ElcomSoft Tool Extracts Android WhatsApp Backups from Google

Moscow, Russia – January 24, 2018 - ElcomSoft Co. Ltd. releases a major update to Elcomsoft eXplorer for WhatsApp, the company's all-in-one tool for extracting, decrypting and analyzing WhatsApp communication histories. The tool can now extract and decrypt WhatsApp backups produced by the Android app and stored in the user's Google Account.

The decryption is possible with access to a verified phone number or SIM card, and requires authenticating into the user's Google account. A WhatsApp encryption key must be only obtained once, and can be used to access all previously created and all future backups for a given combination of Google Account and phone number. The tool provides automatic download and decryption for WhatsApp backups and comes with a built-in viewer.

"With more than 1.3 billion active users, WhatsApp is by far the popular instant messaging tool in Europe and North America", says **Vladimir Katalov**, ElcomSoft CEO. *"Due to its overwhelming popularity, WhatsApp is frequently used or targeted by the criminals. With our tool, investigators can now access Android users' encrypted WhatsApp communication histories backed up in Google Drive – provided that they have the user's authentication credentials and can receive a confirmation code sent to the user's WhatsApp phone number."*

Notably, a cloud backup may, in certain cases, contain even more information than stored on the device itself. This particularly applies to attachments (photos and videos) sent and received by WhatsApp users and then deleted from the device.

WhatsApp for Android: Not an Easy Target

For several years, WhatsApp has been encrypting its backup databases. Both stand-alone and cloud backups produced by the Android app and are securely protected with industry-standard AES256 encryption. The encryption key is generated by WhatsApp at the time of the first backup. The key is unique per account and per phone number. If the user has multiple WhatsApp accounts and only one Google Account, each WhatsApp account will use a unique encryption key.

The encryption keys are generated by WhatsApp servers; they are never stored in Google Drive. Extracting the encryption keys from a local Android may or may not be possible depending on the phone's root status and the version of Android it is running.

Making things even more complicated is the fact that the many versions of WhatsApp released during the last years are employing different encryption algorithms. This makes it difficult to build an all-in-one acquisition tool compatible with all versions of WhatsApp.

Elcomsoft Explorer for WhatsApp 2.30 gains the ability to download WhatsApp backups for Android devices directly from the user's Google account, retrieve cryptographic keys from WhatsApp servers and decrypt the content of WhatsApp backups including conversation histories and messages.

In order to obtain the encryption key from WhatsApp, access to the user's trusted phone number or SIM card is required. The authentication code is requested and delivered as a text message. Based on that authentication code, Elcomsoft Explorer for WhatsApp automatically creates a cryptographic key that will be used to decrypt all existing and future backups for a given combination of Google Account and phone number. In addition, the user's authentication credentials are required to log in to their Google Account.

If the expert does not have access to the user's SIM card or trusted phone number, Elcomsoft Explorer for WhatsApp can access contacts and media files (pictures and videos) the users send and receive with WhatsApp.

Step-by-step WhatsApp acquisition guide: https://blog.elcomsoft.com/2018/01/extract-and-decrypt-whatsapp-backups-from-google/

About Elcomsoft Explorer for WhatsApp

Elcomsoft Explorer for WhatsApp is an all-in-one tool for extracting, decrypting and viewing WhatsApp communication histories from iOS and Android devices and cloud services. Supporting a wide range of acquisition options, Elcomsoft Explorer for WhatsApp can extract WhatsApp data from local iTunes backups, iCloud and Google Drive backups. The tool can extract WhatsApp communication histories from most rooted and non-rooted Android devices. Cloud acquisition requires entering the correct authentication credentials. Access to a verified phone number or SIM card is required for decrypting stand-alone backups in Apple iCloud and Google Drive.

The built-in viewer offers convenient access to contacts, messages and pictures sent and received during conversations. Multiple WhatsApp databases can be analyzed at the same time. Searching and filtering make it easy locating individual messages or finding communication sessions that occurred over a certain date range.

Pricing, availability and system requirements

Elcomsoft eXplorer for WhatsApp is immediately available. Elcomsoft Explorer for WhatsApp Home is available to North American customers for $79. Local pricing may vary. Elcomsoft eXplorer for WhatsApp supports Windows 7, 8, 8.1, and Windows 10 as well as Windows 2008, 2012 and 2016 Server.

About ElcomSoft Co. Ltd.

Founded in 1990, ElcomSoft Co. Ltd. develops state-of-the-art computer forensics tools, provides computer forensics training and computer evidence consulting services. Since 1997, ElcomSoft has been providing support to businesses, law enforcement, military, and intelligence agencies. ElcomSoft tools are used by most of the Fortune 500 corporations, multiple branches of the military all over the world, foreign governments, and all major accounting firms. ElcomSoft is a Microsoft Partner (Gold Application Development), Intel Premier Elite Partner and member of NVIDIA's CUDA/GPU Computing Registered Developer Program.