Tracce digitali all'interno di Smartphone e Tablet

3 Maggio 2013

Università degli Studi di Camerino
Dott. Mattia Epifani
mattia.epifani@digital-forensics.it

Chi sono

- Mattia Epifani
- Digital Forensics Specialist
- Socio della REALITY NET – System Solutions
- Responsabile formazione IISFA (International Information Systems Forensics Association) Italian Chapter
- Presidente associazione DFA (Digital Forensics Alumni)
- Certificato CIFI, CHFI, CEH, CCE, ACE, AME, ECCE, MPSC

Cosa vedremo

- Definizione di Digital Forensics e Digital Evidence
- Identificazione, isolamento e repertamento di dispositivi *mobile*
- Acquisizione di SIM Card
- Acquisizione della memoria interna (logica e/o fisica)
- Case study: iPhone/iPad

Digital Forensics

*La **Digital Forensics** (**Informatica Forense**) è la scienza che studia l'**individuazione**, la **conservazione**, la **protezione**, l'**estrazione**, la **documentazione** e ogni altra forma di trattamento del dato informatico per essere valutato in un processo giuridico e studia, ai fini probatori, le **tecniche e gli strumenti per l'esame metodologico dei sistemi informatici***

Digital Evidence

- Una **digital evidence** può essere definita come **qualsiasi informazione avente valore probatorio che sia memorizzata o trasmessa in forma digitale**
- Una digital evidence può quindi essere estratta da:
  - Un **dispositivo di memorizzazione digitale**
    - Personal computer, notebook, hard disk esterno, NAS, floppy, nastro, CD/DVD, memory card, USB drive,…
    - **Telefoni cellulari, SIM, SmartPhone, Tablet, Navigatori satellitari**,…
  - Una **Rete Intranet/Internet**
    - Intercettazione di traffico dati
    - Pagine Web, Blog, Social Network, Chat/IM, P2P, ecc.

Digital Evidence

- Una **digital evidence** è **fragile per natura**, ovvero facilmente modificabile
  - Se il dispositivo che contiene le informazioni di interesse **viene spento**, i dati che non sono stati salvati possono andare definitivamente persi
  - Se il dispositivo viene rivenuto spento, **l'accensione comporta modifiche al sistema e/o ai dati in esso contenuti**
  - Se il dispositivo è connesso ad Internet o ad una rete aziendale, **possono avvenire accessi dall'esterno con l'obiettivo di cancellare le informazioni**

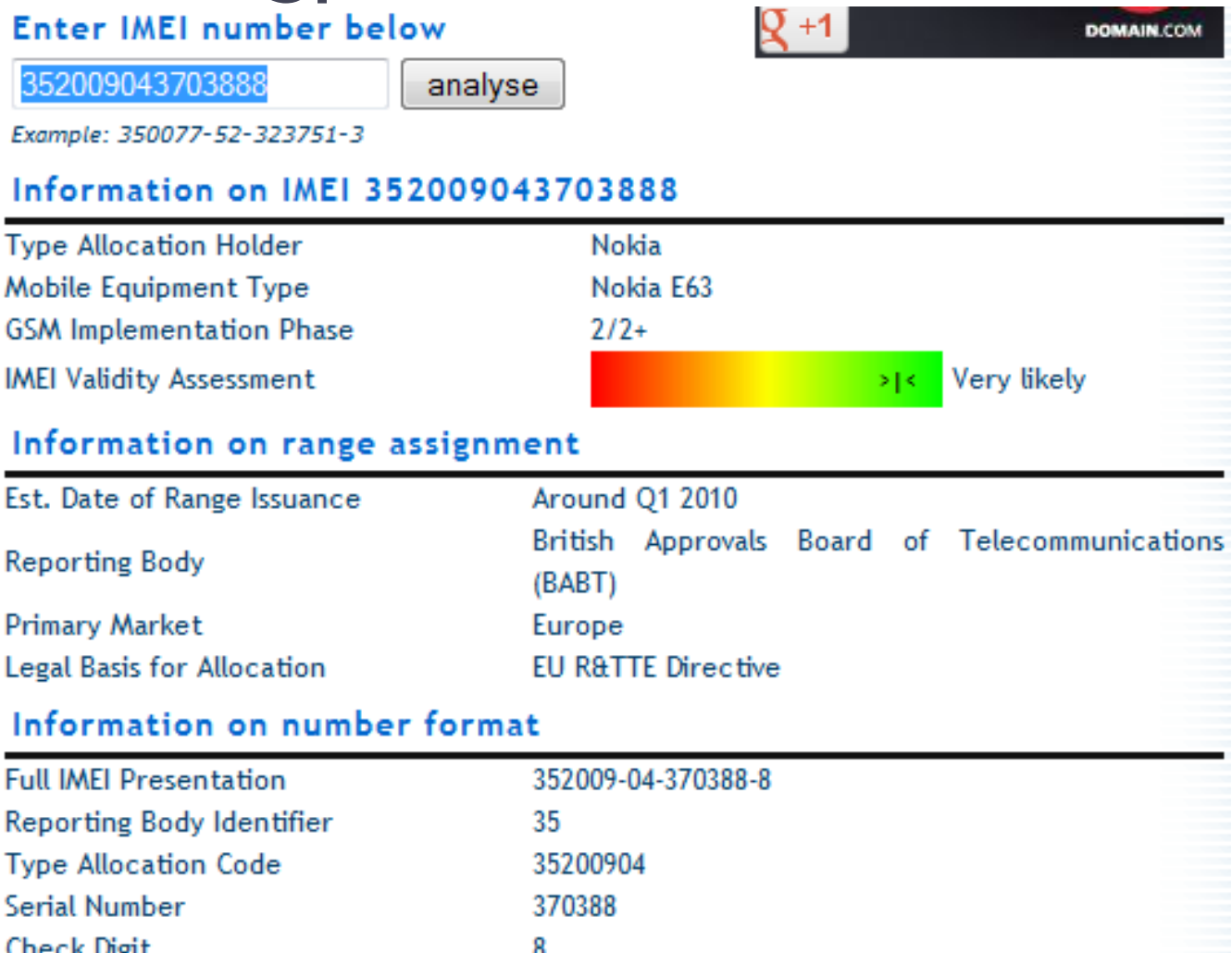
Passi operativi

- **Identificazione e repertamento**
- Acquisizione e verifica
- Conservazione
- Analisi
- Valutazione e presentazione

IMEI

- I terminali radiomobili GSM sono caratterizzati da un **codice di quindici cifre** detto **International Mobile Equipment Identifier (IMEI)**, che viene utilizzato per identificare il dispositivo all'interno della rete cellulare
- Tale codice **rappresenta in maniera univoca la casa costruttrice, il modello e la nazione in cui il terminale è stato prodotto**
- **Se il dispositivo è spento, le informazioni si trovano solitamente sotto la batteria o sul retro dello stesso**
- **Se il dispositivo è acceso, è possibile identificarne il suo IMEI digitando la combinazione di tasti *#06#**
- Diversi siti consentono di verificare l'associazione tra modello del telefono e IMEI
  - http://www.numberingplans.com/
  - http://www.trackimei.com/

Numberingplans.com



Enter IMEI number below

+1 DOMAIN.COM

352009043703888 analyse

Example: 350077-52-323751-3

Information on IMEI 352009043703888

Type Allocation Holder	Nokia
Mobile Equipment Type	Nokia E63
GSM Implementation Phase	2/2+
IMEI Validity Assessment	>|< Very likely

Information on range assignment

Est. Date of Range Issuance	Around Q1 2010
Reporting Body	British Approvals Board of Telecommunications (BABT)
Primary Market	Europe
Legal Basis for Allocation	EU R&TTE Directive

Information on number format

Full IMEI Presentation	352009-04-370388-8
Reporting Body Identifier	35
Type Allocation Code	35200904
Serial Number	370388
Check Digit	8

Scheda SIM

- Per poter accedere alla rete di servizi cellulari GSM o UMTS, è necessario inserire all'interno del dispositivo radiomobile una particolare Smart Card, detta **Subscriber Identity Module (SIM)**

- La SIM è caratterizzata da un codice univoco detto **Integrated Circuit Card Identification (ICCID)**

- Il sito http://www.numberingplans.com/ permette di individuare l'operatore associato a una scheda SIM mediante l'inserimento dell'ICCID

Numberingplans.com

Analysis of SIM card numbers

All mobile phone SIM cards have each been assigned a unique SIM card number. Below you can enter a SIM card number to check its validity as well as find out more about the mobile network that issued the chip.

Enter SIM card number below

8939992280156205063 analyse

Example: 8923440000000000003

Information on SIM card number

Network name	H3G
Operator name	H3G
Country or global network	Italy
MCC-MNC	222-99

Repertamento

- Consiste in una serie di «regole» da seguire per garantire il miglior risultato possibile in termini di **integrità e disponibilità dei dati** contenuti nel dispositivo da analizzare
- A seconda della tipologia di dispositivo e/o localizzazione, si possono identificare delle "**best practises**"
  - Computer spento (**Post Mortem Forensics**)
  - Computer acceso (**Live Forensics**)
  - Cellulare/Tablet acceso
  - Cellulare/Tablet spento

Best Practices

- Esistono linee guida dettagliate con le corrette metodologie di acquisizione:
  - RFC3227 - Guidelines for Evidence Collection and Archiving (2002)
  - USA – Department of Justice - Searching and Seizing Computers (2002)
  - USA – IACP - Best Practices for Seizing Electronic Evidence (2006)
  - USA – DoJ – Electronic Crime Scene Investigation v. 2 (2008)
  - UK – ACPO – Computer Based Evidence Guidelines v.4 (2008)
  - Model Standard Operating Procedures for Computer Forensics – SWGDE (Scientific Working Group on Digital Evidence) (2011)
  - **ISO 27037 - Guidelines for identification, collection, acquisition and preservation of digital evidence (2012)**
  - **Electronic Evidence Guide – Council of Europe (2013)**

Smartphone/Tablet

- **Mettere in sicurezza il telefono**
- **Non permettere a nessuno di operare sul dispositivo**
- Annotare eventuali **problemi fisici evidenti riscontrati** (per esempio *display* rotto)
- **Fotografare** tutti gli **aspetti esterni del telefono**
- **Documentare tutte le azioni intraprese**
- Verificare lo stato del telefono **(acceso o spento)**
- **Se è spento lasciarlo spento**

Smartphone/Tablet

- Se è **acceso**
  - Documentare le **informazioni presenti sullo schermo del dispositivo**
  - Se possibile **registrare data e ora del dispositivo** verificandone l'eventuale scarto rispetto all'ora reale
  - **Non navigare nel menu** o aprire alcun messaggio in questa fase
  - **Mantenerlo acceso, isolandone l'accesso alle diverse reti**
    - Bluetooth (ver. 2.1) 2,45GHz
    - Wi-Fi (802.11. a/b/g/n) 2.4GHz
    - GSM/UMTS (ITALIA) 900MHz e 1800MHz e 1885 - 2025 MHz
    - GPS 1575MHz e 1227MHz

  oppure
  - **Spegnerlo rimuovendo la batteria (se possibile) o attraverso un normale shutdown**

Smartphone/Tablet: isolamento

- Esistono almeno **3 tecniche** per isolare un dispositivo in fase di repertamento:
  - **Jammer**
  - **Gabbia di Faraday**
  - **Airplane mode**

Jammer

Gabbia di Faraday

Airplane Mode

- La modalità **Airplane Mode** consente di disattivare tutte le forme di comunicazioni supportate dal dispositivo modificando una sola opzione nelle Impostazioni
- In alcuni modelli (es. iPhone) è possibile impostare la modalità aerea lasciando attive alcune funzionalità (es. ricezione WiFi). In questo caso è necessario porre attenzione a **disattivare effettivamente tutte le possibili connessioni**

Spegnimento vs. Isolamento

- Lo **spegnimento del dispositivo** potrebbe attivare il codice di autenticazione del telefono (es. il PIN della scheda SIM oppure il codice di sblocco del telefono). In alcuni casi questi codici **potrebbero essere molto complessi o impossibili da recuperare, rendendo quindi di fatto impossibile un'analisi forense**
- L'**isolamento del telefono mediante jammer o gabbia di Faraday** comporta un **maggior consumo di batteria da parte del dispositivo** che cercherà di connettersi (senza successo) alla rete. Queste tecniche devono quindi essere accompagnate dalla **connessione del dispositivo con una fonte di carica (corrente elettrica o batterie esterne)**
- La **modalità Airplane** garantisce l'isolamento senza spreco ulteriore di batteria, tuttavia richiede l'interazione da parte dell'operatore con la tastiera del telefono. **Potrebbe comportare dei rischi se non si ha familiarità con lo specifico dispositivo (p.es. errori di attivazione)**.

Smartphone/Tablet

- **Sequestrare**, unitamente al dispositivo, anche:
  - i **cavi di connessione**
  - il **caricabatteria**
  - gli **imballaggi**
  - le **memorie di massa** o rimovibili
  - i **manuali** d'uso
  - i **supporti contenenti il software del telefono**
  - le **bollette telefoniche** associate all'utenza
  - la **confezione della SIM** (che riporta il PIN e il PUK di fabbricazione)
- Documentare il sequestro con le informazioni utili:
  - **Nome dell'operatore** che procede al sequestro
  - **Data e ora di sequestro** del dispositivo
  - **Posizione** in cui il telefono è stato rinvenuto (indirizzo, coordinate GPS, ecc.)

Passi operativi

- Identificazione e repertamento
- **Acquisizione e verifica**
- Conservazione
- Analisi
- Valutazione e presentazione

Acquisizione di dispositivi mobile

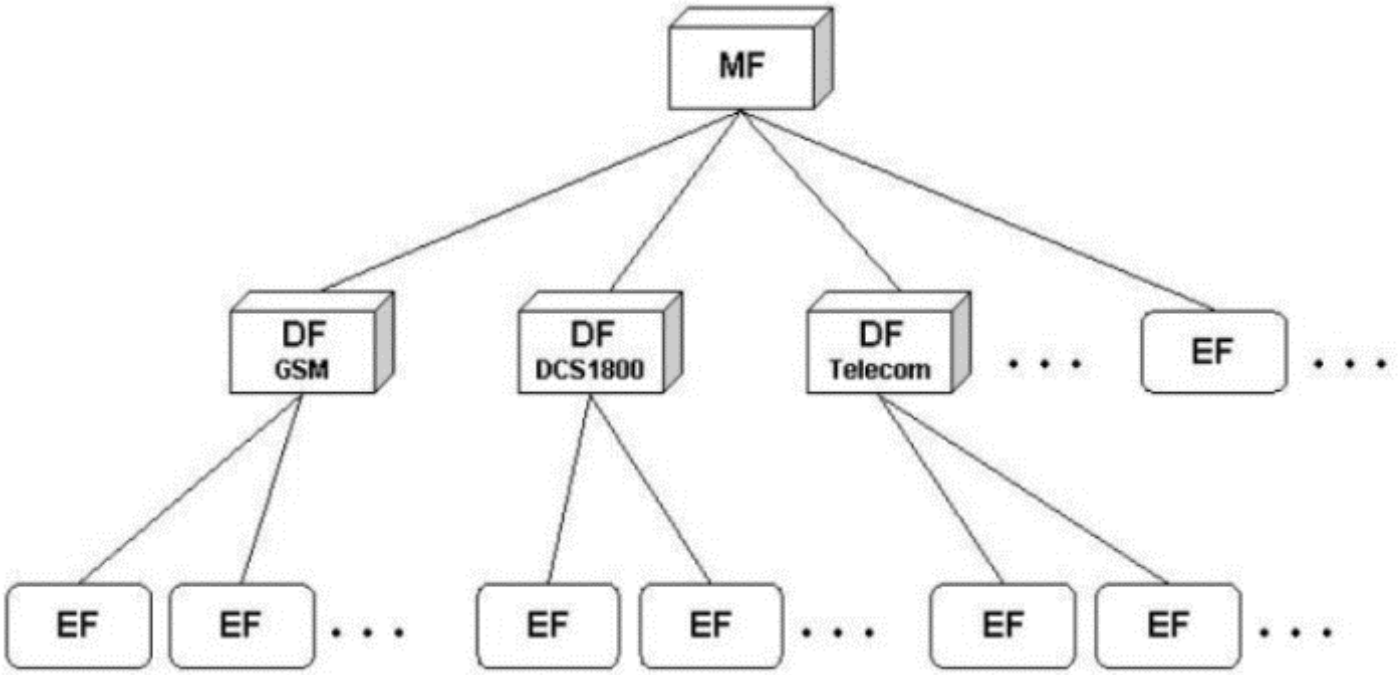
- L'analisi di uno dispositivo mobile a fini probatori riguarda tipicamente tre **aree di ricerca**, ovvero:
  - La **scheda SIM**
  - La **memoria rimovibile** (es. SD Card)
  - La **memoria interna** del terminale radiomobile
- Per la memoria interna, in base al tipo di dispositivo, al sistema operativo installato e agli strumenti di analisi disponibili si possono effettuare due tipi di acquisizione:
  - **Logica**, ovvero acquisizione dei file attualmente presenti nel file system
  - **Fisica**, ovvero acquisizione dell'intero contenuto della memoria NAND presente nel dispositivo

Scheda SIM

- La sicurezza di una SIM è garantita dalla possibilità di attivare **meccanismi interni di cifratura dei dati**
- Se tali meccanismi sono attivati è necessario inserire, ad ogni accensione del telefono, un **PIN (Personal Identification Number)**, ovvero un codice composto da **quattro a otto cifre**.
- L'inserimento di un codice errato per **tre volte** manda usualmente la scheda in **blocco temporaneo**
- In questo caso per sbloccare la scheda è necessario richiedere al Network Service Provider il **PUK (Personal Unlocking Key)**, ovvero un codice di **dieci cifre** da digitare sul telefono bloccato
- L'inserimento del codice PUK errato per 10 volte manda la SIM in **blocco definitivo**
- Attualmente **non esistono strumenti hardware o software in grado di estrarre o superare i codici PIN e PUK di una scheda SIM**

Scheda SIM

- La memoria interna della scheda SIM è organizzata secondo una struttura gerarchica ad albero, composta da 3 elementi:



Scheda SIM

- I file nelle cartelle **DF_{GSM}** e **$DF_{DCS1800}$** contengono prevalentemente informazioni sulla rete, mente i file nella cartella **$DF_{TELECOM}$** contengono informazioni relative ai servizi attivi del gestore
- Le informazioni di maggior interesse recuperabili da una scheda SIM sono:
  - ICCID (Integrated Circuit Card Identification)
  - IMSI (International Mobile Subscriber Identity)
  - Rubrica (Abbreviated Dialing Numbers – ADN)
  - Registro chiamate (Last Dialed Number – LDN)
  - Short Message Service (SMS)
  - Short Message Parameters (SMSP)
  - **Location information (LOCI)**
  - SIM Service Table (SST)
  - Public Land Mobile Network (PLMN) selector
  - Forbidden PLMNs
  - Service Dialing Numbers (SDNs)

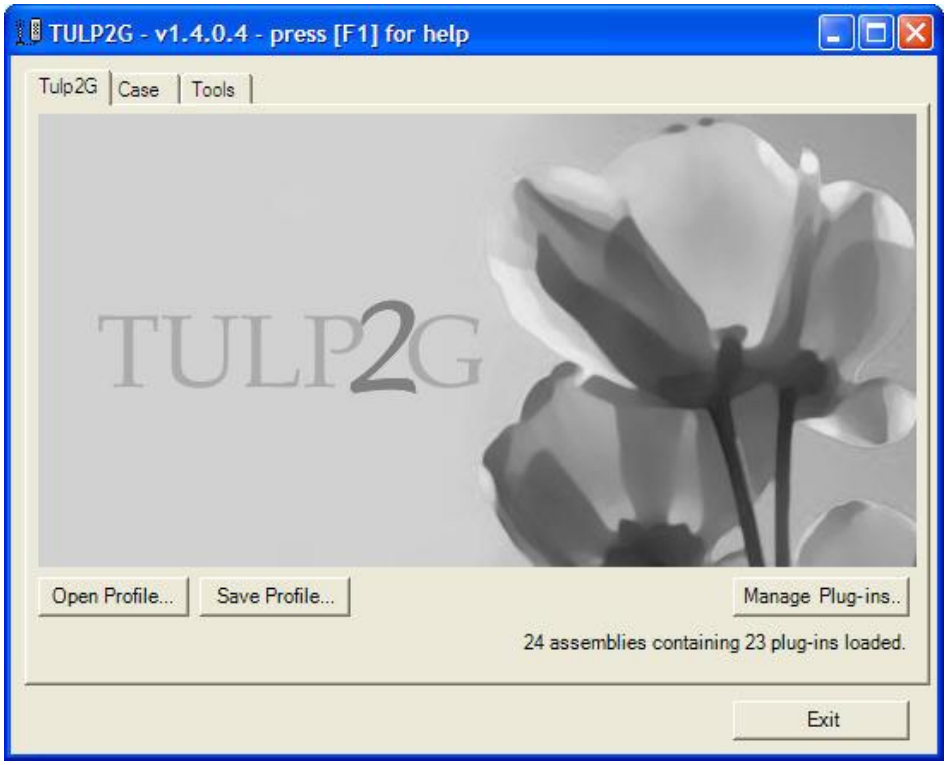
Scheda SIM

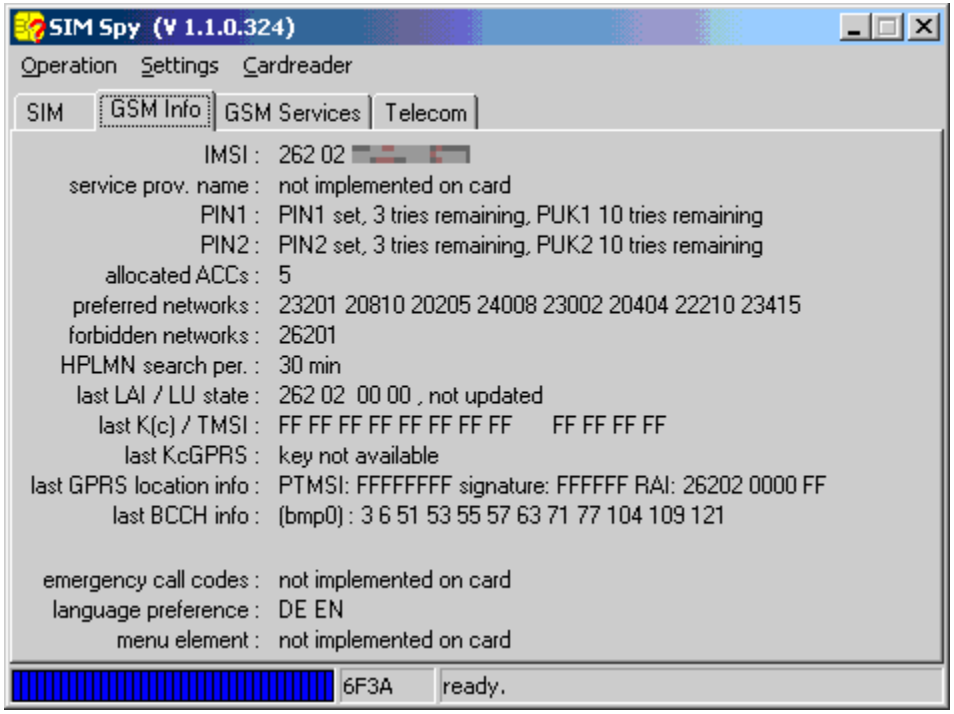
- L'estrazione delle informazioni dalla scheda viene effettuata rimuovendo la SIM dall'alloggiamento nel telefono e inserendolo all'interno di un lettore di SIM Card
- Il lettore deve supportare lo **standard PC/SC (http://www.pcscworkgroup.com/)**

Scheda SIM

- I principali software disponibili per l'analisi sono:
  - **SIMiFOR** - http://www.forensicts.co.uk/ (commerciale)
  - **SIMcon** - http://www.simcon.no/ (commerciale)
  - **USIM Detective** - http://www.quantaq.com (commerciale)
  - **Dekart SIM Manager** - http://www.dekart.com (commerciale)
  - **SIMSpy2** - http://www.nobbi.com/ (freeware)
  - **Tulp2G** - http://tulp2g.sourceforge.net/ (freeware)

Scheda SIM





Memoria rimovibile

- Utilizzata per aumentare la ridotta capacità di memorizzazione della memoria flash integrata
- All'interno si trovano solitamente **dati multimediali e documenti**
- Può contenere qualsiasi dato in forma digitale e costituisce un semplice strumento per l'occultamento di dati, anche grazie alle **dimensioni geometriche ridotte**
- L'acquisizione può essere effettuate mediante tradizionali tecniche (es. write blocker + DD)

Memoria interna

- La fase di acquisizione è caratterizzata da diversi aspetti che ne condizionano il risultato e la quantità e qualità di informazioni recuperabili
- Ad esempio:
  - Produttore
  - Modello
  - Sistema operativo (tipo)
  - Versione del sistema operativo
  - Codici di protezione (es. PIN Sim, Passcode dispositivo)
  - File system
  - Presenza di cifratura

Sistemi Operativi mobile

iOS 6

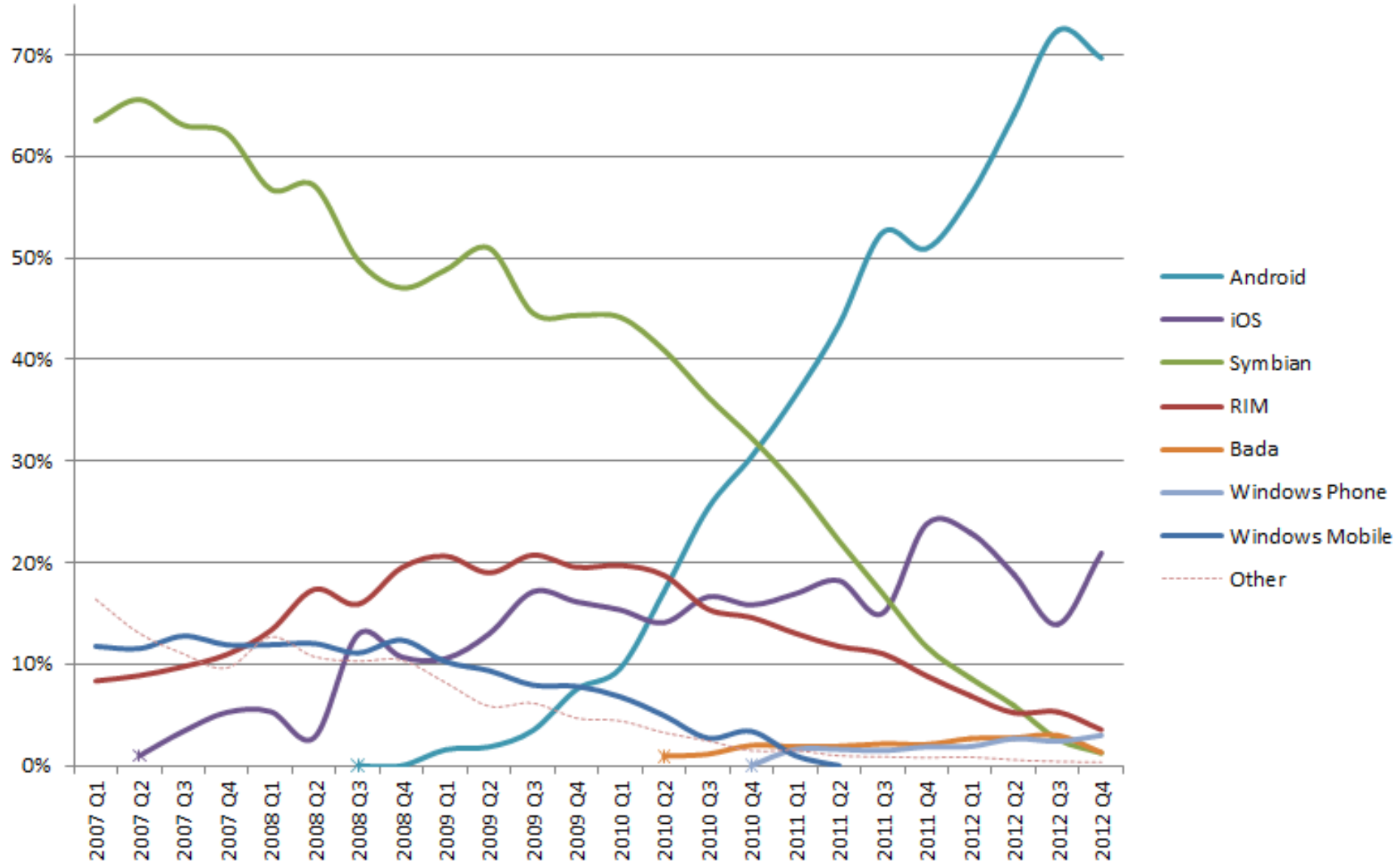
Windows 8 Phone

bada

BlackBerry 7

symbian OS

World-Wide Smartphone Sales (%)



Memoria interna

- Come detto l'analisi della memoria interna può essere di tipo **logico** (file visibili) o **fisico** (copia integrale della memoria)
- In entrambi i casi l'analisi dei dati sarà effettuata:
  - Utilizzando un personal computer su cui sia installato un software di estrazione dei dati (software di backup del telefono oppure software dedicato per la mobile forensics)

  oppure
  - Utilizzando un dispositivo hardware dedicato
- **In entrambi i casi, è necessario garantire una connessione tra il telefono cellulare e lo strumento di acquisizione**

Memoria interna

- A seconda del modello la connessione si può realizzare:
  - via cavo
  - tramite infrarossi
  - via onde radio Bluetooth
- La connessione **più sicura, affidabile e con minor impatto sui dati** è quella via **cavo**
- Qualora non sia disponibile il cavo di connessione per il modello sequestrato, è consigliabile utilizzare una connessione ad infrarosso (se disponibile)
- La connessione Bluetooth deve essere utilizzata come *extrema ratio*, poiché genera modifiche al dispositivo durante la fase di attivazione e autenticazione della connessione

Acquisizione logica (backup)

- Principali software per l'**acquisizione logica** mediante **backup**:
  - iTunes (Apple)
  - BlackBerry Desktop Manager
  - Nokia Suite
  - Samsung Kies





Acquisizione logica (software)

- Principali software forensi per l'**acquisizione logica**
  - Oxygen Forensics Suite
  - Compleson Lab MOBILedit! Forensic
  - Paraben Device Seizure
  - Mobile Phone Examiner

Santoku Linux

Acquisizione logica (hardware)

- Principali hardware forensi per l'**acquisizione logica**
  - Cellbrite UFED
  - Micro Systemation XRY
  - CellDEK

Acquisizione fisica

- Gli strumenti e le tecniche per l'acquisizione fisica differiscono a seconda del produttore e della versione del sistema operativo
- Il vantaggio nell'effettuare un'acquisizione fisica risiede nel fatto di **poter recuperare (in alcuni casi) informazioni cancellate**
- Vedremo dopo alcune tecniche per i dispositivi con sistema operativo iOS

iPhone/iPad Forensics

iPhone/iPad Forensics

- iDevice e sistema operativo iOS
- Acquisizione dei dati
  - Acquisizione logica
  - Acquisizione fisica
  - Analisi dei backup
- Cifratura e relativi attacchi
- Analisi dei dati

iDevice

- **iDevice** in its widest sense, is an unofficial general term that can refer to any mobile electronic devices marketed by Apple that start with "i", or more specifically any of their devices (sometimes then referred to as iOS Devices) that use the iOS operating system, which includes:
  - iPad
  - iPhone
  - iPod
  - iPod Touch

iPhone

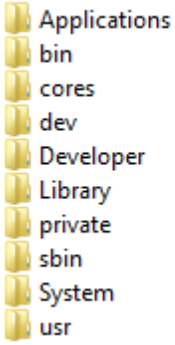
- Famiglia di **smartphone** con funzioni multimediali prodotta da Apple e basata sul sistema operativo iOS
- L'interfaccia principale del dispositivo si chiama **springboard** ed è composta dalle icone delle applicazioni con un dock con le applicazioni Telefono – E-Mail – Safari e iPod
- Apple ha realizzato finora 5 versioni:
  - iPhone Edge (2007)
  - iPhone 3G (2008)
  - iPhone 3GS (2009)
  - iPhone 4 (2010)
  - iPhone 4S (2011)
  - iPhone 5 (2012)

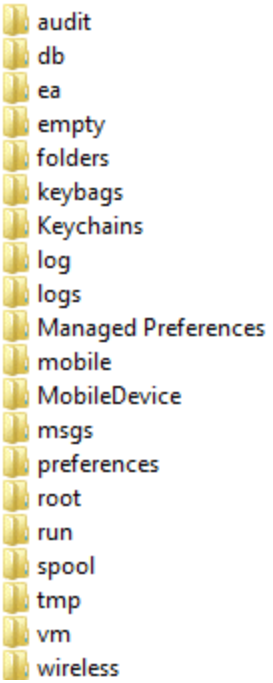
iPad

- Famiglia di **tablet** con funzioni multimediali prodotta da Apple e basata sul sistema operativo iOS
- Concepito per l'accesso a media audio-visivi quali libri, film, musica, giochi e contenuti web
- Utilizza un'interfaccia grafica simile a quella degli iPhone
- Ha dimensioni maggiori e prestazioni più performanti
- Non consente di effettuare telefonate e inviare SMS utilizzando la rete cellulare
- Apple ha realizzato finora 3 versioni:
  - iPad 1 (2010)
  - iPad 2 (2011)
  - iPad 3 (2012)

File system e partizioni

- I dispositivi basati su iOS utilizzano file system **HFSX** (una variante di HFS+ case sensitive)
- Il sistema operativo iOS divide il disco in **due partizioni**: una partizione di sistema e una dati
- La partizione di sistema è **accessibile in sola lettura** (a meno di attività di **jailbreaking**)
- La partizione dati è **accessibile in lettura e scrittura** e conserva la maggior parte delle informazioni utili durante un'investigazione digitale
- La dimensione della partizione di sistema è pari a 1-1,5 GB, mentre la dimensione della partizione dati è variabile in funzione della dimensione complessiva della memoria NAND presente nel dispositivo





Principali applicazioni

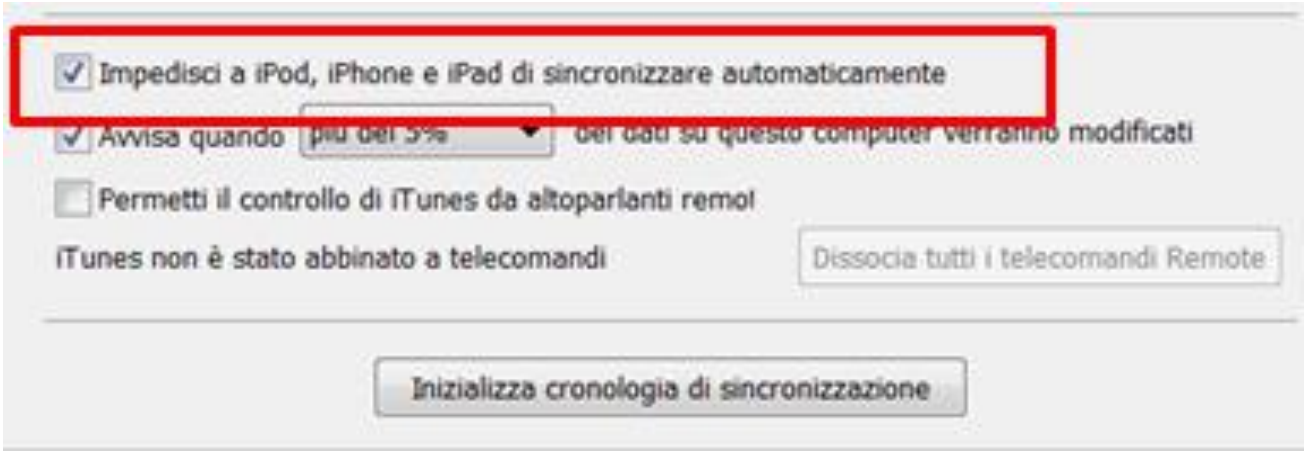
- Calendario (iPhone/iPad)
- Contatti (iPhone/iPad)
- Telefono (iPhone)
- SMS (iPhone)
- Note (iPhone/iPad)
- Mappe (iPhone/iPad)
- Immagini (iPhone/iPad)
- Video (iPhone/iPad)
- iTunes (iPhone/iPad)
- iBooks(iPhone/iPad)
- iPod (iPhone/iPad)
- YouTube (iPhone/iPad)
- Safari (iPhone/iPad)
- Mail (iPhone/iPad)
- AppStore (iPhone/iPad)

Acquisizione logica dei dati

- L'**acquisizione «logica»** consiste nell'estrazione delle informazioni «visibili» dalla partizione che contiene i dati generati dall'utente
- Può essere effettuata principalmente con 2 metodologie
  - **Utilizzando la funzionalità di backup fornita da iTunes**
  - **Utilizzando software/hardware dedicati per l'analisi forense**

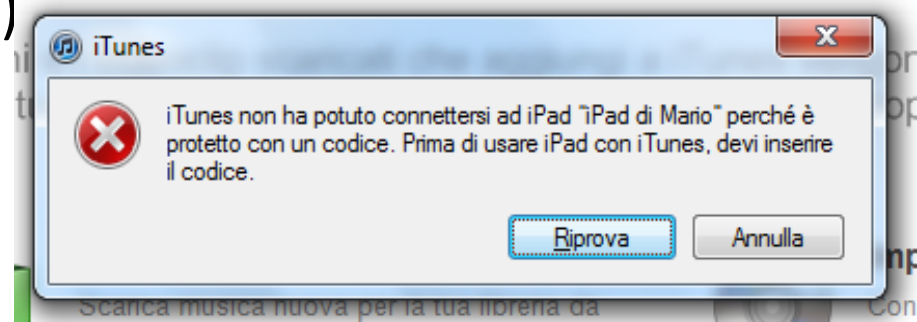
Backup con iTunes

- Prima di procedere alla creazione di un backup tramite iTunes è necessario:
  - Verificare che il dispositivo **non sia bloccato con un passcode**, poiché in questo caso **il software non può accedere alle informazioni memorizzate**
  - Assicurarsi che l'**opzione di sincronizzazione automatica in iTunes** (Modifica > Preferenze > Dispositivi) **sia disabilitata**



Acquisizione logica di dispositivi con passcode

- Se il dispositivo è protetto da un passcode, non è possibile effettuarne un'acquisizione logica indipendentemente dal software utilizzato (iTunes o software forense)
- **Non sono note tecniche di bruteforce del passcode con il dispositivo acceso**
- L'unico modo per superare questo vincolo consiste nell'**estrarre i certificati di sincronizzazione** (Lockdown file) **da un computer utilizzato almeno una volta per la sincronizzazione del dispositivo** (es. Personal Computer, Mac, ecc.)



Acquisizione logica di dispositivi con passcode

- I file in formato plist che consentono al dispositivo di effettuare l'operazione di sincronizzazione, anche se bloccato, sono conservati in cartelle diverse a seconda del sistema operativo utilizzato.
- **Per poter accedere al dispositivo dal computer di acquisizione, è necessario copiare i file dei certificati nella corrispondente cartella**

Sistema operativo	Percorso relativo al file .plist contenente i certificati
Windows 7	C:\ProgramData\Apple\Lockdown
Windows Vista	C:\Users\[username]\AppData\roaming\Apple Computer\Lockdown
Windows XP	C:\Documents an Settings\[username]\Application Data\Apple Computer\Lockdown
Mac OS X	/private/var/db/lockdown

Backup con iTunes

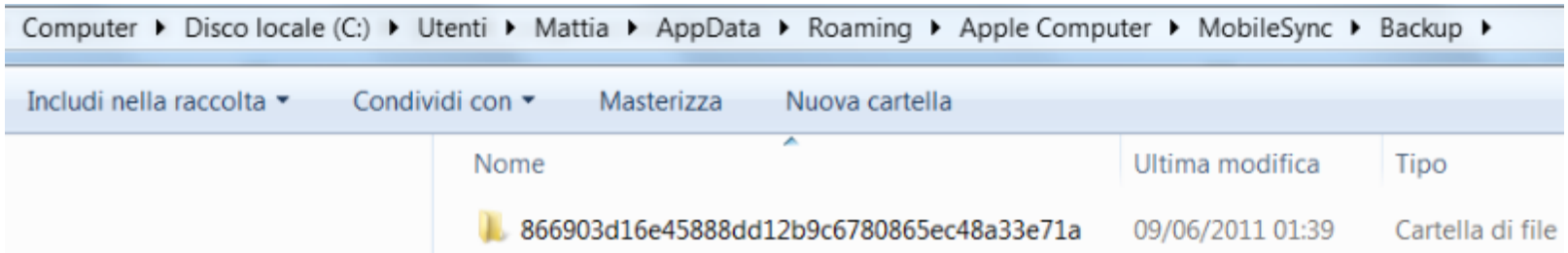
- La procedura di backup può essere avviata accedendo all'interfaccia grafica del software iTunes, facendo click col tasto destro sul nome del dispositivo rilevato e selezionando la voce "Backup" nel menu a tendina

Backup con iTunes

- A seconda del sistema operativo utilizzato per l'estrazione, il backup viene salvato in percorsi differenti

Sistema operativo	Percorso di salvataggio del backup
Windows XP	C:\Documents and Setting\[username]\Application Data\Apple Computer\MobyleSync\Backup
Window 7\Vista	C:\Users\[username]\AppData\Roaming\Apple Computer\MobileSync\Backup
Mac OS X	Users/Username/Library/Application Support/MobileSync/Backup

- Il software iTunes crea una cartella per ogni dispositivo di cui si effettua il backup. Il nome della cartella corrisponde con il **UDID (Unique Device Identifier) del dispositivo**, ovvero una stringa di 40 caratteri alfanumerici la cui funzione è simile a quella del numero seriale.



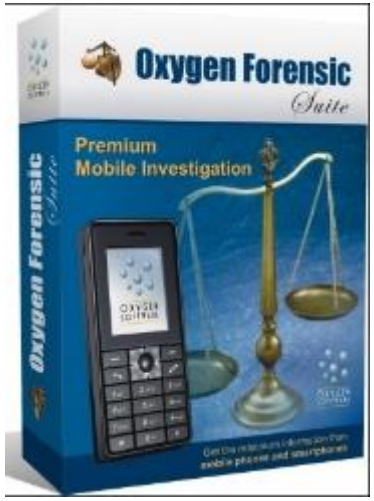
Analisi dei backup di iTunes

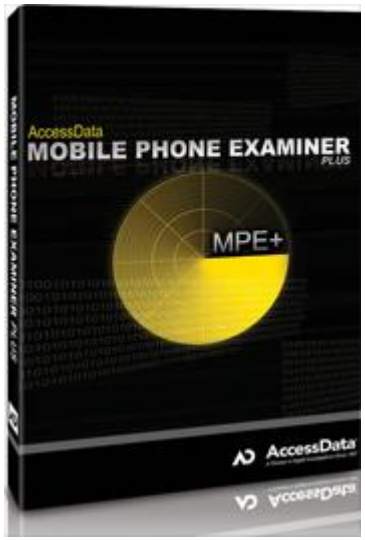
- Per estrarre i dati dal backup generato con iTunes esistono diverse soluzioni software:
  - **iPhone Backup Analyzer,** opensource
  - **iPhone Backup Extractor**, freeware per ambienti MacOSX
  - **Oxygen Forensics Suite**, commerciale
  - **iBackupBot**, commerciale per ambienti Microsoft
  - **iPhone Backup Extractor**, commerciale per ambienti Microsoft

- Tale tecnica può essere utilizzata anche per **l'analisi di backup rinvenuti sul computer del proprietario del dispositivo**: è infatti possibile che l'utente abbia sincronizzato il contenuto del proprio dispositivo durante il periodo di utilizzo per avere a disposizione una copia di backup dei dati in esso contenuti.
- Qualora un eventuale backup rinvenuto sul computer fosse **protetto da password** è possibile utilizzare il software **Elcomsoft Phone Password Breaker**, che permette di generare un attacco a dizionario o bruteforce sui file.

Acquisizione logica con software/hardware dedicati

- In commercio esistono diverse soluzioni hardware e software per l'acquisizione di dispositivi iOS.
- Per una trattazione completa si rimanda al white paper pubblicato sul sito viaforensics.com (A.Hogg).
- I principali strumenti disponibili sono:
  - **Oxygen Forensics Suite**
  - **Cellbrite UFED**
  - AccessData Mobile Phone Examiner Plus
  - Katana Forensics Lantern
  - EnCaseNeutrino
  - Micro Systemation XRY
  - Compleson Lab MOBILedit! Forensic
  - Paraben Device Seizure
  - CellDEK
  - Subrosa MacLock Pick
  - Black Bag Technology Mobilyze

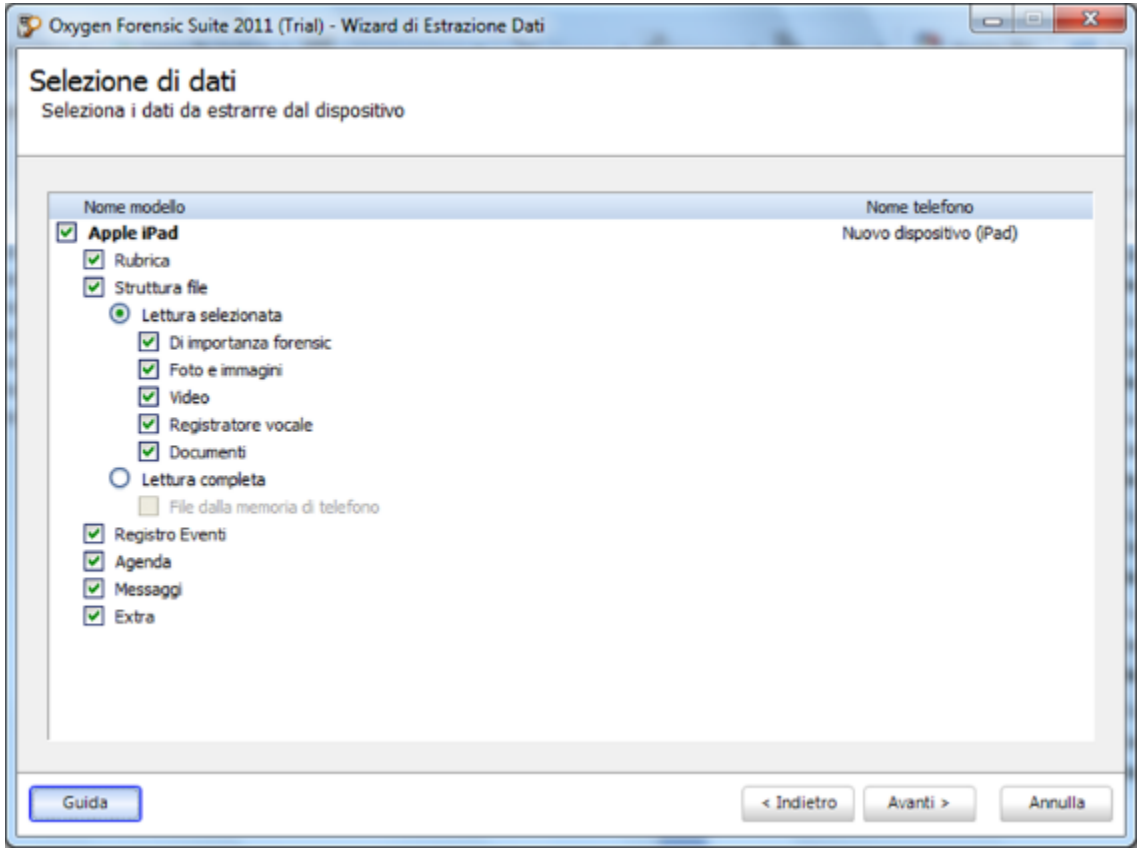




Oxygen Forensics Suite – Connessione del dispositivo

Oxygen Forensics Suite – Connessione del dispositivo

Oxygen Forensics Suite – Estrazione dei dati

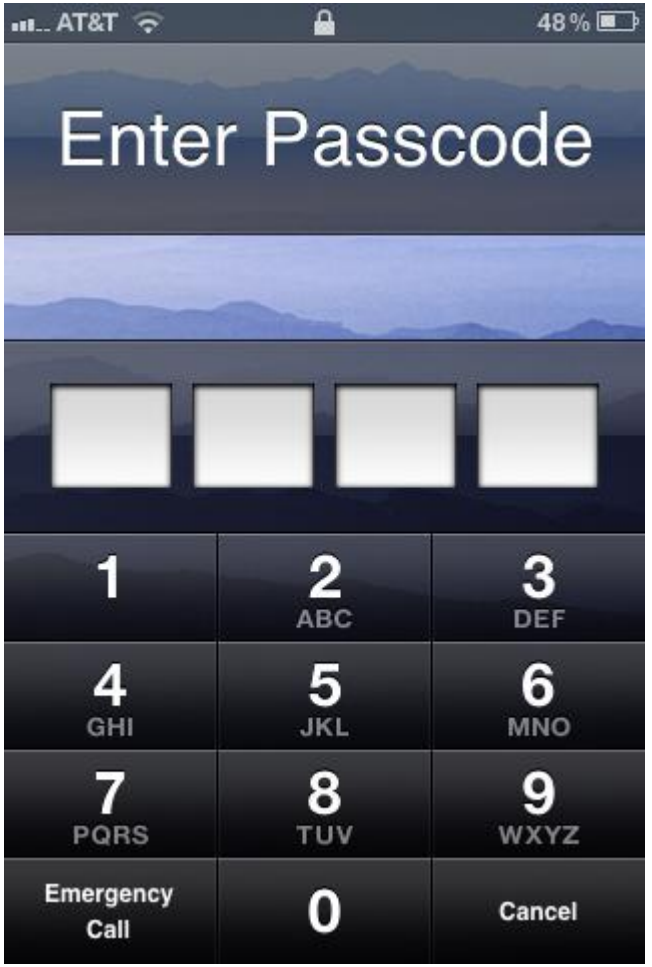


Acquisizione fisica

- L'acquisizione fisica di un dispositivo mobile consiste **nella creazione di una copia bit a bit della memoria interna o di una sua partizione**
- Per obbligare l'utente di un iDevice all'utilizzo dell'App Store per l'installazione di nuove applicazioni, **Apple implementa in iOS un meccanismo di jail che impedisce all'utente l'accesso alla partizione di sistema**.
- Per aggirare questo meccanismo che impedisce l'acquisizione fisica di un iDevice esistono due metodologie:
  - Effettuare un **jailbreaking del dispositivo**
  - **Utilizzare la modalità DFU** (Device Firmware Update) e le tecniche alla base del jailbreaking per **caricare un RAM Disk che contenga strumenti per fare la copia bit a bit della partizione di sistema e di quella dati ed eventualmente il bruteforce del passcode**

Cifratura nei dispositivi iDevice

- A partire dal modello iPhone 3GS, Apple ha incluso nei dispositivi un **componente hardware per la cifratura AES utilizzato per velocizzare le operazioni**
- A partire dalla versione 4 di iOS è stato inoltre introdotta la **Full Disk Encryption dei file system presenti nelle due partizioni (sistema e dati)**
- La memoria NAND presente nel dispositivo è suddivisa in blocchi: la maggior parte dei blocchi sono utilizzati per conservare i file presenti all'interno della partizione di sistema e della partizione dati
- Il blocco 1 della memoria NAND, detto PLOG, è utilizzato per conservare le chiavi di cifratura e altre informazioni utili per effettuare un wiping rapido del dispositivo
- Il blocco PLOG conserva 3 chiavi di cifratura:
  - **BAGI**
  - **Dkey**
  - **EMF!**



Cifratura nei dispositivi iDevice

- **La chiave EMF! è utilizzata per cifrare il file system**
- Ogni volta che un dispositivo viene wipato, **la chiave viene scartata e ricreata**
- **Il file è conservato nell'area PLOG della NAND e senza la EMF Key originale, la struttura del filesystem non può essere recuperata**

- iOS mette a disposizione diverse classi di protezione, ciascuna delle quali identificata da una master key
- Le due classi di protezione principali sono disponibili solamente dopo l'ìnserimento da parte dell'utente del passcode e quindi **i file protetti con tali livelli di protezione possono essere decifrati solamente conoscendo il passcode**

- La maggior parte dei file presenti sui dispositivi, tuttavia, **non appartengono a nessuna classe di protezione (NSFileProtectionNone) e sono quindi sempre disponibili per il sistema operativo**
- I file che appartengono a questa categoria sono cifrati utilizzando una master key speciale detta **Dkey**, che è memorizzata nell'area PLOG della NAND

Cifratura nei dispositivi iDevice

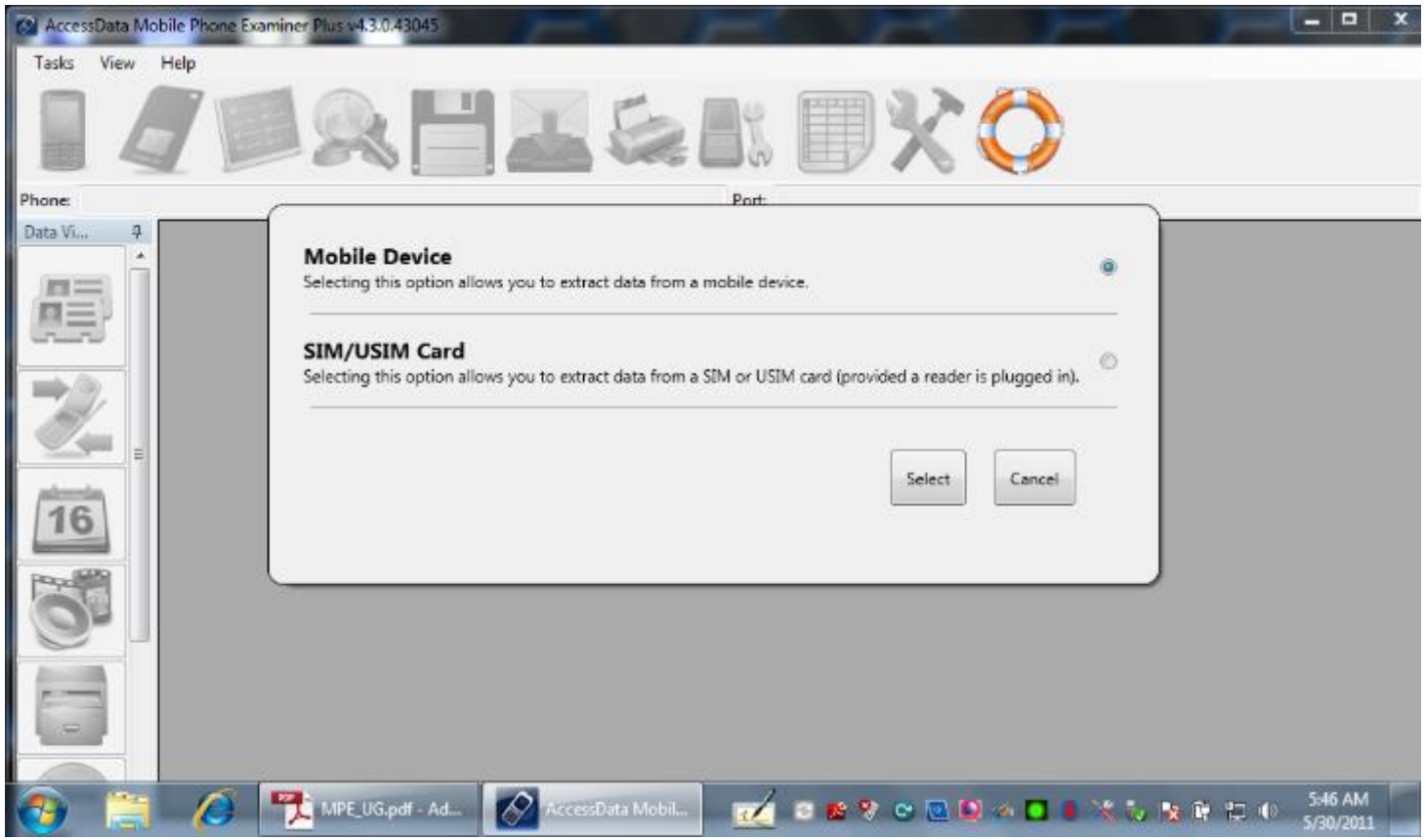
- Effettuando il boot del dispositivo con un RAM disk è possibile accedere alle chiavi memorizzate nell'area PLOG e in particolare **la chiave EMF! (cifratura del file system) e la chiave Dkey (master key per la cifratura dei file senza protezione da passcode)**
- Fino a iOS versione 5 incluso gli unici file appartenenti a classi di protezione dipendenti dal passcode sono:
  - **Messaggi di posta elettronica**
  - **File contenente le password di accesso alle reti wifi o a siti web (keychain)**
  - **File di dati di applicazioni di terze parti che utilizzino strong- encryption (es. Whattsap)**
- Per questo motivo, **anche senza conoscere il passcode del dispositivo o effettuarne il brute-force, è possibile estrarre tutti i file presenti sul dispositivo ad eccezione di quelli illustrati al punto precedente**
- Inoltre, effettuando il boot del device con un RAM disk, è possibile **effettuare un attacco brute-force al passcode senza correre il rischio di attivare le funzionalità di wiping automatico**
- Nel caso di passcode semplice (quattro cifre), **il tempo necessario per il brute force richiede tra 20 e 40 minuti, a seconda del tipo di dispositivo**
- Conoscendo **il passcode è possibile accedere ai file con classe di protezione più elevata**

Acquisizione Fisica con software/hardware dedicati

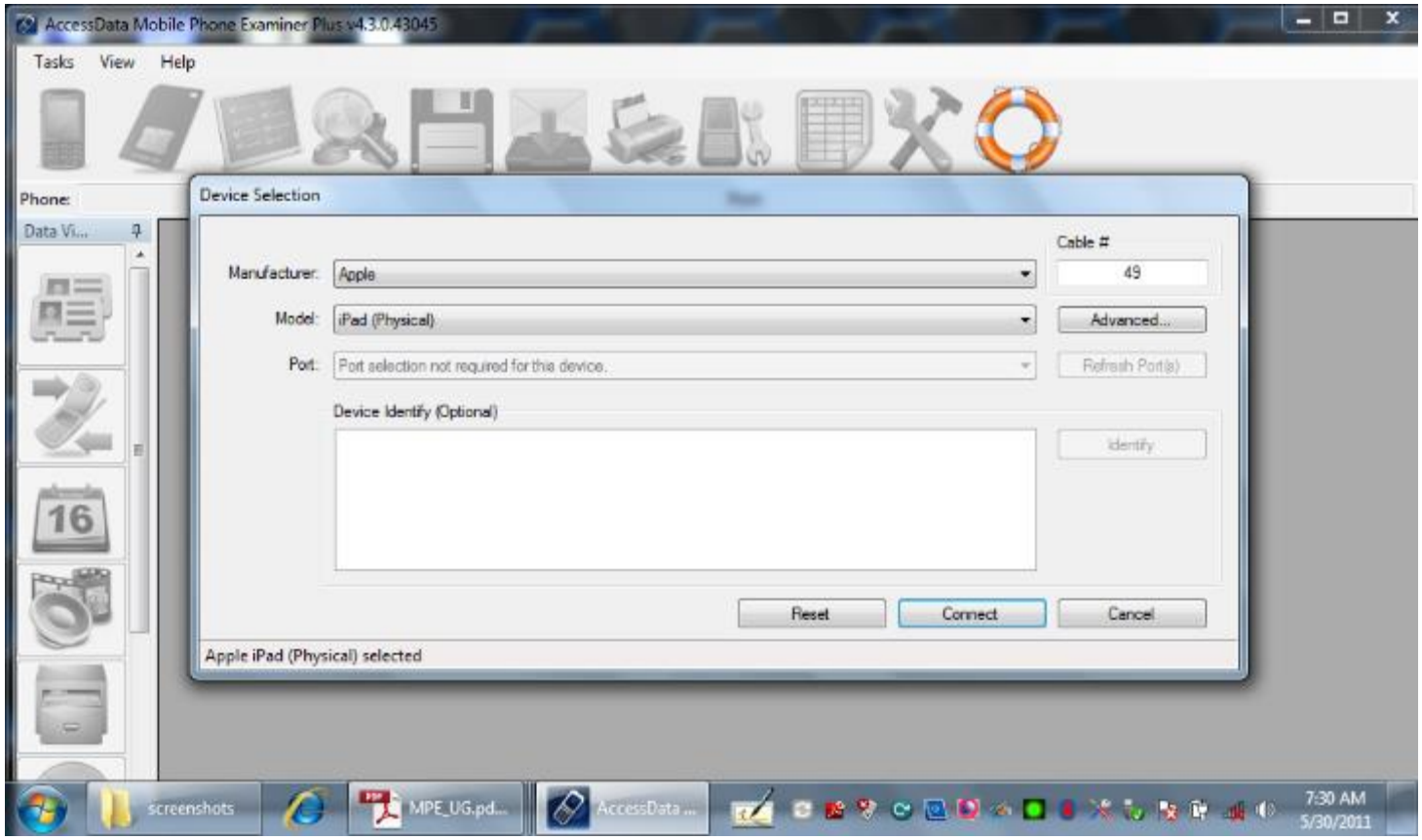
- Attualmente sono disponibili diverse soluzioni che consentono l'acquisizione fisica di un iDevice:
  - **Zdziarski Method and Tools, riservato a Law Enforcement** (http://www.iosresearch.org)
  - **Lantern Lite**, freeware per Mac
  - **Elcomsoft iOS Acquisition Toolkit**, commerciale per Windows e Mac
  - **AccessData Mobile Phone Examiner Plus**, commerciale per Windows
  - **Cellbrite UFED**, commerciale per Windows
  - **iXAM**, commerciale per Windows

- **L'acquisizione fisica di dispositivi iPad 2 e iPhone 4S è supportata al momento del software Elcomsoft e solo in seguito a jailbreaking**

AccessData MPE+
Acquisizione fisica –iPhone 4/iPad



AccessData MPE+ Acquisizione fisica

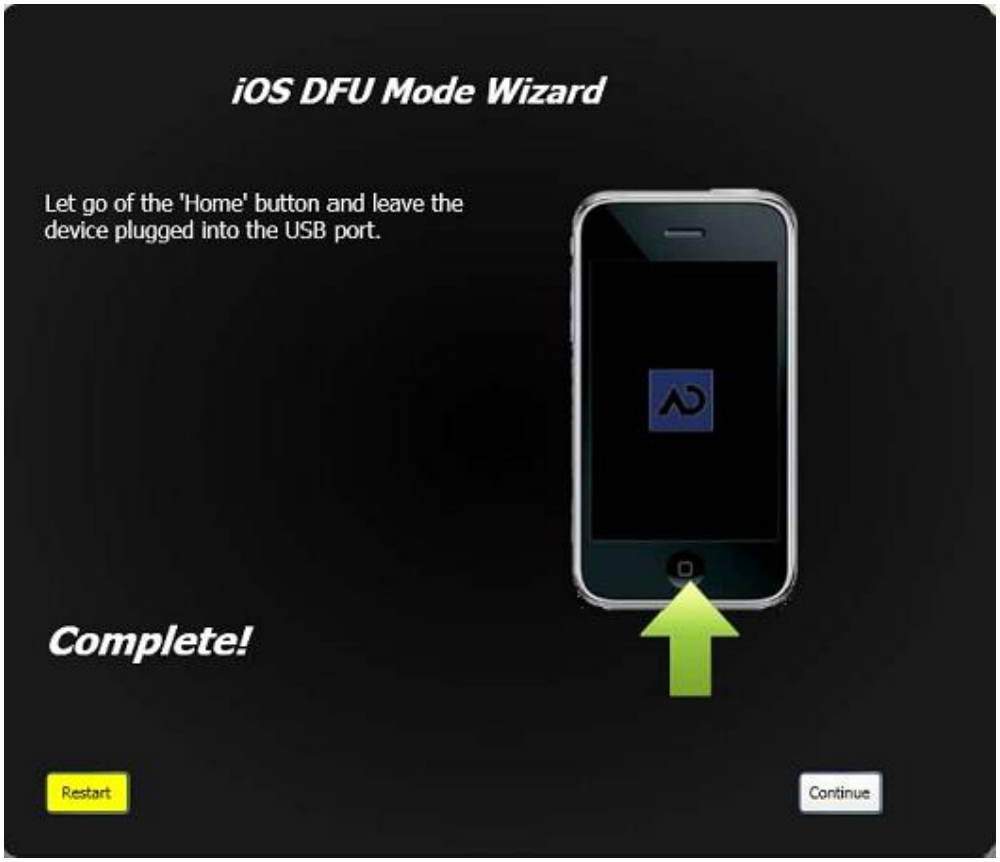


AccessData MPE+ DFU Mode Wizard

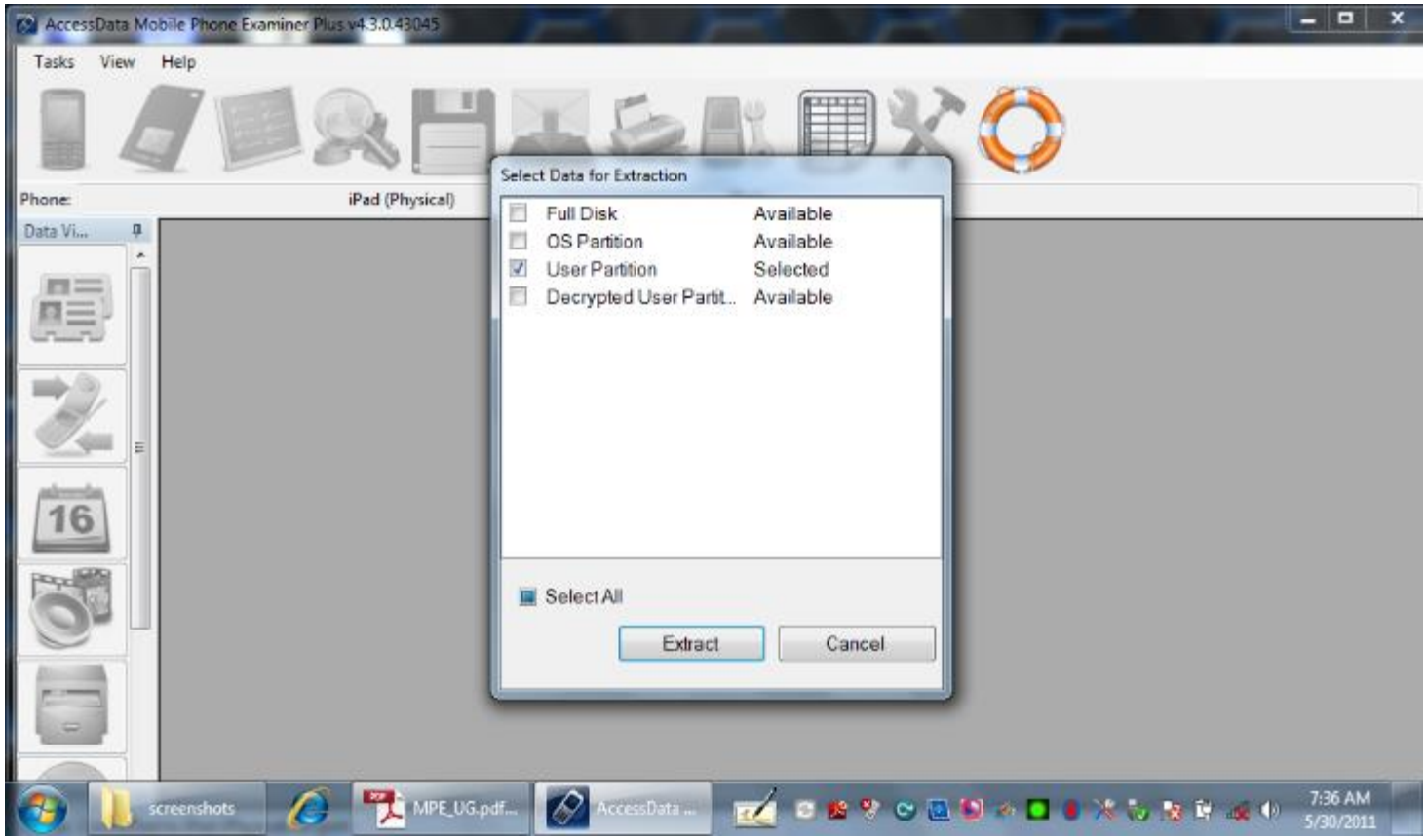
AccessData MPE+ DFU Mode Wizard

AccessData MPE+ DFU Mode Wizard

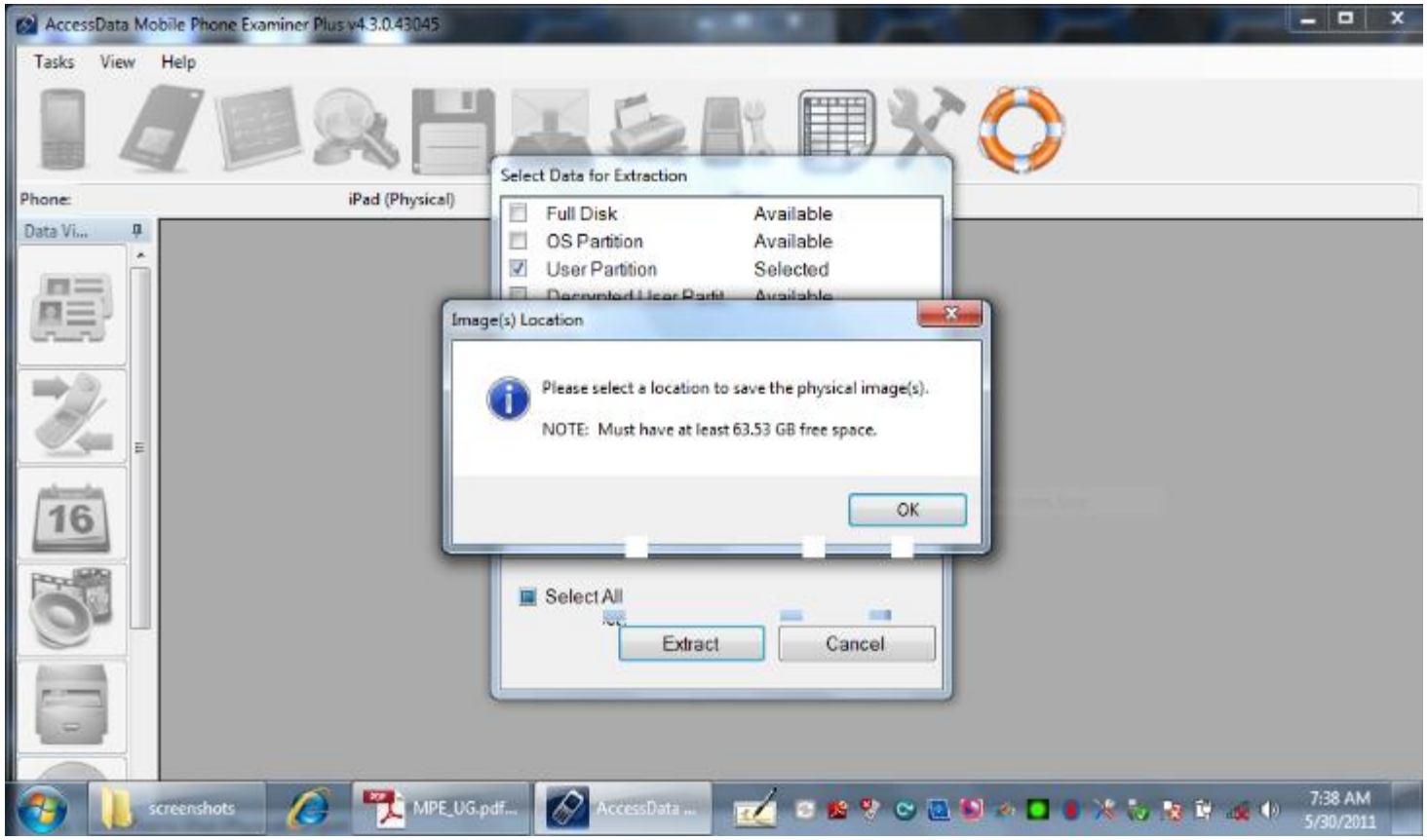
AccessData MPE+ DFU Mode Wizard



AccessData MPE+ Acquisizione fisica

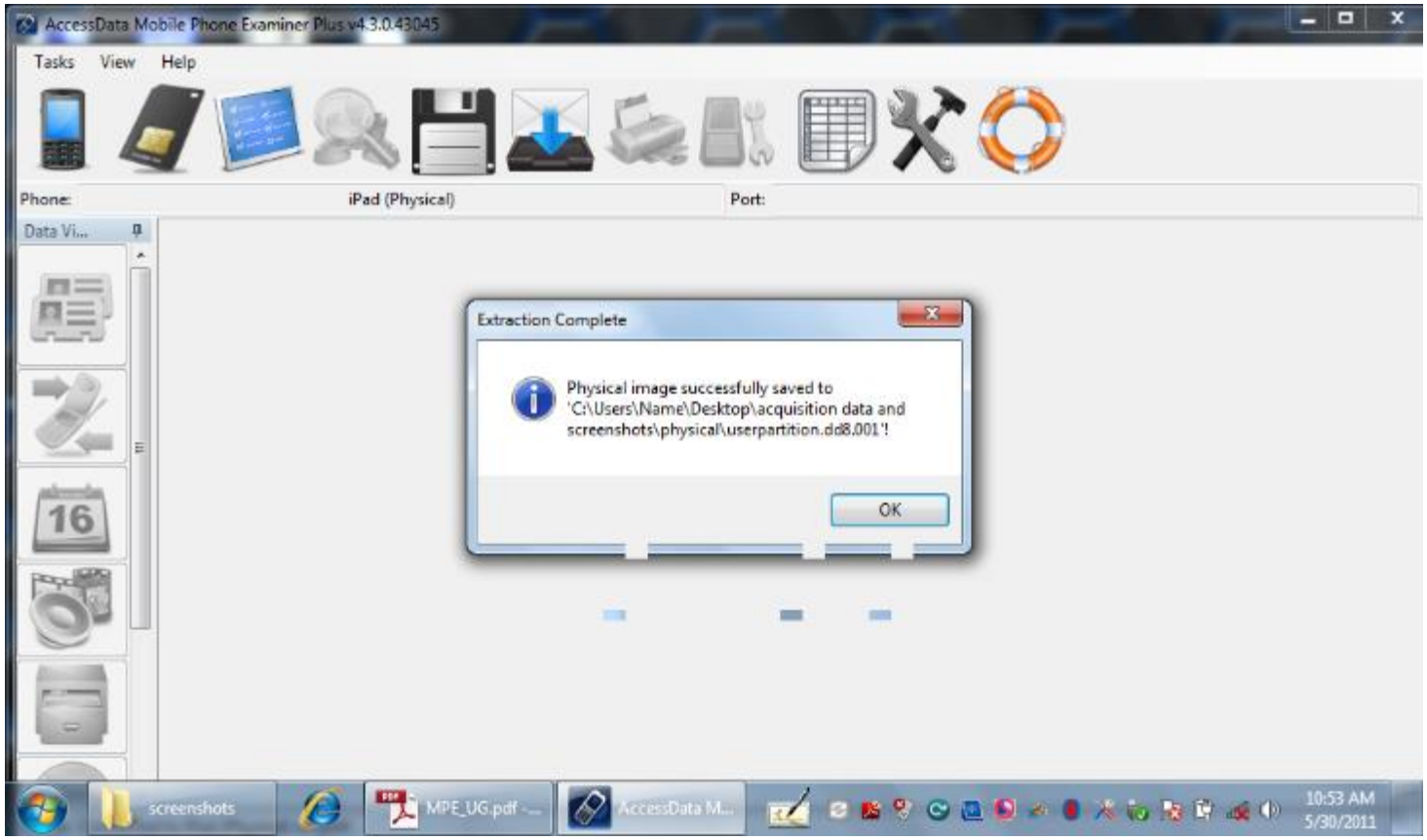


AccessData MPE+ Acquisizione fisica



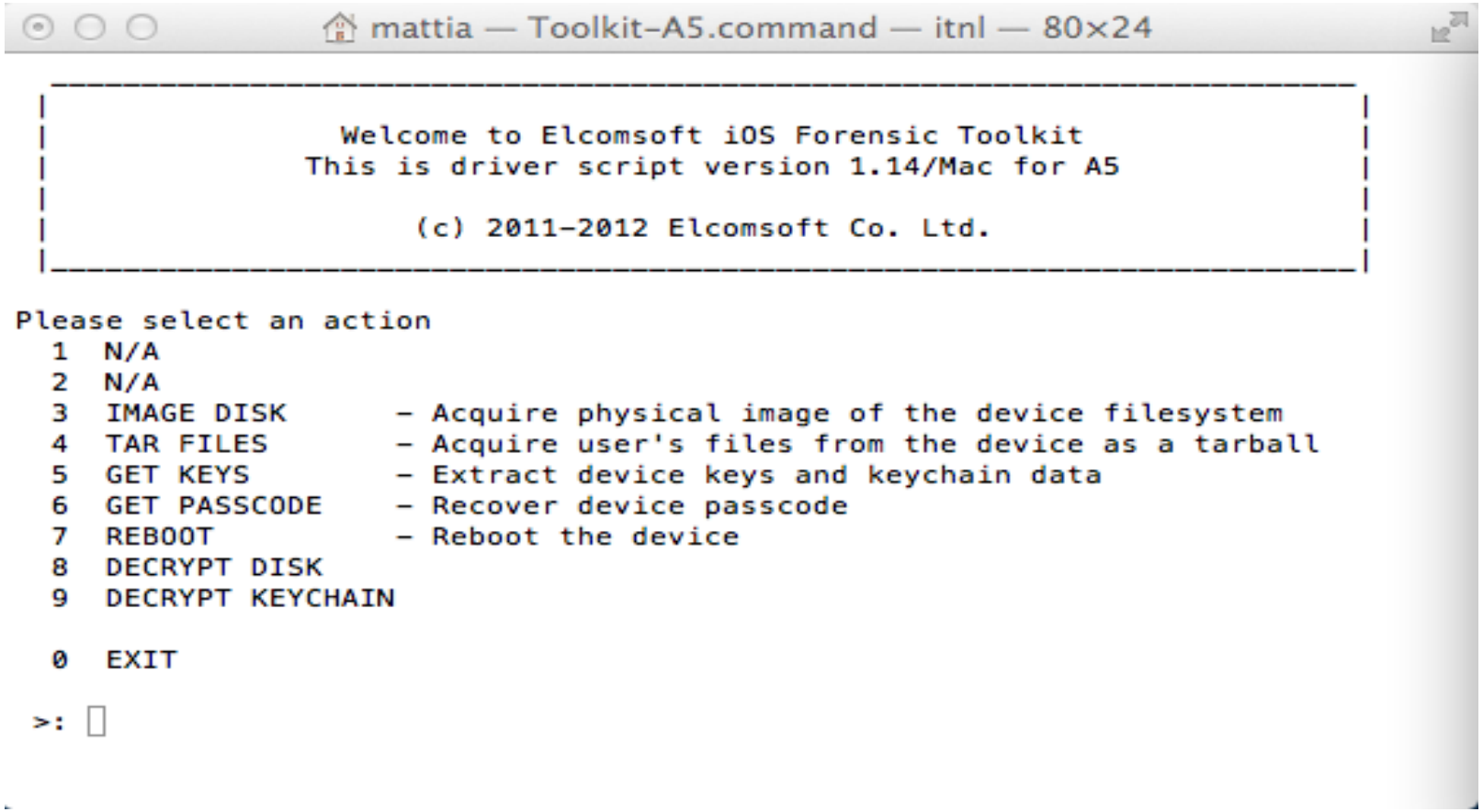
AccessData MPE+
Acquisizione fisica

AccessData MPE+ Acquisizione fisica



Elcomsoft iOs Forensic Toolkit Acquisizione fisica di iPhone4s/iPad2

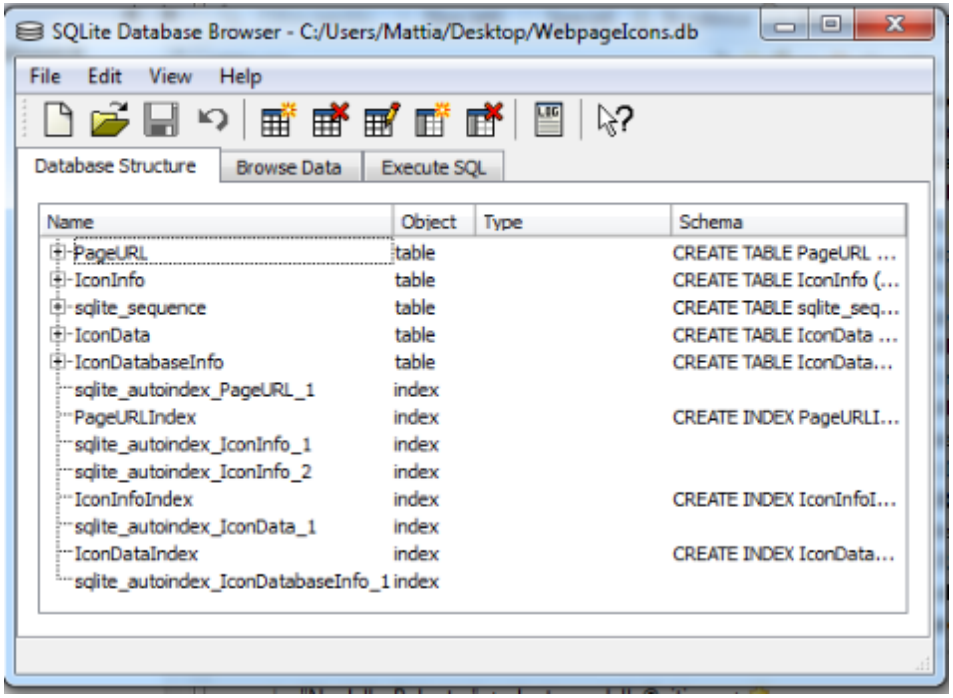
Elcomsoft iOs Forensic Toolkit Acquisizione fisica di iPhone4s/iPad2

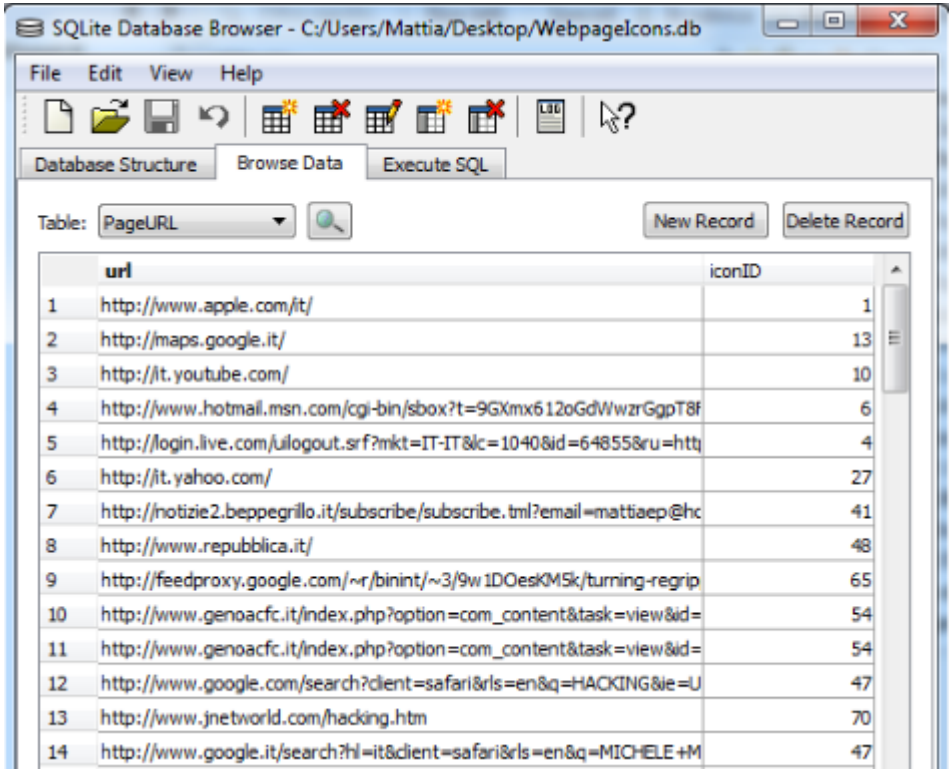


Analisi dei dati

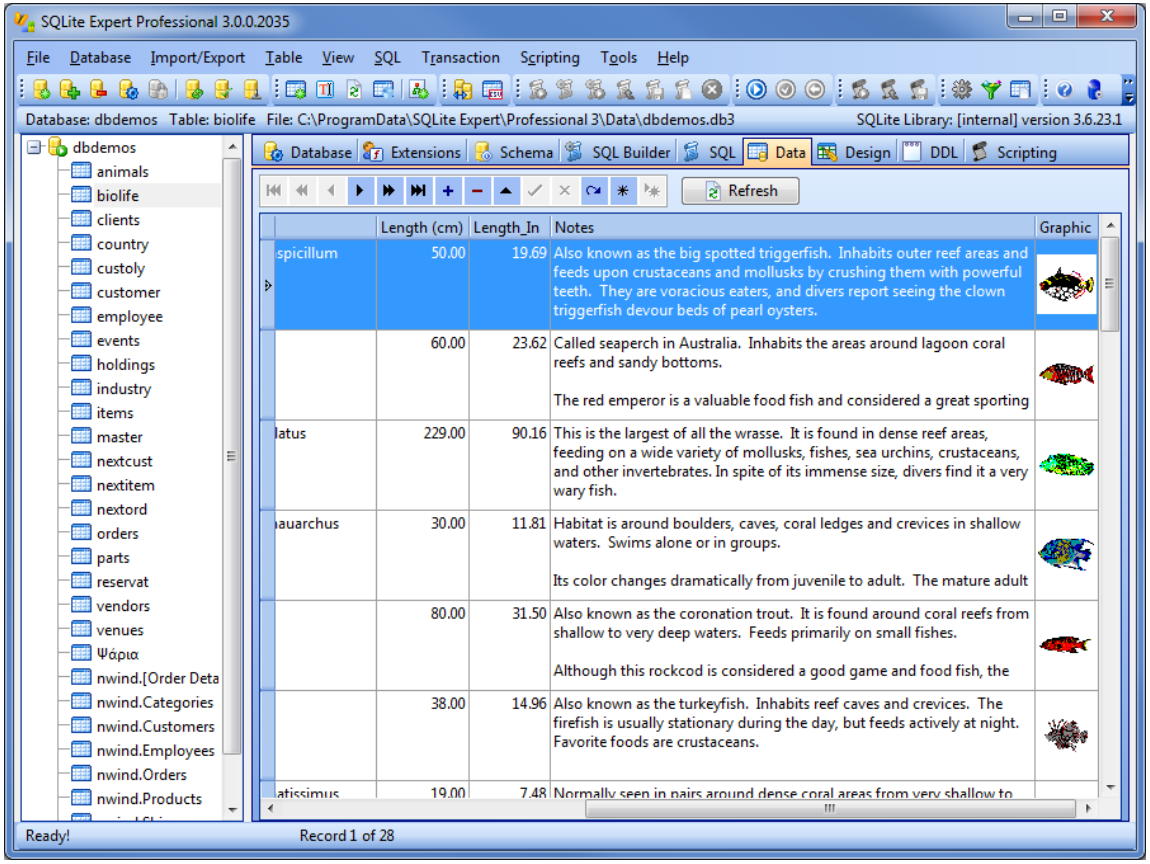
- I dati delle applicazioni sono salvati dal sistema operativo iOS utilizzando prevalentemente 2 strutture dati
  - **Property List File**
  - **Database SQLite**
- **La maggior parte delle informazioni di interesse da un punto di vista forense si trova quindi all'interno di file di questo tipo.**
- I file plist sono utilizzati per la **gestione dei file di configurazione del sistema operativo e dei principali applicativi** (analogo al registro di configurazione di Windows)
- I **database SQLite contengono i dati veri e propri**

Analisi dei dati
SQLite Database Browser

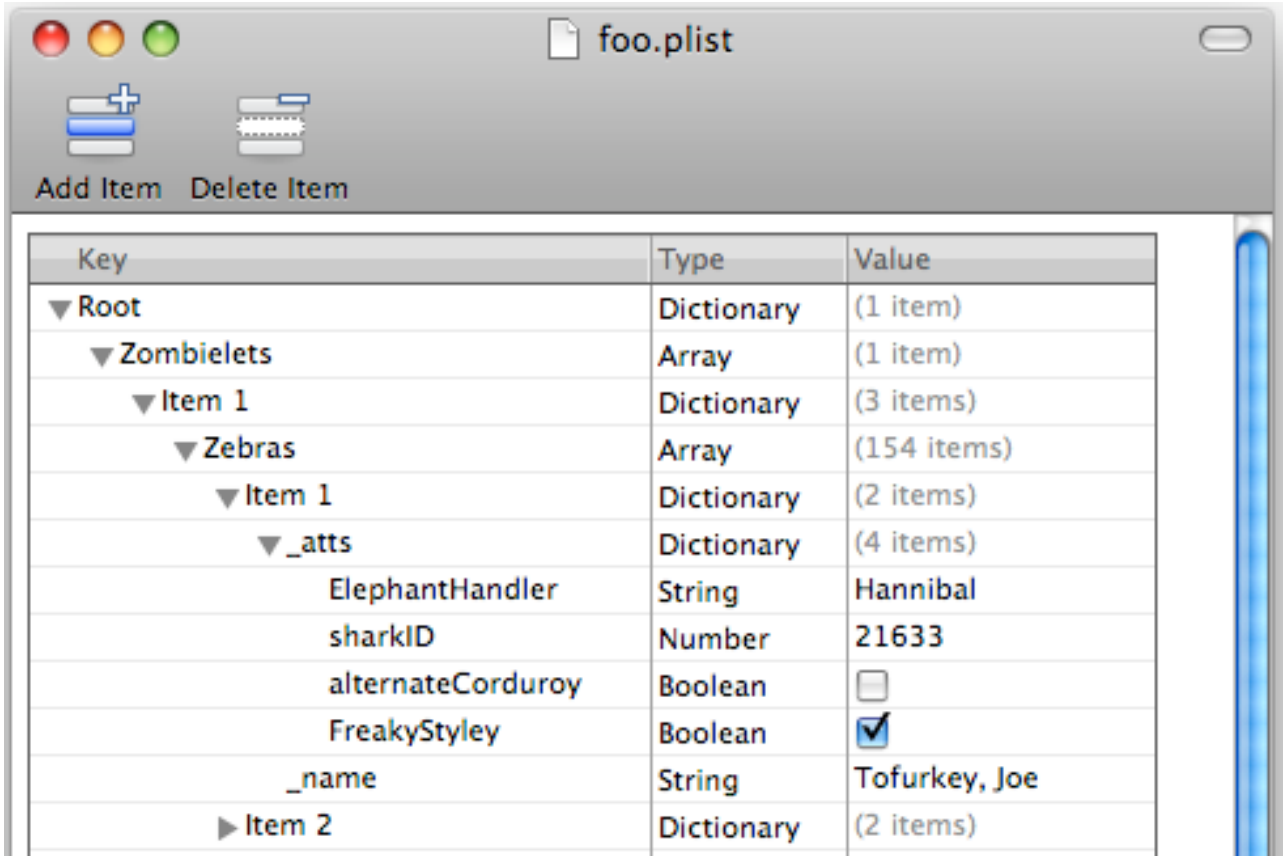




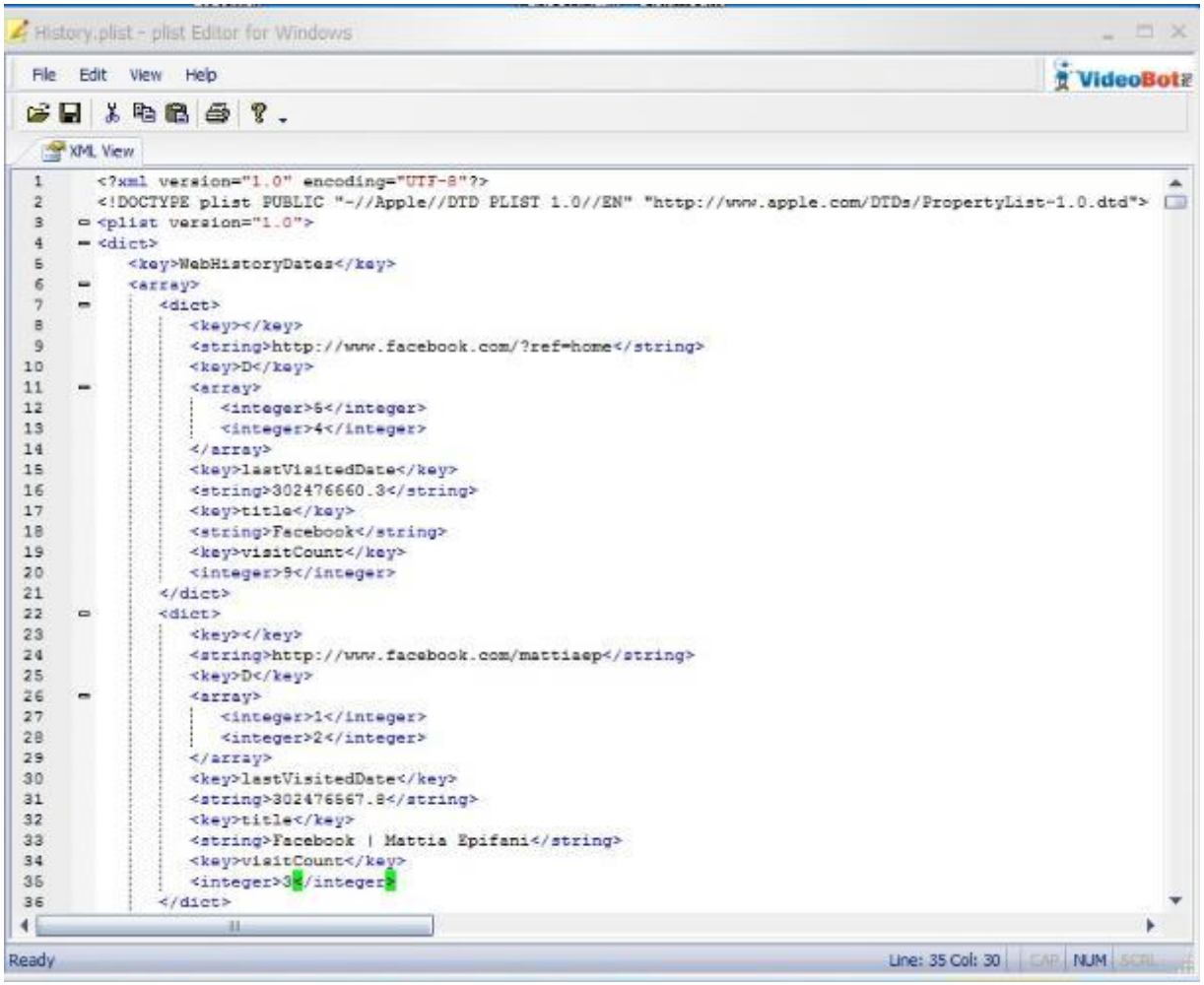
Analisi dei dati
SQLite Expert Professional



Analisi dei dati
Property List Editor for Mac



Analisi dei dati
plist Editor for Windows



Acquisizione logica: cosa trovo?

- Informazioni sul dispositivo e impostazioni
- Rubrica (elenco contatti e ultimi destinatari di messaggi di posta)
- Messaggi (SMS, MMS, iMessage)
- Registro Chiamate (Entrata, Uscita, Perse)
- Calendario
- Note
- Mappe (preferiti e ultime ricerche)
- Safari (cronologia, bookmarks, ultime finestre aperte, cache, cookies)
- Libri acquistati e scaricati
- Immagini e video (non cancellati)
- Configurazioni email (indirizzi ma **non il contenuto della posta**)
- Applicazioni (Skype, Whatsapp, Viber, ecc.)
- Dizionari
- Posizioni

Whatsapp Xtract

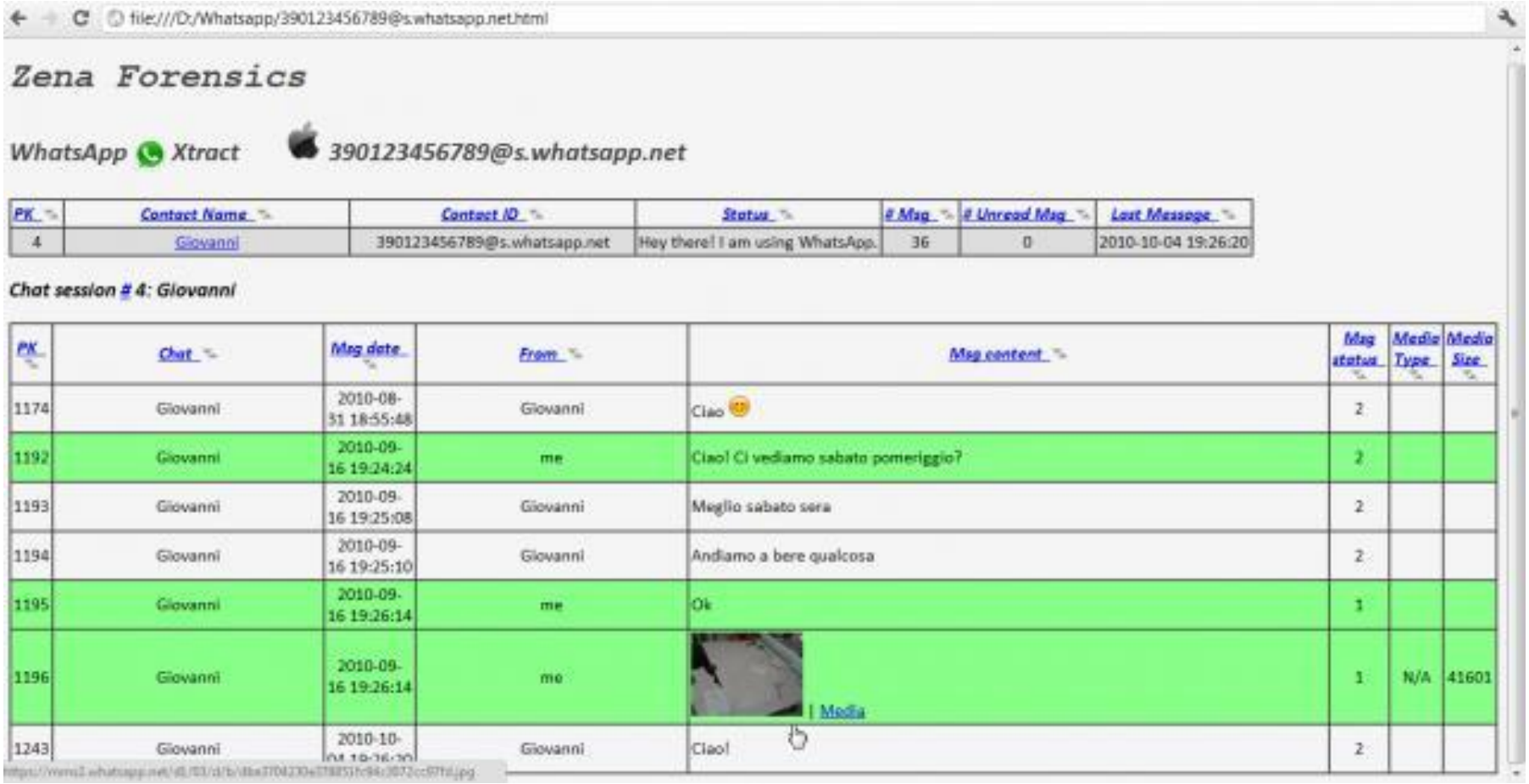
- Fabio Sangiacomo (fabio.sangiacomo@digital-forensics.it) ha realizzato un tool per il parsing delle chat di Whattsapp su dispositivi Android e iOS
- Il tool è liberamente scaricabile dal sito

  http://blog.digital-forensics.it/2012/05/whatsapp-forensics.html
- Nei dispositivi iOS Il database delle chat viene automaticamente inserito da iTunes all'interno di un backup

  Net.whatsapp.WhatsApp/Documents/ChatStorage.sqlite

- All'interno del database sono presenti 4 tabelle di interesse
  - ZWASTATUS contatti
  - ZWACHATSESSION sessioni di chat
  - ZWAMESSAGE messaggi
  - ZWAMEDIAITEM contenuti multimediali allegati

Whatsapp Xtract



file:///D:/Whatsapp/390123456789@s.whatsapp.net.html

Zena Forensics

WhatsApp Xtract 390123456789@s.whatsapp.net

PK	Contact Name	Contact ID	Status	# Msg	# Unread Msg	Last Message
4	Giovanni	390123456789@s.whatsapp.net	Hey there! I am using WhatsApp.	36	0	2010-10-04 19:26:20

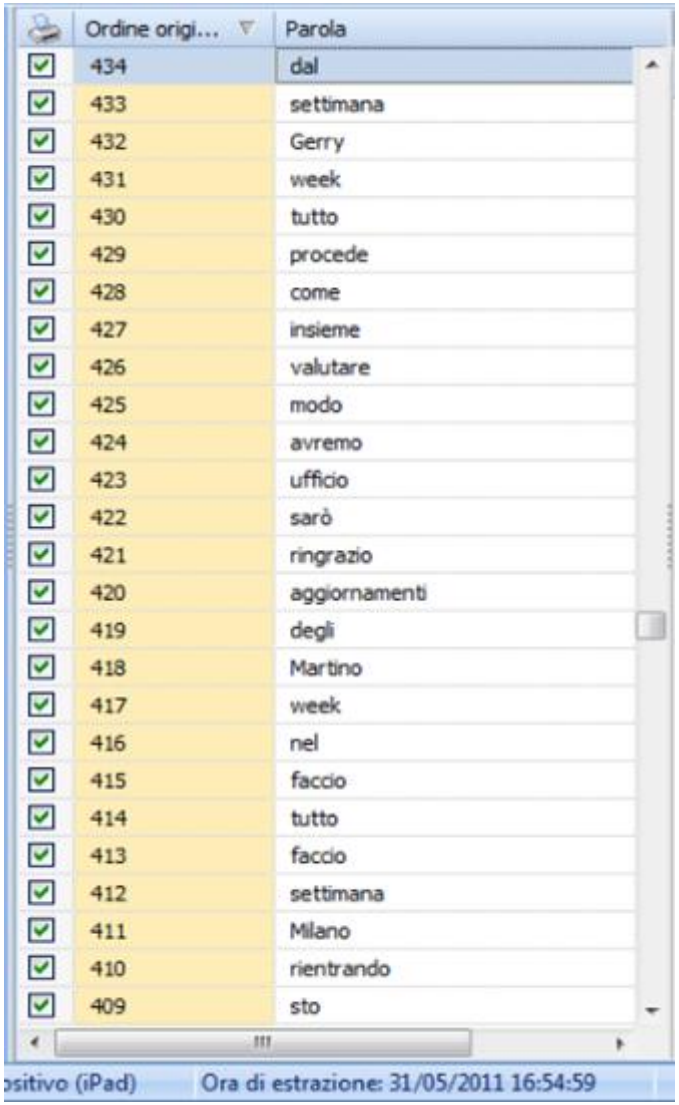
Chat session # 4: Giovanni

PK	Chat	Msg date	From	Msg content	Msg status	Media Type	Media Size
1174	Giovanni	2010-08-31 18:55:48	Giovanni	Ciao	2		
1192	Giovanni	2010-09-16 19:24:24	me	Ciao! Ci vediamo sabato pomeriggio?	2		
1193	Giovanni	2010-09-16 19:25:08	Giovanni	Meglio sabato sera	2		
1194	Giovanni	2010-09-16 19:25:10	Giovanni	Andiamo a bere qualcosa	2		
1195	Giovanni	2010-09-16 19:26:14	me	Ok	1		
1196	Giovanni	2010-09-16 19:26:14	me	| Media	1	N/A	41601
1243	Giovanni	2010-10-04 19:26:20	Giovanni	Ciao!	2		

Analisi dei dati Dizionario

Il file di testo **/mobile/Library/Keyboard/[locale]-dynamic-text.dat** contiene le parole digitate per semplificare la scrittura con la tastiera su schermo.

L'ordine cronologico delle parole permette spesso di estrarre frasi di senso compiuto.

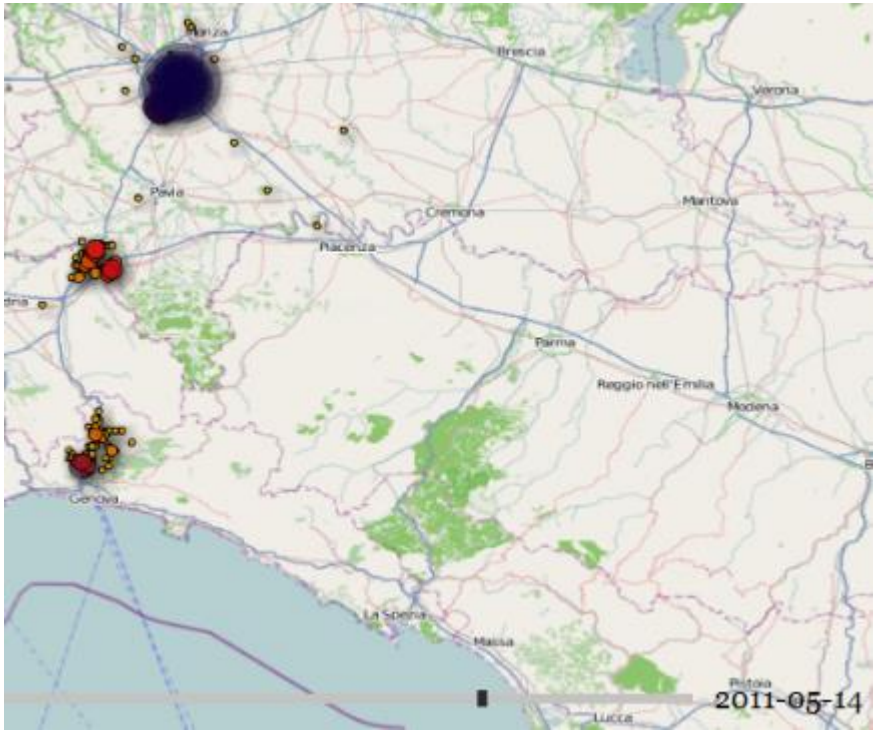


Ordine origi...	Parola
434	dal
433	settimana
432	Gerry
431	week
430	tutto
429	procede
428	come
427	insieme
426	valutare
425	modo
424	avremo
423	ufficio
422	sarò
421	ringrazio
420	aggiornamenti
419	degli
418	Martino
417	week
416	nel
415	faccio
414	tutto
413	faccio
412	settimana
411	Milano
410	rientrando
409	sto

sitivo (iPad) Ora di estrazione: 31/05/2011 16:54:59

Analisi dei dati Consolidated.db

- Da iOS 4.0 fino a iOS 4.3.2 venivano **salvati tutti gli hotspot Wi-Fi e celle agganciate e relativo timestamp**
- Dati salvati anche disabilitando il servizio di localizzazione in un database non cifrato
- Automaticamente salvato nei backup
- Bug scoperto nel aprile 2011 da Pete Warden e Alasdair Allen
- Corretto in iOS 4.3.3 e successivi



- Diversi tool freeware disponibili per l'analisi:
  - iPhoneTracker
    http://petewarden.github.com/iPhoneTracker
  - iPhoneTrackerWin
    http://huseyint.com/iPhoneTrackerWin/
  - iOS Tracker .NET
    http://tom.zickel.org/iostracker/

Acquisizione fisica

- Brute force del passcode
- Messaggi di posta elettronica
- Applicazioni di terze parti con codifica complessa
- Snapshot
- Immagini e video cancellati

Analisi dei dati
Snapshot

- Quando l'utente preme il tasto "Home" per uscire da un'applicazione e tornare alla schermata principale del dispositivo, **l'applicazione scatta uno snapshot che viene memorizzato nella cartella**

  /mobile/Library/Caches/Snapshots

- I file vengono **costantemente cancellati, tuttavia è possibile recuperarli mediate tecniche di file carving**
- Poiché tali immagini sono scattate in tempi casuali, a seconda dell'attività dell'utente, spesso contengono informazioni di interesse.
- Per esempio, **se un utente torna alla schermata principale mentre sta leggendo o componendo una mail è possibile recuperare un'immagine contenente il testo.**

Analisi dei dati
Carving di snapshot

- Sono stati effettuati test su dispositivo iPad di prima generazione, modello Wi-Fi + 3G, con 64 GB di spazio disco già utilizzato abitualmente per qualche mese sia per svago sia per lavoro
- Sul dispositivo esaminato sono stati recuperati:
  - 9.525 immagini in formato PNG
  - 1.808 immagini in formato JPEG
- Tra i file PNG molti erano riferibili a screenshot delle attività di navigazione su Internet tramite il browser Safari:
  - 758 screenshot di dimensione 218x290 pixel
  - 117 screenshot di dimensione 304x205 pixel
- La bassa risoluzione delle immagini non permette di leggere l'intero contenuto della pagina, ma è comunque possibile capire quali siti sono stati visitati.

Analisi dei dati
Carving di snapshot

- Tra i file JPG sono stati invece individuati **368 screenshot di dimensione 1004x768**, realizzati dal dispositivo durante il normale utilizzo dell'iPad da parte dell'utente.

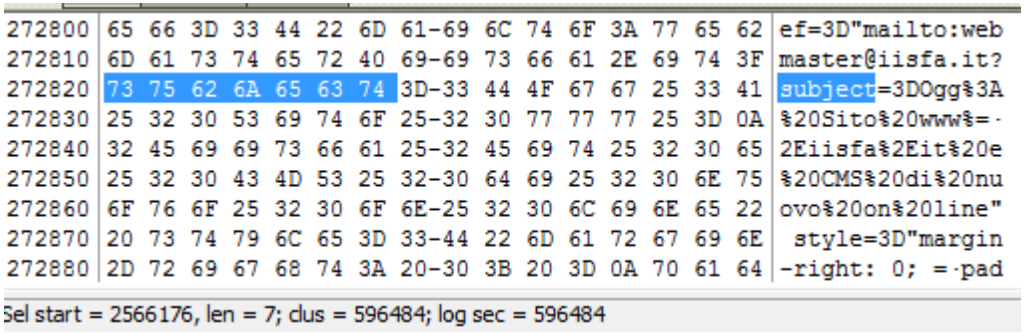
- Poiché i file sono stati recuperati tramite operazioni di carving, i metadati relativi alle date di creazione, modifica e accesso non sono presenti: **non è quindi possibile determinare per tutte le immagini il momento in cui queste siano state create**.

- All'interno di alcune immagini sono **tuttavia presenti riferimenti a date e ore che possono essere utili per costruire una timeline** ed eventualmente incrociare le informazioni con altre estratte durante l'acquisizione logica (es. cronologia di navigazione del browser Safari).

Analisi dei dati
Carving di snapshot

Analisi dei dati Keyword Search

- La ricerca per parola chiave è utile per recuperare informazioni cancellate e non estraibili mediante file carving.
- Un esempio è costituito dalle email in formato EMLX che sono cancellate dal dispositivo in modo logico (p.es accesso tramite IMAP)
- Le parole chiave che si possono utilizzare a tal fine sono:
  - Subject
  - References
  - From
  - Content-Transfer-Encoding
  - Content-Type
  - In-Reply-To
  - Message-Id
  - Mime-Version
  - Indirizzi email del mittente e del destinatario



Dispositivi senza codice di protezione

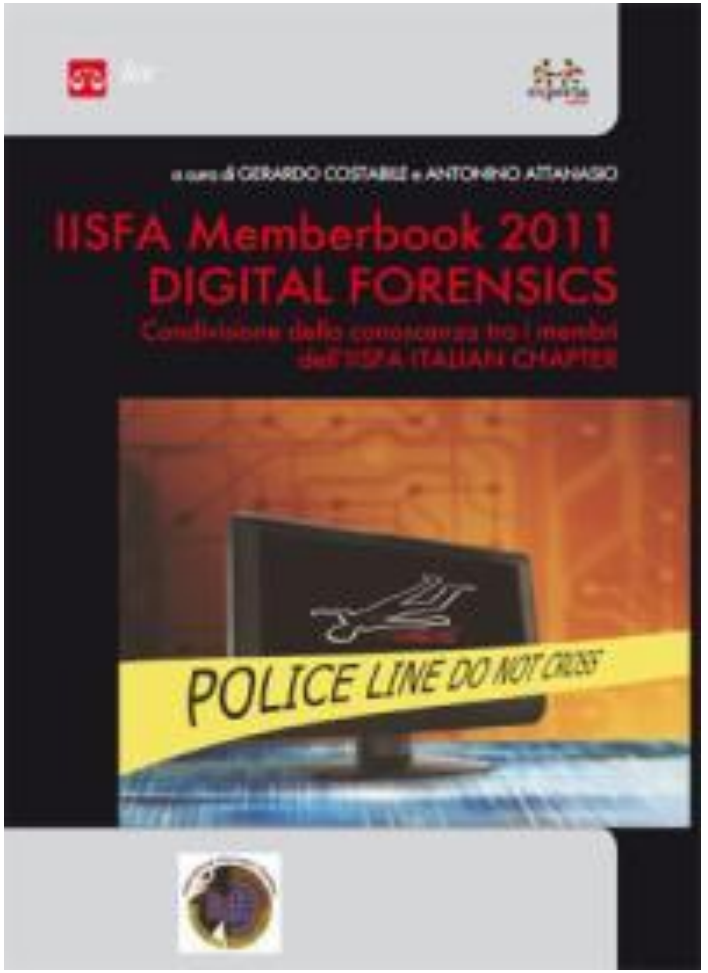
Modello	Acquisizione logica /Backup	Acquisizione fisica
iPhone 3G	Si	Si
iPhone 3Gs	Si	Si
iPhone 4	Si	Si
iPhone 4s	Si	Solo con jailbreaking
iPhone 5	Si	No
iPad	Si	Si
iPad 2	Si	Solo con jailbreaking
The new iPad	Si	

Dispositivi con codice di protezione

Modello	Acquisizione logica /Backup	Acquisizione fisica
iPhone 3G	Si, mediante modalità DFU Oppure con Lockdown File ricavabili da un PC/MAC utilizzato per sincronizzare il dispositivo	Si, previo bruteforce
iPhone 3Gs		
iPhone 4		
iPhone 4s	Lockdown File ricavabili da un PC/MAC utilizzato per sincronizzare il dispositivo	Solo se già jailbroken e con SSH installato
iPhone 5		No
iPad	Si, mediante modalità DFU Oppure con Lockdown File ricavabili da un PC/MAC utilizzato per sincronizzare il dispositivo	Si, previo bruteforce
iPad 2	Lockdown File Ricavabili da un PC/MAC utilizzato per sincronizzare il dispositivo	Solo se già jailbroken e con SSH installato
The new iPad		

Riferimenti

- «**iPad Forensics**», capitolo 9
- Dott. Mattia Epifani
- Dott. Litiano Piccin



Riferimenti

- **iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices**
  A. Hoog, K. Strzempka
  Syngress, 2011
- **iOS Forensic Analysis: for iPhone, iPad, and iPod touch**
  Sean Morrissey, Apress, 2010
- **Mac OS X, iPod, and iPhone Forensic Analysis DVD Toolkit**
  R. Kubasiak, S.Morrissey, J. Varsalone
  Syngress, 2008
- **iPhone 3GS Forensics: Logical analysis using Apple iTunes Backup Utility**
  M.Bader, I.Baggili
  http://www.ssddfj.org/papers/SSDDFJ_V4_1_Bader_Bagilli.pdf
- **Overcoming iOS data protection to re-enable iPhone forensic**
  A.Belenko
  https://media.blackhat.com/bh-us-11/Belenko/BH_US_11_Belenko_iOS_Forensics_WP.pdf
- **iOS Application Forensics**
  S.Edwards
  http://www.scribd.com/doc/57611934/CEIC-2011-iOS-Application-Forensics
- **Demystifing iPhone Forensics on iOS 5**
  http://securityxploded.com/demystifying-iphone-forensics-on-ios5.php

Mattia Epifani

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