

¿Crees tener algo en tu móvil que demuestra tu inocencia?

¿Sabes qué es una prueba **pericial informática**? La ciencia forense digital es una ciencia aplicada sobre la resolución de delitos relacionados con la información informática, sobre el estudio de la evidencia digital, los métodos de búsqueda, obtención y aseguramiento de dicha evidencia.

A medida que el mundo se vuelve más dependiente de la tecnología digital para las funciones básicas de la vida, aumenta el ciberdelito. **Hoy en día, es difícil encontrar un caso que no tenga un nexo con la tecnología informática.**

Soy José Luis Martir Millán, perito informático colegiado y en este artículo te indico todo lo que necesitas saber si deseas usar como prueba digital un mensaje que tienes en tu smartphone para demostrar tu inocencia.



Conoce el [funcionamiento de un laboratorio informática forense](#)

¿Qué es una prueba pericial informática?

La ciencia forense digital es una rama de la ciencia forense que implica identificar, recopilar, analizar y documentar información encontrada en dispositivos digitales. **Estos datos se pueden utilizar como prueba en un tribunal de justicia en relación con un delito cibernético.**

Como especialista en análisis forense digital me suelen contratar para investigar delitos que involucran [Internet](#) y dispositivos digitales como computadoras y teléfonos móviles.

Mediante el uso de técnicas forenses digitales podemos extraer datos de dispositivos y correos electrónicos, acceder a datos encriptados u ocultos, organizar archivos de evidencia para referencias. **Evitando además la manipulación de datos.**

¿Es posible demostrar la inocencia mediante un mensaje en un smartphone?

Para poder usar un mensaje de un dispositivo informático en particular como evidencia probatoria se debe recopilar y preservar de una manera que sea adecuada para su presentación en un tribunal de justicia.

El propósito de la pericial informática es llevar a cabo una investigación estructurada manteniendo la cadena documentada de evidencias y determinar exactamente qué ocurrió en un dispositivo informático y quién fue el responsable.

En otras palabras, se debe llevar a cabo la recuperación de datos con pautas de cumplimiento legal para que la información sea admisible en procedimientos legales.

Para ello, es esencial recopilar la información de manera que se mantenga su integridad. Luego, analizar los datos o el sistema para determinar si se modificó, cómo se modificó y quién realizó los cambios.

¿Por qué es importante la informática forense?

En los sistemas de justicia civil y penal, la informática forense permite garantizar la integridad de las pruebas digitales en los casos judiciales.

La evidencia digital no solo ayuda a resolver delitos en el mundo digital, como el robo de datos, las violaciones de la red y las transacciones ilegales online. **También se utiliza para resolver delitos del mundo físico, como robos, asaltos, accidentes de fuga y asesinatos.**



Todo lo que necesitas saber para [contratar un perito odontólogo](#)

Tipos de análisis forense digital

El análisis forense digital se puede dividir en las siguientes subcategorías:

Informática forense

Rama de la ciencia forense que se ocupa de la identificación, el análisis, la recopilación y el informe de pruebas encontradas en computadoras portátiles, computadoras de escritorio y dispositivos de almacenamiento para su investigación.

Análisis forense de dispositivos móviles

Es una rama del análisis forense digital que se relaciona con la extracción de evidencia digital de dispositivos móviles, a saber, teléfonos inteligentes, dispositivos de juego, dispositivos GPS, tablets, etc.

Consiste en recuperar y analizar la información que contienen los dispositivos móviles, incluidos contactos, mensajes de texto entrantes y salientes, imágenes y archivos de video.

Análisis forense de la memoria

Es un análisis de la memoria de acceso aleatorio (RAM) y la caché de una computadora para identificar e investigar ataques avanzados.

Análisis forense de redes

Es una sub rama del análisis forense digital que se relaciona con el monitoreo, identificación y análisis de actividades / eventos de red para localizar el origen de un ataque a la seguridad. **En la búsqueda de pruebas podemos utilizar herramientas como un cortafuegos o un sistema de detección de intrusos.**

Análisis forense de imágenes digitales

Es un campo de investigación que tiene como objetivo analizar y autenticar la validez de las imágenes digitales (normalmente mediante metadatos).

Forense de Video / Audio

Se relaciona con la investigación de grabaciones de video y sonido digital con el propósito de establecer su autenticidad.

Análisis forense del correo electrónico

El análisis forense del correo electrónico es la práctica de recuperar y analizar el contenido del correo electrónico y cualquier otra información contenida en plataformas de correo electrónico, como horarios y contactos para recopilar pruebas.

Se utiliza en la investigación de delitos relacionados con el correo electrónico, como ataques de phishing, fugas de datos, etc.



Descubre lo que hace un [Perito de Whatsapp](#)

¿Cómo se lleva a cabo el análisis forense digital?

Como perito informático forense he utilizado una variedad de técnicas para adquirir y procesar la evidencia digital disponible.

Algunas de ellas han sido escanear datos en busca de palabras clave específicas, documentar fechas y horas correctas de archivos importantes, detalles de ubicación como direcciones IP, direcciones MAC de servidores remotos y / o computadoras involucradas en los delitos, etc. A continuación, describo los pasos que debemos seguir:

Recopilación de datos

A menudo, esto implica aislar físicamente el dispositivo que se está investigando para garantizar que no pueda ser contaminado o manipulado accidentalmente.

Para ello, hacemos una copia digital, también llamada imagen forense, del medio de almacenamiento del dispositivo. Luego bloqueamos el dispositivo original en un lugar seguro o en otra instalación segura para mantener su estado prístino.

Análisis

Durante el análisis de las copias digitales de los medios de almacenamiento debemos garantizar un entorno estéril al recopilar la información de un caso.

Presentación

Presentamos los hallazgos para que el juez pueda valorar el dictamen pericial forense y determinar el resultado de la demanda. En una situación de recuperación de datos, presentamos lo que se haya podido recuperar del sistema comprometido.



¿Cómo se establecen [los honorarios de los peritos?](#)

¿Necesitas una prueba pericial informática?

Si quieres usar el mensaje que tienes en tu smartphone para demostrar tu inocencia, te recomiendo asesorarte y estar bien informado. **Recuerda que solo un dictamen pericial elaborado por un perito forense colegiado puede dar validez a esa prueba digital.**

Como perito informático forense con una gran experiencia en el ámbito de la obtención y manejo de pruebas periciales, te puedo ayudar. Soy José Luis Martir Millán y me puedes contar directamente a través de lluis@peritinformatic.com www.peritinformatic.com. Además, recuerda que en peritobarcelona.com tenemos un perito para cada especialidad.