Profesor

Constantino Malagón

Informática Forense

Presentación

Universidad Francisco de Vitoria UFV Madrid

Grado en Ingeniería Informática
Escuela Politécnica Superior

Introducción

Universidad Francisco de Vitoria UFV Madrid

- La informática forense incluye la recolección y el análisis de datos en formato digital de forma que se puedan usar en una investigación
- Un experto en informática forense debe saber cómo extraer esa información en una forma que luego sea admisible como posible prueba en un juicio
- Para que una evidencia sea admisible los investigadores deben seguir cuidadosamente unas reglas
- Ninguna acción llevada a cabo por los investigadores puede cambiar en lo más mínimo los datos

Introducción

Universidad Francisco de Vitoria UFV Madrid

- La informática forense es una rama de la Ciencia Forense en general y está reconocida por la mayoría de los tribunales
- Una definición dada por el primer congreso Digital Forensic Research Workshop (DFRWS) es:

Introducción

Universidad Francisco de Vitoria UFV Madrid

- The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Introducción

- Este proceso tiene cinco fases básicas:
- Identificación – La primera fase consiste en identificar las posibles fuentes de información o evidencias relevantes (básicamente dispositivos) así como la localización de dichos datos (normalmente discos duros o dispositivos de almacenamiento en general)

Introducción

- Custodia – Es el proceso de custodiar la información relevante almacenada digitalmente (ESI o process of preserving relevant electronically stored information)
- Se necesita también proteger la “escena del crimen” y documentar toda la información relevante sobre las evidencias y cómo han sido detectadas.

Introducción

- Recolección (collection) – es la extracción de información digital que pueda ser relevante para la investigación.
- Esta fase implica la identifiación de los dispositivos de almacenamiento en los cuales está almacenada dicha información, para a continuación realizar una imagen (formato ISO, dd,…), copiar e imprimir dicho contenido.

Introducción

- Análisis – es la búsqueda exhaustiva y en profundidad de evidencias relacionadas con el incidente que se está investigando en las imágenes sacadas en la fase anterior.
- El análisis intenta apuntar conclusiones basadas en las evidencias encontradas.

Introducción

- Informes (Reporting) – primero, hay que señalar en los informes que nuestro proceso está basado en técnicas conocidas y en una metodología clara, describiendo éstas.
- Es decir, es necesario que nuestros métodos sean tales que otros forenses sean capaces de duplicar y reproducir los mismos resultados.
- Todo tiene que ser lo más objetivo posible.

Introducción

- La informática forense está en continua evolución y tiene varios campos o especialidades:
- Computer Forensics – the identification, preservation, collection, analysis and reporting on evidence found on computers, laptops and storage media in support of investigations and legal proceedings.

Introducción

- Network Forensics – the monitoring, capture, storing and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents, i.e. worms, virus or malware attacks, abnormal network traffic and security breaches.
- Mobile Devices Forensics – the recovery of electronic evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets and game consoles.

Introducción

- Digital Image Forensics – the extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.
- Digital Video/Audio Forensics – the collection, analysis and evaluation of sound and video recordings. The science is the establishment of authenticity as to whether a recording is original and whether it has been tampered with, either maliciously or accidentally.
- Memory forensics – the recovery of evidence from the RAM of a running computer, also called live acquisition.