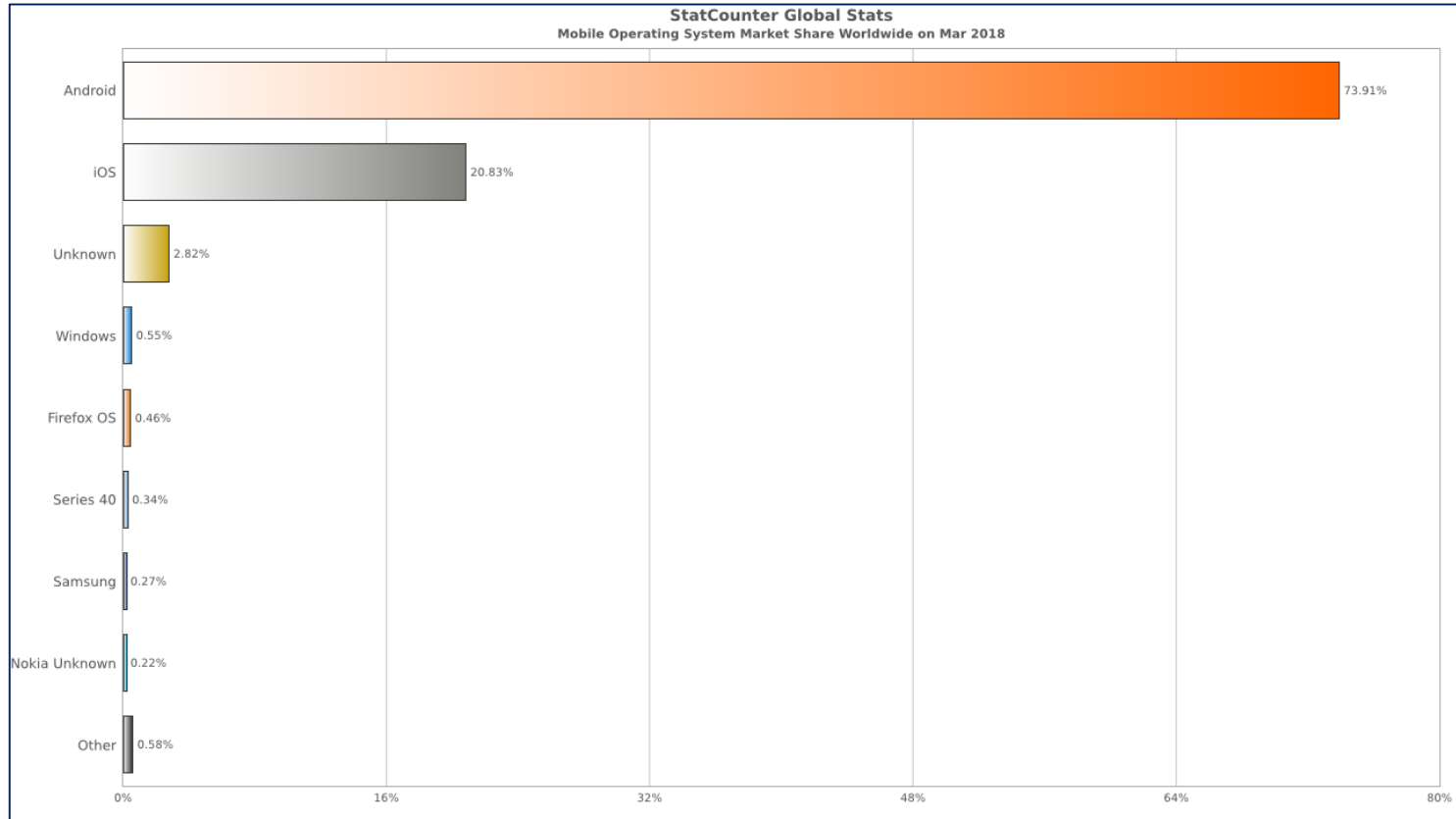




L'analisi forense di iPhone: overview e stato dell'arte

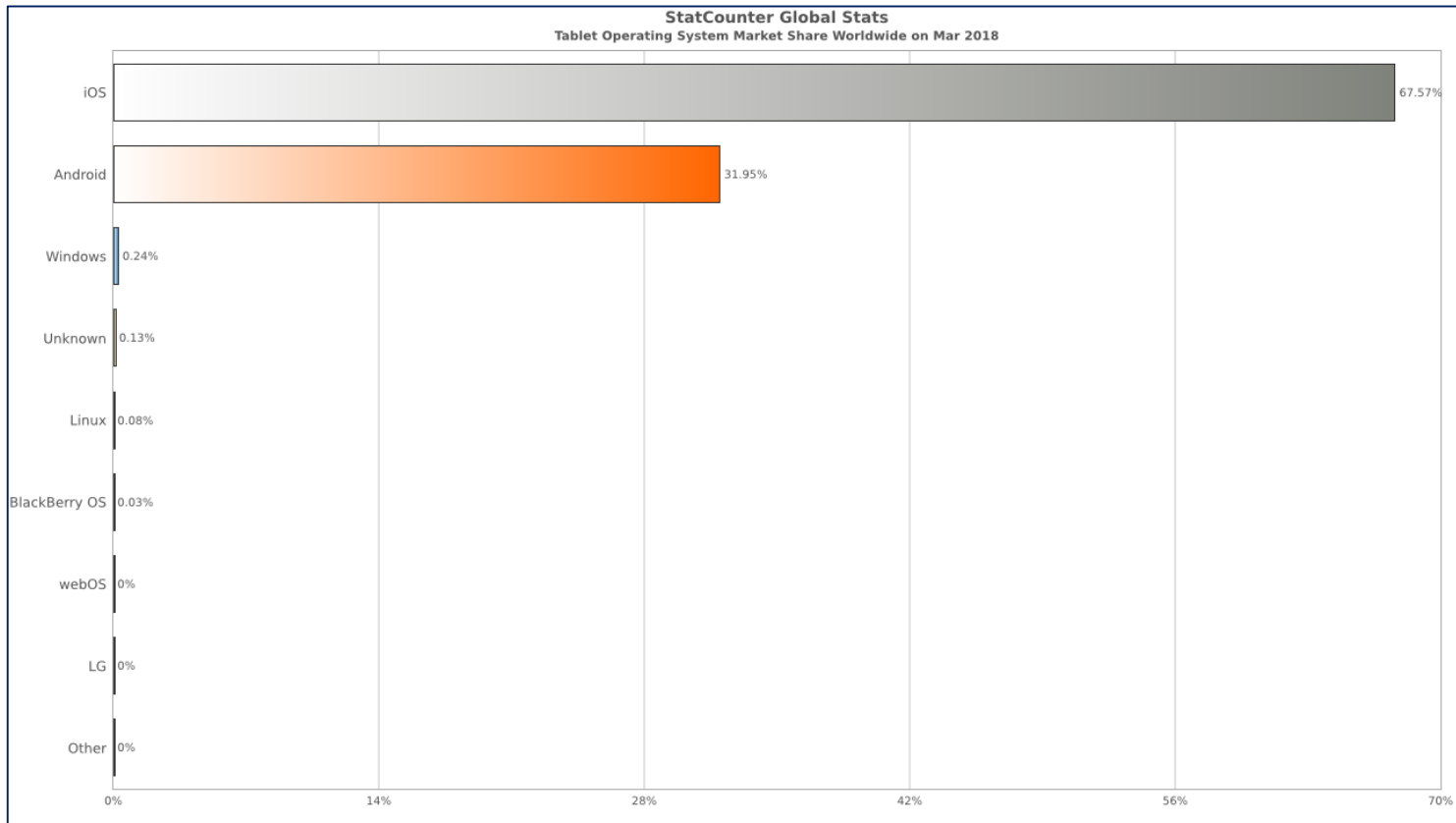
Perchè iOS Forensics?

Marzo 2018 – Mobile OS (fonte Statcounter.com)



Perchè iOS Forensics?

Marzo 2018 – Tablet OS (fonte Statcounter.com)

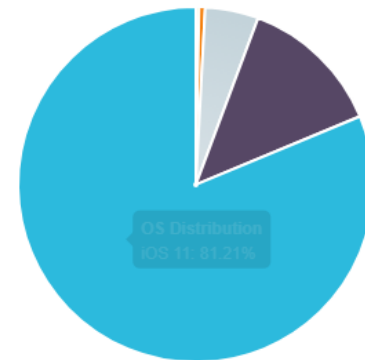


iOS Versions – Market Share Marzo 2018 (fonte Aptelligent)

Version	Codename	Distribution
6.0	iOS 6	0.01%
6.1	iOS 6	0.04%
7.0	iOS 7	0.05%
7.1	iOS 7	0.2%
8.0	iOS 8	0.03%
8.1	iOS 8	0.2%
8.2	iOS 8	0.04%
8.3	iOS 8	0.1%
8.4	iOS 8	0.2%
9.0	iOS 9	0.08%
9.1	iOS 9	0.10%
9.2	iOS 9	0.2%
9.3	iOS 9	4.5%
10.0	iOS 10	0.6%
10.1	iOS 10	0.7%
10.2	iOS 10	2.2%
10.3	iOS 10	9.5%
11.0	iOS 11	4.3%
11.1	iOS 11	4.7%
11.2	iOS 11	72.3%

Data Last Updated: 2018-03-08

■ iOS 6 (0.06%)
 ■ iOS 7 (0.23%)
 ■ iOS 8 (0.55%)
 ■ iOS 9 (4.85%)
 ■ iOS 10 (13.03%)
 ■ iOS 11 (81.21%)



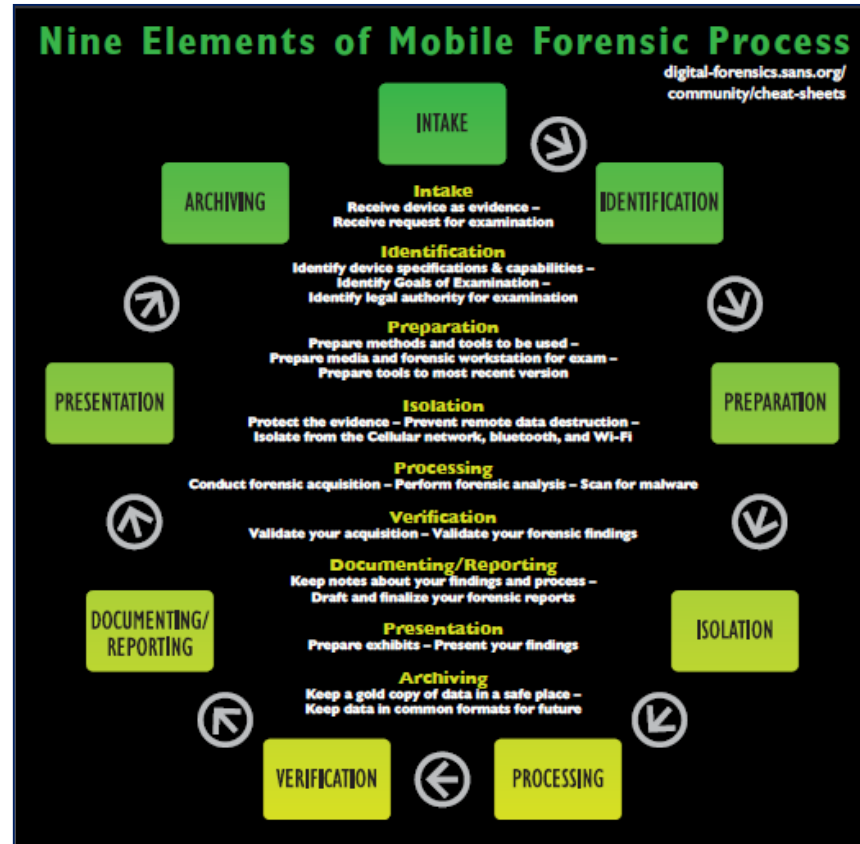
January 2018 (fonte iossupportmatrix.com)

 @isupportmatrix



Notes: All dates refer to the US product launch date. Code names are courtesy of iMore.com. Winter feedback supplied by: Dave Mundock and Sigurdur Heljason. the matrix will return in Spring 2018.

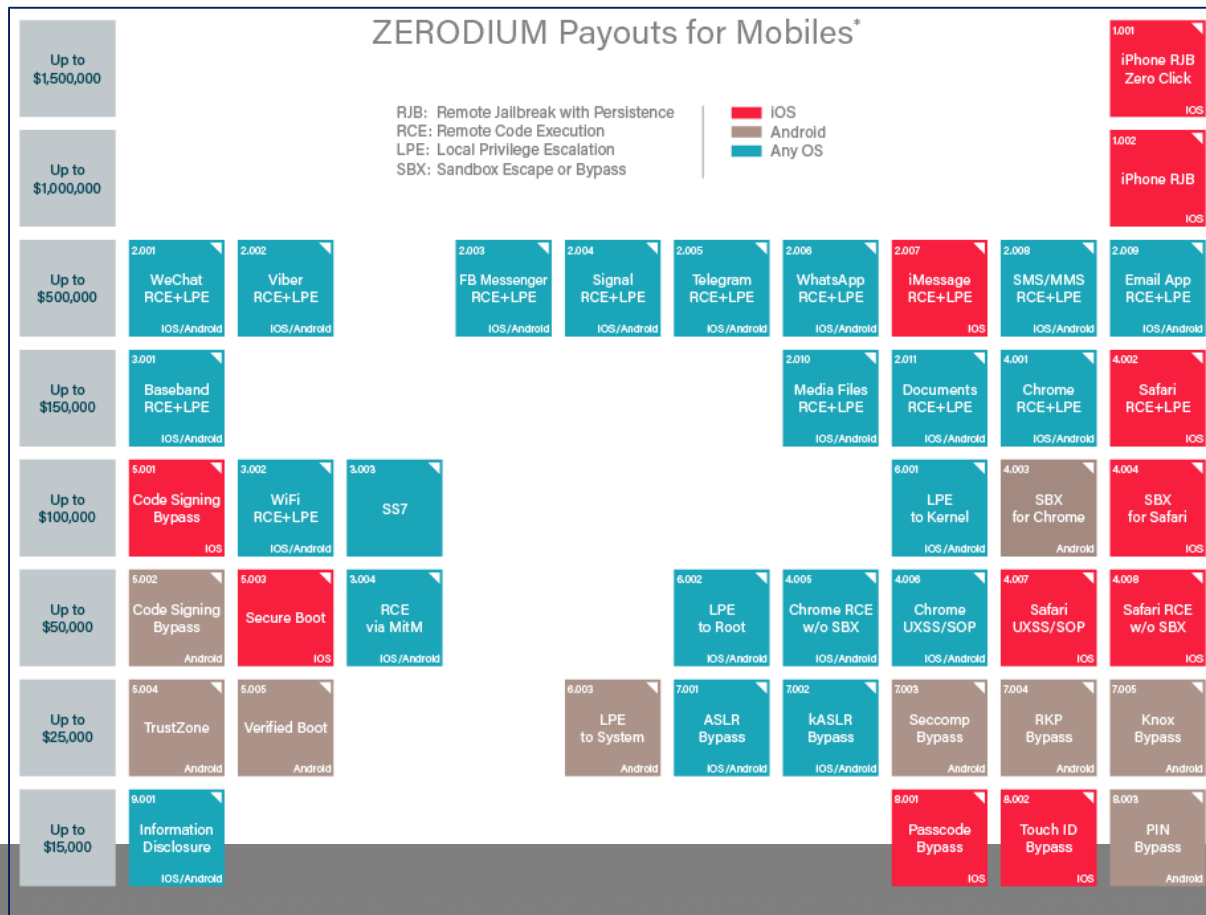
Mobile Forensics Process – SANS Mobile Forensic Poster



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...



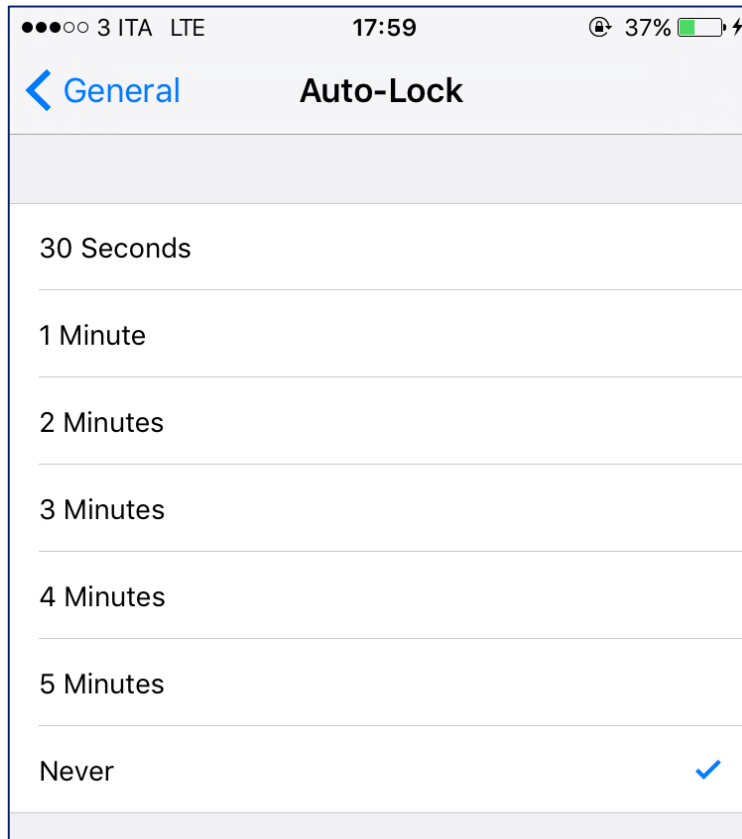
- **Dispositivo acceso
(bloccato o sbloccato)**
 - **NON SPEGNERLO E
RIFLETTERE!**
- **Dispositivo spento**

PRESERVATION – ACCESO E SBLOCCATO

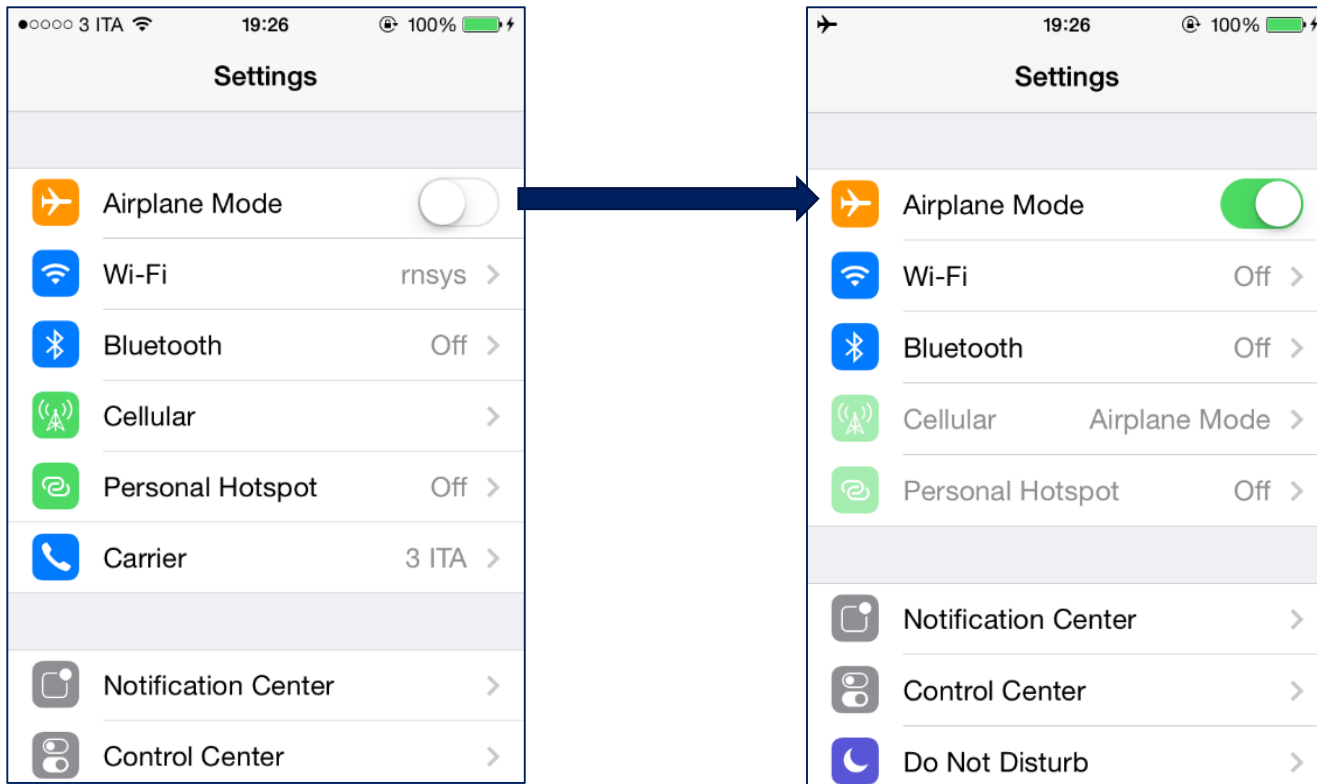
1. **Prevenire che il dispositivo vada in blocco!**
Non premere alcun pulsante!
2. **Disabilitare Auto-Lock!**
3. Attivare la **modalità aerea**
4. **Verificare se il passcode è attivo o no!**
5. Collegarlo a **una sorgente di corrente** (es. batteria esterna)
6. Identificare il **modello**
7. Identificare 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)

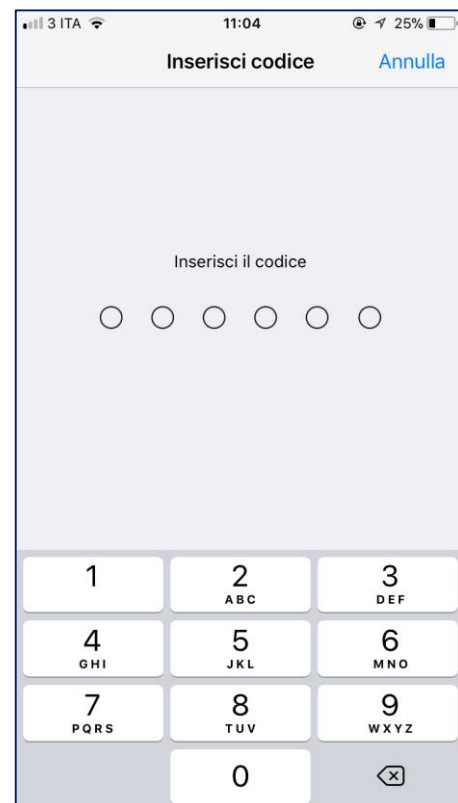
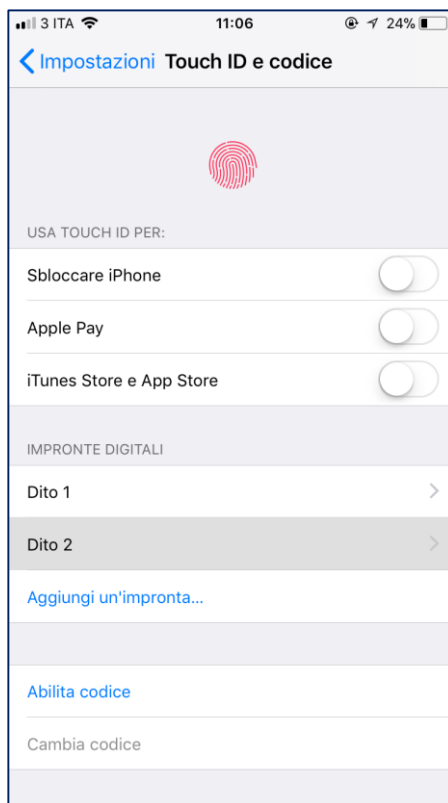
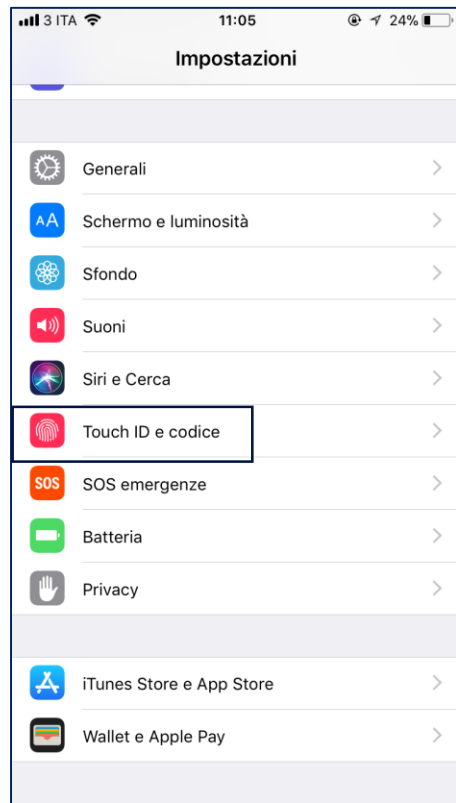


PRESERVATION - Attivazione Airplane Mode - Sbloccato



PRESERVATION

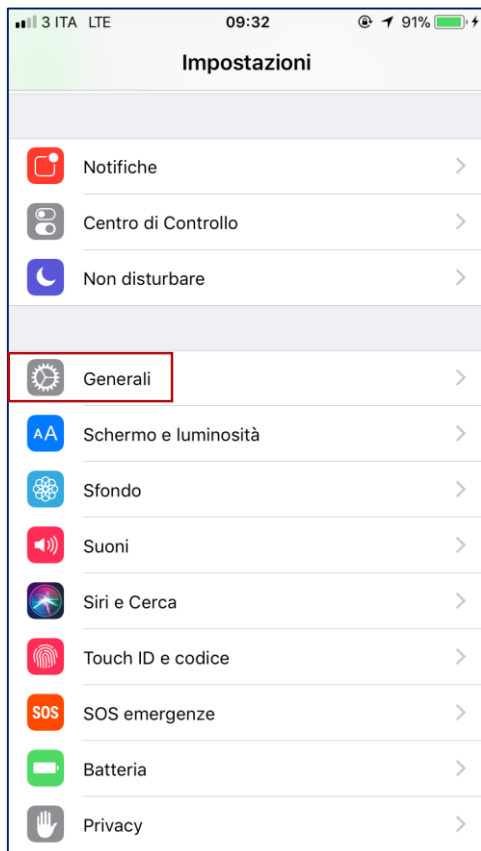
VERIFICARE SE E' PRESENTE UN PASSCODE (Disable Auto-Lock)



IDENTIFICATION – Identificazione del modello - <https://everymac.com/>



IDENTIFICATION - Identificazione dell versione di iOS



ACQUISITION – iOS 11 – Pairing

- **Prima di iOS 11 era sufficiente collegare il dispositivo e autorizzare!**

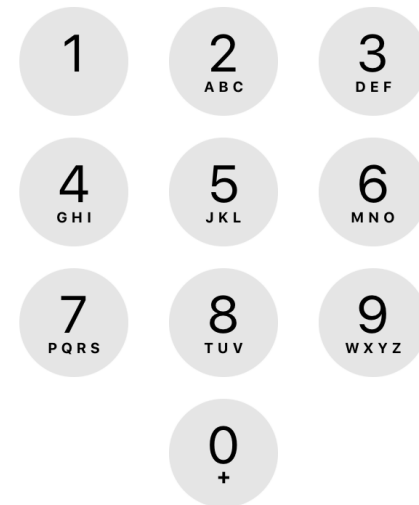


- **Da iOS 11 Generare il trust (“pairing”) con il PC richiede la conoscenza del passcode!**

Enter iPhone Passcode to Trust
This Computer

Your settings and data will be accessible from this
computer when connected.

○ ○ ○ ○ ○ ○



Cancel

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**

ACQUISITION – Certificati di pairing – iOS 11.3

USB

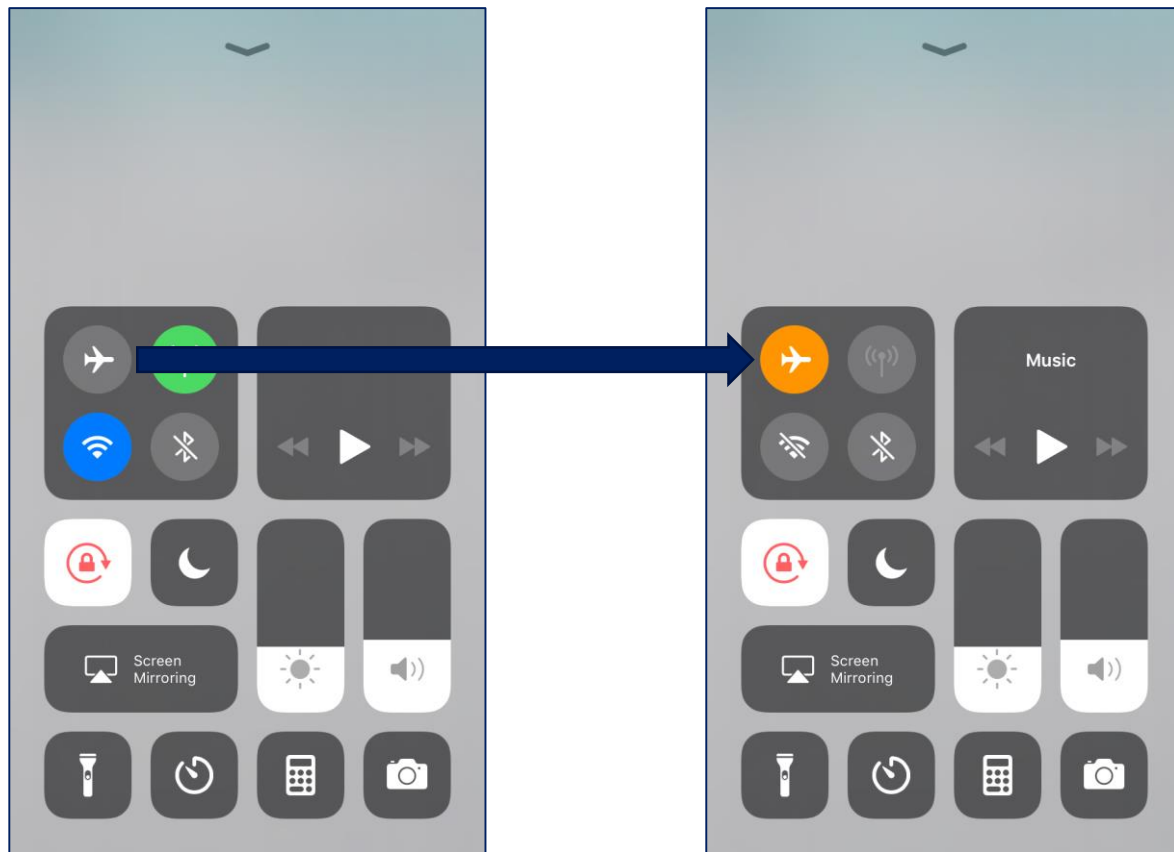
To improve security, for a locked iOS device to communicate with USB accessories you must either connect an accessory via lightning connector to the device while unlocked or enter your device passcode while connected, at least once a week.

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.

PRESERVATION – ACCESO e BLOCCATO

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. **Valutare 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



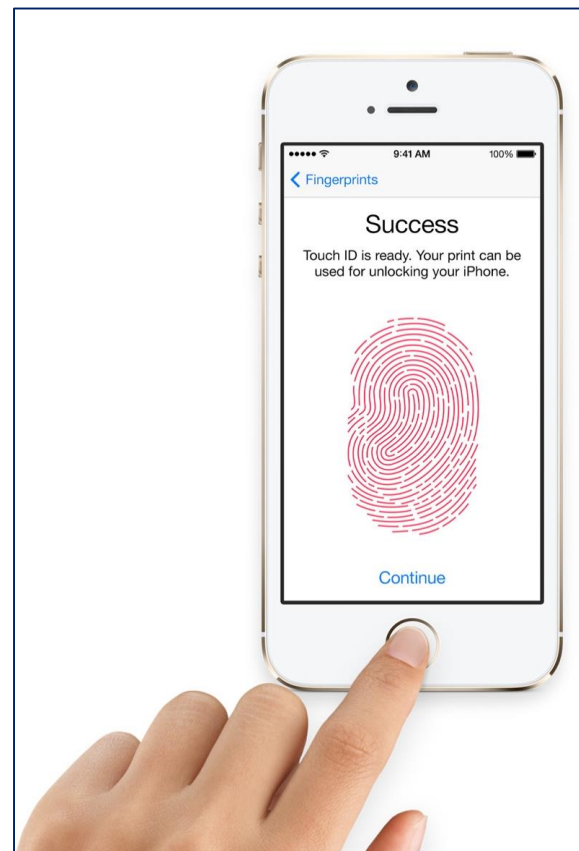
- **Libimobiledevice** (Linux/Mac)
<http://www.libimobiledevice.org/>
- **iMobiledevice** (Windows)
<http://quamotion.mobi/iMobileDevice/>
- **ideviceinfo -s**
- **Funziona anche senza pairing e quindi anche su dispositivi bloccati/spenti!**

IDENTIFICATION - Identificazione del modello e versione iOS

```
C:\imobiledevice>ideviceinfo -s
BasebandCertId: 3840149528
BasebandKeyHashInformation:
  AKeyStatus: 2
  SKeyHash: u+/tcCwvaQ+1Y9t40I4yegCEmB28mALLaR0haIVGBWo=
  SKeyStatus: 0
BasebandSerialNumber: CKyShA==
BasebandVersion: 4.00.01
BoardId: 4
BuildVersion: 15A402
ChipID: 32771
DeviceClass: iPhone
DeviceColor: #272728
DeviceName: iPhone mattia
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
```

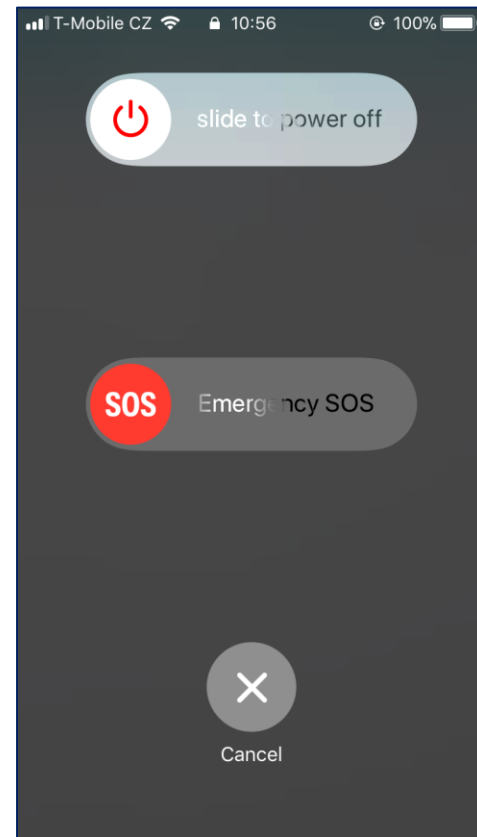
ACQUISITION – Fingerprint Unlock

- *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*
- <https://support.apple.com/en-us/HT204587>



ACQUISITION - iOS 11 – SOS Mode

- Apple has added an 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**



ACQUISITION – Vulnerabilità di una specifica versione

- <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)*

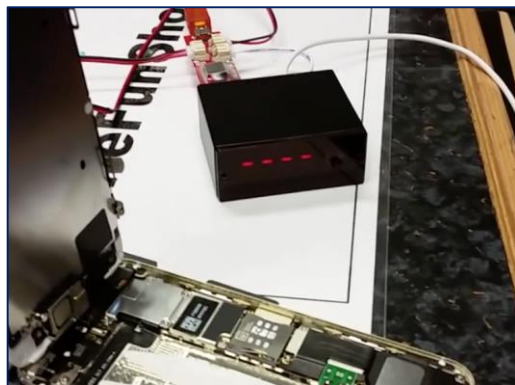
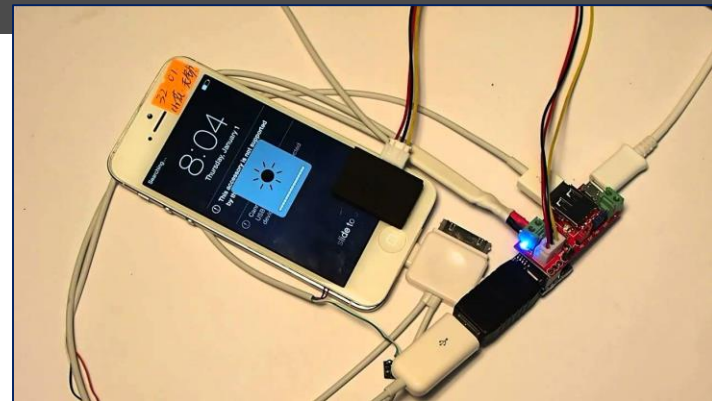


PRESERVATION – SPENTO

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



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 [i7 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 brute force cracking on the iPhone 7 and 7 Plus running iOS 10.

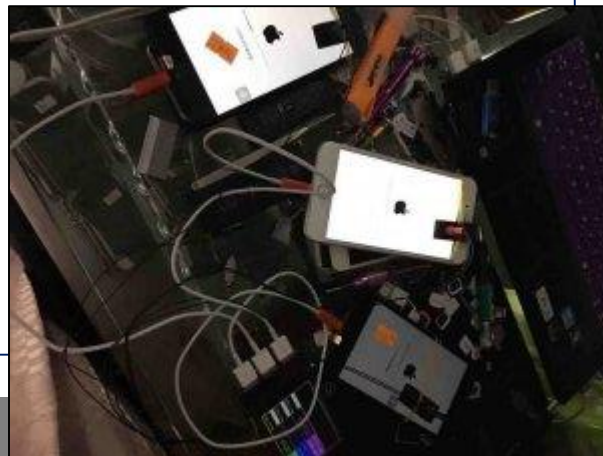
IP BOX 3 can also crack the passcodes on 3 different iPhone 7 or 7 Plus simultaneously

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



[Next product](#) →

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 Bundle on USB Stick For i7 Box (+€45.93)



ACQUISITION – Unlocking services – Cellebrite

Cellebrite Advanced Services

Advanced Unlocking & Extraction Services

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 S6/S7/S8, A5/A7/A8, J1/J3/J5/J7, Note 5/Note 8.
- 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

Functionality

- Successfully unlocks Apple iOS devices
- Controlled by simple web UI
- Plug and play platform; requires no special training
- Supports before *and* after first unlock state
- Prioritizes common and date-based passcodes
- Supports 4-digit, 6-digit, and complex passcodes
- Complete File System Extraction
- Extracts data not accessible in iTunes backups
- Supports disabled iOS devices
- Continually updated for new iOS versions
- Integrates with the leading Forensic Analysis Tools

iOS Support

Apple iOS 9.x (*coming soon*)
Apple iOS 10.x
Apple iOS 11.x

Device Support

iPhone 5 (*coming soon*)
iPhone 5c (*coming soon*)
iPhone 5s
iPhone 6 & 6 Plus
iPhone SE
iPhone 6s & 6s Plus
iPhone 7 & 7 Plus
iPhone 8 & 8 Plus
iPhone X

iPad Air & Air 2
iPad mini 2, 3, 4
iPad (2017)
iPad Pro (1st & 2nd gen)

iPod Touch (5th & 6th gen)

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.

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

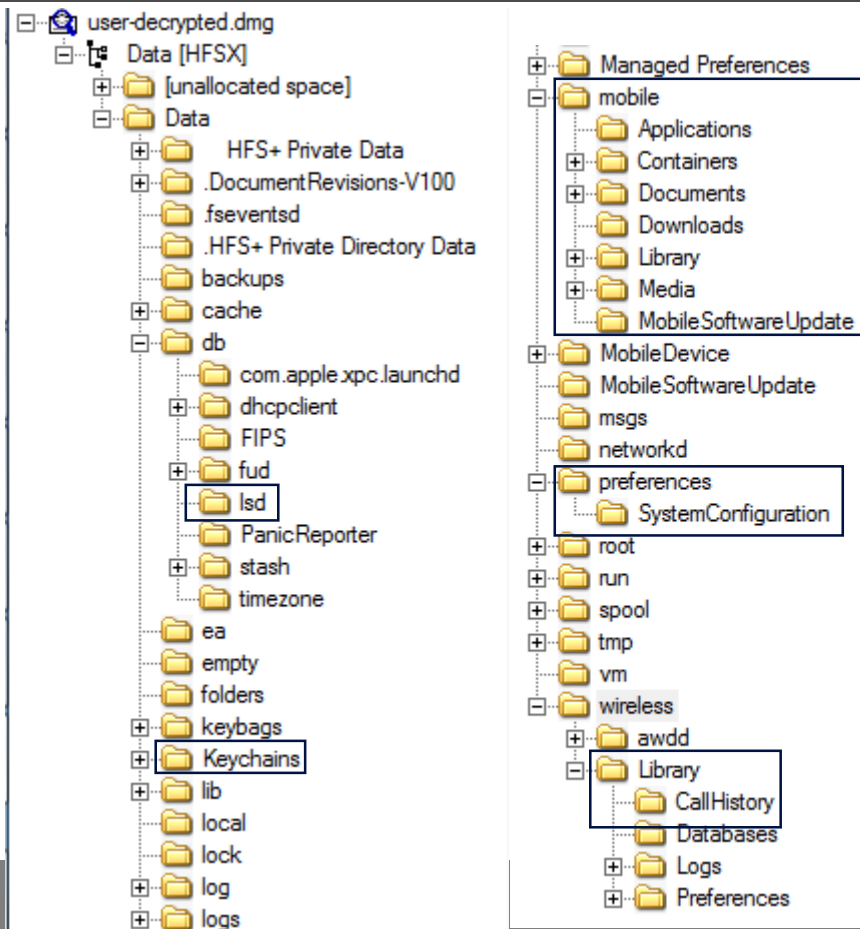
- **Disponibile fino a iPhone 4**
- Possibile su dispositivi **jailbroken**
- **Sostanzialmente inutile da un punto di vista forense!**

ACQUISITION – Fino ad iPhone 4

- 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.)

	Length	Avg. Crack time
Digits	4	20 minutes
	6	35 hours
	7	2 weeks
	8	4.5 months
	10	40 years
lowercase letters & spacebar	5	3 weeks
	6	1.5 years
	8	1000 years
Mixed case letters & spacebar	4	11 days
	5	1.6 years
	6	88 years

ACQUISITION – Backup vs. Physical Acquisition



ACQUISITION – Encrypted backup

iPhone 6s

Capacity: 55,53 GB

Phone Number: +39 334 2340899

Serial Number: F17QT811GRY9

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.

Change Password...

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



ACQUISITION – Encrypted backup

iPhone 6s

Capacity: 55,53 GB

Phone Number: +39 334 2340899

Serial N

iOS 9.3.5

Your iPhone software is up to date. iTunes will automatically

Oxygen Forensic® Extractor v.6.3.0.758

Oxygen Forensic® Extractor

Password recovery. Please wait.

» 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

Backups

Automa

☐ iCloud

Back

iCloud

☒ This

A full

computer.

Today 22:13 to this computer

☒ Encrypt iPhone backup

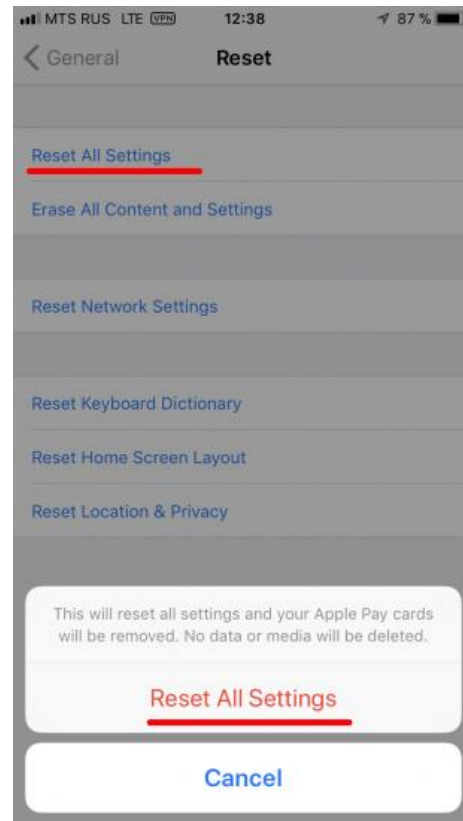
This will allow account passwords, Health, and HomeKit data to be backed up.

Change Password...

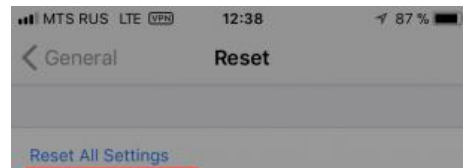
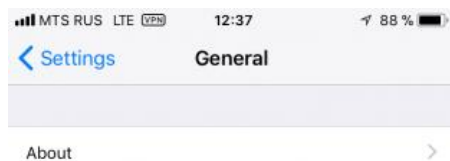
Help

Cancel

ACQUISITION – Encrypted backup – iOS 11

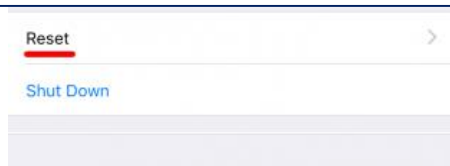


ACQUISITION – Encrypted backup – iOS 11

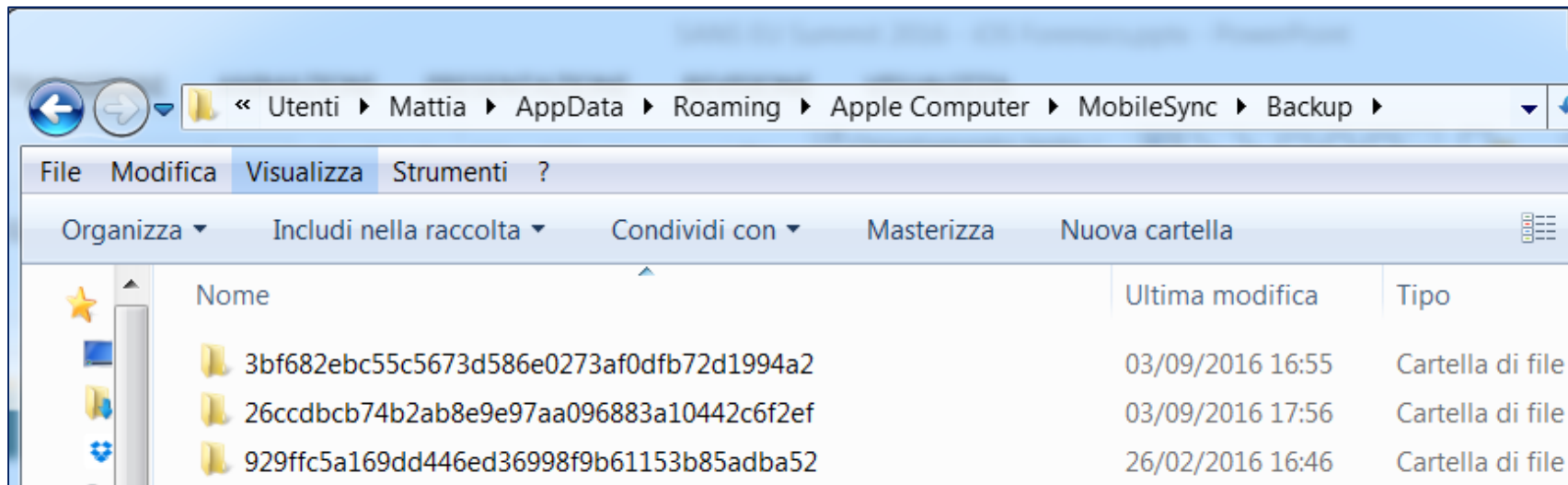


Using “Reset All Settings” will erase the following settings:

- » 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**

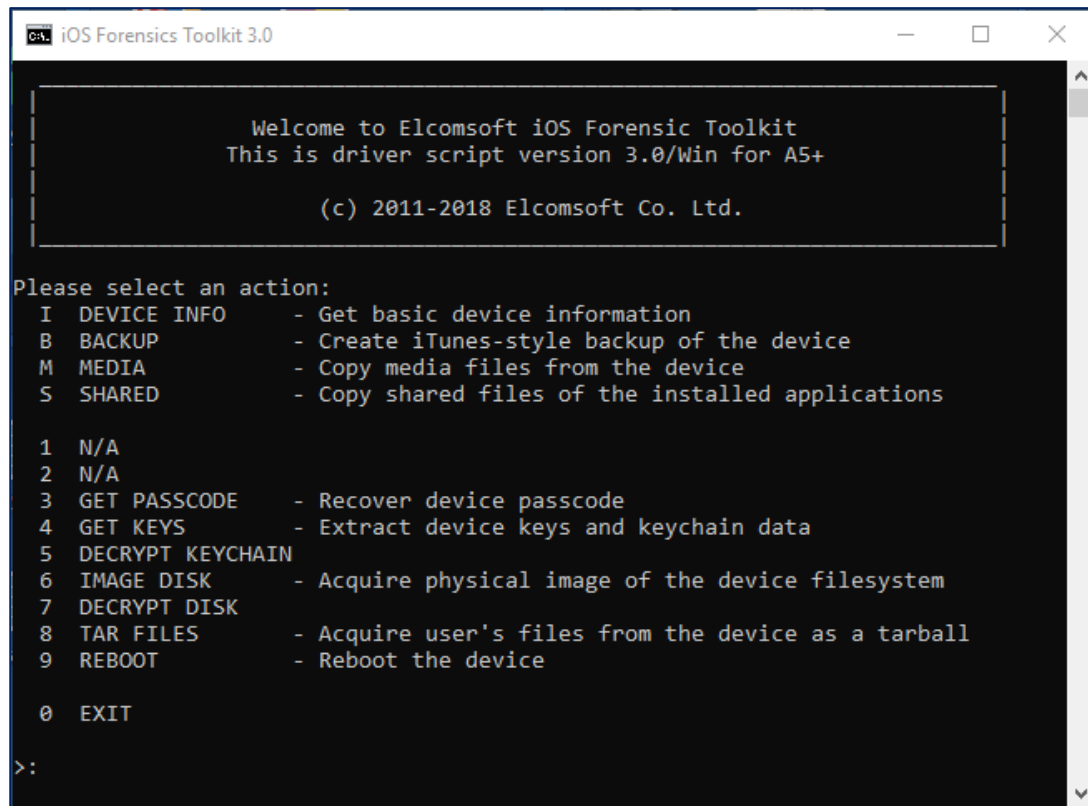


ACQUISITION – Backup memorizzati su PC/MAC



JAILBREAKING

<https://www.theiphonewiki.com/wiki/Jailbreak>



```
iOS Forensics Toolkit 3.0

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

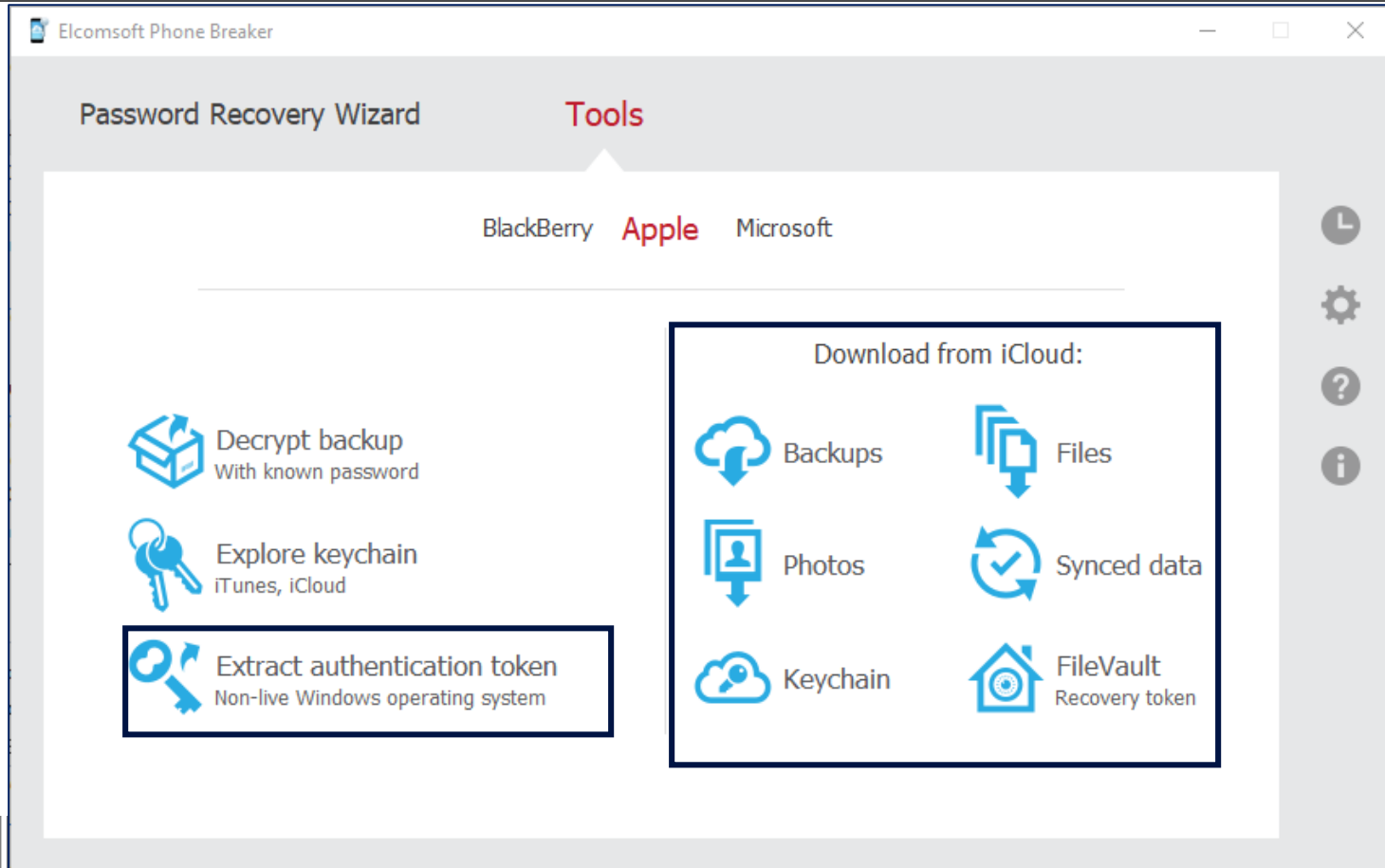
0  EXIT

>:
```

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**
 - **FileVault – Recovery Token**

ACQUISITION – Acquisizione dati da iCloud



ACQUISITION – Acquisizione dati da iCloud

Elcomsoft Phone Breaker

Password Recovery Wizard **Tools**

[All tools](#) Download backup from iCloud

Authentication type **Password** Token ?

Apple ID (example@example.com)

Password 

☒ Save credentials for future use ?

Sign in

⌚ ⚙️ ? ⓘ

ACQUISITION – Acquisizione dati da iCloud

Elcomsoft Phone Breaker

Password Recovery Wizard **Tools**

[All tools](#) Download backup from iCloud

Authentication type Password **Token** ?

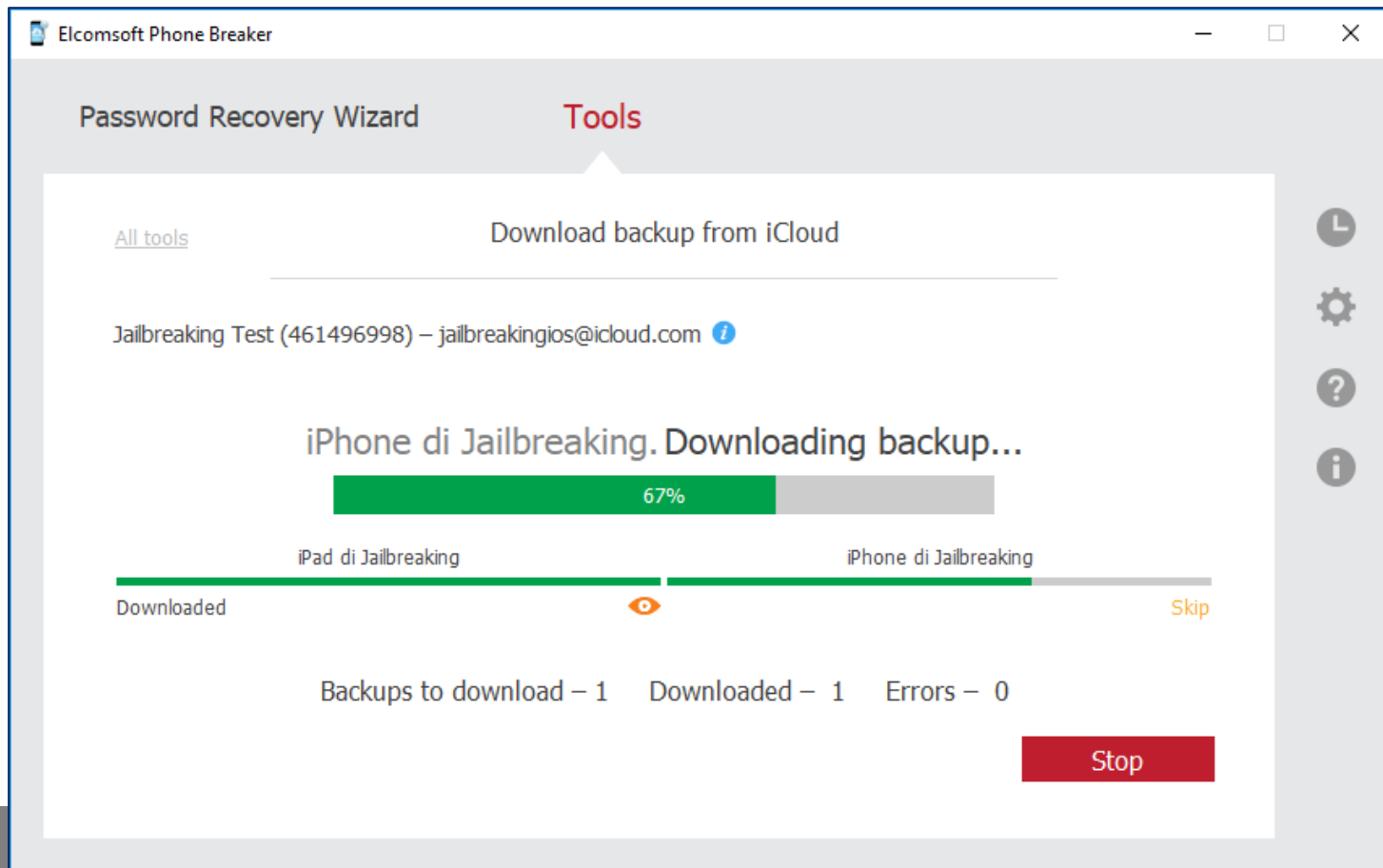
Token

☒ Save credentials for future use ?

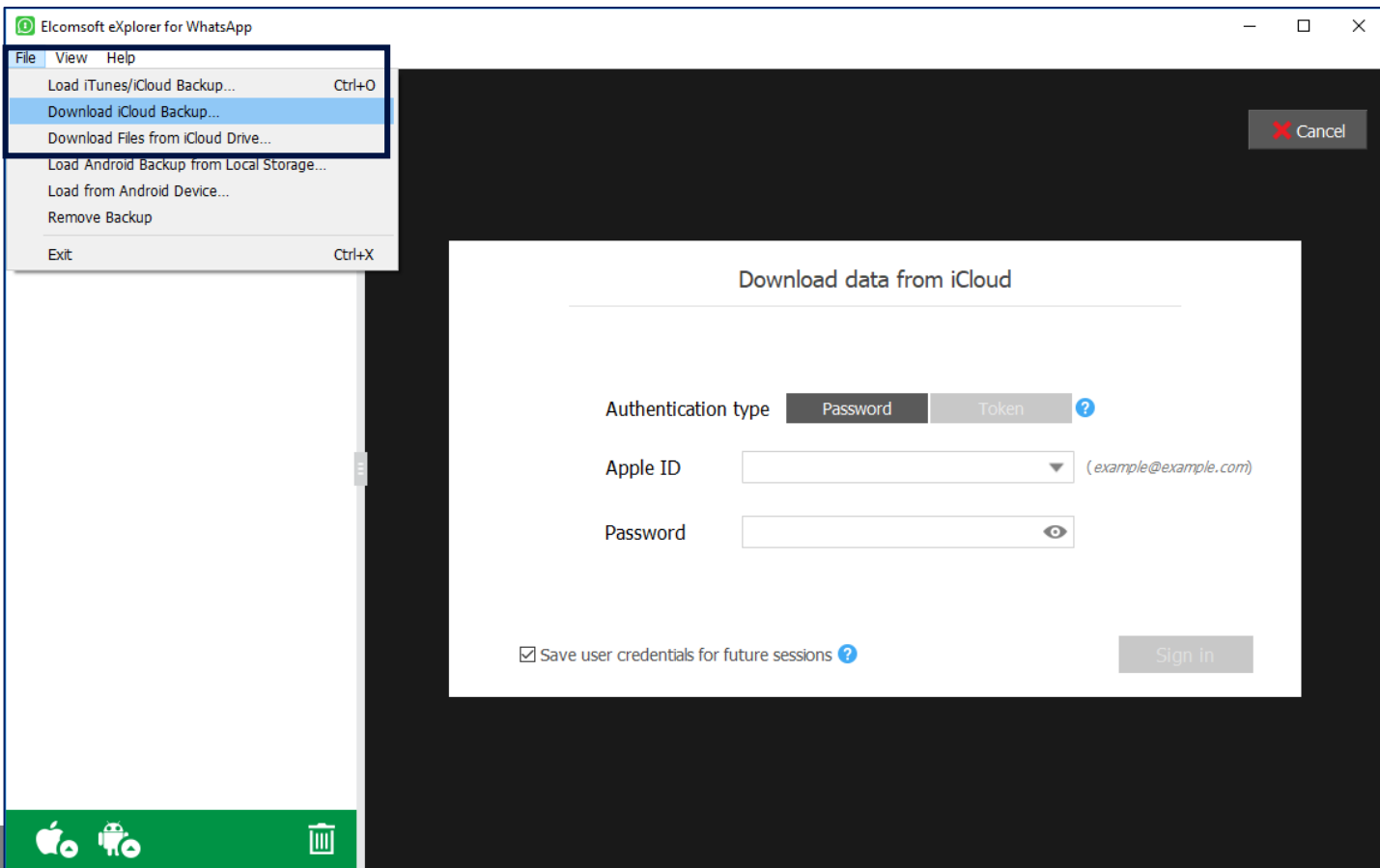
Sign in

⌚ ⚙️ ? ⓘ

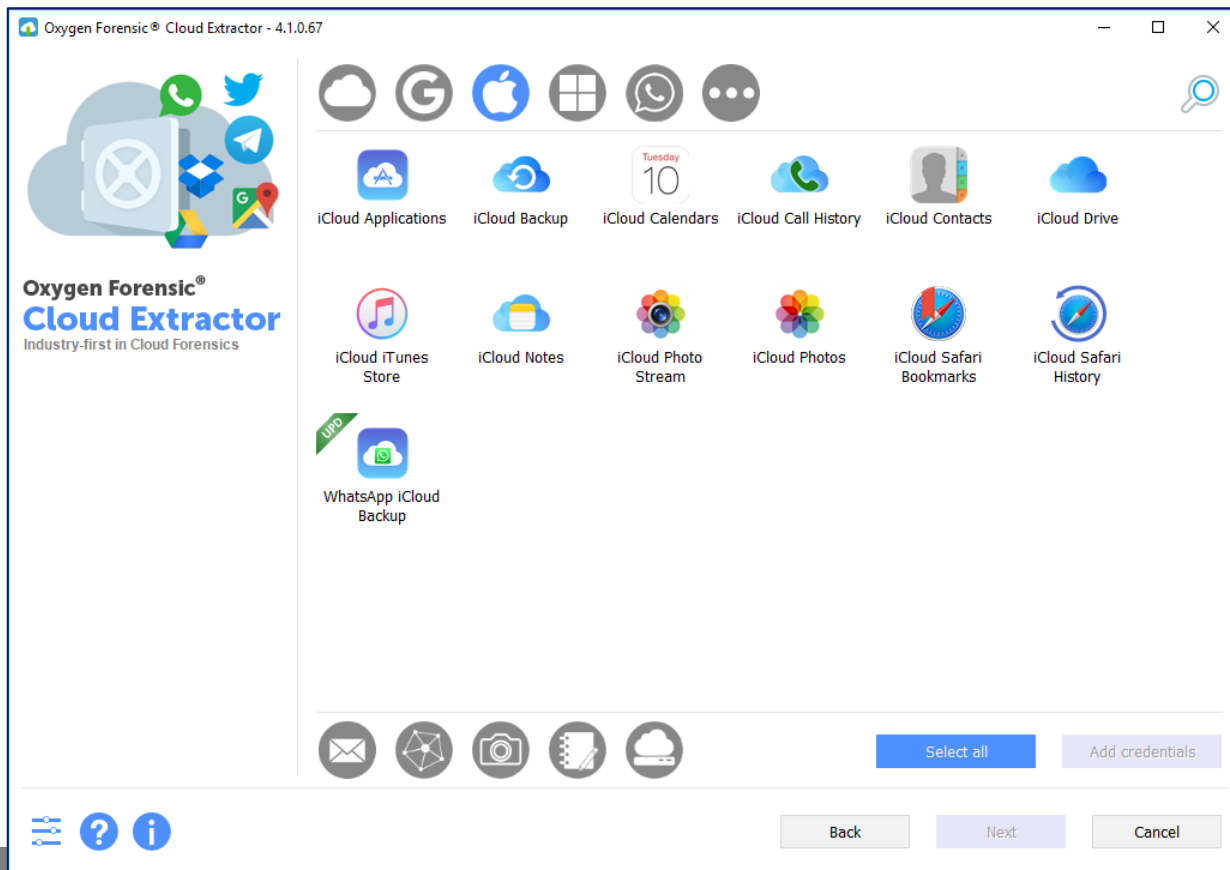
ACQUISITION – Acquisizione dati da iCloud



ACQUISITION – Acquisizione dati da iCloud



ACQUISITION – Acquisizione dati da iCloud



ACQUISITION – Acquisizione dati da iCloud

Oxygen Forensic® Cloud Extractor - 4.1.0.67



Oxygen Forensic®
Cloud Extractor
Industry-first in Cloud Forensics

Extract iCloud token from Windows PC

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

1. com.apple.AOSKit.plist file contains encrypted token.
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-XX-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXX

User password 

ACQUISITION - Richiesta di supporto ad Apple

- 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

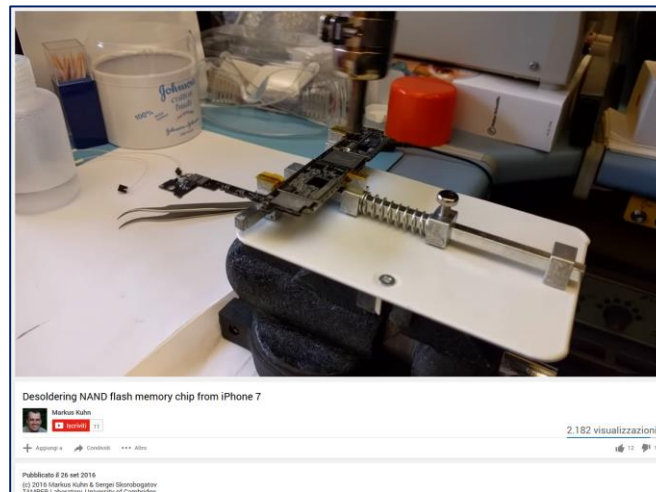
Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. Mail logs, if available, may be obtained with a court order under 18 U.S.C. § 2703(d) or a court order with an equivalent legal standard or a search warrant. iCloud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

ACQUISITION - Chip Off (tecniche sperimentali!)

- Ricerca pubblicata da Sergei Skorobogatov
- **The bumpy road towards iPhone 5C NAND mirroring**
 - http://www.cl.cam.ac.uk/~sps32/5c_proj.html
 - <https://arxiv.org/pdf/1609.04327v1.pdf>
 - <https://www.youtube.com/watch?v=tM66GWrwbsY>



Informazioni

Tasks

- Reread coordinates
- Reread coordinates and maps
- Show checked locations on OxyMaps

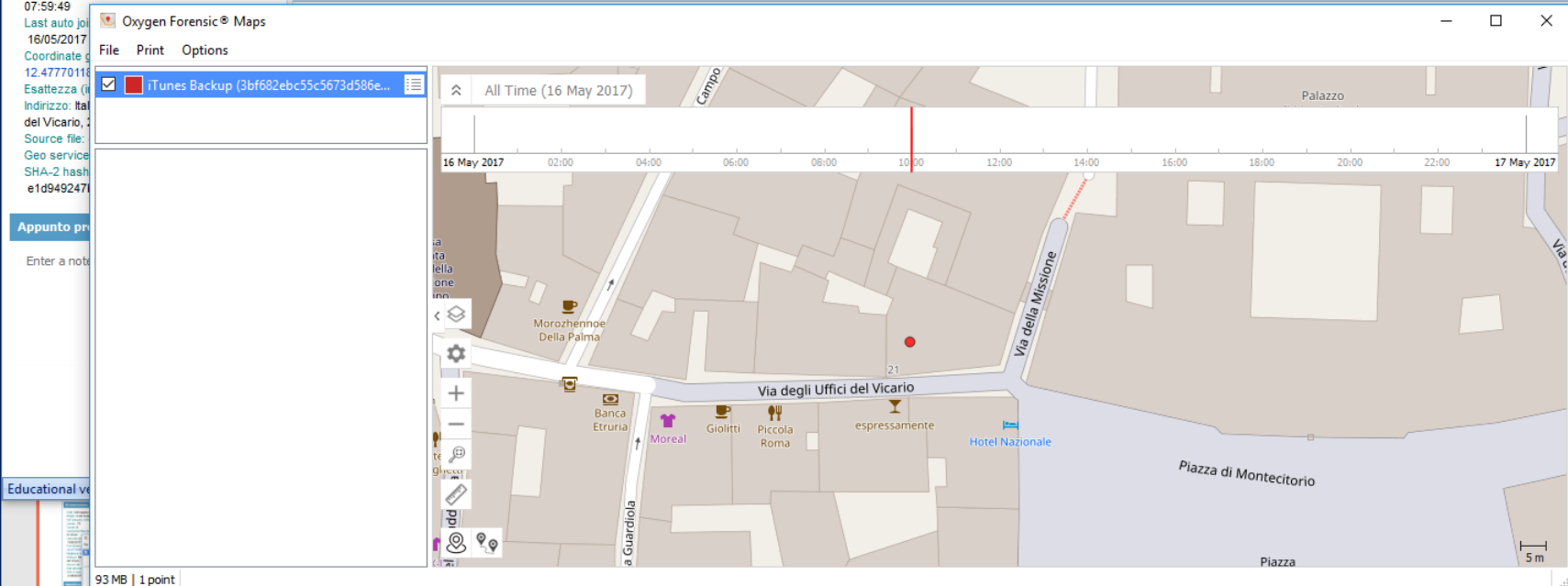
&Compressione:

SSID: Wifi-SalaRiunione01
BSSID: 7c:95:f3:6d:1e:14
WiFi security (WPA/WPA2): Yes
Canale: -79
Canale: 6
Last joined time (Device time): 16/05/2017 07:59:49
Last auto join: 16/05/2017
Coordinate g: 12.47770118
Esattezza (n): 140
Indirizzo: Italia, Lazio, Roma, Via degli Uffici del Vicario, 21, 00186 (N 41.9011840820313, E 12.4777011871338)
Source file:
Geo service
SHA-2 hash: e1d949247f

IP connections

	SSID	BSSID	Canale	Canale	Last joined time (Device time)	Last auto joined time (Device time)	Coordinate geo	Esattezza (n ...)	Indirizzo	SHA-2 hash
☒	Espace_Business	78:ba:f9:fa:99:c0	-53	1	29/05/2017 12:14:09	N/A	N 49.005416870117...	140	N/A	55c2ca4
☒	*WIFI-AIRPORT	ccd8:c1e0:d6:8e	-65	36	29/05/2017 10:12:07	29/05/2017 12:23:36	N 49.005306243896...	140	N/A	99c82ab
☒	#Free WiFi MilanoCentrale	84:24:8d:30:f1:10	-68	1	27/06/2017 16:47:13	09/07/2017 19:07:59	N 45.486213684082...	140	Italy, Lo...	15f796f
☒	Starhotels	2c:5d:93:1e:b6:68	-70	11	15/06/2017 16:33:25	16/06/2017 07:20:42	N 45.464153289794...	140	Italy, Lo...	144cfb4
☒	Mondial_Wifi	00:1f:9d:d9:c5:20	-45	8	16/05/2017 12:42:11	N/A	N 41.901515960693...	140	Italy, La...	0f52a76
☒	Wifi-SalaRiunione01	7c:95:f3:6d:1e:14	-79	6	16/05/2017 07:59:49	16/05/2017 10:00:10	N 41.901184082031...	140	Italy, La...	e1d9492
☒	HOTEL ARGENTINA	4c:60:de:47:cf:06	-63	11	15/05/2017 13:31:39	16/05/2017 16:56:17	N 41.899719238281...	140	Italy, La...	2e1c707
☒	El Nacional	00:1f:d4:03:54:81	-71	11	10/06/2017 21:44:23	10/06/2017 23:55:29	N 41.390560150146...	140	Spain, C...	6fb1555
☒	attwifi	00:0d:67:17:82...	-74	149	22/05/2017 01:42:27	N/A	N 36.112663269043...	140	N/A	62c2fd5

Italy, Lazio, Roma, Via degli Uffici del Vicario, 21, 00186 (N 41.9011840820313, E 12.4777011871338)



Datenquelle Educational

File Mostra Strumenti Servizio Guida

← → All devices ▸ Unassigned devices ▸ iTunes Backup (3bf682ebc55c5673d586e0273af0dfb72d1994a2) - 19/10/2017 12:30:20 [355427078639925] ▸ Navigation ▸ Waze

Connetti il dispositivo ▾ Esporta ▾ Stampa ▾ Recupero dati ▾ Modalità visualizzazione Imposta fuso orario Annulla filtri Guida

Informazioni << User data (7) Application files (50) Application information (87)

Informazioni Applicazione ▾

Parole chiavi ▾ Copia negli appunti ▾ Mostra miniature Mappe e Percorsi ▾ Esporta in KML ▾ Ridimensiona

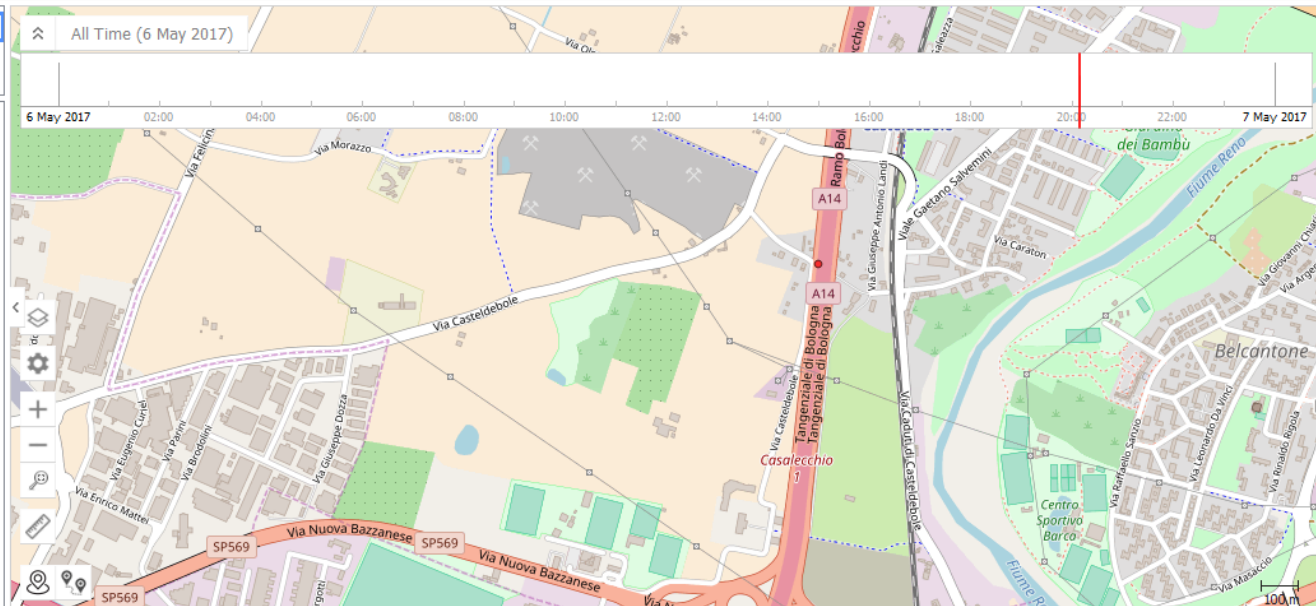
Waze
7 items
com.waze.iphone
Container:

	Account	First name	Last name	User name	Categorie
☒	Account			world_d3ccrk5	All categories 7
☒	Session info	Time stamp (Device time)	GPS position	Last navigation coordinates	Account 1
☒		06/05/2017 18:09:25	44.499485;11.271516	41.797172;12.486316	Session info 1
☒	Viewed addresses	Address	State	City	Viewed addresses 2

Oxygen Forensic® Maps

File Print Options

☒ iTunes Backup (3bf682ebc55c5673d586e0273af0dfb72d1994a2)



104 MB | 1 point

Educational version: 10.1.0.100

iTunes Backup (3bf682ebc55c5673d586e0273af0dfb72d1994a2)

Total: 7

Filtered: 7

Information
int.
the
ession.
e info about
avorites. (As
addresses
the device
pp cookies.

Mostrare mai

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

SANS FOR 585 - Advanced Smartphone Forensics

Course Syllabus

+ FOR585.1: Malware Forensics, Smartphone Overview, and SQLite Introduction

+ FOR585.2: Android Forensics

+ FOR585.3: Android Backups and iOS Device Forensics

+ FOR585.4: iOS Backups, Windows, and BlackBerry 10 Forensics

+ FOR585.5: Third-Party Application and Knock-Off Forensics

+ FOR585.6: Smartphone Forensic Capstone Exercise

SANS FOR 585 - Advanced Smartphone Forensics

Type	Topic	Course / Location / Instructor	Date	Register
 Training Event	Mobile Devices	FOR585: Advanced Smartphone Forensics (In English) SANS Paris June 2018 Paris, France Cindy Murphy	Jun 25, 2018 - Jun 30, 2018	
 Training Event	Mobile Devices	FOR585: Advanced Smartphone Forensics SANS Stockholm 2018 Stockholm, Sweden Heather Mahalik	Nov 26, 2018 - Dec 1, 2018	

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

Title	Certification	Instructor
FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting (In Italian)	GCFA	Francesco Picasso
FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response	GNFA	Matt Bromiley

FOR500
Windows Forensics
GCFE



FOR518
Mac Forensics



FOR526
Memory Forensics
In-Depth



FOR585
Advanced Smartphone
Forensics GASF



SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

OPERATING
SYSTEM &
DEVICE
IN-DEPTH



INCIDENT
RESPONSE
& THREAT
HUNTING

FOR508
Advanced IR
and Threat Hunting GCFA



FOR572
Advanced Network Forensics
and Analysis GNFA



FOR578
Cyber Threat Intelligence



FOR610
REM: Malware Analysis
GREM



SEC504
Hacker Tools, Techniques,
Exploits, and Incident Handling
GCIH



@sansforensics



sansforensics



dfir.to/DFIRCast

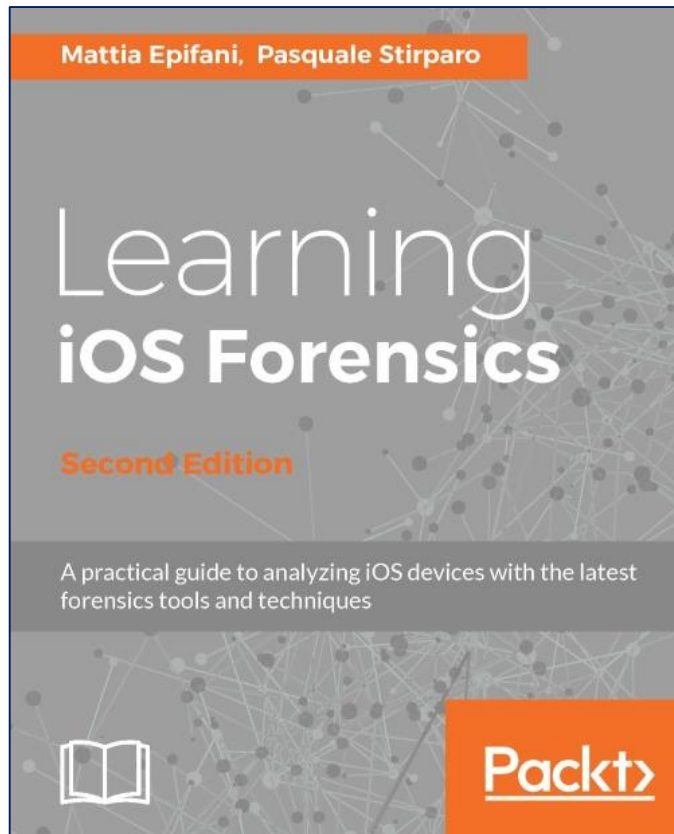


dfir.to/gplus-sansforensics



dfir.to/MAIL-LIST

Learning iOS Forensics – Second Edition



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](https://twitter.com/mattiaep)



<http://www.linkedin.com/in/mattiaepifani>



<http://www.realitynet.it>



<http://blog.digital-forensics.it>