[AF] Introducción al análisis forense

Esta asignatura se centra en la informática forense (Digital Forensics o Computer Forensics). Esta muy relacionada con respuesta a incidentes, por ello suele ser conocida como DFIR. Se define como el proceso de identificar, preservar, analizar y preservar evidencias de una forma legal y aceptable, en este caso, aplicando técnicas científicas y analíticas especializadas a infraestructura tecnológica.

Principio de Locard

Siempre que dos objetos entran en contacto, transfieren parte del material que incorporan al otro objeto. Por lo que se podría decir que siempre que alguien hace algo, deja un rastro.

Funciones de ámbito o actuación

- Recopilación y preservación de pruebas digitales
- Analizar pruebas digitales
- Recuperar datos
- Investigar incidentes de seguridad
- Analizar redes y comunicaciones
- Creación de informes y testimonios en tribunales
- Asesoría y capacitación
- Investigación y desarrollo

Guías para el proceso de investigación Forense

Existen varios estándares que pueden ser utilizados como guía para realizar un análisis pericial completo.

Normas AENOR

Pueden ser utilizadas en cualquier organización independientemente de su ámbito y tamaño.

- UNE 71505:2013:
  - 71505:2013-1: Vocabulario y principios generales
  - 71505:2013-2: Buenas prácticas en la gestión de las evidencias electrónicas
  - 71505:2013-3: Formatos y mecanismos técnicos
- UNE 71506:2013: Metodología para el análisis forense de las evidencias electrónicas. Hay varias fases: Preservación, Adquisición, Documentación, Análisis y Prentación
- UNE 197010:2015: Criterios para la elaboración de informes periciales.

Normas ISO

- ISO/IEC 27037:2012: Habla de las guias para la identificación, colección adquisición y preservación de pruebas digitales

Normas RFC

- RFC 3227: Guias para la recolección y manejo de evidencias
- RFC 4810: Guias para el archivado de pruebas a largo plazo

Proceso de investigación Forense

Preparación del caso

Es importante realizar una preparación previa para poder adquirir las evidencias correctamente y que todo el proceso sea correcto a nivel legal.

- Contar con permisos adecuados
- Autorización por escrito
- Contrato

Asegurar la escena: Proteger la escena para evitar la modificación o destrucción de las evidencias digitales existentes.

Identificación

Consiste en detecatr y localizar posibles fuentes e evidencia digital. Hya que determinar la fuente de los datos, su ubicación y la relación con el incidente investigado.

Revisión del entorno legal que protege el bien

Se analizan normativas y regulaciones aplicables a la evidencia digital y al bien protegido, asegurando la recolección, adquisición y análisis de los datos se realicen de manera legal y sean admisibles en el proceso legal.

Cadena de custodia

Para garantizar la cadena de custodia es necesario documentar donde, cuando y quien recolectó la evidencia, donde, cuando y quien la manejó, quien la ha custodiado, durante cuanto tiempo y como se ha almacenado y si existe un cambio de custodia en algún momento

Adquisición

Consiste en recopilar las pruebas digitales.

Orden de volatilidad

Hay datos más volátiles que otros, por ejemplo, los que están en memoria, registros y caché son los más volátiles y los que están en un almacenamiento externo serían los más volátiles. Se debe recopilar primero la información más volátil.

Modos de adquisición

- Equipo modo Live: el equipo está encendido. Se quieren recuperar datos volátiles del equipo para analizar. Debe ser muy documentado.
- Equipo modo dead: el equipo se apaga de forma brusca quitando la corriente a machete y se procede a clonar el disco, es la forma recomendada

Clonado

- Copia exacta bit a bit del disco duro, incluyendo errores y sectores defectuosos
- Se busca disponer de una copia sobre la que realizar el análisis sin alterar la prueba

Existen múltiples formas y herramientas

- Software: Proceso muy potente y flexible con multitud de herramientas. El problema es que aumenta la probabilidad de dañar la prueba y es más difícil de justificar el proceso ante un juez
    - Herramientas como dd, dcfldd, dc3dd, FTK imager, Acronis...
        - DD: Para copiar de un disco A a un disco B, se debe determinar el tipo de disco (IDE o SATA) y realizar el clonado con “dd if=/dev/sda of=/dev/sdb”
    - NO SE DEBE MONTAR EL DISCO BAJO NINGÚN CONCEPTO
- Hardware: Se suelen usar clonadoras. Están más limitadas, pero te aseguras que no se monta el disco y que se preserva la prueba tal y como estaba. También es mucho más caro.

Integridad

Hay que asegurar que los datos clonados son copia exacta de los originales, se pueden usar funciones hash como SHA-2 o SHA-3, otras funciones como SHA-1 y MD5 se consideran obsoletas. Esto se puede hacer con muchas herramientas:

- A partir de la imagen clonada, por ejemplo, usando DD y luego SHA-3 desde linux. Se debe tomar el hash de tanto el HDD original como del clonado. Hay mejoras del comando DD que permiten hacer esto directamente. para esto se usa dc3cc con el comando dc3dd if=/devsdb of=/imagen5.img

Preservación

Tratamiento de las evidencias garantizando la cadena de custodia, documentando todos los procedimientos realizados, almacenando la prueba en un sitio seguro con control de accesos. A veces se considera parte de la adquisición

Análisis

Se examinan los datos recopilados para identificar patrones, rastrar actividades delictivas y descubrir información relevante para el caso.

- Recuperación de archivos eliminados
- Recuperación e identificación de e-mails
- Búsqueda de acciones específicas de los usuarios de la máquina
- Búsqueda de archivos específicos
- Recuperación de los últimos sitios visitados, recuperación de caché de navegador.

Herramientas

- Autopsy: solución completa para el análisis de evidencias, puede ser ampliado con plugins. Es multiplataforma. Pensada para equipos grandes, bastante compleja de usar.
- Volatiliry: Análisis forense de memoria, ampliable mediante plugins. Es como Autopsy pero para memoria volátil. Se le pasa un volcado de memoria y deja buscar información sobre procesos, contenido del portapapeles, etc... De la versión 2 a la versión 3 se hace un cambio importante y algunas funcionalidades de la 2 no funcionan correctamente en la 3, pero la 3 automatiza algunas funcionalidades facilitando su uso.
- Cellebrite: Especializada en dispositivos móviles. Es en realidad un producto software, pero se vende preinstalado en unas tablets ruggerizadas. Utiliza herramientas de cracking para obtener datos de un móvil sin manipular sus contenidos. Emite informes sobre los datos obtenidos de un dispositivo móvil. Es muy caro.
- MOBILedit Forensic: Permite realizar análisis forense de smartwatches, algo que el Cellerite no puede hacer.
- EnCase Forensic

Distribuciones para análisis forense

- SIFT (Sans Investigative Forensic Toolkit): Distro basada en ubuntu con multitud de herramientas orientadas al análisis forense. Es proporcionada por el SANS, una organización reputada del sector.
- CAINE (Computer Aided INvestigative Environment): Ofrece entorno seguro con bloqueo automático de escritura para dispositivos conectados a nivel de Kernel.
- Parrot Security OS
- TSURUGI: Recomendada por el profe