A cura di:

Francesco Carotenuto
Angelo D'Amato
Antonio Eletto

Professore:

Alfredo De Santis

Mobile Forensic

Linee guida

Introduzione

- Il **Mobile Forensic** è la scienza che si occupa di recuperare prove digitali da un dispositivo mobile usando dei metodi che non compromettano il loro stato probatorio.
- In questo lavoro affrontiamo :
  - una discussione sulle problematiche inerenti alle attività di analisi forense su dispositivi mobile
  - le procedure per la preservazione, acquisizione, investigazione, analisi e reporting delle informazioni digitali, che avranno valore probatorio in una inchiesta giudiziaria.

Motivazioni

- Gli apparecchi mobili sono spesso coinvolti in attività criminali legate
  - Crimine tradizionale
    (es. acquisto di droga, rapine, molestie ecc..)
  - Crimine elettronico
    (es. il furto di informazioni sensibili ecc...)

OUTLINE

- Background
- Procedure e principi
- Processo di analisi forense
  - Preservazione
  - Acquisizione
  - Ispezione ed Analisi
  - Reporting
- Tool
- Caso di studio

Telefonia cellulare

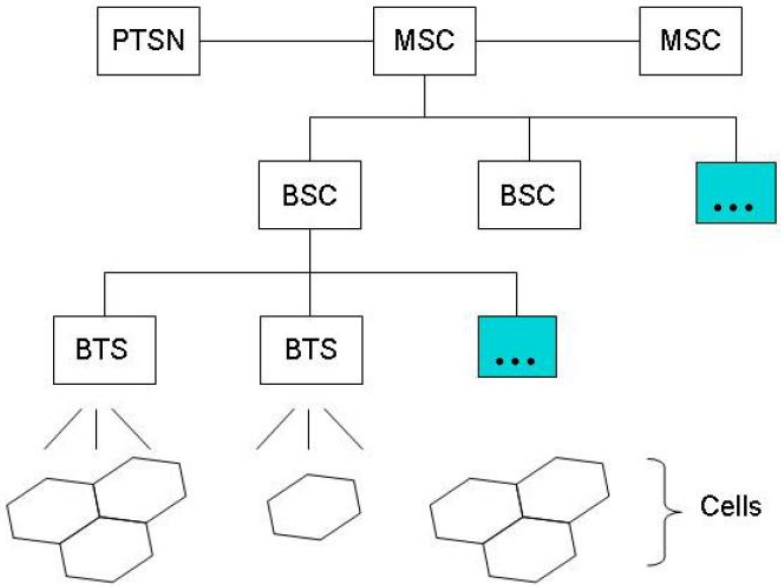
- E’ una tipologia di accesso ad una rete telefonica realizzata per mezzo di onde radio e ricetrasmettitori terrestri.
  - Ogni connessione, o conversazione, richiede la sua specifica frequenza dedicata.
  - Due celle possono utilizzare la stessa frequenza per conversazioni diverse, a patto che le celle non siano adiacenti.

Telefonia cellulare

- Il controller **BSC (*Base Station Controller*)** effettua l'assegnazione del canale e gestisce un sistema di switching per la rete cellulare gestendo la comunicazione tra interfaccia radio e rete fissa.

- Lo switch **MSC (Mobile Switching Center)** è l'elemento che interfaccia il controller BSC, con la rete telefonica fissa **PSTN (*Public Switched Telephone Network*)**

- La **Stazione Radio Base** o **BTS (*Base Transceiver Station*)** si occupa della comunicazione con i dispositivi mobili.



Standard principali

- **2G** (Standard di seconda generazione)
  - **GSM (Global System for Mobile comunication)** per quanto riguarda la seconda generazione basato sulle tecniche di accesso al canale di tipo *TDMA* (Time Division Multiple Access) e *FDMA* (Frequency Division Multiple Access)

  - **2.5G**
    - GPRS (*General Packet Radio Service*)
    - EDGE (*Enhanced Data rates for GSM Evolution*)

- **3G** (Standard di terza generazione)
  - **UMTS (Universal Mobile Telecommunications System)** per la terza basato invece sulla tecnica *CMDA* (Code Division Multiple Access) che, a differenza dei protocolli di seconda generazione consente velocità e numero di utenti maggiori.

    Vedi algoritmo di Viterbi.

Caratteristiche hardware dei dispositivi mobili

	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

Caratteristiche software dei dispositivi mobili

	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

Modulo di identificazione

- la cosiddetta **SIM card** (**Subscriber Identity Module)**
  - E’ un piccolo chip programmabile (smart card) al quale è associato un numero seriale detto IMSI (**International Mobile Subscriber Identity**) che sui sistemi informativi di un operatore telefonico consente di risalire a un determinato cliente dei propri servizi di telefonia mobile consentendo l’autenticazione per l’accesso alla rete.
  - E’ di proprietà del gestore, cui deve essere restituita su richiesta. La SIM non costituisce infatti il servizio venduto al cliente, bensì lo strumento attraverso il quale il cliente viene identificato e, quindi, usufruisce del servizio.
  - Per le recenti disposizioni antiterrorismo (pacchetto Pisanu), le carte non sono completamente funzionanti sino ad avvenuto caricamento dei dati anagrafici dell'acquirente presso il rivenditore.

Dati significativi

Dati contenuti nella SIM

- International Mobile Subscriber Identity (IMSI);
- preferenze di lingua e di rete (provider di servizi);
- contatori di costi e durata chiamate;
- informazioni circa la corrente (o la più recente) posizione del telefono;
- rubrica;
- messaggi SMS inviati e ricevuti;
- ultimi numeri chiamati.

Dati contenuti nel telefono

- impostazioni del telefono cellulare;
- calendario;
- SMS/MMS;
- registro delle chiamate;
- ora e data;
- suonerie;
- dati necessari per produrre funzioni extra (ad es. registrazioni audio, video, e immagini);
- dati generici memorizzati nella memoria del telefono;
- applicazioni eseguibili.

OUTLINE

- Background
- Procedure e principi
- Processo di analisi forense
  - Preservazione
  - Acquisizione
  - Ispezione ed Analisi
  - Reporting
- Tool
- Caso di studio

Il metodo di Daubert

Propone delle linee guida standard da seguire per garantire l'attendibilità dei risultati di un'analisi forense:

- **Accettazione e Testabilità** – le tecniche usate durante l'analisi dovrebbero essere condivise dalla comunità scientifica e comunque essere suscettibili di verifica.

- **Tasso di errore** – tutte le analisi di tipo scientifico sono soggette ad errori. Il tasso di errore delle tecniche usate per il recupero delle prove, dovrebbe essere noto e ben documentato.

- **Credibilità** – gli esperti chiamati ad investigare dovrebbero essere qualificati ed avere un grado di credibilità significativo presso la comunità scientifica.

- **Semplicità e chiarezza** – le tecniche usate per l'analisi dovrebbero poter essere spiegate con sufficiente chiarezza e semplicità a coloro che sono chiamati a giudicare.

Bisogna tener presente che le procedure di raccolta dei dispositivi, acquisizione delle prove e documentazione, hanno un effetto significativo sull'ammissibilità delle prove stesse durante la fase processuale.

Principi probatori

Come per qualsiasi altro tipo di investigazione, sono stati proposti dei principi conformi al trattamento di prove digitali che, per propria natura sono estremamente fragili, specialmente quelle trovate sui cellulari:

- Non compromettere i dati - Nessuna azione eseguita dagli investigatori deve compromettere i dati contenuti sul dispositivo digitale o sui dispositivi di memorizzazione.
- Documentare le fasi di acquisizione - Ogni accesso ai dati originali deve essere fatto in maniera sequenziale in modo che sia possibile documentare ogni azione e che l'insieme dei passi sia riproducibile.
- Documentare i risultati - Il processo di investigazione e le prove ottenute devono essere accuratamente documentate in modo da non generare ambiguità di lettura.
- Adottare procedure consentite dalla legge - Le persone coinvolte nell'investigazione hanno la responsabilità di applicare procedure in accordo alle leggi governative.

OUTLINE

- Background
- Procedure e principi
- Processo di analisi forense
  - Preservazione
  - Acquisizione
  - Ispezione ed Analisi
  - Reporting
- Tool
- Caso di studio

Preservazione

La preservazione è il primo passo da eseguire nella raccolta di prove digitali.

Da un punto di vista pratico coincide con la raccolta vera e propria del materiale sospetto o di interesse.

Il termine preservazione deriva dal fatto che le prove devono essere preservate. Procedure non corrette potrebbero causare perdita di dati digitali e fisici (es. impronte).

Preservazione - fase preliminare

- Bisognerebbe fotografare e descrivere l' ambiente prima di raccoglierne gli oggetti di interesse.
- Bisognerebbe evitare di toccare a mani nude o contaminare l'ambiente stesso e i dispositivi.
- Spegnere eventuali interfacce wireless o bluetooth per evitare interazioni non volute.
- Verificare la presenza di accessori relativi al dispositivo (es. cavi, adattatori).
- Verificare la presenza di strumenti correlati (es. pc per la sincronizzazione).

Preservazione - raccolta delle prove

- Registrare data e ora del dispositivo verificando l'eventuale scarto rispetto all'ora corrente.
- Isolare il cellulare da altri dispositivi.
- Se il telefono è acceso quando viene trovato, bisogna isolarlo dalla rete per evitare che nuovo traffico sovrascriva i dati esistenti; esistono diverse possibilità per farlo, ma ognuna presenta degli svantaggi:
  - Spegnerlo.
  - Inserirlo in un borsa isolante.
  - Airplane mode.

Preservazione - raccolta delle prove

- **Spegnimento:** spegnere il cellulare potrebbe attivare il codice di autenticazione (es., il codice di sicurezza sulla SIM o il PIN impostato sul cellulare) richiesto per l'accesso.

- **Isolamento:** c'è uno spreco di batteria maggiore perché il dispositivo cercherà senza successo di connettersi ad una rete. Un certo periodo di fallimento della ricerca, in certi telefoni causa la cancellazione dei dati relativi alla rete che però potrebbero essere utili nella investigazione.

- **Airplane mode:** richiede l'interazione con la tastiera del telefono. Questo pone alcuni rischi, a meno che, il tecnico che fa questa operazione non abbia familiarità con il dispositivo in questione o ci sia una documentazione delle azioni fatte.

Preservazione – catalogazione

- Etichettare ogni dispositivo inserendo la data e l'ora del ritrovamento.
- Allegare fatture, manuali e materiali di imballaggio che potrebbe fornire utili informazioni per valutare le capacità del dispositivo, la rete usata, una sua descrizione e codici di sblocco come il PIN.
- Se il display del dispositivo è in uno stato visibile, il contenuto dello schermo dovrebbe essere fotografato e, se necessario, registrato manualmente, catturando il tempo, lo stato del servizio, il livello di batteria e altre icone mostrate.

Preservazione - documentazione

Oltre a contenere tutto il materiale allegato ai dispositivi, una buona documentazione relativa a questa fase dovrebbe rispondere alle seguenti domande:

- Chi ha raccolto i dispositivi?
- Come e dove sono stati raccolti?
- Chi li custodisce?
- Come sono state memorizzate e protette le prove raccolte in dispositivi di storage?
- Chi analizza le prove e perché?

creando quella che viene chiamata catena di custodia

OUTLINE

- Background
- Procedure e principi
- Processo di analisi forense
  - Preservazione
  - Acquisizione
  - Ispezione ed Analisi
  - Reporting
- Tool
- Caso di studio

Acquisizione

- L’investigazione forense inizia con l’identificazione del dispositivo; il tipo, il sistema operativo e altre caratteristiche. Ottenute queste informazioni si può procedere alla creazione di una copia forense del contenuto del device.
- PROBLEMA
  - Soltanto pochi dei tool forensi che esistono creano una copia forense per certi tipi di cellulari e nessun singolo tool può essere usato per fare una copia forense di tutti i tipi di cellulari.
  - Dal tipo di telefono, perciò, dipende la scelta di quali tool usare per l'investigazione.

Isolamento Radio

- Il laboratorio in cui si esegue l'acquisizione dovrebbe essere isolato dalle frequenze radio.
- PROBLEMA
  - poiché la comunicazione viene impedita, il dispositivo tenta di mandare continuamente un segnale più forte per cercare di stabilire un contatto con la rete. Questa attività riduce significativamente la durata di vita della batteria.
- TECNICHE
  - *Uso di jamming o dispositivi di spoofing*
    - consiste nell'emissione di un segnale più forte rispetto a quello supportato dal cellulare in modo da interferire con il segnale o addirittura rendere il dispositivo stesso inutilizzabile.
  - *Uso di una area di lavoro protetta*
    - Una “Faraday tent” (tenda Faraday) : una sorta di laboratorio “nomade” isolato da contaminazioni radio.
  - *Uso di una (U)SIM sostitutiva*
    - una nuova carta (U)SIM viene usata per imitare l’identità della scheda originale e prevenire accessi alla rete.

Identificazione del dispositivo

- Per poter avanzare nell'investigazione, abbiamo bisogno di identificare marca e modello dei dispositivi ed il service provider utilizzato. Queste informazioni permettono agli investigatori di selezionare gli appropriati tool per l'acquisizione.
- PROBLEMA
  - Occorre prestare attenzione poiché potrebbero essere state apportate delle modifiche.
  - Esempi: rimozione etichetta produttore, rimozione splash screen etc

Tecniche per identificazione dei dispositivi

- **Caratteristiche fisiche del dispositivo**
  - Sul Web è possibile trovare database interrogabili a partire dagli attributi fisici, capaci di identificare un particolare dispositivo
- **Interfacce del dispositivo**
  - Es. l'alimentatore è tipicamente specifico di un unico produttore e potrebbe servire ad identificare la classe del dispositivo
- **Etichette presenti sul dispositivo**
  - per i telefoni spenti, le informazioni possono essere ottenute dalla cavità della batteria.
  - Esistono identificatori univoci come il codice identificativo dell'apparecchio (IMEI o ESN)
    - Per dispoditivi GSM esiste codice International Mobile Equipment Identifier (IMEI)
      - Per ottenere codice digitare sul dispositivo *#06#
    - Per dispositivi CDMA esiste Electronic Serial Number (ESN)
- **Reverse Lookup**
  - se il numero del telefono è conosciuto, può essere usato un reverse lookup per identificare un operatore di rete, la città e lo stato di origine. FoneFinder è un esempio di servizio che permette di ottenere tali informazioni .

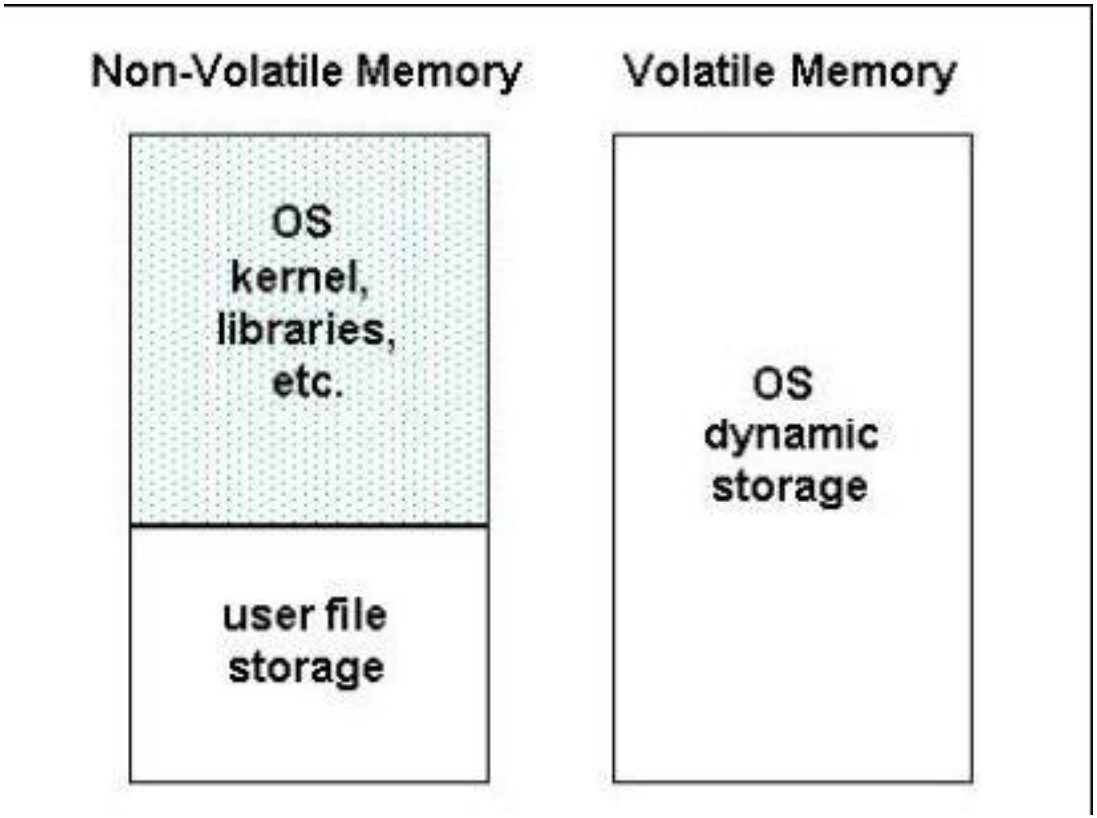
Selezione del tool

- Una volta che marca e modello del telefono sono note, possono essere recuperati i relativi manuali e studiati.
- Criteri :
  - **Usabilità** – la capacità del tool di presentare i dati in una forma significativa per un investigatore
  - **Comprensibilità** – la capacità di presentare tutti i dati in modo da rendere evidenti sia quelli che incriminano sia quelli che scagionano l'imputato
  - **Accuratezza** – la qualità dell'output sia stata verificata e abbia un margine di errore certo
  - **Determinismo** – la capacità di produrre lo stesso output a partire dallo stesso insieme di istruzioni e di dati in input
  - **Verificabilità** – la capacità di garantire l'accuratezza dell'output attraverso l'accesso a rappresentazioni intermedie dei risultati

Considerazioni sulle memorie

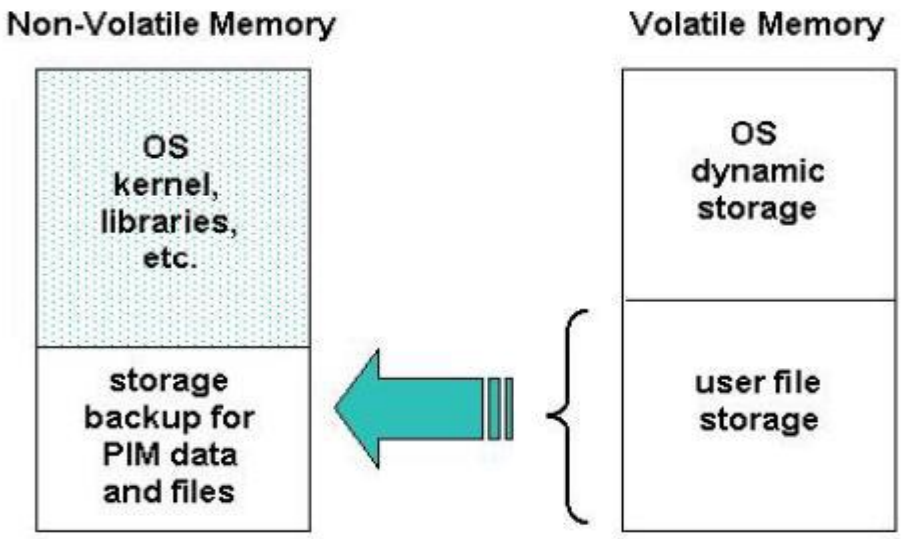
- La struttura della memoria del telefono potrebbe avere una struttura rigida come un file system formattato, venire assegnata dinamicamente o essere partizionato in aree dedicate: area per la rubrica, area per gli eventi del calendario, log delle chiamate e così via.

Considerazioni sulle memorie (1)

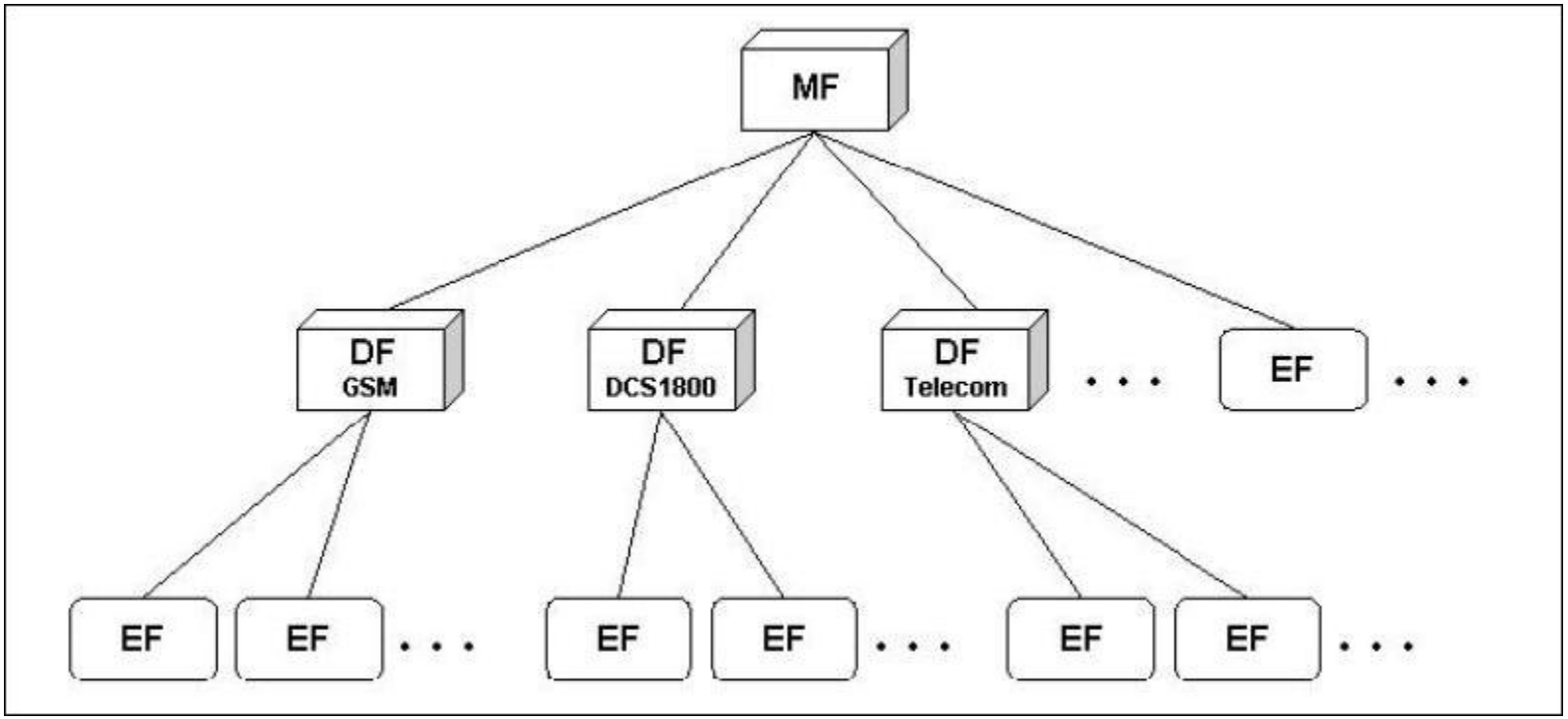


Considerazioni sulle memorie (2)

- La memoria volatile è usata per la memorizzazione dinamica e i file utenti. La memoria non volatile è usata principalmente per mantenere il codice del sistema operativo e possibilmente i dati delle applicazioni PIM



Considerazioni su filesystem SIM



Considerazioni su filesystem SIM(1)

- I file nelle directory DF_{GSM} e $DF_{DCS1800}$ contengono principalmente informazioni relative alla rete.
- I file in $DF_{TELECOM}$ contengono informazioni relative ai servizi attivi del gestore.
- I file EF sono importanti perché possiamo ricavare info su:
  - **Informazioni correlate al servizio**, incluso l'identificatore univoco per la (U)SIM, l' Integrated Circuit Card Identification (ICCID), informazioni sull'abbonato, l' International Mobile Subscriber Identity (IMSI)
  - **Rubrica e informazioni sulle chiamate**, conosciute rispettivamente come Abbreviated Dialling Numbers (ADN) e Last Numbers Dialled (LND)
  - **Informazioni di messaging**
  - **Informazione di locazione,** incluso Location Area Information (LAI) per la comunicazione vocale e Routing Area Information (RAI) per le comunicazioni dati

Dispositivi non ostruiti

- Dispositivi per la quale non è richiesta autenticazione per l'accesso ai contenuti
  - Acquisizione
    - Dei dati contenuti nel cellulare con appropriati tool o utilizzando l'interfaccia hardware JTAG.
    - Dei dati contenuti sulla (U)Sim tramite direttive chiamata Application Protocol Data Units (APDU).

Nokia 3220 JTAG interface

Dispositivi Ostruiti

- Quei dispositivi che necessitano di una corretta autenticazione affinché possano essere accesi vengono detti **ostruiti.**
- Esistono tre tipici approcci per recuperare dati dai telefoni ostruiti:
  - metodi investigativi
  - metodi che agiscono sul software
  - metodi che agiscono sul hardware.

OUTLINE

- Background
- Procedure e principi
- Processo di analisi forense
  - Preservazione
  - Acquisizione
  - Ispezione ed Analisi
  - Reporting
- Tool
- Caso di studio

Ispezione ed Analisi

- Scoprire le prove da portare in un processo, incluse quelle che possono essere nascoste e oscurate.
- L'investigatore o l'analista forense forniscono informazioni su cosa cercare, mentre l'esaminatore forense fornisce il mezzo per cercare potenziali informazioni rilevanti .
- A seconda del caso, la strategia cambia. Per esempio in un caso di pedofilia si può iniziare con lo scandagliare tutte le immagini grafiche presenti sul sistema, mentre in un caso relativo ad ingiurie su Internet, si inizia a scandagliare tra i file della cronologia del browser.

Potenziali Prove

- Le potenziali prove :
  - Dati abbonato
  - E-mail
  - Data e orologio
  - Linguaggio impostato
  - Documenti elettronici
  - Foto, file multimediali
  - SMS, MMS
  - Elementi della rubrica
  - Instant messaging
  - Cronologia del browser
  - Informazioni di localizzazione
  - Registro chiamate entranti, uscenti e perse e log delle chiamate.

Scopi

- In base alla conoscenza del caso, l'esaminatore forense e l'analista possono procedere verso la realizzazione dei seguenti obiettivi:
  - **Chi** - Raccogliere informazioni sulle persone coinvolte.
  - **Cosa** - Determinare con esattezza la natura degli eventi .
  - **Quando** - Costruire la successione temporale degli eventi.
  - **Perché** - Scoprire informazioni che possano giustificare il movente.
  - **Come** - Scoprire quali strumenti o azioni sono state necessarie.

Obiettivi che si possono raggiungere con particolari informazioni

	Who	What	Where	When	Why	How
Subscriber/Device Identifiers	X					
Call Logs	X			X		
Phonebook	X					
Calendar	X	X	X	X	X	X
Messages	X	X	X	X	X	X
Location			X	X		
Web URLs/Content	X	X	X	X	X	X
Images/Video	X	X	X	X		X
Other File Content	X	X	X	X	X	X

Record delle chiamate e dell'abbonato

- I record mantenuti dal service provider, forniscono informazioni riguardanti i dettagli delle chiamate o degli SMS inviati da un cellulare.
- il database generalmente contiene le seguenti informazioni:
  - Nome e indirizzo dell'utente
  - Eventuali indirizzi di posta elettronica
  - Eventuali altri numeri di telefono
  - Dettagli di fatturazione dell'utente
  - Numero di telefono (MSISDN)
  - Numero seriale della (U)SIM (ICCID)
  - PIN/PUK della (U)SIM
  - Servizi permessi
  - Numero delle carte di credito usate per il pagamento

OUTLINE

- Background
- Procedure e principi
- Processo di analisi forense
  - Preservazione
  - Acquisizione
  - Ispezione ed Analisi
  - Reporting
- Tool
- Caso di studio

Reporting

- Processo di generazione di un sommario dettagliato che illustra l'intera fase investigativa.
  - Passi eseguiti e risultati e conclusioni raggiunte
- Un buon report, descrive con molta cura
  - Azioni eseguite e le eventuali osservazioni
  - Risultati dei test e delle ispezioni
  - Ragionamenti maturati sullo studio delle prove
  - Note fotografiche e contenuti generati dai tool
- Le prove ricavate, tool, tecniche e metodologie utilizzate, sono oggetto di dibattito durante il processo, pertanto la documentazione si rivela essenziale

Reporting e riproducibilità

- Includere una copia del software usato insieme all'output che si otterrebbe applicando la procedura
  - Evita che una diversa versione dello stesso software ottenga diversi risultati
  - Utile quando la procedura deve essere riprodotta a distanza di tempo nei successivi dibattimenti o dalla difesa

OUTLINE

- Background
- Procedure e principi
- Processo di analisi forense
  - Preservazione
  - Acquisizione
  - Ispezione ed Analisi
  - Reporting
- Tool
- Caso di studio

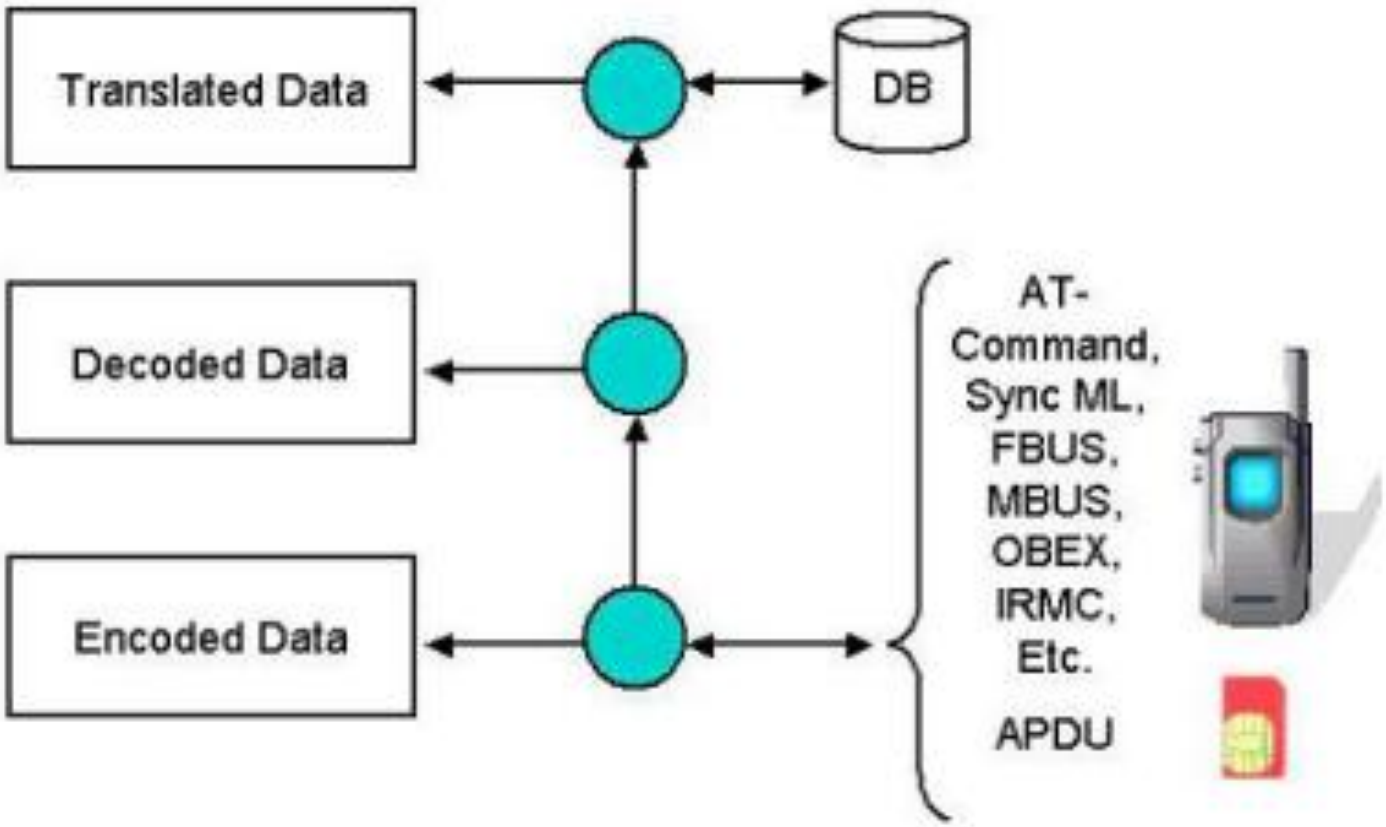
Situazione dei dispositivi mobile

- Esistono varie famiglie
  - Cellulari, Smartphone, PDA
- Esistono varie piattaforme hardware e software
  - Symbian, Windows Mobile, Android, etc.
- Protocolli di comunicazione diversi
  - OBEX, FBUS, Comandi AT
- Innovazione continua
- Avremo tool mobile forensic che lavorano per una particolare famiglia, marca, piattaforma.

Modalità di acquisizione dati

- Acquisizione Fisica: copia bit a bit della memoria fisica del dispositivo.
  - Lettura dei singoli chip di memoria, JTag, etc.
  - Si recuperano molte informazioni
  - Dispendiosa in termini di tempo, conoscenze e costi.
- Acquisizione Logica: copia bit a bit degli oggetti di memoria logici.
  - Poco costosa in termini di tempo, conoscenze e costi
  - Si recuperano poche informazioni

Schema di un tool mobile forensic



Caratteristiche di Tool per il Mobile Forensic

- Acquisire le informazioni senza alterare il contenuto sul dispositivo mobile
- Meccanismi di conservazione dell'integrità dei dati acquisiti
- Decodificare i dati acquisiti in modo da renderli facilmente interpretabili dall'utente
- Presentare un report dettagliato con le informazioni recuperate
- Classificheremo i MFT in base al target
  - MFT per handset, (U)SIM e Toolkit

MFT per (U)SIM

- Dedicati al recupero dati dalle (U)SIM
  - ID dell'utente, seriale , SMS, Rubrica, Registro chiamate.
- Utilizzano lettori di (U)SIM
- Forensic Card Reader
  - Effettua un report dei dati acquisiti in un file XML
- SIM Card Seizure
  - Hashing dei dati acquisiti
  - Report in formato ASCII
- USIMdetective
  - Hashing dei dati acquisti
  - Possibilità di scegliere l'accuratezza del report

MFT per handset

- Derivati da tool dedicati a PDA o da Phone Manager
  - Acquisizione logica utilizzando cavi o interfacce wireless
- Paraben Device Seizure
  - Acquisizione fisica su più SO
  - Strumenti di hashing e di reporting
- Oxygen Phone Manager (versione forense)
  - Phone manager con funzionalità di scrittura disattivate
- BitPIM
  - Open Source e dedicato a cellulari LG e Motorola

Mobile Forensic toolkit

- Acquisiscono anche da (U)SIM
- Paraben Cell Seizure
  - Simile a Device Seizure
- MOBILedit! Forensic
  - Versione forense di un Phone manager
- TULP2G
  - Open Source
  - Acquisizione da USB e interfacce wireless
  - Generazione del report in XML

Altre tecniche per acquisire dati

- Phone manager
  - Nokia PC Suite, etc.
  - Possono alterare le informazioni presenti nel dispositivo da analizzare
- Port Filtering
  - Intercettare la comunicazione tra cellulare e un phone manager
  - Implementazione di un filtro che si “aggancia” alle API del SO della macchina ove è installato PM

Isolamento e valutazione dei tool forensi

- Più tool che girano sulla stessa macchina possono essere incompatibili
- Per ogni tool o insieme di tool tra loro incompatibili realizzare una macchina virtuale
- Far girare contemporaneamente le VM realizzate
- Effettuare alcuni test su dispositivi di prova uguali a quello sequestrati.

OUTLINE

- Background
- Procedure e principi
- Processo di analisi forense
  - Preservazione
  - Acquisizione
  - Ispezione ed Analisi
  - Reporting
- Tool
- Caso di studio

Recupero SMS cancellati da un dispositivo Symbian

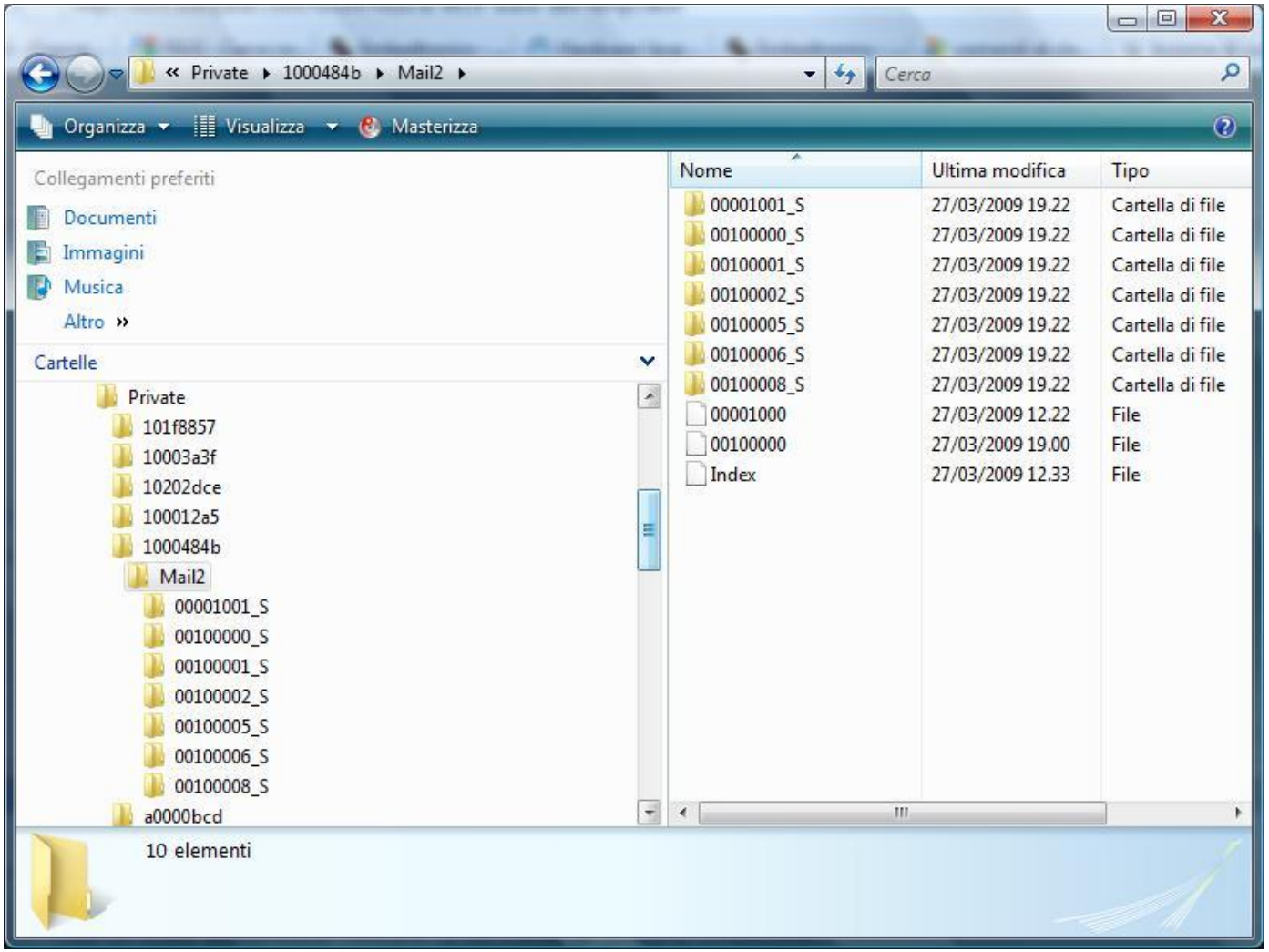
- Tre possibili soluzioni
  - Acquisizione fisica
    - Dispendiosa in termini di tempo e di costi
  - Chiediamo aiuto a MacGyver
    - Puntata trasmessa da La7 il 19/1/2009

  - Sfruttiamo un hack
    - Recupero di un file che contiene informazioni su SMS cancellati
      - Non necessita di particolari tool o apparecchiature
      - Facile, veloce, economico.

Directory private di Symbian

- Conservano alcune informazioni importanti riguardanti il dispositivo
  - Lista dispositivi BT utilizzati
  - Registro applicazioni installate
  - SMS, MMS Mail in entrata, uscita e bozze
- Contenute in C:\
- Contraddistinte da un codice numerico
- Non visibili dall'utente se non attraverso alcuni programmi da installare sul dispositivo
  - ROMPatcher, HelloOX, etc.

Directory 1000484B



File Index

- Indicizza SMS, in entrata e in uscita.
- Ogni entry contiene informazioni tipo:
  - Descrizione: Parte iniziale del testo del sms.
  - Numero telefono del destinatario
- Tali informazioni sono in chiaro
- E’ possibile recuperare al massimo i primi 60 caratteri del SMS indicizzato
  - Dipende dalle riscritture

Procedura di recupero del file Index

- Scollegamento del dispositivo dalla rete cellulare
- Inserimento di una miniSD nel dispositivo
- Inserire una serie di comandi sul dispositivo che consentono di salvare gli SMS sulla miniSD
- Inserimento della miniSD in un lettore per SD
- Recupero e visualizzazione del file Index con un file manager

Computer Forensic – Approfondimenti

- La criminalità informatica: metodi d'indagine e la collaborazione delle aziende bancarie"
  - http://www.marcodimartino.it/documenti/pdf/Vulpiani_Criminalita_informatica_metodi_dindagine.pdf
- Diritto penale nell'informatica. Sono presenti alcuni interessanti articoli sulla esperienza italiana nella computer crime.
  - http://www.marcodimartino.it/articoli_it.htm
- Norme italiane in ambito giuridico
  - http://www.diritto.it/materiali/tecnologie/valeri.html
- ICT LAW
  - http://www.fiammella.it/ICT_Law.htm

Domande ?