sepian

Seguridad Digital
de Andalucía

WEBINAR

Herramientas de Análisis Forense bajo GPL

¿Qué? ¿Quién? ¿Dónde? ¿Cuándo? ¿Cómo? ¿Por qué?

JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

Contenidos

Qué vamos a tratar

Contenidos

1. Conceptos claves, procedimientos y técnicas
2. Software usado en informática forense
3. Despliegue y uso del software forense

Conceptos claves, procedimientos y técnicas

sedian Seguridad Digital de Andalucía

- La **evidencia digital** es la información que es relevante para una investigación y se almacena en dispositivos informáticos.
- Matices:
  - **Evidencia física**: hace referencia al dispositivo físico: HDD, USB, SD...
  - **Evidencia digital o electrónica**: es la información que se almacena en formato digital (en las evidencias físicas).
- No es sinónimo de **prueba digital** (esta implica un matiz probatorio).

La parte defensora intentará invalidar las evidencias que se admitan como prueba

Para ello debemos evitar cometer errores como:

- No usar bloqueadores de escritura.
- En la adquisición, siempre hashear las evidencias físicas que se comporten como volumen de datos.
- No usar MD5 o SHA-1 como algoritmos de hash. Presentan demasiadas colisiones.
- Respetar escrupulosamente tu papel en la cadena de custodia.
- No extralimitarse en la adquisición de evidencias.


Preservación
Adquisición
Documentación
Análisis
Presentación
Preservación: Mantener la validez y confiabilidad de las evidencias originales
Adquisición: Clonado de datos originales
Documentación: Documentación del procedimiento completo, desde el inicio del análisis hasta el envío del informe
Análisis: Procesos y tareas realizadas para averiguar las causas del evento que motivó la investigación
Presentación: Realización del informe pericial con toda la información obtenida

- Algoritmo matemático que toma como entrada una secuencia de bits de tamaño variable y devuelve otra de tamaño fijo.
- Puerta única (irreversible).
- Probabilidad de las colisiones.
- MD5 criptográficamente predecible. Puede no admitirse.
- Mejor SHA-256.

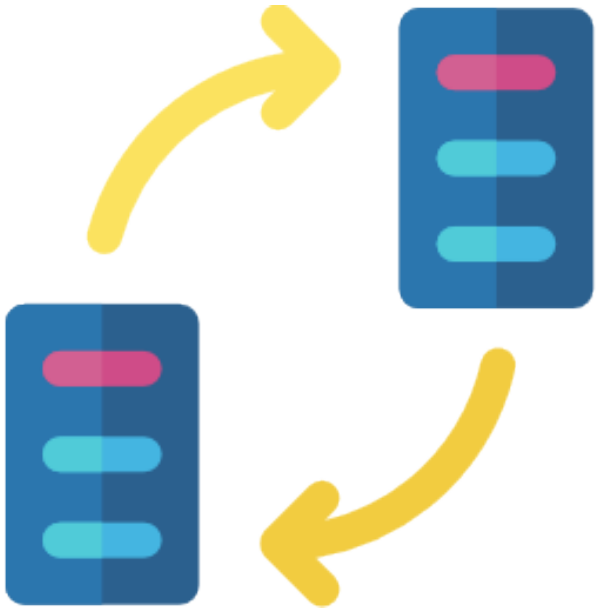
- Conocer sistema de particiones comunes: FAT, NTFS, EXT, etc.
- La información interesante puede estar en **unallocated** (eliminada permanentemente) o en **allocated** (papelera de reciclaje).
- Se puede recuperar información después del borrado o borrados del disco (hasta cierto punto).

- Si el dispositivo está **encendido**, la buena práctica obliga a capturar la evidencia inmediatamente.
- No debe apagarse.
- Usar herramientas portables para adquirir:
  - Archivo de hibernación.
  - Comunicaciones establecidas.
  - Logs del sistema/ Registro de Windows.
  - Unidades de red.
  - Archivos SQLite (móviles)...
  - Dejar para lo último La RAM y el Archivo de paginación o swap. (BSOD).
- Es interesante hacer una foto de la pantalla para incorporar al informe.

- Se realiza partiendo del equipo apagado.
- Se pueden extraer los discos y realizar adquisición por clonación.
- Se pierde la información volátil no persistente.

La **adquisición** es el procedimiento para volcar los datos de un sistema de archivos. Se puede realizar:

- A nivel **físico**: clonación. Genera una imagen. Generalmente Post-Mortem.
- A nivel **lógico**: copia de archivos. No incluye unallocated. Típica en móviles. Puede realizarse en vivo.



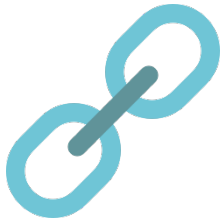
- Almacenan información complementaria.
- Muy importantes para la IF.
- Ciertos formatos ofrecen información de calidad (EXIF).
- El sistema operativo solo muestra los metadatos más básicos y se requiere software especializado para leerlos (FOCA).

Software usado en Informática Forense

Las herramientas que usa el análisis forense

sedian Seguridad Digital de Andalucía

Listado de herramientas forenses digitales:



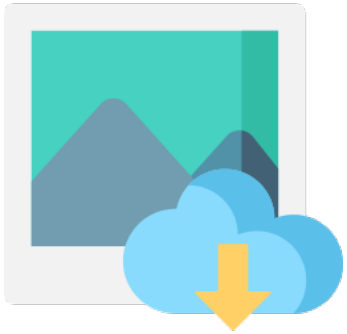
https://en.wikipedia.org/wiki/List_of_digital_forensics_tools

Despliegue y uso del software forense

Empezamos con las prácticas

sedian Seguridad Digital de Andalucía

- Bloqueadores de escritura.
- Permiten salvaguardar la evidencia original garantizando que no se modifica ni un solo bit.
- Localizar información sobre bloqueadores comerciales por hardware: precios, interfaces que admite, etc.



FTK Imager: Herramienta de adquisición para Windows.

Caine. Distro de Linux de Open Source de primer nivel.

- Facilita la adquisición y análisis de un equipo en forma Post-Mortem.
- Instalar CAINE en USB y realizar captura y análisis de un equipo (triaje).

Práctica: Usar GUYMAGER para capturar los discos de equipo.

AUTOPSY
DIGITAL FORENSICS

sedian Seguridad Digital de Andalucía

Despliegue y uso del software forense

Práctica: Usar Autopsy para análisis forense.

sedian Seguridad Digital de Andalucía