Elcomsoft iOS Forensic Toolkit
Version 6.20

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 6.20 fills the gaps for jailbreak-free extraction of previously unsupported versions of iOS. The new release expands the availability of the extraction agent all the way back to the original iOS 10.0, while adding compatibility for previously unsupported versions of iOS 12 on the iPhone 5s and 6.

Essential updates

Full jailbreak-free support for iOS 10

The latest release plugs the gap of excepted and unsupported iOS releases, now offering full keychain decryption and file system extraction support without a jailbreak for systems as old as iOS 10.0 running on any supported hardware. Forensic labs still process devices running the older version of the OS, so this update of EIFT adds support for the oldest version of iOS capable of running on the iPhone 7 generation of devices.

Jailbreak-free file system extraction for iOS 12

In addition, we were able to add limited support for the previously unsupported versions of iOS 12 running on the iPhone 5s and 6 devices. For these versions of iOS, Elcomsoft iOS Forensic Toolkit can extract the file system image.

Full support for Apple TV acquisition

Finally, we have expanded support for the Apple TV devices, now offering keychain decryption in addition to file system extraction for both Apple TV 4 (Apple TV HD) and Apple TV 4K running tvOS 13.4 through 13.4.5. The acquisition is made possible with unc0ver jailbreak; more on that in our blog article Jailbreaking Apple TV 4K.
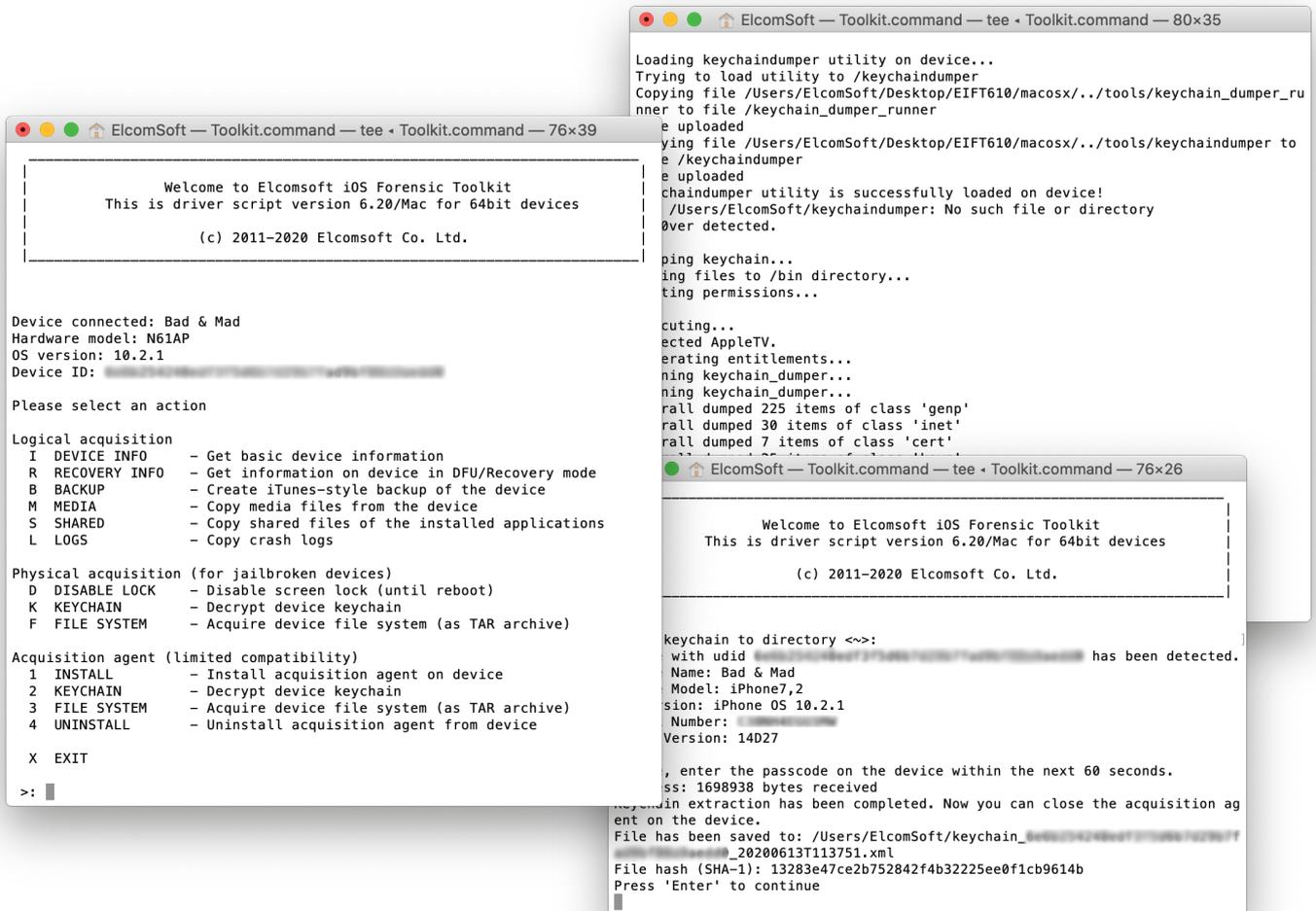
Developer account with Apple

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.

Version 6.20 change log

- Added support for keychain acquisition for Apple TV 4 & 4K running tvOS 13.4 to 13.4.5
- Added full file system and keychain acquisition for iOS 10 (no jailbreak, agent-based)

- Added support for iPhone 5s and iPhone 6 running previously unsupported versions of iOS 12 (no jailbreak, agent-based); file system only

```
| ElcomSoft — Toolkit.command — tee ‹ Toolkit.command — 80×35
Loading keychaindumper utility on device...
Trying to load utility to /keychaindumper
Copying file /Users/ElcomSoft/Desktop/EIFT610/macosx/../tools/keychain_dumper_ru
nner to file /keychain_dumper_runner
e uploaded
ying file /Users/ElcomSoft/Desktop/EIFT610/macosx/../tools/keychaindumper to
e /keychaindumper
e uploaded
chaindumper utility is successfully loaded on device!
/Users/ElcomSoft/keychaindumper: No such file or directory
over detected.

ping keychain...
ing files to /bin directory...
ting permissions...

cuting...
ected AppleTV.
erating entitlements...
nning keychain_dumper...
nning keychain_dumper...
rall dumped 225 items of class 'genp'
rall dumped 30 items of class 'inet'
rall dumped 7 items of class 'cert'
```

```
| ElcomSoft — Toolkit.command — tee ‹ Toolkit.command — 76×39
|─────────────────────────────────────────────────────────────|
|              Welcome to Elcomsoft iOS Forensic Toolkit        |
|        This is driver script version 6.20/Mac for 64bit devices |
|                                                               |
|                  (c) 2011-2020 Elcomsoft Co. Ltd.             |
|─────────────────────────────────────────────────────────────|

Device connected: Bad & Mad
Hardware model: N61AP
OS version: 10.2.1
Device ID:

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  UNINSTALL        - Uninstall acquisition agent from device

  X  EXIT

>:
```

```
| ElcomSoft — Toolkit.command — tee ‹ Toolkit.command — 76×26
|─────────────────────────────────────────────────────────────|
|              Welcome to Elcomsoft iOS Forensic Toolkit        |
|        This is driver script version 6.20/Mac for 64bit devices |
|                                                               |
|                  (c) 2011-2020 Elcomsoft Co. Ltd.             |
|─────────────────────────────────────────────────────────────|

keychain to directory <~>:
 with udid                              has been detected.
 Name: Bad & Mad
 Model: iPhone7,2
sion: iPhone OS 10.2.1
 Number:
Version: 14D27

, enter the passcode on the device within the next 60 seconds.
ss: 1698938 bytes received
keychain extraction has been completed. Now you can close the acquisition ag
ent on the device.
File has been saved to: /Users/ElcomSoft/keychain_
        _20200613T113751.xml
File hash (SHA-1): 13283e47ce2b752842f4b32225ee0f1cb9614b
Press 'Enter' to continue
```

Steps to renew

1. All active users of Elcomsoft iOS Forensic Toolkit are invited to obtain the new version 6.20 by entering product registration key in the online form: https://www.elcomsoft.com/key.html

2. Users having an expired license of Elcomsoft iOS Forensic Toolkit are welcome to renew their license at corresponding cost that is available by entering registration key in the online form: https://www.elcomsoft.com/key.html.

Contact us at sales@elcomsoft.com for any further questions on updating and license renewing.