UNIVERSIDAD PARAGUAYO ALEMANA

Ingeniería en Tecnologías de la Información Empresarial TIE

Seguridad en TICs

Prof.: Chrystian Ruiz Diaz

DISCLAIMER

Todo el contenido de esta presentación se proporciona **exclusivamente con fines didácticos y educativos en el ámbito académico**.

El uso inapropiado de las técnicas y/o conocimientos expuestos en esta presentación puede violar leyes nacionales e internacionales.

El autor y la institución educativa no se hacen responsables del uso indebido de la información contenida en esta presentación.

Se enfatiza que la información debe ser empleada únicamente para propósitos éticos, legales y con la debida autorización de las autoridades competentes.

Introducción al Análisis Forense Digital

Contenido

- Etapas En El Análisis Forense De Un Incidente Informático
- Principios durante la recolección de evidencias
- Captura de las evidencias volátiles y no volátiles
- Orden de volatilidad
- Preservación de las evidencias digitales: cadena de custodia
- Análisis de las evidencias obtenidas
- Procedimiento de recolección
- El procedimiento de almacenamiento
- Herramientas necesarias
- HERRAMIENTAS DE ANÁLISIS FORENSE
- Organismos Y Medios Especializados En Informática Forense
- Acciones que deben evitarse
- Consideraciones sobre la privacidad

Conceptos

La **Ciencia Forense** nos proporciona los principios y técnicas que facilitan la investigación de los delitos criminales, mediante la identificación, captura, reconstrucción y análisis de las evidencias.

Una evidencia es toda aquella información que podrá ser capturada y analizada posteriormente para interpretar de la forma más exacta posible el incidente de seguridad: en qué ha consistido, qué daños ha provocado, cuáles son sus consecuencias y quién pudo ser el responsable

Introducción al Análisis Forense Digital

Etapas Análisis Forense de un Incidente Informático

1. Identificación y captura de las evidencias.
2. Preservación de las evidencias.
3. Análisis de la información obtenida.
4. Elaboración de un informe con las conclusiones del análisis forense.

Principios durante la recolección de evidencias

1. Capturar una imagen del sistema tan precisa como sea posible.
2. Realizar notas detalladas, incluyendo fechas y horas indicando si se utiliza horario local o UTC.
3. Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
4. En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.
5. Recoger la información según el orden de volatilidad (de mayor a menor).
6. Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera

Introducción al Análisis Forense Digital

Las evidencias digitales o electrónicas pueden ser **admitidas como prueba en un juicio**, si se ofrecen unas determinadas garantías en las distintas etapas del análisis forense

Evidencias Tangibles
Evidencias Intangibles

Volcado de la memoria global del sistema y de cada proceso ➔ dificultad

- Procesos y servicios en ejecución dentro del sistema
- Controladores (drivers) instalados para gestionar distintos recursos hardware del sistema
- Información de la situación y configuración de los servicios y las tarjetas de red: configuración del protocolo TCP/IP, puertos abiertos, caché del protocolo ARP, caché de DNS, etc
- Usuarios y grupos de usuarios activos dentro del sistema: qué sesiones se encuentran abiertas en el momento de llevar a cabo el análisis del equipo

Introducción al Análisis Forense Digital

Orden de volatilidad

El orden de volatilidad hace referencia al período de tiempo en el que está accesible cierta información. Es por ello que se debe recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor

Lista ordenada de mayor a menor volatilidad

- Registros y contenido de la caché.
- Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria.
- Información temporal del sistema.
- Disco
- Logs del sistema.
- Configuración física y topología de la red.
- Documentos.

Introducción al Análisis Forense Digital

Cadena de Custodia

A la hora de preservar las evidencias digitales será necesario contemplar una serie de tareas de tipo técnico y de medidas de carácter organizativo, teniendo en cuenta las recomendaciones de la IOCE (*International Organization on Computer Evidence, Organización Internacional sobre Evidencias Informáticas*)

1. Utilizar un **adecuado método de identificación, precinto, etiquetado y almacenamiento de las evidencias**, considerando la posible incorporación de una firma temporal (digital timestamp)
2. Estas evidencias digitales deberán ser **preservadas de factores ambientales adversos**: campos magnéticos, fuentes de radiación
3. Garantizar que los datos digitales adquiridos de copias **no puedan ser alterados**, por lo que para su obtención se deberían emplear herramientas de generación de imágenes bit a bit, que incorporen códigos de comprobación (checksums o algoritmos de huella digital como SHA-1 o MD5)
4. **Profesionales con los conocimientos adecuados**
5. Documentación clara y precisa

Introducción al Análisis Forense Digital

Análisis de las evidencias obtenidas

El análisis de las evidencias digitales capturadas en las etapas anteriores podría ser realizado mediante **herramientas especializadas** (como EnCase) que permiten analizar la imagen obtenida de los discos duros **sin tener que volcarla** a otro disco o unidad de almacenamiento.

- Búsqueda de información (cadenas de caracteres alfanuméricos) para localizar ficheros sospechosos
- Comprobación de la integridad en los ficheros y librerías del sistema, para detectar posibles manipulaciones (presencia de rootkits en el sistema)

Introducción al Análisis Forense Digital

Para los ficheros realizar lo siguiente:

- Identificar de los tipos de archivos, a partir de sus extensiones o del estudio de los “números mágicos” (Magic Numbers), es decir, de la información contenida en la cabecera de cada fichero
- Visualizar del contenido de los ficheros gráficos
- Estudiar de las fechas de creación, cambio y último acceso a los ficheros, para detectar qué ficheros han experimentado cambios o han sido creados en las fechas próximas al incidente
- Revisar los permisos de acceso y ejecución de los ficheros, así como de la información sobre quiénes son sus propietarios
- Revisar los distintos ficheros temporales obtenidos en la imagen del sistema: memoria temporal (caché) del navegador, direcciones URL que se han tecleado en la caja de direcciones, contenido del historial del navegador, caché del protocolo ARP, archivo de paginación del sistema (swap)

Introducción al Análisis Forense Digital

Ficheros ocultos

- Activación del atributo “oculto” en las propiedades de algún fichero para que no sea mostrado por el sistema operativo.
- Información y ficheros ocultos en otros ficheros mediante técnicas esteganográficas.
- Mecanismo ADS (Alternate Data Streams) del sistema de ficheros NTFS de Windows, utilizado para mantener información sin estructura asociada a un fichero (un icono, por ejemplo)

Introducción al Análisis Forense Digital

Procedimiento de recolección

1. **Transparencia**: Los métodos utilizados para recolectar evidencias deben de ser transparentes y reproducibles

2. **Pasos**: Listar qué sistemas están involucrados en el incidente y de cuáles de ellos se deben tomar evidencias.

- Establecer qué es relevante. En caso de duda es mejor recopilar mucha información que poca.
- Fijar el orden de volatilidad para cada sistema.
- Obtener la información de acuerdo al orden establecido.
- Comprobar el grado de sincronización del reloj del sistema.
- Según se vayan realizando los pasos de recolección preguntarse qué más puede ser una evidencia.
- Documentar cada paso.
- No olvidar a la gente involucrada. Tomar notas sobre qué gente estaba allí, qué estaban haciendo, qué observaron y cómo reaccionaron.

Introducción al Análisis Forense Digital

El procedimiento de almacenamiento

- **Cadena de custodia**

  - ¿Dónde?, ¿cuándo? y ¿quién? descubrió y recolectó la evidencia.
  - ¿Dónde?, ¿cuándo? y ¿quién? manejó la evidencia.
  - ¿Quién ha custodiado la evidencia?, ¿cuánto tiempo? y ¿cómo la ha almacenado?

- **Dónde y cómo almacenarlo**

Se debe almacenar la información en dispositivos cuya seguridad haya sido demostrada y que permitan detectar intentos de acceso no autorizados.

Introducción al Análisis Forense Digital

Herramientas necesarias

- Se deben utilizar **herramientas ajenas al sistema** ya que éstas pueden haberse visto comprometidas, principalmente en los casos de malware.
- Se debe procurar utilizar **herramientas que alteren lo menos posible el escenario**, **evitando** el uso de herramientas de **interfaz gráfico** y aquellas cuyo uso de memoria sea grande.
- Los programas que se vayan a utilizar para **recolectar las evidencias** deben estar ubicados en un dispositivo de **sólo lectura (CDROM, USB, etc.).**
- Se debe preparar un conjunto de **utilidades adecuadas a los sistemas operativos** con los que se trabaje.
- El kit de análisis debe incluir los siguientes tipos de herramientas
  - Programas para listar y examinar procesos.
  - Programas para examinar el estado del sistema.
  - Programas para realizar copias bit a bit.

Introducción al Análisis Forense Digital

Organismos Y Medios Especializados En Informática Forense

- IACIS: http://www.iacis.com/.
- IOCE: http://www.ioce.org/.
- RFC 2350 - Expectations for Computer Security Incident Response: http://www.ietf.org/rfc/rfc2350.txt.
- RFC 3227 - Guidelines for Evidence Collection and Archiving: http://www.ietf.org/rfc/rfc3227.txt.
- Computer Forensic: http://www.computer-forensic.com/.
- The International Journal of Digital Evidence: http://www.ijde.org/.
- The Electronic Evidence Information Center, con recursos sobre análisis forense digital: http://www.e-evidence.info/.

Introducción al Análisis Forense Digital

Acciones que deben evitarse

Se deben evitar las siguientes acciones con el fin de no invalidar el proceso de recolección de información ya que debe preservarse su integridad con el fin de que los resultados obtenidos puedan ser utilizados en un juicio en el caso de que sea necesario:

- **No apagar el ordenador** hasta que se haya recopilado toda la información.
- **No confiar en la información proporcionada por los programas del sistema** ya que pueden haberse visto comprometidos. Se debe recopilar la información mediante programas desde un medio protegido como se explicará más adelante.
- **No ejecutar programas que modifiquen la fecha y hora de acceso** de todos los ficheros del sistema.

Introducción al Análisis Forense Digital

Consideraciones sobre la privacidad

Es muy importante tener en consideración las pautas de la empresa en lo que a privacidad se refiere.

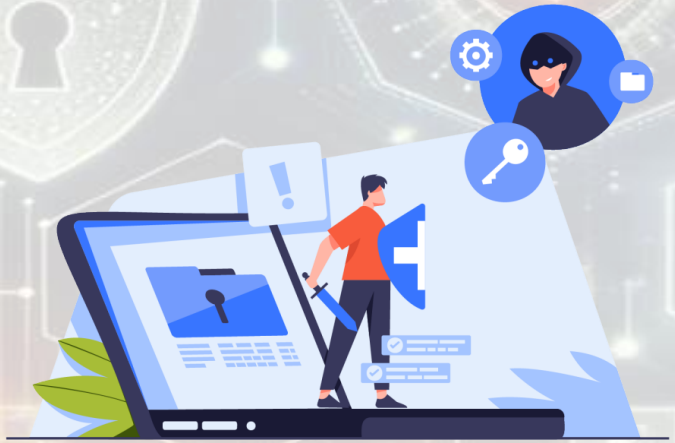
- Es habitual **solicitar una autorización por escrito** de quien corresponda para poder llevar a cabo la recolección de evidencias. Este es un aspecto fundamental ya que puede darse el caso de que se trabaje con **información confidencial o de vital importancia para la empresa**, o que la disponibilidad de los servicios se vea afectada.
- **No hay que entrometerse en la privacidad de las personas sin una justificación**.
- **No se deben recopilar datos de lugares a los que normalmente no hay razón para acceder**, como ficheros personales, a menos que haya suficientes indicios

¿PREGUNTAS?

Referencias

- COSTAS SANTOS, J. (2014). Seguridad informática. RA-MA, SA.
- ESCRIVA, G. R. (2013). Seguridad Informática. España: Macmillan Iberia SA .
- INCIBE. (21 de 04 de 2021). https://www.incibe-cert.es/blog/rfc3227. Obtenido de INCIBE RFC3227: https://www.incibe-cert.es/blog/rfc3227
- Internautas. (07 de 04 de 2020). Internautas. Obtenido de https://www.internautas.org/w-scanonline.php

Actividad de Proceso



Muchas Gracias..!!