ACQUISIZIONE DI DISPOSITIVI IOS

MATTIA EPIFANI

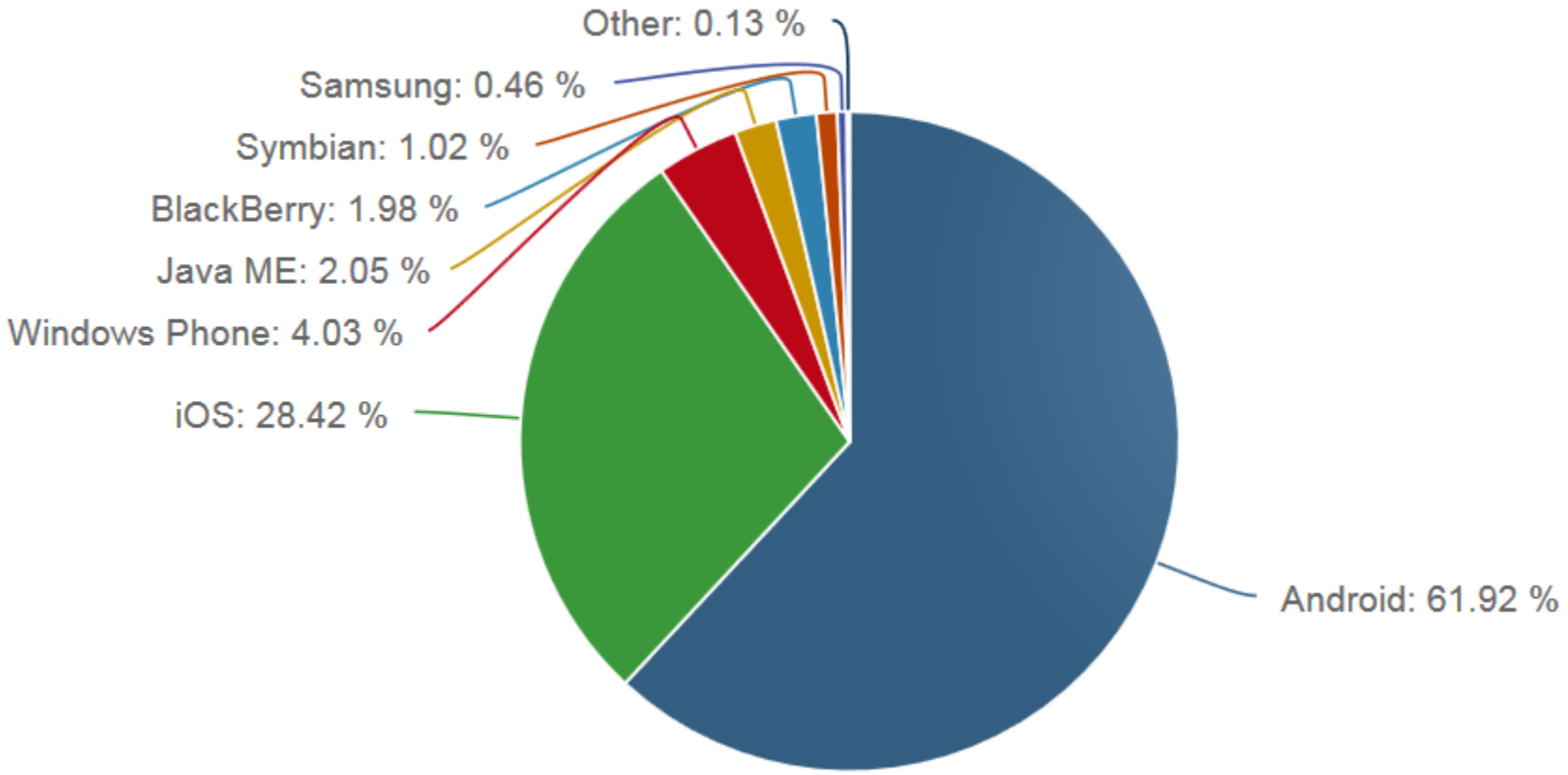
UNIMI

MILANO, 24 MAGGIO 2016

MOBILE FORENSICS

- Settore della Digital Forensics (Informatica Forense) che si occupa **dell'acquisizione e dell'analisi di dispositivi mobile**
- Tipicamente smartphone, tablet, navigatori satellitari, ecc.
- Uno dei settori in maggiore crescita, poichè i dispositivi mobile contegono al giorno d'oggi informazioni spesso di interesse per una indagine

PERCHE' IOS FORENSICS? (APRILE 2016)



IOS

Introdotto nel 2007

- iPhone OS (v 1-3)
- iOS (v4+)

Versione corrente: iOS 9.3.2 (Maggio 2016)

iDevices

- iPhone
- iPad
- Apple TV
- iPod Touch
- Apple Watch

Versione "lite" di OS X

- Due account utente: "**mobile**" e "**root**"
- Struttura del file system molto simile

OS X VS. IOS

OS X

- Intel x86 - 64
- HFS+
- Mouse and Keyboard
- Sandboxing (Containers)
- Finder

iOS

- ARM 32/64
- HFS+
- Touch
- Sandboxing (Jail)
- Springboard

IOS - PARTIZIONI

System

/dev/disk0s1s1
(HFSX+, HX Volume Signatures)

Mount Point: /

~1-2 GB
(a seconda della versione)

Data

/data/disk0s1s2
(HFSX+, HX Volume Signatures)

Mount Point: /private/var

Fino a 127 GB
(a seconda del tipo di iDevice)

ACQUISIZIONE DI UN DISPOSITIVO IOS

- Due casi:
  - **Dispositivo spento**
    - **LO LASCIAMO SPENTO**
  - **Dispositivo acceso (bloccato o sbloccato)**
    - **NON SPEGNERLO E RIFLETTERE!**

DISPOSITIVO ACCESO E BLOCCATO

1. Attivare la modalità aerea
2. Collegarlo a una sorgente di corrente (es. batteria esterna)
3. Individuare lo specifico modello
4. Identificare la versione del sistema operativo

TIPOLOGIE DI PASSCODE

- **Solo numeri**
- Lunghezza = 4

TIPOLOGIE DI PASSCODE

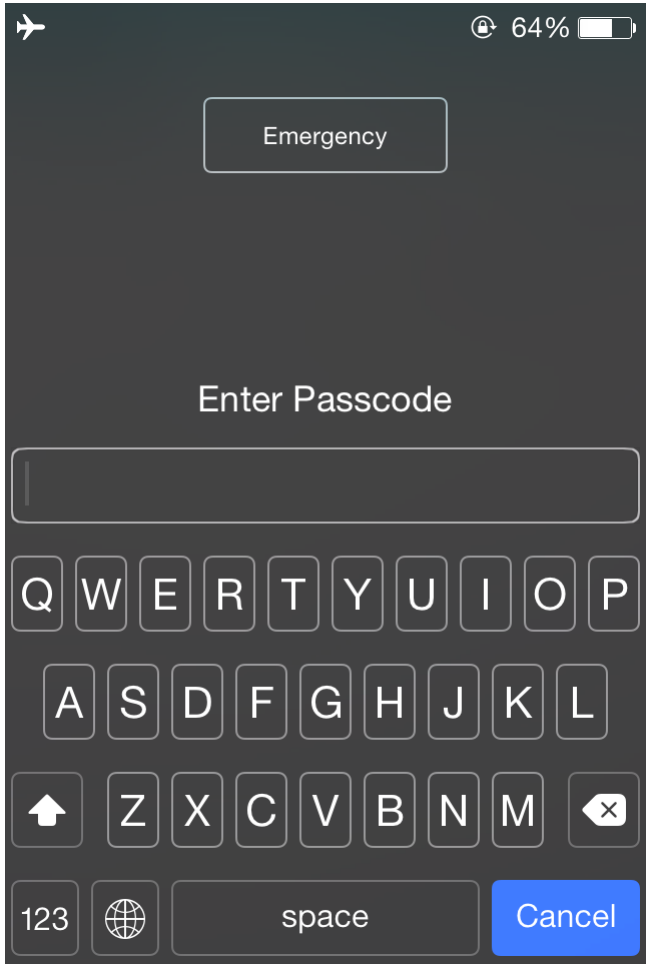
- **Solo numeri**
- Lunghezza = 6

TIPOLOGIE DI PASSCODE

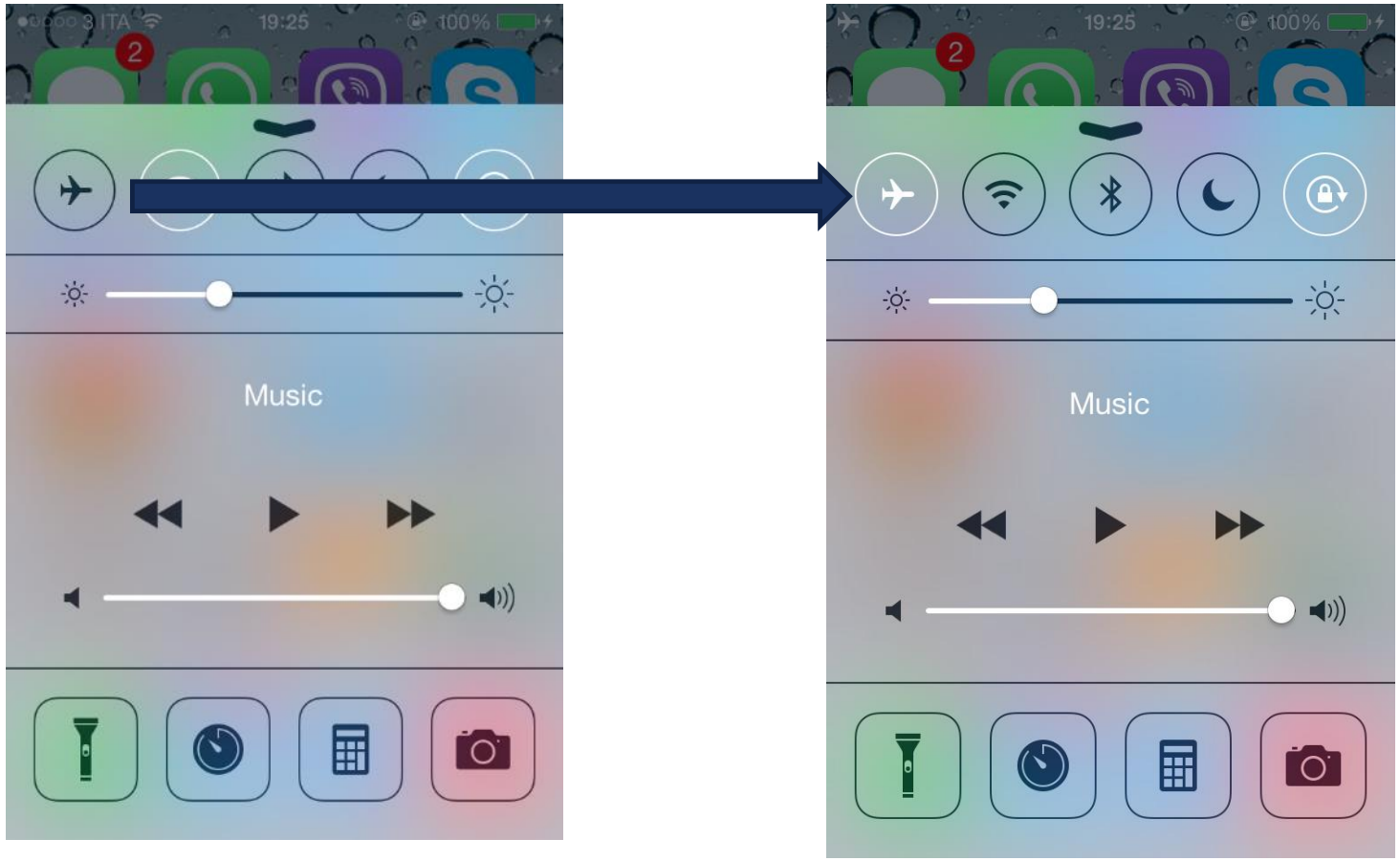
- **Solo numeri**
- Lunghezza diversa da 4 e 6

TIPOLOGIE DI PASSCODE

- **Contiene caratteri diversi dai numeri**
- Qualsiasi lunghezza



ATTIVAZIONE AIRPLANE MODE
DISPOSITIVO BLOCCATO



IDENTIFICAZIONE DEL MODELLO

- Il numero di modello si trova sul retro del dispositivo

IPHONE MODEL CHART

Device name	Model number	Internal Name	Identifier	Year	Capacity (GB)
iPhone SE	A1662 – A1723 – A1724	N69AP	iPhone8,4	2016	16,64
iPhone 6s Plus	A1634 – A1687 – A1699 – A1690	N66AP	iPhone8,2	2015	16,64,128
iPhone 6s	A1633 – A1688 – A1700 – A1691	N71AP	iPhone8.1	2015	16,64,128
iPhone 6 Plus	A1522 – A1524 – A1593	N56AP	iPhone7,1	2014	16,64,128
iPhone 6	A1549 – A1586	N61AP	iPhone7,2	2014	16,64,128
iPhone 5S (CDMA)	A1457 – A1518 – A1528 – A1530	N53AP	iPhone6,2	2013	16, 32
iPhone 5S (GSM)	A1433 – A1533	N51AP	iPhone6,1	2013	16, 32, 64
iPhone 5C (CDMA)	A1507 – A1516 – A1526 – A1529	N49AP	iPhone5,4	2013	16, 32
iPhone 5C (GSM)	A1456 – A1532	N48AP	iPhone5,3	2013	16, 32
iPhone 5 rev.2	A1429 – A1442	N42AP	iPhone5,2	2012	16, 32, 64
iPhone 5	A1428	N41AP	iPhone5,1	2012	16, 32, 64
iPhone 4s (China)	A1431	N94AP	iPhone4,1	2011	8, 16, 32, 64
iPhone 4S	A1387			2011	8, 16, 32, 64
iPhone 4 - CDMA	A1349	N92AP	iPhone3,2	2011	8, 16, 32
iPhone 4 - GSM	A1332	N90AP	iPhone3,1	2010	8, 16, 32
iPhone 3GS (China)	A1325	N88AP	iPhone2,1	2009	8, 16, 32
iPhone 3GS	A1303			2009	8, 16, 32
iPhone 3G (China)	A1324	N82AP	iPhone1,2	2009	8, 16
iPhone 3G	A1241			2008	8, 16
iPhone 2G	A1203	M68AP	iPhone1,1	2007	4, 8, 16

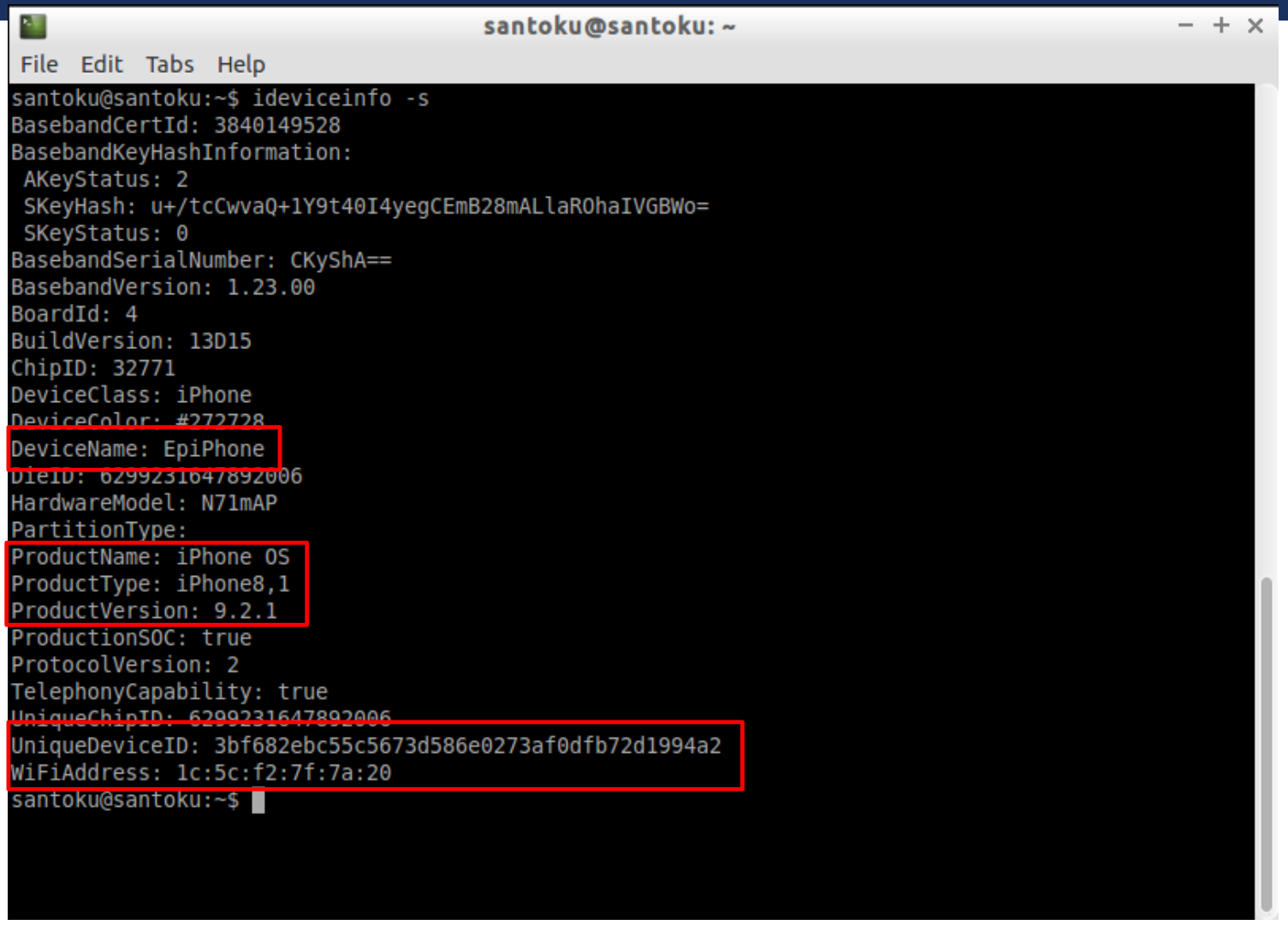
IDENTIFICAZIONE DEL MODELLO E DEL SISTEMA OPERATIVO

- Effettuare boot del proprio PC con **Santoku Live CD** o **DEFT 8.2**
- **https://santoku-linux.com/**
- Tool: **ideviceinfo** (libimobiledevice.org)
- Opensource
- **Funziona anche se il dispositivo è bloccato con un passcode**

IDENTIFICAZIONE DEL MODELLO E DEL SISTEMA OPERATIVO

```
santoku@santoku:~$ ideviceinfo -s
ActivationPublicKey: LS0tLS1CRUdJTiBSU0EgUFVCTElDIEtFWS0tL
oMXo5cHFjdmZnTXBZYTVIVWJUMnBrSFgKdFFZUU0ydlAzblZtN2JqNFhTQ
rcwoyNWpmck5Rc25JdStsK0ZRS1dUckdNMmpldzBhVXFIU0haL2xCRDFQS
tLS0tLQo=
BoardId: 10
BuildVersion: 10B146
ChipID: 35138
DeviceClass: iPad
DeviceName: iPad di Mattia
DevicePublicKey: LS0tLS1CRUdJTiBSU0EgUFVCTElDIEtFWS0tLS0tC
zWGpNOFY5N2l3NHBmY282ci9VeCsKanNPOWVSSWVaZmR6UmZYKy9kY1FyZ
BSnhwVVBtUllod1VaNDhrYUdVS21aVmZDYUpCNVpRclRyNnFBZVJoeEpGV
tLQo=
DieID: 3609108662014788576
HardwareModel: P105AP
PartitionType:
ProductVersion: 6.1.2
ProductionSOC: true
ProtocolVersion: 2
TelephonyCapability: false
UniqueChipID: 1823148166600
UniqueDeviceID: 08399bf9b65bc55e2783776b559c02dc90bd65ef
WiFiAddress: e0:f5:c6:31:02:54
```

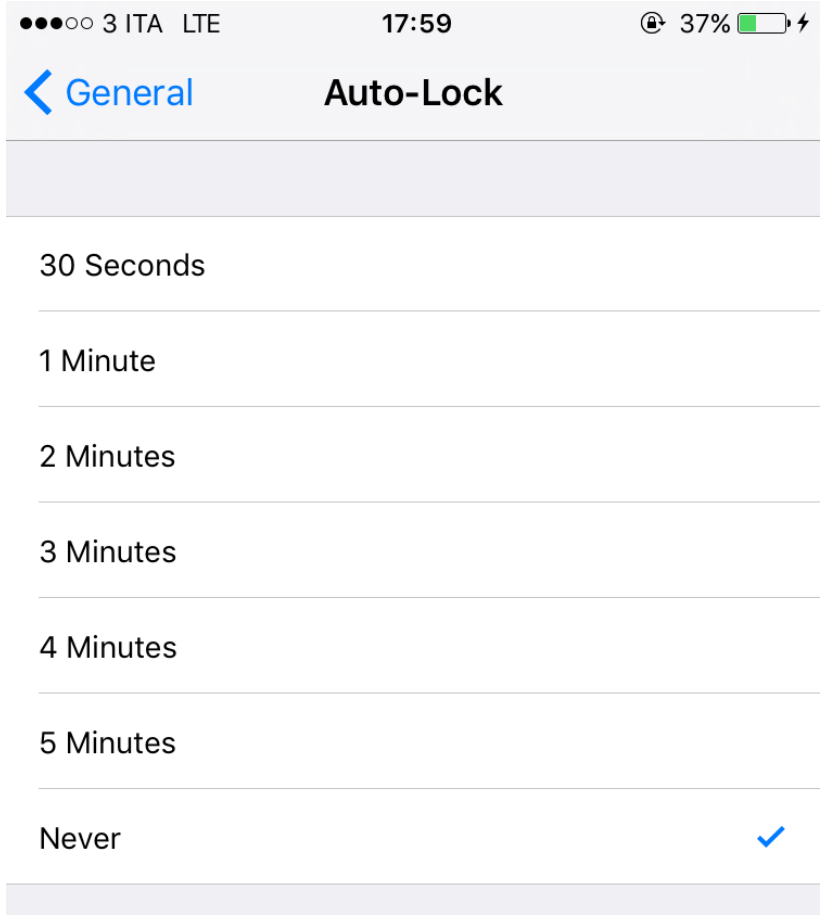
IDENTIFICAZIONE DEL MODELLO E DEL SISTEMA OPERATIVO



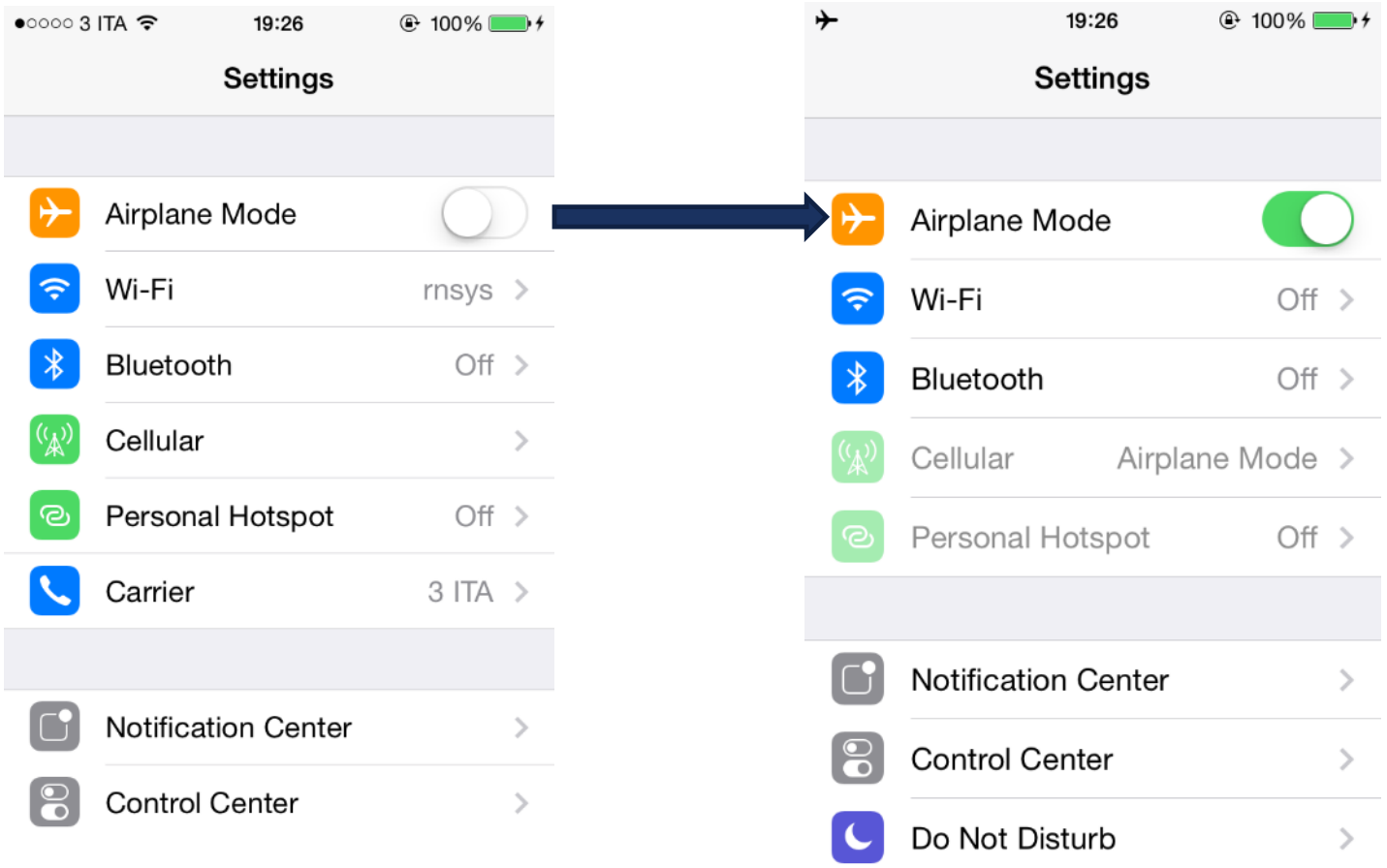
DISPOSITIVO ACCESO E SBLOCCATO

1. Prevenire che il dispositivo vada in blocco
2. Attivare la modalità aerea
3. Collegarlo a una sorgente di corrente (es. batteria esterna)
4. Individuare lo specifico modello
5. Identificare la versione del sistema operativo

PREVENIRE CHE IL DISPOSITIVO VADA IN BLOCCO (DISABILITARE AUTO-LOCK)



ATTIVAZIONE AIRPLANE MODE DISPOSITIVO SBLOCCATO



IOS – TECNICHE DI ACQUISIZIONE

Acquisizione fisica

- Immagine bit-stream della memoria interna

Acquisizione File System

- Estrazione di parte del file system
- 3 metodologie
  - **iTunes Backup** — Può essere protetto da password
  - **Apple File Relay** — Basato su Lockdown Services Zdziarski, 2014
  - **Apple File Conduit**

IPHONE 4 E PRECEDENTI

- E’ sempre possibile effettuare una **acquisizione fisica basata su exploit a livello di bootrom**, anche se il dispositivo è protetto con un passcode complesso
- Se il dispositivo è senza codice di blocco o se è bloccato con un codice che può essere violato in un tempo ragionevole, allora possiamo accedere a **tutti i contenuti**
- Se non è possibile fare il cracking del codice non è possibile accedere alle email e alle applicazioni di terze parti, ma **si possono recuperare le altre informazioni native** (rubrica, SMS/MMS, immagini, video, cronologia di navigazione, ecc.)

IPHONE 4 – TEMPI DI CRACKING

	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

IPHONE 4S E SUCCESSIVI – SBLOCCATI

- Non sono noti exploit a livello di bootrom, quindi **non è possibile effettuare una acquisizione fisica** [in modo non invasivo]
- Se il dispositivo è **sbloccato** è **sempre possibile effettuare una acquisizione di parte del file system**

IPHONE 4S E SUCCESSIVI – BLOCCATI E ACCESI

- Se il dispositivo è **bloccato** e **acceso** abbiamo sostanzialmente 3 possibilità:
  - Certificato di Lockdown
  - Vulnerabilità della specifica versione del S.O.
  - Forzare un backup su iCloud
- Certificato di lockdown
  - Verificare la disponibilità di un computer che è stato utilizzato per collegare il telefono
  - Ricercare sul computer il certificato di lockdown dello specifico dispositivo
  - Copiare il certificato di lockdown in un computer con iTunes o un software forense
  - Creare un backup e/o effettuare una acquisizione attraverso Apple File Relay
- Queste azioni devono essere effettuate **live e prima di spegnere il dispositivo**
- Il dispositivo deve essere stato **sbloccato almeno una volta nelle ultime 48 ore**

CERTIFICATI LOCKDOWN

- Memorizzati in:
  - C:\Program Data\Apple\Lockdown — Win 7/8
  - C:\Users\[username]\AppData\roaming\Apple Computer\Lockdown — Vista
  - C:\Documents and Settings\[username]\Application Data\Apple Computer\Lockdown — XP
  - /private/var/db/lockdown — Mac OS X
- Un certificato per ciascun dispositivo sincronizzato con il computer
- Nome del certificato → **Device_UDID.plist**
- Il **Device UDID** può essere estratto utilizzando il tool illustrato prima
- **Possiamo prendere il certificato memorizzato in un computer e copiarlo in un altro, avendo così accesso al contenuto del dispositivo**

IPHONE 4S E SUCCESSIVI – BLOCCATI E SPENTI

- Se il dispositivo è **bloccato** e **spento** possiamo distinguere **quattro casi**:
  - Il sistema operativo è **fino ad iOS 7** ed **è disponibile un certificato di Lockdown**
  - Il sistema operativo è **fino ad iOS 7** e **non è disponibile un certificato di Lockdown**
  - Il sistema operativo è **iOS 8** ed è **disponibile un certificato di Lockdown**
  - Il sistema operativo è **iOS 8** e **non è disponibile un certificato di Lockdown**
  - Il sistema operativo è **iOS 9**

IPHONE 4S E SUCCESSIVI – BLOCCATI E SPENTI
IOS 7 E CERTIFICATO DI LOCKDOWN

- Non è possibile effettuare il backup con iTunes
- E' possibile effettuare l'acquisizione basata su **Apple File Relay** (Lockdown Services)
- **Funziona anche se l'utente ha impostato una password di backup**
- **Identifying back doors, attack points, and surveillance mechanisms in iOS devices**
  http://www.zdziarski.com/blog/wp-content/uploads/2014/08/Zdziarski-iOS-DI-2014.pdf

IPHONE 4S E SUCCESSIVI – BLOCCATI E SPENTI
IOS 7 E NO CERTIFICATO DI LOCKDOWN

- Diverse soluzioni che permetto di **trasmettere il passcode attraverso USB**
- Possibile effettuare il brute force di passcode semplici (4 numeri)
- Funzionano **anche se il dispositivo è disabilitato**
- Può essere **utilizzato per sbloccare il dispositivo se lo schermo è rotto**
- In caso di funzionalità di wiping attiva si può perdere l'accesso ai dati in via definitiva
- UFED User Lock Code Recovery Tool
- IB-BOX

IPHONE 4S E SUCCESSIVI – BLOCCATI E SPENTI
IOS 8 E CERTIFICATO DI LOCKDOWN

- Non è possibile effettuare il backup con iTunes
- Non è possibile effettuare l'acquisizione basata su Apple File Relay
- E' possibile effettuare una acquisizione attraverso protocollo Apple File Conduit
- Il risultato in termini di quello che si ottiene dipende fortemente dalla versione del sistema operativo
- In generale è **possibile recuperare contenuti multimediali e informazioni relative (es. Libreria di iTunes)**

IPHONE 4S E SUCCESSIVI – BLOCCATI E SPENTI
IOS 8 E NO CERTIFICATO DI LOCKDOWN

- Se il dispositivo è a 32 bit (iPhone 4s, 5, 5c) è possibile utilizzare il servizio offerto da Cellebrite (CAIS)
- Garantiscono il recupero di passcode semplici senza necessità di interventi hardware e rischi di wiping
- Per tutti gli altri dispositivi, fino ad iOS 8.1, è possibile utilizzare IP-BOX
  - Necessità di smontare il dispositivo
  - Rischio di wiping

CELLEBRITE CAIS SERVICE

HTTP://WWW.CELLEBRITE.COM/PAGES/CELLEBRITE-SOLUTION-FOR-LOCKED-APPLE-DEVICES-RUNNING-IOS-8X

UNLOCK APPLE DEVICES RUNNING IOS 8.X WITH NO RISK OF DEVICE WIPE OR HARDWARE INTERVENTION

CELLEBRITE'S SOLUTION FOR LOCKED APPLE DEVICES RUNNING IOS 8.X

Locked Apple devices. What do you do? Is it really a dead end?

One of the greatest challenges faced in the forensic industry today is the need to quickly access mobile device evidence from locked Apple devices running iOS 8. Even with the most sophisticated mobile forensics tools and technology available, additional expertise and skills are required to unlock these devices.
Cellebrite has a unique unlock capability for devices running iOS 8.x that will provide you with unprecedented access to evidence you can stand behind.

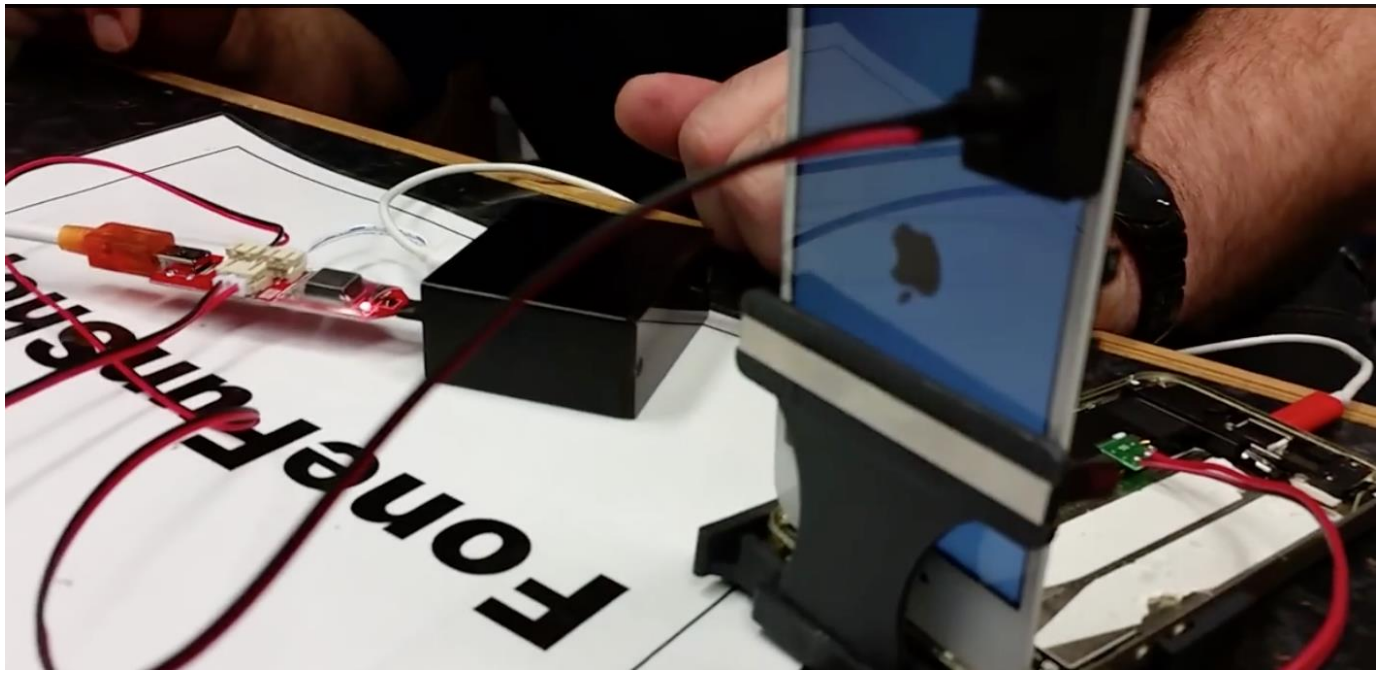
CELLEBRITE CAIS SERVICE

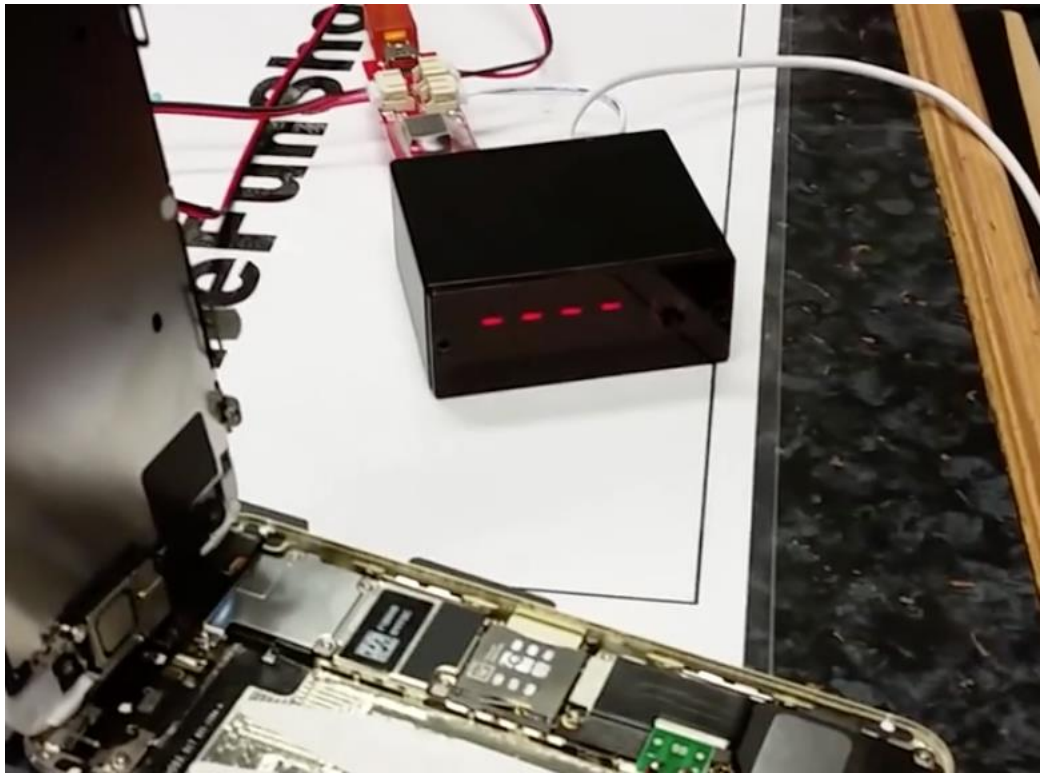
HTTP://BLOG.CELLEBRITE.COM/BLOG/2016/05/17/DISCOVER-BEST-PRACTICES-AND-ADVANCED-DECODING-WITH-UFED-PHYSICAL-ANALYZER-QA-FROM-CELLEBRITES-WEBINAR/

Q: Has Cellebrite been able to bypass the iOS pin on iPhones?

A: Cellebrite has the unique unlocking services provided by Cellebrite Advanced Investigative Services (CAIS). The current offering is for iOS 8 running on the iPhone 4S, 5, and 5c, as well as associated iPad and iPod touch models. The service helps investigators in important cases for which traditional mobile forensic tools do not have support. Ongoing efforts by our leading team of researchers is continuing for newer models and those running iOS 9. Please contact CAIS@cellebrite.com for more details.

IPHONE 4S E SUCCESSIVI – BLOCCATI E SPENTI
IOS 8 E NO CERTIFICATO DI LOCKDOWN





IPHONE 4S E SUCCESSIVI – BLOCCATI E SPENTI
IOS 9

- Se è un dispositivo a 32 bit…FBI? ☺
- Con gli strumenti e le tecniche note **non è possibile effettuare alcun tipo di acquisizione**
- Non sono note allo stato attuale tecniche di brute force o bypass del codice di blocco
- Si possono estrarre unicamente **le informazioni relative al dispositivo** (tool ideviceinfo)

MA MAI DIRE MAI….

India claims to have tool to defeat iPhone encryption

The country's communications and IT minister says the government has a forensics tool that can handle smartphones, including Apple's.

Phones

May 9, 2016
9:17 AM PDT

by Lance Whitney
@lancewhit

India allegedly has a secret technology to decrypt iPhones.

Ravi Shankar Prasad, India's communications and IT minister, said Friday that a tool for mobile forensics has been developed that can handle smartphones, including Apple's iPhone, according to the New Indian Express. Prasad didn't reveal details about how the tool works

The Indian government apparently has a way to handle

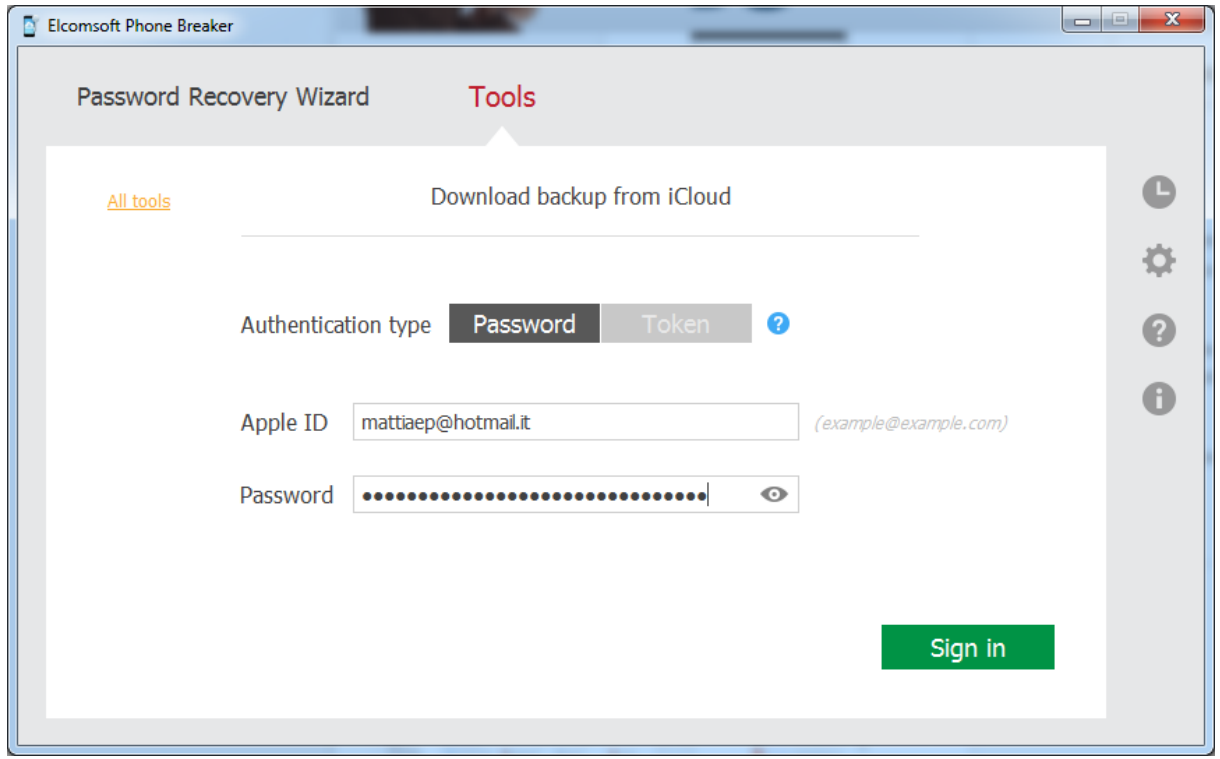
IPHONE 4S E SUCCESSIVI
JAILBREAKING

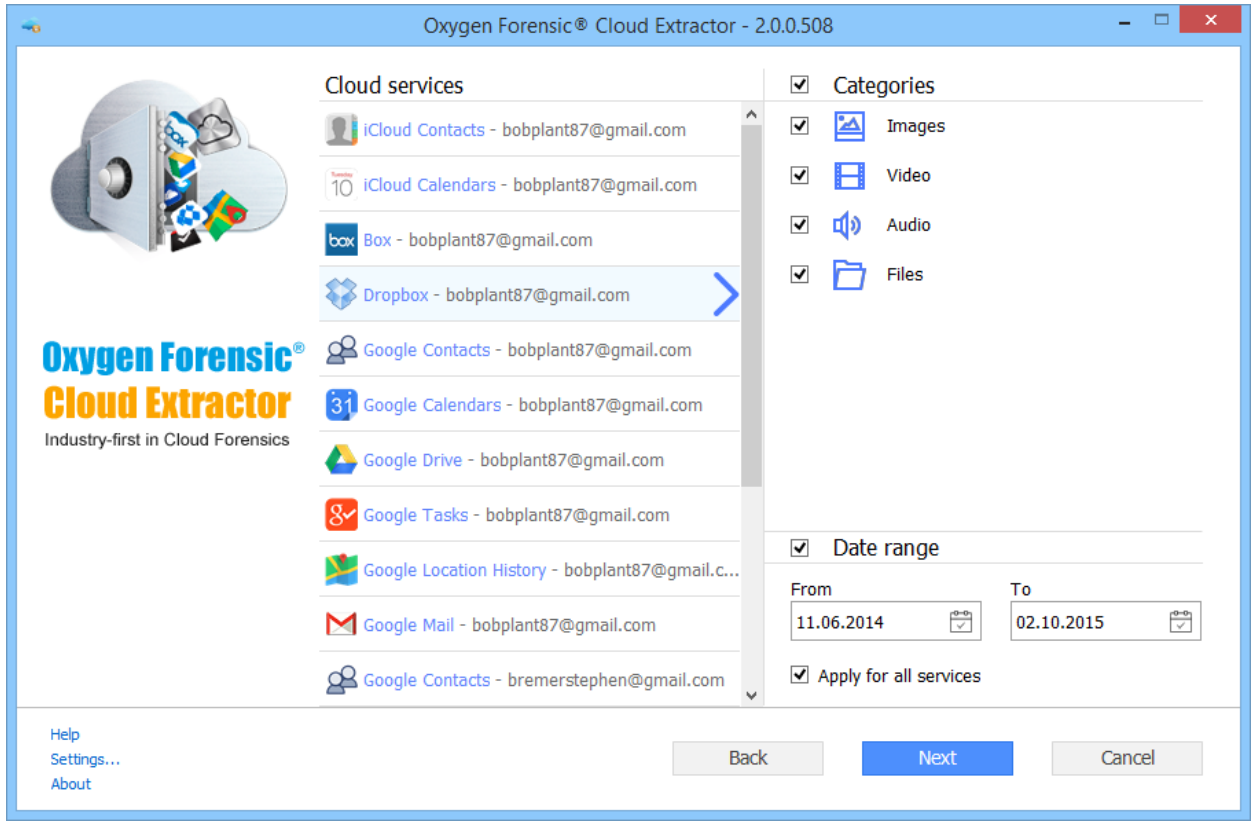
- Se il dispositivo non è protetto con un codice di blocco è possibile effettuare **jailbreak** e utilizzare **Elcomsoft iOS Forensic Toolkit**
- Possibile allo stato attuale fino a **iOS 9.1**
- Se il dispositivo è **protetto da un codice di blocco**, deve essere già stato precedentemente sottoposto a jailbreaking per poter effettuare una acquisizione
- **ATTENZIONE: IL JAILBREAKING E' UNA OPZIONE INVASIVA!**
- Perché prendere il rischio? Perchè alcune informazioni non sono disponibili in una acquisizione file system (es. **Email all'interno dell'applicazione native Mail**)

ACQUISIZIONE DA ICLOUD

- Se si hanno a disposizione le **credenziali dell'account iCloud associato al dispositivo** è possibile effettuare un accesso online per recuperare:
  - iCloud Device Backup
  - iCloud Calendars
  - iCloud Contacts
  - Photo Streams
  - Email
- Diversi software supportano questa funzionalità
- I migliori sono **Elcomsoft Phone Breaker** e **Oxygen Forensic Cloud Extractor**
- Il primo supporta anche **il recupero di Token da computer con installato iCloud Control Panel**
- Le attività di download sono trasparenti al proprietario dell'utente

ACQUISIZIONE DA ICLOUD





RICHIESTA DI SUPPORTO AD APPLE
HTTP://IMAGES.APPLE.COM/PRIVACY/DOCS/LEGAL-PROCESS-GUIDELINES-US.PDF

I. Extracting Data from Passcode Locked iOS Devices

For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions as data extraction tools are no longer effective. The files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

For iOS devices running iOS versions earlier than iOS 8.0, upon receipt of a valid search warrant issued upon a showing of probable cause, Apple can extract certain categories of active data from passcode locked iOS devices. Specifically, the user generated active files on an iOS device that are contained in Apple's native apps and for which the data is not encrypted using the passcode ("user generated active files"), can be extracted and provided to law enforcement on external media. Apple can perform this data extraction process on iOS devices running iOS 4 through iOS 7. Please note the only categories of user generated active files that can be provided to law enforcement, pursuant to a valid search warrant, are: SMS, iMessage, MMS, photos, videos, contacts, audio recording, and call history. Apple cannot provide: email, calendar entries, or any third-party app data.

The data extraction process can only be performed at Apple's Cupertino, California headquarters for devices that are in good working order. For Apple to assist in this process, the language outlined below must be included in a search warrant, and the search warrant must include the serial or IMEI number of the device. For more information on locating the IMEI and serial number of an iOS device, refer to http://support.apple.com/kb/ht4061.

RICHIESTA DI SUPPORTO AD APPLE
HTTP://IMAGES.APPLE.COM/PRIVACY/DOCS/LEGAL-PROCESS-GUIDELINES-US.PDF

- Si possono invece richiedere:
  - Subscriber information
  - Mail logs
  - Email content
  - Other iCloud Content (iOS Device Backups, Photo Stream, Docs, Contacts, Calendars, Bookmarks)
  - Find My iPhone
  - Game Center
  - iOS Device Activation
  - Sign-on logs
  - My Apple ID e 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.

SOFTWARE DI ACQUISIZIONE

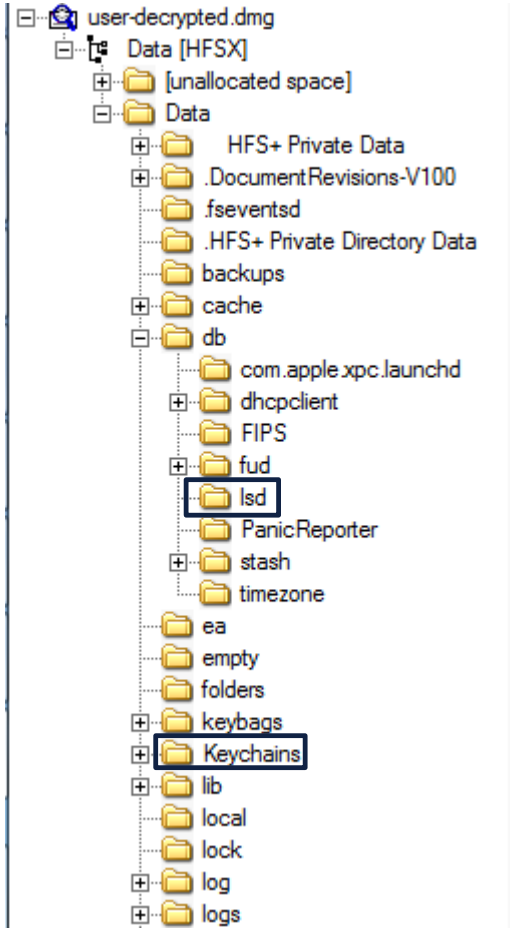
Forensic Tools

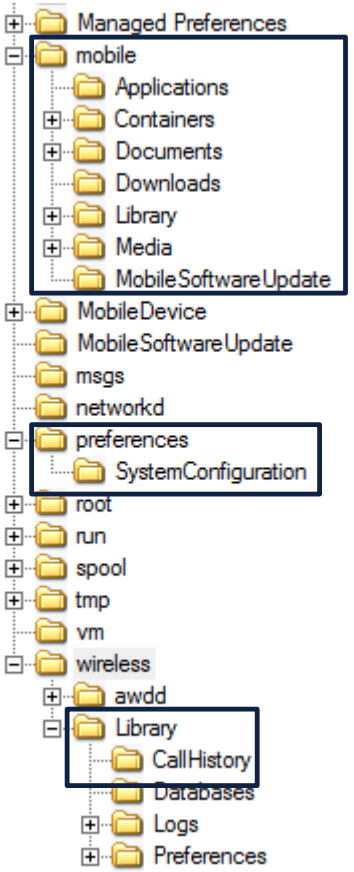
- Cellebrite Physical Analyzer
- MPE+
- XRY
- Oxygen
- Elcomsoft Phone Breaker
- Elcomsoft iOS Forensic Toolkit
- Magnet Acquire

Other tools

- iTunes
- Libimobiledevice
- iFunBox
- iTools
- iExplorer

ACQUISIZIONE FISICA VS BACKUP - DIFFERENZE





IOS BACKUP

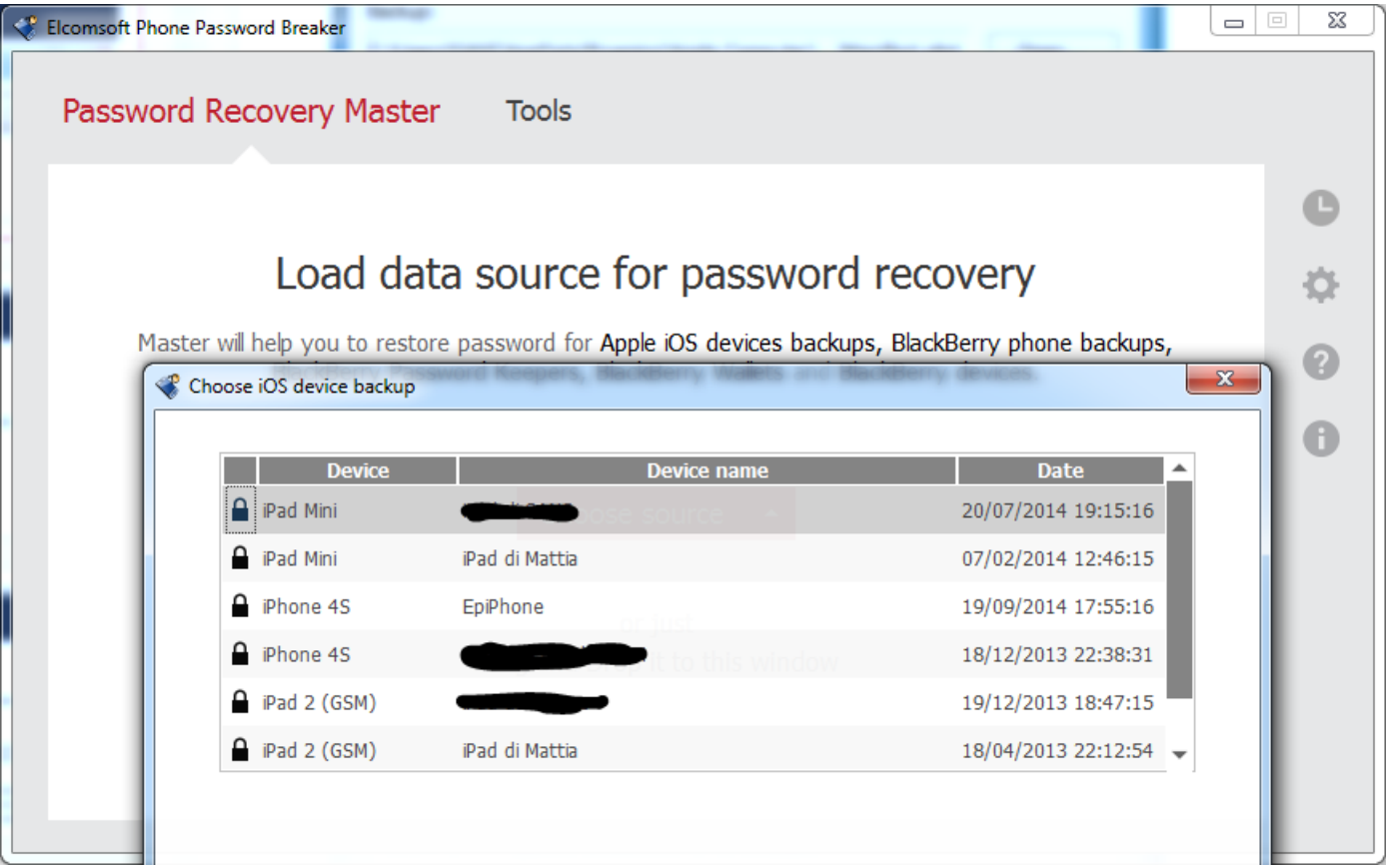
iTunes

- Windows e Mac OS X
- Manuale (USB) o automatico (Wi-Fi)
- Cifrato o non cifrato
- Windows 7/8/10:
  - \Users\<username>\AppData\Roaming\Apple Computer\Mobile Sync\Backup
- Mac OS X
  - /Users/<username>/Library/Application Support/MobileSynce/Backup

iCloud

- Salvato su server Apple
- Cifrato (ma solo con credenziali utente)
- Manuale e/o automatico quando il device è connesso alla corrente e in carica

BACKUP PROTETTI DA PASSWORD



COSA E' PRESENTE IN UN BACKUP?

Informazioni sul device
Account configurati
Reti Wi-Fi
Lingua
Timezone
Springboard

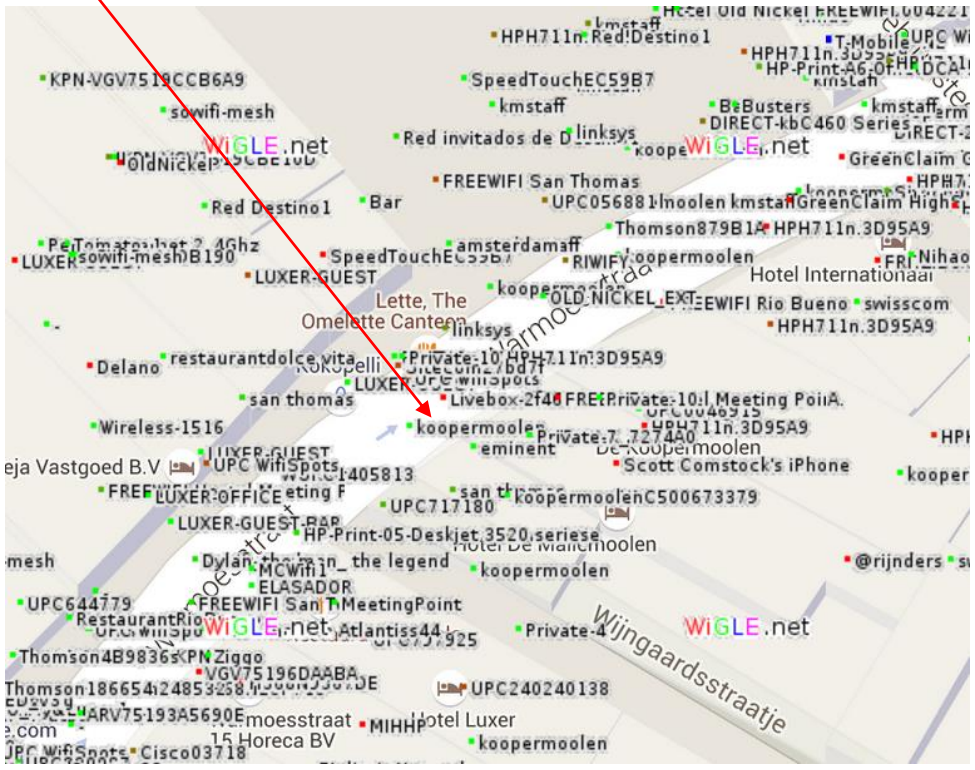
Rubrica
Registro Chiamate
Calendario
Note
SMS/MMS
Messaggi vocali/Voicemail

Foto e Video
Documenti
Safari (dati e configurazioni)
Mail (informazioni su account)
Mappe
Applicazioni di Terze Parti
Keychain (solo su backup cifrato)

RETI WI-FI

koopermoolen	ac:86:74:15:3f:a2	Device time: 16/05/2015 15:49:00 UTC: 16/05/2015 14:49:00
wifitoscane	ac:86:74:07:5b:1a	Device time: 15/05/2015 20:17:33 UTC: 15/05/2015 19:17:33
argentinos	2a:a4:3c:69:ae:18	Device time: 14/05/2015 19:17:09 UTC: 14/05/2015 18:17:09
RockPlanet	90:f6:52:83:24:d5	Device time: 13/05/2015 22:03:07 UTC: 13/05/2015 21:03:07
ibahn_conferencing	00:03:52:9f:95:21	Device time: 13/05/2015 07:13:41 UTC: 13/05/2015 06:13:41
The_Bulldog	c0:7b:bc:23:7e:30	Device time: 12/05/2015 22:09:54 UTC: 12/05/2015 21:09:54
lunaspot	ac:86:74:12:b9:2a	Device time: 12/05/2015 19:22:18 UTC: 12/05/2015 18:22:18
FREEWIFI Cafe The Pint	ee:94:f6:67:dc:81	Device time: 12/05/2015 00:23:03 UTC: 11/05/2015 23:23:03
moevenpick	e0:10:7f:21:af:78	Device time: 11/05/2015 19:19:28 UTC: 11/05/2015 18:19:28
FREEWIFI Cocos Likes Tjiller	c6:4a:00:e4:51:cf	Device time: 10/05/2015 17:42:54 UTC: 10/05/2015 16:42:54
Hotel Fita 01	00:02:6f:55:86:6f	Device time: 10/05/2015 08:46:29 UTC: 10/05/2015 07:46:29

Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long
AC:86:74:15:3F:A2	koopermoolen		infra	2014-02-09 13:47:51	2015-02-14 00:21:03		52.37617874	4.89931870



PASSWORD MEMORIZZATE

- Il **file keychain** memorizza le password del WiFi, della e-mail e delle applicazioni di terze parti
- Se il backup è **non cifrato** → Il file keychain è cifrato utilizzando una chiave hard-coded nel dispositivo
- Se il backup è **cifrato** → Il file keychain è cifrato utilizzando la password scelta dall'utente
- Se l'utente **non ha impostato una password di backup** allora possiamo effettuare il backup con una password nota e accedere alle password memorizzate nel dispositivo
- Se l'utente **ha impostato una password sul backup** allora possiamo fare un attacco sulla password

SOFTWARE DI ANALISI

Commerciali

- Cellebrite Physical Analyzer
- MPE+
- XRY
- Oxygen
- Elcomsoft Phone Viewer
- Elcomsoft Explorer WhatsApp
- Internet Evidence Finder
- X-Ways/FTK/Encase

Open/Free/Trial

- iBackupbot
- iPhone Backup Extractor
- iExplorer
- iPhone Backup Analyzer

IOS ANTI FORENSICS IN 8 PASSI

1. Se possedete un iPhone 4 o precedenti, **cambiatelo immediatamente**
2. Se possedete un iPhone 4s o successivi, **aggiornate all'ultima versione disponibile del sistema operativo e impostate un codice di accesso**
3. **Autorizzate un computer solamente se necessario** (es. per effettuare un backup)
4. **Non autorizzate l'accoppiamento con computer non di vostra proprietà** o sotto il vostro controllo
5. **Rimuovere periodicamente i certificati di lockdown** dai computer utilizzati per sincronizzare il telefono
6. Se decidete di fare backup in locale, **impostate una password molto forte**
7. Se decidete di fare backup su iCloud, **scegliete una password molto forte per il vostro account**
8. **Non effettuate jailbreaking**. E se proprio volete/dovete farlo, modificate la password di root scegliendone una molto forte

Q&A?

Mattia Epifani

- Digital Forensics Expert
- CEO @ REALITY NET – System Solutions
- CLUSIT, DFA, IISFA, ONIF, Tech and Law Center
- GCFA, GREM, GNFA, GMOB
- CEH, CHFI, CCE, CIFI, ECCE, AME, ACE, MPSC

Mail	**mattia.epifani@realitynet.it**
Twitter	**@mattiaep**
Linkedin	**http://www.linkedin.com/in/mattiaepifani**
Web	**http://www.realitynet.it**
Blog	**http://blog.digital-forensics.it**