



# Personal Digital Evidence

*Una introduzione alla  
Mobile forensics*

Corso di Informatica Forense - OIG  
Facoltà di Giurisprudenza  
Università degli studi di Bologna

**Dr. Stefano Fratepietro**

**m@il: stefano.fratepietro@unibo.it**

**skype: stefano.fratepietro**



CIRSFID



stevelab.net

## Contenuti

- **Dispositivi**
- Cell Forensics
- SmartPhones Forensics
- PDA Forensics
- Ibrid mobile Forensics
- Sim/Usim Forensics

## Definizioni



- Per "Personal Digital Device" si intende un componente hardware provvisto di un sistema operativo atto a svolgere operazioni su dati per fornire servizi.
- Sono ormai praticamente ovunque:
  - Cellulari
  - Palmari
  - Lettori mp3
  - IPod
  - Navigatori satellitari

## Dispositivi per la comunicazione I



- GSM (Global System for Mobile Communications): tecnologia applicata a dispositivi portatili atti alla sola comunicazione vocale e alla trasmissione di messaggi in formato testuale
  - uso di sim card
- GPRS (General Packet Radio Services): è stato introdotto per la trasmissione di contenuti multimediali tra due dispositivi gprs
  - aumento dell'ampiezza di banda
  - prime connettività Internet
- EDGE (Enhanced Data rates for Global Evolution): evoluzione del GPRS, l'ampiezza di banda può raggiungere il limite massimo di 236 kbps

## Dispositivi per la comunicazione II



- UMTS (Universal Mobile Telecommunications System): tecnologia applicata a dispositivi portatili atti alla comunicazione multimediale ad alta velocità
  - introduzione della video chiamata
  - non usa le normali Sim ma le Usim
  - velocità di trasmissione dati massima di 1920 kbit/s
- HSDPA (High Speed Downlink Packet Access): evoluzione dell' UMTS, permette una velocità di trasmissione di 14.4 Mbit/s

## Architetture I



- Non esiste uno standard
- Più produttori di chip per dispositivi mobile
- Come i sistemi informatici, anche i cellulari hanno diversi tipi di architetture a seconda della casa produttrice.
- A seconda dell'architettura utilizzata vi sono vari sistemi operativi residenti nella memoria rom del dispositivo

## Architetture II



- La struttura di un cellulare è completamente diversa da quella di uno SmartPhone o di un PDA
- Allo stesso modo saranno diversi (se esistenti) i metodi di analisi forense.

## Architetture – Mobile OS



- Rim Black Barry
- Linux
- Palm
- Windows mobile
- Windows Pocket Pc
- Symbian
- Altri...



## Contenuti

- Dispositivi
- **Cell Forensics**
- SmartPhones Forensics
- PDA Forensics
- Ibrid mobile Forensics
- Sim/Usim Forensics



## Cell Forensics I

- Non sempre è possibile eseguire una acquisizione di un cellulare
- Spesso è possibile fare solo acquisizioni logiche e non fisiche
- I software a disposizione sono a codice chiuso e con licenze commerciali
- Un buon 20% dei cellulari sono attualmente inaccessibili, spesso sono dispositivi di marche sconosciute e o progetti che non hanno avuto molto successo nel grande mercato



## Cell Forensics II

### Motivo?

- Le architetture diventano subito obsolete con la conseguenza di essere subito sostituite con progetti completamente nuovi
- Non vi è una adeguata documentazione per lo sviluppo di software (forense)
- Non vi è un mercato (forense)



## Cell Forensics III

- Nokia
- Motorola
- Samsung
- Sony Ericsson
- Philips **(ha annunciato di cessare la produzione)**
- Siemens
- Nec
- Alcatel
- Apple **(???)**

## Cell Forensics IV



- Attualmente non esiste un software avente la possibilità di eseguire acquisizione ed analisi di tutti i dispositivi di tutte le marche
- Esistono soluzioni "ad hoc" o collezioni di soluzioni "ad hoc" per un determinato mercato di dispositivi
- Attualmente il Paraben Device Seizure è il software con il maggior supporto.

## Procedure



- Garantire una alimentazione continuativa del dispositivo
- Isolamento totale da onde radio
- Garantire l'inalterabilità dei dati della sim/usim e del dispositivo con procedure "possibilmente" non invasive
- Documentare con fotografie o filmati le operazioni svolte

## Dispositivi di isolamento



paraben's  
**stronghold  
box**



## In caso di supporto assente I



- E se non esiste un software per l'acquisizione e o l'analisi del reperto?

**Screenshot fotografici dello schermo  
ad alta definizione!**

## In caso di supporto assente II



## Dati rilevanti



- IMEI del dispositivo
- Versione del software/sistema operativo
- Informazioni contenute nella sim/usim
- Chiamate in entrata ed uscita
- Rubrica telefonica
- SMS/MMS
- File multimediali
- Appunti
- Applicazioni installate
- Log della applicazioni installate
- Documenti salvati
- Cache del browser
- Altro... (a seconda dell'esigenza)

## Contenuti



- Dispositivi
- Cell Forensics
- **SmartPhones Forensics**
- PDA Forensics
- Ibrid mobile Forensics
- Sim/Usim Forensics

## SmartPhone Forensics I



- Dispositivo portatile che abbia funzionalità di gestione di dati e di telefono con possibilità di installare software
- Uno SmartPhone, generalmente, si differenzia da un PDA per la potenza di calcolo ridotta (non più per la memoria e il touch screen)



## SmartPhone Forensics II

- Generalmente uno SmartPhone ha due memorie:
  - una interna, non removibile
  - una esterna, fisicamente removibile
- Da circa 2 anni gli SmartPhone hanno la possibilità di espandere la memoria con delle memorie esterne di piccole dimensioni ma capaci di immagazzinare dati oltre i 4GB
  - SD memory
  - MMC
  - Memory Stick

**Tutte con File System FAT32**



## SmartPhone Forensics III

- Symbian OS, erede del EPOC OS, è il sistema operativo più utilizzato dagli SmartPhone attualmente in commercio
  - Progettato per funzionare solo sui dispositivi mobile
  - Facilità uso
  - Ottima gestione risparmio energetico
  - Vasta gamma di software



## SmartPhone Forensics IV

- I maggiori utilizzatori di Symbian OS sono:
  - Nokia
  - Sony Ericson
  - Samsung
  - Siemens
- Symbian Ltd, società controllata dalle principali case produttrici di cellulari, sviluppa una versione base di Symbian OS, versione che verrà personalizzata a seconda della casa madre produttrice finale



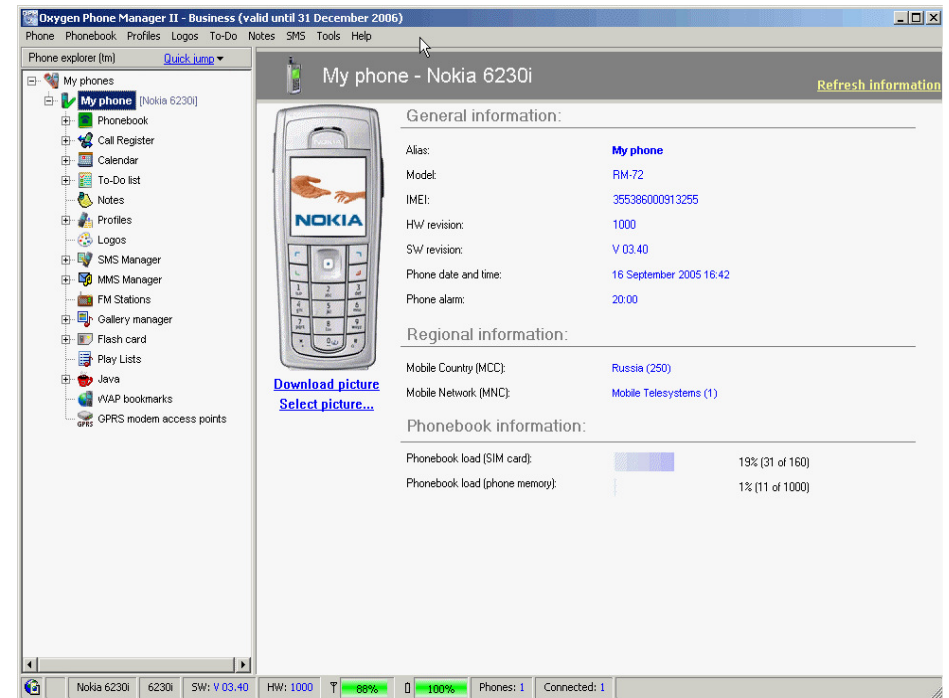
## Dispositivi di comunicazione

- L'iterazione a "basso livello" tra computer e SmartPhone cambia a seconda del modello, essa può avvenire tramite:
  - Cavo USB (non esiste standard)
  - Bluetooth
  - Irda
- Necessità di un driver per l'interfacciamento "computer -> cavo -> dispositivo"

## Iterazione PC – Symbian OS I



- L'unico modo per effettuare un' acquisizione, ed una eventuale analisi, di un reperto avente Symbian è tramite il software Oxygen
- Oxygen è un'applicazione client/server che permette mediante un agent acquisizioni logiche e analisi forensi



## Iterazione PC – Symbian OS II



- Il software agent di Oxygen è:
  - invasivo
  - altera il reperto
  - è l'unica soluzione offerta dal mercato
- Va utilizzato solo in caso di accertamenti tecnici non ripetibili

## Contenuti



- Dispositivi
- Cell Forensics
- SmartPhones Forensics
- PDA Forensics
- Ibrid mobile Forensics
- Sim/Usim Forensics



## PDA Forensics I

- Acronimo di personal digital assistant, un PDA è un computer "palmare" di ridotte dimensioni, tale da essere portato sul palmo di una mano, dotato di uno schermo touch screen e dispositivi di comunicazione
  - Vero e proprio mini computer
  - Sistema operativo con funzioni avanzate
  - Buona potenza di calcolo



## PDA Forensics II

- Generalmente un PDA ha due memorie:
  - una interna, non removibile
  - una esterna, fisicamente removibile
- Da circa 2 anni i PDA hanno la possibilità di espandere la memoria con delle memorie esterne capaci di immagazzinare dati oltre i 4GB
  - SD memory
  - MMC
  - Memory Stick

**Tutte con File System FAT32**



## PDA Forensics III

- Rim Black Barry 30%
- Linux 2 %
- Palm 8%
- Windows mobile 60%



## PDA Forensics IV

- Rim Black Barry, Linux, Palm, Windows mobile sono supportati dal Paraben Device Seizure che permette una facile gestione dei dati contenuti nel reperto
- Metodo non invasivo (no agent)
- A seconda del modello del dispositivo, sono possibili acquisizione sia logiche che fisiche



## Contenuti

---

- Dispositivi
- Cell Forensics
- SmartPhones Forensics
- PDA Forensics
- **Ibrid mobile Forensics**
- Sim/Usim Forensics



## Ibrid mobile forensics I

---

- Per Ibrid mobile forensics si intende un qualsiasi dispositivo mobile atto a compiere operazioni su dati
  - IPOD
  - PSP
  - Nintendo DS
  - Lettori mp3



## Ibrid mobile forensics II

---

- IPOD: acquisizione ed analisi come un normale disco esterno
- PSP: acquisizione ed analisi della Memory Stick removibile
- Nintendo DS: acquisizione ed analisi della memoria removibile
- Lettori mp3: acquisizione ed analisi come un normale disco esterno

**Tutte con File System FAT32**



## Contenuti

---

- Dispositivi
- Cell Forensics
- SmartPhones Forensics
- PDA Forensics
- Ibrid mobile Forensics
- **Sim/Usim Forensics**

## Sim I



- Il Subscriber Identity Module (Modulo d'identità del sottoscrittore, o SIM) è una piccola carta programmabile contenente la chiave di identificazione dell'abbonato al servizio cellulare
- contiene i codici di identificazione di un abbonato al servizio mobile digitale,
- La carta SIM rappresenta la chiave di protezione sulle reti GSM
- E' di proprietà del gestore telefonico

## Sim II



- Contiene il proprio numero telefonico e in alcuni casi anche la rubrica e gli SMS in essa archiviati
- Lo stesso operatore telefonico può diffondere diversi tipi di SIM che si differenziano a seconda della memoria che contengono (8k, 16K, 32K, 64K, 128K, 256k ecc...)
- PIN (Personal Identification Number) codice da digitare ogni volta che si accende al dispositivo per abilitare l'uso della Sim
- PIN Unblocking Key (puk) è un codice di otto cifre che permette di sbloccare la SIM card nel caso si sia inserito per tre volte consecutive il codice PIN errato

## USIM



- L'Universal Subscriber Identity Module (USIM) è un particolare tipo di Smart Card, con le stesse caratteristiche di una SIM, utilizzabile in telefonini, modem e altri apparecchi che ne consentono l'utilizzo
- creata appositamente per i cellulari di terza generazione
- ampia capacità di memoria
- una più rapida presentazione CPU
- maggiore capacità di codificazione/criptazione

## Acquisizione ed analisi di Sim/Usim



- Lettore Sim
- Lettore Usim
- Paraben Device Seizure (solo Sim)

