Clase 14 - Modulos autopsy

Victor Gerardo Rodríguez Barragán

21 de mayo de 2024

Módulos principales:

- Ingesta: Este módulo se utiliza para adquirir y analizar imágenes de discos, unidades extraíbles y archivos de memoria.
- Línea de tiempo: Este módulo crea una línea de tiempo de los eventos que tuvieron lugar en el sistema informático examinado.
- Hashing: Este módulo calcula sumas de verificación hash para los archivos y otros datos para verificar su integridad y detectar posibles manipulaciones.
- Búsqueda de palabras clave: Este módulo busca palabras clave específicas en archivos, registros y otros datos.
- Extracción de datos: Este módulo extrae datos de archivos y aplicaciones, como documentos, correos electrónicos, imágenes y registros de chat.
- Análisis de malware: Este módulo analiza archivos en busca de malware y otro código malicioso.
- Visualización de datos: Este módulo proporciona herramientas para visualizar los datos recopilados durante la investigación, como gráficos, tablas y mapas.
- Analizador de Android: interpreta archivos de dispositivos Android.

Autopsy también incluye una serie de módulos adicionales que proporcionan funciones especializadas, como:

- Análisis de archivos de registro: Este módulo analiza archivos de registro para identificar eventos de seguridad y actividad del usuario.
- Análisis de red: Este módulo analiza el tráfico de red para identificar posibles intrusiones y ataques.
- Análisis de imágenes: Este módulo analiza imágenes para identificar objetos y personas.

- Análisis de correo electrónico: Este módulo analiza correos electrónicos para identificar mensajes maliciosos y pistas de investigación.

Autopsy se puede integrar con otras herramientas forenses digitales, como Volatility y The Sleuth Kit, para ampliar sus capacidades.

- Video Triage: Efficiently triage video content by splitting video files up into easily viewable thumbnail images (keyframes).
- Law Enforcement Bundle: Integrate Project Vic and C4P/All databases to identify known child exploitation images.