



CURSO DE ANÁLISIS FORENSE ACERCAMIENTO AL ANÁLISIS FORENSE

Dirigido a: Personas dedicadas o no a la seguridad informática y tengan o no tengan experiencia ni formación en temas de informática forense. Dirigido a profesionales que buscan un mayor conocimiento acerca de los principales fundamentos sobre los que trabajan las principales herramientas de informática forense.

MODULO 1

Este módulo sirve como acercamiento a los procedimientos, herramientas y conocimiento general de un análisis forense.

1.1 INTRODUCCION A LA INFORMÁTICA / AUDITORÍA FORENSE

- Definición: qué es exactamente la informática forense.
- Finalidad de un análisis forense.
- Principales razones que desencadenan un análisis forense.
- La cadena de custodia.

1.2 VERTIENTES DE UN ANÁLISIS FORENSE

1.2.1 Dispositivos de almacenamiento.

- Identificación de objetivos.
- Preservación de evidencias.
 - Metodología de trabajo.
 - Procedimiento de clonado.
 - Revisión del checksum.
 - Herramienta.
- Recuperación y análisis.
 - Recuperación de datos borrados / perdidos.
 - Aplicación de técnicas de análisis sobre los datos adquiridos.
- Presentación de resultados y objetivos del proceso de análisis forense.
 - Importancia de la documentación durante el proceso.
 - Reglas para la realización de un buen informe.

1.2.2 Sistemas telemáticos. Objetivo del análisis forense en sistemas telemáticos.

- Confirmar la sospecha y analizar los movimientos del atacante.
- Marcando los objetivos.
- La importancia de contener la amenaza.
- Principales técnicas utilizadas por los atacantes.
- Estudio de los procesos activos y sus comportamientos.
 - Herramientas y técnicas de análisis forense.
 - Funcionamiento.

1.3 CONCLUSIONES

MÓDULO 2

En este modulo se analiza de forma práctica los fundamentos y las posibles dificultades de un Análisis Informático Forense.

2.1 ANALIZANDO LOS FUNDAMENTOS DE LA FORÉNSICA

- Estructura física de un disco duro.
- Estructura lógica de un disco duro.

- FAT
- NTFS
- EXT2, EXT3, EXT4
- ReiserSF
- Borrado de datos
 - Qué es realmente el borrado.
 - Borrado seguro.
- Recuperación de datos borrados.

2.2 POSIBLES DIFICULTADES EN UN ANÁLISIS FORENSE.

- Sectores defectuosos.
- Condiciones de trabajo adversas.
- Discos duros dañados.
- Sistemas RAID
- Encriptación.
- Antiforensica

MÓDULO 3

En este modulo se realiza de forma práctica el proceso de recopilación de evidencias y análisis de las mismas. Los asistentes se familiarizarán con el proceso y con las herramientas más comúnmente utilizadas en el Análisis Informático Forense

3.1 RECOPIACIÓN DE EVIDENCIAS.

- Metodología de trabajo.
- Diferentes herramientas para clonado de discos duros y teléfonos móviles

3.2 ANÁLISIS DE DATOS Y RECONSTRUCCIÓN DE EVIDENCIAS.

3.2.1 Análisis Informático con distintas herramientas software de investigación.

Utilización de Herramientas:

- EnCase
- WinHex
- Sleuthkit.

3.2.2 Metadatos. Información disponible. Como visualizar los datos y componer evidencias

3.2.3 Análisis “manual”. Recuperación de datos. Recuperación detallada de e-mails. Visualización de archivos y ficheros

3.2.4 Análisis en caliente. Posibilidades de investigación y recolección de evidencias sin modificar contenidos del dispositivo a investigar.

3.2.5 Análisis remoto. Qué y cómo y investigar a distancia con software forense a través del Network.

3.3 ANÁLISIS DE SISTEMAS OPERATIVOS.

3.3.1 Qué queremos buscar.

3.3.2 Dónde buscar

3.4 INFOME TECNICO. Muestras de informes con distintos contenidos según tipo de investigación.