

**May 2019**

Vladimir Katalov

# Forensic Implications of iOS Jailbreaking

The benefits, drawbacks and forensic implications of jailbreaking iOS devices



# Forensic Implications of iOS Jailbreak

## In This Talk (1 of 2)

iOS extraction methods compared

- Offline backups & logical acquisition
- Cloud (Over-the-Air) acquisition
- “Physical” (file system) acquisition

Why we need a jailbreak

- Accessing the file system
- Extracting and decrypting the keychain



# Forensic Implications of iOS Jailbreak

## In This Talk (2 of 2)

### Jailbreaks: Classic vs. Rootless

- Installing and removing
- Offline installation
- Traces and consequences
- Forensic implications

### Cellebrite and GrayKey

- Unknown exploits vs. public jailbreaks

### Not just the iPhone

- Jailbreaking and extracting the Apple TV



# Forensic Implications of iOS Jailbreak

## iOS acquisition methods

### Logical acquisition (backups)

- Cleanest and easiest acquisition method (by far)
- Extracts local backup, media files, crash logs, shared files
  - Backups can be encrypted
  - Locked iPhone extraction: may be able to use lockdown/pairing records

### Over-the-air (iCloud) extraction

- Apple ID/password or binary authentication token (limited use)
- Extracts iCloud backups; synchronized data; passwords; Health, Messages; media files
  - Apple constantly improves iCloud protection
  - Can be obtained from Apple with court order (but limited data)

# Forensic Implications of iOS Jailbreak

## iOS acquisition methods

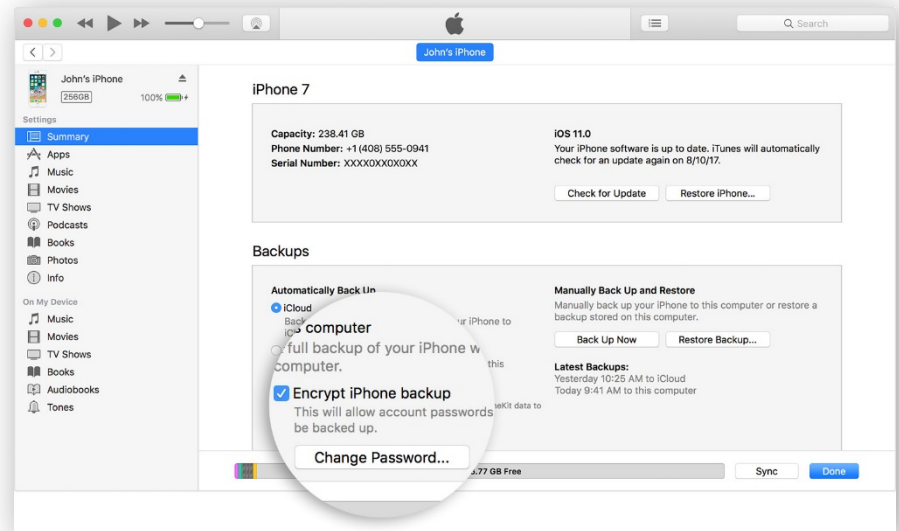
### Physical acquisition

- The most **in-depth extraction** method available:
  - Extracts the complete file system, sandboxed app data, full keychain, system logs etc.
- The most **demanding** method as well
- Device must be unlocked
- **Jailbreak is required**
  - Some installation methods require **Internet connectivity**
  - **Jailbreaking carries multiple consequences and implications**
  - Some jailbreaks are better than others

# Forensic Implications of iOS Jailbreak

## Backup Passwords

- Encrypted backups contain more information than unencrypted
- Must set known backup password before acquisition
- Otherwise, keychain items will be encrypted with a hardware key and cannot be decrypted



# Forensic Implications of iOS Jailbreak

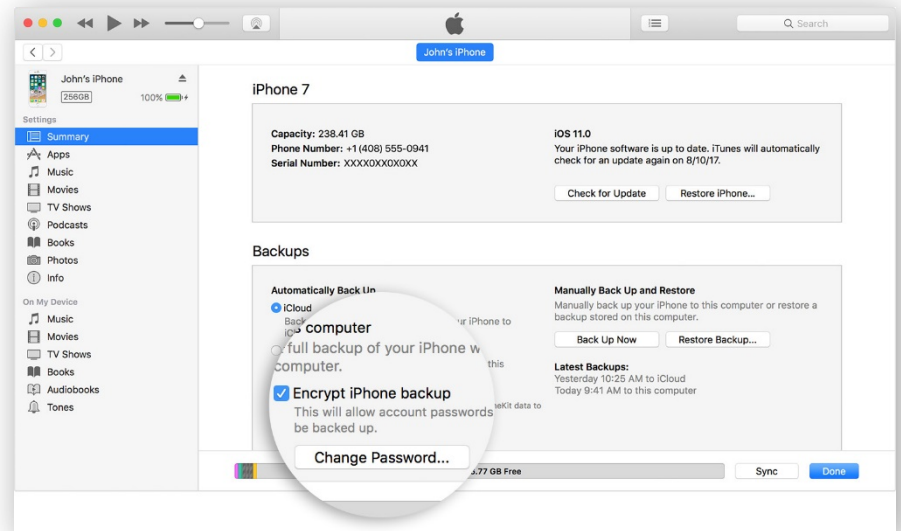
## iTunes Backup Password

If you don't know the password:

**iOS 8..10:** No way to reset or remove it

Can still access device info including Serial Number

**iOS 11/12:** You can reset the password

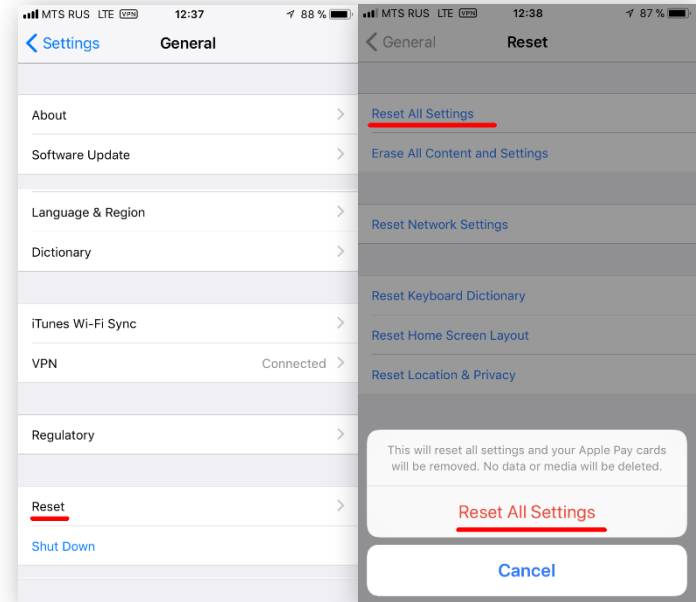


# Forensic Implications of iOS Jailbreak

## iOS 11, 12: Resetting iTunes Backup Password

iOS 11 and 12 allow resetting the iTunes backup password

- Unlock the iPhone with Touch ID, Face ID or passcode.
- Open the **Settings** app and navigate to **General**.
- Scroll all the way down and tap **Reset**.
- Tap and confirm **Reset All Settings**.

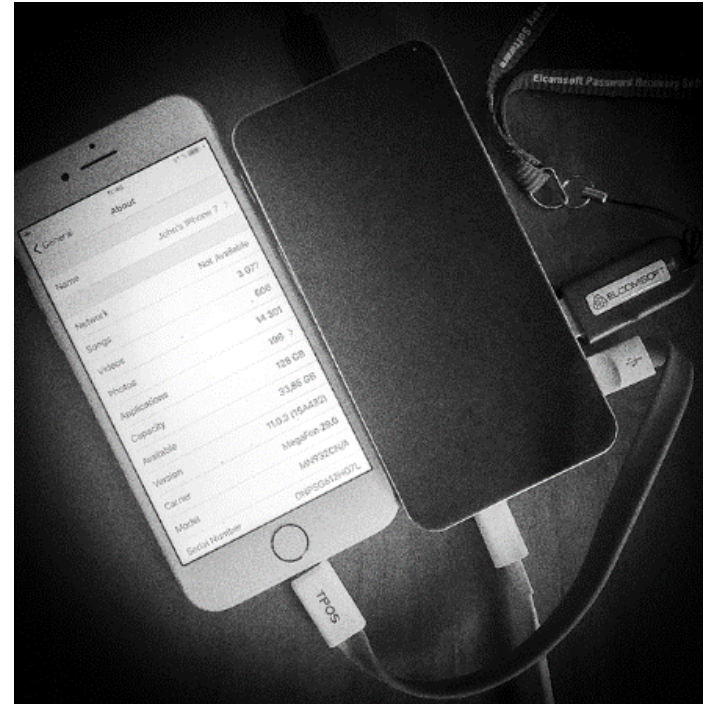




# Forensic Implications of iOS Jailbreak

## Physical Acquisition

- No exactly “physical” acquisition, but complete copy of the file system
- Deleted files cannot be recovered anyway
- On newer (64-bit) devices, jailbreak is required
- **Device must remain unlocked during the entire acquisition process**
- No jailbreak for some versions of iOS (12.1.3+) for now



# Forensic Implications of iOS Jailbreak

## The types of jailbreaks

### Classic jailbreaks

- Dangerous, no guaranteed outcome
- System partition remounted R/W
- Modifications to system partition
- Older jailbreaks patch kernel
- Installs lots and lots of stuff we don't need
  - Such as the Cydia store and code required to disable code signing
- Not forensically sound, introduces artifacts

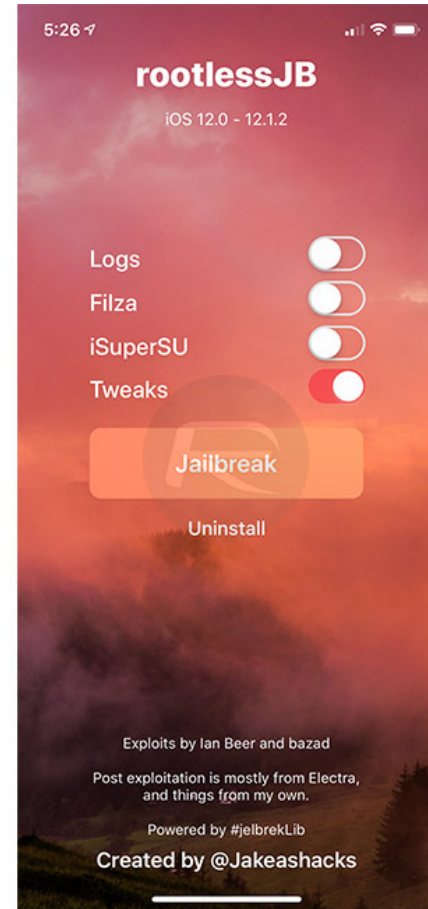


# Forensic Implications of iOS Jailbreak

## The types of jailbreaks

### Rootless jailbreak

- RootlessJB only available for iOS 12.0 through 12.1.2 (should be possible for older versions as well)
- More forensically sound
- Does not remount the file system (much more safe)
  - No access to the root of the file system “/”, hence the name “rootless”
- Does not modify system partition



# Forensic Implications of iOS Jailbreak

## The types of jailbreaks

### Rootless jailbreak (continued)

- Can be installed by compiling and pushing the IPA with Xceed
  - Forensically sound but complex
  - Must use developer Apple Account
- Can be also installed directly on the iPhone via Safari by visiting **ignition.fun**
  - Online installation is dangerous
  - Risk of remote wipe
  - ...until you set up a proxy to prevent access to FindMyPhone services

Exploits by Ian Beer and bazad

Post exploitation is mostly from Electra, and things from my own.

Powered by #jailbrekLib  
Put together by @Jakeashacks :)



Install iSuperSU

Tweaks

**Jailbreak!**

Uninstall

```
[~] installing bootstrap...
[+] Creating symlinks...
[+] Installed bootstrap!
[+] binaries already trusted?
[-] Failed to launch dropbear
[*] Starting fun
[i] Kernel base: 0xfffffff01f404000
[i] uid: 0
```

```
[+] Escaped sandbox!
    Wrote file 0x108d319c8
[+] binaries already trusted?
[-] Failed to launch dropbear
```

# Forensic Implications of iOS Jailbreak

## Files modified by the Rootless jailbreak

**At least the following paths are added or altered with the rootless jailbreak:**

- */var/containers/Bundle/Application/rootlessJB* – the jailbreak itself
- */var/containers/Bundle/iosbinpack64* – additional binaries and utilities
- */var/containers/Bundle/iosbinpack64/LaunchDaemons* – launch daemons
- */var/containers/Bundle/tweaksupport* – filesystem simulation where tweaks and stuff get installed
- Symlinks include: */var/LIB*, */var/ulb*, */var/bin*, */var/sbin*, */var/Apps*, */var/libexec*

# Forensic Implications of iOS Jailbreak

## Classic jailbreak

- Remounts the file system
- Access to “/” and below
- Modifies the system partition
- Breaks OTA updates
- Complete removal is difficult. System may remain unstable.
- Allows Cydia/Sileo and third-party package managers. Disables signature check.

## Rootless jailbreak

- Does not remount the file system
- Access to “/var” and below
- Does not modify the system partition
- Does not affect OTA updates
- Traces may be left after removal. No known system instabilities.
- No third-party package managers supported. Signature check bypassed for bundled apps only.

# Forensic Implications of iOS Jailbreak

## Classic jailbreak

- May or may not bundle an SSH daemon
- Supports file system acquisition including the system partition
- Full access to the keychain (acquisition and decryption)
- Allows to run unsigned applications easily

## Rootless jailbreak

- Bundles SSH daemon
- System system remains R/O but also being acquired
- Full access to the keychain (acquisition and decryption)
- Not that easy to run unsigned apps lbut still possible by patching *trusted cache* (in memory)

# Forensic Implications of iOS Jailbreak

## Classic jailbreak

- A variety of classic jailbreaks is available for many versions of iOS
- Supported for iOS 10.x (all versions), iOS 11.x (all versions), iOS 12.0-12.1.2
- Unc0ver and Undecimus (Cydia)  
<https://github.com/pwn20wndstuff/Undecimus/releases>
- Chimera (Electra Team) (Sileo)  
<https://chimera.sh/>

## Rootless jailbreak

- RootlessJB remains the only rootless jailbreak available
- Only supported for iOS 12.0-12.1.2
- RootlessJB  
<https://github.com/jakeajames/rootlessJB>  
or direct installation from [ignition.fun](https://ignition.fun)



# Forensic Implications of iOS Jailbreak

## Common for both types of jailbreaks

- Semi-tethered jailbreaks expire in 7 days
- If Apple Developer account is used, expire in 1 year

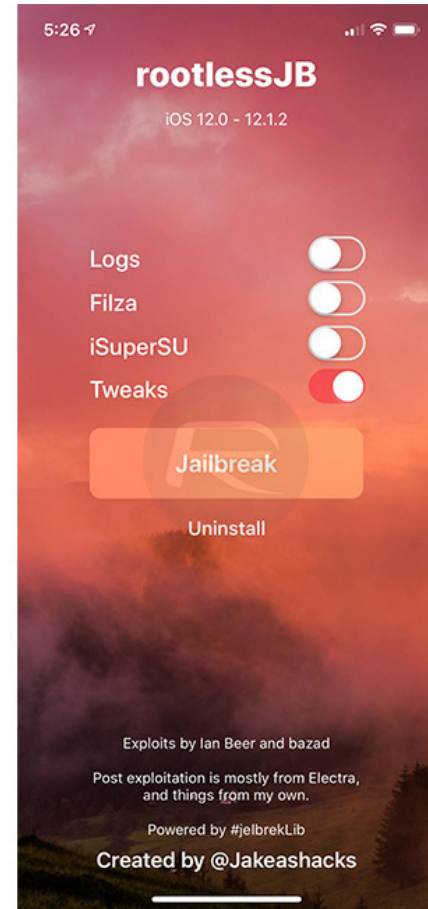
## Installing a jailbreak: developer vs. disposable account

- Each Apple Developer account can be used to sign IPA files to jailbreak a limited number of devices (200)
  - **Using a Developer account allows offline jailbreak installation (no need to verify signature on device)**
- Using a disposable Apple ID to jailbreak also works
  - **Internet connection required!!**
  - **Risk of syncing or remote wipe**

# Forensic Implications of iOS Jailbreak

## Rootless Jailbreak

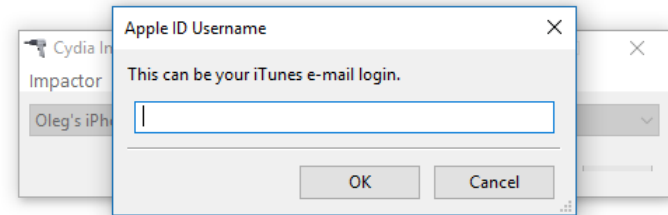
- Latest development in jailbreaks
- Supports iOS 12 to 12.1.2 (and some iOS 11 versions)
- Does not have as many forensic implications as classic jailbreaks
  - Does not remount the file system
  - Does not alter the system partition in any way
  - Does not allow other apps to alter system partition
  - Can be removed almost completely
- Does not allow access to the root of the file system
  - Hence the name is “rootless”
- Comes with SSH daemon
- Provides everything we need for **all we need for “physical” acquisition** (file system copy)



# Forensic Implications of iOS Jailbreak

## Installing classic jailbreaks

- Cydia Impactor  
<http://www.cydaimpactor.com/>
- Drag & drop jailbreak IPA to Cydia Impactor
- Sign jailbreak IPA with an Apple ID
- Enter Apple ID and password (developer's account is recommended; app-specific password for 2FA)
- Jailbreak IPA will be sideloaded to device



# Forensic Implications of iOS Jailbreak

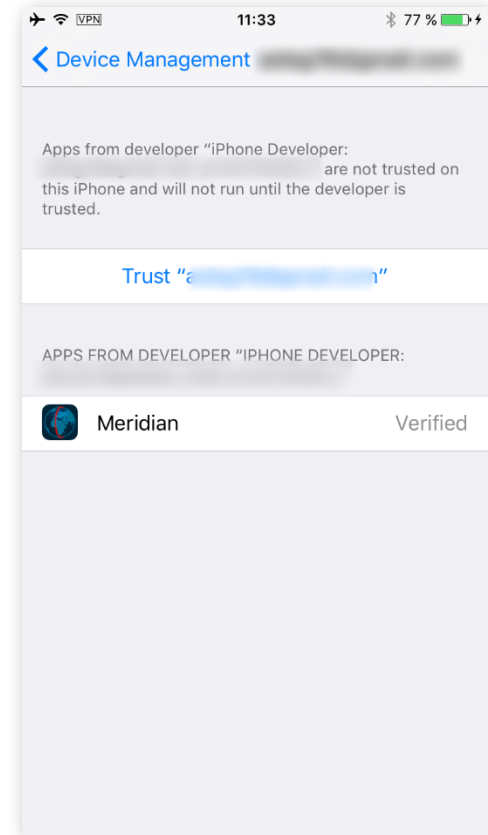
## Installing classic jailbreaks

For non-dev accounts:

- Trust developer certificate on iOS device
- **Settings > General > Device Management**
- Warning: Internet connection required!

For developer accounts:

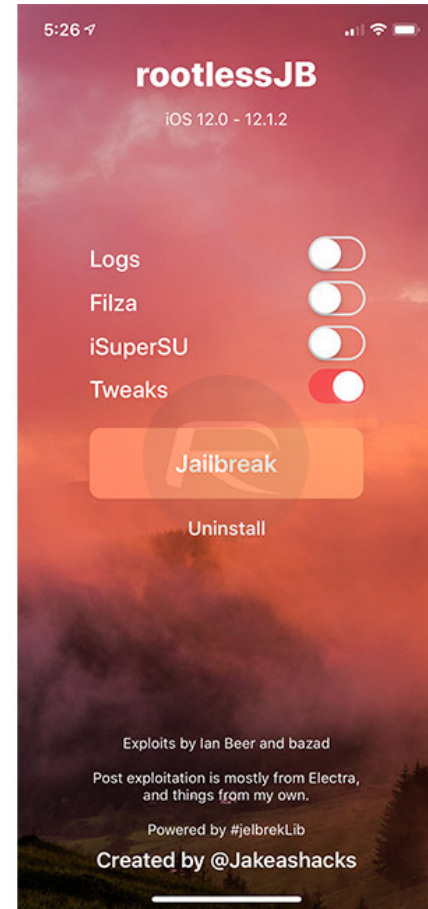
- This is it!



# Forensic Implications of iOS Jailbreak

## Installing RootlessJB

- Rootless jailbreak uses a different installation procedure
- **Can be easily installed online by opening a link in Safari browser**
- If offline installation is required, one must have a Developer Account with Apple
  - Compile rootlessJB IPA
  - Sign with developer account credentials
  - Then sideload with Cydia
  - No need to manually trust the certificate
  - No need for internet connection on iOS device



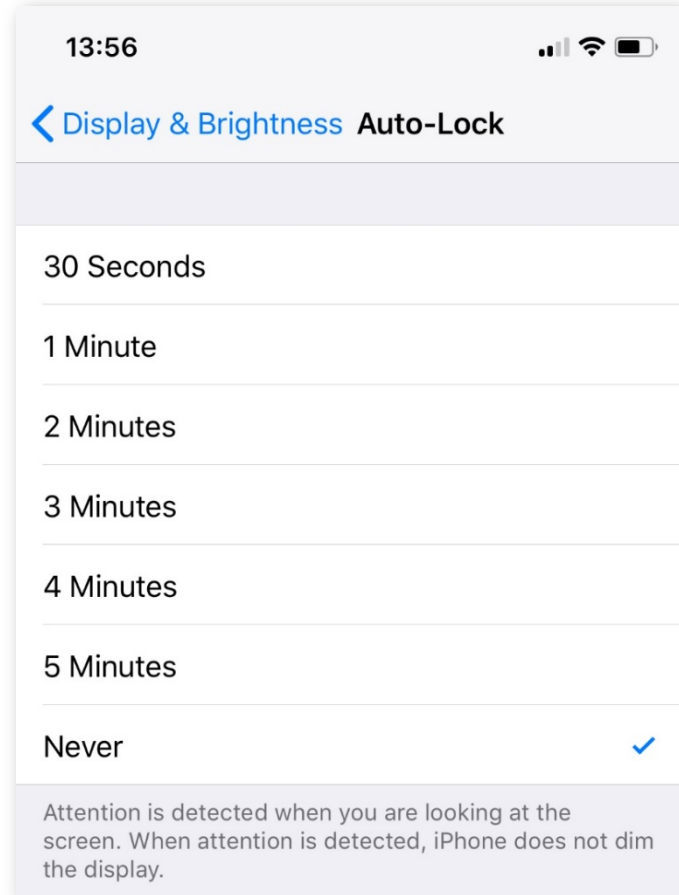
# Forensic Implications of iOS Jailbreak

## Physical Acquisition: 64-bit

- Imaging 64-bit devices is different
- Acquires file system image (TAR)
- No passcode recovery
- Must unlock the device, ensure it stays unlocked through the process
  - Settings > Display & Brightness > Auto-Lock > Never
  - Or use “DISABLE LOCK” in acquisition software

### F: “FILE SYSTEM”

- Extracts file system image
- Keychain extracted but not decrypted

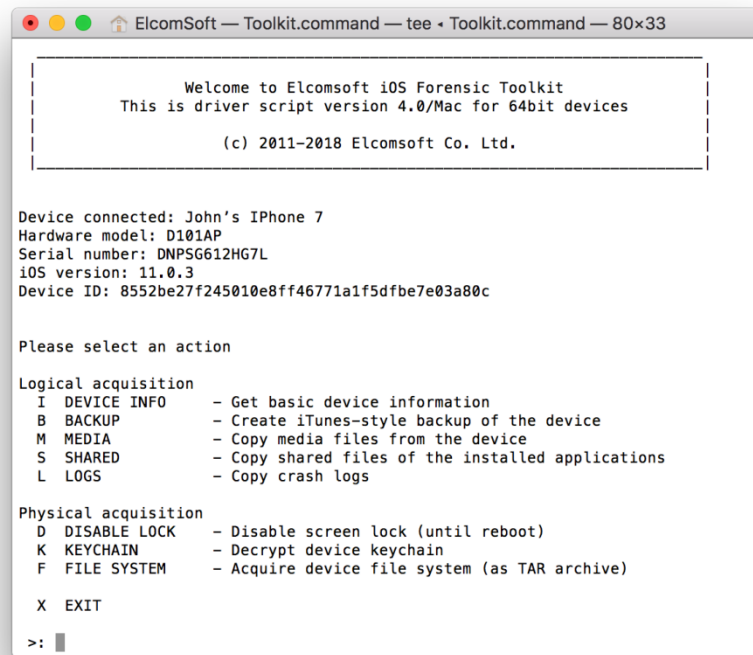


# Forensic Implications of iOS Jailbreak

## “Physical” Acquisition: 64-bit devices

### Physical acquisition steps

1. D - Disable screen lock
2. K - Decrypt keychain items
3. F - Extract files and folders



```
ElcomSoft — Toolkit.command — tee • Toolkit.command — 80x33

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 4.0/Mac for 64bit devices

(c) 2011-2018 Elcomsoft Co. Ltd.

Device connected: John's iPhone 7
Hardware model: D101AP
Serial number: DNPSG612HG7L
iOS version: 11.0.3
Device ID: 8552be27f245010e8ff46771a1f5dfbe7e03a80c

Please select an action

Logical acquisition
I DEVICE INFO      - Get basic device information
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 Implications of iOS Jailbreak

## Keychain acquisition: logical vs. physical

- User passwords (Safari): both
- App passwords: both
- Wi-Fi passwords: both
- Apple ID password and token: both (if present)
- Password to local (iTunes) backups: **physical**
- Some encryption keys (WhatsApp, Signal etc.): **physical**
- Items with *ThisDeviceOnly* attribute: **physical**



# Forensic Implications of iOS Jailbreak

## Inside the file system

- Location data (/private/var/root/Library/Caches/locationd)
- Downloaded mail (/private/var/mobile/Library/Mail)
- Health data (/private/var/mobile/Library/Health)
- Push notifications (/private/var/mobile/Library/ApplePushService)
- Spotlight data (/private/var/mobile/Library/Spotlight)
- Keyboard cache (/private/var/mobile/Library/Keyboard)
- Bluetooth devices  
(private/var/mobile/Library/com.apple.MobileBluetooth.ledevices.plist)
- Application data and caches
  - /private/var/mobile/Containers/Data/Application/
  - /private/var/mobile/Library/Caches)

# Forensic Implications of iOS Jailbreak

## Inside the file system (cont-d)

- Battery usage (/private/var/mobile/Library/BatteryLife)
- Network and data usage (/private/var/networkd, /private/var/wireless/Library/Databases)
- Various log files (/private/var/log, /private/var/logs, /private/var/wireless/Library/Logs, /private/var/mobile/Library/Logs)
- Applications activity (/private/var/mobile/Library/AggregateDictionary)
- More app activity: KnowledgebaseC and Screen Time data  
Application and system activities (/private/var/mobile/Library/CoreDuet/Knowledge)  
Screen Time (/private/var/mobile/Library/Application Support/com.apple.remotemanagementd)
- HomeKit (private/var/mobile/Library/homed)
- SHM and WAL files for all SQLite databases (delayed transactions)

# Forensic Implications of iOS Jailbreak

## Alternative extraction methods

If a jailbreak is not available for any reason, the following acquisition methods may be available:

- Logical: backups, media files, crash logs, shared files
  - Encrypted backups allow access to saved passwords
- Cloud: backups, media files, synced data, additional protected data (iCloud Keychain, Health, Messages)
  - No passwords in backups; accessing iCloud Keychain and other protected data requires device passcode (device from the trusted circle)

# Forensic Implications of iOS Jailbreak

## Cellebrite/GrayKey

- Cellebrite and GrayKey do not rely on public jailbreaks (?)
- Both companies use private/unknown exploits to escalate privilege level and gain access to the file system
- Forensic implications of these exploits are similar to the rootless jailbreak
- Traces still left (e.g. some system log entries)

# Forensic Implications of iOS Jailbreak

## Bonus: Apple TV Acquisition

- No passcode on the device, it is always unlocked
- Logical acquisition is limited: no backup service, so media files only (sometimes including information on deleted pictures and videos; location information is usually available from EXIF)
- A lot of information on user account is available
- Keychain is also there (though not synced to the iCloud; only Wi-Fi passwords are there, plus from some applications and services)
- iCloud authentication token can often be extracted, so allowing access to most account data (but not device backups)
- Jailbreaks exist for some tvOS 9-10, tvOS 11 (all), tvOS 12.0-12.1.1

**Thank you!**

# Forensic Implications of iOS Jailbreaking

The benefits, drawbacks and forensic implications of jailbreaking iOS devices

