Extract and Decrypt WhatsApp Backups from iCloud

By Oleg Afonin

Published: 2017-07-20 · Archived: 2026-04-05 14:36:00 UTC

Facebook-owned WhatsApp is the most popular instant messaging tool worldwide. Due to its point-to-point encryption, WhatsApp is an extremely tough target to extract.

As we already wrote in yesterday's article, WhatsApp decryption is essential for the law enforcement since due to its popularity and extremely tough security it is a common choice among the criminals. However, the need for WhatsApp decryption is not limited to law enforcement. Us mere mortals may need access to our own communications when re-installing WhatsApp, changing devices or extracting conversations occurred on a device we no longer possess. Since WhatsApp data is not always available in iOS system backups, using WhatsApp' own stand-alone cloud backup system is the more reliable choice compared to pretty much everything else.

Elcomsoft Explorer for WhatsApp can now access iPhone users' encrypted WhatsApp communication histories stored in Apple iCloud Drive. If you have access to the user's SIM card with a verified phone number, you can now use Elcomsoft Explorer for WhatsApp to circumvent the encryption and gain access to iCloud-stored encrypted messages. In this article, we'll tell you how it works, and provide a step-by-step guide to extracting and decrypting WhatsApp backups from iCloud Drive.

Background

In December 2016, WhatsApp was updated to version 2.16.17. In this build, the company started encrypting its stand-alone backups stored in iCloud Drive, instantly rendering existing extraction methods ineffective. Before the change, Elcomsoft Explorer for WhatsApp could be used to successfully access WhatsApp chat archives by logging in to the user's iCloud account using their valid authentication credential (a combination of login and password or binary authentication token extracted from the user's computer). WhatsApp encryption dropped a significant roadblock, effectively preventing this practice and only allowing WhatsApp extraction from iOS system backups (local and iCloud-based).

How It Works

Since last year, both manual and daily stand-alone backups stored by WhatsApp in iCloud Drive are automatically encrypted. The encryption key, generated by WhatsApp when the user makes a backup for the first time, is unique per each combination of Apple ID and phone number. Different encryption keys are generated for different phone numbers registered on the same Apple ID. These encryption keys are generated and stored server-side by WhatsApp itself; they are never stored in iCloud, and they cannot be extracted from the device.

Elcomsoft Explorer for WhatsApp 2.10 gains the ability to generate encryption keys for WhatsApp's iCloud backups, successfully bypassing encryption and gaining access to WhatsApp conversation history and underlying messages. In order to generate the encryption key, experts must be able to receive a WhatsApp verification code sent to the phone number for which a given backup was created. In addition, the user's Apple ID and password (or binary authentication token) are required to gain access to the backup itself.

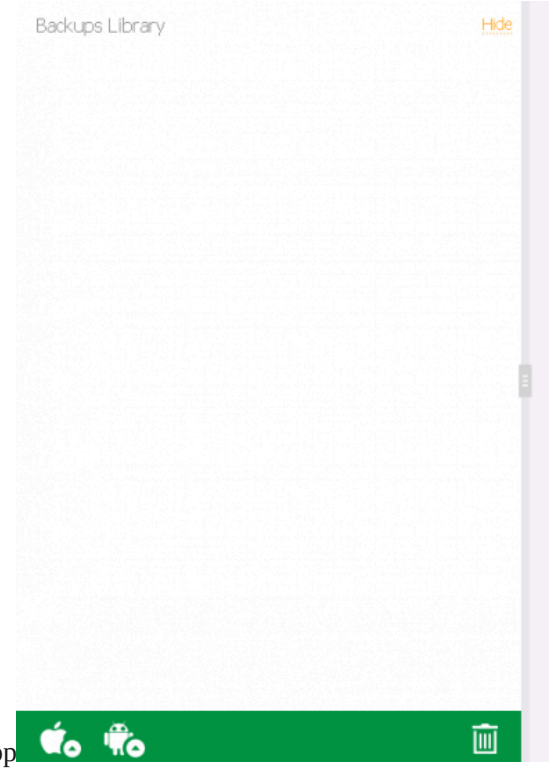
By using the associated phone number and iCloud authentication credentials, Elcomsoft Explorer for WhatsApp initiates the process of registering itself as a new "device" with WhatsApp. After passing the verification process, the tool can request the encryption from WhatsApp and use that key for decrypting the backup.

Permanent decryption key: The decryption key received by Elcomsoft Explorer for WhatsApp is permanent and does not change even if the user changes their Apple ID password. The decryption key remains valid even after re-authenticating WhatsApp with the same phone number and Apple ID. The same key can be used to decrypt older backups created before the key was retrieved.

Note: since WhatsApp is restricted to only running on a single device, the user's iPhone will no longer be able to send or receive WhatsApp messages after transferring WhatsApp registration to Elcomsoft Explorer for WhatsApp unless the user re-registers it again.

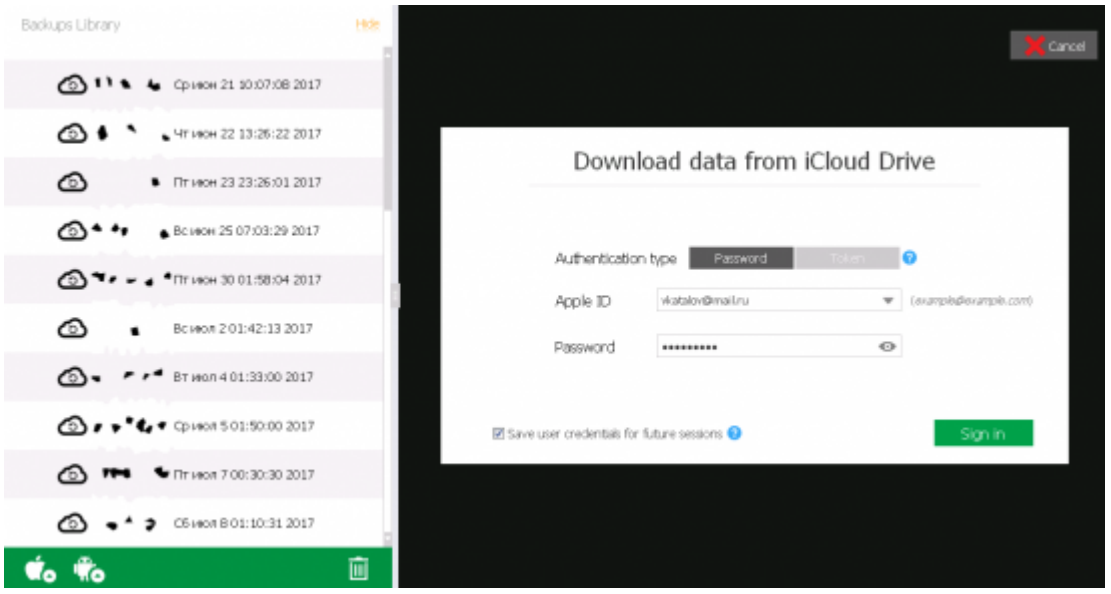
Elcomsoft Explorer for WhatsApp employs a smart workaround for processing WhatsApp extraction from iCloud. This is how it works.

In order to generate an encryption key, do the following.

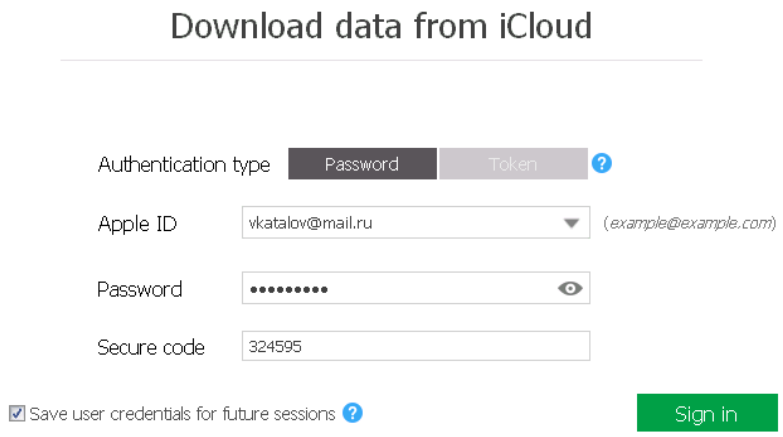


1. Launch Elcomsoft Explorer for WhatsApp
2. In Elcomsoft Explorer for WhatsApp, observe the two green icons "iOS" and "Android" located in the bottom left part of the main window. Click on the iOS icon. (Refer to online manual)

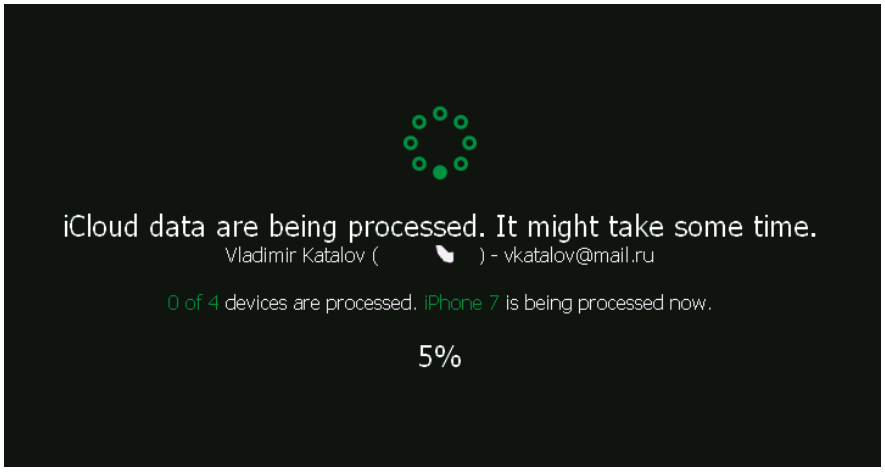
3. Click on the green iOS icon again. Select “Download files from iCloud Drive” from the menu. Note: you will not have to repeat the authentication process as Elcomsoft Explorer for WhatsApp will use cached credentials from the previous steps.
   – Download files from iCloud Drive
   – Download iCloud backup
   – Load iTunes/iCloud backup



4. If the Apple ID account has two-factor authentication, you will be prompted for a code

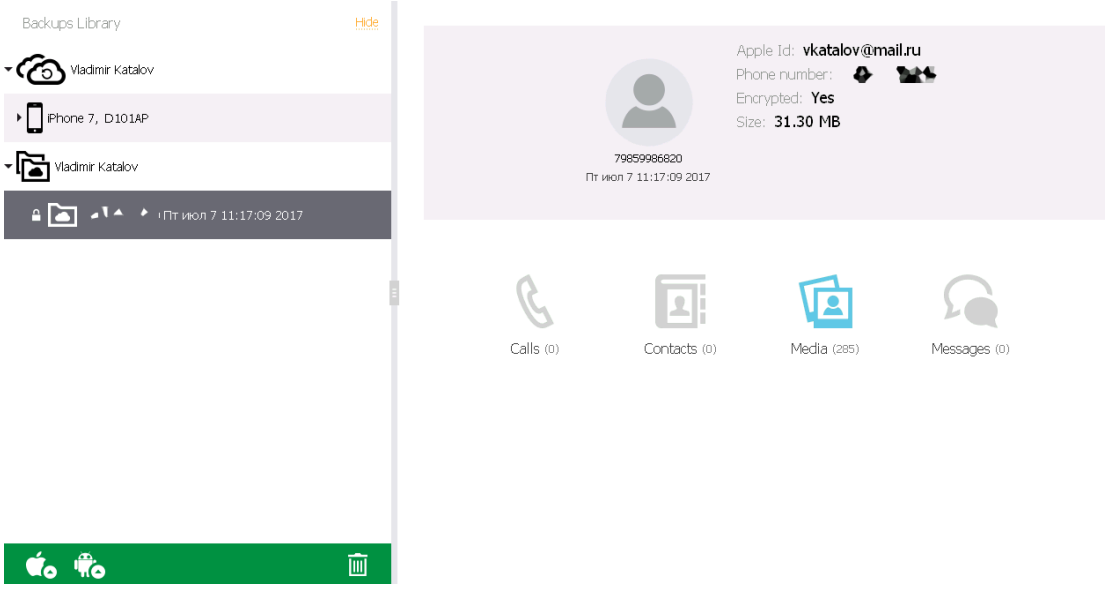


5. Enter the 2FA code
6. The downloading process begins. If the Apple ID account has data for multiple devices and/or multiple backups, the process may take a while

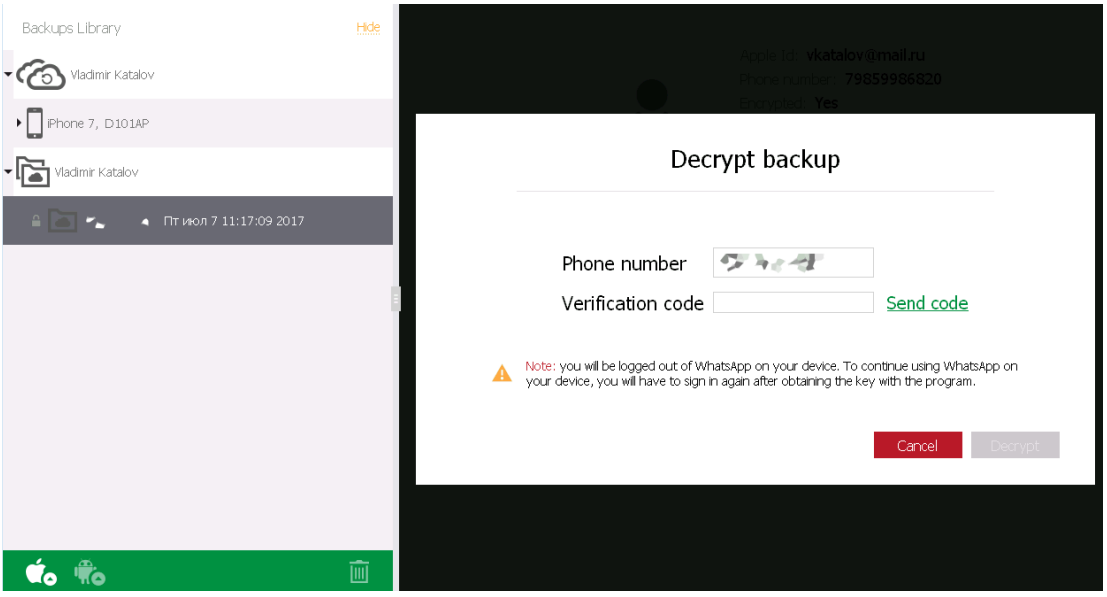


7. Once the download completes, you will see a message that warns that the data is encrypted.

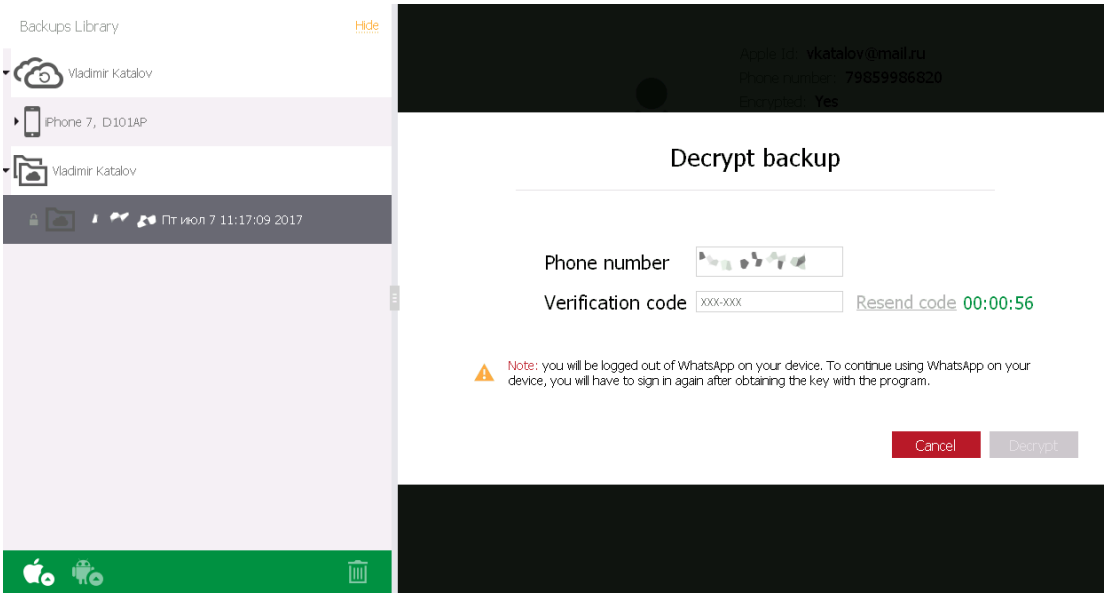
8. You can use the **Decrypt** option to instantly decrypt data. Alternatively, you may click **Open** to have data loaded into the viewer. At this time, you can only access media files; text conversations are still encrypted.



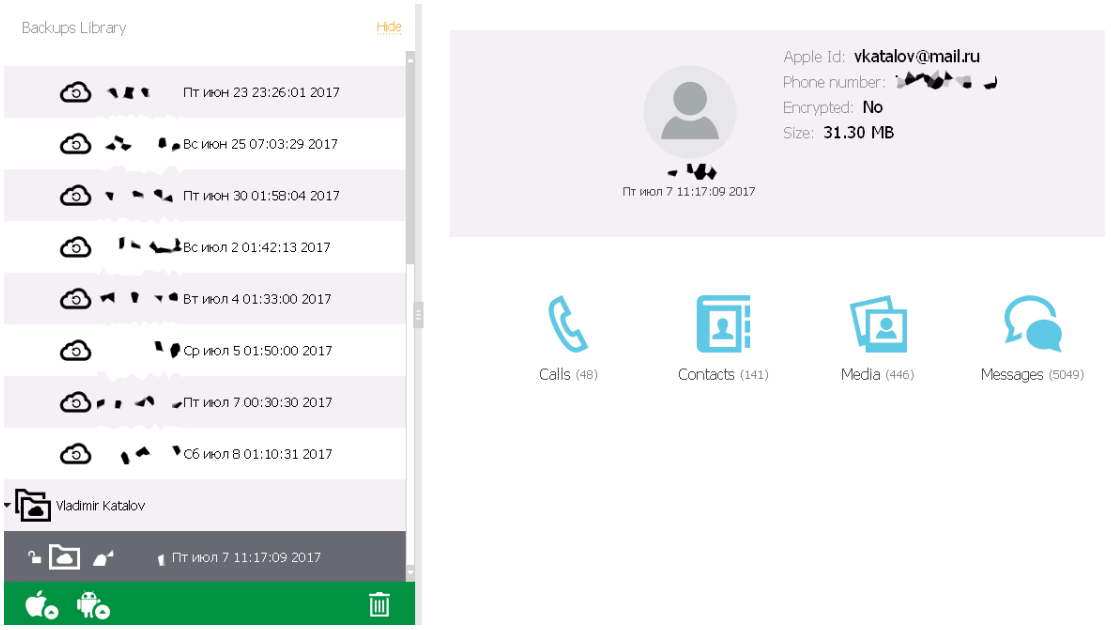
9. If you attempt to access encrypted data, you will be prompted for a code.



10. Click **Send** to request a code. The code will be delivered to the phone number. Enter the code into the "Verification code" box.



11. Once the correct code is entered, the data is instantly decrypted. If you have other encrypted data, click on the lock sign to instantly decrypt. Newly downloaded data will be decrypted automatically.



Attachments: Still No Encryption

Until last week, WhatsApp users could only exchange pictures, videos and PDF files. The recent update removed that limitation, now allowing users exchanging all types of files. Interestingly, WhatsApp does not encrypt attachments once they are received and backed up. Once Elcomsoft Explorer for WhatsApp obtains a backup, it also receives all attachments. Unlike messages, attachments are stored unencrypted, and can be accessed even if you don't have access to the registered phone number.

Elcomsoft Explorer for WhatsApp saves attachments to a single archive (the way they are kept in the cloud): %AppData%\Elcomsoft\Elcomsoft eXplorer for WhatsApp\Backups**N**\57T9237FN3~net~whatsapp~WhatsApp\WhatsApp\Accounts**xxxxxx**\backup\document.tar

In the path above, "N" represents the EXWA-assigned backup number, while "xxxxxx" would be the registered phone number.

WhatsApp Extraction: What's Supported and What Is Not

At this time, WhatsApp acquisition is possible via a number of different methods.

OS	Source	Encryption	Extraction Method
iOS	iCloud Drive (before WhatsApp 2.16.17)	No	iCloud Drive download

OS	Source	Encryption	Extraction Method
iOS	iCloud Drive (WhatsApp 2.16.17 and newer)	Yes, AES 256	1. iCloud Drive download 2. phone number verification 3. extraction of WhatsApp encryption key
iOS	iTunes backups	No	Local backup analysis
iOS	iCloud backups	No	iCloud backup download
Android	ADB backups		
Android	Google Drive backups	Yes	
Android	SD card backups	Yes	
Android	Extraction from a rooted device	No	Low-level extraction of the original database using root access
Android	Extraction from devices without root access	No	Downgrading WhatsApp Creating a WhatsApp backup

Note: WhatsApp only encrypts text messages and calls. Media files (photos, videos, attachments and voice messages) are never encrypted.

Conclusion

Despite the discovered workaround allowing experts to decrypt WhatsApp conversations, WhatsApp remains one of the most reliable instant messaging services. Based on Whisper Systems communication protocols, its traffic cannot be decrypted even if someone manages to intercept it.

Cloud backups remain one of the few vectors of attack allowing to remotely access WhatsApp communication history. If you have cloud backups enabled in WhatsApp and your iPhone is suddenly de-registered from your WhatsApp account, watch out as someone could have accessed your data. As always, we recommend activating two-factor authentication to protect your Apple ID.

REFERENCES:

Elcomsoft Explorer for WhatsApp

Elcomsoft Explorer for WhatsApp is a tool to download, decrypt and display WhatsApp communication histories. The tool automatically acquires WhatsApp databases from one or multiple sources, processes information and displays contacts, messages, call history and pictures sent and received. The built-in viewer offers convenient searching and filtering, and allows viewing multiple WhatsApp databases extracted from various sources.

Elcomsoft Explorer for WhatsApp official web page & downloads »
