INFORME DE LABORATORIO 02

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025

INFORME DE LABORATORIO 02

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

RAFAEL SANDOVAL MORALES

Docente

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

En este laboratorio se abordó la aplicación práctica de herramientas forenses especializadas como Autopsy y FTK Imager, ejecutadas tanto en entornos Kali Linux como Windows, con el fin de comprender los procedimientos de creación y verificación de imágenes forenses, así como la integridad de los datos mediante el uso de algoritmos hash.

2. OBJETIVOS

2.1 Objetivo general

Realizar el análisis forense de una memoria USB utilizando las herramientas Autopsy y FTK Imager en los sistemas operativos Kali Linux y Windows

2.2 Objetivos específicos

- Configurar el dispositivo USB dentro de VirtualBox para la captura y análisis forense.
- Generar y verificar los valores hash de la evidencia digital para asegurar su autenticidad e integridad.
- Crear una imagen forense bit a bit de la memoria USB empleando comandos de Kali Linux.
- Instalar e importar la imagen forense utilizando Autopsy.
- Instalar y ejecutar FTK Imager en Windows para examinar la misma evidencia.

3. ALCANCE

El presente informe abarca el proceso completo de análisis forense digital aplicado a una memoria USB, desde la configuración inicial del entorno virtual hasta la verificación final de los valores hash de los archivos examinados. Las actividades se desarrollan en dos sistemas operativos distintos los cuales son Kali Linux y Windows.

El alcance de esta práctica se limita a la fase de adquisición, preservación y análisis básico de evidencias digitales.

4. CAPITULO 1 – ANALISIS FORENSE CON AUTOPSY EN KALI LINUX

4.1 Configuración de dispositivos USB en VirtualBox

En el menú de dispositivos de VirtualBox, luego USB seleccionar el dispositivo "Generic Flash Card Reader/Writer" la cual es el nombre de nuestra memoria USB insertada (el nombre puede variar), esto permite que la memoria esté disponible dentro de la máquina virtual Kali Linux para el análisis forense.

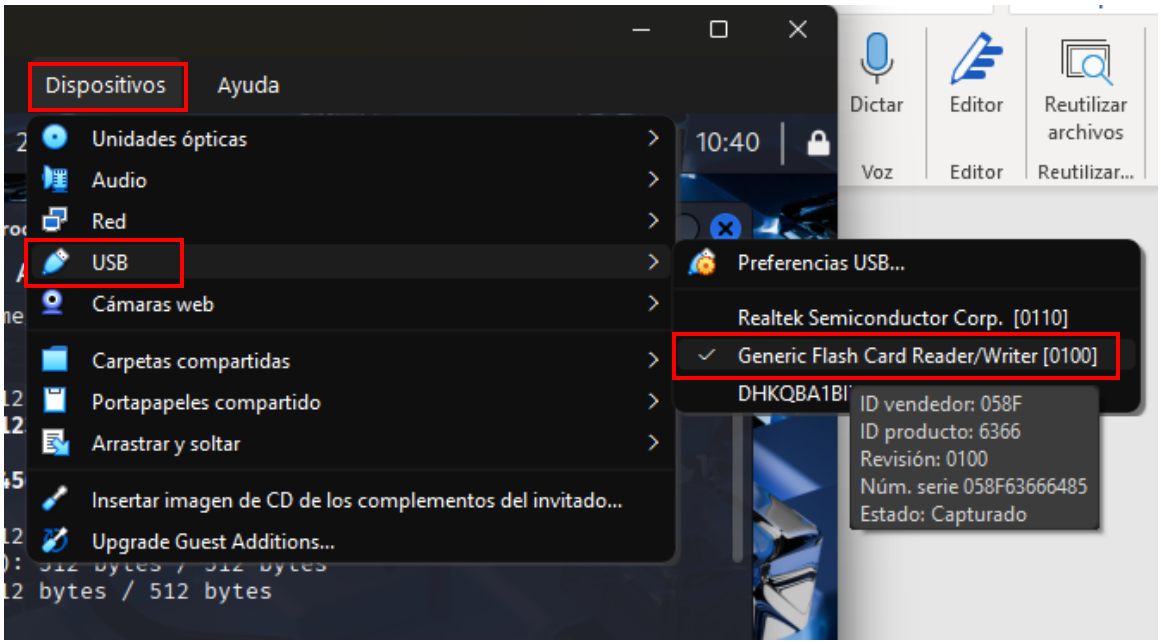

Ilustración 1. Configuración de dispositivos USB

4.2 Identificación de discos con el comando fdisk

En la terminal de Kali Linux ingresar al modo superusuario y luego ejecutar el comando **fdisk -l** para listar los discos disponibles. Se identifican dos dispositivos: /dev/sda (disco principal del sistema) y /dev/sdb (memoria USB de 3.75 GB conectada).

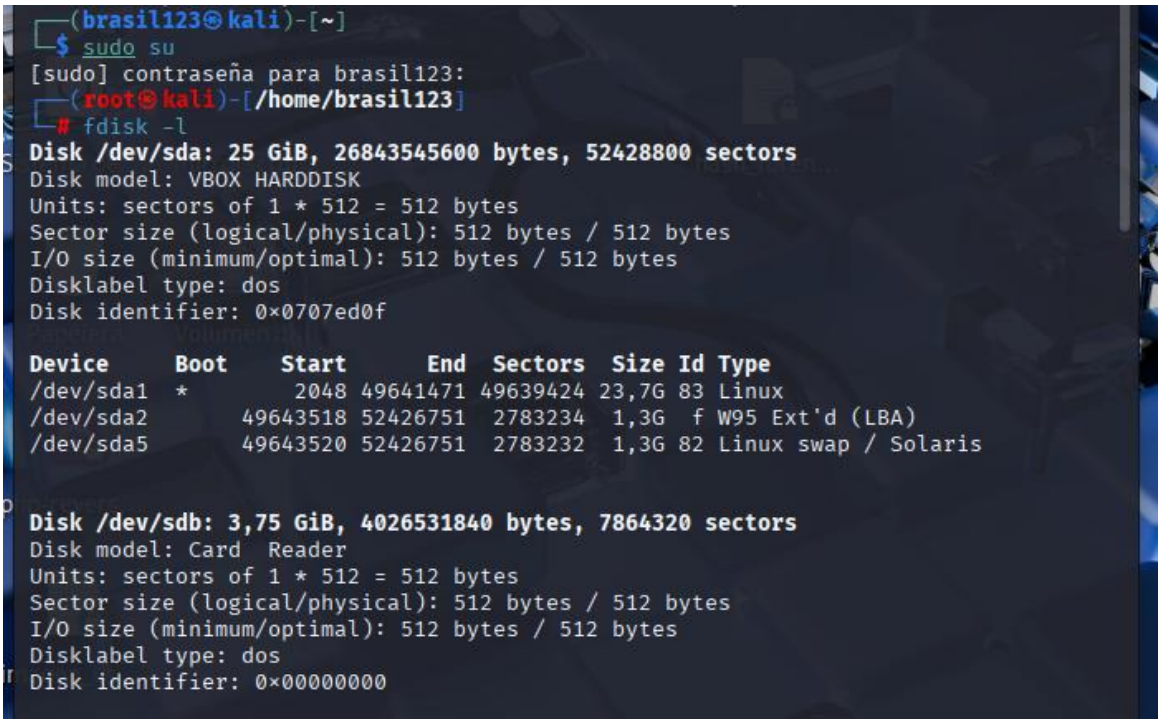

Ilustración 2. Identificación de discos

4.3 Generación de hash forense de la memoria USB

Con el comando **shalsum /dev/sdb > /home/brasil123/Escritorio/hash_forense.sha1** se calcula y guarda el hash SHA1 de toda la memoria USB en un archivo.

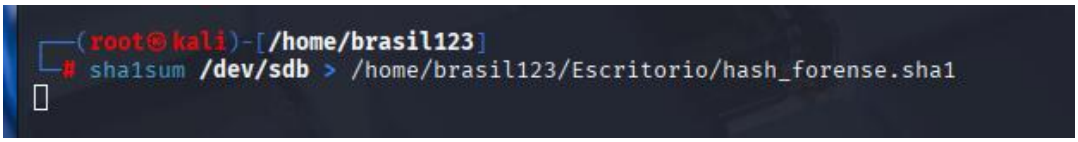

Ilustración 3. Generación de hash forense

4.4 Escritorio de Kali Linux con archivo forense

Vista del escritorio de Kali Linux mostrando el archivo generado durante el proceso forense.

Ilustración 4. Archivo hash forense

4.5 Verificación del hash forense generado

Contenido del archivo **hash_forense.sha1** mostrando el hash SHA1 de la memoria USB, que servirá para verificar la integridad de la evidencia.

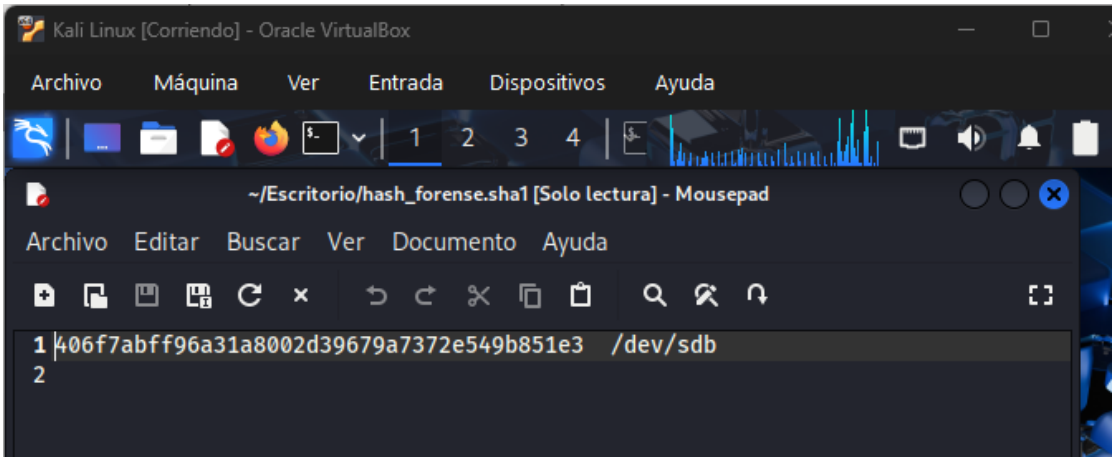

Ilustración 5. Verificación del hash forense generado

4.6 Creación de imagen forense con dd

Ejecutar **dd if=/dev/sdb of=/home/brasil123/Escritorio/imagen_usb_forense.dd** comando que crea una imagen forense bit-a-bit de toda la memoria USB.

```
┌──(root㉿kali)-[/home/brasil123]
└─# dd if=/dev/sdb of=/home/brasil123/Escritorio/imagen_usb_forense.dd conv=noer
ror,sync
7864320+0 records in
7864320+0 records out
4026531840 bytes (4,0 GB, 3,8 GiB) copied, 945,278 s, 4,3 MB/s
```

Ilustración 6. Creación de imagen forense

4.7 Verificación de integridad de la imagen forense

Usamos el comando **shalsum** a la imagen forense creada, confirmando que el hash SHA1 coincide exactamente con el original, validando la integridad de la imagen durante el proceso de análisis.

```
┌──(root㉿kali)-[/home/brasil123]
└─# sha1sum /home/brasil123/Escritorio/imagen_usb_forense.dd
406f7abff96a31a8002d39679a7372e549b851e3  /home/brasil123/Escritorio/imagen_usb_f
orense.dd
```

Ilustración 7. Verificación de integridad de la imagen forense

4.8 Propiedades del archivo de imagen forense

Haciendo clic derecho se pueden ver las opciones disponibles para el archivo de imagen forense, incluyendo ver propiedades.

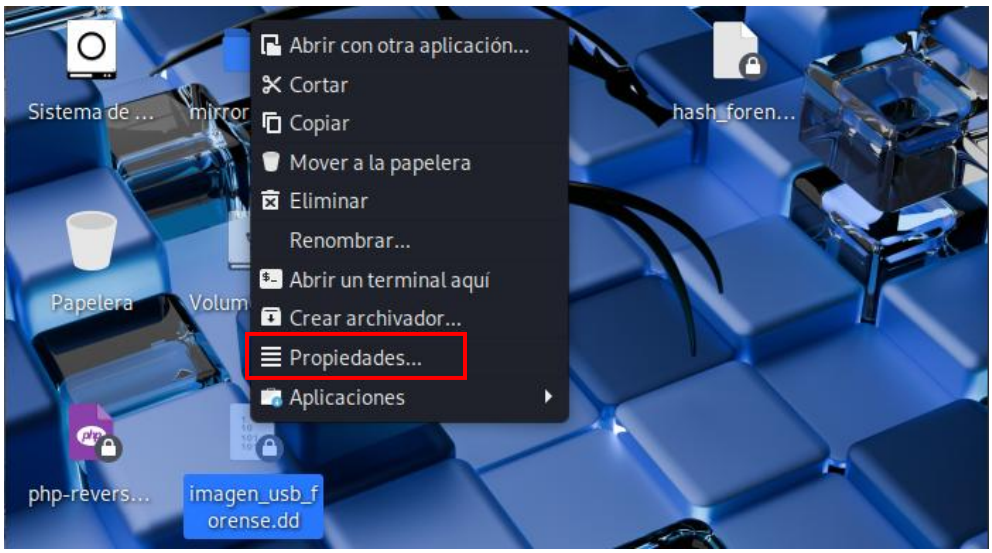

Ilustración 8. Ver propiedades de la imagen forense

Ventana de propiedades del archivo **imagen_usb_forense.dd** mostrando que tiene un tamaño de 3.8 GB, confirmando que se capturó completamente el contenido de la memoria USB.

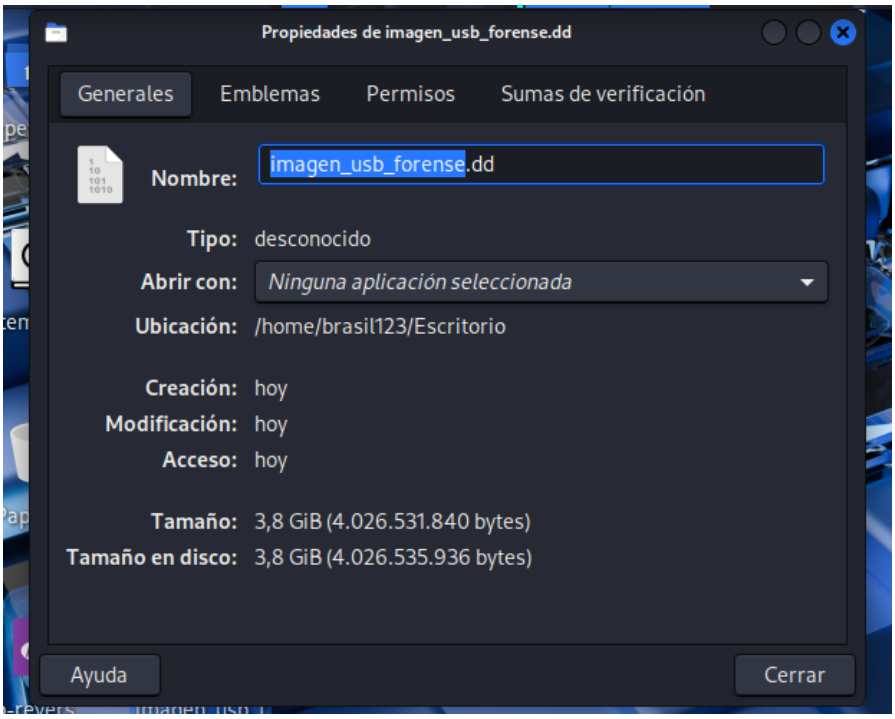

Ilustración 9. Propiedades de la imagen forense

4.9 Menú de aplicaciones de Kali Linux

En el nenú de aplicaciones de Kali Linux buscar Autopsy, que será utilizada para el análisis de la evidencia.

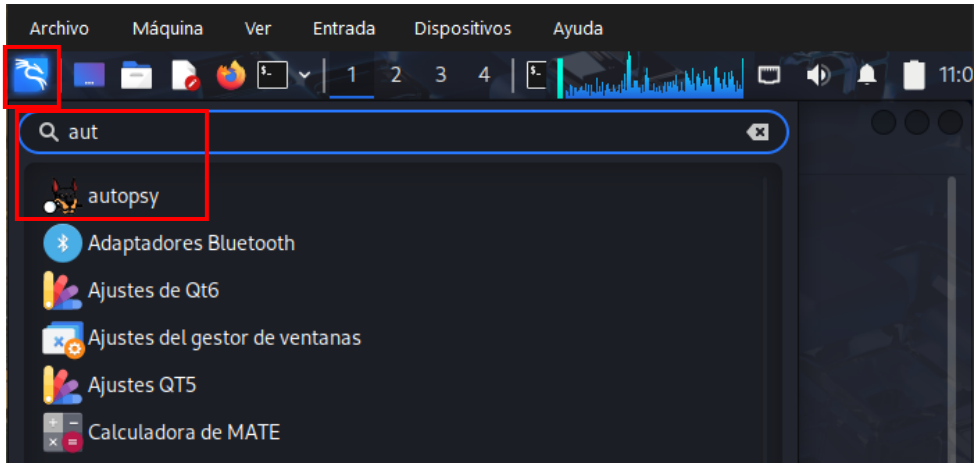

Ilustración 10. Menú de aplicaciones de Kali Linux

4.10 Inicio de Autopsy desde terminal

Terminal de Kali Linux mostrando la ejecución del comando **sudo autopsy** para iniciar la herramienta de análisis forense Autopsy. Posteriormente ingresar la contraseña de nuestro Kali.

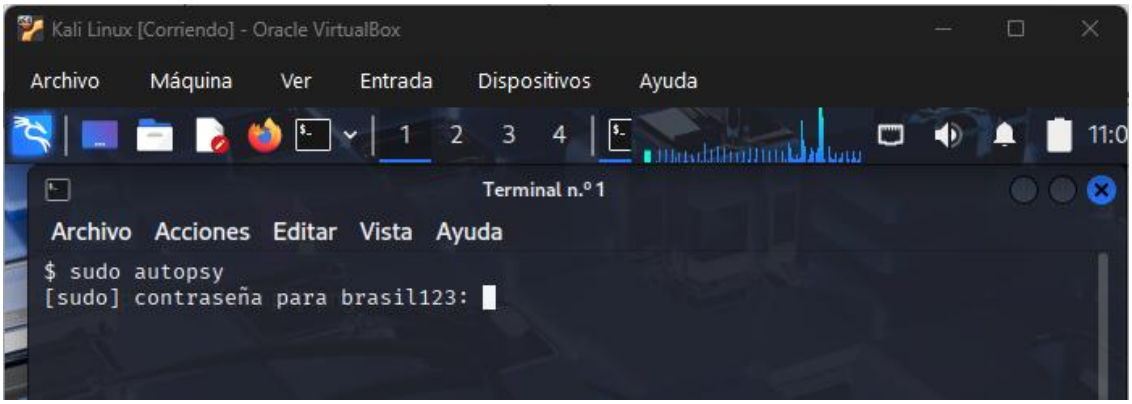

Ilustración 11. Inicio de Autopsy

Confirmación de que el servicio Autopsy se ha iniciado correctamente en el puerto 9999, proporcionando la URL **http://localhost:9999/autopsy** para acceder a la interfaz web.

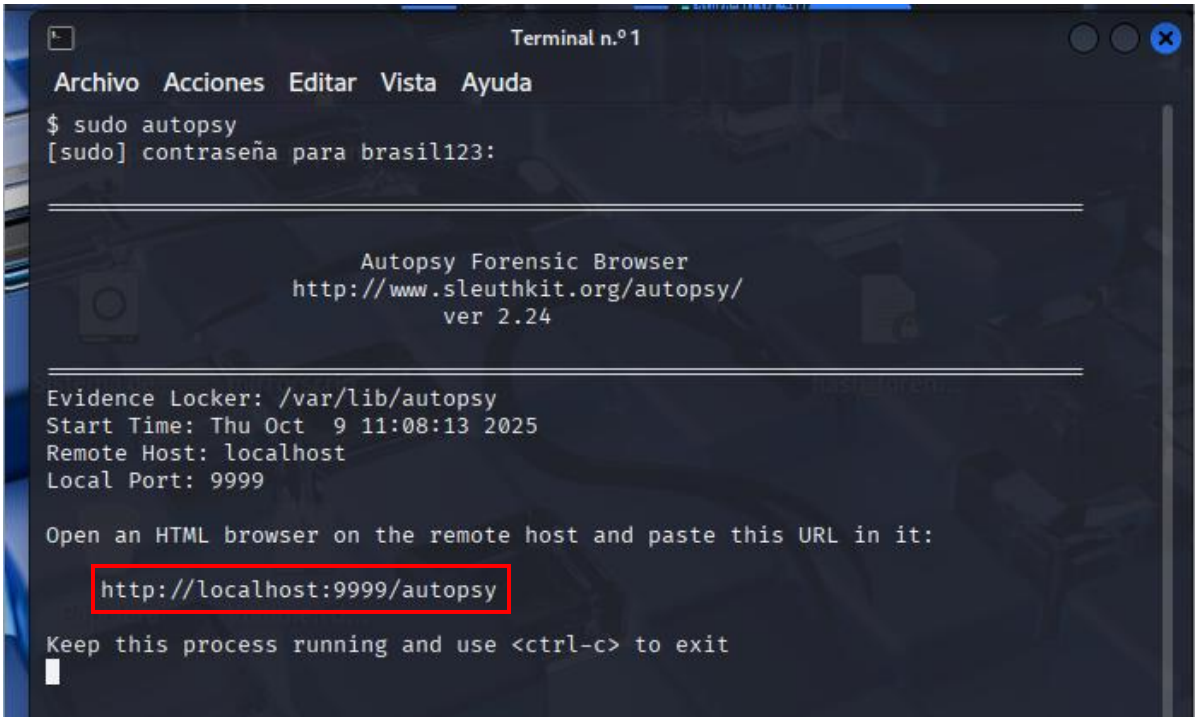

Ilustración 12. Servicio Autopsy iniciado correctamente

4.11 Interfaz web de Autopsy Forensic Browser

En el navegador de Kali Linux ingresamos la URL que nos proporcionó el servicio de Autopsy. Una vez hecho podemos ver la pantalla de advertencia inicial de Autopsy sobre JavaScript, seguida de la pantalla principal de la herramienta forense lista para comenzar el análisis haciendo clic en el link http que se muestra abajo del dibujo.

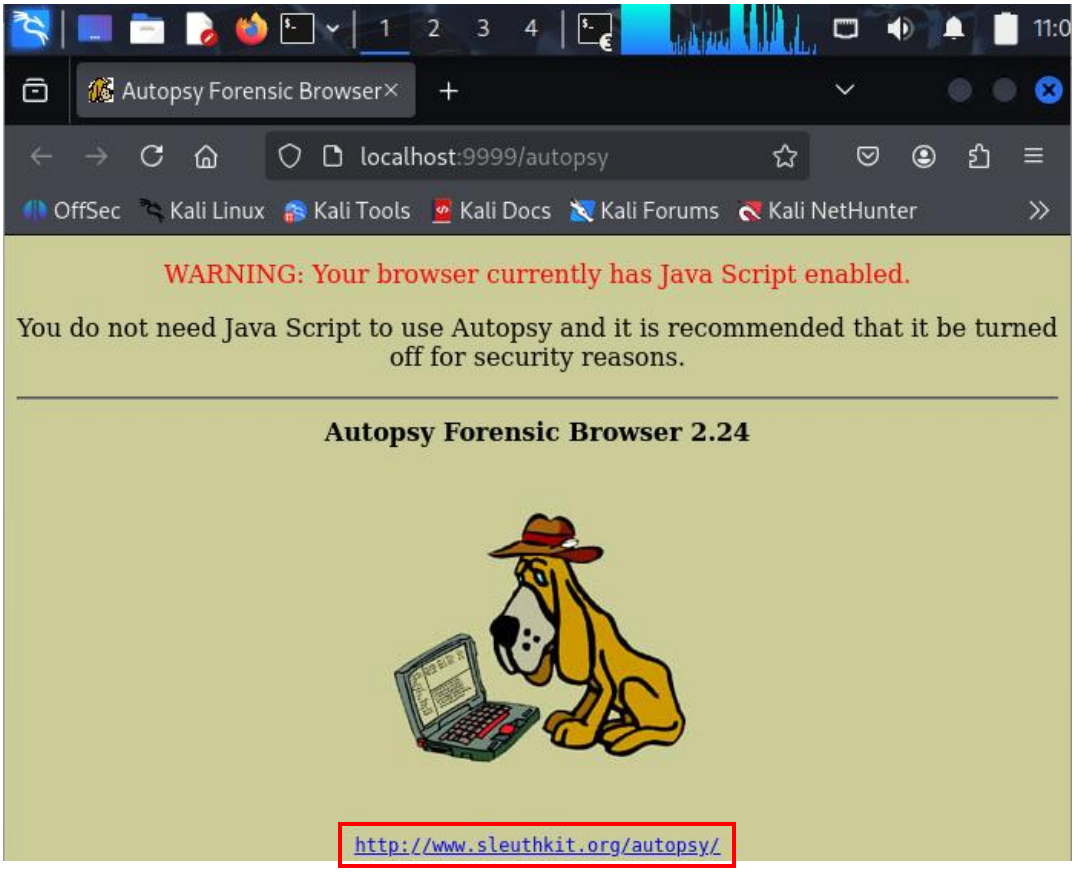

Ilustración 13. Interfaz web de Autopsy

4.12 Creación de nuevo caso forense

Ahora veremos un formulario para crear un nuevo caso forense, le pondremos el nombre de "miPrimerCaso1" con descripción "Analisis Forense USB Clase" y los investigadores Indira_Florez y Rosa_Elvira. Una vez llenados los campos damos clic en **“New Case”.**

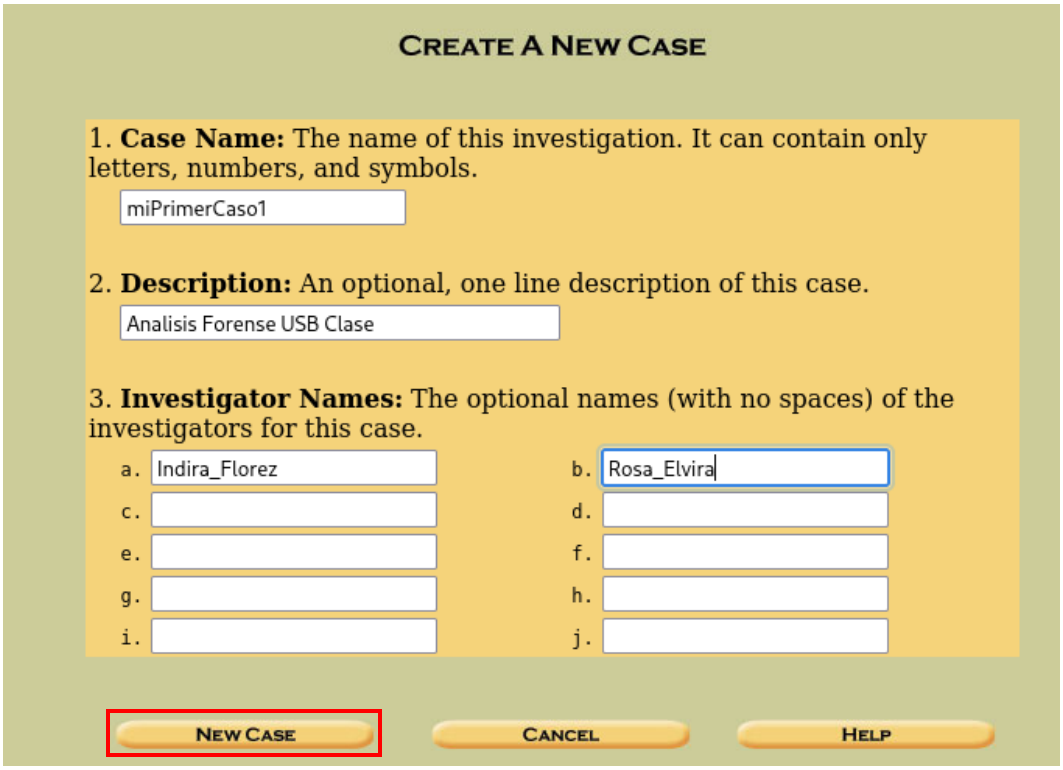

Ilustración 14. Creación de nuevo caso forense

Mensaje de confirmación de que el caso **"miPrimerCaso1"** ha sido creado exitosamente, procediendo a la creación del host para el análisis haciendo clic en **"Add Host".**

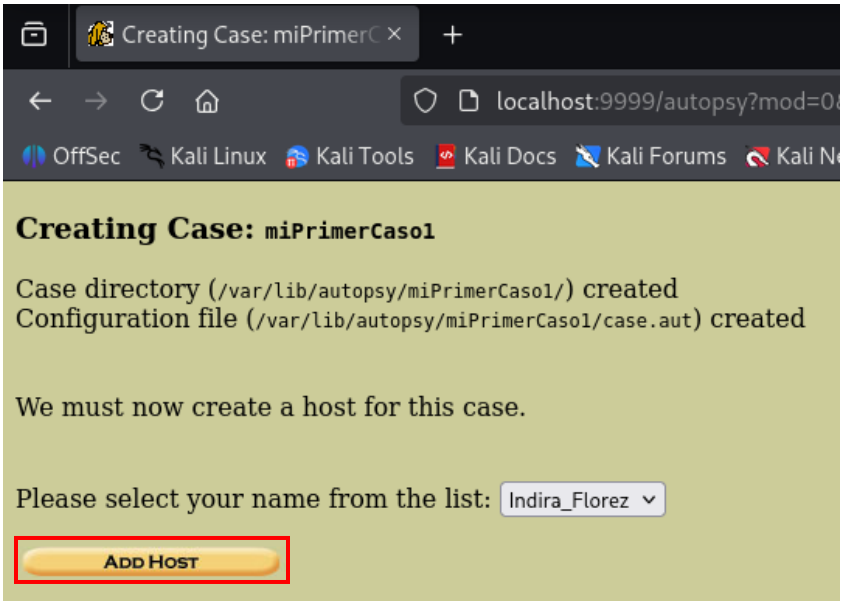

Ilustración 15. Confirmación de creación del caso

Formulario para agregar un nuevo host el cual llevará el nombre de "MVKaliPIT11" con descripción "Portatil_HP" que representará el sistema bajo investigación.

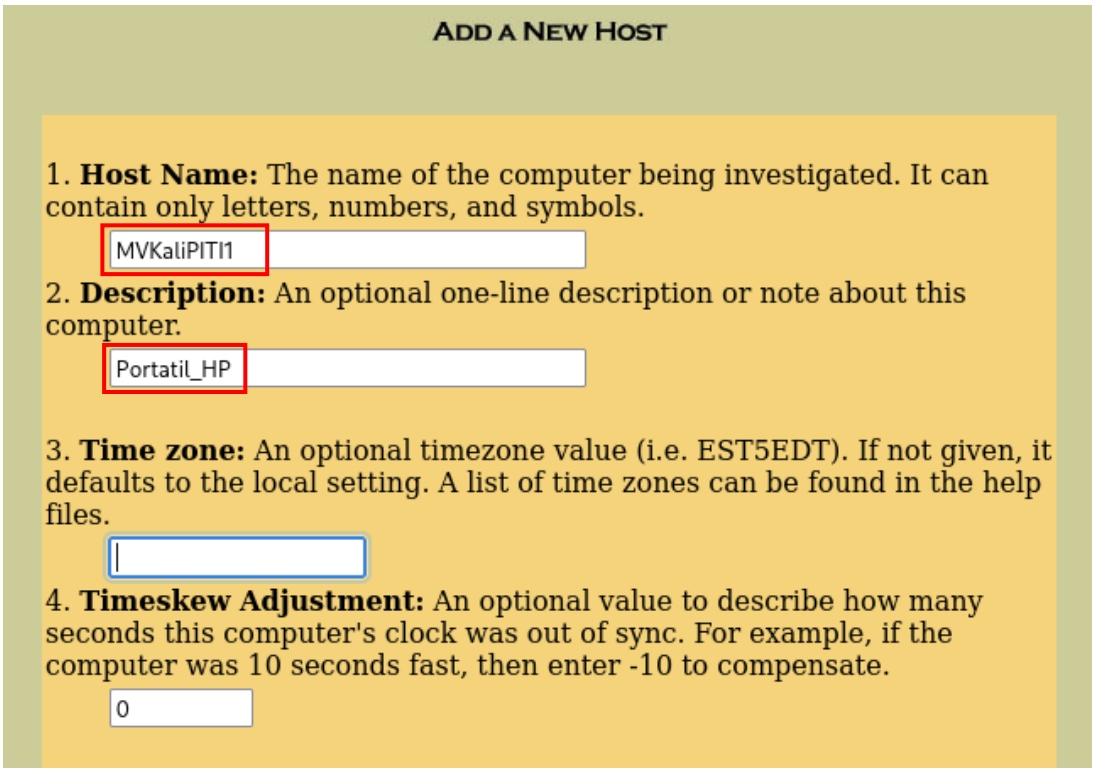

Ilustración 16. Configuración de nuevo host forense

Confirmación de que el host "MVKaliPIT11" ha sido agregado al caso, procediendo a importar la imagen forense para análisis haciendo clic en **"Add Image"**.

Ilustración 17. Host creado exitosamente

Pantalla del host recién creado mostrando que no hay imágenes agregadas aún, hacemos clic en el botón **"ADD IMAGE FILE"** para importar la evidencia.

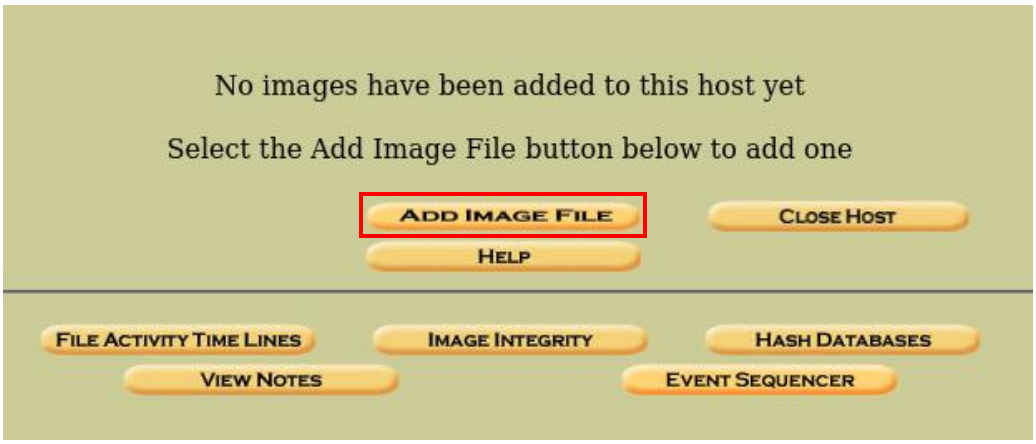

Ilustración 18. Interfaz de gestión de host sin imágenes

4.13 Asignación de permisos a la imagen forense

En una nueva terminal de Kali Linux en el modo superusuario ejecutamos el comando **chmod 777** sobre la imagen forense para asegurar que Autopsy tenga los permisos necesarios para acceder al archivo.

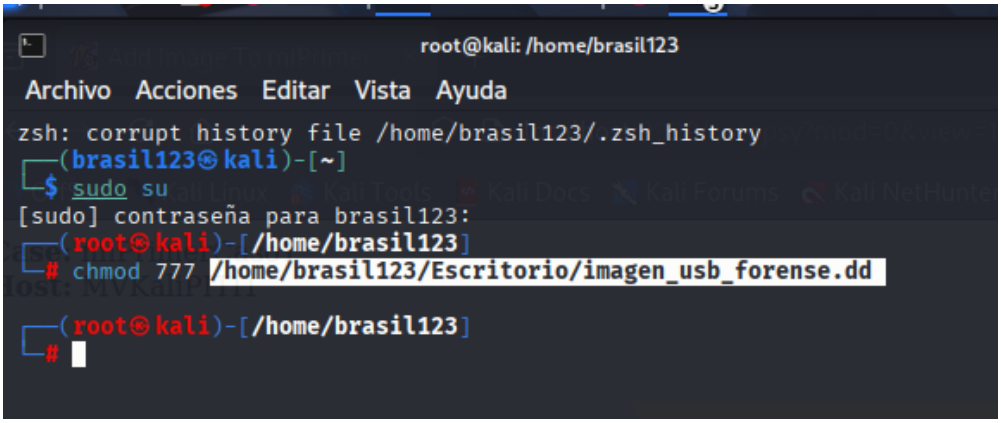

Ilustración 19. Permisos a la imagen forense

4.14 Configuración de importación de imagen forense

Formulario de Autopsy para importar la imagen forense, especificando la ruta de la imagen, seleccionando tipo "Disk" y método "Symlink". Luego damos clic en **“Next”.**

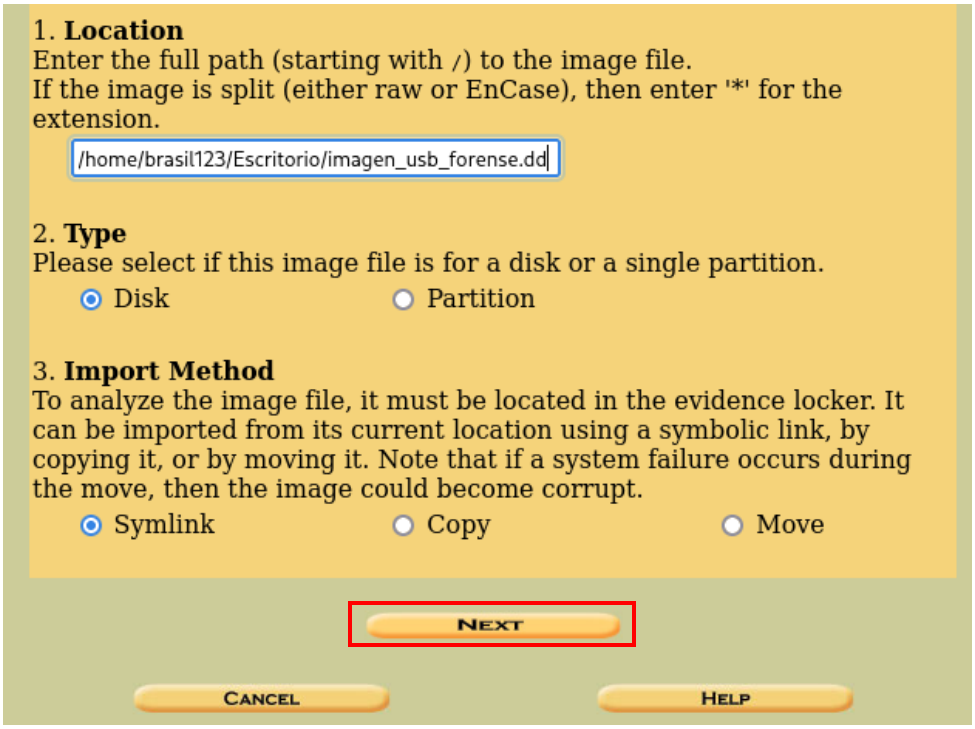

Ilustración 20. Importando imagen forense

Pantalla que muestra los detalles de la imagen importada, incluyendo la partición FAT32 identificada y el rango de sectores (32 to 7864319). Luego hacemos clic en **"Add".**

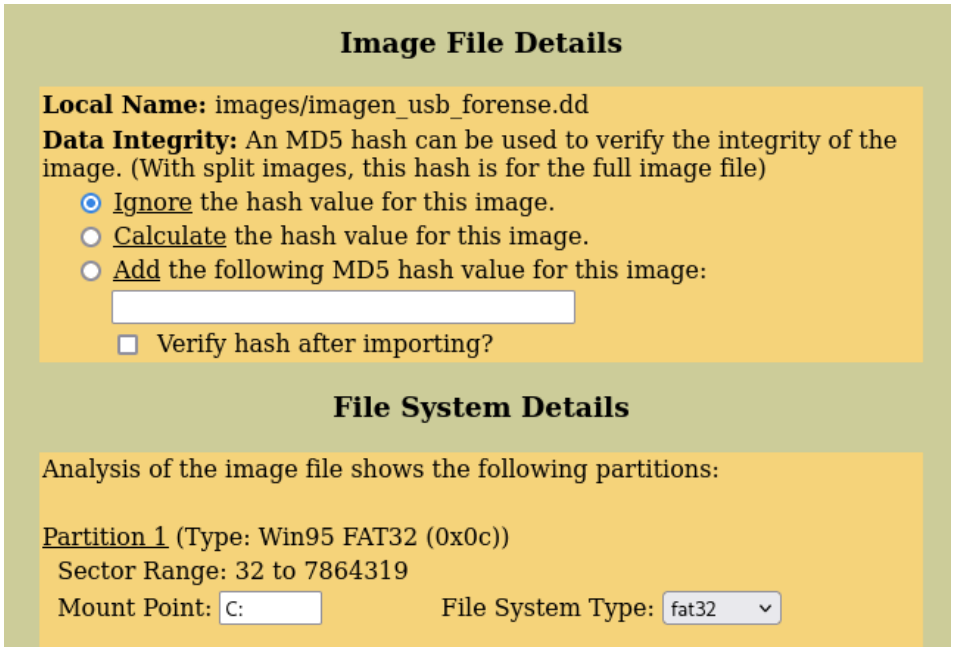

Ilustración 21. Detalles de la imagen forense importada

Mensaje de confirmación de que la imagen forense ha sido agregada exitosamente con ID img1, y los volúmenes correspondientes han sido identificados.

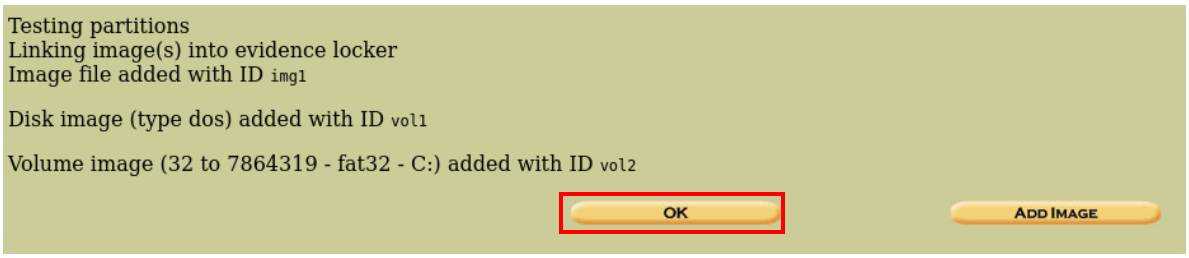

Ilustración 22. Confirmación de imagen agregada exitosamente

4.15 Módulo de análisis de archivos en Autopsy

Pantalla principal de Autopsy mostrando los volúmenes disponibles para análisis: el disco completo y la partición FAT32, listos para ser analizados.

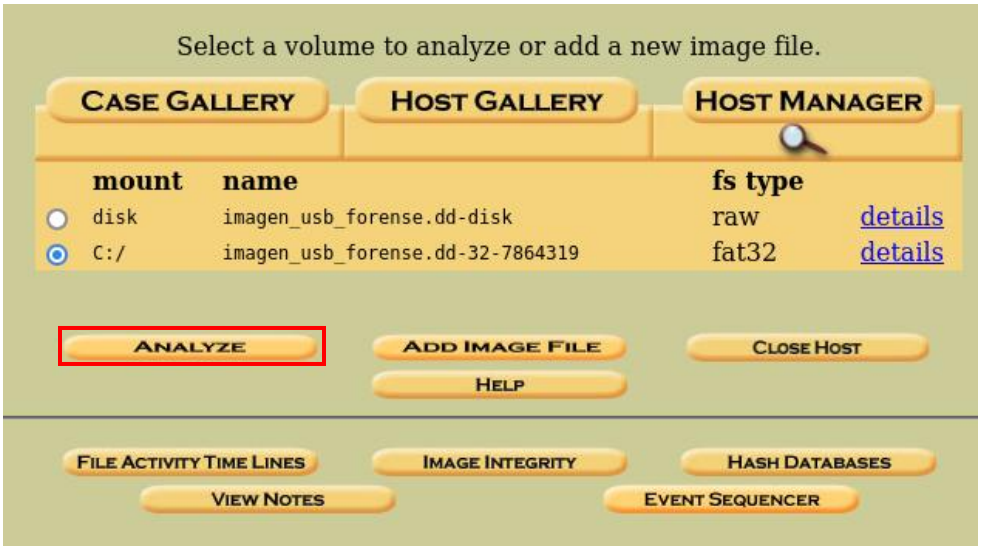

Ilustración 23. Interfaz principal de análisis forense

Esta imagen muestra la interfaz del módulo de Análisis de Archivos (File Analysis), donde se explora el contenido de la memoria USB previamente capturada. Se muestra los archivos recuperados de la imagen forense, también una lista detallada de todos los archivos existentes en la ubicación seleccionada, incluyendo sus nombres, tamaños, fechas de modificación y tipos.

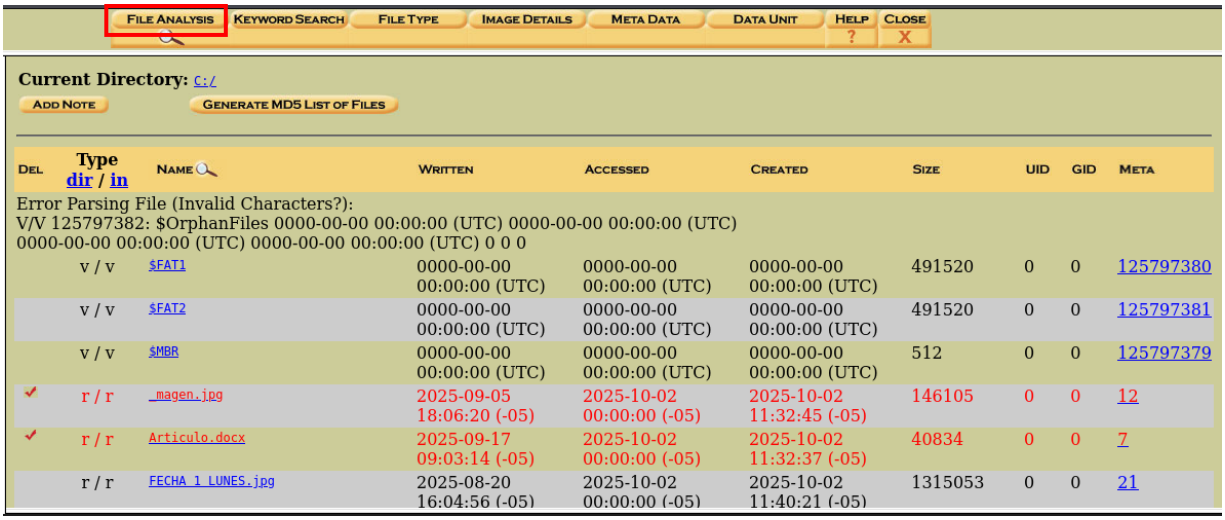

Ilustración 24. Módulo de análisis de archivos en Autopsy

En la sección inferior, la herramienta muestra una vista previa en miniatura de la imagen seleccionada y proporciona detalles técnicos del tipo de archivo, identificando correctamente el formato JPEG con metadatos EXIF que incluyen información sobre el fabricante (Apple), resolución y software de creación.

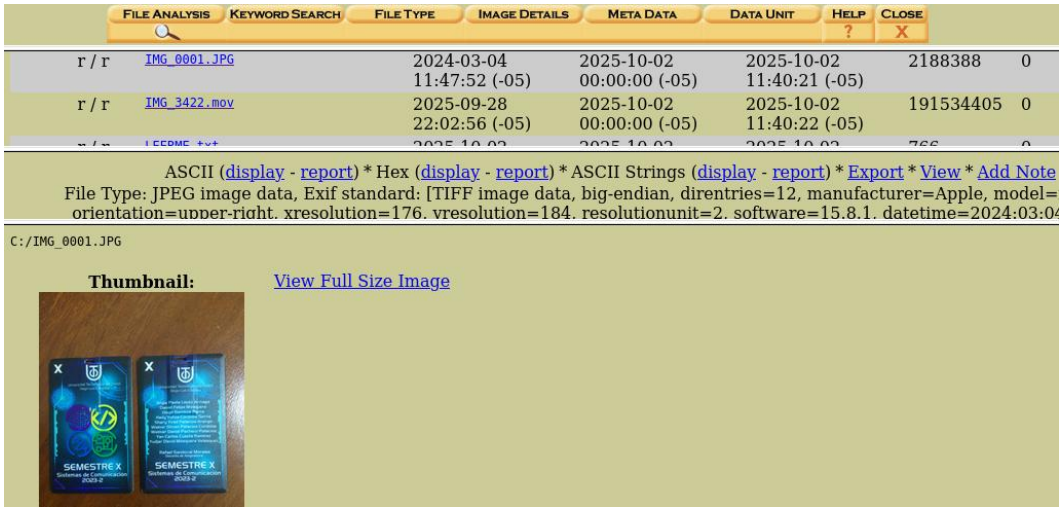

Ilustración 25. Análisis detallado de archivos

4.16 Cálculo de hash MD5 para verificación de integridad

Pantalla principal de Autopsy mostrando los volúmenes disponibles para análisis

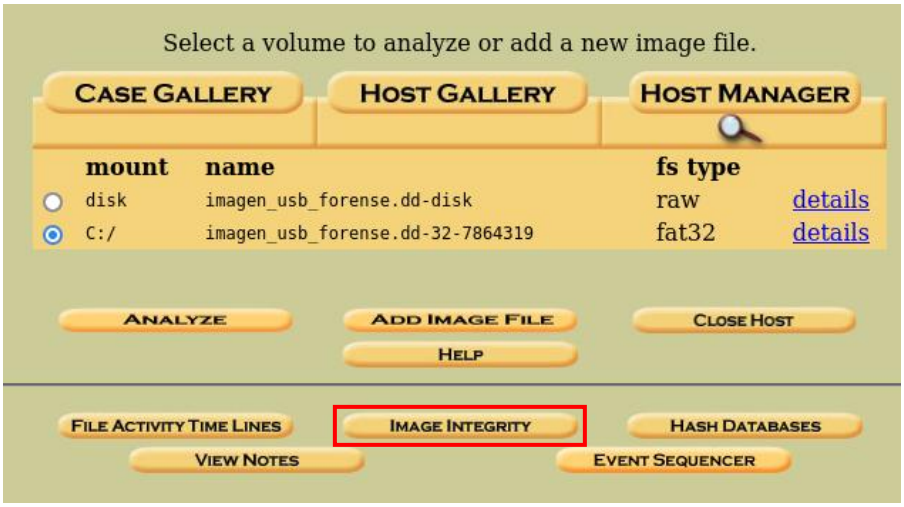

Ilustración 26. Interfaz principal de gestión de volúmenes en Autopsy

Proceso de cálculo de hash MD5 para la imagen forense **"imagen_usb_forense.dd".** Autopsy muestra una ventana de progreso indicando que está realizando el cálculo criptográfico.

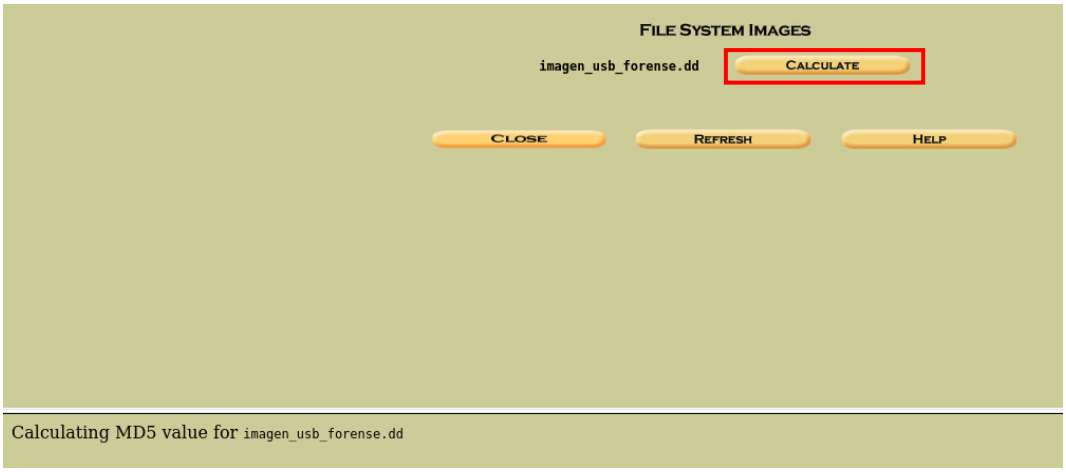

Ilustración 27. Cálculo de hash MD5

Resultado exitoso del cálculo de hash MD5, generando el valor único. El sistema confirma que el hash ha sido guardado en el archivo del host.

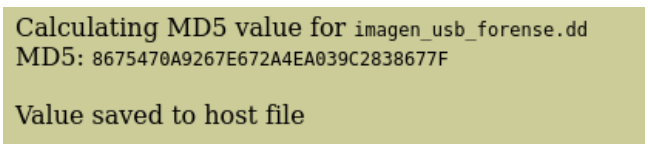

Ilustración 28. Hash MD5 calculado y almacenado exitosamente

Volvemos a la interfaz del módulo de Análisis de Archivos que tiene la opción para generar listas MD5 de archivos y damos clic en ella.

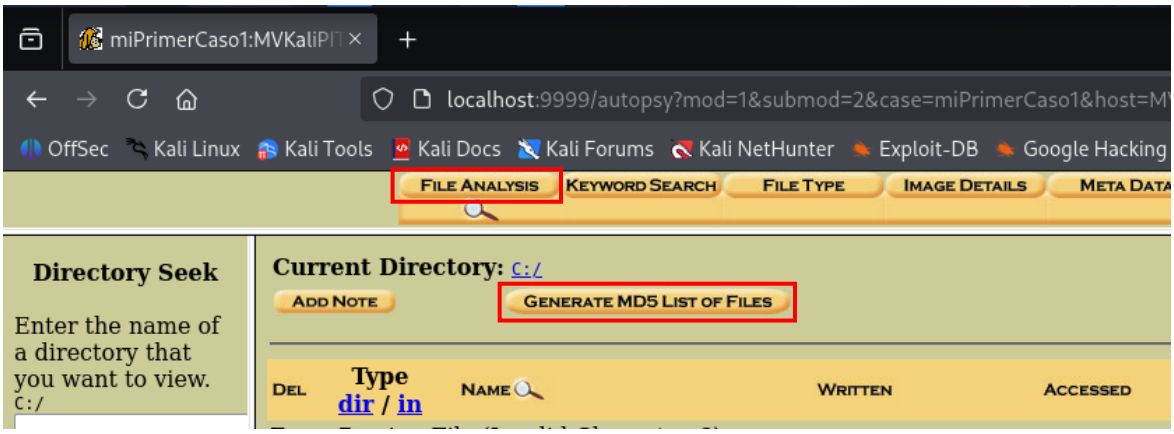

Ilustración 29. Generar listas MD5 de archivos

Resultados de la generación de hashes MD5 para los archivos específicos contenidos en la memoria USB. Se listan los valores hash únicos para cada archivo recuperado, incluyendo documentos importantes y archivos multimedia.

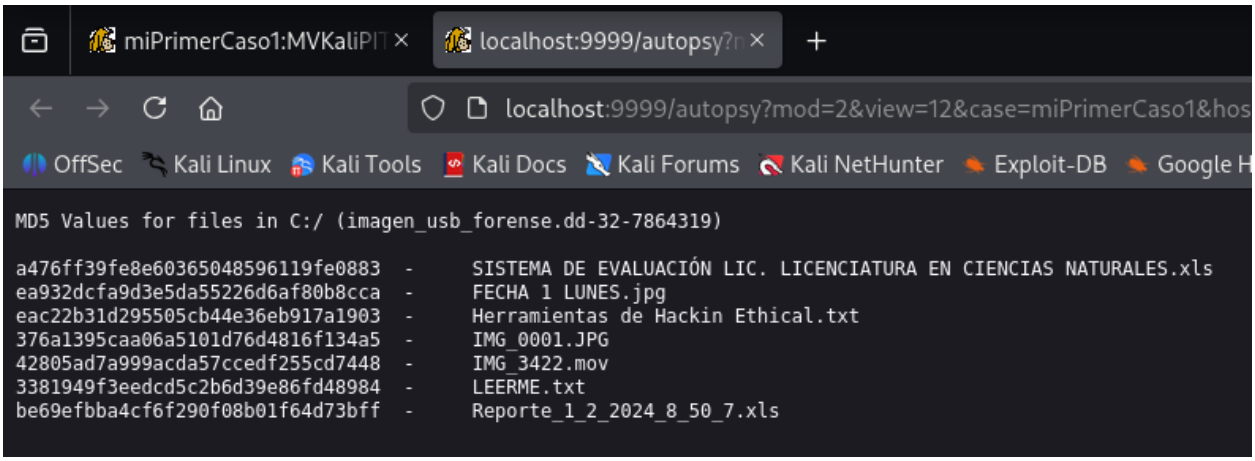

Ilustración 30. Hashes MD5 de archivos específicos recuperados

5. CAPITULO 2 - INSTALACIÓN Y ANALISIS FORENSE CON AUTOPSY EN WINDOWS

5.1 Búsqueda en Google de Autopsy para Windows

Se inició el procedimiento realizando una búsqueda en el navegador web con el término "**autopsy win**". El resultado principal dirigió a la página oficial de descarga de Autopsy.

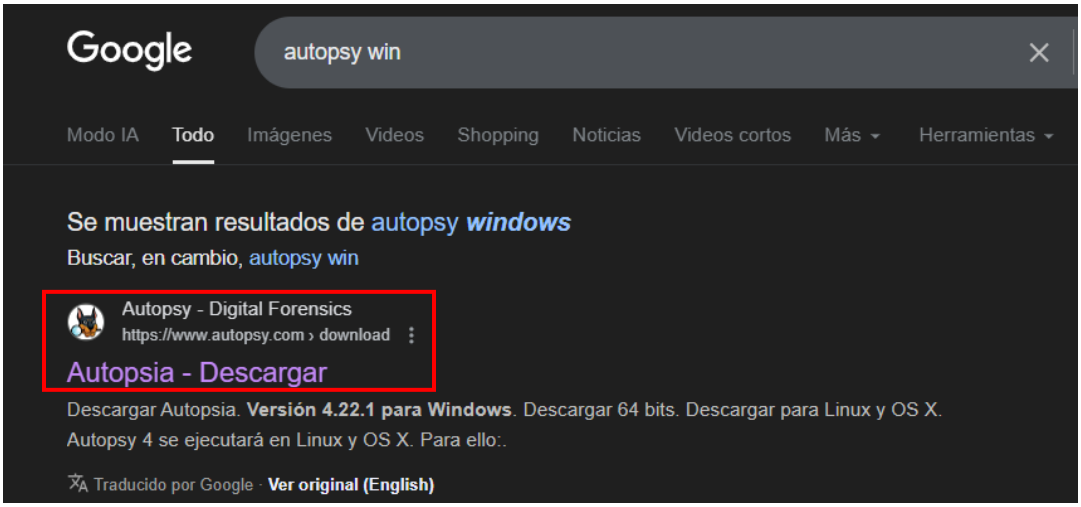

Ilustración 31. Búsqueda del Software

5.2 Página oficial de descarga de Autopsy

En la página web oficial de Autopsy, se seleccionó la versión 4.22.1 para Windows de 64 bits y se procedió a hacer clic en el enlace de descarga.

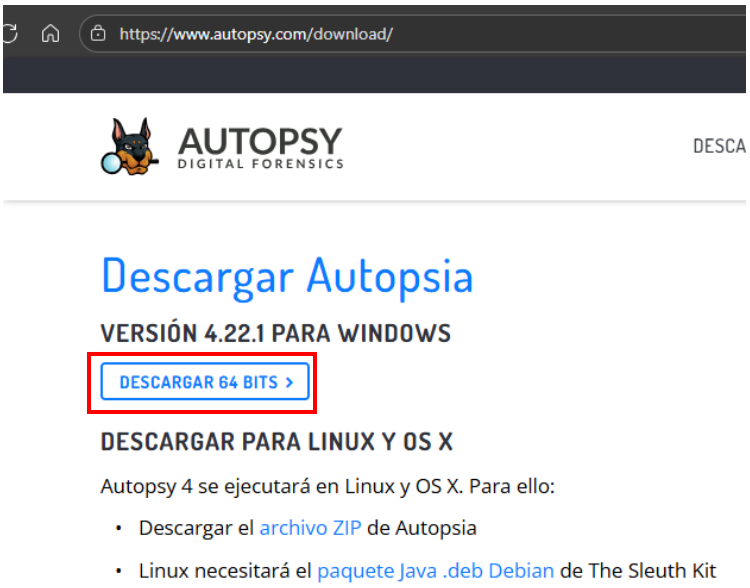

Ilustración 32. Descarga desde la Página Oficial

5.3 Diálogo de descarga del archivo de instalación

El navegador mostró un cuadro de diálogo preguntando qué acción realizar con el archivo "autopsy-4.22.1-64bit (1).msi". Se eligió la opción "Guardar" para descargar el instalador en el sistema.

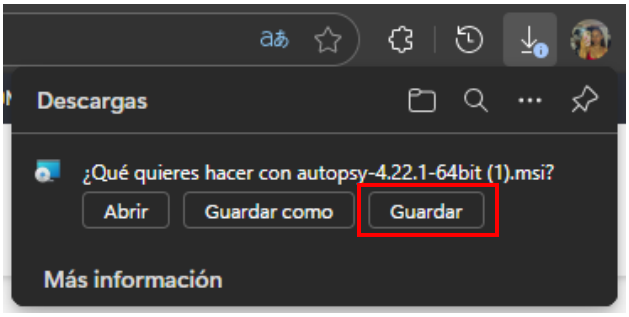

Ilustración 33. Confirmación de Descarga

5.4 Gestor de descargas del sistema

Se accedió a la carpeta **"Descargas"** del sistema para verificar que el archivo "autopsy-4.22.1-64bit (1).msi" se había descargado correctamente.

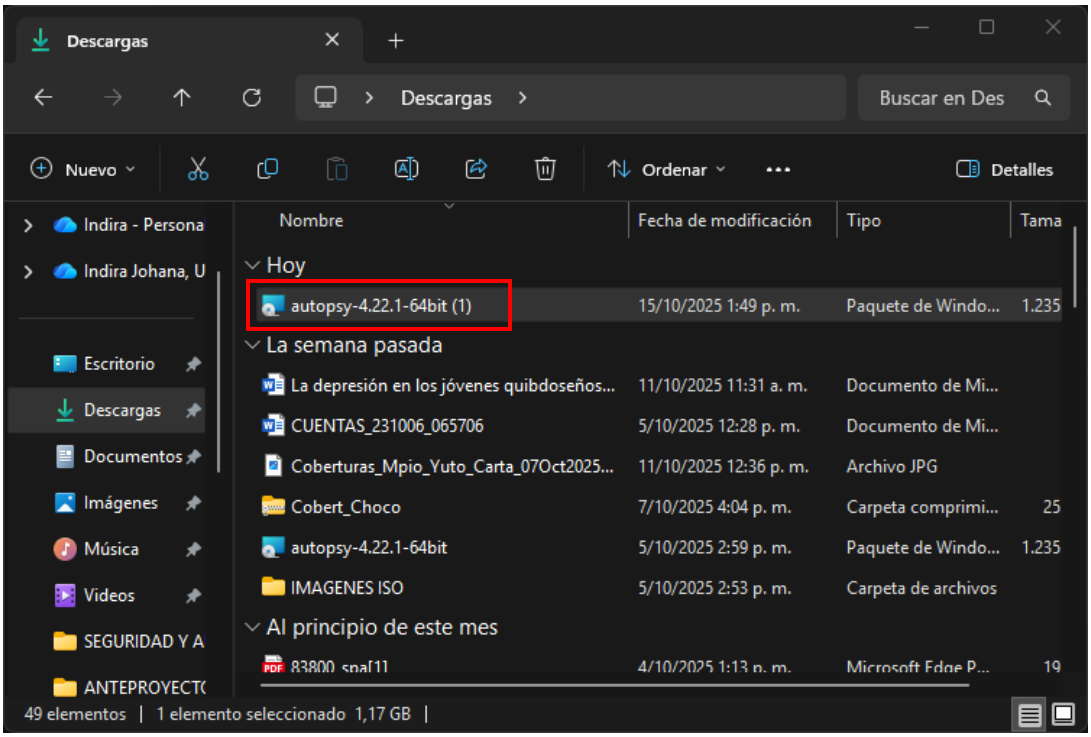

Ilustración 34. Verificación del Archivo Descargado

5.5 Instalación de Autopsy en Windows

Se ejecutó el archivo descargado, lo que abrió el Asistente de Instalación de Autopsy. En esta ventana de bienvenida, se hizo clic en "Next" para comenzar el proceso de instalación.

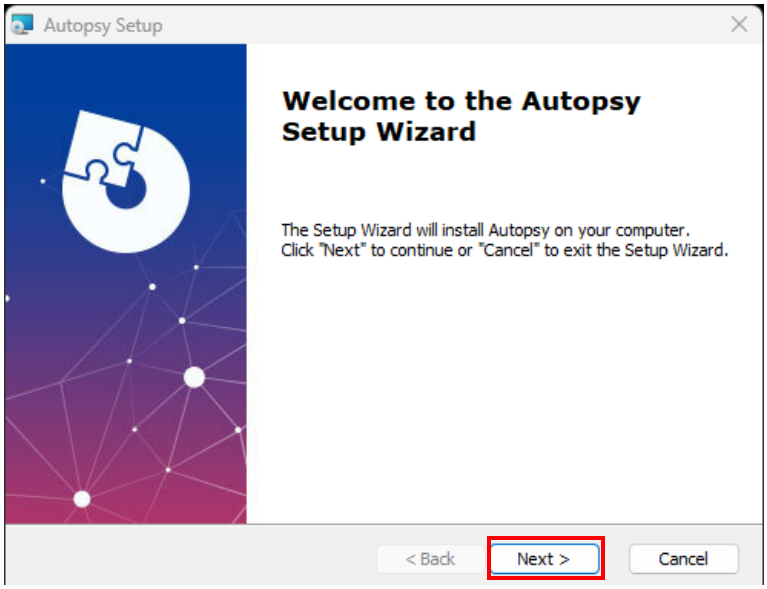

Ilustración 35. Inicio del Asistente de Instalación

El asistente presentó la opción de seleccionar la carpeta de instalación. Se mantuvo la ruta por defecto ("C:\Program Files\Autopsy-4.22.1") y se hizo clic en "Next" para continuar.

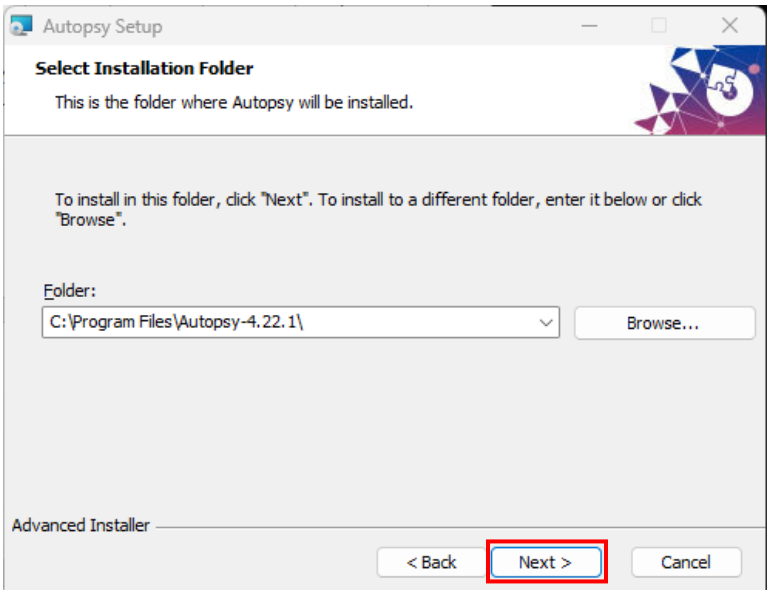

Ilustración 36. Selección de la Carpeta de Destino

En la ventana "Ready to Install", se hizo clic en el botón "Instalar" para iniciar la copia de archivos y la configuración del software.

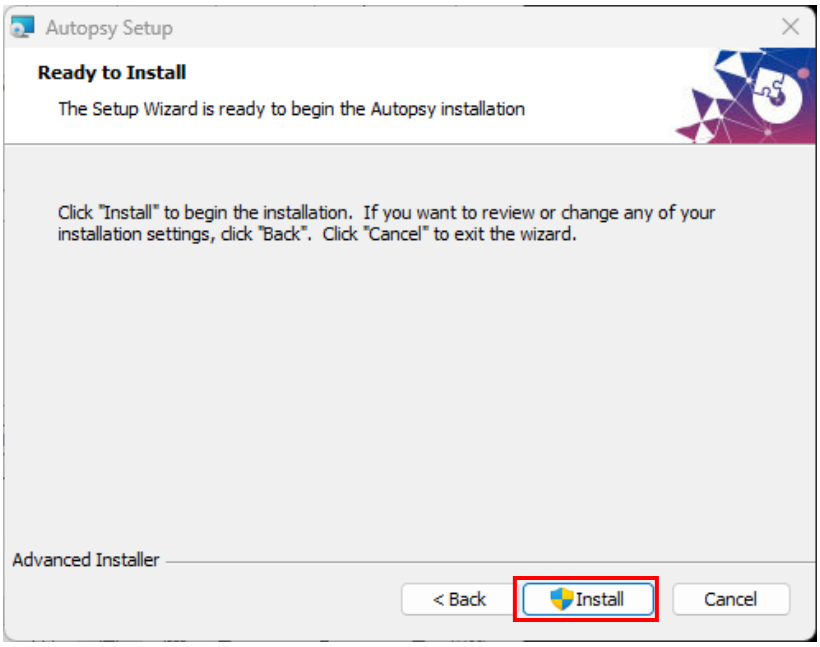

Ilustración 37. Confirmación para Instalar

Se esperó a que el proceso se completara.

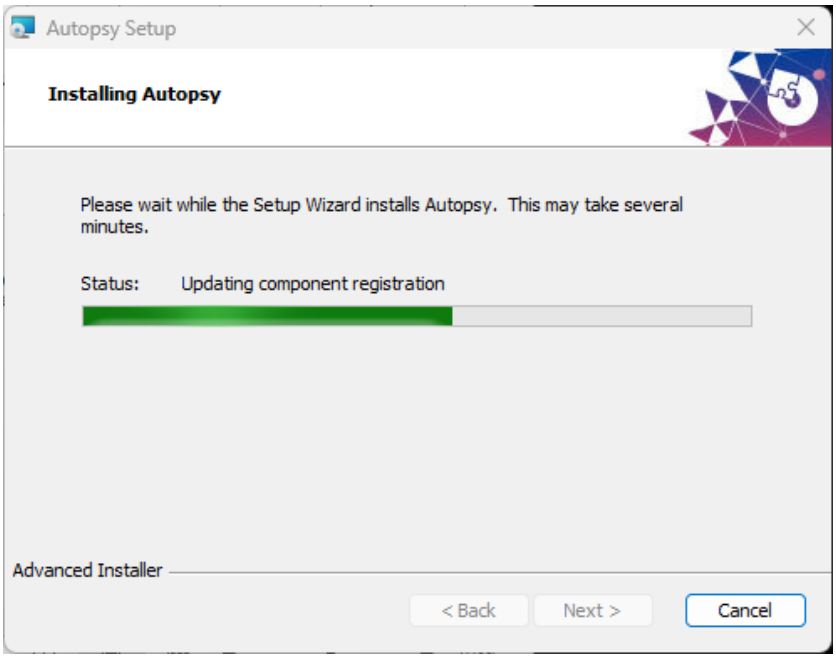

Ilustración 38. Proceso de Instalación en Curso

Al concluir el proceso, el asistente mostró la ventana "Completando el Asistente de Instalación de Autopsy". Se hizo clic en el botón **"Finalizar"** para salir del wizard.

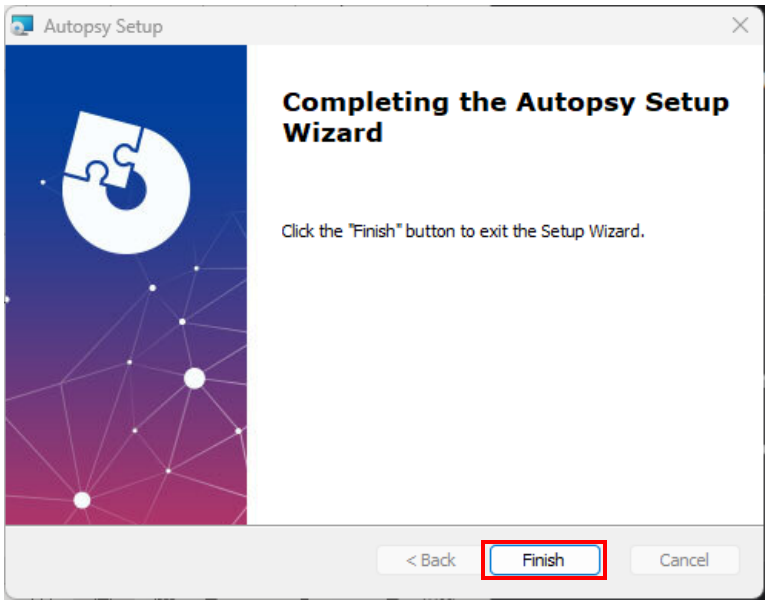

Ilustración 39. Finalización de la Instalación

5.6 Acceso directo de Autopsy en el escritorio

Como evidencia final de una instalación exitosa, se verificó que el acceso directo de "Autopsy 4.22.1" estaba disponible en el escritorio, listo para ser ejecutado.

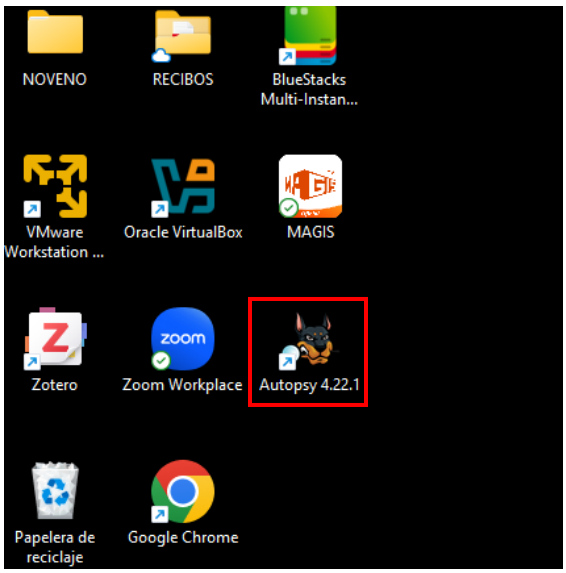

Ilustración 40. Software Instalado y Accesible

5.7 Inicio de Autopsy y Carga de Módulos

Se ejecutó la aplicación Autopsy, mostrando la pantalla inicial con el lema "OPEN EXTENSIBLE FAST". La aplicación inició el proceso de carga y activación de sus módulos de análisis forense.

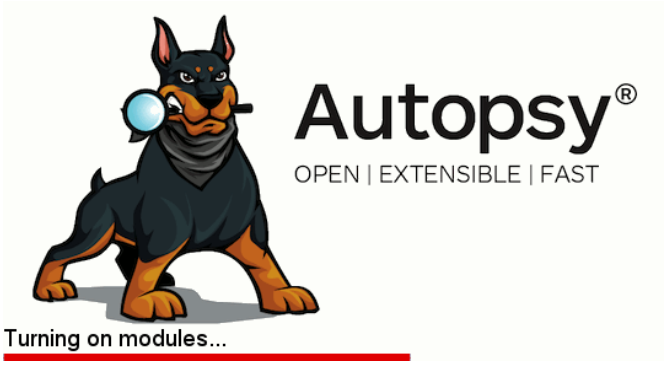

Ilustración 41. Inicio de Autopsy

Al abrir Autopsy, se presentó la ventana principal de bienvenida con las opciones para crear un nuevo caso **"New Case",** abrir un caso reciente **"Open Recent Case"** o abrir un caso existente **"Open Case".**

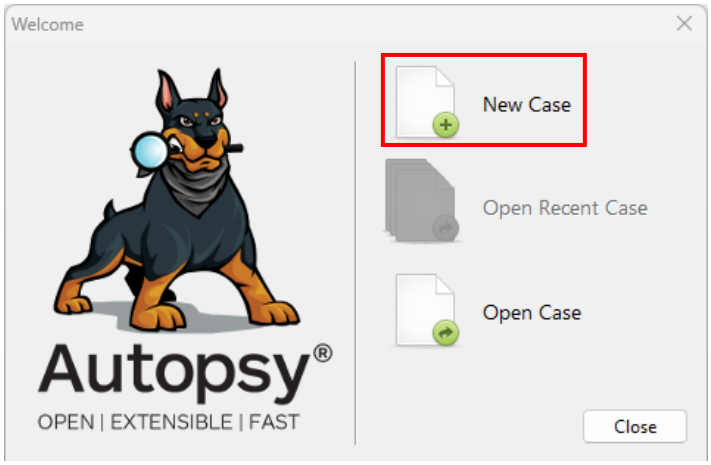

Ilustración 42. Ventana Principal de Bienvenida

Se seleccionó **"New Case"** y se procedió a llenar la información básica del caso. Se definió el nombre del caso y el directorio base donde se almacenarían los datos, manteniendo la opción "Single-User" seleccionada.

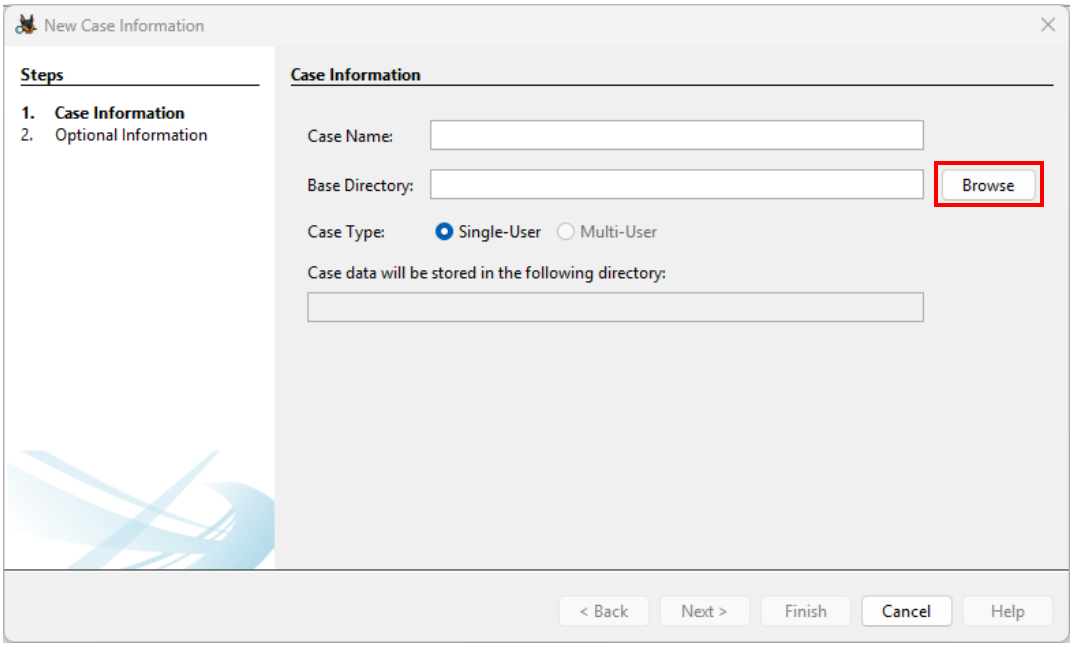

Ilustración 43. Creación de Nuevo Caso - Información Básica

Al hacer clic en "**Browse**" para seleccionar el directorio base, se abrió una ventana de navegación de archivos mostrando las unidades y carpetas disponibles en el sistema, incluyendo el disco local (C:).

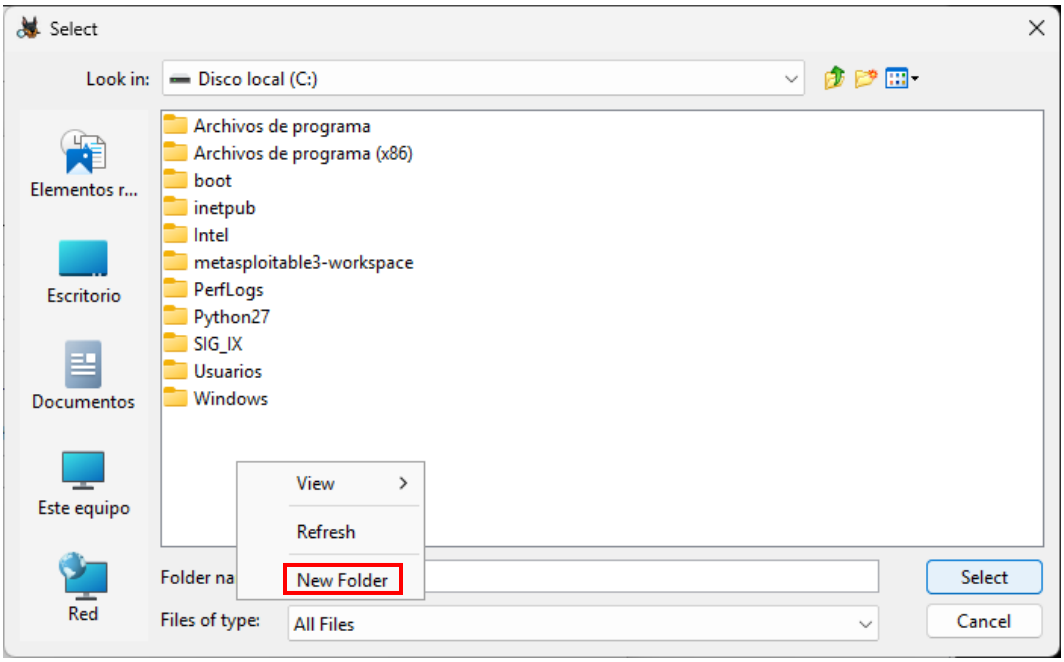

Ilustración 44. Navegación para Seleccionar Directorio

En la ventana de navegación, se creó la carpeta **"Analisis_Forense"** como ubicación para almacenar todos los datos relacionados con el caso forense, haciendo clic derecho y seleccionando la opción **"New Folder"** para crear la carpeta.

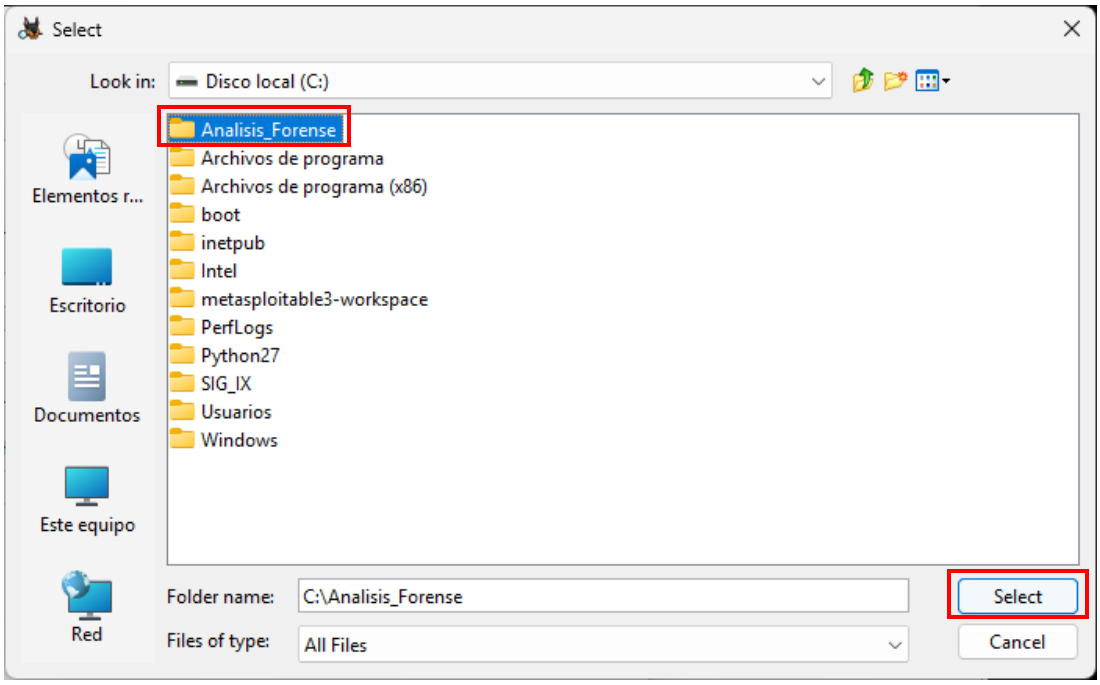

Ilustración 45. Creación de la Carpeta de Análisis Forense

Se verificó y confirmó la información del caso creado, mostrando el nombre **"MiPrimerCaso"** y la ruta de almacenamiento **"C:\Analisis_Forense\MiPrimerCaso".**

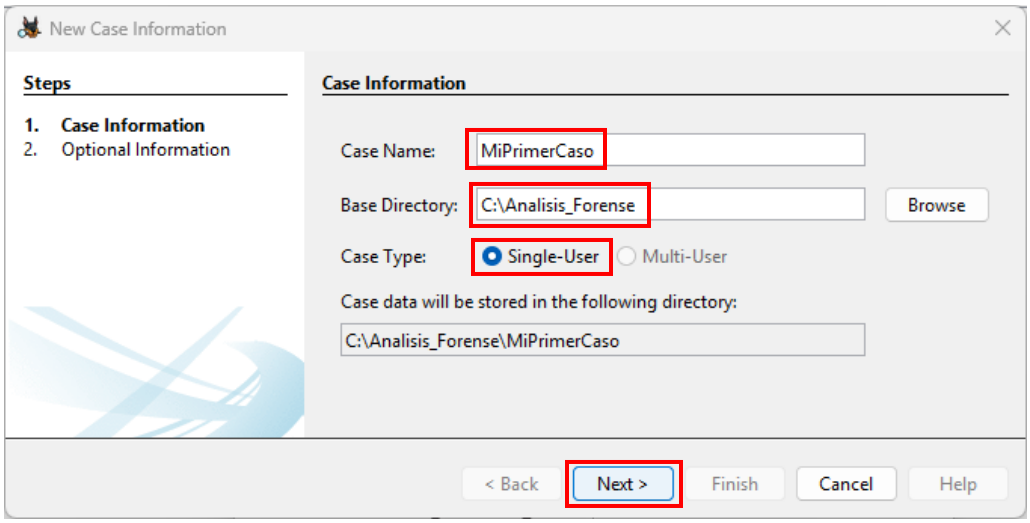

Ilustración 46. Confirmación de Información del Caso

Se completó la información opcional del examinador, incluyendo nombre, teléfono, correo electrónico y notas del caso. También se asignó un número de caso (01) para fines de documentación y trazabilidad.

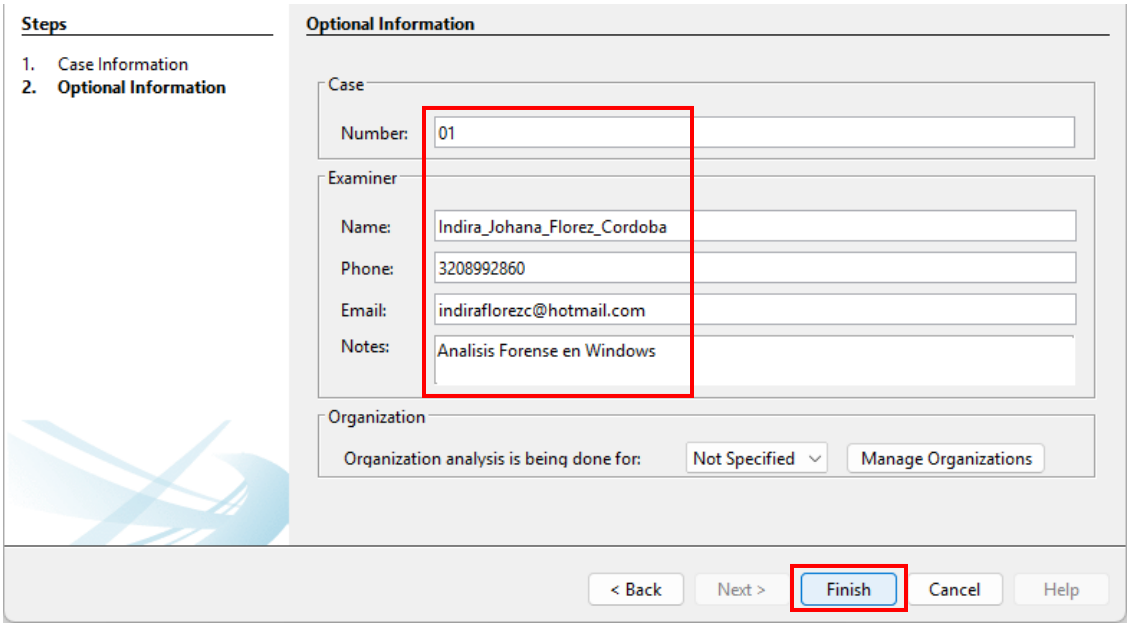

Ilustración 47. Información Opcional del Examinador

Al agregar una fuente de datos, se configuró la opción de host seleccionando **"Generate new host name based on data source name"** para organizar los datos dentro del caso.

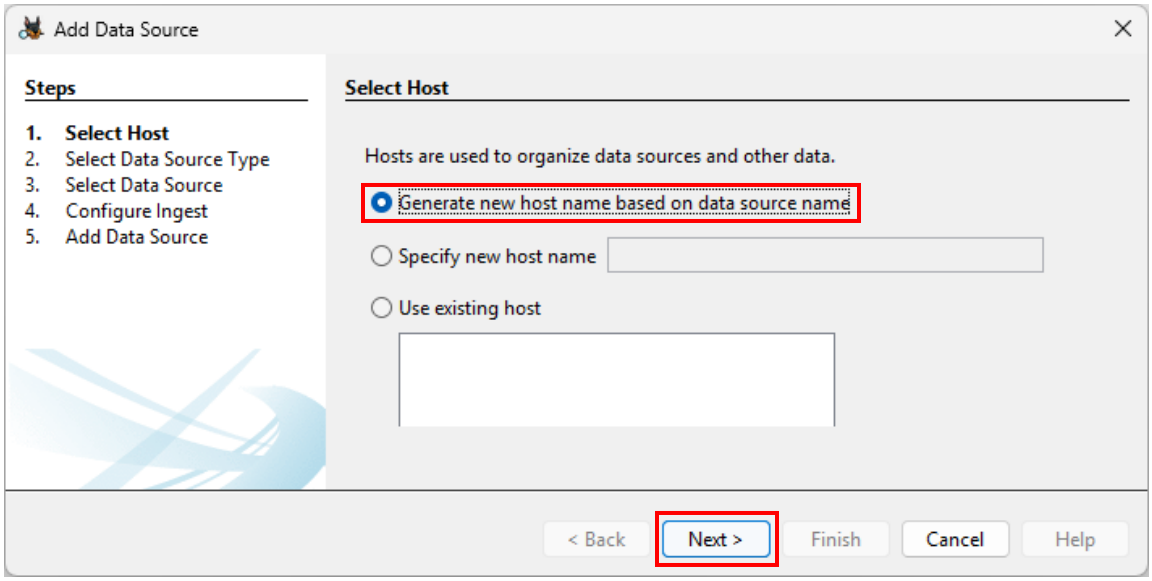

Ilustración 48. Selección de Host para la Fuente de Datos

Se eligió el tipo de fuente de datos **"Disk Image or VM File"** para cargar una imagen forense previamente creada.

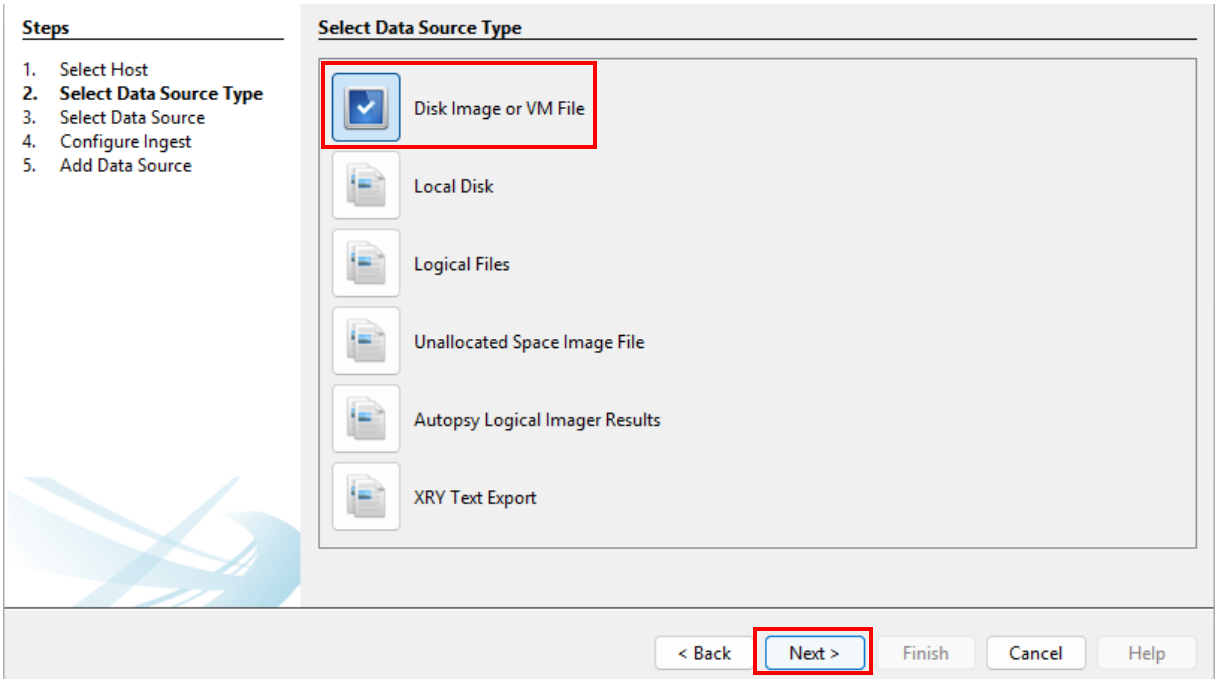

Ilustración 49. Selección del Tipo de Fuente de Datos

5.8 Creación de la carpeta donde se guardará la imagen forense

En la estructura de carpetas generada automáticamente para el caso **"MiPrimerCaso"** se va a crear una carpeta llamada **"imagen"** para guardar la imagen que se encuentra en Kali Linux en esa carpeta, haciendo clic derecho, seleccionando **"Nuevo"** y luego **"Carpeta"**.

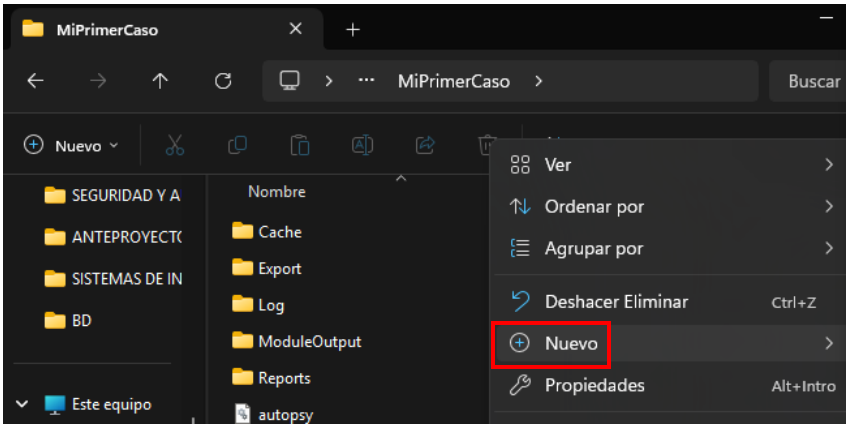

Ilustración 50. Seleccionar opción para crear la nueva carpeta

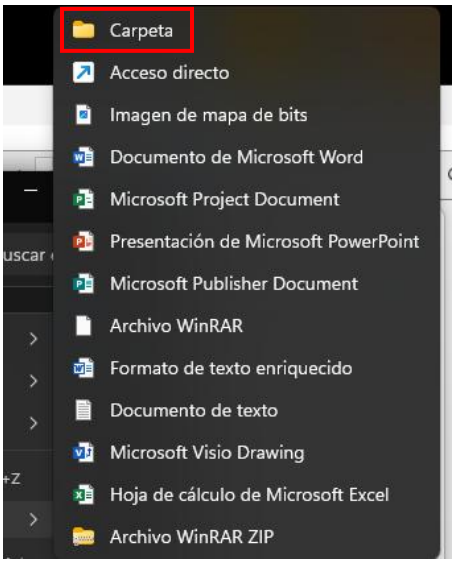

Ilustración 51. Crear nueva carpeta donde se guardará la imagen de que está en Kali Linux

Confirmando la correcta creación de la carpeta **“imagen”**.

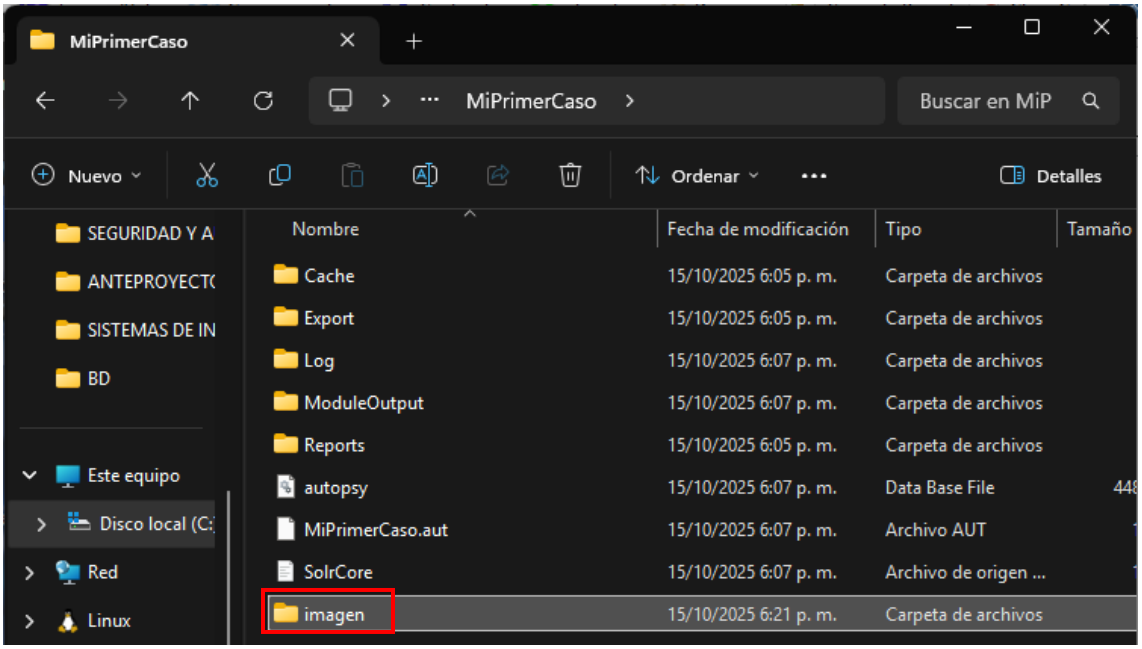

Ilustración 52. Carpeta "imagen" creada

5.9 Transferencia de Imagen Forense desde Kali Linux a Windows

Se capturó el proceso de copia del archivo de la imagen forense **"imagen_usb_forense.dd"** desde la máquina virtual Kali Linux hacia la carpeta **“Imagen”** que está en Windows, mostrando el progreso de la transferencia de 3.8 GB.

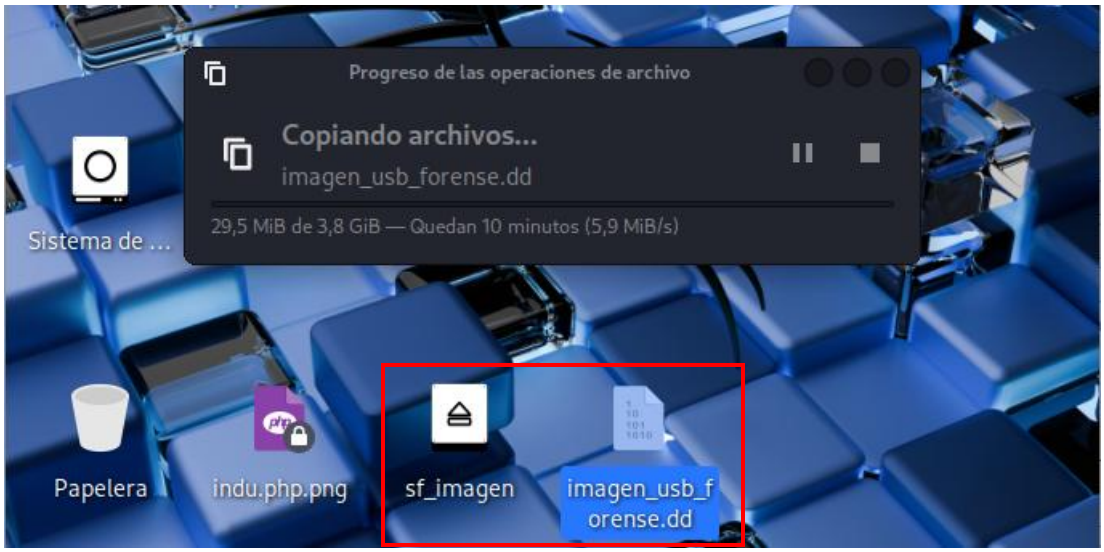

Ilustración 53. Transferencia de Imagen Forense desde Máquina Virtual

5.10 Selección del Archivo de Imagen Forense

En Autopsy, se navegó hasta la ubicación del archivo de imagen forense **"imagen_usb_forense.dd"** y se procedió a seleccionarlo para agregarlo como fuente de datos al caso.

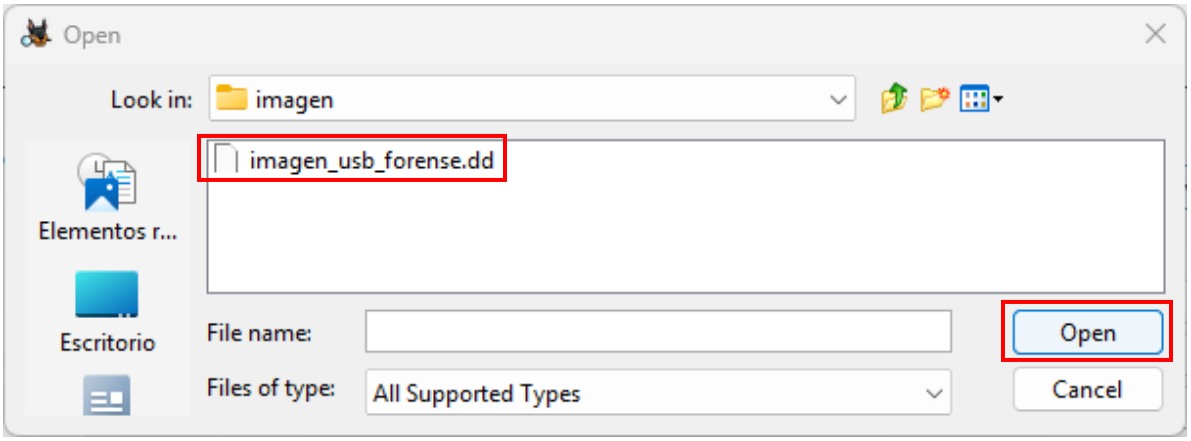

Ilustración 54. Selección del Archivo

Se configuraron los parámetros específicos para la fuente de datos, incluyendo la zona horaria (America/Bogota) y opciones de tamaño de sector.

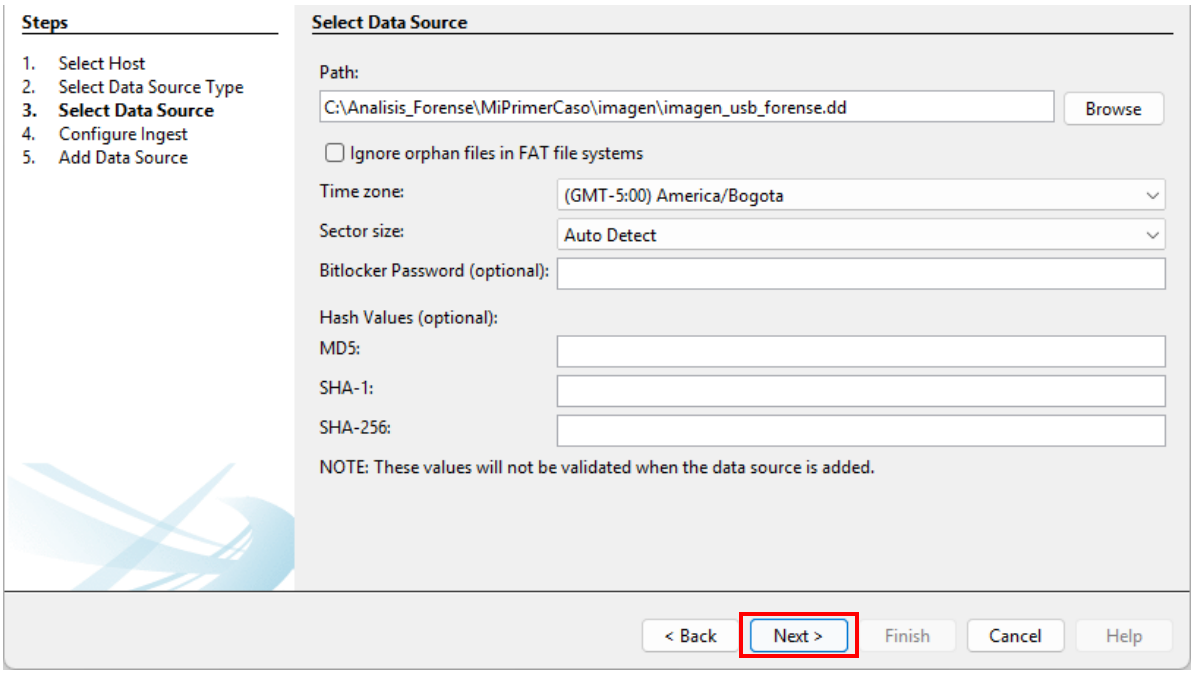

Ilustración 55. Configuración de Parámetros de la Fuente de Datos

Se configuraron los módulos de análisis que se ejecutarían sobre la imagen.

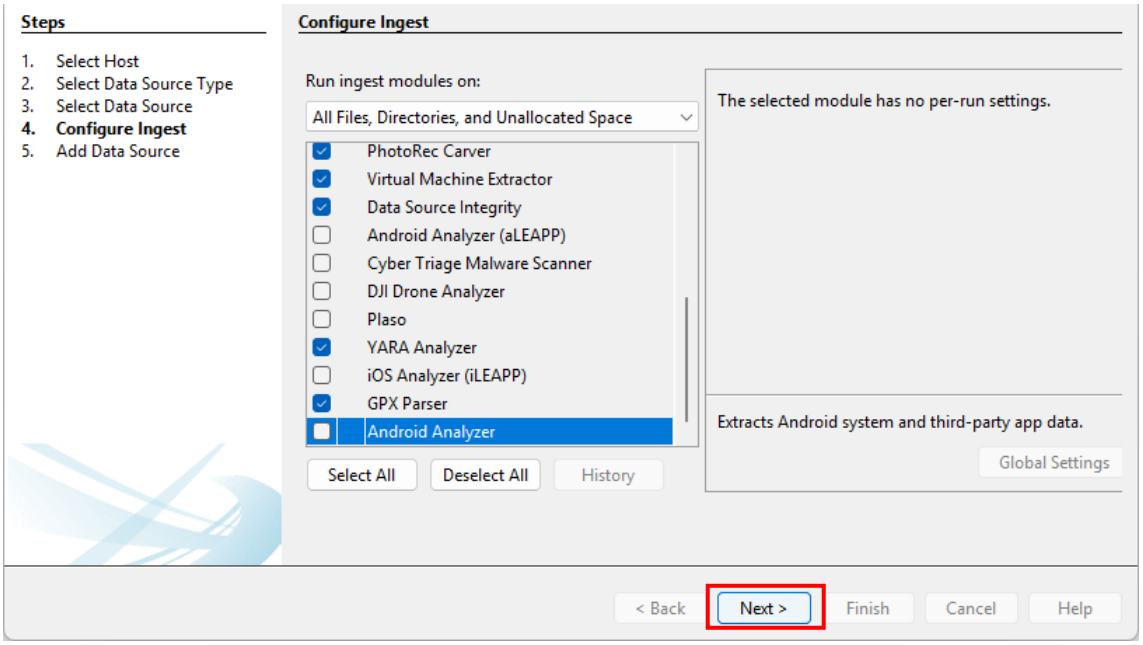

Ilustración 56. Selección de Módulos de Ingesta

Autopsy inició el procesamiento de la fuente de datos, mostrando un mensaje indicando que este proceso podría tomar tiempo dependiendo del tamaño de la imagen.

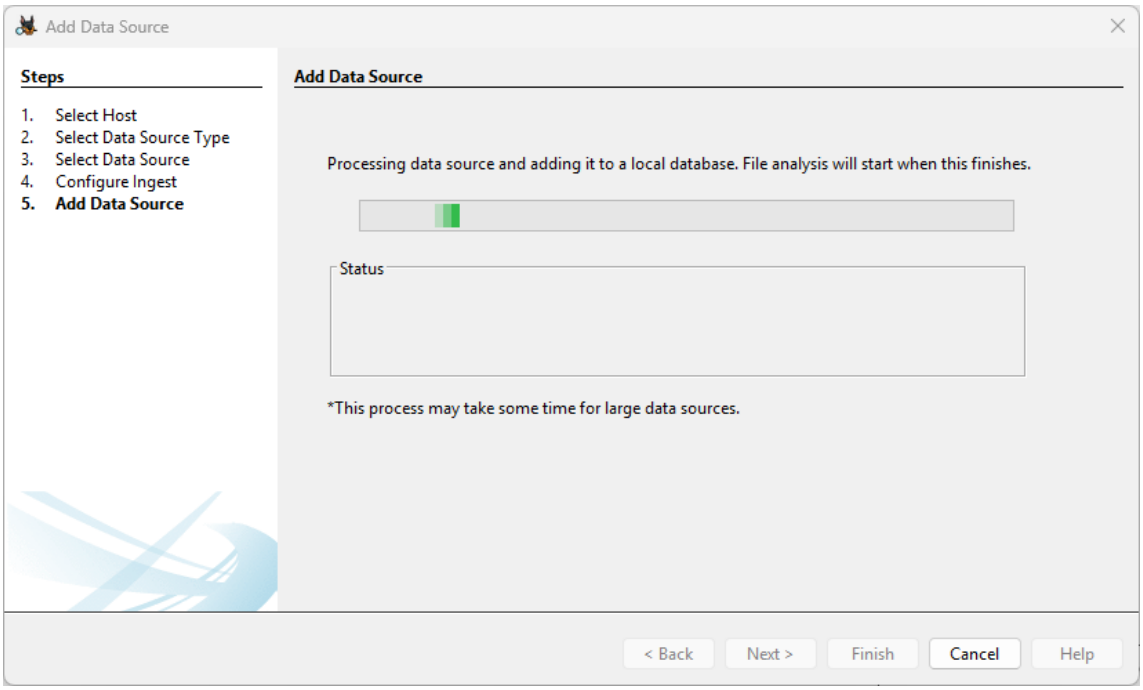

Ilustración 57. Procesamiento Inicial de la Fuente de Datos

Se confirmó que la fuente de datos fue añadida exitosamente a la base de datos local y que el análisis de archivos estaba comenzando automáticamente.

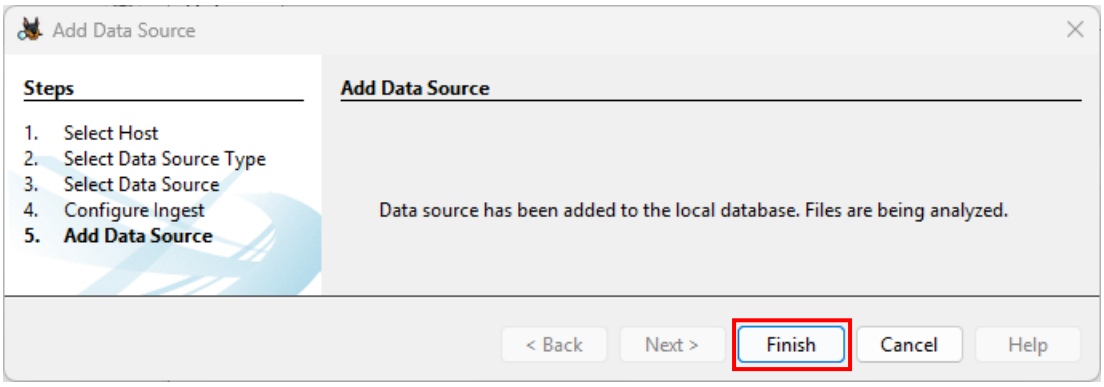

Ilustración 58. Finalización de la Adición de Fuente de Datos

Se muestra la interfaz principal de Autopsy con la barra de progreso al 100% indicando la finalización del procesamiento inicial.

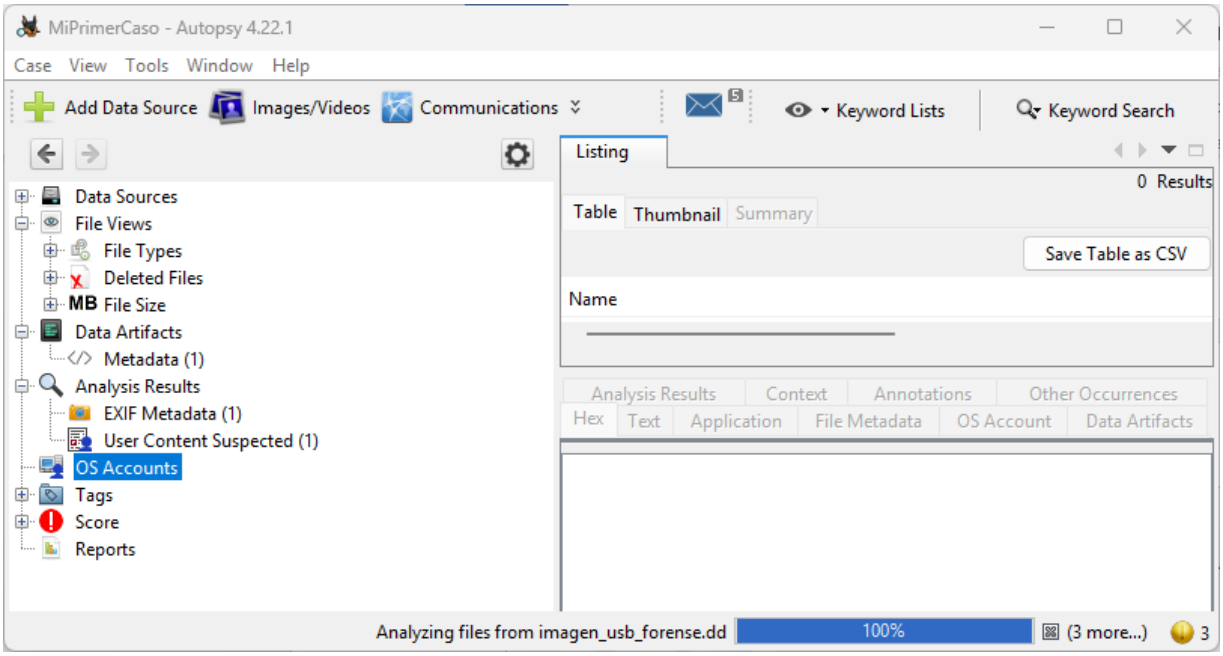

Ilustración 59. Interfaz Principal de Análisis en Progreso

Se visualiza la estructura de la imagen forense **"imagen_usb_forense.dd"** cargada en Autopsy. La imagen contiene dos volúmenes: **vol1** y **vol2**.

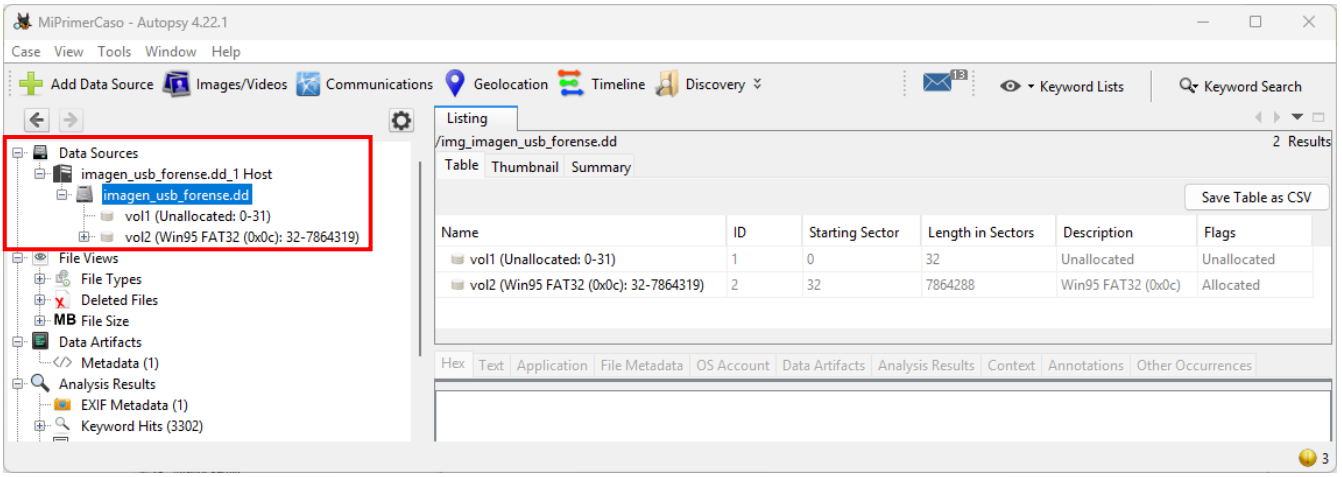

Ilustración 60. Estructura de la Fuente de Datos y Volúmenes

Se examina el volumen no asignado (vol1) donde se identifica un fragmento de datos denominado "Unalloc_3_0_16384" con tamaño de 16.384 bytes. Todos los timestamps de este

fragmento aparecen como "0000-00-00 00:00:00", lo que es característico de espacio no asignado que no contiene metadatos de sistema de archivos.

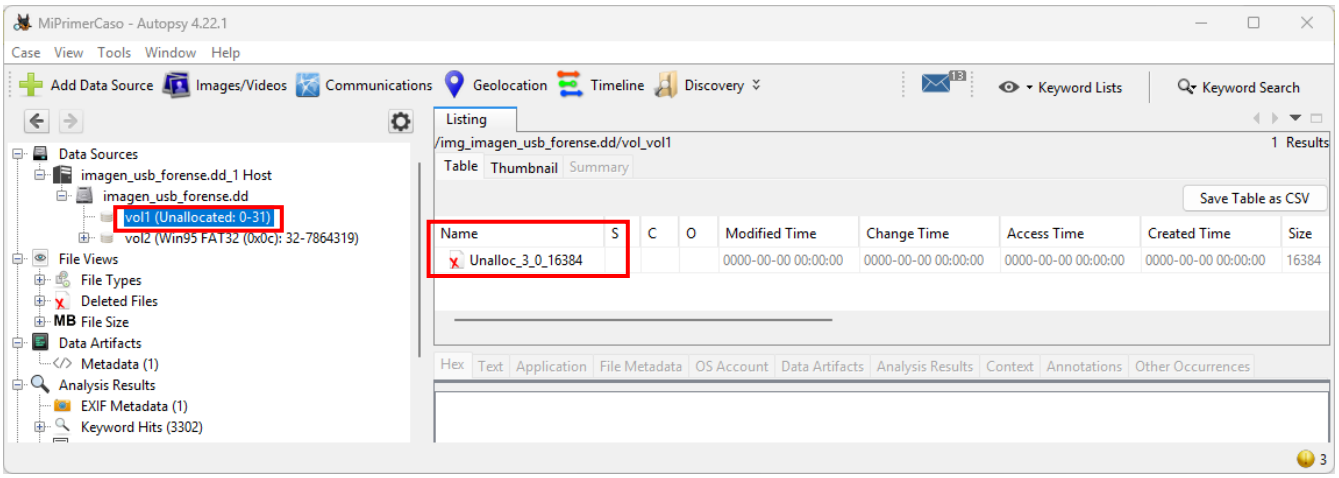

Ilustración 61. Análisis del Espacio No Asignado (vol1)

Se muestra el contenido del volumen FAT32 con 17 archivos recuperados. Entre los archivos identificados se encuentran: "X_imagen.jpg", "X_Articulo.docx", "FECHA 1 LUNES.jpg", "Herramientas de Hacking Ethical.txt", "IMG_0001.JPG", "IMG_3422.mov", y documentos PDF como "PROPUESTA DE ANTEPROYECTO.pdf". Los metadatos muestran fechas de modificación entre 2021 y 2025.

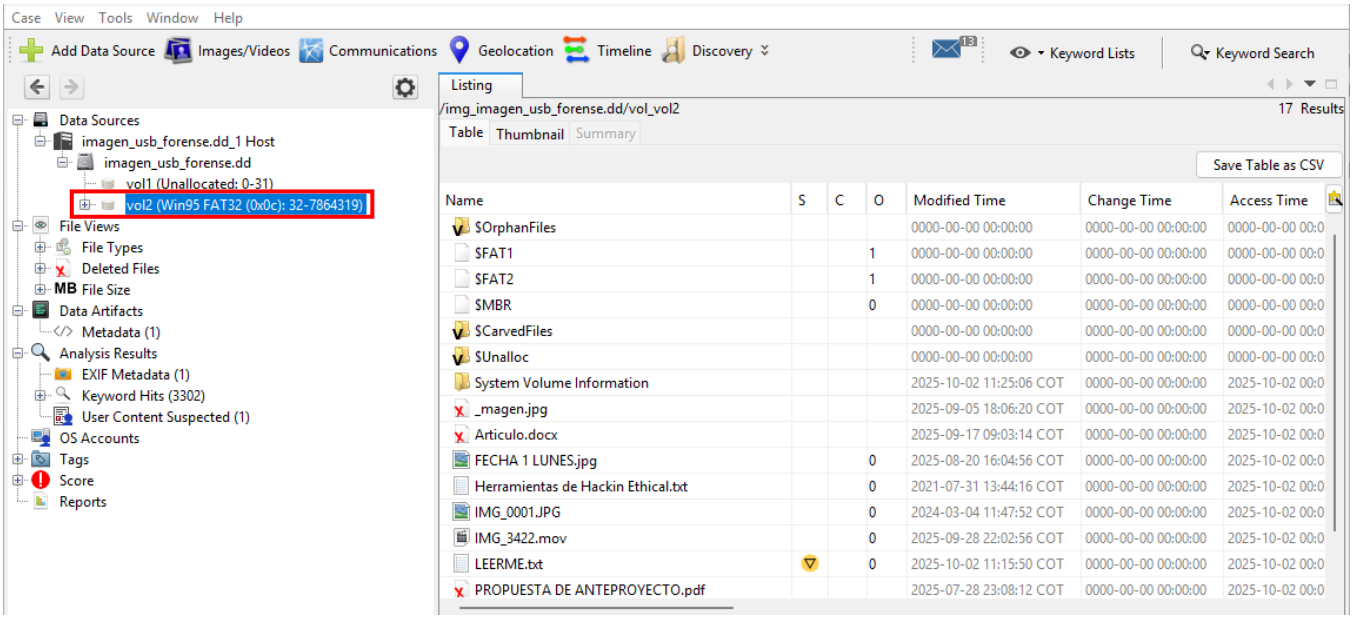

Ilustración 62. Contenido del Sistema de Archivos FAT32 (vol2)

Se presenta una vista detallada de los archivos del volumen FAT32.

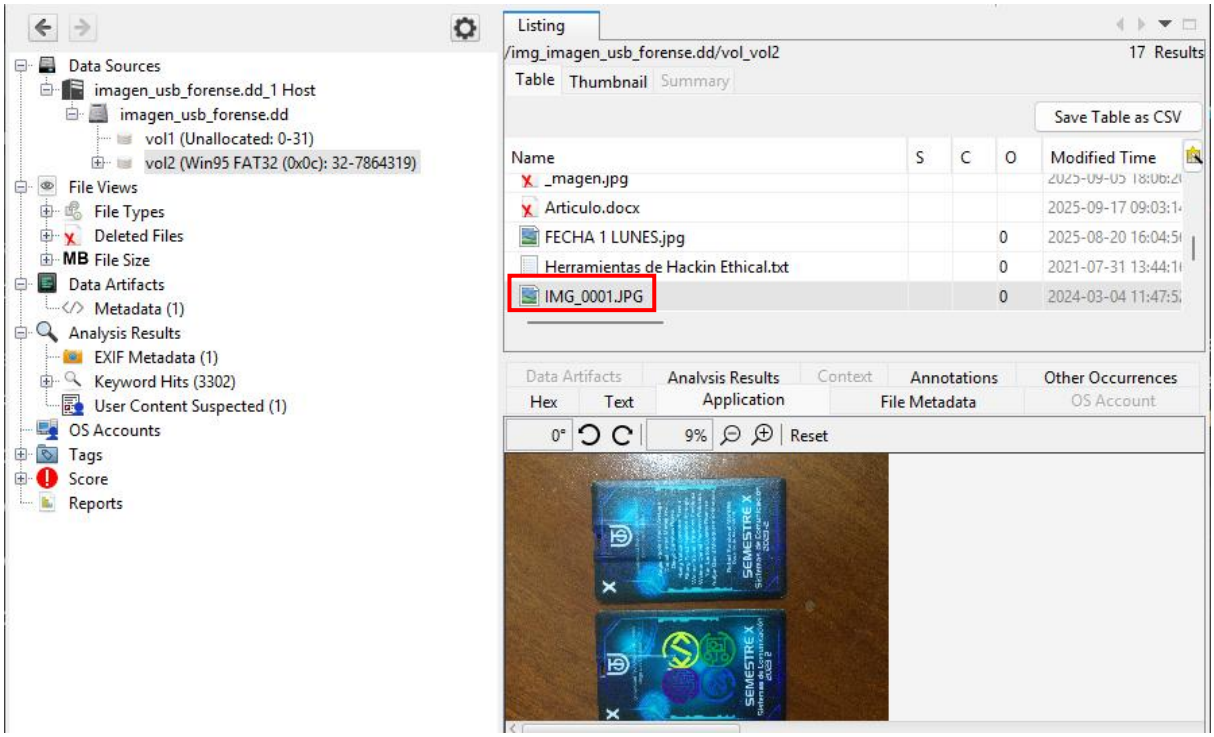

Ilustración 63. Vista Expandida de Archivos

Se realiza un análisis forense avanzado mostrando los valores hash (MD5 y SHA-256) de los archivos recuperados, junto con sus tipos MIME identificados.

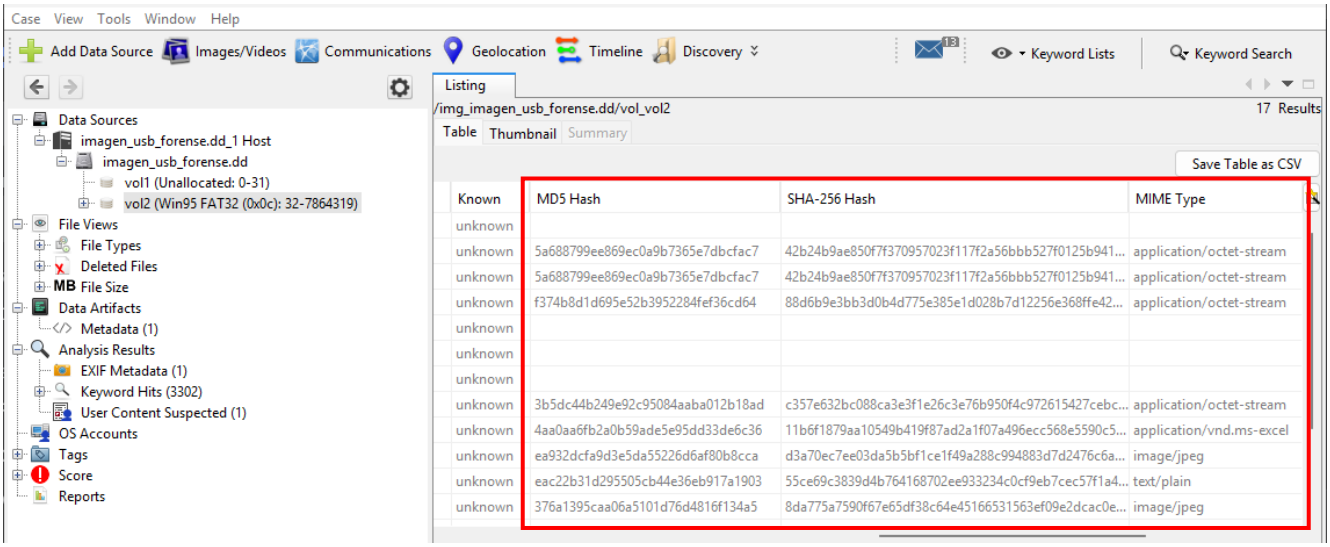

Ilustración 64. Análisis de Hashes y Tipos MIME

6. CAPITULO 3 – ANALISIS FORENSE CON FTK IMAGER EN WINDOWS

6.1 Búsqueda y Selección de FTK Imager

Se realizó una búsqueda en Google con el término "ftk imager 4.7.1 superior" para descargar la herramienta. El resultado principal dirigió al sitio oficial de Exterro.

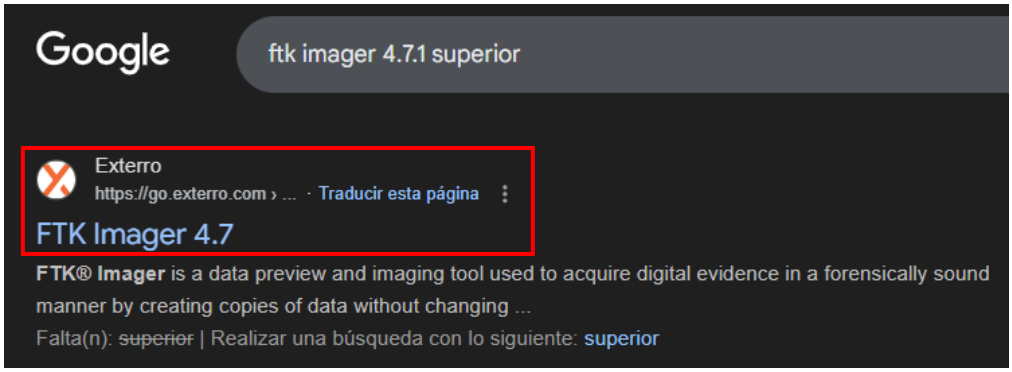

Ilustración 65. Búsqueda en Google de FTK Imager

6.2 Descarga desde el Sitio Oficial de Exterro

En la página oficial de Exterro, se accedió al formulario de descarga de FTK Imager versión 4.7. Se completó el formulario con los datos personales y profesionales requeridos.

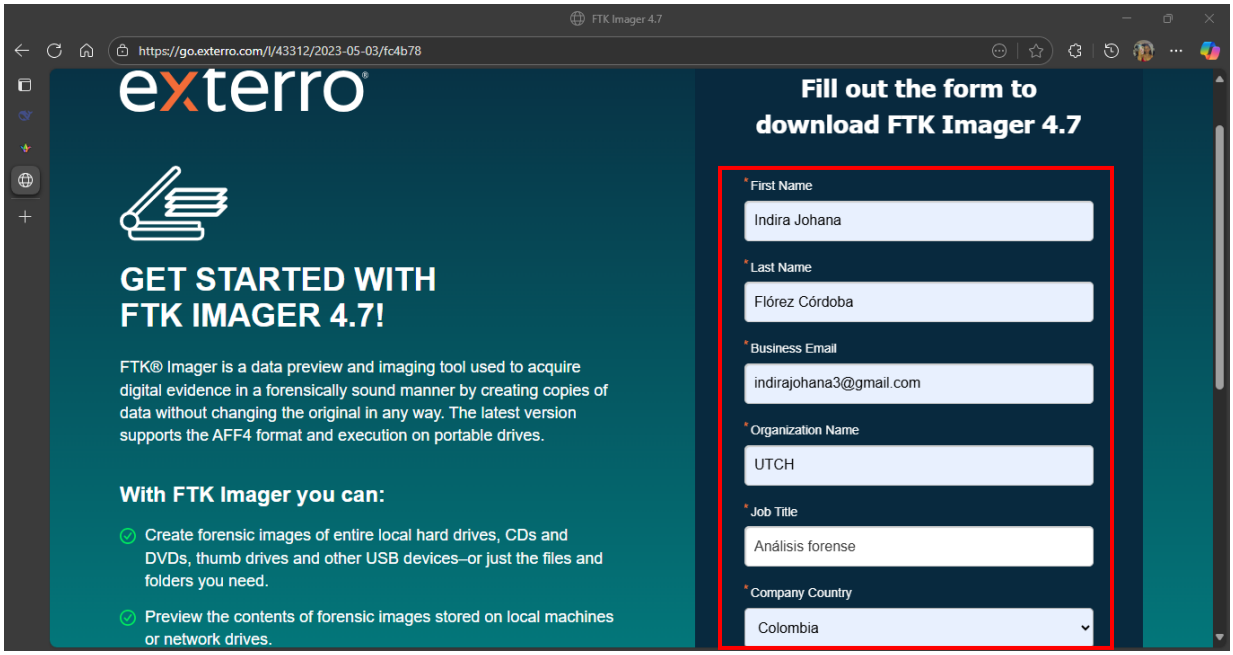

Ilustración 66. Formulario de descarga

6.3 Confirmación de Descarga del Instalador

El navegador mostró el diálogo de descarga, se seleccionó la opción **"Guardar"** para proceder con la descarga del instalador en el sistema.

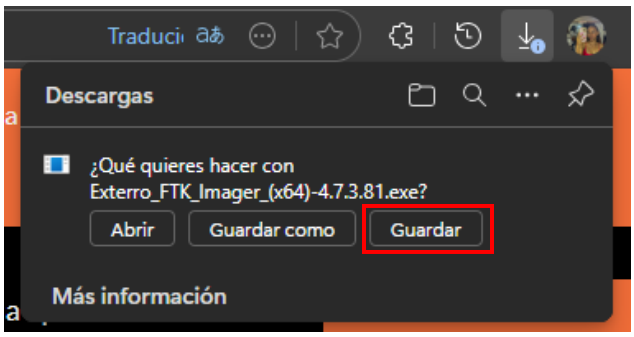

Ilustración 67. Confirmación de descarga de FTK Imager

6.4 Verificación del Archivo Descargado

Se accedió a la carpeta de **"Descargas"** del sistema para verificar que el archivo se había descargado correctamente.

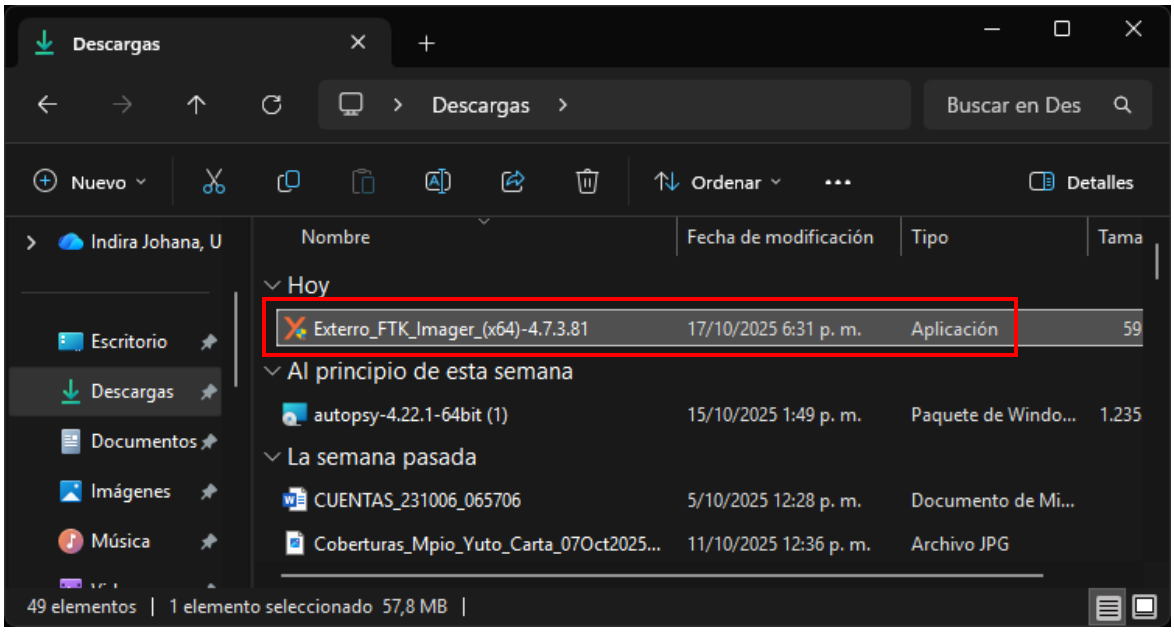

Ilustración 68. Archivo FTK Imager en la carpeta de descargas

6.5 Instalación de FTK Imager

Se ejecutó el archivo descargado, lo que inició el InstallShield Wizard para FTK Imager. Se presentó la pantalla de bienvenida y se hizo clic en "**Next**" para comenzar la instalación.

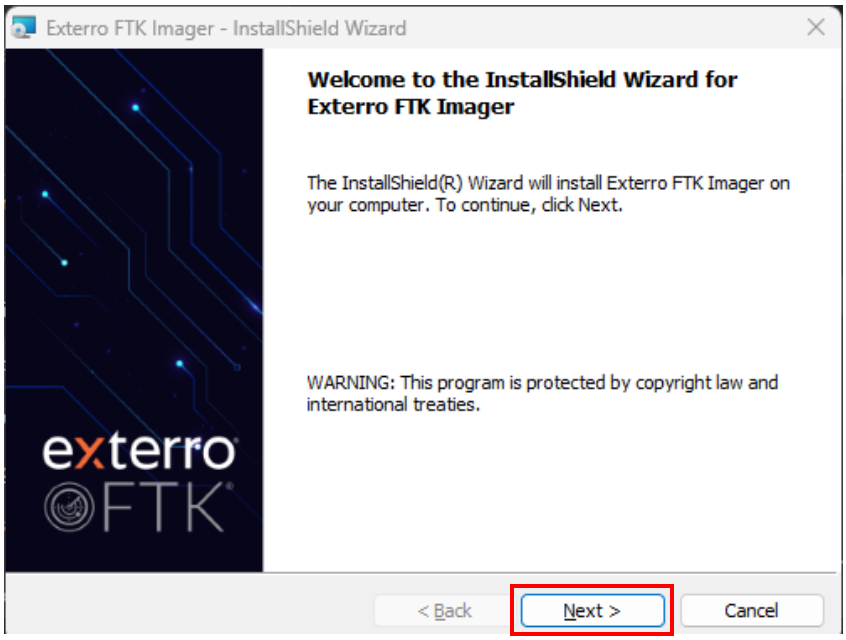

Ilustración 69. Instalación de FTK Imager

Se presentó el Acuerdo de Licencia y se seleccionó la **opción "Acepto los términos del acuerdo de licencia"** para poder continuar con la instalación del software forense.

Ilustración 70. Aceptación del Acuerdo de Licencia

El asistente de instalación mostró la carpeta destino predeterminada para la instalación: "C:\Program Files\AccessData". Se mantuvo esta ubicación por defecto y se marcó la opción adicional **"Add Installation File path in Windows Defender Exclusion List"** para evitar interferencias del antivirus durante el uso de la herramienta forense.

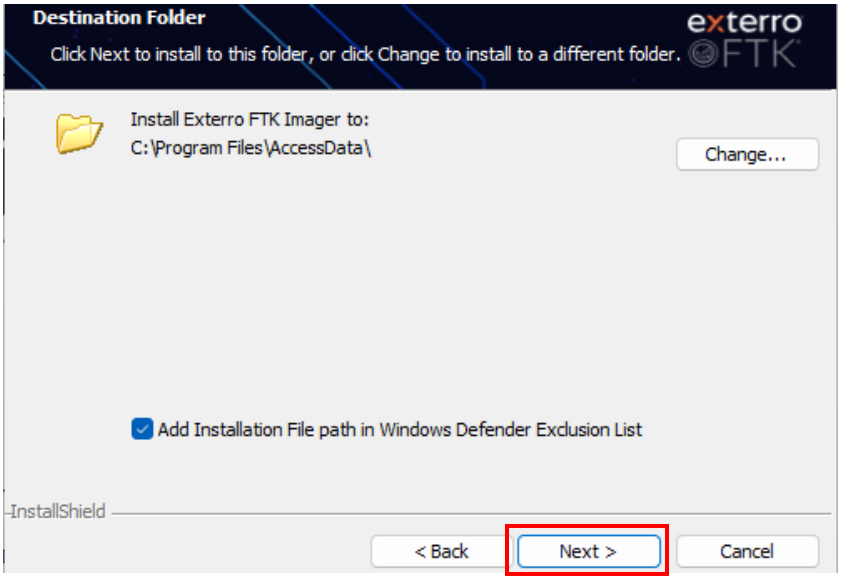

Ilustración 71. Selección de Carpeta de Destino

Ventana de confirmación final donde se hizo clic en el botón **"Install"** para iniciar el proceso de instalación propiamente dicho.

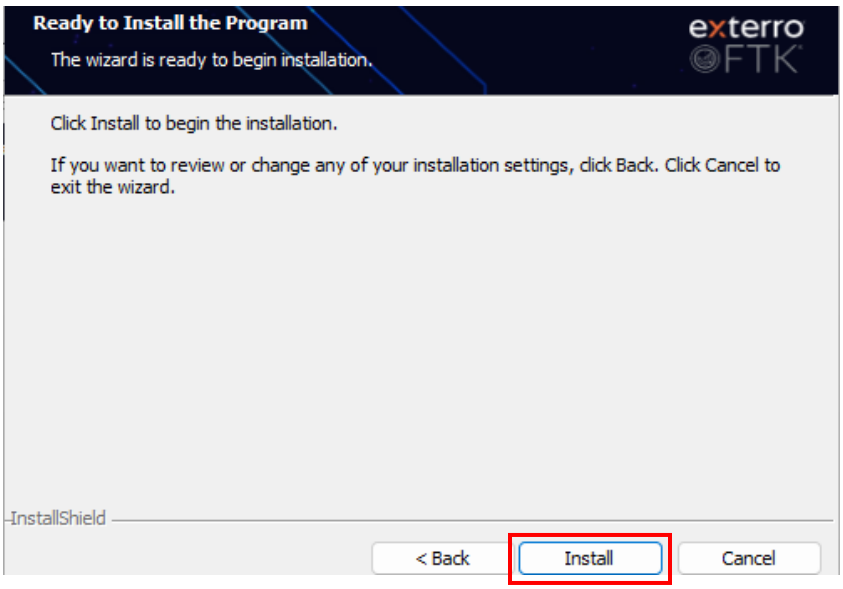

Ilustración 72. Confirmación Final antes de la Instalación

Progreso de la instalación, indicando el estado actual **"Registering product".** Este proceso tomó varios minutos mientras el sistema copiaba los archivos necesarios y configuraba los registros del sistema.

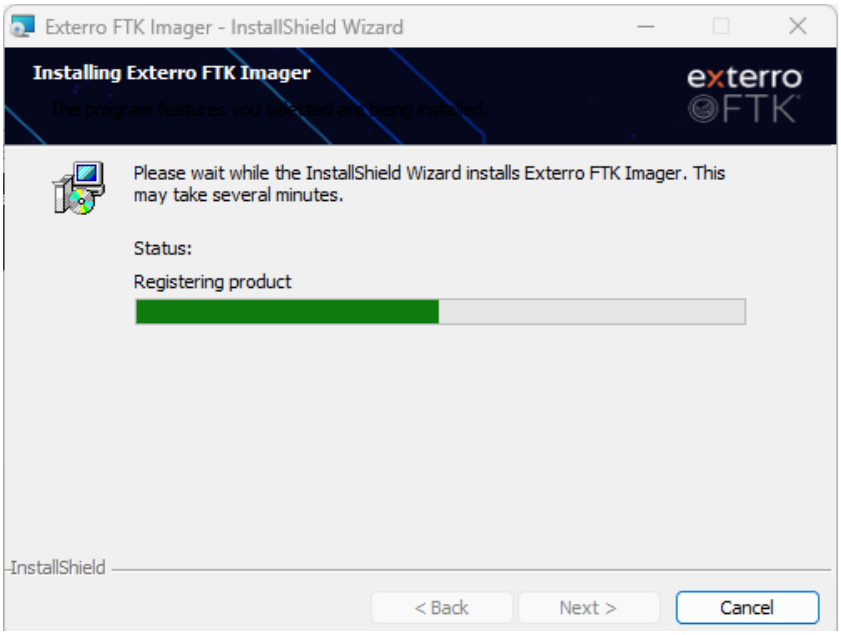

Ilustración 73. Progreso de la Instalación

Finalización exitosa de la instalación. Se marcó la opción **"Launch Exterro FTK Imager"** para ejecutar automáticamente la aplicación al hacer clic en **"Finish"**.

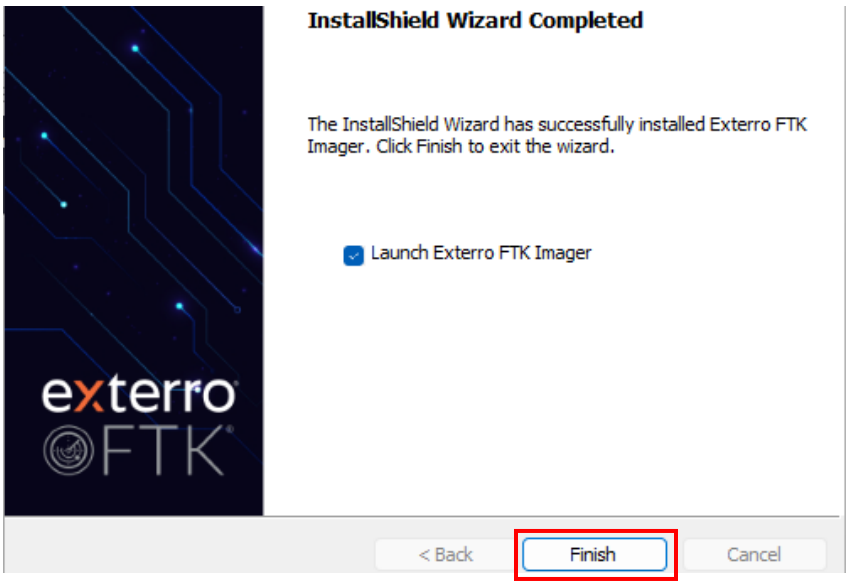

Ilustración 74. Finalización Exitosa de la Instalación

6.6 Inicio de FTK Imager

Se inició la aplicación FTK Imager, mostrando la interfaz principal con el árbol de evidencia, lista de archivos y opciones para manejar fuentes de contenido personalizadas

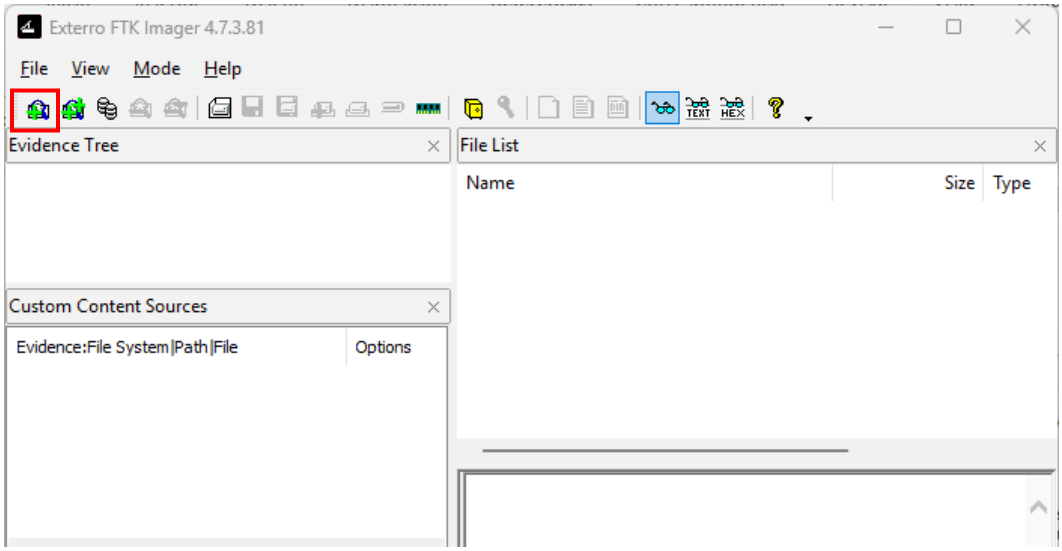

Ilustración 75. Interfaz Principal de FTK Imager

Al agregar una nueva evidencia, se seleccionó la opción **"Image File"** como tipo de fuente de evidencia, indicando que se trabajaría con una imagen forense previamente creada.

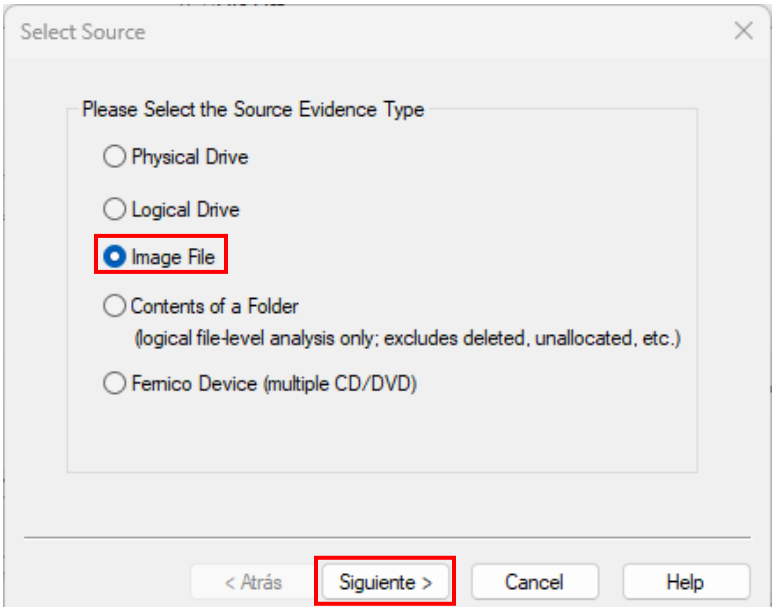

Ilustración 76. Selección del Tipo de Fuente de Evidencia

Se utilizó el botón **"Browse"** para navegar hasta la ubicación del archivo de imagen forense **"imagen_usb_forense.dd".**

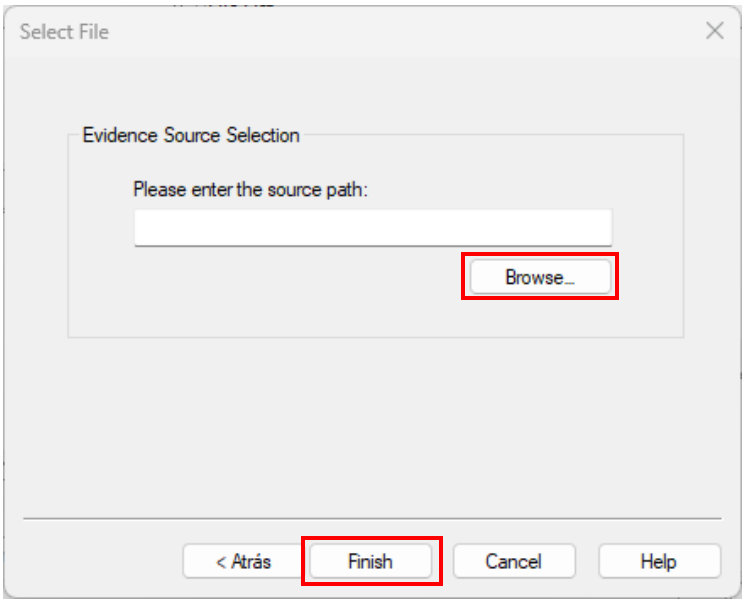

Ilustración 77. Navegación para Seleccionar Archivo de Imagen

Se verificó la ruta del archivo de imagen forense.

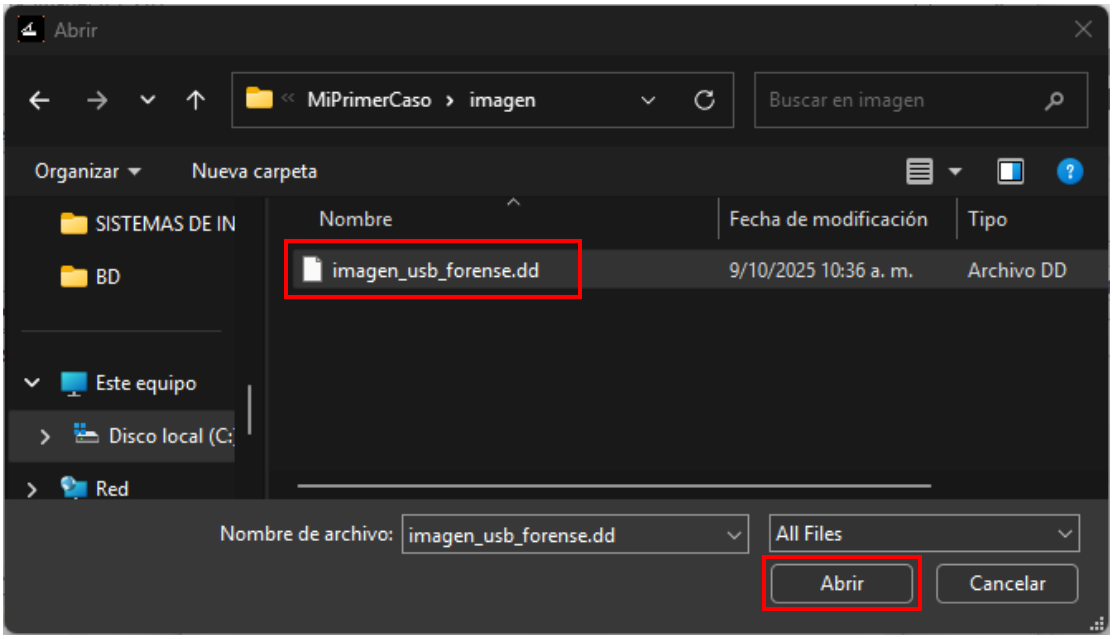

Ilustración 78. Verificación de la Ruta de la Imagen Forense

Se confirmó la ruta completa del archivo de imagen forense.

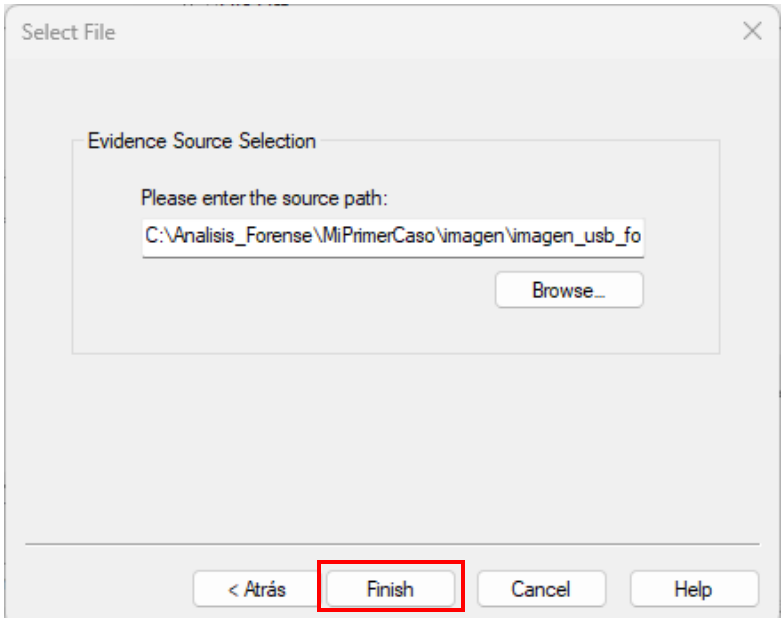

Ilustración 79. Confirmación de la Ruta de la Imagen Forense

FTK Imager mostró la estructura de la imagen forense, identificando **"Partition 1 [3839MB]"** con sistema de archivos **FAT32** y espacio no particionado.

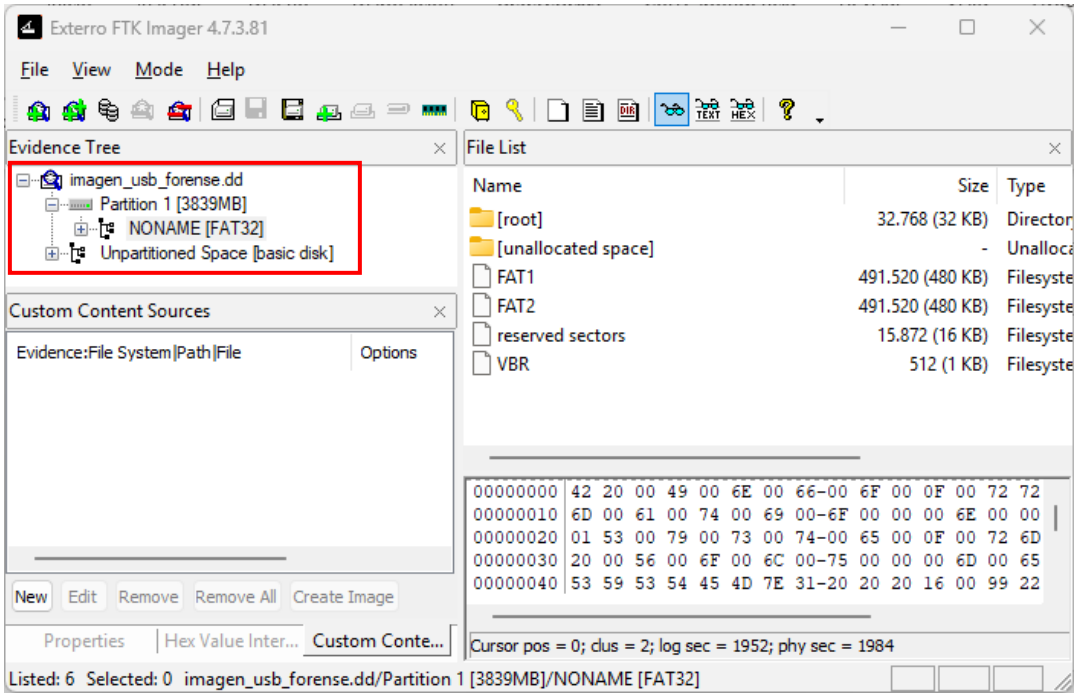

Ilustración 80. Estructura de Particiones de la Imagen

Se examinó el contenido del directorio raíz de la partición FAT32, identificando 18 elementos.

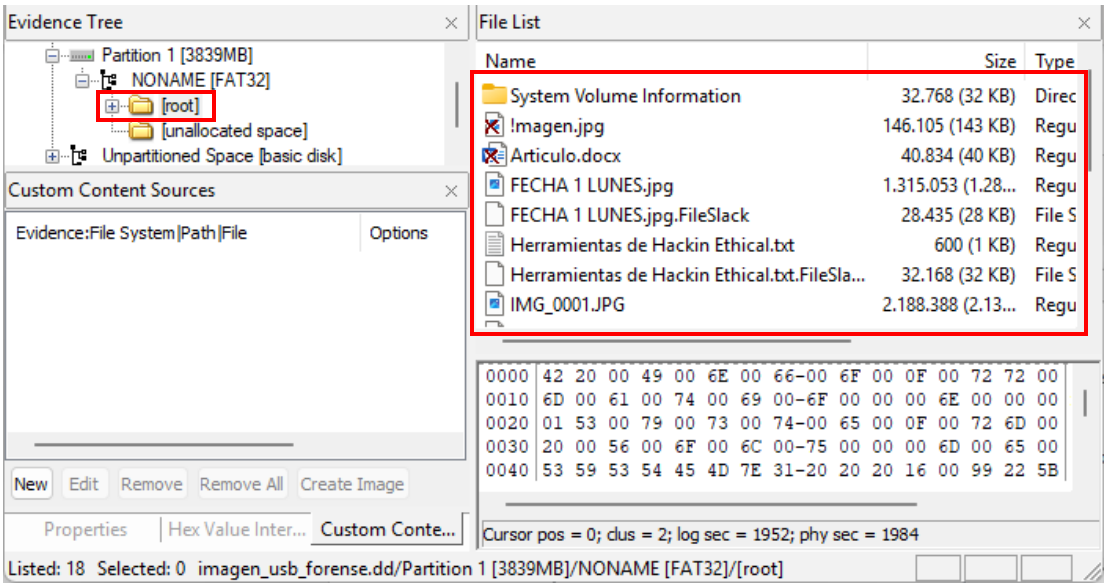

Ilustración 81. Contenido del Directorio Raíz FAT32

Se visualizó la lista detallada de archivos mostrando los archivos regulares. Se seleccionó específicamente "IMG_0001.JPG" para su análisis, mostrando su tamaño de 2.13 MB.

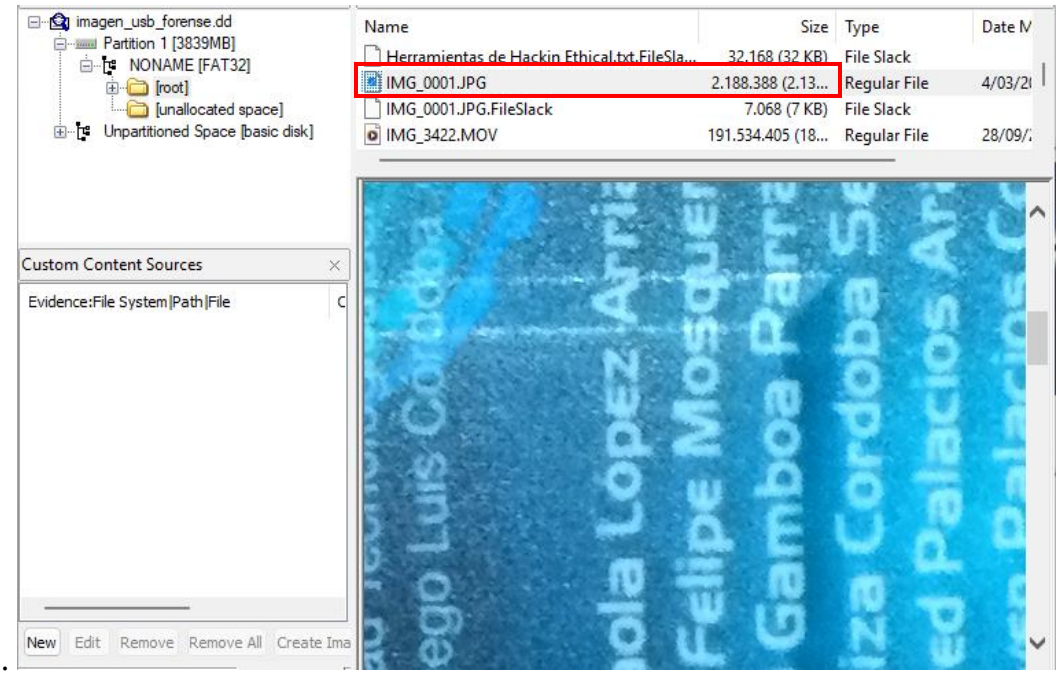

Ilustración 82. Análisis Detallado de Archivos

Se seleccionaron todos los archivos en el sistema de archivos FAT32, incluyendo documentos PDF, archivos Excel, imágenes JPEG, video MOV y archivos de texto para guardar los hash.

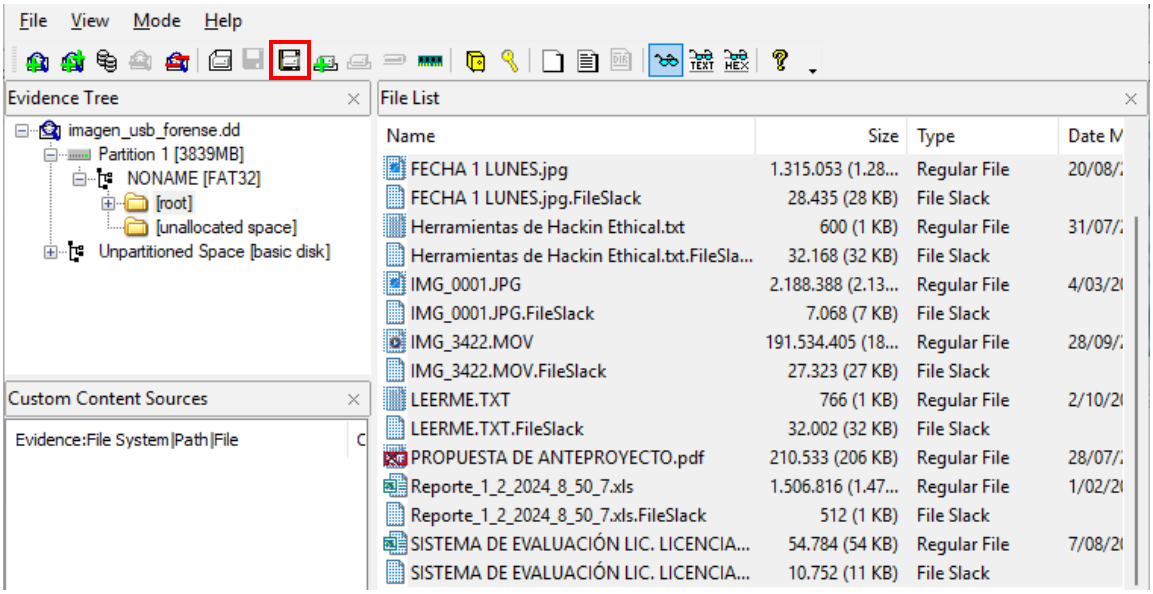

Ilustración 83. Lista Completa de Archivos Recuperados

Se inició el proceso de exportación de los resultados del análisis para documentar los hallazgos forenses en un formato estructurado y procesable.

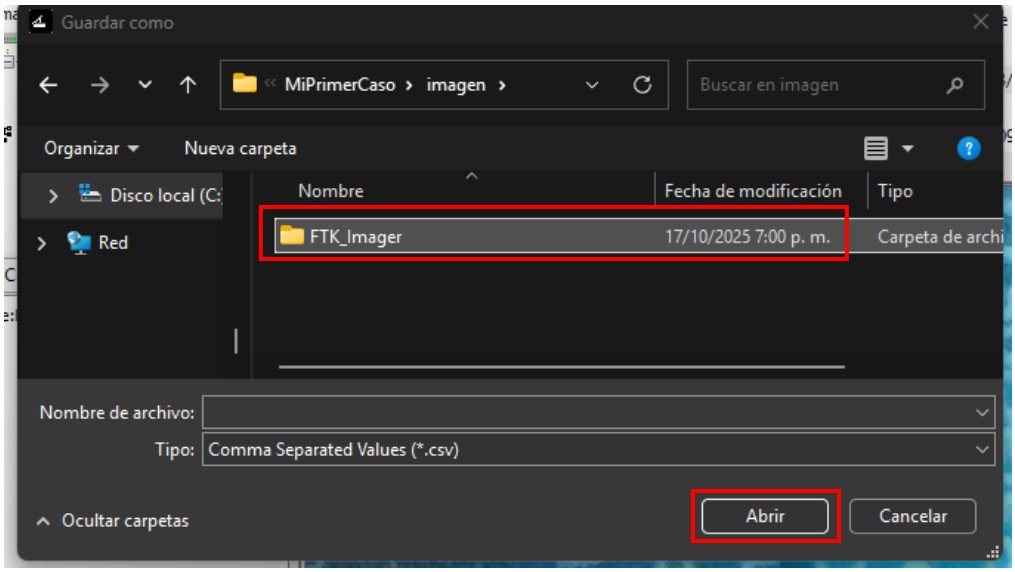

Ilustración 84. Exportación de Resultados a CSV

Se configuró la exportación específicamente para generar un archivo de valores hash, seleccionando el formato CSV y asignando el nombre "hash" al archivo de salida.

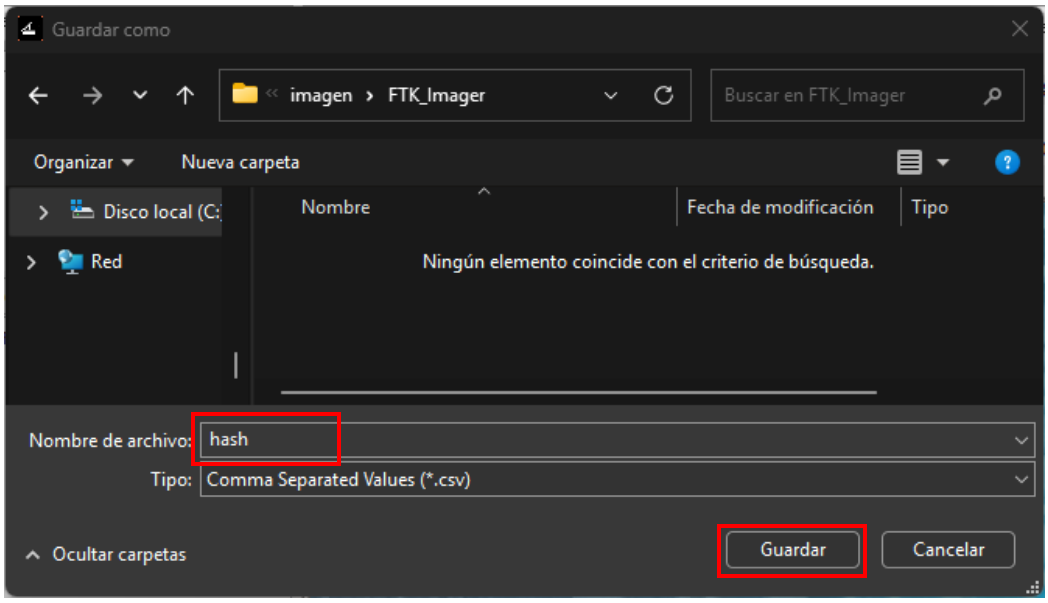

Ilustración 85. Configuración de Exportación de Hash

Se confirmó la creación exitosa del archivo **"hash.csv"** en la carpeta **"FTK_Imager"**, validando que la exportación de los valores hash de los archivos analizados se completó correctamente.

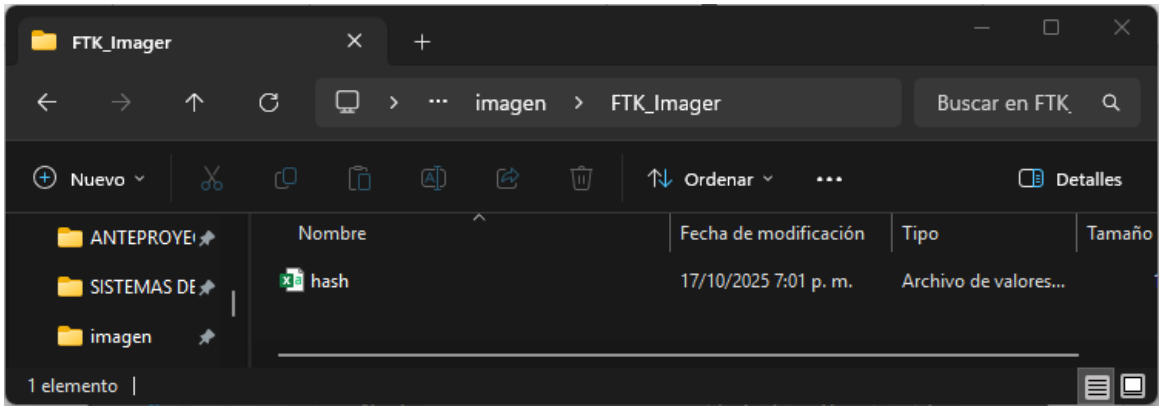

Ilustración 86. Verificación del Archivo de Hash Exportado

Archivo hash abierto.

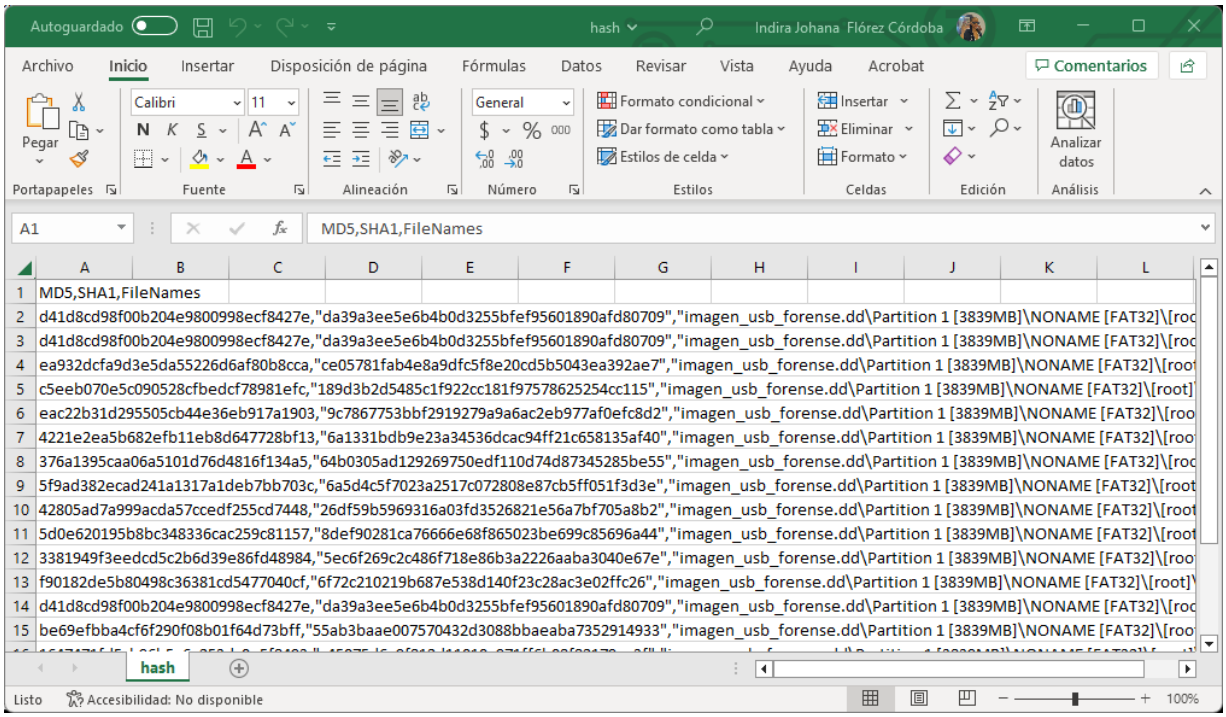

Ilustración 87. Archivo hash

7. CONCLUSIÓN

El uso de Autopsy y FTK Imager facilitó la identificación, clasificación y verificación de archivos contenidos en la memoria USB, demostrando la eficiencia de ambas herramientas en entornos operativos distintos.

Asimismo, se confirmó que los valores hash obtenidos antes y después del proceso coincidieron, validando la preservación íntegra de los datos.

8. BIBLIOGRAFIA

Morales, R. S. (25). *INFORME DE LABORATORIO 02*. Quibdó, Colombia: Universidad Tecnologia del Chocó Diego Luis Córdoba. Recuperado el 16 de 10 de 2025