



WhatsApp Forensics on Smartphones

WhatsApp is a popular chat app, which provides free cross-platform messaging and VoIP services to its users.

In this article, we intend to examine WhatsApp from a forensic standpoint (as an application found) on Android and iOS devices. We will briefly review the data extraction process involving this app and the artifacts associated with it.

And finally, you will learn what data you can extract from a suspect's smartphone using Belkasoft Evidence Center.

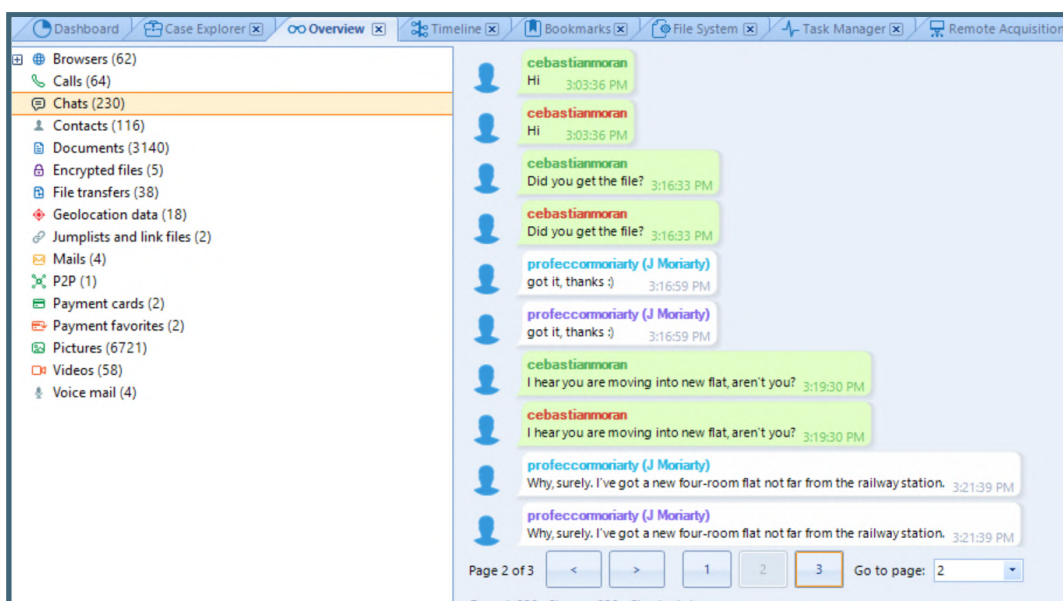


Figure 1 – WhatsApp chat history extracted from a smartphone shown in Belkasoft Evidence Center

Why is WhatsApp an important source of information?



Figure 2 – WhatsApp on a smartphone

With over 2 billion users in 180 countries, WhatsApp is by far the most popular and widely-used messaging application across smartphones.

And with over 100 billion messages sent every day on the platform, WhatsApp is easily one of the most frequently used apps on mobile devices.

Therefore, the chances of WhatsApp being the application housing important messages or correspondences are quite high.

In the last few years, WhatsApp implemented new features like end-to-end encryption, which made decryption of intercepted messages over the air practically impossible.

While users and privacy advocates welcomed the new setup supposed to keep their messages more secure, it spelled trouble for law enforcement agencies who had to find new methods of obtaining suspects' communications history.

WhatsApp does not keep messages on its servers. Messages and notifications (for unanswered calls, for example) are stored on the server

temporarily (until they get delivered). For this reason and others, WhatsApp data stored on the smartphone memory or cloud (iCloud, for example) provide the only means through which investigators get to access suspects' communications.

Note: WhatsApp can be accessed on desktop computers (on popular browsers) through WhatsApp Web, which is simply an extension or mirror for the WhatsApp app installed on a mobile device. WhatsApp also provides applications for the Windows and macOS platforms. However, WhatsApp forensics for those apps on PCs and Macs are beyond the scope of our work in this guide.

WhatsApp on Android devices



Figure 3 – WhatsApp on the menu screen of an Android smartphone

On smartphones running Android, WhatsApp houses its chat database in a sandbox.

New Android devices are configured to exclude that chat database from ADB backups. And, in theory, this means root access is required to access the chat database.

Potential case 1: Downgrade WhatsApp to get an unencrypted backup file

You might be able to access the WhatsApp database on an old non-rooted smartphone by sideloading a special (old) WhatsApp version and instructing it to bring back the original (unencrypted) database to the host.

Old WhatsApp versions (before a specific date) lack the encryption function. Therefore, by downgrading the app to bring back an old WhatsApp build while not deleting the user's data, you can obtain an unencrypted backup file.

You can then extract WhatsApp data from the created file. The procedure described here will not work on new Android devices, though.

Potential case 2: Decrypt an available backup—if you have the means to do so

On some Android devices, you might find standalone backups, which were created for WhatsApp. Those backups are usually encrypted.

Encrypted WhatsApp backups usually appear as **.cryptXX** where **XX** is a number.

To access the backup, you have to decrypt it using an encryption key that is stored in the WhatsApp sandbox. Well, this brings you back to the sandbox, which can only be accessed with superuser permissions (if the device has been rooted).

Potential case 3: Access the original database—if the device is rooted

Then again, if you have superuser privileges, then you are better off getting what you need from the original WhatsApp database in the application sandbox instead of getting data from a backup.

It makes sense for you to get data from a backup only when you are sure the data you need is in that backup.

Note: WhatsApp only creates backups when users configure the app to do so. The backups are optional; users can disable the backup setup.

WhatsApp backups typically contain chats and pictures. Some backups might contain videos. You are unlikely to find contacts in WhatsApp backups.

The chats package in WhatsApp backups is usually encrypted, but the media files are left bare.

Where does WhatsApp keep its data on Android devices?

WhatsApp application files on Android devices are housed in **Userdata** directories (where regular user data is stored). You might still find some subdirectories and programs files in the folders along this path:

/data/data/com.whatsapp/

There are two important databases:

- **wa.db**

From the **wa.db** database, you get to access the full list of the WhatsApp user's contacts (and phone numbers), displays names, timestamps, and similar details.

- **msgstore.db**

From the **msgstore.db** database, you get information on conversations or sent messages, such as contact numbers, the contents of the messages, status, timestamps, information on attached files, and similar data.

The databases above house all the valuable WhatsApp artifacts.

WhatsApp might end up storing its stuff on an SD card—if space on a smartphone's memory is limited or if the device has to conserve space. In such a scenario, you will find a WhatsApp folder on the SD card's root directory. In that folder, you are likely to see the **Share**, **Trash**, and **Databases** subfolders.

- **Share** houses copies of files that got sent to other WhatsApp users
- **Trash** keeps some deleted files
- **Databases** stores encrypted backup copies, which can be decrypted using the key file (extracted from the device's memory).

Note: Some Android devices—especially those running modified Android builds (with altered settings)—store WhatsApp artifacts in locations that differ from the above.

Xiaomi smartphones, which have the Second Space feature enabled, for example, might store WhatsApp data in the directory equivalent paths based on the function's rules (for example, in **/data/user/10/**) instead of the regular directory used by other Android devices (in **/data/user/0/**).

WhatsApp on iOS devices



Figure 4 – WhatsApp on the menu screen of an iPhone

Potential case 1: Get the backup from iTunes

On iPhones and iPads, the easiest method of accessing WhatsApp conversations requires you to acquire and analyze the backup from iTunes. The WhatsApp data in such backups are not encrypted.

If a password was set, though, you will have to enter the password. Alternatively, in such a scenario, you can try recovering the password or resetting it on the device involved.

Potential case 2: Get the backup from iCloud backups

WhatsApp data also exist in iCloud backups, so you might want to check for them there too. The WhatsApp data stored in iCloud backups are similar to those stored in iTunes-style backups. They are unencrypted.

To access a user's iCloud, though, you will need to enter the user's credentials and use two-factor authentication (if the user set it up) or an authentication token.

In any case, once you manage to gain access to a user's iCloud, you will find it easy to retrieve whatever WhatsApp data is hosted there.

Potential case 3: Get the standalone backup from iCloud or a similar storage facility

Some users configure WhatsApp on their iOS devices to create standalone backups, which are stored on the iCloud drive.

WhatsApp standalone backups on iCloud drives are encrypted, so you will have to decrypt them first to view the conversations in them.

The same thing goes for standalone WhatsApp backups stored on Google Drive, OneDrive, and other cloud storage facilities.

Where does WhatsApp keep its data on iOS devices?

In contrast to Android devices, which store WhatsApp data in multiple SQLite databases, iOS devices store all WhatsApp data in a single database (**ChatStorage.sqlite**).

You can find the database in the folder along this path:

net.whatsapp.WhatsApp/Documents/ChatStorage.sqlite

If the WhatsApp data exists on an iTunes backup—which means you will not have to extract data from the device file system or create a memory dump—then you can access most of the relevant information from the

ChatStorage.sqlite database inside the backup. And in this case:

- The file typically exists along this path:
/private/var/mobile/Applications/group.net.whatsapp.WhatsApp.shared/
- Or you might find it displayed in some programs path this way:
AppDomainGroup-group.net.whatsapp.WhatsApp.shared

In the **ChatStorage.sqlite** database for WhatsApp, the ZWAMESSAGE and ZWAMEDIAITEM tables are the most important of the lot.

They store items containing data corresponding to messages, sender and recipients, timestamps, geolocation data, path/location of media that got shared between contacts, and so on.

Besides the **ChatStorage.sqlite** database, you should see the **Contacts.sqlite** data in the same location. From the latter, you might be able to extract some additional details about a user's WhatsApp contact, but you are unlikely to find the unique identifier for individual contacts.

Extracting WhatsApp data from smartphones using Belkasoft Evidence Center

Belkasoft Evidence Center (BEC) is a digital forensics tool used to acquire, search, analyze, store, and share digital evidence from computers, smartphones, RAM, and cloud services.

To illustrate how digital forensics tools work with WhatsApp databases from smartphones, we will walk you through the data extraction process from an Android device using Belkasoft Evidence Center.

Sample procedure: Acquiring data from an Android physical backup

From the **Add data source** screen in BEC (figure 5), you can create a backup for a suspect's device.

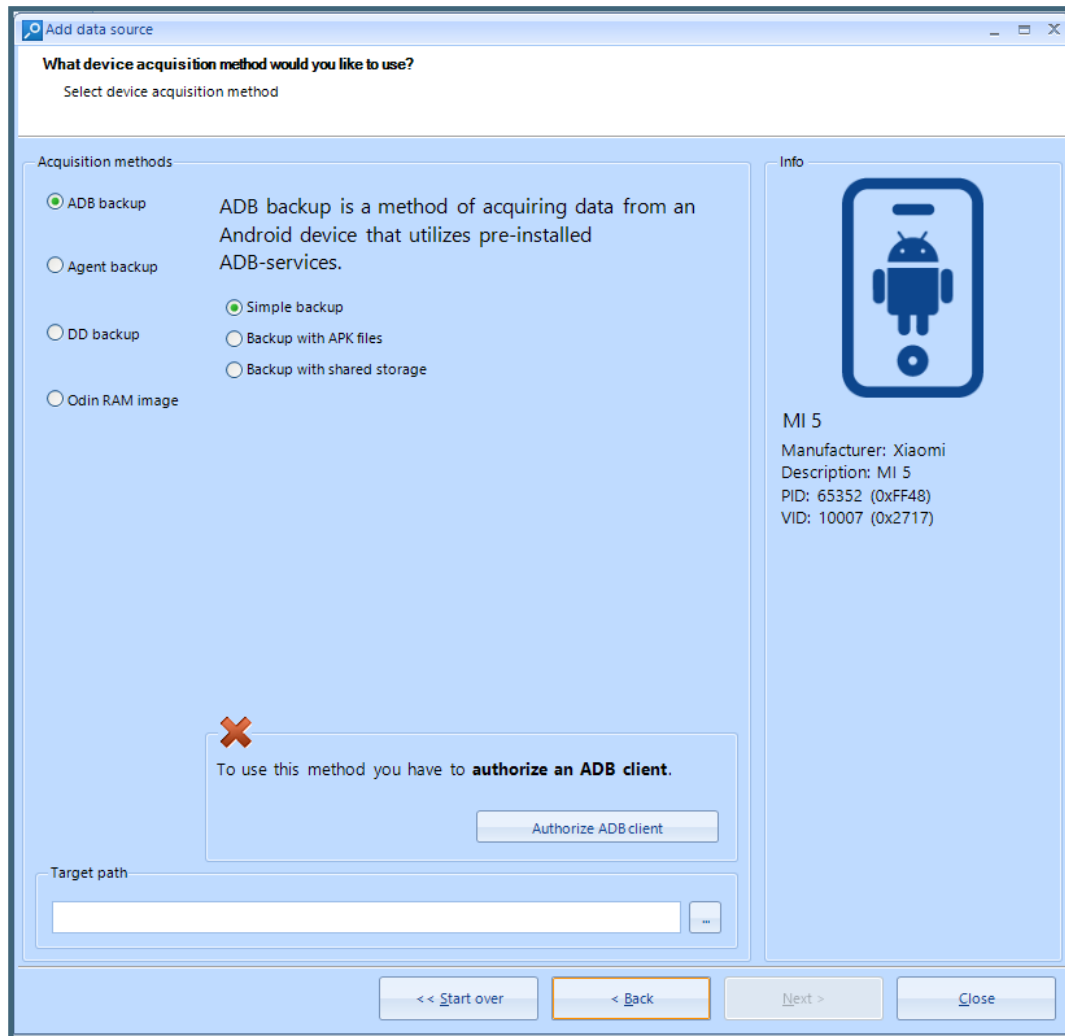


Figure 5 – Belkasoft Evidence Center showing its Add data source screen

After creating the backup, you can instruct BEC to analyze the image for artifacts.

On the **File System** tab (figure 6), you can view the items contained in the backup.

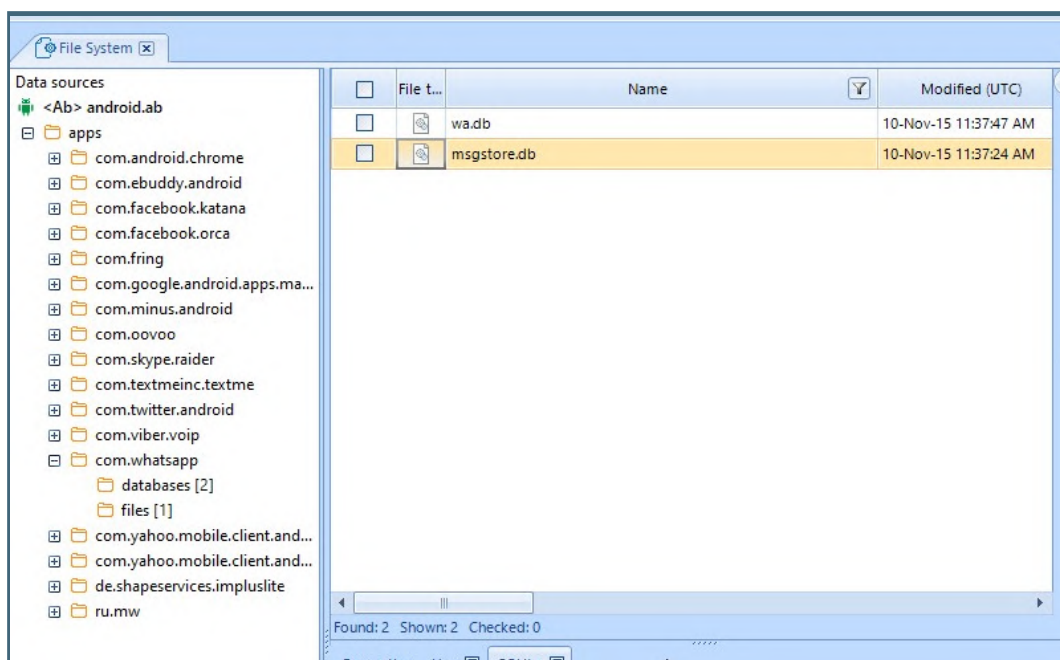


Figure 6 – The File System tab in Belkasoft Evidence Center showing the contents of the typical backup for an Android device

Once the analysis tasks get done, you can go to the **Case Explorer** tab (as seen below) to view the relevant artifacts in their respective groups. For example, under **Instant messengers**, you should see WhatsApp chats.

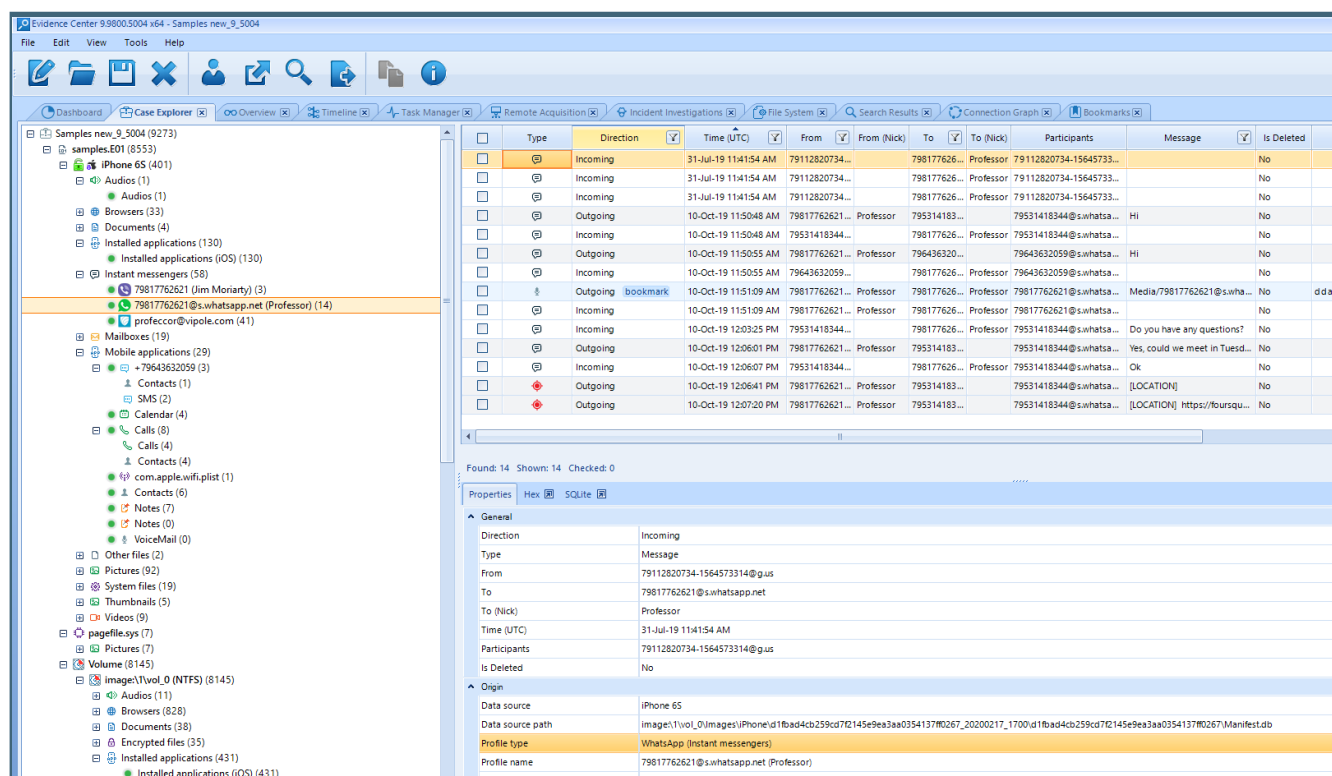


Figure 7 – Belkasoft Evidence Center presenting WhatsApp data extracted from an Android device.

In general, depending on the variables in a case, with Belkasoft Evidence Center, you can extract and analyze WhatsApp data in these forms:

Android

- Messages
- Avatars
- Geolocation information
- Forwarded contact information (from the address book)
- Forwarded Images
- Voice messages

iOS

- Messages
- Geolocation information
- Forwarded contacts information (from the address book)
- Forwarded Images
- Voice messages

The screenshot displays the Belkasoft Evidence Center interface. On the left, a file explorer shows the directory structure of an iPhone backup, with the file '79643632059@s.whatsapp.net (Doc) (10)' selected. The main window shows a list of messages with columns for Type, Time (UTC), From, To, Participants, Message, Is Deleted, and Names of attachments. A message from 79643632059@s.whatsapp.net to 79643632059@s.whatsapp.net is highlighted. Below the list, a detailed view of the selected message is shown, including its origin path and file details.

Type	Time (UTC)	From	To	Participants	Message	Is Deleted	Names of attachments
Doc	12-Mar-20 8:37:02 AM	79643632059...	79643632059...	79643632059@s.w...	Hil How are you?	No	
Doc	12-Mar-20 8:37:02 AM	79643632059...	79643632059...	79643632059@s.w...		No	
Doc	12-Mar-20 8:37:02 AM	79643632059...	79643632059...	79643632059@s.w...	Great! I will come to you soon	No	
Doc	12-Mar-20 8:41:22 AM	79643632059...	79643632059...	79643632059@s.w...	I'm going to the supermark...	No	
Doc	12-Mar-20 8:42:49 AM	79643632059...	79643632059...	79643632059@s.w...	Well, everyone has been talk...	No	
Doc	12-Mar-20 8:45:13 AM	79643632059...	79643632059...	79643632059@s.w...	(LOCATION) https://toursqu...	No	
Doc	12-Mar-20 8:46:10 AM	79643632059...	79643632059...	79643632059@s.w...	So, why don't you pick up s...	No	
Doc	12-Mar-20 8:48:17 AM	79643632059...	79643632059...	79643632059@s.w...	(PICTURE TRANSFER) 5622f...	No	5622f7c7-3ea1-4e38-9f68-7825a9b12...

Found: 10 Show: 10 Checked: 0

Item text	Properties	Attachments	Hex	SQLite
General				
Direction	Incoming			
Type	Picture transfer			
From	79643632059@s.whatsapp.net			
To	79643632059@s.whatsapp.net			
To (Nick)	Doc			
Time (UTC)	12-Mar-20 8:48:17 AM			
Message	(PICTURE TRANSFER) 5622f7c7-3ea1-4e38-9f68-7825a9b127211.thumb; 5622f7c7-3ea1-4e38-9f68-7825a9b127211.jpg; Media/79643632059@s.whatsapp.net/5/6/5622f7c7-3ea1-4e38-9f68-7825a9b127211.jpg			
Participants	79643632059@s.whatsapp.net			
Names of attachments	5622f7c7-3ea1-4e38-9f68-7825a9b127211.thumb; 5622f7c7-3ea1-4e38-9f68-7825a9b127211.jpg			
Is Deleted	No			
Origin				
Data source	Apple_device_CPID_14_BDID_14_20200318_1453.tar			
Data source path	D:\Data\Apple_device_CPID_32789_20200319_1448\Apple_device_CPID_14_BDID_14_20200318_1453.tar			
Profile type	WhatsApp (Instant messengers)			
Profile name	79643632059@s.whatsapp.net (Doc)			
Profile path	image\1\vol_0\private\var\mobile\Containers\Shared\AppGroup\BE93FE6F-F155-4DFA-9D6F-7B8683DDB393\ChatStorage.sqlite			
Origin path	Apple_device_CPID_14_BDID_14_20200318_1453.tar\private\var\mobile\Containers\Shared\AppGroup\BE93FE6F-F155-4DFA-9D6F-7B8683DDB393\ChatStorage.sqlite\ZWAMESSAGE			
File local offset (bytes)	43218			
Length (bytes)	111			
Origin	Common			

Figure 8 – Belkasoft Evidence Center showing WhatsApp call logs

In certain scenarios, on an iOS or Android device, you might be able to extract and analyze information on group chats in WhatsApp, ranging from the group name to the messages posted in it.

You can use Belkasoft to extract data from encrypted WhatsApp databases (crypt 12, for example) on Android devices.

Conclusion

WhatsApp currently dominates the instant messenger market and will probably keep its place for a long time. The implementation of encryption and other security mechanisms has made it difficult for investigators and researchers to obtain suspects' communications.

In certain cases (based on variables defined in this article)—and with Belkasoft Evidence Center—there are ways through which you get to extract and analyze important WhatsApp data associated with a user, which may serve as evidence for different purposes.

Useful links

[Read more Belkasoft articles on digital forensic issues](#)

[Download the trial version of Belkasoft Evidence Center](#)

[Request a quote](#)

For more information contact us at
sales@belkasoft.com

Visit belkasoft.com
Try free at <https://belkasoft.com/trial>
30 days trial

702 San Conrado Terrace, Unit 1
Sunnyvale CA 94085
+1 650-272-0384 (USA)
<https://belkasoft.com>