Elcomsoft iOS Forensic Toolkit
Version 6.30

Elcomsoft iOS Forensic Toolkit helps forensic experts perform physical and logical acquisition of iOS devices, by imaging device file system, extracting device secrets (passwords, encryption keys and protected data) and decrypting the file system image.

Summary

In this release, Elcomsoft iOS Forensic Toolkit 6.30 expands jailbreak-free extraction all the way back to iOS 9, now supporting all 64-bit devices running all builds of iOS 9. In addition, the new release can now extract user data only, speeding up the acquisition process by skipping the static system files.

Essential updates

Full jailbreak-free support for iOS 9

In Elcomsoft iOS Forensic Toolkit 6.30, we have further expanded the capabilities of jailbreak-free extraction. The agent-based extraction now delivers full keychain decryption and file system extraction support without a jailbreak for systems as old as iOS 9.0 running on any supported 64-bit hardware.

Originally released with the iPhone 6s, iOS 9 is supported on a relatively wide range of Apple devices. iOS 9.0 through 9.3.5 is available on the iPhone 5s, iPhone 6 and 6 Plus, iPhone 6s and 6s Plus models. The original 4-inch iPhone SE was released with iOS 9.3 on board. The corresponding iPad versions are also supported, including iPad Air, iPad Air 2, iPad Mini 2 through 4, and the first-generation iPad Pro. While one is hardly likely to encounter an iOS 9 device in the wild, forensic labs still process devices running the older version of the OS.

Installing the agent requires the use of an Apple ID registered in Apple's Developer Program. More about that in our blog article Why Mobile Forensic Specialists Need a Developer Account with Apple.

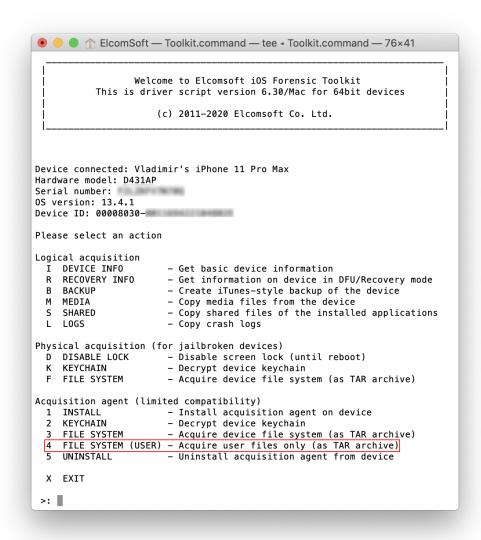### New option for user file system extraction

This update brings a new acquisition option: file system extraction of user data. This new extraction option helps experts save time and disk space by pulling only the content of the data partition while leaving the static system partition behind. Data in the system partition contains read-only executable files, system libraries and other data required for the operating system to run. Unless jailbroken, the content of the system partition does not vary across devices of the same model running the same version of iOS and is far less relevant for the investigation compared to user data.

For small-capacity iPhones, the new option can speed up the extraction two to three times compared to full device extraction. Higher capacity devices offer comparatively lesser time savings, yet the user-targeted set is still easier to analyze.

Version 6.30 change log

- Added jailbreak-free file system and keychain acquisition with extraction agent for iOS 9

- Added the ability to extract user data only (skipping system files)

```
● ● ●      ⌂ ElcomSoft — Toolkit.command — tee ‹ Toolkit.command — 76×41

 _____
|                                                                     |
|               Welcome to Elcomsoft iOS Forensic Toolkit             |
|        This is driver script version 6.30/Mac for 64bit devices     |
|                                                                     |
|                   (c) 2011-2020 Elcomsoft Co. Ltd.                  |
|_____|


Device connected: Vladimir's iPhone 11 Pro Max
Hardware model: D431AP
Serial number:
OS version: 13.4.1
Device ID: 00008030-

Please select an action

Logical acquisition
    I  DEVICE INFO      - Get basic device information
    R  RECOVERY INFO    - Get information on device in DFU/Recovery mode
    B  BACKUP           - Create iTunes-style backup of the device
    M  MEDIA            - Copy media files from the device
    S  SHARED           - Copy shared files of the installed applications
    L  LOGS             - Copy crash logs

Physical acquisition (for jailbroken devices)
    D  DISABLE LOCK     - Disable screen lock (until reboot)
    K  KEYCHAIN         - Decrypt device keychain
    F  FILE SYSTEM      - Acquire device file system (as TAR archive)

Acquisition agent (limited compatibility)
    1  INSTALL          - Install acquisition agent on device
    2  KEYCHAIN         - Decrypt device keychain
    3  FILE SYSTEM      - Acquire device file system (as TAR archive)
    4  FILE SYSTEM (USER) - Acquire user files only (as TAR archive)
    5  UNINSTALL        - Uninstall acquisition agent from device

    X  EXIT

 >:
```