

Mobile Forensics

Tecniche e strumenti per l'acquisizione e
l'analisi di dispositivi mobili

Mattia Epifani – Litiano Piccin



Clusit
Education

Chi sono

- Mattia Epifani
- Socio della REALITY NET – System Solutions
- Mi occupo di Digital Forensics dal 2008
- Responsabile formazione IISFA
- Presidente associazione DFA (Digital Forensics Alumni)
- Certificato CIFI, CHFI, CCE, ACE, ECCE, MPSC

IISFA

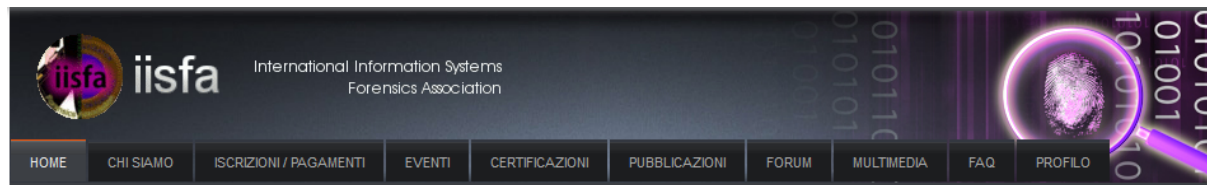
- **L'International Information Systems Forensics Association (IISFA)** è un'organizzazione senza scopo di lucro con la missione di **promuovere la disciplina dell'information forensics attraverso la divulgazione, l'apprendimento e la certificazione**
- L'associazione si compone di :
 - ◆ una **Board of Directors** che rappresenta la cabina di regia e di governo della stessa
 - ◆ Di un **Comitato Scientifico** ed un **Comitato Tecnico**, composti da esponenti di rilievo ed esperti del settore i quali, volontariamente, contribuiscono al raggiungimento degli obiettivi dell'associazione.

IISFA - Obiettivi

- **Rendere disponibile un ambiente professionale e stimolante per lo scambio di idee** e di informazioni relative alle tematiche del Forensics tra esperti del settore essendo anche il punto di riferimento per tutti coloro che si avvicinano a tali argomenti .
- **Combinare le esperienze reali con le conoscenze** dei professionisti dell'information security.
- Creare un **network di relazioni tra i membri dell'associazione**, favorendo la nascita di opportunità per il miglioramento e la crescita professionale.
- Difendere la cultura della professionalità anche attraverso la diffusione della **certificazione CIFI**.

IISFA - Formazione certificazione

- La formazione dei soci è uno dei punti chiave dello statuto dell'associazione IISFA – Italian Chapter
- L'offerta formativa dell'associazione comprende:
 - ◆ Seminari di aggiornamento
 - ◆ Convegni
 - ◆ Pubblicazioni
 - ◆ Sito web e newsletter
 - ◆ Corso Intensivo di Computer e Mobile Forensics
 - ◆ Corsi intensivi dedicati
 - ◆ Piattaforma di e-learning
 - ◆ Piattaforma di social network
 - ◆ Certificazione CIFI




News
Uscirà a breve l'ultima newsletter IISFA....



News
Corso Intensivo IISFA
Roma-Novembre 2011




News
Digital Profiling: A Computer Forensics Approach
Comunicato_Vienna (134.46 kB)



Altri articoli...

cerca...



Cerca Consulenti

> Cerca Consulenti

Login

Salve reallitynet,

Esci

Home

Benvenuto nel Portale IISFA

----- *IN EVIDENZA* -----
IISFA NETWORK
the New International Information System Forensics Network
[HTTP://IISFA-NETWORK.ORG](http://iisfa-network.org)

Cari Amici e Colleghi di IISFA,

il portale IISFA è cambiato e rinnovato, sia per la parte pubblica che, specialmente, per l'area riservata ai soci!

IISFA è l'organizzazione internazionale dei tecnici e giuristi impegnati nella promozione scientifica dell'informatica forense attraverso la divulgazione, l'apprendimento e la certificazione riconosciuta in ambito internazionale. In Italia, IISFA è presente dal 2007 come prima associazione con focus specifico sulla "Information Forensics".

Le attività ruotano intorno a un codice etico e alla partecipazione a un network di professionisti. IISFA realizza un programma formativo di eccellenza basato su seminari periodici con specifiche sessioni di laboratorio, corsi di alta formazione in Computer Forensics, forum, newsGroup, pubblicazioni/Quaderni, laboratori scientifici.

Il nostro scopo è altresì quello di costituire insieme, nel medio periodo, un punto di riferimento nello specifico settore, allo stato sottolineato da forti individualità. Questa strada non sarà facile perché l'Associazione è indipendente, ha un rigido codice etico ed ha una forte impostazione tecnico-scientifica

Se Vi riconoscete in queste caratteristiche, Vi aspettiamo!

Richiedete l'iscrizione all'Associazione tramite il modulo on line su questo portale!

Gerardo Costabile
Presidente IISFA Italia

IISFA Newsletter

Data __ Marzo 2011

Nr. 2 anno 1



International Information Systems Forensics Association

Newsletter 5



Editoriale:

In questa prima newsletter del 2011 riportiamo oltre agli articoli curati dai Soci, anche un reportage fotografico dell'IISFA Christmas 2010 e Convegno sul Cybercrime tenuto presso la bellissima struttura del Castello Arechi a Salerno e



Sommario:

Eventi IISFA	1
Di Massimiliano Graziani	
STRUMENTI PER L'ANALISI DEI SOFTWARE P2P	3
Di Mattia Epifani	
La copia di BACKUP	7

IISFA – Corsi intensivi

- **Corso Intensivo di Computer e Mobile Forensics**
 - ◆ 2 edizioni annuali
 - ◆ Milano (febbraio/marzo) e Roma (ottobre/novembre)
 - ◆ Sconti per soci CLUSIT, grazie a convenzione
 - ◆ Comprende il voucher per sostenere la certificazione CIFI

IISFA – Corsi dedicati

■ Corsi dedicati

- ◆ Windows Forensics (2 giorni)
- ◆ Macintosh Forensics (2 giorni)
- ◆ Memory Forensics (2 giorni)
- ◆ Malware Forensics (3 giorni)
- ◆ Live Forensics (1 giorno)
- ◆ Internet Forensics (1 giorno)
- ◆ Mobile Forensics (2 giorni)
- ◆ iOS Forensics (1 giorno)
- ◆ Android Forensics (1 giorno)

Preparation KIT CIFI

Sei collegato come **Mattia Epifani**. (Esci)

IISFA ▶ CIFI101

?

Cambia ruolo in ...

Attiva modifica

Persone

Partecipanti

Attività

Certificati
Chat
Compiti
Forum
giochi
Libri
Media Players
Questionari
Quiz
Risorse
SCORM/AICC
Wiki

Ricerca nei forum

Vai

Ricerca avanzata

Amministrazione

Attiva modifica
Impostazioni
Ruoli
Valutazioni
Obiettivi
Corsi figli
Gruppi
Backup
Ripristina

Attività settimanale

- Forum News
- CHAT
- Wiki Forensics
- Attestato di superamento del Corso - 10 cpe e Voucher Gratuito CIFI
- Study Guide
- File didattici
- INCIDENT RESPONSE
- QUIZ - CIFI - SKILL TEST
- QUIZ - CIFI Preparation KIT
- QUIZ di preparazione alla CIFI
- QUIZ -Basic preparation kit
- EXAM - CIFI FINAL TEST
- Seminario sul Phishing
- ISTRUZIONI PER LA COMPILAZIONE E CONSEGNA DEI COMPITI
- Compito Nr.1 - Sample Unallocated Clusters (Liv. BASE)
- File - Compito nr.1- Sample Unallocated Clusters
- Compito nr.2 - Password recovery (Liv. BASE)
- File Compito nr. 2 - Password Recovery
- Compito nr.3 - Network (Liv. BASE)
- File Compito nr.3 - Network
- Compito nr.4 - Attacco Terroristico (Liv. BASE)
- File Compito nr.4 - Attacco Terroristico
- Compito nr. 5 - Puzzle Forensics (LIV. MEDIO)
- File Compito nr.5 - Puzzle Forensics
- Compito nr.6 - Ricostruzione dei File Header (liv. medio)
- File nr.6 - Ricostruzione dei File Header (liv. medio)
- Compito nr.7 - Crypto Analysis - (Liv. Base)
- Compito nr.8 - Network Intrusion - Liv (HARD)
- File nr.8 - Network Intrusion - Liv (HARD)
- Compito nr.9 . Validazione di un write blocker
- Compito nr.10 Liv. (HARD) NTFS File Record

Ultime notizie

Aggiungi nuovo argomento...

26 ott, 10:49

Giuseppe Mazzaraco
Piattaforma di social network - iisfa (Messaggio del presidente) leggi...

20 ott, 16:09

Giuseppe Mazzaraco
CIFI 2.0 - ESAME DA REMOTO leggi...

20 ott, 11:50

Gianfranco D'alena
risposte errate su quiz cifi
leggi...

30 apr, 17:23

Francesco Acchiappati
Perplexità su entry \$MFT
leggi...

17 apr, 17:35

Giuseppe Mazzaraco
CYBERCOP 2011 - CERCASI COMPONENTI SQUADRE
leggi...

Argomenti precedenti ...

Attività recente

Attività a partire da martedì, 25 ottobre 2011, 13:23
Report completo dell'attività recente...

http://iisfa-network.org/

The screenshot shows the IISFA Network website forums page. At the top, there is a banner with the IISFA logo and the text "International Information Systems Forensics Association". Below the banner is a navigation menu with buttons for Home, People, Spy, Tags, Forums, Categories, Photos, Videos, Files, and a search icon. The "Forums" button is highlighted. Below the navigation menu is a "Forums" section with a document icon and the word "Forums". Underneath, there is a "Forums Home" section with links for Forums Index, Subscriptions, My Topics, Spy, and Search. The main content area is divided into two columns. The left column is titled "Forums Index" and contains sections for "Normativa" (with links for Sentenze su casi reali, Normativa Aziendale e Computer Forensics, and Richieste dai tecnici ai giuristi), "DIGITAL INVESTIGATION" (with a link for Digital Forensics), and "General" (with a link for General discussions). The right column is titled "Recent Topics" and contains three entries: "EnCase Forensic version 7.01 has been released" (created by Certification 01.07.2011 05:12, last reply by Certification 01.07.2011 05:12, 1 posts), "WEBCASE - Online Evidence Tool -" (created by Certification 24.05.2011 08:56, last reply by Certification 24.05.2011 08:56, 1 posts), and "EnCase Forensic version 6.18.1" (created by Certification 23.05.2011 02:46, last reply by Certification 23.05.2011 02:46, 1 posts). At the bottom of the "Recent Topics" section, there is a pagination control showing "1-3 of 3" and navigation arrows. At the very bottom of the page, there is a footer with links for "about us", "privacy", "terms", "faq", "invite a friend", "contact us", and "bookmark", and a copyright notice "Copyright © 2011 IISFA .".



IISFA FORUM & CYBERCOP CHALLENGE 2012

Computer Forensics & Digital Investigation

Venerdì 18 maggio 2012

Castello di Arechi - via Frà Generoso, Salerno

Sabato 19 maggio 2012

Castello di Arechi - via Frà Generoso, Salerno





PROGRAMMA

Venerdì 18 maggio 2012

Castello di Arechi, Salerno

ore 9.30

INDIRIZZI DI SALUTO

On. Edmondo Cirielli – Presidente Provincia di Salerno
Prof. Raimondo Pasquino - Magnifico Rettore Università di Salerno
Prefettura di Salerno
Dr. Antonio De Iesu - Questore di Salerno
Diego Di Simone – Responsabile Sicurezza Confindustria
Gerardo Costabile – IISFA Italian Chapter - Presidente

ore 10.00

INFORMATICA FORENSE, SPIONAGGIO INDUSTRIALE E INFEDeltÀ AZIENDALE

Sessione Mattutina

Chairman: Avv. Mario Ianulardo - Avvocato in Napoli

Fraud Prevention Program e Best practices per le organizzazioni aziendali

Fabio Tortora - Presidente dell'Association of Certified Fraud Examiner (ACFE)

Spionaggio industriale ed indagini informatiche nell'esperienza investigativa nazionale

Sergio Mariotti - Primo Dirigente Servizio Polizia Postale e delle Comunicazioni

COFFEE BREAK

Furto di informazioni e infedeltà aziendale: aspetti giuridici e tecnologici della tutela del segreto aziendale

Avv. Raffaele Zallone
Studio Zallone - Milano

Social Network e indagini aziendali: aspetti tecnici

Matteo Flora - CEO The Fool srl – esperto di informatica forense

ore 13.30-14.45 Pausa Pranzo

ore 15.00

TABLET, IPHONE E BLACKBERRY: MOBILE INVESTIGATION & FORENSICS

Sessione Pomeridiana

Chairman: Prof. Alfredo De Santis,
Università di Salerno

iOS and BlackBerry Forensics

Andrey Belenko - Chief Security Researcher - ElcomSoft Co. Ltd.

Attività di Mobile Forensics su dispositivi danneggiati: ricostruzione, acquisizione, analisi forense

Ing. Giuseppe Finizia
Computer forensics Expert

COFFEE BREAK

Intercettazioni, multicanalità e crittografia

Ing. Maurizio Bedarida - JNP Forensics

Reti Mobili 4G, tecnologie Long Term Evolution ed indagini tecniche

Fabrizio Marcelli - Information Security Governance Manager



Cosa vedremo

- Definizione di Digital Forensics e Digital Evidence
- Identificazione, isolamento e repertamento di dispositivi mobile
- Acquisizione di SIM Card e memoria interna (logica e/o fisica)
- Case study:
 - ◆ iOS
 - ◆ Android
 - ◆ Blackberry
 - ◆ Symbian

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**
 - ◆ Se la digital evidence si trova su Internet (sito web, profilo di social network, ecc.), **può essere modificata e/o rimossa dall'owner della pagina**

Passi operativi

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

Identificazione

- La fase di identificazione avviene in corrispondenza dell'**analisi della scena del crimine**
- Il processo di identificazione deve seguire le cosiddette **“best practises”**
- Esempi di contenitori di dati possono essere:
 - ◆ Personal computer, notebook e server
 - ◆ Hard disk non inseriti nel computer (smontati o esterni)
 - ◆ Dischi allo stato solido
 - ◆ Network Attached Storage (NAS)
 - ◆ Floppy disks
 - ◆ Nastri di backup
 - ◆ Cartucce ZIP/JAZ
 - ◆ CD/DVD/BluRay
 - ◆ Memory card
 - ◆ USB Drives
 - ◆ MP3 Player, Videocamere, Fotocamere digitali
 - ◆ Dispositivi di rete (Router, Switch, Firewall, IDS/IPS, Syslog Server)
 - ◆ **Dispositivi mobile (telefoni cellulari, SIM, SmartPhone, Tablet, Navigatori satellitari)**

Cellulari/Smartphone/Tablet Classificazione NIST (hardware)

Table 1: Hardware Characterization

	Basic	Advanced	Smart
Processor	Limited Speed	Improved Speed	Superior Speed
Memory	Limited Capacity	Improved Capacity	Superior Capacity, Built-in Hard Drive Possibility
Display	Grayscale	Color	Large size, 16-bit Color (65,536 colors) or Higher
Card Slots	None	MiniSD or MMCmobile	MiniSDIO or MMCmobile
Camera	None	Still	Still, Video
Text Input	Numeric Keypad	Numeric Keypad, Soft Keyboard	Touch Screen, Handwriting Recognition, Built-in QWERTY-style Keyboard
Cell Interface	Voice and Limited Data	Voice and High Speed Data	Voice and Very High Speed Data
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, WiFi
Battery	Fixed, Rechargeable Lithium Ion Polymer	Removable, Rechargeable Lithium Ion Polymer	Removable, Rechargeable Lithium Ion

Cellulari/Smartphone/Tablet Classificazione NIST (software)

Table 2: Software Characterization

	Basic	Advanced	Smart
OS	Proprietary	Proprietary	Linux, Windows Mobile, RIM OS, Palm OS, Symbian
PIM	Simple Phonebook	Phonebook and Calendar	Reminder List, Enhanced Phonebook and Calendar
Applications	None	MP3 Player	MP3 Player, Office Document Viewing
Messaging	Text Messaging	Text with Simple Embedded Images and Sounds (Enhanced Text)	Text, Enhanced Text, Full Multimedia Messaging
Chat	None	SMS Chat	Instant Messaging
Email	None	Via Network Operator's Service Gateway	Via POP or IMAP Server
Web	None	Via WAP Gateway	Direct HTTP
Wireless	IrDA	IrDA, Bluetooth	IrDA, Bluetooth, WiFi

Tecnologia di trasmissione

- A livello europeo la tecnologia dominante è il **GSM (Global System for Mobile Communication)**
- Gli standard 2G e 3G (evoluzione del GSM) più noti sono:
 - ◆ **GPRS (General Packet Radio Service)**
 - ◆ **EDGE (Enhanced Data Rates for GSM Evolution)**
 - ◆ **3GSM**
 - ◆ **UMTS (Universal Mobile Telecommunications System)**
 - ◆ **HSPA (High Speed Packet Access)**
- Lo standard di prossima generazione 4G è l'**LTE Advanced**

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**
- 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



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:
 - ◆ **Integrated Circuit Card Identification (ICCID)**
 - ◆ **International Mobile Subscriber Identity (IMSI)**
- 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

Example: 8923440000000000003

Information on SIM card number

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

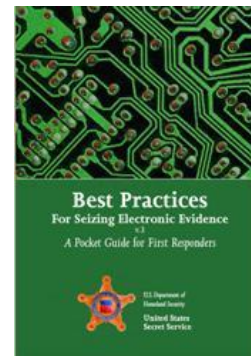
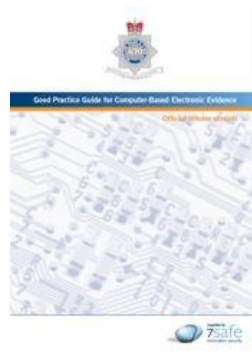


Repertamento

- 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**” per il repertamento
 - ◆ 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)
 - ◆ ISO 27037 (Draft) - Guidelines for identification, collection, acquisition and preservation of digital evidence
 - ◆ Model Standard Operating Procedures for Computer Forensics – SWGDE (Scientific Working Group on Digital Evidence) (2011)



Computer spento

- **Mettere in sicurezza la scena** e prendere il controllo dell'area che contiene il dispositivo
- **Allontanare le persone presenti** dal computer e dai dispositivi di alimentazione
- **Fotografare o fare una ripresa video della scena del crimine** e di tutte le componenti interessate.
- Se non è disponibile una fotocamera, **disegnare la scena**
- **Assicurarsi che il computer sia effettivamente spento.** Alcuni screen saver o modalità del computer (es. stand-by) possono far apparire il computer come spento quando è ancora acceso
- **NON ACCENDERE IL COMPUTER PER NESSUN MOTIVO**

Computer spento

- **Rimuovere la batteria (se notebook)**, verificando prima che il notebook non si trovi in standby
- **Scollegare l'alimentazione** e gli altri dispositivi dal lato del computer (per evitare problemi in caso di UPS)
- **Etichettare le porte e i cavi** in modo tale da poter ricostruire il computer successivamente
- Assicurarsi che tutte **gli oggetti siano stati siglati** e compilare un report di sequestro per ciascuno
- Ricercare sulla scena del crimine **diari, appunti o pezzi di carta con password**, che spesso si trovano attaccati o vicini al computer
- Valutare se chiedere all'utente informazioni sul setup del sistema, incluse password di accesso
- **Prendere nota dettagliata di tutte le operazioni compiute in relazione ai dispositivi informatici**

Computer accesso

- **Mettere in sicurezza la scena** e prendere il controllo dell'area che contiene il dispositivo
- **Allontanare le persone presenti** da tutti i computer e i dispositivi di alimentazione
- **Fotografare o fare una ripresa video della scena** del crimine e di tutte le componenti interessate.
- Se non è disponibile una fotocamera, **disegnare la scena** e etichettare le porte e i cavi in modo tale che il sistema possa essere ricostruito successivamente
- Valutare se chiedere all'utente informazioni sul setup del sistema, incluse password di accesso
- **Registrare le informazioni presenti sul monitor, effettuando fotografie e trascrivendo il testo visibile**
- **Non toccare la tastiera o fare click con il mouse**

Computer accesso

- Qualora lo si ritenga necessario o indispensabile, **estrarre le informazioni che andrebbero sicuramente perse** (processi in esecuzione, stato della rete, ecc.) (**LIVE FORENSICS**)
- **Assicurare che tutte le azioni eseguite e le modifiche apportate al sistema siano note e registrate**
- Se non è disponibile **uno specialista per l'analisi live, scollegare l'alimentazione e gli altri dispositivi dal lato del computer** (per evitare problemi in caso di UPS) **senza chiudere alcun programma**
- **Rimuovere tutte le altre connessioni in uscita dal computer verso la rete o verso altri dispositivi esterni**
- Assicurarsi che tutte gli **oggetti siano stati siglati e compilare un report di sequestro per ciascuno**
- Ricercare sulla scenda del crimine diari, **appunti o pezzi di carta con password**, che spesso si trovano attaccati o vicini al computer
- Prendere nota dettagliata di tutte **le operazioni compiute in relazione ai dispositivi informatici**

Live Forensics: necessità vs. invasività

- Un intervento di *live forensics* si rende necessario (o molto utile) quando:
 - ◆ Il sistema **non è fisicamente rimovibile**
 - ◆ Il sistema **non può essere spento**
 - Militari
 - Videosorveglianza
 - Strumenti medicali
 - Database server condivisi
 - Server in hosting/housing
 - ◆ Il sistema **non può essere acquisito nella sua interezza**
 - ◆ **Le informazioni “volatili” sono rilevanti** rispetto alle indagini (es. traffico di dati di rete in corso, come il trasferimento di un file)
 - ◆ Siamo in presenza di **volumi cifrati** (BitLocker, TrueCrypt, PGP, ecc.)

Live Forensics: necessità vs. invasività

- Per contro utilizzando tecniche di *live forensics*:
 - ◆ Il sistema viene **sicuramente perturbato**:
 - Le modifiche apportate sono note?
 - Le modifiche apportate sono documentabili?
 - Le modifiche apportate intaccano significativamente il risultato dell'analisi?
 - Ogni modifica apportata può distruggere un altro dato...
 - ◆ **Gli accertamenti svolti su sistemi accesi non saranno ripetibili**

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

- ◆ **Spegnere 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

- Il principio di funzionamento è molto semplice e basato sull'idea di **riprodurre un segnale portante sull'intera banda utilizzata dai canali di comunicazione.**
- Un generatore di tensione variabile invia in ingresso ad un oscillatore-modulatore una tensione variabile che produce in uscita un segnale variabile (disturbo)
- Tale segnale, opportunamente amplificato, viene inviato nell'etere attraverso un'antenna omnidirezionale ad alto guadagno
- **Tutto ciò che si trova nelle immediate vicinanze e lavora su una frequenza compresa nel range variabile dell'oscillatore-modulatore viene disturbato**
- Esistono dispositivi di Jamming per il disturbo in contemporanea di reti GSM, UMTS, Wi-Fi e Bluetooth
- **Soluzione migliore, ma è legale?**

Jammer



Gabbia di Faraday

- Teoricamente è un contenitore perfettamente isolato elettromagneticamente dall'esterno
- **Un qualsiasi dispositivo inserito dentro che utilizzi onde radio rimane isolato.** Le onde infatti non possono penetrare al suo interno
- Il linea pratica, il rivestimento dell'involucro non è perfettamente conduttore e quindi **non esiste la gabbia perfetta**
- **Il segnale non viene quindi annullato bensì notevolmente ridotto**
- I produttori offrono schede tecniche dettagliate e sono disponibili in rete i risultati dei test effettuati con diversi dispositivi e in diverse situazioni

Gabbia di Faraday



PARABEN'S WIRELESS EVIDENCE BAG

Case # _____ Date _____ Officer _____
Collected By: _____ (Name/Title) _____ (Date/Location)
Description of Item: _____
Location Found: _____

CHAIN OF CUSTODY

DATE	TIME	RECEIVED FROM	BY	PURPOSE/REASON

PARABEN'S WIRELESS EVIDENCE BAG

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

- Il principio fondamentale della fase di acquisizione in ambito di Digital Forensics consiste nel **preservare lo stato del dispositivo originale e di effettuarne una copia forense**
- Quando i dati sono conservati all'interno di un hard disk sono note **tecniche per la duplicazione mediante l'apposizione di blocchi in scrittura (hardware e/o software) che prevengano l'alterazione delle informazioni**
- Per garantire l'acquisizione di tutti i dati presenti sul dispositivo è opportuno (ove possibile) effettuare una **copia bit-a-bit (o bit-stream o copia forense o immagine)** del supporto originale, ovvero una **copia esatta del supporto originale**
- Questa operazione è differente da un semplice backup dei dati, che consiste nella copia di file noti e trascurando lo spazio non allocato
- **L'acquisizione viene solitamente effettuata leggendo ogni bit del supporto originale (prevenendo qualsiasi possibile scrittura) e scrivendo un file immagine su un supporto esterno (disco USB o network)**

Acquisizione (duplicatori)



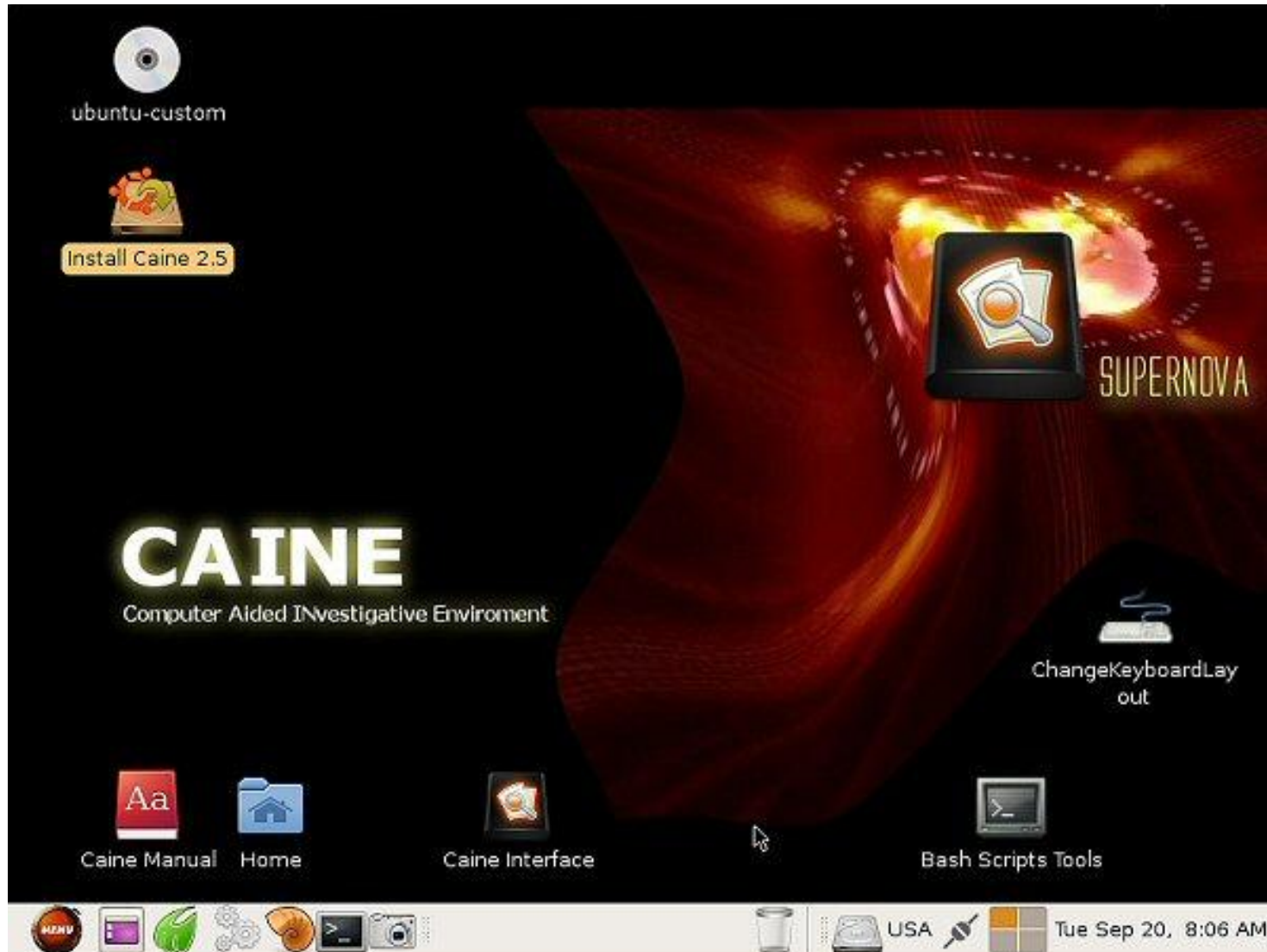
Acquisizione (write blocker)



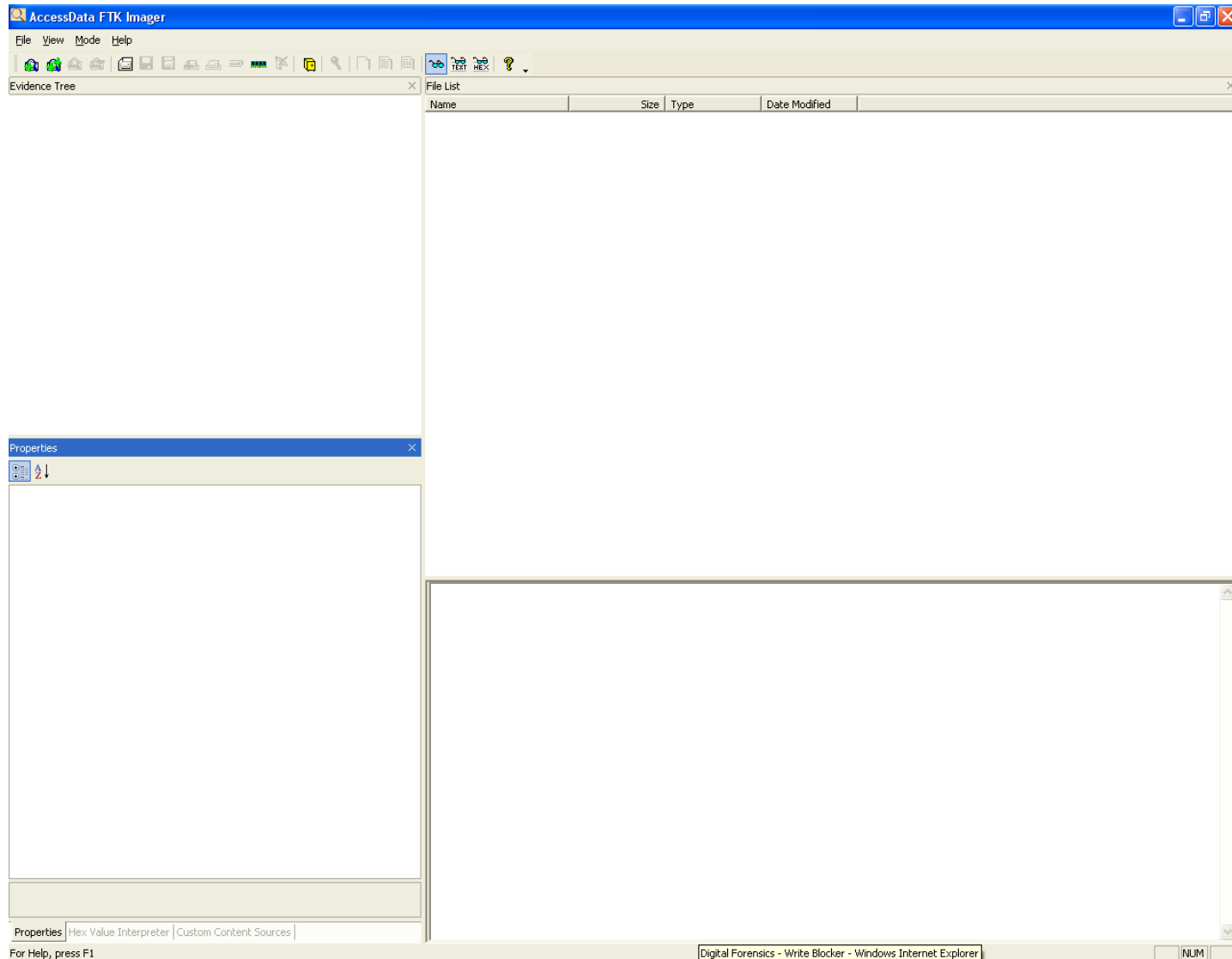
DEFT



CAINE



FTK Imager



Acquisizione di dispositivi mobile

- Quando i dati sono conservati all'interno di memorie saldate in dispositivi mobile (es. SmartPhone e Tablet), **l'operazione di rimozione del chip può essere complesso e addirittura inutile** (es. in caso di cifratura dei dati)
- Per questo motivo **l'acquisizione dei dati viene solitamente effettuata utilizzando il dispositivo stesso**
- Poiché questa operazione può comportare la modifica di informazioni presenti nella memoria, **è consigliabile trattarla come accertamento tecnico non ripetibile**
- **Non esiste un unico strumento in grado di operare su tutti i modelli di dispositivi mobile**
- In base al tipo di dispositivo da acquisire sarà necessario scegliere il tool da utilizzare per l'investigazione

Mobile Forensics Central



THE DIGITAL INVESTIGATOR'S RESOURCE FOR MOBILE DEVICE FORENSIC INFORMATION

New to MFC? [Start here](#)
Already Registered? [Sign-in](#)

Find a Phone (enter make/model)

[Browse Phones](#) [go](#)

[Products](#) : [Product Updates](#) : [Product Matrix](#) : [Education Center](#) : [News](#) : [Examiners Exchange](#) : [About](#)

Industry Info and News >

Cellular Phone Evidence -
Data Extraction and
Documentation

by Det. Cindy Murphy

Announcing the... MFC SCRIPT EXCHANGE

A place for practitioners to submit, share and validate
mobile device data scripts.

[Submit Your Script](#)

PRODUCT UPDATES

- Oxygen Forensic Suite 2011 2012 4.204/11/2012
- Secure View 3.6.1 04/03/2012
- Lantern 2.2.3 03/28/2012
- .XRY 6.2.0 03/21/2012

[more info »](#)

Find a Phone

Search the MFC database to obtain a **Phone Report** that delivers a detailed list of Mobile Device Forensic Software, Tools & Accessories for the mobile device you specify.



Search the Mobile Forensics Central Database

Enter Make/Model:

[go](#)

or

Search by Make and Model

Make:

-- choose phone make --

Model:

-- choose phone model --

[go](#)

MOBILE FORENSICS CENTRAL

Providing Essential Information
for Mobile Device Analysis

- Generate Custom PHONE REPORT
- Find Compatible Software and Cables
- Get Latest Updates from Software Providers
- Learn of Training Opportunities
- Read Papers and Articles
- Join Industry Forums

[browse products](#)

[View Sample
Phone Report](#)



Browse the
MFC
Product
Database



Get the **Latest!**

Industry News
& Software Updates

[click
here](#)

Looking for Training?
Need Outside Resources?

Visit the MFC
Education Center

[go](#)



Isolamento

- Analogamente all'isolamento in fase di sequestro, anche in fase di analisi in laboratorio si dovrà garantire l'isolamento dalle frequenze radio
- Le tecniche disponibili sono (in parte) simili a quelle già illustrate per la fase di sequestro:
 - ◆ **Jammer**
 - ◆ **Gabbia di Faraday**
 - ◆ **Airplane mode**
 - ◆ **SIM Cloning**
 - ◆ **Richiesta di blocco all'operatore**

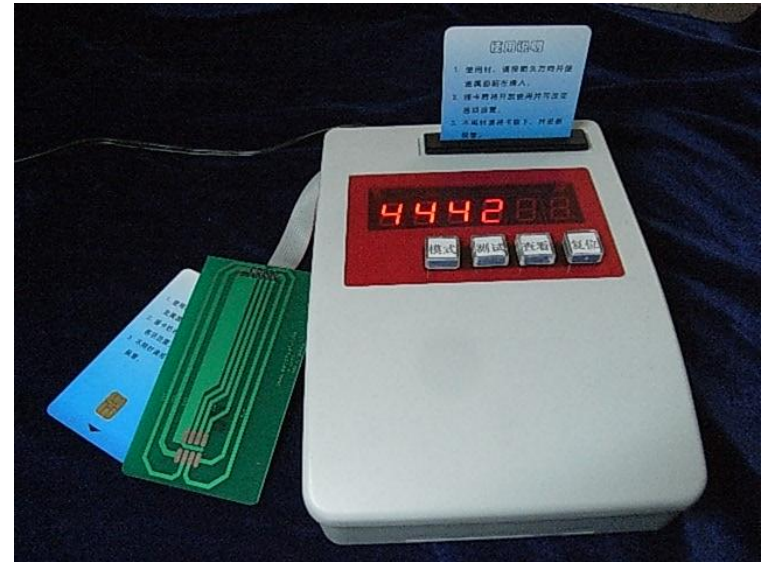
Faraday Tent



SIM Cloning

- Ad ogni accensione alcuni dei moderni cellulari **verificano se la SIM inserita è diversa dalla SIM precedentemente contenuta nel dispositivo**
- Nel caso in cui la SIM risulti cambiata **il telefono elimina alcune informazioni** (es. SMS, MMS, elenco delle chiamate perse, ricevute e fatte, ecc.)
- Per ovviare a tale inconveniente si può utilizzare la tecnica di **SIM Cloning** ovvero viene inserita una SIM “CLONATA” che riporta lo stesso **IMSI** e **ICCID** dell’originale.
- L’unica differenza è che questa SIM **non permette di connettersi ad un operatore di telefonia**
- E’ una tecnica molto efficace, che tuttavia **non previene le alterazioni derivanti da reti Wi-Fi, connessioni bluetooth o GPS** e deve quindi essere utilizzate insieme ad altre tecniche

SIM Cloning



Blocco da parte dell'operatore

- La richiesta del **blocco dell'utenza al Network Service Provider** è un'ottima alternativa al SIM Cloning, tuttavia
 - ◆ Richiede molto tempo
 - ◆ Non è sempre praticabile quando la SIM è di proprietà di un operatore estero
- Analogamente al SIM cloning, **non previene le alterazioni derivanti da reti Wi-Fi, connessioni bluetooth o GPS** e deve quindi essere utilizzate insieme ad altre tecniche

Identificazione del dispositivo

- Al fine di individuare il miglior tool per l'acquisizione è necessario identificare **marca** e **modello** del dispositivo
- Per identificare il dispositivo sono disponibili diverse tecniche:
 - ◆ **Caratteristiche fisiche del dispositivo**
 - ◆ **Interfacce del dispositivo** (es. alimentatore)
 - ◆ **Etichette presenti sul dispositivo**
- Un altro aspetto utile da identificare è il **codice IMEI**
 - ◆ Se il dispositivo è **spento**, le informazioni si trovano solitamente sotto la batteria o sul retro dello stesso (es. iPhone/iPad)
 - ◆ Se il dispositivo è **acceso**, è possibile identificarne il suo IMEI digitando la combinazione di tasti ***#06#**

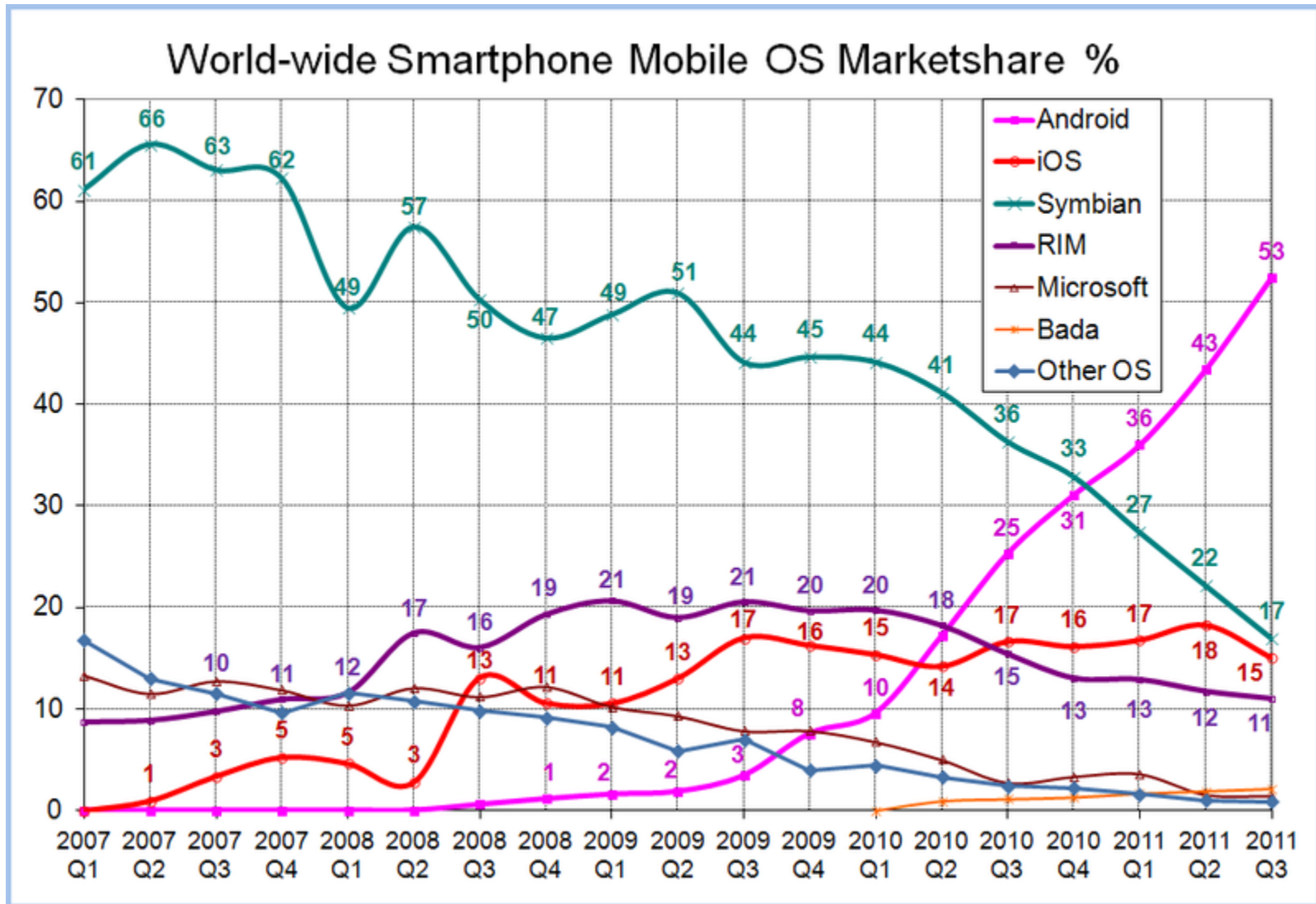
Acquisizione di dispositivi mobile

- 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



Sistemi operativi mobile



Acquisizione di dispositivi mobile

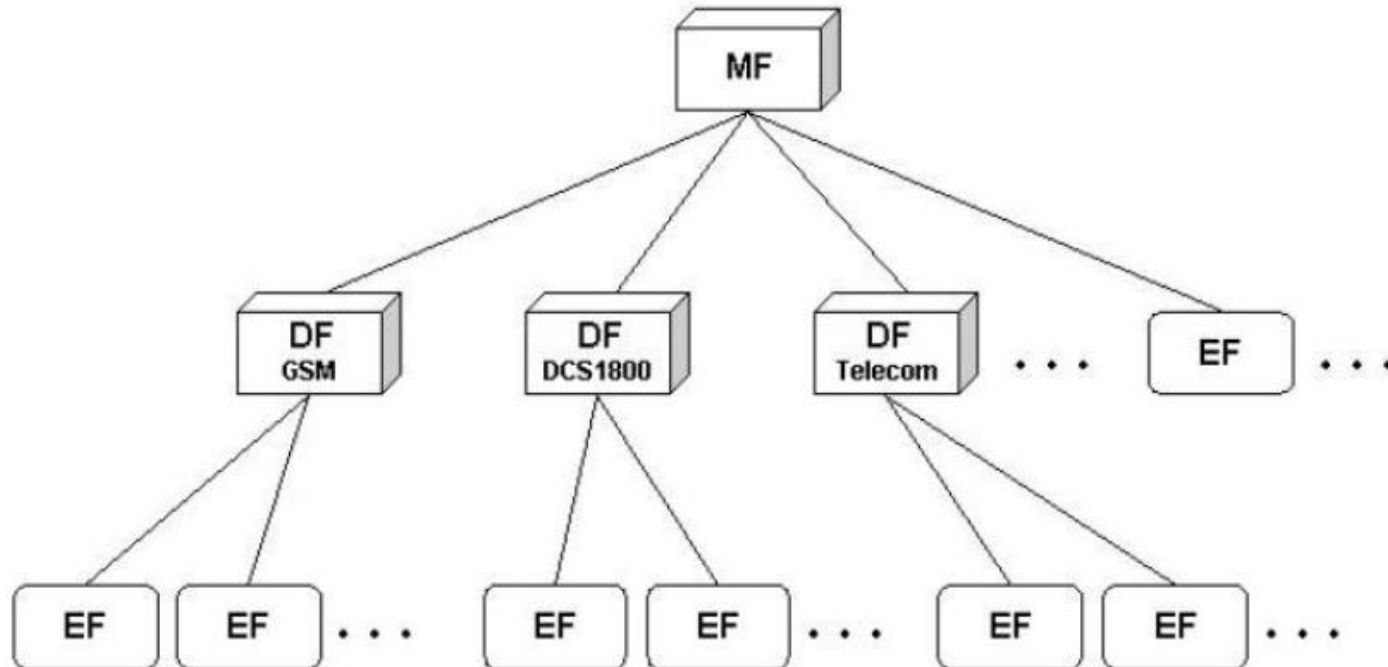
- L'analisi di uno dispositivo mobile a fini probatori riguarda tipicamente quattro **aree di ricerca**, ovvero:
 - ◆ La **memoria interna** del terminale radiomobile
 - ◆ La **scheda SIM**
 - ◆ La **memoria rimovibile aggiuntiva** (es. SD Card)
 - ◆ Il **Network Service Provider**
- Per la memoria interna, 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:
 - ◆ Master File (MF) (radice del file system)
 - ◆ Dedicated File (DF) (cartelle)
 - ◆ Elementary File (EF) (file)



Scheda SIM

- I file nelle cartelle **DF_{GSM}** e **DF_{DCS1800}** contengono prevalentemente informazioni sulla rete, mentre 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/>)



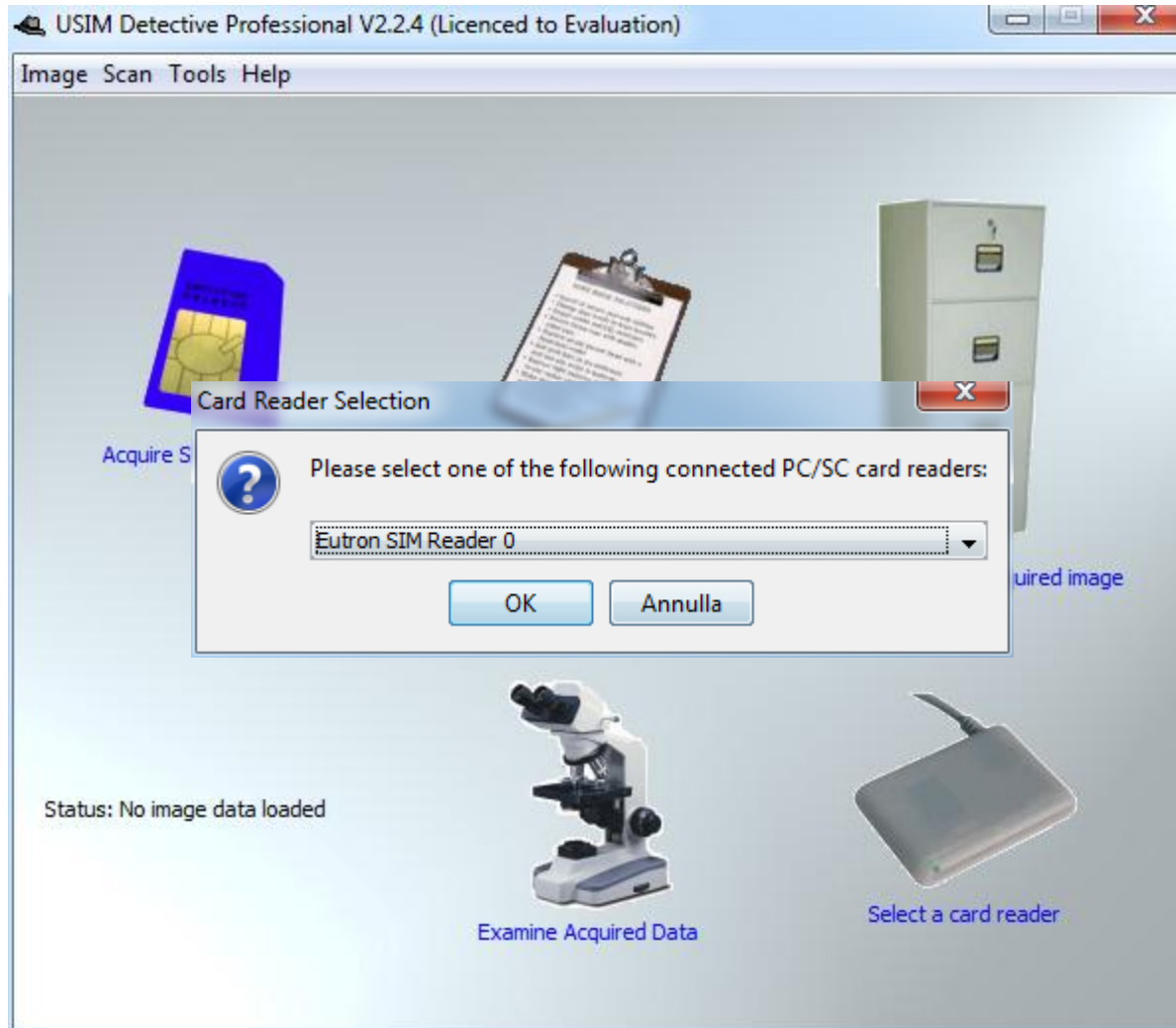
Scheda SIM

- 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)

USIM Detective



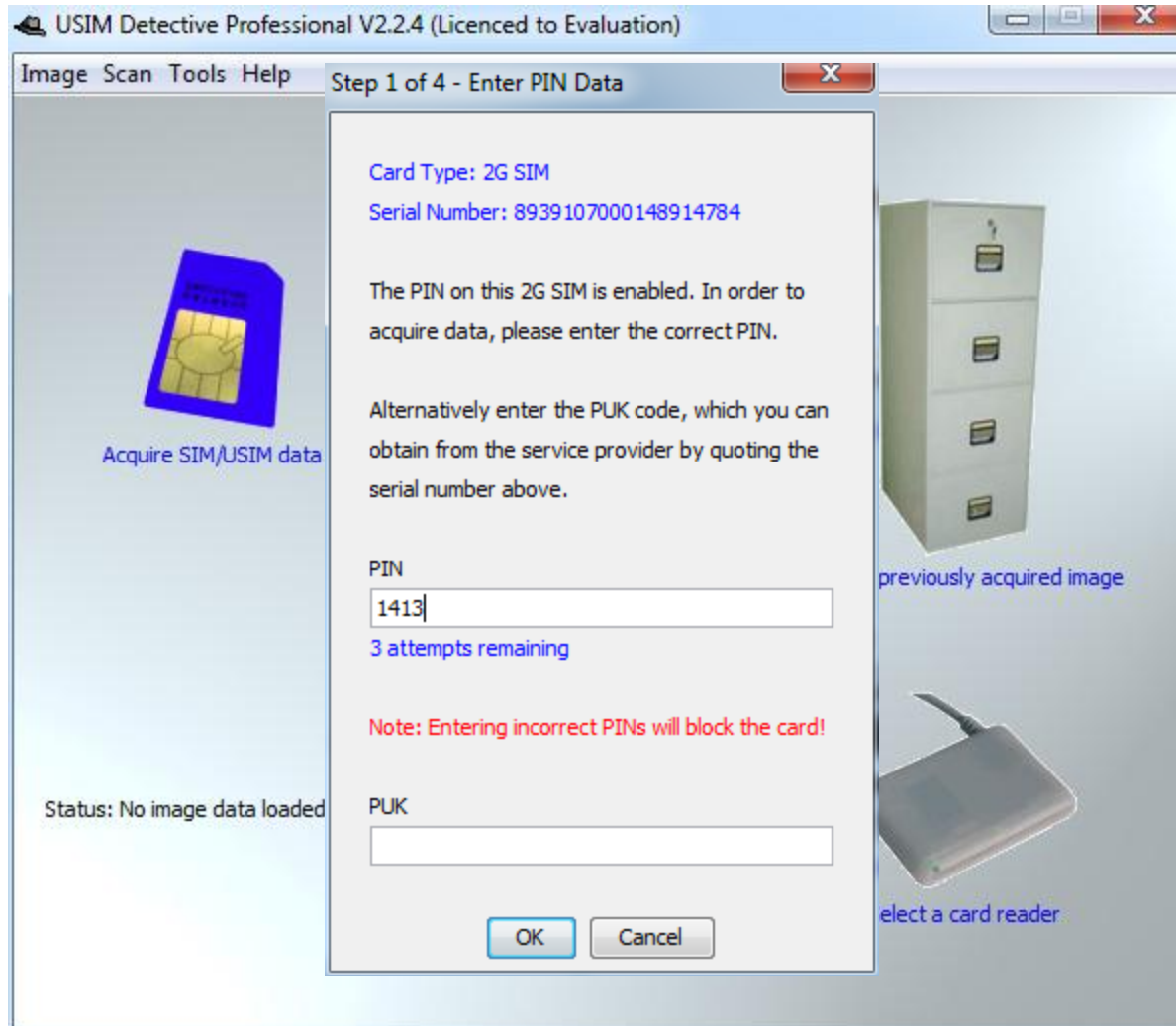
USIM Detective



USIM Detective



USIM Detective



USIM Detective

USIM Detective Professional V2.2.4 (Licenced to Evaluation)

Image Scan Tools Help

Step 2 of 4 - Enter Reference Data

All fields are optional. Any information entered will appear in subsequent reports produced.

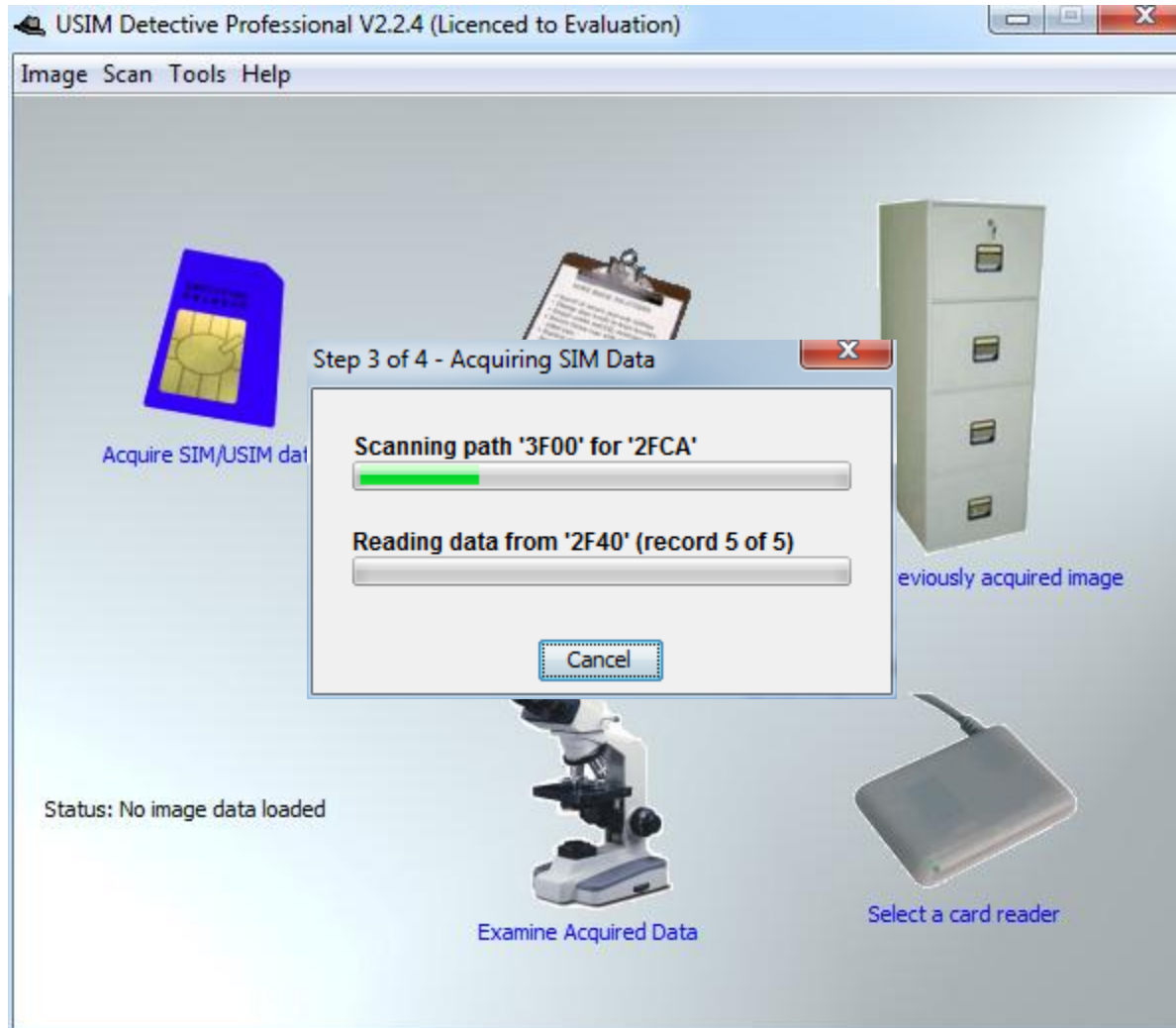
Operater Details	Digits/Data Printed on Physical Card
Operator Name <input type="text"/>	<input type="text"/>
Acquisition Reference <input type="text"/>	
Case Reference	Any Accompanying Handset
Case Number <input type="text"/>	Handset Manufacturer <input type="text"/>
Case Officer <input type="text"/>	Handset Model <input type="text"/>
Exhibit Details	IMEI Printed on Back <input type="text"/>
Exhibit Number <input type="text"/>	IMEI Displayed via *#06# <input type="text"/>
Exhibit Seal No. <input type="text"/>	
Additional Notes	Current Time
<input type="text"/>	Tue Apr 17 13:10:32 CEST 2012
	<input type="checkbox"/> Click here to confirm above time is correct

Status:

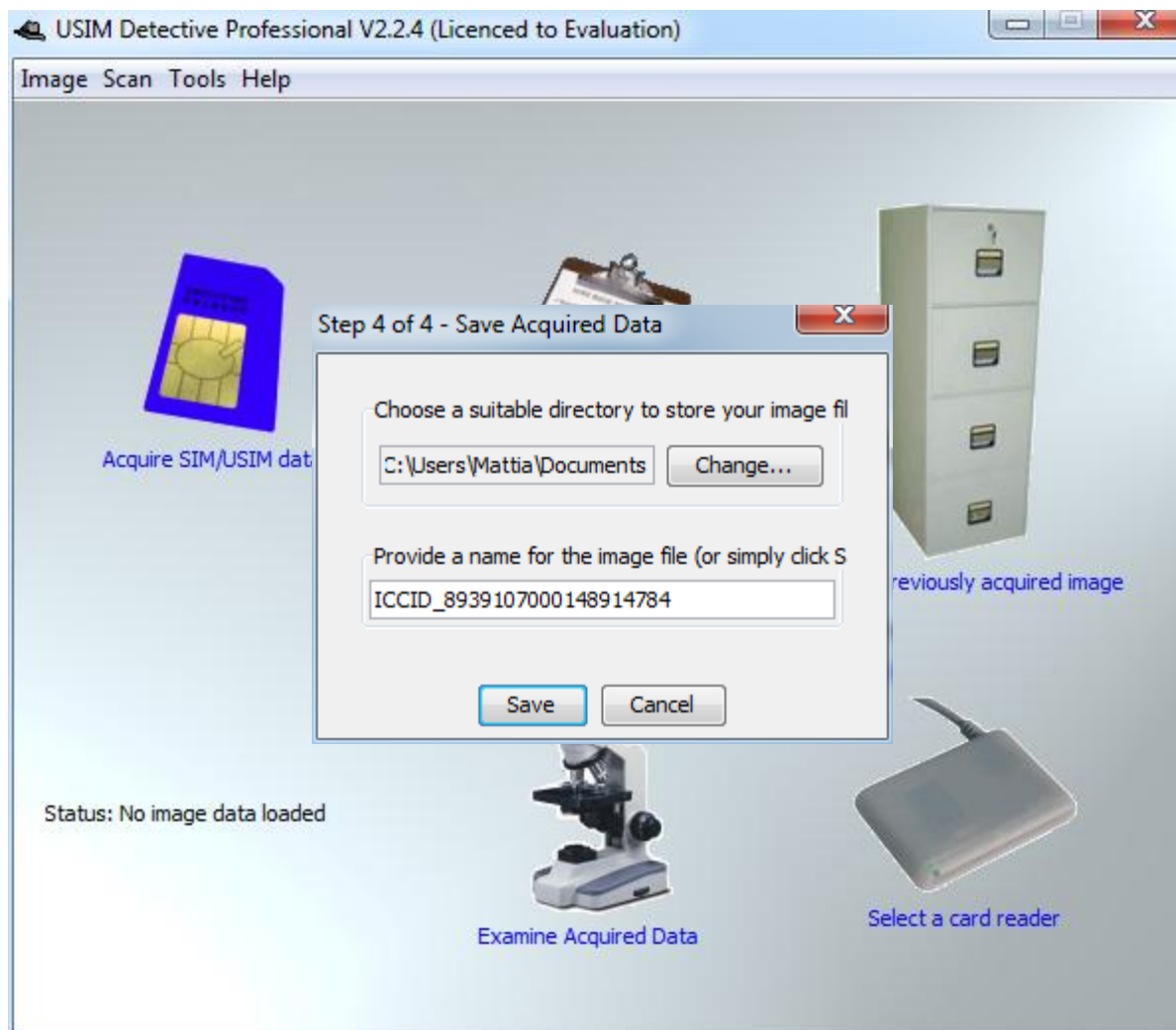
OK Cancel Update Time Displayed

Examine Acquired Data Select a card reader

USIM Detective



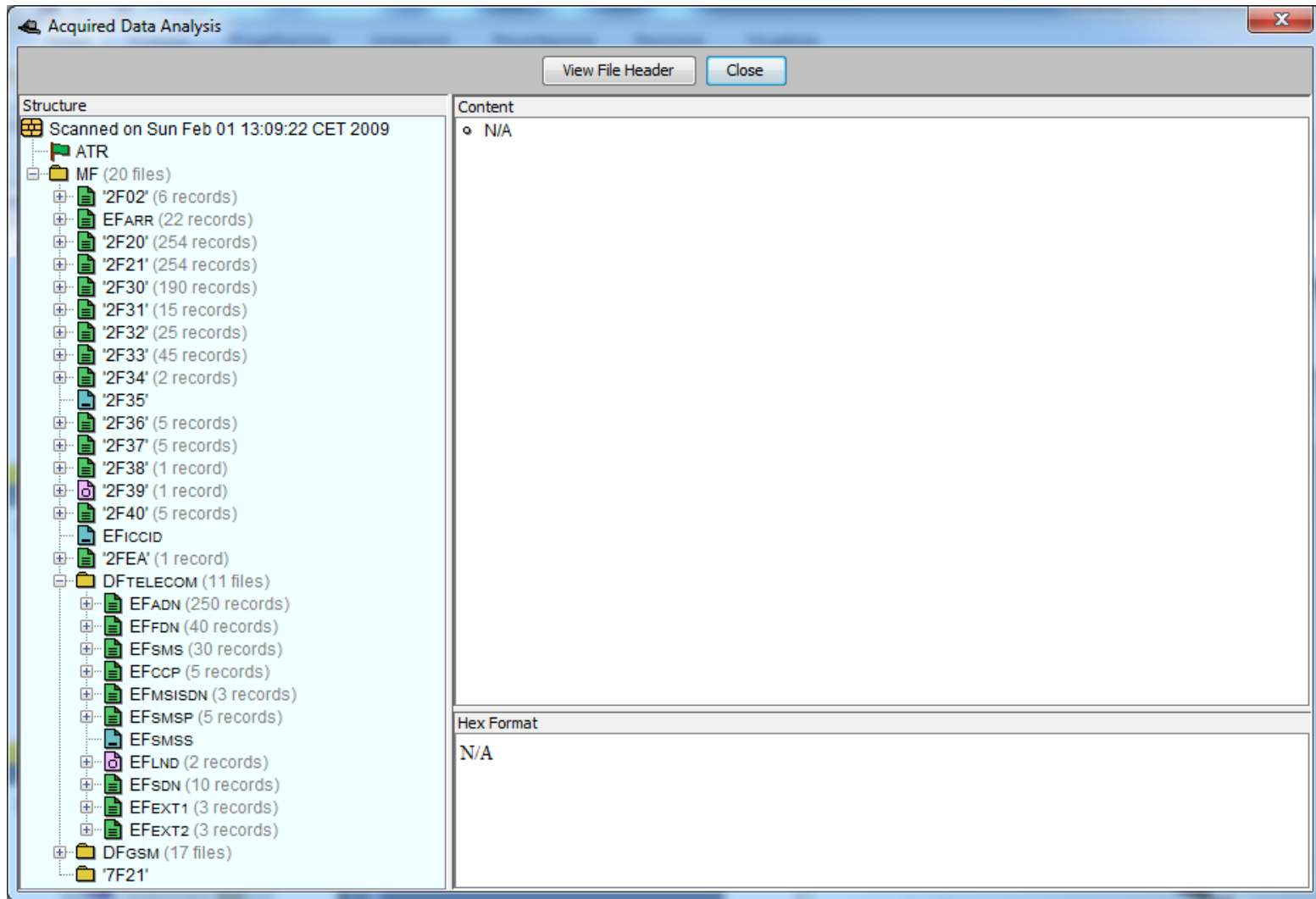
USIM Detective



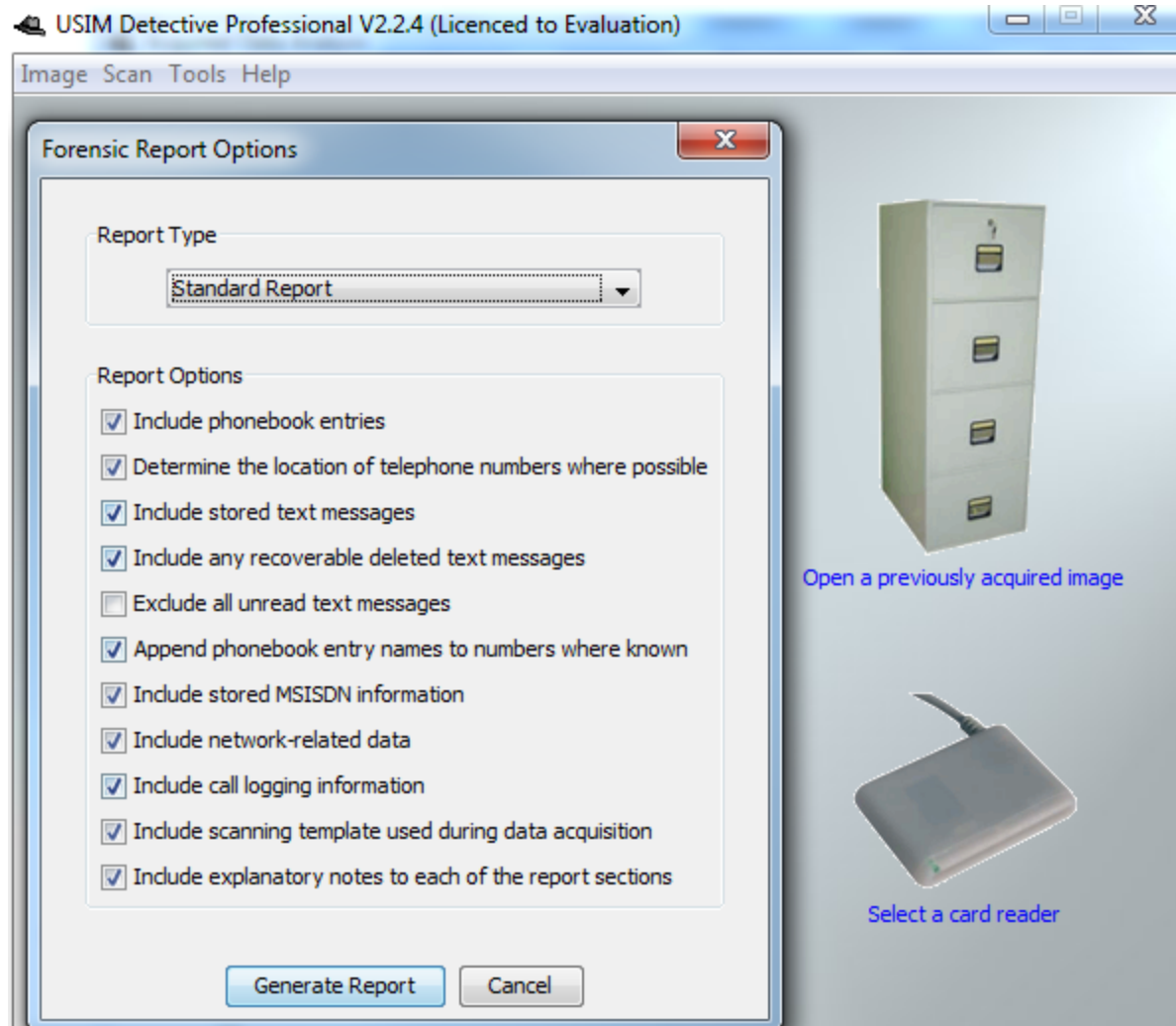
USIM Detective



USIM Detective

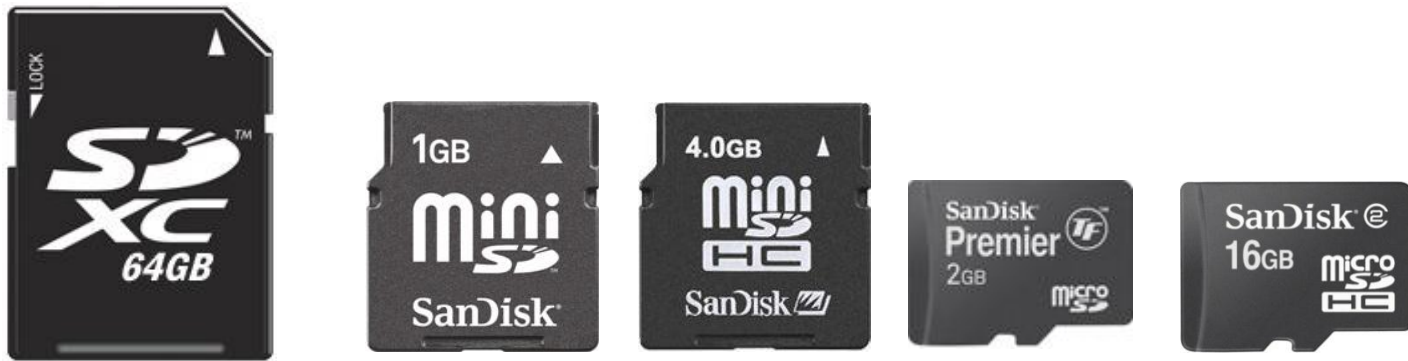


USIM Detective



Memoria interna 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 effettuata mediante tradizionali tecniche (es. write blocker + DD)



Analisi presso il Network Service Provider

- In base al **D.lvo 109/2008**, i dati che si possono ottenere dal Provider riguardo a comunicazioni cellulari sono:
 - ◆ Numero telefonico chiamante
 - ◆ Nome e indirizzo dell'utente registrato
 - ◆ Numero composto, ovvero il numero o i numeri chiamati e, nei casi che comportino servizi supplementari (come l'inoltro o il trasferimento di chiamata), il numero o i numeri verso i quali è diretta la chiamata
 - ◆ Nome e indirizzo dell'abbonato o dell'utente registrato
 - ◆ Data e ora dell'inizio e della fine della comunicazione
 - ◆ IMSI del chiamante e del chiamato
 - ◆ IMEI del chiamante e del chiamato
 - ◆ Etichetta di ubicazione (Cell ID) all'inizio della comunicazione

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 (software)

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



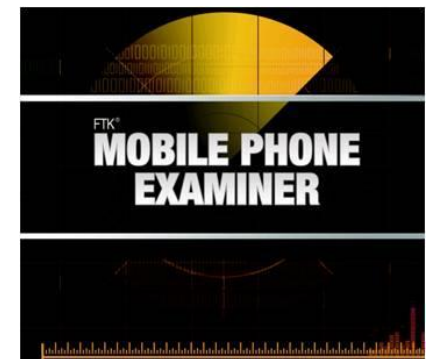
Kies

Acquisizione logica (software)

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



paraben's
device
seizure



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
- Vedremo dopo alcune tecniche per i dispositivi con sistema operativo iOS e Android

iPhone/iPad Forensics



iPhone/iPad Forensics

- iDevice e sistema operativo iOS
- Isolamento del dispositivo
 - ◆ Airplane mode
- 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)



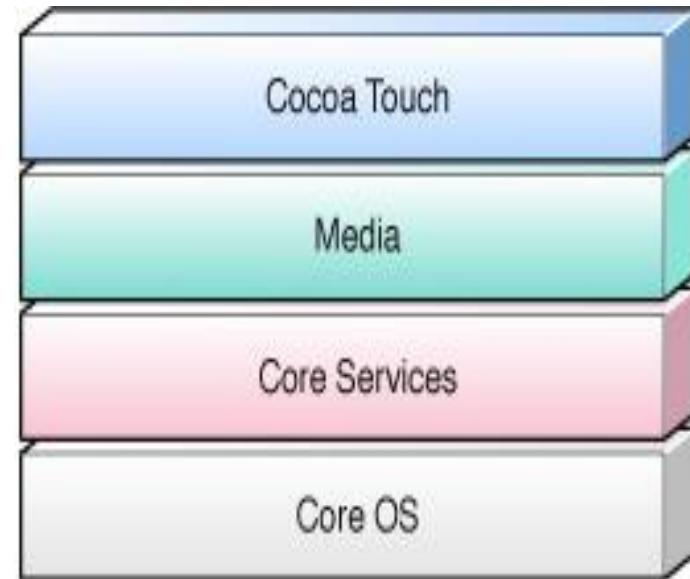
iPad

- 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)



Sistema operativo iOS

- iOS è il sistema operativo Apple per dispositivi mobile
- L'interfaccia utente usata da iOS è basata sul concetto di manipolazione diretta
- Apple mette a disposizione per gli sviluppatori l'iOS SDK che contiene gli strumenti e le interfacce utili allo sviluppo, l'installazione, l'esecuzione e il test delle applicazioni native
- Il sistema operativo iOS è composto da quattro strati
 - ◆ **Core OS layer** (gestione hardware, memoria, file system, networking, power management, ecc.)
 - ◆ **Core Services layer** (SQLite, plist, Geolocation, ecc.)
 - ◆ **Media layer** (Core Graphics, OpenGL, Core Audio)
 - ◆ **Cocoa Touch layer** (Multitasking, Touch, Accelerometro, ecc.)



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

- Applications
- bin
- cores
- dev
- Developer
- Library
- private
- sbin
- System
- usr

- audit
- db
- ea
- empty
- folders
- keybags
- Keychains
- log
- logs
- Managed Preferences
- mobile
- MobileDevice
- msgs
- preferences
- root
- run
- spool
- tmp
- vm
- wireless

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)



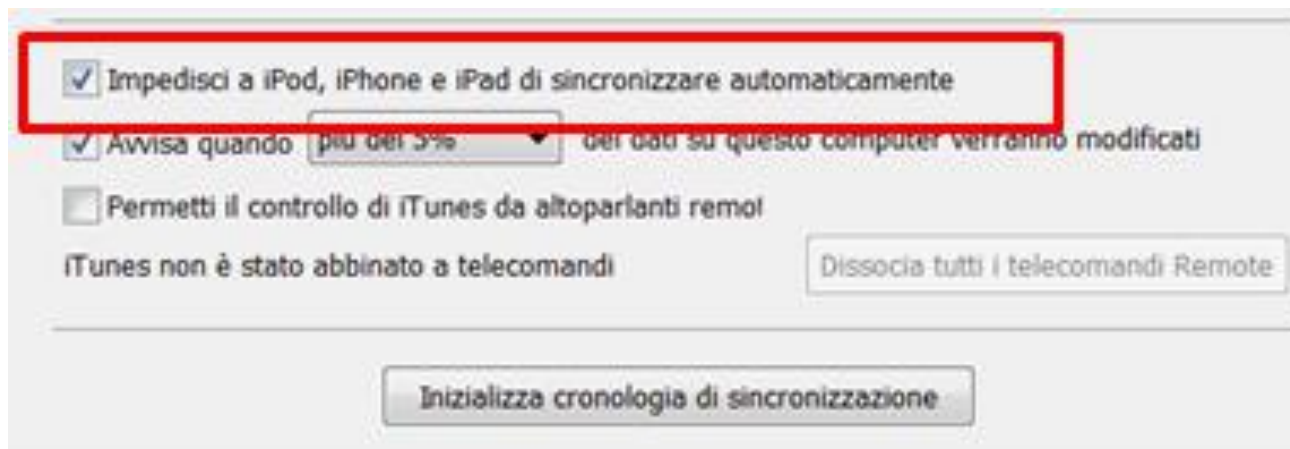
Acquisizione logica dei dati

- 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**
 - Facile da realizzare
 - Costo «zero»
 - Una volta realizzato il backup è necessario tuttavia dotarsi di
 - Strumenti per l'estrazione dei backup**
 - e/o
 - Strumenti dedicati per l'analisi dei file**
 - ◆ **Utilizzando software/hardware dedicati per l'analisi forense**
 - Non esistono strumenti freeware e/o open source
 - Integrano gli strumenti di analisi dei file (es. plist e SQLite viewer)



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**



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.



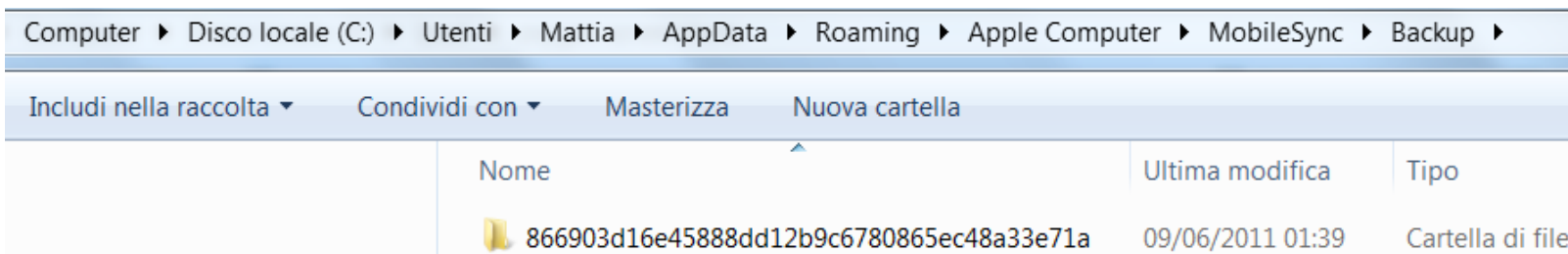
A screenshot of the iTunes application interface. On the left, a sidebar menu lists categories like Musica, Film, Programmi TV, Podcast, Libri, and Radio. Below these are sections for STORE (iTunes Store, Ping, Acquisti) and DISPOSITIVI (iPod/iPad). The 'iPod/iPad' section is expanded, showing a context menu with options: Espelli, Nuova playlist, Trasferisci acquisti, Backup (highlighted with a red box), Ripristina da backup..., and Azzera avvisi. The main area displays the 'iPad' device card with a small image of the iPad and fields for 'Nome:', 'Capacità:', 'Versione software:', and 'Numero di serie:'. The 'Versione software:' field is highlighted in red. Below the device card, there is a 'Versione' section with two buttons: 'Aggiorna' and 'Ripristina'. The 'Aggiorna' button has a tooltip that reads: 'È disponibile una nuova versione del software iPad (versione 4.3.3). Per aggiornare iPad con l'ultima versione, fai clic su Aggiorna.' The 'Ripristina' button has a tooltip that reads: 'Se hai problemi con iPad, puoi ripristinare le impostazioni predefinite facendo clic su Ripristina.'

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\MobileSync\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.



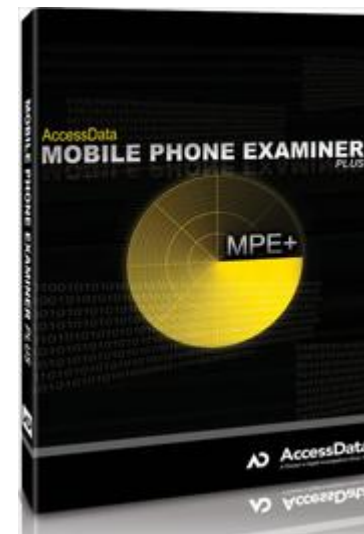
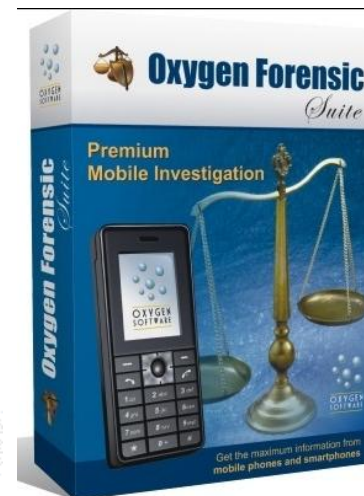
Analisi dei backup di iTunes

- 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.

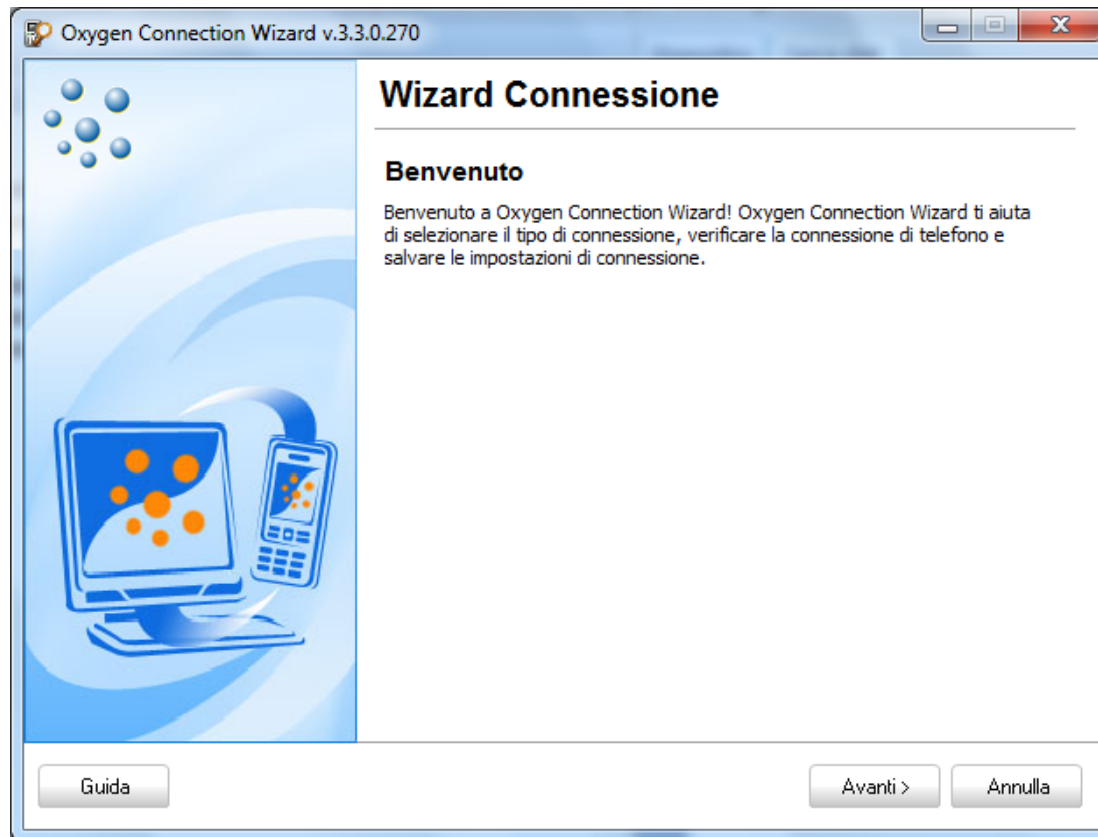


Acquisizione logica con software/hardware dedicati

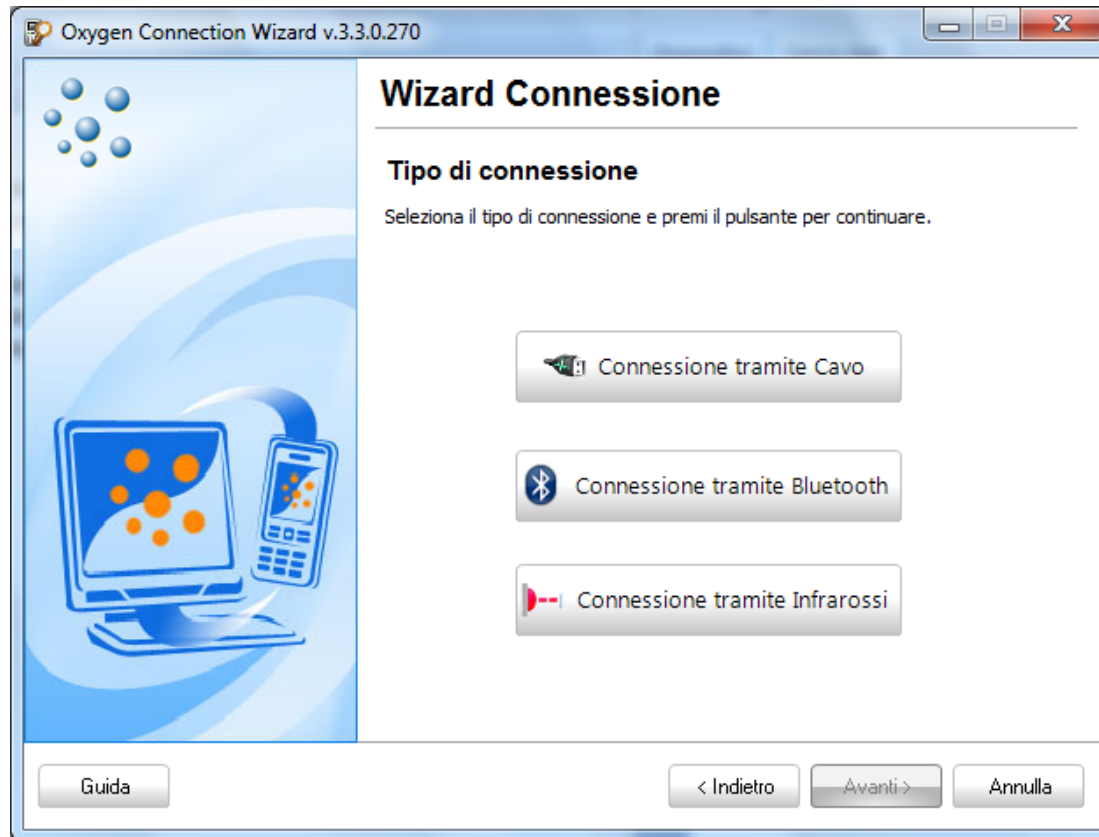
- In commercio esistono diverse soluzioni hardware e software per l'acquisizione di dispositivi iOS.
- Per una trattazione completa si rimanda al white paper pubblicato sul sito viaforensics.com (A.Hogg).
- I principali strumenti disponibili sono:
 - AccessData Mobile Phone Examiner Plus
 - Cellbrite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



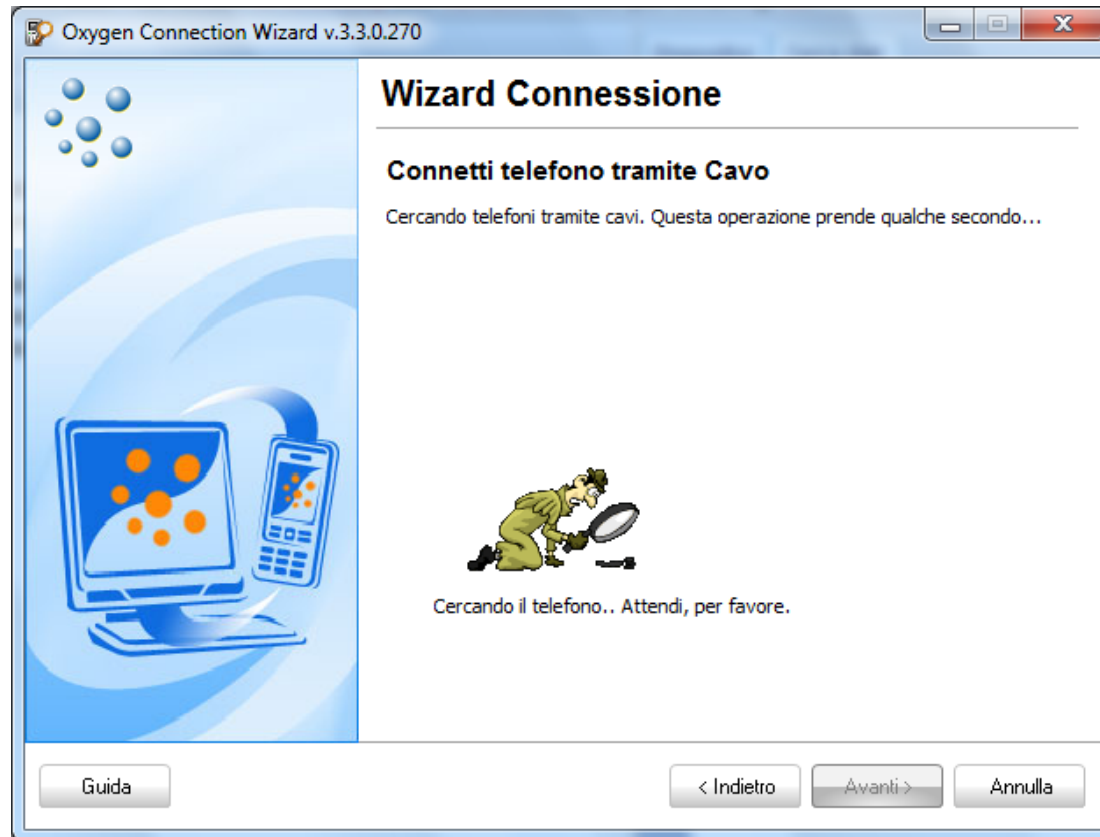
Oxygen Forensics Suite – Connessione del dispositivo



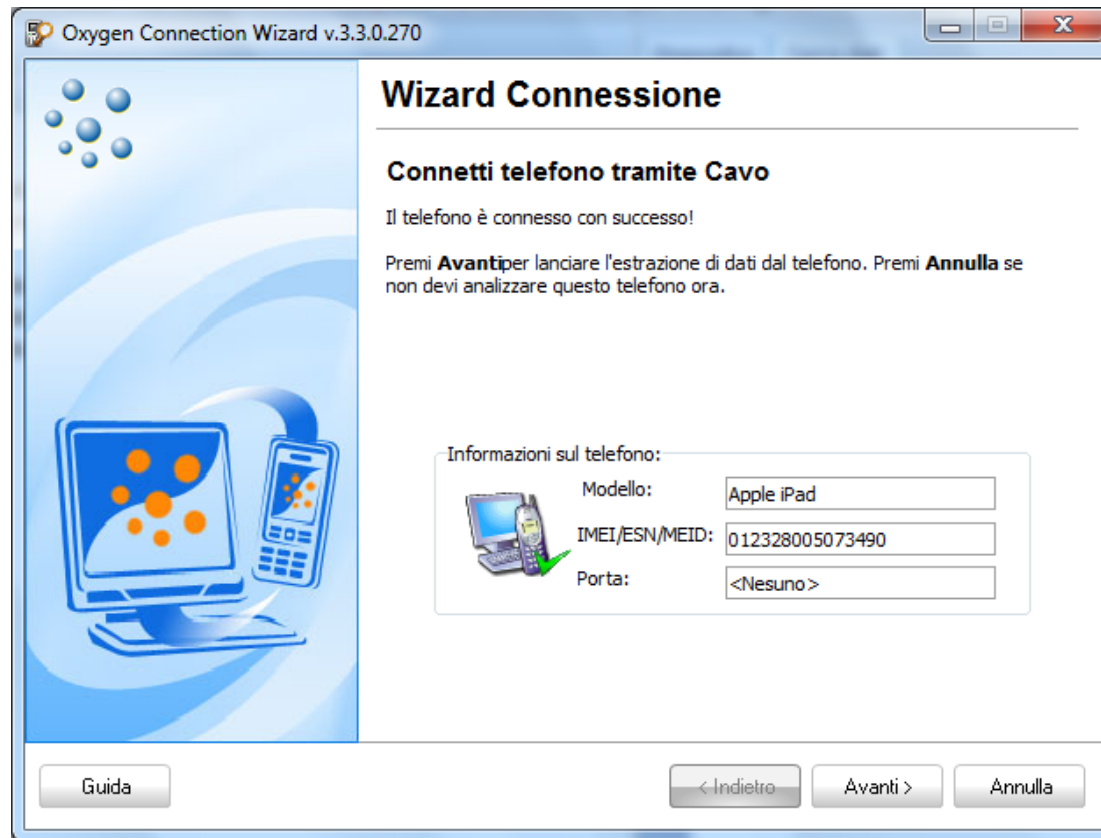
Oxygen Forensics Suite – Connessione del dispositivo



Oxygen Forensics Suite – Connessione del dispositivo



Oxygen Forensics Suite – Connessione del dispositivo



Oxygen Forensics Suite – Estrazione dei dati



Oxygen Forensics Suite – Estrazione dei dati

Oxygen Forensic Suite 2011 (Trial) - Wizard di Estrazione Dati

Identificazione dispositivo

Inserisci l'informazione per descrivere il dispositivo e la causa qui

Nome telefono
Nuovo dispositivo (iPad)

Numero causa
▼

Numero indizio

Note dispositivo

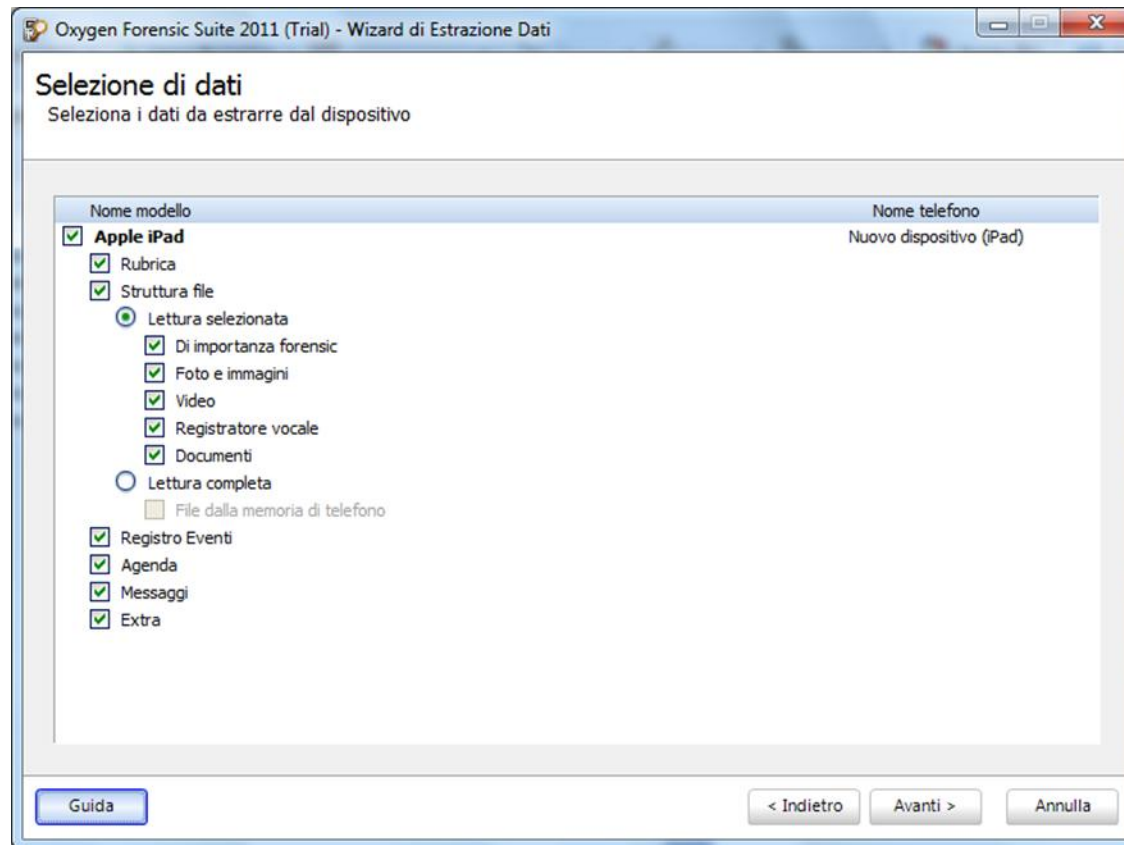
Possessore dispositivo

Algoritmo Hash
MD5 ▼

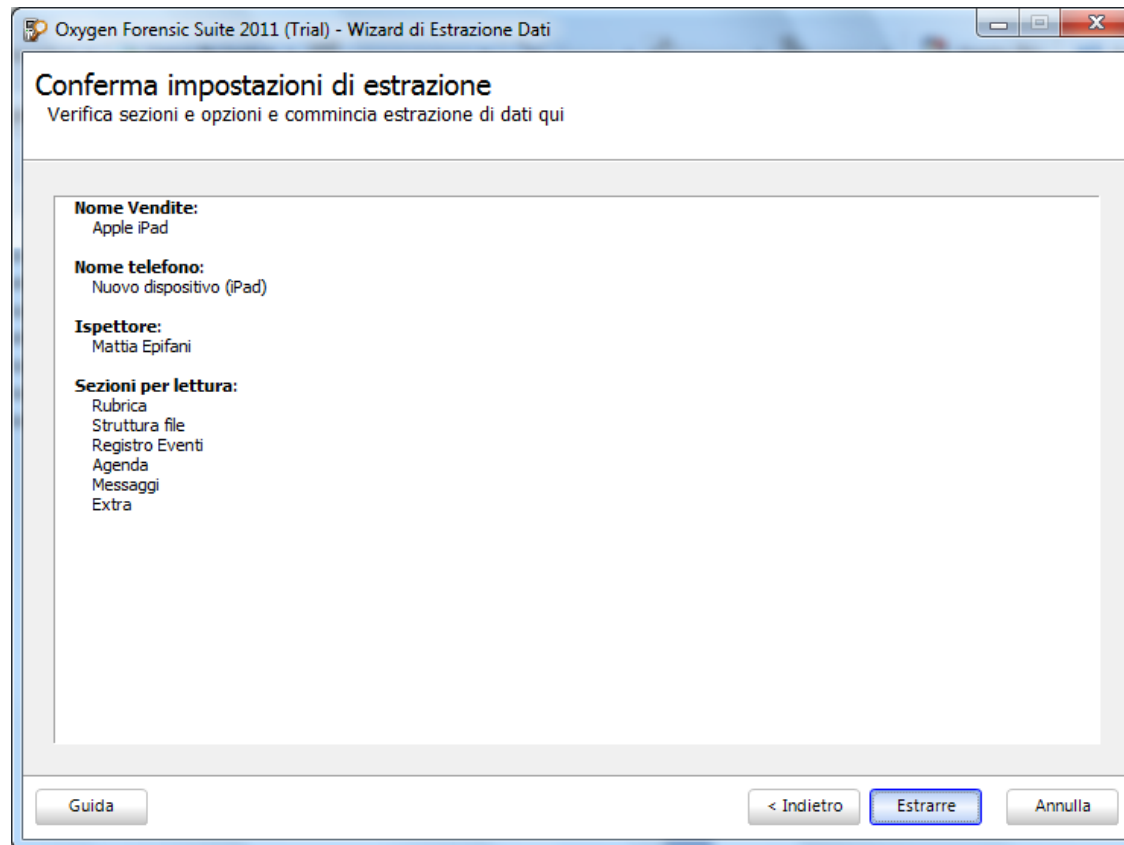
Ispettore
Mattia Epifani ▼

Guida < Indietro Avanti > Annulla

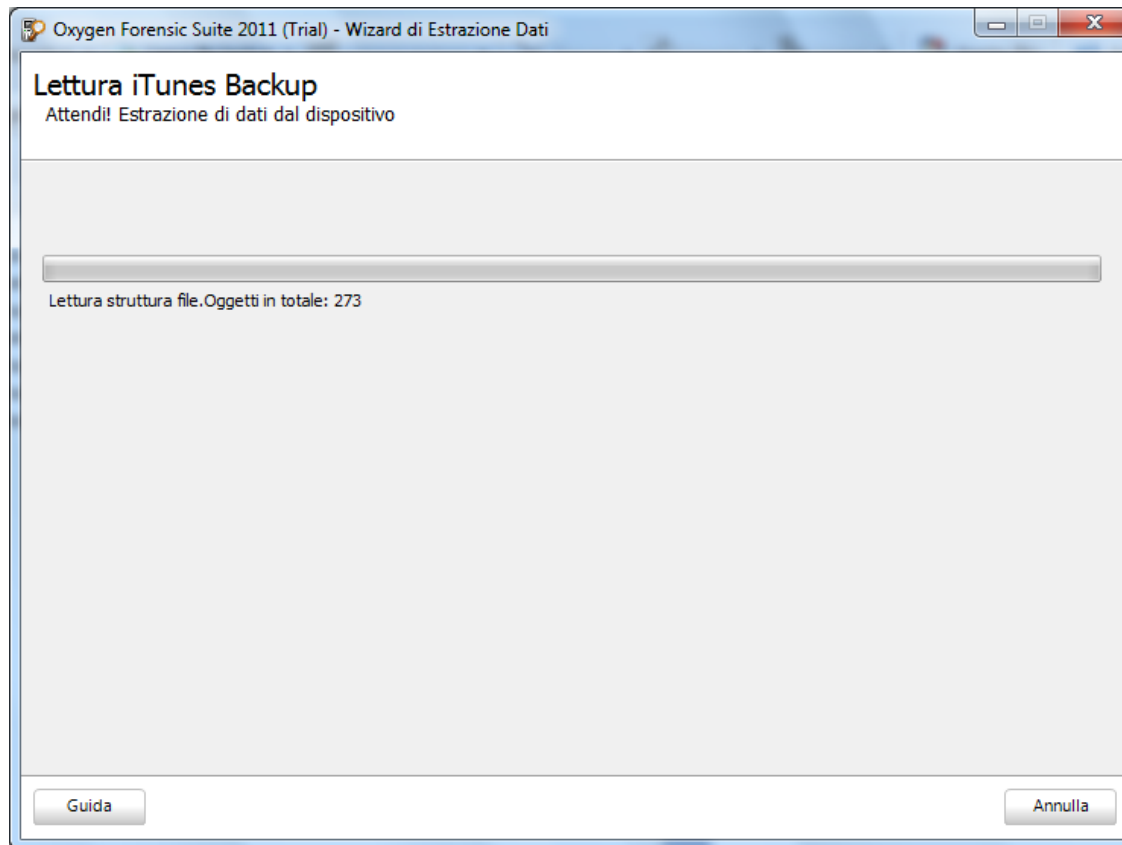
Oxygen Forensics Suite – Estrazione dei dati



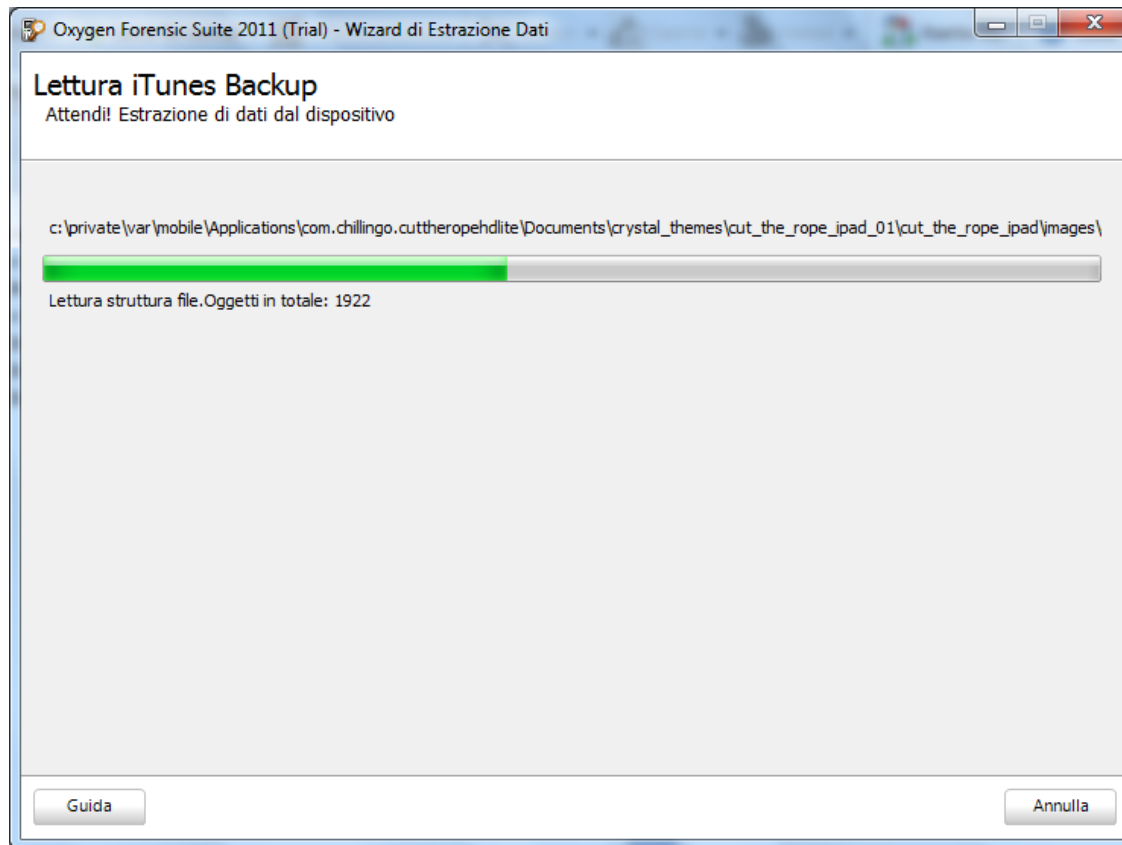
Oxygen Forensics Suite – Estrazione dei dati



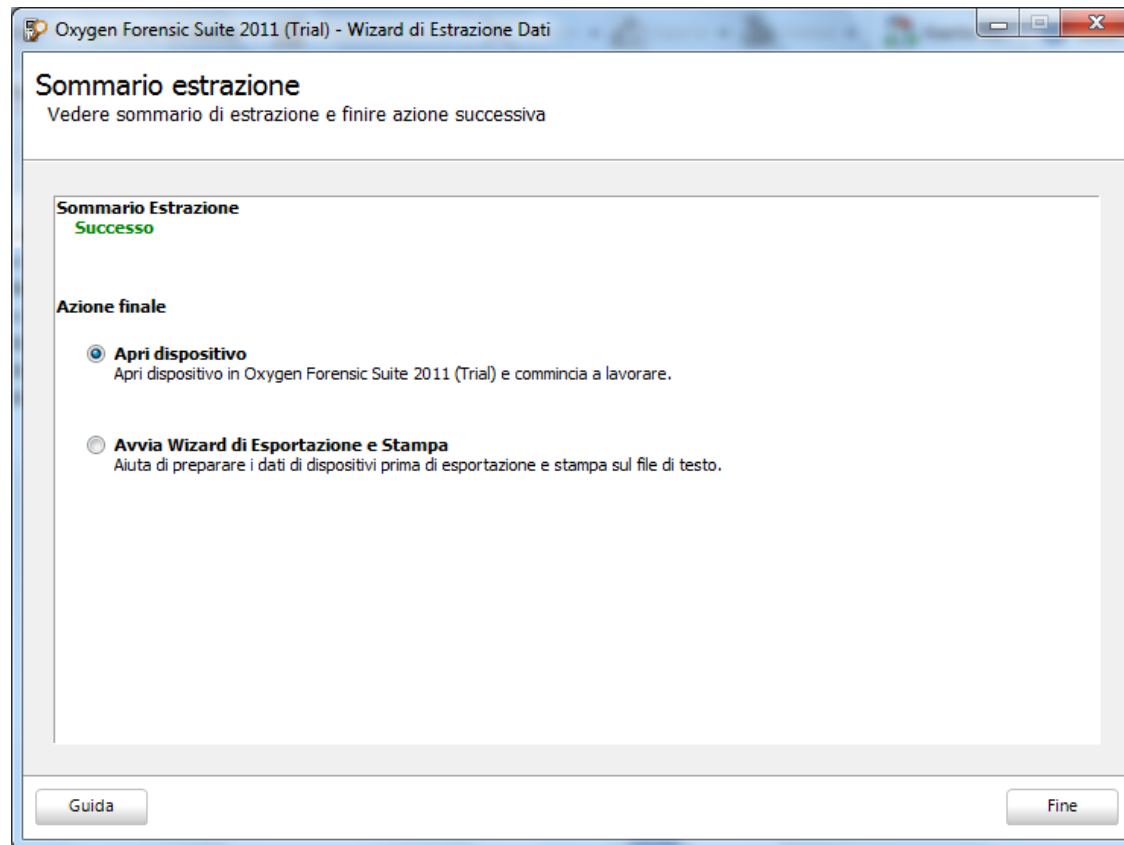
Oxygen Forensics Suite – Estrazione dei dati



Oxygen Forensics Suite – Estrazione dei dati

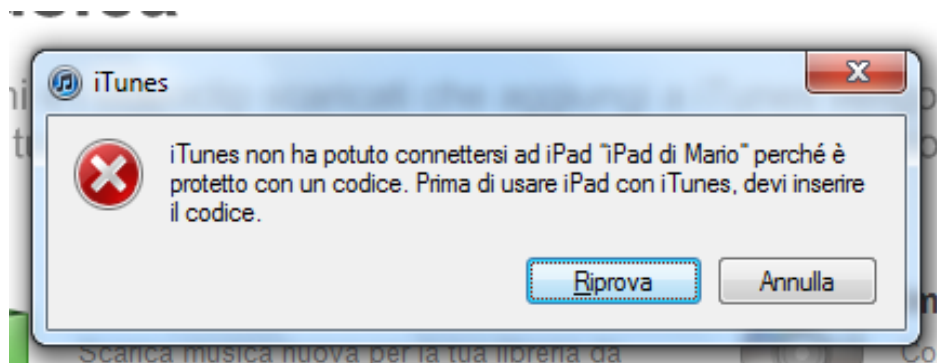


Oxygen Forensics Suite – Estrazione dei dati



Acquisizione logica di dispositivi con passcode

- Se il dispositivo è protetto da un passcode, non è possibile effettuare 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 and Settings\[username]\Application Data\Apple Computer\Lockdown
Mac OS X	/private/var/db/lockdown

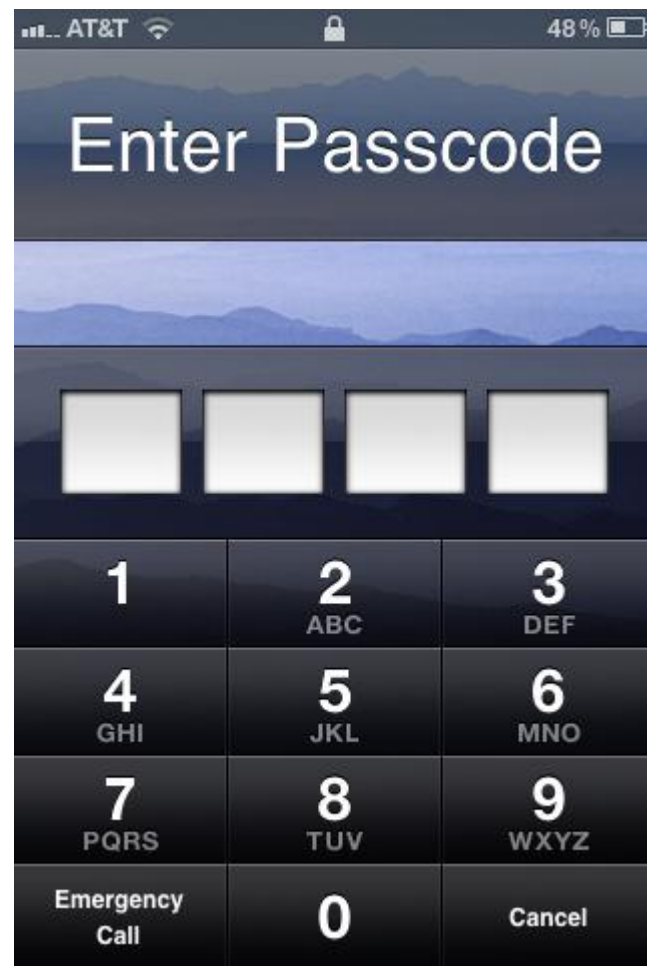
Acquisizione fisica

- 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 wipeato, **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**
- Ciascun file è inoltre cifrato con una **chiave univoca**
- Quando un file presente nel file system viene cancellato, **la chiave univoca per il file viene cancellata rendendo sostanzialmente impossibile il recupero del contenuto**
- **La chiave di cifratura di ciascun file viene a sua volta cifrata con una master key**
- iOS in particolare 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'inserimento 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 **non appartengono a nessuna classe di protezione (NSFileProtectionNone) e sono quindi sempre disponibili per il sistema operativo**
- Le chiavi di cifratura per questi file sono cifrate utilizzando una master key speciale detta **Dkey**, che è memorizzata nell'area PLOG della NAND

Cifratura nei dispositivi iDevice

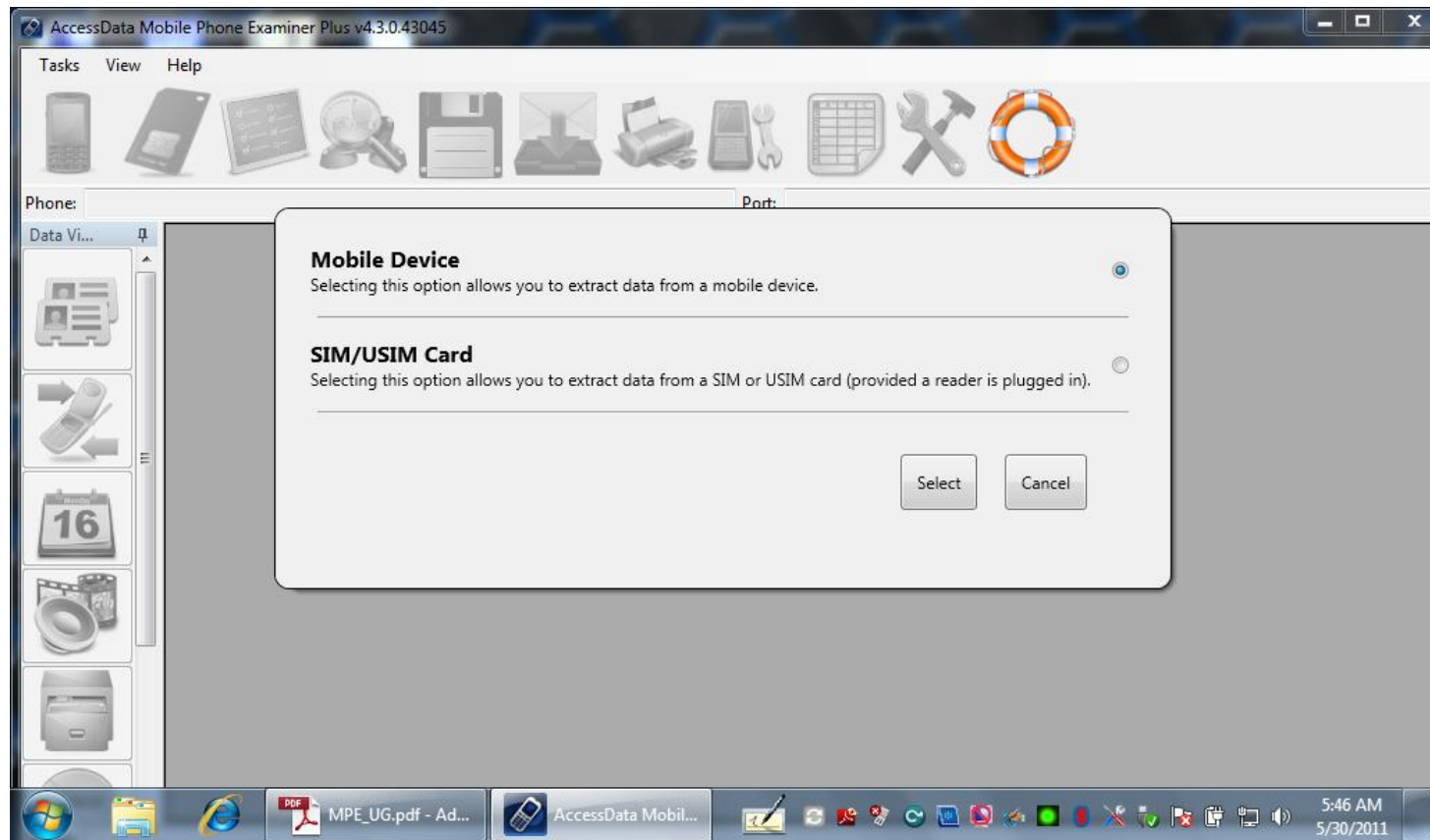
- Effettuando il boot del dispositivo con un RAM disk è possibile accedere alle chiavi memorizzate nell'area PLOG e in particolare **la chiave EMF! (cifratura del file system) e la chiave Dkey (master key per la cifratura dei file senza protezione da passcode)**
- Fino a iOS versione 5 incluso gli unici 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. Whatsapp)**
- Per questo motivo, **anche senza conoscere il passcode del dispositivo o effettuare 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

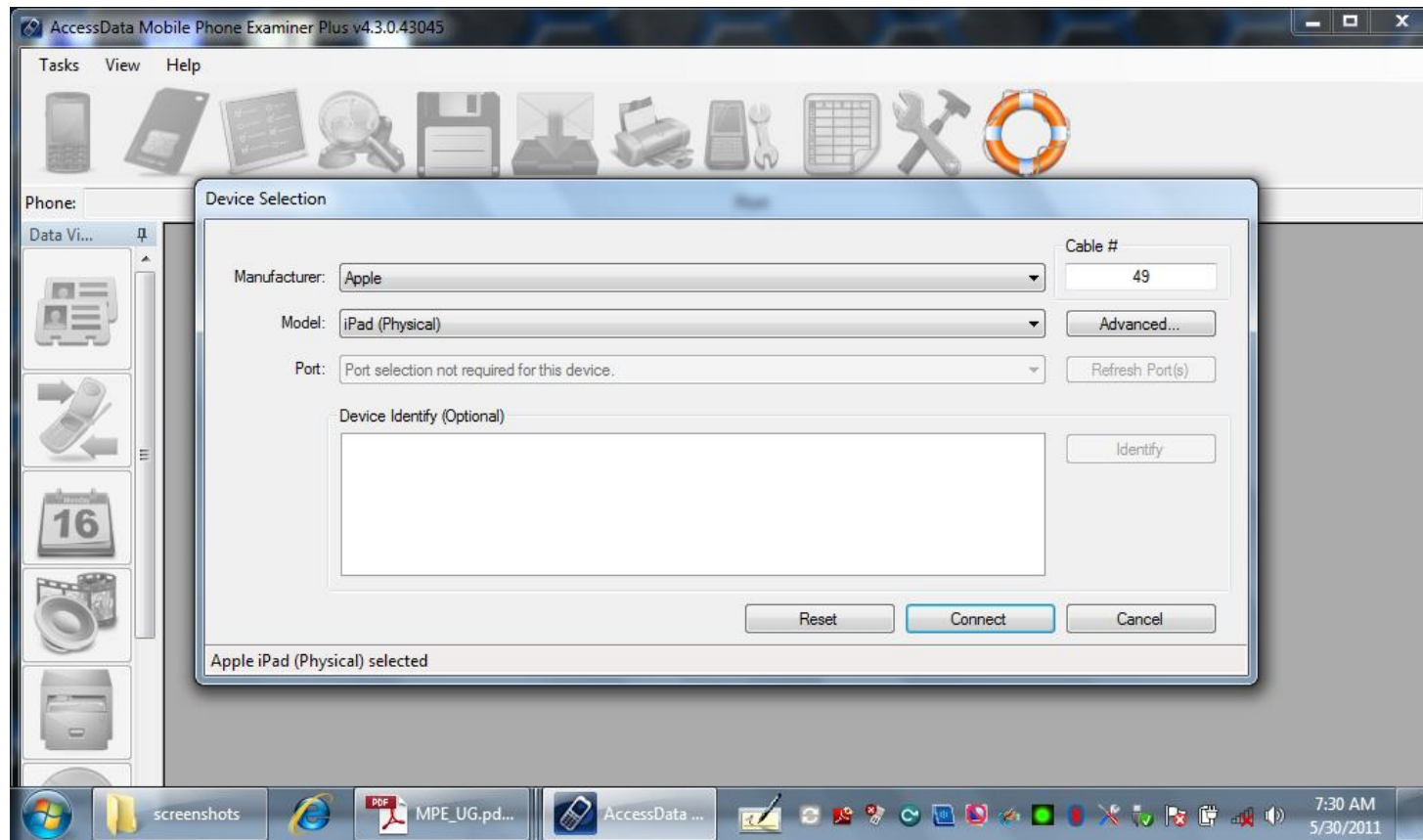
- Attualmente sono disponibili diverse soluzioni che consentono l'acquisizione fisica di un iDevice:
 - **Zdziarski Method and Tools**, riservato a **Law Enforcement** (<http://www.iosresearch.org>)
 - **Lantern Lite**, freeware per Mac
 - **Elcomsoft iOS Acquisition Toolkit**, commerciale per Windows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



AccessData MPE+ Acquisizione fisica



AccessData MPE+ DFU Mode Wizard



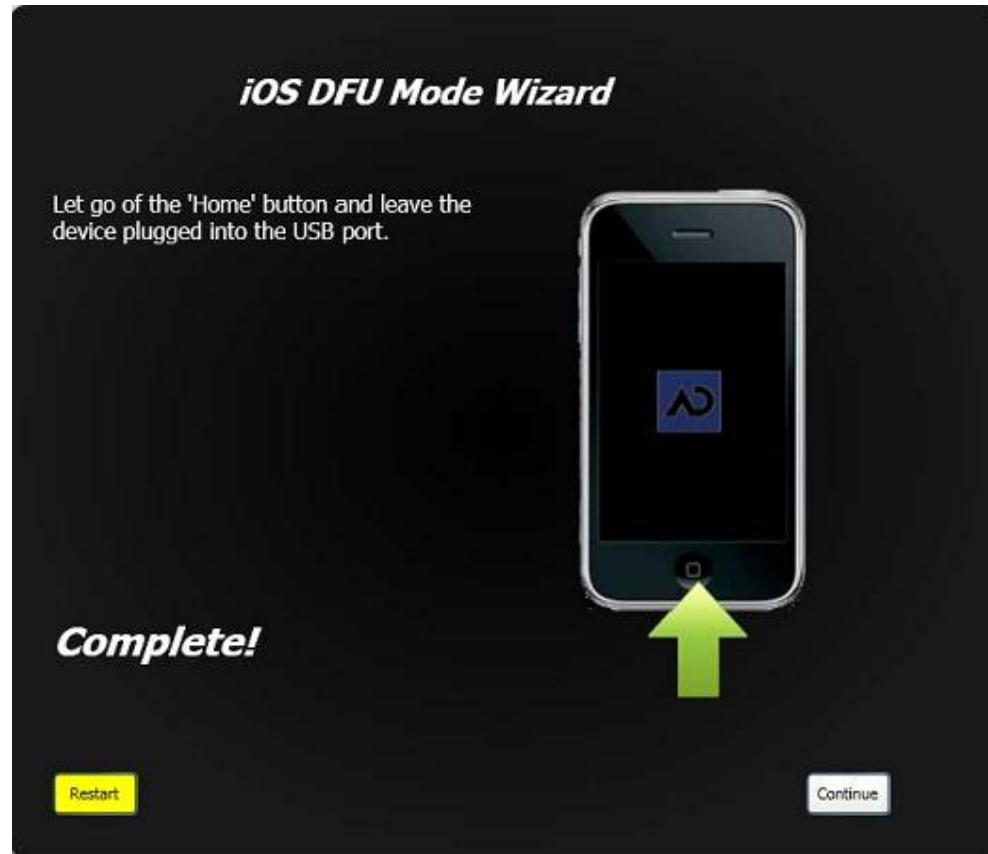
AccessData MPE+ DFU Mode Wizard



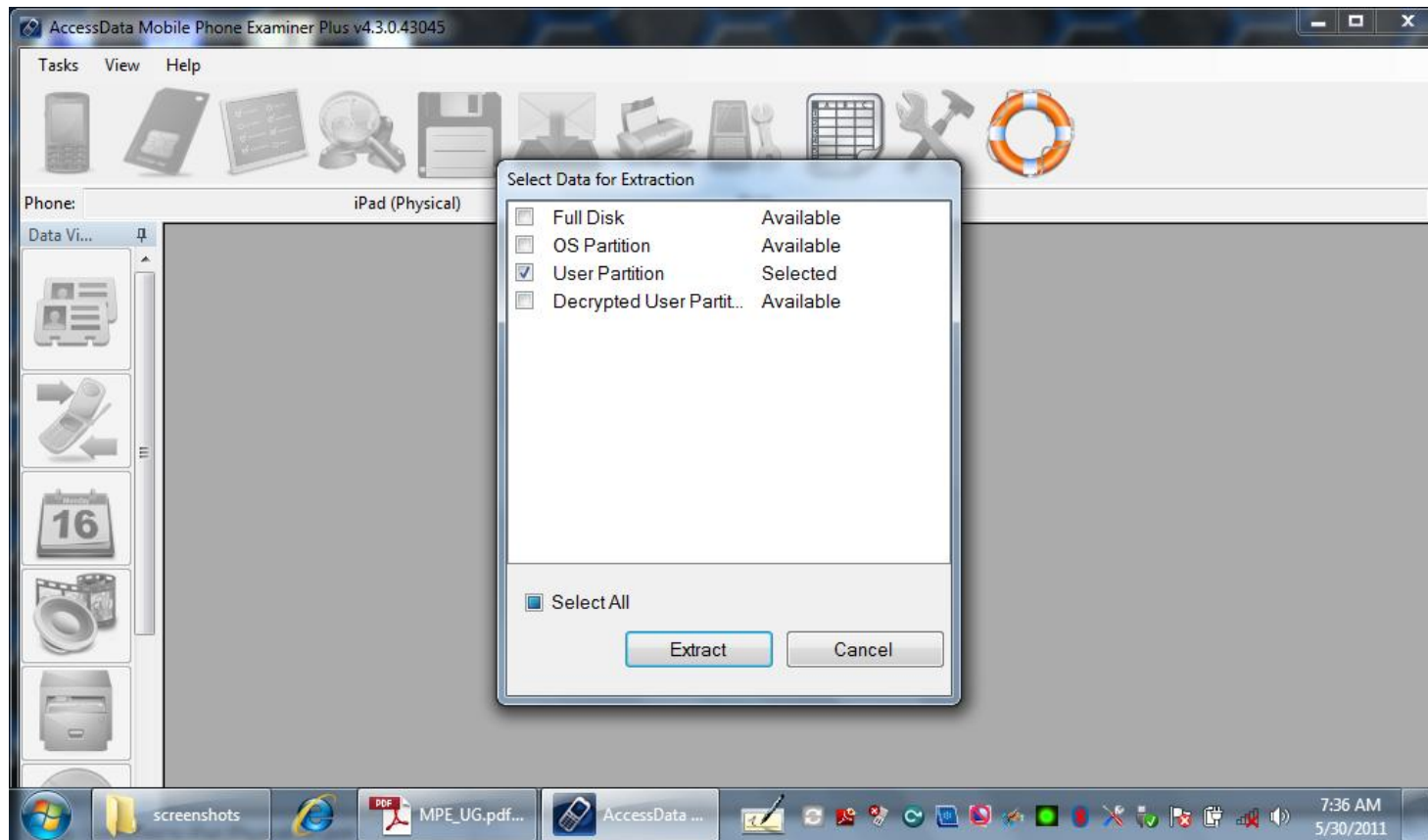
AccessData MPE+ DFU Mode Wizard



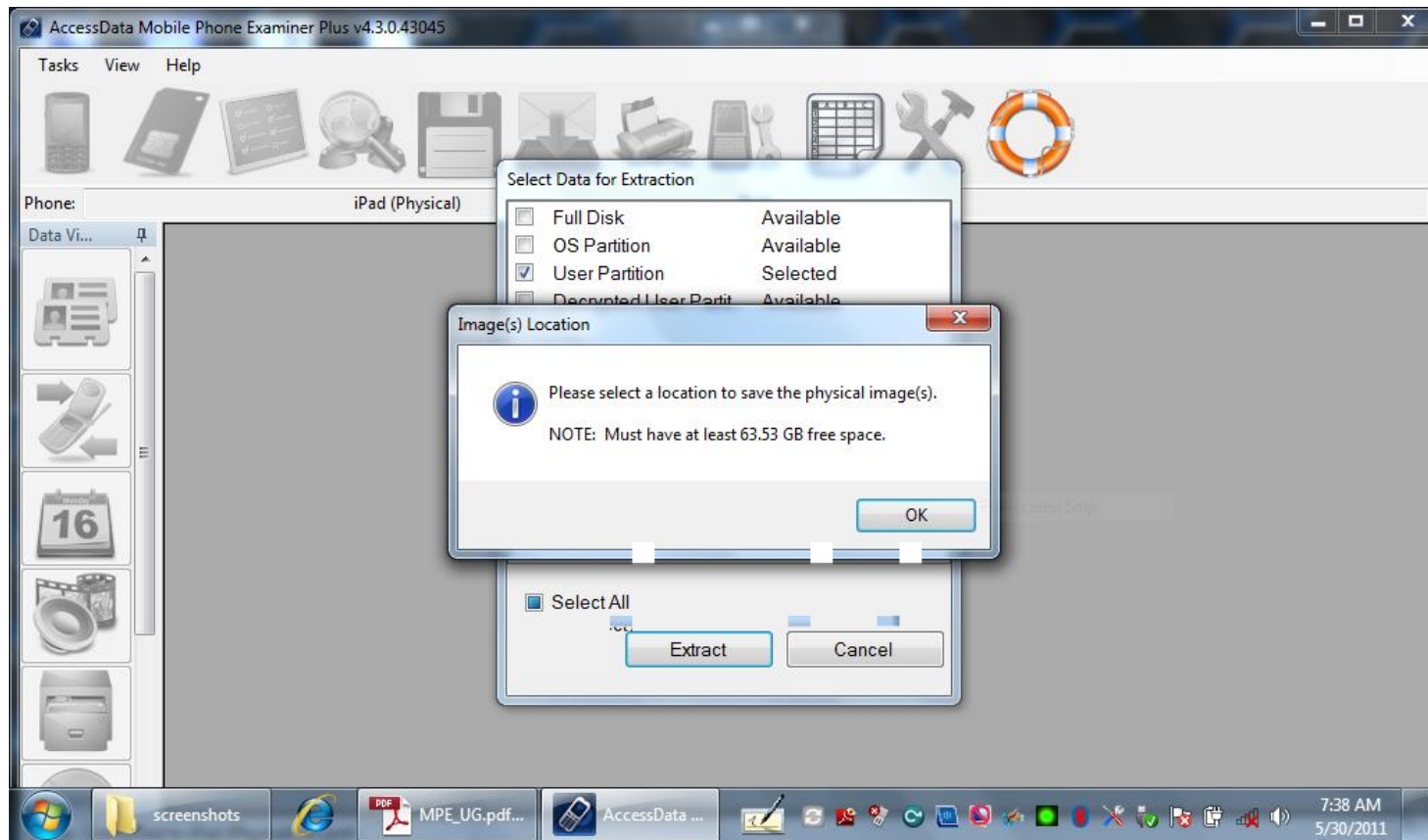
AccessData MPE+ DFU Mode Wizard



AccessData MPE+ Acquisizione fisica



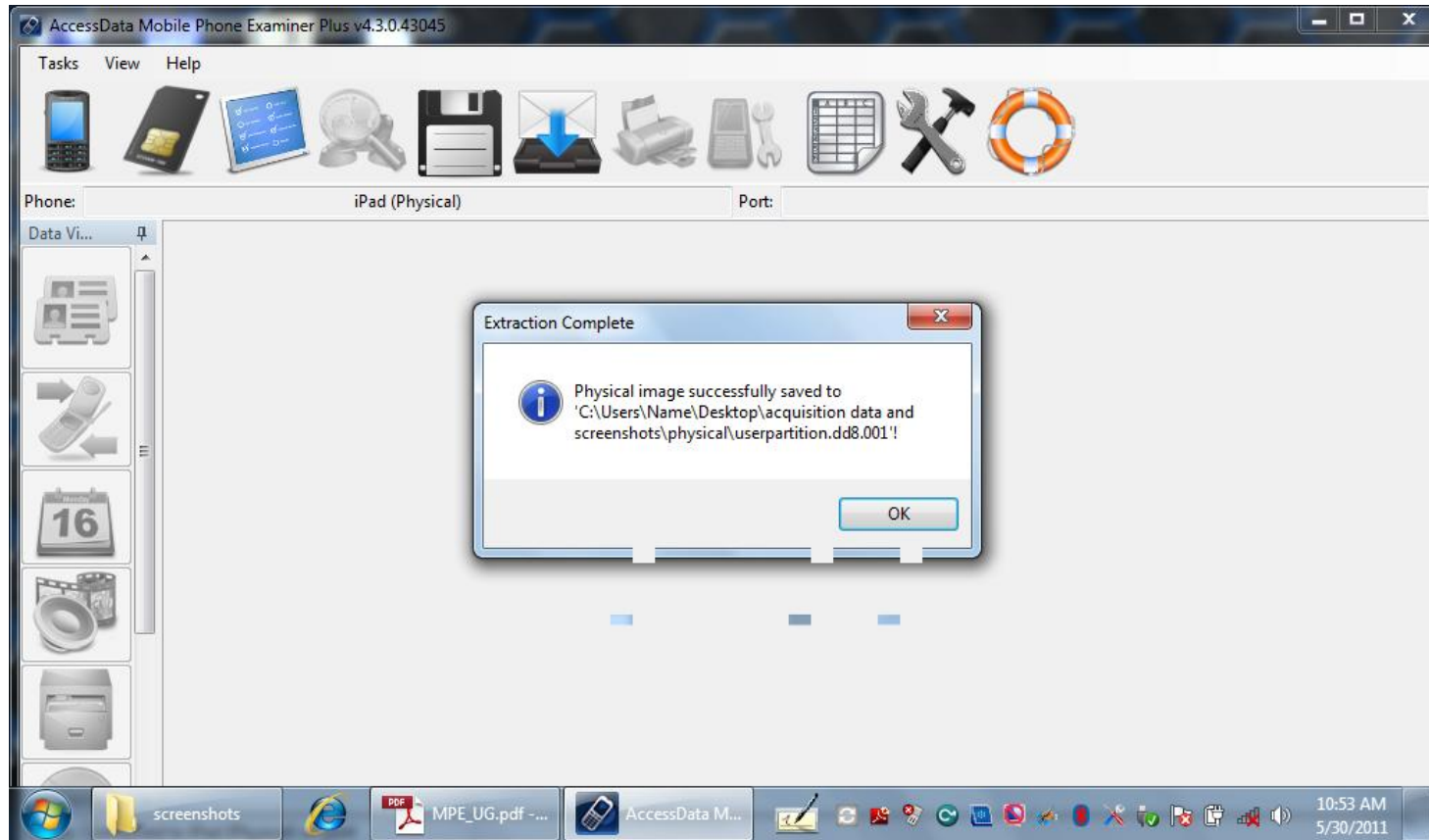
AccessData MPE+ Acquisizione fisica



AccessData MPE+ Acquisizione fisica



AccessData MPE+ Acquisizione fisica



Elcomsoft iOs Forensic Toolkit

Acquisizione fisica di iPhone4s/iPad2

- Collegamento del dispositivo alla workstation di acquisizione
- Avvio del software di jailbreaking Chronic-Dev Absinthe – Version 0.4



Elcomsoft iOs Forensic Toolkit

Acquisizione fisica di iPhone4s/iPad2

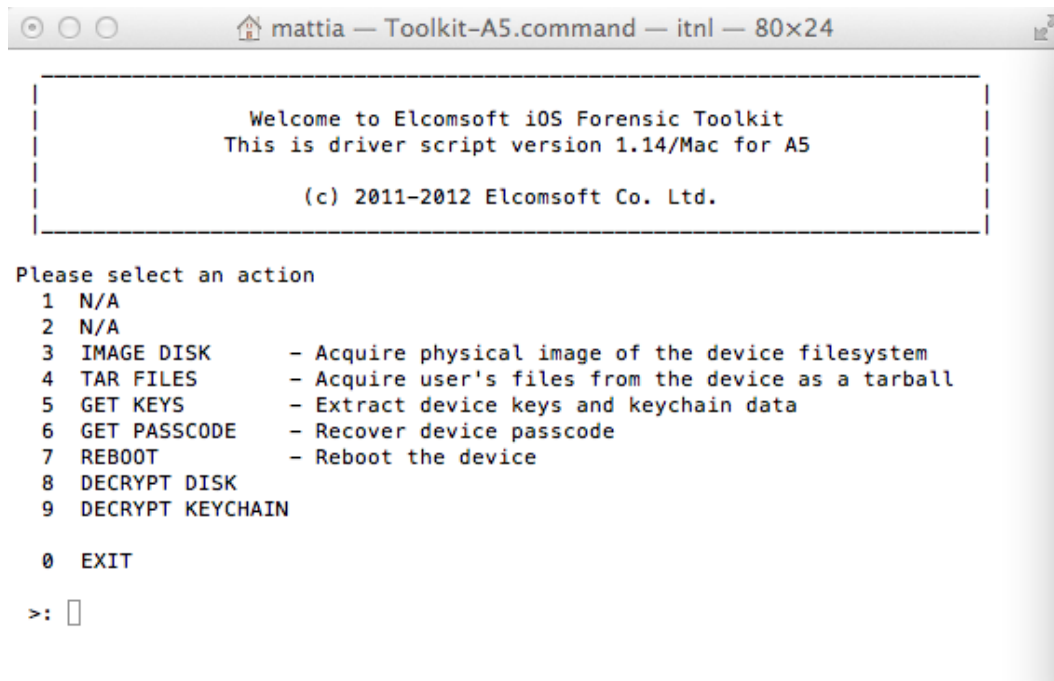
- Esecuzione delle attività di jailbreaking automatizzate



Elcomsoft iOS Forensic Toolkit

Acquisizione fisica di iPhone4s/iPad2

- Attivazione della connessione WiFi per completare le operazioni di jailbreaking mediante l'installazione del software di "installazione applicazioni" Cydia
- Installazione, attraverso Cydia, del software Open SSH
- Disattivazione della connessione WiFi
- Esecuzione di iOS Forensic Toolkit per dispositivi con processore A5 (script Toolkit-A5.command)



The screenshot shows a terminal window titled "mattia — Toolkit-A5.command — itnl — 80x24". The terminal output is as follows:

```
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.14/Mac for A5

(c) 2011-2012 Elcomsoft Co. Ltd.

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

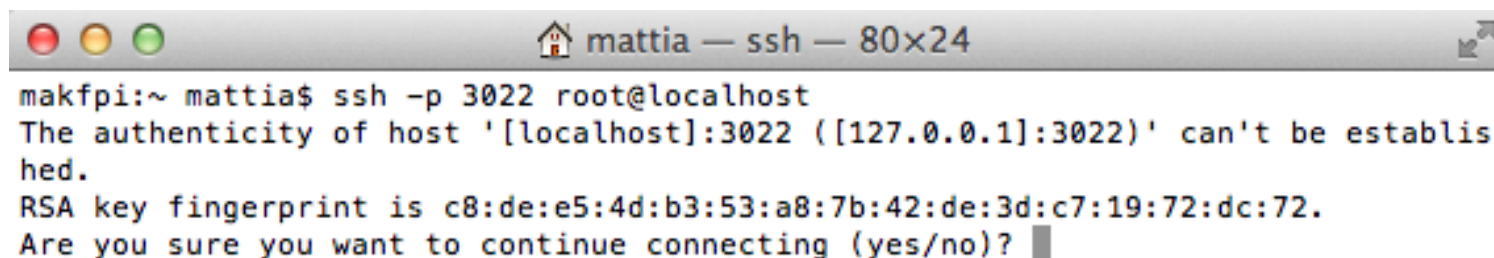
0 EXIT

>: █
```

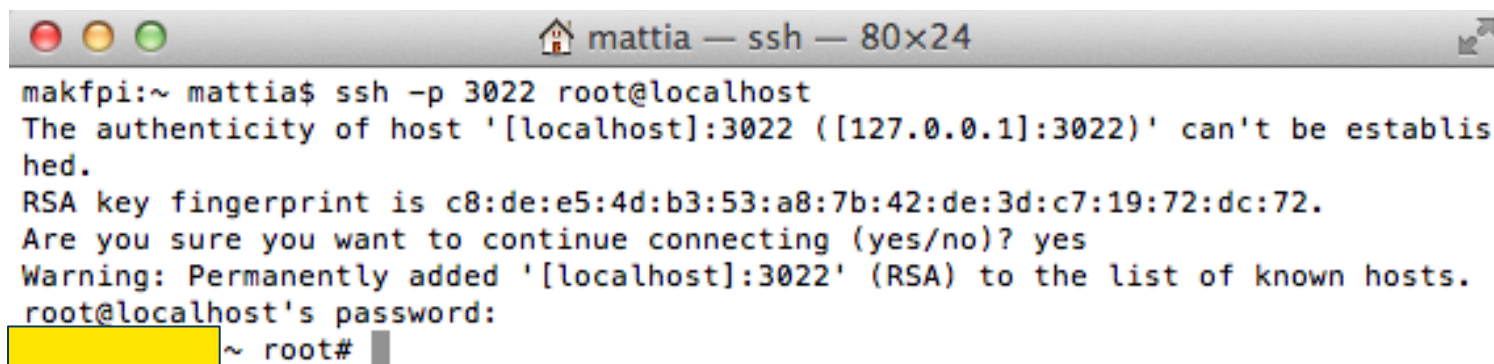
Elcomsoft iOs Forensic Toolkit

Acquisizione fisica di iPhone4s/iPad2

- Connessione mediante SSH da terminale attraverso il comando `ssh -p 3022 root@localhost`
- Inserimento della password di default (**alpine**)



```
mattia$ ssh -p 3022 root@localhost
The authenticity of host '[localhost]:3022 ([127.0.0.1]:3022)' can't be established.
RSA key fingerprint is c8:de:e5:4d:b3:53:a8:7b:42:de:3d:c7:19:72:dc:72.
Are you sure you want to continue connecting (yes/no)?
```



```
mattia$ ssh -p 3022 root@localhost
The authenticity of host '[localhost]:3022 ([127.0.0.1]:3022)' can't be established.
RSA key fingerprint is c8:de:e5:4d:b3:53:a8:7b:42:de:3d:c7:19:72:dc:72.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:3022' (RSA) to the list of known hosts.
root@localhost's password:
~ root#
```

Elcomsoft iOS Forensic Toolkit

Acquisizione fisica di iPhone4s/iPad2

- Estrazione delle chiavi memorizzate nel dispositivo attraverso l'utilizzo del software iOS Forensic Toolkit, opzione 5

```
mattia — Toolkit-A5.command — itnl — 80x24

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.14/Mac for A5

(c) 2011-2012 Elcomsoft Co. Ltd.

Please note that to extract device secrets you need to copy
acquisition tools to the device first. If you haven't done this
yet, please consult with documentation and Advisory 2012-01.

Continue? (Y/n): Y
Device passcode (optional):
Escrow file (optional):
Save data to file (relative to home directory) <keys.plist>: [redacted]
[redacted]

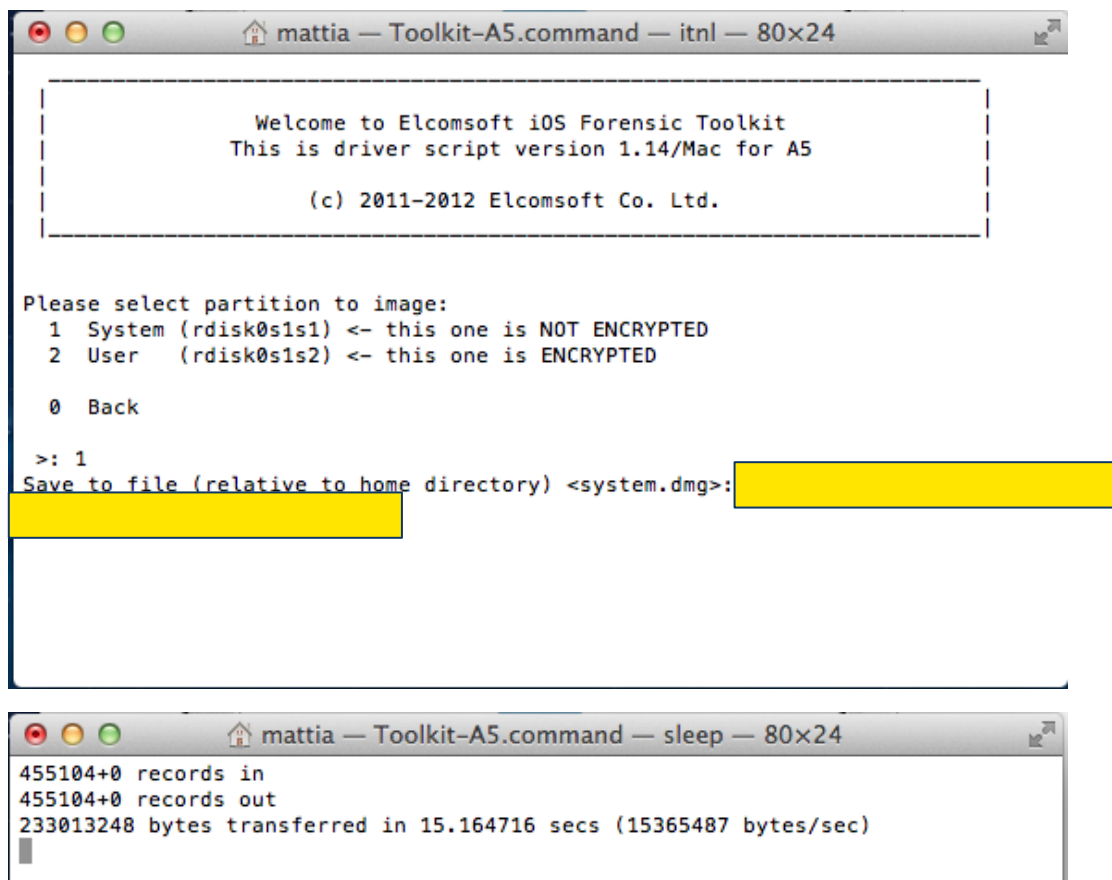
[INFO] Found running kernel at 0x80001000
[INFO] Device Serial Number: [redacted]
[INFO] Device does not have passcode set.
[INFO] Keychain version: 5
[INFO] Device does not have backup password set.

Press 'Enter' to continue
█
```

Elcomsoft iOS Forensic Toolkit

Acquisizione fisica di iPhone4s/iPad2

- Esecuzione della copia forense del **volume di sistema** (non cifrato) mediante l'utilizzo del software iOS Forensic Toolkit, opzione 3 e salvataggio nel file



```
mattia — Toolkit-A5.command — itnl — 80x24
-----
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.14/Mac for A5

(c) 2011-2012 Elcomsoft Co. Ltd.

Please select partition to image:
 1 System (rdisk0s1s1) <- this one is NOT ENCRYPTED
 2 User   (rdisk0s1s2) <- this one is ENCRYPTED
 0 Back

>: 1
Save to file (relative to home directory) <system.dmg>:
-----

mattia — Toolkit-A5.command — sleep — 80x24
455104+0 records in
455104+0 records out
233013248 bytes transferred in 15.164716 secs (15365487 bytes/sec)
```

Elcomsoft iOS Forensic Toolkit

Acquisizione fisica di iPhone4s/iPad2

- Esecuzione della copia forense del **volume dati**(cifrato) mediante l'utilizzo del software iOS Forensic Toolkit, opzione 3 e salvataggio nel file

```
mattia — Toolkit-A5.command — itnl — 80x24

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.14/Mac for A5

(c) 2011-2012 Elcomsoft Co. Ltd.

Please select partition to image:
 1 System (rdisk0s1s1) <- this one is NOT ENCRYPTED
 2 User (rdisk0s1s2) <- this one is ENCRYPTED

 0 Back

>: 2
Save to file (relative to home directory) <user.dmg>: 
```

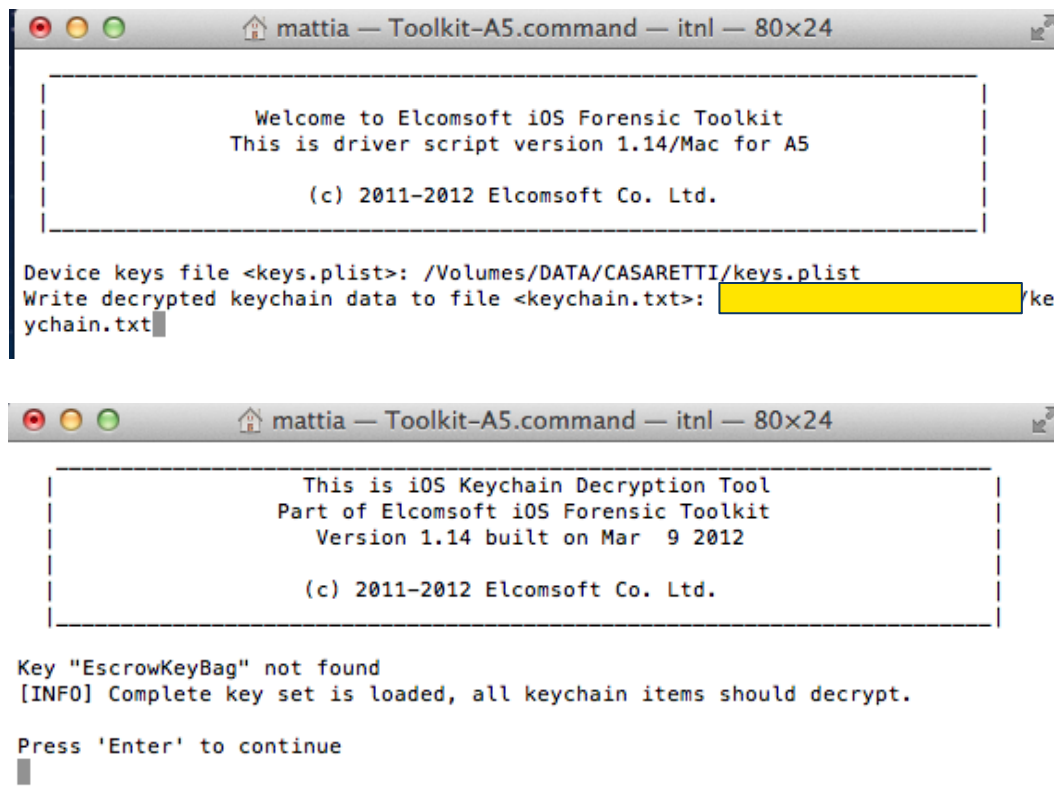
```
mattia — Toolkit-A5.command — sleep — 80x24

1254592+0 records in
1254592+0 records out
642351104 bytes transferred in 35.046090 secs (18328752 bytes/sec)
```

Elcomsoft iOS Forensic Toolkit

Acquisizione fisica di iPhone4s/iPad2

- **Decifratura del file keychain** mediante l'utilizzo del software iOS Forensic Toolkit, opzione 9 e salvataggio nel file **keychain.txt**



```
mattia — Toolkit-A5.command — itnl — 80x24

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.14/Mac for A5

(c) 2011-2012 Elcomsoft Co. Ltd.

Device keys file <keys.plist>: /Volumes/DATA/CASARETTI/keys.plist
Write decrypted keychain data to file <keychain.txt>: [redacted]keychain.txt

mattia — Toolkit-A5.command — itnl — 80x24

This is iOS Keychain Decryption Tool
Part of Elcomsoft iOS Forensic Toolkit
Version 1.14 built on Mar 9 2012

(c) 2011-2012 Elcomsoft Co. Ltd.

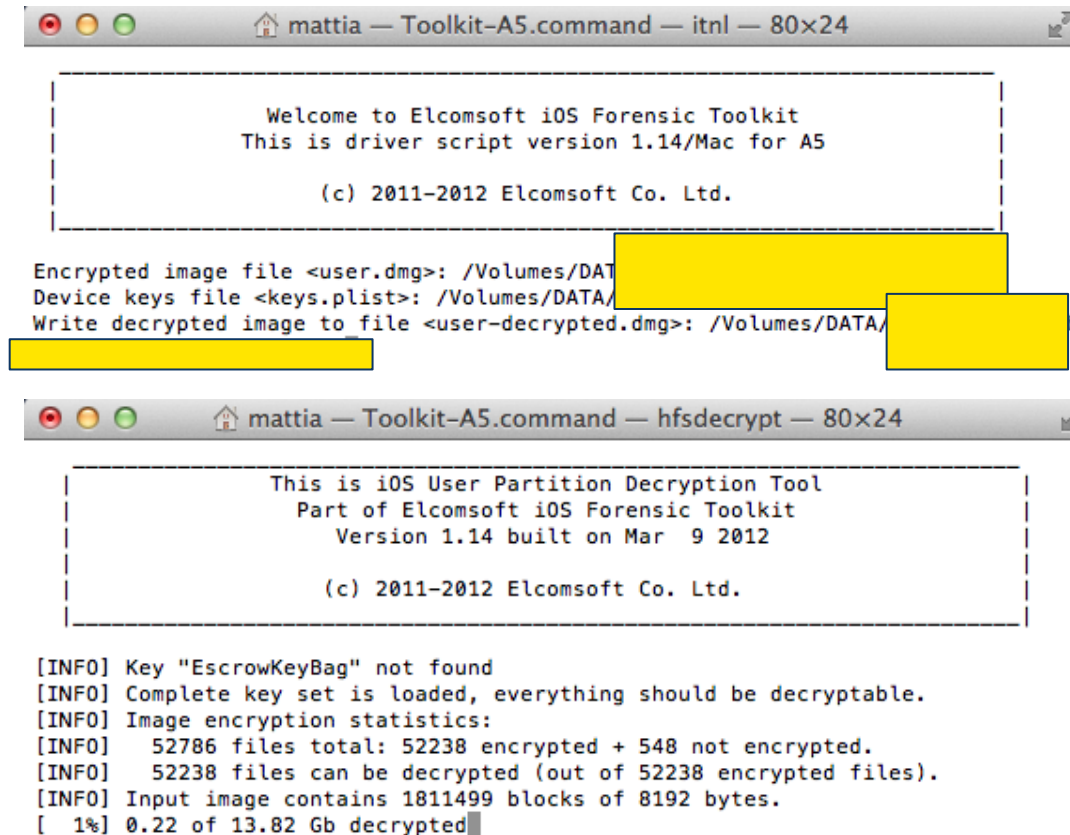
Key "EscrowKeyBag" not found
[INFO] Complete key set is loaded, all keychain items should decrypt.

Press 'Enter' to continue
```


Elcomsoft iOS Forensic Toolkit

Acquisizione fisica di iPhone4s/iPad2

- **Decifratura della partizione dati** mediante l'utilizzo del software iOS Forensic Toolkit, opzione 8 e salvataggio nel file



```
mattia — Toolkit-A5.command — itnl — 80x24
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.14/Mac for A5

(c) 2011-2012 Elcomsoft Co. Ltd.

Encrypted image file <user.dmg>: /Volumes/DATA/
Device keys file <keys.plist>: /Volumes/DATA/
Write decrypted image to file <user-decrypted.dmg>: /Volumes/DATA/

mattia — Toolkit-A5.command — hfsdecrypt — 80x24
This is iOS User Partition Decryption Tool
Part of Elcomsoft iOS Forensic Toolkit
Version 1.14 built on Mar 9 2012

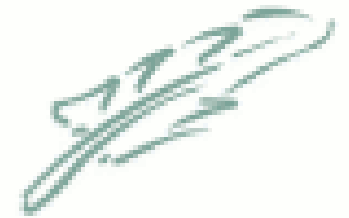
(c) 2011-2012 Elcomsoft Co. Ltd.

[INFO] Key "EscrowKeyBag" not found
[INFO] Complete key set is loaded, everything should be decryptable.
[INFO] Image encryption statistics:
[INFO] 52786 files total: 52238 encrypted + 548 not encrypted.
[INFO] 52238 files can be decrypted (out of 52238 encrypted files).
[INFO] Input image contains 1811499 blocks of 8192 bytes.
[ 1%] 0.22 of 13.82 Gb decrypted
```

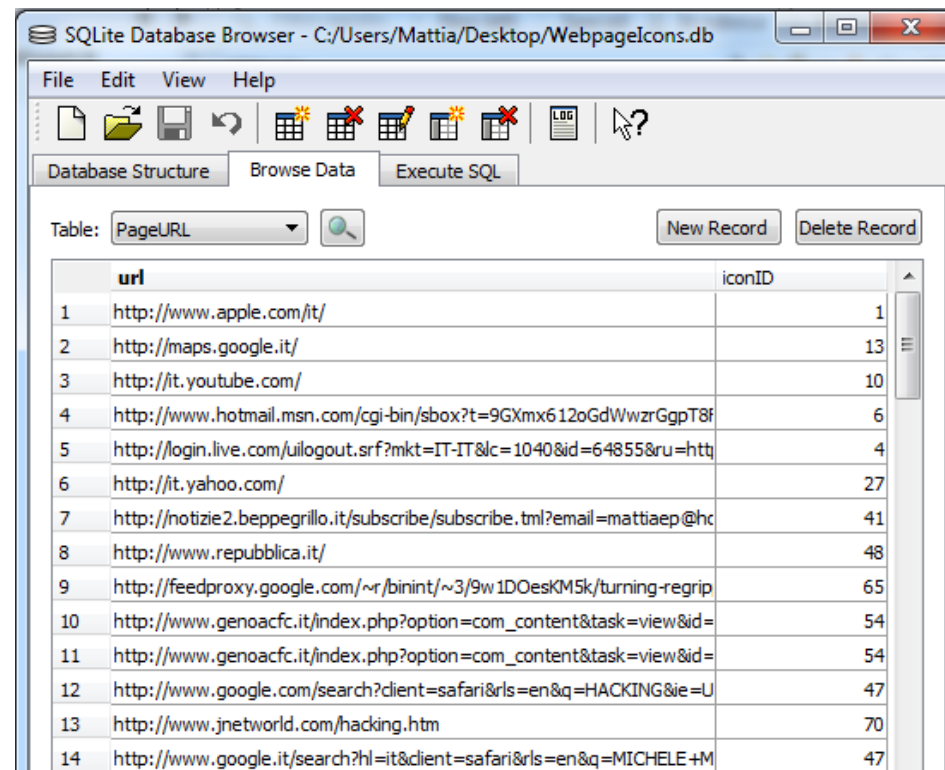
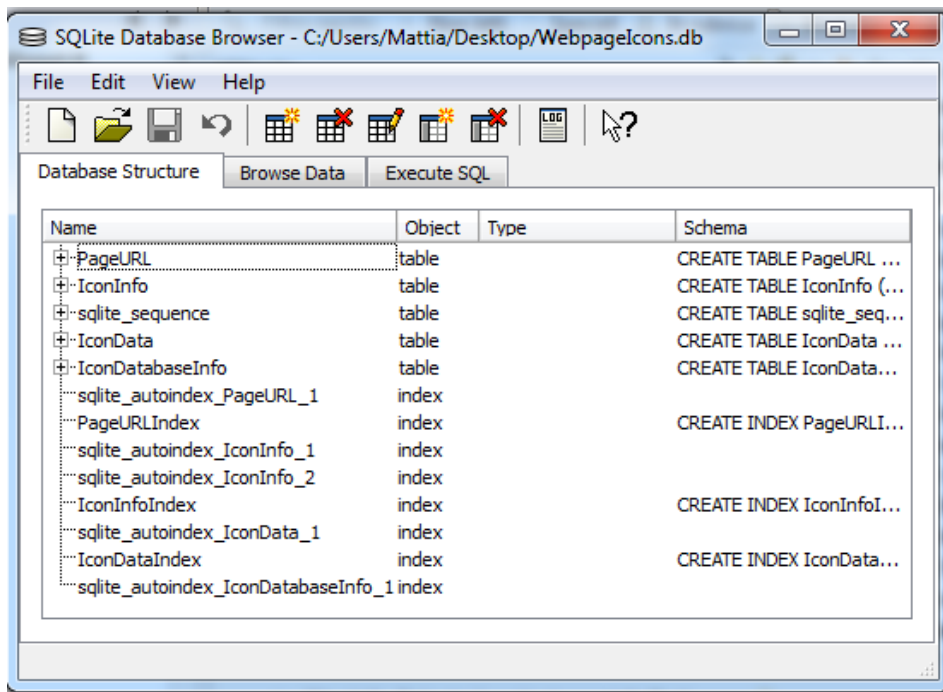
Analisi dei dati

- 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). Tipicamente si tratta di semplici file di te formattati in XML e n alcuni casi possono contenere dati in formato b
- Strumenti per la visualizzazione di tali file sono:
 - **SQLite Database Browser**, freeware per Windows, Linux e Mac
 - **SQLite Expert**, commerciale per Windows
 - **SQLite Manager**, plugin per Firefox
 - **plist Editor**, freeware per Windows
 - **PlistEdit** , commerciale per Mac
 - **Plist Viewer**, commerciale per Windows
 - **PIP**, commerciale per Window

SQLite



Analisi dei dati SQLite Database Browser









Analisi dei dati SQLite Expert Professional

SQLite Expert Professional 3.0.0.2035

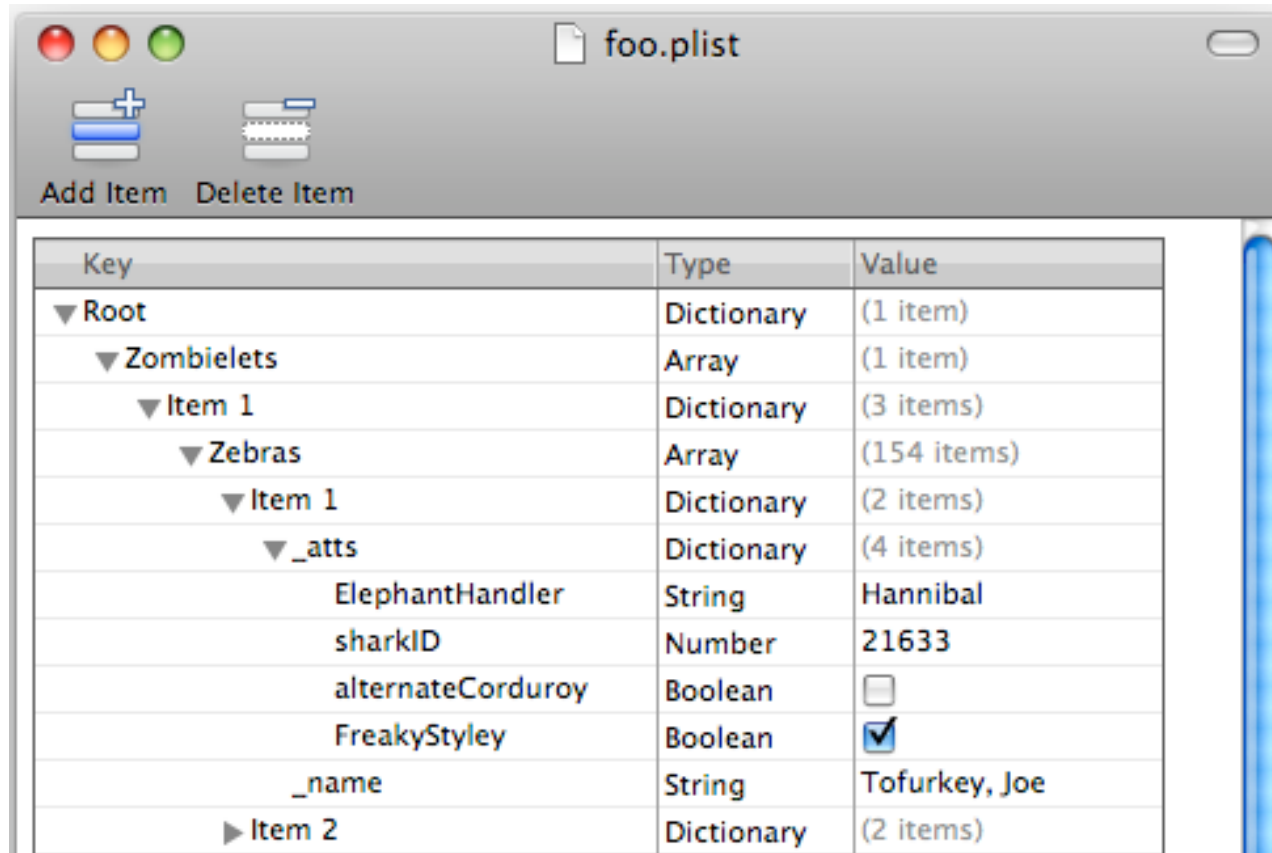
File Database Import/Export Table View SQL Transaction Scripting Tools Help

Database: dbdemos Table: biolife File: C:\ProgramData\SQLite Expert\Professional 3\Data\dbdemos.db3 SQLite Library: [internal] version 3.6.23.1

	Length (cm)	Length_In	Notes	Graphic
spicillum	50.00	19.69	Also known as the big spotted triggerfish. Inhabits outer reef areas and feeds upon crustaceans and mollusks by crushing them with powerful teeth. They are voracious eaters, and divers report seeing the clown triggerfish devour beds of pearl oysters.	
	60.00	23.62	Called seaperch in Australia. Inhabits the areas around lagoon coral reefs and sandy bottoms. The red emperor is a valuable food fish and considered a great sporting	
latus	229.00	90.16	This is the largest of all the wrasse. It is found in dense reef areas, feeding on a wide variety of mollusks, fishes, sea urchins, crustaceans, and other invertebrates. In spite of its immense size, divers find it a very wary fish.	
auarchus	30.00	11.81	Habitat is around boulders, caves, coral ledges and crevices in shallow waters. Swims alone or in groups. Its color changes dramatically from juvenile to adult. The mature adult	
	80.00	31.50	Also known as the coronation trout. It is found around coral reefs from shallow to very deep waters. Feeds primarily on small fishes. Although this rockcod is considered a good game and food fish, the	
	38.00	14.96	Also known as the turkeyfish. Inhabits reef caves and crevices. The firefish is usually stationary during the day, but feeds actively at night. Favorite foods are crustaceans.	
laticimus	19.00	7.48	Normally seen in pairs around dense coral areas from very shallow to	

Ready! Record 1 of 28

Analisi dei dati Property List Editor for Mac



Key	Type	Value
▼ Root	Dictionary	(1 item)
▼ Zombielets	Array	(1 item)
▼ Item 1	Dictionary	(3 items)
▼ Zebras	Array	(154 items)
▼ Item 1	Dictionary	(2 items)
▼ _atts	Dictionary	(4 items)
ElephantHandler	String	Hannibal
sharkID	Number	21633
alternateCorduroy	Boolean	<input type="checkbox"/>
FreakyStyley	Boolean	<input checked="" type="checkbox"/>
_name	String	Tofurkey, Joe
▶ Item 2	Dictionary	(2 items)

Analisi dei dati plist Editor for Windows

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
3 = <plist version="1.0">
4 = <dict>
5 = <key>WebHistoryDates</key>
6 = <array>
7 = <dict>
8 = <key></key>
9 = <string>http://www.facebook.com/?ref=home</string>
10 = <key>D</key>
11 = <array>
12 = <integer>5</integer>
13 = <integer>4</integer>
14 = </array>
15 = <key>lastVisitedDate</key>
16 = <string>302476660.3</string>
17 = <key>title</key>
18 = <string>Facebook</string>
19 = <key>visitCount</key>
20 = <integer>9</integer>
21 = </dict>
22 = <dict>
23 = <key></key>
24 = <string>http://www.facebook.com/mattiaep</string>
25 = <key>D</key>
26 = <array>
27 = <integer>1</integer>
28 = <integer>2</integer>
29 = </array>
30 = <key>lastVisitedDate</key>
31 = <string>302476567.8</string>
32 = <key>title</key>
33 = <string>Facebook | Mattia Epifani</string>
34 = <key>visitCount</key>
35 = <integer>3</integer>
36 </dict>
```

Analisi dei dati Calendario

- Le informazioni relative agli eventi in agenda sono conservate in 1 file SQLite

File/Percorso

Descrizione

/mobile/Library/Calendar/Calendar.sqlite3

Lista degli eventi in agenda

Oxygen Forensic Suite 2011 (Trial)

Main Mostra Strumenti Servizio Guida

Tutti i dispositivi Dispositivi senza causa Nuovo dispositivo (iPad) - 31/05/2011 16:54:59 [012328005073490] Agenda Criterio di filtro ...

Cerca Esporta Stampa Risetta filtri Guida

You can start Oxygen Forensic Suite 2011 Trial version 30 times only until 11/06/2011. Attempts remaining: 19. [Ordina la versione completa ora!](#)

Info	Tipo	Inizio	Fine	Allarme	Testo
<input checked="" type="checkbox"/>	Appuntamenti	17/02/2011 08:00	17:00		[perfezionisti] Segnalazione convegno domani {01}

Informazione d'evento

Appuntamenti
Inizio: 17/02/2011 08:00
Fine: 17/02/2011 17:00
Testo: [perfezionisti] Segnalazione convegno domani {01}
MD5 Hash:
ad5d555b764997c9b257037f3be50e1d

[perfezionisti] Segnalazione convegno domani {01}

Generali Memo Ricorrenza

Testo: [perfezionisti] Segnalazione convegno domani {01}

Posizione:

Inizio: 17/02/2011 su 08:00

Fine: su 17:00

Allarme: Nessun segnale

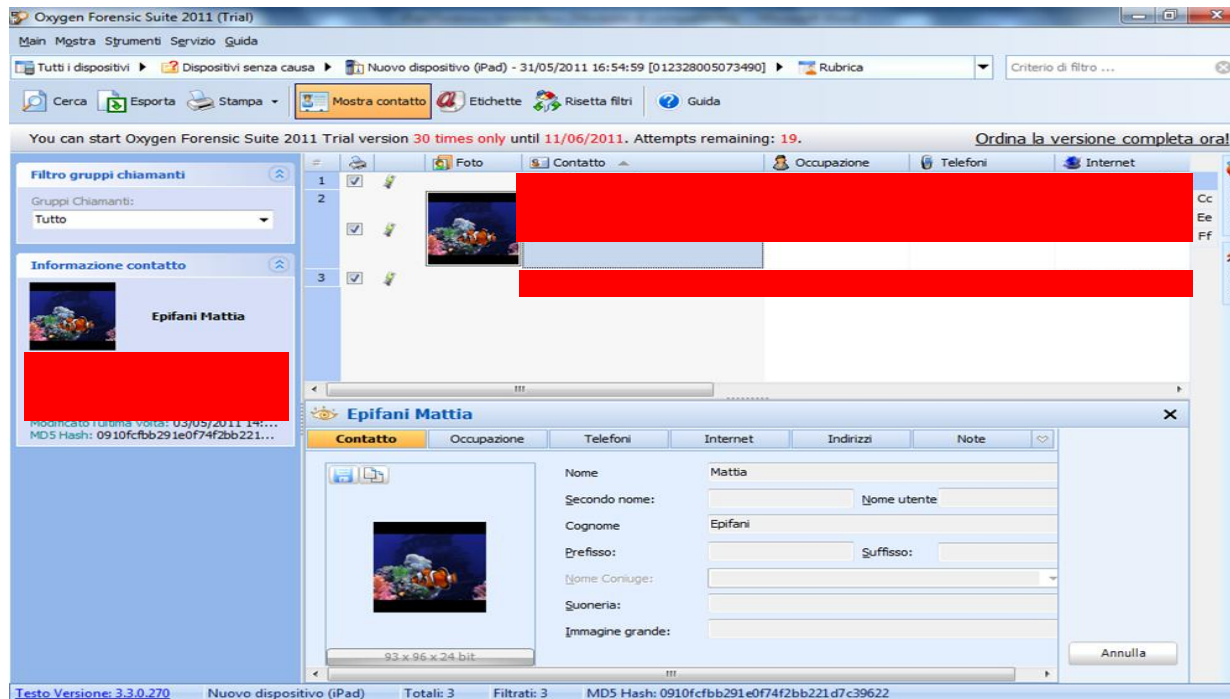
Annulla

Testo Versione: 3.3.0.270 Nuovo dispositivo (iPad) Totali: 1 Filtrati: 1 MD5 Hash: ad5d555b764997c9b257037f3be50e1d

Analisi dei dati Address Book

- Le informazioni relative ai contatti sono conservate in **3 file SQLite**

File/Percorso	Descrizione
/mobile/Library/AddressBook/AddressBook.sqlitedb	Lista dei contatti ed e-mail usate di recente
/mobile/Library/AddressBook/AddressBookImages.sqlitedb	Immagini associate ai contatti
/mobile/Library/Preferences/com.apple.MobileAddressBook.plist	Ultima pagina selezionata e ultimo contatto selezionato



Analisi dei dati

Mappe e Note

- Le informazioni relative all'utilizzo dell'applicativo Mappe sono conservate in **3 file plist**:

File/Percorso	Descrizione
/mobile/Library/Maps/Directions.plist	Cronologia dei luoghi e dei percorsi cercati (i dati sono codificati in Base64)
/mobile/Library/Maps/History.plist	
/mobile/Library/Preferences/com.apple.Maps.plist	Ultima posizione vista e ultima locazione dell'utente codificata in Base64

- Le informazioni relative all'utilizzo dell'applicativo Note sono conservate in **1 file SQLite**:

File/Percorso	Descrizione
/mobile/Library/Notes/notes.db	Note

Analisi dei dati Safari

File/Percorso	Descrizione
/mobile/Library/Safari/Bookmarks.db	Bookmark
/mobile/Library/Safari/History.plist	Cronologia dei siti visitati
/mobile/Library/Safari/SuspendState.plist	Stato in cui si trovava Safari quando è stato chiuso l'ultima volta
/mobile/Library/Caches/Safari/RecentSearches.plist	Ricerche effettuate con Safari
/mobile/Library/Caches/com.apple.mobilesafari/Cache.db	Cache di Safari
/mobile/Library/Cookies/Cookies.binarycookies	Cookie di Safari

Analisi dei dati Safari

Oxygen Forensic Suite 2011 (Trial)

Main Mgrsta Strumenti Servizio Guida

Tutti i dispositivi >> Nuovo dispositivo (iPad) - 31/05/2011 16:54:59 [012328005073490] > Analizzatore Cache Browser > Safari

Cerca Esporta Stampa Filtri Anteprime Ordina Guida

You can start Oxygen Forensic Suite 2011 Trial version 30 times only until 11/06/2011. Attempts remaining: 19. [Ordina la versione completa oral](#)

Impegni per oggetti selezionati

- Salva su ...
- Mostra proprietà

Informazione oggetto

Nome: SuspendState.plist
Tipo: File PLIST
Dimensione: 8,85 KB
Percorso: c:\private\var\mobile\Library\Safari
MD5 Hash: 1d7dbb94413013d3a29a72010338cf9a

Name	Path	Type	Size
SuspendState.plist	c:\private\var\mobile\Library\Safari\	File PLIST	8,85 KB
History.plist	c:\private\var\mobile\Library\Safari\	File PLIST	10,56 KB
D21E3D07-CF20-4139-8EA...	c:\private\var\mobile\Library\Caches\Safari\Thumbnails\	IrfaView PNG File	28,46 KB
Cookies.binarycookies	c:\private\var\mobile\Library\Cookies\	File BINARYCOOKIES	12,97 KB
com.apple.itunesstored.plist	c:\private\var\mobile\Library\Cookies\	File PLIST	1,48 KB
com.apple.itunesstored.2.s...	c:\private\var\mobile\Library\Cookies\	File SQLITEDB	12,01 KB
com.apple.iAd.cookieadb	c:\private\var\mobile\Library\Cookies\	File COOKIEDB	12,01 KB
Bookmarks.db	c:\private\var\mobile\Library\Safari\	Data Base File	68,01 KB
42471AD8-858E-41B0-8F9...	c:\private\var\mobile\Library\Caches\Safari\Thumbnails\	IrfaView PNG File	22,48 KB
3485907B-822A-4010-9E0...	c:\private\var\mobile\Library\Caches\Safari\Thumbnails\	IrfaView PNG File	29,78 KB

Modalità: Testo Codificazione: ANSI (Windows)

Modalità: Testo Codificazione: ANSI (Windows) Nessuna selezione

Testo Versione: 3.3.0.270 Nuovo dispositivo (iPad) Totali:10 oggetti (8,85 KB) Selezionato: SuspendState.plist MD5 Hash: 1d7dbb94413013d3a29a72010338cf9a

Analisi dei dati Mail

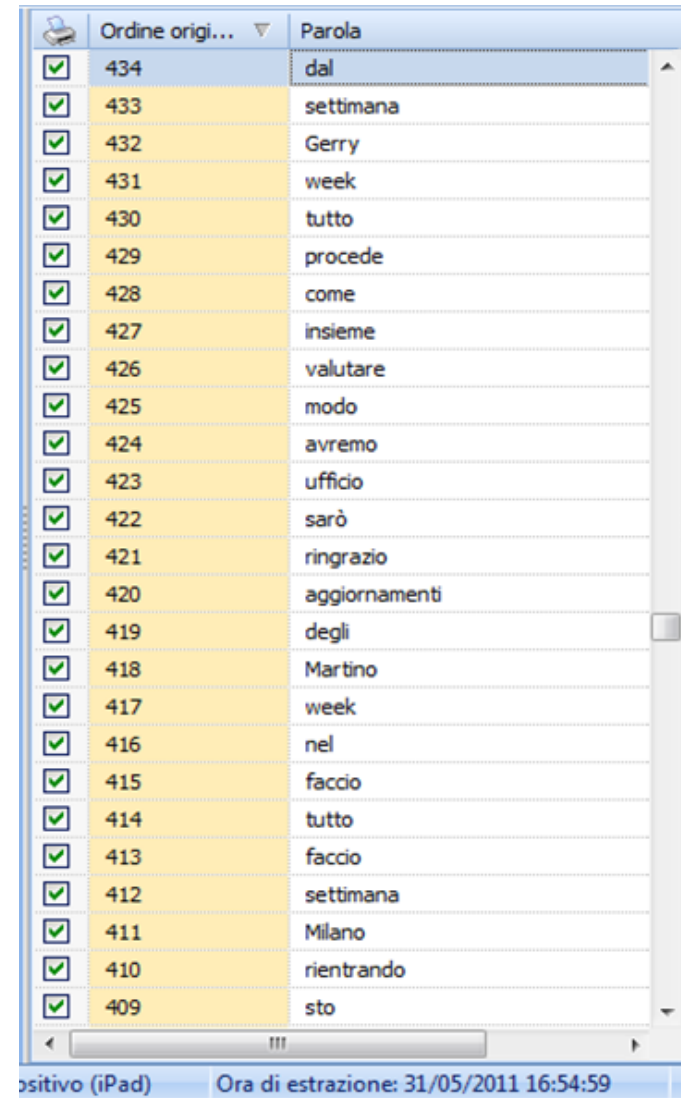
- Le informazioni relative al software Mail sono conservate in **2 file SQLite, 1 file plist e file in formato EMLX**:

File/Percorso	Descrizione
/mobile/Library/Mail/Envelope Index	Database SQLite, contiene le mailbox usate e i messaggi (solo timestamp e associazione intestazione/contenuto del messaggio)
/mobile/Library/Mail/Protected Index	Database SQLite, contiene i messaggi (intestazione/contenuto del messaggio)
/mobile/Library/Mail/OrphanedDraft-[app]	Draft di e-mail in formato testo scritte ma non inviate attraverso un'app (es.: com.apple.youtube)
/mobile/Library/Mail/Attachments/	Allegati
/mobile/Library/Mail/	Cartelle contenente messaggi in formato EMLX
/mobile/Library/Mail/metadata.plist	Mailbox usate
/mobile/Library/Preferences/com.apple.accountsettings.plist	Account e-mail configurati

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.

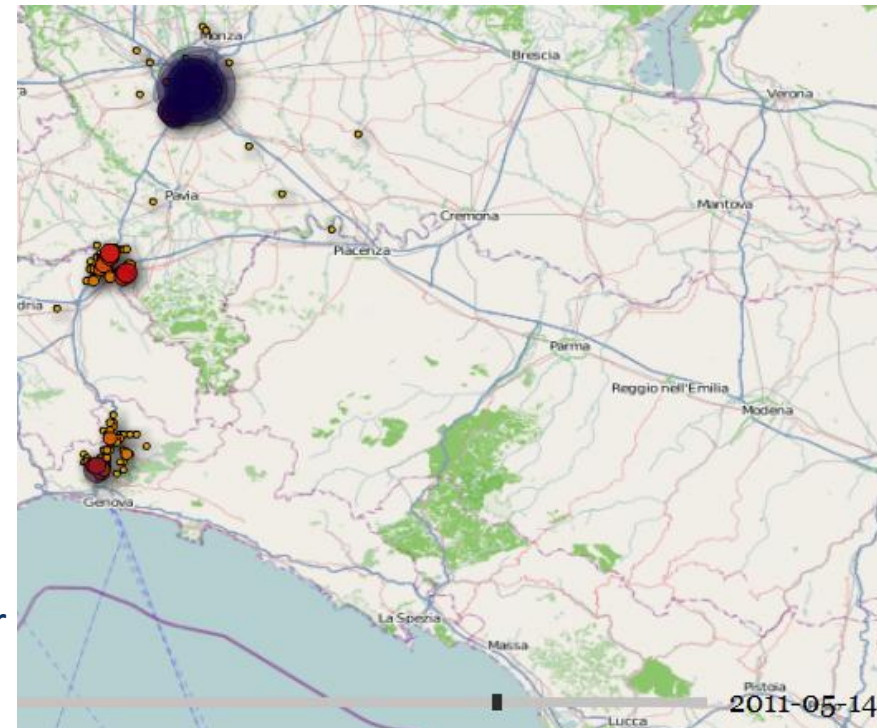


Ordine origi...	Parola
434	dal
433	settimana
432	Gerry
431	week
430	tutto
429	procede
428	come
427	insieme
426	valutare
425	modo
424	avremo
423	ufficio
422	sarò
421	ringrazio
420	aggiornamenti
419	degli
418	Martino
417	week
416	nel
415	faccio
414	tutto
413	faccio
412	settimana
411	Milano
410	rientrando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

positivo (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/>



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 mediante 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

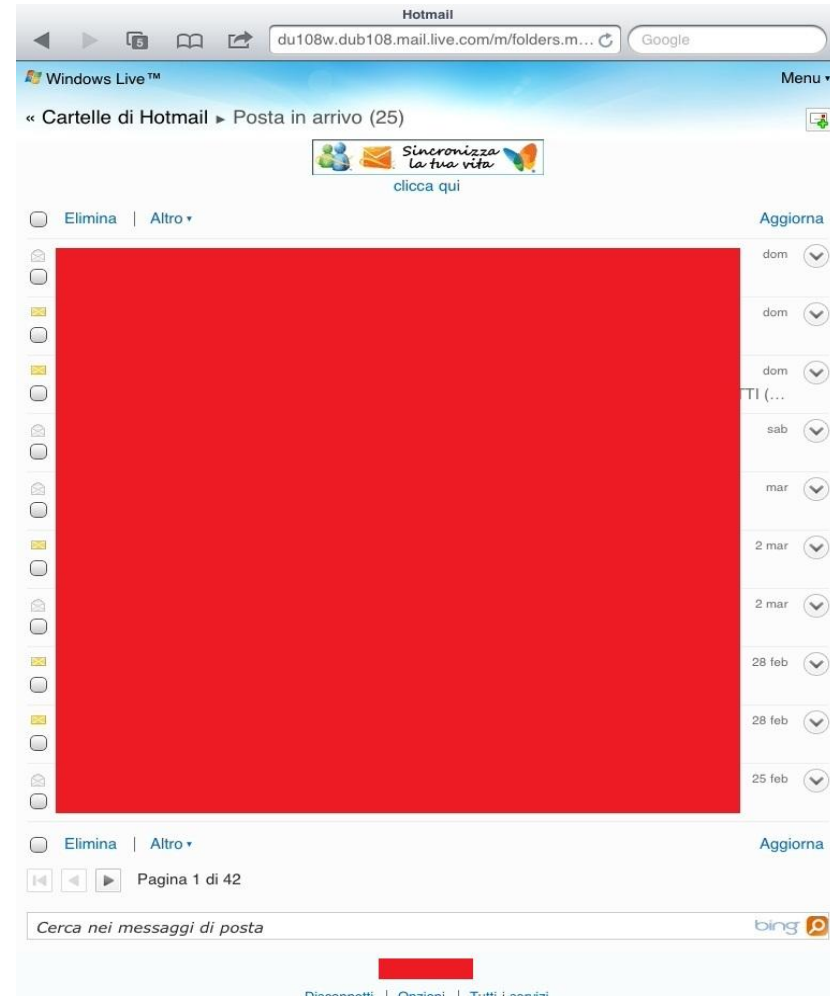
- Sono stati effettuati test su dispositivo iPad di prima generazione, modello Wi-Fi + 3G, con 64 GB di spazio disco già utilizzato abitualmente per qualche mese sia per svago sia per lavoro
- Sul dispositivo esaminato sono stati recuperati:
 - 9.525 immagini in formato PNG
 - 1.808 immagini in formato 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



Tanto per fare un esempio di informazione "non standard". il menu

Analisi dei dati Keyword Search

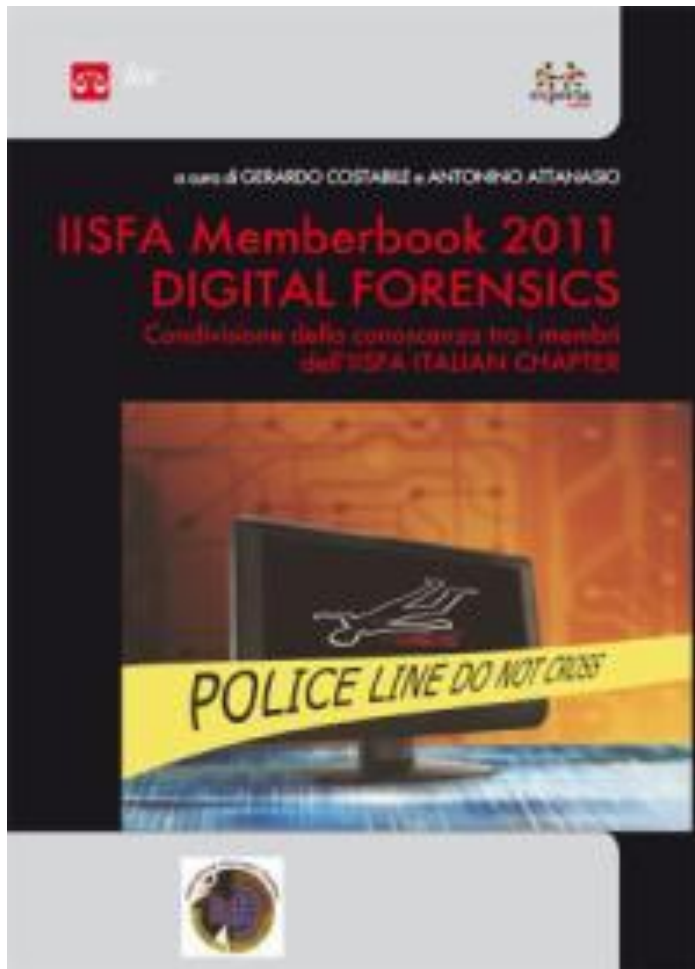
- La ricerca per parola chiave è utile per recuperare informazioni cancellate e non estraibili mediante file carving.
- Un esempio è costituito dalle email in formato EMLX che sono cancellate dal dispositivo in modo logico (p.es accesso tramite IMAP)
- Le parole chiave che si possono utilizzare a tal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

```
272800 65 66 3D 33 44 22 6D 61-69 6C 74 6F 3A 77 65 62 ef=3D"mailto:web
272810 6D 61 73 74 65 72 40 69-69 73 66 61 2E 69 74 3F master@iisfa.it?
272820 73 75 62 6A 65 63 74 3D-33 44 4F 67 67 25 33 41 subject=3Dogg%3A
272830 25 32 30 53 69 74 6F 25-32 30 77 77 77 25 3D 0A %20Sito%20www%20
272840 32 45 69 69 73 66 61 25-32 45 69 74 25 32 30 65 2Eiisfa%2Eit%20e
272850 25 32 30 43 4D 53 25 32-30 64 69 25 32 30 6E 75 %20CMS%20di%20nu
272860 6F 76 6F 25 32 30 6F 6E-25 32 30 6C 69 6E 65 22 ovo%20on%20line"
272870 20 73 74 79 6C 65 3D 33-44 22 6D 61 72 67 69 6E style=3D"margin
272880 2D 72 69 67 68 74 3A 20-30 3B 20 3D 0A 70 61 64 -right: 0; =-pad
Sel start = 2566176, len = 7; clus = 596484; log sec = 596484
```

I bugs non finiscono mai....

- Dall'uscita di iOS 5 diversi sono stati i bugs riscontrati.
- Tra i più curiosi:
- **Anyone with a Smart Cover can break into your iPad 2**, pubblicato il 20/10/2011
<http://9to5mac.com/2011/10/20/anyone-with-a-smart-cover-can-break-into-your-ipad-2/>
- **Bad Siri! She'll let anyone use a locked iPhone 4S**, pubblicato il 19/10/2011
http://news.cnet.com/8301-27080_3-20122632-245/bad-siri-shell-let-anyone-use-a-locked-iphone-4s/#ixzz1mZ7n7Zll
- L'aggiornamento di Apple (iOS 5.0.1), pubblicato il 10/11/2011, ha risolto entrambi i problemi.
- Ma non è finita qui....
- **Incorrect time setting could leak iOS 5 album pictures**, pubblicato il 31/12/2011
<http://peekay.org/2011/12/31/incorrect-time-setting-could-leak-ios-5-album-pictures/>
- **Perusing the private address book and making live video calls — all from a locked iPhone 4**, pubblicato il 5/2/2012
<http://peekay.org/2012/02/05/more-fun-with-locked-iphone-4/>

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>
- **Demystifying iPhone Forensics on iOS 5**
<http://securityxploded.com/demystifying-iphone-forensics-on-ios5.php>

Android Forensics

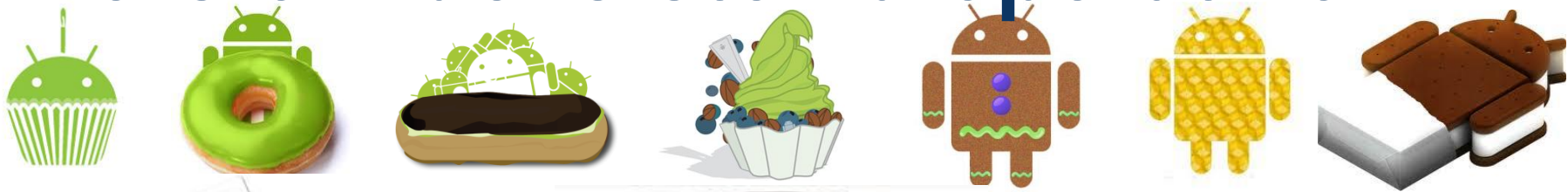


Android

- Android è una piattaforma mobile open source basata sul kernel 2.6 di linux e gestita da Open Handset Alliance (di cui Google è capofila)
- Primo modello: ottobre 2008

Mobile operators	Software companies	Commercialization companies	Semiconductor companies	Handset manufacturers
<ul style="list-style-type: none">• KDDI Corporation• NTT DoCoMo• Sprint Nextel• T-Mobile• China Mobile• Telecom Italia• Telefónica	<ul style="list-style-type: none">• Ascender Corporation• eBay• Google• LivingImage• Myriad• Nuance Communications• PacketVideo• SkyPop• SONIVOX	<ul style="list-style-type: none">• Aplix• Noser Engineering• The Astonishing Tribe• Wind River Systems	<ul style="list-style-type: none">• Audience• Broadcom Corporation• CSR Plc. (joined as SiRF)• Intel Corporation• Marvell Technology Group• Nvidia Corporation• Qualcomm• Synaptics• Texas Instruments	<ul style="list-style-type: none">• HTC• LG• Sony• Motorola Mobility (joined as Motorola)• Samsung Electronics

Versioni del sistema operativo



- April 15, 2009: ver. 1.5 (**Cupcake**)
- September 16, 2009: ver. 1.6 (**Donut**)
- October 5, 2009: ver. 2.0/2.1 (**Éclair**)
- May 20, 2010: ver. 2.2 (**Froyo**)
- December 6, 2010: ver. 2.3 (**Gingerbread**)
- February 2011: ver. 3.0 (**Honeycomb**)
- 19 October 2011: ver. 4.0 (**Ice Cream Sandwich**)

Caratteristiche

- Android nasce dall'inizio come sistema operativo **«always on-line»**
- Ha la possibilità di estendere facilmente le proprie funzionalità tramite l'installazione di applicazioni tramite «Android market» (oggi «Play Store»)
- L'utente ha la possibilità di trasportare nel telefono i propri dati, nella memoria flash interna (NAND) oppure nella memoria estraibile (SD card)

Componenti

- CPU (ARM)
- Baseband Modem/Radio
- Memoria RAM
- NAND Flash
- GPS
- Wireless
- Bluetooth
- Scheda SD
- Monitor
- Fotocamera
- Accelerometro
- Giroscopio
- USB

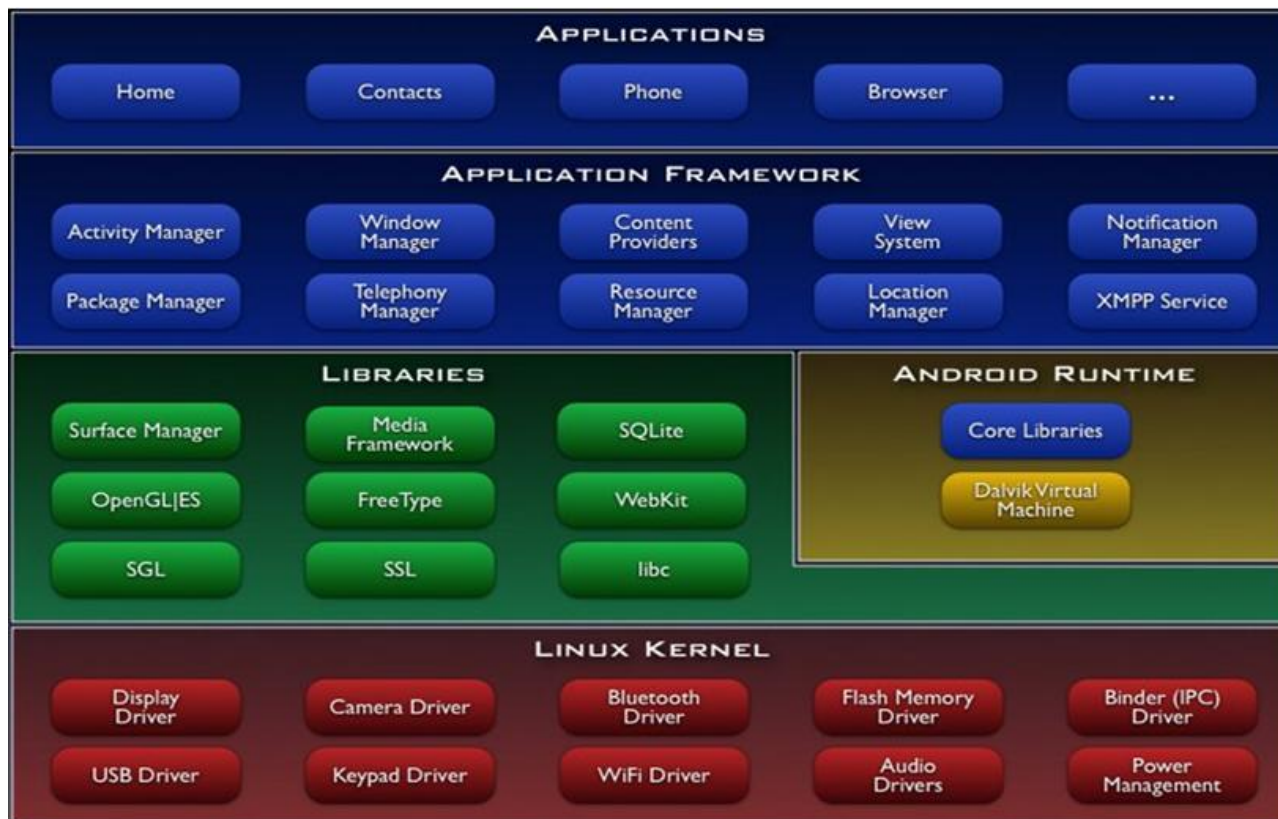
Boot process

1. **Power on:** Esecuzione del Boot “ROM” code (specifico per la CPU). Copia del boot loader in RAM
2. **The boot loader:** esecuzione in RAM del “IPL” (Initial program loader) che prepara l’avvio del “SPL”. “SPL” (Second program loader) inizializza i componenti hardware, identifica il Linux Kernel e lo copia in RAM
3. **The Linux kernel:** legge il root filesystem dalla NAND
4. **The init process:** come in Linux lo script init avvia il sistema ed i processi utente
5. **Zygote and Dalvik:** ogni applicazione gira in una “sandbox”. Zygote inizializza l’ambiente. Dalvik è la macchina virtuale in cui girano le applicazioni (the sandbox).
6. **The system server:** esegue le applicazioni base come la telefonia e la rete
7. **Boot complete:** comunica a tutte le applicazioni che il boot è completo

Architettura

- Android è basato sul kernel 2.6 di linux che fornisce il software fondamentale per gestire sia l'hardware che le applicazioni
- Un set di librerie è stato implementato per permettere agli sviluppatori di accedere alle funzionalità principali
- La libreria SQLite fornisce un metodo per gestire il salvataggio dei dati strutturati

Architettura



[http://en.wikipedia.org/wiki/Android_\(operating_system\)](http://en.wikipedia.org/wiki/Android_(operating_system))

Architettura

- La **Dalvik Virtual Machine (sandbox)** è stata realizzata per creare un ambiente sicuro e efficiente per le applicazioni mobile
- **Ogni applicazione Android gira in un'istanza separata della DVM**

Content provider

- I content provider sono il sistema con cui un applicazione può «esporre» i dati per condividerli con altre applicazioni
- Per esempio le applicazioni di terze parti possono accedere a SMS, Contatti, Calendario e Gmail attraverso i content provider

OS Security

- Quando si installa un'applicazione, **Android verifica che il file di installazione (.apk) abbia un certificato valido** (opzione disabilitabile). Poi verifica a quali risorse accede l'applicazione e richiede l'autorizzazione all'utente.
- Android crea un'istanza della Dalvik VM (con uno specifico user e group ID).
- L'applicazione può accedere esclusivamente ai dati ed alla memoria della propria macchina virtuale

Rooting

- Il «Rooting» del dispositivo consiste nel processo di acquisizione dei diritti amministrativi (root access) sul sistema android.
- Tale operazione viene eseguita per bypassare le limitazioni imposte dal sistema.
 - ◆ Installazione di applicazioni specifiche
 - ◆ Installazione di sistemi operativi alternativi (cooked roms)
- **Il rooting è analogo al jailbreaking dei sistemi operativi Apple iOS**

Rooting

- Il rooting del dispositivo di base sulla presenza di «bug» nelle varie versioni di Android o specifiche dei singoli prodotti
- Le community sviluppano e rilasciano continuamente applicazioni che sfruttano i «bug» per ottenere i privilegi di root

Android OS Debug Bridge

- Quando si connette un dispositivo tramite porta USB, viene presentato un menu con quattro opzioni
 - ◆ Ricarica del telefono
 - ◆ Sincronizzazione dei dati
 - ◆ Utilizzo del dispositivo come disco USB
 - ◆ Utilizzo del dispositivo come modem

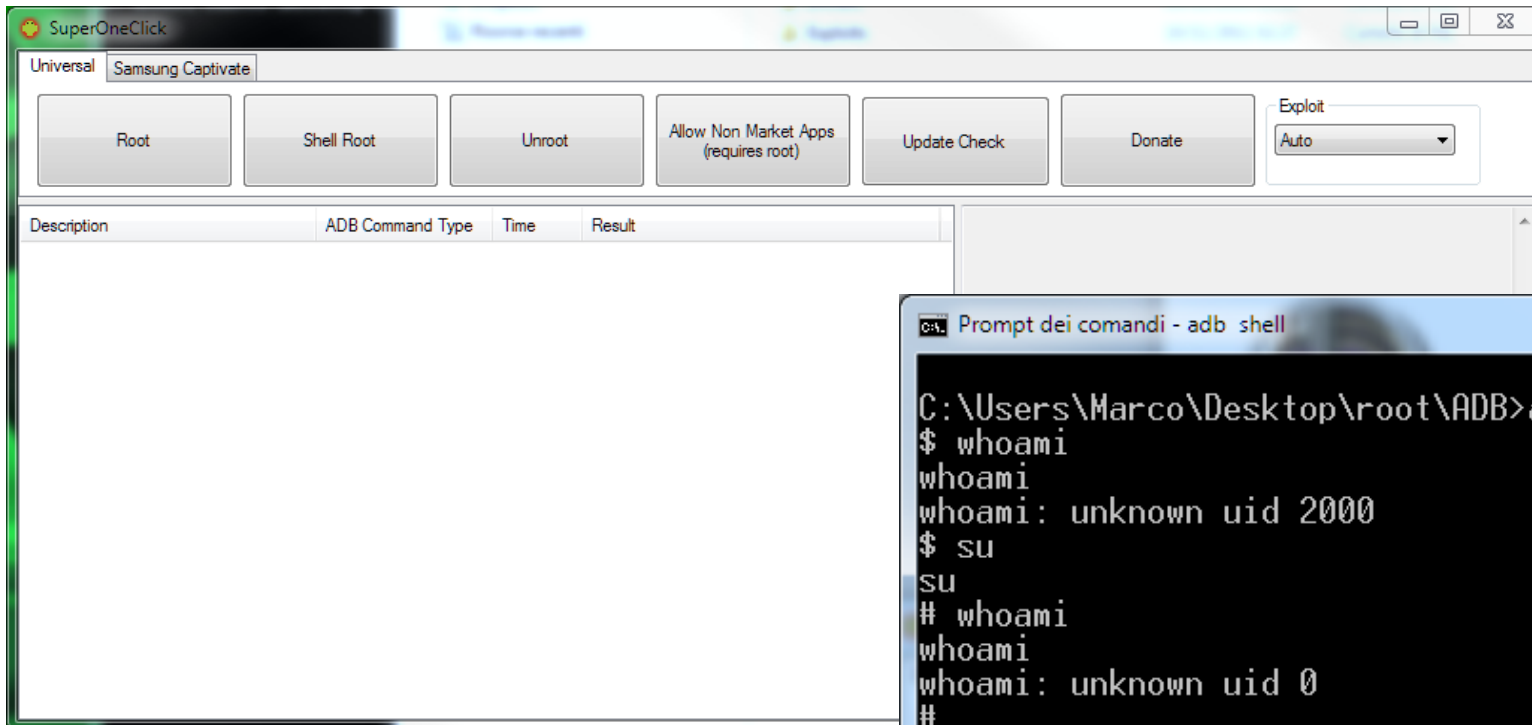
Android OS Debug Bridge

- Esiste una quinta opzione che va abilitata esplicitamente denominata **ADB (Android Debug Bridge)**
- Una volta abilitata è possibile connettersi al dispositivo attraverso una utility (ADB.exe) a riga di comando che apre una shell remota
- La shell viene aperta con privilegi limitati
- **Nei dispositivi «rootati» l'accesso avviene con diritti amministrativi**

Android OS Debug Bridge

- Android OS Debug Bridge permette di
 - ◆ Eseguire comandi della shell
 - ◆ Installare applicazioni da riga di comando
 - ◆ Copiare file e cartelle dal dispositivi al PC (e viceversa)
 - ◆ Visualizzare i file di log

Processo di rooting



The image shows the SuperOneClick software interface for rooting a Samsung Captivate. The interface includes buttons for 'Root', 'Shell Root', 'Unroot', 'Allow Non Market Apps (requires root)', 'Update Check', and 'Donate'. A dropdown menu for 'Exploit' is set to 'Auto'. Below these buttons is a table with columns for 'Description', 'ADB Command Type', 'Time', and 'Result'. In the foreground, a terminal window titled 'Prompt dei comandi - adb shell' displays the following commands and output:

```
C:\Users\Marco\Desktop\root\ADB>adb shell
$ whoami
whoami
whoami: unknown uid 2000
$ su
su
# whoami
whoami
whoami: unknown uid 0
#
```

Filesystem in Android

Android supporta numerosi tipi di filesystem:

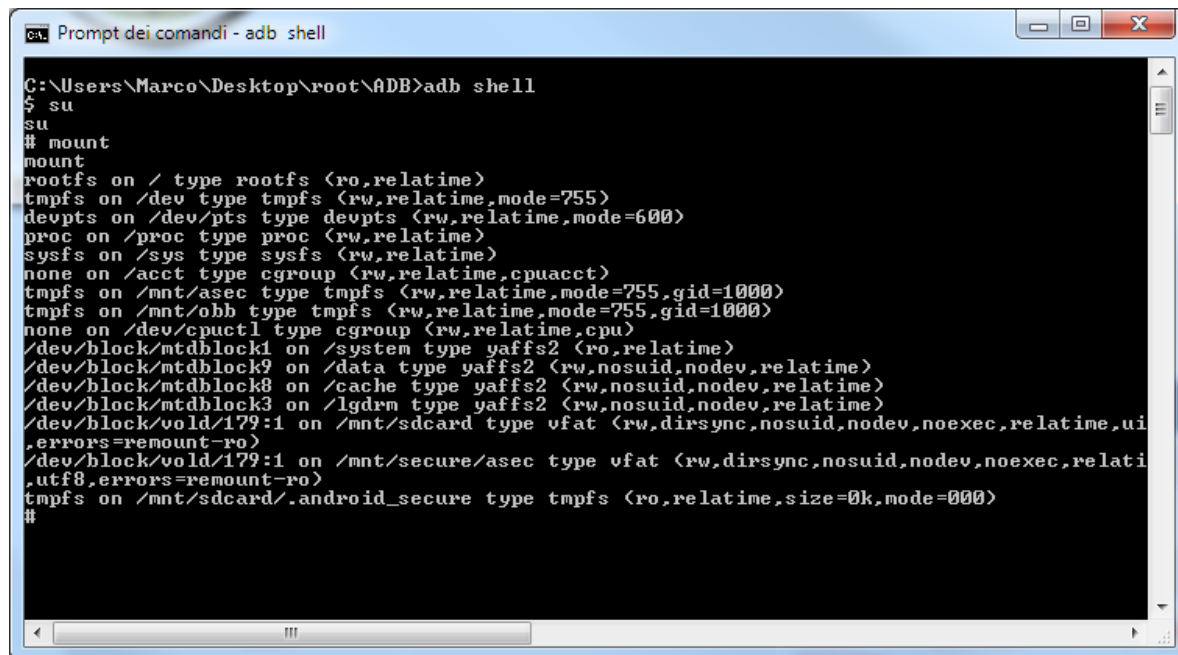
- **EXT(2-3-4)**: generalmente usato per system image (*/system*), user data (*/data*) and cache (*/cache*).
- **FAT32**: generalmente usato per la SD card (*/mnt/sdcard*, */mnt/secure/asec*, */mnt/emmc*).
- **YAFFS2** (Yet Another Flash File System): file system open source veloce e dotato di correzione degli errori per le memorie interne (NAND)

Mount point

Mount Point	File System	Note
/	rootfs	Read-only.
/proc	proc	System state and statistics.
/system	YAFFS2	System image (read-only).
/data or /data/data	YAFFS2/EXT3/EXT4	Apps Data Storage Directory. Setuid not allowed for security reasons.
/app-cache	tmpfs	Temporary cache used by Apps.
/cache	YAFFS2/EXT3/EXT4	Persistent directory used by Apps and System.
/mnt/sdcard /mnt/secure/asec /mnt/emmc	vfat	<i>sdcard</i> and <i>emmc</i> can be shared by USB MASS STORAGE (UMS). Only root can mount <i>asec</i> .

Filesystem in Android

Per visualizzare i file system utilizzati in un dispositivo è necessario accedere alla shell tramite ADB ed eseguire il comando mount



```
Prompt dei comandi - adb shell
C:\Users\Marco\Desktop\root\ADB>adb shell
$ su
su
# mount
mount
rootfs on / type rootfs (ro,relatime)
tmpfs on /dev type tmpfs (rw,relatime,mode=755)
devpts on /dev/pts type devpts (rw,relatime,mode=600)
proc on /proc type proc (rw,relatime)
sysfs on /sys type sysfs (rw,relatime)
none on /acct type cgroup (rw,relatime,cpuacct)
tmpfs on /mnt/asec type tmpfs (rw,relatime,mode=755,gid=1000)
tmpfs on /mnt/obb type tmpfs (rw,relatime,mode=755,gid=1000)
none on /dev/cpuctl type cgroup (rw,relatime,cpu)
/dev/block/mtdblock1 on /system type yaffs2 (ro,relatime)
/dev/block/mtdblock9 on /data type yaffs2 (rw,nosuid,nodev,relatime)
/dev/block/mtdblock8 on /cache type yaffs2 (rw,nosuid,nodev,relatime)
/dev/block/mtdblock3 on /lgdrm type yaffs2 (rw,nosuid,nodev,relatime)
/dev/block/vold/179:1 on /mnt/sdcard type vfat (rw,dirsync,nosuid,nodev,noexec,relatime,ui
.errors=remount-ro)
/dev/block/vold/179:1 on /mnt/secure/asec type vfat (rw,dirsync,nosuid,nodev,noexec,relati
.utf8.errors=remount-ro)
tmpfs on /mnt/sdcard/.android_secure type tmpfs (ro,relatime,size=0k,mode=000)
#
```

Analisi del dispositivo

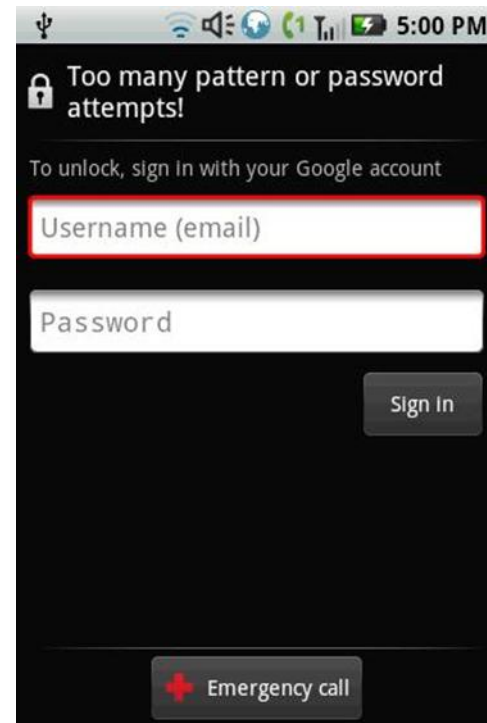
- Quando ci si prepara ad analizzare un dispositivo Android acceso, bisogna ricordarsi che ogni interazione provoca delle modificazioni (art. 360). Tuttavia se il dispositivo implementa qualche tipo di cifratura della memoria NAND, lo spegnimento potrebbe comportare la perdita definitiva della possibilità di analisi.

Analisi del dispositivo

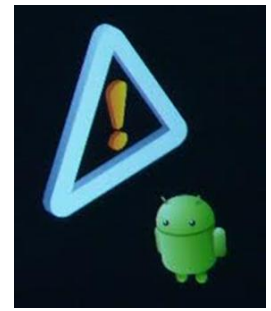
- Prima di procedere, con il dispositivo acceso è necessario eseguire i seguenti passi:
 1. Disabilitare il blocco schermo
 2. Abilitare la «modalità aereo»
 3. Abilitare il «Debug USB» (ADB)
 4. Abilitare la funzionalità di «sempre attivo»

Bypassare il blocco schermo

- Se il telefono è protetto da un pass code, ma siamo a conoscenza delle credenziali Gmail associate, alcuni dispositivi, dopo un certo numero di passcode errati richiedono le credenziali Gmail per eseguire il reset del codice.



Modalità recovery



- A dispositivo spento, può essere utile verificare se il modello in questione prevede una modalità «recovery»*
- In questo caso potrebbe essere possibile, con un po' di fortuna, accedere ai dati in modalità ADB senza avviare il sistema operativo (se il proprietario del telefono aveva preventivamente eseguito il root)

* Bisogna prestare molta attenzione in questa fase, alcuni telefoni, sprovvisti di recovery potrebbero «formattare» il dispositivo

Preparazione della macchina da acquisizione e test ADB

- Sulla macchina da acquisizione e necessario installare il Software Development Kit di Android che include l'Android Debug Bridge (ADB)
- Per verificare se ADB è abilitato sul telefono è possibile usare il comando «adb devices» per avere la lista dei dispositivi connessi

```
C:\Users\litianop>  
C:\Users\litianop>  
C:\Users\litianop>adb devices  
List of devices attached  
015F4A6510011013      device
```

Acquisizione

- Verificata la presenza di ADB, per estrarre i file e le cartelle da un dispositivo Android, come per tutti i dispositivi mobile, si possono seguire due strade:
 - ◆ Acquisizione fisica
 - ◆ Acquisizione logica

Acquisizione fisica

- Una volta ottenuti i permessi di «root» è possibile accedere alla shell tramite ADB ed eseguire il comando «dd» per l'acquisizione fisica della memoria del telefono su scheda SD
- Bisogna identificare il «device» che contiene la partizione dati.
- Nel nostro esempio sembrerebbe:
`/dev/block/mtdblock9` con filesystem **YAFFS2**

Acquisizione fisica

- In realtà il device da acquisire è

`/dev/mtd/mtd9`

- Tramite il comando

```
dd if=/dev/mtd/mtd9 of=/sdcard/data.dd bs=4096
```

Acquisizione fisica

- Se il filesystem è di tipo **EXT**, sarà sufficiente importarlo in qualunque tool forensics per analizzarlo
- Se il filesystem è di tipo **YAFFS(2)** , sarà necessario un tool specifico per l'estrazione dei files (es. **unyaffs per linux**)

Acquisizione logica

- Indipendentemente dal tipo di filesystem (EXT o YAFFS) è **sempre possibile, una volta ottenuti i permessi di root, copiare l'intero contenuto della cartella /data (o delle altre cartelle di interesse) sulla SD esterna tramite il comando linux cp:**

```
#cp /data /sdcard/data
```

- Alternativamente si può eseguire l'acquisizione delle cartelle tramite il comando

```
C:\AndroidSDK\adb pull /data
```

Analisi dei dati

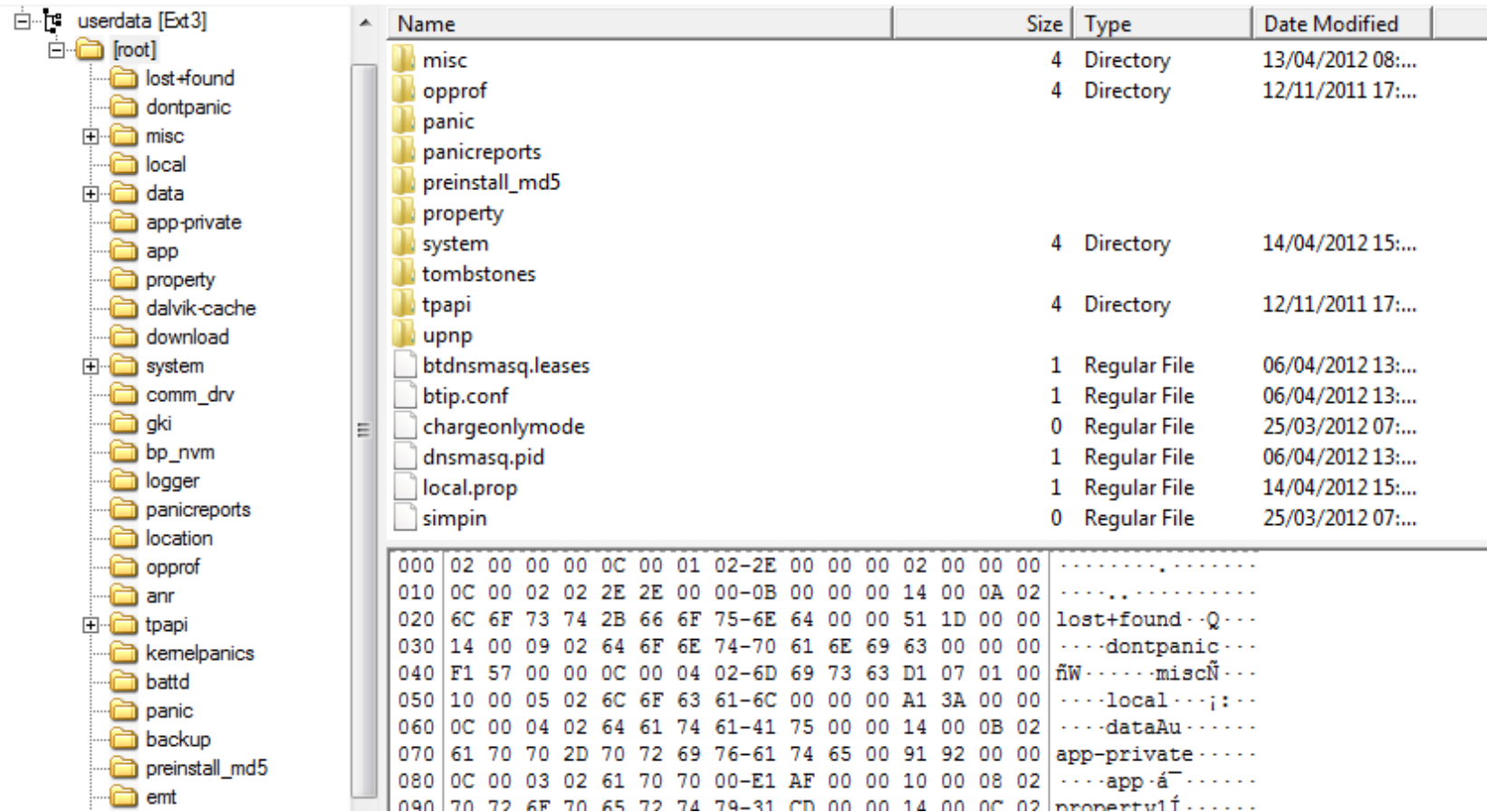
- /system

The screenshot shows a software interface with two main panes. The left pane, titled 'Evidence Tree', displays a hierarchical file system structure. The root of the tree is 'android.sys', which contains a sub-directory 'system [Ext3]'. Inside 'system', there is an '[unallocated space]' folder and a 'root' folder. The 'root' folder is currently selected and highlighted with a blue border. Below 'root', the following folders are listed: 'app', 'lib', 'usr', 'xbin', 'framework', 'media', 'etc', 'preinstall', 'fonts', 'bin', 'tts', and 'lost+found'. Some folders have a '+' icon next to them, indicating they are collapsed. The right pane, titled 'File List', shows a table with a 'Name' column. It lists the same folders as the 'Evidence Tree' pane, plus two files: 'build.prop' and 'default.prop'.

Name
app
bin
etc
fonts
framework
lib
lost+found
media
preinstall
tts
usr
xbin
build.prop
default.prop

Analisi dei dati

■ /data



Name	Size	Type	Date Modified
misc	4	Directory	13/04/2012 08:...
opprof	4	Directory	12/11/2011 17:...
panic			
panicreports			
preinstall_md5			
property			
system	4	Directory	14/04/2012 15:...
tombstones			
tpapi	4	Directory	12/11/2011 17:...
upnp			
btdnsmasq.leases	1	Regular File	06/04/2012 13:...
btip.conf	1	Regular File	06/04/2012 13:...
chargeonlymode	0	Regular File	25/03/2012 07:...
dnsmasq.pid	1	Regular File	06/04/2012 13:...
local.prop	1	Regular File	14/04/2012 15:...
simpin	0	Regular File	25/03/2012 07:...

000 02 00 00 00 0C 00 01 02-2E 00 00 00 02 00 00 00
010 0C 00 02 02 2E 2E 00 00-0B 00 00 00 14 00 0A 02
020 6C 6F 73 74 2B 66 6F 75-6E 64 00 00 51 1D 00 00 lost+found ··Q··
030 14 00 09 02 64 6F 6E 74-70 61 6E 69 63 00 00 00 ····dontpanic··
040 F1 57 00 00 0C 00 04 02-6D 69 73 63 D1 07 01 00 fñW····miscÑ··
050 10 00 05 02 6C 6F 63 61-6C 00 00 00 A1 3A 00 00 ····local···;:·
060 0C 00 04 02 64 61 74 61-41 75 00 00 14 00 0B 02 ····dataAu····
070 61 70 70 2D 70 72 69 76-61 74 65 00 91 92 00 00 app-private····
080 0C 00 03 02 61 70 70 00-E1 AF 00 00 10 00 08 02 ····app-ã····
090 70 72 6F 70 65 72 74 79-31 CD 00 00 14 00 0C 02 propertyüf····

Analisi dei dati

- /cache

The screenshot displays a forensic analysis interface with two main panels:

- Evidence Tree:** Shows a hierarchical view of the 'cache.dd' image. The tree structure is as follows:
 - cache.dd
 - cache [Ext3]
 - [unallocated space]
 - [root]
 - lost+found
 - recovery

- File List:** A table listing the contents of the selected folder. The table has a header 'Name' and lists the following items:

Name
[root]
[unallocated space]
bad blocks
block bitmap
boot record
group descriptor table
inode bitmap
inode table
journal
superblock

Analisi dei dati

- Cartelle e file di interesse

PATH	CONTENT
/data/data/com.*.email/databases/	DB Email.
/data/data/com.google.android.gm/databases/	DB Gmail.
/data/data/com.android.providers.calendar/databases/calendar.db	DB Calendar.
/data/data/com.android.providers.telephony/databases/mmssms.db	DB MMS and SMS.
/data/data/com.android.providers.telephony/databases/telephony.db	DB Call. Log.
/data/data/com.android.providers.settings/databases/settings.db	General Settings.
/data/data/com.google.android.apps/databases/da_destination_history	DB Path History.
/data/data/com.google.android.apps/files/	Google MAPS activity.
/system/etc/backup_target_cvs	Backup preferences.
/data/data/com.google.android.location/files/	LOCATION SERVICE (if enable).

Strutture dati di Android

- Android supporta cinque metodi per salvare i dati nei dispositivi:
 - *Shared preferences: XML format*
 - *Internal storage: data structure saved in “/data” subdirectory*
 - *External storage: data structure saved in SD card*
 - *SQLite: single cross-platform file*
 - *Network: data structure saved on the web*

Mail

The screenshot shows a forensic analysis tool interface. On the left, a tree view under 'Evidence Items' shows a directory structure for 'com.android.email' containing a 'databases' folder with 'EmailProvider.db'. The 'tables' folder within 'EmailProvider.db' is expanded, showing an 'Account' table. On the right, the 'File Content' pane displays the content of the 'Account' table in a table format. The table has columns for 'rowid', '_id', 'displayName', 'emailAddress', 'syncKey', and 'syncLook'. A single row is visible with the following data: rowid 1, _id 1, displayName m.scarito@realitynet.it, emailAddress m.scarito@realitynet.it, syncKey [NULL], and syncLook 2. Below the table, there are tabs for 'File Content', 'Properties', and 'Hex Interpreter'. At the bottom, a 'File List' table shows a list of files, including 'rows_0000000_000000...' with item number 28578 and path 'lg [AD1]/data/com.andr...'. The file is categorized as HTML and has a size of n/a.

Account

rows 0-0

rowid	_id	displayName	emailAddress	syncKey	syncLook
1	1	m.scarito@realitynet.it	m.scarito@realitynet.it	[NULL]	2

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created
rows_0000000_000000...		28578		lg [AD1]/data/com.andr...	HTML	n/a	n/a				n/a

Mail

Evidence Items

- tables
 - Account
 - android_metadata
 - Attachment
 - blobs
 - HostAuth
 - Mailbox
 - Message
 - Message_Deletes
 - Message_Updates
 - sqlite_sequence
- EmailProviderBody.db
 - tables
 - android_metadata
 - Body
 - sqlite_sequence
- Esp.db
- Hiddenesp.db
- Settings.db
- webview.db
- webviewCache.db
- files
- shared_prefs
- com.android.mms
- com.android.phone
- com.android.providers.calendar
- com.android.providers.contacts
- databases
 - contacts2.db

File Content

Hex Text Filtered Natural

Item #	Offset	Size	MD5	SHA1	SHA256	Created	Accessed	Modified
73	73	41027	1334440824000	MDaemon at static-82-85-92-196.clienti.tiscali.it	1334440821000			Mail Statistics Summary - static-82-85-92-196.clienti.tiscali.it - Sat, 14 Apr 2012
74	74	41028	1334440831000	Assistenza commerciale e tecnica MDAemon	1334440831000			È disponibile un aggiornamento per il software MDAemon.
78	78	41031	1334480313000	Booking.com	1334480361000			Ti presentiamo la nostra nuovissima app
79	79	41032	1334503042000	Tati.fr	1334503139000			Bientot la fin des 10 jours TATI !
80	80	41033	1334506650000	Lulu Castagnette	1334506750000			info flash lulu: jusqu a moins 60 pourcent
81	81	41034	1334511856000	Mattia Epifani	1334511953000			Fwd: Fwd: Questionario per gli Esercizi convenzionati con la tessera Green

File Content Properties Hex Interpreter

File List

Normal Display Time Zone: ora legale Europa occidentale (From local machine)

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
rows_0000000_000002...		28565		lg [AD1]/data/com.andr...	HTML	n/a	n/a				n/a		n/a

Gmail

Evidence Items

- android_metadata
- preferences
- mailstore.marcoscarito@gmail.com.db
 - tables
 - android_metadata
 - attachments
 - conversation_labels
 - conversations
 - conversations_to_fetch
 - custom_from_prefs
 - custom_label_color_prefs
 - engine_settings
 - info_overload
 - labels
 - message_labels
 - messages
 - blobs
 - messages_to_fetch
 - operations
 - send_without_sync_conversations_to_f
 - server_preferences
 - sqlite_sequence
 - sync_settings
- webview.db
- webviewCache.db
- shared_prefs
- com.google.android.googlequicksearchbox
- com.google.android.gsf

File Content

Hex Text Filtered Natural

messages

rows 0-21

rowid	_id	messageId	conversation	fromAddress	toAddresses
19	19	1398783076292717839	1398783076292717839	"Marco Scarito" <marcoscarito@gmail.com>	
33	33	1399097865662572951	1399097865662572951	"PremiumPerTe" <premiumperte@mediasetmail.it>	"" <MARCOSCARITO@gmail.com>
34	34	1399111617229035888	1399111617229035888	"Google Calendar" <calendar-notification@google.com>	"Marco Scarito" <marcoscarito@gmail.com>

File Content Properties Hex Interpreter

File List

Normal Display Time Zone: ora legale Europa occidentale (From local machine)

☑	▲	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
☐	📁	blobs		32544		lg [AD1]/data/com.goog...	Placeh...	n/a	n/a				n/a		n/a
☐	📄	rows_0000000_000002...		32543		lg [AD1]/data/com.goog...	HTML	n/a	n/a				n/a		n/a

Contacts

Evidence Items

- com.android.phone
- com.android.providers.calendar
- com.android.providers.contacts
 - databases
 - contacts2.db
 - tables
 - _sync_state
 - _sync_state_metadata
 - accounts
 - activities
 - agg_exceptions
 - android_metadata
 - calls
 - contacts
 - data
 - deleted_records
 - groups
 - mimetypes
 - name_lookup
 - nickname_lookup
 - packages
 - phone_lookup
 - properties
 - raw_contacts
 - settings
 - sqlite_sequence
 - sqlite_stat1
 - status_updates
 - v1_settings

File Content

Hex Text Filtered Natural

calls

rows 0-462

rowid	_id	number	date	duration	type	new	name	numbertype	numberlabel	modified	modified_time
1	1	34610	1328295196864	0	2	0	[NULL]	[NULL]	[NULL]	1	1334253749058
2	2	08119	1328606527801	0	2	0	[NULL]	[NULL]	[NULL]	1	1334253749416
3	3	+3939	1328799338739	0	3	0	Flor	2	[NULL]	1	1334313147610
4	4	+3933	1329043924686	0	2	0	Anit	2	[NULL]	1	1334313148181
5	5	+3934	1328126740273	1	2	0	Anit	-2	[NULL]	1	1334253751080
6	6	33556	1328270231422	0	2	0	[NULL]	[NULL]	[NULL]	1	1334253752509
7	7	33556	1328273546018	76	2	0	[NULL]	[NULL]	[NULL]	1	1334253752825
8	8	+3934	1329412068628	0	2	0	Flor	-2	[NULL]	1	1334253754529
9	9	+3939	1329465657651	0	2	0	Flor	2	[NULL]	1	1334313147610
10	10	+3901	1329485976763	0	3	0	REA	3	[NULL]	1	1334253984521
11	11	+3939	1329509506988	0	3	0	Fab	-2	[NULL]	1	1334253758288
12	12	+3933	1330074541582	0	3	0	Tin	-2	[NULL]	1	1334253759571

PRIVACY

PRIVACY

File List

Normal Display Time Zone: ora legale Europa occidentale (From local machine)

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
rows_0000000_000046...		28284		lg [AD1]/data/com.andr...	HTML	n/a	n/a				n/a		n/a

SMS

Evidence Items

- com.android.phone
- com.android.providers.calendar
- com.android.providers.contacts
- com.android.providers.downloads
- com.android.providers.media
- com.android.providers.settings
- com.android.providers.telephony
- databases
 - mmsms.db
 - tables
 - addr
 - android_metadata
 - attachments
 - canonical_addresses
 - delete_sms
 - drm
 - part
 - pdu
 - pending_msgs
 - rate
 - raw
 - sms
 - sqlite_sequence
 - sr_pending
 - threads
 - words
 - words_content
 - words_segdir
 - words_segments

File Content

Hex Text Filtered Natural

Item #	Text	Filtered	Natural
45	45	15	Google [NULL] 1328194830163 0 1 -1 1 [NULL] [NULL] Promemoria: ECIPA-3 MOD-1 II gio 2 feb Scarito)
46	46	3	+39393 273 1328205370735 0 1 -1 1 [NULL] [NULL] Ciao, La al ferrar casa. B
47	47	16	+39347 [NULL] 1328260206170 0 1 -1 1 [NULL] [NULL] Ti ho ce 03/02/1 Informa servizio
48	48	17	Cinema: [NULL] 1328260325706 0 1 -1 1 [NULL] [NULL] Richiedi gratis al 'Benven tanti alt 4082 o grandec
49	49	15	Google [NULL] 1328288427838 0 1 -1 1 [NULL] [NULL] Promem casa pri 7:50PM
50	50	18	+39010 200 1328517484376 0 1 -1 1 [NULL] [NULL] Ciao Ma ventura - Alice Ma

PRICACY

PRICACY

File List

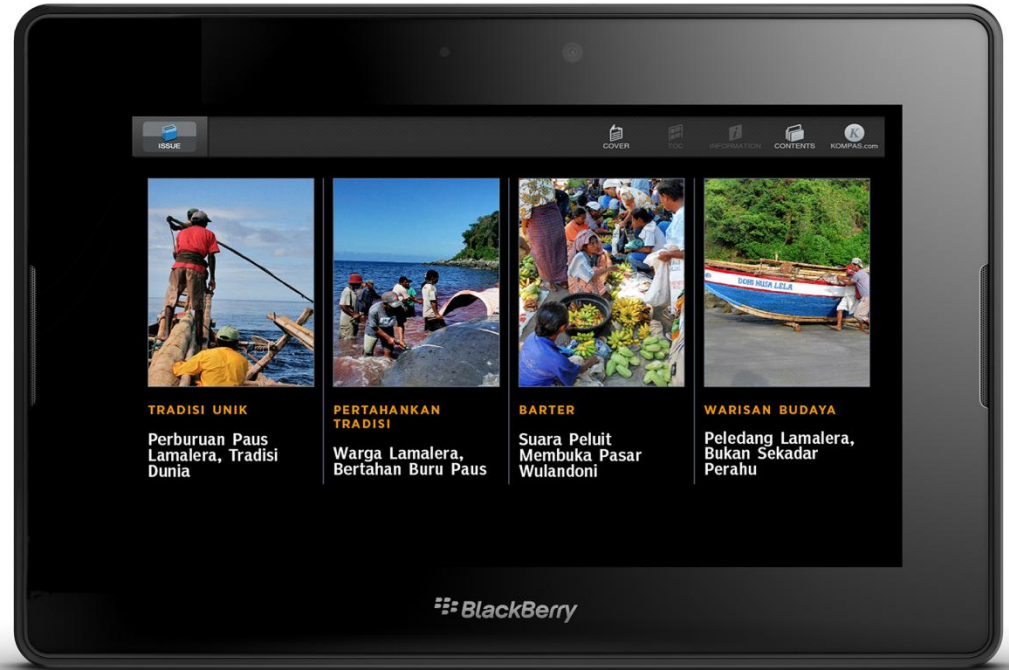
Normal Display Time Zone: ora legale Europa occidentale (From local machine)

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
rows_0000000_000027...		32709		lg [AD1]/data/com.andr...	HTML	n/a	n/a				n/a		n/a

Acquisizione e analisi con prodotti commerciali

- La maggior parte dei prodotti commerciali per mobile forensics supportano Android
 - ◆ Oxygen Forensics
 - ◆ Cellebrite UFED
 - ◆ Compelson MOBILedit!
 - ◆ EnCase Neutrino
 - ◆ Micro Systemation XRY
 - ◆ Paraben Device Seizure
- Tutti i software supportano l'acquisizione logica tramite **content provider**
- Per alcuni modelli è supportata l'acquisizione fisica (previo root del dispositivo)

Blackberry Forensics



Blackberry Forensics



- «Introduzione alla Blackberry Forensics», capitolo 10
- Ing. Simone Tacconi
- Direttore della Sezione «Informatica Forense» del Servizio Polizia Postale e delle Telecomunicazioni, presso il Dipartimento della Pubblica Sicurezza del Ministero dell'Interno

Blackberry Forensics

- Caratteristiche dei dispositivi BlackBerry
- Servizi accessibili
- Meccanismi di protezione dei dati
- Fonti di digital evidence
- Acquisizione logica dei dispositivi
- Analisi dei backup e dei backup cifrati
- Acquisizione fisica dei dispositivi

Blackberry

- Famiglia di *smartphone* commercializzati dalla società canadese RIM (Research in Motion), fondata nel 2007
- Concepiti per essere commercializzati in un contesto aziendale, anche se hanno avuto un buon successo anche nel segmento consumer
- La quota di mercato ha oscillato tra il 10% e il 20% dal 2007 al 2011 (attualmente 11%)

Caratteristiche dei dispositivi

- I dispositivi sono equipaggiati con **Blackberry OS**, un sistema operativo proprietario
- Supportano GSM (quad-band), UMTS e CDMA
- Offrono funzionalità tipiche come rubrica, calendario appuntamenti, player multimediali e fotocamera digitale
- Solitamente equipaggiati con
 - ◆ tastiera full QWERTY e *trackwheel* o *trackball*
 - ◆ touchscreen
- Batteria proprietaria che contiene componenti elettroniche che impediscono l'uso di altre batterie

Famiglie di modelli



Servizi accessibili

- Navigazione su web
- **Posta elettronica**
 - ◆ Gestita in modalità *push*
 - ◆ I messaggi in entrata sono inviati dal server di posta verso il client, senza che quest'ultimo debba eseguire una richiesta
- **SMS/MMS**
- **Messaggistica istantanea proprietaria (PIN-to-PIN)**
 - ◆ Consente di inviare messaggi da uno *smartphone* all'altro, conoscendo il codice identificativo PIN del terminale destinatario
 - ◆ PIN = codice non modificabile di otto caratteri esadecimali che identifica in modo univoco un device

Servizi accessibili

- **BlackBerry Instant Messenger (BBIM)**

- ◆ Opzione di **clear history** per la cancellazione delle chat attive
- ◆ Opzione di **copy history** per salvare su note o memory card
 - Sono salvati il contenuto e il PIN e non i timestamps

- Supportano anche sistemi di IM di terze parti

- ◆ Skype
- ◆ Yahoo Messenger
- ◆ Google Talk
- ◆ Windows Live Messenger
- ◆ AOL Instant Messenger
- ◆ ICQ
- ◆ IBM Lotus Sametime
- ◆ Novell GroupWise Messenger

Acesso ai servizi

- Modalità **Blackberry Internet Service (BIS)**, per privati e piccole realtà aziendali
 - ◆ L'utente accede alla mail con protocolli POP3/IMAP, mediante la rete di un operatore di telefonia mobile
 - ◆ Per abilitare il terminale, generalmente, l'utente si registra su un portale del gestore specificando PIN e IMEI del dispositivo
- Modalità **Blackberry Enterprise Server (BES)**, per aziende medio-grandi
 - ◆ Permette di integrare le funzioni del Blackberry con i servizi aziendali (Es. Microsoft Exchange Server)
 - ◆ E' necessario un middlewere dedicato, detto **server BES**

Meccanismi di protezione

■ Password di accesso al dispositivo

- ◆ Impostata dall'amministratore del sistema BES o dall'utente
- ◆ Lunghezza tra 4 e 40 caratteri
- ◆ Numero massimo di tentativi consentito pari a 10 (default)
- ◆ Superato il limite il dispositivo effettua un wiping della memoria

■ Wiping del dispositivo

- ◆ Utilizza un pattern di riempimento costituito da una sequenza di zeri
- ◆ Può essere attivato mediante policy impostate dall'amministratore del BES
- ◆ **L'amministratore può compiere da remoto il wiping dei dispositivi**

■ Crittografia delle comunicazioni

- ◆ Basata su AES a 256 bit
- ◆ Tutti i flussi di comunicazione tra BES e terminale o tra BIS e sistemi back-end di RIM

Meccanismi di protezione

■ Crittografia dei dati della memoria interna

- ◆ I dati possono essere crittografati. **Non è abilitato di default ma può essere attivato dall'utente o tramite group policies**
- ◆ Sono protetti messaggi, rubrica, dati di navigazione del browser, calendario degli appuntamenti, tasks, memo
- ◆ Protezione trasparente all'utente (On The Fly Encryption)

■ Rimozione della batteria

- ◆ La rimozione della batteria non modifica i dati dell'utente ma può causare un reset delle impostazioni di data e ora
- ◆ Il reinserimento della batteria nel dispositivo comporta un'accensione automatica se la batteria ha carica sufficiente

■ Always on

- ◆ Dispositivo sempre acceso se non si esegue uno shutdown tramite PC

Fonti per digital evidence

- Si possono identificare diverse fonti di informazioni all'interno di un BlackBerry:
 - ◆ **Informazioni mantenute dalla Società RIM**, secondo le policy di data retention;
 - ◆ **Dati conservati nei server BES aziendali**;
 - ◆ **Personal computer utilizzato per il backup e sincronizzazione del dispositivo** (Desktop Blackberry Manager)
 - ◆ **Contenuto della memoria interna**
 - ◆ **Contenuto della memoria estraibile**
 - ◆ **Contenuto della scheda SIM**

Informazioni conservate da RIM

- La società RIM conserva alcune informazioni relative al traffico di alcuni servizi, in particolare:
 - ◆ Messaggistica PIN-to-PIN
 - ◆ Posta elettronica
 - ◆ Navigazione Web
- Le informazioni possono essere acquisite solo a seguito di provvedimento in regime di **rogatoria internazionale**
- In modalità BIS, l'utente accede ai servizi con l'attivazione di un piano tariffario per il traffico dati presso il proprio gestore
- Il gestore assegna un indirizzo IP allo smartphone e RIM conserva l'**associazione tra tale indirizzo e l'identificativo PIN del dispositivo**

Informazioni su messaggi

- Le informazioni relative ai **messaggi PIN-to-PIN** sono conservate per 6 mesi
- Si possono ottenere:
 - ◆ Identificativi PIN dei terminali con cui sono avvenuti scambi di contatti
 - ◆ Data e orario di comunicazioni
- Le informazioni relative alla **posta elettronica** sono conservati per un periodo tra 14 e 30 giorni
 - ◆ Se l'utente elimina i messaggi dal telefono, questi sono rimossi anche dai server di posta RIM
 - ◆ La posta può essere richiesta specificando numero di telefono, PIN, indirizzo di posta, codice IMEI, codice ICCID della SIM

Informazioni sulla navigazione

- Conservazione **completa delle URL** degli ultimi 7 giorni
- Conservazione delle **landing page** per 30 giorni
- Se si visita una pagina web e poi si seguono i link di questa a pagine più profonde del sito
 - ◆ Sottopagine per 7 giorni
 - ◆ Pagina di partenza 30 giorni

Attività sul server BES

- E' opportuno avvalersi dell'amministratore del server BES che possiede competenze e privilegi per operare
- Se il server non può essere spento bisogna effettuare operazioni di live forensics
 - ◆ Acquisire informazioni volatili
 - ◆ Ottenere rapidamente informazioni
 - ◆ Disabilitare meccanismi di protezione e/o wiping
- Accessibili con l'account **BESAdmin** mediante il software **Blackberry Manager**
- Informazioni presenti:
 - ◆ Modello, codice IMEI e numero telefonico associato
 - ◆ Nome account utente e data di creazione
 - ◆ Indirizzi di posta abbinati e data e ora ultima sincronizzazione

Informazioni sulle comunicazioni

- I dati conservati non riguardano i contenuti
- Sono conservati:
 - ◆ Mittenti/chiamanti
 - ◆ Destinatari/riceventi
 - ◆ Date e ore
- I messaggi di posta elettronica sono conservati sul server di posta (es. Exchange) associato al BES

File di log su server BES

- Conservati secondo le policy di logging definite dall'azienda
 - File in formato testuale collocato nella cartella
`\Program Files\Research in Motion\BlackBerry Enterprise Server\Logs\`
all'interno di sottocartelle create giornalmente (nomenclatura
YYYYMMDD)
 - Log di maggiore interesse quelli relativi alle comunicazioni tra
utenti
 - ◆ PhoneCallLog
 - ◆ PINLog
 - ◆ SMSLog
- Nomenclatura: **Log-Type_YYYYMMDD.csv**

Blackberry Desktop Manager

- **Blackberry Desktop Manager** gestisce le connessioni tra lo smartphone e il PC dell'utente, giunto alla **versione 6.1**
- La connessione può avvenire **mediante cavo USB o connessione bluetooth**
- Utilizzato prevalentemente per:
 - ◆ Sincronizzare email, contatti, calendario, memo, tasks, ecc.
 - ◆ Creare un backup o ripristinare un backup precedente
 - ◆ Trasferire file tra il computer e il BlackBerry
 - ◆ Caricare nuove applicazioni
- Nella cartella
`\Documents and Settings\\Application Data\Research In Motion\BlackBerry\Loader History`
è conservato un file **PIN_terminale.xml** per ogni smartphone collegato, contenente informazioni sul dispositivo

Acquisizione logica dei dati

- Il telefono potrebbe essere stato impostato per consentire l'accesso solo a seguito di autenticazione mediante password
- **Non esistono metodi noti per aggirare questa protezione**, che impedisce quindi l'acquisizione della memoria del dispositivo
- Se è abilitata la cifratura anche sulla scheda di memoria, si può utilizzare **Elcomsoft Phone Password Breaker** (<http://www.elcomsoft.com/eppb.html>) per attacchi
- Se il telefono è amministrato attraverso un server BES accessibili è possibile compiere **un reset da remoto della password** mediante l'utente BES Admin
- Il fattore “tempo” è fondamentale: **di default i messaggi sono cancellati dopo 30 giorni** (può essere cambiata della opzioni)

Backup con Blackberry Desktop Manager

- La funzionalità di backup del software **Blackberry Desktop Manager** può essere utilizzata per un'acquisizione logica
- Il software non è stato concepito per scopi forensi, ma il backup prodotto è analogo a quello generato da altri strumenti commerciali di mobile forensics
- Il file prodotto ha estensione **IPD** e può essere aperto utilizzando:
 - ◆ Un visualizzatore separato
 - ◆ Un simulatore di terminale
- Per default il software utilizza la nomenclatura **Backup-(YYYY-MM-DD).ipd** e viene salvato nella cartella “Documenti” dell'utente

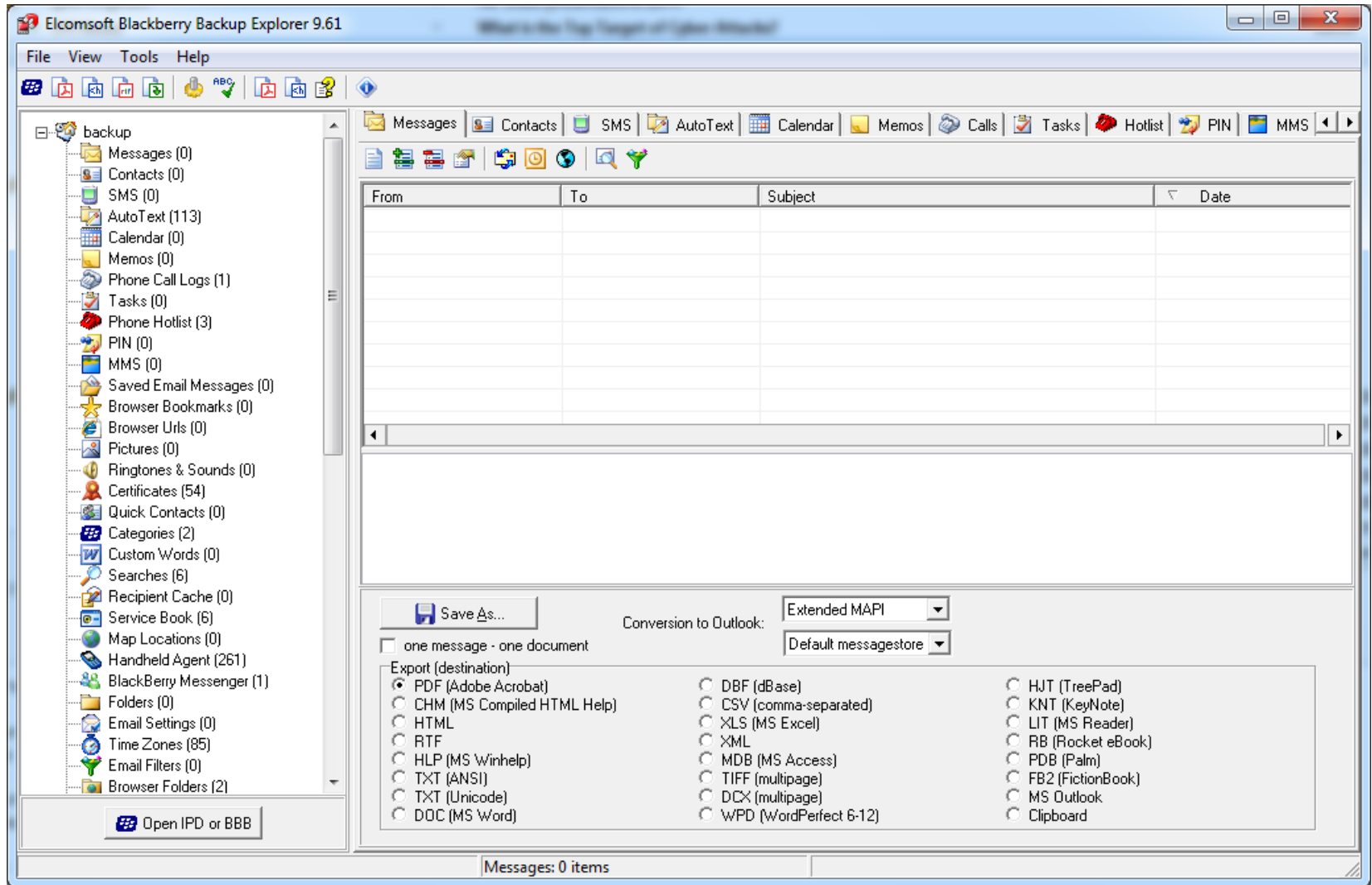
BlackBerry Desktop Manager



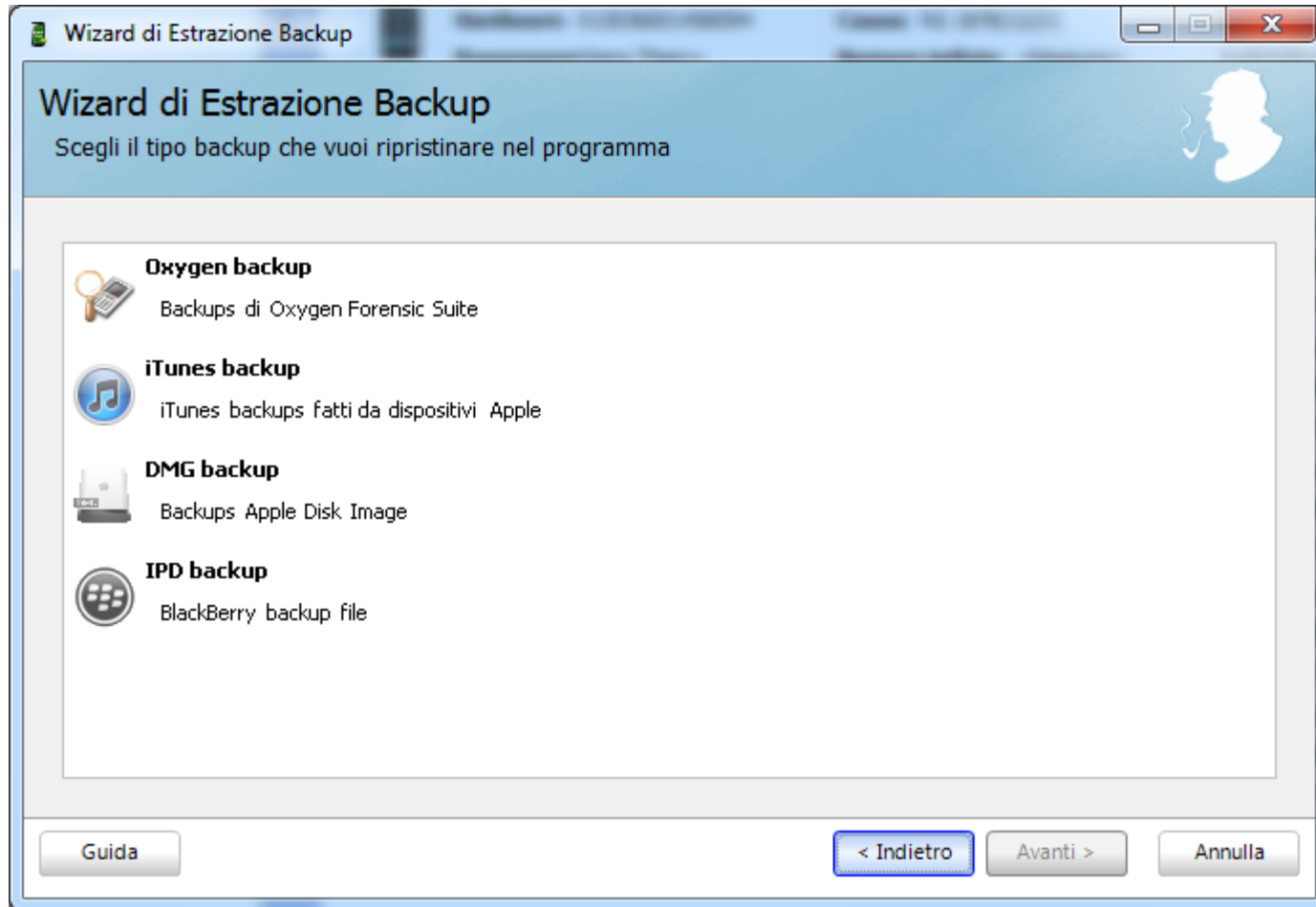
Visualizzatori di file IPD

- Esistono diversi software per la visualizzazione dei file di backup:
 - ◆ **Elcomsoft Blackberry Backup Explorer**, commerciale
 - ◆ **Oxygen Forensics Suite**, commerciale
 - ◆ **Paraben Device Seizure**, commerciale
 - ◆ **MagicBerry IPD Software**, freeware
 - ◆ **CCL Forensics Rubus**, freeware

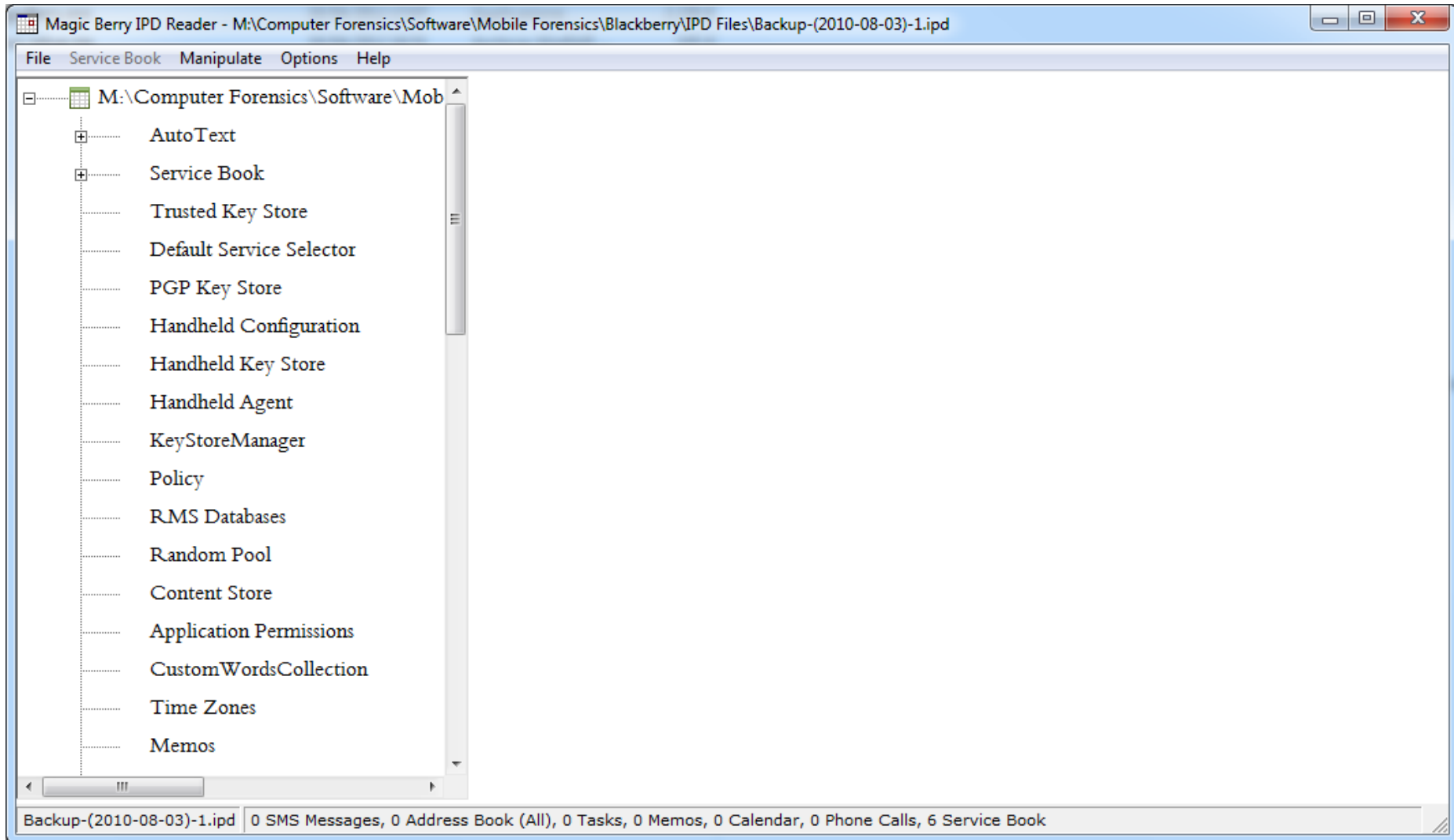
Blackberry Backup Explorer



Oxygen Forensic Suite



MagicBerry



Rubus

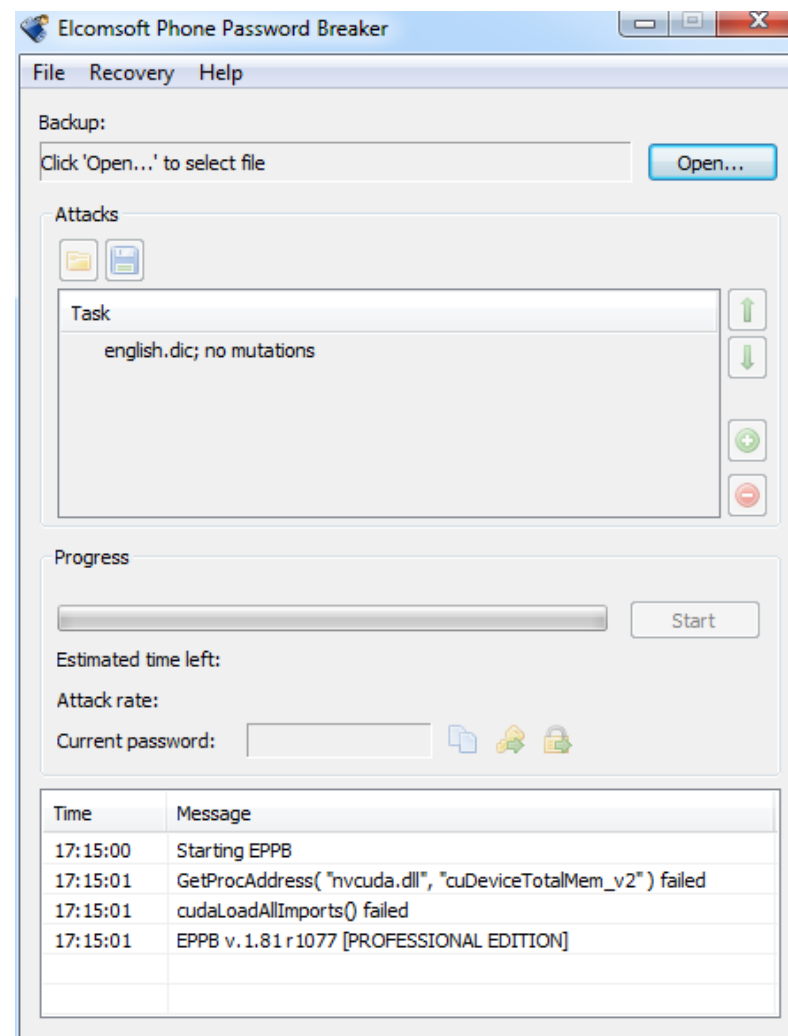
The screenshot shows the Rubus application window. The left pane displays a file tree under the root 'backup.ipd'. The right pane shows a hex view of the selected file. The hex view contains the following data:

Hex Address	Hex Data	ASCII Data
00000000	81 D6 E2 B7 60 00 0E 53 65 67 6E 61 6C 69 62 72	.Öâ`..Segnalibr
00000010	69 20 57 41 50	i WAP

At the bottom of the window, the status bar displays: Start: 0 End: 0 Length: 0

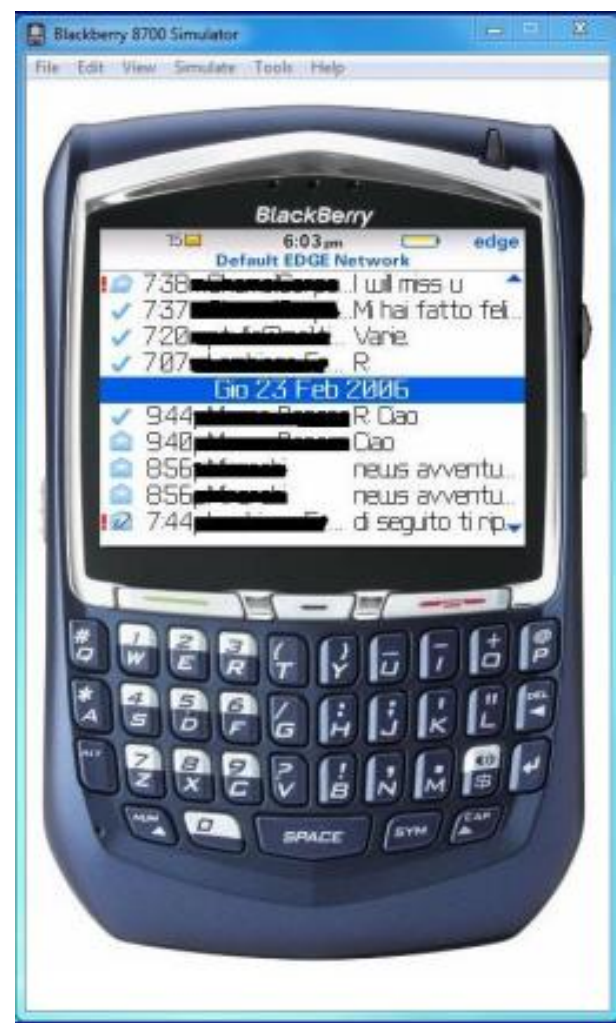
Backup protetti da password

- Se sul computer viene rinvenuto un backup protetto con password è possibile fare un attacco utilizzando Elcomsoft Phone Password Breaker
- Supporta
 - ◆ Attacco a dizionario
 - ◆ Attacco bruteforce



Utilizzo di simulatori

- I file di backup si possono visualizzare anche utilizzando simulatori
- Consentono di simulare l'uso del terminale e visualizzarne i contenuti originali, ottenendo una sorta di “virtualizzazione” del dispositivo reale



Informazioni estratte

 Messages	 Recipient Cache
 Contacts	 Service Book
 SMS	 Map Locations
 AutoText	 Handheld Agent
 Calendar	 BlackBerry Messenger
 Memos	 Folders
 Phone Call Logs	 Email Settings
 Tasks	 Time Zones
 Phone Hotlist	 Email Filters
 PIN	 Browser Folders
 MMS	 Browser Data Cache
 Saved Email Messages	 RMS Databases
 Browser Bookmarks	 Options
 Browser Urls	 Attachments
 Pictures	 WAP Push Messages
 Ringtones & Sounds	 Contact Groups
 Certificates	 Password Keeper
 Quick Contacts	 Recent Contacts
 Categories	 BlackBerry Wallet
 Custom Words	
 Searches	
 Recipient Cache	

Software forensi per l'acquisizione logica

- Diversi software forensi supportano l'acquisizione logica dei dati presenti su dispositivi Blackberry
- I principali
 - ◆ Oxygen Forensic Suite
 - ◆ Paraben Device Seizure
 - ◆ Access Data Mobile Phone Examiner
 - ◆ MobilEdit! Forensic

BlackBerry Instant Messenger

- Le informazioni relative alla chat BlackBerry **non sono salvate all'interno dei backup**
- La rimozione della batteria non comporta la cancellazione delle chat e dei contatti
- Possono essere salvate unicamente **mediante un'ispezione manuale del telefono** (es. Fernico ZRT)
- Necessario visualizzare separatamente i contatti e le chat



BlackBerry Instant Messenger

- **Messaggio con icona blu** = conversazione letta
- **Messaggio con icona gialla** = conversazione non ancora letta
- **Messaggio con X rossa** = messaggio non recapitato al destinatario
- **Mesaggio con lettera D** = messaggio consegnato (delivered) al destinatario
- **Messaggio con lettera R** = messaggio letto dal destinatario (read)
- **Messaggio con icona a orologio** = messaggio ricevuto dal desitnatario ma non ancora aperto

Acquisizione fisica

- Recentemente Cellebrite UFED ha rilasciato una versione del firmware che supporta l'acquisizione fisica di diversi modelli di BlackBerry
- Funziona unicamente su **dispositivi non bloccati con password e dove non sia attiva la cifratura**

BlackBerry Breakthrough for Cellebrite's UFED System

We are proud to be the first to release physical extraction and decoding for dozens of BlackBerry devices via the [UFED Ultimate](#).

The physical extraction for unlocked devices only is performed using Cellebrite's proprietary boot loaders, in a forensically sound manner.

This release enables decoding for BlackBerry NAND devices running OS 4, 5, 6 and 7 physical extraction.

- Device info
- Address book
- SMS
- Call logs
- MMS (including attachments)
- Email (excluding attachments)
- Installed applications
- Paired Bluetooth devices
- BlackBerry Messenger (BBM) contacts and chat
- Deleted data and much more

Phone History Database

- Phone History Database: database utilizzato per velocizzare l'inserimento di un numero di telefono (una sorta di "dizionario" dei numeri più utilizzati)
- Non viene cancellato quando si rimuove l'elenco delle chiamate

<http://www.swiftforensics.com/2012/01/blackberry-ipd-research-phone-history.html>

- Non viene cancellato quando si rimuove l'elenco delle chiamate

BBThumbs.dat

- “The purpose of a thumbnail cache in any system, is generally to speed up the browsing of large numbers of graphic or video files”
- “When conducting a digital forensics analysis of a computer, looking for these thumbnail caches often provide clues as to what files may have existed before they were deleted off the file system”

<https://github.com/sheran/bbt>

<http://chirashi.zenconsult.net/puttering-around-with-blackberry-forensics-part-1/>

<http://www.digiconf.net/index.php?download=roma2011.pdf>

Symbian Forensics



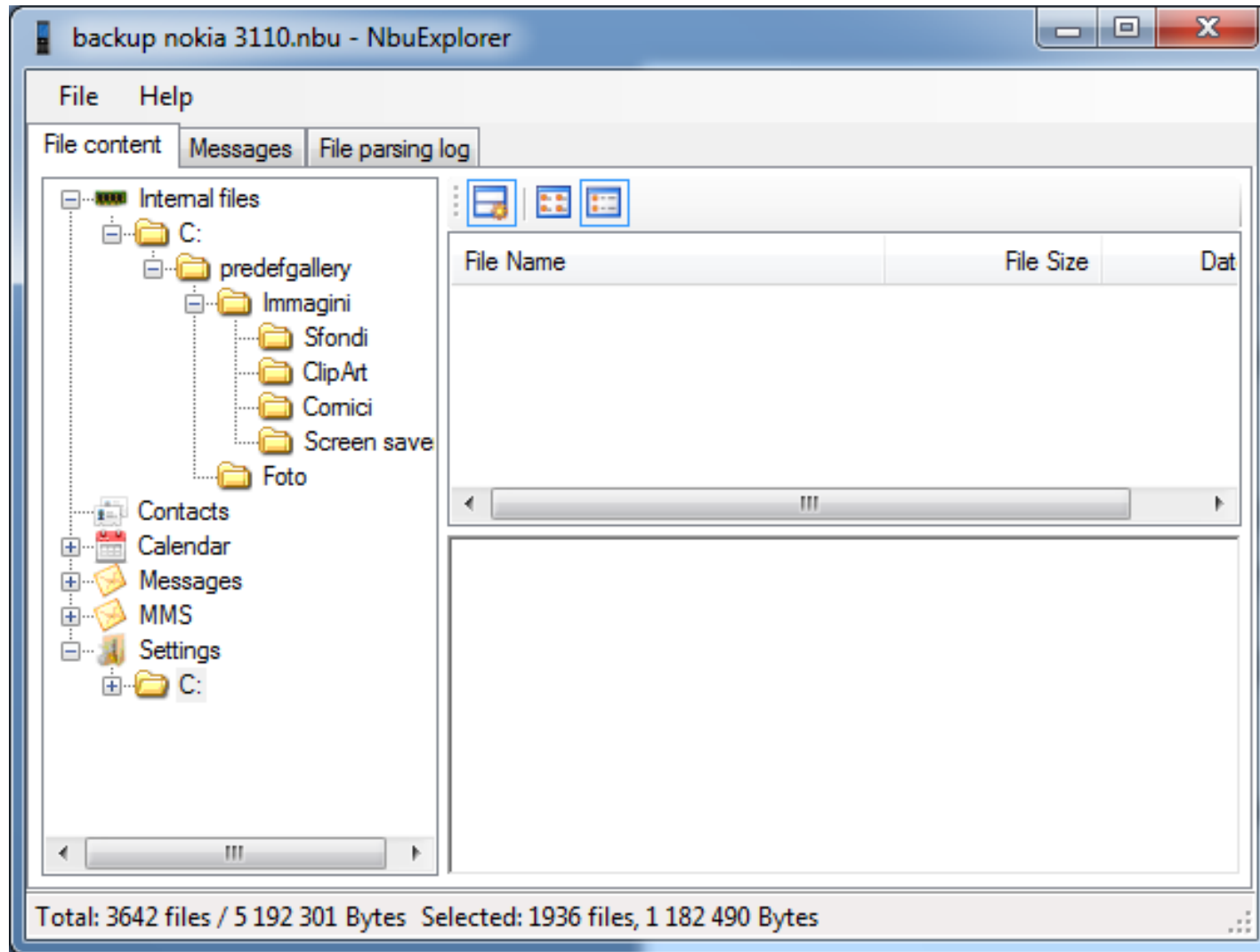
Acquisizione logica

- L'acquisizione logica di smartphone con sistema operativo Symbian può essere effettuata:
 - ◆ Realizzando un backup utilizzando il software Nokia Suite
 - ◆ Utilizzando un software di acquisizione forense
- L'acquisizione mediante software di backup può essere effettuata collegando lo smartphone a un PC e attivando l'opzione "Nokia PC Suite" sullo schermo del dispositivo

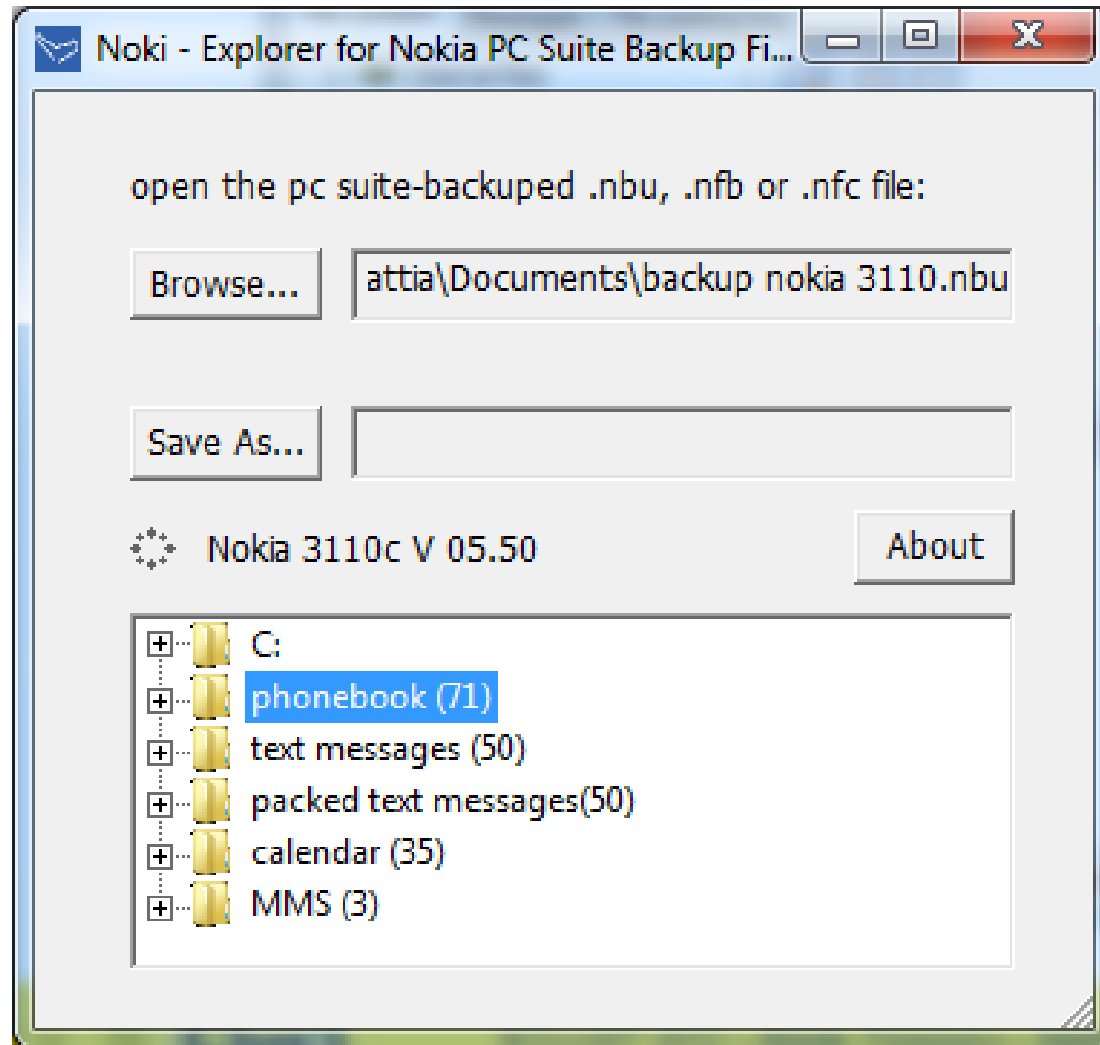
Analisi dei backup

- Il file prodotto dal software Nokia Suite è in formato NBU
- Per visualizzarne il contenuto è necessario utilizzare software di terze parti
- I principali software per l'apertura di file in formato NBU sono:
 - ◆ NBU Explorer, freeware
 - ◆ Noki, commerciale

NBU Explorer



Noki



Acquisizione logica Oxygen Forensics Suite

- Si deve installare una applicazione (OxyAgent) nel dispositivo per estrarre i dati
- L'applicazione non modifica i dati contenuti nello smartphone

http://www.oxygen-forensic.com/download/articles/Oxygen_Agent_Application_Approach.pdf

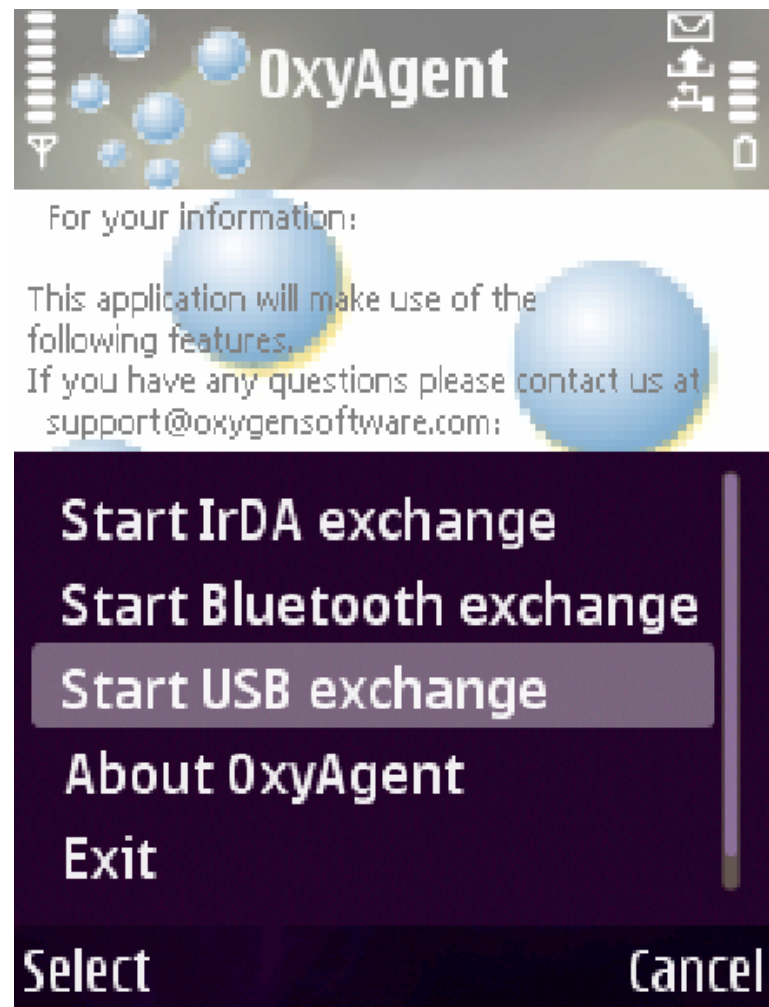
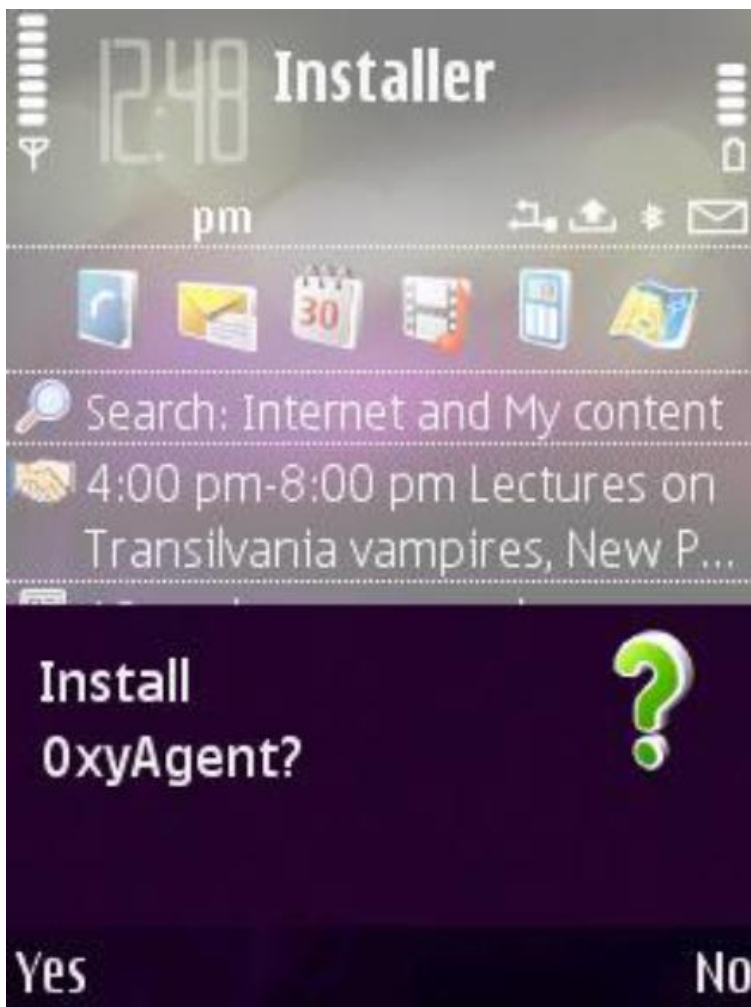
- Il dettaglio delle operazioni da eseguire per l'installazione e l'estrazione dei dati è riportato sul sito del produttore

http://www.oxygen-forensic.com/download/articles/Oxygen_Forensic_Suite-How_to_connect_SymbianOS_devices.pdf

Acquisizione logica Oxygen Forensics Suite



Acquisizione logica Oxygen Forensics Suite





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>