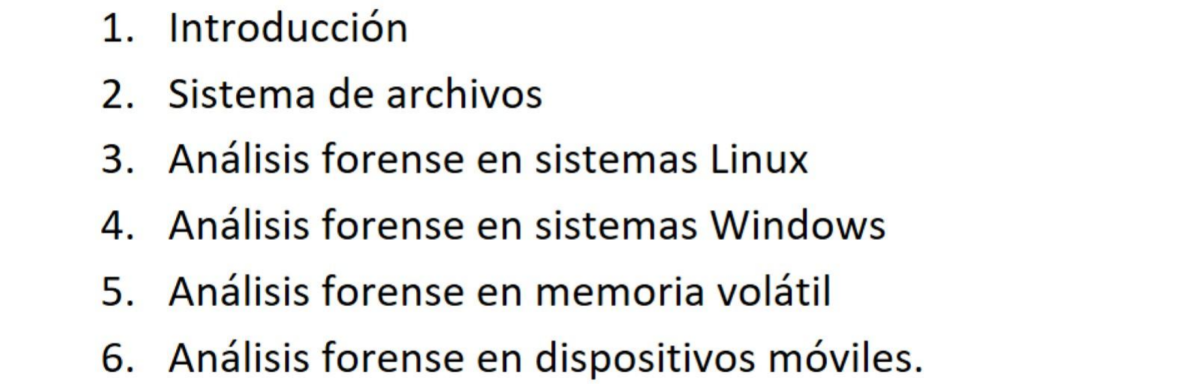
***Clase Viernes 31 de mayo de 2025 - ACCIÓN Y REACCIÓN***

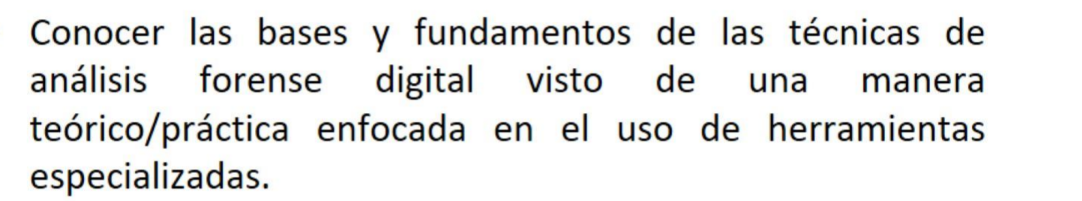
***3.3 Análisis forense***

******

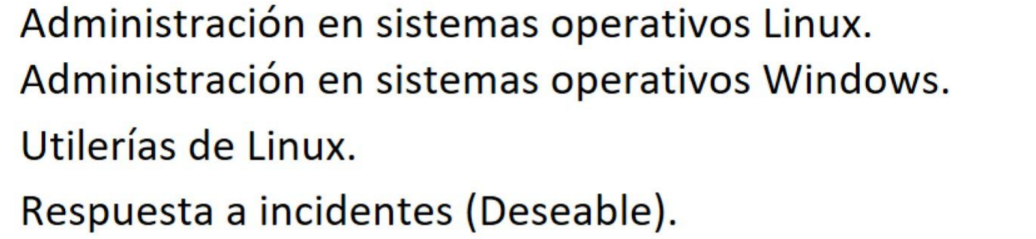
***TEMARIO***

******

***OBJETIVO***

******

***ANTECEDENTES***

******

***Tema 1. Introducción***

******

***Triada de la seguridad***

Integridad, Disponibilidad y Confidencialidad

***Catalogar si es un evento o un incidente, la autenticación de un usuario a un sistema critico a las 3am.***

Hay que revisar que se realizo cuando este entro al sistema crítico y quien fue o que se hizo, si es un cambio programado se tiene que hacer en ciertas horas de la madrugada donde el nivel de usuarios baja y en caso de error es mínimo. Así que por mas sospechoso que parezca un evento hay que ***conocer el contexto*** del negocio o investigar que es lo que se hace y por qué se hace.

***¿QUÉ ES LA INFORMÁTICA FORENSE?***

Rama de la computación dedicada a la aplicación de técnicas científicas y analíticas para la captura, procesamiento, análisis e investigación de información almacenada en computadoras utilizando una metodología donde la evidencia descubierta es aceptable en un proceso legal.

**El método científico** es un proceso sistemático para obtener conocimiento objetivo a través de la observación, planteamiento del problema, hipótesis, experimentación, análisis de datos y conclusión

**PRINCIPIO DE INTERCAMBIO DE LOCARD**

*“Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto”*

* **Edmond Locard**

**OBJETIVOS DEL ANÁLISIS FORENSE**

****

La imparcialidad debe ser el foco de todo lo que nosotros hagamos, sin beneficiar o afectar a cualquiera, buscando reflejar la verdad tomando como referencia las características del método científico.

Generar registro de todo, Generar un informe, Minimizar la perdida de evidencia y Analizar la evidencia recopilada.

Preservar el estado original de la evidencia. Y todo debe estar documentado en un registro

FTK es una Suite con utilidades para ser adquisición y uso de videncia forense, donde puedes montar imágenes, extraer artefactos, adquisición de memoria RAM, levanta una GUI, y este tipo de herramientas es peligroso en un sistema vivo, pero no esta prohibido su uso. Dependerá de la situación en la que se esta llevando para determinar si es viable o no utilizarla.

Se desarrollan hipótesis explicando eventos y se determina si los hallazgos identificados en la investigación las respaldan o las contradicen.

A lo largo de la investigación se van generando hipótesis acerca de lo sucedido. Se debe buscar información que soporte o contradiga las hipótesis generadas.

**PLANTEAMIENTO DE UNA HIPOTESIS**

Se definen características generales del objeto que se esta buscando. Preguntas clave:

* ¿Qué estamos buscando?
* ¿En dónde esperamos encontrarlo?

GUIA PARA EL INVESTIGADOR

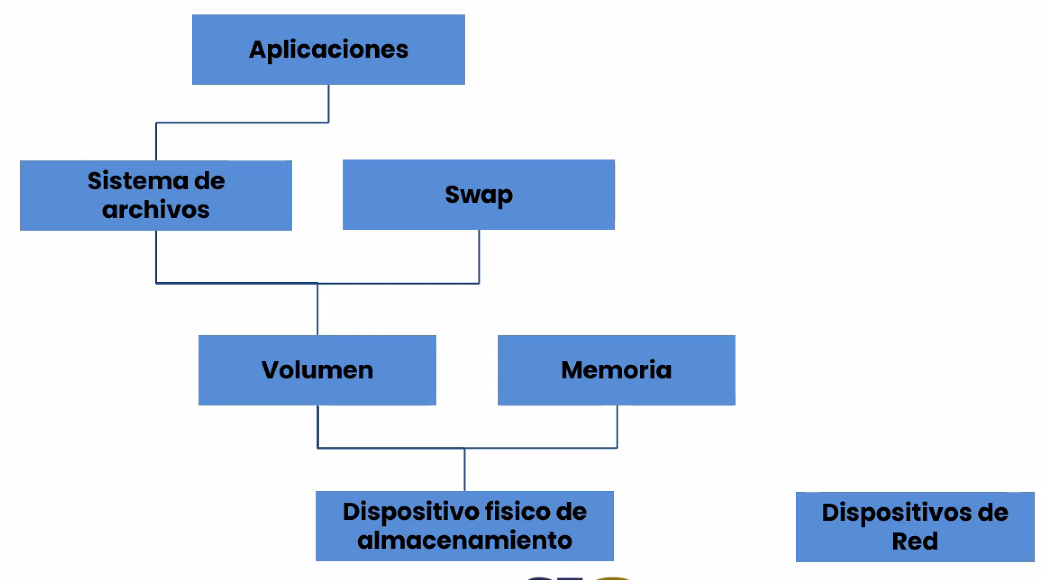
* ¿Qué ocurrió? (WHAT)
* ¿Cuándo ocurrió? (WHEN)
* ¿Cómo ocurrió? (HOW)
* ¿Desde donde lo hizo? (WHERE)
* ¿Quién lo hizo? (WHO)
* ¿Por qué lo hizo? (WHY)

**Evidencia Digital**

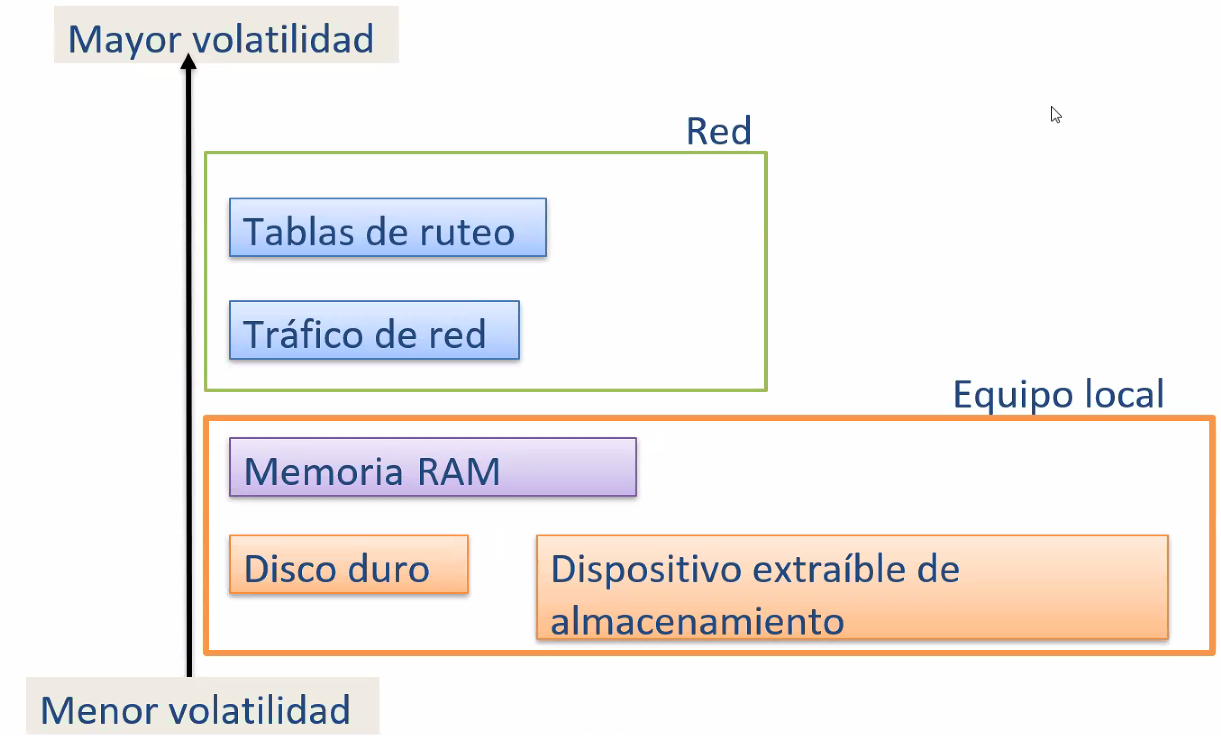
* Computadoras personales
* Dispositivos inteligentes
* Servidores
* Drones
* Electrodomésticos

**Tipos de contenedores**

Cuando se realiza una investigación se debe tomar en cuenta recolectar información para su análisis de distintos puntos, no solo a partir del dispositivo de almacenamiento



**Escala De Volatilidad**

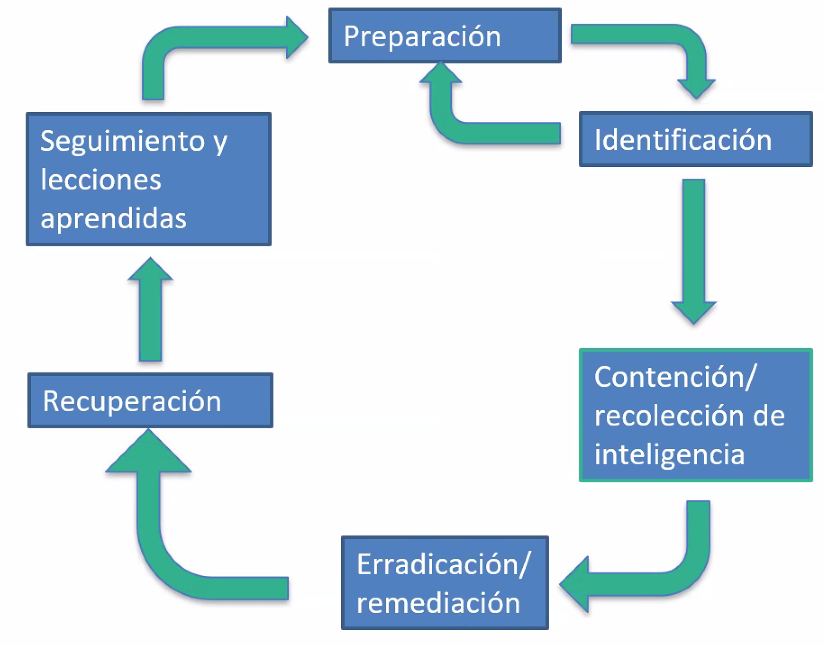
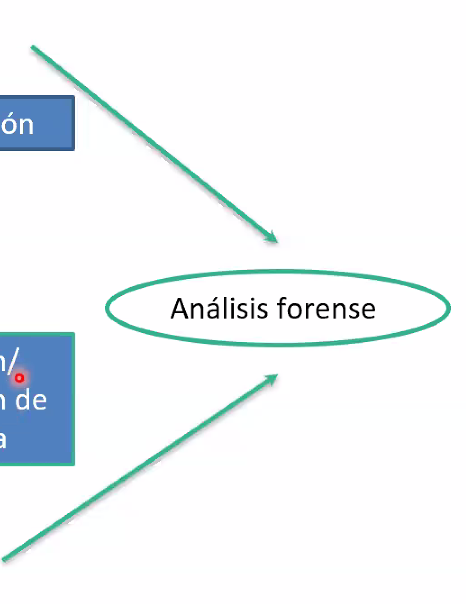


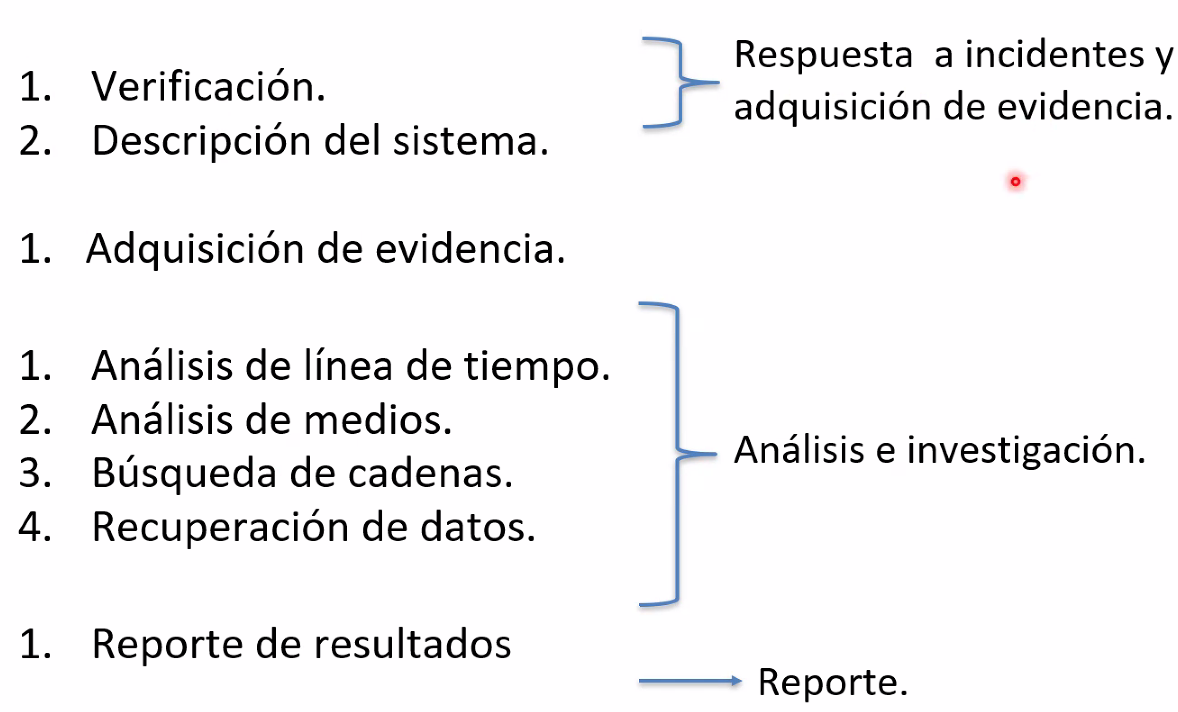
**RESPUESTA A INCIDENTES Y ANÁLISIS FORENSE**

Existe una relación muy estrecha entre la respuesta a incidentes y el análisis forense. Cuando se sigue un proceso de respuesta, el análisis es parte clave del mismo, los resultados del analista permiten ejecutar las medidas de contención de forma efectiva.

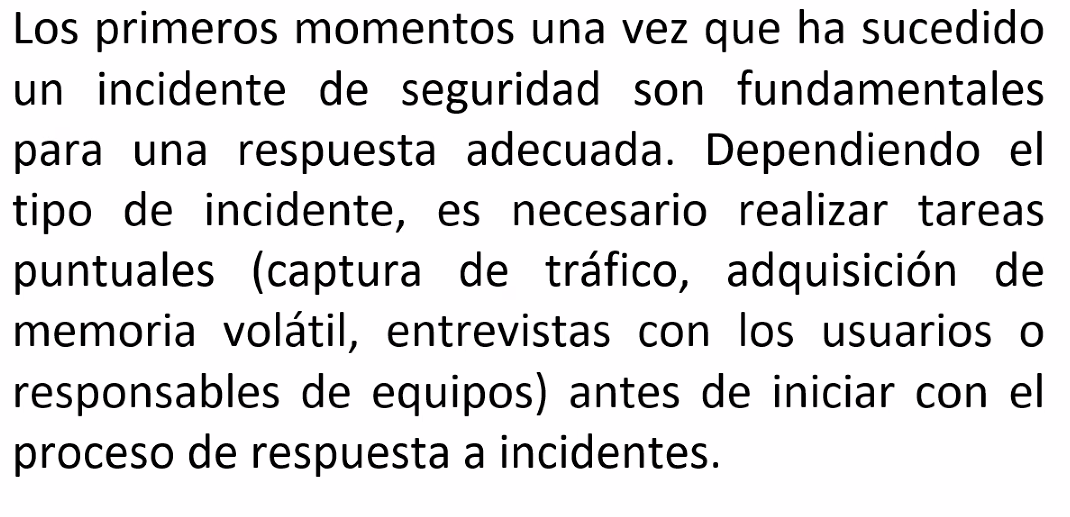
Adicionalmente, la aplicación correcta de una primera respuesta garantiza que la información a analizar ha sido modificada lo menos posible o se mantiene intacta. Es ideal que los procedimientos de esta primera respuesta contemplen los procesos de preservación y manejo de evidencia.

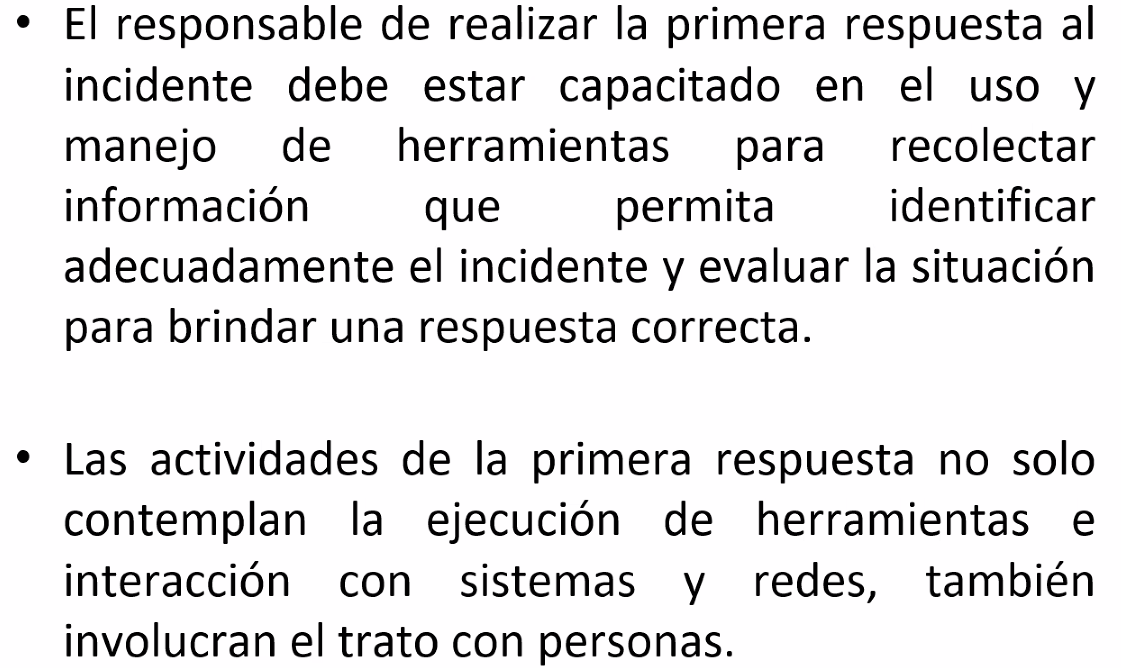
**PROCESO DE RESPUESTA A INCIDENTES EN 6 ETAPAS**



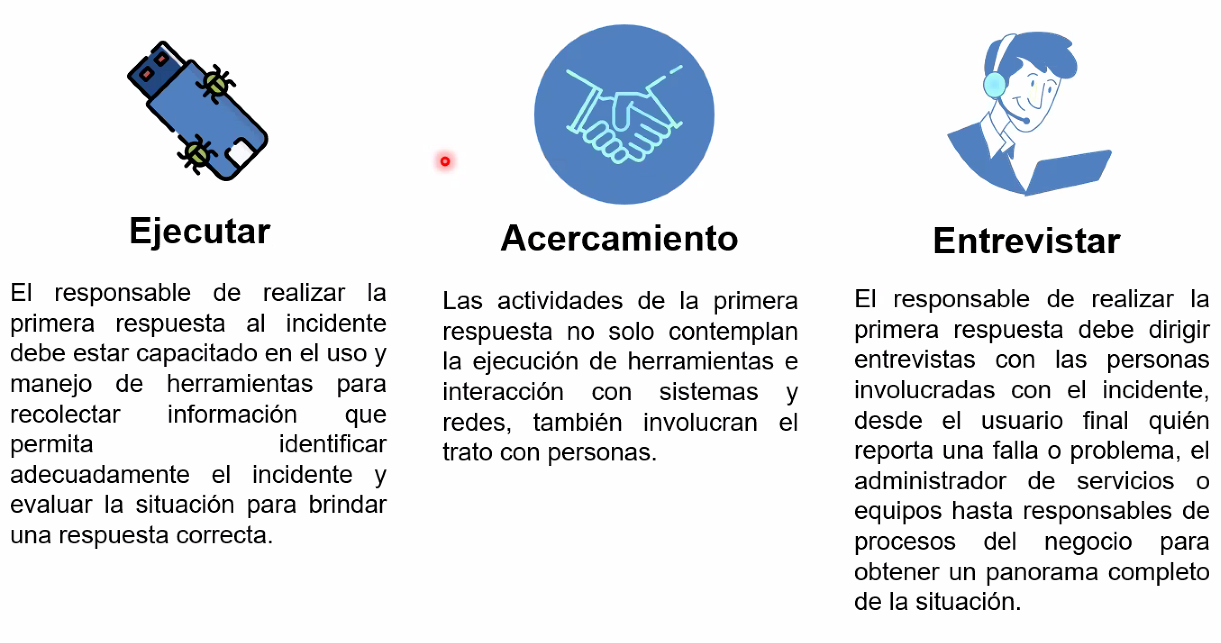


1. **Verificación**





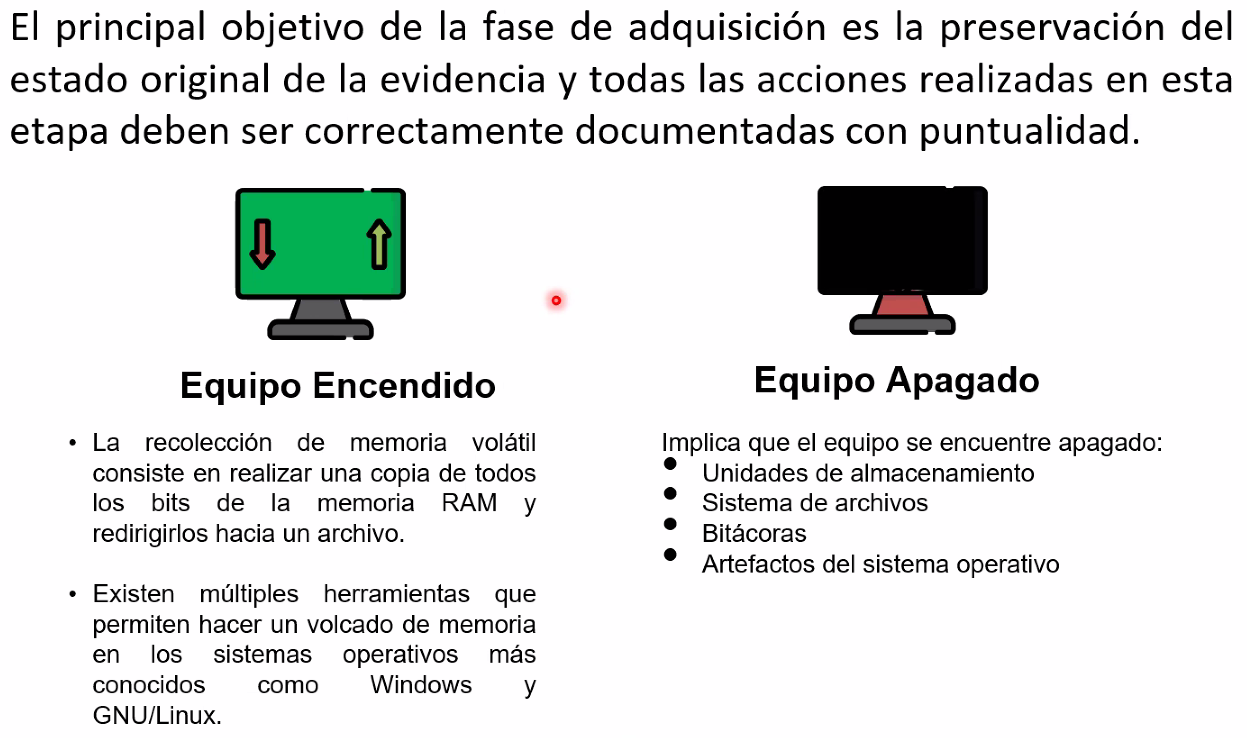
**Primera respuesta al incidente**



**Descripción del sistema**



**Adquisición de evidencia**



Tipos de escenarios

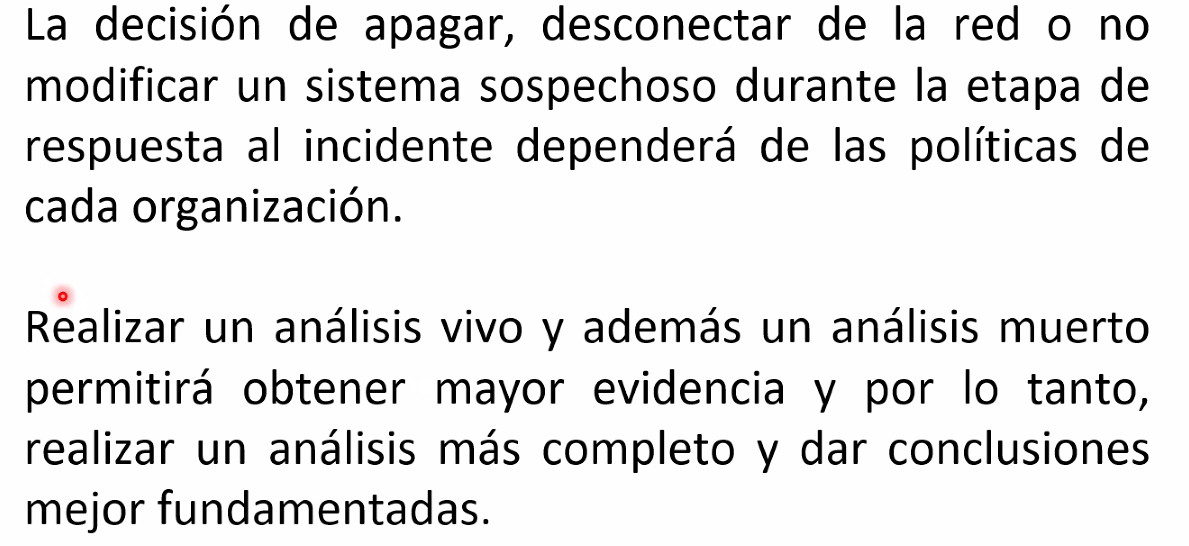
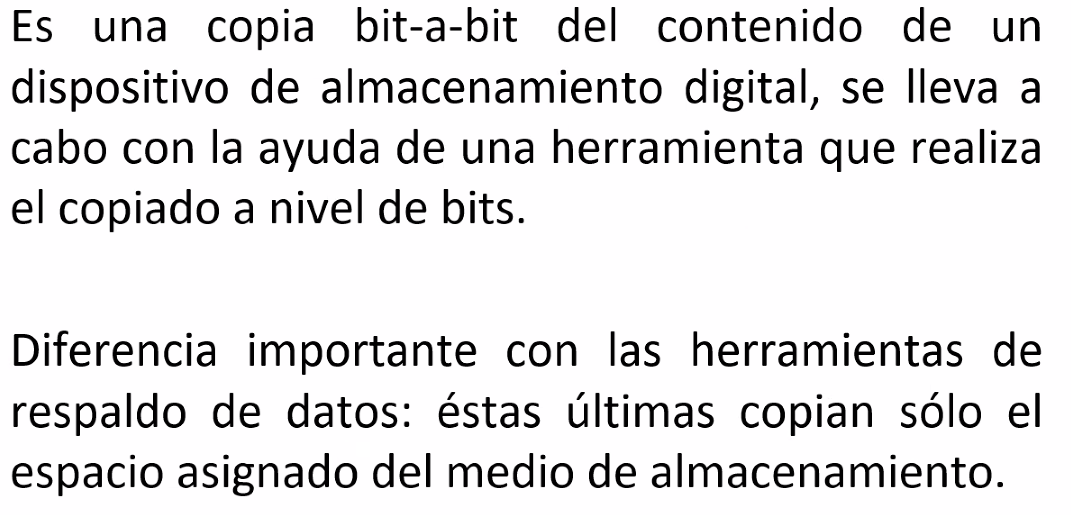
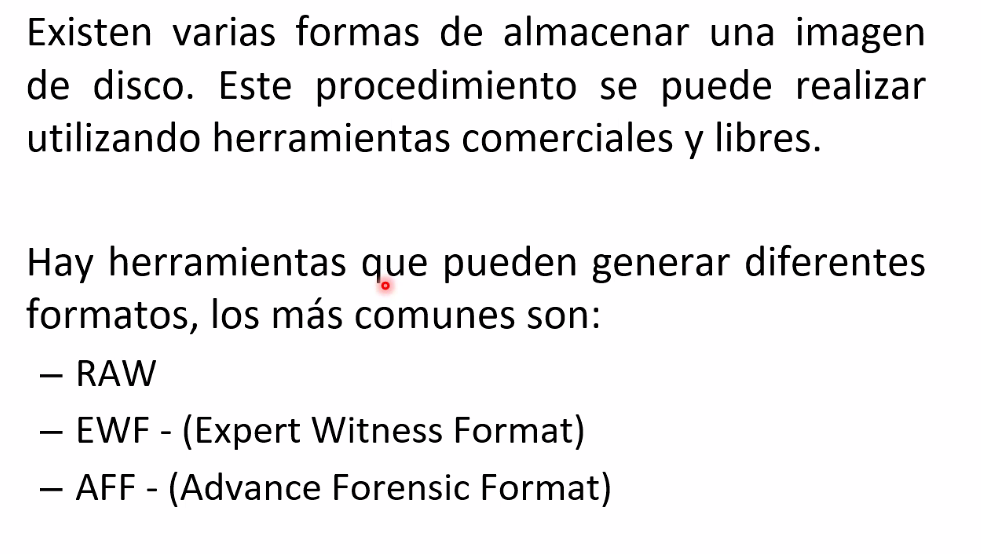


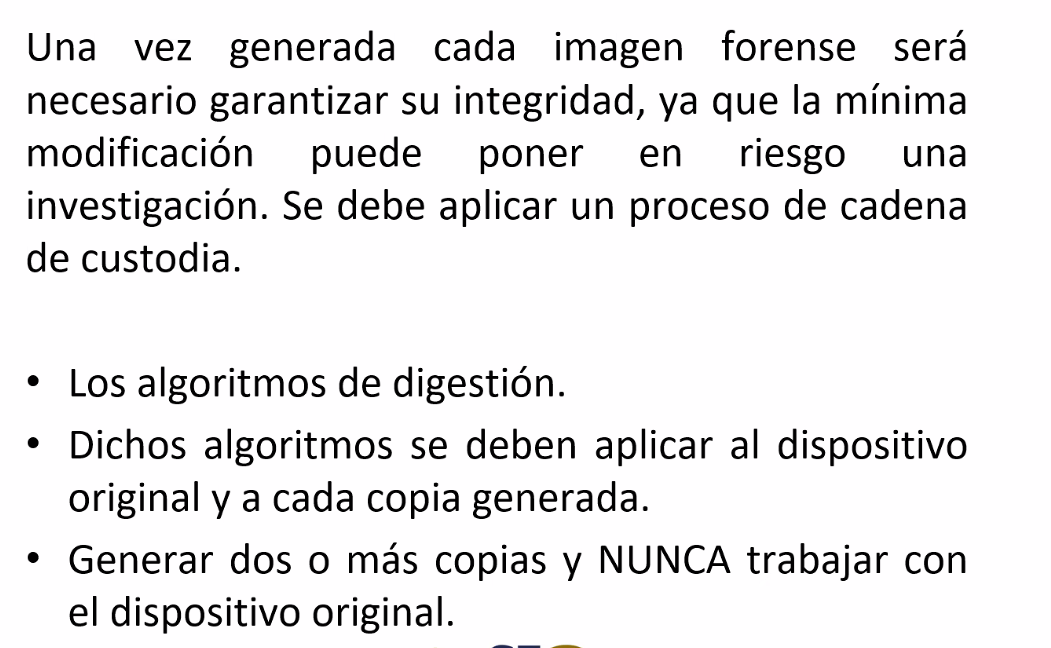
IMAGEN FORENSE



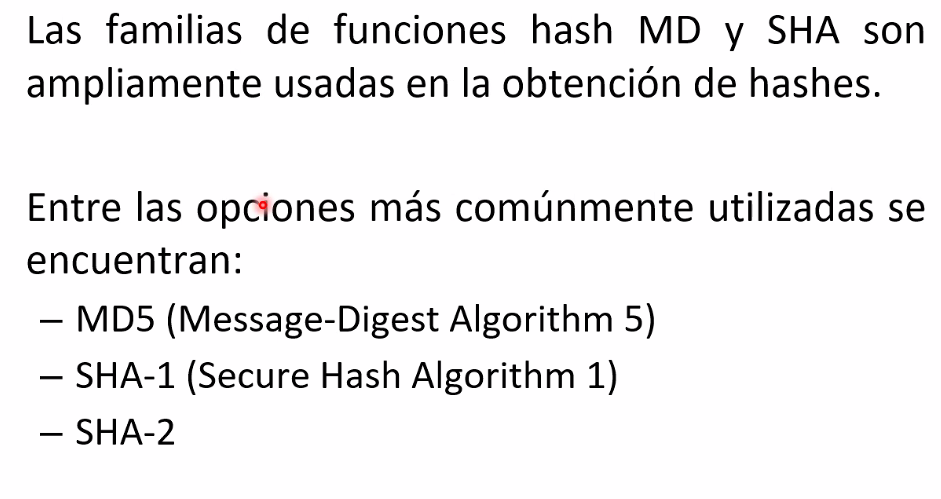
FORMATO DE IMAGEN FORENSE

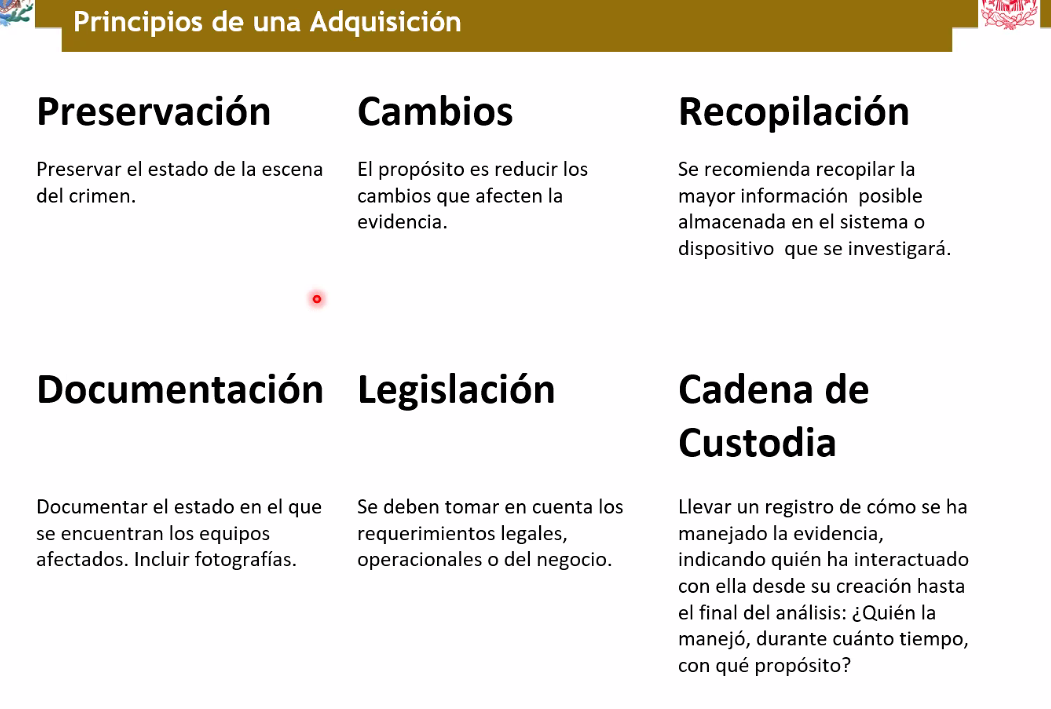


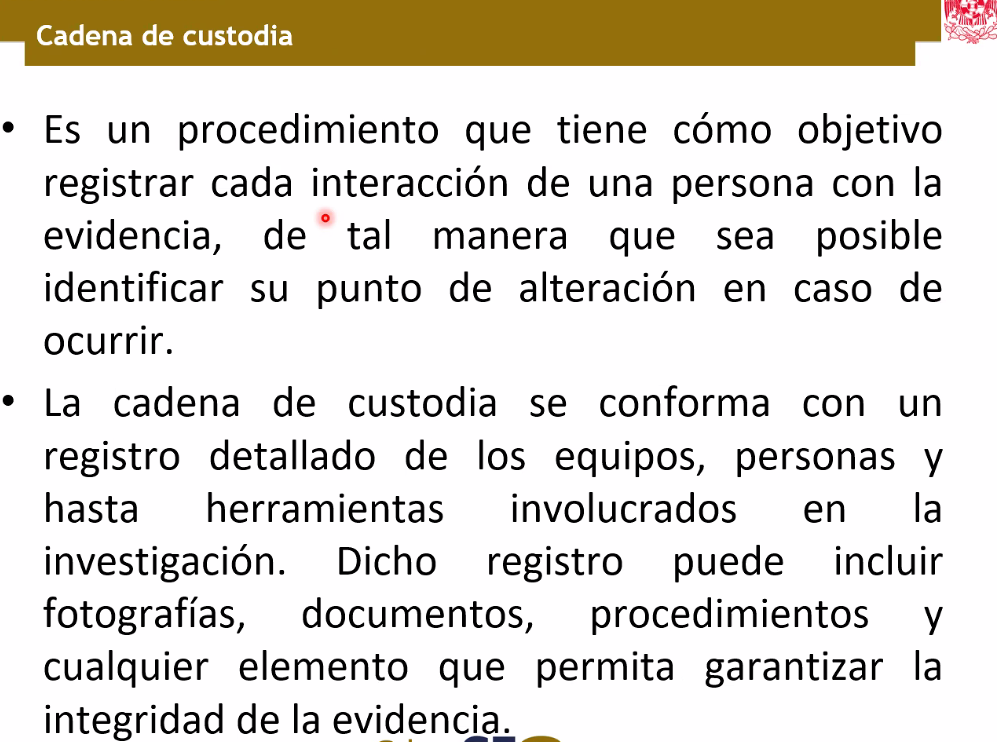
INTEGRDAD DE IMAGEN FORENSE

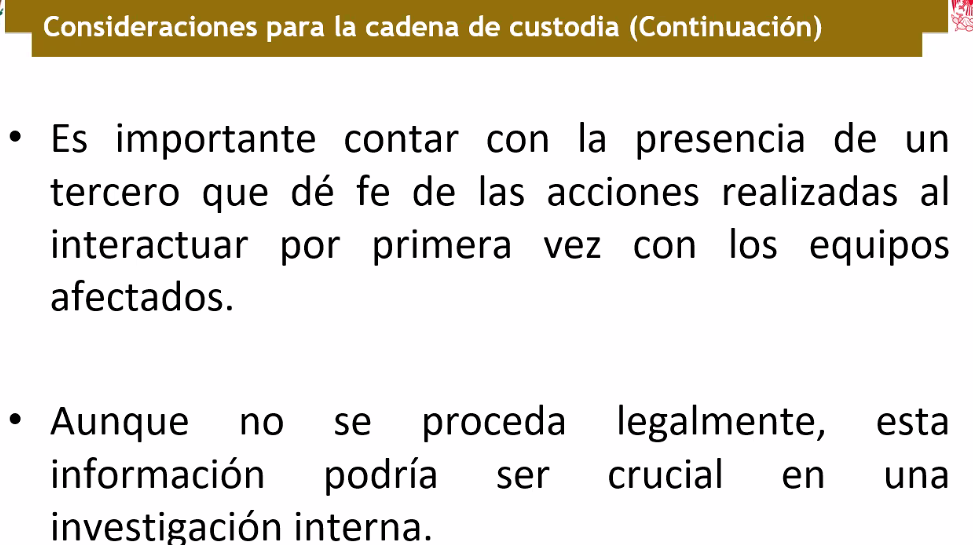


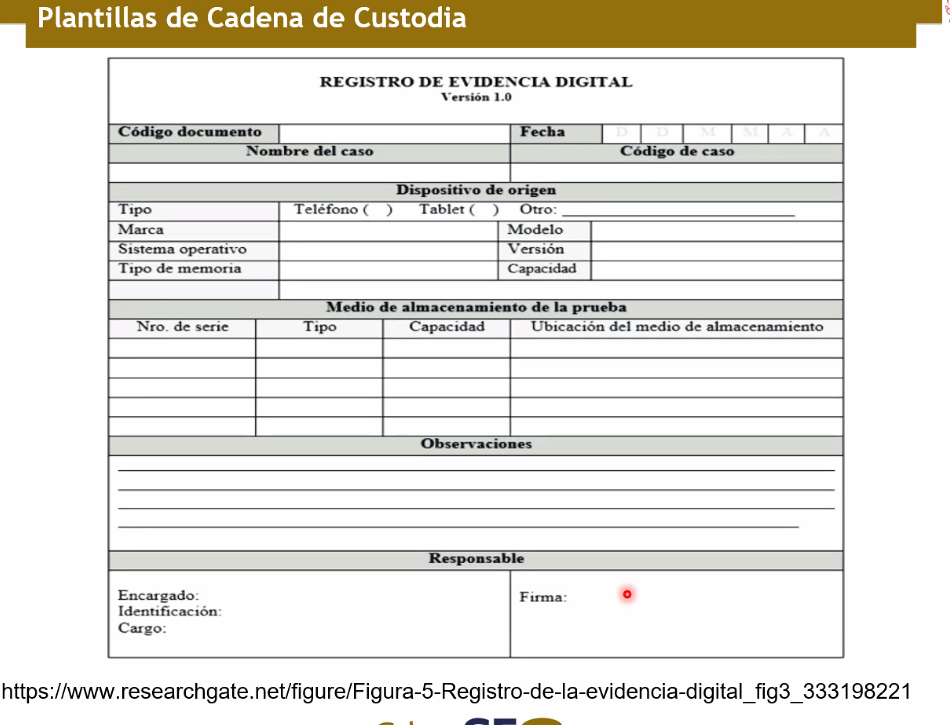
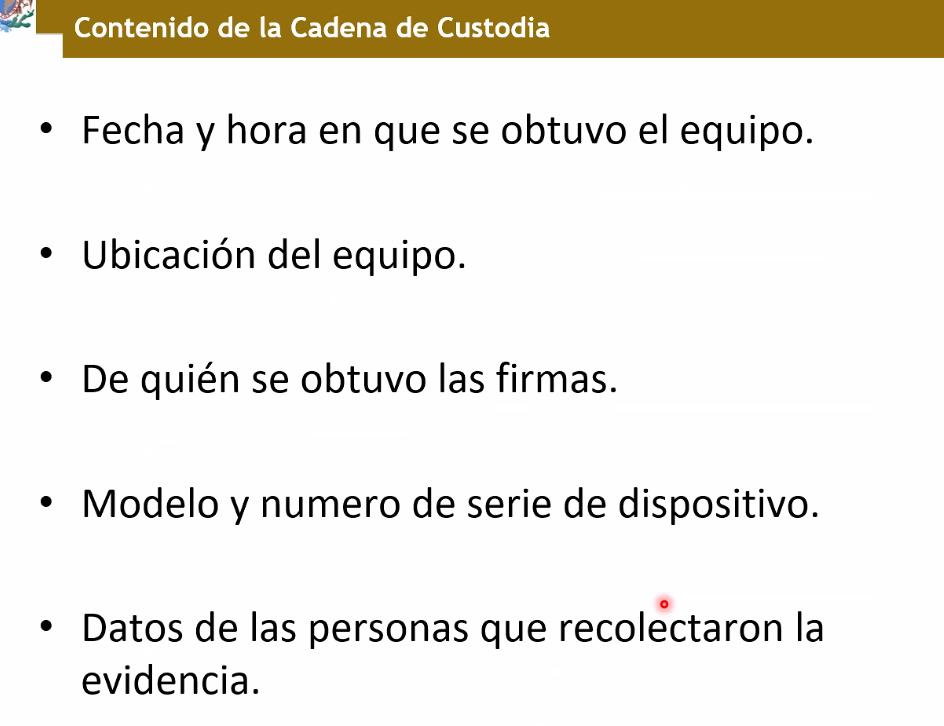
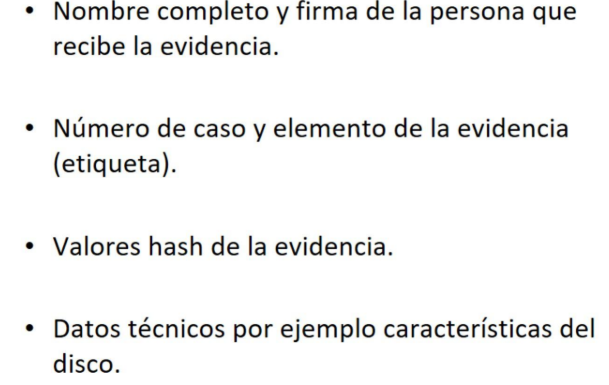
Un algortimo de digestion , a través de una serie clave o HASH







**🧠 Notas de la Clase – Viernes 31 de mayo de 2025**

**📌 Tema Central:**

**Análisis Forense Informático**

**🔷 Objetivo del Tema**

Aplicar técnicas científicas para el análisis e investigación de evidencia digital, garantizando su aceptación en un proceso legal.

**🧱 Fundamentos Clave**

**🔒 Triada de la Seguridad**

* **Integridad**
* **Disponibilidad**
* **Confidencialidad**

**🧪 Informática Forense**

**❓ ¿Qué es?**

Rama de la computación enfocada en analizar evidencia digital utilizando métodos científicos aceptables en contextos legales.

**📖 Principios:**

* **Método Científico:** Observación → Hipótesis → Experimentación → Análisis → Conclusión
* **Principio de Intercambio de Locard:** "Todo contacto deja un rastro".

**🎯 Objetivos del Análisis Forense**

* Imparcialidad.
* Documentar todo el proceso.
* Minimizar la pérdida de evidencia.
* Generar informes claros.
* Preservar el estado original de la evidencia.

**🛠️ Herramientas de Forense Digital**

* **FTK (Forensic Toolkit):**
  + Montaje de imágenes forenses.
  + Extracción de artefactos.
  + Adquisición de memoria RAM.
  + GUI para análisis.
  + Su uso en sistemas vivos requiere evaluación de riesgo.

**🧩 Formulación de Hipótesis**

* Preguntas clave:
  + ¿Qué buscamos?
  + ¿Dónde esperamos encontrarlo?
* Hipótesis deben contrastarse con la evidencia encontrada.

**🕵️ Guía para el Investigador Forense**

| **Pregunta** | **Significado** |
| --- | --- |
| What | ¿Qué ocurrió? |
| When | ¿Cuándo ocurrió? |
| How | ¿Cómo ocurrió? |
| Where | ¿Desde dónde se hizo? |
| Who | ¿Quién lo hizo? |
| Why | ¿Por qué lo hizo? |

**💻 Tipos de Evidencia Digital**

* Computadoras personales
* Dispositivos inteligentes
* Servidores
* Drones
* Electrodomésticos

**🗂️ Tipos de Contenedores**

Se refiere a las distintas fuentes o dispositivos de almacenamiento de donde se extrae evidencia.

**🔄 Escala de Volatilidad**

(No desarrollada, pero se entiende como la jerarquía de datos desde más volátil —como RAM— hasta más persistente —como discos duros).

**🚨 Respuesta a Incidentes & Análisis Forense**

* Están interrelacionados.
* El análisis es crucial para tomar decisiones de contención.
* La **primera respuesta** debe preservar la integridad de la evidencia.

**🧾 Formato de Imagen Forense**

* Debe garantizar la **integridad**, generalmente mediante algoritmos de **hash** (MD5, SHA1, SHA256).
* Se requiere un proceso riguroso y documentado.