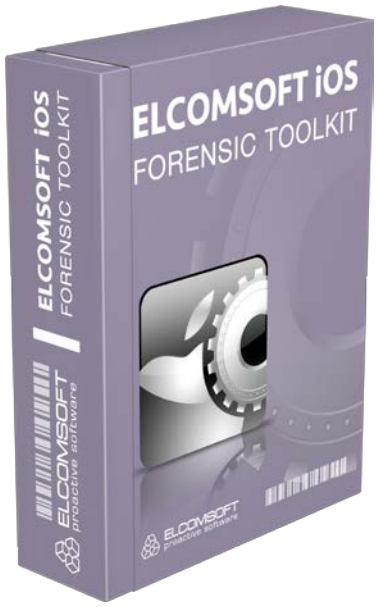
ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

Elcomsoft Decrypts Secrets from iPhone Devices and Extracts User Passwords



Moscow, Russia – June 20, 2018 - ElcomSoft Co. Ltd. updates iOS Forensic Toolkit, the company's mobile forensic tool for extracting data from iPhones, iPads and iPod Touch devices. Version 4.0 shifts adds the ability to extract and decrypt users' passwords and device secrets stored in the system keychain. In addition, the new release can now extract iOS crash logs even on devices without a jailbreak, giving investigators insight on the apps used in the past that are not currently installed.

In iOS Forensic Toolkit 4.0, physical acquisition support is available for all 64-bit Apple devices (iPhone 5s, 6/6s/7/8/Plus, iPhone SE and iPhone X) on which a jailbreak can be installed.

Decrypting Device Secrets

In iOS, most passwords to the user's online accounts, authentication tokens, certificates, encryption keys, payment data and app-specific credentials are stored in a the most protected and highly secure area called the keychain. While some keychain items can be recovered by analyzing a password-protected local backup, records protected with ThisDeviceOnly attribute can be only decrypted on the device itself. Such records cannot be accessed by analyzing a local backup.

The keychain is securely encrypted with a hardware-specific key. In 64-bit hardware (iPhone 5s and all newer iOS devices), this key is additionally protected with Secure Enclave. Until today, no third-party forensic solution existed to extract and decrypt keychain items from 64-bit iOS devices with Secure Enclave. Jailbreak or not, bypassing Secure Enclave protection was long considered impossible.

iOS Forensic Toolkit 4.0 adds the ability to extract and decrypt keychain items during the course of physical acquisition, successfully bypassing Secure Enclave protection on jailbroken devices. Notably, the entire content of the keychain is decrypted including records secured with ThisDeviceOnly attribute, allowing to extract the most valuable secrets such as authentication tokens. This in turn enables investigators to access all social media and instant messaging accounts ever used on the device. The tool prevents automatic screen lock of the iOS device during the acquisition to make sure that even those records with the strongest security attributes are successfully extracted and decrypted.

Access to Crash Logs

Crash logs are an important part of the evidence that are not included into a local backup but may be extractable from the device. From a forensic point of view, crash logs may contain the list of installed and uninstalled apps. Once the expert discovers a crash log entry created by an app that is no longer present in the system, an assumption can be made that the app was installed on the device at least up to the date and time specified in the crash log entry.

iOS Forensic Toolkit 4.0 adds the ability to extract crash logs from iOS devices with or without a jailbreak. Access to crash logs requires a paired device or access to a valid lockdown file.

Streamlined Usage Experience

In iOS Forensic Toolkit 4.0 presents a refreshed user interface offering streamlined user experience and straightforward acquisition workflow. iOS Forensic Toolkit 4.0 fully supports logical acquisition of iOS devices (with or without a jailbreak), extracting more evidence than available through iTunes backups. The tool and provides additional physical acquisition options for jailbroken devices.

Pricing and Availability

Elcomsoft iOS Forensic Toolkit 4.0 is immediately available in Mac and Windows editions. North American pricing starts from $1,499. 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 devices running some versions of iOS logical acquisition is the only available method. iOS Forensic Toolkit supports most devices running iOS 7 through iOS 11.

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 11.x. 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 including Apple iPhone 5S, 6/6s/7/8 and their Plus versions, as well as the iPhone X, iPad Pro and Apple TV 4 and 4K (subject to jailbreak availability). Physical acquisition for 64-bit devices returns significantly more information compared to logical and over-the-air approaches.

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 Certrified Partner (Gold competency), and Intel Software Premier Elite Partner.