Análisis Forense Informático

Principios y Metodología

Informática Forense

Definición

- El término "forense" se refiere a la aplicación del conocimiento científico a un problema.
- Informática forense: aplicación del método científico para **reconstruir una secuencia de eventos** que involucran computadoras e información.

¿Podemos averiguar, tras la ocurrencia de un incidente, lo que sucedió en un sistema de información?

Informática Forense

Aplicación

Principio de Intercambio de Locard

En la comisión de un delito, el perpetrador deja algo en la escena del crimen y se lleva algo de la escena del crimen. Estos “algos” son evidencia.

Esto aplica también al mundo digital:

- Visitar un sitio web: deja registro en el servidor de ese sitio web, genera una cookie, …
- Intentar acceder a un sistema: queda constancia de los intentos, exitosos o no.
- Un ataque MITM (Man In The Middle): se manifiesta con diferencias en claves, direcciones IP, …

Ejemplos de evidencias

En hosts remotos

- Ultimos accesos (Comando **last**)
- Intentos de login (Archivo **/var/log/auth.log**)
- Historial de comandos (Comando **history**)

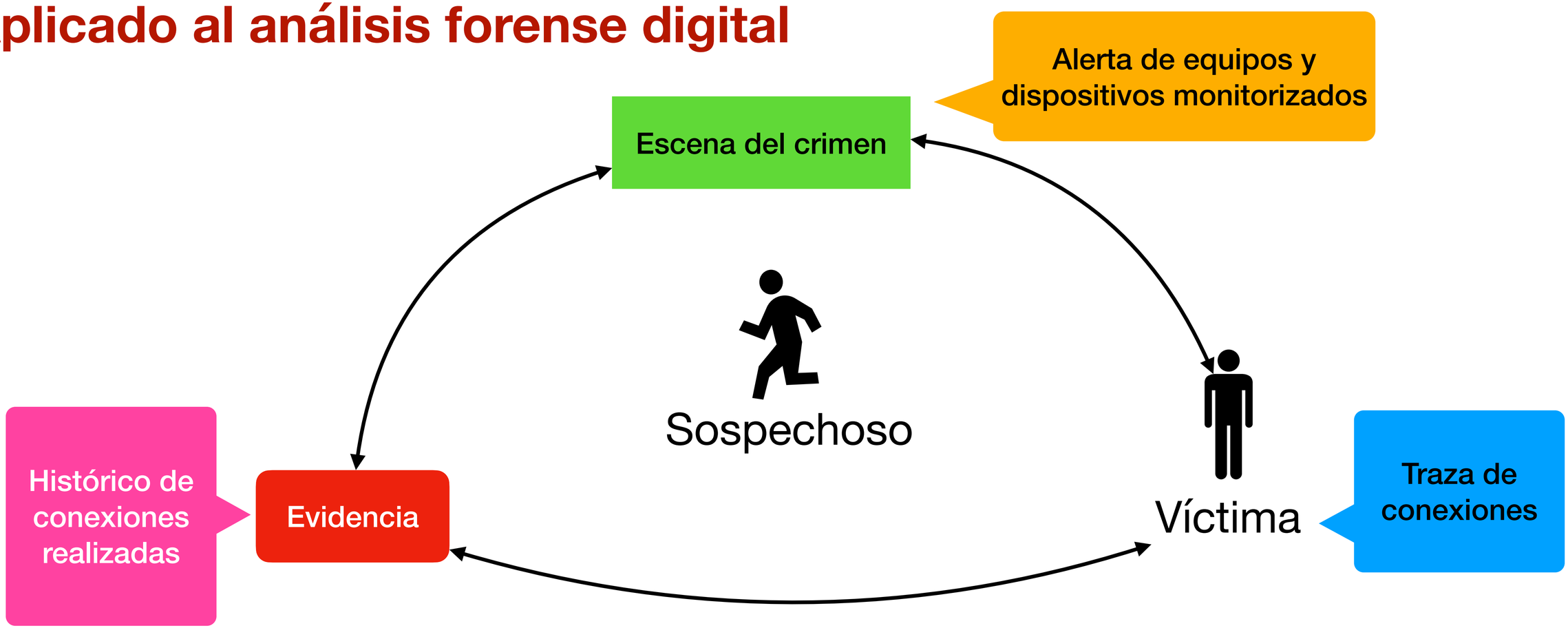
En dispositivos personales

- Caché e historial del navegador
- Archivos accedidos recientemente
- Redes inalámbricas utilizadas
- Recursos en red accedidos
- Metadatos presentes en los documentos

La captura de estas evidencias se llevará a cabo de diversos métodos, dependiendo del sistema que se trate en cada caso.

Principio de Locard

Aplicado al análisis forense digital



Cadena de Custodia Digital

Cadena de Custodia Digital

Definición del procedimiento

- Permite conocer identidad, integridad y autenticidad de los indicios digitales relacionados con un acto delictivo.
- Va desde que esos indicios son encontrados hasta que se aportan al proceso judicial como pruebas.

Pruebas digitales

Características

1. **Intangibles**: no pueden apreciarse directamente a través de los sentidos. Se requieren medios informáticos para su observación.

2. **Replicables**: pueden ser copiadas o replicadas tantas veces como se desee.

3. **Volátiles**: es posible modificarlas o alterarlas, complicando la capacidad probatoria de éstas.

4. **Delebles**: pueden destruirse con bastante facilidad.

5. **Parciales**: a veces las pruebas digitales están formadas por múltiples ficheros informáticos, añadiendo complejidad al proceso.

Fases de la Cadena de Custodia Digital

Fase 1: Obtención de datos producidos, almacenados o transmitidos.

Fase 2: Incorporación al proceso de los datos relevantes.

- Pertinentes
- Necesarios
- Lícitos
- Cumplen los requisitos que exigen las leyes procesales

Fase 3: Valoración de los datos por el órgano juzgador.

Recogida de Evidencias Electrónicas

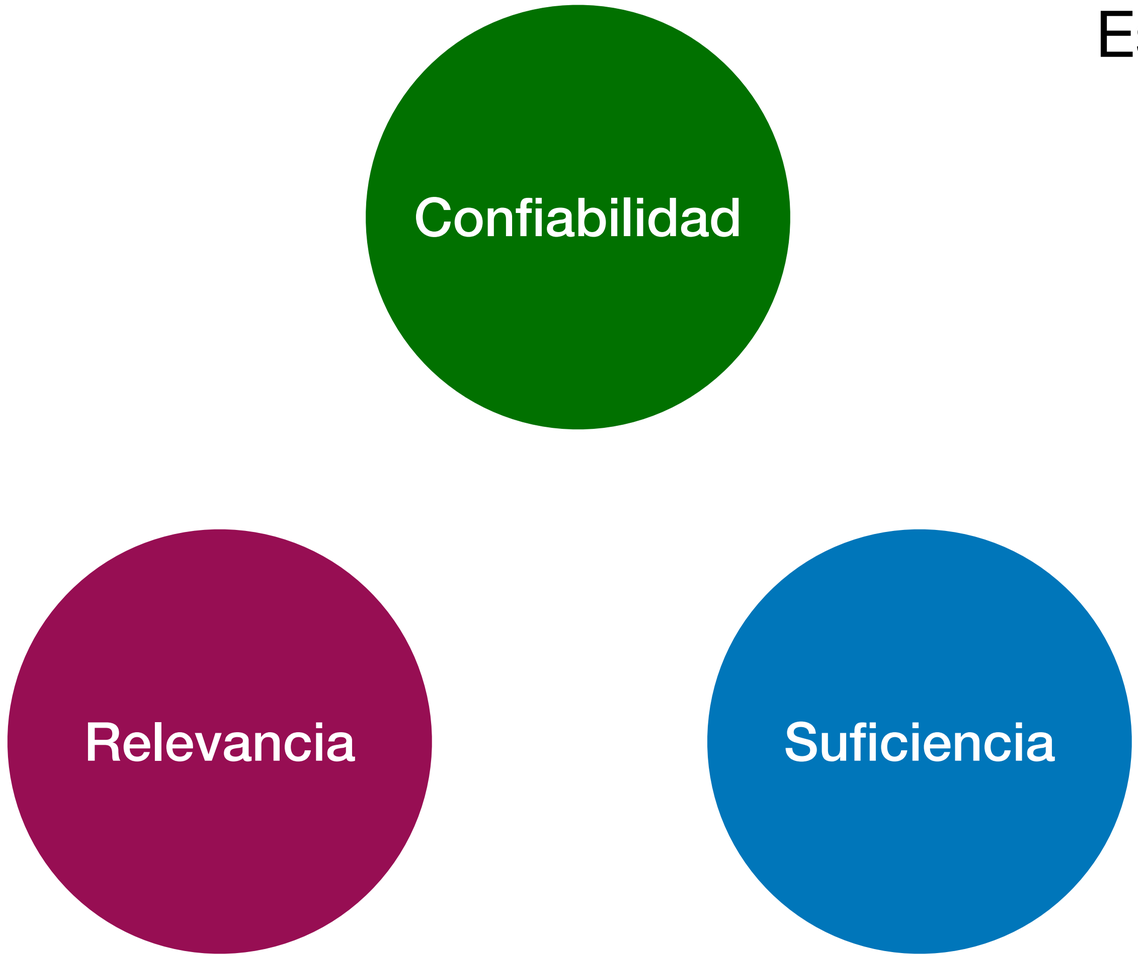
Normativa de referencia

Norma ISO/IEC 27037:2012

- Proporciona pautas para el manejo de la evidencia digital.
- Sistematiza la identificación, recolección, adquisición y preservación de evidencias.
- Aplicación de procesos diseñados para respetar la integridad de la evidencia.
- Metodología aceptable para la admisión de evidencias en procesos legales.

Evidencia Digital

Principios fundamentales



Estos principios definen la calidad de cualquier investigación basada en evidencia digital.

Evidencia que se puede recopilar digitalmente

- Documentos de computadora
- Correos electrónicos
- Mensajes de texto o instantáneos
- Transacciones
- Imágenes
- Historiales de navegación en Internet