Introducción al Análisis Forense Informático.

Caso práctico

María es una joven analista forense que se incorpora a un equipo de respuesta ante incidentes informático, DFIR (Digital Forensics and Incident Reponse). En su primer caso acude con su maletín de herramientas forenses a casa de un sospechoso de haber realizado un ataque informático.

En su primer caso le asignan la investigación forense de un ciber ataque perpetrado supuestamente por un atacante contra una entidad financiera, robando una importante cantidad de dinero y provocado que varios sistemas internos dejarán de funcionar.

Pixabay. *Mano Lupa* (Dominio público)

Ella, aún si haberse puesto a trabajar en el caso, sabe que debe contestar a varias preguntas clave

- ¿Qué ha sucedido realmente? ¿ha sido un atacante desde fuera o alguien desde dentro?
- ¿Dónde ha sucedido? ¿En qué sistemas o redes?
- ¿Quienes son los responsables del ataque?
- ¿Cual ha sido la fecha y hora exacta del ataque? ¿Cuánto ha durado?
- ¿Qué motivación tenía el atacante? ¿Qué herramientas ha usado?

En esta unidad el alumno aprenderá:

1.- Identificar los dispositivos a analizar para garantizar la preservación de evidencias.

2.- Utilizar los mecanismos y las herramientas adecuadas para la adquisición y extracción de las evidencias.

3.- Asegurar la escena y conservación de la cadena de custodia.

4.- Documentar el proceso realizado de manera metódica.

5.- Considerar la línea temporal de las evidencias.

6.- Elaborar un informe de conclusiones a nivel técnico y ejecutivo.

7.- Presentar y exponer las conclusiones del análisis forense realizado.

1.- Análisis Forense Informático.

Caso práctico

Pixabay (Dominio público)

María es una joven analista forense que se incorpora a un equipo de respuesta a incidentes informáticos.

Antes de entrar en temas técnicos repasa la metodología y los distintos objetivos de cada fase para garantizar que no se deja nada y cubre todo lo que un buen análisis forense debe cubrir.

Definimos el Análisis Forense Informático como todo el conjunto de técnicas y procedimientos para extraer, sin alterar su estado, evidencias forenses de distintos soportes digitales. En una sociedad eminentemente tecnológica, dónde se ha producido un importante proceso de transformación digital tanto en el ámbito empresarial, como a nivel del invididual 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.

Pixabay. (Dominio público)

La transformación digital ha derivado que en muchos ámbitos se ha cambiado de paradigma, donde antes todo era físico y no había presencia digital a un mundo donde lo digital tiene a veces 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 -y sus aplicaciones-, comunicaciones, llamadas, correos electrónicos, etc) debido a este auge que ha sufrido la sociedad y su transformación tecnológica, el análisis forense ha cobrado especial importancia.

El principal objetivo de un analista forense no es más que la de 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 que podremos encontrarnos distinguiríamos dos escenarios, uno mas centrado en los aspectos legales y otro en los tiempos de respuesta y mitigaciones:

1.- **Forense dentro de un proceso judicial:** dónde el procesamiento, documentación y cadena de custodia de las evidencias adquiere una especial relevancia puesto que su objetivo es ser presentables a nivel judicial. También requerirá de otro figuras importantes como notarios que certifiquen el proceso que estamos siguiendo.
2.- **Forense dentro de la respuesta a un ciber incidente:** donde se busca analizar de forma rápida las evidencias para así poder entender mejor la motivación del ataque, cuándo ha sucedido y que información nos han robado.

Ambos tipos de forense no son excluyentes, ya que muchas veces en la respuesta ante un ciber ataque es posible que tengamos que presentar nuestros resultados en un proceso judicial. Por norma general un forense que va a ser llevado ante un proceso judicial requerirá

de más tiempo, puesto que tiene que haber una figura (notario) que certifique todo lo que el analista forense está realizando.

Caso práctico

María, sabe que a día de hoy dentro de lo que se conoce cómo el análisis forense puede tener dos escenarios bien distintos. Uno con la respuesta ante ciber incidentes que salen todos los días en los medios de comunicación (por ejemplo casos de ataque de ***ransomware***) y otro en investigaciones que van a ir a un proceso judicial (que también puede ser debido a un ciber incidente).

El proceso judicial necesita que todas las evidencias, así como su proceso de recolección esté documentado, sea auditable y verificable y por tanto los tiempos de ejecución son distintos. Mientras que en un ciber incidente la prioridad es poder mitigar la amenaza cuanto antes siendo raro el escenario en el que se llega luego a un juicio.

Por tanto María sabe que debe estar preparada ante ambos escenarios, desde una respuesta rápida hasta un proceso minucioso de preparación, presentación y cadena de custodia de las evidencias

1.1.- Objetivos y fases.

Pixabay (Dominio público)

Como comentábamos el objetivo fundamental es poder responder varias preguntas claves, lo que se denomina como "las 5 Ws" (W de "What/Where/Who/When/Why en inglés), así como aportar las evidencias fehacientes que sustentan las respuestas a esas preguntas. Las preguntas son:

1.- **¿Qué ha pasado?**
2.- **¿Dónde han sucedido los hechos?**
3.- **¿Quién está involucrado?**
4.- **¿Cuándo han sucedido los hechos?**
5.- **¿Por qué y cómo ha sucedido?**

El proceso de análisis forense puede dividirse en 5 fases bien diferenciadas, siendo las dos primeras (identificación y adquisición) de vital importancia ya que condicionarán todo el proceso y afectarán de forma notable al resultado final.

1.- **Identificación**
2.- **Adquisición**
3.- **Preservación**

4.- **Análisis**
5.- **Presentación**

1.2.- Metodología.

Pixabay (Dominio público)

La metodología seguida para un proceso de análisis forense, debe ser minuciosa y respetar una serie de características si queremos que sea válida en una investigación y dentro de un proceso judicial llegado el caso.

Este punto es de vital importancia, puesto que en un proceso judicial la parte contraría es probable que quiera poner en cuestión la metodología que hemos seguido en nuestro trabajo. Por eso debemos de ser minuciosos, trabajar con hechos y pruebas fehacientes y presentarlas de forma clara. A nivel general nuestro proceso forense debe de cumplir las siguientes características:

Verificable:

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

Reproducible:

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

Documentado:

- Todo el proceso debe estar correctamente documentado y debe realizarse de manera comprensible y detallada.
- Cuanta mas información podamos aportar al proceso de cómo hemos procesado una evidencia o cómo se ha hecho el proceso de análisis mas completo será nuestro informe y mas validez tenga 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.

Para saber más

A nivel metodológico y normativo tenemos varias guías de referencia que pueden ayudarnos a entender cómo debe de hacerse de forma correcta el análisis forense y aportar una guía de buenas prácticas, algunos ejemplos son

- UNE-EN ISO/IEC 27037:2016
- UNE 71506:2013
- Electronic Crime Scene Investigation

1.3.- Identificación.

Uno de los puntos clave dentro de una investigación forense es poder dictaminar qué dispositivos o elementos son susceptibles de ser analizados a nivel forense para extraer evidencias, a este respecto podremos encontrar dispositivos físicos (discos duros, portátiles, teléfonos móviles) como dispositivos lógicos (ficheros, imágenes, etc).

Cuando accedemos a una escenario forense, deberemos de trabajar el escenario, es decir deberemos tomar nuestro tiempo en identificar de forma minuciosa qué fuentes de información tenemos disponibles, éste punto es de vital importancia para que no haya una posible evidencia que se quede fuera de la investigación. ¿Cómo hacerlo?

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 en responder algunas de las preguntas que tenemos que responder

Por lo tanto deberemos tomar nota de todas las fuentes de información disponibles dentro del entorno, anotándolas en nuestros registros para así poder tenerlas controladas.

Dentro de las fuentes de información más comunes dentro de una investigación forense tendríamos:

- **Dispositivos físicos**: equipos de sobremesa, portátiles, discos duros, dispositivos de almacenamiento externo, teléfonos móviles, etc
- **Fuentes lógicas**: ficheros, tabla de procesos, contenido memoria RAM, papelera de reciclaje

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

Pixabay (Dominio público)

Citas Para Pensar

"Es imposible que un delincuente actúe, sobre todo teniendo en cuenta la intensidad de un delito, sin dejar rastros de esta presencia". Edmon Locard

1.4.- Adquisición, Preservación y Cadena de Custodia.

Una vez localizadas e identificadas todas las fuentes de información el paso siguiente es la adquisición. El objetivo principal de la adquisición es conseguir una copia lo más fiel posible de la información original, garantizando en todo momento que no se modifica el estado del dispositivo (o que, si se hace, se hace forma mínima, controlada y documentada).

Las fuentes de información tienen un tiempo de vida determinado por su naturaleza, por ejemplo no es lo mismo el contenido de la memoria RAM de un ordenador que solamente estará disponible mientras el ordenador esté encendido que la información contenida en un USB que puede estar disponible durante años sin verse alterada. Es por eso que en la fase de adquisición trabajamos priorizando las fuentes de información que tienen un índice de volatilidad mayor.

Entendemos el orden de volatilidad como la prioridad en que las fuentes de información deben de ser adquiridas, desde las más volátiles, y que por tanto pueden desaparecer mas rápido, a las menos volátiles.

Deforma general podríamos definir el siguiente **orden de volatilidad:**

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**

De la misma forma que se debe de adquirir correctamente, la evidencia tiene que ser preservada. El proceso de preservación de las evidencias es fundamental dentro del análisis forense, ya que si no se sigue correctamente las evidencias podrán ser impugnadas en un proceso judicial por la parte contraria no adminitendose 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, es decir su objetivo es garantizar que lo analizado fue lo mismo que lo recogido.

Cada persona que tiene contacto con la evidencia se convierte en un eslabón garante de 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 sobre la cadena de custodia se centra en la fiabilidad de la prueba. No en el de su validez.

Autoevaluación

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

Sugerencia

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

Un disco externo mediante USB es una fuente de información poco volátil

La memoria RAM es uno de los registros mas volátiles ya que su contenido desaparece si el ordenador es reiniciado o deja de tener corriente eléctrica

Un CD-ROM es una fuente de información poco volátil

Un fichero dentro del ordenador es una información volátil pero menos volátil que la memoria RAM del ordenador

Solución

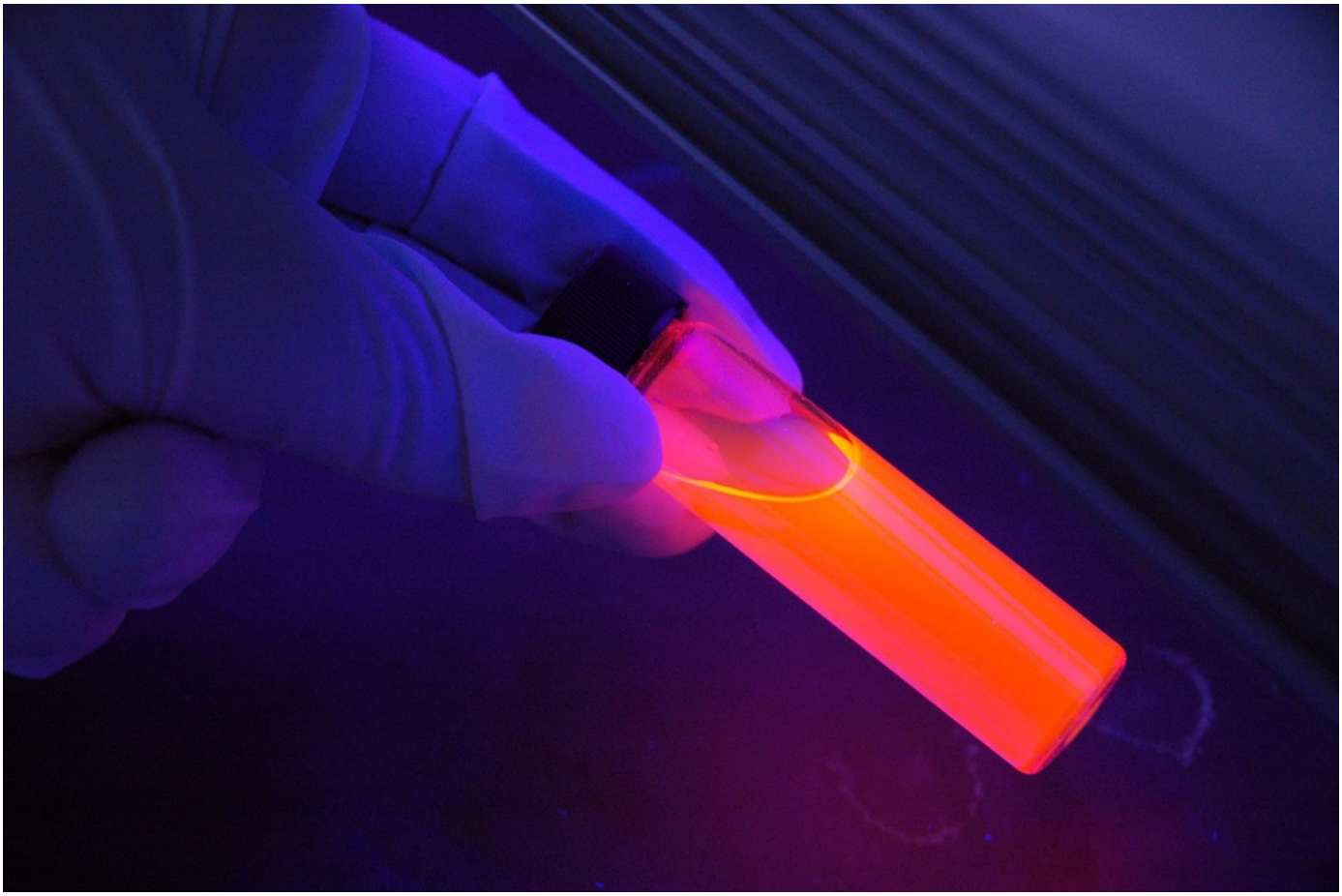
1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

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 dentro de una investigación, así como material para poder transportarlas y conservarlas sin que se vean alteradas, convirtiéndose así en un pequeño laboratorio portátil.

Contenidos tradicionales de un maletín de herramientas forenses:

- Hardware forense para clonado de 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 cualquier modificación de 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)



Pixabay (Dominio público)

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*** es decir un fichero donde se registran todos los sucesos que se han producido para un sistema o aplicativo.

Dicho fichero tiene lo que denominamos ***timestamp*** o marca de tiempo, que marca la fecha exacta (con hora, minuto, segundo) que ha sucedido ese hecho. Para un investigador forense es de vital importancia saber cómo trabajar estos ficheros para así poder extraer y correlar la información.

Las herramientas mas 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.

Como introducíamos al principio es importante poder presentar la información y resultado de nuestro análisis, contestando a las preguntas vitales del incidente en base a los hechos y evidencias obtenidas. Todos nuestros resultados se recogen en nuestro informe forense, dicho informe tiene dos partes o ámbitos bien diferenciados:

1.- **Resumen ejecutivo:** dónde 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.

Por otra parte, el informe debe dar salidas a las 5 preguntas iniciales que comentábamos pero también debe de responder:

- ¿Cuál creemos que ha sido el origen del incidente? ¿Qué lo ha disparado?
- La cronología o **timeline** de los hechos
- Cuales son los hechos y evidencias que sustentan las conclusiones
- ¿Qué actores y qué motivaciones pueden tener?

Pixabay (Dominio público)

Para saber más

En muchos casos, y debido a los cambios regulatorios que ha habido a nivel de protección de datos personales, es necesario reflejar qué datos personales se han comprometido y de qué manera (integridad, confidencialidad y disponibilidad)

Mas info sobre la Ley de Protección de Datos y Derechos Digitales