dispositivos conectados a la red local y potencialmente identificar equipos no autorizados o sospechosos que hayan interactuado con el sistema comprometido.



```
Windows PowerShell
PS C:\Users\Administrador> arp -a > \\PORTATIL-YERAY\Users\Proyecto2\Desktop\carperacompartida\arp
PS C:\Users\Administrador>
```

| | |
|-----------------------------------|--|
| Técnico Responsable | Yeray Almoguera González |
| Ubicación física | Disco Duro #05 |
| Algoritmos hash utilizados | SHA-256 |
| Valores hash generados | DA78A7C3F77AAFBFA8D9D148FFBA62E08E87 3D08E958CF15D1C8E91EE6682963 |
| Fecha de adquisición | 11/11/2024 |
| Hora de adquisición | 11:30 PM |

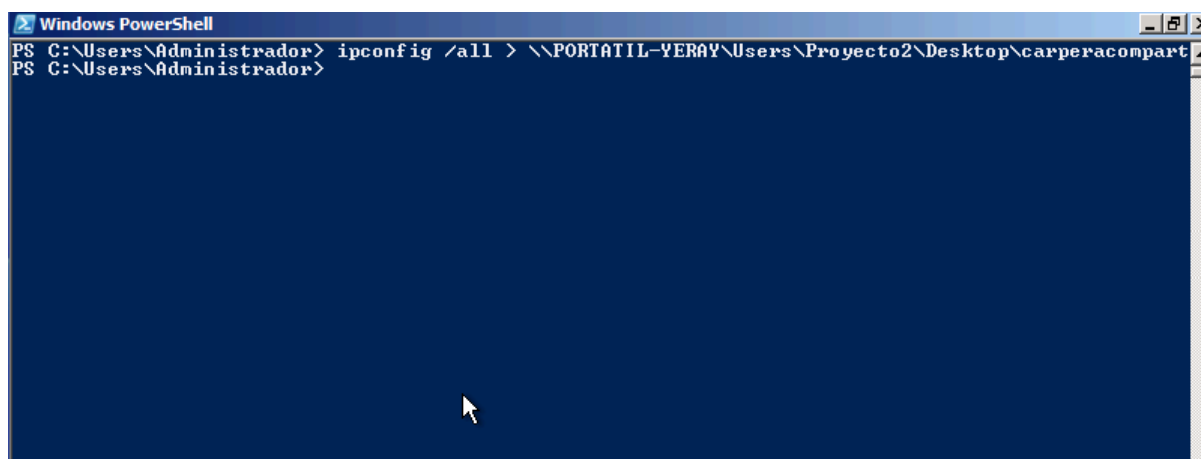
Topología de red

| | |
|--------------------------|---|
| Herramienta usada | PowerShell |
| Comando Usado | ipconfig /all > ruta_carpera_compartida |

Continuando con el proceso de adquisición de evidencias volátiles, el siguiente paso fue capturar la topología de red del sistema comprometido. Utilizando la misma sesión de PowerShell con privilegios elevados de administrador, se procedió a ejecutar el comando `ipconfig /all > \ruta_de_la_carpeta_compartida`.

Este comando captura una imagen completa de la configuración de red del equipo, incluyendo direcciones IP, máscaras de subred, puertas de enlace predeterminadas, servidores DNS, y otra información relevante sobre las interfaces de red activas en el sistema.

Como en los casos anteriores, inmediatamente después de la captura, se verificó la integridad del archivo generado calculando su valor hash. La adquisición de la topología de red es esencial en la investigación forense, ya que proporciona una visión detallada de cómo el sistema estaba conectado a la red en el momento del incidente. Esta información puede ser crucial para identificar posibles vectores de ataque, conexiones no autorizadas, o configuraciones de red sospechosas que puedan haber facilitado el compromiso del sistema.



```
Windows PowerShell
PS C:\Users\Administrador> ipconfig /all > \\PORTATIL-YERAY\Users\Proyecto2\Desktop\carperacompart
PS C:\Users\Administrador>
```

| | |
|-----------------------------------|--|
| Técnico Responsable | Yeray Almoguera González |
| Ubicación física | Disco Duro #05 |
| Algoritmos hash utilizados | SHA-256 |
| Valores hash generados | 36D50EA330285454CDC551D454C05BA2AC23E 3897979845C894E963F47824185 |
| Fecha de adquisición | 11/11/2024 |
| Hora de adquisición | 11:32 PM |

2. Cadena de custodia

| Etapa | Descripción | Detalles |
|-----------------------|---|--|
| Descubrimiento | Detección inicial del incidente | <ul style="list-style-type: none">- Fecha: 10/11/2024- Hora: 6:00 PM- Detectado por: Equipo de monitorización del CSIRT- Método de detección: IDS |
| Notificación | Comunicación del incidente | <ul style="list-style-type: none">- Fecha: 11/11/2024- Hora: 5:00 PM- Notificado por: Andres Pérez Jimenez- Notificado a: Yeray Almoguera Gonzalez |
| Recolección | Proceso de recolección de evidencias | <ul style="list-style-type: none">- Fecha: 11/11/2024- Hora de inicio: 5:13 PM- Hora de finalización: 11:32 PM- Realizado por: Yeray Almoguera Gonzalez |
| Empaquetado | Preparación de evidencias para transporte | <ul style="list-style-type: none">- Realizado por: Yeray Almoguera Gonzalez- Método: Bolsas antiestáticas- Etiquetado: Etiqueta del disco duro #05 |
| Transporte | Traslado de evidencias al laboratorio | <ul style="list-style-type: none">- Fecha y hora de salida: 12/11/2024 7:00 AM- Fecha y hora de llegada: 12/11/2024 7:30 AM- Transportado por: Ruben Alcedo Perez- Método de transporte: Vehículo forense |
| Custodia | Almacenamiento seguro de evidencias | <ul style="list-style-type: none">- Ubicación: Laboratorio forense de la empresa- Custodio responsable: Marty McFly- Método de almacenamiento: Caja Fuerte |

3. Almacenamiento de la evidencia

Método de Almacenamiento:

Las evidencias digitales recolectadas se han almacenado en discos duros forenses designados específicamente para este propósito. Estos dispositivos han sido verificados y documentados antes de su uso, garantizando que estén libres de datos previos y aptos para la preservación de evidencias. Este proceso asegura un entorno adecuado para la preservación de los datos.

Ubicación y Seguridad Física:

Los discos duros que contienen las evidencias se encuentran resguardados en una caja fuerte ubicada en el laboratorio forense de la empresa. Esta caja fuerte cumple con las normativas de seguridad física y cuenta con acceso restringido a personal autorizado. Las interacciones con la caja fuerte son monitorizadas mediante un sistema de videovigilancia y un registro de acceso con marcas de tiempo para mantener un control estricto.

Protección y Garantía de Integridad:

Para proteger la integridad de las evidencias, se han calculado y documentado los hashes criptográficos de cada archivo utilizando el algoritmo SHA-256 o SHA-1 y MD5. Estos hashes permiten verificar en cualquier momento que no se ha producido ninguna alteración en los datos. Los valores hash se almacenan junto con la documentación detallada de la evidencia, y se mantienen copias de seguridad en ubicaciones seguras para mayor protección.

4. Metodología aplicada

Asegurar la escena: Se documentó el estado inicial del equipo y su entorno.

Identificar y recolectar evidencias: Se priorizó la recolección de datos volátiles antes de proceder con los menos volátiles.

Preservar las evidencias: Se siguió una estricta cadena de custodia y se utilizaron métodos forenses para la adquisición de datos.

Analizar las evidencias: Pendiente de realizar en la siguiente fase de la investigación.

Redactar informes: Este documento forma parte de la documentación inicial del proceso de recolección.