INFORMÁTICA FORENSE

Concepto

- El cómputo forense, también llamado INFORMATICA FORENSE, computación forense, análisis forense digital, examinación forense digital o Forensic es la aplicación de técnicas científicas y analíticas especializadas en infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

- Esta disciplina hace uso no solo de tecnología de punta para poder mantener la integridad de los datos y del procesamiento de los mismos; sino que también requiere de una especialización y conocimientos avanzados en materia de informática y sistemas para poder detectar dentro de cualquier dispositivo electrónico lo que ha sucedido.

Generalidades

- Se reconoce generalmente a Dan Farmer y Wietse Venema, los creadores del Forensics Toolkit, como los pioneros de la informática forense.

- Actualmente, Brian Carrier es probablemente uno de los mayores expertos mundiales en el tema.

- La Informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos. Gracias a ella, las empresas obtienen una respuesta a problemas de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial surgidos a través de uso indebido de las tecnologías de la información.

¿Para qué sirve?

- Para garantizar la efectividad de las políticas de seguridad y la protección tanto de la información como de las tecnologías que facilitan la gestión de esa información.

¿En qué consiste?

- Consiste en la investigación de los sistemas de información con el fin de detectar evidencias de la vulneración de los sistemas.

¿Cuál es su finalidad?

- Cuando una empresa contrata servicios de Informática forense puede perseguir objetivos preventivos, anticipándose al posible problema u objetivos correctivos, para una solución favorable una vez que la vulneración y las infracciones ya se han producido.

¿Cuál es la forma correcta de proceder? Y, ¿por qué?

- Todo el procedimiento debe hacerse teniendo en cuenta los requerimientos legales para no vulnerar en ningún momento los derechos de terceros que puedan verse afectados. Ello, para que, llegado el caso, las evidencias sean aceptadas por los tribunales y puedan constituir un elemento de prueba fundamental, si se plantea un litigio, para alcanzar un resultado favorable.

Objetivos

- Finalidad preventiva, en primer término.

- Por otro lado, cuando la seguridad de la empresa ya ha sido vulnerada, la informática forense permite recoger rastros probatorios para averiguar, siguiendo las evidencias electrónicas, el origen del ataque (si es una vulneración externa de la seguridad) o las posibles alteraciones, manipulaciones, fugas o destrucciones de datos a nivel interno de la empresa para determinar las actividades realizadas desde uno o varios equipos concretos.

Para realizar un adecuado análisis de Informática forense se requiere:

- Un equipo multidisciplinar que incluya profesionales expertos en derecho de las TI y expertos técnicos en metodología forense. Esto es así porque se trata de garantizar el cumplimiento tanto de los requerimientos jurídicos como los requerimientos técnicos derivados de la metodología forense.

Uso de las herramientas a nivel mundial

- Delitos contra la Propiedad Intelectual, en caso de Software Pirata o documentos con el debido registro de derechos de Autor.
- Robo de Propiedad Intelectual y Espionaje industrial.
- Lavado de Dinero, vía transferencia de fondos por Internet.
- Acoso Sexual (vía e-mail); Chantaje o amenazas (vía e-mail).
- Acceso no autorizado a propiedad intelectual.
- Corrupción.
- Destrucción de Información Confidencial.
- Fraude (en apuestas, compras, etc. Vía e-mail).
- Pornografía en todas sus formas, inclusive en la más devastadora: Pornografía infantil.

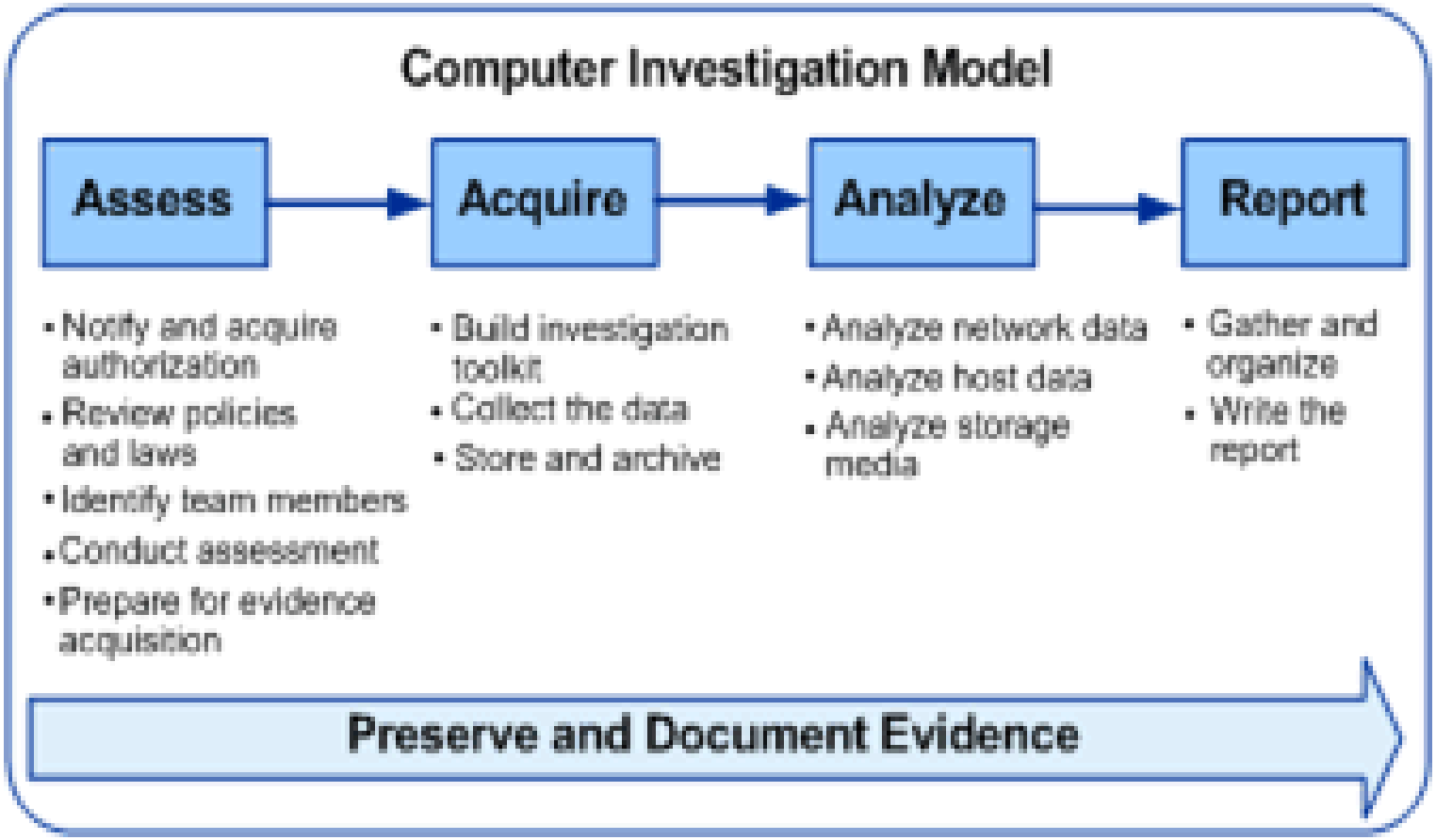
Técnicas de detección de evidencias

- Determinar si la computadora en cuestión tiene o no información relevante al proceso judicial.
- Asistir en la preparación y respuesta a interrogatorios.
- Recibir y examinar información que está sólo accesible a través del uso de métodos y programas forenses.
- Planificar y proveer testimonio del perito.

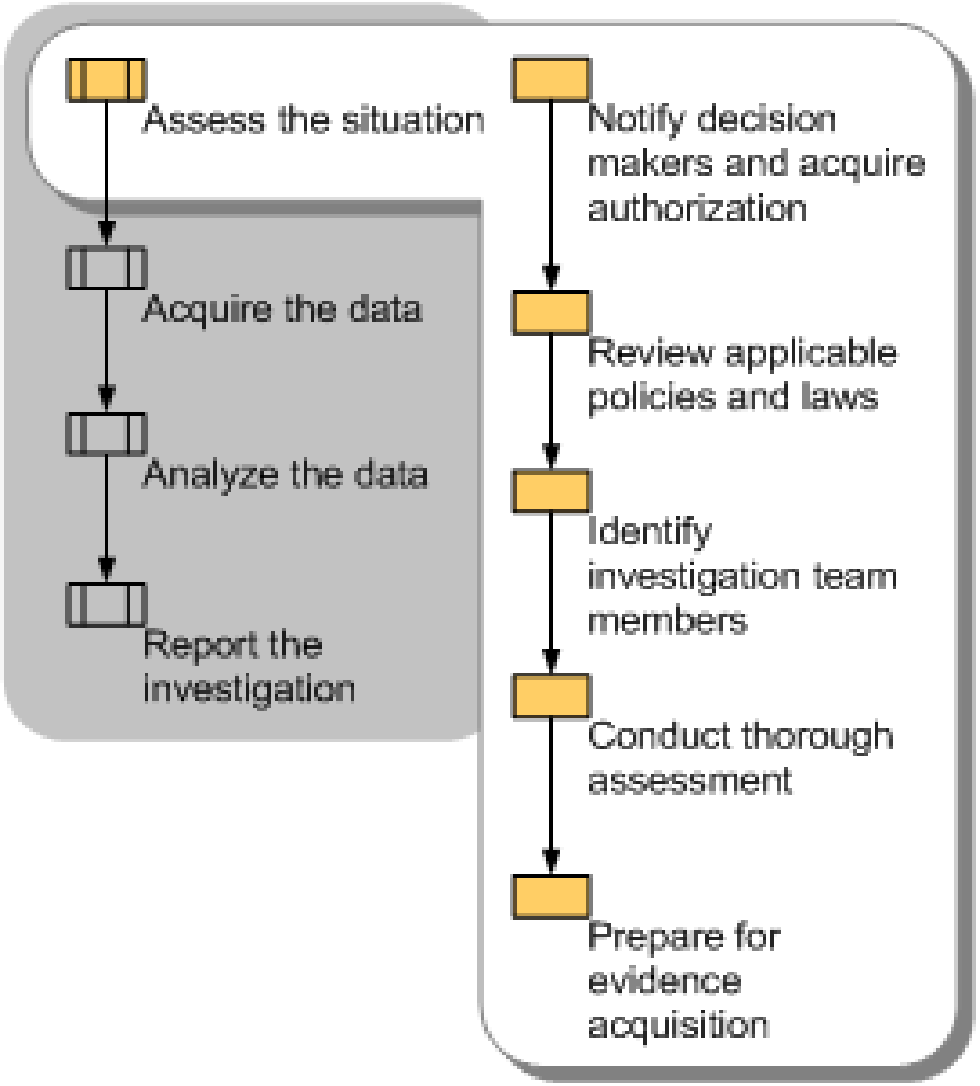
Elementos a recuperar

- Recuperación de evidencias en discos
- Recuperación de contraseñas
- Detección y recuperación de Virus, Troyanos y Spyware
- Seguridad en el correo electrónico
- Análisis de Redes P2P
- Procesos en el puesto de usuario
- Anonimato
- Investigación de información

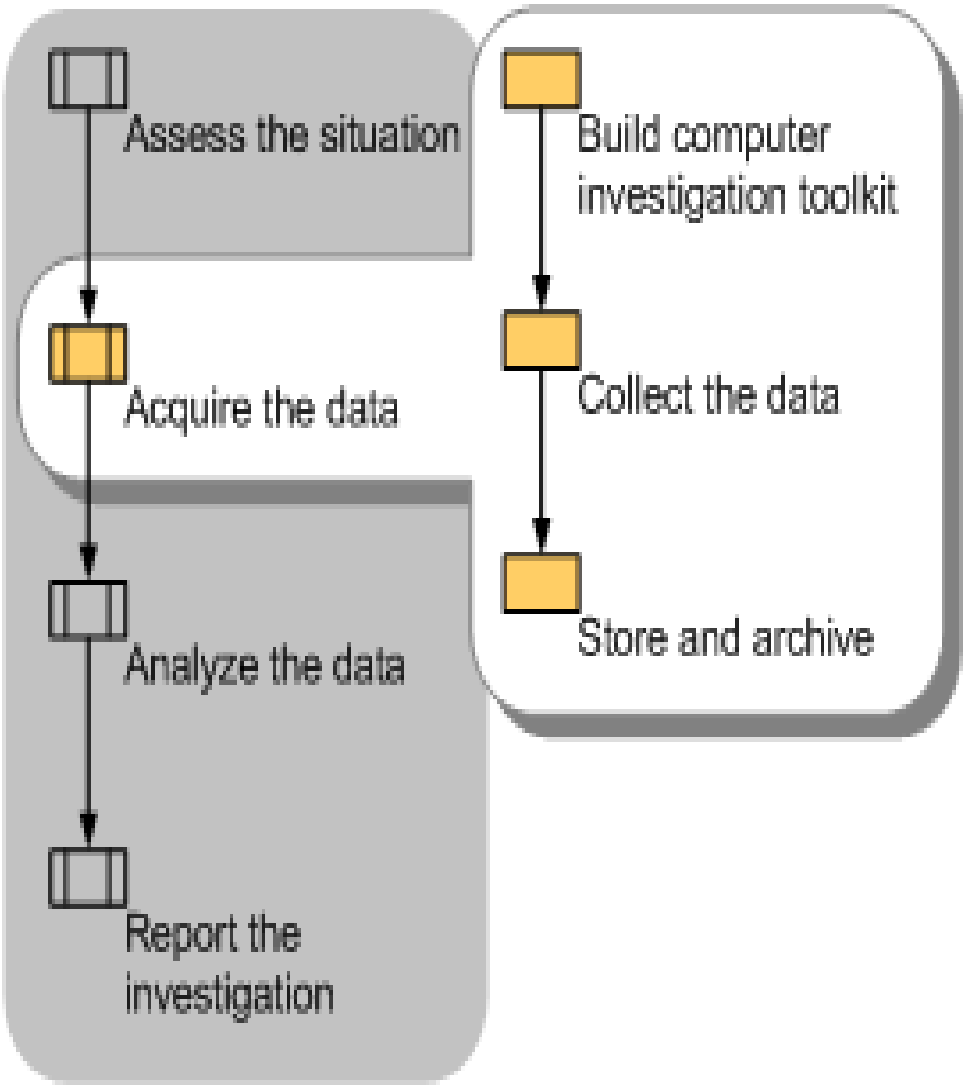
Metodología Básica de Análisis Forense



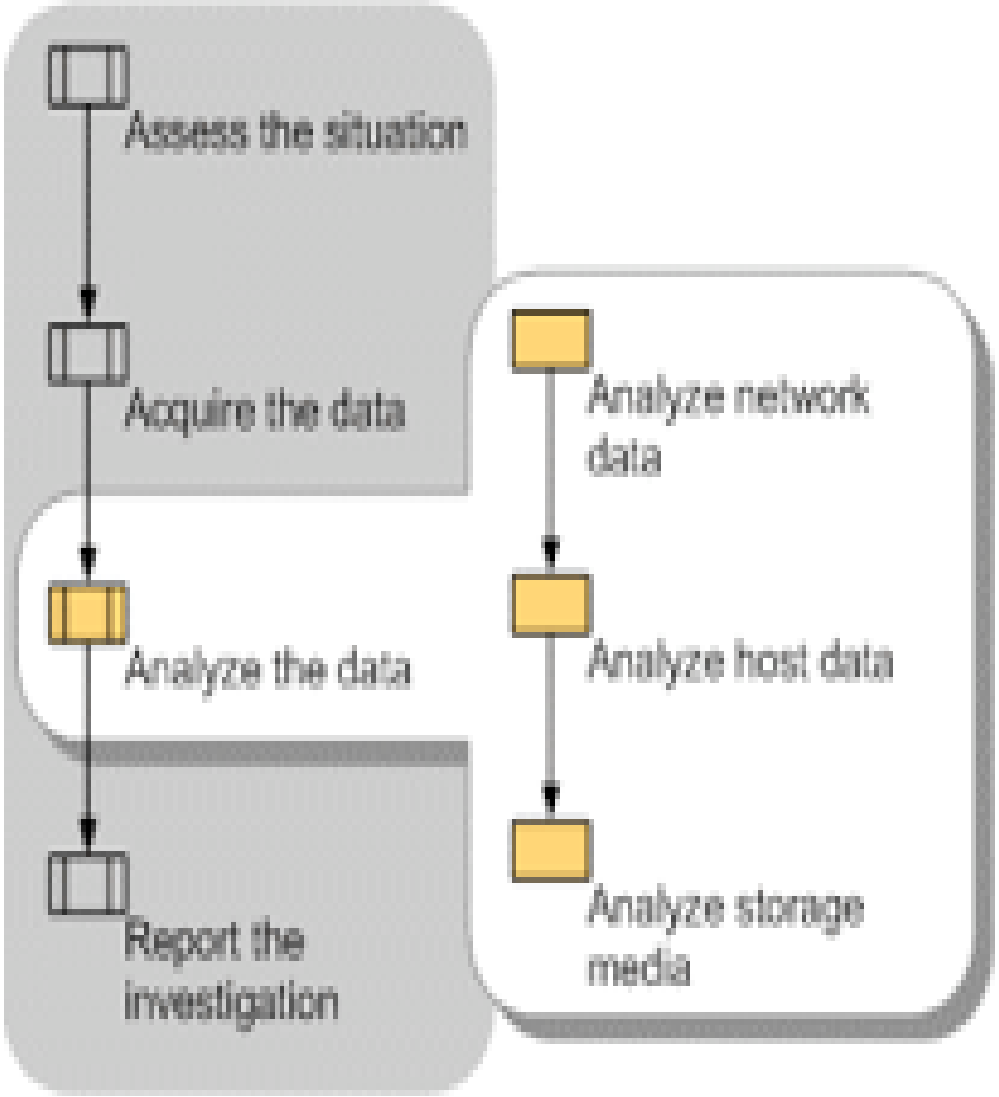
Identificación:



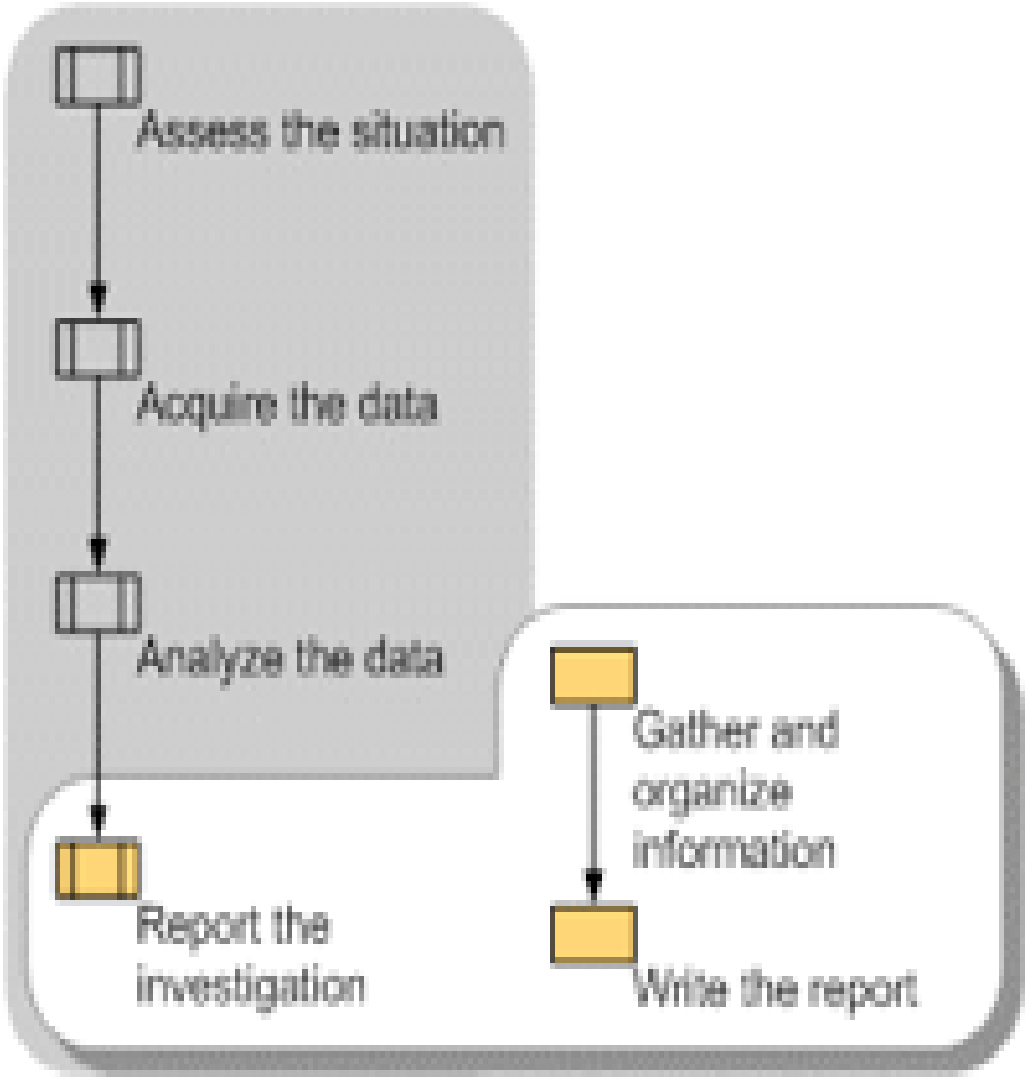
Adquisición:



Análisis de datos



Preparación del Informe



ACTIVIDAD

Informática Forense

- ¿Qué es?
- ¿Para qué sirve?
- ¿En qué consiste?
- ¿Cuál es su finalidad?
- ¿Forma de proceder?
- ¿Objetivos?
- ¿Requerimientos?
- Mencione al menos 5 herramientas a nivel mundial
- Elementos que se pueden recuperar
- Mencione 4 técnicas de detección de evidencia
- Describa la metodología básica