

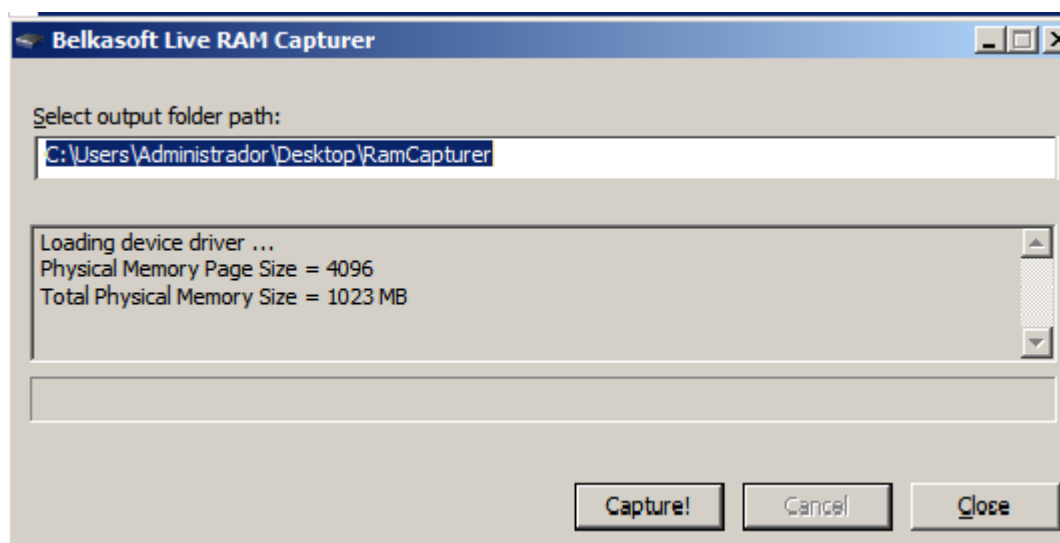
INCIDENT INVESTIGATION



1. MEMORIA VOLÁTIL:.....	2
2. MEMORIA NO VOLÁTIL:.....	2
3. ARCHIVOS TEMPORALES.....	3
4. TRIAJE.....	5
5. COMANDO ROUTE PRINT.....	6
6. PROTOCOLO ARP.....	7
8. ACTA DE ADQUISICIÓN DE EVIDENCIAS DIGITALES:.....	8
9. CADENA DE CUSTODIA:.....	11

1.MEMORIA VOLÁTIL:

Para la adquisición de la memoria volátil, hemos utilizado la herramienta RAM Capture, diseñada específicamente para capturar el contenido de la memoria RAM en tiempo real. Este proceso es fundamental para obtener información que solo existe temporalmente en el sistema y que se pierde al apagar el equipo. Al capturar la RAM, se obtiene un archivo que contiene toda la información almacenada en ese momento. Posteriormente, se generó un hash de este archivo para asegurar su integridad y garantizar que no se altera en futuras etapas de análisis.



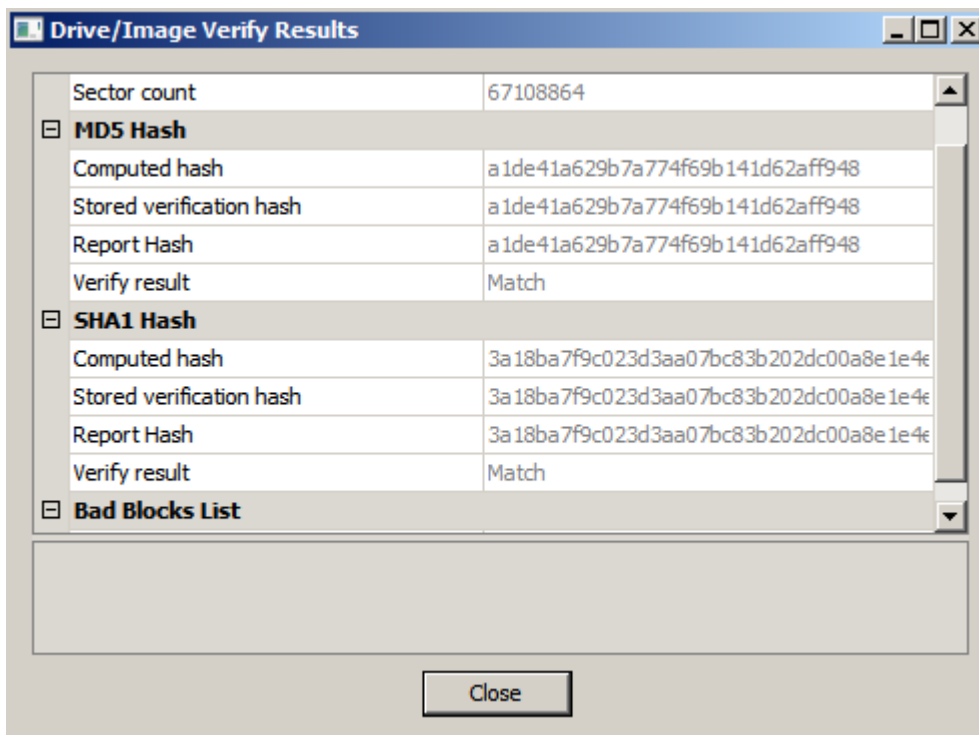
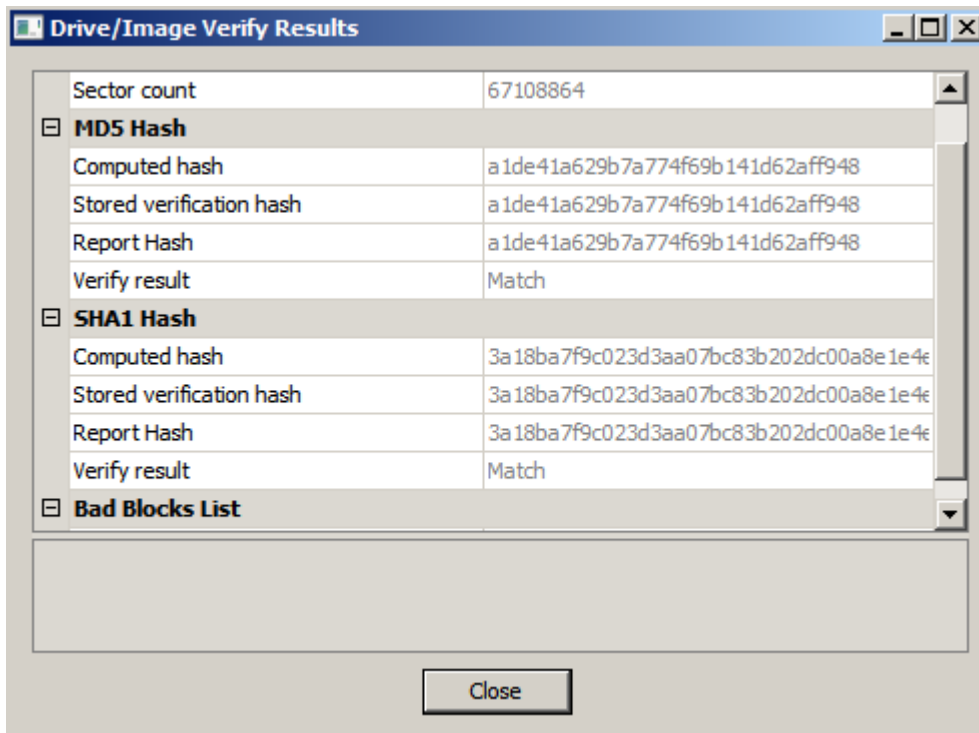
```
C:\Users\Administrador>certutil -hashfile \\192.168.0.199\CarpetaCompartida\MemoriaRAM\20241111.mem MD5
MD5 hash of file \\192.168.0.199\CarpetaCompartida\MemoriaRAM\20241111.mem:
8b cf 8e 5a 0d e6 0e 6e ab 75 87 c9 e1 00 5e e3
CertUtil: -hashfile command completed successfully.

C:\Users\Administrador>certutil -hashfile \\192.168.0.199\CarpetaCompartida\MemoriaRAM\20241111.mem SHA1
SHA1 hash of file \\192.168.0.199\CarpetaCompartida\MemoriaRAM\20241111.mem:
24 94 ba df 7c 74 0b d1 b9 22 23 cb d8 64 a2 9b 69 96 f4 84
CertUtil: -hashfile command completed successfully.
```

[Enlace Adquisición RAM](#)

2.MEMORIA NO VOLÁTIL:

Para la memoria no volátil, como el disco duro, se utilizó FTK Imager. Esta herramienta permite crear una imagen forense del disco, copiando fielmente todos los datos sin alterarlos. Durante el proceso, FTK Imager genera un hash de la imagen adquirida, que actúa como una huella digital del disco en el momento de la captura. Este hash es esencial para verificar en cualquier momento que la evidencia no ha sido modificada y conserva su autenticidad original.

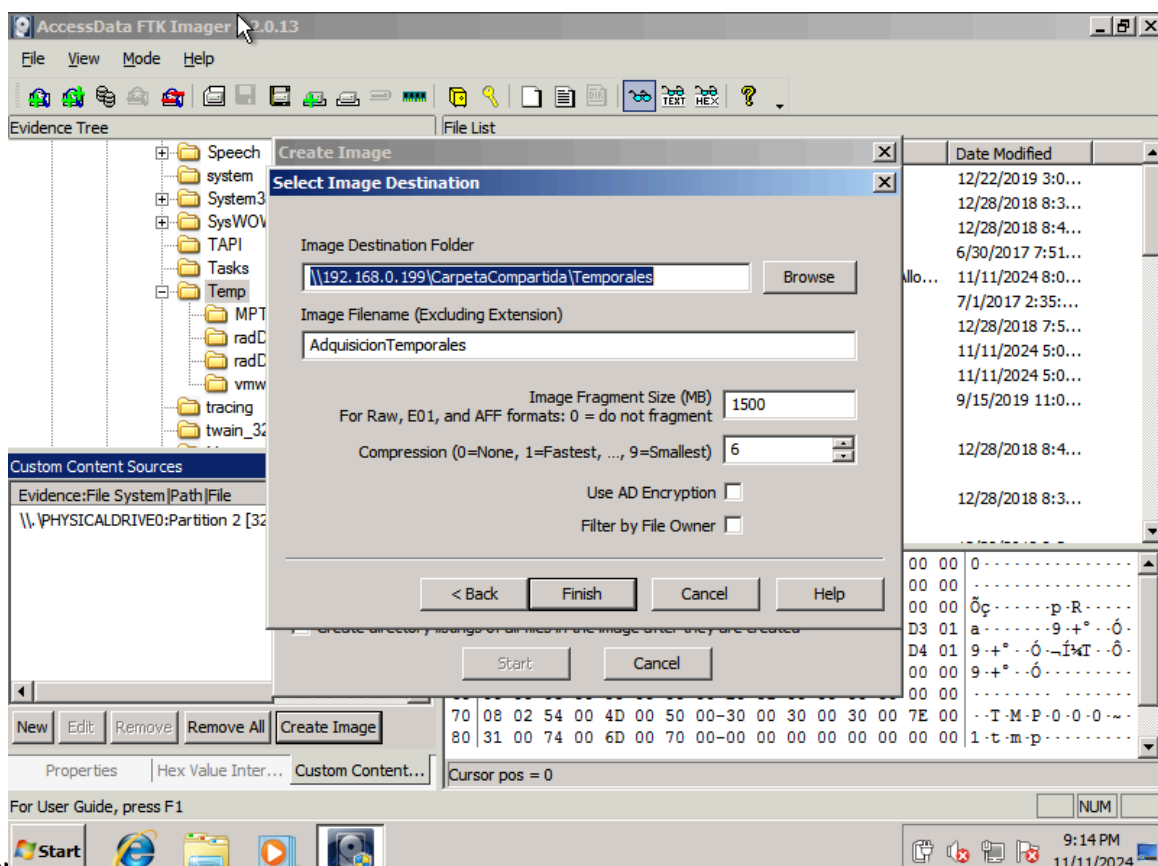
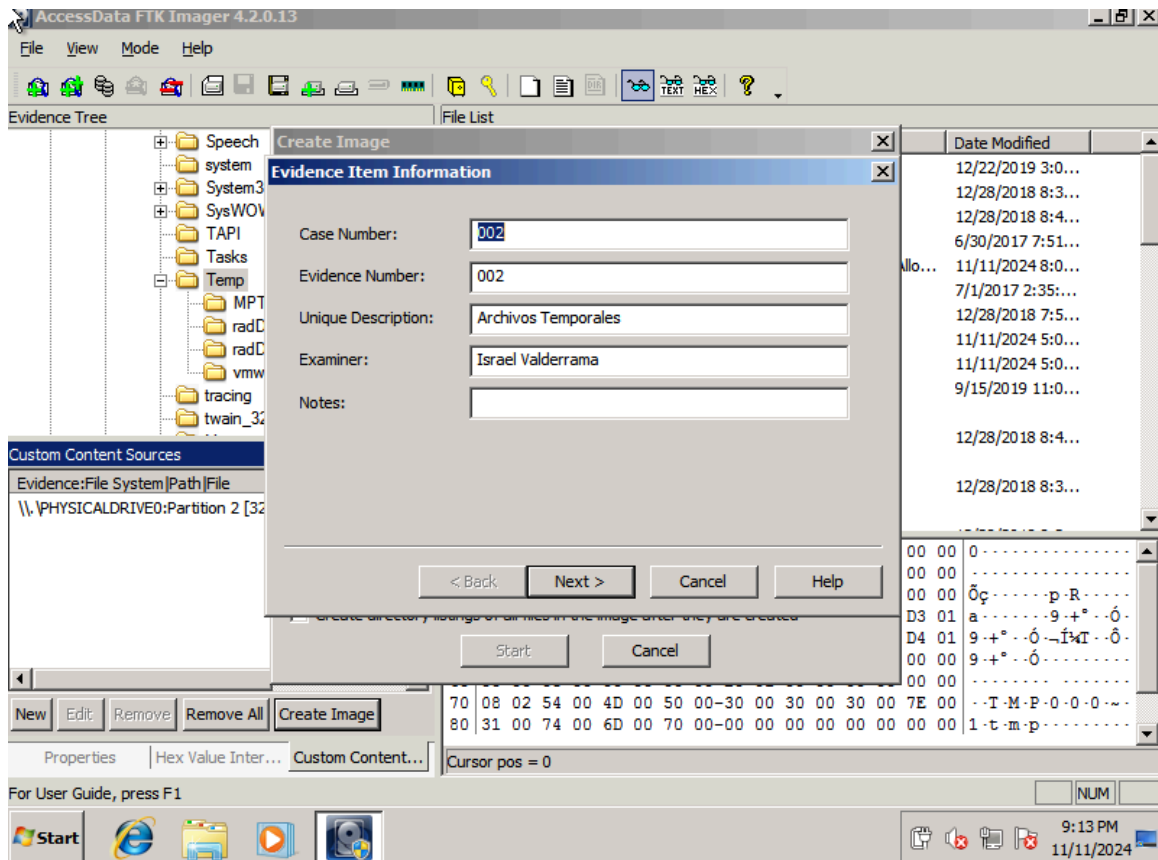


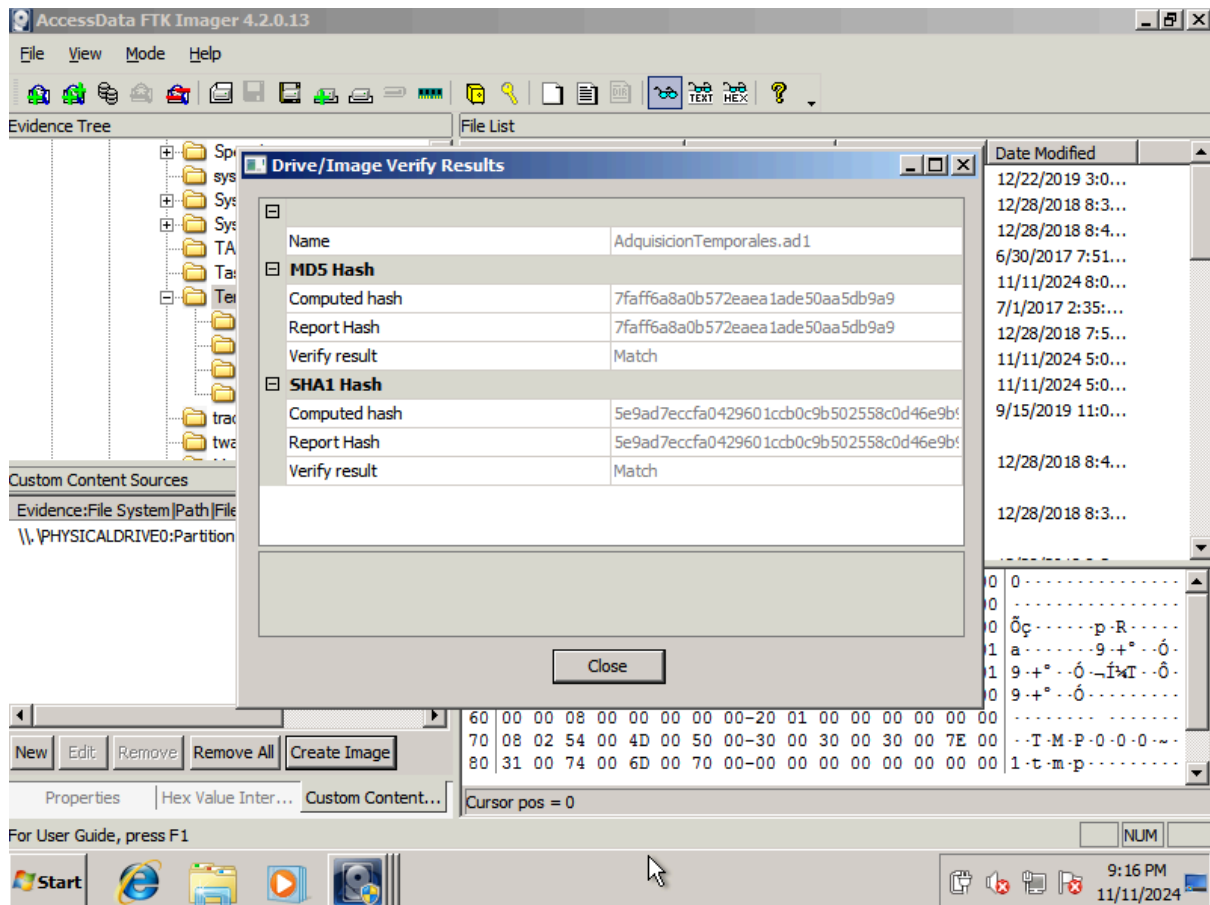
[Enlace Adquisición Disco](#)

3.ARCHIVOS TEMPORALES.

Los archivos temporales son fragmentos de datos generados por el sistema operativo o las aplicaciones durante su funcionamiento. Para capturarlos, empleamos FTK Imager,

dirigiéndonos específicamente a la carpeta de archivos temporales, ubicada generalmente en Windows > Temp. Al concluir el proceso, se generó un hash de los archivos temporales seleccionados, permitiendo su autenticidad y conservación para el análisis.

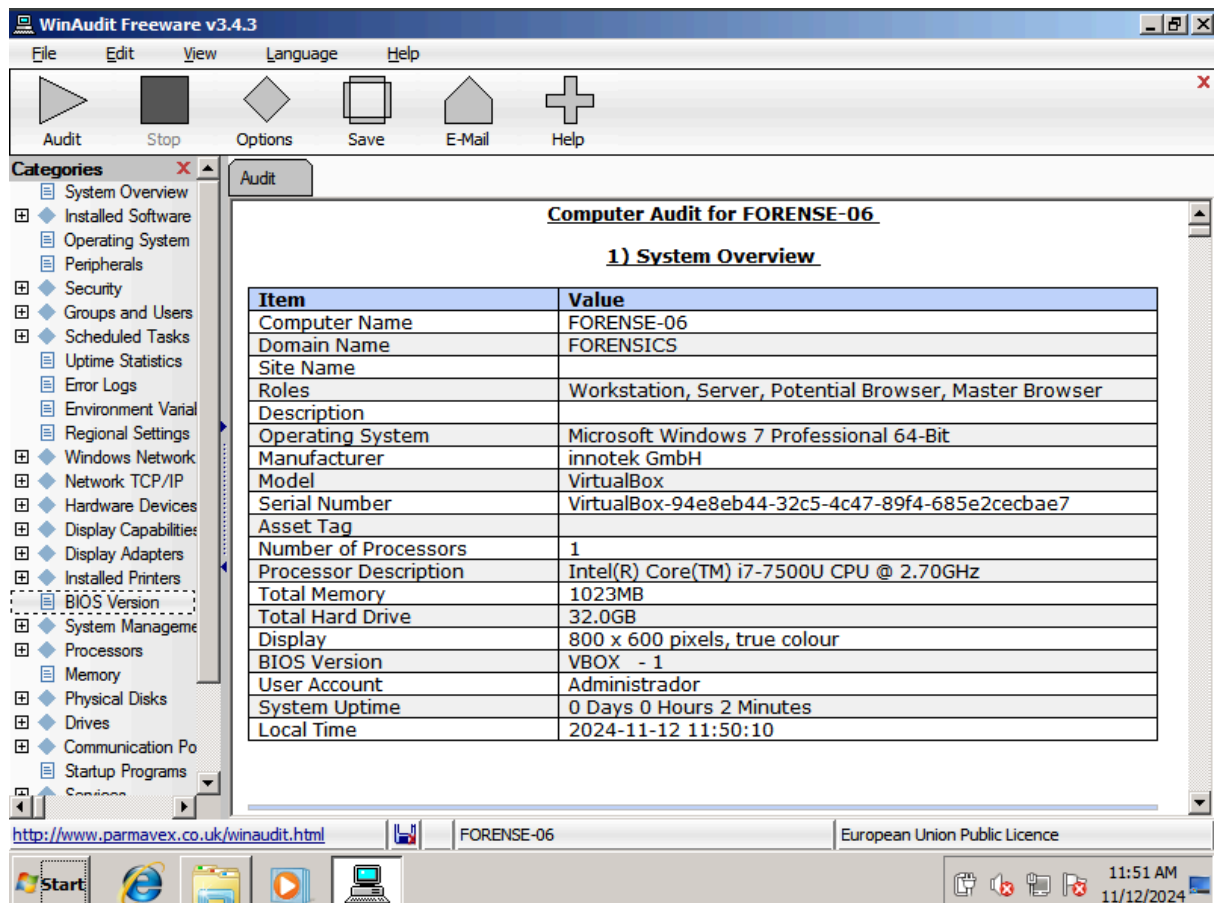




[Enlace Archivos Temporales](#)

4. TRIAJE

Para el triaje forense, empleamos la herramienta WinAudit, que proporciona un informe exhaustivo en formato HTML con un inventario completo del sistema, incluyendo software instalado, configuraciones y archivos relevantes. Esta información preliminar facilita identificar rápidamente áreas de interés para análisis posteriores. Tras generar el informe, se calculó su hash, garantizando la integridad del archivo y que no haya sido alterado después de su creación.



```
MD5 hash de FORENSE-06.html:
6173ef2769ef0fb52d68b82072ce4de4
CertUtil: -hashfile comando completado correctamente.
```

```
SHA1 hash de FORENSE-06.html:
c4915f1f96f6d42463d65c53283cbc4fffd8b71e9
CertUtil: -hashfile comando completado correctamente.
```

[Enlace Triage](#)

5.COMANDO ROUTE PRINT

El comando route print en sistemas Windows permite visualizar la tabla de enrutamiento de la red. Esta tabla contiene instrucciones sobre cómo manejar el tráfico de red según la dirección IP de destino, ayudando a entender cómo se gestionan las conexiones de red en el sistema en el momento de la captura.

```

=====
Interface List
17...08 00 27 2d 9a 3a .....Intel(R) PRO/1000 MT Network Connection #3
1.....Software Loopback Interface 1
12...00 00 00 00 00 00 e0 Microsoft ISATAP 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          192.168.0.1       192.168.0.24     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
192.168.0.0                255.255.255.0    On-link           192.168.0.24     266
192.168.0.24              255.255.255.255  On-link           192.168.0.24     266
192.168.0.255             255.255.255.255  On-link           192.168.0.24     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           192.168.0.24     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           192.168.0.24     266
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1       306 ::1/128                      On-link
17      266 fe80::/64                    On-link
17      266 fe80::d49c:311:8a74:d3a9/128 On-link
1       306 ff00::/8                      On-link
17      266 ff00::/8                      On-link
=====
Persistent Routes:
None

C:\Users\Administrador>

```

6.PROTOCOLO ARP

El Protocolo de Resolución de Direcciones (ARP) se utiliza en redes locales para vincular direcciones IP con direcciones físicas (MAC). Esto es esencial, ya que aunque la comunicación entre dispositivos ocurre a nivel IP, la transferencia de datos reales depende de las direcciones MAC. Al iniciar una comunicación, el dispositivo consulta mediante una solicitud ARP la dirección MAC correspondiente a la IP objetivo. Este protocolo asegura que los datos lleguen a su destino dentro de la red.

```

C:\Users\Administrador>arp -a

Interface: 192.168.0.24 --- 0x11
Internet Address      Physical Address      Type
192.168.0.1           10-62-d0-7f-13-4d    dynamic
192.168.0.19          a4-22-49-4f-65-c6    dynamic
192.168.0.22          20-3d-bd-36-24-86    dynamic
192.168.0.199         3c-52-82-2c-95-1b    dynamic
192.168.0.209         b8-be-f4-19-71-d2    dynamic
192.168.0.255         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

```


7. IPCONFIG

El comando ipconfig en Windows permite obtener información de configuración de red de las interfaces del equipo, incluyendo direcciones IP, máscaras de subred y puertas de enlace predeterminadas. Esto es útil en el análisis forense para identificar la configuración de red y posibles conexiones activas en el momento de la adquisición.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrador>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix . . . : 
    Link-local IPv6 Address . . . . . : fe80::d49c:311:8a74:d3a9%17
    IPv4 Address. . . . . : 192.168.0.24
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.{40B100EE-87EB-4505-8F81-A148FE22DCCC}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : 

Tunnel adapter 6T04 Adapter:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:


    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : 

C:\Users\Administrador>
```

8. ACTA DE ADQUISICIÓN DE EVIDENCIAS DIGITALES:

Este documento oficial detalla el proceso de adquisición y garantiza que la evidencia digital se recolecta de acuerdo con procedimientos forenses estandarizados. Incluye información relevante sobre el caso, el dispositivo adquirido, la metodología de adquisición empleada, y los detalles de tiempo y lugar de la adquisición. Además, contiene el hash de verificación, que asegura la integridad de los datos recopilados.

Acta de Adquisición de Evidencias Digitales	
Sección	Detalles
1. INFORMACIÓN GENERAL	
Número de Caso	001
Fecha y Hora de Adquisición	13/11/2024 10:15
Lugar de Adquisición	C/ Amiel, s/n – 11012, Cádiz (Cádiz)
Analista Forense	Israel Valderrama García
Número de Identificación del Analista	1
2. DESCRIPCIÓN DEL DISPOSITIVO/EVIDENCIA	
Tipo de Dispositivo	Máquina virtual
Marca y Modelo	Windows Vista
Capacidad de Almacenamiento	32 GB
3. METODOLOGÍA DE ADQUISICIÓN	
Estado Físico	Activo.
Herramientas Utilizadas	FTK Imager, RAM Capturer, winaudit.
Método de Adquisición	ISO/IEC 27037:2012(E)
Hash de Verificación MD5	a1de41a629b7a774f69b141d62aff948
Hash de Verificación SHA-1	3a18ba7f9c023d3aa07bc83b202dc00a8e1e4e41
4. DETALLES DEL PROCESO	
Hora de Inicio	19:41
Hora de Finalización	22:30
Observaciones	Primero hemos obtenido el contenido de la memoria volátil, después hemos obtenido el contenido y el hash de la memoria

	no volátil. Por último hemos hecho la adquisición de los archivos temporales y el triaje.
5. DECLARACIÓN DEL ANALISTA	
Declaraciones	Yo, Israel Valderrama, certifico que la información contenida en esta acta es verdadera y precisa según mi mejor conocimiento y habilidad. La adquisición de evidencias se realizó siguiendo los procedimientos forenses estándar y manteniendo la integridad de la evidencia en todo momento.
Firma del Analista	
Fecha	13/11/2024

9. CADENA DE CUSTODIA:

La cadena de custodia documenta cada fase de la adquisición, preservación y transferencia de la evidencia digital para asegurar que no se manipule ni altere en ningún momento. Cada entrega de la evidencia se registra con fecha, hora y firma del responsable, lo cual permite mantener la trazabilidad de la evidencia desde el momento de la adquisición hasta su presentación en instancias legales.

CADENA DE CUSTODIA	
Sección	Campo
1. INFORMACIÓN DEL CASO	
Número de Caso	01
Tipo de Investigación	Adquisición de memoria volátil.
Fecha de Adquisición	11/11/2024
Lugar de Adquisición	C/ Amiel, s/n – 11012, Cádiz (Cádiz)
Número de Caso	02
Tipo de Investigación	Adquisición de memoria no volátil.
Fecha de Adquisición	11/11/2024
Lugar de Adquisición	C/ Amiel, s/n – 11012, Cádiz (Cádiz)
Número de Caso	03
Tipo de Investigación	Adquisición de archivos temporales.
Fecha de Adquisición	11/11/2024
Lugar de Adquisición	C/ Amiel, s/n – 11012, Cádiz (Cádiz)
Número de Caso	04
Tipo de Investigación	Triaje
Fecha de Adquisición	11/11/2024
Lugar de Adquisición	C/ Amiel, s/n – 11012, Cádiz (Cádiz)
2. DESCRIPCIÓN EVIDENCIA EN ORIGINAL	
Tipo de Dispositivo	Memoria RAM

Hash de la Evidencia Original	MD5: 8bcf8e5ae60e6eab7587c9e1005ee3 SHA1: 2494badf7c740bd1b92223cbd864a29b6996f484
Tipo de Dispositivo	Disco Duro
Hash de la Evidencia Original	MD5: a1de41a629b7a774f69b141d62aff948 SHA1: 3a18ba7f9c023d3aa07bc83b202dc00a8e1e4e41
Tipo de Dispositivo	Archivos temporales
Hash de la Evidencia Original	MD5: 7faff6a8a0b572eaea1ade50aa5db9a9 SHA1: 5e9ad7eccfa0429601ccb0c9b502558c0d46e9b9
Tipo de Dispositivo	Triaje
Hash de la Evidencia Original	MD5: 6173ef2769ef0fb52d68b82072ce4de4 SHA1: c4915f1f96f6d42463d65c53283cbc4ffd8b71e9
3. PRESERVACIÓN DE LA EVIDENCIA ORIGINAL	
Fecha de Entrega	13/11/2024
Hora de Entrega	23:59
Recibido por	Manuel Jesús Rivas Sánchez
Ubicación en el Juzgado	C/ Amiel, s/n – 11012, Cádiz (Cádiz)
4. CREACIÓN Y VERIFICACIÓN DE COPIAS	
Fecha y Hora de Creación	13/11/2024, 19:48
Técnico Responsable	Israel Valderrama
Hash de la Copia	MD5: a1de41a629b7a774f69b141d62aff948 SHA1: 3a18ba7f9c023d3aa07bc83b202dc00a8e1e4e41
Verificación de Integridad	Si
Entregado a	Manuel Jesús Rivas Sánchez
Fecha y Hora de Entrega	19/11/2024, 23:59
5. REGISTRO DE ACCESOS Y VERIFICACIONES	
Fecha y Hora	13/11/2024, 19:53
Propósito	Análisis de evidencias

Hash Verificado	MD5: a1de41a629b7a774f69b141d62aff948 SHA1: 3a18ba7f9c023d3aa07bc83b202dc00a8e1e4e41
Coincide con Original (Acceso)	Si