Elcomsoft Decrypts Non-Text Content of iCloud Messages, Accesses Attached Photos, Media and Other Files

ElcomSoft Co. Ltd. updates Elcomsoft Phone Breaker, the company's forensic extraction tool. In addition to iCloud Messages extraction, version 8.40 gains the ability to remotely access non-text content such as attached media, documents and other data stored in Apple iCloud. Elcomsoft Phone Breaker becomes the first forensic tool on the market to extract those types of evidence from the cloud. Elcomsoft Phone Viewer received an update to support the new data categories.

"It is hard to overestimate the importance of real-time evidence", says Elcomsoft CEO Vladimir Katalov. "iMessage conversations in particular are extremely tough to obtain. Point-to-point encryption protects messages and attached content against main-in-the-middle attacks, while their cloud copies are securely protected with industry-standard encryption. We are now offering a solution allowing to extract and decrypt the entire content of the chats including media files, documents and other types of data sent or received with iMessages".

Background

Apple makes active use of cloud sync, and is continuously expanding the amount of information synchronized with iCloud. Synchronized information is removed from iCloud backups. iOS 11.4 brought message sync, automatically synchronizing messages across devices. Conversation histories are an important part of real-time evidence. Attached media files can provide valuable insight about the user's location at the time of sending the message. In addition, non-text content may include videos, voice recordings and other media files, shared locations and full-size previews of linked Web sites sent and received by the user. These previews may remain available even after the original linked Web site is no longer accessible.

Elcomsoft Phone Breaker can extract chats from the user's iCloud account just moments after new messages arrive. The latest update gains the ability to access non-text content such as attached pictures and media, documents, shared locations and other types of data. To access that content, experts may use a combination of Apple ID and password as well as the one-time code to pass two-factor authentication. In addition, a device passcode or account password from one of the already enrolled devices is required to decrypt messages and attachments.

Extracting Non-Text Content of iCloud Messages

While previous versions of Elcomsoft Phone Breaker were able to access messages synced with iCloud, the new release brings support for non-text content included with iMessage attachments. Non-text content such as media files and locations can provide essential evidence during investigations. Many iMessage attachments are pictures captured with the iPhone, so analyzing EXIF data may return a number of location points. One can preview and save media files using the latest version of Elcomsoft Phone Viewer that has been updated to support iMessage attachments.

Since messages and attachments are point-to-point encrypted with a key derived from the user's

www.elcomsoft.com
© ElcomSoft Co. Ltd.

Microsoft Partner
Gold Application Development
Gold Intelligent Systems

intel Software Partner

passcode, access is impossible without a passcode. Apple does not have access to messages stored in iCloud. As a result, neither iMessages nor attachments are delivered as part of LE or GDPR requests. Elcomsoft Phone Breaker is the only forensic tool on the market to access iCloud Messages and attachments we well as other major evidence stored in iCloud. In order to access Messages and attachments, one needs the correct device passcode or system password to one of the devices already enrolled in the sync, which is in addition to iCloud/Apple ID login and password.

About Elcomsoft Phone Breaker

Elcomsoft Phone Breaker is an all-in-one mobile acquisition tool to extract information from a wide range of sources. Supporting offline and cloud backups created by Apple, BlackBerry and Windows mobile devices, the tool can extract and decrypt user data including cached passwords and synced authentication credentials to a wide range of resources from local backups. Cloud extraction with or without a password makes it possible to pull communication histories, searches and browsing habits, and retrieve photos that have been deleted by the user a long time ago. The tool offers the most advanced support for Apple iCloud, decrypting many types of data that Apple itself will not return when serving Law Enforcement and GDPR pullout requests. This includes users' passwords stored in iCloud Keychain, iCloud Messages and attachments.

Pricing and Availability

Elcomsoft Phone Breaker 8.40 is immediately available for Windows and macOS. This update is free to existing users with currently valid licenses. Home, Professional and Forensic editions are available. iCloud support is only available in Professional and Forensic editions, while password-free iCloud access as well as the ability to download arbitrary information from iCloud and iCloud Drive are only available in the Forensic edition. Two-Factor Authentication is available in all editions.

Elcomsoft Phone Breaker Pro is available to North American customers for $199. The Forensic edition enabling over-the-air acquisition of iCloud data and support for binary authentication tokens is available for $799. The Home edition is available for $79. Local pricing may vary.

System Requirements

Elcomsoft Phone Breaker supports Windows 7, 8, 8.1, and Windows 10 as well as Windows 2008, 2012 and 2016 Server. The Mac version supports Mac OS X 10.7 and newer. Elcomsoft Phone Breaker operates without Apple iTunes or BlackBerry Link being installed. In order to access iCloud Keychain, Windows users must have iCloud for Windows installed, while Mac users must run macOS 10.11 or newer.

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.