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
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
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

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

---

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: N7/1AP
OS version: 13.2.2
Device ID: 5895ca80e8cd4a4956644c939cc8b3c28e119b2163

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

---

[*]: 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...
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
## Methods of data acquisition

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

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
- 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

Full file system & keychain acquisition:
- With jailbreak
- With checkra1n/checkme0
- 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
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.