Informática Forense, una introducción con Autopsy

Autor:
Pablo Díaz,

Contents

1 Introducción

En el ámbito de la informática forense, el análisis de dispositivos digitales es una tarea fundamental para la recolección de evidencia en investigaciones criminales y auditorías de seguridad. En esta práctica, se empleará **Autopsy**, una herramienta de código abierto basada en la suite *Sleuth Kit*, diseñada para la recuperación y análisis de datos almacenados en discos duros, dispositivos móviles y otros medios de almacenamiento digital.

El objetivo principal de esta práctica es familiarizarse con los procedimientos básicos del análisis forense digital, explorando técnicas de recuperación de archivos eliminados, análisis de registros del sistema, extracción de metadatos y detección de actividad sospechosa. Para ello, se trabajará con una imagen de dispositivo extraída de un caso de estudio realista, lo que permitirá aplicar métodos de investigación forense para la identificación y correlación de evidencia digital.

Se llevará a cabo la creación de un caso en **Autopsy**, la configuración de los módulos de análisis y la interpretación de los resultados obtenidos. Adicionalmente, se evaluarán herramientas de filtrado de archivos y bases de datos de hashes para la identificación de elementos relevantes dentro de la investigación.

A lo largo de la práctica, se responderán una serie de preguntas clave sobre la evidencia analizada, como la identificación de archivos relevantes, la recuperación de información oculta y la vinculación de un sospechoso con actividades ilícitas. De esta manera, se obtendrá una visión práctica de los principios fundamentales de la informática forense y su aplicación en escenarios reales.

2 Realización de la Práctica

2.1 Recuperación de Imágenes de Rinocerontes

Para recuperar imágenes relacionadas con rinocerontes, se utilizó la herramienta **Autopsy**. Se inició la búsqueda explorando imágenes en formato JPG mediante la barra de búsqueda.

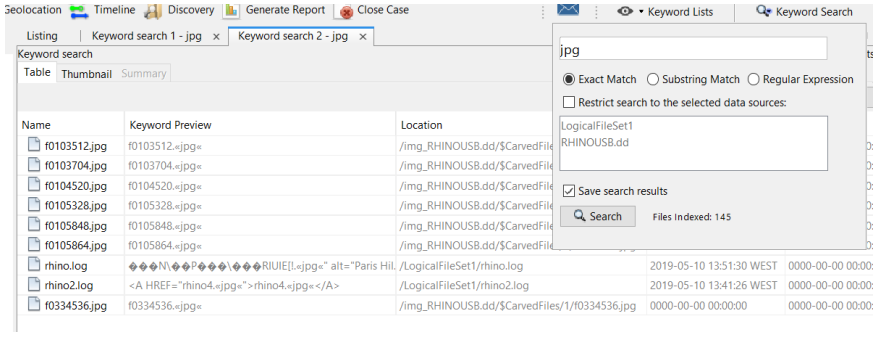

Figure I: Búsqueda de imágenes en formato JPG en Autopsy.

Durante esta búsqueda, se encontraron varias imágenes, algunas de ellas de rinocerontes, pero también se identificaron imágenes de cocodrilos. Además, se exploró la sección de **ficheros sospechosos**, donde se localizaron archivos en formato `.gif` que contenían imágenes relevantes.

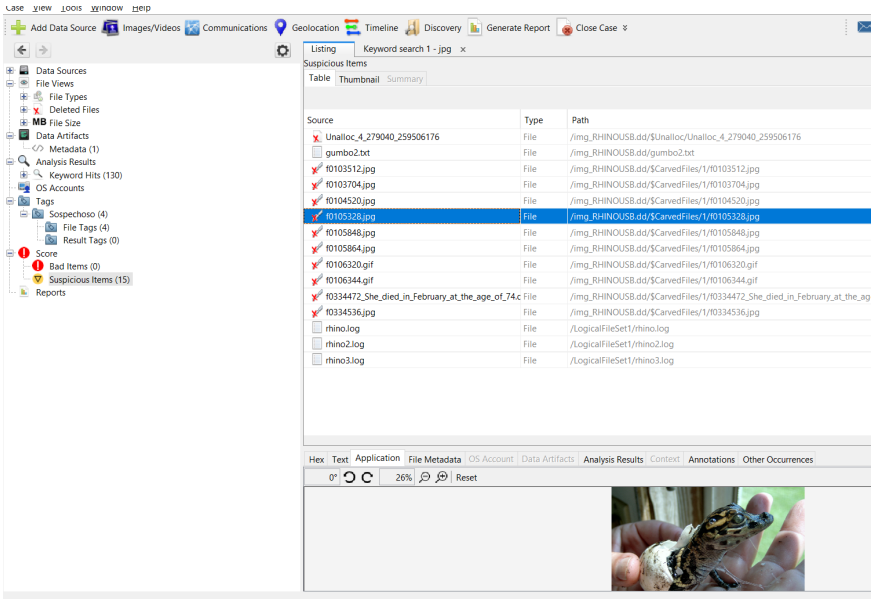

Figure II: Exploración de la sección de archivos sospechosos en Autopsy.

Gracias a esta búsqueda, se lograron identificar **cuatro imágenes de rinocerontes** con los nombres:

- `f0105848.jpg`
- `f0105864.jpg`
- `f0106320.gif`
- `f0106344.gif`

Adicionalmente, se identificaron imágenes de cocodrilos marcadas como sospechosas, lo cual podría indicar el uso de técnicas de **esteganografía**.

2.2 Análisis de Paquetes de Red con Wireshark

Para continuar con la búsqueda de más imágenes, se utilizaron los **paquetes de red** disponibles en el sistema. Se identificaron **tres logs** de tráfico de red para su análisis en **Wireshark**.

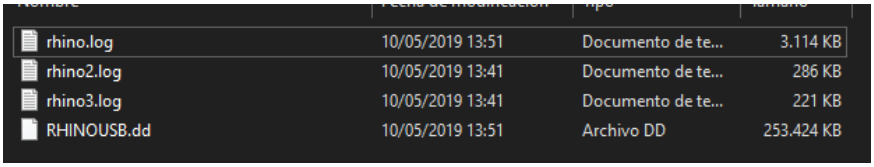

Figure III: Paquetes de red disponibles para análisis en Wireshark.

Mediante el análisis del tráfico FTP, se logró extraer credenciales de acceso (usuario y contraseña) utilizadas en la transferencia de archivos.

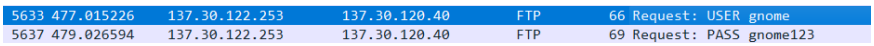

Figure IV: Extracción de credenciales FTP desde los paquetes de red.

Gracias a este análisis, se localizaron **dos imágenes adicionales** de rinocerontes, denominadas:

- `rhino1.jpg`
- `rhino3.jpg`

Para extraer estas imágenes desde los paquetes de red, se siguieron los siguientes pasos:

1. Identificar los paquetes de transferencia asociados a las imágenes.
2. Seleccionar la opción **Seguir flujo TCP (Follow TCP Stream)**.
3. Cambiar el formato a **RAW**.
4. Guardar el contenido como un archivo `.jpg`.

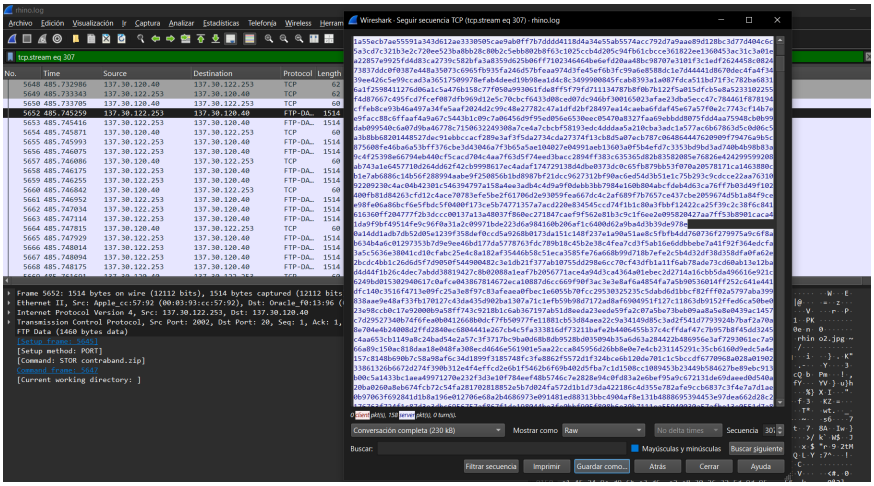

Figure V: Extracción de imágenes mediante análisis de tráfico en Wireshark.

Hemos también recuperado un archivo .zip llamado contraband.zip. Estaba protegido mediante contraseña. Probamos con la contraseña encontrada anteriormente (gnome123) pero no funcionó.Decidimos llevar a cabo un ataque de fuerza bruta, utilizamos por tanto, la herramienta John The Ripper. John no trabaja directamente con archivos zip sino con hashes por lo que lo pasamos a hash:

Figure VI: Hasheamos zip para poder usar John the Ripper.

Procedemos a hacer fuerza bruta:

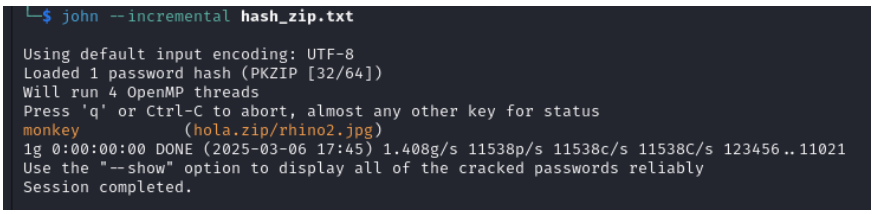

Figure VII: Usamos John the Ripper para encontrar contraseña archivo zip.

Obtenemos que la contraseña de nuestro archivo es monkey, podemos por tanto obtener la imagen que estaba comprimida (rhino2.jpg) y resulta que es la misma que ya habiamos obtenido pero con otro nombre (f0105864.jpg)

2.3 Resumen de Imágenes Recuperadas

En total, se lograron recuperar **seis imágenes de rinocerontes** mediante dos técnicas principales:

- **Análisis de archivos en Autopsy:** Se encontraron cuatro imágenes en la sección de archivos sospechosos.
- **Análisis de tráfico de red con Wireshark:** Se extrajeron dos imágenes adicionales desde paquetes FTP.

Este proceso permitió realizar una recuperación forense efectiva, identificando imágenes clave a partir de diferentes fuentes de evidencia digital.

(a) Imagen 1

(b) Imagen 2

Figure VIII: Dos imágenes juntas con subcaptions

(a) Imagen 1

(b) Imagen 2

Figure IX: Dos imágenes juntas con subcaptions

3 Preguntas a responder

3.1 ¿Quién generó la cuenta FTP asociada al acusado?

Leyendo uno de los archivos de texto marcados como sospechosos encontramos bastante información relevante que nos sirve para responder varias de las preguntas.

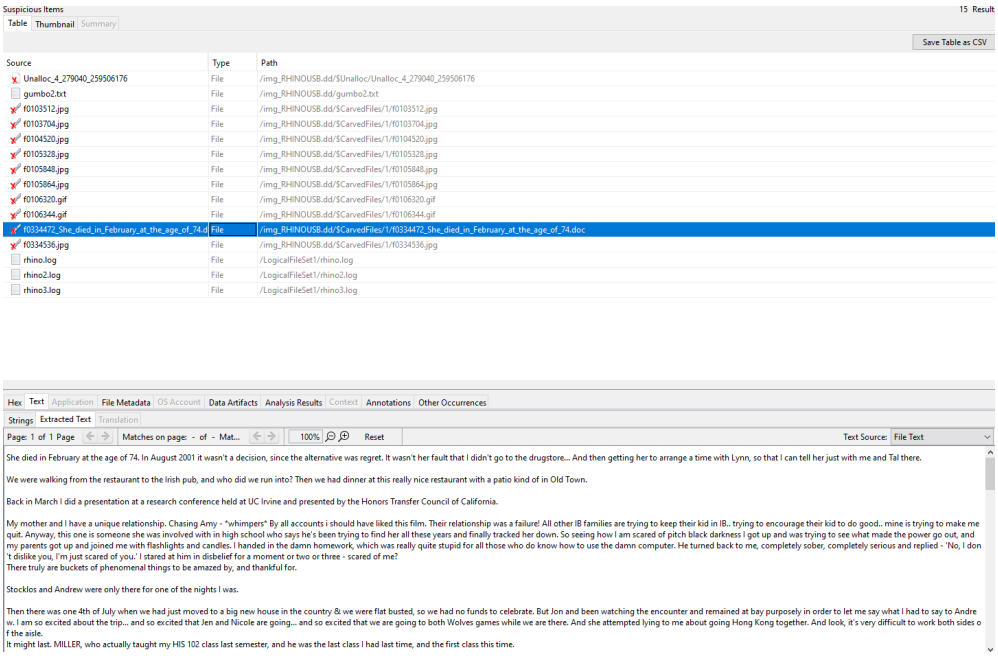

Figure X: Buscamos pistas en archivo de texto sospechoso.

Encontramos un páragrafo que nos revela que Jeremy le dio la cuenta FTP:

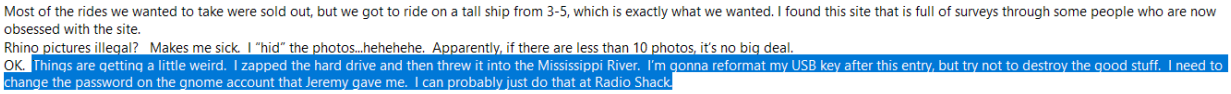

Figure XI: Encontramos que Jeremy creó la cuenta FTP

3.2 Nombre de usuario y contraseña de la cuenta FTP

Como explicamos antes, para obtener las credenciales de acceso a la cuenta FTP, se analizó el tráfico de red en Wireshark, identificando una sesión FTP en la que se enviaban el nombre de usuario y la contraseña en texto plano. A continuación, se muestra de nuevo la captura de los paquetes correspondientes:

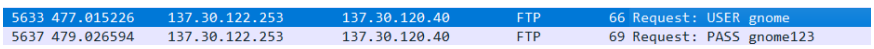

Figure XII: Extracción del usuario y contraseña FTP mediante análisis de tráfico.

En la captura de red, se observa lo siguiente:

- **Usuario:** `gnome`
- **Contraseña:** `gnome123`

3.3 ¿Qué transferencias de archivos relevantes aparecen en las trazas de red?

¿Qué le ha pasado al disco duro del ordenador? ¿Dónde está? De nuevo, en el archivo de texto sospechoso encontramos que el usuario ha lanzado el disco duro del ordenador al río

Mississippi:

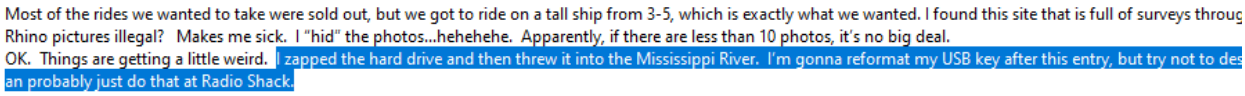

Figure XIII: El disco duro del ordenador está en el río Mississippi.

3.4 ¿Qué le ha pasado al dispositivo USB?

En el mismo texto encontramos que el sospechoso ha formateado el USB:

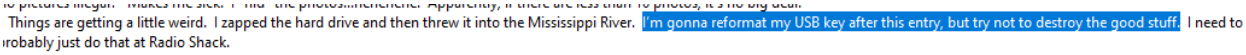

Figure XIV: Ha formateado el USB.

3.5 ¿Qué es recuperable de la imagen dd del dispositivo USB?

Tenemos la información del dispositivo USB:

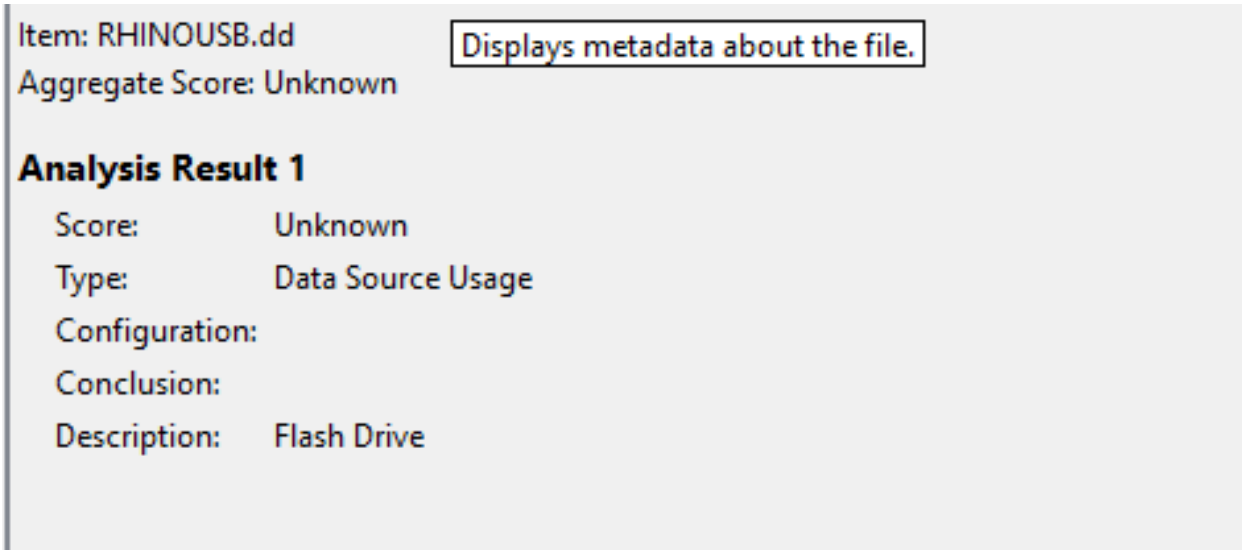

Figure XV: Imagen dd del dispositivo USB.

La información recuperable del mismo es la siguiente:

Unalloc_4_279040_259506176	File	/img_RHINOUSB.dd/$Unalloc/Unalloc_4_279040_259506176
gumbo2.txt	File	/img_RHINOUSB.dd/gumbo2.txt
f0103512.jpg	File	/img_RHINOUSB.dd/$CarvedFiles/1/f0103512.jpg
f0103704.jpg	File	/img_RHINOUSB.dd/$CarvedFiles/1/f0103704.jpg
f0104520.jpg	File	/img_RHINOUSB.dd/$CarvedFiles/1/f0104520.jpg
f0105328.jpg	File	/img_RHINOUSB.dd/$CarvedFiles/1/f0105328.jpg
f0105848.jpg	File	/img_RHINOUSB.dd/$CarvedFiles/1/f0105848.jpg
f0105864.jpg	File	/img_RHINOUSB.dd/$CarvedFiles/1/f0105864.jpg
f0106320.gif	File	/img_RHINOUSB.dd/$CarvedFiles/1/f0106320.gif
f0106344.gif	File	/img_RHINOUSB.dd/$CarvedFiles/1/f0106344.gif
f0334472_She_died_in_February_at_the_age_of_74.d	File	/img_RHINOUSB.dd/$CarvedFiles/1/f0334472_She_died_in_February_at_the_age_of_74.doc
f0334536.jpg	File	/img_RHINOUSB.dd/$CarvedFiles/1/f0334536.jpg

Figure XVI: Información recuperable imagen dd

Tenemos diferentes imagenes que ya hemos examinado (cocodrilos y rinocerontes) así como archivos de texto como el que ya hemos comentado o el de gumbo2.txt que contiene una receta.

3.6 ¿Existen evidencias que relacionen el dispositivo USB con las trazas de red? En caso de ser así, ¿cuáles?

Hemos encontrado que la imagen de rinoceronte en el USB: f0105864.jpg es la misma encontrada en la traza rhino.log pero con nombre rhino2.jpg. Por lo tanto, podemos concluir que existe una relación directa entre el dispositivo USB y las trazas de red.

3.7 ¿A qué se refiere el acrónimo RDS?

El término RDS hace referencia a Reference Data Set, una colección de firmas digitales de software recopiladas y mantenidas por el National Software Reference Library (NSRL) del NIST. Este conjunto de datos incluye aplicaciones comerciales, sistemas operativos y herramientas que pueden ser utilizadas con fines legítimos o maliciosos, como scripts de hacking y programas de esteganografía.

3.8 ¿Para qué se utiliza?

Su principal utilidad es facilitar las investigaciones forenses, permitiendo a las agencias de seguridad y analistas reducir el volumen de datos a examinar. Al comparar los valores hash de los archivos de un sistema con los almacenados en el RDS, es posible determinar si un archivo pertenece a software conocido, lo que agiliza el análisis y ayuda a focalizarse en archivos sospechosos o no identificados.

3.9 Intégralo en el análisis con Autopsy realizado en clase. Para ello sigue los siguientes pasos. En Autopsy selecciona Tools-¿ Options-¿Hash Sets e importa el fichero NSLRFile.txt asociándole la ruta donde has descomprimido el fichero. El tipo de base de datos que debes especificar es Known. Indexa la base de datos para poder disponer de ella. Ten paciencia también esta vez. Revisa los resultados obtenidos ahora ¿Se han descartado ficheros del análisis?

Nos dirigimos a Tools, Options y Hash Sets:

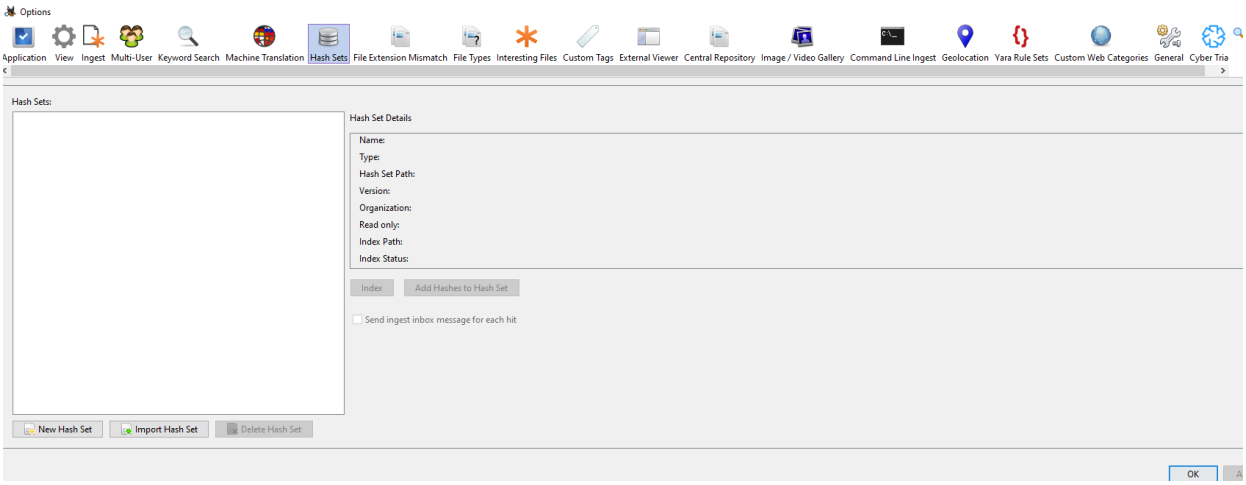

Figure XVII: Import Hash Set

3.10 En la web https://toolcatalog.nist.gov/taxonomy/ se indican las características o capacidades forenses de las herramientas disponibles, averigua cuales están presentes en Autopsy

4 Supuesto 2