Proyecto 02.1 - Recolección y almacenamiento de evidencias

Víctor Jiménez Corada

Índice

1. Recolección de evidencias

Para la adquisición de evidencia digital nos vamos a basar en la norma ISO/IEC 27037:2012(E) ya que está diseñada para aplicarse en el ámbito internacional.

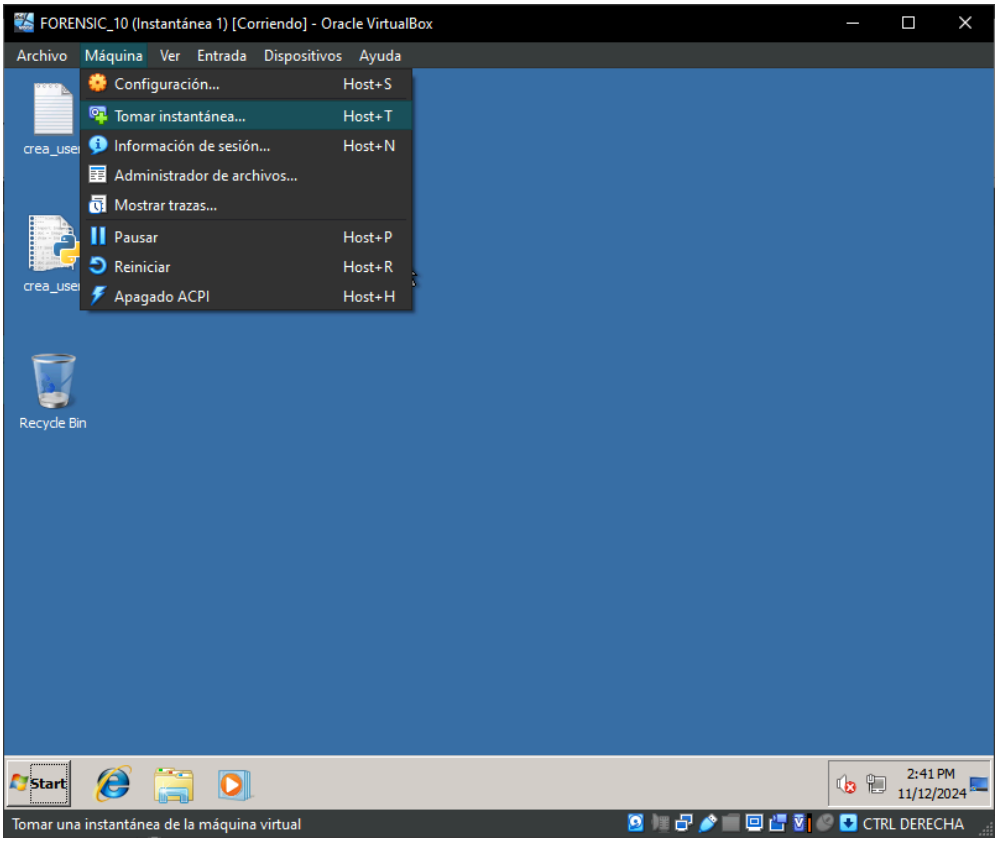
Para realizar la recolección de evidencia digital de la máquina comprometida se usará VirtualBox, siguiendo un proceso meticuloso y usando herramientas específicas y comandos de red para obtener datos cruciales. A continuación, se detallan los pasos que se han seguido para la recolección y el almacenamiento de evidencias:

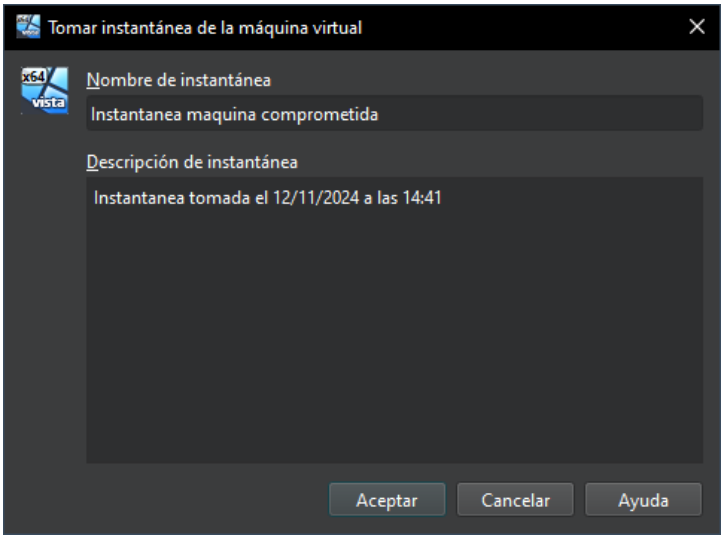
1.1. Snapshot de VirtualBox

Primero, se ha realizado una instantánea o “snapshot” del estado actual de la máquina virtual. Esto permite guardar una copia fiel del sistema tal como se encuentra en ese preciso momento, incluyendo la configuración del sistema operativo, las aplicaciones abiertas y cualquier proceso que esté en ejecución. Los pasos seguidos para crear la snapshot en VirtualBox han sido los siguientes:

- Ir a la máquina virtual en VirtualBox.
- Seleccionar “Máquina” > “Tomar Instantánea”.
- Asignar un nombre descriptivo al snapshot que refleje la fecha y hora de la captura.

Este snapshot garantiza la disponibilidad de una versión intacta del sistema que puede ser utilizada para análisis posteriores, facilitando la reproducción del entorno inicial.



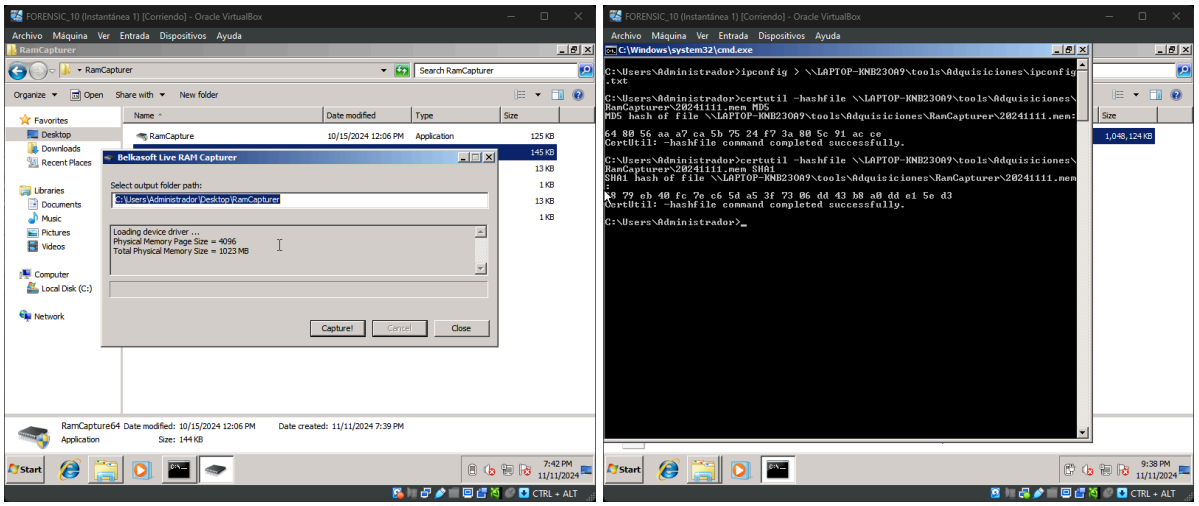


1.2. Captura de Memoria RAM (RamCapturer)

Para capturar el contenido de la memoria RAM hago uso de la herramienta **RamCapturer**. La memoria RAM contiene datos cruciales de procesos activos, conexiones de red, y otra información temporal que podría desaparecer una vez que el sistema se apague o reinicie. Con RamCapturer en ejecución dentro de la máquina virtual, se realiza la copia de la memoria volátil, generando un archivo de captura que luego se almacena de forma segura. Este archivo se etiqueta con detalles de la fecha, hora y tamaño, asegurando así que pueda ser identificado fácilmente durante las etapas posteriores de análisis. Una vez adquirida la imagen se han calculado los hashes usando los siguiente comandos:

certutil -hashfile \\LAPTOP-KNB230A9\tools\Adquisiciones\RamCapturer\20241111.mem MD5

certutil -hashfile \\LAPTOP-KNB230A9\tools\Adquisiciones\RamCapturer\20241111.mem SHA1

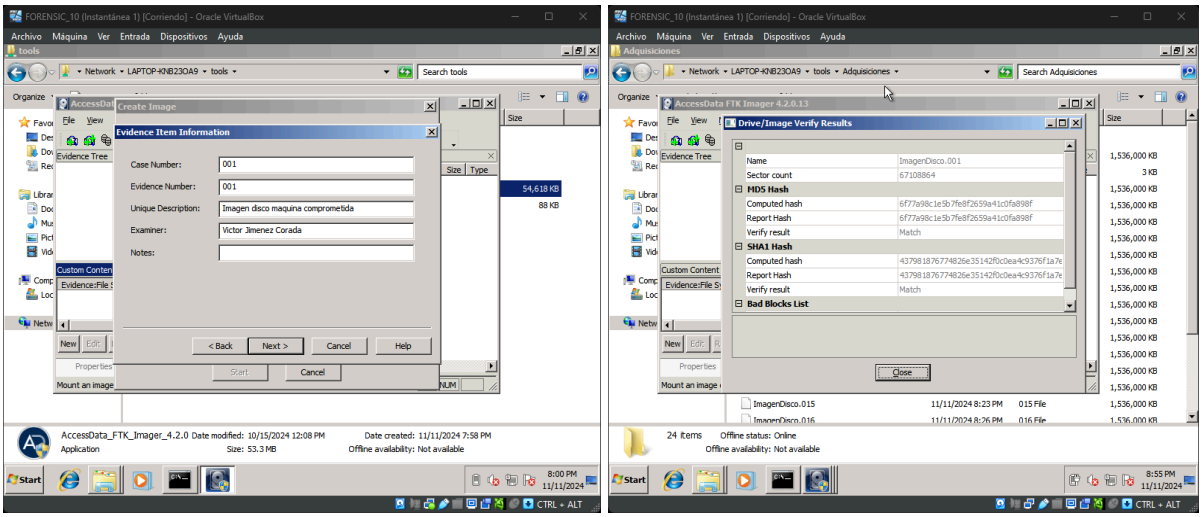


1.3. Adquisición del Disco Duro (FTK Imager)

La adquisición del disco duro se ha realizado empleando **FTK Imager**, una herramienta forense de confianza. Este paso es esencial para asegurar que el contenido del almacenamiento no volátil, que incluye archivos del sistema, registros de eventos, y archivos de usuario. Con FTK Imager, se crea una imagen completa del disco en un formato seguro y sin alteración, la cual es posteriormente guardada en un medio de almacenamiento adecuado para su análisis. Durante este proceso, se generan hashes de verificación que certifican la integridad del archivo de imagen; estos se documentan junto con otros detalles técnicos como el formato y las condiciones bajo las cuales se realizó la adquisición.

Para generar una imagen del disco duro con FTKImager se han seguido los siguientes pasos:

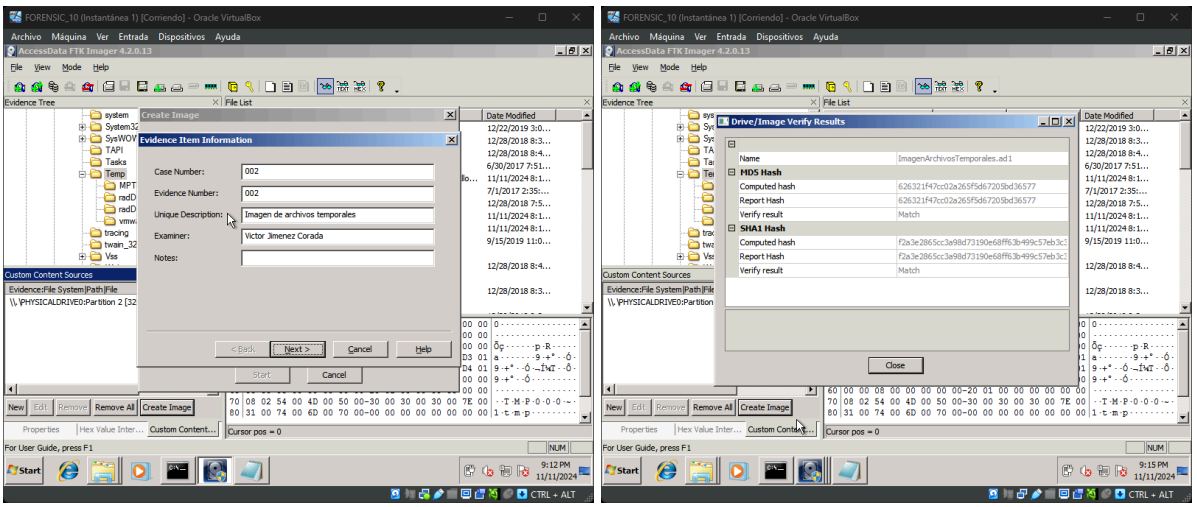
- Abrir FTK Imager y seleccionar la opción para crear una imagen de disco.
- Seleccionar el disco como fuente y configurar FTK Imager para realizar una imagen completa en formato de archivo seguro. Una vez completada, guardarla en un medio de almacenamiento forense adecuado.



1.4. Extracción de Archivos Temporales (FTK Imager)

Para la extracción de archivos temporales específicos, nuevamente se utilizará **FTK Imager**. Los archivos temporales pueden proporcionar información sobre actividad reciente en el sistema, incluyendo datos de aplicaciones y navegadores que pudieran ser relevantes para la investigación. Se han identificado y exportado aquellos archivos que pueden contener información útil. Los archivos extraídos son etiquetados y documentados, anotando sus ubicaciones exactas en el sistema de archivos. Los pasos a seguir han sido los siguientes:

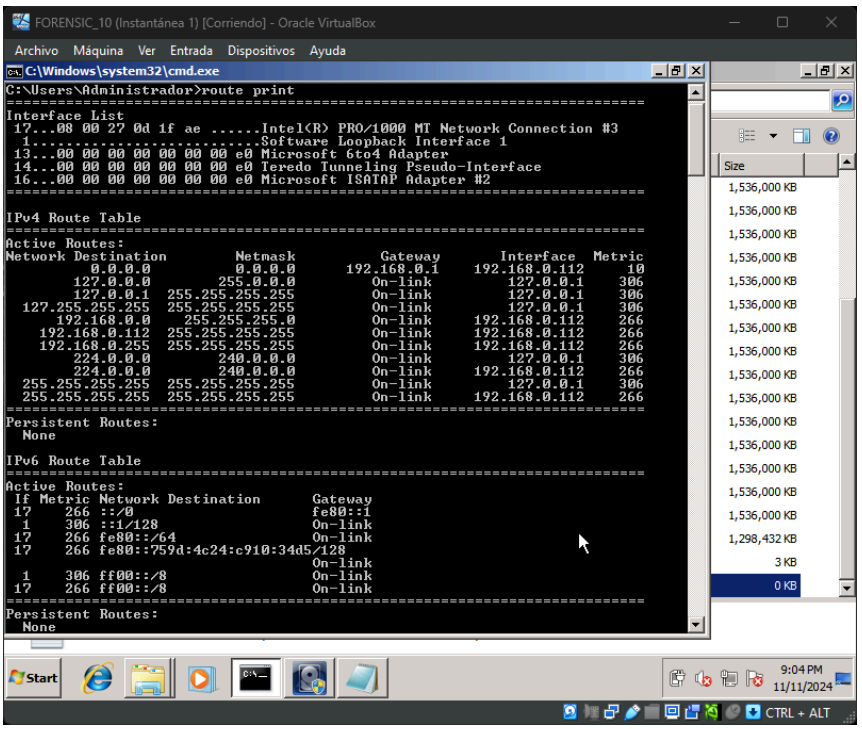
- Navegar a las ubicaciones de archivos temporales dentro del sistema de archivos de la imagen.
- Seleccionar y exportar archivos que se consideren relevantes, especialmente los ubicados en carpetas temporales del sistema y el navegador.



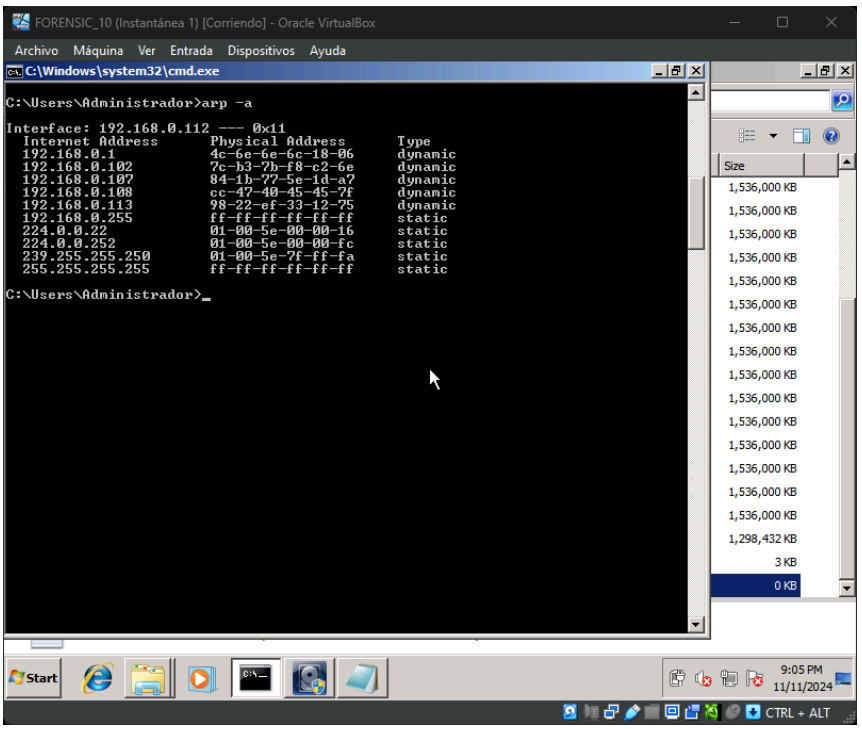
1.5. Comandos de Red

Para capturar información sobre el estado y configuración de red en el momento de la recolección, se ejecutan una serie de comandos en la consola. Los comandos ejecutados han sido los siguientes:

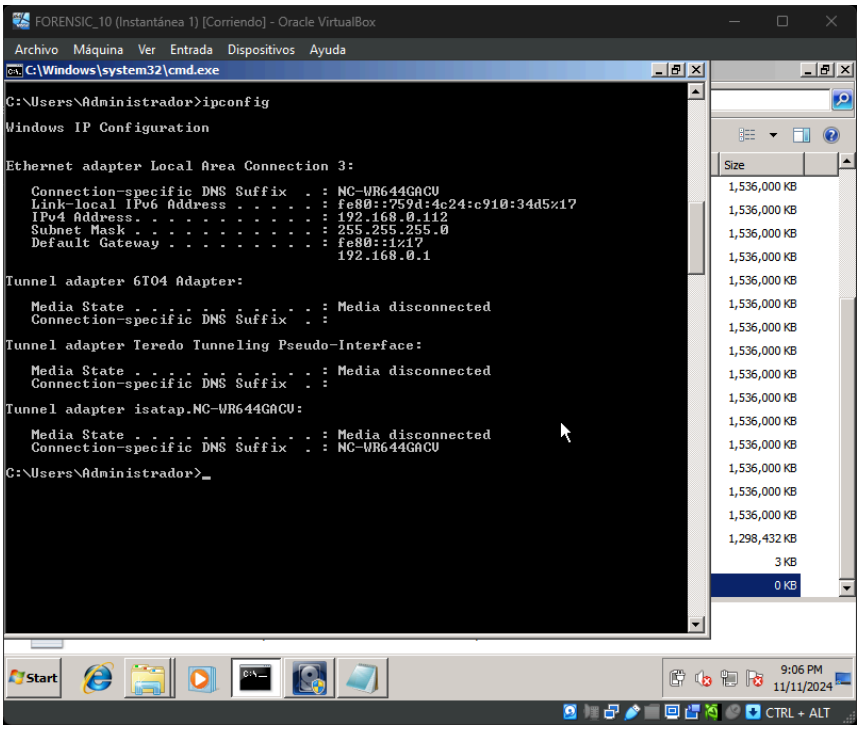
- **`route print`**: Permite obtener la tabla de enrutamiento actual del sistema, proporcionando detalles sobre rutas y conexiones de red.



- **`arp -a`**: Lista las direcciones IP y MAC de dispositivos conectados al sistema, ayudando a reconstruir interacciones recientes con otros dispositivos en la red.



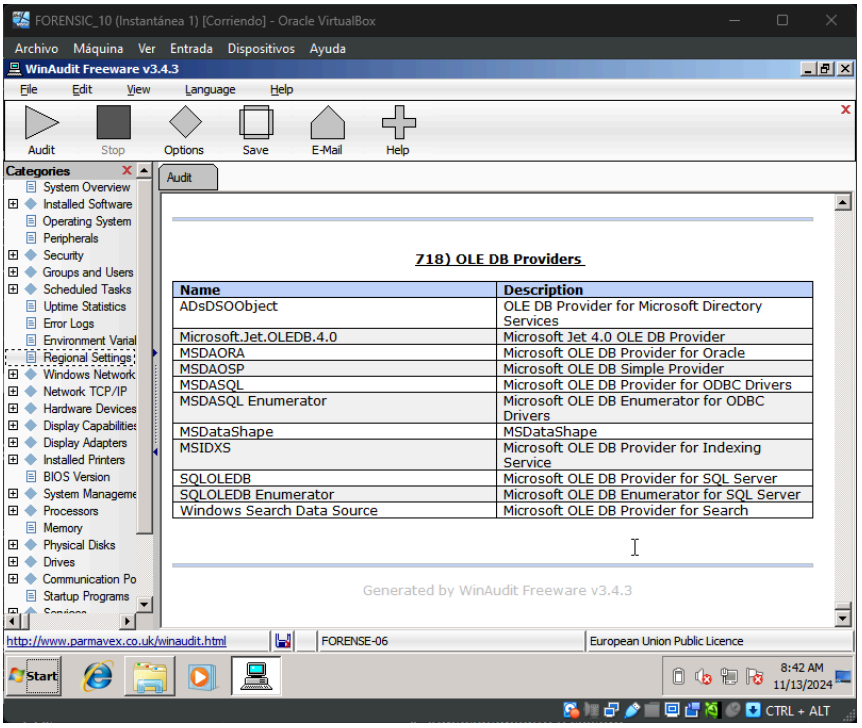
- **`ipconfig`**: Muestra la configuración de red actual, incluyendo direcciones IP asignadas y detalles de las interfaces de red.



Los resultados de estos comandos se guardan en archivos de texto, los cuales son almacenados en una ubicación segura junto con otras evidencias recolectadas.

1.6. Triage (WinAudit)

Para recoger la información referida al triage de la máquina se ha utilizado WinAudit. Al ejecutarse en el dispositivo, genera un archivo html que contiene toda la información.



2. Descripción de la evidencia

Las evidencias obtenidas durante el proceso de adquisición son las siguientes:

- RAM:
  - **20241111.mem**: Imagen de la memoria RAM completa capturada para análisis forense.
  - **20241111.txt**: Archivo que contiene los hashes de la imagen de la RAM, asegurando la integridad y autenticidad de la evidencia.
- Disco duro:
  - **ImagenDisco.001**: Imagen completa del disco duro, creada para análisis de datos almacenados.
  - **ImagenDisco.001.txt**: Archivo con información detallada sobre la imagen del disco duro, incluyendo metadatos relevantes.
- Archivos temporales:
  - **ImagenArchivosTemporales.ad1**: Imagen de los archivos temporales generados por el sistema o aplicaciones.
  - **ImagenArchivosTemporales.ad1.txt**: Archivo con información sobre la imagen de archivos temporales, útil para contexto y verificación.

- Red:
  - **arp.txt**: Resultado del comando **`arp -a`**, proporcionando información sobre las tablas ARP y conexiones activas de la máquina en el momento de la adquisición.
  - **routeprint.txt**: Resultado del comando **`route print`**, que muestra la tabla de enrutamiento y configuraciones de red del sistema.
  - **ipconfig.txt**: Resultado del comando **`ipconfig`**, que detalla la configuración de red y direcciones IP asignadas al sistema.
- Triage:
  - **Triage.html**: Archivo html que contiene la información referida al triage de la máquina.

3. Cadena de custodia

En primer lugar, se debe rellenar el Acta de Adquisición de Evidencias Digitales. Para ello usaremos el siguiente modelo:

Acta de Adquisición de Evidencias Digitales	
Sección	**Detalles**
1. INFORMACIÓN GENERAL	
Número de Caso	02.1
Fecha y Hora de Adquisición	07/11/2024, 08:00
Lugar de Adquisición	C. Amiel, s/n, 11012 Barriada de la Paz, Cádiz
Analista Forense	Víctor Jiménez Corada
Número de Identificación del Analista	-
2. DESCRIPCIÓN DEL DISPOSITIVO/EVIDENCIA	
Tipo de Dispositivo	Máquina completa
Marca y Modelo	-
Número de Serie	-
Capacidad de Almacenamiento	31,8 GB (20,9 GB en uso)
3. METODOLOGÍA DE ADQUISICIÓN	

Estado Físico	-
Herramientas Utilizadas	RamCapturer, FTKImager, WinAudit
Método de Adquisición	ISO/IEC 27037:2012(E)
Hash de Verificación MD5	6f77a98c1e5b7fe8f2659a41c0fa898f
Hash de Verificación SHA1	437981876774826e35142f0c0ea4c9376f1a7efe
4. DETALLES DEL PROCESO	
Hora de Inicio	19:40
Hora de Finalización	22:00
Observaciones	Adquisición de imágenes referentes a los siguientes apartados: RAM, Disco duro, Archivos temporales, Redes y Triage
5. TESTIGOS	
Nombre del Testigo 1	-
Firma Testigo 1	-
Nombre del Testigo 2	-
Firma Testigo 2	-
6. DECLARACIÓN DEL ANALISTA	
Declaraciones	Yo, Víctor Jiménez Corada, 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
7. ANEXOS	
Fotografías del dispositivo	-
Logs de la herramienta de adquisición	-

Otros documentos relevantes	-

Una vez rellenado el acta de adquisición, se documenta la cadena de custodia. Este documento hace referencia al proceso por el que pasan las evidencias desde que se ha llevado a la adquisición. Recoge a quien se entrega las evidencias, datos sobre la misma, si se crean copias de las evidencias, comprobaciones de hash, etc. El modelo que se ha rellenado es el siguiente:

CADENA DE CUSTODIA	
Sección	**Campo**
1. INFORMACIÓN DEL CASO	
Número de Caso	02.1
Tipo de Investigación	Análisis completo de máquina comprometida
Fecha de Adquisición	07/11/2024
Lugar de Adquisición	C. Amiel, s/n, 11012 Barriada de la Paz, Cádiz
2. DESCRIPCIÓN DE LA EVIDENCIA ORIGINAL	
Tipo de Dispositivo	Máquina completa
Marca y Modelo	-
Número de Serie	-
Hash de la Evidencia Original	MD5: 6f77a98c1e5b7fe8f2659a41c0fa898f SHA1: 437981876774826e35142f0c0ea4c9376f1a7efe
3. PRESERVACIÓN DE LA EVIDENCIA ORIGINAL	
Fecha de Entrega al Juzgado	07/11/2024
Hora de entrega	08:00
Recibido por	Manuel Rivas Sández
Ubicación en el Juzgado	C. Amiel, s/n, 11012 Barriada de la Paz, Cádiz
Firma del Funcionario Judicial	-
4. CREACIÓN Y VERIFICACIÓN DE COPIAS	
Fecha y Hora de Creación (Defensa)	11/11/2024, 20:05

Técnico Responsable (Defensa)	Víctor Jiménez Corada
Hash de la Copia (Defensa)	MD5: 6f77a98c1e5b7fe8f2659a41c0fa898f SHA1: 437981876774826e35142f0c0ea4c9376f1a7efe
Verificación de Integridad (Defensa)	MD5: 6f77a98c1e5b7fe8f2659a41c0fa898f : verified SHA1: 437981876774826e35142f0c0ea4c9376f1a7efe : verified
Entregado a (Defensa)	Víctor Jiménez Corada
Fecha y Hora de Entrega (Defensa)	07/11/2024, 08:00
Firma del Receptor (Defensa)	-
5. REGISTRO DE ACCESOS Y VERIFICACIONES	
Fecha y Hora (Acceso)	11/11/2024, 19:40
Parte Accediendo (Acceso)	Defensa
Propósito (Acceso)	Recolección y almacenamiento de evidencias
Hash Verificado (Acceso)	MD5: 6f77a98c1e5b7fe8f2659a41c0fa898f : verified SHA1: 437981876774826e35142f0c0ea4c9376f1a7efe : verified
Coincide con Original (Acceso)	Sí
Firma (Acceso)	-

4. Almacenamiento de la evidencia

Las evidencias obtenidas se almacenaron inicialmente en una memoria USB en el momento de su adquisición, asegurando que toda la información se mantuviera intacta y accesible. Además, para aumentar la seguridad y prevenir cualquier riesgo de pérdida o corrupción de los datos, se realizó una copia de seguridad en la nube. Este proceso garantiza una doble protección, dando tanto un acceso inmediato a las evidencias como una alternativa segura en caso de fallo o daño en el dispositivo físico.

La copia de seguridad de los datos en la nube se encuentra en el siguiente enlace: Adquisiciones.

5. Metodología aplicada

La metodología aplicada durante el proceso de adquisición y almacenamiento de las evidencias encontradas en la máquina comprometida ha sido la siguiente:

5.1. Acta de Adquisición de Evidencia Digital:

En primer lugar, se ha redactado un Acta de Adquisición de Evidencias Digitales, en la que se documenta la identificación del dispositivo, su estado y las condiciones bajo las cuales se lleva a cabo la adquisición. Este acta certifica el consentimiento de los responsables y la presencia de testigos o agentes, según corresponda, proporcionando un registro detallado para futuras consultas.

5.2. Manejo de la máquina comprometida:

Al tratarse de un dispositivo encendido, lo pasos que se han seguido son los siguientes:

1. **Adquisición de Memoria Volátil:** Se ha realizado una captura de la memoria volátil (RAM). Esta fase es crítica, ya que en la RAM se almacena información temporal y vital, como los procesos activos, conexiones de red y posibles contraseñas en memoria, datos que se perderían si el equipo se apaga antes de capturarlos.
2. **Adquisición de Memoria No Volátil:** Adquisición de los datos de la memoria no volátil, almacenados en el disco duro. Este proceso se realiza con precaución para evitar cualquier alteración de los datos durante la extracción.
3. **Apagado del Dispositivo:** Una vez obtenida la evidencia crítica, se apaga el dispositivo de forma controlada, reduciendo el riesgo de daños en el almacenamiento o pérdida de datos.
4. **Retiro de Cables y Accesorios Conectados:** Se retiran y documentan todos los cables, dispositivos o accesorios conectados, para preservar el contexto en el cual se encontraba la máquina al momento de la intervención.
5. **Protección del dispositivo:** Se cubre o bloquea el botón de encendido y el lector de CD para prevenir manipulaciones involuntarias o accidentales posteriores.
6. **Almacenamiento Seguro de la Evidencia:** Los datos adquiridos se guardan en dispositivos de almacenamiento externo seguros, siguiendo protocolos estrictos para evitar alteraciones o pérdidas.

5.3. Preservación y Almacenamiento de la Evidencia:

La fase de preservación se rige por la norma UNE 71506:2013, que garantiza la integridad de la evidencia digital al mantenerla en su estado original. Este enfoque es esencial para que los datos preserven su validez y fiabilidad en futuros análisis o contraanálisis, asegurando que la información se mantenga sin alteraciones.

5.4. Cadena de Custodia:

Para mantener la trazabilidad de la evidencia y garantizar su autenticidad, el informe de cadena de custodia se estructura en cinco secciones:

- **Información del caso:** Se presentan los detalles y contexto general del caso.
- **Descripción de la evidencia original:** Se documenta detalladamente el estado de la evidencia digital al momento de su recolección, sin ninguna modificación.
- **Preservación de la evidencia original:** Describe las medidas adoptadas para preservar la evidencia en su estado inicial.
- **Creación y verificación de copias:** Explica el proceso de generación de copias y la verificación de su integridad mediante hashes, asegurando que las copias son idénticas a la evidencia original.
- **Registro de accesos y verificaciones:** Se lleva un registro minucioso de cada acceso o verificación realizado sobre la evidencia, proporcionando un historial claro de todas las acciones realizadas.

Esta metodología asegura que la evidencia digital recopilada se mantenga intacta y verificable, preservando su autenticidad y valor para un posible uso judicial.