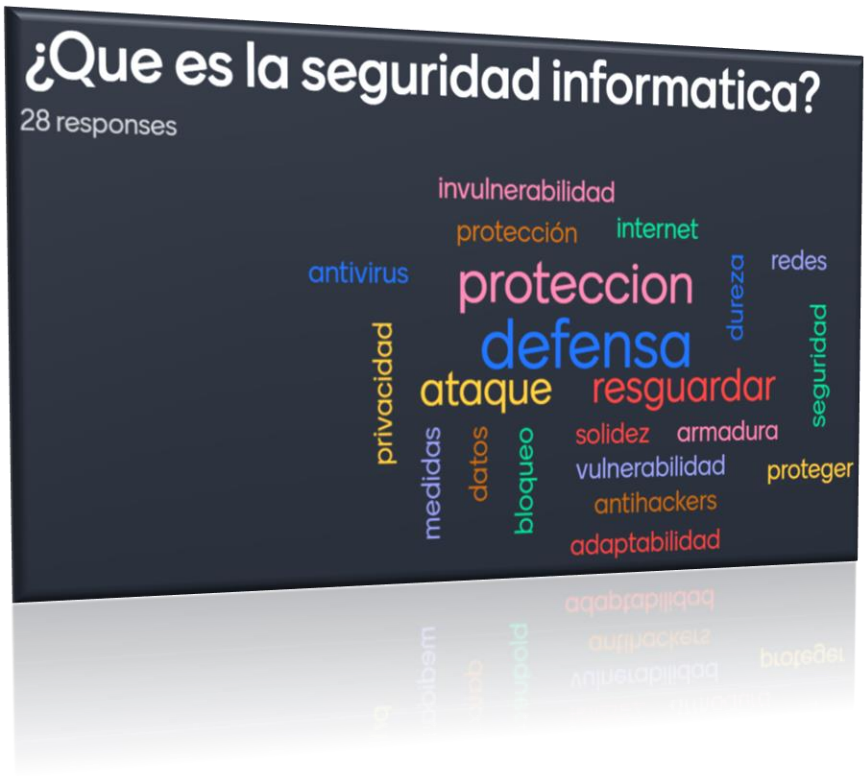
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

Introducción al Análisis Forense Digital

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.

La Ciencia Forense recurre a la aplicación de un método científico para analizar las evidencias disponibles y formular hipótesis sobre lo ocurrido.

El trabajo de la Ciencia Forense se basa en el "Principio de Transferencia de Locard", según el cual cualquier persona u objeto que entra en la escena del crimen deja un rastro en la escena o en la propia víctima, y viceversa, es decir, también se lleva consigo algún rastro de la escena del crimen.

Por su parte, la Informática Forense se encarga de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional (definición propuesta por el FBI).

Un equipo de análisis forense estará constituido por expertos con los conocimientos y experiencia necesarios en el desarrollo de estas actividades. Además, sus miembros deberían contar con el entrenamiento adecuado, prestando especial atención a la puesta al día de sus conocimientos y habilidades.

Para poder realizar este trabajo resultará fundamental contar con los medios y el material especializado para las distintas técnicas del análisis forense, así como disponer de un manual detallado de los procedimientos de actuación, definiendo de forma clara y precisa todas las actividades que se realizarán en cada una de las etapas del análisis forense en sistemas informáticos.

Podemos señalar que una interesante referencia para el análisis forense en los sistemas informáticos es la guía Best Practices for Seizing Electronic Evidence, publicada por el Servicio Secreto de Estados Unidos y accesible en la dirección de Internet http://info.publicintelligence.net/usssbestpractices.pdf.

Etapas En El Análisis Forense De Un Incidente Informático

Podemos distinguir las siguientes etapas en el análisis forense de un incidente informático:

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

Seguidamente se estudiarán las actividades y aspectos a tener en cuenta en cada una de estas actividades

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 (INCIBE, https://www.incibe-cert.es/blog/rfc3227, 2021).

Captura de las evidencias volátiles y no volátiles

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. También se pueden considerar como evidencias los campos magnéticos y los pulsos electrónicos emitidos por los equipos informáticos.

A pesar de ser intangibles, 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, mediante el aislamiento de la escena del crimen para evitar la corrupción de ésta y de las posibles evidencias que en ella puedan hallarse.

Así mismo, es posible generar distintas copias de las evidencias digitales para facilitar su conservación y posterior análisis. La tecnología informática permitirá averiguar si alguna de estas copias ha sido modificada o falsificada, comparándola con la original.

Debemos tener en cuenta, por lo tanto, que el proceso de captura de evidencias digitales no debe alterar el escenario objeto de análisis. En la práctica esto es muy difícil de conseguir, ya que las herramientas utilizadas van a modificar la memoria del sistema informático en el que se ejecutan. De hecho, la ejecución de determinados comandos en

el sistema podría alterar la información registrada en el disco: así, por ejemplo, un simple listado del contenido de un directorio va a modificar la fecha de último acceso a cada fichero.

Además, conviene utilizar herramientas grabadas en un pendrive, en un CD-ROM o en otro soporte de almacenamiento, que se puedan ejecutar directamente sin requerir instalación ni utilizar un entorno gráfico, para que resulten lo menos intrusivas posible y no afecten a la imagen en los discos duros del sistema.

No es recomendable emplear las propias herramientas del sistema, ya que éstas podrían haber sido manipuladas por terceros, mediante rootkits o troyanos. Así mismo, es necesario emplear medios forénsicamente estériles para guardar una copia de las evidencias digitales, es decir, medios que no hayan tenido datos previos en ellos.

También es conveniente obtener la imagen fotográfica de todas las pantallas que muestra el sistema informático durante el proceso de captura de las evidencias digitales.

La captura de las evidencias digitales se complica aún más con las evidencias volátiles, entendiendo como tales a toda aquella información que se perderá al apagar un equipo informático objeto de análisis. Podemos considerar la siguiente relación de evidencias digitales volátiles:

Volcado de la memoria global del sistema y de cada proceso: ante la dificultad de realizar un análisis en profundidad, se podrá utilizar el volcado de memoria para buscar determinadas cadenas de caracteres que puedan dar pistas sobre el incidente que ha afectado al equipo.

- Procesos y servicios en ejecución dentro del sistema: de cada proceso o servicio sería conveniente identificar el fichero ejecutable y los parámetros de ejecución, así como la cuenta de usuario bajo la que se ejecuta, los ficheros que está usando y qué otro proceso o servicio lo ha llamado (árbol de ejecución), para posteriormente poder comparar esta información con la situación estable del sistema objeto de estudio.
- 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, enlaces entre los protocolos y las distintas interfaces de red…
- 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.

Tras haber capturado todas las evidencias volátiles, se procederá a obtener la información de los discos duros del sistema. Para ello, conviene apagar de forma repentina el equipo, de modo que se pueda evitar que en el proceso de apagado desde el sistema operativo se puedan borrar algunas evidencias, ya que el atacante podría haber incluido alguna rutina para eliminar evidencias de sus actuaciones dentro del sistema cuando éste fuera apagado. Seguidamente se procederá a arrancar el sistema informático

procurando no alterar la información existente en los discos duros: arranque desde CD-ROM o disquete, cargando un sistema operativo como MS-DOS o Linux.

Para la obtención de la imagen de los discos del sistema informático se tendrá que realizar una duplicación de la información de los discos duros del equipo a analizar, empleando herramientas especializadas como dd, Ghost, Safeback o EnCase, que son capaces de realizar una duplicación sector a sector de cada disco duro, copiando todos los bits en el proceso.

Así, estas herramientas especializadas en la duplicación de discos duros pueden copiar los bits pertenecientes a ficheros válidos, aunque hayan sido registrados como ocultos por el sistema operativo, bits que determinan el used space (espacio utilizado) del disco; los bits de los ficheros marcados como eliminados y que forman parte del free space (espacio libre o disponible); e incluso los bits que se encuentran en las zonas marcadas como no utilizadas dentro de cada sector (slack space) y en los espacios de separación entre particiones y sectores

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.

De acuerdo a esta escala se puede crear la siguiente lista en orden de mayor a menor volatilidad (INCIBE, https://www.incibe-cert.es/blog/rfc3227, 2021):

- 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.

Preservación de las evidencias digitales: 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).

Así, en primer lugar, se deberá utilizar un adecuado método de identificación, precinto, etiquetado y almacenamiento de las evidencias, considerando la posible

incorporación de una firma temporal (digital timestamp) en cada evidencia para que quede registrado el momento en que fue capturada.

Estas evidencias digitales deberán ser preservadas de factores ambientales adversos: campos magnéticos, fuentes de radiación, etcétera. Por este motivo, se recomienda conservar los soportes informáticos donde se han registrado las evidencias digitales en bolsas de plástico antiestáticas.

Así mismo, es necesario 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) para facilitar la comprobación de la integridad de estos datos.

Otro aspecto de gran importancia es la documentación de todo el proceso de adquisición de evidencias, llevado a cabo por profesionales con los conocimientos adecuados. En dicha documentación se debe reflejar de forma clara y precisa la identificación de las personas que intervienen en el proceso, así como el momento y lugar en que se captura cada una de las evidencias. También se puede prever la posibilidad de realizar una grabación en vídeo por parte del equipo encargado de la captura de evidencias digitales.

Por último, resultará fundamental, sobre todo desde un punto de vista legal, el mantenimiento de la cadena de custodia de las evidencias. Con tal motivo, deben estar perfectamente definidas las obligaciones y funciones de cada uno de los miembros del equipo de análisis forense.

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.

La labor de análisis puede comenzar con la búsqueda de información (cadenas de caracteres alfanuméricos) en el volcado de la memoria del sistema o en las imágenes de los discos duros para localizar ficheros sospechosos, como podrían ser programas ejecutables, scripts o posibles troyanos.

A continuación, se podrán ejecutar estos ficheros sospechosos en un entorno de pruebas totalmente controlado (por ejemplo, en una máquina virtual creada mediante la herramienta VMware con la misma configuración que el sistema que ha sufrido el incidente), para estudiar su comportamiento: interacción con el sistema, llamadas a otras aplicaciones o ficheros que intenta modificar (para esto último se pueden emplear herramientas como Filemon o Regmon en los sistemas Windows).

Así mismo, se tendrá que realizar una comprobación de la integridad en los ficheros y librerías del sistema, para detectar posibles manipulaciones (presencia de rootkits en el sistema). Para ello, será necesario disponer de la información sobre el estado del sistema previo al incidente (firmas digitales de los ficheros y librerías, mediante algoritmos como SHA- 1 o MD5). También es posible consultar una base de datos de firmas para

instalaciones típicas de distintos sistemas operativos, como la base de datos NSRL (National Software Reference Library) del Instituto de Estándares NIST de Estados Unidos (www.nsrl.nist.gov).

El análisis de las evidencias también debe contemplar la revisión de los ficheros de configuración del sistema, donde se establecen los parámetros básicos de arranque, los servicios que se van a ejecutar y las directivas de seguridad. Por este motivo, será necesario comprobar la ejecución programada de aplicaciones, así como revisar la configuración de las aplicaciones servidoras que se ejecutaban en el sistema informático objeto de estudio (servidor WWW, servidor FTP…) y los registros de actividad de estas aplicaciones (logs). Se debería tener en cuenta, además, la posibilidad de obtener datos adicionales de los logs de otros equipos y dispositivos de la red (como, por ejemplo, los cortafuegos o los IDS) para llevar a cabo un análisis más completo de estos registros de actividad.

En relación con los ficheros incluidos en la copia del disco o discos del sistema, conviene realizar las siguientes tareas:

- Identificación 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.
- Visualización del contenido de los ficheros gráficos.
- Estudio 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. Hay que tener en cuenta la fecha y hora del sistema en el momento de obtener las evidencias.
- Revisión de los permisos de acceso y ejecución de los ficheros, así como de la información sobre quiénes son sus propietarios.
- Revisión de 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), spooler de impresión, etcétera.

La tarea de análisis de los ficheros se puede ver dificultada por el hecho de que algunos de estos ficheros se encuentren comprimidos y/o cifrados (en este último caso resultará mucho más difícil el análisis si se ha utilizado un algoritmo de cifrado robusto).

Del mismo modo, será difícil localizar y analizar los ficheros ocultos mediante distintas técnicas dentro del sistema:

- 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). No obstante, este mecanismo puede ser empleado por un intruso para ocultar archivos asociados a otros sin que sean detectados por el administrador del sistema.

El equipo de análisis forense deberá tener especial cuidado a la hora de localizar aquellos ficheros marcados como borrados en el disco pero que todavía no habían desaparecido de éste, es decir, los sectores que todavía no habían sido asignados a otros ficheros, por lo que formaban parte del free space (espacio libre del disco).

Con las herramientas adecuadas también es posible recuperar fragmentos de antiguos ficheros, además de facilitar el análisis de los datos que pudieran encontrarse en los espacios de separación entre particiones y sectores, así como en el espacio no utilizado dentro de cada sector (slack space).

Procedimiento de recolección

El procedimiento de recolección debe de ser lo más detallado posible, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones.

1. Transparencia

Los métodos utilizados para recolectar evidencias deben de ser transparentes y reproducibles. Se debe estar preparado para reproducir con precisión los métodos usados, y que dichos métodos hayan sido testados por expertos independientes.

2. Pasos

¿Dónde está la evidencia? 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.

El procedimiento de almacenamiento

1. Cadena de custodia

Debe estar claramente documentada y se deben detallar los siguientes puntos:

- ¿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?

En el caso de que la evidencia cambie de custodia indicar cuándo y cómo se realizó el intercambio, incluyendo número de albarán, etc.

2. 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.

Herramientas necesarias

Existen una serie de pautas que deben de ser seguidas a la hora de seleccionar las herramientas con las que se va a llevar a cabo el proceso de recolección:

- 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 (INCIBE, https://www.incibe-cert.es/blog/rfc3227, 2021):
    - Programas para listar y examinar procesos.
    - Programas para examinar el estado del sistema. -
    - Programas para realizar copias bit a bit.

HERRAMIENTAS DE ANÁLISIS FORENSE

Las herramientas de análisis forense permiten asistir al especialista durante el análisis de un delito informático, automatizando buena parte de las tareas descritas en los apartados anteriores para facilitar la captura, preservación y posterior análisis de las evidencias digitales.

Además, se distinguen por su capacidad para trabajar con distintos sistemas de ficheros: FAT y FAT32, NTFS de Windows, Ext2/3 de Linux, HFS de Macintosh, etcétera. De las herramientas de análisis forense disponibles en el mercado podríamos considerar que las más populares serían: EnCase, Autopsy, The Forensic Toolkit, The Sleuth Kit o The Coroner’s Toolkit, entre otras.

Organismos Y Medios Especializados En Informática Forense

Entre los principales organismos internacionales especializados en la Informática Forense destacan la IACIS (International Association of Computer Investigative Specialists) y la IOCE (International Organization on Computer Evidence). La IACIS (Asociación Internacional de Especialistas en Investigación Informática) es una organización sin ánimo de lucro dedicada a la formación de los profesionales de la ley en el área del análisis informático forense (www.iacis.com).

Por su parte, la IOCE (Organización Internacional sobre las Evidencias Informáticas) es un organismo creado en 1995 para constituir un foro en el que las agencias de ley de todo el mundo pudieran intercambiar información sobre el análisis forense informático (www.ioce.org).

- 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/.

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.

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.

