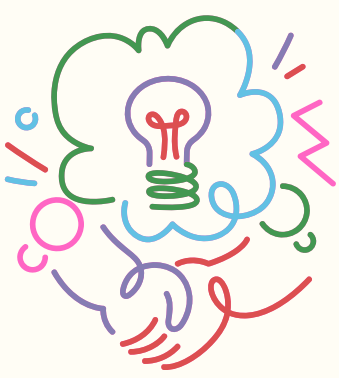
ANALISIS DE LA PRUEBA DIGITAL E INVESTIGACION

En esta etapa, el perito analiza la evidencia digital recolectada, revisando tanto los datos como los metadatos. Primero se verifica el embalaje para asegurar la cadena de custodia. El análisis se enfoca en responder preguntas clave, ajustándose al tipo de delito y al sistema operativo del dispositivo (Windows, Linux, Mac, Android, etc.).

En la fase de análisis pueden aparecer diferentes categorías de datos que se deben analizar, buena parte de los cuales serán lógicamente accesibles, es decir, datos contenidos en ficheros, directamente accesibles. En este proceso de análisis podemos encontrar varios problemas, como los que mencionamos a continuación:

DEMASIADA INFORMACION

El análisis forense puede implicar dispositivos con muchos gigas de datos, lo que dificulta identificar archivos relevantes. Para ello, se usan herramientas que permiten filtrar la información, como búsquedas por cadenas o exclusión de archivos con hash conocido.

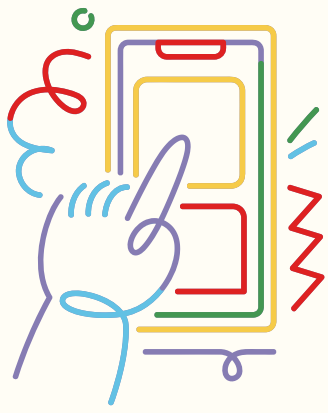


FICHEROS TROYANIZADOS

Son archivos con código oculto que puede ser peligroso. Se detectan con antivirus, análisis de integridad, ejecución en entornos seguros y comprobación de hash en bases de datos online.

FIHEROS CIFRADOS Y PROTEGIDOS

Los archivos con cifrado fuerte no se pueden analizar fácilmente. En cambio, los protegidos con contraseñas simples (como documentos de Office o archivos comprimidos) pueden abrirse con herramientas especializadas.



DATOS OCULTO MEDIANTE ESTEGANOGRAFIA

Ya sea que lo hagas tú o lo delegues a otra persona, tener muy bien organizadas las finanzas de tu emprendimiento te ayudará a que crezca y sea sostenible.

DATOS LOCALIZADOS AMBIENTE DATA

Son datos ocultos en zonas no visibles del sistema, como el file slack o los unallocated clusters, que pueden contener información residual recuperable con herramientas especiales.

WRITE BLOCKERS

Son dispositivos o programas que evitan que el disco duro original sea modificado durante el análisis, protegiendo la integridad de la evidencia.