



Dammi il tuo iPhone  
e ti dirò chi sei (forse...)

HACKINBO

23 MAGGIO 2015

MATTIA EPIFANI



## Chi sono, perché sono qui e perché stasera non sarò a cena con voi

- ▶ Mattia Epifani
- ▶ Laurea in Informatica, Socio di REALITY NET, Consulente informatico forense
- ▶ Appassionato e umile sperimentatore di tecnologie informatiche
- ▶ (in ordine alfabetico) Socio di CLUSIT, DFA, IISFA, ONIF e T&L
- ▶ L'amico Mario mi ha dato la possibilità di parlare a questo evento, che considero tra i più «stimolanti» a livello nazionale
- ▶ Quando mi ha invitato (settembre 2014) ho accettato con entusiasmo all'idea di fare una «due giorni» teorico-pratica su un argomento a me caro
- ▶ Ma a un giorno all'improvviso...

# Genoa Cricket and Football Club 1893

## Il club più antico d'Italia

- Un giorno all'improvviso mi innamorai di te  
il cuore mi batteva  
non chiedermi perché  
di tempo ne è passato  
ma siamo ancora qua  
e oggi come allora  
io tifo Genoa



# Digital Forensics

- ▶ Non voglio tediarvi con le classiche definizioni di «digital forensics»
- ▶ Ma solo pochi concetti fondamentali:
  - ▶ Garantire **autenticità e affidabilità dei dati** (ove possibile con ripetibilità delle operazioni)
  - ▶ **Scientificità** in tutte le fasi di gestione della «evidenza»
  - ▶ Conoscere i limiti della tecnologia e saper scegliere la **migliore soluzione per il caso in esame**, ove necessario rendendo partecipi tutte le parti in causa



# Digital Forensics e dispositivi mobile

- ▶ Documenti di riferimento:
  - ▶ Guidelines on Mobile Device Forensics, NIST, 2014
  - ▶ Developing Process for Mobile Device Forensics, Murphy, 2014
- ▶ Conservazione della sorgente
  - ▶ Isolamento dalle reti
  - ▶ Spegnimento (non sempre consigliabile, come vedremo...)
  - ▶ Packaging
  - ▶ Trasporto
- ▶ Identificazione
- ▶ Acquisizione
- ▶ Analisi

# Digital Forensics e dispositivi mobile

- ▶ Obiettivo: garantire la migliore acquisizione possibile in funzione della tipologia di informazioni che si stanno ricercando
- ▶ Cosa vuol dire «migliore»?
  - ▶ Quella più a basso livello?
  - ▶ Quella che mi riporta sempre e comunque più informazioni?
  - ▶ Quella meno invasiva?
  - ▶ Quella meno rischiosa?
- ▶ La risposta NON è universale: l'approccio da seguire è quello di valutare, caso per caso, come comportarsi

# Apple e iPhone

- ▶ L'ingresso di Apple nel mercato «mobile» nel 2007 ha totalmente rivoluzionato il concetto di telefono cellulare
- ▶ Da allora, in un tempo relativamente breve, sono stati immessi sul mercato
  - ▶ 10 modelli
  - ▶ 8 versioni del sistema operativo
- ▶ Inoltre iPad, iPod Touch, Apple TV, Apple Watch
- ▶ Allo stato attuale, insieme ad Android, domina il mercato mobile (smartphone e tablet)
- ▶ Per questo motivo è uno dei dispositivi che maggiormente si analizzano durante le investigazioni digitali

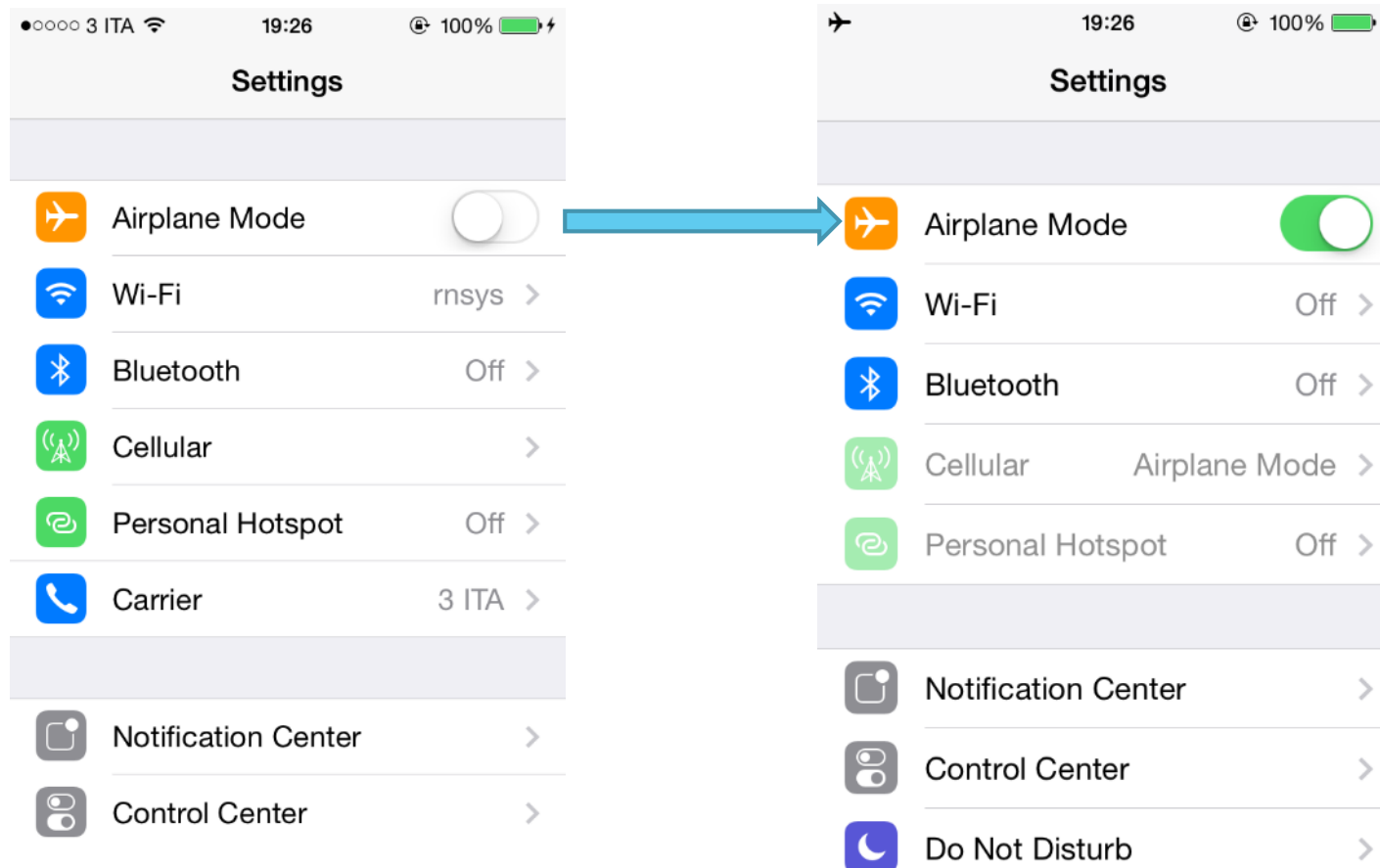
# Conservazione e Identificazione

- ▶ Distinguiamo due casi:
  - ▶ Dispositivo spento
    - ▶ Lo lasciamo spento
  - ▶ Dispositivo acceso
    - ▶ Posso attivare la modalità aerea?
    - ▶ Che modello è?
    - ▶ E' bloccato con un codice di blocco?
    - ▶ Il codice di blocco è semplice o complesso?



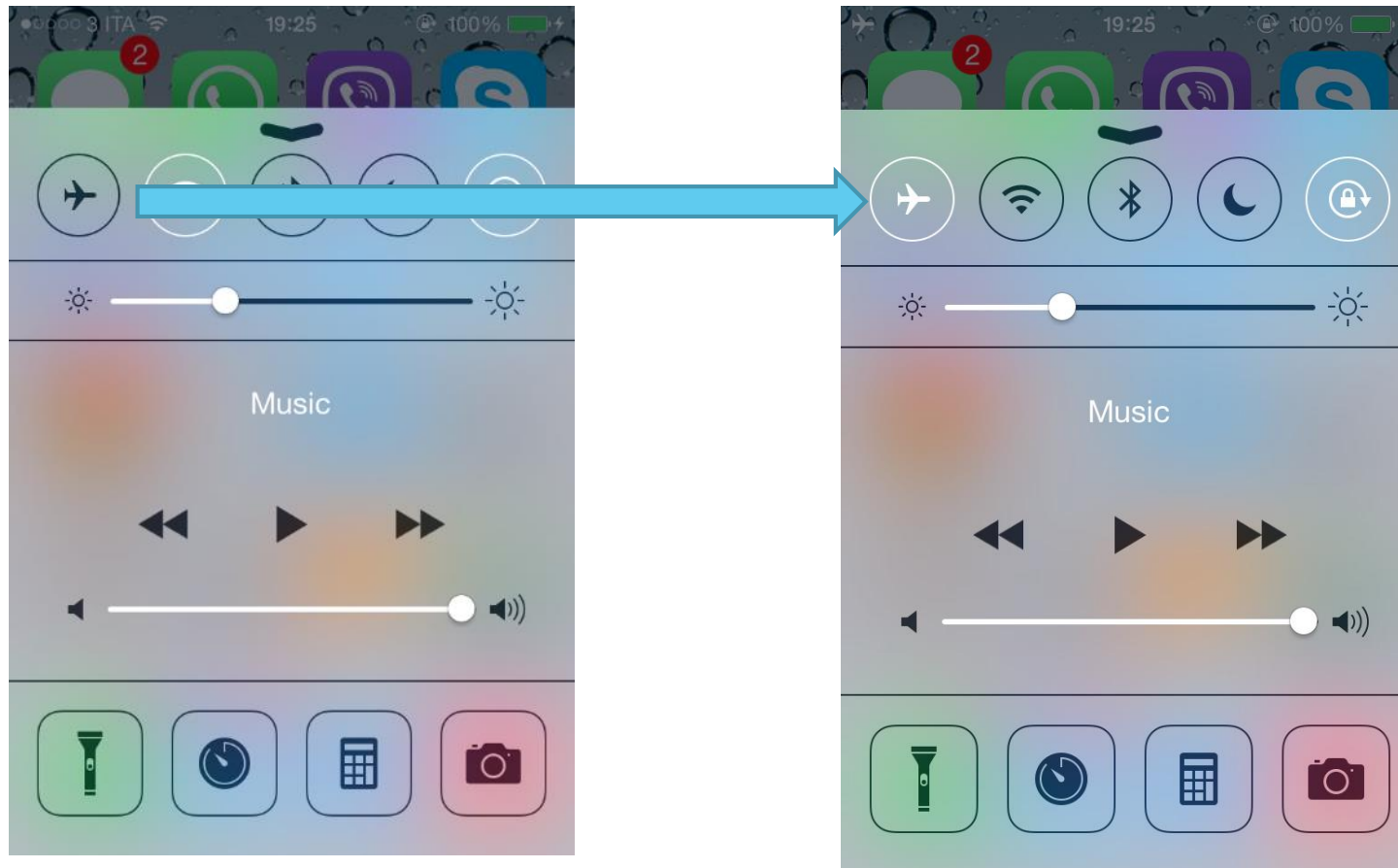
# Attivazione modalità aerea

- ▶ Se possibile lo mettiamo subito in modalità aerea
  - ▶ Dispositivo sbloccato



# Attivazione modalità aerea

- ▶ Se possibile lo mettiamo subito in modalità aerea
  - ▶ Dispositivo bloccato



# Identificazione del modello

- La strada più semplice: guardo il numero del modello sul retro del dispositivo



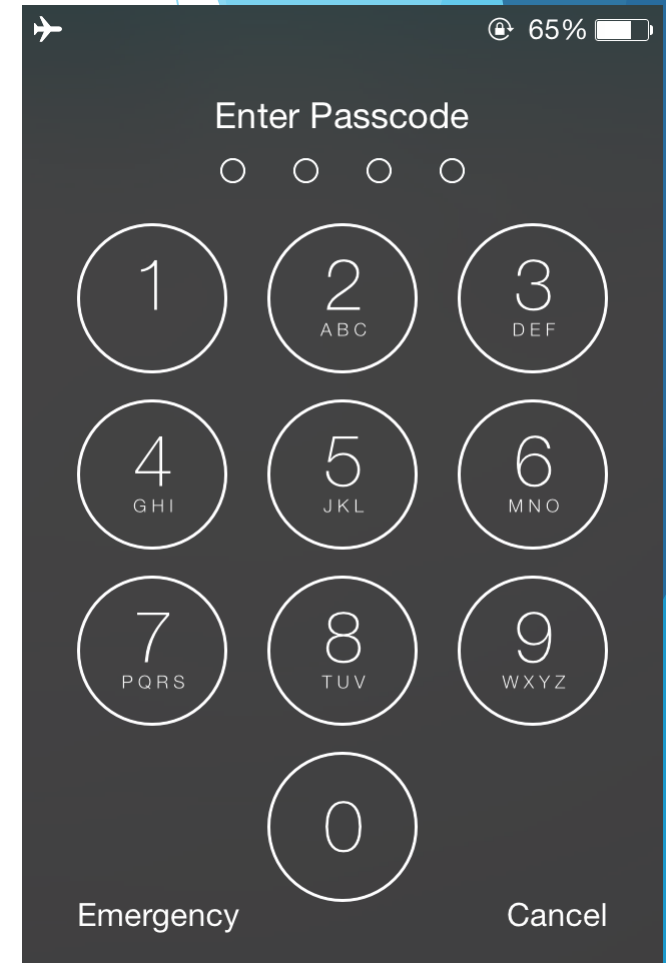


# Identificazione del modello

Device name	Model number	Internal Name	Identifier	Year	Capacity (GB)
iPhone 6 Plus	A1522 - A1524	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

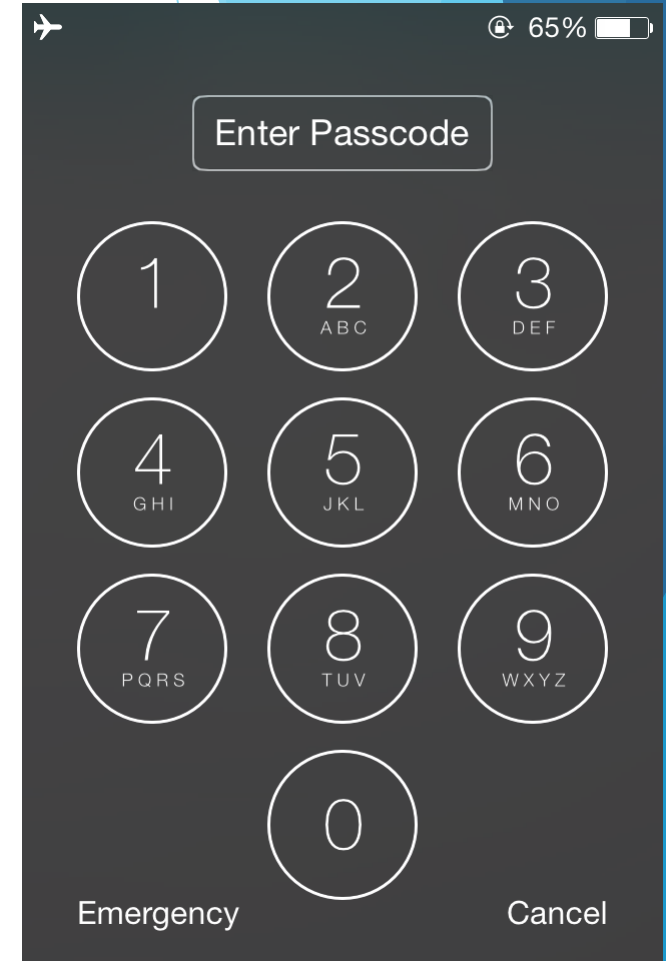
# E' bloccato con un codice?

- Solo numeri
- Lunghezza = 4 (passcode semplice)



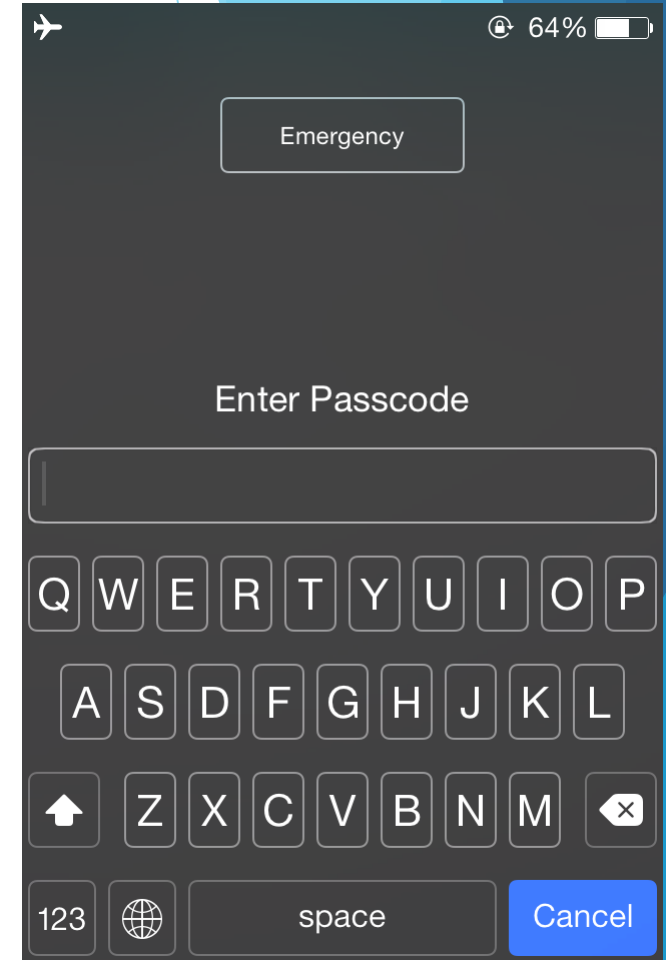
# E' bloccato con un codice?

- Solo numeri
- Lunghezza > 4  
(passcode complesso)



# E' bloccato con un codice?

- Alfabetico
- Lunghezza non nota



# Tipologie di acquisizione

- ▶ Fisica
  - ▶ Copia bit-a-bit della memoria interna
  - ▶ Possibile solo in determinate condizioni
- ▶ File System
  - ▶ Estrazione di (parte del) file system
  - ▶ Possibile attraverso 2 modalità:
    - ▶ iTunes Backup  
[NOTA - Potrebbe essere protetto da password]
    - ▶ Lockdown Services / Apple File Conduit



## Fino a iPhone 4...

- ▶ Acquisizione fisica sempre possibile e basata su exploit a livello di bootrom
- ▶ **Indipendentemente dalla presenza di un codice di blocco**
- ▶ Accesso a tutti i contenuti se il dispositivo:
  - ▶ Non è bloccato
  - ▶ E' bloccato con un codice che può essere violato in un «tempo ragionevole»
- ▶ **Altrimenti**
  - ▶ Non è possibile accedere ai contenuti cifrati con il passcode (es. email)
  - ▶ Ma possiamo accedere i dati di molte applicazioni (es. rubrica, SMS, immagini, video, navigazione Internet, ecc.)

# Quanto tempo ci vuole? (iPhone 4)

	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

# Dopo iPhone 4 - Dispositivi senza codice

- ▶ Non sono note vulnerabilità a livello di bootrom e quindi l'acquisizione fisica (non invasiva) non è possibile
- ▶ Dobbiamo quindi valutare le possibilità di acquisizione in funzione della presenza o meno del codice
- ▶ Se il dispositivo è **sbloccato** possiamo **sempre effettuare acquisizione di parte del file system** utilizzando una delle tecniche sopra descritte
- ▶ Tipicamente realizzata attraverso
  - ▶ Software forense
    - ▶ UFED Cellebrite, Oxygen Forensics, XRY, AccessData MPE+, Mobil Edit, ...
  - ▶ Backup con iTunes e analisi del backup
  - ▶ iDevice Browsing Tools **[ATTENZIONE! → Modalità lettura/scrittura]**
    - ▶ iFunBox, DiskAid, iExplorer

## Dopo iPhone 4 - Dispositivi con codice e accesi

- ▶ Se il dispositivo è **bloccato** ed è **stato rinvenuto acceso** la migliore modalità è la seguente:
  - ▶ Verificare la versione del sistema operativo installata
  - ▶ Verificare se nell'ambito dell'attività di sequestro è presente un computer utilizzato almeno una volta per collegare il telefono (es. per fare un backup, scaricare le foto, ecc.)
  - ▶ Estrarre il certificato di sincronizzazione [Lockdown]
  - ▶ Copiare il certificato di sincronizzazione all'interno di un computer con installato iTunes o un software forense
  - ▶ Effettuare una acquisizione mediante backup
- ▶ Questo significa **operare direttamente sul dispositivo durante il sequestro per prevenire l'impossibilità di estrarre i dati**

# Verifica del sistema operativo

- ▶ Avviare il PC con una distribuzione forense che contenga **libimobiledevice**
  - ▶ Santoku (<https://santoku-linux.com/>)
  - ▶ DEFT (<http://www.deftlinux.net/it/>)
- ▶ Accendere il telefono e collegarlo al computer
- ▶ Eseguire il comando **ideviceinfo -s**
- ▶ Funziona anche con dispositivi bloccati

# ideviceinfo -s

```
santoku@santoku: ~/Desktop
File Edit Tabs Help
santoku@santoku:~/Desktop$ ideviceinfo -s
BasebandCertId: 2
BasebandKeyHashInformation:
  AKeyStatus: 2
  SKeyHash: 7MQEUyvzG4gjjZc7KsNNAVTS8g4=
  SKeyStatus: 0
BasebandSerialNumber: JxnwkQ==
BasebandVersion: 5.2.00
BoardId: 8
BuildVersion: 11D201
ChipID: 35136
DeviceClass: iPhone
DeviceColor: black
DeviceName: EpiPhone
DevicePublicKey: LS0tLS1CRUdJTiBSU0EgUFVCTELDIETFS0tLS0tCk1JR0pBb0dCQUtHUjZMOUM
weE56dlhaNmdQd3hleUF1RUJGUjlQYm1mUmlNdTlvaDliOWppZXJpVVFYWnVFTE4KampZew0zVVQvbnd
Za0hN0FhsVWx2YUJtMWdJS2NveWlyOE5JbVd3S2N5ak4lb2pEbDE5NnJhWlBqUmZEVVJXYQpsUXVUUC8
4SDZTRFJ2N0NianU20Eg0MFJocURJY1Njbi9oUXAvd2s5Q2IydHdxWlFpQnNKQWdNQkFBRT0KLS0tLS1
FTkQgUlnBIFBVQkxJQyBLRVktLS0tLQo=
DieID: 2242306697049237152
HardwareModel: N94AP
PartitionType:
ProductVersion: 7.1.1
ProductionSOC: true
ProtocolVersion: 2
TelephonyCapability: true
UniqueChipID: 3491071820683
UniqueDeviceID: 26ccdbcb74b2ab8e9e97aa096883a10442c6f2ef
WiFiAddress: 84:fc:fe:d3:ac:e2
santoku@santoku:~/Desktops
```



# Certificati di 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 → **DeviceUDID.plist**



## Dopo iPhone 4 - Dispositivi con codice e spenti

- ▶ Se il dispositivo è stato invece rinvenuto spento oppure, come nella maggior parte dei casi, vi viene consegnato spento dobbiamo distinguere ulteriori tre casi
  - ▶ Abbiamo un certificato di lockdown e la versione del sistema operativo è fino ad iOS 7.1.2
  - ▶ Non abbiamo un certificato di lockdown e la versione del sistema operativo è fino ad iOS 8.0.3
  - ▶ Abbiamo un certificato di lockdown e la versione del sistema operativo è compresa tra iOS 8.0.1 e iOS 8.3
  - ▶ Non abbiamo un certificato di lockdown e la versione del sistema operativo è compresa tra iOS 8.1 e 8.3





## Sistema operativo iOS 7 e certificato di lockdown

- ▶ Posso copiare il certificato nella macchina di acquisizione, anche se il dispositivo è stato spento, ed effettuare una acquisizione mediante i servizi di lockdown
- ▶ 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>
- ▶ Funziona anche se l'utente ha impostato una password di backup
- ▶ UFED Cellebrite e Oxygen Forensics supportano questo tipo di acquisizione

# Sistema operativo è iOS 7 - No lockdown

- ▶ **IP-BOX**
- ▶ Strumento hardware che **trasmette il codice al device via USB**
- ▶ Il «successo» è basato sul cambio cromatico che si registra sul dispositivo nel momento in cui il codice corretto viene inserito
- ▶ Altri aspetti interessanti:
  - ▶ Funziona anche se il telefono è disabilitato
  - ▶ Posso inviare un codice direttamente da un computer (es. schermo guasto)
- ▶ Testato personalmente in queste condizioni:
  - ▶ iPhone 4s bloccato e non disabilitato
  - ▶ iPhone 4s bloccato e disabilitato
  - ▶ iPhone 4s bloccato e con tastiera guasta

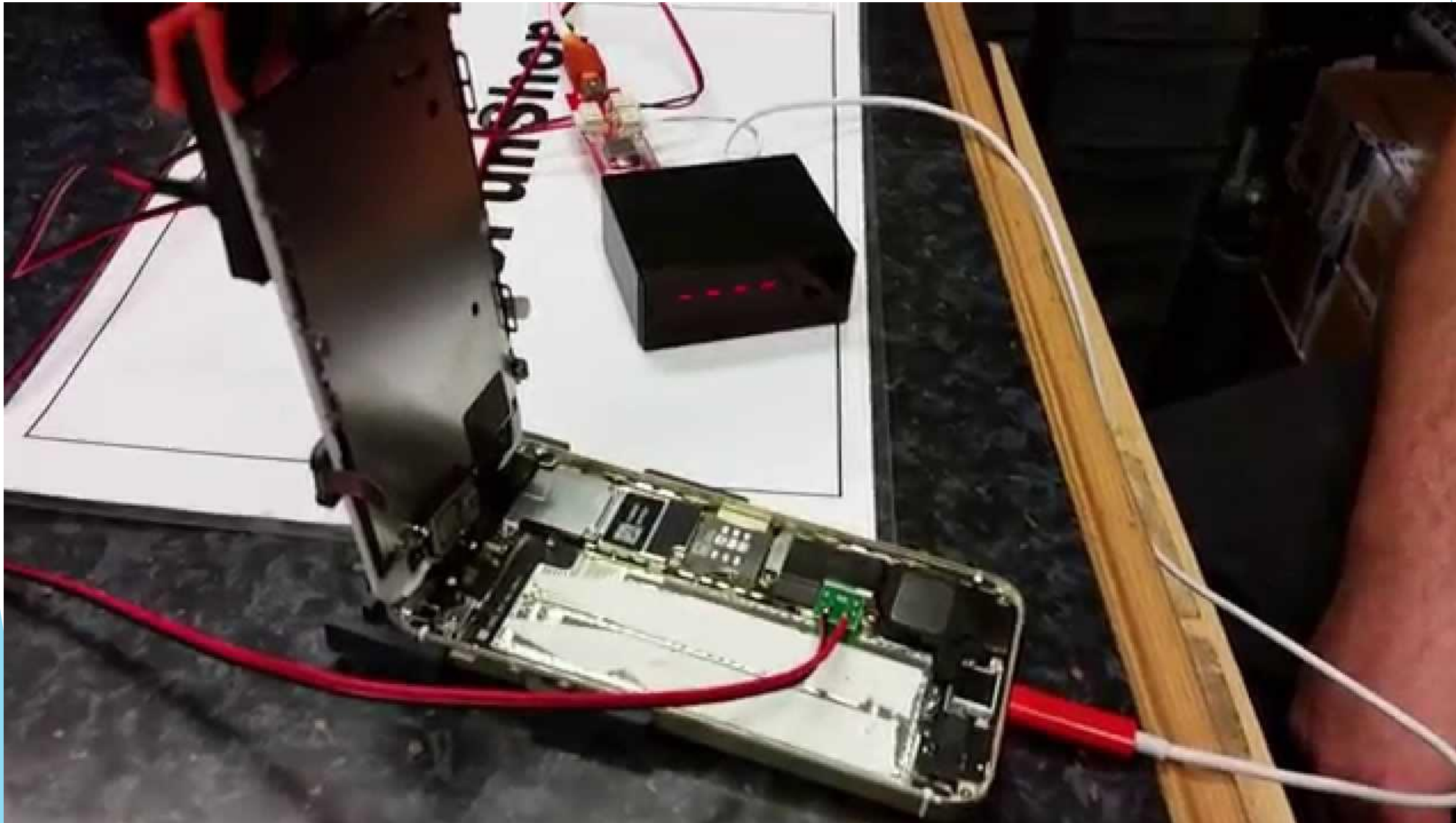


# IP BOX

- ▶ **ATTENZIONE!**
- ▶ Non è uno strumento «forense»
- ▶ Sono stati riportati casi in cui il dispositivo è stato wipato poiché era attiva la cancellazione sicura dopo 10 tentativi
- ▶ Nei test da me effettuati non si è mai verificato
- ▶ Per contro...esiste anche un hardware aggiuntivo che funziona fino ad **iOS 8.0.3**
- ▶ Prevede l'apertura del telefono e la connessione diretta alla **batteria**
- ▶ Ancora in fase di testing
- ▶ Per approfondimenti:
  - ▶ **iP-BOX: Breaking Simple Pass Codes on iOS Devices rev. 2**, Murphy, 2015

<http://www.teeltech.com/wp-content/uploads/2014/11/IP-Box-documentation-rev2-1-16-2015.pdf>

Se il sistema operativo è iOS 8.0.3





## Se il sistema operativo è superiore a iOS 8.1

- ▶ Possibilità residuali...
- ▶ Fino a iOS 8.2, se il proprietario aveva effettuato jailbreaking senza modificare la password di root (default **alpine**) posso utilizzare **Elcomsoft iOS Forensic Toolkit** e fare **brute force del passcode**
- ▶ Se ho un certificato di lockdown posso ancora estrarre qualcosa attraverso il **protocollo AFC** e il servizio **lockdown**

	Fisica	File System No codice	File System Bloccato Accesso Si Lockdown	File System Bloccato Spento Si Lockdown iOS 7	File System Bloccato Spento No Lockdown iOS 7	File System Bloccato Spento No Lockdown iOS 8.0.1 - 8.0.3	File System Bloccato Spento Si Lockdown iOS 8.0.1 - iOS 8.3	File System Bloccato Spento No Lockdown iOS 8.1 - iOS 8.3
iPhone 6 Plus	No	Backup AFC/Lock	Backup AFC/Lock	N/A	N/A	IP BOX + Adapter	Lockdown parziale	Solo Informazioni device
iPhone 6	No	Backup AFC/Lock	Backup AFC/Lock	N/A	N/A	IP BOX + Adapter	Lockdown parziale	Solo Informazioni device
iPhone 5S	No	Backup AFC/Lock	Backup AFC/Lock	AFC/Lock	IP BOX	IP BOX + Adapter	Lockdown parziale	Solo Informazioni device
iPhone 5C	Jailbroken <iOS 8.3	Backup AFC/Lock	Backup AFC/Lock	AFC/Lock	IP BOX	IP BOX + Adapter	Lockdown parziale	Solo Informazioni device
iPhone 5	Jailbroken <iOS 8.3	Backup AFC/Lock	Backup AFC/Lock	AFC/Lock	IP BOX	IP BOX + Adapter	Lockdown parziale	Solo Informazioni device
iPhone 4S	Jailbroken <iOS 8.3	Backup AFC/Lock	Backup AFC/Lock	AFC/Lock	IP BOX	IP BOX + Adapter	Lockdown parziale	Solo Informazioni device
iPhone 4	Si	Backup AFC/Lock	Backup AFC/Lock	AFC/Lock	N/A	N/A	N/A	N/A
iPhone 3GS	Si	N/A	N/A	N/A	N/A	N/A	N/A	N/A
iPhone 3G	Si	N/A	N/A	N/A	N/A	N/A	N/A	N/A
iPhone 2G	Si	N/A	N/A	N/A	N/A	N/A	N/A	N/A



# Analisi

- ▶ In caso di acquisizione fisica sono disponibili tutti i contenuti se è stato possibile violare il passcode (o è noto o non impostato) altrimenti alcuni non sono disponibili (es. email)
- ▶ Nell'ipotesi di acquisizione file system la quantità e la tipologia di dati è fortemente influenzata dal metodo utilizzato e dallo stato del dispositivo
- ▶ In linea generale le informazioni di interesse sono memorizzate in:
  - ▶ File plist
  - ▶ Database SQLite

# Analisi

- ▶ **Applicazioni native** (Rubrica, SMS/MMS/iMessage, Note, Agenda)
- ▶ **Navigazione Internet** (Safari, Chrome, Opera, Mercury, Dolphin, Atomic)
- ▶ **Mail** (Apple Mail, Gmail, Yahoo, Hotmail)
- ▶ **Chat Messaging** (WhatsApp, Viber, Skype, Facebook Messenger, Yahoo Messenger, WeChat, Telegram, Kik, ChatOn, Tango, Snapchat, Silent Text, testPlus, Tiger Text, Zello, Voxer, ICQ, Hangouts, ooVoo, BBM, ...)
- ▶ **Social Network** (Facebook, Twitter, Linkedin, Instagram, Foursquare, Google+, YouTube, Tinder, Badoo, Find My Friends, ...)
- ▶ **Navigazione** (Apple Maps, Google Maps, Waze, Yandex, ...)
- ▶ **Produttività** (Dropbox, Google Drive, iBooks, Google Translate, Google Calendar, ...)
- ▶ **Viaggi** (Booking, Skyscanner, Tripadvisor, ...)
- ▶ **Dizionario utente**
- ▶ **Geolocalizzazione** (Conessioni a reti WiFi, metadati nelle immagini, utilizzo di applicazioni di navigazione, ecc.)
- ▶ **Password memorizzate**





# Reti WiFi

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

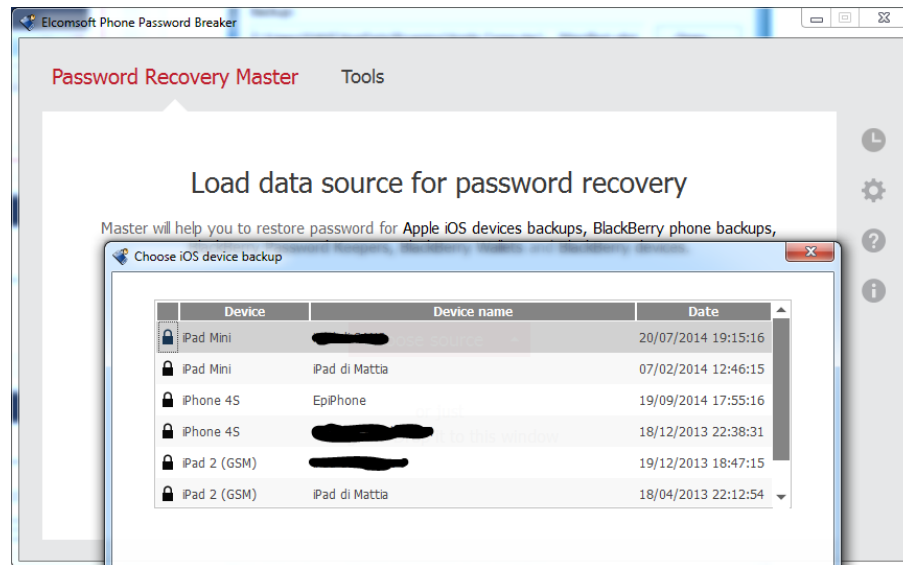


# Estrazione delle password memorizzate

- ▶ Il file **keychain** è utilizzato da iPhone per memorizzare le credenziali (username/password o certificato) di:
  - ▶ Reti WiFi
  - ▶ Indirizzi e-mail configurati nell'applicazione Mail
  - ▶ Password/certificati di applicazioni di terze parti
- ▶ Sul device il file keychain è cifrato con una chiave memorizzata nel dispositivo
- ▶ Se ho una acquisizione fisica, posso leggere questa chiave e quindi a decifrare il contenuto del keychain
- ▶ Il file keychain è presente anche all'interno del backup di iTunes
- ▶ Se il backup **non è protetto da password** → il file keychain file è cifrato utilizzando la chiave memorizzata nel dispositivo
- ▶ Se il backup è **protetto da password** → il file keychain è cifrato utilizzando la password scelta dall'utente

# Estrazione delle password memorizzate

- ▶ Se l'utente aveva già impostato la password → Posso provare a fare cracking
- ▶ Se l'utente non aveva impostato la password → Posso scegliere una password nota, fare un backup e decifrare il keychain!



# Si possono recuperare file cancellati?

- ▶ Il sistema di cifratura dei dati utilizzato da Apple è particolarmente complesso
- ▶ Non abbiamo il tempo per approfondirlo
- ▶ Ma è importante spiegare un concetto fondamentale:
  - ▶ Quando un file viene creato viene cifrato con una chiave di cifratura univoca contenuta nei metadati del file system HFSX (utilizzato da iPhone), in particolare nel file Catalog
  - ▶ Il file è quindi memorizzato su disco cifrato e viene decifrato «al volo» dal sistema operativo
  - ▶ Quando un file viene cancellato il record nel file Catalog viene sovrascritto, e con esso la chiave di cifratura
- ▶ Per questo motivo, anche avendo a disposizione una acquisizione fisica le **tecniche di file carving sullo spazio non allocato non sono applicabili**

# Si possono recuperare file cancellati?

- ▶ Tuttavia...qualche caso particolare:
  - ▶ Esiste una ricerca dimostrata su dispositivi iPhone 4 per il **recupero della chiave di cifratura utilizzando il file di Journal**
    - ▶ iOS Forensics: How can we recover deleted image files with timestamp in a forensically sound manner? (D'Orazio et. Al., 2013)
  - ▶ iOS 8 ha introdotto una nuova funzionalità per la quale **le foto cancellate sono conservate in un “cestino” per 30 giorni...per ora non tutti gli utenti sembrano esserene a conoscenza**
  - ▶ Nel caso delle immagini e dei video, analizzando le **thumbnails** è spesso possibile **recuperare le anteprime di file non più presenti**



# Si possono recuperare record cancellati?

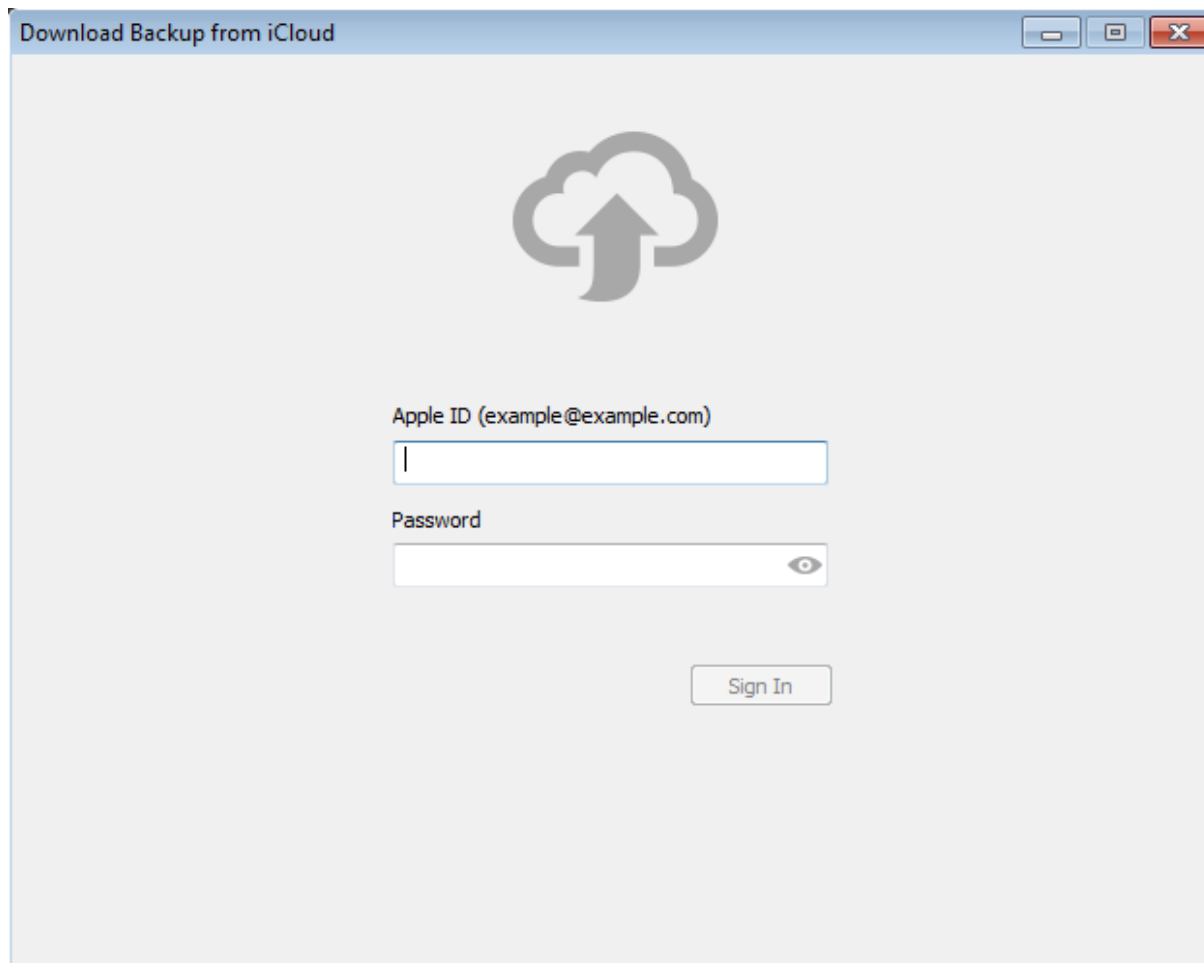
- ▶ Le informazioni memorizzate all'interno di database SQLite (la maggior parte, in iOS) e cancellate possono essere, sotto determinate condizioni, recuperate
- ▶ L'argomento è complesso e oggetto di costante studio
- ▶ Consiglio le letture di:
  - ▶ <http://sandersonforensics.com/forum/content.php?222-Recovering-deleted-records-from-an-SQLite-database>
  - ▶ [http://www.researchgate.net/publication/226423207\\_A\\_recovery\\_method\\_of\\_deleted\\_record\\_for\\_SQLite\\_database](http://www.researchgate.net/publication/226423207_A_recovery_method_of_deleted_record_for_SQLite_database)
- ▶ E l'utilizzo di:
  - ▶ Software forensi con questa funzionalità (UFED, Oxygen, ecc.)
  - ▶ SQLite Forensic Explorer
  - ▶ Undark
  - ▶ Sqlite Deleted Records Parser



## E i dati su iCloud?

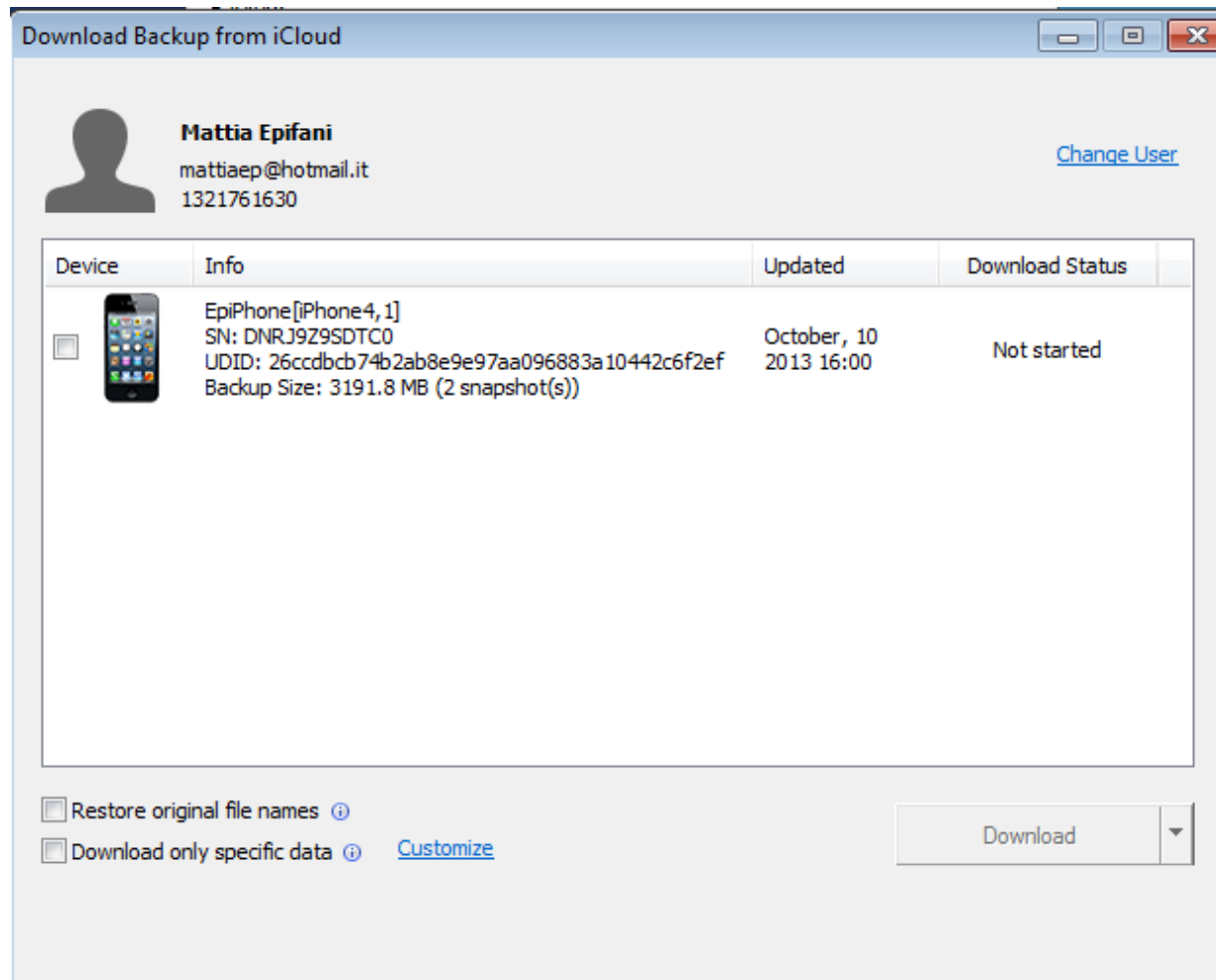
- ▶ Posso utilizzare software per l'accesso ai backup memorizzati su iCloud
  - ▶ Elcomsoft Phone Breaker (commerciale)
  - ▶ iloot (opensource)
- ▶ La procedura di estrazione delle password permette di ottenere le credenziali di iCloud in chiaro!
- ▶ Tecniche di bruteforce sugli account sono state utilizzate per il furto delle foto «sexy» delle star americane (The Fappening - [http://en.wikipedia.org/wiki/2014\\_celebrity\\_photo\\_hack](http://en.wikipedia.org/wiki/2014_celebrity_photo_hack))

# E i dati su iCloud?

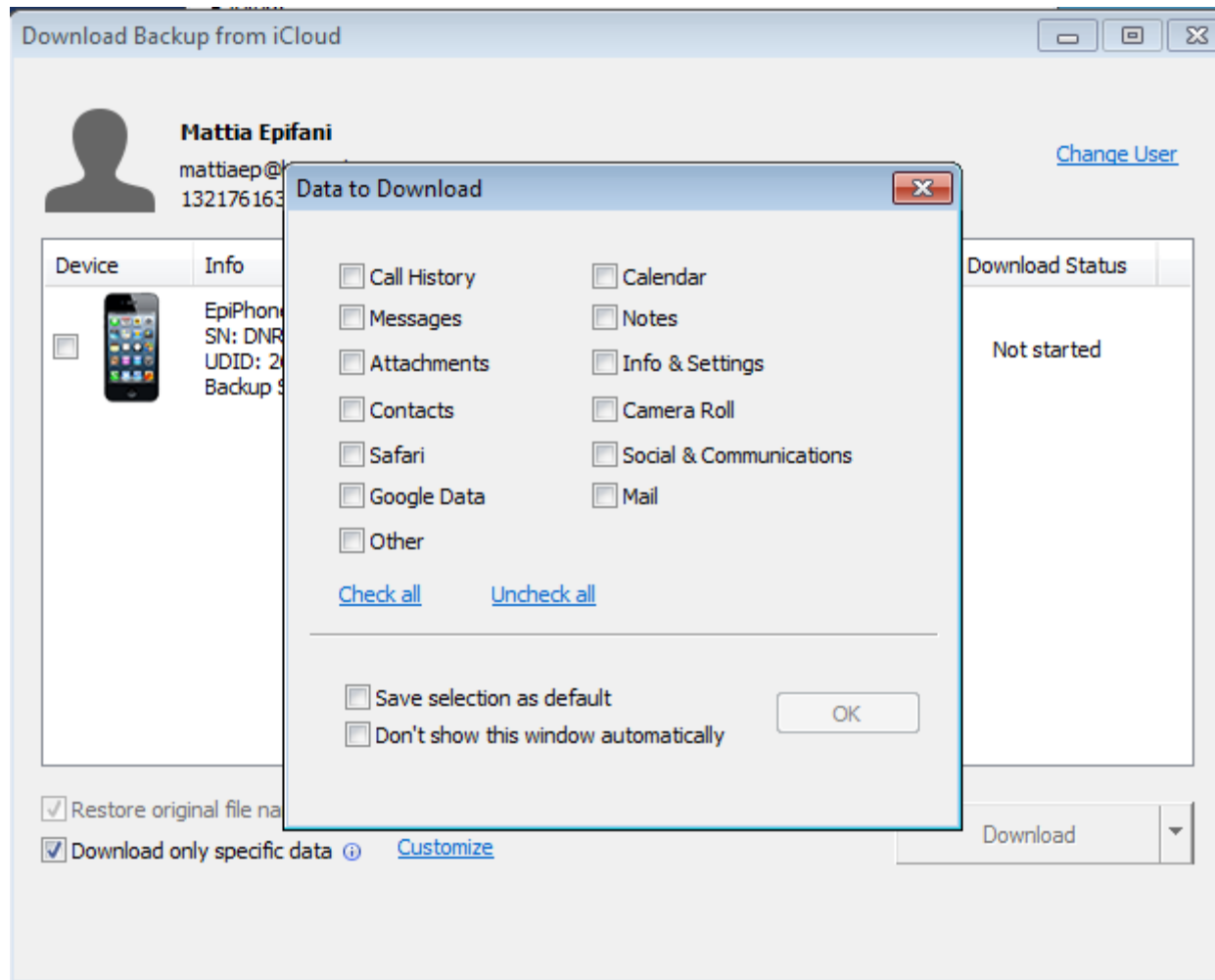
A screenshot of a web application window titled 'Download Backup from iCloud'. The window has a light gray background and a blue border. At the top, there is a title bar with standard window controls (minimize, maximize, close). Below the title bar, there is a large, stylized gray icon of a cloud with an upward-pointing arrow. Underneath the icon, there are two input fields. The first is labeled 'Apple ID (example@example.com)' and contains a single vertical line cursor. The second is labeled 'Password' and has a small eye icon to its right, indicating a password field. At the bottom center of the form, there is a button labeled 'Sign In'.



# E i dati su iCloud?



# E i dati su iCloud?





# Conclusioni - Ovvero 8 step per fregarci

1. Se avete un iPhone 4 o precedente, **cambiatelo subito!**
2. Se avete un iPhone 4s
  1. **Aggiornate ad iOS 8.3**
  2. **Impostate un passcode semplice**
3. **Autorizzate/accoppiate il vostro computer solo se è strettamente necessario (es. per fare un backup)**
4. Periodicamente (mio suggerimento: ogni volta che avete finito l'azione per la quale avete autorizzato l'accoppiamento) **rimuovete con cancellazione sicura il certificato di lockdown dal vostro computer**
5. **Non autorizzate/accoppiate nessun altro computer che non sia vostro**
6. Se effettuate un backup locale, **scegliete una password estremamente complessa**
7. Se effettuate un backup su iCloud (se proprio non ne potete fare a meno...) **scegliete una password estremamente complessa per il vostro account**
8. **Non fate jailbreaking oppure, se lo volete fare, modificate la password di root**

# Q&A

## Mattia Epifani

- ▶ Digital Forensics Analyst  
Mobile Device Security Analyst
- ▶ CEO @ REALITY NET - System Solutions
- ▶ Autore del libro Learning iOS Forensics
- ▶ Socio CLUSIT, DFA, IISFA, ONIF, Tech and Law Center
- ▶ GREM, GCFA, GNFA, GMOB, CEH, CHFI, CCE, CIFI, ECCE, AME, ACE, MPSC

Mail [mattia.epifani@realitynet.it](mailto:mattia.epifani@realitynet.it)  
Twitter [@mattiaep](https://twitter.com/mattiaep)  
Linkedin <http://www.linkedin.com/in/mattiaepifani>  
Blog <http://mattiaep.blogspot.com>

