Guía para la Recolección Correcta de Evidencia Digital en Mensajería Instantánea (WhatsApp)

La Importancia de la integridad en evidencias digitales y los riesgos de las capturas de pantalla.

- **Autor**: Matías N. C. Silva
- **Fecha**: Octubre, 2024

Declaración de Propósito

Este proyecto es de carácter personal y no tiene fines de lucro. Su intención es informar y educar sobre la correcta recolección y preservación de evidencia digital, especialmente en el contexto de mensajería instantánea. Se busca aportar conocimientos prácticos que mejoren la integridad y la autenticidad de las pruebas digitales, reduciendo la dependencia de métodos inseguros como las capturas de pantalla.

Nota: Este material está destinado exclusivamente a fines educativos.

Índice

Introducción

En la era digital, la mensajería instantánea, especialmente a través de aplicaciones como WhatsApp, se ha convertido en una herramienta clave para la comunicación. Sin embargo, la recolección de evidencia digital de estas plataformas es crítica en investigaciones judiciales y personales. Esta guía tiene como objetivo resaltar la importancia de levantar evidencia correctamente, enfatizando las limitaciones de métodos comunes, como las capturas de pantalla. A través de una recopilación adecuada y el uso de herramientas forenses, se busca garantizar la integridad y autenticidad de las pruebas digitales, asegurando su validez en contextos legales.

La Importancia de Levantar Evidencias Digitales Correctamente

En el contexto actual de la evidencia digital, WhatsApp juega un papel clave en investigaciones, tanto a nivel personal como en el ámbito judicial. La manera en que se recopila y se presenta la información de una conversación puede determinar su validez ante los tribunales, su autenticidad y su uso como prueba confiable. Levantar evidencia digital correctamente significa seguir ciertos protocolos y procesos técnicos que aseguran que la información sea veraz, íntegra y, sobre todo, que no haya sido alterada.

Levantar evidencia de WhatsApp de manera profesional implica no solo capturar el contenido visible de los mensajes, sino también **preservar la integridad de los metadatos**. Los metadatos incluyen información valiosa, como la fecha, hora exacta y otros detalles asociados con el origen y destino de los mensajes. Estos elementos se pierden si solo se toman capturas de pantalla. Para que una evidencia sea válida y tenga peso, es fundamental que no haya sido manipulada y que la información esté completa, reflejando la conversación en su totalidad.

Problema: Las Limitaciones de las Capturas de Pantalla como Evidencia en WhatsApp

Uno de los métodos más comunes, especialmente en comisarías y otras instituciones, es tomar capturas de pantalla de conversaciones de WhatsApp para documentarlas. Sin embargo, esta práctica presenta múltiples riesgos y limitaciones:

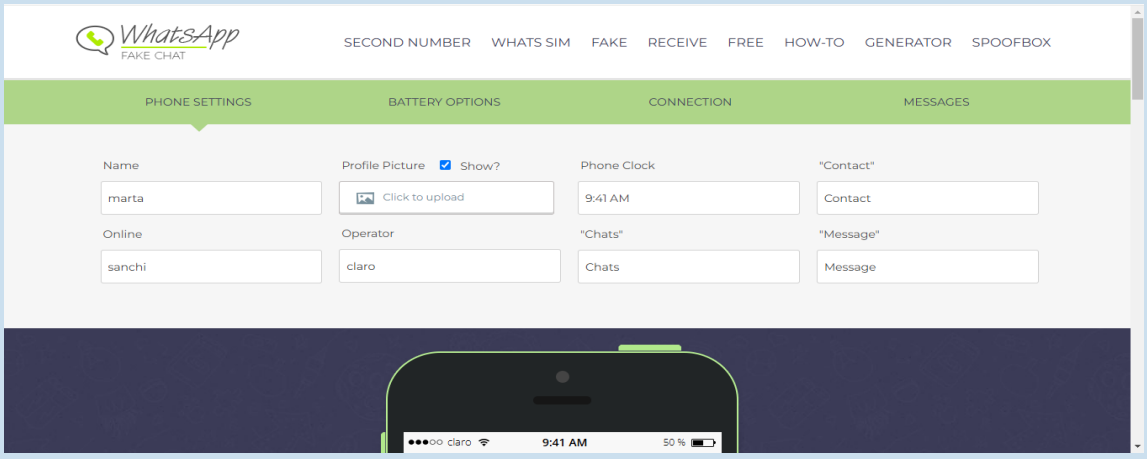
1. **Facilidad de Manipulación**
   Las capturas de pantalla son extremadamente fáciles de editar, ya sea mediante herramientas de edición de imágenes o programas avanzados de manipulación de datos. Por ejemplo: Fakewhats, es sencillo alterar el contenido del mensaje, cambiar el remitente o modificar la hora. Esto presenta un problema grave en situaciones legales, donde cualquier modificación podría poner en duda la autenticidad de la prueba.
2. **Ausencia de Metadatos**
   Las capturas de pantalla no contienen los metadatos necesarios para verificar su origen y autenticidad. Los metadatos pueden incluir detalles como la identidad del emisor y receptor, la ubicación del dispositivo al momento de enviar el mensaje, y hasta los códigos de tiempo exactos que ayudan a rastrear el flujo de la conversación. Sin estos datos, no hay manera de confirmar que la información de la captura sea verdadera y completa.
3. **No Cumplen con los Estándares Forenses**
   En forense digital, la cadena de custodia y la integridad de los datos son fundamentales. Los métodos forenses requieren la conservación de una copia original y la verificación mediante hashing para garantizar que no haya alteraciones. Las capturas de pantalla, al carecer de esta verificación, no cumplen con estos estándares y, en muchos casos, pueden ser rechazadas como evidencia en juicios.

   El **hashing** : es como una "huella digital" para archivos y datos. Se trata de un proceso que convierte cualquier archivo (como un mensaje de WhatsApp o una foto) en una serie única de letras y números. Si el archivo cambia aunque sea un poco, el "hash" o esta "huella" también cambiará, lo que ayuda a verificar que el archivo no ha sido alterado. Para generar esta "huella", puedes usar software gratuito como **HashMyLife** o cualquier página web de confianza que ofrezca esta función. Esto asegura que la evidencia digital sea auténtica y confiable.

Ejemplos: Plataformas y Herramientas de Manipulación de Mensajes (Fakewhats.com)

Las plataformas de edición de mensajes, como fakewhats.com, facilitan la creación de mensajes falsos que imitan la apariencia de WhatsApp. Estas herramientas permiten que cualquier persona diseñe conversaciones ficticias en cuestión de minutos, modificando:

- Nombres de contacto.
- Hora y fecha de los mensajes.
- Contenido de los mensajes, incluso replicando tonos y emojis específicos de WhatsApp.
- Indicadores de recepción y lectura, como los "ticks" azules.

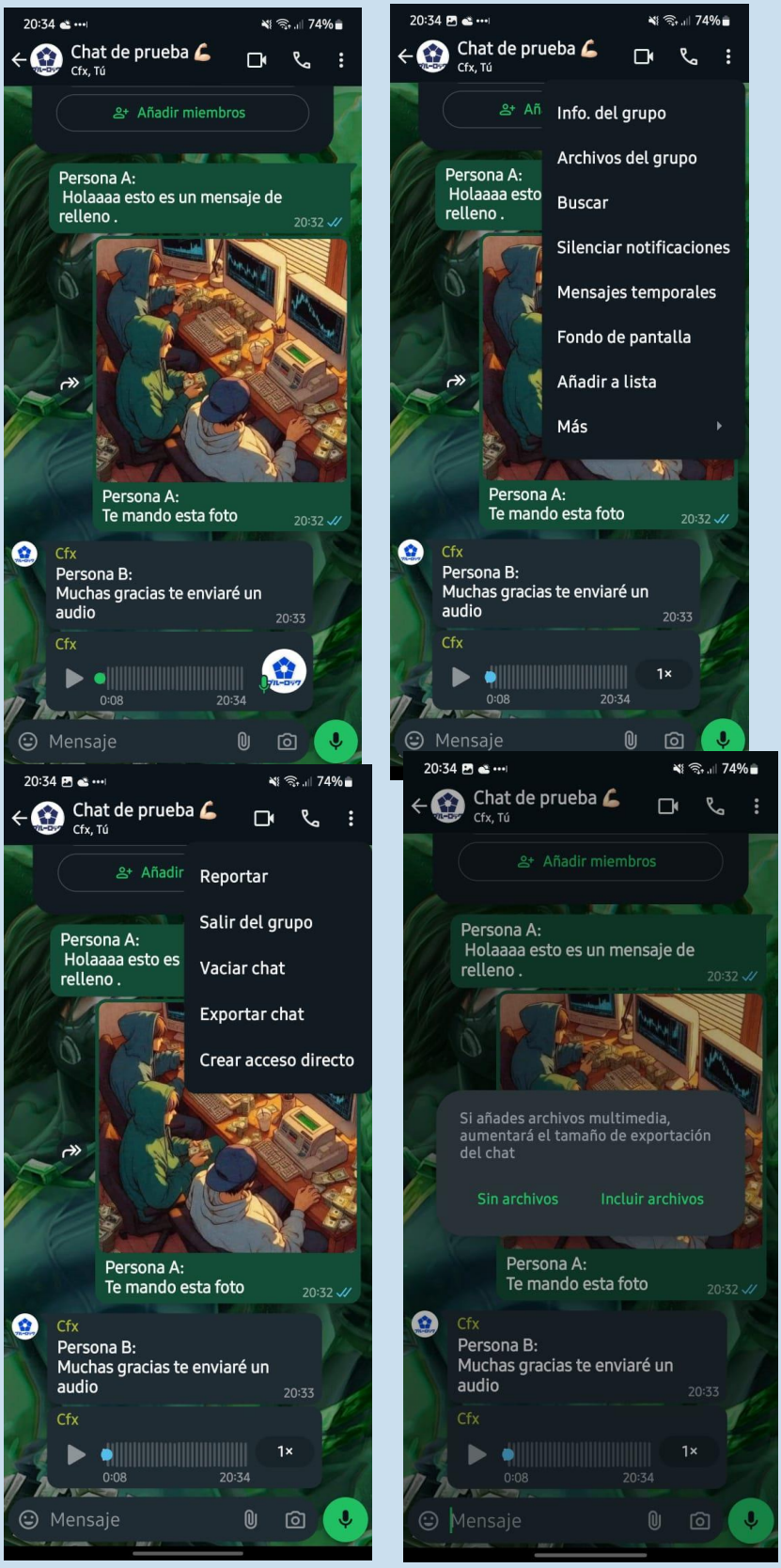


RIESGO PARA LA EVIDENCIA DIGITAL

La existencia de estas plataformas presenta un serio riesgo para la confiabilidad de las capturas de pantalla. Una captura de pantalla falsa puede hacerse pasar fácilmente por una conversación real, y sin una verificación técnica adecuada, es difícil distinguir entre una conversación legítima y una manipulada. En investigaciones, esto puede llevar a acusaciones incorrectas, decisiones judiciales basadas en pruebas poco confiables y a la desestimación de casos por falta de evidencia válida.

En conclusión, es fundamental adoptar métodos que aseguren la integridad y la autenticidad de los datos de WhatsApp. Esto incluye la **exportación de chats** mediante los sistemas internos de la aplicación y la **verificación de datos mediante herramientas de hashing**. También es esencial educar a las fuerzas policiales y a otros profesionales en la recolección correcta de evidencia digital para reducir la dependencia de métodos inseguros y poco confiables.

Manera Correctos para Capturar Evidencia

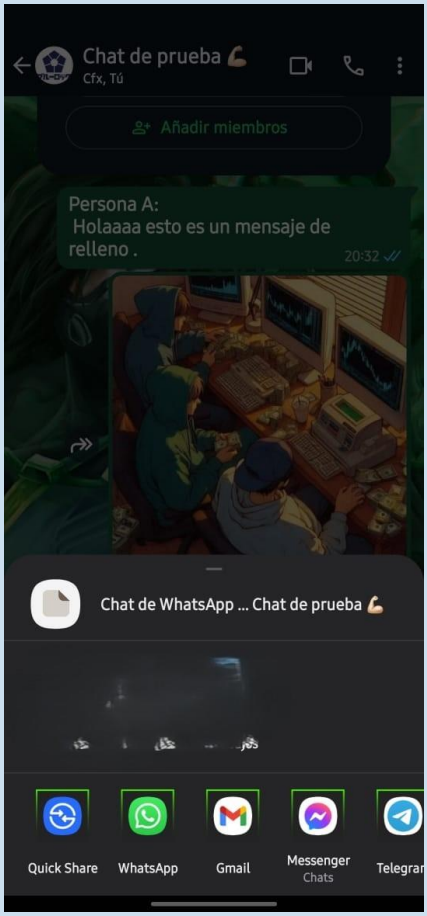


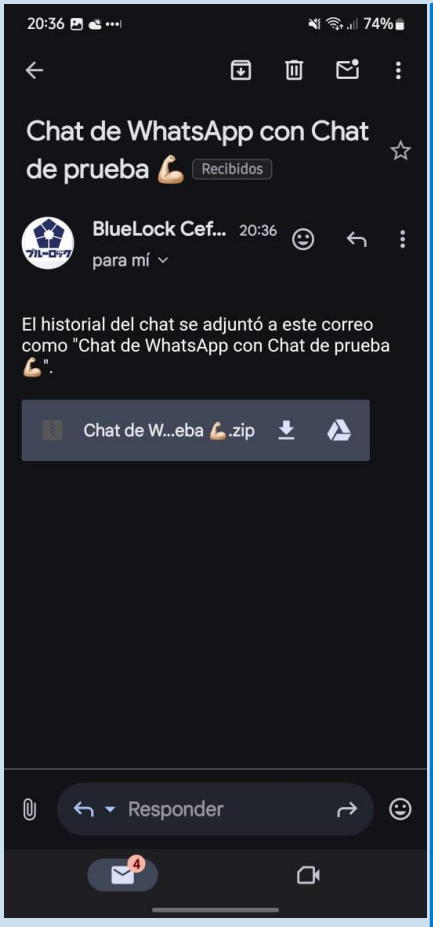
Para exportar un chat de WhatsApp que se desea presentar como evidencia en un caso judicial, se deben seguir ciertos pasos. Al realizar esta acción, se generará un archivo comprimido con la extensión .rar. Este archivo contiene un documento de texto que incluye los mensajes del chat, así como datos importantes como la fecha y hora de cada mensaje. Además, dentro del archivo .rar también se incluirán imágenes, audios y otros archivos que formaban parte de la conversación.

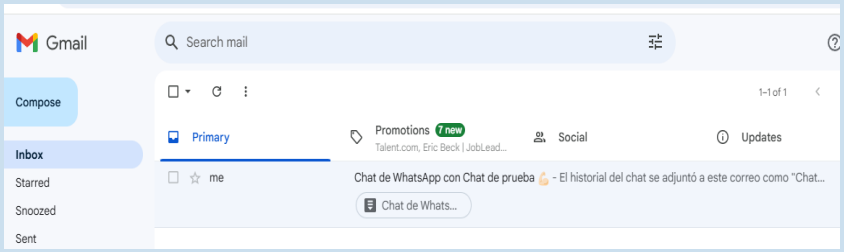
presionar
3 puntitos – mas - exportar chat - incluir archivos

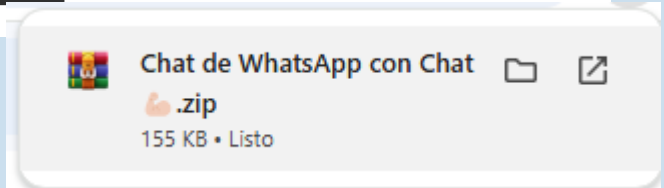
¿Qué es un archivo? rar?

Un archivo .rar es un tipo de archivo comprimido que agrupa varios archivos en uno solo. Esto hace que ocupen menos espacio y sean más fáciles de enviar o almacenar. Cuando descomprimes un archivo .rar, puedes acceder a todos los documentos y archivos que hay dentro, como mensajes, imágenes y audios.

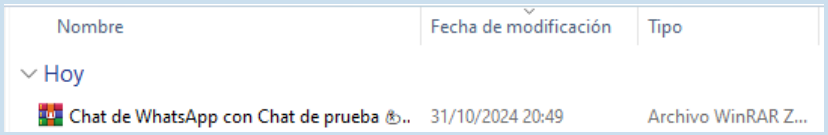


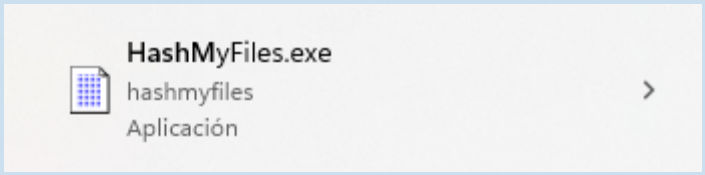


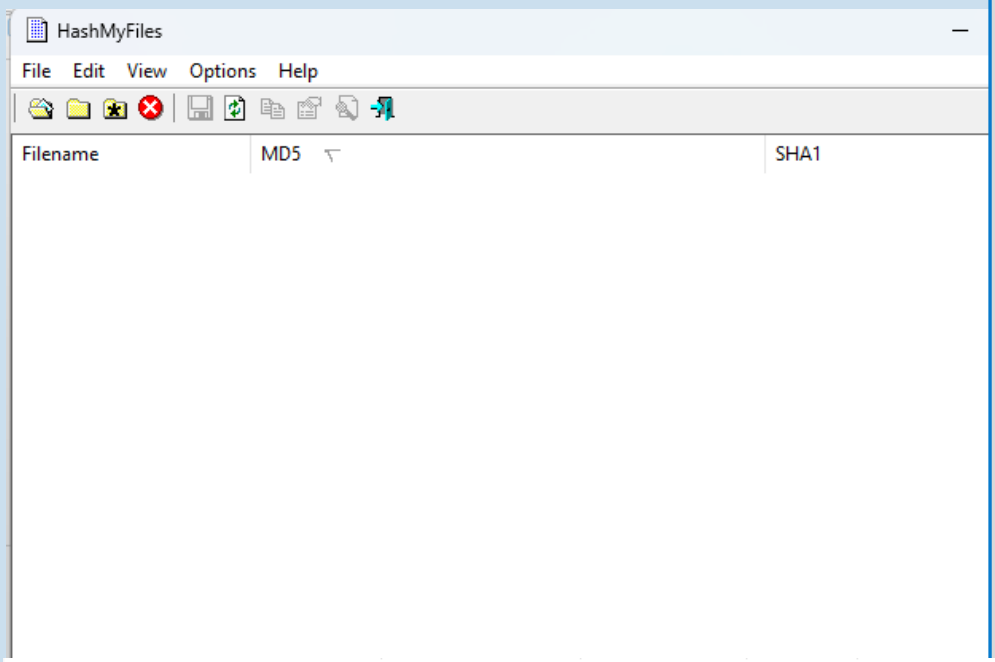


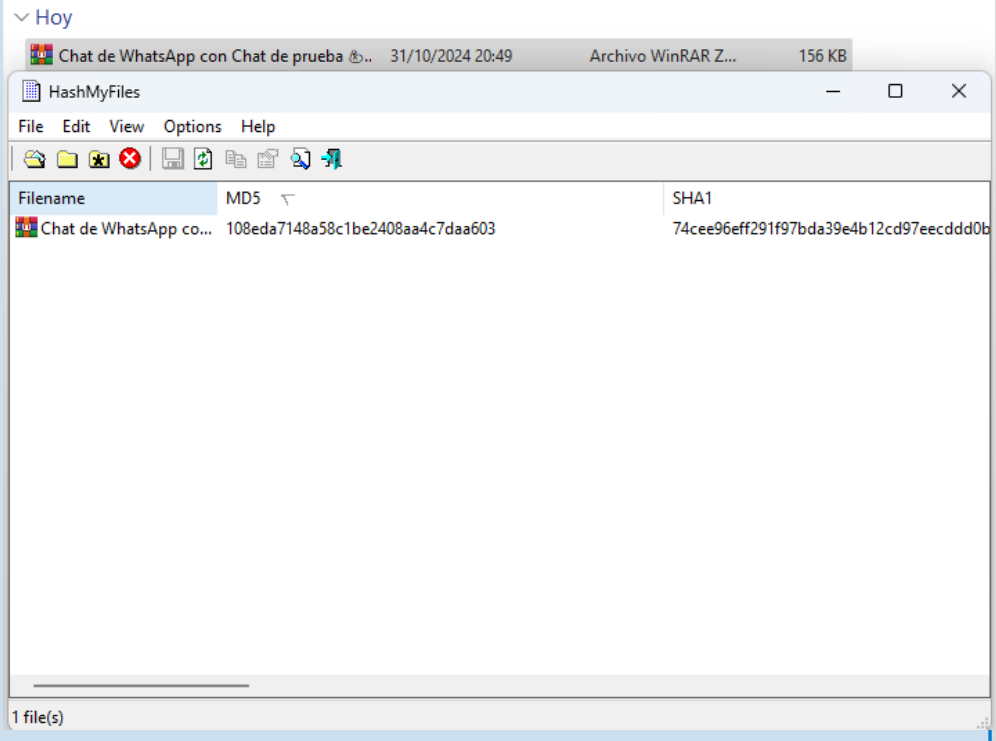


Una vez exportado el chat, seleccionamos la opción de enviarlo por correo electrónico para facilitar su manejo y preservación, aunque también se podría optar por Bluetooth. En este caso, se envió por correo electrónico Es esencial documentar cada paso de este proceso detalladamente, asegurando la transparencia de la evidencia. El archivo exportado suele generarse en formatos comprimidos como .zip o .rar, que son extensiones comunes para conservar la estructura del contenido en un tamaño menor, Una vez completada la exportación y el envío, verificamos la recepción en la bandeja de entrada de Gmail. Si el archivo ha llegado correctamente, procedemos a descargarlo desde la opción "Download" Aquí es importante confirmar el tamaño del archivo descargado (en este caso, 155 KB) para garantizar que no hubo alteraciones durante la transferencia. Finalmente, ubicamos el archivo en la carpeta de descarga predeterminada y, de ser necesario, lo trasladamos a la carpeta designada para evidencias digitales.

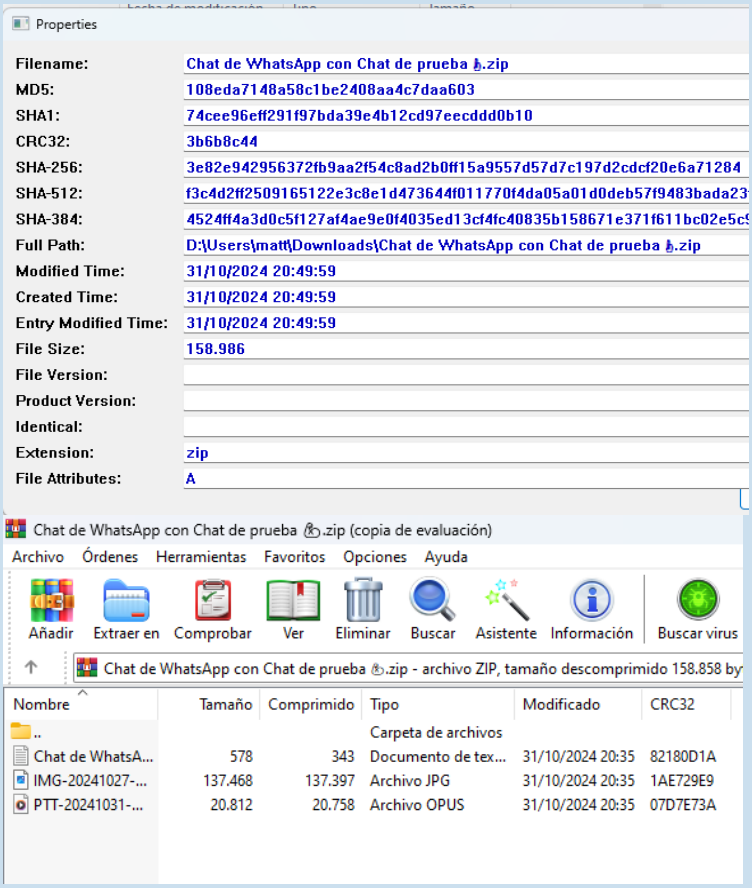


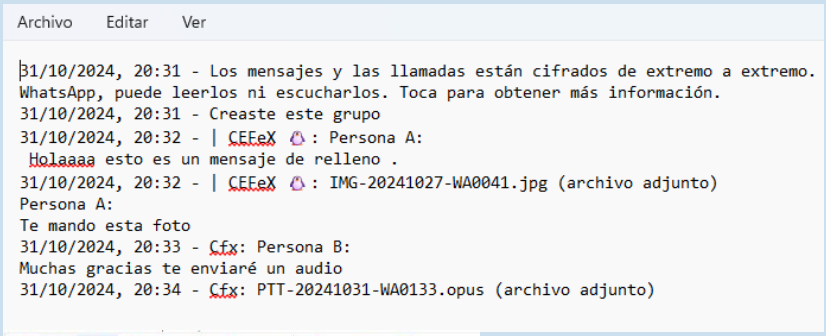


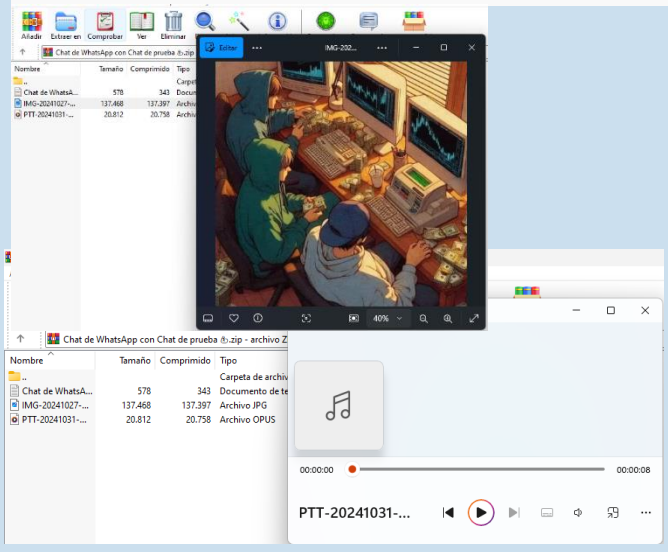




Con el archivo descargado, abrimos el programa HashMyFiles.exe (el enlace de descarga estará en la última página del PDF). Al abrir el programa, arrastramos el archivo .zip o .rar y lo soltamos en la ventana de HashMyFiles. Automáticamente, el programa lee la evidencia y genera un conjunto de números conocido como "hash". Este hash es una especie de "huella digital" del archivo, que permite confirmar su autenticidad y resguardar su integridad a lo largo del tiempo. Es fundamental documentar este número y prestar especial atención al hash generado en el apartado SHA-256, ya que actualmente es el método más confiable para detectar cualquier cambio o alteración en el archivo. Si el archivo fuera modificado de cualquier forma, el hash cambiaría por completo, evidenciando cualquier alteración.







Como podemos observar a la izquierda, al realizar la acción mencionada, obtenemos un cuadro con todos los hash en sus distintas variantes. Más abajo, si ingresamos al archivo .zip, encontramos el chat en formato .txt junto con los archivos multimedia, como imágenes y audios que formaban parte de la conversación. El archivo .txt contiene la conversación detallada, y su importancia radica en los metadatos que alberga. Estos metadatos serán analizados por personal especializado en informática forense, por lo cual es crucial mantener el archivo sin modificaciones para preservar su valor como evidencia.

Un metadato es información adicional que describe detalles de un archivo o un dato específico, como fechas de creación y modificación, el dispositivo usado para su creación y la ubicación geográfica en algunos casos. En informática forense, los metadatos son esenciales, ya que pueden aportar contexto y detalles clave sobre la autenticidad y procedencia de la evidencia digital.

CONCLUSIÓN

La exportación de un chat de WhatsApp para presentarlo como evidencia en un caso judicial es un proceso crítico que debe realizarse con sumo cuidado. El archivo comprimido generado, con extensión .rar, es fundamental, ya que contiene no solo el documento de texto con la conversación y los datos temporales de cada mensaje, sino también archivos multimedia relevantes. **Es importante mencionar que, aunque las capturas de pantalla pueden ser útiles como referencia visual y parte de la evidencia, su uso debe ir acompañado de métodos más robustos de recolección, como la exportación de chats. Al combinar ambos enfoques, se fortalece la integridad y autenticidad de la prueba, brindando un soporte más sólido ante el tribunal.** Es crucial enviar este archivo .rar al órgano fiscal o superior correspondiente, junto con la documentación o acta que detalle el hash generado y los pasos que realizamos para obtenerlo.

La integridad del archivo debe mantenerse intacta, ya que cualquier modificación podría invalidar su valor como evidencia. El hash SHA-256, que sirve como huella digital del archivo, proporciona una forma confiable de asegurar que no ha habido alteraciones. Documentar cuidadosamente cada paso del proceso garantiza la transparencia y la trazabilidad de la evidencia, lo que es esencial para su aceptación en el ámbito judicial. Por lo tanto, asegurar el envío del archivo .rar/.zip y la documentación correspondiente es un paso crucial en la correcta administración de la evidencia digital.

RECOMENDACIONES

- **Conservación Segura:** Mantenga el archivo original sin modificaciones en un medio de almacenamiento seguro, como un disco duro externo (USB) o un almacenamiento en la nube cifrada (Google Drive).

- **Copias de seguridad:** Realice copias de seguridad del archivo .rar y de la documentación asociada para evitar la pérdida de información.

- **Verificación del Hash:** Antes de enviar el archivo, verifique nuevamente el hash para asegurarse de que no se haya producido ninguna alteración durante el proceso de exportación y envío. **Además, considere Hashear las capturas de pantalla, si se utilizan, para garantizar su integridad y autenticidad. Minimice la manipulación de la evidencia para preservar su validez.**

- **Registro Detallado:** Mantenga un registro detallado de todas las realizadas, incluyendo fechas, horas y personas involucradas en el proceso de acciones, para fortalecer la cadena de custodia.

- **Capacitación:** Asegúrese de que el personal involucrado en la manipulación de la evidencia esté debidamente capacitado en procedimientos de informática forense y manejo de datos digitales.

- **Revisión Legal:** Consulte con un asesor legal para garantizar que todos los procedimientos cumplan con las normativas y leyes aplicables en su jurisdicción.

CONTACTO Y REDES SOCIALES

Matías N. C. Silva Auxiliar en Seguridad informática y Forense digital

- **LinkedIn:** Matías Silva
- **Instagram:** Cefex03
- **Correo Electrónico:** Itbluelock@gmail.com

DESPEDIDA

Agradezco su atención y espero que esta información sea de utilidad para la correcta gestión de la evidencia digital. No duden en contactarme para cualquier consulta o aclaración adicional mis redes sociales y correo electrónico se encuentran a su disposición.

HERRAMIENTAS UTILIZADAS

- **HashMyFiles:** https://www.nirsoft.net/utils/hashmyfiles.zip
- **WinRAR:** https://www.winrar.es/descargas/103/descargar-winrar-para-windows-x64-en-espa-ol
- **Video Explicativo:** https://www.youtube.com/@BlueLockIT

¡Gracias por su interés y atención!