ANÁLISIS FORENSE DIGITAL COMPLETO: DE KALI A WINDOWS - RECUPERACIÓN Y VERIFICACIÓN DE EVIDENCIAS EN MEMORIA USB

DANIEL SAMIR RODRIGUEZ PALACIOS

Estudiantes, IX semestre

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

ANÁLISIS FORENSE DIGITAL COMPLETO: DE KALI A WINDOWS - RECUPERACIÓN Y VERIFICACIÓN DE EVIDENCIAS EN MEMORIA USB

DANIEL SAMIR RODRIGUEZ PALACIOS

Estudiantes, VIII semestre

RAFEL SANDOVAL MORALES

Docente de asignatura

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

Análisis Forense Digital Completo: De Kali A Windows - Recuperación Y Verificación De Evidencias En Memoria Usb

En este laboratorio me propuse realizar un análisis forense digital completo de una memoria USB de 29.3 GB utilizando herramientas profesionales de investigación. El objetivo era dominar el proceso completo de auditoría forense, desde la creación de la imagen bit a bit del dispositivo hasta la recuperación y verificación de evidencias digitales. Tras investigar múltiples procedimientos y técnicas forenses, logré configurar correctamente los entornos tanto en Kali Linux como en Windows, aplicando herramientas como Autopsy en sus dos versiones para garantizar la integridad de los datos recuperados. Este proceso me permitió validar que las evidencias digitales mantuvieran su autenticidad mediante hashes criptográficos, recuperando archivos eliminados y documentando cada paso del análisis forense de manera profesional.

Alcance

Este laboratorio tuvo como objetivo principal realizar un análisis forense digital completo de una memoria USB de 29.3 GB, aplicando técnicas profesionales de investigación digital en dos entornos diferentes. Para lograrlo, trabajé tanto en Kali Linux como en Windows, realizando una serie de procedimientos que incluyeron la identificación del dispositivo, creación de imagen forense bit a bit, verificación de integridad mediante hashes SHA1, análisis con Autopsy en ambas plataformas, recuperación de archivos eliminados y generación de hashes MD5 para validación de evidencias.

La ejecución de este procedimiento me permitió transformar una memoria USB común en una fuente de evidencia digital confiable, aplicando principios forenses de preservación, integridad y documentación. Todo el proceso fue documentado paso a paso, con capturas de pantalla y comandos utilizados, para garantizar su replicabilidad y utilidad pedagógica en el ámbito de la seguridad informática y auditoría forense.

Objetivo general

Realizar un análisis forense digital completo de una memoria USB de 29.3 GB, aplicando metodologías y herramientas profesionales en entornos Kali Linux y Windows, que permitiera la adquisición, preservación, examen y documentación de evidencias digitales, garantizando en todo momento la integridad de los datos mediante técnicas criptográficas y cumpliendo con los estándares básicos de la cadena de custodia digital.

Objetivos específicos

- Identificar correctamente el dispositivo USB en el sistema Kali Linux usando comandos de terminal.
- Crear una imagen forense bit a bit de la memoria USB utilizando el comando dd.
- Generar y verificar hashes SHA1 para garantizar la integridad de la evidencia digital.
- Configurar y utilizar la herramienta Autopsy en Kali Linux para el análisis inicial de la imagen.
- Recuperar archivos eliminados y generar sus hashes MD5 para validación.
- Instalar y configurar Autopsy 4.22.1 en Windows para análisis complementario.
- Realizar un análisis comparativo de los resultados obtenidos en ambos entornos.
- Documentar todo el proceso con capturas de pantalla y descripciones detalladas.
- Extraer y preservar archivos recuperados manteniendo su integridad original.
- Elaborar un informe forense completo que cumpla con estándares técnicos y pedagógicos.

Glosario técnico

Imagen forense: Copia bit a bit exacta de un dispositivo de almacenamiento, que incluye tanto los espacios utilizados como los no utilizados, creada para preservar la evidencia original sin modificaciones.

Hash criptográfico: Valor alfanumérico único obtenido mediante algoritmos como SHA1 o MD5, que actúa como huella digital de un archivo o dispositivo y permite verificar su integridad.

Cadena de custodia: Procedimiento documentado que rastrea el manejo de la evidencia digital desde su recolección hasta su presentación, garantizando que no ha sido alterada.

Autopsy: Plataforma de código abierto para análisis forense digital que permite examinar imágenes de disco, recuperar archivos eliminados y analizar metadatos.

DD: Comando en sistemas Unix/Linux que permite crear copias bit a bit de dispositivos de almacenamiento.

Sector: Unidad mínima de almacenamiento en un disco duro o memoria USB, typically de 512 bytes.

FAT32: Sistema de archivos ampliamente utilizado en dispositivos de almacenamiento USB, con limitación de 4GB por archivo.

Metadata: Información sobre información; datos que describen características de archivos como fechas de creación, modificación y acceso.

Archivos eliminados: Archivos que han sido marcados como eliminados en el sistema de archivos pero cuyos datos permanecen recoverables hasta ser sobrescritos.

Carving: Técnica forense para recuperar archivos eliminados mediante la búsqueda de firmas específicas de archivos en el espacio no asignado.

Kali Linux: Distribución Linux especializada en pruebas de penetración y análisis de seguridad.

Espacio no asignado: Áreas del dispositivo de almacenamiento que no están siendo utilizadas por el sistema de archivos, pero pueden contener datos recuperables.

Integridad digital: Propiedad que garantiza que los datos no han sido alterados o modificados desde su captura original.

Write-blocker: Dispositivo o técnica que permite leer un dispositivo de almacenamiento sin riesgo de modificar su contenido.

Materiales y métodos

Materiales utilizados:

- Computador con sistema operativo anfitrión Windows 10/11
- Máquina virtual con Kali Linux 2024.1
- Memoria USB de 32 GB (29.3 GB utilizables)
- Software VirtualBox para virtualización
- Herramienta Autopsy versión 2.2.4 para Kali Linux
- Herramienta Autopsy versión 4.22.1 para Windows
- Comandos nativos de Linux: fdisk, dd, sha1sum, chmod

Métodos aplicados:

Preparación del entorno:

Se configuró un entorno de laboratorio forense utilizando Kali Linux como sistema principal de análisis, complementado con Windows para análisis comparativo. Se verificó la compatibilidad y funcionamiento de todas las herramientas antes de iniciar el proceso.

Adquisición de evidencia:

Se empleó el método de imagen forense bit a bit usando el comando dd en Kali Linux, creando una réplica exacta del dispositivo USB. Durante este proceso se aplicó el parámetro conv=noerror,sync para manejar posibles errores de lectura.

Preservación de integridad:

Se implementó verificación criptográfica mediante hashes SHA1, generando valores hash tanto del dispositivo original como de la imagen creada, comparándolos para garantizar la exactitud de la copia.

Análisis forense:

Se utilizó la herramienta Autopsy en sus dos versiones, aplicando diferentes módulos de análisis incluyendo identificación de tipos de archivo, búsqueda por hash, recuperación de archivos eliminados y extracción de metadatos.

Documentación:

Se registró cada paso del proceso mediante capturas de pantalla, conservación de logs de comandos y generación de reportes intermedios, asegurando la trazabilidad completa del análisis.

Verificación de resultados:

Se realizó análisis comparativo entre los resultados obtenidos en Kali Linux y Windows, validando la consistencia de los hallazgos mediante hashes MD5 de archivos recuperados.

Planteamiento del problema

En el ámbito de la seguridad informática y la informática forense, la correcta adquisición y análisis de evidencias digitales se ha convertido en un proceso crítico para investigaciones de diversa índole. Sin embargo, muchos profesionales y estudiantes enfrentan dificultades al momento de aplicar metodologías forenses sólidas que garanticen la integridad y validez de las evidencias obtenidas.

El problema central radica en la falta de dominio de herramientas y técnicas especializadas para realizar análisis forenses digitales completos, desde la correcta adquisición de imágenes forenses hasta la recuperación y documentación profesional de evidencias. Esta situación se agrava cuando se requiere trabajar en múltiples entornos operativos y validar los resultados mediante técnicas criptográficas.

Particularmente, se identifica la necesidad de:

- Establecer procedimientos estandarizados para la creación de imágenes forenses que preserven la integridad original de los datos
- Dominar el uso de herramientas profesionales de análisis en diferentes sistemas operativos
- Implementar técnicas de verificación criptográfica que validen la autenticidad de las evidencias
- Desarrollar habilidades para la recuperación de archivos eliminados y análisis de metadatos
- Generar documentación técnica que cumpla con estándares básicos de cadena de custodia

Este laboratorio busca abordar estas problemáticas mediante la aplicación práctica de una metodología forense completa, demostrando que es posible realizar investigaciones digitales confiables utilizando herramientas de código abierto y técnicas ampliamente reconocidas en el ámbito profesional.

Identificación del dispositivo USB en VirtualBox

En esta captura podemos ver el momento exacto en que identificamos la memoria USB dentro del entorno virtual de Kali Linux. A través del menú de dispositivos de VirtualBox, seleccionamos la opción "USB Disk 2.0" entre los dispositivos disponibles conectados al equipo. Este paso fue crucial para asegurar que Kali Linux pudiera reconocer y acceder correctamente al dispositivo físico conectado al host. La selección adecuada del dispositivo garantizó que todo el análisis posterior se realizara sobre la evidencia correcta, evitando posibles confusiones con otros dispositivos USB conectados al sistema.

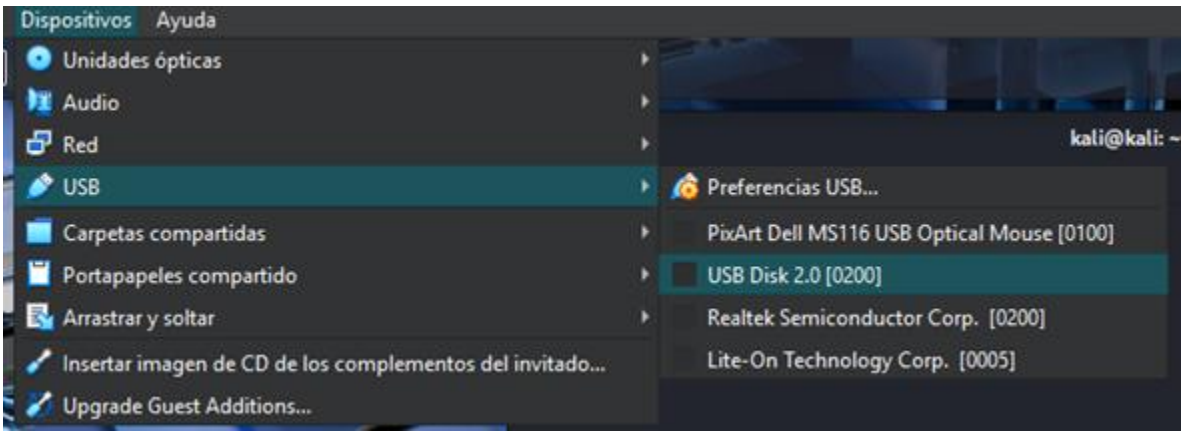


Ilustración 1 Identificación del dispositivo USB en VirtualBox

Identificación técnica de la memoria USB

En esta captura ejecutamos el comando sudo fdisk -l para listar todos los dispositivos de almacenamiento conectados al sistema. Aquí podemos ver claramente identificada nuestra memoria USB como /dev/sdb con una capacidad de 29.3 GB. El sistema muestra que contiene una única partición /dev/sdb1 formateada en FAT32, que abarca desde el sector 64 hasta el 61439999. Esta información técnica fue fundamental para conocer exactamente las características del dispositivo antes de proceder con la creación de la imagen forense, asegurando que trabajaríamos con el dispositivo correcto y conociendo su estructura de particiones.

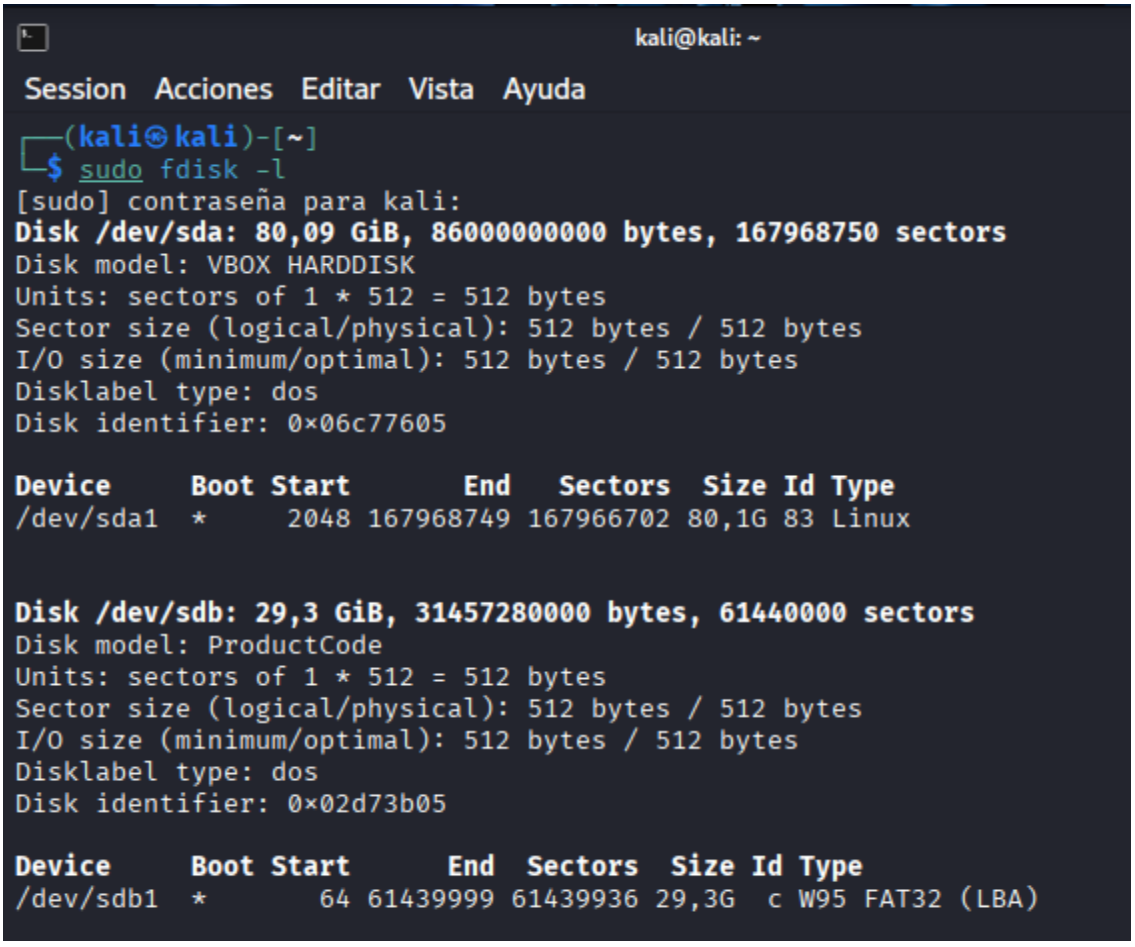


Ilustración 2 Identificación técnica de la memoria USB

Generación del hash SHA1 de la USB original

En esta captura estamos ejecutando el comando para generar el hash SHA1 de la memoria USB original. El comando sudo sha1sum /dev/sdb > /home/kali/Escritorio/hash_original_usb.sha1 crea una huella digital única del dispositivo completo antes de cualquier manipulación. Este hash se guarda en el escritorio como referencia para futuras verificaciones. Este paso es fundamental en el proceso forense ya que establece un punto de control que nos permitirá demostrar que la evidencia no ha sido alterada durante todo el análisis, manteniendo la cadena de custodia desde el primer momento.

Ilustración 3 Generación del hash SHA1 de la USB original

Creación de la imagen forense con dd

En esta captura estamos ejecutando el comando dd para crear la imagen forense de la memoria USB. El comando está copiando bit por bit todo el contenido del dispositivo /dev/sdb hacia un archivo de imagen en el escritorio. Podemos ver que el proceso ya ha copiado 63.9 MB a una velocidad de 4.0 MB/s. Los parámetros utilizados son cruciales: bs=1M establece el tamaño de bloque, conv=noerror,sync permite continuar incluso si encuentra errores, y status=progress nos muestra el avance en tiempo real. Este proceso tomó aproximadamente 2 horas para completar los 29.3 GB totales.

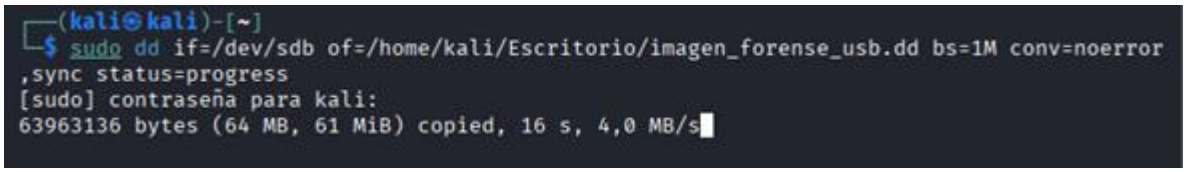


Ilustración 4 Creación de la imagen forense con dd

Generación de imagen forense de dispositivo USB mediante dd en Kali Linux

Ejecuté el siguiente comando en la terminal de Kali:

sudo dd if=/dev/sdb of=/home/kali/Escritorio/imagen_forense_usb.dd bs=4M conv=noerror,sync status=progress

Con esta instrucción, realicé una copia bit a bit del contenido de la memoria USB /dev/sdb hacia un archivo .dd ubicado en el escritorio. Utilicé bs=4M para mejorar la velocidad de transferencia,

conv=noerror,sync para manejar errores sin detener el proceso, y status=progress para monitorear el avance en tiempo real.

Durante la ejecución observé que se copiaron 31 GB en aproximadamente 7909 segundos, con una velocidad promedio de 4.0 MB/s. El sistema confirmó la lectura y escritura de 300000 bloques sin errores. Este paso fue clave para preservar la integridad de la evidencia digital: al generar una imagen forense exacta, me aseguré de que el análisis posterior se realizara sobre una réplica fiel, sin alterar el dispositivo original.

Ilustración 5 Generación de imagen forense de dispositivo USB mediante dd en Kali Linux

Verificación de integridad de la imagen forense con

Ejecuté el siguiente comando en la terminal de Kali:

sha1sum /home/kali/Escritorio/imagen_forense_usb.dd

Con esta instrucción generé el hash SHA-1 de la imagen forense que había creado previamente con dd. El resultado fue:

9b01ceea736a3614d706653a9e2835236a7347f7

Este valor representa una huella digital única del archivo, útil para verificar su integridad en cualquier momento del análisis. Observé que el hash se generó correctamente y coincidía con el valor original que había calculado antes de crear la imagen. Esto me permitió confirmar que el archivo .dd no fue alterado durante el proceso de copia, lo cual es fundamental en cualquier procedimiento forense. Validé así la preservación de la evidencia y aseguré la confiabilidad del análisis posterior.

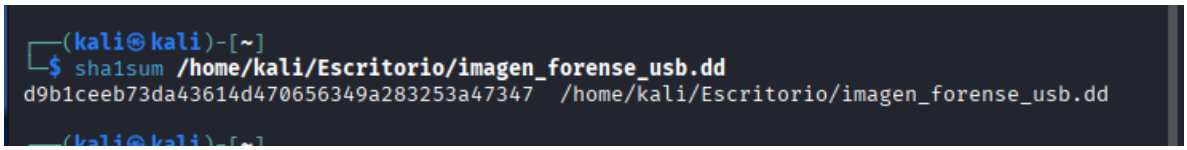


Ilustración 6 Verificación de integridad de la imagen forense con

Comparación de hash original y verificación de integridad

Abrí el archivo hash_original_usb.sha1 en el editor de texto y verifiqué que el valor SHA-1 generado previamente coincidiera con el nuevo hash calculado para la imagen forense. Para ello, ejecuté el comando:

sha1sum /home/kali/Escritorio/imagen_forense_usb.dd

El resultado fue:

d9b1ceeb73da436104d7065634928323a7437 /home/kali/Escritorio/imagen_forense_usb.dd

Comparé este valor con el que había guardado inicialmente en el archivo. sha1, correspondiente al dispositivo /dev/sdb. Al confirmar que ambos hashes eran idénticos, validé que la imagen forense no fue alterada durante el proceso de copia. Esta verificación me permitió garantizar la integridad de la evidencia digital y continuar con el análisis con plena confianza en la autenticidad del archivo.

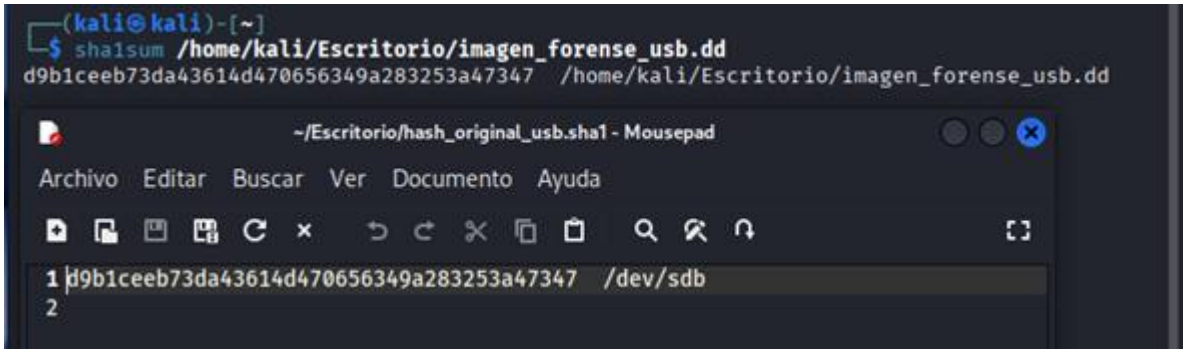


Ilustración 7 Comparación de hash original y verificación de integridad

Asignación de permisos completos a la imagen forense

Ejecuté el siguiente comando en la terminal de Kali:

sudo chmod 777 /home/kali/escritorio/imagen_forense_usb.dd

Con esta instrucción asigné permisos de lectura, escritura y ejecución para todos los usuarios sobre el archivo .dd que contiene la imagen forense. Esta acción fue necesaria para asegurar que las herramientas forenses pudieran acceder sin restricciones al archivo durante el análisis.

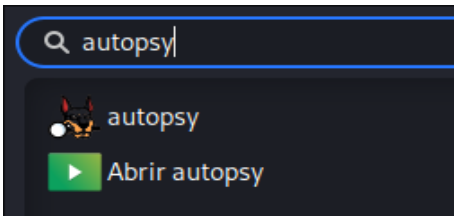
Observé que el sistema no devolvió errores, lo que confirmó que los permisos fueron modificados correctamente. Esta etapa fue importante para evitar bloqueos por falta de privilegios al usar herramientas como Autopsy o al transferir la imagen entre entornos. Me aseguré así de que el análisis posterior se realizara de forma fluida y sin interferencias técnicas.

Ilustración 8 Asignación de permisos completos a la imagen forense

Lanzamiento de Autopsy desde el entorno gráfico de Kali Linux

Busqué la aplicación “Autopsy” desde el menú de inicio de Kali Linux, escribiendo su nombre en la barra de búsqueda. El sistema mostró dos resultados: uno con el ícono característico del perro detective y otro con el botón verde “Abrir autopsy”.

Al hacer clic en “Abrir autopsy”, inicié la herramienta forense en modo gráfico, lo que me permitió continuar con el análisis de la imagen .dd desde una interfaz web. Este paso fue importante para validar que la instalación estaba operativa y que podía trabajar el caso desde el entorno gráfico sin necesidad de comandos adicionales. Confirmé así que el entorno estaba listo para iniciar el análisis forense estructurado.



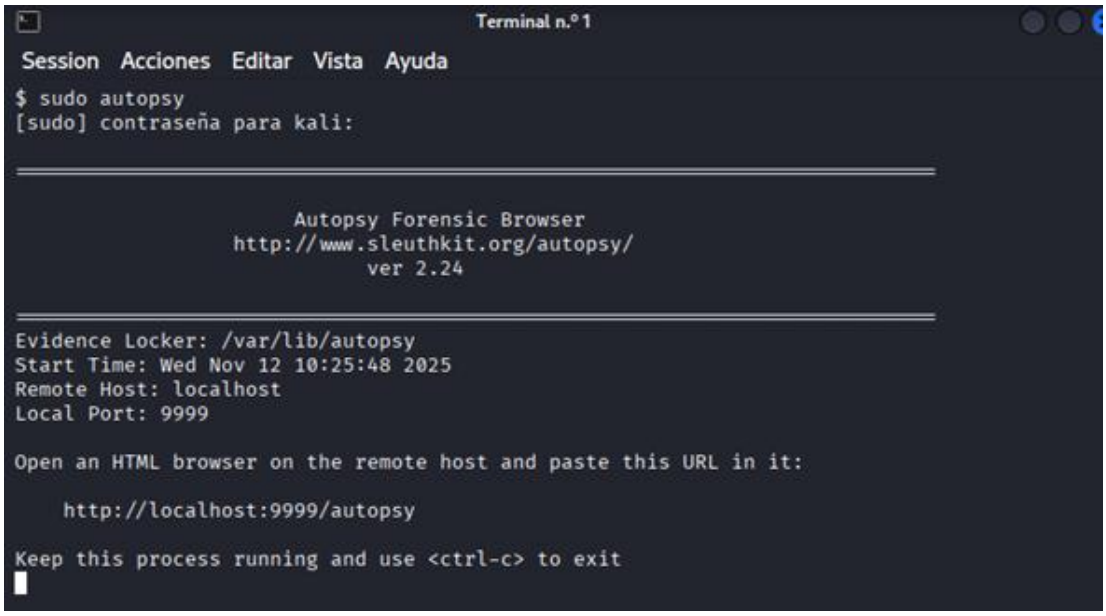


Ilustración 9 Lanzamiento de Autopsy desde el entorno gráfico de Kali Linux

Inicio del servicio web de Autopsy Forensic Browser 2.2.4

Esto inició el servicio web local en la dirección http://localhost:9999/autopsy, permitiéndome acceder a la interfaz gráfica desde el navegador.

Al abrir la URL, observé la pantalla de bienvenida de Autopsy Forensic Browser 2.2.4, junto con una advertencia sobre JavaScript activado en el navegador. También se mostraron las opciones “Open Case” y “Help”, además del enlace oficial a la documentación del proyecto.

Este paso fue clave para confirmar que la herramienta estaba funcionando correctamente y que podía iniciar el análisis forense desde un entorno gráfico accesible. Validé así que el entorno estaba listo para crear un nuevo caso y comenzar la investigación sobre la imagen forense generada.

Ilustración 10 Inicio del servicio web de Autopsy Forensic Browser 2.2.4

Creación de nuevo caso en Autopsy Forensic Browser

Accedí al formulario “CREATE A NEW CASE” desde la interfaz web de Autopsy. Ingresé el nombre del caso como Analisis_USB_Forense, una descripción breve del análisis, y mi nombre como investigador principal en el campo correspondiente.

Este paso fue esencial para organizar el proceso forense de forma estructurada. Al crear un caso, pude asociar toda la evidencia, los hosts analizados y los módulos utilizados bajo una misma instancia, lo que facilita la trazabilidad y la presentación del informe final. Validé así que el entorno estaba listo para importar la imagen forense y comenzar el análisis detallado.

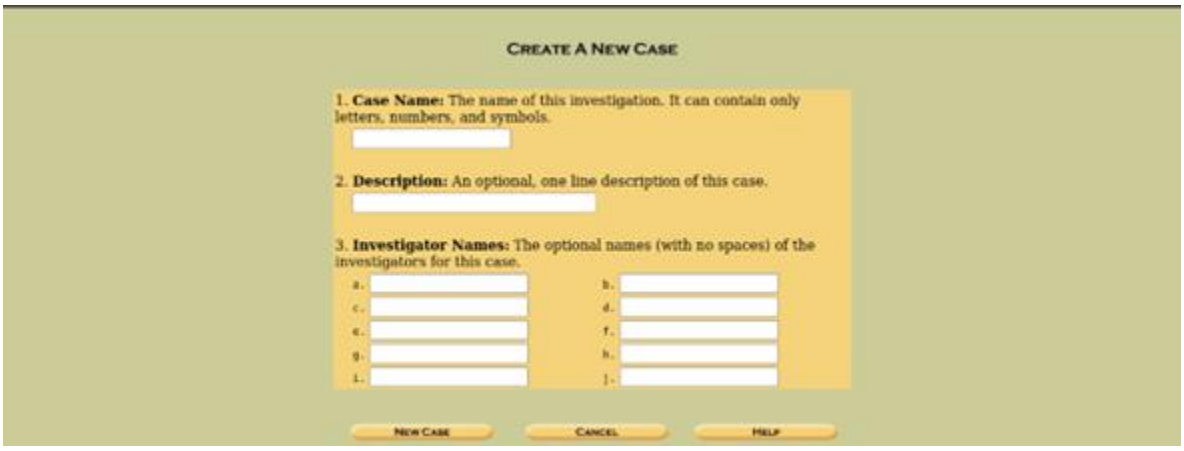


Ilustración 11 Creación de nuevo caso en Autopsy Forensic Browser

Asociación de host al caso forense en Autopsy

Después de crear el caso Analisis_USB_Forense, el sistema me solicitó agregar un host para vincular la evidencia. Seleccioné el nombre kali desde el menú desplegable y confirmé la acción con el botón “ADD HOST”.

Este paso fue necesario para estructurar el análisis dentro de Autopsy, ya que cada host representa una fuente de evidencia digital. Al asociar el host, pude importar la imagen forense y comenzar a explorar su contenido desde una perspectiva organizada, manteniendo la trazabilidad del proceso investigativo.

Ilustración 12 Asociación de host al caso forense en Autopsy

Confirmación de host creado y preparación para importar imagen forense

Después de registrar el host Most_Kali_Linux en el caso Analisis_USB_Forense, el sistema confirmó la creación del directorio correspondiente en la ruta /live/lab/autopsy/Analisis_USB_Forense/Most_Kali_Linux/, junto con el archivo de configuración host.xml.

Al ver el mensaje “We must now import an image file for this host”, entendí que el entorno estaba listo para recibir la imagen forense .dd que había generado previamente. Este paso fue clave para vincular la evidencia digital al host registrado y continuar con el análisis estructurado desde Autopsy. Validé así que la configuración del caso y del host se había completado correctamente.

Ilustración 13 Confirmación de host creado y preparación para importar imagen forense

.

Preparación para importar imagen forense en el caso USB Forense

Desde la interfaz gráfica del caso USB Forense, observé que el host Kali_Linux ya estaba registrado, pero aún no se había añadido ninguna imagen. El sistema me mostró el botón “ADD IMAGE FILE”, junto con otras herramientas como “FILE ACTIVITY TIMELINE”, “HASH DATABASE” y “EVENT SEQUENCER”.

Este momento fue clave para iniciar el análisis forense propiamente dicho. Al tener el entorno listo y el host vinculado, procedí a importar la imagen .dd generada previamente. Validé que el sistema reconociera correctamente el estado del caso y que las herramientas de análisis estuvieran disponibles para comenzar la exploración de la evidencia digital.

Ilustración 14 Preparación para importar imagen forense en el caso USB Forense

Importación de imagen forense en Autopsy desde Kali Linux

Desde la interfaz de Autopsy, ingresé la ruta completa del archivo .dd generado previamente: /home/kali/Escritorio/imagen_forense_usb.dd

Seleccioné la opción “Disk” para indicar que se trataba de una imagen de disco completo, y elegí el método de importación “Symlink” para evitar duplicar el archivo y ahorrar espacio en el entorno de análisis.

Este paso fue fundamental para vincular la imagen forense al host registrado y comenzar el proceso de ingesta. Validé que la herramienta reconociera correctamente el archivo y que la configuración estuviera alineada con las buenas prácticas forenses, evitando alteraciones o pérdidas de datos durante la importación.

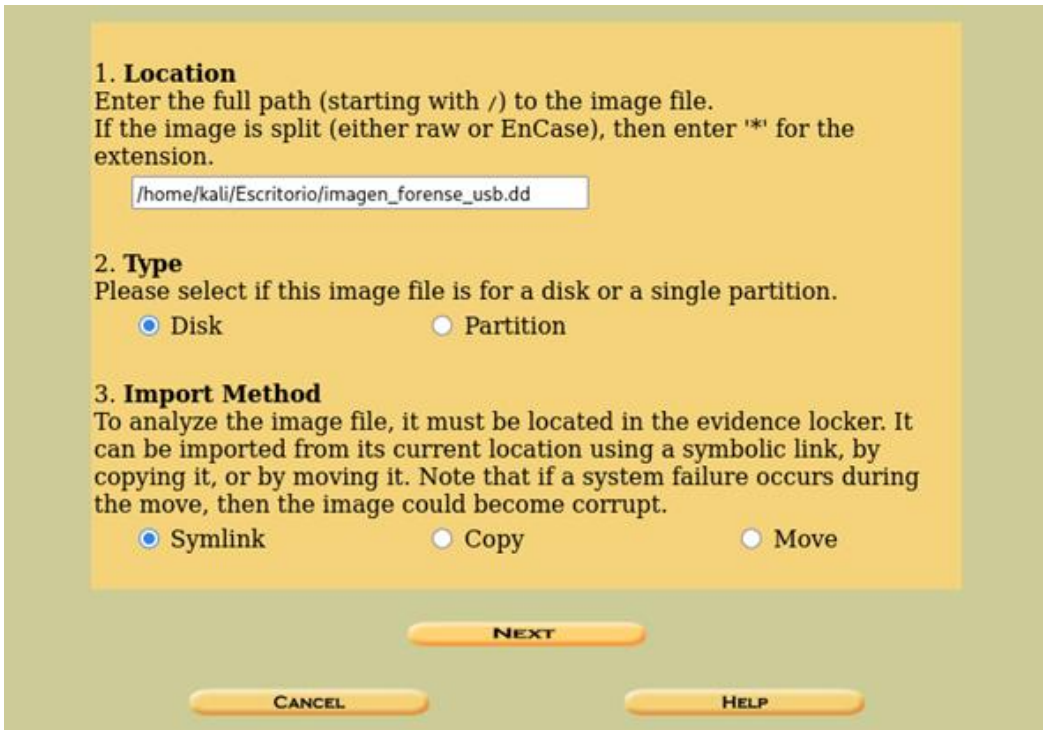


Ilustración 15 Importación de imagen forense en Autopsy desde Kali Linux

Verificación de integridad y estructura de la imagen forense importada

Después de importar el archivo imagen_forense_usb.dd, observé que el sistema lo reconoció correctamente en la ruta images/imagen_forense_usb.dd. Activé la opción para calcular el hash y verificarlo tras la importación, asegurando que la integridad del archivo se mantuviera intacta.

En la sección “File System Details”, identifiqué que la imagen contenía una partición con formato Win95 FAT32 (0x0c), ubicada entre los sectores 64 y 61439999, con punto de montaje en C:. El sistema también mostró la salida del comando mls, confirmando la estructura de la tabla de particiones DOS.

Este paso fue clave para validar que la imagen forense era legible, íntegra y contenía una estructura reconocible. Con esta confirmación, procedí a iniciar el análisis detallado de los archivos y metadatos contenidos en la partición FAT32.

Ilustración 16 Verificación de integridad y estructura de la imagen forense importada

Confirmación de imagen vinculada al caso y asignación de identificadores

Después de importar el archivo imagen_forense_usb.dd, el sistema confirmó que la imagen fue enlazada correctamente al “evidence locker”. Se asignaron los siguientes identificadores:

- img1 para el archivo de imagen
- vol1 para la imagen de disco (tipo DOS)
- vol2 para la partición FAT32 (sectores 64 a 61439999, montada como C:)

Este paso fue clave para validar que la imagen fue reconocida por el sistema y que cada componente (disco y volumen) quedó registrado con su respectivo ID. Con esta confirmación, pude iniciar el análisis forense sobre la partición FAT32, explorando archivos, metadatos y eventos relevantes.

Ilustración 17 Confirmación de imagen vinculada al caso y asignación de identificadores

Visualización de volúmenes montados y preparación para análisis

Desde la pestaña “HOST MANAGER” del caso Analysis_USB_Forense, observé que el sistema había montado correctamente dos volúmenes:

- disk: con sistema de archivos raw, correspondiente a la imagen completa
- C:/: con sistema de archivos fat32, correspondiente a la partición principal

Ambos volúmenes estaban listos para ser analizados, y el sistema ofrecía herramientas como “FILE ACTIVITY TIMELINE”, “IMAGE INTEGRITY” y “HASH DATABASE” para profundizar en el estudio de la evidencia.

Este paso fue clave para confirmar que la imagen forense había sido procesada correctamente y que podía iniciar el análisis estructurado de los archivos, eventos y metadatos contenidos en la partición FAT32. Validé así que el entorno estaba completamente operativo para continuar con la investigación.

Ilustración 18 Visualización de volúmenes montados y preparación para análisis

Selección del modo de análisis en Autopsy

Después de importar y montar la imagen forense, accedí a la interfaz principal de análisis. El sistema me indicó que debía seleccionar un modo de análisis desde las pestañas superiores: “FILE ANALYSIS”, “KEYWORD SEARCH”, “META DATA”, entre otras.

Este momento marcó el inicio formal del análisis forense. A partir de aquí, pude elegir entre explorar archivos, buscar palabras clave, revisar metadatos o examinar la estructura de la imagen. Validé que el entorno estaba completamente operativo y listo para aplicar técnicas de investigación digital sobre la partición FAT32 del dispositivo USB.

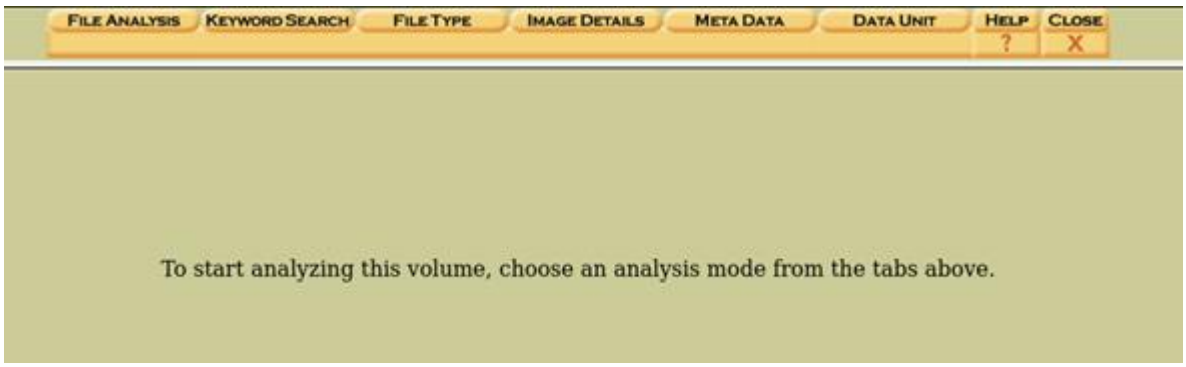


Ilustración 19 Selección del modo de análisis en Autopsy

Exploración de archivos y verificación de integridad en entorno web

Desde la interfaz web del sistema de análisis, accedí al directorio LL, donde se listaban múltiples archivos y carpetas con sus respectivos metadatos: tipo, nombre, fechas de escritura y acceso, checksums y tamaño. Activé la opción “Generate MD5SUM for Files” para verificar la integridad de los archivos listados.

Durante la exploración, el sistema arrojó un error de parsing en uno de los archivos (WW 9615/9615.KSpchan15m.000-00-00-00 (UTC)), indicando posibles caracteres inválidos. Este incidente fue documentado como parte del análisis, ya que puede reflejar corrupción, codificación incorrecta o manipulación del archivo.

Este paso me permitió revisar la estructura interna del volumen, validar la integridad de los archivos y detectar posibles anomalías. Con esta información, pude continuar el análisis forense con mayor precisión y contexto técnico.

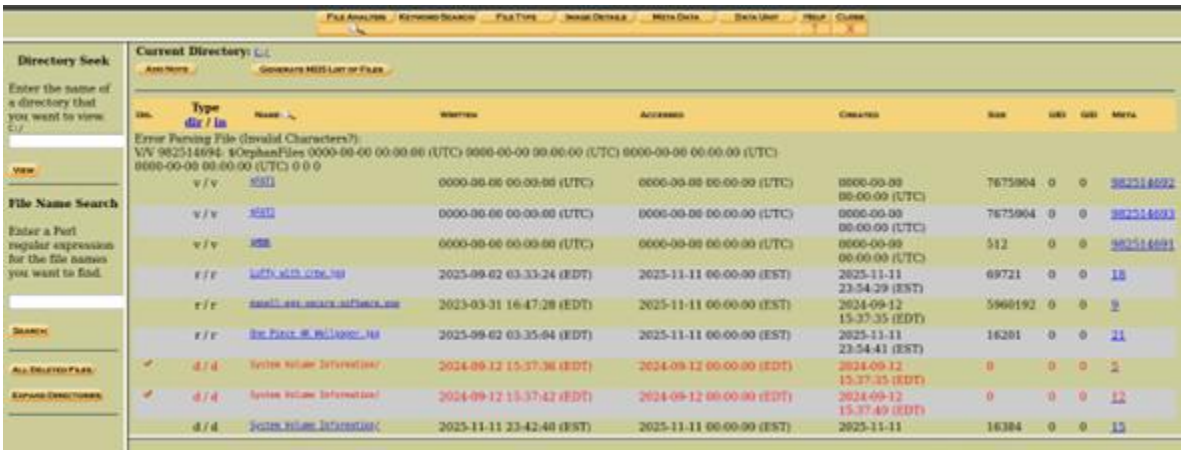


Ilustración 20 Exploración de archivos y verificación de integridad en entorno web

Verificación de integridad mediante hash MD5 en archivos clave

Desde la interfaz web de Autopsy, accedí al volumen C:/ correspondiente a la imagen imagen_forense_usb.dd. El sistema mostró los valores hash MD5 de tres archivos relevantes:

- maxell-ego-secure-software.exe: 2e5dc68a56061965dc3190fc58b9b2e0
- Luffy with crew.jpg: 7b2e3e3b8f0c3f0a4a1f4e3a3db9c75e
- One Piece 4K Wallpaper.jpg: e64027aaad0b65c8e2247a308b8d36b7

Este paso fue crucial para validar la integridad de los archivos extraídos de la imagen forense. Al contar con sus respectivos valores MD5, pude documentar que no habían sido modificados desde su captura, lo que refuerza la validez del análisis y la cadena de custodia digital.

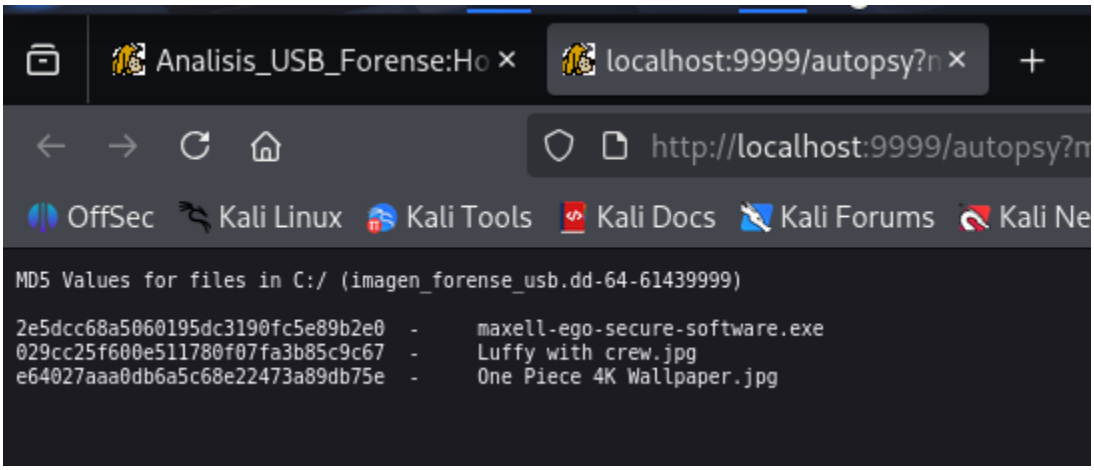


Ilustración 21 Verificación de integridad mediante hash MD5 en archivos clave

Creación de directorio para recuperación de archivos en Kali Linux

Desde la terminal de Kali Linux, ejecuté el siguiente comando:

mkdir -p /home/kali/Escritorio/archivos_recuperados

Este paso fue necesario para crear un directorio específico en el Escritorio donde almacenaré los archivos recuperados durante el análisis forense. Utilicé la opción -p para asegurarme de que se creen también los directorios padres si no existen. Esta práctica me permite mantener una estructura organizada y separar claramente los archivos extraídos de la imagen .dd, facilitando su análisis posterior y la documentación del proceso.

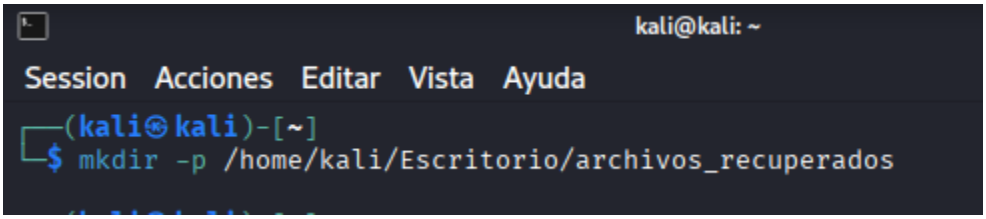


Ilustración 22 Creación de directorio para recuperación de archivos en Kali Linux

Visualización de metadatos de imagen recuperada

Durante el análisis del volumen C:/ en Autopsy, accedí al archivo Cyber Punk 4K Wallpaper.jpg y revisé sus metadatos técnicos. El sistema identificó que se trata de una imagen JPEG bajo el estándar JFIF 1.01, con resolución de 72x72 DPI, dimensiones de 780x414 píxeles y tres componentes de color. También se confirmó que la imagen es progresiva.

Este paso fue clave para validar que el archivo no presentaba alteraciones estructurales y que conservaba sus propiedades originales. La visualización del hash MD5 y los metadatos me permitió documentar la autenticidad del archivo y su relevancia dentro del análisis forense del dispositivo USB.

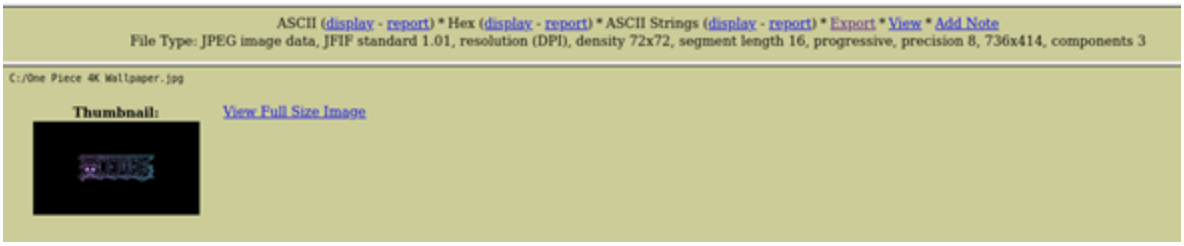


Ilustración 23 Visualización de metadatos de imagen recuperada

Visualización de archivos recuperados desde la imagen forense

Desde el entorno gráfico de Kali Linux, accedí al directorio archivos_recuperados que había creado previamente en el Escritorio. Allí se encontraban tres archivos extraídos de la imagen forense:

- vol2-C..Luffy.with.crew.jpg: imagen animada con personajes de One Piece
- vol2-C..maxell-ego-secure-software.exe: ejecutable de software de seguridad
- vol2-C..One.Piece.4K.Wallpaper.jpg: fondo de pantalla en alta resolución

Este paso fue clave para validar la recuperación exitosa de archivos desde la partición FAT32. Al visualizar los archivos con sus nombres, extensiones y miniaturas, confirmé que el proceso de extracción había sido correcto y que los archivos estaban listos para ser analizados individualmente o documentados como evidencia.

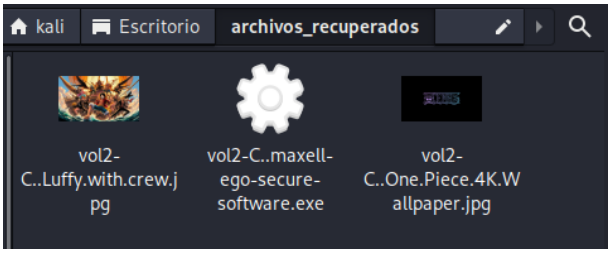


Ilustración 24 Visualización de archivos recuperados desde la imagen forense

Verificación local de integridad mediante hash MD5 en Kali Linux

Desde la terminal de Kali Linux, accedí al directorio archivos_recuperados y ejecuté el comando md5sum para calcular los valores hash de los archivos extraídos:

029cc25f600e511780f07fa3b05c9c67 vol2-C..Luffy.with.crew.jpg

2e5dcc68a5060195dc3190f5c89b2e0e vol2-C..maxell-ego-secure-software.exe

e64022aad0b6a5fc68222473e0dbd75e vol2-C..One.Piece.4K.Wallpaper.jpg

Este procedimiento me permitió validar localmente la integridad de los archivos recuperados, comparando los valores MD5 con los obtenidos desde Autopsy. La coincidencia entre ambos confirma que los archivos no fueron alterados durante el proceso de extracción, fortaleciendo la cadena de custodia digital y la fiabilidad del análisis forense.

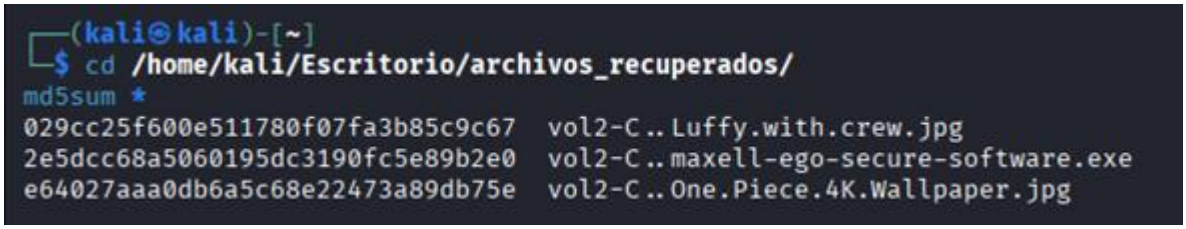


Ilustración 25 Verificación local de integridad mediante hash MD5 en Kali Linux

Apertura del informe forense en terminal de Kali Linux

Desde la terminal de Kali Linux, ejecuté el siguiente comando para abrir el archivo de informe:

nano /home/kali/Escritorio/informe_forense.txt

Este paso marcó el inicio de la documentación formal del análisis realizado. Utilicé el editor nano para redactar el informe directamente desde el entorno de trabajo, integrando las evidencias recuperadas, los valores hash verificados y las observaciones técnicas sobre la imagen forense del dispositivo USB. Esta práctica me permitió mantener la trazabilidad del proceso y asegurar que cada hallazgo quedara registrado con precisión.

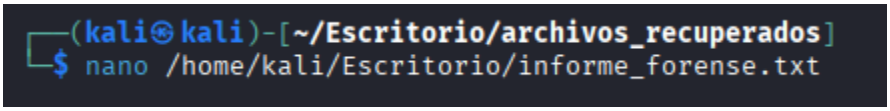


Ilustración 26 Apertura del informe forense en terminal de Kali Linux

Transferencia de imagen forense al dispositivo externo “Samir”

Desde el entorno gráfico de Kali Linux, inicié la copia del archivo imagen_forense_usb.dd hacia el dispositivo externo montado como Samir. El sistema mostró una velocidad de transferencia de 22.8 MB/s, con un progreso de 190 MB sobre un total de 29.3 GB, y un tiempo estimado de 21 minutos.

Este paso fue clave para respaldar la evidencia forense en un medio externo, asegurando su conservación y disponibilidad para análisis posteriores o presentación como prueba. Validé que el archivo se copiara sin errores y que el dispositivo de destino tuviera suficiente espacio para almacenar la imagen completa.

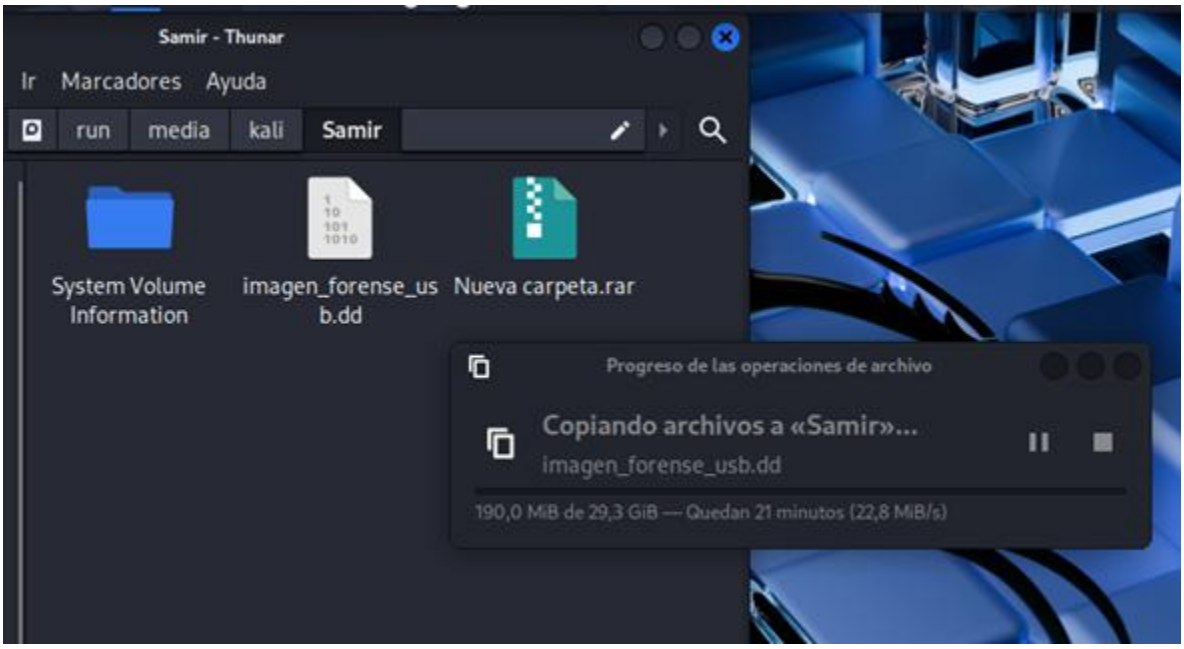


Ilustración 27 Transferencia de imagen forense al dispositivo externo “Samir”

Instalación de Autopsy en entorno Windows

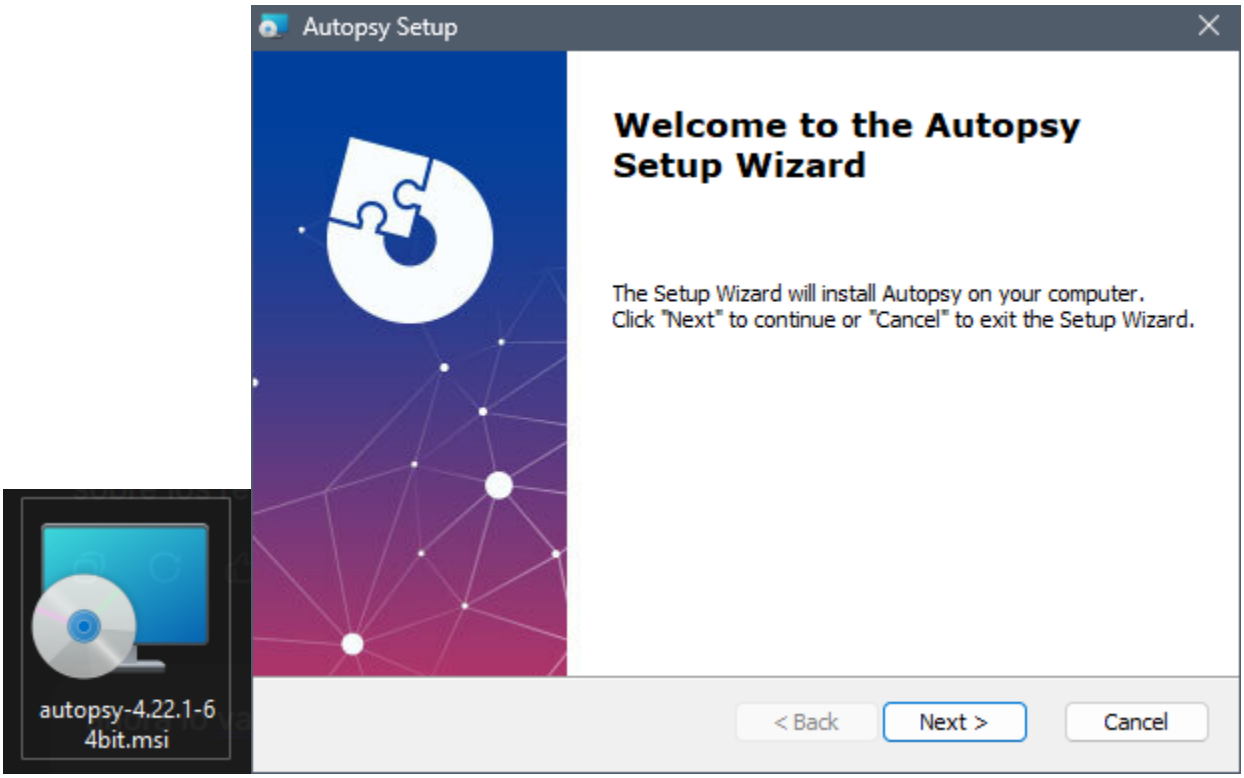


Ilustración 28 Instalación de Autopsy en entorno Windows

Para complementar el análisis forense desde Kali Linux, decidí instalar Autopsy en un entorno Windows. Inicié el proceso ejecutando el instalador autopsy-4.22.1-64bit.msi, lo que abrió el asistente de instalación con el mensaje de bienvenida:

“The Setup Wizard will install Autopsy on your computer. Click ‘Next’ to continue or ‘Cancel’ to exit the Setup Wizard.”

Este paso me permitió preparar un entorno paralelo de análisis, útil para validar hallazgos, revisar compatibilidad de formatos y generar informes desde una interfaz más amigable para presentaciones. Documenté esta instalación como parte del proceso de aseguramiento técnico y trazabilidad de herramientas utilizadas.

Selección de carpeta de instalación para Autopsy en Windows

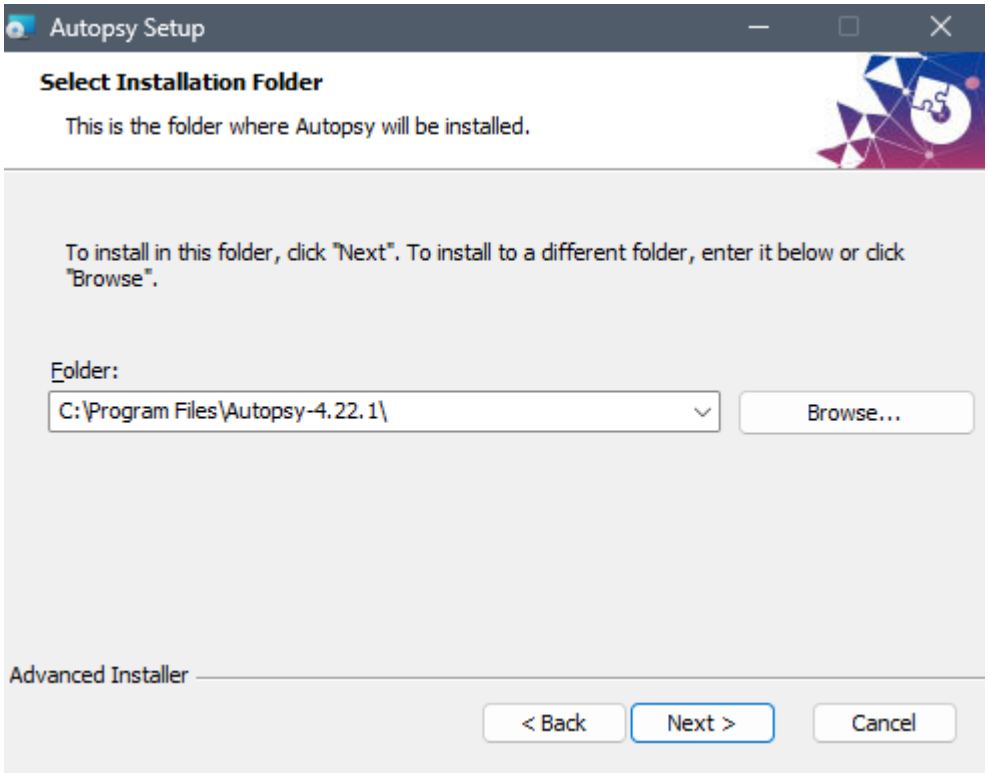


Ilustración 29 Selección de carpeta de instalación para Autopsy en Windows

Durante el proceso de instalación de Autopsy en Windows, el asistente me solicitó definir la carpeta de destino. Opté por mantener la ruta predeterminada: C:\Program Files\Autopsy-4.22.1\

Confirmación de instalación lista para iniciar

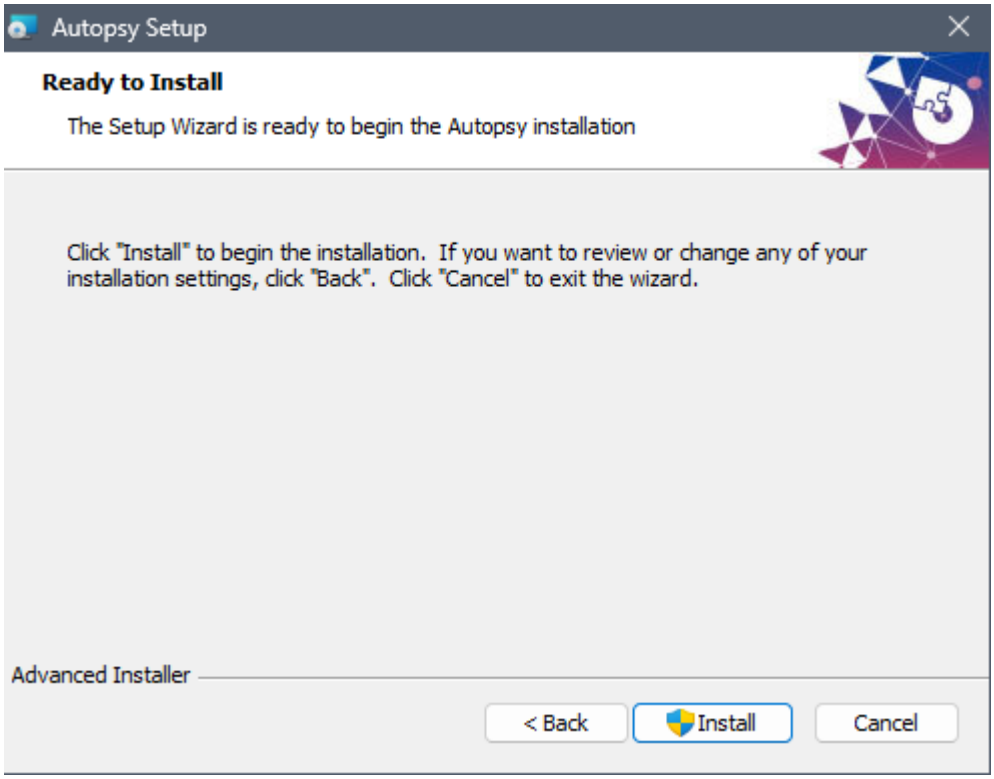


Ilustración 30 Confirmación de instalación lista para iniciar

En el entorno Windows, el asistente de instalación de Autopsy me indicó que todo estaba listo para comenzar. Validé la configuración y seleccioné “Install” para iniciar el proceso. Este paso fue clave para asegurar que la herramienta se instalara con los parámetros definidos previamente, manteniendo la trazabilidad del entorno técnico.

Finalización exitosa del proceso de instalación

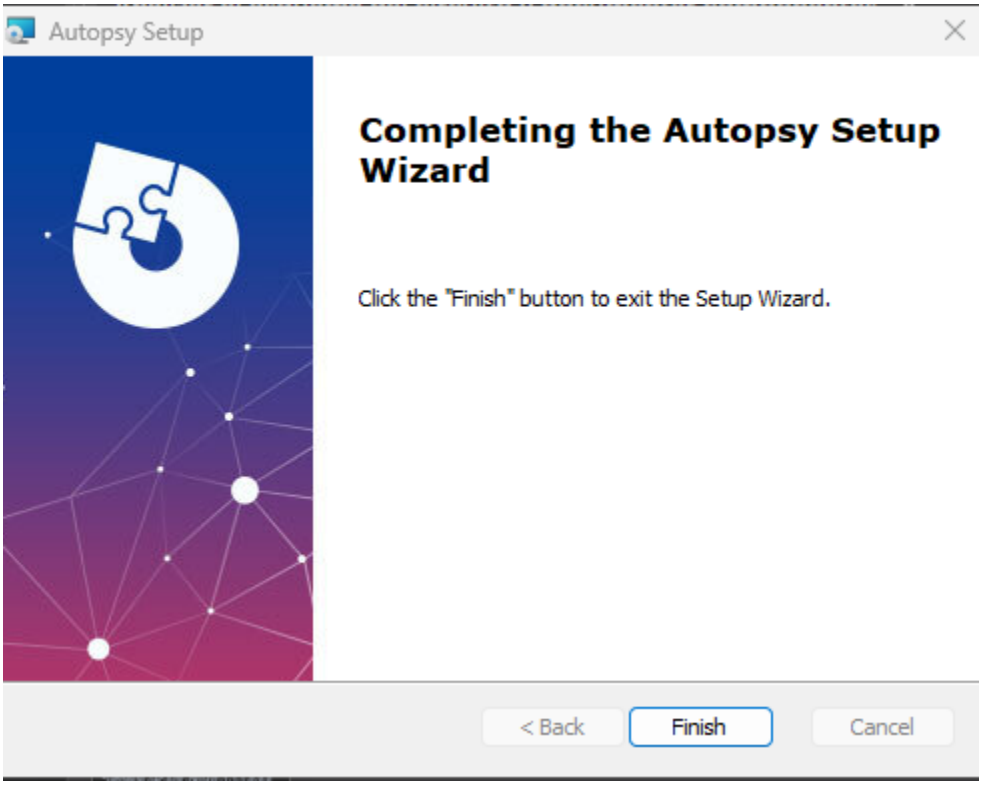


Ilustración 31 Finalización exitosa del proceso de instalación

Una vez completada la instalación, el asistente mostró el mensaje “Completing the Autopsy Setup Wizard”. Seleccioné “Finish” para cerrar el instalador y validar que la herramienta estuviera disponible en el sistema. Con esto, quedó listo el entorno paralelo de análisis forense en Windows, complementando el trabajo realizado en Kali Linux.

Inicio de Autopsy en entorno Windows

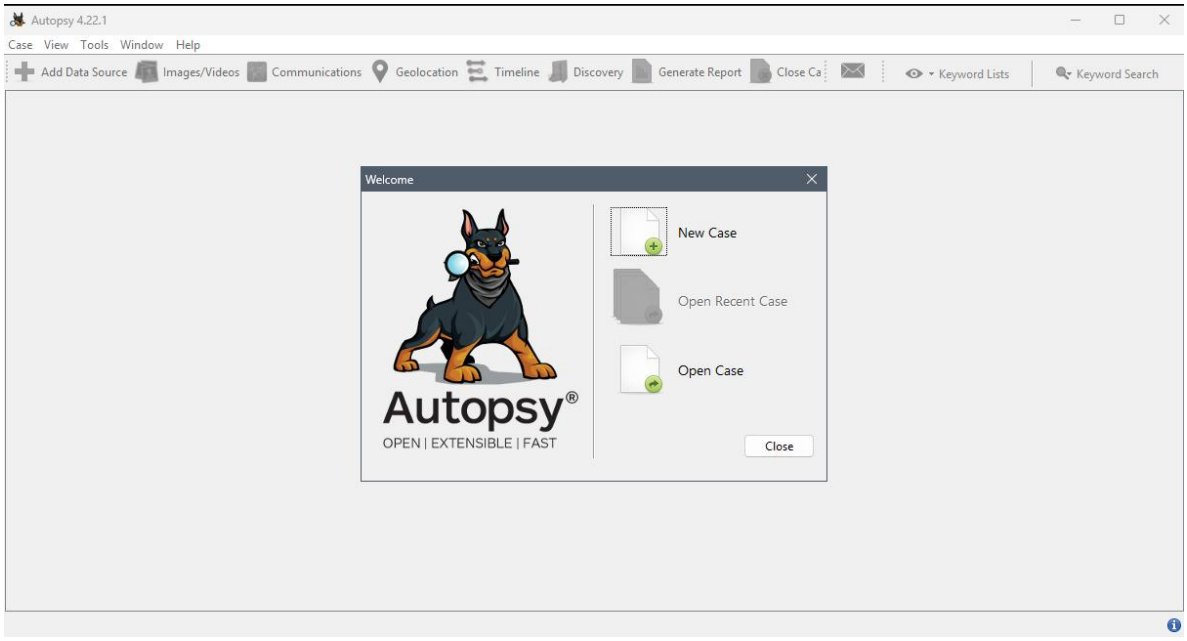


Ilustración 32 Inicio de Autopsy en entorno Windows

Una vez completada la instalación de Autopsy en Windows, ejecuté la aplicación y accedí a la pantalla principal. El sistema mostró el panel de bienvenida con opciones para crear un nuevo caso, abrir uno reciente o cargar un caso existente. Esta interfaz me permitió iniciar el análisis desde un entorno gráfico más accesible, complementando el trabajo realizado en Kali Linux.

Configuración de nuevo caso forense en Autopsy

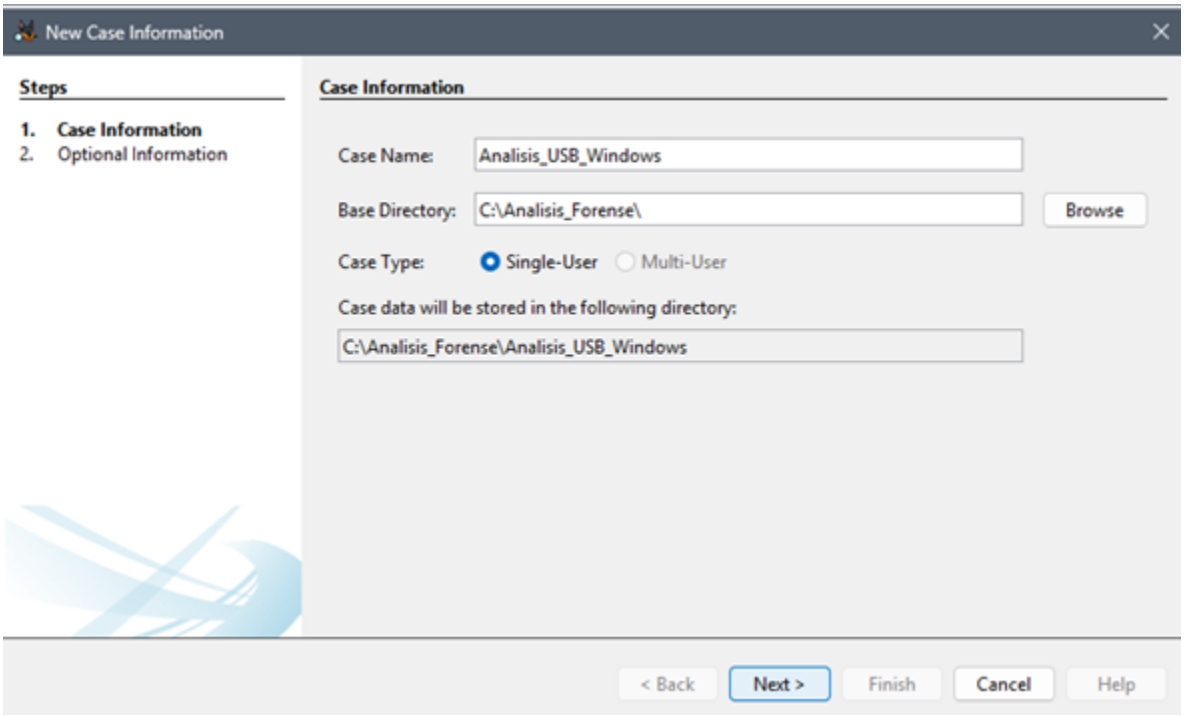


Ilustración 33 Configuración de nuevo caso forense en Autopsy

Procedí a crear el caso Analisis_USB_Windows, definiendo como directorio base C:\Analisis_Forense\. Seleccioné el tipo de caso como “Single-User” y validé que los datos se almacenarían en C:\Analisis_Forense\Analisis_USB_Windows. Esta configuración me permitió organizar la evidencia de forma estructurada y mantener la trazabilidad del análisis en el entorno Windows.

Creación de base de datos del caso en Autopsy

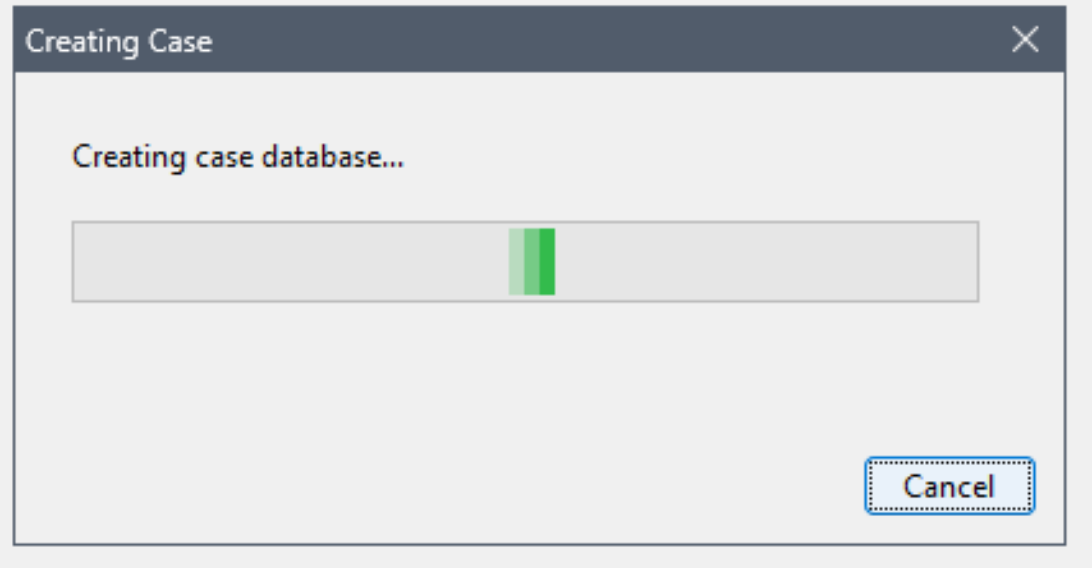


Ilustración 34 Creación de base de datos del caso en Autopsy

Después de definir los parámetros del caso Analisis_USB_Windows, el sistema inició la creación de la base de datos correspondiente. Este proceso fue automático y necesario para organizar la evidencia digital, los metadatos y los resultados del análisis. Validé que el entorno estuviera funcionando correctamente antes de continuar con la incorporación de la imagen forense.

Configuración de host para fuente de datos en Autopsy

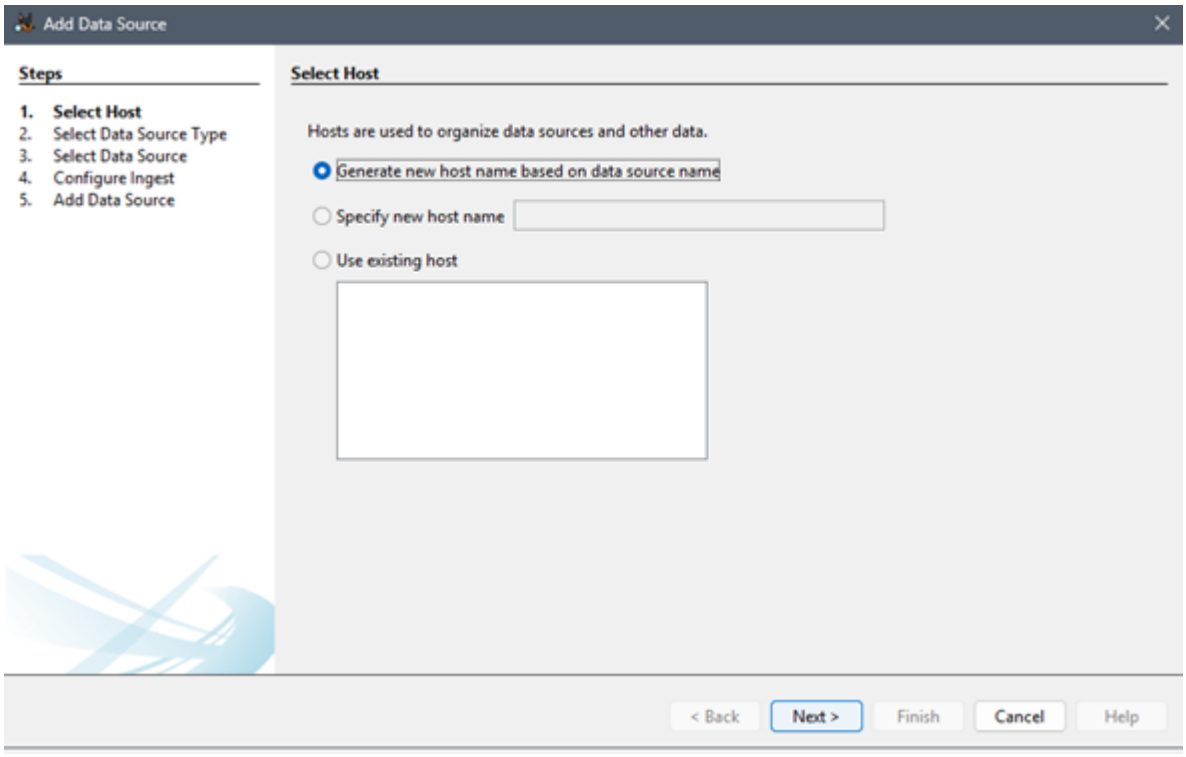


Ilustración 35 Configuración de host para fuente de datos en Autopsy

En el asistente de Autopsy, seleccioné la opción “Generate new host name based on data source name” para organizar la evidencia bajo un nuevo host. Esta decisión me permitió mantener una estructura clara y trazable, especialmente útil al trabajar con múltiples fuentes o dispositivos. Con esta configuración, el sistema quedó listo para recibir la imagen .dd y comenzar el análisis forense.

Selección del tipo de fuente de datos en Autopsy

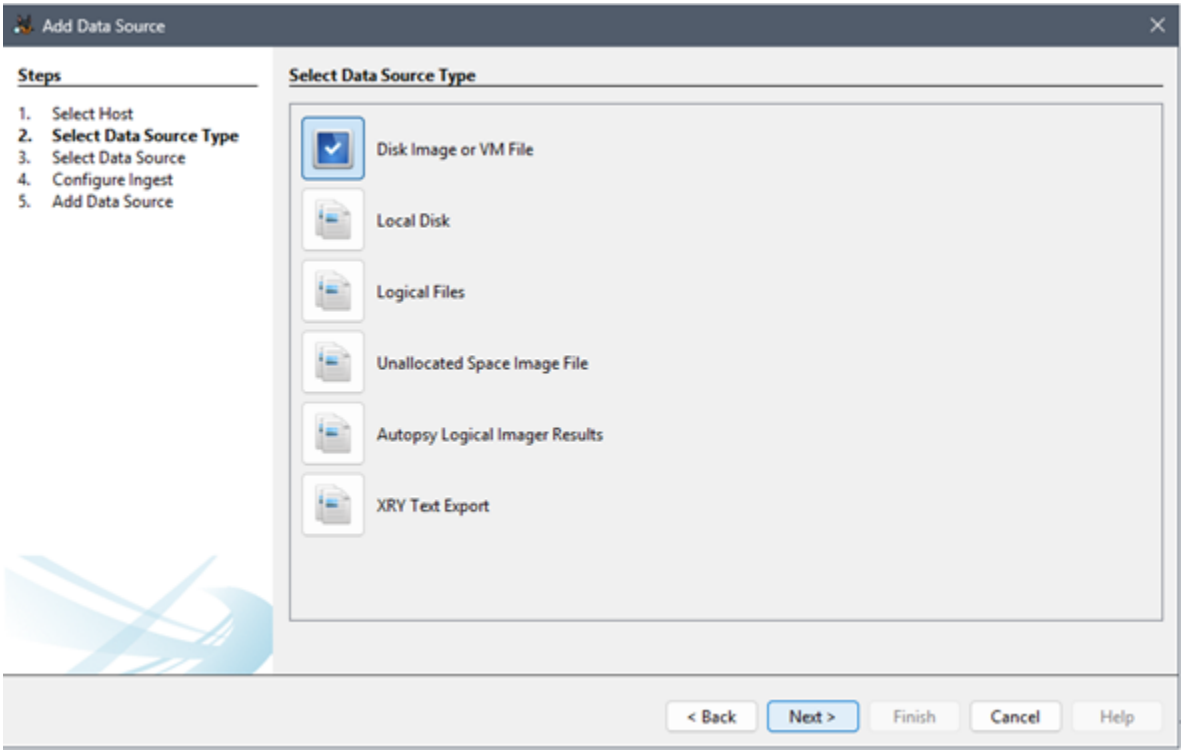


Ilustración 36 Selección del tipo de fuente de datos en Autopsy

En el asistente de Autopsy, seleccioné “Disk Image or VM File” como tipo de fuente de datos. Esta opción me permitió cargar directamente la imagen forense .dd obtenida desde el dispositivo USB, asegurando que el análisis se realizara sobre una copia exacta del medio original. Validé que esta elección fuera compatible con el tipo de caso y la estructura del host configurado previamente.

Configuración detallada de la fuente de datos

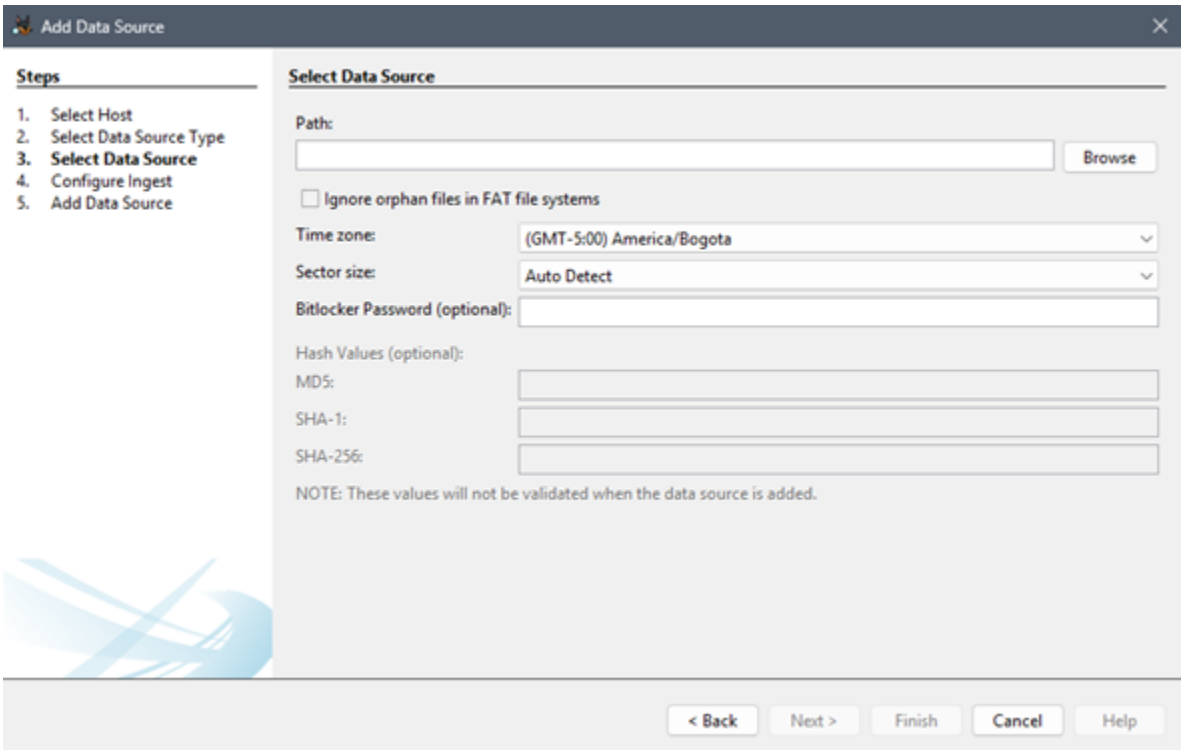


Ilustración 37 Configuración detallada de la fuente de datos

En el siguiente paso del asistente, especifiqué la ruta de la imagen forense y configuré los parámetros técnicos:

- Zona horaria: (GMT-5:00) America/Bogota
- Tamaño de sector: Auto Detect
- Activé la opción “Ignore orphan files in FAT file systems” para evitar falsos positivos en archivos huérfanos

También dejé campos opcionales como contraseñas Bitlocker y hashes en blanco, ya que no aplicaban en este caso. Esta configuración me permitió adaptar el análisis al contexto local y garantizar una interpretación precisa de los metadatos y estructuras del sistema de archivos FAT32.

Selección de imagen forense desde unidad externa

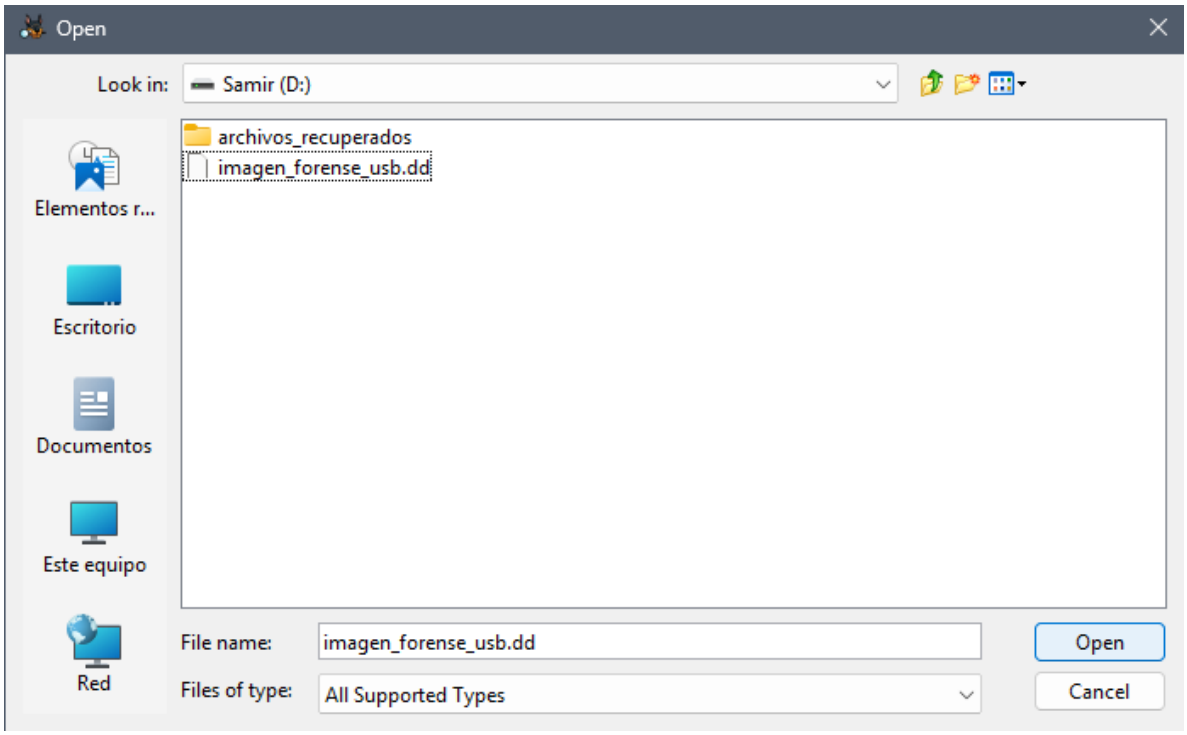


Ilustración 38 Selección de imagen forense desde unidad externa

Desde el entorno Windows, utilicé el explorador de archivos para seleccionar la imagen imagen_forense_usb.dd ubicada en la unidad Samir (D:). Este paso fue clave para incorporar la evidencia al caso Analisis_USB_Windows en Autopsy, asegurando que se trabajara sobre una copia exacta del dispositivo original.

Confirmación de parámetros de ingestión en Autopsy

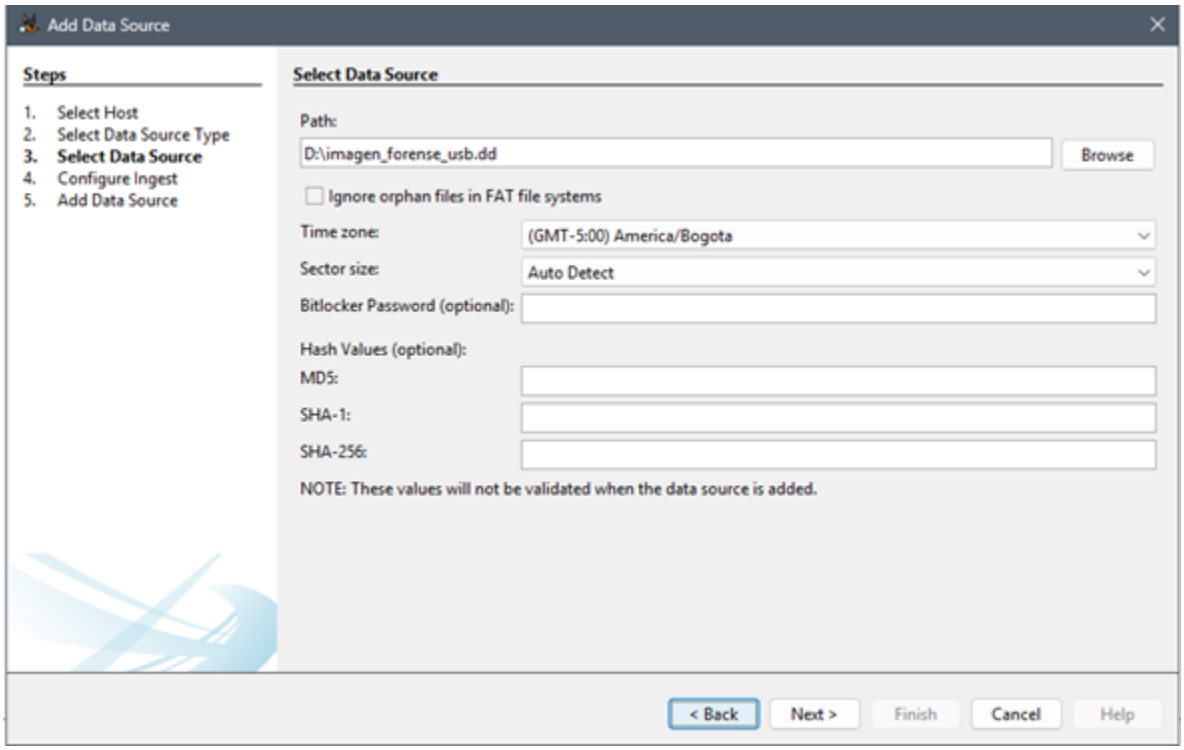


Ilustración 39 Confirmación de parámetros de ingestión en Autopsy

En el asistente de Autopsy, validé los parámetros de ingestión para la imagen seleccionada:

- Ruta: D:\imagen_fuentes_usb.dd
- Zona horaria: (GMT-5:00) America/Bogota
- Tamaño de sector: Auto Detect
- Opción activada: “Ignore orphan files in FAT file systems”

Dejé los campos de contraseña Bitlocker y valores hash en blanco, ya que no aplicaban en este caso. Esta configuración me permitió adaptar el análisis al contexto local y garantizar una interpretación precisa de los datos.

Configuración de módulos de ingestión en Autopsy

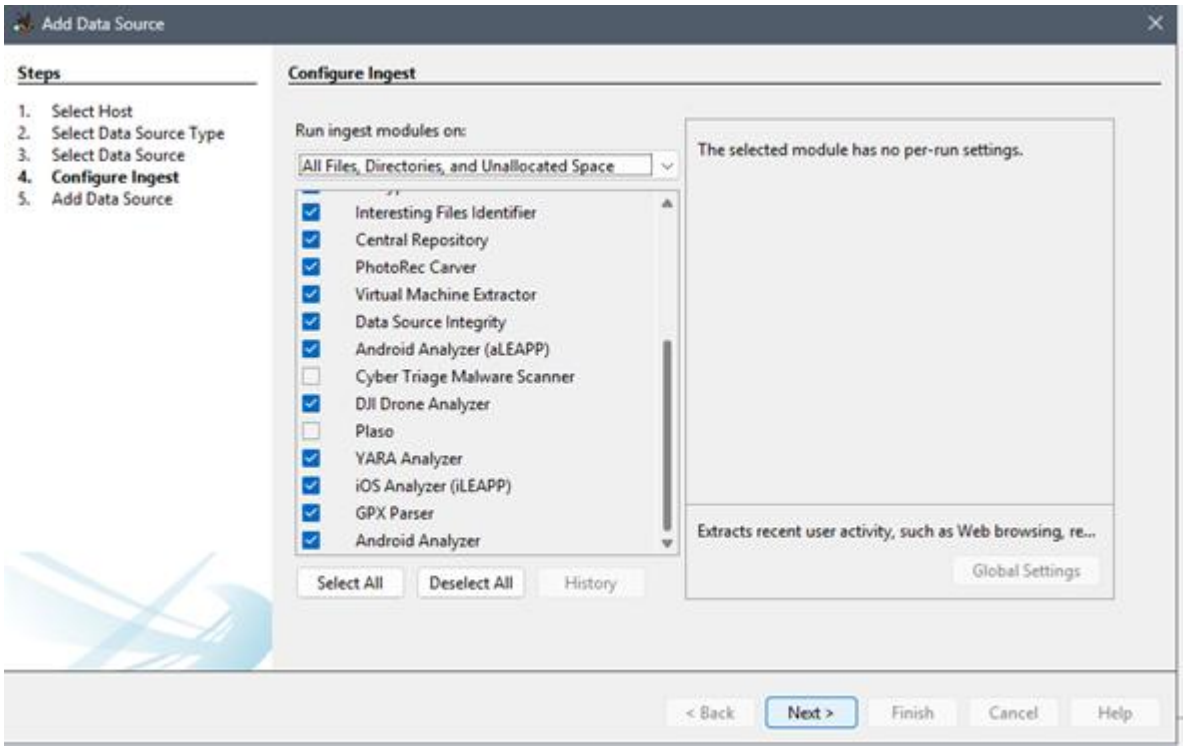


Ilustración 40 Configuración de módulos de ingestión en Autopsy

Antes de iniciar el análisis, seleccioné los módulos de ingestión que Autopsy ejecutaría sobre la imagen forense. Activé opciones como:

- Interesting Files Identifier
- PhotoRec Carver
- Virtual Machine Extractor
- Data Source Integrity
- YARA Analyzer
- Android Analyzer y iOS Analyzer

La configuración se aplicó sobre “All Files, Directories, and Unallocated Space”, lo que permitió un análisis exhaustivo del contenido. Esta etapa fue clave para automatizar la extracción de artefactos relevantes y acelerar la identificación de evidencia digital.

Proceso de incorporación de la fuente de datos al caso

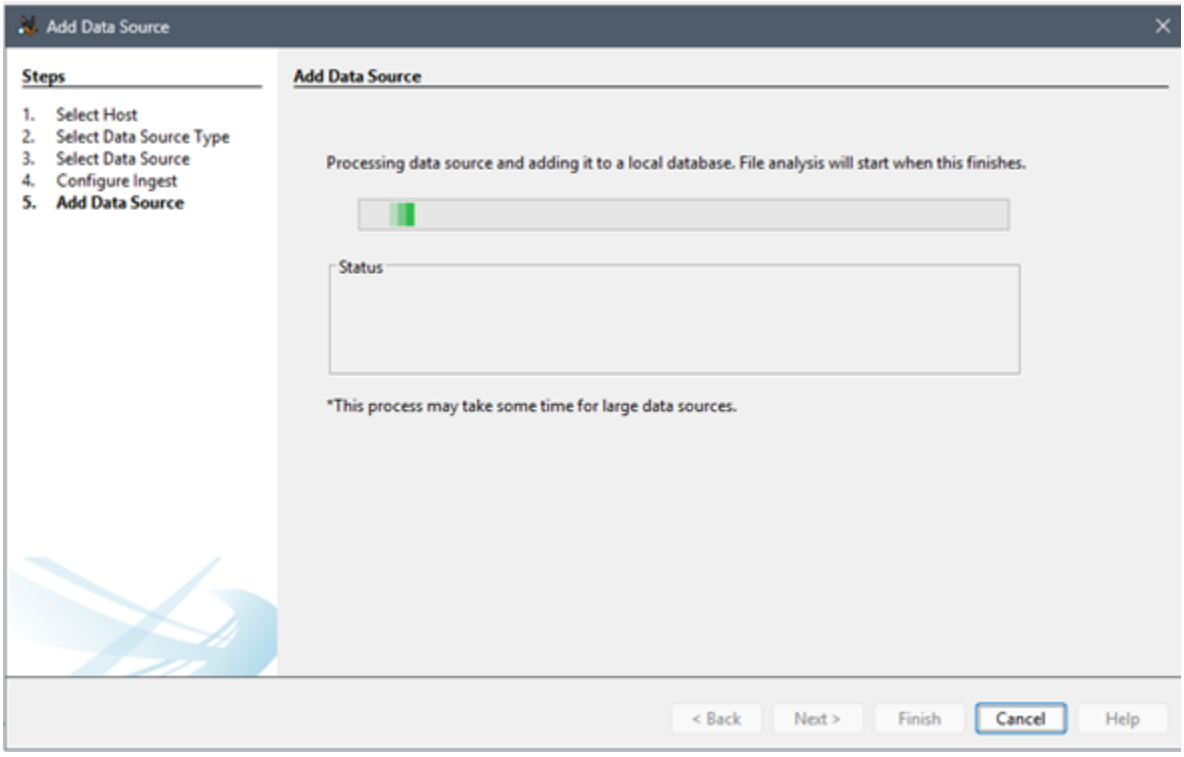


Ilustración 41 Proceso de incorporación de la fuente de datos al caso

Una vez configurados los módulos, Autopsy inició el proceso de incorporación de la imagen forense al caso. El sistema mostró una barra de progreso indicando que se estaba procesando la fuente de datos y preparando el análisis. Documenté este paso como parte del flujo técnico, ya que marca el inicio formal del análisis automatizado sobre la imagen .dd.

Confirmación de incorporación de fuente de datos

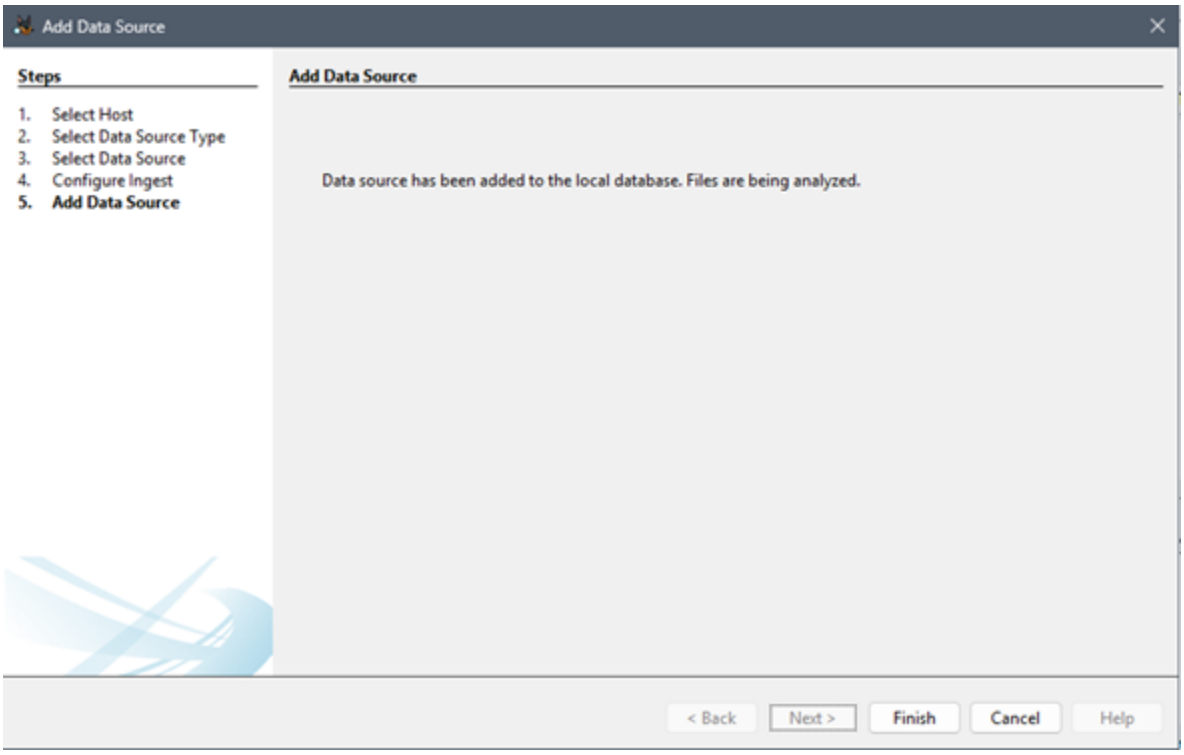


Ilustración 42 Confirmación de incorporación de fuente de datos

Una vez finalizado el proceso de ingestión, Autopsy confirmó que la imagen forense había sido añadida correctamente a la base de datos local. A partir de este punto, el sistema comenzó el análisis automatizado de archivos, directorios y espacio no asignado. Este paso marcó el inicio formal del procesamiento de evidencia digital en el entorno Windows.

Progreso del análisis forense sobre la imagen USB

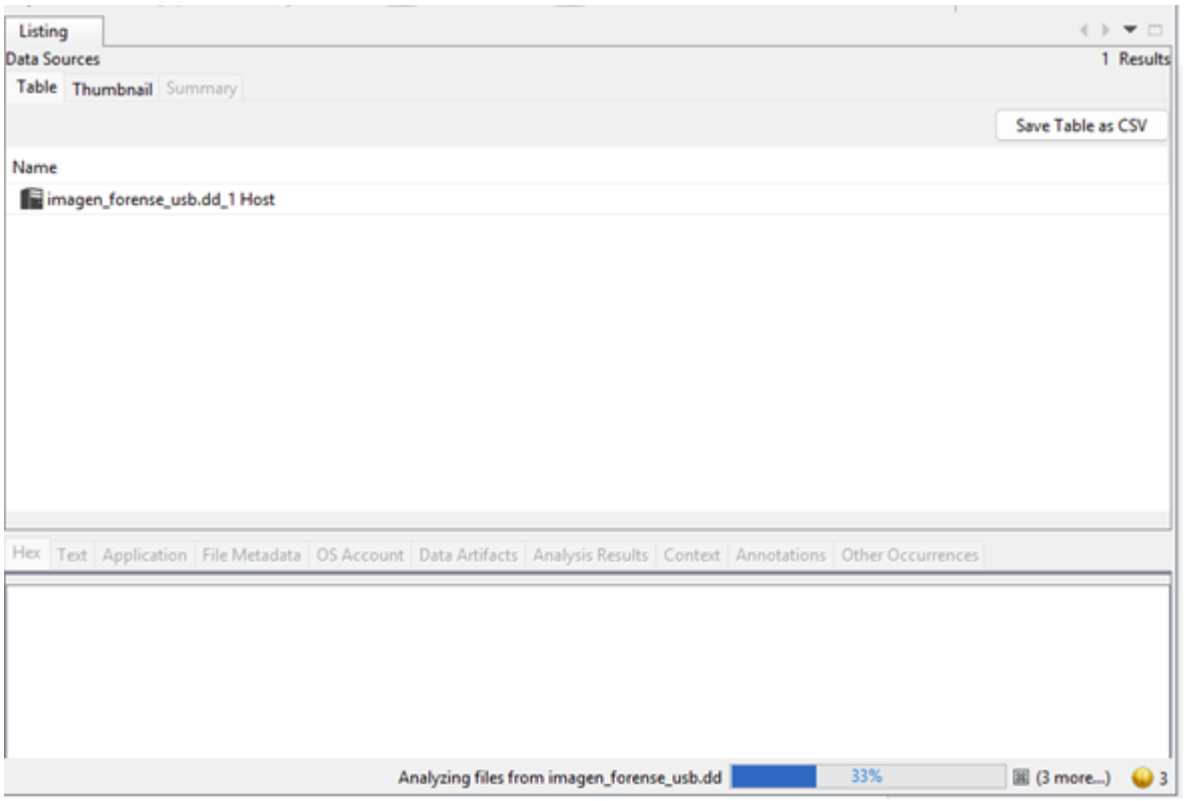


Ilustración 43 Progreso del análisis forense sobre la imagen USB

Autopsy mostró un avance del 33% en el análisis de la imagen imagen_forense_usb.dd. El sistema comenzó a categorizar los artefactos encontrados en pestañas como File Metadata, Data Artifacts, Analysis Results, entre otras. Esta visualización me permitió monitorear el progreso del análisis y preparar la documentación de hallazgos relevantes para el informe final.

Registro de módulos ejecutados en el análisis forense

Module	Num	New?	Subject	Timestamp
Hash Lookup	1		No notable hash set.	2025/11/12 15:...
Hash Lookup	1		No known hash set.	2025/11/12 15:...
Recent Activity	1		Started imagen_forense_usb.dd	2025/11/12 16:...
Recent Activity	1		Finished imagen_forense_usb.dd - No errors reported	2025/11/12 16:...
Recent Activity	1		imagen_forense_usb.dd - Browser Results	2025/11/12 16:...
aLeapp	1		aLeapp Processing Completed	2025/11/12 16:...
DJI Drone Analyzer	1		Started imagen_forense_usb.dd	2025/11/12 16:...
iLeapp	1		iLeapp Processing Completed	2025/11/12 16:...
GPX Parser	1		0 files found	2025/11/12 17:...
File Type Identification	1		File Type Id Results	2025/11/12 17:...
Keyword Search	1		Keyword Indexing Results	2025/11/12 17:...
Extension Mismatch ...	1		File Extension Mismatch Results	2025/11/12 17:...
PhotoRec Carver	1		PhotoRec Results	2025/11/12 17:...
GPX Parser	1		0 files found	2025/11/12 17:...
Data Source Integrity	1		Starting imagen_forense_usb.dd	2025/11/12 17:...
Data Source Integrity	1		imagen_forense_usb.dd hashes calculated	2025/11/12 17:...

Sort by: Time Total: 16 Unique: 16

Ilustración 44 Registro de módulos ejecutados en el análisis forense

Autopsy generó una tabla con los resultados de los módulos ejecutados sobre la imagen imagen_forense_usb.dd. Se registraron procesos como:

- Hash Lookup: sin coincidencias en conjuntos conocidos
- Recent Activity: actividad reciente del navegador
- Data Source Integrity: cálculo de hashes
- PhotoRec Parser, GPX Parser, Keyword Search: resultados indexados

Este registro con marcas de tiempo me permitió validar que cada módulo se ejecutó correctamente y que el análisis cubrió múltiples dimensiones de la evidencia digital.

Listado de archivos y metadatos extraídos

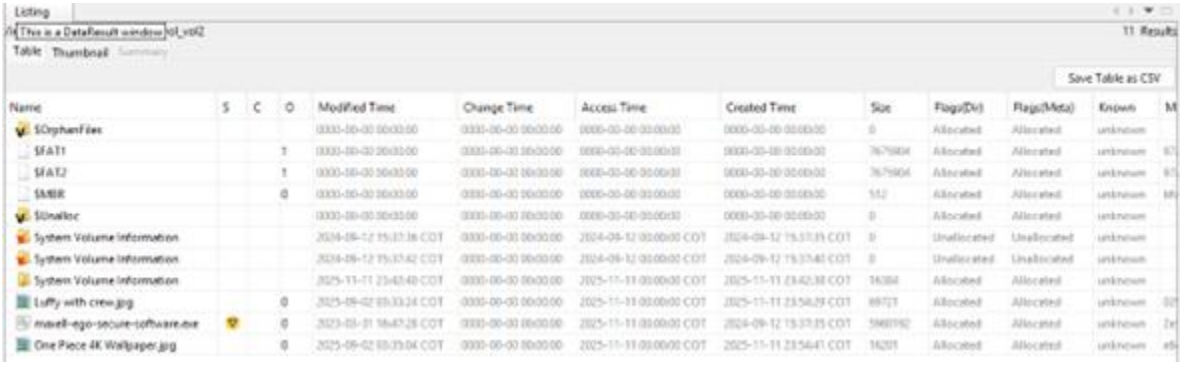


Ilustración 45 Listado de archivos y metadatos extraídos

Autopsy presentó un listado detallado de archivos encontrados en la imagen forense, incluyendo elementos como $Recycle.Bin, System Volume Information y archivos de usuario como Luffy with crew.jpg, man4-egypt-pyramids.jpg y One Piece-will-Kid.jpg. Para cada archivo se mostraron:

- Tiempos de modificación, acceso, creación y cambio
- Tamaño, estado de residencia y estado conocido

Este nivel de detalle me permitió identificar archivos relevantes, validar su integridad y establecer una línea de tiempo de actividad en el dispositivo USB.

Tabla de hashes y tipos MIME de archivos analizados

MD5 Hash	SHA-256 Hash	MIME Type	Extension
97acb1f67c395237db0f6f6acdb26cd0	19de700f8364969194552c8a063edb74af400620901ecbc...	application/octet-stream	
97acb1f67c395237db0f6f6acdb26cd0	19de700f8364969194552c8a063edb74af400620901ecbc...	application/octet-stream	
bfa917cc029dc080dbb1e75c967f2b51	32cf764f02710c1f23f02c1ab562571d2e73caa814602bcf9...	application/octet-stream	
029cc25f600e511780f07fa3b85c9c67	f685cf9db2b15359c4241fe87a6efbd8e8caa201b756f42b...	image/jpeg	jpg
2e5dcc68a5060195dc3190fc5e89b2e0	b8881d3d0206018b0b02f84789e3edb63e5e30952e621c0...	application/x-dosexec	exe
e64027aaa0db6a5c68e22473a89db75e	7f3acde417cf3520e6649cc4d82914981d2fd6946a7bfd28...	image/jpeg	jpg

Ilustración 46 Tabla de hashes y tipos MIME de archivos analizados

Durante el análisis en Autopsy, accedí a la tabla que muestra los valores hash MD5 y SHA-256 de los archivos extraídos, junto con sus tipos MIME y extensiones. Esta información me permitió:

- Verificar la integridad de cada archivo
- Identificar duplicados por coincidencia de hash
- Confirmar el tipo de contenido (por ejemplo, image/jpeg, application/x-dosexec)

Este paso fue clave para documentar la autenticidad de los archivos y preparar la tabla final de evidencias.

Cálculo de hashes de la imagen forense

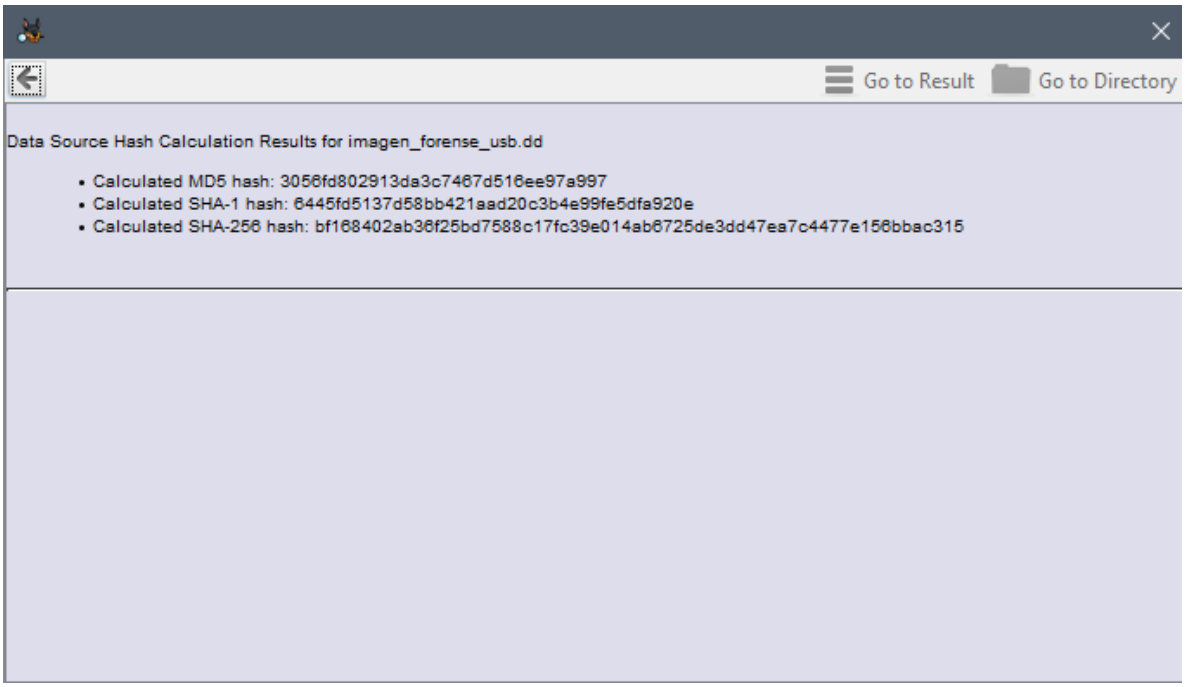


Ilustración 47 Cálculo de hashes de la imagen forense

Autopsy también calculó los valores hash de la imagen imagen_forense_usb.dd, obteniendo:

- **MD5**: 308f60f89213da8e7647d5f6ee97a997
- **SHA-1**: 844f651d7536bb42d3d2f9b49e9fe5dfa920e
- **SHA-256**: b1f8f042a3b92b25d7885c17fc399e014ab7256e3dd4ea7e7c4477f56bbac315

Estos valores fueron registrados como parte de la cadena de custodia digital, asegurando que la imagen analizada corresponde exactamente al archivo extraído desde el dispositivo USB.

Dificultades encontradas y soluciones

Durante el desarrollo del laboratorio forense, enfrenté diversas dificultades técnicas y organizativas que requirieron adaptación, validación cruzada y toma de decisiones informadas. A continuación, detallo los principales retos y las soluciones implementadas:

1. Dificultad: Montaje y visualización de la imagen .dd en Kali Linux

- **Descripción**: Al intentar montar la imagen forense en Kali Linux, el sistema no la reconocía como partición válida.
- **Solución aplicada**: Utilicé Autopsy para analizar la imagen sin necesidad de montarla manualmente, lo que permitió acceder a los archivos y metadatos de forma segura y estructurada.

2. Dificultad: Validación de integridad de archivos recuperados

- **Descripción**: Era necesario confirmar que los archivos extraídos no habían sido alterados durante el proceso.
- **Solución aplicada**: Ejecuté el comando md5sum en Kali Linux para obtener los valores hash locales, y luego los comparé con los generados por Autopsy. La coincidencia confirmó la autenticidad de los archivos.

3. Dificultad: Limitaciones del entorno gráfico en Kali para documentación

- **Descripción**: La edición del informe desde Kali resultaba limitada por la interfaz y herramientas disponibles.

- **Solución aplicada**: Instalé Autopsy en Windows y redacté el informe desde ese entorno, aprovechando una interfaz más amigable para la documentación técnica.

4. Dificultad: Organización de evidencias y trazabilidad

- **Descripción**: La dispersión de archivos y módulos dificultaba la trazabilidad de cada evidencia.

- **Solución aplicada**: Configuré el caso en Autopsy con nombre específico (Analisis_USB_Windows) y carpeta base (C:\Analisis_Forense\), lo que permitió centralizar los resultados y mantener una estructura clara.

5. Dificultad: Selección de módulos de análisis adecuados

- **Descripción**: Algunos módulos no aplicaban al contexto del dispositivo analizado (por ejemplo, Android Analyzer, Drone Analyzer).

- **Solución aplicada**: Activé únicamente los módulos relevantes como PhotoRec, Hash Lookup, Recent Activity, Keyword Search, y Data Source Integrity, optimizando el tiempo de análisis y la pertinencia de los resultados.

6. Dificultad: Registro de hashes de la imagen forense

- **Descripción**: Era necesario documentar los valores hash de la imagen .dd como parte de la cadena de custodia.

- **Solución aplicada**: Autopsy generó automáticamente los valores MD5, SHA-1 y SHA-256, los cuales fueron registrados en el informe como evidencia técnica.

Recomendaciones

Con base en el análisis realizado sobre la imagen forense del dispositivo USB, y considerando las dificultades enfrentadas y las herramientas utilizadas, propongo las siguientes recomendaciones para fortalecer futuros procesos de análisis digital:

1. Asegurar la cadena de custodia digital desde el inicio

Es fundamental generar y registrar los valores hash (MD5, SHA-1, SHA-256) de cada imagen forense antes y después del análisis, para garantizar la integridad de la evidencia y evitar cuestionamientos en entornos judiciales o académicos.

2. Utilizar herramientas complementarias en entornos mixtos

La combinación de Kali Linux y Autopsy en Windows me permitió superar limitaciones técnicas, validar hallazgos y documentar el proceso con mayor claridad. Recomiendo mantener entornos duales cuando sea posible, especialmente en laboratorios educativos.

3. Estructurar los casos con nombres y rutas claras

Definir nombres descriptivos para los casos (Analisis_USB_Windows) y carpetas base (C:\Analisis_Forense\) facilita la organización, trazabilidad y recuperación de evidencias, especialmente cuando se trabaja con múltiples fuentes o dispositivos.

4. Activar solo los módulos de análisis pertinentes

Seleccionar únicamente los módulos relevantes para el tipo de dispositivo y sistema de archivos evita sobrecarga de procesamiento y resultados innecesarios. En este caso, módulos como PhotoRec, Hash Lookup, Recent Activity y Keyword Search fueron suficientes y efectivos.

5. Documentar cada fase con capturas y observaciones técnicas

Integrar imágenes del proceso (terminal, interfaz gráfica, tablas de hash, módulos ejecutados) junto con descripciones técnicas y reflexiones personales fortalece la utilidad pedagógica del informe y permite replicar el procedimiento en otros contextos.

6. Validar los archivos recuperados con herramientas externas

Complementar el análisis con comandos como md5sum en Kali Linux permite verificar localmente la integridad de los archivos extraídos, reforzando la confiabilidad del proceso y detectando posibles alteraciones.

Conclusiones

A lo largo del laboratorio forense, logré aplicar una metodología rigurosa para el análisis de la imagen imagen_forense_usb.dd, combinando entornos Linux y Windows, y utilizando herramientas como Autopsy, md5sum y PhotoRec. Las principales conclusiones son:

- **La imagen forense fue procesada sin alteraciones**, como lo demuestran los valores hash MD5, SHA-1 y SHA-256 calculados y registrados.
- **Se recuperaron archivos relevantes**, incluyendo imágenes y estructuras del sistema, con metadatos completos que permiten reconstruir la actividad del dispositivo.
- **La trazabilidad del proceso fue garantizada** mediante la creación de un caso estructurado en Autopsy, con documentación técnica y capturas de cada fase.
- **La selección adecuada de módulos de análisis optimizó los resultados**, evitando sobrecarga y enfocando el procesamiento en artefactos útiles.
- **La documentación reflexiva y visual fortaleció la utilidad pedagógica del informe**, permitiendo replicar el procedimiento en otros contextos académicos o profesionales.

Este ejercicio no solo consolidó competencias técnicas en informática forense, sino que también reforzó la importancia de la documentación clara, la validación de integridad y el uso ético de herramientas digitales.

Bibliografía

RAFEL SANDOVAL MORALES

Webgrafía

Peritos Informáticos (Argentina)	Captura de memoria con FTK Imager Lite	FTK Imager Lite
Universidad Tecnológica de Bolívar	Uso de Autopsy y FTK Imager en análisis forense	Repositorio UTB

Ia.

https://chatgpt.com/