ADQUISICIÓN Y ANÁLISIS FORENSE DE UN DISPOSITIVO USB

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

ADQUISICIÓN Y ANÁLISIS FORENSE DE UN DISPOSITIVO USB

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

RAFAEL SANDOVAL MORALES

Docente de asignatura.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIAS DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

TABLA DE FIGURAS

1. Introducción

La disciplina de la informática forense digital juega un papel esencial en la preservación y el análisis científico de la evidencia electrónica. Este documento tiene como objetivo principal detallar las fases críticas de la **adquisición y el análisis forense de un dispositivo de almacenamiento USB**.

El presente informe detalla el proceso de adquisición bit a bit (creación de imagen forense) de un dispositivo de almacenamiento USB y su posterior preparación para el análisis utilizando la herramienta forense de código abierto Autopsy Forensic Browser.

El procedimiento incluye la creación de una copia bit a bit inalterada del dispositivo fuente, utilizando herramientas de línea de comandos como `dd` y `sha1sum` en un entorno Linux. La copia fiel de la evidencia, o **imagen forense**, garantiza que el análisis se realice sobre una réplica exacta, manteniendo la cadena de custodia intacta.

Posteriormente, el informe describe la configuración e importación de esta imagen al **Autopsy Forensic Browser**, una herramienta de código abierto que facilita la gestión del caso, la organización de la evidencia por host, y el análisis exhaustivo del sistema de archivos. Este proceso metodológico busca no solo extraer información oculta o eliminada, sino también demostrar la aplicación práctica de los principios de integridad y no alteración de la evidencia digital.

También El trabajo está estructurado en tres capítulos temáticos para un desarrollo completo:

Capítulo 1: Se enfoca en la **Adquisición y Análisis con Autopsy en Linux**, cubriendo desde la identificación del dispositivo y el cálculo de hash, hasta la clonación forense y el entorno de verificación de integridad de la imagen en Autopsy.

Capítulo 2: Se centra en la **Instalación y Descarga de Autopsy en Windows**, demostrando la disponibilidad y el proceso de configuración de la herramienta en un entorno operativo alternativo.

Capítulo 3: Introduce una herramienta complementaria, **FTK Imager**, ilustrando su uso para la creación o gestión de imágenes forenses (.dd) en el entorno de Windows.

Este proceso metodológico busca no solo extraer información oculta o eliminada, sino también demostrar la aplicación práctica de los principios de **integridad** y **no alteración** de la evidencia digital.

2. Objetivos

2.2 Objetivo general

Demostrar la aplicación de la metodología de la informática forense, documentando las fases de **adquisición bit a bit** y el establecimiento de un entorno de **análisis forense** en plataformas Linux y Windows, utilizando herramientas clave de código abierto y propietario como **Autopsy Forensic Browser** y **FTK Imager**.

2.3 Objetivos Específicos:

2.3.1 Ejecutar el Proceso de Adquisición (Capítulo 1): Realizar la adquisición bit a bit de un dispositivo USB y calcular los valores hash SHA1/MD5 para establecer y verificar la integridad de la evidencia digital, utilizando herramientas de línea de comandos en un entorno Linux.

2.3.2 Establecer el Entorno de Análisis (Capítulos 1 y 2): Configurar y utilizar el Autopsy Forensic Browser para la gestión del caso, la importación del host y la imagen forense, incluyendo el manejo de la verificación de integridad de archivos y el proceso de instalación en sistemas operativos Windows.

2.3.3 Explorar Herramientas Alternativas (Capítulo 3): Describir y demostrar el uso de FTK Imager como una herramienta alternativa o complementaria en Windows para la manipulación y gestión de archivos de imagen forense (.dd).

3. Capítulo 1

3.1 Paso 1: Identificación y Adquisición del Dispositivo

Este paso muestra la identificación de los dispositivos de almacenamiento conectados al sistema y la preparación para la adquisición de la imagen forense.

El comando fdisk -1 se utiliza para listar los dispositivos de disco y sus particiones. Se identifica el disco del sistema (/dev/sda) y el dispositivo de evidencia, un USB (/dev/sdb), de **7.68 GiB** con una partición **FAT32**.

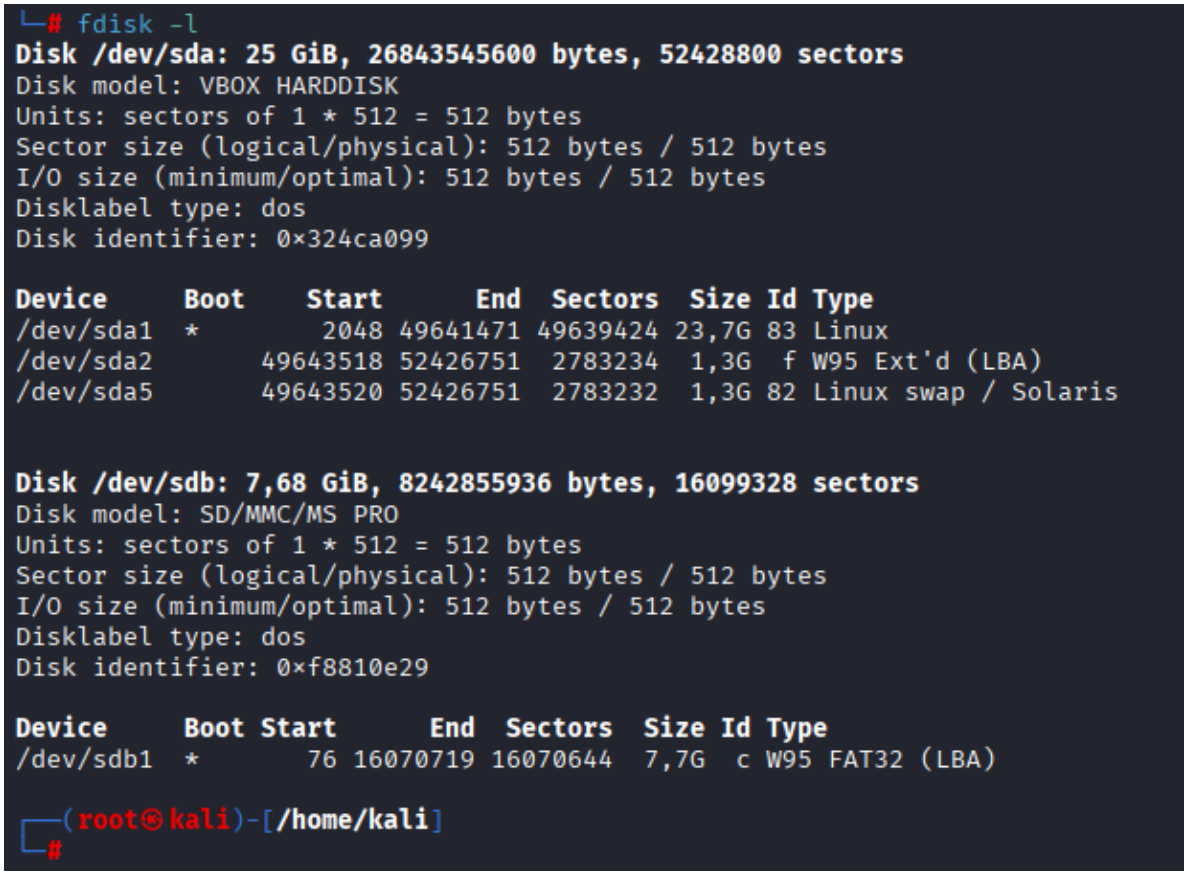


Ilustración 1 Identificación y Adquisición del Dispositivo

3.2 Cálculo de Hash Pre-Adquisición (Integridad)

sha1sum /dev/sdb > ...

Se calcula el **valor hash SHA1** del dispositivo fuente (/dev/sdb) antes de la adquisición. Este *hash* es la "huella digital" de la evidencia y es fundamental para demostrar la **integridad** e inalterabilidad del dispositivo antes de copiarlo.

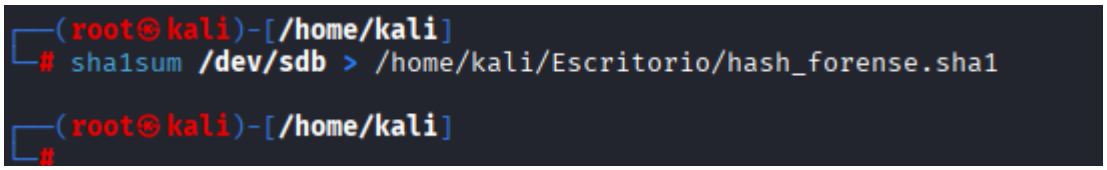


Ilustración 2 Cálculo de Hash Pre-Adquisición (Integridad

3.3 Adquisición Bit a Bit (Clonación Forense)

dd if=/dev/sdb of=/home/kali/Escritorio/imagen_usb_forense.dd ... Se emplea la utilidad **dd** para realizar una **copia bit a bit** completa del dispositivo fuente (/dev/sdb) al archivo de imagen imagen_usb_forense.dd. La opción conv=noerror,sync se usa para asegurar que la clonación continúe a pesar de los errores de lectura.

Ilustración 3 Adquisición Bit a Bit (Clonación Forense)

3.4 Hash de la imagen

Se realiza el hash para la imagen utilizando el comando sha1sum /dev/sda >/home/kali/Escritorio/imagen_usb_forense.dd

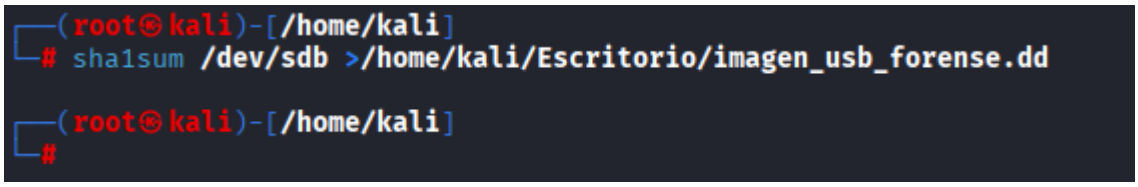


Ilustración 4 Hash de la Imagen

El siguiente comando que se evidencia en la imagen se usa para desbloquear el archivo de la imagen.

Ilustración 5 Desbloquear Hash de Imagen Forense

Durante este paso se realizó la comparación de hash principal y hash de la imagen donde se puede evidenciar que los dos son iguales

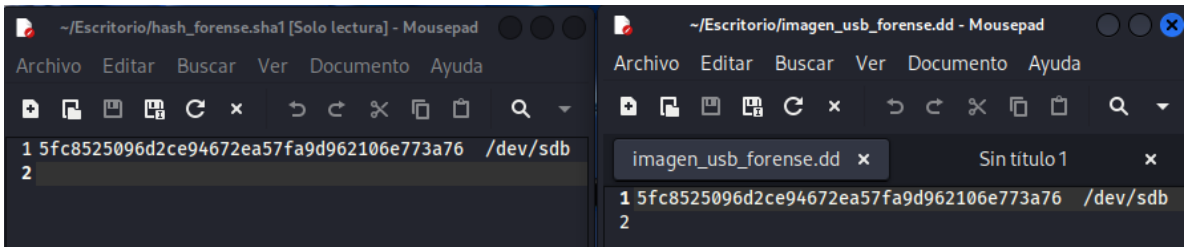


Ilustración 6 Comparación de Hash principal y Hash de la Imagen

3.5 Inicialización del Autopsy

En la barra superior del Kali no dirigimos al buscador y buscamos el autopsy lo abrimos dándole clic

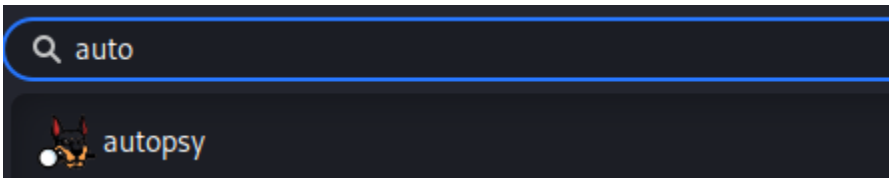


Ilustración 7 Búsqueda del Autopsy

Al abrir el autopsy no despliega lo siguiente imagen donde me pide la contraseña del Kali.

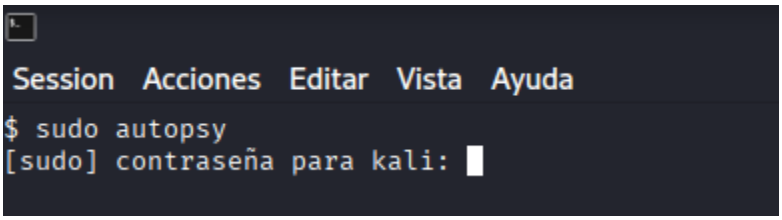


Ilustración 8 Credenciales del Kali

3.6 Ejecución de Autopsy

Una vez se ingresan las credenciales se despliega la siguiente pestaña en la cual se encontrará dos rutas una para ver si hay nuevas versiones y la otra que me muestra la página de inicialización en este link se ingresa presionando la tecla control más clic si está en Windows y coman clic si estas en sistema operativo macOS.

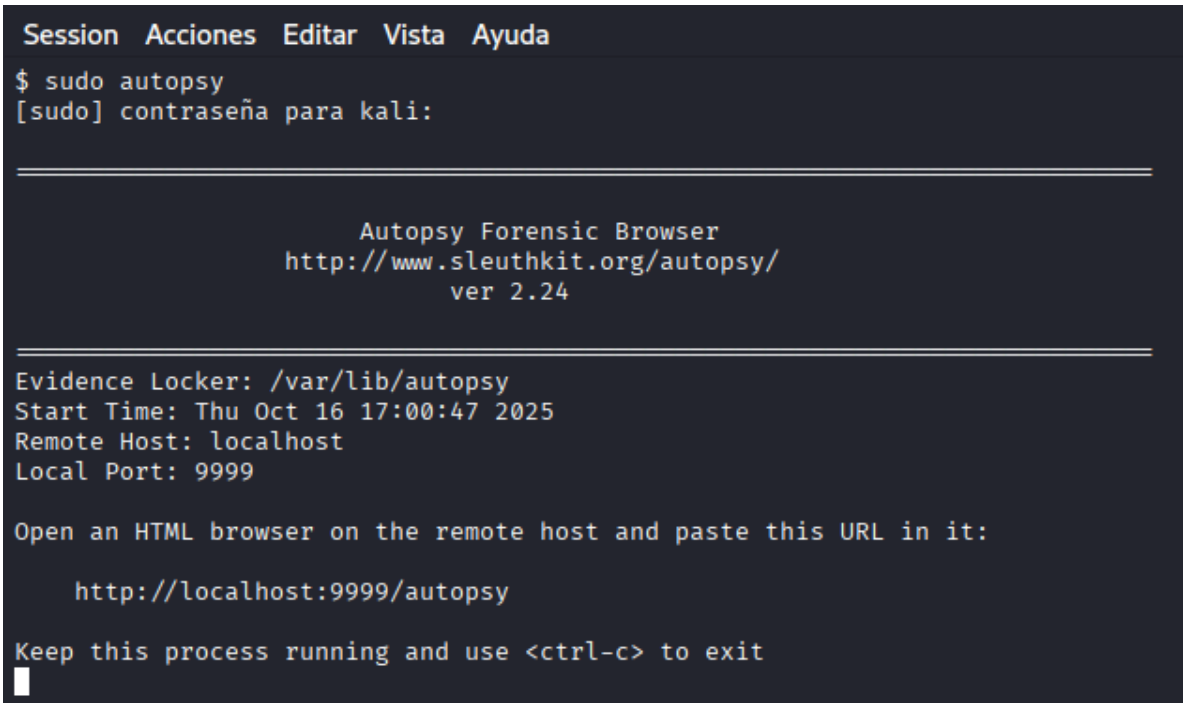


Ilustración 9 Rutas del Autopsy

3.7 Acceso a la Interfaz Web

Este paso inicia la herramienta de análisis que se utilizará para examinar la imagen, a pesar del error de adquisición. Autopsy se ejecuta como un servicio web local, proporcionando la siguiente UR **http://localhost:9999/autopsy** para acceder a la interfaz gráfica a través de un navegador

Ilustración 10 Acceso a la Interfaz Web

3.7.1 Configuración Inicial del Caso y Host

Se siguen los procedimientos estándar para la gestión de cosas en la herramienta forense **Creación del Caso.**

Aquí se establece un nuevo caso con un nombre descriptivo y se asocia el nombre del investigador responsable para este caso se le dio como **Nombre:** MiprimerCaso1, y el **Investigador:** Javier_Moreno.

3.7.2 Adición del Host

El **Nombre:** MVKALIPITI **Descripción:** Portatil Lenovo Se añade el sistema informático (host) del que procede la evidencia. Esta estructura ayuda a organizar los múltiples dispositivos de almacenamiento (imágenes) asociados a una única investigación

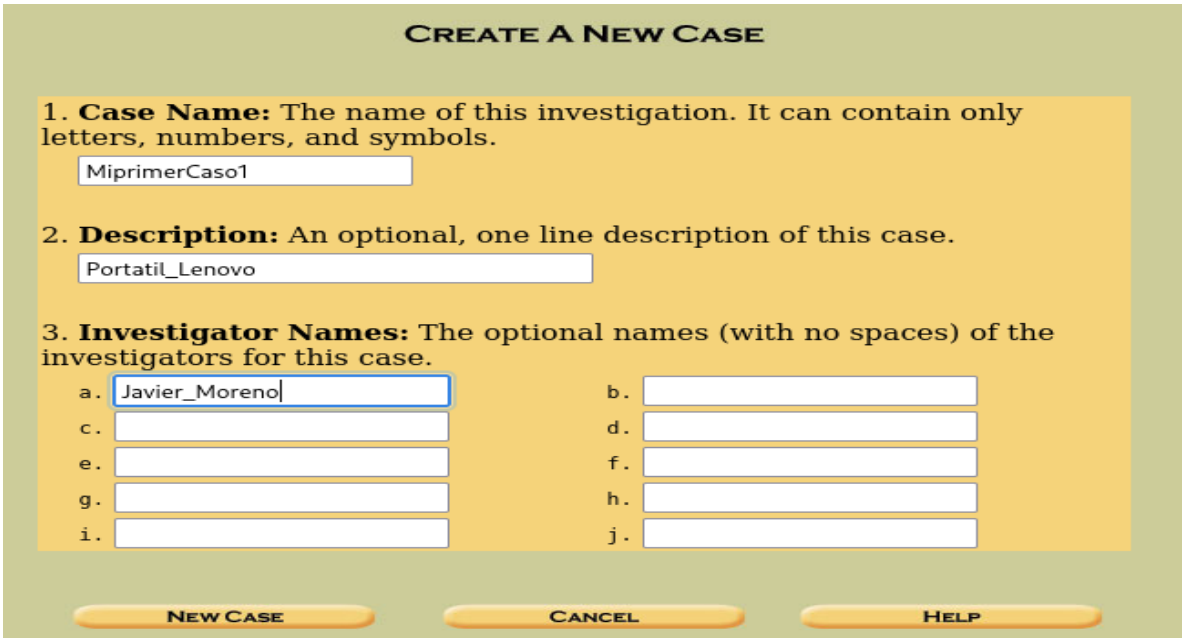


Ilustración 11 Creación del Caso

3.7.3 Ruta y Tipo

Se especifica la ubicación del archivo de imagen y se define como una imagen de Disco completo (no de partición).

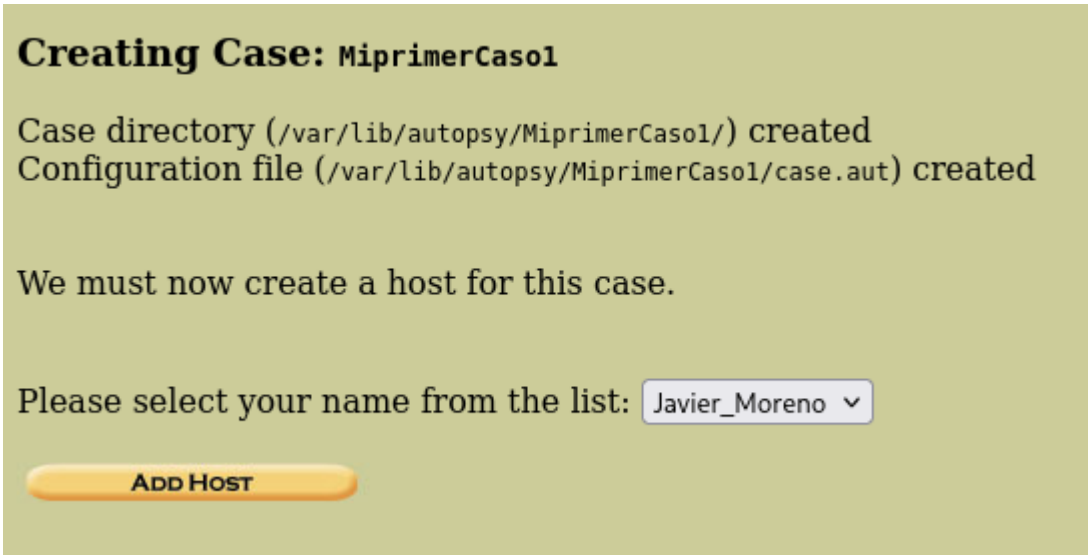


Ilustración 12 Ruta y Tipo

3.7.4 ADD A NEW HOST

ADD A NEW HOST (Añadir un Nuevo Host): Muestra la pantalla de configuración para definir el sistema de origen de la evidencia. Se ha ingresado el nombre del host como **MVKALIPITI** y la descripción como **Portatil Lenovo**. Se dejan en blanco los campos opcionales como Zona Horaria, Ajuste de Desviación Temporal (Timeskew) y bases de datos de hash.

Ilustración 13 ADD A NEW HOST

3.7.5 Host Creado

Host Creado y Preparación para Imagen: Confirma la adición exitosa del host **MVKALIPITI** al caso **MiprimerCaso1** y la creación de los directorios y archivos de configuración asociados. El sistema indica que el siguiente paso es importar un archivo de imagen para este host mediante el botón **ADD IMAGE**.

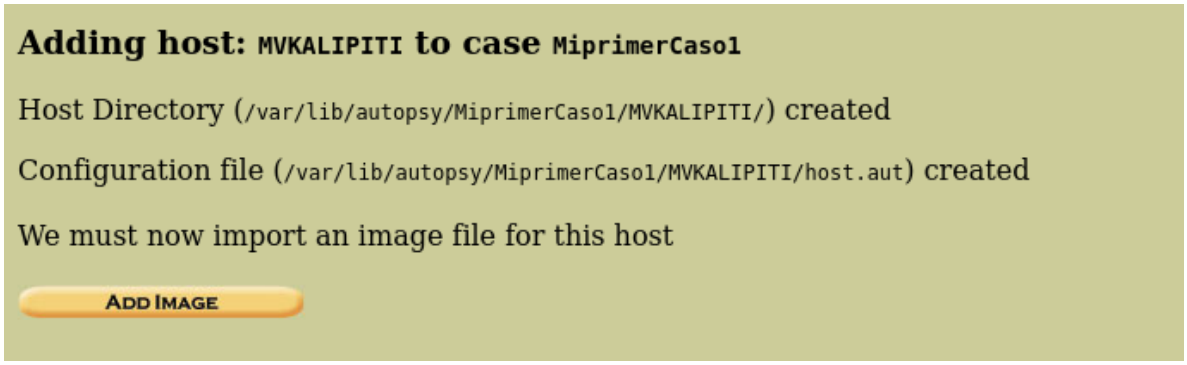


Ilustración 14 Host Creado

3.7.6 Punto de Partida para Agregar Imagen

Gestión de Imágenes de Host: Muestra el panel de gestión del Host **MVKALIPITI**. Indica que **"No images have been added to this host yet"** (Aún no se han añadido imágenes a este host). Se insta al usuario a seleccionar el botón **ADD IMAGE FILE** para comenzar a agregar la evidencia digital, y se muestran las opciones de análisis disponibles como IMAGE INTEGRITY y FILE ACTIVITY TIME LINES.

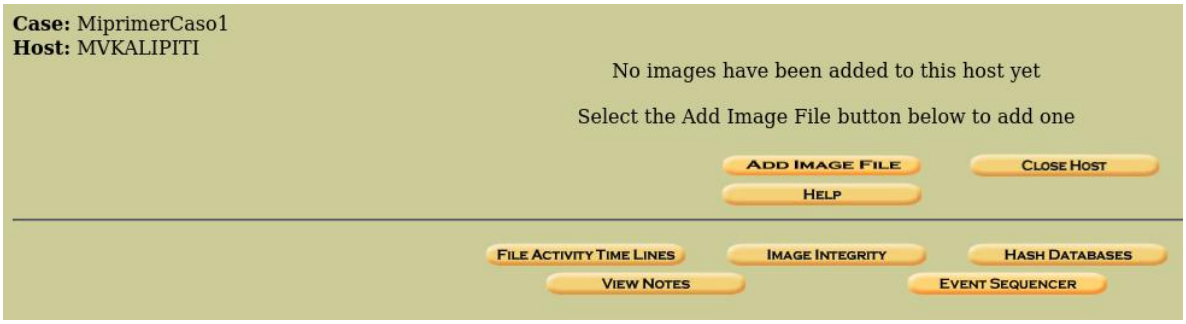


Ilustración 15 Host Gallery (Vista de la Evidencia)

3.7.7 Configuración de la Imagen

ADD A NEW IMAGE (Añadir una Nueva Imagen): Pantalla para especificar los detalles de la imagen forense. Se introduce la ruta completa del archivo, /home/kali/Escritorio/imagen_usb_forense.dd, se selecciona el **Type** como **Disk** (Disco), y se elige **Symlink** como el **Import Method** (Método de Importación). Esto indica que se utilizará un enlace simbólico para acceder a la imagen en lugar de copiarla o moverla al Evidence Locker.

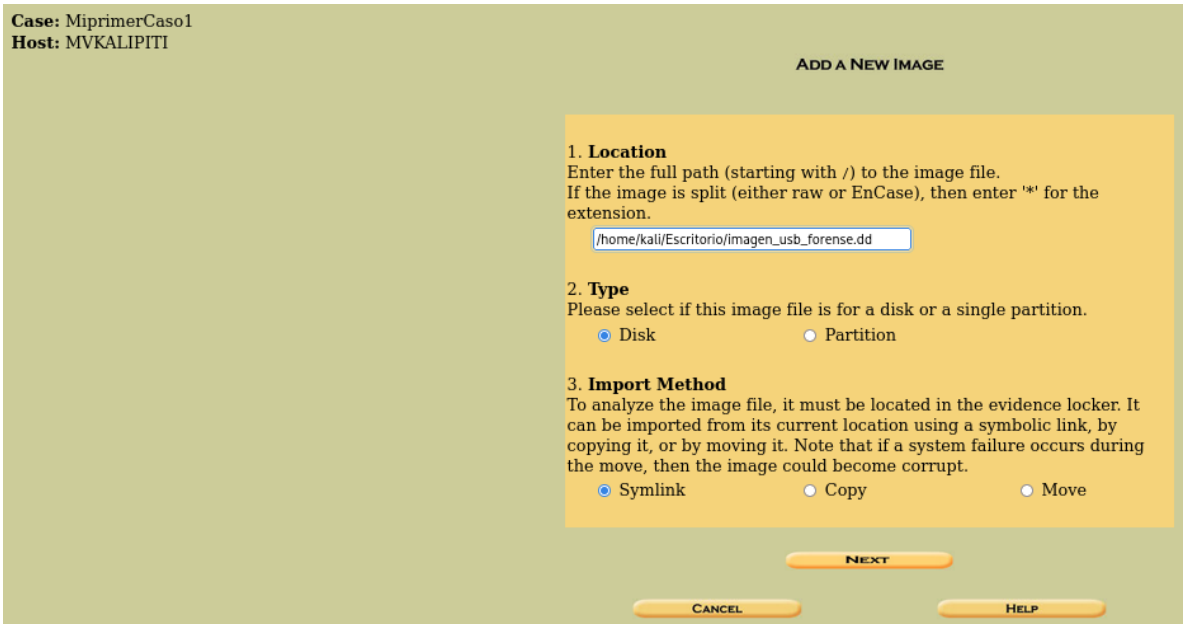


Ilustración 16 Punto de Partida para Agregar Imagen

3.7.8 Advertencia de Tipo de Volumen

Selección Manual de Tipo de Volumen: Aparece una advertencia indicando que Autopsy no pudo determinar automáticamente el tipo de sistema de volumen (la tabla de particiones) para la imagen de disco. El usuario debe seleccionar el tipo manualmente y se elige **dos** (correspondiente a una tabla de particiones MBR/DOS).

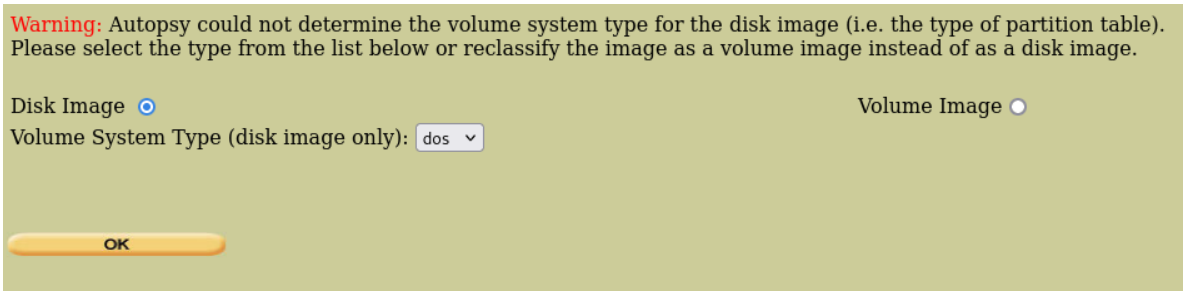


Ilustración 17 Configuración de la Imagen

3.7.9 Paso de Integridad de Datos (Final)

Opciones de Integridad de la Imagen (Añadir Hash): Muestra una configuración alternativa, donde se selecciona la opción **Add the following MD5 hash value for this image** (Añadir el siguiente valor hash MD5 para esta imagen). También se activa la casilla **Verify hash after importing?** (¿Verificar hash después de importar?). Esto permite al investigador ingresar el hash previamente calculado del dispositivo fuente para que Autopsy verifique la integridad.

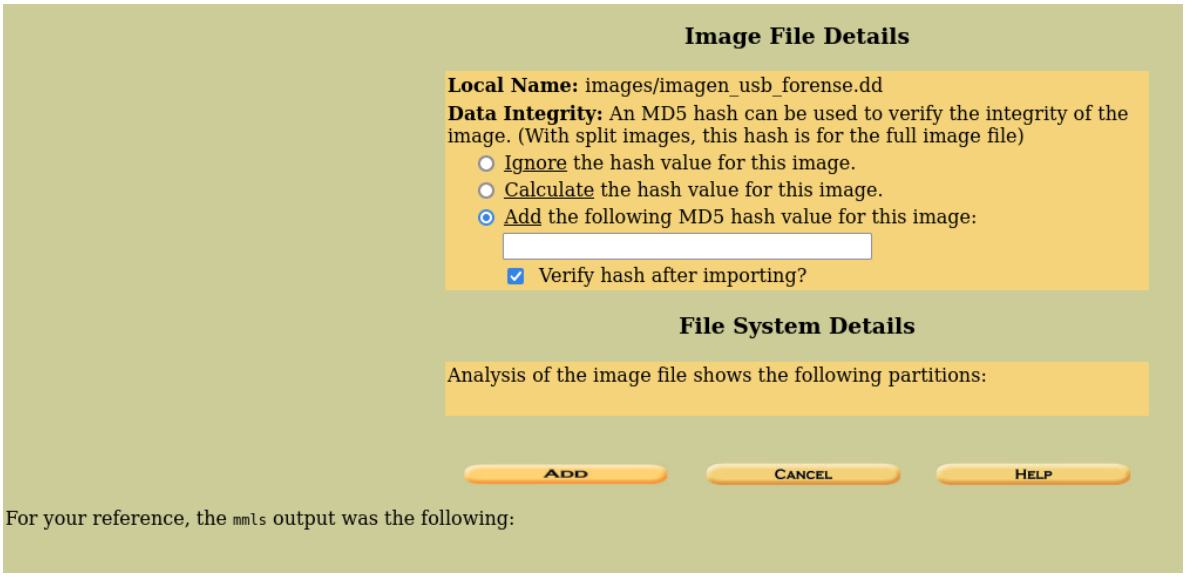


Ilustración 18 Paso de Integridad de Datos (Final)

3.7.10 Resultado del Cálculo de Hash

Cálculo y Fallo de Integridad: Muestra el resultado de Autopsy al calcular el hash MD5. El valor calculado es **D41D8CD98F00B204E9800998ECF8427E**, que corresponde al hash de un archivo vacío. El mensaje **"MD5 value missing"** (Valor MD5 faltante) indica que no se pudo encontrar o verificar un hash de referencia. Esto corrobora el error de adquisición donde la imagen fue sobrescrita.

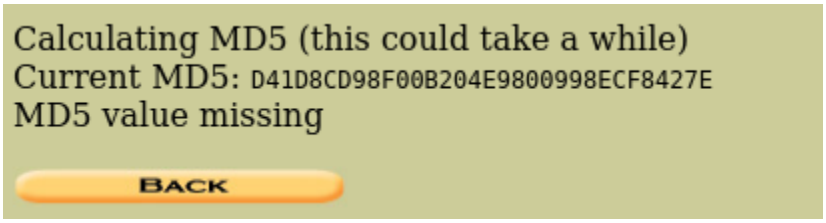


Ilustración 19 Resultado del Cálculo de Hash

3.8 Paso de Integridad de Datos (Inicial)

Opciones de Integridad de la Imagen (Image File Details): Muestra la pantalla de Autopsy donde se configuran los detalles del archivo de imagen. Se muestra el nombre local de la imagen: images/imagen_usb_forense.dd. En la sección de **Data Integrity** (Integridad de Datos), se ofrecen tres opciones para manejar el hash MD5: **Ignore** (Ignorar), **Calculate** (Calcular), o **Add the following MD5 hash value** (Añadir el siguiente valor hash MD5). En esta vista particular, la opción **Calculate** está seleccionada, lo que indica que Autopsy intentará generar el hash MD5 de la imagen antes de continuar el análisis. La sección de **File System Details** (Detalles del Sistema de Archivos) es donde se listarían las particiones encontradas, pero permanece vacía en este punto.

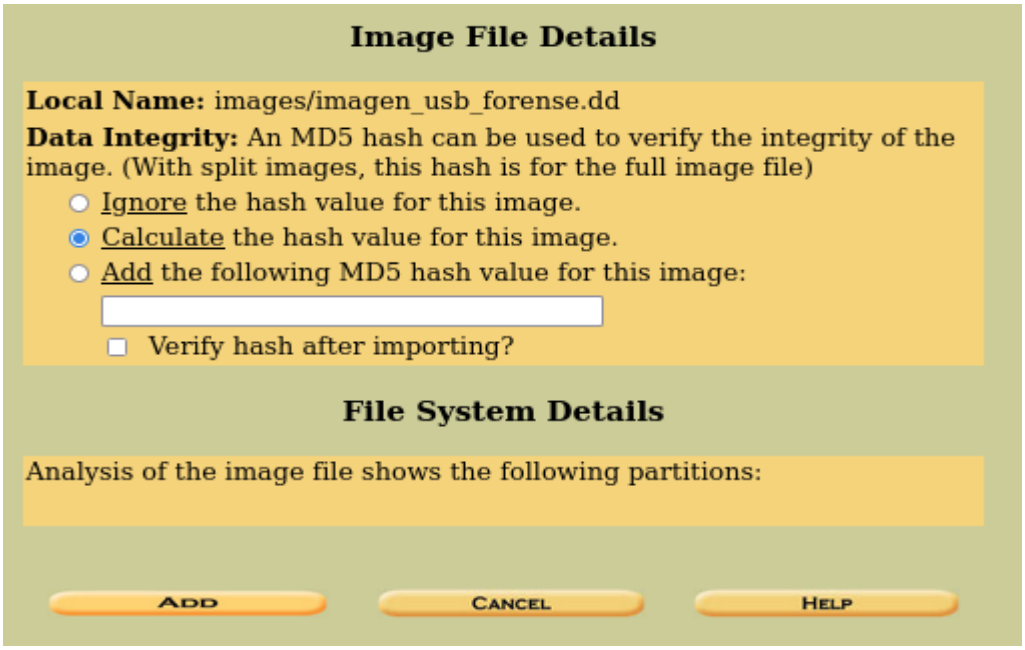


Ilustración 20 Paso de Integridad de Datos (Inicial)

3.8.1 Paso de Imagen Importada y Lista para Análisis

Gestión de Imágenes y Análisis de Volumen (Host Manager): Muestra la sección **Host Manager** para el Host **MVKALIPITI** dentro del caso **MiprimerCaso1**. Confirma que la imagen forense ha sido agregada, listada bajo la columna **name** como **imagen_usb_forense.dd-disk**. La imagen tiene un punto de montaje (mount) de **disk** y un tipo de sistema de archivos (fs type) como **raw** (crudo). El sistema solicita al usuario que seleccione un volumen para analizar. Los botones en la parte inferior, como **ANALYZE** (Analizar), **IMAGE INTEGRITY** (Integridad de la Imagen), y **HASH DATABASES** (Bases de Datos de Hash), indican las opciones disponibles para el proceso de análisis.

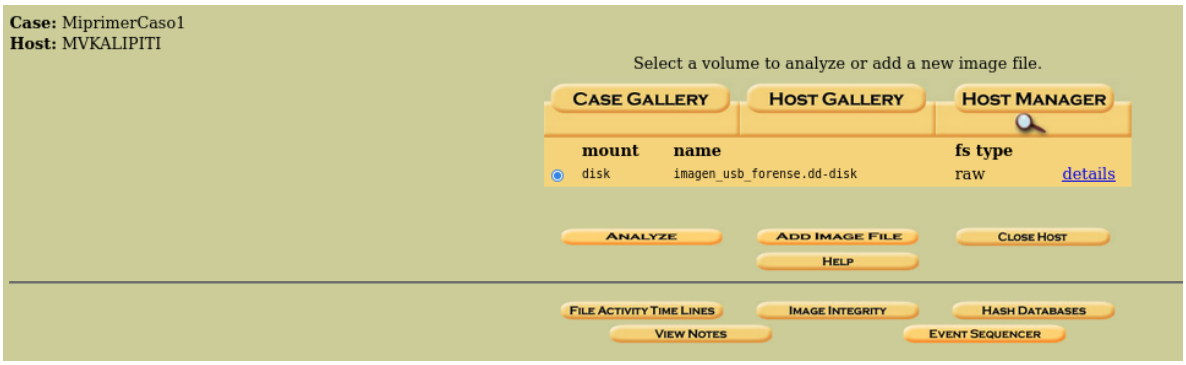


Ilustración 21 Paso de Imagen Importada y Lista para Análisis

3.8.2 Paso de Galería de Host y Selección

Galería de Host (Host Gallery): Muestra la vista principal de la **HOST GALLERY** (Galería de Host) dentro del caso **MiprimerCaso1**. En esta galería, se listan todos los sistemas o equipos (Host) asociados al caso de investigación. Se puede observar el host llamado **MVKALIPITI**, cuya descripción es **Portatil Lenovo**. El usuario puede seleccionar este host y hacer clic en **OK** para abrirlo e iniciar el análisis de la evidencia asociada, o seleccionar un investigador para los reportes (Javier_Moreno).

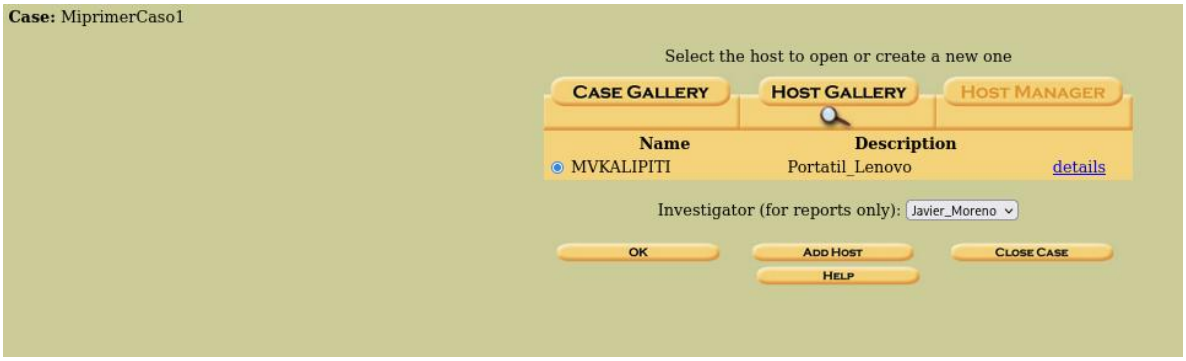


Ilustración 22 Paso de Galería de Host y Selección

3.8.3 Verificación de Integridad de Archivos

Validación de la Integridad de la Imagen y Archivos de Cadenas: Lo cual muestra la pantalla de Autopsy dedicada a la verificación de la integridad de los archivos de evidencia mediante sus valores hash. En la sección **FILE SYSTEM IMAGES** (Imágenes del Sistema de Archivos), el archivo de imagen imagen_usb_forense.dd está listado con el hash MD5: **D41D8CD98F00B204E9800998ECF8427E**. Este hash es universalmente reconocido como el hash MD5 de un archivo vacío, lo que confirma el error crítico de adquisición donde la imagen no contiene los datos del disco original. La sección **STRINGS FILES** (Archivos de Cadenas) lista los archivos de cadenas de texto extraídos de la imagen, los cuales también tienen el mismo hash, reforzando la conclusión de que la imagen de origen no contenía datos analizables. El botón **VALIDATE** permite al usuario verificar si el hash calculado coincide con un hash conocido y esperado.

Ilustración 23 Verificación de Integridad de Archivos

4. Capítulo 2

4.1 Instalación de Autopsy en Windows

Para este paso nos dirigimos a la página principal autopsy una vez ingresamos ubicamos la ruta de descarga del autopsy le damos clic se comenzará a descargar

Ilustración 24 Pagina de descarga del Autosy

Como se evidencia en la imagen aquí veras el proceso de descarga

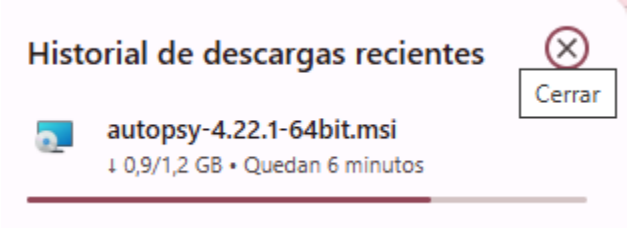


Ilustración 25 Proceso de Descarga del Autosy

Una vez descargado la apalicación nos aparecera una el instalador

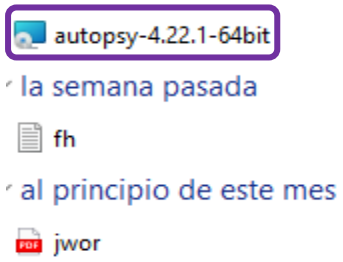


Ilustración 26 Descarga Final

4.2 Proceso de instalación de autopsy

En primer lugar, inicio el asistente de instalación del software Autopsy, donde se me presenta una ventana de bienvenida que confirma que el instalador se ejecutó correctamente. **A continuación**, hago clic en el botón **"Next"**

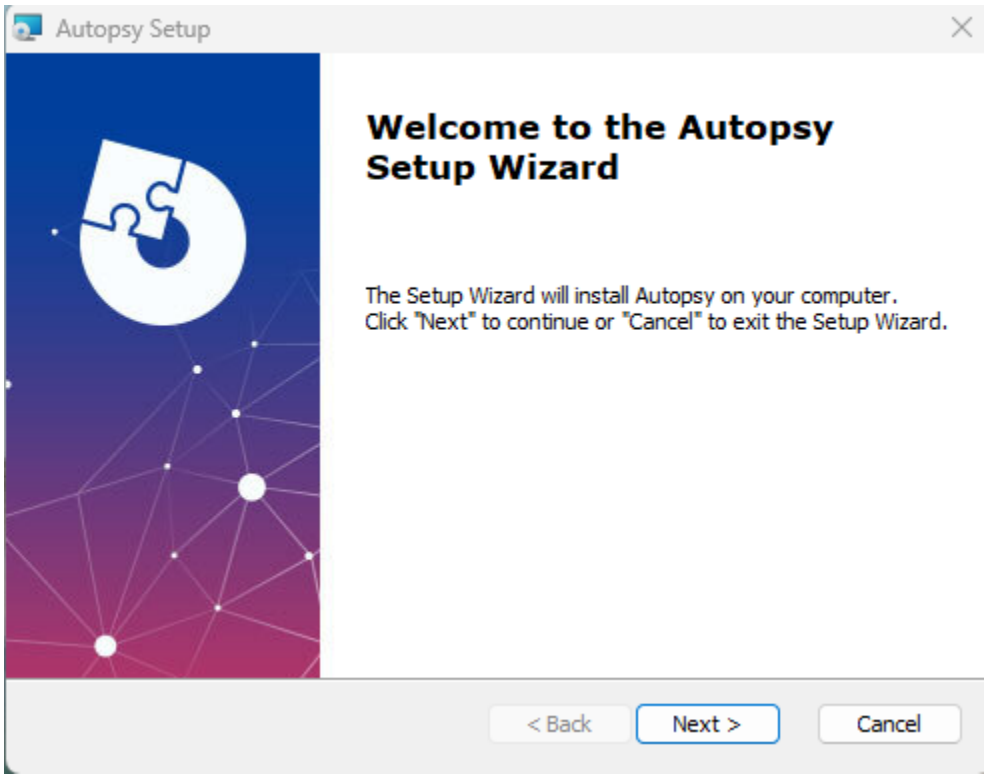


Ilustración 27 Arrancar la instalación

A continuación, el asistente de instalación me dirige al paso donde debo seleccionar la carpeta de destino para instalar Autopsy. En esta etapa, se me muestra una ruta predeterminada dentro del directorio *C:\Program Files\Autopsy-4.22.1*. En caso de requerirlo, puedo modificar esta ubicación haciendo clic en el botón “Browse…”, lo que me permite elegir otra carpeta dentro del sistema. Sin embargo, al estar conforme con la ruta sugerida, mantengo la opción por defecto. Finalmente, hago clic en el botón “Next” para continuar con la instalación.

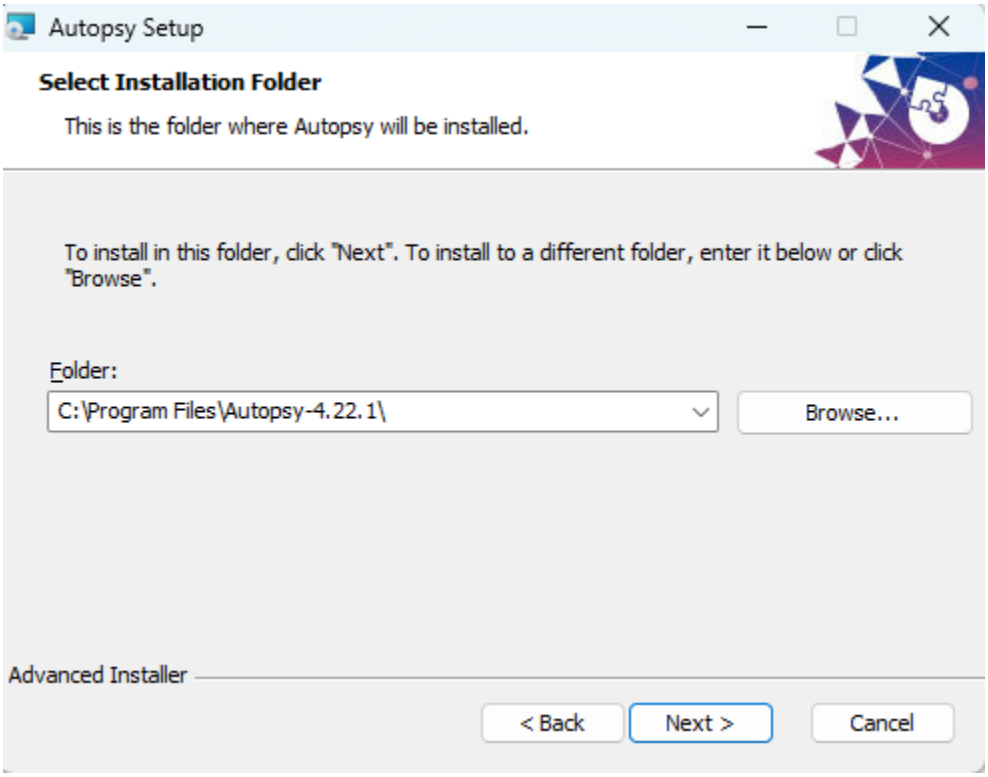


Ilustración 28 Ruta de archivos

Posteriormente, el asistente me muestra una ventana de confirmación denominada “Ready to Install”, donde se indica que todo está listo para iniciar la instalación del software Autopsy. En este punto, se me informa que, si deseo revisar o modificar alguna de

las configuraciones previas, puedo regresar haciendo clic en **“Back”**. **No obstante**, al verificar que los parámetros establecidos son correctos, procedo a continuar con el proceso. **Por esa razón**, hago clic sobre el botón **“Install”**, dando inicio a la copia de archivos y configuración automática del programa en mi equipo.

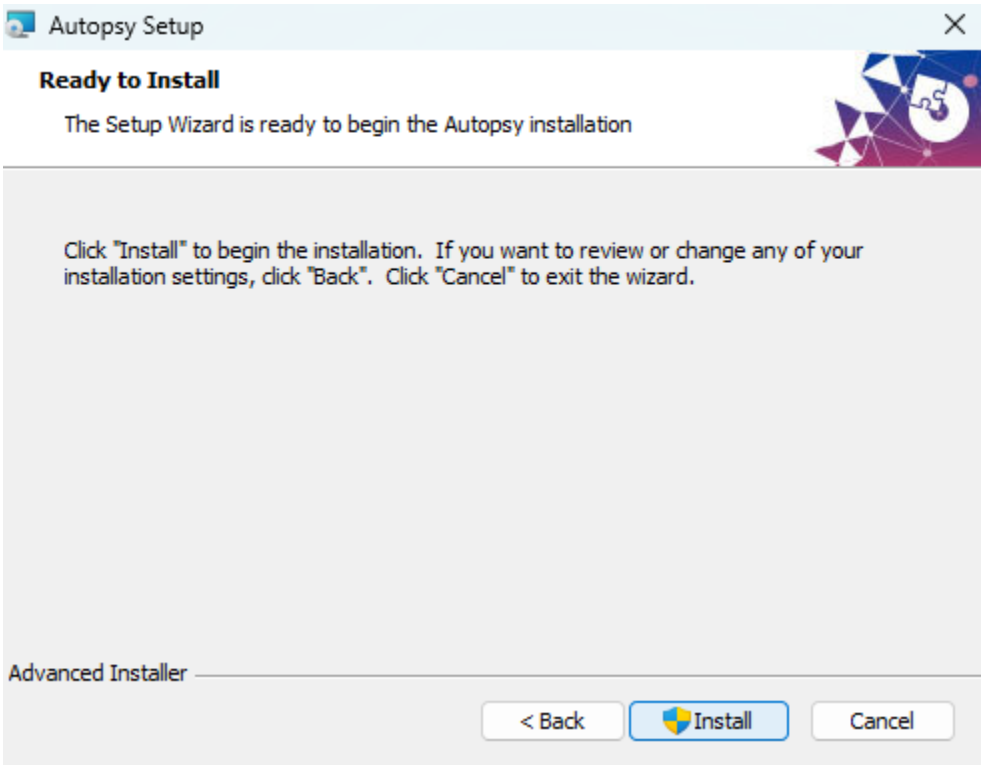


Ilustración 29 Instalar el autopsy

una vez iniciado el proceso, el asistente muestra la ventana titulada *“*Installing Autopsy*”*, donde puedo observar que el sistema ha comenzado a copiar los archivos necesarios para la instalación del software. En esta pantalla aparece una barra de progreso bajo el indicador **“Status:”**, la cual se irá completando a medida que avanza el proceso. **Durante este momento**, solo debo esperar a que el instalador finalice su labor, ya que los botones de navegación anterior y siguiente permanecen deshabilitados. **De esta manera**,

permito que el sistema configure automáticamente todos los componentes y dependencias necesarias para el funcionamiento correcto de Autopsy en mi equipo.

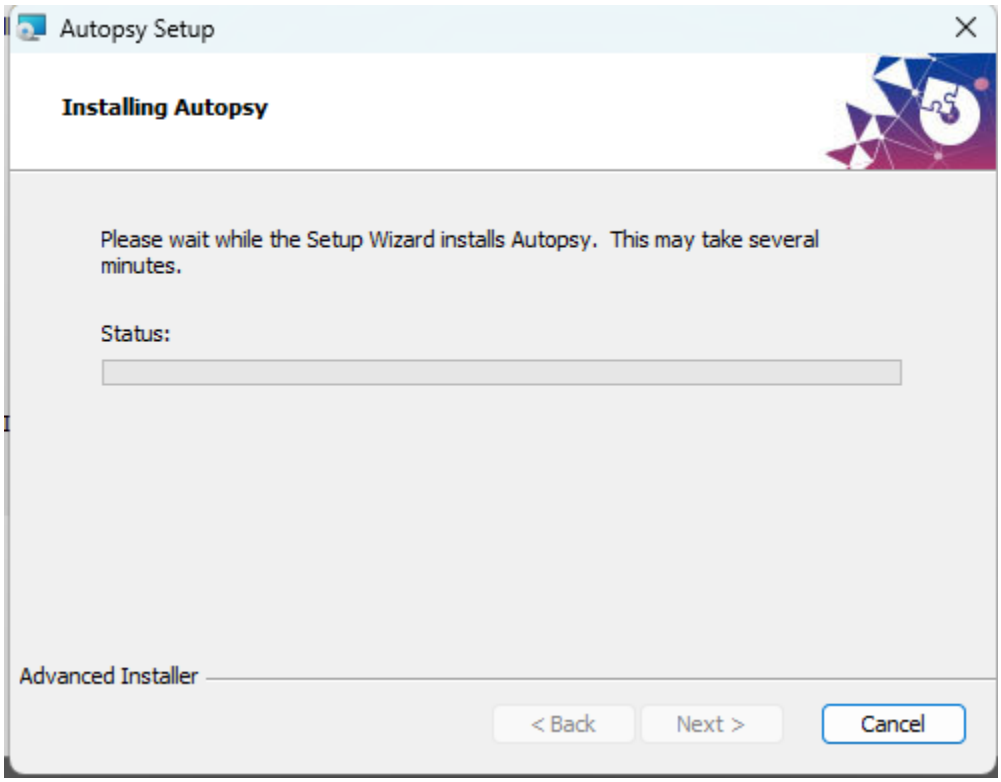


Ilustración 30 Copiar archivos

Finalmente, una vez concluido el proceso de instalación, el asistente me muestra la ventana titulada *"*Completing the Autopsy Setup Wizard*"*. En esta pantalla se indica que el software Autopsy ha sido instalado correctamente en mi equipo. **En este punto**, el sistema me solicita confirmar la finalización del procedimiento mediante el botón **"Finish"**, el cual habilita el cierre del asistente. **Por lo tanto**, hago clic en **"Finish"** para salir del instalador y dejar listo el programa para su ejecución posterior. **De esta forma**, doy por completado todo el proceso de instalación de Autopsy de manera exitosa.

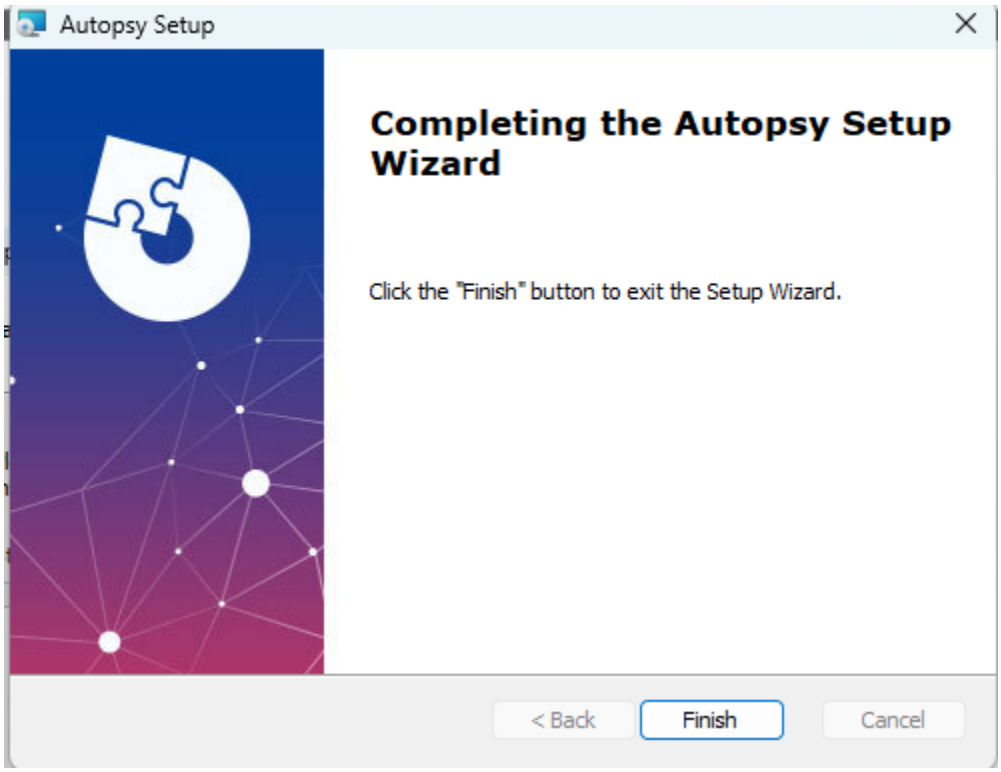


Ilustración 31 finalización de la instalación

Posteriormente, al finalizar la instalación, puedo observar que en el escritorio de mi equipo se ha creado un acceso directo identificado como **"Autopsy 4.22.1"**. Dicho ícono muestra la ilustración de un perro de aspecto vigilante sosteniendo una lupa en el hocico, lo que representa la función investigativa del software dentro del análisis forense digital.

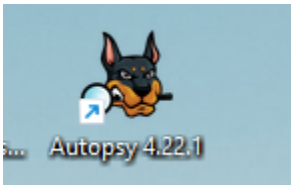


Ilustración 32 acceso directo de Ayutopsy

al ejecutar el software por primera vez, se presenta la ventana de bienvenida de Autopsy. En ella, se muestran tres opciones principales para comenzar el trabajo forense

digital: **“New Case”**, que me permite crear un nuevo caso de investigación; **“Open Recent Case”**, que brinda acceso rápido a casos abiertos recientemente; y **“Open Case”**, con la cual puedo cargar un caso ya existente dentro del sistema.

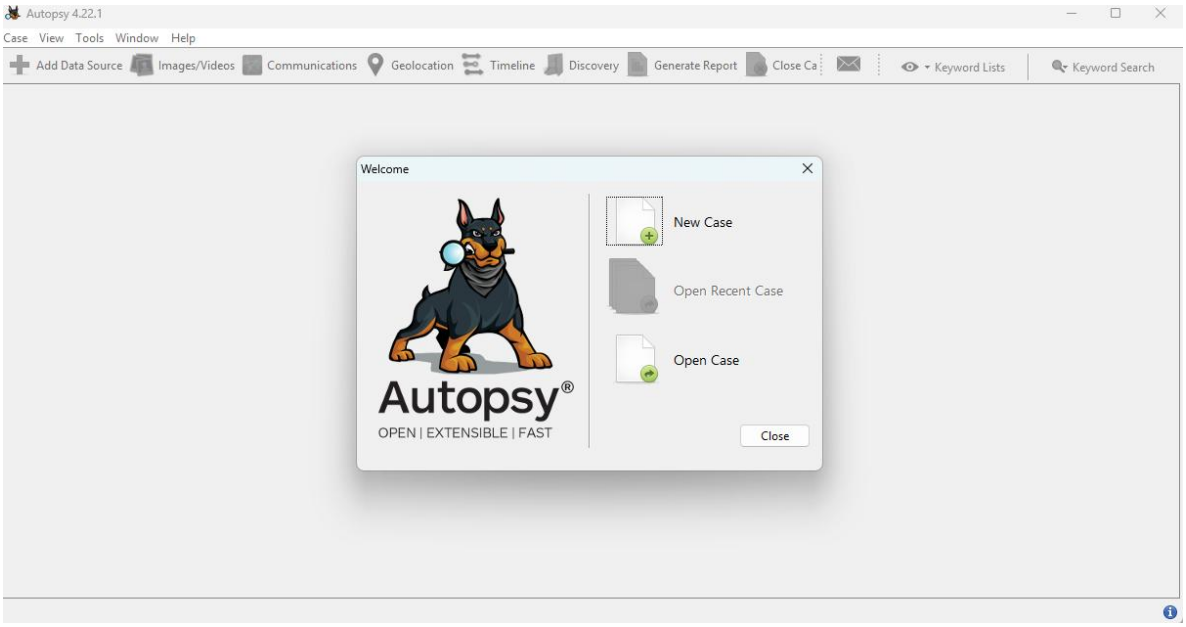


Ilustración 33 ejecutar el software por primera vez

A continuación, dentro de la ventana de bienvenida del software, centro mi atención en la opción **“New Case”**, ya que es desde este apartado donde puedo iniciar la creación de un nuevo caso forense. En esta sección se visualiza un ícono de documento marcado con un símbolo “+”, el cual indica la función de agregar un nuevo proyecto de investigación digital. **En este momento**, Autopsy me permite comenzar el proceso formal de documentación, organización y análisis de las evidencias que serán cargadas posteriormente. **Por ello**, selecciono la opción **“New Case”** con el propósito de registrar un nuevo caso y continuar con el flujo de trabajo forense.

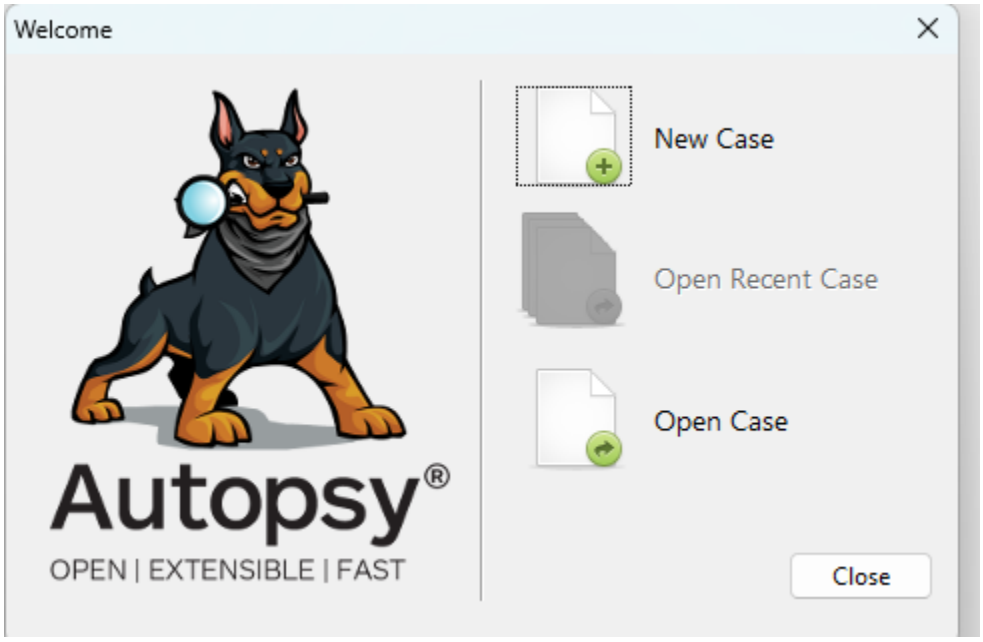


Ilustración 34 Empezar el proceso

Seguidamente, tras seleccionar la opción de crear un nuevo caso, se abre la ventana denominada **"New Case Information"**, donde debo ingresar la información básica del caso que iniciaré. En primer lugar, introduzco el nombre del caso en el campo **"Case Name"**, el cual será el identificador principal dentro del sistema. **Además**, selecciono la ruta donde se almacenarán los datos del caso a través del apartado **"Base Directory"**, pudiendo modificarla mediante el botón **"Browse"** en caso de ser necesario como lo es me dirijo a la ruta de la carpeta Autopsy.

Asimismo, Autopsy me solicita elegir el tipo de caso: **"Single-User"** o **"Multi-User"**. En este ejemplo, mantengo marcada la opción **Single-User**, ya que el análisis será realizado únicamente por mí desde este equipo. Una vez verificada toda la información, **procedo a hacer clic en el botón "Next"**, con el fin de continuar hacia el siguiente paso de configuración opcional del caso.

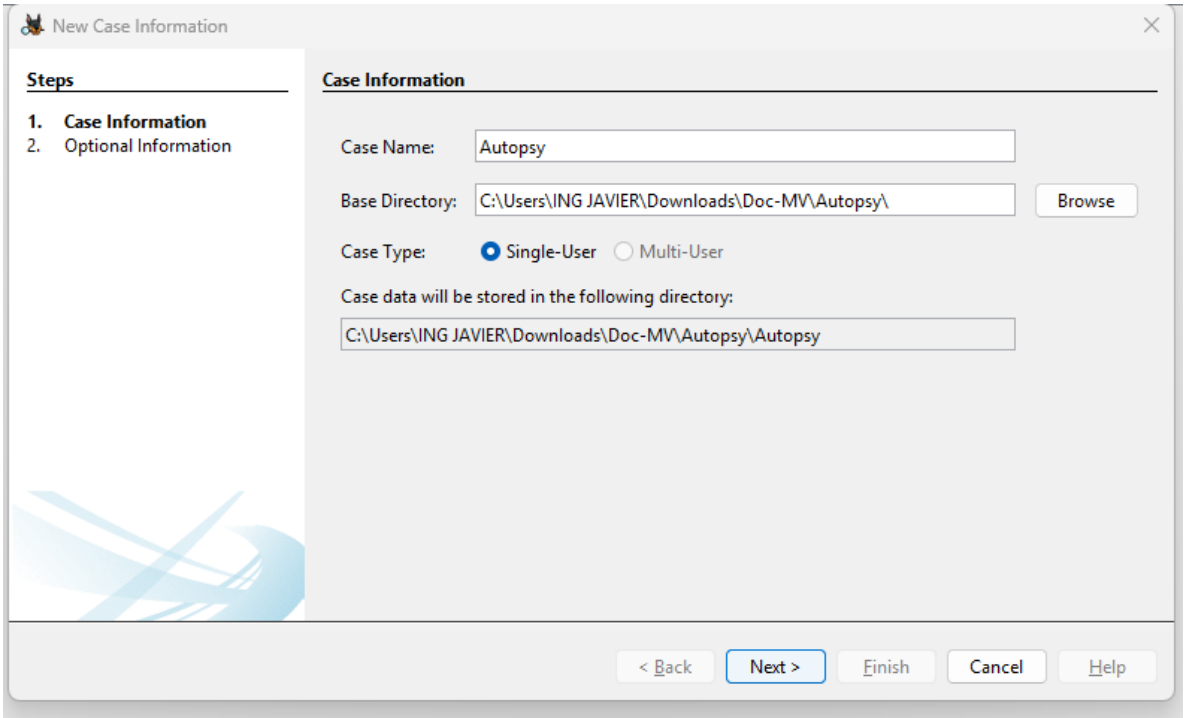


Ilustración 35 Caso informacion

A continuación, el asistente me presenta la sección llamada **"Optional Information"**, donde tengo la posibilidad de registrar información adicional sobre el caso y el examinador. En la parte superior, ingreso el **número del caso para este será 01**, lo cual permite llevar un control interno y una mejor organización en futuras investigaciones.

Luego, en el apartado **"Examiner"**, completo mis datos como analista forense, incluyendo mi nombre para este caso se usó **Javier Stiwar**, seguido de número de contacto **312837137**, y correo electrónico **javiermoreno@gmail.com**, con el objetivo de identificar al responsable del análisis dentro del informe y los registros del sistema. También cuento con un espacio denominado **"Notes"**, donde puedo añadir observaciones relevantes sobre el caso si así lo considero necesario.

Finalmente, en el segmento **"Organization"**, Autopsy me ofrece la opción de especificar si el análisis es realizado para una institución en particular, pudiendo gestionar

dicha información mediante el botón **“Manage Organizations”**. Una vez verificados todos los campos, **presiono el botón “Finish”**, con lo cual se crea oficialmente el nuevo caso y quedo listo para iniciar el proceso de análisis forense digital.

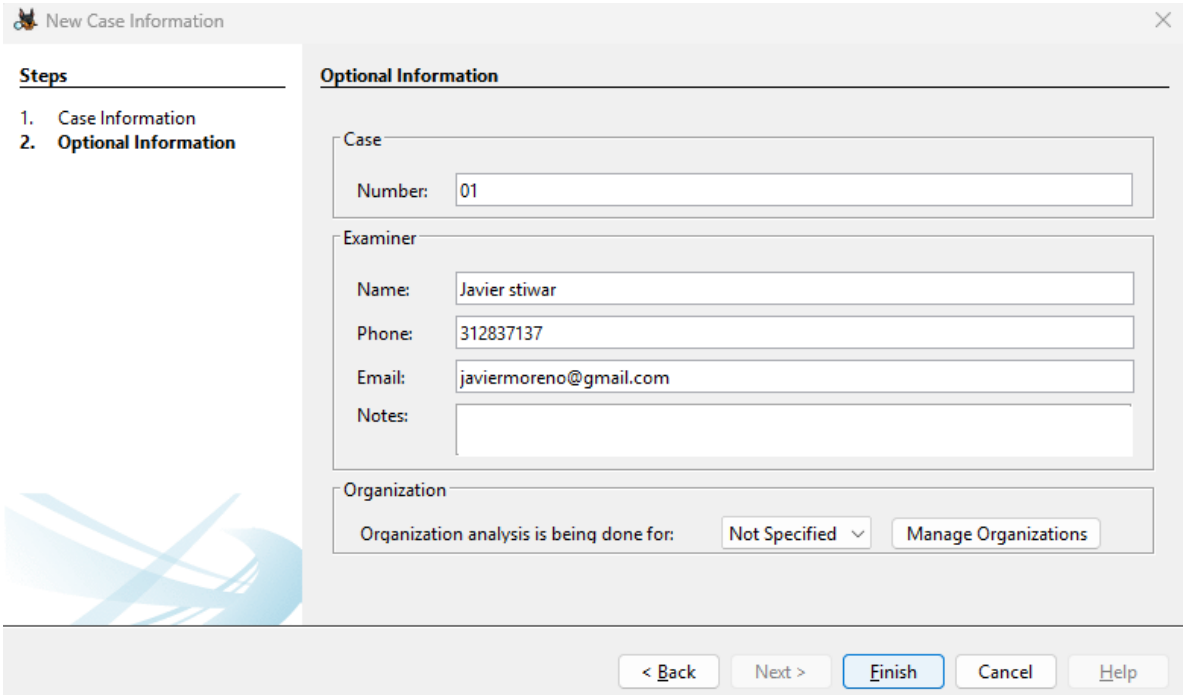


Ilustración 36 informacion de perito

Después de finalizar la configuración del caso, Autopsy comienza automáticamente la creación de la base de datos asociada al mismo. En esta ventana emergente, puedo observar un mensaje que indica “Creating case database..”, acompañado de una barra de progreso que avanza conforme el sistema genera los archivos internos necesarios para la gestión de evidencias y metadatos del análisis forense.

Durante este proceso, no es necesario realizar ninguna acción adicional, ya que la herramienta se encarga de estructurar toda la información requerida para almacenar los resultados que se obtendrán más adelante. **Por lo tanto**, simplemente espero a que la barra

se complete para continuar con las siguientes etapas de la investigación digital dentro de Autopsy.

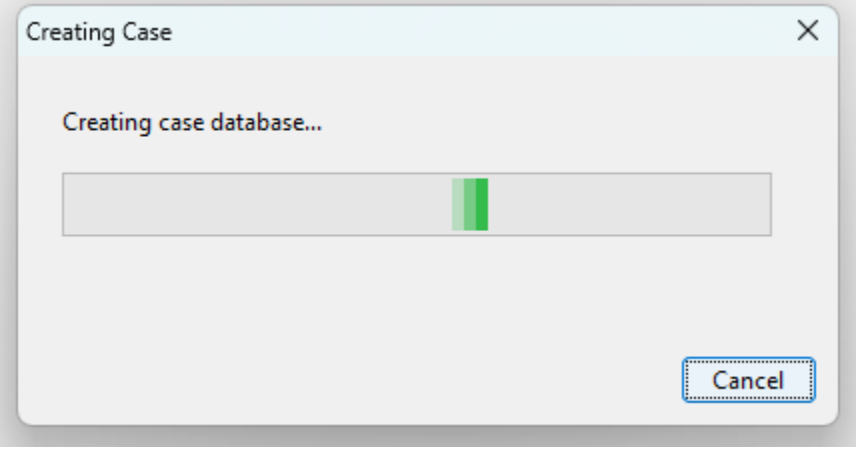


Ilustración 37 Creando de la base de datos

Una vez creada la base de datos del caso, Autopsy me dirige a la ventana **"Add Data Source"**, donde debo comenzar a agregar las evidencias digitales que serán analizadas. En esta primera etapa, correspondiente a **"Select Host"**, se configura el *host*, el cual Autopsy utiliza para organizar las fuentes de datos dentro del caso.

Por defecto, el sistema selecciona la opción **"Generate new host name based on data source name"**, lo que significa que se asignará un nombre automáticamente al host según la evidencia que se cargue posteriormente. **No obstante**, también tengo la posibilidad de elegir la opción **"Specify new host name"** si deseo asignar un nombre personalizado, o seleccionar **"Use existing host"** en el caso de que ya haya un host creado previamente dentro del mismo caso.

Finalmente, al estar conforme con la configuración predeterminada, hago clic en **"Next"** para avanzar al siguiente paso del proceso de incorporación de evidencias.

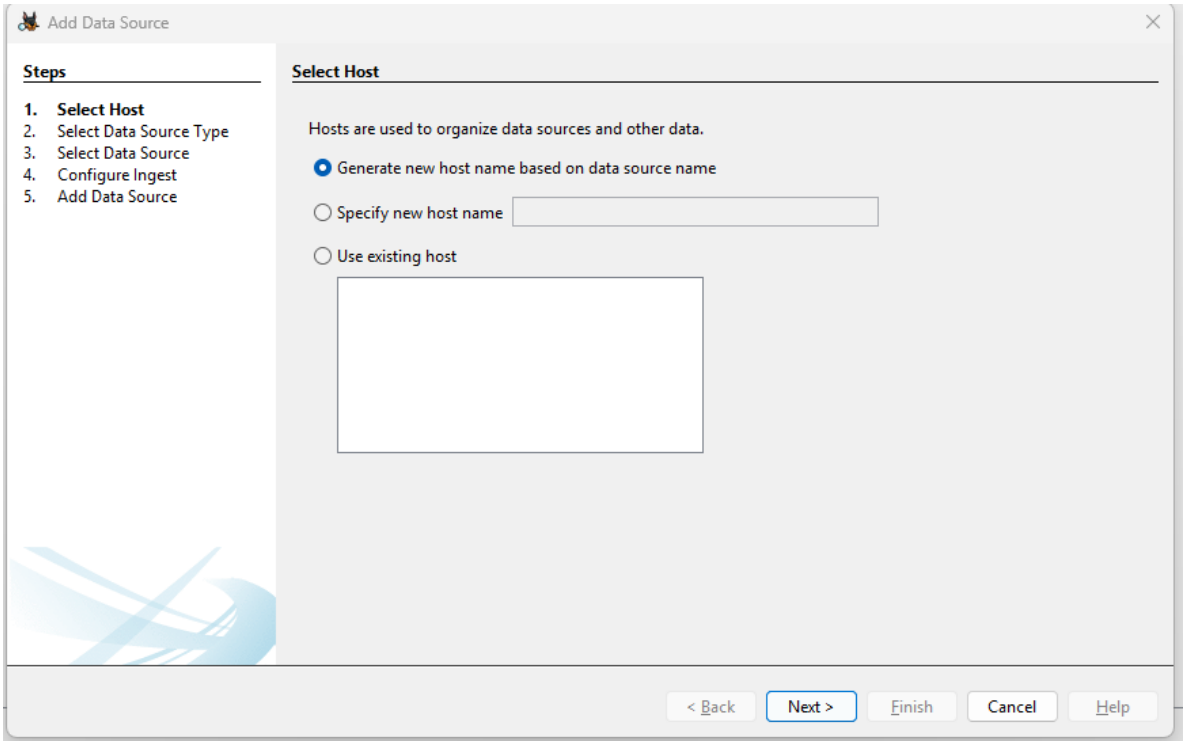


Ilustración 38 Empezamos el proceso

A continuación, al avanzar al apartado **"Select Data Source Type"**, Autopsy me solicita definir el tipo de fuente de datos que analizaré dentro del caso. En esta sección se presentan diferentes opciones, dependiendo del origen de la evidencia digital que se desea examinar.

En primer lugar, se encuentra seleccionada por defecto la opción **"Disk Image or VM File"**, la cual se utiliza para analizar imágenes forenses de discos o archivos provenientes de máquinas virtuales. Esta alternativa es la más común en investigaciones

forenses, ya que permite trabajar sobre una copia exacta del medio original, evitando la alteración de la evidencia.

En mi caso, mantengo la opción **"Disk Image or VM File"** seleccionada, ya que la evidencia que analizaré corresponde a una imagen de disco. Posteriormente, hago clic en **"Next"** para continuar con el proceso de incorporación de la fuente de datos.

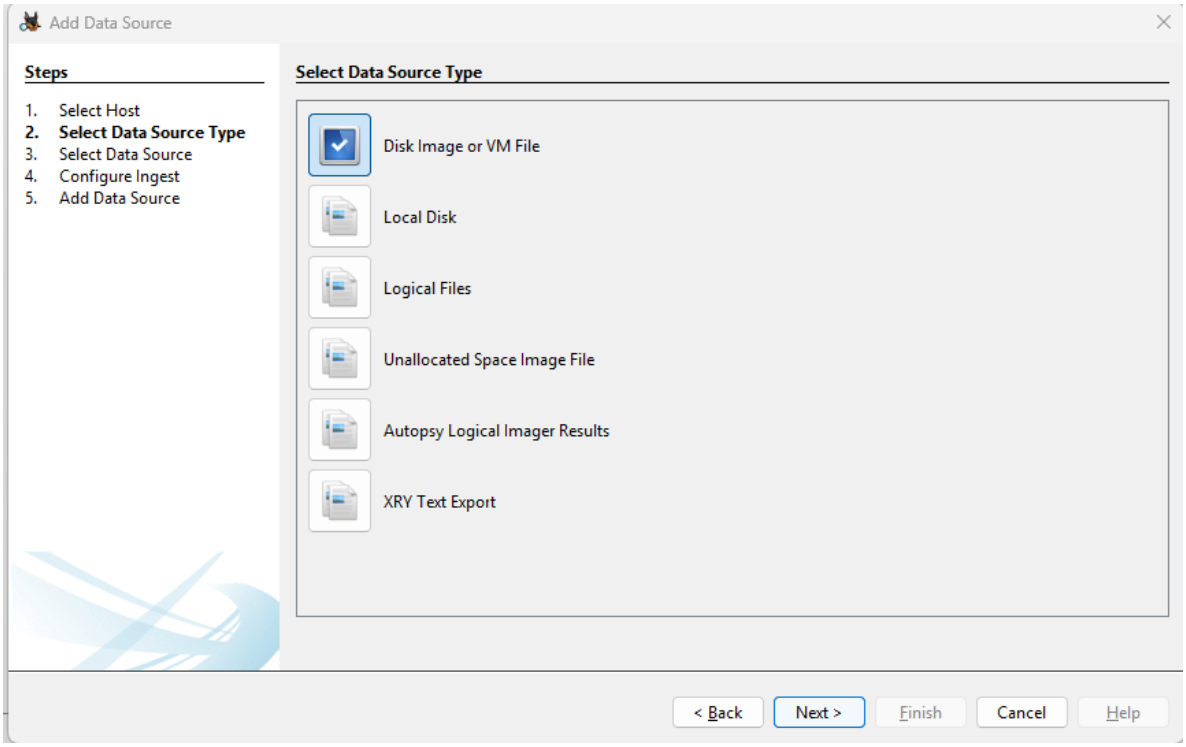


Ilustración 39 Seleccionar el tipo de datos

En el asistente **Add Data Source** de Autopsy, se selecciona la imagen forense. Se especifica la ruta del archivo de imagen (.../imagen_usb_forense.dd) y se configura la zona horaria ((GMT-5:00) America/Bogota). Se observan campos opcionales para *hashes* de

verificación (MD5/SHA-1/SHA-256), que se usarían para validar la integridad del archivo antes del análisis.

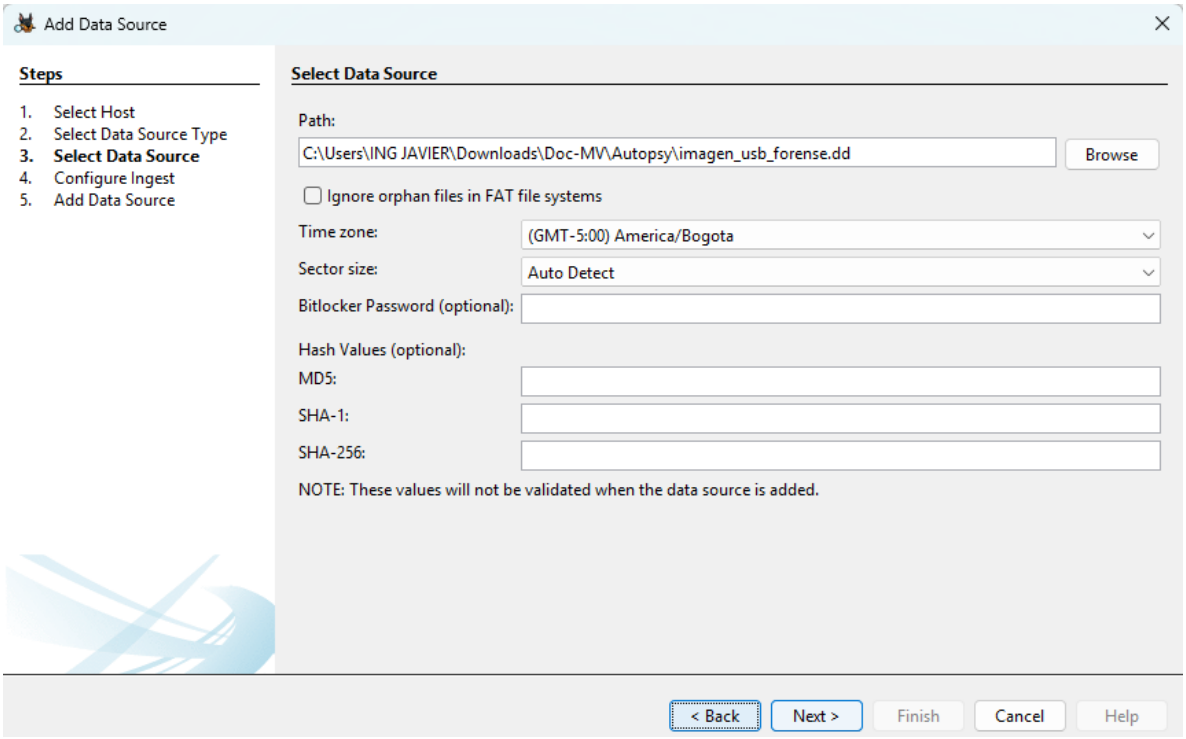


Ilustración 40 Selección de la Fuente de Datos

Se configuran los *Ingest Modules* (Módulos de Ingesta) que se ejecutarán automáticamente en la imagen forense. Se han habilitado módulos críticos como: **Recent Activity** (para rastrear uso reciente), **Hash Lookup** (para identificar archivos conocidos/maliciosos), **File Type Identification** (para detectar extensiones manipuladas) y **Keyword Search** (para buscar términos definidos por el caso).

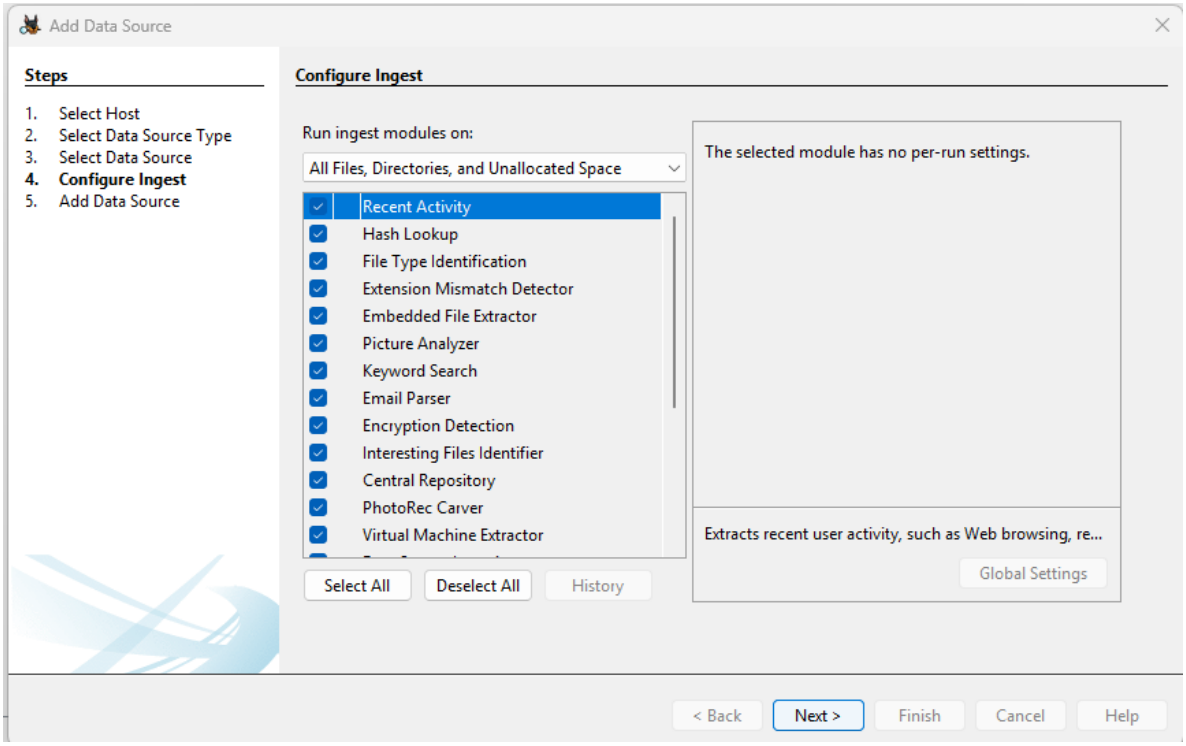


Ilustración 41Configuración de los Módulos de Ingesta.

Autopsy inicia el proceso de añadir la fuente de datos a su base de datos local y comienza a ejecutar los módulos de ingesta configurados. Este proceso puede llevar tiempo, dependiendo del tamaño de la imagen forense.

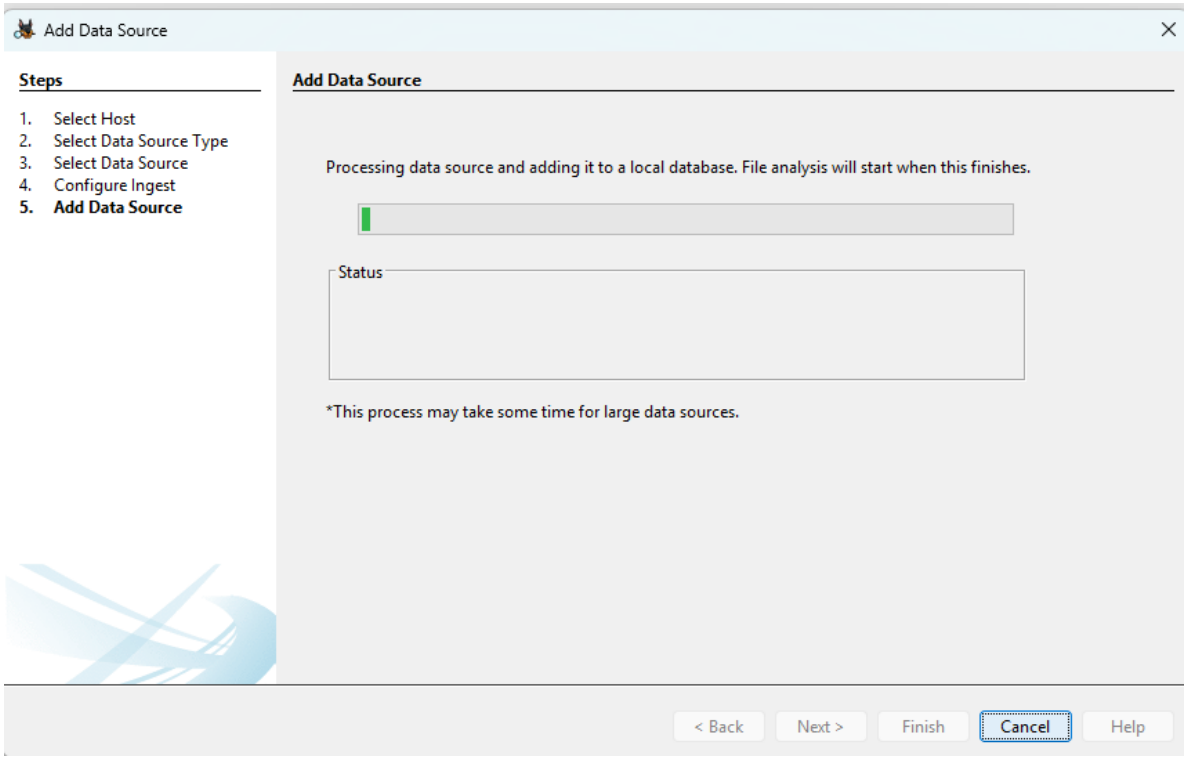


Ilustración 42 Procesamiento de la Fuente de Datos

El proceso de adición ha finalizado, indicando que la *Data Source* fue añadida con errores no críticos, lo cual es común. Se hace clic en **Finish** para comenzar la navegación y

el análisis de los resultados.

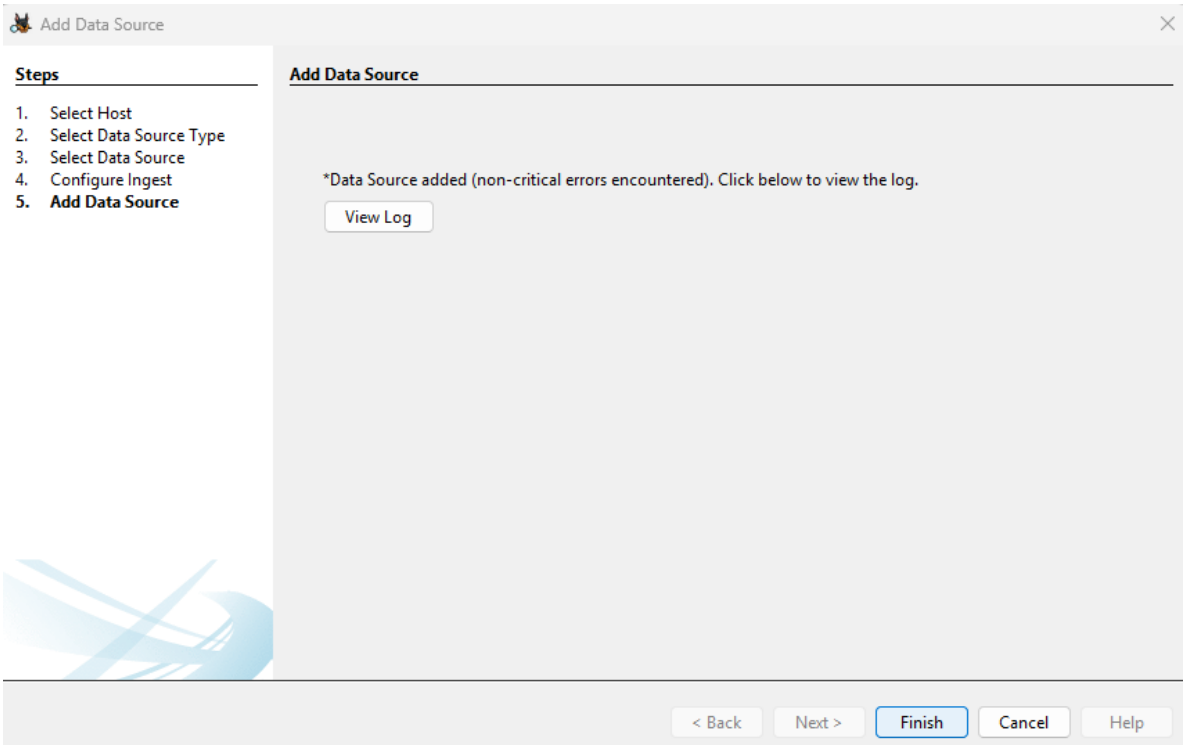


Ilustración 43 Finalización de la Adición de la Fuente de Datos.

Se muestra la imagen forense cargada en el panel de navegación (Data Sources). La fuente se identifica como imagen_usb_forense.dd_1 Host.

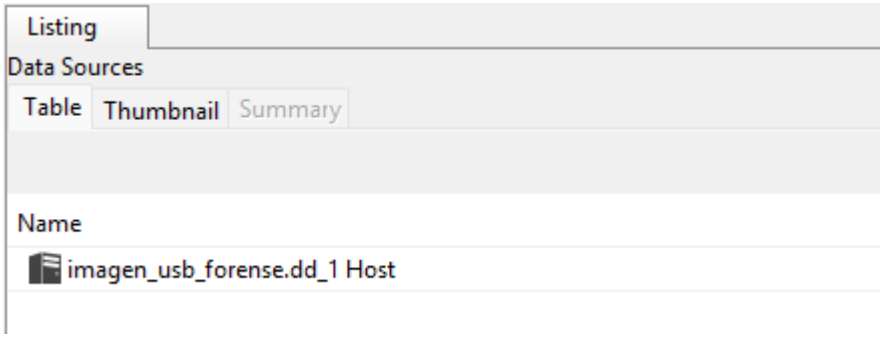


Ilustración 44 Panel de Fuentes de Datos (Data Sources)

En el panel de resultados, se muestran los detalles técnicos de la imagen, incluyendo su tamaño en *bytes*, el tamaño de sector (512), la zona horaria (America/Bogota) y un identificador del dispositivo

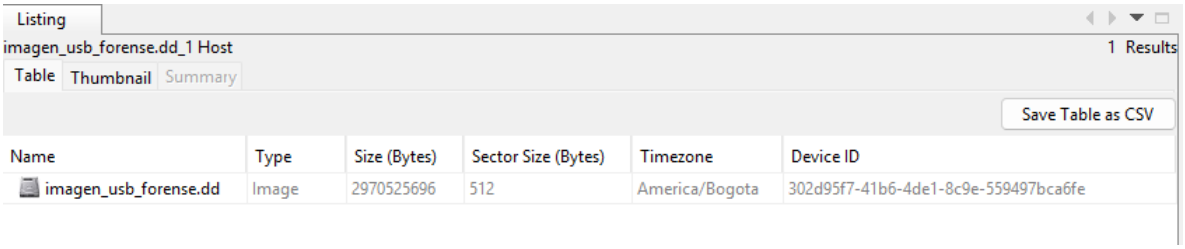


Ilustración 45 Detalles de la Imagen Forense

Se visualiza la estructura de volúmenes dentro de la imagen. Se identifican: **vol1 (Unallocated)**, un área no asignada, y **vol2 (Win95 FAT32)**, un volumen asignado, lo que permite al examinador navegar por la estructura del sistema de archivos.

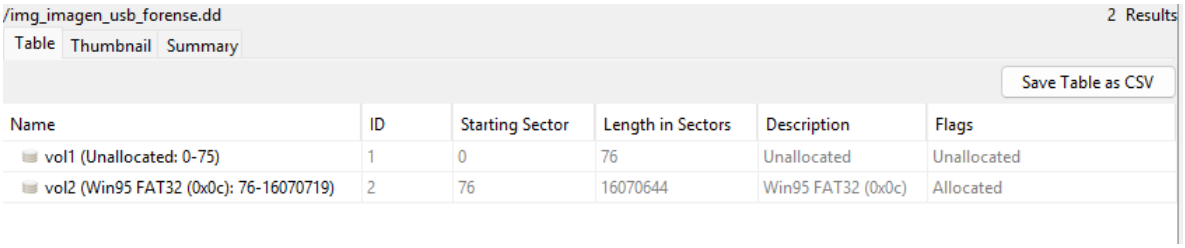


Ilustración 46 Detalles de las Particiones y Volúmenes.

Luego se navega al volumen no asignado (vol1). Se observa un archivo recuperado (Unalloc_3_0_38912) con una marca Unalloc (No Asignado), lo que indica la posible recuperación de datos eliminados en esa área.

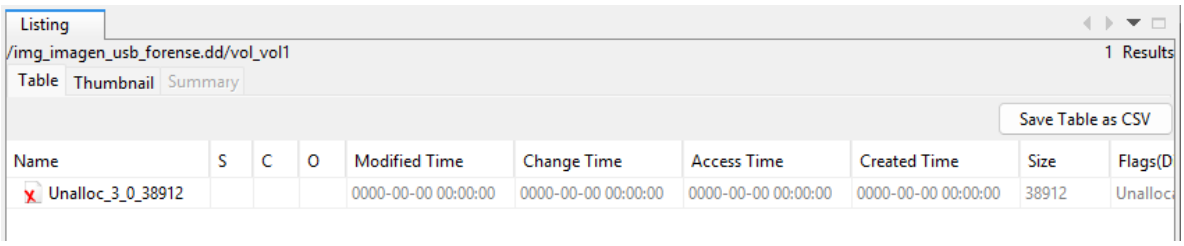


Ilustración 47 Contenido del Espacio No Asignado (vol1)

Se visualiza el contenido del volumen FAT32 asignado (vol2). Se aprecian carpetas del sistema ($MBR, System Volume Information) y un archivo de interés llamado **notas**, con una marca de tiempo de modificación, cambio y acceso (2025-10-11).

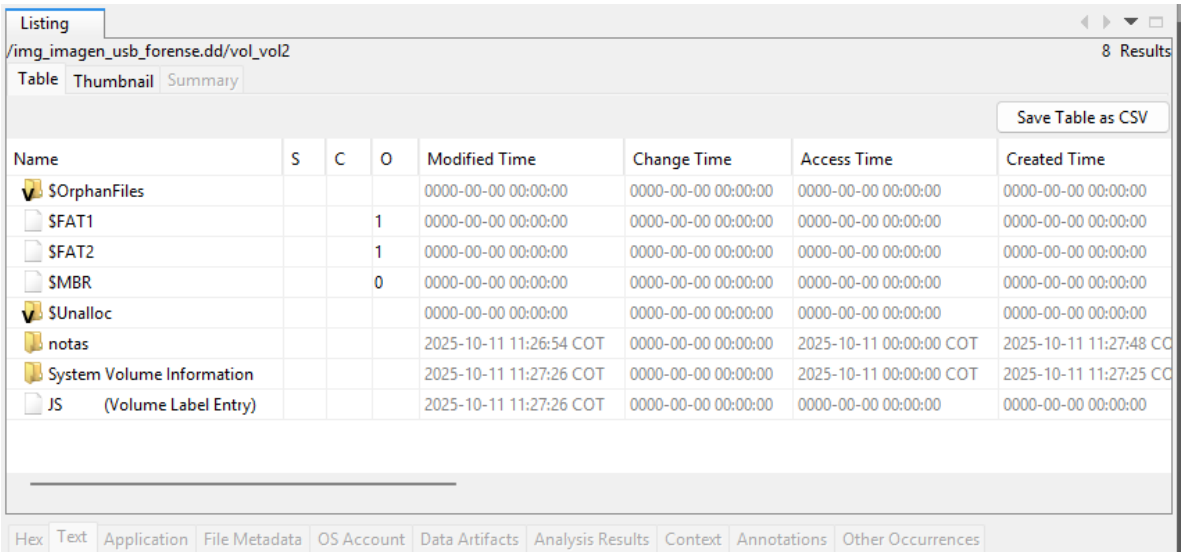


Ilustración 48 Contenido del Volumen Asignado (vol2)

Una vez en el árbol de navegación de la izquierda, se selecciona el volumen activo (vol2) y se resalta el archivo **notas** en el panel de listado. El árbol de resultados de la ingesta muestra categorías como Deleted Files (Archivos Eliminados) y Keyword Hits (Coincidencias de Palabras Clave), lo que indica resultados importantes del análisis forense.

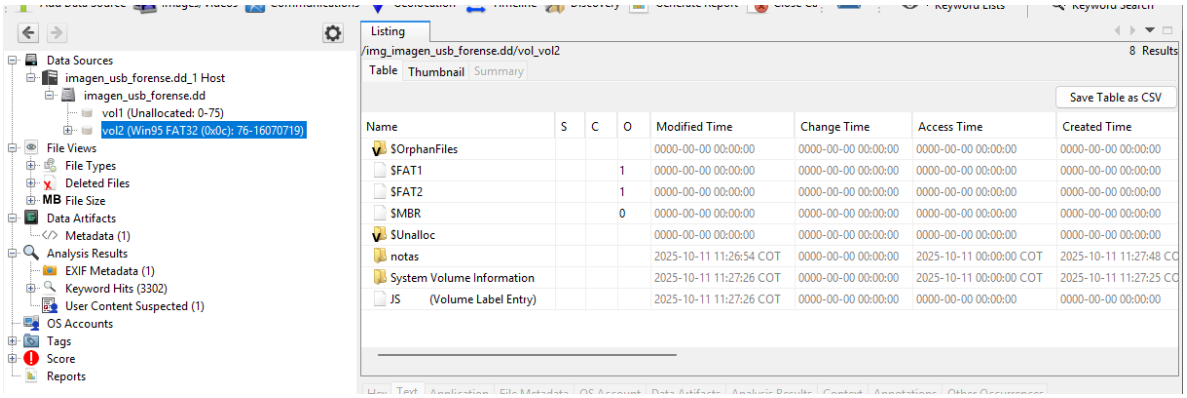


Ilustración 49 Árbol de Evidencia y Navegación del Archivo de Interés

Se selecciona la pestaña **File Metadata** (Metadatos de Archivo) en el panel inferior para el archivo notas. En el panel de texto hexadecimal se comienza a visualizar el contenido interno, permitiendo analizar los *headers* y la estructura a bajo nivel del archivo.

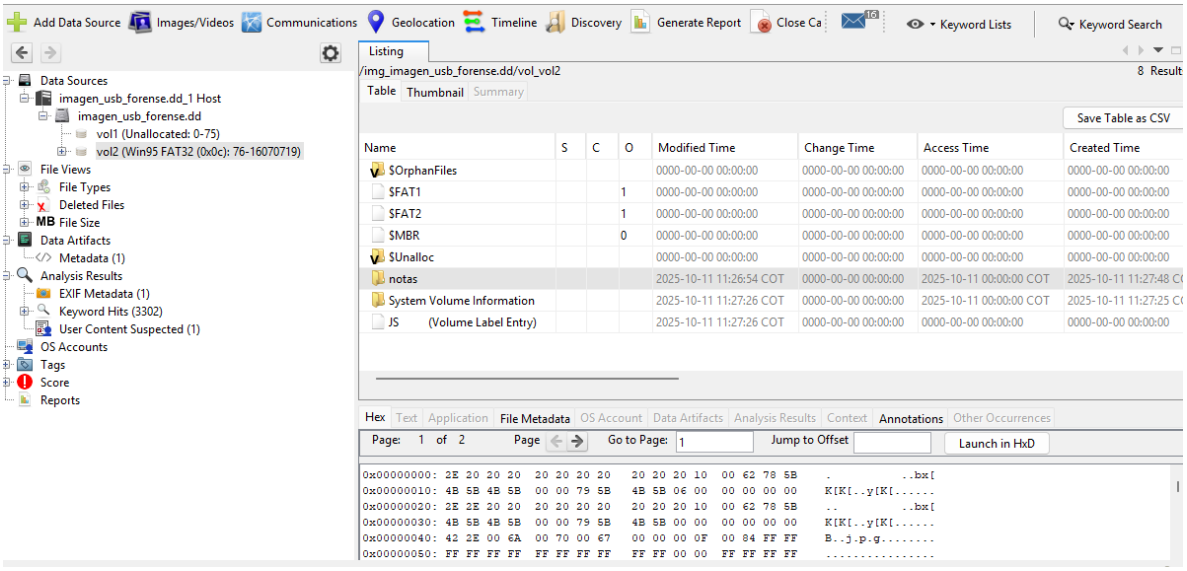
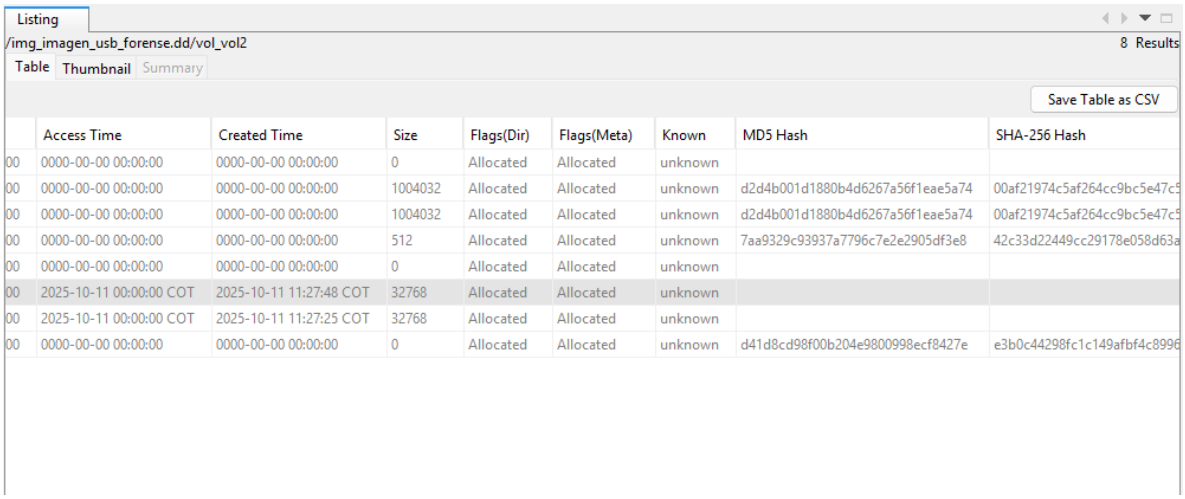


Ilustración 50 Metadatos y Vista de Archivo Seleccionado.

Después me muestra la tabla con los valores *hash* (MD5 y SHA-256) calculados para los archivos dentro del volumen 2. El valor *hash* del archivo **notas** se muestra como

unknown, lo que indica que no es un archivo de sistema conocido y podría ser relevante para la investigación.


Listing
/img_imagen_usb_forense.dd/vol_vol2
8 Results
Table Thumbnail Summary
Save Table as CSV

	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	MD5 Hash	SHA-256 Hash
00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown		
00	0000-00-00 00:00:00	0000-00-00 00:00:00	1004032	Allocated	Allocated	unknown	d2d4b001d1880b4d6267a56f1eae5a74	00af21974c5af264cc9bc5e47c5
00	0000-00-00 00:00:00	0000-00-00 00:00:00	1004032	Allocated	Allocated	unknown	d2d4b001d1880b4d6267a56f1eae5a74	00af21974c5af264cc9bc5e47c5
00	0000-00-00 00:00:00	0000-00-00 00:00:00	512	Allocated	Allocated	unknown	7aa9329c93937a7796c7e2e2905df3e8	42c33d22449cc29178e058d63a
00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown		
00	2025-10-11 00:00:00 COT	2025-10-11 11:27:48 COT	32768	Allocated	Allocated	unknown		
00	2025-10-11 00:00:00 COT	2025-10-11 11:27:25 COT	32768	Allocated	Allocated	unknown		
00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	d41d8cd98f00b204e9800998ecf8427e	e3b0c44298fc1c149afbf4c8996

Ilustración 51 Hashes de los Archivos en el Volumen 2.

5. Capítulo 3

5.1 FTK Imaginar Navegador

En este paso utilizo el navegador web para buscar la herramienta forense **FTK Imager** en el sitio oficial de Exterro. Este paso es fundamental para asegurar la descarga de la versión legítima y más reciente de la herramienta.

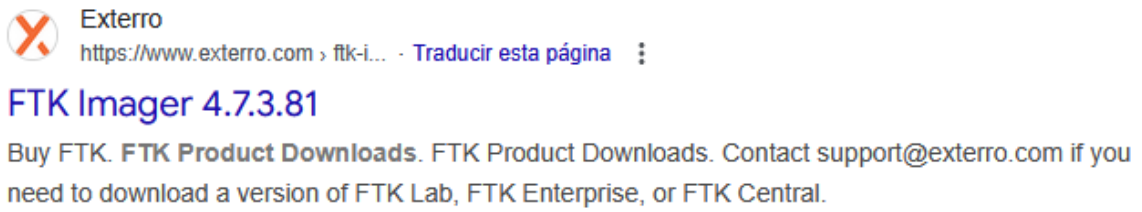

Exterro
https://www.exterro.com › ftk-i... · Traducir esta página
FTK Imager 4.7.3.81
Buy FTK. **FTK Product Downloads**. FTK Product Downloads. Contact support@exterro.com if you need to download a version of FTK Lab, FTK Enterprise, or FTK Central.

Ilustración 52 3] Búsqueda y Acceso al Software

Posterior a eso ingrese a la página y verifique la versión disponible (**FTK Imager 4.7.3.81**) y se observa el valor **MD5 hash (3815b9c2a6aa8898ecbe55353aaf4b79)**. La verificación del hash es una buena práctica forense para confirmar la integridad del archivo descargado.

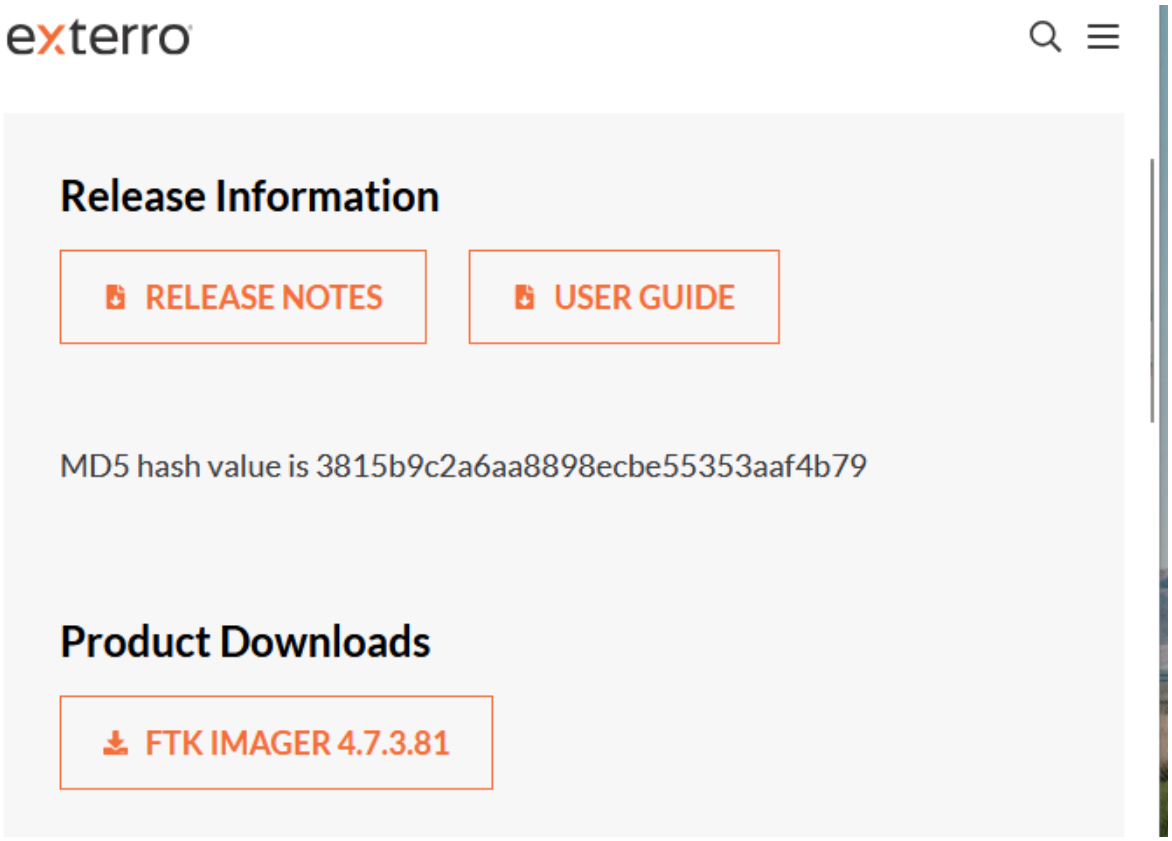


Ilustración 53 Información de la Versión y Hash de Verificación

Para obtener la herramienta gratuita, se completa el formulario de registro con la información del examinador (Nombre, Apellido, Correo Electrónico, Organización y Título Profesional). Este paso forma parte del control de licencias y acceso al software.

Ilustración 54 Registro de Usuario para Descarga.

En la Pantalla principal de Exterro que dirige al enlace de descarga gratuita de FTK Imager, la herramienta estándar en el sector forense para la previsualización y adquisición de datos, qui procedí a darle en descarga gratuita.

Ilustración 55 Página de Descarga del Producto.

Una vez realice esto se muestra la descarga del archivo binario Exterro_FTK_Imager_(x64)-4.7.3.81.exe. El tamaño y el nombre del archivo deben ser verificados.

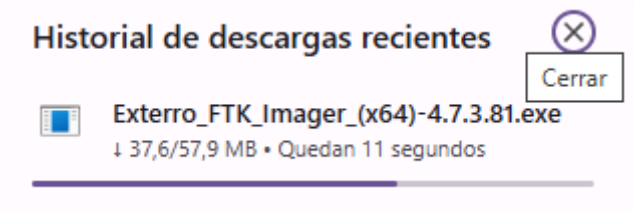


Ilustración 56 Progreso de la Descarga del Fichero Ejecutable.

5.2 INSTALACION DE PROGRAMA DE FTK

Se inicia el instalador de **Exterro FTK Imager** a través del *InstallShield Wizard*, dando la bienvenida y un aviso de protección legal del software.

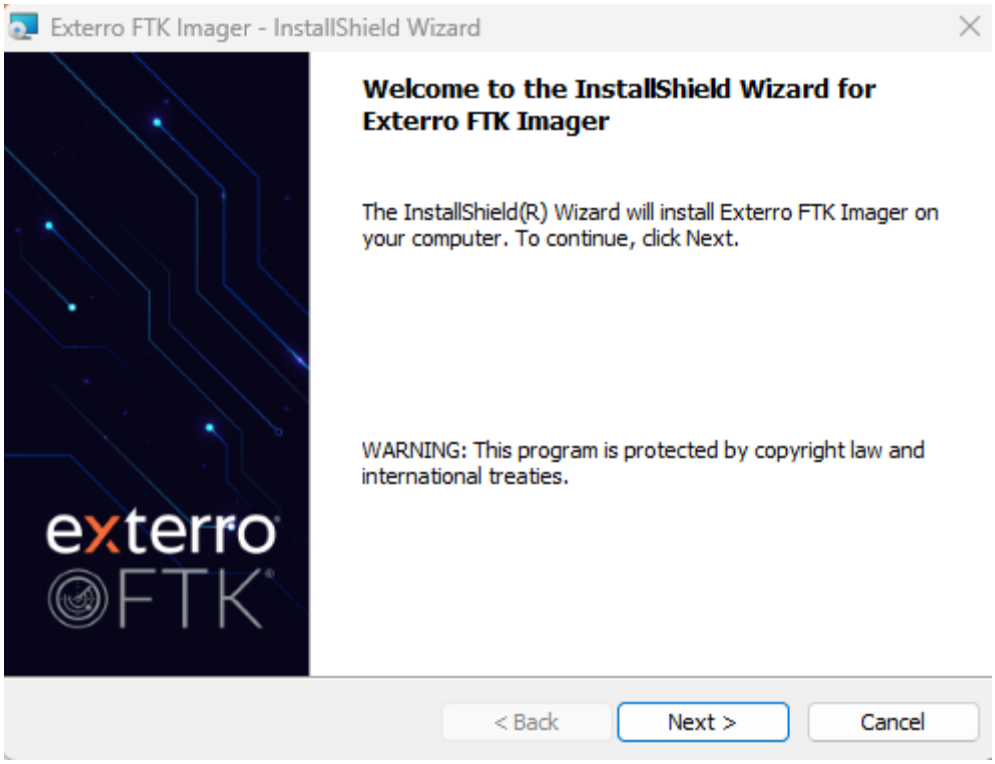


Ilustración 57 Inicio del Asistente de Instalación

Es un paso obligatorio en la instalación. Se acepta el **Acuerdo de Licencia de Usuario Final (EULA)** para proceder con la instalación del software forense.

Ilustración 58 Aceptación del Acuerdo de Licencia (EULA).

Luego se confirma la ruta de instalación por defecto (C:\Program Files\AccessData\) y se marca la opción para **añadir la ruta de instalación a la lista de exclusión de Windows Defender**, lo cual previene posibles interferencias del antivirus durante el uso de la herramienta.

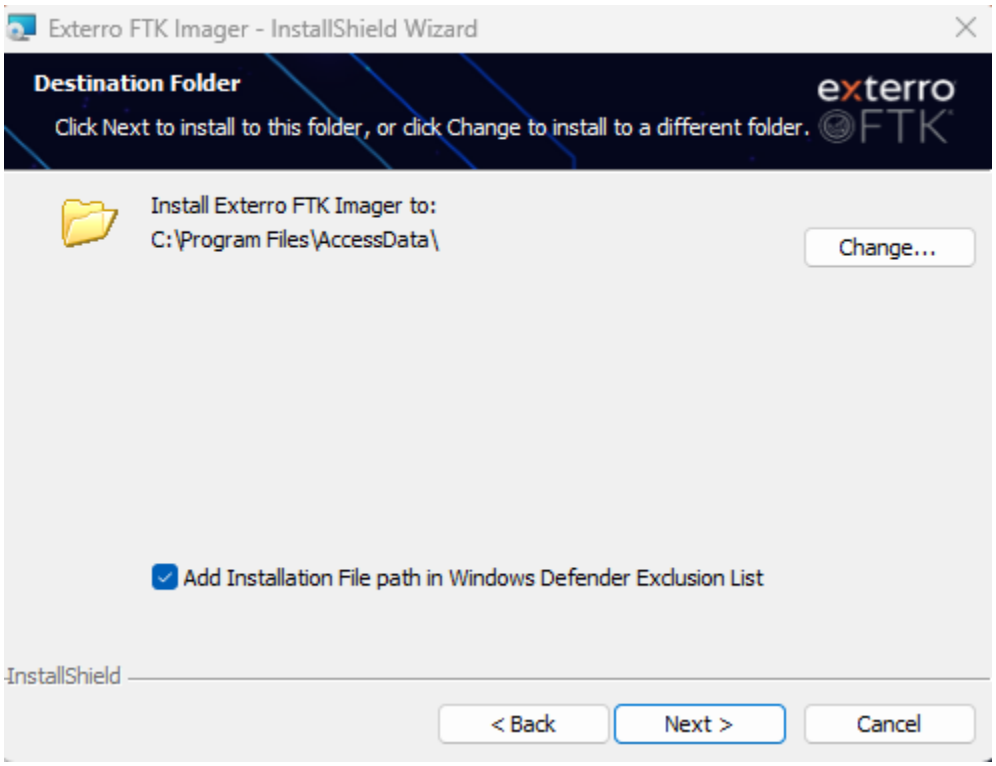


Ilustración 59 Selección de la Carpeta de Destino

Aquí el asistente indica que está listo para iniciar la copia de archivos. Se hace clic en **Install** para comenzar el proceso.

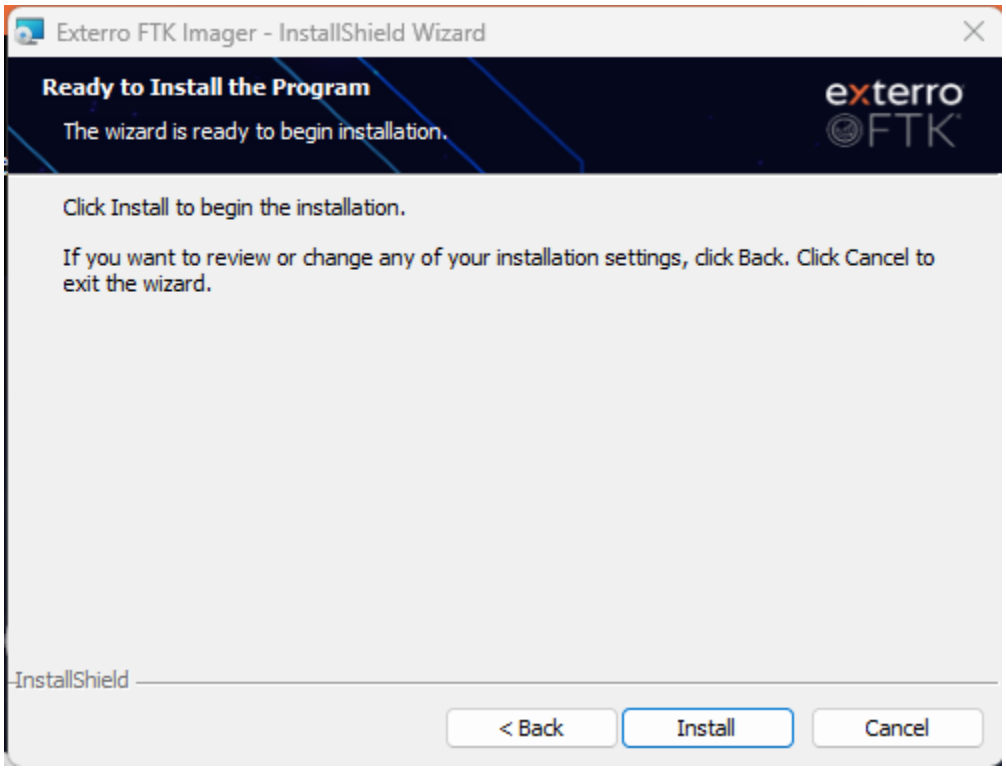


Ilustración 60 Confirmación de Instalación

La instalación se completa exitosamente. Se mantiene marcada la opción **Launch Exterro FTK Imager** para abrir la aplicación de inmediato y comenzar

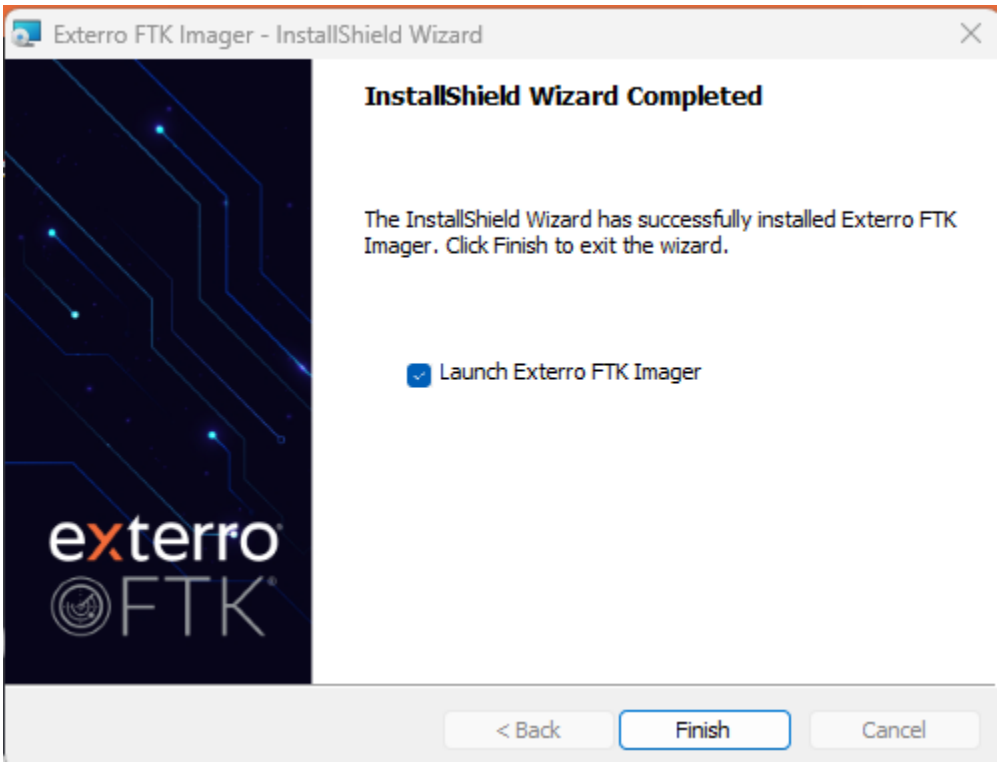


Ilustración 61 Finalización de la Instalación.

5.3 Principal de FTK

Interfaz gráfica inicial de FTK Imager. Presenta el menú de control (Evidence Tree), el panel de listado de archivos (File List) y el panel inferior para la visualización del contenido.

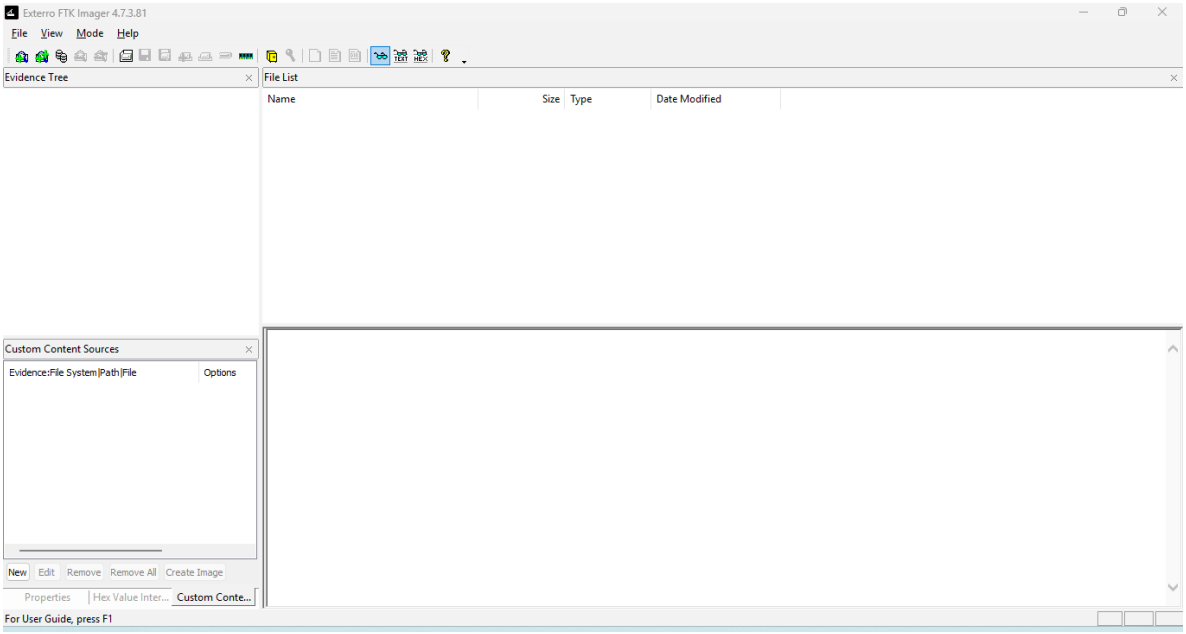


Ilustración 62 Ventana Principal de FTK Imager.

Al iniciar el proceso de adquisición (File > Create Disk Image), seleccione el tipo de fuente de evidencia. En este caso, se elige **Physical Drive** para realizar una copia *bit a bit* del medio físico.

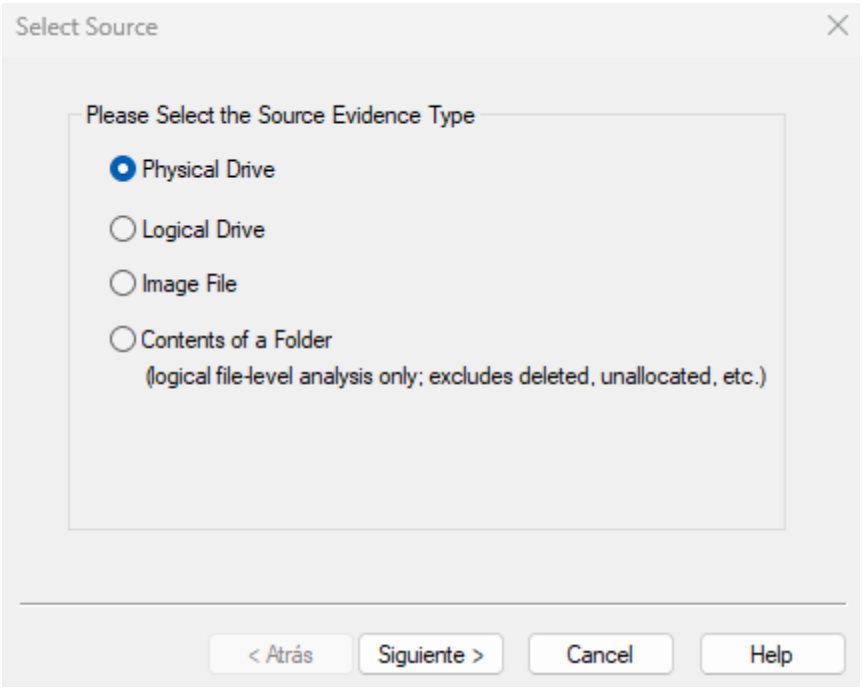


Ilustración 63 Selección de la Fuente de Evidencia.

Luego se identifica y selecciona la unidad de origen para la imagen forense. En este ejemplo, se selecciona la unidad **\.\PHYSICALDRIVE0 - KINGSTON SA400S37240G [240GB ID]**, asegurando la selección correcta antes de proceder.

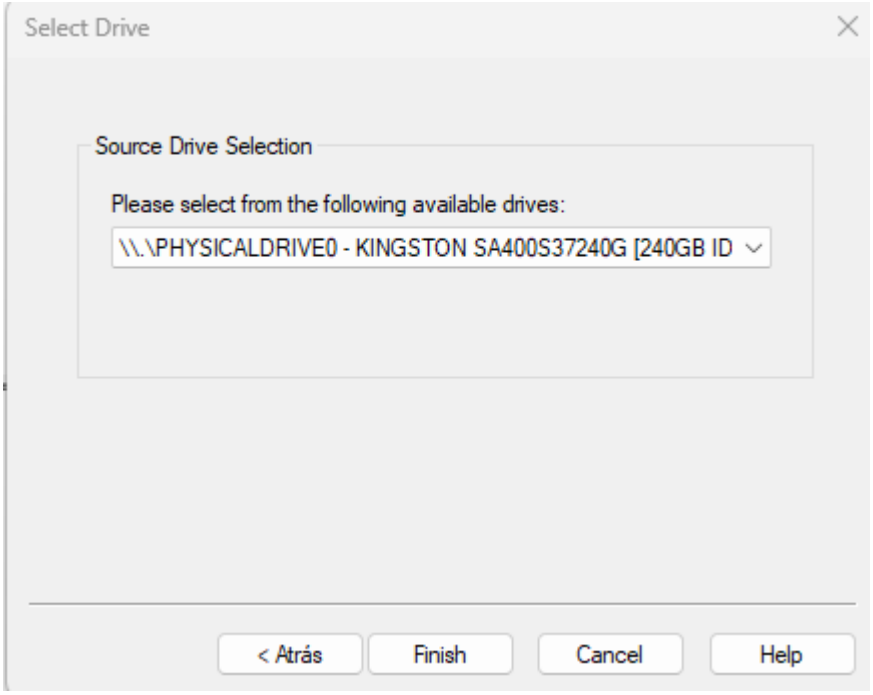


Ilustración 64 Selección de la Unidad Física.

Una vez que se muestra la estructura de directorios y archivos dentro de la fuente de datos cargada. Se pueden observar directorios del sistema de archivos NTFS (como $Recycle.Bin, Program Files, Recovery), metadatos del sistema ($SI30), y archivos regulares.

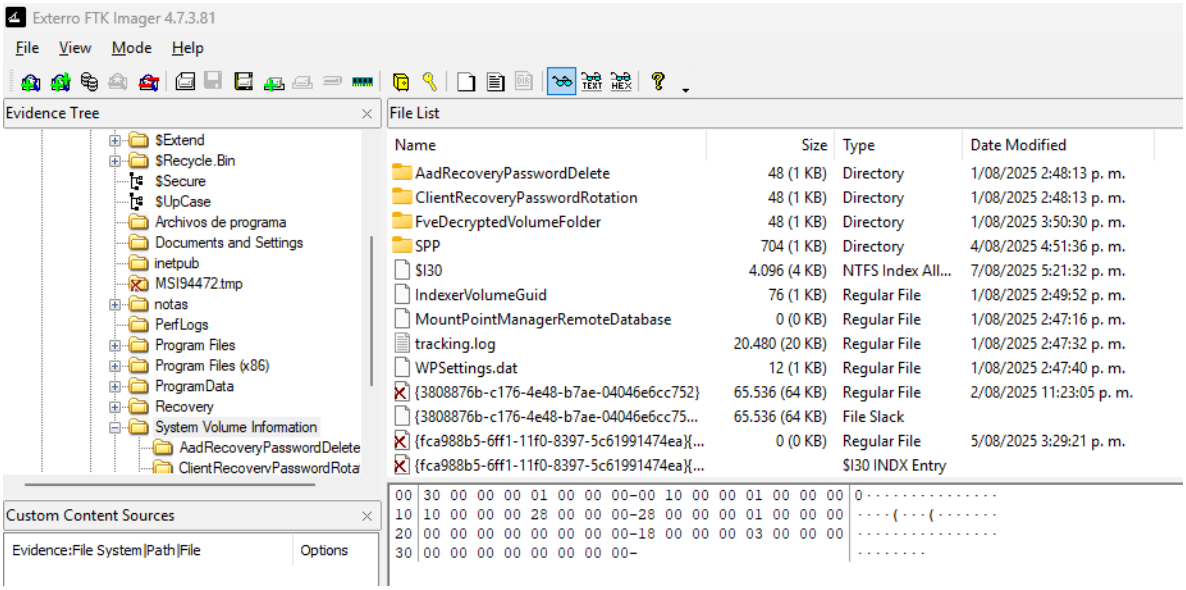


Ilustración 65 Visualización de Archivos y Estructura del Disco.

Aquí se visualiza el contenido de un archivo a nivel de *bytes* en formato hexadecimal. Esta vista es crucial en el análisis forense para examinar datos no visibles o residuales, como el contenido de File Slack o los *Metadata* de un archivo.

File List

Name	Size	Type	Date Modified
AadRecoveryPasswordDelete	48 (1 KB)	Directory	1/08/2025 2:48:13 p. m.
ClientRecoveryPasswordRotation	48 (1 KB)	Directory	1/08/2025 2:48:13 p. m.
FveDecryptedVolumeFolder	48 (1 KB)	Directory	1/08/2025 3:50:30 p. m.
SPP	704 (1 KB)	Directory	4/08/2025 4:51:36 p. m.
$I30	4.096 (4 KB)	NTFS Index All...	7/08/2025 5:21:32 p. m.
IndexerVolumeGuid	76 (1 KB)	Regular File	1/08/2025 2:49:52 p. m.
MountPointManagerRemoteDatabase	0 (0 KB)	Regular File	1/08/2025 2:47:16 p. m.
tracking.log	20.480 (20 KB)	Regular File	1/08/2025 2:47:32 p. m.
WPSettings.dat	12 (1 KB)	Regular File	1/08/2025 2:47:40 p. m.
{3808876b-c176-4e48-b7ae-04046e6cc752}	65.536 (64 KB)	Regular File	2/08/2025 11:23:05 p. m.
{3808876b-c176-4e48-b7ae-04046e6cc75...	65.536 (64 KB)	File Slack	
{fca988b5-6ff1-11f0-8397-5c61991474ea}{...	0 (0 KB)	Regular File	5/08/2025 3:29:21 p. m.
{fca988b5-6ff1-11f0-8397-5c61991474ea}{...		$I30 INDX Entry	

```
000 49 4E 44 58 28 00 09 00-32 B8 7F AD 00 00 00 00 INDX(···2¸·-····
010 00 00 00 00 00 00 00 00-28 00 00 00 90 06 00 00 ········(·······
020 E8 0F 00 00 00 00 00 00-B8 00 00 00 02 00 00 00 è·······¸·······
030 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····************
040 C7 98 01 00 00 00 01 00-88 00 74 00 00 00 00 00 Ç·········t·····
050 B7 92 01 00 00 00 02 00-B1 2C A5 4E F3 02 DC 01 ········±,¥Nó·Ü·
060 B1 2C A5 4E F3 02 DC 01-4D 27 77 97 58 4B DC 01 ±,¥Nó·Ü·M'w·XKÜ·
070 4D 27 77 97 58 4B DC 01-00 00 00 00 00 00 00 00 M'w·XKÜ·········
080 00 00 00 00 00 00 00 00-00 00 00 10 00 00 00 00 ····************
090 19 01 41 00 61 00 64 00-52 00 65 00 63 00 6F 00 ··A·a·d·R·e·c·o·
0a0 76 00 65 00 72 00 79 00-50 00 61 00 73 00 73 00 v·e·r·y·P·a·s·s·
0b0 77 00 6F 00 72 00 64 00-44 00 65 00 6C 00 65 00 w·o·r·d·D·e·l·e·
0c0 74 00 65 00 61 00 74 00-C7 98 01 00 00 00 01 00 t·e·a·t·Ç·······
0d0 68 00 52 00 00 00 00 00-B7 92 01 00 00 00 02 00 h·R·····¸·******
0e0 B1 2C A5 4E F3 02 DC 01-B1 2C A5 4E F3 02 DC 01 ±,¥Nó·Ü·±,¥Nó·Ü·
0f0 4D 27 77 97 58 4B DC 01-4D 27 77 97 58 4B DC 01 M'w·XKÜ·M'w·XKÜ·
100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ····************
110 00 00 00 10 00 00 00 00-08 02 41 00 41 00 44 00 ··········A·A·D·
120 52 00 45 00 43 00 7E 00-31 00 63 00 6F 00 76 00 R·E·C·~·1·c·o·v·
130 BE 92 01 00 00 00 03 00-90 00 7E 00 00 00 00 00 ¾·········~·····
```

Ilustración 66 Vista en Hexadecimal de Archivos Eliminados o Slack Space

Se utiliza la opción **Exportar/Guardar como** para exportar la lista de archivos visibles en formato **CSV**. Este *triage* rápido documenta la evidencia en la ruta de destino seleccionada.

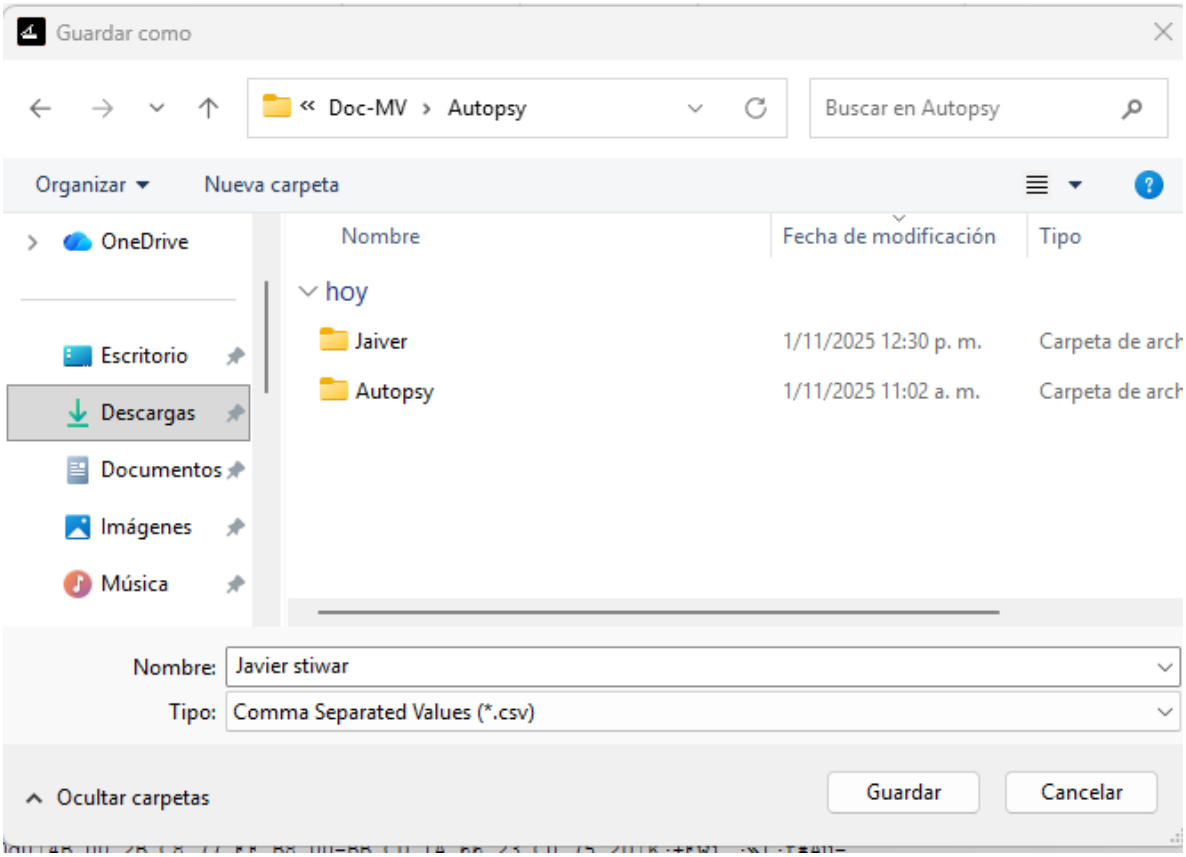


Ilustración 67 Guardado de Listado de Archivos.

verifico en el explorador de archivos que se han generado dos elementos clave: el archivo de la imagen forense (por ejemplo, imagen_usb_forense.dd) y el listado de archivos exportado (Javier stiwar.csv), ambos esenciales para la cadena de custodia.

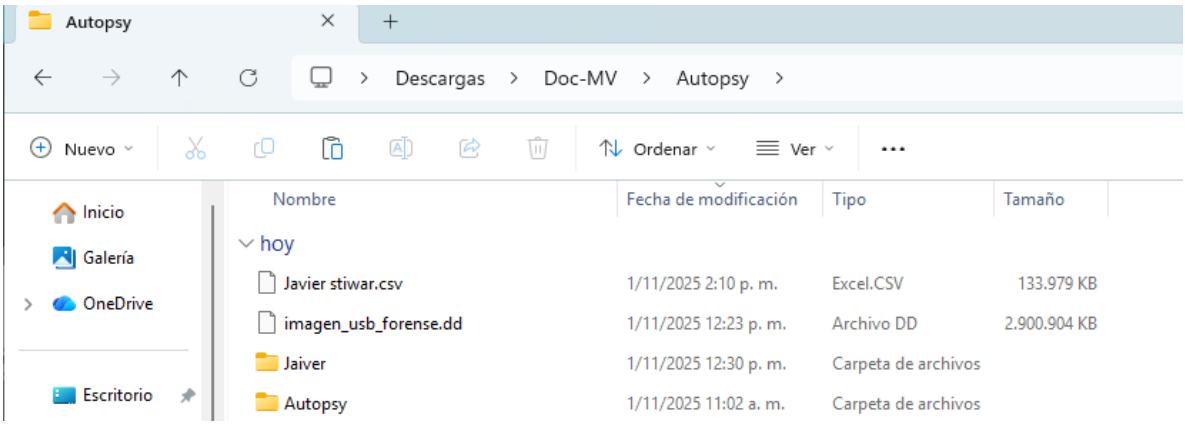


Ilustración 68 Archivo de Imagen y Listado Generado

Posterío a eso abro el archivo **CSV** en Microsoft Excel. La hoja de cálculo organiza datos clave extraídos por FTK Imager, como los valores **MD5** y **SHA-1** de los archivos, y las rutas originales dentro del sistema de archivos. Esta lista sirve como resumen de la evidencia encontrada.

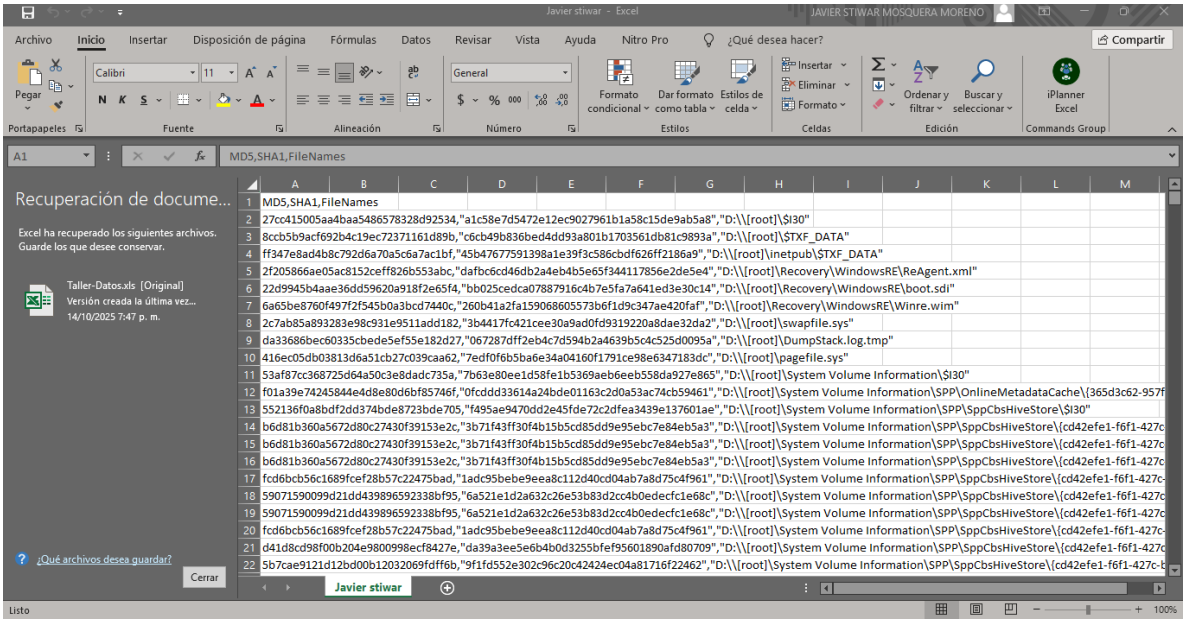


Ilustración 69 Revisión del Listado Exportado en Excel.

6. CONCLUSIÓN

El informe documenta un proceso de **adquisición y análisis forense digital** de un dispositivo USB, logrando establecer un entorno de trabajo formal y **técnico** en el Autopsy Forensic Browser. Sin embargo, el ejercicio ilustra un punto **crítico** en la informática forense: la susceptibilidad de la evidencia a errores **procedimentales**.

La fase de adquisición inicial del dispositivo (dd) se vio **comprometida** por un error de falta de espacio, seguido de un fallo de comando que sobrescribió el archivo de imagen parcial. La subsiguiente verificación de **integridad** en Autopsy validó el fallo al calcular un hash MD5 (D41D8CD98F00B204E9800998ECF8427E), confirmando que la imagen de evidencia estaba **vacía** y, por lo tanto, **inválida** para el análisis.

En resumen, aunque se demostró la competencia en la configuración de la herramienta (creación de caso, host e importación), el resultado final subraya la necesidad **imperativa** de la doble verificación de los recursos (espacio en disco) y la **rigurosa** ejecución de los comandos para mantener la **cadena de custodia** y la validez de la evidencia **digital**.