ANALISIS FORENSE CON USB MEDIANTE AUTOPSY EN KALI LINUX Y WINDOWS A SU VEZ EL USO DE FTK IMAGER

KEVIN STIVEN JARAMILLO CORDOBA

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"
FACULTAD DE INGENIERÍA
INGENIERIA DE TELECOMUNICACIONES
SEGURIDAD Y AUDITORIA DE REDES
QUIBDÓ-CHOCO (COLOMBIA)
2025

ANALISIS FORENSE CON USB MEDIANTE AUTOPSY EN KALI LINUX Y WINDOWS A SU VEZ EL USO DE FTK IMAGER

KEVIN STIVEN JARAMILLO CORDOBA

Estudiantes, IX semestre

ING. RAFAEL SANDOVAL MORALES

Docente de la asignatura

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"

FACULTAD DE INGENIERÍA

INGENIERIA DE TELECOMUNICACIONES

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCO (COLOMBIA)

2025

Contenido

Tema……**Pagina**

Tabla de Ilustración

1. Introducción

Este laboratorio muestra cómo se puede examinar una memoria USB de forma segura usando dos programas especiales: Autopsy en Kali Linux para analizar archivos borrados de la USB, y FTK Imager en Windows para hacer una copia exacta de la memoria. Todo el proceso se hizo paso a paso, cuidando que la información no se alterara, como si se tratara de una investigación real en la que lo que se encuentra en la USB es importante como prueba.

2. Objetivos

2.1. Objetivo General

Realizar un análisis forense a una memoria USB utilizando las herramientas Autopsy y FTK Imager, con el fin de recuperar y examinar datos de manera confiable.

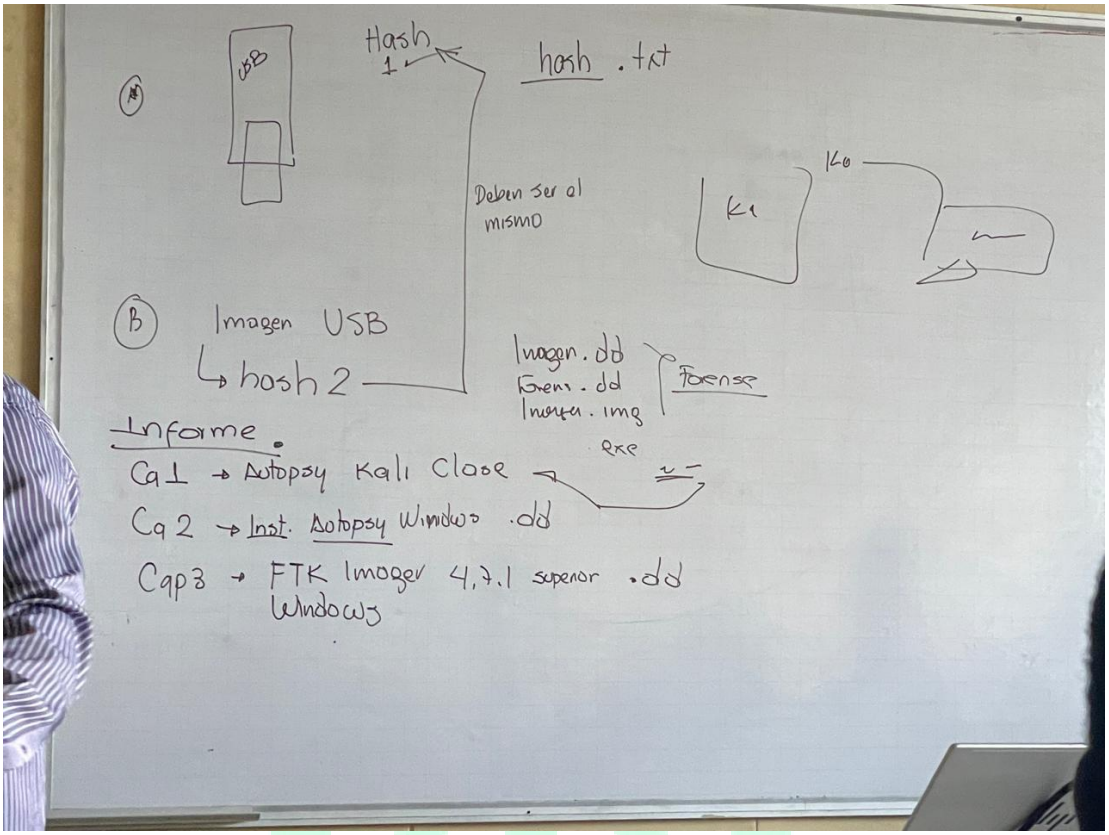
2.2.Objetivos Específicos

- Crear una imagen forense de la memoria USB usando FTK Imager.
- Analizar la imagen con Autopsy en Kali Linux para identificar archivos.
- Documentar los pasos seguidos y los resultados obtenidos de manera clara y ordenada.

3. Justificación

Este trabajo es importante porque nos enseña cómo recuperar información de dispositivos como memorias USB usando programas como Autopsy y FTK Imager. Aprender a manejar estas herramientas no solo es útil en los estudios, sino también en trabajos reales, como cuando hay que investigar filtraciones de información en una empresa o apoyar procesos legales con pruebas digitales. De esta forma, esta práctica nos prepara para actuar de forma correcta y segura cuando ocurren problemas relacionados con datos o seguridad.

4. Planteamiento de la Actividad



Cuando se necesita recuperar información de una memoria USB de manera confiable y sin alterar su contenido, es importante usar herramientas especiales que garanticen que los datos no se modifiquen durante el proceso.

Este trabajo se divide en tres partes principales:

- **Capítulo 1: Uso de Autopsy en Kali Linux**

  Se explora la configuración de Autopsy en Kali Linux para examinar una imagen forense, con el fin de identificar archivos e información relevante almacenada en la memoria USB.

- **Capítulo 2: Instalación y uso de Autopsy en Windows**

  Se instala Autopsy en Windows para comparar cómo funciona en un sistema diferente y ver si los resultados son similares.

- **Capítulo 3: Creación de una copia de la USB con FTK Imager**

  Se usa el programa FTK Imager en Windows para hacer una copia exacta de la memoria USB y verificar que esa copia sea idéntica al original usando un código único (hash SHA1).

5. Desarrollo del tema

5.1.Capítulo #1

5.1.1 Comando para Detección de Dispositivos Conectados

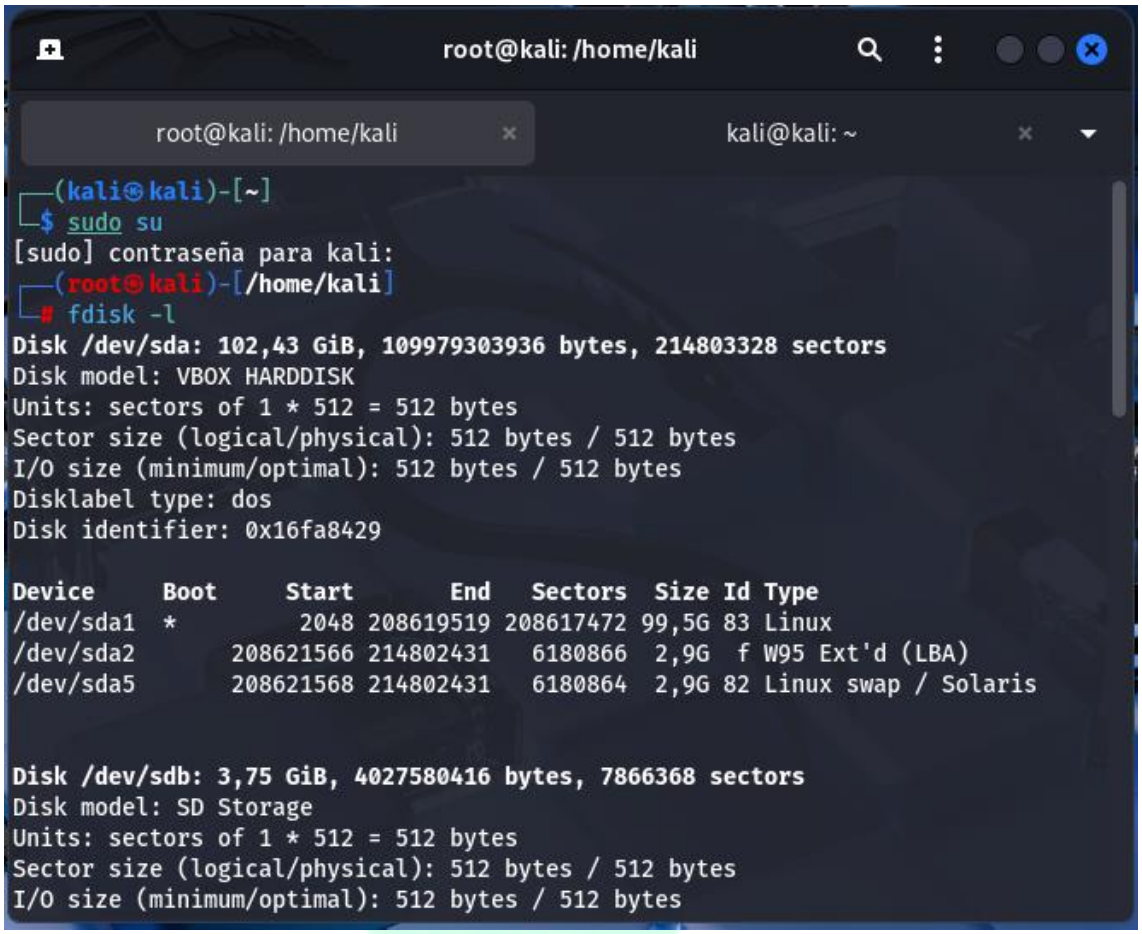


Ilustración 1. Identificación de Dispositivos

En esta imagen se muestra la ejecución del comando fdisk -l , utilizado para identificar los dispositivos de almacenamiento conectados al sistema. Se puede observar la detección del disco principal /dev/sda y la unidad USB /dev/sdb (memoria de 3.75 GB), que corresponde al dispositivo objetivo del análisis forense.

5.1.2 Configuración de Filtros USB.

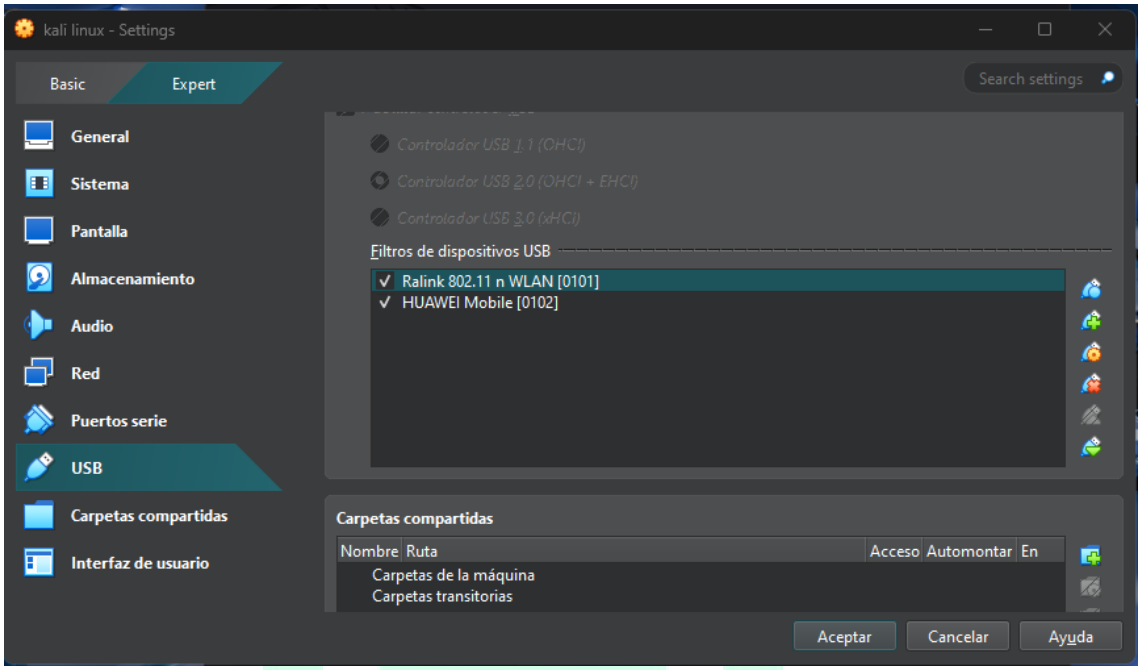


Ilustración 2. Configuración de Dispositivos USB

Esta imagen muestra la ventana de configuración de USB en VirtualBox para Kali Linux. Se observa la habilitación de los controladores USB, esenciales para garantizar la correcta conexión y comunicación con el dispositivos USB físicos. Además, se ha configurado el filtro específico para la memoria USB HUAWEI Mobile, lo que permite el acceso directo y preferencial dela memoria desde el sistema virtual.

5.1.3 Creación de Hash SHA1

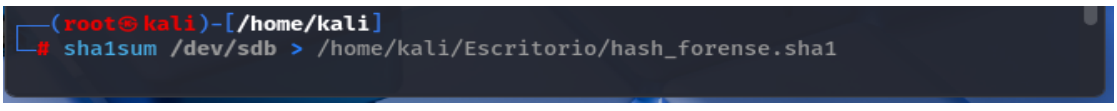


Ilustración 3, Generación de Hash de la Memoria USB

En esta captura se muestra la ejecución del comando shalsum dirigido al dispositivo USB /dev/sdb para generar un valor hash SHA1. El resultado se redirige al archivo hash_forense.sha1 en el Escritorio de Kali Linux.

5.1.4 Hash SHA1 de la Memoria USB Almacenado

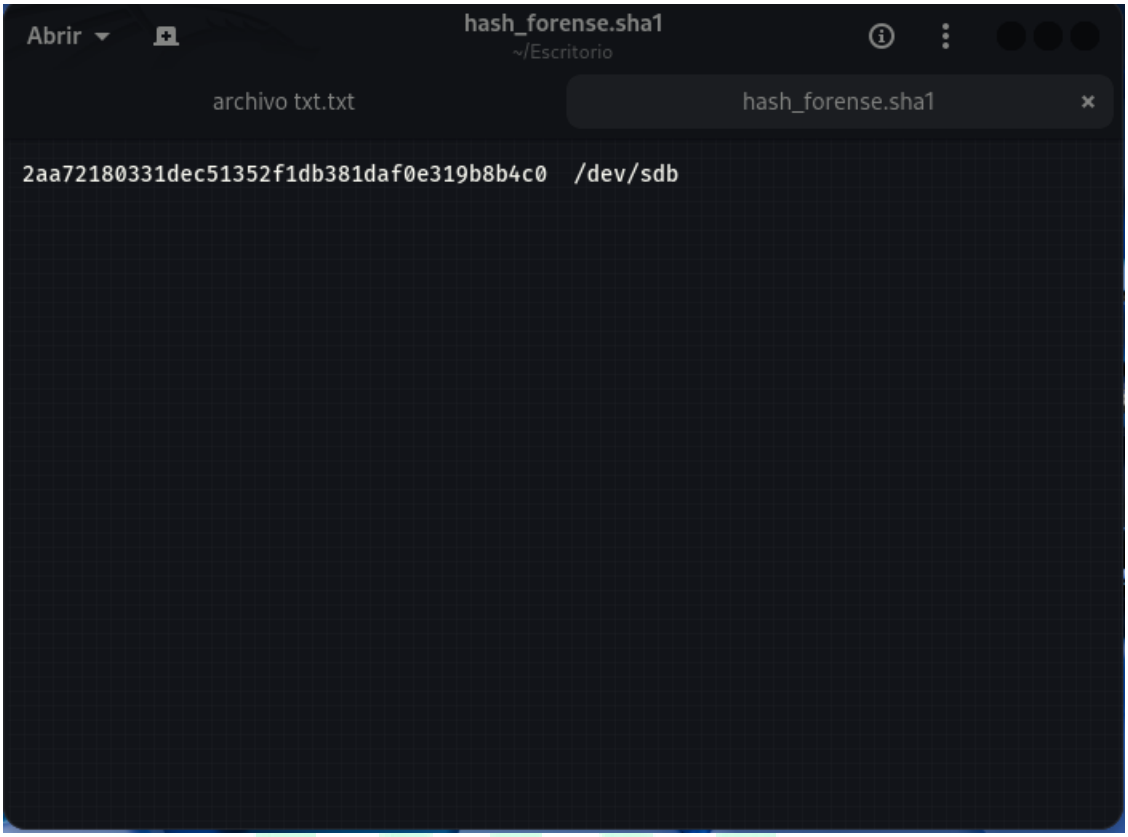


Ilustración 4. Archivo de Hash Generado

Esta imagen muestra el contenido del archivo hash_forense.sha1 generado en el escritorio de Kali Linux, el cual contiene el valor hash SHA1 único correspondiente al dispositivo USB /dev/sdb. El código alfanumérico 2aa72180331dec51352f1db381daf0e319b8b4c0 actúa como identificador digital único de la evidencia.

5.1.5 Comando dd para Generar Imagen de la USB

Ilustración 5. Creación de Imagen USB

En esta captura se muestra la ejecución del comando dd en Kali Linux para crear una imagen forense bit a bit del dispositivo USB /dev/sdb. El comando especifica como entrada (if) el dispositivo USB y como salida (of) el archivo imagen_usb_forense.dd en el escritorio. Los parámetros conv=noerror,sync aseguran que el proceso continúe incluso si encuentra errores.

5.1.6 Proceso de Imagen USB Completado

Ilustración 6. Finalización de la Creación de la Imagen

Esta captura muestra la finalización exitosa del comando dd para crear la imagen de la memoria USB. Se puede observar que se copiaron 7,866,368, equivalentes a 4.0 GB (3.8 GiB) de datos, confirmando que se realizó una copia completa del dispositivo.

5.1.7 Comparación de Hash Dispositivo Original e Imagen

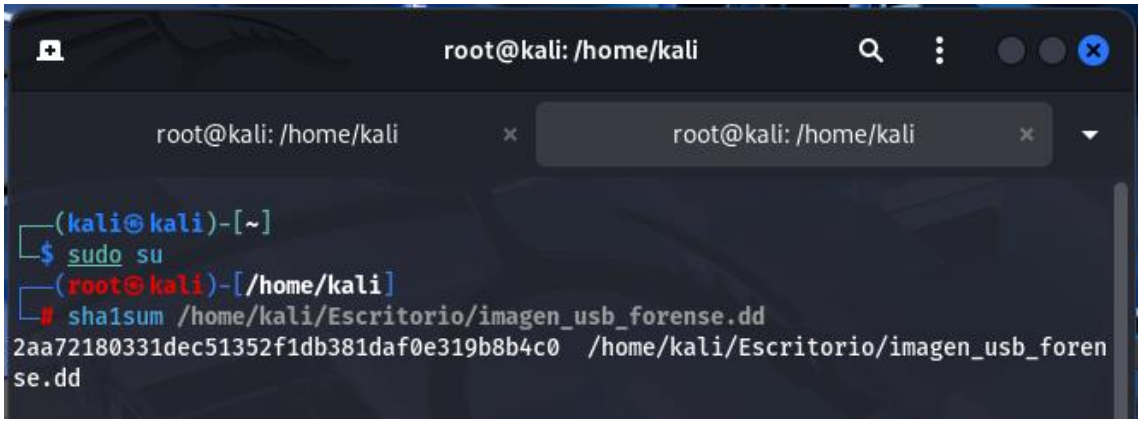


Ilustración 7. Verificación de la Imagen USB

En esta imagen se muestra el proceso de verificación mediante el comando sha1sum aplicado a la imagen generada imagen_usb_forense.dd. El valor hash resultante (2aa72180331dec51352f1db381daf0e319b8b4c0) coincide exactamente con el hash previamente calculado del dispositivo USB original /dev/sdb.

5.1.8 Asignación de Permisos

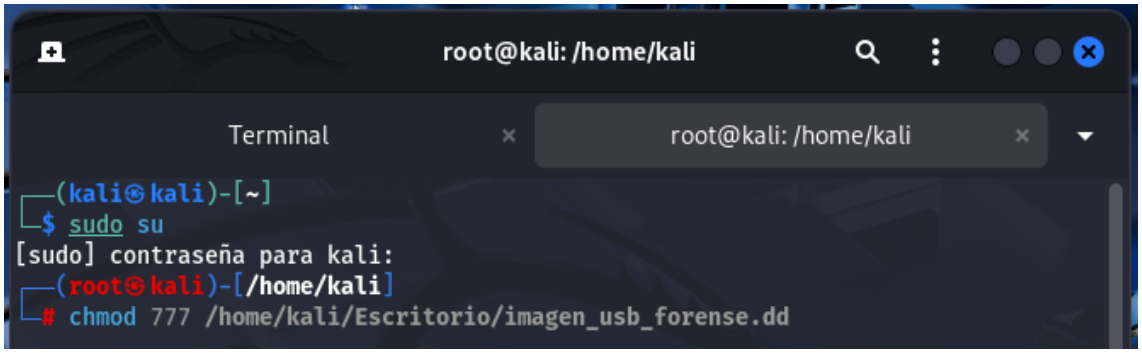


Ilustración 8. Configuración de Permisos de la Imagen

Esta captura muestra la ejecución del comando chmod 777 sobre la imagen imagen_usb_forense.dd en el escritorio de Kali Linux. Este comando asigna permisos de lectura, escritura y ejecución para el propietario, grupo y otros usuarios, garantizando acceso completo al archivo.

5.1.9 Acceso Directo e Icono de Autopsy

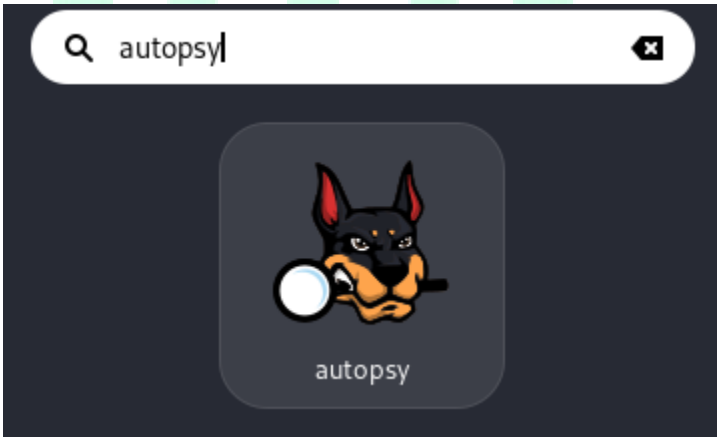


Ilustración 9. Icono de la Aplicación Autopsy

Esta imagen muestra el icono de acceso directo de Autopsy en el entorno de Kali Linux.

5.1.10 Servicio Autopsy Iniciado

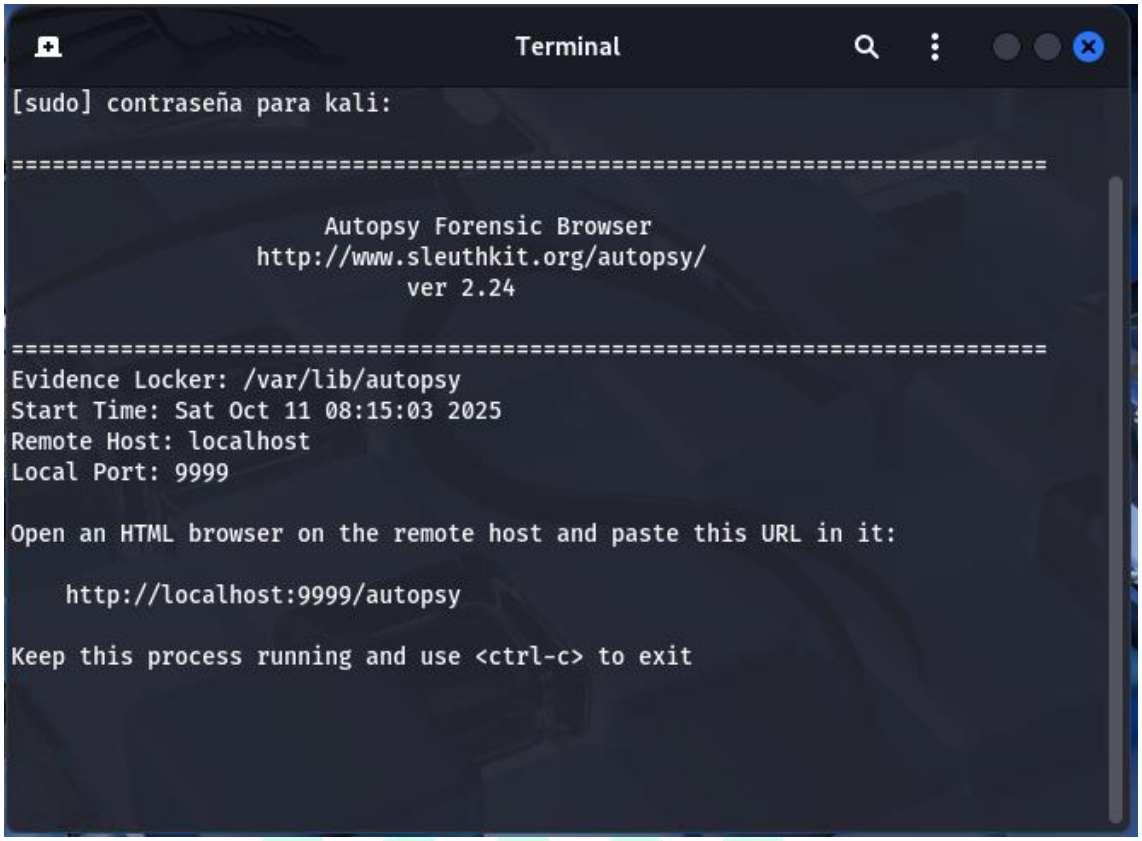


Ilustración 10. Inicialización del Servicio Web de Autopsy

Esta imagen muestra la salida en terminal después de ejecutar Autopsy, indicando que el servicio forense se ha iniciado correctamente. La herramienta funciona como un servidor web local accesible mediante la URL http://localhost:9999/autopsy.

5.1.11 Página de Inicio de Autopsy

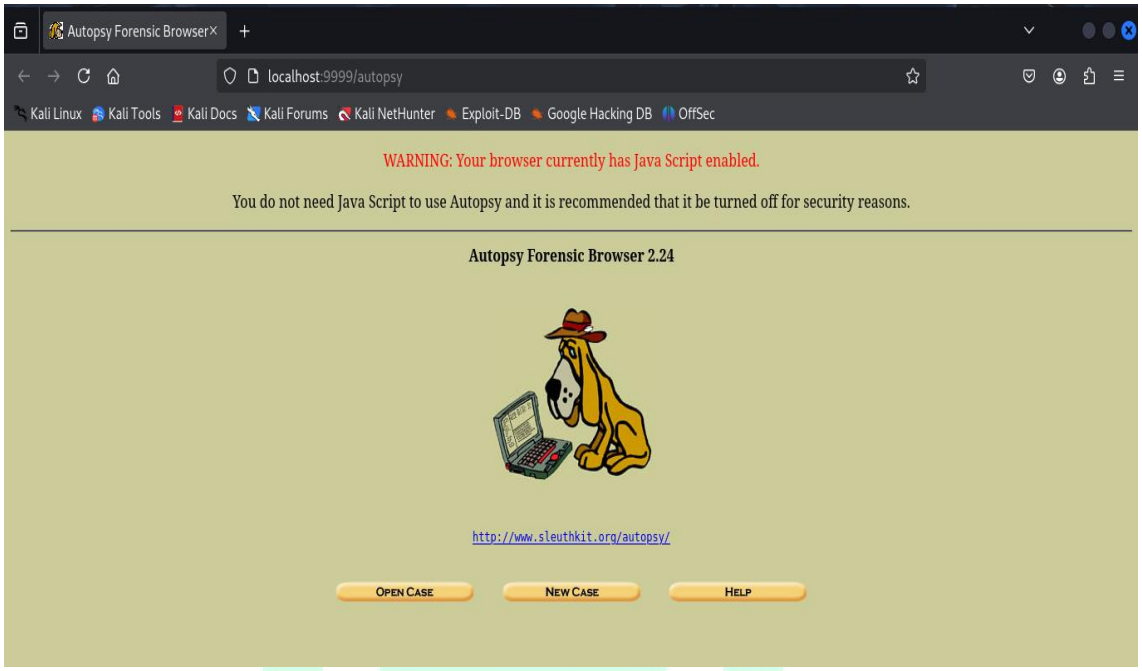


Ilustración 11. Interfaz Principal de Autopsy

Esta imagen muestra la interfaz web inicial de Autopsy Desde esta pantalla principal, el usuario debe hacer clic en Nuevo Caso (New Case) para comenzar a crear un caso forense, que permitirá cargar la imagen de la memoria USB.

5.1.12 Formulario de Configuración de Nuevo Caso

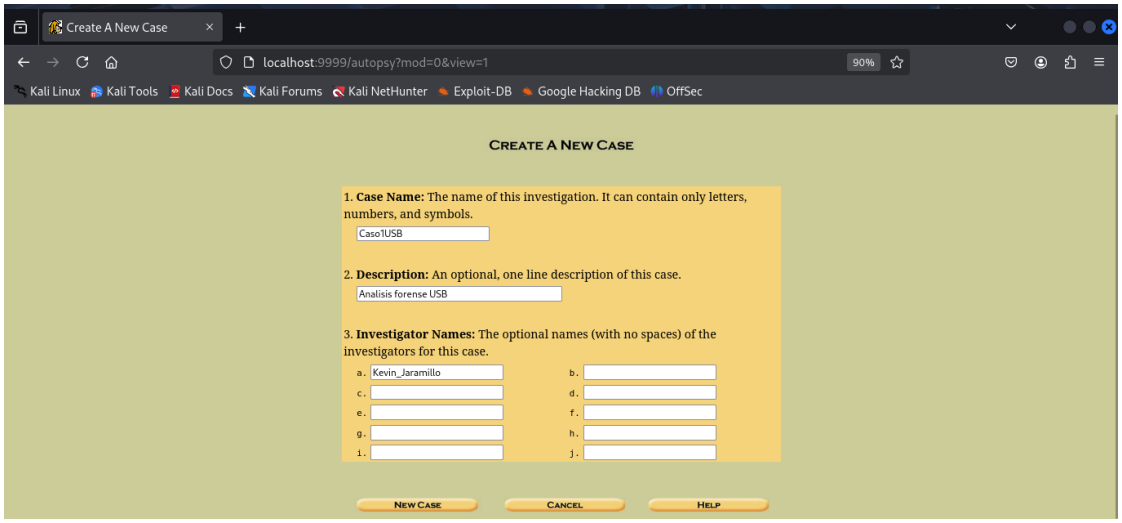


Ilustración 12. Creación de Nuevo Caso

Esta imagen muestra el formulario para crear un nuevo caso forense en Autopsy. Se observa la configuración inicial donde se define el nombre del caso (que solo puede contener letras, números y símbolos), una descripción opcional del caso "Análisis forense USB", y los nombres de los investigadores involucrados (en este caso, Kevin_Jaramillo).

5.1.13 Caso Creado Exitosamente en Autopsy

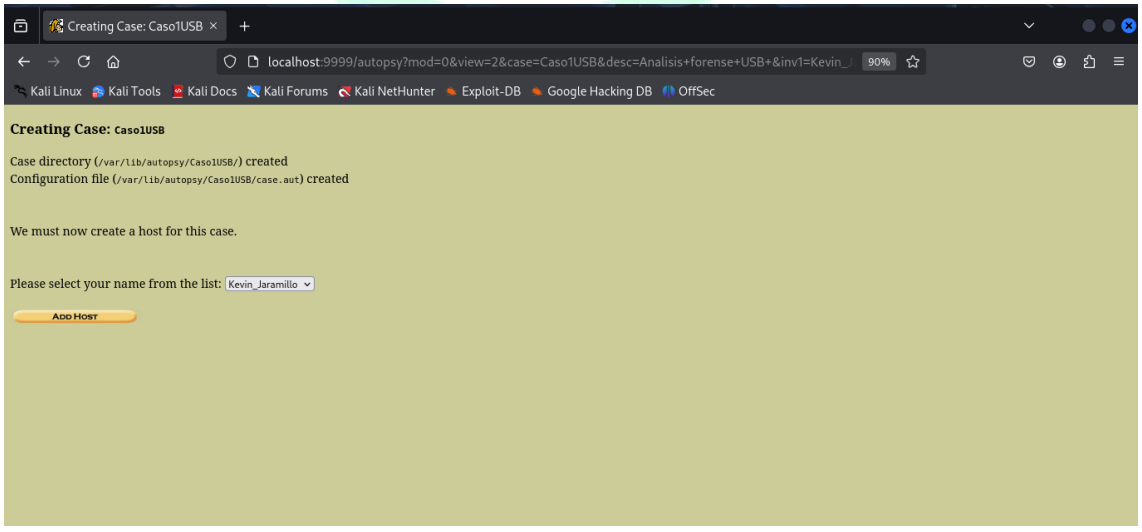


Ilustración 13. Confirmación de Creación del Caso Forense

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

5.1.14 Parámetros Opcionales de Configuración

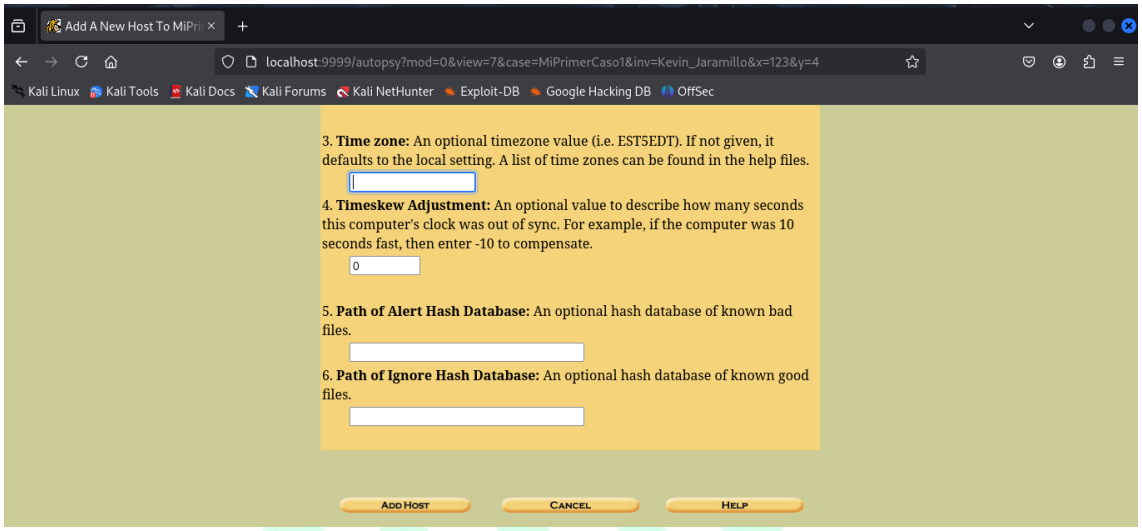


Ilustración 14. Configuración Avanzada del Host

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).

5.1.15 Configuración de Host Completada

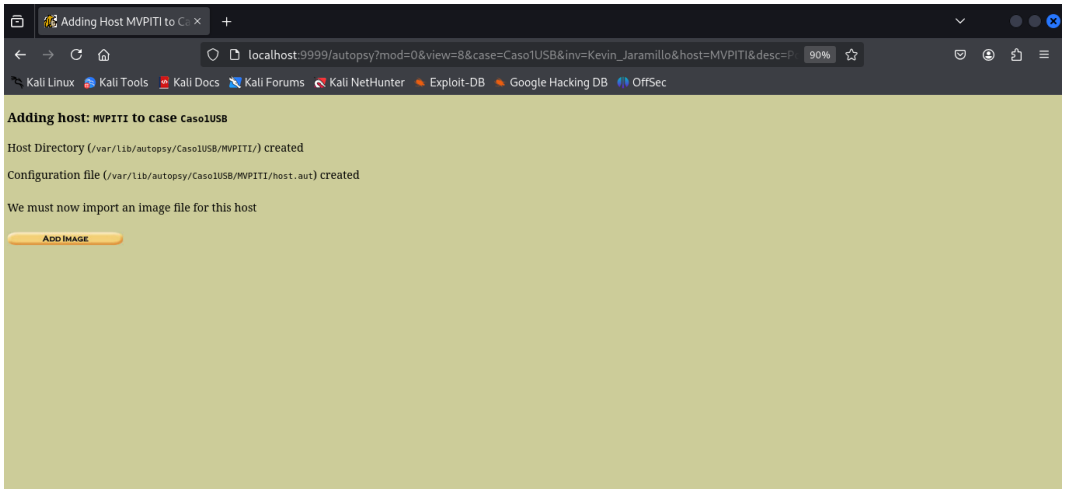


Ilustración 15. Host Creado Exitosamente

Confirmación de la creación del host "MVPITI" en el caso forense. El sistema está listo para importar la imagen de la memoria USB y comenzar el análisis.

5.1.16 Interfaz de Host Listo para Importar Imagen

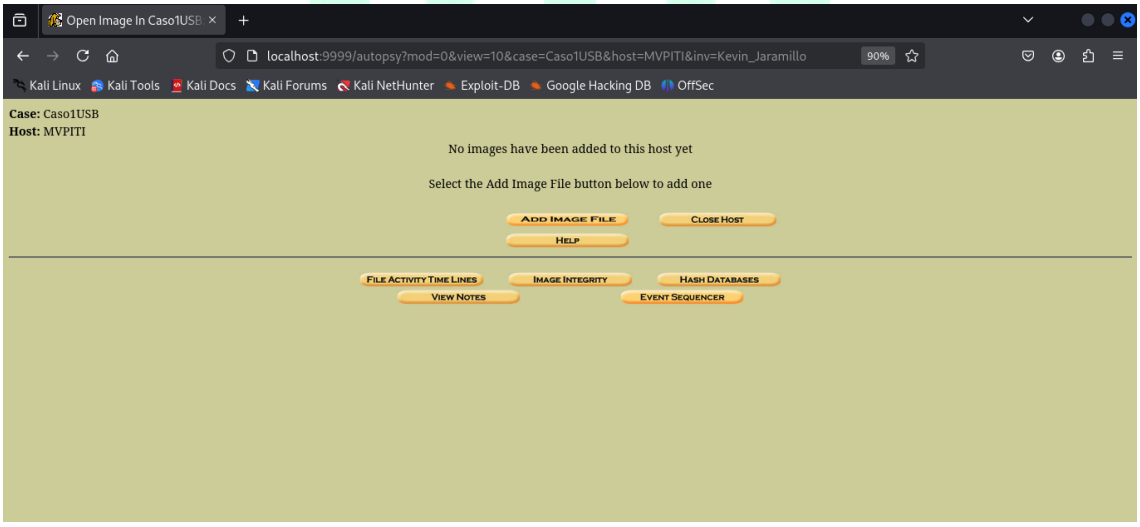


Ilustración 16. Host sin Imagen

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.

5.1.17 Formulario para Agregar Imagen Forense al Host

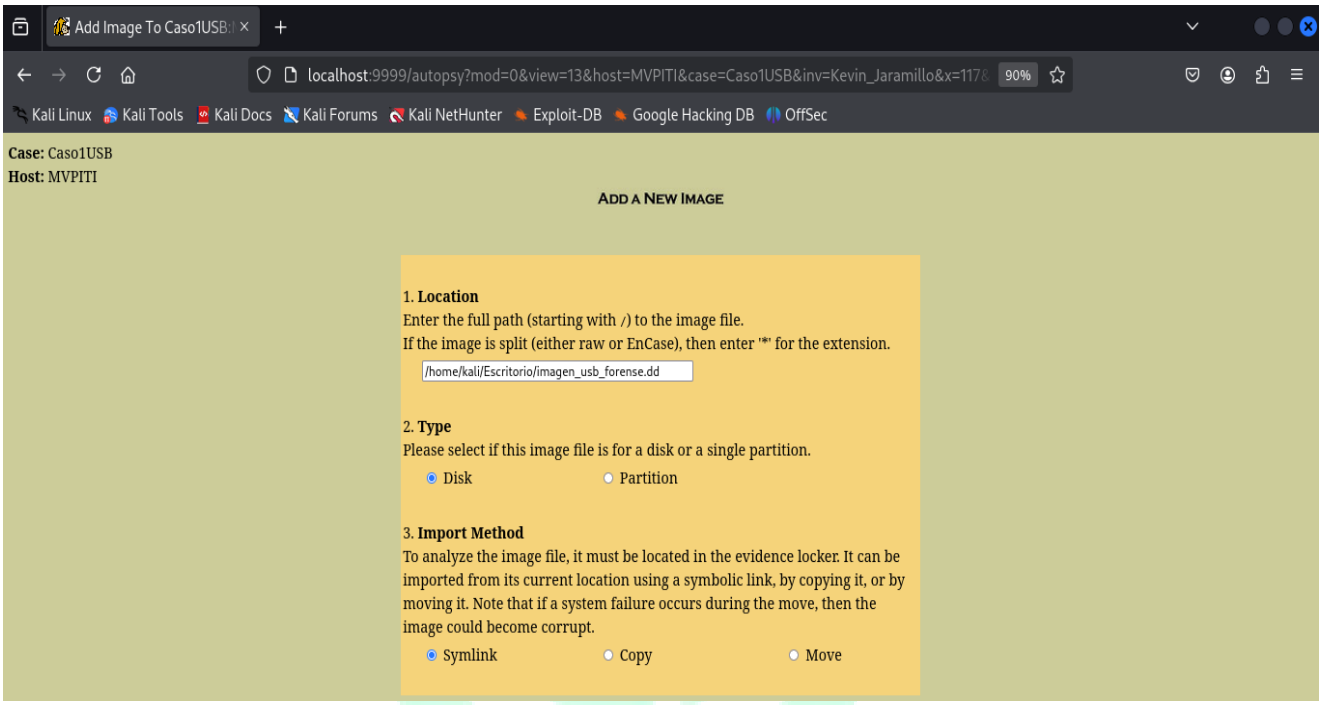


Ilustración 17. Configuración de Importación de Imagen

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.

5.1.18 Configuración de Hash y Detección de Partición

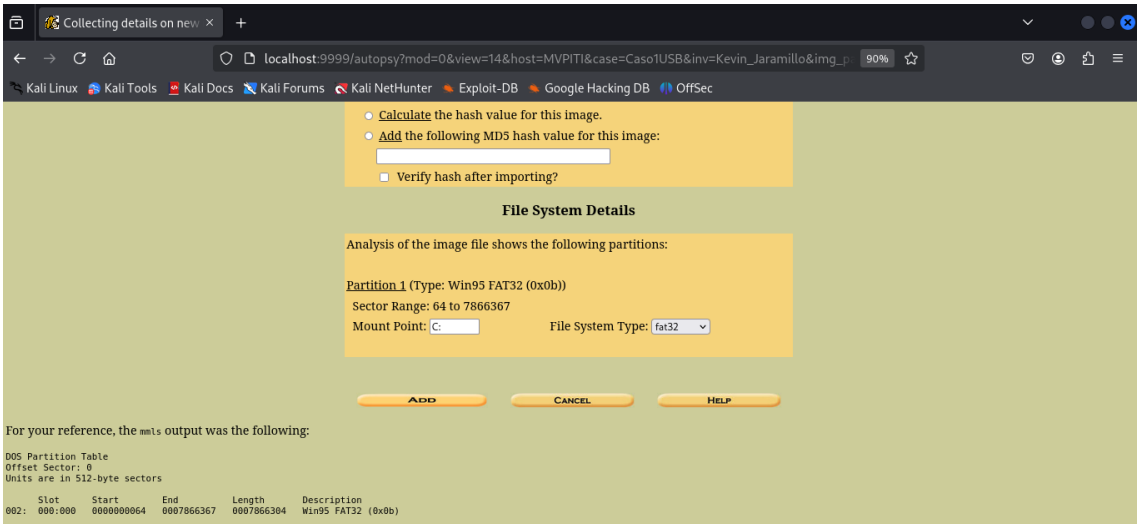


Ilustración 18. Detalles de Partición y Hash

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.

5.1.19 Proceso de Importación de Imagen Completado

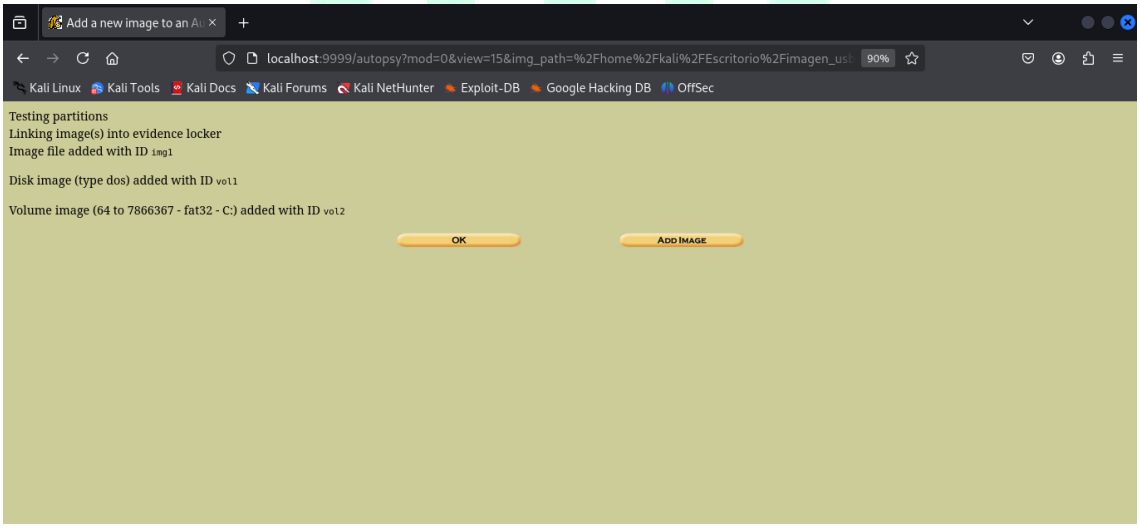


Ilustración 19. Imagen Importada Exitosamente

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.

5.1.20 Interfaz de Selección de Volumen

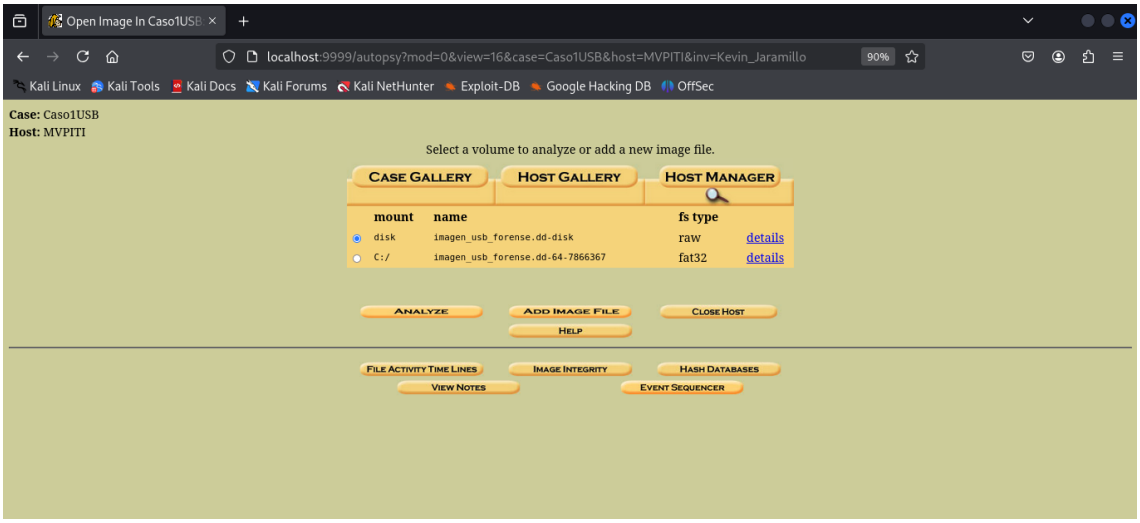


Ilustración 20. Volumen Listo para Análisis

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.

5.1.21 Opciones de Búsqueda y Navegación de Archivos

Ilustración 21. 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.

5.1.22 Proceso de Cálculo de Hash MD5 de la Imagen

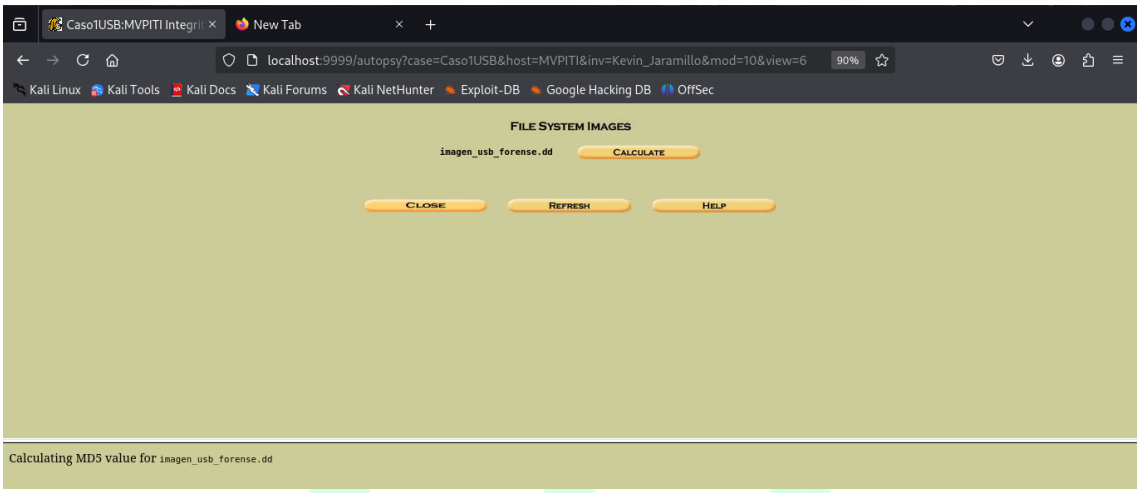


Ilustración 22. Cálculo de Hash MD5

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

5.2.Capitulo #2

5.2.1 Descarga de Autopsy Para Windows

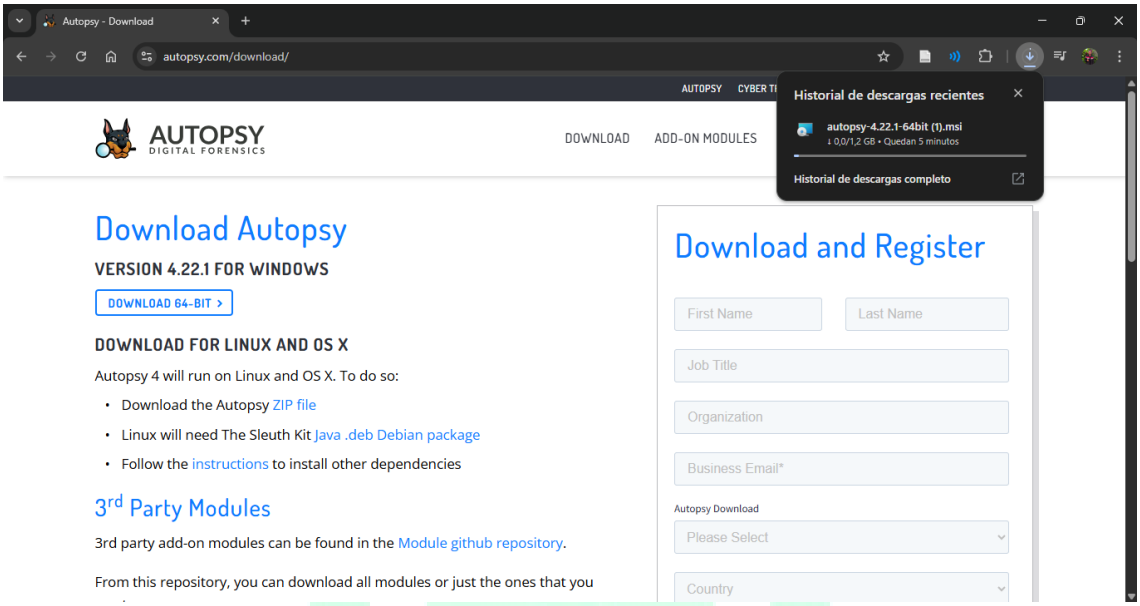


Ilustración 23. Página de Descarga de Autopsy

Captura de la página oficial de descarga de Autopsy, mostrando la versión 4.22.1 para Windows

https://www.autopsy.com/download/

5.2.2 Advertencia de Ejecución de Archivo Autopsy

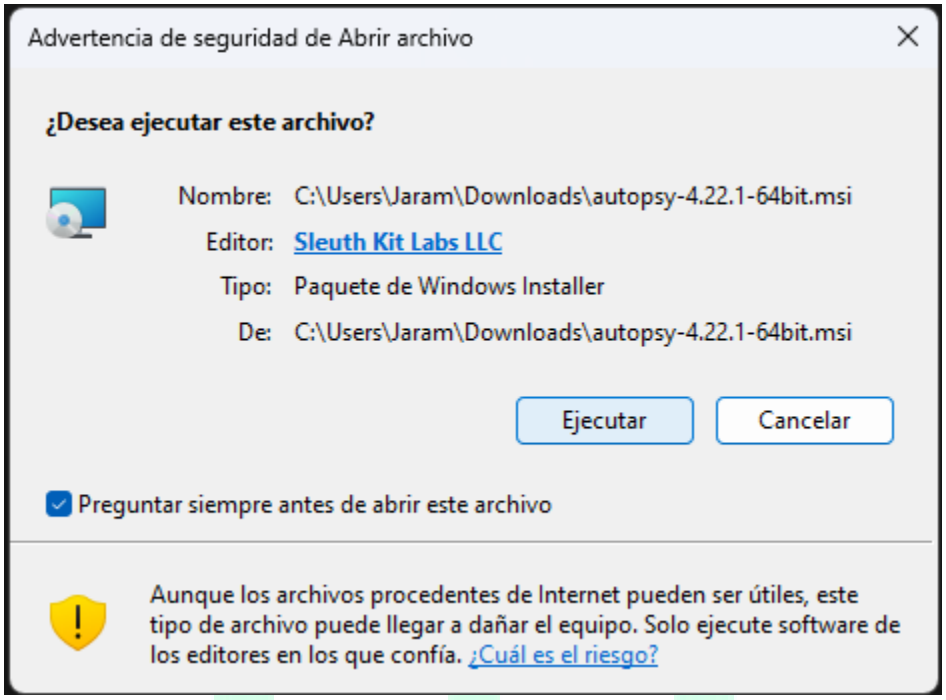


Ilustración 24. Advertencia de Seguridad Windows

Ventana de seguridad de Windows alertando sobre la ejecución del instalador de Autopsy. Solicita confirmación antes de instalar el software.

5.2.3 Inicio del Asistente de Instalación de Autopsy

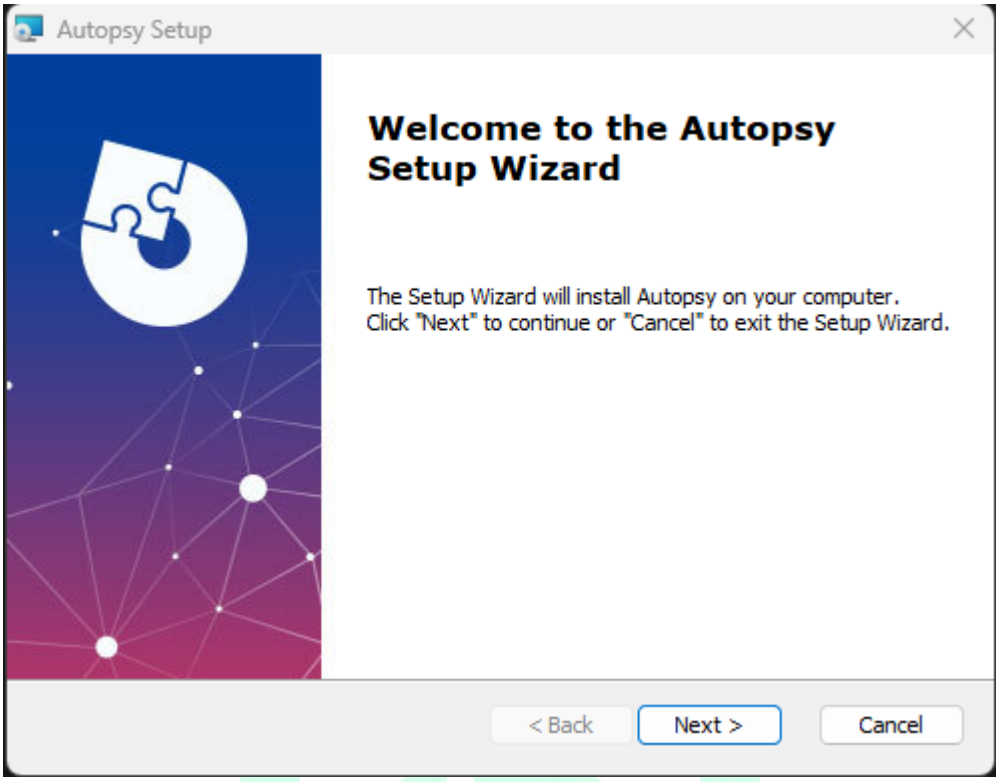


Ilustración 25. Asistente de Instalación

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

5.2.4 Configuración de Carpeta de Instalación

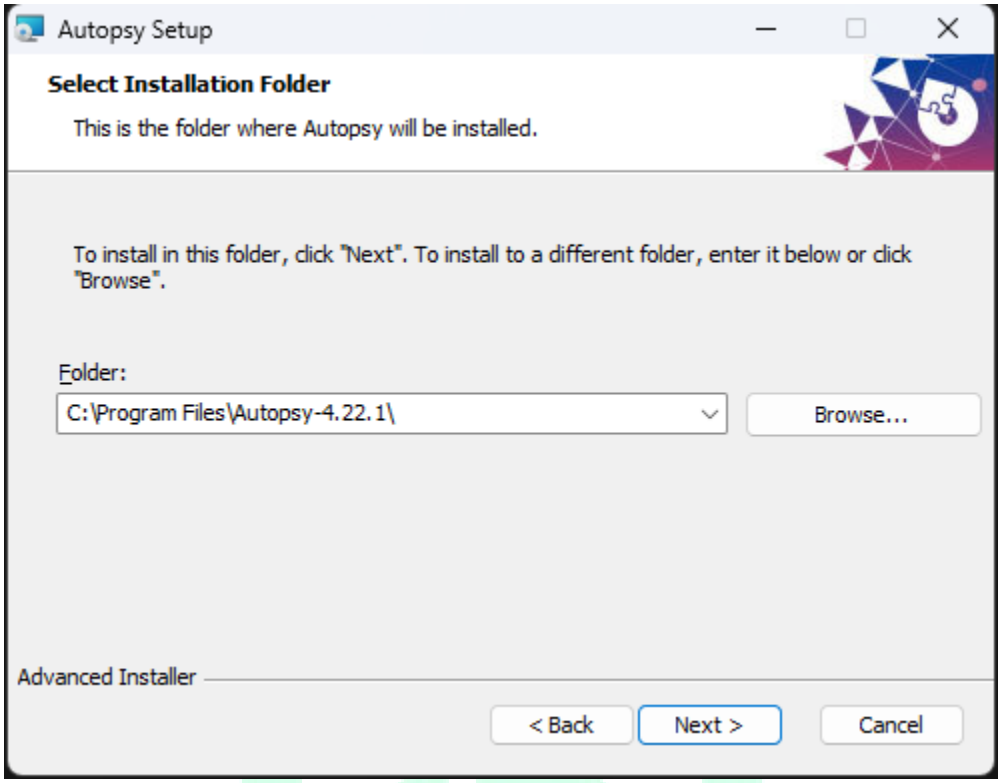


Ilustración 26. Selección de Directorio

Pantalla del instalador donde se define la ruta de instalación de Autopsy. Por defecto se instala en C:\Program Files\Autopsy-4.22.1\ pero permite cambiar la ubicación.

5.2.5 Listo para Instalar Autopsy

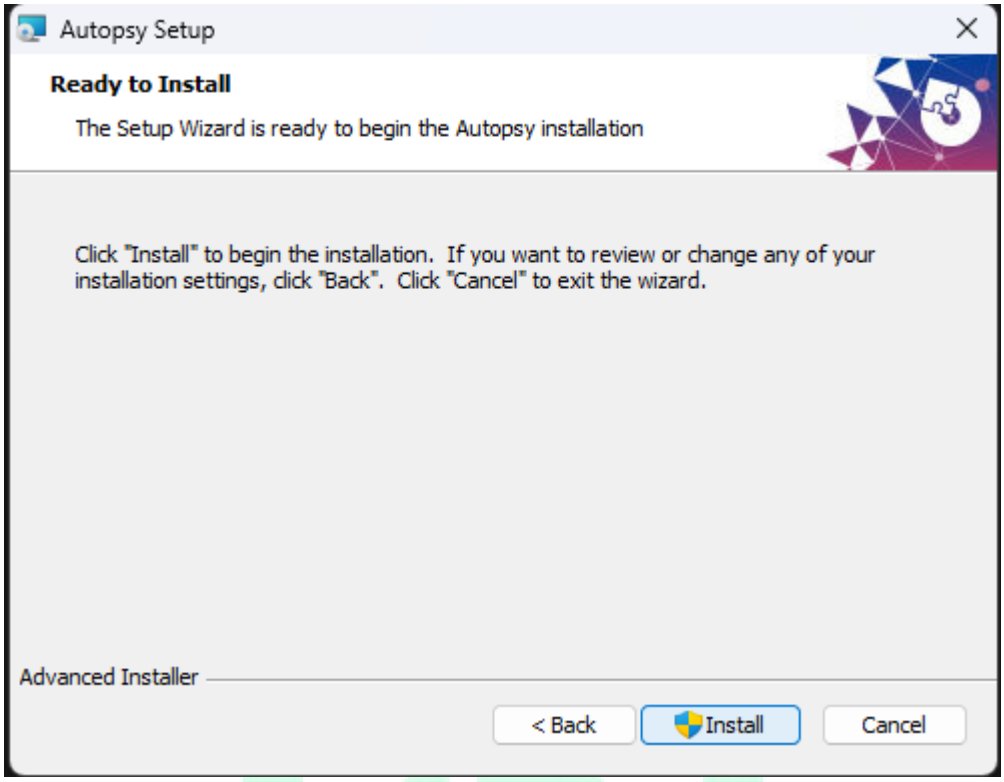


Ilustración 27. Confirmación de Instalación

Pantalla final del asistente confirmando que está listo para instalar Autopsy. Permite revisar configuraciones antes de iniciar la instalación definitiva.

5.2.6 Finalización Exitosa de la Instalación

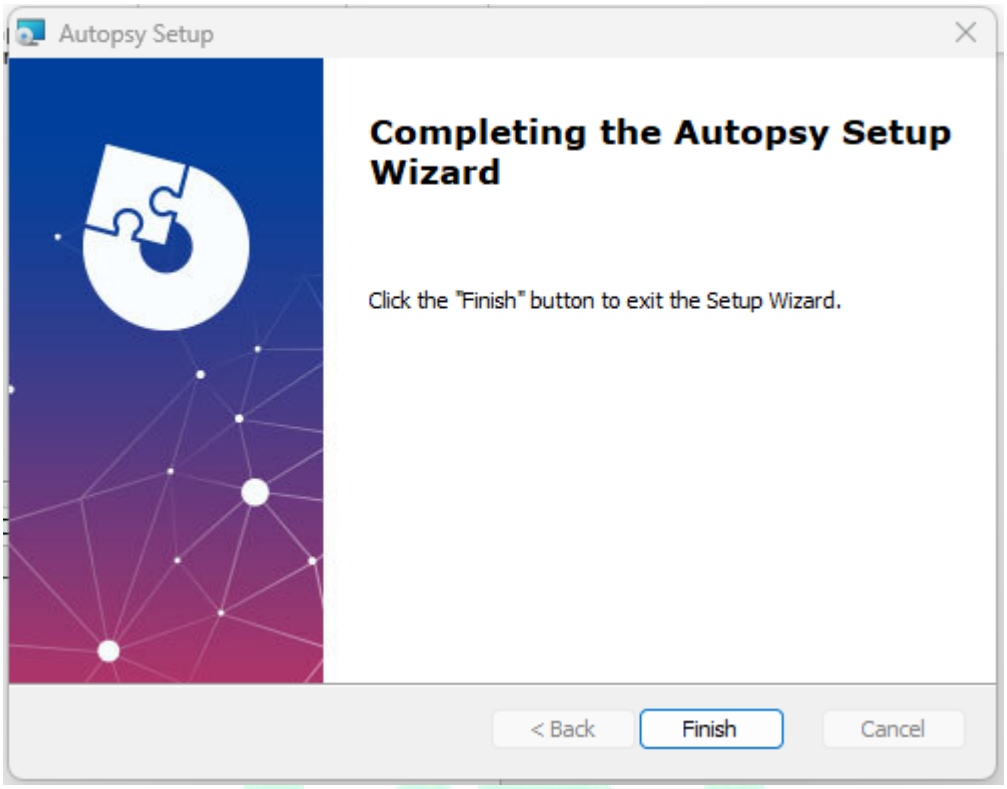


Ilustración 28. Instalación Completada

Pantalla que confirma la instalación exitosa de Autopsy. Al hacer clic en "Finish" se cierra el asistente y el programa queda listo para usar.

5.2.7 Configuración de Carpetas Compartidas

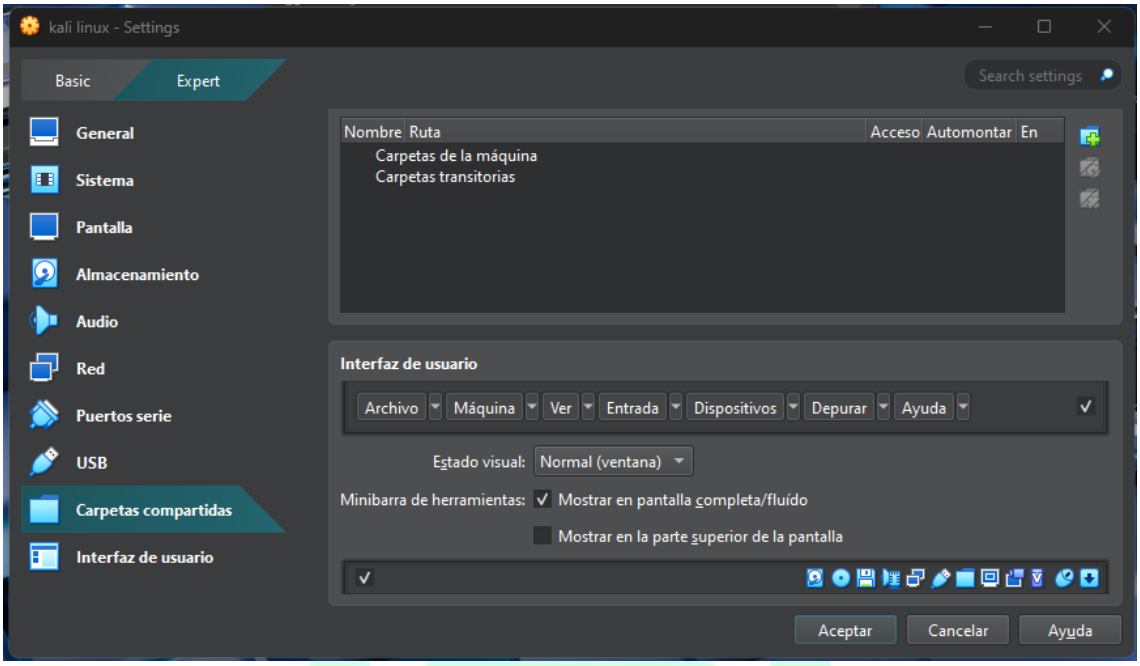


Ilustración 29. Configuración de Carpetas Compartidas

Pantalla de configuración de VirtualBox mostrando la sección de Carpetas compartidas. Desde aquí se puede definir la ruta de la carpeta compartida entre Windows y la máquina virtual para transferir archivos.

5.2.8 Creación de Carpeta en Windows

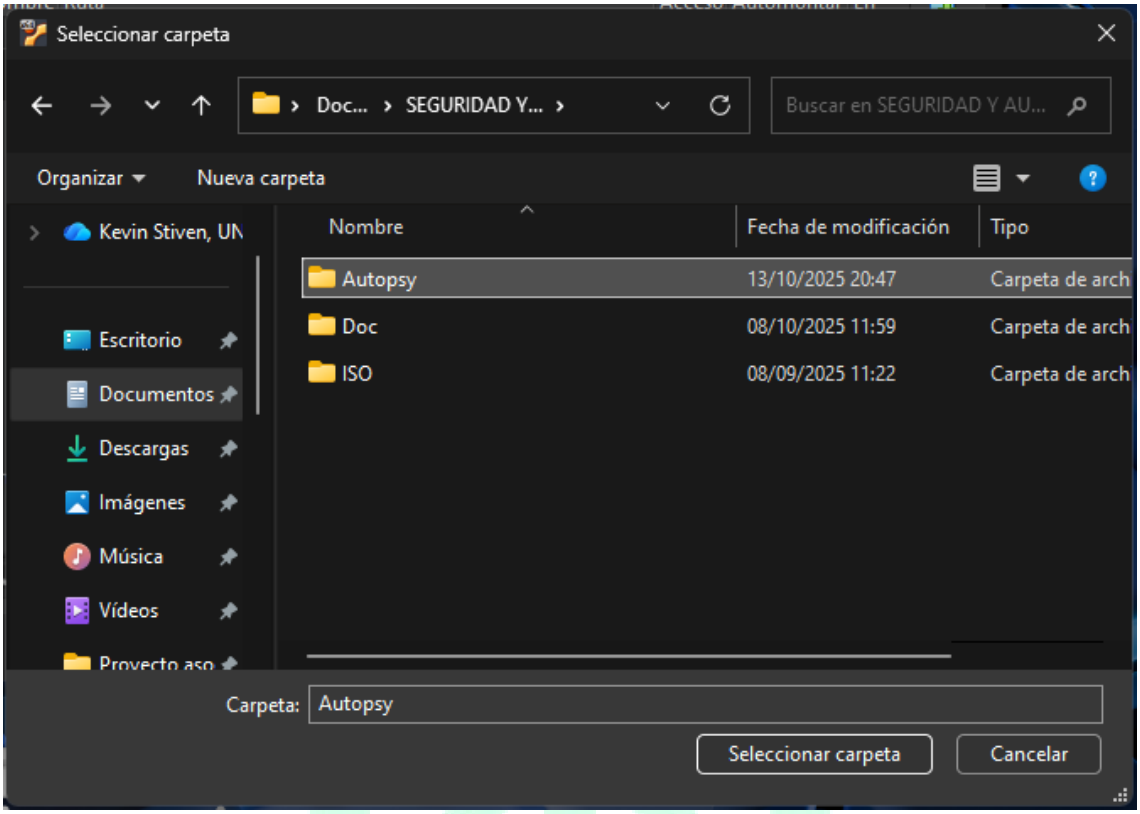


Ilustración 30. Carpeta "Autopsy" Creada

Explorador de Windows mostrando la carpeta Autopsy recién 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.

5.2.9 Agregando Carpeta Compartida

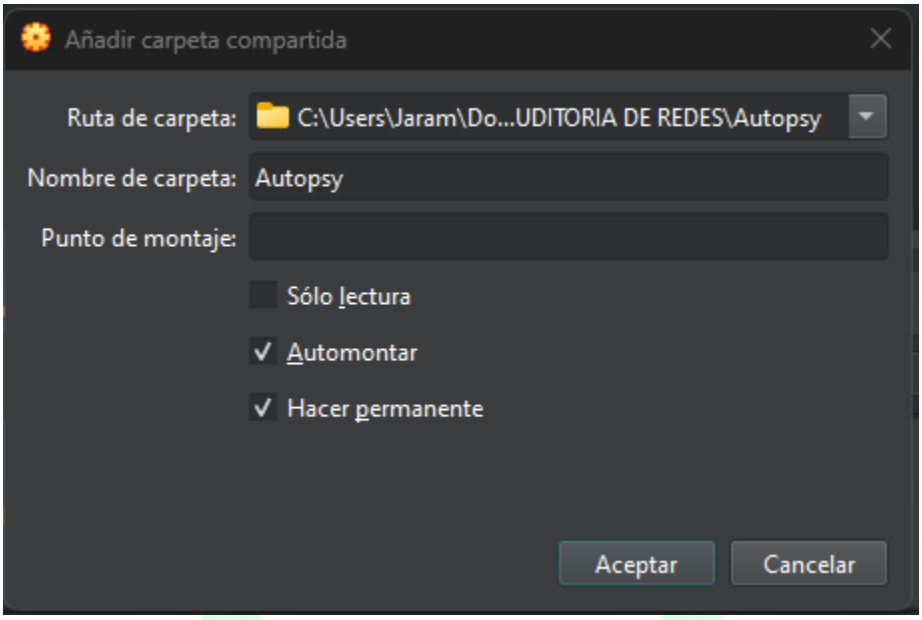


Ilustración 31. Configuración de Carpeta Compartida

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.

5.2.10 Carpeta Autopsy Correctamente Compartida

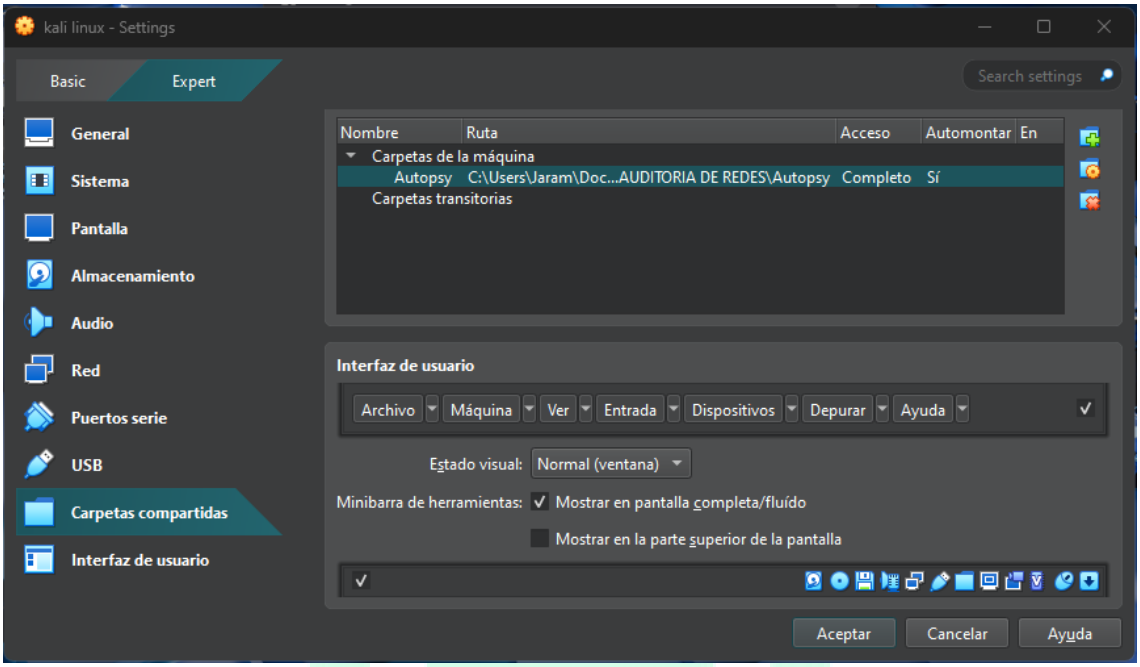


Ilustración 32. Carpeta Compartida Configurada

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.

5.2.11 Archivos Transferidos Vía Carpeta Compartida

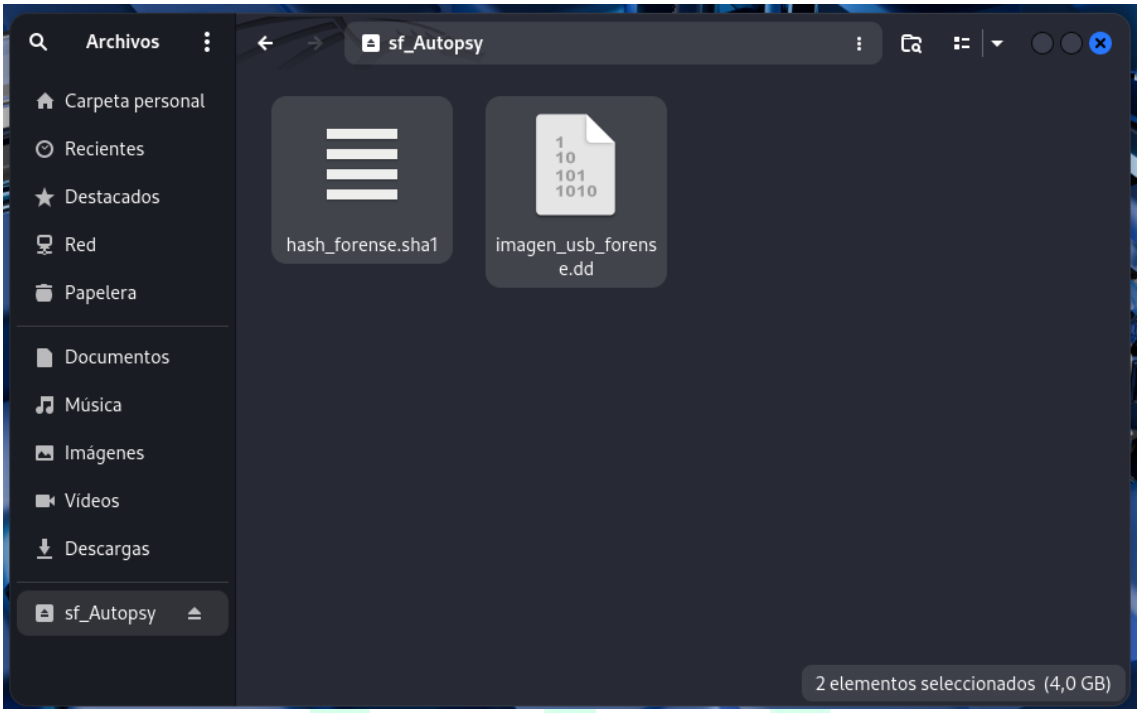


Ilustración 33. Archivos Transferidos a Windows

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

5.2.12 Archivos Disponibles en Windows

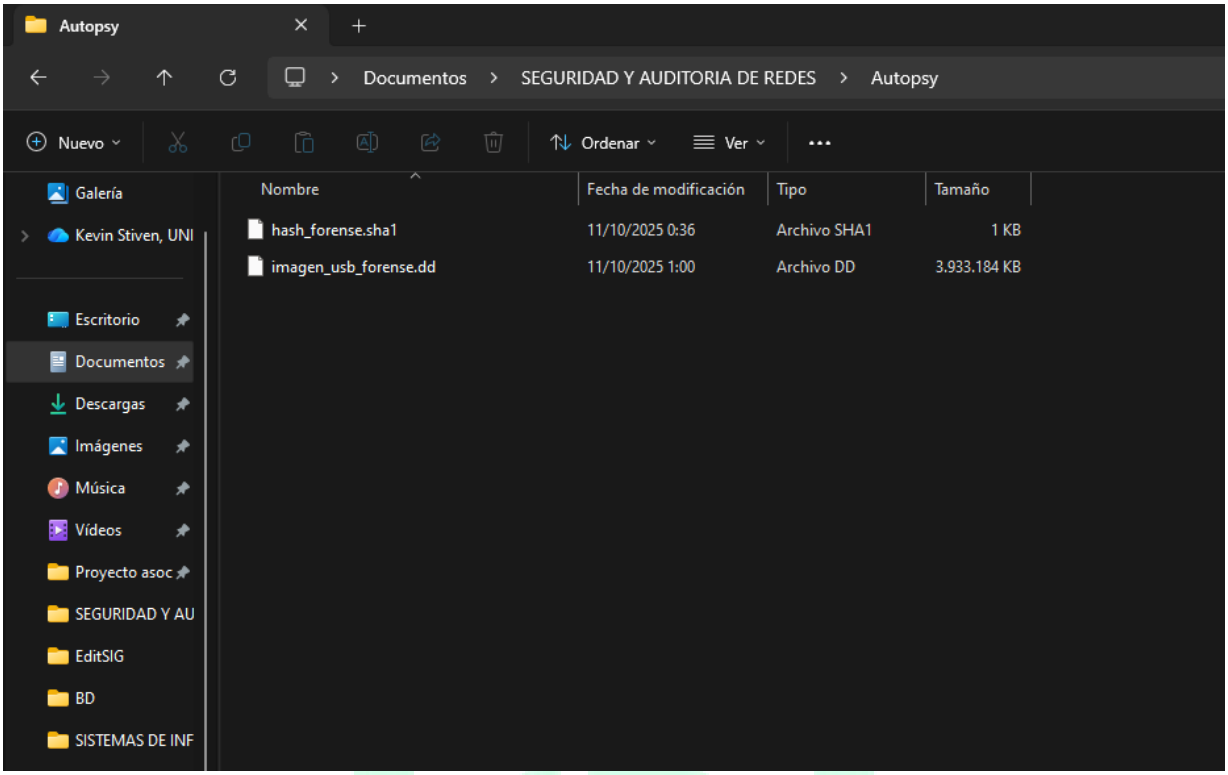


Ilustración 34. Archivos Forenses en Windows

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.

5.2.13 Pantalla de Inicio de Autopsy en Windows

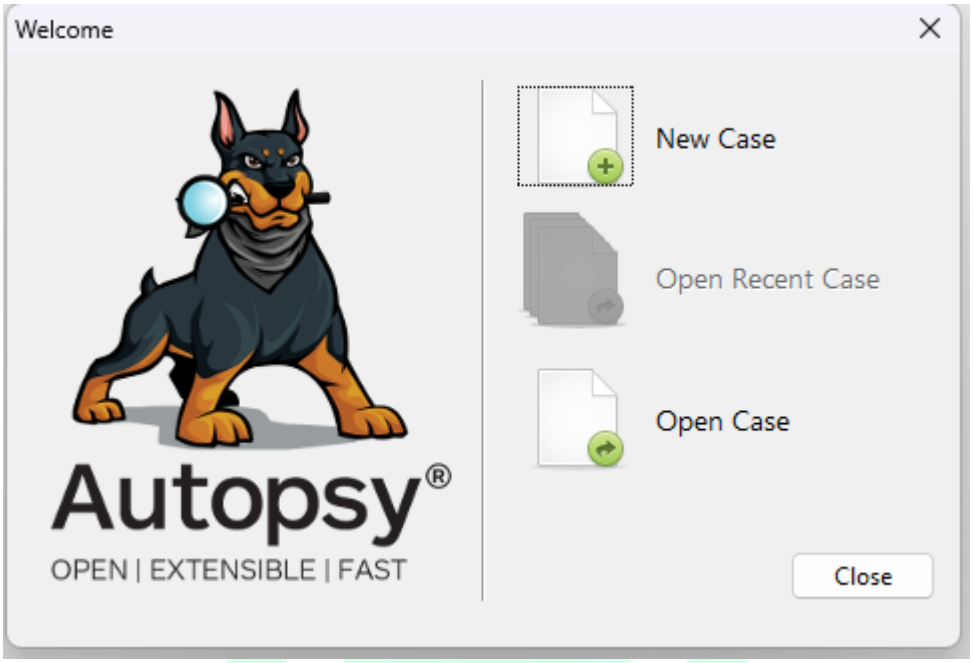


Ilustración 35. Interfaz Principal de Autopsy Windows

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.

5.2.14 Creación del Caso "Win_Analisis_forense_USB"

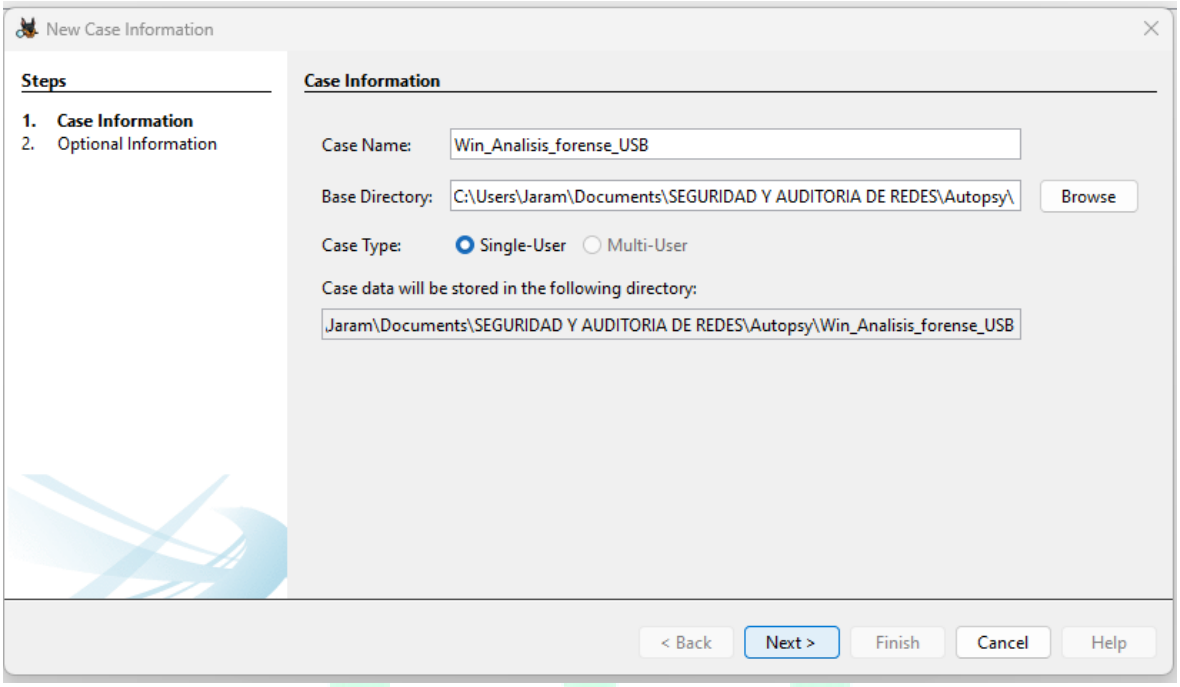


Ilustración 36. Configuración del Caso en Windows

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.

5.2.15 Metadatos del Caso Forense

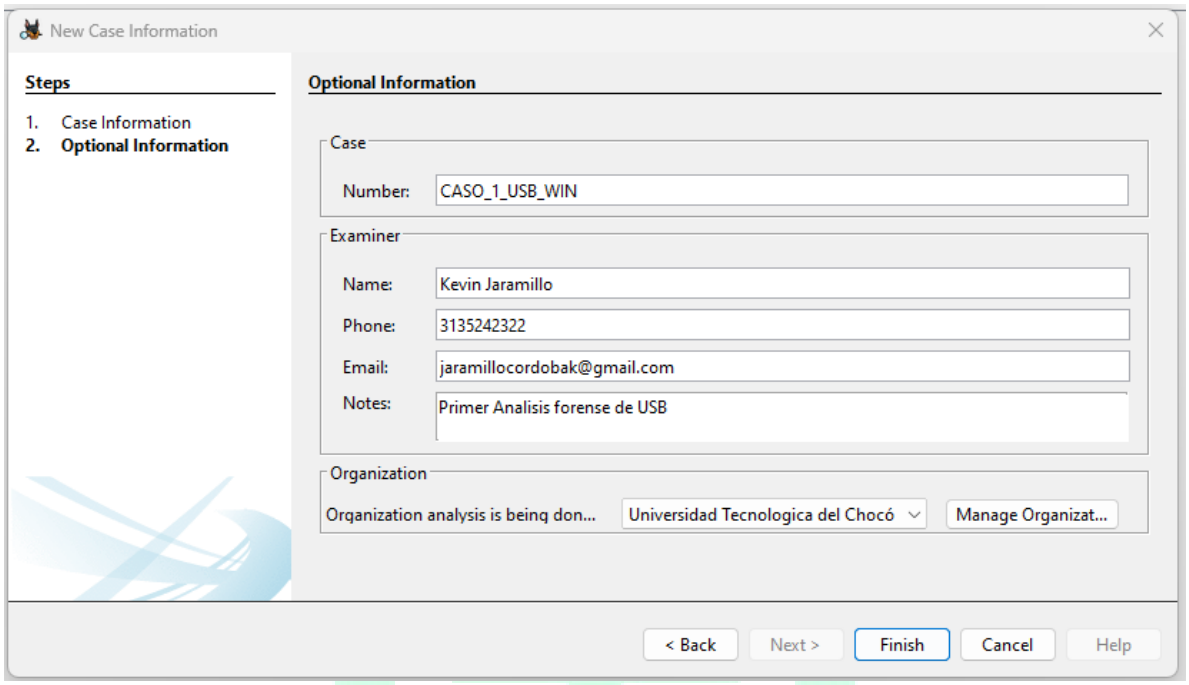


Ilustración 37. Información Adicional del Caso

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

5.2.16 Configuración de Host para Fuente de Datos

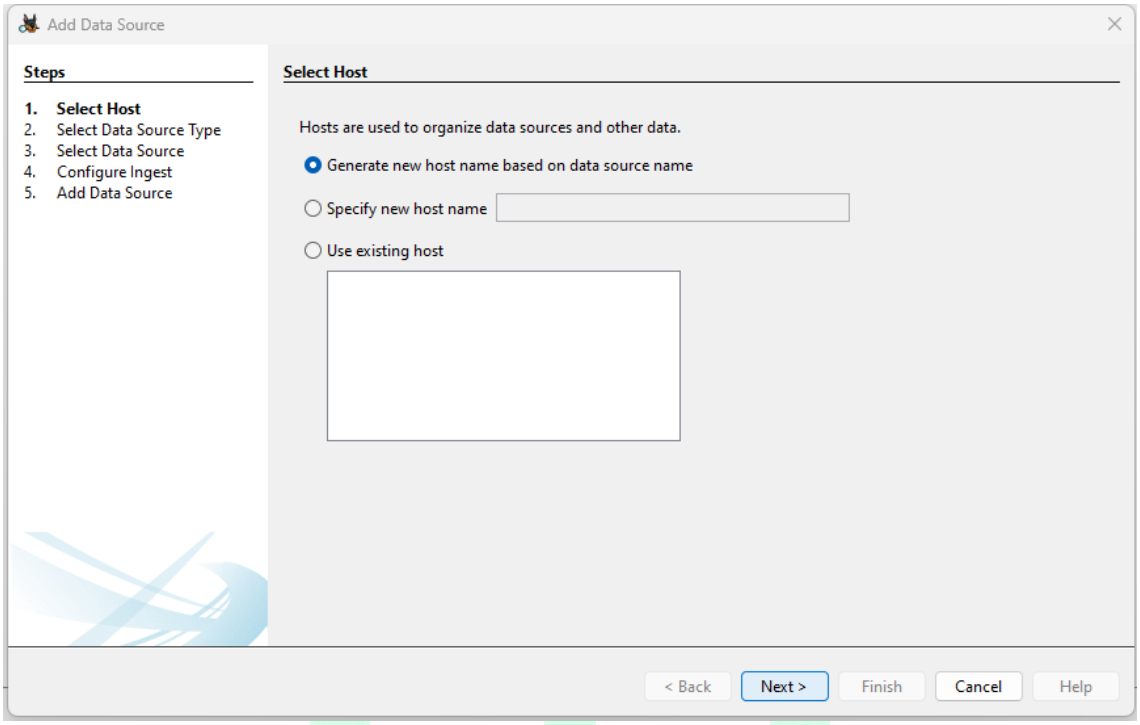


Ilustración 38. Selección de Host

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.

5.2.17 Selección de Tipo de Fuente de Datos

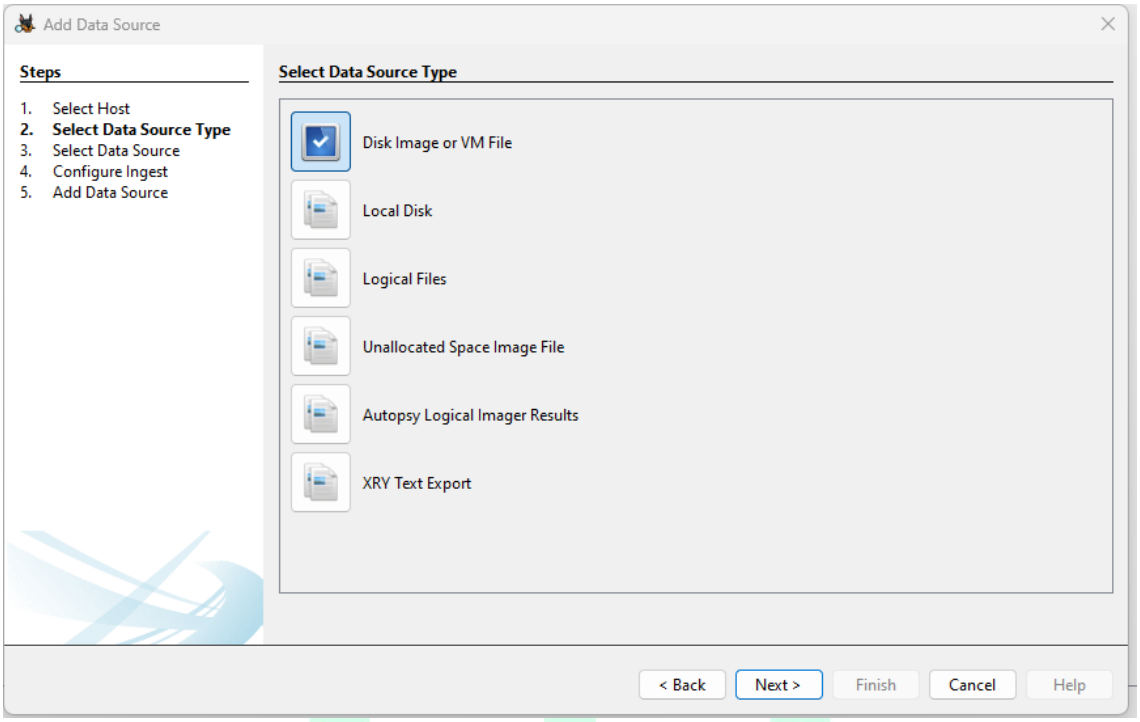


Ilustración 39. Tipo de Fuente de Datos

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.

5.2.18 Cargando Archivo de Imagen Forense .dd

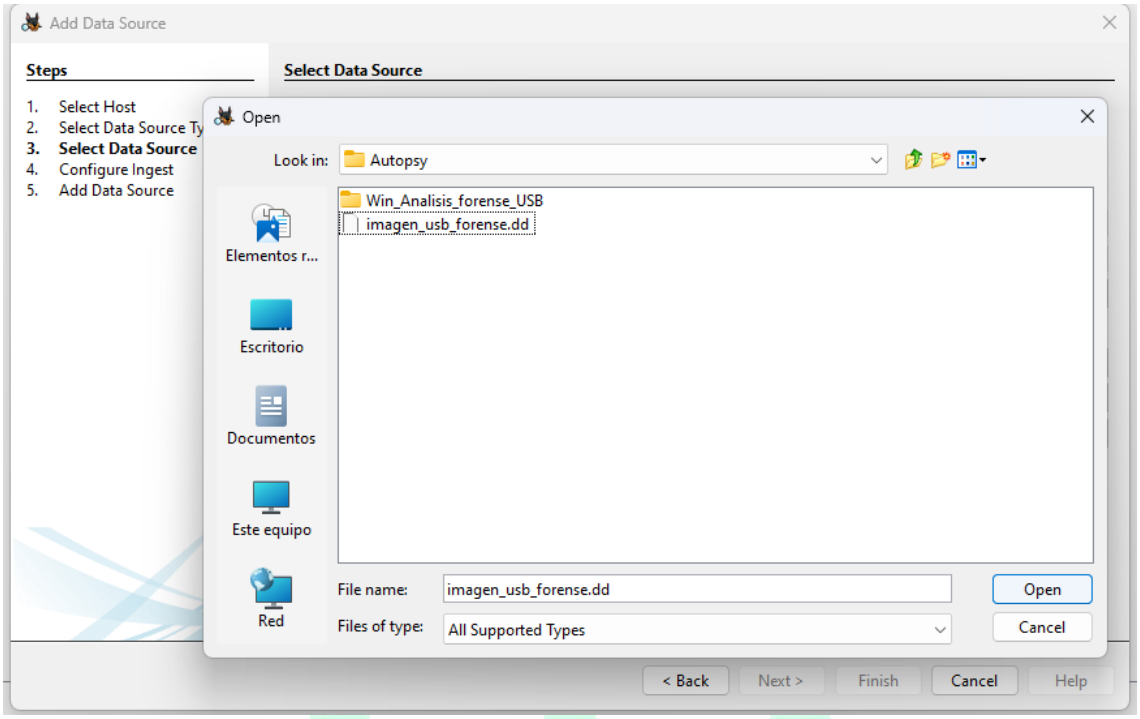


Ilustración 40. Selección de Imagen Forense

Ventana de Autopsy para seleccionar la imagen forense imagen_usb_forense.dd desde la carpeta compartida, que será analizada como fuente principal del caso.

5.2.19 Parámetros de la Imagen y Hash de Verificación

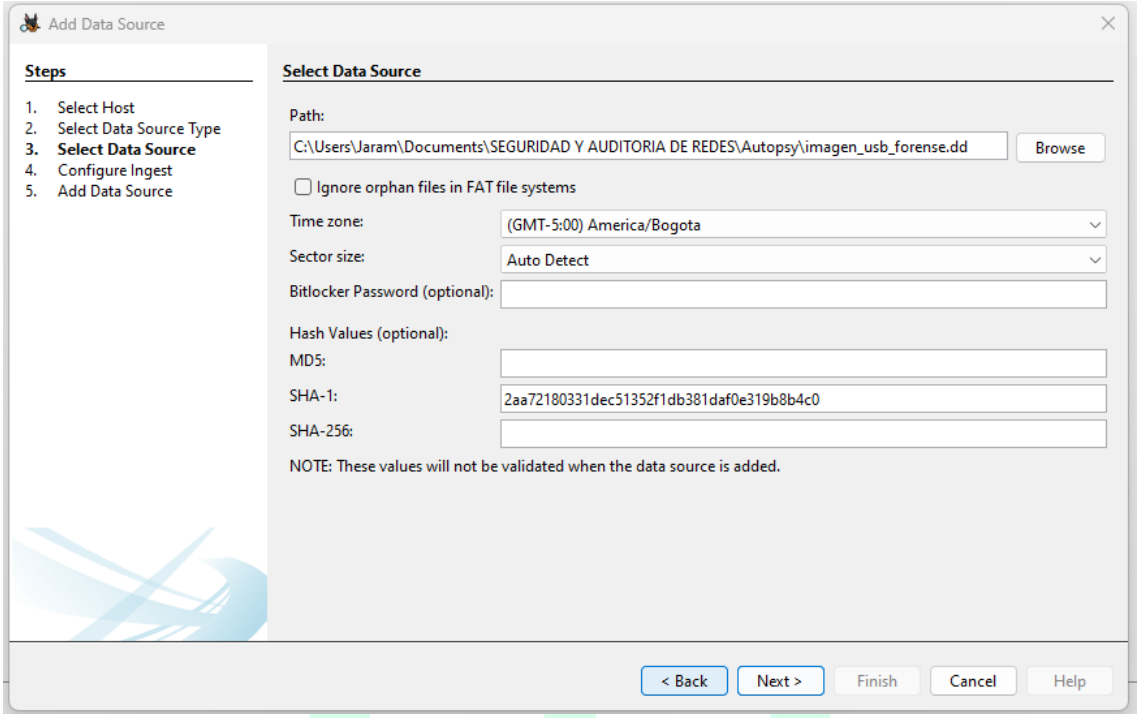


Ilustración 41. Configuración de Imagen Forense

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.

5.2.20 Selección de Módulos para Análisis

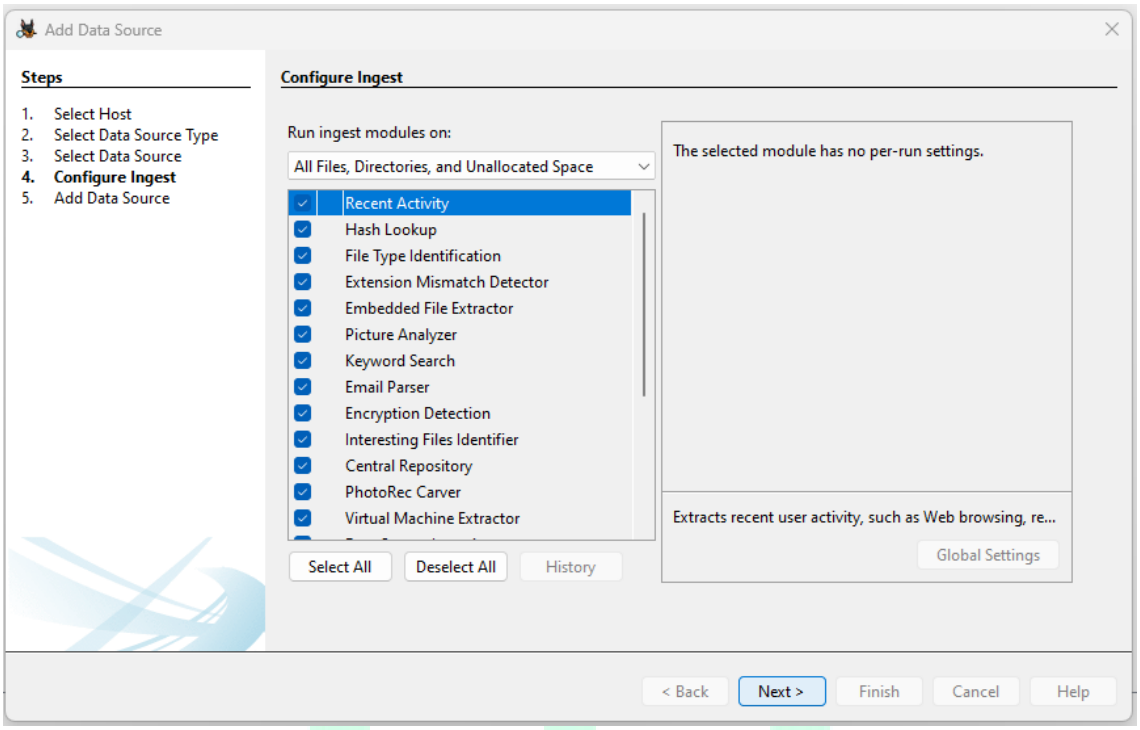


Ilustración 42. Módulos de Análisis

Pantalla de configuración de módulos de Autopsy donde se seleccionan las herramientas de análisis para examinar la imagen forense de manera automatizada.

5.2.21 Imagen Forense Cargada

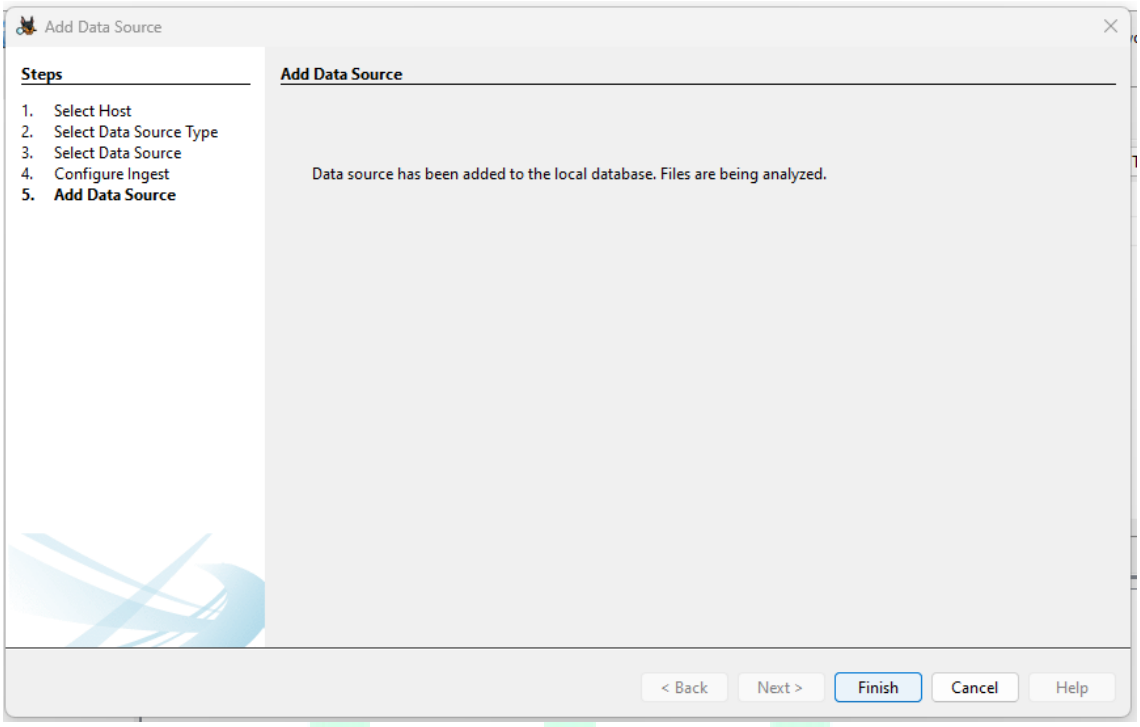


Ilustración 43. Fuente de Datos Agregada

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.

5.2.22 Interfaz de Análisis de Autopsy

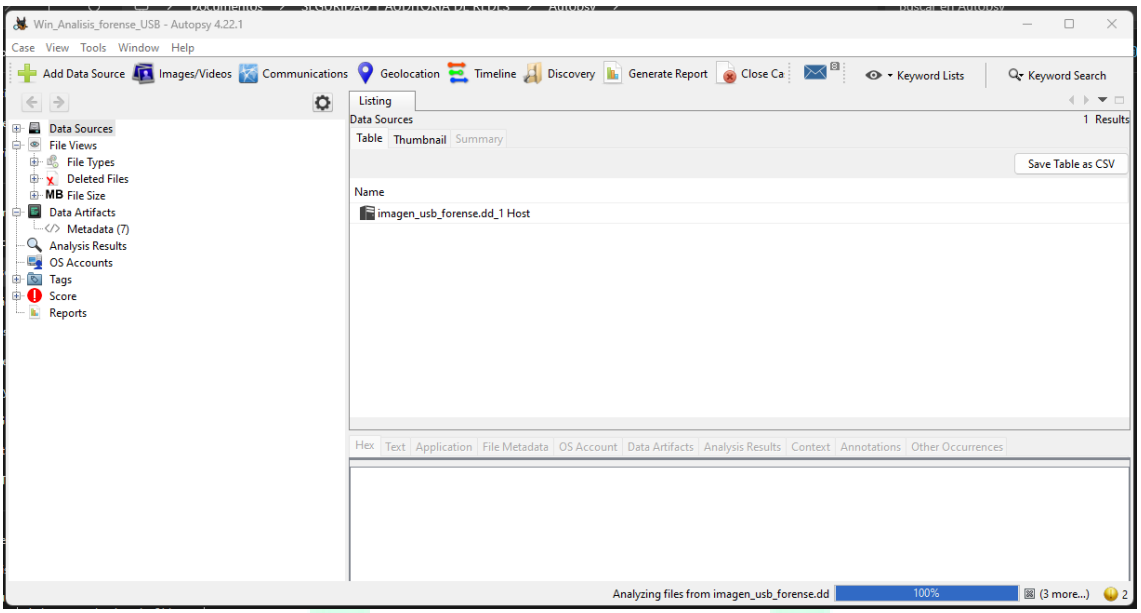


Ilustración 44. Análisis en Progreso

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

5.2.23 Archivos Recuperados de la Memoria USB

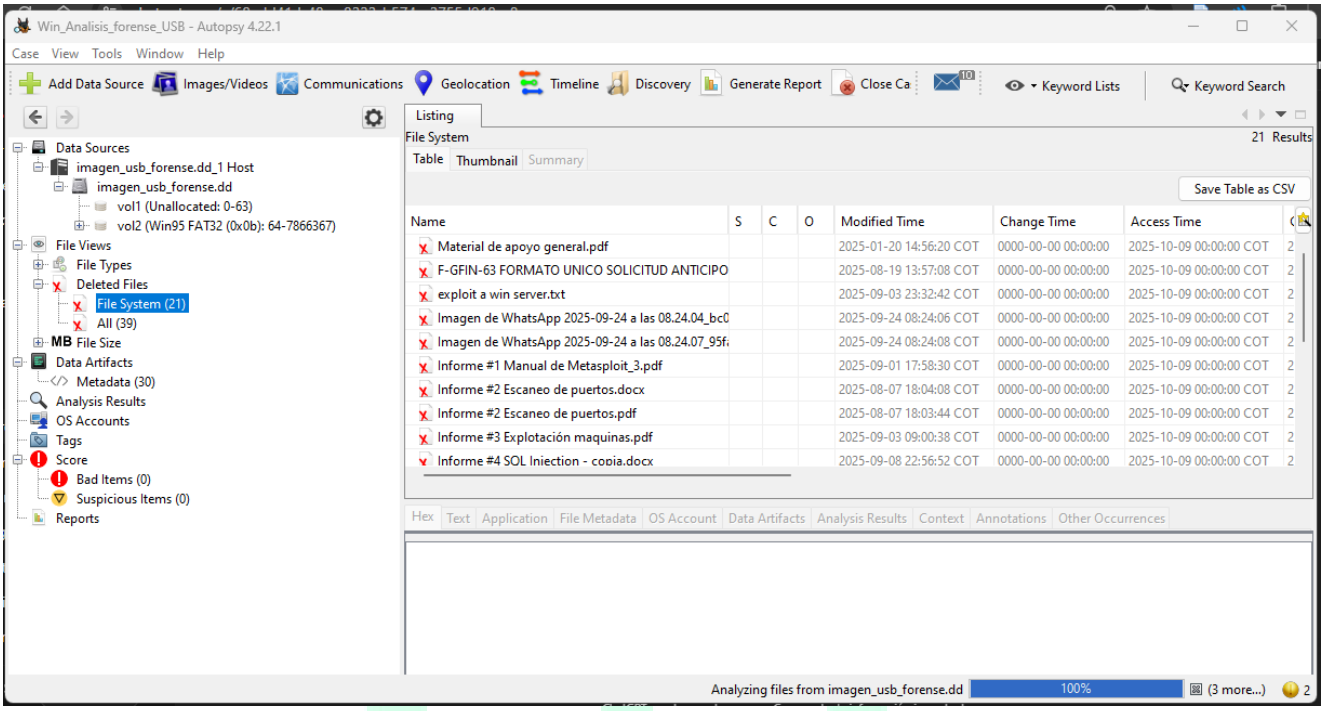


Ilustración 45. Resultados del Análisis Forense

Autopsy Windows mostrando los 39 archivos recuperados de la memoria USB, incluyendo documentos PDF, Word, imágenes de WhatsApp y archivos de texto.

5.2.24 Vista Detallada de Archivos

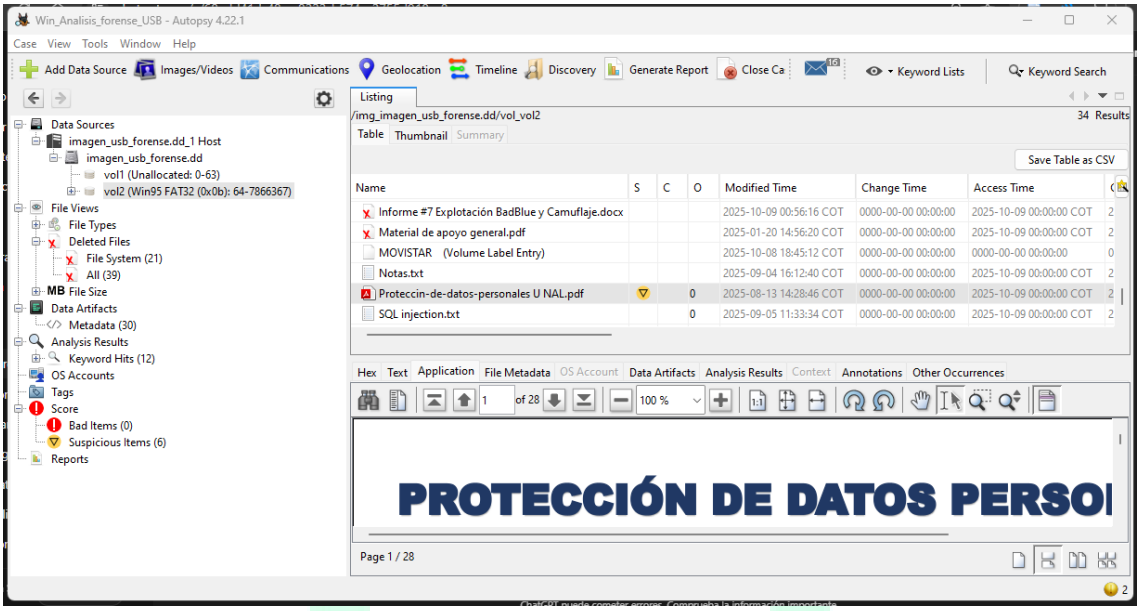


Ilustración 46. Archivos del Sistema y Resultados de Análisis

Autopsy muestra archivos del sistema recuperados, incluyendo documentos de informes, archivos PDF y notas. Se detectaron elementos sospechosos de archivos.

5.2.25 Extracción de Archivos desde la Imagen Forense

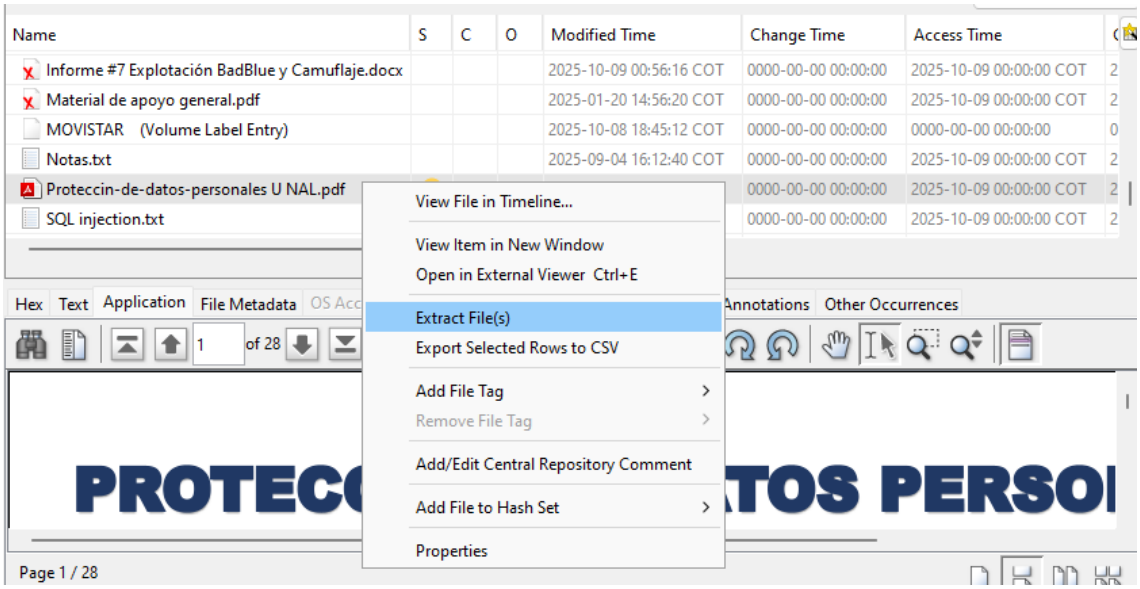


Ilustración 47. Exportación de Archivos Recuperados

Menú contextual de Autopsy mostrando la opción Extract File(s) para exportar archivos recuperados de la imagen forense.

5.2.26 Exportación de Archivo PDF Recuperado

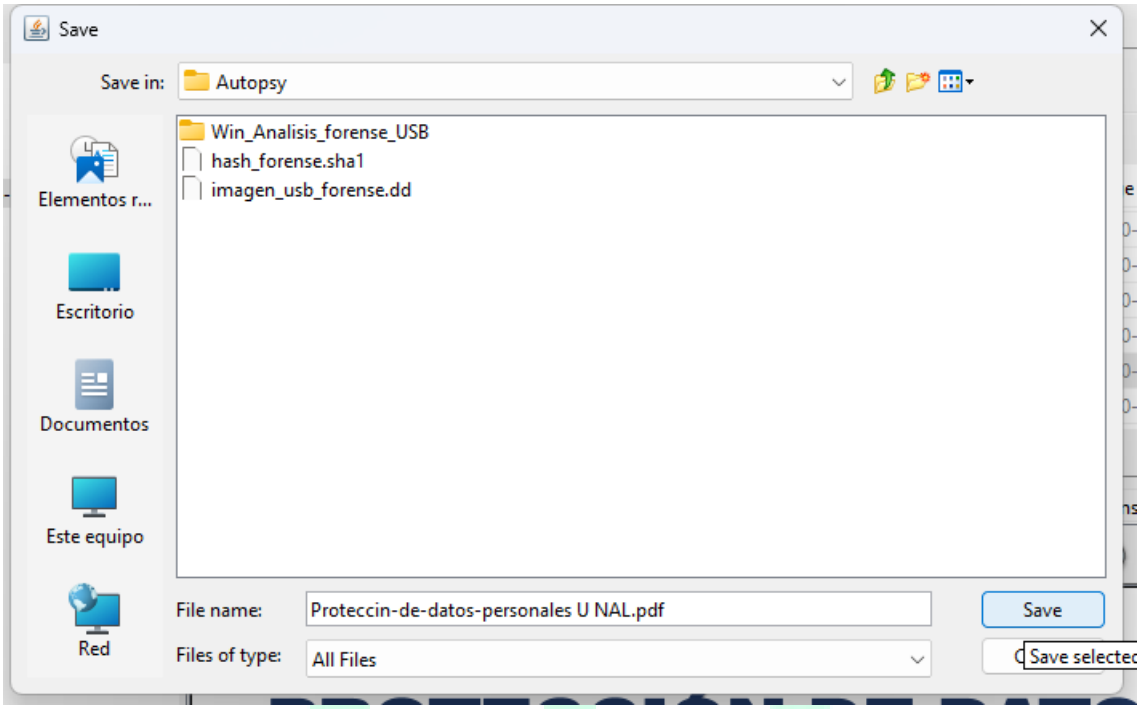


Ilustración 48. Guardando Archivo Extraído

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.

5.2.27 Archivo Exportado Correctamente

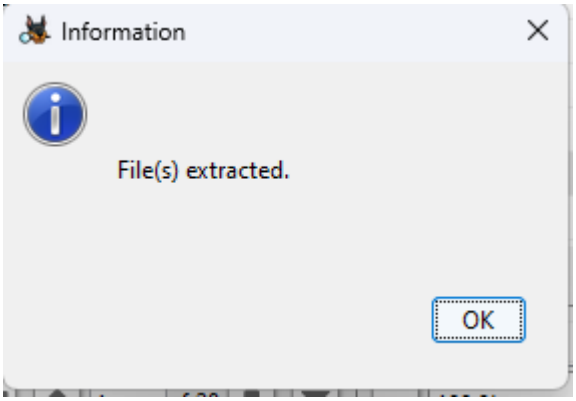


Ilustración 49. Extracción Exitosa

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.

5.2.28 PDF Recuperado Exitosamente de la Imagen

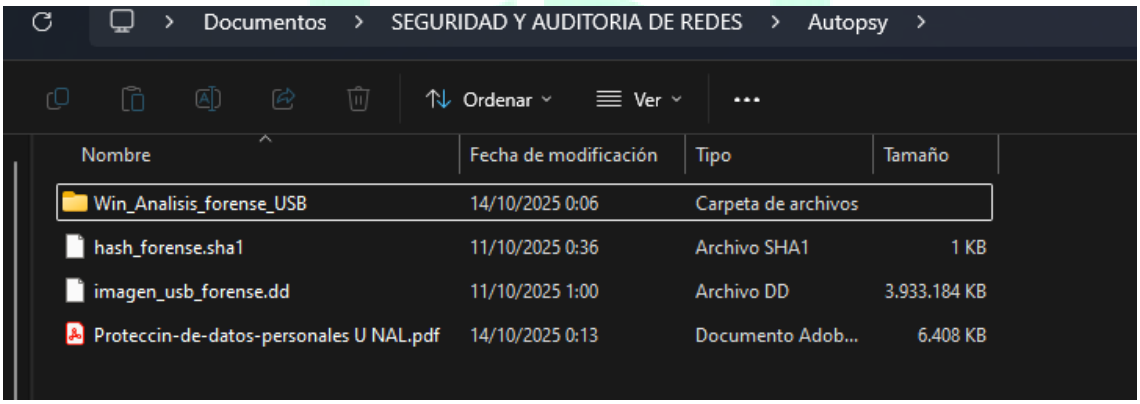


Ilustración 50. Archivo Extraído Confirmado

Explorador de Windows mostrando el archivo "Proteccion-de-datos-personales U NAL.pdf"extraído exitosamente de la imagen forense.

5.3.Capitulo #3

5.3.1 Descarga de FTK Imager

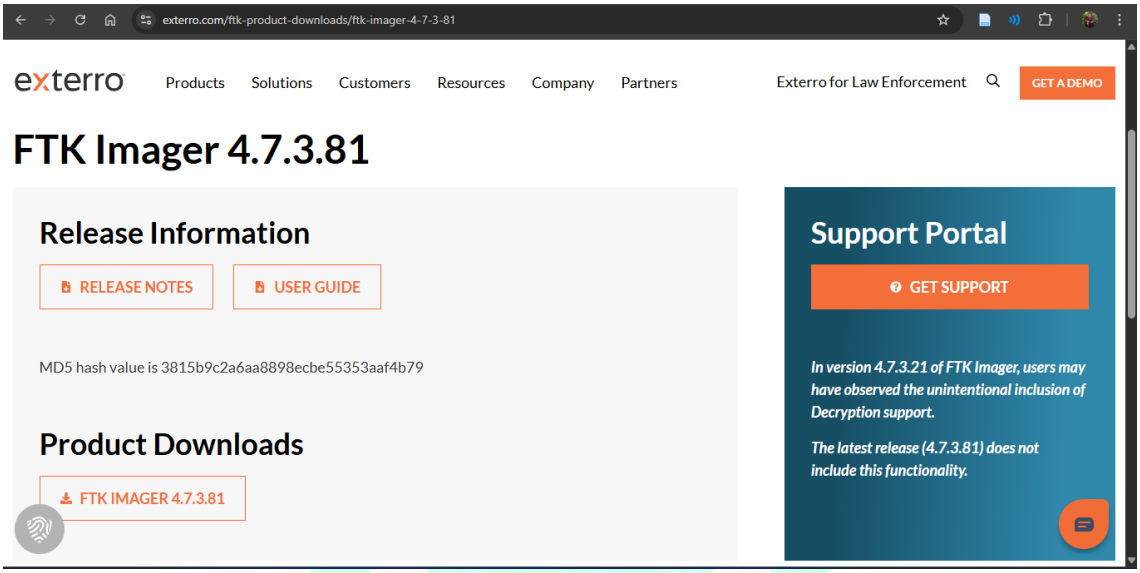


Ilustración 51. Página de Descarga de FTK Imager

Página oficial de Exterro para descargar FTK Imager 4.7.3.81, herramienta profesional para creación de imágenes forenses.

5.3.2 Formulario de Registro para FTK Imager

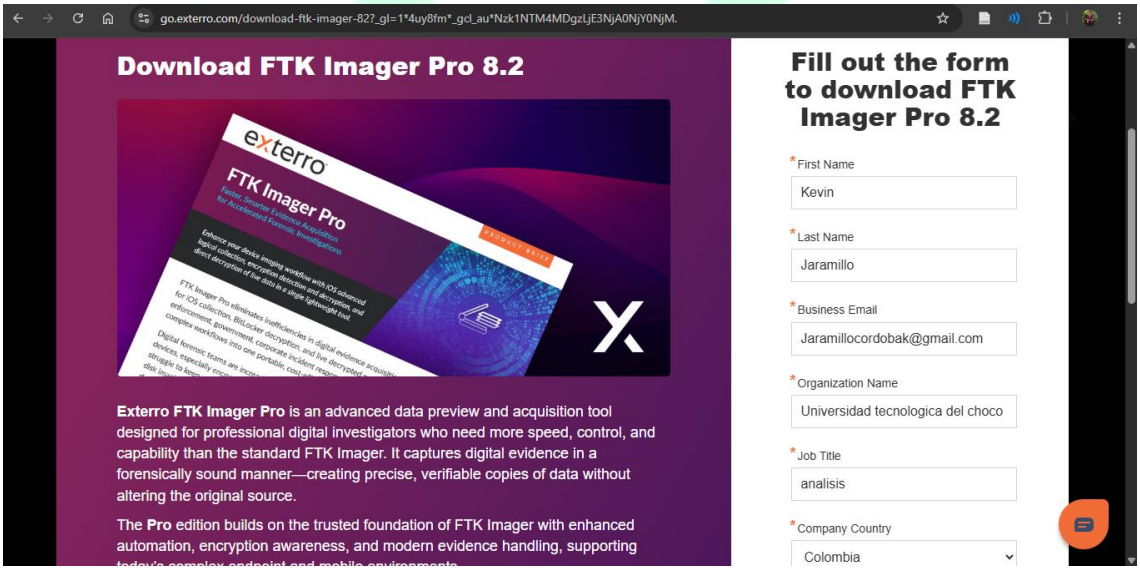


Ilustración 52. Descarga de FTK Imager Pro

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.

5.3.3 Confirmación de Descarga de FTK Imager

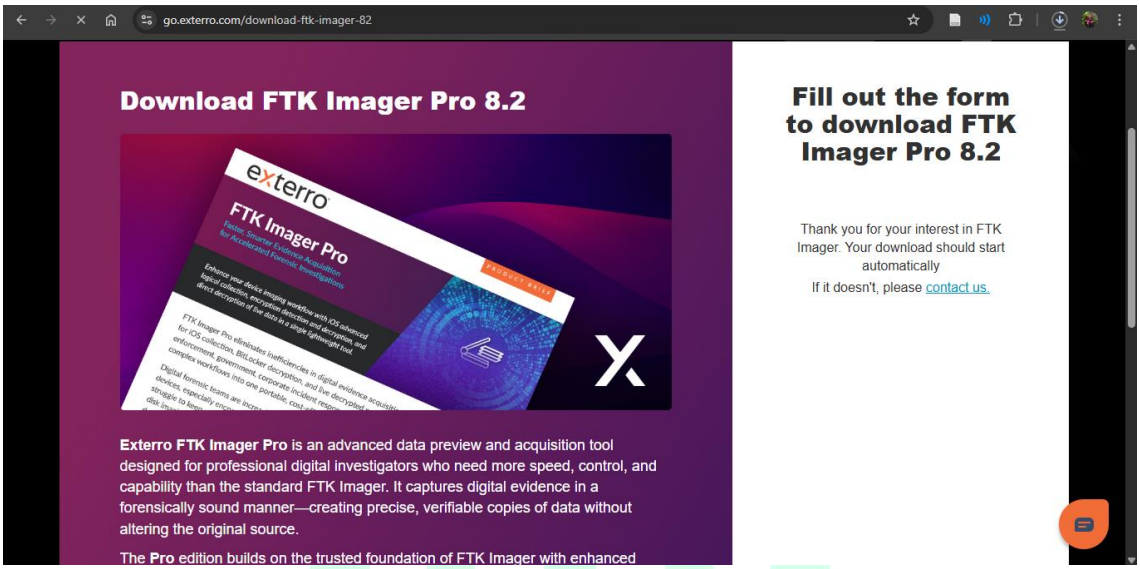


Ilustración 53. Descarga Exitosa FTK Imager

Mensaje de éxito confirmando que la descarga de FTK Imager Pro 8.2 ha comenzado automáticamente.

5.3.4 Descompresión del Instalador de FTK Imager

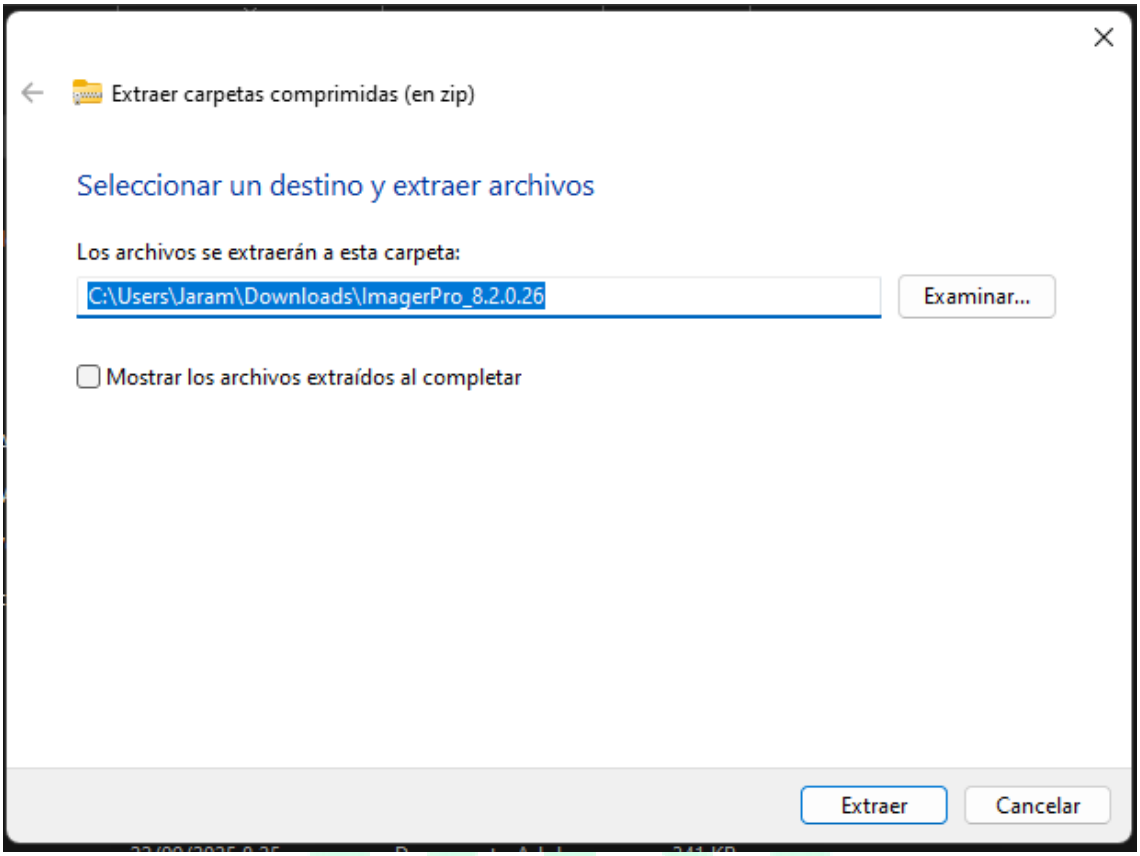


Ilustración 54. Extracción de Archivos de FTK Imager

Ventana de extracción de archivos comprimidos de FTK Imager en la carpeta de Descargas, preparando los archivos necesarios para la instalación del software forense.

5.3.5 Instalación de CodeMeter Runtime para FTK Imager

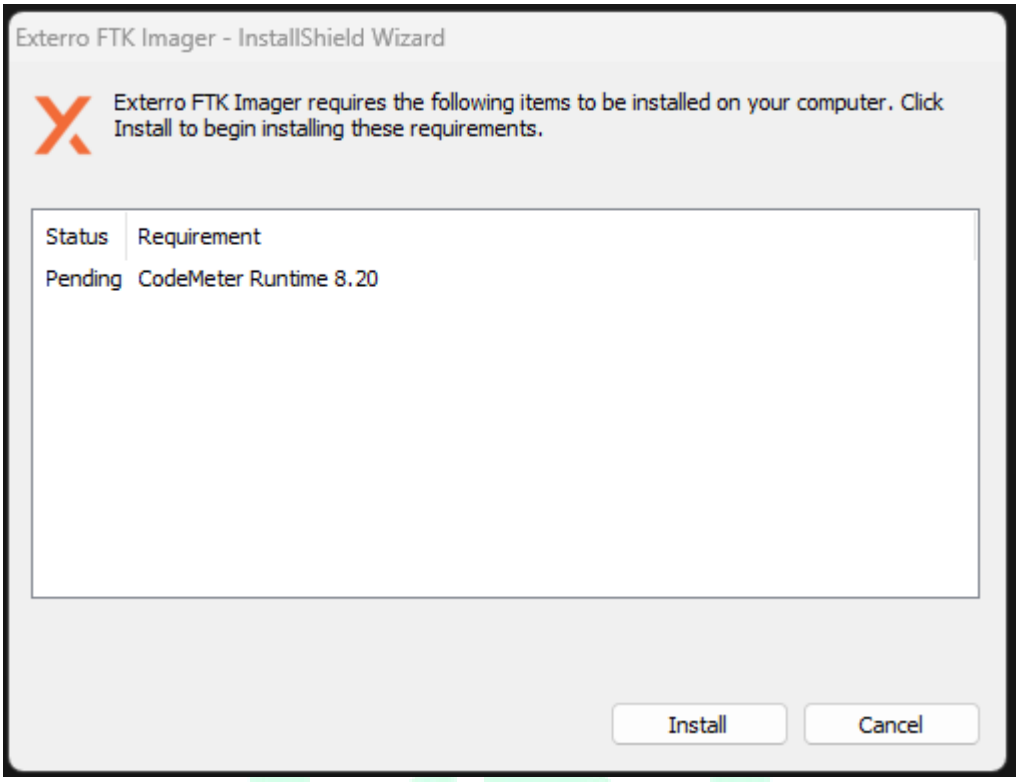


Ilustración 55. Requisitos del Sistema

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

5.3.6 Inicio del Instalador de Exterro FTK Imager

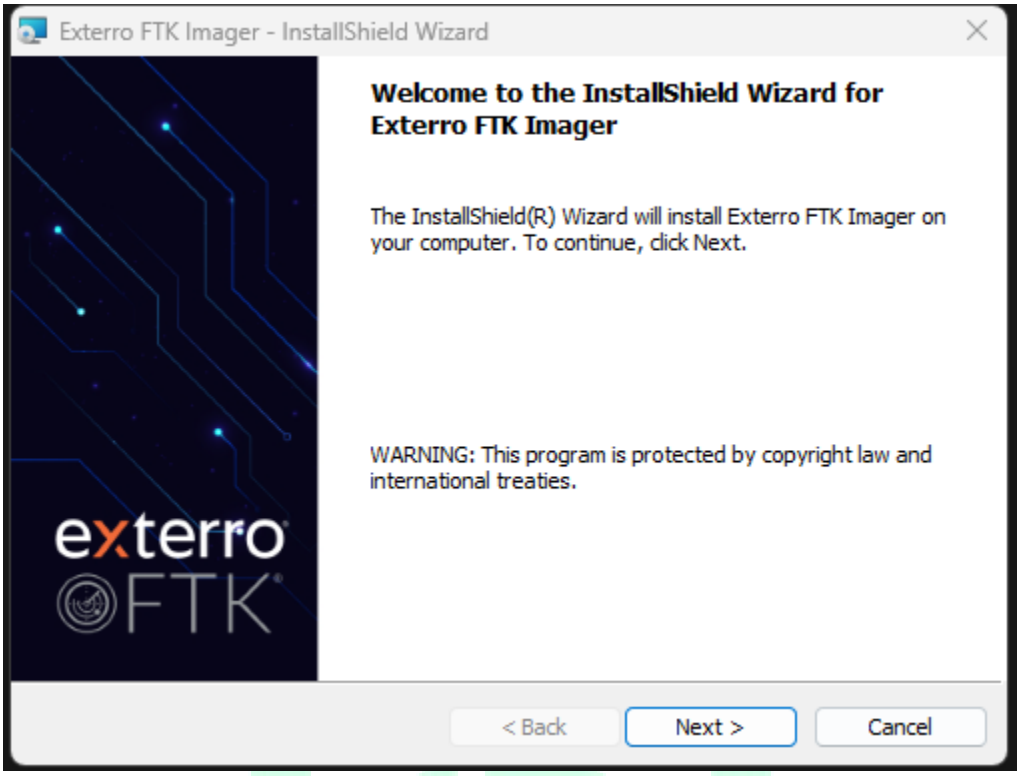


Ilustración 56. Asistente de Instalación FTK Imager

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.

5.3.7 Aceptación de licencia de FTK Imager

Ilustración 57. Acuerdo de Licencia

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.

5.3.8 Configuración de Ruta de Instalación de FTK Imager

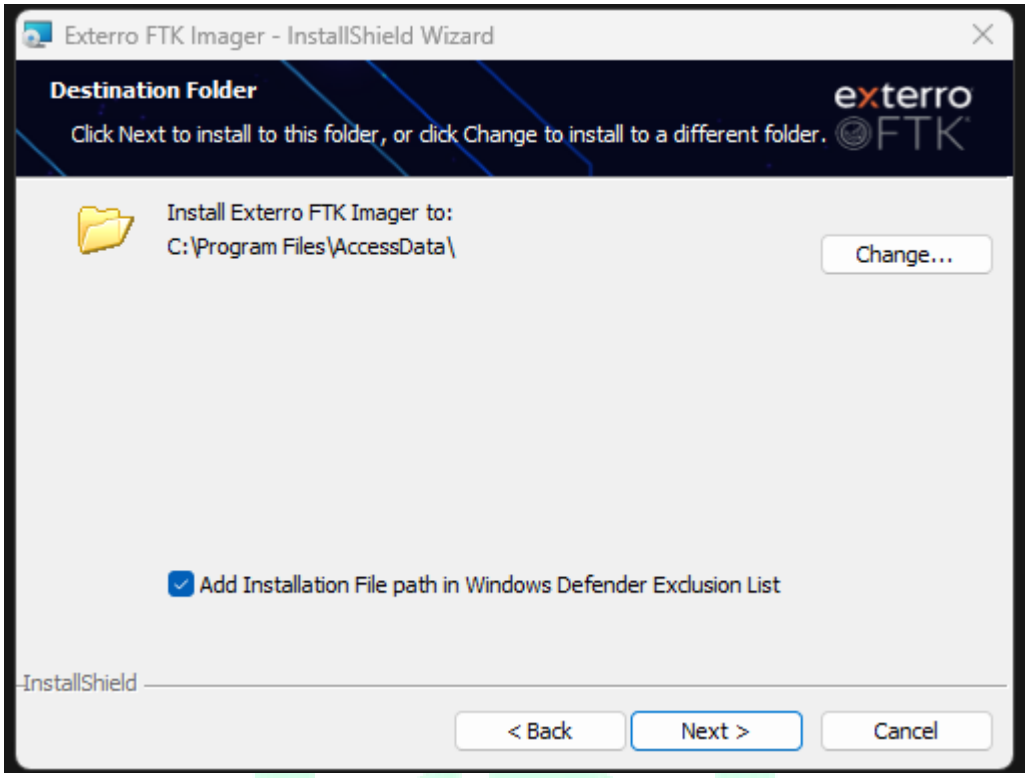


Ilustración 58. Carpeta de Destino

Pantalla de 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.

5.3.9 Confirmación Final de Instalación de FTK Imager

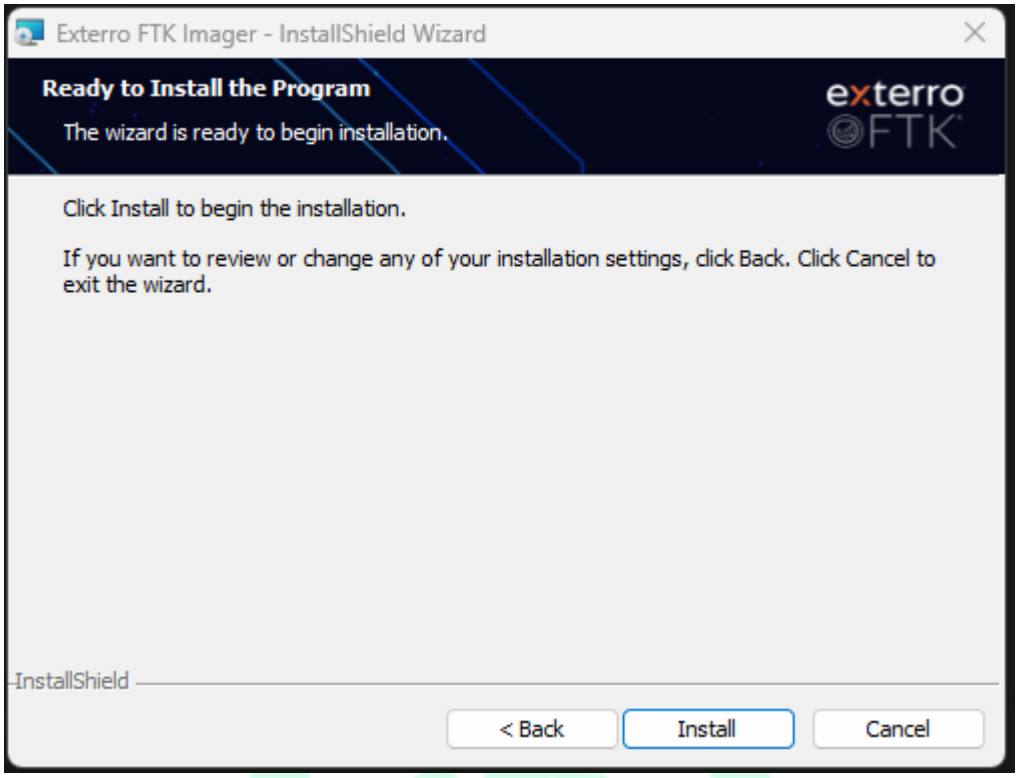


Ilustración 59. Listo para Instalar

Pantalla final del asistente confirmando que está listo para instalar FTK Imager.

5.3.10 Finalización Exitosa de la Instalación

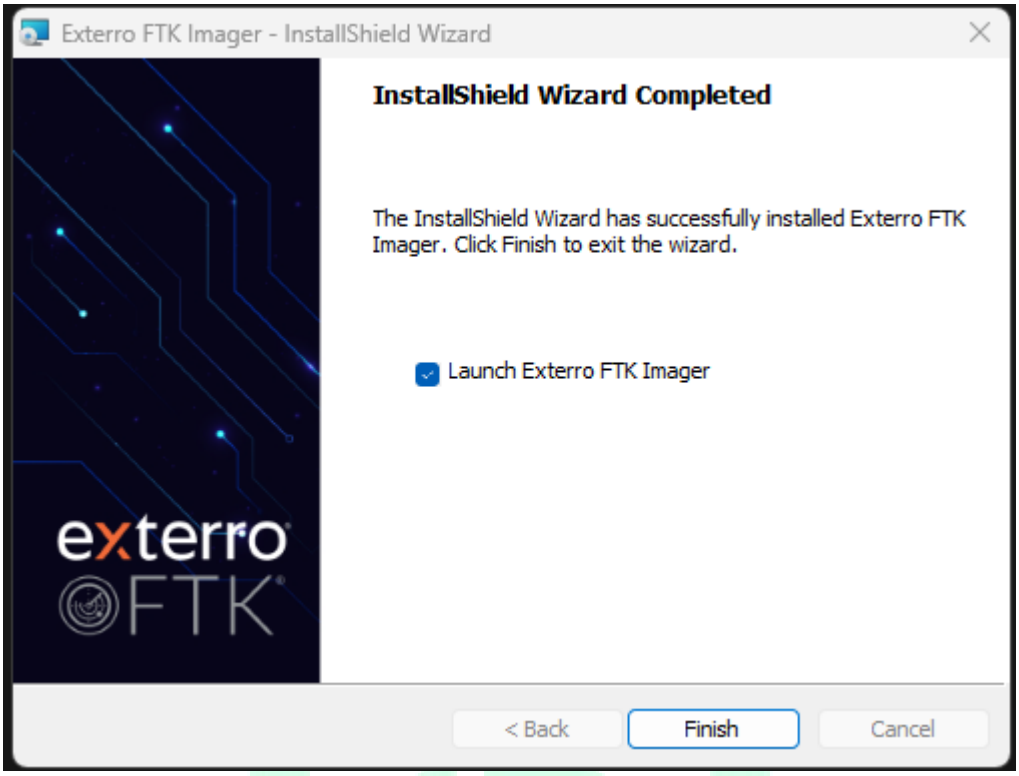


Ilustración 60. Instalación Completada

Mensaje de confirmación de 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.

5.3.11 FTK Imager Listo para Crear Imagen

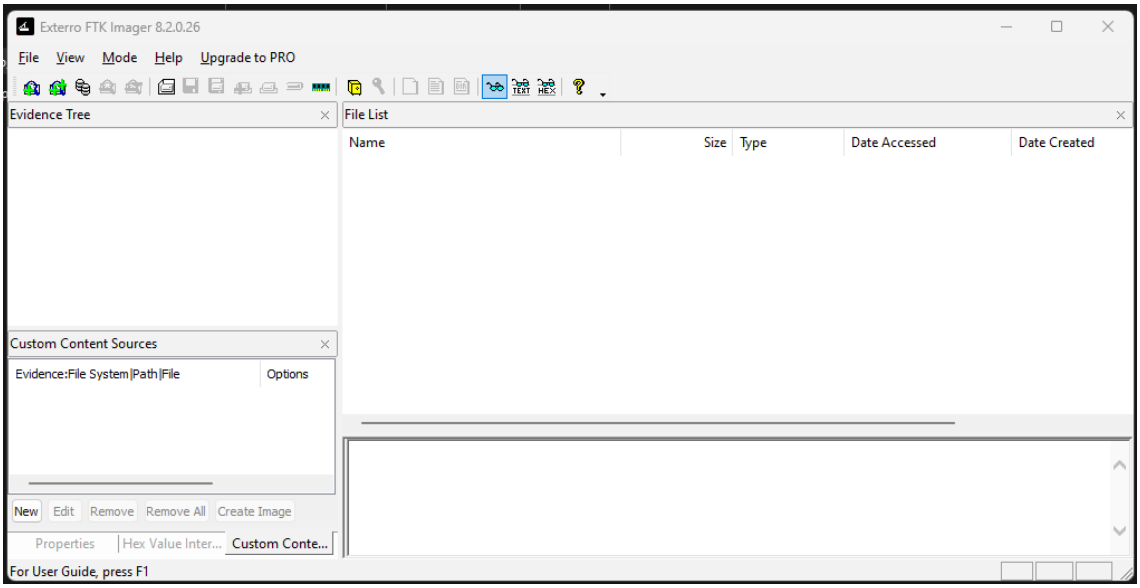


Ilustración 61. Interfaz Principal FTK Imager

Interfaz principal de FTK Imager mostrando el árbol de evidencia y opciones para crear nuevas imágenes forenses.

5.3.12 Configuración de Fuente de Evidencia

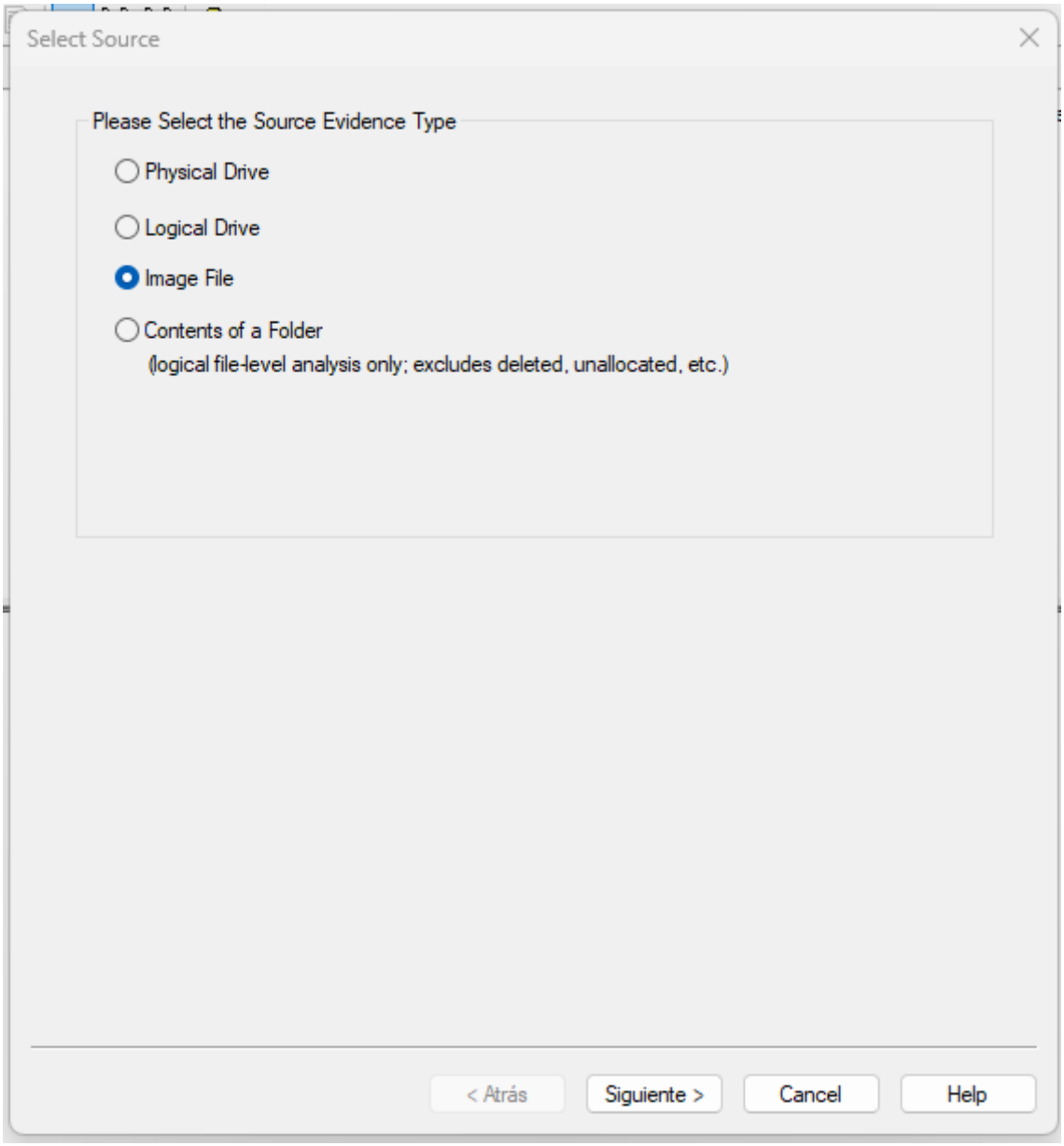


Ilustración 62. Selección de Tipo de Fuente

Ventana de 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.

5.3.13 Cargando Archivo de Imagen DD en FTK Imager

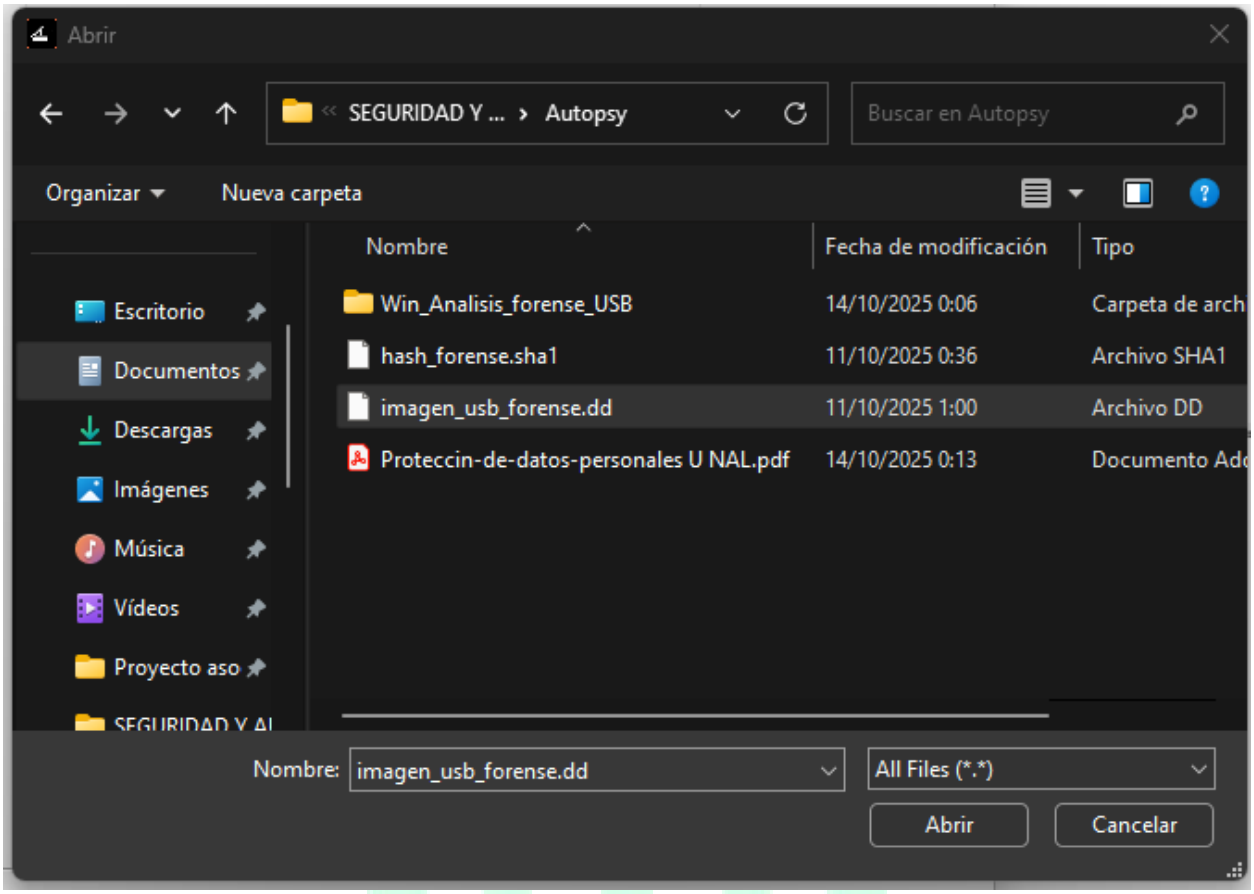


Ilustración 63. Selección de Imagen Forense

Ventana de FTK Imager para seleccionar la imagen forense imagen_usb_forense.dd desde la carpeta Autopsy.

5.3.14 Fuente de Evidencia Definida en FTK Imager

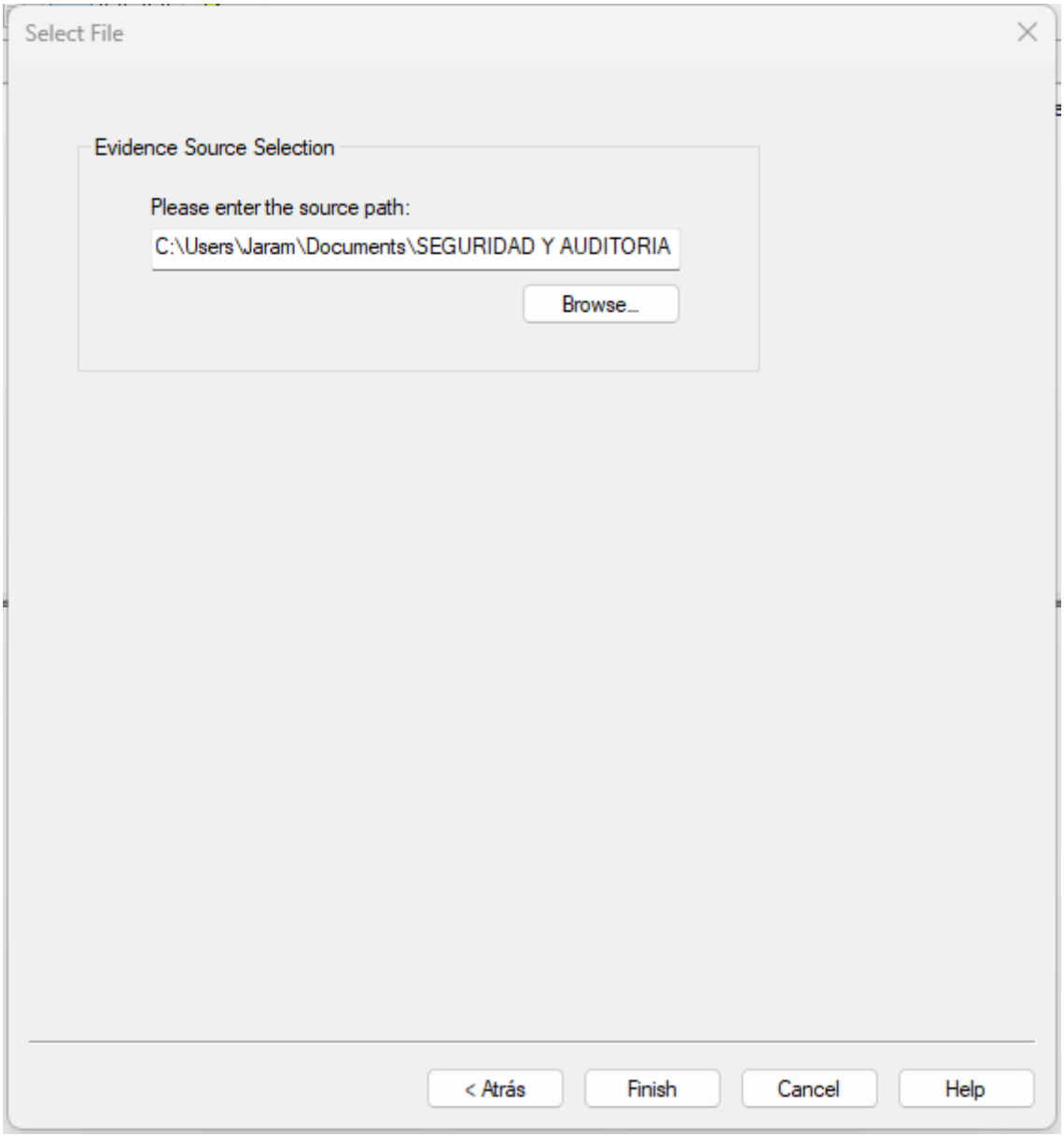


Ilustración 64. Ruta de Evidencia Configurada

FTK Imager con 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.

5.3.15 Contenido de la Memoria USB en FTK Imager.

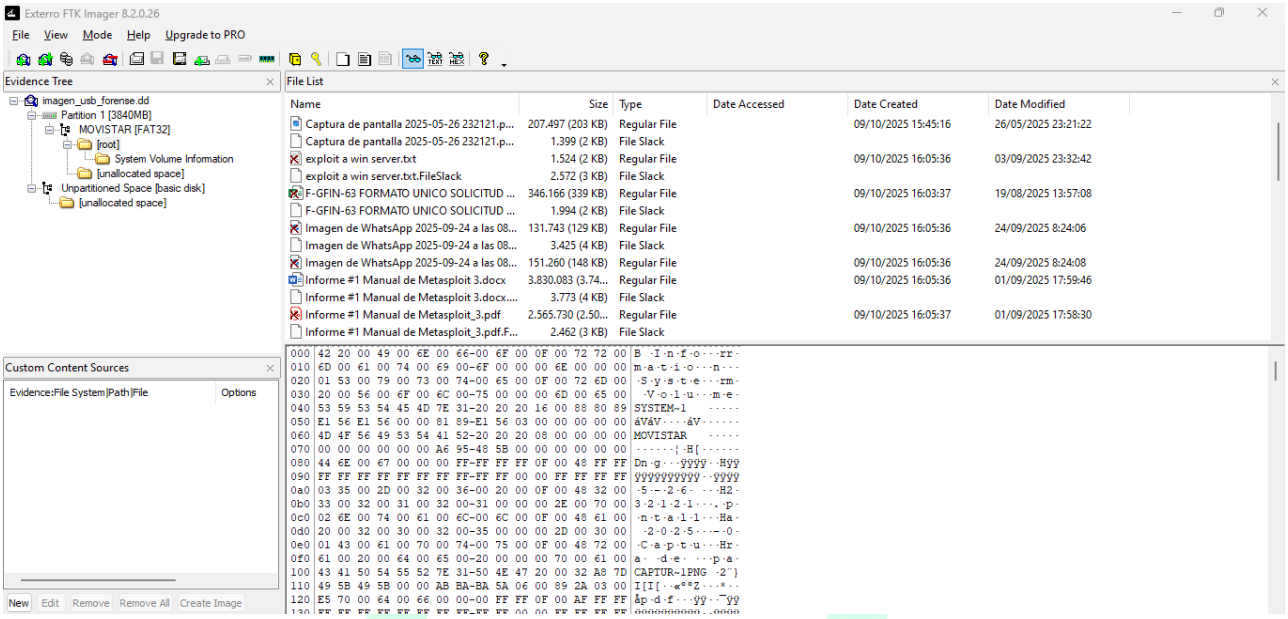


Ilustración 65. Análisis de Imagen en FTK Imager

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

5.3.16 Documentos de Recuperados de la USB

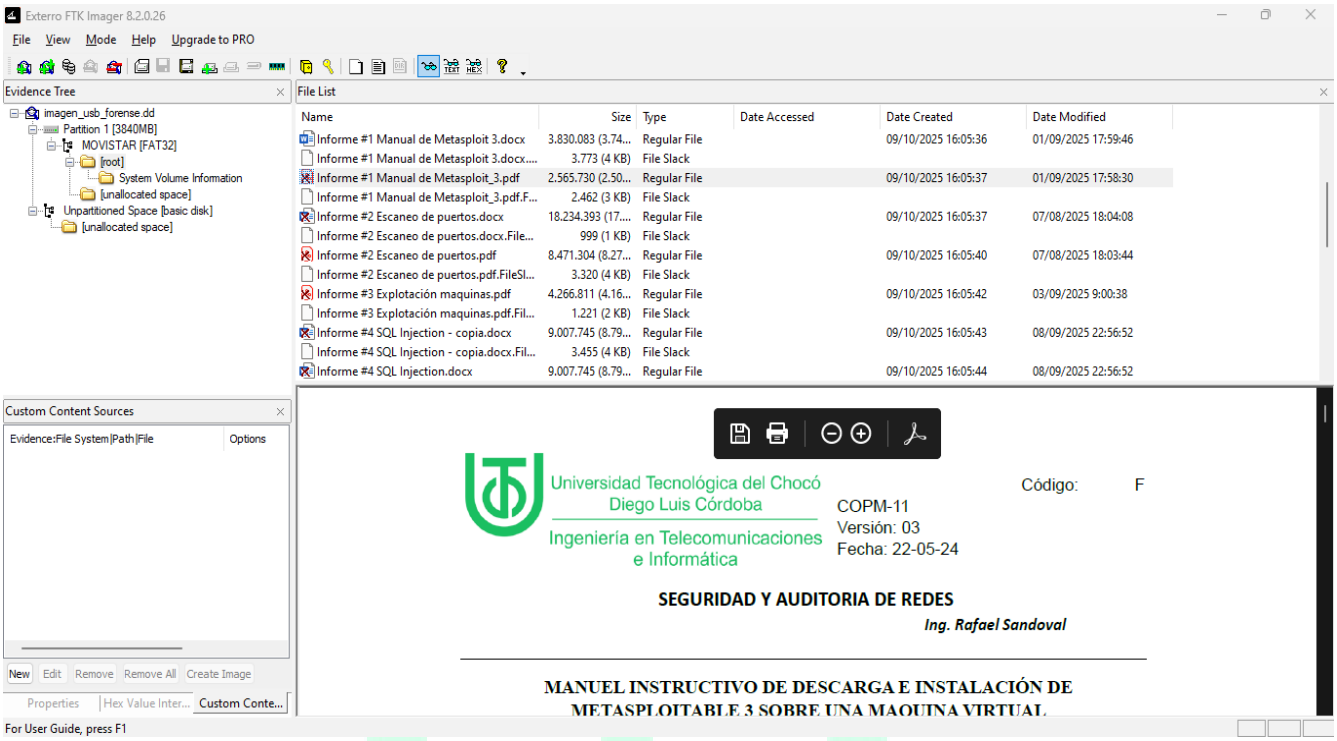


Ilustración 66. Informes de Análisis en FTK Imager

FTK Imager mostrando múltiples informes de seguridad recuperados de la memoria USB, incluyendo el manual de Metasploit.

5.3.17 Archivo Exportado Correctamente

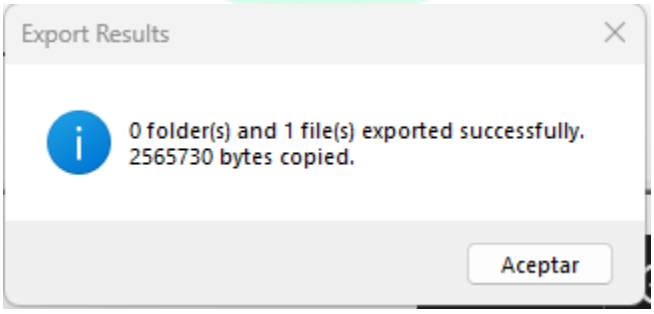


Ilustración 67. Exportación Exitosa

Mensaje de confirmación de FTK Imager indicando la exportación exitosa de 1 archivo, correspondiente a uno de los documentos recuperados de la imagen forense.

6. Problemas encontrados

Durante el desarrollo de la práctica no se presentaron inconvenientes. El seguimiento detallado de las instrucciones proporcionadas por el docente permitió ejecutar todos los procedimientos con Autopsy en Kali Linux y Windows, así como con FTK Imager, sin interrupciones.

7. Recomendaciones

- Mantener un registro de los comandos y procedimientos exitosos para réplica en futuros análisis.
- Realizar pruebas en un entorno controlado antes de aplicarlos en una investigación real.

8. Conclusión

El análisis de la memoria USB se realizó con éxito, demostrando que tanto Autopsy como FTK Imager son herramientas muy útiles y se complementan para obtener y revisar información de forma confiable.

Los resultados confirman que es importante usar programas especializados que garanticen que los datos no se alteran y que el proceso se puede repetir de la misma manera, tal como exigen los procedimientos forenses.

Esta práctica permitió aprender cómo se realiza una investigación digital paso a paso, destacando la importancia de ser ordenado y seguir un método claro en cada etapa.

9. Bibliográfica

Rafael Sandoval Morales (2025). ANALISIS FORENSE CON USB MEDIANTE AUTOPSY EN KALI LINUX Y WINDOWS A SU VEZ EL USO DE FTK IMAGER