Manual Técnico: Análisis Forense con Autopsy - Disco Local (C:)

---

1. Introducción a Autopsy

Autopsy es una herramienta gratuita y de código abierto utilizada para realizar análisis forenses en imágenes de disco o dispositivos locales que contienen evidencia digital. Permite a los investigadores profundizar en los datos, identificar y recuperar archivos eliminados, analizar la actividad reciente en un sistema, entre otras funciones. Su facilidad de uso y la capacidad de generar informes hacen que sea una herramienta utilizada por agencias de seguridad, fuerzas del orden y empresas privadas.

En este manual técnico, utilizaremos Autopsy para analizar el Disco Local (C:) de un sistema Windows. El objetivo es extraer evidencia relevante, como archivos eliminados, registros de actividad reciente y otros artefactos forenses.

---

2. Instalación y Configuración

Paso 1: Descarga e instalación de Autopsy

1. Ve al sitio oficial de Autopsy: https://www.autopsy.com.
2. Descarga la versión adecuada para tu sistema operativo e instálala siguiendo las instrucciones del asistente de instalación.

Paso 2: Crear un nuevo caso

1. Al abrir Autopsy, selecciona Nuevo Caso en la pantalla principal.
2. Introduce el nombre del caso (ej. "Análisis Disco Local C:") y selecciona una carpeta donde deseas guardar el caso.
3. Completa la información adicional, como número de caso y notas relevantes sobre el análisis (ej. "Análisis de un disco local para recuperación de archivos eliminados y actividad reciente").

Paso 3: Seleccionar el host y la fuente de datos

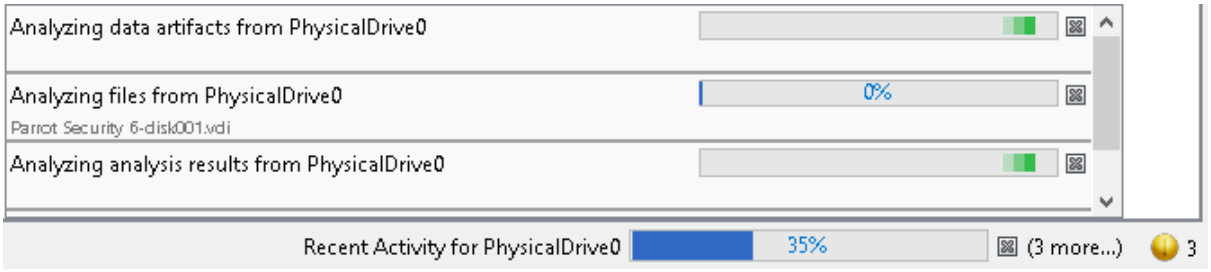
1. En la siguiente pantalla, selecciona el host del sistema que se va a analizar. Si no aparece un host, créalo nombrando el equipo o sistema que estás investigando.
2. Añade la fuente de datos: selecciona Local Disk para analizar directamente el Disco Local (C:) del sistema.

---

3. Proceso de Análisis

Paso 1: Comenzar el análisis del Disco Local (C:)

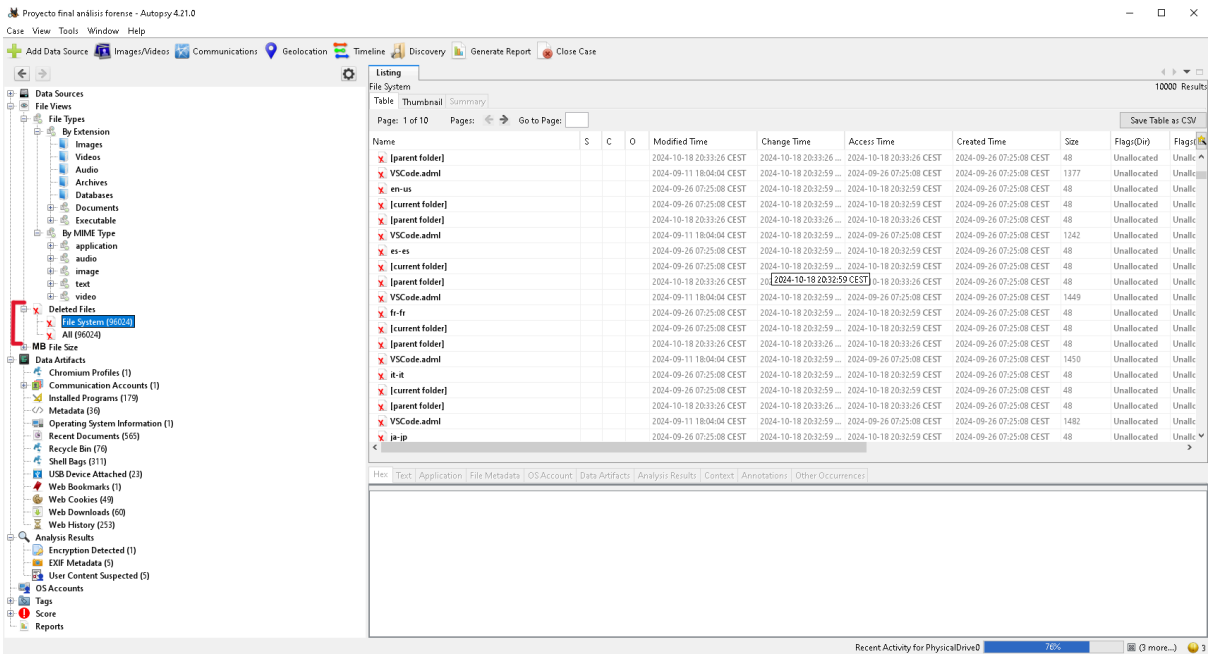
1. Una vez seleccionada la fuente de datos, Autopsy comenzará a analizar el Disco Local (C:).
2. Este proceso puede tardar varios minutos o incluso horas dependiendo del tamaño del disco y la cantidad de datos presentes.



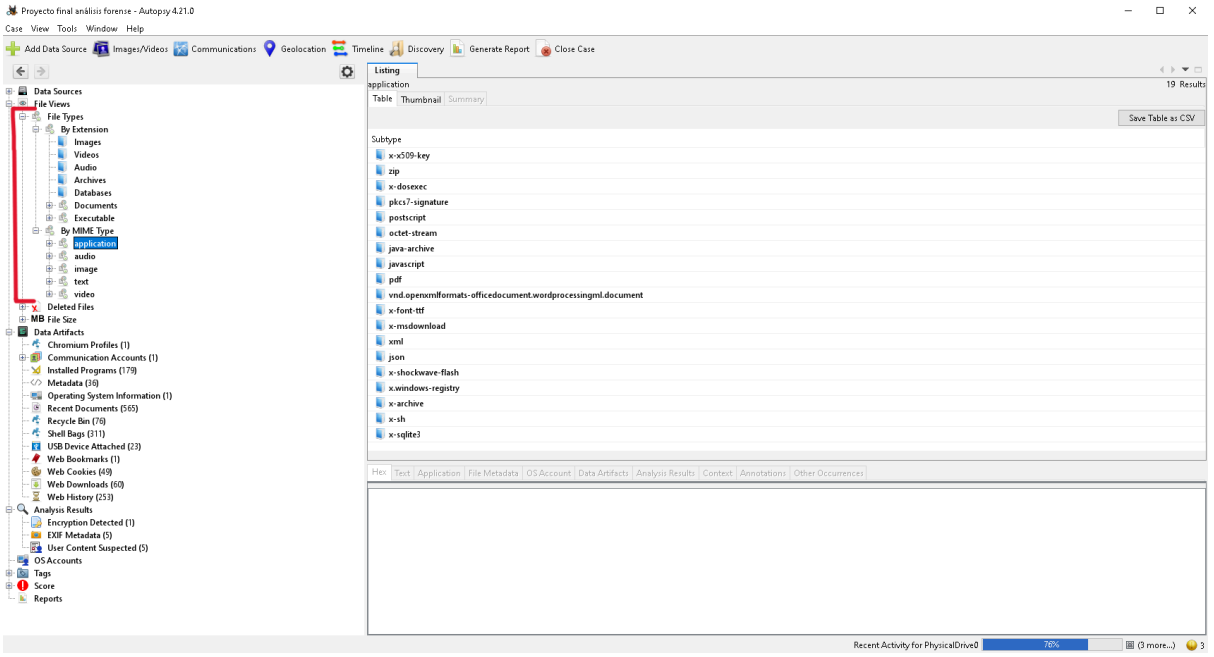
Paso 2: Explorar los artefactos encontrados

Una vez finalizado el análisis, puedes explorar las diferentes secciones que Autopsy ha generado automáticamente.

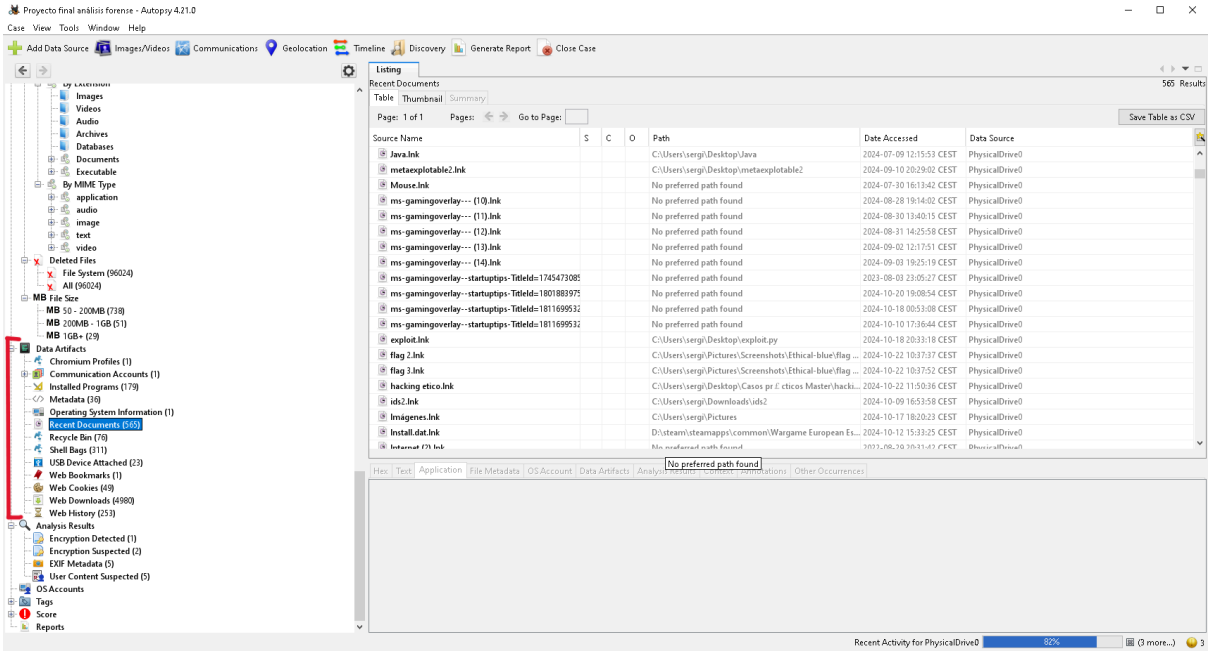
- **Deleted Files**: En esta sección puedes visualizar los archivos que han sido eliminados pero que Autopsy ha podido recuperar



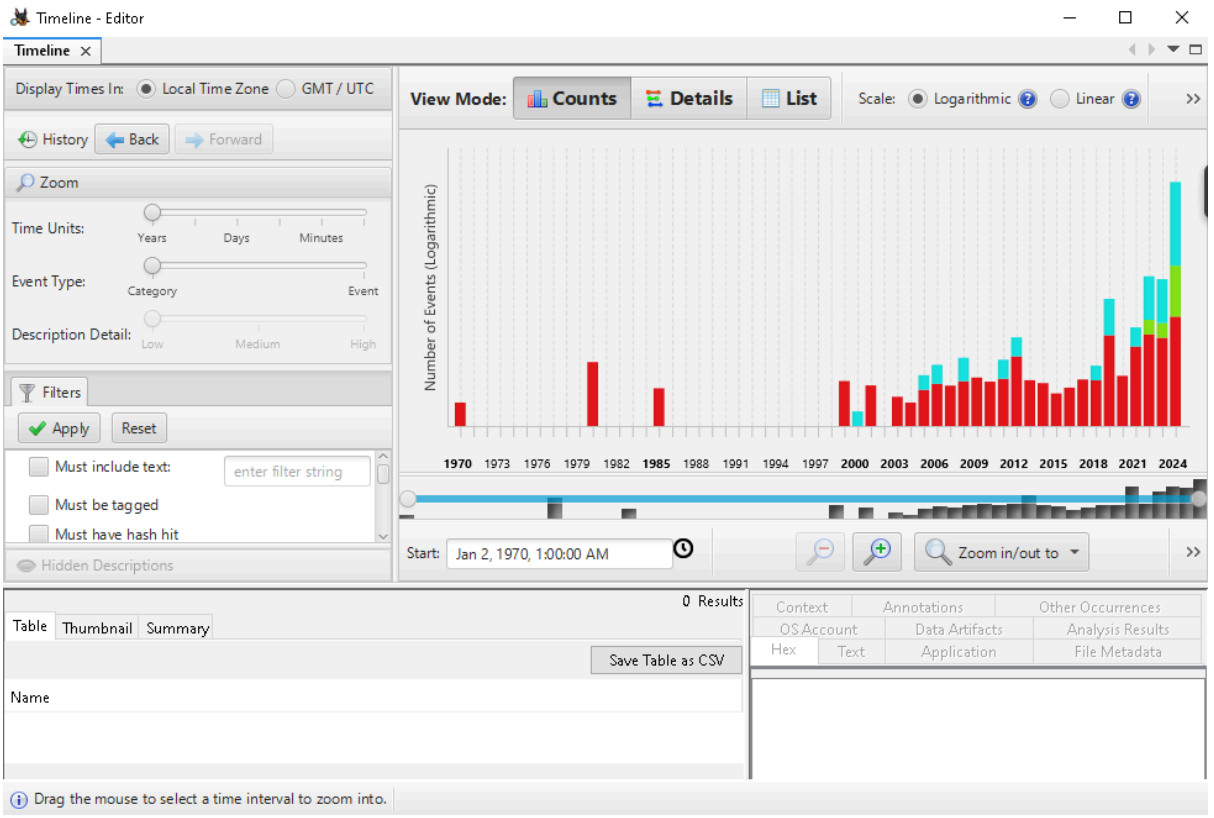
- **Tipos de archivos(por tamaño o MIME):** En este apartado podremos investigar todos los archivos del Ordenador, ya sean imágenes, videos, audios, etc.



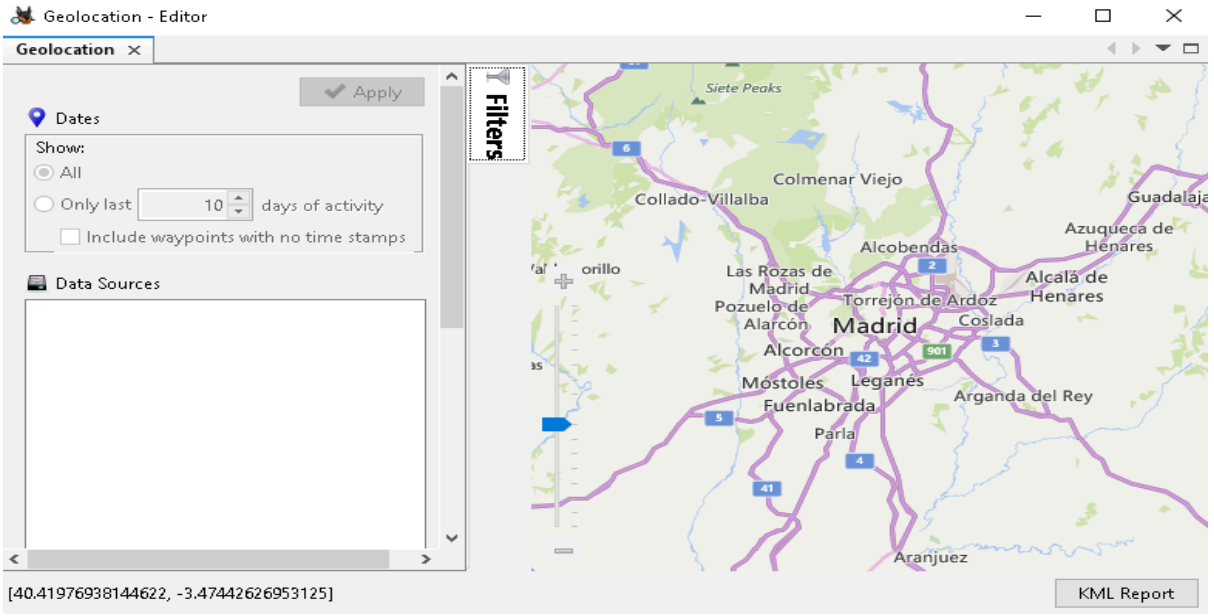
- **Data artifacts:** En esta sección se pueden encontrar diversos tipos de información clasificada de manera automática para facilitar su revisión. Entre los datos presentes se incluyen el historial de navegación web, los archivos eliminados, que Autopsy ha podido recuperar. También se listan los documentos recientes abiertos por el usuario, las cuentas de usuario del sistema, y los archivos temporales generados por el sistema operativo o las aplicaciones. Por último, es posible acceder a los metadatos de los archivos, que ofrecen información relevante sobre fechas de creación, modificación y acceso, entre otros detalles.



- **Timeline:** Esta sección se encuentra en la barra superior derecha, y al hacer click sobre ella nos mostrará un análisis del tiempo de uso del dispositivo analizado.



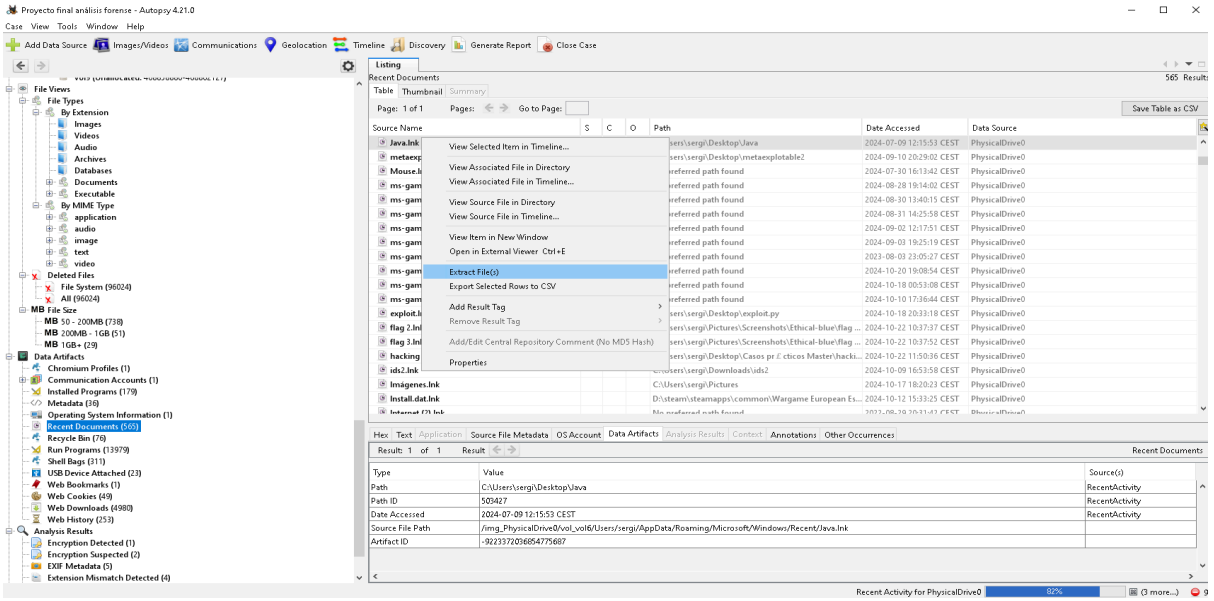
- **Geolocation:** Aquí se nos muestran los lugares en los que se ha localizado el dispositivo y se podrá elegir en desde qué fecha se muestra la geolocalización, información que podría ser de gran relevancia para la investigación.*

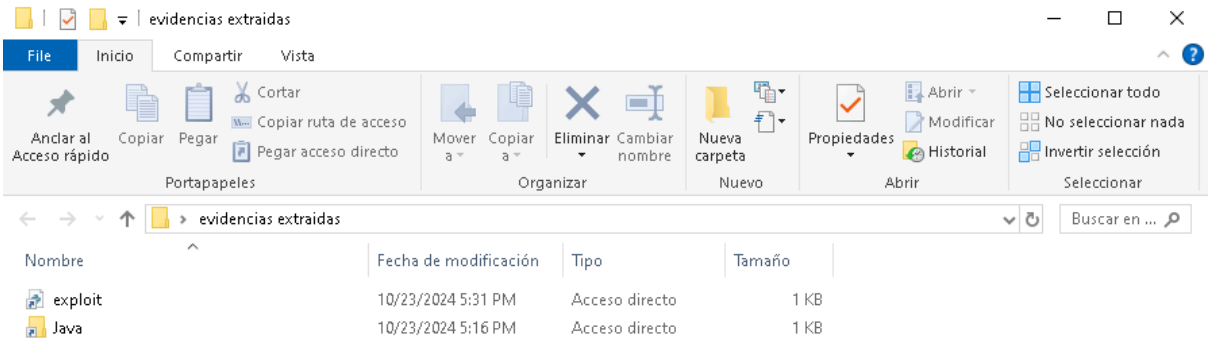


*En este caso no hay artefactos que permitan la geolocalización ya que en este PC tengo esas funciones bloqueadas tanto en el PC como en los navegadores.

Paso 3: Selección y extracción de evidencias

1. Si encuentras algún archivo o artefacto que consideres importante, puedes hacer clic derecho sobre él y seleccionar Extract File(s) para guardarlo en tu sistema.





2. Toma capturas de pantalla de los hallazgos más importantes para documentar el proceso.

---

4. Interpretación de los Resultados

Una vez revisadas las diferentes categorías de datos, Autopsy te permitirá ver detalles específicos sobre los archivos y eventos identificados.

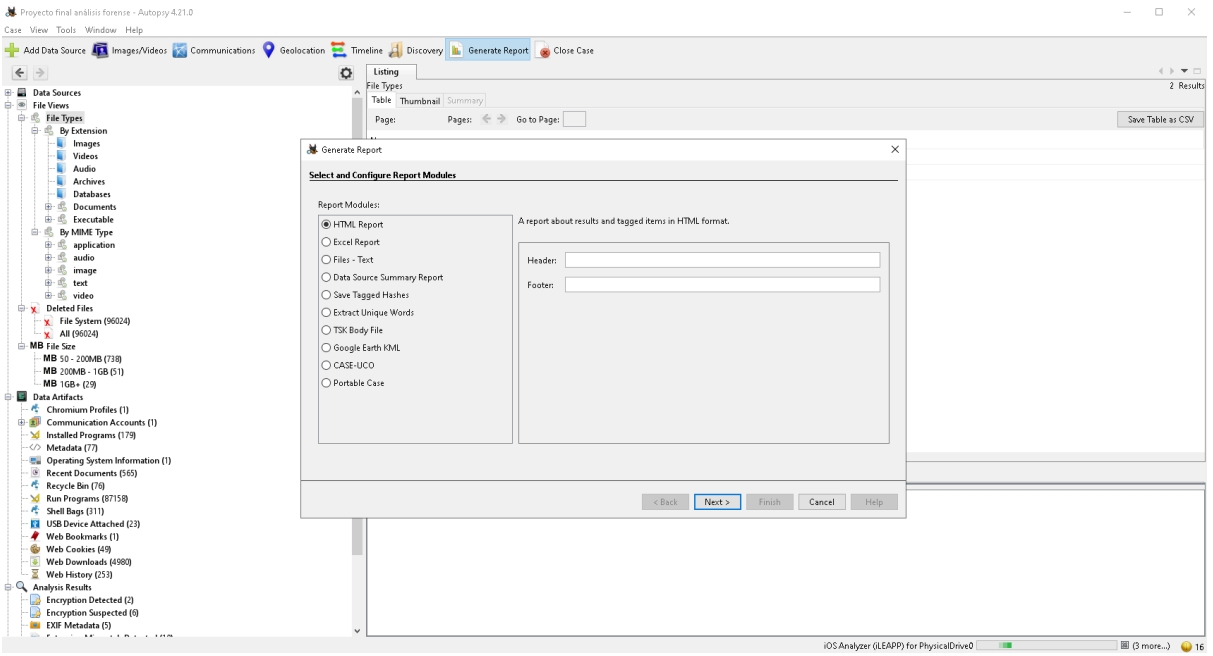
Por ejemplo, a través de las diversas capturas de pantalla que se han adjuntado y a los archivos extraídos,se podría deducir que el usuario del disco C:, utilizó el dispositivo con muchísima frecuencia en 2024 y tiene conocimientos en programación y bases de datos, ya que si observamos la pestaña application, que se muestra en la tercera captura de pantalla podemos comprobar que hay programas como JavaScript y SQLlite y se extrajo un archivo con contenido de java que se encontraba en la pestaña Recent Documents, tambien se extrajo un documento llamado exploit, lo que podría denotar que este tiene alguna relación con la ciberseguridad. Todas estas pruebas podrían ser importantes en una hipotética investigación y cambiar el devenir de esta.

---

5. Generación de Informe

Paso 1: Generar el informe

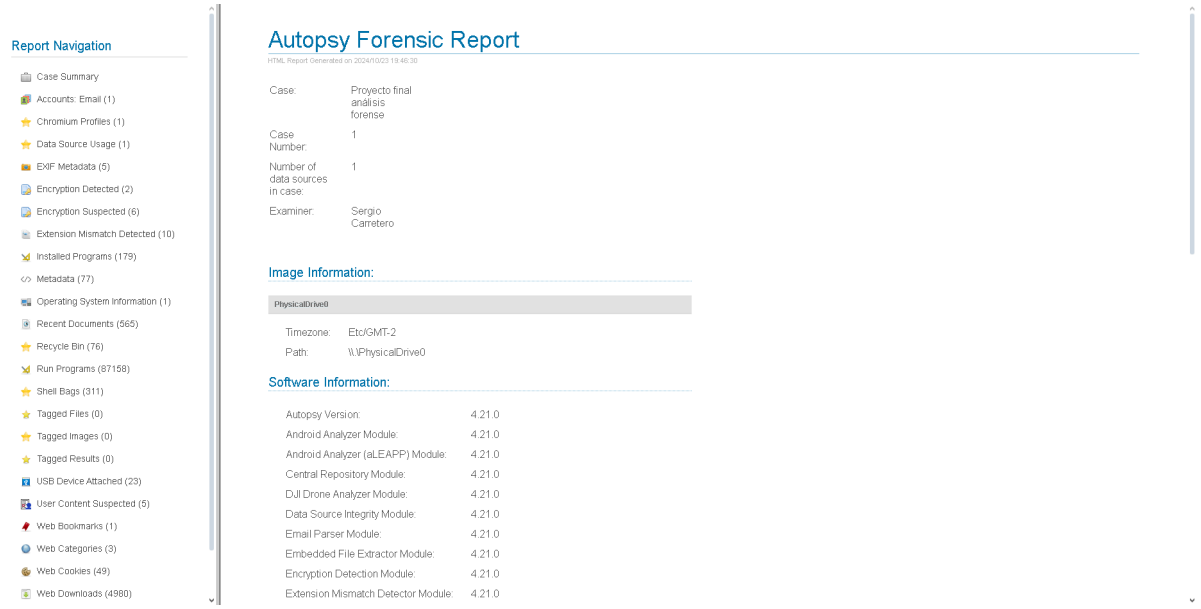
1. Una vez que hayas identificado las evidencias importantes, ve a la opción Generate Report" en la barra superior de Autopsy.



2. Elige el formato en que deseas exportar el informe. Recomiendo utilizar el formato HTML, ya que es fácil de visualizar y compartir.
3. Añade un encabezado o pie de página al informe si es necesario y haz clic en Finish para completar la exportación.

Paso 2: Revisión del informe

1. Revisa el informe generado para asegurarte de que toda la información relevante ha sido incluida, como los archivos eliminados, logs de eventos y cualquier otro artefacto forense relevante.
2. Adjunta las capturas de pantalla y cualquier otro detalle que hayas documentado durante el análisis.



file:///D:/Proyecto%20final%20análisis%20forense/Proyecto%20final%20análisis%20forense/Reports/Proyecto%20final%20análisis%20forense%20HTML%20Report%2010-23-2024-19-46-30/report.html

---

Bibliografía

Autopsy User Documentation: Autopsy User's Guide. (s/f). Sleuthkit.org. https://sleuthkit.org/autopsy/docs/user-docs/4.21.0//

Thatipalli, S. A. (2023, mayo 19). *Why using the Autopsy tool is best for Digital Forensics*. Packt SecPro. https://security.packt.com/why-using-the-autopsy-tool-is-best-for-digital-forensics/

(S/f). Todo-servidores.com. https://todo-servidores.com/que-es-autopsy-y-como-funciona/