ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

Elcomsoft Extracts Critical Evidence from iOS 12 Devices

ElcomSoft Co. Ltd. releases a major update of iOS Forensic Toolkit, the company's mobile forensic tool for extracting data from a range of Apple devices. Version 5.0 adds forensic extraction support for a wide range of Apple devices running iOS 12. To gain low-level access to the file system of devices being imaged, iOS Forensic Toolkit makes use of the new generation of rootless jailbreaks. Rootless jailbreaks offer the benefit of significantly smaller forensic footprint without remounting the file system of modifying the system partition while still allowing unrestricted access to the file system.

"Critical evidence may not be available without low-level access to the file system", says **Vladimir Katalov**, ElcomSoft CEO. *"iOS Forensic Toolkit opens the door to pretty much everything the user has on the device. Secret chats, deleted messages, working databases and cached items are just a few things that are exclusively available via physical extraction."*

Physical Acquisition for iOS 12 Devices

Elcomsoft iOS Forensic Toolkit 5.0 enables forensic experts to perform physical extraction of a range of Apple devices running all versions of iOS 12 up to and including iOS 12.1.2, making physical extraction available for a range of fairly recent versions of iOS. The Toolkit enables file system extraction for all supported devices, and allows decrypting the keychain to extract stored passwords and authentication credentials. iOS keychain is Apple's tightly secured system storage for keeping secret data.

Physical acquisition offers numerous benefits compared to all other acquisition methods by enabling access to protected parts of the file system and extracting data that is not synced with iCloud or included in local backups. In particular, physical acquisition is the only method for accessing keychain items targeting the highest protection class. ElcomSoft has developed a process for extracting and decrypting protected keychain items returning significantly larger amount of evidence compared to logical or cloud extraction. Keychain items that are exclusively available through physical extraction include passwords to secure apps as well as authentication tokens to email accounts, online services and social networks that are never uploaded to iCloud or saved in system backups.

File system extraction gains full access to application sandboxes and all system areas. Downloaded email messages, databases of secure instant messaging apps, secrets from two-factor authentication apps, system logs and low-level location data are just a few things that are exclusively available with file system extraction.

Support for Rootless Jailbreak

Low-level access to the file system requires elevated privileges that are not available on "stock" versions of iOS. A privilege escalation through exploit or public jailbreak is required to image the file system. Previous versions of iOS Forensic Toolkit used to rely on public jailbreaks to gain privileged access to protected parts of the device. For the purpose of mobile forensic, classic jailbreaks are far from perfect due to the significant footprint they leave on the device even after being removed. Traditional jailbreaks make steps to remount the file system and alter the content of the system partition making the device difficult to revert to unmodified condition.

For the first time, iOS Forensic Toolkit does not rely on a full stand-alone jailbreak to access the file system. Instead, the Toolkit makes use of a rootless jailbreak "rootlessJB" that comes with significantly smaller forensic footprint compared to traditional jailbreaks used to image previous versions of iOS. Unlike traditional jailbreaks, rootless jailbreak does not remount the file system and does not alter the content of the system partition. As a result, rootless jailbreak can be fully removed after the acquisition without requiring a system restore to return the system partition to its original unmodified state.

At this time, rootless jailbreak is supported for most devices capable of running iOS 12. We expect the list of supported devices to grow in the course of further development.

> More information about the new acquisition process and rootless jailbreak available in ElcomSoft blog post **Physical Extraction and File System Imaging of iOS 12 Devices**

Pricing and Availability

Elcomsoft iOS Forensic Toolkit 5.0 is immediately available in Windows and Mac editions. North American pricing starts from $1,499 (local pricing may vary). 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. Elcomsoft iOS Forensic Toolkit is available stand-alone and as part of Elcomsoft Mobile Forensic Bundle, which offers many additional features including cloud extraction.

Compatibility

Windows and macOS 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; for some versions of iOS logical acquisition is the only available method. iOS Forensic Toolkit supports all devices running iOS 7 through iOS 12.1.2.

About Elcomsoft iOS Forensic Toolkit

Elcomsoft iOS Forensic Toolkit provides forensic access to encrypted information stored in popular Apple devices running iOS. By performing physical acquisition of the device, 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 (subject to jailbreak availability). Physical acquisition for 64-bit devices returns significantly more information compared to logical and over-the-air approaches.