

ElcomSoft Brings New Life to iOS Forensics, Adds Physical Acquisition Support for iPhone 5 and iPad 4



Moscow, Russia – July 17, 2013 - ElcomSoft Co. Ltd. updates [iOS Forensic Toolkit](#), enabling physical acquisition of jailbroken iOS 5 and iOS 6 devices including iPhone 4S and 5, iPad 2, 3 and 4, iPad Mini as well as the last generations of iPod Touch. Support for iPhone 4S and 5 has been highly demanded by forensic customers. By enabling physical acquisition of last-generation Apple devices, the updated Elcomsoft iOS Forensic Toolkit makes forensic analysis of these iOS devices once again a feasible enterprise.

In addition, the latest release of iOS Forensic Toolkit automates the acquisition of jailbroken devices, getting rid of previously required manual steps, reducing required manual interaction to absolute minimum. Finally, the acquisition of legacy devices is now completely automated with automatic detection of devices being connected.

[Elcomsoft iOS Forensic Toolkit](#) continues providing unrestricted support for legacy iOS devices such as iPhone 4 and earlier regardless of the iOS version they are running. Passcodes protecting these legacy devices can be recovered; however, physical acquisition can be carried out in somewhat limited mode even without a passcode. However, physical acquisition support for last-generation iOS devices is subject to certain technical limitations. iPhone 4S and 5 as well as the last generations of iPad devices can only be acquired if already jailbroken, or if the investigator is able to jailbreak the device. At this time, non-jailbroken devices that are locked with an unknown passcode cannot be acquired, which does limit this tool's scope of use.

Passcode recovery speed on jailbroken iPhone 5 devices is increased to 15.5 passcodes per second, allowing iOS Forensic Toolkit to break typical 4-digit passcodes in about 10 minutes.

iOS 6 Physical Acquisition Background

Previous versions of [iOS Forensic Toolkit](#) already supported jailbroken iPhone 4S and iPad 2 and 3 models running iOS 5. However, iOS 6 implements new security measures. Up until now, general agreement was that is not possible to use physical acquisition on devices running iOS 6. Apparently, ElcomSoft did what most thought was impossible once again.

The Benefits of Physical Acquisition

Physical acquisition is the method of choice for accessing information stored in iOS devices. When having a choice, forensic customers performing physical acquisition will obtain more information from the device than by using any other method such as logical acquisition or backup analysis. While it is difficult to predict how long it would take to break a password protecting an offline backup, physical acquisition operates on fixed-timeframe basis, which guarantees the delivery of the entire content of a 32-GB device in 40 minutes or less (depending on the amount of information stored in the device). Much more information is available with physical acquisition compared to backup analysis, creating a bit-precise image of the device in real time. It also returns more data than logical acquisition, as many files are locked by the operating system and not accessible during the process of logical acquisition.

Providing near-instant forensic access to encrypted information stored in the latest iPhone and iPad devices, [Elcomsoft iOS Forensic Toolkit](#) enables access to protected file system dumps extracted from supported Apple devices even if the original device passcode is unknown.

Other Acquisition Methods

If physical acquisition is not possible, ElcomSoft offers additional acquisition options via a separate product. Elcomsoft Phone Password Breaker allows accessing information stored in offline backups produced by the device on a local computer, and acquiring a copy of device's content from Apple iCloud. Elcomsoft Phone Password Breaker is available at <http://www.elcomsoft.com/eppb.html>

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 3

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

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

At this time, physical acquisition has been tested on iOS 6.1.2 and all prior versions. Newer versions of iOS are not currently supported on recent devices as no jailbreak is available.

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 6. 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.