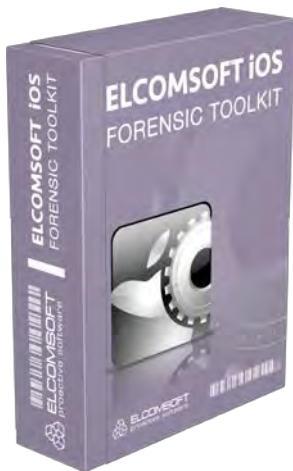# Elcomsoft iOS Forensic Toolkit:
Physical Acquisition for 64-bit Devices and iOS 9 Support

Moscow, Russia - November 18, 2015 - ElcomSoft Co. Ltd. updates iOS Forensic Toolkit, adding physical acquisition for 64-bit Apple devices and enabling support for iOS 9 (jailbreak required).

Elcomsoft iOS Forensic Toolkit 2.0 adds physical acquisition support for jailbroken 32-bit and 64-bit Apple devices running any version of up to and including iOS 9. Physical acquisition is now available for all jailbroken 32-bit and 64-bit Apple devices including iPhone 4S, 5/5C, 5S, 6/6S and their Plus versions, as well as all existing iPads. Finally, iOS Forensic Toolkit 2.0 can extract a limited amount of information from jailbroken devices locked with an unknown passcode.

"Physical acquisition support for 64-bit devices is finally here", says Vladimir Katalov, ElcomSoft CEO. "For a long time, we could do nothing to help our customers acquire information from recent Apple smartphones. iOS Forensic Toolkit 2.0 opens a new advanced venue for extracting data from 64-bit devices, and adds iOS 9 support along the way."

Physical acquisition is only available on jailbroken devices with known or empty passcode. Since no jailbreak is currently available for iOS 9.1, devices running this version of iOS are excluded. Acquisition of a limited data set is available for all jailbroken devices regardless of their lock status.

Physical Acquisition for Jailbroken 64-bit Devices

Since September 2013, the day when Apple introduced its first 64-bit device, the iPhone 5S, the mobile forensic community was constantly looking for a way to acquire information from Apple devices featuring the new architecture. Available acquisition options included logical (backup analysis) and over-the-air (iCloud/iCloud Drive extraction), and returned limited amounts of information. Apple was little help, citing its official government request policy to deny requests to unlock devices running iOS 8 and newer on the basis of technical unfeasibility, and refusing to unlock even an older iPhone 5S running iOS 7.

Elcomsoft iOS Forensic Toolkit 2.0 offers physical acquisition support for jailbroken 64-bit devices, allowing investigators to extract more information than any other acquisition method available for devices featuring Apple's 64-bit SoC. Compared to logical and over-the-air acquisition, the new process can extract downloaded mail, geolocation information browser cache and cookies, and full application data including protected data.

Unlike physical acquisition for 32-bit devices, the new 64-bit extraction process returns a UNIX-style TAR archive of the file system instead of a bit-precise image. In addition, the 64-bit process extracts but does not decrypt the keychain, which makes stored passwords unavailable. Finally, the 64-bit extraction process requires unlocking the device with the correct passcode followed by removing passcode protection altogether in iOS security settings of the device.

iOS 9 Support

According to Apple, as many as 66 per cent of compatible devices are now running Apple's latest OS. Adding forensic support for devices running iOS 9 enables experts extract information from compatible jailbroken devices, and allows performing physical acquisition of devices carrying no passcode lock (providing that a jailbreak can be installed).

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 (*). 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.

(*) Keychain decryption available for 32-bit devices only, and not available via physical acquisition for 64-bit devices.

Extracting Data from Jailbroken Devices Locked with Unknown Passcode

Devices locked with an unknown passcode were long considered to be forensically inaccessible. With Apple refusing to even touch iDevices running iOS 8 onwards, every bit of information that can be extracted from such devices matters.

Elcomsoft iOS Forensic Toolkit 2.0 comes with the ability to extract a limited amount of data from jailbroken iOS devices that are locked with an unknown passcode. Incoming calls, text messages, log files, SQLite WAL files and limited amount of geolocation data may be extracted. More information about on what can be obtained from locked devices is available in a blog post. Note that this feature requires a jailbroken device, and thus not available for devices running iOS 9.1 for which no jailbreak is available at this time.

Pricing and Availability

Elcomsoft iOS Forensic Toolkit 2.0 is immediately available. North American pricing starts from $1,499. 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.

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.

About Elcomsoft iOS Forensic Toolkit

Elcomsoft iOS Forensic Toolkit provides forensic access to encrypted information stored in popular Apple devices running iOS versions 3 to 9. By performing a physical acquisition analysis of the device itself, 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 and Gold Intelligent Systems), Intel Premier Elite Partner and member of NVIDIA's CUDA/GPU Computing Registered Developer Program.