ELCOMSOFT

Bedford, March 2020

Data acquisition from iOS devices. New approaches and possibilities.

Extracting evidence from a seized iPhone:
Using the latest exploits

iOS Forensics

In This Talk

Physical acquisition at a glance

- Hardware and software limitations
- Pros and cons

Latest exploits and solutions

- Classic jailbreaks
- Rootless jailbreak
- Checkm8 and Checkra1n
- Data acquisition in BFU mode
- Full File System acquisition

iOS Forensics

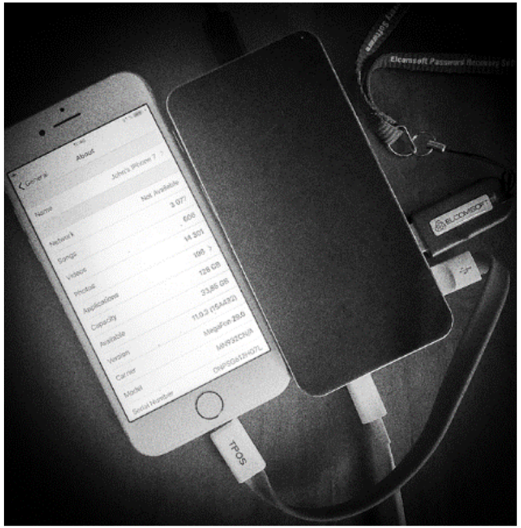
Acquisition Methods That Don’t Work

- Some acquisition methods common on other platforms are not available for iOS
- JTAG: there is no test access port (but technically USB port can be used)
- Chip-off: full-disk encryption makes offline attacks completely useless

Acquiring data from iOS device

Situation before the end of 2019

- Physical acquisition: available for old devices only (with 32-bit CPUs)
- Passcode brute-force is available for old devices
- On newer devices, **jailbreak is required**
- Passcode **must be known** or recovered (using GrayKey or social engineering)
- No jailbreak for certain versions of iOS
- Jailbreaks leave very many traces, corrupt system files and can “brick” the device
- USB restriction mode (iOS 11.4.1, July 2018) blocks all wired connections when the device is locked



Acquiring data from iOS device

Classic jailbreak: Issues

- Jailbreak has many forensic implications
- Dangerous, no guaranteed outcome
- Not forensically sound, introduces artifacts
- Process must be carefully documented
- Semi-tethered jailbreaks expire in 7 days (unless Apple Developer account is used)
- Cydia Impactor does not work with personal accounts anymore
- Each Apple Developer account can be used to sign IPA files to jailbreak a limited number of devices

中文
Change log
革故鼎新
Jailbreak, or not jailbreak, that is NOT a question any more
Download & Help
9.3
for iOS 9.2 - 9.3.3
64-bit devices only
Jailbreak discussion and feedback

Jailbreaks for iOS

What iOS jailbreak actually does

- Escalates privileges of user, allowing:
  - Download, install and run any application, including unsigned ones
  - Access all application sandboxes (many viruses exist for jailbroken iOS devices)
  - In some cases access to all system files including kernel

Jailbreaks for iOS

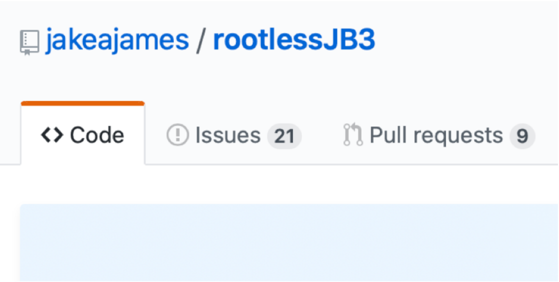
Classic jailbreak

- Allows access to the root of device file system – “/”
- Requires to remount file system to gain access to /
- Modifies many system files
- OTA iOS update becomes impossible
- Leaves very many traces
- In some cases device is unstable until full restore with iTunes

Jailbreaks for iOS

Rootless jailbreak

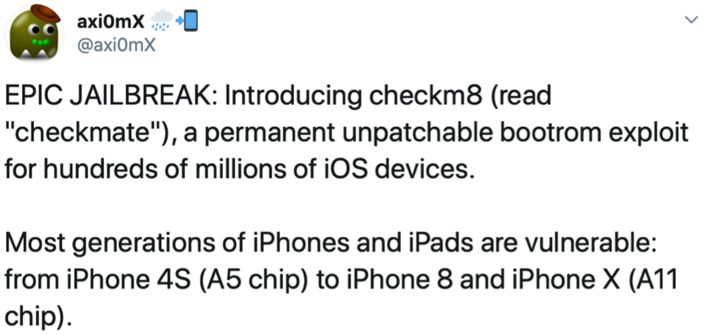
- “Rootless” does not mean “without root access”, it means “without access to the root of file system”
- Can be applied offline with developer account
- File system is **accessible from /var folder**
- Modifies **only files inside /var**
- Leaves significantly less traces than classic JB
- System is more stable
- Rootless jailbreaks are more forensically sound than classic ones


jakeajames / rootlessJB3

Jailbreaks for iOS

Checkm8 hardware exploit

- Was introduced at September 27, 2019
- Uses **exploit in CPU hardware** (boot ROM)
- **Cannot be patched by Apple at all**
- Supports Apple CPUs from A5 to A11
- Supports iOS devices with **ANY iOS version**
- All devices from iPhone 4S to iPhone X are vulnerable



axi0mX 🌧➡📱
@axi0mX

EPIC JAILBREAK: Introducing checkm8 (read "checkmate"), a permanent unpatchable bootrom exploit for hundreds of millions of iOS devices.

Most generations of iPhones and iPads are vulnerable: from iPhone 4S (A5 chip) to iPhone 8 and iPhone X (A11 chip).

Jailbreaks for iOS

Checkra1n jailbreak

- Uses checkm8 exploit
- Device must in DFU mode to apply jailbreak
- Cydia Impactor is not required
- **USB port is always accessible in DFU mode.** No USB restriction mode.
- Many files and databases can be acquired in BFU (before first unlock) state
- **Cannot** recover device passcode
- Any acquisition tool can be used to extract the entire file system of device

Data acquisition in BFU mode

What data is available Before First Unlock

- List of installed applications
- Some Wallet data
- Media files
- Wi-fi connections
- Notifications
- Some location points
- Unprotected records of Keychain

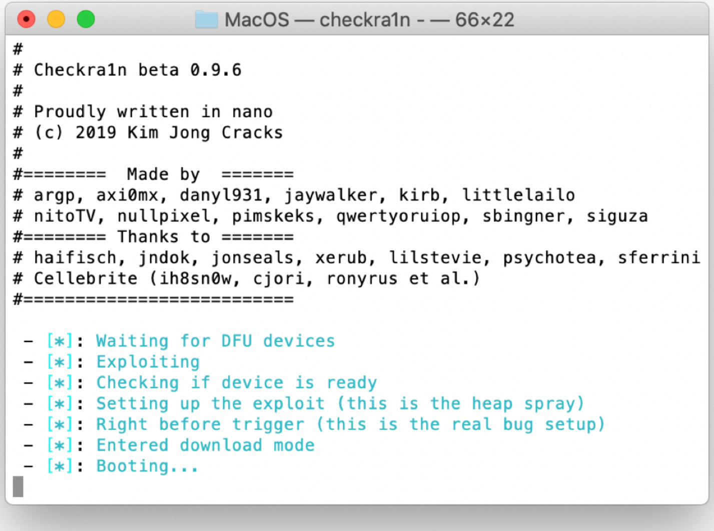
Jailbreaks for iOS

Checkra1n jailbreak: cons

- Many system files are modified by jailbreak – not forensically sound
- Most modifications are not required for file system extraction
- Certain versions put device in USB restricted mode after reboot from DFU
- **iOS 13.4 beta allows DFU mode only with full device wipe**

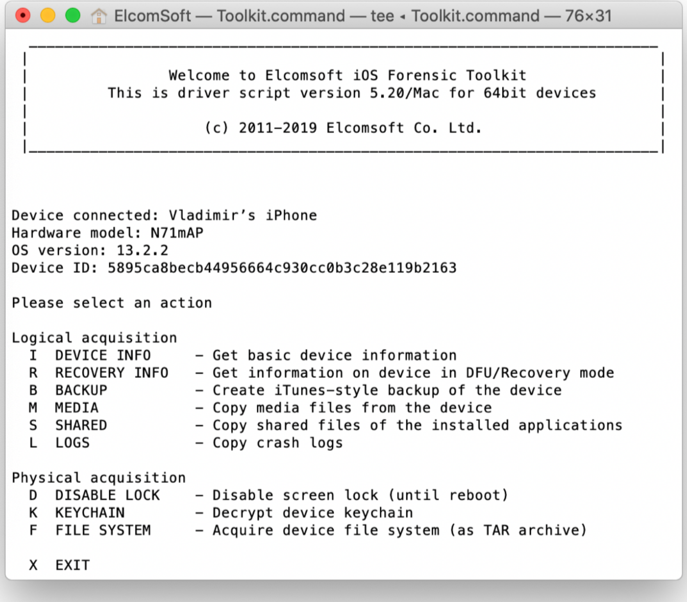
Jailbreaks for iOS

Using EIFT with checkra1n jailbreak



```
#
# Checkra1n beta 0.9.6
#
# Proudly written in nano
# (c) 2019 Kim Jong Cracks
#
#========  Made by  =======
# argp, axi0mx, danyl931, jaywalker, kirb, littlelailo
# nitoTV, nullpixel, pimskeks, qwertyoruiop, sbingner, siguza
#======== Thanks to =======
# haifisch, jndok, jonseals, xerub, lilstevie, psychotea, sferrini
# Cellebrite (ih8sn0w, cjori, ronyrus et al.)
#==========================

 - [*]: Waiting for DFU devices
 - [*]: Exploiting
 - [*]: Checking if device is ready
 - [*]: Setting up the exploit (this is the heap spray)
 - [*]: Right before trigger (this is the real bug setup)
 - [*]: Entered download mode
 - [*]: Booting...
```



```
 __________________________________________________________________________
|                                                                          |
|                   Welcome to Elcomsoft iOS Forensic Toolkit              |
|            This is driver script version 5.20/Mac for 64bit devices      |
|                                                                          |
|                      (c) 2011-2019 Elcomsoft Co. Ltd.                    |
|__________________________________________________________________________|


Device connected: Vladimir’s iPhone
Hardware model: N71mAP
OS version: 13.2.2
Device ID: 5895ca8becb44956664c930cc0b3c28e119b2163

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

  X  EXIT
```

Forensic usage of jailbreak

What jailbreak features we don’t need

~~System modification~~

~~Cydia install~~

~~OTA updates disable~~

~~SSH and other apps~~

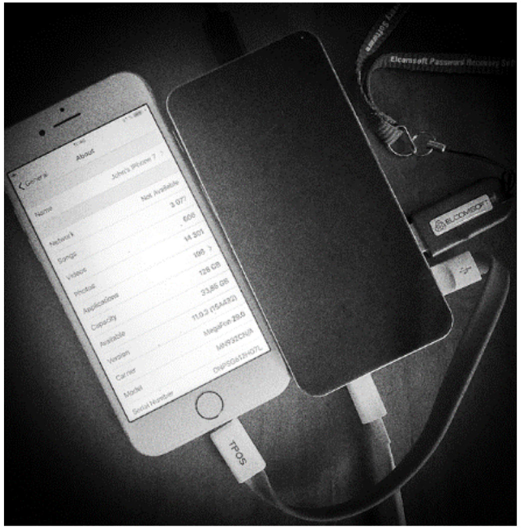
All we need is:

✓ Full file system

FFS Acquisition with agent

Full File System acquisition – acquire data without jailbreak

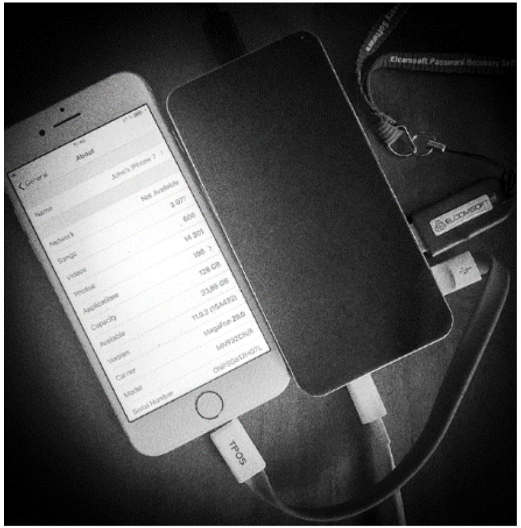
- Most features of jailbreak are not required for forensic acquisition
- ANY jailbreak is not forensically sound, leaves many traces and makes many changes
- ANY jailbreak can “brick” the device
- All we need is **access the device file system and extract Keychain**



FFS Acquisition with agent

Full File System acquisition – acquire data without jailbreak

- Agent (IPA file) is signed by developer’s certificate and uploads to device
- Agent is launching on the device
- Agent exploits system kernel to get file system access
- Connected PC initiates file transfer from agent
- Files are packed in TAR archive
- Keychain can be acquired
- Agent can be deleted from the device
- Leaves only some records in system logs



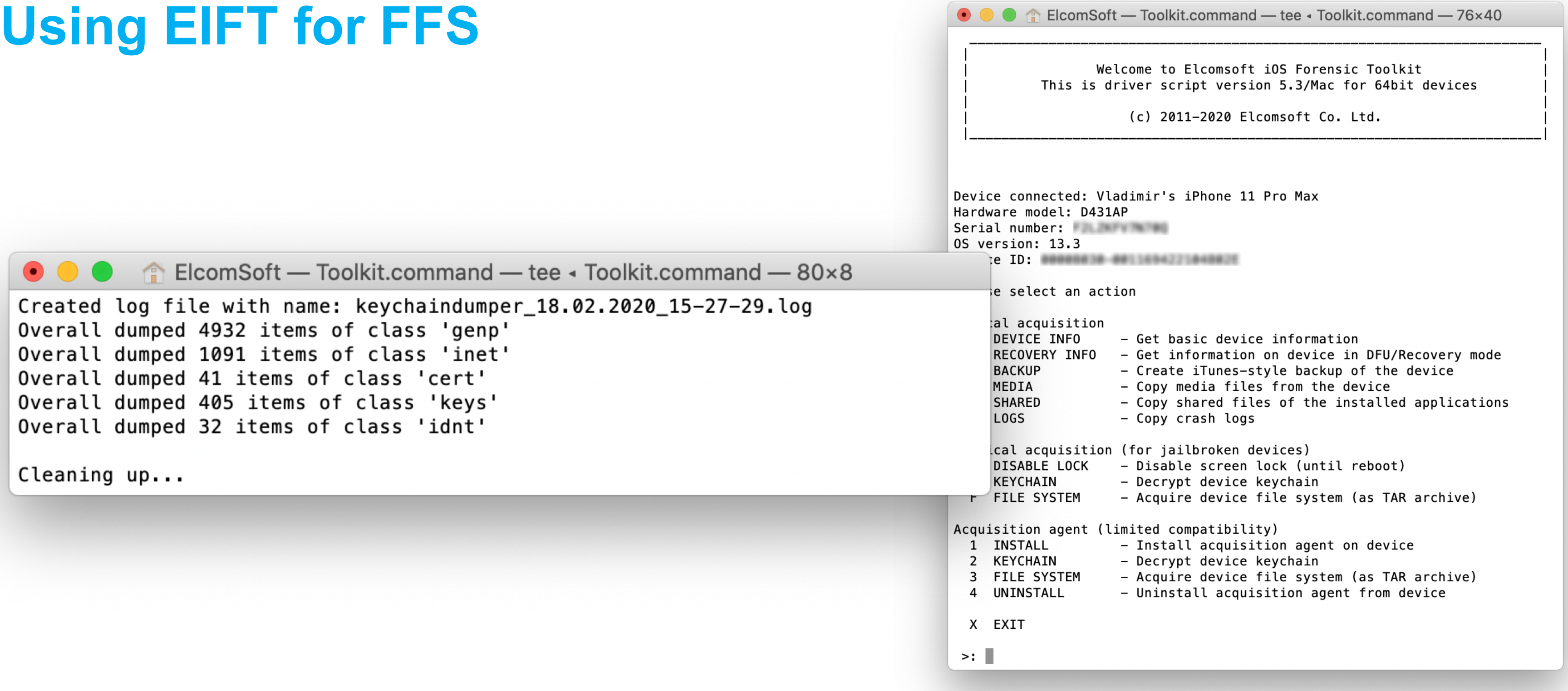
FFS Acquisition with agent

Full File System acquisition – limitations

- Device must be unlocked
- Device passcode must be known
- Certain versions of iOS are not supported
- Certain device models are not supported

FFS Acquisition

Using EIFT for FFS



ElcomSoft — Toolkit.command — tee ◂ Toolkit.command — 80×8

```
Created log file with name: keychaindumper_18.02.2020_15-27-29.log
Overall dumped 4932 items of class 'genp'
Overall dumped 1091 items of class 'inet'
Overall dumped 41 items of class 'cert'
Overall dumped 405 items of class 'keys'
Overall dumped 32 items of class 'idnt'

Cleaning up...
```

ElcomSoft — Toolkit.command — tee ◂ Toolkit.command — 76×40

```
 _________________________________________________________________________
|                                                                         |
|                Welcome to Elcomsoft iOS Forensic Toolkit                |
|       This is driver script version 5.3/Mac for 64bit devices           |
|                                                                         |
|                    (c) 2011-2020 Elcomsoft Co. Ltd.                     |
|_________________________________________________________________________|



Device connected: Vladimir's iPhone 11 Pro Max
Hardware model: D431AP
Serial number: [redacted]
OS version: 13.3
     :e ID: [redacted]

     :e select an action

     :al acquisition
     DEVICE INFO      - Get basic device information
     RECOVERY INFO    - Get information on device in DFU/Recovery mode
     BACKUP           - Create iTunes-style backup of the device
     MEDIA            - Copy media files from the device
     SHARED           - Copy shared files of the installed applications
     LOGS             - Copy crash logs

     .cal acquisition (for jailbroken devices)
     DISABLE LOCK     - Disable screen lock (until reboot)
     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

 >:
```

Methods of data acquisition

Method	Hardware	iOS versions	Root access	Traces	Reliability
Physical	32-bit CPU only: iPhone – iPhone 5C	Up to iOS 7	Yes	No	Reliable, data is acuired in DFU mode
Classic jailbreak	All devices	Up to 12.4, 13.0 – 13.3	Yes	A lot of traces: many applications are installed, system files are modified.	System files modification can “brick” device
Rootless jailbreak	All A7-A11 devices: iPhone 5S – iPhone X	iOS 11-12	No	Few. Only SSH app is installed, does not modify system files at all	Reliable, only /var folder is modified
Checkra1n	iPhone 5S – iPhone X	iOS 12.3 – 13.3.1	Yes	As classic JB	Reliable in most cases, but sometimes “bricks”the device
FFS	All devices	Up to 12.4, 13.0 – 13.3	Yes	Few. Only some records in system logs	Reliable. Doesn’t install applications, doesn’t modify system files.

iPhone 5s/6/6s/7/8/X

all versions of iOS

7–11, 12.0–12.2, 12.4, 13.0–13.3

12.3–12.4.1, 13.0–13.3

AGENT up to 11, 11.0–11.4.1, 12.0– 12.2, 12.4, 13.0–13.3

Full file system & keychain acquisition: with jailbreak with checkra1n/checkm8 AGENT via agent

Advanced logical acquisition

13.0 — supported iOS version
13.0 — support is on its way

iPhone Xr/Xs (A12)

all versions of iOS

12.0–12.2, 12.4, 13.0–13.3

AGENT 12.0– 12.2, 12.4, 13.0–13.3

Full file system & keychain acquisition: with jailbreak with checkra1n/checkm8 AGENT via agent

Advanced logical acquisition

13.0 — supported iOS version
13.0 — support is on its way

iPhone 11 (A13)

all versions of iOS

13.0–13.3

AGENT 13.0–13.3

Full file system & keychain acquisition: with jailbreak with checkra1n/checkm8 AGENT via agent

Advanced logical acquisition

13.0 — supported iOS version
13.0 — support is on its way

Elcomsoft Mobile Forensic Bundle

Our complex solution for mobile forensics

- Acquisition from iOS devices with installed Jailbreak (checkra1n is supported)
- Full file system acquisition with agent
- Decrypt and analyze iTunes backups
- Download iCloud backups (all iOS versions and 2FA are supported)
- Download iCloud synchronized data
- Download from Google cloud
- Convenient viewer to explore acquired data

ELCOMSOFT
MOBILE FORENSIC
BUNDLE
ELCOMSOFT MOBILE FORENSIC BUNDLE
ELCOMSOFT proactive software
ELCOMSOFT proactive software

Official web site:

https://www.ELCOMSOFT.com

Technical blog:

https://BLOG.elcomsoft.com

“Why Mobile Forensic Specialist Need a Developer Account with Apple”

Data acquisition from iOS devices. New approaches and possibilities.

ElcomSoft Co. Ltd.

http://www.elcomsoft.com
http://blog.elcomsoft.com

Facebook: ElcomSoft
Twitter: @elcomsoft