# Informe 2 Parcial # 3

Camilo Andrés Tello Mosquera

Universidad Tecnológica del Chocó Diego Luis Córdoba

Facultad de Ingeniería

Ingeniería de telecomunicaciones e informática

Auditoria y Seguridad de redes

Prof. Rafael Sandoval Morales

Quibdó-Choco

# Tabla de contenido

# TABLA DE ILUSTRACIONES

# INTRODUCCIÓN

En este laboratorio desarrollé una práctica orientada al uso de herramientas forenses en entornos controlados, con el propósito de comprender el proceso de **adquisición, verificación y análisis de una memoria USB**.

El trabajo se realizó empleando **Autopsy** (tanto en **Kali Linux** como en **Windows**) y **FTK Imager**, herramientas ampliamente utilizadas por los profesionales de la ciberseguridad y el análisis forense digital.

Durante la práctica ejecuté la creación de una imagen forense de una memoria USB, generé y comparé los valores hash, y analicé la evidencia digital desde distintos sistemas operativos para comprobar su integridad y comportamiento.

Este informe documenta paso a paso todo el proceso, con explicaciones técnicas, comandos utilizados y observaciones personales que pueden servir de guía para otros estudiantes interesados en el tema.

# OBJETIVOS

## Objetivo General

Realizar un proceso completo de análisis forense sobre una memoria USB utilizando las herramientas **Autopsy** y **FTK Imager**, con el fin de aprender cómo se obtiene, se protege y se analiza la información digital sin alterarla y cómo verificar su integridad

## Objetivos Específicos

- Generar el hash original del dispositivo USB y compararlo con el hash de su imagen forense para verificar la integridad.
- Crear una imagen forense del dispositivo USB utilizando el comando dd.
- Analizar la imagen con Autopsy en entornos Linux y Windows, reconociendo diferencias de entorno y proceso.
- Instalar y utilizar FTK Imager para examinar la imagen forense y generar los hashes de los archivos.

# 1 CAPÍTULO 1 – AUTOPSY EN KALI LINUX

## 1.1 Identificación de USB y creación del hash

Después de iniciar la máquina virtual con **Kali Linux**, el primer paso fue conectar la memoria USB que iba a analizar.
Para ello, desde el menú de VirtualBox seleccioné la opción **Dispositivos → USB** y elegí el dispositivo conectado.
Una vez reconocido por el sistema, abrí una terminal y ejecuté el siguiente comando:

**fdisk -l**

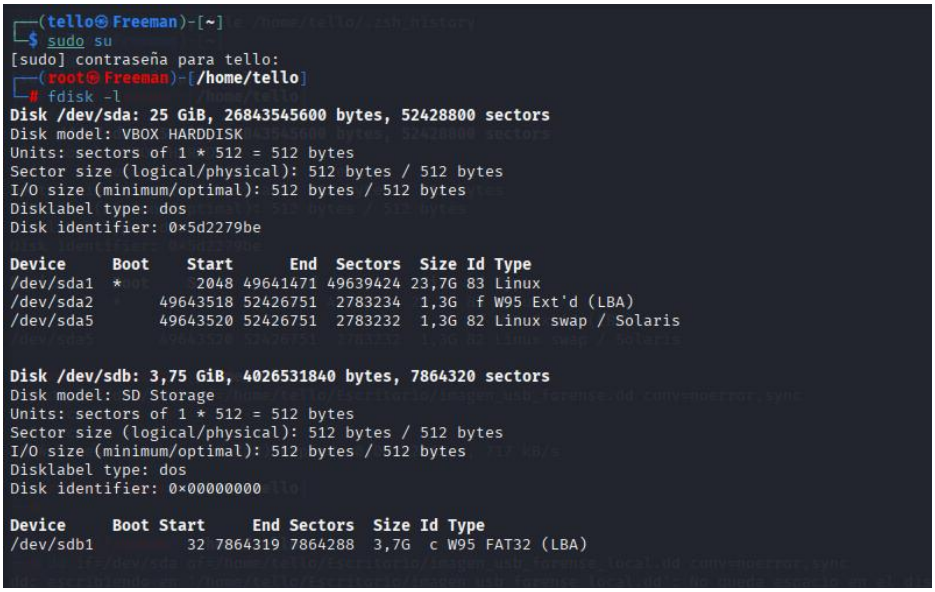



*Ilustración 1Identificación de USB*

Este comando permite listar todos los dispositvos de almacenamiento conectados al sistema.

Entre los resultados identifiqué que la memoria USB correspondía al disco **/dev/sdb.**

Posteriormente, generé el **hash SHA1** del dispositivo completo, con el siguiente comando:

**sha1sum /dev/sdb > /home/camilo/Escritorio/hash_forense_usb.sha1**

Con esto se creó un archivo llamado **hash_forense_usb.sha1**, que contiene el hash original de la memoria USB.

Este valor será utilizado más adelante para comprobar que la imagen forense sea idéntica al dispositivo original.

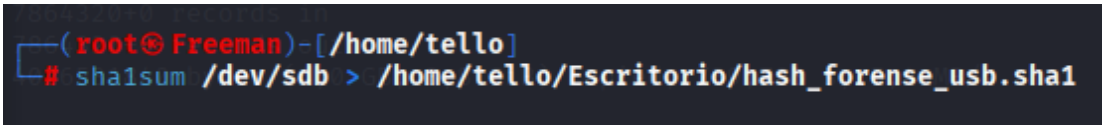



*Ilustración 2 creación del hash*

Con esto se creó un archivo llamado **hash_forense_usb.sha1**, que contiene el hash original de la memoria USB.
Este valor será utilizado más adelante para comprobar que la imagen forense sea idéntica al dispositivo original.

### 1.2 Creación de la imagen de la USB

Una vez obtenido el hash original, procedí a **crear una copia bit a bit de la memoria USB**, conocida como **imagen forense**.

Esto se hace con el comando dd, que permite clonar dispositivos sin alterar su contenido:

```
dd if=/dev/sdb of=/home/camilo/Escritorio/imagen_usb_forense.dd
conv=noerror,sync
```

- **if=** indica el archivo de entrada, en este caso la USB.
- **of=** especifica el archivo de salida (la copia).
- **conv=noerror,sync** garantiza que el proceso continúe incluso si hay errores de lectura.

```
┌──(root㉿Freeman)-[/home/tello]
└─# dd if=/dev/sdb of=/home/tello/Escritorio/imagen_usb_forense_usb.dd conv=noerror,sync
7864320+0 records in
7864320+0 records out
4026531840 bytes (4,0 GB, 3,8 GiB) copied, 739,783 s, 5,4 MB/s
```

Tras unos minutos, se generó la imagen **imagen_usb_ forense.dd** en el escritorio.

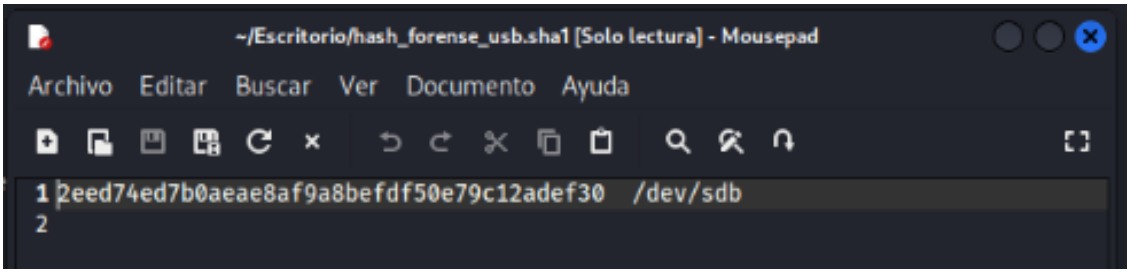
Luego obtuve el hash SHA1 de esa imagen para comparar con el hash original:

```
sha1sum /home/camilo/Escritorio/imagen_usb_forense.dd
```

El resultado mostró un valor idéntico al hash anterior, lo que confirma que la imagen es una copia exacta del dispositivo original.

```
┌──(root㉿Freeman)-[/home/tello]
└─# sha1sum /home/tello/Escritorio/imagen_usb_forense_usb.dd
2eed74ed7b0aeae8af9a8befdf50e79c12adef30  /home/tello/Escritorio/imagen_usb_forense_usb.dd
```

*Ilustración 3 imagen_usb_forense.dd*




## 1.3 Comparación de hash original y hash de la imagen

Con ambos hashes obtenidos, realicé la comparación visual para verificar que coincidieran.

Como se observó, el hash de la memoria y el hash de la imagen eran **exactamente iguales**, lo cual indica que **no hubo alteración alguna** durante el proceso de copia.

Esto demuestra que la **información se mantiene íntegra** y que la imagen puede ser usada como evidencia digital confiable.

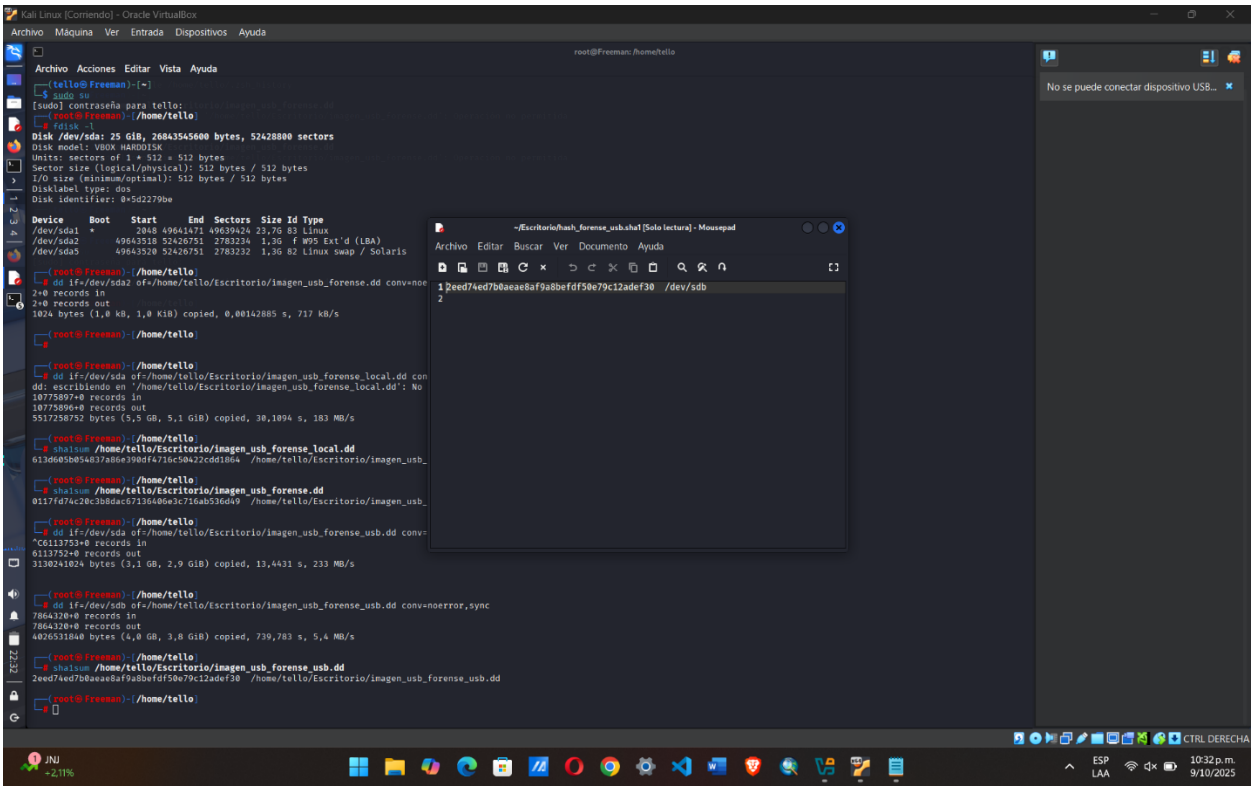



*Ilustración 4 Comparación de hash original y hash de la imagen*

## 1.4 Asignación de privilegios a la imagen

Antes de analizar la imagen en Autopsy, fue necesario **asignarle permisos de lectura y escritura** para evitar restricciones durante el análisis.

Para ello ejecuté el siguiente comando:

```
chmod 777 /home/camilo/Escritorio/imagen_usb_forense.dd
```


*Ilustración 5 Asignación de privilegios a la imagen*

Este comando otorga **permisos totales (lectura, escritura y ejecución)** sobre el archivo.

De esta forma, Autopsy puede acceder libremente a su contenido.

## 1.5 Ejecución de Autopsy

Una vez listos los permisos, busqué **Autopsy** en el menú de Kali Linux y lo ejecuté. Automáticamente se abrió una **consola de comandos** pidiendo autenticación de superusuario (sudo).

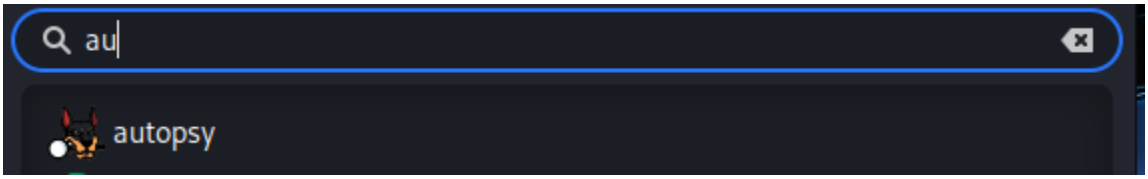
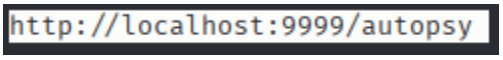



*Ilustración 6 Buscar Autopsy*


Tras ingresar la contraseña, el sistema mostró un mensaje de inicio y una dirección web del tipo:

http://localhost:9999/autopsy

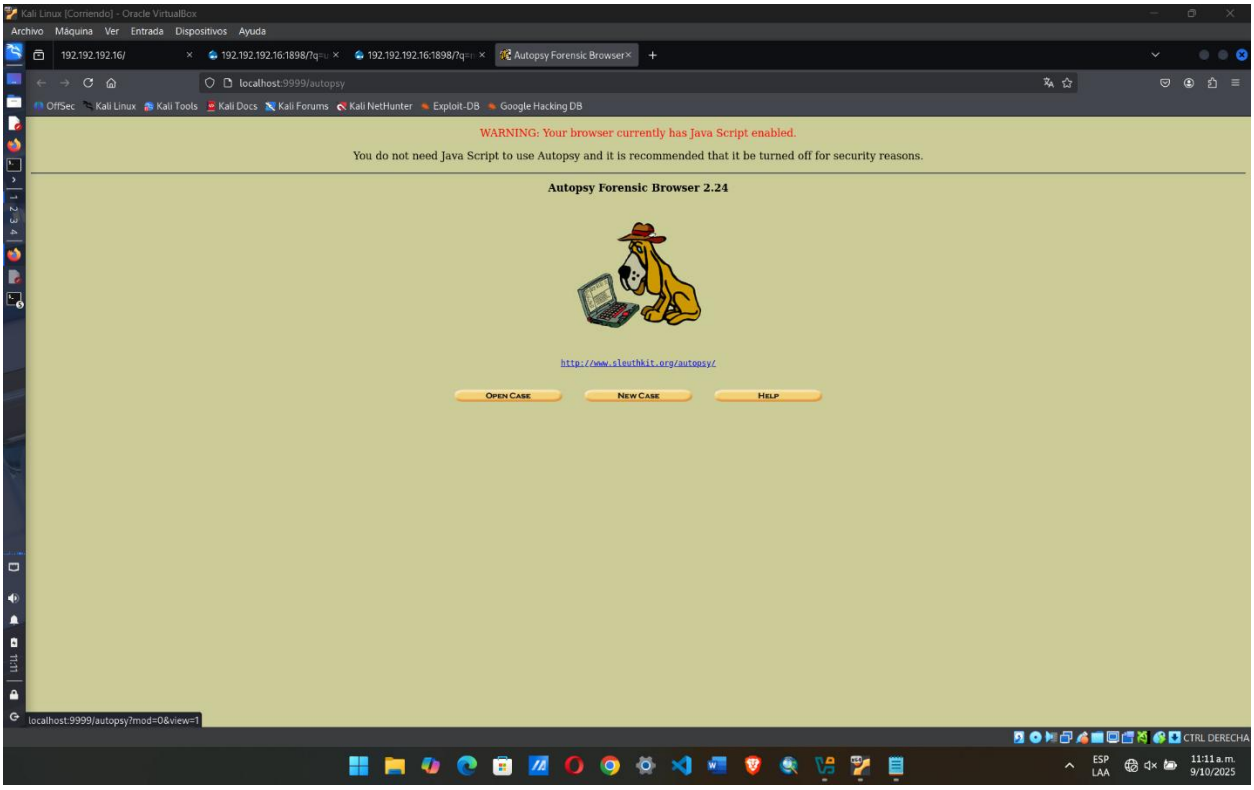



Esta dirección permite acceder a la interfaz gráfica de Autopsy desde el navegador.

Ingresé al enlace, donde aparecieron tres opciones principales:

- **Open Case**
- **New Case**
- **Help**

Seleccioné **"New Case"** para crear un nuevo caso de análisis.




## 1.6 Creación del caso forense

En la siguiente pantalla ingresé los datos solicitados:

- **Nombre del caso**
- **Descripción**
- **Investigador** (mi nombre)

Después pulsé **Next**.

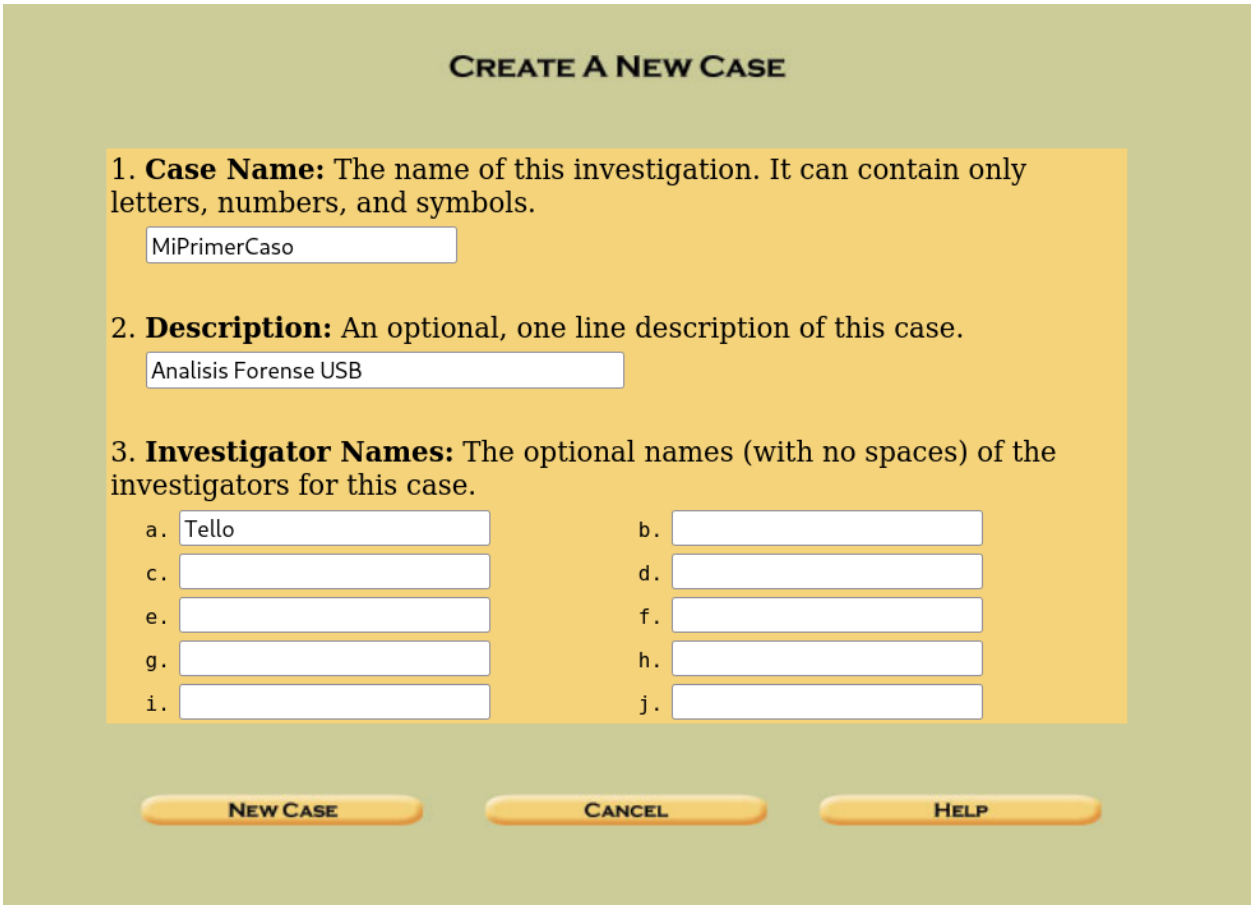
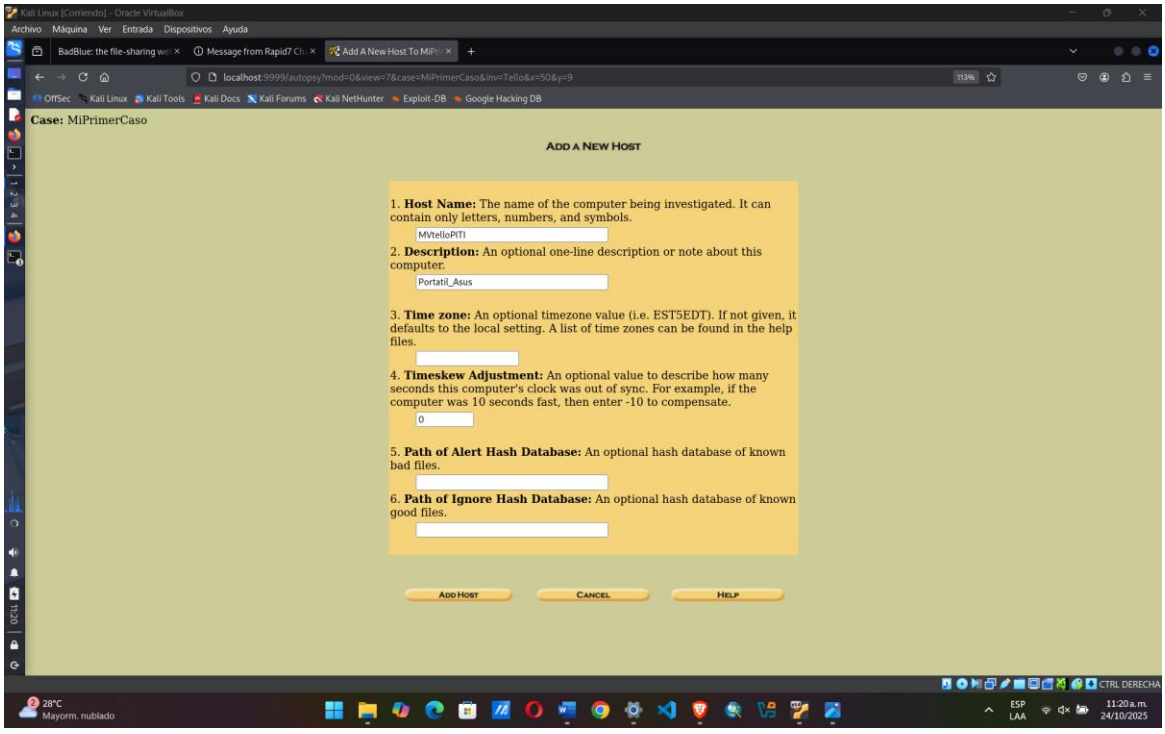



*Ilustración 7 Creación del caso forense*

El sistema redirigió a la sección de **Add Host**, donde añadí la información del dispositivo analizado y guardé los cambios.


*Ilustración 8 Add Host*

Al oprimir dicha opción se abre una nueva pagina que pide el nombre del dispositivo, descripción, entre otros datos. Se llenan los que se deseen y nuevamente se oprime la opción de add host.



Luego seleccioné **Add Image** para añadir la imagen forense previamente creada.

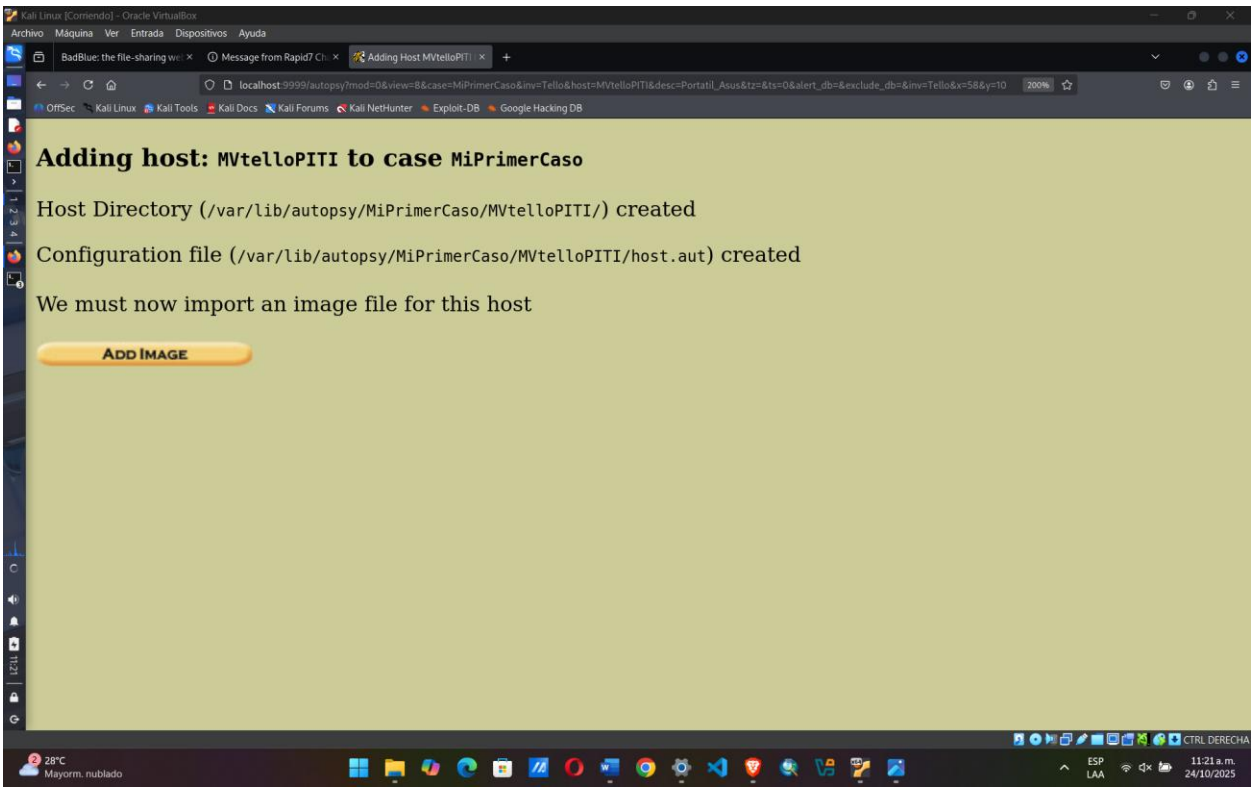



*Ilustración 9 Add Image*

Al hacer clic en **Add Image File**,

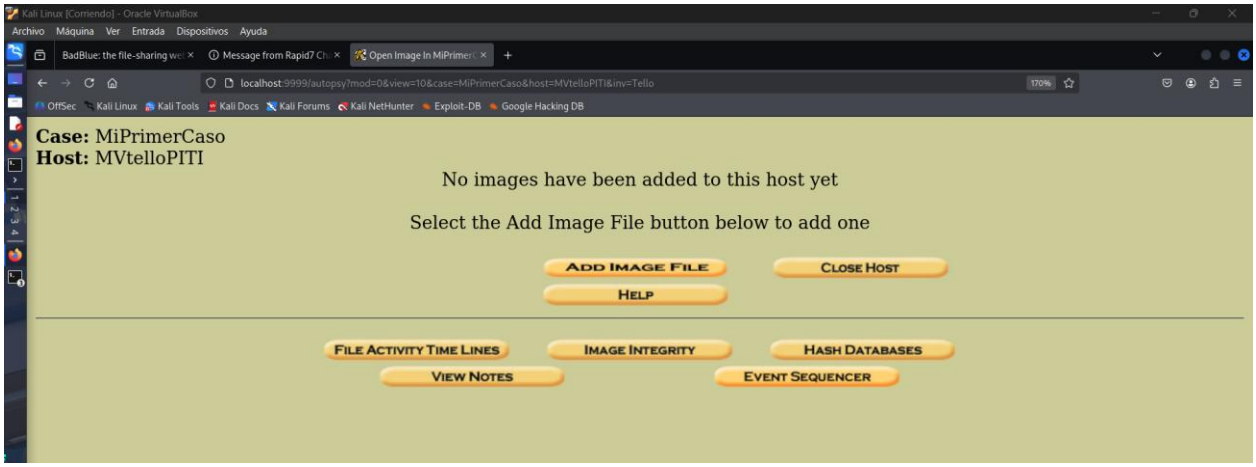



*Ilustración 10 Add Image File*

Autopsy me pidió la **ruta completa** del archivo. Pegué la dirección correspondiente a la imagen y seleccioné el tipo **Disk Image (dd)**. También elegí el primer método de importación (por defecto) y pulsé **Next**.

```
/home/tello/Escritorio/imagen_usb_forense_usb.dd
```

*Ilustración 11 ruta completa*

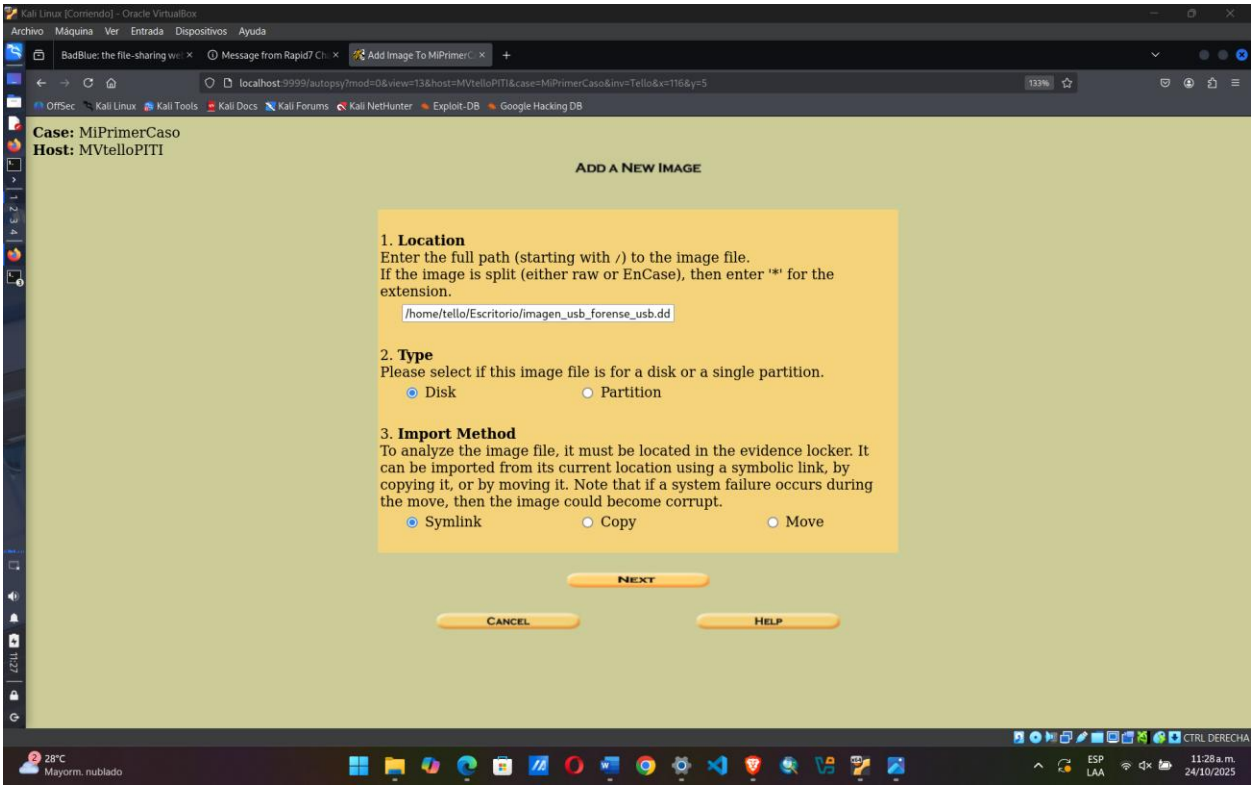



*Ilustración 12 Add a New Image*

Autopsy procesó la información y mostró un **resumen con los detalles de la imagen**, como:

- Sistema de archivos (FAT32/NTFS)
- Tamaño total
- Particiones encontradas

Finalmente, pulsé **Add Image** para continuar.

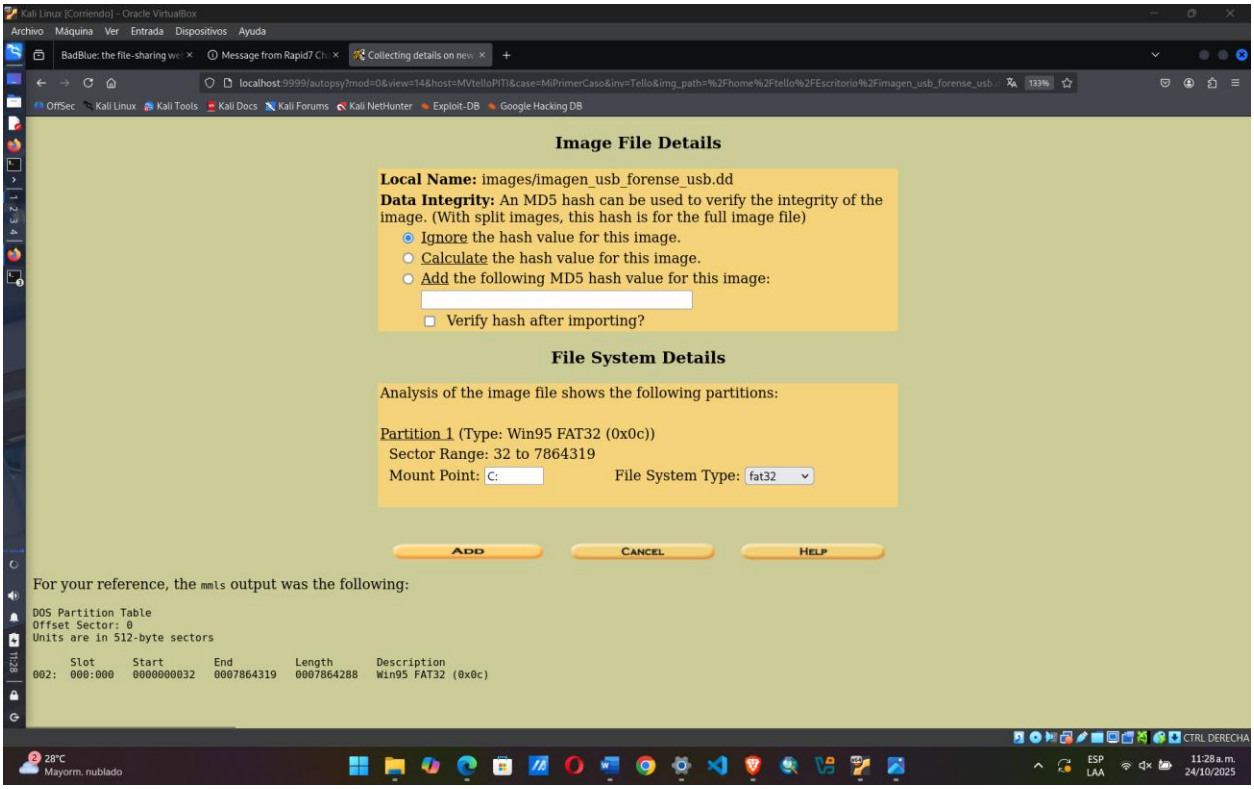
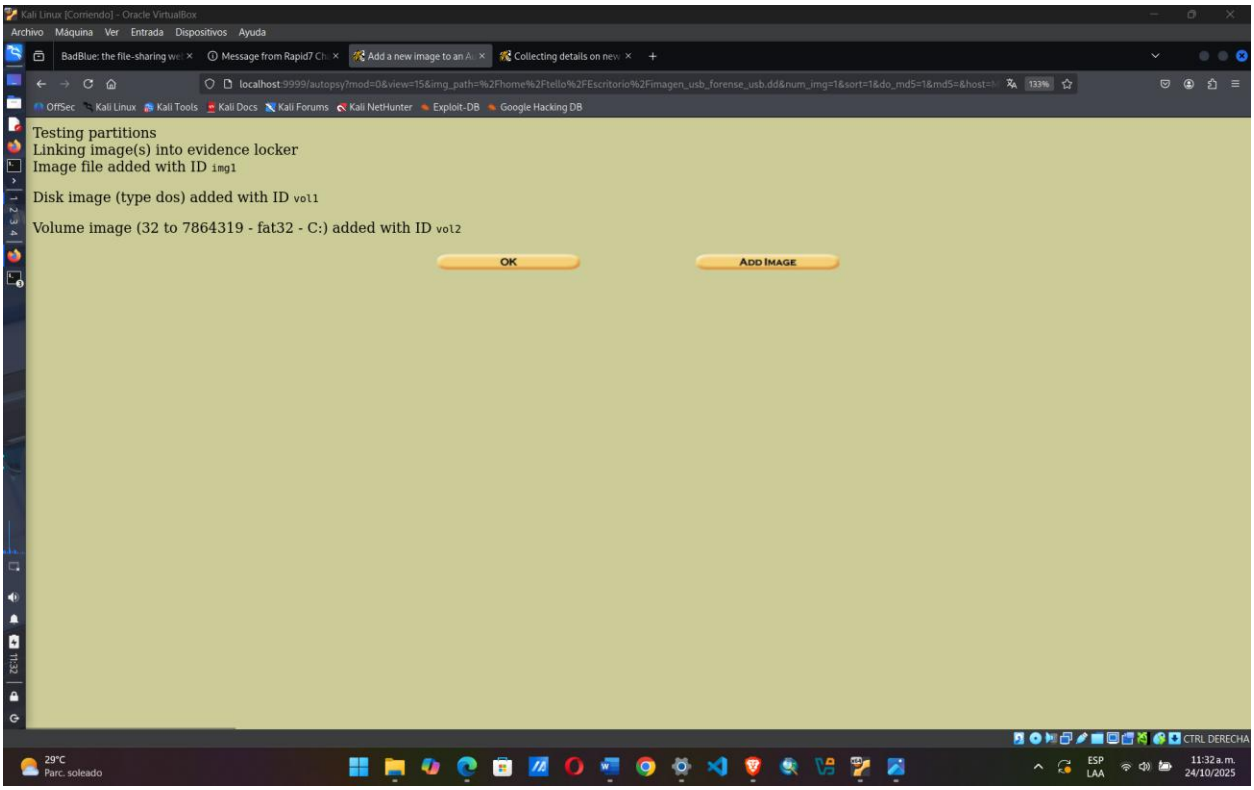


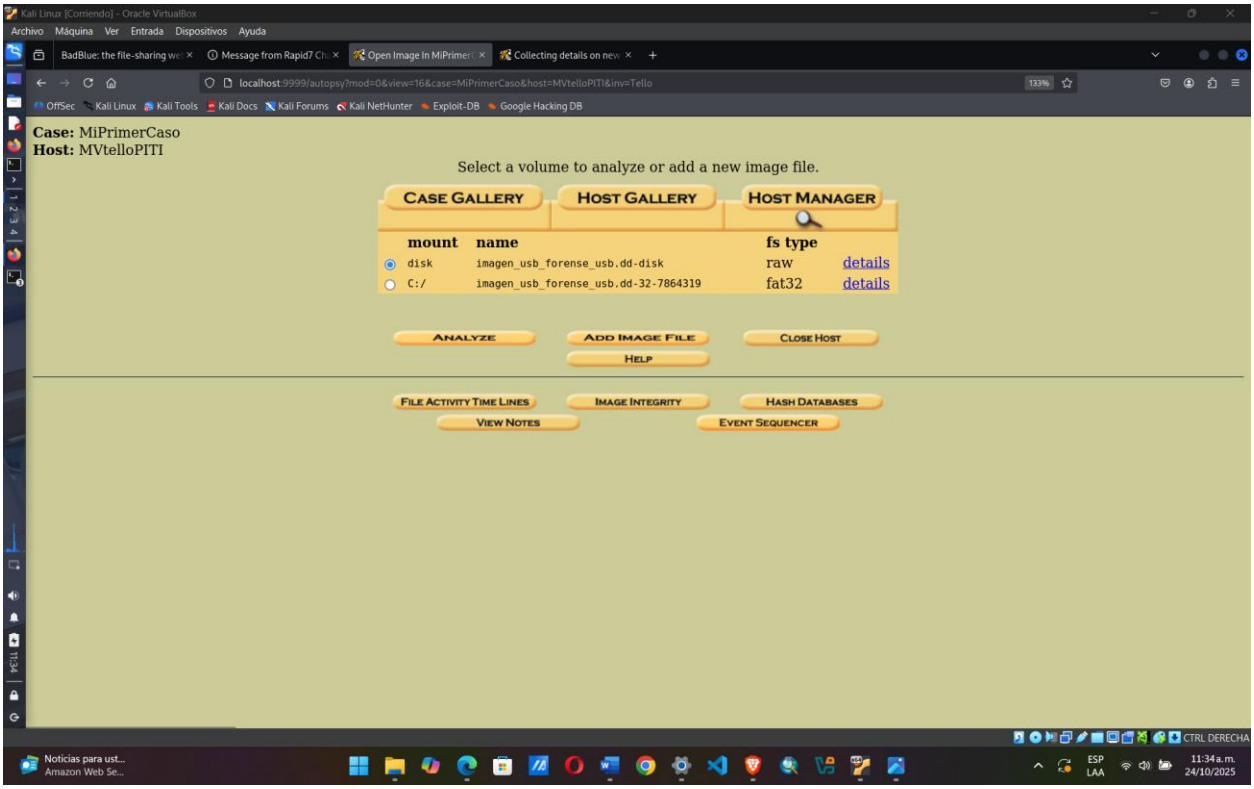

*Ilustración 13 Image file details*

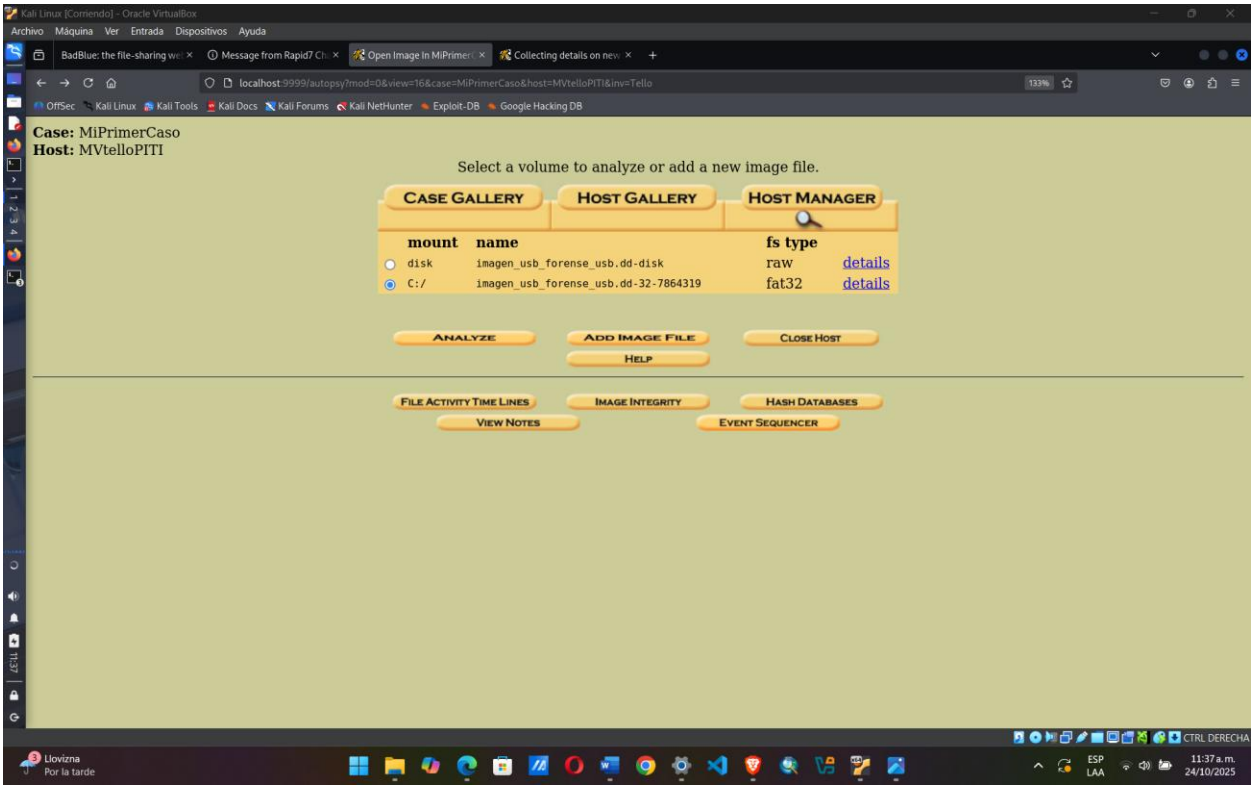


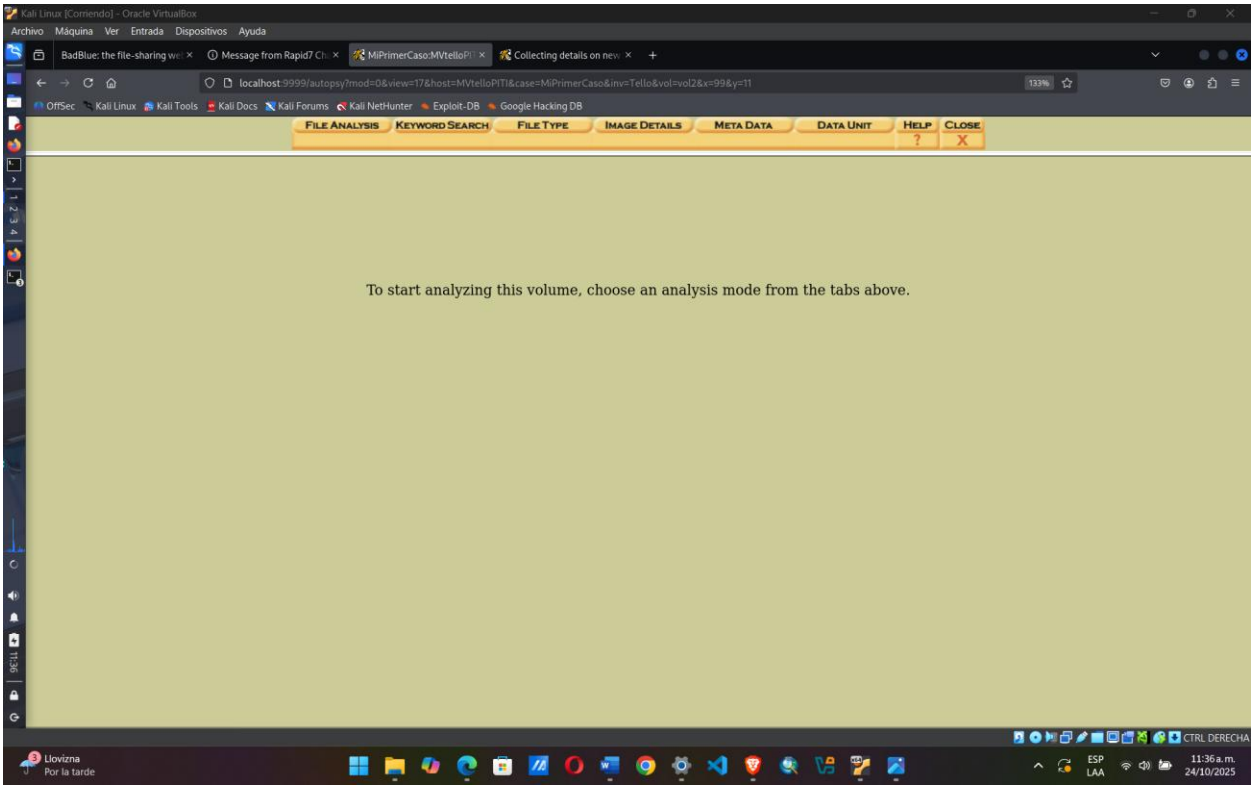
## 1.7 File Analysis: exploración de archivos y metadatos

1. Cuando el análisis avanzó, seleccioné la opción **File Analysis** para revisar los archivos encontrados.

Seleccionamos C y le damos ANALYZE




Case: MiPrimerCaso
Host: MVtelloPITI
Select a volume to analyze or add a new image file.
CASE GALLERY
HOST GALLERY
HOST MANAGER
mount
name
fs type
disk
imagen_usb_forense_usb.dd-disk
raw
details
C:/
imagen_usb_forense_usb.dd-32-7864319
fat32
details
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER


FILE ANALYSIS
KEYWORD SEARCH
FILE TYPE
IMAGE DETAILS
META DATA
DATA UNIT
HELP
CLOSE
To start analyzing this volume, choose an analysis mode from the tabs above.

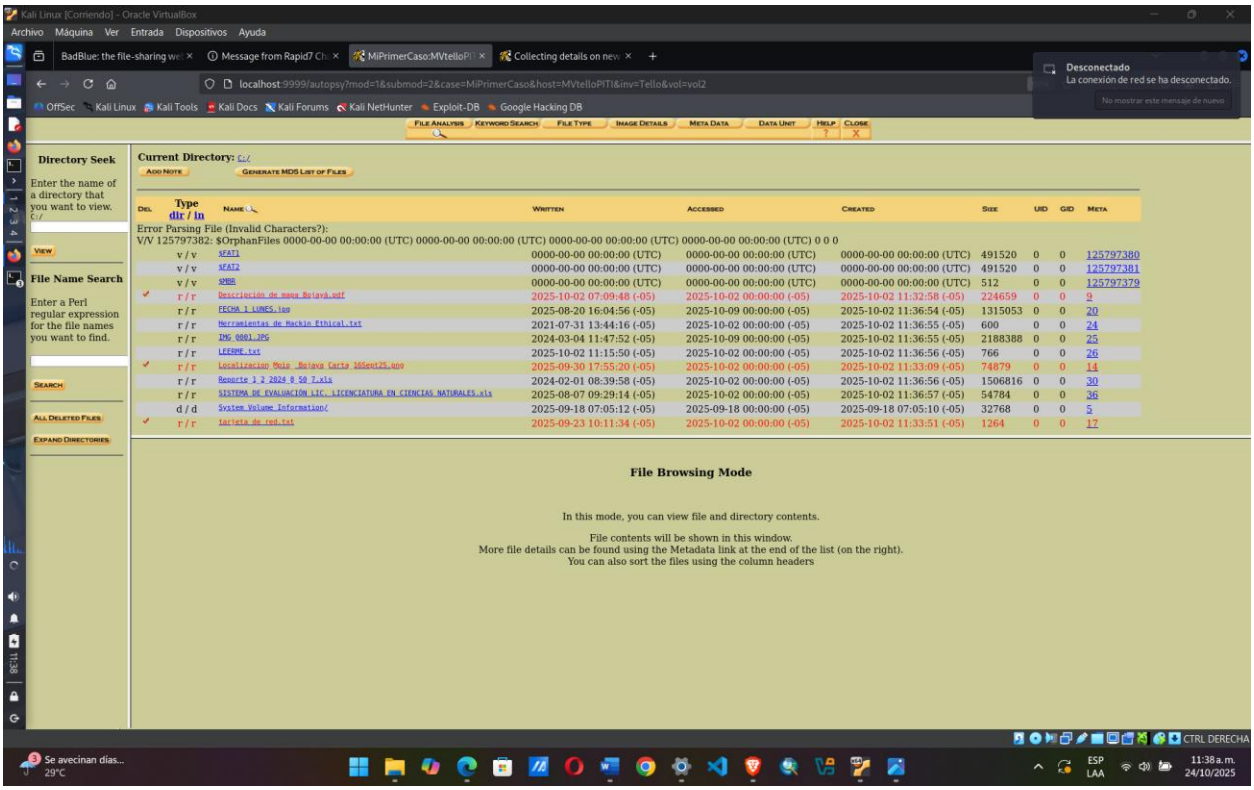
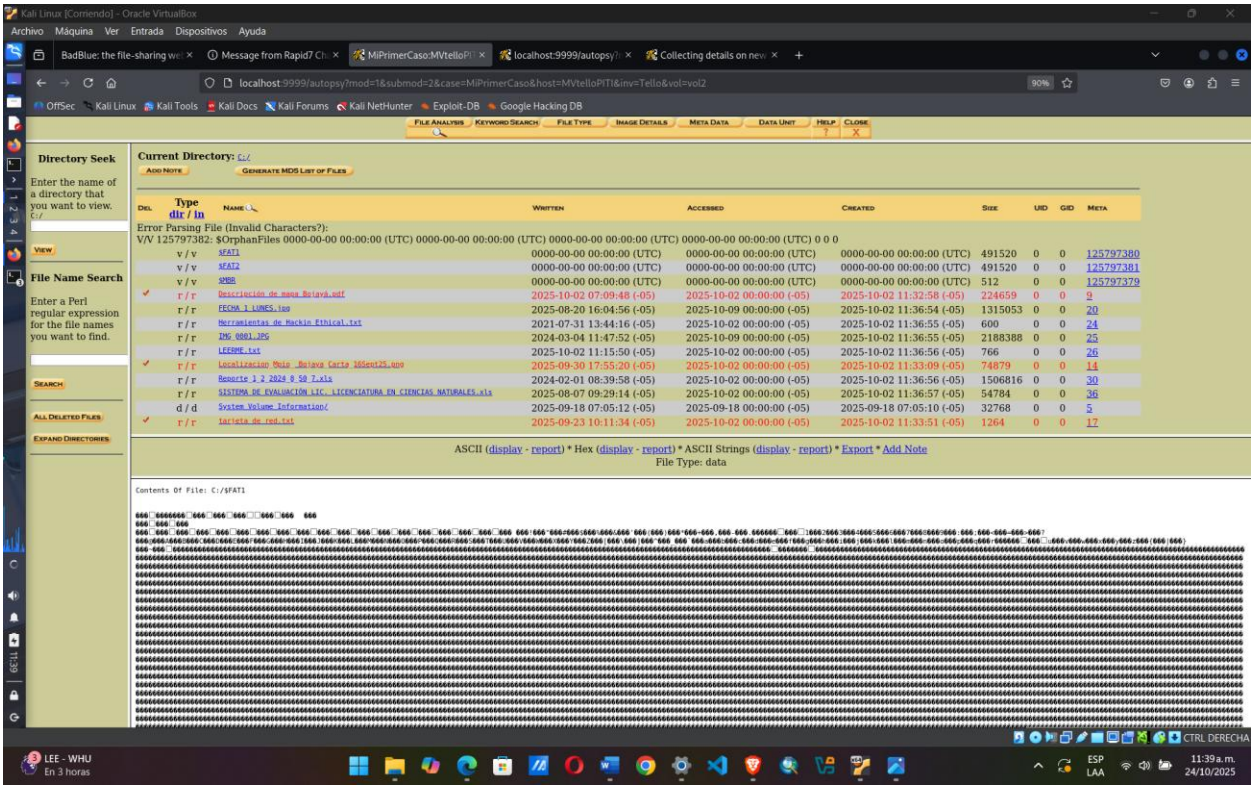



*Ilustración 14 FILE ANALYZE*

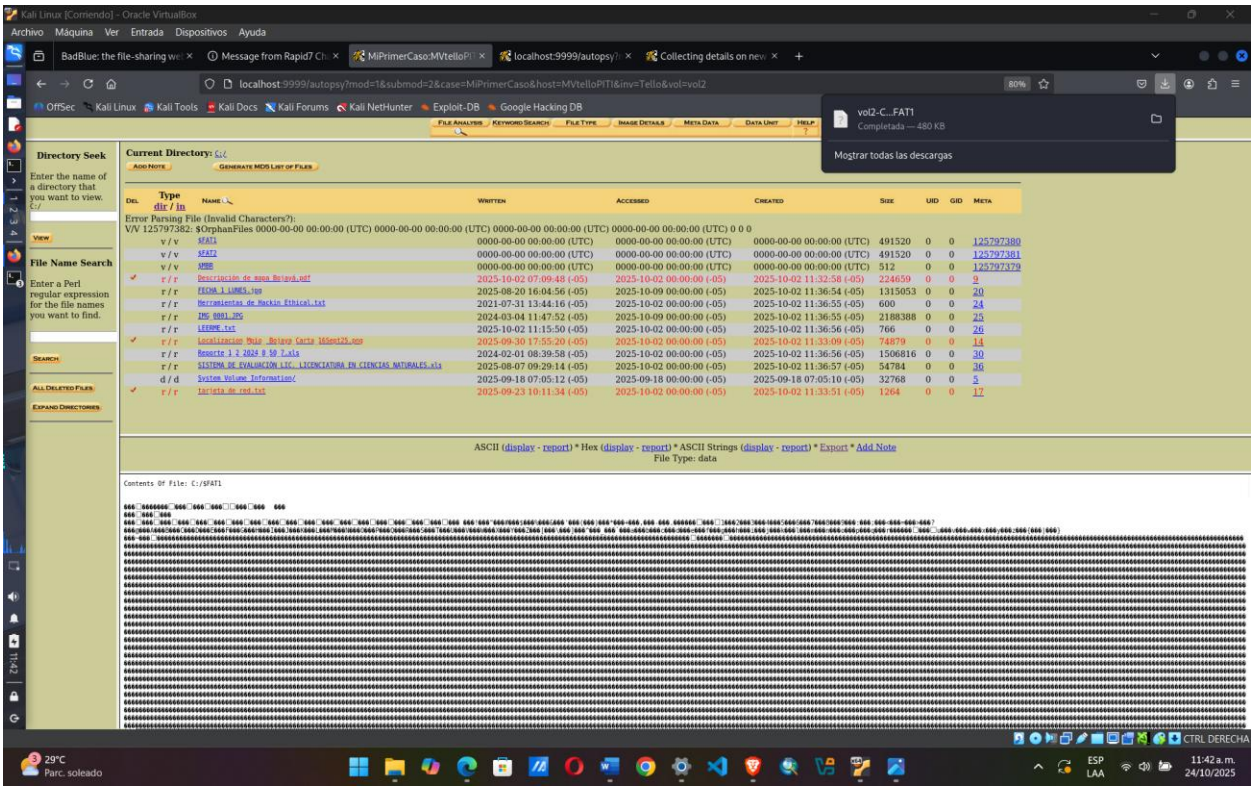
Qué se muestra: lista de archivos, archivos eliminados marcados en rojo, fechas (modified, accessed, created), tamaño y tipo.

Pude examinar archivos concretos: abrir previsualizaciones, revisar rutas y ver metadatos.

Si un archivo estaba eliminado, Autopsy mostraba indicaciones (borrado lógico, fragments).




Le damos Export



## 1.8 Generar lista MD5 de archivos inspeccionados

En la parte superior del panel de **File Analysis** se encuentra la opción **Generate MD5 List of Files**. seleccioné dicha opción para que Autopsy calcule el **MD5** de cada archivo ya procesado/visualizado: esto produce un listado con pares ruta, MD5.

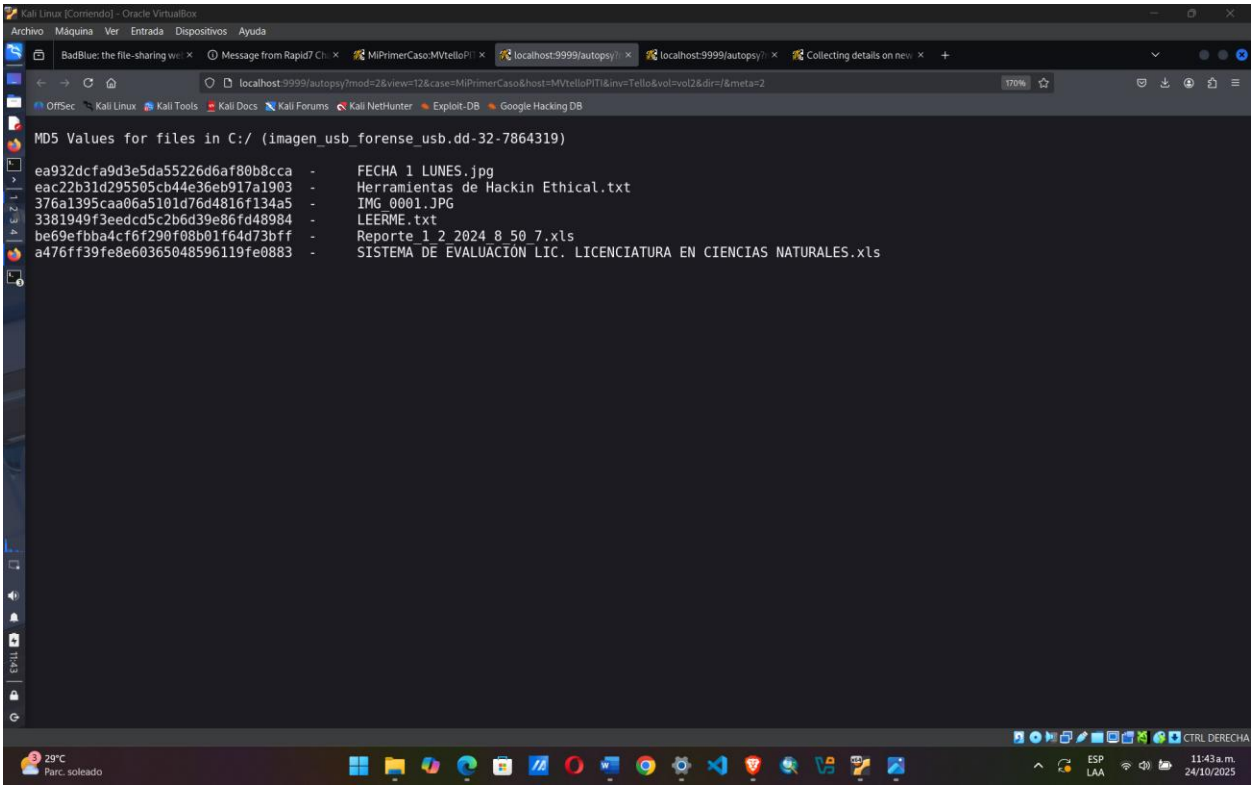



*Ilustración 15 Generar lista MD5 de archivos inspeccionados*

Posteriormente, exploré la sección **Image Details**, donde Autopsy despliega los metadatos de la imagen forense analizada.

Allí se puede consultar el **tipo de sistema de archivos (por ejemplo FAT32, NTFS, ext4, etc.)**, el **nombre del dispositivo original**, la **capacidad total** de la unidad, así como su **estructura de particiones**.

Estos datos son esenciales para corroborar que la imagen se generó correctamente, sin errores, y que conserva la estructura lógica del dispositivo físico original.

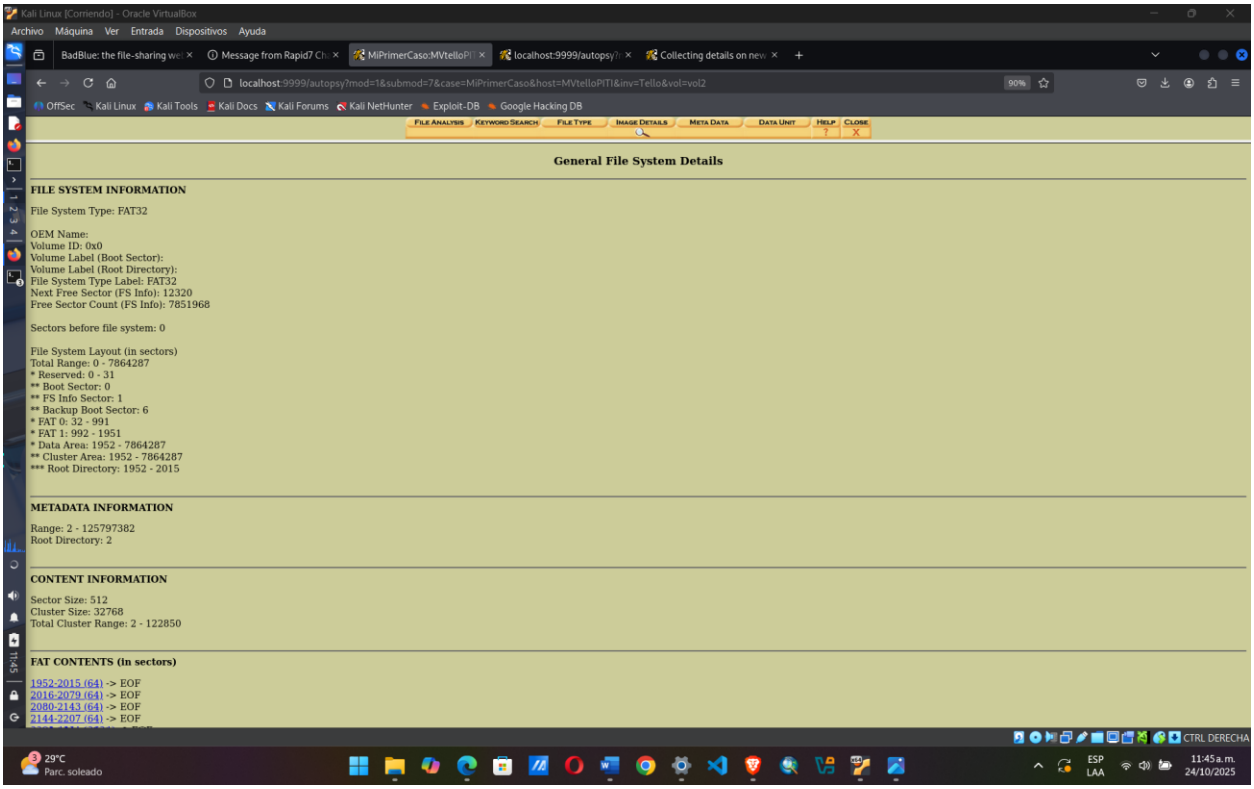
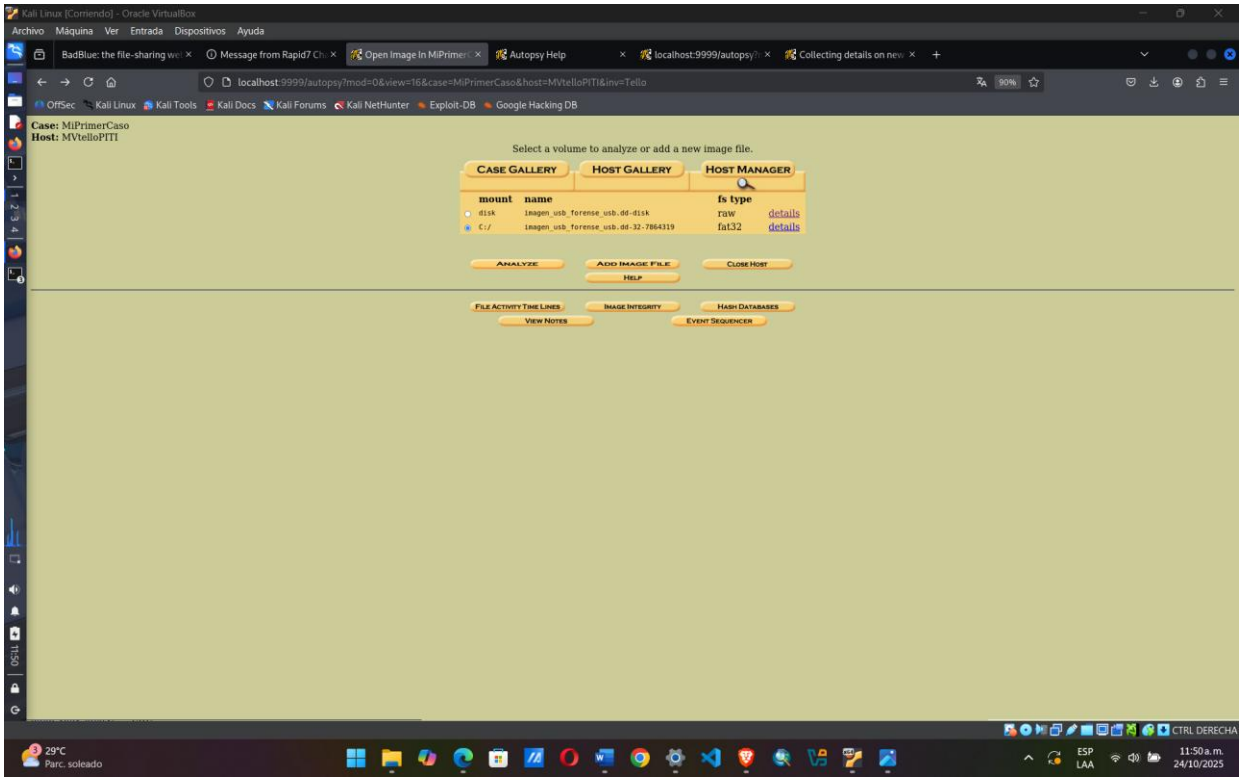



*Ilustración 16 IMAGE DETAILS*

## 1.9 Image Integrity — cálculo y confirmación

En la interfaz de Autopsy existe una sección para **Image Integrity** que permite calcular y verificar el hash global de la imagen; entré en esa opción y ejecuté **Calculate** (tal como se aprecia en tu captura).

Tras el cálculo, Autopsy muestra el valor del hash calculado y su estado (coincidente / no coincidente) respecto al valor de referencia si se ha cargado. Autopsy muestra el resultado de Calculate y el panel inferior con la salida).



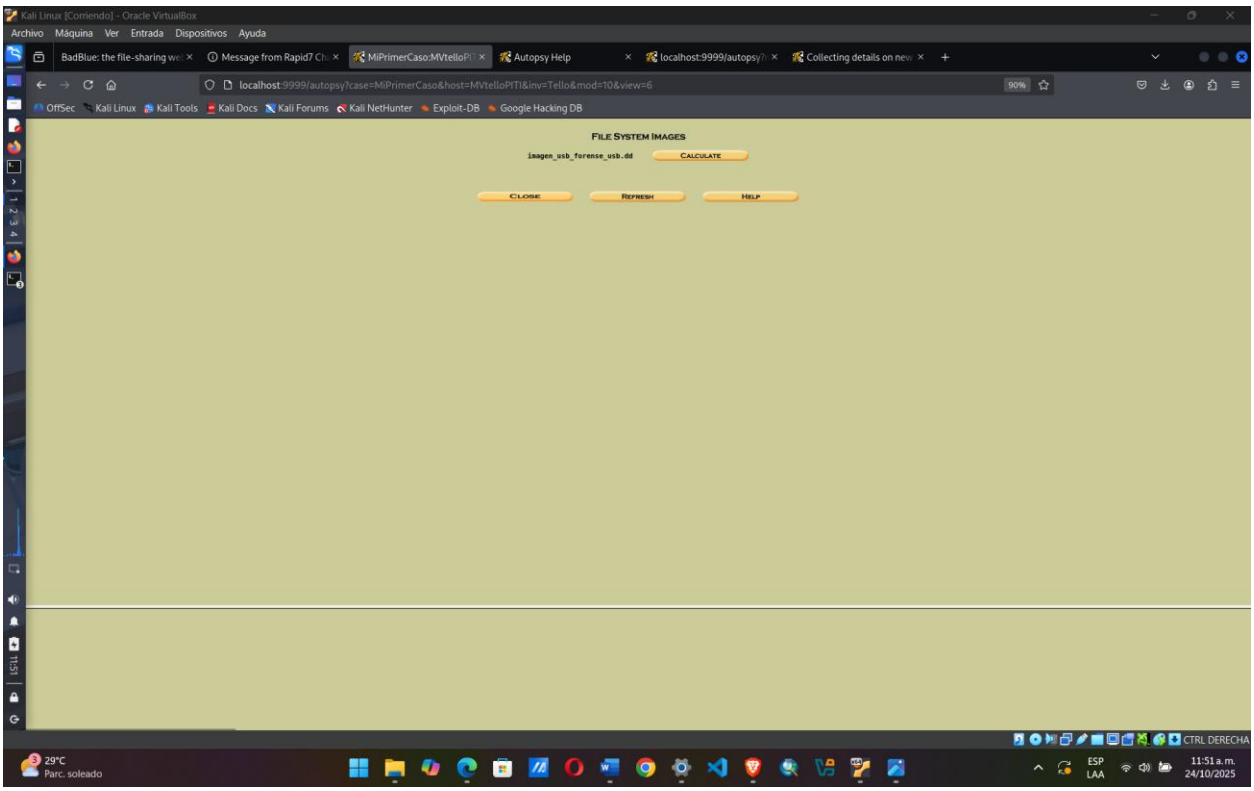




*Ilustración 17 Image Integrity*

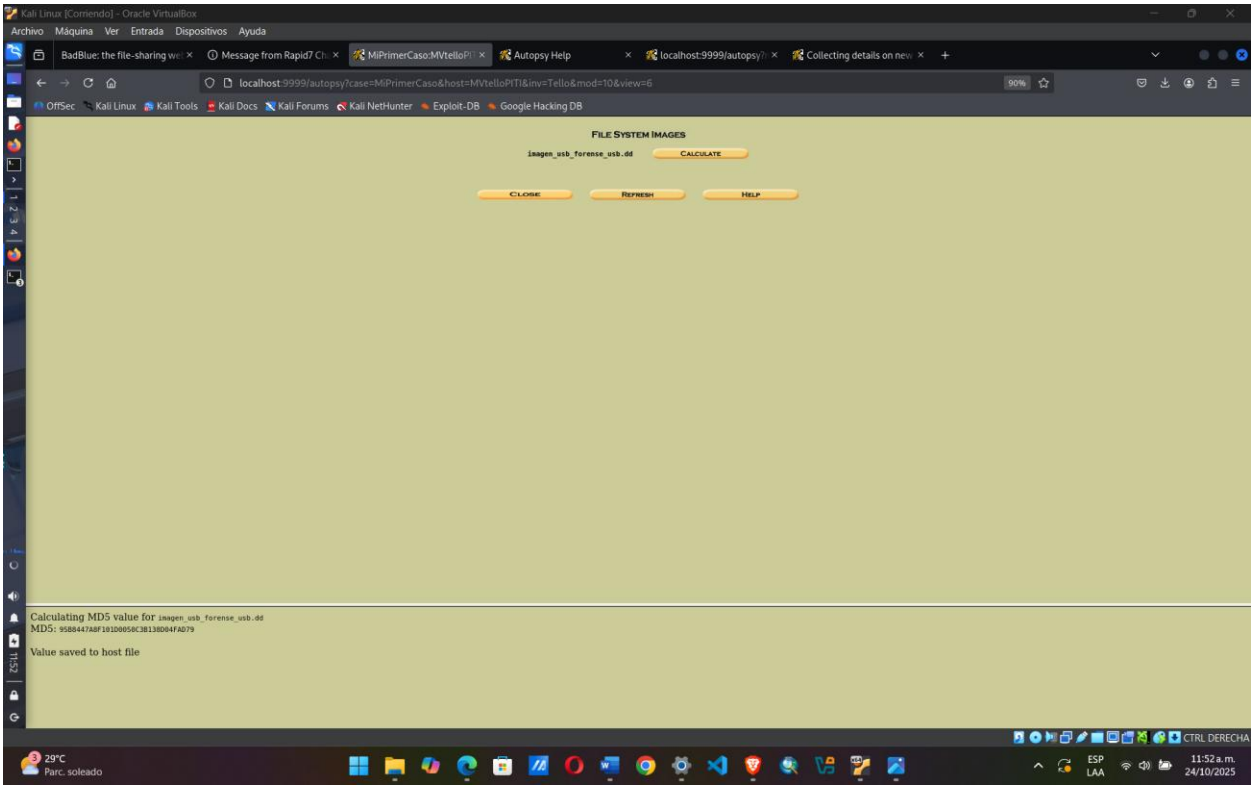



*Ilustración 18 calculate*

# 2 CAPÍTULO 2 DESCARGAR AUTOSY EN WINDOWS Y ANALISIS FORENSE EN WINDOWS

## 2.1 Transferencia de la imagen desde Kali Linux hacia el sistema Windows

Una vez finalizado el análisis inicial de la imagen forense en **Kali Linux**, fue necesario **transferir el archivo de imagen (.dd)** al sistema **Windows** para continuar con las siguientes fases del laboratorio, que incluían el uso de **Autopsy** y **FTK Imager** en ese entorno.

Para realizar esta transferencia de forma sencilla dentro del entorno virtualizado, configuré las opciones de **VirtualBox** para habilitar el **portapapeles compartido**.

Desde el menú superior de la máquina virtual seleccioné **Dispositivos → Portapapeles compartido**, y verifiqué que estuviera en modo **Bidireccional**. También activé la opción **Enable Clipboard File Transfers**, que permite copiar y pegar archivos directamente entre la máquina virtual de Kali y el sistema operativo anfitrión (Windows). Estas configuraciones son útiles en entornos de práctica, ya que facilitan el intercambio de archivos sin necesidad de servicios externos ni montajes de red adicionales.

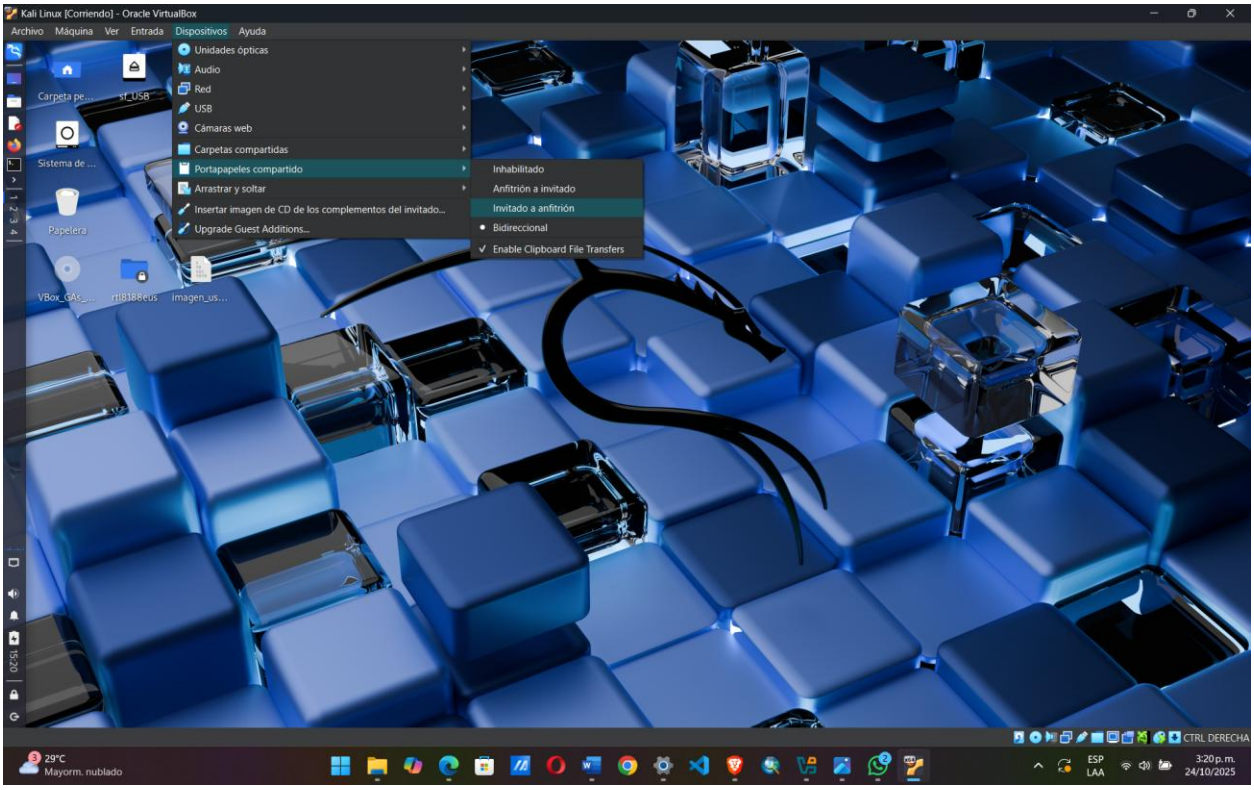



*Ilustración 19 portapapeles compartido*

Una vez confirmadas las opciones de transferencia, me dirigí al directorio donde se encontraba almacenada la imagen forense, en este caso el archivo **imagen_usb_forense.dd**, ubicado en el escritorio de Kali.

Hice clic derecho sobre el archivo y seleccioné la opción **Copiar**, con el fin de preparar el archivo para su traslado hacia el entorno Windows.

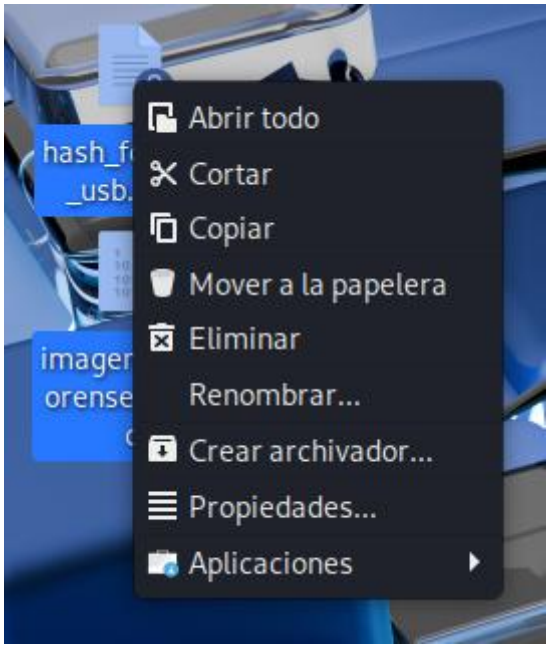



*Ilustración 20 Copiar archivos*

Posteriormente, en el sistema anfitrión (Windows), abrí la carpeta donde deseaba guardar la copia del archivo y seleccioné **Pegar**.

Una vez concluida la operación, pude verificar que el archivo **imagen_usb_forense.dd** se encontraba correctamente copiado en la carpeta seleccionada dentro de Windows. Este paso confirmó que la imagen forense fue transferida de manera íntegra, manteniendo su tamaño y estructura original, lista para ser analizada posteriormente con **Autopsy en Windows** y **FTK Imager**.

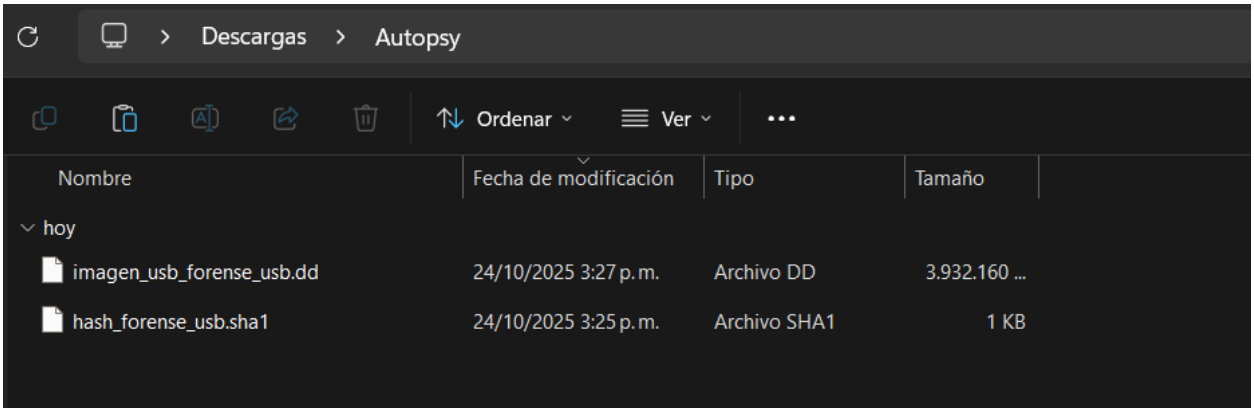


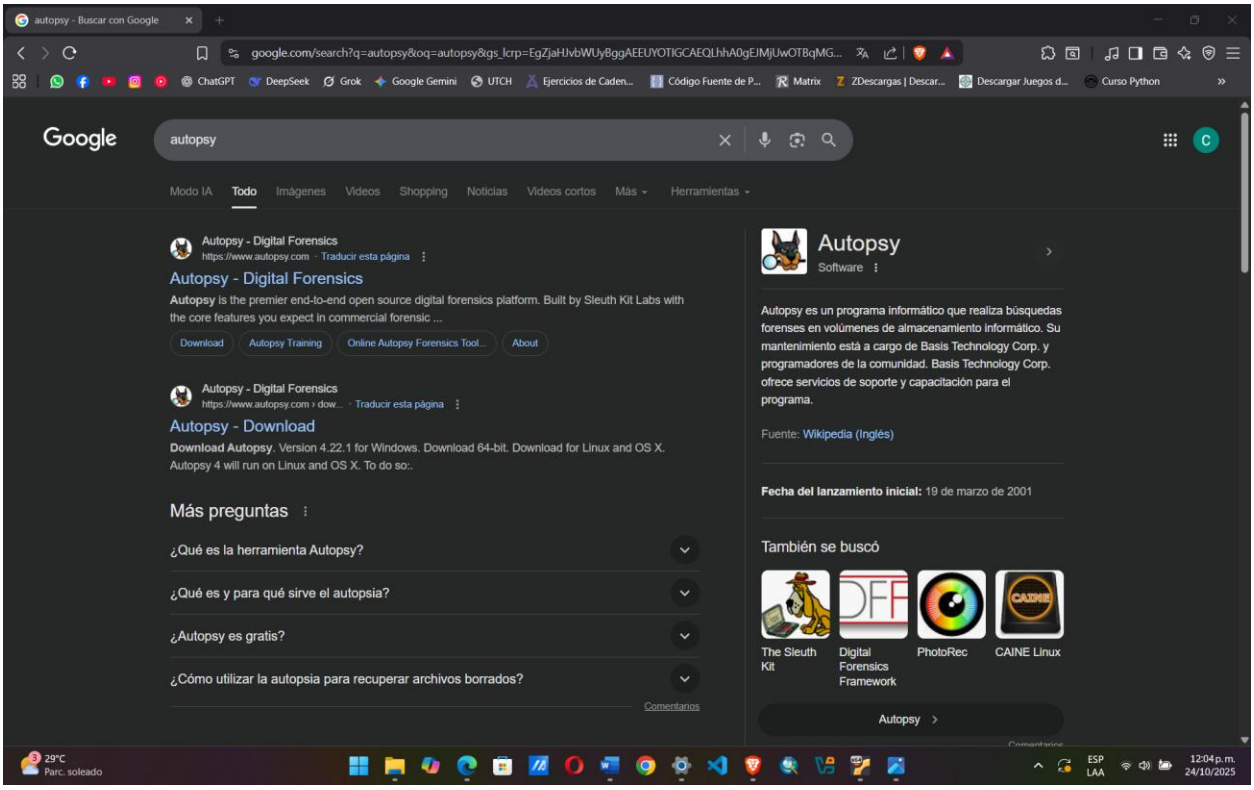

*Ilustración 21 Archivosa pegados en Windows*

## 2.2 Instalación de Autopsy

## 2.3 Búsqueda y descarga del instalador

El primer paso consistió en **buscar el instalador de Autopsy** para Windows.

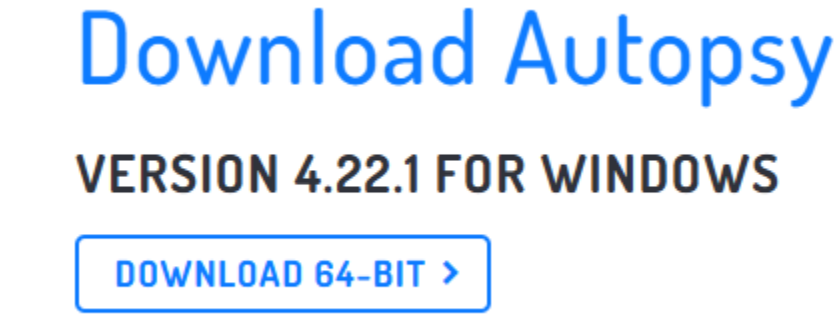
Desde el navegador accedí al buscador y escribí:

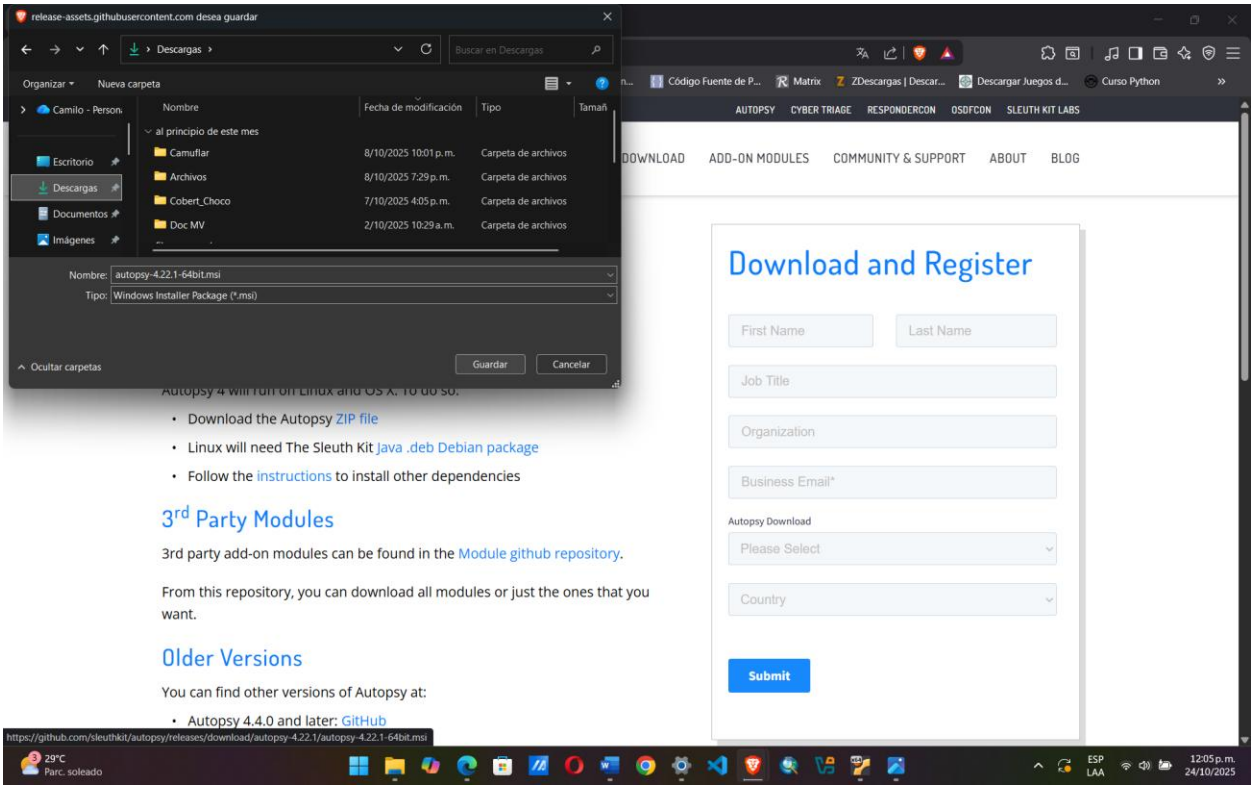


Entre los resultados, seleccioné el enlace oficial de **Autopsy (sleuthkit.org)**, donde se encuentra la versión más reciente del programa.

Una vez dentro del sitio, ubiqué la sección de descargas y procedí a descargar el archivo ejecutable (.exe) correspondiente al instalador.

El archivo se guardó en la carpeta **Descargas** del sistema.



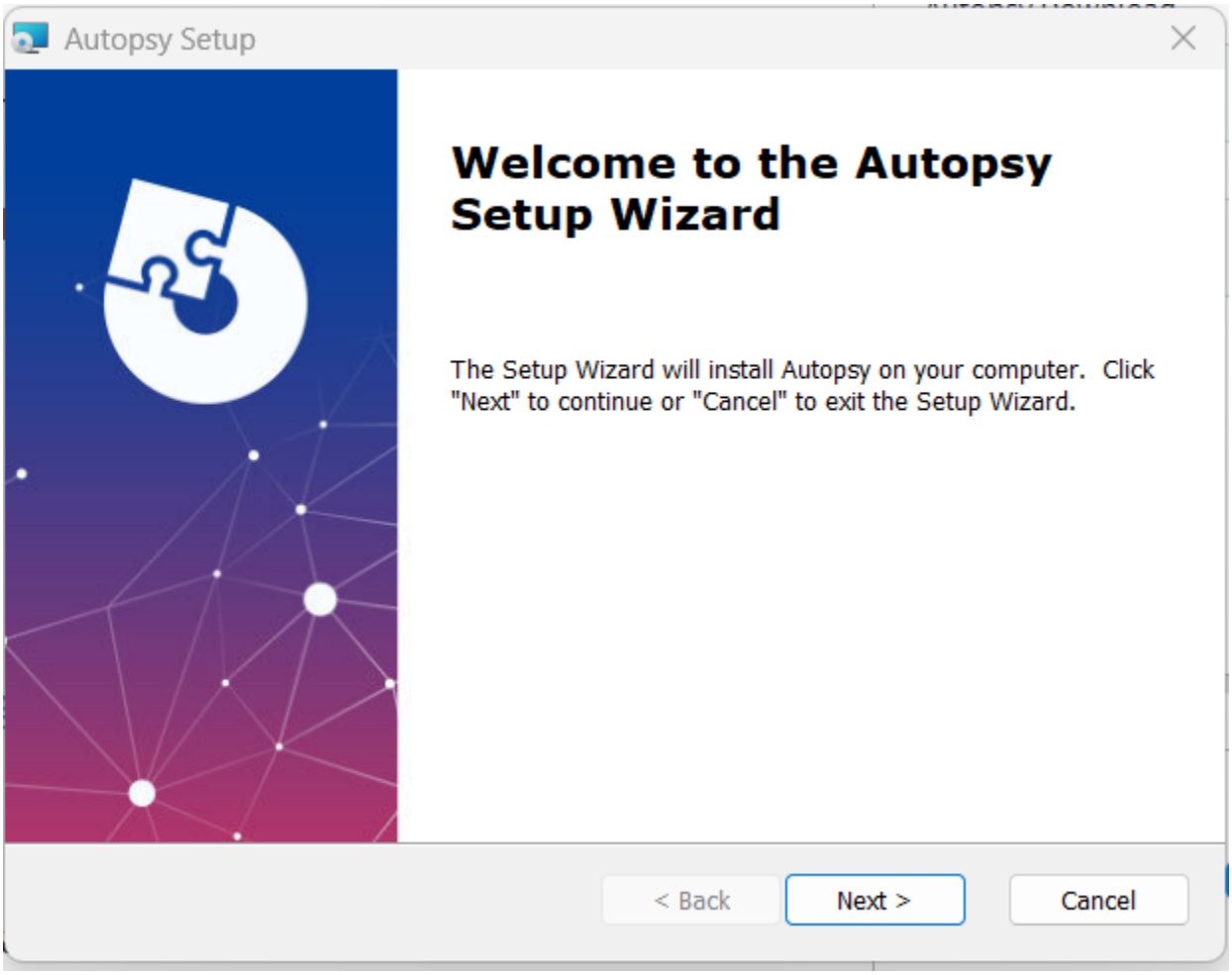



### 2.3.1 Ejecución del instalador

Con la imagen forense ya copiada desde Kali Linux al sistema anfitrión, se procedió a instalar **Autopsy** en **Windows** para realizar el análisis en este entorno.

El primer paso consistió en **ejecutar el instalador previamente descargado**.

Aparece el asistente de instalación, en el cual se selecciona **Next** para continuar.



### 2.3.2 Inicio del proceso de instalación

Después de confirmar la ruta de instalación, se hace clic nuevamente en **Next**, lo que da inicio al proceso de instalación.

En esta etapa, el sistema muestra una barra de progreso que indica el avance de la copia de archivos y configuración del entorno.

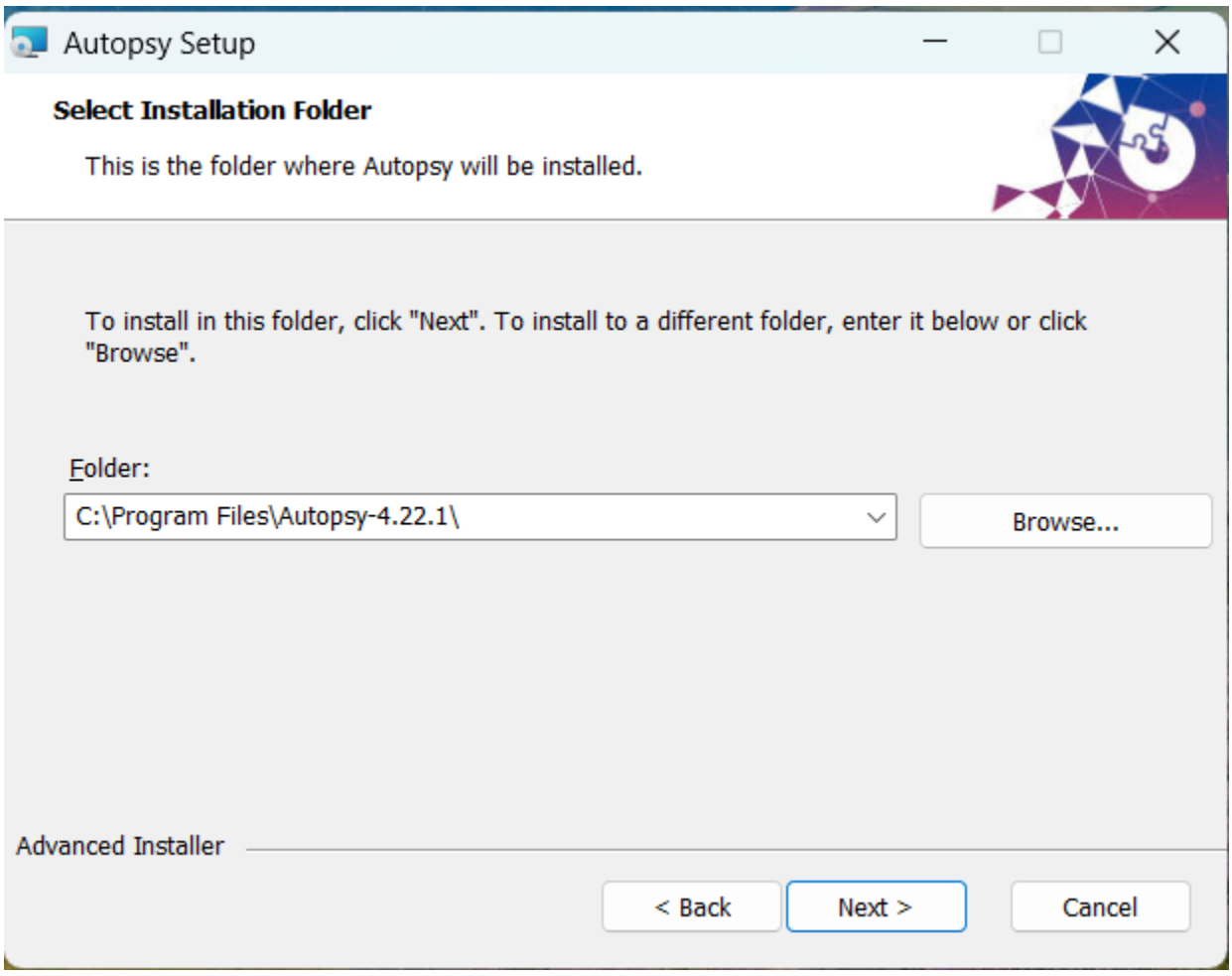
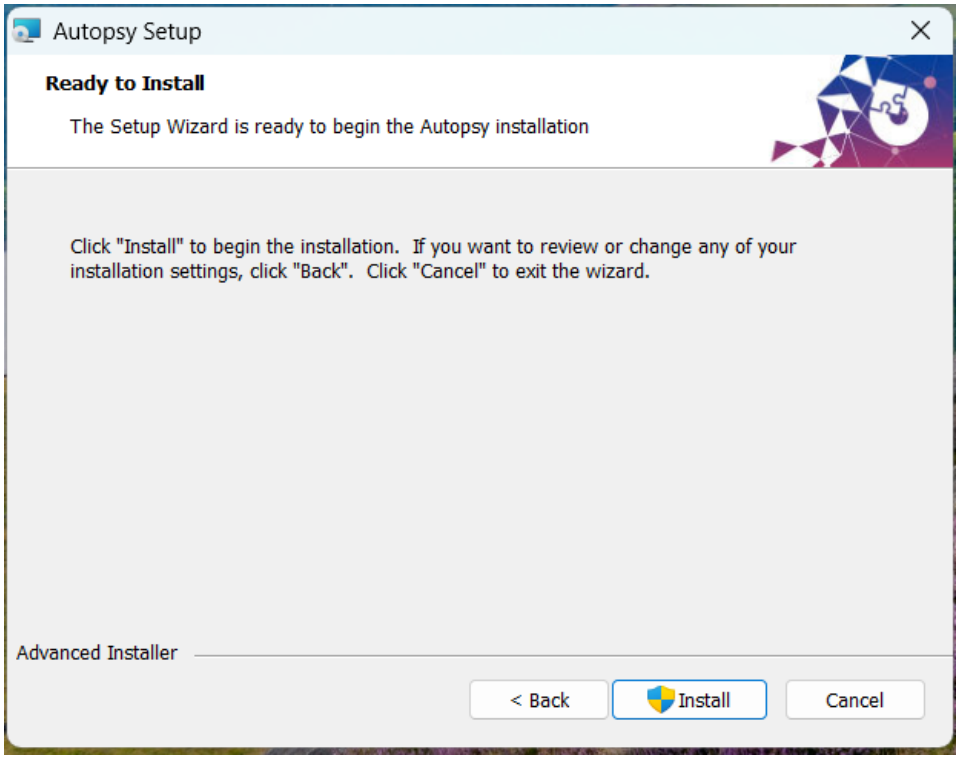



*Ilustración 22 Ruta instalacion autopsy*

Durante el proceso, **Windows solicita permisos de administrador** para permitir la instalación; se acepta para continuar correctamente. Una vez finalizado, el instalador muestra una ventana de confirmación indicando que la instalación se ha completado con éxito. Finalmente, se hace clic en **Finish** para cerrar el asistente.



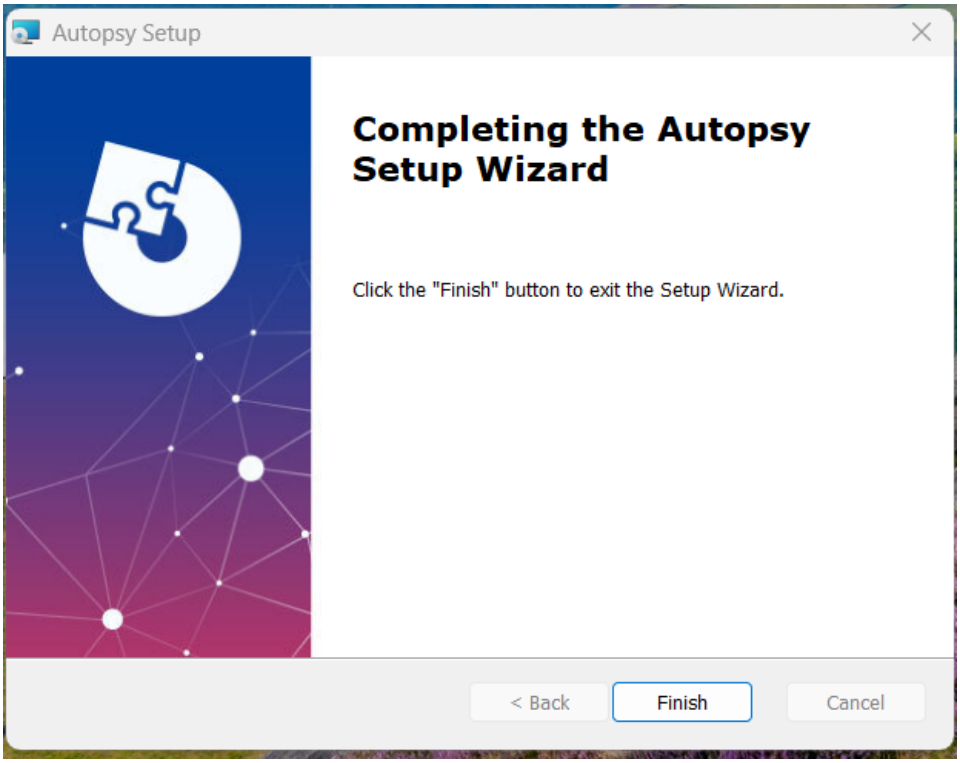



*Ilustración 23 Finalización instalación autopsy*

### 2.3.3 Ejecución de la aplicación

Tras completar la instalación, se ejecuta Autopsy desde el menú de inicio o desde el acceso directo en el escritorio.

La herramienta se inicia mostrando una interfaz limpia con opciones para crear o abrir casos forenses.


*Ilustración 24 Autopsy*

## 2.4 Inicio de un nuevo caso

Al abrir Autopsy, se muestra una pantalla con las opciones principales del programa: **New Case**, **Open Case** y **Recent Cases**.

Seleccioné **New Case** para crear un nuevo análisis.

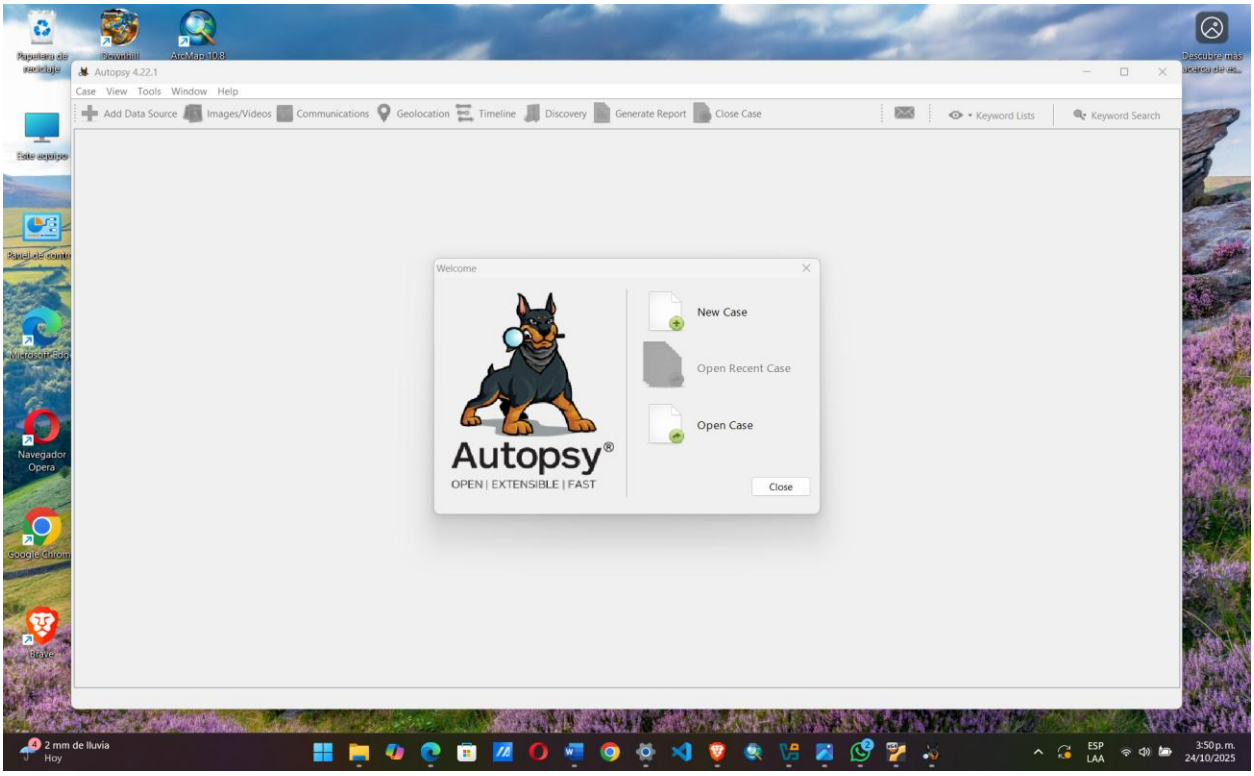



*Ilustración 25Creación de un nuevo caso (New Case)*

## 2.5 Configuración de la información del caso

El sistema solicita la información básica del nuevo caso, incluyendo:

- **Case Name:** nombre del caso.
- **Case Directory:** ruta donde se almacenarán los archivos generados.
- **Case Number (opcional):** identificador del análisis.

Se define la carpeta donde se guardará el caso y se continúa con **Next**.

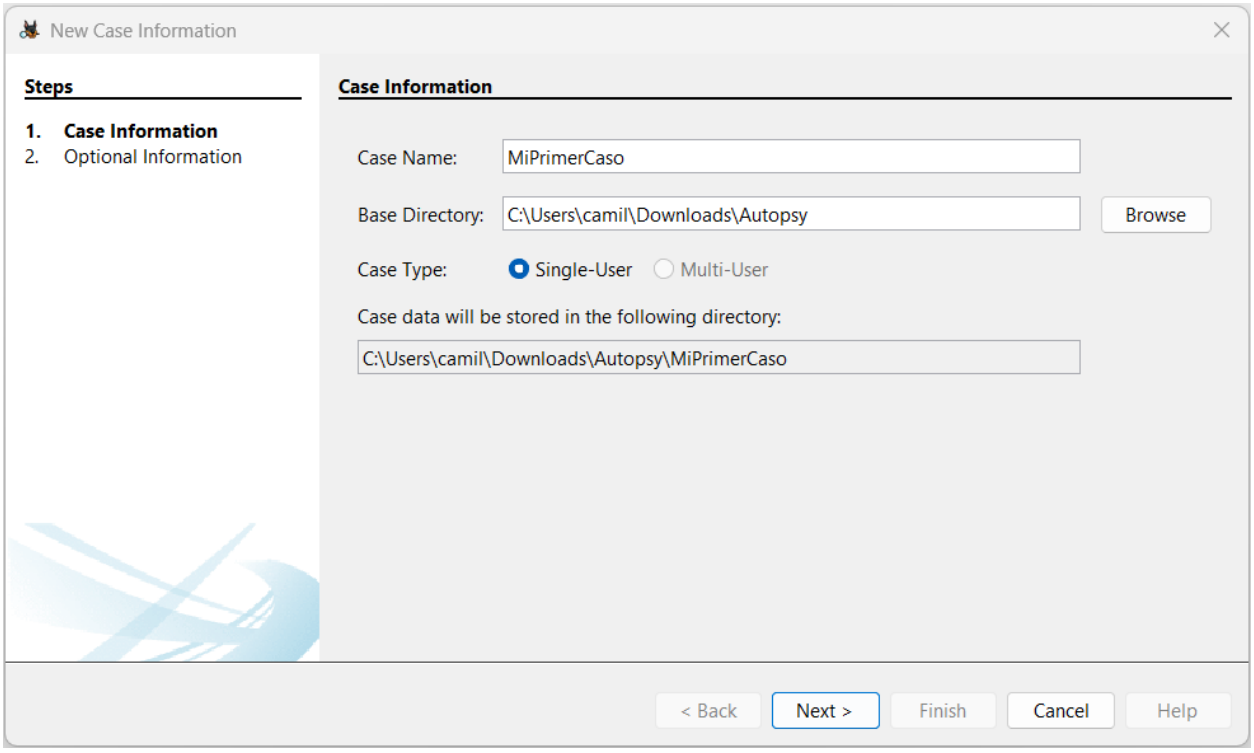



*Ilustración 26 Información del caso*

## 2.6 Datos del examinador

A continuación, Autopsy solicita los **datos del examinador**, como el nombre del analista, organización y comentarios adicionales. Estos datos son útiles para identificar quién realizó el análisis y documentar la autoría del informe.

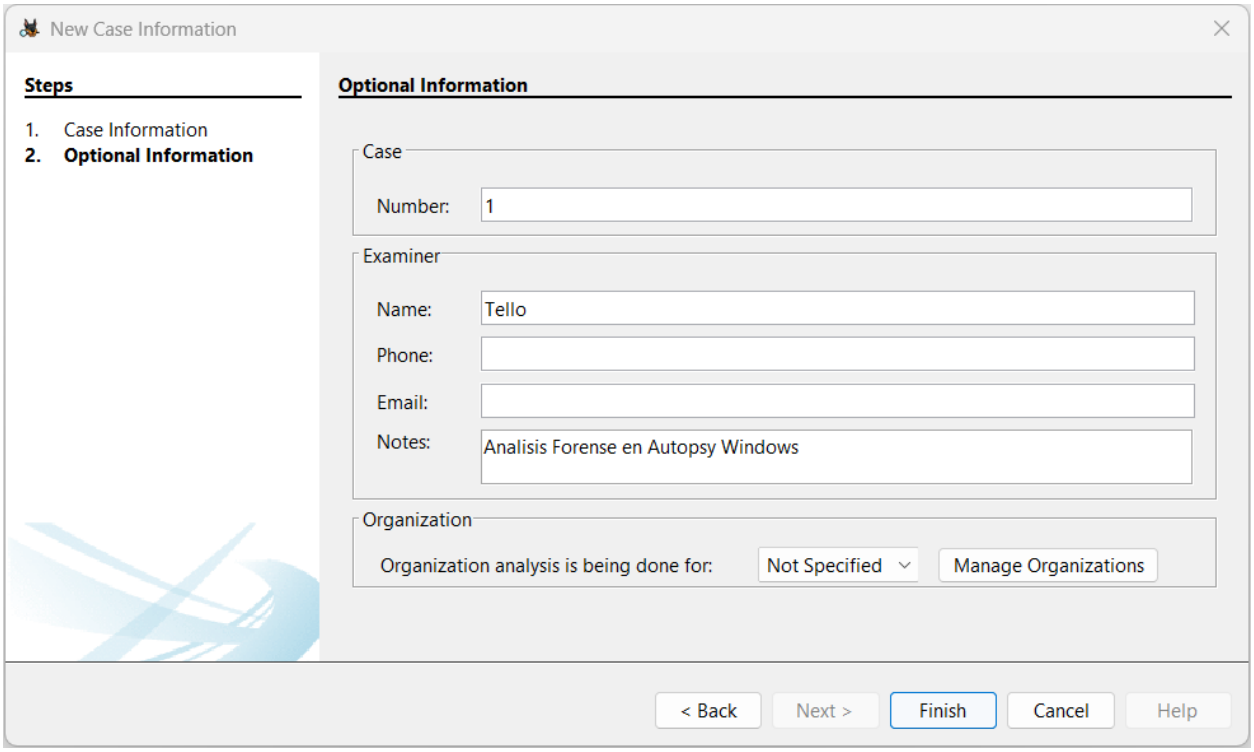



*Ilustración 27 Datos del examinador*

## 2.7 Creación del entorno de trabajo

Finalmente, se crea la estructura de directorios del caso, donde Autopsy almacenará automáticamente los logs, bases de datos y reportes. Una vez completado, aparece un mensaje indicando que el caso fue creado exitosamente.

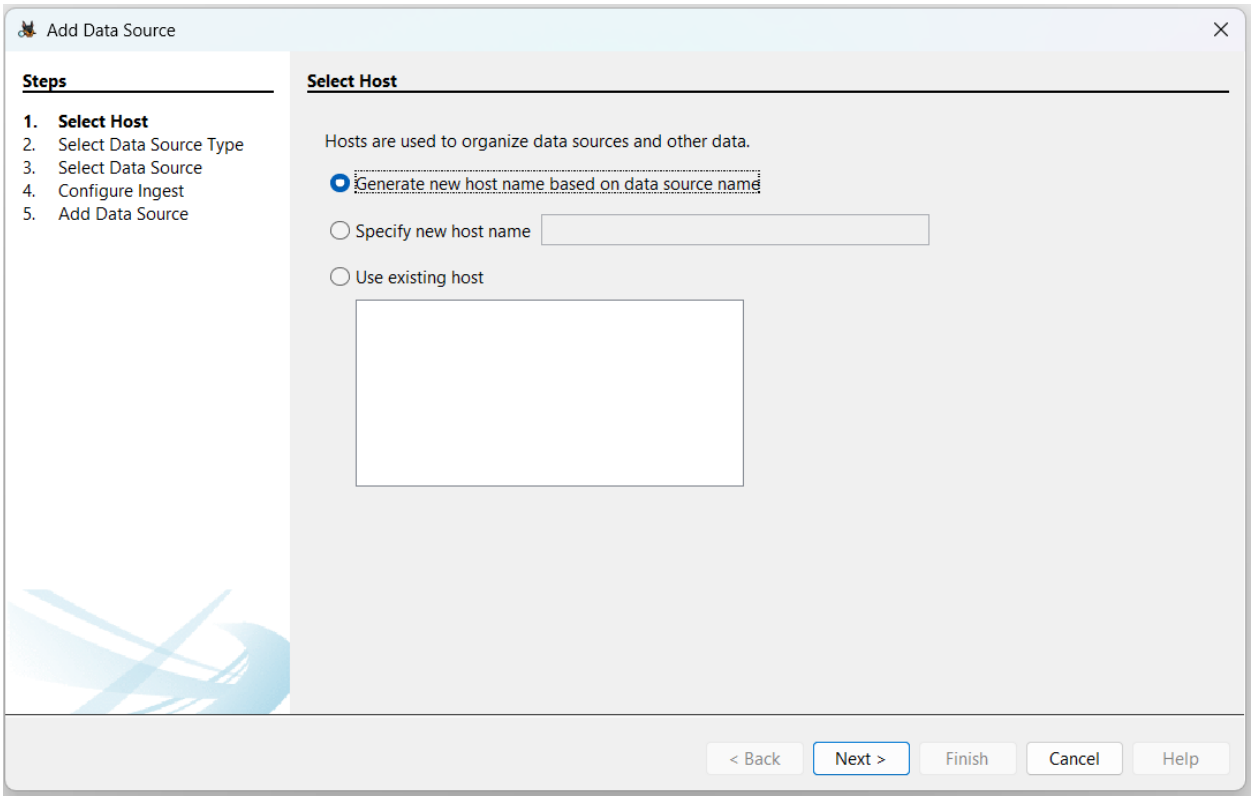



*Ilustración 28 Creación del entorno de trabajo*

## 2.8 Adición de la imagen forense

### 2.8.1 Selección de tipo de fuente de datos

Con el caso creado, Autopsy solicita agregar una **fuente de datos (Data Source)**. Para este laboratorio se seleccionó la opción correspondiente a **una imagen o disco local**.

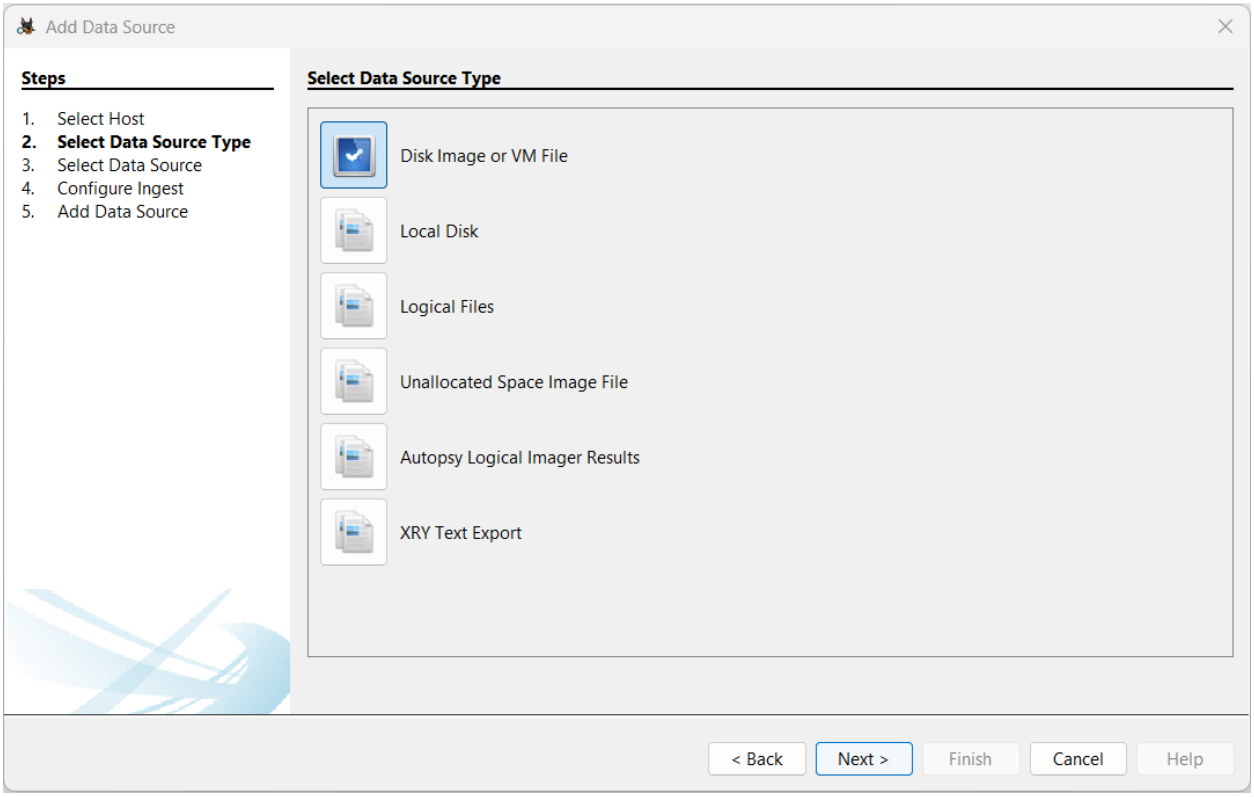



*Ilustración 29 Selección de tipo de fuente de datos*

### 2.8.2 Selección del archivo de imagen

Posteriormente, se navega por el sistema hasta ubicar el archivo **imagen_usb_forense.dd**, que fue copiado desde Kali Linux.

Se selecciona el archivo y se continúa con el proceso.

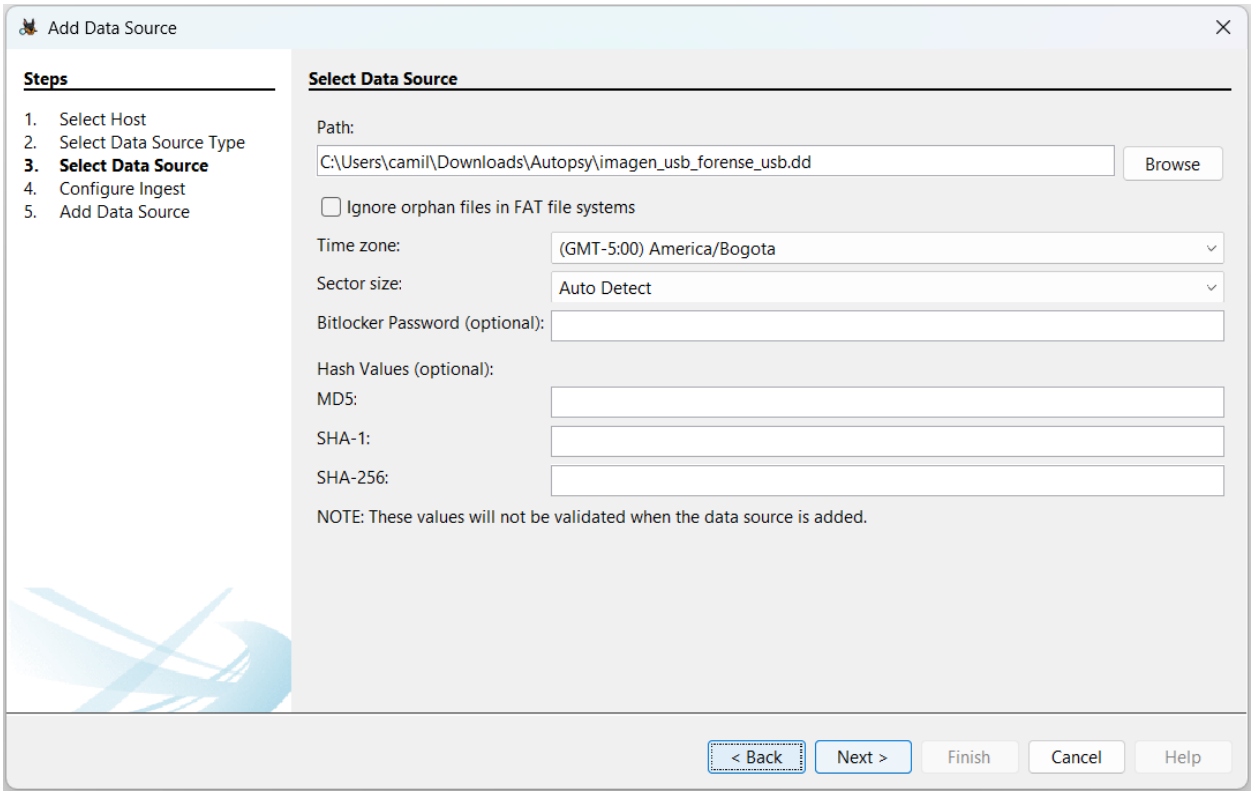



*Ilustración 30 Selección del archivo de imagen*

### 2.8.3 Configuración de los módulos de análisis

Autopsy permite elegir los tipos de análisis a realizar. En este caso, se seleccionaron **todos los módulos disponibles**, incluyendo:

- Análisis de archivos eliminados,
- Extracción de metadatos,
- Indexación de texto,
- Generación de hashes,
- Y detección de tipos de archivo.

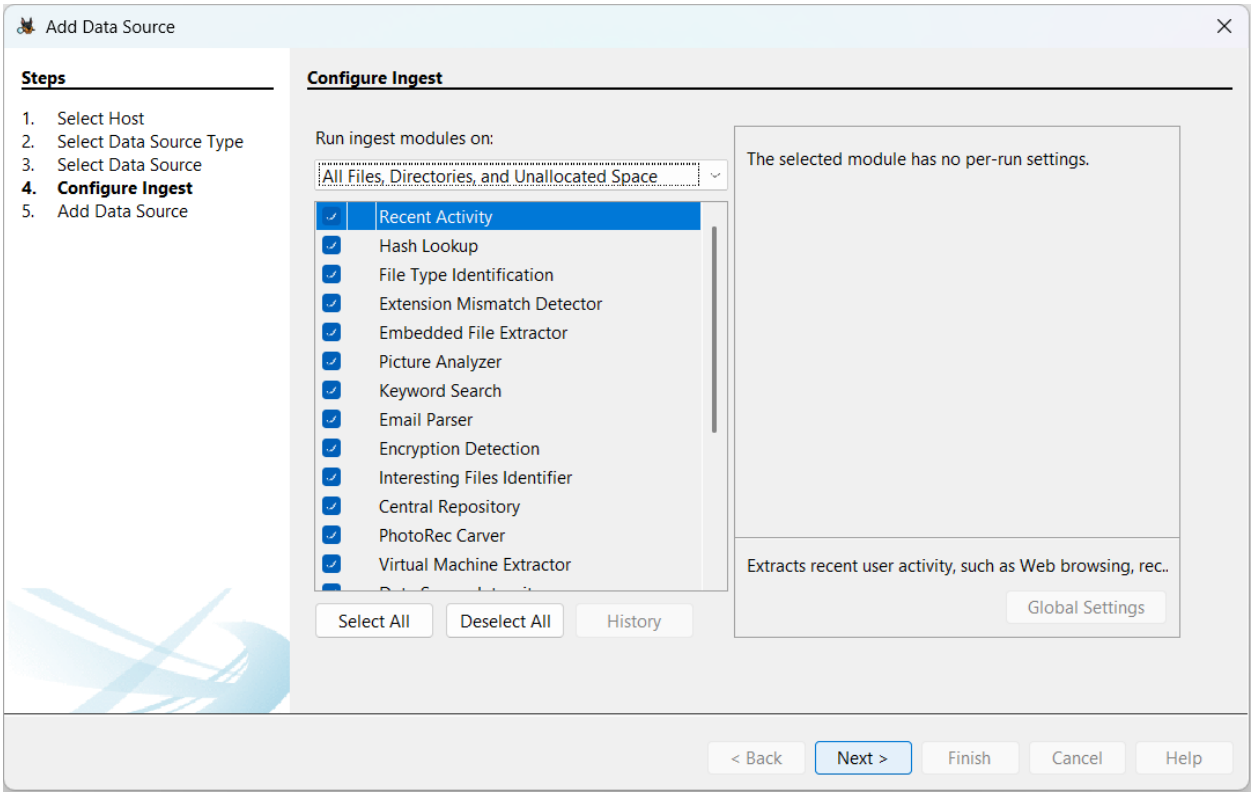



*Ilustración 31 Configuración de los módulos de análisis*

### 2.8.4 Carga de la imagen forense

Después de configurar los módulos, Autopsy inicia el **proceso de carga** de la imagen. Durante este tiempo, el programa analiza la estructura del sistema de archivos, monta los volúmenes y genera las bases de datos necesarias.

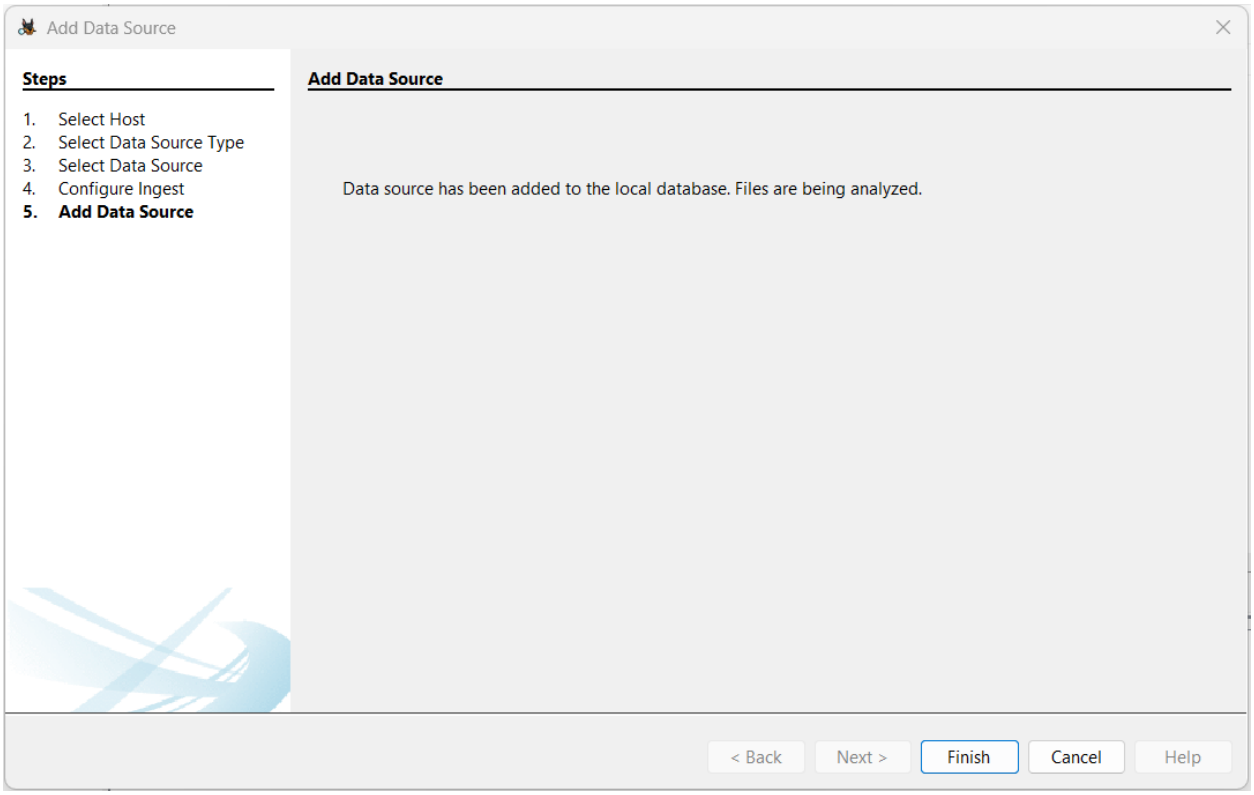



*Ilustración 32 Carga de la imagen forense*

## 2.9 Exploración y análisis de los datos

### 2.9.1 Exploración del contenido de la imagen

Una vez completado el análisis preliminar, la interfaz principal de Autopsy muestra un **panel de navegación** en el lado izquierdo con la estructura de carpetas, tipos de archivo, y estadísticas del contenido.

Desde esta vista se puede examinar todo el contenido del dispositivo, incluyendo archivos activos, eliminados, carpetas ocultas y documentos recuperables.

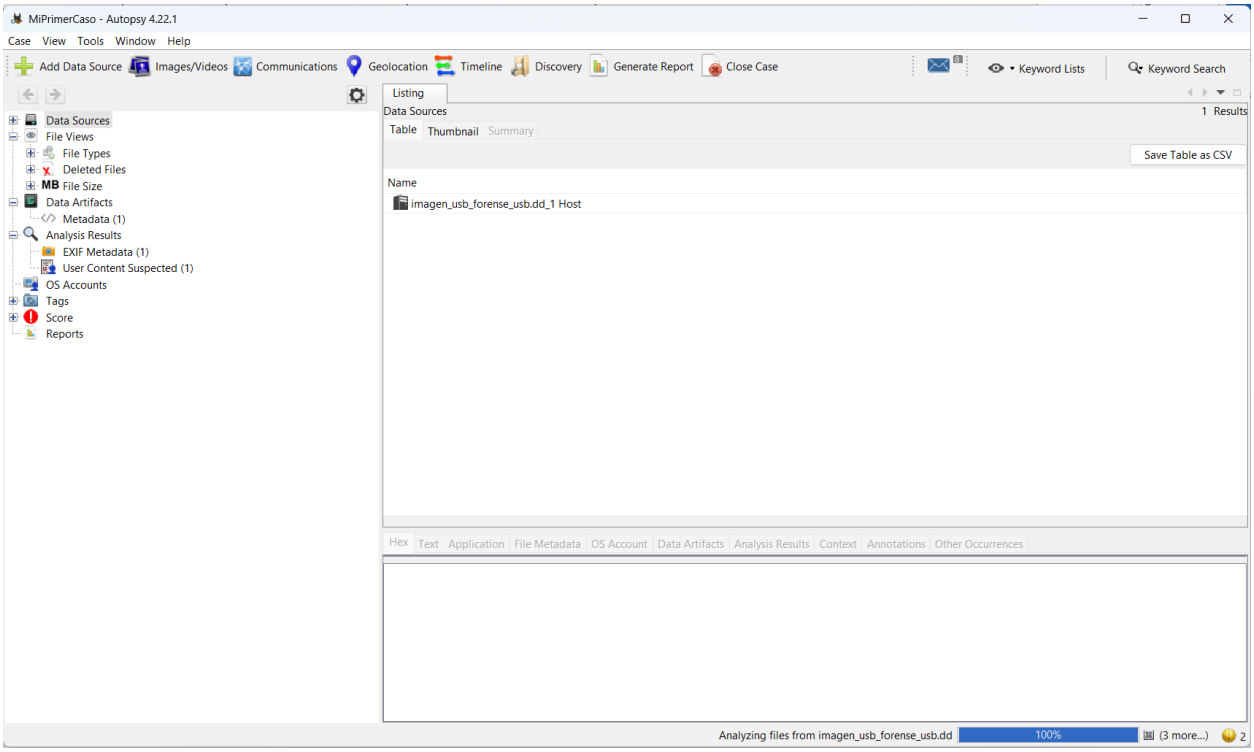



*Ilustración 33 Exploración del contenido de la imagen*

### 2.9.2 Comparación de hashes

Una parte esencial del proceso consiste en **verificar los hashes** generados en Autopsy de Windows y compararlos con los obtenidos previamente en Autopsy de Kali Linux.

Para ello, se filtraron los archivos tipo Office, que fueron los mismos a los que se les calculó el hash en el entorno anterior.

Los valores coincidieron, lo que confirma que la imagen no sufrió modificaciones durante su transferencia o análisis.

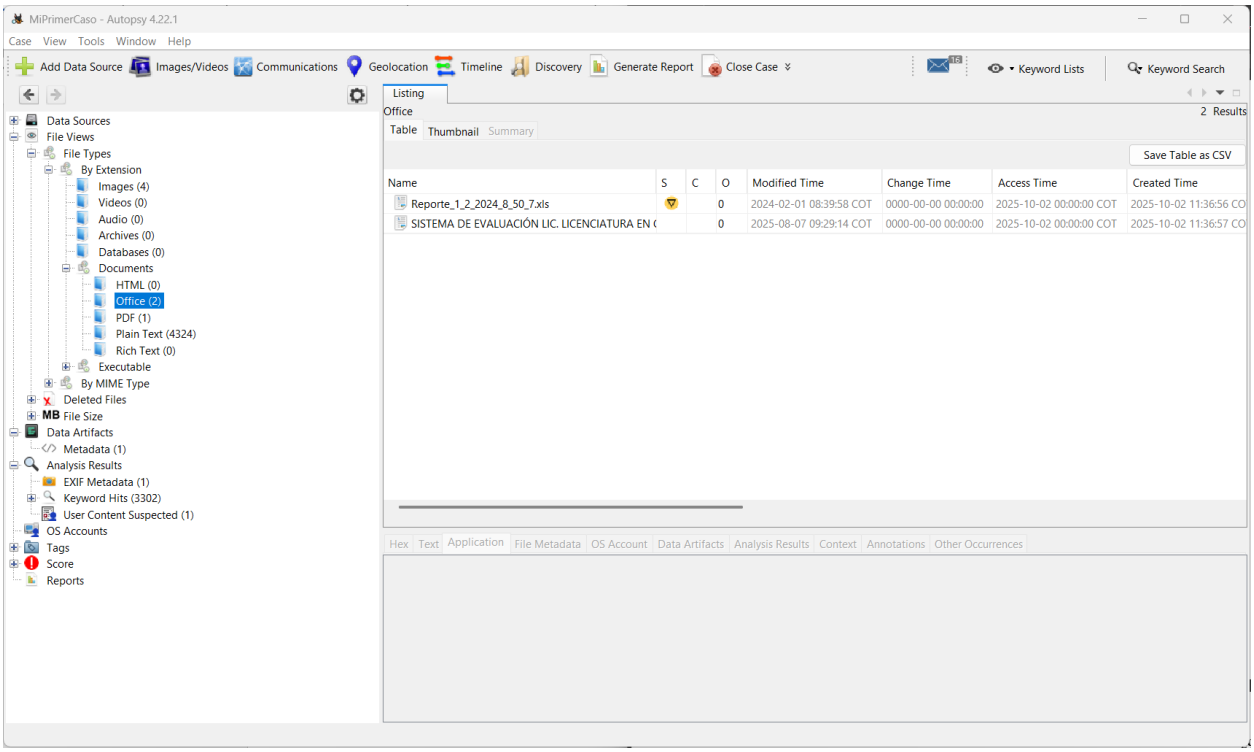



*Ilustración 34 Comparación de hashes*

## 2.10 Obtención de metadatos

Finalmente, se accedió a la sección de **metadatos** de Autopsy, donde se pueden observar detalles específicos de cada archivo, como:

- Propietario,
- Fechas de creación, modificación y acceso,
- Software utilizado,
- Tamaño en bytes,
- Y ubicaciones dentro del sistema de archivos.

Esta información permite identificar con precisión el origen, comportamiento y manipulación de los datos dentro del dispositivo.

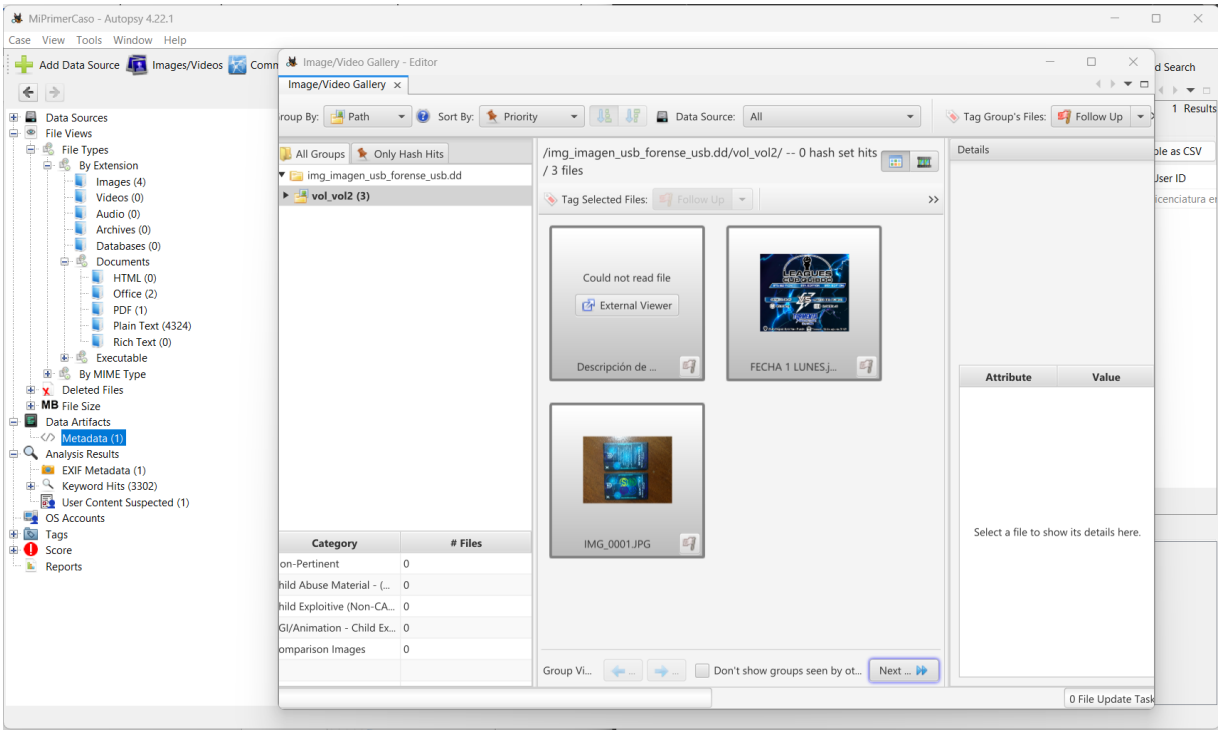



*Ilustración 35 Obtención de metadatos*

## 2.11 Conclusiones del análisis en Autopsy Windows

La versión de **Autopsy para Windows** ofrece las mismas funcionalidades que la versión de **Kali Linux**, variando únicamente en la interfaz gráfica y la forma de configurar los módulos.
El análisis permitió confirmar la integridad de la evidencia digital y evidenciar que los resultados de ambos sistemas coinciden perfectamente.

La coincidencia de los valores hash y la correcta recuperación de metadatos demuestran que la **imagen forense fue generada y analizada sin alteraciones**, cumpliendo con los principios fundamentales de la informática forense:
**integridad, trazabilidad, y preservación de la evidencia digital.**

# 3 CAPÍTULO 3 FTK IMAGER INSTALACION Y ANALISIS

## 3.1 Instalación de FTK Imager

### 3.1.1 Buscar y descargar FTK Imager

Abrí el navegador y busqué **"FTK Imager download"** o ingresé al sitio oficial de AccessData.

Descargué el instalador apropiado para Windows (FTKImager_setup.exe).

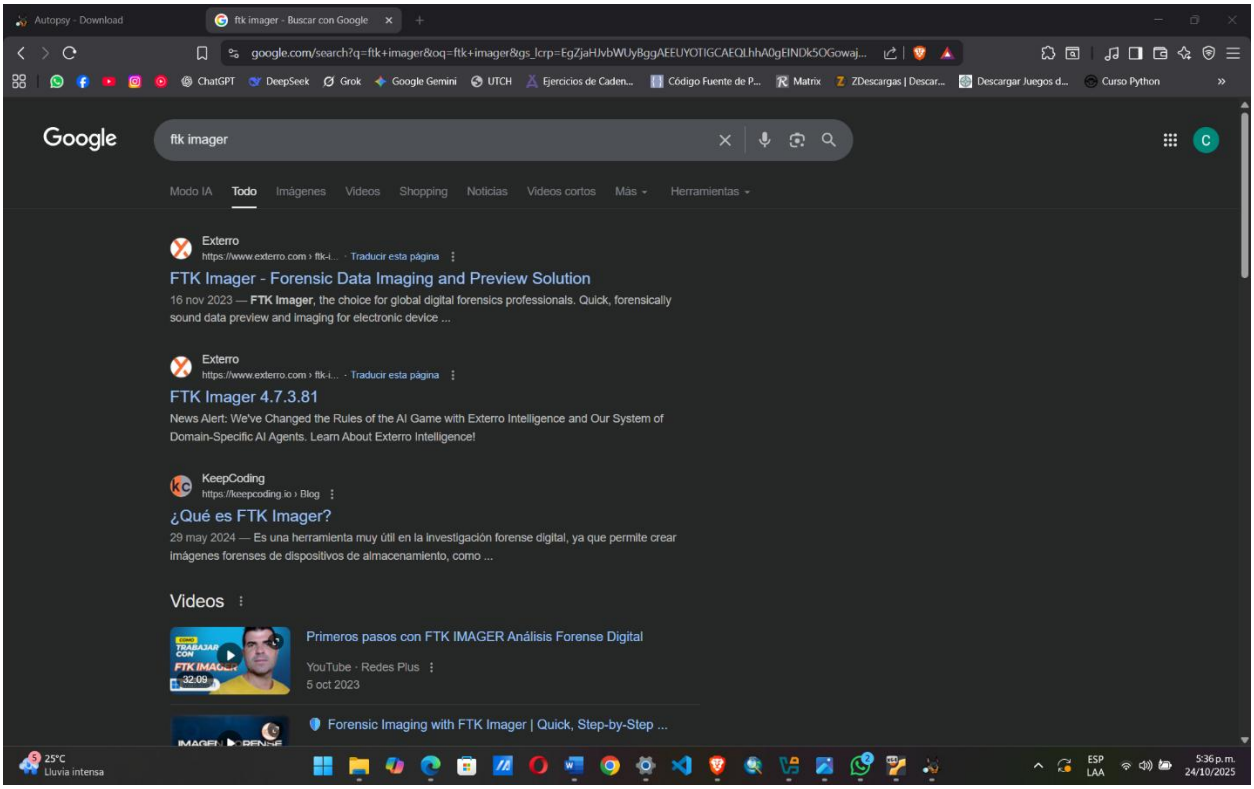
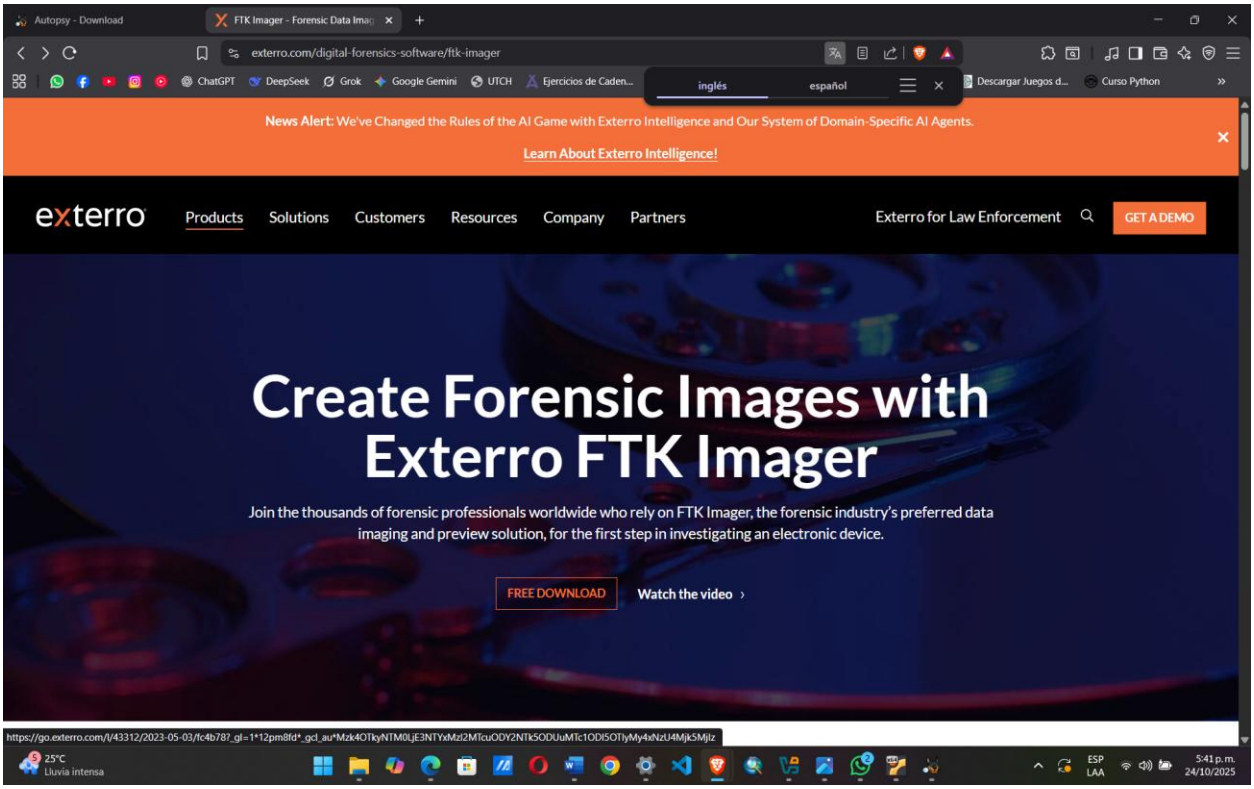



*Ilustración 36 Buscar y descargar FTK Imager*



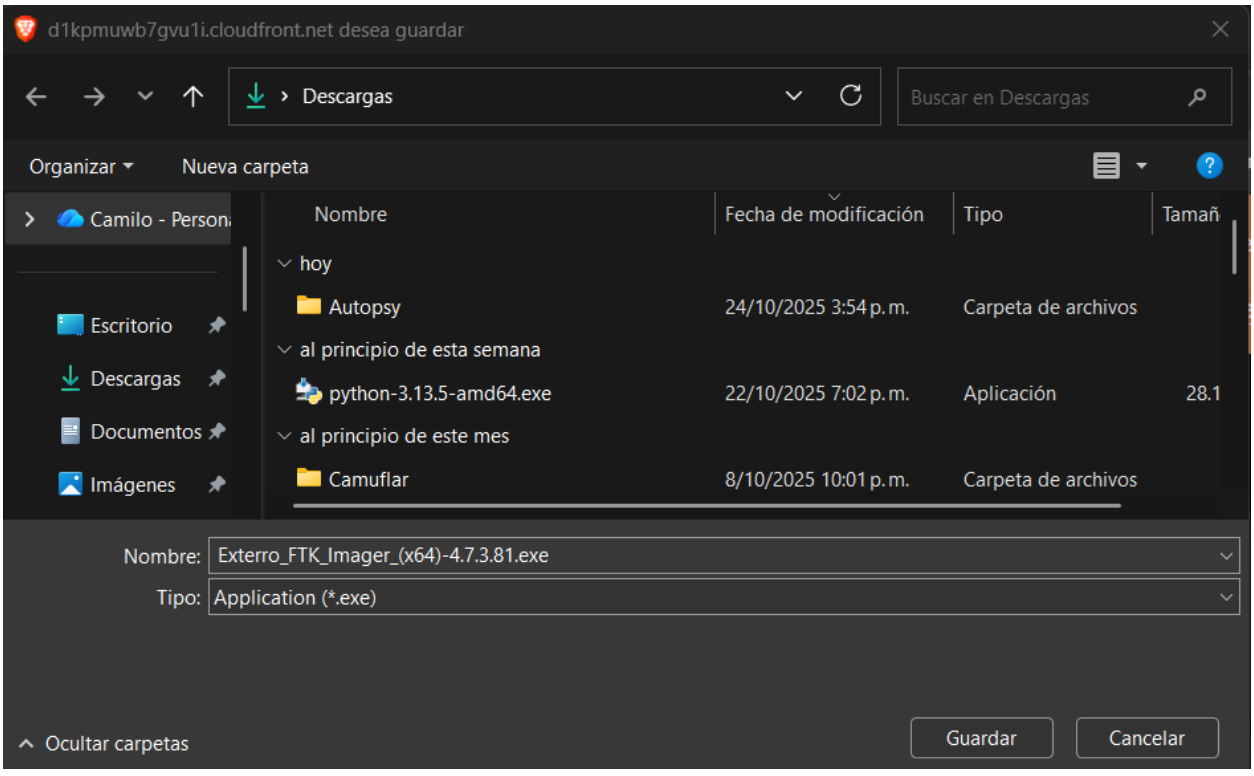
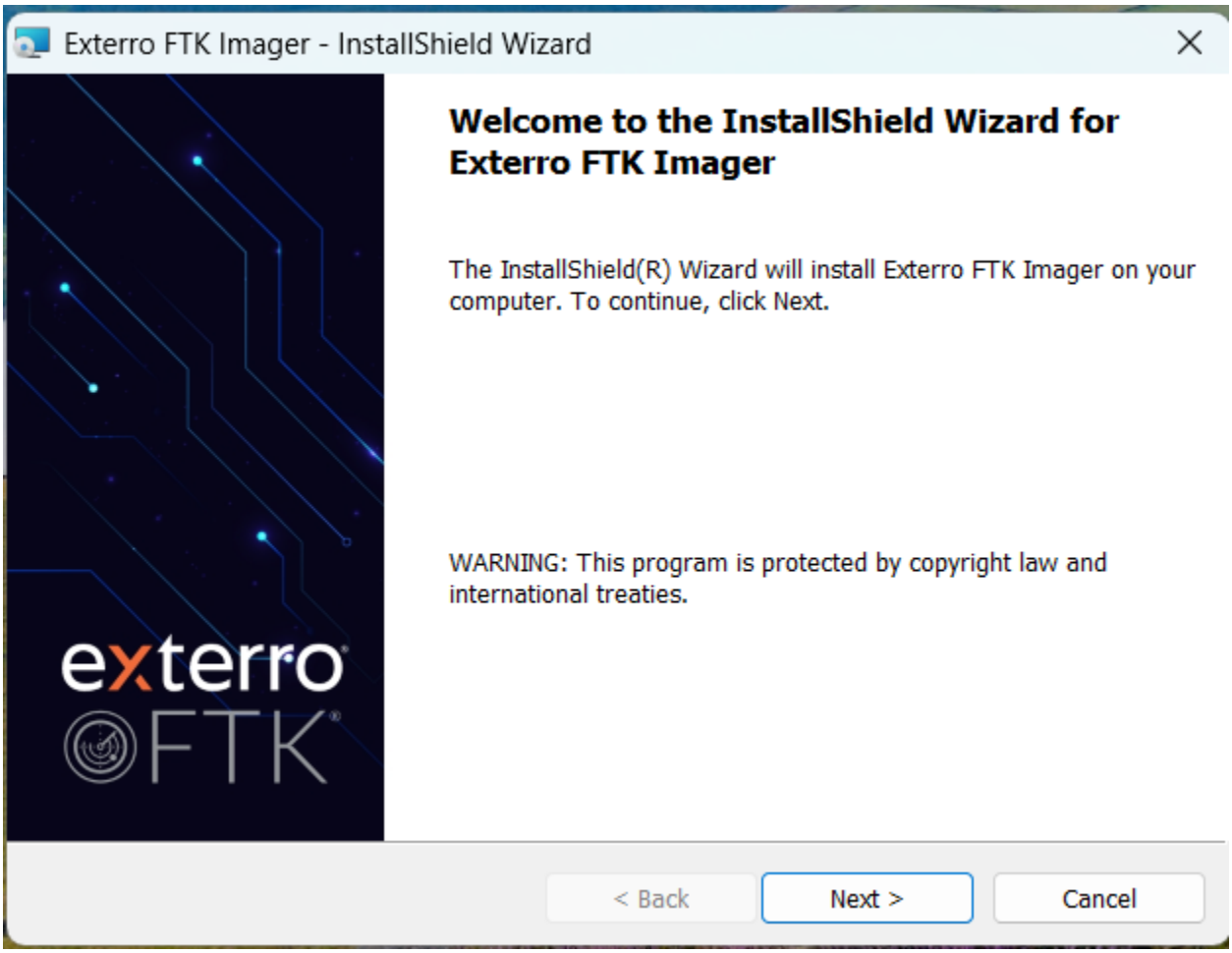




*Ilustración 37 FTKImager_setup.exe*

### 3.1.2 Ejecutar instalador y complemento requerido

1. Ejecuté el instalador .exe con doble clic.

2. El instalador detectó que se necesita un **complemento** (pre-requisito) y mostró la opción **Install**. Pulsé **Install** para agregarlo primero.



Acepté los **términos y condiciones** marcando la casilla correspondiente y pulsé **Next**.

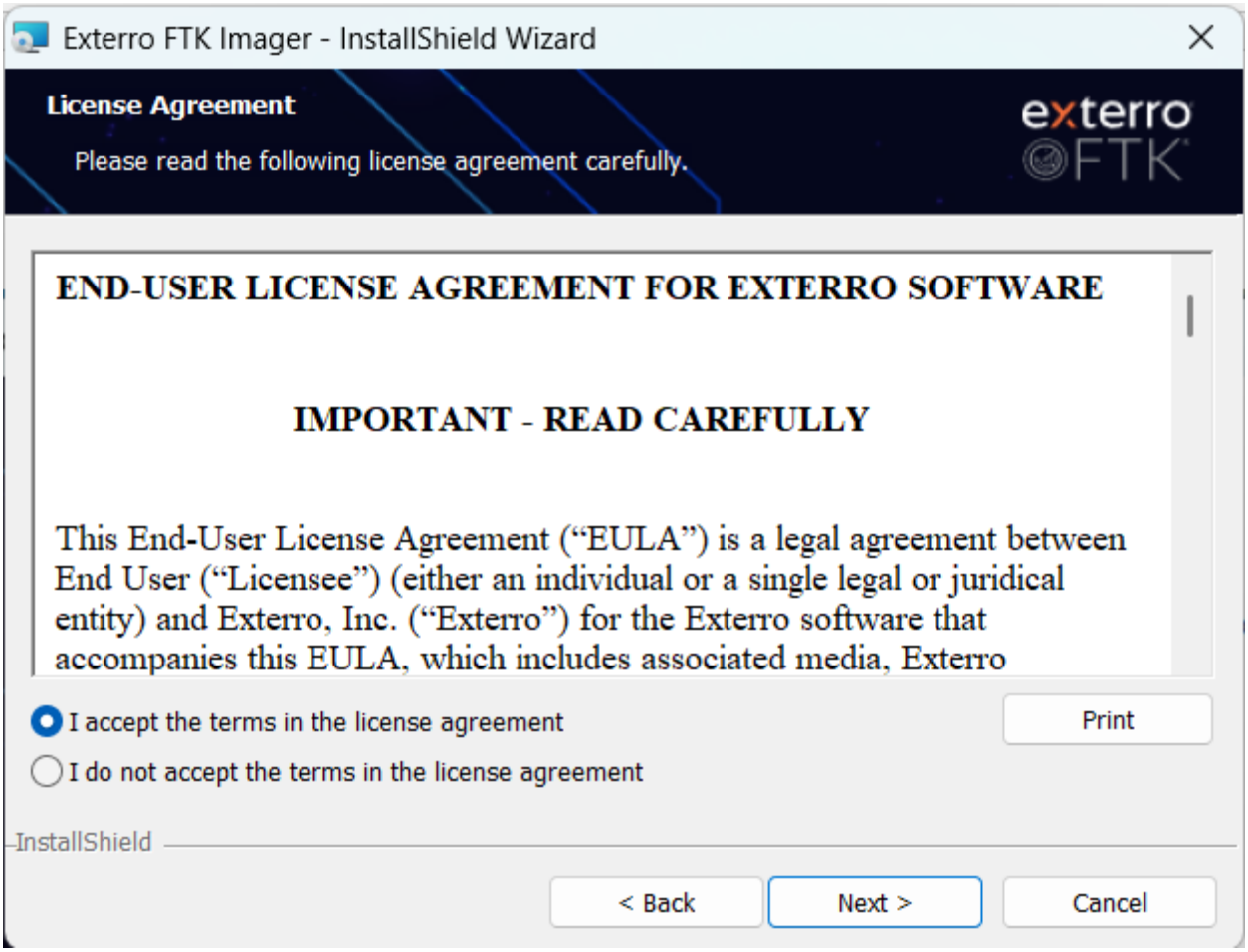


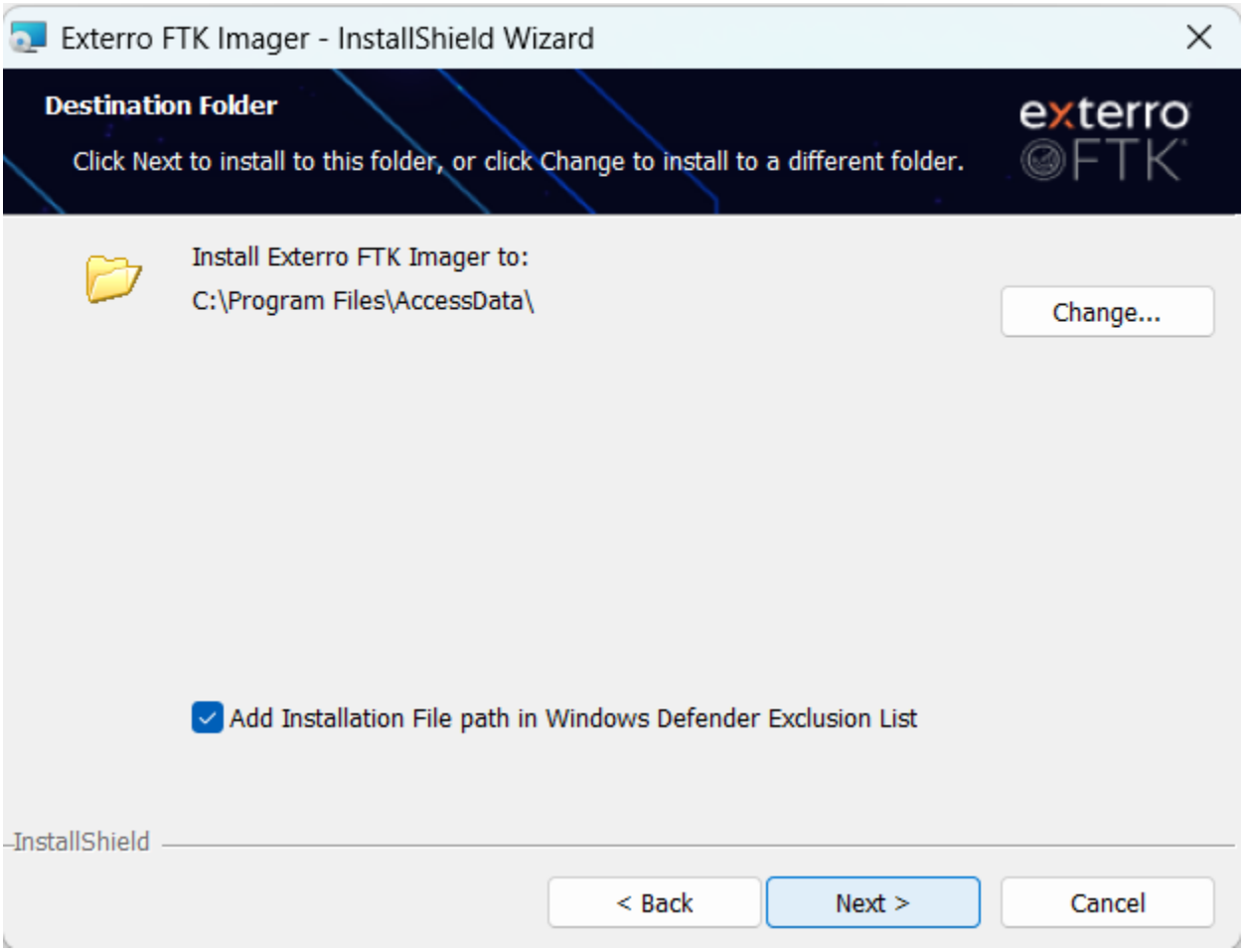

*Ilustración 38 términos y condiciones*

### 3.1.3 Añadir exclusión en Windows Defender

Antes o durante el proceso, Windows Defender puede advertir. Para evitar interferencias, añadí FTK Imager a la **lista de exclusiones**:

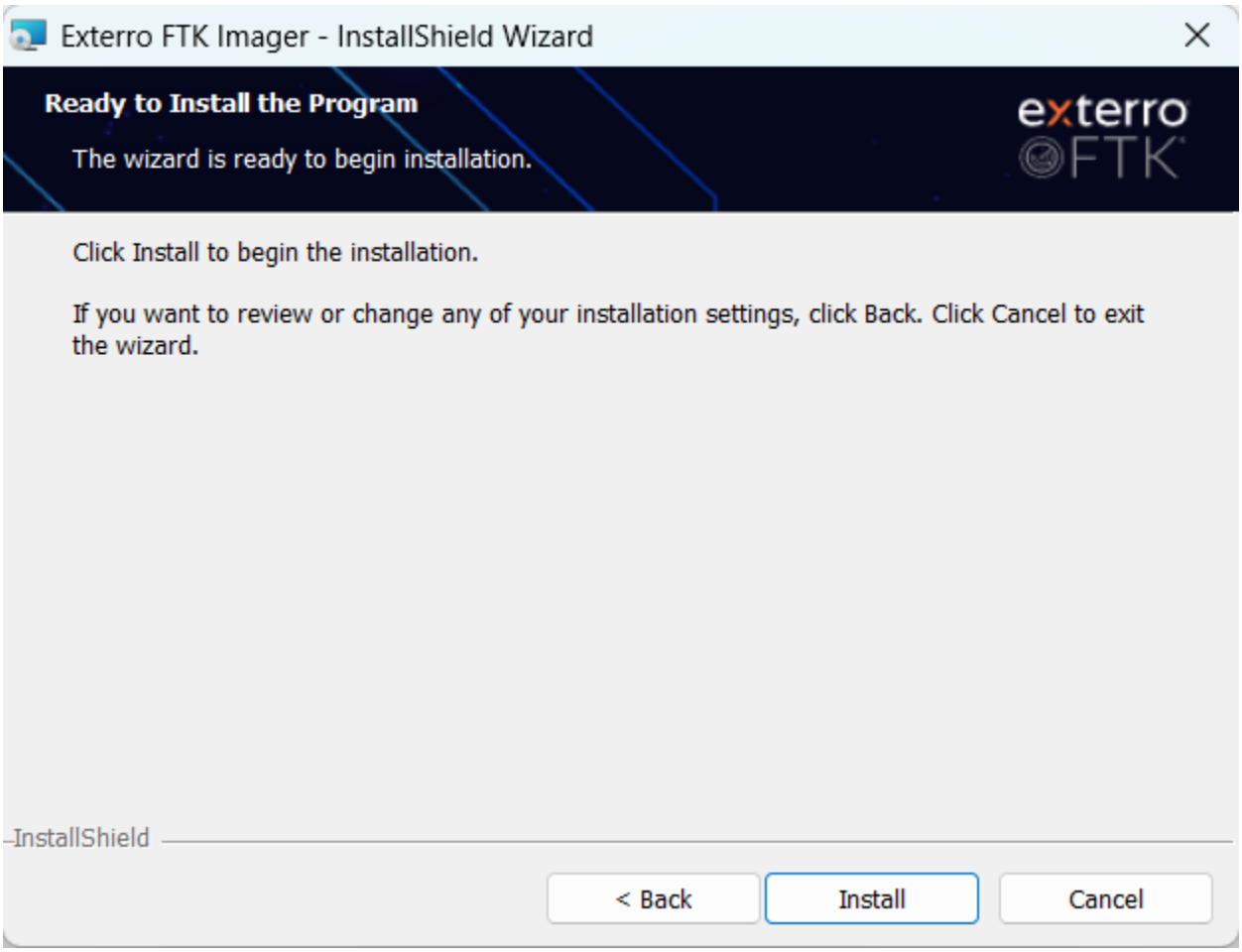
Abrí **Windows Security → Virus & threat protection → Manage settings → Exclusions → Add or remove exclusions**.

Pulsé **Add an exclusion → Folder** y seleccioné la carpeta donde se instaló FTK Imager (o el ejecutable).

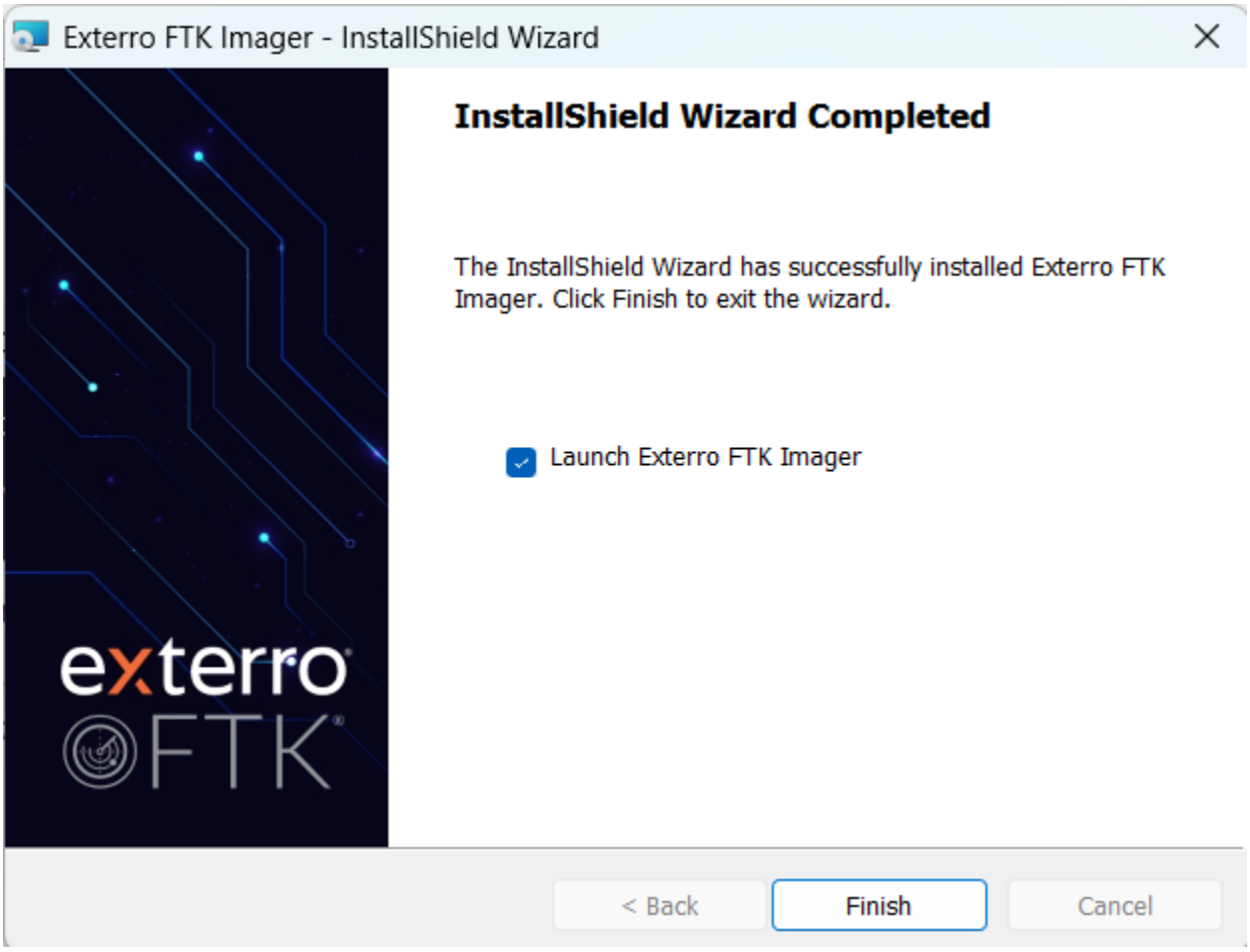


### 3.1.4 Progreso y finalización

Observé la barra de instalación hasta que concluyó.



Al finalizar, la ventana de asistente indicó **Installation complete** y ofreció lanzar la aplicación. Pulsé **Finish / Launch**.




## 3.2 Uso de FTK Imager para generar CSV de hashes — paso a paso

### Abrir FTK Imager

Ejecuté FTK Imager desde el menú Inicio o icono del escritorio (es recomendable Ejecutar como administrador).

### 3.2.1 Agregar evidencia (Add Evidence Item)

En el menú principal fui a **File → Add Evidence Item**.

Se abrió la ventana para seleccionar el **tipo de evidencia**; elegí **Image File (or Physical Drive)** (la primera opción en tu flujo).

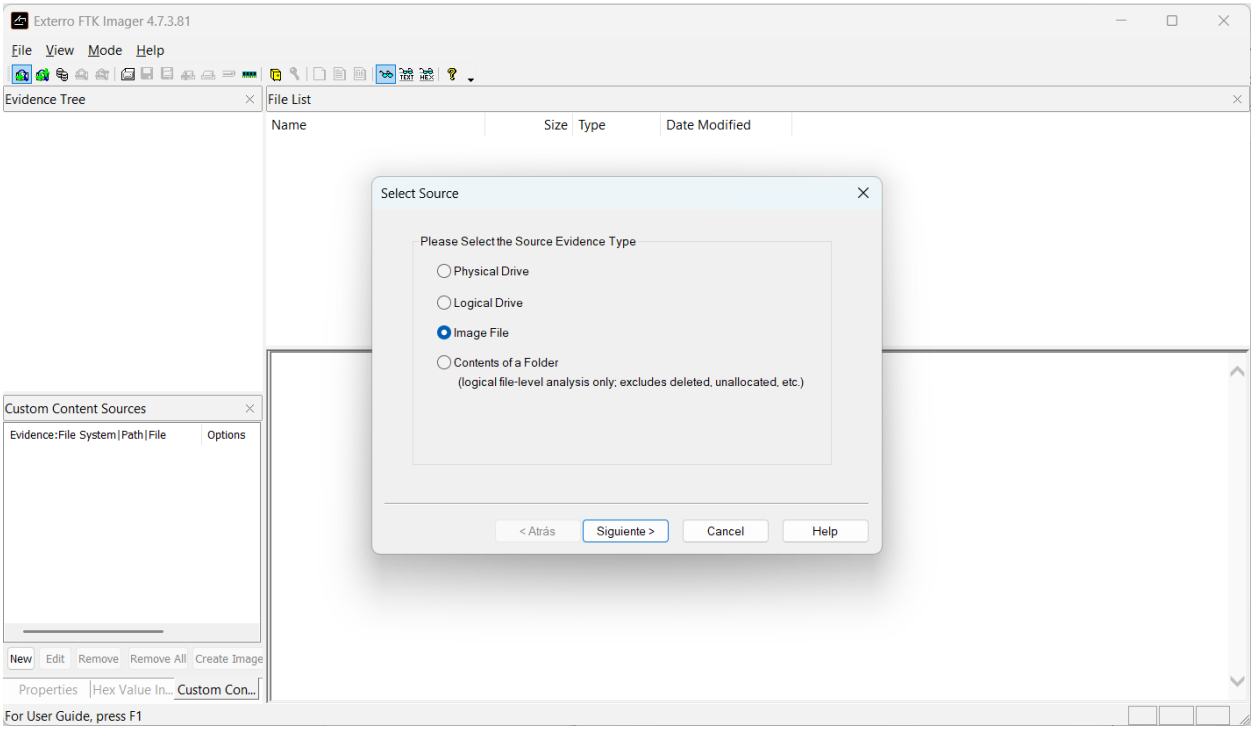



*Ilustración 39 Image File*

### 3.2.2 Seleccionar la imagen

Navegué hasta la ubicación del archivo imagen_usb_forense.dd y lo seleccioné.

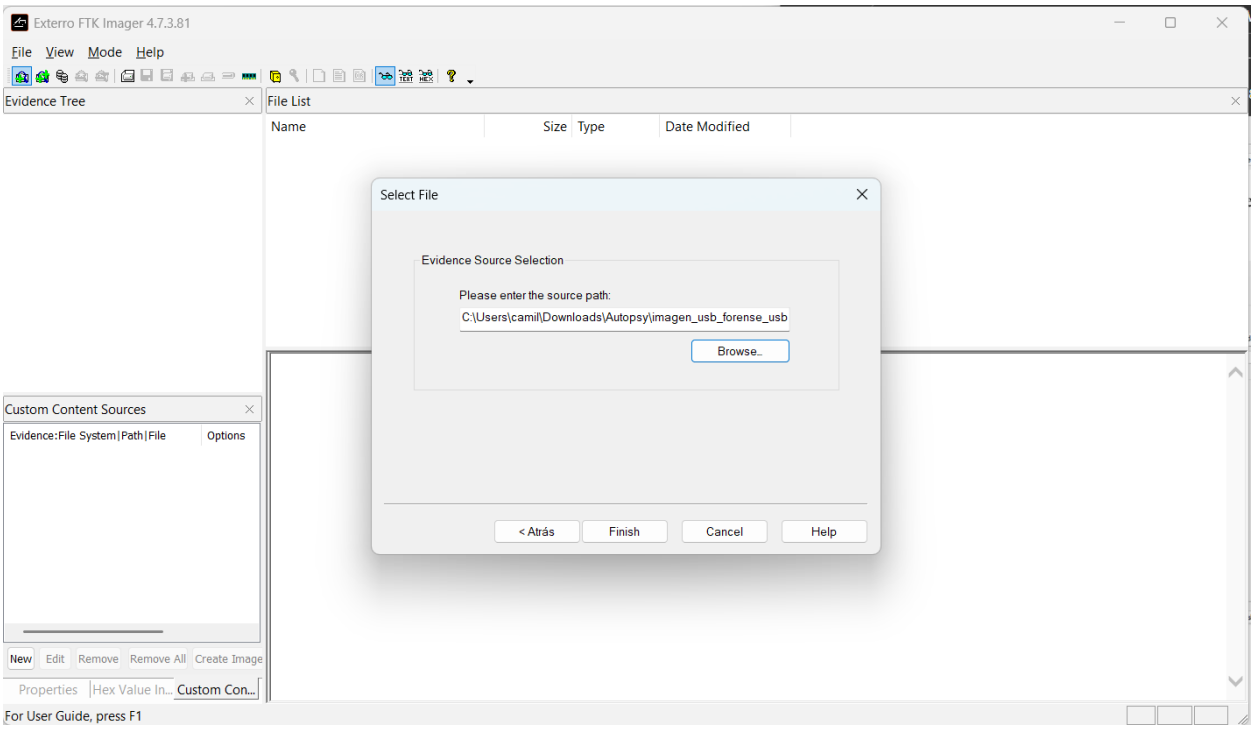



*Ilustración 40 Seleccionar la imagen*

### 3.2.3 Explorar la imagen

FTK montó la imagen y en el panel izquierdo apareció el nombre del dispositivo

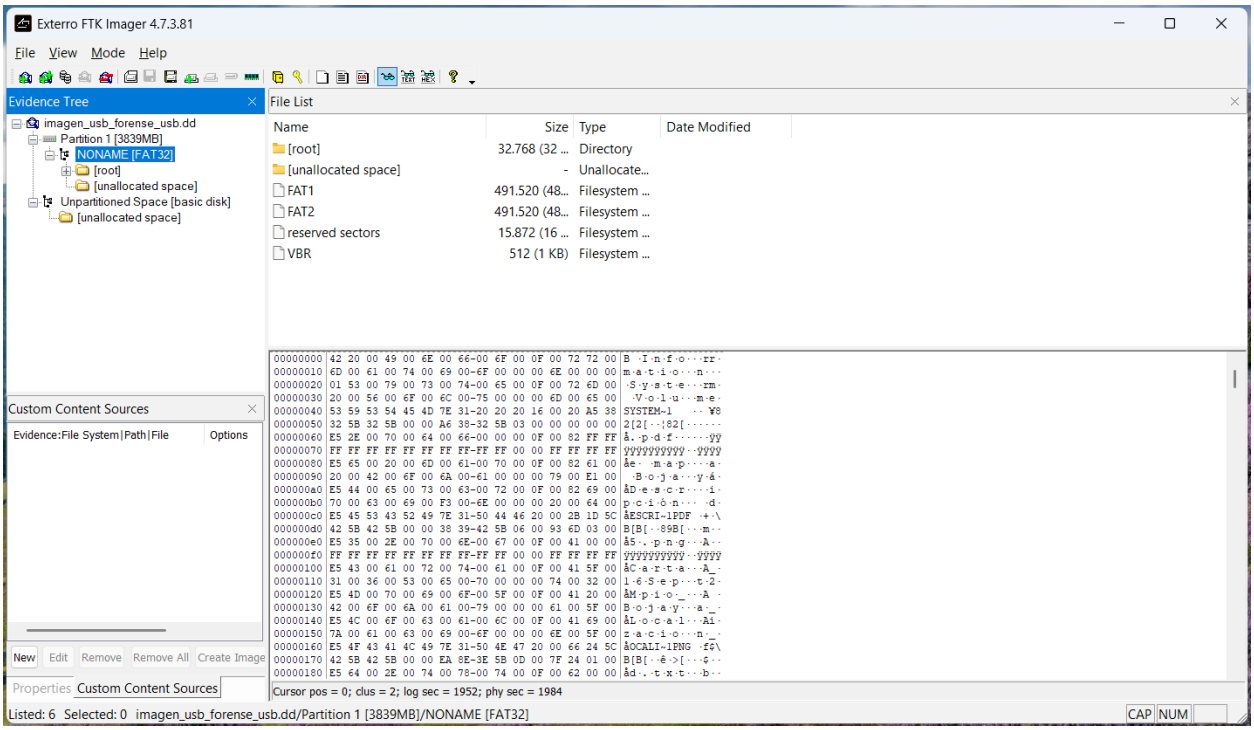



*Ilustración 41 Explorar la imagen*

### 3.2.4 Exportar lista de hashes (Export File Hash List)

Seleccioné el volumen/principal nodo

Hice clic derecho o busqué la opción **Export → Export File Hash List** (o menú equivalente).

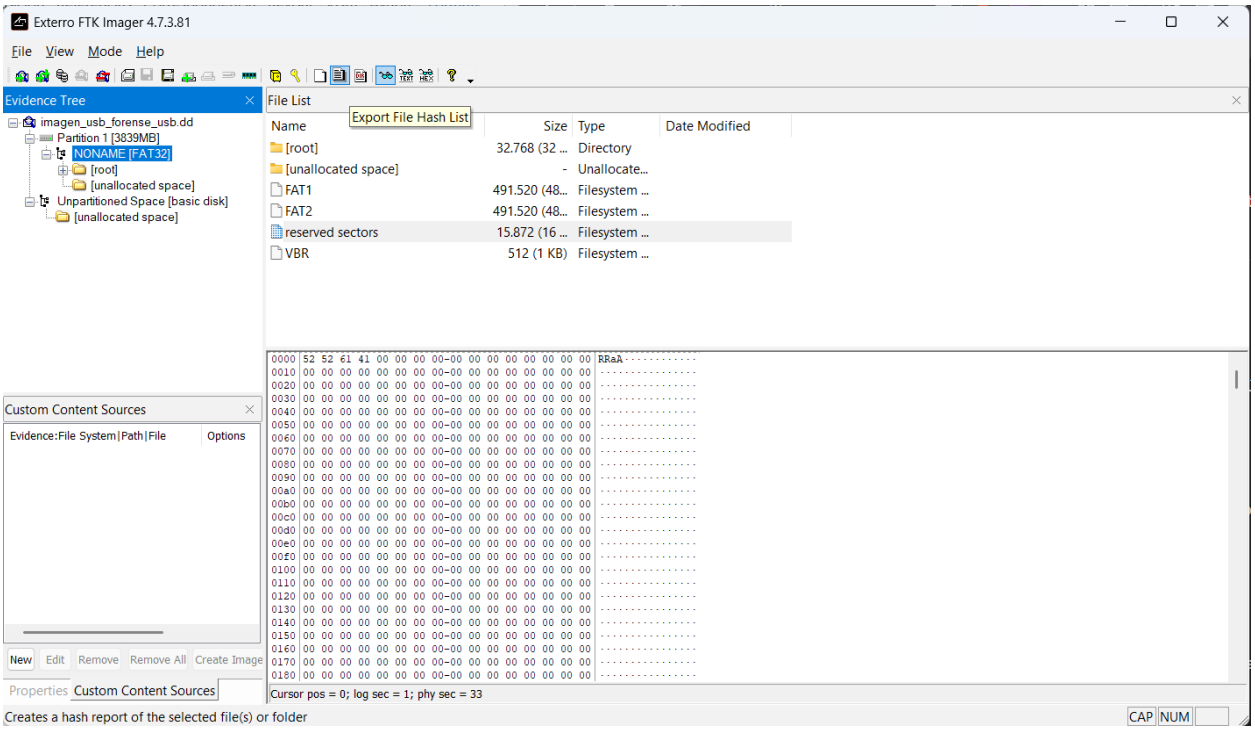



*Ilustración 42 Export*

### 3.2.5 Guardé el fichero en formato .csv

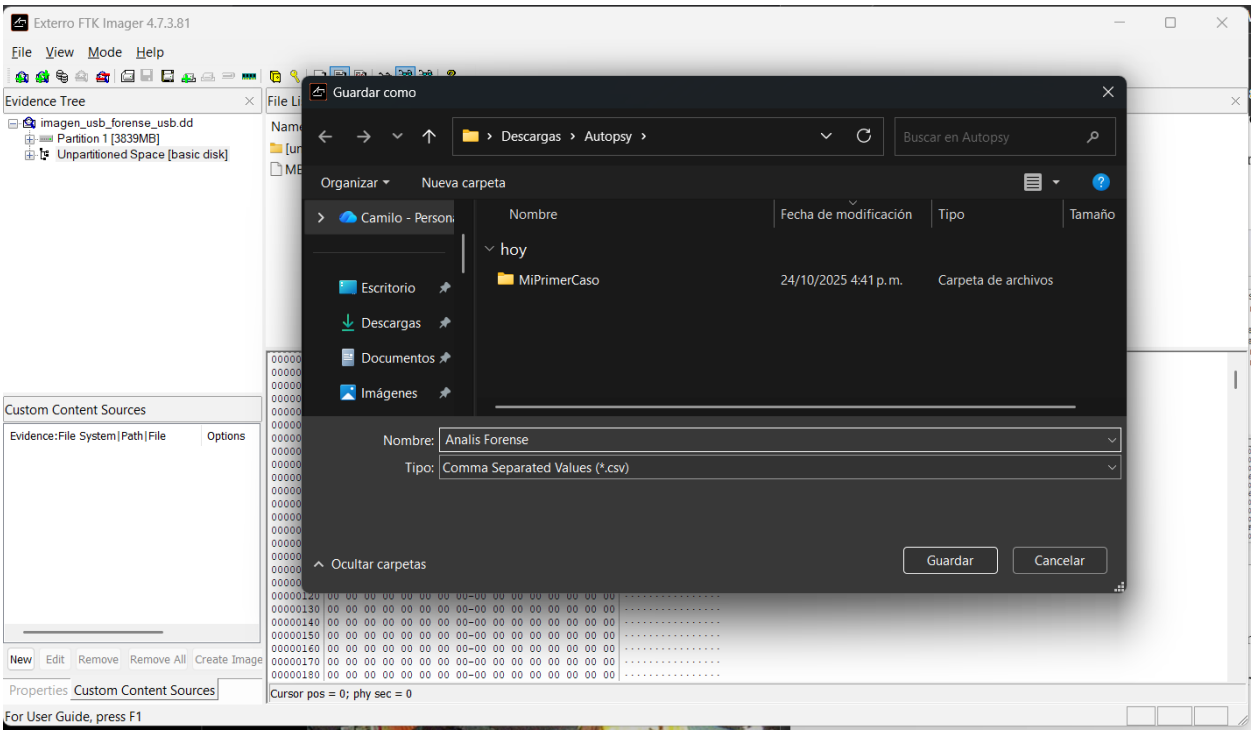
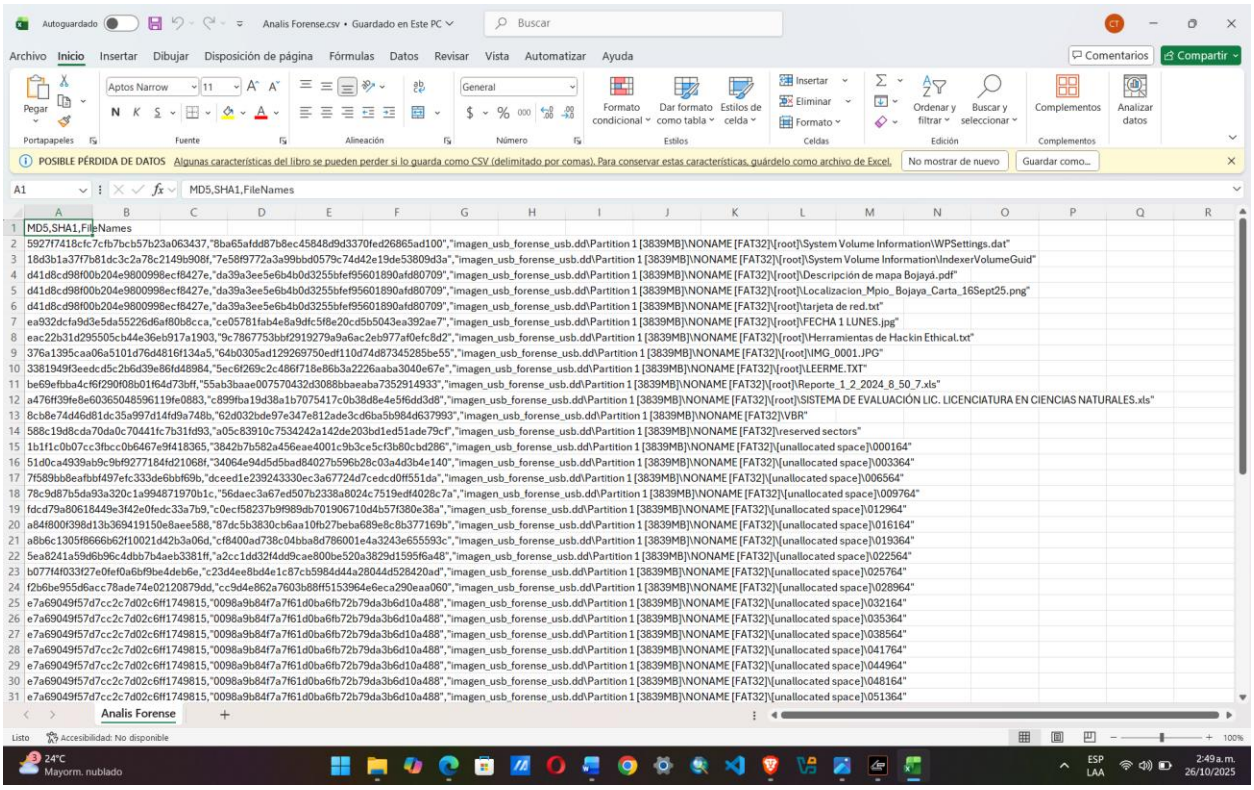



*Ilustración 43 Guardé el fichero en formato .csv*

### 3.2.6 Verificación

Abrí el CSV con Excel/Notepad para revisar que contenga: ruta del archivo, nombre y hash MD5.

Comparé algunos valores con las listas generadas por Autopsy para confirmar coincidencia.



# CONCLUSIÓN

Durante el desarrollo del análisis forense digital se logró instalar y configurar correctamente las herramientas **Autopsy** y **FTK**, así como instalar los complementos necesarios para su funcionamiento. Se realizó la transferencia de la imagen forense desde Kali Linux a Windows y se verificó su integridad mediante hashes. Posteriormente, se analizaron los datos contenidos en la imagen, identificando información relevante y generando reportes claros y precisos.

La práctica permitió comprender la importancia de seguir procedimientos metodológicos estrictos para asegurar la **integridad de la evidencia digital**, así como la utilidad de estas herramientas en investigaciones de seguridad informática.

## REFERENCIAS


- Kali Linux Documentation. https://www.kali.org/docs/
- Morales, R. S. (2025). Quidbo.
- Tello, C. A. (2025). Quibdo.
- FTK. https://www.exterro.com/digital-forensics-software/ftk-imager
- Autpsy. https://www.autopsy.com/download/