INFORME PERICIAL FORENSE DIGITAL - ANÁLISIS DE IMAGEN DE USB

Informe Pericial Forense Digital - Análisis De Imagen De USB

Universidad Tecnológica del Chocó “Diego Luis Córdoba”

Docente

ING Rafael Sandoval Morales

Asignatura

Seguridad y Auditoría en Redes

Estudiante

Yeiber A. Mena Robledo

Quibdó/Chocó

15/10/2025

INFORME PERICIAL FORENSE DIGITAL - ANÁLISIS DE IMAGEN DE USB

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INSTRODUCCION

En el marco de la asignatura Seguridad y Auditoría en Redes, orientada por el Ingeniero Rafael Sandoval Morales en la **Universidad Tecnológica del Chocó "Diego Luis Córdoba"**, se desarrolló un ejercicio práctico de análisis forense digital aplicado a un dispositivo de almacenamiento portátil.

Este tipo de análisis permite examinar, recuperar y evaluar la información contenida en una memoria USB con el fin de detectar posibles archivos ocultos, datos eliminados o rastros de uso que puedan ser relevantes desde el punto de vista de la seguridad informática.

La práctica se llevó a cabo con una memoria física entregada por el docente, permitiendo aplicar técnicas y herramientas propias del análisis forense en medios digitales, bajo un enfoque académico que busca fortalecer las competencias del estudiante en el manejo de evidencias digitales, utilizando las herramientas especializadas de código abierto **Autopsy** y **AccessData FTK Imager**.

2. OBEJETIVOS

Objetivo General:

Realizar un análisis forense a la imagen digital de la memoria USB con el fin de identificar y recuperar información relevante, aplicando herramientas informáticas que permitan examinar la estructura de datos y evidencias digitales presentes en el dispositivo.

Objetivos Específicos:

- Examinar el contenido de la memoria USB entregada por el docente.
- Identificar posibles archivos ocultos o eliminados.
- Analizar las propiedades técnicas del dispositivo y su sistema de archivos.
- Elaborar un informe detallado con base en las evidencias encontradas durante el análisis.

3. CAPITULO#1 DESARROLLO DEL LABORATORIO

3.1 Descripción del problema

En el marco de la asignatura **Seguridad y Auditoría en Redes**, dirigida por el docente **Ing. Rafael Sandoval Morales**, se realizó un análisis forense a una memoria USB de color azul entregada por el docente, con el propósito de examinar su contenido, identificar rastros de información almacenada y aplicar herramientas forenses que permitan recuperar o analizar datos relevantes.

El problema planteado radica en la necesidad de **verificar la integridad, procedencia y posible manipulación de los archivos** contenidos en la memoria, con el fin de determinar si ha sido utilizada previamente, si contiene evidencias digitales relevantes o si presenta signos de borrado o alteración de información. Este tipo de análisis resulta esencial en el contexto de la seguridad informática, ya que permite aplicar técnicas prácticas de investigación digital y manejo de evidencias.

3.2 Descripción de la memoria USB

El dispositivo analizado corresponde a una **memoria USB de color azul**, de tamaño compacto, comúnmente utilizada para el almacenamiento y transporte de información personal o académica.

El **tamaño físico de la memoria es de 121 MiB (126.877.696 bytes)**, lo que indica que se trata de una unidad de baja capacidad, posiblemente formateada previamente o con un sistema de archivos optimizado para pruebas de laboratorio.

Durante la inspección inicial, se constató que la memoria se encontraba funcional, aunque no contenía carpetas visibles a simple vista. Sin embargo, a través del análisis forense se buscó determinar la existencia de archivos ocultos, borrados o con posibles rastros de manipulación.

3.3 Identificación del dispositivo mediante el comando fdisk -l

En la primera etapa del análisis forense se utilizó el comando **fdisk -l** desde el entorno Linux para listar los dispositivos de almacenamiento conectados al sistema. En la captura se observa la detección de dos unidades: el disco duro principal del sistema (/dev/sda) y la **memoria USB analizada**, identificada como **/dev/sdb**.

La salida del comando muestra que la memoria tiene un tamaño físico de **121 MiB (126.877.696 bytes)**, con un único sector activo de tipo **W95 FAT32**, correspondiente a la partición **/dev/sdb1**. Esta información permitió confirmar que el sistema reconocía correctamente el dispositivo, estableciendo su estructura de particiones, el modelo de almacenamiento (“Storage Device”) y los parámetros técnicos asociados al formato FAT32, datos fundamentales para el proceso forense posterior.

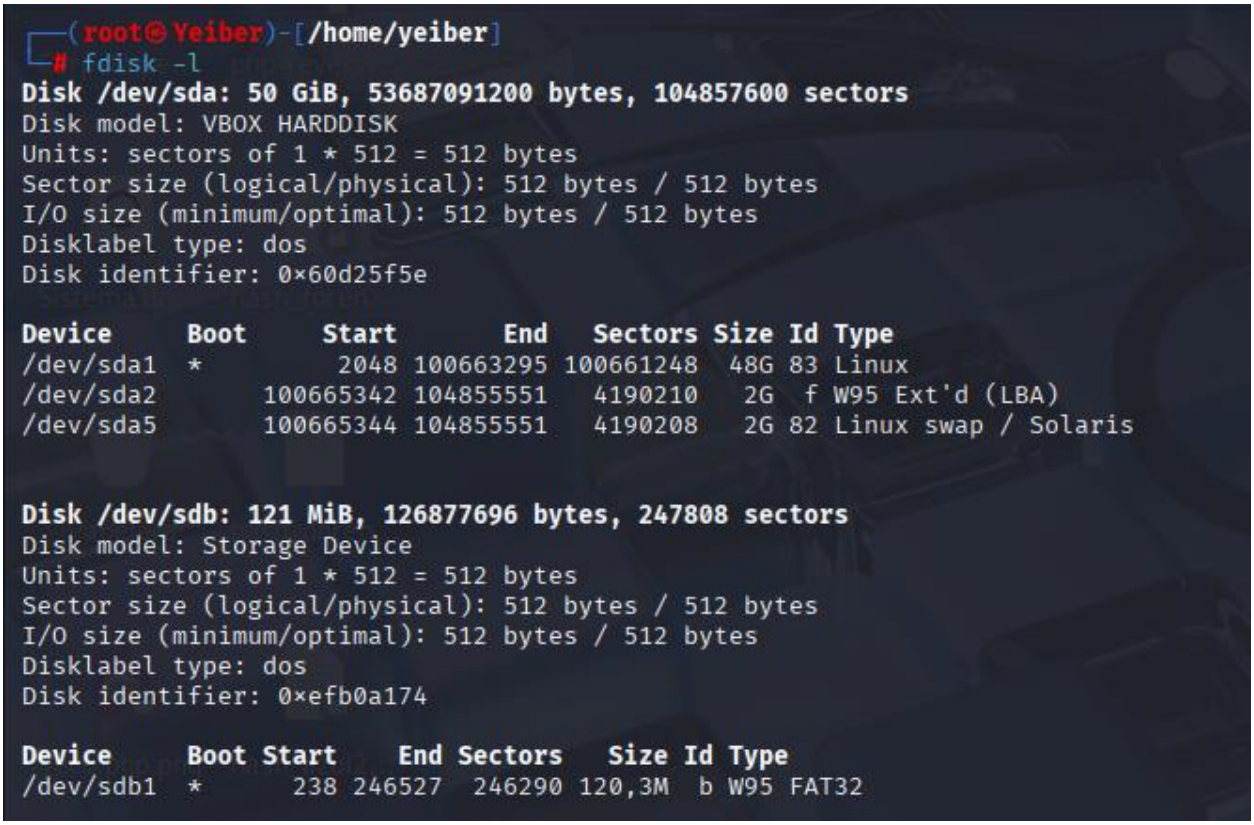

Ilustración 1-Identificación del dispositivo mediante el comando fdisk -l

3.4 Generación del hash SHA1 de la memoria USB

En esta etapa se aplicó el comando **sha1sum** sobre el dispositivo **/dev/sdb** con el fin de generar un valor **hash SHA1** que permita verificar la integridad de los datos contenidos en la memoria USB azul.

El resultado del comando fue redirigido al archivo **hash_azul2forense.sha1**, almacenado en el directorio *Escritorio*, como evidencia del proceso. Este procedimiento asegura que cualquier copia o análisis posterior pueda ser comparado con el hash original, garantizando que la información no sea modificada durante el peritaje digital.

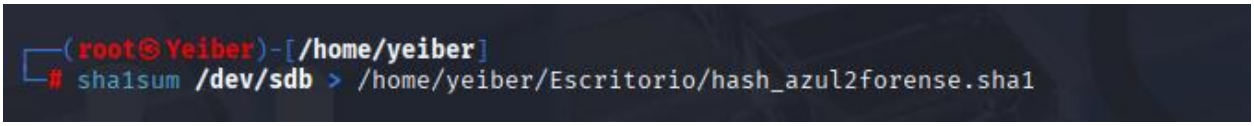

Ilustración 2-Generación del hash SHA1 de la memoria USB

3.5 Creación de imagen forense del dispositivo y verificación de integridad

En esta fase se procedió a crear una **imagen forense** de la memoria USB azul mediante el uso del comando **dd** en Linux.

El comando copió el contenido completo del dispositivo **/dev/sdb** hacia el archivo **imagen_usb_azul2_forense.dd**, ubicado en el directorio *Escritorio*.

El resultado indicó una copia total de **126.877.696 bytes (121 MiB)**, lo que confirma que la totalidad de la memoria fue clonada correctamente sin errores de lectura.

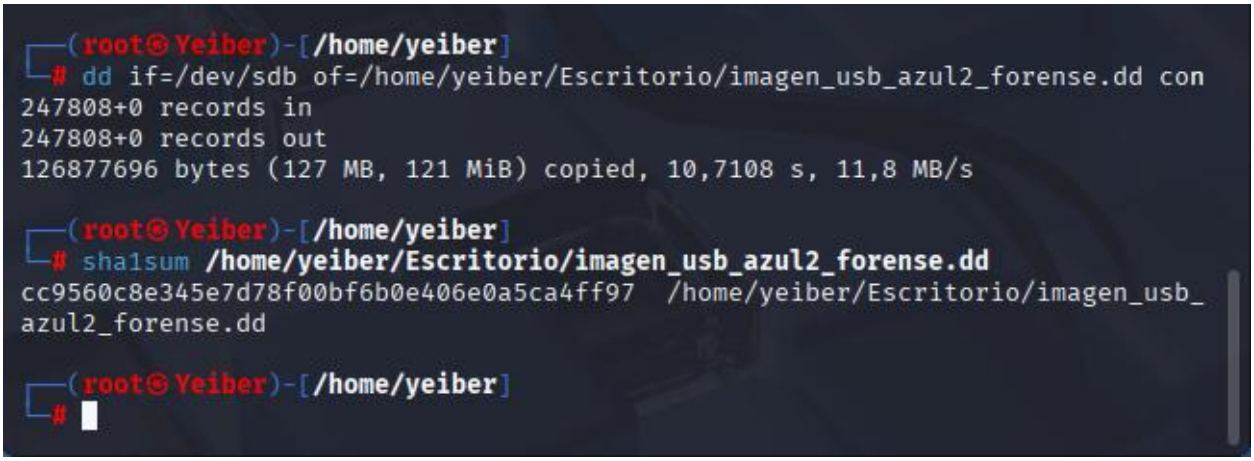

Ilustración 3-Creación de imagen forense del dispositivo y verificación de integridad

Se generó nuevamente un **hash SHA1** de la imagen obtenida, con el fin de comprobar que la copia es idéntica al dispositivo original. El valor hash mostrado coincidió con el generado previamente, lo que garantiza la **integridad y autenticidad de la evidencia digital**.

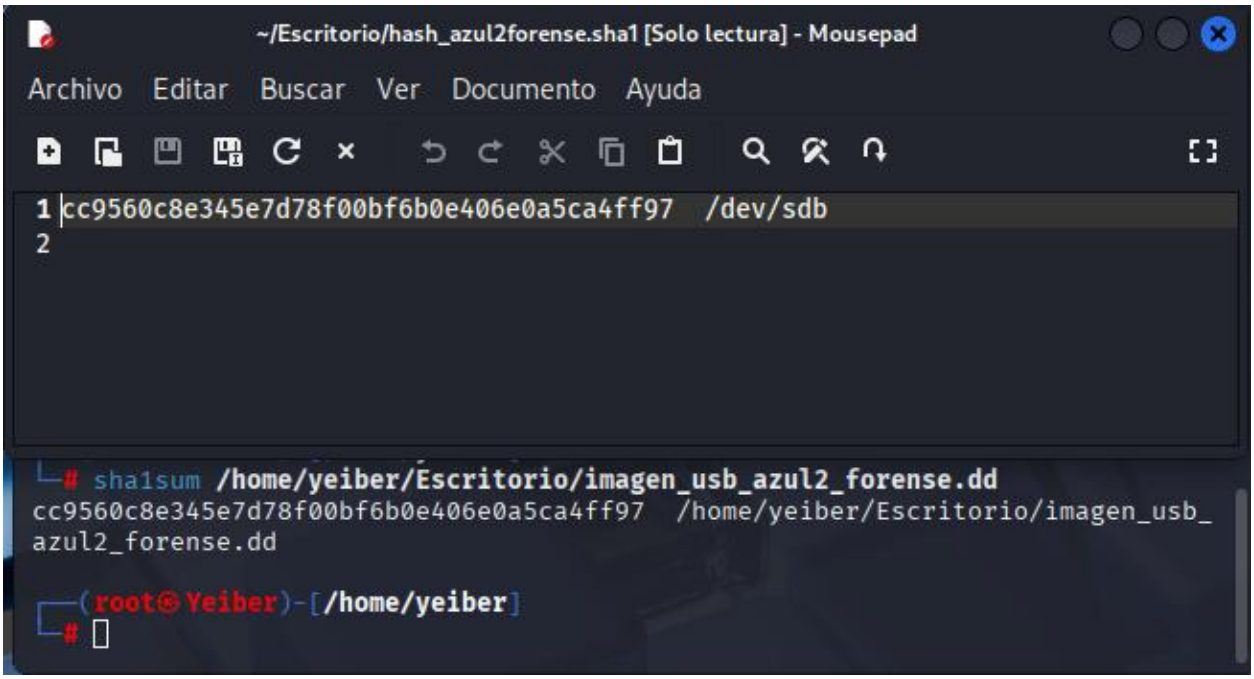

Ilustración 4-integridad y autenticidad de la evidencia digital

3.6 Establecimiento de permisos para la imagen forense

En esta etapa del procedimiento, se ejecutó el comando chmod 777 sobre el archivo de la imagen forense, **imagen_usb_azul2_forense.dd**.

La finalidad de esta acción fue **otorgar permisos completos** (lectura, escritura y ejecución) a todos los usuarios del sistema, lo cual es necesario para que las herramientas forenses posteriores, que a menudo se ejecutan bajo diferentes privilegios, puedan **acceder y procesar el archivo de imagen** sin restricciones. Este paso asegura que la etapa de análisis de datos se pueda llevar a cabo de forma eficiente y sin interrupciones por problemas de acceso al archivo.

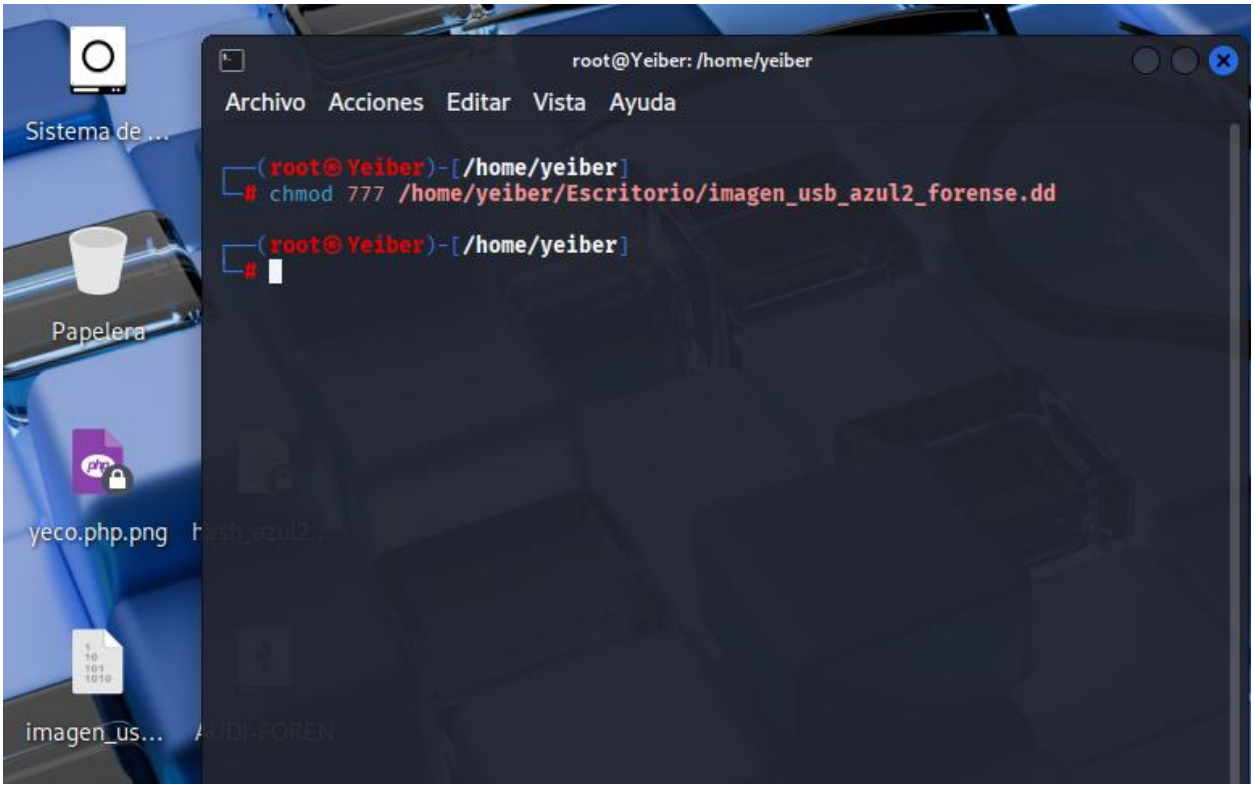

Ilustración 5-Establecimiento de permisos para la imagen forense

3.7 Inicialización de la herramienta Autopsy Forensic Browser

Una vez que la imagen forense fue creada y sus permisos ajustados, se procedió a inicializar la herramienta de análisis **Autopsy Forensic Browser**.

En este apartado se aprecia la ventana de inicio de sesión de la herramienta, en su versión **2.24**, accesible a través del navegador web local. Autopsy fue el entorno de trabajo elegido para **navegar, indexar y extraer datos** de la imagen forense previamente adquirida. Esta interfaz permite realizar búsquedas de palabras clave, analizar la línea de tiempo de los eventos y examinar los metadatos de los archivos, tanto visibles como eliminados.

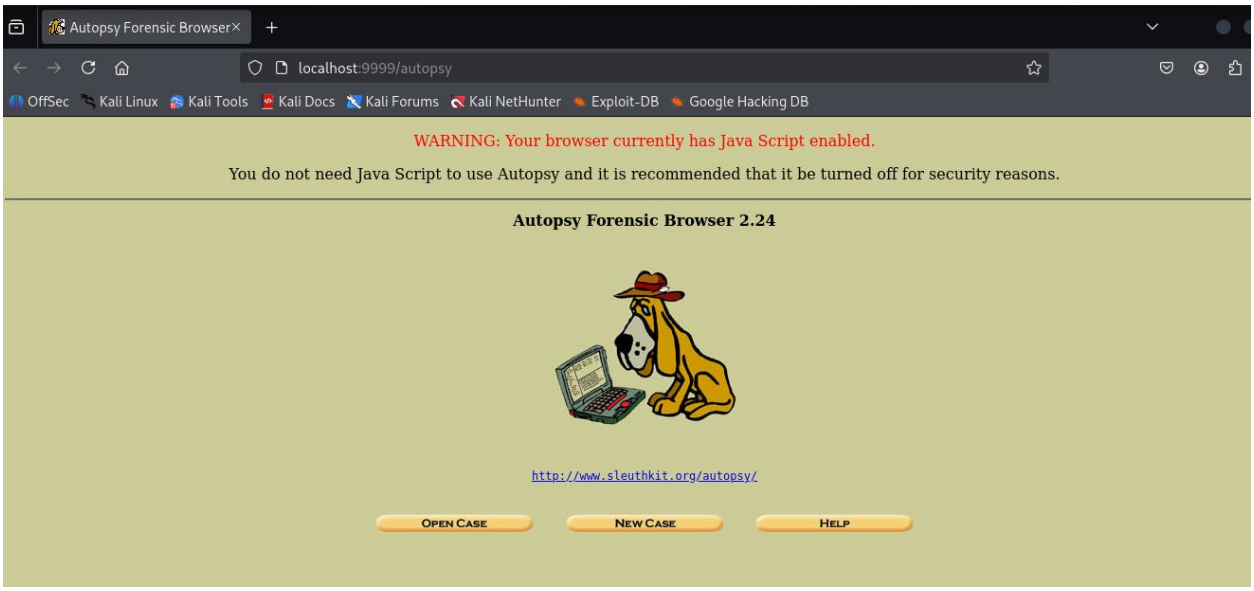

Ilustración 6-Inicialización de la herramienta Autopsy Forensic Browser

3.8 Creación de un nuevo caso en Autopsy

Posterior a la inicialización de la herramienta, se procedió a **crear el caso forense** dentro de Autopsy para organizar la evidencia digital.

La captura de pantalla muestra los datos introducidos para la investigación:

- **Nombre del Caso (*Case Name*):** Se asignó **MIprimercaso1** como identificador único de la investigación.
- **Descripción (*Description*):** Se especificó el propósito del análisis con el texto **Analsis Forence USB clase**.
- **Nombre del Investigador (*Investigator Name*):** Se registró el nombre del estudiante responsable, **Yeiber_A._Mena_Robledo**, para establecer formalmente la cadena de custodia y la autoría de las acciones realizadas.

El registro de estos datos es una **práctica estándar** que garantiza la trazabilidad y la **autenticidad** del análisis, permitiendo auditar quién, cómo y por qué se llevó a cabo el procedimiento forense sobre la imagen de la memoria USB.

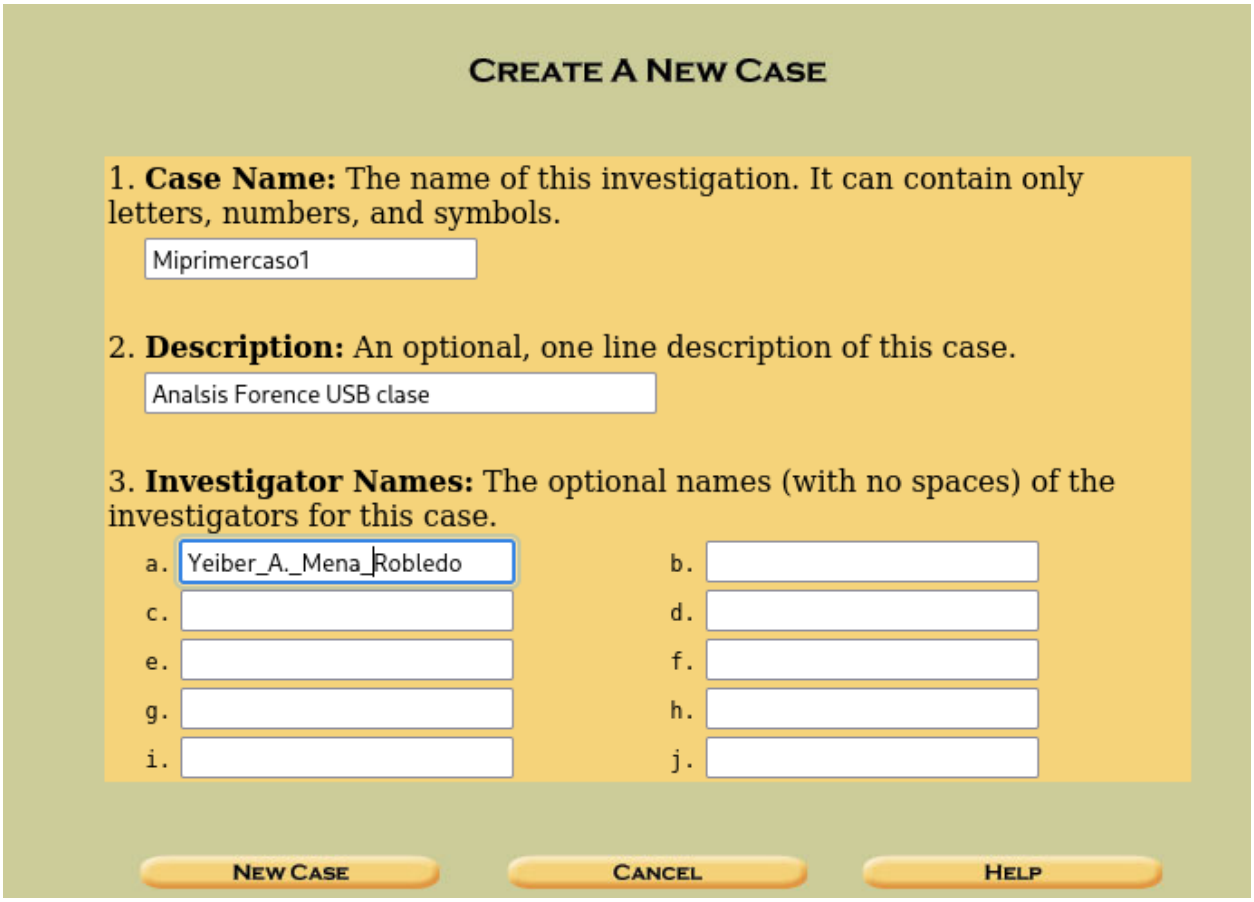

Ilustración 7-Creación de un nuevo caso en Autopsy

3.9 Confirmación de la creación del caso y preparación del Host

Después de ingresar los detalles del caso, la herramienta Autopsy mostró la **confirmación de la creación exitosa** del entorno de trabajo, denominado **MIprimercaso1**.

La pantalla indica que tanto el directorio de trabajo como el archivo de configuración (case.aut) fueron generados en la ruta del sistema, lo cual valida la estructura del caso. El siguiente paso

esencial, tal como lo indica la herramienta, es **crear un *Host***. Un *Host* representa la máquina o el entorno digital al que pertenece la evidencia (en este caso, la memoria USB analizada), siendo fundamental para la organización y contextualización de la prueba dentro del análisis forense.

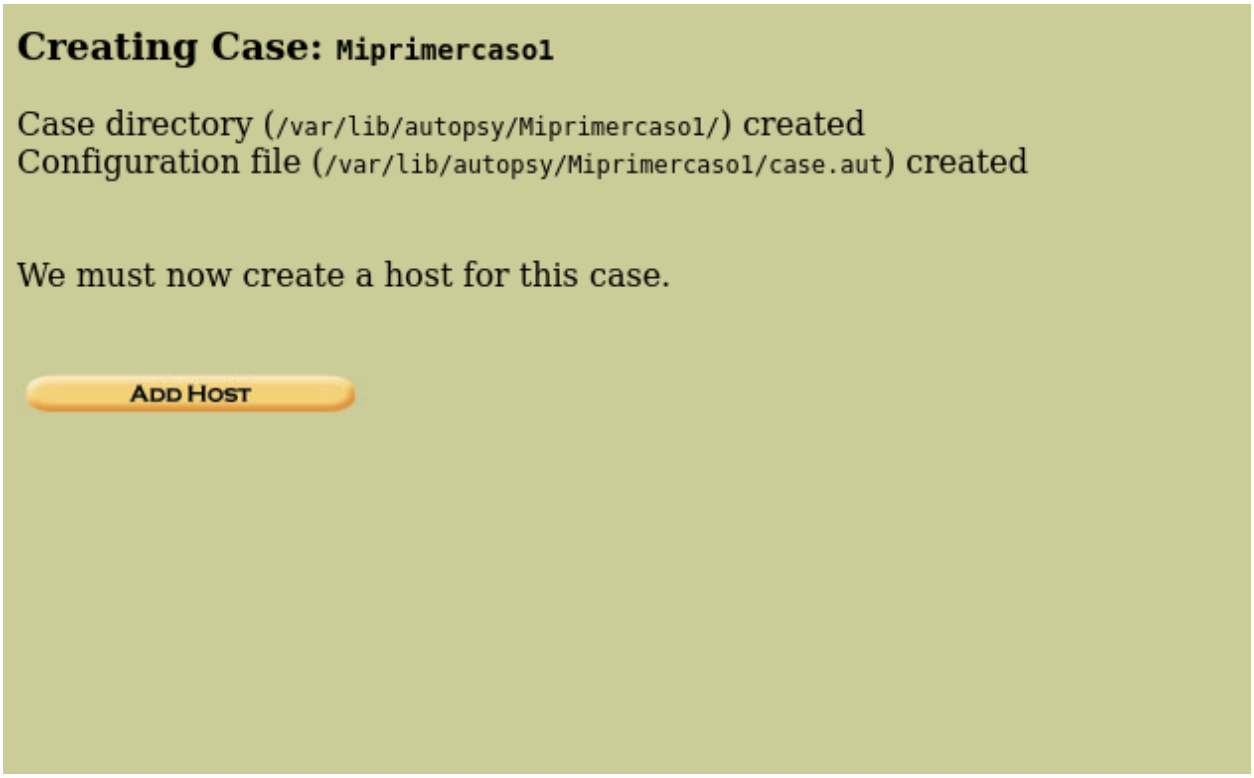

Ilustración 8-Confirmación de la creación del caso y preparación del Host

3.10 Adición y configuración de un nuevo Host

Como paso consecuente a la creación del caso, se procedió a registrar el *Host*, es decir, el contexto de la máquina donde se originó o analizó la evidencia.

La captura muestra la introducción de los siguientes parámetros:

- **Nombre del *Host* (*Host Name*):** Se ingresó **MWKaliPIT1** para identificar el equipo utilizado en el laboratorio, en este caso, una máquina con Kali Linux.

- **Descripción (*Description*):** Se añadió la nota **Equipo_Dell_Portatil** para describir la naturaleza del hardware asociado al análisis.
- **Ajuste de Desviación de Tiempo (*Timeskew Adjustment*):** Se dejó el valor en **0**, indicando que no fue necesario aplicar ninguna corrección o ajuste a la hora del sistema operativo, factor que es crítico para el análisis cronológico de los archivos.

Esta configuración es vital en informática forense, ya que **contextualiza temporal y físicamente** la evidencia, lo que resulta fundamental para la validez de los metadatos y la línea de tiempo de los eventos dentro de la investigación.

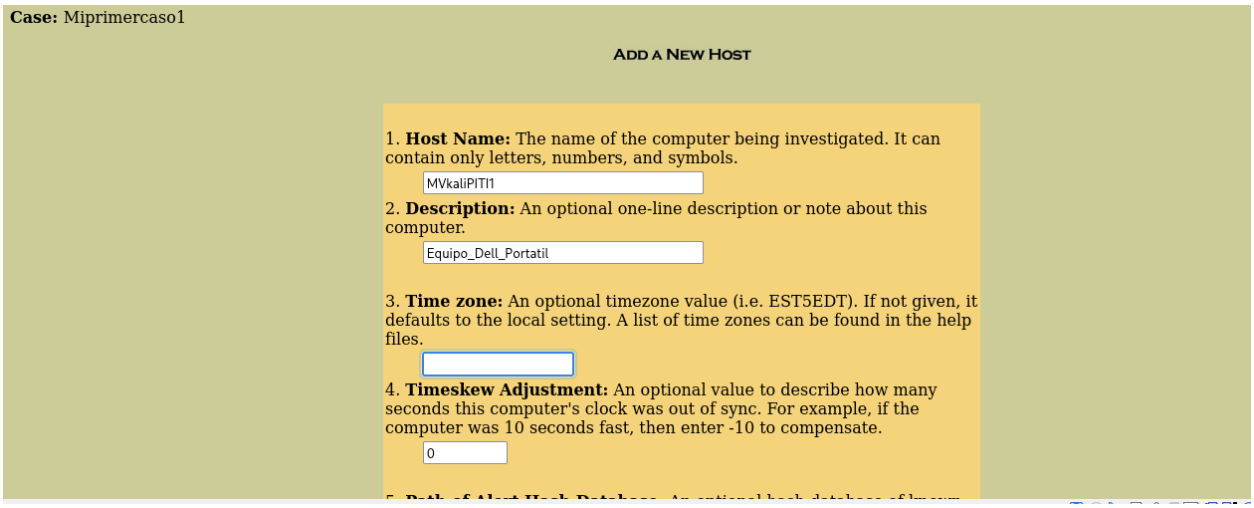

Ilustración 9-Adición y configuración de un nuevo Host

3.11 Confirmación de la adición del Host y solicitud de importación de la imagen

La herramienta Autopsy confirmó la correcta adición del *Host* **MWKaliPIT1** al caso **MIprimercaso1**.

Esta confirmación indica que la estructura organizativa del caso se ha completado, incluyendo la creación de un **directorio** y un **archivo de configuración** específicos para el *Host*. El mensaje

subsecuente indica el paso más crítico del proceso forense dentro de Autopsy: la necesidad de **importar el archivo de imagen** (.dd) de la memoria USB, el cual contiene la copia bit a bit de la evidencia digital.

Ilustración 10-Confirmación de la adición del Host y solicitud de importación de la imagen

3.12 Importación de la imagen forense al caso

En este punto crucial, se ingresaron los parámetros necesarios para que Autopsy pudiera procesar la evidencia digital. La imagen forense, que es la copia exacta de la memoria USB, fue finalmente importada al caso.

Se configuraron los siguientes campos:

- **Localización (*Location*):** Se especificó la ruta completa donde se guardó la imagen forense, en este caso: **/me/yeiber/Escritorio/imagen_usb_azul2_forense.dd**.
- **Tipo (*Type*):** Se seleccionó la opción **Disk**, lo que es correcto, ya que la imagen fue creada a partir de todo el dispositivo físico (/dev/sdb) y no de una partición específica.

- **Método de Importación (*Import Method*):** Se eligió la opción **Symlink** (enlace simbólico). Este método es preferido en la forense, ya que permite que la herramienta acceda y analice la imagen **sin moverla ni copiarla** a un nuevo lugar, minimizando el riesgo de corrupción de la evidencia.

La correcta importación de la imagen en modo *Symlink* asegura que el análisis se realice bajo los principios de **preservación y no alteración de la evidencia**.

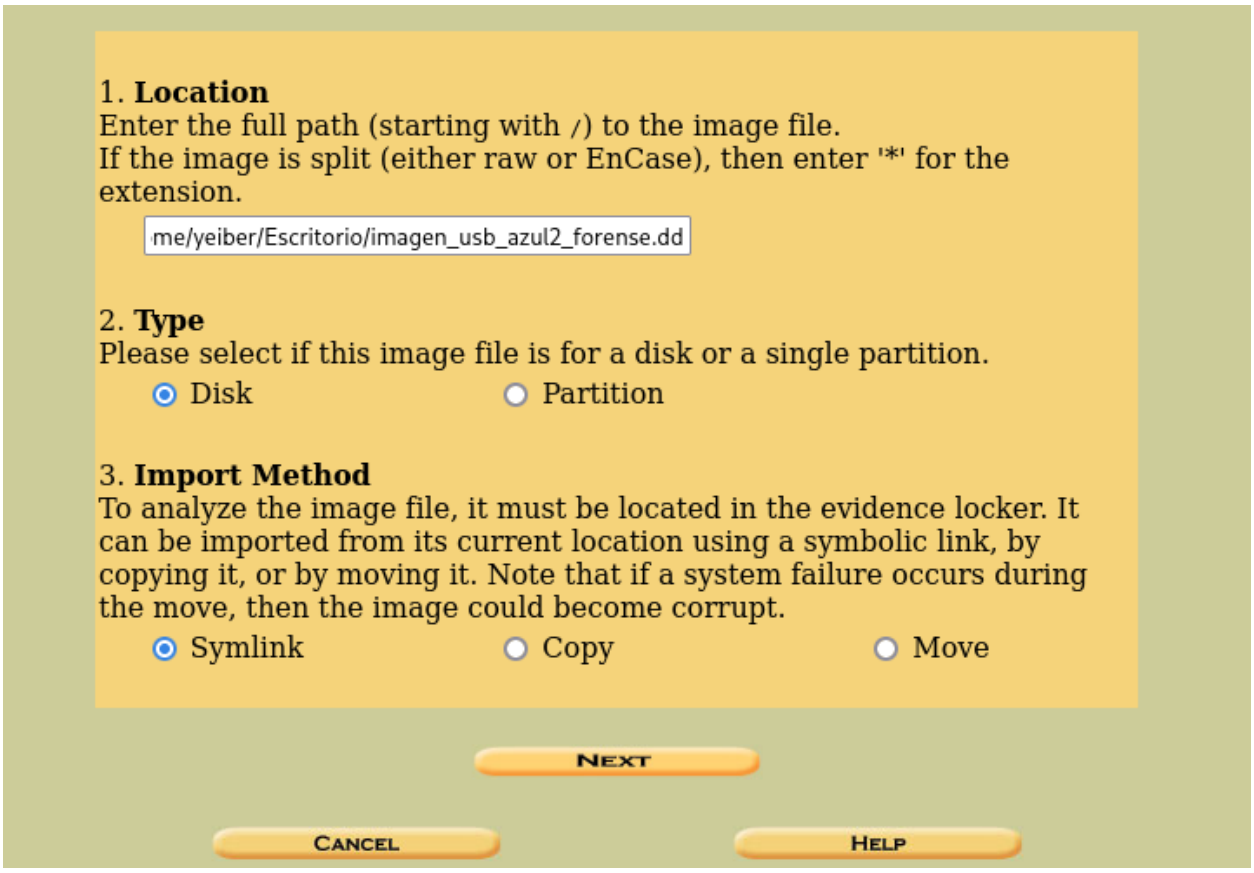

Ilustración 11-Importación de la imagen forense al caso

3.13 Detalles de la imagen forense y sistema de archivos

Esta captura muestra la pantalla de Autopsy donde se confirman los **detalles técnicos** de la imagen forense antes de su procesamiento final.

En la sección de **Integridad de Datos**, se seleccionó la opción **Ignore the hash value for this image**. Aunque en la práctica forense el *hash* es fundamental, en este contexto académico se optó por no ingresar el valor MD5, permitiendo que la herramienta continuara con el análisis de la estructura.

La sección **Detalles del Sistema de Archivos** confirmó automáticamente los datos de la memoria USB:

- **Partición 1:** Fue identificada como de tipo **Win95 FAT32 (0x0b)**, lo que corrobora la información obtenida previamente con el comando fdisk -l (Figura 1).
- **Rango de Sectores:** Se muestra el rango **238 to 246527**, lo que define el espacio exacto del disco que será analizado.
- **Tipo de Sistema de Archivos:** Aunque se detectó FAT32, la herramienta permite seleccionar la opción **fat16** en el *dropdown* para el punto de montaje, indicando flexibilidad en la interpretación de sistemas de archivos de baja capacidad.

La confirmación de estos detalles permitió al examinador avanzar a la etapa de **análisis profundo**, con pleno conocimiento de la estructura de datos que estaba siendo investigada.

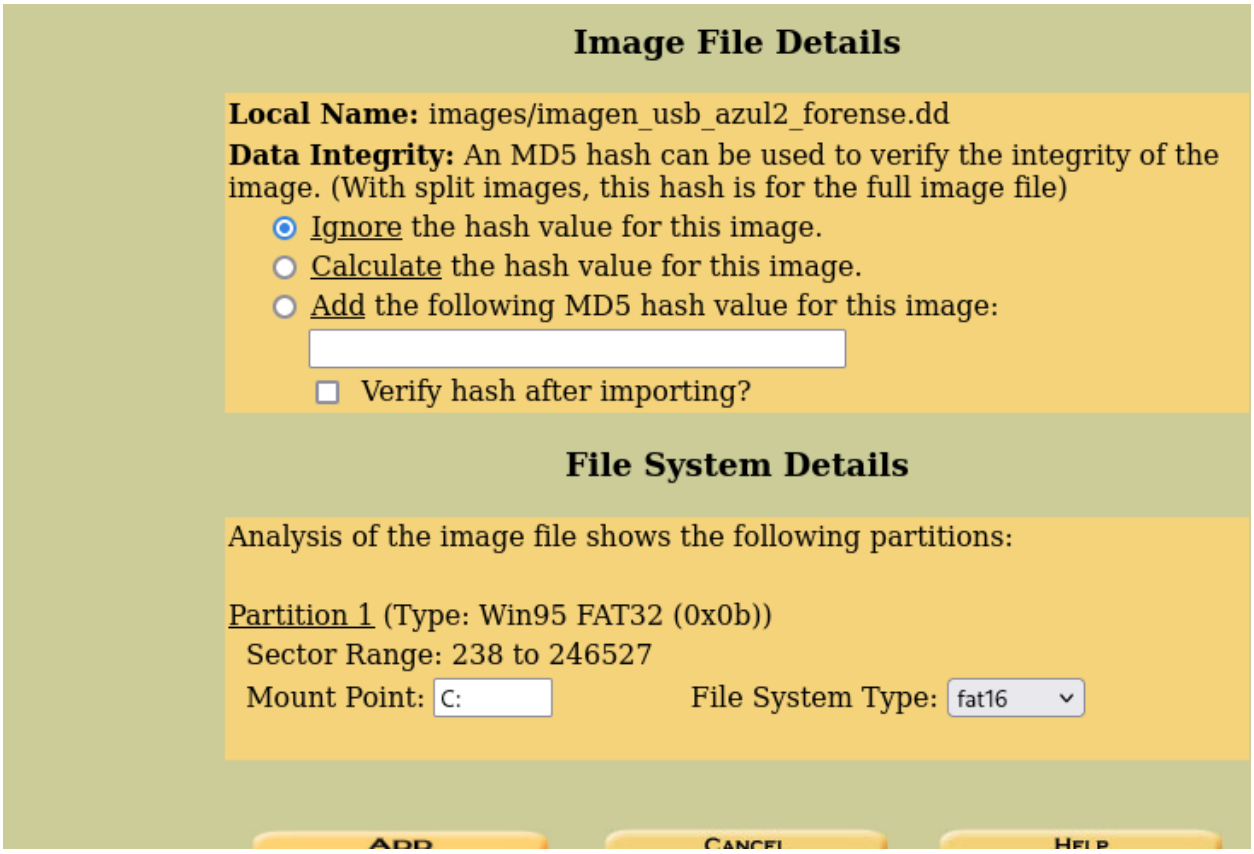

Ilustración 12-Detalles de la imagen forense y sistema de archivos

3.14 Confirmación de la adición de la imagen y las estructuras de volumen

Esta captura muestra la **finalización exitosa del proceso de importación** de la imagen forense al caso dentro de Autopsy.

La herramienta reporta que el archivo de imagen fue **enlazado al *evidence locker*** (repositorio de evidencias) y se le asignó el identificador **img1**. Adicionalmente, Autopsy procedió a **indexar las estructuras lógicas** de la imagen, identificando:

- **vol1** (tipo dos): Que representa la estructura general del disco.
- **vol2** (rango 238 to 246527 - fat16 - C:): Que corresponde al volumen principal de datos de la memoria USB (la partición FAT16 de 121 MiB).

La aparición de estos identificadores confirma que la imagen forense ha sido cargada correctamente y que la herramienta está lista para que el perito inicie el **análisis detallado** de los archivos y metadatos contenidos en el volumen vol2.

Ilustración 13-Confirmación de la adición de la imagen y las estructuras de volumen

3.15 Panel principal de Autopsy: Selección de volumen para el análisis

Esta captura muestra el **panel de control principal** de Autopsy para el caso MIprimercaso1, asociado al Host MWKaliPIT1.

El panel presenta los volúmenes detectados y cargados de la imagen forense, listos para ser analizados:

- **disk:** Representa la estructura física *raw* (en crudo) del disco, con el nombre imagen_usb_azul2_forense.dd-disk.
- **C:/:** Representa la partición lógica de interés, identificada como **fat16** y con el rango de sectores que contiene los datos de la memoria USB (imagen_usb_azul2_forense.dd-238-246527).

El examinador debe **seleccionar el volumen C:/** y hacer clic en **ANALYZE** para iniciar el análisis profundo sobre el sistema de archivos de la memoria, lo que permitirá buscar archivos

ocultos, eliminados y extraer metadatos. La interfaz también ofrece otras funcionalidades importantes como la **Línea de Tiempo de Archivos** (*File Activity Time Lines*) y la revisión de **Bases de Datos de *Hash***, esenciales para la investigación forense.

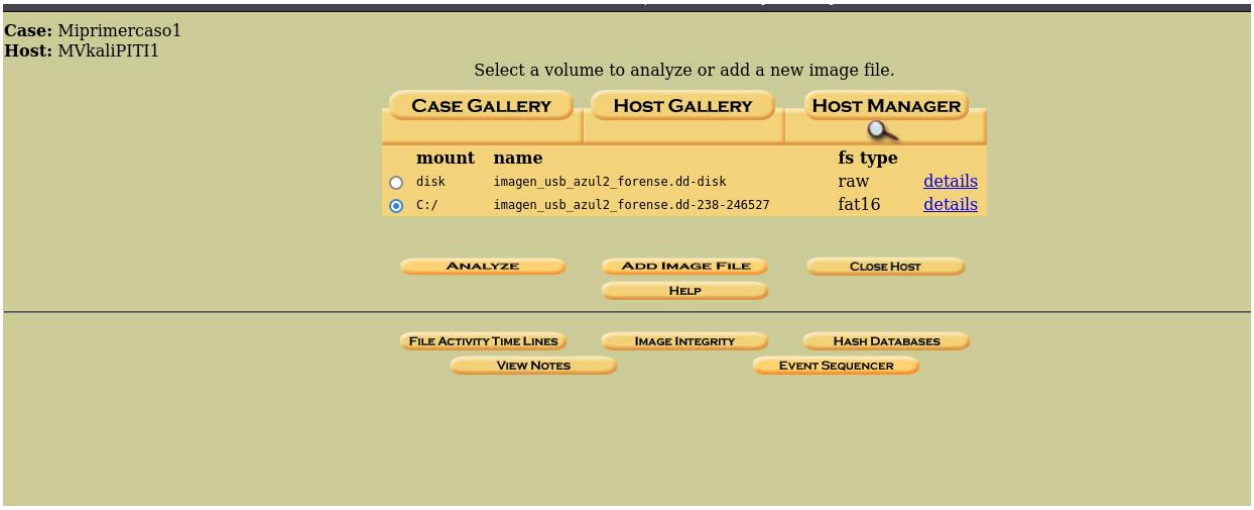

Ilustración 14-Panel principal de Autopsy: Selección de volumen para el análisis

3.16 Análisis del directorio raíz y detección de archivos eliminados

Al seleccionar el volumen C:/ para el análisis, la herramienta Autopsy muestra el **contenido del directorio raíz** del sistema de archivos FAT de la memoria USB.

La parte superior de la ventana muestra la barra de herramientas de análisis, incluyendo las opciones de **Análisis de Archivos**, **Búsqueda por Palabras Clave** y **Metadatos**. En la lista de archivos, la columna **Type** muestra la evidencia crítica: los archivos con un **símbolo de papelera roja (r/r)** indican que son archivos que fueron **previamente eliminados** de la memoria, pero cuyos datos aún son **recuperables** o visibles en el sistema de archivos.

Entre los rastros de información recuperada se encuentran:

- **AccessData FTK Imager 4.7.1.exe**: Una aplicación de *software* forense.

- **_Cifrados 2.docx**: Un documento de Word.
- **_Cyber3.tgg**: Un archivo con extensión no común.

Esta detección confirma el objetivo del análisis forense, que era encontrar rastros de información previamente usada en la memoria azul, a pesar de que no se mostraban en la inspección inicial.

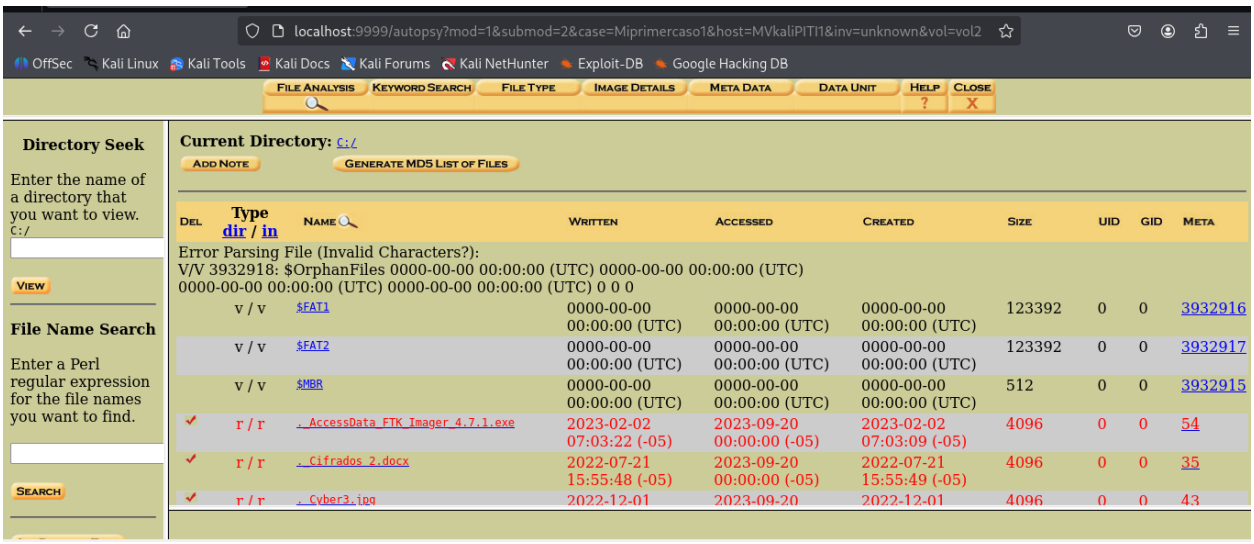

Ilustración 15-Análisis del directorio raíz y detección de archivos eliminados

3.17 Valores Hash (MD5) de los archivos recuperados

Una vez finalizado el proceso de escaneo del volumen C:/ dentro de Autopsy, se generó un listado de los **valores *hash* MD5** para los archivos identificados y recuperados en el sistema de archivos de la memoria USB.

Esta captura es la evidencia más importante de la fase de análisis, pues relaciona una **huella digital única** (el valor MD5) con el **nombre de cada archivo recuperado**. Entre el contenido identificado se encuentran:

- Archivos de imagen (IMG 0001.JPG, FECHA 1 LUNES.jpg).

- Archivos de texto (Herramientas de Hackin Ethical.txt, LEERME.TXT).
- Documentos académicos o de reporte (Reporte 1 2_2024 8 50 7.xls, SISTEMA DE EVALUACIÓN LICENCIATURA EN CIENCIAS NATURALES.xls).

La generación de estos *hashes* es fundamental para la **integridad de la evidencia**, ya que permite demostrar que el contenido de estos archivos **no ha sido alterado** desde el momento en que fueron recuperados de la imagen forense.

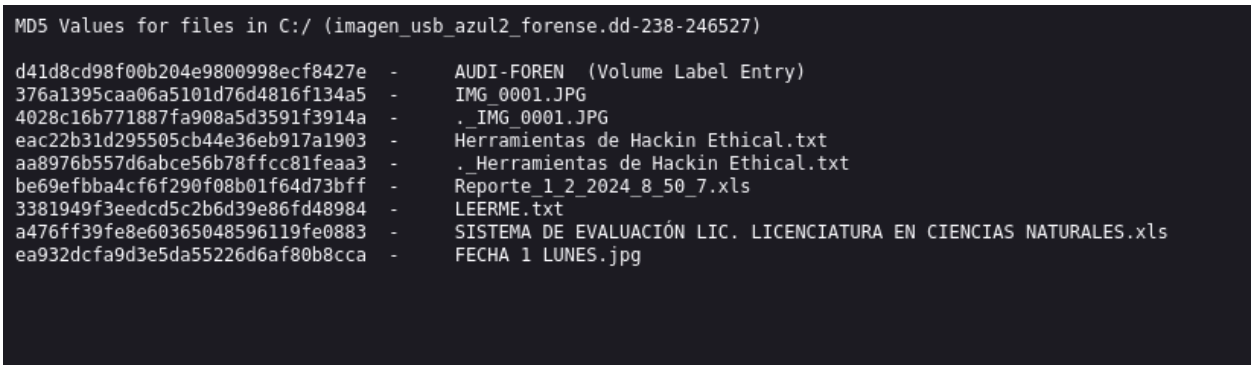

Ilustración 16-Valores Hash (MD5) de los archivos recuperados

3.18 Extracción de archivos recuperados desde Autopsy

Esta última captura evidencia la fase final del proceso de análisis: la **extracción** de uno de los archivos eliminados y recuperados.

Se observa la ventana de descarga del sistema operativo que indica la extracción del archivo **VOL2-C_...AccessData_FTK_Imager_4.7.1.exe**, cuyo nombre completo fue previamente identificado en el listado de elementos eliminados (Figura 15). El mensaje **"Completed - 2.0 KB"** confirma que la herramienta Autopsy facilitó la recuperación de este archivo para su **análisis fuera del entorno forense**, un paso crucial para inspeccionar su contenido o ejecutarlo de forma segura en un entorno controlado (sandbox).

La exitosa extracción de archivos eliminados valida la eficacia de las herramientas y técnicas forenses aplicadas, demostrando que la información no fue sobrescrita en la memoria USB.

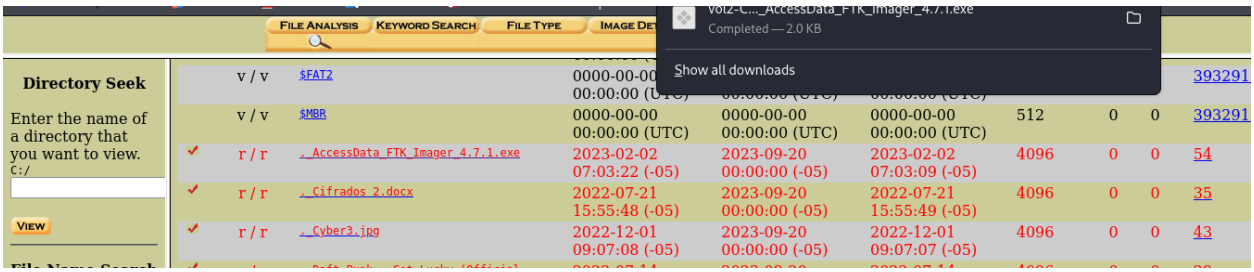

Ilustración 17-Extracción de archivos recuperados desde Autopsy

4. CAPITULO#2 DESARROLLO DEL LABORATORIO

4.1 Fase de Preparación y Herramientas

4.1.1 Instalación de la Herramienta Principal de Análisis (Autopsy)

La herramienta seleccionada para el análisis fue **Autopsy**, una plataforma de código abierto que facilita la investigación forense digital. Se procedió a su instalación en el sistema operativo Windows del laboratorio forense.

Inicio del Asistente: Se ejecutó el instalador previamente descargado. La Figura 18 muestra la pantalla de bienvenida del asistente de configuración, confirmando el inicio del proceso de instalación de Autopsy en el equipo.

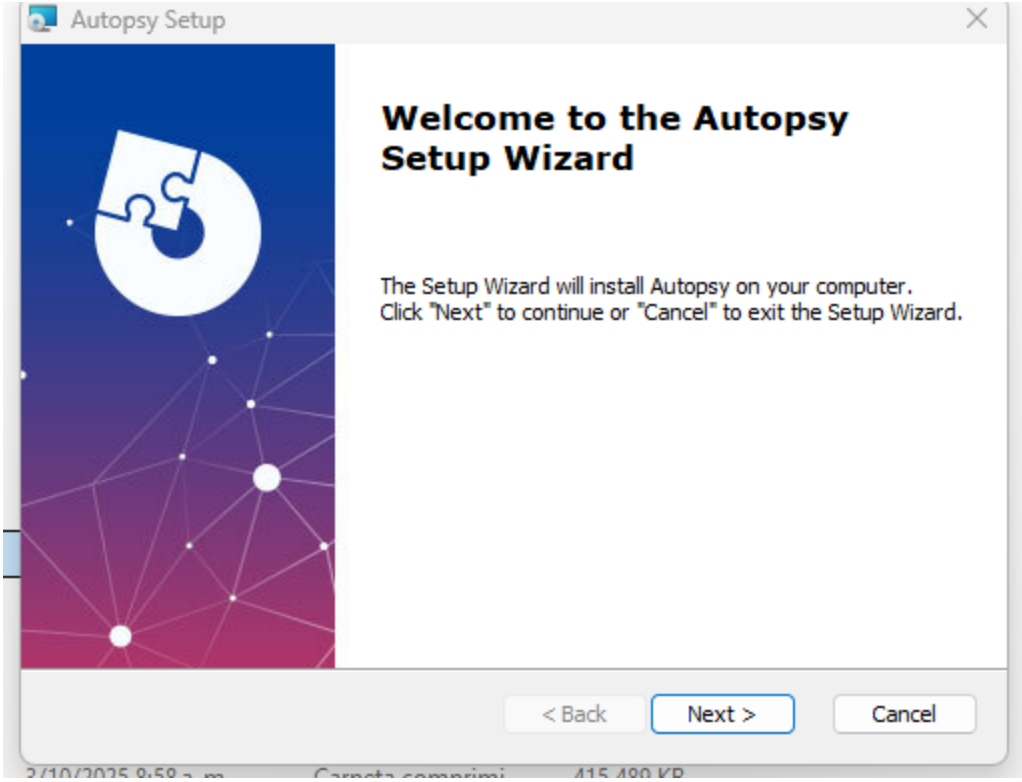

Ilustración 18-. Instalación de la Herramienta Principal de Análisis (Autopsy)

4.1.2 Selección del Directorio

Tras la pantalla de bienvenida, el asistente avanzó a la selección del directorio de instalación. El examinador confirmó la ruta por defecto, estableciendo la ubicación de la instalación en **C:\Program Files\Autopsy-4.22.1**. Una vez validado el destino, se seleccionó **"Next"** para continuar con el proceso de configuración.

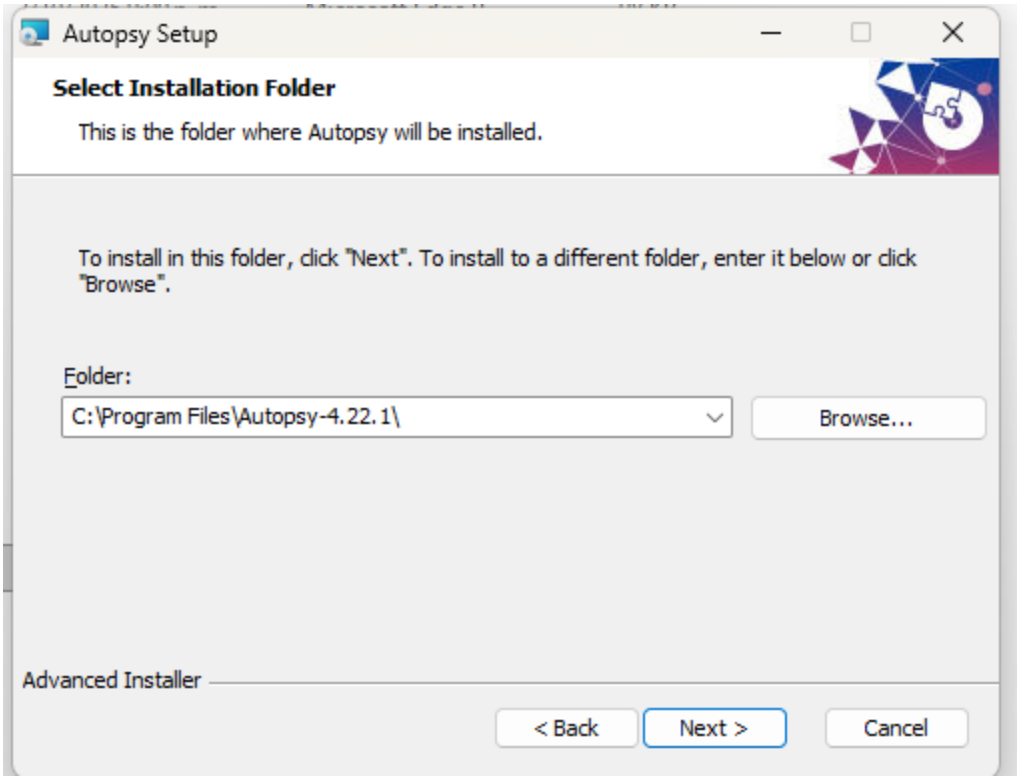

Ilustración 19-Selección del Directorio

4.1.3 Revisión Final e Inicio de la Instalación

Después de confirmar la ruta de instalación, el asistente de configuración de Autopsy presentó la pantalla de revisión final ("Ready to Install"), confirmando que el *Setup Wizard* estaba listo para iniciar la instalación. Se indicó que, para comenzar la instalación, se debía seleccionar el botón **"Install"**. En este punto, el examinador procedió a ejecutar la instalación del *software* forense en el sistema.

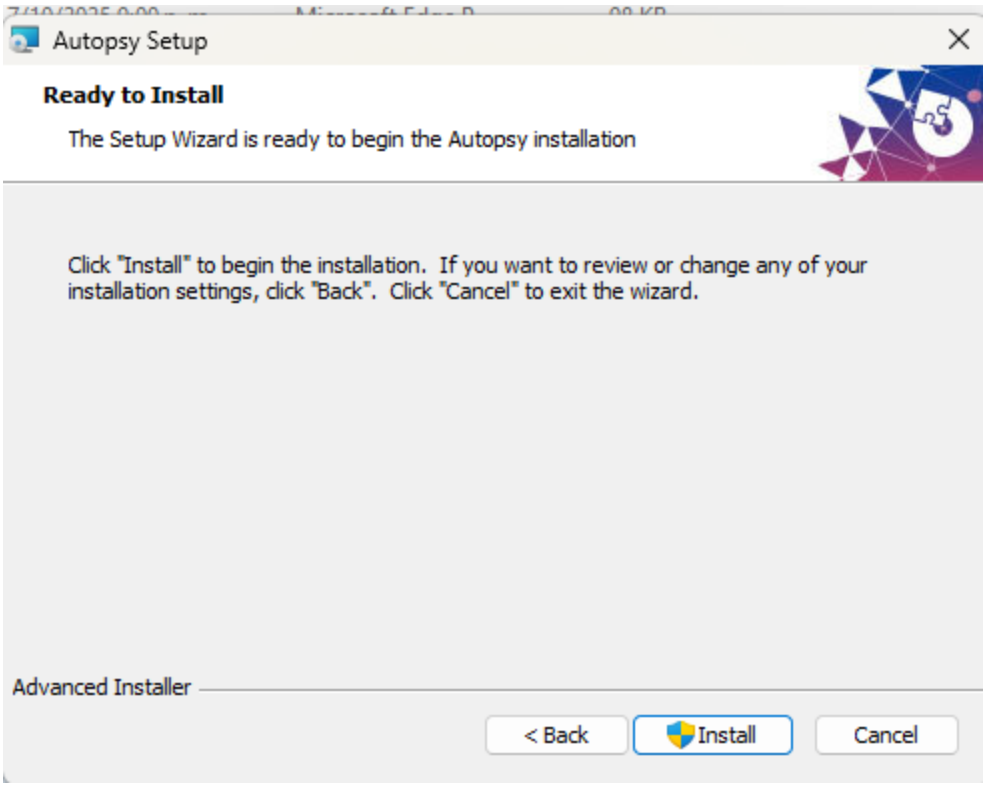

Ilustración 20-Revisión Final e Inicio de la Instalación

4.1.4 Finalización de la Instalación

Una vez completada la copia de archivos, el Asistente de Configuración de Autopsy mostró la notificación de finalización. Se instruyó al examinador a seleccionar el botón **"Finish"** para salir del asistente y dar por concluida la instalación del *software* forense en el sistema

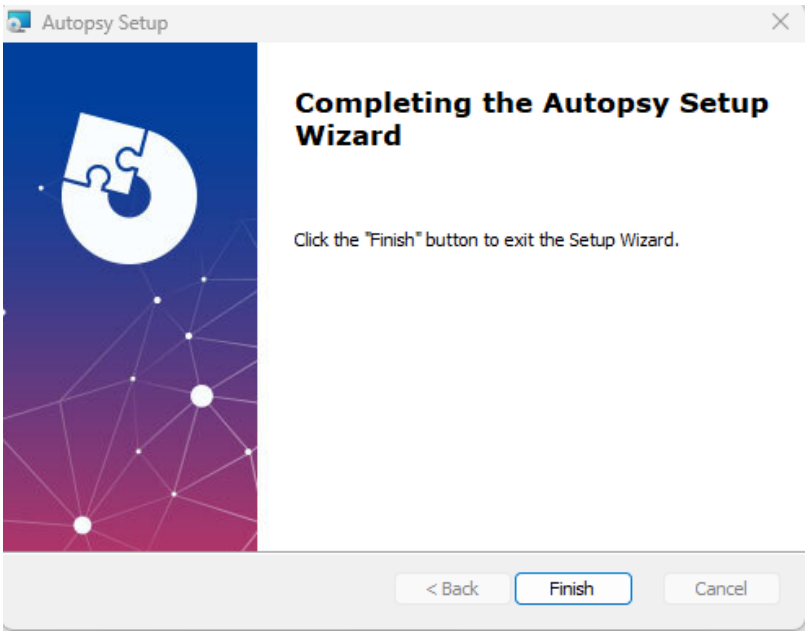

Ilustración 21-Finalización de la Instalación

4.2 Fase de Análisis y Procesamiento

4.2.1 Inicialización de Autopsy y Creación de Nuevo Caso

Al iniciar la aplicación, se mostró la ventana de bienvenida que ofrecía las opciones de "New Case" (Nuevo Caso), "Open Recent Case" (Abrir Caso Reciente) o "Open Case" (Abrir Caso). Para comenzar la investigación sobre la memoria USB, el examinador seleccionó la opción de crear un nuevo caso.

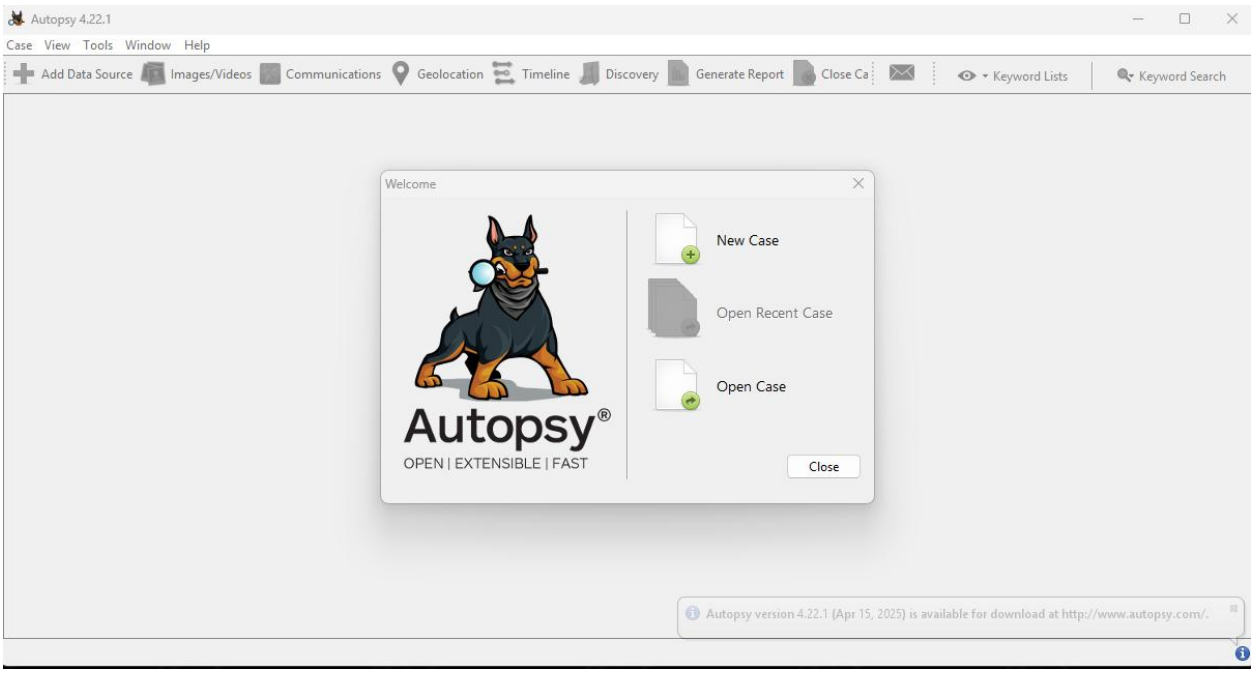

Ilustración 22-Inicialización de Autopsy y Creación de Nuevo Caso

4.2.2 Manejo de la Imagen Forense en el Entorno de Análisis

Antes de la importación formal al caso, fue necesario asegurar la accesibilidad de la imagen forense al entorno de trabajo de Autopsy. La evidencia digital, denominada imagen_usb_azul2_forense.dd, fue creada previamente en un entorno Linux y luego fue accedida a través de una carpeta compartida en el entorno Windows de análisis.

Acceso a la Evidencia:

La Figura 23 muestra la configuración de las carpetas compartidas del entorno virtual, donde se puede observar que el archivo de imagen forense se encuentra accesible desde la ruta de escritorio del usuario. Esto fue un paso logístico crucial para que el *software* de análisis pudiera localizar la copia *bit a bit* de la memoria USB.

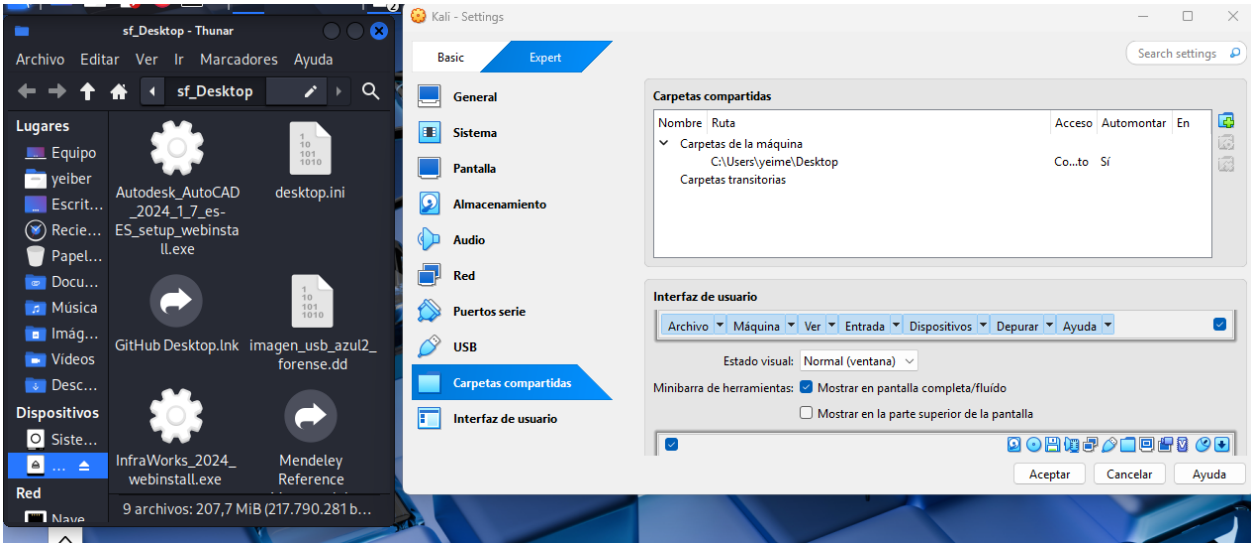

Ilustración 23-Manejo de la Imagen Forense en el Entorno de Análisis

4.2.3 Verificación de la Evidencia

La Figura 24 muestra el archivo de la imagen forense, identificado como imagen_usb_azul2_forense.dd, el cual es la copia *bit a bit* de 121 MiB de la memoria USB azul. La verificación visual de la existencia y la correcta nomenclatura del archivo fue el paso previo a su importación dentro del *software* Autopsy.

Ilustración 24-Verificación de la Evidencia

4.2.4 Creación y Configuración del Caso Forense

Tras la inicialización de Autopsy, el examinador procedió a la creación de un nuevo caso para organizar la evidencia de la memoria USB, ingresando la información esencial requerida.

Información Básica del Caso:

La Figura 25 muestra la pantalla donde se registraron los parámetros iniciales del caso:

- **Nombre del Caso (*Case Name*):** Se asignó el identificador **MI_SEGUNDO_CASO_FORENCE**.
- **Directorio Base (*Base Directory*):** Se especificó la ruta **C:\SEGUNDO ANALISIS FORENCE** para el almacenamiento de los metadatos y la base de datos del caso.
- **Tipo de Caso (*Case Type*):** Se seleccionó **Single-User** (Usuario Único).
- **Directorio de Datos:** El sistema confirmó que los datos del caso se almacenarían en la ruta C:\SEGUNDO ANALISIS FORENCE\MI_SEGUNDO_CASO_FORENCE.

Una vez ingresados los datos, se seleccionó **"Next"** para continuar con la información opcional del caso.

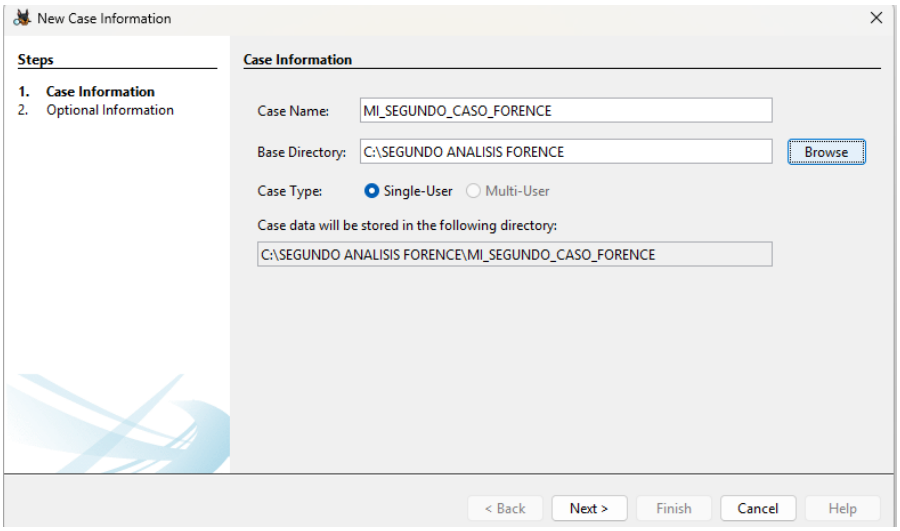

Ilustración 25-Creación y Configuración del Caso Forense

4.2.5 Información del Analista

Después de ingresar la información básica del caso, se procedió a registrar los datos del examinador y los detalles opcionales, como se muestra en la Figura 26.

Información Opcional y del Examinador:

- **Número de Caso:** Se registró como **ANALISIS FOTRENCE29**.
- **Nombre del Examinador (*Examiner Name*):** Se ingresó **YEIBER A. MENA ROBLEDO**, estableciendo la autoría y la trazabilidad de las acciones realizadas.
- **Contacto del Examinador:** Se incluyó el número de teléfono **3206653005** y el correo electrónico **yeimena53@gmail.com**.
- **Organización:** El campo de organización se dejó en el estado **"Not Specified"**.

Una vez completados todos los campos de información, se seleccionó el botón **"Finish"** para finalizar la configuración y crear formalmente la estructura del caso en la base de datos de Autopsy.

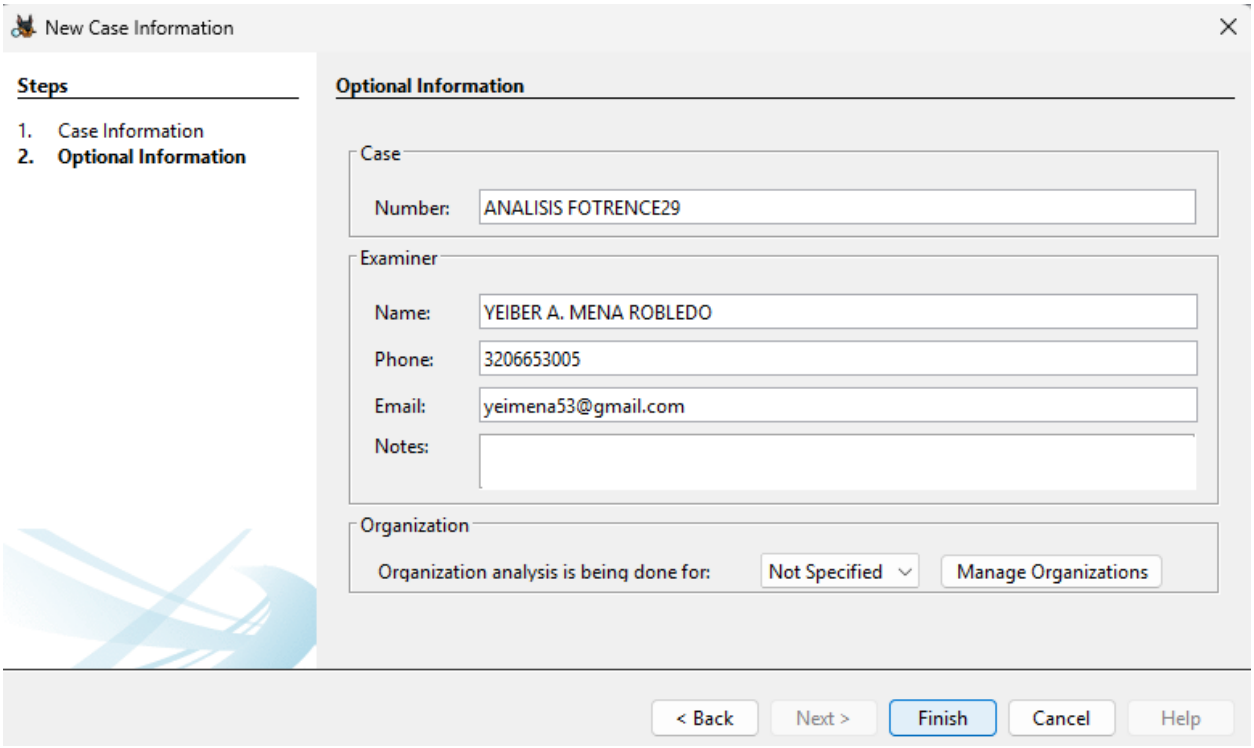

Ilustración 26-Información del Analista

4.2.6 Adición de la Fuente de Datos (Imagen Forense)

Una vez creado el caso, se procedió a incorporar la imagen forense de la memoria USB (imagen_usb_azul2_forense.dd) como la fuente de datos a examinar. Este proceso se inicia con la selección del **Host**, el cual organiza la información y otras fuentes de datos.

Selección del Host:

En la Figura 27, se observa la primera etapa del asistente de adición de fuentes de datos. El examinador optó por la opción **"Generate new host name based on data source name"** (Generar un nuevo nombre de *host* basado en el nombre de la fuente de datos), permitiendo que Autopsy asignara automáticamente un nombre al *host* a partir del archivo de la imagen forense.

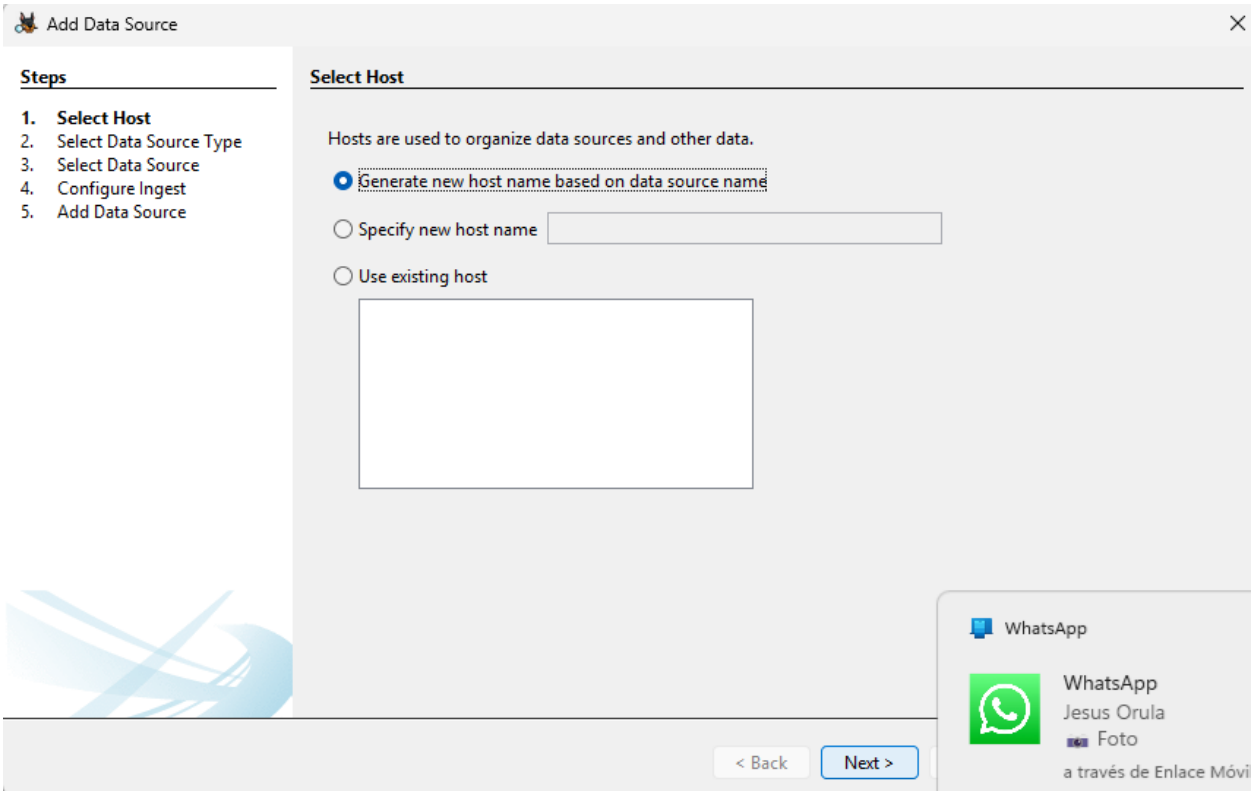

Ilustración 27-Adición de la Fuente de Datos (Imagen Forense)

4.2.7 Selección del Tipo de Fuente de Datos

Continuando con el asistente para añadir la fuente de datos, el examinador especificó la naturaleza de la evidencia digital. Dado que el análisis se realiza sobre una copia *bit a bit* del dispositivo USB, la opción correcta seleccionada fue **"Disk Image or VM File"** (Imagen de Disco o Archivo de Máquina Virtual), tal como se observa en la Figura 28. Esta elección es

fundamental para que Autopsy interprete el archivo .dd como una imagen forense completa que incluye el sistema de archivos y el espacio no asignado.

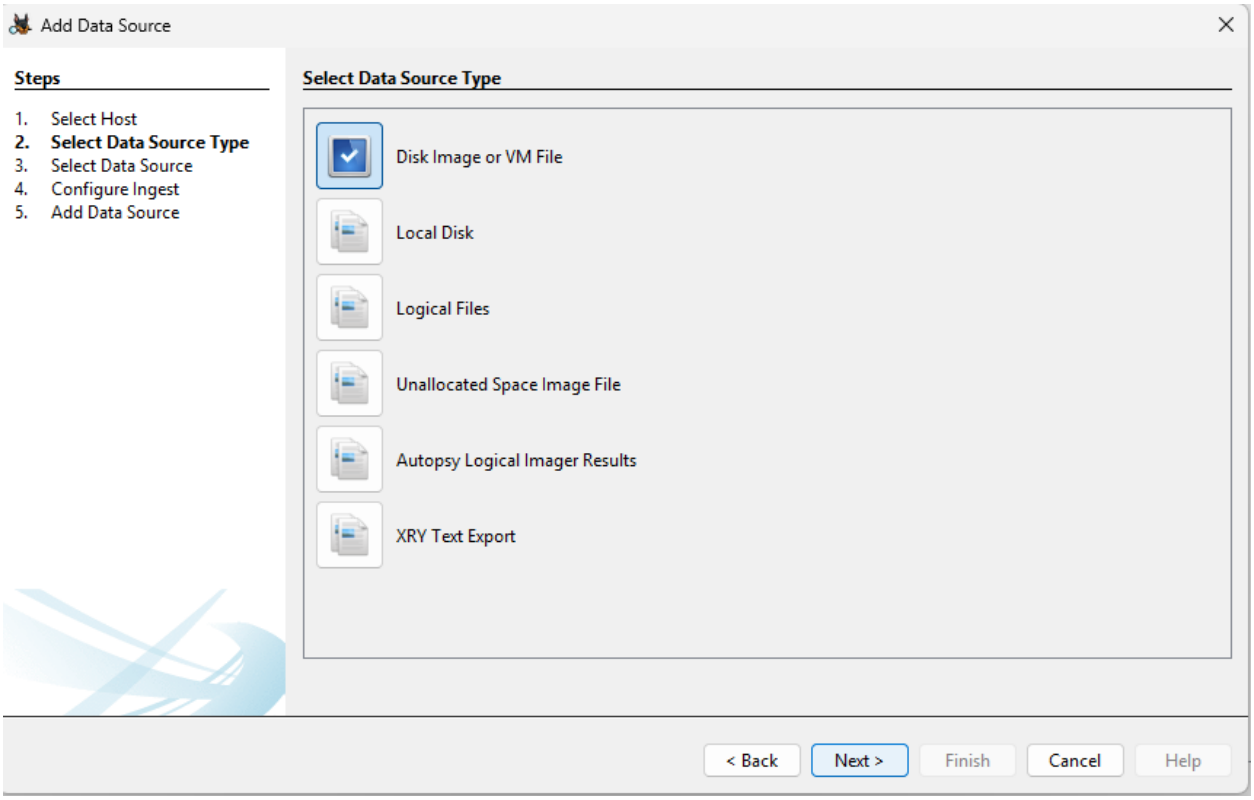

Ilustración 28-Selección del Tipo de Fuente de Datos

4.2.8 Selección de la Fuente de Datos (Ruta del Archivo)

Como tercer paso del asistente para añadir la fuente de datos, se procedió a buscar el archivo de imagen forense dentro del sistema de archivos del laboratorio. La Figura 29 muestra la ventana de diálogo "Open" (Abrir), donde el examinador navegó hasta el directorio **"Escritorio"** y seleccionó el archivo **imagen_usb_azul2_forense.dd**. Esta acción localizó la copia bit a bit de la memoria USB que se analizará. Se seleccionó **"Open"** y luego **"Next"** para avanzar al siguiente paso de configuración.

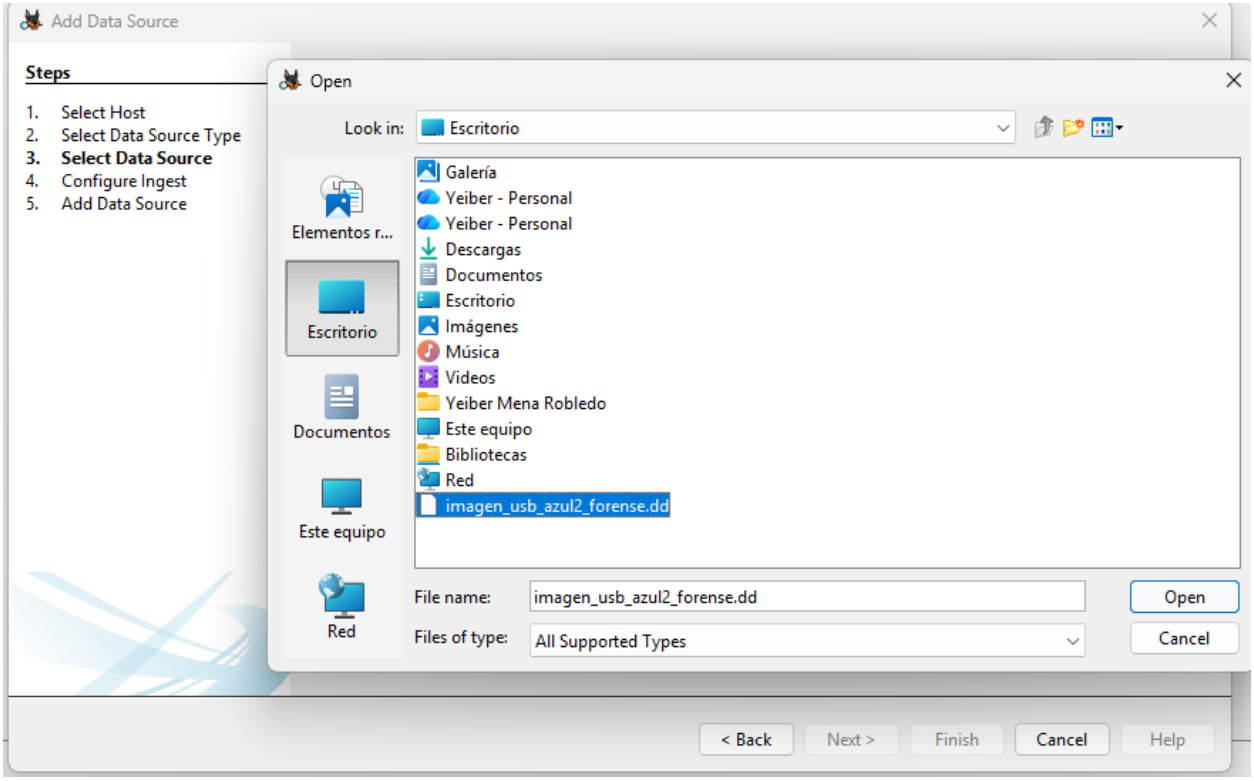

Ilustración 29-Selección de la Fuente de Datos (Ruta del Archivo)

4.2.9 Configuración de la Fuente de Datos

La Figura 30 ilustra la pantalla de configuración donde se establecieron los parámetros técnicos de la imagen forense antes de iniciar el proceso de ingesta.

- **Ruta (*Path*):** Se confirmó la ruta de acceso local al archivo: C:\Users\yeime\Desktop\imagen_usb_azul2_forense.dd.
- **Zona Horaria (*Time zone*):** Se seleccionó **(GMT-5:00) America/Bogota**, lo cual es crítico para la correcta interpretación de las marcas de tiempo (MAC times) de los archivos.
- **Tamaño de Sector (*Sector size*):** Se dejó en **Auto Detect**.

- **Valores Hash:** Los campos para el ingreso de los valores Hash (MD5, SHA-1, SHA-256) se dejaron en blanco, aunque se documentó previamente que el hash SHA1 de la imagen fue verificado al momento de su creación.

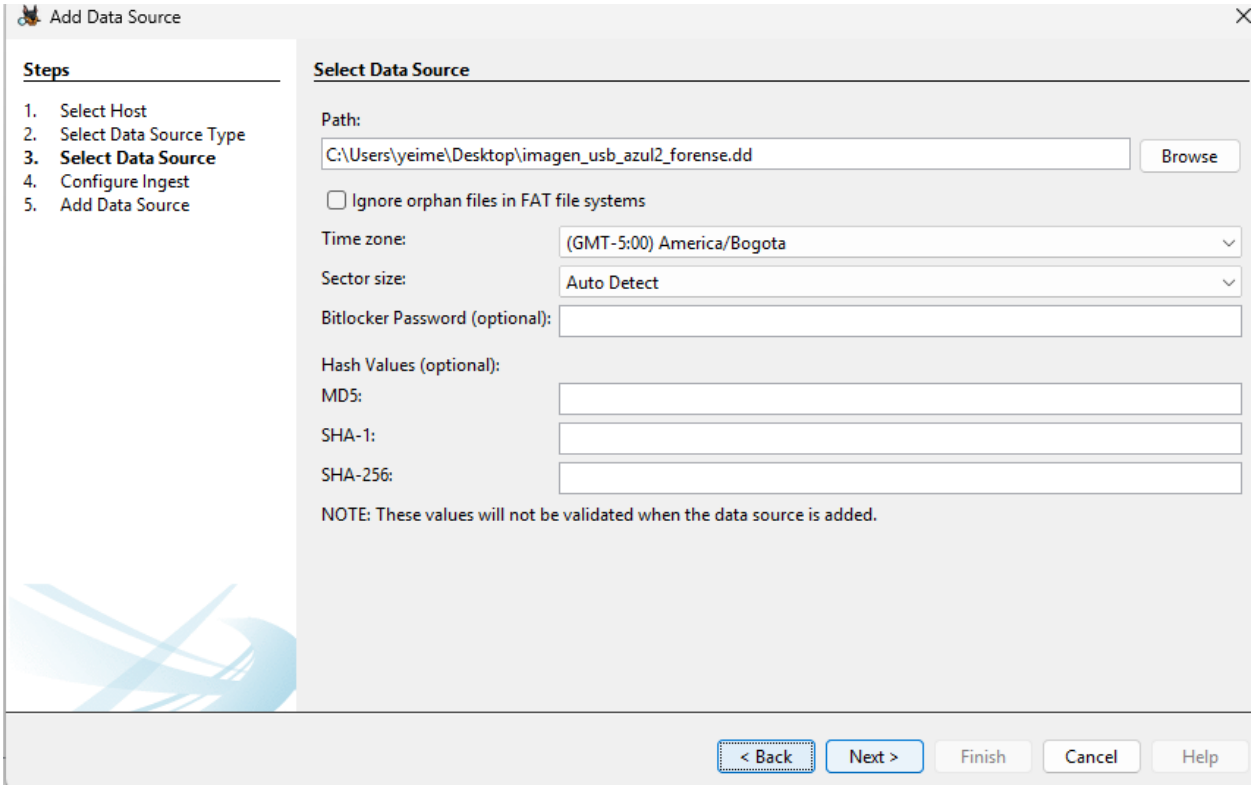

Ilustración 30-Configuración de la Fuente de Datos

4.2.10 Configuración de los Módulos de Ingesta

El cuarto paso del asistente consistió en la selección de los módulos de ingesta, que son las herramientas automatizadas que Autopsy ejecuta sobre la fuente de datos para extraer artefactos y generar la base de datos de análisis.

Como se muestra en la Figura 31, se seleccionó ejecutar los módulos sobre **"All Files, Directories, and Unallocated Space"** (Todos los Archivos, Directorios y Espacio No Asignado) de la imagen forense. Entre los módulos activados por el examinador se incluyeron:

- **Recent Activity** (Actividad Reciente).
- **Hash Lookup** (Búsqueda de Hash).
- **File Type Identification** (Identificación de Tipo de Archivo).
- **Keyword Search** (Búsqueda de Palabras Clave).
- **PhotoRec Carver** (Recuperación de Archivos Eliminados).
- **Encryption Detection** (Detección de Cifrado).

Esta selección exhaustiva de módulos garantizó una recopilación profunda de artefactos, archivos eliminados y metadatos antes del análisis manual.

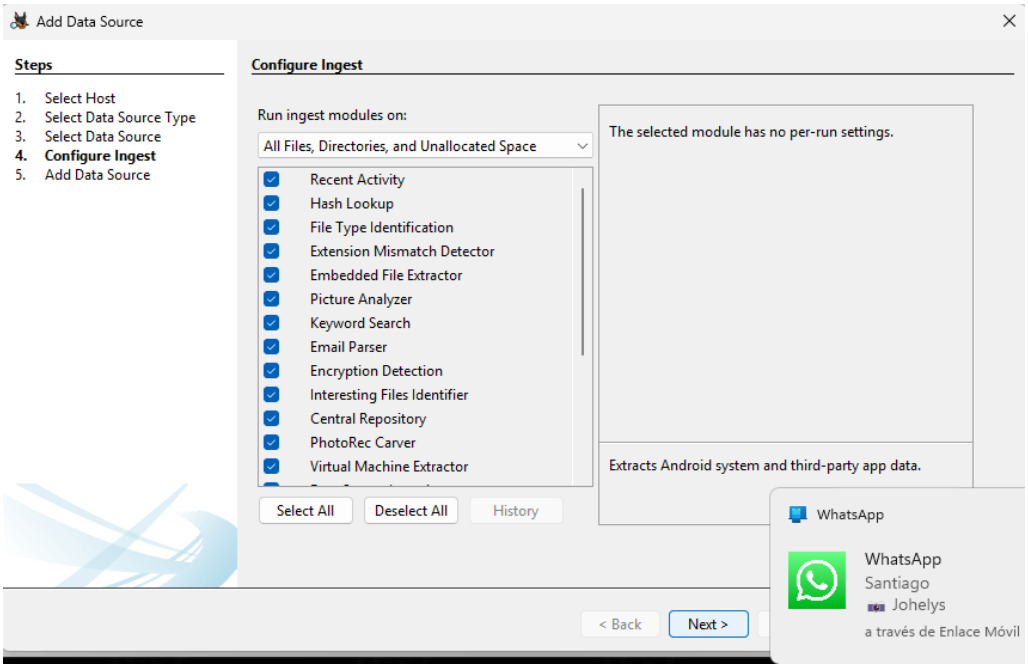

Ilustración 31-Configuración de los Módulos de Ingesta

4.2.11 Adición Final de la Fuente de Datos

El paso final del asistente confirmó que la imagen forense fue añadida con éxito a la base de datos local del caso. La Figura 32 muestra la notificación de que la fuente de datos ha sido incorporada, y que los archivos están siendo analizados por los módulos de ingesta previamente configurados. En este punto, el examinador seleccionó el botón **"Finish"** para cerrar el asistente y acceder a la interfaz principal de análisis de Autopsy.

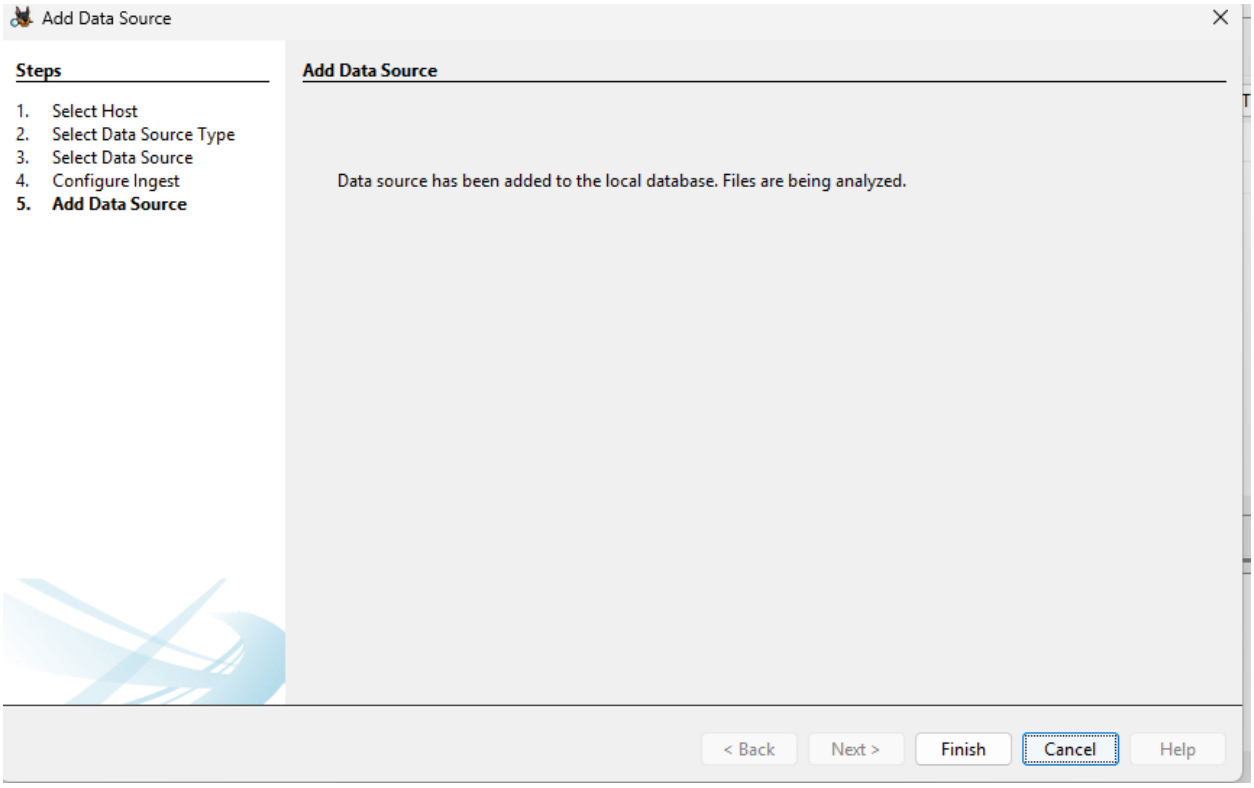

Ilustración 32-Adición Final de la Fuente de Datos

4.2.12 Interfaz Principal de Análisis y Verificación de la Evidencia

Tras la finalización del asistente, el examinador accedió a la interfaz principal de Autopsy para iniciar el análisis manual de la evidencia.

Vista General del Caso Cargado:

La Figura 33 muestra la interfaz de Autopsy (versión 4.22.1) con el caso **MISEGUNDOCASO** abierto.

- En el panel de la izquierda (árbol de navegación), se visualiza la estructura del caso, incluyendo las categorías de artefactos generados por los módulos de ingesta (Archivos Eliminados, Artefactos de Datos, Resultados de Análisis, etc.).
- En el panel central, bajo la sección *Data Sources* (Fuentes de Datos), se confirma la correcta adición de la imagen forense, la cual fue nombrada automáticamente como **imagen_usb_azul2_forense.dd_1_Host**.

Con la fuente de datos correctamente cargada y los módulos de ingesta en funcionamiento, el examinador puede proceder al análisis detallado de los artefactos.

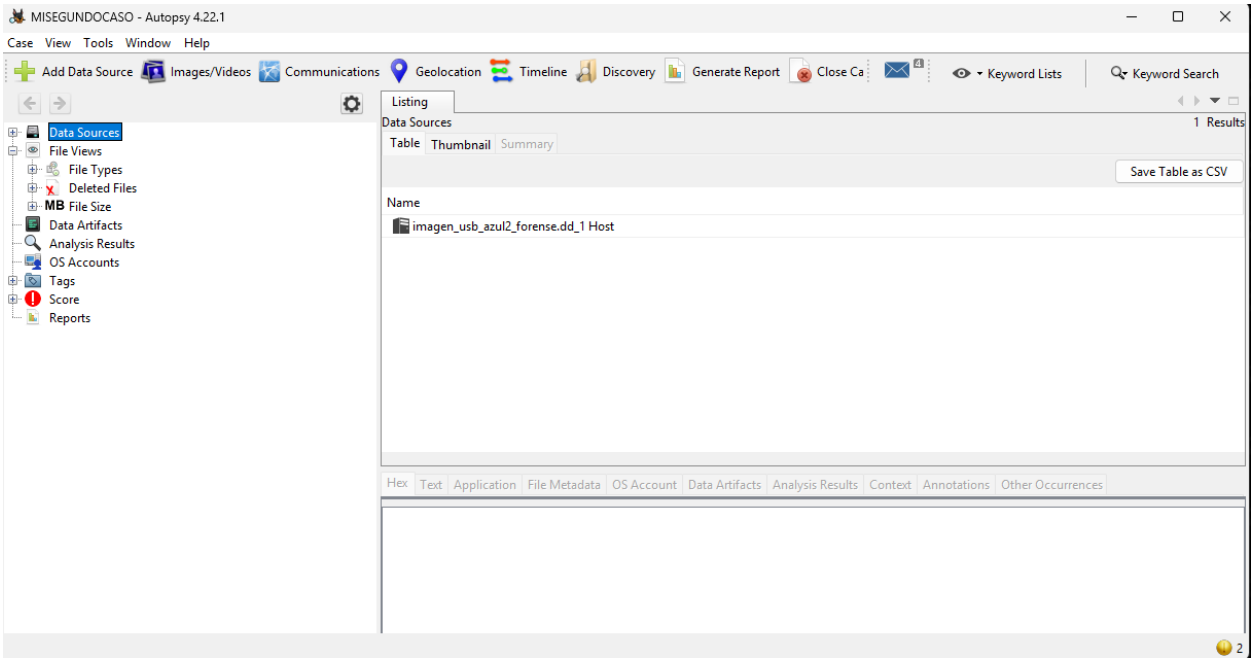

Ilustración 33-. Interfaz Principal de Análisis y Verificación de la Evidencia

4.2.13 Exploración de Estructuras de Volumen y Particiones

El examinador procedió a la exploración de la imagen forense (imagen_usb_azul2_forense.dd) para identificar y analizar las estructuras lógicas que componen la evidencia digital.

Identificación de Volúmenes:

La Figura 34 muestra el árbol de navegación de datos y el panel de listado de volúmenes:

- **vol1 (Unallocated):** Identificado como espacio no asignado (sectores 0-237), de tipo Unallocated.
- **vol2 (Partición Principal):** Esta partición fue identificada con el rango de sectores 238-246527, de tipo **Win95 FAT32 (0x0b)**, que corresponde al volumen principal de la memoria USB.
- **vol3 (Unallocated):** Un segundo bloque de espacio no asignado (sectores 246528-247807), también de tipo Unallocated.

El hallazgo de estos volúmenes y del espacio no asignado (Unallocated) fue crucial, ya que el análisis forense se enfocará principalmente en el contenido de la partición principal (vol2) y en la posible recuperación de datos del espacio no asignado.

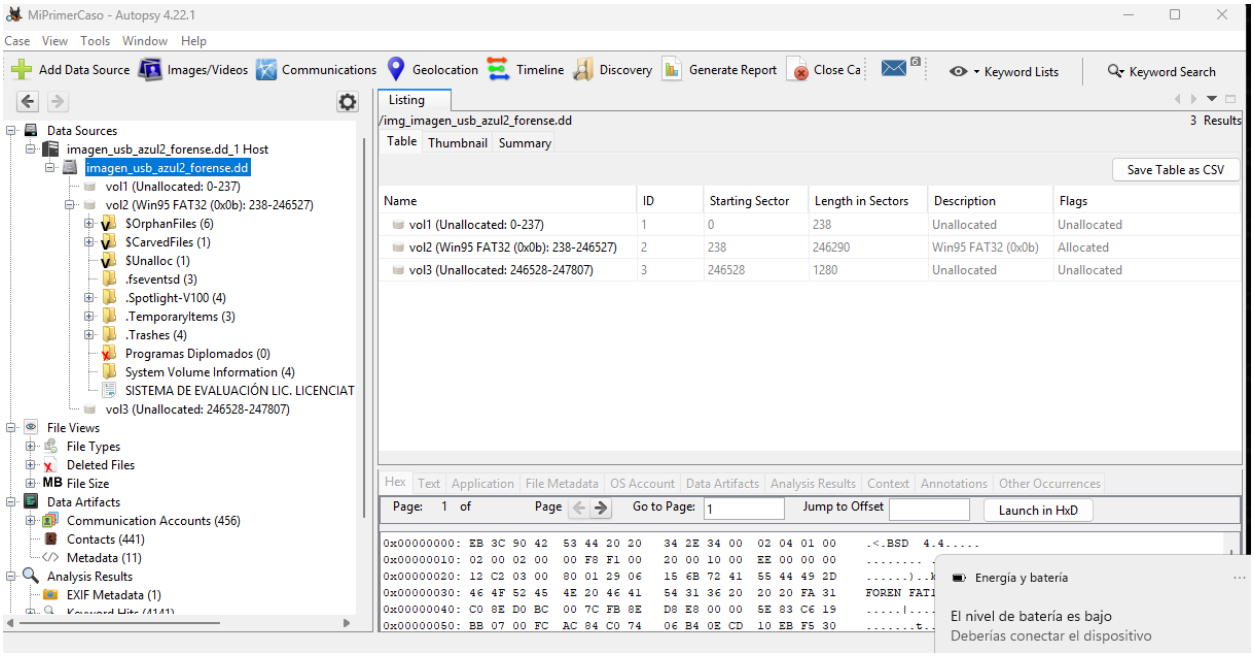

Ilustración 34-Exploración de Estructuras de Volumen y Particiones

4.2.14 Análisis del Volumen Principal (vol2)

El examinador procedió a analizar el contenido del volumen principal (vol2), la partición de tipo Win95 FAT32 de 121 MiB de la memoria USB.

Visualización del Contenido:

La Figura 35 ilustra la vista de lista del volumen (vol2), mostrando los archivos y artefactos identificados por Autopsy. Esta vista proporciona información crítica, incluyendo:

- **Búsqueda de Archivos Eliminados:** En el panel de navegación izquierdo, se observa la categorización de los archivos, destacando el acceso a **Deleted Files** (Archivos Eliminados) y **$CarvedFiles** (Archivos Recuperados por *Carving*).

- **Valores Hash:** En el panel de listado de archivos, la herramienta generó automáticamente los valores **Hash MD5 y SHA-256** para cada elemento, lo cual permite la verificación de integridad y la comparación con bases de datos de *hash* conocidos.
- **Estructuras de Directorio:** Se observa la presencia de estructuras lógicas como directorios de sistema (ej. \$OrphanFiles, \$Recycled), así como carpetas con nombres de contenido (Programas Diplomados, SISTEMA DE EVALUACIÓN LICENCIATURA) que fueron indexadas de la imagen forense.

Este análisis inicial confirmó la capacidad de Autopsy para extraer metadatos y proporcionar una base para la búsqueda de información crítica oculta o eliminada.

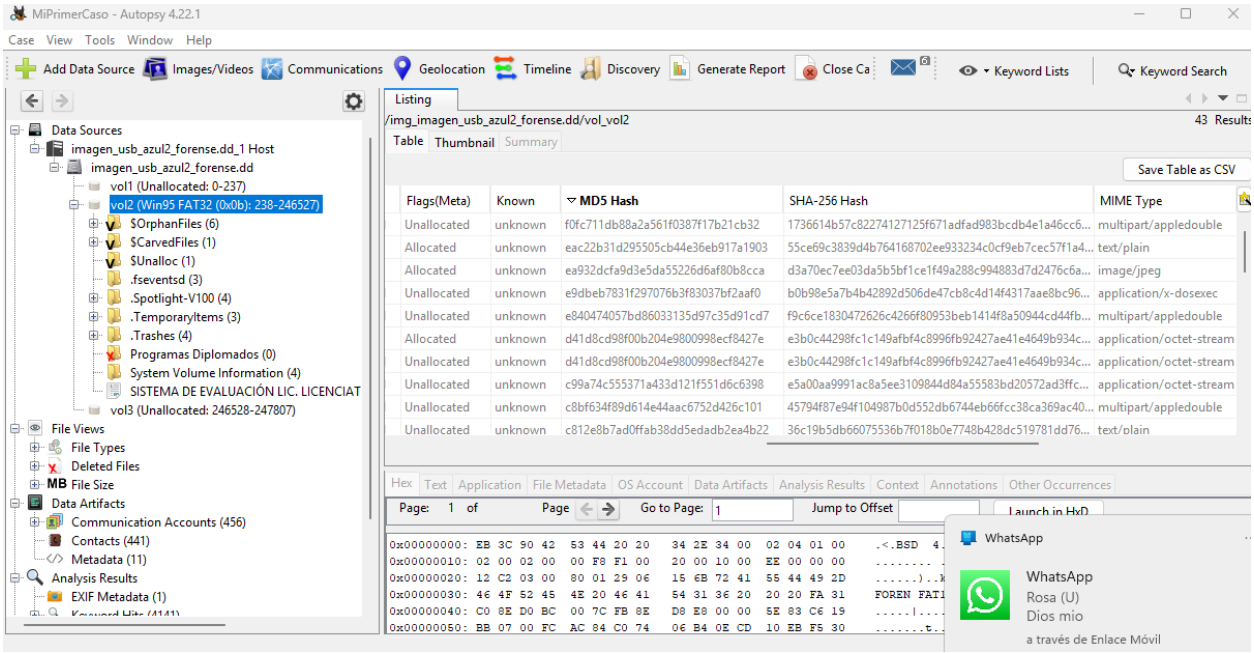

Ilustración 35-Análisis del Volumen Principal (vol2)

5. CAPITULO#3 DESARROLLO DEL LABORATORIO

5.1 Análisis Complementario con FTK Imager

Se decidió realizar un análisis complementario de la imagen forense (imagen_usb_azul2_forense.dd) utilizando la herramienta gratuita **AccessData FTK Imager**, principalmente reconocida por sus capacidades de adquisición y visualización de bajo nivel.

5.1.1 Descarga e Instalación de FTK Imager

Descarga del Instalador:

La Figura 36 documenta el proceso inicial de obtención del *software* FTK Imager. Se observó que la versión descargada fue la **3.1.2 (x86)**, con un tamaño de archivo de **28.4 MB**. Esta acción fue el primer paso para la preparación de la herramienta complementaria de análisis

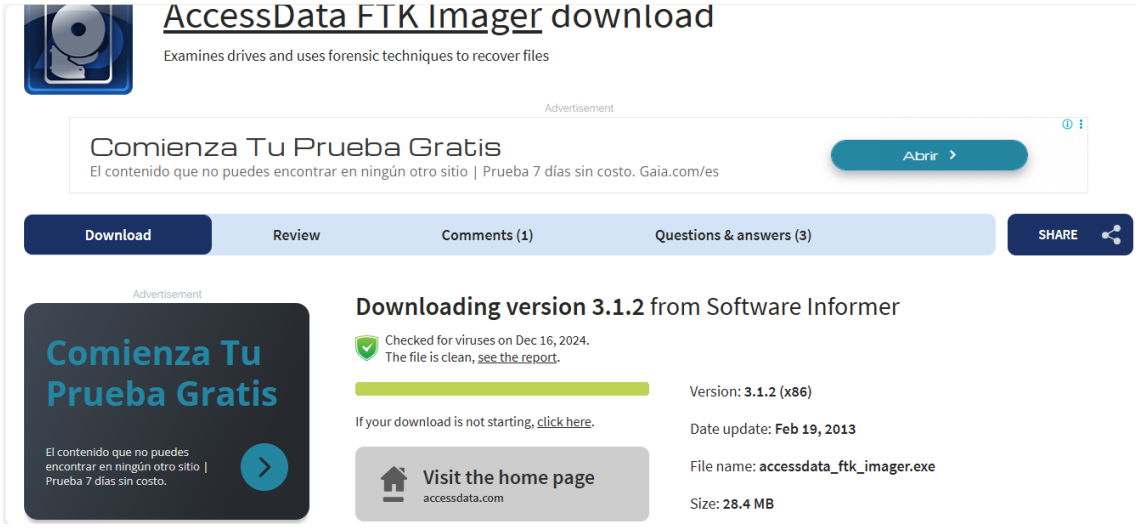

Ilustración 36-Descarga e Instalación de FTK Imager

5.1.2 Descarga e Instalación de FTK Imager

Inicio del Instalador:

Una vez descargado el archivo, se ejecutó el *InstallShield Wizard* para comenzar la instalación de AccessData FTK Imager. La Figura 37 muestra la pantalla de bienvenida del asistente, la cual notifica que el *software* está protegido por derechos de autor y tratados internacionales.

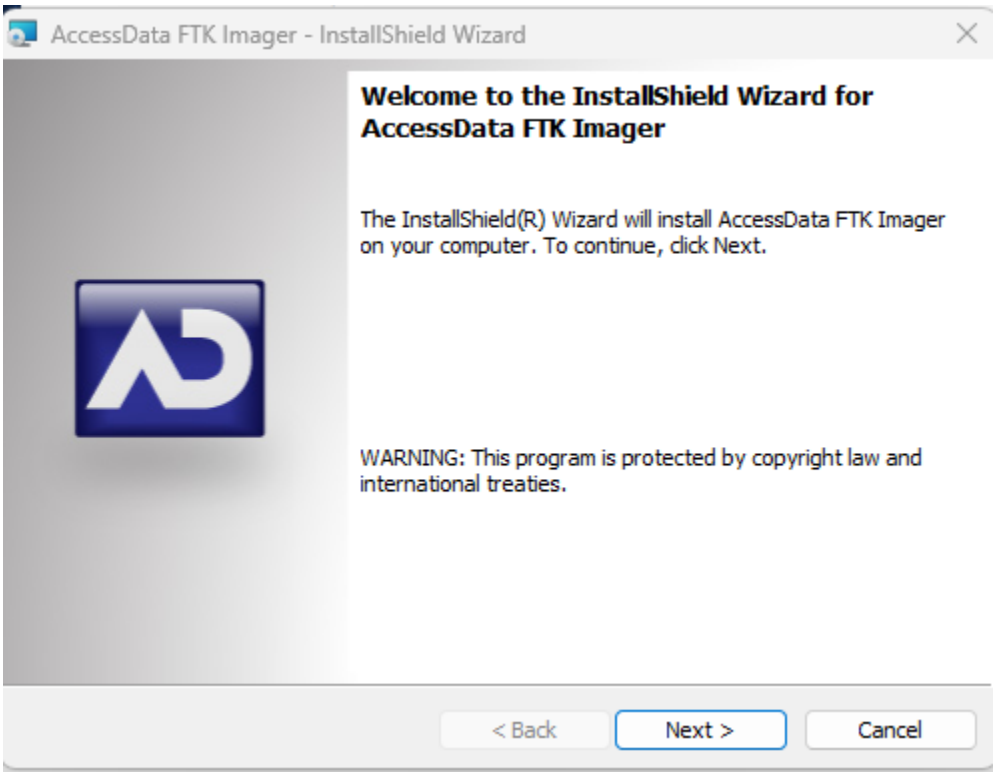

Ilustración 37-Descarga e Instalación de FTK Imager

5.1.3 Selección del Directorio de Destino

Luego de aceptar los términos de la licencia, el asistente de instalación de FTK Imager solicitó al examinador que especificara la carpeta de destino para el *software*. Como se aprecia en la Figura 38, se confirmó la ruta por defecto: **C:\Program Files (x86)\AccessData**.

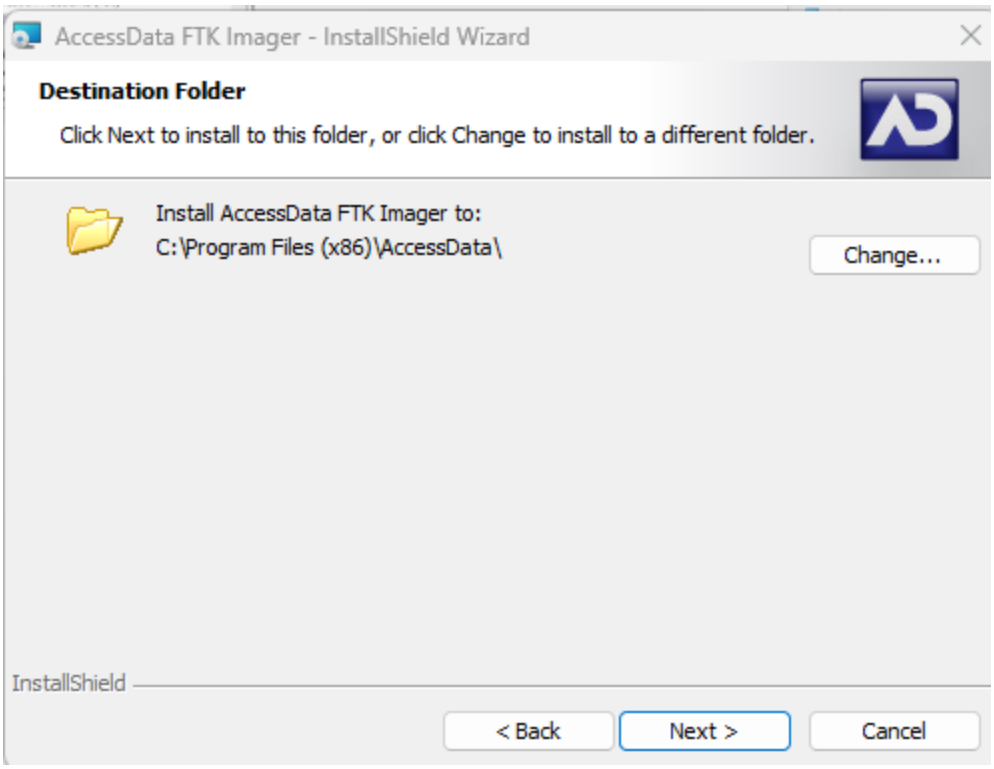

Ilustración 38-Selección del Directorio de Destino

5.1.4 Revisión Final e Instalación del Programa

Habiendo confirmado el directorio de destino, el *InstallShield Wizard* presentó la pantalla de revisión final ("Ready to Install the Program"). Esta etapa indicó que el asistente estaba listo para comenzar la instalación del *software* FTK Imager. El examinador procedió a seleccionar el botón **"Install"** para iniciar la copia de los archivos del programa en el sistema de laboratorio.

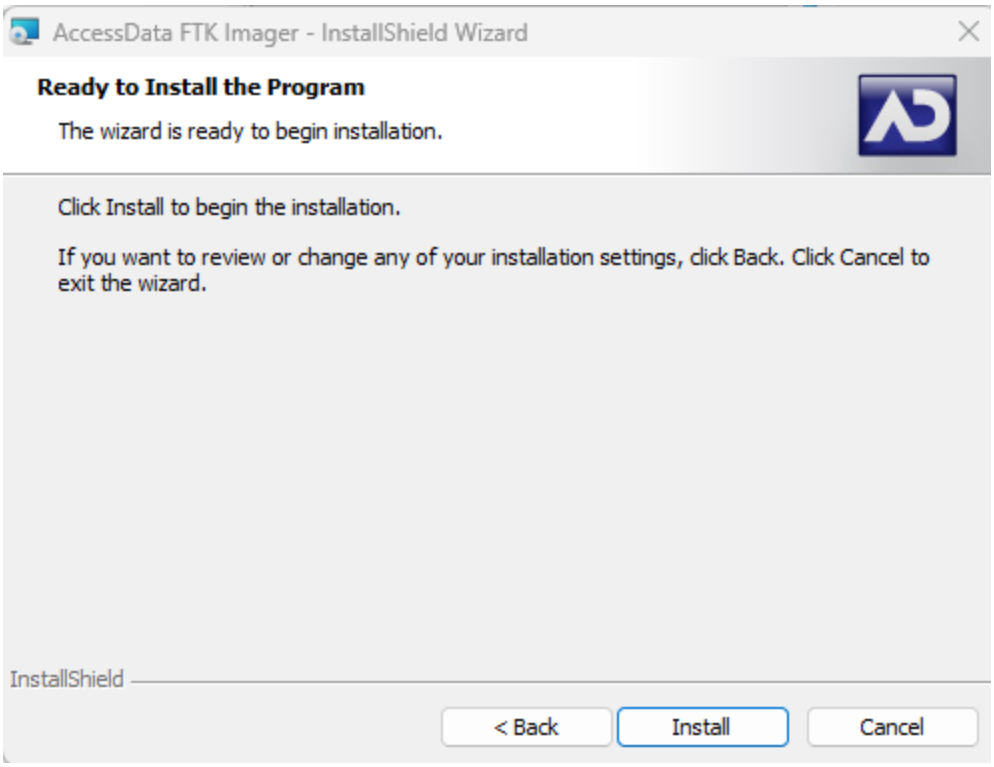

Ilustración 39-Revisión Final e Instalación del Programa

5.1.5 Inicialización de FTK Imager

Lanzamiento y Vista de la Interfaz:

Una vez finalizada la instalación de AccessData FTK Imager, el examinador procedió a la ejecución del programa. La Figura 40 muestra la interfaz principal de la versión 3.1.2.0, lista para cargar la evidencia. La interfaz se divide en tres paneles principales: el **Evidence Tree** (Árbol de Evidencia) a la izquierda, el **File List** (Lista de Archivos) en la parte superior central, y el panel de **Visualización/Hexadecimal** en la parte inferior, herramientas esenciales para la exploración de la evidencia digital.

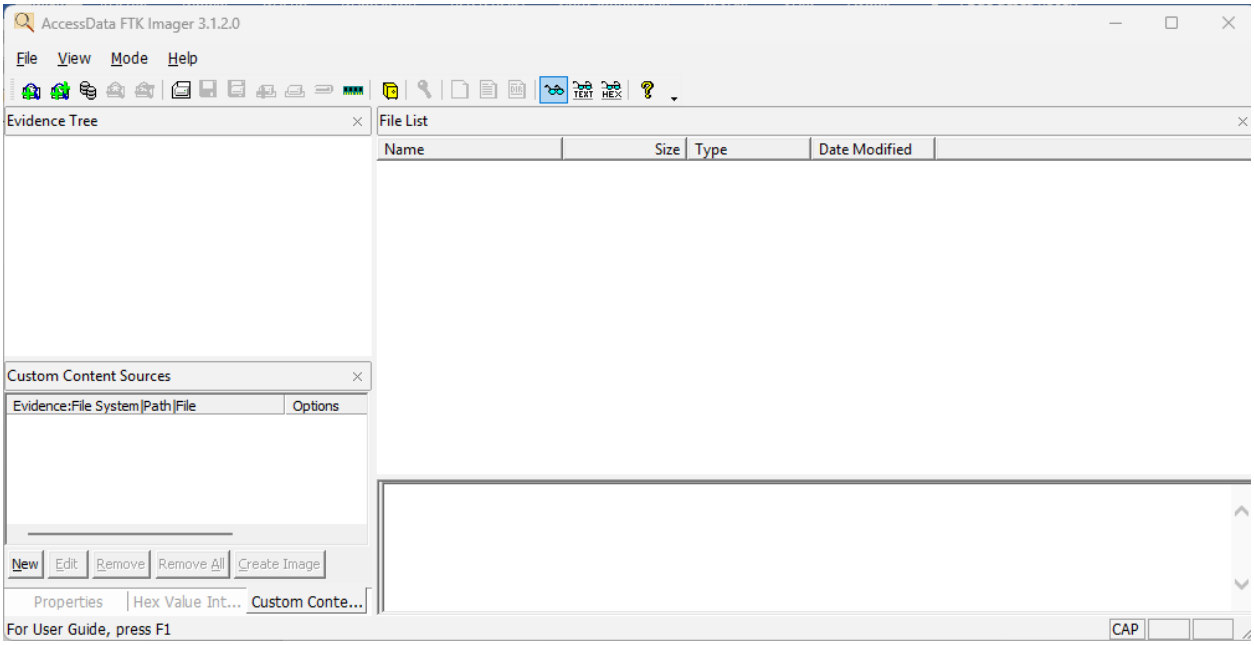

Ilustración 40-Inicialización de FTK Imager

5.1.6 Adición de la Imagen Forense

Para iniciar el análisis, se procedió a cargar la imagen forense previamente adquirida (imagen_usb_azul2_forense.dd) en FTK Imager.

Selección del Tipo de Fuente de Evidencia:

Al añadir una nueva fuente de evidencia, el examinador seleccionó la opción **"Image File"** (Archivo de Imagen) , como se muestra en la Figura 41. Esta opción es la adecuada para trabajar con la copia bit a bit del dispositivo USB.

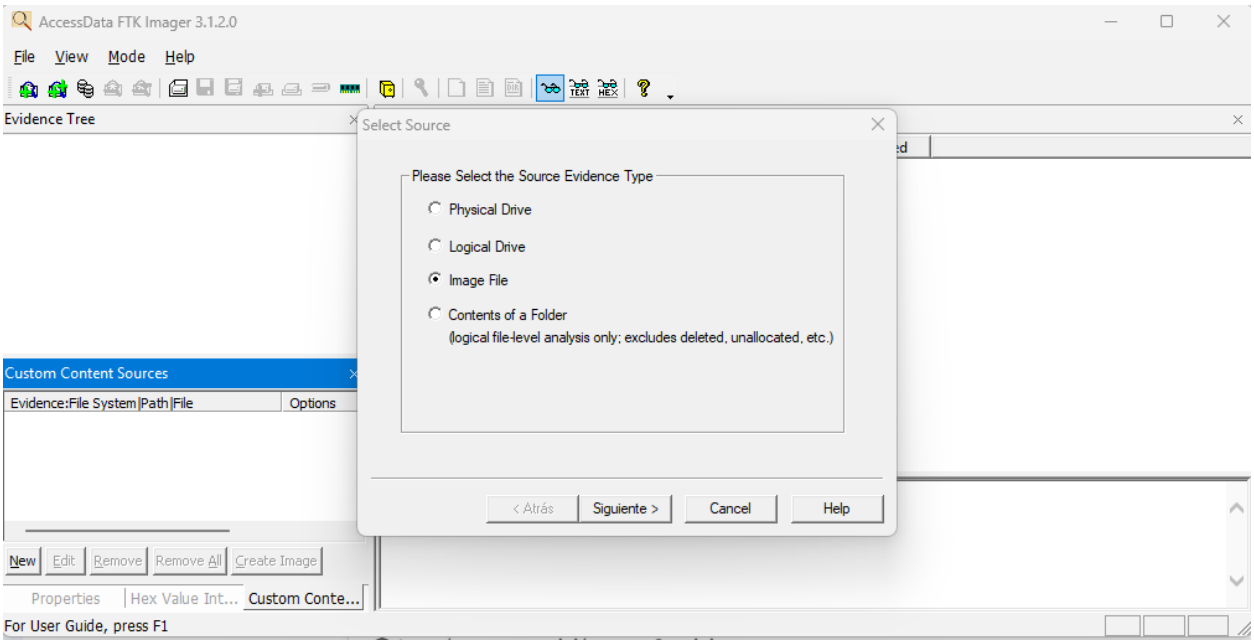

Ilustración 41-Adición de la Imagen Forense

5.1.7 Localización del Archivo de Imagen Forense

Después de seleccionar el tipo de fuente como "Image File", el asistente de FTK Imager solicitó la ruta del archivo de evidencia. La Figura 43 muestra que el examinador navegó hasta el directorio "Escritorio" y seleccionó el archivo **imagen_usb_azul2_forense.dd**. Este archivo corresponde a la copia *bit a bit* de la memoria USB azul.

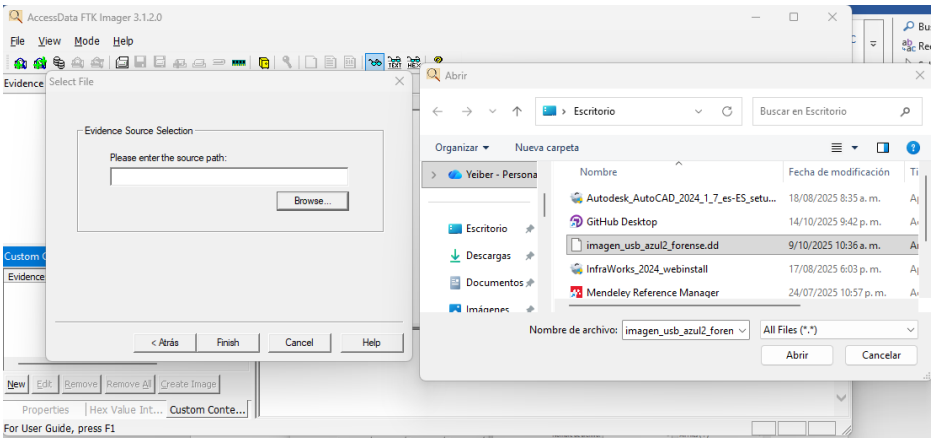

Ilustración 42-Localización del Archivo de Imagen Forense

5.1.8 Carga y Visualización de la Imagen Forense

Una vez cargada la imagen forense, el examinador procedió a expandir la estructura de volumen en el panel **Evidence Tree** para acceder a los datos lógicos de la memoria USB.

Estructura del Disco:

La Figura 45 muestra la estructura del disco tal como fue interpretada por FTK Imager:

- Se identificó la imagen principal (imagen_usb_azul2_forense.dd).
- Dentro de la imagen, se detectó el **Unpartitioned Space [Basic disk]** (Espacio No Particionado [Disco Básico]) y la partición principal: **Partition 1 [120MB]**.
- Al seleccionar la **Partition 1**, el panel hexadecimal inferior muestra información de bajo nivel correspondiente al inicio de esa partición lógica (sector físico 238).
- La vista hexadecimal en el *offset* 00000030 muestra caracteres que sugieren el tipo de sistema de archivos o una etiqueta de volumen, en este caso, **"AUDI FOREN FAT16"**.

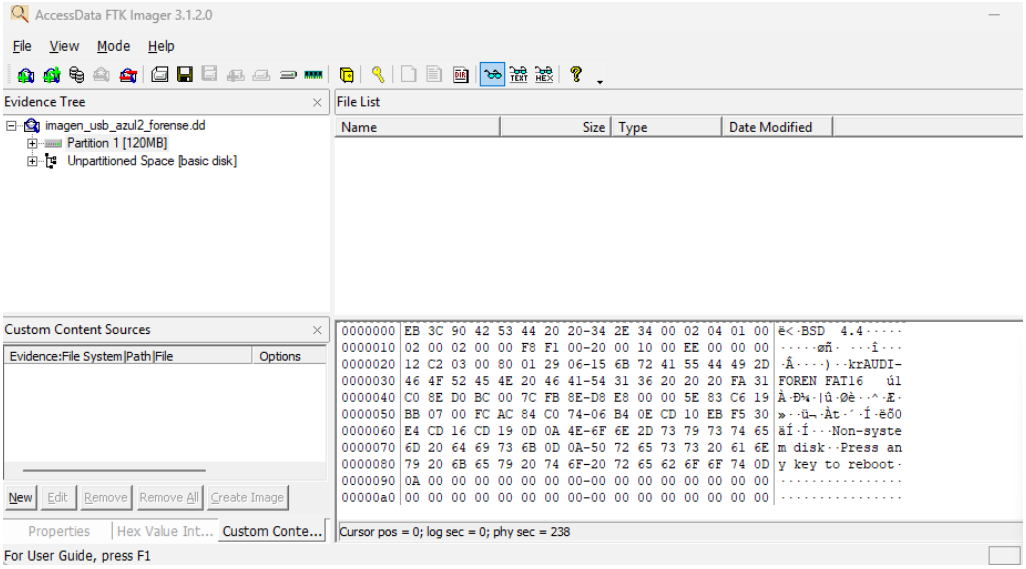

Ilustración 43-Carga y Visualización de la Imagen Forense

6. CONCLUSIÓN

El análisis forense digital practicado sobre la imagen de la memoria USB azul (imagen_usb_azul2_forense.dd) demostró la existencia de rastros de actividad y archivos previamente eliminados, confirmando así el objetivo de la investigación.

1. **Integridad de la Evidencia:** Se garantizó la autenticidad de la evidencia mediante la verificación de que el hash SHA1 del dispositivo original coincidiera con el hash SHA1 de la imagen forense, manteniendo la cadena de custodia.

2. **Archivos Recuperados:** La exploración de la imagen mediante la herramienta Autopsy (versión 2.24 y 4.22.1) fue exitosa en la identificación de archivos eliminados, señalados con el indicador de papelera roja (r/r). Entre la información recuperada se encuentran archivos de diversa naturaleza, incluyendo documentos ofimáticos (_Cifrados 2.docx), imágenes (IMG 0001.JPG), archivos de texto, y un ejecutable relacionado con el *software* forense (AccessData FTK Imager 4.7.1.exe).

3. **Validación de Técnicas:** La exitosa extracción de archivos eliminados, así como la generación de hashes MD5 de los elementos recuperados, valida la eficacia de las herramientas y técnicas forenses aplicadas, demostrando que la información no fue sobrescrita en el medio de almacenamiento.

7. REFERENCIAS

ING Rafael Sandoval Morales