

É possível recuperar mídias de visualização única no WhatsApp?

13/03/2026

Essa é uma pergunta que muitas pessoas acreditam ter uma resposta definitiva e ingênua: não. Entretanto, na prática forense digital, a resposta pode ser diferente. Em determinadas circunstâncias, a resposta pode ser sim, inclusive quando se trata de mídias de visualização única que já foram abertas pelo usuário e que, aparentemente, estão inacessíveis em nenhum dos dispositivos envolvidos na conversa (de quem enviou e de quem recebeu).

Figura 1 – Exemplo de áudio de visualização única.

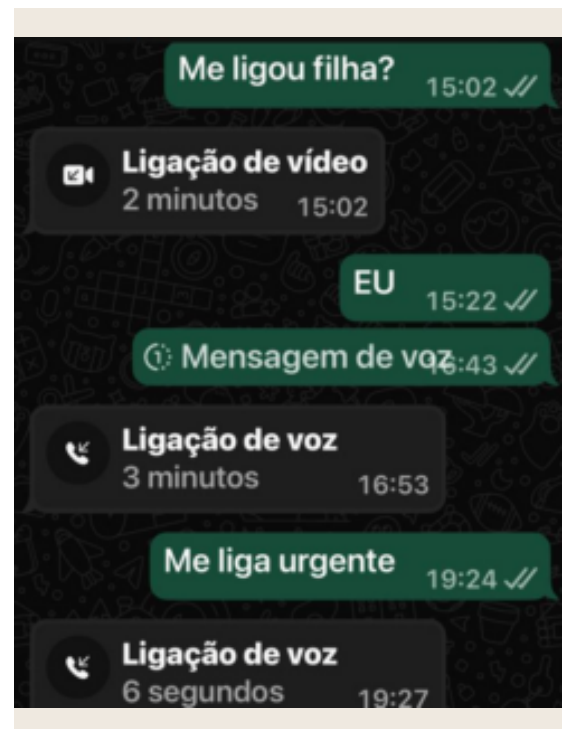
De fato, quando uma mídia de visualização única (imagem, vídeo ou áudio) é aberta no *WhatsApp*, observa-se que, após a visualização, esses arquivos são removidos do dispositivo que recebeu a mensagem. O mesmo comportamento ocorre no dispositivo do remetente: a mídia não permanece armazenada de forma acessível após a visualização pelo destinatário. À primeira vista, pode parecer que o conteúdo foi eliminado por completo. Entretanto, surge a seguinte questão: essa informação pode permanecer armazenada temporariamente em outro local?

A resposta é sim. Pasmem. Ao final assista o vídeo demonstrando como funciona. Antes entenda “como”.

Quando qualquer tipo de mídia é enviada pelo *WhatsApp* (seja de visualização única ou não) o arquivo não é transmitido diretamente de um dispositivo para outro. Inicialmente, o aplicativo realiza o upload da mídia para os servidores da Meta. Antes desse envio, o arquivo é criptografado, sendo armazenado no servidor no formato *.ENC*.

Somente após esse processo, o destinatário pode realizar o download da mídia. Caso o usuário tenha desativado o download automático de mídias, será necessário tocar na mensagem para iniciar o download manual.

O ponto relevante para a perícia digital é que o link de download dessa mídia criptografada e sua respectiva chave de descriptografia estão registrados no banco de dados do *WhatsApp*. Essas informações ficam armazenadas em uma tabela específica denominada *Zmediatem*, em dispositivos *iOS* e *message_media* no Android. As tabelas armazenam metadados relacionados às mídias enviadas e recebidas, incluindo:



- [a] URL do arquivo criptografado hospedado no servidor da Meta;
- [b] Chave criptográfica necessária para realizar a descriptografia do conteúdo

Exemplo de URL de mídia armazenada nos servidores da Meta

```
https://mmg.whatsapp.net/v/t62.7117-  
24/55953391_2332414870600753_2482950450302715659_n.enc?ccb=11-  
4&oh=01_Q5Aa3wG-cWb5NeQsyHuiaEiHSLicNAS6-wWtQR-  
IB1dppOUNnA&oe=69C66515&_nc_sid=5e03e0&mms3=true
```

Exemplo de chave criptográfica armazenada no banco de dados do WhatsApp

```
9a3a0e39605da55e739997ffa25622573dcfb4a51a9e626077d3bf9cf3972383
```

Durante análises realizadas no dispositivo destinatário, observou-se que, após a visualização da mídia de visualização única, além da remoção do arquivo temporário armazenado localmente, a chave criptográfica é removida do banco de dados do aplicativo. No entanto, o link para o arquivo criptografado pode permanecer registrado.

Figura 2 – Banco de dados do WhatsApp

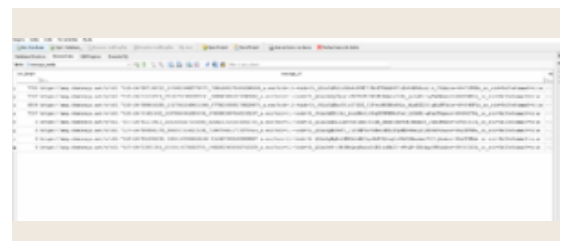
A questão então passa a ser: como recuperar essa mídia?

Estudos demonstraram que, no dispositivo do remetente, tanto o link da mídia quanto a chave criptográfica podem permanecer armazenados e ativos no banco de dados do *WhatsApp*, mesmo após a visualização da mídia pelo destinatário. Dito diretamente: significa que, em determinadas circunstâncias, é possível recuperar mídias de visualização única a partir do dispositivo de quem enviou o conteúdo.

De posse do link e da chave criptográfica (e considerando que o link permanece ativo nos servidores da Meta por um período aproximado de até 15 dias) o perito pode realizar o download do arquivo criptografado e posteriormente executar o processo de descriptografia utilizando a chave associada.

O procedimento pode ser automatizado por ferramentas forenses especializadas, dentre elas:

- [a] [Avilla Forensics](#)
- [b] [Iped \(Indexador e Processador de Evidências Digitais\)](#)



Essas ferramentas são capazes de identificar os registros no banco de dados, realizar o download do arquivo .ENC e executar a descriptografia, reconstruindo a mídia original.

Entretanto, para que a recuperação seja possível, o tempo é um fator crítico. Após determinado período, os links armazenados deixam de estar ativos nos servidores da Meta, impossibilitando o download da mídia.

Por esse motivo, é altamente recomendável que a perícia seja realizada o mais rapidamente possível e, sempre que viável, em ambos os dispositivos envolvidos na comunicação. Isso se deve ao fato de que a recuperação das mídias geralmente depende das informações ainda preservadas no dispositivo do remetente, ou em ambos os dispositivos caso cada usuário tenha enviado mídias de visualização única na mesma conversa.

Caso prático de aplicação da técnica

Um caso real em que essa técnica foi aplicada ocorreu em março de 2026, quando foi possível recuperar um áudio de visualização única, já visualizado pelo destinatário, em um iPhone 14 (iOS 26.3). O conteúdo possuía extrema relevância para o caso e, após a visualização, havia se tornado completamente inacessível em ambos os dispositivos envolvidos na comunicação.

A situação teve início em uma conversa aparentemente comum entre uma avó e seu neto. Durante o diálogo, a criança revelou algo que até então nunca havia sido mencionado: relatou que um conhecido da família teria cometido abusos sexuais.

Diante da gravidade da situação e visivelmente abalada, a avó decidiu registrar aquela conversa. Por meio do *WhatsApp*, gravou um áudio com o intuito de encaminhar o conteúdo a um familiar que residia nos Estados Unidos. Entretanto, sem perceber, enviou o áudio com a opção de visualização única ativada.

O destinatário chegou a visualizar o conteúdo, porém, logo em seguida, o acesso à mídia foi perdido, tanto para quem recebeu quanto para quem enviou a mensagem.

Sem saber se seria possível recuperar aquele material, a família decidiu encaminhar o caso para análise pericial especializada.

Após a realização dos procedimentos técnicos descritos anteriormente, foi possível obter êxito na recuperação do áudio, demonstrando, na prática, a viabilidade da técnica de recuperação de mídias de visualização única em determinadas circunstâncias.

Mas, se você ficou cético, assista ao vídeo em que o subscritor Daniel Avilla mostra como funciona [\[link aqui\]](#).

Se quiser saber mais sobre o tema, Daniel e Joaquim ministram um curso sobre o tema neste sábado (14/3): “A prova mais perigosa do processo penal: celular” [\[saiba como funciona aqui\]](#)





E mais uma coisa: a tecnologia é cabulosa; prega peças. Por enquanto, a possibilidade de recuperar os registros desaparece em cerca de 15 dias. Então, respire parcialmente aliviado. De qualquer forma, no caso, todo cuidado deve ser “master”.

P.S. Lembre-se que as inovações não param. Dentre elas, aplicativos de mensageria sem uso da internet/web que dispensam acesso à rede ou consumo de dados e que funcionam em smartphones, como o bitcht [confira [aqui](#), baixe na [apple store](#) ou na [google store](#)]. Mas isso é tema de outra coluna, com novas perplexidades e desafios.

Referências:

AVILLA, Daniel Hubscher. Avilla Forensics: Mobile Digital Forensics Tool. GitHub, 2021. Disponível [aqui](#).

META. Enviar fotos e vídeos de visualização única no WhatsApp. Central de Ajuda do WhatsApp. Disponível [aqui](#).

NASSIF, Luís Filipe et al. Iped — Indexador e Processador de Evidências Digitais. GitHub, Polícia Federal Brasileira, 2019. Disponível [aqui](#).

Fonte: <https://conjur.jumps.com.br/2026-mar-13/e-possivel-recuperar-midias-de-visualizacao-unica-no-whatsapp/>