# Informe Pericial

---

**Nombre:**
Yeray Almoguera González

**Fecha:**
Jueves 5 de Diciembre de 2024

**Firma:**

## Índice



## Índice de figuras

Anexo.pdf

## 1- Juramento y declaración de abstención y tacha

Juramento y declaración de abstención y tacha.pdf

## 2- Palabras clave

**Autopsy**: Herramienta de análisis forense digital de código abierto utilizada para examinar discos duros y extraer información relevante.

**MiTeC Windows Registry Recovery**: Software especializado en la exploración y recuperación de datos almacenados en el registro de Windows.

**Imagen forense**: Copia bit a bit de un medio de almacenamiento, creada para análisis sin alterar el contenido original.

**Hash**: Código único generado matemáticamente que verifica la integridad de los datos.

**Metadatos**: Información asociada a un archivo (como fecha de creación, modificación o ubicación), utilizada para rastrear su origen y uso.

**Registro de Windows (Windows Registry)**: Base de datos del sistema operativo que almacena configuraciones y opciones del software y hardware instalados.

**Evidencia digital**: Datos electrónicos que pueden ser utilizados como prueba en un procedimiento legal.

## 4- Resumen ejecutivo

Este informe pericial presenta los resultados del análisis forense de un disco duro decomisado en una investigación por tráfico de estupefacientes. Utilizando herramientas como Autopsy y MiTeC Windows Registry Recovery, se garantizó la integridad de las evidencias. Se hallaron datos relevantes sobre la actividad de usuarios, archivos protegidos y metadatos, que se documentan en el anexo. El informe concluye con una evaluación objetiva de las evidencias obtenidas.

## 5- Introducción

### 5.1- Antecedentes

Durante un registro policial en un domicilio compartido, se decomisó un ordenador vinculado a un presunto delito de tráfico de estupefacientes. La brigada especializada clonó el disco duro, preservando la cadena de custodia, y envió la imagen forense al laboratorio para su análisis.

El objetivo del análisis fue identificar evidencia digital que relacionara el dispositivo con actividades ilícitas. Este informe pericial detalla los procedimientos y hallazgos, garantizando la integridad de las evidencias.

### 5.2- Objetivos

Los objetivos principales de este informe son:

1. Examinar la imagen forense del disco duro decomisado para identificar información relevante.
2. Documentar las metodologías y herramientas utilizadas durante el análisis, garantizando la reproducibilidad de los resultados.
3. Presentar las evidencias encontradas, incluyendo datos sobre usuarios, archivos y metadatos.
4. Contribuir al procedimiento judicial proporcionando información técnica que ayude a esclarecer los hechos.

## 6- Fuentes de información

Los datos analizados en este informe fueron proporcionados por la brigada especializada del cuerpo policial, quienes realizaron la adquisición de las evidencias digitales bajo los estándares legales y técnicos correspondientes. La fuente principal de información es la imagen forense obtenida del disco duro decomisado, con las siguientes características:

- **Dispositivo original:** Ordenador personal intervenido en el domicilio inspeccionado.
- **Método de adquisición:** Creación de una copia bit a bit mediante herramientas forenses, garantizando la integridad de los datos mediante el cálculo y verificación del hash de adquisición.

En el apartado 6.1, se detalla el procedimiento seguido para la obtención de la evidencia digital, preservando su autenticidad y minimizando cualquier riesgo de contaminación.

Cualquier alteración en los datos originales podría haber modificado el código hash asociado, lo cual no ocurrió, asegurando así la validez de las pruebas analizadas.

**6.1- Adquisición de evidencias**
La imagen forense analizada es una copia exacta, íntegra y no contaminable del contenido del disco duro original decomisado. El proceso de adquisición siguió los protocolos establecidos para garantizar la integridad de las evidencias, preservando la autenticidad mediante la verificación de valores hash. Hashes-Adquisicion-Proyecto2.pdf

## 7- Análisis

### 7.1- Herramientas utilizadas

Para garantizar un análisis exhaustivo y confiable, se emplearon las siguientes herramientas especializadas:

**Autopsy (v4.21.0)**: Herramienta de análisis forense que permite explorar datos, recuperar archivos eliminados y extraer metadatos.

**MiTeC Windows Registry Recovery**: Herramienta para analizar el registro de Windows y extraer información clave sobre usuarios y configuración del sistema.

### 7.2- Procesos

**7.2.1- Imágenes**
Anexo - Documentos de Google

**7.2.2- Documentos PDF**
Anexo - Documentos de Google

**7.2.3- Documentos XLS**
Anexo - Documentos de Google

**7.2.4- Documentos .link**
Anexo - Documentos de Google

**7.2.5- Documentos .url**
Anexo - Documentos de Google

**7.2.6- Archivos .log**
Anexo - Documentos de Google

**7.2.7- Archivos .zip**
Anexo - Documentos de Google

**7.2.8- Datos de navegación**
Anexo - Documentos de Google

**Firma:** 

## 8- Limitaciones

Durante el análisis forense, se identificó un archivo comprimido protegido con contraseña. A pesar de los esfuerzos realizados, no se ha podido acceder al contenido de dicho archivo debido a la imposibilidad de descifrar la contraseña. Esta limitación se detalla en el anexo correspondiente, donde se documentan los intentos de acceso y las herramientas utilizadas para tratar de obtener la clave.

## 9- Conclusiones

En resumen, el análisis forense ha proporcionado evidencia valiosa que puede contribuir a la resolución del caso, a pesar de las limitaciones encontradas. Se recomienda continuar con la investigación de los archivos accesibles y explorar posibles métodos para recuperar el contenido del archivo comprimido protegido.

**Firma:**