

## Servicio de perito informático para conversaciones de WhatsApp en Madrid

En el **servicio de perito informático para conversaciones de WhatsApp en Madrid** estamos conscientes de que la aplicación para teléfonos inteligentes WhatsApp se ha convertido en una de las principales preocupaciones para las investigaciones forenses.

Para quién escribe este artículo, el experto José Luis Martir Millán, es de suma importancia aclarar todos los puntos relevantes sobre este servicio.

Por ello si está interesado, no deje de leerlo y solicitar cualquier aclaratoria a [lluis@peritinformatic.com](mailto:lluis@peritinformatic.com) o en la página web [www.peritinformatic.com.com](http://www.peritinformatic.com.com).



### Servicio de perito informático para conversaciones de WhatsApp en Madrid

Entremos en el tema de **servicio de perito informático para conversaciones de WhatsApp en Madrid**. Esta aplicación (WhatsApp), propiedad de Facebook, es una aplicación de mensajería multiplataforma que ofrece comunicaciones encriptadas, llamadas, mensajes de texto ilimitados e intercambio de archivos multimedia.

**Los usuarios más atentos saben que sus comunicaciones están encriptadas y pueden explotar esta característica para sus propias necesidades.** Este conocimiento, y el hecho de que no hay ningún coste para el usuario final, ha aumentado su popularidad.

#### Definición de términos

En mi trabajo como experto para la obtención de pruebas en procesos judiciales y elaboración de un informe pericial, obtenidas de dispositivos informáticos y en el contexto de este artículo, revisemos algunos términos de uso común.

## 1- Informática forense

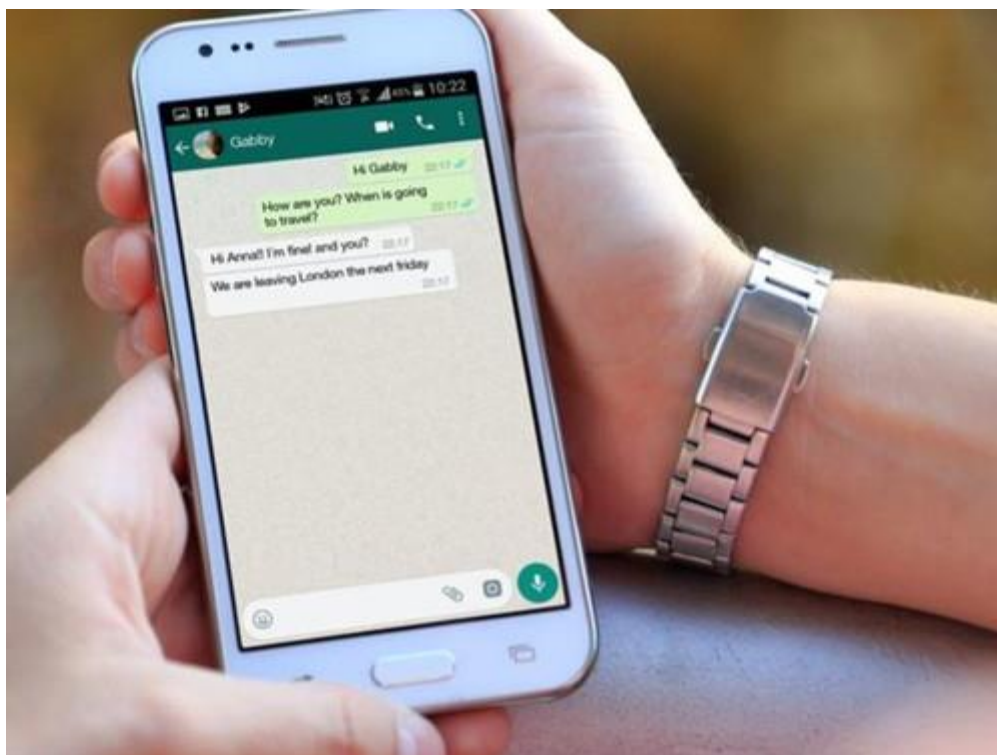
**La informática forense es una de las ciencias forenses que se ocupa de las pruebas legales que se encuentran en los ordenadores y medios de almacenamiento digital.** Muchas áreas de la ciencia se utilizan e involucran en un crimen o caso criminal por un interés legal y de justicia, donde dicha ciencia se conoce como ciencia forense.

## 2- Forense móvil

**La ciencia forense móvil es una rama de la ciencia forense digital que se lleva a cabo para obtener y analizar las pruebas digitales de los dispositivos móviles;** con fines de investigación. Actualmente, la mayoría de los españoles tienen más de un aparato electrónico.

## 3- Visor de WhatsApp

WhatsApp Viewer se utiliza para ver el chat de los [smartphones](#) de WhatsApp que se extrae en el dispositivo del usuario. WhatsApp Viewer tiene la capacidad de mostrar los chats de un archivo msgstore.db extraído de Android.



### **Introducción de datos de WhatsApp como prueba durante un proceso judicial**

Los teléfonos inteligentes ejecutan la aplicación localmente y pueden almacenar fotos, vídeos y mensajes de voz, pero **el contenido de texto de WhatsApp está cifrado y no está disponible de forma nativa para su revisión** a través de una imagen forense del teléfono.

**Al revisar las pruebas directamente en el teléfono, se puede ver el contenido, pero hacerlo puede afectar negativamente a la autenticidad de los datos.** Esto crea potencialmente problemas de manipulación y expoliación al introducirlo como prueba.

En la imagen forense, las fotos, los vídeos y los mensajes de voz pueden ser difíciles de conciliar, incluso con la utilización de herramientas forenses, ya que se extraen sin una marca de tiempo o información del remitente.

### **Las imágenes multimedia no suelen ser recuperables**

**Por el contrario, el contenido de texto puede estar disponible en la nube de WhatsApp, pero las imágenes multimedia, como los mensajes de vídeo y voz, se eliminan del servidor una vez que se envían al destinatario.** Así que, de nuevo, la relación entre el mensaje y el contenido se rompe y hay que reconciliarla manualmente.



**Acceder a los datos de WhatsApp es mucho más fácil con la cooperación del propietario del teléfono**

**Si el propietario del teléfono coopera, proporcionando el teléfono en el que está activa la aplicación y las contraseñas, es posible recoger el contenido cifrado.** Aunque no es imposible, sin esta cooperación será difícil.

**Se puede acceder a los datos en un ordenador**

La app también puede utilizarse en un ordenador, llamado WhatsApp Web, una vez que el usuario permite el acceso a través del teléfono y un código QR.

**Las copias de seguridad de los chats se pueden respaldar en iCloud y en la nube de Google también, lo que presenta múltiples vías para la posible recopilación de contenido relevante de WhatsApp.**

### **Los archivos de WhatsApp que pueden contener pruebas**

Cuando se trata de WhatsApp en teléfonos basados en Android, las bases de datos SQLite llamadas msgstore.db y wa.db son las más importantes, como explico en los siguientes apartados.

### **msgstore.db de WhatsApp**

**Contiene dos tablas.** La tabla de mensajes contiene todos los mensajes de WhatsApp que se han enviado y recibido e incluye el número de teléfono del contacto, el contenido del mensaje, el estado del mensaje (si se ha recibido), las marcas de fecha y hora del mensaje y los detalles de los archivos adjuntos al mensaje.

**Si se envía un archivo adjunto a través de WhatsApp, este tiene su propia entrada dentro de la tabla y el campo de contenido del mensaje es nulo.** Se almacena una miniatura y un enlace a la imagen, y la propia imagen también se almacena en el archivo msgstore.db de WhatsApp.

**La tabla también puede incluir coordenadas de ubicación que pueden permitir a un investigador identificar la ubicación específica de un individuo en ese momento.** La tabla denominada Chat\_list dentro de WhatsApp contiene todos los números de teléfono con los que se ha comunicado.

### **wa.db de WhatsApp**

**El archivo wa.db contiene una lista de los contactos del usuario de WhatsApp, incluyendo el nombre, el número, la marca de tiempo y el resto de la información proporcionada cuando se registró la cuenta.** Los archivos de la base de datos de WhatsApp se almacenan en la memoria del teléfono.

Sin embargo, el archivo msgstore.db puede almacenarse como copia de seguridad en cualquier tarjeta de memoria presente como msgstore.db.crypt, que está encriptado y no puede examinarse sin descifrarlo primero a partir de una clave que normalmente se almacena en la partición de datos dentro de la carpeta de WhatsApp.

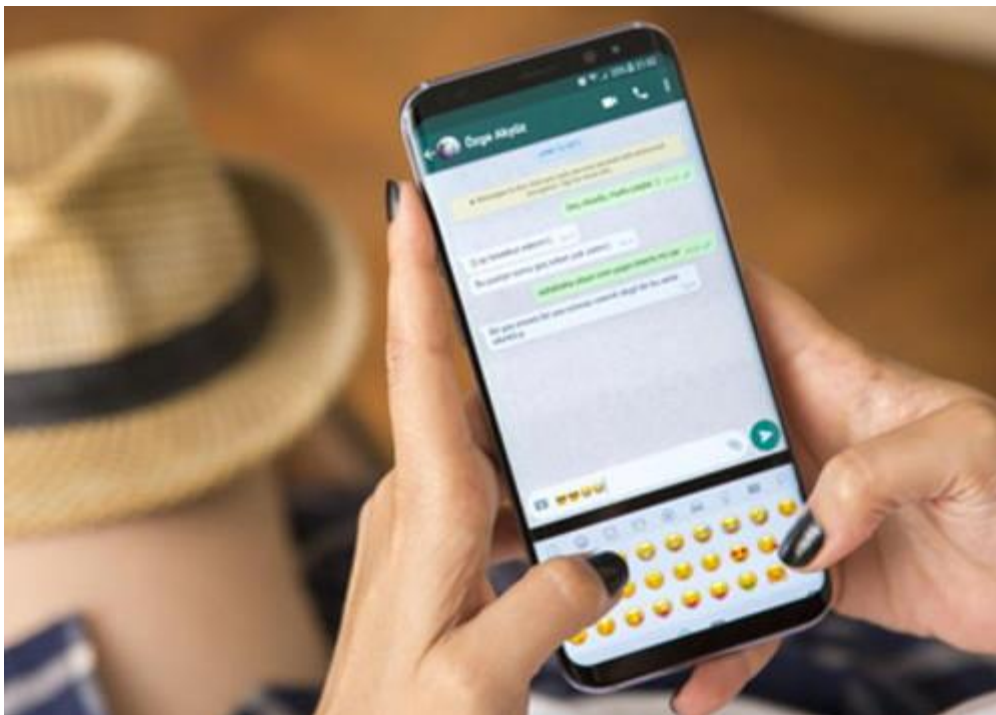


### **Análisis forense de WhatsApp en Apple iOS**

**Apple iOS almacena todos los datos de WhatsApp en una base de datos denominada ChatStorage.sqlite que se encuentra en la ruta del directorio net.WhatsApp.WhatsApp/Documents/ChatStorage.sqlite.**

Las tablas MESSAGE y MEDIAITEM contienen los mensajes, el remitente, el destinatario, las marcas de fecha y hora, la información de ubicación y la ubicación de los archivos adjuntos enviados/recibidos dentro de esos mensajes de WhatsApp.

La aplicación WhatsApp en Apple iOS también almacena una base de datos llamada contacts.sqlite dentro del mismo directorio; que incluye los detalles del remitente y del destinatario, el contenido del mensaje, el estado del mensaje, las marcas de fecha y hora del mensaje y los detalles de los archivos adjuntos al mensaje.



### **Los problemas de compatibilidad presentan otros desafíos**

**Los proveedores de herramientas forenses están actualizando constantemente sus conjuntos de herramientas para seguir el ritmo de las actualizaciones de WhatsApp.** Las compatibilidades entre los dispositivos, los sistemas operativos Android e iOS y las versiones de WhatsApp tienen un impacto adicional en los desafíos forenses.

Lo primero que hago es contactar a cada proveedor con la marca/modelo y la versión del sistema operativo del teléfono que se está investigando y la versión de WhatsApp para ver qué capacidades tiene cada uno para recuperar datos directamente del teléfono.

**Como todas las aplicaciones, WhatsApp cambia constantemente.** El éxito de la recogida de datos de WhatsApp para la investigación forense depende de sus diferentes versiones, de la cooperación del usuario, así como de los perfiles y teléfonos activos.

Al contratar el servicio de perito informático para conversaciones de WhatsApp en Madrid, puedo asesorarte para aclarar cualquier duda, o prepararte un [informe pericial judicial](#) de ser necesario. Puede escribirme al contacto [lluis@peritinformatic.com](mailto:lluis@peritinformatic.com), y con gusto me pondré en contacto con usted.