2008

Mobile Forensic

Linee Guida

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 questa guida affrontiamo una discussione sulle problematiche inerenti alle attività di analisi forense su dispositivi mobile e le procedure per la preservazione, acquisizione, investigazione, analisi e reporting delle informazioni digitali, che avranno valore probatorio in una inchiesta giudiziaria.

A cura di :

Carotenuto Francesco
<francesco.carotenuto@gmail.com>
D'Amato Angelo
<damatoangelo@gmail.com>
Eletto Antonio
<antele@gmail.com>

Professore

Alfredo De Santis

Corso di SICUREZZA SU RETI 2

SOMMARIO

1. Introduzione

Un dispositivo mobile è potenzialmente in grado di contenere una grande quantità di informazioni, sia relative alle azioni compiute dall'utente, sia relative ai dati in esso contenuti. Tali informazioni sono sempre più richieste come prove in indagini della magistratura poiché, a causa della loro enorme diffusione nella nostra società, gli apparecchi mobili sono spesso coinvolti in attività criminali legate, sia al crimine tradizionale, quali acquisto di droga, rapine, molestie ecc., sia al crimine elettronico, come ad esempio il furto di informazioni sensibili, che, grazie all'integrazione delle comunicazioni e all'interoperabilità con Internet, si dimostra in costante crescita. In particolare, il veloce sviluppo del settore della telefonia mobile, sta portando alla produzione di dispositivi sempre più potenti e con maggiori funzionalità; Questa crescente complessità li rende sempre più vulnerabili ad attacchi, tanto più gravi se si considera l'aumento del carico informativo che tali strumenti sono capaci di contenere.

Per poter capire quali siano i dati potenzialmente rilevanti contenuti in un dispositivo mobile e quali strategie adottare per ottenerli, è necessario avere una profonda conoscenza delle caratteristiche hardware e software del dispositivo stesso. La comunità forense deve affrontare una costante sfida per tenersi al passo con le ultime tecnologie ed ottenere quelle informazioni che potrebbero essere fondamentali per il buon esito di una analisi investigativa.

Nel seguito, dopo una breve introduzione sulle caratteristiche delle reti cellulari e dei dispositivi mobili, studieremo i principi e metodi per effettuare una analisi forense, vedremo come i dati ottenuti debbano essere trattati al fine di costituire delle valide prove in un contesto processuale, presenteremo una panoramica sui tool disponibili per questo tipo di analisi ed infine un caso pratico affrontato.

2. Background

Le reti di telefonia mobile sono basate su una gamma di differenti tecnologie. In questo capitolo vogliamo darne una descrizione sia dal punto di vista hardware che dal punto di vista software .

Sebbene non si tratti di una descrizione esaustiva, molti di questi concetti saranno utili per comprendere i prossimi capitoli, in cui entreremo più nel dettaglio delle tecniche usate per l'analisi forense.

2.1 CARATTERISTICHE SULLE RETI CELLULARI

La **telefonia cellulare** è una tipologia di accesso ad una rete telefonica realizzata per mezzo di onde radio e ricetrasmettitori terrestri. Il termine "cellulare" si riferisce al fatto che il sistema di comunicazione senza fili utilizzato, suddivide le grandi aree geografiche in aree più piccole chiamate celle ognuna supervisionata da una **Stazione Radio Base** o **BTS (*Base Transceiver Station*)** che occupa della comunicazione con i dispositivi mobili. Ogni conversazione o canale, richiede una coppia di frequenze dedicate, una per permettere la comunicazione tra il dispositivo mobile e la BTS (frequenza uplink) e una per la comunicazione tra BTS e dispositivo mobile (frequenza downlink) tali frequenze vengono prese da due insiemi di frequenze distinte.

L'organizzazione a celle permette di riutilizzare la stessa frequenza per celle diverse tra loro distanti, senza che ci siano interferenze. Ciò è reso possibile dal fatto che la potenza del segnale diviene sempre più debole man mano che ci si allontana dalla BTS. Le celle sono raggruppate in cluster. Ad ogni cluster viene assegnata l'intera banda e ogni cella appartenente al cluster utilizza frequenze diverse rispetto ad una qualsiasi altra cella all'interno dello stesso cluster. Il clustering assicura che le celle che utilizzano la stessa frequenza siano separate da una distanza minima chiamata distanza di riuso.

La Figura 1, illustra un esempio semplificato di clustering, in cui le celle colorate indicano un singolo cluster. Ogni cella di un cluster utilizza una sola frequenza delle 7 disponibili, mentre la linea tratteggiata mostra la distanza di riuso D, tra due celle che utilizzano la stessa frequenza ma che appartengono a cluster diversi.

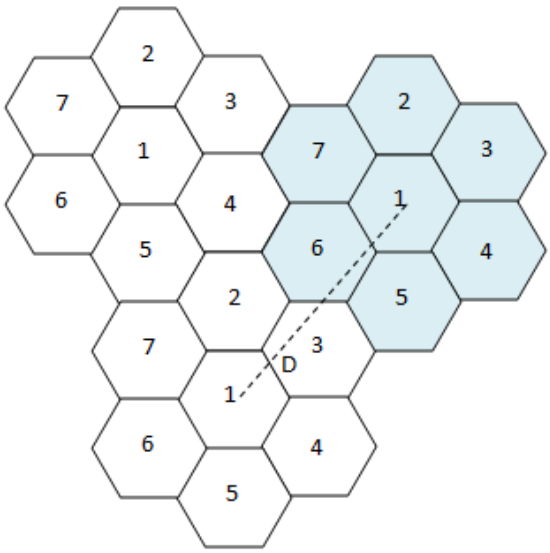

FIGURA 1: ESEMPIO DI CLUSTERING

Oltre alla BTS e alla celle in un sistema di telefonia cellulare sono presenti anche il controller **BSC (*Base Station Controller*)** che effettua l'assegnazione del canale (ossia una coppia di frequenze downstream e upstream) 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*)**. Il controller di fatto fa da ponte tra il Mobile Switching Center e le Base Transceiver Station. L'MSC controlla un insieme di BSC e gestisce la comunicazione

attraverso la rete cellulare, incluso l'interfacciamento alla rete di telefonia pubblica. La Figura 2 illustra un sistema generico di organizzazione delle reti cellulari.

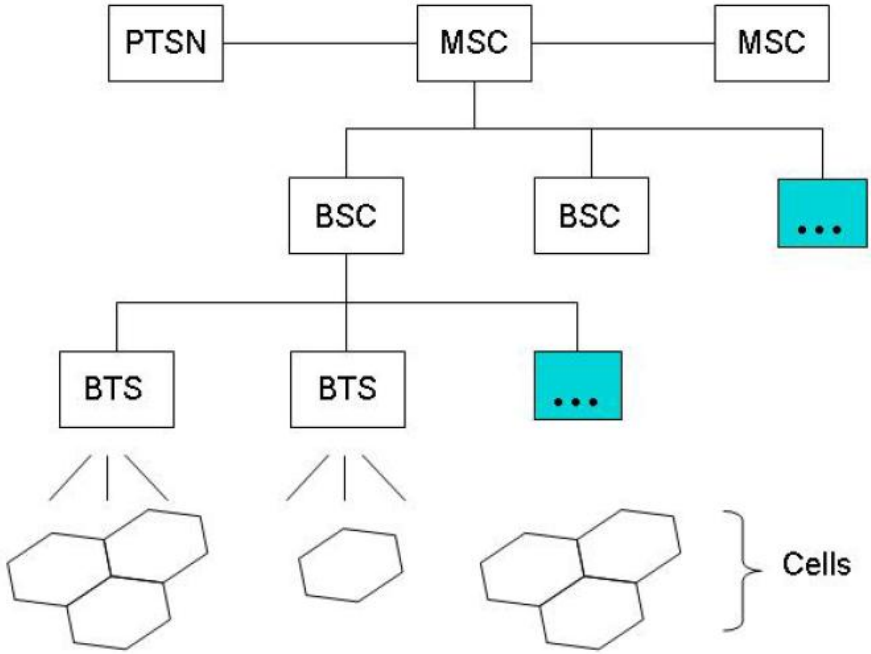

FIGURA 2: ORGANIZZAZIONE DELLE RETI CELLULARI

Per eseguire i suoi task, l'MSC usa diversi database. Il database principale è il sistema di memorizzazione centrale, chiamato Home Location Register(HLR), dove sono memorizzati i dati degli abbonati e informazioni di servizio. Un altro database usato in congiunzione con HLT per il roaming dei telefoni cellulari al di fuori della propria area di servizio è il Visitor Location Register. Le informazioni di account, come dati sull'abbonato, i servizi sottoscritti, si trovano nell' HLR e sono usate dall'MSC per istradare chiamate e messaggi e per memorizzare dettagli della comunicazione. I dati di accounting dell'abbonato e i record delle chiamate effettuate e ricevute sono spesso una sorgente di prove in una investigazione.

Tra le differenti tecnologie su cui si basa la telefonia mobile, quelle attualmente più utilizzate sono quella **2G** (di seconda generazione) e quella **3G** (di terza generazione). In particolare, lo standard **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) e lo standard **UMTS (Universal Mobile Telecommunications System)** per la terza basato invece sulla tecnica W-CMDA (Wideband Code Division Multiple Access) che, a differenza dei protocolli di seconda generazione consente velocità e numero di utenti maggiori.

2.2 CARATTERISTICHE DEI DISPOSITIVI MOBILI

I dispositivi mobile dispongono di un'ampia gamma di funzionalità, da semplici agende digitali a caratteristiche vicine a quelle di un personal computer. Compatti, leggeri ed alimentati a batteria, sono costruiti per facilitare la mobilità. Molti di essi hanno un insieme base di caratteristiche e capacità confrontabili. Sono dotati di microprocessore, ROM, RAM, un modulatore radio, un processore di segnali digitali, un microfono, uno speaker, una varietà di interfacce hardware e di un display a cristalli liquidi (LCD). Il sistema operativo del dispositivo è contenuto nella **ROM** che, con opportuni tool, può essere cancellata e riprogrammata elettronicamente. La **RAM**, in alcuni modelli potrebbe essere usata per memorizzare dati dell'utente ed è tenuta attiva da una batteria che, se si rompe o si esaurisce, può provocare la perdita delle informazioni. Gli ultimi modelli sono equipaggiati con microprocessori a livello di sistema che riducono il numero di chip di supporto richiesti e vantano un sostanziale incremento di memoria grazie all'uso di memorie di tipo flash come **Secure Digital (MiniSD)**, **MultiMedia Card Mobile (MMC)** o card **SDIO** dotate di interfacce per il **bluetooth** o il **WiFi**. I dispositivi hanno caratteristiche fisiche e tecniche che variano rispetto la dimensione, grandezza, velocità del processore, capacità della memoria. Possono fornire capacità di espansione per l'aggiunta di nuove funzionalità. Molti modelli di cellulari includono ormai funzionalità simili a quelle di un **PDA**, quali: **Global Positioning Systems(GPS)**, fotocamera, videocamera.

In definitiva, possono essere classificati come:

- ✓ **cellulari di base:** usati solo per chiamate vocali e per inviare **SMS**;
- ✓ **telefoni avanzati:** rispetto ai modelli di base, offrono caratteristiche aggiuntive e servizi per il multimedia;
- ✓ **smart phones:** fondono le caratteristiche di un telefono avanzato con quelle di un PDA.

Le differenze principali tra le te classi sono evidenziate nella seguente tabella 1:

TABELLA 1 CARATTERISTICHE HARDWARE

	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

Chiaramente le tre classi hanno un confine abbastanza flessibile. C'è una forte tendenza ad aggiungere caratteristiche avanzate anche nei dispositivi base, mentre ne vengono aggiunte di nuove a quelli di fascia alta. Ne consegue che la classificazione data serve solo per dare una visione e una linea guida generale.

Indipendentemente dal tipo di cellulare, tuttavia, tutti includono il supporto vocale, quello per il text messaging (SMS) e sono dotati di un insieme di applicazioni dette **Personal Information Management (PIM)** che includono la gestione della rubrica, un calendario e altre facilities, come la possibilità di sincronizzare i dati con un computer. I dispositivi più avanzati permettono anche l'invio di messaggi multimediali (MMS), connessione a internet e navigazione sul web, consentendo lo scambio di posta elettronica e l'uso di messaggistica istantanea in aggiunta ad applicazioni PIM che lavorano su hardware integrato come, ad esempio, una (video/foto)camera.

Pur avendo dimensioni solitamente più grandi rispetto ad altri telefoni, gli smart phone, includono le capacità di un **PDA** per la gestione di documenti elettronici (esempio, slide, pdf, documenti di testo) e permettono l'esecuzione di un'ampia varietà di applicazioni special-purpose. Sono dotati di un display più grande (esempio, ¼ **VGA** e più grandi) e potrebbero avere una tastiera QWERTY integrata o un touch sensitive screen. In genere, offrono anche più possibilità di espansione e protocolli di sincronizzazione per scambiare altri tipi di dati oltre a quelli gestiti dalle applicazioni PIM (esempio, immagini, audio, e formati per la compressione di file).

La tabella 2 lista le differenze nelle caratteristiche software delle classi di dispositivi mobili identificati.

TABELLA 2 CARATTERISTICHE SOFTWARE

	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

I cellulari base e quelli di fascia alta tipicamente usano un sistema operativo proprietario come Palm OS, Windows Mobile (phone edition), RIM OS, Symbian OS, sebbene ci sia un crescente interesse verso le piattaforme aperte basate su Linux.

2.3 CARATTERISTICHE DEI MODULI DI IDENTIFICAZIONE

Uno dei componenti più importanti e distintivi del sistema GSM è la cosiddetta **SIM card**, acronimo di **Subscriber Identity Module**. La SIM è una Smart card su cui sono memorizzati i dati descrittivi dell'abbonato, compreso il numero di telefono, e che ha la funzione principale di fornire autenticazione ed autorizzazione all'utilizzo della rete. Trasferendo la SIM card da un telefono all'altro è possibile mantenere tutte le informazioni relative all'abbonamento. Chiaramente, l'abbonato può anche cambiare operatore, mantenendo lo stesso telefono e cambiando la propria SIM card. Alcuni operatori, tuttavia, inibiscono questa funzionalità, consentendo l'uso di una sola SIM card su ogni terminale; Questa pratica, illegale in alcuni paesi, è chiamata SIM locking. Negli USA, la maggior parte degli operatori bloccano i terminali da loro venduti. Questo, perché il prezzo del terminale è in gran parte sovvenzionato dai profitti dell'abbonamento, gli operatori dunque, cercano di evitare di favorire i concorrenti in caso di migrazione. Gli abbonati hanno il diritto di rimuovere il blocco dietro pagamento di una tariffa qualora lo richiedessero. Nella maggior parte dei paesi, la rimozione del blocco non è considerata illegale. In Italia è previsto lo sblocco a pagamento dopo 9 mesi e gratuito dopo 18.

Oltre alle classiche SIM, molto diffuse nei sistemi GSM, si sono diffuse anche le cosiddette **Ultra SIM** o, più semplicemente, **USIM** (**Universal Subscriber Identity Module [USIM]**), particolari tipi di Smart Card con caratteristiche simili a quelle di una SIM, ma appositamente create per i cellulari di terza generazione; Dotate inizialmente di una capacità di memoria tipicamente compresa tra i 64 e i 256 kB, recentemente sono stati realizzati modelli con tecnologia Flash capaci di memorizzare dati per 128 Megabytes.

Le USIM hanno le dimensioni fisiche tipiche delle SIM, ma, rispetto a queste ultime, alcuni anni fa è stato introdotto un terzo fattore di forma (12×15 mm) con lo scopo di

consentirne l'utilizzo in terminali mobili di ridotte dimensioni. Questo fattore di forma tuttavia, oggi poco diffuso a causa dei problemi di compatibilità con i terminali esistenti.

La USIM card solitamente memorizza le credenziali necessarie all'autenticazione del cliente (algoritmi di autenticazione e chiavi di sicurezza), i dati privati del cliente, quali la rubrica telefonica personale (nome, numero di telefono, secondo numero di telefono, secondo nome, e-mail, gruppi) ed i messaggi SMS, nonché alcune informazioni tipiche dell'operatore mobile che distribuisce la card (come la lista delle reti preferite).

I dettagli sulle caratteristiche delle USIM possono essere reperiti direttamente dalla specifica tecnica 3GPP TS 31.102 scaricabile dal sito del 3GPP.

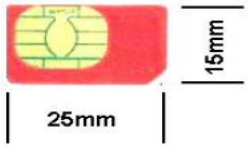

Figure 2: (U)SIM Format

FIGURA 3 (U)SIM FORMAT

2.4 I DATI POTENZIALMENTE SIGNIFICATIVI

Le informazioni memorizzate su un dispositivo mobile soggette al recupero e all'analisi, possono trovarsi sulla carta SIM, sulla memoria rimovibile e sulla memoria interna del telefono. Oltre a queste, ci sono le informazioni memorizzate dal fornitore dei servizi che, per ovvi motivi, non sono soggette a questo tipo di analisi.

La carta SIM, che permette di identificare l'abbonato nella rete, contiene un certo numero di file dai quali è possibile ricavare informazioni relative all'utente:

- 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.

Occorre tener presente però, che molte delle funzioni disponibili sulla carta SIM sono opzionali, pertanto, alcune informazioni potrebbero non essere presenti sulla scheda.

In aggiunta alla memoria SIM, è disponibile la memoria interna del telefono, dove risiede il software. Questo spazio può essere utilizzato per estendere la memoria SIM e/o per memorizzare dati aggiuntivi alla rubrica, ai log delle chiamate e così via. Alcuni esempi delle informazioni che si possono trovare in una memoria interna sono:

- 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.

Molti telefoni cellulari moderni vengono forniti con una grande quantità di memoria, con l'opzione di estenderla con una scheda di memoria rimovibile. Queste schede rimovibili sono generalmente utilizzate per la memorizzazione di file multimediali, come ad esempio audio, video, immagini e messaggi MMS. Ciò non toglie, tuttavia, che possano essere utilizzate per il trasferimento e lo stoccaggio di qualsiasi forma di dati. Sebbene il telefono cellulare possa non essere in grado di riconoscere o visualizzare determinati dati, può comunque essere utilizzato come una generica periferica di archiviazione.

I informazioni conservate dal fornitore del servizio, come specificato in precedenza, non sono inerenti al recupero dati, tuttavia, includono informazioni importanti sull'abbonato, sulla posizione geografica del telefono e tutto ciò che riguarda la fatturazione. Ogni volta che viene effettuata una chiamata o viene inviato un messaggio di testo, viene creato e memorizzato un record di dati.

Nello specifico, tali informazioni, contengono:

- i numeri di telefono del chiamante e del ricevente;
- la durata della chiamata;
- le posizioni geografiche iniziali e finali delle due parti.

3. Procedure e Principi

In ogni procedimento investigativo, le indagini vengono condotte in modi diversi in relazione alle circostanze dell'incidente, alla gravità ed alla preparazione ed esperienza del team. Le investigazioni digitali sono spesso basate sui principi relativi alle tecniche di investigazione tradizionali delle forze dell'ordine. Questo capitolo si propone di dare una visione generale dei vari modelli procedurali che sono stati proposti e dei principi che li regolano.

3.1 Ruoli e Responsabilità

Qualunque sia il tipo di incidente la pianificazione del processo investigativo dovrebbe essere volta a stabilire i ruoli delle persone coinvolte nell'indagine. Questo paragrafo fornisce un modello organizzativo generico. Le diverse situazioni potrebbero rendere necessarie delle modifiche. Tuttavia, distinguere i ruoli è un modo utile per identificare le responsabilità associate ad ogni membro del team ed essere sicuri che tutte le attività di investigazione vengano eseguite con efficienza.

- ***First Responder*** è personale addestrato che arriva per primo sulla scena dell'incidente e fa una valutazione iniziale. Le responsabilità dei First Responder consistono nel garantire l'integrità della scena dell'incidente e fornire adeguato supporto e assistenza necessari alla raccolta delle prove.

- ***Investigator*** pianifica e gestisce la preservazione, acquisizione, valutazione, analisi, e reporting delle prove digitali.

- **Lead Investigator** ha il compito di assicurarsi che le attività svolte sulla scena dell'incidente siano eseguite nel giusto ordine e nei modi e nei tempi adeguati. Il Lead Investigator potrebbe essere responsabile del trattamento delle prove e della preparazione di report relativi al caso.

- **T*echnician*** compie le azioni sotto la direzione del Lead Investigator. È responsabile nell'identificazione e conservazione delle prove e deve documentare la scena dell'incidente. Dev'essere specializzato e dotato dell'equipaggiamento elettronico necessario per l'acquisizione delle immagini digitali residenti nella memoria del dispositivo preso in analisi. Più di un tecnico è coinvolto in una indagine, perché c'è la necessità di differenti abilità e conoscenze.

- ***Evidence Custodian*** ha il compito di proteggere tutte le prove raccolte che sono conservate in un deposito centrale. Cataloga le prove raccolte dai technician, assicurandosi che siano debitamente etichettate e messe in una custodia protettiva.

- ***Forensic Examiner*** è personale specializzato nella acquisizione delle informazioni a partire dalle immagini originali tramite equipaggiamento per l'estrazione e il recovering di dati digitali. Gli examiner rendono probative le informazioni contenute sul device. Potrebbero acquisire dati più elusivi usando equipaggiamento altamente specializzato, un intensivo reverse engineering o altri metodi appropriati che non sono accessibili ai Forensic Technician.

3.2 Principi Probatori

Come qualsiasi altro tipo di investigazione, sono stati proposti principi conformi al trattamento di prove digitali che, per propria natura, sono estremamente fragili, specialmente quelle trovate sui cellulari. Le linee guida dell'Association of Chief Police Officers inglese [ACPO], suggeriscono quattro principi fondamentali:

- ✓ Nessuna azione eseguita dagli investigatori deve compromettere i dati contenuti sul dispositivo digitale o sui dispositivi di memorizzazione.

- ✓ Ogni accesso ai dati originali deve essere fatta in maniera sequenziale in modo che sia possibile documentare ogni azione.

- ✓ Il processo di investigazione e le prove ottenute devono essere accuratamente documentate.

- ✓ Le persone che sono coinvolte nell'investigazione hanno la responsabilità di applicare le procedure menzionate in accordo alle leggi governative.

Il **Proposed Standards for the Exchange of Digital Evidence [IOCE]** suggerisce un insieme di principi simili per standardizzare la fase di recupero dati da dispositivi digitali:

- ✓ Dopo il recupero delle prove digitali, le azioni effettuate non dovrebbero compromettere i dati originali.

- ✓ Quando è necessario per una persona accedere alle prove digitali originali, quella persona deve essere competente nell'ambito forense.

- ✓ Tutte le attività di recupero, accesso, memorizzazione o trasferimento di prove digitali devono essere completamente documentate, preservate e accessibili.

- ✓ L'investigatore è responsabile per tutte le azioni prese rispetto alle prove digitali nel periodo in cui le prove stesse restano in suo possesso.

- ✓ Ogni agenzia che è responsabile del sequestro, dell'accesso, della memorizzazione o del trasferimento delle prove digitali è tenuta ad aderire a questi principi.

Il suddetto insieme di principi permette di essere sicuri della integrità e stabilire le responsabilità. Un opportuno trattamento delle prove digitali è sempre vitale per renderle valide durante un procedimento penale. Comunque, differenti standard potrebbero essere applicati a differenti tipi di investigazioni.

Il metodo di **Daubert [Oco04]**, 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.

La cosa da tenere sempre presente è che le procedure usate per acquisire le prove hanno effetto sull'ammissibilità delle prove stesse.

3.3 Modelli Procedurali

L' "Electronic Crime Scene Investigation", guida per i First Responders, prodotta dal dipartimento di giustizia degli Stati Uniti [DOJ01], offre le seguenti proposte:

- **Sicurezza e valutazione della Scena** – assicurarsi della sicurezza necessaria ad identificare e proteggere l'integrità delle potenziali prove.

- **Documentazione della Scena** – creare una documentazione permanente della scena, accuratamente ripresa da strumentazioni digitali.

- **Raccolta delle prove** – raccogliere le prove tradizionali e digitali in una maniera che si preservi la loro validità; prendendo le adeguate precauzioni quando si imballano, trasportano, e memorizzano le prove, mantenendo una catena di custodia.

Le ricerche condotte dalle Air Force degli U.S. [EDFM], propongono i seguenti passi quando abbiamo a che fare con una investigazione forense:

- **Identificazione** – riconoscere e determinare il tipo di incidente.

- **Preparazione** – preparare tool, tecniche e autorizzazioni.

- **Strategia di approccio** – massimizzare l'insieme di prove non contaminate, minimizzando l'impatto sulla vittima.

- **Preservazione** – isolare, rendere sicuro e preservare lo stato delle prove fisiche e digitali.

- **Raccolta** – registrare la scena fisica e duplicare le prove digitali.

- **Ispezione** – cercare le prove correlate al crimine sospettato.

- **Analisi** – determinare il significato, ricostruire i frammenti di dati ed estrarre conclusioni basate sulle prove trovate. La fase di analisi dovrebbe essere ripetuta finché non avvalora una qualche teoria.

- **Presentazione** – riassumere e fornire una spiegazione delle conclusioni.

- **Restituzione delle prove** – essere sicuri che le proprietà fisiche e digitali siano restituite al proprietario.

Sebbene questi punti siano stati sviluppati per i sistemi di computer, ognuno dei modelli procedurali citati sopra e i principi probatori discussi contengono importanti punti che dovrebbero essere considerati avendo a che fare con prove digitali contenute da telefoni cellulari.

I capitoli rimanenti di questa guida riguardano quattro tipiche aree: sequestro dei dispositivi, copia forense dei contenuti, recupero di elementi probatori a partire dalle copie, generazione di report relativi alle prove ottenute ed al procedimento usato.

4. PRESERVAZIONE

La preservazione delle prove è il processo di raccolta di materiale sospetto (es. dispositivi e memorie rimovibili) senza alterare i dati contenuti. Il fallimento della fase di preservazione delle prove nel loro stato originale potrebbe compromettere una intera investigazione.

In questo capitolo ne diamo una introduzione concentrandoci sui tratti relativi ai dispositivi mobili, quali la ricerca, il riconoscimento, la documentazione e la raccolta di prove digitali.

4.1 SICUREZZA E VALUTAZIONE DELLA SCENA

Prima di iniziare una investigazione occorre assicurarsi di avere le opportune autorizzazioni (es., avere un mandato o il consenso dal proprietario). Un'altra cosa importante è quella di considerare che, procedure non corrette o un improprio uso di un cellulare durante un sequestro, potrebbero causare perdita di dati digitali potenzialmente importanti. Inoltre, le misure applicate nelle tradizionali procedure forensi, come prendere in esame impronte digitali o tracce di DNA, potrebbero essere eseguite per stabilire una connessione tra un telefono cellulare e il suo utente o per altre ragioni. Se il dispositivo non è correttamente maneggiato, le prove fisiche possono essere facilmente contaminate o rese inutili. È essenziale stare attenti alle caratteristiche del dispositivo e dispositivi annessi (es, memorie) e avere una certa familiarità con gli accessori quali dispositivi di memorizzazione, cavi e adattatori di alimentazione. Le sorgenti probatorie di un cellulare includono il dispositivo, la (U)SIM e le memorie rimovibili, ma l'interesse ricade anche su eventuali periferiche, cavi, adattatori di alimentazione e altri eventuali accessori. Bisognerebbe, inoltre, verificare la presenza di altre prove nell'area circostante e nelle stanze dove è stato trovato il dispositivo. Per evitare iterazioni non volute con il dispositivo bisognerebbe spegnere le interfacce wireless come Bluetooth e WiFi. Le periferiche associate al cellulare, come memorie rimovibili, (U)SIM o perfino personal computer sincronizzati con esso, potrebbero contenere più prove del cellulare in se.

4.2 DOCUMENTAZIONE DELLA SCENA

Le prove devono essere accuratamente documentate e identificate. Prove non elettroniche come fatture, manuali e materiali di imballaggio potrebbero essere utili informazioni per valutare le capacità del dispositivo, la rete usata, una sua descrizione e codici di sblocco come il PIN. Il processo di etichettamento dovrebbe comprendere il numero del caso, una breve descrizione, un protocolaggio e la data e l'ora in cui la prova è stata raccolta. Potrebbe essere di aiuto fotografare la scena del crimine, in congiunzione con la documentazione dello stato di ogni dispositivo digitale (eventuali personal computer potrebbero contenere utili dati che non sono stati sincronizzati con il cellulare del proprietario).

Bisogna evitare di toccare o contaminare il telefono e l'ambiente dove è stato trovato quando si sta fotografando il dispositivo e la scena del crimine. 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. Si dovrebbero notare altre

caratteristiche come l'attività del LED (es. intermittenze), condizioni fisiche, connettività, etc. Sulla scena, ci dovrebbe essere un individuo incaricato di custodirne l'integrità, affiancato da un partner responsabile di documentarne i contenuti. Azioni effettuate per vedere dati sul dispositivo possono compromettere il valore probatorio. Per esempio, lanciare una applicazione su uno smart phone può sovrascrivere parte della memoria. Inoltre, questa azione potrebbe attivare un Trojan o causare accidentalmente effetti inaspettati.

La catena di eventi relativa alla procedura di custodia deve essere documentata durante tutto il ciclo di vita del caso, non solo per protegge l'integrità delle prove, ma anche per renderne difficile la contaminazione da parte di terzi. La documentazione 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?

4.3 Raccolta delle prove

Il Mobile Phone Forensics Sub-Group dell' Interpol European Working Party sull'IT Crime ha identificato i principi da applicare per trarre prove utili da dispositivi mobili sequestrati. Alcuni punti chiave vengono riassunti qui di seguito.

Isolare il cellulare da altri dispositivi usati per la sincronizzazione dei dati è importante al fine di evitarne la contaminazione. Se il device viene trovato connesso ad un computer via cavo, togliere il cavo potrebbe provocare la cancellazione o sovrascrittura dei dati trasmessi. Le Memory card, le (U)SIMs e gli altri hardware residenti nel telefono non dovrebbero essere rimosse. È importante anche sequestrare il computer a cui è stato connesso il telefono poiché sul suo hard disk potrebbero trovarsi dati sincronizzati che erano presenti sul cellulare. Tutto l'hardware associato al telefono dovrebbe essere confiscato assieme ai manuali, le confezioni e il software. Se il telefono è acceso quando viene trovato, bisogna isolarlo dalla rete per evitare che nuovo traffico sovrascriva i dati esistenti. Ci potrebbe essere anche il rischio che vengano sfruttate delle vulnerabilità. Per esempio, è stato dimostrato che mandando un messaggio malformato ad un Nokia 6210 rende il telefono completamente inutilizzabile, proprio come succede quando inviamo un pacchetto ICMP malformato detto "ping of death" a sistemi Windows di vecchia generazione.

Per evitare questo genere di problemi è possibile spegnere il dispositivo nel momento del sequestro o metterlo in una borsa che lo isola dalla rete. In alternativa, se il dispositivo ha la funzione "Airplane Mode", si potrebbe abilitare questa impostazione.

Ognuno di questi metodi tuttavia, presenta alcuni problemi:

- 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. Questo potrebbe complicare l'acquisizione e ritardare l'analisi delle prove.

- Tenendo il telefono acceso, ma isolato dalla rete radio, 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. D'altra parte, i contenitori, certamente attenuano il segnale radio, ma non necessariamente lo eliminano, con la eventuale possibilità di connessione ad una Base Station, nelle immediate vicinanze.

- Abilitare l'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.

Se i dati dell'utente risiedono in una memoria volatile dipendente da alimentazione, l'esaurimento della batteria può comportare problemi come la perdita dei dati stessi. Prima di raccogliere un telefono, dobbiamo considerare lo stato dell'alimentazione. Per esempio, il dispositivo deve essere completamente carico. Questa condizione risulta un problema quando vogliamo isolare il dispositivo in una borsa che isola dalla rete radio e quindi, dovremmo dotare il contenitore di un sistema di alimentazione portatile che non faccia esaurire la batteria del telefono. Se non può essere generata abbastanza alimentazione, si dovrebbe considerare lo spegnimento del cellulare per preservare lo stato della batteria, documentando lo stato corrente del dispositivo e annotando l'ora e la data dello spegnimento. Perfino quando il telefono è isolato, i dati contenuti su di esso potrebbero avere dei cambiamenti non desiderati, dovuti ad esempio, all'esecuzione di uno script schedulato che cancella i vecchi dati. Alcuni telefoni si spengono se il livello della batteria scende al di sotto di un livello stabilito, comportando la perdita di dati nella memoria voltatile, in contrasto con il nostro scopo di tenere il cellulare acceso. Di contro, va osservato che nella maggior parte dei casi, i sistemi di protezione come autenticazione e crittografia dei dati, non sono molto utilizzati. Se non è disponibile un modo per alimentare il dispositivo e si decide di spegnerlo per preservare il contenuto della memoria, il rischio di incontrare un meccanismo di protezione quando lo riaccendiamo, è abbastanza basso. Per questa ragione, spesso, si tende a raccomandare lo spegnimento. Inoltre, alcuni smart phone, usano batterie ricaricabili sostituibili; una piccola carica contenuta nel dispositivo può consentirne la sostituzione senza perdita di dati nella memoria volatile, a patto di sostituire la batteria velocemente.

Il tempo registrato dal telefono può essere impostato in maniera diversa da quello della rete. È utile annotare anche il tempo mostrato al momento dell'accensione del dispositivo e confrontarlo con un tempo di riferimento per notare qualsiasi inconsistenza.

Nella fase di imballaggio, dobbiamo assicurarci di aver registrato l'azienda manifatturiera e il modello del dispositivo confiscato, nonché le sue condizioni. Queste informazioni di solito appaiono nella parte anteriore del telefono sotto la

batteria. Ad ogni modo, non dovremmo rimuovere la batteria per leggerle se il telefono acceso.

Certi tipi di modifiche al software potrebbero influire sul modo in cui deve essere trattato il dispositivo in fase di investigazione. Di seguito ci sono una lista di esempi di classi di modifiche da considerare:

- **Aumento della sicurezza** – organizzazioni e individui potrebbero cambiare i meccanismi di sicurezza sui loro dispositivi. Sono disponibili, per gli smart phone, una varietà di login visuali, biometrici, basati su token, da essere usati per sostituire o rafforzare i meccanismi basati su password. Una interazione sbagliata con il meccanismo di autenticazione potrebbe comportare il blocco del dispositivo e perfino la cancellazione di ogni suo contenuto. Questo riguarda in particolar modo quei meccanismi di autenticazione che usano token la cui presenza viene costantemente monitorata.

- **Programmi maliziosi** – un dispositivo mobile potrebbe contenere virus o software malizioso. Tali malware potrebbero diffondersi tramite interfacce wireless o infrarossi sostituendo utilities o funzioni comuni col fine di alterare o danneggiare i dati presenti sul telefono. Esistono anche alcuni programmi Trojan-bearing che possono essere attivati o disattivati da parametri di input, come combinazioni particolari di tasti. Alcune informazioni più precise possono essere trovate al seguente indirizzo: http://www.eweek.com/article2/0,1895,1750109,00.asp

- **Rimappatura della tastiera** – La mappatura hardware della tastiera può essere modificata per eseguire una diversa funzione rispetto a quella di default. Un tasto premuto o una combinazione di essi potrebbe mettere in esecuzione un programma arbitrario.

4.4 Imballaggio, Trasporto e memorizzazione delle prove

Come abbiamo già accennato, una volta che il dispositivo è pronto per essere sequestrato, dovrebbe essere messo in una borsa etichettata che lo isola dalla rete. L'etichetta dovrebbe contenere la data del sequestro ed il dispositivo dovrebbe essere posto in modo da evitare che qualche tasto venga premuto accidentalmente. Esistono contenitori rigidi costruiti e suggeriti per questo uso. Borse isolate dalla frequenza radio sono disponibili per attenuare il segnale del dispositivo e dovrebbero essere usate quando si abbia la necessità di tenere il telefono acceso. Un alimentatore esterno può essere connesso e messo nella borsa con il dispositivo per tenere il livello di alimentazione alto per tutta la durata del viaggio. I dispositivi mobili sono fragili e facilmente danneggiabili. Quando un dispositivo viene trasportato, dovrebbe essere maneggiato con cura ed adeguatamente protetto da shock, rotture e temperature estreme ed, in fine, conservato in un'area sicura con accesso controllato.

Si consulti il sito Web http://www.forensicts.co.uk/fts-packaging.asp per maggiori approfondimenti sui diversi tipi di imballaggio.

5. ACQUISIZIONE

In questo capitolo discutiamo l'acquisizione, ovvero, il processo di estrapolazione delle informazioni da un dispositivo digitale. Assumiamo di avere disponibili in un laboratorio forense, la strumentazione necessaria ed il dispositivo da analizzare.

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 dispositivo. Soltanto pochi dei mobile forensic tool (MFT, da questo momento in poi MFT o tool avranno lo stesso significato) 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 presenti sul mercato. Dal tipo di telefono, perciò, dipende la scelta di quali tool usare per l'investigazione.

5.1 ISOLAMENTO RADIO

Il laboratorio in cui si esegue l'acquisizione dovrebbe essere isolato dalle frequenze radio. Esistono numerose tecniche per isolare il telefono mobile dalla torretta cellulare. 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, come già citato, riduce significativamente la durata di vita della batteria, pertanto, il dispositivo dovrebbe essere completamente caricato prima di essere preso in esame e per questo scopo occorre dotarsi di una fonte di energia fissa o portatile.

- **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. Un'altra tecnica utilizzabile consiste nell'ingannare il dispositivo emulando un segnale di "no service". Tali tecniche tuttavia, possono interferire e compromettere anche altre comunicazioni esterne al laboratorio; per questo motivo molti paesi le considerano illegali.

- **Uso di una area di lavoro protetta** – rendere sicura una intera area può essere molto costoso, ma è un modo efficacie per condurre l'investigazione in modo sicuro in un posto fisso. Una "Faraday tent" (tenda Faraday) è un modo alternativo e più economico e in più, permette la portabilità. 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. Questa tecnica permette di condurre l'investigazione in maniera sicura in qualunque locazione.

5.2 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. Occorre prestare attenzione poiché potrebbero essere state apportate delle modifiche. L'alterazione del dispositivo può andare dalla rimozione dell'etichetta dell'azienda produttrice alla modifica o sostituzione del sistema operativo e/o delle applicazioni, facendo assumere al dispositivo caratteristiche differenti da quelle che ci si sarebbe aspettato. Per esempio, la rimozione o sostituzione dello splash screen è una procedura diffusamente spiegata nei forum di cellulari. Il nome dell'azienda produttrice, la famiglia del sistema operativo e il nome del service provider che spesso appaiono sul display, potrebbero essere stati rimossi. Sebbene tali informazioni siano usualmente stampate su etichette presenti nella cavità della batteria (es. Marca, modello, IMEI o ESN), rimuoverla, può compromettere lo stato del dispositivo perfino quando questo è spento, particolarmente per quanto riguarda la perdita di dati dalla memoria volatile. Inoltre, se il telefono è acceso, la rimozione della batteria e la riaccensione, potrebbero causare l'attivazione di un qualche meccanismo di autenticazione. Ad ogni modo conoscere la marca e il modello può essere di notevole aiuto durante la fase di analisi, se non altro, aiuta a limitare il numero di potenziali service provider, differenziando il tipo di rete supportato dal dispositivo (es. GSM, non-GSM).

Di seguito elenchiamo una serie di metodi utili per identificare il dispositivo:

- **Caratteristiche fisiche del dispositivo** – il modello e il produttore del telefono può essere ricavato analizzando le caratteristiche fisiche del dispositivo (es. larghezza, dimensione e forma). In particolare, se dotato di un design non comune. Sul Web è possibile trovare database interrogabili a partire dagli attributi fisici, capaci di identificare un particolare dispositivo per il quale possono poi essere fornite specifiche più dettagliate [WWW].

- **Interfacce del dispositivo** – l'alimentatore è, tipicamente, specifico di un unico produttore e potrebbe servire ad identificare la classe del dispositivo, analogamente a quanto accade per i connettori di collegamento a personal computer.

- **Etichette presenti sul dispositivo** – per i telefoni spenti, le informazioni possono essere ottenute dalla cavità della batteria. L'etichetta del produttore spesso svela anche la marca e il numero del modello del telefono ed anche identificatori univoci come il Federal Communications Commission Identification Number (FCC ID) ed il codice identificativo dell'apparecchio (IMEI o ESN).

  Per I dispositivi GSM, la (U)SIM è generalmente locata sotto la batteria ed è tipicamente etichettata da un identificativo univoco chiamato Integrated Circuit Card Identification (ICCID). Per I dispositivi GSM e UMTS in modalità accesa, il codice International Mobile Equipment Identifier (IMEI) può essere ottenuto digitando sulla tastiera *#06#. Codici simili esistono per ottenere anche l'Electronic Serial Number (ESN) da telefonini basati su tecnologia CDMA. Ci sono vari siti Internet dove vengono offerte interfacce a database che dal codice identificativo forniscono informazioni sul dispositivo.

- Il codice IMEI è un numero di 15 cifre che indica produttore, modello, tipo e paese di approvazione per dispositivi GSM. Le prime 8 cifre del codice IMEI, sono conosciute come Type Allocation Code (TAC) e danno informazioni sul modello e l'origine. La parte restante del codice IMEI è specifica del fornitore del dispositivo, con una cifra di controllo alla fine. h

  Il seguente sito Web offre un servizio di analisi del codice IMEI e permette di ricavare informazioni sul dispositivo: http://www.numberingplans.com/?page=analysis&sub=imeinr

- L' ESN è un identificatore univoco di 32 bit memorizzato dal produttore su di un chip del dispositivo mobile. I primi 8-14 bit identificano il fornitore, i restanti coincidono col serial number. Su alcuni telefoni, attraverso un codice digitato da tastiera, si può accedere ad un menu nascosto che attiva la modalità "test mode". Tramite il codice ESN, è possibile ricavare altre utili informazioni come il numero del dispositivo. I codici dei fornitori possono essere verificati on-line sul sito web della Telecommunications Industry Association, all'indirizzo: http://www.tiaonline.org/standards/resources/esn/codes.cfm

- Il codice ICCID della (U)SIM può essere più lungo di 20 cifre. Consiste di un identificatore che fa da prefisso per l'industria (89 per le telecomunicazioni), seguito dal codice del paese, da un identificativo del produttore e da un numero di account di identificazione. Se l' ICCID non dovesse apparire sulla (U)SIM, può essere sempre ottenuto tramite un tool di acquisizione da (U)SIM. Il sito web del piano di numerazione GSM, all'indirizzo: http://www.numberingplans.com/?page=analysis&sub=simnr supporta le interrogazioni ICCID.

- I primi 3 caratteri del FCC ID sono il codice della compagnia; i successivi 14 sono il codice del prodotto. L' FCC fornisce un database e un servizio di lookup che può essere usato per identificare il fornitore di un dispositivo e recuperare informazioni sul telefono, incluse foto, manuale utente e test di radio frequenza (http://www.fcc.gov/oet/fccid/).

- **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 inserendo il codice dell'area utente, un prefisso di tre cifre e la settima cifra del numero del telefono. Il sito web dell'operatore di rete, tipicamente contiene una lista dei telefoni che supporta. Poiché i numeri di telefono possono essere portati da un operatore all'altro, in molte situazioni c'è bisogno di informazioni più aggiornate. Negli Stati Uniti e in Canada, il Number Portability Administration Center (NPAC) fornisce un sistema automatico per determinare il service provider correntemente assegnato ad un numero (http://www.fonefinder.net/).

5.3 SELEZIONE DEL TOOL

Una volta che marca e modello del telefono sono note, possono essere recuperati i relativi manuali e studiati. Il sito web del produttore è un buon posto per iniziare. Digitando il modello nella pagina di ricerca di Google o di un altro motore di ricerca, possiamo scoprire altre informazioni sul dispositivo. Come già discusso precedentemente, dal tipo di dispositivo dipende la scelta del tool forense adatto. In generale, dovrebbero essere valutati i seguenti 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

Altri fattori che incidono sulla scelta dei tool software sono le considerazioni di Daubert menzionate precedentemente ed in particolare i seguenti punti:

- **Qualità** – supporto tecnico, affidabilità e possibilità di upgrade di versioni
- **Capacità** – un insieme di feature supportate, performance e ricchezza di feature che considerano la flessibilità e la costumizzazione
- **Fattibilità** – costo contro benefici nella produttività

5.4 CONSIDERAZIONI SULLE MEMORIE

Un cellulare contiene vari tipi di memoria volatile e non volatile in cui possono risiedere diverse categorie di dati generici: codice del sistema operativo, incluso il kernel, driver dei device e librerie di sistema; memoria volatile per l'esecuzione del sistema operativo e delle applicazioni e memoria utente per memorizzare testo, immagini, audio, video e altri tipi di file, incluse le applicazioni dati PIM.

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

Il tipo di memoria in cui risiede ogni categoria di dati e la struttura impiegata per gestirla, varia da produttore a produttore e spesso è legata al tipo di sistema operativo usato.

La Figura 4 mostra una strutturazione nella quale il sistema operativo e i file dell'utente risiedono in una memoria non volatile (Flash ROM o micro hard drive). La memoria volatile invece, viene usata per la memorizzazione dinamica e i suoi contenuti vanno persi quando l'alimentazione viene a mancare.

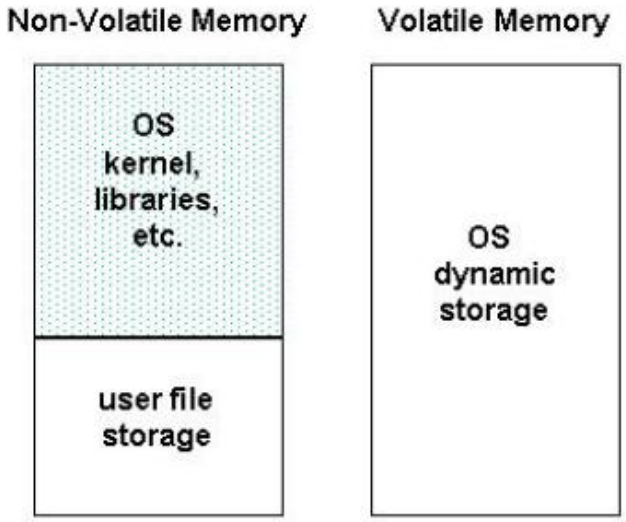

FIGURA 4 ASSEGNAMENTO DELLA MEMORIA

Una comune alternativa di strutturazione della memoria, usata principalmente negli smart phones, è mostrata nella Figura 5, dove, 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 o altri file di cui è stato fatto il backup dalla memoria volatile dell'utente. L'esaurimento completo dell'alimentazione del telefono comporta la cancellazione di tutto il contenuto della memoria volatile, mentre quella non volatile non è affetta da questo inconveniente.

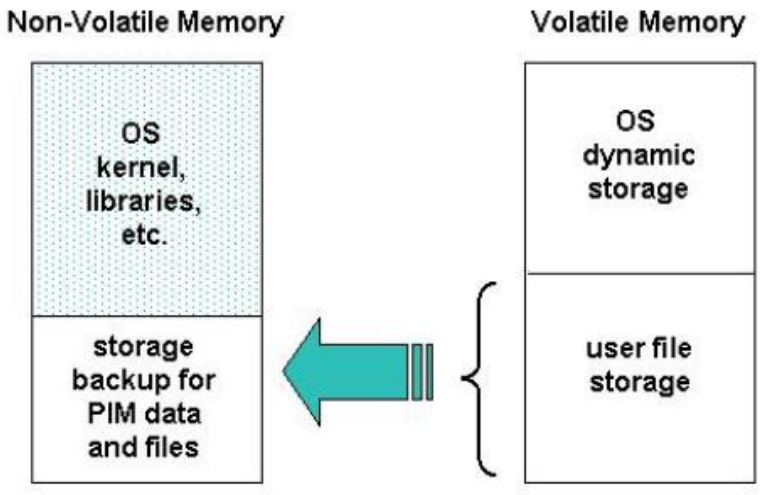

FIGURA 5 : ASSEGNAMENTO ALTERNATIVO DELLA MEMORIA

Anche la (U)SIM similmente ad un cellulare è dotata di memoria volatile e di memoria non volatile ed entrambe, possono contenere lo stesso insieme generico di categorie di dati. In effetti, possiamo considerare la SIM come un co-processore che si interfaccia al telefono e prende l'alimentazione da esso. Il file system risiede nella

memoria non volatile organizzata in una struttura gerarchica ad albero simile a quella di Figura 6, composta da tre tipi di elementi: la radice del file system (MF), alcune directory subordinate (DF) e file che contengono dati elementari (EF). I file nelle directory DFGSM e DFDCS1800 contengono principalmente informazioni relative alla rete. I file in DFTELECOM contengono informazioni relative ai servizi attivi del gestore.

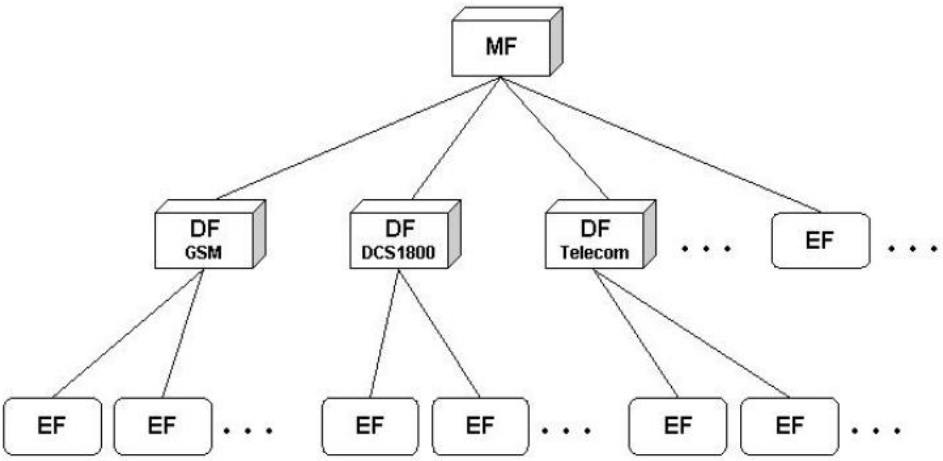

FIGURA 6: FILE SYSTEM DELLA SIM

I file elementari possono avere un'importanza notevole nella ricerca di prove digitali. Copie degli stessi dati possono essere trovate sia nella SIM che nella memoria del dispositivo mobile. Di seguito elenchiamo alcune informazioni ricavabili da tali file:

- 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, incluse sia gli Short Message Service (SMS) messaggi testuali che gli Enhanced Messaging Service (EMS) semplici messaggi multimediali.
- Informazione di locazione, incluso Location Area Information (LAI) per la comunicazione vocale e Routing Area Information (RAI) per le comunicazioni dati

In generale, oltre ai file standard definiti dalle specifiche GSM, una (U)SIM potrebbe contenere anche dati introdotti dall'operatore di rete .

5.5 DISPOSITIVI NON OSTRUITI

Un dispositivo non sprovvisto di (U)SIM e che non richieda forme di autenticazione per l'accesso ai contenuti, viene detto **non ostruito**. Fortunatamente, molti dei dispositivi sequestrati nelle investigazioni ricadono in questa categoria.

Prove potenziali, ed in particolare i dati utente, potrebbero risiedere sia nella memoria volatile che in quella non volatile. Per preservarne l'integrità, gli esaminatori dovrebbero maneggiare i dispositivi il meno possibile. Per questo motivo è raccomandabile creare una copia forense detta **master copy**. Attraverso questa, vengono poi create altre copie che serviranno per l'analisi e l'esamina delle prove . Una crittografia one-way hash (es. SHA1) dovrebbe essere eseguita per avere la certezza che le immagini della master copy siano identiche.

5.5.1 ACQUISIZIONE DA DISPOSITIVI MOBILE

Spesso i telefoni sono sottomessi ad analisi di laboratorio solo per ottenere specifiche informazioni richieste per la fase di recupero dati, come immagini e log delle chiamate. Per l'acquisizione, deve essere stabilita una connessione tra il dispositivo e la workstation forense. Prima di procedere però, sarebbe opportuno documentare la versione del tool che utilizzato e le eventuali patch applicate. Una volta che la connessione è stata stabilita, la software suite forense può procedere all'acquisizione dei dati dal dispositivo. I passi necessari consistono nel selezionare una connessione, identificare il dispositivo da cui fare l'acquisizione, identificare i dati che devono essere recuperati ed analizzarli.

Sebbene da un punto di vista teorico non si dovrebbero apportare modificare ai dati, durante l'acquisizione logica reale, i MFT moderni, richiedono che il dispositivo sia acceso. Alcune aree della memoria subiranno necessariamente delle modifiche, si pensi ad esempio alla memoria utilizzata per le comuni attività di servizio dell'apparecchio. L'obiettivo principale durante l'acquisizione dunque, è quello di influire il meno possibile sui contenuti avendo una buona conoscenza di quello che realmente accade, in modo da poter documentare tutto il processo.

Eventuali attributi di data e ora relativi ai dati acquisiti, rappresentano un'importante parte delle informazioni. Poiché tali valori possono essere impostati manualmente da parte dell'utente, se il telefono viene trovato acceso al momento del sequestro, sarebbe opportuno documentare la variazione tra la la data e l'ora corrente e quella segnata dal dispositivo. In alternativa, queste informazioni devono essere immediatamente registrate quanto il telefono viene acceso per la prima volta in laboratorio. Si osservi che, azioni fatte durante l'acquisizione, come la rimozione della batteria potrebbero avere effetti sulle impostazioni di data e ora del dispositivo.

Diversamente dai personal computer o dalle reti di server, i telefoni non sono dotati di un hard disk, ma fanno affidamento su memorie a semiconduttore. Esistono software specializzati per eseguire l'acquisizione logica dei dati PIM e, per alcuni cellulari, possono anche produrre una immagine fisica della memoria. Se il telefono è dotato di uno slot per le memory card, può essere effettuata la relativa acquisizione diretta dopo aver acquisito con successo i dati contenuti sul telefono.

Lo specialista forense dovrebbe sempre confermare che il contenuto del dispositivo sia stato catturato correttamente. Un tool ad esempio, potrebbe fallire il suo compito senza dare nessuna notifica di errore o soffrire di incompatibilità con alcuni tipi di dispositivi. Così, dove possibile, è consigliabile avere più tool disponibili nel caso che uno fallisse.

Spesso, i dati visibili sul telefono usando i menù disponibili possono non essere catturati attraverso acquisizione logica. Per esempio, i messaggi contenuti nelle bozze e archiviati non sempre vengono recuperati dai MFT. Quando si esamina manualmente il contenuto del telefono passando per il relativo menu, si devono filmare tutte le azioni eseguite, avendo la massima cura nel preservare l'integrità del dispositivo. I dati cancellati non possono essere recuperati né tramite acquisizione logica, né tramite accesso manuale. In mancanza di un tool software capace di eseguire una acquisizione fisica, è possibile sfruttare tecniche hardware. Due di queste, comunemente usate per le memorie non volatili, sono: l'acquisizione attraverso un'interfaccia standardizzata chiamata Joint Test Action Group (JTAG) test interface, se supportata dal dispositivo, e acquisizione diretta della memoria rimossa dal dispositivo. Questi tipi di tecniche saranno descritte successivamente.

5.5.2 Considerazione sui telefoni GSM

I telefoni GSM, a differenza di quelli CDMA, sono leggermente più complessi da trattare a causa della presenza di un identity module (SIM) i cui dati dovrebbero essere acquisiti insieme al telefono o separatamente.

Se il telefono è attivo, una acquisizione del suo contenuto insieme a quello della SIM dovrebbe essere effettuata prima di passare all'acquisizione diretta dei dati sulla card. Ad esempio, l'acquisizione diretta recupera i messaggi cancellati presenti su una SIM, mentre l'acquisizione indiretta non lo fa. La SIM deve essere rimossa dal telefono e inserita nell'appropriato lettore per l'accesso diretto. Una delle ragioni che giustifica questa sequenza di azioni è che nella rimozione della SIM, tipicamente posta sotto la batteria, ci potrebbe essere la perdita dei dati nella memoria non volatile. In più, il fatto che il dispositivo è stato tenuto attivo quando è stato sequestrato potrebbe indicare la presenza di sistemi di autenticazione o altri meccanismi di sicurezza attivabili automaticamente se l'alimentazione viene a mancare. Una problematica conosciuta che sorge nell'ambito forense è che lo stato riportato dei messaggi di testo SMS non letti è inconsistente tra ogni acquisizione (U)SIM – la prima volta viene dichiarato come non letto, mentre la seconda volta come letto. Un modo per evitare questo tipo di inconsistenze è di omettere la selezione di recovery degli SMS nella (U)SIM quando effettuiamo l'acquisizione combinata, ovviamente se il tool permette tale opzione.

Se il telefono è inattivo, il contenuto della (U)SIM potrebbe essere acquisito indipendentemente dal contenuto del dispositivo. L'acquisizione dati dalla (U)SIM dovrebbe essere fatta direttamente da un lettore (U)SIM. Successivamente, si può provare l'acquisizione dall'handset senza la scheda. Purtroppo, non tutti i telefoni la supportano. Se ci si trova in questo caso occorrerà reinserirla e fare un altro tentativo. Eseguendo acquisizioni indipendenti e separate permette di evitare che qualche sistema forense correlato legga in maniera indiretta i dati della (U)SIM.

5.5.3 (U)SIMs

Per acquisire i dati dalla (U)SIM, si deve stabilire una connessione tra la postazione forense e il dispositivo, usando un lettore. Una volta che la connessione è stata stabilita, il software forense può procedere all'acquisizione. La cattura diretta di una immagine della (U)SIM è solitamente impedita da meccanismi di protezione incorporati nel modulo. I MFT quindi, usano direttive chiamate Application Protocol Data Units (APDU) che estraggono i dati logicamente, senza apportare modifiche di alcun genere. Il protocollo APDU si basa su di un semplice scambio comando-risposta. Ogni elemento del file system definito nello standard GSM ha un identificativo numerico univoco, che può essere usato per navigare il file system ed eseguire alcune operazioni, come la lettura dei contenuti.

Poiché le (U)SIM sono dispositivi altamente standardizzati, esistono pochi problemi riguardo all'acquisizione logica.

5.6 Dispositivi ostruiti

Quei dispositivi che necessitano di una corretta autenticazione affinché possano essere accesi vengono detti **ostruiti**. Le operazioni per poter bypassare o superare i meccanismi di sicurezza devono esser fatti con cura da personale esperto e adeguatamente addestrato, dato che basta una semplice azione per poter causare il blocco del cellulare sequestrato o perdere delle informazioni. È consigliabile effettuare degli esperimenti su dispositivi di test che sono dello stesso modello e presentano lo stesso software del cellulare sequestrato.

Esistono tre tipici approcci per recuperare dati dai telefoni ostruiti: metodi investigativi, metodi che agiscono sul software e metodi che agiscono sull' hardware.

5.6.1 Metodi investigativi

I metodi investigativi più ovvi da usare in queste circostanze sono i seguenti:

- Chiedere al sospettato se il dispositivo è in qualche modo protetto (PIN, password, ecc).
- Esaminare il materiale sequestrato. Password o PIN possono essere scritti su pezzi di carta rinvenuti vicino al dispositivo sequestrato oppure vicino al computer utilizzato insieme al dispositivo o ancora tra gli effetti personali del sospettato stesso. Nella confezione del dispositivo inoltre, è possibile trovare il codice PUK utile per resettare il PIN.
- Provare manualmente con degli input ricorrenti stando attenti a non bloccare definitivamente il telefono. Può accadere che un'utente utilizzi una sequenza molto semplice da ricordare come (es. 1234, 0000).

- Chiedere al fornitore del servizio. Se un telefono GSM è protetto da un PIN, l'identificatore della SIM può servire per ottenere il PUK dal fornitore del servizio. Spesso viene fornito un servizio che consente di ottenere il PUK digitando il numero di telefono via web.

- Scoprire possibili settaggi insicuri. Alcuni modelli di cellulare permettono l'accesso sfruttando alcuni errori di configurazione comuni. Per esempio, i cellulari Motorola hanno un tipo di accesso al dispositivo a due livelli; un blocco al telefono necessario per poter accedere al dispositivo e un codice di sicurezza necessario per resettare il codice di blocco. Dato che il codice di sicurezza di solito non viene cambiato dall'utente, si può accedere al dispositivo digitando il codice di sicurezza di default.

5.6.2 METODI CHE AGISCONO SUL SOFTWARE

Di seguito elenchiamo alcuni metodi software correntemente utilizzati:

- Exploit dovuti alla debolezza del meccanismo di autenticazione. Esempi di debolezze possono riguardare gli schemi di protezione delle password, come quello di Palm OS che offuscava le password usando un algoritmo reversibile e pertanto, utilizzando una apposita utility era possibile recuperarle facilmente. Il protocollo ActiveSync invece, prevedeva infiniti tentativi di autenticazione senza andare incontro ad un blocco del dispositivo, permettendo così un attacco con dizionari di password comunemente usate. Alcuni dispositivi inoltre, avevano una master password inclusa nel meccanismo di autenticazione attraverso la quale bypassare il blocco del telefono impostato dall'utente. Per alcuni dispositivi tale master password può essere calcolata direttamente utilizzando l'identificatore del dispositivo. Se non si conosce il PIN o la (U)SIM è stata rimossa dal dispositivo, a volte è possibile creare una (U)SIM che emuli quella originale. Bisogna prestare attenzione perché i dispositivi mantengono in memoria i dati della (U)SIM, se questa viene sostituita, il cellulare cancellerà i dati precedentemente acquisiti oppure li sovrascriverà con i dati della nuova (U)SIM. Pertanto, bisogna creare una (U)SIM che mantenga alcune informazioni dell'originale, come ad esempio lo stesso ICCID e IMSI, in modo che il cellulare non si accorga della sostituzione.

- Guadagnare l'accesso attraverso blackdoor. I produttori a volte costruiscono delle blackdoor nel loro software in modo da poter facilitare il lavoro di testing. Alcuni tool sono in grado di sfruttare i protocolli diagnostici o di debbuging per acquisire dati dalla memoria che potrebbe anche contenere informazioni utili per eseguire l'autenticazione. Inoltre, alcuni dispositivi hanno un boot loader che, attraverso combinazioni di tasti o via porta seriale, può fornire una copia della memoria o della memory card.

- Esplorare vulnerabilità conosciute del software. In particolar modo quelle che riguardano il protocollo standard d'interfaccia che se

sfruttate possono bypassare l'autenticazione. Ad esempio, accedere al dispositivo sfruttando un servizio di rete configurato male, una falla nello standard del protocollo di rete o un errore nella sua implementazione (es. buffer overflow). Possibili interfacce utilizzabili per l' esplorazione sono USB, IrDA, Bluetooth, WiFi e risorse GSM/GPRS.

5.6.3 METODI CHE AGISCONO SULL'HARDWARE

Oltre ai metodi che agiscono sul software, esistono diversi metodi che agiscono sull'hardware e che, solitamente, sono specializzati per funzionare solo su alcuni tipi di dispositivi ed in genere procedono adottando i seguenti metodi:

- Guadagnare l'accesso attraverso backdoor. Alcuni cellulari hanno attivi sulla circuiteria dei test point hardware che possono essere usati per sondare il dispositivo. Esiste anche un'interfaccia standard denominata JTAG utilizzata da molti produttori per effettuare test per processori, memorie e altri chip contenuti sul dispositivo. Un esaminatore può comunicare con un componente JTAG utilizzando un software ed un controller hardware appropriati oppure attraverso un dispositivo programmatore che sonda specifici test point. JTAG offre uno strumento utile per poter recuperare informazioni da dispositivi bloccati o che hanno subito dei lievi danneggiamenti.

- Esaminare direttamente i chip di memoria del telefono. L'istituto forense dei Paesi Bassi ha sviluppato un tool generico per esaminare una vasto gamma di chip di memoria. Una volta che ci si è connessi fisicamente al chip di memoria attraverso un memory clip, il tool è in grado leggere e salvare i dati acquisiti. In alternativa si può smontare il chip di memoria dal dispositivo e usare un lettore di memorie per accedere ai dati.

- Cercare ed esplorare le vulnerabilità. Di solito si agisce attraverso reverse engineering. Occorre recuperare il codice del sistema operativo dalla ROM di un cellulare identico a quello sotto esame, quindi analizzarlo in modo da capirne la struttura e le tecniche d'accesso alle risorse hardware. Attraverso questo lavoro è possibile scoprire delle vulnerabilità che possono essere sistematicamente testate al fine di trovare degli exploit utili. Per esempio, per il meccanismo di autenticazione mediante password, è possibile usare una memory injection per sovrascrivere la password con un valore conosciuto o sostituire il programma di autenticazione con una versione che autentifica sempre con successo.

- Ricavare informazioni dal monitoraggio delle caratteristiche fisiche del dispositivo. Esistono tecniche per il monitoraggio del consumo di energia o altre caratteristiche che sono state sfruttate per ottenere password e PIN. In alcuni dispositivi ad esempio, è possibile scoprire l'area di memoria in cui si trova la password, per cui, man mano che vengono inseriti i caratteri, monitorando i dati e il bus

indirizzi di queste locazioni di memoria è possibile ricavare il valore della password carattere per carattere. Ancora, è possibile usare il DPA (Differential Power Analysis), una tecnica di attacco capace di sniffare password e chiavi segrete da smart card o da altri device crittografici, a partire dalle fluttuazioni nel consumo di corrente elettrica dei microprocessori contenuti nei lettori hardware.

- Utilizzare strumenti automatici di attacco a forza bruta, applicabile quando il meccanismo di autenticazione permette un numero infinito di tentativi. Ovviamente un attacco del genere diventa fattibile con un dispositivo automatico che inserisce password.

5.7 Dispositivi di memorizzazione associati

Di solito un dispositivo mobile viene utilizzato in combinazione ad altri dispositivi come le memory card e i normali personal computer. Quest'ultimi vengono usati soprattutto per le funzioni di sincronizzazione dei contenuti e sono anche chiamati dispositivi sincronizzati. Le memory card (es. SD, MMC), fungono da memorie ausiliarie ed hanno dimensioni talmente contenute da essere facilmente perse o nascoste.

5.7.1 Dispositivi sincronizzati

La sincronizzazione delle informazioni può avvenire sia a livello di record o livello di file. Quando viene fatta a livello di file, qualsiasi discrepanza tra una vecchia sincronizzazione a una più nuova viene annullata. Occasionalmente un intervento manuale può essere necessario se le due versioni vengono modificate indipendentemente da quando c'è stata l'ultima sincronizzazione dei dati. La sincronizzazione a livello di record è simile a quella a livello di file, ma con una maggiore granularità; solo le parti out-of-date del file vengono modificate. Lo scambio di dati tra cellulare e pc avviene in entrambe le direzioni. Per questa ragione, dati significativi possono essere rinvenuti su entrambi i dispositivi. Tra l'altro, poiché le divergenze tra i due tendono a crescere velocemente nel tempo, alcune informazioni importanti potrebbero trovarsi sull'uno piuttosto che sull'altro e viceversa.

5.7.2 Memory Card

Alcuni MFT sono in grado di acquisire il contenuto delle memory card che vengono utilizzate per memorizzare dati come gli SMS o altri tipi di media. Se l'acquisizione è logica, allora non sarà possibile recuperare i dati cancellati, ma solo quelli ancora presenti sulla memoria. Fortunatamente alcuni tipi di memory card possono essere trattati come degli hard disk removibili e quindi e possibile farne un'immagine e analizzarli utilizzando MFT abbinati ai lettori di memory card che possono avere interfaccia IDE oppure USB.

Così come per i normali hard disk anche i dati cancellati da questo tipo di memorie possono essere recuperati. Uno dei principali inconvenienti è dovuto al fatto che alcuni modelli, come quelli che rispettano lo standard MMC 4.1, supportano meccanismi di protezione mediante password che possono bloccare il recupero delle informazioni.

6. Ispezione e analisi

L'ispezione, come avevamo già brevemente anticipato, avviene su copie ricavate dalle immagini originali delle memorie dei dispositivi mobili e costituisce una parte importante nella fase di investigazione forense. Il suo ruolo consiste nello scoprire le prove da portare in un processo, incluse quelle che possono essere nascoste e oscurate. Per far ciò, si applicano dei metodi scientifici che dovrebbero descrivere pienamente ed in modo semanticamente corretto, il contenuto e lo stato dei dati in esame, includendo per ognuno la descrizione della sorgente da cui è stato ricavato. L'analisi differisce dall'ispezione, in quanto si occupa di elaborare i risultati di quest'ultima per rilevarne il significato diretto ed il relativo valore probatorio.

L'esaminatore dovrebbe aver studiato il caso ed aver familiarità con i parametri delle trasgressioni, le parti coinvolte e le potenziali prove che possono essere trovate. L'investigatore o l'analista forense forniscono informazioni su cosa cercare, mentre l'esaminatore forense fornisce il mezzo per cercare potenziali informazioni rilevanti .

Se l'esaminatore forense effettua l'analisi senza il supporto diretto dell'analista o dell'investigatore, la conoscenza acquisita dallo studio del caso dovrebbe fornirgli un'idea inerente il tipo di dati da cercare e le parole chiave da utilizzare per la ricerca. 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.

L'esaminatore a volte scopre anche password, tracce di attività su Internet, logon name. Alcuni dati possono fornire un collegamento ad altri potenziali sorgenti di prove mantenute altrove, in particolare dai service provider.

6.1 Prove Potenziali

I produttori di telefoni cellulari offrono strumenti quali browser web e client di posta elettronica utili per gestire le informazioni. Questi strumenti possono variare da dispositivo a dispositivo, a seconda del tipo di firmware installato dal produttore e delle modifiche effettuate dal fornitore del servizio o dall'utente.

Le potenziali prove su questi dispositivi consistono nei seguenti oggetti: i dati dell'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.

A volte anche una suoneria può avere rilevanza in questa fase, soprattutto se il dispositivo consente di associarne una diversa per ogni utente registrato in rubrica. Un testimone ad esempio, potrebbe ricordarne la melodia e dare un aiuto nell'identificazione del colpevole.

In generale, qualunque informazione di rete trovata su una (U)SIM può essere utile nelle indagini. Per esempio, se una rete rifiuta un aggiornamento di locazione da un cellulare che a sua volta vorrebbe registrarsi , la lista delle reti in cui il dispositivo è stato interdetto, denominata Forbidden PLMN, consiste in un file aggiornato

contenente il codice esatto del luogo in cui la rete coinvolta si trova. In questo modo è possibile capire se il sospettato si è mosso nei dintorni della scena del crimine.

Oltre che gli oggetti fisici associati al dispositivo, sono importanti anche i servizi voce e dati a cui l'utente è abbonato. Per esempio, se l'utente ha sottoscritto dei servizi voce, ma non servizi dati, questo consente di escludere dalla ricerca tutto ciò che vi è correlato, come ad esempio, i log di connessione ad Internet.

E' possibile definire due tipi di investigazione forense a seconda se il colpevole è sconosciuto oppure se il colpevole è conosciuto. 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.

La Tabella , mostra i riferimenti incrociati delle generiche sorgenti di prove comunemente trovate su un dispositivo mobile e il loro contributo nel soddisfare gli obiettivi sopra elencati.

	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

TABELLA 3 : TABELLA CHE METTE IN RELAZIONE LE SORGENTI DELLE PROVE E GLI OBIETTIVI CHE SI POSSONO RAGGIUNGERE MEDIANTE LO STUDIO DELLE SORGENTI STESSE

Molte sono le sorgenti di prove come i dati PIM, i dati delle chiamate, SMS, MMS (anche quelli non recapitati) informazioni relative alle navigazioni Internet. Da non trascurare le applicazioni che girano sul dispositivo che possono fornire elementi utili alle indagini, così come i file contenuti, come foto, video, fogli di calcolo, documenti di testo o presentazioni. Molto importanti sono anche le informazioni che si possono recuperare dal fornitore dei servizi. Infatti, quest'ultimi mantengono database per la fatturazione o l'addebito dei conti in base al log delle chiamate. Tali informazioni possono essere utilizzate per fare delle interrogazioni utilizzando i subscriber o gli equipment identifiers.

6.2 PREPARAZIONE DEI TOOL

Una volta completata la fase di acquisizione, il passo successivo consiste nel ricercare i dati, identificare le prove, creare boorkmarks e sviluppare i contenuti del report finale. La buona conoscenza dei tool da utilizzare, può velocizzare in maniera significativa il processo di investigazione.

I MFT sono una componente cruciale; traducono i dati da un formato raw ad un formato strutturato che possa essere letto e compreso da un investigatore, agevolando l'identificazione ed il recupero delle prove. Ciò è utile soprattutto considerando che per rappresentare i dati in un telefono o in una (U)SIM, vengono spesso usate una varietà di differenti e inusuali codifiche, come l'alfabeto GSM a 7 bit per la codifica del testo, molto difficile da codificare manualmente. Da questo punto di vista tuttavia, è importante tener presente che un tool forense potrebbe essere soggetto a bug capaci di rendere la traduzione dei dati inaccurata. Bisogna prestare molta attenzione ed eseguire delle verifiche sui risultati.

Un sospettato abile potrebbe aver manomesso le informazioni contenute nel dispositivo, ad esempio, cambiando deliberatamente i nomi delle estensioni dei file per ostacolare il lavoro di un tool forense o alterando la data e l'ora del telefono per falsificare i timestamp associati alle attività loggate, creando false transazioni nella memoria del telefono e della (U)SIM o usando un tool di cancellazione per rimuovere o eliminare i dati dalla memoria.

L'esperienza acquisita nell'uso di un tool forense, permette di capirne i limiti e compensarne le carenze, distinguendo i dati reali da quelli che potrebbero essere affetti da errori.

La guida "*Forensic Examination of Digital Evidence*" [DOJ04] prodotta dal dipartimento di giustizia statunitense, offre i seguenti suggerimenti per analizzare i dati ricavati:

- **Appartenenza dei dati** – identificare il proprietario e le eventuali altre persone che hanno creato, modificato o avuto accesso ad un file.
- **Analisi dei file** – Identificare informazioni rilevanti esaminandone i contenuti.
- **Analisi dei log** – Determinare quando è successo un evento esaminando i file di log presenti sul dispositivo.
- **Analisi dei dati nascosti** – Individuare e recuperare i dati nascosti o intenzionalmente offuscati.

Lo strumento di ricerca gioca un ruolo significativo nello scoprire le informazioni usate per la creazione di bookmarks e report finali. Per esempio, alcuni tool usati per cercare prove testuali identificano e classificano i file basandosi sulla loro estensione. Alcuni tool hanno un semplice motore di ricerca che fa il mach rispetto ad una stringa data in input e permettono solo di fare ricerche semplici. Altri incorporano motori di ricerca più evoluti che permettono di fare ricerche a partire da espressioni regolari, similmente all'utility grep dei sistemi operativi unix.

6.3 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. Alcuni service provider possono salvare anche informazioni su chiamate fatte tramite VOIP. Il contenuto ed il formato di tali record è abbastanza diverso da un provider ad un altro, tuttavia, permettono quasi sempre di ottenere i dati dell'abbonato, il dispositivo usato, il numero chiamato e la durata della conversazione.

I provider conservano tali informazioni per periodi di tempo limitato, il che richiede un immediato recupero per evitarne la perdita. I dati che si potrebbero recuperare sono: il contenuto delle email rimaste nel server (es., mail non mandate) ed i relativi log, i log di RADIUS o di altri sistemi di autenticazione basati su indirizzo IP, il contenuto di SMS e MMS.

Oltre ai dettagli delle chiamate, per i sistemi GSM, 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)
- ✓ IMSI
- ✓ Numero seriale della (U)SIM (ICCID)
- ✓ PIN/PUK della (U)SIM
- ✓ Servizi permessi
- ✓ Numero delle carte di credito usate per il pagamento

I criteri di ricerca per scoprire eventuali prove possono essere di varia natura, per esempio, si potrebbero analizzare tutte le chiamate ricevute da un certo numero di telefono (es. quello della vittima) o le chiamate gestite da una base station responsabile di una particolare cella (es. per determinare dove era l'indagato in una particolare momento).

L'analisi di un iniziale insieme di record, generalmente porta a richiedere altri record inerenti ad altri abbonati. Per esempio, la vittima potrebbe aver ricevuto frequenti chiamate da un altro numero di telefono su cui è utile investigare per identificare il rispettivo abbonato.

.

7. REPORTING

Il reporting è il processo che si occupa di creare un sommario dettagliato di tutti i passi effettuati e le conclusioni raggiunte durante la fase di investigazione. Un buon report, dovrebbe descrivere con molta cura le azioni eseguite e le eventuali osservazioni, i risultati dei test e delle ispezioni, spiegare dettagliatamente i ragionamenti maturati a seguito dello studio delle prove e dovrebbe essere basato su una solida documentazione, note fotografiche e contenuti generati dai tool.

Molti MFT hanno alcune funzionalità che facilitano la generazione dei report mettendo a disposizione dei template eventualmente personalizzabili. Tali report solitamente includono il nome dello specialista, il numero del caso, la data di generazione ed un titolo, l'insieme delle prove rinvenute, divise per categorie e una raccolta di quelle con maggiore rilevanza per il caso in esame. Possono contenere tutti i dati ricavati o solo alcuni selezionati dall'esaminatore, questo per minimizzare le dimensioni del report oltre che migliorarne la chiarezza.

Le funzionalità di reporting possono variare a seconda del tool di acquisizione e possono andare dalla generazione del report completo in qualche formato di file specifico (es. .txt, .rtf, .csv, .doc, .html), alla semplice esportazione di item di dati usabili per produrre il report manualmente. Nel caso in cui un tool non preveda alcuna funzionalità di reporting l'esaminatore dovrà effettuare gli screenshot delle varie interfacce che mostrano i risultati ottenuti e costruirsi il report manualmente. A volte, è richiesto anche l'uso di tecniche di acquisizione ausiliarie. Molti MFT, ad esempio, non sono in grado di acquisire le registrazioni video, per cui, si dovrà adoperare un qualche programma di video editing per acquisire le immagini e includerle nel report. Alcuni tipi di dati (es. audio, video) non possono essere presentati in un formato stampabile e quindi dovrebbero essere inclusi come allegati da memorizzare su supporti adeguati (es CD-ROM, DVD-ROM).

Il report generato dovrebbero includere le seguenti informazioni:

- ✓ Identità dell'agenzia di reporting
- ✓ Identificativo del caso
- ✓ Identità dell'investigatore che ha operato sul caso
- ✓ Identità del submitter
- ✓ Data di ricezione
- ✓ Data del report
- ✓ Descrizione della lista degli oggetti sottomessi per l'ispezione, incluso numero seriale, produttore e modello del dispositivo.
- ✓ Identità e firma dell'investigatore
- ✓ L'equipaggiamento e le impostazioni usate nell'investigazione
- ✓ Breve descrizione dei passi fatti durante l'ispezione
- ✓ Materiale di supporto come stampe, copie digitali della prova e documentazione sulla catena di custodia
- ✓ Dettagli delle ricerche:

- Specifici file relativi alla ricerca
- Altri file, inclusi i file cancellati di supporto alle ricerche
- Stringhe di ricerca
- Prove relative al traffico Internet, come analisi sul traffico su siti, chat log, cache, e-mail e attività su newsgroup
- Analisi delle immagini grafiche
- Indicatori di proprietà
- Analisi dei dati
- Descrizione dei programmi rilevanti utilizzati sugli oggetti esaminati
- Tecniche usate per nascondere o mascherare dati, come crittografia, stenografia, attributi nascosti, partizioni nascoste e nomi di file anomali

✓ Conclusioni del report

Le prove ricavate, così come i tool, le tecniche e le metodologie utilizzate nell'ispezione, sono oggetto di dibattito durante il processo, una opportuna documentazione si rivela dunque essenziale durante queste fasi. Come parte del processo di reporting si dovrebbe anche includere una copia del software usato insieme all'output che si otterrebbe applicando la procedura descritta nel report. Questo è utile per evitare che una diversa versione dello stesso software ottenga diversi risultati, magari in successive riproduzione lungo l'intera durata del procedimento.

8. MOBILE FORENSIC TOOL

Mentre i personal computer sono progettati per essere general purpose, i telefoni cellulari sono progettati per specifiche applicazioni che effettuano un certo numero di task predefiniti. Inoltre, ogni produttore di telefoni cellulari cerca di imporre per i suoi prodotti, un proprio sistema operativo. Tutto ciò comporta la necessità di dotarsi di diversi Mobile forensic tool (MFT) che operano su diversi insiemi di dispositivi. Ad esempio, esistono tool che lavorano solo su cellulari di una determinata marca oppure altri che lavorano solo su una determinato sistema operativo oppure solo su dispositivi che condividono una particolare architettura hardware. A ciò si aggiunga che nuovi dispositivi vengono immessi sul mercato in tempi molto brevi e questo costringe i produttori di MFT di rivedere continuamente i loro prodotti in modo da poter rispondere adeguatamente alle esigenze dei nuovi dispositivi. Essendo questo un compito molto gravoso da parte degli sviluppatori, spesso si hanno ritardi significativi nei rilasci di nuove versioni, complicando ulteriormente il lavoro di recupero dei dati.

8.1 MODALITÀ DI ACQUISIZIONE

I MFT utilizzano le seguenti modalità per acquisire dati dai dispositivi:

- Acquisizione Fisica: ossia la copia bit a bit dell'intera memoria fisica (es. chip di memoria) del dispositivo.
- Acquisizione Logica: implica la copia bit a bit degli oggetti di memoria logici, come file e directory che risiedono nella memoria logica (es. filesystem)

L'acquisizione fisica è preferibile rispetto all'acquisizione logica perché consente di recuperare dati rimasti in memoria di qualsiasi tipo (es. memoria non allocata o spazio sul filesystem) per poi poterli analizzare. Questo processo di estrazione dell'immagine della memoria del dispositivo, analisi, decodifica e traduzione dei dati nell'immagine è abbastanza tediosa ed impiega molto tempo se fatta manualmente. Perciò conviene ricavarsi l'immagine fisica, importarla in un tool che automaticamente analizzi l'immagine e ne crei un report. Purtroppo, non ci sono molti tool creati appositamente per ottenere l'intera immagine della memoria del cellulare.

L'acquisizione logica è molto più limitata rispetto all'acquisizione fisica, anche se offre il vantaggio di riuscire a recuperare i dati sotto forma di file e directory facilmente utilizzabili in fase di analisi. Pertanto, è consigliabile effettuare entrambe le acquisizioni, in particolar modo, bisognerebbe procedere prima ad una analisi fisica e, successivamente, farne una logica.

8.2 CARATTERISTICHE DEI MFT

Gli MFT sono progettati per acquisire dati all'interno della memoria dell'handset e/o dalla (U)SIM, senza alterare il contenuto del dispositivo ed effettuando un calcolo dell'hashing (utilizzando algoritmi come MD5, SHA, ecc) per preservare l'integrità dei dati acquisiti.

Un generico MFT esegue, solitamente una serie di passi ben definiti, per trasformare le informazioni presenti su un dispositivo in prove utilizzabili in un processo forense. Nella Figura 7 mostra le fasi in questione, che sono nell'ordine: acquisizione, decodifica e traduzione, nella stessa figura si può notare come queste fasi agiscono in maniera sequenziale ossia che l'output di una fase diventa l'input della fase successiva a cominciare dalla fase di acquisizione che stabilisce una comunicazione col dispositivo alfine di recuperare le informazioni in essa presenti, utilizzando per lo più protocolli di comunicazione come i comandi AT, FBUS e OBEX per comunicare con l'handset, oppure APDU per comunicare con la SIM facendo così acquisizione logica anche se ci sono alcuni MFT che possono effettuare acquisizione fisica anche se solo ma solo per alcune tipologie di telefoni cellulari.

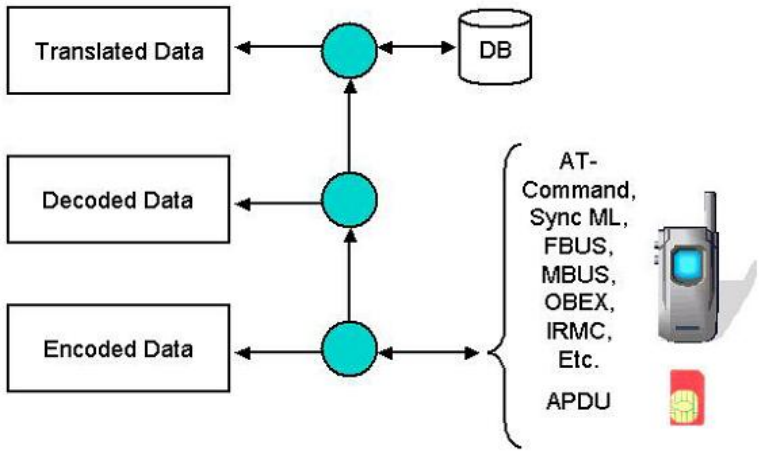

FIGURA 7 SCHEMA CHE RIASSUME LE FASI DI ACQUISIZIONE, DECODIFICA E TRADUZIONE COMPIUTI DA UN GENERICO MFT.

Dato che un handset può supportare più di un protocollo, un tool ne può eseguire più di uno in successione, in modo da poter recuperare più informazioni possibile. Normalmente, anche se si utilizza più di un protocollo per recuperare informazioni su un handset, può accadere di non riuscire comunque a recuperare tutte le informazioni. Tool differenti possono usare differenti protocolli per acquisire lo stesso dato. La Tabella mostra un esempio di richiesta e di risposta legato all'acquisizione dell'IMEI da un cellulare Nokia 6101 (356661005704092 nell' esempio) effettuato da tre MFT diversi che utilizzando due protocolli ossia Comandi AT per GSM .XRY, mentre PhoneBase e Secure View utilizzano il protocollo FBUS.

TABELLA 4: ESEMPIO DI ACQUISIZIONE DEL IMEI CON TRE MFT DIVERSI

	Request/Response (Hex)	Request/Response (ASCII)
GSM .XRY	41 54 2B 43 47 53 4E 0D	A T + C G S N .
	0D 0A **33 35 36 36 36 31 30 30 35 37 30 34 30 39 32** 0D 0A 0D 0A 4F 4B 0D 0A	. . **3 5 6 6 6 1 0 0 5 7 0 4 0 9 2** . . . . O K . .
PhoneBase	1E 00 0C 7F 00 02 D2 01 C0 7C 1E 00 10 1B 00 07 00 01 00 00 41 01 41 00 0E 1C	. . . □ . . Ò . À | . . . . . A . A . . .
	1E 10 00 7F 00 02 1B 01 05 6C 1E 10 00 1B 00 1C 01 39 00 01 00 01 41 14 00 10 **33 35 36 36 36 31 30 30 35 37 30 34 30 39 32** 00 01 42 5B 50	. . . □ . . . . . l . . . . . 9 . . . . A . . . **3 5 6 6 6 1 0 0 5 7 0 4 0 9 2** . . B [P
Secure View	55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 … (6 more rows) 1E 00 10 1B 00 07 00 04 00 00 41 01 60 00 2F 19	U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U U … . . . . . A . ` . / .
	1E 10 00 7F 00 02 1B 00 05 6D 1E 10 00 1B 00 1C 04 39 00 01 00 01 41 14 00 10 **33 35 36 36 36 31 30 30 35 37 30 34 30 39 32** 00 01 45 5E 57	. . . □ . . . . . m . . . . . 9 . . . . A . . **. 3 5 6 6 6 1 0 0 5 7 0 4 0 9 2** . . E ^ W

Alcuni di questi protocolli sono proprietari mentre altri sono standardizzati e pubblici, anche se, di solito, includono delle estensioni o varianti introdotte dai produttori di cellulari.

Una volta recuperati i dati grezzi mediante dall'acquisizione da un telefono o una (U)SIM, è possibile che questi dati siano codificati senza rispettare una particolare convenzione. Il testo, ad esempio, può essere rappresentato con un alfabeto GSM a 7 bit per simbolo oppure, con i più facilmente interpretabili Binary Coded Decimal (BCD) o Unicode. Pertanto, i tool devono anche occuparsi di effettuare la decodifica di questi dati, in modo da facilitare il lavoro all'operatore così come illustrato nella Figura 7.

Infine c'è la fase di traduzione che consente di migliorare ulteriormente la leggibilità dei dati acquisiti. Per esplicitare questa fase può essere utilizzato un database, come nel caso della traduzione del codice numerico che rappresenta un determinato paese nel corrispondente nome del paese.

8.3 STRUMENTI E TECNICHE DI ACQUISIZIONE ALTERNATIVE

Nell'analisi forense su dispositivi mobile è di norma utilizzare strumenti diversi dai MFT oppure delle particolari tecniche come il port filtering. Di seguito illustreremo la ragioni e le considerazioni da fare nel decidere di utilizzare questi strumenti nell'analisi forense, in particolar modo per quanto riguarda l'utilizzo dei phone manager.

8.3.1 PHONE MANAGER

I Phone Manager come sono delle applicazioni in grado di poter gestire i dati presenti su un dispositivo mobile la rubrica, sms, file multimediali, ecc). Un esempio di phone manager è il Nokia PC Suite che gestisce i dati sui cellulari Nokia. Essi possono essere dei validi strumenti alla pari dei MFT nell'analisi forense su dispositivi mobile. Questo perché possono rappresentare l'unico mezzo per recuperare prove importanti da utilizzare in un processo forense. Questi tool non forensi utilizzano gli stessi protocolli di comunicazione con il dispositivo utilizzati dai MFT, ma sono usati per modificare e aggiungere contenuti (es. aggiungere suonerie, sfondi, ecc). Gli addetti all'analisi forense, spesso utilizzano una collezione di MFT e tool non forensi. Tuttavia, prima di considerare l'utilizzo di tool non forensi, si dovrebbe procedere ad una valutazione accurata ed essere a conoscenza delle implicazioni associate alle questioni forensi.

8.3.2 PORT FILTERING

Oltre che acquisire dati in modo diretto da un dispositivo, si possono studiare le comunicazioni che avvengono normalmente tra il dispositivo stesso e la workstation su cui gira un'applicazione non forense di gestione delle informazioni (es. Nokia PC Suite). Questo lo si può fare monitorando le porte e le funzionalità di logging per dispositivi cablati tipo Portman e Serial Monitor, oppure, analizzando lo scambio di messaggi Bluetooth o IrDA attraverso una workstation dedicata all'intercettazione del traffico wireless generato. Il monitoraggio delle porte può anche essere esportato con un tool forense in modo da poter recuperare ulteriori informazioni oppure, semplicemente, per catturare il log completo di una acquisizione.

Ad esempio, nel port filtering della comunicazione tra un cellulare Nokia e la Nokia PC Suite fatta con un protocollo FBUS, le tecniche utilizzate per la realizzazione del filtro consistono nell'intercettazione delle chiamate dell'NPCS alle API del sistema operativo ospitante; in particolare per quanto riguarda le API di acquisizione dei dati e le chiamate a funzioni come CreateFile e ReadFile. Si passa dunque all'interpretazione del contenuto e alla restituzione di una risposta appropriato al NPCS.

L'**API hooking** è il termine usato per descrivere l'intercettazione di chiamate a funzioni per esplicare un qualche scopo, come personalizzare ed estendere una funzionalità o anche per monitorare alcuni aspetti di un'applicazione. In passato ad esempio, questa tecnica è stata usata per realizzare firewall e antivirus o anche codice malizioso come i rootkits. Nel caso di Windows, le funzioni più interessanti da filtrare sono quelle che appartengono alle API di sistema, ma ciò non toglie che si possano filtrare anche quelle appartenenti a generiche applicazioni, librerie o DLL.

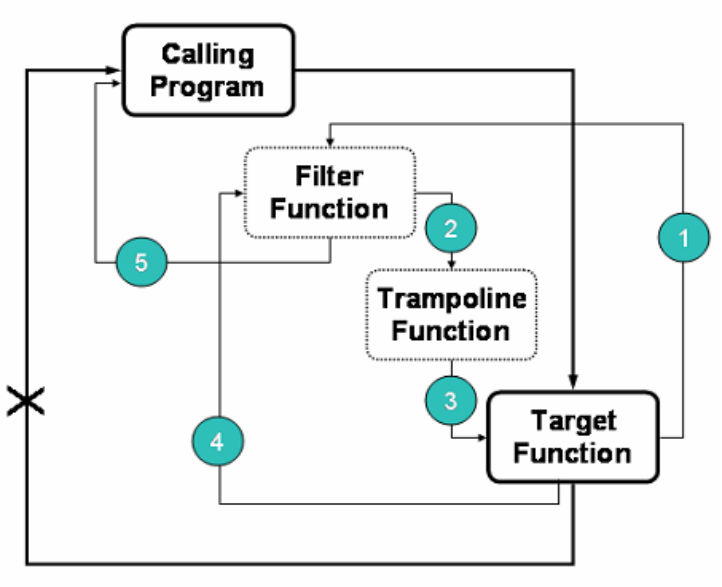

FIGURA 8: SCHEMA DI COME AVVIENE L'INTERCETTAZIONE DELLE CHIAMATE API

L'approccio generico per la realizzazione di un filtro è quello illustrato in Figura 8. Come prima istruzione della *funzione target,* viene inserito un jump (salto) alla *funzione filtro* che sostituisce le istruzioni presenti nella funzione target con che saranno conservati in una funzione denominata funzione trampolino. La funzione trampolino agisce da relay, ritornando poi alla funzione target in modo da completare il proprio lavoro dopo che le istruzioni preservate siano state eseguite. La funzione filtro può o chiamare la funzione trampolino che invocherà la funzione target oppure restituire il controllo direttamente al programma chiamante e bypassare completamente la funzione target. Inoltre la funzione target presenta degli aggiustamenti in modo che il controllo viene ritornato al filtro dopo aver finito le sue istruzioni e facendo seguito a queste ultime l'esecuzione del filtro in modo da effettuare delle operazioni successive a quelle già effettuate dalla funzione target.

L'uso di queste tecniche di creazione di filtri è fortemente condizionata dal sistema di cui si vuol manipolare le API inoltre nel caso dei sistemi Win32 solo alcune funzioni delle sue API sono parzialmente sovrascrivibili.

8.4 CLASSIFICAZIONE DEI MFT

Gli MFT, si rivolgono ad un ampio intervallo di dispositivi, gestiscono le più comuni situazioni investigative e non richiedono particolari conoscenze per poter esser usati. Sono indirizzati a trattare solo dispositivi di certi produttori, con uno specifico sistema operativo o su dispositivi che condividono una particolare architettura hardware. Quindi, per poter coprire quanti più dispositivi e (U)SIM possibili, c'è bisogno di un certo numero di tool differenti.

La Tabella 3 offre una panoramica dei MFT disponibili e illustra le funzionalità che loro stessi forniscono: acquisizione, analisi o reporting.

TABELLA 3: ELENCO DEGLI MFT

	Function	Target Devices
Forensic Card Reader	Acquisition, Reporting	▪ SIMs
ForensicSIM	Acquisition, Examination, Reporting	▪ SIMs and USIMs
SIMCon[8]	Acquisition, Examination, Reporting	▪ SIMs and USIMs
SIMIS	Acquisition, Examination, Reporting	▪ SIMs and USIMs
USIMdetective	Acquisition, Examination, Reporting	▪ SIMs and USIMs
BitPIM	Acquisition, Examination	▪ Certain CDMA phones using Qualcomm chipsets
Oxygen PM (forensic version)	Acquisition, Examination, Reporting	▪ Nokia phones
Oxygen PM for Symbian (forensic version)	Acquisition, Examination, Reporting	▪ Symbian phones
PDA Seizure[9]	Acquisition, Examination, Reporting	▪ Palm OS, Windows Mobile/Pocket PC, and Blackberry devices
Pilot-Link	Acquisition	▪ Palm OS devices

	Function	Target Devices
Cell Seizure[10]	Acquisition, Examination, Reporting	▪ TDMA, CDMA, and GSM phones ▪ SIMs and USIMs
CellDEK	Acquisition, Examination, Reporting	▪ GSM and CDMA phones ▪ SIMs and USIMs
GSM .XRY	Acquisition, Examination, Reporting	▪ GSM and CDMA phones ▪ SIMs and USIMs
MobilEdit!	Acquisition, Examination, Reporting	▪ GSM phones ▪ SIMs
PhoneBase	Acquisition, Examination, Reporting	▪ GSM phones ▪ SIMs and USIMs
Secure View	Acquisition Examination Reporting	▪ TDMA, CDMA, and GSM phones ▪ SIMs
TULP 2G	Acquisition, Reporting	▪ GSM phones ▪ SIMs

Gli strumenti sono raggruppati in base al target ossia: (U)SIM, handset e i Toolkit che operano sia su (U)SIM che su handset. Nei successivi paragrafi descriveremo nei gli MFT più importanti per (U)SIM, handset e Toolkit.

8.4.1 MFT PER (U)SIM

Alcuni MFT sono specializzati nella lettura diretta della (U)SIM, senza utilizzare l'handset.

Il valore e le finalità dei dati acquisiti varia con le capacità e le funzionalità degli strumenti. Molti di questi tool acquisiscono, oltre che le informazioni inerenti al gestore e alla località della (U)SIM, anche i seguenti dati: International Mobile Subscriber Identity (IMSI), Integrated Circuit Card ID (ICCID), Abbreviated Dialling Numbers (ADN), gli ultimi numeri chiamati, messaggi SMS e Location Information (LOCI). Possono tentare il recupero dei messaggi cancellati e dei messaggi EMS e fornire particolari funzionalità inerenti all'amministrazione del PIN.

Tra tutti gli strumenti progettati per acquisire dati dalle (U)SIM, vale la pena citare:

- **Forensic Card Reader** della Becker & Partner che estrae contenuti dalla SIM fornendo l'output dei dati acquisiti in un formato XML leggibile attraversi uno specifico editor. Purtroppo esso non garantisce alcuna protezione hash per l'integrità e nemmeno funzionalità di reporting. I dati vengono acquisiti usando un lettore di (U)SIM.

- **SIM Card Seizure** di Paraben salva i dati in un file contenente tutte le informazioni di interesse per il caso in cui è coinvolta la SIM. Il file ha un formato proprietario ma può essere esportato anche sotto forma di testo ASCIII. L'acquisizione viene eseguita attraverso un lettore di (U)SIM PC/SC compatibile e, come strumento per salvaguardare l'integrità dei dati acquisiti, utilizza SHA1. Offre anche la funzionalità di import di file che rappresentano un determinato caso e permette di esportare i risultati in un report finale.

- **Quantaq Solutions USIMdetective** è un tool di acquisizione ed analisi e generatore di report forensi per qualsiasi tipo di (U)SIM. Utilizzato in abbinamento ad un lettore di carte PC/SC compatibile, mostra gli elementi acquisiti in formato testuale o esadecimale. È dotato di una funzionalità interna per l'hashing che assicura l'integrità dei dati acquisti e li preserva da manomissioni. Image Integrity Check (.iic) sono i file che vengono creati ad ogni acquisizione. SHA1 e MD5 assicurano che il file d'acquisizione originario resti consistente anche in eventuali analisi successive. USIMdetective fornisce più tipi di report che differiscono tra loro per le quantità di dettagli forniti. Si va da uno Standard Report essenziale fino ad un “File Content Report” molto dettagliato.

8.4.2 MFT PER HANDSET

Oltre ai MFT completamente dedicati alle carte (U)SIM, ci sono quelli dedicati al recupero di informazioni dalla memoria interna dell'handset. Tali strumenti sono spesso derivati da tool che operano su PDA, quindi sono utilizzabili anche con gli smart phone provvisti di un sistema operativo simile, come Palm OS o Windows Mobile. Altri invece, sono derivati da strumenti di gestione dei cellulari a cui sono state apportate modifiche che impediscono di sovrascrivere i dati sul dispositivo. Questi tool, solitamente, non hanno alcuna possibilità di acquisire dati dalla (U)SIM utilizzando la lettura diretta. Di seguito ne riportiamo una breve panoramica:

- **Device Seizure** è un toolkit di Paraben che fornisce un mezzo per estrarre dati da dispositivi mobili che supportano Palm OS, Windows Mobile e Symbian OS. Il file che contiene le informazioni estratte ha un formato proprietario e l'output può essere convertito in HTML. L'acquisizione può avvenire via a cavo, IrDA, o Bluetooth; non c'è bisogno di hardware aggiuntivo. Tra le funzionalità sono incluse l'acquisizione logica e, per alcuni dispositivi, anche l'acquisizione fisica. Un digest MD5 viene creato per ogni oggetto acquisito e per il file che contiene le informazioni relative al caso. Quest'ultimo, viene criptato in modo da prevenirne la modifica. Infine, consente di creare report personalizzati, importare file di casi archiviati e gestisce la ricerca e i segnalibri sui dati acquisiti.

- **Oxygen Phone Manager** (versione forense) della Oxygen Software è una variante del gestore di cellulare prodotto con lo stesso nome e lavora principalmente con telefoni dotati di sistema operativo Symbian. La versione forense differisce da quella non forense per il fatto che non può effettuare operazioni di modifica dei dati sul dispositivo target. Fornisce esaminatori che sono in grado di estrarre dati da un cellulare operante sulla rete GSM. Purtroppo, non effettua l'esportazione su di un unico file delle prove ottenute, ma consente di memorizzare i risultati su file multipli (es. Rubrica, SMS e contenuti multimediali) non protetti con funzioni di hashing.

- **BitPIM** è un software open source disponibile sotto licenza GNU. Effettua principalmente operazioni di gestione dati dei telefoni cellulari di diversi produttori. La peculiarità di questo software è quella di poter disattivare facilmente le funzionalità di scrittura, rendendolo così uno strumento adatto all'acquisizione. Così come OPM, effettua il salvataggio dei dati acquisiti su diversi file non protetti con una funzione hash.

8.4.3 MOBILE FORENSIC TOOLKIT

Sono capaci di acquisire dati sia dalle (U)SIM sia dagli handset. Il vantaggio principale risiede nella possibilità di inserire nello stesso report i risultati di entrambe le acquisizioni. Di seguito citiamo i principali toolkit integrati:

- **Cell Seizure** di Paraben supporta dispositivi GSM, non GSM (es. CDME, TDMA) e (U)SIM. Il file probatorio può essere o in formato

ASCII oppure in formato HTML. L'acquisizione avviene via cavo, IrDA o Bluetooth. Per acquisire i dati dalla (U)SIM viene utilizzato un lettore (U)SIM completo di cavi e driver, incluso all'interno nel software. Cell Seizure include funzionalità di acquisizione logica e fisica, fornendo una vista della memoria interna. Ad ogni dato acquisito viene associato un valore hash MD5 e SHA1.

- **MOBILedit! Forensic** di Compelson Labs supporta l'acquisizione logica dei dati da telefoni GSM, non GSM e da (U)SIM card. Il tool è basato sull'equivalente non-forense che si occupa della gestione dei cellulari. I dati sono acquisiti dal telefono utilizzando il cavo o le connessioni Bluetooth o IrDA. Utilizza un lettore di carte SIM PC/SC compatibile per le (U)SIM. I dati vengono memorizzati in un file probatorio che ha un formato proprietario e può essere esportato in XML, ma permette anche di creare reports personalizzati. Purtroppo, non protegge con hashing i dati acquisiti.
- **TULP2G** è un tool forense open source sviluppato dal Netherlands Forensic Institute che permette l'acquisizione da telefoni GSM, non GSM e (U)SIM. I dati possono essere acquisiti con il cavo, il Bluetooth o l'interfaccia IrDA. Per leggere le SIM è necessario un lettore di smart card PC/SC. TULP2G genera i suoi report in formato XML convertibile in un formato leggibile applicando un foglio distile XSL.

8.5 Isolamento dei MFT

L'utilizzo di più tool però, si possono verificare dei conflitti la cui risoluzione può essere molto onerosa e portare via molto tempo, fino alla necessità di replicare tutte le macchine che eseguono i tool.

Un modo per evitare questi problemi consiste nell'utilizzo di virtual machine (VM) su cui far girare il tool desiderato. Ogni tool viene installato col proprio sistema operativo su una macchina virtuale, in modo da renderlo indipendente dagli altri. Un modo alternativo per isolare tool o insiemi di MFT incompatibili tra loro, nel clonare una VM con i tool installati che mantengono una certa configurazione base e distribuire i cloni su altre workstation. In questo modo otteniamo un ambiente computazionale comune che ci consente di semplificare la fase di configurazione, dal momento che più VM possono girare simultaneamente su una singola workstation, più tools o un insieme particolare di tool tra loro incompatibili possono girare tranquillamente.

8.6 Funzionalità dei MFT

Come abbiamo visto finora, ci sono molti MFT tutti sensibilmente differenti tra loro per funzionalità offerte e capacità di reporting. Inoltre, alcune situazioni come ad esempio il recupero di dati cancellati, può richiedere l'uso di tool speciali e a volte anche lo smontaggio del dispositivo. Anche i cavi, i driver utilizzati e i lettori di (U)SIM possono variare da prodotto a prodotto. È necessaria, dunque, una analisi

qualitativa che ci consenta di capire quali siano i MFT più adatti alle nostre esigenze. La validazione di un tool avviene utilizzando dei test data ben definiti, caricati all'interno del dispositivo utilizzando gli stessi metodi utilizzati comunemente dagli utenti. Su tali dati viene poi effettuata la procedura di acquisizione che permette di validare l'intero processo. Bisogna tener presente che la maggior parte dei tool per cellulari viene sviluppato in tempi molto brevi, provocando delle limitazioni sia per quanto riguarda l'ampiezza delle prove trovate, sia per quanto riguarda la profondità dell'analisi; non di rado poi, accade di trovarsi di fronte ad errori subdoli non facili da scovare ed a versioni nuove del tool meno efficaci rispetto alle precedenti.

La più importante tra le caratteristiche dei MFT è la loro capacità di mantenere l'integrità dei dati sorgenti e dei dati estratti. Per raggiungere questo scopo è necessario eliminare o bloccare qualsiasi richiesta di scrittura sui dati del dispositivo e calcolare un hash crittografico del contenuto dei file che sarà utile per verificare che non siano state apportate modifiche.

La preservazione dell'integrità non solo mantiene la credibilità delle prove da un punto di vista legale, ma è indispensabile per poter effettuare successive indagini, come ad esempio, quelle eseguite dalla controparte nel processo.

9. APPENDICE: UN CASO PRATICO DI RECUPERO DI PARTE DEGLI SMS CANCELLATI DA UN TELEFONO SYMBIAN

9.1 INTRODUZIONE

Il recupero di informazioni cancellate su un dispositivo mobile da usare in sede forense, come ad esempio gli sms inviati e ricevuti, può essere un attività molto dispendiosa in termini di tempo oltre a richiedere attrezzature e software particolari che consentano di effettuare un'acquisizione fisica di tutti i supporti di memoria utilizzati dal dispositivo posto sotto indagine.

Nonostante ciò, per alcuni dispositivi mobili, nel nostro caso quelli dotati di sistema operativo Symbian che equipaggia molti dispositivi mobile tra cui quelli marchiati Nokia e Samsung, è possibile scoprire informazioni significative sugli sms cancellati, semplicemente ispezionando alcune directory del sistema operativo e, in particolar modo, un file.

In questa parte del lavoro ci occuperemo di descrivere un po' le directory utilizzate da Symbian per memorizzare le informazioni riguardanti l'uso del dispositivo, in particolare quella che contiene le informazioni sugli sms, concentrandoci sul contenuto del file index, di cui daremo una breve descrizione prima di analizzare cosa accade in seguito alla cancellazione dei messaggi. In fine, vedremo una semplice procedura di recupero dei messaggi stessi.

In questo lavoro ci riferiremo al sistema Symbian S60 3rd Edition 9.1 v3.83.

9.2 DIRECTORY PRIVATE DI SYMBIAN

Symbian si avvale di alcune directory dove immagazzina numerose informazioni sullo stato del dispositivo, come ad esempio il database dei contatti, il registro delle applicazioni installate, gli sms, ecc. Tali directory sono contenute in una sezione non accessibile all'utente, rappresentata dalla directory "Private" che si trova in C:\ (la radice della memoria interna dei dispositivi Symbian).

Per poter accedere si dovrebbe utilizzare un programma particolare da installare sul nostro dispositivo Symbian che ci consente di navigare le directory contenute in C:\Private. Uno di questi software è **ROM Patcher**, utilizzato in primo momento per cercare di accedere direttamente alla memoria interna del cellulare per recuperare le informazioni contenute nella directory degli sms denominata 1000484b. Al lettore curioso lasciamo, nella bibliografia, i riferimenti ad alcuni link a siti che descrivono come poter accedere a queste directory utilizzando il programma ROM Patcher e una lista delle directory contenute in C:\Private con le informazioni sul loro contenuto.

9.3 DIRECTORY 1000484B E IL FILE INDEX

All'interno della directory 1000484b è presente una directory denominata Mail2 che contiene alcuni file di cui il più importante è index che mantiene traccia di sms, mms e email, così come mostrato nella Figura 9.

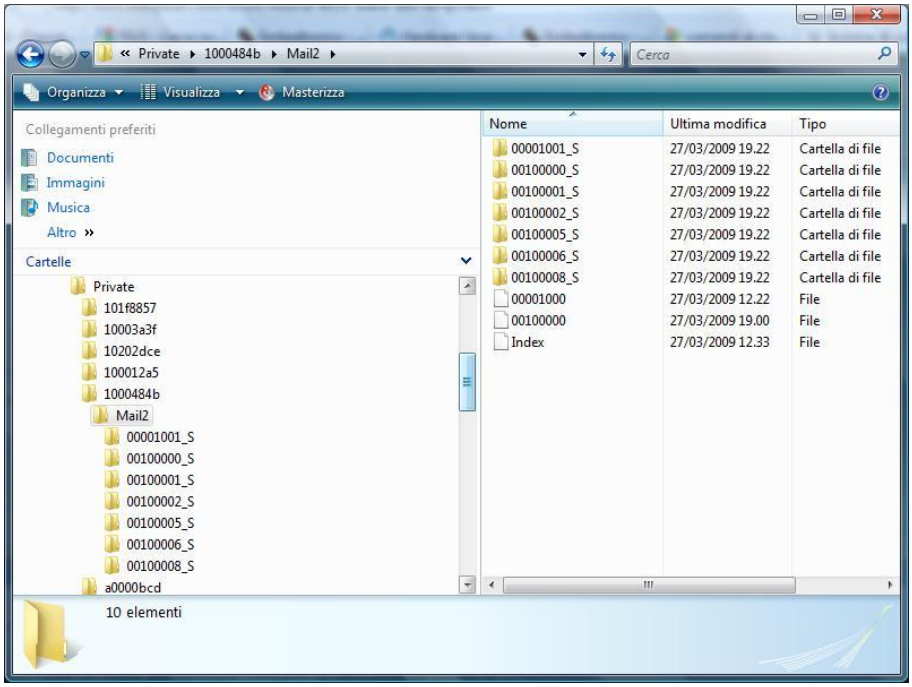

FIGURA 9 STRUTTURA DELLE DIRECTORY PRIVATE E 1000484B OLTRE AL CONTENUTO DELLA DIRECTORY MAIL2.

Tale directory contiene diverse sotto directory contraddistinte da nomi tipo 00001001_S, 00001002_S, etc. La più significativa di queste è 00001001_S all'interno della quale ci sono diverse directory ognuna corrispondente ad una cifra esadecimale (0,1,2,…,f) e ciascuna di queste contiene dei file in cui è salvato il testo integrale degli sms in chiaro e il numero di telefono del destinatario. Ciò è valido sia per I messaggi in entrata e sia per quelli e per le bozze.

Il file index recuperato utilizzando la procedura che descriveremo successivamente , contiene del testo in chiaro che rappresenta i primi 60 caratteri di ogni SMS memorizzato correntemente nel telefono e dal numero di telefono con relativo riferimento alla rubrica del destinatario.

Analizzando diverse istanze di questo file, ottenute cancellando diversi sms, abbiamo verificato che le entry corrispondenti agli sms cancellati permanevano e pertanto, salvo ulteriori sovrascritture (in questo caso il numero di caratteri recuperabili diminuisce fino a che la entry non sparisce del tutto) era possibile recuperare i primi 60 caratteri di ogni sms cancellato e il numero di telefono del destinatario.

Almeno per quanto riguarda alcune versioni di Symbian precedenti a quella utilizzata nei nostri test come la 7.0, tale file mantiene un campo ID, un campo type che definisce se la entry descrive un folder, un messaggio, un servizio o un attachment e diverse informazioni tra cui un flag indicante se il messaggio è stato cancellato oppure no e soprattutto un campo che contenente la descrizione del messaggio composta dalla parte iniziale del testo del sms. Inoltre, sempre per quanto riguarda la versione 7.0, esiste una libreria apposita per realizzare

programmi in C++ che leggono il file index in cui ogni entry è modellata dall'oggetto TMsgEntry che dovrebbe contenere le info descritte sopra.

9.4 Procedura di recupero del file index

La seguente procedura è stata provata su un Nokia 6120 con Symbian S60 3rd Edition 9.1 v3.83.

Se gli SMS sono contenuti sulla memoria interna del cellulare bisogna far in modo che vengano copiati su una memory card, nel nostro caso una MiniSD, in questo caso dobbiamo accedere dal menu presente sul cellulare alla funzionalità di gestione degli SMS.

Prima di fare ciò è necessario isolare il dispositivo dalla rete cellulare, questo lo si può fare premendo il tasto di accensione del dispositivo una sola volta, e scegliere dal menù la voce Offline.

1. Scegliere il menu delle Opzioni e da questo portarsi sulla voce Impostazioni.
2. Una volta aperto il pannello delle impostazioni scegliere la voce Altro.
3. Selezionare voce Memoria in uso e scegliere Memory card, a questo punto ci verrà chiesto di copiare tutti i nostri messaggi dalla memoria del cellulare alla memory card.
4. A questo punto non ci rimane che estrarre la miniSD che abbiamo messo nel nostro telefono e inserirla all'interno di un lettore di memorie SD collegato ad un PC.
5. Aprire la cartella Private presente nella root della miniSD e ritroviamo tutte le directory descritte nel paragrafo precedente.

10. GLOSSARIO

Acquisizione – Un processo nel quale la prova digitale è copiata.

Analisi – Ispezione dei dati acquisiti per estrapolare eventuali valori probatori.

Bluetooth – Un protocollo wireless che permette a due dispositivi di comunicare l'uno con l'altro entro brevi distanze (es., 30 metri.).

Code Division Multiple Access (CDMA) – è una tecnica di accesso, da parte di più sorgenti di informazione, allo stesso canale di trasmissione, tramite l'impiego della stessa banda di frequenze.

Enhanced Data for GSM Evolution (EDGE) – è un'evoluzione dello standard GPRS per il trasferimento dati sulla rete cellulare GSM che consente maggiori velocità di trasferimento dei dati.

Enhanced Messaging Service (EMS) – è un'estensione dello standard SMS. I telefoni che supportano EMS possono inviare e ricevere messaggi contenenti testo formattato, disegni, suoni....

Fast Bus (FBUS) - ANSI/IEEE data bus utilizzato per la comunicazione tra telefoni cellulari. Lo standard specifica che la trasmissione avviene con dispositivo che funge da Master (quello che manda una richiesta), e l'altro come slave (ritornando una risposta). F-Bus è bi-direzionale full-duplex ed effettua trasmissioni seriali.

Federal Communications Commission Identification Number (FCC ID) – è un codice identificativo trovato in tutti i componenti hardware del computer. E' un identificativo utile nella ricerca di informazioni sui produttori dei dispositivi hardware.

Global Positioning System – un sistema di posizionamento su base satellitare, a copertura globale e continua, gestito dal dipartimento della difesa statunitense.

Global System for Mobile Communications (GSM) – standard di telefonia mobile più diffuso del mondo. Più di 3 miliardi di persone in 200 paesi usano telefoni cellulari GSM.

Hashing – Il processo di usare un algoritmo matematico per produrre una valore numeriche che è rappresentativo per un insieme di dati.

Integrated Circuit Card ID (ICCID) – E' un numero seriale assegnato ad una (U)Sim..

Integrated Digital Enhanced Network (iDEN) – Una tecnologia proprietaria di comunicazione mobile sviluppata dalla Motorola.

International Mobile Equipment Identity (IMEI) – Il codice IMEI (acronimo di International Mobile Equipment Identity) è un codice alfanumerico che identifica univocamente un terminale mobile (Mobile Equipment), che può essere un telefonino o un modem.

International Mobile Subscriber Identity (IMSI) – IMSI è la sigla di International Mobile Subscriber Identity ("identità internazionale di utente di

telefonia mobile"). Si tratta di un unico numero che viene associato a tutti gli utenti di telefonia mobile di reti GSM o UMTS.

Joint Test Action Group (JTAG) - è un consorzio di 200 imprese produttrici di circuiti integrati e circuiti stampati allo scopo di definire un protocollo standard per il test funzionale di tali dispositivi, che tendono ad essere sempre più complessi e difficili da controllare, fino a rendere impraticabili i tradizionali metodi manuali o automatici (e ad aumentare in modo non competitivo il "Time to market").

Mobile Subscriber Integrated Services Digital Network (MSISDN) – è il numero univocamente associato ad un contratto telefonico di telefonia mobile (GSM o UMTS): in pratica è il numero che viene digitato per chiamare un utente. L'abbreviazione ha diverse interpretazioni, la più comune è la seguente: "Mobile subscribers integrated services digital network", ossia "Rete digitale di servizi integrati per utenti di telefonia mobile".

Multimedia Messaging Service (MMS) – Uno standard per messaging che permette agli utenti di inviare e ricevere messaggi formattati con testo, foto, audio e video clip.

OBject EXchange (OBEX) – Protocollo di comunicazione che consente lo scambio oggetti binari tra dispositivi. OBEX è simile ad HTTP in quanto i client utilizzano una connessione affidabile per collegarsi ad un server per scambiarsi gli oggetti.

Public Land Mobile Network (PLMN): area di servizio di una rete GSM gestita da un unico operatore e relativa ad un area di servizio contenuta entro I confini di un unico paese. Più PLMN concorrenti possono esistere in ogni singolo Paese. Un utente deve attivare un contratto con (almeno) una PLMN: Questa prende il nome di Home-PLMN; quando l'utente riceve servizio da un'altra PLMN, questa si chiama Visited-PLMN

Personal Information Management (PIM) – L'insieme di dati come rubrica, calendario, note, memo, che possono essere sincronizzati su un personal computer.

Short Message Service (SMS) – Servizio che consente di inviare dei brevi messaggi di testo attraverso la rete GSM. Ogni messaggio ha una dimensione fissa di 140 byte, ciò si traduce in pratica nella possibilità di usare 160 caratteri di testo (a 7 bit).

Simple Mail Transfer Protocol (SMTP) – Protocollo usato per traferire messaggi di posta elettronica mail su internet.

Subscriber Identity Module (SIM) – una smart card specializzata per essere usata nelle reti GSM.

UMTS Subscriber Identity Module (USIM) – Un modulo simile alla SIM per le reti GSM/GPRS, ma con caratteristiche compatibili alle reti 3G .

Universal Mobile Telecommunications System (UMTS) – Una tecnologia mobile di terza generazione (3G) successore di GSM.

Universal Serial Bus (USB) – Una interfaccia hardware per periferiche a bassa velocità come tastier, mouse, joystick, scanner, stampante.

Memoria volatile – memoria che perde il suo contenuto quando viene a mancare l'alimentazione.

Wireless Application Protocol (WAP) – Uno standard che definisce il modo nel quale le comunicazioni internet sono fornite su un dispositivo mobile.

Wireless Fidelity (WiFi) – Un termine che descrive una rete wireless locale che osserva il protocollo IEEE 802.11.

11. BIBLIOGRAFIA

11.1 ARTICOLI DI RIFERIMENTO

Questo lavoro è basato sui seguenti articoli:

Wayne Jansen, Rick Ayers, Guidelines on Cell Phone Forensics, NIST SP 800-101, May 2007.
http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf

Wayne Jansen, Aurelien Delaitre, Forensic Protocol Filtering of Phone Managers, International Conference on Security and Management (SAM'08), July 2008.
http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_forensics/PM-Protocol-Filtering-FINAL-formatted-e.pdf

11.2 RIFERIMENTI NEL DOCUMENTO

[ACPO] Good Practice Guide for Computer-based Electronic Evidence, Association of Chief Police Officers, Version 3, http://www.devon-cornwall.police.uk/v3/pdfstore/ElecEvid.pdf

[DOJ01] Electronic Crime Scene Investigation: A Guide for First Responders, U.S.Department of Justice, NCJ 187736, July 2001, http://www.ncjrs.org/pdffiles1/nij/187736.pdf

[DOJ04] Forensic Examination of Digital Evidence: A Guide for Law Enforcement, U.S. Department of Justice, NCJ 199408, April 2004, http://www.ncjrs.org/pdffiles1/nij/199408.pdf

[EDFM] Mark Reith, Clint Carr, and Gregg Gunsch, An Examination of Digital Forensic Models, International Journal of Digital Evidence, Fall 2002, Volume 1, Issue 3, *http://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf*

[IOCE] Digital Evidence: Standards and Principles, Scientific Working Group on DigitalEvidence (SWGDE), International Organization on Computer Evidence (IOCE),Forensic Science Communications, Vol. 2, No. 2, April 2000, http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

[Oco04] Thomas R. O'connor, Admissibility of Scientific Evidence Under Daubert, North Carolina Wesleyan College, March 2004.

[USIM] Definizione USIM
http://it.wikipedia.org/wiki/Universal_Subscriber_Identity_Module
http://www.3gpp.org/ftp/Specs/html-info/31102.html

[WWW] Alcuni esempi di siti web per l'identificazione di telefonini a partire dalle caratteristiche fisiche del dispositivo:
http://www.phonescoop.com/phones/finder.php
http://www.gsmarena.com/search.php3

11.3 Riferimenti Appendice

Elenco e descrizione delle cartelle contenute in C:\Private
http://www.ipmart-forum.it/showthread.php?t=20591

Guida a RomPatcher
http://www.nokioteca.net/home/forum/index.php?showtopic=11661

Formato dei messaggi su Symbian con una interessante discussione in cui viene illustrato uno script java che cerca di leggere il file index
http://jumpjack.wordpress.com/2008/02/02/symbian-messages-format-before-9x-version/

Articolo che tratta la realizzazione di programmi C++ per Symbian che si occupano di manipolare gli sms
http://jumpjack.wordpress.com/2007/01/22/appunti-di-gestione-sms-in-symbian-c/

Symbian 7.0 Developer Guide relativa all'oggetto TMsgEntry

http://www.symbian.com/developer/techlib/v70sdocs/doc_source/reference/cpp/MessagingArchitecture/TMsvEntryClass.html#%3a%3aTMsvEntry

12. APPROFONDIMENTI WEB

- Domenico Vulpiani, "La criminalità informatica: metodi d'indagine e la collaborazione delle aziende bancarie", Luglio 2002
  - http://www.marcodimartino.it/documenti/pdf/Vulpiani_Criminalita_informatica_metodi_dindagine.pdf
- Sono presenti una lista di 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

Siti web consigliati :

- http://www.e-evidence.info/n.html
- http://www.mobileforensicsworld.com/
- http://www.mobileforensicsinc.com/

Molte definizioni sono state prese da :

- http://wikipedia.it