

# Manual práctico AUTOPSY

---

Autopsy es una herramienta de análisis forense digital de código abierto utilizada principalmente por investigadores, analistas de seguridad y profesionales de la informática forense para examinar y recuperar datos de dispositivos de almacenamiento, como discos duros, unidades flash y otros medios digitales. Desarrollada originalmente por el Departamento de Defensa de los Estados Unidos, Autopsy ofrece una interfaz gráfica amigable que facilita la realización de investigaciones forenses.

## Las funciones principales de Autopsy son:

- **Análisis de imágenes de disco:** permite la creación y el análisis de imágenes de disco completas, lo que permite examinar el contenido de un disco duro o cualquier otro medio de almacenamiento de manera detallada.
  - **Recuperación de archivos eliminados:** Autopsy puede recuperar archivos que han sido borrados, brindando la posibilidad de analizar información que se creía perdida.
  - **Análisis de actividades recientes:** facilita la identificación de las actividades más recientes realizadas en un sistema, lo que es útil para entender el comportamiento y las acciones llevadas a cabo en el dispositivo.
  - **Búsqueda de palabras clave:** permite la búsqueda de palabras clave específicas en todo el medio de almacenamiento, facilitando la localización de información relevante para una investigación.
  - **Identificación de tipos de archivo:** Autopsy puede clasificar y organizar archivos según sus extensiones y firmas internas, facilitando la identificación de diferentes tipos de archivos.
-

- 
- **Análisis de línea de tiempo:** proporciona una visualización de eventos en una línea de tiempo, permitiendo a los investigadores ver cómo y cuándo ocurrieron ciertas actividades en el dispositivo.
  - **Generación de reportes:** permite generar reportes detallados de los hallazgos, que pueden ser utilizados como evidencia en investigaciones legales o internas.
  - **Módulos de ingesta:** Autopsy cuenta con diversos módulos que se pueden activar para realizar análisis específicos, como la búsqueda de hash, la identificación de tipos de archivo, y la búsqueda de palabras clave.

### **Autopsy puede ser utilizado para:**

- **Investigación forense:** Autopsy se utiliza para investigar incidentes de seguridad, analizar comportamientos sospechosos, y recolectar evidencia digital para procesos legales.
- **Auditorías de seguridad:** las organizaciones pueden utilizar Autopsy para auditar sistemas y asegurarse de que no se han producido accesos no autorizados o actividades maliciosas.
- **Recuperación de datos:** profesionales de recuperación de datos pueden utilizar Autopsy para intentar recuperar archivos borrados accidentalmente.
- **Educación y capacitación:** Autopsy es una herramienta valiosa en entornos educativos para enseñar informática forense y análisis de seguridad.

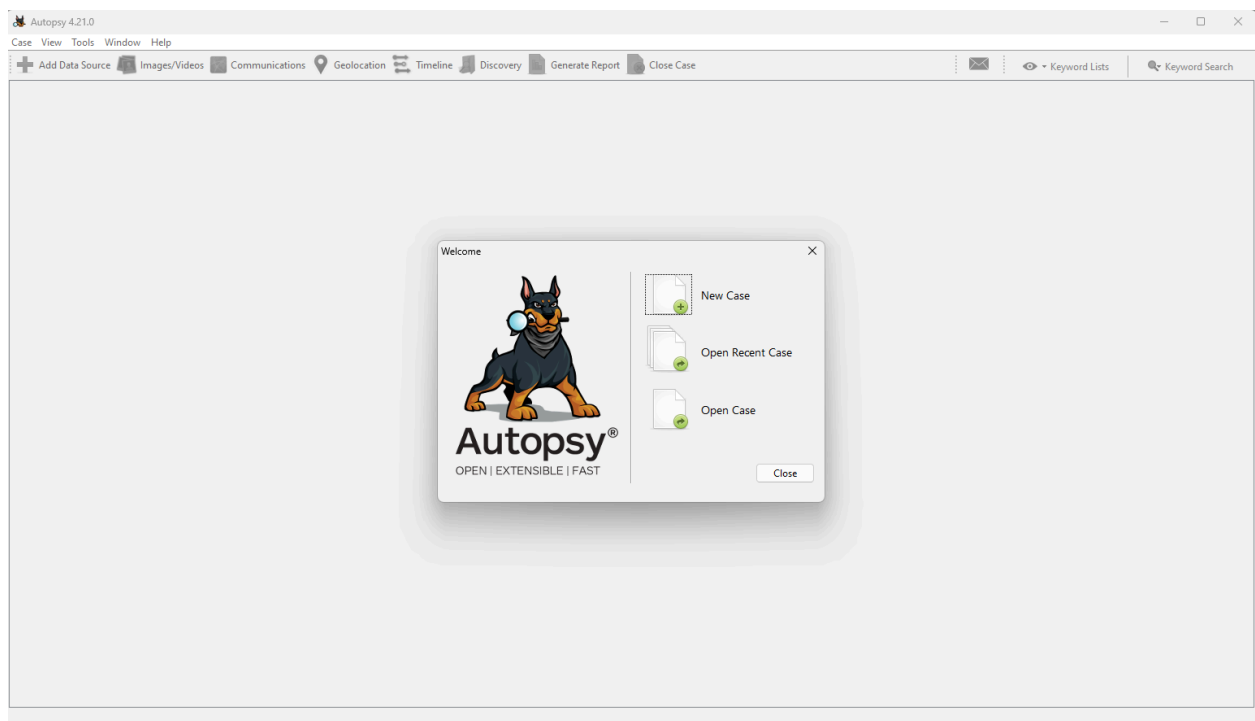
En resumen, Autopsy es una herramienta esencial en el campo de la informática forense, proporcionando una amplia gama de funcionalidades para la recuperación, análisis y reporte de datos digitales.

Para descarga Autopsy podemos hacerlo desde la siguiente liga:

### CREACIÓN DE UN NUEVO CASO

Primero, asegúrate de que todos los componentes necesarios estén instalados y el software esté funcionando correctamente. Al abrir un nuevo caso te solicitará ingresar detalles básicos y información relevante para tu investigación. Este proceso inicial es crucial ya que organiza y estructura tu análisis, permitiéndote rastrear y gestionar eficientemente todos los datos y hallazgos durante la investigación forense.

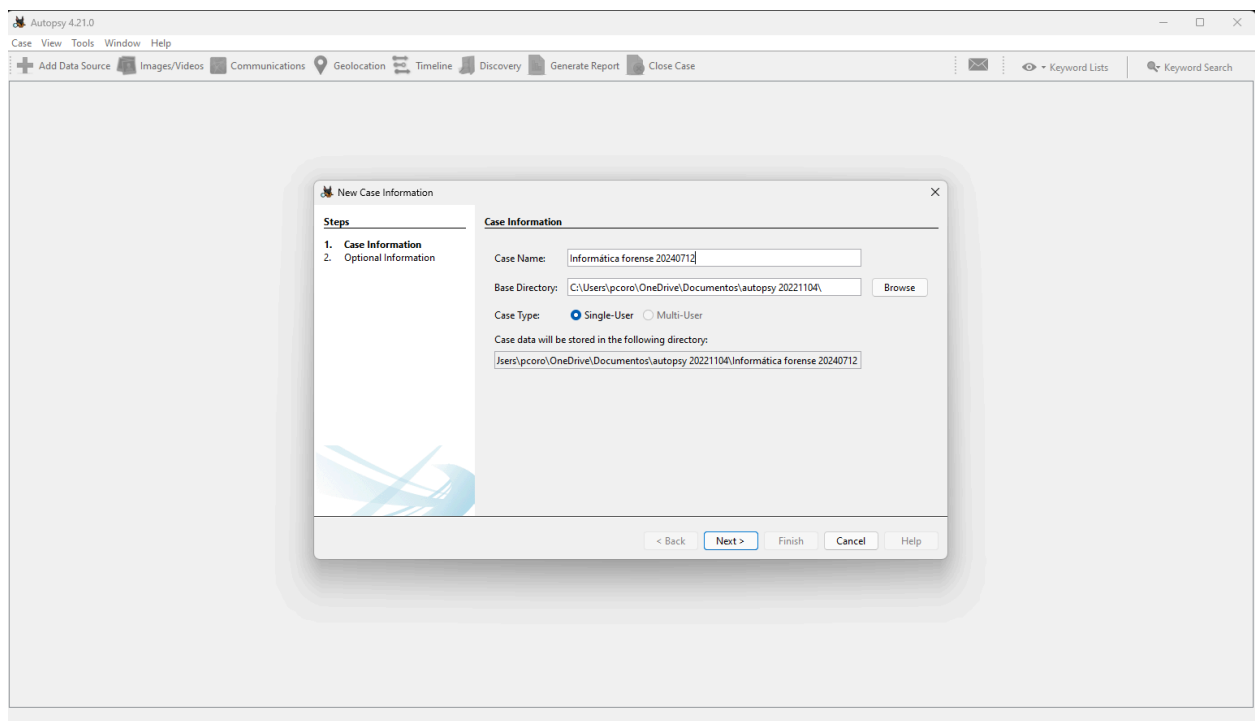
Inicia la herramienta Autopsy en tu sistema operativo Windows. Una vez que el programa esté abierto, dirígete a la opción que dice "New Case" o "Nuevo Caso". Esta función te permitirá comenzar un nuevo proyecto de análisis forense. Aquí es donde configurarás un nuevo caso en el que podrás importar y examinar datos digitales.



---

## Crear nuevo caso en Autopsy

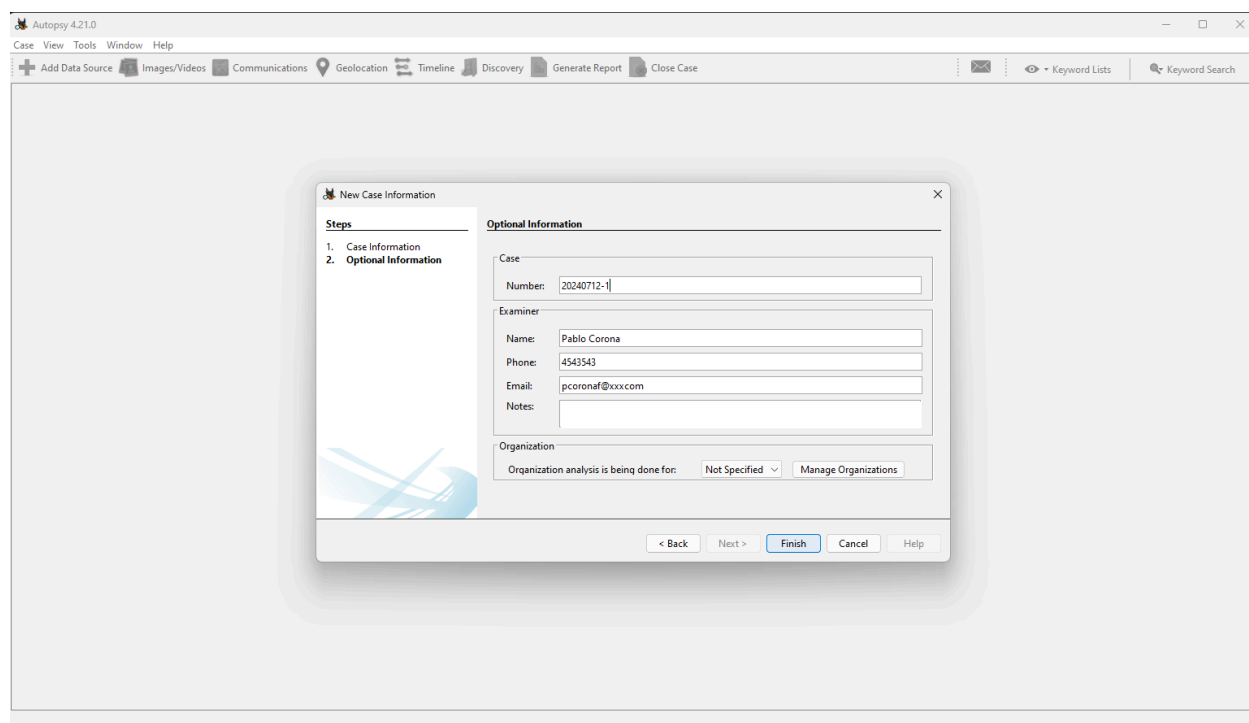
A continuación, completa toda la información requerida para el caso. Ingresa un nombre descriptivo para identificar fácilmente el caso en el futuro. Luego, selecciona un directorio base donde se almacenarán todos los datos asociados con este caso. Este directorio servirá como el lugar centralizado para guardar todos los archivos, informes y evidencias que vayas recopilando durante tu investigación. Es importante elegir una ubicación adecuada y segura para garantizar que toda la información esté organizada y accesible cuando la necesites.



### Información de caso

También tienes la opción de agregar información adicional sobre el caso si lo consideras necesario. Esto puede incluir detalles como el número de caso, los nombres de los investigadores involucrados, la fecha de inicio de la investigación y cualquier otra información relevante que pueda ser útil para el seguimiento y la documentación del caso.

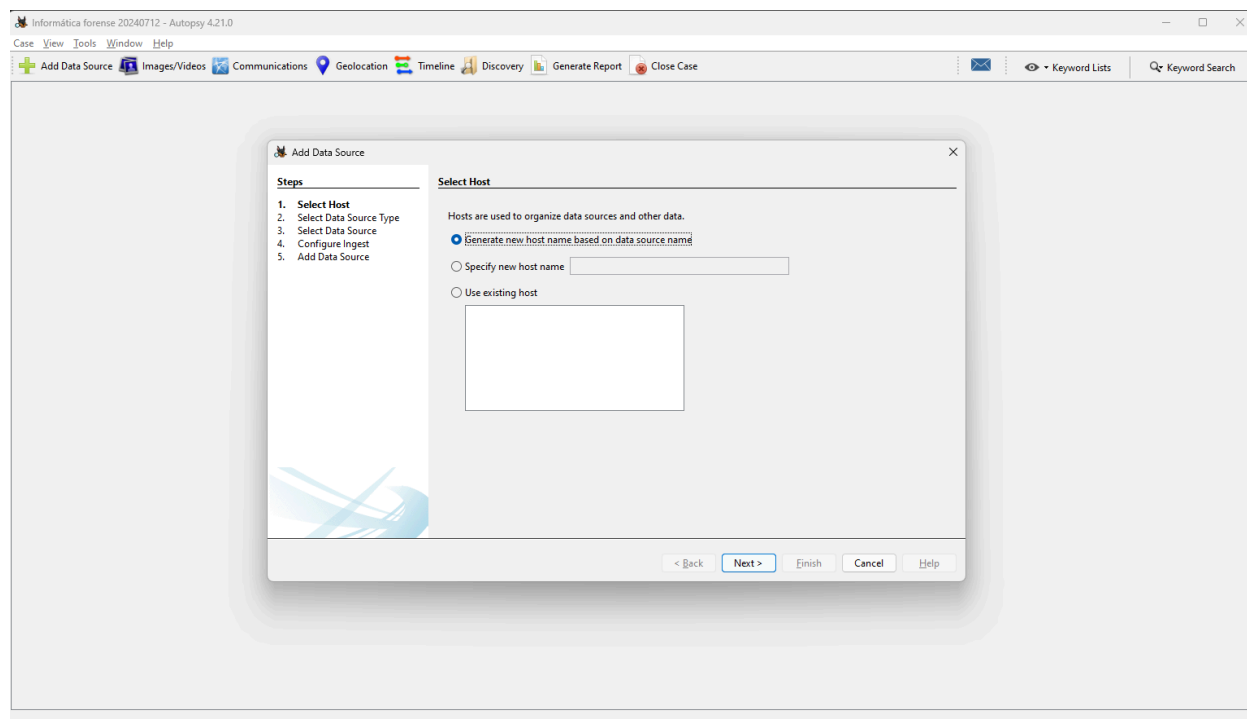
Añadir estos detalles adicionales puede ayudar a proporcionar un contexto más completo y facilitar la organización y el manejo del caso a lo largo del proceso de análisis.



## Información opcional adicional

Selecciona el lugar donde se almacenará la información del caso. Puedes optar por crear un nuevo host o utilizar uno existente si ya has creado uno previamente. En este caso, elegiremos la opción predeterminada de crear un nuevo host o utilizar uno existente.

Esta elección permitirá organizar y gestionar la información de manera eficiente, asegurando que todos los datos relevantes del caso estén accesibles y centralizados en un único lugar.



## Host name

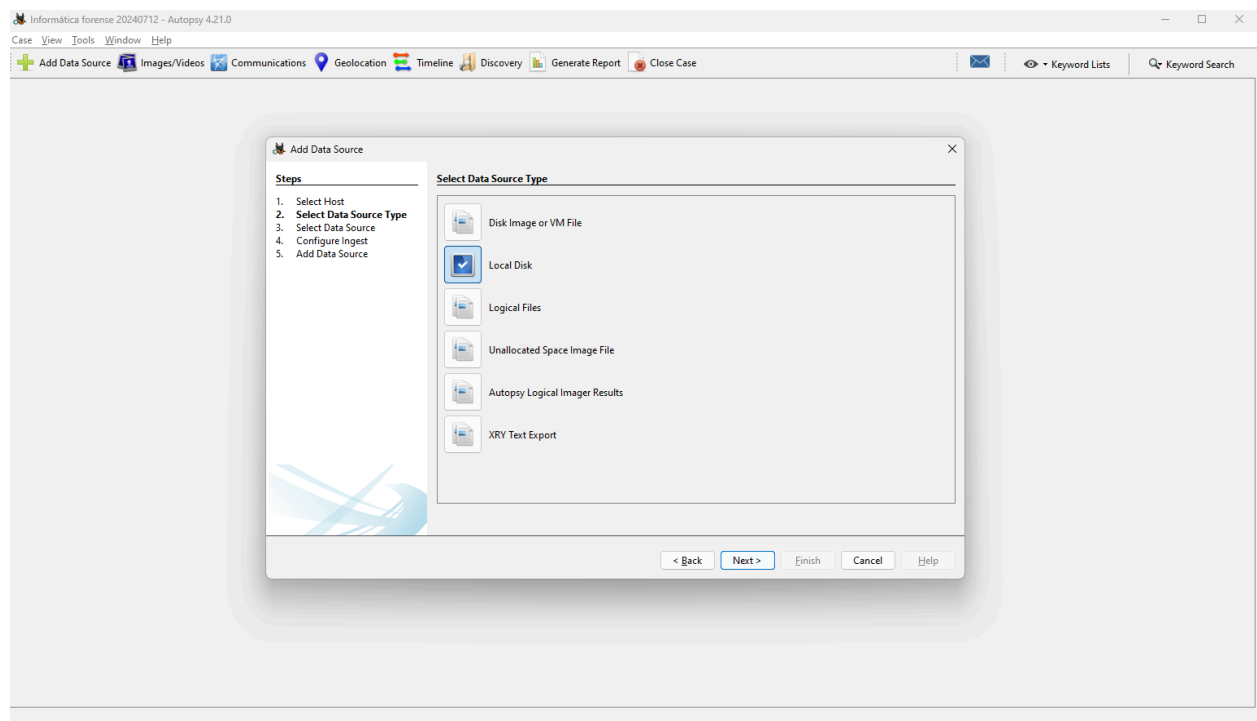
Ahora vamos a añadir el tipo de fuente de datos que vamos a analizar. Hay varias opciones disponibles para elegir según el tipo de datos que necesitas examinar:

- **Disk Image or VM file (Archivo de imagen de disco o máquina virtual):** Esta opción permite trabajar con archivos de imagen que son copias exactas de un disco duro, una tarjeta de memoria o incluso una máquina virtual.
- **Local Disk (Disco Local):** Incluye dispositivos de almacenamiento físico conectados al sistema, como discos duros, unidades USB, tarjetas de memoria, entre otros.
- **Logical Files (Archivos Lógicos):** Permite analizar imágenes de carpetas o archivos específicos que se encuentran en el sistema local.
- **Unallocated Space Image File (Archivo de imagen de espacio no asignado):** Estos son archivos que no contienen un sistema de archivos

definido y se analizan mediante el uso del módulo Ingest para extraer datos útiles.

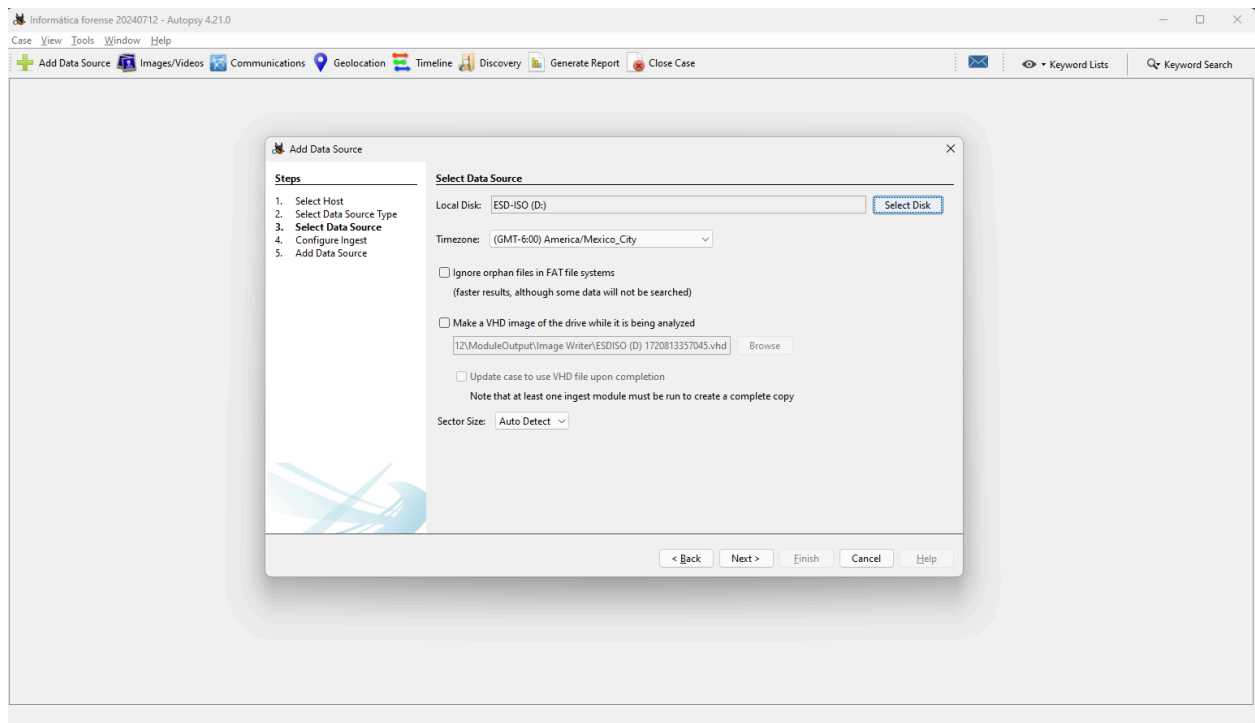
- **Autopsy Logical Imager Results (Resultados del Imager Lógico de Autopsy):** Utiliza las fuentes de datos generadas por la herramienta de creación de imágenes lógicas de Autopsy.
- **XRY Text Export (Exportación de texto de XRY):** Permite analizar datos exportados en formato de texto desde la herramienta XRY, utilizada comúnmente en análisis forense de dispositivos móviles.

Selecciona el tipo de fuente de datos que mejor se ajuste a tu caso para proceder con el análisis forense.



## Tipos de Fuente de datos

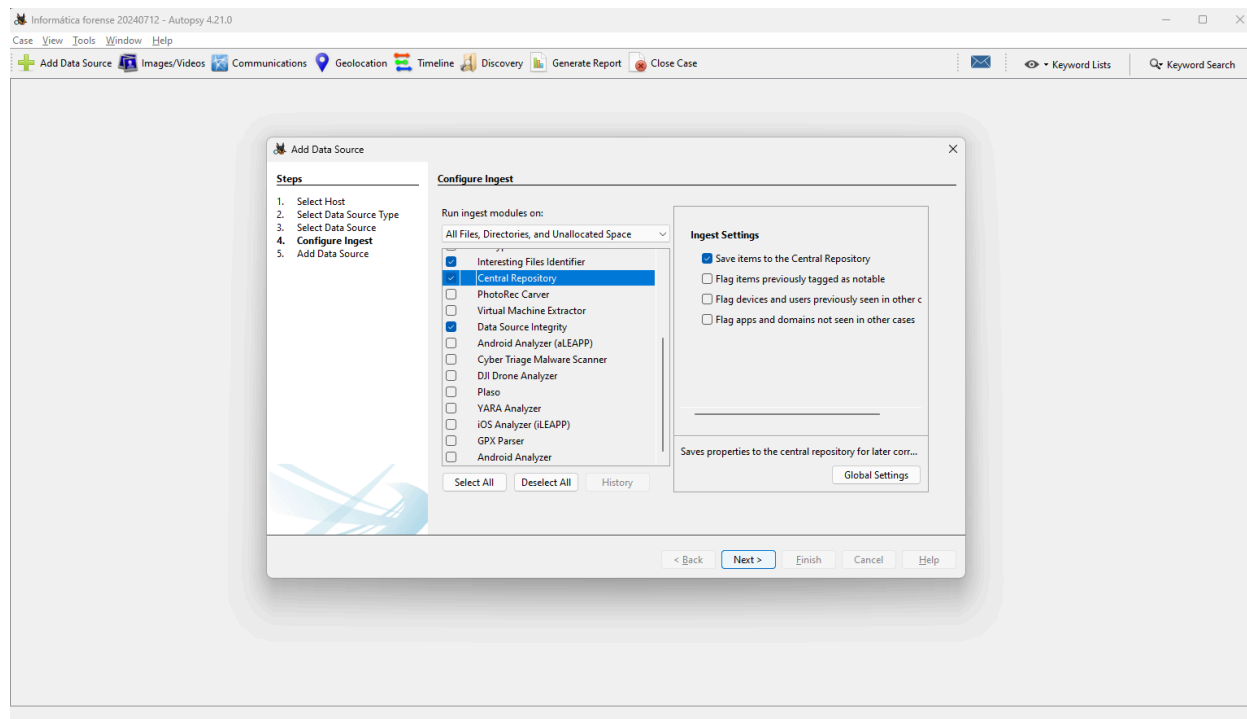
Ahora vamos a añadir la fuente de datos. En este caso, seleccionaremos un dispositivo USB. Para hacerlo, elige la opción "Local Disk" (Disco Local). Luego, selecciona el disco correspondiente al dispositivo USB que desees agregar para el análisis. Este paso es crucial para asegurarte de que el contenido del dispositivo sea correctamente identificado y analizado dentro de tu caso forense.



## Analizar unidad USB

A continuación, se te solicitará que configures el módulo Ingest. Este módulo es responsable de procesar y analizar los datos de la fuente seleccionada. Aquí podrás elegir y activar diferentes módulos de análisis según las necesidades específicas de





## Configurar módulo Ingest

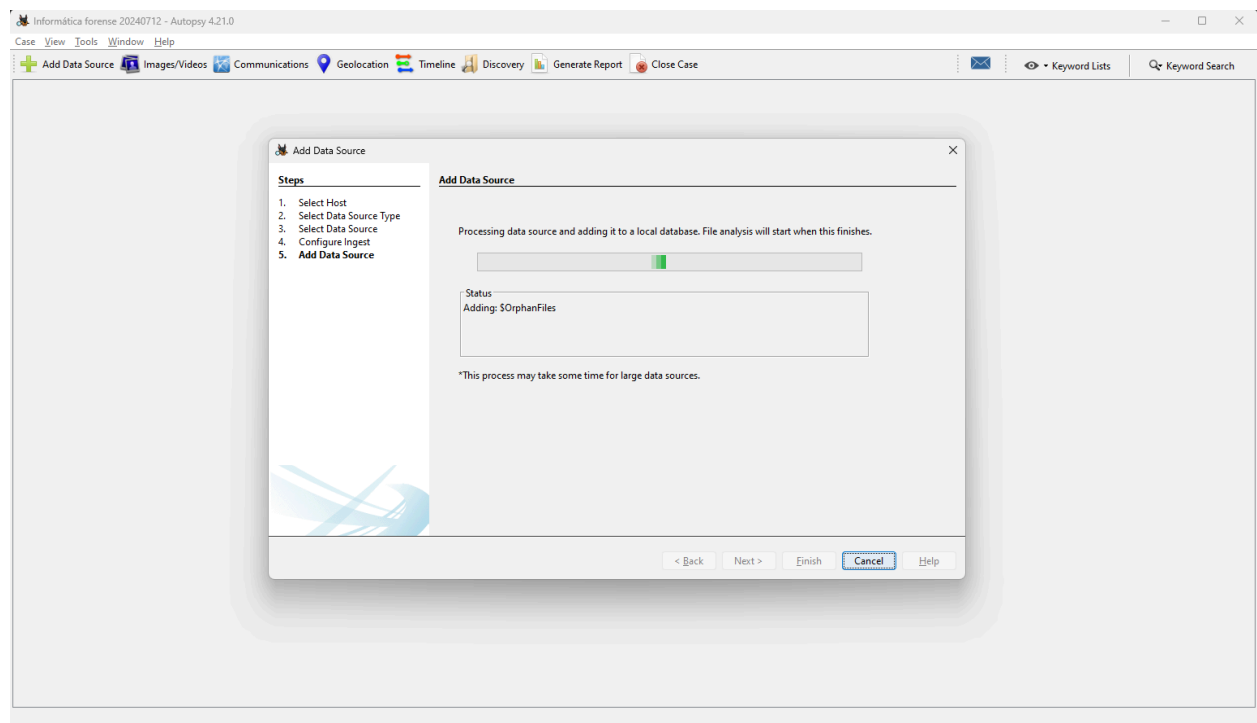
El módulo Ingest incluye una serie de submódulos que se pueden configurar para realizar diversos análisis sobre la fuente de datos seleccionada. A continuación se detalla el contenido y la descripción de cada submódulo disponible:

- **Recent Activity:** Utilizado para descubrir las operaciones recientes realizadas en el disco, como los archivos abiertos recientemente.
- **Hash Lookup:** Identifica archivos específicos mediante sus valores hash, permitiendo verificar la integridad y autenticidad de los archivos.
- **File Type Identification:** Identifica archivos basándose en sus firmas internas, no solo en sus extensiones, para asegurar una correcta categorización.
- **Extension Mismatch Detector:** Detecta archivos cuyas extensiones han sido alteradas para ocultar su verdadero contenido.
- **Embedded File Extractor:** Extrae archivos incrustados dentro de otros archivos, como archivos comprimidos (.zip, .rar), para su posterior análisis.

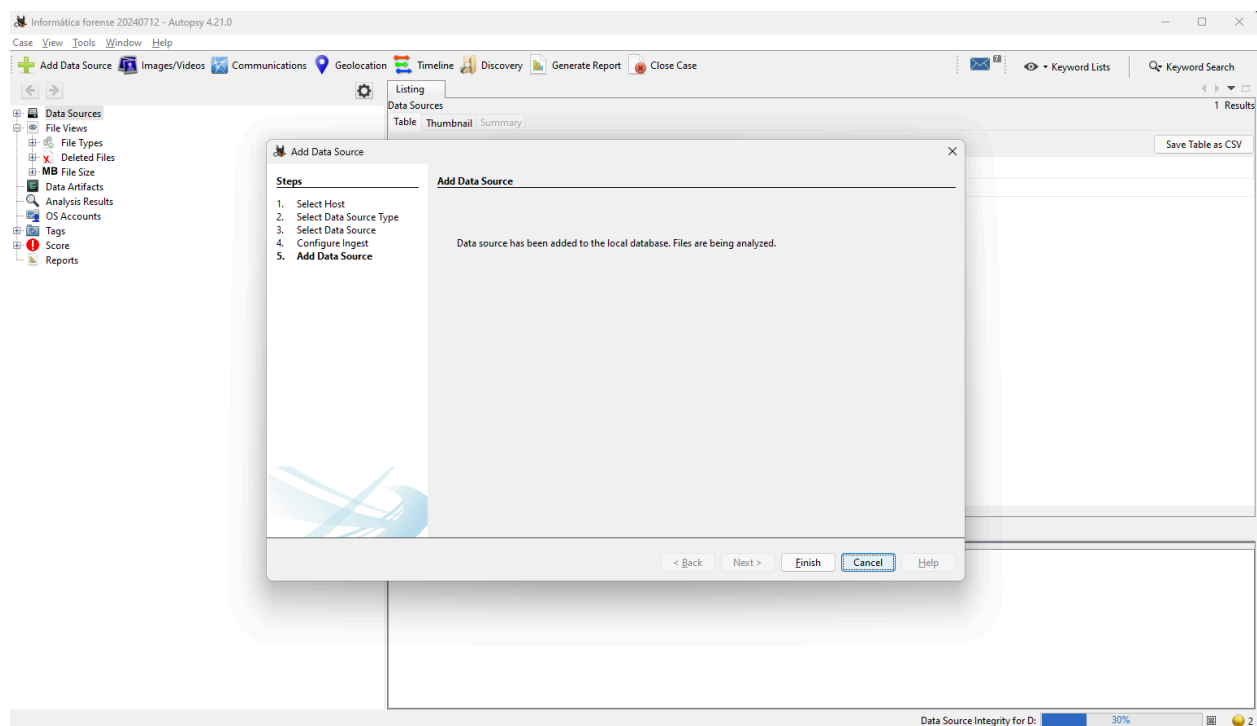
- 
- **Keyword Search:** Permite buscar palabras clave específicas o patrones dentro de la imagen del disco, facilitando la localización de información relevante.
  - **Email Parser:** Extrae información de archivos de correo electrónico, útil si la fuente de datos contiene bases de datos de correos.
  - **Encryption Detection:** Ayuda a detectar e identificar archivos protegidos por contraseña o encriptados.
  - **Interesting File Identifier:** Notifica al examinador cuando se encuentran archivos que corresponden a un conjunto de reglas predefinidas, facilitando la identificación de archivos relevantes.
  - **Central Repository:** Guarda propiedades en un repositorio central para su posterior correlación y análisis.
  - **PhotoRec Carver:** Permite recuperar archivos, fotos y otros datos del espacio no asignado en la imagen del disco.
  - **Virtual Machine Extractor:** Extrae y analiza máquinas virtuales encontradas en la imagen del disco.
  - **Data Source Integrity:** Calcula el valor hash de la fuente de datos y lo almacena en la base de datos para verificar la integridad.

Estos módulos son esenciales para realizar un análisis exhaustivo y detallado de la fuente de datos seleccionada, proporcionando diversas herramientas y técnicas para descubrir, extraer y analizar la información contenida en el dispositivo.

El proceso de ingesta puede tardar algunos minutos, incluso horas, dependiendo del tamaño del medio de almacenamiento que estamos capturando.



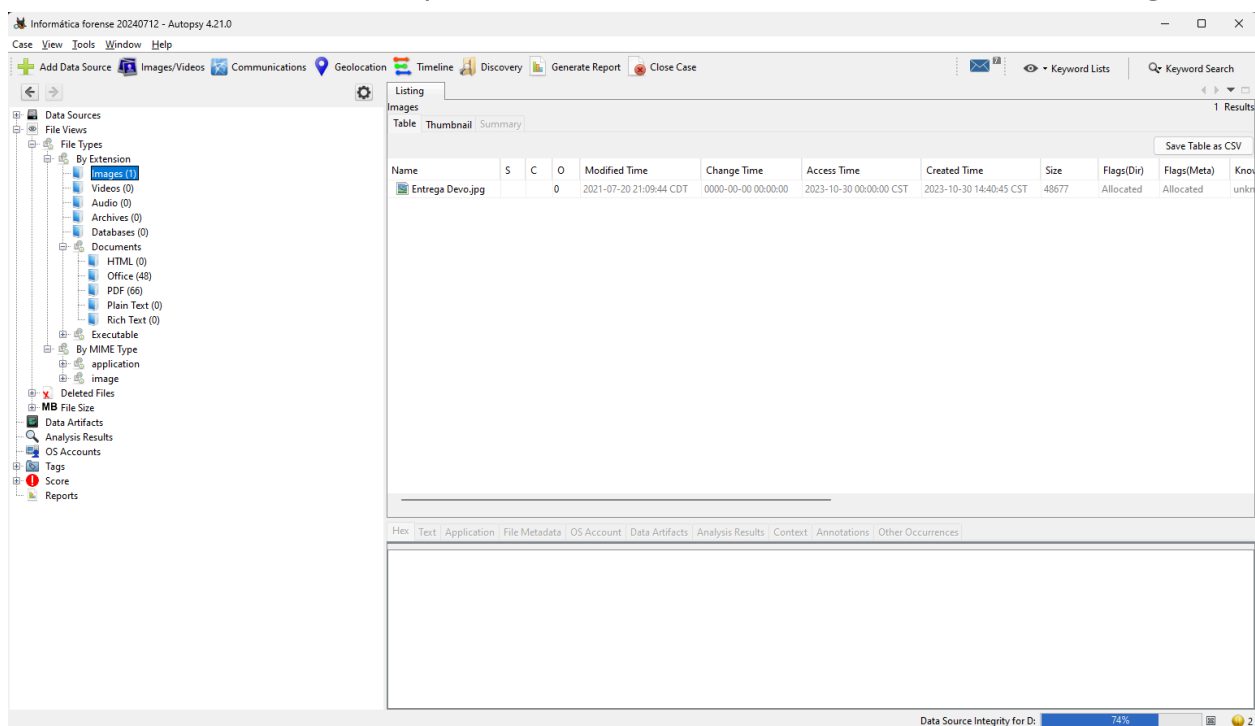
Una vez que concluya nos mostrará que la fuente de datos fue agregada a la base de datos.



## Resultados del Módulo Ingest

La información de la fuente de datos (Data Source) muestra los metadatos básicos del dispositivo seleccionado, como el tamaño del disco, el sistema de archivos, y otros detalles técnicos relevantes. Un análisis más detallado de estos datos se presenta en la parte inferior de la pantalla.

Puedes examinar esta información de manera secuencial, extrayendo y analizando cada elemento uno tras otro para obtener una comprensión completa del contenido y las características del dispositivo. Este proceso te permite identificar rápidamente áreas de interés y profundizar en los datos específicos que sean relevantes para tu investigación.



## Información de Data Source

### ESTRUCTURA DEL CASO

La estructura del caso en Autopsy permite clasificar los archivos según su extensión de archivo o tipo MIME. Esto proporciona una visión clara de cómo los archivos son utilizados y manejados por el sistema operativo y los navegadores web.

---

## File Type (Tipo de archivo):

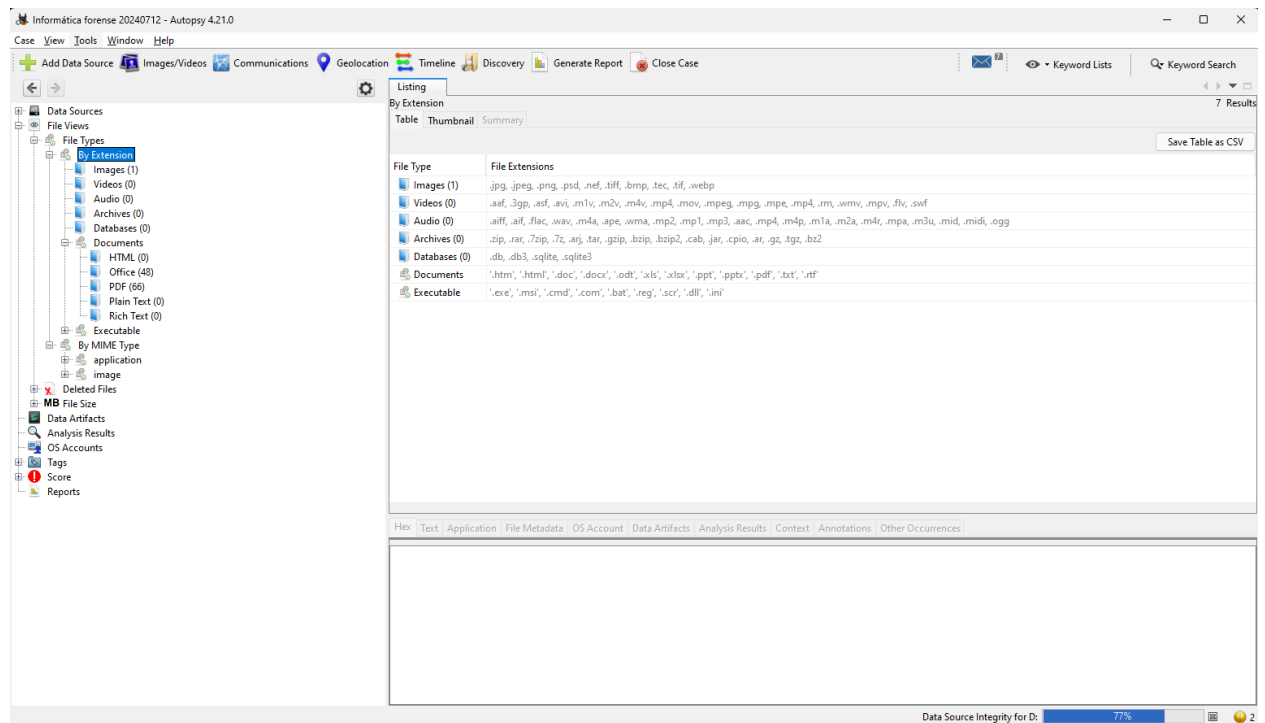
- **Extensiones de Archivo:** Proporciona información sobre las extensiones de archivo comunes que son reconocidas y utilizadas por el sistema operativo.
- **Tipos MIME:** Utilizados por los navegadores web para determinar cómo representar y manejar diferentes tipos de datos.

Además, esta sección también muestra los archivos eliminados, permitiendo recuperar y analizar información que ha sido borrada del sistema.

## Clasificación de Tipos de Archivo:

- **Extension (Extensión):** Archivos clasificados según su extensión, como .txt, .jpg, .pdf, etc.
- **Documents (Documentos):** Archivos de documentos, incluyendo archivos de texto, hojas de cálculo, presentaciones, entre otros.
- **Executables (Ejecutables):** Archivos ejecutables que pueden incluir programas y scripts.

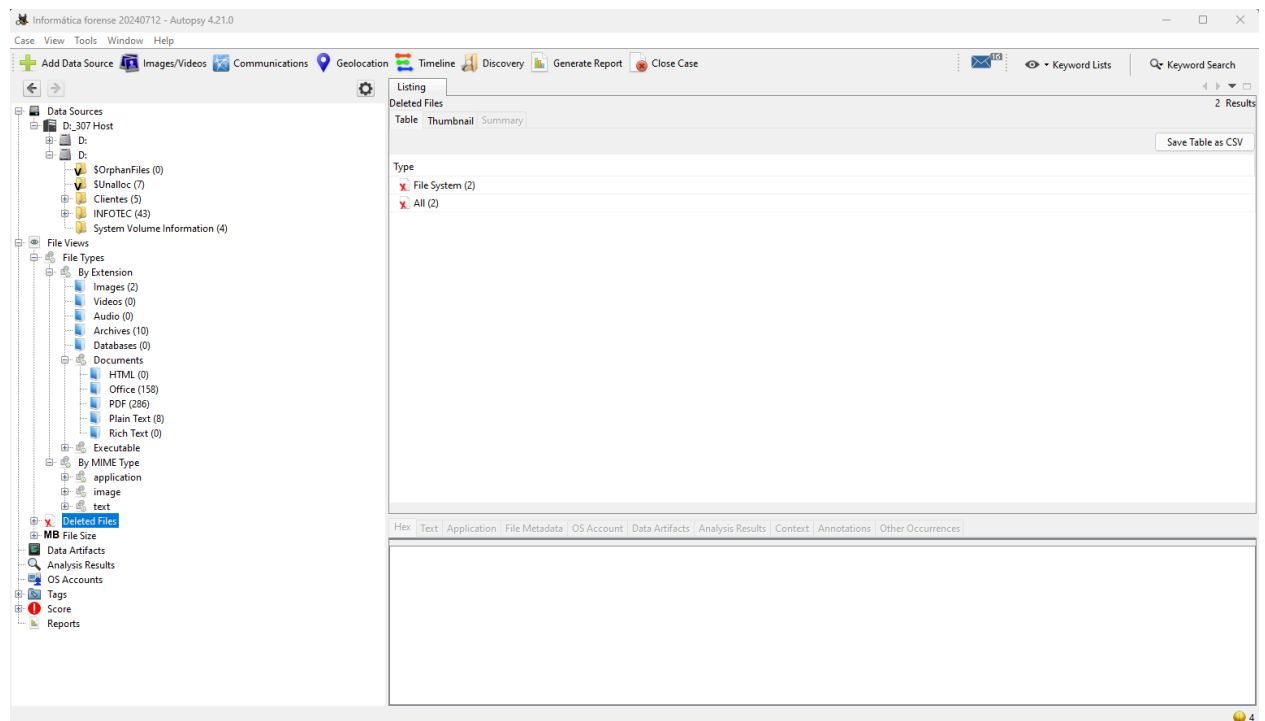
**Nota:** Esta clasificación permite una organización eficiente de los archivos, facilitando la búsqueda y análisis de tipos de archivos específicos que pueden ser relevantes para la investigación forense.



Sección

File

Types



---

## Vista por Extensión

En la categoría **Tipos de archivo por extensión (By Extension)**, los archivos están subdivididos en varias categorías específicas, tales como imágenes, vídeos, audios, archivos comprimidos, bases de datos, entre otros.

### 1. Explorar Imágenes:

- Haz clic en la subcategoría de imágenes para explorar todas las imágenes que se han recuperado.
- Esta acción te permitirá examinar visualmente cada imagen y determinar su relevancia para el caso.

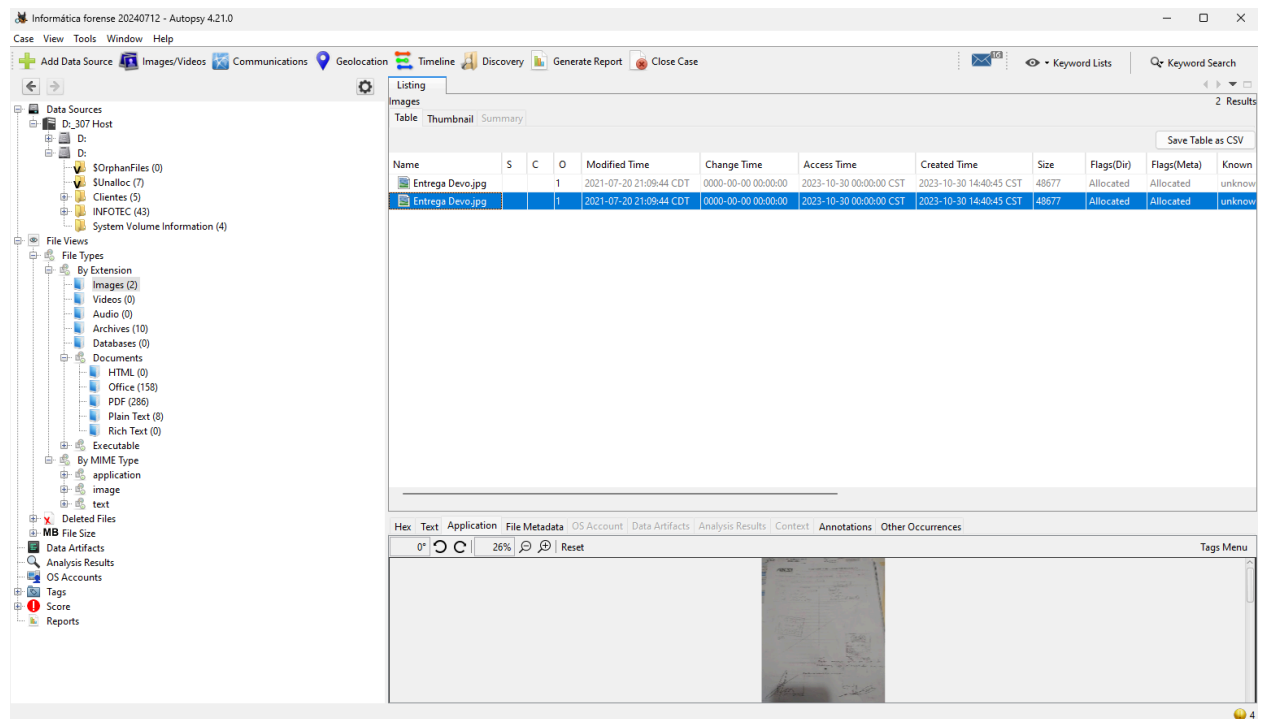
### 2. Filtros By Extension:

- Utiliza los filtros disponibles para refinar tu búsqueda dentro de la categoría seleccionada.
- Los filtros te ayudarán a localizar rápidamente archivos específicos según su extensión, optimizando así el proceso de análisis.

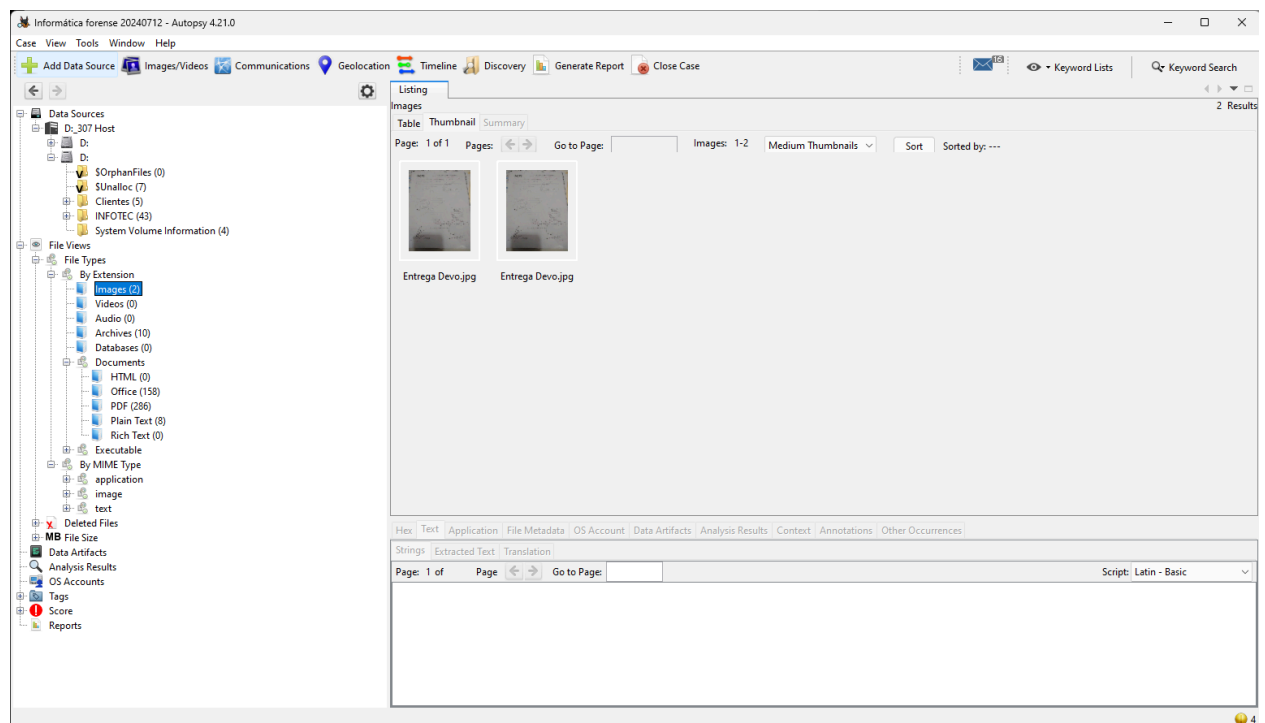
### 3. Miniaturas de Imágenes:

- Además, es posible ver miniaturas de las imágenes, lo que facilita la identificación rápida de archivos de interés sin necesidad de abrir cada uno individualmente.
- Las miniaturas proporcionan una vista previa visual, ahorrando tiempo y mejorando la eficiencia durante el análisis.

Esta funcionalidad de clasificación y visualización por extensión permite organizar y analizar grandes volúmenes de datos de manera eficiente, ayudando a los investigadores a centrarse en los archivos más pertinentes para su investigación forense.



Ver miniatura de imágenes





Al ver la miniatura se pueden ver los metadatos del archivo y los detalles de la imagen.

The screenshot shows the Autopsy 4.21.0 interface. On the left, the 'Data Sources' pane shows a tree view of the file system. The 'File Views' pane shows a list of file types, including 'Images (2)'. The main pane displays a table of results for the selected file type. The table has columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), Flags(Meta), and Known. Two rows are shown, both for 'Entrega Devo.jpg'. The first row has a blue background and the second row has a green background. Below the table, the 'Metadata' pane shows detailed information for the selected file.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
Entrega Devo.jpg			1	2021-07-20 21:09:44 CDT	0000-00-00 00:00:00	2023-10-30 00:00:00 CST	2023-10-30 14:40:45 CST	48677	Allocated	Allocated	unknown
Entrega Devo.jpg			1	2021-07-20 21:09:44 CDT	0000-00-00 00:00:00	2023-10-30 00:00:00 CST	2023-10-30 14:40:45 CST	48677	Allocated	Allocated	unknown

**Metadata**

Name: /img\_Di/Cientes/AKSI/Reportes Entregas/Entrega Devo.jpg  
Type: File System  
MIME Type: image/jpeg  
Size: 48677  
File Name Allocation: Allocated  
Metadata Allocation: Allocated  
Modified: 2021-07-20 21:09:44 CDT  
Accessed: 2023-10-30 00:00:00 CST  
Created: 2023-10-30 14:40:45 CST  
Changed: 0000-00-00 00:00:00  
MD5: ec445a0b2ba7d3a80250a03707ea686  
SHA-256: a38136a242c02311d34d987c5c944254b84b3f75205105a0cd5a50f06e2205bf  
Hash Lookup Results: UNKNOWN  
Internal ID: 195

## Metadatos y detalles de Imagen

Aquí también podemos ver algunos archivos del tipo "Archives" que se han recuperado. Podemos extraer estos archivos del sistema y visualizarlos utilizando varios programas.

## Extraer

## archivos

## recuperados

The screenshot shows the Autopsy 4.21.0 interface. On the left, the 'Data Sources' pane shows a tree structure with 'D:\\_307 Host' expanded, showing 'S\OrphanFiles (0)', 'S\Unallic (7)', 'S\Cientes (5)', 'S\INFOTEC (43)', and 'System Volume Information (4)'. The 'File Views' pane shows 'File Types' with 'Archives (10)' selected. The main pane shows a table of files with columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, and Flags. The table lists several files, including '2022.08.18.firma\_electronica\_COFP790721HDFR80', '2023.08.17.firma\_electronica\_COFP790721HDFR80', 'Informatica Forensic-2023042211935042-001.zip', 'Listas de cotejo.zip', 'Informatica Forensic-20230630T2153282-001.zip', 'Insuomos drive-download-20240710T200010Z-001.zip', 'Informa\_forensic\_2022-2-Entrega U1, 1A, Mapa mer', 'Informa\_forensic\_2022-2-Entrega U1, 1B, Reporte so', and 'Informatica forensic-20230321T1914282-001.zip'. Below the table, the 'Hex Text' pane shows a hex dump of the selected file, with columns for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences.

## Documentos

Los documentos se clasifican en cinco tipos principales:

1. **HTML**
2. **Office**
3. **PDF**
4. **Texto sin formato (Plain Text)**
5. **Texto enriquecido (Rich Text)**

## Exploración de Documentos:

### 1. Ver Documentos:

- Al seleccionar la opción de documentos, podrás ver todos los documentos presentes en cada categoría.
- Por ejemplo, al hacer clic en la categoría de **PDF**, se listarán todos los archivos PDF encontrados en la imagen del disco.

## 2. Visualizar Archivos Importantes:

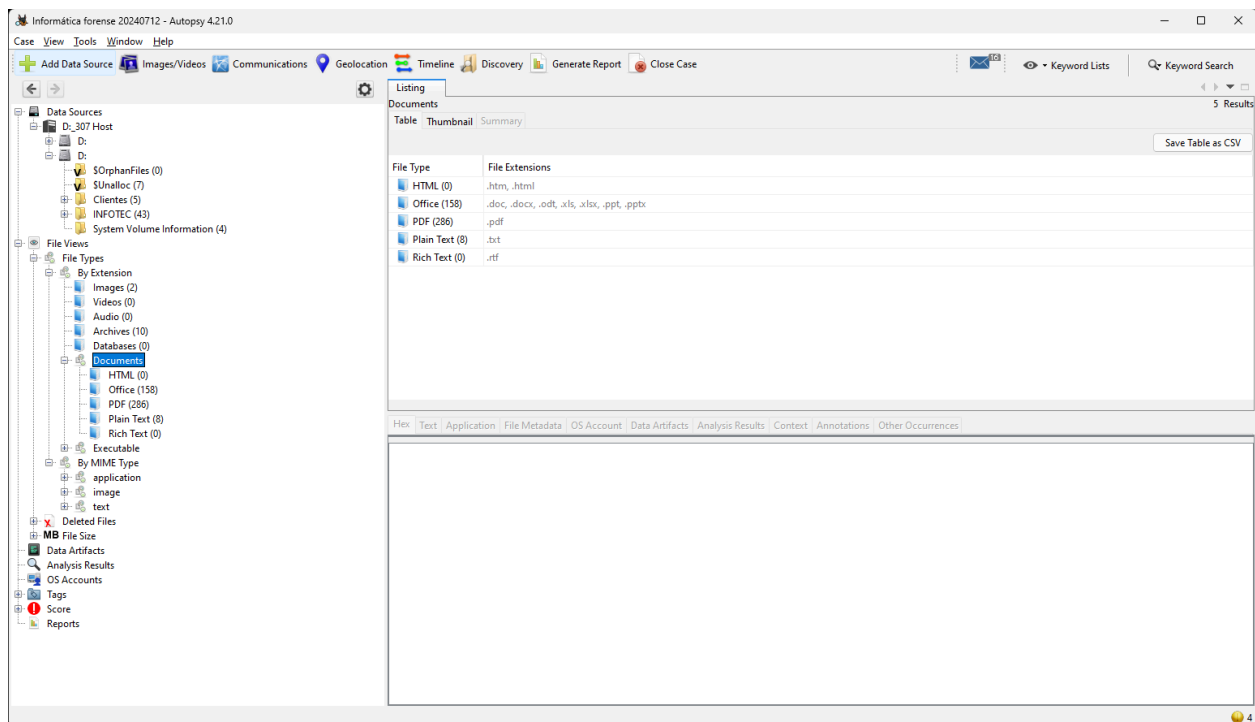
- Puedes revisar cada documento y hacer clic en los archivos importantes para abrirlos y examinarlos más detalladamente.
- Esta funcionalidad es útil para identificar y analizar documentos críticos que pueden contener información relevante para tu investigación.

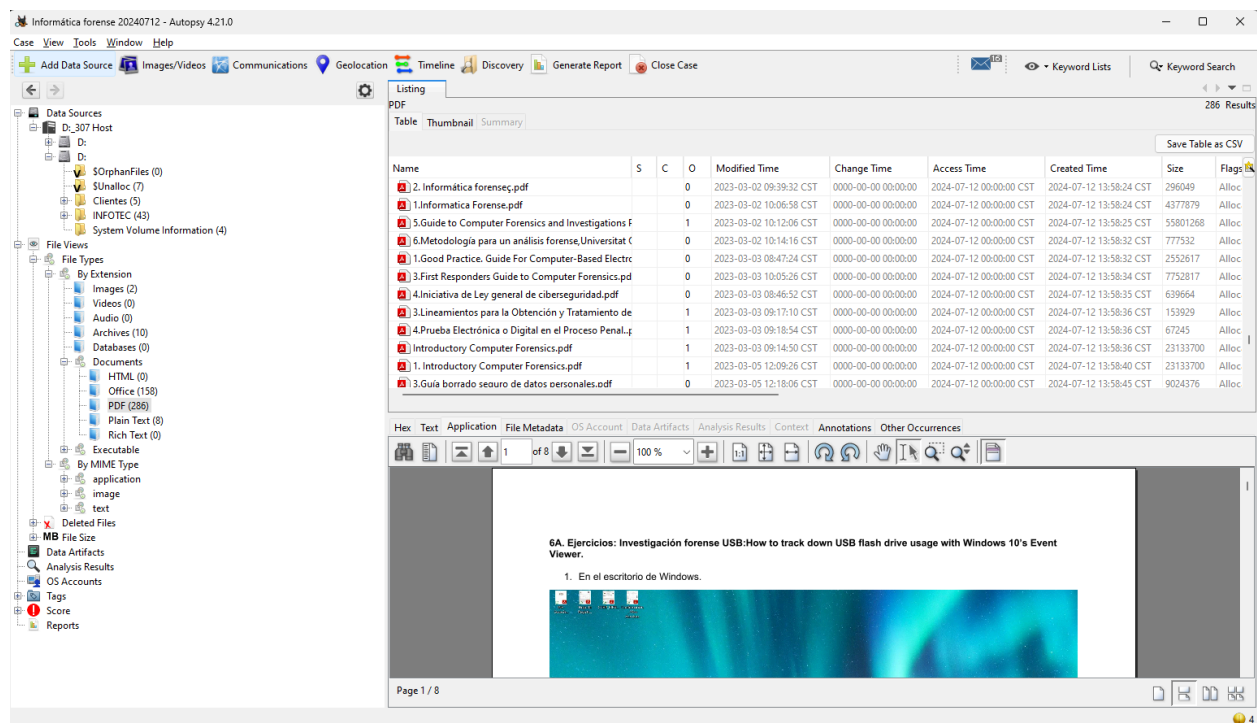
## 3. Encontrar Documentos Clave:

- Al explorar la opción de **PDF**, también puedes localizar archivos PDF específicos que sean importantes dentro de la imagen del disco.
- Esto facilita la búsqueda y revisión de documentos significativos, optimizando el proceso de análisis.

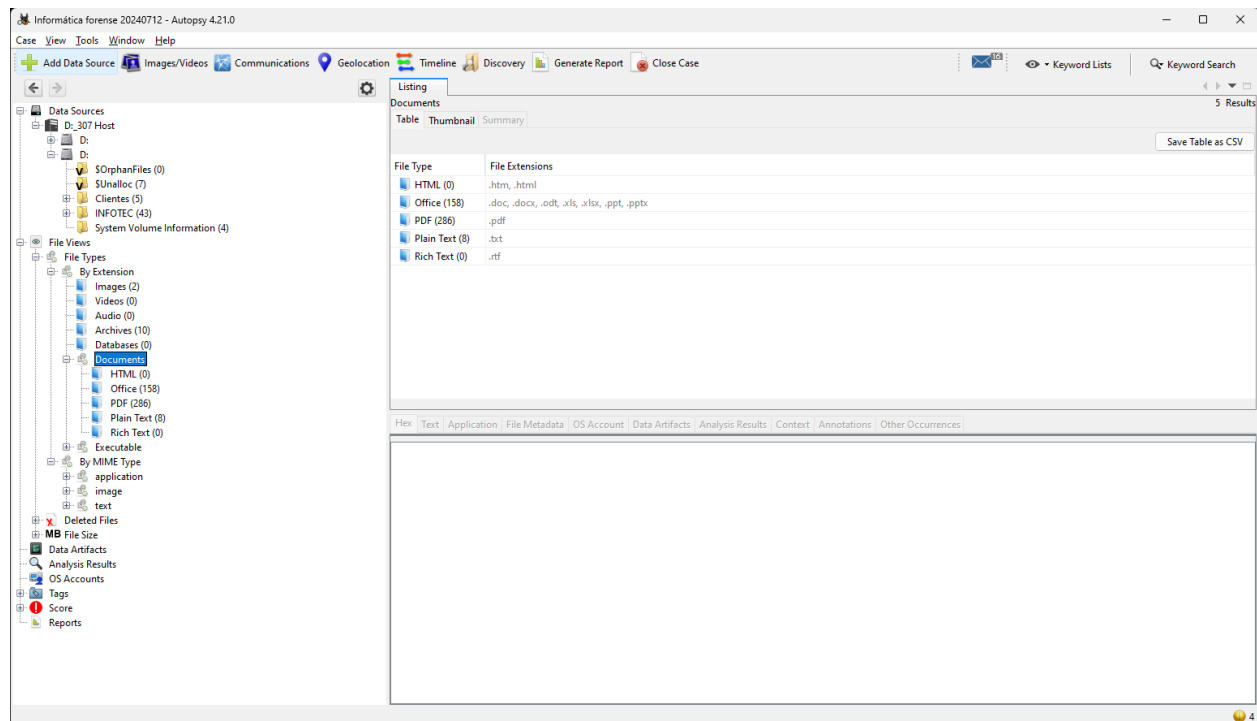
Esta clasificación y capacidad de exploración de documentos permite a los investigadores organizar y revisar eficientemente grandes cantidades de archivos textuales, ayudando a identificar rápidamente la información relevante para el caso forense.

Tipos de documentos





## Tipos de documentos 2



---

## Exploración de Archivos de Texto Plano

Del mismo modo, puedes explorar y visualizar los diversos archivos de texto plano presentes en la imagen del disco.

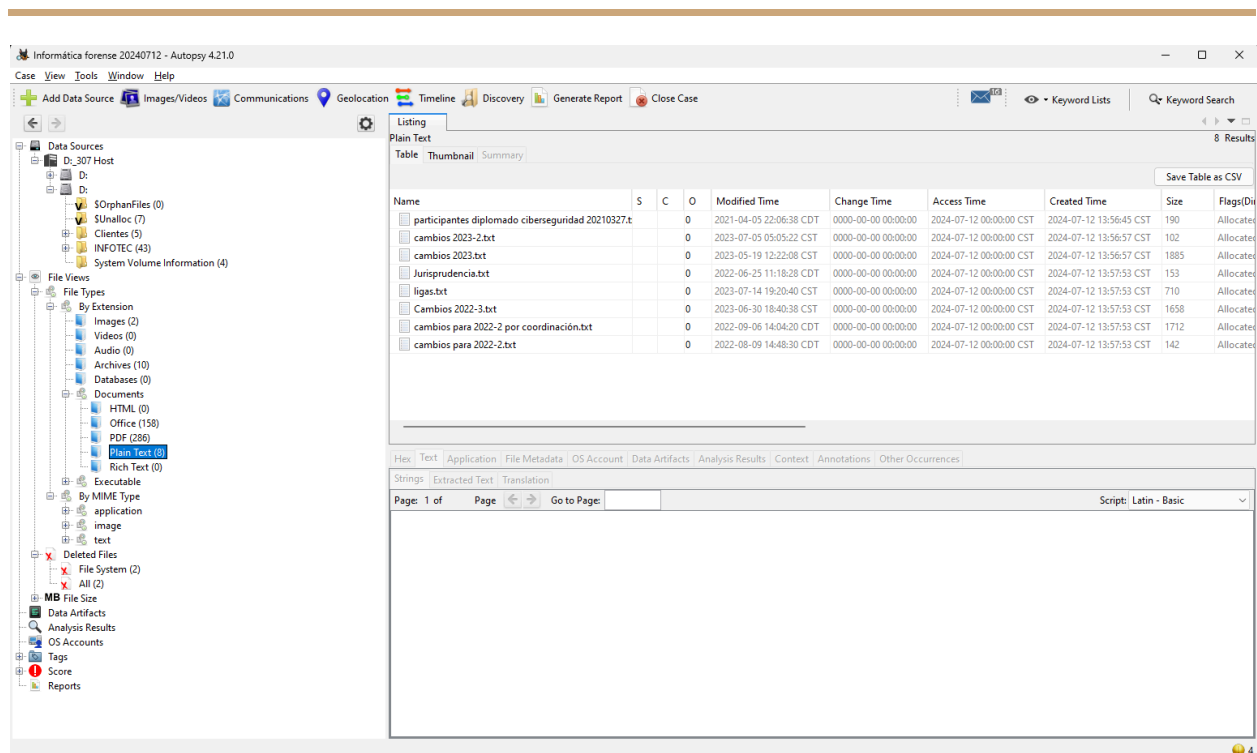
### 1. Ver Archivos de Texto Plano:

- Al seleccionar la categoría de **Texto sin formato (Plain Text)**, se mostrarán todos los archivos de texto plano disponibles.
- Puedes abrir y revisar cada uno de estos archivos para evaluar su contenido y relevancia para tu investigación.

### 2. Recuperar Archivos Eliminados:

- Además, Autopsy permite recuperar archivos de texto plano que hayan sido eliminados.
- Esta funcionalidad es especialmente útil para recuperar información que podría haber sido borrada intencionalmente o accidentalmente, proporcionando una visión más completa de los datos disponibles.

Esta capacidad de explorar y recuperar archivos de texto plano, incluidos aquellos que han sido eliminados, es fundamental para realizar un análisis exhaustivo y detallado durante el proceso de investigación forense.



Recuperar archivos en texto plano

## Archivos Eliminados

### 1. Visualización de Archivos Eliminados:

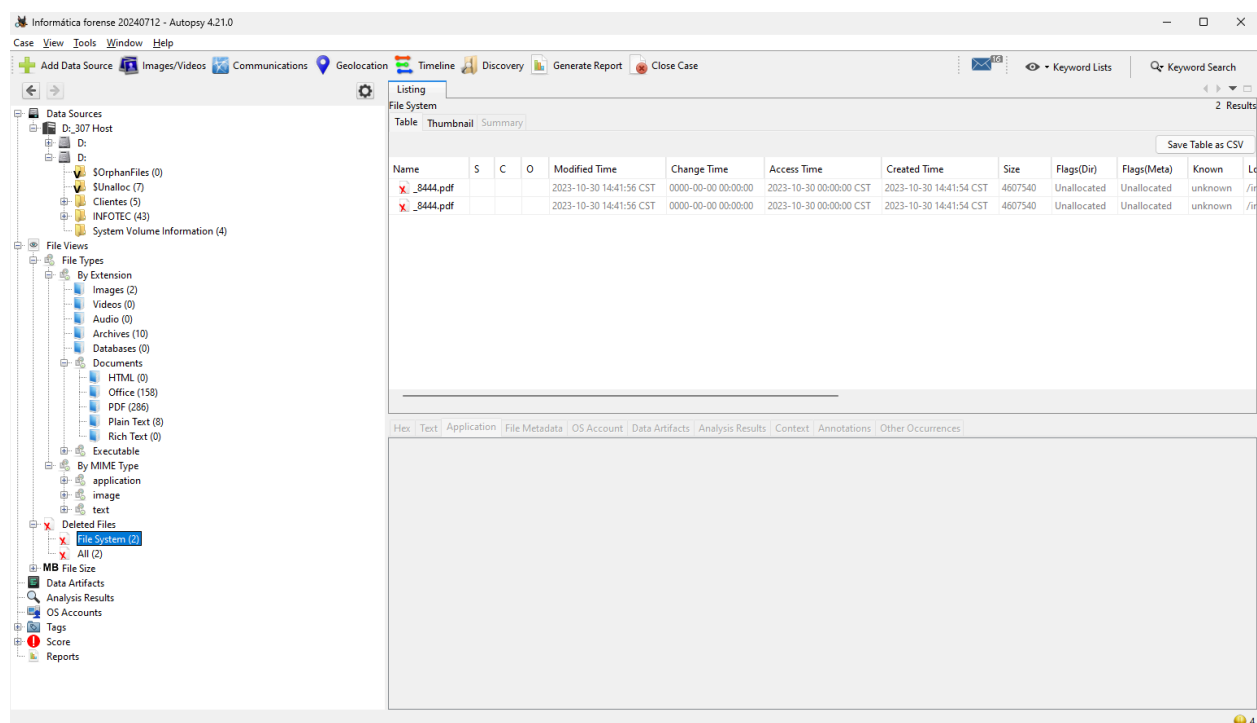
- En esta sección, se muestra información sobre los archivos que han sido eliminados del dispositivo.
- La interfaz proporciona detalles sobre cada archivo eliminado, incluyendo su nombre, ubicación original, y otros metadatos relevantes.

### 2. Recuperación de Archivos:

- Desde esta vista, puedes seleccionar los archivos eliminados que desees recuperar.
- Autopsy ofrece herramientas para restaurar estos archivos, permitiéndote analizarlos como parte de tu investigación forense.

Esta funcionalidad es esencial para recuperar y examinar información que pudo haber sido borrada, proporcionando una visión completa y detallada de todos los datos relevantes en el caso.

Es MUY IMPORTANTE que la recuperación de los archivos eliminados la realizamos en otro medio de almacenamiento que no sea el que analizamos originalmente.



Recuperar archivos eliminados

## Resultados

En esta sección, obtenemos información detallada sobre el contenido que fue extraído durante el análisis.

### Contenido Extraído (Extracted Content)

Todo el contenido que fue extraído está segregado en diferentes categorías detalladas. Algunos de los elementos comunes encontrados son metadatos, la

---

papelera de reciclaje y las descargas web. A continuación, exploramos cada uno de estos elementos:

- **Metadatos (Metadata):** Aquí puedes ver toda la información relevante sobre los archivos, como la fecha de creación, fecha de modificación, propietario del archivo, entre otros detalles importantes.
  - **Sección Metadata:** Permite una visualización exhaustiva de los metadatos de todos los archivos extraídos.
- **Descargas Web (Web Downloads):** Esta sección muestra todos los archivos que fueron descargados desde internet.
  - **Sección Web Downloads:** Facilita la identificación y análisis de archivos descargados.

### Palabras Clave (Keyword Hits)

Esta sección permite buscar cualquier palabra clave específica dentro de la imagen de disco. Las búsquedas pueden ser realizadas mediante coincidencia exacta, coincidencias de subcadena, correos electrónicos, palabras literales, expresiones regulares, entre otros métodos.

- **Búsqueda de Palabras Clave:** Puedes realizar búsquedas detalladas y obtener resultados específicos según tus criterios de búsqueda.
  - **Filtro por correo electrónico:** Facilita la búsqueda de direcciones de correo electrónico disponibles en la imagen.
  - **Exportar en formato CSV:** Permite exportar los resultados de las búsquedas a un formato CSV para un análisis más detallado.

### Línea de Tiempo (Timeline)

Mediante esta función, puedes obtener información sobre el uso del sistema en diferentes formatos: estadístico (statistical), detallado (detailed) o lista (list).

- **Formato Estadística:** Proporciona una visión general en forma de gráficos estadísticos.



- 
- **Formato Detallado:** Muestra un desglose detallado de eventos específicos.
  - **Formato Lista:** Presenta los datos en un formato de lista sencillo para facilitar la revisión.

## Descubrimiento (Discovery)

Esta opción permite encontrar medios utilizando diferentes filtros que están presentes en la imagen de disco.

- **Filtros de Medios:** Aplicando diversos filtros puedes descubrir medios específicos como imágenes y vídeos.
  - **Resultado de Filtros:** Obtén resultados precisos según las opciones de filtro seleccionadas.

## Imágenes/Vídeos

Permite encontrar y categorizar imágenes y vídeos mediante varias opciones y múltiples categorías.

- **Resultado de Imágenes y Vídeos:** Proporciona una vista organizada y detallada de los archivos multimedia recuperados.

## Añadir Etiqueta de Archivo

El etiquetado se utiliza para crear marcadores, hacer seguimiento y marcar elementos notables.

- **Etiquetado de Archivos:** Facilita la organización y clasificación de archivos importantes mediante el uso de etiquetas.
  - **Filtros por Etiquetas:** Visualiza los archivos etiquetados de acuerdo con varias categorías predefinidas.

## Generar Informe

Una vez finalizada la investigación, puedes generar un informe en varios formatos según tu preferencia.

- **Generación de Informe:** Selecciona la fuente de datos para la cual deseas generar el informe.
  - **Informe en Formato HTML:** Elige crear el informe en formato HTML para una presentación web detallada.

## Ejemplo de Generación de Informe:

- **Informe Generado en HTML:** Visualiza y revisa el informe completo de tu investigación forense.

Report Navigation

- Case Summary
- ★ Data Source Usage (2)
- ★ Tagged Files (0)
- ★ Tagged Images (0)
- ★ Tagged Results (0)

prueba de reporte

### Autopsy Forensic Report

HTML Report Generated on 2024/07/12 14:54:31

Case: Informática forense  
20240712

Case Number: 20240712-1

Number of data sources in case: 2

Examiner: Pablo Corona

#### Image Information:

D: [Redacted]

Timezone: America/Mexico\_City

Path: \\.\D:

D: [Redacted]

Timezone: America/Mexico\_City

Path: \\.\D:

#### Software Information:

Autopsy Version:	4.21.0
Central Repository Module:	4.21.0
Data Source Integrity Module:	4.21.0
File Type Identification Module:	4.21.0
Hash Lookup Module:	4.21.0
Interacting File Identifier Module:	4.21.0