ELCOMSOFT
PROACTIVE SOFTWARE

ElcomSoft All-In-One iOS Forensic Toolkit: Now with Keychain Decryption, Windows Support and iOS 4.3.4 Acquisition

Moscow, Russia – July 25, 2011 - ElcomSoft Co. Ltd. releases a major update to its iOS Forensic Toolkit, implementing an all-in-one toolkit for iOS acquisition on both Windows and Mac platforms. The company adds multiple new features to make iOS analysis faster, easier and more comprehensive at the same time. Elcomsoft iOS Forensic Toolkit provides near-instant forensic access to encrypted information stored in iPhone devices, and offers researchers the ability to access protected file system dumps extracted from iPhone devices even if the data was encrypted with a security chip by iOS 4.

The newest release adds Windows support, supports logical acquisition in addition to physical acquisition, and can instantly retrieve the original passcode in devices running iOS 3.x. Brute-force passcode recovery is available for devices running iOS 4.x. In addition, Elcomsoft iOS Forensic Toolkit now supports full recovery of keychain information, decrypting login and password information to Web sites and protected resources, and records a comprehensive log of all operations. The latest iOS 4.3.4 featuring additional anti-tampering measures is now fully supported.

Physical Acquisition as The Most Sophisticated iOS Forensic Analysis Method

The physical acquisition method uses the dumped contents of the physical device to perform a comprehensive analysis of user and system data stored in the device. Before Elcomsoft iOS Forensic Toolkit, decrypting the encrypted dump was simply not possible, with or without the passcode. The process is possible without brute-forcing the original passcode (a lengthy process that was slowing down forensic investigations based on the analysis of iPhone backup files). Typically, the complete acquisition of a 32 Gb iPhone 4 running iOS 4.x takes less than 1.5 hours.

Physical acquisition analysis provides access to a lot more information about the usage of an iOS device than a backup file can store, and offers investigators a number of additional benefits not available with the analysis of backup files.

- Zero footprint: no changes are made to the device or its contents;
- All-in-one solution;
- Bit-precise images: physical acquisition deals with complete system dumps, precise to the last bit;
- Typical acquisition time of under two hours;
- Industry-standard forensic analysis products can be used to analyze the decrypted dump.

The new edition of Elcomsoft iOS Forensic Toolkit can also perform logical acquisition faster by transferring only actual user files and omitting unallocated disk space. With logical acquisition, the decryption is performed by the device itself (although files requiring passcode for decryption are not included with the logical acquisition image).

(Continued on next page)

Passcode Not Required (But Comes Handy at Times)

Elcomsoft iOS Forensic Toolkit implements the ability to brute-force passcodes right on the iOS 4.x devices being acquired, although this is not always needed.

The toolkit does not require the forensic analyst to know the original passcode. The complete acquisition of an iOS 3.x device is possible without knowing the passcode; in addition, Elcomsoft iOS Forensic Toolkit can instantly extract the original passcode from such devices.

In iOS 4.x devices, certain information such as keychains and email messages will not be accessible without having either a passcode or a valid escrow file (obtainable from a computer to which the iOS device has been connected/synced to). Recovering a typical 4-digit passcode with Elcomsoft iOS Forensic Toolkit normally takes no longer than 20 to 40 minutes.

Background

iPhone users accumulate huge amounts of highly sensitive information stored in their smartphones. Besides the obvious pieces such as pictures, email and SMS messages, iPhone devices store advanced usage information such as historical geolocation data, viewed Google maps and routes, Web browsing history and call logs, login information (usernames and passwords), and nearly everything typed on the iPhone.

Some but not all of this information ends up being stored in iPhone backups when they're produced with Apple iTunes. However, the amount of information that can be extracted from phone backups is naturally limited.

Forensic specialists are well aware of the amount of valuable information stored in these devices. Physical acquisition offers forensic analysts several important benefits over the analysis of information stored in iPhone backups. While offering full access to all of the data stored inside these devices, physical acquisition is the only fully accountable, zero-footprint method that, in addition to all user information such as SMS and email messages, can also access protected information stored in keychains.

About Elcomsoft iOS Forensic Toolkit

Elcomsoft iOS Forensic Toolkit provides forensic access to encrypted information stored in popular Apple devices running iOS 3.x and 4.x. 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 and the original plain-text user passcode. The tool can also perform logical acquisition of iOS devices, or provide forensic access to encrypted iOS file system dumps.

Availability and Distribution

Elcomsoft iOS Forensic Toolkit is available immediately. Access to the new tool is limited to forensic, law enforcement, and select government agencies. Pricing available by request; discounts for existing customers are available.

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 and its officers are members of the Russian Cryptology Association. ElcomSoft is a Microsoft Gold Certified Partner and an Intel Software Partner.