INFORME AUDITORIA FORENSE CON AUTOPSY

JUAN CARLOS PALACIOS VALENCIA

INTEGRANTE

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENIERIA EN TELECOMUNICACIONES E INFORMATICA

QUIBDO-CHOCÓ

9/09/2025

INFORME AUDITORIA FORENSE CON AUTOPSY

INTEGRANTE

JUAN CARLOS PALACIOS VALENCIA

DOCENTE

RAFAEL SANDOVAL

ASIGNATURA

SEGURIDAD Y AUDITORIA

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENIERIA EN TELECOMUNICACIONES E INFORMATICA

QUIBDO-CHOCÓ

9/09/2025

1. CONTENIDO

2. CAPITULO 1 AUDITORIA FORENSE CON AUTOPSY EN LINUX 7

2.1. Visualización de las particiones y dispositivos de almacenamiento 7

2.2. Generación del hash SHA1 de la memoria USB 8

2.3. Creación de la imagen forense de la memoria USB 8

2.4. Cambio de permisos de archivo 9

2.5. Agregando un equipo a un caso en Autopsy 9

3. CAPITULO 2 AUDITORIA FORENSE CON AUTOPSY EN WINDOWS 13

3.1. Descargar e instalar autopsy en Windows 13

3.2. Creación de un nuevo caso en Autopsy 14

TABLA DE IMÁGENES

Ilustración 1 Listado de discos y particiones en Linux con fdisk 7

Ilustración 2 Generación de hash SHA1 de un dispositivo USB en Linux 8

Ilustración 3 Valor hash SHA1 obtenido del dispositivo USB /dev/sdb..... 8

Ilustración 4 Copia forense del dispositivo USB sin alteración de datos 8

Ilustración 5 Cálculo del hash SHA-1 de la imagen forense 9

Ilustración 6 Aplicación de permisos 777 al archivo de imagen forense..... 9

Ilustración 7 Adición de un nuevo host al caso en Autopsy 9

Ilustración 8 Importación de la imagen forense en Autopsy..... 10

Ilustración 9 Verificación de integridad y configuración del sistema de archivos en Autopsy 11

Ilustración 10 Importación exitosa de la imagen forense en Autopsy 11

Ilustración 11 Gestión de volúmenes y selección de imagen en Autopsy 12

Ilustración 12 erificación de integridad de archivos dentro de la partición analizada..... 12

Ilustración 13 buscador de google 13

Ilustración 14 Descarga de Autopsy 13

Ilustración 15 Pantalla de bienvenida del instalador de Autopsy 14

Ilustración 16 Interfaz principal de bienvenida de Autopsy 14

Ilustración 17 Configuración inicial del caso forense en Autopsy 15

Ilustración 18 Registro de información opcional para el caso forense 15

Ilustración 19 Selección de host para la fuente de datos en Autopsy 16

Ilustración 20 Selección del tipo de fuente de datos en Autopsy..... 16

Ilustración 21 Configuración de carpetas compartidas para el análisis forense 17

Ilustración 22 Archivo de imagen forense (.dd) generado para el análisis 17

Ilustración 23 Selección de la imagen forense para análisis en Autopsy..... 17

Ilustración 24 Selección de la imagen forense para análisis en Autopsy..... 18

Ilustración 25 Configuración de módulos de análisis (Ingest) en Autopsy 18

Ilustración 26 Visualización de archivos no asignados en Autopsy 19

Ilustración 27 Visualización de archivos asignados en el volumen analizado con Autopsy 19

Ilustración 28 Tabla de análisis forense de archivos con valores hash y tipo MIME en Autopsy 20

2. INTRODUCCION

En el mundo digital actual, los dispositivos de almacenamiento como discos duros y memorias USB guardan gran cantidad de información que puede ser clave en una investigación. La auditoría forense digital permite analizar estos dispositivos sin alterar la evidencia original, asegurando que los datos se mantengan íntegros y verificables. En este trabajo se documenta el proceso de análisis forense utilizando la herramienta Autopsy**,** tanto en sistemas Linux como en Windows, mostrando paso a paso cómo crear un caso, generar hashes, crear imágenes forenses y examinar la evidencia digital.

3. OBJETICO GENERAL

Realizar una auditoría forense digital utilizando el programa Autopsy en los sistemas operativos Linux y Windows**,** con el fin de identificar, analizar y preservar evidencia digital de manera segura y verificable.

4. OBJETIVO ESPECÍFICO

- Visualizar las particiones y dispositivos de almacenamiento en un entorno Linux para identificar las fuentes de evidencia.
- Generar el hash SHA1 de una memoria USB para garantizar su integridad antes del análisis.
- Crear una imagen forense del dispositivo USB sin alterar el contenido original.
- Configurar y gestionar un caso forense en Autopsy, importando la imagen y verificando su validez mediante hashes MD5.
- Repetir el procedimiento en un entorno Windows, instalando Autopsy, creando un nuevo caso y analizando la evidencia digital.

• Evaluar los resultados obtenidos del análisis en ambos sistemas operativos, comparando sus características y funcionamiento.

DESARROLLO

5. CAPITULO 1 AUDITORIA FORENSE CON AUTOPSY EN LINUX

5.1. Visualización de las particiones y dispositivos de almacenamiento

Iniciamos ejecutando el comando **fdisk -l** este nos muestra el disco duro de la computadora que es de 100 GiB, aparece una memoria de 7,22 GiB que usa un formato compartido con Windows.

```
┌──(root㉿vbox)-[/home/linux]
└─# fdisk -l
Disk /dev/sda: 100 GiB, 107374182400 bytes, 209715200 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×af2cb4ca

Device     Boot     Start       End   Sectors  Size Id Type
/dev/sda1  *         2048 199743487 199741440 95,2G 83 Linux
/dev/sda2       199745534 209713151   9967618  4,8G  f W95 Ext'd (LB
/dev/sda5       199745536 209713151   9967616  4,8G 82 Linux swap /


Disk /dev/sdb: 7,22 GiB, 7756087296 bytes, 15148608 sectors
Disk model: DataTraveler 2.0
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×7a7d44aa

Device     Boot Start      End  Sectors  Size Id Type
/dev/sdb1          63 15148223 15148161  7,2G  7 HPFS/NTFS/exFAT
```

Ilustración 1 Listado de discos y particiones en Linux con fdisk

5.2. Generación del hash SHA1 de la memoria USB

Ahora vamos a ejecutar el comando **sha1sum/dev/sdb > /home/linux/Escritorio/hash_fore.sha1** este crea una huella digital del contenido de la memoria USB y la guarda en un archivo para poder verificar más adelante que no se haya modificado.

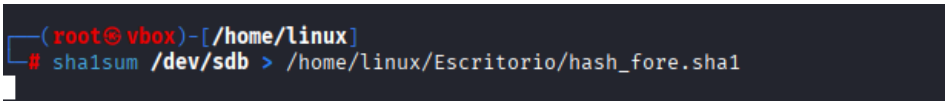

Ilustración 2 Generación de hash SHA1 de un dispositivo USB en Linux

Este valor es la **huella digital única** del dispositivo, usada para verificar su integridad o comprobar que no se ha modificado.

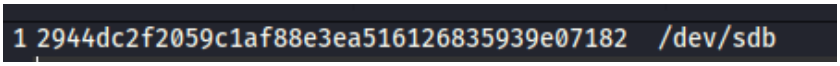

Ilustración 3 Valor hash SHA1 obtenido del dispositivo USB /dev/sdb

5.3. Creación de la imagen forense de la memoria USB

Con el comando **dd** se hizo una copia completa de la memoria USB para analizarla sin modificar el original.

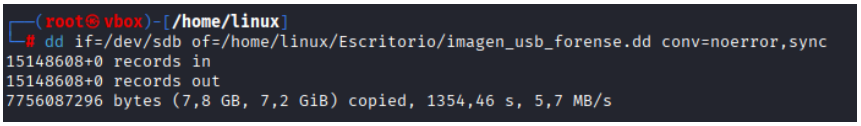

Ilustración 4 Copia forense del dispositivo USB sin alteración de datos

Con el comando **sha1sum** se comprobó que la copia de la memoria USB es exacta al original.

```
┌──(root㉿vbox)-[/home/linux]
└─# sha1sum /home/linux/Escritorio/imagen_usb_forense.dd
2944dc2f2059c1af88e3ea516126835939e07182  /home/linux/Escritorio/imagen_usb_forense.dd
```

Ilustración 5 Cálculo del hash SHA-1 de la imagen forense

5.4. Cambio de permisos de archivo

Este comando cambia los permisos del archivo para que todos los usuarios tengan permisos de lectura, escritura y ejecución**.**

```
┌──(root㉿vbox)-[/home/linux]
└─# chmod 777 /home/linux/Escritorio/imagen_usb_forense.dd
```

Ilustración 6 Aplicación de permisos 777 al archivo de imagen forense

5.5. Agregando un equipo a un caso en Autopsy

Ahora se está añadiendo un nuevo host (mvkalip1tl) a un caso forense (miprimercaso1) en el programa Autopsy. El sistema ha creado el directorio del host y su archivo de configuración**,** y ahora indica que se debe importar una imagen forense (archivo de disco o evidencia) para continuar con el análisis.

Ilustración 7 Adición de un nuevo host al caso en Autopsy

En esta pantalla de **Autopsy**, se está añadiendo una nueva imagen forense al caso.

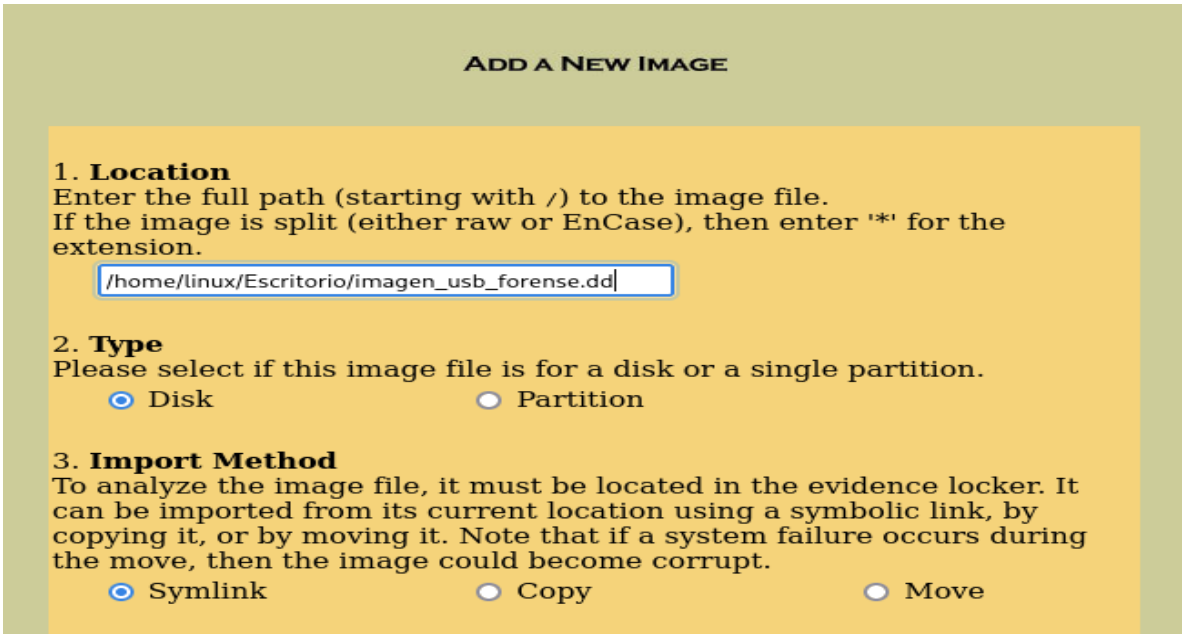

Ilustración 8 Importación de la imagen forense en Autopsy

Ahora se realizó la importación de una imagen forense para su análisis. Durante el proceso se verificó la integridad mediante hash MD5 y se identificó una partición con sistema de archivos NTFS/exFAT Esta información permite examinar el contenido del dispositivo de manera controlada y sin alterar la evidencia original.

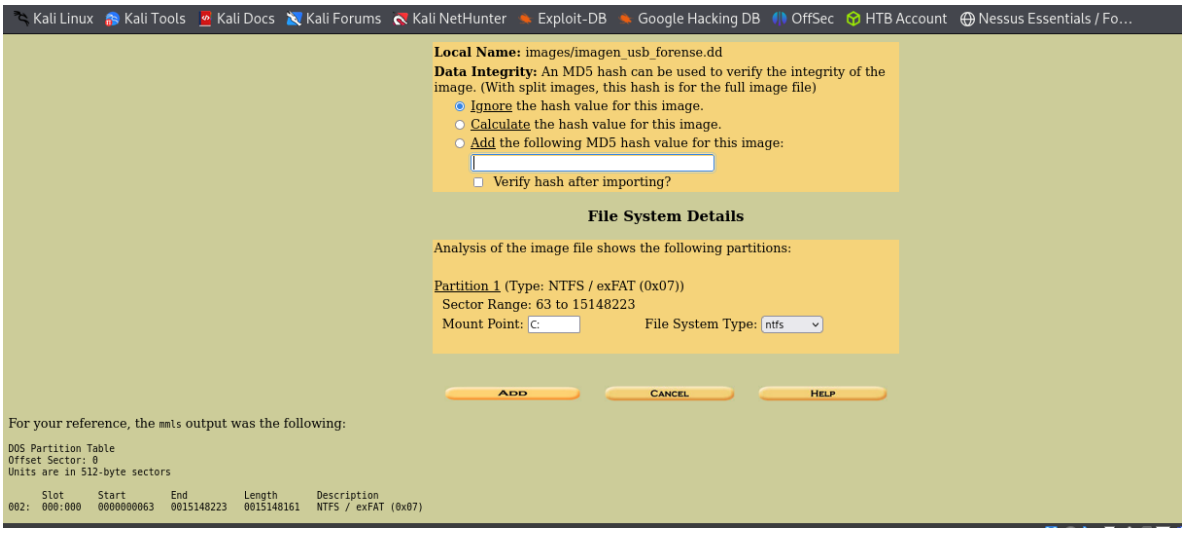

Ilustración 9 Verificación de integridad y configuración del sistema de archivos en Autopsy

En este paso se confirma que la imagen de disco y su volumen asociado fueron añadidos exitosamente al evidencie locker.

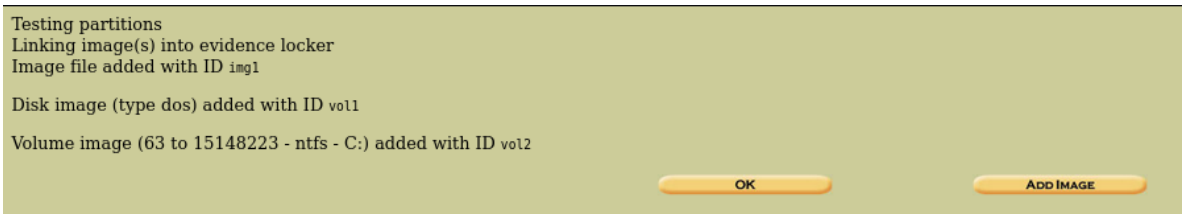

Ilustración 10 Importación exitosa de la imagen forense en Autopsy

La imagen muestra el programa Autopsy con un caso llamado miprimercaso1. Se han cargado discos en formato raw y NTFS para analizarlos, verificar su integridad y usar herramientas como la línea de tiempo y el visor de eventos.

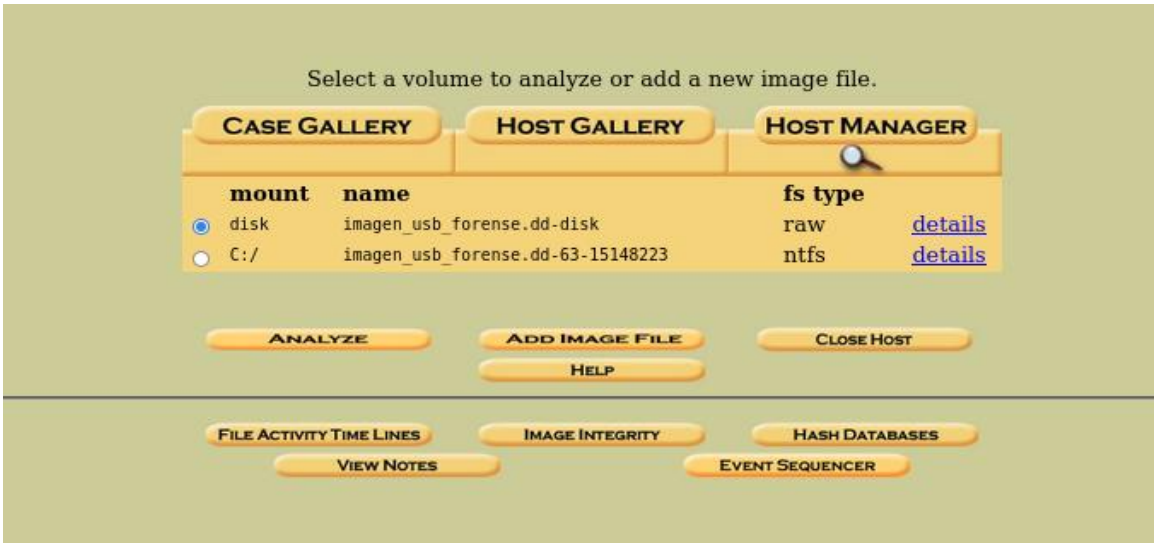

Ilustración 11 Gestión de volúmenes y selección de imagen en Autopsy

Se calcularon los valores MD5 de todos los archivos extraídos de la imagen forense para asegurar que no hayan sido modificados y poder identificarlos de forma única.

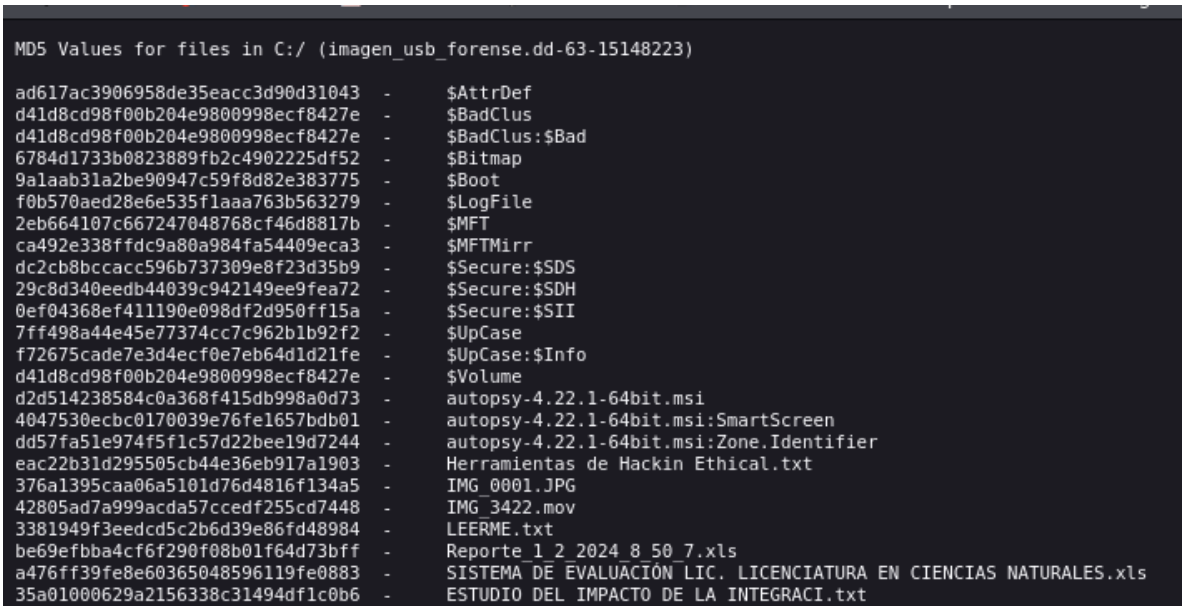

Ilustración 12 erificación de integridad de archivos dentro de la partición analizada

6. CAPITULO 2 AUDITORIA FORENSE CON AUTOPSY EN WINDOWS

6.1. Descargar e instalar autopsy en Windows

Iniciamos descargando e instalando el programa Autopsy para Windows. Entonces debemos ir al buscador de Google y poner descargar Autopsy y nos arrojara varias opciones.

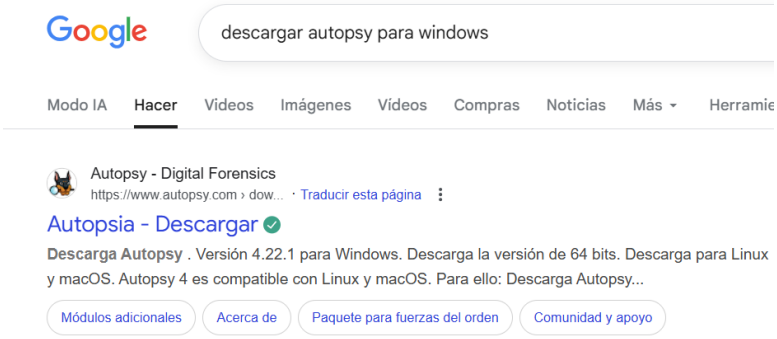

Ilustración 13 buscador de google

Lugo de haber entrado a la pagina vamos a descargar la versión que nos dice que es para Windows.

Ilustración 14 Descarga de Autopsy

Al haber culminado la descarga vamos abrir el archivo y iniciamos con la instalación.

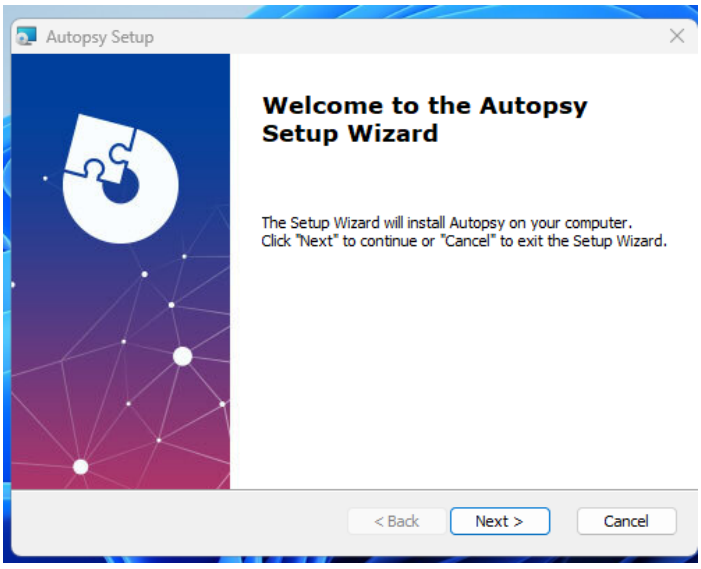

Ilustración 15 Pantalla de bienvenida del instalador de Autopsy

6.2. Creación de un nuevo caso en Autopsy

Ahora vamos a darle en crear nuevo caso.

Ilustración 16 Interfaz principal de bienvenida de Autopsy

En el siguiente paso vamos a configurar los datos del análisis forense que vamos a realizar. Aquí ponemos nombre del caso, la ruta donde se almacenará la información y el tipo de caso.

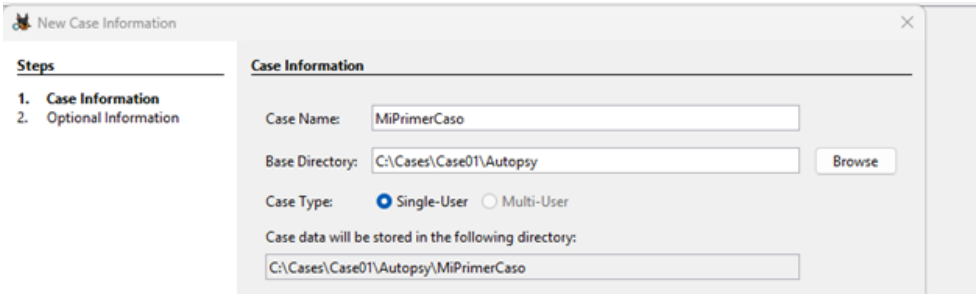

Ilustración 17 Configuración inicial del caso forense en Autopsy

En este paso esta información es opcional.

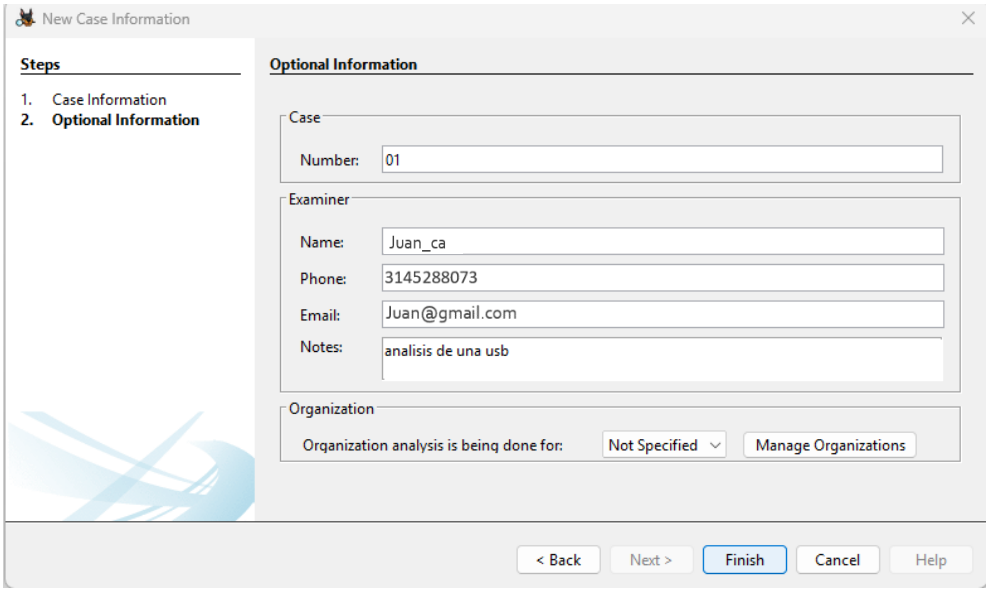

Ilustración 18 Registro de información opcional para el caso forense

En esta etapa se crea o elige un host dentro de Autopsy para asociar y gestionar la imagen o fuente de datos que será analizada en el caso.

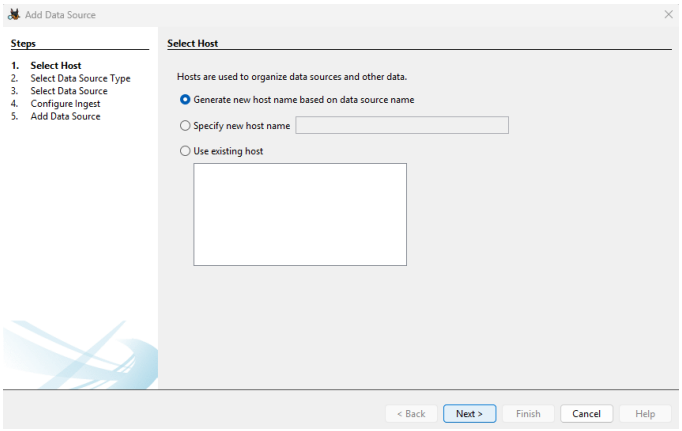

Ilustración 19 Selección de host para la fuente de datos en Autopsy

Aquí el usuario debe elegir qué tipo de evidencia se va a examinar. En este caso, está seleccionada la opción “Disk Image or VM File”, que permite analizar una imagen de disco o un archivo de máquina virtual.

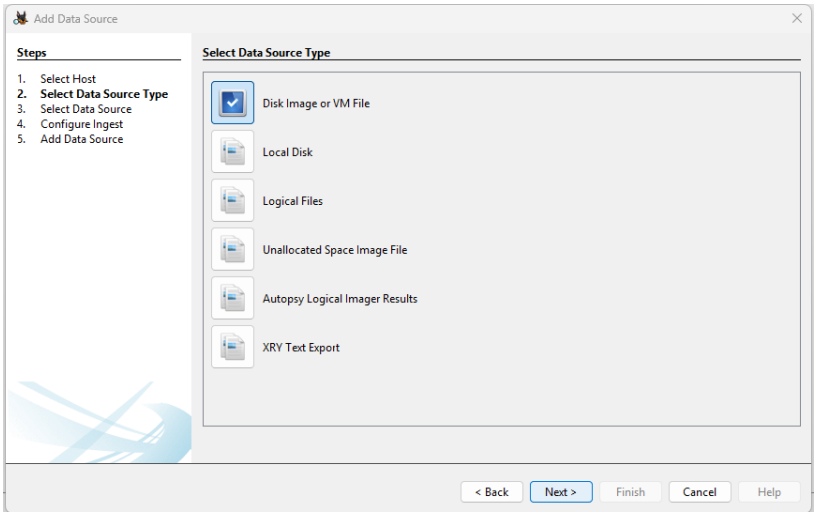

Ilustración 20 Selección del tipo de fuente de datos en Autopsy

Se crea una carpeta compartida.

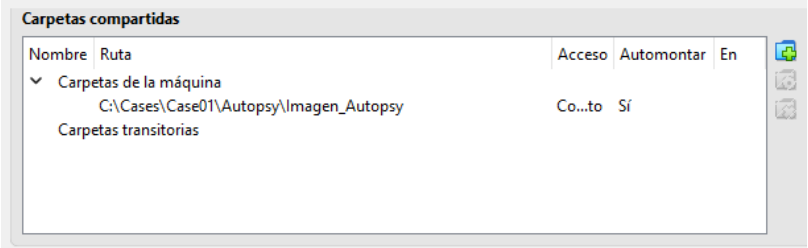

Ilustración 21 Configuración de carpetas compartidas para el análisis forense

Imagen USB forense.dd

Ilustración 22 Archivo de imagen forense (.dd) generado para el análisis

En este paso se elige en Autopsy la imagen forense imagen_usb_forense.dd**,** una copia exacta de un dispositivo USB para su análisis.

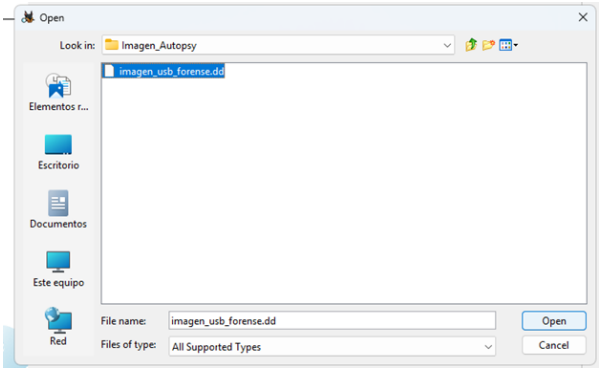

Ilustración 23 Selección de la imagen forense para análisis en Autopsy

En este paso se configura en Autopsy la fuente de datos a analizar, indicando la ruta del archivo **imagen_usb_forense.dd**, la zona horaria (GMT-5:00 América/Bogotá), el tamaño del sector y los hashes opcionales para verificar la integridad de la evidencia.

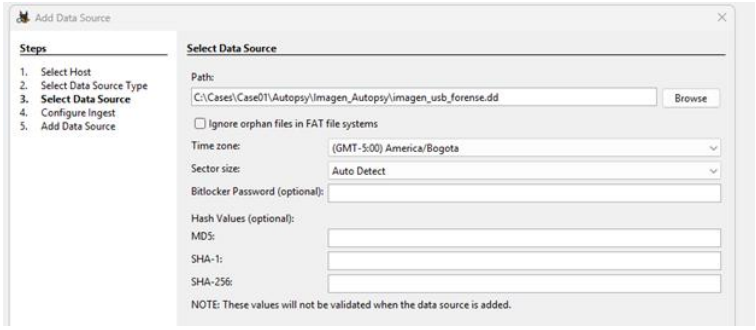

Ilustración 24 Selección de la imagen forense para análisis en Autopsy

En este paso se configuran los módulos de análisis en Autopsy, donde se eligen las herramientas que se aplicarán a la imagen forense, como análisis de archivos, metadatos, malware o datos GPS.

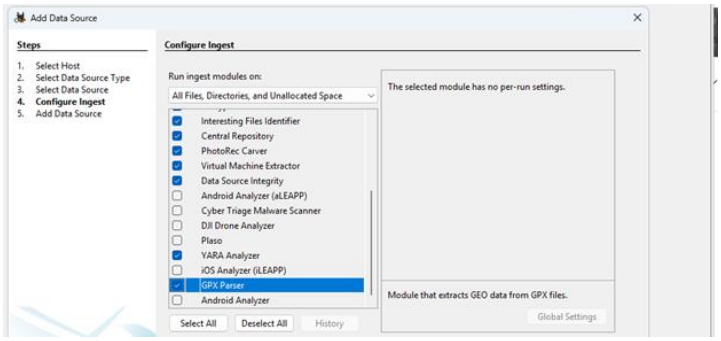

Ilustración 25 Configuración de módulos de análisis (Ingest) en Autopsy

En este paso se muestra una interfaz de análisis tipo visor de registros o correo, enfocada en el directorio megan.smith.framework. Se aprecia información técnica de componentes del

sistema, donde destaca un elemento bloqueado (ícono rojo) con método de entrada y fecha de modificación

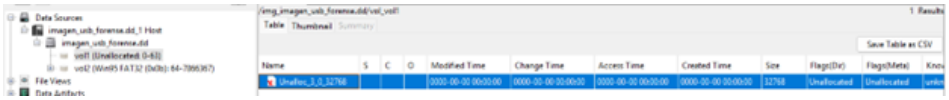

Ilustración 26 Visualización de archivos no asignados en Autopsy

En este paso se visualiza la carpeta **usr/Downloads/4-01** dentro del entorno forense, donde se listan varios archivos (imágenes, documentos y mapas). Todos los metadatos aparecen en ceros, lo que indica posibles datos corruptos o no disponibles, algo común en copias forenses. Esta información ayuda a analizar la actividad del usuario y la integridad de los archivos.

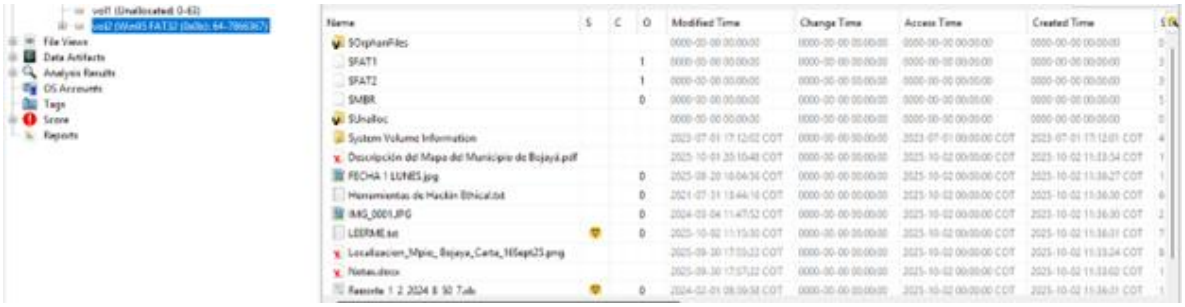

Ilustración 27 Visualización de archivos asignados en el volumen analizado con Autopsy

En este paso se muestra una tabla de análisis del dispositivo USB en la ruta /img_imagen_usb_forense.dd/vol_vol2**,** con columnas como Flags**,** MD5**,** SHA-256 **y** MIME Type**.** Estos datos permiten verificar la integridad y tipo de los archivos, además de identificar

están asignados o no, lo que ayuda a detectar posibles manipulaciones o archivos ocultos.

Flags(Dir)	Flags(Meta)	Known	MD5 Hash	SHA-256 Hash	MIME Type
Allocated	Allocated	unknown			
Allocated	Allocated	unknown	045776a6163054651fbeba5678fa4285	419a9a5c1dac6a0f4db417356f7163b901e86b153c17d4c...	application/octet-stream
Allocated	Allocated	unknown	045776a6163054651fbeba5678fa4285	419a9a5c1dac6a0f4db417356f7163b901e86b153c17d4c...	application/octet-stream
Allocated	Allocated	unknown	eb86354b83081752a48f29b9389066ac	0e59571558b820da819707e655c64705c46520819fc6ef45...	application/octet-stream
Allocated	Allocated	unknown			
Allocated	Allocated	unknown			
Unallocated	Unallocated	unknown	cd33588981ec9d8818c5a6c47cffed1a	a9a71fb7c26b754e390333a8ddc68fa0a73aeb00f015cde...	application/octet-stream
Allocated	Allocated	unknown	ea932dcfa9d3e5da55226d6af80b8cca	d3a70ec7ee03da5b5bf1ce1f49a288c994883d7d2476c6a...	image/jpeg
Allocated	Allocated	unknown	eac22b31d295505cb44e36eb917a1903	55ce69c3839d4b764168702ee933234c0cf9eb7cec57f1a4...	text/plain
Allocated	Allocated	unknown	376a1395caa06a5101d76d4816f134a5	8da775a7590f67e65df38c64e45166531563ef09e2dcac0e...	image/jpeg
Allocated	Allocated	unknown	3381949f3eedcd5c2b6d39e86fd48984	572d315a03649417fb289aed6b425d8a5af346f70e404519...	text/plain
Unallocated	Unallocated	unknown	232de1b6ec01ee8b407175684fba12e6	5b1a6bc2b627fb6a81364cafec91d1a8f43569cdcec7c50...	application/octet-stream

Ilustración 28 Tabla de análisis forense de archivos con valores hash y tipo MIME en Autopsy

7. CONCLUCION

El uso de **Autopsy** en auditoría forense facilita la gestión y análisis de evidencia digital de forma controlada y profesional. En **Linux**, se destaca la flexibilidad del sistema y el uso de comandos para crear y verificar imágenes forenses, mientras que en **Windows**, la interfaz gráfica simplifica la configuración y el análisis de datos. En ambos casos, se logró mantener la integridad de la evidencia mediante el uso de hashes, demostrando que es posible realizar investigaciones digitales efectivas en diferentes entornos operativos. Este tipo de prácticas son esenciales para el desarrollo de habilidades en el ámbito de la **informática forense**, contribuyendo a la comprensión de cómo se preservan y examinan los datos en una investigación real.

8. REFERENCIA

Autopsy Digital Forensics Platform. (2024). The Sleuth Kit and Autopsy Documentation. Recuperado de: https://www.sleuthkit.org/autopsy

Nelson, B., Phillips, A., & Steuart, C. (2020). Guide to Computer Forensics and Investigations (6th ed.). Cengage Learning.

Carvey, H. (2019). Windows Forensic Analysis Toolkit. Elsevier.

Stallings, W. (2021). Computer Security: Principles and Practice. Pearson Education.

Documentación de comandos Linux: fdisk, sha1sum, dd, chmod.