Informática forense

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Informática forense

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01

Indice

- ¿Qué es la informática forense?
- El proceso
    1. Identificación
    2. Conservación
    3. Análisis
    4. Exposición

¿Qué es la Informática forense?

Disciplina criminalística

Investigar sistemas informáticos para obtener y procesar información (evidencias digitales):

- Con validez jurídica
- Para la simple investigación privada (accesos no autorizados, sospechas de robos de información, etc.)

¿Qué es la Informática forense?

Trata de responder:

- ¿Qué?
- ¿Quién?
- ¿Cómo?
- ¿Cuándo?
- ¿Por qué?

¿Qué es la Informática forense?

Es utilizada por:

- Agentes de la ley
- Compañías de seguros
- Compañías privadas
- Personas particulares
- …

¿Qué es la Informática forense?

Consiste en:

- Extraer información de un sistema
- Recuperar información cifrada/eliminada/dañada
- Monitorizar el comportamiento de un sistema
- Detectar incumplimientos de las políticas de la empresa
- …

¿Qué es la Informática forense?

Principio de intercambio de Locard:

- "Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto"
- Todas las acciones dejan un rastro

¿Qué es la Informática forense?

Principio de incertidumbre de Heisenberg:

- "El mero hecho de medir el estado de un sistema lo altera"
- No se puede obtener información de un sistema sin modificar el sistema
- Obtener la mayor cantidad de información posible minimizando las alteraciones y su impacto

¿Qué es la Informática forense?

La validez jurídica de una evidencia digital la decide el juez

Todo documento, log, máquina, etc. ha podido ser manipulado/accedido por terceros

¿Un documento con una firma electrónica reconocida tiene validez jurídica?

¿Qué es la Informática forense?

… ¿Y si el acusado alega que le robaron el certificado (la tarjeta)? ¿Hay denuncia? ¿Se solicitó la revocación del certificado inmediatamente?

¿Qué es la Informática forense?

Para que las evidencias digitales tengan validez jurídica hay seguir procesos que aseguren:

- Que se ha respetado la ley para obtenerlas
- Que la información es exactamente la que se recogió
- Que durante su análisis no se ha modificado/creado/eliminado nada
- El análisis realizado tiene que poder ser reproducible

¿Qué es la Informática forense?

Forensic Examination of Digital Evidence: A Guide for Law Enforcement

Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition

UNE 71506 - Metodología para el análisis forense de las evidencias electrónicas

¿Qué es la Informática forense?

Good Practice Guide for Computer-Based Electronic Evidence

RFC 3227 - Guidelines for Evidence Collection and Archiving

ISO/IEC 27037:2012 Information technology -- Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

Informática forense. Proceso

1. Identificación
2. Conservación
3. Análisis
4. Exposición

Informática forense. Proceso

Es imprescindible tomar notas, grabaciones, fotografías, vídeos, etc. de todo lo que se realiza con fechas y horas

Puede ser necesario recordar todo el proceso con la mayor cantidad de detalles posibles en un juicio (años después)

Identificación

Identificar los sistemas (evidencias) que van a ser necesarios en la investigación

Es aconsejable la presencia de un notario que de fe de todo lo que se realiza

Conviene tomar fotografías que muestren su disposición/configuración

Identificación

Desde el primer momento hay que activar la cadena de custodia: registrar de manera exhaustiva quién maneja las evidencias recogidas indicando fechas, horas, dónde se almacenan, quien es el responsable de su custodia, etc.

Si son sistemas que están en marcha, evitar que se sigan usando y recoger toda la información volátil (Podría borrarse al apagar el sistema): Usar programas externos para realizar copias, accesos, etc.

Identificación

La información de la memoria RAM es muy importante (Hay que copiarla modificándola lo menos posible):

- Procesos en ejecución
- Módulos y DLL's en ejecución
- Archivos abiertos
- Claves del registro abiertas
- Versiones desencriptadas de datos

Identificación

La información de la memoria RAM es muy importante (Hay que copiarla modificándola lo menos posible):

- Adjuntos de Email, imágenes, fragmentos de chat
- Llaves criptográficas
- Contraseñas en texto plano
- ...

Identificación

Herramientas para volcar el contenido de la RAM:

- pd Proccess Dumper
- FTK Imager
- Volatility
- EnCase

Identificación

Habrá que recoger también la información sobre los procesos en marcha, los servicios, los usuarios conectados a la máquina, los puertos abiertos, etc.

Cuidado!, Si no hay un notario que de fe de qué se ha hecho y de la información que se ha obtenido... ¿Quién asegura que eso era exactamente lo que había en el sistema en ese momento?

Identificación

Una vez recogida toda la información volátil se apaga el sistema y se copia toda la información no volátil (Discos duros, USBs, etc.)

Es conveniente el uso de Write Blockers, sistemas que permiten acceder a la información, pero evitan la escritura en el disco

Identificación

Se hace una copia bit a bit: Duplicado forense (Así se copian los “restos” y la información oculta que haya por el disco duro)

Se calcula (y se almacena) el resumen criptográfico del original y de la copia para asegurar que son idénticos

Se realiza otro duplicado forense de la copia, para evitar tener que trabajar

Identificación

Herramientas de clonado bit a bit:

- dd (comando Linux)
- Helix3 Pro
- EnCase
- FTK Imager

Conservación

Se deben evitar (Cadena de custodia):

- Pérdidas
- Contaminación
- Daño, alteración, manipulación

Conservación

Documentar exhaustivamente toda la información recogida

Etiquetar todos los dispositivos recogidos

Indicar marca, modelo, número de serie, etc.

Conservación

Fecha, datos y firma de las personas que lo trasladen y manipulen

El original debe quedar a buen recaudo (por ej: en poder del notario)

Se puede entregar una copia a todas las partes interesadas

Siempre es aconsejable tener una copia de respaldo

Análisis

Analizar toda la información obtenida es una tarea tediosa y "casi imposible"

Se usan muchos tipos de herramientas:

- Recuperación de elementos borrados
- Crackeo de passwords
- Analizadores de logs
- ...

Hay que ser ordenado y meticuloso; la intuición del analista es esencial

Análisis

Sitios típicos de búsqueda de información:

- Correos electrónicos
- Herramientas de mensajería
- Ficheros eliminados
- Metadatos de los ficheros (creación, último acceso, etc.)
- Historiales de navegación
- Logs de aplicaciones y del sistema
- Conexiones a otras máquinas

Análisis

Es importante manejar la línea temporal del sistema:

- Cuándo se instaló X
- Cuándo se accedió a Y
- Cuándo se borró Z

Análisis

Es imprescindible respetar la LOPD y el derecho al secreto de las comunicaciones (No se pueden leer correos electrónicos con su médico ni con un amante si no son relevantes para la investigación)

Análisis

Solución: Búsqueda ciega (Intuición del analista)

- No se examina toda la información
- Se realizan búsquedas por palabras clave
- Sólo se analiza la información donde figuran esas palabras clave

Todo un informe pericial puede ser desestimado si se ha violado alguna ley para realizarlo

Presentación

Se realiza un informe explicando todo el proceso y los resultados obtenidos

Por muy bueno que haya sido el proceso, y los resultados obtenidos si el informe no lo refleja correctamente, no tendrá valor

El informe está dirigido a personas no técnicas (jueces, abogados, empresarios, etc.). Debe entenderse (¡Entrega 2!)

El informe debe ser imparcial. El perito no debe expresar opiniones, sólo reflejar pruebas y resultados

Presentación

Partes de un informe:

- Antecedentes
- Evidencias
- Análisis y tratamiento
- Resultados
- Conclusiones

Presentación

Antecedentes: cuál es la situación que ha hecho necesaria la intervención de un perito

Evidencias: evidencias que se han recogido y los procesos que se han seguido de recogida, duplicación, conservación, etc.

Análisis y tratamiento: técnicas y herramientas usadas para analizar la información

Presentación

Resultados: se expondrán de modo claro y entendible qué resultados dieron las técnicas empleadas

Conclusiones: el apartado más importante. Es en el que el experto explica qué se puede deducir de los resultados obtenidos. Todas las conclusiones tienen que derivarse de algún resultado, si no es una suposición

Presentación

En el caso de que haya un juicio, el perito actuará en calidad de testigo

Tendrá que explicar el informe que elaboró en su momento y responder a las preguntas de los abogados

Debido a la lentitud de la justicia, han podido pasar varios años. Es conveniente repasar el informe unos días antes del juicio

Presentación

A veces se llama a declarar a un perito para que desmonte el informe de otro perito:

- Porque se rompió la cadena de custodia y las evidencias se pudieron alterar
- Porque las conclusiones del informe no son directamente derivables de los resultados obtenidos
- Porque aplicando técnicas distintas se obtienen resultados que contradicen los obtenidos en el informe