Extracted Notifications Offer Valuable Insight for iOS Forensics

Moscow, Russia – March 2, 2017 - ElcomSoft Co. Ltd. updates Elcomsoft Phone Viewer, a lightweight forensic tool for quickly accessing information extracted from local and cloud mobile backups. Version 3.30 for Windows and macOS adds support for viewing unread device notifications that are included in iOS backups. Unread notifications can go several years back; on one occasion, ElcomSoft were able to extract some 1200 notifications going back to 2012.

"Notifications are an essential part of iOS", says ***Vladimir Katalov****, ElcomSoft CEO. "They can contain a lot of sensitive information. Notifications are extensively used by instant messaging apps, email clients, online banking, shopping and delivery tracking apps, booking and taxi services. Unread notifications are saved automatically to iCloud and local backups, and can be viewed with Elcomsoft Phone Viewer 3.30. These bits of data are not available elsewhere."*

iOS developers are free to choose what data exactly gets into a backup. For example, most instant messengers flag their data so that neither conversations nor individual messages are ever saved into cloud or local backups. Downloaded mail is not saved into a backup either. As a result, extracting messages would be only possible via physical acquisition (with jailbreak), which may or may not be available. Extracting iOS notifications can provide valuable insight into the user's communications and other day-to-day activities.

Elcomsoft Phone Viewer 3.30: Reading iOS Notifications

iOS relies heavily on notifications to deliver time-sensitive, text-based information. Notifications can be thrown by email clients, instant messengers, two-factor authentication apps, as well as apps used by travelers to book airplane tickets, hotels and taxis.

The Uber app as well as many local taxi services can push notifications about the cab arriving (often including precise time and place and even the car license plate number). Many banks push real-time information about credit transactions and account updates as notifications as opposed to using text messages. It's not uncommon for banking apps to deliver sign-in confirmation codes as push notifications.

Shopping apps such as Amazon can push delivery status information about orders. Google Trips, Booking and Expedia apps can display notifications about upcoming travel events. Skype, Facebook, Twitter, LinkedIn, Pinterest and many other apps push notifications about current activities such as comments, likes, friend requests or retweets.

This volatile, real-time information is frequently overlooked by investigators, yet it can pose a significant value during investigations. Unless read or dismissed, iOS notifications are included to local and cloud backups. Once backed up, notifications can be kept in the cloud (or in newly made local backups) for years. When analyzing one particularly old account, ElcomSoft researchers discovered as many as 1200 notifications received between 2012 and 2017 (although most notifications belong to the period starting in August 2015).

Elcomsoft Phone Viewer 3.30 can automatically discover notifications in iOS backups, displaying their full content along with metadata (date and time, app package name, as well as the full text content).

About Elcomsoft Phone Viewer

Elcomsoft Phone Viewer is a compact, fast and easy to use mobile forensic tool to enable experts viewing information stored in unprotected local and cloud backups. Supporting backups produced by popular Apple, BlackBerry and Windows Phone devices, the tool offers access to contacts, messages, call logs, notes and calendar, media files and Web activities, and allows viewing information about the device. The small, affordable tool offers a simple and convenient user interface that matches the usage experience of Elcomsoft Phone Breaker, thus requiring no additional learning curve.

Experts using Elcomsoft Phone Viewer together with other ElcomSoft tools such as Elcomsoft Phone Breaker save time by reviewing essential bits of information in just a few moments. By quickly download selective information from Apple iCloud with Elcomsoft Phone Breaker and viewing acquired information in Elcomsoft Phone Viewer, investigators can instantly access information about the suspect’s activities such as their calls, messages, address books, notifications and location history in a matter of minutes.

Pricing and Availability

Elcomsoft Phone Viewer is available immediately. A single Standard edition is available for $79 to North American customers; local pricing may vary.

System Requirements

At this time, Elcomsoft Phone Viewer is available for Windows PCs and Macs. Elcomsoft Phone Viewer runs in 32-bit and 64-bit editions of Windows 7, 8, 8.1 and 10, as well as Windows 2008, 2012 and 2016 Server, and supports macOS 10.8 and newer. Elcomsoft Phone Viewer works without Apple iTunes or BlackBerry Desktop Software being installed.

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.