ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS

Elcomsoft Implements BFU Keychain Extraction from Locked and Disabled iPhones

ElcomSoft Co. Ltd. updates iOS Forensic Toolkit, the company's mobile forensic tool for extracting data from a range of Apple devices. Version 5.21 adds partial extraction of iOS Keychain from select Apple devices running all versions of iOS from iOS 12 to iOS 13.3. Partial keychain extraction is now possible from disabled and locked iPhones in BFU (Before First Unlock) state even if the screen lock password is not known.

BFU keychain extraction is available on select Apple devices, and requires installing the checkra1n jailbreak. Supported devices range from the iPhone 5s all the way up to the iPhone X, iPad models from iPad mini 2 to iPad Pro 10.5 and the new iPad (2018).

About the iPhone BFU Mode

The BFU stands for "Before First Unlock". BFU devices are phones that have been powered off or rebooted and have never been subsequently unlocked, not even once, by entering the correct screen lock passcode.

In Apple's world, the content of the iPhone remains securely encrypted until the moment the user taps in their screen lock passcode. The screen lock passcode is required by Secure Enclave to produce the encryption key, which in turn is used to decrypt the iPhone's file system. In other words, almost everything inside the iPhone remains encrypted until the user unlocks it with their passcode after the phone starts up.

It is the "almost" part of the "everything" that's being targeted by Elcomsoft iOS Forensic Toolkit. The company has discovered certain parts of data being available in iOS devices even before the first unlock. In particular, some keychain items containing authentication credentials for email accounts and a number of authentication tokens are available before first unlock to allow the iPhone to start up correctly before the user punches in the passcode.

Partial Keychain Extraction from BFU iPhones

For the first time, iOS Forensic Toolkit 5.21 enables forensic extraction of iOS Keychain from BFU (Before First Unlock) devices, as well as for locked devices with unknown screen lock passcode.

Compared to unlocked extraction, the new BFU extraction mode can only unlock a limited number of keychain records. In particular, records with authentication credentials for some email accounts and a number of authentication tokens can be extracted.

Accessing the keychain in BFU mode requires installing the checkra1n jailbreak that targets vulnerabilities in Apple bootrom. The jailbreak is installed via DFU mode and is available for all compatible devices regardless of their lock state of BFU/AFU status.

Usability Improvements

In addition to BFU keychain extraction, the update implements a new, unambiguous file naming

convention for the file system image and keychain TAR files. The files are named UDID_timestamp.tar and keychain_UDID_timestamp.xml. The unique device ID and timestamp in the file names make extracted file system images and keychain dumps easily archivable.

Supported Devices

The list of supported devices includes models based on Apple's A7 through A11 SoC. This includes the iPhone 5s, 6, 6s, SE, 7 and 8 along with the Plus versions, as well as the iPhone X. Apple iPad devices running on the corresponding CPUs are also supported, which includes models ranging from the iPad mini 2 all the way up to the 2018 iPad, iPad 10.2, iPad Pro 12.9 (1.Gen) and iPad Pro 10.5.

Pricing and Availability

Elcomsoft iOS Forensic Toolkit 5.21 is immediately available in Windows and Mac editions. North American pricing starts from $1,495 (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.

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.

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.