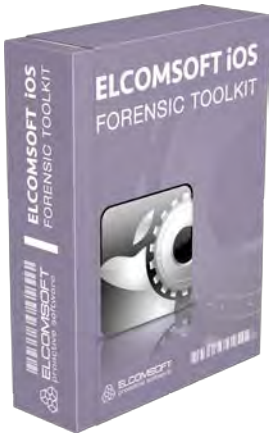
Elcomsoft iOS Forensic Toolkit Adds Logical Acquisition, Supports Physical Acquisition of iOS 9.2-9.3.3



Moscow, Russia – August 11, 2016 - ElcomSoft Co. Ltd. updates iOS Forensic Toolkit, adding physical acquisition support to most modern devices with iOS 9.2-9.3.3; logical acquisition as a new option (passcode may not be needed).

The new release adds logical acquisition support for all generations of iPhone, iPad, iPad Pro and iPod Touch regardless of iOS version or jailbreak status. Unlike acquisition via Apple iTunes, iOS Forensic Toolkit enables the use of lockdown files (pairing records) to unlock iOS devices without using passcode or Touch ID. By adding logical acquisition to its physical acquisition toolkit, ElcomSoft strives to deliver the complete all-in-one forensic acquisition solution for the widest range of iOS devices. The toolkit is available for both Windows and Mac OS X platforms.

In addition, version 2.1 adds physical acquisition support to Apple devices running iOS 9.3.3 with newly released Pangu jailbreak for 64-bit devices. Finally, the new release adds the option to extract device information from all types of iOS devices regardless of iOS version or jailbreak status even if they are locked with an unknown password.

*"iOS Forensic Toolkit was all about physical acquisition", says **Vladimir Katalov**, ElcomSoft CEO. "We were the first to acquire iPhone 4s, 5 and 5c. We pioneered physical acquisition for 64-bit devices, but until now we didn't offer an option to acquire devices without a jailbreak. If you have a non-jailbroken iPhone or iPad, we can now dump its contents into an iTunes-style backup without actually using iTunes, and sometimes even without a passcode."*

The logical acquisition process requires the device to be unlocked at least once after cold boot. Examiners will have to unlock the device by using passcode, Touch ID or non-expired pairing record (lockdown file) collected from the user's computer.

*"We've been without a jailbreak for months", says **Andy Malyshev**, ElcomSoft CTO. "We couldn't do anything with iOS 9.2 or 9.3 without a jailbreak. The new Pangu jailbreak allowed us to resume development and add physical acquisition support to the latest versions of iOS".*

Logical Acquisition: Works with All iOS Devices

Logical acquisition is a simpler and safer acquisition method compared to physical. Logical acquisition produces a standard iTunes-style backup of information stored in the device. While logical acquisition returns less information than physical, experts are recommended to create a logical backup of the device before attempting more invasive acquisition techniques.

The new release of iOS Forensic Toolkit now provides an option to perform logical acquisition of iOS devices by creating an iTunes-style backup. Logical acquisition works with all devices running iOS 4 or newer regardless or hardware generation and jailbreak status. However, the device must be unlocked at least once after cold boot; otherwise, the device backup service cannot be started.

Experts will need to unlock the device with passcode or Touch ID, or use a non-expired lockdown file (iTunes pairing record) extracted from the user's computer. Lockdown files are pairing records created on computers connecting to a given iOS device. Lockdown files are created to relieve users from manually unlocking their iOS devices every time they sync with iTunes. If a computer was seized together with an iOS device, it can be enough to successfully acquire information from a locked iOS device.

If the device is configured to produce password-protected backups, experts must use Elcomsoft Phone Breaker to recover the password and remove encryption. Apple iTunes is not required to produce a backup.

Logical backups produced by Elcomsoft iOS Forensic Toolkit can be analyzed with Elcomsoft Phone Viewer of third-party forensic tools. If a backup comes out encrypted with an unknown password, one can use Elcomsoft Phone Breaker to recover that password and decrypt the backup. If no backup password is set, the tool will automatically configure the system with a temporary password in order to be able to decrypt keychain items (password will be reset after the acquisition).

Physical Acquisition: iOS 9.3.3 Support with New Pangu Jailbreak

Apple users are quick to adopt the latest technology. According to Apple, some 86% of users run iOS 9 on compatible devices. During the past 4 months, no jailbreak was available to any version of iOS newer than iOS 9.1. The Pangu team has recently released a public jailbreak for iOS 9.2 through 9.3.3, allowing investigators to jailbreak Apple devices running the last versions of Apple iOS and perform physical acquisition. Instructions on installing the new Pangu jailbreak are available at http://en.pangu.io/help.html

Physical acquisition is the most comprehensive acquisition method available for iOS devices. It is the only acquisition method that enables full access to all encrypted information stored in Apple's secure storage, the keychain (for 32-bit devices only). This includes Web site and application passwords including the password to the user's Apple ID account. Email messages and attachments, log files and histories, as well as certain application data are only accessible via physical or advanced logical acquisition.

Pricing and Availability

Elcomsoft iOS Forensic Toolkit 2.1 is immediately available. North American pricing starts from $1,495. Both Windows and Mac OS X versions are supplied with every order. Existing customers can upgrade at no charge or at a discount depending on their license expiration.

Elcomsoft iOS Forensic Toolkit is also available as part of Elcomsoft Mobile Forensic Bundle ($2995). Elcomsoft Mobile Forensic Bundle integrates all Elcomsoft tools for logical, physical and cloud forensics.

Compatibility

Windows and Mac OS X versions of Elcomsoft iOS Forensic Toolkit are available. Physical acquisition support for the various iOS devices varies depending on lock state, jailbreak state and the version of iOS installed. Unrestricted acquisition is available for very old devices (iPhone 4 and older). iPhone 4S through 5C, iPad mini can only be acquired if jailbroken. Physical acquisition for 64-bit devices supports iPhone 5S through 6S (and their Plus versions), iPad mini 2 through 4, and 64-bit versions of full-sized iPads. The 64-bit acquisition process can extract but cannot decrypt the keychain.

Logical acquisition is available for all iOS devices regardless of jailbreak status if the device can be unlocked with passcode, Touch ID or pairing record (lockdown file). iOS Forensic Toolkit produces standard iTunes-style backups and does not require Apple iTunes to be installed to perform logical acquisition.

About Elcomsoft iOS Forensic Toolkit

Elcomsoft iOS Forensic Toolkit provides forensic access to encrypted information stored in popular Apple devices running iOS versions 3 through 9.3.3. By performing physical acquisition of the device, the Toolkit offers instant access to all protected information including SMS and email messages, call history, contacts and organizer data, Web browsing history, voicemail and email accounts and settings, stored logins and passwords, geolocation history, the original plain-text Apple ID password, conversations carried over various instant messaging apps such as Skype or Viber, as well as all application-specific data saved in the device.

iOS Forensic Toolkit is the only tool on the market to offer physical acquisition for Apple devices equipped with 64-bit SoC including Apple iPhone 5S, 6/6S and their Plus versions. Physical acquisition for 64-bit devices returns significantly more information compared to logical and over-the-air approaches.

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.