INFORME #2 ANÁLISIS PRÁCTICO DE TÉCNICAS GENERACIÓN DE HASH FORENSE Y EXPLOTACIÓN DE VULNERABILIDADES EN ENTORNOS VIRTUALIZADOS CON KALI LINUX Y WINDOWS XP

EDWARD CAMILO CAICEDO BENITEZ

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIÓNES E INFORMÁTICA

SEGURIDAD Y AUDITORIAS EN REDES

DOCENTE

RAFAEL SANDOVAL MORALES

QUIBDÓ-CHOCÓ-COLOMBIA

2025

Tabla de contenido

INTRODUCCIÓN

El presente informe tiene como propósito analizar y aplicar diversas técnicas de generación de hash forense y explotación de vulnerabilidades en entornos virtualizados, utilizando herramientas como **Kali Linux**, **Autopsy** y **FTK Imager**. Estas prácticas permiten comprender los procedimientos empleados en la **ciencia forense digital**, especialmente en la preservación, análisis y validación de evidencias electrónicas.

A través del uso de imágenes forenses (.dd) y el cálculo de valores hash (SHA1 y MD5), se busca garantizar la integridad de la información manipulada, evidenciando la importancia de los métodos de duplicación bit a bit, la cadena de custodia y la verificación de autenticidad. Este trabajo representa un ejercicio práctico de auditoría forense aplicada al contexto académico, fortaleciendo competencias técnicas en el ámbito de la **seguridad informática y redes**.

OBJETIVOS

Objetivo general

Realizar un análisis práctico de las técnicas de generación de hash forense y verificación de integridad de evidencias digitales en entornos virtualizados con Kali Linux y Windows XP, empleando herramientas especializadas para la detección y preservación de información.

Objetivos específicos

Implementar procesos de duplicación forense y verificación de integridad mediante la generación de hashes SHA1 y MD5 en dispositivos de almacenamiento.

Utilizar las herramientas Autopsy y FTK Imager para la creación, análisis y comparación de imágenes forenses en diferentes entornos operativos.

Evaluar la importancia del hash forense como elemento de autenticación y trazabilidad dentro del análisis digital de evidencias.

PLANTEAMIENTO DEL PROBLEMA

En el ámbito de la seguridad informática, uno de los mayores retos consiste en garantizar la **integridad y autenticidad de la información** durante el proceso de análisis digital. Las evidencias electrónicas pueden ser fácilmente alteradas o corrompidas si no se aplican técnicas adecuadas de preservación forense.

En entornos virtualizados, donde múltiples sistemas operativos interactúan simultáneamente, resulta fundamental aplicar métodos confiables de adquisición de datos, como la duplicación bit a bit y la verificación mediante valores hash. Sin estos procedimientos, la validez de una investigación forense podría verse comprometida.

Este trabajo aborda la problemática desde la práctica, analizando las etapas críticas del proceso forense digital para garantizar que las copias de evidencia sean auténticas, verificables y válidas ante auditorías técnicas o legales.

METODOLOGÍA

La metodología empleada se basa en un **enfoque práctico y experimental**, desarrollado en entornos virtualizados controlados mediante **Oracle VirtualBox**.

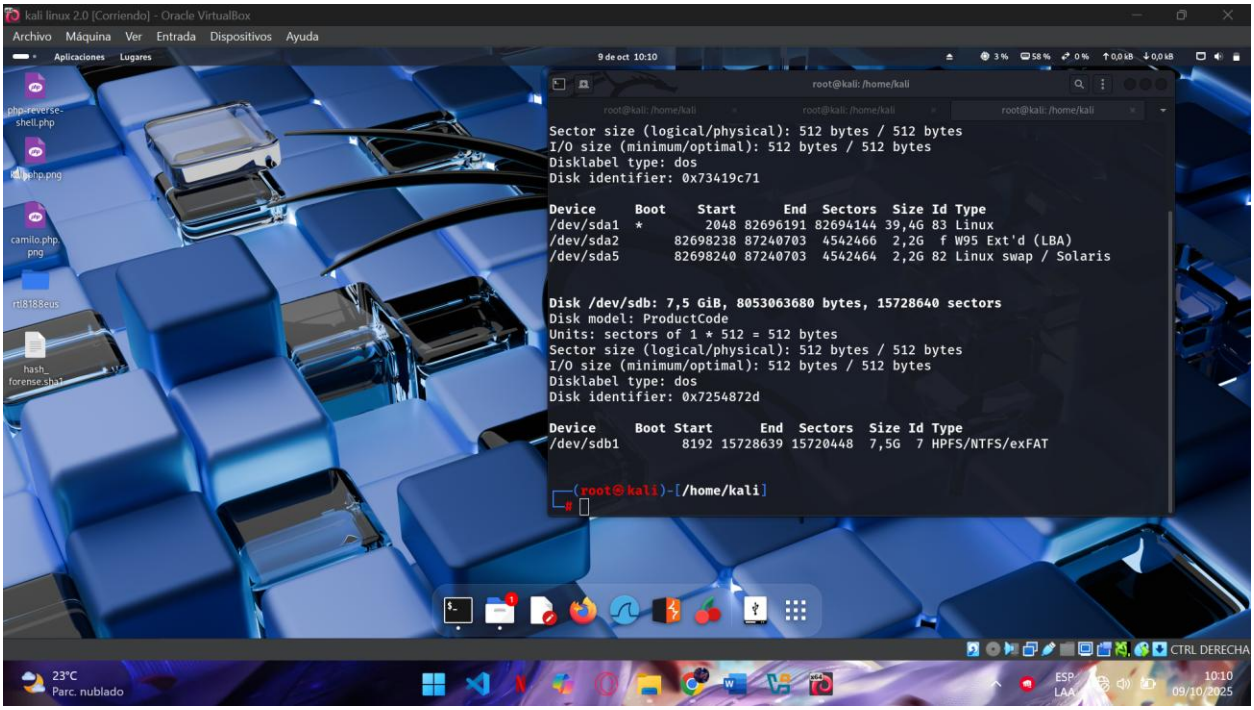
1. **Preparación del entorno:** Instalación de sistemas operativos Kali Linux y Windows XP para realizar las pruebas.
2. **Obtención y duplicación de evidencia:** Uso del comando dd para crear imágenes forenses (.dd) de dispositivos USB y generar valores hash iniciales.
3. **Verificación de integridad:** Comparación de los valores hash SHA1 y MD5 entre el dispositivo original y la imagen creada para comprobar su autenticidad.
4. **Análisis forense:** Uso de las herramientas **Autopsy** y **FTK Imager** para examinar el contenido de las imágenes, identificar archivos eliminados y generar reportes de evidencia.
5. **Comparación de resultados:** Validación cruzada de los valores hash obtenidos en ambos entornos (Linux y Windows) para confirmar la correspondencia exacta y la integridad de los datos.

PRÁCTICA EN CLASES

CAPITULO 1 AUTOSI KALI AUDITORIA FORENSE

Paso 1

En esta imagen se muestra la ejecución del comando fdisk -l dentro del entorno Kali Linux, el cual permite listar los dispositivos de almacenamiento conectados al sistema. Se observan las particiones del disco principal y una memoria USB de 7,5 GB con formato **HPFS/NTFS/exFAT**, que será objeto de análisis forense.



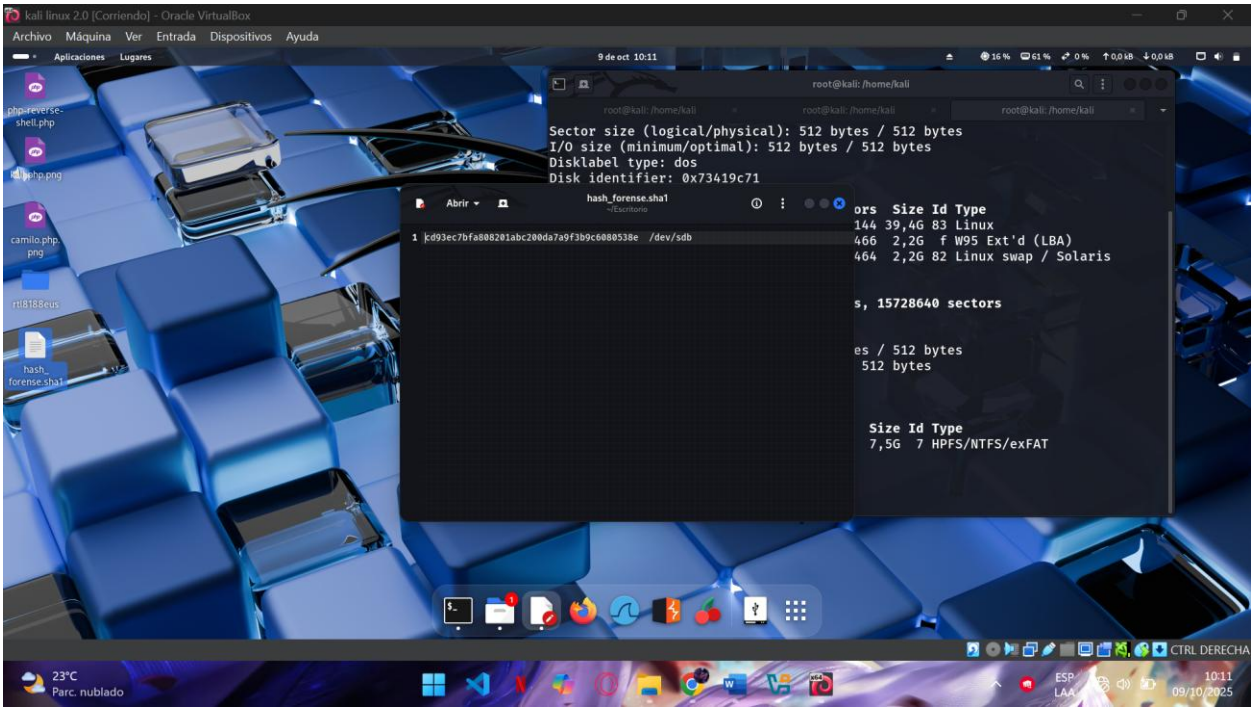
1. Identificación de dispositivos conectados

La figura evidencia la creación de un hash de tipo **SHA1** mediante el comando sha1sum /dev/sdb > /home/kali/Escritorio/hash_forense.sha1. Este procedimiento genera una huella digital única del dispositivo antes de realizar cualquier manipulación, garantizando la **integridad de la evidencia digital**.

```
┌──(root㉿kali)-[/home/kali]
└─# sha1sum /dev/sdb > /home/kali/Escritorio/hash_forense.sha1
```

2.Generación de hash inicial del dispositivo USB

En esta captura se aprecia el archivo **hash_forense.sha1** generado previamente, que contiene el valor hash correspondiente al dispositivo USB. Este valor servirá como referencia para validar la autenticidad de los datos en etapas posteriores del análisis.



3. Verificación del hash forense generado

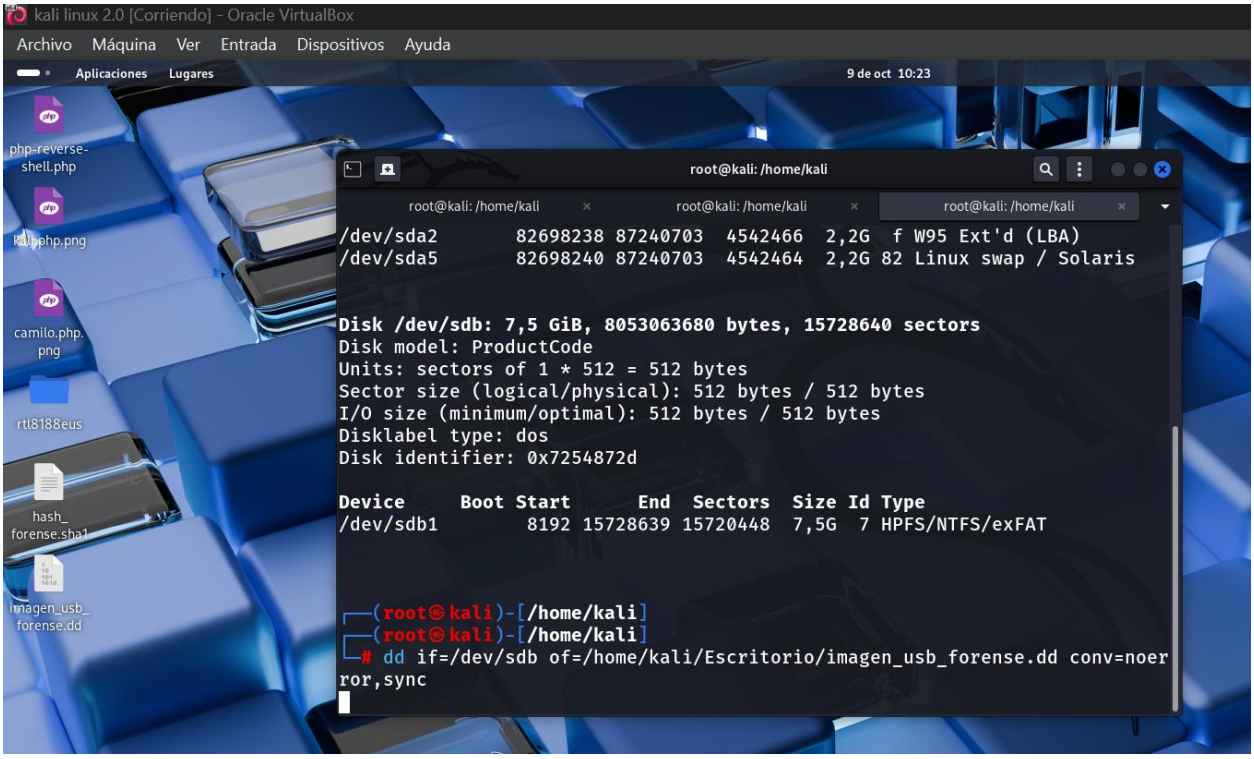
Paso 2

La imagen muestra la preparación del comando dd if=/dev/sdb of=/home/kali/Escritorio/imagen_usb_forense.dd conv=noerror,sync. Con este proceso se realiza una **copia bit a bit** del dispositivo USB, garantizando una réplica exacta sin alterar el contenido original.

```
┌──(root㉿kali)-[/home/kali]
└─# dd if=/dev/sdb of=/home/kali/Escritorio/imagen_usb_forense.dd conv=noerror,sync
```

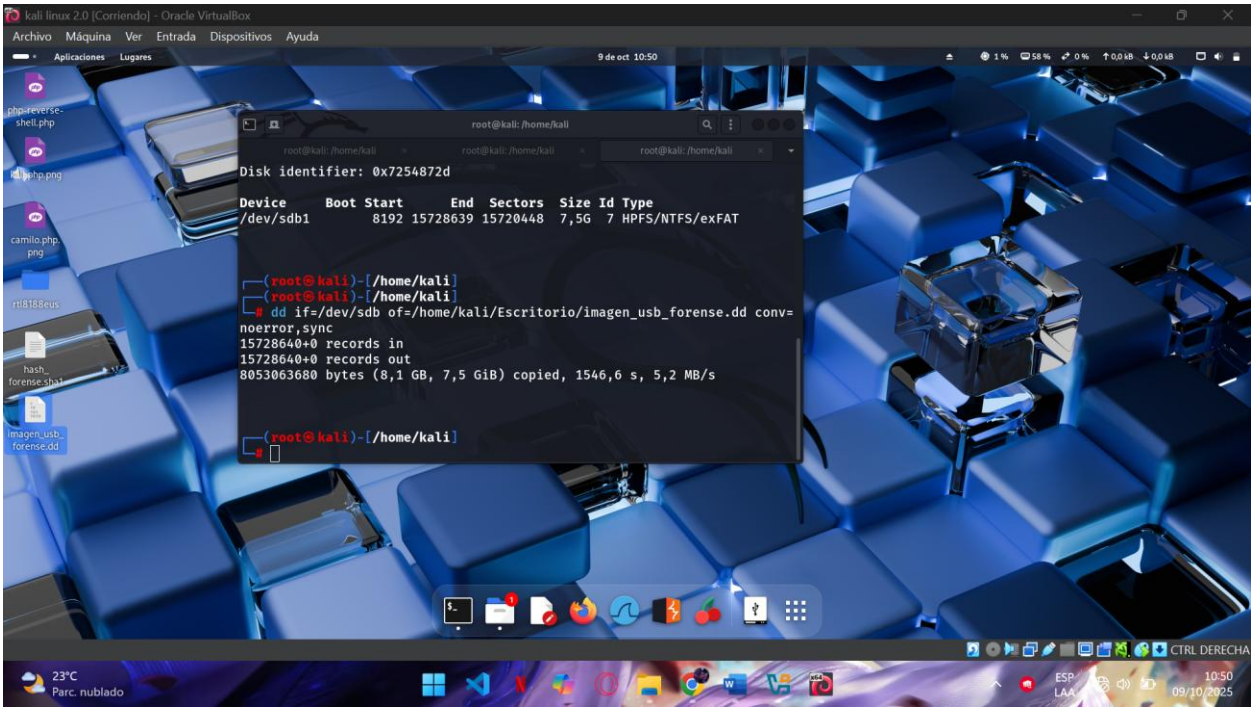
4.Creación de la imagen forense del dispositivo

Aquí se observa el comando dd en ejecución, copiando la información del dispositivo USB hacia un archivo de imagen con extensión **.dd**. Este paso es fundamental para trabajar sobre una copia de la evidencia y preservar la original intacta.



5. Proceso de creación de imagen forense en ejecución

En esta figura se muestra la finalización satisfactoria del proceso de duplicación, con un total de **7,5 GiB copiados** y una velocidad media de transferencia de **5,2 MB/s**. El archivo resultante, **imagen_usb_forense.dd**, queda listo para el análisis.



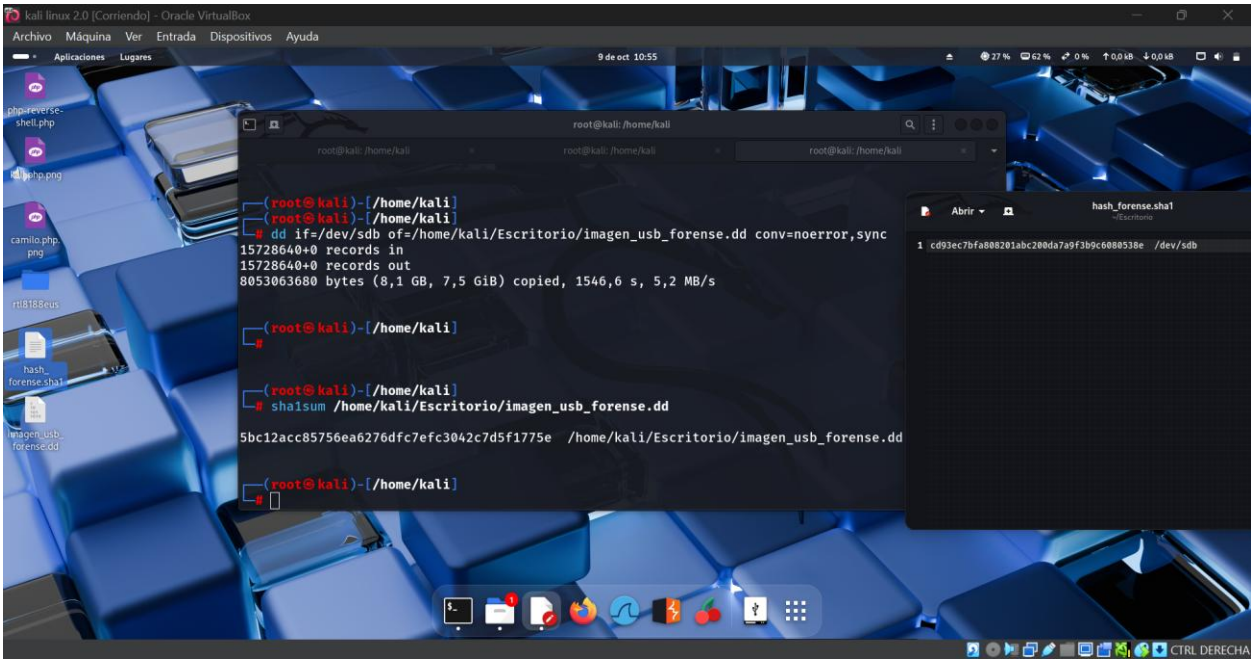
6. Finalización del proceso de duplicación forense

Se presenta la ejecución del comando sha1sum /home/kali/Escritorio/imagen_usb_forense.dd, utilizado para generar el hash SHA1 de la imagen creada. Este valor se compara con el hash inicial del dispositivo para comprobar si la copia mantiene su integridad.

7. Cálculo del hash de la imagen forense

La figura final muestra la comparación entre los hashes del dispositivo original y la imagen forense. El resultado indica **diferencia en los valores hash**, lo que sugiere que los archivos del dispositivo pudieron ser **manipulados durante el transcurso de la semana**, alterando su integridad digital.

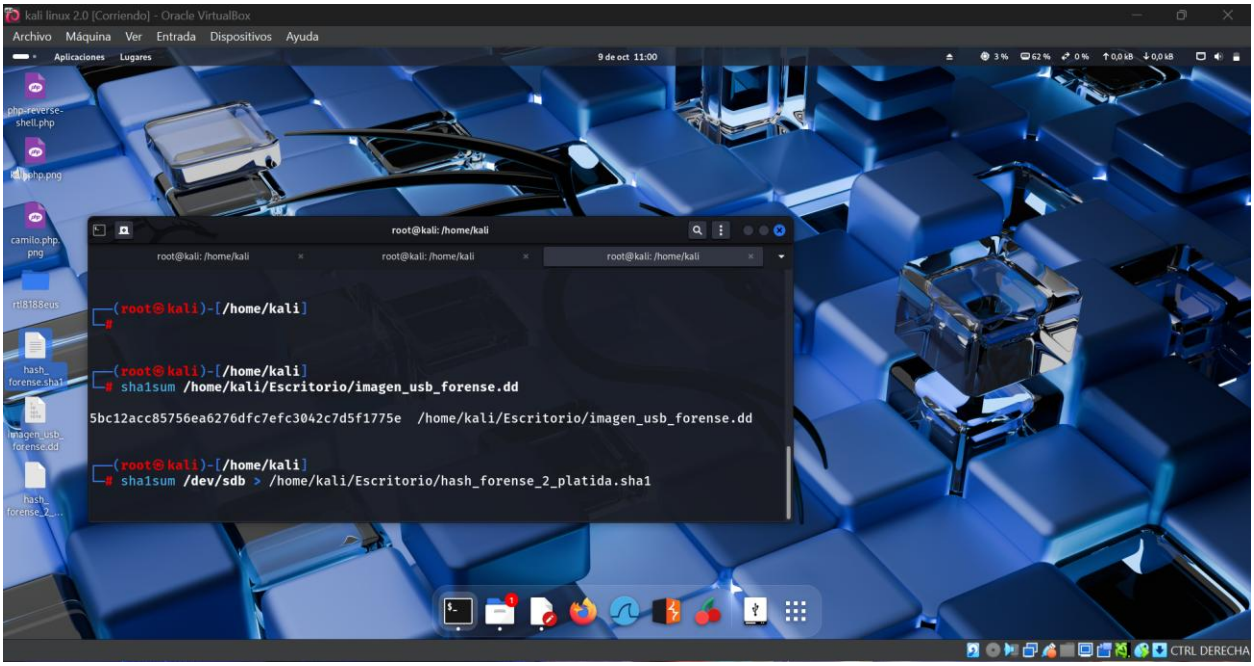
No dio el mismo cifrado debió a que manipularon archivos durante en el transcurso de la semana



8. Comparación de hashes y verificación de integridad

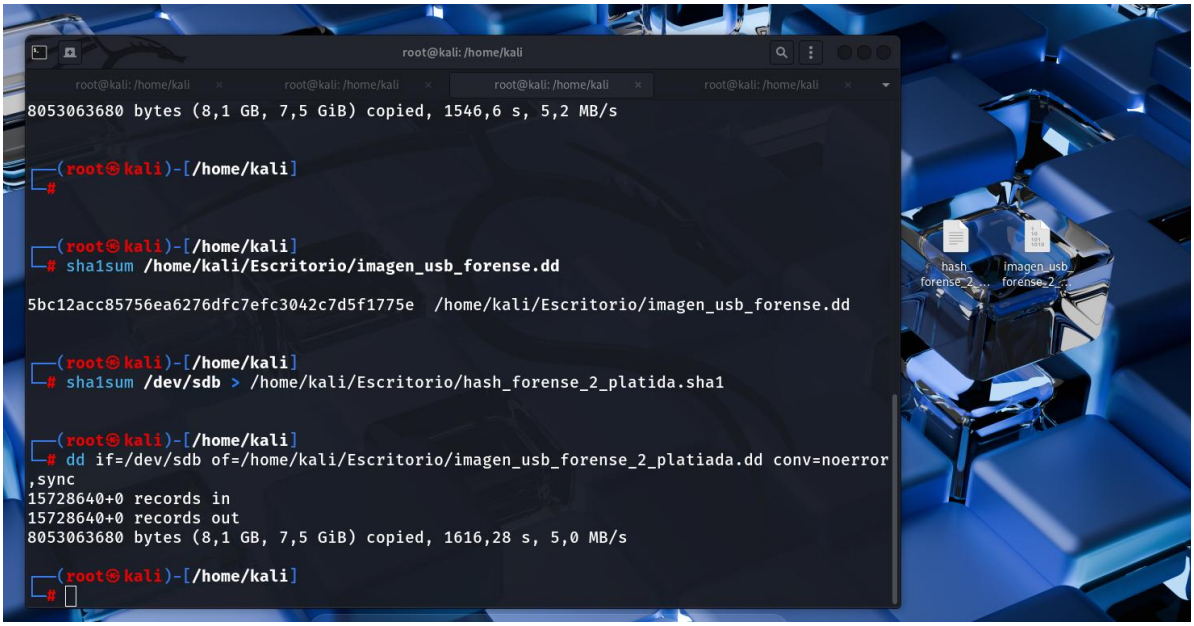
Volvemos hacer el proceso

En esta imagen se observa el reinicio del procedimiento forense para la obtención y verificación del hash SHA1 tanto de la imagen generada como del dispositivo USB original. El objetivo es **repetir el proceso de validación** y descartar posibles alteraciones producidas en el primer intento.



9. Repetición del proceso de verificación y duplicación

La figura muestra la ejecución del comando dd if=/dev/sdb of=/home/kali/Escritorio/imagen_usb_forense_2_platiada.dd conv=noerror,sync, con el cual se realiza una **segunda copia bit a bit** del dispositivo USB. Este paso permite generar una nueva imagen forense bajo condiciones controladas y con parámetros de consistencia garantizados.

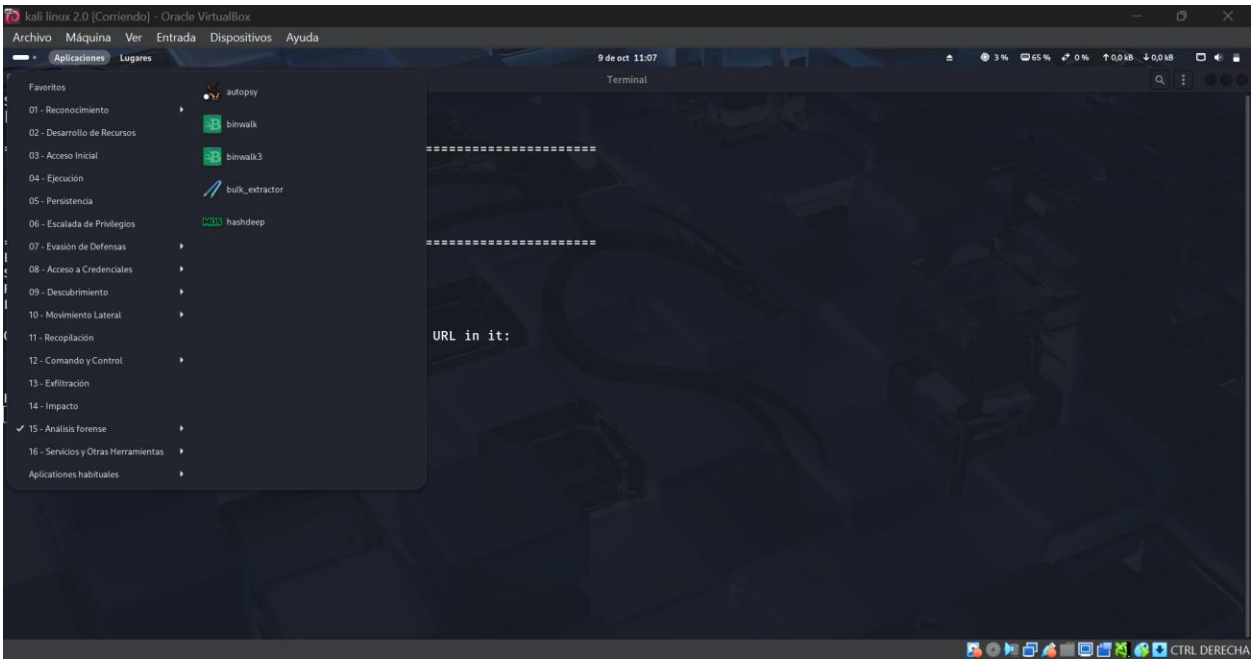


10.Ejecución del comando de duplicación forense (segunda copia)

En esta última imagen se aprecia la comparación entre el hash del dispositivo /dev/sdb y el hash de la nueva imagen forense imagen_usb_forense_2_platiada.dd. Ambos valores coinciden, lo que **confirma la integridad de la copia forense** y demuestra que la evidencia fue correctamente duplicada sin alteraciones

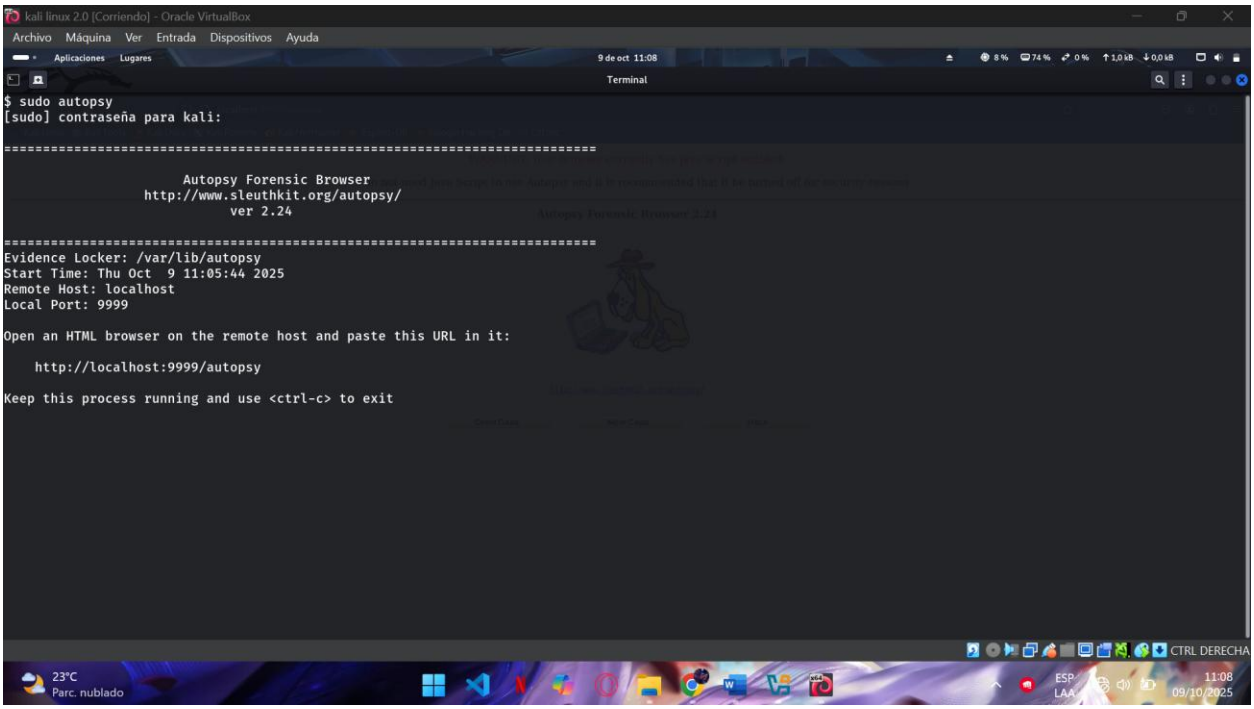
11. Verificación de integridad entre imagen forense y dispositivo original

Paso 3: se observa la interfaz principal de **Kali Linux 2.0** dentro de **Oracle VirtualBox**, mostrando la ejecución del comando autopsy desde el menú de aplicaciones forenses. Este entorno es empleado para realizar análisis digitales bajo condiciones controladas, garantizando la integridad del entorno de trabajo.



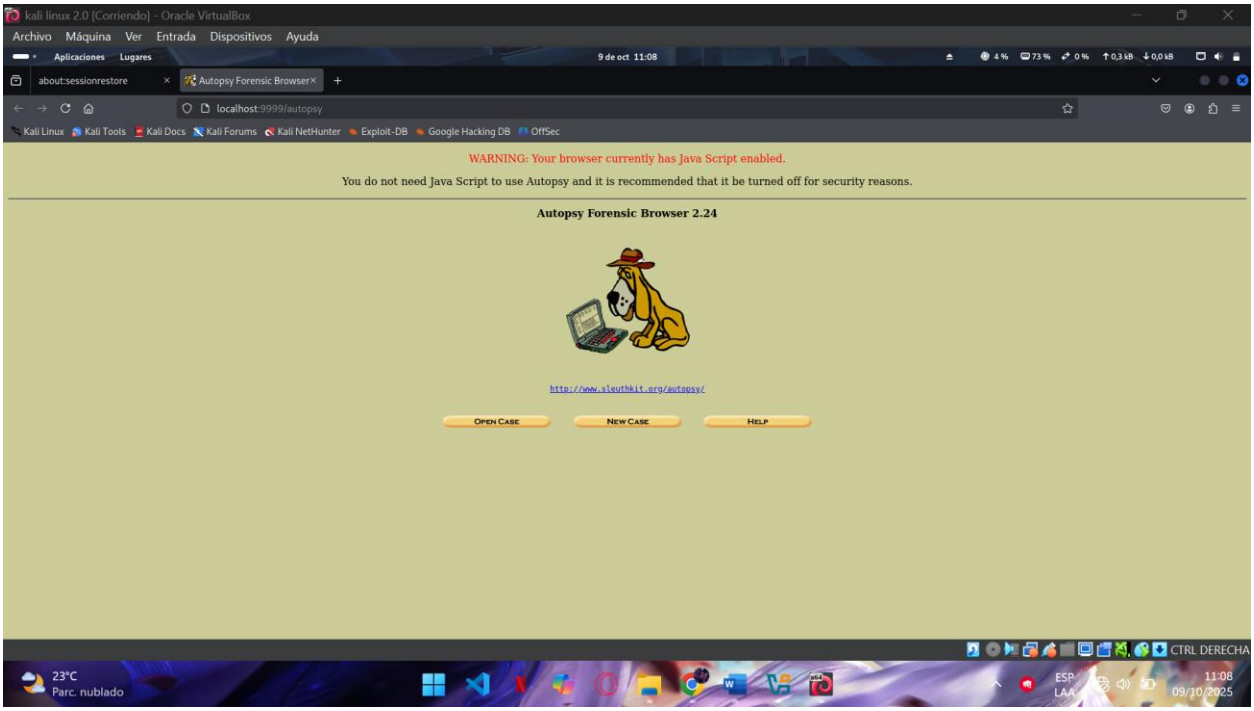
12. Ejecución de Autopsy en Kali Linux

la ejecución del comando sudo autopsy, con el cual se inicia el **Autopsy Forensic Browser versión 2.24**. El sistema indica el directorio de almacenamiento de evidencia, el puerto local de conexión (9999) y la dirección de acceso al entorno gráfico, necesario para la gestión de casos forenses.



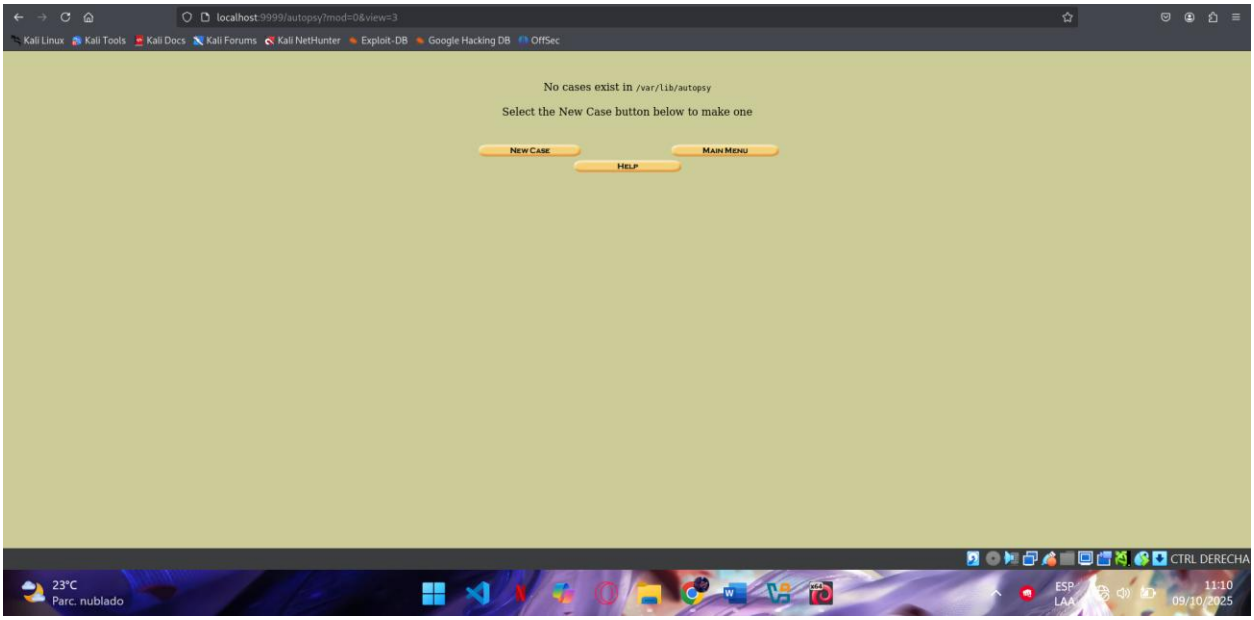
13. Inicialización del servidor Autopsy Forensic Browser

se aprecia la interfaz web del **Autopsy Forensic Browser**, accedida mediante localhost:9999/autopsy. Desde este entorno, el usuario puede **abrir un caso existente o crear uno nuevo**, lo que constituye el punto de partida para la gestión de investigaciones digitales.



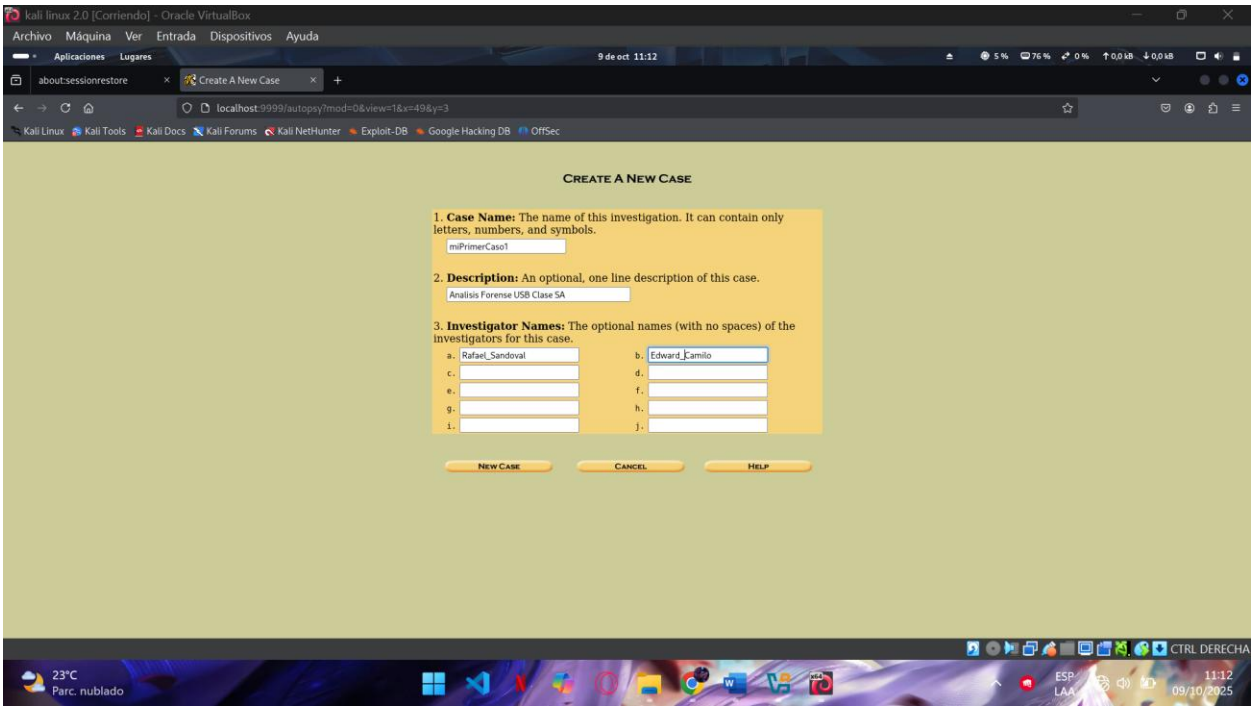
14. Interfaz principal del Autopsy Forensic Browser

la interfaz de Autopsy cuando no existen casos activos registrados en el sistema. Se presenta la opción de crear un nuevo caso mediante el botón **"New Case"**, lo que permite iniciar una nueva sesión de análisis pericial sobre evidencias digitales.



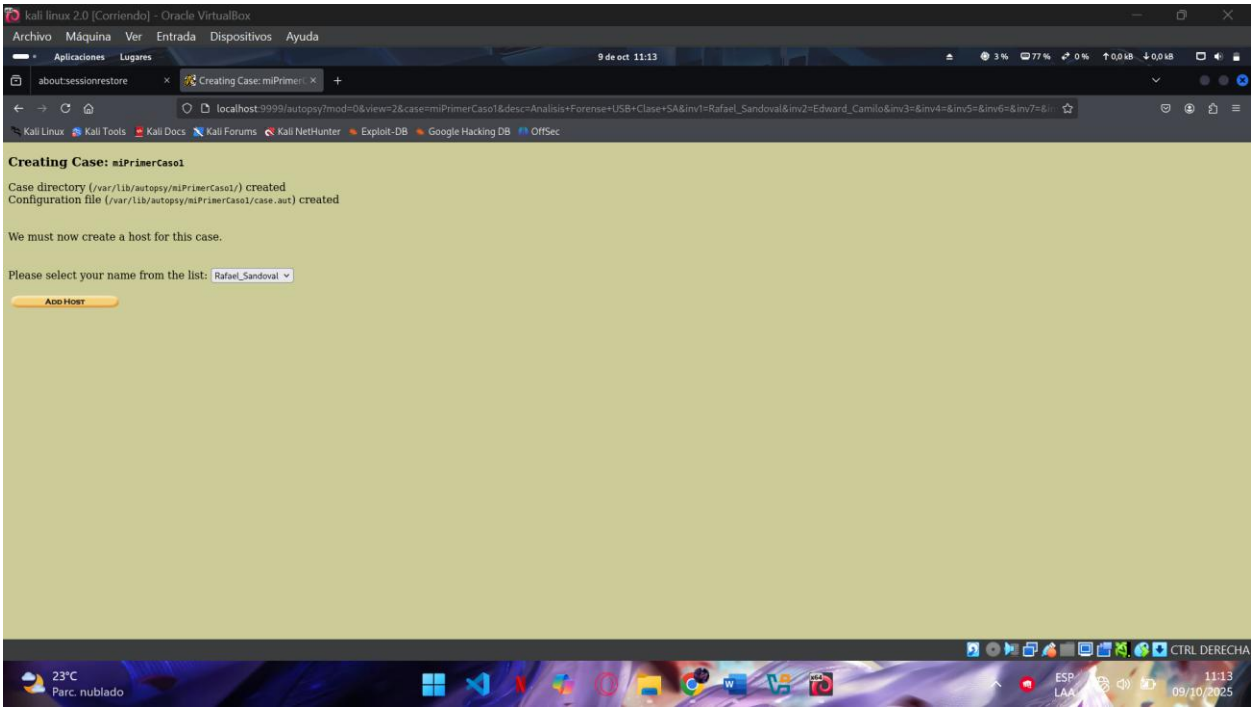
15. Interfaz sin casos activos

el formulario de creación de un nuevo caso dentro de Autopsy. Se definen los campos **“Case Name”**, **“Description”** y **“Investigator Names”**, que permiten asignar nombre, descripción y responsables de la investigación digital. Este registro inicial es fundamental para mantener la trazabilidad del proceso forense.



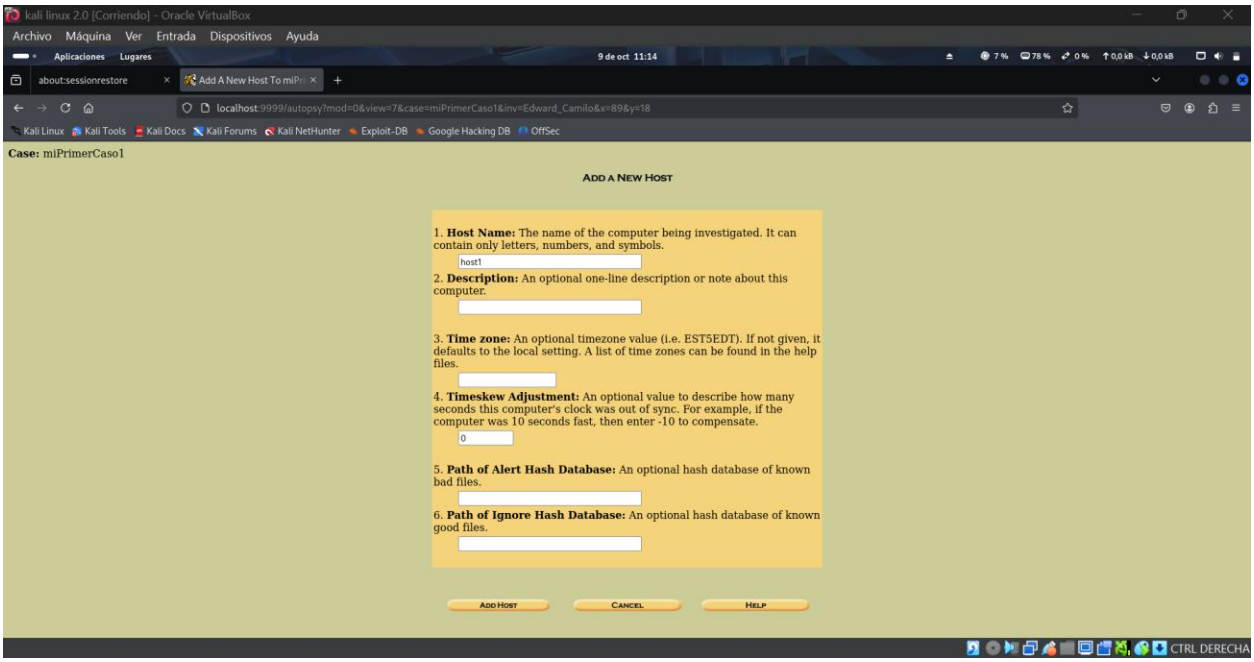
16. Creación de un nuevo caso

la confirmación del sistema tras la creación del caso denominado *miPrimerCaso1*. En este punto, el sistema solicita la selección de un **investigador principal** y permite proceder con la adición de un nuevo **host** asociado al caso.



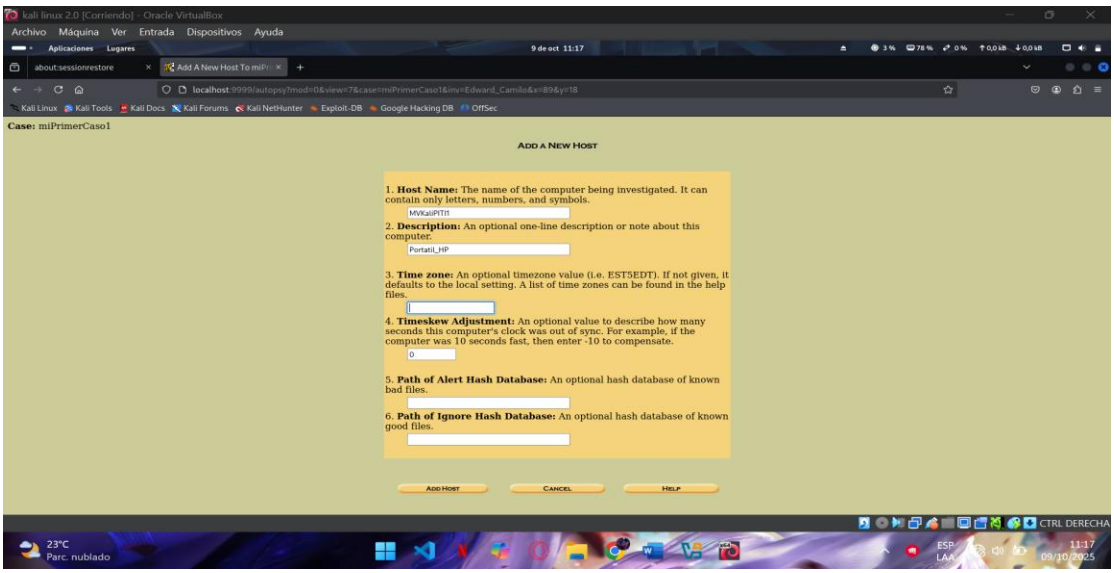
17. Confirmación de la creación del caso

se despliega el formulario **“Add a New Host”**, donde se deben ingresar los parámetros identificativos del sistema analizado, tales como el nombre del equipo (*Host Name*), descripción, zona horaria y ajustes temporales. Estos datos facilitan la correcta asociación entre la evidencia digital y el entorno pericial.



18. Registro de un nuevo host en Autopsy

se completan los campos del formulario con la información correspondiente al equipo bajo análisis. En este ejemplo, se asigna el nombre **“MiXPvMTI”** y la descripción **“Portatil_HP”**. Este registro asegura la correcta documentación y vinculación del dispositivo analizado dentro del caso forense.

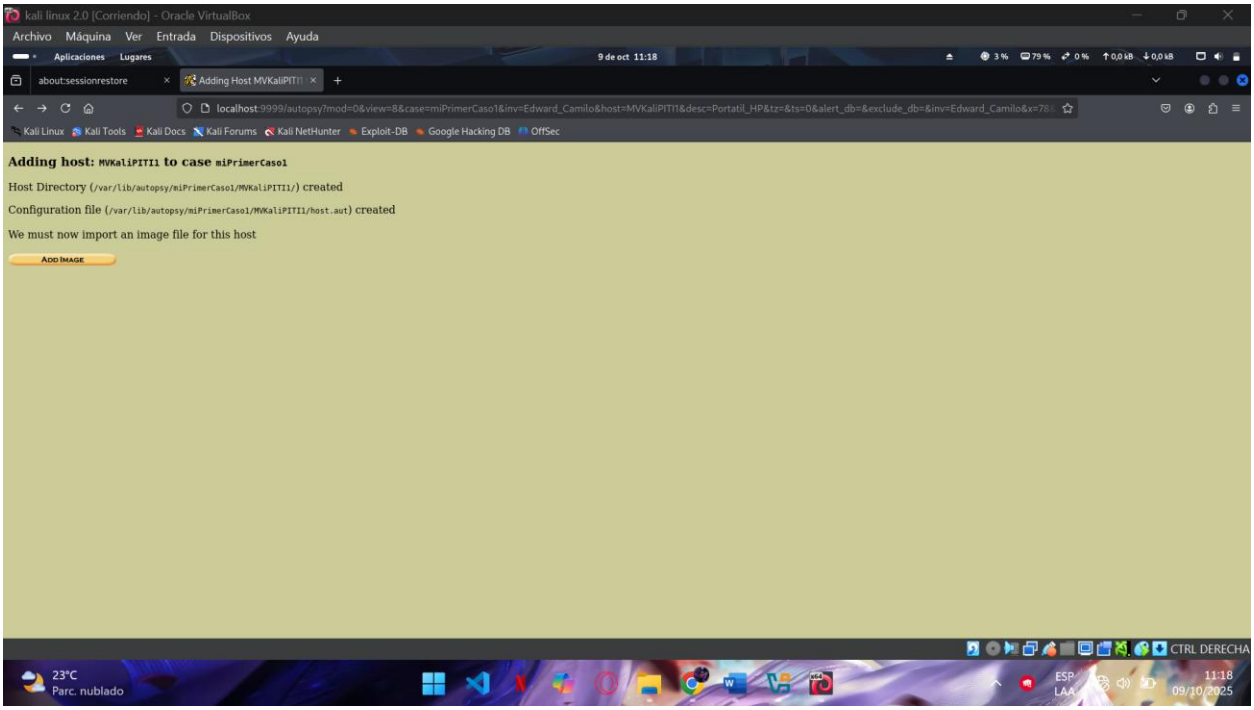


19. Configuración del host analizado

la creación de un nuevo host denominado **“MVKaliPIT11”** dentro del caso **“miPrimerCaso1”** en la herramienta Autopsy.

El sistema confirma la generación automática del directorio correspondiente en la ruta /var/lib/autopsy/miPrimerCaso1/MVKaliPIT11/, donde se almacenarán los archivos de configuración y evidencias asociadas al host.

Este proceso constituye el paso inicial para la organización de la evidencia digital dentro del entorno de análisis.

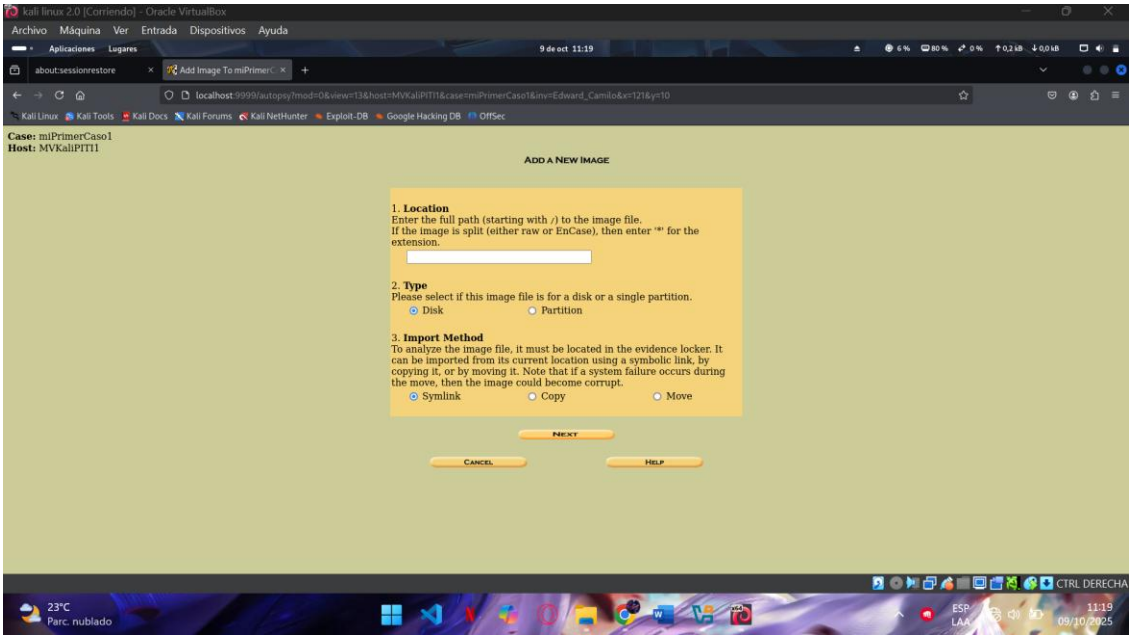


20. Creación del host en Autopsy

Al seleccionar la opción **“Add Image File”**, utilizada para incorporar una nueva evidencia digital al caso activo.

En esta ventana se especifican los parámetros de importación, tales como la ruta del archivo, el tipo de dispositivo (disco o partición) y el método de carga (Symlink, Copy o Move). Este procedimiento permite establecer la fuente de análisis a partir de una copia forense previamente obtenida.

Add image file

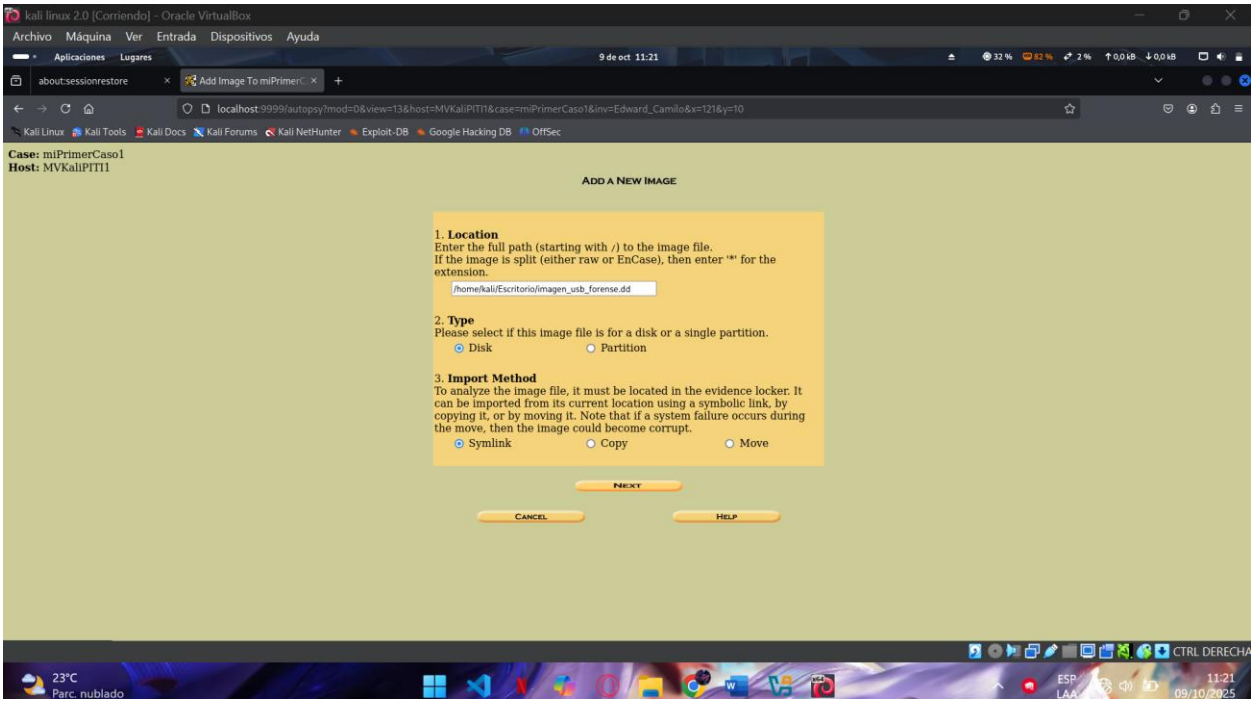


21. Adición de imagen forense al caso

se introduce la ruta absoluta del archivo **“imagen_usb_forense.dd”**, ubicado en el escritorio del usuario Kali Linux.

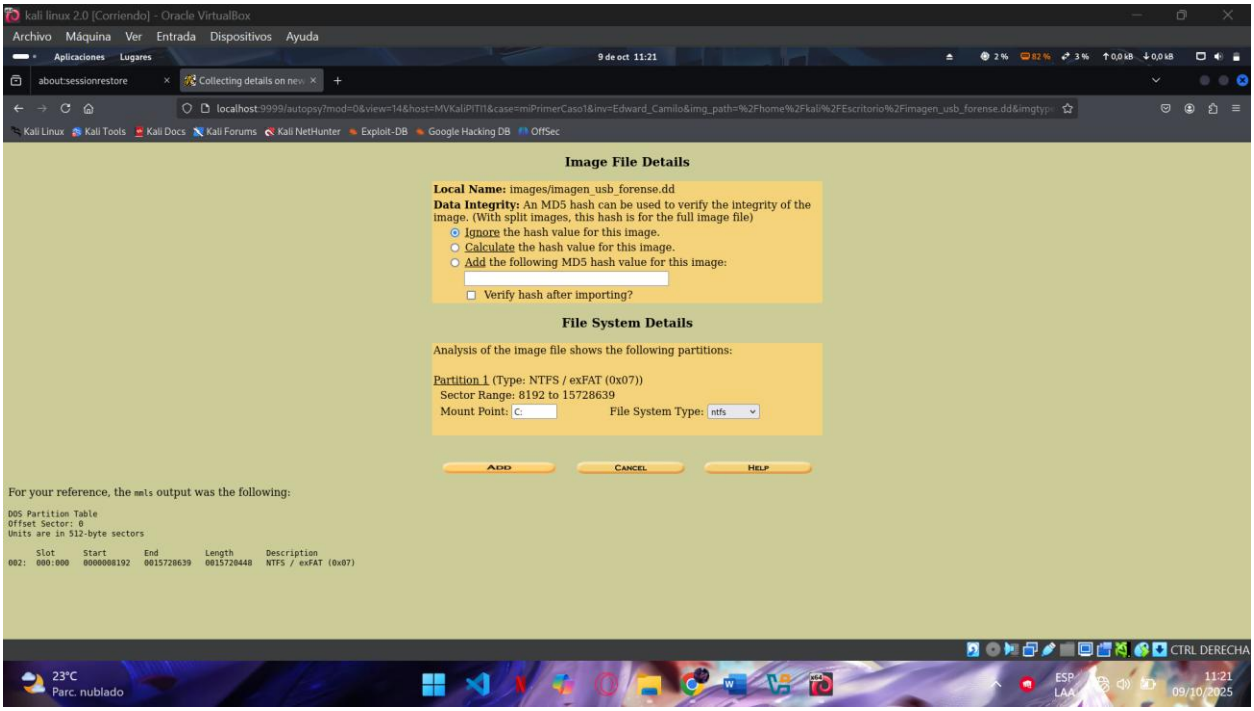
El tipo de evidencia seleccionada corresponde a un **disco completo (Disk)** y el método de importación elegido es **Symlink**, lo que garantiza que el archivo original permanezca inalterado durante el análisis.

Este paso asegura la correcta vinculación de la imagen forense con el entorno de trabajo.



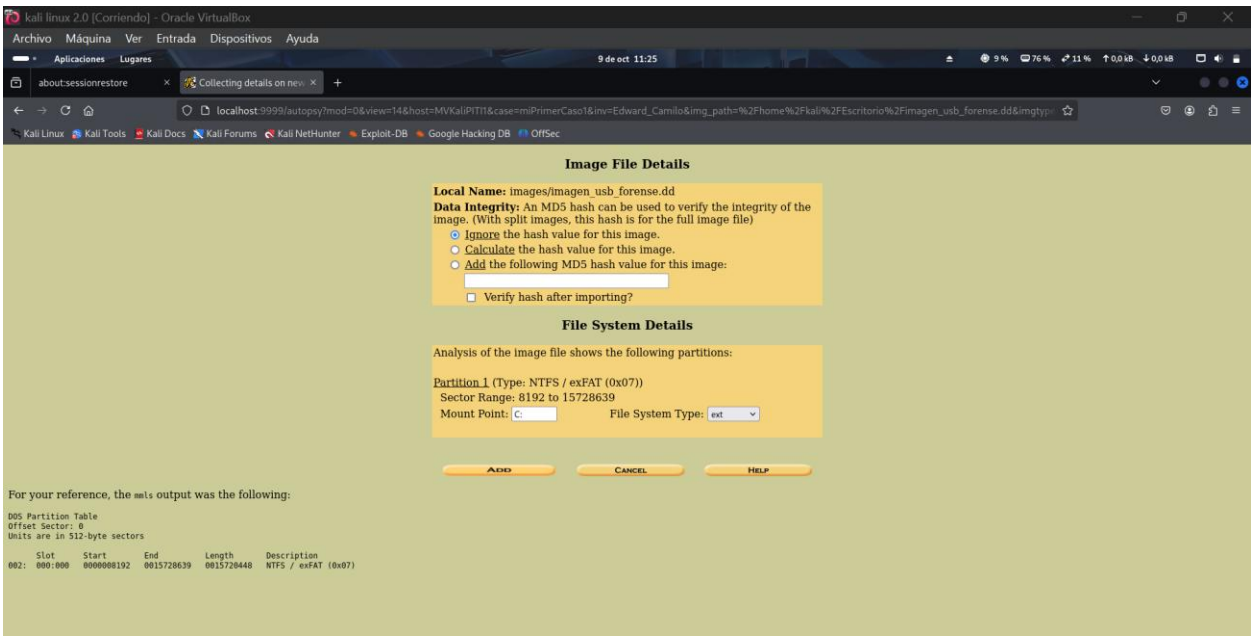
22.efinición de parámetros de la imagen forense

el proceso de análisis automático realizado por Autopsy, que identifica una **partición de tipo NTFS/exFAT (0x07)** dentro de la imagen forense. Se muestra información detallada sobre el volumen, incluyendo el rango de sectores **8192 a 15728639** y el punto de montaje lógico **C:**. Esta etapa confirma la estructura del sistema de archivos presente en la evidencia y permite preparar la partición para su exploración.



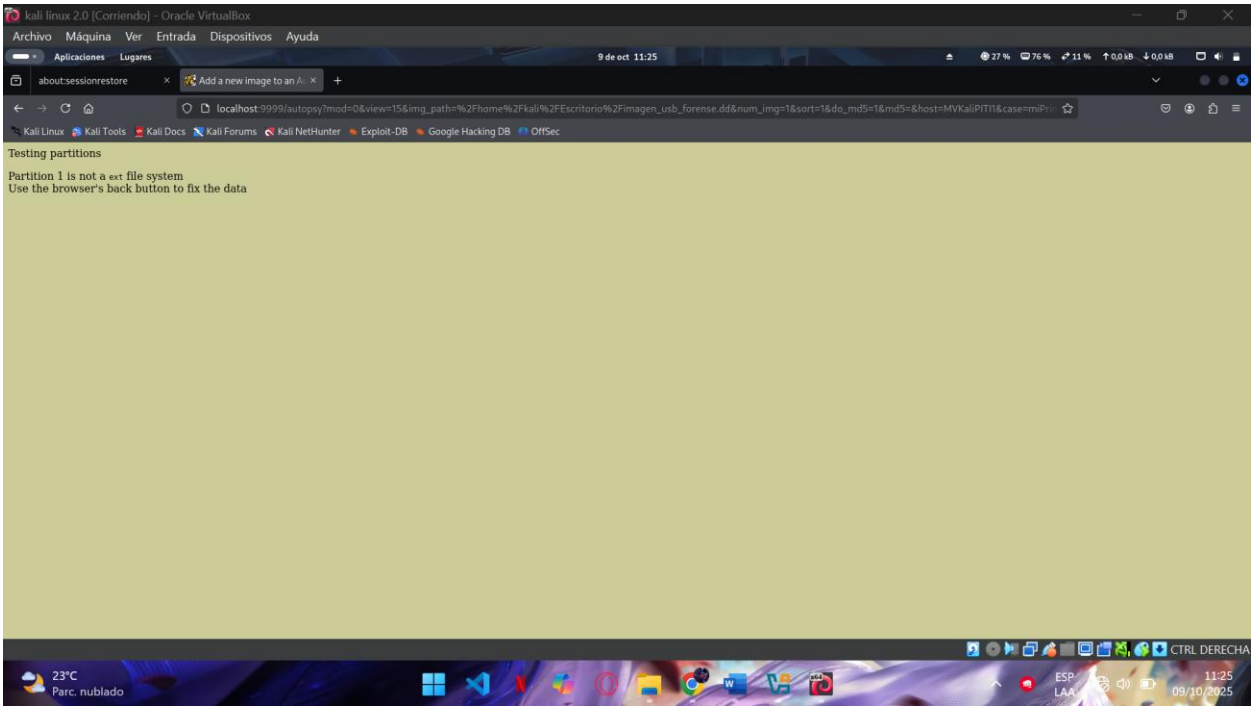
23. Detección de partición NTFS en la imagen

el sistema genera un mensaje de error indicando que la partición no corresponde a un sistema **EXT**



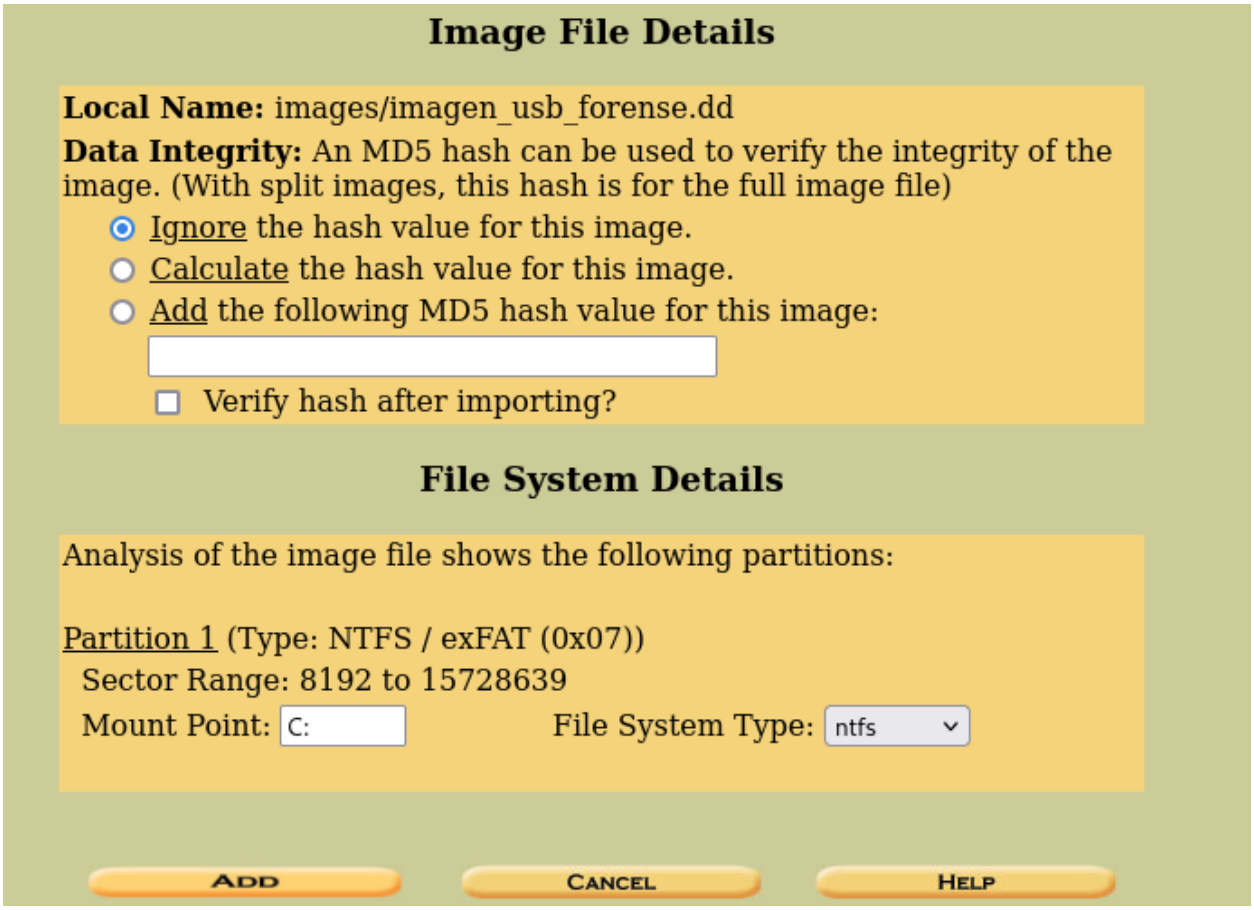
24. Error en la identificación del sistema de archivos

la corrección del parámetro de sistema de archivos, estableciendo el tipo **NTFS** como formato válido de la partición detectada.
El sistema vuelve a analizar la imagen y confirma la configuración mediante los valores de sector y volumen previamente reconocidos.
Este ajuste asegura la correcta interpretación del contenido de la evidencia durante el análisis posterior.



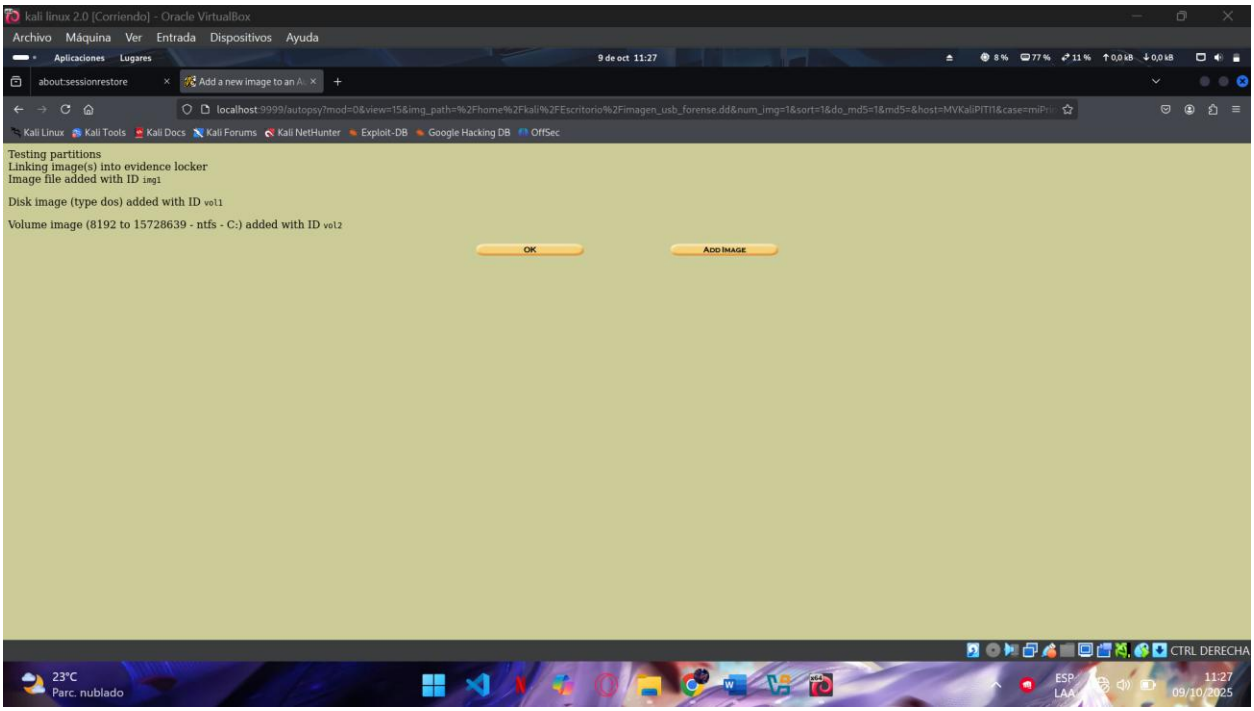
25. Confirmación del tipo de partición NTFS

En el momento en que Autopsy asocia de manera definitiva la imagen forense **“imagen_usb_forense.dd”** al caso **“miPrimerCaso1”**.
El sistema genera identificadores internos para el disco (vol1) y la partición (vol2), garantizando la trazabilidad y autenticidad de la evidencia dentro del registro del caso.
Con este paso, la imagen queda formalmente incorporada al repositorio pericial del sistema.



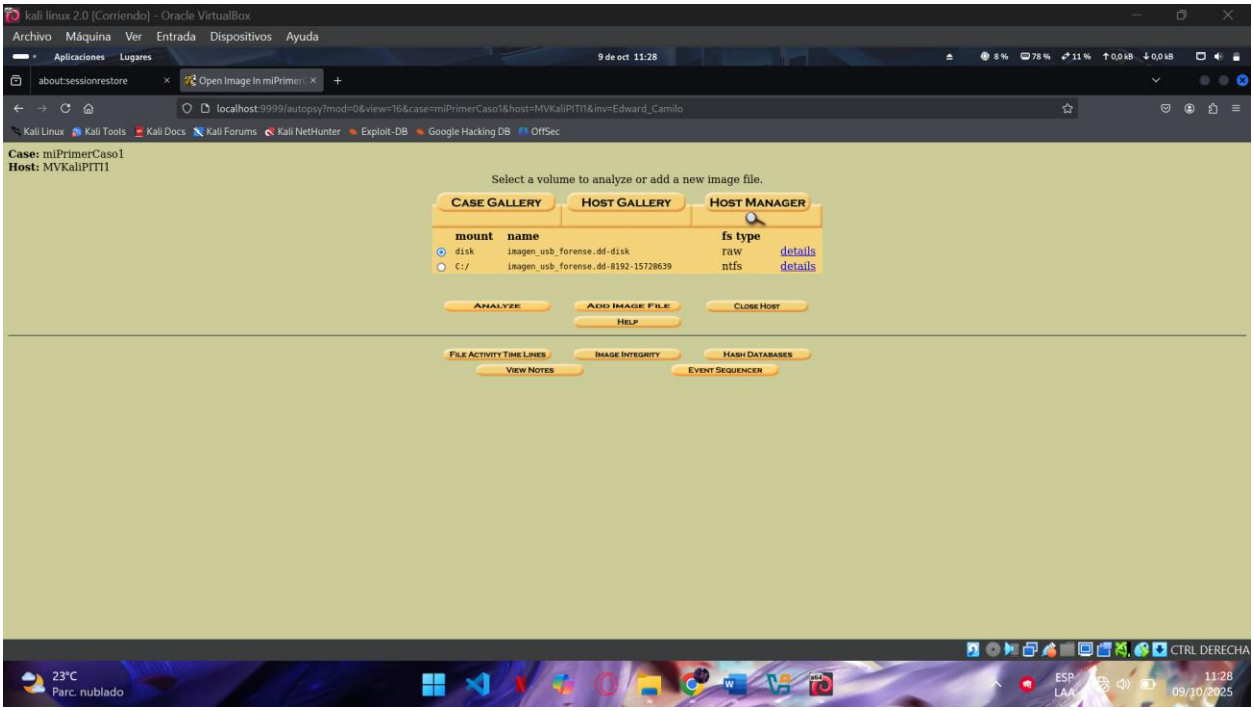
26. Vinculación de la imagen al caso activo

la vista general del caso activo, donde se listan los elementos disponibles para análisis. Entre ellos se identifican el disco completo y la partición montada como **C:**, ambos derivados del archivo **"imagen_usb_forense.dd"**. Desde esta interfaz, el perito puede acceder a las funciones de exploración de archivos, búsqueda de artefactos, extracción de datos o generación de reportes.



27. Visualización general del caso con imagen añadida

panel principal de Autopsy con las opciones disponibles para continuar el proceso de investigación. Entre las herramientas visibles se encuentran **Analyze**, **Add Image File**, **Hash Databases**, **Event Sequencer** y **Image Integrity**. esta pantalla marca el cierre de la fase de configuración e inicio del **análisis forense detallado** sobre el dispositivo representado por la imagen digital adquirida.



28. Panel principal de opciones de análisis

se realiza la selección de la unidad de análisis. Se elige el volumen correspondiente a la ruta *C:/*, y posteriormente se ejecuta la opción **"Analyze"** para iniciar el proceso de exploración de la imagen forense asociada al caso "miPrimerCaso1".

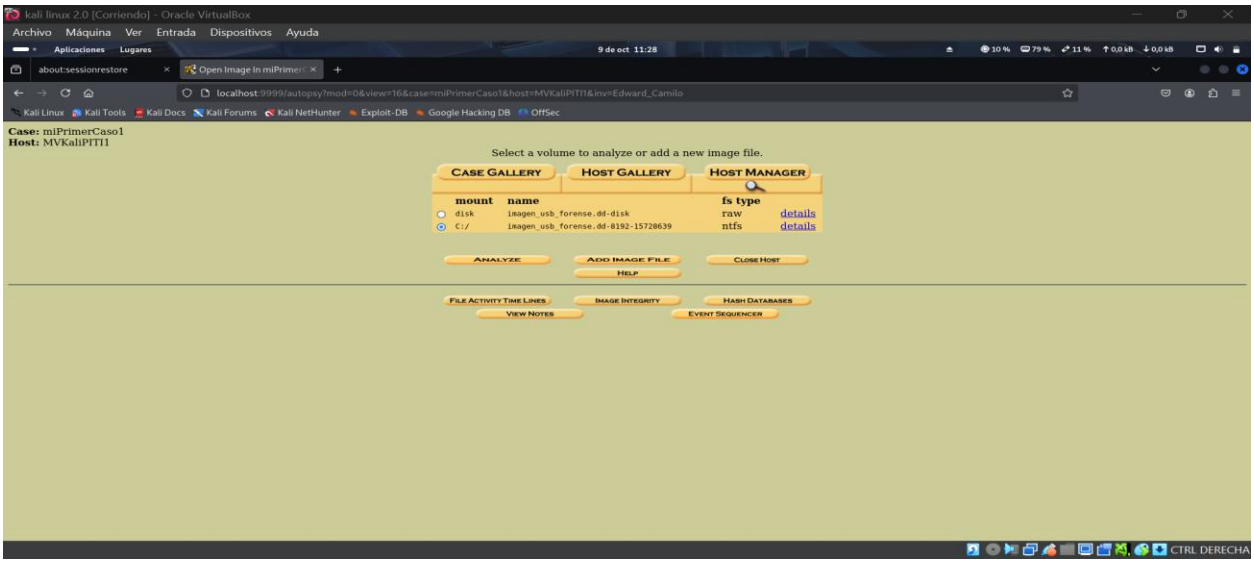


Ilustración 29. Selección de la unidad de análisis en Autopsy

La figura presenta el contenido del directorio raíz *C:/* dentro del entorno de análisis de Autopsy. En esta vista se pueden observar diversos archivos y carpetas listados junto con sus atributos de creación, modificación y acceso, lo cual permite examinar de manera detallada la estructura del sistema de archivos recuperado.

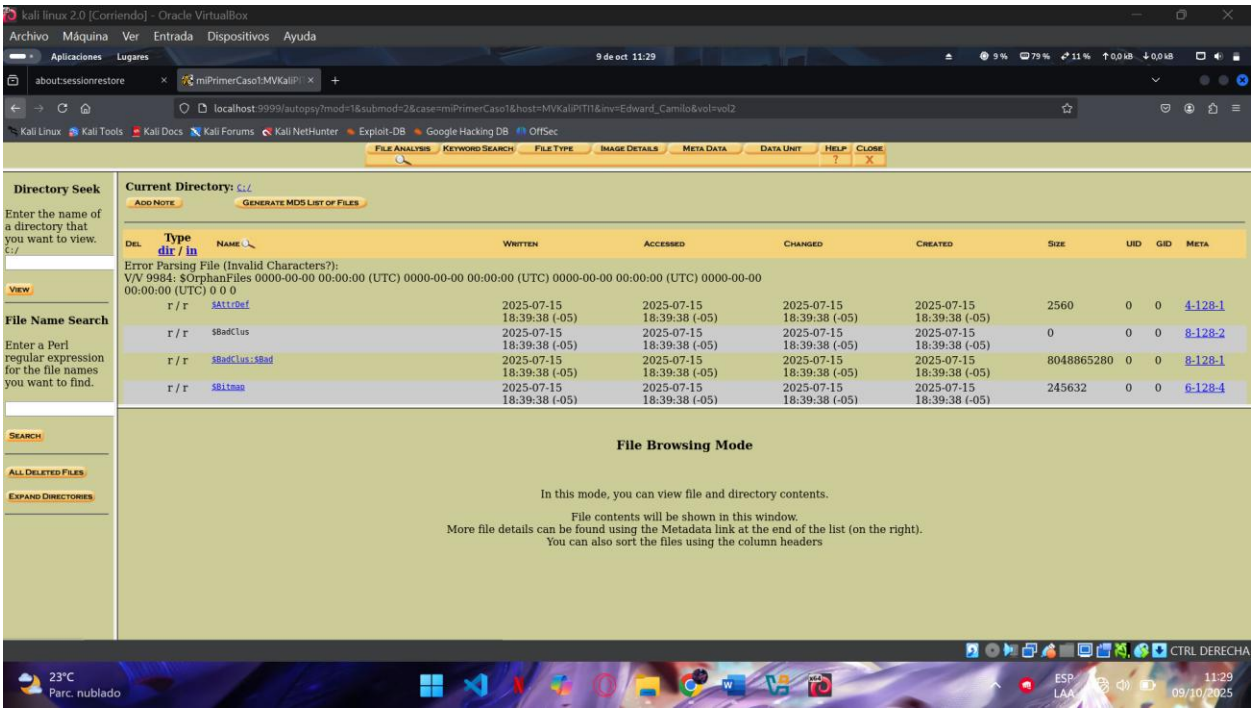


Ilustración 30. Visualización del directorio raíz C:/

Le damos exporta, se aprecia el proceso de exportación de un archivo identificado dentro de la imagen forense. Autopsy permite al analista descargar una copia del archivo para su posterior revisión o análisis especializado, conservando la integridad de la evidencia original mediante la función **“Export”**.

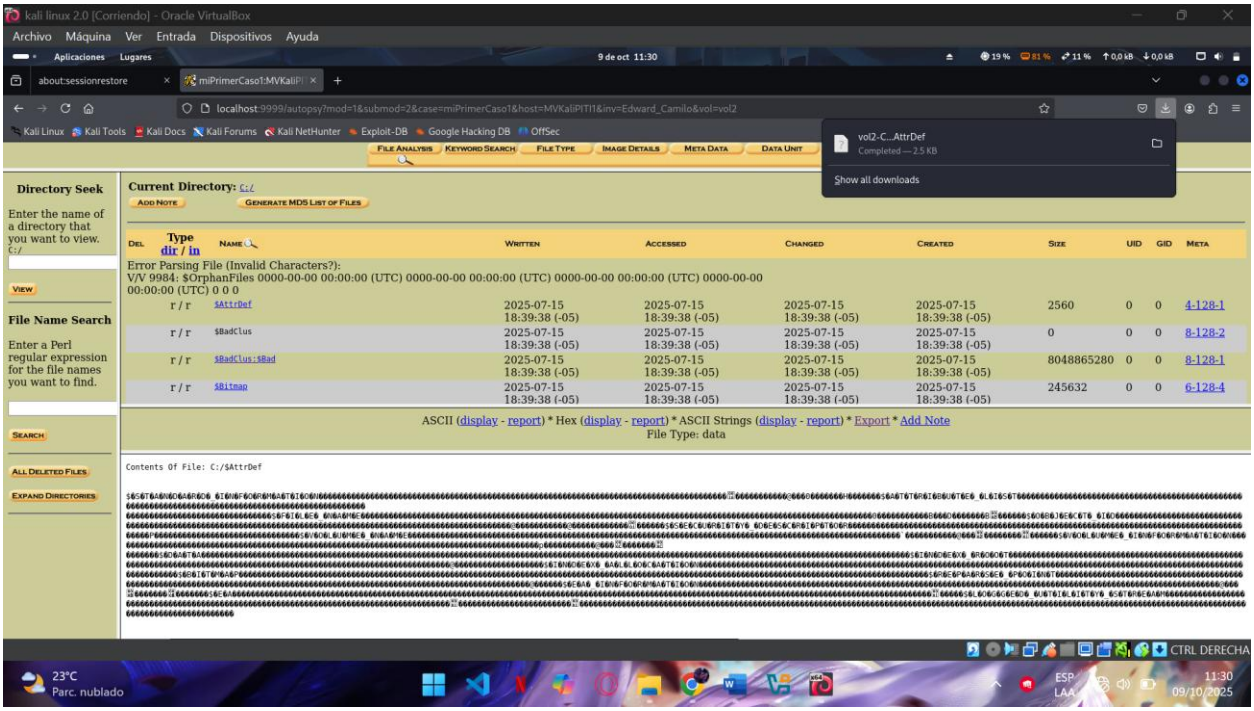


Ilustración 31. Exportación de archivo seleccionado

la detección de archivos marcados en color rojo dentro del listado de Autopsy, lo que indica que dichos elementos fueron **eliminados del dispositivo original**, aunque aún pueden ser recuperados o analizados parcialmente desde la imagen forense.

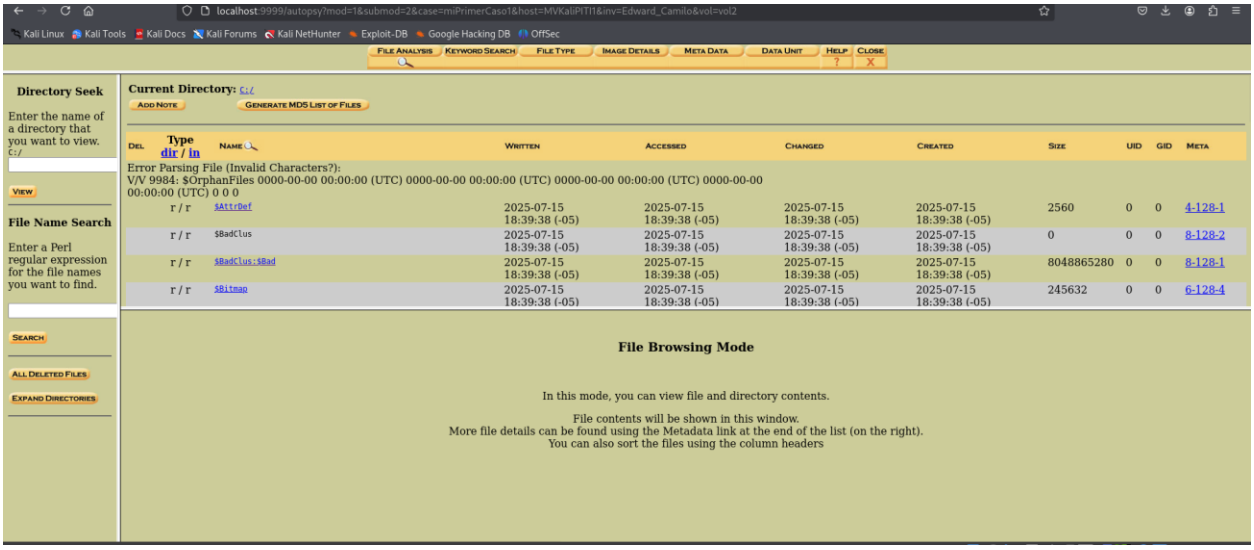


Ilustración 32. Identificación de archivos eliminados

la ejecución de la función **"Generate MD5 List of Files"**, mediante la cual Autopsy genera un listado de valores hash MD5 para cada archivo contenido en la imagen forense. Este procedimiento permite verificar la integridad de los datos y establecer la trazabilidad de los elementos analizados dentro de la investigación digital.

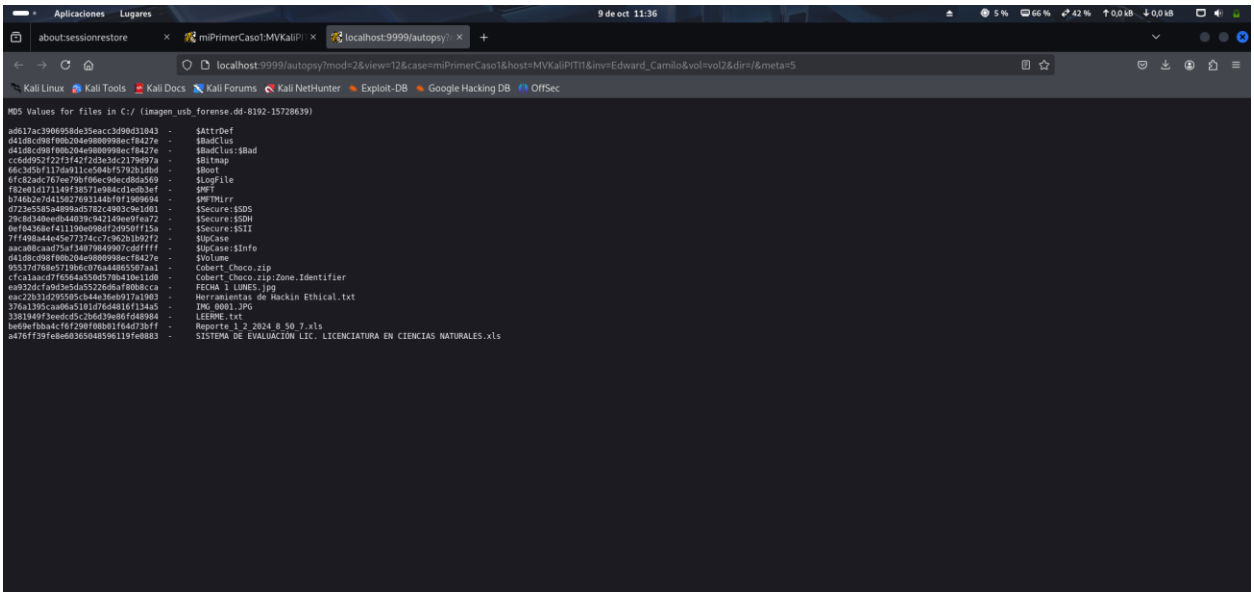


Ilustración 33. Generación del listado de valores hash MD5

se observan los detalles generales del sistema de archivos del dispositivo analizado. Se incluye información del sistema de archivos NTFS, metadatos como el número de serie del volumen, versión del sistema operativo (Windows XP), y parámetros técnicos como el tamaño de clúster, sector y directorios raíz

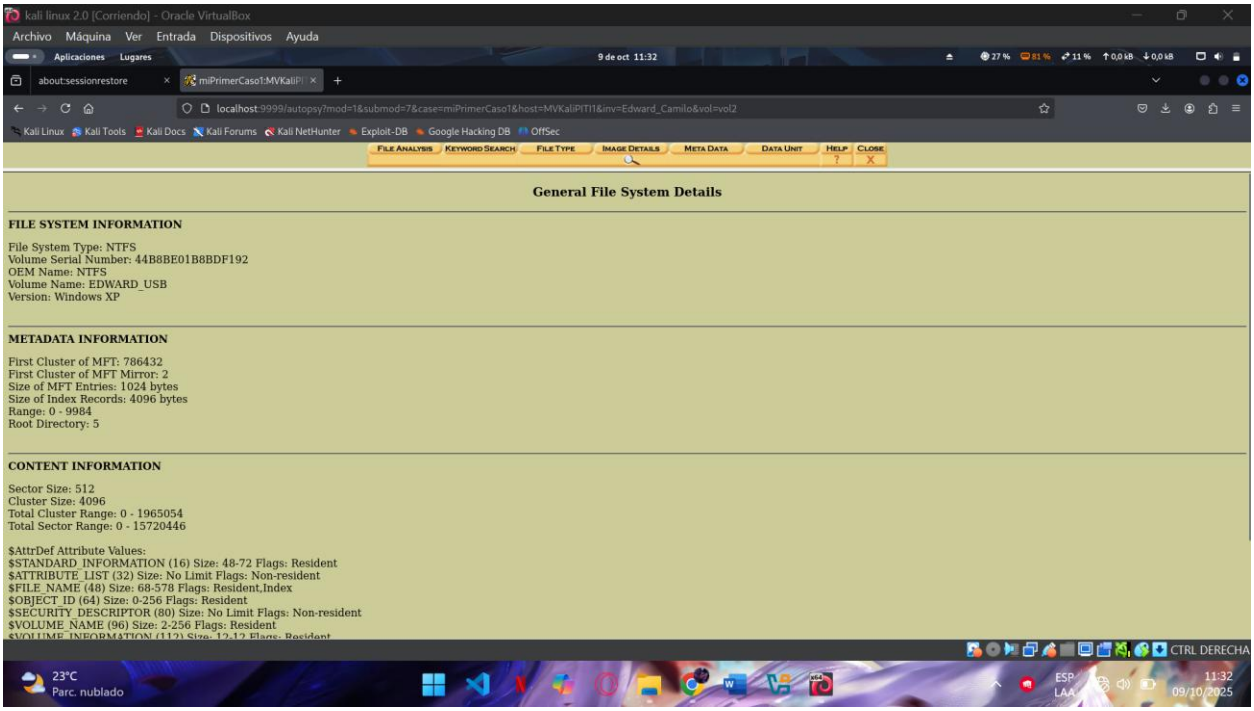


Ilustración 34. Detalles del sistema de archivos NTFS

el proceso de cálculo del hash MD5 de la imagen forense denominada *imagen_usb_forense.dd*. Esta operación se realiza en Autopsy para verificar la integridad de la evidencia digital, garantizando que no haya sido modificada durante el análisis.

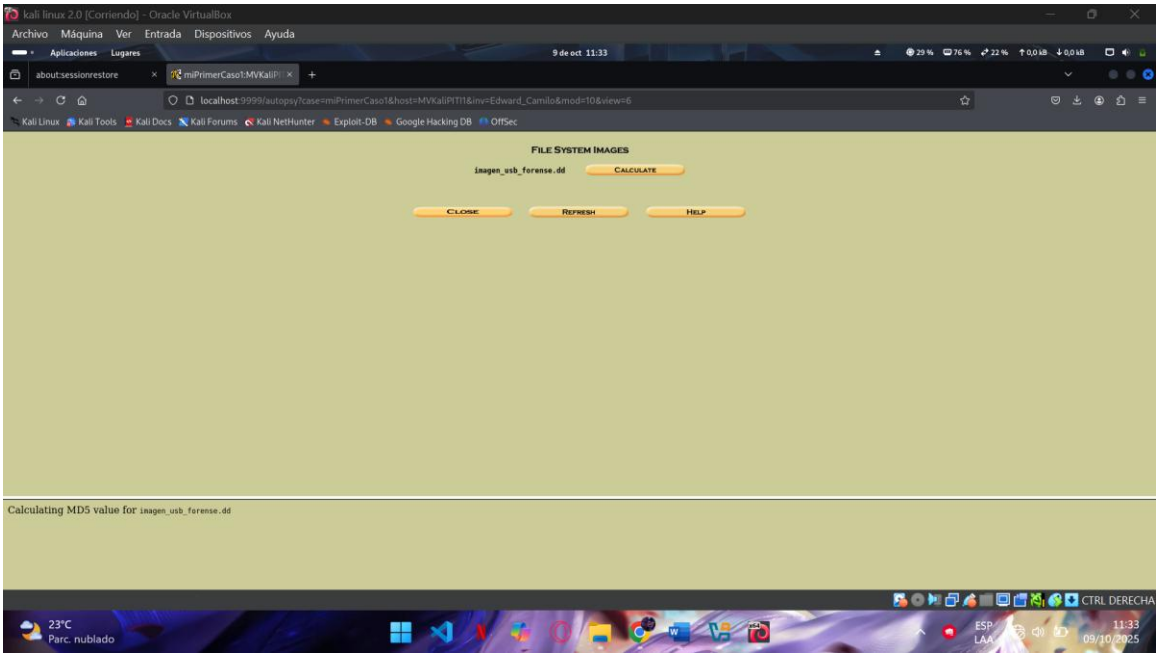


Ilustración 35. Cálculo del valor MD5 de la imagen forense

n se visualiza el valor MD5 generado para la imagen *imagen_usb_forense.dd*, confirmando la finalización exitosa del cálculo y el almacenamiento del resultado en el archivo del host. Este valor servirá como referencia de autenticidad durante todo el proceso de análisis forense.

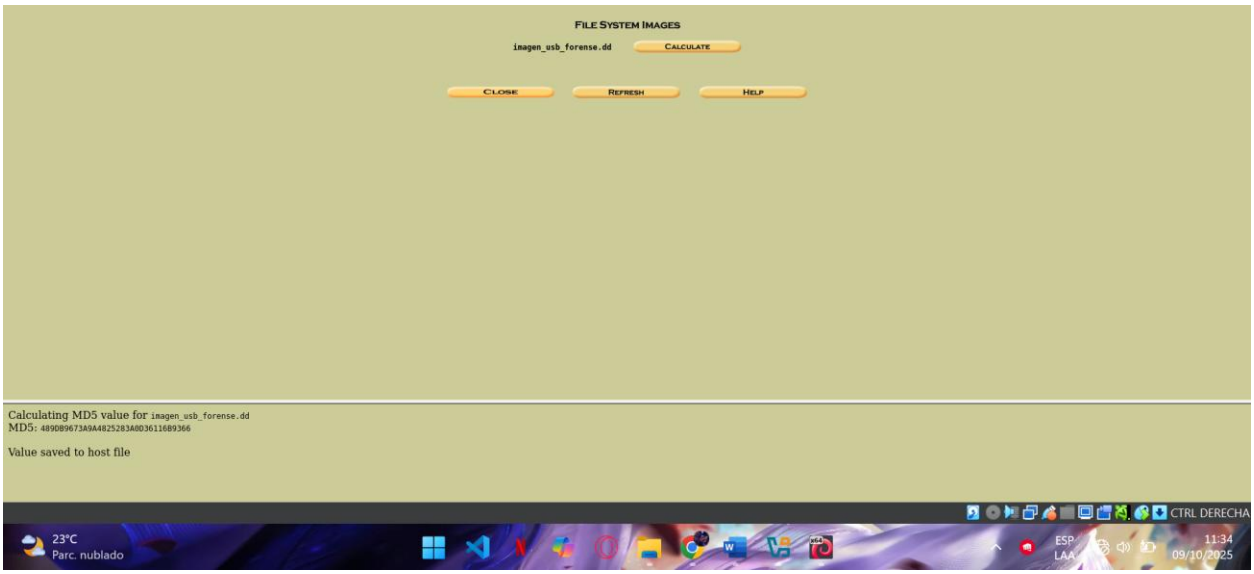


Ilustración 36. Resultado del cálculo MD5 de la imagen forense

CAPITULO 2 DESCARGAR AUTOSY EN WINDOWS Y ANALISIS FORENSE EN WINDOWS

Paso 1: Descargar e instalar en Windows

el sitio oficial de Autopsy desde donde se realiza la descarga de la versión 4.22.1 para sistemas Windows de 64 bits. En la parte superior derecha se observa el historial de descargas del navegador indicando el progreso de la descarga del archivo instalador en formato *.msi*, correspondiente a la herramienta de análisis forense digital.

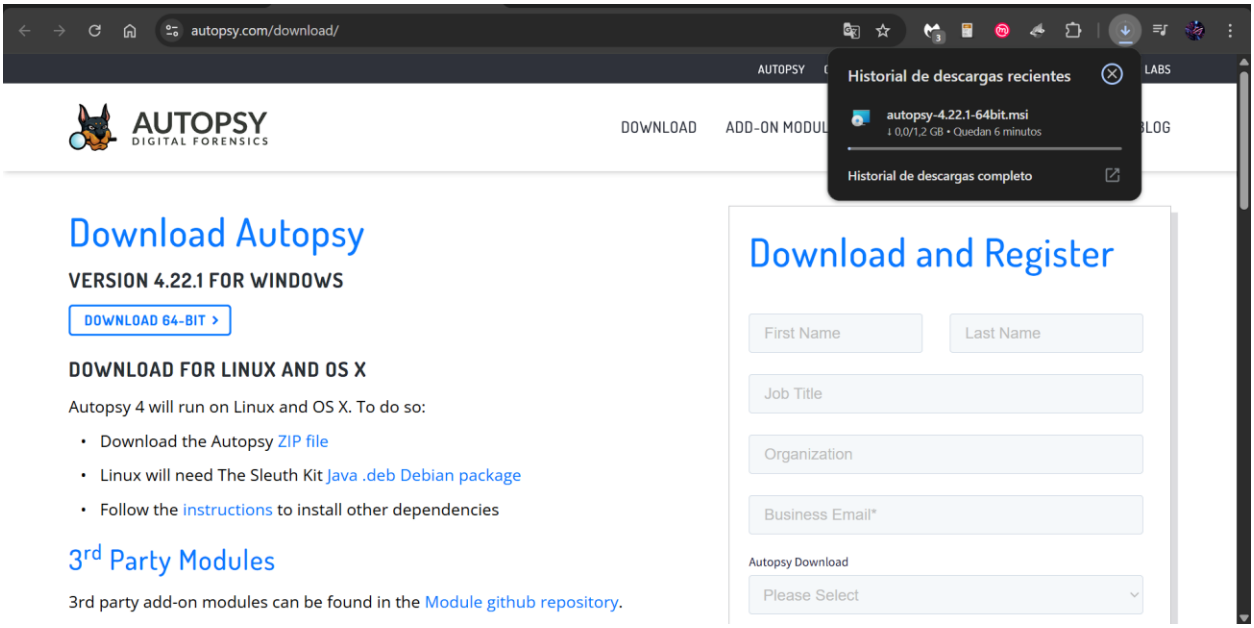


Ilustración 37. Descarga del instalador de Autopsy

En la carpeta de descargas del sistema operativo Windows, donde se encuentra el archivo instalador *autopsy-4.22.1-64bit.msi*. La imagen evidencia que la descarga se completó exitosamente y que el archivo está listo para proceder con la instalación de la herramienta forense Autopsy.

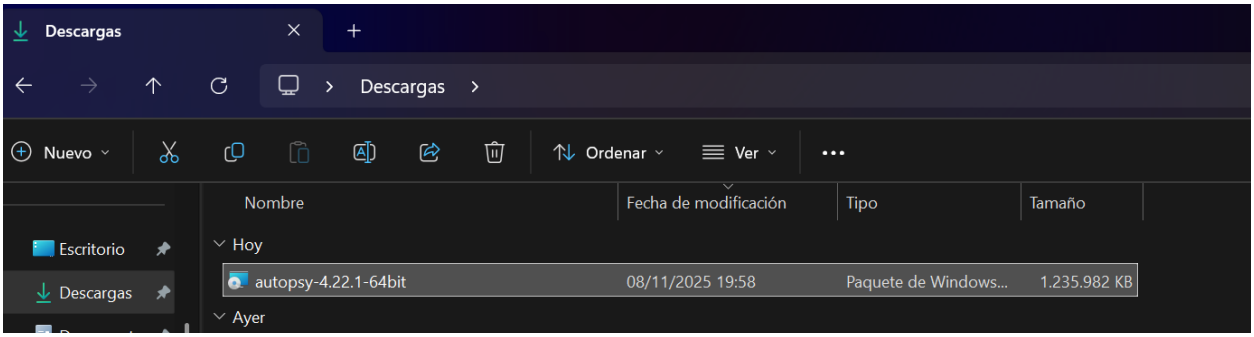


Ilustración 38. Archivo instalador de Autopsy descargado correctamente

En esta ventana se muestra el inicio del asistente de instalación del software Autopsy. Desde aquí se da la bienvenida al usuario y se ofrece la opción de continuar con el proceso de instalación haciendo clic en “Next” o cancelar con “Cancel”.

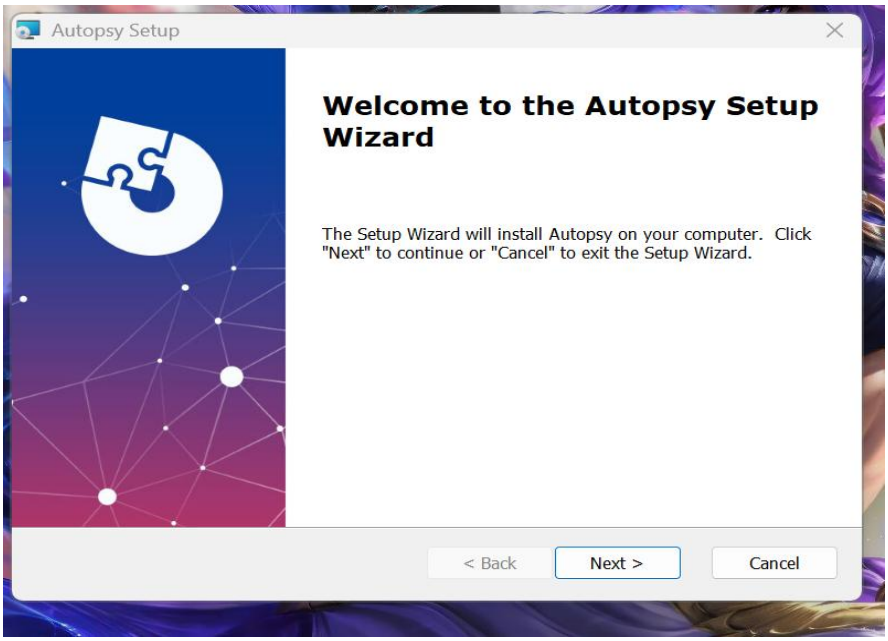


Ilustración 39.Inicio del asistente de instalación de Autopsy

El asistente comienza a instalar los componentes del programa en el sistema. Durante esta etapa, se muestra una barra de progreso que indica el avance de la instalación, la cual puede tardar varios minutos.

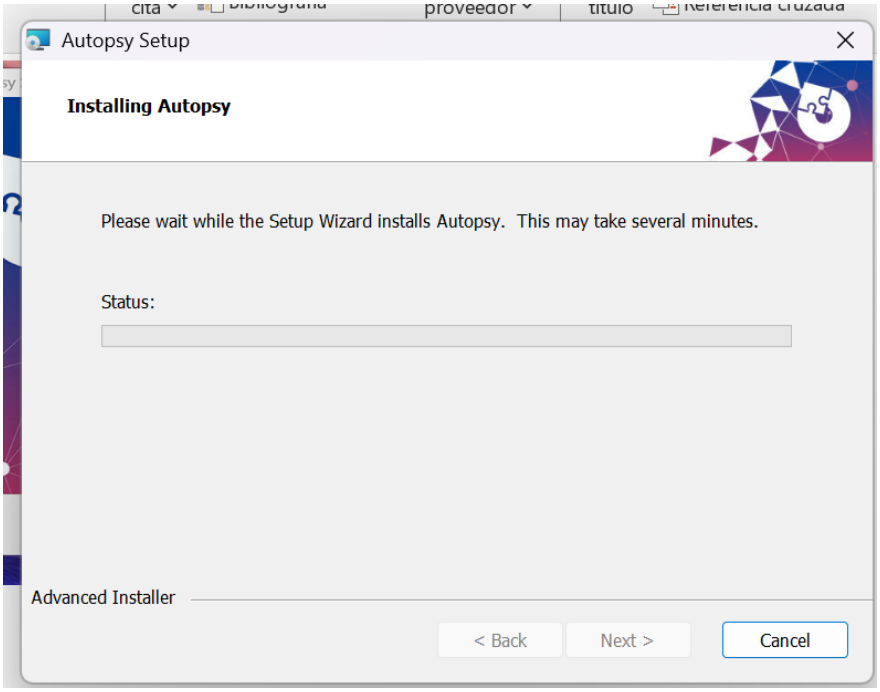


Ilustración 40. Proceso de instalación de Autopsy

Una vez completada la instalación, el asistente muestra la ventana final donde se confirma la correcta instalación del programa. El usuario puede cerrar el asistente seleccionando el botón "Finish".

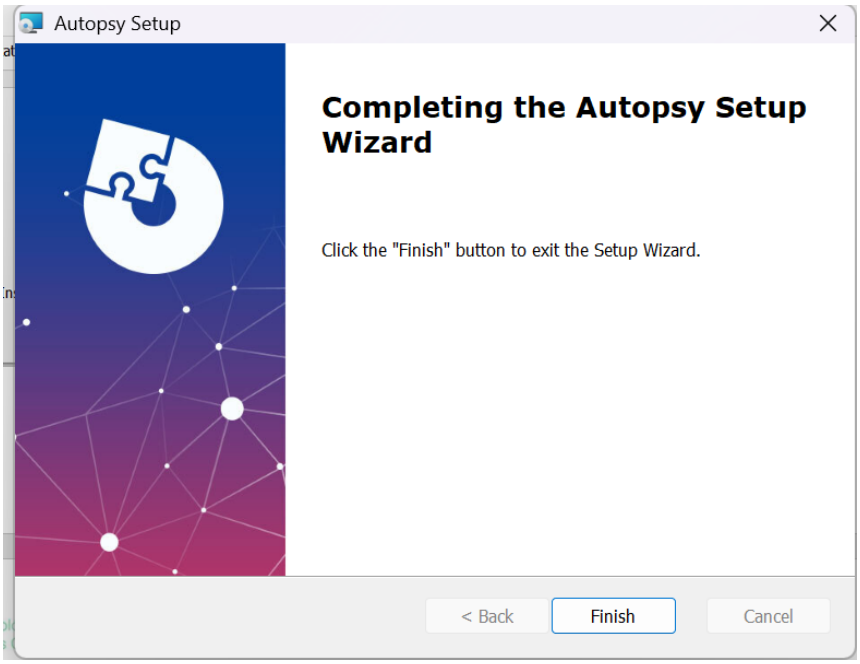


Ilustración 41.Finalización del asistente de instalación

Después de la instalación, se genera un acceso directo en el escritorio del sistema operativo. Este icono permite ejecutar Autopsy fácilmente, mostrando además la versión instalada (4.22.1).

Ilustración 42. Acceso directo de Autopsy creado en el escritorio

Paso 2:

Al iniciar Autopsy, aparece una pantalla de carga con el logotipo característico del programa. En esta fase, el software inicia la lectura de los módulos necesarios para su funcionamiento.

Ilustración 43.Pantalla de carga inicial de Autopsy

Una vez cargado el programa, se presenta la interfaz principal. Desde esta ventana el usuario puede crear un nuevo caso, abrir un caso reciente o acceder a un caso previamente guardado, facilitando la gestión de investigaciones digitales

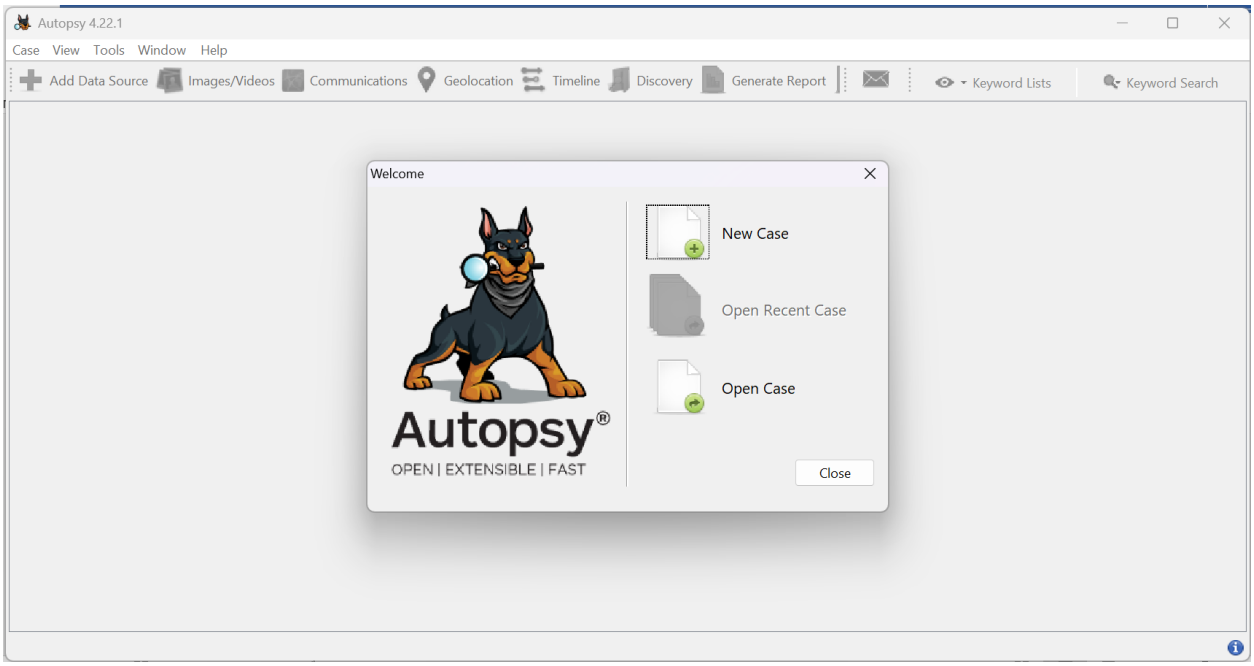


Ilustración 44. Ventana principal de Autopsy

El asistente de Autopsy solicita la información básica del nuevo caso, como el nombre del caso, la ubicación del directorio base y el tipo de caso (usuario único o multiusuario). Esta configuración inicial permite definir la estructura del análisis forense.

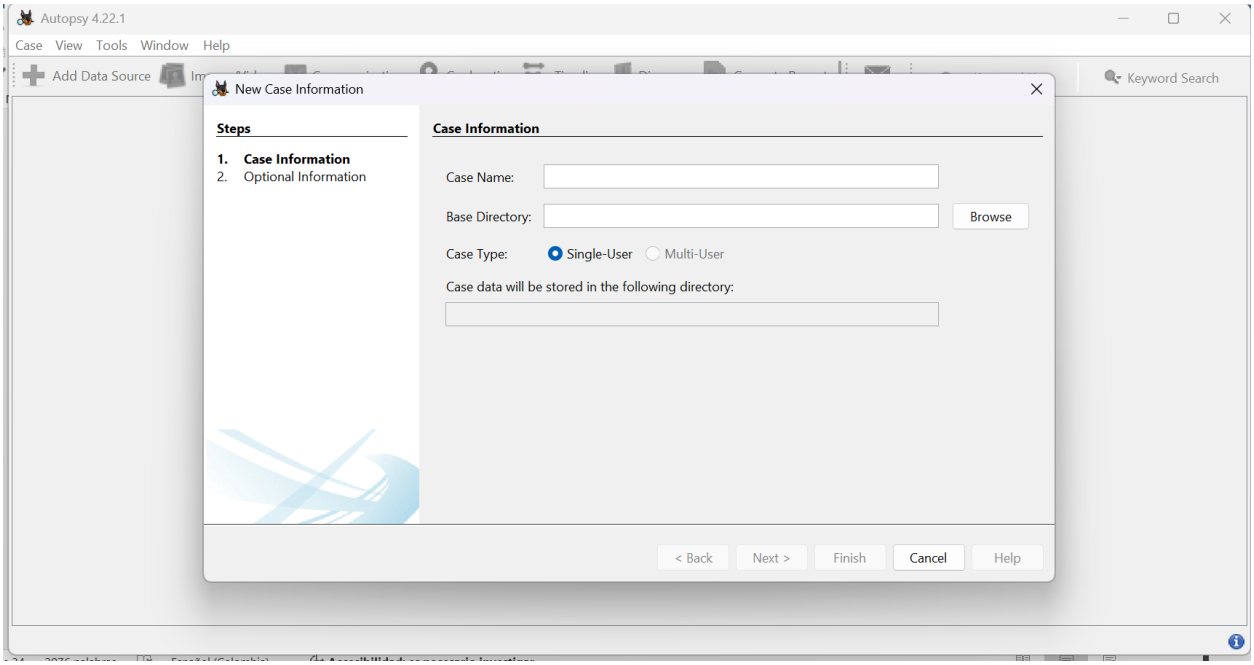


Ilustración 45. Creación de un nuevo caso

En esta etapa, el usuario ingresa los datos identificativos del caso, incluyendo el nombre, la ubicación del directorio y el tipo de usuario. Esta información determina la ruta donde se almacenarán los resultados y archivos relacionados con la investigación.

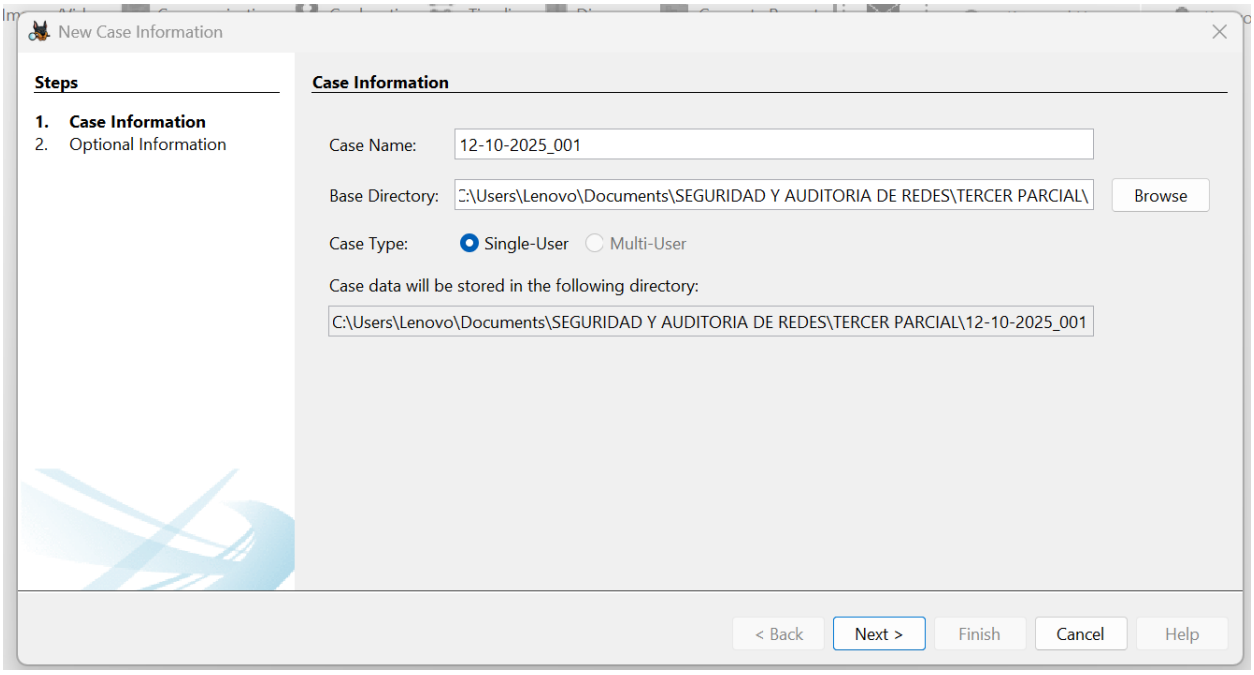


Ilustración 46. Registro de la información del caso

Autopsy permite añadir información complementaria, como el número del caso, el nombre del examinador, teléfono, correo electrónico y organización. Estos datos sirven para documentar adecuadamente la autoría y trazabilidad del análisis.

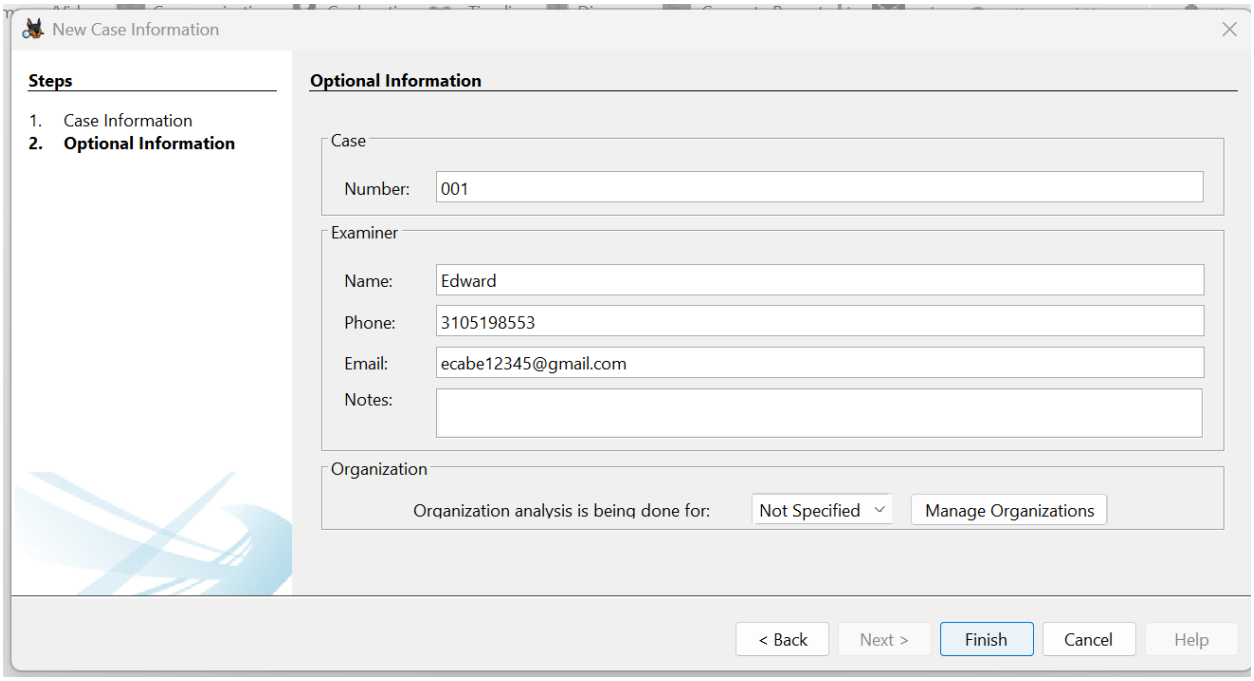


Ilustración 47. Información opcional del caso

Finalmente, el programa crea la base de datos correspondiente al nuevo caso. Este proceso inicializa la estructura interna donde se guardarán las evidencias digitales, resultados de los módulos y reportes generados durante el análisis.

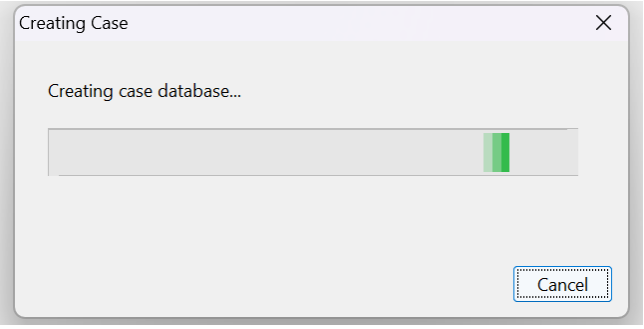


Ilustración 48. Creación de la base de datos del caso

Paso 3

En esta etapa del asistente para agregar una fuente de datos, Autopsy permite definir el host (equipo o fuente) sobre el cual se realizará el análisis. El usuario puede generar automáticamente un nuevo nombre basado en la fuente de datos, especificar uno manualmente o seleccionar un host existente.

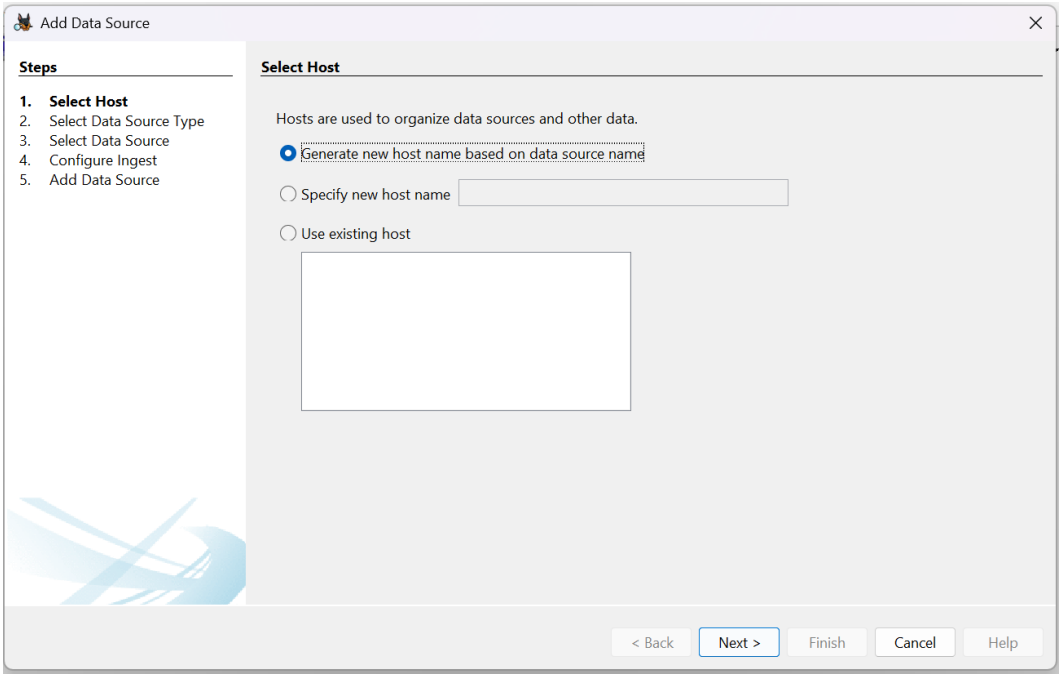


Ilustración 49. Selección del host de análisis

Autopsy ofrece diferentes tipos de fuentes de datos para analizar, como imágenes de disco, discos locales, archivos lógicos, espacio no asignado o exportaciones de texto. En este caso, se selecciona la opción **"Local Disk"**, indicando que el análisis se realizará directamente sobre una unidad física conectada al sistema.

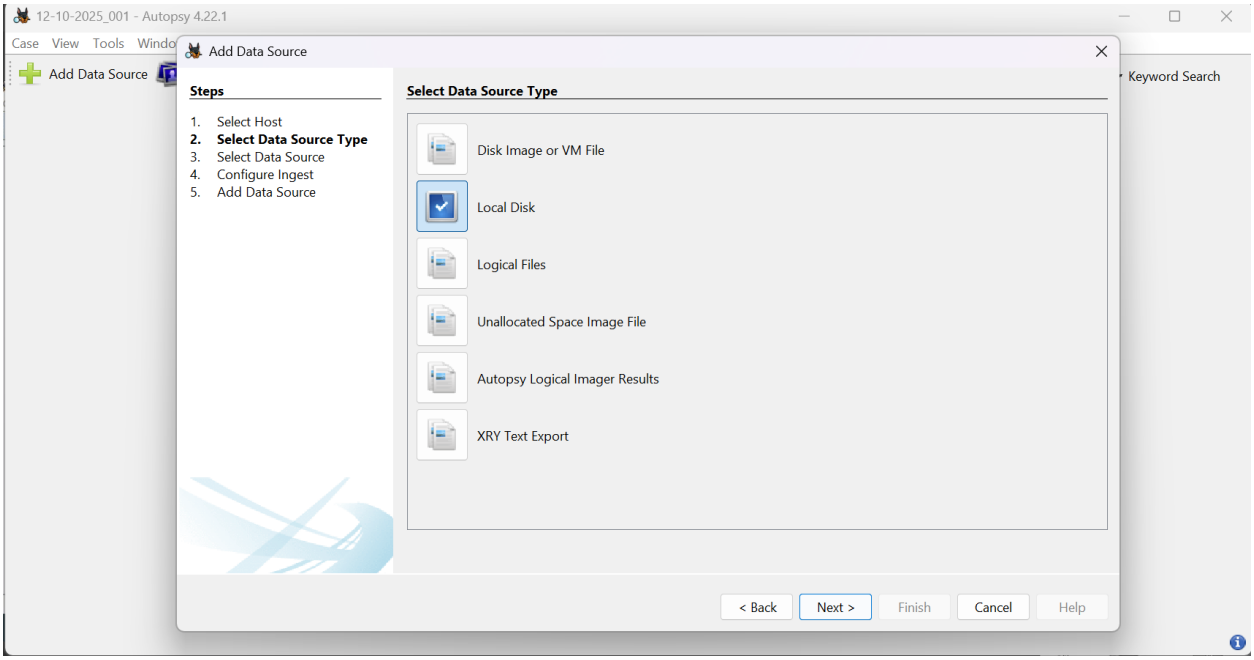


Ilustración 50. Selección del tipo de fuente de datos

En esta ventana, el usuario elige el disco local que será objeto de análisis. Además, se configuran parámetros como la zona horaria y la posibilidad de crear una imagen VHD del disco durante el proceso. Estas opciones permiten un control detallado del entorno forense.

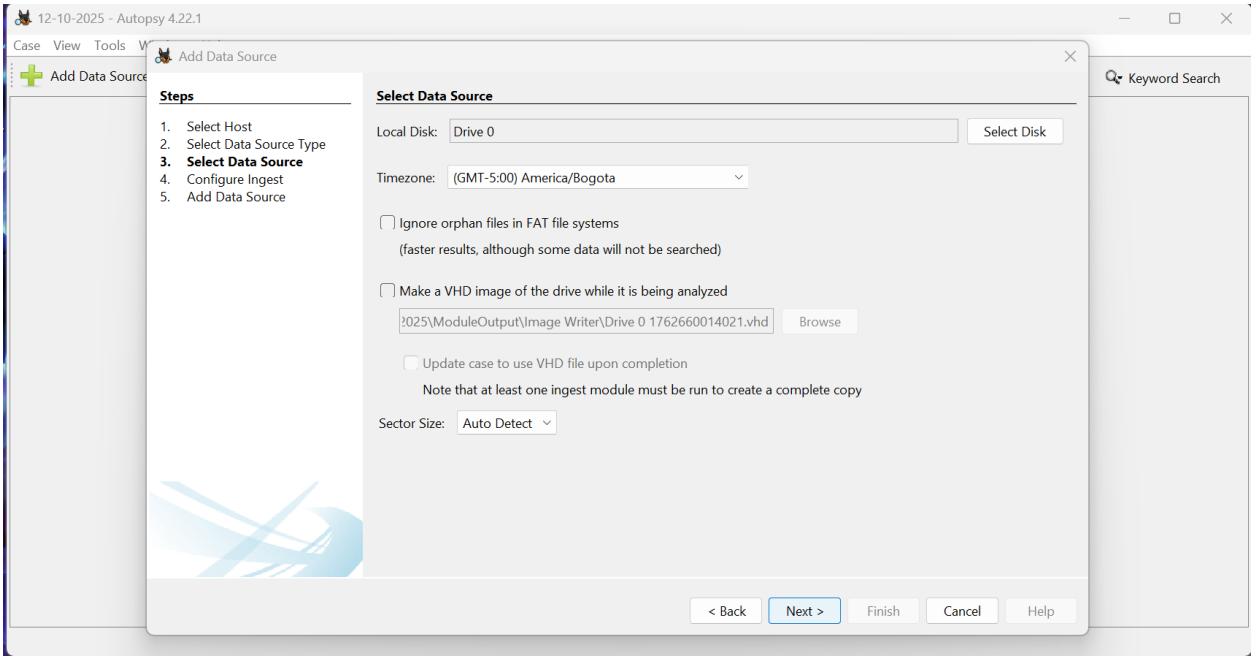


Ilustración 51. Selección de la fuente de datos (disco local)

Autopsy permite seleccionar los módulos de análisis (“ingest modules”) que se ejecutarán sobre la fuente de datos. Entre los más relevantes se incluyen la detección de actividad reciente, identificación de tipos de archivos, búsqueda por palabras clave, análisis de imágenes y extracción de correos electrónicos. Esta configuración determina el alcance del análisis forense.

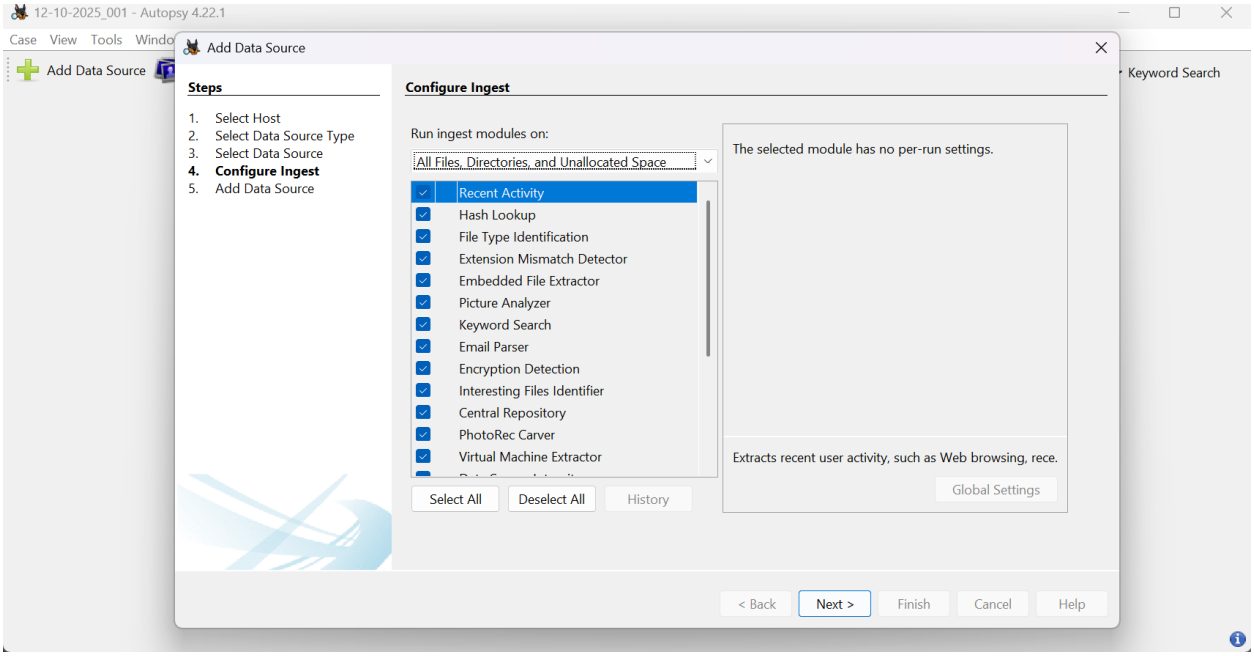


Ilustración 52. Configuración de módulos de análisis

el sistema comienza a procesar la fuente de datos seleccionada, añadiéndola a la base de datos local del caso. Durante esta etapa, Autopsy analiza archivos, directorios y sectores no asignados, lo que puede tomar tiempo dependiendo del tamaño del disco.

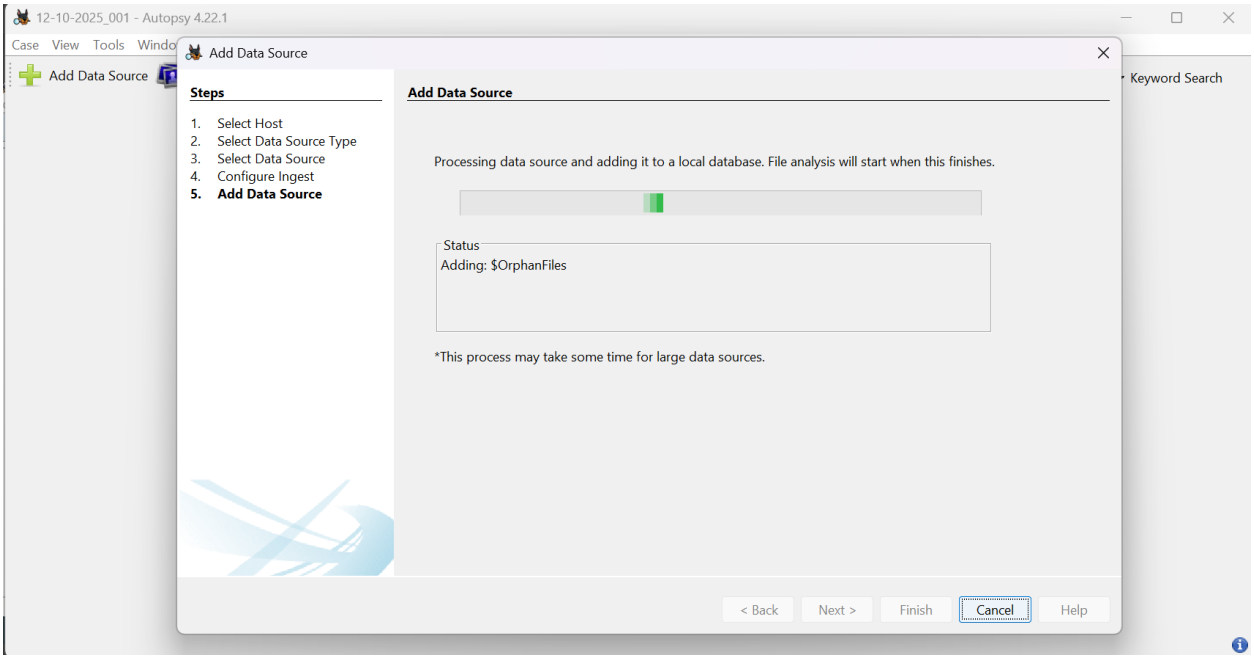


Ilustración 53. Adición y procesamiento de la fuente de datos

Durante el proceso de incorporación de la fuente de datos en Autopsy, se generó un error no crítico. El mensaje indica que el sistema no pudo determinar el tipo de sistema de archivos debido a un sector reservado de Microsoft. Este tipo de advertencia puede presentarse cuando existen particiones protegidas o áreas del disco que no contienen datos reconocibles por el programa.

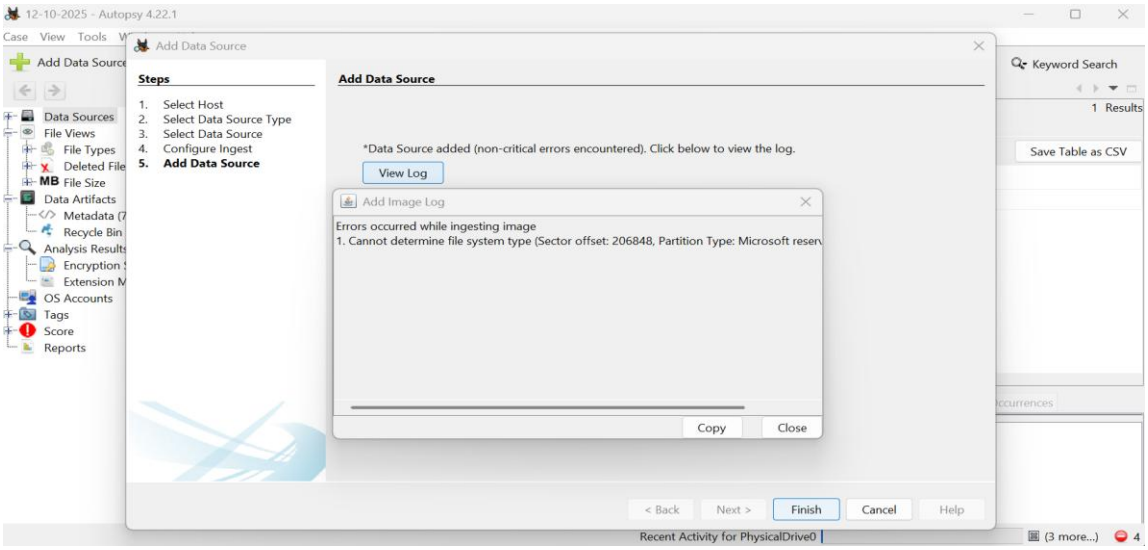
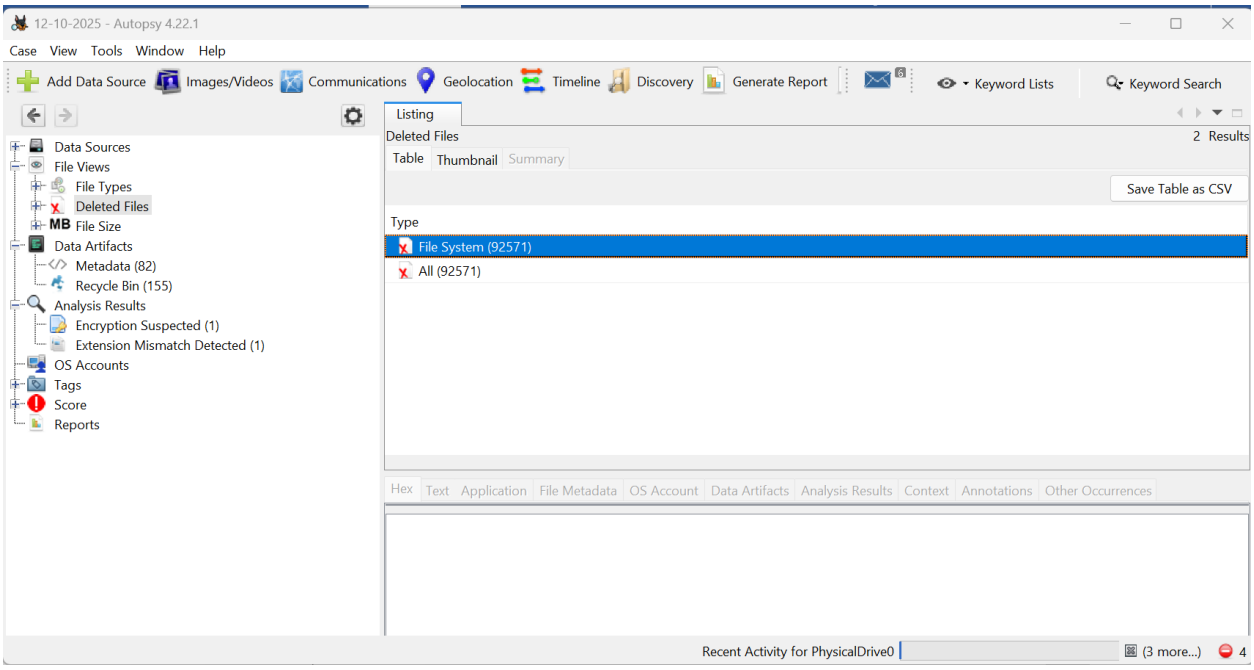


Ilustración 54. Error al procesar la fuente de datos

Finalmente, Autopsy muestra los resultados del análisis con un total de 92,571 archivos eliminados detectados. En la vista de “Deleted Files”, se puede observar la categorización de los archivos tanto por sistema de archivos como por tipo general. Esta información es útil para recuperar y examinar posibles evidencias digitales que hayan sido eliminadas del dispositivo analizado.



CAPITULO 3 INTALAR EN WINDOWS FTK IMAGER .dd Y HACER ANÁLISIS FORENSE DEBE DAR LOS MISMO CIFRADO

Paso 1

página oficial de Exterro que presenta la herramienta FTK Imager, destacando la opción para descargar gratuitamente la utilidad forense para crear imágenes digitales.

Ilustración 55. Página principal de Exterro FTK Imager

el sitio web donde se muestra el formulario necesario para descargar FTK Imager Pro 8.2, solicitando datos como nombre, correo y organización del usuario.

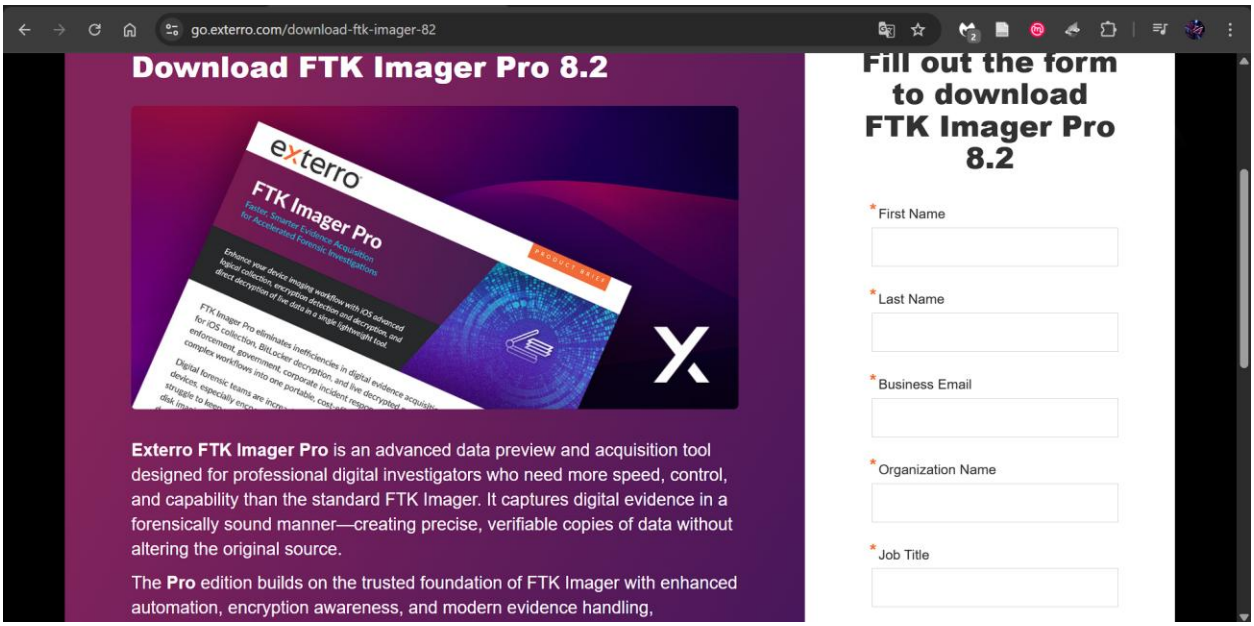


Ilustración 56. Formulario de descarga de FTK Imager Pro 8.2

la descarga activa del archivo comprimido ImagerPro_8.2.0.26.zip, junto a la descarga previa de Autopsy.

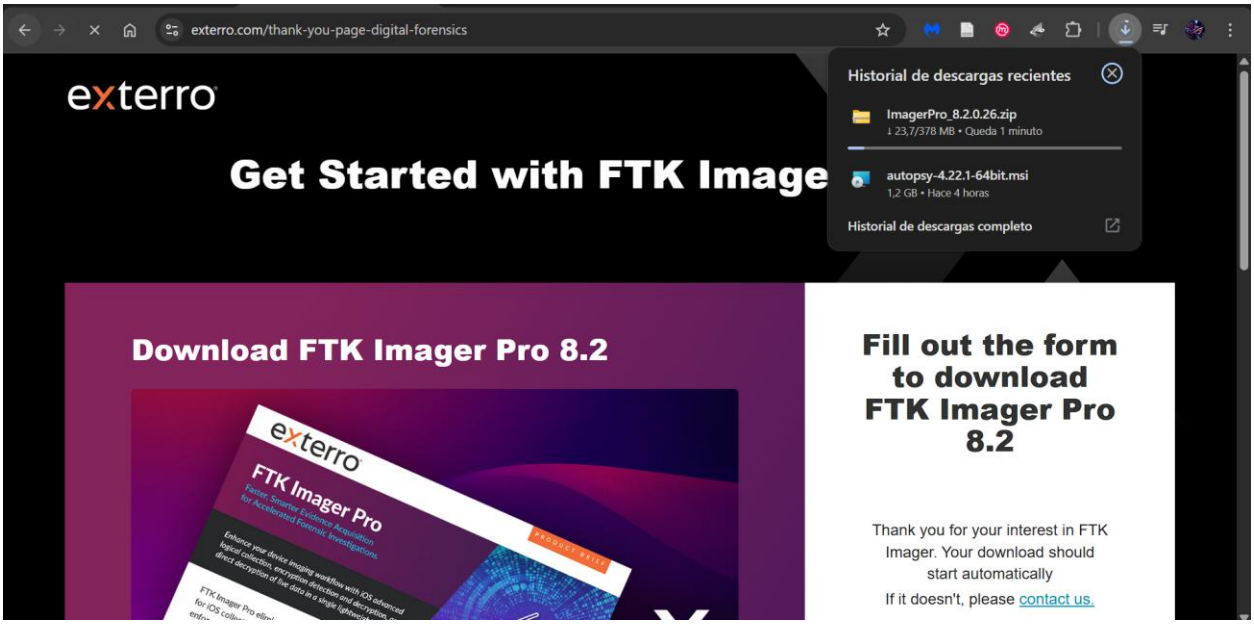


Ilustración 57. Descarga de FTK Imager Pro en progreso

Vista del explorador de archivos mostrando el instalador Exterro_FTK_Imager_(x64) y la carpeta ISSetupPrerequisites, generados tras la descarga y extracción del archivo ZIP.

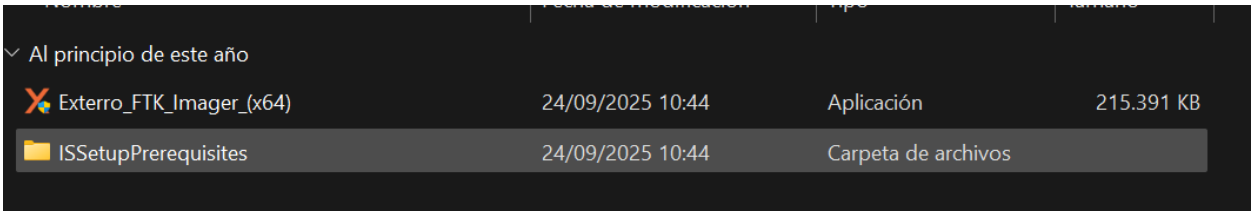


Ilustración 58.Archivos del instalador de FTK Imager

asistente de instalación de FTK Imager mostrando el proceso de instalación de CodeMeter Runtime 8.20, requisito previo necesario para ejecutar la herramienta.

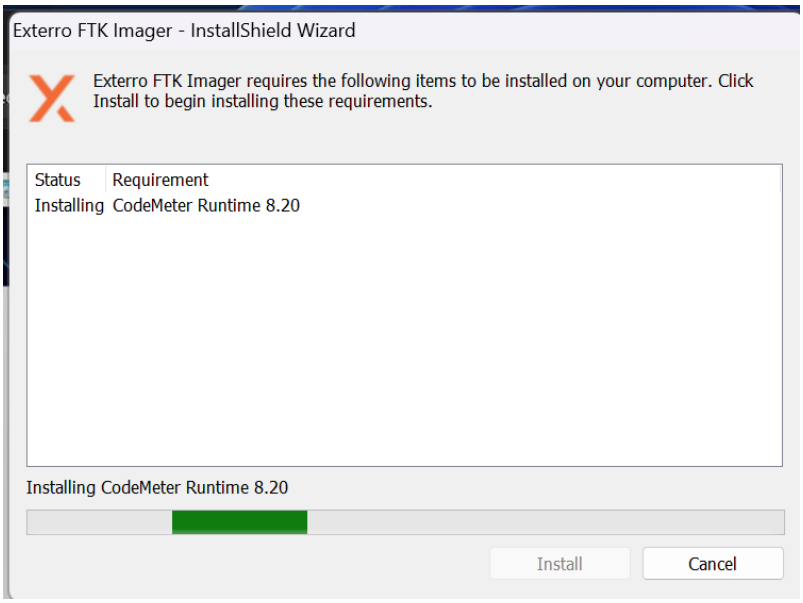


Ilustración 59. Instalación de CodeMeter Runtime 8.20

Captura del escritorio de Windows con el acceso directo creado automáticamente por la instalación de Exterro FTK Imager, indicando que la instalación fue completada con éxito.

Ilustración 60.Icono de Exterro FTK Imager en el escritorio

Paso 2

Interfaz inicial del programa FTK Imager 8.2.0.26, lista para iniciar el proceso de adquisición forense. En este punto no se ha agregado ninguna evidencia.

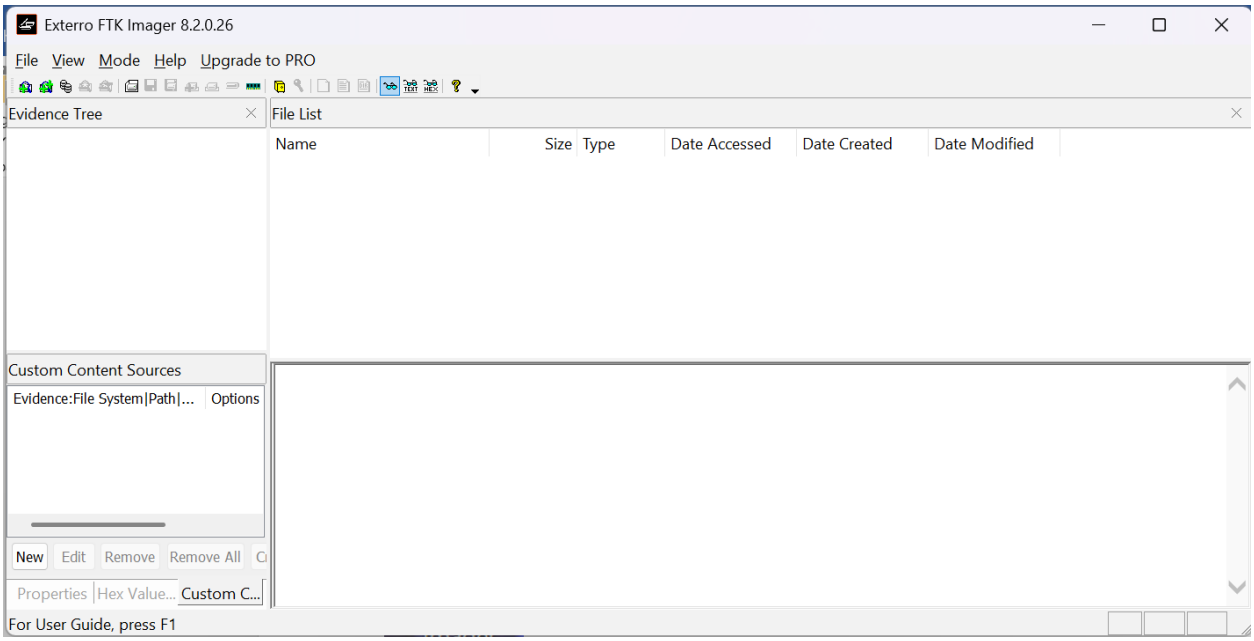


Ilustración 61. Ventana principal de FTK Imager

Desde el menú *File*, se selecciona la opción **"Create Disk Image"** para comenzar la creación de una imagen forense de un dispositivo físico o lógico.

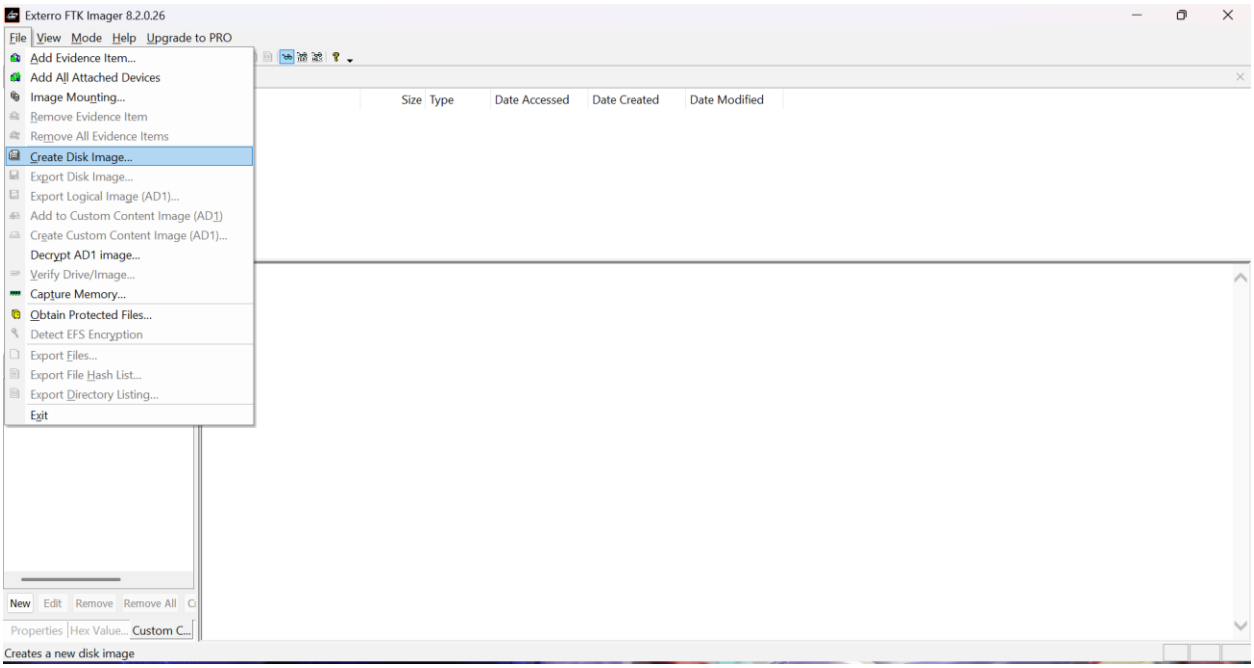


Ilustración 62. Menú "Create Disk Image"

Se abre la ventana **"Select Source"**, donde se elige el tipo de origen de evidencia. En este caso, se selecciona **"Physical Drive"** para clonar un dispositivo físico completo.

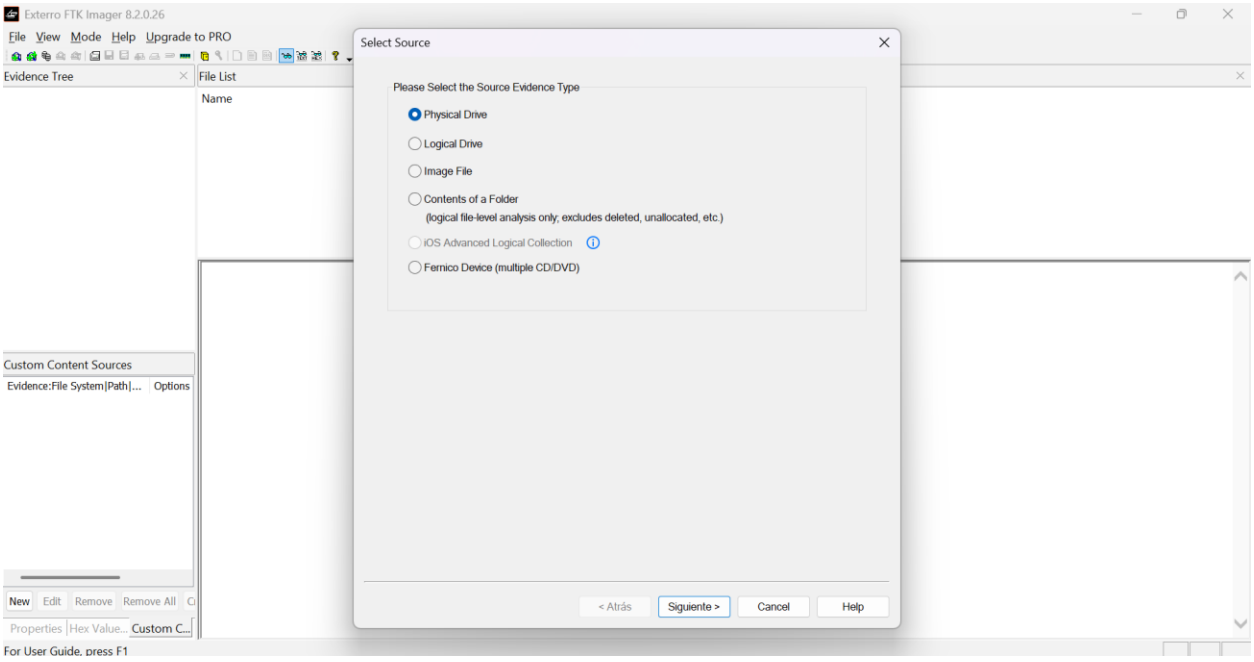


Ilustración 63.Selección del tipo de evidencia

Se listan los dispositivos físicos detectados por el sistema. El usuario selecciona la unidad USB que será utilizada como fuente de la imagen forense.

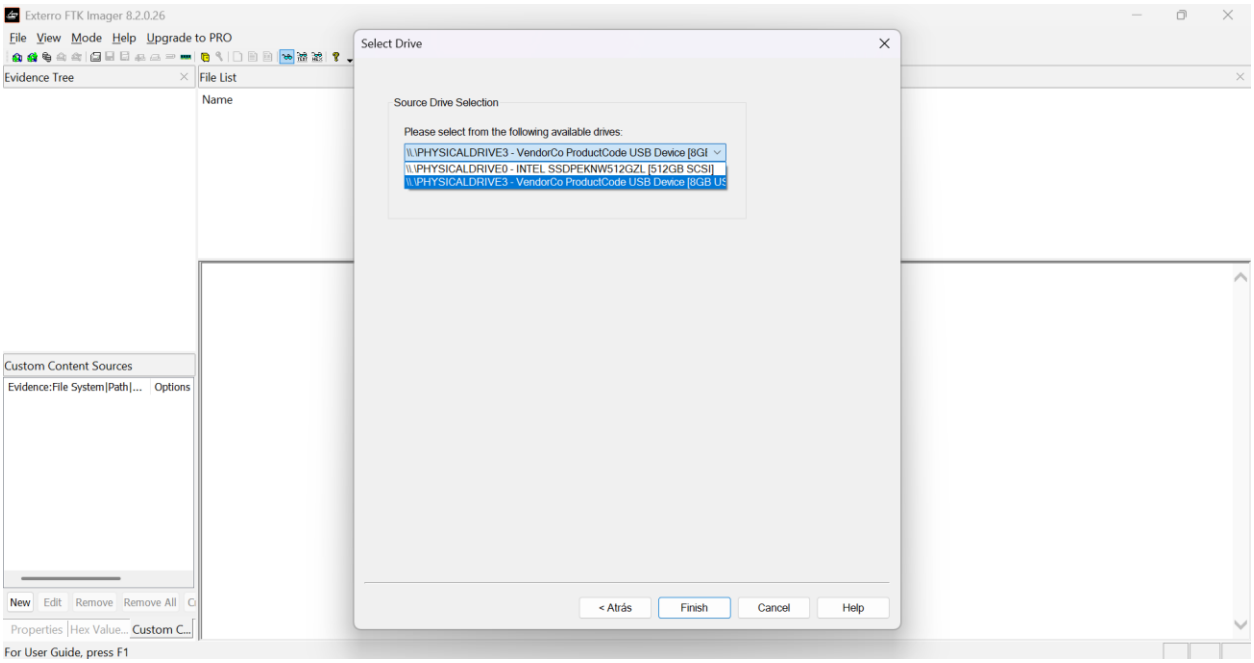


Ilustración 64. Selección del dispositivo de origen

En la ventana **"Select Image Type"**, se selecciona el formato **RAW (dd)**, el cual crea una copia bit a bit del dispositivo sin compresión.

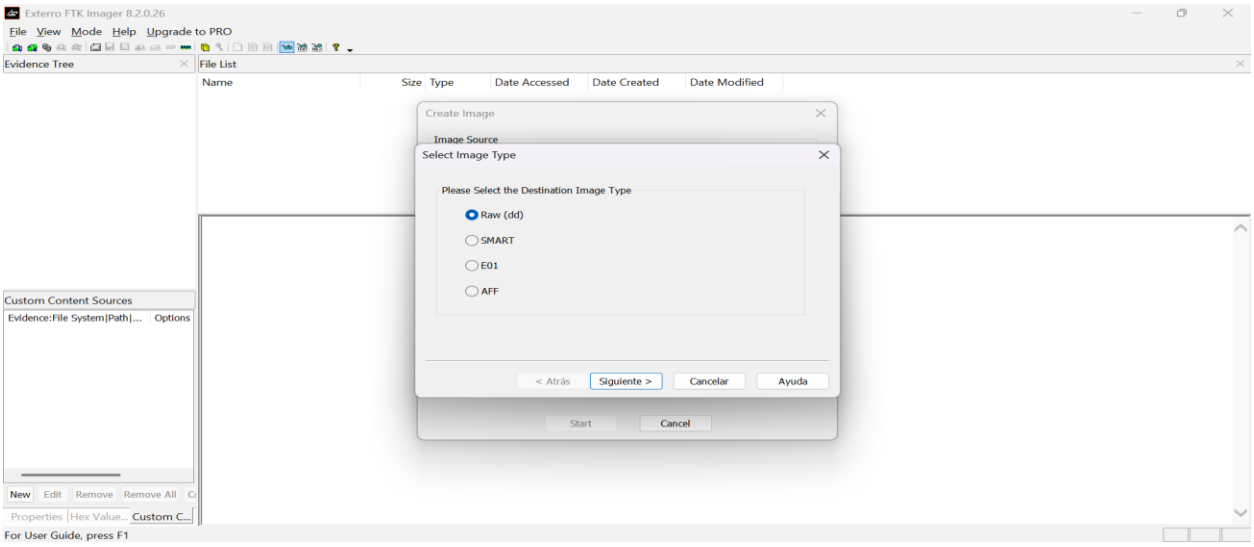


Ilustración 65. Tipo de imagen a generar

Se completan los campos de identificación del caso: número, evidencia, descripción, examinador y notas. Esta información permite mantener la cadena de custodia y documentación del proceso.

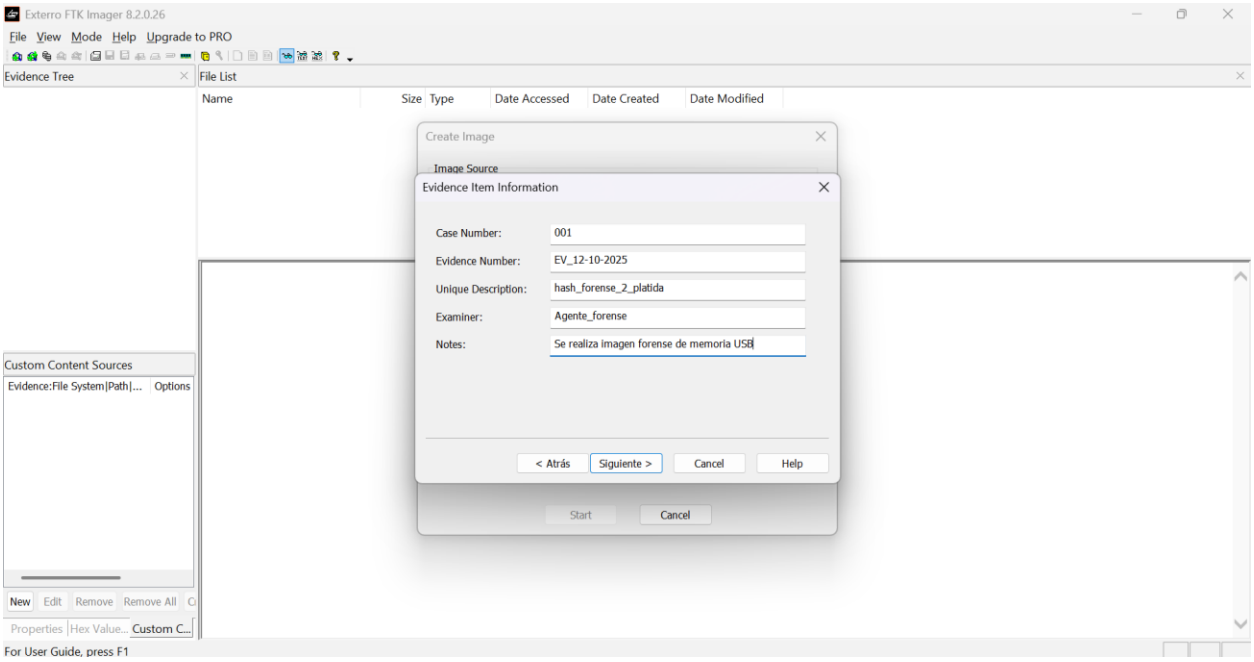


Ilustración 66. Información del caso

El usuario especifica la carpeta donde se guardará la imagen forense y asigna un nombre al archivo de salida. Se deja activada la opción de **encriptación AD** para mayor seguridad.

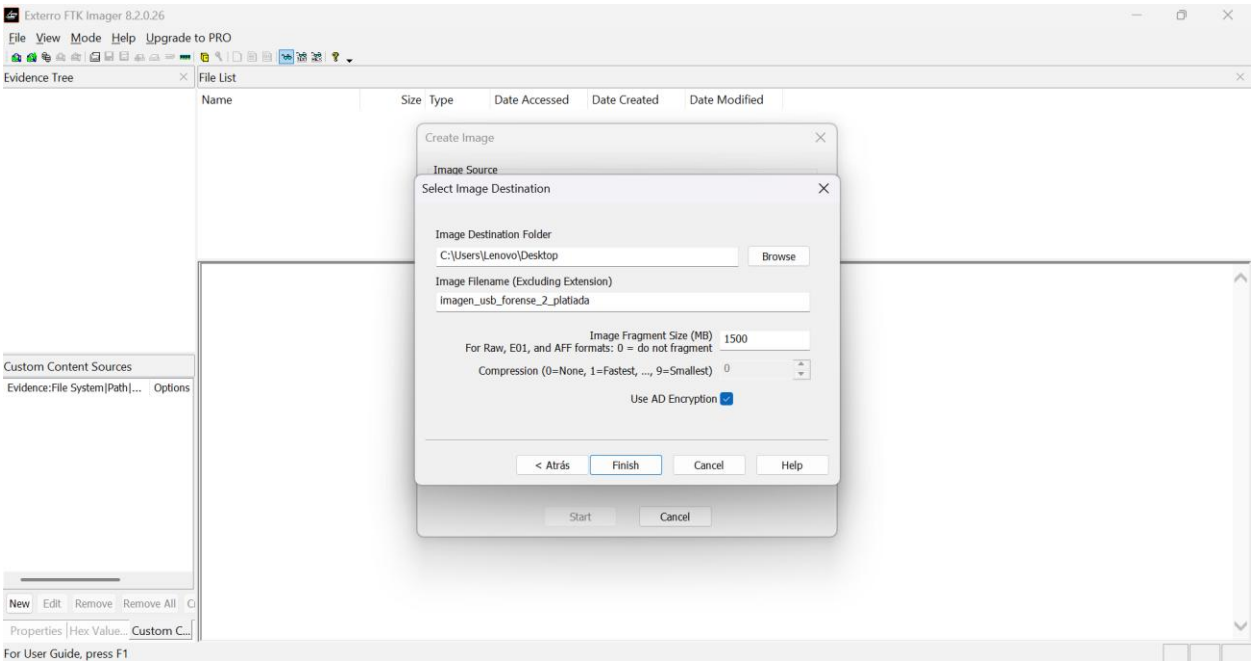


Ilustración 67. Selección de la ubicación de destino

En esta ventana se muestra el resumen de configuración antes de iniciar el proceso. Se presiona **"Add"** para agregar la ruta de destino y luego **"Start"** para comenzar la creación de la imagen.

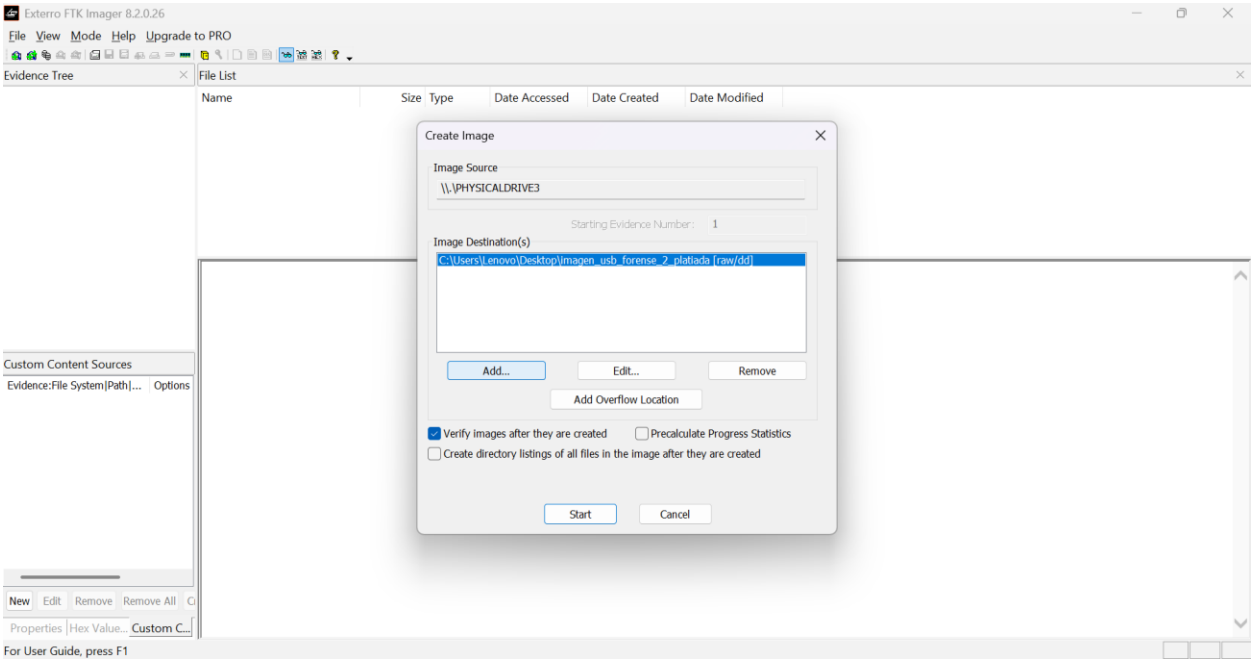


Ilustración 68. Confirmación de los datos

FTK Imager inicia la copia forense del dispositivo USB seleccionado. Se observa el progreso del proceso junto con el tiempo transcurrido y estimado.

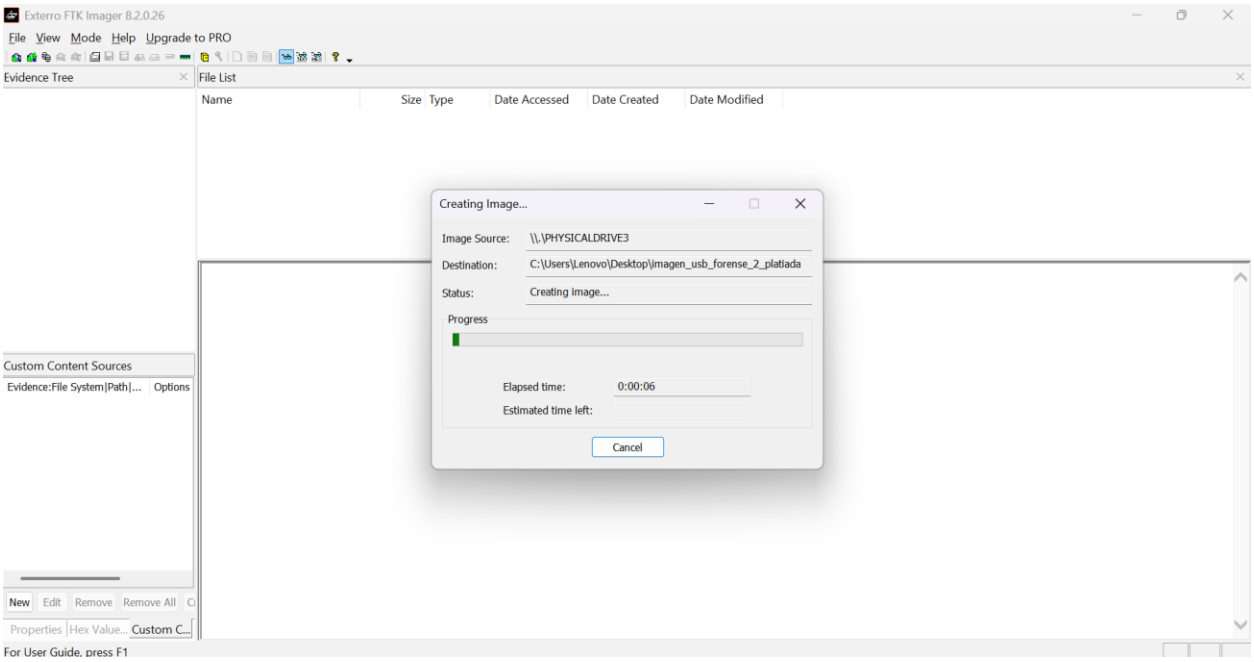


Ilustración 69. Proceso de creación de la imagen

Paso 3

En esta ventana de FTK Imager se muestran los resultados de la verificación de la imagen forense. Los valores hash MD5 y SHA1 calculados coinciden con los registrados en el reporte, confirmando la integridad de la evidencia y que no existen bloques dañados en la imagen generada.

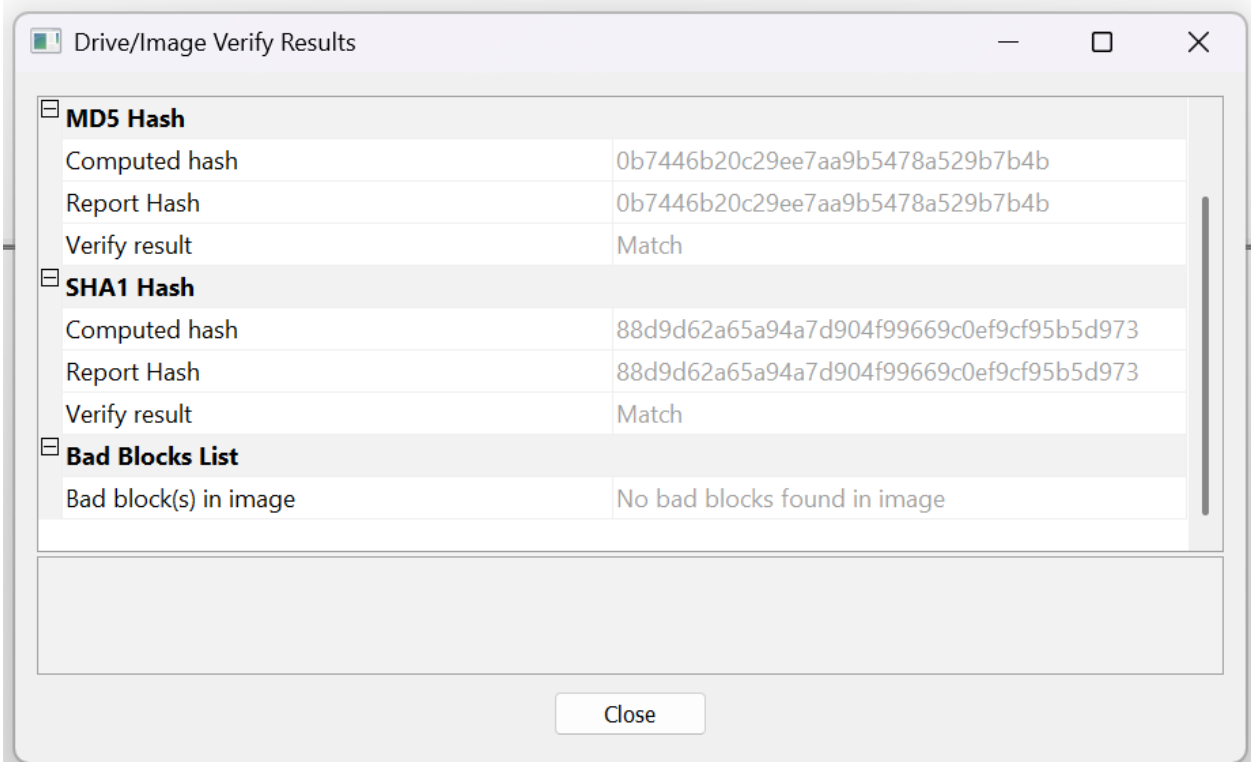


Ilustración 70. Verificación de integridad de imagen forense

Se observa la comparación de los valores hash SHA1 generados tanto en Kali Linux como en FTK Imager. Los resultados coinciden exactamente, garantizando la autenticidad de la imagen forense y validando que no hubo alteraciones durante el proceso de adquisición de la evidencia digital.

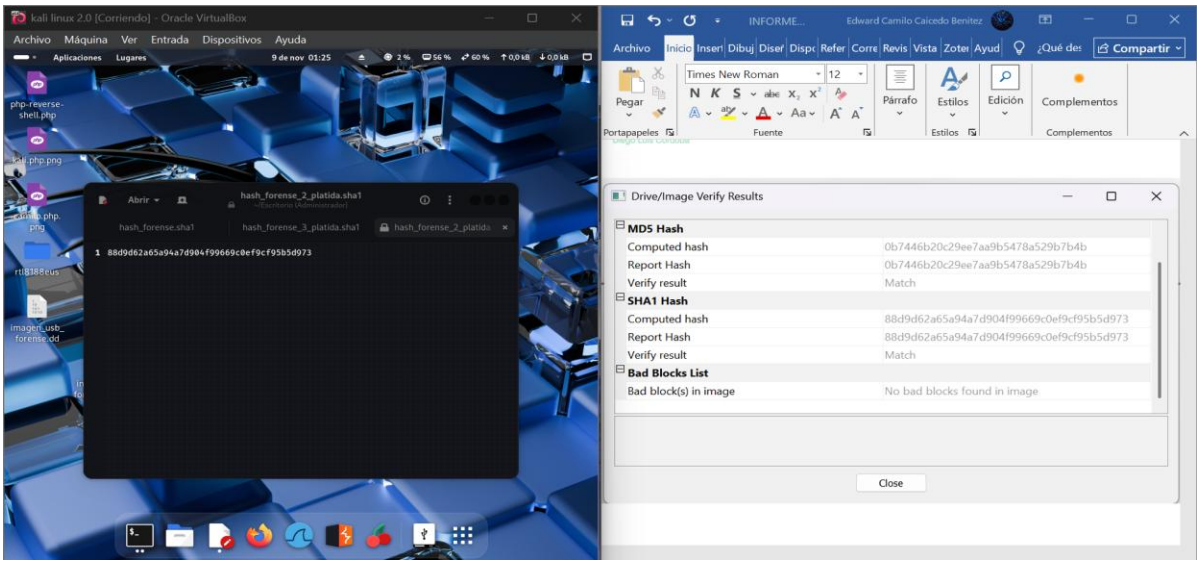


Ilustración 71. Comparación de hash entre Kali Linux y FTK Imager

PUNTOS DESTACADOS DEL INFORME

- Aplicación exitosa de técnicas de duplicación forense y verificación de integridad con hash SHA1 y MD5.
- Implementación de análisis comparativo entre entornos Linux y Windows con herramientas especializadas (Autopsy y FTK Imager).
- Detección de alteraciones en los valores hash iniciales debido a modificaciones en los archivos del dispositivo, lo que permitió evidenciar la importancia de repetir el proceso bajo condiciones controladas.
- Verificación final exitosa de integridad al obtener coincidencia entre los valores hash del dispositivo original y su imagen forense.
- Comprensión práctica del flujo completo de un proceso forense: adquisición, preservación, análisis y validación de evidencias.

CONCLUSIÓN

La práctica permitió comprender de manera integral los principios fundamentales del **análisis forense digital**, especialmente la relevancia de la integridad de la evidencia y la trazabilidad de los procesos. El uso combinado de **Kali Linux, Autopsy y FTK Imager** demostró la eficacia de las herramientas forenses en la identificación, preservación y análisis de datos digitales.

El cálculo y comparación de los valores hash garantizaron la **autenticidad de las copias forenses**, reforzando el principio de no alteración de la evidencia. Además, la práctica resaltó la necesidad de realizar procesos repetidos y controlados para descartar errores humanos o técnicos. En conclusión, el ejercicio fortaleció habilidades técnicas en auditoría y seguridad digital, consolidando conocimientos clave para la aplicación de metodologías forenses en entornos virtuales y reales.

REFERENCIA BIBLIOGRÁFICA

Ingeniero Rafael Sandoval

Castro, G. [@GabrielCastro-py4uw]. (s/f). *Como hacer una imagen forense de una USB usando FTK Imager* [[Object Object]]. Youtube. de https://www.youtube.com/watch?v=Wh2KeqirTX4

Plus, R. [@RedesPlus]. (s/f). *@Primeros pasos con FTK IMAGER Análisis Forense Digital* [[Object Object]]. Youtube, de https://www.youtube.com/watch?v=6OUQcL_8XXA&t=550s

TecnoSender [@TecnoSender]. (s/f). *cómo instalar FTK imager en windows | herramienta forense Paso a Paso* [[Object Object]]. Youtube. de https://www.youtube.com/watch?v=W8SiveR2Pt0

íTecnoCode [@iTecnoCode]. (s/f). *¿Cómo descargar e instalar Autopsy en Windows?* [[Object Object]]. Youtube. de https://www.youtube.com/watch?v=P6SUJpzsDLM

FTK Imager - forensic data imaging and preview solution. (2023, agosto 21). Exterro; Daylight. https://www.exterro.com/digital-forensics-software/ftk-imager

(S/f). Autopsy.com. de https://www.autopsy.com/download/