ELCOMSOFT

Rome, November 2019

The iPhone's Forensic Workflow: The Steps to Access Critical Evidence

Extracting evidence from a seized iPhone: systematic approach, tools and challenges

iOS Forensics

In This Talk

Preserving evidence

- Seizing and storing the device
- Common mistakes and their consequences

Vectors of attack

- Cloud and Over-the-Air Acquisition
- Offline Backups
- Physical Acquisition
- Common mistakes and consequences

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
- Bypassing screen lock: encryption key derived from passcode

iOS Forensics

Seizing and Preserving Evidence

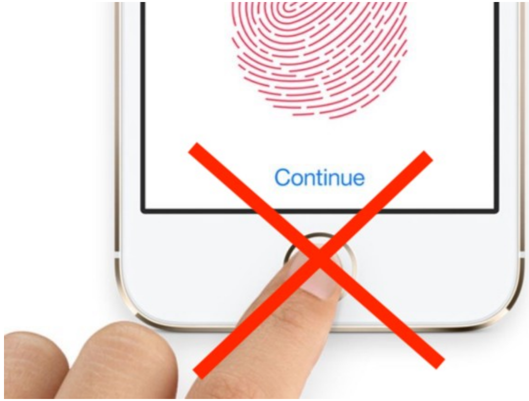
Seizing and storing the device properly is <u>extremely important</u>

iOS Forensics

Seizing and Preserving Evidence

Wrong:

- **Do nothing**
  Device susceptible to remote erase command; lost evidence; background activities
- **Switch off**
  Disables Touch ID/Face ID; requires PIN to unlock; disables the ability to use pairing records to unlock; disables Wi-Fi until unlocked
- **Push Touch ID button or look at Face ID camera**
  Wastes 1 of 5 available unlock attempts



iOS Forensics

Seizing and Preserving Evidence

Right:

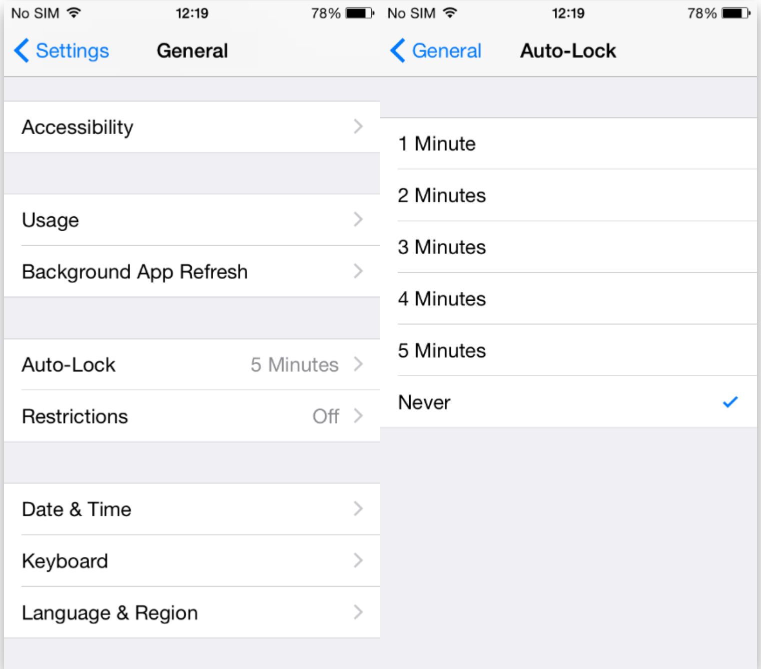
- To turn on display, use Sleep/Wake button
- Isolate (Faraday bag) or turn off radios (Airplane mode)
- If it’s on, don’t switch it off
- If unlocked, don’t let it lock. If possible, unlock the device on the spot and prevent locking
- USB Restricted Mode engages after 1 hour since last unlock

iOS Forensics

Seizing and Preserving Evidence

If unlocked, don’t let it lock

- Settings – General – Auto Lock – Never
  - May not be possible for devices with MDM/Exchange policies
- Much easier acquisition
- Will be able to produce offline backup



No SIM 12:19 78%

< Settings General

Accessibility >

Usage >

Background App Refresh >

Auto-Lock 5 Minutes >

Restrictions Off >

Date & Time >

Keyboard >

Language & Region >

No SIM 12:19 78%

< General Auto-Lock

1 Minute

2 Minutes

3 Minutes

4 Minutes

5 Minutes

Never ✓

iOS Forensics

Seizing and Preserving Evidence

Use Faraday bag; Connect to a charger

- Isolates from wireless networks
- Otherwise, remote wipe easily possible
- What can happen:
  - BBC News: Cambridgeshire, Derbyshire, Nottingham, and Durham police "There were six incidents, but **we don't know how people wiped them**.“ (9.Oct.14)
  - Darvel Walker, Morristown wiped his iPhone remotely, charged with tampering with evidence (7.Apr.15)

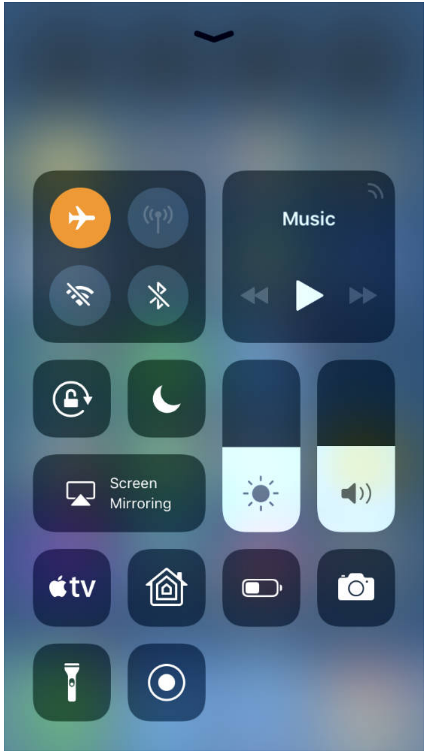
Hint: Microwave oven is effective as a shield against radio signals. But don’t turn it on ☺

iOS Forensics

Seizing and Preserving Evidence

If no Faraday bag is available:

- Switch to **Airplane mode**
  - This is possible even if the device is locked
- Otherwise, do risk assessment of two strategies:
  - Keep device on and connected > can use Touch ID, pairing records to unlock; possibility of remote wipe command (may be low if escorting subject)
  - Switch off the device > remote lock and remote erase impossible; must use passcode to unlock; Touch ID, pairing records and Wi-Fi disabled



iOS Forensics

Biometric Unlock: Touch ID and Face ID

64-bit Apple devices equipped with fingerprint reader

- iPhone 5S+, iPad mini3+, Air 2, Pro

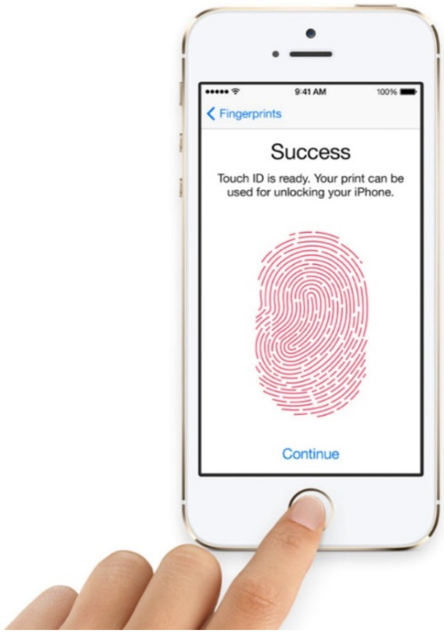
Convenient, utilized by most users

Unavailable after cold boot

- Device must be unlocked with passcode at least once to use Touch ID

Can use Touch ID to unlock the device

- Within 48 hours of last use
- But not after power-on or cold boot



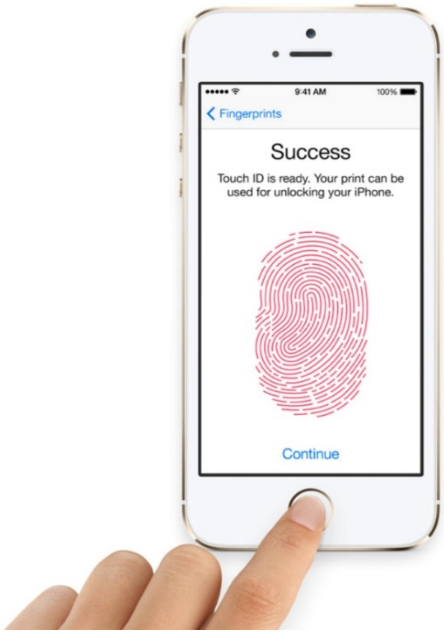
Success

Touch ID is ready. Your print can be used for unlocking your iPhone.

iOS Forensics

Touch ID (continued)

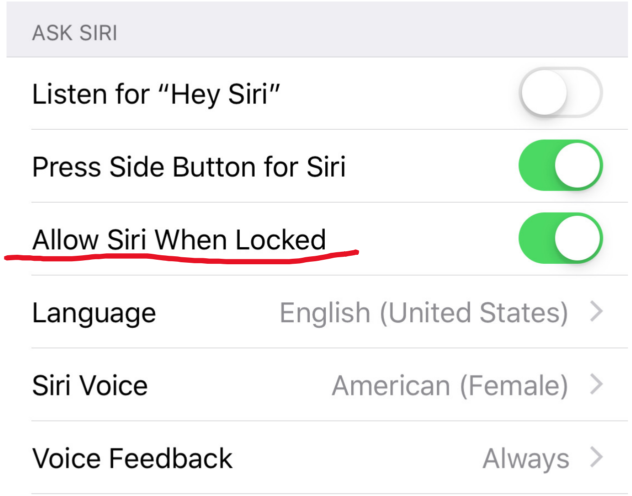
- Touch ID unlocks must be properly timed
  - Expires according to multiple rules
    - After 48 hours
    - If passcode not used for 6 days AND not unlocked with Tou Touch ID for 8 hours
  - You only have 5 attempts
  - When checking device lock status, **DO HOT PUSH THE HOM BUTTON** (or you lose one of the 5 attempts)
  - **iPhone X**: don’t look at the screen…
  - Use Sleep/Wake button instead


9:41 AM
100%
Fingerprints
Success
Touch ID is ready. Your print can be used for unlocking your iPhone.
Continue

iOS Forensics

Ask Siri

- “Allow Siri When Locked” is enabled by default
- Questions that don’t require device unlocking:
    - What’s my name?
    - Last call
    - Calendar
- These questions work on the lock screen but require device unlocking:
    - Call “name”
    - How long till home?



ASK SIRI

Listen for “Hey Siri” ○

Press Side Button for Siri ●

Allow Siri When Locked ●

Language English (United States) >

Siri Voice American (Female) >

Voice Feedback Always >

iOS Forensics

Vectors of Attack

Logical Acquisition (Backups)

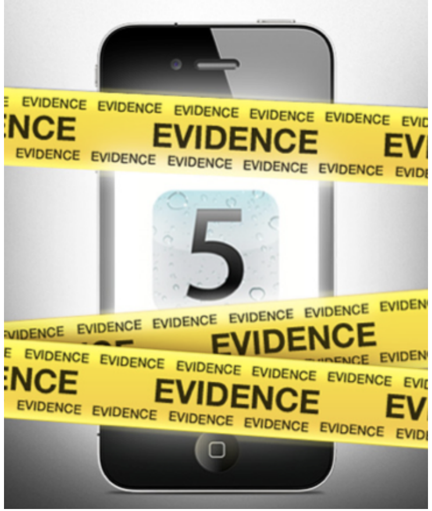
- Backup can be encrypted with unknown password
    - **iOS 11+** allows resetting backup password; passcode required
    - Slow (100 p/s w/GPU); recovery timeframe unpredictable, result not guaranteed
    - Can use lockdown/pairing records (extremely durable and do not seem to expire)

Over-the-Air (Cloud) Extraction

- Apple ID/password or binary authentication token
- Can be obtained from Apple with court order

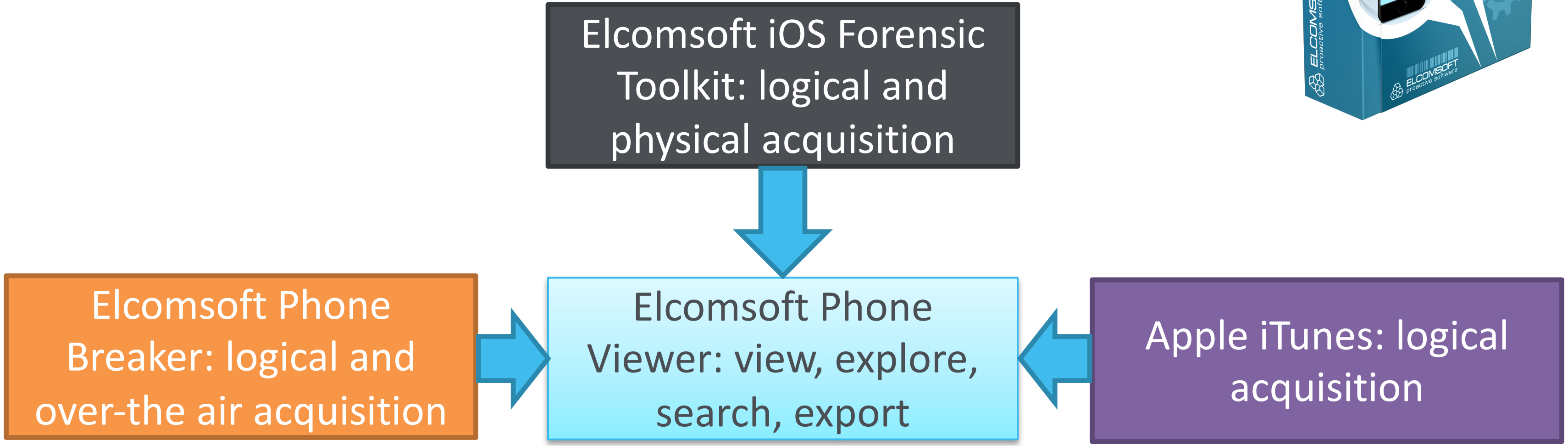
Physical Acquisition

- On recent devices, must unlock/know the passcode
- Jailbreak required, multiple issues arise



iOS Forensics

Software to use



Elcomsoft iOS Forensic Toolkit: logical and physical acquisition

Elcomsoft Phone Breaker: logical and over-the air acquisition

Elcomsoft Phone Viewer: view, explore, search, export

Apple iTunes: logical acquisition

iOS Forensics

Device Is Unlocked

If device is unlocked or can be unlocked, several acquisition options may be available, in this order:

1. Make local backup: set your own password if password empty
2. Attempt jailbreak, perform physical acquisition
3. If local backup protected with unknown password:
   - Force cloud backup (via Settings – iCloud – Backups) or
   - Disable backup password (iOS 11+ only) via Settings – General – Reset All Settings

iOS Forensics

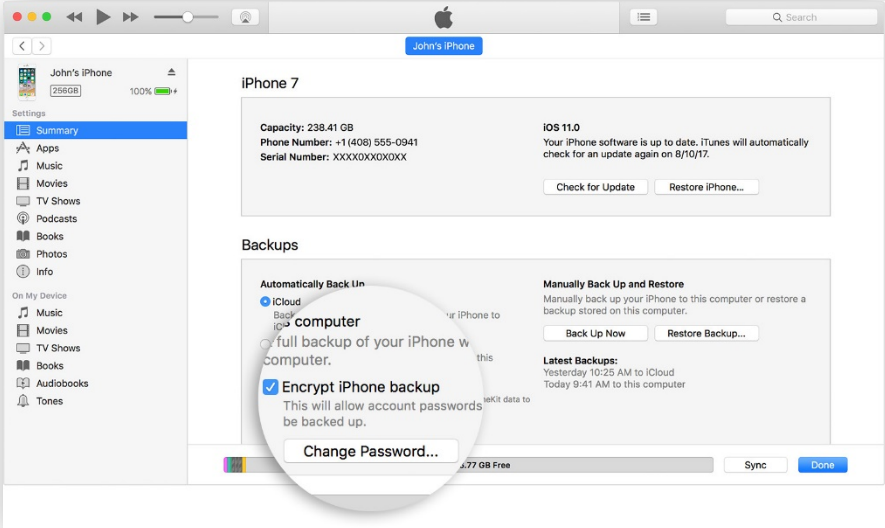
Make a Local Backup

Acquisition steps:

- Make the device produce a backup or
- Access information stored in existing backup

Limitations:

- Device must be unlocked (with passcode, Touch ID, iTunes or lockdown file)
- **iOS 11+ requires a passcode to pair**
    - Lockdown files can be used instead (if available)
- May produce encrypted backup
    - Must break password (no guaranteed timeframe, no guarantee of success)
- Limited amount of information



iPhone 7

Capacity: 238.41 GB
Phone Number: +1 (408) 555-0941
Serial Number: XXXX0XX0X0XX

iOS 11.0
Your iPhone software is up to date. iTunes will automatically check for an update again on 8/10/17.

Backups

Automatically Back Up
● iCloud
Back ... ur iPhone to iC... computer
○ full backup of your iPhone w... computer. ... this
☑ Encrypt iPhone backup
This will allow account passwords ...eKit data to be backed up.

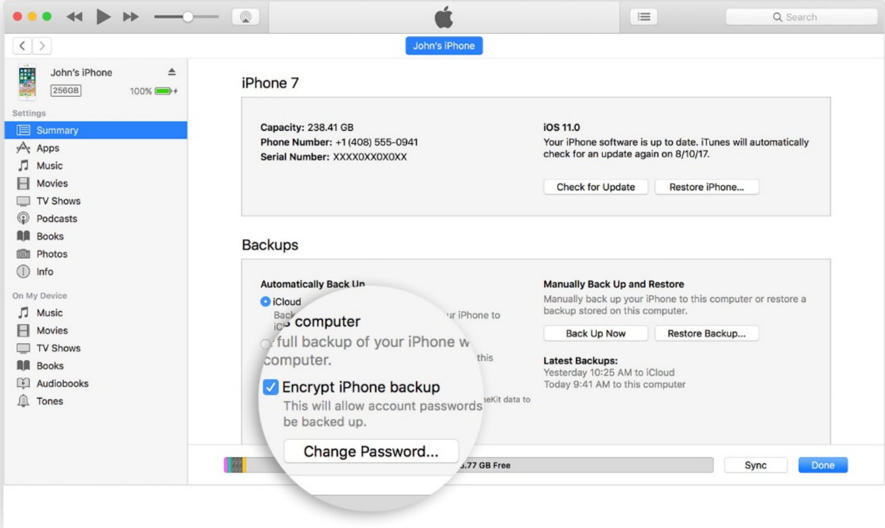
Manually Back Up and Restore
Manually back up your iPhone to this computer or restore a backup stored on this computer.

Latest Backups:
Yesterday 10:25 AM to iCloud
Today 9:41 AM to this computer

iOS Forensics

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



iPhone 7

Capacity: 238.41 GB
Phone Number: +1 (408) 555-0941
Serial Number: XXXX0XX0X0XX

iOS 11.0
Your iPhone software is up to date. iTunes will automatically check for an update again on 8/10/17.

Backups

Automatically Back Up

● iCloud
Back ... ur iPhone to iC... computer

○ ... full backup of your iPhone w... computer. ... this

☑ Encrypt iPhone backup
This will allow account passwords ...eKit data to be backed up.

Manually Back Up and Restore
Manually back up your iPhone to this computer or restore a backup stored on this computer.

Latest Backups:
Yesterday 10:25 AM to iCloud
Today 9:41 AM to this computer

.77 GB Free

iOS Forensics

Using Lockdown Files (Pairing Records)

Extract lockdown record from user’s computer

Windows Vista, 7, 8, 8.1, Windows 10: %ProgramData%\Apple\Lockdown

Windows XP: %AllUsersProfile%\Application Data\Apple\Lockdown

Mac OS X: /var/db/lockdown

Use to establish pairing relationship

* Since iOS 8, lockdown files expire after factory reset. Pairing records for iOS 7 and earlier persist through factory resets, available with Apple

iOS Forensics

What If…?

The Encrypt iPhone backup option is activated and you don’t know the password

- **iOS 8..10:** Password cannot be changed without specifying the old password
- **iOS 11+:** Password can be reset if you can unlock the device. Use Settings – General – Reset – Reset All Settings
- Make the phone produce a backup nevertheless. Attempt recovering backup password with Elcomsoft Phone Breaker

iOS Forensics

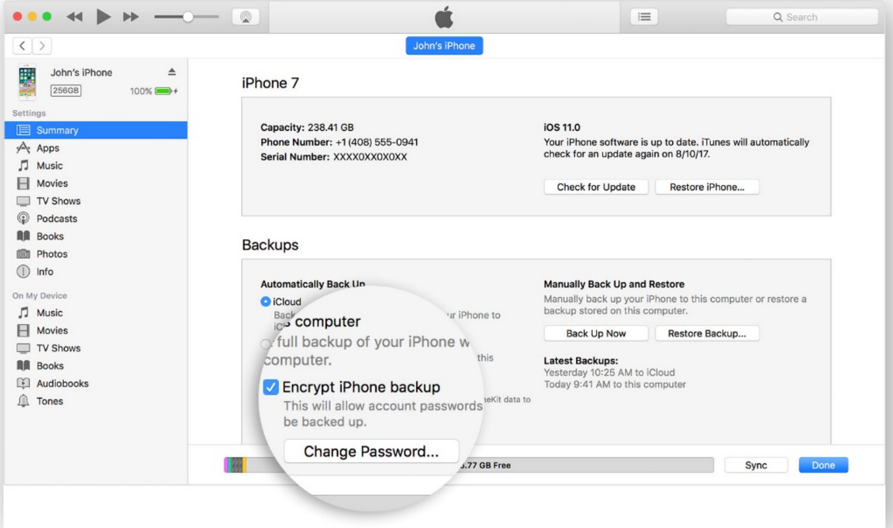
iTunes Backup Password

If backup password is specified (in iTunes):

No unencrypted data leaves the phone*

All encryption is performed inside the device (iPhone, iPad)

iTunes pulls encrypted data stream



iPhone 7

Capacity: 238.41 GB
Phone Number: +1 (408) 555-0941
Serial Number: XXXX0XX0X0XX

iOS 11.0
Your iPhone software is up to date. iTunes will automatically check for an update again on 8/10/17.

Backups

Automatically Back Up

● iCloud

○ computer
full backup of your iPhone w computer.

☑ Encrypt iPhone backup
This will allow account passwords be backed up.

Manually Back Up and Restore
Manually back up your iPhone to this computer or restore a backup stored on this computer.

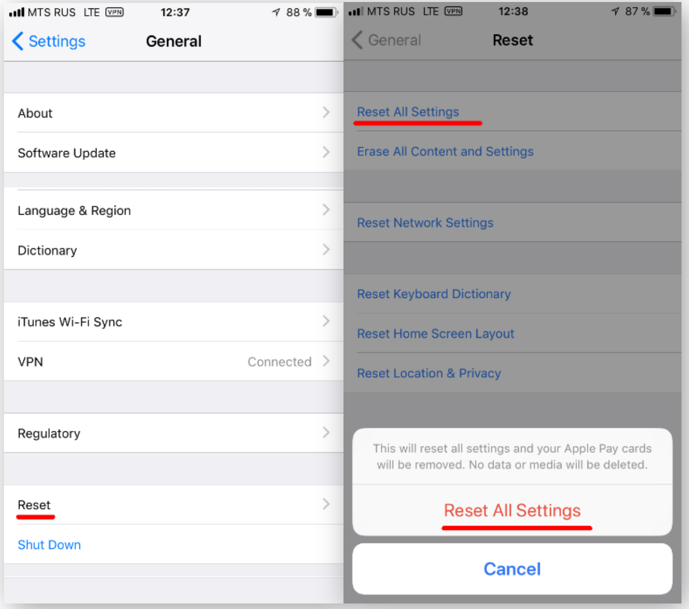
Latest Backups:
Yesterday 10:25 AM to iCloud
Today 9:41 AM to this computer

iOS Forensics

iOS 11: Resetting iTunes Backup Password

iOS 11 allows to reset 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**.



This will reset all settings and your Apple Pay cards will be removed. No data or media will be deleted.

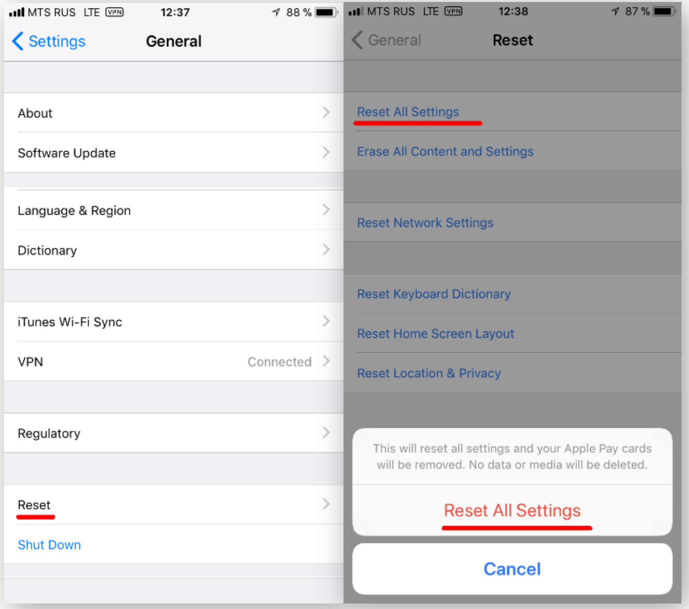
iOS Forensics

iOS 11: Resetting iTunes Backup Password

Using “Reset All Settings” will erase the following settings:

- Display brightness
- Whether or not to display battery percentage
- All Wi-Fi passwords (but **not** any other passwords or tokens stored in the Keychain)
- com.apple.wifi.plist
- **iTunes backup password**

All existing lockdown (pairing) records, data, and all keychain items (except Wi-Fi) are preserved



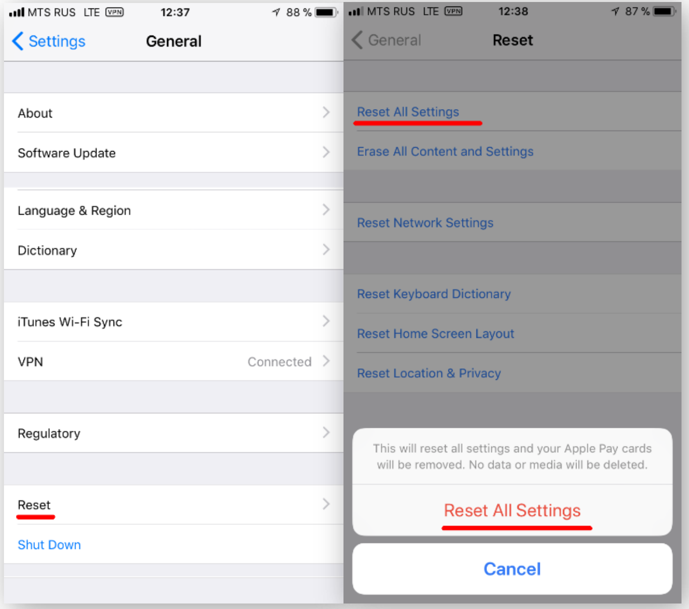
This will reset all settings and your Apple Pay cards will be removed. No data or media will be deleted.

iOS Forensics

iOS 11: Unknown iTunes Backup Password (1 of 2)

- Perform steps to create a local backup. You may still attempt attacking the original backup password.
- Disconnect the iPhone from the computer.
- Unlock the iPhone with Touch ID, Face ID or passcode.
- In Settings – General – Reset, tap and confirm Reset All Settings.
- Reconnect the iPhone to the computer.

Note: iOS Forensic Toolkit will set a temporary password of “123”; this will allow you to decrypt keychain items. You may use an existing lockdown file (pairing record) to create the backup.

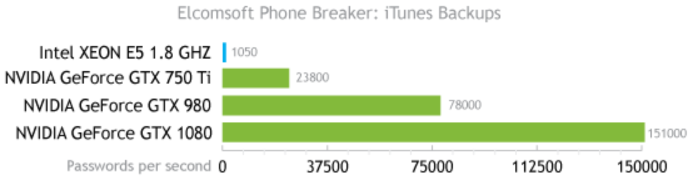


This will reset all settings and your Apple Pay cards will be removed. No data or media will be deleted.

iOS Forensics

Breaking iTunes Backup Password

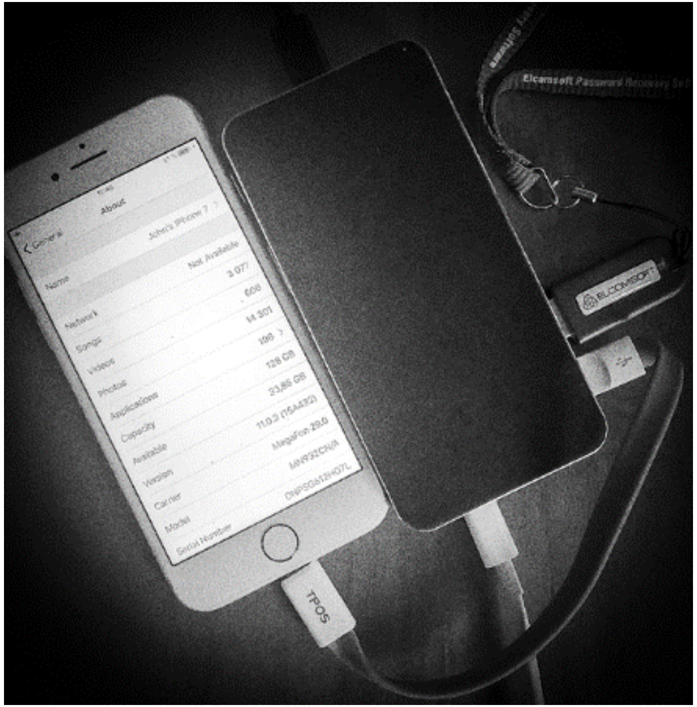
- Unknown backup password MUST be recovered
- Backups are securely encrypted
- iOS 9: 2400 combinations per second with CPU; 150,000 with GTX 1080
- iOS 10, iOS 11, iOS12: extremely slow at 100 p/s with GTX 1080 GPU



iOS Forensics

Step 2: Physical Acquisition

- On newer devices, jailbreak is required
- Passcode must be known or recovered
- **iPhone 5S and newer: must keep device unlocked during entire acquisition process**
  - Use (D)isable Lock in iOS Forensic Toolkit
- No jailbreak for some versions of iOS



iOS Forensics

Jailbreak: How To

- Unified installation procedure for all modern jailbreaks
- Device must be paired and unlocked
- Use Cydia Impactor to sideload jailbreak
  - Use Apple ID/password (disposable account) to sign the jailbreak IPA
  - This is very unstable, multiple tries may be required
- Trust developer certificate in device settings
- Launch the jailbreak
- Ensure SSH connectivity; if SSH daemon not pre-installed, install OpenSSH from Cydia

iOS Forensics

Jailbreak: Issues

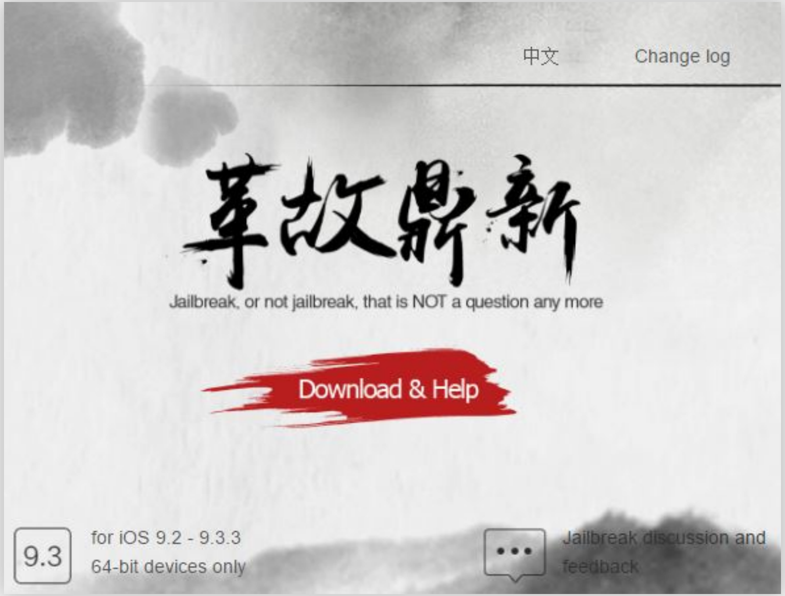
Jailbreak has many forensic implications

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)
- Each Apple Developer account can be used to sign IPA files to jailbreak a limited number of devices
- Disposable Apple ID to jailbreak is a good idea



Jailbreak, or not jailbreak, that is NOT a question any more

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

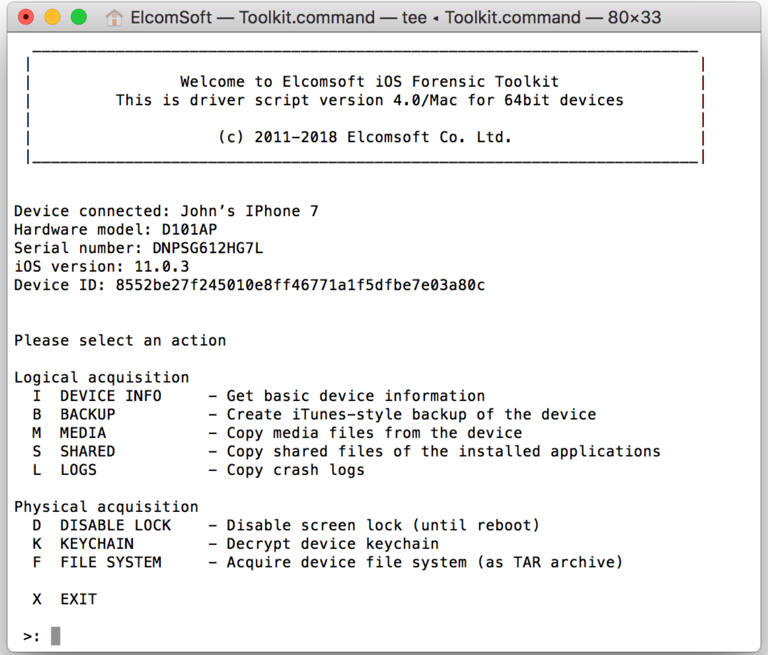
- “Rootless” does not mean “without root access”, it means “without access to root of file system”
- Can be applied offline with developer account
- File system is accessible from /var folder
- Modifies only files inside /var
- Leaves significantly less traces than classic JB
- System is more stable
- We recommend to use rootless jailbreaks for forensic analysis

Mobile Forensics

Physical Acquisition: 64-bit devices

Physical acquisition steps

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



```
  ________________________________________________________________________
 |                                                                        |
 |                 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

 >: 
```

iOS Forensics

Step 3: Producing Cloud Backup

Cloud backups are produced when:

- Device connected to a known Wi-Fi network (matching SSID and password)
- Connected to a charger
- Screen locked

WARNING: exposing device to wireless connectivity makes it subject to remote lock and remote erase

iOS Forensics

Forcing a Cloud Backup on Locked iPhone

Make the phone produce a fresh cloud backup

- Try other methods first if passcode known or unlock possible
- Bring to the proximity of a known Wi-Fi network
- SSID and password must match
- Connect to a charger
- Leave "overnight"
- If iCloud backups are enabled, the phone should produce a fresh cloud backup
- Request from Apple

iOS Forensics

Forcing Cloud Backup on Unlocked iPhone

If device is unlocked or can be unlocked:

- Fresh iCloud backup can be forced
- Settings – iCloud – Storage & Backup – Back Up Now

iOS Forensics

Risks and Issues

- Device susceptible to remote wipe command (that’s why try other methods first)
- Won’t connect to Wi-Fi if device was turned off and never unlocked afterwards (at least once)
- iCloud backups may not be enabled
- If the phone can be unlocked, try other methods first (iTunes backup, physical acquisition)

iOS Forensics

Apple ID Password

- If you know the password to user's Apple ID, perform cloud acquisition first
- If you don't, DO NOT RESET APPLE ID PASSWORD EVEN IF YOU CAN
- Otherwise, you won't be able to make the phone produce a fresh cloud backup without unlocking it first
  - What can happen:
- San-Bernardino case: password reset, iCloud backup impossible even with Apple cooperation

iOS Forensics

Not That Easy

“Auto Join” Wi-Fi network is enabled in device settings

Device unlocked at least once after booting *

- Device was discovered powered on, and
- It was kept powered on in a Faraday bag

Wi-Fi enabled on the device

* The device must be unlocked with passcode at least once after booting. Otherwise, Wi-Fi passwords remain encrypted, and the device will not attempt to connect to any Wi-Fi network.

iOS Forensics

Apple ID Password Already Known

Use Elcomsoft Phone Breaker to download cloud backup

What can go wrong:

- Two-factor authentication may be an issue
- Access to secondary authentication factor is required (unless using authentication token)
- Cloud backup may not exist
- It can be very old

iOS Forensics

PC with iCloud for Windows

- If iCloud for Windows is installed, binary authentication token may exist
  - Locate and extract the token
  - Download cloud backup using the authentication token

What can go wrong:

- In iOS 8.x, iCloud authentication tokens expire quickly
- In iOS 9.x, iCloud Drive is used, tokens do not expire

iOS Forensics

Over-the-Air Acquisition

You have:

- Apple ID and password, or
- PC synced with iCloud (binary authentication token)
- Acquisition steps:
- Use Apple ID and password to download the backup
- Extract binary authentication tokens, use to download backup

My Apple ID

What's an Apple ID?

An Apple ID is your user name for everything you do with Apple: Shop the iTunes Store, enable iCloud on all your devices, buy from the Apple Online Store, make a reservation at an Apple Retail Store, access the Apple Support website, and more.

Learn more about Apple ID ›

Change preferences, edit privacy settings, and keep your details current.

Reset your password ›

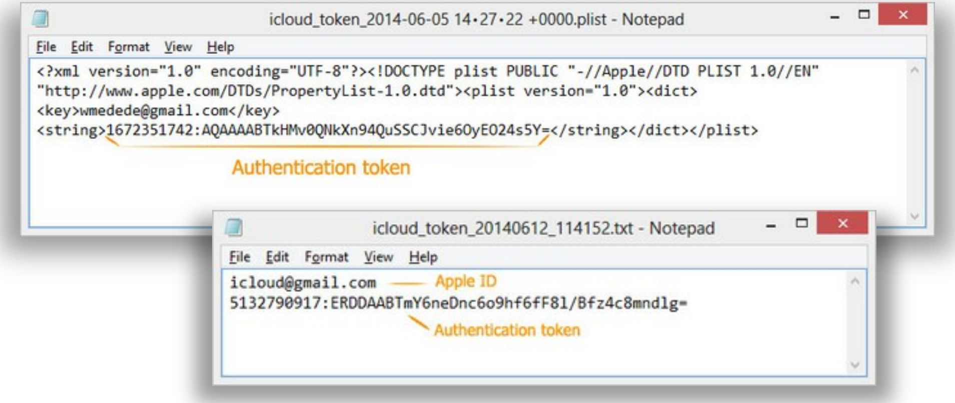
Signing up is quick, easy, and gives you access to all things Apple.

Find your Apple ID ›

iOS Forensics

iCloud Authentication Tokens

- Authentication tokens are used for convenience
- Saved on a Mac or PC used to access iCloud
- Allow users to avoid entering for Apple ID and password every time
- Technically, an authentication token is **stored in a file** on the user's computer (see figure)
- Locating the file and extracting the token allows bypassing login/password authentication and 2FA


icloud_token_2014-06-05 14•27•22 +0000.plist - Notepad
File Edit Format View Help

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd"><plist version="1.0"><dict>
<key>wmedede@gmail.com</key>
<string>1672351742:AQAAAABTkHMv0QNkXn94QuSSCJvie6OyEO24s5Y=</string></dict></plist>
```

Authentication token

icloud_token_20140612_114152.txt - Notepad
File Edit Format View Help

```
icloud@gmail.com
5132790917:ERDDAABTmY6neDnc6o9hf6fF81/Bfz4c8mndlg=
```

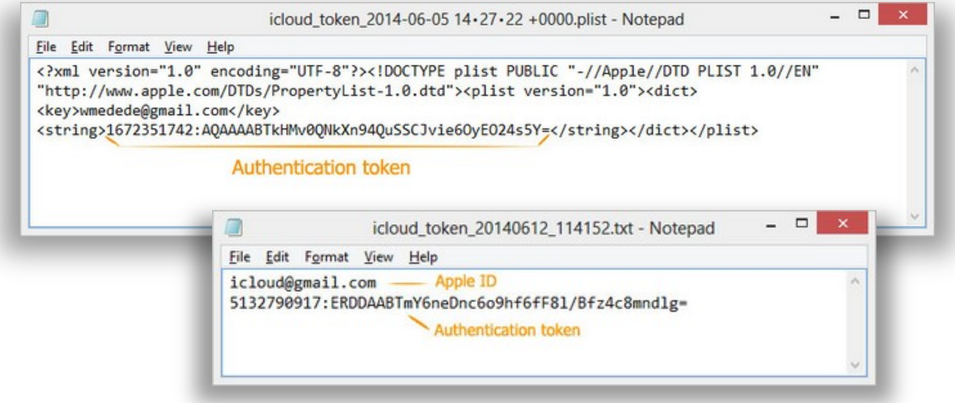
Apple ID

Authentication token

iOS Forensics

What Authentication Tokens Are Not

- Authentication tokens do not contain a password to the user’s Apple account
- They don’t contain a hash of the password either
- They cannot be used to brute-force the original plain-text password



icloud_token_2014-06-05 14•27•22 +0000.plist - Notepad
File Edit Format View Help

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd"><plist version="1.0"><dict>
<key>wmedede@gmail.com</key>
<string>1672351742:AQAAAABTkHMv0QNkXn94QuSSCJvie6OyEO24s5Y=</string></dict></plist>
```

Authentication token
icloud_token_20140612_114152.txt - Notepad
File Edit Format View Help

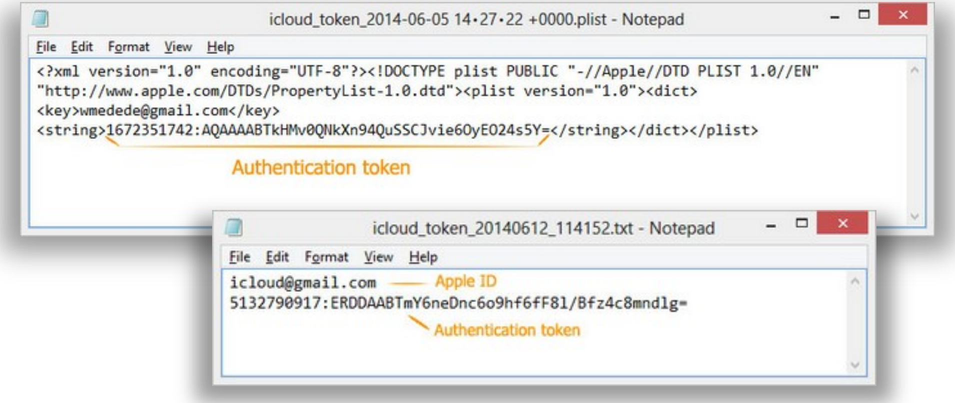
```
icloud@gmail.com
5132790917:ERDDAABTmY6neDnc6o9hf6fF81/Bfz4c8mndlg=
```

Apple ID
Authentication token

iOS Forensics

Obtaining a Binary Authentication Token

- Will need a PC synced with iCloud, its hard drive or forensic disk image
- Full instructions available online
- **PC**: www.elcomsoft.com/help/en/eppb/extracting_authentication_win.html
- **Mac**: www.elcomsoft.com/help/en/eppb/extracting_authentication_mac.html


icloud_token_2014-06-05 14•27•22 +0000.plist - Notepad
File Edit Format View Help

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd"><plist version="1.0"><dict>
<key>wmedede@gmail.com</key>
<string>1672351742:AQAAAABTkHMv0QNkXn94QuSSCJvie6OyEO24s5Y=</string></dict></plist>
```

Authentication token

icloud_token_20140612_114152.txt - Notepad
File Edit Format View Help

```
icloud@gmail.com
5132790917:ERDDAABTmY6neDnc6o9hf6fF81/Bfz4c8mndlg=
```

Apple ID

Authentication token

iOS Forensics

What If…?

The iCloud authentication token has expired

- Expired tokens cannot be used to download cloud backups

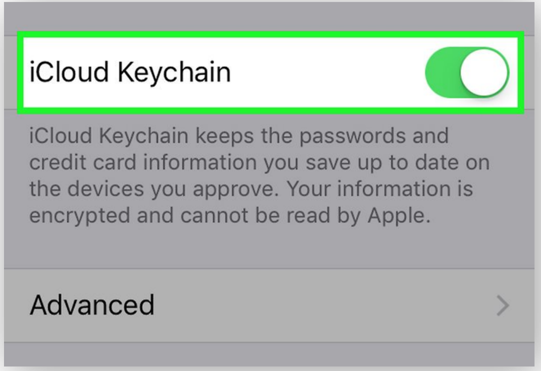
The Apple ID password has been changed

- All existing authentication tokens are immediately invalidated
- Must enter the correct password and overcome 2FA
- To force the creation of a new cloud backup, unlock the device and enter the new Apple ID password

iOS Forensics

iCloud Keychain

- Passwords, tokens and payment information synchronized through iCloud
- Apple does not provide any tools or APIs to access iCloud Keychain
- Several different implementations
  - Passwords may or may not be stored in iCloud

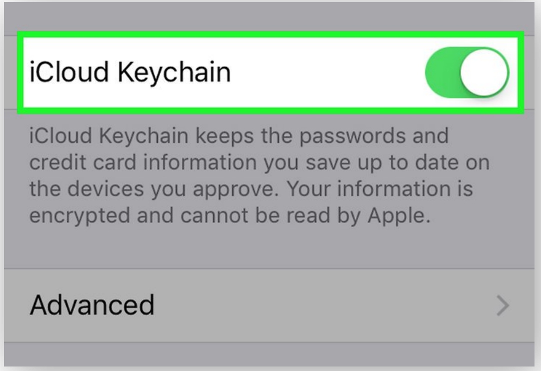


iCloud Keychain keeps the passwords and credit card information you save up to date on the devices you approve. Your information is encrypted and cannot be read by Apple.

iOS Forensics

iCloud Keychain

- **No 2FA and no iCloud Security Code**
  - The keychain is NOT stored in the cloud; direct synchronization across devices.
- **No 2FA, iCloud Security Code is present**
  - The keychain is AVAILABLE in the cloud.
- **2FA is enabled**
  - There can be no iCloud Security Code; the keychain is ALWAYS stored in the cloud.
  - Access to iCloud Keychain only possible after successfully passing 2FA and entering a passcode (or system password) of one of the already enrolled devices.



iCloud Keychain

iCloud Keychain keeps the passwords and credit card information you save up to date on the devices you approve. Your information is encrypted and cannot be read by Apple.

iOS Forensics

Extracting iCloud Keychain with Elcomsoft Phone Breaker

No Two-Factor Authentication

- Sign in with an Apple ID and password
- Supply iCloud Security Code, if one is configured
- Receive and enter a one-time code delivered to the user's registered phone number as a text message (SMS)
- **If iCloud Security Code is NOT configured, iCloud Keychain cannot be obtained**

iOS Forensics

Extracting iCloud Keychain with Elcomsoft Phone Breaker

Two-Factor Authentication enabled

- Sign in with Apple ID and password
- Confirm 2FA prompt on the device; use one-time code displayed to complete sign in
- Enter device passcode or system password of an iOS or macOS device already enrolled into iCloud Keychain
- iCloud Keychain will be downloaded. The process may take from several seconds to several minutes depending on the number of records in iCloud Keychain.

iOS Forensics

Exploring iCloud Keychain

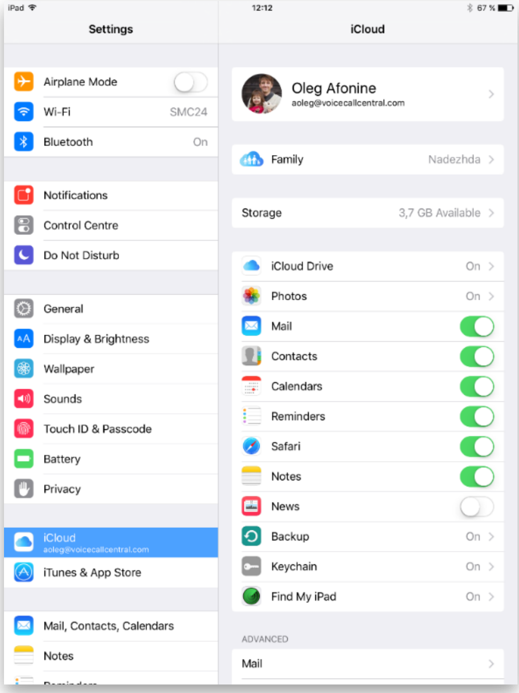
What’s inside?

- Passwords
- Tokens
- Payment data
- Wi-Fi networks

iOS Forensics

iCloud Data Sync

- If Settings | iCloud | Safari is enabled, it syncs:
  - Bookmarks
  - Open tabs
  - Reading list
  - Browsing history
  - **Call logs** (not in the Settings; syncs if iCloud Drive is enabled)
- Contacts, Notes, Calendars, Wallet (including boarding passes), Maps (searches and bookmarks)
- Keychain
  - With luck, password to Google Account
- Messages (iMessages, SMS): since iOS 11.4



Airplane Mode ○
Wi-Fi SMC24
Bluetooth On

iCloud
aoleg@voicecallcentral.com

iCloud

Oleg Afonine
aoleg@voicecallcentral.com

Family Nadezhda

Storage 3,7 GB Available

iCloud Drive	On
Photos	On
Mail	●
Contacts	●
Calendars	●
Reminders	●
Safari	●
Notes	●
News	○
Backup	On
Keychain	On
Find My iPad	On

ADVANCED

Mail

ELCOMSOFT

iOS Forensics: Acquisition Methods and Techniques

Extracting evidence from a seized iPhone: systematic approach, tools and challenges

ElcomSoft Co. Ltd.

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

Facebook: ElcomSoft
Twitter: @elcomsoft