INFORME LABORATORIO ANÁLISIS FORENSE KALI LINUX Y WINDOWS

Natalia Espinosa Mena

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba

INFORME LABORATORIO ANÁLISIS FORENSE KALI LINUX Y WINDOWS

Docente

Rafael Sandoval Morales

Ingeniero

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba

CONTENIDO

Pág.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

LISTA DE ILUSTRACIONES

Pág.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

INTRODUCCIÓN

El presente informe de laboratorio tiene como propósito exponer el desarrollo del análisis forense digital aplicado a una USB, primero se desarrolló en el entorno de Kali Linux. El laboratorio busca simular una situación frecuente en respuesta a incidentes, donde, se recibe un dispositivo potencialmente relevante, se debe obtener una copia forense bit a bit sin alterar el original, preservar su integridad mediante hashes (MD5/SHA-256) y, con esa imagen ya validada, proceder al análisis en las herramientas forenses Autopsy y FTK Imager. En Kali se identificó el dispositivo USB conectado a la máquina virtual, se realizó la adquisición forense mediante dd (generando un archivo de imagen con extensión .dd) y se calcularon sus valores de integridad. La imagen obtenida en Kali fue transferida a través de una segunda unidad USB y en Windows se cargó la misma imagen en Autopsy y en FTK Imager para examinar la estructura interna del sistema de archivo.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

PLANTEAMIENTO DEL PROBLEMA

Durante el desarrollo del laboratorio de análisis forense digital, el principal desafío consiste en garantizar la integridad del proceso en cada una de sus etapas. Desde la creación de la imagen forense hasta su análisis con las herramientas Autopsy y FTK Imager, es esencial mantener la autenticidad de la evidencia digital y evitar cualquier alteración que comprometa los resultados.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

OBJETIVOS

General: Desarrollar el laboratorio de manera que se comprendan los pasos a seguir en un análisis forense digital.

Especificos:

- Generar la imagen .dd de la evidencia.
- Verificar la integridad de le evidencia.
- Realizar el análisis forense en Kali Linux con Autopsy.
- Desarrollar el análisis forense en Windows utilizando Autopsy.
- Ejecutar el análisis forense en Windows con FTK Image.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

1 CAPITULO 1: ANÁLISIS FORENSE EN KALI LINUX

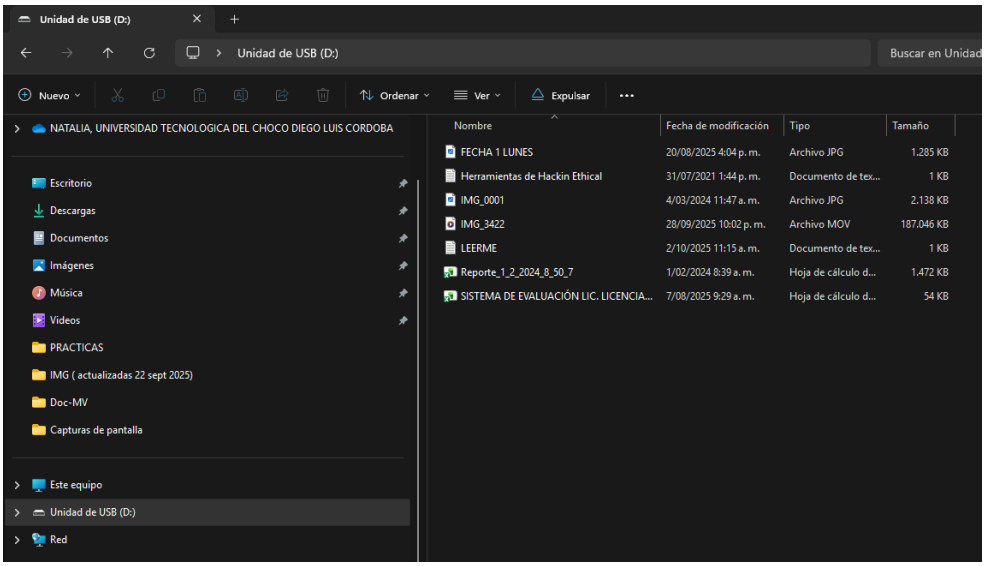


Ilustración 1 Conexión de memoria al equipo

En este primer paso se conectó la memoria USB al equipo y se copiaron en ella varios archivos de prueba. Entre los archivos guardados se encuentran documentos de texto, imágenes, videos y hojas de cálculo.

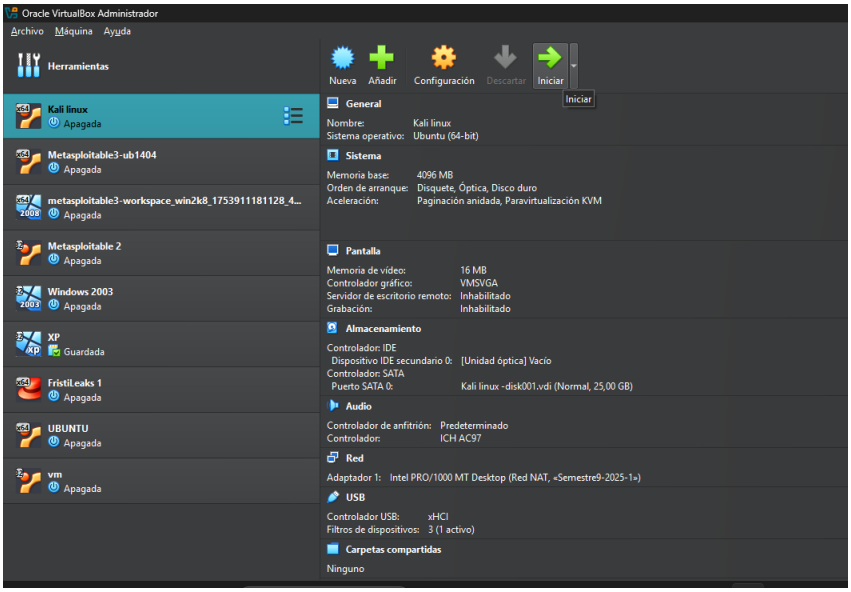
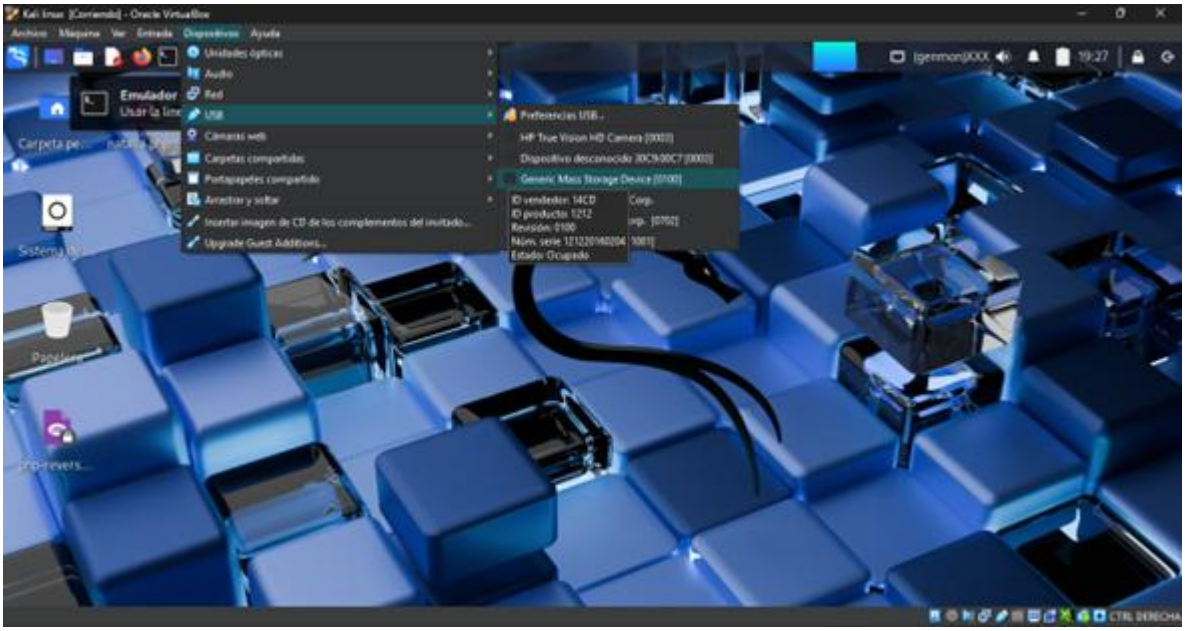


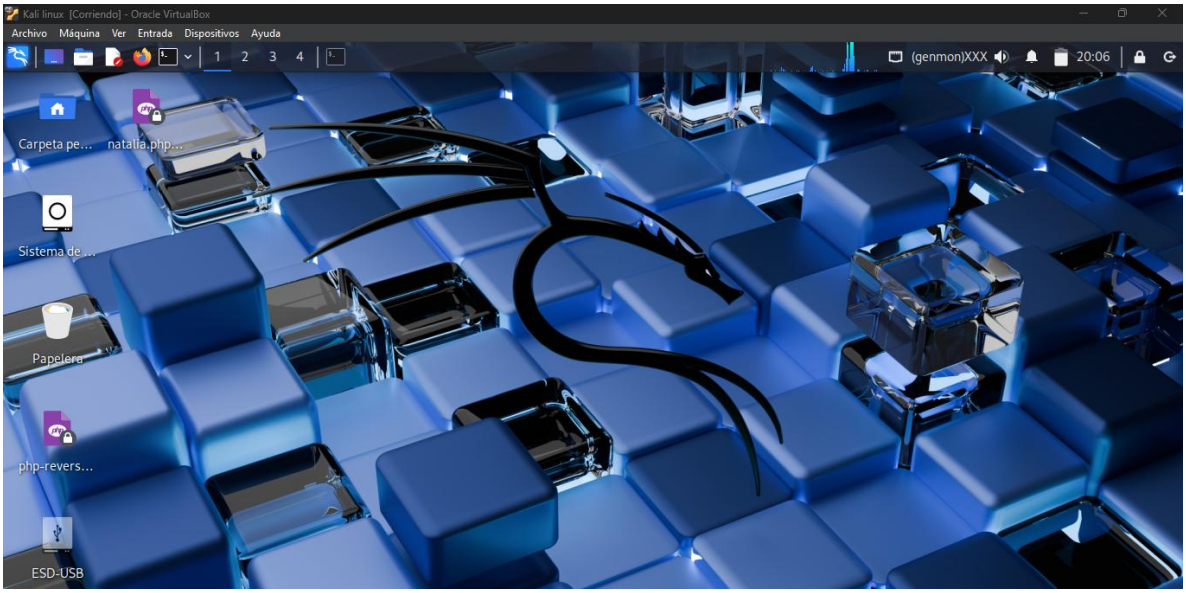
Ilustración 2 Inicio de VM Kali Linux

En este paso se abrió el programa Oracle VM VirtualBox y se seleccionó la máquina virtual con el sistema operativo Kali Linux. Desdé la ventana principal de VirtualBox se presionó el botón **Iniciar** para encender la máquina



Con la máquina virtual Kali Linux ya encendida, se procedió a conectar la memoria USB al entorno virtual.

Para hacerlo, en la barra superior de VirtualBox se ingresó al menú **Dispositivos**, luego, la opción **USB,** se muestra una lista de preferencias de USB y desde allí se seleccionó la opción **Generic Mass Storage Device**, que corresponde a la memoria USB conectada al equipo físico.



Después de conectar la memoria desde el menú de VirtualBox, se confirmó que el sistema operativo Kali Linux la reconoció correctamente.

En el escritorio se puede observar el icono con el nombre ESD-USB, que corresponde al dispositivo conectado.

Esto indica que la memoria está lista para ser utilizada dentro del entorno Kali y que el sistema la ha montado de manera correcta.

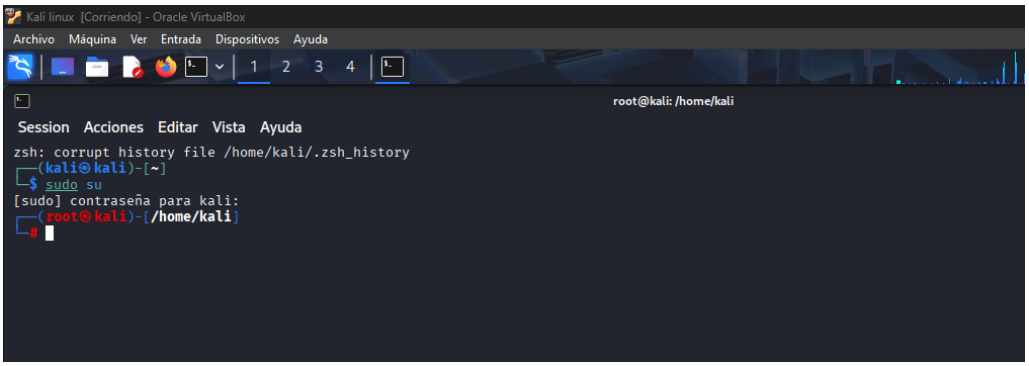


Ilustración 3 Permisos de superusuario

En este paso se abrió una terminal para comenzar a trabajar con los comandos necesarios en el proceso forense.

Primero se ejecutó el comando **sudo su**, que permite obtener permisos de administrador (root) dentro del sistema.

Estos permisos son importantes porque algunas tareas que requieren privilegios elevados.

Una vez se ingresa la contraseña del usuario, el indicador del terminal cambió a root@kali, confirmando que se tienen los permisos necesarios para continuar como superusuario.

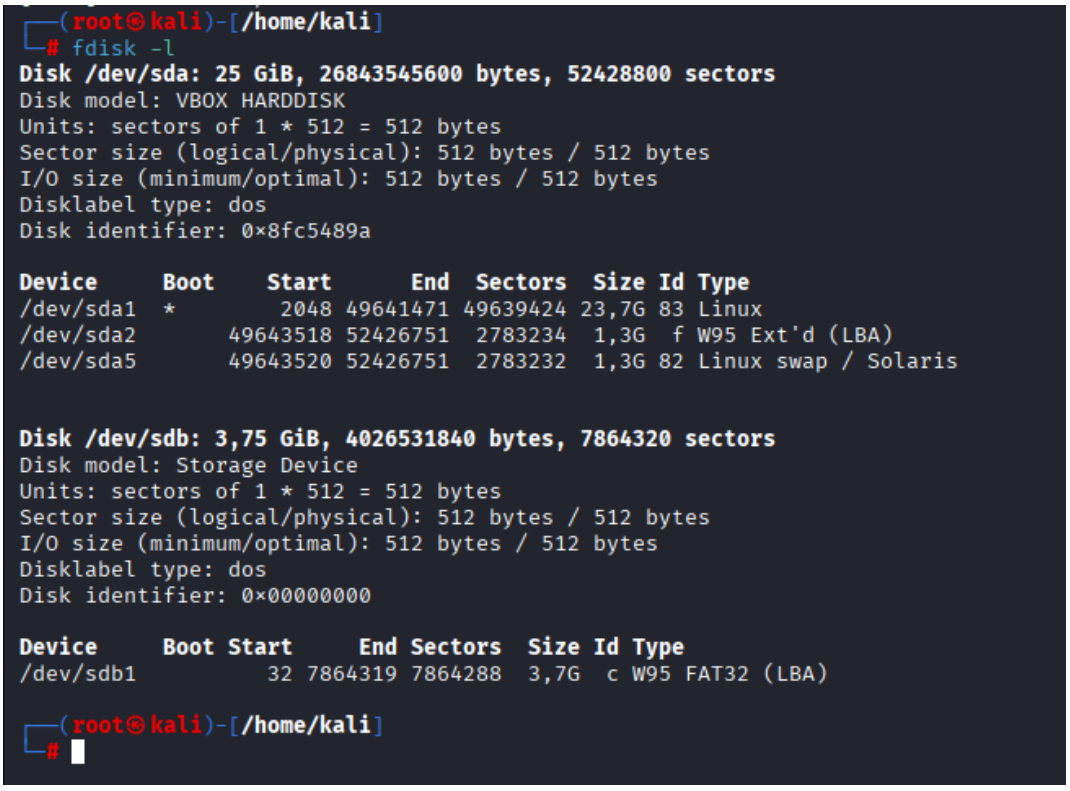


Ilustración 4Verificación de dispositivos conectados con el comando fdisk -l

Con los permisos de administrador activados, se utilizó el comando fdisk -l para listar todos los discos y particiones reconocidos por el sistema.

En la salida del comando se observan dos dispositivos principales:

/dev/sda: corresponde al disco duro virtual del sistema Kali Linux (25 GB).

/dev/sdb: corresponde a la memoria USB conectada (3.75 GB), la cual contiene una partición /dev/sdb1 con formato FAT32.

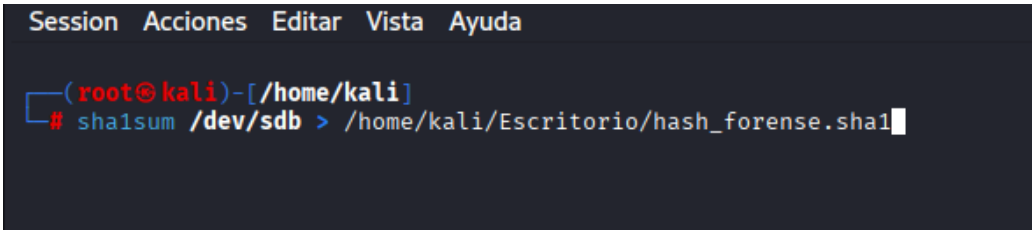


Ilustración 5 Generación del valor hash del dispositivo USB

Continuando en la terminal, en este paso se ejecutó el comando sha1sum /dev/sdb > /home/kali/Escritorio/hash_forense.sha1 con el objetivo de generar el valor hash SHA1 del contenido completo de la memoria USB.

Este valor hash funciona como una huella digital del dispositivo y permite comprobar más adelante si la información fue modificada.

./dev/sdb > corresponde a la memoria USB, la cual el comando sha1sum le crea el hash y lo guarda en el archivo que se indicó. El archivo fue llamado hash_forense.sha1, y se dicta /home/kali/Escritorio/hash_forense.sha1para que lo guarde en el escritorio de Kali Linux.

Con este registro se asegura la integridad de la evidencia antes de proceder con la creación de la imagen forense del dispositivo.

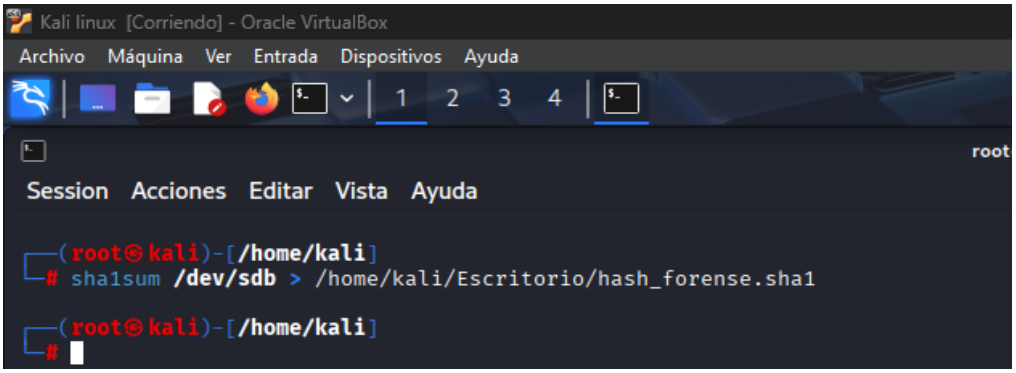


Ilustración 6 Finalización del proceso de generación del hash

Después de esperar un rato de la ejecución comando sha1sum, el sistema completó el cálculo del valor hash del dispositivo USB sin mostrar errores.

Esto indico que el proceso si se realizó correctamente y que el resultado fue guardado en el archivo hash_forense.sha1 que está ubicado en el escritorio del usuario de Kali Linux.

Ilustración 7 Verificación del archivo hash generado en el escritorio

Después que finalizo el cálculo del hash, se verificó que el archivo hash_forense.sha1 estuviera efectivamente en el escritorio de Kali Linux.

Como se puede observar en la imagen, el archivo hash_forense1.sha1 se encuentra en el Escritorio de Kali, lo que confirma que el sistema guardó el resultado del proceso anterior. Este archivo contiene el valor hash del dispositivo USB y será utilizado más adelante para comprobar que la imagen forense, para poder garantizar la integridad de la evidencia.

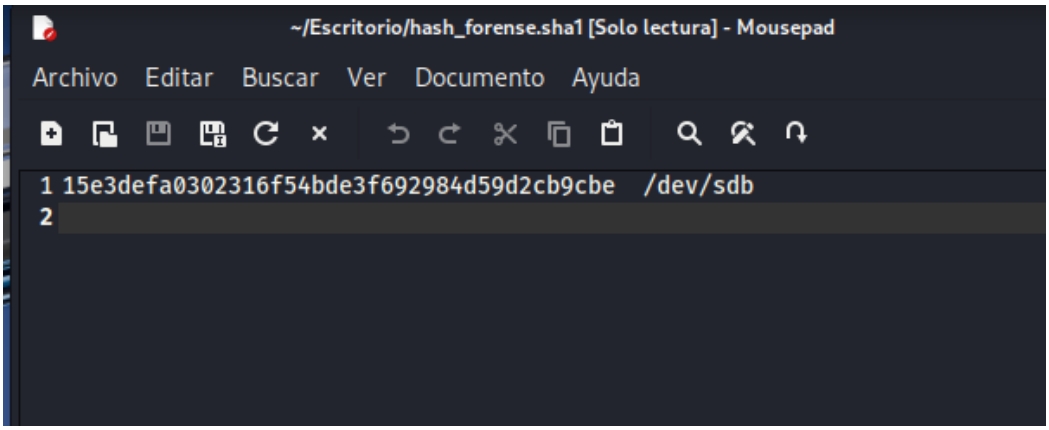


Ilustración 8 Verificación del valor hash generado

En este paso se abrió el archivo hash_forense. sha1 con el editor de texto para revisar el resultado del cálculo.

Dentro del archivo se muestra el valor hash obtenido para el dispositivo /dev/sdb, que corresponde a la memoria USB.

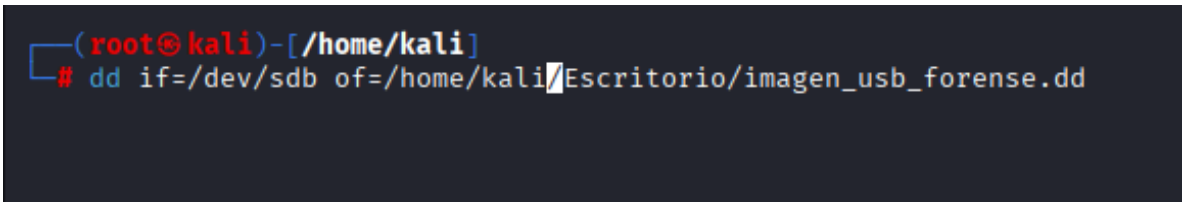


Ilustración 9 Creación de la imagen forense del dispositivo USB

Luego de verificar el valor hash del dispositivo, se procedió a crear la imagen forense de la memoria USB. Para esto se utilizó el comando mostrado en la imagen.

En este comando:

- if=/dev/sdb indica el dispositivo de origen, es decir, la memoria USB.
- of=/home/kali/Escritorio/imagen_usb_forense.dd define el archivo de destino donde se guardará la copia forense.

El programa dd realiza una copia exacta, bit a bit, del contenido del dispositivo, asegurando que no se modifique nada del original.

La imagen generada se guardará en el escritorio de Kali Linux con el nombre imagen_usb_forense.dd

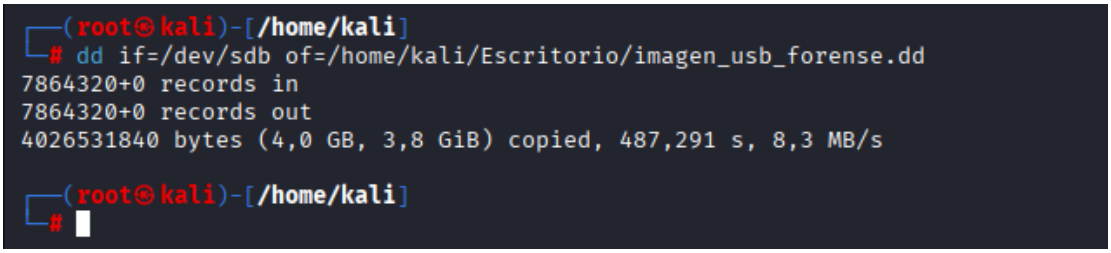


Ilustración 10 Finalización del proceso de creación de la imagen forense

Después de una breve espera de la ejecución del comando dd, el sistema completó el proceso de copia de la memoria USB.

En la salida se muestra la cantidad de datos copiados y la velocidad promedio del proceso. El mensaje final indica que el comando se ejecutó correctamente y que el archivo imagen_usb_forense.dd fue creado correctamente en el escritorio de Kali Linux.

Este archivo representa una copia exacta del contenido original de la memoria USB, y será utilizado para realizar el análisis forense sin necesidad de manipular el dispositivo físico.

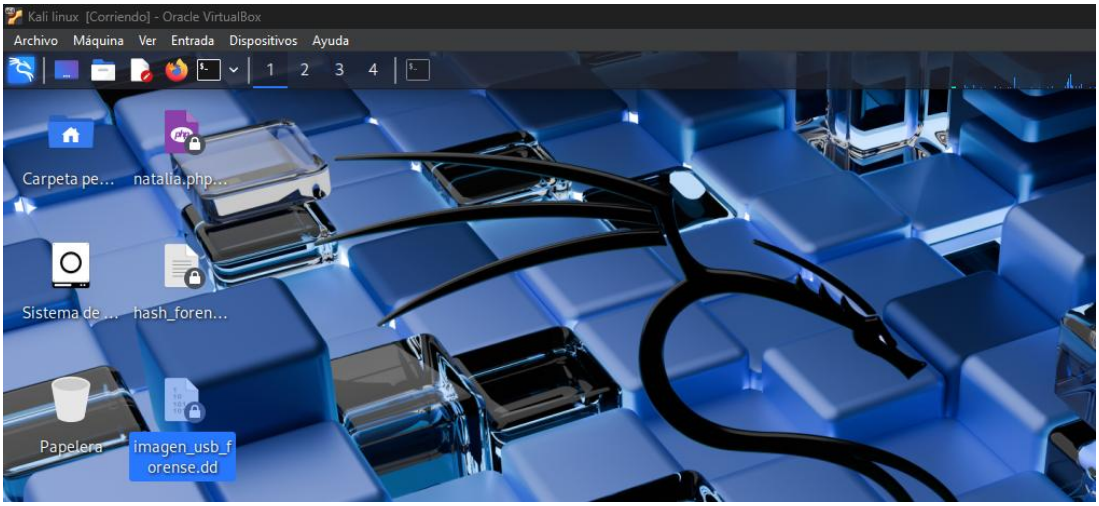


Ilustración 11 Verificación de la imagen forense en el escritorio

Después de que finalizo el proceso con el comando dd, se verificó visualmente la creación del archivo imagen_usb_forense.dd en el escritorio de Kali Linux.

Como se observa en la imagen el archivo se encuentra en el Escritorio, lo que confirma que la copia forense del dispositivo USB se generó correctamente.

Ilustración 12 Verificación del hash de la imagen forense

Ya una vez creada la imagen imagen_usb_forense.dd, se ejecutó nuevamente el comando sha1sum para calcular su valor hash y comprobar la integridad de la imagen.

El comando utilizado fue: sha1sum /home/kali/Escritorio/imagen_usb_forense.dd

El resultado coincide exactamente con el valor obtenido previamente del dispositivo USB original.

ORIGINAL:

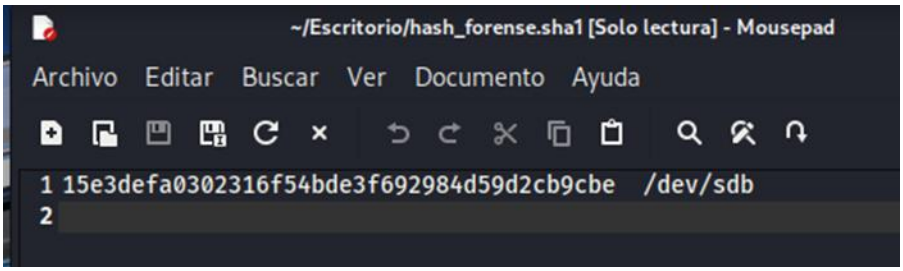


IMAGEN:

Esto confirmo que la imagen forense fue generada correctamente y que no sufrió alteraciones durante la realización de la copia. Con este paso se valida la integridad de la evidencia y confirma, que la imagen es una copia fiel del contenido original de la memoria USB.

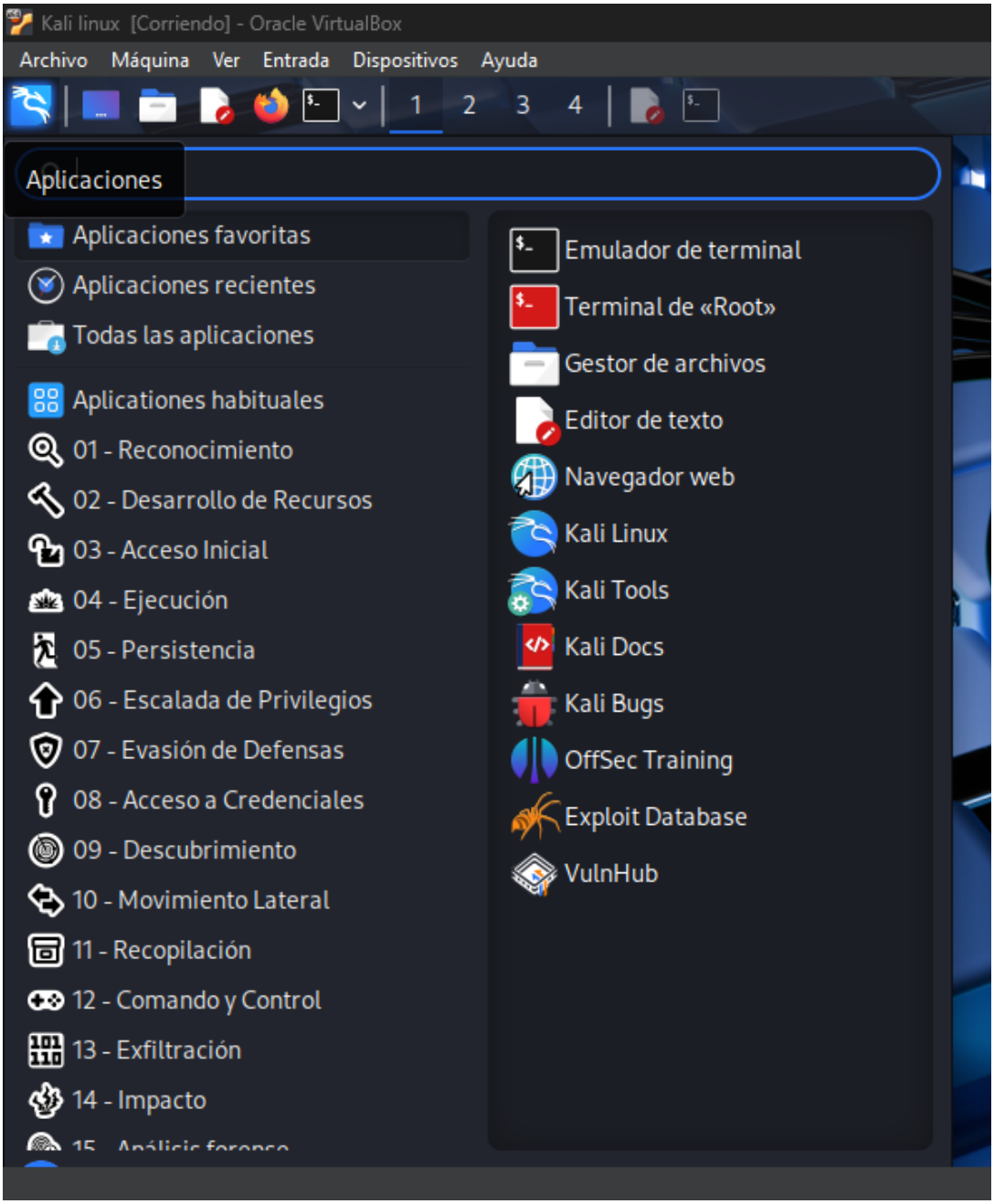


Ilustración 13 Visualización del menú de aplicaciones en Kali Linux

Se abrió el menú principal de Kali Linux para observar las diferentes herramientas disponibles en el sistema.

En la parte izquierda se muestran las categorías organizadas por tipo de actividad, como reconocimiento, acceso a credenciales, escalada de privilegios, evasión de defensas y análisis forense.

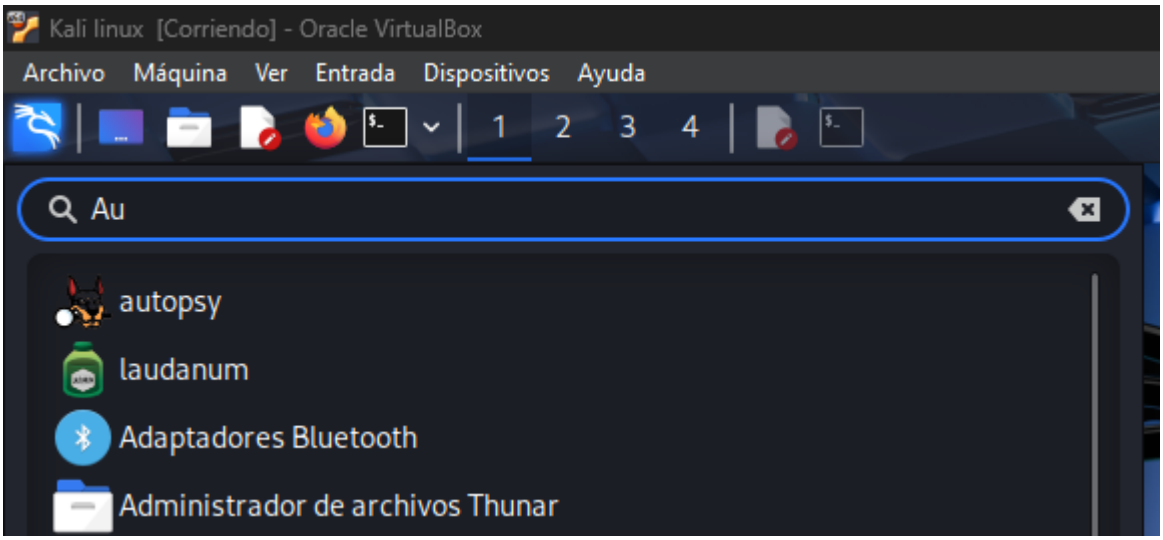


Ilustración 14 Buscar y seleccionar Autopsy

En el menú de aplicaciones se escribió Au en la caja de búsqueda para localizar rápidamente la aplicación Autopsy. Cuando apareció en la lista, se seleccionó Autopsy para abrirla.

Al ejecutar el programa me lleva a la siguiente terminal:

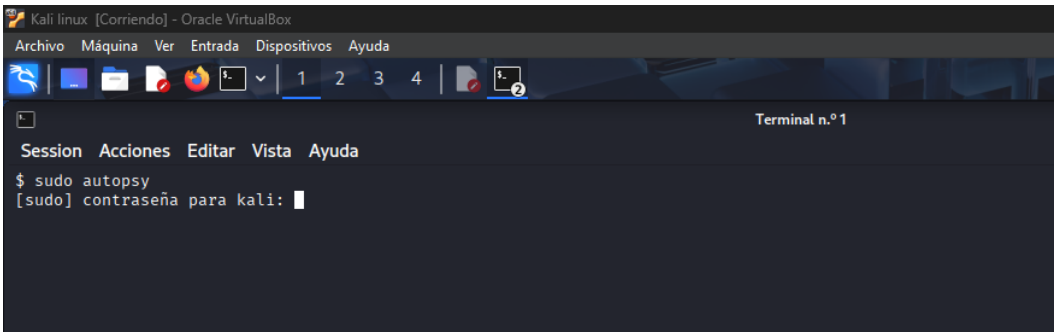


Ilustración 15 Ejecución del programa Autopsy

Al seleccionar la aplicación Autopsy desde el menú de Kali Linux, el sistema abrió automáticamente una ventana de terminal.

En esta terminal se pide ingresar la contraseña del usuario, ya que el programa necesita permisos de administrador para poder ejecutarse.

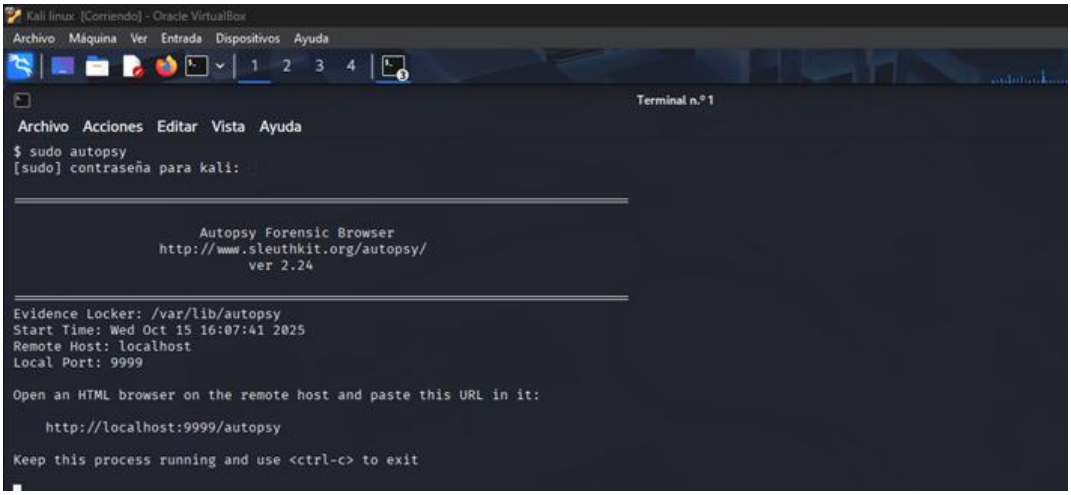


Ilustración 16 Carga del servicio Autopsy

Después de ingresar la contraseña del usuario, se inició correctamente el programa Autopsy. En la terminal se muestra la información del servicio, incluyendo:

- La ruta donde se guardarán los archivos del caso (/var/lib/autopsy)
- La dirección del servidor local (localhost)
- El puerto utilizado (9999)

También se indica la dirección que debe abrirse en el navegador para acceder a la interfaz de Autopsy: http://localhost:9999/autopsy

Esta ventana debe permanecer abierta mientras se utiliza la herramienta, ya que mantiene activo el servicio web de Autopsy.

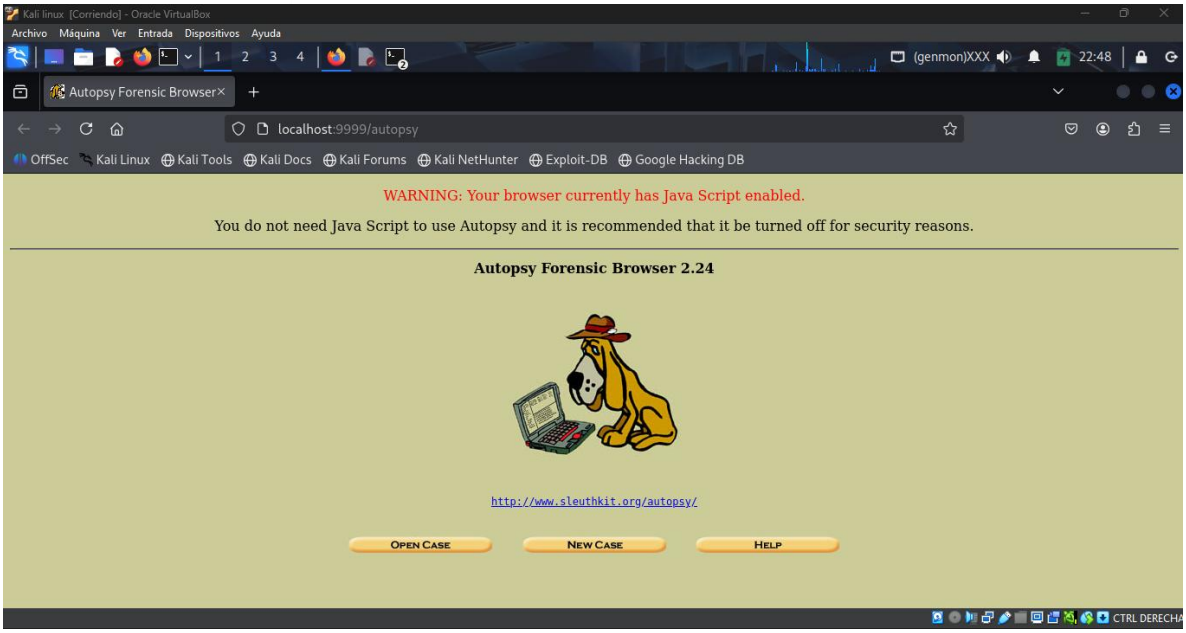


Ilustración 17 Acceso a la interfaz web de Autopsy

Una vez iniciado el servicio de Autopsy en la terminal, se abrió el navegador web e ingresó la dirección http://localhost:9999/autopsy

Al cargar la página, se muestra la pantalla principal del programa Autopsy Forensic Browser versión 2.24, con el logotipo característico del perro investigador. En esta ventana inicial se presentan tres opciones:

- Open Case: abrir un caso ya existente.
- New Case: crear un nuevo caso para comenzar un análisis.
- Help: acceder a la ayuda del programa.

Desde aquí se dio inicio al trabajo de análisis forense sobre la imagen USB, seleccionando la opción **New Case** para crear un nuevo caso de investigación.

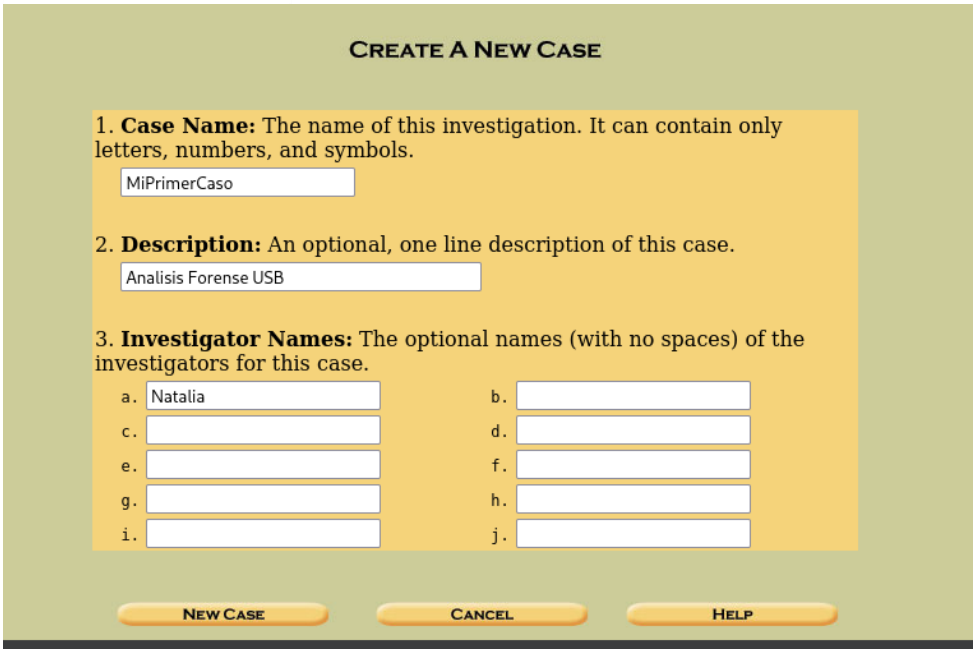


Ilustración 18 Creación de un nuevo caso en Autopsy

Después de hacer clic en la opción **New Case**, se abrió la ventana para registrar un nuevo caso de análisis forense.

En este formulario se completaron los siguientes campos:

- Case Name: MiPrimerCaso, que identifica el nombre del caso dentro del sistema.
- Description: Análisis Forense USB, una breve descripción del objetivo del caso.
- Investigator Names: Natalia, nombre de la persona encargada de la investigación.

Una vez completados los campos, se presionó el botón **New Case** para continuar con la configuración del caso.

Ilustración 19 Creación del host dentro del caso

Después de registrar los datos del caso, Autopsy muestro esta nueva ventana donde confirma la creación de la carpeta del caso (/var/lib/autopsy/MiPrimerCaso/) y del archivo de configuración asociado (case.aut).

En esta misma pantalla se solicita crear un host, es decir, el equipo o dispositivo que será analizado dentro del caso.

Para continuar, se seleccionó el nombre del investigador Natalia desde la lista y se hizo clic en el botón **Add Host**.

Este paso permite asociar la evidencia (la imagen forense del USB) con un caso y un responsable específico dentro del sistema de Autopsy.

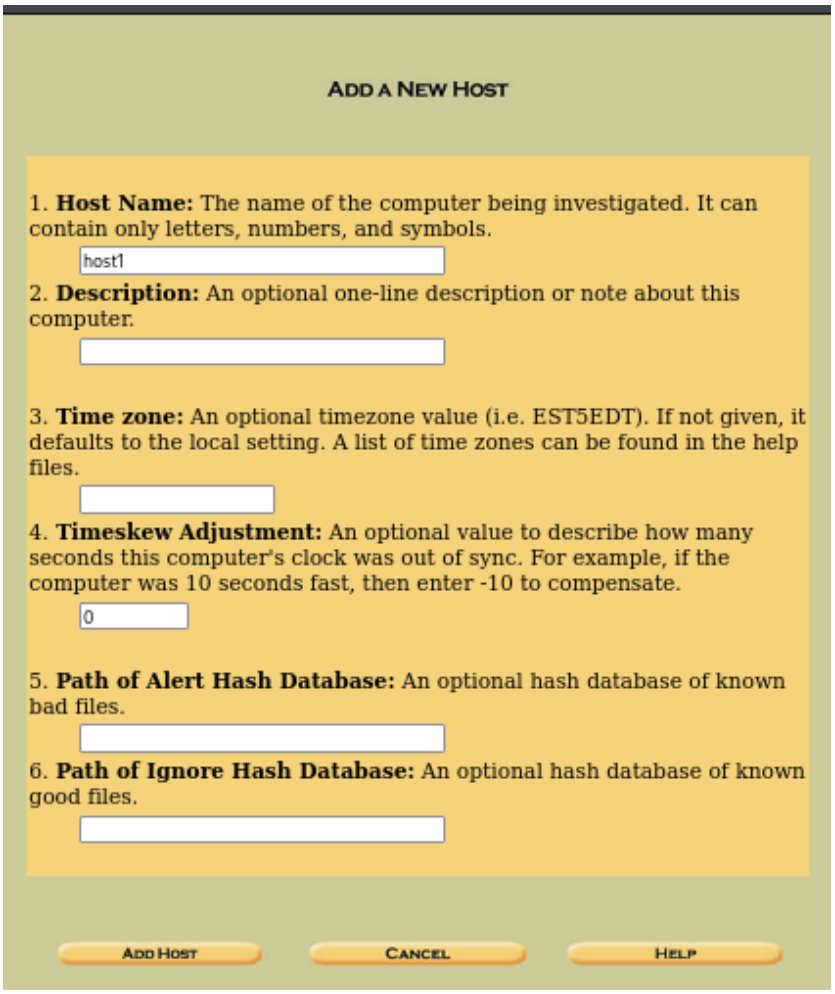


Ilustración 20 Configuración del nuevo host en Autopsy

Tras añadir el investigador, se muestra la ventana para crear un **nuevo host**, que representa el dispositivo o equipo que se va a analizar dentro del caso.

Ilustración 21 Configuración del nuevo host en Autopsy

En esta pantalla se completan los siguientes campos:

- Host Name: Nombre del host.
- Description: Se puede agregar una breve descripción del equipo.
- Time zone: zona horaria del análisis (por defecto usa la del sistema).
- Timeskew Adjustment: permite ajustar diferencias de tiempo si el reloj del dispositivo analizado estaba desfasado (se deja en 0).
- Path of Alert Hash Database / Path of Ignore Hash Database: rutas opcionales de bases de datos de hashes conocidos (no se utilizan en este ejercicio).

Una vez se llenaron los datos correspondientes se presionó el botón **Add Host** para continuar con la creación del entorno donde se cargará la imagen forense del USB.

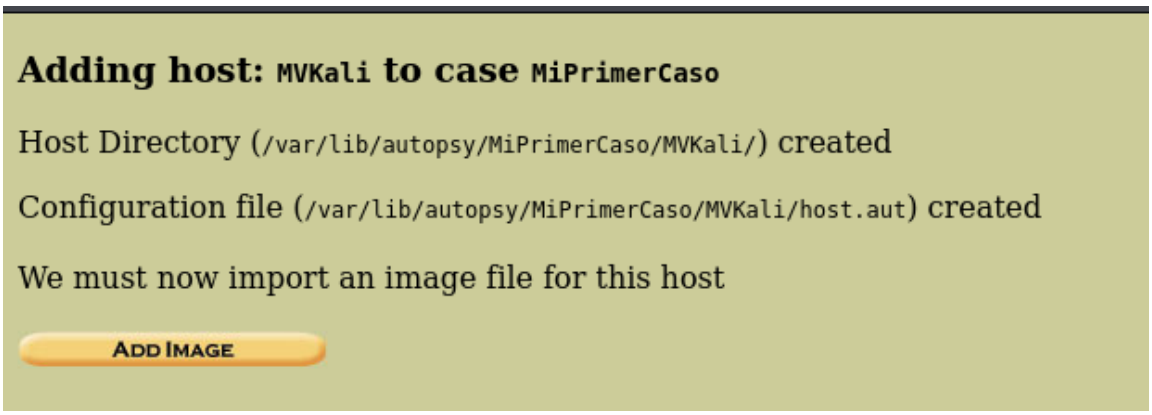


Ilustración 22 Creación del host y preparación para importar la imagen forense

Después de completar la configuración del host, Autopsy muestro el mensaje indicando que el host se ha agregado correctamente al caso MiPrimerCaso.

En la ventana se confirma la creación de los siguientes elementos:

Host Directory: la carpeta donde se almacenará la información del análisis (/var/lib/autopsy/MiPrimerCaso/MVKali/).

Configuration file: el archivo de configuración del host (host.aut).

Como paso siguiente el programa solicita importar una imagen forense para comenzar el proceso de análisis.

Para ello, se realiza clic en el botón **Add Image**:

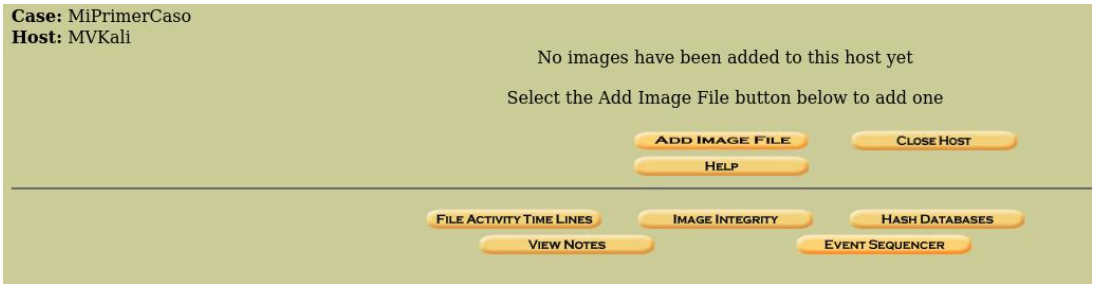


Ilustración 23 Preparación para agregar la imagen forense al host

Después de hacer clic en el botón **Add Image** en la ventana anterior, se abrió esta nueva pantalla donde se muestra que aún no se ha agregado ninguna imagen al host MVKali del caso MiPrimerCaso.

Desde aquí, el programa indica que se debe presionar el botón **Add Image File** para seleccionar el archivo de imagen forense que será analizado.

Este paso sirve para vincular la evidencia digital en este caso, el archivo imagen_usb_forense.dd con el caso creado en Autopsy y comenzar el proceso de análisis.

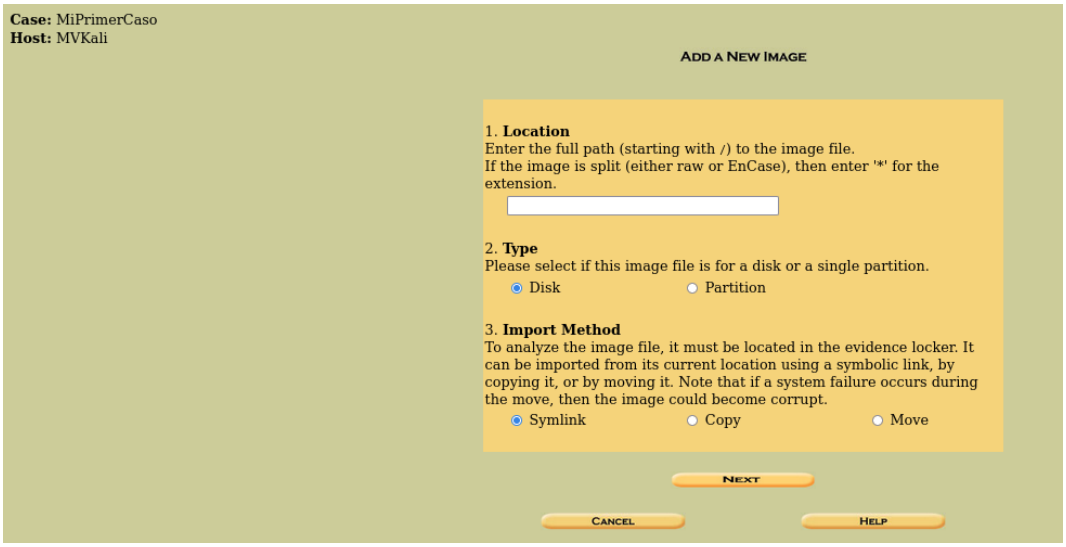


Ilustración 24 Configuración para agregar la imagen forense al caso

Después de hacer clic en Add Image File, se abrió la ventana de configuración para añadir una nueva imagen al caso MiPrimerCaso y al host MVKali.

- Location: se ingresa la ruta completa del archivo de imagen que se va a analizar.
- Type: se selecciona el tipo de imagen. En este caso se marca Disk, ya que corresponde a una copia completa del dispositivo USB.
- Import Method: se elige cómo se importará la imagen. Se selecciona Symlink, que crea un enlace simbólico sin mover ni copiar el archivo original, evitando modificaciones en la evidencia.

Ilustración 25 Asignación de permisos al archivo de imagen forense

Antes de poder agregar la imagen forense en Autopsy, fue necesario otorgarle permisos de acceso. Para ello, se utilizó el comando:

chmod 777 /home/kali/Escritorio/imagen_usb_forense.dd

Este comando permite que el archivo pueda ser leído, modificado y ejecutado por cualquier usuario del sistema, garantizando que Autopsy tenga los permisos necesarios para acceder al archivo durante el análisis.

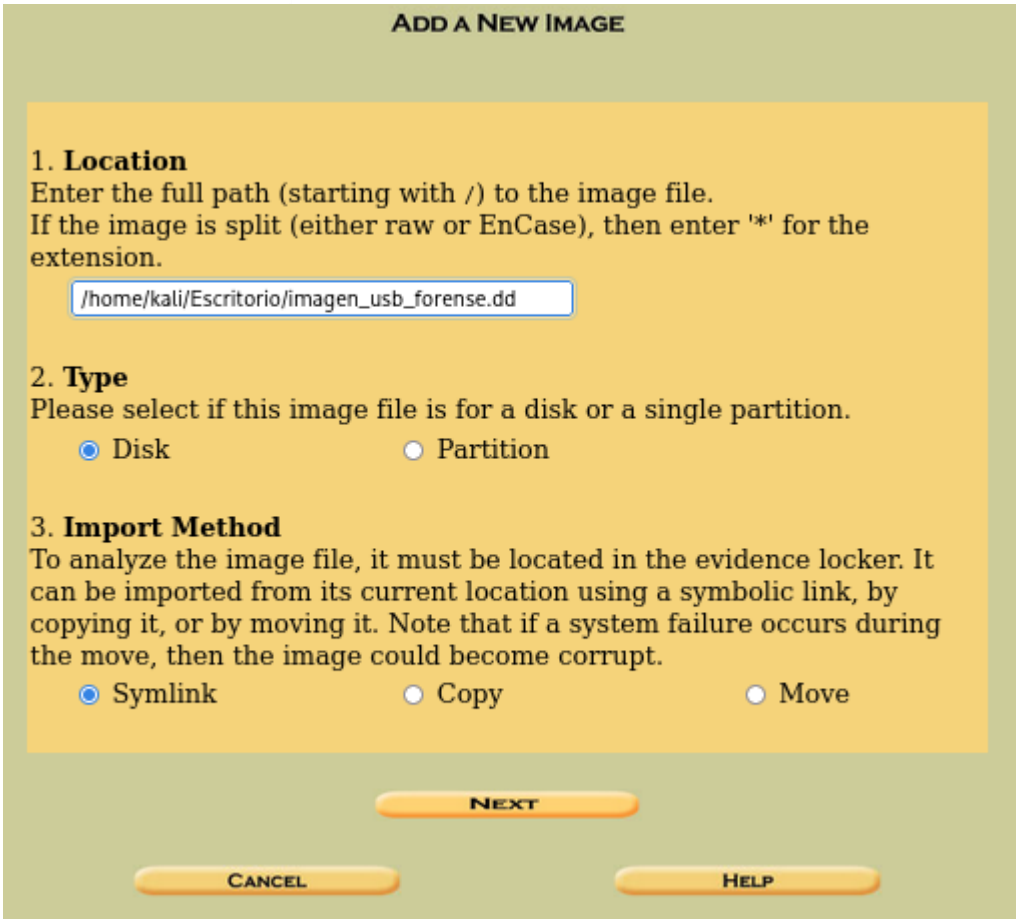


Ilustración 26 Ingreso de la ruta de la imagen forense en Autopsy

Después de asignar los permisos al archivo, se regresó a la ventana de Autopsy para continuar con la importación de la imagen.

En el campo Location se escribió la ruta completa del archivo de imagen forense: /home/kali/Escritorio/imagen_usb_forense.dd

Una vez verificada la información, se hizo clic en el botón Next para continuar con el proceso de carga de la imagen al caso.

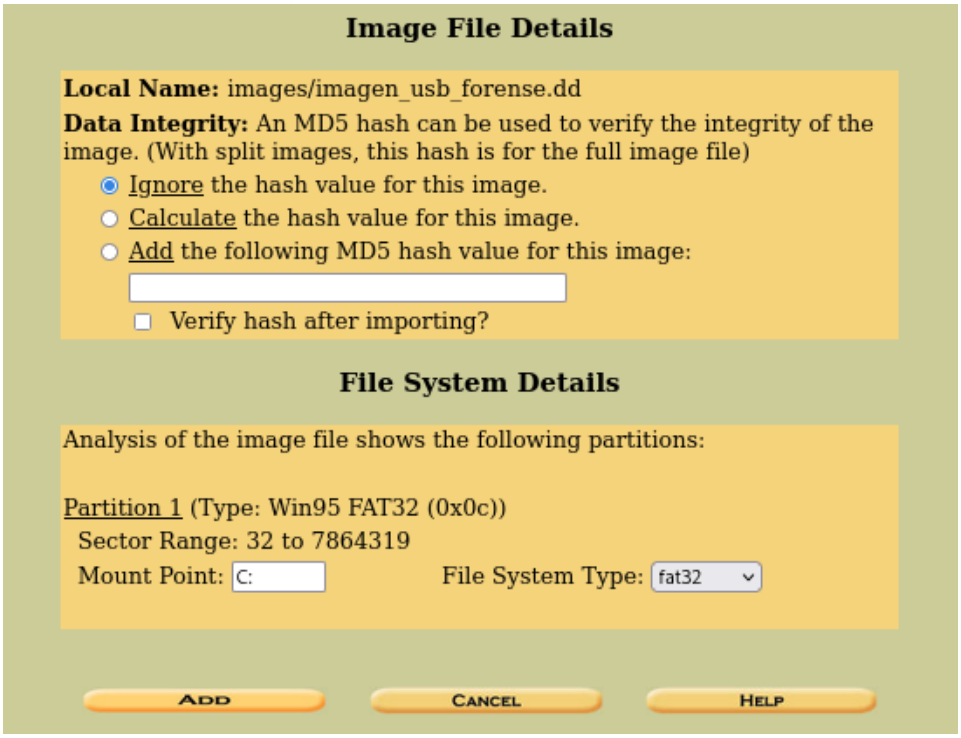


Ilustración 27 Configuración de los detalles de la imagen en Autopsy

En esta ventana se muestran los detalles del archivo de imagen que será analizado.

En la sección Image File Details, Autopsy ofrece varias opciones para la verificación de integridad mediante hash. En este caso, se seleccionó Ignore the hash value for this image, ya que el valor hash ya había sido previamente calculado en Kali durante la adquisición de la evidencia y no era necesario volver a generarlo.

En la parte inferior, dentro de File System Details, Autopsy detectó automáticamente que la imagen pertenece a un sistema de archivos Win95 FAT32 (0x0c), con un rango de sectores entre 32 y 7,864,319, lo cual corresponde al espacio total del dispositivo USB copiado.

Una vez confirmados los datos, se presionó el botón **Add** para incorporar la imagen al caso.

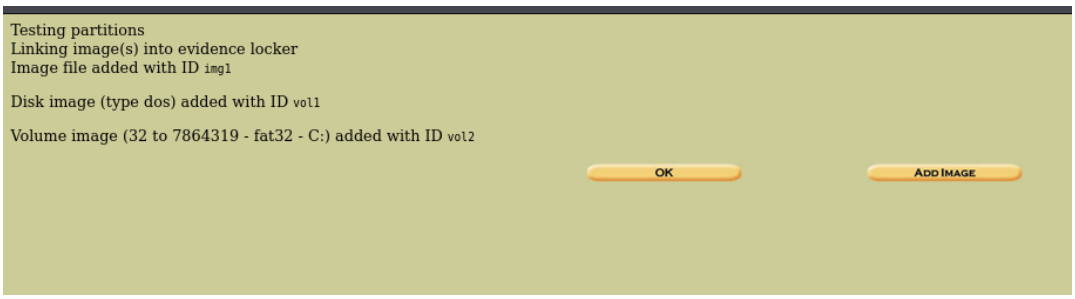


Ilustración 28 Confirmación de la carga de la imagen en Autopsy

Una vez agregada la imagen forense, Autopsy realiza automáticamente el proceso de verificación de las particiones y enlaza el archivo al evidence locker, es decir, al repositorio interno donde se almacena la evidencia dentro del caso.En la pantalla se muestra el resultado del proceso:

- Se añadió el archivo de imagen con el identificador img1.
- Se reconoció un disco tipo DOS con el identificador vol1.

Y se detectó el volumen de tipo FAT32, correspondiente a la partición principal del dispositivo USB, con el identificador vol2.

Estos mensajes confirman que la imagen fue correctamente cargada y está lista para su análisis dentro del entorno de Autopsy.

Como siguiente, se hace clic en el botón OK para continuar.

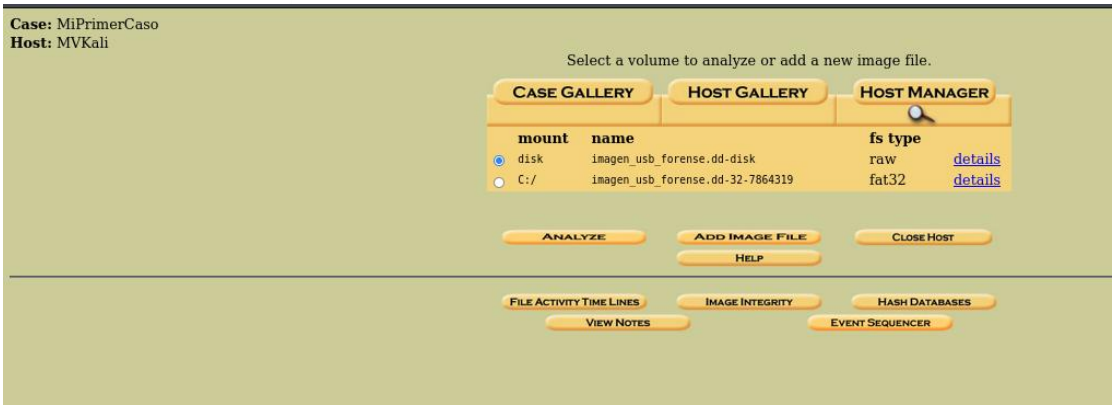


Ilustración 29Selección del volumen para análisis

Luego de cargar correctamente la imagen forense, Autopsy muestra la ventana de Host Manager, donde se visualizan los volúmenes detectados dentro del archivo de imagen.

En este caso, se observan dos entradas:

disk, representa el disco completo copiado desde la memoria USB.

C:/ corresponde a la partición principal del dispositivo, con sistema de archivos FAT32, que es el que contiene los datos del usuario.

Para continuar con el análisis, se seleccionó la partición C:/ y luego, se realizó clic en el botón **Analyze**.

Esto permitió que Autopsy accediera a la estructura interna de archivos para listar los elementos almacenados en la memoria USB original.

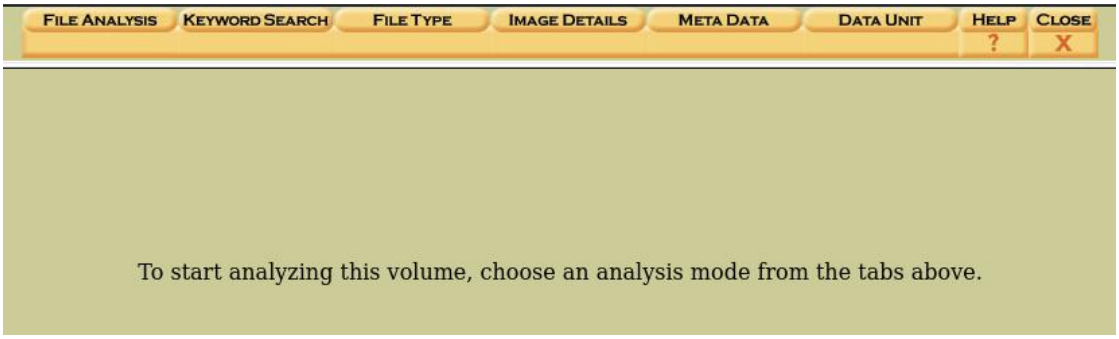


Ilustración 30 Inicio del análisis del volumen en Autopsy

Tras seleccionar la partición C:/ para analizar, Autopsy muestro está nueva interfaz con diferentes pestañas de opciones para explorar la evidencia.

En la parte superior se observan varias secciones, como:

- File Analysis: permite examinar directamente los archivos y carpetas recuperados del dispositivo.
- Keyword Search: habilita la búsqueda de palabras clave dentro del contenido.
- File Type, Meta Data, Image Details y Data Unit: ofrecen distintos enfoques de análisis técnico, como tipos de archivo, metadatos o estructura de bloques.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Para comenzar la revisión del contenido almacenado en la imagen forense, se hace clic en la pestaña **File Analysis** para abrir la vista de navegación de archivos dentro de la imagen USB copiada.

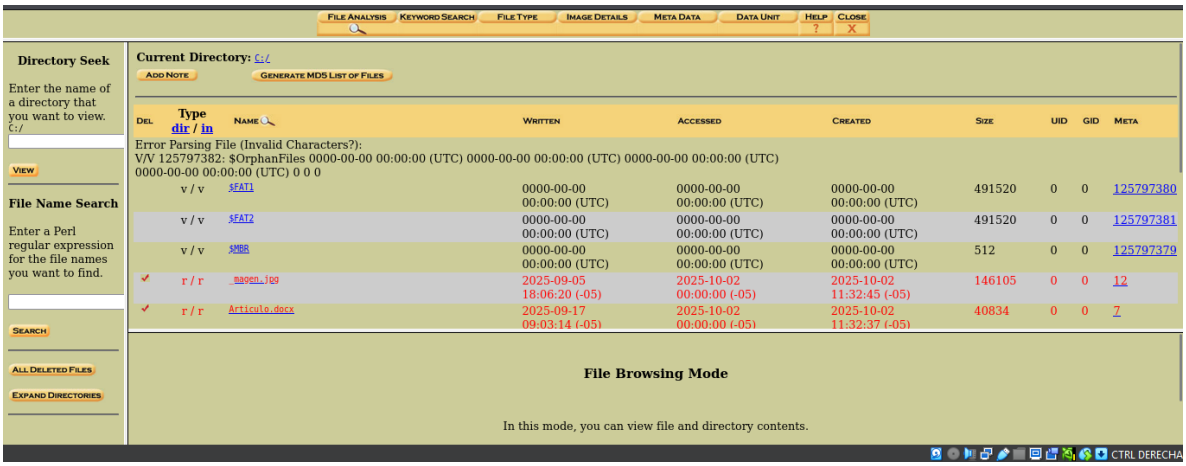
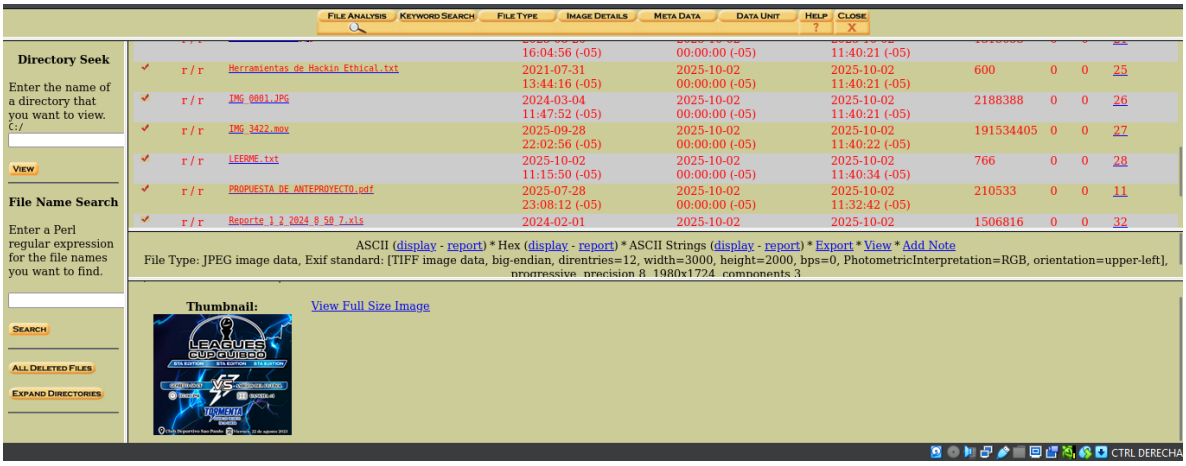


Ilustración 31 Visualización del contenido de la imagen forense

Al seleccionar la opción File Analysis, Autopsy mostro en pantalla la estructura interna de la memoria USB copiada.

En esta vista se listan los directorios y archivos recuperados del dispositivo original, junto con información relevante sobre cada uno, como:



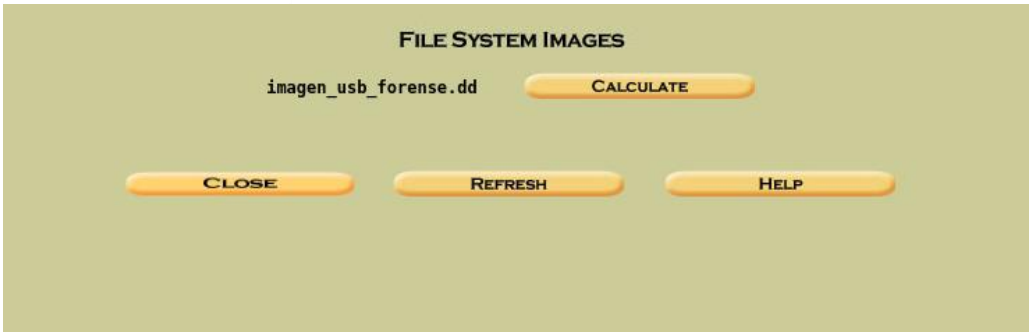
- Nombre del archivo, Fechas de creación, acceso y modificación, Tamaño (Size), Identificador único (UID/GID), Tipo de archivo (File Type)

En la evidencia se observan archivos de diferentes formatos y desde esta ventana el investigador puede continuar explorando carpetas, revisar metadatos o generar un listado completo de archivos para incluir en su informe final.

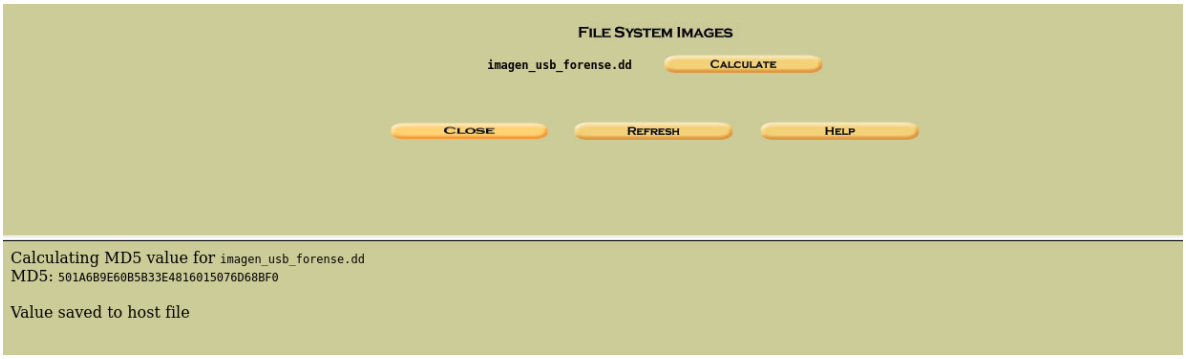
Ilustración 32 Menú superior

Mientras se encontraba en la pestaña File Analysis, para poder regresar al panel principal de gestión de la imagen y calcular su integridad, fue necesario presionar el botón Close, ubicado en la parte superior de la ventana.

Una vez de vuelta en la vista general del caso, se accedió a la pestaña **Image Integrity**, donde se muestra el archivo **imagen_usb_forense.dd** junto con la opción **Calculate**.



Al presionar este botón, Autopsy calcula el valor hash MD5 de la imagen forense.



Esta verificación confirma que la imagen analizada mantiene su integridad y no ha sido alterada desde su adquisición inicial.

De forma adicional, si se desea obtener los valores hash de todos los archivos individuales contenidos en la evidencia, se debe volver a la pestaña File Analysis y seleccionar el botón Generate MD5 List of Files.

Con esta función, Autopsy genera una tabla con los hashes MD5 de cada archivo.

2 CAPITULO 2: ANÁLISIS FORENSE CON AUTOPSY EN WINDOWS

En este capítulo del laboratorio, se continúa con el proceso de análisis de la imagen forense generada previamente en Kali Linux

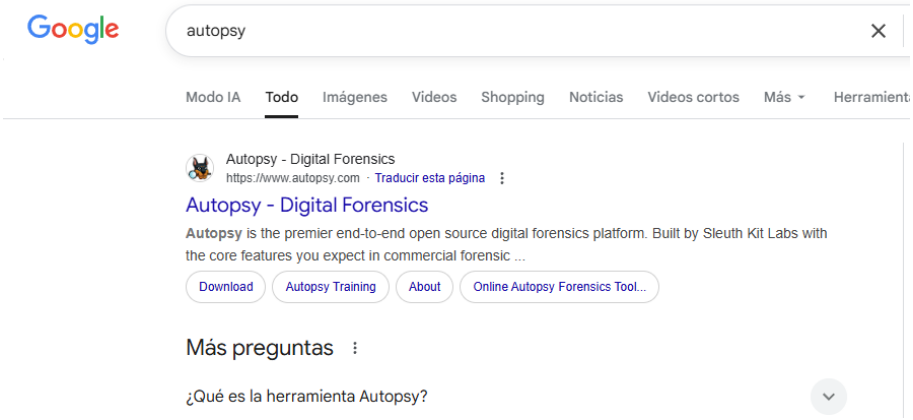


Ilustración 33 Búsqueda de la herramienta Autopsy en Windows

El primer paso consistió en realizar la búsqueda y descarga del software Autopsy desde su página oficial, disponible en https://www.autopsy.com

Al ingresar al sitio, se carga la siguiente pestaña:

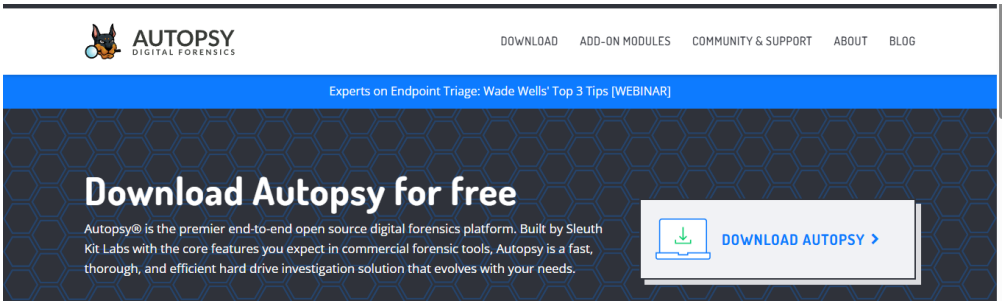


Ilustración 34 Descarga de la herramienta Autopsy

Desde aquí se procede a la descarga de la aplicación seleccionando el botón **DOWNLOAD AUTOPSY**.

Ilustración 35 Selección de la versión para descarga

Se muestra esta pestaña de descarga donde se muestra la versión más reciente disponible para el sistema operativo Windows, en este caso Autopsy 4.22.1.

Desde esta página se seleccionó la opción Download 64-bit, que corresponde al instalador compatible con el equipo.

También se muestran aquí enlaces para descargar versiones destinadas a Linux y macOS, junto con las dependencias necesarias para su instalación.

Ilustración 36Descarga del instalador de Autopsy

Una vez completada la descarga, se pudo observar el archivo instalador de Autopsy guardado en el equipo, con el nombre autopsy-4.22.1-64bit.

Este archivo corresponde al instalador ejecutable para sistemas operativos Windows de 64 bits, y contiene todos los componentes necesarios para iniciar el proceso de instalación del software. El paso siguiente fue ejecutar el archivo.

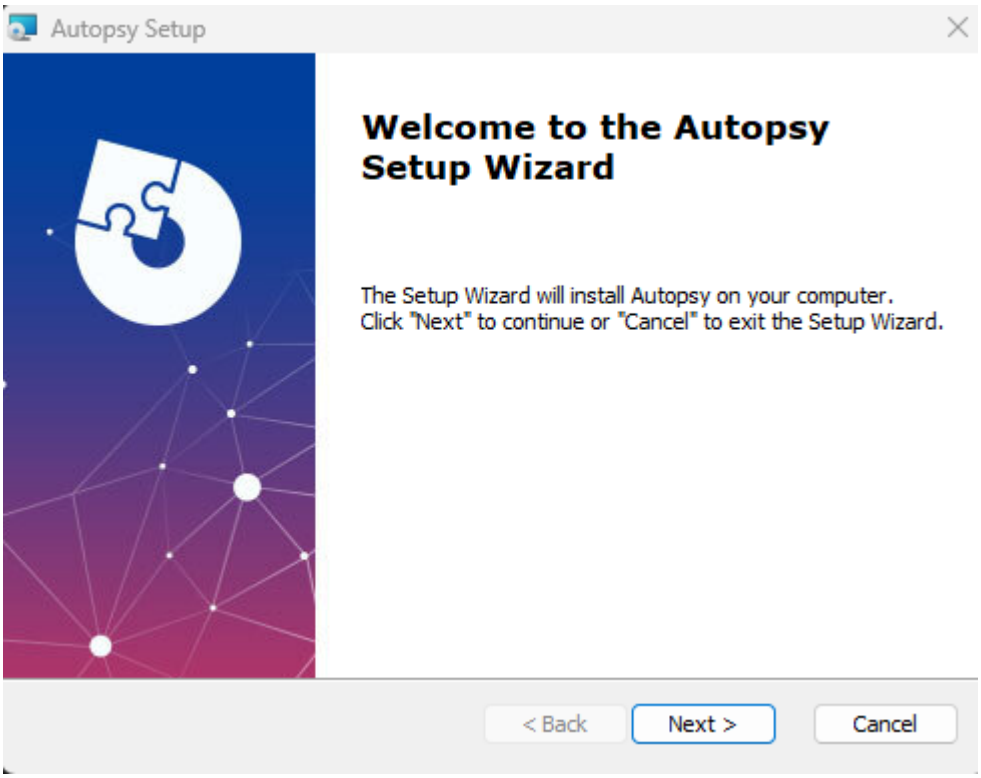


Ilustración 37 Inicio del asistente de instalación de Autopsy

En este paso, al ejecutar el archivo descargado autopsy-4.22.1-64bit, se inició el asistente de instalación (Setup Wizard) de Autopsy.

En la ventana de bienvenida se confirma que el programa procederá a instalar la aplicación en el equipo.

El instalador guía la instalación paso a paso a través del proceso, comenzando con la opción Next para continuar o Cancel para salir del asistente.

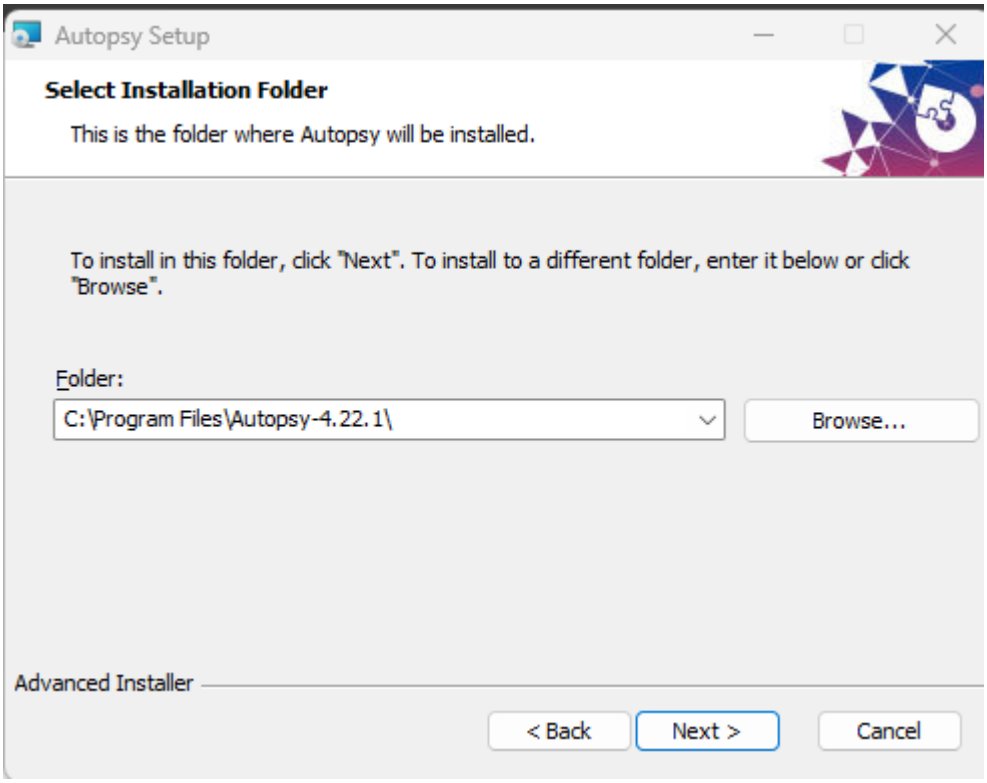


Ilustración 38 Selección del directorio de instalación

En esta ventana, el asistente de instalación solicita definir la carpeta donde se almacenarán los archivos del programa Autopsy. Por defecto, el instalador propone la ruta, la cual se dejó establecida así y se continuo.

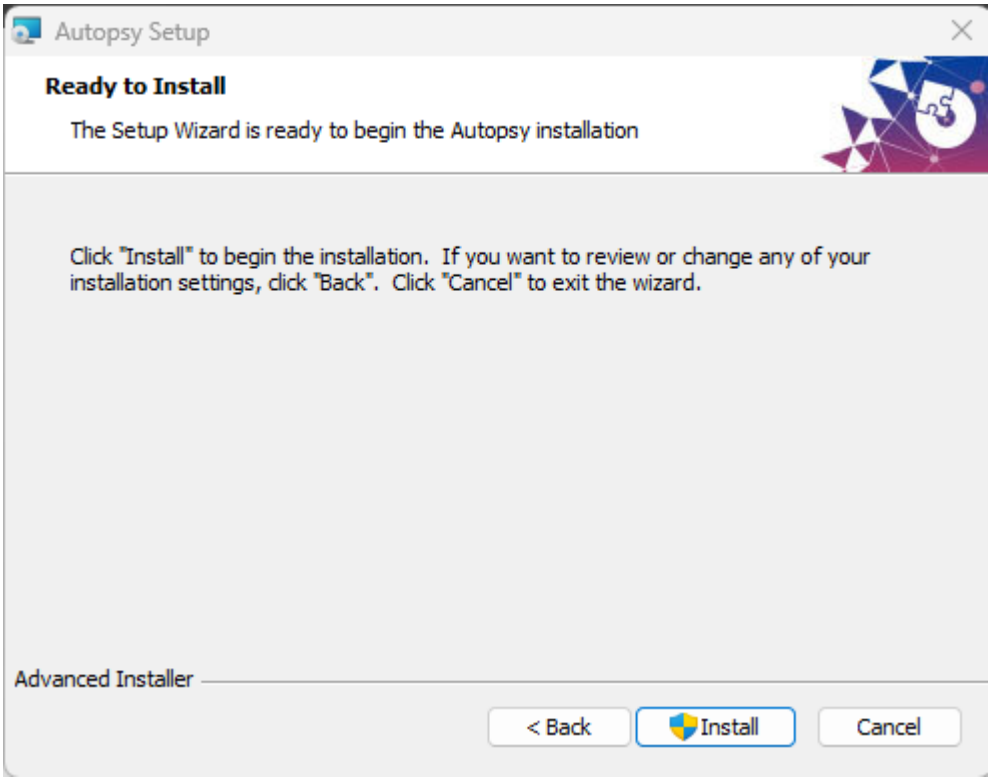


Ilustración 39 Confirmación e inicio de la instalación

En esta ventana, el asistente de instalación muestra un resumen final indicando que está todo listo para comenzar el proceso de instalación de Autopsy.

En caso de necesitar revisar o modificar alguna configuración previa, se puede retroceder con **Back,** o cancelar el proceso con **Cancel.**

Para continuar, se hizo clic en el botón **Install**, dando inicio al proceso de instalación de Autopsy en el sistema operativo Windows.

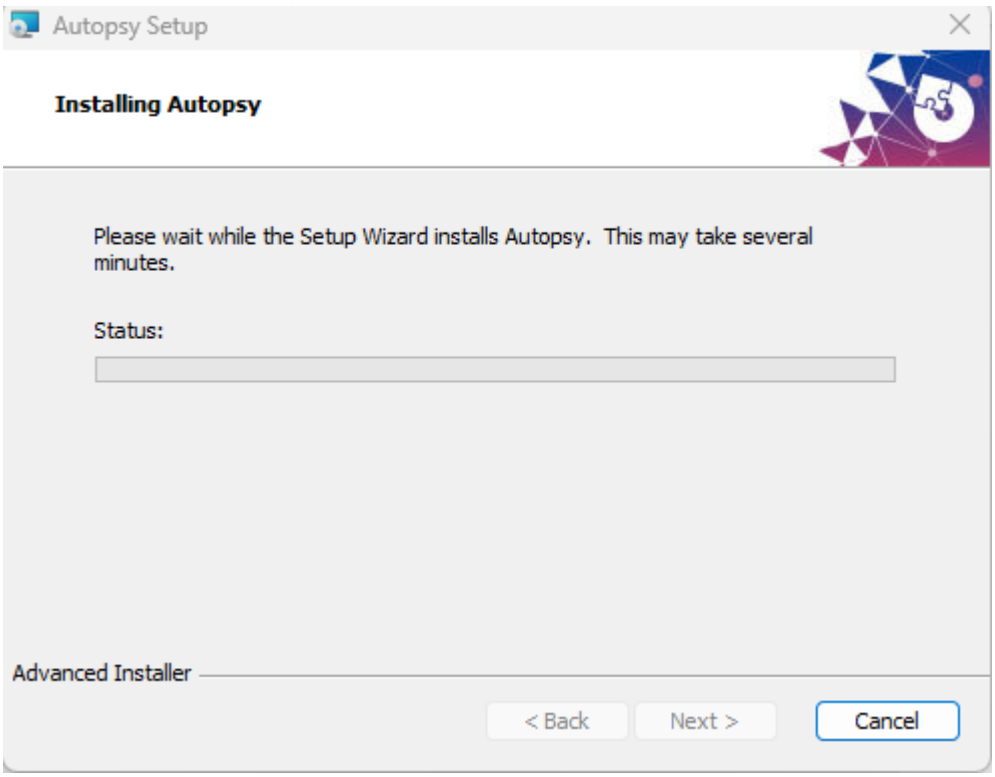


Ilustración 40 Instalación en proceso

En esta ventana se muestra el mensaje **Installing Autopsy**, indicando que el asistente de instalación está copiando los archivos necesarios al sistema.

El texto informa que el proceso puede tardar varios minutos mientras se completa la instalación.

En la parte inferior aparece la barra de progreso junto al campo Status, donde se muestra el avance del proceso.

En este paso, se debió esperar hasta que finalizara la instalación sin cerrar la ventana ni presionar ningún botón.

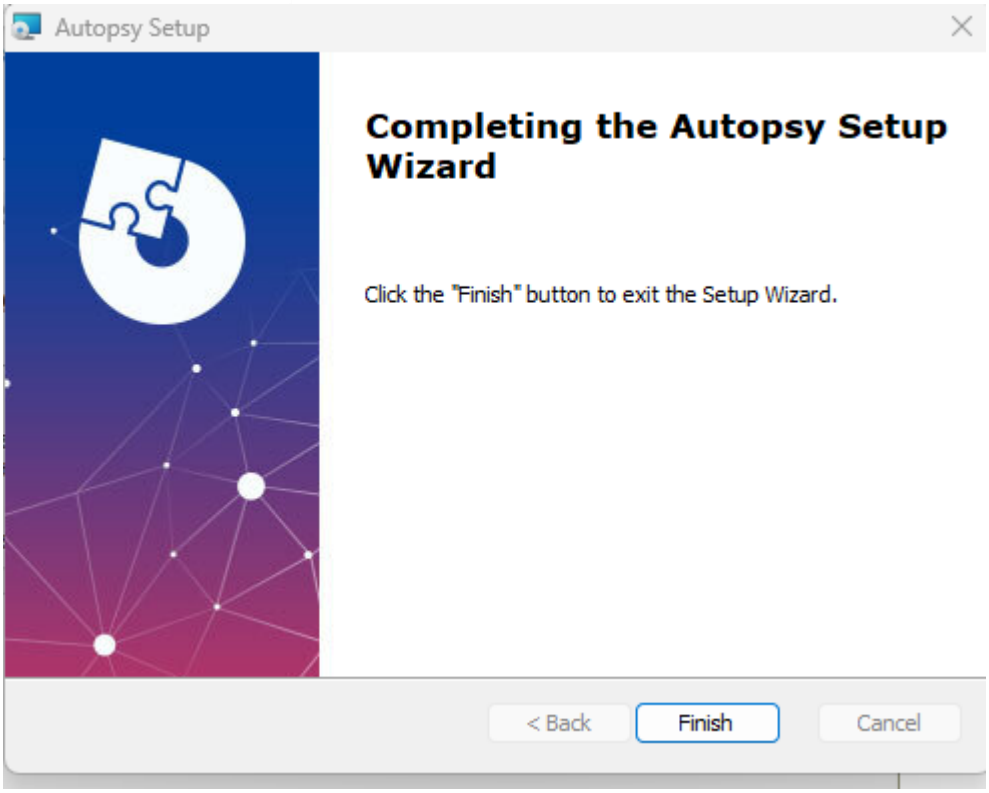


Ilustración 41 Finalización de la instalación de Autopsy

Una vez completado el proceso, aparece la ventana con el título Completing the Autopsy Setup Wizard, indicando que la instalación ha finalizado correctamente.

El asistente mostro también el mensaje Click the Finish button to exit the Setup Wizard, que solicita hacer clic en el botón **Finish** para cerrar el instalador.

En la parte inferior se encuentran los botones Back, Finish y Cancel, pero en este punto únicamente está habilitado Finish, ya que el proceso de instalación ha concluido.

Para completar el procedimiento, se presionó el botón **Finish**, y se cerró el asistente automáticamente.

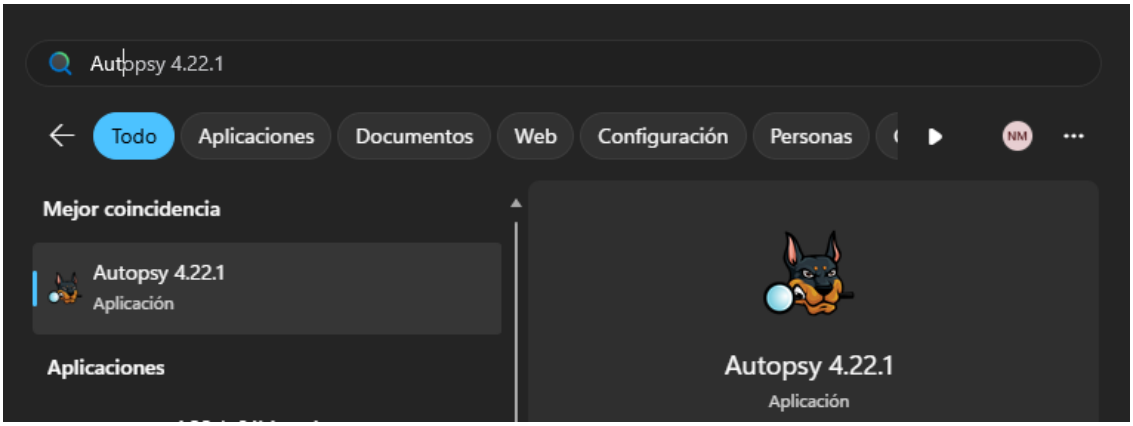


Ilustración 42 Búsqueda del programa Autopsy

Una vez completada la instalación, se procedió a abrir el programa.

Para ello, en la barra de búsqueda de Windows se escribió Autopsy. El sistema mostró como mejor coincidencia la aplicación Autopsy 4.22.1, junto con su ícono característico (un perro con una lupa) Para iniciar el software, se seleccionó la opción Autopsy 4.22.1 - Aplicación.

Ilustración 43 Carga inicial de Autopsy

Después de seleccionar la aplicación, se muestra la pantalla de inicio de Autopsy, donde aparece su logotipo característico, acompañado del texto Autopsy – Open |Extensible | Fast.

Durante este paso, el programa realiza la carga de sus módulos principales, lo que se indica en la parte inferior con el mensaje Turning on modules… y la barra de progreso.

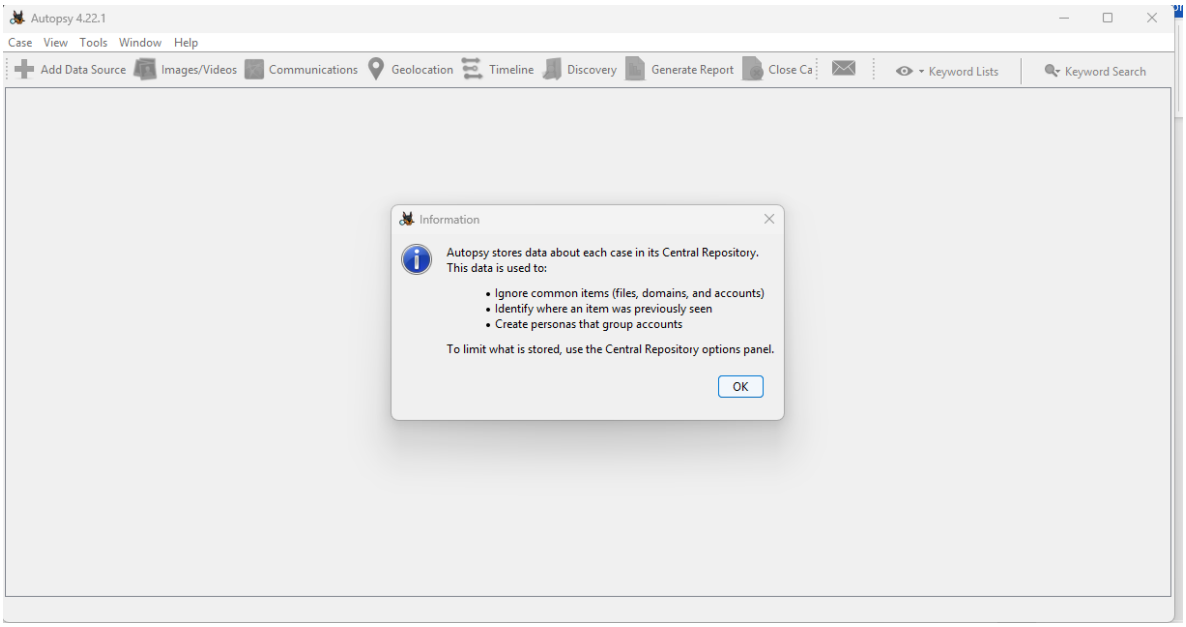


Ilustración 44 Primera ejecución de Autopsy

Una vez completada la carga de los módulos, se abre la interfaz principal del programa Autopsy 4.22.1, mostrando el entorno de trabajo.

Al iniciar por primera vez, aparece esta ventana emergente de información titulada Information, que indica que Autopsy almacena datos sobre cada caso en su repositorio central (Central Repository).

El mensaje explica que esta base de datos se utiliza para:

- Ignorar elementos comunes (archivos, dominios y cuentas).

- Identificar en qué casos anteriores se ha visto un mismo ítem.
- Crear personas que agrupan cuentas relacionadas.

También, se indica que para limitar qué información que guarda, se puede configurar esta opción desde el panel Central Repository.

Para continuar con el uso del programa, se realizó clic en el botón **OK** ubicado en la parte inferior del cuadro de diálogo.

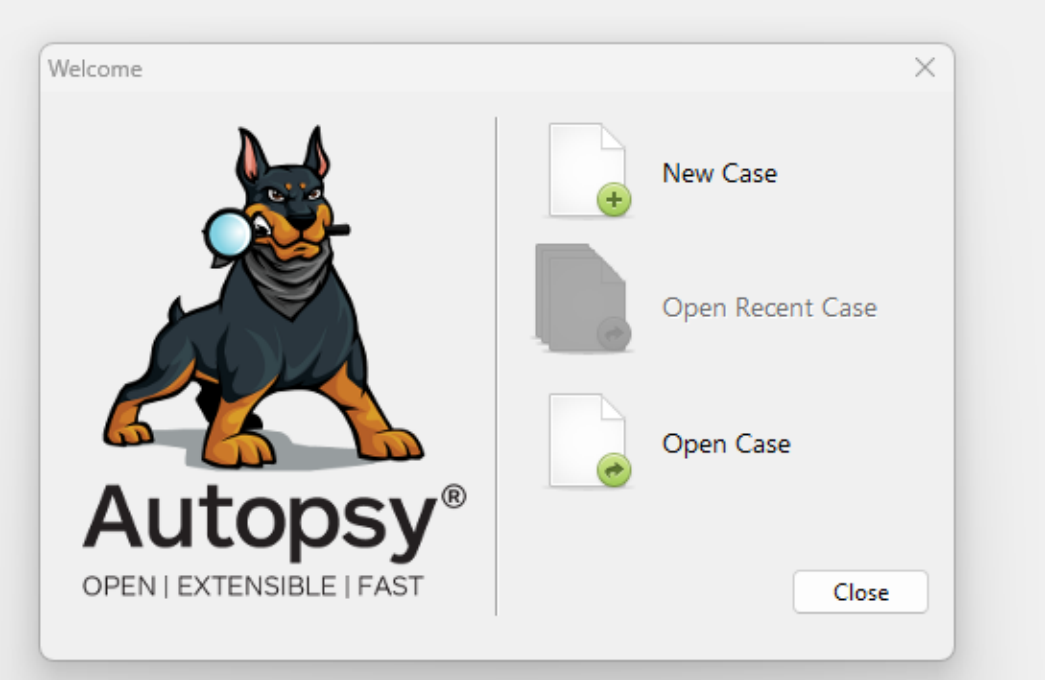


Ilustración 45 Ventana de inicio de Autopsy

Después de confirmar el mensaje anterior con el botón OK, se muestra la ventana de bienvenida del programa Autopsy, identificada con el título **Welcome**.

En esta vista aparece nuevamente el logotipo acompañado del texto Autopsy – Open | Extensible | Fast, que representa los principios del software: abierto, ampliable y rápido.

A la derecha se presentan tres opciones principales:

- New Case: permite crear un nuevo caso de análisis forense desde cero.
- Open Recent Case: ofrece la posibilidad de abrir un caso reciente trabajado anteriormente.
- Open Case: permite seleccionar y abrir un caso almacenado previamente en el sistema.

Y en la parte inferior derecha se encuentra el botón Close, que cierra esta ventana inicial. Para continuar con el laboratorio, se seleccionó la opción **New Case**, para crear un nuevo caso de análisis.

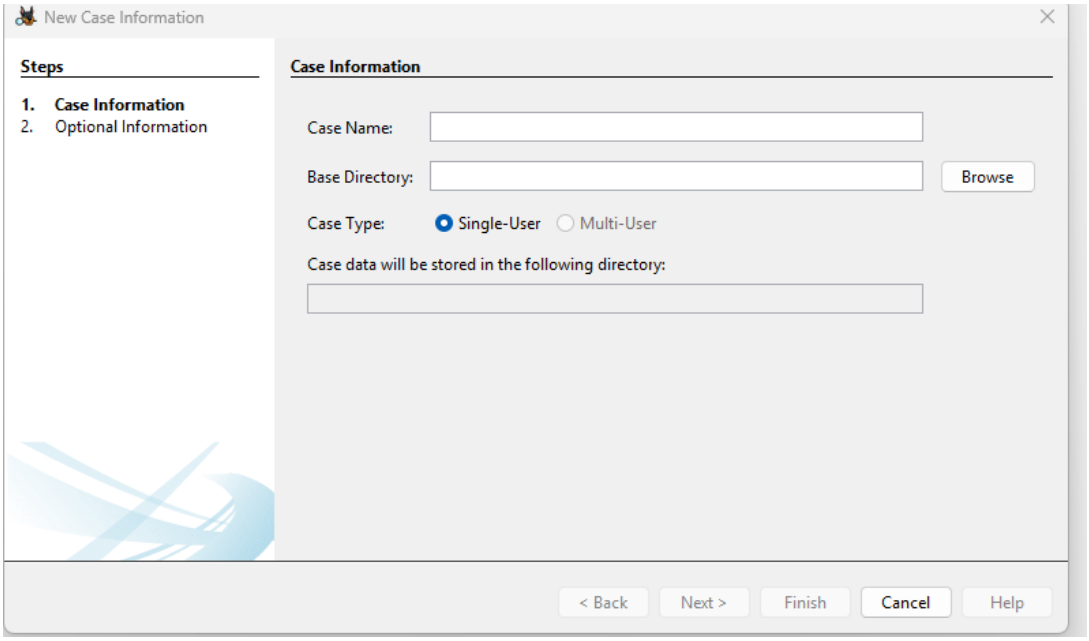


Ilustración 46 Creación de un nuevo caso

Después de seleccionar la opción New Case, se cargó esta |ventana New Case Information, en la cual se deben ingresar los datos básicos del nuevo caso de análisis.

En la sección principal, bajo el título Case Information, se encuentran los siguientes campos:

Case Name: aquí se escribe el nombre del caso que se desea crear.

Base Directory: indica la ubicación donde se almacenarán los archivos del caso. Se puede seleccionar de una carpeta específica mediante el botón **Browse**.

Case Type: ofrece dos opciones:

Single-User: seleccionada por defecto, permite que el caso sea gestionado por un único usuario.

Multi-User: opción destinada a entornos colaborativos.

En la parte inferior se muestra la ruta donde se guardarán los datos del caso una vez completado el proceso de creación. Para continuar, se ingresa la información correspondiente y clic en el botón **Next**.

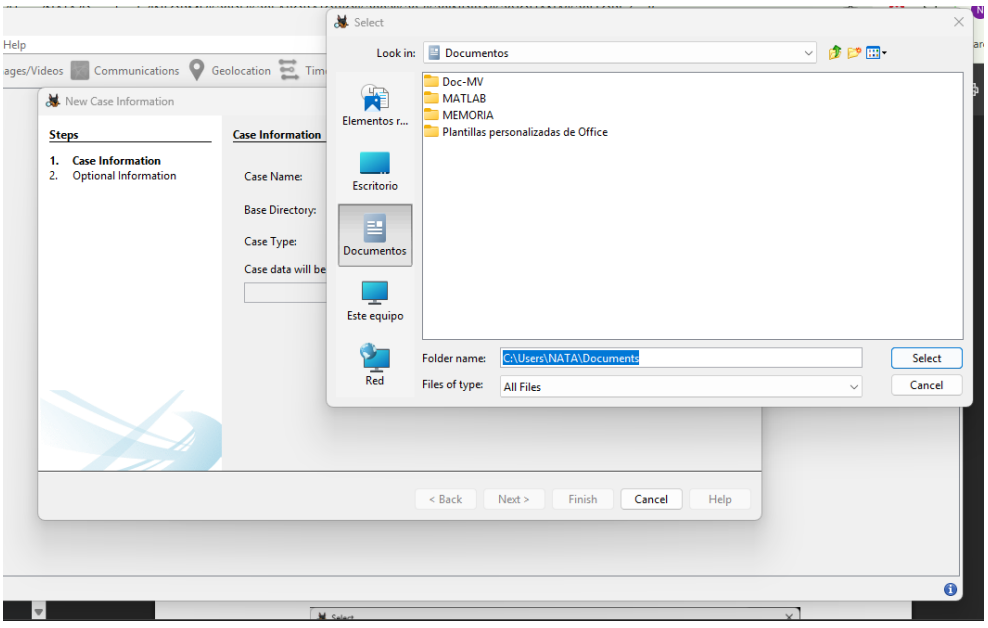


Ilustración 47 Selección del directorio base para el caso

En este paso, se realizó clic en el botón Browse, al hacerlo, se despliega esta nueva ventana titulada **Select**, que permite elegir la carpeta donde se almacenarán los archivos del caso forense.

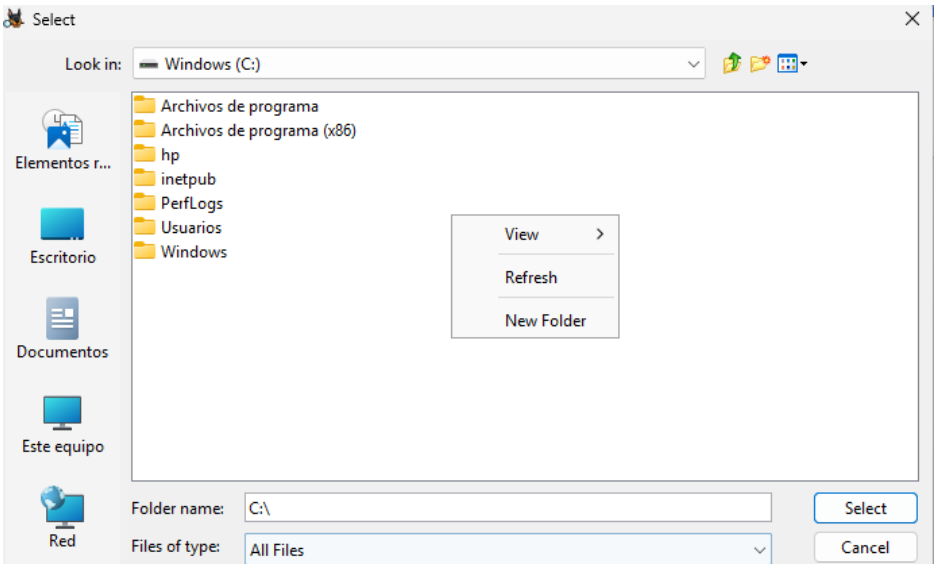


Ilustración 48Creación de un nuevo directorio para el caso

Con el explorador de archivos abierto, se decidió crear una nueva carpeta destinada exclusivamente al almacenamiento del caso forense, se hizo clic derecho en el área central del explorador, lo que desplegó un pequeño menú contextual con las siguientes opciones: View, Refresh, New Folder. A continuación, se seleccionó la opción **New Folder.**

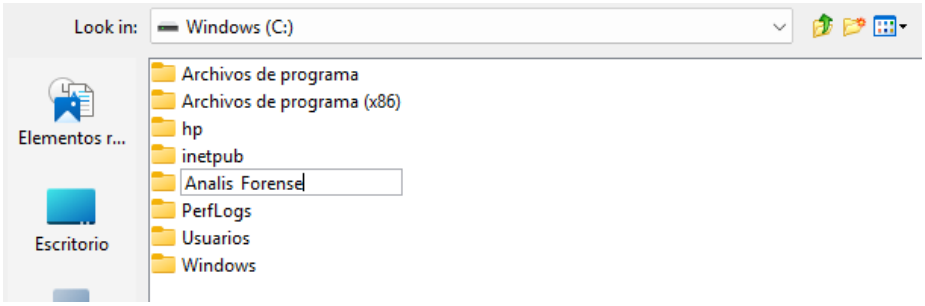


Ilustración 49 Asignación de nombre al nuevo directorio

Después de seleccionar la opción New Folder, se creó una nueva carpeta dentro del disco principal C: En ese momento, el sistema permitió editar el nombre del nuevo directorio. Se escribió el nombre **Análisis Forense**, el cual servirá como contenedor principal para todos los archivos y evidencias relacionadas con el caso.

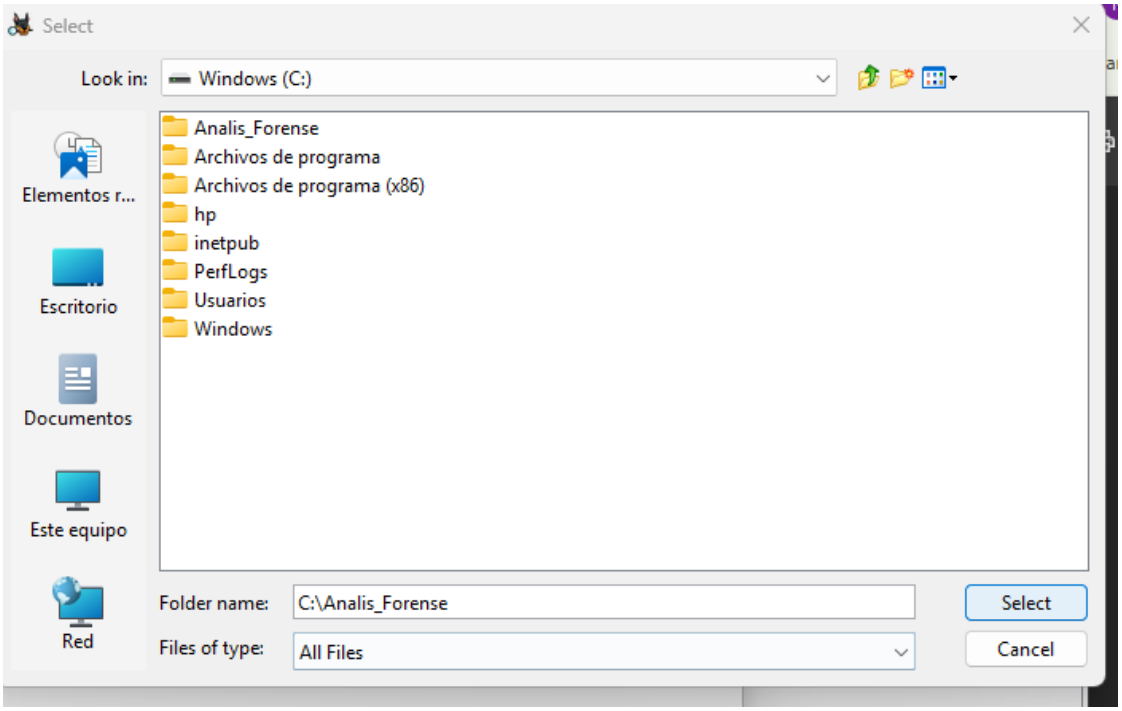


Ilustración 50 Selección del directorio creado

Después de nombrar la carpeta Analisis_Forense, se procedió a seleccionarla como la ubicación principal donde se almacenarán los archivos del caso.

En la ventana Select, se muestra la carpeta recién creada en la parte superior del listado del disco C:, junto con otras carpetas del sistema.

En el campo Folder name, ubicado en la parte inferior de la ventana, se visualiza la ruta completa del directorio: C:\Analisis_Forense

Para continuar, se hizo clic en el botón **Select,** se retornó automáticamente a la ventana de configuración del caso, donde la ruta seleccionada quedó registrada en el campo **Base Directory.**

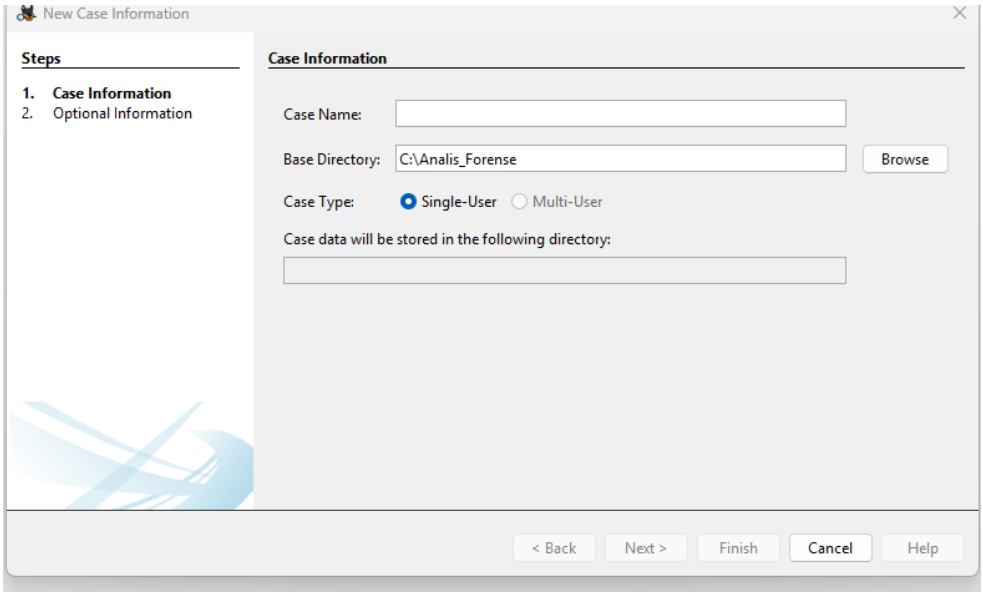


Ilustración 51Configuración de la información del caso

Una vez seleccionada la carpeta Analisis_Forense como directorio base, se mostró nuevamente esta ventana New Case Information con la ruta elegida reflejada en el campo Base Directory.

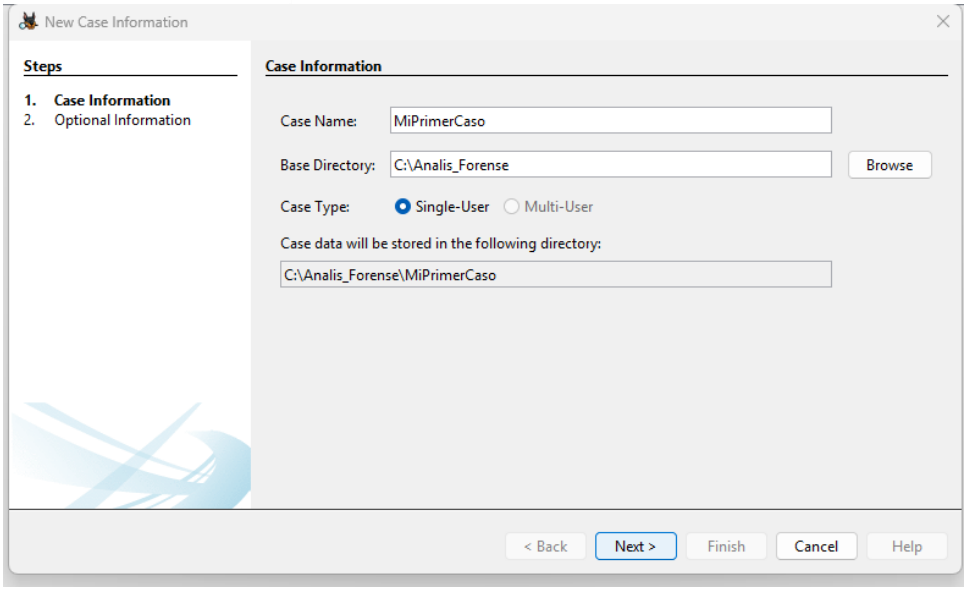


Ilustración 52 Asignación del nombre al caso

Con la ruta base ya configurada, se procedió a asignar un nombre al caso en el campo Case Name, el nombre que se ingresó fue **MiPrimerCaso**, el cual identifica de manera única la investigación que se llevará a cabo.

Al completar este campo, el programa genera automáticamente la ruta completa donde se almacenarán los archivos y resultados asociados al caso, la cual se muestra en la parte inferior de la ventana como: C:\Analisis_Forense\MiPrimerCaso

Se mantuvo la opción Single-User activada, ya que el análisis es realizado por un único usuario. Ya completados los datos, se hizo clic en el botón **Next** para continuar con la configuración del caso.

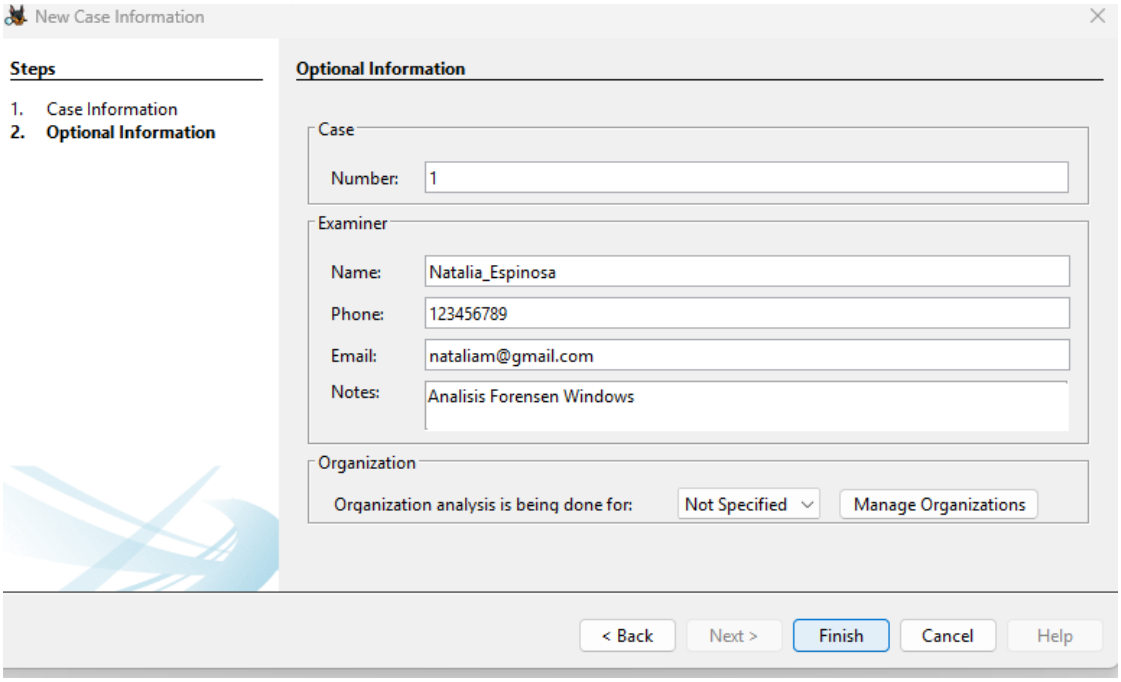


Ilustración 53 Ingreso de la información opcional del caso

Al hacer clic en Next, se cargó la ventana **Optional Information**, donde se completaron los campos adicionales del caso. Esta sección permite registrar datos que facilitan la identificación y documentación de la investigación.

En el primer apartado, Case, el programa pide un número al caso, al ser el primero, asigno: Number: 1

En la sección Examiner, se introdujeron los datos del analista responsable del caso. Estos campos sirven para dejar constancia de la autoría y el contexto del análisis realizado. En el apartado Organization, se mantiene la opción por defecto Not Specified, ya que no se asocia el caso a una organización en particular.

Una vez completados todos los datos, se presionó el botón **Finish** para crear el caso.

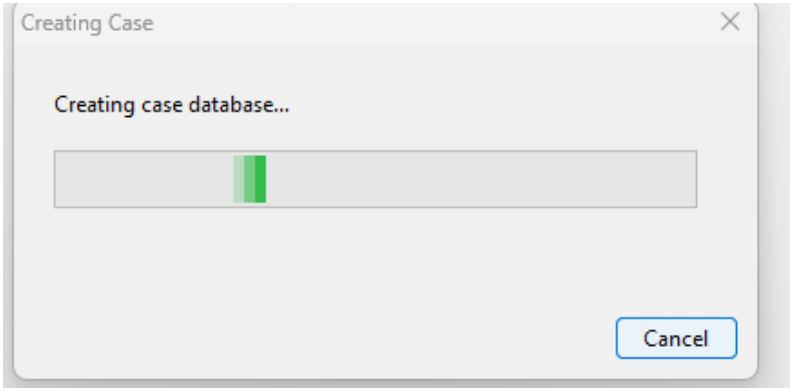


Ilustración 54Creación de la base de datos del caso

Después de presionar el botón Finish, el programa inició automáticamente el proceso de creación de la base de datos correspondiente al caso. Durante este proceso, se mostró una ventana con la barra de progreso y el mensaje Creating case database…,

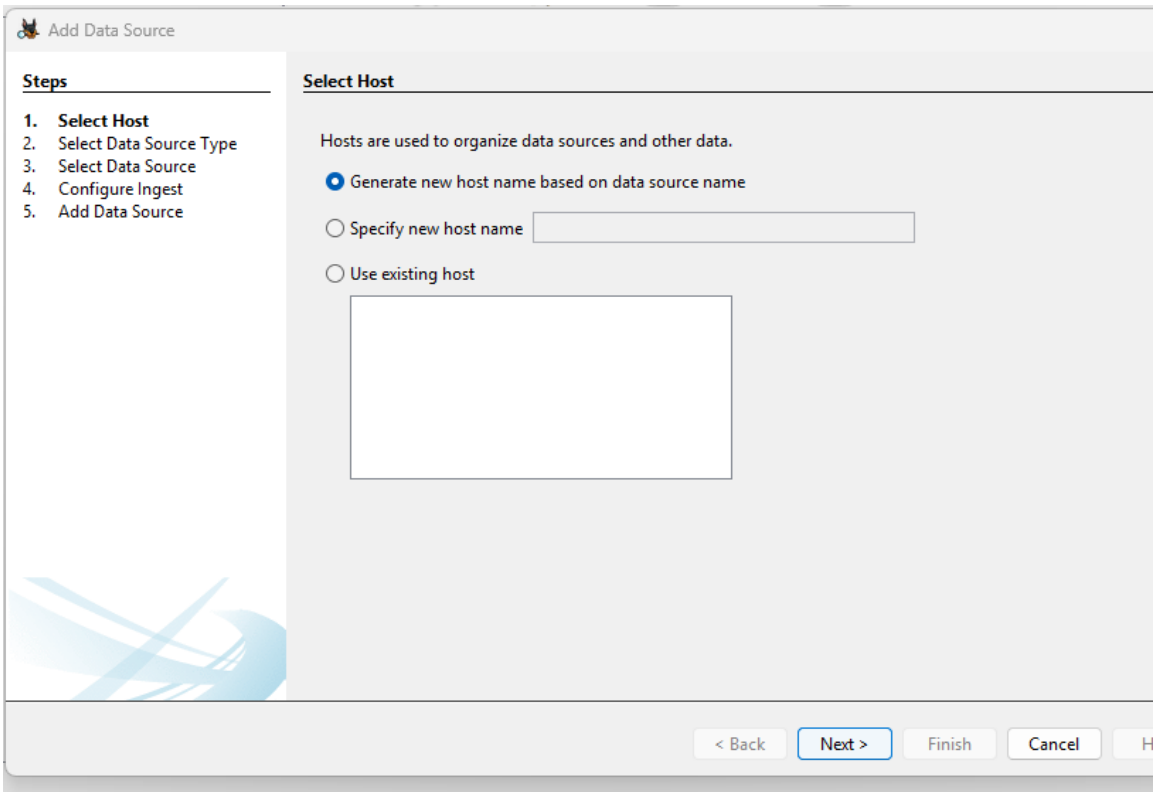


Ilustración 55 Selección del host para la fuente de datos

Una vez finalizada la creación de la base de datos del caso, Autopsy cargo esta ventana Add Data Source, donde se inicia el proceso para agregar la evidencia digital que será analizada. En esta primera parte, denominada Select Host, el sistema solicita definir el host al que se asociará la fuente de datos.

Se dejó seleccionada la opción **predeterminada Generate new host name based on data source name**, la cual permite que el programa genere automáticamente un nombre de host a partir del nombre del archivo o dispositivo que se importará. Una vez confirmada la opción, se hizo clic en el botón **Next** para avanzar a la siguiente sección.

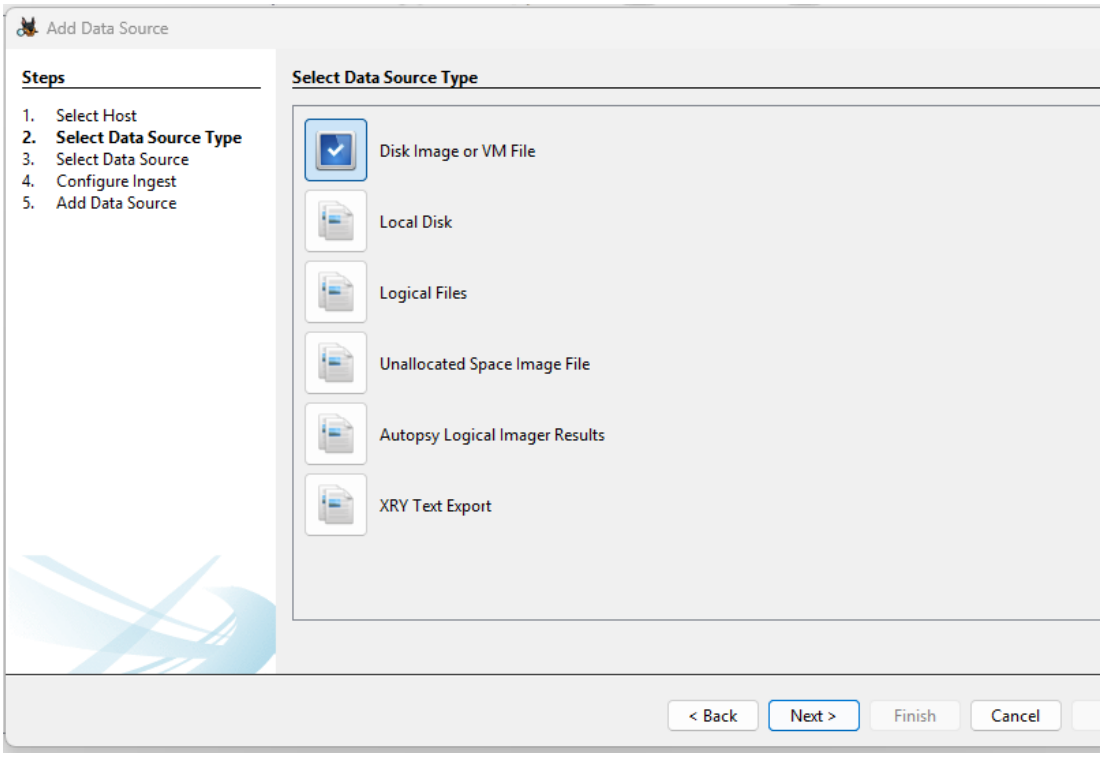


Ilustración 56 Selección del tipo de fuente de datos

Después de definir el host, Autopsy mostró la ventana Select Data Source Type, en la cual se debe especificar el tipo de evidencia que se incorporará al caso para su análisis. En este caso, se seleccionó la opción Disk Image or VM File: permite importar una imagen de disco o un archivo de máquina virtual.

Una vez marcada la opción, se hizo clic en el botón **Next** para continuar con la selección del archivo de imagen que será analizado.

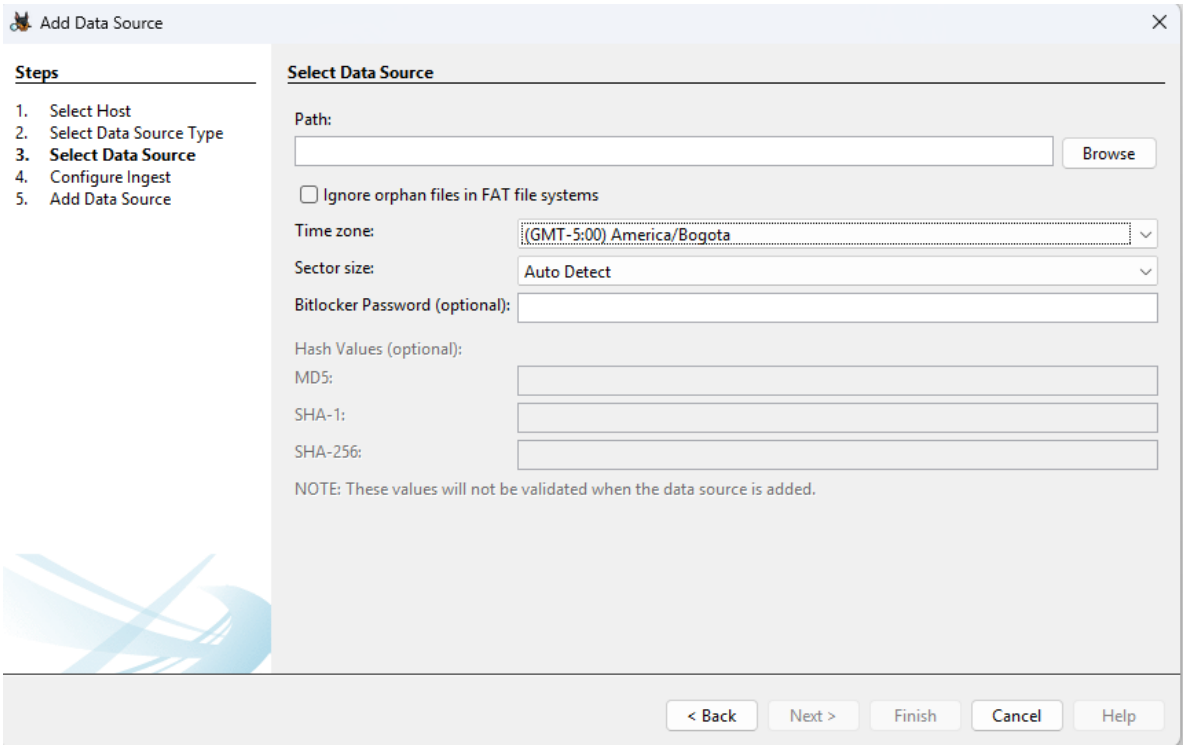


Ilustración 57 Selección de la fuente de la imagen forense

A continuación, se mostró la ventana **Select Data Source**, donde fue necesario indicar la ubicación del archivo de imagen que se desea analizar. Para localizar la imagen, se hizo clic en el botón **Browse**, lo que permitió abrir una nueva ventana del explorador de archivos para buscar la evidencia digital.

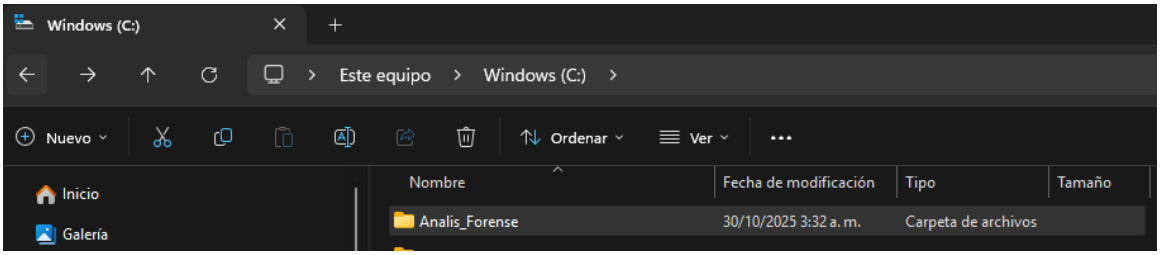


Ilustración 58 Ubicación de la carpeta de análisis

Se abrió el explorador de archivos de Windows, donde se navegó hasta la unidad C: del sistema. En esta ubicación se accedió a la carpeta Análisis_Forense, creada previamente para almacenar toda la información y los resultados asociados al caso

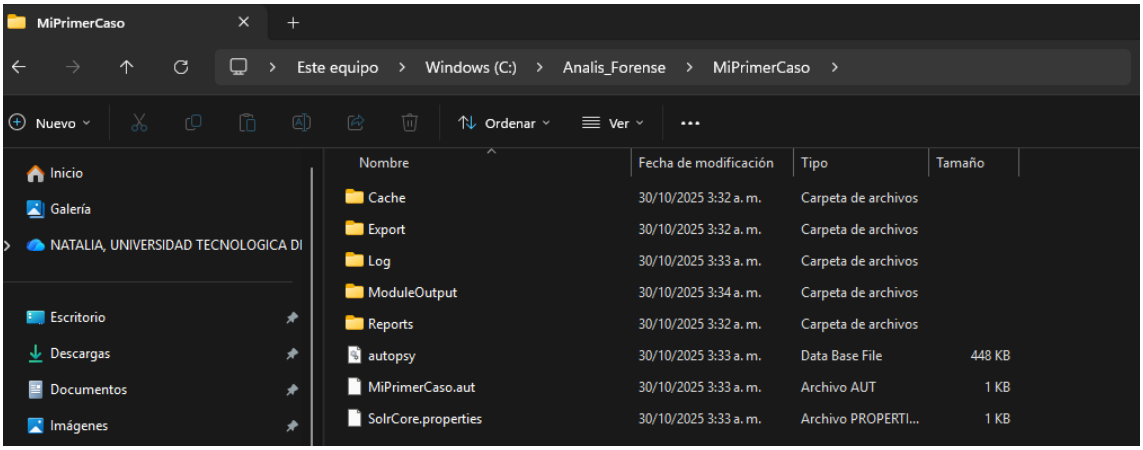


Ilustración 59 Acceso a la carpeta del caso creado

Después de ubicar la carpeta Analisis_Forense, se navegó dentro de ella hasta encontrar el directorio correspondiente al caso previamente configurado en Autopsy, denominado MiPrimerCaso.

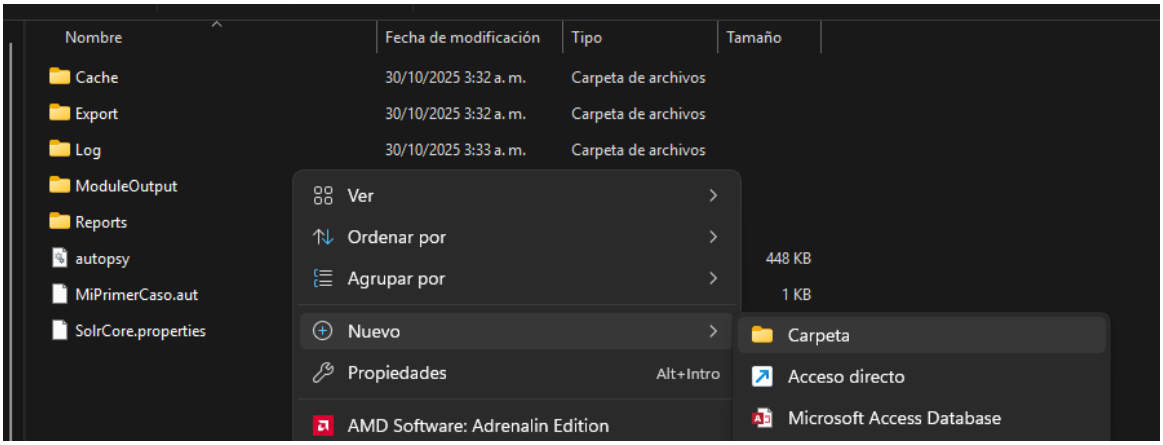


Ilustración 60 Creación de carpeta para almacenar la evidencia

Dentro del directorio del caso MiPrimerCaso, se creó una nueva carpeta para almacenar la imagen. Para ello, se hizo clic derecho dentro de la ventana del explorador y se seleccionó la opción Nuevo, Carpeta.

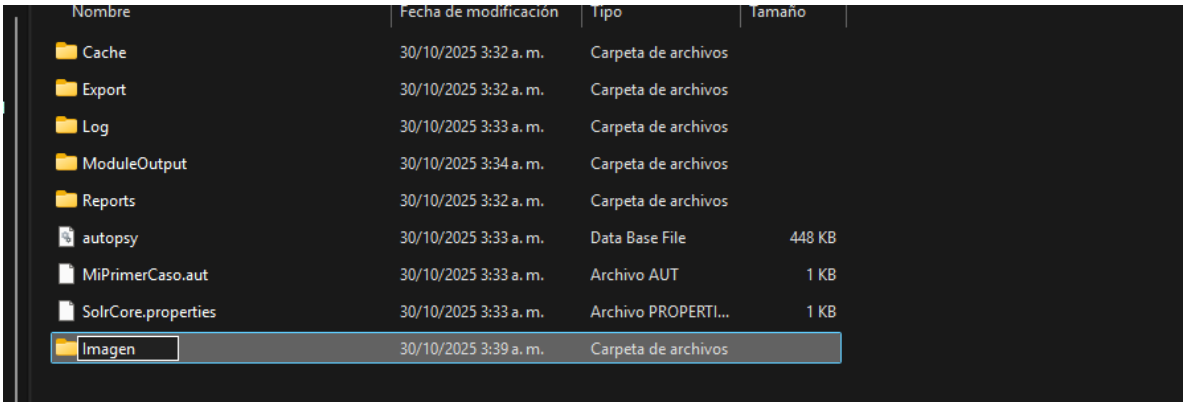


Ilustración 61 Asignación de nombre a la carpeta creada

Se dio el nombre Imagen a la carpeta, con el objetivo de identificarla claramente como el contenedor donde se almacenará la evidencia digital a analizar.

En los siguientes pasos, se detuvo temporalmente el trabajo en Windows y se continuó el proceso en el entorno Kali Linux, con el propósito de acceder a la memoria USB que contiene la imagen forense previamente creada.

```
┌──(root㉿kali)-[/home/kali]
└─# fdisk -l
Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 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: 0x8fc5489a

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sda1  *        2048 49641471 49639424 23,7G 83 Linux
/dev/sda2       49643518 52426751  2783234  1,3G  f W95 Ext'd (LBA)
/dev/sda5       49643520 52426751  2783232  1,3G 82 Linux swap / Solaris


Disk /dev/sdc: 238,47 GiB, 256060514304 bytes, 500118192 sectors
Disk model: able SSD 256
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: gpt
Disk identifier: FE577200-47B9-46ED-A817-F5D04D8CBC7B

Device         Start       End   Sectors   Size Type
/dev/sdc1       2048 500116015 500113968 238,5G Microsoft basic data
/dev/sdc2  500116050 500118128      2079     1M Microsoft basic data
```

Ilustración 62 Verificación de la USB

Se conectó una memoria USB al equipo y en Kali Linux, utilizando la opción Dispositivos, USB del menú de VirtualBox, se reconoció la memoria en la máquina virtual.

Una vez reconocida la unidad, se ejecutó el siguiente comando en la terminal para verificar los dispositivos de almacenamiento disponibles: fdisk -l

El comando mostró un listado detallado de los discos conectados, incluyendo sus tamaños, tipos de partición y rutas de acceso. Entre ellos, se identificó la memoria USB como el dispositivo /dev/sdc1, con una capacidad aproximada de 238.47 GiB, correspondiente a la USB conectada.

```
┌──(root㉿kali)-[/home/kali]
└─# mount /dev/sdc1 /mnt/usb
The disk contains an unclean file system (0, 0).
The file system wasn't safely closed on Windows. Fixing.
```

Ilustración 63 Montaje de la memoria USB en Kali Linux

Una vez verificada la detección correcta del dispositivo, se procedió a montar la memoria USB en el sistema de archivos de Kali Linux, para poder de acceder a su contenido. Para ello, primero se creó el directorio /mnt/usb, el cual serviría como punto de montaje, mediante el siguiente comando: mkdir -p /mnt/usb

Luego, se ejecutó el comando de montaje: mount /dev/sdc1 /mnt/usb

Una vez finalizado el proceso, la memoria quedó montada correctamente en la ruta /mnt/usb, lista para transferir el archivo.

Ilustración 64 Copia de la imagen forense a la memoria USB

Después de montar correctamente la memoria USB en el sistema, se procedió a copiar la imagen forense generada en el capítulo 1, hacia la USB. La imagen se encontraba almacenada en la ruta: /home/kali/Escritorio/imagen_usb_forense.dd Para realizar la transferencia, se ejecutó el comando: cp /home/kali/Escritorio/imagen_usb_forense.dd /mnt/usb

Este comando copio el archivo imagen_usb_forense.dd desde su ubicación original en el escritorio hacia la carpeta montada en /mnt/usb, que corresponde al contenido de la memoria USB.

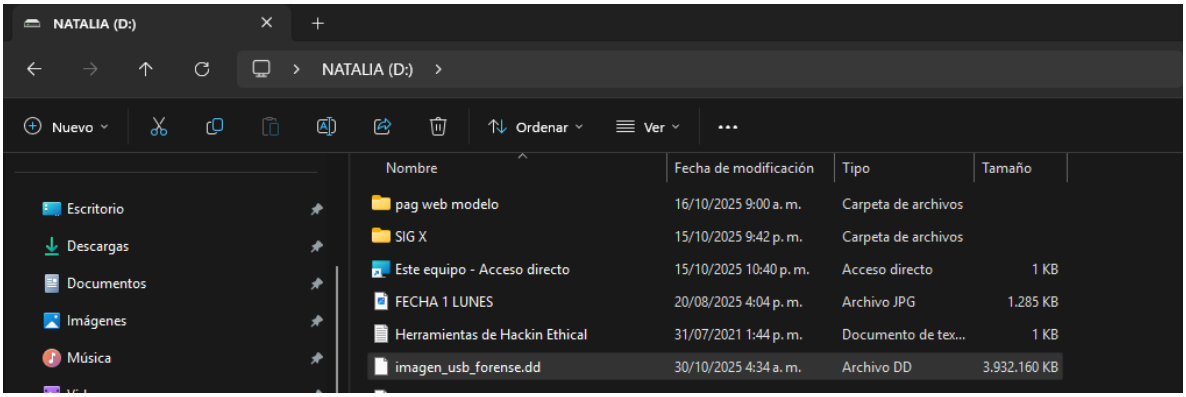


Ilustración 65 verificación en Windows de la imagen

Una vez finalizada la copia de la imagen forense en la USB, se procedió a desconectarla de forma segura desde el entorno de Kali Linux. La desconexión se realizó desde el menú de Dispositivos, USB de la máquina virtual, desmarcando la memoria conectada. Esto liberó el control del dispositivo del entorno Linux, permitiendo que el sistema Windows la reconociera nuevamente.

Y al acceder al Explorador de archivos de Windows, se verificó que el proceso de copia se había realizado correctamente, observándose dentro de la memoria el archivo imagen_usb_forense.dd

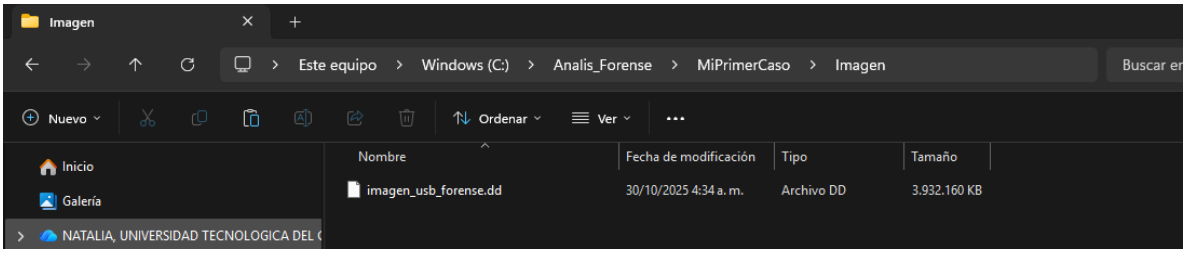


Ilustración 66 Copia de la imagen forense a la carpeta del caso

Una vez que la memoria USB fue reconocida nuevamente por Windows, se procedió a copiar el archivo imagen_usb_forense.dd hacia la carpeta del caso creada previamente en el directorio del análisis.

La copia se realizó dentro de la ruta C:\Analis_Forense\MiPrimerCaso\Imagen, carpeta que había sido creada específicamente para almacenar la imagen forense. De esta manera, la evidencia digital quedó almacenada dentro del entorno del caso en Autopsy.

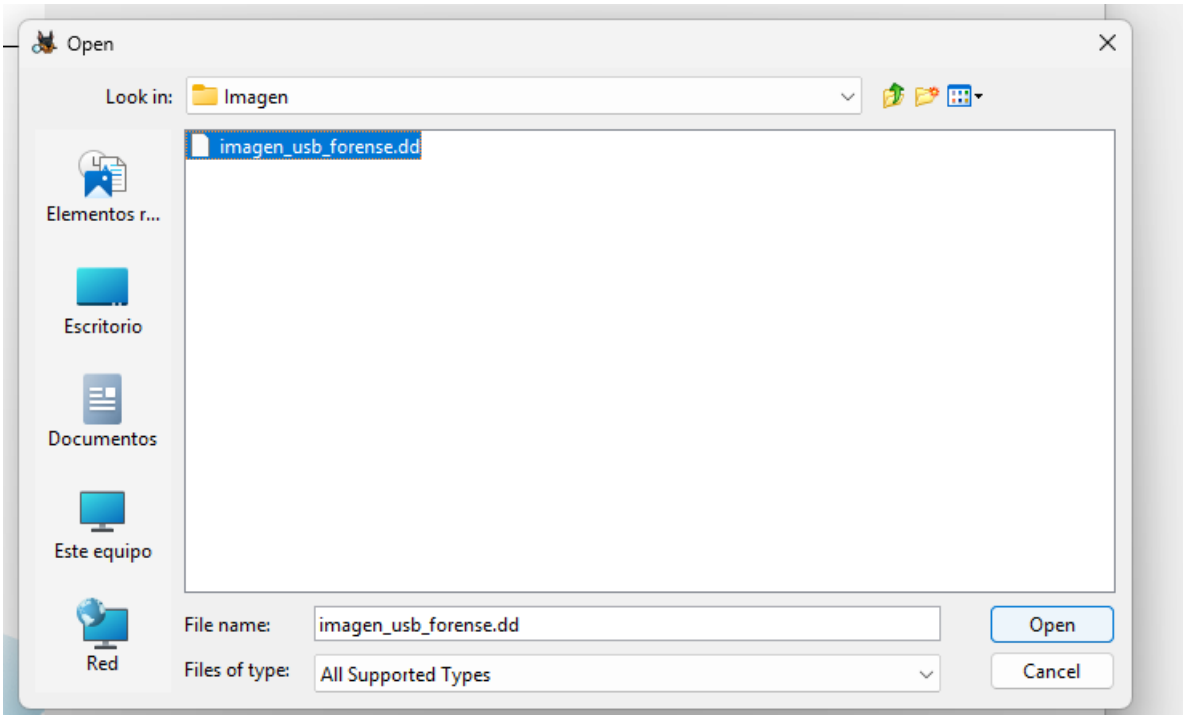


Ilustración 67 Selección de la imagen forense en Autopsy

Una vez copiada la evidencia digital en el sistema Windows, se retomó el proceso dentro de la herramienta Autopsy, exactamente desde el punto donde se había pausado.

Desde la ventana del explorador de archivo que se había cargado, desde allí, se navegó hasta la carpeta C:\Analis_Forense\MiPrimerCaso\Imagen, donde se almaceno la imagen forense.

Dentro de dicha carpeta, se seleccionó el archivo imagen_usb_forense.dd,y se realizó clic en el botón Open:

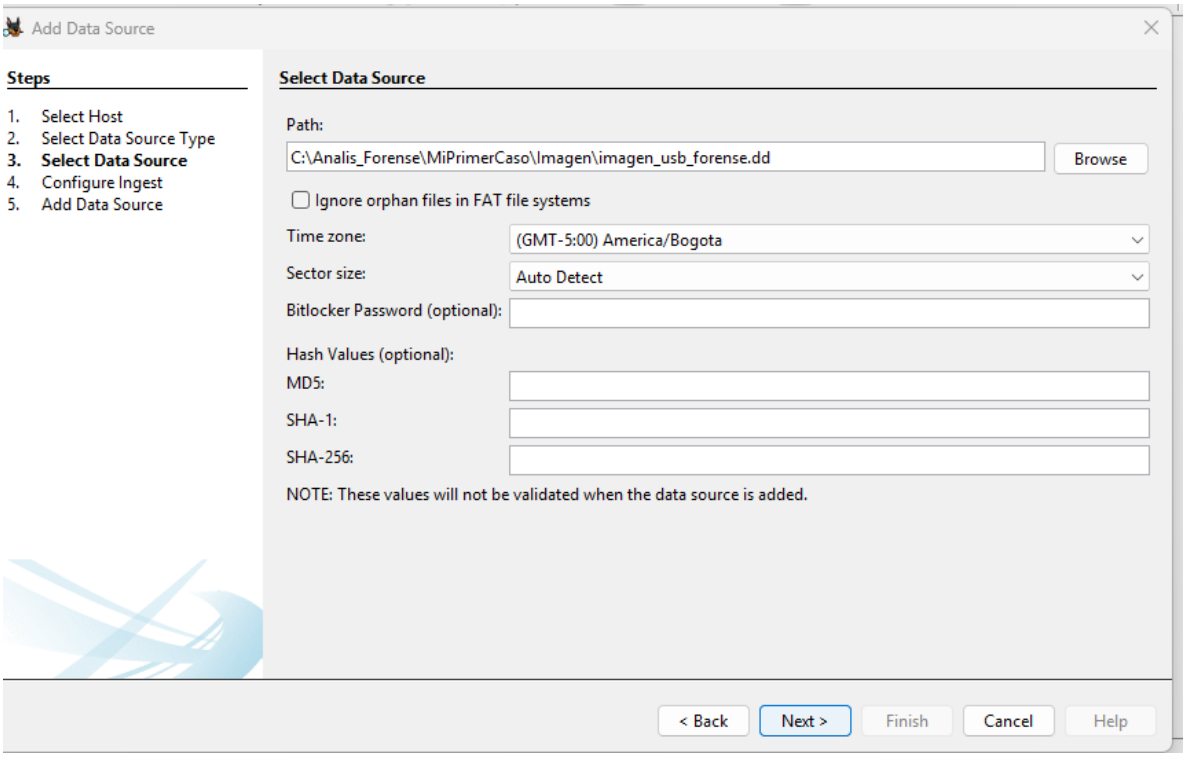


Ilustración 68 Configuración de la fuente de datos en Autopsy

Una vez seleccionada la imagen forense imagen_usb_forense.dd, se cargó automáticamente su ruta completa en el campo Path, mostrando la dirección de la ruta.

En el campo Time zone, se seleccionó la zona horaria (GMT-5:00) America/Bogota, correspondiente a la ubicación local donde se realiza el análisis. Y se continuó con el proceso haciendo clic en el botón **Next.**

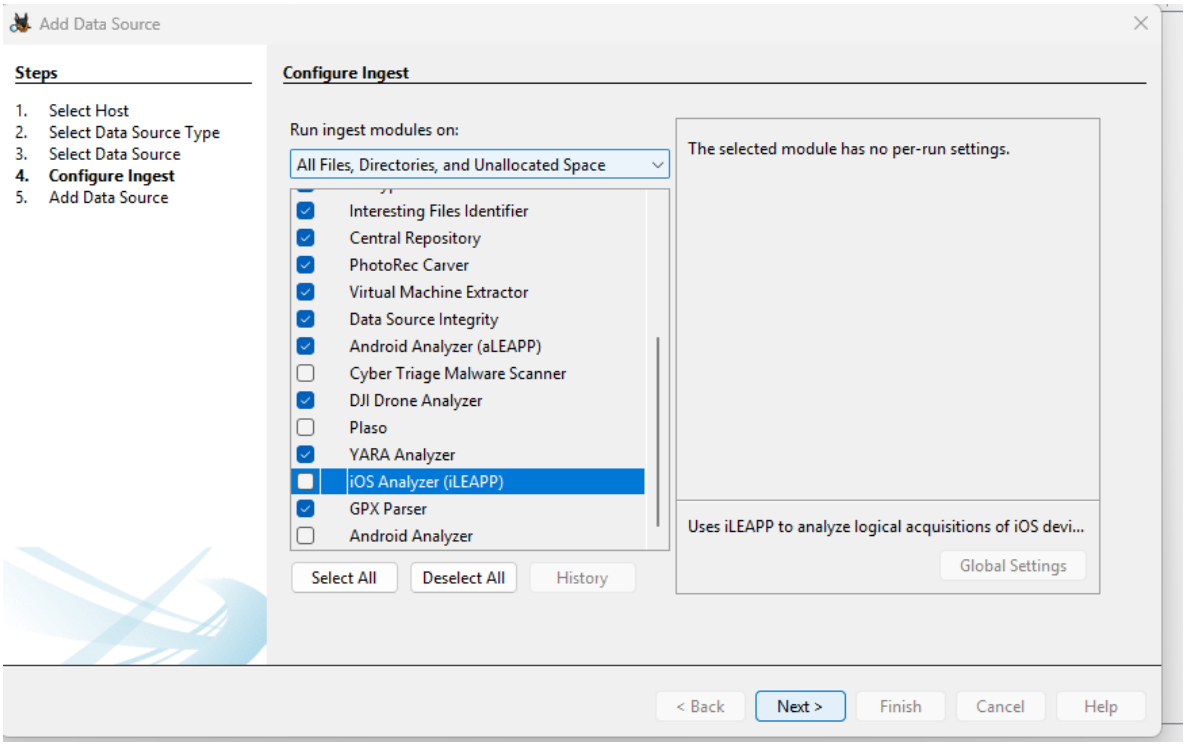


Ilustración 69 Configuración de los módulos de análisis

En esta ventana, denominada Configure Ingest, se presentaron los distintos módulos que Autopsy ofrece para realizar el análisis forense sobre la imagen cargada.

En el menú desplegable superior Run ingest modules on, se seleccionó la opción All Files, Directories, and Unallocated Space, con el propósito de analizar todos los archivos, directorios y espacios no asignados de la imagen forense, asegurando así una revisión completa del contenido.

También, se verificaron los módulos que se ejecutarían durante el proceso, se seleccionaron los necesarios para el análisis forense .

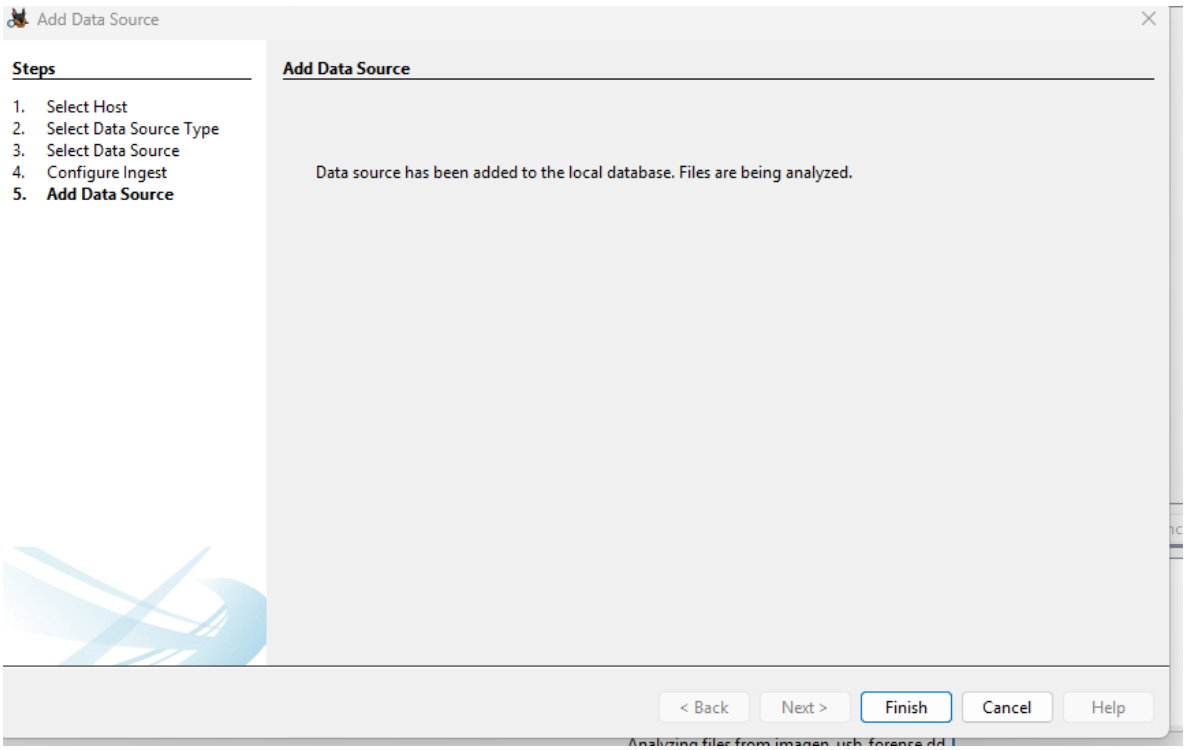


Ilustración 70 Análisis de la fuente de datos

Una vez configurados los módulos de análisis, se continuo al último paso del asistente, llamado Add Data Source. En esta ventana se confirmó que la fuente de datos que es la imagen forense imagen_usb_forense.dd y que había sido correctamente añadida a la base de datos local del caso.

Para continuar con los siguientes pasos, se hizo clic en el botón **Finish**, finalizando el asistente de configuración e ingresando a la interfaz principal del análisis del caso.

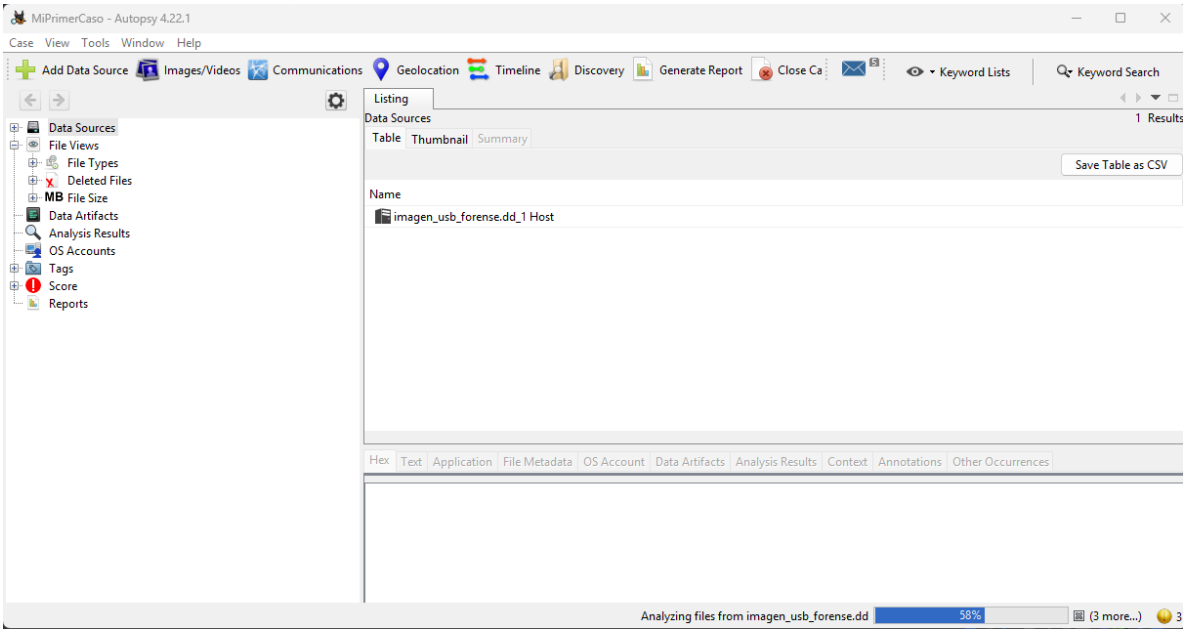
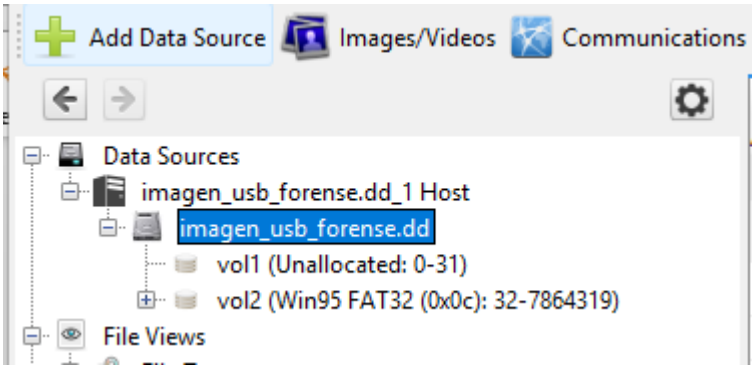


Ilustración 71 Interfaz principal de análisis en Autopsy

Al finalizar la configuración del caso, se cargó la interfaz principal de Autopsy, mostrando el entorno de trabajo correspondiente al caso “MiPrimerCaso”. En esta vista se evidenció que el análisis de la imagen forense imagen_usb_forense.dd había iniciado correctamente.



En el panel izquierdo de la ventana, se presentaron las distintas secciones que componen la estructura del caso, entre ellas: Data Sources: lista de fuentes de datos cargadas, donde se muestra la imagen imagen_usb_forense.dd como principal.

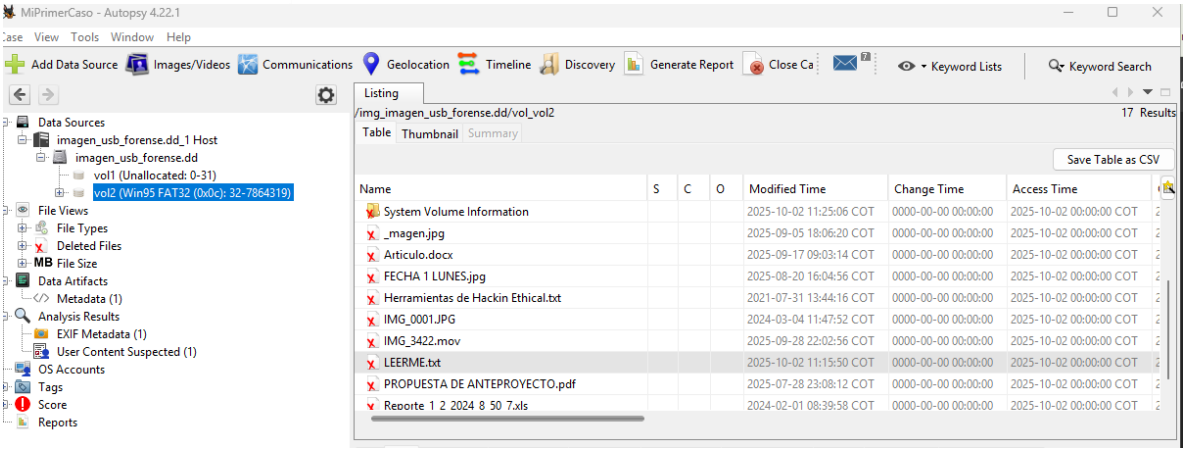


Ilustración 72 Visualización de archivos recuperados

En este paso, se procedió a explorar el contenido de la fuente de datos, presionando el icono + se logró abrir los volúmenes, la estructura interna de la imagen imagen_usb_forense.dd contiene dos volúmenes:

- vol1 (Unallocated 0-31)
- vol2 (Win95 FAT32 0:0b; C32–7864319)

Se seleccionó el volumen vol2, correspondiente al sistema de archivos FAT32, que es el formato utilizado por la USB.

Al seleccionarlo, en el panel central cargo la pestaña listado(Listing) de archivos contenidos en dicho volumen , entre los que se pudieron identificar varios tipos de evidencia digital, como: Imágenes, Videos y Documentos.

En la parte superior de la tabla se mostraron las columnas correspondientes a la información de metadatos de cada archivo, el nombre, fecha de modificación (Modified Time), fecha de cambio (Change Time) y fecha de acceso (Access Time):

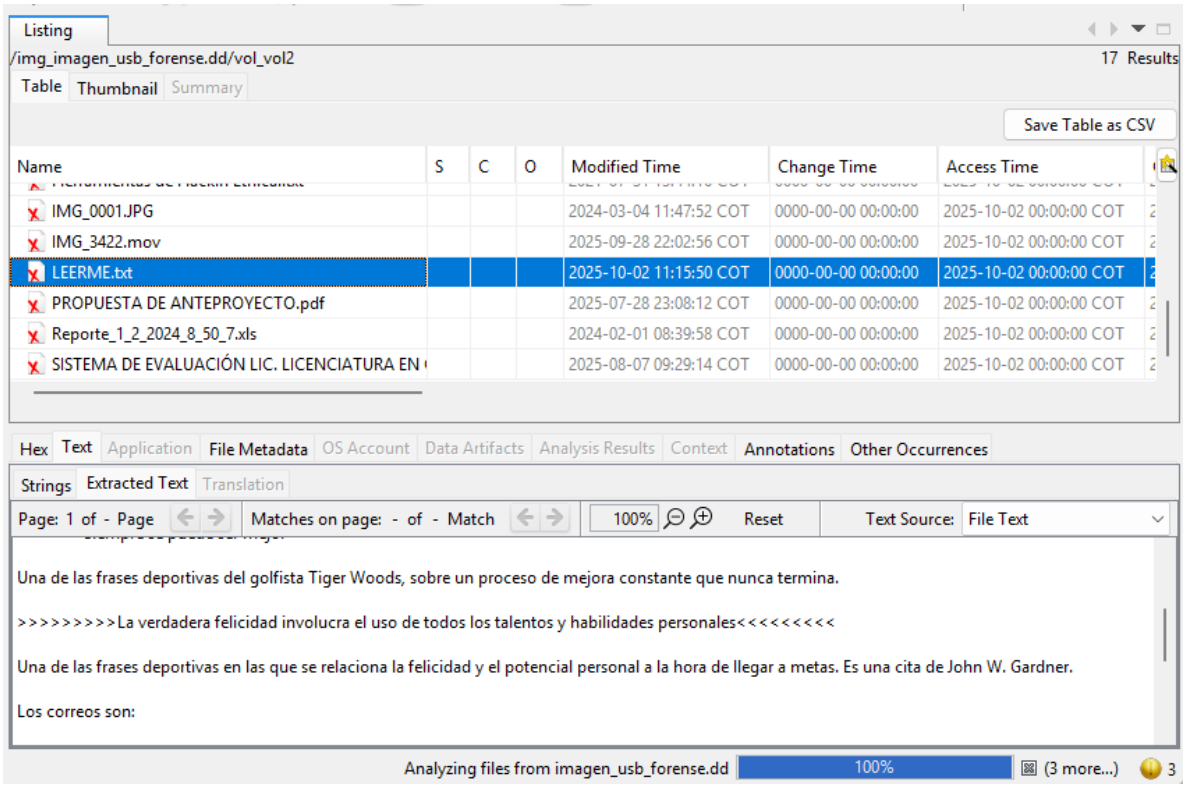


Ilustración 73 Visualización de archivos recuperados parte dos

En este paso, se seleccionó el archivo LEERME.txt, el cual forma parte del volumen vol2 (Win95 FAT32) de la imagen imagen_usb_forense.dd.

En la parte inferior de la interfaz, se cargó la pestaña Text, donde Autopsy mostró el contenido interno del archivo en formato de texto plano. El panel de análisis permite alternar entre diferentes vistas, como:

- Hex: para observar la estructura en formato hexadecimal.
- Text: para visualizar el contenido legible.
- File Metadata: donde se muestran los metadatos asociados (fechas de creación, modificación y acceso).

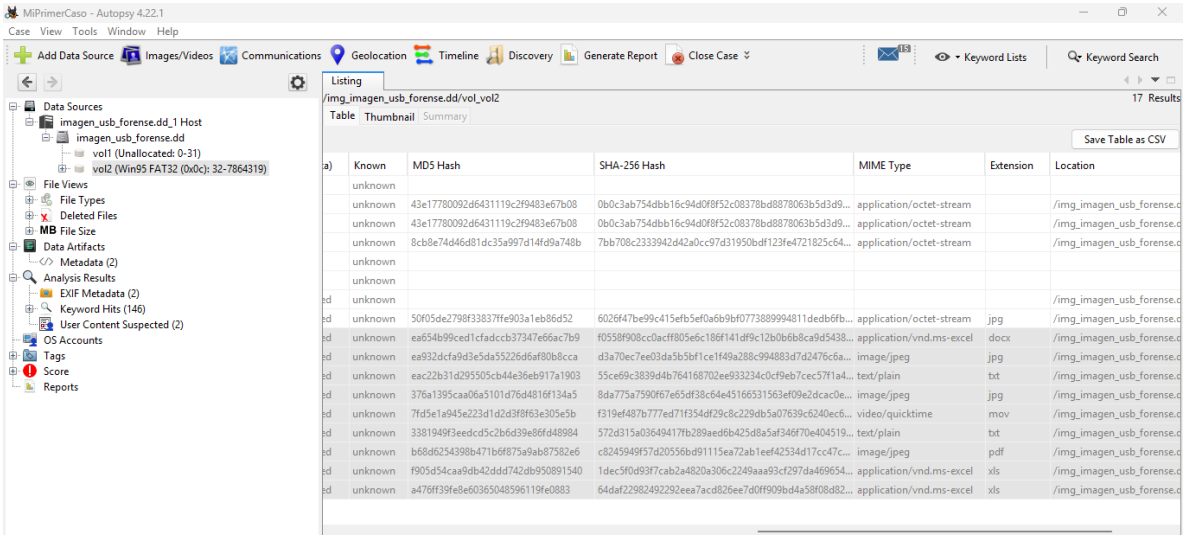


Ilustración 74 Visualización de archivos recuperados hash

En este último paso, al desplazarse hacia la derecha en la vista de tabla dentro del panel Listing, fue posible visualizar las columnas correspondientes a los valores hash generados por Autopsy para cada uno de los archivos analizados.

Entre las columnas mostradas se incluyen los identificadores: MD5 Hash, SHA-256 Hash, MIME Type, Extension, Location.

Estos valores permiten validar la integridad y autenticidad de los archivos recuperados durante el análisis, y así, se concluyó exitosamente el análisis forense de la imagen imagen_usb_forense.dd en Autopsy sobre Windows

3 CAPITULO 3: ANÁLISIS FORENSE CON FTK IMAGER EN WINDOWS

En este capítulo se documenta el proceso de análisis forense utilizando la herramienta FTK Imager, que al igual que Autopsy, permite visualizar, capturar y examinar datos digitales de forma segura sin alterar la evidencia original.

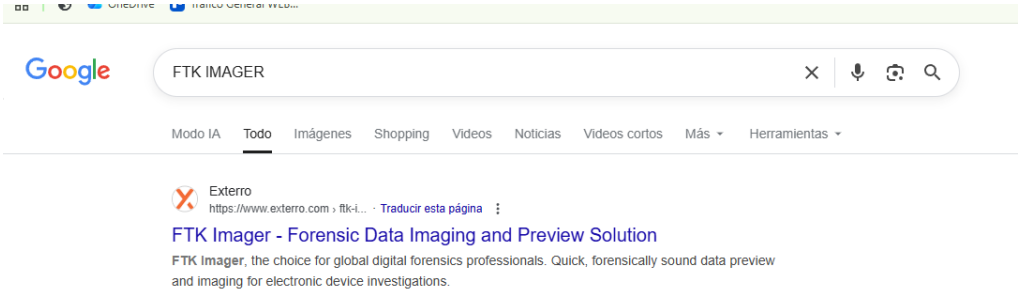


Ilustración 75 Búsqueda del software

Para iniciar, se realizó la búsqueda del programa FTK Imager en el navegador web. En los resultados de búsqueda de Google, se identificó el sitio oficial de la herramienta, alojado en el dominio www.exterro.com bajo el nombre FTK Imager – Forensic Data Imaging and Preview Solution, tal como se muestra en la imagen.

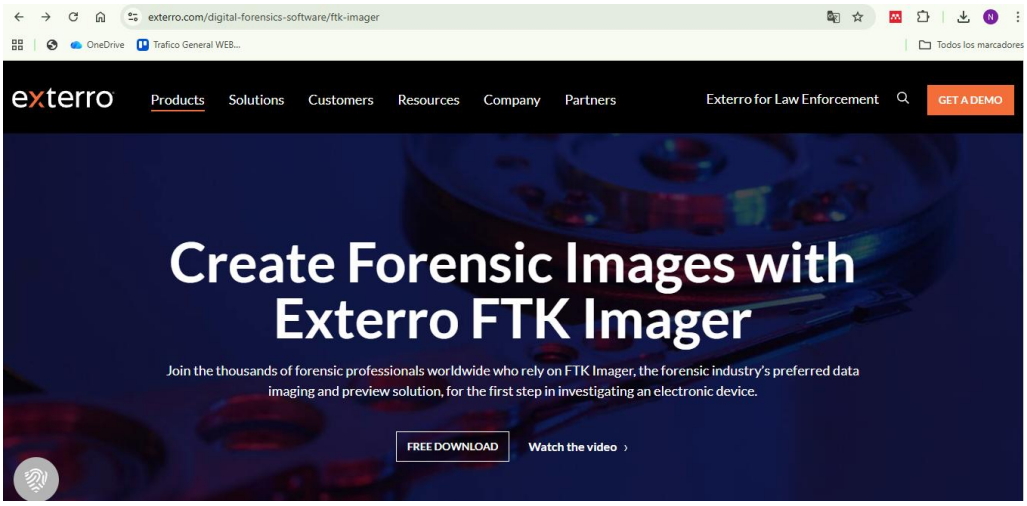


Ilustración 76 Sitio oficial de FTK Imager

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Al ingresar al sitio web oficial de Exterro, se presentó la página principal del producto FTK Imager. En la parte central de la ventana se muestra el botón de acción identificado como FREE DOWNLOAD, el cual permite acceder al proceso de descarga.

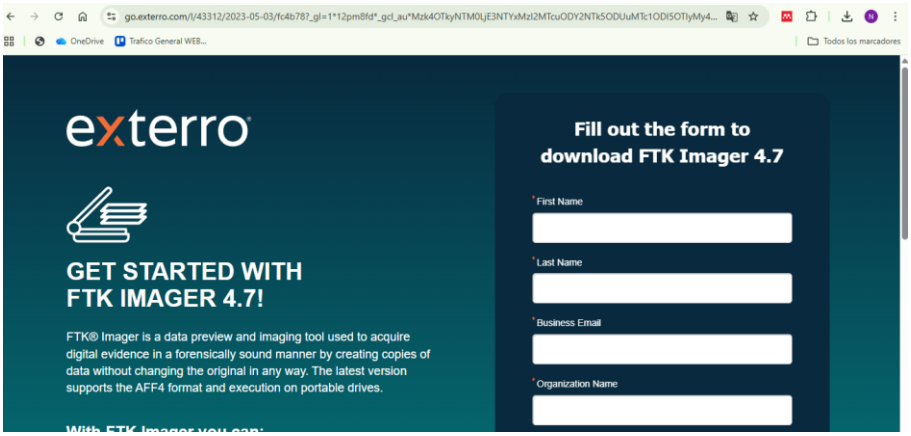


Ilustración 77 Acceso a la página de descarga oficial

Al hacer clic en dicho botón, el navegador redirigió a esta nueva pestaña donde se desplegó el formulario de registro para la obtención de la versión FTK Imager 4.7. En esta vista se solicitó el ingreso de información básica para poder generar una cuenta de acceso al instalador.

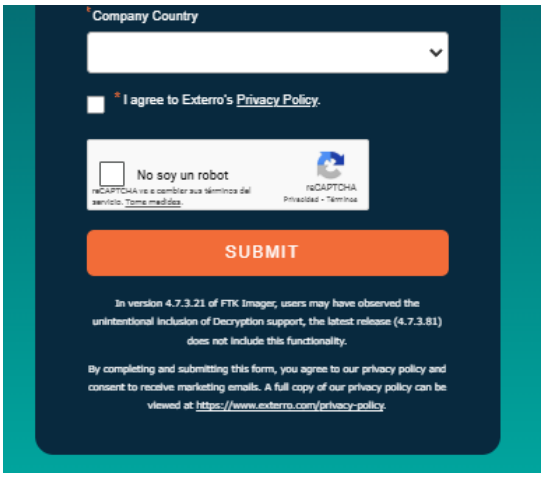


Ilustración 78 Botón de descarga

Una vez completados los campos requeridos, se presionó el botón de SUBMIT iniciando la descarga.

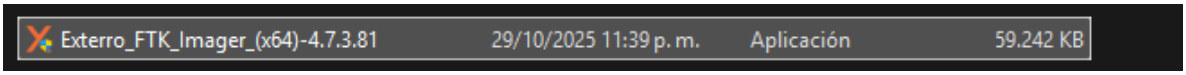


Ilustración 79 Verificación del archivo descargado

Este archivo corresponde al instalador oficial del programa, el cual contiene todos los componentes necesarios para ejecutar la herramienta forense.

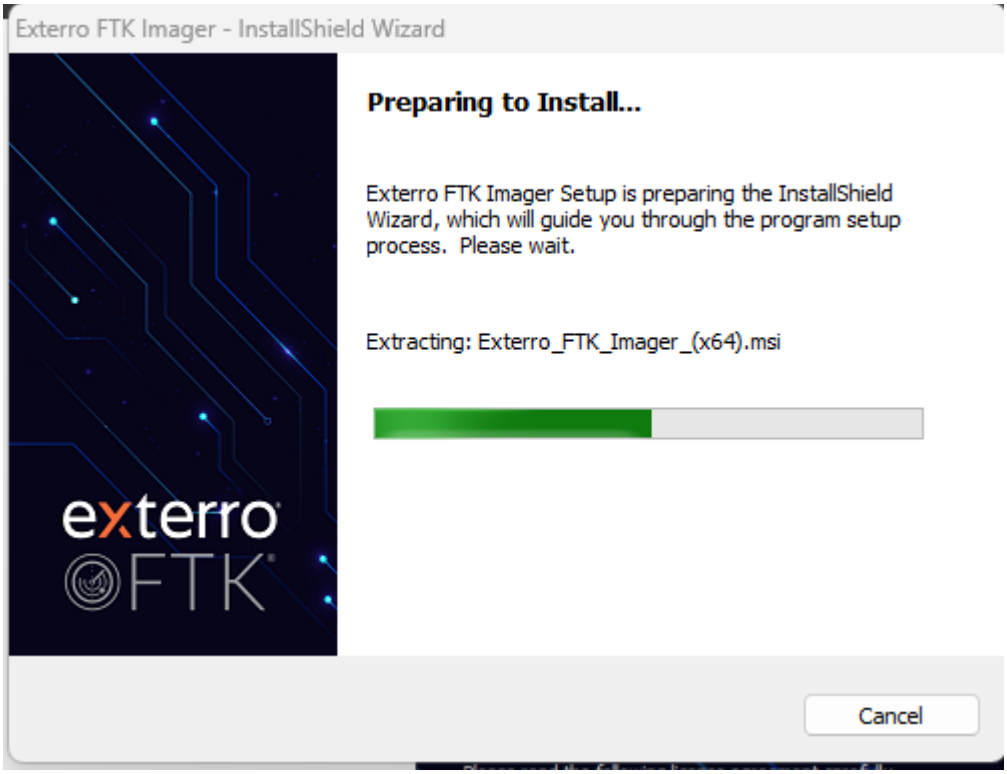


Ilustración 80 Ejecución del instalador de FTK Imager

En este paso, una vez verificado el archivo descargado, se procedió a ejecutar el instalador y se cargó esta ventana para iniciar la instalación.Durante este proceso, se visualizó una barra de progreso que avanzó hasta completar la extracción de los datos, y al terminar, el asistente continuo con la instalación guiada del software cargando la siguiente ventana:

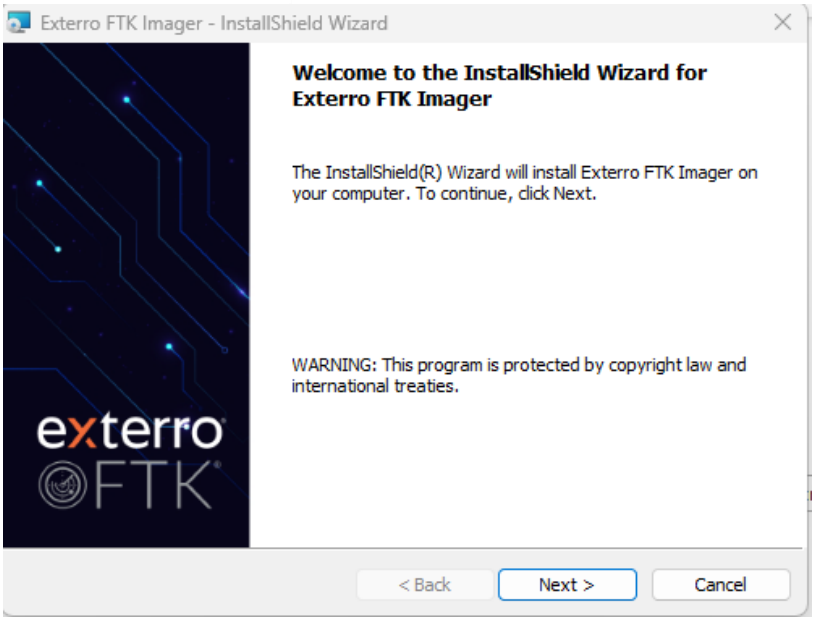


Ilustración 81 Inicio del asistente de instalación

Para continuar con el proceso de instalación, se presionó el botón Next, e

Ilustración 82 Aceptación del acuerdo de licencia

Como paso siguiente, el asistente de instalación mostró la ventana del acuerdo de licencia, para continuar fue necesario seleccionar la opción “I accept the terms in the license agreement”, aceptando así los términos y condiciones establecidos por el fabricante.

Una vez marcada esta opción, se habilitó el botón Next para avanzar al siguiente paso.

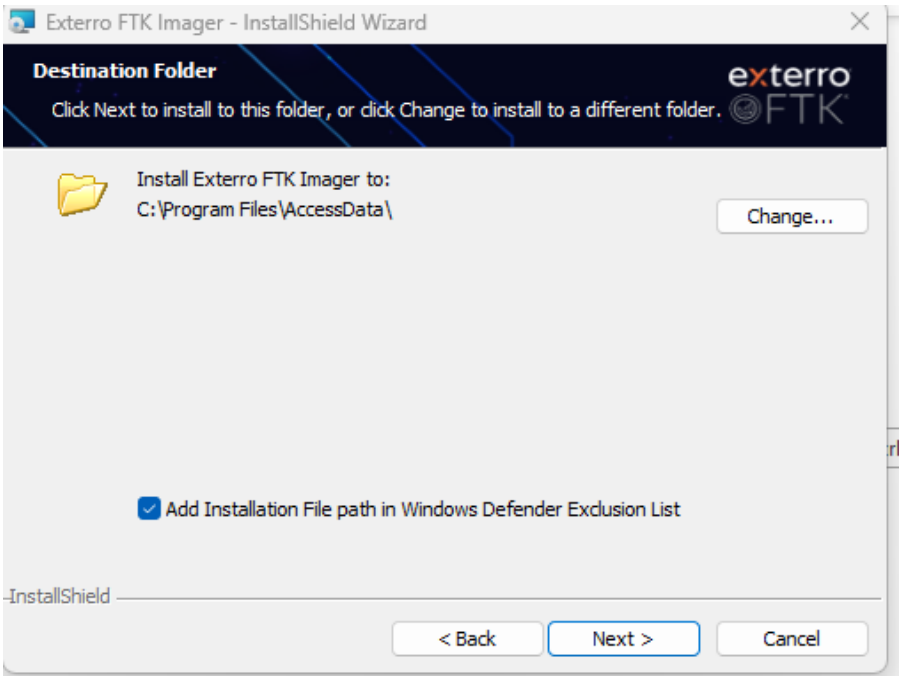


Ilustración 83 Selección de la carpeta de instalación

A continuación, el asistente mostró la ventana Destination Folder, donde se especifica la ruta en la cual se instalará el programa Exterro FTK Imager, se dejó la establecida por defecto y se continuó presionado el botón Next.

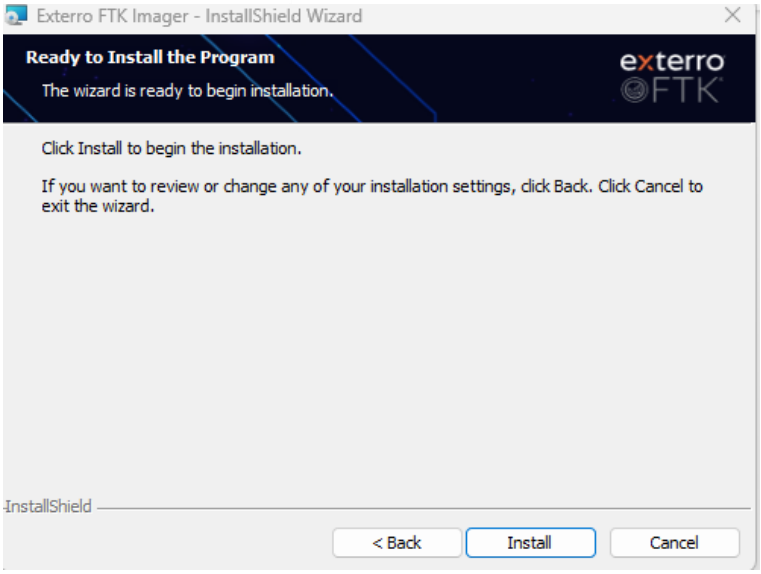


Ilustración 84 Confirmación para iniciar la instalación

En esta ventana del asistente, se confirmó que todos los parámetros de instalación estaban correctamente configurados y el sistema estaba listo para comenzar el proceso. Por eso, se seleccionó el botón Install para comenzar la instalación.

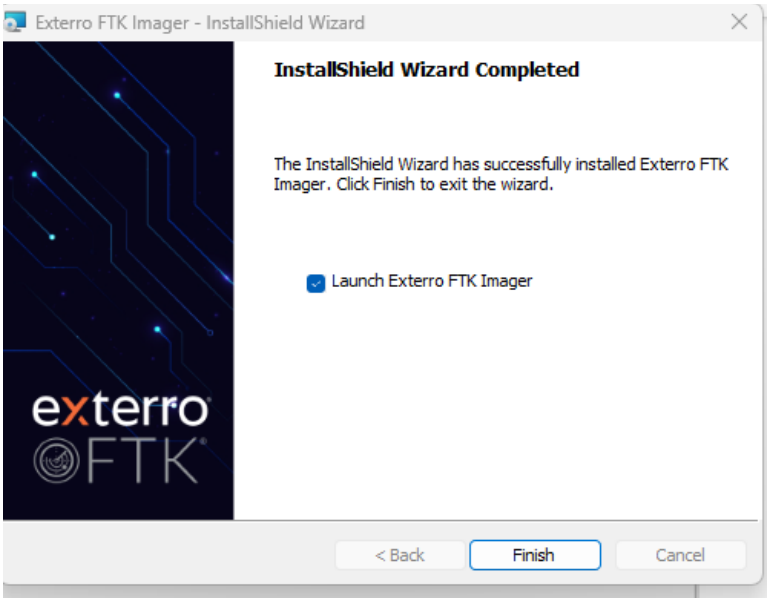


Ilustración 85 Finalización de la instalación

Una vez completado el proceso de instalación, el asistente mostró esta ventana indicando que el programa Exterro FTK Imager se había instalado correctamente en el sistema se presionó el botón, **Finish** para cerrar el asistente de instalación.

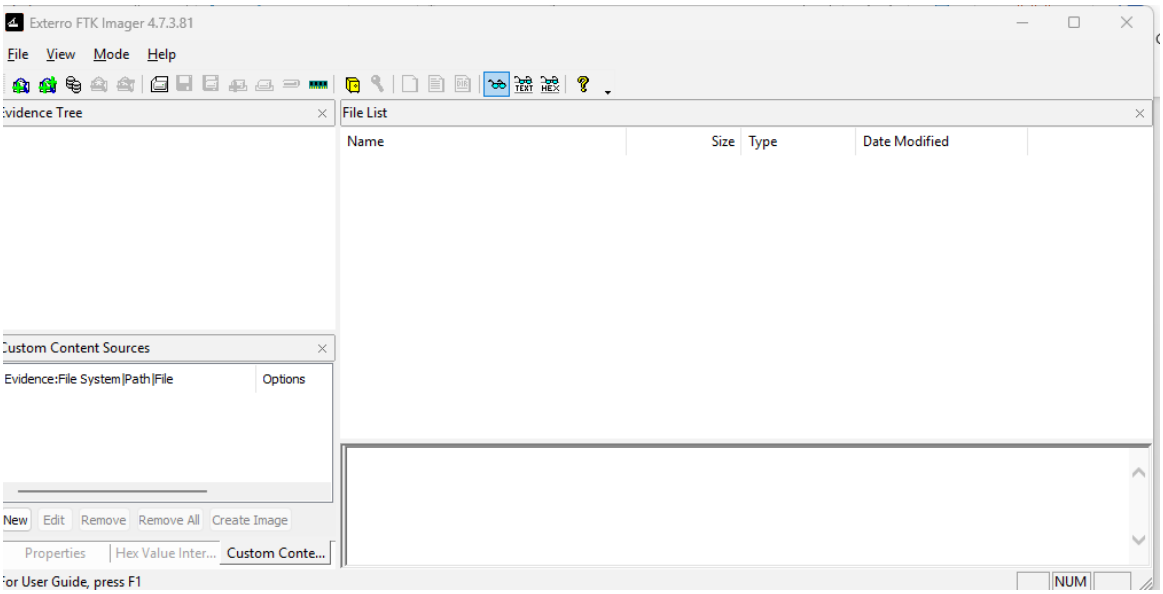


Ilustración 86 Apertura de Exterro FTK Imager

Al finalizar la instalación y presionar el botón Finish, se ejecutó automáticamente el programa Exterro FTK Imager. En la ventana inicial del software se observa la interfaz principal compuesta por diferentes secciones:

En la parte izquierda se encuentra el panel Evidence Tree, destinado a mostrar la estructura jerárquica de los dispositivos o archivos de evidencia cargados.

En la parte central superior se ubica la sección File List, donde se listarán los archivos contenidos en la evidencia seleccionada, junto con información como nombre, tamaño, tipo y fecha de modificación.

Y en la parte inferior izquierda aparece el panel Custom Content Sources, que permite agregar, eliminar o crear imágenes forenses a partir de distintas fuentes de datos.

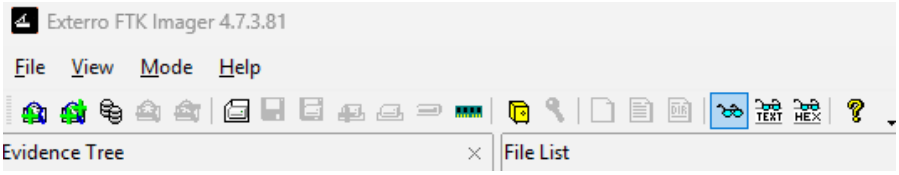


Ilustración 87 Iconos en la barra de herramientas de FTK Imager

En la parte superior de la ventana principal de Exterro FTK Imager se encuentra una barra de herramientas con una serie de íconos que facilitan el acceso rápido a las funciones más utilizadas del programa:

Agregar evidencia (Primer icono de derecha a izquierda): Permite añadir una nueva fuente de evidencia, ya sea un disco físico, una unidad lógica, una imagen de disco o una carpeta. Es el primer paso para iniciar un análisis o crear una copia forense, entre ellas.

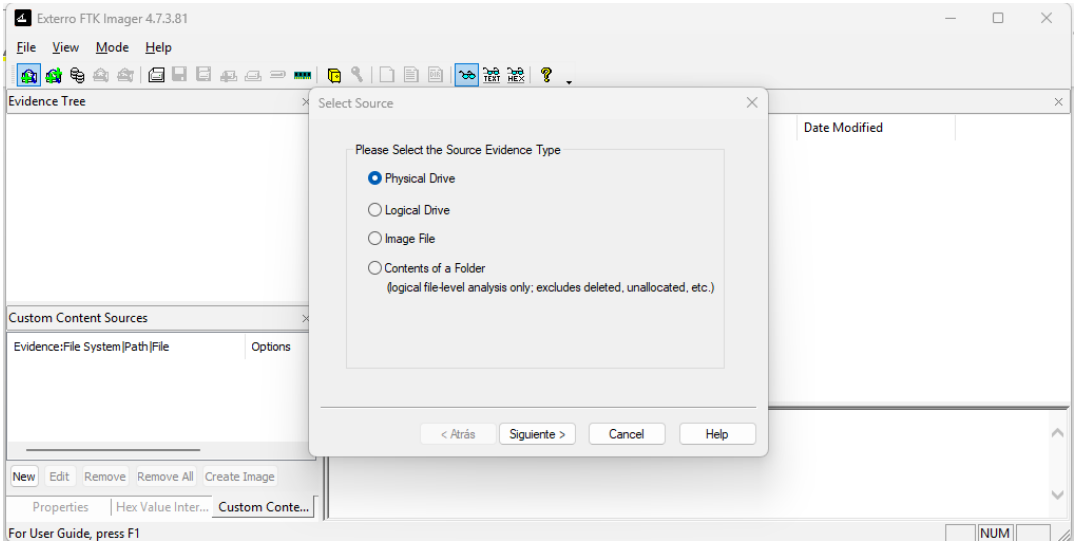
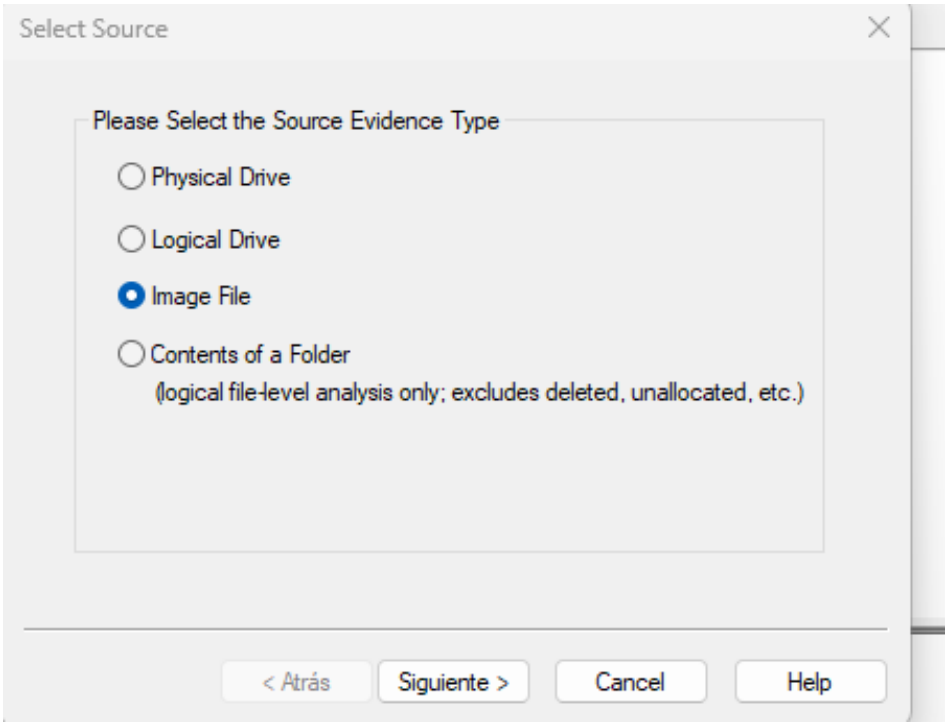


Ilustración 88 Tipo de evidencia

Se hizo clic en dicho botón de añadir evidencia, se abrió la ventana Select Source, en la que se presentan las diferentes opciones de tipo de evidencia que pueden seleccionarse.



- Physical Drive: Permite capturar una imagen completa de un disco físico, incluyendo todos sus sectores.
- Logical Drive: Crea una imagen solo de una partición o volumen lógico.
- Image File: Carga una imagen de disco previamente creada (.dd, .E01,etc).
- Contents of a Folder: Analiza el contenido lógico de una carpeta específica.

Para este análisis, se seleccionó la opción ImagenFile, Luego, se hizo clic en el botón Siguiente.

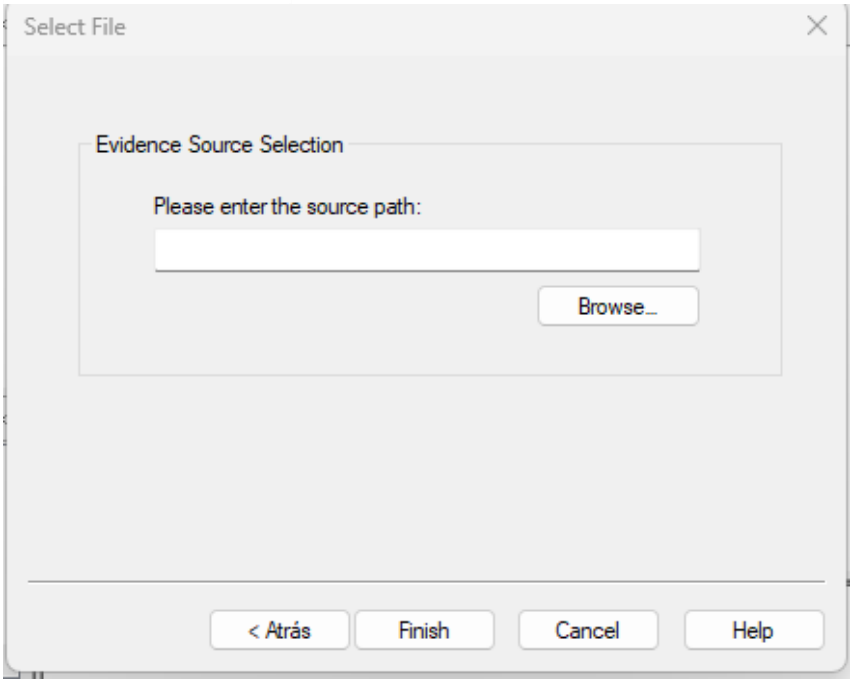


Ilustración 89 Selección de la ruta de la evidencia

Esta ventana permite especificar la ubicación del archivo o dispositivo que se desea examinar. Se muestra un campo Please enter the source path , donde se debe ingresar la ruta exacta del archivo de evidencia o, utilizar el botón Browse… para buscarlo manualmente dentro del sistema.

Para continuar con el proceso, se hizo clic en el botón “Browse…”, con el fin de ubicar la imagen forense previamente generada y almacenada en el sistema, la cual se analizará con FTK Imager.

Cabe recordar que dicha imagen fue generada en Kali Linux, posteriormente copiada a Windows y almacenada dentro de la carpeta Image en el disco C:

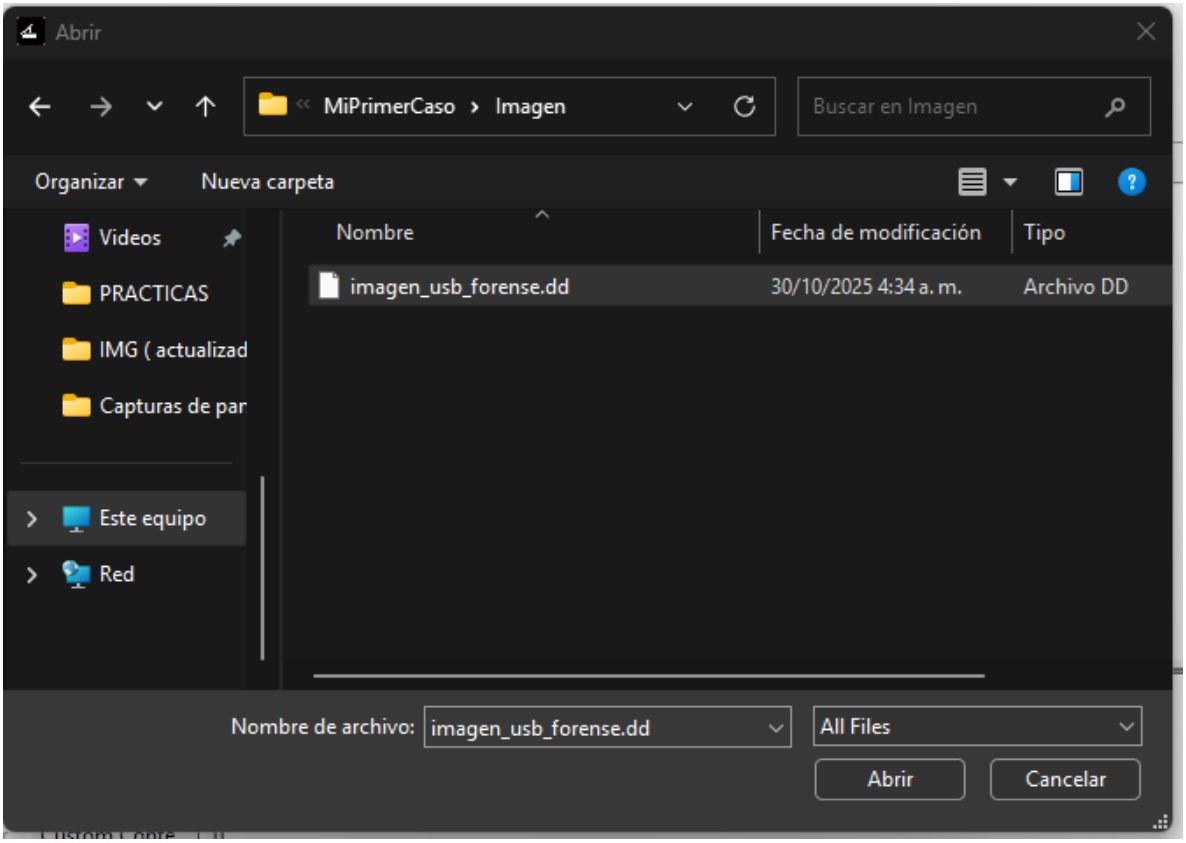


Ilustración 90 Explorador de archivos

Al presionar el botón Browse…, se abrió el explorador de archivos de Windows, permitiendo navegar por las carpetas del sistema para ubicar la imagen forense.

Se procedió a ingresar a la ruta C:\Análisis_Forense\MiPrimerCaso\Imagen, donde se encontraba almacenado el archivo imagen_usb_forense.dd, generado durante las etapas anteriores del laboratorio.

Una vez localizado el archivo, se seleccionó y se presionó el botón Abrir para cargarlo en FTK Imager, continuando así con el proceso de análisis de la evidencia digital.

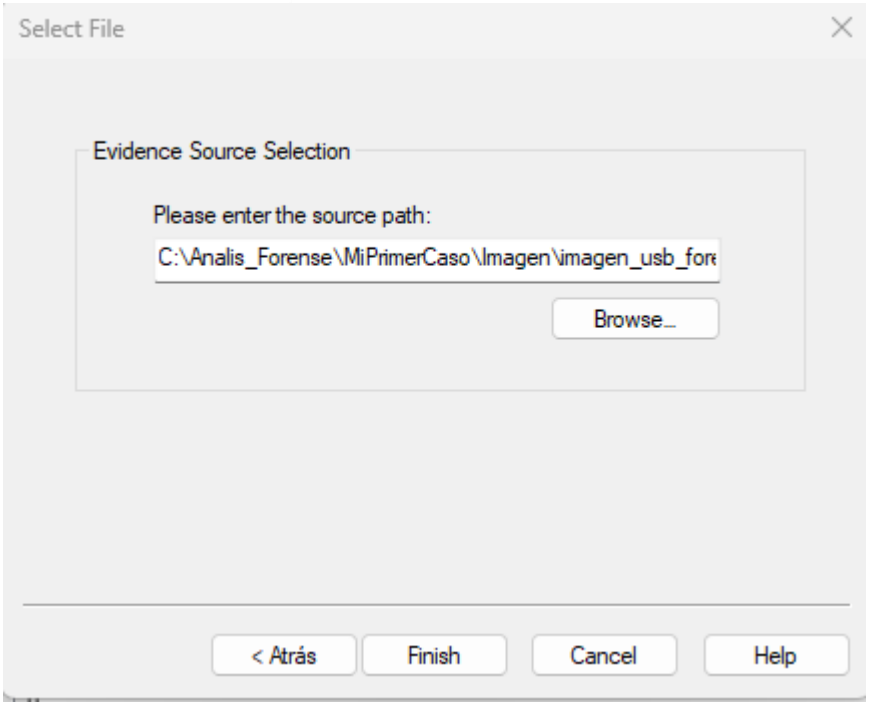


Ilustración 91 Confirmación de la ruta del archivo de evidencia

Luego de seleccionar el archivo imagen_usb_forense.dd desde el explorador, la ruta completa se cargó automáticamente en el campo Please enter the source path dentro de la ventana Evidence Source Selection.

Una vez verificada la ruta correcta, se procedió a confirmar la selección presionando el botón Finish, con lo cual el programa FTK Imager cargó la imagen para iniciar el análisis forense correspondiente.

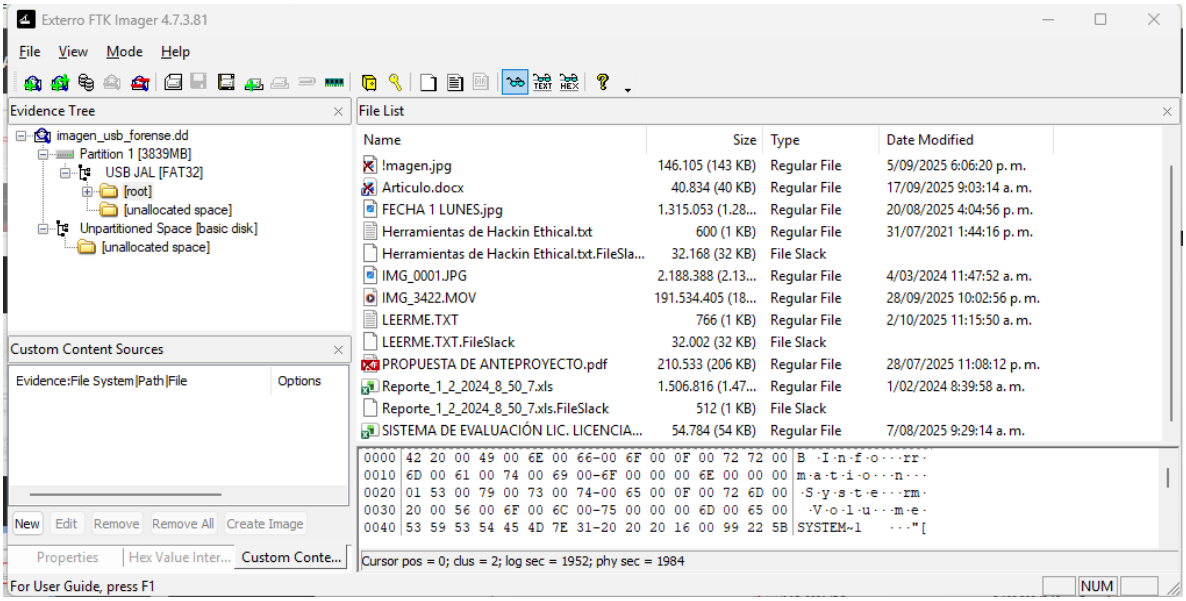
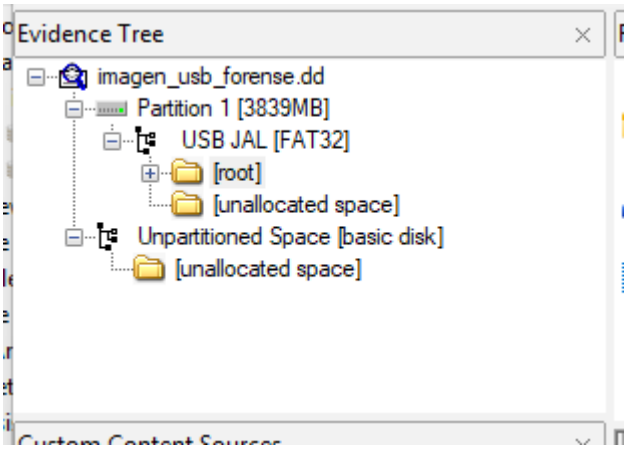


Ilustración 92 Visualización del contenido de la imagen forense

Una vez cargada la imagen **imagen_usb_forense.dd**, el programa desplegó su contenido en la interfaz principal.



En el panel izquierdo, dentro del árbol denominado **Evidence Tree**, se puede observar la estructura del dispositivo analizado, organizada en particiones y áreas no asignadas.

En este caso, se identifica una partición principal etiquetada como USB JBAL [FAT32], la cual contiene los archivos recuperados, así como un espacio no particionado (Unpartitioned Space) que puede contener información residual o datos eliminados.

En el panel derecho (File List), se listan los archivos encontrados en la partición, junto con sus detalles como nombre, tamaño, tipo y fecha de modificación. Entre los elementos se destacan documentos de texto, imágenes, archivos PDF y hojas de cálculo que fueron parte del contenido original del dispositivo.

En la parte inferior se muestra la vista en HEX y TEXT, permitiendo examinar los datos a nivel binario o legible según el tipo de archivo seleccionado.

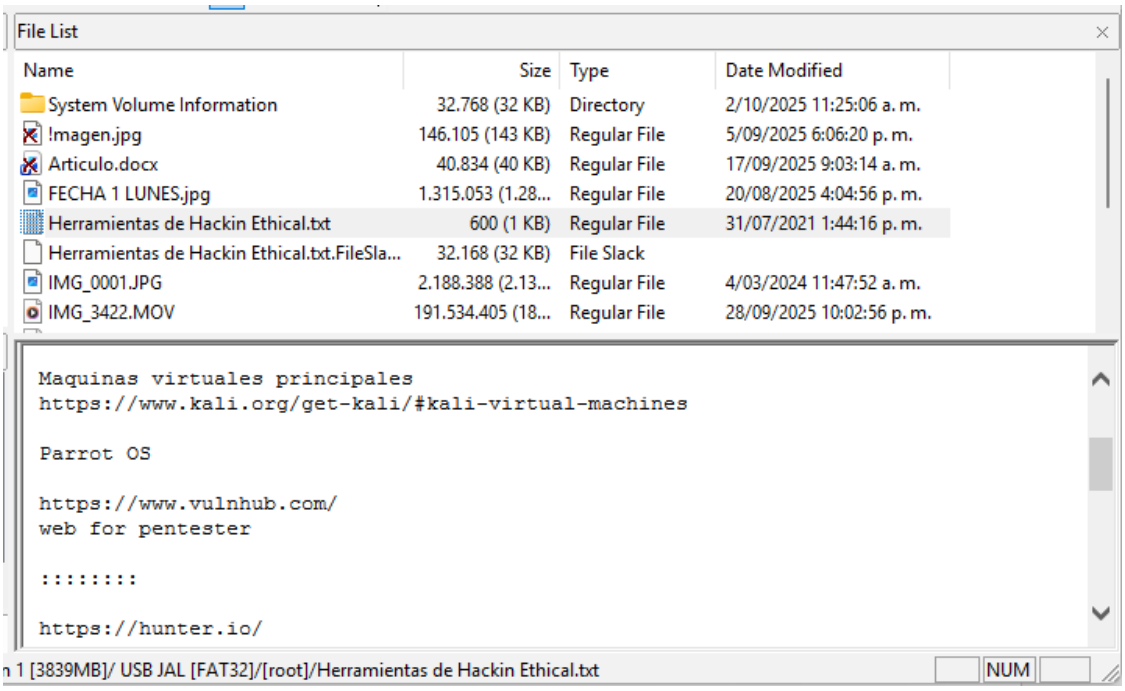


Ilustración 93 Visualización del contenido de los archivos

Al seleccionar un archivo dentro de la lista de resultados, FTK Imager permite visualizar su contenido directamente desde la interfaz, sin necesidad de extraerlo o modificarlo.

4 CONCLUSIÓN

El desarrollo de este laboratorio se llevó a cabo con éxito, cumpliendo satisfactoriamente los tres capítulos planteados. A lo largo del proceso se comprendió de manera práctica cómo realizar un análisis forense digital, desde la adquisición de la evidencia hasta su análisis e interpretación.

Se comprendió la importancia de que, como investigador forense, se preste atención a cada detalle del procedimiento, manteniendo siempre la integridad de la evidencia. Para ello, resulta fundamental calcular y comparar los valores hash antes y después de generar la imagen forense, para verificar que no haya sido alterada durante el proceso. También se reforzó la comprensión sobre la verificación minuciosa de los datos, la adecuada documentación de cada paso y la relevancia que estos elementos tienen para garantizar resultados confiables de un análisis forense y por último, este tipo de laboratorios contribuyen al fortalecimiento de los conocimientos necesarios para diseñar y mantener sistemas informáticos más seguros.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

5 BIBLIOGRAFÍA

Morales, R. S. (25). INFORME DE LABORATORIO ANÁLISIS FORENSE. Quibdó, Colombia: Universidad Tecnológica del Chocó Diego Luis Córdoba. Recuperado el 20 de 10 de 2025