Herramientas para investigación forense.

Como revisamos en el contenido anterior, las metodologías OSINT poseen una gran cantidad de herramientas que nos ayudan a abordar la ciberseguridad desde diferentes enfoques, por lo que, también puede utilizarse para mantener la integridad, confidencialidad y disponibilidad de los datos.

Existen dos herramientas que son fundamentales para análisis forenses, estas son **FTK Imager** y **Autopsy.**

FTK Imager.

FTK Imager consiste en un programa que nos ayudará a crear una imagen forense sobre un dispositivo de almacenamiento digital, sea volátil o no volátil, para mantener la integridad del dispositivo original y analizar su contenido en una copia bit a bit del almacenamiento original.

Una Imagen Forense Informática no es más que una copia realizada bit a bit desde un dispositivo de almacenamiento, que realiza tal duplicado en un medio diferente. Gracias a esta Imagen Forense Informática es posible buscar y obtener datos relevantes que han sido eliminados u ocultados.

Su principal ventaja consiste en mantener la evidencia original intacta y en analizar los resultados en una imagen fiel del contenido original.

Cabe destacar que el tamaño de la imagen forense creada es del mismo tamaño del dispositivo de almacenamiento y su tiempo de creación dependerá completamente del equipo que está creando la imagen y la cantidad de información presente en el medio de almacenamiento que se desea estudiar.

Autopsy.

Una vez que ya tenemos la imagen forense a analizar, debemos utilizar un programa que nos permita abrir esa imagen en búsqueda de conclusiones, es allí donde entra en juego el programa Autopsy.

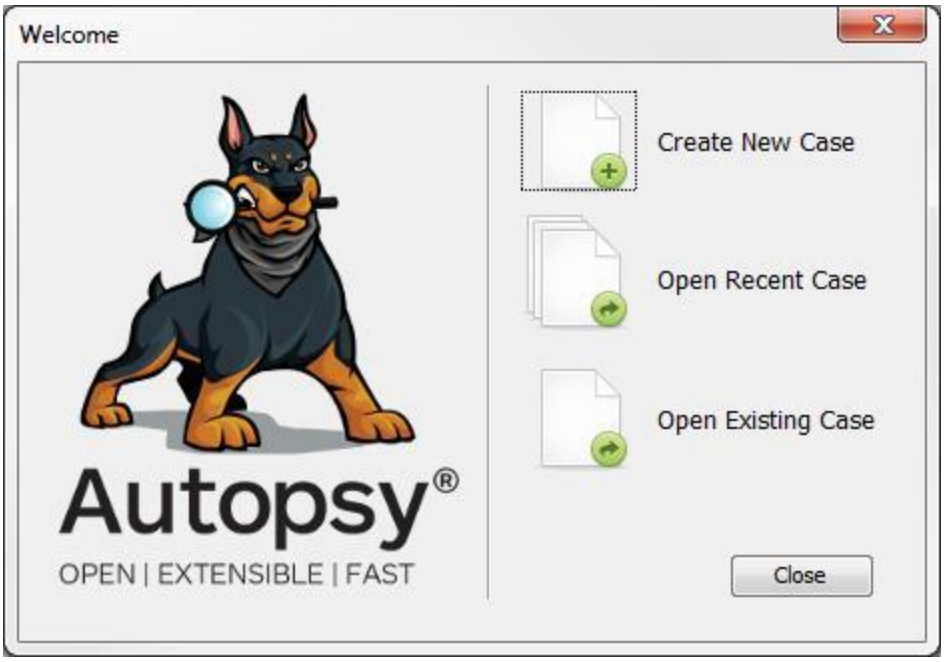

Foto de interfaz de la herramienta Autopsy.

Autopsy es una plataforma digital forense de código abierto. Analiza discos rígidos, tarjetas de memoria, celulares y otros dispositivos de almacenamiento de datos. Se destaca por su facilidad de uso, rapidez de resolución y plugins para realizar numerosas tareas específicas.

Fotos, videos, archivos de texto, email, mensajes de whatsapp y todo tipo de archivos pueden ser recuperados. incluso aunque el investigado los haya borrado en un intento de evadir a las autoridades y la justicia.

Bibliografía.

- *Imagen Forense Informática Para Los Delitos Digitales. (2023). Peritos Judiciales GPI.* *https://gabinetepericialgpi.com/blog/imagen-forense-informatica-para-delitos/*
- *Tusclases. (2020). Autopsy, una herramienta de análisis digital forense. Clases particulares.* *https://www.tusclases.com.ar/blog/autopsy-herramienta-analisis-digital-forense*