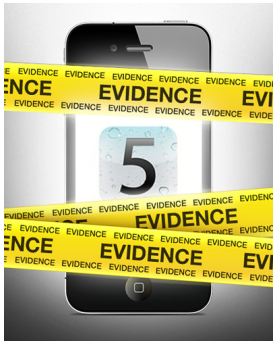
ElcomSoft Updates iOS Forensic Toolkit with iOS 5 Support and Faster Acquisition Times



Moscow, Russia – November 1, 2011 – ElcomSoft Co. Ltd. updates iOS Forensic Toolkit, adding iOS 5 to the list of supported systems. With iOS 5 support, Elcomsoft iOS Forensic Toolkit can recover device passcodes and/or perform physical acquisition analysis of Apple devices running iOS 3.x, 4.x and 5. In addition, the speed of physical acquisition was improved 2 to 2.5 times. With more than double the acquisition speed of the earlier versions, the updated Elcomsoft iOS Forensic Toolkit can acquire a 16-Gb iPhone 4 in about 20 minutes, or a 32-Gb version in 40 minutes.

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.

Forensic Analysis of iOS 5 Devices

With the release of iOS 5, Apple made some minor tweaks and some major changes to data encryption. *"There was no break-through in the iOS security model"*, says Andrey Belenko, ElcomSoft leading developer. *"The architectural changes are more of an evolution of the existing model. However, we highly welcome these changes, as they present better security to the end user. In particular, the number of keychain items that can be decrypted without the passkey is now less than it used to be. Device passcode is one of the hallmarks of Apple's security model, and they are expanding the use of it to cover more data than ever before."*

While the majority encryption algorithms appear to be simply tweaked a bit, Apple made a significant change to security settings regarding the keychain protection, replacing the keychain encryption algorithm entirely. In addition, Apple made Escrow Keybag useless to forensic specialists by protecting the escrow keys with device passcode. Apparently, the protection of sensitive information stored in iOS 5 devices relies more heavily on device passcode than in earlier versions.

"I love challenges", says Dmitry Sklyarov, ElcomSoft's leading cryptanalysis specialist. *"The new system release presented a perfect case. When we just started, we didn't even know if we have a chance to break it. There are all-new encryption algorithms, changed keychain protection, new data structures… the list goes on and on. We did most of it before at the time of iOS 4 release, but the new system presented some unexpected challenges."*

Keychains contain significant amounts of information that is highly valuable to forensic investigators. This information includes stored logins and passwords to Web sites, Wi-Fi access passwords, email and application passwords, and more. In the light of the new encryption used to protect keychain items, Elcomsoft iOS Forensic Toolkit is the first commercially available product to offer full support for recovering keychain information in iOS 5 devices.

The recovery of most keychain items requires the knowledge of the original device passcode. Elcomsoft iOS Forensic Toolkit can recover the original passcode by performing a brute-force attack. Knowing the plain-text passcode, Elcomsoft iOS Forensic Toolkit can decrypt all items stored in the keychain.

Background

Forensic specialists are well aware of the amount of valuable information stored in Apple iOS devices such as the iPhone. 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.

The physical acquisition analysis uses the dumped contents of the actual device to perform a comprehensive investigation of user and system data stored in the device. 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. Before Elcomsoft iOS Forensic Toolkit, decrypting the encrypted dump was simply not possible, whether or not the original passcode was available. The latest version of Elcomsoft iOS Forensic Toolkit makes such acquisition possible in about 20 minutes for a 16-Gb iPhone to 40 minutes for a 32-Gb version.

About Elcomsoft iOS Forensic Toolkit

Elcomsoft iOS Forensic Toolkit provides forensic access to encrypted information stored in popular Apple devices running iOS 3.x, 4.x, and iOS 5. 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 generally provided to qualified 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 Premier Elite Partner*.

Elcomsoft iOS Forensic Toolkit supports Windows (XP, Vista, Windows 7, Server 2003 and Server 2008 Server) and MacOS X (10.6 'Snow Leopard' and 10.7 'Lion'), and is available to select government and law enforcement customers. More information at http://ios5.elcomsoft.com/