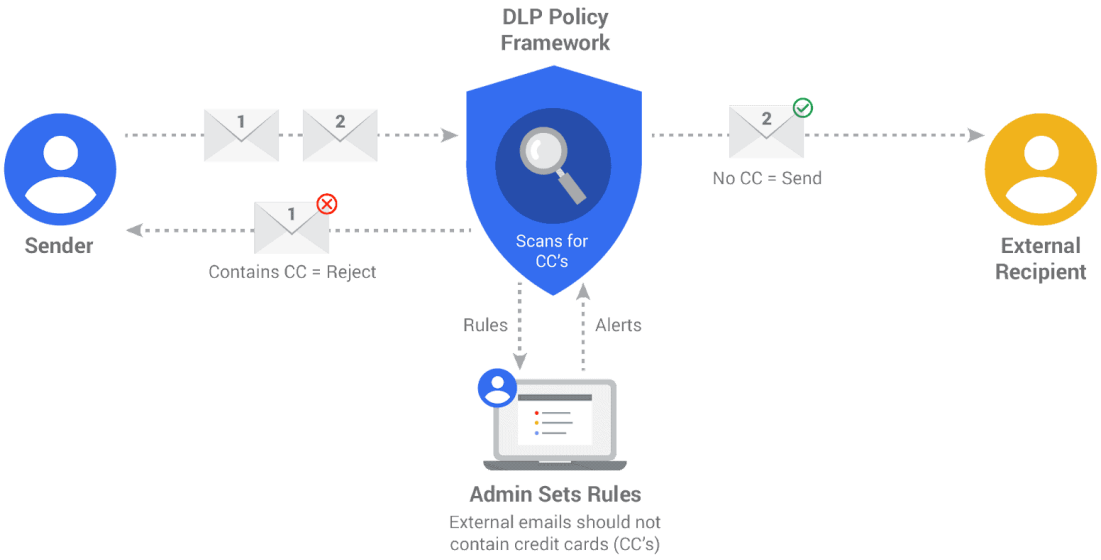
Análisis Forense Digital – Autopsy 4.22.1



Gianfranco Colque Zegarra

1. Introducción

Este informe documenta los hallazgos extraídos del análisis forense digital realizado sobre una imagen de disco forense con extensión. **E01**, identificada como **windows-machine-evidence.E01_1 Host**, mediante el software de análisis forense **Autopsy 4.22.1**. El objetivo principal del análisis es recuperar evidencias digitales relevantes relacionadas con una posible actividad sospechosa, así como documentar de forma detallada la información encontrada durante el proceso.

2. Herramientas utilizadas

Una de ellas para este análisis forense digital que se utilizaron fue:

- Autopsy: herramienta de código abierto que se utiliza para poder hacer análisis exhaustivo de los discos duros o cualquier otra unidad de almacenamiento.

3. Visión General de los Artefactos Detectados

El panel izquierdo del software presenta múltiples categorías relevantes. A continuación, se detallan los elementos más destacados encontrados en la sección **Data Artifacts** y **Analysis Results**:

3.1. Artefactos del Sistema y Usuario

3.1.1. Extensiones de Chromium (36)

Se han identificado 36 extensiones del navegador basadas en Chromium. Estas pueden incluir herramientas útiles, pero también potenciales extensiones maliciosas como adware, keyloggers o redirectores de tráfico.

3.1.2. Perfiles de Chromium (2)

Indica que existen al menos dos perfiles de usuario en navegadores basados en Chromium (como Google Chrome o Edge), lo que sugiere múltiples cuentas o usuarios activos en el sistema.

3.1.3. Favicon (50)

Se encontraron 50 íconos de sitios web visitados, lo cual permite rastrear páginas frecuentadas por el usuario.

3.1.4. Programas Instalados (28)

Se han identificado 28 programas instalados. La revisión de esta lista permite detectar posibles herramientas de hacking, software sospechoso o aplicaciones no autorizadas.

3.1.5. Información del Sistema Operativo

El sistema detectó metadatos sobre el sistema operativo Windows instalado. Esto puede incluir versión, arquitectura, nombre del host, entre otros.

3.1.6. Documentos Recientes (13)

El historial de archivos abiertos recientemente revela actividad del usuario que puede ser clave para reconstruir eventos.

3.1.7. Shell Bags (11)

Los Shell Bags muestran cómo el usuario navegó por las carpetas del sistema, revelando estructura de directorios accedidos recientemente.

3.1.8. Dispositivos USB Conectados (2)

Se detectaron dos dispositivos USB conectados previamente. Esto es crucial para investigar posibles extracciones o inserciones de datos fuera del sistema.

3.2. Artefactos de Navegación Web

3.2.1. Web Cache (1056)

Una gran cantidad de archivos de caché web (1056) sugiere una navegación activa. Este contenido puede incluir páginas cargadas, imágenes, scripts, etc.

3.2.2. Web Cookies (98)

Las cookies permiten identificar sesiones activas, logins persistentes, sitios web accedidos y patrones de navegación.

3.2.3. Historial Web (34)

El historial revela qué sitios web fueron visitados por el usuario, lo que permite rastrear intención o comportamiento sospechoso.

3.2.4. Búsquedas Web (8)

Se detectaron 8 búsquedas realizadas. Este campo es valioso para entender el propósito de las acciones del usuario (búsqueda de herramientas, soluciones técnicas, etc.).

3.2.5. Descargas Web (2)

Muestra que el usuario descargó al menos 2 archivos desde la web. Este dato es fundamental para evaluar si se descargaron scripts, ejecutables o archivos maliciosos.

3.2.6. Marcadores Web (2)

Reflejan sitios de interés guardados por el usuario, lo cual puede ayudar a identificar patrones de navegación frecuentes o vínculos con sitios oscuros.

3.3. Resultados del Análisis Automático

3.3.1. Encryption Suspected (2)

El sistema sospecha que al menos dos archivos están cifrados. Esto puede indicar la presencia de técnicas de ocultamiento, ransomware o protección de información.

3.3.2. Mismatch de Extensión Detectado (54)

Se identificaron 54 archivos con una extensión que no coincide con su contenido real. Esto puede ser usado como técnica de evasión para ocultar malware (por ejemplo, archivos .jpg que en realidad son .exe).

3.3.3. Web Categories (4)

Se agruparon sitios web visitados por categoría. Esto puede ayudar a identificar tendencias de navegación, como acceso a sitios de hacking, redes sociales, contenido adulto, etc.

4. Conclusiones Preliminares

El análisis de esta imagen forense revela una importante cantidad de evidencia digital relevante:

- Navegación web intensiva con datos recuperables.
- Posibles conexiones de dispositivos USB que deben investigarse por extracción de datos.
- Presencia de archivos cifrados y extensiones inconsistentes que podrían indicar actividades maliciosas.
- Múltiples perfiles de usuario y extensiones del navegador que pueden requerir un análisis individual.

5. Recomendaciones

1. **Análisis Manual de Archivos Sospechosos:** Revisar los archivos con extensión inconsistente o cifrado.
2. **Evaluación de Actividad USB:** Analizar el contenido de los dispositivos USB conectados.
3. **Seguimiento de Historial Web y Descargas:** Comparar patrones de búsqueda y descargas con posibles indicadores de compromiso.
4. **Análisis de Extensiones de Navegador:** Clasificar las 36 extensiones como benignas, desconocidas o maliciosas.
5. **Exportación de Artefactos Clave:** Como favoritos, búsquedas, historial de descargas, documentos recientes y registros USB para documentación legal.