APUNTES 01

APLICACIÓN DE METODOLOGÍAS DE ANÁLISIS FORENSES

ANÁLISIS FORENSE INFORMÁTICO

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

Esta unidad trata de:

- Introducción al Análisis Forense Informático
- Identificar los dispositivos a analizar para garantizar la preservación de evidencias.
- Utilizar los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.
- Asegurar la escena y conservación de la cadena de custodia.
- Documentar el proceso realizado de manera metódica.
- Considerar la línea temporal de las evidencias.
- Elaborar un informe de conclusiones a nivel técnico y ejecutivo.
- Presentar y exponer las conclusiones del análisis forense realizado.

1. ANÁLISIS FORENSE INFORMÁTICO

Metodología y los distintos objetivos de cada fase y lo que un buen análisis forense debe cubrir

Análisis Forense Informático: conjunto de técnicas y procedimientos para extraer evidencias forenses de distintos soportes digitales sin alterar su estado. En una sociedad tecnológica, dónde se ha producido un importante proceso de transformación digital en el ámbito empresarial y a nivel del invidividual, cada vez es más necesario poder extraer evidencias de los medios digitales, ya sea por un requerimiento judicial o por la respuesta ante un ciber incidente.

En muchos ámbitos se ha cambiado de paradigma debido a la transformación digital, antes todo era físico y no había presencia digital, ahora lo digital tiene más representación que lo propiamente físico. Uno de estos ámbitos ha sido el de los delitos, la mayoría de delitos tienen una componente digital (ordenadores, móviles, aplicaciones, comunicaciones, llamadas, correos electrónicos, etc.) El análisis forense ha cobrado especial importancia debido al auge que ha sufrido la sociedad y su transformación tecnológica.

El objetivo de un analista forense es poder contar una historia de lo que ha sucedido, aportando las evidencias que sustentan los hechos de la historia. Para poder realizar éste proceso deberemos poder contestar una serie de preguntas que serán de vital importancia dentro de una investigación forense.
Dentro de los análisis forenses distinguimos dos escenarios, uno más centrado en los aspectos legales y otro en los tiempos de respuesta y mitigaciones:

- Forense dentro de un proceso judicial: es un proceso minucioso de recolección, procesamiento, documentación y cadena de custodia de las evidencias, deben ser auditables y verificables. Este proceso adquiere una especial relevancia puesto que su objetivo es ser presentables a nivel judicial. También requerirá de figuras importantes como notarios que certifiquen el proceso que estamos siguiendo.
- Forense dentro de la respuesta a un ciber incidente: se busca analizar de forma rápida las evidencias para entender la motivación del ataque, cuándo ha sucedido y qué información nos han robado. Con el objetivo de dar una respuesta y mitigar la amenaza cuanto antes.

Ambos tipos de forense no son excluyentes, ya que muchas veces en la respuesta ante un ciber ataque es posible que tengamos que presentar los resultados en un proceso judicial. Por norma general un análisis forense que va a ser llevado ante un proceso judicial requerirá de más tiempo, porque debe haber una figura (notario) que certifique lo que el analista forense está realizando.

1.1. OBJETIVOS Y FASES

El objetivo fundamental de un análisis forense es poder responder las preguntas claves, “las 5 Ws”, así como aportar las evidencias que sustentan las respuestas a esas preguntas.

- What ¿Qué ha pasado?
- Where ¿Dónde han sucedido los hechos? ¿En qué sistemas o redes?
- Who ¿Quién es el/ los responsables? Personas involucradas, dentro o fuera de la red/empresa
- When ¿Cuándo han sucedido los hechos? Fecha, hora y duración
- Why ¿Por qué y cómo ha sucedido? Motivación y herramientas utilizadas

El proceso de análisis forense se divide en 5 fases, siendo las dos primeras de vital importancia ya que condicionarán todo el proceso y afectarán al resultado final.

1. Identificación
2. Adquisición
3. Preservación
4. Análisis
5. Presentación

1.2. METODOLOGÍA

La metodología seguida en un proceso forense, debe ser minuciosa y debe respetar una serie de características (trabajar pruebas fehacientes y presentarlas de forma clara) si queremos que sea válida en una investigación dentro de un proceso judicial. Ya que la parte contraría, querrá poner en cuestión la metodología seguida.
Características a cumplir en un proceso forense:
Verificable:

- Se debe poder comprobar la veracidad de las conclusiones extraídas a partir de la realización del análisis.
- El proceso seguido debe ser fiable, tratando hechos y datos de carácter objetivo.

Reproducible:

- Se deben poder reproducir las pruebas realizadas durante el proceso.
- Otro analista o perito forense debería de poder llegar a las mismas conclusiones.

Documentado:

- El proceso debe estar correctamente documentado y debe realizarse de manera comprensible y detallada.
- Aportar la máxima información del proceso, de cómo se ha procesado una evidencia o cómo se ha hecho el análisis, más completo será nuestro informe y tendrá más validez ante un proceso judicial.

Independiente:

- Las conclusiones obtenidas deben ser las mismas, independientemente de la persona que realice el proceso y de la metodología utilizada.
- La objetividad y los hechos contrastados deben de ser básicos en nuestro informe.

1.3. IDENTIFICACIÓN

Uno de los puntos clave es poder dictaminar qué dispositivos o elementos son susceptibles de ser analizados a nivel forense para extraer evidencias, podemos encontrar dispositivos físicos (discos duros, portátiles, teléfonos móviles) o dispositivos lógicos (ficheros, imágenes, etc).
Cuando accedemos a una escenario forense, se debe identificar de forma minuciosa qué fuentes de información tenemos disponibles, este punto es de vital importancia para que no haya evidencias que se queden fuera de la investigación. Pasos:

1. Observar el entorno de forma minuciosa.
2. Anotar cualquier elemento, físico o lógico que pueda aportar algo de información.
3. Verificar si esa fuente de información aporta visibilidad para responder algunas de las preguntas.

Por lo tanto, deberemos tomar nota en nuestro registro de todas las fuentes de información disponibles dentro del entorno, para poder tenerlas controladas. Dentro de las fuentes de información más comunes en una investigación forense:

- Dispositivos físicos: sobremesa, portátiles, discos duros, almacenamiento externo, móviles…
- Fuentes lógicas: ficheros, tabla de procesos, contenido memoria RAM, papelera de reciclaje

Hay que tener en cuenta que en entornos cloud, tendremos que descargar los artefactos o las máquinas a analizar desde el proveedor de cloud donde estén estos servicios.

1.4. ADQUISICIÓN, PRESERVACIÓN Y CADENA DE CUSTODIA

El objetivo principal de la adquisición es conseguir una copia lo más fiel posible de la información original, garantizando que no se modifica el estado del dispositivo (o se hace de forma mínima, controlada y documentada). Las fuentes de información tienen un tiempo de vida determinado por su naturaleza, (no es lo mismo una memoria RAM, disponible con el ordenador encendido, que la información de un USB). En esta fase trabajamos priorizando las fuentes de información que tienen un índice de volatilidad mayor.
El orden de volatilidad es la prioridad en que las fuentes de información deben de ser adquiridas, desde las más volátiles, que pueden desaparecer más rápido, a las menos volátiles.
Orden de volatilidad de forma general:

1.- Cachés de memoria, registros CPU
2.- Memoria RAM, Tabla ARP, tabla de procesos, swap, ficheros temporales
3.- Discos duros
4.- Configuraciones físicas, topologías de red

El proceso de preservación de una evidencia es fundamental, si no se sigue correctamente pueden ser impugnadas en un proceso judicial por la parte contraria no admitiendose los resultados del análisis.

Para garantizar todo el proceso de adquisición de evidencias, así como el cambio de manos que puede seguir una evidencia forense durante la investigación y proceso judicial, surge la cadena de custodia. El objetivo de la cadena de custodia es garantizar la exacta identidad de lo incautado y de lo analizado.
Cada persona que tiene contacto con la evidencia, se convierte en una parte de la cadena que garantiza su resguardo. Se permite así comprobar la trazabilidad que siguen las evidencias, las condiciones adoptadas para su salvaguarda y las personas encargadas de su custodia.
Para examinar adecuadamente si se ha producido una ruptura relevante de la cadena de custodia no es suficiente con el planteamiento de dudas de carácter genérico, es necesario precisar en qué momentos, a causa de qué actuaciones y en qué medida se ha producido tal interrupción.
En una cadena de custodia hay varios elementos mínimos que deben quedar reflejados:

1.- Identificación unívoca de las evidencias (marca, modelo, capacidad, número de serie)
2.- Preservación de la evidencia
3.- Marcado de tiempo (timestamp) de cuándo se recoge y quien recoge la evidencia
4.- Localización física de la evidencia y quien se hace responsable de ella en ese momento
5.- Documentación y registros de control, el debate es sobre la fiabilidad de la prueba, no en su validez.

Autoevaluación
¿Cuál de las siguientes fuentes de información deberían de recolectarse antes en un análisis forense?

A) Disco externo USB
B) Memoria RAM del ordenador
C) CD-ROM
D) Fichero dentro del ordenador

a) Incorrecto. Un disco externo mediante USB es una fuente de información poco volátil
B) Opción correcta. La memoria RAM es uno de los registros más volátiles ya que su contenido desaparece si el Ordenador es reiniciado o deja de tener corriente eléctrica
C) Incorrecto. Un CD-ROM es una fuente de información poco volátil
d) Incorrecto. Un fichero dentro del ordenador es una información volátil pero menos volátil que la memoria RAM del ordenador

1.5. HERRAMIENTAS NECESARIAS

Los analistas forenses suelen llevar consigo un maletín de trabajo con sus herramientas, tanto físicas como a nivel de software para poder extraer evidencias y material para poder transportarlas y conservarlas sin que se vean alteradas Contenidos tradicionales de un maletín de herramientas forenses:

- Hardware forense para clonar el discos con distintas interfaces (ATA, SATA, IDE, PCI, SCSI, USB, Firewire, etc)
- Cables para conectar cualquier disco o periférico
- Protectores de escritura o write blockers para prevenir modificaciones en la evidencia mientras se copia

- Juego de destornilladores
- Software para extracción de evidencias lógicas
- Herramientas para análisis de logs
- Material para almacenamiento y conservación de evidencias (tanto a nivel físico como lógico)

Respecto al análisis de evidencias, mostramos algunas de las herramientas más comunes de procesado según el tipo de evidencias:

Análisis de memoria RAM: Volatility
Análisis de discos: EnCase, FTK suite, MagnetForensics Suite
Análisis de dispositivos móviles: Cellebrite
Suites de herramientas: SIFT (SANS)

Debes conocer
Cuando analizamos información de sistemas o entornos Cloud, normalmente trabajaremos con ficheros de log, donde se registran todos los sucesos que se han producido para un sistema o aplicativo.
Dicho fichero tiene el timestamp o marca de tiempo, que indica la fecha exacta en la que ha sucedido ese hecho.
Un investigador forense debe saber cómo trabajar estos ficheros para poder extraer y relacionar la información.
Las herramientas más usadas para esta tarea son:

- Hojas de cálculo
- Herramientas de consola
    - cut, grep, etc en entornos Unix
    - powershell en entornos Windows
- SIEMs para indexado de gran cantidad de información (e.g Splunk)
- Herramientas procesado logs: greylog, goaccess

1.6. REPORTE

Los resultados se recogen en el informe forense, dicho informe tiene dos partes o ámbitos bien diferenciados:

1.- Resumen ejecutivo: presentamos los resultados y conclusiones más importantes de nuestro análisis a alto nivel. Se busca, sin entrar en detalles técnicos, saber las principales conclusiones de nuestro análisis forense

2.- Desglose técnico de nuestro trabajo: dónde se muestra todo el proceso a bajo nivel y detallado de todo nuestro trabajo, de cada una de las fases (evidencias identificadas, su análisis, qué hemos encontrado, cuales son nuestras conclusiones y porqué).

Uno de los puntos clave de todo el proceso de comunicación y reporte de nuestro trabajo es poder explicar la cronología de lo que ha sucedido. A nivel forense ésta cronología se llama línea de tiempo, o timeline y es uno de los puntos clave. Todo hecho tiene un momento y necesitamos trasladar una visión ordenada de los mismos. Además a nivel de investigación entender cuando han sucedido las cosas y en qué orden es clave puesto que aporta una visión clara de cómo han sucedido, pudiendo aportar incluso información sobre la motivación del incidente.

TEST

1- Dentro del análisis forense podemos encontrar dos escenarios, dependiendo si el caso será llevado ante un proceso judicial.
   a) Verdadero
   b) Falso

2- En una investigación forense deberemos de reflejar en qué sistemas ha sucedido el ataque.
   a) Verdadero
   b) Falso

3- Necesitaremos de herramientas específicas tanto físicas como lógicas en el análisis forense.
   a) Verdadero
   b) Falso

4- El objetivo de un analista forense es poder contar la historia que ha sucedido.
   a) Verdadero
   b) Falso

5- Un forense a nivel informático tiene mucha de la base de los forenses tradicionales (metodología, preguntas a responder, etc.).
   a) Verdadero
   b) Falso

6- ¿Qué deberemos hacer como prioridad de la fase de identificación?
   a) Someter a una verificación exhaustiva todas las evidencias.
   b) Saber que miembros del equipo trabajarán con nosotros.
   c) Eliminar cualquier elemento que pudiera distraernos.
   d) Anotar las fuentes de información que pudiéramos considerar interesantes.

7- En una investigación forense deberemos de responder las siguientes preguntas:
   a) ¿Qué ha sucedido?
   b) Todas las anteriores
   c) ¿Dónde ha sucedido?
   d) ¿Qué motivación había?

8- ¿Qué elementos mínimos debe de tener el documento de cadena de custodia? (Multirespuesta)
   a) Código fuente.
   b) Línea de tiempo.
   c) Identificación unívoca.
   d) Registro de control.

9- Los analistas forenses suelen llevar sus herramientas lógicas en portátiles o discos externos.
   a) Verdadero
   b) Falso

10- ¿Qué significa DFIR?
   a) Digital Forensic Investigation and Response.
   b) Decimated Forensic Investigation and Response.
   c) Digital Forensic and Incident Response.
   d) Decimated forensic Investigation and Response.

Respuestas:

1. a), 2. a), 3. a), 4. a), 5. a), 6. d), 7. b), 8. b), c), d), 9. a), 10. c)