ElcomSoft Gives iOS Forensics a Boost, Adds Physical Acquisition Support for iOS 7 Devices

Moscow, Russia – January 30, 2014 - ElcomSoft Co. Ltd. updates iOS Forensic Toolkit, adding physical acquisition support for jailbroken iOS 7 devices. Physical acquisition support is now available for jailbroken devices running Apple iOS 7 including iPhone 4S, 5 and 5C, iPad 2nd to 4th gen, iPad Mini, iPod Touch 5th gen, and either having no passcode protection or carrying a jailbreak installed. In addition, the new release adds support for previously unavailable versions of iOS 6.1.3-6.1.5.

With more than 83% of all iOS devices now running iOS 7, ElcomSoft gives the mobile forensic industry a boost. Elcomsoft iOS Forensic Toolkit is still remaining the only commercially available forensic product that is able to perform physical acquisition of iPhone 4S, iPad 2 and newer generation hardware.

Physical acquisition allows extracting information from Apple's protected storage, the keychain. In many cases, the enhanced iOS 7 keychain contains the original passwords to Apple ID accounts. This allows investigators seamlessly accessing information stored in the iCloud as well as tracking the users' geolocation coordinates in real-time by using Apple iCloud Find My Phone service.

At this time, physical acquisition of last-generation iOS 7 devices is only possible if either of the following is true:

- There is no passcode protection on the device, or
- The investigator knows the passcode, or
- The device has been jailbroken by the user

"*Apple users are fast when it comes to upgrades*", says Vladimir Katalov, ElcomSoft CEO. "*The latest version of iOS, iOS 7, is already installed on some 83 per cent of compatible devices. We are proud to be the first to make a tool for our customers that gives them access to valuable information stored in these devices.*"

ELCOMSOFT
PROACTIVE SOFTWARE

Background

At this time, 8 models of iPhone, 7 models of iPad and 5 generations of iPod Touch are available. With more than 700 million iOS devices around and 83% of them using iOS 7, the updated iOS Forensic Toolkit opens the door to acquiring information from some 580 million devices.

iOS 7 Physical Acquisition

Physical acquisition has long been the method of choice for accessing information stored in iOS devices among law enforcement and forensic customers. Physical acquisition allows investigators obtain the complete bit-precise image of the device in real time, including device secrets and unallocated data blocks that may contain deleted files and destroyed evidence. Physical acquisition returns significantly more information from the device than any other method such as logical acquisition or backup analysis, including data stored in Apple's protected storage, the keychain.

Finally, physical acquisition operates on fixed-timeframe basis, which guarantees timely delivery of the entire content of the device. Acquisition time depends on the model of the device being aquired, as well as on the amount of memory carried by that device. For example, acquisition time for a 32-GB iPhone 5 device is 25 minutes, while a 32-GB iPhone 4 with a slower controller is acquired in approximately 40 minutes.

With the release of iPhone 4S featuring stronger security, physical acquisition became impossible to all but ElcomSoft customers. Elcomsoft iOS Forensic Toolkit has been the first and remains the only commercially available product that can perform physical acquisition of last-generation Apple hardware running the latest versions of iOS up to and including iOS 7.

On jailbroken iOS 7 devices, iOS Forensic Toolkit can break the original passcode with brute force or dictionary attack. Passcode recovery speed on jailbroken iPhone 5 and 5C devices is approximately 15.5 passcodes per second, allowing iOS Forensic Toolkit to break typical 4-digit passcodes in about 10 minutes.

Physical Acquisition Benefits

Physical acquisition offers numerous benefits over other acquisition methods. Fixed timeframe and guaranteed delivery are just a few things to mention. Physical is the only acquisition method that can extract the following information:

1. Cached (downloaded) mail, regardless of the type of an email account. Cached mail is not available in offline or online backups.
2. Geolocation data. While iTunes and iCloud backups contain only some very basic geolocation data, physical acquisition extracts comprehensive information including frequent locations and geolocation data requested by all Apple and third-party applications and system services. Geolocation information is requested (and stored) on many events such as using maps, calibrating the compass, for the purpose of tracking advertisements, when looking for mobile and Wi-Fi networks, etc. As a result, comprehensive geolocation data extracted with physical acquisition makes it possible to create a precise reconstruction of the phone owner's whereabouts for every minute of time.
3. System logs and crash logs, detailing which applications were launched or installed.
4. Cached application data, such as cached Web pages and addresses, and many other types of data are only available via physical acquisition. Considering that many iOS applications are using Internet access, the amount of cached data available via physical acquisition can be overwhelming.

Extended Keychain Acquisition

iOS 7 introduced some changes to the format and content of Apple's protected storage, the keychain. In iOS 7 devices, a device registered to a certain Apple ID may contain a cached copy of the iCloud keychain for that Apple account, depending on whether or not the user authorized this feature. If present, this data opens a whole new perspective to forensic specialists, enabling instant access to stored passwords and credit card information stored in other Apple devices on the same Apple ID.

ELCOMSOFT
PROACTIVE SOFTWARE

iCloud Access as a Bonus

iOS 7 keeps more information in the keychain than any previous version of iOS. As a result, investigators performing physical acquisition may be able to receive, among other things, the online credentials required to log in to Apple iCloud (subject to certain conditions). If present, this information enables forensic specialists to download information Apple iCloud, acquiring online backups to all iOS devices registered on the same account. A separately available product, Elcomsoft Phone Password Breaker, is required to download information from the iCloud. In addition, by using Find My Phone service from Apple iCloud investigators can track geographic location of iOS devices on that account in real time.

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.

The tool can perform physical acquisition of the following iOS devices regardless of lock and jailbreak state, and regardless of iOS version:

- Legacy iPhone models up to and including iPhone 4, all GSM & CDMA models supported
- The original iPad
- iPod Touch generations 1 through 4

Physical acquisition can be performed for the following models if they are running iOS 5, all versions of iOS 6, or iOS 7 and are jailbroken, or if jailbreak code can be installed by the investigator:

- iPhone 4S, 5 and 5C
- iPad 2, 3 and 4
- iPad Mini
- iPod Touch 4th and 5th gen

Support for iPhone 5S, iPad Air and iPad Mini with Retina is under development.
For non-jailbroken iOS 7 devices with unknown passcode physical acquisition support is currently unavailable.

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 7. 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 iTunes password and conversations carried over various social networks such as Facebook, as well as all application-specific data saved in the device. The tool can also perform logical acquisition of iOS devices, or provide forensic access to encrypted iOS file system dumps.

About ElcomSoft Co. Ltd.

Founded in 1990, ElcomSoft Co.Ltd. is a global industry-acknowledged expert in computer and mobile forensics providing tools, training, and consulting services to law enforcement, forensics, financial and intelligence agencies. ElcomSoft pioneered and patented numerous cryptography techniques, setting and exceeding expectations by consistently breaking the industry's performance records. ElcomSoft is Microsoft Gold Independent Software Vendor, Intel Software Premier Elite Partner, member of Russian Cryptology Association (RCA) and Computer Security Institute.