L’analisi forense di iPhone: overview e stato dell’arte
Perchè iOS Forensics?
Marzo 2018 – Mobile OS (fonte Statcounter.com)
Perché iOS Forensics?
Marzo 2018 – Tablet OS (fonte Statcounter.com)
**iOS Versions – Market Share Marzo 2018 (fonte Apteligent)**

<table>
<thead>
<tr>
<th>Version</th>
<th>Codename</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0</td>
<td>iOS 6</td>
<td>0.01%</td>
</tr>
<tr>
<td>6.1</td>
<td>iOS 6</td>
<td>0.04%</td>
</tr>
<tr>
<td>7.0</td>
<td>iOS 7</td>
<td>0.05%</td>
</tr>
<tr>
<td>7.1</td>
<td>iOS 7</td>
<td>0.2%</td>
</tr>
<tr>
<td>8.0</td>
<td>iOS 8</td>
<td>0.03%</td>
</tr>
<tr>
<td>8.1</td>
<td>iOS 8</td>
<td>0.2%</td>
</tr>
<tr>
<td>8.2</td>
<td>iOS 8</td>
<td>0.04%</td>
</tr>
<tr>
<td>8.3</td>
<td>iOS 8</td>
<td>0.1%</td>
</tr>
<tr>
<td>9.4</td>
<td>iOS 8</td>
<td>0.2%</td>
</tr>
<tr>
<td>9.0</td>
<td>iOS 9</td>
<td>0.08%</td>
</tr>
<tr>
<td>9.1</td>
<td>iOS 9</td>
<td>0.10%</td>
</tr>
<tr>
<td>9.2</td>
<td>iOS 9</td>
<td>0.2%</td>
</tr>
<tr>
<td>9.3</td>
<td>iOS 9</td>
<td>4.5%</td>
</tr>
<tr>
<td>10.0</td>
<td>iOS 10</td>
<td>0.6%</td>
</tr>
<tr>
<td>10.1</td>
<td>iOS 10</td>
<td>0.7%</td>
</tr>
<tr>
<td>10.2</td>
<td>iOS 10</td>
<td>2.2%</td>
</tr>
<tr>
<td>10.3</td>
<td>iOS 10</td>
<td>9.5%</td>
</tr>
<tr>
<td>11.0</td>
<td>iOS 11</td>
<td>4.3%</td>
</tr>
<tr>
<td>11.1</td>
<td>iOS 11</td>
<td>4.7%</td>
</tr>
<tr>
<td>11.2</td>
<td>iOS 11</td>
<td><strong>72.3%</strong></td>
</tr>
</tbody>
</table>

Data Last Updated: 2018-03-08
Nine Elements of Mobile Forensic Process

- **Intake**
  - Receive device as evidence
  - Receive request for examination

- **Identification**
  - Identify device specifications & capabilities
  - Identify scope of examination
  - Identify legal authority for examination

- **Preparation**
  - Prepare methods and tools to be used
  - Prepare media and forensic workstation for exam
  - Prepare tools to most recent version

- **Isolation**
  - Protect the evidence
  - Prevent remote data destruction
  - Isolate from the cellular network, Bluetooth, and Wi-Fi

- **Processing**
  - Conduct forensic acquisition
  - Perform forensic analysis
  - Scan for malware

- **Verification**
  - Validate your acquisition
  - Validate your forensic findings

- **Documenting/Reporting**
  - Keep notes about your findings and process
  - Draft and finalize your forensic report

- **Presentation**
  - Prepare exhibits
  - Present your findings

- **Archiving**
  - Keep a gold copy of data in a safe place
  - Keep data in common formats for future

- **Presentation**
  - Display findings to stakeholders

- **Verification**
  - Validate findings before finalization

- **Archiving**
  - Maintain data in a secure location
  - Keep data updated for future analysis

- **Intake**
  - Receive device as evidence
  - Receive request for examination
Problemi per l’acquisizione di dispositivi iOS

- I dispositivi iOS utilizzano full disk encryption
- Ci sono altri livelli di cifratura (per-file key, backup password, …)
- Per comunicare con il dispositivo è necessario un «pairing»
- Non sono presenti porte JTAG
- Le tecniche di chip off non sono praticabili a causa della full disk encryption
Caccia alle vulnerabilità...

### ZERODIUM Payouts for Mobiles

<table>
<thead>
<tr>
<th>Payout</th>
<th>Device</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to $1,000,000</td>
<td>iOS</td>
<td>Remote Jailbreak with Persistence</td>
</tr>
<tr>
<td>Up to $120,000</td>
<td>Android</td>
<td>Remote Code Execution</td>
</tr>
<tr>
<td>Up to $150,000</td>
<td>Any OS</td>
<td>Local Privilege Escalation</td>
</tr>
<tr>
<td>Up to $50,000</td>
<td>iOS/Android</td>
<td>$SBX: Sandbox Escape or Bypass</td>
</tr>
</tbody>
</table>

- **RJB**: Remote Jailbreak with Persistence
- **RCE**: Remote Code Execution
- **LPE**: Local Privilege Escalation
- **$SBX**: Sandbox Escape or Bypass
• Dispositivo acceso (bloccato o sbloccato)
  • NON SPEGNERLO E RIFLETTERE!
• Dispositivo spento
1. Prevenire che il dispositivo vada in blocco! 
   Non premere alcun pulsante!
2. Disabilitare Auto-Lock!
3. Attivare la modalità aerea
4. Verificare se il passcode è attivo o no!
5. Collegarlo a una sorgente di corrente (es. batteria esterna)
6. Identificare il modello
7. Identificare la versione del sistema operativo
8. Se il sistema operativo è precedente ad iOS 11, collegare il device a un computer per generare un «pairing»
9. Se il sistema operativo è iOS 11
   1. Ricercare un certificato di lockdown su un PC e procedere all’acquisizione
   2. Acquisire fotograficamente quanto presente a schermo
PRESERVATION
PREVENIRE CHE IL DISPOSITIVO VADA IN BLOCCO! (Disable Auto-Lock)
**PRESERVATION - Attivazione Airplane Mode - Sbloccato**

<table>
<thead>
<tr>
<th>Settings</th>
<th>19:26</th>
<th>19:26</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airplane Mode</td>
<td>Off</td>
<td>On</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Cellular</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Hotspot</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Carrier</td>
<td>3 ITA</td>
<td></td>
</tr>
<tr>
<td>Notification Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control Center</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Before:**
- Airplane Mode: Off
- Wi-Fi: Off
- Bluetooth: Off
- Personal Hotspot: Off

**After:**
- Airplane Mode: On
- Wi-Fi: Off
- Bluetooth: Off
- Personal Hotspot: Off

**Other Options:**
- Notification Center
- Control Center
- Do Not Disturb
PRESERVATION
VERIFICARE SE E’ PRESENTE UN PASSCODE (Disable Auto-Lock)
IDENTIFICATION – Identificazione del modello - https://everymac.com/
## IDENTIFICATION - Identificazione dell versione di iOS

<table>
<thead>
<tr>
<th>Generali</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schermo e luminosità</td>
<td>Versione</td>
</tr>
<tr>
<td>Sfondo</td>
<td>11.2.6 (15D100)</td>
</tr>
<tr>
<td>Suoni</td>
<td></td>
</tr>
<tr>
<td>Siri e Cerca</td>
<td></td>
</tr>
<tr>
<td>Touch ID e codice</td>
<td></td>
</tr>
<tr>
<td>SOS emergenze</td>
<td></td>
</tr>
<tr>
<td>Batteria</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rete</td>
</tr>
<tr>
<td></td>
<td>3 ITA</td>
</tr>
<tr>
<td></td>
<td>Brani</td>
</tr>
<tr>
<td></td>
<td>105</td>
</tr>
<tr>
<td></td>
<td>Video</td>
</tr>
<tr>
<td></td>
<td>104</td>
</tr>
<tr>
<td></td>
<td>Foto</td>
</tr>
<tr>
<td></td>
<td>1.148</td>
</tr>
<tr>
<td></td>
<td>Applicazioni</td>
</tr>
<tr>
<td></td>
<td>62</td>
</tr>
<tr>
<td></td>
<td>Capienza</td>
</tr>
<tr>
<td></td>
<td>64 GB</td>
</tr>
<tr>
<td></td>
<td>Spazio disponibile</td>
</tr>
<tr>
<td></td>
<td>36.49 GB</td>
</tr>
</tbody>
</table>

**Versione**: 11.2.6 (15D100)
• Prima di iOS 11 era sufficiente collegare il dispositivo e autorizzare!
• Da iOS 11 Generare il trust ("pairing") con il PC richiede la conoscenza del passcode!
ACQUISITION – Certificati di pairing («lockdown»)

• Memorizzati in:
  • C:\Program Data\Apple\Lockdown Win 7/8/10
  • /private/var/db/lockdown Mac OS X

• Nome del certificato → Device_UDID.plist

• Sotto determinate condizioni, il certificato di pairing può essere utilizzato per “bypassare” il passcode
  • Lockdown certificate can be used within 48 hours since last user unlocked with the passcode
  • Lockdown certificate stored on a computer is valid for 30 days
USB

To improve security, for a locked iOS device to communicate with USB accessories you must either connect an accessory via lightning connector to the device while unlocked or enter your device passcode while connected, at least once a week.

If you use iAP USB accessories over the Lightning connector (including assistive devices and wired CarPlay) or connect to a Mac/PC, you may therefore need to periodically enter your passcode if you have a passcode set on your iPhone, iPad, or iPod Touch.
1. Attivare la modalità aerea
2. Collegarlo a una sorgente di corrente (es. batteria esterna)
3. Identificare il modello
4. Identificare la versione del sistema operativo
5. Valutere tutte le strade per acquisire il telefono prima di spegnerlo
   1. Certificato di lockdown su un PC?
   2. Fingerprint?
   3. Vulnerabilità della specifica versione?
PRESERVATION – Attivazione Airplane Mode - Bloccato
IDENTIFICATION - Identificazione del modello e versione iOS

• Libimobiledevice (Linux/Mac)
  http://www.libimobiledevice.org/
• iMobiledevice (Windows)
  http://quamotion.mobi/iMobileDevice/
• ideviceinfo -s
• Funziona anche senza pairing e quindi anche su dispositivi bloccati/spenti!
IDENTIFICATION - Identificazione del modello e versione iOS

C:\imobiledevice>ideviceinfo -s
BasebandCertId: 3840149528
BasebandKeyHashInformation:
  AKeyStatus: 2
  SKeyHash: u+/tcCwvaQ+1Y9t40I4yegCEmB28mALlaROhaIVGBWo=
  SKeyStatus: 0
BasebandSerialNumber: CKyShA==
BasebandVersion: 4.00.01
BoardId: 4
BuildVersion: 15A402
ChipID: 32771
DeviceClass: iPhone
DeviceColor: #272728
DeviceName: iPhone mattsia
DieID: 6299231647892006
HardwareModel: N71mAP
HasSiDP: true
PartitionType: GUID_partition_scheme
ProductName: iPhone OS
ProductType: iPhone8,1
ProductVersion: 11.0.1
ProductionSOC: true
ProtocolVersion: 2
TelephonyCapability: true
UniqueChipID: 6299231647892006
UniqueDeviceID: 3bf682ebc55c5673d586e0273af0dfb72d1994a2
WiFiAddress: 1c:5c:f2:7f:7a:20
To configure Touch ID, you must first set up a passcode. Touch ID is designed to minimize the input of your passcode; but your passcode will be needed for additional security validation:

- After restarting your device
- When more than 48 hours have elapsed from the last time you unlocked your device
- To enter the Touch ID & Passcode setting

Apple has added a new **emergency feature** designed to give users an intuitive way to call emergency by simply **pressing the Power button five times in rapid succession**.

This SOS mode not only allows quickly calling an emergency number, but also **disables Touch ID**.
• http://blog.dinosec.com/2014/09/bypassing-ios-lock-screens.html
• Latest available for iOS 11.1
• A person with physical access to an iOS device may be able to access photos from the lock screen (CVE-2017-13844)
1. Rimuovere la SIM Card
2. Identificare il **modello**
3. Se scarico, collegarlo a **una sorgente di corrente**
4. Accendere il dispositivo e **verificare se è presente un passcode**
5. Se il passcode non è presente
   1. Attivare la **modalità aerea**
   2. Identificare la **versione del sistema operativo**
   3. **Generare un certificato di pairing** e acquisire il telefono
6. Se è presente il passcode
   1. Identificare la **versione del sistema operativo**
   2. Valutare i possibili approcci...
ACQUISITION – Unlocking tools

- iOS 7 e iOS 8
  - UFED User Lock Code Recovery Tool
  - IP-BOX
  - MFC Dongle
  - Xpin Clip
ACQUISITION – Unlocking tools (iPhone 7)

IP Box 3 - iPhone 7 Passcode Unlock Tool

⭐⭐⭐⭐⭐ — 1 | Add review

ATTENTION - IP-Box 3 is now out of stock, and we cannot get any more stock. Look at 17 Box as an alternative solution to brute force iPhone 7 and 7 Plus.

Built on the success of the original IP-Box, the new IP Box 3 now supports passcode bruteforce cracking on the iPhone 7 and 7 Plus running iOS 10.

IP BOX 3 can also crack the passcodes on 3 different iPhone 7 or 7 Plus simultaneously.

This item is not available

€459.37 excluding VAT

- Add Software / Guides / Firmware Bundle on USB Stick For IP-BOX 3
**ACQUISITION – Unlocking tools (iPhone 7)**

**i7 Box**

**i7 Box - iPhone 7 Passcode Unlock Tool**

★★★★★ — 1 | [Add review](#)

Using the same method and technology as the [iP Box 3](#), the i7 Box supports passcode bruteforce cracking on the iPhone 7 and 7 Plus running upto iOS 10 (up to 10.3.2).

The difference is the i7 Box can only brute force one iPhone at any time and the iP-box 3 can brute force 3 handsets.

**In stock** (Only 10 left in stock)

**€411.60** excluding VAT

[Add Software / Guides / Firmware B undle on USB Stick For i7 Box (+€45.93)](#)
Cellebrite Advanced Services (CAS) experts provide law enforcement agencies with forensically sound, early access to sensitive mobile digital intelligence. Advanced Services provide:

- Unlocking and extraction for the latest Apple iOS devices including all iPhone models (iPhone 4S to iPhone X), iPad, iPad mini, iPad Pro and iPod touch, running iOS 5 to iOS 11.
- Unlocking and decrypted physical extraction of most Samsung devices including Galaxy S8/S7/S6, S5/S4/S3, Note 5/4/3.
- Decrypted Physical extractions available for most models.
- Decrypted contents of Samsung SecureFolder available.
- Limitations may apply based on iOS/Android version and Security patch level.
- Some models must be submitted to Cellebrite lab location for extended processing times.
- Technical services and supported device list are continuously updated. Check with your local sales representative for the latest supported models.

Advanced Services are only available to law enforcement with legal authority to unlock phones.

## ACQUISITION – Unlocking services – GreyKey?

### FEATURES

<table>
<thead>
<tr>
<th>Functionality</th>
<th>iOS Support</th>
<th>Device Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Successfully unlocks Apple iOS devices</td>
<td>Apple iOS 9.x <em>(coming soon)</em></td>
<td>iPhone 5</td>
</tr>
<tr>
<td>- Controlled by simple web UI</td>
<td>Apple iOS 10.x</td>
<td>iPhone 5c</td>
</tr>
<tr>
<td>- Plug and play platform; requires no special training</td>
<td>Apple iOS 11.x</td>
<td>iPhone 5s</td>
</tr>
<tr>
<td>- Supports before and after first unlock state</td>
<td></td>
<td>iPhone 6 &amp; 6 Plus</td>
</tr>
<tr>
<td>- Prioritizes common and date-based passcodes</td>
<td></td>
<td>iPhone SE</td>
</tr>
<tr>
<td>- Supports 4-digit, 6-digit, and complex passcodes</td>
<td></td>
<td>iPhone 6s &amp; 6s Plus</td>
</tr>
<tr>
<td>- Complete File System Extraction</td>
<td></td>
<td>iPhone 7 &amp; 7 Plus</td>
</tr>
<tr>
<td>- Extracts data not accessible in iTunes backups</td>
<td></td>
<td>iPhone 8 &amp; 8 Plus</td>
</tr>
<tr>
<td>- Supports disabled iOS devices</td>
<td></td>
<td>iPhone X</td>
</tr>
<tr>
<td>- Continually updated for new iOS versions</td>
<td></td>
<td>iPad Air &amp; Air 2</td>
</tr>
<tr>
<td>- Integrates with the leading Forensic Analysis Tools</td>
<td></td>
<td>iPad mini 2, 3, 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad (2017)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPad Pro (1st &amp; 2nd gen)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>iPod Touch (5th &amp; 6th gen)</td>
</tr>
</tbody>
</table>

[https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/#1e0485ad2950](https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/#1e0485ad2950)
ACQUISITION – Unlocking services – GreyKey?

GrayKey Annual License
GRAYSHIFT

The GrayKey license term is one year from the date of initial device activation. An active license is required to use the GrayKey. There are two available license modes for purchase.

Online: $15,000

The Online license requires a continuous Internet connection when in use. The GrayKey establishes an encrypted connection to Grayshift solely for the purposes of license enforcement, software updates, and error reporting.

The Online license requires the GrayKey to be operated from where it is initially activated, enforced with geolocation. The license is limited to 300 uses during the license term.

Offline: $30,000

The Offline license is available as an option for customers that require the GrayKey to have no active Internet access during or after being used on an evidentiary device. In Offline licenses the following applies:

- GrayKey only needs to connect to the Internet during the initial activation
- Software updates are delivered out of band for offline installation
- Geolocation enforcement is disabled
- There is no limit to the number of uses during the license term

To safeguard access to GrayKey's proprietary technology, token-based two factor authentication is required for Offline licenses.

https://www.forbes.com/sites/thomasbrewster/2018/03/05/apple-iphone-x-graykey-hack/#1e0485ad2950
ACQUISITION – Tecniche di acquisizione

File System

- **iTunes Backup**
  - Necessario pairing
  - Tutte le versioni di iOS

- **Apple File Conduit**
  - Necessario pairing
  - Il risultato dipende dalla versione di iOS

- **Crash Logs**
  - Necessario pairing
  - Tutte le versioni di iOS

- **Full file system**
  - Possibile su dispositivi jailbroken o tramite vulnerabilità

- **iCloud**
  - Necessarie credenziali o token di autenticazione

Physical

- **Disponibile fino a iPhone 4**
- Possibile su dispositivi jailbroken
- Sostanzialmente inutile da un punto di vista forense!
L’acquisizione fisica è sempre possibile.

I passcode semplici possono essere identificati in tempi ragionevoli e questo permette di decifrare tutti i dati presenti sul dispositivo.

Nel caso di passcode complessi che non è possibile violare, è comunque possibile avere accesso alle informazioni delle applicazioni native (rubrica, SMS, note, immagini, video, ecc.).
ACQUISITION – Backup vs. Physical Acquisition
ACQUISITION – Encrypted backup

iPhone 6s

Capacity: 55.53 GB  
Phone Number: +39 334 2340899  
Serial Number: F1ZQ811GRY9

iOS 9.3.5
Your iPhone software is up to date. iTunes will automatically check for an update again on 08/09/2016.

- Check for Update  
- Restore iPhone...

Backups

Automatically Back Up

- iCloud  
  Back up the most important data on your iPhone to iCloud.

- This computer  
  A full backup of your iPhone will be stored on this computer.

- Encrypt iPhone backup  
  This will allow account passwords, Health, and HomeKit 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.

- Back Up Now  
- Restore Backup...

Latest Backup:
Today 22:13 to this computer

Oxygen Forensic® Extractor v.6.2.0.788

Password recovery. Please wait.

Please note while Password Kit Forensic program is searching for the image password. If you know the password, please stop the process and enter the password for the current image.

Current algorithm: Password Kit Attacks List  
Estimated time: 00:00:11

Closed time: 00:00:29  
Reading Device: Apple iPhone 4S  
5SN: 01318808087237540

- Stop...  
- I know the password  
- Change algorithm

- Help  
- Cancel
» iOS 4 to 9 (and 10.1): about 150,000 passwords per second on GPU (NVIDIA GeForce 1080)

» iOS 10.0: about 6,000,000 passwords per second with Intel i5 CPU due to a bug we discovered

» iOS 10.2 and up (incl. iOS 11): about 5 passwords per minute (CPU); ~100 passwords per second on GPU
ACQUISITION – Encrypted backup – iOS 11

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)
» apple.wifi.plist
» iTunes backup password

ACQUISITION – Backup memorizzati su PC/MAC

<table>
<thead>
<tr>
<th>Nome</th>
<th>Ultima modifica</th>
<th>Tipo</th>
</tr>
</thead>
<tbody>
<tr>
<td>3bf682ebc55c5673d586e0273af0dfb72d1994a2</td>
<td>03/09/2016 16:55</td>
<td>Cartella di file</td>
</tr>
<tr>
<td>26ccdbcb74b2ab8e9e97aa096883a10442c6f2ef</td>
<td>03/09/2016 17:56</td>
<td>Cartella di file</td>
</tr>
<tr>
<td>929ffc5a169dd446ed36998f9b61153b85adba52</td>
<td>26/02/2016 16:46</td>
<td>Cartella di file</td>
</tr>
</tbody>
</table>
JAILBREAKING
https://www.theiphonewiki.com/wiki/Jailbreak

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 3.0/Win for A5+
(c) 2011-2018 Elcomsoft Co. Ltd.

Please select an action:
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
1 N/A
2 N/A
3 GET PASSCODE - Recover device passcode
4 GET KEYS - Extract device keys and keychain data
5 DECRYPT KEYCHAIN
6 IMAGE DISK - Acquire physical image of the device filesystem
7 DECRYPT DISK
8 TAR FILES - Acquire user’s files from the device as a tarball
9 REBOOT - Reboot the device
0 EXIT

>:}
ACQUISITION – Acquisizione dati da iCloud

• Necessario avere
  • Credenziali utente
    oppure
  • Token estratto da un computer (Windows/Mac)
    • Presente solo se iCloud Control Panel è installato!
• Si possono estrarre
  • Backup dei dispositivi
  • iCloud Drive
    • Dati applicazioni terze parti!
  • Dati sincronizzati
    • Contatti, Note, Calendari, Calls, Safari, Apple Maps, Wi-Fi, Wallet, iBooks
  • Photo Streams
  • Email
  • Keychain
  • FileVaul – Recovery Token
ACQUISITION – Acquisizione dati da iCloud
ACQUISITION – Acquisizione dati da iCloud

Password Recovery Wizard

Tools

Download backup from iCloud

Authentication type

Password  Token

Apple ID

Password

Sign in

Save credentials for future use
ACQUISITION – Acquisizione dati da iCloud

Password Recovery Wizard

Tools

Download backup from iCloud

Authentication type

Password

Token

Token

Save credentials for future use

Sign in
ACQUISITION – Acquisizione dati da iCloud

Password Recovery Wizard

Tools

Download backup from iCloud

Jailbreaking Test (461496998) – jailbreakingios@icloud.com

iPhone di Jailbreaking. Downloading backup...

67%

iPad di Jailbreaking

Downloaded

Skip

Backups to download – 1  Downloaded – 1  Errors – 0

Stop
ACQUISITION – Acquisizione dati da iCloud
ACQUISITION – Acquisizione dati da iCloud
Extract iCloud token from Windows PC

Fill in the fields below with the data collected from the user Windows PC.

   Usually it is located in C:\Users\Username\AppData\Roaming\Apple Computer\Preferences
2. "Protect" folder contains information required to decrypt com.apple.AOSKit.plist file.
   You can find this folder in C:\Users\Username\AppData\Roaming\Microsoft
3. SID is a user security descriptor.
   This field will be filled in automatically once you specify the "Protect" folder.
4. Enter the password of the Windows user whose com.apple.AOSKit.plist file you specified.

Path to AOSKit.plist file

Path to "Protect" folder

SID: S-X-X-X-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

User password

Save token Extract token

Extract cloud data
Si possono ottenere:

- Subscriber information
- Mail logs
- Email content
- Other iCloud Content
  - iOS Device Backups
  - iCloud Photo Library
  - iCloud Drive
  - Contacts
  - Calendar
  - Bookmarks
  - Safari Browsing History
- Find My iPhone
- Game Center
- iOS Device Activation
- Sign-on logs
- My Apple ID and iForgot logs
- FaceTime logs

### i. Subscriber Information

When a customer sets up an iCloud account, basic subscriber information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. iCloud subscriber information and connection logs with IP addresses can be obtained with a subpoena or greater legal process. Connection logs are retained up to 30 days.

### ii. Mail Logs

Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. Mail logs, if available, may be obtained with a court order under 18 U.S.C. § 2703(d) or a court order with an equivalent legal standard or a search warrant. iCloud mail logs are retained up to 60 days.

### iii. Email Content and Other iCloud Content

- My Photo Stream, iCloud Photo Library, iCloud Drive, Contacts, Calendars, Bookmarks, Safari Browsing History, iOS Device Backups

iCloud stores content for the services that the subscriber has elected to maintain in the account while the subscriber’s account remains active. Apple does not retain deleted content once it is cleared from Apple’s servers. iCloud content may include email, stored photos, documents, contacts, calendars, and bookmarks. iCloud browsing history and iOS device backups. iOS device backups may include photos and videos in the Camera Roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail. All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centres. iCloud content, as it exists in the subscriber’s account, may be provided in response to a search warrant issued upon a showing of probable cause.
• Ricerca pubblicata da Sergei Skorobogatov
• The bumpy road towards iPhone 5C NAND mirroring
  • http://www.cl.cam.ac.uk/~sps32/5c_proj.html
  • https://www.youtube.com/watch?v=tM66GWrwbsY
## iOS Forensics - Tools

### Forensic Tools
- Cellebrite Physical Analyzer
- Magnet IEF/AXIOM/Acquire
- Oxygen Forensic
- Elcomsoft Phone Breaker
- Elcomsoft Phone Viewer
- Elcomsoft iOS Forensic Toolkit
- XRY
- MPE+
- Paraben Device Seizure
- X-Ways/FTK/Encase

### Altri tools
- iTunes
- Libimobiledevice
- iMobiledevice
- iBackupbot
- iPhone Backup Extractor
- iFunBox
- iTools
- iExplorer
- Plisteditor
- SQLite Database Browser
<table>
<thead>
<tr>
<th>Course Syllabus</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR585.1: Malware Forensics, Smartphone Overview, and SQLite Introduction</td>
</tr>
<tr>
<td>FOR585.2: Android Forensics</td>
</tr>
<tr>
<td>FOR585.3: Android Backups and iOS Device Forensics</td>
</tr>
<tr>
<td>FOR585.4: iOS Backups, Windows, and BlackBerry 10 Forensics</td>
</tr>
<tr>
<td>FOR585.5: Third-Party Application and Knock-Off Forensics</td>
</tr>
<tr>
<td>FOR585.6: Smartphone Forensic Capstone Exercise</td>
</tr>
</tbody>
</table>
## SANS FOR 585 - Advanced Smartphone Forensics

<table>
<thead>
<tr>
<th>Type</th>
<th>Topic</th>
<th>Course / Location / Instructor</th>
<th>Date</th>
<th>Register</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training Event</td>
<td>Mobile Devices</td>
<td>FOR585: Advanced Smartphone Forensics (In English)</td>
<td>Jun 25, 2018 - Jun 30, 2018</td>
<td><a href="#">Register</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SANS Paris June 2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Paris, France</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cindy Murphy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training Event</td>
<td>Mobile Devices</td>
<td>FOR585: Advanced Smartphone Forensics</td>
<td>Nov 26, 2018 - Dec 1, 2018</td>
<td><a href="#">Register</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SANS Stockholm 2018</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stockholm, Sweden</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Heather Mahalik</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SANS MILAN JUNE 2018!

Welcome to SANS Milan June 2018

Save 250 EUR when you register and pay for any 4-6 day course by April 25!

Available Courses

<table>
<thead>
<tr>
<th>Title</th>
<th>Certification</th>
<th>Instructor</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR508: Advanced Digital Forensics, Incident Response, and Threat</td>
<td>GCFA</td>
<td>Francesco Picasso</td>
</tr>
<tr>
<td>Hunting (In Italian)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and</td>
<td>GNFA</td>
<td>Matt Bromiley</td>
</tr>
<tr>
<td>Incident Response</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Learning iOS Forensics – Second Edition

Mattia Epifani, Pasquale Stirparo

Learning iOS Forensics
Second Edition

A practical guide to analyzing iOS devices with the latest forensics tools and techniques

Packt
Mattia Epifani

- CEO @ REALITY NET – System Solutions
- Digital Forensics Analyst
- Mobile Device Security Specialist
- Member of Clusit, DFA, IISFA, ONIF, Tech&Law
- GCFA, GCFE, GASF, GREM, GNFA, GMOB, GCWN
- CEH, CHFI, CCE, CIFI, ECCE, AME, ACE, MPSC

mattia.epifani@realitynet.it
@mattiaep
http://www.linkedin.com/in/mattiaepifani
http://www.realitynet.it
http://blog.digital-forensics.it