PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA.

SEGURIDAD Y AUDITORIA DE REDES

Análisis forense en kali linux y windows11 con herramienta autopsy a microSD utilizando adaptador USB.

LABORATORIO #8

LUIS JADER CUESTA MOYA
Estudiante**.**

SEMESTRE:
VIII

QUIBDÓ-CHOCÓ

Fecha: 26/10/2025

INTRODUCCION

El presente informe describe de forma detallada el proceso de análisis forense digital aplicado a una memoria microSD de 4 GB, utilizando un Adaptador USB y herramientas del entorno Kali Linux. Durante el desarrollo del laboratorio se emplearon comandos y utilidades especializadas como fdisk, dd, sha1sum y la herramienta forense Autopsia, las cuales garantizan que la evidencia se mantenga intacta. El documento explica paso a paso cómo se realizó la adquisición bit a bit del dispositivo, la verificación de la integridad mediante valores hash, la creación de la imagen forense y su posterior análisis en Autopsy. Además, se documentan los problemas encontrados durante la importación de la imagen .dd y las soluciones aplicadas para culminar el proceso con éxito.

Este trabajo contribuye al fortalecimiento de competencias en seguridad informática, preservación de evidencia digital, análisis técnico y uso de herramientas forenses profesionales, aspectos esenciales dentro de la labor de un ingeniero en telecomunicaciones y seguridad de redes.

Tabla de contenido

Tabla de Ilustraciones.

Planteamiento del problema

En el desarrollo del laboratorio de análisis forense, se presentó una interrupción crítica durante la Fase de Análisis al intentar cargar la imagen forense .dd, en la herramienta Autopsy. A pesar de que la imagen fue creada correctamente y su integridad verificada mediante SHA1, Autopsy arrojó una advertencia al no poder determinar el tipo de sistema de volumen de la imagen. Este error impidió visualización y el montaje correcto de la partición de archivos, Este inconveniente generó múltiples intentos de recrear la imagen, calcular nuevos hashes y abrir casos adicionales sin éxito. Finalmente, se determinó que el problema estaba relacionado con la clasificación incorrecta del tipo de volumen al momento de la importación.

Objetivo General

Realizar un análisis forense a una memoria microSD de 4GB mediante un adaptador USB utilizando herramientas como fdisk, sha1sum, dd y Autopsy en un entorno Kali Linux, asegurando la integridad y autenticidad de la evidencia obtenida.

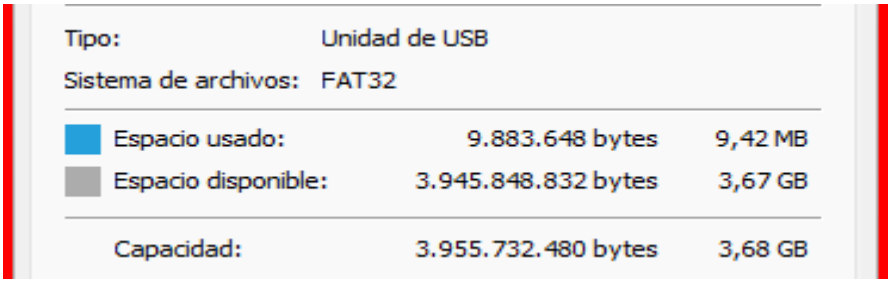
Objetivos específicos

Adquirir una copia bit a bit del dispositivo de almacenamiento mediante el comando dd, preservando la evidencia original, Calcular y verificar valores hash (SHA1) para confirmar la autenticidad de la imagen forense creada, Importar y analizar la imagen forense en Autopsy, identificando los artefactos digitales y posibles evidencias relevantes, Registrar y documentar todo el proceso de adquisición y análisis conforme a las buenas prácticas de la informática forense, Identificar errores y proponer soluciones técnicas, mejorando la comprensión de la configuración y el manejo de imágenes forenses en Autopsy.

Capítulo 1

1. ANÁLISIS FORENSE

En este laboratorio busco realizar un análisis forense a una tarjeta **microSD** de 4GB de almacenamiento utilizando un adaptador USB en una distribución como lo es Kali Linux.



En este laboratorio se llevaron a cabo tres fases en el proceso, entre estas tenemos:

Adquisición:
Es cuando creamos el **hash**, huella digital o una copia exacta de la unidad de almacenamiento que estamos usando se conoce como imagen forense, para que el análisis posterior se realice sobre la copia, preservando la evidencia original intacta.
Análisis:
Se realiza el análisis sobre el archivo de imagen**.dd** para buscar artefactos digitales.
Reporte y documentación:
Todo el proceso debe ser meticulosamente documentado para ser admisible en un proceso legal.

1.1. Adquisición

El primer comando que utilice es al comando **fdisk –L** que se utiliza para listar todas las particiones de disco tipo **MBR** disponibles y sus detalles. Para usar es este comando debemos estar en modo privilegiado o root para ser más claro en la imagen posterior veremos la información de la micro que se usó para este laboratorio en la parte inferior de la imagen con nombre /dev/sdb1

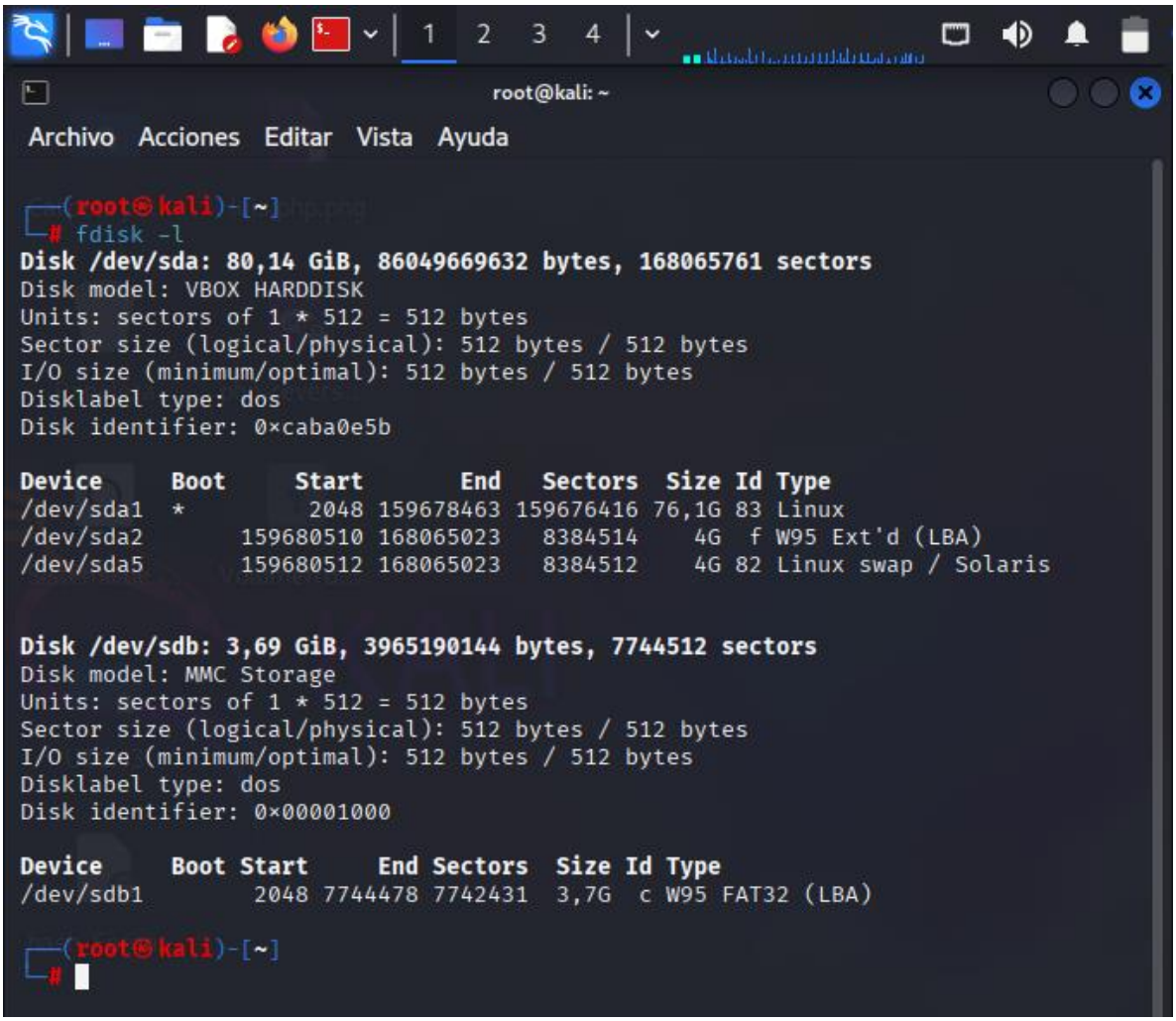


Ilustración 1 fdisk -L ----- listar particiones

El siguiente paso se basa en la creación del hash de toda la partición bit por bit utilizando el comando **sha1sum /dev/sdb1 > /home/luis/Escritorio/hash_Forence.sha1** como resultado de este proceso se creara un archivo de tipo sha1 llamado **hash_Forence.sha1** esta operación forense se utiliza para registrar una huella criptográfica de la unidad de almacenamiento lo que garantiza que se pueda verificar si el contenido de esta no haya sido alterado.

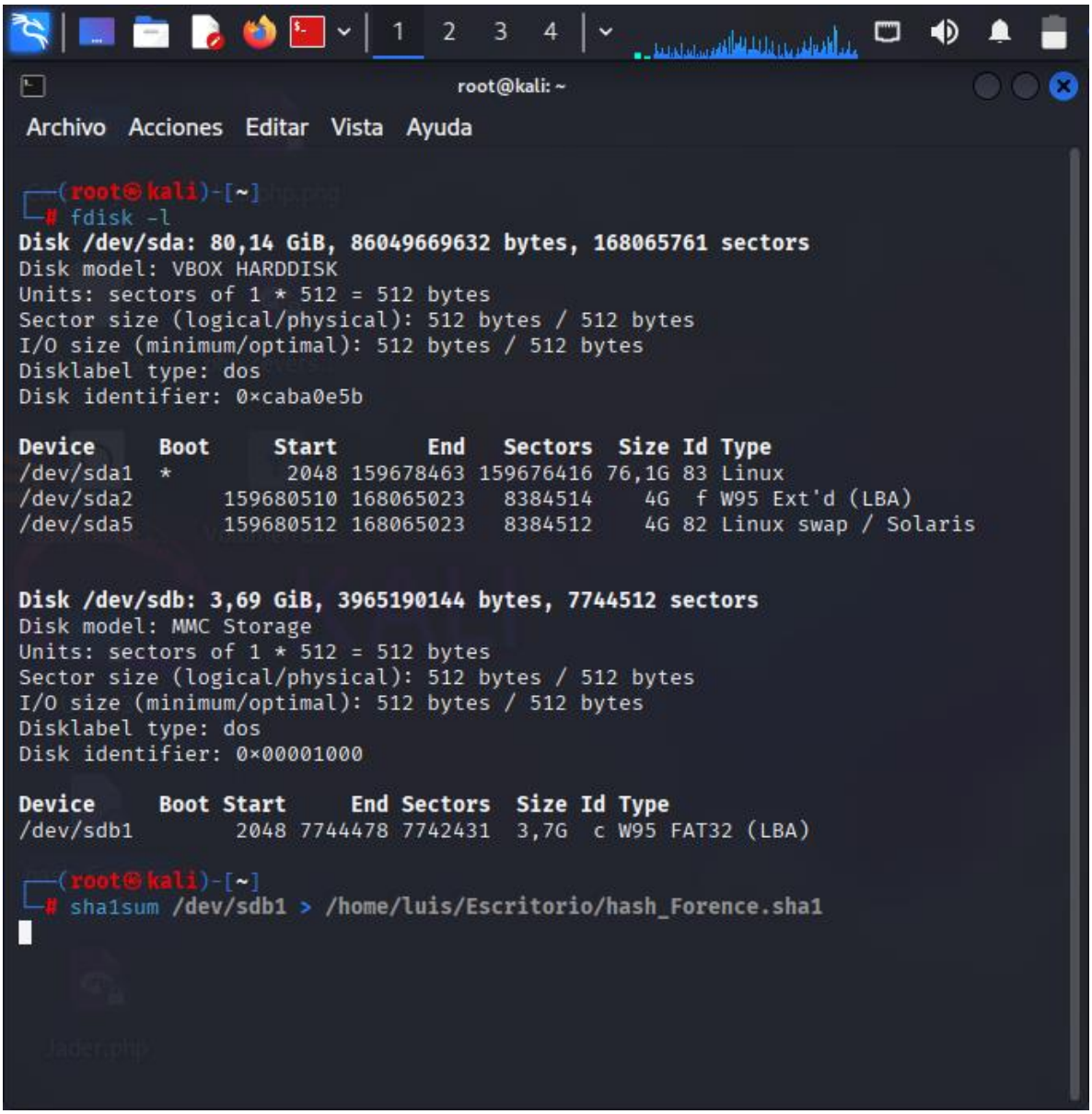


Ilustración 2 creación del hash.

El primer archivo necesario para hacer este tipo de inspección forense a estos dispositivos lo podemos ver en la siguiente ilustración donde se almaceno en el escritorio de nuestro sistema operativo kali-linux con el nombre que se le asigno en el comando anterior.

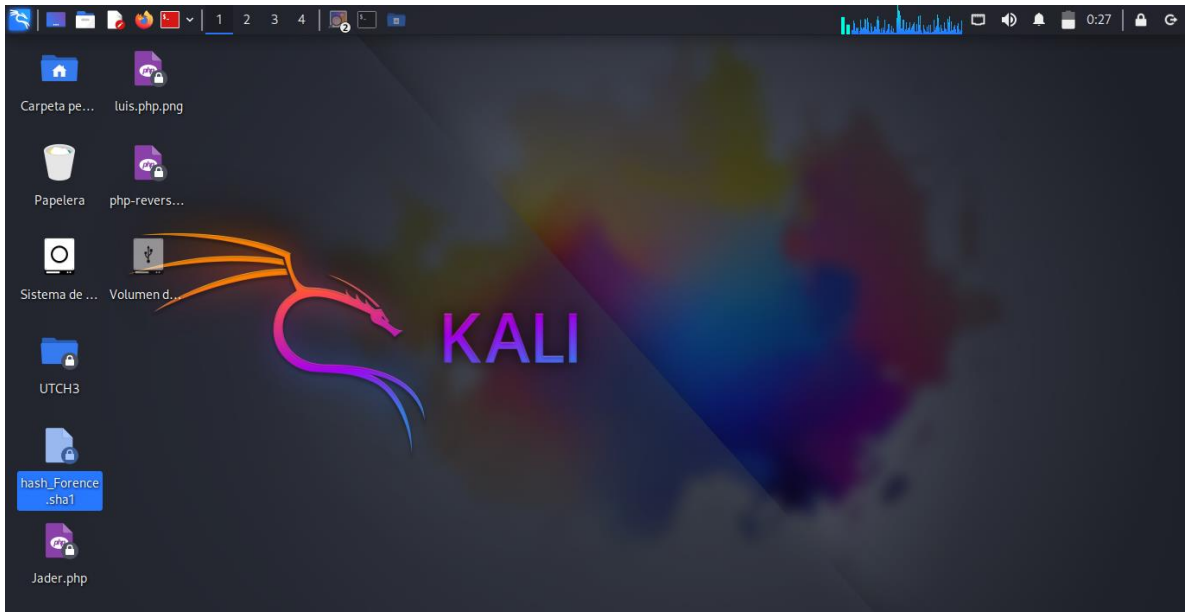


Ilustración 3 vista de archivo hash en el escritorio.

Al abrir el archivo vamos a notar que en su interior almacena una serie de código alfanuméricos como el que apreciamos a continuación.

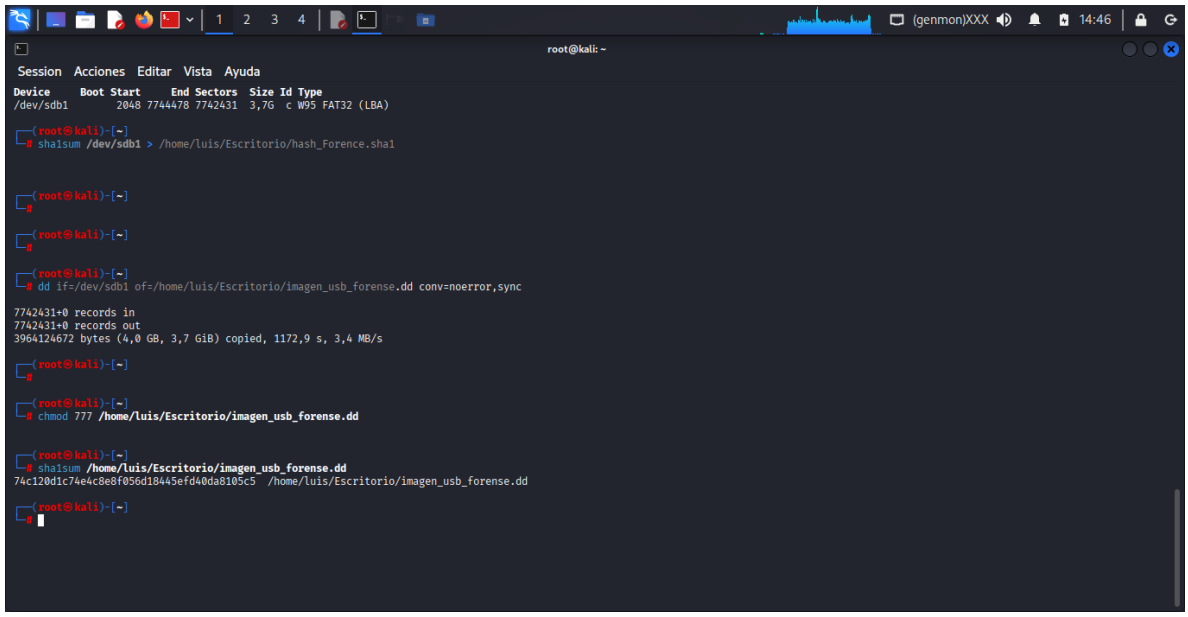


Ilustración 4 vista interna del archivo hash

Posteriormente usamos el comando **dd if=/dev/sdb1 of=/home/Luis/Escritorio/imagen_usb_forense.dd conv=noerror,sync** con el cual crearemos la imagen o en otras palabras clonamos nuestro dispositivo este

comando está conformado por varias partes de código donde cada una de ellas cumple con las siguientes tareas:

Parte	Significado
dd	Herramienta de bajo nivel para copiar datos bit a bit.
if=/dev/sdb1	Input file origen: la partición o dispositivo que vas a clonar (en este caso microSD en adaptador USB /dev/sdb1).
of=/home/Luis/Escritorio/imagen_usb_forense.dd	Output file destino: el archivo de imagen que se generará en el escritorio.
conv=noerror,sync	Opciones importantes para análisis forense: noerror continúa copiando incluso si hay errores de lectura. Sync rellena con ceros los bloques dañados, manteniendo el tamaño original.

Como resultado obtuvimos los siguientes resultados:
77424310+0 records in = número de archivos leídos del dispositivo
77424310+0 records out = número de archivos escritos en la imagen
3961494272 bytes (4,0 GB, 3,7 GiB) tamaño total de los datos copiados y tamaño del dispositivo coinciden correctamente.
copied, 1144,35 s, 3,5 MB/s tiempo total 1144 segundos
Lo que nos confirma que el comando dd se ejecutó correctamente y completo la copia forense

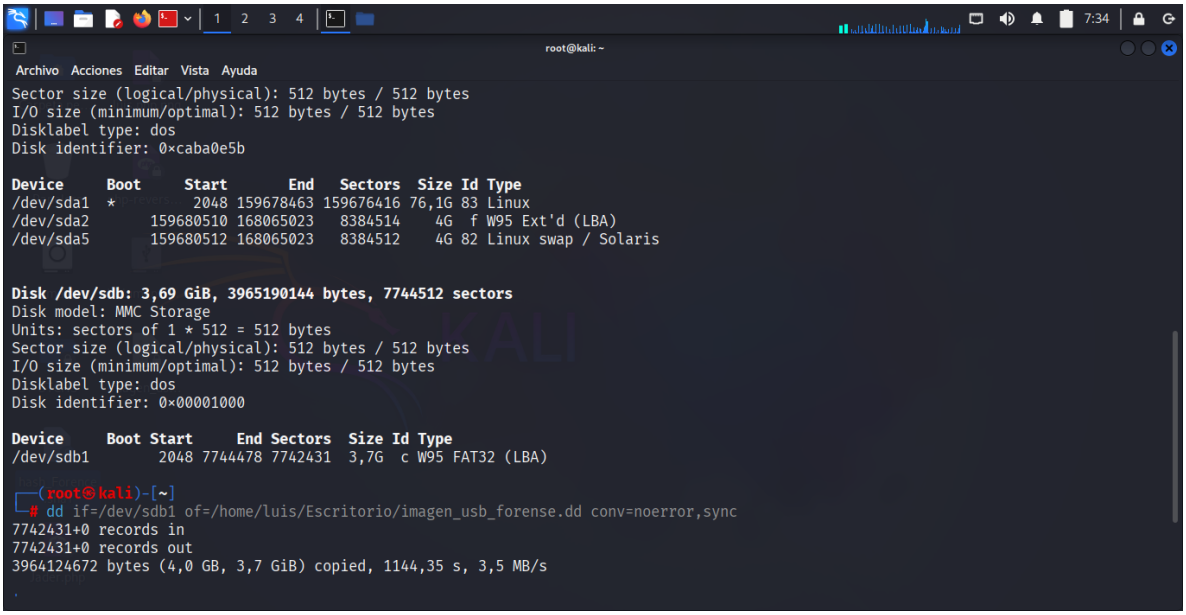


Ilustración 5 creación de imagen dd.

Ya creada la imagen usamos el comando **chmod 777 /home/Luis/Escritorio/imagen_usb_forense.dd** para otorgarle nuevos permisos al archivo como son vista, lectura y escritura. Podemos ver que esta imagen o

archivo se almaceno en la misma ruta asignada con el siguiente nombre: **imagen_usb_forense.dd**

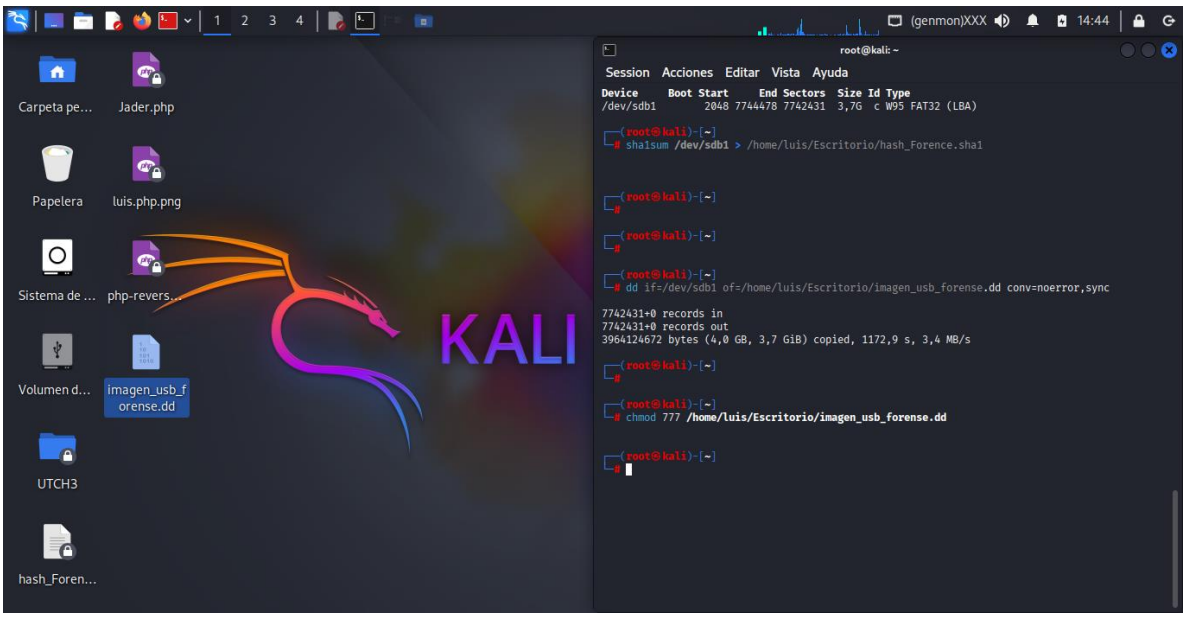


Ilustración 6 vista del archivo imagen_usb_forense.dd en el escritorio.

Este sería el último paso del proceso forense de adquisición de evidencia digital. Utilizando el comando: **sha1sum /home/luis/Escritorio/imagen_usb_forense.dd** el resultado nos arroja una cadena de 40 caracteres hexadecimal como lo veremos en la imagen de ilustración 8

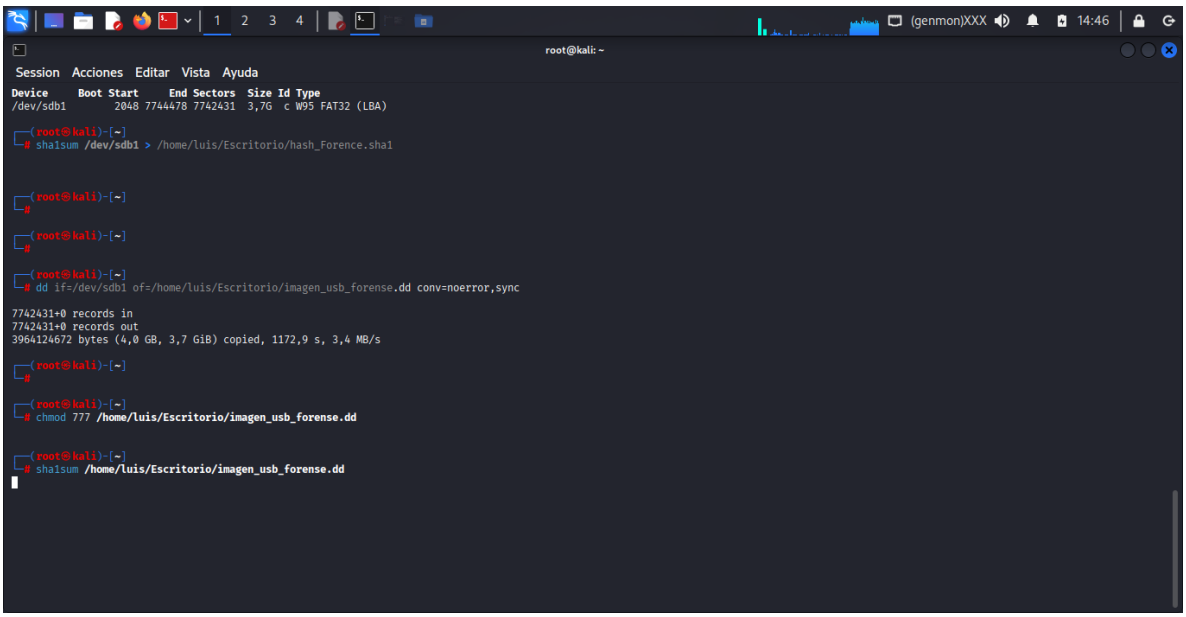


Ilustración 7 cálculo de la huella digital o hash.

Si el código resultado de este comando es idéntico al código generado inicialmente en el hash, significa que la imagen es una copia exacta y sin alteraciones del dispositivo original. Si son diferente en lo mínimo significa que pudo haber alteraciones en el dispositivo o posiblemente surgió algún error durante la copia, en ese caso no se podría asegurar la validez de la imagen como evidencia hasta no demostrar lo contrario, podría ser repitiendo los procesos para corroborar dicha alteración.

Conclusión: El **hash SHA1** del dispositivo original **(/dev/sdb1)** y el **hash SHA1** de la imagen **(imagen_usb_forense.dd)** son idénticos como podemos ver y corresponde al siguiente código: **74c12d01c74c8c8ef850d1844e5efd40da8105c5**

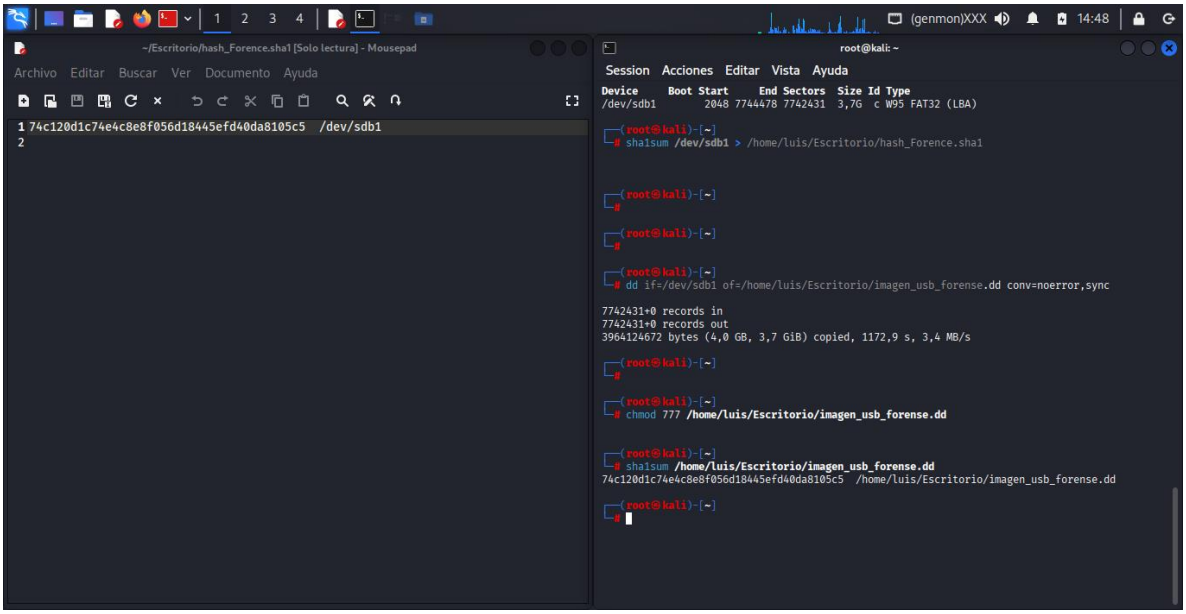


Ilustración 8 coincidencia del hash.

1.2. Análisis

Es el segundo paso dentro de este proceso donde vamos a realizar la parte de análisis utilizando la herramienta **autopsy** como vemos también requiere privilegios de administrador para acceder al sistema de archivos forense, luego de ingresar la contraseña de usuario veremos la interfaz inicial para abrir los servicios de locales.

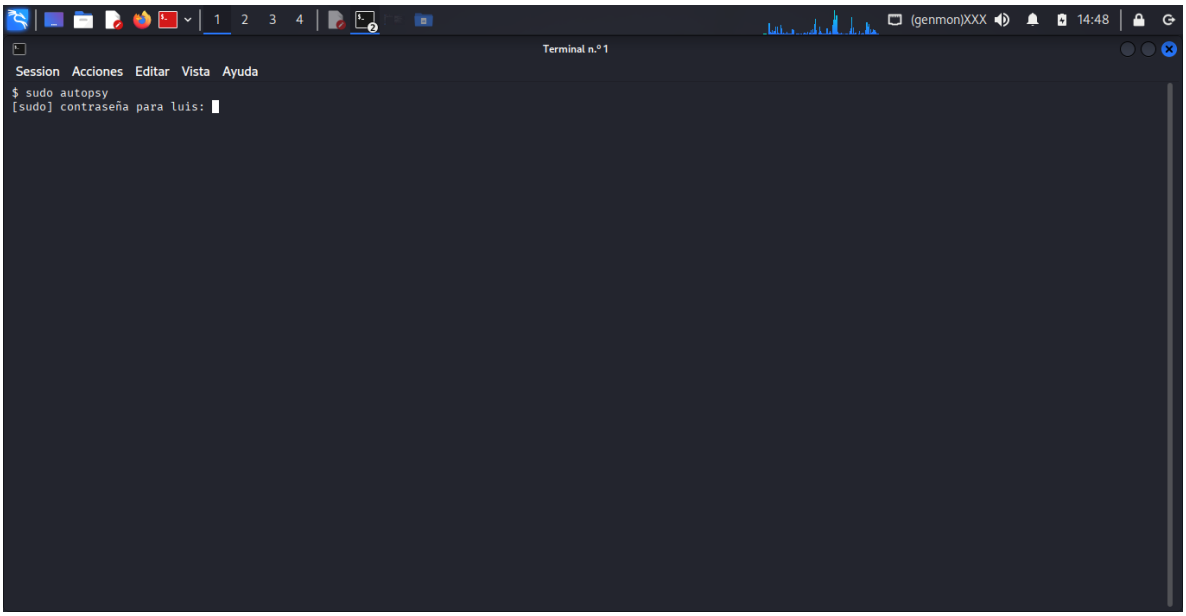


Ilustración 9 ingreso a la interfaz autopsy.

Vemos como la interfaz nos indica que el servidor local está corriendo en la siguiente url: **http://localhost:9999/autopsy** al abrir el enlace podemos apreciar que ya estaremos tratando temas como son casos que por lo general son términos que se utilizan en las áreas judiciales.

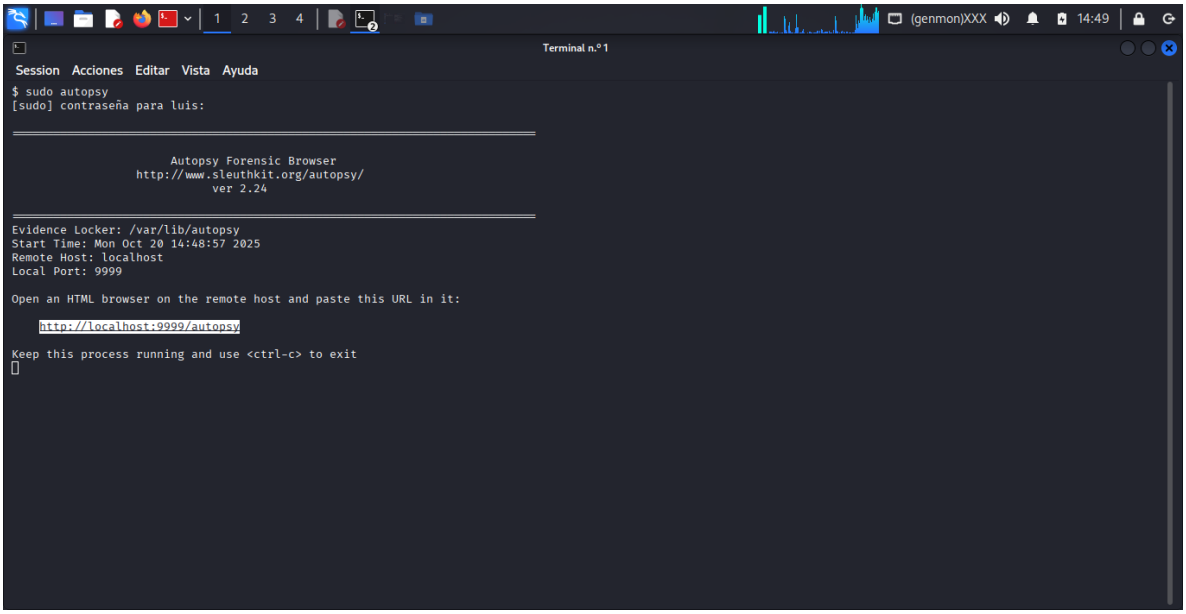


Ilustración 10 interfaz principal autopsy

Podemos notar que el navegador no muestra el menú principal con las siguientes opciones:

- Abrir caso.
- Crear caso.
- Ayuda.

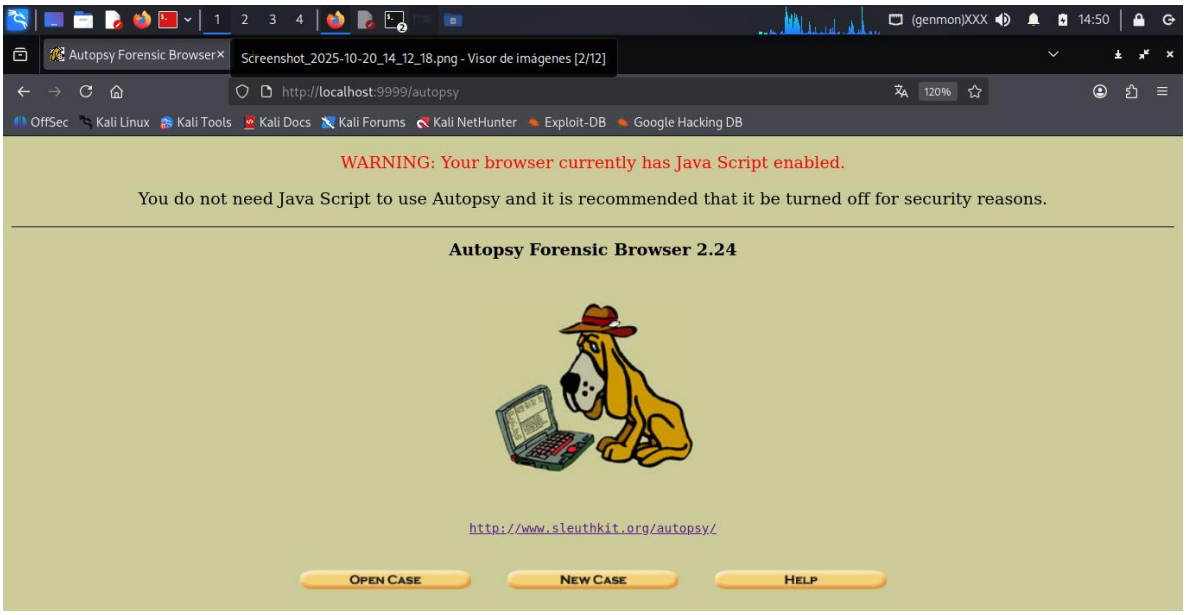


Ilustración 11 menú principal autopsy.

Nuestro primer caso los diligenciamos de la siguiente manera:
Nombre del caso: miPrimerCaso1
Description: Análisis Forense USB
Nombres de los Investigadores: a. Luis_Jader b. Edward_Camilo

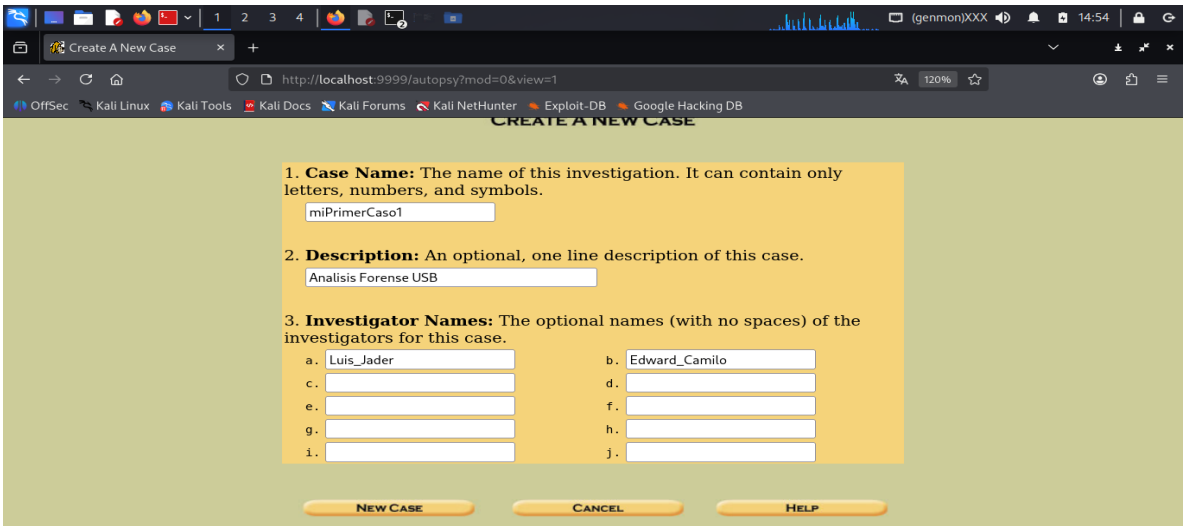


Ilustración 12 crear caso.

Se observa la que al agregar un nuevo host no fue necesario diligenciar algunos campos, los campos requeridos fueron los siguientes

- Nombre del host: **MyAPART1.**
- Descripción: **Portal_HP.**

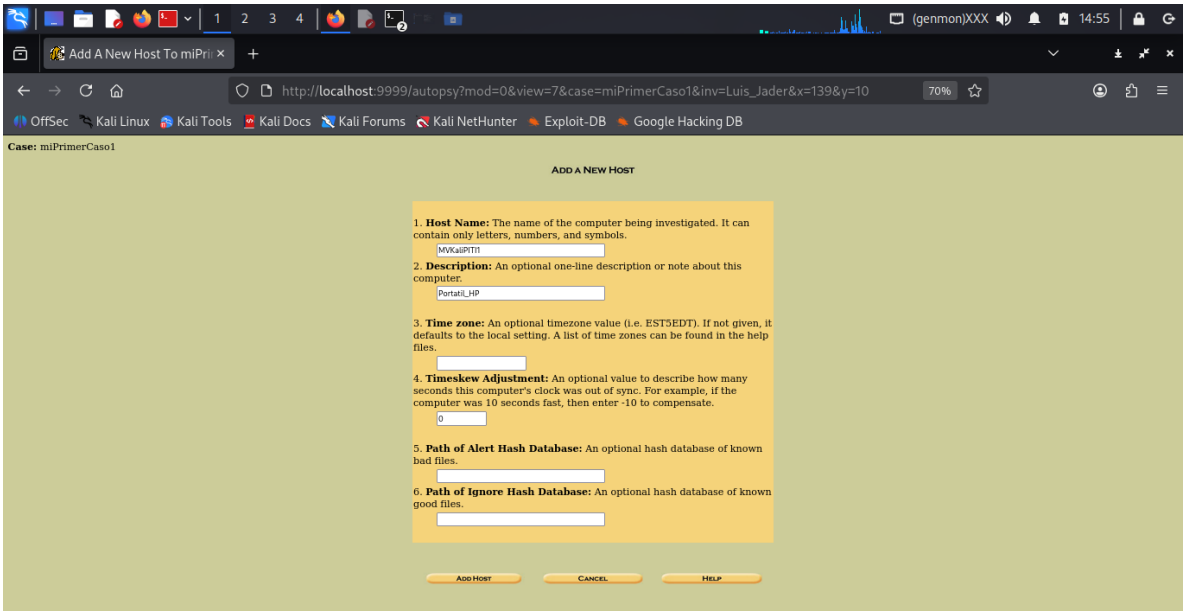


Ilustración 13 Agregar un nuevo host.

Se confirma la configuración de un nuevo host en Autopsy la configuración se muestra configuración dentro de un caso activo. El sistema genera automáticamente los siguientes elementos estructurales esenciales para la administración del caso:

Dirección de host: /var/lib/autopsy/miPrimerCaso1/MVKaliPT1/
Esta ruta corresponde al directorio donde se almacenan los archivos y configuraciones asociadas a este host. Autopsy organiza la evidencia de manera jerárquica para mantener la integridad y separación entre los distintos dispositivos analizados.

Configurado:
/var/lib/autopsy/miPrimerCaso1/MVKal/var/lib/autopsy/miPrimerCaso1/MVKaliPT1/host.aut

El siguiente paso es importar la imagen para lograr el análisis completo de este caso.

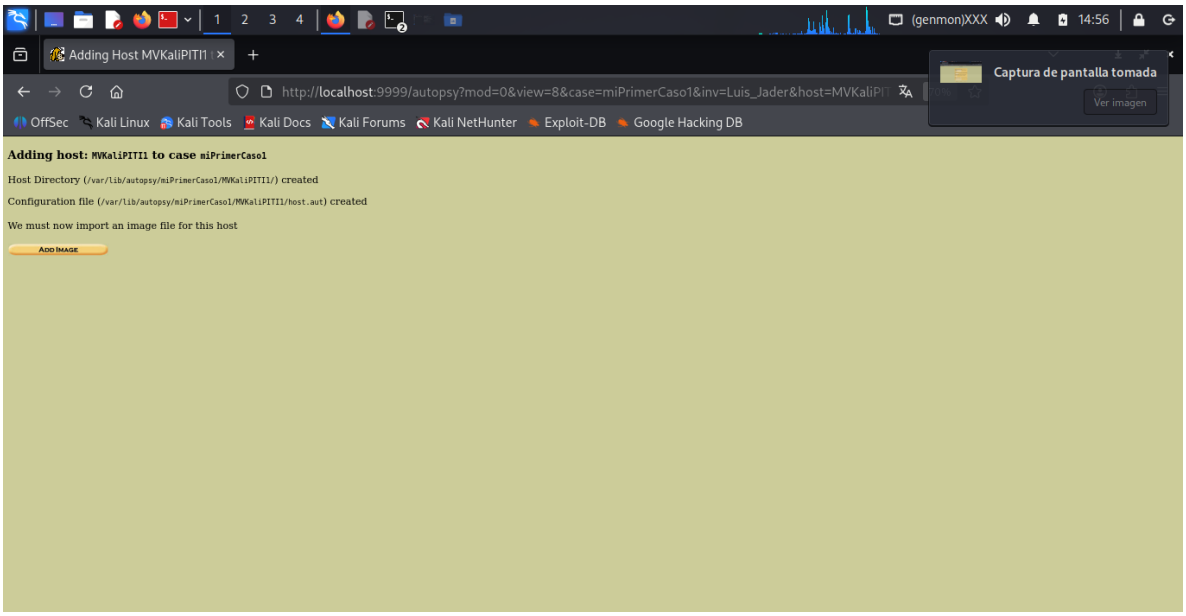


Ilustración 14 Importar imagen dd 1.

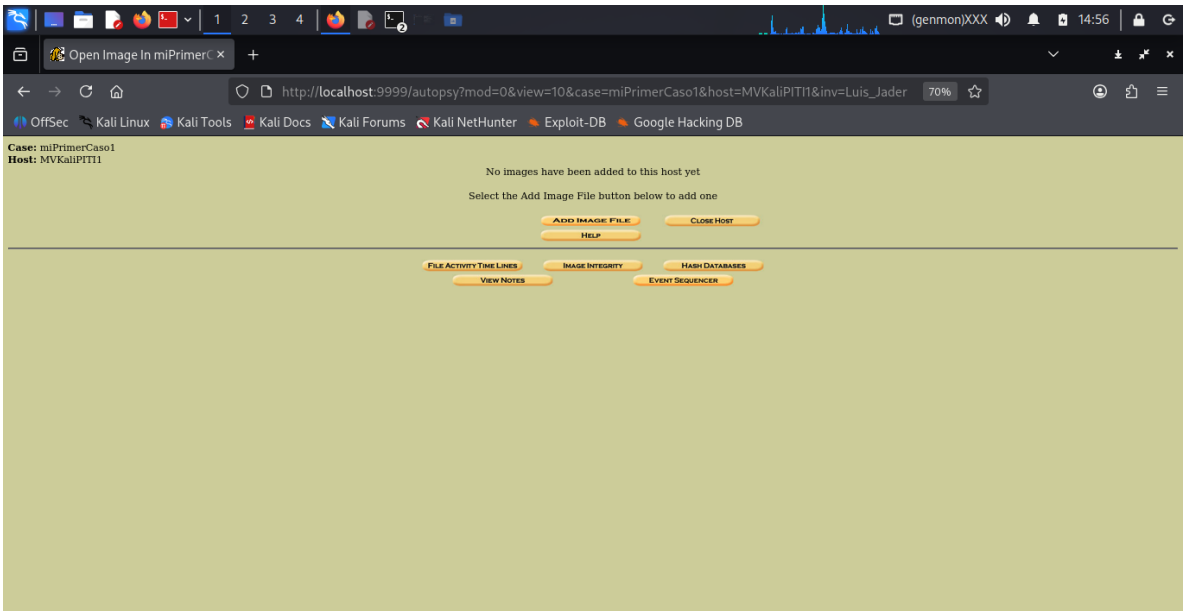


Ilustración 15 Importación de una imagen forense en Autopsy 2

Importación de una imagen forense en Autopsy, una vez creado el host MVKaliPT1 dentro del caso miPrimerCaso1, el siguiente paso en la investigación forense consiste en importar la imagen forense correspondiente al dispositivo o medio de almacenamiento que se analizará.

En la interfaz mostrada en la imagen, Autopsy indica que aún no se han agregado imágenes a este host Por ello, se debe seleccionar el botón agregar Imagen, con el fin de vincular la imagen obtenida durante la fase de adquisición de evidencia digital.

Esta etapa es crítica, ya que la imagen forense generalmente en formato .dd, representa una copia bit a bit del medio físico original. Este archivo conserva la estructura exacta del dispositivo, incluyendo archivos visibles, ocultos y espacio no asignado, lo que garantiza la integridad y exhaustividad del análisis.
Además, la interfaz ofrece diversas herramientas que se activarán una vez se importe la imagen, entre ellas:
Esta etapa asegura que la evidencia digital se analice en un entorno controlado y reproducible, cumpliendo con los principios de la informática forense: preservación, integridad, autenticidad y trazabilidad.
En **conclusión**, esta pantalla confirma que el entorno de análisis está preparado para recibir la imagen forense correspondiente al host MVKaliPT1, dando inicio formal al proceso de examen y correlación de evidencias digitales dentro del caso.

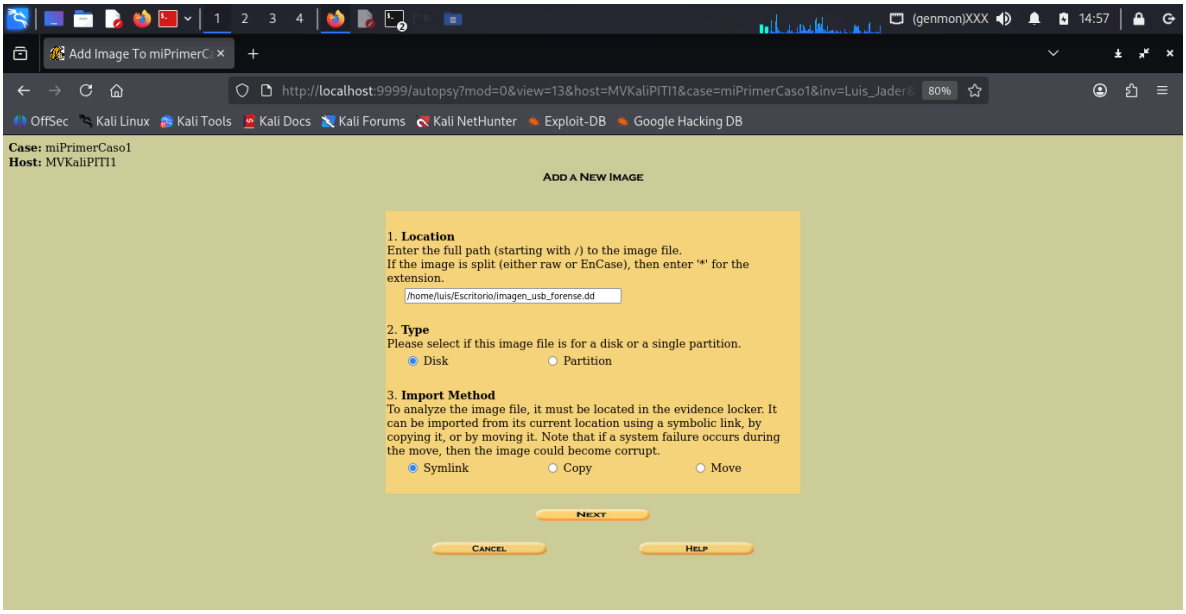


Ilustración 16 imagen seleccionada y lista para usar.

Se procede a importar la imagen forense en una localización conocida como escritorio de la siguiente forma: **/home/luis/Escritorio/imagen_usb_forense.dd** este método es uno de los más utilizados en la adquisición de evidencias digitales por su fidelidad y compatibilidad con herramientas forenses.
A partir de este momento iniciaron mis frustraciones debido a que estaba insistiendo en hacer el laboratorio igual a las instrucciones dadas por el tutor y en mi caso debía seleccionar otro tipo de sistema de volumen por eso La autopsia no pudo determinar de forma automática el tipo de sistema de volumen presente en la imagen. Este tipo de errores puede ocurrir porque:

- La imagen proviene de un dispositivo con una estructura de particiones no estándar.
- El sector de arranque (MBR o GPT) está dañado o modificado.

- Se trata de una copia parcial o de un medio que contiene datos sin formato.

En mi caso debía seleccionar **volumen Image** para poder avanzar como era de esperar de lo contrario me mostraría algo diferente a lo que habíamos visto en la práctica con el docente.

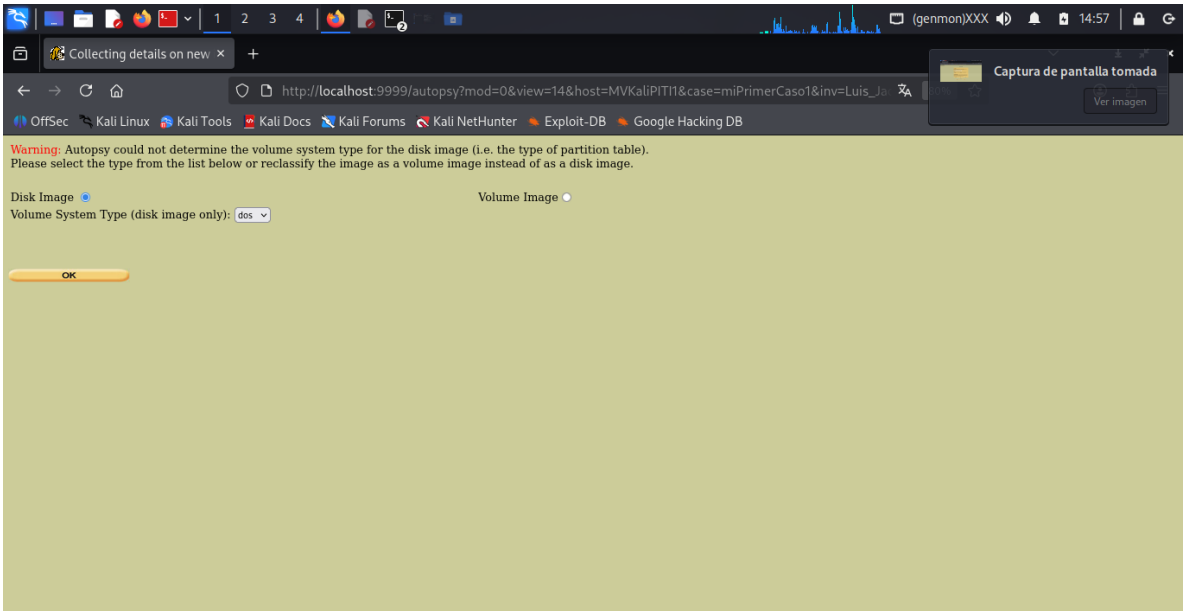


Ilustración 17 identificación del tipo de sistema de volumen.

Se puede apreciar que en este paso no se está mostrando la partición **C** como debía verse esto es debido al error que se estaba notificando anteriormente. Aunque la imagen se haya cargado.

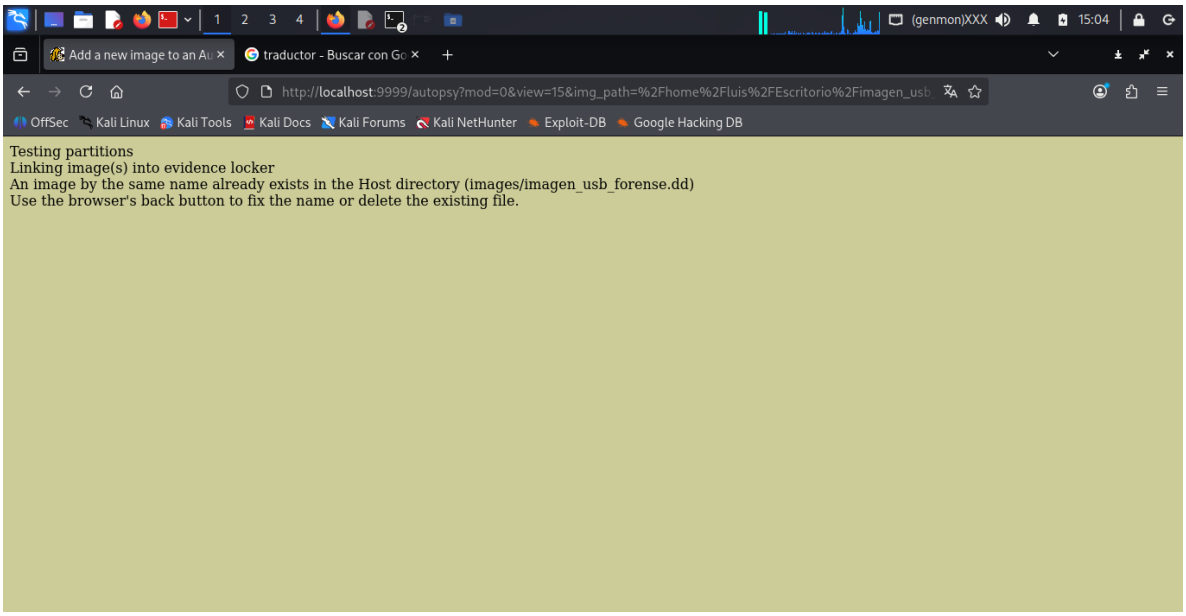


Ilustración 18 intentos repetidos para cargar la imagen de la forma correcta.

Debido a que no había seleccionado el tipo de volumen correcto para mi imagen me seguía mostrando los detalles del archivo de imagen pero sin una partición c como debería sin que eso pasara era una perdida de tiempo creer que podría avanzar con normalidad para ver los archivos contenidos luego del análisis.

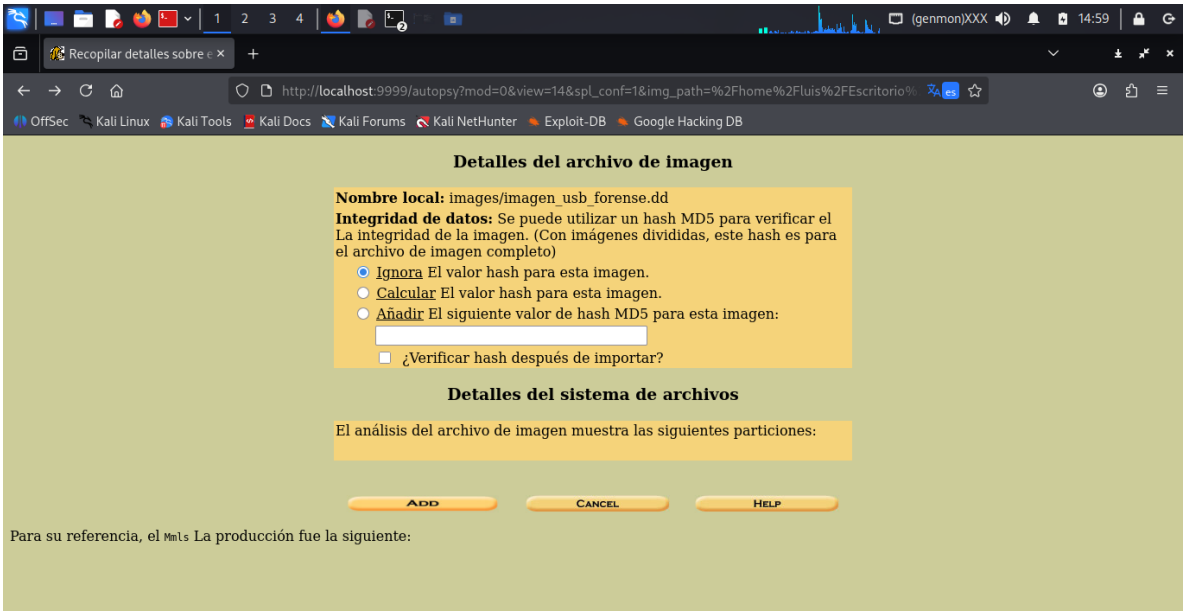


Ilustración 19 Detalles del Archivo de Imagen.

Se puede apreciar que llegue a crear hasta más de 2 imagen forense .dd en este caso se nota como estoy procesando la creación de una segunda imagen.

Ilustración 20 creación de una segunda imagen forense .dd.

se procedió agregar la imagen varias veces por desconocimiento del tema y no me funcionaba, finamente decidí crear una segunda imagen y hasta un nuevo hash tratando dar solución al asunto y esto no resolvía mi angustiosa situación, tanto que hasta llegue a escribirle al docente vía WhatsApp para que me asesorara en dicho tema.

Ilustración 21 segunda imagen forense creada.

Se crea una segunda imagen tratando de llegar hasta la solución del inconveniente y esto no resolvía tal error.

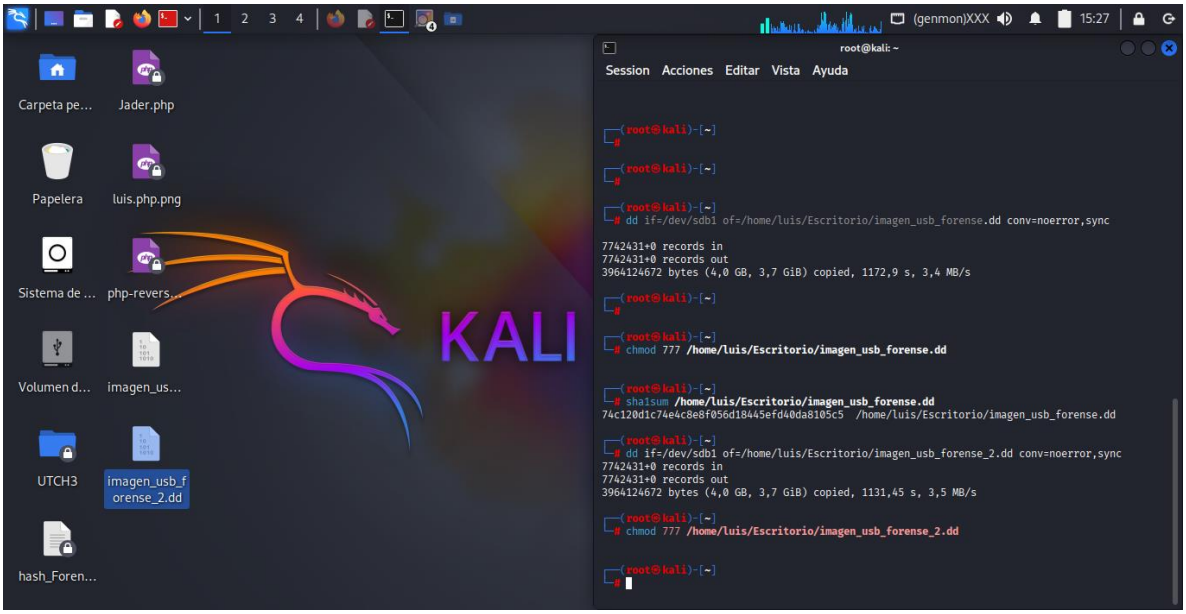


Ilustración 22 vista segunda imagen creada.

Pude llegar a crear hasta más de un caso y esto no solucionaba mi situación.

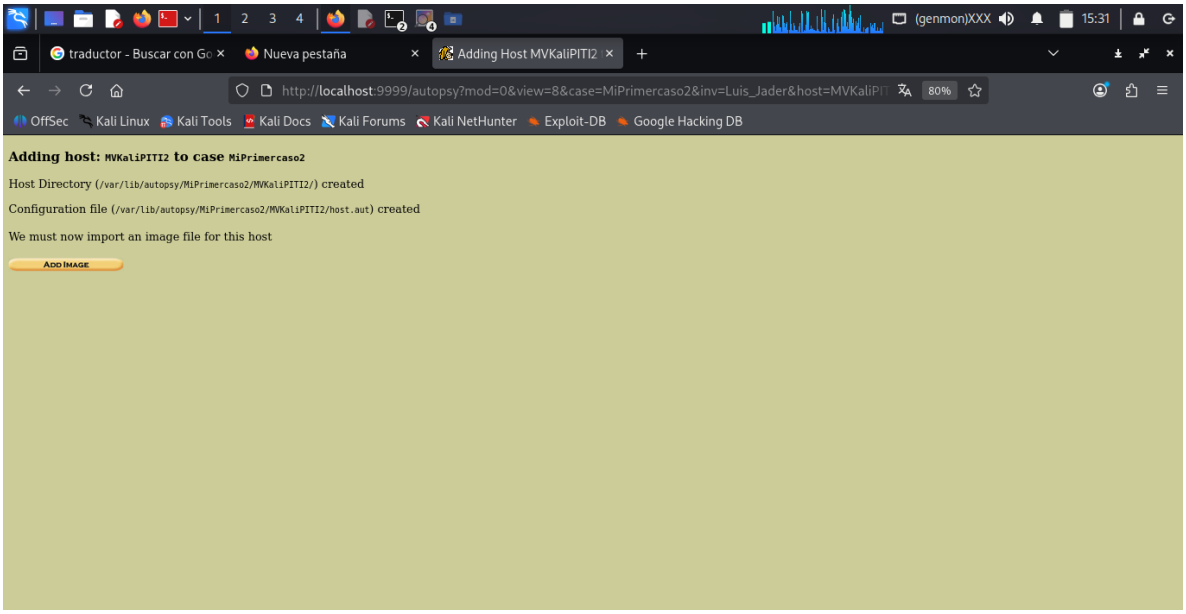


Ilustración 23, segundo caso creado llamado MiPrimercaso2

Posteriormente cree mi tercera clase no todas quedaron registradas en capturas debido a que no conseguía resultados el desespero me estaba ganando el caso.

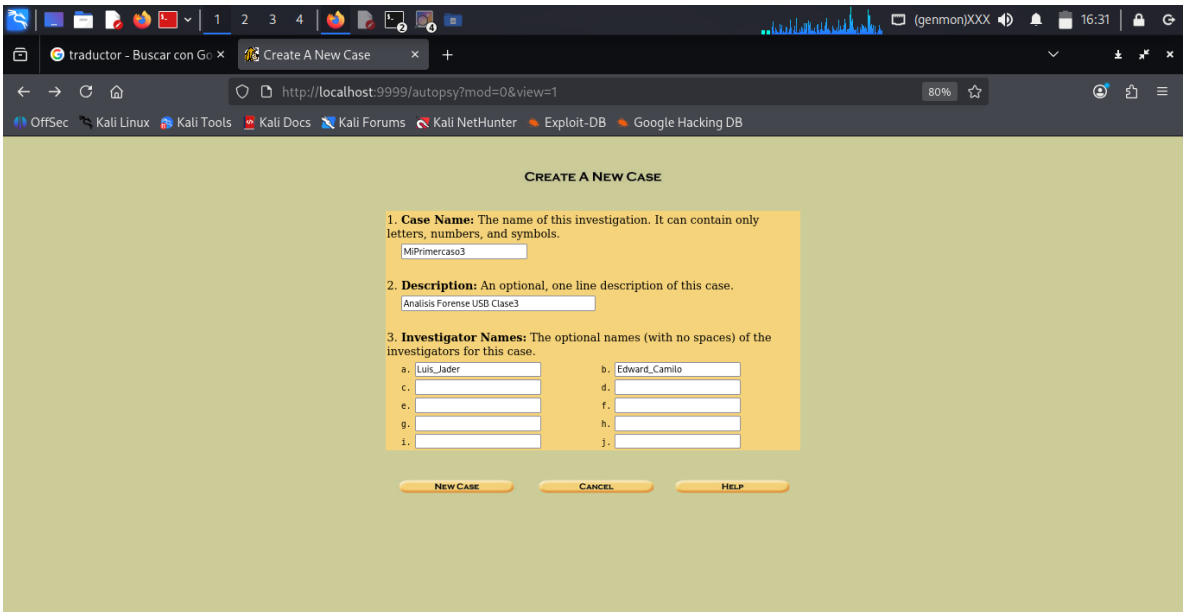


Ilustración 24 tercer caso creado llamado MiPrimercaso3

Tercer imagen creada y cargada después de pasar por alto algunos pasos repetidos como creación de hash y de imágenes forenses llegue a la conclusión: que el problema no era de estos archivos el problema radicaba en otra cosa.

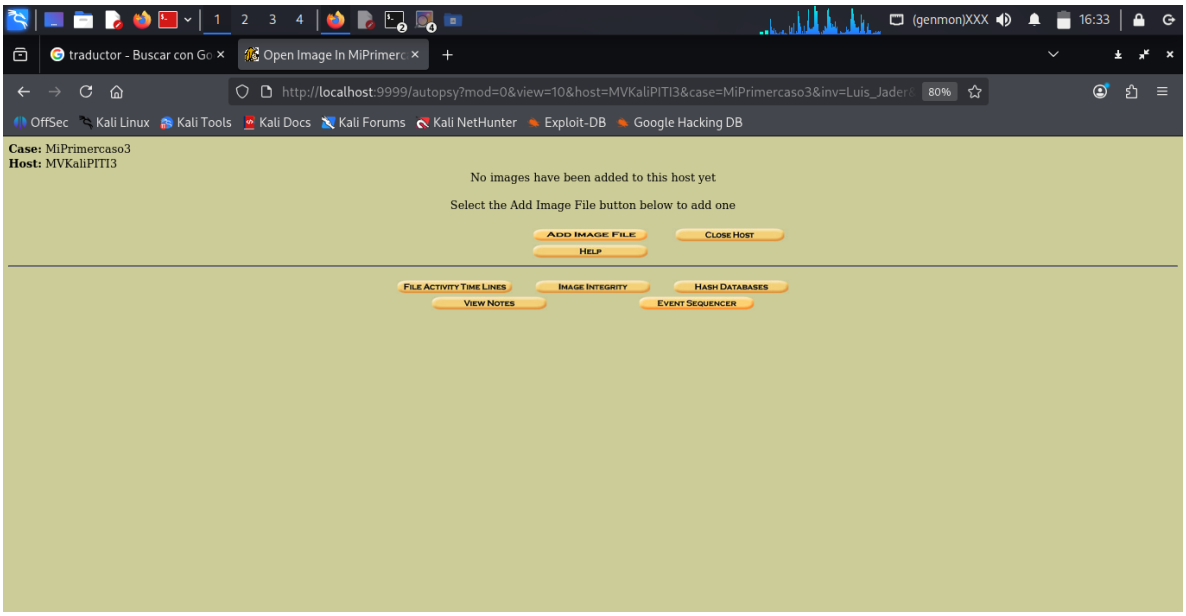


Ilustración 25 carga última imagen.

En este paso acabaron mis preocupaciones ya que intente con otro tipo de volumen llamado volumen de imagen, y fue allí cuando note que el avance se vio afectado debido a una configuración incorrecta del tipo de volumen.

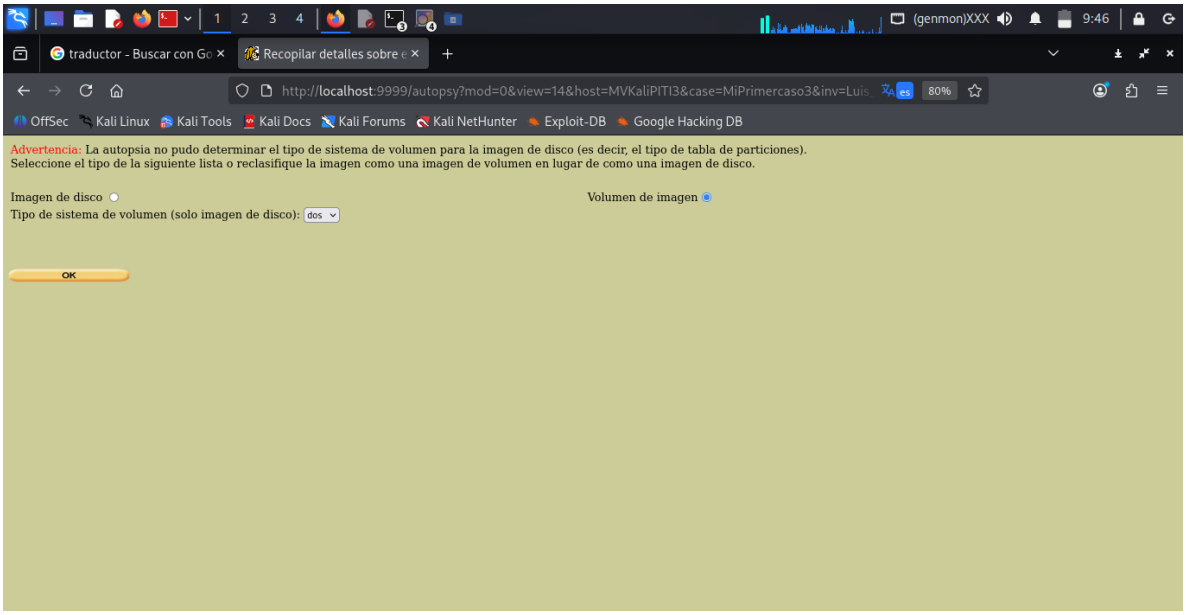


Ilustración 26 cambio de Imagen de disco a volumen de imagen.

Podemos apreciar que al cambiar la selección del tipo de volumen, este laboratorio siguió su rumbo porque pude llegar a la etapa final de importación y montaje de la imagen forense dentro de autopsy, ya reconoció correctamente el sistema de archivo y se encuentra listo para su análisis.

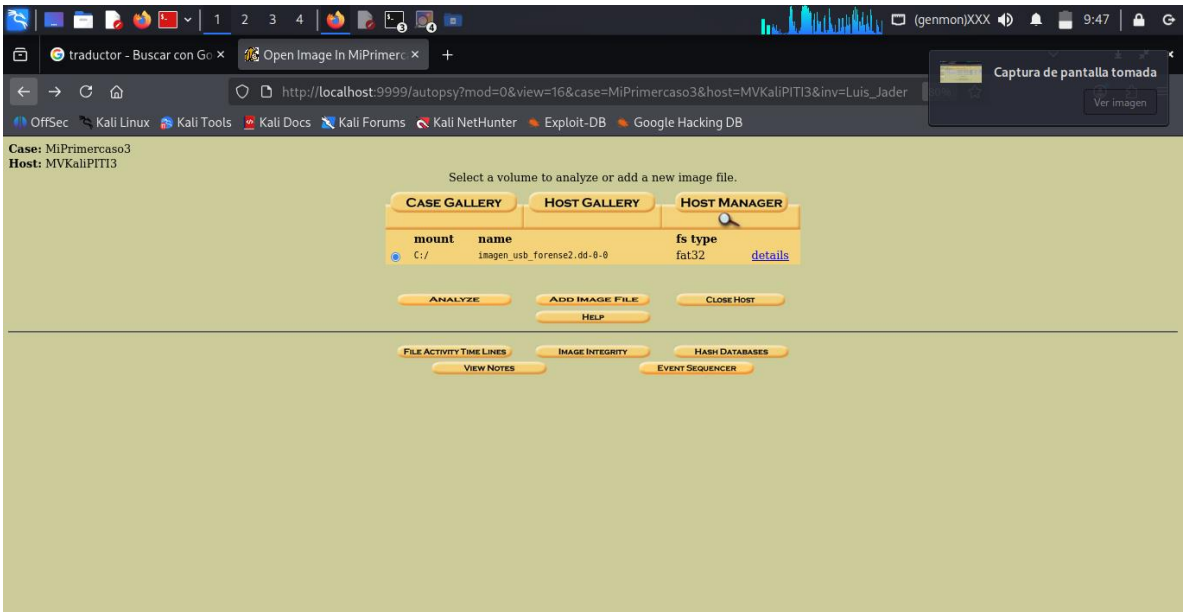


Ilustración 27imagen forense 2 montada en el directorio Raíz C:/

Finalmente pude realizar el análisis completo pero mi caso terminó siendo:
Caso: **MiPrimerCaso3.**
El host: **MVKaliPITI3**

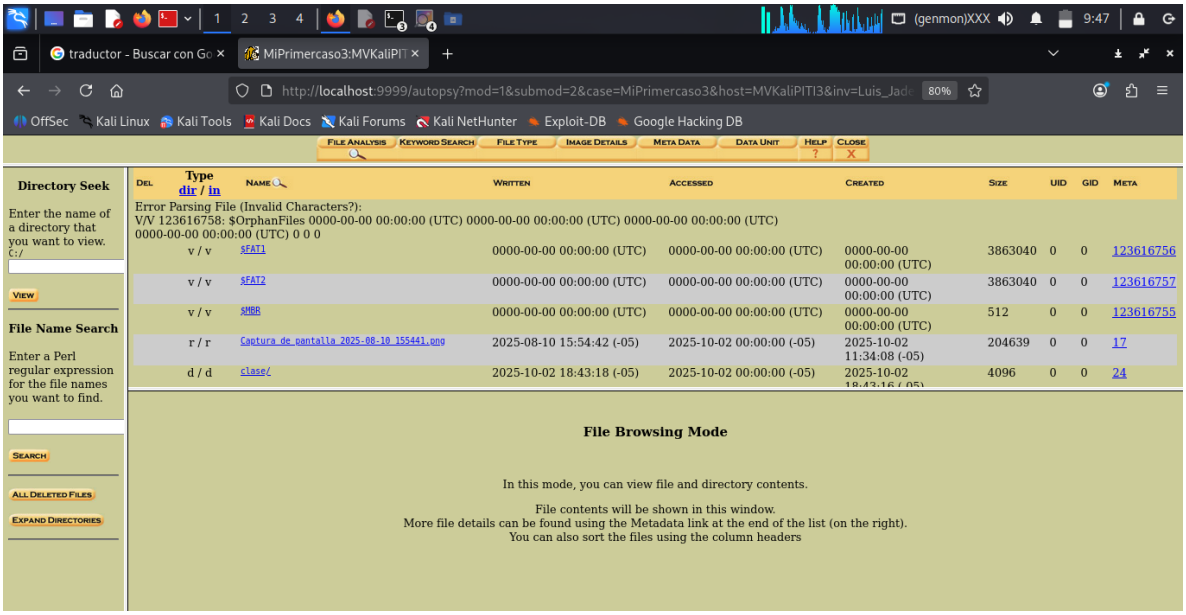


Ilustración 28 vista de archivos analizados desde la imagen forense.

En **conclusión**, esta etapa representa el inicio del **análisis sustantivo de la evidencia digital**, en la que se examina la estructura del sistema de archivos, los directorios y los objetos almacenados. Los resultados obtenidos permitirán identificar información de relevancia, reconstruir actividades de usuario y establecer

posibles correlaciones temporales que apoyen las hipótesis de la investigación forense.

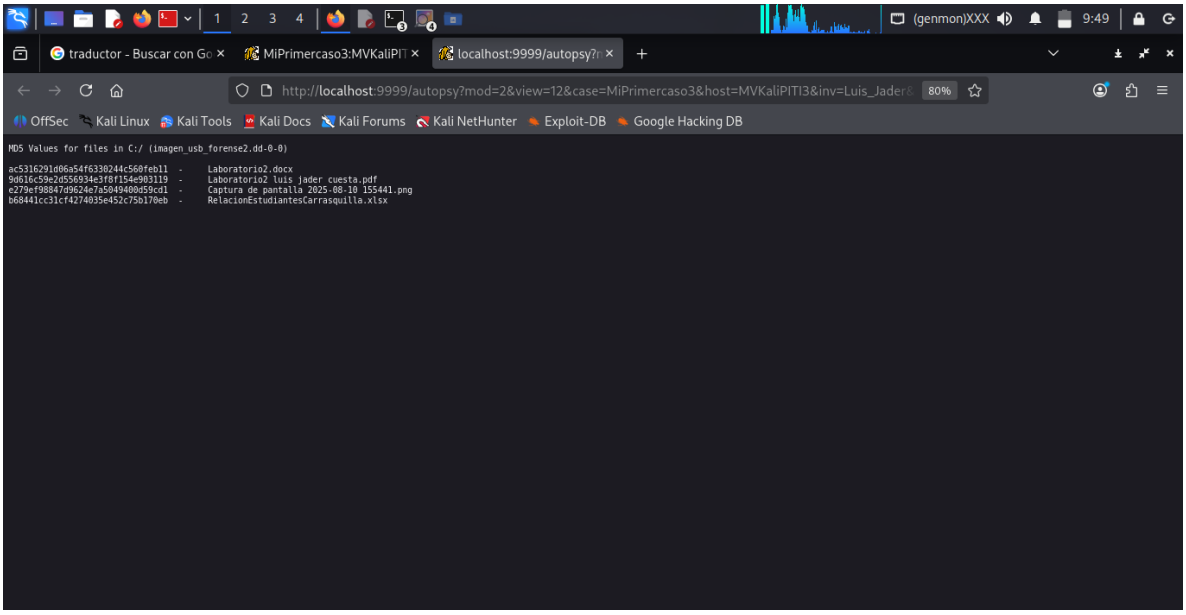


Ilustración 29 cálculo de valores hash.

Como parte del procedimiento de análisis forense, se realizó el cálculo de los valores **hash MD5** de los archivos contenidos en la imagen forense **imagen_usb_forense2.dd**, montada en la herramienta **Autopsia**.

Así concluye el capítulo 1 del análisis forense.

Capítulo 2

2. INSTALACIÓN FTK IMAGER

Esta sería la interfaz del instalación de la herramienta **FTK** en **Windows** se logra ver la pantalla de bienvenida, esta es una herramienta forense digital usada para crear imágenes forenses y analizar datos sin alterar el original.

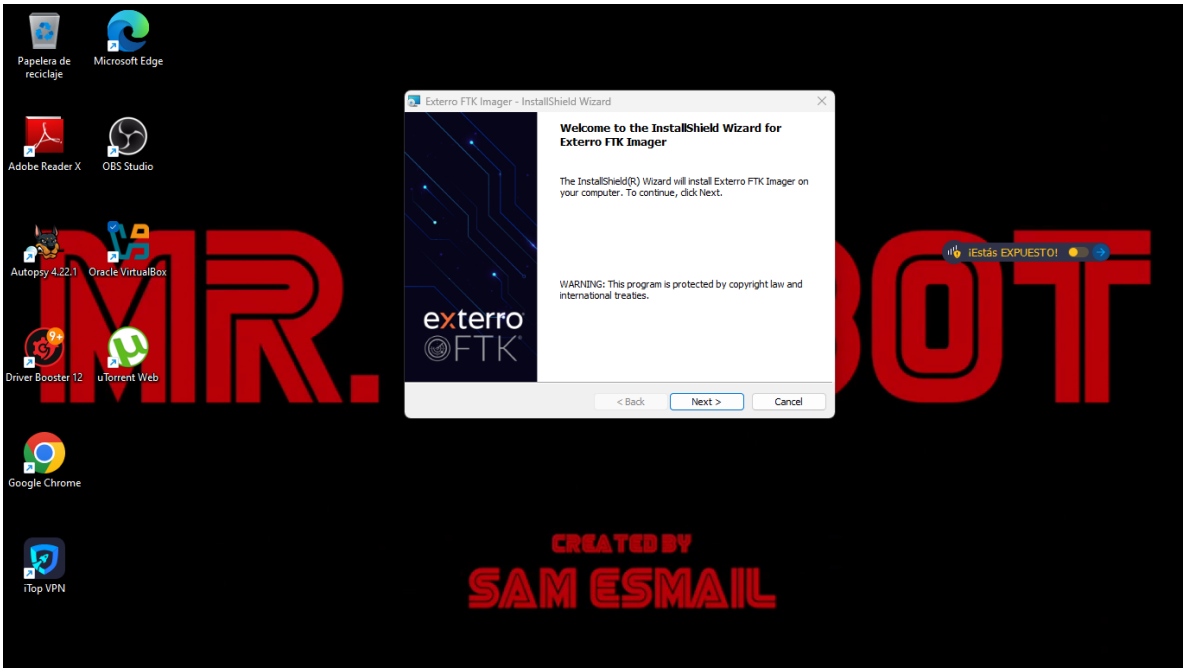


Ilustración 30 interfaz de instalación FTK

Acuerdo de licencia que el usuario debe leer y aceptar antes de continuar.

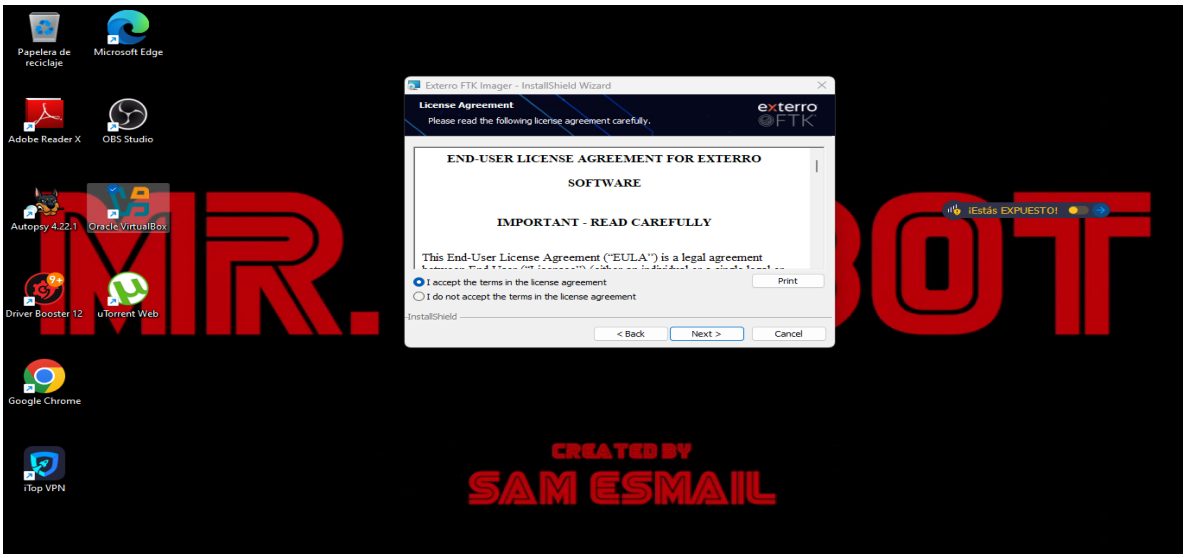


Ilustración 31 acuerdo de licencia de usuario

Este paso muestra la ruta donde se instalara esta herramienta.

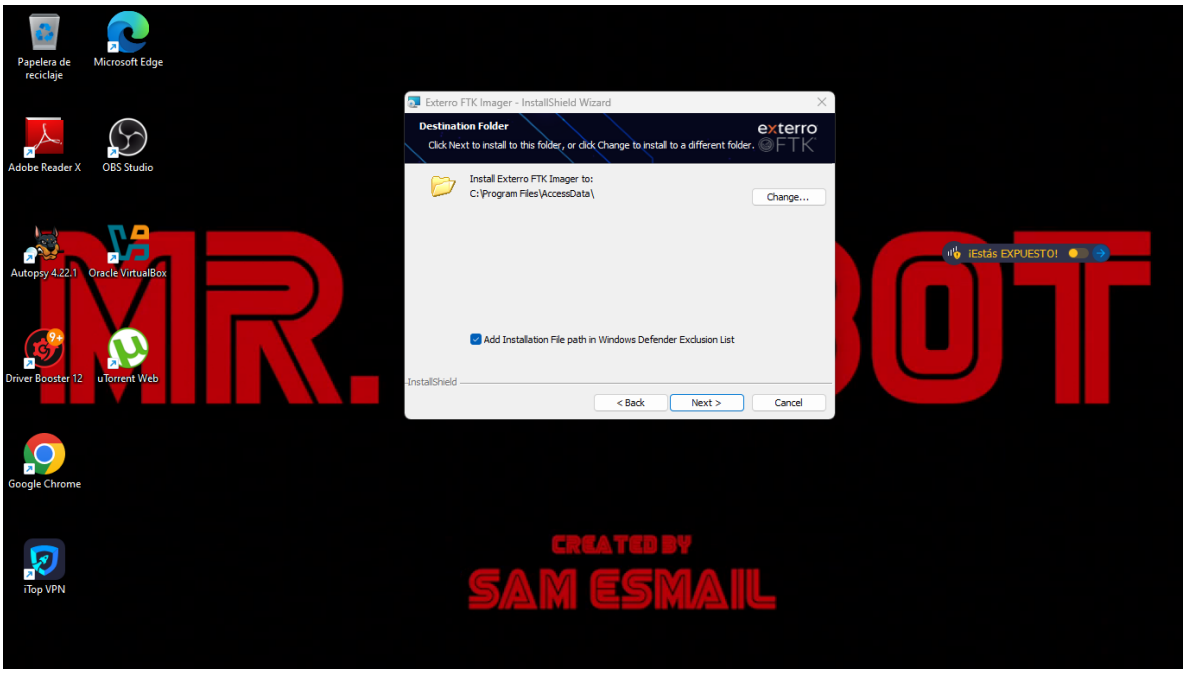


Ilustración 32 Ruta de Instalación.

Se indica que las configuraciones de instalación para esta herramienta ya fueron instaladas.

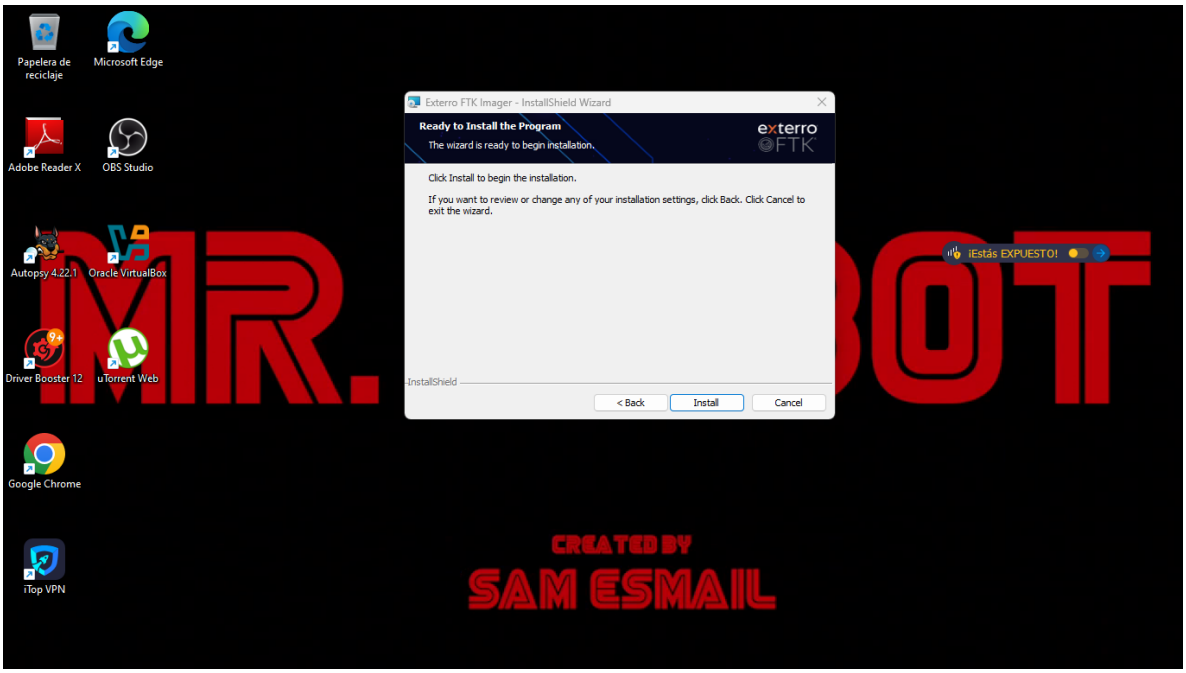


Ilustración 33 Ready to Install the Program

Instalación de FTK Imager se completó correctamente lo que confirma que el proceso fue exitoso lo siguiente es dar clip en el botón finalizar.

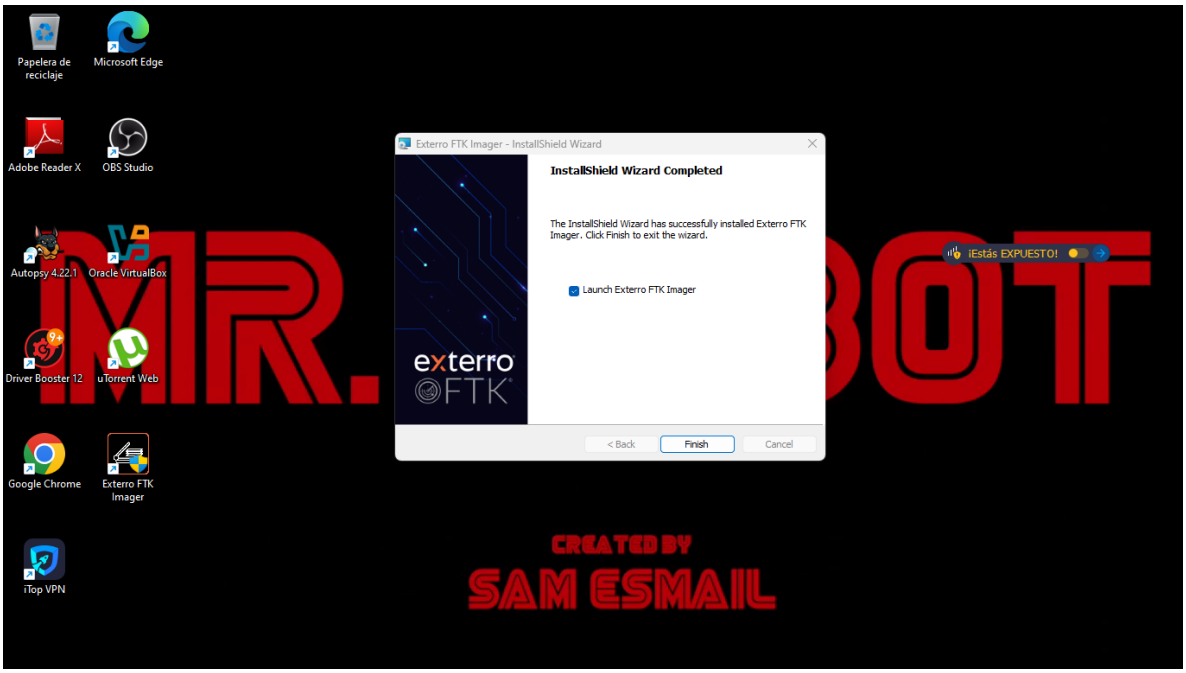


Ilustración 34 Instalación Finalizada.

La interfaz inicial de la herramienta FTK se ha abierto correctamente y está lista para usarse.

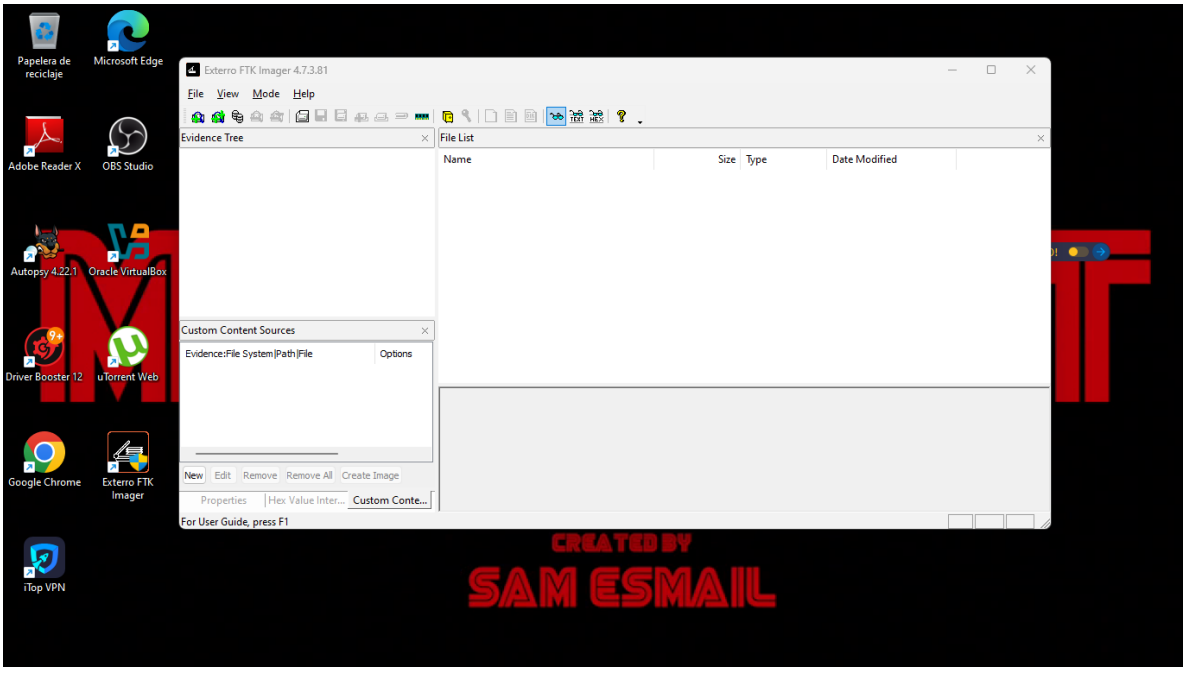


Ilustración 35 La interfaz inicial de la herramienta FTK.

2.1. Adquisición y resguardo de la imagen forense.

Esta ventana corresponde al paso correcto dentro de **FTK Imager** cuando se va a crear una imagen forense**.**

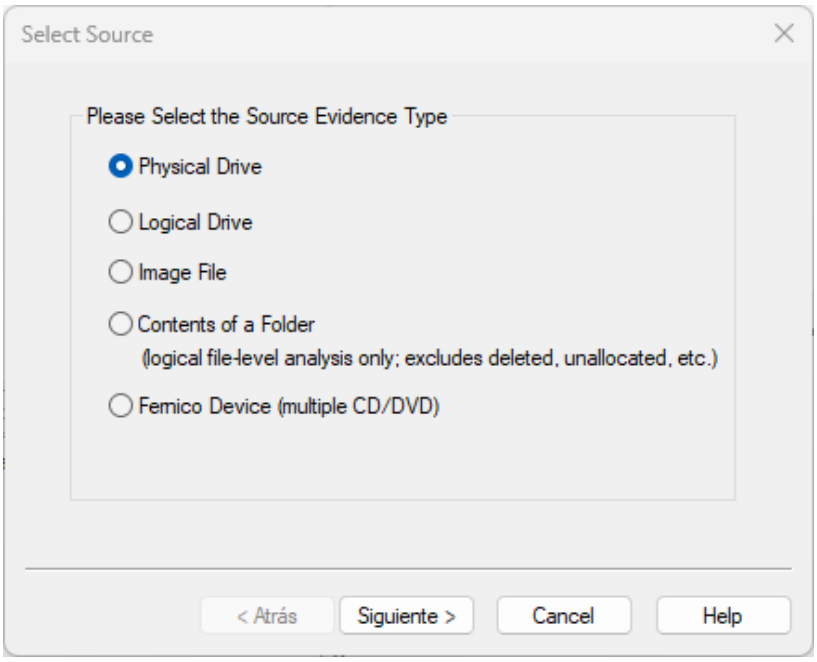


Ilustración 36 seleccionar el tipo de evidencia de origen

Paso dentro de **FTK Imager**, donde se elige el dispositivo físico de origen para crear la imagen forense. Se ha detectado una **unidad USB** conectada al sistema debemos tener cuidado para no perder el tiempo analizando otro dispositivo por errores a la hora de seleccionar el dispositivo a analizar.

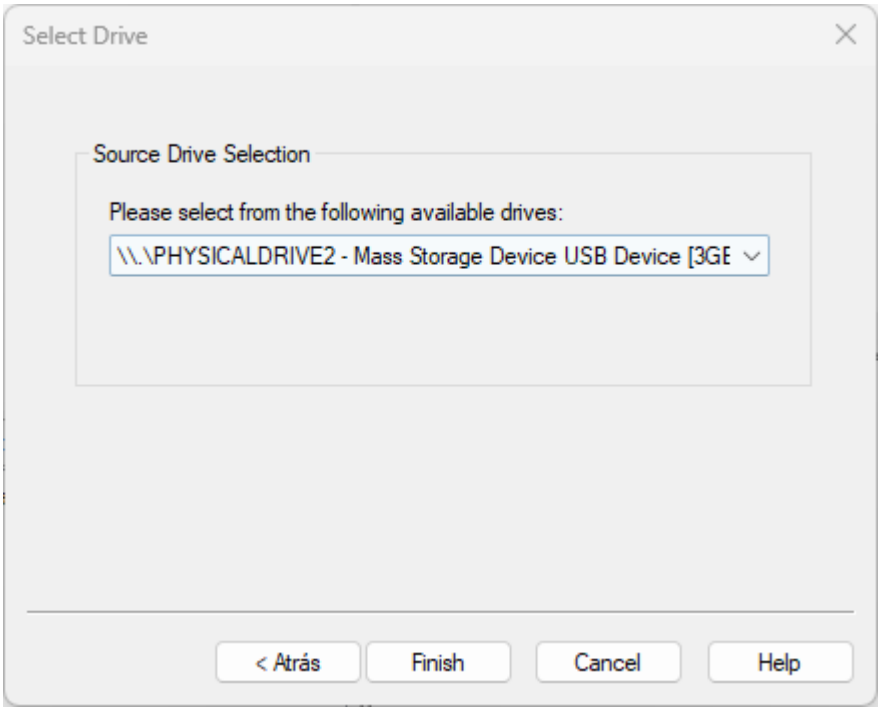


Ilustración 37 Select Drive.

Ya estás en la ventana clave de FTK Imager para configurar la creación de la imagen forense, Esta parte define dónde se guardará la evidencia y cómo se procesará. Una vez hayas agregado el destino y configurado el formato, el botón Start se activará. Al hacer clic en Start, FTK Imager iniciará la creación de la imagen forense.

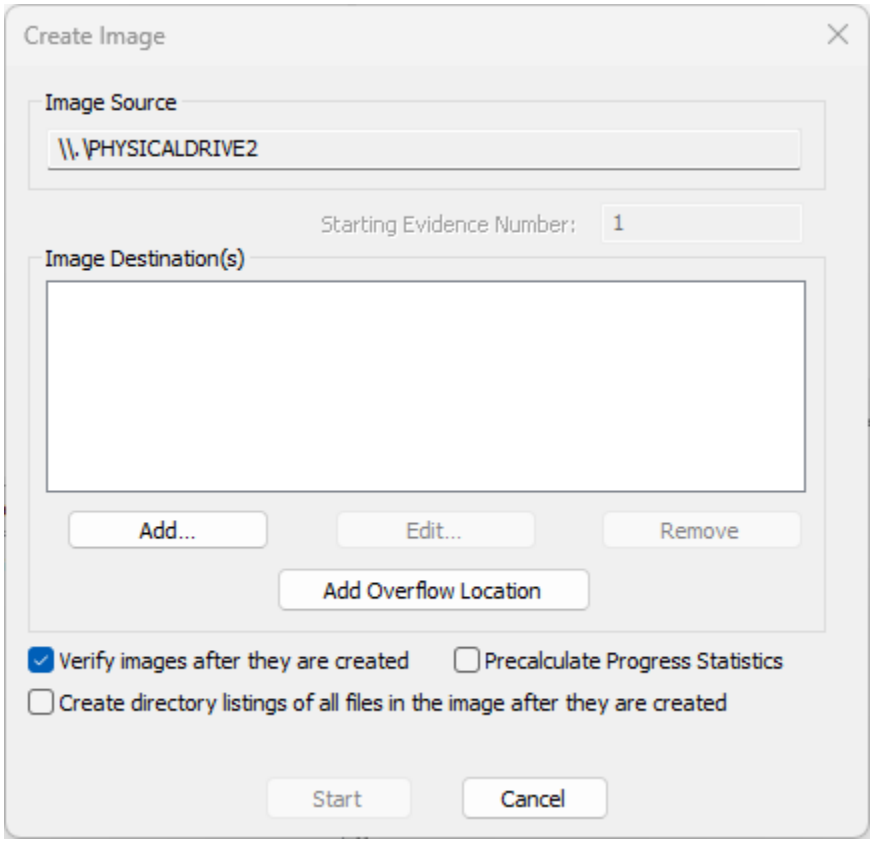


Ilustración 38 Image Source.

Es donde se debe elegir el formato del archivo de imagen forense que se creará.

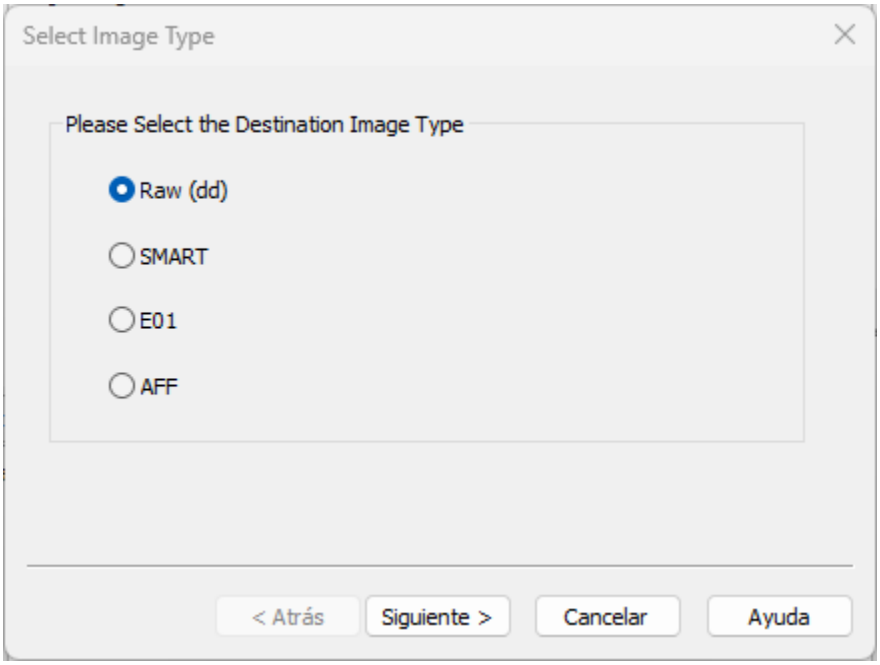


Ilustración 39 Select Image Type.

Esta ventana corresponde al paso Evidence Item Information en FTK Imager, donde ingresas los metadatos del caso forense.

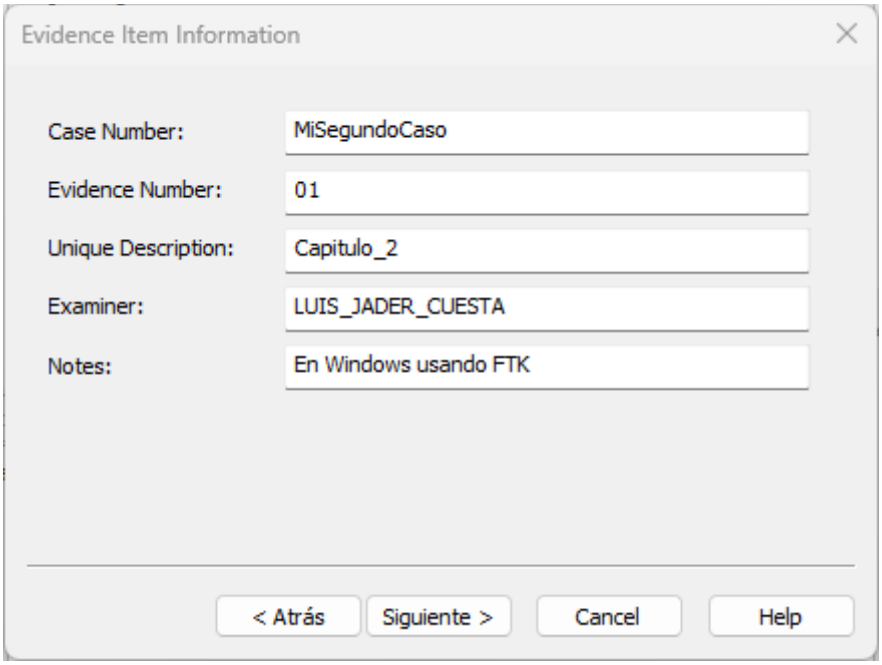


Ilustración 40 ingreso de los metadatos del caso forense.

Esta ventana es la **configuración final antes de crear la imagen forense** en FTK Imager.

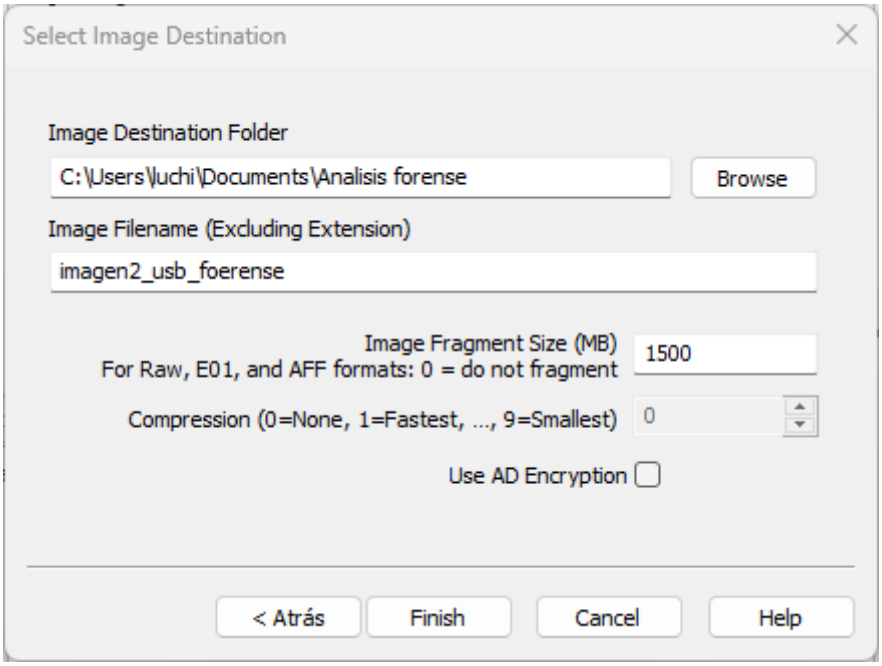


Ilustración 41 selec image Destination.

Crear imagen forense se utiliza en el contexto de la informática forense para realizar una **adquisición forense** de un dispositivo de almacenamiento.

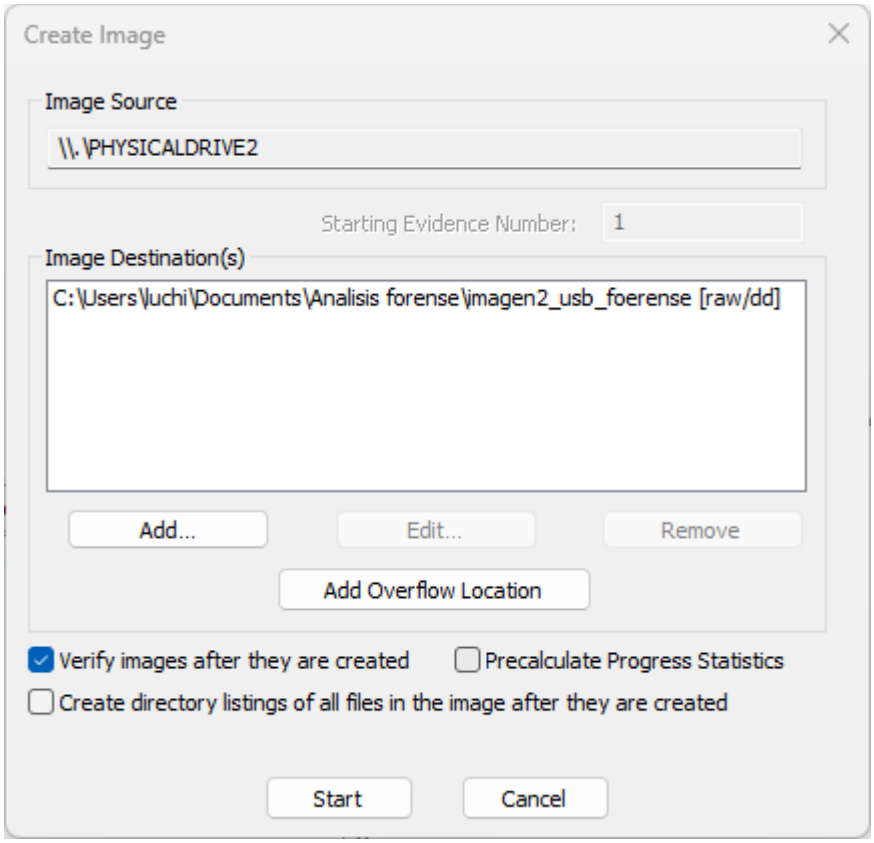


Ilustración 42 Image Source

La imagen muestra la ejecución del proceso de creación de una imagen forense.

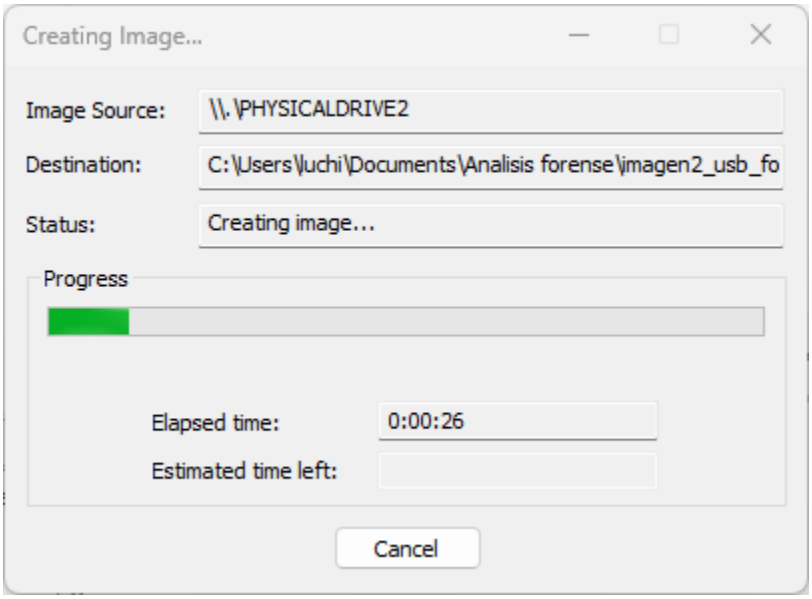


Ilustración 43 creacion de imagen en progreso.

Finalización exitosa del proceso de adquisición y verificación de la imagen forense, lo que marca el final de la fase de **preservación de evidencia** en una investigación digital.

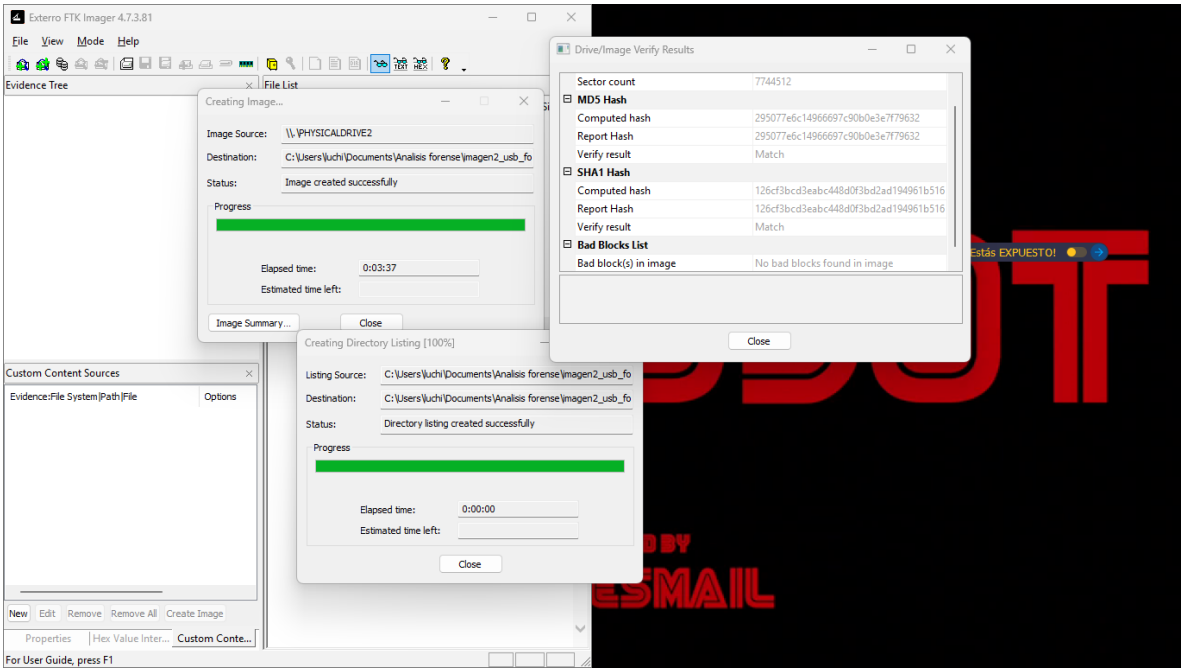


Ilustración 44 Análisis de la Evidencia Finalizada.

Registro de metadatos esenciales que acompaña a la imagen forense creada. Este resumen documenta la información del caso, los detalles del examinador y las especificaciones técnicas exactas del dispositivo de origen.

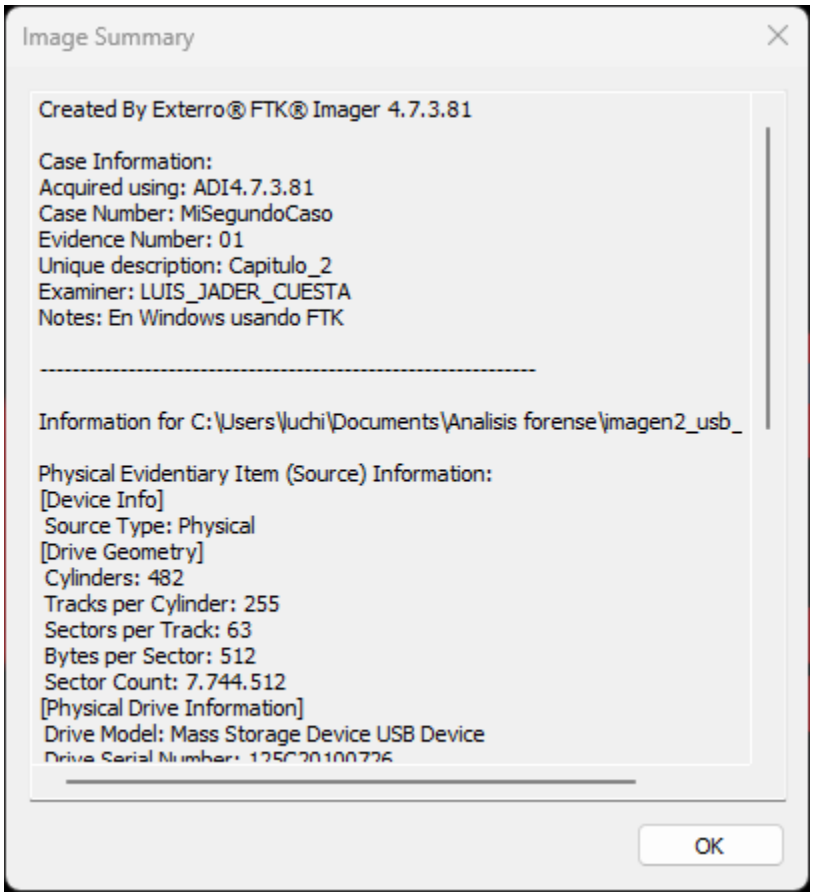


Ilustración 45 Registro de metadatos 1

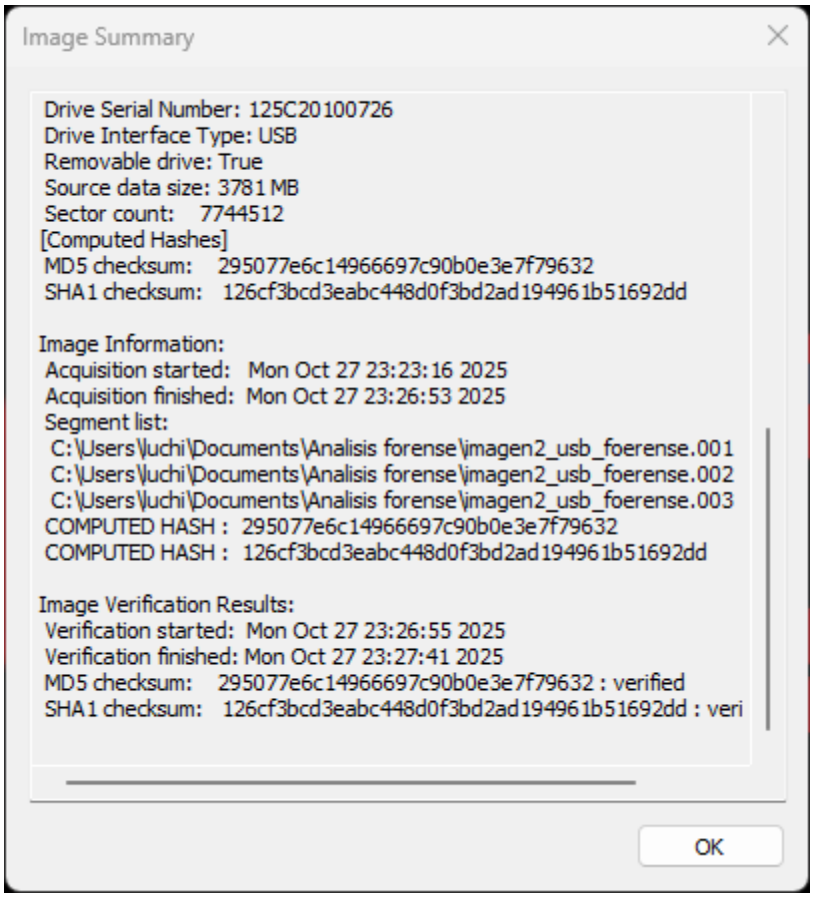


Ilustración 46 Registro de metadatos 2

Capítulo 3

3. INSTALACIÓN AUTOPSY

Durante la fase de adquisición de evidencia digital, se realizó la copia de la imagen forense denominada **imagen2_usb_foerense.001**, la cual contiene el volcado completo de un dispositivo USB previamente analizado.

Ilustración 47 pantalla de presentación

Preparando para instalar.

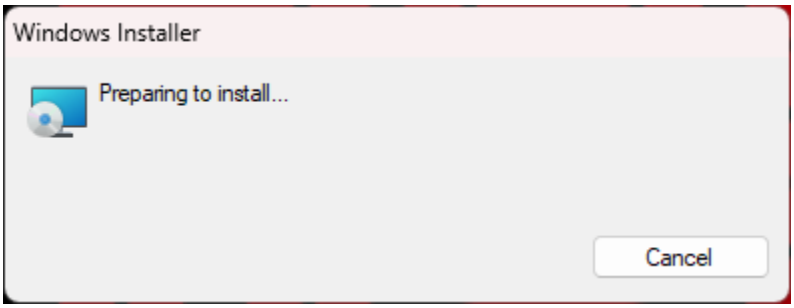


Ilustración 48 Windows Installer.

Paso inicial del asistente de instalación para el *software* de análisis forense Autopsy.

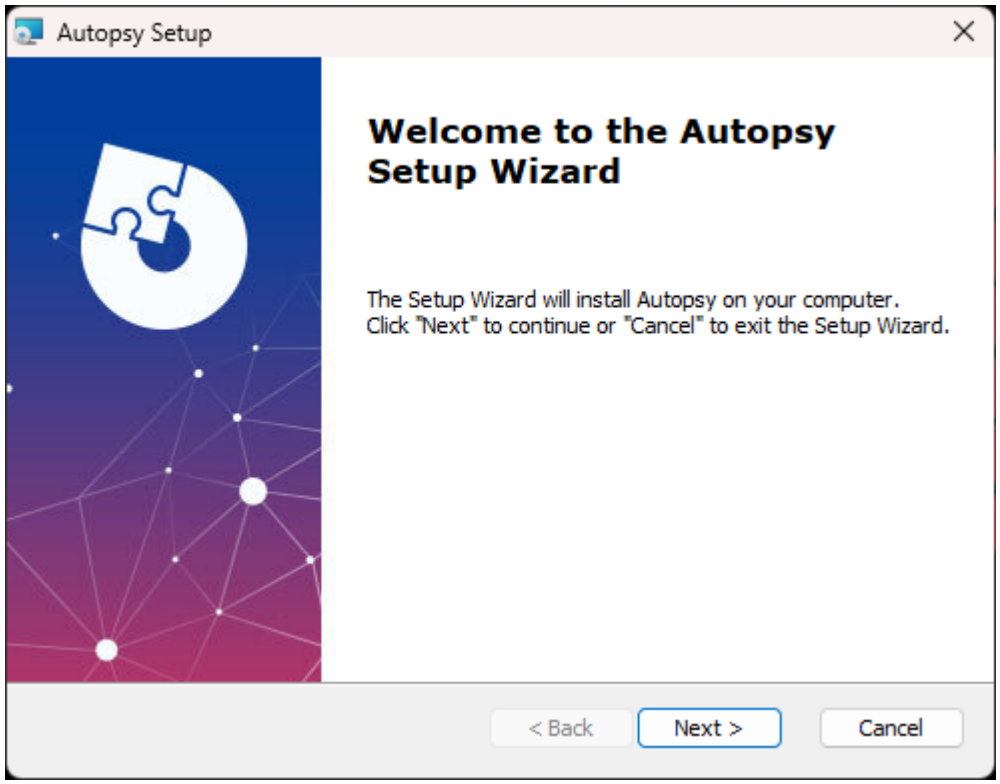


Ilustración 49 asistente de instalación.

Seleccionar Carpeta de Instalación.

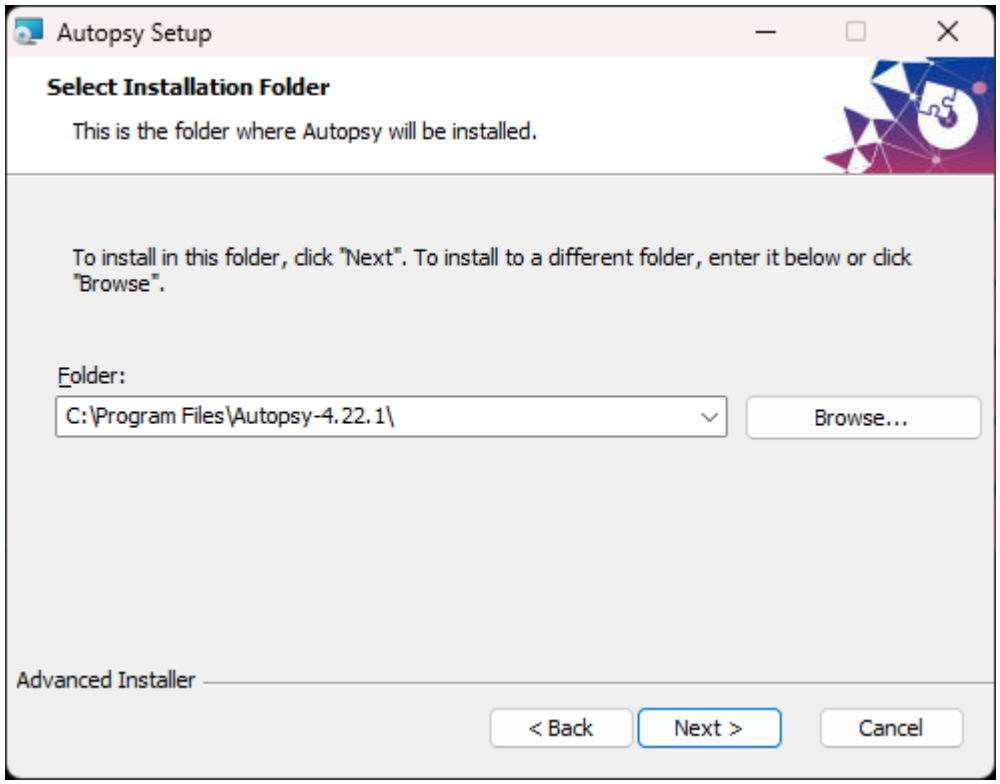


Ilustración 50 Seleccionar Carpeta de Instalación.

Listo para Instalar, asistente de configuración de **Autopsy**.

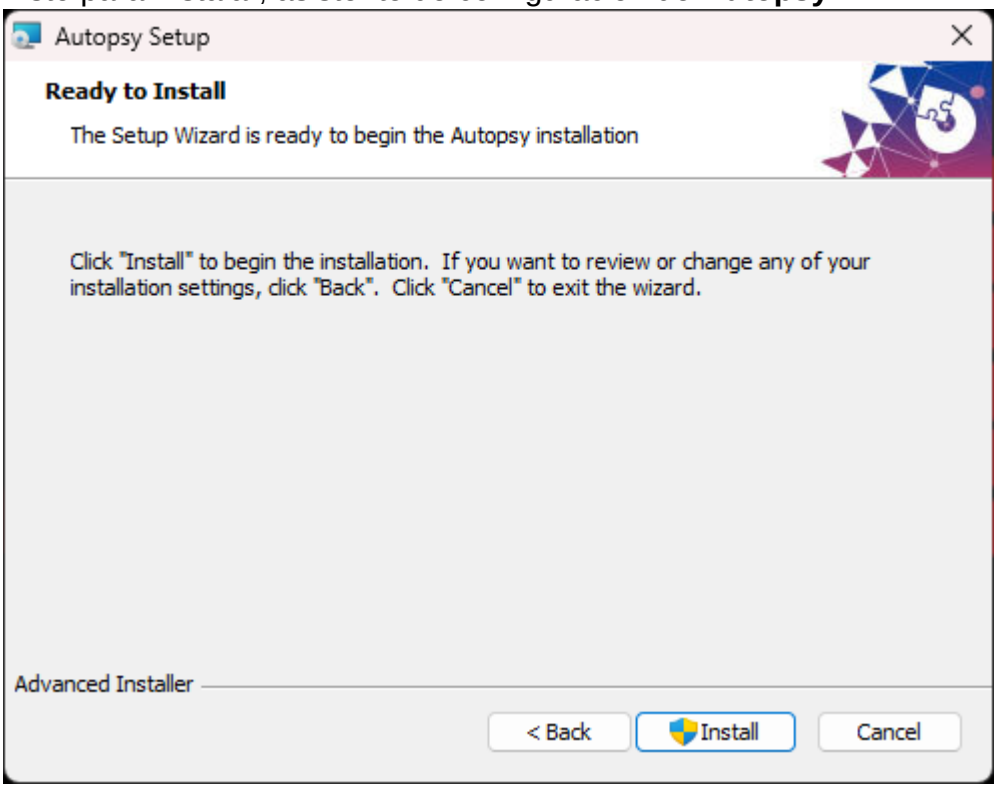


Ilustración 51 Ready to Install.

Indicacion que la instalación del *software* de análisis forense está actualmente en progreso

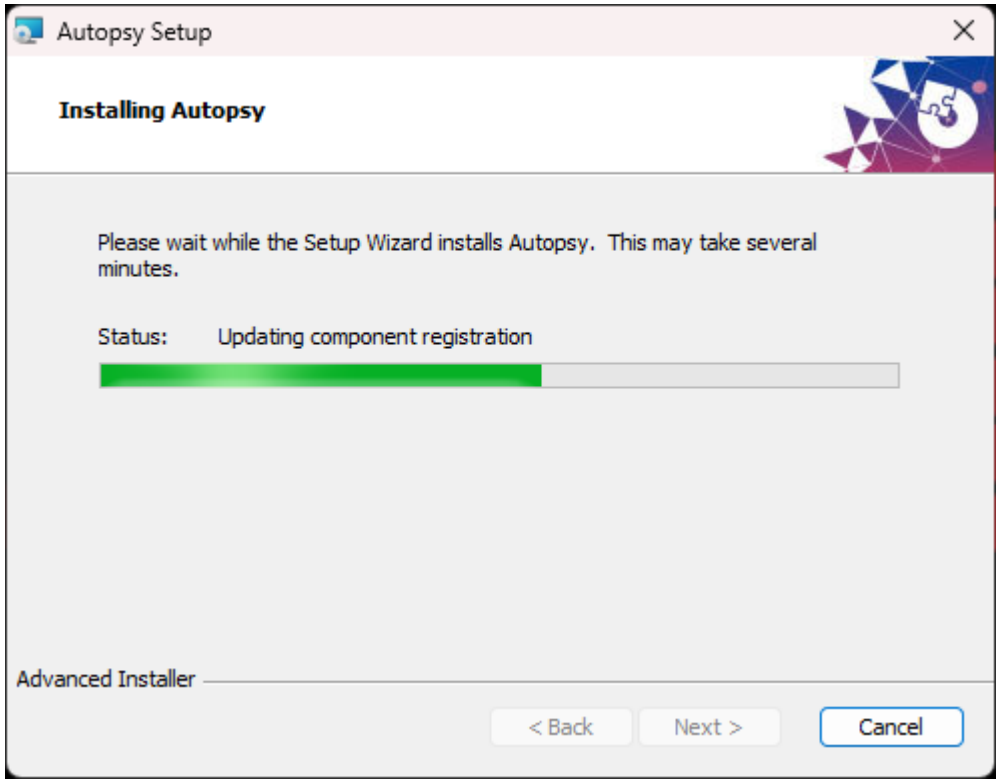


Ilustración 52 Instalando Autopsy.

el Asistente de Configuración de Autopsy Completado, lo que indica que la instalación del *software* de análisis forense Autopsy ha finalizado con éxito

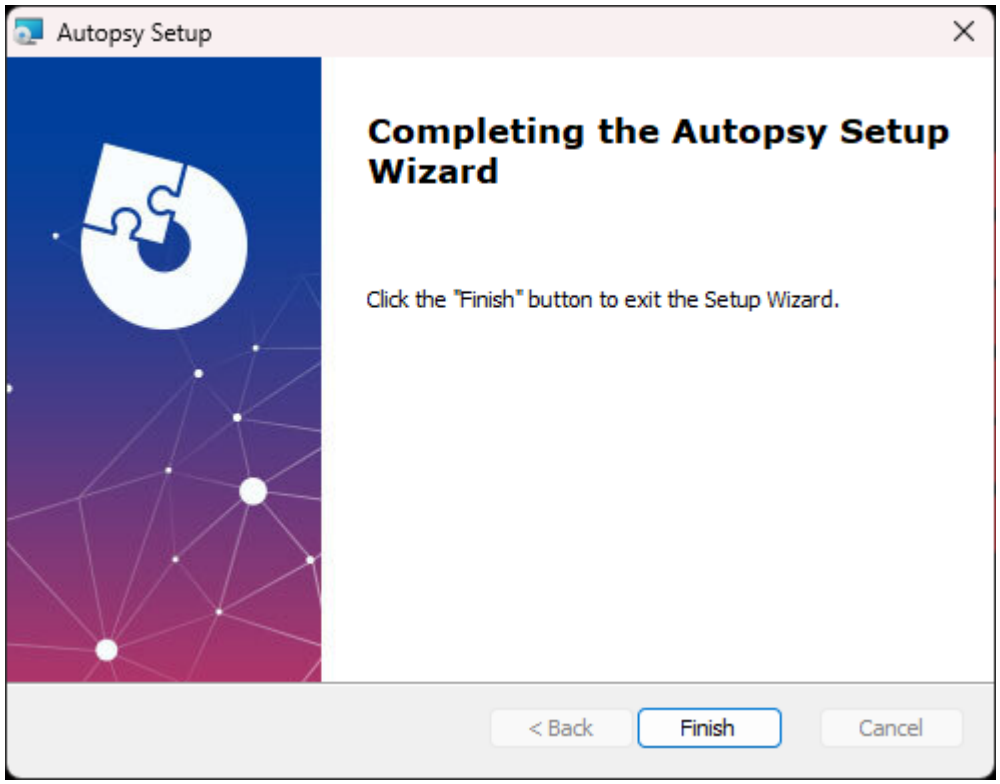


Ilustración 53 Finalización de la Instalación.

3.1. Análisis

Interfaz **de Autopsy**, una herramienta forense digital utilizada para analizar discos duros, imágenes de discos y otras fuentes de datos.
La ventana de bienvenida ofrece 3 opciones:

Nuevo caso: para iniciar un nuevo caso/proyecto forense.
Abrir caso reciente: para volver a abrir un caso en el que se trabajó recientemente, claro que en este caso se muestra deshabilitada puede ser porque no hay registro de algún caso abierto ya que es primera vez que se usa en este equipo.
Abrir caso: para abrir un archivo de caso existente.

Ilustración 54 Interfaz Autopsy.

Tras seleccionar la opción: **nuevo caso** en las opciones antes presentadas de la interfaz autopsy se detalla el siguiente campo para definir la información de un nuevo caso, como nombre del caso en esta oportunidad lo definimos de la siguiente manera: **Misegundocaso** y en la ubicación se definió de la siguiente forma: **C:\Users\luchi\Documents\Analisis forense**.

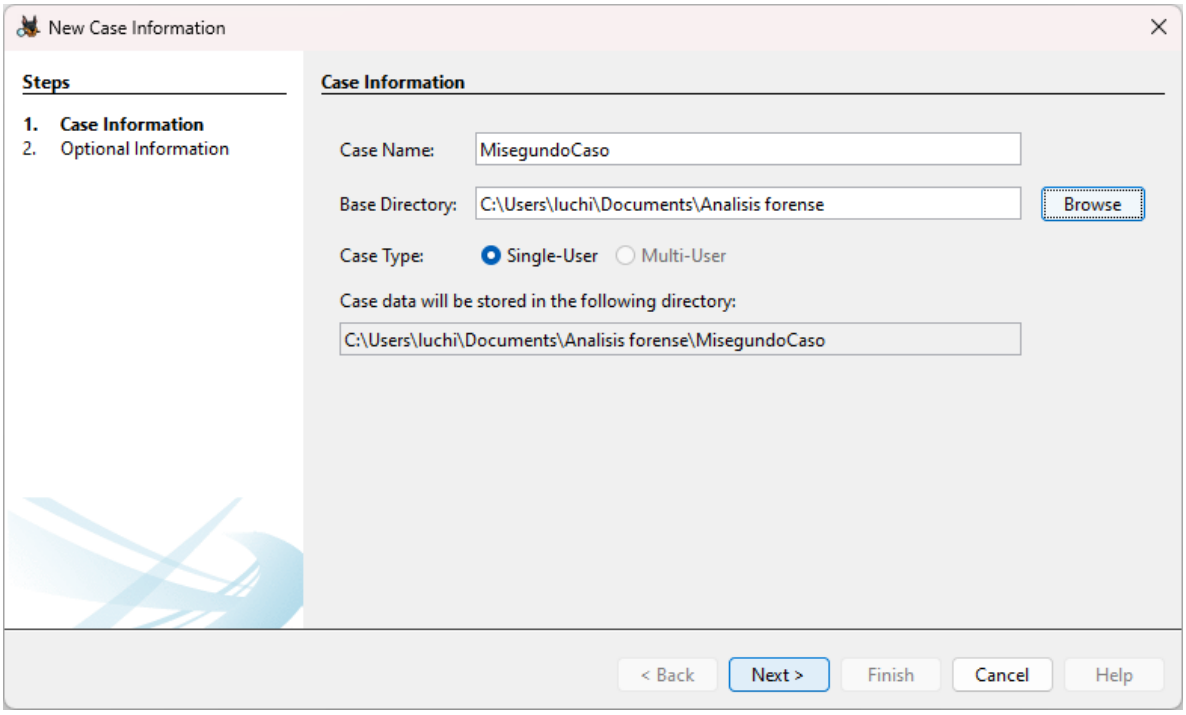


Ilustración 55 creación del caso.

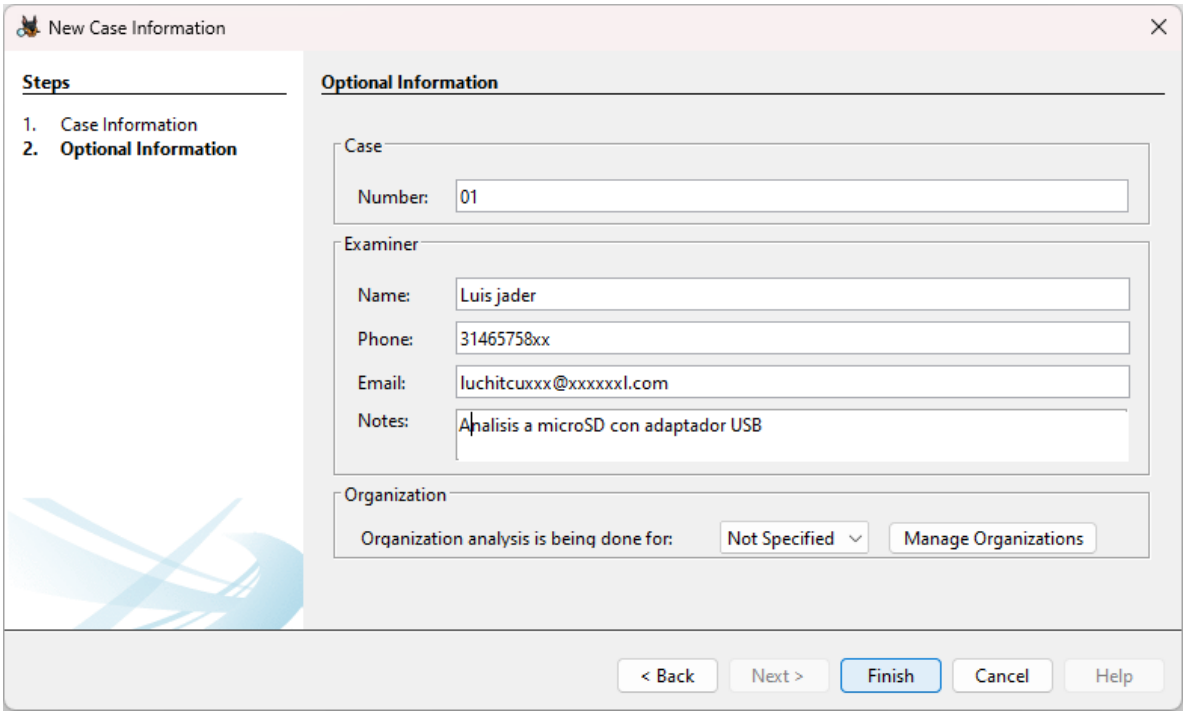


Ilustración 56 Información opcional.

Al finalizar se nos muestra una nueva ventana de carga o progreso donde se estaría creando el nuevo caso luego de hacer clip en finalizar.

Ilustración 57 ventana de progreso.

La imagen muestra el paso Seleccionar y Añadir Fuente de Datos en la herramienta de análisis forense. Este paso es crucial para **organizar** la evidencia digital dentro de la estructura de un caso.

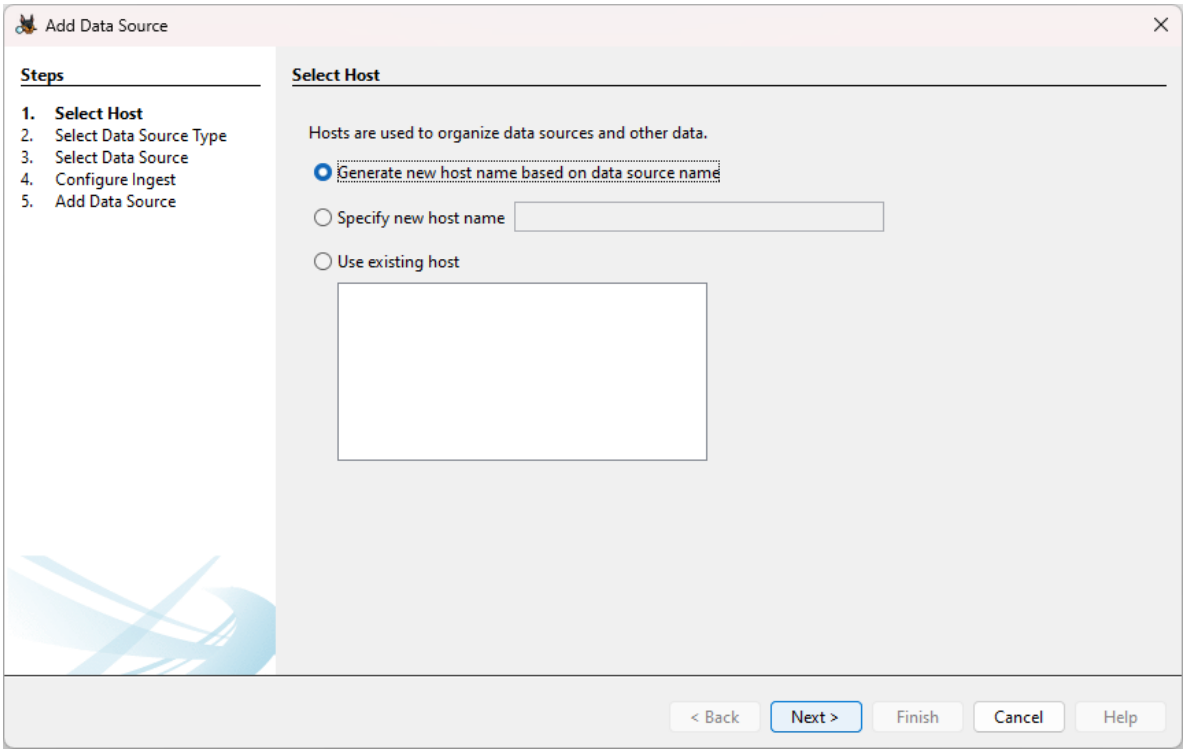


Ilustración 58 Seleccionar Host.

Seleccionar tipo de fuente de datos del proceso de agregar evidencia a autopsy para análisis forense. Este paso define el formato de la evidencia que se va a procesar.

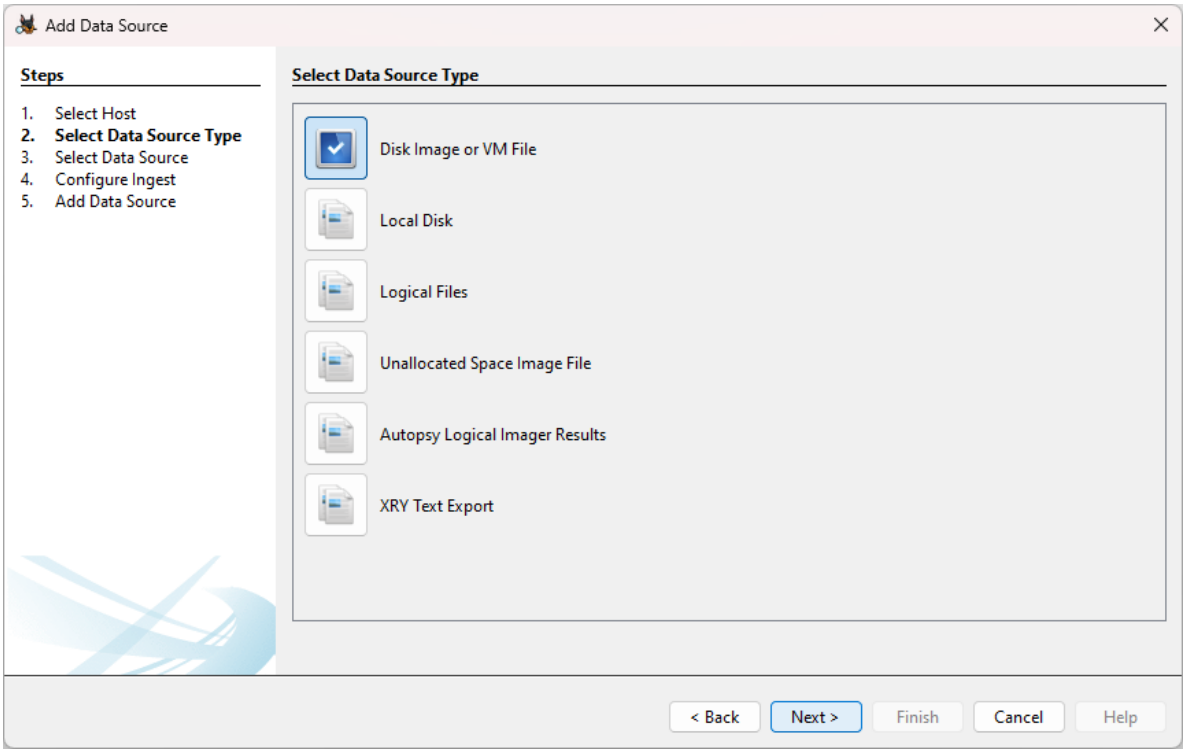


Ilustración 59 Seleccionar tipo de fuente de datos.

La imagen muestra la selección del archivo de imagen forense.

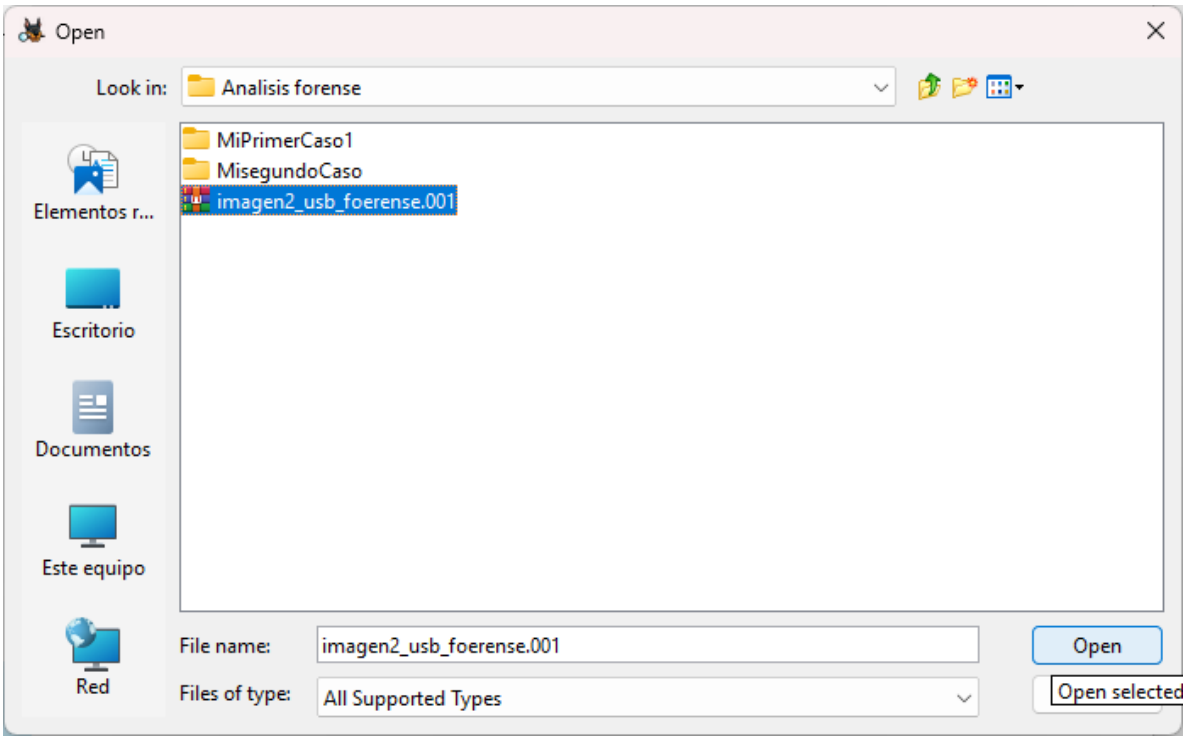


Ilustración 60 selección del archivo de imagen forense.

Agregar orígenes de datos, es la ventana que se muestra tras la carga de crear el nuevo caso autopsy. En este paso se puede importar la evidencia que conocemos como imagen de disco u archivos para su análisis.

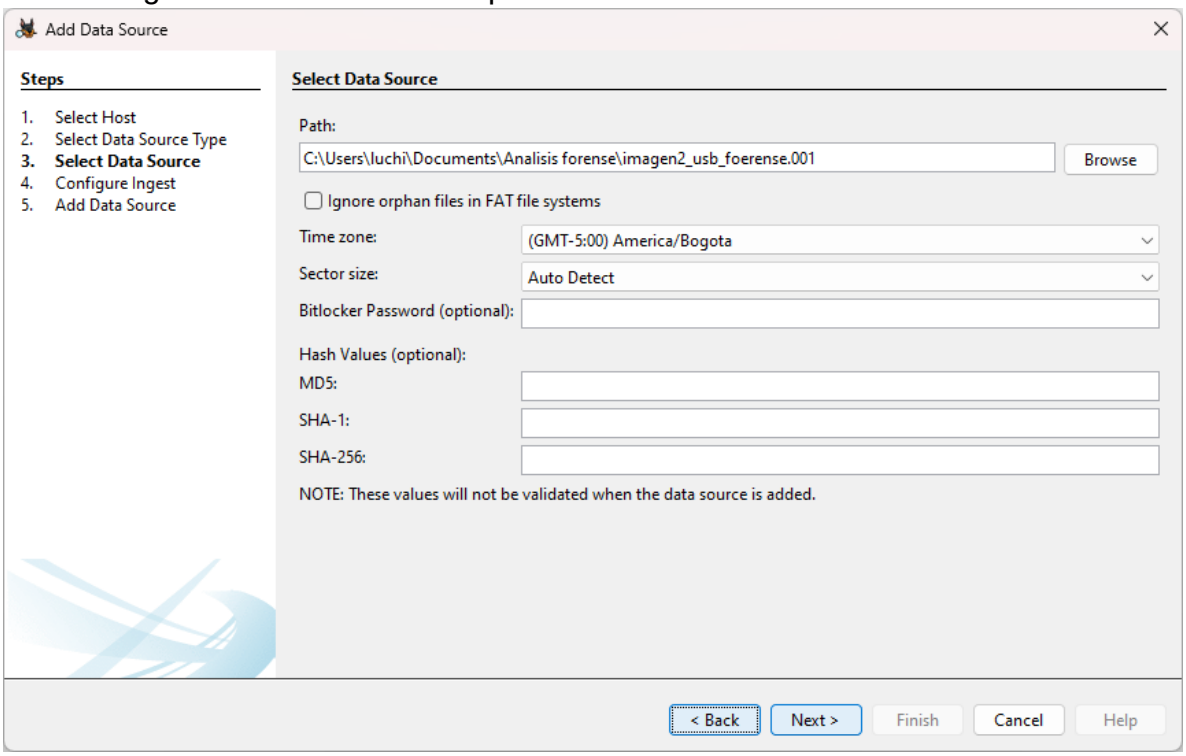


Ilustración 61 Seleccionar fuente de datos.

Configuración de la ingesta del asistente, aquí se decide que módulos de análisis se ejecutaran automáticamente sobre la imagen forense que se añadió.

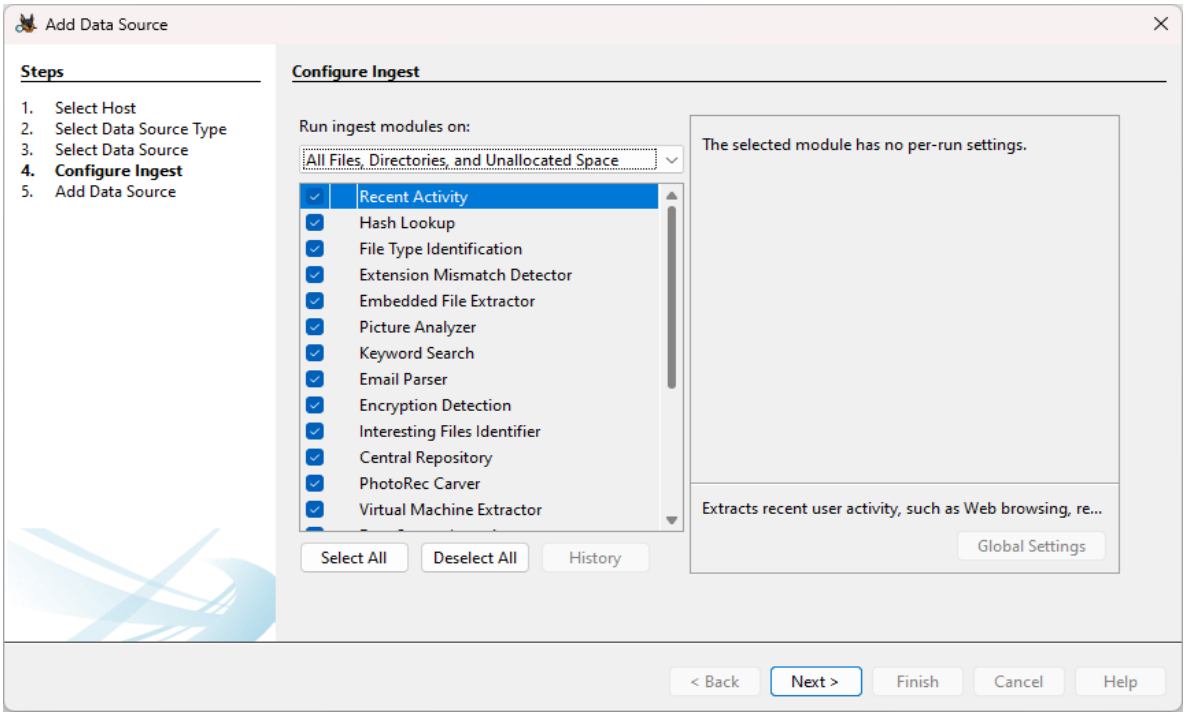


Ilustración 62 Configure Ingest.

Una vez se presione siguiente iniciara un proceso interno que recorre toda la imagen forense, cada módulo analiza diferentes tipo de evidencia como archivos, logos, espacios libres entre otros. Los resultados se ordenan en una base de datos SQL.

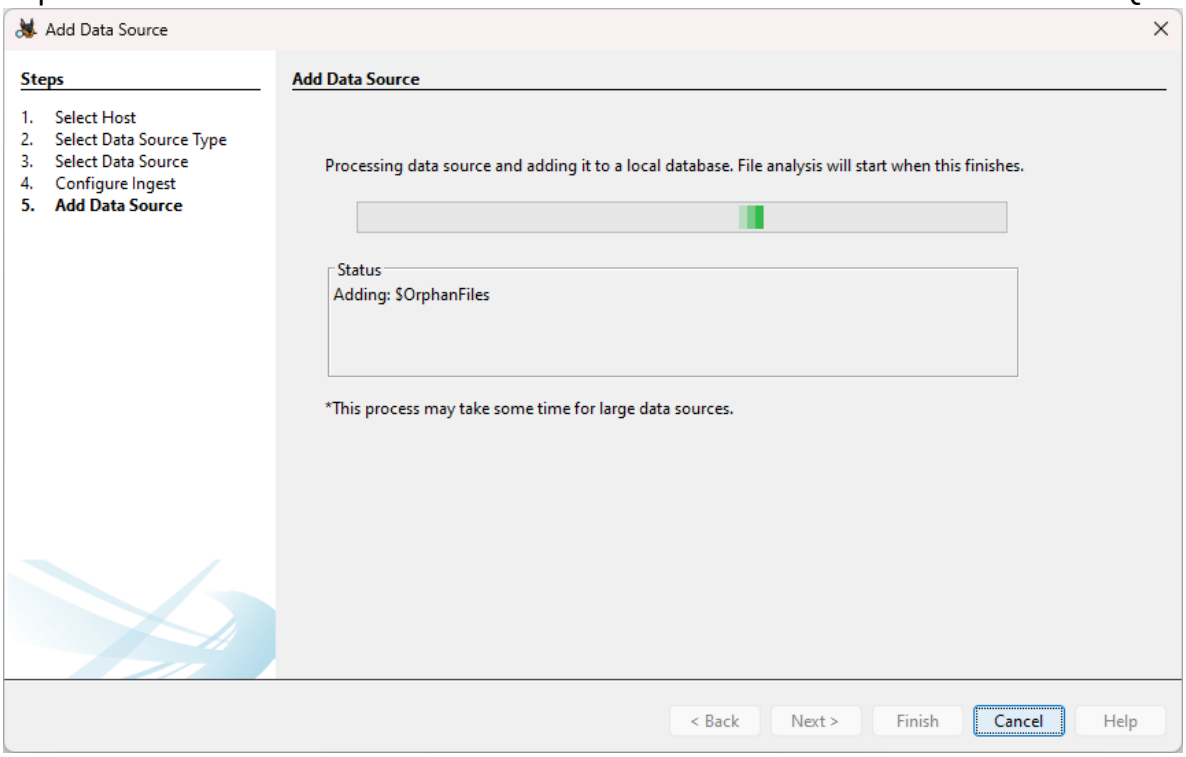


Ilustración 63 Agregar Fuente de Datos.

Interfaz principal Autopsy se muestra una vez el programa ha comenzado el proceso de análisis, en la parte inferior derecha de la pantalla podemos notar una barra de progreso donde podemos evidenciar lo que ha avanzado el proceso y en la vista del panel lateral izquierdo se muestran algunos campos como:

Metadata (4)
Analysis Results
EXIF Metadata (1)
User Content Suspected (1)

Al ver que estos campos contienen un numero x de contenido podemos estar más seguros de que el proceso como tal ha comenzado procesar los datos.

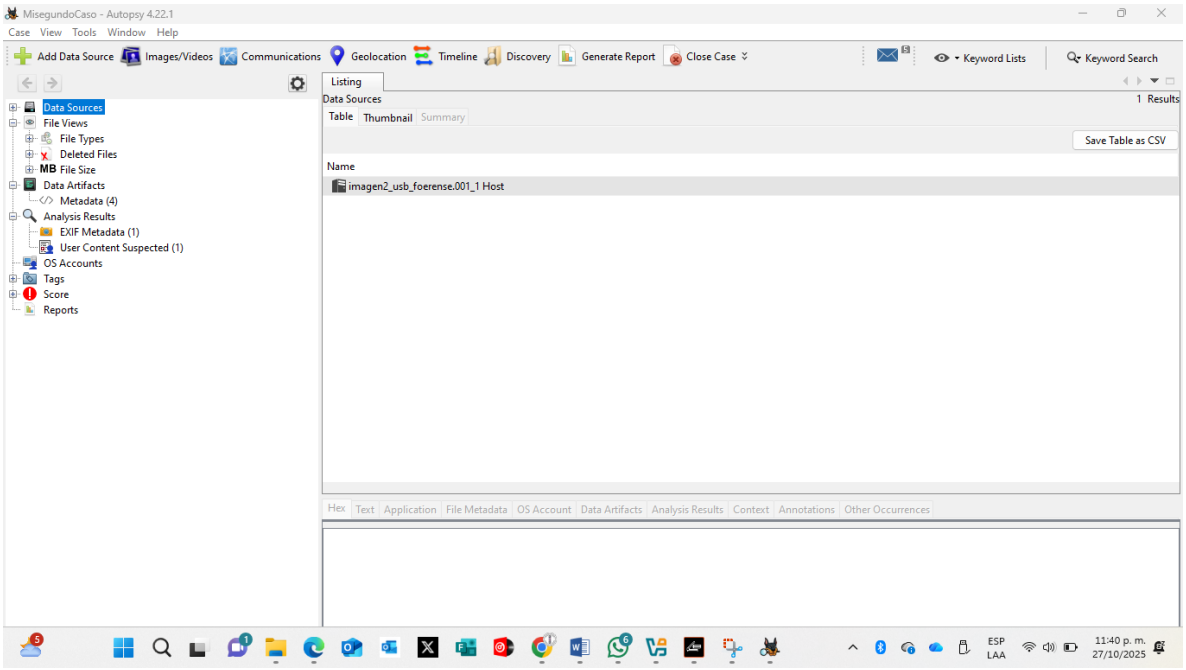


Ilustración 64 Interfaz principal Autopsy en progreso de análisis.

La siguiente imagen muestra la interfaz principal de la herramienta forense **Autopsy 4.22.1**, cargando y examinando los datos extraídos de la imagen forense previamente adquirida. Específicamente, está mostrando la vista de los archivos contenidos en la evidencia digital.

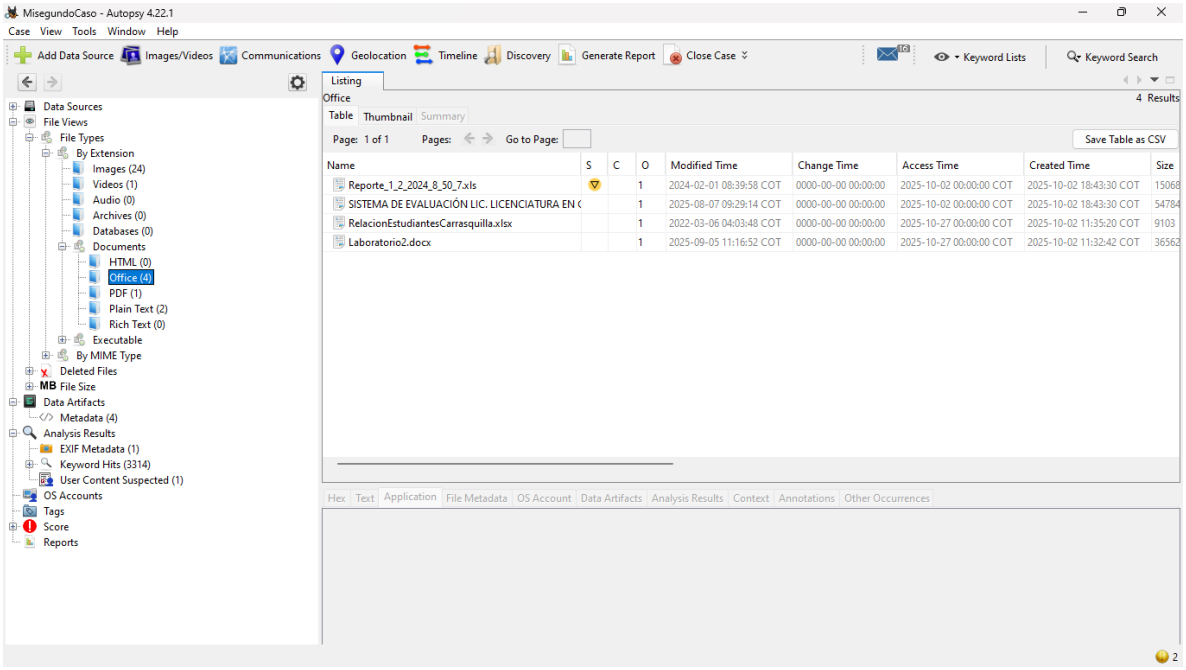


Ilustración 65 Análisis de la interfaz de autopsia

Recomendaciones

Realizar siempre una copia de respaldo de la evidencia original antes de iniciar cualquier proceso de análisis, evitando la manipulación directa del medio original.
Ejecutar herramientas forenses con privilegios de administrador solo cuando sea necesario, reduciendo el riesgo de alteraciones accidentales.
Verificar los valores hash (MD5 o SHA1) antes y después de la creación de la imagen para garantizar la integridad de la evidencia.
Nombrar los archivos y directorios de forma estandarizada, lo que facilita la trazabilidad y la organización de los casos.
Documentar cada paso realizado, incluyendo fechas, comandos, herramientas, versiones y observaciones de errores o anomalías.
Seleccionar correctamente el tipo de volumen o partición al importar imágenes forenses en Autopsy para evitar errores de montaje.

Conclusión general

El laboratorio permitió comprender de manera práctica las fases esenciales del análisis forense digital, aplicadas a una microSD.
Se logró realizar correctamente la adquisición, creación, conferencia
En el resultado final evidencia una adecuada aplicación de principios forenses como la integridad, autenticidad, trazabilidad y preservación de la evidencia digital.
El laboratorio permitió comprender de manera práctica las fases esenciales del análisis forense digital, desde la adquisición hasta la documentación final de la evidencia, Se logró generar una imagen forense exacta y verificable de una memoria microSD mediante dd, SHA1 entre la imagen y el dispositivo original.
Durante la fase de análisis con Autopsy, se evidenció la importancia de configurar correctamente el tipo de volumen para garantizar una interpretación adecuada del sistema de archivos. Este hallazgo permitió resolver los problemas iniciales y completar satisfactoriamente el proceso forense.
El trabajo demuestra la aplicación efectiva de principios fundamentales de la informática forense:

El ejercicio fortaleció las habilidades prácticas en el uso de herramientas forenses, análisis de evidencias digitales y documentación técnica, competencias esenciales para el desempeño profesional en seguridad informática y auditoría de redes.