THE BRIDGE

CYBER SECURITY

Fundamentos de Análisis Forense

Análisis Forense Digital

- El **análisis forense**, o **forense digital**, es el proceso de investigar y recolectar pruebas de dispositivos electrónicos (como computadoras, teléfonos móviles, servidores, etc.) con el fin de identificar, preservar, analizar y presentar datos que puedan ser relevantes para un caso legal o de investigación.

- El objetivo principal es descubrir pruebas digitales que ayuden en la resolución de delitos, fraudes, intrusiones informáticas o cualquier tipo de incidente relacionado con la tecnología.

- Existen varios tipos de análisis forense dependiendo del contexto:

  - **Forense informático.**
  - **Forense de redes.**
  - **Forense de dispositivos móviles.**
  - **Forense de malware**
  - **Forense en la nube**

https://www.securityartwork.es/2016/02/10/analisis-forense-cadena-de-custodia-de-la-evidencia-digital/

Evidencia Digital

- La evidencia digital es cualquier información almacenada o transmitida en formato digital que puede ser utilizada en un tribunal de justicia u otra investigación formal.
- Incluye archivos, correos electrónicos, logs, registros de bases de datos, tráfico de red, mensajes en redes sociales, entre otros.
- Características de la evidencia digital:
  - **Fragilidad.**
  - **Volatilidad.**
  - **Reproducibilidad**.
- Tipos de evidencia digital:
  - **Archivos electrónicos.**
  - **Metadatos.**
  - **Registros de sistemas y redes.**
  - **Datos eliminados o ocultos.**

https://ciberseguridadtips.com/evidencias-digitales/

Cadena de Custodia

- La cadena de custodia es el proceso que garantiza la documentación de cada paso que sigue una evidencia digital, desde su identificación hasta su presentación en un tribunal.

- Cada persona que manipula o tiene acceso a la evidencia debe estar registrada para asegurar que no haya sido alterada.

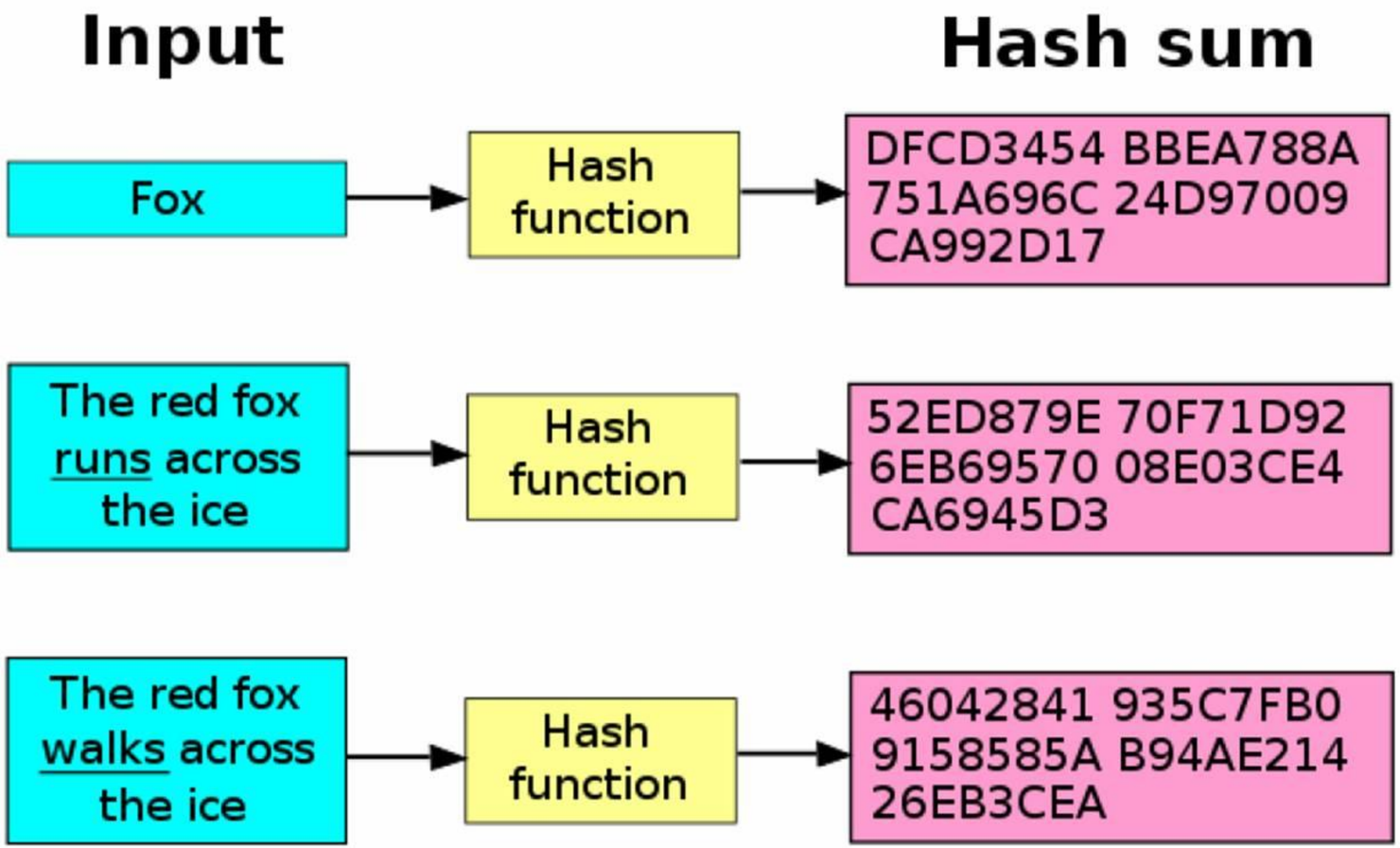
- **Importancia**:
  - La cadena de custodia es crucial para que la evidencia sea aceptada en un tribunal.
  - Si no se puede demostrar que la evidencia fue manejada adecuadamente, podría ser invalidada.
  - Protege contra cualquier alegación de que la evidencia haya sido manipulada o alterada.

- **Elementos de la cadena de custodia:**
  - Identificación de la evidencia.
  - Registro detallado.
  - Métodos de preservación.
  - Almacenamiento seguro.

https://www.precintia.com/blog/cadena-custodia-precintos-seguridad/

Integridad de la Evidencia

- La integridad de la evidencia digital se refiere a la garantía de que los datos no han sido modificados desde su recolección.
- Para comprobar esto, se utilizan técnicas de **hashing**.
- Importancia en el análisis forense
  - Si la integridad de los datos no se puede demostrar, la evidencia puede no ser aceptada en un tribunal, ya que podría haber sido alterada.



https://xeushack.com/on-hashes

Recuperación de Datos Eliminados

- La recuperación de datos eliminados es un proceso clave en el análisis forense digital, en el que se emplean herramientas especializadas para intentar restaurar archivos que han sido borrados o sobrescritos en un sistema.

- **Cómo funciona:**

  - Cuando un archivo se elimina de manera convencional, en muchos sistemas el archivo no se borra de inmediato del disco.

  - Lo que se elimina es la referencia a ese archivo en la tabla del sistema de archivos, pero el contenido puede permanecer en el disco hasta que sea sobrescrito.

- Las Herramientas forenses permiten escanear los sectores del disco en busca de esos datos "huérfanos" y recuperarlos si no han sido sobrescritos.

- Algunos Programas
  - Recuva
  - The Sleuth Kit
  - EnCase

https://www.losmejoresdiscosssd.es/programas-para-recuperar-datos-de-un-disco-duro-externo/

Recuperación de Datos Eliminados – Data Carving

- El **data carving** (también conocido como **file carving**) es una técnica para recuperar datos de archivos que han sido eliminados, fragmentados o cuyo sistema de archivos ha sido corrompido.

- Este no depende de la información del sistema de archivos (como las tablas de archivos o directorios), sino que se enfoca en la estructura interna de los archivos y patrones de datos para reconstruirlos.

- Pasos del Data Carving
  - **Análisis del Disco (o Imágenes Forenses).**

  - **Identificación de Headers y Footers**
    - Por ejemplo:
      - **JPEG**: Comienza con FFD8 y termina con FFD9.
      - **PDF**: Comienza con %PDF- y puede terminar con %%EOF.
      - **MP3**: Comienza con ID3 o secuencias de bytes específicas del formato de audio.

  - **Reunión de Fragmentos (en casos de fragmentación).**

  - **Reparación de Archivos Parcialmente Recuperados.**

- **Herramientas**
  - The Sleuth Kit (TSK) y Autopsy:
  - Foremost
  - FTK Imager
  - PhotoRec

https://medium.com/@starusrecovery.com/data-carving-signature-based-data-recovery-9f22b828c521

Imágenes Forense

- Una imagen forense es una copia bit a bit de un dispositivo de almacenamiento (disco duro, USB, etc.).
- Esta copia exacta asegura que todos los datos, incluyendo los espacios vacíos o sectores defectuosos, son clonados para su análisis posterior.
- **Importancia**:
  - El análisis se realiza sobre la imagen y no sobre el dispositivo original, para evitar alterar la evidencia original.
  - Las imágenes forenses permiten recrear el estado exacto de un dispositivo en el momento de su adquisición.
- **Herramientas**:
  - FTK Imager
  - EnCase
  - dd

https://www.profesionalreview.com/2021/02/06/como-copiar-disco-duro/

El proceso de Análisis Forense Digital

- El **análisis forense** sigue un protocolo riguroso para asegurar que las pruebas digitales sean válidas en un tribunal y no se vean comprometidas.
- Las etapas clave suelen incluir:
  - **Identificación de la evidencia**
  - **Adquisición de la evidencia**
  - **Preservación de la evidencia**
  - **Análisis de la evidencia**
  - **Presentación de la evidencia.**

https://www.dominuxsecure.com/analisis-forense-digital/

Identificación de la Evidencia

- Localizar posibles fuentes de evidencia digital.
- Esta fase es crucial para identificar qué dispositivos, sistemas o redes pueden contener la información relevante para la investigación. Se identifican elementos como discos duros, servidores, memorias USB, dispositivos móviles, correos electrónicos, cuentas en la nube, entre otros.
- **Tareas principales:**
  - **Determinación de los dispositivos relevantes**
  - **Mapeo de la infraestructura de red**
  - **Identificación de testigos clave o usuarios involucrados.**
  - **Determinación del tipo de evidencia digital**
  - **Registro de cuentas de usuario y contraseñas**

https://www.dominuxsecure.com/analisis-forense-digital/

Adquisición de la Evidencia

- Recopilar los datos de manera controlada y estructurada.
- En esta fase se procede a la adquisición de los datos digitales de los sistemas identificados. Es esencial seguir métodos rigurosos que eviten la contaminación de las pruebas.
- **Tareas principales:**
  - **Clonación de discos duros.**
  - **Captura de datos en sistemas virtualizados.**
  - **Captura de datos en la nube.**
  - **Captura de dispositivos móviles.**
  - **Extracción de bases de datos.**

https://www.dominuxsecure.com/analisis-forense-digital/

Preservación de la Evidencia

- Garantizar que las evidencias digitales no sean alteradas o destruidas.
- La preservación de las evidencias es fundamental en el análisis forense digital.
- En esta fase, se toman medidas para proteger y salvaguardar los datos, asegurando que no se alteren durante el proceso de investigación.
- La cadena de custodia y la integridad de los datos son aspectos críticos.
- Tareas principales:
  - **Desconexión segura del sistema.**
  - **Bloqueo de escritura.**
  - **Captura de la memoria RAM.**
  - **Documentación fotográfica de la escena.**
  - **Recolección de dispositivos de almacenamiento extraíbles.**

https://www.dominuxsecure.com/analisis-forense-digital/

Análisis de la Evidencia

- Examinar las evidencias recolectadas en busca de patrones, indicios o eventos relevantes.
- Esta fase es el corazón del proceso forense.
- Los datos obtenidos se analizan en profundidad, con el objetivo de identificar actividades sospechosas, recuperar datos eliminados y establecer una línea de tiempo de los eventos.
- Tareas principales:
  - **Creación de línea de tiempo.**
  - **Identificación de aplicaciones maliciosas.**
  - **Análisis de correos electrónicos.**
  - **Detección de patrones de uso indebido de cuentas.**
  - **Recuperación de historial de navegación y cookies.**
  - **Desarrollo de análisis estadísticos.**

https://www.dominuxsecure.com/analisis-forense-digital/

Preservación de la Evidencia

- Objetivo: Elaborar y comunicar los resultados de manera comprensible y adecuada.
- Descripción: Una vez obtenido el análisis completo, los hallazgos se documentan de manera formal para ser utilizados en un tribunal o ante otras partes interesadas. La presentación de los resultados debe ser clara, completa y comprensible para audiencias técnicas y no técnicas.
- Tareas principales:
  - **Redacción de un informe técnico detallado.**
  - **Preparación para defensa en juicio.**
  - **Elaboración de resúmenes ejecutivos.**
  - **Defensa de la cadena de custodia.**
  - **Responder a cuestionarios legales.**

https://www.dominuxsecure.com/analisis-forense-digital/

Evidencias Post-Informe

- Después de la finalización del análisis forense, las evidencias deben almacenarse de forma segura o, en caso de ser necesario, destrucción controlada según los procedimientos legales.
- Esta fase es crítica para garantizar que las pruebas no puedan ser reutilizadas o comprometidas en el futuro.
- Tareas principales:
  - **Revisión y archivado de la cadena de custodia.**
  - **Almacenamiento en dispositivos seguros.**
  - **Revisión periódica de evidencias almacenadas.**
  - **Preparación para apelaciones o nuevas investigaciones.**
  - **Destrucción segura de las evidencias.**

https://www.precintia.com/blog/cadena-custodia-precintos-seguridad/


THE
BRIDGE