INSTITUTO NACIONAL DE CIBERSEGURIDAD

ANÁLISIS FORENSE DIGITAL

Unidad 1 - Introducción

INDICE

1. El proceso de investigación.
2. Pruebas y evidencias.
3. Legislación en materia de evidencias digitales.
4. Las preguntas a responder por el análisis forense.
5. Los dos enfoques, pericial y el de respuesta ante incidentes, enfocado a la mejora de la seguridad.
6. El flujo de trabajo en la gestión de incidentes.

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

universidad de león

SAPROMIL

MINISTERIO DE DEFENSA

UNIDAD 1 - INTRODUCCIÓN

1. El proceso de investigación.

❑¿En qué consiste?

Las actividad forense se centra en tres ejes:

I. Determinación, adquisición y preservación de evidencias para su posterior análisis, incluso para ser aportadas en procesos judiciales.

II. Análisis de evidencias dando lugar a conclusiones o hallazgos que se soportan de forma objetiva en las evidencias obtenidas.

III. Elaboración del informe forense o dictamen pericial, que es el trabajo entregable del perito forense. En él se recogen minuciosamente todos los detalles de las evidencias, su adquisición, análisis y las conclusiones y es usado para la evaluación del caso así como para aportar en procesos judiciales.

✓ La actividad forense está guiada por el rigor, la objetividad y la minuciosidad en los pasos dados y la documentación de cada uno de ellos.

✓ Como ciencia que es, plantea hipótesis cuya validez o invalidez demuestra mediante la obtención de pruebas.

UNIDAD 1 - INTRODUCCIÓN

2. Pruebas y evidencias.

❑Evidencias en el análisis forense digital

- ✓ Las evidencias, en general, son aquellas pruebas encontradas en relación a unos hechos que nos permiten dar veracidad a las afirmaciones sobre esos hechos.
- ✓ El análisis forense digital se sustenta sobre evidencias digitales principalmente, y también sobre evidencias de tipo físico, como son fotografías del lugar de los hechos, de dispositivos, del conexionado de estos y de sus periféricos.
- ✓ Por Evidencia Digital nos referimos al valor probatorio que tiene cualquier información almacenada o transmitida en/por un dispositivo. Es decir, las evidencias se obtienen durante el análisis de la información adquirida durante una investigación forense.
- ✓ Dado el valor probatorio en procesos legales de las evidencias, la gestión de estas para garantizar su validez y admisión en un juicio deben de cumplir un proceso determinado.
- ✓ El principio que debe guiar cualquier procedimiento de obtención de evidencias es que “partiendo de la misma información, repitiendo los pasos que se detallen en el procedimiento, se obtienen los mismos resultados”.

Por lo tanto, es importante SIEMPRE:

- ✓ Disponer de, al menos, una copia de la información original, para repetir el proceso.
- ✓ Disponer de mecanismos de comprobación de integridad en cada paso.
- ✓ Detallar los pasos realizados para obtener la conclusión, con nivel de detalle que indique herramientas, versiones y procedimientos concretos.

UNIDAD 1 - INTRODUCCIÓN

2. Pruebas y evidencias.

❑Ciclo de vida de la evidencia digital

UNIDAD 1 - INTRODUCCIÓN

2. Pruebas y evidencias.

❑Cadena de custodia, CdC

- ✓ Se trata del procedimiento que refleja todas y cada una de las actuaciones de recogida, traslado, proceso o conservación llevadas a cabo sobre una evidencia, desde su adquisición hasta su presentación en un tribunal. El objetivo es garantizar la integridad de estas evidencias a lo largo del proceso mediante la trazabilidad de estas acciones y las personas que las llevan a cabo.
- ✓ La CdC se implementa mediante un documento asociado a la evidencia, en la que consta la identificación de esta desde el momento de la adquisición y el resto de actuaciones.
- ✓ En la adquisición se recoge la siguiente información:
  - Identificador único de la evidencia.
  - Cuando, dónde y por quién.
  - Anotaciones relevantes para la investigación.

Además, para cada actuación después de la adquisición:

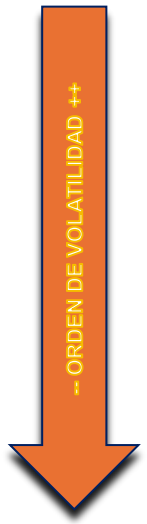
- Quién, cuándo y dónde se llevo a cabo la actuación, así como para qué.

UNIDAD 1 - INTRODUCCIÓN

2. Pruebas y evidencias.

❑Orden de volatilidad de las evidencias

Entendemos por volátiles aquellas evidencias digitales que se perderán ante un corte de corriente o reinicio de un SSOO. Priorizaremos en orden de mayor a menor volatilidad:



- ✓ Registros del procesador y cache.
- ✓ Memoria RAM total de la máquina o de uno o varios procesos. La adquirimos con herramientas que modifiquen lo mínimo de esta memoria.
- ✓ Ficheros temporales, fichero de paginación, conexiones de red, usuarios actuales, ficheros abiertos, hora del sistema. Nos lo llevamos con herramientas del SSOO. Ojo con la integridad de estas.
- ✓ Archivos del sistema o sistemas de ficheros del disco.

UNIDAD 1 - INTRODUCCIÓN

2. Pruebas y evidencias.

❑Tipos de adquisición

- ✓ La adquisición es un proceso complejo, dependiente de los dispositivos implicados, SSOO, discos, hw y del caso.
- ✓ La adquisición tradicional, la enfocada a los procesos judiciales, se ha venido realizando de forma completa y “en frío”, es decir, se realiza una copia forense de un sistema apagado, garantizando su validez legal, para ser analizada posteriormente.
- ✓ Actualmente es cada vez más difícil este enfoque, debido a:

  - Los tamaños de los dispositivos involucrados
  - El alto número de equipos afectados en un incidente
  - La lentitud del proceso tradicional

- ✓ Este escenario viene cambiando en el campo de DFIR, dónde se necesitan realizar varias adquisiciones y análisis en tiempos mínimos para poder tomar decisiones en el momento de la respuesta al incidente. Aquí es habitual el uso de técnicas de adquisición parcial “en caliente” para su inmediato análisis o triaje.
- ✓ Las evidencias adquiridas con estas últimas técnicas ya se admiten en los procesos judiciales, si bien hay que aportar las mismas garantías de integridad que en el proceso tradicional.

UNIDAD 1 - INTRODUCCIÓN

2. Pruebas y evidencias.

❑Proceso forense

Primera intervención

Las actuaciones según se llega a “escena del crimen” son fundamentales:

- ✓ Asegurar el área.
- ✓ Toma de datos de contexto, croquis, fotos 360º, pantalla y entrevistas.
- ✓ Determinar los dispositivos de los que se van tomar evidencias o incautar.
- ✓ En función del tipo de incidente, se podrá desconectar el cable de red para detener un incidente que está ocurriendo en ese momento.

Si un equipo está encendido, se deja encendido.
Si un equipo está apagado, no se enciende.

UNIDAD 1 - INTRODUCCIÓN

2. Pruebas y evidencias.

❑Distribuciones específicas para el campo del análisis forense.

Disponemos de múltiples distribuciones para las distintas ramas de la seguridad informática. Las distribuciones específicas para forense disponen de:

- ✓ Prevención de modificación de datos, montando todos los sistemas de ficheros en RO.
- ✓ Herramientas de adquisición de evidencias, como software de clonado de disco con control de errores y verificación, así como soporte de los formatos forenses.
- ✓ Herramientas de análisis de evidencias.
- ✓ Herramientas para documentar las evidencias y el caso.

SIFT

- ❑ PALADIN. Una distribución muy difundida y mantenida por la empresa de herramientas forenses, SUMURI. Se puede descargar de forma gratuita previo registro, de https://sumuri.com/software/paladin/
- ❑ SIFT, Distribución de SANS Institute. Una de las instituciones que ofrece formación en ciberseguridad de mayor reputación a nivel mundial. Basada en Ubuntu, dispone de infinidad de utilidades para el acceso a sistemas de ficheros y artifacts como las instantáneas. Se puede descargar de forma gratuita desde https://digital-forensics.sans.org/community/downloads.
- ❑ CAINE es un proyecto completamente Opensource, que mantiene una evolución constante. Muy usado en entornos profesionales para análisis forense. Se puede descargar desde la página del proyecto, https://www.caine-live.net/

UNIDAD 1 - INTRODUCCIÓN

3. Legislación en materia de evidencias digitales

❑Normativa de referencia

- ✓ En España, el reconocimiento de las evidencias digitales como fuentes de prueba, se recoge en la Ley de Enjuiciamiento Civil, artículos 299 a 386.
- ✓ Asimismo, la recogida y tratamiento de evidencias digitales se recoge dentro de las siguientes normativas:

  - RFC 3227, Directrices para la recopilación y almacenamiento de evidencias digitales.

  - ISO/IEC 27037:2016. Directrices para la identificación, recogida, adquisición y preservación de evidencias digitales.

Actividad: Leer artículo https://www.incibe-cert.es/blog/rfc3227

UNIDAD 1 - INTRODUCCIÓN

4. Las preguntas a responder por el análisis forense

❑Análisis Forense Digital

Consiste en el conjunto de técnicas aplicadas una vez se ha producido un incidente de seguridad, con o sin quebranto de la ley. Básicamente, su fin es responder a las siguientes preguntas:

- ✓ ¿Qué sistemas se han visto afectados?. Esta pregunta hace relación al alcance, es básico saber hasta dónde ha llegado el ataque y conocer que sistemas y datos se han podido ver afectados.
- ✓ ¿Cómo se ha producido el ataque?. Responder a esta pregunta es fundamental para poder corregir la vulnerabilidad o vulnerabilidades explotadas por el atacante para conseguir su objetivo. Es importante reflejar aquí que las técnicas no siempre están relacionadas con un ataque, sino que pueden ser usadas para confirmar que se ha llevado a acabo una determinada acción.
- ✓ ¿Cuándo ha tenido lugar la acción?. Situar temporalmente los acontecimientos es básico en el análisis forense, lo que se suele reflejar mediante una línea de tiempo de los hechos de estudio.
- ✓ ¿Quién ha llevado a cabo la acción?. En casos de ataques de ciberdelincuentes, es realmente complicado concluir una identidad, pero se trata de recoger indicadores que nos permitan apuntar en la dirección de una persona/entidad bien para identificar o bien que permitan continuar la investigación fuera de nuestro alcance. (Operadores de telecomunicaciones, otras empresas o países)

UNIDAD 1 - INTRODUCCIÓN

5. Los distintos enfoques del análisis forense digital

❑Enfoque pericial VS enfoque IR

Las técnicas de análisis forense las preguntas son únicas en los dos casos. Si bien, si el caso está o puede acabar judicializado, conviene:

- ✓ Extremar el detalle en la adquisición.
- ✓ Cálculo de hashes em todo lo adquirido, de forma que permita comprobar la integridad de la prueba en cualquier momento del proceso de investigación.
- ✓ Dejar constancia del proceso y resultado preferentemente con notario y en su defecto, testigos.
- ✓ Cuidar y documentar la cadena de custodia.
- ✓ Ser escrupuloso con la preservación de la intimidad y con la legislación de protección de datos vigente.

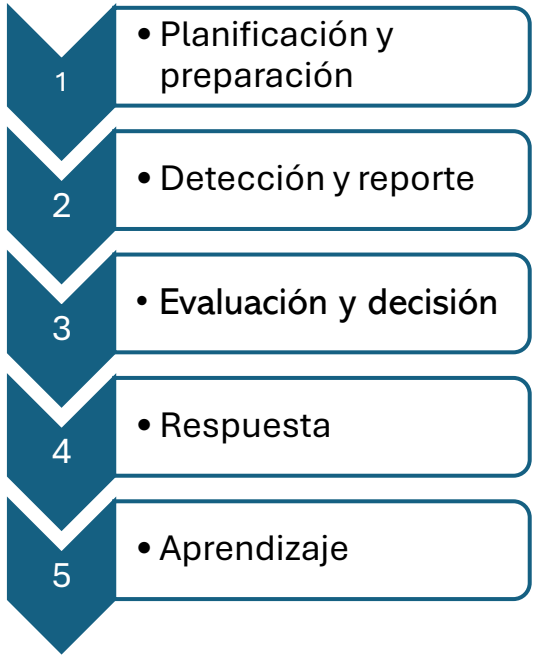
En los casos enfocados a la respuesta ante incidentes:

- ✓ Utilizar técnicas de adquisición y o análisis “live” , primando los tiempos de respuesta.
- ✓ Búsqueda de causa raíz del incidente, para evitar su repetición.
- ✓ Iteración del proceso según se va ampliando el alcance del incidente.

6. El flujo de trabajo en la gestión de incidentes

❑Metodología de gestión de incidentes

- ✓ Si bien en su origen son técnicas usadas por fuerzas y cuerpos de seguridad en búsqueda de culpable, su aplicación en el campo digital es mucho más extensa.
- ✓ En la gestión de incidentes, las técnicas forenses se usan principalmente en la detección y en la evaluación, siendo necesarias para determinar el alcance de un incidente
- ✓ También son necesarias en la determinación de los indicadores de compromiso, en la fase de aprendizaje, al aportar detalles del suceso y finalmente, para responder a las preguntas planteadas.
- ✓ Cada vez está más integrado en la gestión de incidentes, de manera que ha dado fruto al término DFIR, Digital Forensic and Incident Response.
- ✓ Las técnicas de análisis forense son útiles en el día a día de un técnico de sistemas, ya que le habilita a llevar a cabo investigaciones rigurosas y metodológicas sobre sucesos en la red, pudiendo adquirir evidencias en forma tal que puedan ser usadas posteriormente de ser necesario.



Fases de la gestión según la ISO/IEC 27035-1:2016

FIN UNIDAD

Unidad 1

INSTITUTO NACIONAL DE CIBERSEGURIDAD