**Informática Forense**

La **Informática Forense** es una rama de la informática que se dedica a la **identificación, preservación, análisis y presentación de evidencias digitales** en un proceso legal o de investigación.

Se aplica principalmente cuando se sospecha de delitos informáticos o cuando la información digital puede servir como prueba en un juicio, auditoría o investigación interna.

**Objetivos principales**

* **Recolectar evidencias digitales** (archivos, registros, correos, actividad en redes, etc.) sin alterarlas.
* **Analizar datos** para reconstruir hechos: qué ocurrió, cuándo, cómo y quién estuvo involucrado.
* **Preservar la cadena de custodia**, es decir, mantener la integridad de la prueba digital para que sea válida legalmente.
* **Presentar resultados** de manera comprensible y objetiva para jueces, fiscales o autoridades.

**Ámbitos de aplicación**

* Casos de **fraude financiero** o estafas en línea.
* **Ataques informáticos** como hackeos, malware o ransomware.
* **Delitos electrónicos**: robo de identidad, acoso en redes sociales, distribución ilegal de material.
* **Auditorías empresariales** y fuga de información confidencial.

**Herramientas típicas**

Se utilizan programas especializados como **EnCase, FTK, Autopsy, Wireshark, Volatility**, entre otros, que permiten examinar discos duros, memorias, redes y sistemas sin alterar la evidencia.

👉 En pocas palabras: la informática forense busca **“hacer hablar” a los dispositivos y datos digitales**, pero de forma técnica y legalmente válida.

Componentes claves para que la investigación sea creíble

* + Metodología del proceso
  + Calificación del MIST
* Visión general creada por IA
* La norma ISO/IEC 27037:2012 establece directrices para la [identificación, recolección, adquisición y preservación](https://www.google.com/search?sca_esv=e5327918f41ad0c6&sxsrf=AE3TifN7036dk5FJQt09WgtKgNYZhURPgw%3A1758887525367&q=identificaci%C3%B3n%2C+recolecci%C3%B3n%2C+adquisici%C3%B3n+y+preservaci%C3%B3n&sa=X&ved=2ahUKEwiD5ZjRrvaPAxXPrpUCHdfEGUoQxccNegQIBxAB&mstk=AUtExfCqEc-PNdFfuCRnwbRSQsu5dM545ilCwB33BDUNhg75fj9ENMxEVTmdRnmYmhl5tQHMAPLSXElL848MoV-_ZTiBeeKy2TzOy37uGC_6LwwTI7ZrD6iTlNDLzDchIXxXMssNrKaA2yt1zjEDyL-DMGDhBeI75d-tfig6NZfzl9aYa6lid9yIRPvX_27zmn7KFk8mMzT2dtH2RY3J_FI86bweuvOAf6HIe6VbZ69XhMjDLtytL7HfRoXsbsgMGw662WiLTS0zIv7n-AqwgQAPiXIQ&csui=3) de evidencia digital, cubriendo desde el momento en que se detecta una posible prueba hasta su conservación para fines probatorios. El objetivo principal es asegurar la integridad y la cadena de custodia de la evidencia digital, garantizando que pueda ser admitida en procesos legales y facilitando su intercambio entre jurisdicciones.

**DEFR vs DES**

**Digital Evidence First Responder (DEFR)**

El DEFR es el primer respondedor, la persona que llega a la escena de un incidente (físico o virtual) y tiene la tarea de asegurar, preservar e identificar la evidencia digital potencial. Es el primer punto de contacto con la evidencia, y su intervención debe ser rápida, precisa y meticulosa para evitar la contaminación o alteración de los datos.

**Funciones y responsabilidades del DEFR:**

* **Identificación:** Localizar los dispositivos y las fuentes que puedan contener información digital relevante, como computadoras, teléfonos móviles o servidores.
* **Aseguramiento de la escena:** Proteger la escena para evitar que personas no autorizadas o factores externos (como la alimentación eléctrica) comprometan la evidencia.
* **Documentación:** Registrar meticulosamente todos los detalles de la escena, incluyendo la ubicación de los dispositivos y el estado en que fueron encontrados.
* **Adquisición inicial:** Realizar la recolección de evidencia en el mismo lugar, priorizando la preservación de datos volátiles (como la memoria RAM) antes de que se pierdan.
* **Empaquetado y transporte:** Asegurar que la evidencia se empaquete de forma adecuada y se transporte al laboratorio forense de forma segura, respetando la cadena de custodia.

**Digital Evidence Specialist (DES)**

El DES es el experto forense que recibe la evidencia recolectada por el DEFR en un entorno de laboratorio controlado. Su función principal es analizar en profundidad la evidencia digital preservada para extraer información relevante y preparar los informes correspondientes para un proceso legal.

**Funciones y responsabilidades del DES:**

* **Análisis forense:** Utilizar herramientas y técnicas especializadas para examinar los datos adquiridos. Esto incluye la recuperación de archivos borrados, el análisis de metadatos, el seguimiento de la actividad del usuario y el análisis de la red.
* **Recuperación de datos:** Intentar recuperar datos de dispositivos dañados, encriptados o manipulados para evitar su detección.
* **Elaboración de informes:** Documentar el proceso de análisis, las metodologías utilizadas y los hallazgos de forma clara y concisa para su presentación en un tribunal o en una investigación.
* **Testimonio pericial:** En caso necesario, el DES puede ser llamado para testificar en un juicio como experto, explicando sus hallazgos y el proceso que siguió para obtenerlos.
* **Colaboración:** Trabajar junto a equipos legales, fuerzas de seguridad y otros expertos para resolver casos complejos.

1. Buscar un pendrive
2. Graven un par de archivos, fotos, videos, pdf
3. Borran todo
4. Correr herramienta Foremost o Photorec 🡪 Lo va a recuperar
5. Ahora borrar con Herramienta WIPE
6. Volver a correr herramientas del paso 4) 🡪 No tendrían que poder recuperar