INFORME DE PRÁCTICA SOBRE ANÁLISIS FORENSE DE UNIDADES USB MEDIANTE AUTOPSY EN KALI LINUX Y WINDOWS, COMPLEMENTADO CON EL USO DE FTK IMAGER

VICTOR MANUEL LONGA MENA

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"

FACULTAD DE INGENIERÍA

INGENIERIA DE TELECOMUNICACIONES

2720409: SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCO (COLOMBIA)

2025

INFORME DE PRÁCTICA SOBRE ANÁLISIS FORENSE DE UNIDADES USB MEDIANTE AUTOPSY EN KALI LINUX Y WINDOWS, COMPLEMENTADO CON EL USO DE FTK IMAGER

VICTOR MANUEL LONGA MENA

Estudiantes, IX semestre

ING. RAFAEL S MORALES

Docente de la asignatura

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"

FACULTAD DE INGENIERÍA

INGENIERIA DE TELECOMUNICACIONES

2720409: SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCO (COLOMBIA)

2025

Contenido

Tabla de Figuras

Introducción

El presente informe muestra de manera detallada el procedimiento para realizar un análisis forense a una memoria USB empleando herramientas especializadas que permiten examinar su contenido sin alterar la información original. Para ello, se trabajó con dos aplicaciones ampliamente reconocidas en el ámbito de la informática forense: Autopsy, ejecutado en el sistema operativo Kali Linux, y FTK Imager, utilizado en un entorno Windows.

El objetivo principal de este proceso fue mostrar cómo es posible examinar, recuperar y preservar datos almacenados en una unidad USB, incluyendo archivos que hayan sido eliminados previamente por el usuario. Con Autopsy se efectuó el análisis profundo del dispositivo, permitiendo visualizar estructuras internas, identificar evidencia digital, y recuperar información borrada. Por otro lado, FTK Imager se utilizó para crear una imagen forense, es decir, una copia exacta y verificable del contenido de la memoria USB, garantizando que la investigación se realice sobre la copia y no sobre el dispositivo original.

Todo el procedimiento se desarrolló siguiendo buenas prácticas forenses, asegurando que los datos no fueran modificados en ningún momento. Esto implica trabajar de forma meticulosa y controlada, como lo haría un perito digital en un caso real, donde cada archivo, metadato o rastro presente en la USB podría constituir evidencia relevante dentro de una investigación formal.

Alcance

Este informe abarca el desarrollo completo de un proceso de análisis forense aplicado a una memoria USB, utilizando múltiples herramientas y sistemas operativos para garantizar una comprensión integral de las técnicas empleadas en la adquisición, preservación y examen de evidencia digital. El trabajo cubre desde la correcta configuración del entorno en Kali Linux y Windows, hasta la creación, verificación y análisis de una imagen forense, aplicando metodologías reconocidas en el ámbito de la informática forense.

1. Objetivos

1.1.General

Realizar un análisis forense completo de una memoria USB utilizando las herramientas Autopsy y FTK Imager, con el fin de identificar, extraer y documentar evidencia digital relevante de acuerdo con buenas prácticas de informática forense.

1.2.Específicos

- Configurar y crear un caso forense en Autopsy, estableciendo adecuadamente los parámetros iniciales como nombre del caso, descripción e investigadores, para garantizar una correcta gestión y trazabilidad del análisis.
- Adquirir y cargar la imagen forense del dispositivo USB mediante FTK Imager y posteriormente incorporarla en Autopsy, asegurando la integridad de los datos mediante el uso de hash y técnicas correctas de duplicación.
- Analizar el contenido estructural y lógico del dispositivo USB, identificando archivos visibles, ocultos, eliminados o recuperables, así como posibles indicios relevantes para el caso.
- Documentar los hallazgos obtenidos durante todo el proceso de análisis, elaborando un informe técnico que integre evidencias, capturas, procedimientos desarrollados, dificultades encontradas y conclusiones fundamentadas.

2. Planteamiento Del Problema

La información digital se ha convertido en uno de los recursos más valiosos para el mundo en general, se puede decir que el volumen de datos que movemos o almacenamos ya sea en la nube o por medios físicos como pueden ser memorias USB es gigantesco, esto hace que el manejo adecuado de los datos adquiere una importancia crítica. El uso cotidiano de dispositivos portátiles de almacenamiento, como las memorias USB, facilita la transferencia de archivos, pero también incrementa significativamente los riesgos asociados a la pérdida, alteración o eliminación intencional o accidental de información relevante. Esta vulnerabilidad convierte a las unidades USB en elementos que con frecuencia deben ser sometidos a procesos de análisis forense digital dentro de investigaciones académicas, corporativas o incluso judiciales.

Aunque existen herramientas avanzadas para realizar análisis forense, como Autopsy y FTK Imager, su uso adecuado requiere de conocimientos técnicos que muchos estudiantes o principiantes en el campo de la informática forense aún no dominan. La falta de comprensión sobre conceptos fundamentales como la creación de una imagen forense, la preservación de la integridad del dispositivo, la recuperación de archivos eliminados o el análisis de metadatos puede generar errores que comprometan la validez de la evidencia digital. En escenarios reales, una mala práctica podría provocar la alteración de datos importantes, afectando la confiabilidad del análisis y la utilidad de la información recolectada como posible prueba.

En el ámbito educativo, este problema se hace aún más evidente. Aunque se enseñan los fundamentos teóricos de la informática forense, no siempre existe una guía clara, práctica y estructurada que permita a los estudiantes ejecutar un proceso de análisis completo y metodológicamente correcto sobre un dispositivo de almacenamiento. La ausencia de procedimientos detallados dificulta la comprensión de las etapas esenciales del análisis forense,

como la adquisición de evidencia, la verificación de integridad, la exploración del sistema de archivos y la documentación de los hallazgos.

Esta situación genera la necesidad de contar con un material que explique de manera clara cómo llevar a cabo el análisis forense de una memoria USB utilizando herramientas profesionales y entornos controlados. Por lo tanto, el presente trabajo surge como respuesta a dicha necesidad, proponiendo una guía detallada del proceso, desde la creación de la imagen forense con FTK Imager hasta el análisis profundo de la evidencia con Autopsy en Kali Linux, replicando un escenario realista pero seguro para el aprendizaje. El objetivo es proporcionar un recurso que permita fortalecer las competencias prácticas, mejorar la comprensión de los procedimientos forenses y asegurar que el análisis de evidencia digital se realice siguiendo estándares técnicos aceptados en el campo.

3. Capítulo 1: Análisis Forense Utilizando Autopsy en Kali Linux

3.1. Configuración de Filtros USB.

Lo primero que debemos hacer antes de realizar nuestro análisis forense es conectar nuestra memoria USB y que se reconocible por nuestro pc físico. Para eso lo único que debemos hacer es conectar nuestra memoria e irla a buscar en el apartado de equipos.

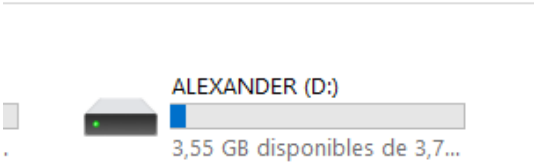


Figura 1. Revisamos que nuestro computador lea la memoria USB

Lo siguiente que hacemos es crear el filtro USB para ello nos vamos a configuración dentro de configuración ingresamos al apartado USB y te dentro de este apartado le damos en el botón de más que no permite agregar los dispositivos detectados por nuestro PC para este caso seleccionamos el general uDisk(0100) que sería nuestra memoria USB.

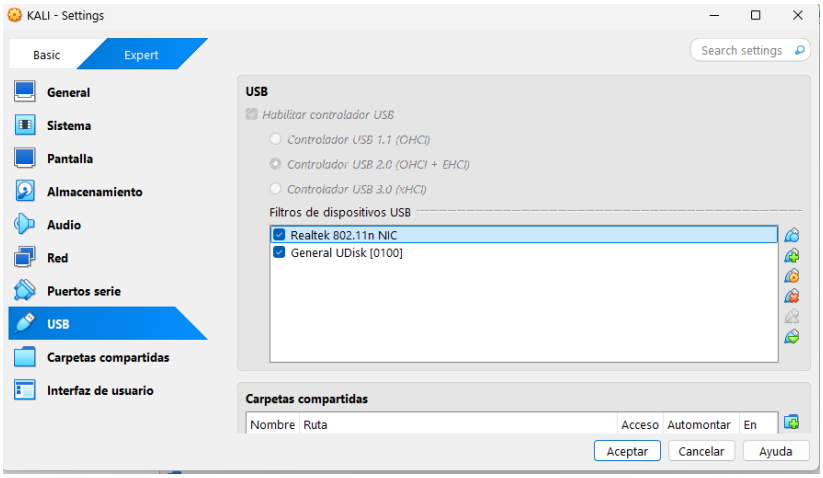


Figura 2. Configuración de Dispositivos USB

Por último, dentro de nuestra máquina virtual de Kali Linux Ingresamos a la opción de dispositivos luego de nuevo al apartado USB y seleccionamos hoy muéstrame mi memoria qué sería la general mass storage (0100)

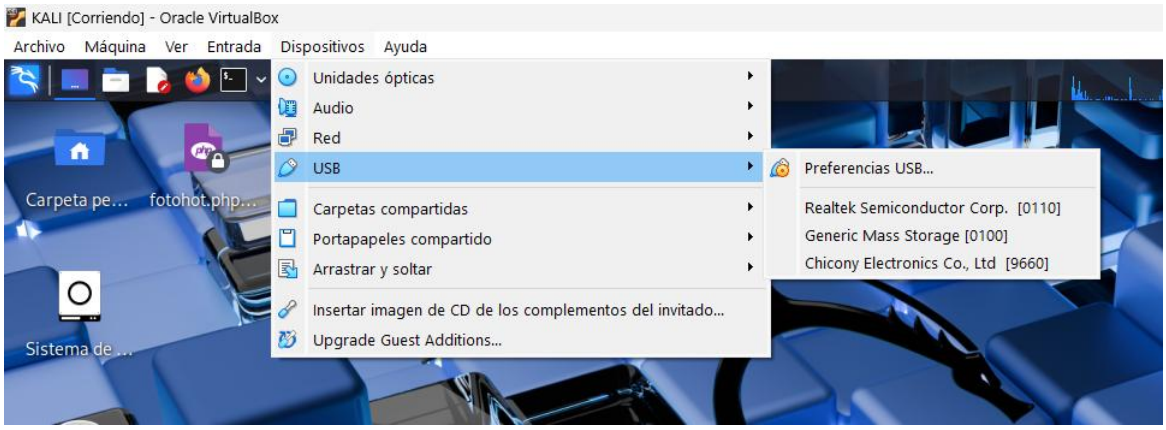


Figura 3. Selección de la USB Desde Kali

3.2.Revisión de la detección del dispositivo

Utilizando el comando **Sudo fdisk -l** Podremos revisar que efectivamente nuestra Memoria USB b ya es detectable en desde nuestro Kali Linux

```
┌──(root㉿kali)-[/home/kali]
└─# sudo fdisk -l

Disk /dev/sda: 25 GiB, 26843545600 bytes, 52428800 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×324ca099

Device     Boot    Start      End  Sectors  Size Id Type
/dev/sda1  *        2048 49641471 49639424 23,7G 83 Linux
/dev/sda2       49643518 52426751  2783234  1,3G  f W95 Ext'd (LBA)
/dev/sda5       49643520 52426751  2783232  1,3G 82 Linux swap / Solaris


Disk /dev/sdb: 3,75 GiB, 4027580416 bytes, 7866368 sectors
Disk model: Flash Disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0×38c258ae

Device     Boot Start     End Sectors  Size Id Type
/dev/sdb1          544 7866367 7865824  3,8G  c W95 FAT32 (LBA)

┌──(root㉿kali)-[/home/kali]
└─#
```

Figura 4. Identificación de Dispositivos

Para identificar los dispositivos de almacenamiento conectados al sistema, primero accedí al modo privilegiado usando **sudo su** e ingresando mi contraseña en la consola. Luego, pude verificar la presencia del disco principal **/dev/sda** y de la unidad USB **/dev/sdb** (una memoria de 3.75 GB), la cual corresponde al dispositivo que será analizado en el proceso forense.

3.3.Creación de Hash SHA1

Figura 5. Generación de Hash de la Memoria USB

Para generar el hash, utilizamos el algoritmo **SHA-1** mediante el comando sha1sum aplicado directamente sobre el dispositivo USB **/dev/sdb**. Este proceso produce un valor hash único (SHA-1), el cual fue redirigido y guardado en con el nombre **hash_forense.sha1**, ubicado en el Escritorio de Kali Linux.

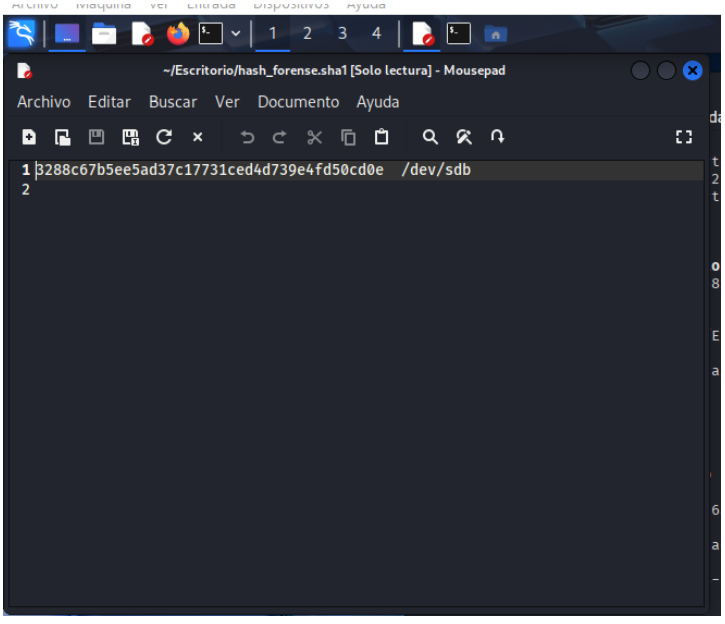


Figura 6. Hash generado.

En análisis forense digital, generar un hash criptográfico es importante ya que permite garantizar la integridad de la evidencia. El hash funciona como una "huella digital" del dispositivo o archivo: si su contenido cambia, aunque sea mínimamente, el hash resultante también cambiará. Esto permite demostrar que la evidencia no ha sido alterada durante el análisis, manteniendo así su validez legal y técnica.

3.4. Generamos la Imagen de la USB

Figura 7. Creación de Imagen USB

Para finalizar, se empleó el **comando dd if=/dev/sdb of=/home/kali/Escritorio/imagen_usb_forense.dd conv=noerror,sync** en Kali Linux con el fin de generar una imagen forense bit a bit del dispositivo USB identificado como /dev/sdb. En el comando se define como entrada (if) el dispositivo USB y como salida (of) el archivo imagen_usb_forense.dd, el cual se almacena en el Escritorio.

Además, se agregaron los parámetros conv=noerror,sync, que permiten que el proceso continúe aun cuando se presenten sectores defectuosos, garantizando así que la copia se realice de forma íntegra y sin interrupciones.

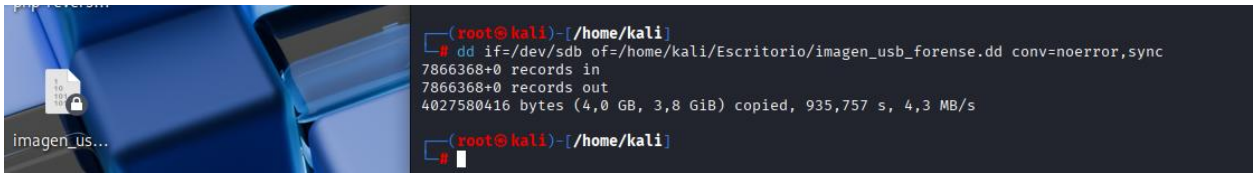


Figura 8. Finalización de la Creación de la Imagen USB

Aquí se muestra la finalización exitosa del proceso de creación de la imagen forense de la memoria USB. Se evidencia que se copiaron 7,866,368 bloques, equivalentes a 4.0 GB (3.8 GiB) de información, lo cual confirma que se obtuvo una copia completa y exacta del dispositivo.

3.5. Hacemos la comparación del Hash Original e Imagen USB

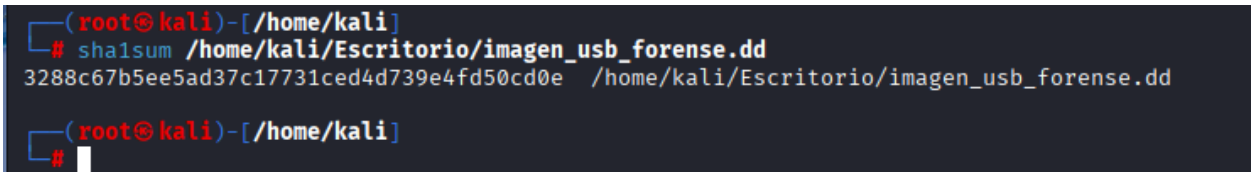


Figura 9. Verificación de la Imagen USB

Después de generar la imagen forense de la memoria USB, procedimos a calcular nuevamente el hash SHA1, esta vez aplicado directamente al archivo **imagen_usb_forense.dd** para verificar la integridad de la copia creada. Para ello utilizamos el comando:

sha1sum /home/kali/Escritorio/imagen_usb_forense.dd

El comando generó el valor hash **3288c67b5ee5ad37c17731ced4d739e4fd50cd0e**, correspondiente a la imagen forense. Este resultado confirma que la copia se realizó correctamente, manteniendo la integridad de los datos tal como se encontraban en el dispositivo original.

3.6.Asignación de Permisos

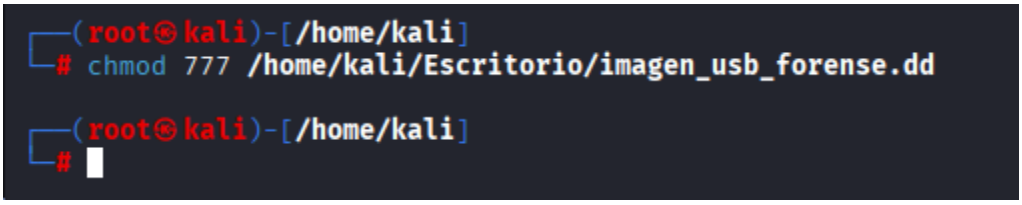


Figura 10. Configuración de Permisos de la Imagen

Luego ejecutamos el comando **chmod 777** aplicado al archivo **imagen_usb_forense.dd** ubicado en el Escritorio de Kali Linux. Con este comando se asignan permisos de **lectura, escritura y ejecución** para el propietario, el grupo y todos los demás usuarios, permitiendo así **acceso completo** al archivo de la imagen forense.

3.7.Ingresamos a Autopsy

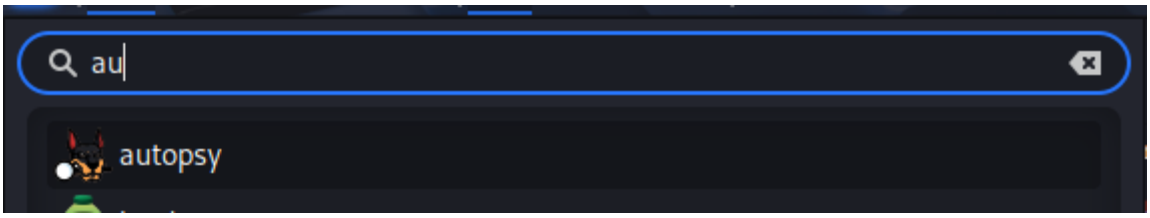


Figura 11. Aplicación Autopsy

Esta imagen muestra como ingresamos a Autopsy en el entorno de Kali Linux, aquí es donde aremos nuestra auditoria forense.

3.8. Servicios de Autopsy Iniciado

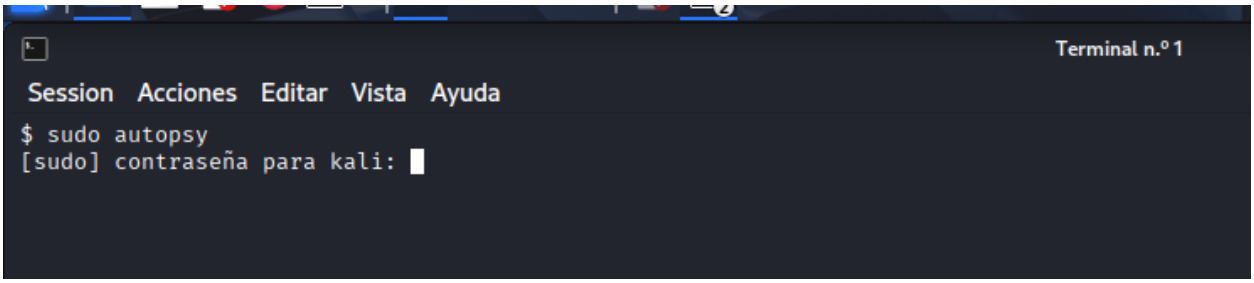


Figura 12. Nos logueamos en autopsy

Luego de ingresar a autopsy lo primero que hacemos es loquearme para esto ingresamos nuestra contraseña de kali

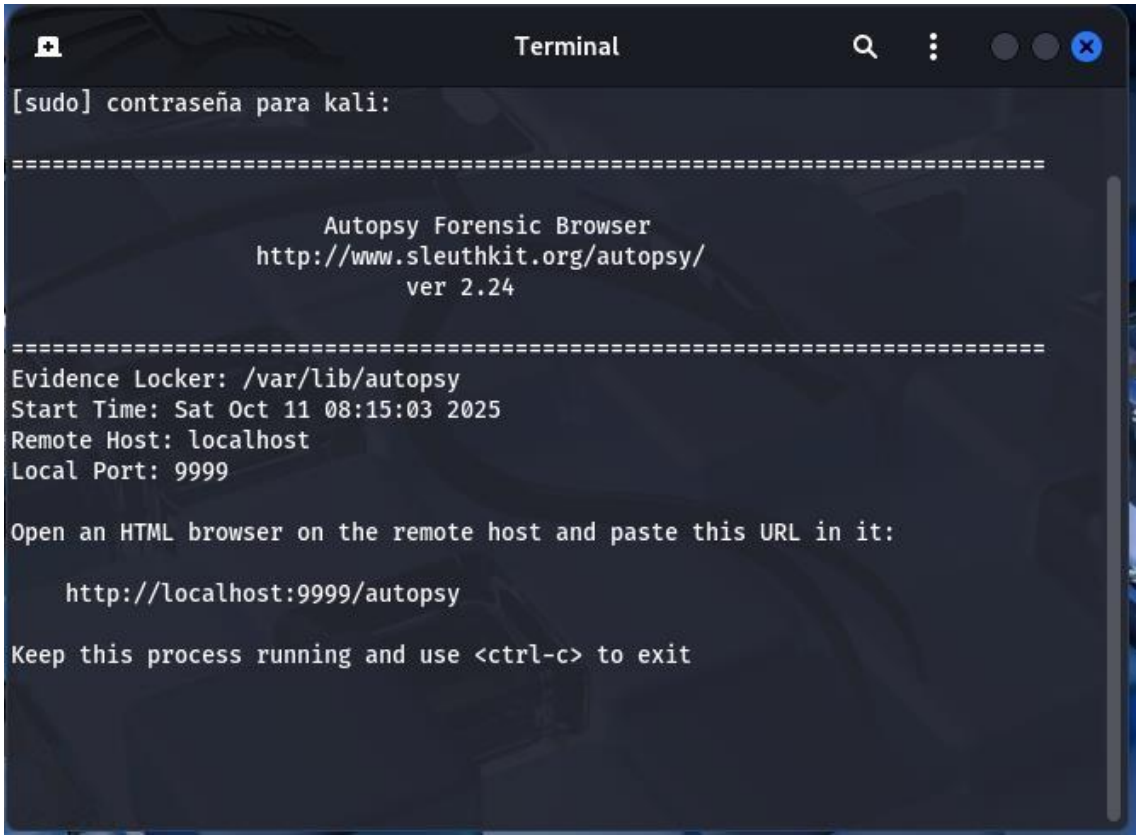


Figura 13. Inicialización del Servicio Web de Autopsy

Después de ejecutaremos Autopsy lo que hiciste aquí fue levantar el servidor local de Autopsy para poder analizar la imagen forense desde un navegador web. Es el paso previo antes de crear un caso y cargar la imagen imagen_usb_forense.dd

3.9.Página de Inicio de Autopsy

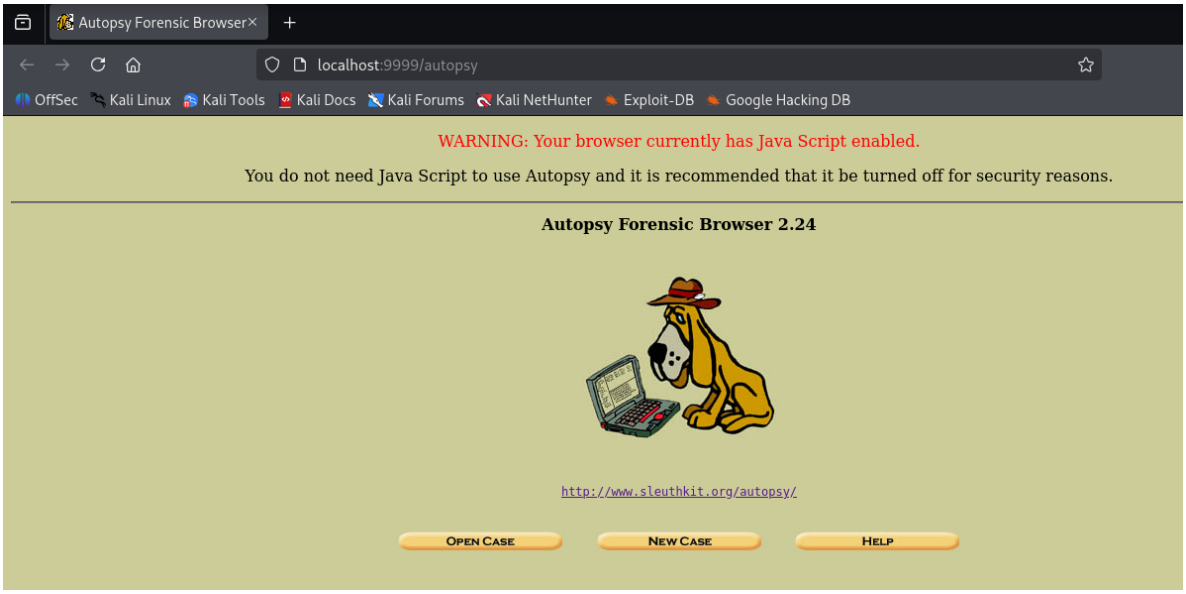


Figura 14. Interfaz Principal de Autopsy

Luego de iniciar el servidor de Autopsy en la terminal, accedimos a la interfaz web a través de la URL proporcionada. Desde esta pantalla principal seleccionamos la opción “Nuevo Caso (New Case)” para comenzar la creación del caso forense, lo cual nos permitirá posteriormente cargar y analizar la imagen forense de la memoria USB.

3.10. Formulario de *Configuración de Caso Nuevo*

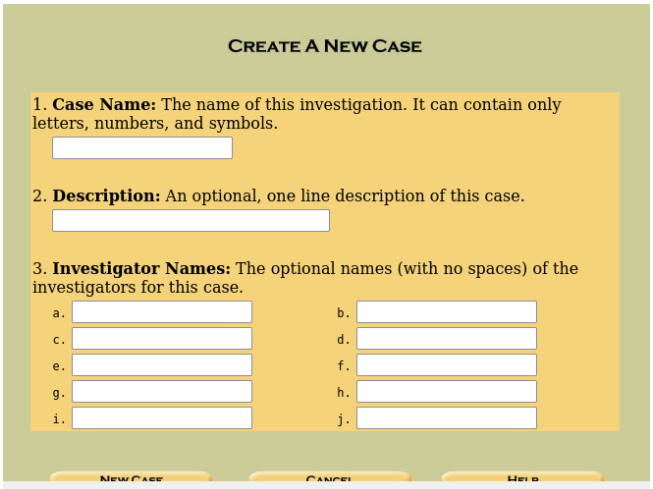


Figura 15. Formulario para crear un caso nuevo

Esta imagen muestra el formulario utilizado para crear un nuevo caso forense en Autopsy. En esta sección se diligencian los datos básicos del caso, tal como se explicó en clase. Primero se asigna un nombre al caso (permitiendo únicamente letras, números y símbolos). Luego se incluye una descripción opcional, en este caso “Análisis forense USB”. Finalmente, se ingresan los nombres del investigador o de los integrantes encargados del análisis. Con esta información se completa la configuración inicial del caso.

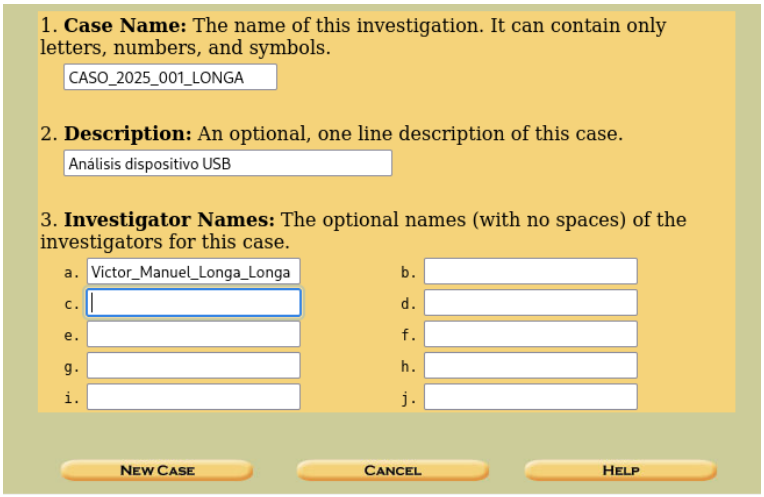


Figura 16. Creamos un caso nuevo a partir del formulario

3.11. Caso Creado Exitosamente en Autopsy

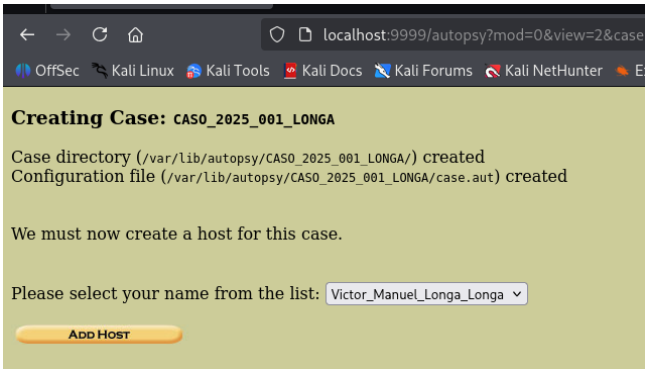


Figura 17. Confirmación de Creación del Caso Forense

Esta imagen confirma la creación exitosa del caso forense "CASO_2025_001_LONGA" en Autopsy. El sistema ha generado automáticamente el directorio del caso en /var/lib/autopsy/

CASO_2025_001_LONGA y el archivo de configuración core.au. El mensaje indica que el siguiente paso es crear un "host" para este caso, que representará el dispositivo o sistema bajo investigación.

3.12. Parámetros Opcionales de Configuración

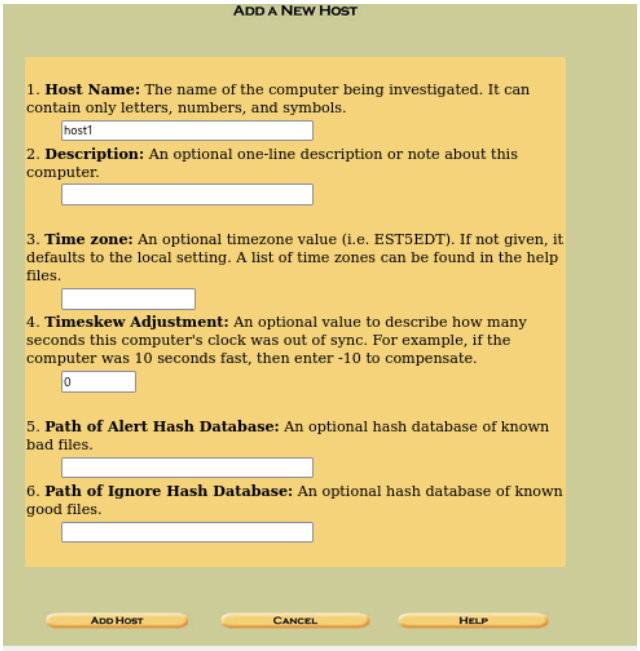


Figura 18. Configuración Avanzada del Host

Esta imagen muestra los parámetros avanzados opcionales para la configuración del host en Autopsy. Incluye la zona horaria, rutas de bases de datos de hashes: una para archivos "maliciosos" conocidos (Alert Hash Database) y otra para archivos "confiables" (Ignore Hash Database).

3.13. Interfaz de Host Listo para Importar Imagen

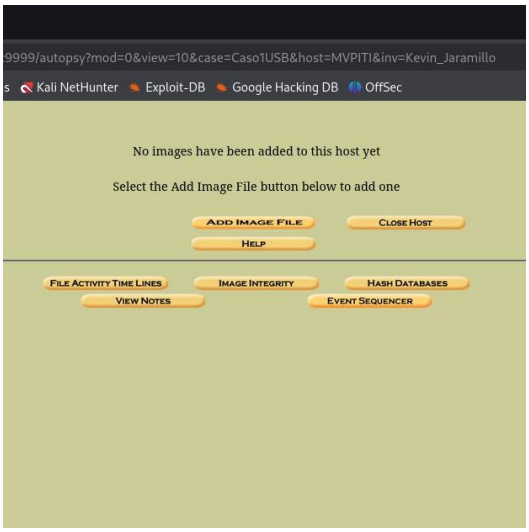


Figura 19. Host sin Imagen

Pantalla de Autopsy mostrando el host "MVPTI" sin imágenes agregadas. Indica que se debe seleccionar "Add Image File" para importar la imagen forense de la memoria USB y comenzar el análisis.

3.14. Formulario para Agregar Imagen Forense al Host

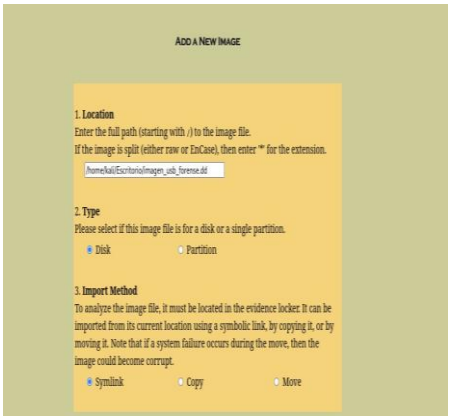


Figura 20. Configuración de Importación de Imagen

Pantalla de Autopsy para importar la imagen forense. Muestra tres configuraciones: ubicación de la imagen (/home/kali/Escritorio/imagen_usb_forense.dd), tipo (Disco o Partición) y método de importación (Enlace, Copiar o Mover). Permite cargar la imagen USB para análisis.

3.15. Configuración de Hash y Detección de Partición

Autopsy detecta automáticamente la partición FAT32 en la imagen y solicita calcular el hash MD5 para verificación. Muestra detalles técnicos de la partición y continuar la importación.

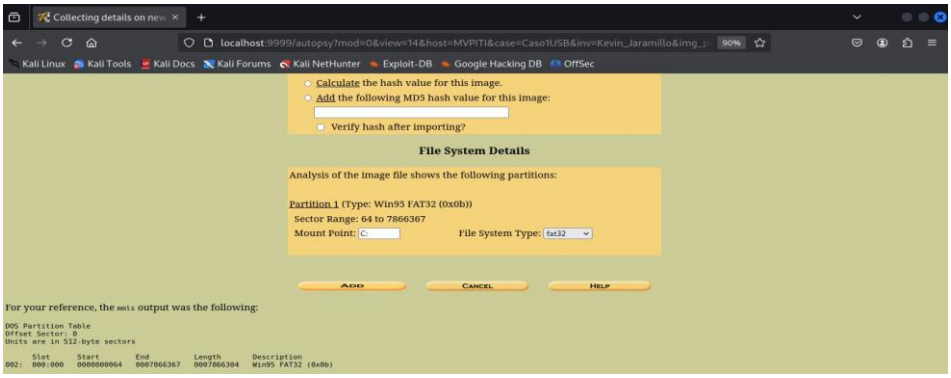


Figura 21. Detalles de Partición y Hash

3.16. Proceso de Importación de Imagen Completado

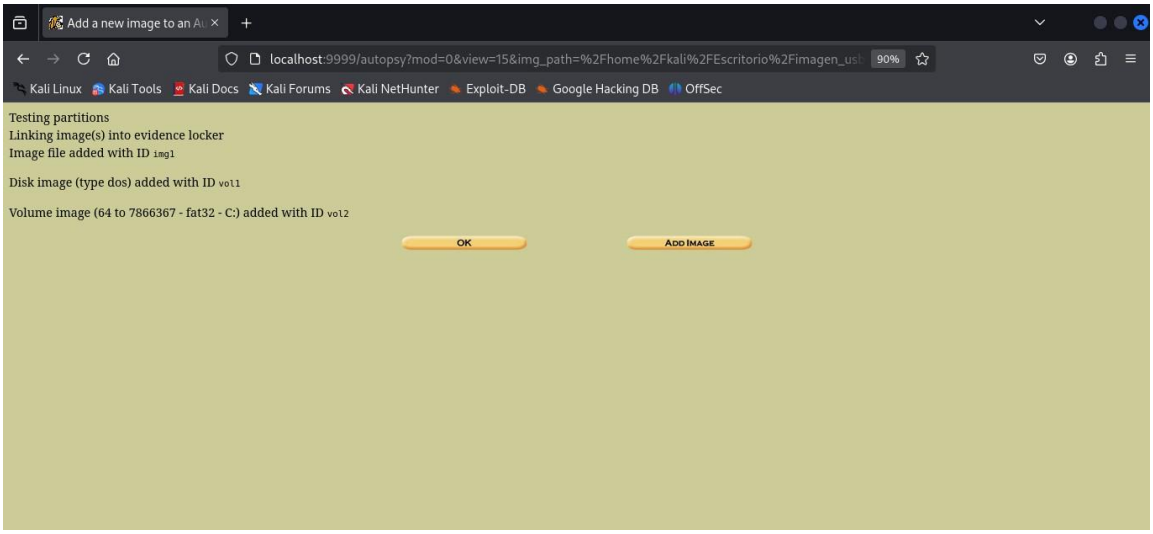


Figura 22. Imagen Importada Exitosamente

Confirmación de que la imagen forense se importó correctamente en Autopsy. El sistema asignó IDs únicos al disco y volumen FAT32 listos para el análisis.

3.17. Interfaz de Selección de Volumen

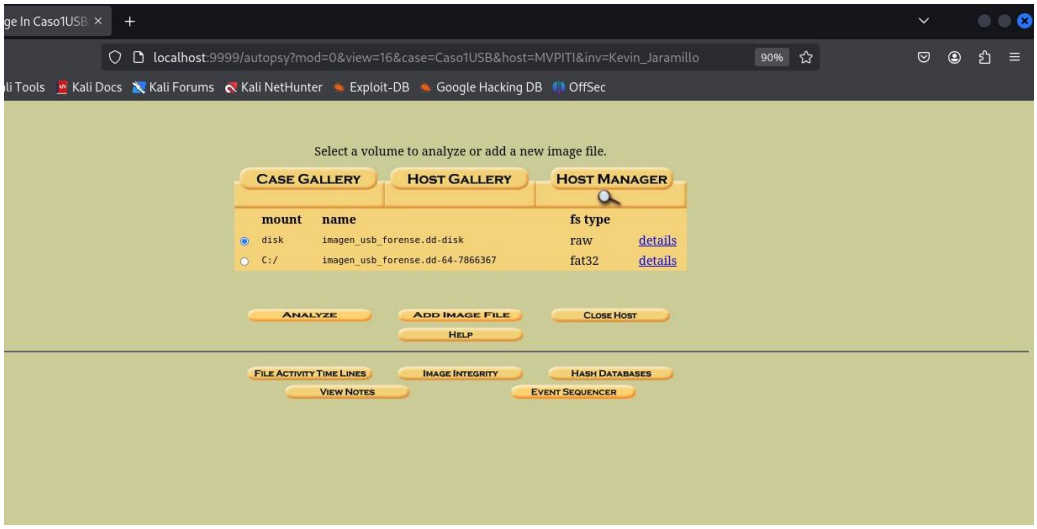


Figura 23. Volumen Listo para Análisis

Pantalla que muestra el volumen FAT32 (C:/) importado correctamente. Permite seleccionar el volumen para iniciar el análisis forense con herramientas como línea de tiempo, integridad de imagen y bases de datos de hash.

3.17.1 Opciones de Búsqueda y Navegación de Archivos

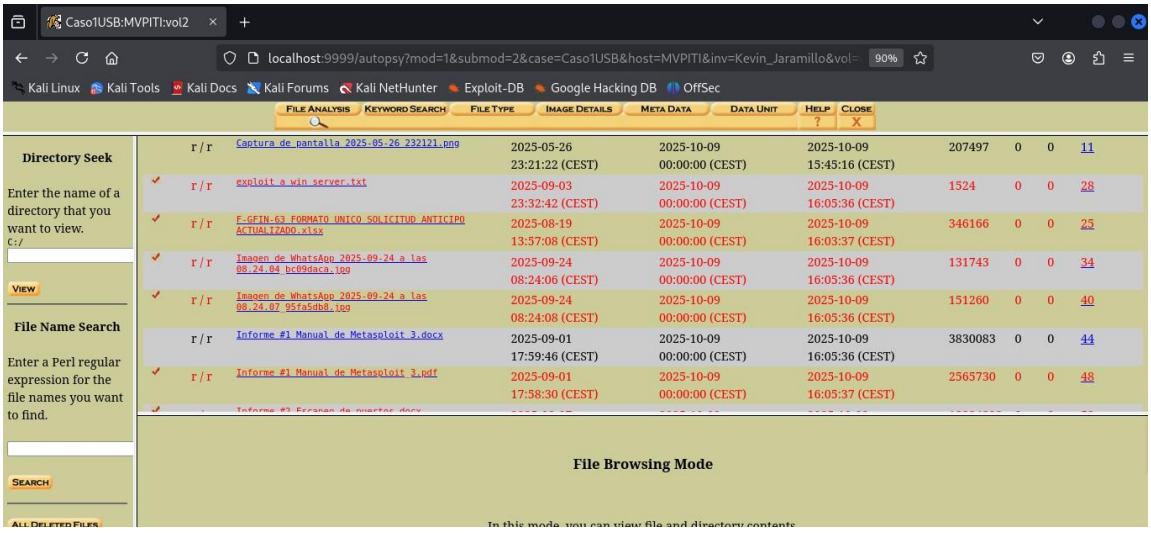


Figura 24.Herramientas de Búsqueda de Archivos

Interfaz de Autopsy con herramientas para buscar directorios específicos o archivos usando expresiones regulares, y modo de navegación para explorar el contenido de la imagen forense.

3.17.2 Proceso de Cálculo de Hash MD5 de la Imagen

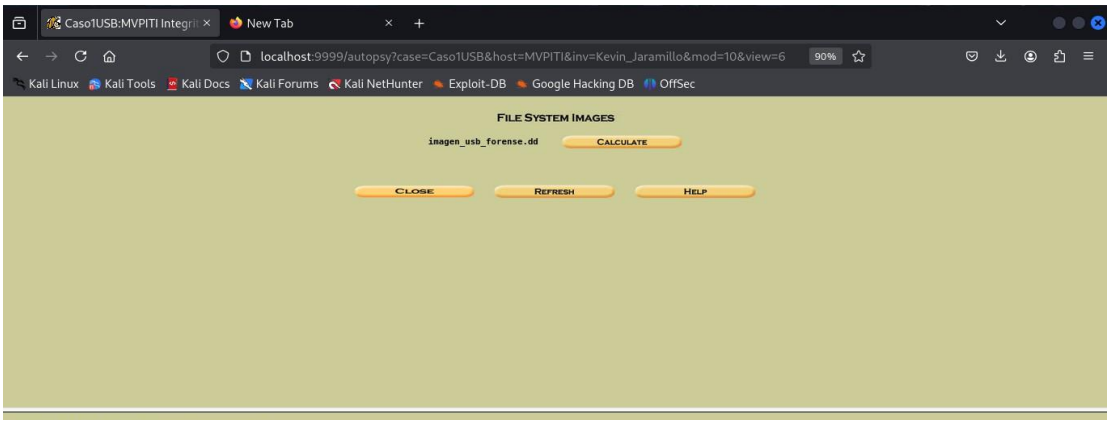


Figura 25. Cálculo de Hash MD5

Autopsy calculando el valor hash MD5 de la imagen forense para verificar su integridad durante el análisis.

4. Capítulo 2: Conducto Para Descargar Autopsy en Windows

Para poder hacer el proceso de auditoría forense con autopsy en Windows lo primero que debemos hacer es descargar el software necesario para poder trabajar en autopsy por ello lo que debemos hacer es lo siguiente.

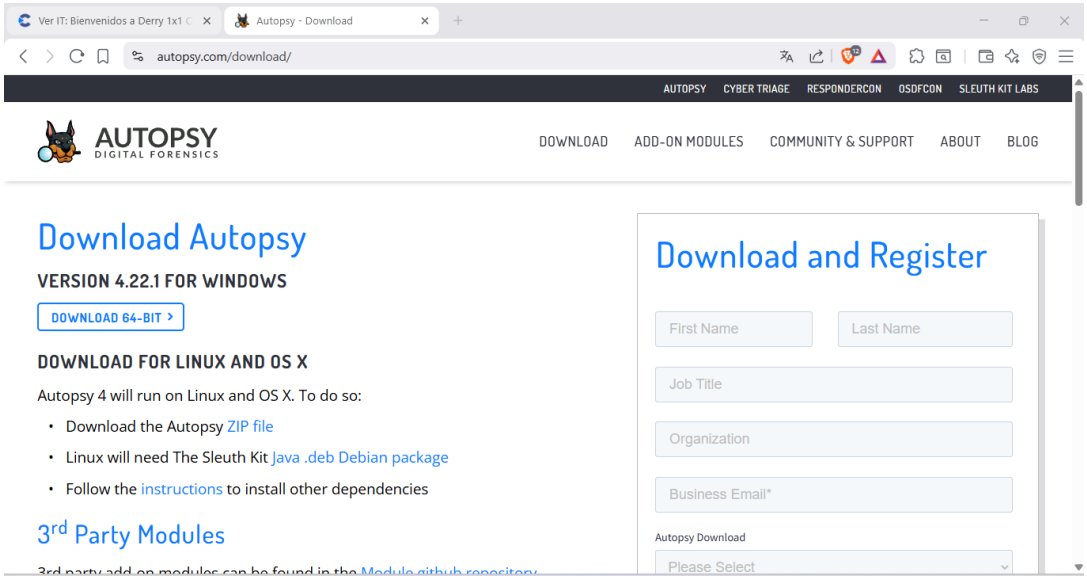


Figura 26. Página de Descarga de Autopsy

Primero nos dirigiremos a la página oficial de descarga de Autopsy https://www.autopsy.com/download/ , y luego descargamos la última versión disponible para Windows.

4.1.Procedemos a instalar Autopsy

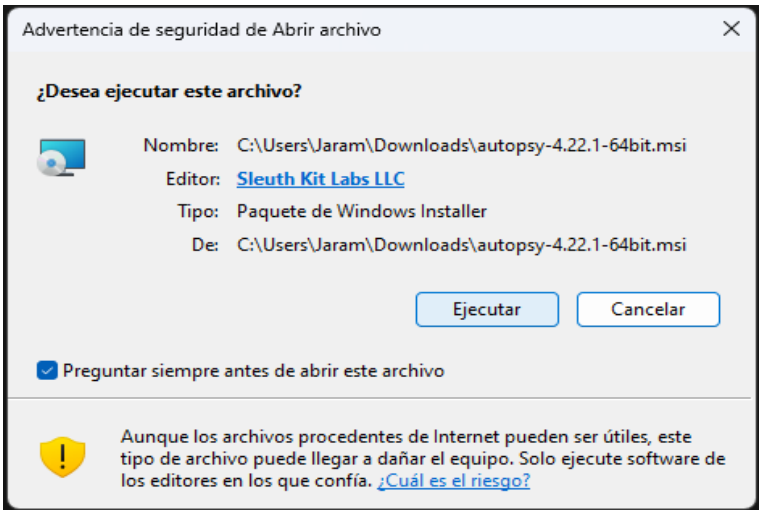


Figura 27. Procedemos a instalar autopsy

Luego que digamos descargado el archivo Para instalar autopsy procedemos h ejecutar lo que nos permitirá instalar el software necesario para poder realizar nuestra auditoría forense En Windows.

4.1.1 Inicio del Asistente de Instalación de Autopsy

Figura 28. Asistente de Instalación

Pantalla inicial del instalador de Autopsy para Windows. El asistente guiará al usuario con el proceso de instalación paso a paso.

4.1.2 Confirmación del entorno para Instalar Autopsy

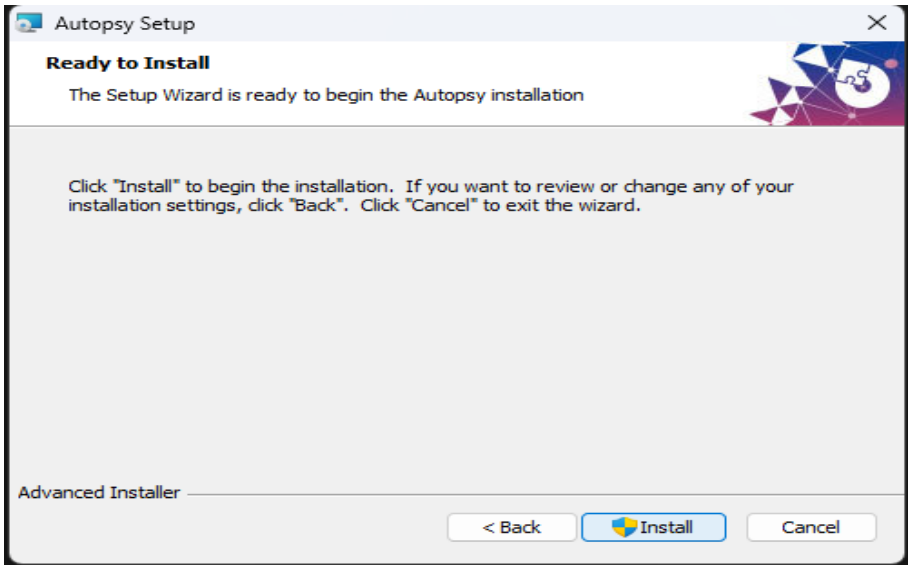


Figura 29. Confirmación de Instalación

Se muestra la confirmación del asistente confirmando que está listo para instalar Autopsy. Permite revisar configuraciones antes de iniciar la instalación definitiva.

4.1.3 Finalización Exitosa de la Instalación

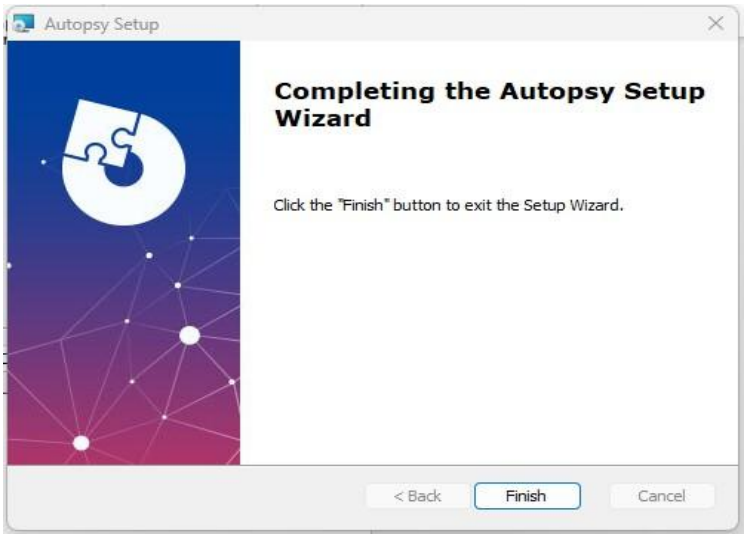
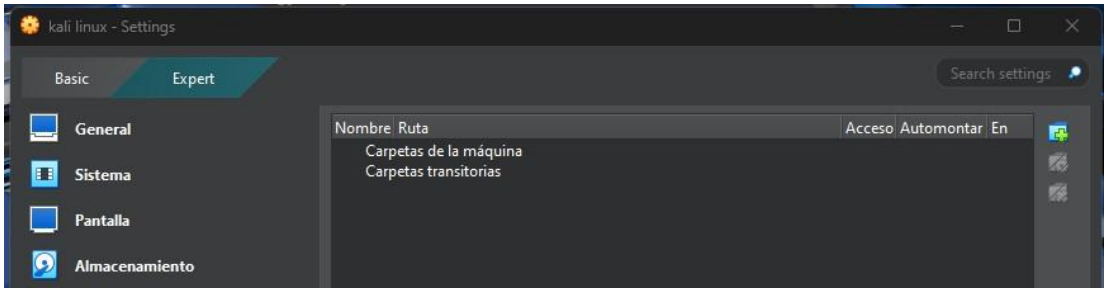


Figura 30. Instalación Completada del software

Finalmente, mostramos como se confirma la instalación exitosa de Autopsy. Al hacer clic en "Finish" se cierra el asistente y el programa queda listo para usar.

4.2.Configuración de Carpetas Compartidas



Para crear la carpeta compartida nos vamos a la pantalla de configuración de VirtualBox una vez aquí hacemos el mismo proceso que hicimos a la hora de crear la carpeta en Windows xp.

4.2.1 Creación de Carpeta en Windows

Figura 31. Configuración de Carpetas Compartidas

Figura 32. Creamos una Carpeta "Autopsy" Creada

Para crear la carpeta compartida seguimos el mismo proceso realizado al momento de crear la carpeta de Windows XP, la imagen anterior muestra al Explorador de Windows mostrando como se creó la carpeta Autopsy, creada dentro del directorio de SEGURIDAD Y AUDITORIA DE RED. Esta carpeta servirá para almacenar y organizar los archivos, incluyendo la imagen de la memoria USB.

4.2.2 Agregamos la Carpeta Compartida

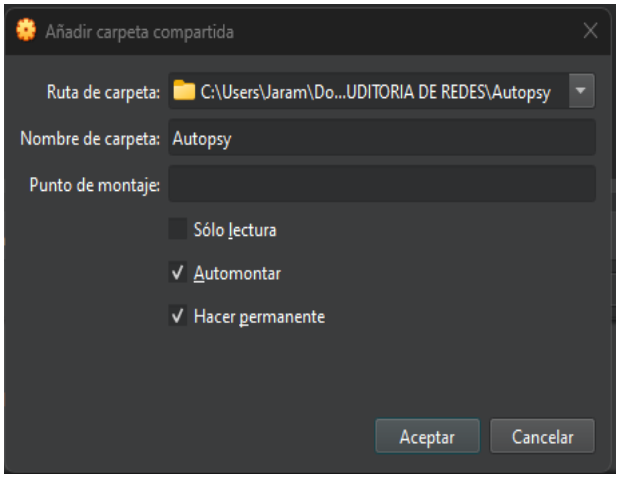


Figura 33.Configuración de Carpeta Compartida

Luego en esta ventana de VirtualBox para añadir la carpeta Autopsy como recurso compartido. Se configura con montaje automático y permanente para acceso continuo entre Windows y la máquina virtual.

4.2.3 Carpeta Autopsy Correctamente Compartida

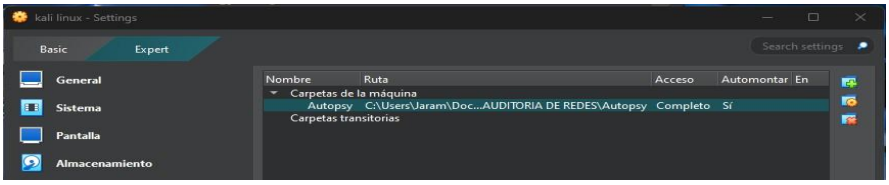


Figura 34. Carpeta Compartida Configurada

Configuración de VirtualBox mostrando la carpeta Autopsy ya agregada como recurso compartido con acceso completo y automontaje, permitiendo transferir archivos entre Windows y Kali Linux.

4.2.4 Transferimos los Archivos a la Carpeta Compartida

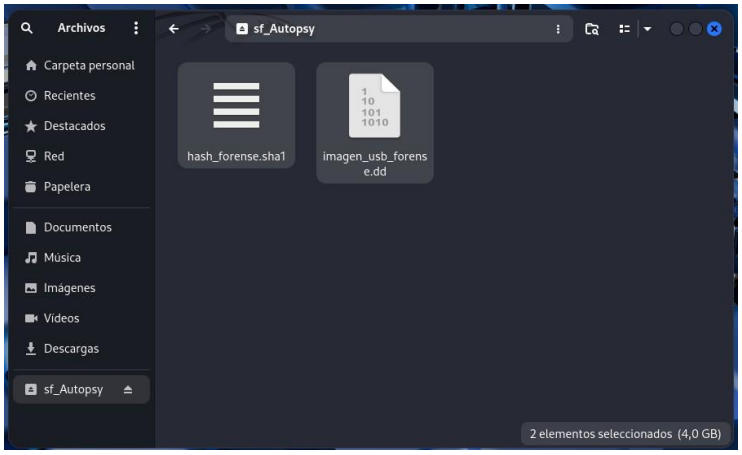


Figura 35. Archivos Transferidos a Windows

mostramos los dos archivos forenses transferidos desde Kali Linux: hash_forense.sha1 y imagen_usb_forense.dd, listos para ser analizados con Autopsy en Windows.

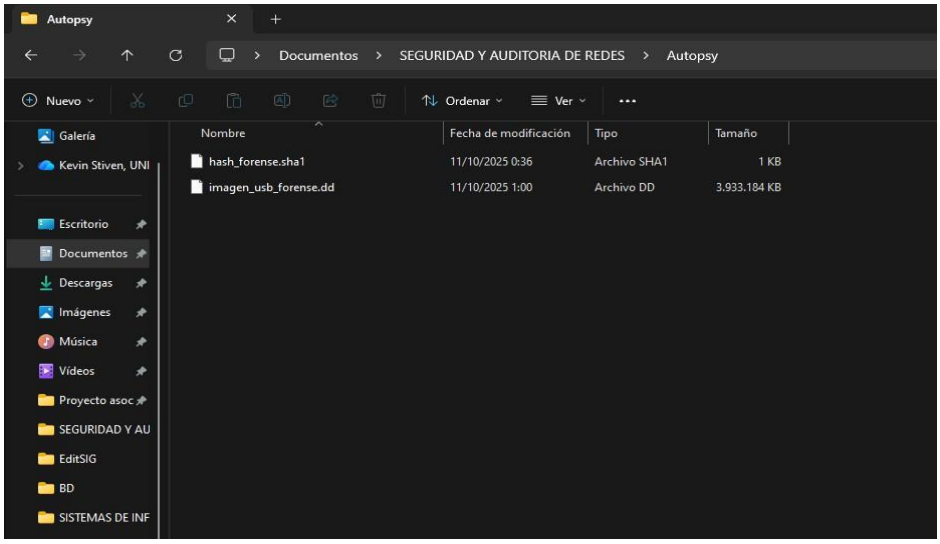


Figura 36. Archivos Forenses en Windows

Carpeta Autopsy en Windows mostrando los archivos forenses transferidos: el hash SHA1 de verificación y la imagen forense DD, listos para ser analizados con Autopsy en Windows.

4.3. Abrimos Autopsy en Windows

Figura 37. Interfaz Principal de Autopsy Windows

Interfaz gráfica de Autopsy en Windows mostrando las opciones para crear nuevo caso o abrir caso existente. Desde aquí se inicia el análisis forense de la imagen USB importada dándole en nuevo caso.

4.3.1 Creación del Caso nuevo caso

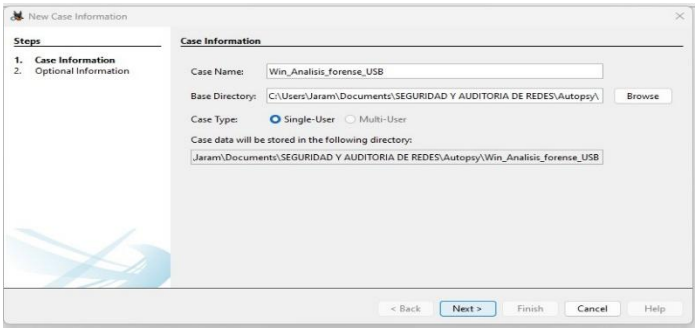


Figura 38. Configuración del Caso en Windows

Pantalla de Autopsy Windows para configurar el nuevo caso forense. Se define el nombre del caso y el directorio base donde se almacenarán todos los datos del análisis en la carpeta Autopsy.

4.3.2 Rellenamos los metadatos para Caso Forense

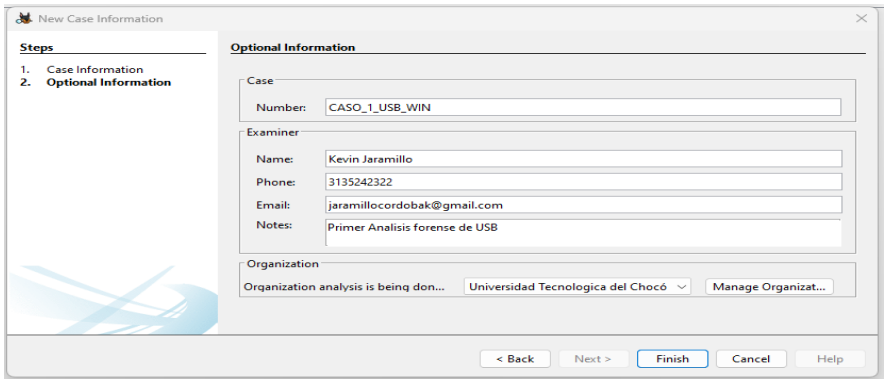


Figura 39.Información Adicional del Caso

Luego llenamos el formulario completado con información opcional del caso: número de caso, datos del analista (Kevin Jaramillo), contacto y notas descriptivas para documentación forense.

4.3.3 Configuración de Host

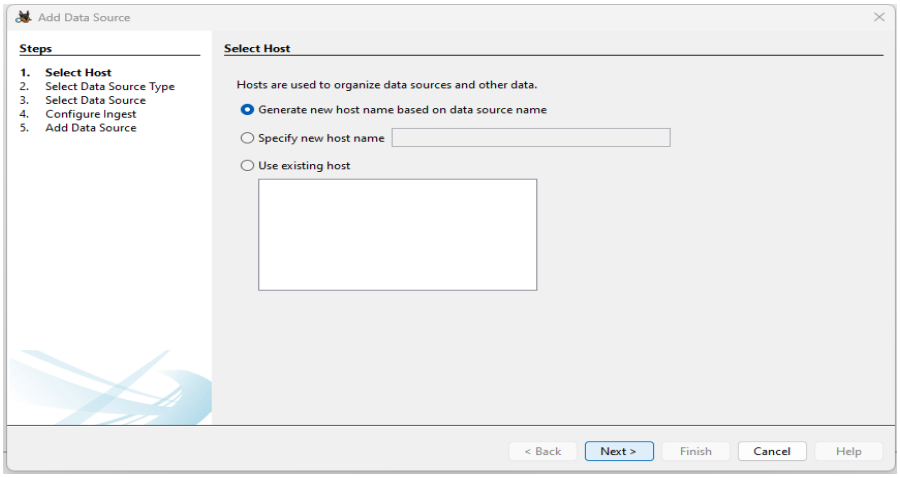


Figura 40. Selección de Host

Pantalla de Autopsy para definir el host que organizará la fuente de datos. Permite generar nombre automático, especificar uno nuevo o usar host existente para el análisis forense.

4.3.4 Selección de Tipo de Fuente de Datos

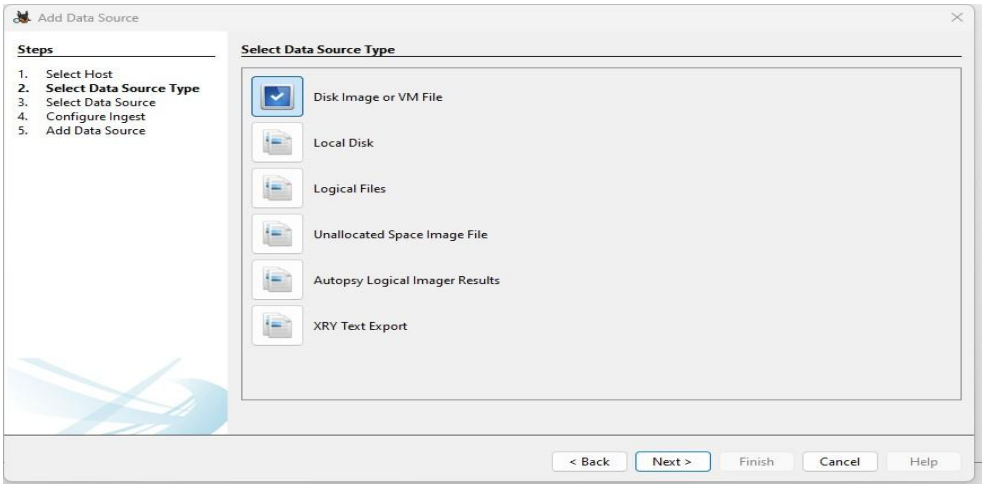


Figura 41. Tipo de Fuente de Datos

Además mostramos la pantalla para elegir el tipo de fuente de datos. Se selecciona Disk Image or VM File para cargar la imagen forense DD de la memoria USB en Autopsy.

4.3.5 Se Carga el Archivo de Imagen Forense .dd

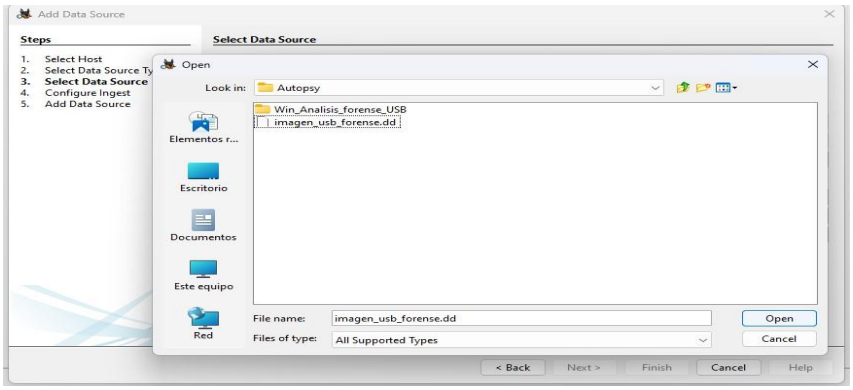


Figura 42. Selección de Imagen Forense

Luego lo que se hace es seleccionar la imagen forense imagen_usb_forense.dd desde la carpeta compartida, que será analizada como fuente principal del caso.

4.3.6 Selección de Parámetros de la Imagen y Hash de Verificación

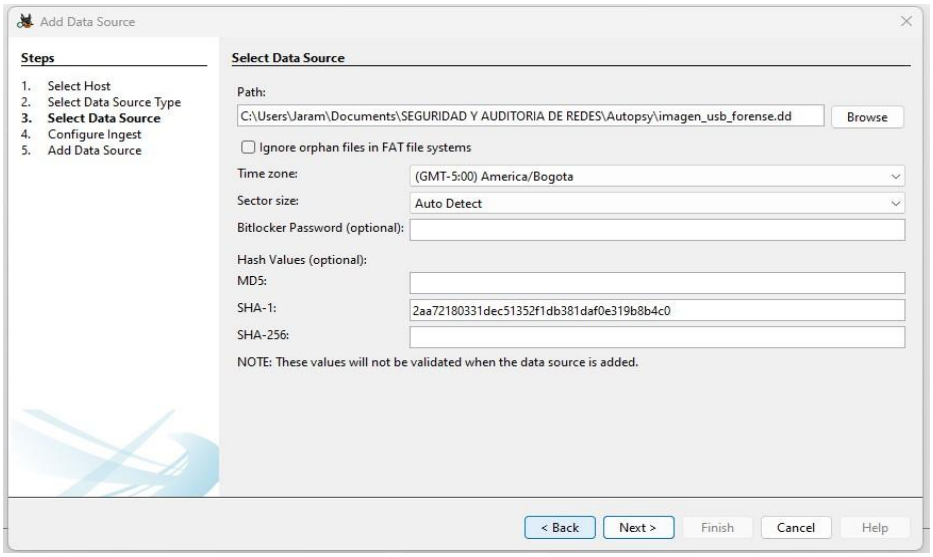


Figura 43. Selección de Parámetros de la Imagen y Hash de Verificación

aquí mostramos la pantalla de configuración mostrando la ruta de la imagen forense, zona horaria Bogotá, y el hash SHA-1 previamente calculado para verificación durante el análisis en Autopsy.

4.3.7 Selección de Módulos para Análisis

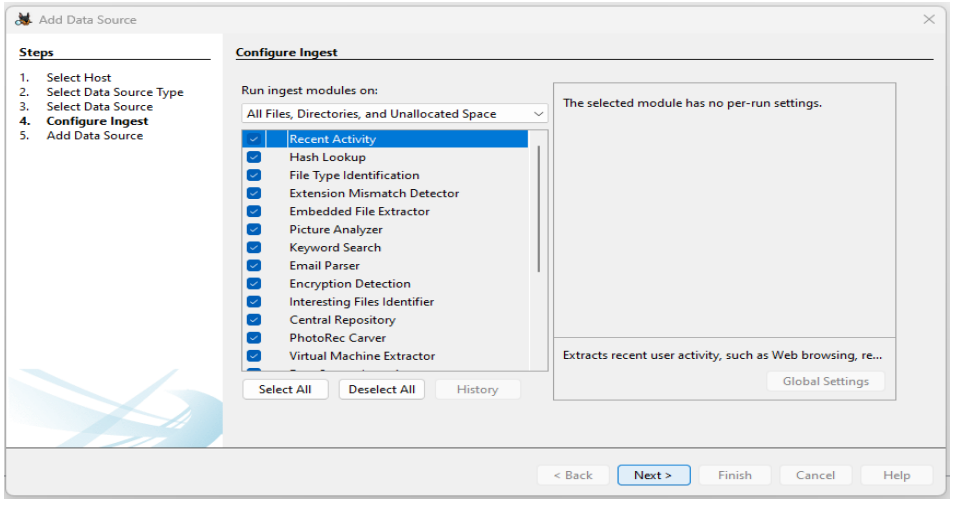


Figura 44. Módulos de Análisis

Lo siguiente es realizar la configuración de módulos de Autopsy donde se seleccionan las herramientas de análisis para examinar la imagen forense de manera automatizada.

4.3.8 Se carga Imagen Forense

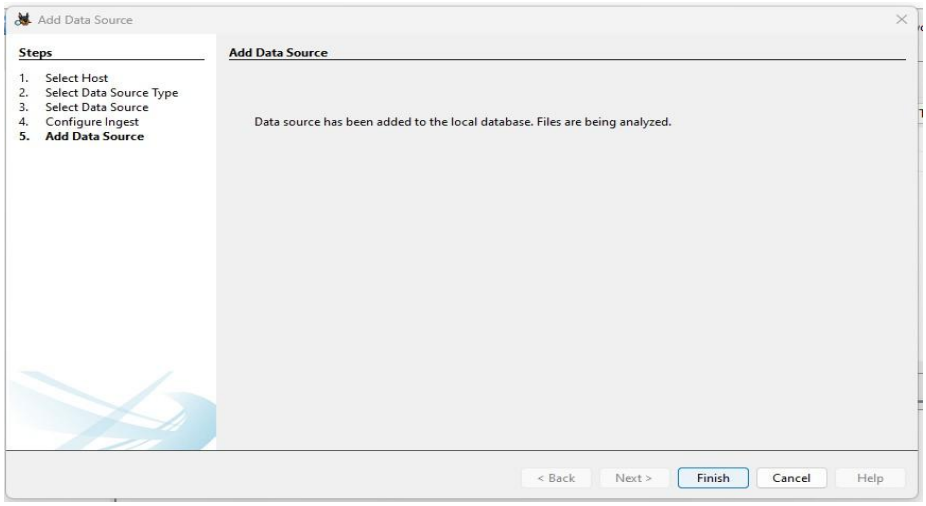


Figura 45. Se carga Imagen Forense y la fuente de Datos Agregada

Aquí miramos la confirmación de que la imagen forense ha sido agregada exitosamente a la base de datos de Autopsy y está siendo analizada automáticamente por los módulos de ingesta seleccionados.

4.4.Interfaz de Análisis de Autopsy

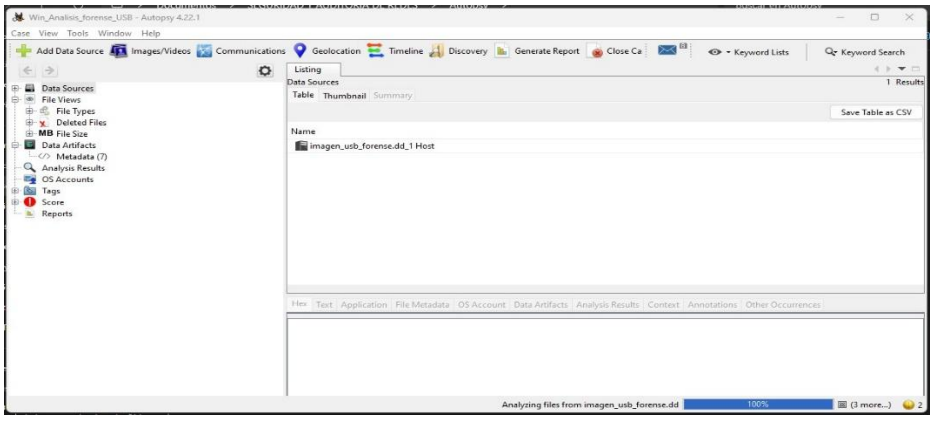


Figura 46. Análisis en Progreso

Autopsy Windows mostrando el análisis en tiempo real de la imagen forense. La barra de progreso indica 100% completado

4.5.Archivos Recuperados de la Memoria USB

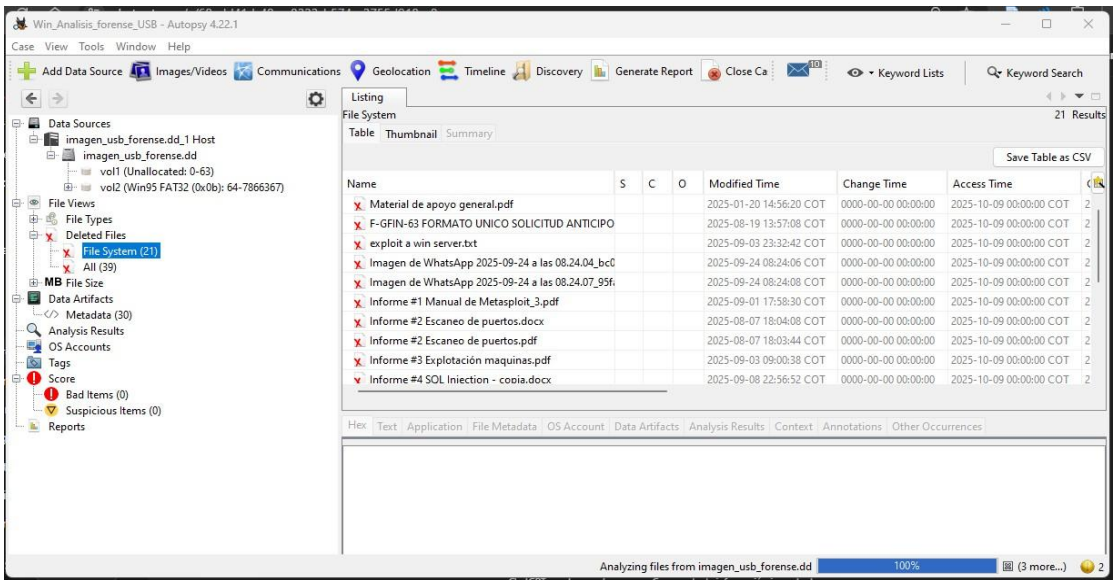


Figura 47. Resultados del Análisis Forense

Por último, mostrando los archivos recuperados de la memoria USB, incluyendo documentos PDF, Word, imágenes de WhatsApp y archivos de texto.

4.6.Extracción de Archivos desde la Imagen Forense

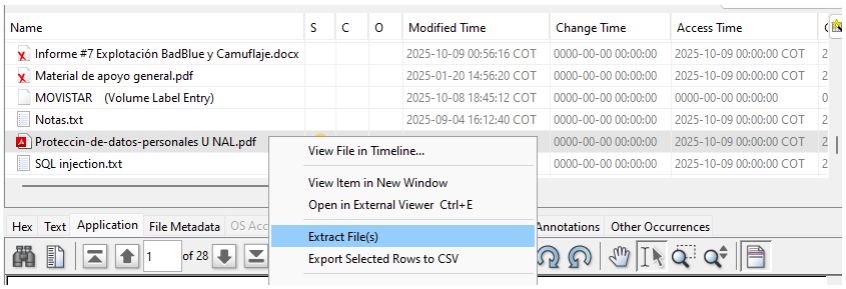


Figura 48. Exportación de Archivos Recuperados

Lo siguiente que hicimos fue buscar la opción Extract File(s) para exportar los archivos recuperados de la imagen forense.

4.6.1 Exportación de Archivo PDF Recuperado

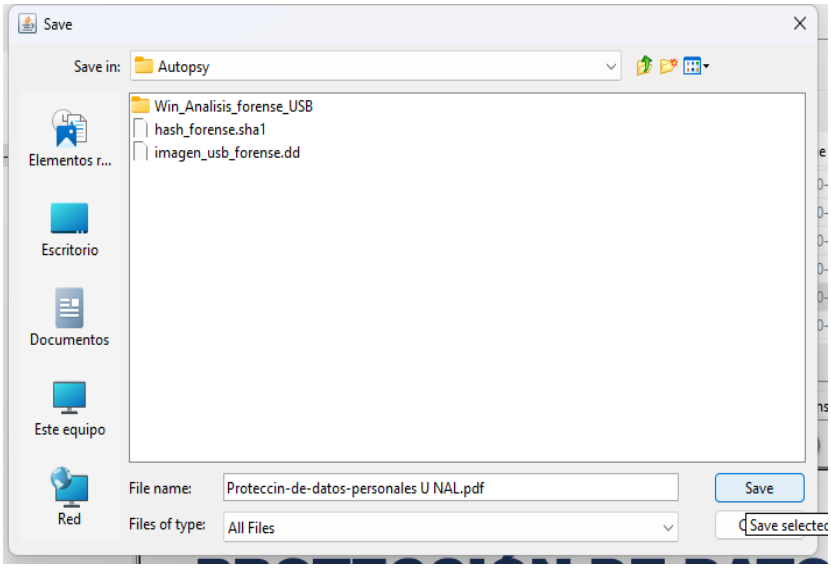


Figura 49. Guardando Archivo Extraído

Aquí se evidencia la ventana de guardar mostrando la extracción del archivo "Proteccion-de-datos-personales U NAL.pdf" desde la imagen forense hacia la carpeta Autopsy en Windows.

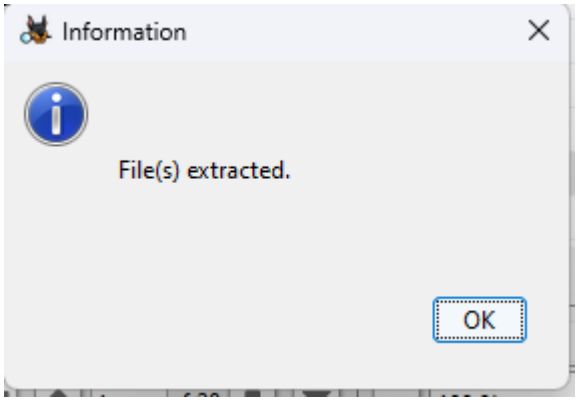


Figura 50. Extracción Exitosa

Finalmente, obtuvimos el mensaje de confirmación de Autopsy indicando que el archivo PDF ha sido extraído exitosamente de la imagen forense y guardado en el sistema de archivos de Windows.

5. Capítulo 3: Descarga de FTK Imager en Windows

Para descargar FTK Imager lo que debemos hacer es ir a nuestro navegador y buscar el sitio oficial de este software.

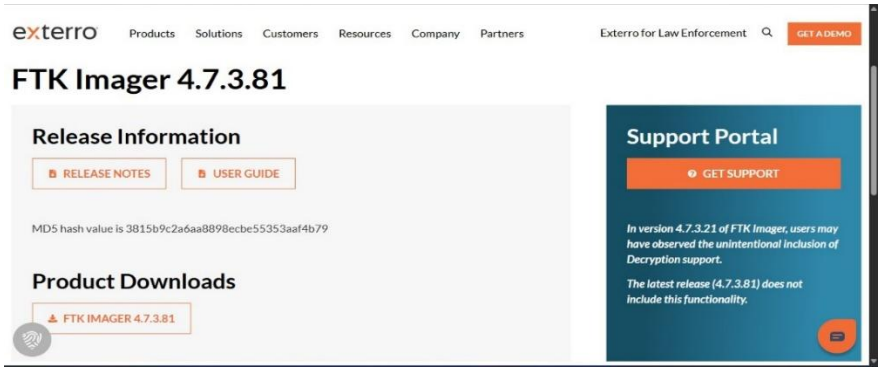


Figura 51. Página de Descarga de FTK Imager

Dentro de la Página oficial buscamos la opción de descargar FTK Imager 4.7.3.81, herramienta profesional para creación de imágenes forenses.

5.1.Formulario de Registro para descargar FTK Imager

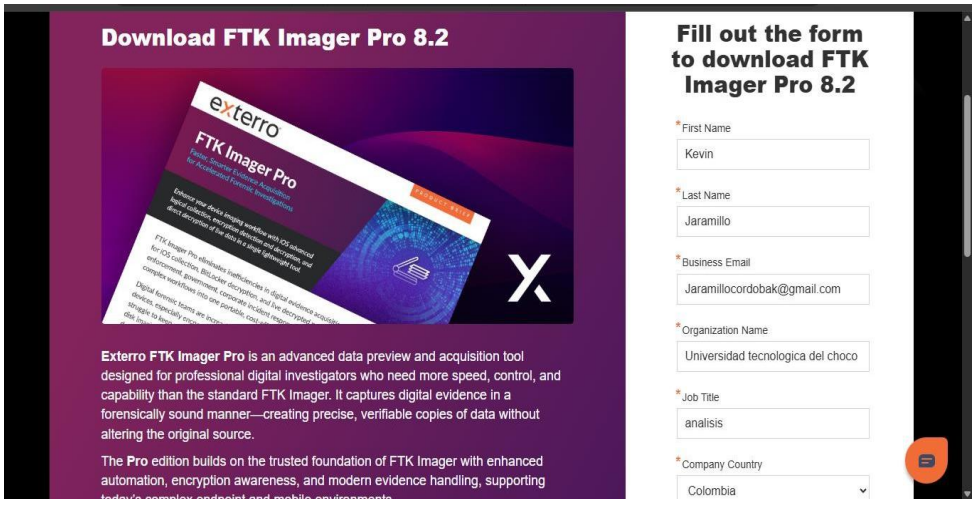


Figura 52. Descarga de FTK Imager Pro

Página de registro para descargar FTK Imager Pro 8.2, versión avanzada con capacidades forenses mejoradas. Se completan los datos de la persona (Kevin Jaramillo) y la institución (Universidad Tecnológica del Chocó) para obtener el software.

5.2.Confirmamos la Descarga de FTK Imager

Figura 53.Descarga Exitosa FTK Imager

Luego obtuvimos un mensaje de éxito confirmando que la descarga de FTK Imager Pro 8.2 ha comenzado automáticamente.

5.2.1 Descompresión del Instalador de FTK Imager

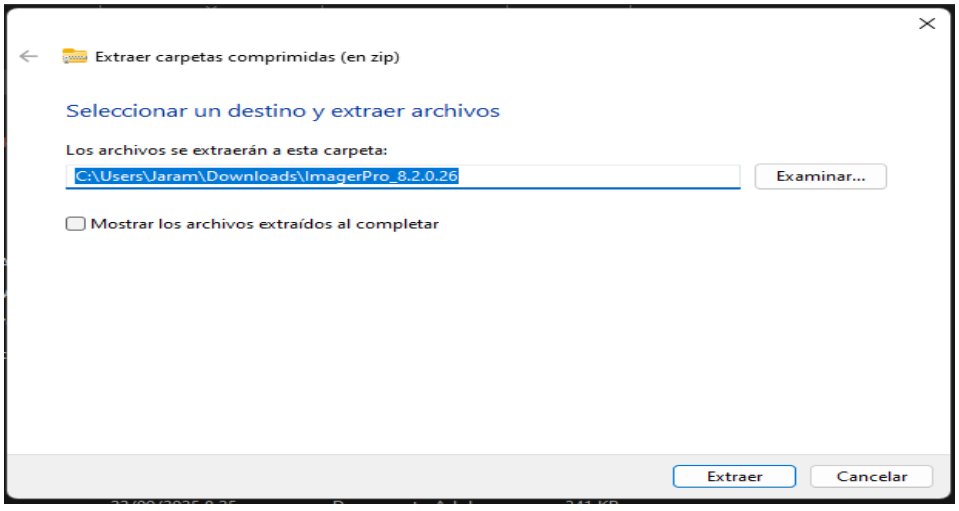


Figura 54. Extracción de Archivos de FTK Imager

Después que descargamos el archivo hicimos la extracción de los archivos comprimidos de FTK Imager en la carpeta de Descargas, preparando los archivos necesarios para la instalación del software forense.

5.3.Instalación de CodeMeter Runtime para FTK Imager

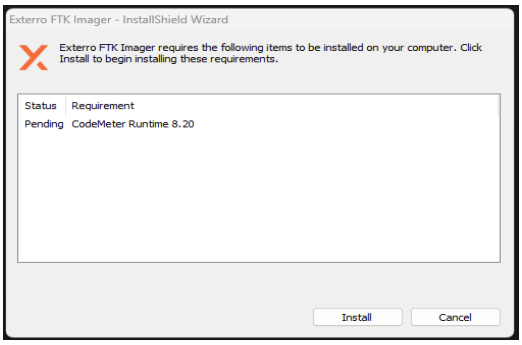


Figura 55. Instalamos los archivos necesarios

Luego realizamos la instalación del asistente CodeMeter Runtime 8.20 como requisito previo para FTK Imager. Este componente es necesario para la gestión de licencias y seguridad del software forense.

5.4.Instalación de Exterro FTK Imager

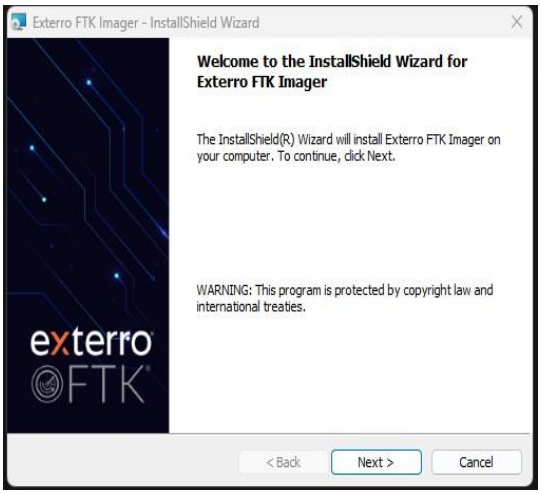


Figura 56. Asistente de Instalación FTK Imager

Pantalla de bienvenida del asistente de instalación de FTK Imager, mostrando la advertencia de protección por derechos de autor antes de comenzar la instalación del software forense.

Figura 57. Acuerdo de Licencia términos y condiciones

Pantalla del acuerdo de licencia que debe ser aceptado para continuar con la instalación de FTK Imager. El usuario debe marcar la casilla de aceptación de términos antes de proceder con la instalación del software.

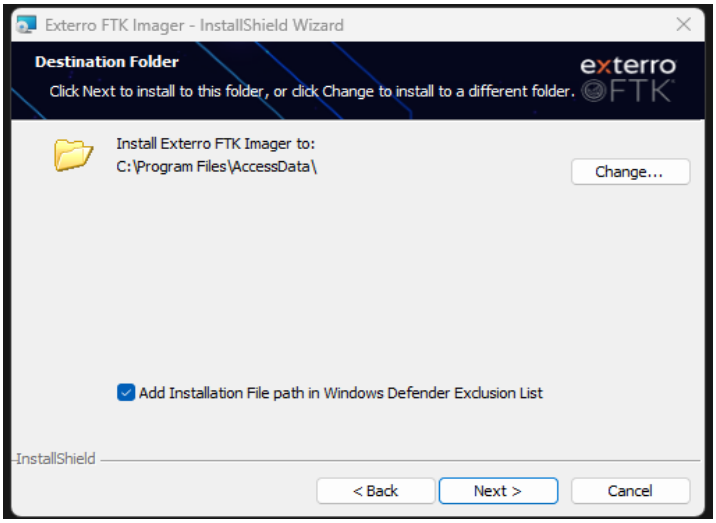


Figura 58. Carpeta de Destino

Obtuvimos esta pantalla en la que se realiza la selección de carpeta de destino para FTK Imager. Por defecto se instala en C:\Program Files\AccessData\ y se da la opción de excluir la ruta en Windows Defender para evitar interferencias durante el análisis forense.

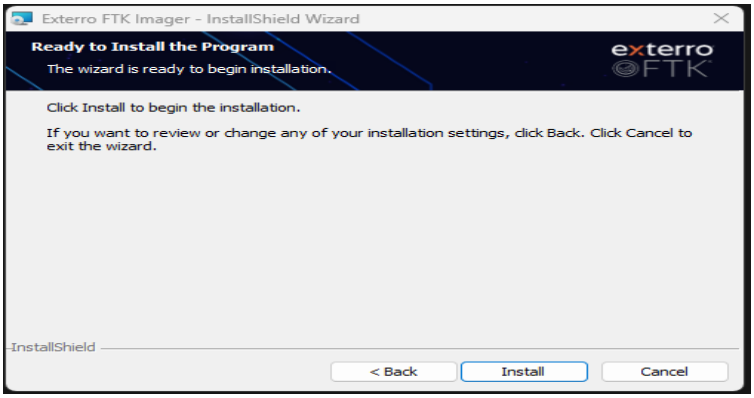


Figura 59. Listo para Instalar

Se muestra la pantalla final del asistente confirmando que está listo para instalar FTK Imager.

5.4.1 Finalización Exitosa de la Instalación

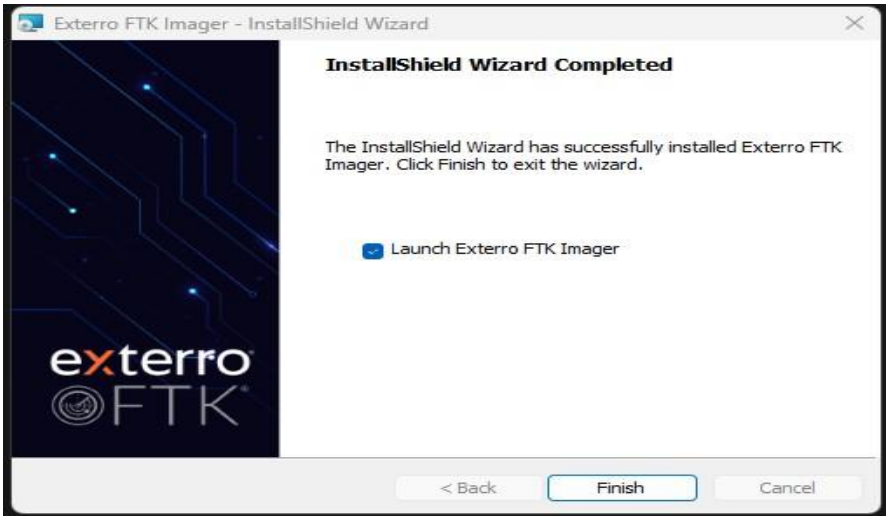


Figura 60. Instalación Completada

Ya en este punto se había hecho una instalación exitosa de FTK Imager. La casilla "Launch Exterro FTK Imager" permite abrir el software inmediatamente para comenzar el análisis forense de la memoria USB.

5.5.Crearcion de la Imagen en FTK Imager

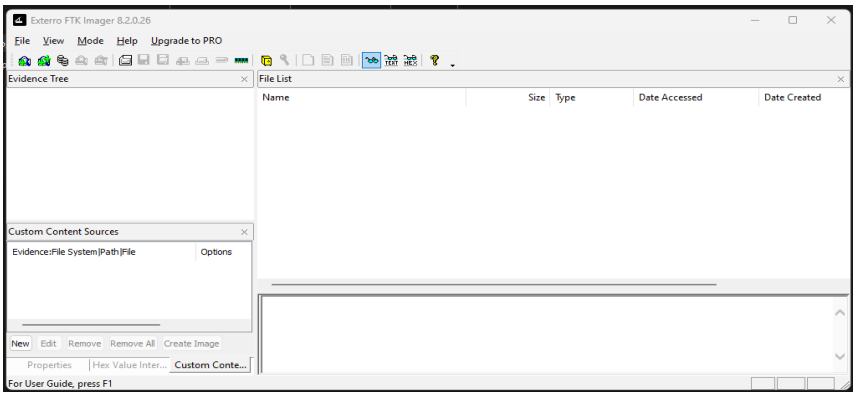


Figura 61. Interfaz Principal FTK Imager

Antes de realizar el proceso de análisis forense ingresamos a FTK y se nos mostró esta interfaz. La interfaz principal de FTK Imager contiene el árbol de evidencia y opciones para crear nuevas imágenes forenses.

5.5.1 Configuración de Fuente de Evidencia

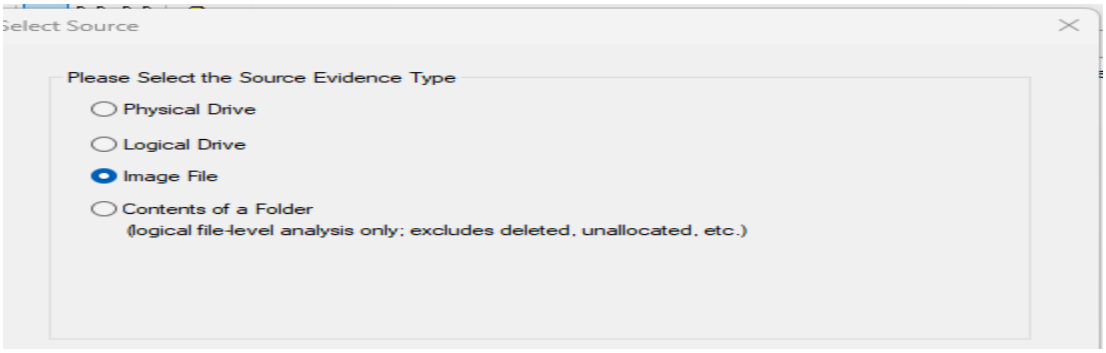


Figura 62. Selección de Tipo de Fuente

Luego, realizamos la selección de tipo de evidencia en FTK Imager. Se elige "Image File" para cargar y analizar la imagen forense previamente creada de la memoria USB.

5.5.2 Cargando Archivo de Imagen DD en FTK Imager

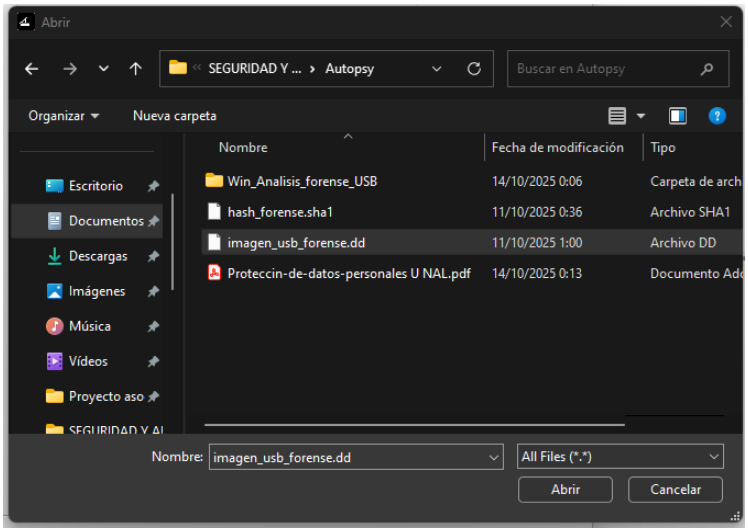


Figura 63. Selección de Imagen Forense

En FTK Imager para seleccionamos la imagen forense imagen_usb_forense.dd desde la carpeta Autopsy.

5.5.3 Fuente de Evidencia Definida en FTK Imager

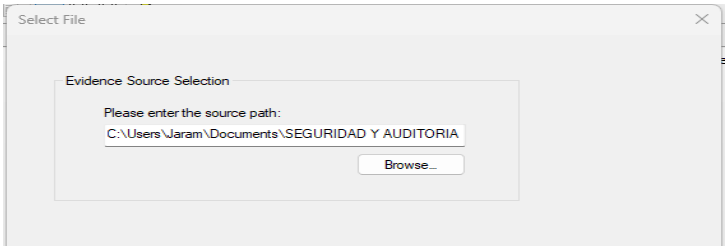


Figura 64.Ruta de Evidencia Configurada

Después en FTK Imager utilizamos la ruta de la imagen forense ya configurada. La herramienta está lista para cargar y analizar el archivo imagen_usb_forense.dd desde la ubicación especificada en el directorio.

5.5.4 Contenido de la Memoria USB en FTK Imager.

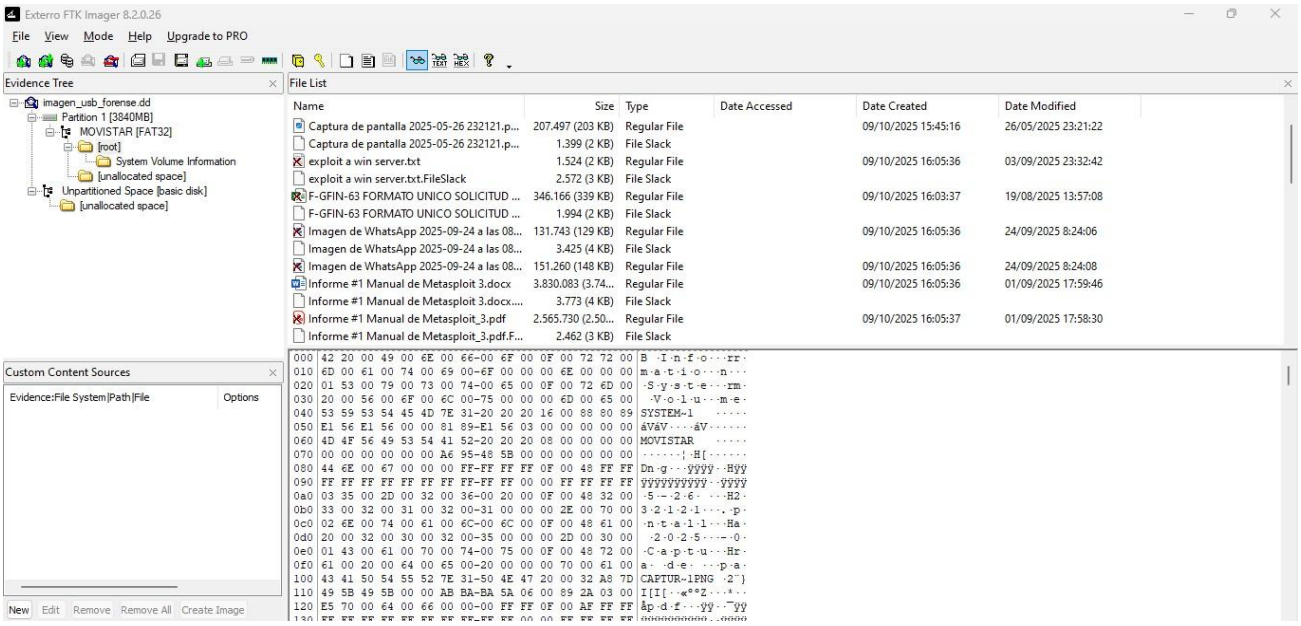


Figura 65. Análisis de Imagen en FTK Imager

Dentro de FTK Imager mostramos el análisis detallado de la imagen forense. Se visualizan documentos, imágenes de WhatsApp y archivos de PDF.

5.6.Archivos Exportado Correctamente

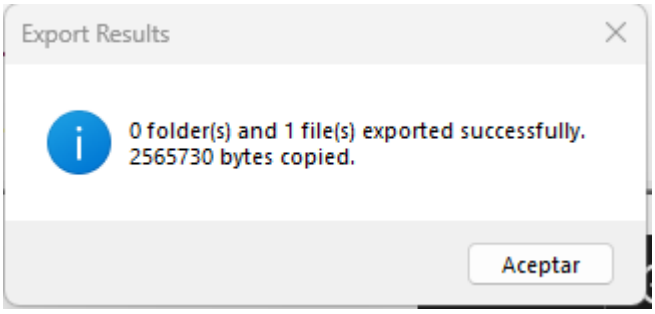


Figura 66. Exportación Exitosa

Por último, mostramos el mensaje de confirmación que indica que exportamos los archivos de forma correcta, cerrando así este sección y la culminación de la práctica.

Problemas Encontrados en la Realización de Este Manual

El principal inconveniente que encontramos al realizar este informe fue conseguir una memoria USB con una capacidad menor a 4 GB, tal como se requería para la práctica. Esta tarea resultó bastante difícil y, finalmente, no fue posible cumplir con esa especificación, por lo que tuvimos que trabajar con un dispositivo USB de 4 GB de almacenamiento.

Solución del Problema

No fue posible cumplir con esa especificación por lo que no técnicamente no se encontró una soluciona para este problema y que tuvimos que trabajar con un dispositivo USB de 4 GB de almacenamiento.

Recomendaciones

Por el momento no tengo una recomendación para el laboratorio como tal, ya que en general me gusto bastante la temática trata. Espero practicar un poco más para dominar el tema que estamos viendo y los temas que veremos más adelante.

Conclusión

Concluimos afirmando que la práctica permitió desarrollar un proceso forense completo, tanto en Kali Linux utilizando herramientas nativas como *dd*, *sha1sum* y Autopsy, como en Windows empleando Autopsy y FTK Imager. A lo largo del procedimiento se logró adquirir, verificar, analizar y extraer evidencias digitales de una memoria USB, garantizando siempre la integridad de los datos mediante la generación y comprobación de valores hash. Aunque uno de los principales retos fue encontrar una memoria USB de menos de 4 GB, se pudo continuar el ejercicio utilizando un dispositivo de mayor capacidad, manteniendo la metodología forense adecuada.

La creación de la imagen bit a bit, la asignación de permisos, la configuración de casos en Autopsy y la importación de la evidencia demostraron el flujo real de un análisis profesional. Las herramientas permitieron visualizar la estructura del dispositivo, recuperar archivos eliminados o existentes, y extraer evidencias relevantes sin alterar el contenido original. El uso de FTK Imager reforzó el aprendizaje al mostrar otra alternativa sólida y ampliamente usada en entornos forenses.

Esta práctica permitió comprender de forma integral cómo se adquiere, preserva, analiza y documenta evidencia digital, destacando la importancia del manejo adecuado de los dispositivos, la validez legal mediante algoritmos criptográficos y la correcta utilización de software especializado. Este procedimiento refleja la metodología base en cualquier investigación forense digital real.

Referencias Bibliográficas

Oracle. (2024). *VirtualBox: Powerful x86 and AMD64/Intel64 virtualization*. Oracle VM VirtualBox. https://www.virtualbox.org/

Kali Linux. (2024). *Kali Linux Downloads*. Offensive Security. https://www.kali.org/get-kali/

Nmap, org. (s. f.). *Guía de referencia de Nmap (Página de manual)*. Recuperado 6 de agosto de 2025, de https://nmap.org/man/es/index.html

Rafael S Morales (2025) *análisis forense a través de autopsy y otras aplicaciones de auditoria forense en Kali Linux y Windows* -Tema explicados en clase.