Consilio

Global Leader in Legal Consulting & Services

Recovering Deleted WhatsApp Messages

By Dr. Tristan Jenkinson

Recovering Deleted WhatsApp Messages

White Paper

Introduction

WhatsApp, the popular instant messaging system, was reported to be the most downloaded Android app in the world in 2018 with nearly 750 million downloads. With its more than 1.5 billion active users across the globe over 60 billion messages are sent or received per day.

As WhatsApp usage has grown, requests for productions from the chat application have become more frequent. One of the most common requests that we have received about producing WhatsApp messages is whether it is possible to recover messages that have been deleted by a user.

While the short answer is that yes, it is possible to recover deleted WhatsApp messages, the process is not *always* guaranteed. In addition, it may be possible to recover fragments of a message, or the content of the messages without the details, such as the date the message was sent and who the messages were sent from or to.

The "recoverability" of deleted WhatsApp messages depends on many variables making it difficult to ascertain in advance. Ruling out these variables often requires collecting the relevant data from the phones, performing intermediate processing, and conducting cursory examination using review software. In some circumstances, even the options to extract WhatsApp messages that have not been deleted may be limited.

A Brief Guide to WhatsApp Terminology

To understand some of the complexities involved in the recovery of deleted messages, some of the terminology used by WhatsApp can provide some important context.

In particular, because of the options and the different ways in which they are treated, it is helpful to distinguish between the below terms:

- **Messages** – Messages are individual communications which are sent or received.
- **Chats** – These are effectively conversations – all the current (i.e., not deleted) messages between you and a (single) contact.
- **Group Chats** – WhatsApp allows for the creation of "Groups" so that multiple people can communicate on the same chat. These are similar to Chats as above, but can involve 2 or more people and must have at least one administrator, who can invite members, etc.

A list of current Chats and Group Chats are available on the main screen so that the user can select the chat that they want to review or post a message in. Alternatively, they can create a new Chat or Group Chat.

For Chats (conversations as opposed to messages) there are several options available;

- **Delete** – If a Chat is deleted, the content is removed and is no longer accessible within WhatsApp. In addition, the entry for the Chat (or Group Chat) is removed and no longer available from the main page.
- **Clear** – This is similar to the delete option, all Messages from the Chat will be removed, but the entry for the Chat will remain on the main page.
- **Archive** – The Chat and all Messages contained therein at the point of archival are saved in an archive location, rather than deleted. These messages are not removed from the database and can be viewed within WhatsApp.

It is worthy of note that Group Chats can be cleared by a user, but they can only be deleted after the user leaves the relevant group.

When deleting Messages (as opposed to Chats) there are several options available;

- **Delete (For Me)** – This option deletes the local copy of the message, however, other users having received the messages would still have a copy of that messages, unless they have also decided to delete it.
- **Delete (For Everyone)** – This option deletes all copies of the message, including those on other recipients devices. It is only possible for a user to select this option for messages that they have sent and it is only available for a specific amount of time (just over 1 hour) after sending the message. This option was intended as a way to delete miss-sent messages.

Note that there is no "Clear" option for single messages – this is only available for Chats and Group Chats.

A High-Level View of How Applications Such as WhatsApp Work

To understand why it is not always clear whether a message may be retrievable, it is helpful to discuss how the messages are stored, as this provides an insight into this issues that can have an impact on the recoverability of a deleted message.

WhatsApp, like many applications designed to run on mobile devices, uses an SQLite database for its storage. This is a database system that is designed to use a small amount of storage, and is not platform specific, so is perfect for applications such as WhatsApp, which runs on multiple platforms such as Android and iOS (the iPhone Operating System).

Database systems contain tables and records. Each table would not be dissimilar to a sheet in a spreadsheet, whereas each record would be a row in that spreadsheet. In the context of instant messages, there may be a "Messages" worksheet (Table) and each message is a row on the sheet with different columns for information such as who the messages was to, from and relevant time and date information, as well as the content of the message itself, as below;

From	To	Date & Time	Message
Bob	Alice	16 Apr 2019 11:34 (UTC)	Have you deleted all of the evidence?
Alice	Bob	16 Apr 2019 11:39 (UTC)	Not yet – will do so tonight.

The way in which records (i.e. the messages and information about them) are stored therefore become a key consideration when considering if (and how) deleted messages can be recovered.

With SQLite, the exact mechanics of what happens upon the deletion of records in the database is dependent on the application which is using the database. The simplest (and quickest) solution is to leave the data in place and remove the references to it. This means that effectively the application which is using SQLite can no longer 'see' the data (as there are no references to it), but the content is still actually present in the database itself. This is effectively the way that many single message deletions are dealt with in instant messaging systems such as WhatsApp. The fact that the data remains in the database means that it can be recovered by analysing the database itself.

Why it is Not Always Possible to Recover Deleted Messages

Given the above explanation of how applications such as WhatsApp work, it may appear that it is always possible to recover deleted messages because although the deleted message is no longer displayed within the application, it still exists within the database.

There are, however, two main reasons deleted messages might not being recoverable;

Access to the Database

In order to recover deleted items from the database, it is necessary to have access to the database. The database itself is typically stored in an encrypted manner, so it would be necessary to have access to the key in order to decrypt the database. This is not always straightforward or possible. If it is not possible to gain access to the database and decrypt it, then this approach to recovering deleted messages will not be successful.

"Vacuuming" the Database

Where deletions are performed by removing references to data, the areas containing the deleted messages could then be reused, but will likely be "sandwiched" between other data. This makes the logistics of inserting new messages in that space difficult. The result is that these areas not being reused, meaning that the database is larger than it needs to be and with each deletion, insertion or update, the database gets increasingly inefficient.

SQLite uses a command called "Vacuum" to rebuild the database, removing the spare space, and repacking the information into smaller space, making it more efficient[1]. After "vacuuming" a database, it is not typically possibly to recover deleted messages, as the database has been rebuilt to use the space that they once occupied.

A Note on Data Which is Overwritten on Delete

As noted above, while removing the reference to messages in order to effectively delete them is a quick and simple method – it is not the only method, since the mechanics of how a message is deleted is down to the application which is using SQLite for its storage. Some applications will overwrite the information that is being deleted, so that it cannot be recovered.

While this doesn't currently apply to WhatsApp there would be nothing preventing them from implementing such an approach in any update to the application. If this was to happen, then it would not be possible to recover content from messages – though there may be other approaches, as discussed further below.

Trigger Points

One of the difficulties with the recoverability of deleted messages stems from the use of the "vacuum" operation, which could be triggered by several potential events, including:

- The amount of usage within the WhatsApp application – the more the database is used, the more inefficient it becomes. This is not ideal for the application's user experience, and it would seem likely that there may be an internal trigger which would cause the database to automatically perform the vacuum operation as a result.
- The deletion of Chats, as opposed to Messages – If a whole chat was deleted, as opposed to just one message, this could potentially result in a lot of fragmentation, as many individual Messages may have been removed. Clearing or deleting chats could result in vacuuming being triggered, whereas the deletion of individual messages may not.
- Other applications could potentially trigger vacuuming to be carried out on the WhatsApp database. Software is available which is designed to "wipe" deleted messages from WhatsApp applications. Although this is not something specifically investigated for this article, it is likely that this uses the vacuum function, and may well identify and overwrite any dropped messages prior to executing the vacuum function.
- Similarly, there could be settings on a device which allow a user to clear space on their device. Once way to do this would be to remove the unused space within the SQLite databases stored on the device, so this could potentially be another trigger point.
- It is also worth considering that WhatsApp is continually changing, (at the time of writing, the current android version for download is version 2.19.105), potentially each of these different updates could (even unintentionally) effect the recoverability of deleted messages, for example by triggering vacuuming.
- Different operating systems (for example Android or iOS on iPhones) use different versions of the programme, so the same usage on an iPhone could result in deleted messages being lost, whereas the same specific usage on an Android device may not.
- The storage used on the device is also a consideration. The storage chip within a mobile handset, independent of applications (or databases), can affect the status of message data. This is because the storage chips are continuously trying to maximise their own efficiency.

[1] It serves a similar function to defragmenting a hard drive.

Other Methods for Recovering Message Content

If there is no longer information residing in the WhatsApp SQLite database itself, there may still be some locations which could be analysed to retrieve some content, though this may only be fragments of chats, without the relevant metadata.

Write Ahead Log

When data is being written to the database, there can be a problem that interrupts this process, and the system may not know if the write failed, was partially written, or was completed successfully. To address this problem, SQLite uses a "Write Ahead Log" ("WAL"). This is a log which records all changes to be made to the database, typically including information to enable the action to be undone or rerun.

This means that all information written to the database, for instance, messages, will have been written to the WAL prior to them being placed into the database itself. Therefore, the WAL may potentially contain some content from deleted messages. However, once the messages have been written and confirmed to be successful, the WAL is effectively redundant, and so would also be subject to permanent deletion, overwriting etc., to improve efficiency and performance. It is possible that the messages from these logs may only exist in a truncated form.

Search Indexes

In order to assist with searching chats, SQLite can use an additional database (under the Full Text Search extension). This database can potentially contain content of messages, though it is not clear under which circumstances the database is populated, or when the content is irretrievably deleted. If the additional database is in use to aid with search functionality, then once the relevant messages are deleted, the corresponding entries in the search database would become obsolete and would likely be subject to deletion or vacuuming in the same manner as the main database.

Temporary Copies

It is possible that old information which has since been deleted from the current database may be recoverable from temporary copies which have been created but deleted. To access these would require full access to the underlying physical media on which the data was stored which may not be possible, depending on the device.

Other Information to Consider

For iPhones it is possible that backups of the chat data may be stored in iCloud, while for Android devices it is possible that backups are saved to the user's Google Drive account, either of which could also be useful to recover messages which have since been deleted.

In addition, full phone backups may have been completed, which may contain chat backups from the time that the backup was completed, providing a good opportunity to recover messages that have since been deleted.

In Summary

While it can be possible to recover deleted WhatsApp messages, there are several factors which can impact efforts to recover them. Without access to the devices and the use of specific forensic tools, it is virtually impossible to determine if deleted messages from a particular device at a particular time would be recoverable.