

ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

SCUOLA DI SCIENZE
Corso di Laurea Magistrale in Scienze di Internet

Metodologie e tecniche per l'analisi forense di dispositivi di telefonia mobile

Tesi di Laurea in Sistemi e reti wireless

Relatore:
Chiar.mo Prof.
LUCIANO BONONI

Presentata da:
MARIAGRAZIA CINTI

Correlatori:
Chiar.mo Prof.
CESARE MAIOLI

Dott.
MICHELE FERRAZZANO

Sessione III
Anno Accademico 2012/2013

A Riccardo

Introduzione

La quotidianità di ogni individuo è oggi scandita dalla continua interazione con una serie di tecnologie, che vanno a costruire intorno alla persona un vero e proprio ecosistema informatico. In tale ambito, qualora fosse ad esempio necessario indagare sull'attuazione di un crimine, si rivela di fondamentale importanza l'intervento delle scienze forensi digitali. Tali discipline si occupano infatti di raccogliere qualunque elemento informatico che possa essere di qualche interesse per il sistema legale, nel pieno rispetto della sua natura e senza che le sue caratteristiche vengano alterate in nessun modo; così facendo si garantisce il valore probatorio dell'informazione raccolta e la sua ammissibilità in giudizio. La complessità dello scenario in cui vanno ad agire gli operatori forensi deriva dalla diffusione capillare di dispositivi con le più varie caratteristiche. Quando tali *device* sono portatili e lontani dalla classica concezione di sistemi informatici entrano in scena le metodologie dalla *mobile device forensics*, disciplina che delinea la corretta gestione dei reperti informatici portatili. Anche in tale contesto si attua l'analisi forense dei reperti: una serie di procedure che riguardano l'acquisizione e l'estrazione di dati che possano essere di qualche interesse per il caso in oggetto.

Scopo di questa tesi è quello di chiarire le modalità di intervento sui dispositivi portatili, con particolare riferimento a quelli di telefonia cellulare mobile. Inoltre, tramite il progetto in essa documentato, si vogliono esplorare le possibilità e i limiti di alcune metodologie; saranno comparati i risultati acquisiti attraverso alcuni *tool* forensi, in grado di attuare estrazioni logiche

e fisiche dei dati, e quelli ottenuti grazie a pratiche non forensi.

Nel capitolo iniziale verrà illustrato il ruolo delle scienze forensi digitali, discipline che hanno lo scopo di raccogliere e gestire propriamente i dati digitali; in particolar modo verranno definiti gli ambiti e l'evoluzione della *computer forensics* e della *mobile device forensics*. Saranno poi esposte le principali criticità legate al rinvenimento di evidenze digitali, relativamente alle fasi di conservazione del reperto, di acquisizione dei dati e della loro conseguente analisi. Infine saranno introdotte le ISO IEC 27037, linee guida che regolamentano le procedure operative.

Nel secondo capitolo verrà delineato brevemente il percorso di formazione di un'evidenza digitale. Verranno fornite nozioni di base sullo svolgimento del processo penale in Italia e quindi descritti gli strumenti a disposizione delle parti per acquisire informazioni in grado di consentire la corretta valutazione degli eventi, ad opera dell'autorità giudiziaria. Nella seconda parte di tale capitolo sarà poi illustrata la normativa vigente in Italia, in riferimento agli aspetti che possono essere di qualche rilevanza per le indagini.

Nel terzo capitolo verrà trattata l'architettura dei diversi tipi di dispositivi di telefonia mobile, in termini di caratteristiche hardware e software. In particolare verranno approfonditi temi come la gestione della memoria e la diversità tra connettori.

Nel quarto capitolo verranno approfonditi aspetti legati alla rete cellulare, per meglio comprendere come avviene la comunicazione nei più diffusi sistemi europei: GSM, GPRS e UMTS. Verranno spiegate le tre diverse architetture e saranno affrontati temi quali copertura e mobilità su rete cellulare, parlando dei meccanismi di *handover* (o *handoff*) e di *roaming* che assicurano rispettivamente la mobilità intra-rete e inter-reti.

Nel quinto capitolo si entrerà nel vivo della tecnica, approfondendo i diversi livelli esistenti di acquisizione dati. Esistono infatti numerose metodologie che possono essere classificate in base al livello di conoscenza e tecnica necessarie, di invasività e di costo.

Nel sesto capitolo si approfondiranno le caratteristiche dei sistemi operativi

Android e iOS e verranno illustrate alcune procedure invasive non forensi per accedere ai dati dell'intero file system abilitando i privilegi da amministratore. Le tecniche analizzate saranno quelle di *rooting* in ambiente Android e di *jailbreaking* per i sistemi iOS.

Nel capitolo finale verrà illustrato lo studio che è stato effettuato: ne verranno descritti gli elementi, le fasi e le problematiche riscontrate. Saranno infine mostrati e comparati i risultati raccolti.

Indice

Introduzione	iii
1 Il ruolo delle scienze forensi digitali	1
1.1 Il dato digitale	1
1.2 Le scienze forensi digitali	2
1.2.1 Computer forensics	2
1.2.2 Mobile device forensics	4
1.3 Rinvenimento di evidenze digitali	5
1.3.1 Criticità legate alla preservazione del reperto	7
1.3.2 Criticità legate all’acquisizione dei dati	11
1.3.3 Criticità legate all’ispezione e all’analisi dei dati	12
1.4 Standard internazionali di riferimento	14
1.4.1 ISO IEC 27037/2012	14
2 Evidenze digitali nell’ambito del processo penale italiano	17
2.1 Il processo penale: definizione dei suoi elementi	17
2.1.1 Mezzi di prova	18
2.1.2 Mezzi di ricerca della prova	18
2.1.3 Accertamenti tecnici	20
2.2 Ratifica della Convenzione di Budapest	21
2.2.1 Effetti della ratifica	22
2.3 Normativa sul trattamento dei dati personali	23
2.3.1 Codice della privacy	23
2.3.2 Delibere del Garante della privacy	23

3	Architettura dei dispositivi di telefonia mobile	25
3.1	Evoluzione del mercato della telefonia	25
3.2	Comparazione dei dispositivi	26
3.2.1	Panoramica sulle caratteristiche software	26
3.2.2	Panoramica sulle caratteristiche hardware	28
3.3	Memoria interna	30
3.3.1	Configurazioni	30
3.3.2	Dati acquisibili	31
3.4	Periferiche di memorizzazione	32
3.4.1	Dati acquisibili	33
3.5	Cablaggi e connettori	33
4	Architettura della rete cellulare	35
4.1	Evoluzione dei sistemi di telefonia	35
4.1.1	Nascita di GSM	36
4.1.2	Nascita di UMTS	37
4.1.3	Panoramica italiana	37
4.2	Funzionamento e componenti della rete	37
4.2.1	Le stazioni mobili (MS)	38
4.2.2	Componenti dell'architettura GSM	40
4.2.3	Componenti dell'architettura GPRS	43
4.2.4	Componenti dell'architettura UMTS	44
4.3	Copertura e mobilità	46
4.3.1	Propagazione del segnale	47
4.3.2	Handover	48
4.3.3	Roaming	51
4.4	Localizzazione a fini investigativi	52
5	Metodologie e strumenti per la mobile device forensics	53
5.1	Livelli di analisi	53
5.2	Metodologie di acquisizione dei dati	55
5.2.1	Estrazione manuale	55

5.2.2	Estrazione logica	56
5.2.3	Estrazione fisica (hex dump)	57
5.2.4	Esportazione dei chip (chip-off)	57
5.2.5	Micro lettura	58
5.3	Strumenti per l’acquisizione dei dati	59
6	Procedure invasive per l’analisi forense di Android e iOS	61
6.1	Acquisizione mediante rooting	62
6.1.1	Nozioni generali sul sistema operativo Android	62
6.1.2	Ottenimento dei diritti di root	64
6.1.3	Acquisizione	65
6.1.4	Analisi dei file di interesse	66
6.2	Acquisizione mediante jailbreaking	66
6.2.1	Nozioni generali sul sistema operativo iOS	66
6.2.2	Rimozione dei meccanismi “di jail”	69
6.2.3	Acquisizione	70
6.2.4	Analisi dei file di interesse	71
7	Risultati ottenuti con metodologie finalizzate all’analisi fo- rense	73
7.1	Presentazione dello studio	73
7.1.1	Device analizzati	73
7.1.2	Software utilizzati	74
7.2	Attuazione dei test	78
7.2.1	Test su device1 (Android)	78
7.2.2	Test su device2 (iOS)	81
7.3	Presentazione dei risultati	87
7.3.1	Risultati acquisizione device 1 (Android)	87
7.3.2	Risultati acquisizione device 2 (iOS)	91
	Conclusioni	98
	Bibliografia e sitografia	99

Elenco delle figure

1.1	Fasi comuni alle scienze forensi digitali	6
3.1	Comparazione caratteristiche software device. Fonte: [ABJ13]	27
3.2	Comparazione caratteristiche hardware device. Fonte: [ABJ13]	28
3.3	Tipologie di configurazione della memoria. Fonte: [ABJ13] . .	31
3.4	Connettori più diffusi: <i>micro USB, mini USB, 30-pin dock e Lightning</i>	34
4.1	Formati delle UICC	39
4.2	Architettura della rete GSM. Fonte: [D'A06]	41
4.3	Architettura della rete GPRS. Fonte: [D'A06]	44
4.4	Architettura della rete UMTS. Fonte: [D'A06]	45
4.5	Suddivisione territoriale in celle. Fonte: [ERti]	46
5.1	Livelli di analisi per la mobile device forensics. Fonte: [ABJ13]	54
5.2	Base di lavoro per acquisizioni manuali. Fonte: [Fer]	59
5.3	Programmatori per l'acquisizione di chip. Fonte: [Swa12] . . .	60
6.1	Architettura del sistema operativo Android.	63
6.2	Architettura del sistema operativo iOS.	67
7.1	Device analizzati: <i>Vodafone 858 Smart e Apple iPhone 3GS</i> .	74
7.2	Software forensi utilizzati.	76
7.3	Shell di ADB	80
7.4	Struttura di una tabella del database <code>mmssms.db</code>	81

7.5	File contenuti nella cartella di backup	83
7.6	Software utilizzati per navigare ed estrarre i file di backup . . .	84
7.7	Directory di iOS copiate tramite SFTP	86

Elenco delle tabelle

7.1	Quantità dati estratti per modalità di acquisizione (Android) .	89
7.2	Percorsi di estrazione dati (Android)	90
7.3	Quantità dati estratti per modalità di acquisizione (iOS) . . .	92
7.4	Percorsi di estrazione dati (iOS)	93

Capitolo 1

Il ruolo delle scienze forensi digitali

1.1 Il dato digitale

La maggior parte delle nostre azioni quotidiane prevede l'uso di sistemi o dispositivi informatici. Da queste interazioni vengono generati dati digitali, entità estremamente delicate, afflitte da tutta una serie di problematiche di natura metodologica. Durante il trattamento dei dati è necessario essere rigorosi dal punto di vista tecnico, e la loro raccolta, come l'analisi, deve essere fatta solo ricorrendo a procedure verificabili e ripetibili; l'acquisizione del dato deve essere completa in modo da garantire la sua integrità, inoltre la sua paternità, e quindi provenienza, deve essere certa e dimostrabile. Altri problemi sono relativi alla sua natura fisica, dal momento che il dato necessita sempre di un supporto di memorizzazione, ha una riproducibilità infinita e per sua natura è volatile, facilmente modificabile e deteriorabile.

I dispositivi mobili di cui ci circondiamo sono idonei ad ospitare una considerevole varietà e quantità di dati. Inoltre, intuitivamente, più tempo un determinato dispositivo resta in possesso di una persona, più informazioni finirà per contenere sulla stessa.

Genericamente queste informazioni personali possono essere classificate in:

- Informazioni relative alle azioni dell'utente, come ad esempio quelle contenute nel registro chiamate, i messaggi inviati e ricevuti, etc.
- Informazioni contenute nel dispositivo, come ad esempio la rubrica, le fotografie, i video, etc.

Entrambe le tipologie sono comunque generate da un'interazione ed egualmente possono essere di qualche utilità per ricostruire una situazione in fase di indagine.

1.2 Le scienze forensi digitali

Le scienze forensi digitali, dall'inglese *digital forensics*, sono quelle discipline che si occupano dell'ottenimento, della preservazione, dell'analisi e della documentazione delle evidenze digitali, anche dette prove. Queste possono essere rinvenute su qualunque dispositivo elettronico, come ad esempio computer, smartphone, fotocamere o qualsiasi altro strumento di memorizzazione. A seconda dell'oggetto da analizzare ci si indirizza alle metodologie di una materia specifica, come ad esempio la *computer forensics* quando occorre agire su computer o server e la *mobile device forensics* per ciò che concerne i *device* portatili di qualunque genere.

1.2.1 Computer forensics

La computer forensics, nota in Italia col nome di *informatica forense*, si occupa del rinvenimento di evidenze digitali su computer, server, e più in generale su sistemi informatici. Concerne quindi la protezione, la conservazione, l'identificazione, l'estrazione e l'interpretazione dei dati, quando questi sono memorizzati su supporti informatici. Condivide con le altre scienze forensi l'obiettivo di riuscire a raccogliere informazioni che abbiano valore probatorio e che quindi possano validamente essere utilizzare in sede giudiziaria.

Per questo motivo tali operazioni dovrebbero essere svolte con rigore e nel rispetto delle *best practices* esistenti: deve essere sempre garantita l'esattezza della prova e la ripetibilità delle procedure.

Nascita ed evoluzione della disciplina

La computer forensics nacque e vide la sua prima applicazione nei Paesi di origine anglossassone, in particolar modo negli Stati Uniti. Iniziò a svilupparsi a partire dagli anni '80 per rispondere alla necessità sempre più pressante di riuscire a contrastare i reati connessi all'informatica. Proprio in quegli anni infatti il grande pubblico iniziava ad interessarsi ai personal computer, il cui successo andava di pari passo con la loro diffusione. Dal momento che le forze di polizia si trovavano sempre più spesso a dover affrontare strumenti informatici per raccogliere dati utili alle indagini, si giunse alla conclusione che fosse opportuno formare degli agenti con specifiche competenze. La prima organizzazione investigativa che attuò concretamente tale proposito fu l'FBI, la quale istituì nel 1984 il CART¹.

Un altro importante passo fu la definizione di linee guida procedurali. Ciò avvenne per la prima volta nel 1994 ad opera del *Dipartimento di Giustizia degli Stati Uniti* che divulgò un documento che introduceva degli standard sulle modalità operative. Le innovazioni procedurali introdotte impiegarono anni per varcare i confini degli Stati Uniti, ma gradualmente ci riuscirono, soprattutto grazie alle conferenze internazionali che iniziarono a tenersi in quegli anni.

La situazione italiana

In Italia iniziative legate alla computer forensics videro la luce con oltre un decennio di ritardo, a partire cioè dalla seconda metà degli anni '90. Il primo reparto specializzato, istituito nel 1996, fu il *Nucleo Operativo di Polizia delle*

¹Acronimo di *Computer Analysis and Response Team*. Questo reparto è attivo ancora oggi e nel solo anno fiscale 2012 ha condotto 13300 perizie che hanno riguardato circa 10500 TB di dati.

Telecomunicazioni. Successivamente il reparto conflù all'interno del *Servizio di Polizia Postale e delle Telecomunicazioni*.

Parallelamente in quegli anni iniziarono a nascere anche i primi laboratori privati specializzati in ambito di sicurezza informatica.

1.2.2 Mobile device forensics

La mobile device forensics (spesso erroneamente definita con *mobile phone forensics*) si occupa del recupero di evidenze digitali da dispositivi portatili come ad esempio telefoni cellulari e smartphone. Rispetto alla computer forensics tratta strumenti per cui devono essere presi accorgimenti particolari di conservazione, in quanto essi possono subire alterazioni anche solo se spostati senza le dovute precauzioni.

La disciplina trova attualmente un'ampia applicazione, dal momento che un consumatore medio possiede ed utilizza personalmente molti dei seguenti media:

- Telefono cellulare;
- Lettore MP3;
- Fotocamera digitale;
- Tablet;
- Memoria USB esterna.

Tutti questi oggetti contengono dati che potenzialmente un tecnico forense potrebbe decidere di analizzare. La più grande sfida in tale ambito è sicuramente quella di mantenere il passo con mercati che danno vita a dispositivi sempre più avanzati, in cui le ultime generazioni si discostano anche di moltissimo dalle precedenti. Ne offre senz'altro un esempio il mercato dei dispositivi di telefonia cellulare che comprende attualmente device di categorie molto diverse: cellulari di base, telefoni con funzionalità avanzate e smartphone.

Evoluzione della disciplina

La mobile device forensics è una disciplina che si è sviluppata abbastanza recentemente, dall'inizio degli anni 2000, per riuscire a gestire una diffusione sempre più rapida dei dispositivi cellulari: pensiamo ad esempio che sul solo suolo italiano, durante il 2012 abbiamo assistito ad un aumento del 35% degli smartphone connessi ad internet (21 milioni di italiani con età compresa tra gli 11 e i 74 anni) e del 160% dei tablet (6 milioni di utilizzatori)².

Dal momento che sono disponibili dispositivi mobili con funzionalità sempre più avanzate e che viene garantita un'interoperabilità altissima tramite rete telefonica e internet, è ovvio che questi strumenti siano coinvolti nell'attuazione di crimini, sia tradizionali che strettamente informatici. Ne consegue che le informazioni in essi contenute possano essere di particolare interesse per qualunque tipo di indagine. Operativamente esistono diverse metodologie praticabili per ottenere le informazioni memorizzate: tali procedure saranno approfondite nei prossimi capitoli.

1.3 Rinvenimento di evidenze digitali

Una buona definizione di prova digitale, o evidenza digitale, può essere quella data dal IOCE³ nel 2000 [Vac12], la quale definisce una *electronic evidence* come:

un'informazione generata, memorizzata o trasmessa attraverso dispositivi elettronici, che può avere valore in tribunale.

Stiamo quindi parlando di qualunque dato digitale che abbia valore probatorio e che quindi possa essere utilizzato dall'autorità giudiziaria per valutare gli eventi.

²Ad ottobre 2013 - statistiche Audiweb

³International Organization on Computer Evidence

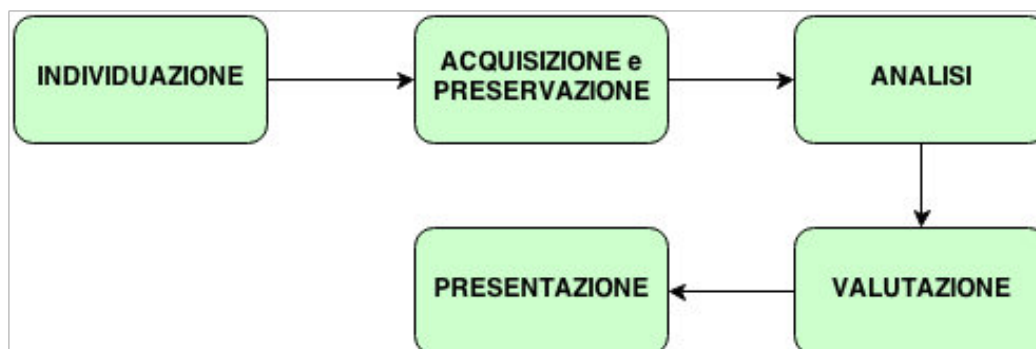


Figura 1.1: Fasi comuni alle scienze forensi digitali

Durante lo svolgimento di indagini giudiziarie si susseguono diverse fasi operative [Figura 1.1], comuni a tutte le scienze forensi, che hanno l'obiettivo ultimo di raccogliere e presentare in tribunale tutte le evidenze digitali utili al caso in esame. Queste fasi sono:

1. **Individuazione** - avviene in corrispondenza dell'analisi alla scena del crimine. Consiste nell'identificazione di qualunque dispositivo che possa contenere al suo interno dati rilevanti.
2. **Acquisizione e preservazione** - consiste di fatto in una serie di procedure consolidate (best practices) da seguire per garantire i migliori risultati possibili in termini di integrità e disponibilità dei dati. Le operazioni da mettere in atto dipendono strettamente dalle caratteristiche e dallo stato in cui il dispositivo è rinvenuto, ad esempio se questo è acceso o spento. Nel primo caso si parla di *live forensics*, nel secondo di *post mortem forensics*. Attuato il sequestro del dispositivo o la raccolta dei dati in esso contenuti, deve conseguire la conservazione del reperto o dei supporti tramite la predisposizione di una corretta catena di custodia.
3. **Analisi** - consiste nell'estrazione dei dati più significativi.

4. **Valutazione** - in questa fase si ricostruisce il contesto in cui sono stati memorizzati i dati estratti e si valuta se le informazioni raccolte siano pertinenti al caso in oggetto.
5. **Presentazione** - è una fase cruciale: rappresenta il momento in cui i periti devono spiegare e far comprendere ai non addetti ai lavori ciò che è stato fatto. Si attua tramite la redazione di un documento in cui sono riportate passo passo tutte le operazioni eseguite nonché i risultati ottenuti.

Ognuna delle fasi appena citate è di per sé estremamente delicata e non priva di criticità. Entriamo più nello specifico.

1.3.1 Criticità legate alla preservazione del reperto

Le best practices da adottare in questo contesto dipendono dallo stato in cui è rinvenuto il dispositivo da analizzare. Un intervento di live forensics si rivela necessario in presenza di:

- Sistemi fisicamente inamovibili;
- Sistemi che hanno la necessità di essere alimentati costantemente o che non possono essere spenti (ad esempio sistemi militari, medicali, di videosorveglianza, server di hosting, housing, database condivisi, etc.);
- Sistemi che non possono essere acquisiti nella loro interezza;
- Sistemi che conservano al loro interno informazioni volatili - quando queste sono rilevanti ai fini dell'indagine;
- Sistemi con volumi cifrati;
- Dispositivi di telefonia cellulare rinvenuti accesi.

In particolar modo negli ultimi due casi, è buona norma non spegnere i dispositivi dal momento che potrebbero verificarsi problemi durante la successiva riaccensione, come ad esempio la richiesta di inserire informazioni di sblocco (pin, password, etc.) non fornite dagli indagati.

Isolamento da connettività generica e cellulare

Per lo spostamento dei dispositivi di telefonia mobile rinvenuti accesi occorre predisporre velocemente una catena di custodia che inibisca i collegamenti con la rete cellulare [Capitolo 4]. Infatti utilizzando impropriamente tali strumenti o attuando procedure non corrette potrebbero verificarsi perdite di dati potenzialmente importanti. Per evitare problematiche di questo tipo esistono diverse tecniche di isolamento radio [Ate11]:

- **Attivazione di “airplane mode” o “radio off”** - è l’azione più semplice da compiere, si tratta di una configurazione che disattiva tutte le connessioni wireless. La sua affidabilità deve essere valutata specificamente caso per caso. Esiste anche l’alternativa, meno pratica, di spegnere le singole connessioni tramite le voci del menu.
- **Utilizzo di un’area di lavoro schermata** - accorgimento attuabile in sede di analisi forense.
- **Utilizzo di tende o borse di Faraday** - alternativa economica rispetto alla precedente che garantisce la portabilità dei reperti. In questo contesto si ha il problema della gestione dei cablaggi, che devono essere opportunamente isolati per non vanificare l’utilizzo di questi strumenti. Manipolare i dispositivi conservati all’interno di questi contenitori risulta fisicamente poco agevole.
- **Utilizzo di contenitori schermati** - si tratta di un compromesso tra le alternative precedenti, che riduce la portabilità ed è più costoso, ma consente l’opportuno isolamento dei cavi e una migliore manipolazione dei dispositivi contenuti.
- **Utilizzo di dispositivi di jamming o spoofing** - strumenti che emettono segnale in grado di inibire quello delle connessioni da gestire. Il *jammer* [Paragrafo 1.3.1] genera rumore che si va a sovrapporre a quello della connettività. Lo *spoofers* invia al dispositivo un falso segnale di “servizio non disponibile”.

- **Utilizzo di (U)SIM forensi sostitutive** - questo caso è specifico per la limitazione della connettività cellulare (fonia e dati). Questi accessori, eventualmente creati clonando le SIM-card originali, forzano il dispositivo a credere di star operando con la SIM-card originale: ne mantengono l'operatività ma impediscono al device di autenticarsi alla rete cellulare. Questo metodo offre vantaggi legati alla portabilità ma implica la manipolazione diretta del reperto e lo spegnimento del dispositivo.
- **Cooperazione col provider di connettività** - anche questo caso, come il precedente, è specifico per la limitazione della connettività cellulare (fonia e dati). Ove possibile si può richiedere al provider di disabilitare tali servizi in determinati luoghi o per certi dispositivi. Tale metodo non è immediato, per via dei tempi di contatto e di risposta del provider, e comporta la manipolazione diretta del device.

Non esiste una modalità operativa di per certo migliore di altre, presentano tutte degli inconvenienti: mantenendo i dispositivi accesi e isolati dalla rete si verificherà un maggior consumo di batteria, in quanto i telefoni proveranno ripetutamente a connettersi ad una rete; abilitando l'airplane mode o sostituendo la SIM-card si dovrà manipolare direttamente il dispositivo, esponendolo in questo modo a rischi molto alti di alterazione.

Limitazioni all'uso di strumenti di jamming

Il *jammer*, o disturbatore di frequenze, è un prodotto in grado di inibire il segnale radio generato da qualunque tipo di connessione, con un raggio d'azione che può andare da qualche metro fino a diversi chilometri. Il suo principio di funzionamento è semplice e si basa sull'idea di riprodurre un segnale portante sull'intera banda utilizzata dai canali di comunicazione. Qualunque dispositivo che si trovi nelle immediate vicinanze e che lavori sulle frequenze comprese in questo range viene disturbato.

Il suo utilizzo è controverso e precisamente normato dalle legislazioni vigenti: usarlo, o anche solo detenerlo, è vietato in molti Paesi della Comunità europea, nonchè in Italia dove si fa riferimento agli artt. 340, 617 e 617 bis del Codice Penale:

Art. 340

“Chiunque, fuori dei casi preveduti da particolari disposizioni di legge, cagiona una interruzione o turba la regolarità di un ufficio o servizio pubblico o di un servizio di pubblica necessità, è punito con la reclusione fino a un anno. [...].”

Art. 617

“Chiunque, fraudolentemente, prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce è punito con la reclusione da sei mesi a quattro anni. [...].”

Art. 617 bis

“Chiunque, fuori dei casi consentiti dalla legge, installa apparati, strumenti, parti di apparati o di strumenti al fine di intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni. [...].”

Spegnimento o mantenimento della carica della batteria

Talune volte lo spegnimento del dispositivo potrebbe essere l'unica soluzione praticabile. Lo stato di alimentazione della batteria è un indicatore molto importante, e un dispositivo per essere isolato elettromagneticamente dovrebbe essere completamente carico. Se così non fosse, bisognerebbe se non altro dotare il dispositivo di un sistema di alimentazione portatile (almeno durante il trasporto, per poi provvedere ad un'alimentazione standard quando il dispositivo raggiungerà una sede stabile) che salvaguardi l'esaurimento

della batteria. Non sempre ciò è possibile, e quindi si dovrebbe considerare lo spegnimento come una possibile opzione. Questa procedura dovrebbe essere eseguita documentando con precisione lo stato corrente del dispositivo e annotando data ed ora dello spegnimento. Statisticamente la possibilità di incontrare un meccanismo di protezione al momento della successiva riaccensione è abbastanza bassa, quindi in certi casi tale misura viene raccomandata. È essenziale prestare attenzione alle caratteristiche del dispositivo principale e di quelli annessi (memorie, UICC, etc.) e verificare se sul luogo dell'indagine sono presenti eventuali periferiche, cavi, adattatori di alimentazione o altri accessori legati al dispositivo, la cui mancanza ostacolerebbe o rallenterebbe le indagini.

1.3.2 Criticità legate all'acquisizione dei dati

Le modalità operative in cui si attua l'acquisizione di un sistema informatico o di qualunque altro dispositivo sono principalmente due: il sequestro o la duplicazione. La tecnica intrapresa più frequentemente è la prima, mentre la duplicazione tramite copie bit-a-bit è più spesso utilizzata nel caso in cui i dati risiedano su sistemi inamovibili. Ovviamente quando si ha a che fare con dispositivi portatili, gli oggetti di studio della mobile device forensic, l'acquisizione dei dati è solitamente rimandata a procedure controllate che possono essere eseguite in laboratorio, nel rispetto delle best practices forensi.

Completezza dell'acquisizione

Una delle criticità maggiori riguarda la completezza dell'acquisizione e può essere espressa da una semplice domanda: *abbiamo la certezza di poter raccogliere tutti i dati utili da un dispositivo?* La risposta raramente è positiva, dal momento che la qualità e quantità dei dati estrapolabili dipende strettamente dal modello del dispositivo, e che la varietà di device presenti sul mercato è oltremodo ampia.

Tool per la generazione di copie forensi

Esistono ovviamente dei tool che permettono di creare copie forensi (le già menzionate copie bit-a-bit), ma non esiste una sola *suite* che possa essere utilizzato per eseguire copie di tutti i tipi di cellulari disponibili sul mercato. A seconda del dispositivo coinvolto nelle indagini sarà necessario indirizzarsi ad uno specifico software.

Inoltre è opportuno ricordare che questi tool sono sviluppati da aziende software e non dagli stessi produttori dei dispositivi, i quali molto spesso, sono gli unici ad avere una conoscenza piena e completa dei loro prodotti. È quindi impossibile garantire che siano estrapolate tutte le informazioni che l'utente ha impresso sul dispositivo, dal momento che non si sa esattamente quanto in là ci si possa spingere per cercarle.

1.3.3 Criticità legate all'ispezione e all'analisi dei dati

Anche in questa fase dobbiamo porci una domanda: *siamo sicuri che l'analisi svolta sui dati del dispositivo sia esaustiva?* La risposta è quasi sempre negativa, non possiamo essere certi dell'eshaustività delle procedure svolte in quanto non esiste un modo univoco di ottenere tali informazioni.

Le scienze forensi digitali hanno la necessità di evolvere velocemente, per mantenere il passo con i prodotti distribuiti. Le software house produttrici di tool forensi, in egual modo, provano a mantenere questi ritmi, ma molto spesso i migliori risultati su un dispositivo di ultima generazione si ottengono sperimentando e utilizzando metodi non convenzionalmente forensi, piuttosto che ricorrendo a versioni aggiornate dei tool.

Prendono quindi pratica comune nella disciplina anche le più varie tecniche di estrazione dei dati proprie dell'informatica, purchè queste soddisfino in generale dei criteri di affidabilità, come ad esempio quelli proposti dalla sentenza Daubert: [O'C04] [DCN07]

- **Verificabilità del metodo** - se può essere controllato mediante esperimenti;

- **Falsificabilità** - la teoria scientifica deve essere sottoposta a tentativi di falsificazione i quali, se hanno esito negativo, la confermano nella sua credibilità;
- **Sottoposizione al controllo della comunità scientifica** - si chiede che il metodo sia reso noto tramite riviste specializzate in modo da essere controllato dalla comunità scientifica;
- **Conoscenza del tasso di errore** - è nota la percentuale di errore accertato o potenziale che il metodo comporta;
- **Generale accettazione** - da parte della comunità degli esperti;
- **Credibilità** - gli esperti chiamati ad eseguire le procedure dovrebbero essere qualificati ed avere credibilità presso la comunità scientifica;
- **Chiarezza** - le tecniche usate dovrebbero poter essere spiegate con sufficiente chiarezza e semplicità a coloro che sono chiamati a giudicare.

Selezione del tool o della tecnica

In generale i criteri per determinare i tool di intervento più appropriati riprendono quelli appena introdotti, e sono:

- **Usabilità e comprensibilità** - la capacità di un tool di presentare i dati in una forma che sia significativa per gli investigatori e che renda immediatamente evidenti gli elementi incriminanti o disculpanti per l'imputato;
- **Accuratezza e verificabilità** - la qualità dell'output deve essere verificata e si deve conoscere il suo margine d'errore. Inoltre deve essere possibile verificare l'operato del tool avendo accesso a rappresentazioni intermedie dei risultati;
- **Determinismo** - deve essere possibile, partendo dal medesimo input, generare più volte lo stesso output.

1.4 Standard internazionali di riferimento

In materia di *information technology* e di digital forensic sono stati negli anni prodotte numerose linee guide. Per quanto riguarda le procedure operative da attuare nelle prime fasi di un'indagine si deve di certo fare riferimento alle ISO IEC 27037/2012, di cui abbiamo già menzionato molte disposizioni nei paragrafi precedenti.

1.4.1 ISO IEC 27037/2012

Le ISO IEC 27037 sono delle linee guida, pubblicate nel 2012, che regolano le fasi di raccolta, acquisizione e conservazione delle evidenze digitali. Gli organi che hanno partecipato alla loro stesura sono l'ISO⁴ e lo IEC⁵, i quali si occupano rispettivamente della definizione di norme tecniche e della definizione di standard in materia di elettricità, elettronica e tecnologie correlate. Ovviamente non è l'unico standard esistente, ma è sicuramente il più ampio e specifico. Nello specifico questa documentazione concerne il trattamento del reperto informatico, e definisce una serie di linee guida da attuare nelle fasi iniziali del processo di gestione della prova informatica. Definisce cioè le metodologie da adottare per far sì che le evidenze digitali conservino la loro integrità e siano ammissibili in giudizio. Si cura di argomenti strettamente operativi, come ad esempio la documentazione dei reperti, la definizione delle priorità di intervento, l'imballaggio e il trasporto dei reperti e i ruoli delle persone coinvolte.

È importante precisare che essendo un documento di respiro internazionale non si cura degli aspetti legali, che variano di Paese in Paese, e non affronta in alcun modo il tema degli strumenti tecnici (quelli solitamente utilizzati nella fase di analisi), in quanto si occupa delle sole fasi di identificazione,

⁴International Organization for Standardization

⁵International Electrotechnical Commission

raccolta, acquisizione e conservazione; inoltre non si occupa del trattamento dei dati analogici.

Capitolo 2

Evidenze digitali nell'ambito del processo penale italiano

Sarà obiettivo di questo capitolo delineare il percorso di formazione di un'evidenza digitale nell'ambito del processo penale, definendo gli strumenti a disposizione dell'autorità giudiziaria e delle parti per la corretta valutazione degli eventi. Nella seconda parte della trattazione verrà invece descritto il panorama normativo italiano, con particolare riguardo per quanto concerne il dato informatico e i reati connessi all'informatica.

2.1 Il processo penale: definizione dei suoi elementi

In Italia lo svolgimento del processo penale e la formazione della prova sono disciplinati dall'articolo 111 della Costituzione. Le disposizioni in esso contenute mirano a garantire il giusto processo, tramite il contraddittorio tra le parti, confronto da svolgersi in condizioni di parità davanti ad un giudice *super partes*. La persona accusata deve disporre del tempo e delle condizioni necessarie a costruire la propria difesa, avendo la possibilità di acquisire ogni mezzo di prova che possa essere a suo favore. Viene inoltre definito il principio del contraddittorio nella formazione della prova, le cui eccezioni per

accertata impossibilità di natura oggettiva [accertamenti tecnici non ripetibili, Paragrafo 2.1.3] sono disciplinate dalla legge.

Il Codice di procedura penale disciplina esaustivamente i fatti che possono divenire oggetto di prova, tramite l'art.187. Il giudice non è però vincolato nelle sue scelte, dal momento che l'art.189 gli dà la possibilità di ammettere al suo giudizio qualunque elemento risulti idoneo a risalire alla verità dei fatti, senza ledere la libertà morale della persona.

2.1.1 Mezzi di prova

Lo stesso Codice disciplina, all'art.220, la perizia come uno dei mezzi di prova, ossia uno degli strumenti utilizzabili dal giudice durante il dibattimento. Tale elemento è ammesso quando si rileva la necessità di attuare acquisizioni, valutazioni o indagini che richiedano determinate competenze, in ambito tecnico, scientifico o artistico.

La perizia

Una perizia può essere disposta d'ufficio dal giudice tramite un'ordinanza motivata, nella quale vengono nominati i periti incaricati, in numero non superiore a due, e definiti gli opportuni provvedimenti per la comparizione, come disposto dall'art.224. Successivamente entrambe le parti processuali hanno facoltà di nominare i propri consulenti tecnici (art.225).

Quando non è stata disposta perizia le parti hanno comunque la possibilità di nominare i propri consulenti tecnici (art.233) allo scopo di raccogliere elementi che possano supportare le tesi di parte.

2.1.2 Mezzi di ricerca della prova

Sono precisamente disciplinati dallo stesso Codice di procedura penale anche i mezzi di ricerca della prova, ossia gli strumenti procedurali che possono

essere intrapresi al fine di individuare le fonti di prova. Queste disposizioni si rivolgono direttamente ai funzionari di Polizia Giudiziaria e ai difensori delle parti. Tali strumenti sono:

- **Ispezione** (artt.244 e seguenti) - si tratta di un accertamento che può avere ad oggetto persone, luoghi o cose. Tale procedura deve essere disposta mediante un decreto motivato dall'Autorità Giudiziaria. Dal momento che ciò comporta la violazione di alcuni dei diritti di libertà della persona sanciti dalla Costituzione, la legge prevede alcune garanzie sostanziali a loro tutela.
- **Perquisizione** (artt.247 e seguenti) - attività diretta ad individuare e acquisire il corpo del reato o cose pertinenti al reato, ovvero ad eseguire l'arresto dell'imputato o dell'evaso. La perquisizione è attuabile previo decreto motivato quando vi è un fondato motivo di trovare gli oggetti in questione. Anche in questo caso ci troviamo di fronte ad un tipo di accertamento che lede i diritti di libertà personali, per cui la legge prevede anche in questo caso alcune garanzie sostanziali. Per quanto riguarda i supporti contenenti dati digitali, la creazione di una copia conforme può avvenire in questa sede o successivamente.
- **Sequestro probatorio** (artt.253 e seguenti) - tale attività è strettamente correlata con la precedente fase di perquisizione, dal momento che riguarda il corpo del reato e le cose ad esso pertinenti; anche in questo caso è necessario un decreto motivato. Laddove non sia possibile l'intervento tempestivo dell'Autorità Giudiziaria è consentito agli ufficiali di Polizia Giudiziaria sequestrare i medesimi beni prima che essi si disperdano nelle more dell'intervento del Pubblico Ministero. Il Codice disciplina poi in modo specifico il sequestro della corrispondenza, dei titoli, dei valori, e delle somme in conti correnti.
- **Intercettazione** (artt.266 e seguenti) - attività atta a captare comunicazioni, conversazioni e altre forme di telecomunicazione informatica o telematica mediante strumenti della tecnica. Anche in questo caso vi

è una limitazione dei diritti di libertà personali (ad esempio la libertà di comunicazione del pensiero, sancita dall'art.15 della Costituzione, e la libertà domiciliare, sancita dall'art.14 della Costituzione) per cui la legge dispone precise norme procedurali per garantire la legittimità formale e sostanziale dell'attività. Vista la delicatezza dell'argomento, in tale ambito vigono sia la riserva di legge¹ sia la riserva di giurisdizione², entrambe previste dalla Costituzione.

2.1.3 Accertamenti tecnici

Durante le indagini potrebbe essere necessario eseguire accertamenti, rilievi segnaletici, descrittivi, fotografici o altre operazioni tecniche per cui sono necessarie specifiche competenze; in questo caso si procede alla nomina di un consulente tecnico. L'accertamento tecnico è lo strumento di cui si dispone in tale eventualità, che sarà attuato dal consulente tecnico incaricato. Gli elementi che egli riuscirà a rilevare, qualora siano ammessi dalla corte, diventeranno mezzi di prova [Ton12]. Nel nostro ordinamento sono previste due diverse tipologie di accertamento: l'accertamento tecnico ripetibile e quello non ripetibile.

Accertamento tecnico ripetibile

Il termine *accertamento tecnico ripetibile* inquadra tutte quelle operazioni di indagine che possono essere ripetute nel tempo senza pregiudizio della loro attendibilità [Ton12]. In tale eventualità il pubblico ministero nomina un consulente tecnico e fa svolgere l'accertamento in segreto. Il verbale dell'atto entrerà a far parte del fascicolo delle indagini.

¹Disposizione che prevede che la disciplina di una determinata materia sia regolata soltanto da una fonte di tipo primario, a garanzia dei diritti fondamentali del cittadino.

²Principio giuridico che prevede che per la disciplina di particolari ambiti possa intervenire solo ed esclusivamente l'autorità giudiziaria.

Accertamento tecnico non ripetibile

Agli artt.360 e seguenti del Codice di procedura penale è disciplinato l'accertamento tecnico non ripetibile. Quest'eventualità si verifica nel caso in cui l'esame riguardi persone, cose, luoghi, il cui stato è soggetto a modificazione oppure casi in cui l'accertamento stesso ne può determinare la modifica. In detti casi viene attribuita all'atto un'efficacia simile a quella della perizia, concordandone tra le parti il momento del suo effettivo svolgimento al fine di garantire un controllo ad opera dell'indagato.

Il Pubblico Ministero deve comunicare alle parti giorno, ora e luogo fissato per il conferimento dell'incarico, dando loro notizia della possibilità di nominare consulenti tecnici, esattamente come avviene nel caso di una perizia. I difensori e i consulenti eventualmente incaricati hanno il diritto di partecipare agli accertamenti e di formulare osservazioni e riserve.

2.2 Ratifica della Convenzione di Budapest

La *Convenzione sul cybercrime di Budapest* [EUR01] è stata aperta alla firma degli Stati membri dell'Unione Europea, i quali hanno partecipato alla sua elaborazione, e a quella degli Stati non membri, nel novembre 2001. Si tratta del primo trattato internazionale dedicato ai reati commessi tramite internet o altre reti informatiche; in particolare tratta argomenti quali la violazione del diritto d'autore, la frode informatica, la pornografia infantile e le violazioni di sicurezza della rete. Contiene inoltre una serie di misure e procedure ideate per il loro contrasto, come ad esempio quelle relative alla perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati.

Il suo principale obiettivo è quello di perseguire una politica penale comune per proteggere la società dagli atti di cybercriminalità, adottando legislazioni che siano in grado di affrontare tale fenomeno e promuovendo la cooperazione internazionale.

2.2.1 Effetti della ratifica

In Italia la Convenzione di Budapest è stata ratificata dalla Legge n.48/2008, la quale ha modificato sostanzialmente il panorama italiano che non veniva aggiornato in materia di criminalità informatica dalla Legge 547/1993³.

La ratifica è entrata in vigore il 5 aprile 2008, a seguito della pubblicazione sulla Gazzetta Ufficiale. Ha apportato modifiche al Codice penale relativamente agli articoli [Cin11]:

- Art.491 bis (documenti informatici)
- Art.244 (casi e forme delle ispezioni)
- Art.247 (casi e forme delle perquisizioni)
- Art.248 (richiesta di consegna)
- Art.254 (sequestro di corrispondenza telematica)
- Art.254bis (sequestro di dati informatici di traffico)
- Art.256 (dovere di esibizione)
- Art.259 (custodia delle cose sequestrate)
- Art.260 (sigillo elettronico o informatico e copia dei dati)
- Art.352 (perquisizioni)
- Art.353 (corrispondenza telematica)
- Art.354 (accertamenti urgenti e sequestro)

Ha inoltre apportato modifiche al Codice della privacy, relativamente al solo articolo [Cin11]:

- Art.10 (conservazione dei dati di traffico)

³Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.

2.3 Normativa sul trattamento dei dati personali

Nell'ambito delle indagini ha grande importanza la tutela dei dati personali. In Italia questo argomento è disciplinato dal Codice in materia di protezione dei dati personali, anche noto come Testo unico sulla privacy o Codice della privacy, sulla cui corretta applicazione vigila l'Autorità Garante per la protezione dei dati personali.

2.3.1 Codice della privacy

La principale fonte di tutela dei dati personali è il Codice della privacy, ossia il Decreto Legislativo 196/03. Il suo obiettivo principale è quello di garantire i diritti che ogni persona ha sui dati che la riguardano, stabilendo alcuni limiti al loro *trattamento*, definito dall'art.4 come

qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Il diritto assoluto di qualunque persona sui propri dati è riconosciuto nell'art.1 di tale Testo, il quale sancisce il diritto alla riservatezza. Scopo degli articoli seguenti è quello di evitare che il trattamento dei dati avvenga senza il consenso dell'interessato, in un modo che possa recargli pregiudizio.

2.3.2 Delibere del Garante della privacy

Il Garante per la protezione dei dati personali è l'autorità amministrativa preposta alla tutela del diritto alla riservatezza sancito nel Codice della privacy. Si tratta di un organo il cui compito principale è quello di controllare

che le operazioni di trattamento avvengano nel rispetto delle norme vigenti. Periodicamente il Garante rilascia delle linee guide che mirano a fornire indicazioni di carattere generale in relazione al trattamento dei dati personali in vari ambiti, al fine di garantire la corretta applicazione dei principi stabiliti dal Codice. Alcune delle deliberazioni che sono state emesse e che hanno importanza per l'informatica forense sono ad esempio la 46/2008⁴ (trattamento dei dati ad opera dei consulenti tecnici) e la 60/2008⁵ (trattamento dei dati durante lo svolgimento di investigazioni).

⁴Linee guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero.

⁵Codice di deontologia e di buona condotta per il trattamento dei dati personali per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria.

Capitolo 3

Architettura dei dispositivi di telefonia mobile

In questo capitolo verranno approfondite le principali caratteristiche, hardware e software, dei dispositivi di telefonia cellulare. Si cercherà di effettuare una panoramica completa, che prenda in considerazione sia i telefoni con funzioni di base che quelli più avanzati, nonché gli smartphone, che sono attualmente i dispositivi più utilizzati e diffusi a livello di mercato europeo. In particolar modo ci si focalizzerà sulle caratteristiche tecniche che possano essere di qualche interesse per l'ambito forense.

3.1 Evoluzione del mercato della telefonia

Nell'arco di un ventennio il mercato della telefonia mobile è mutato, ampliandosi talmente da prevedere oggi al suo interno un'ampia gamma di dispositivi con funzionalità diverse. Attualmente in tale mercato convivono sia strumenti con caratteristiche di base, assimilabili per funzionalità a semplici agende digitali, sia dispositivi dotati di sistemi operativi che li rendono simili, per complessità, ai personal computer.

3.2 Comparazione dei dispositivi

Possiamo riconoscere tre differenti categorie di dispositivi di telefonia cellulare:

- **Telefoni cellulari con funzionalità di base** - strumenti attraverso il quale possono essere compiute poche specifiche azioni, consentendo di fatto il solo avvio e ricezione di chiamate, la memorizzazione dei contatti e l'invio di messaggi testuali;
- **Telefoni cellulare avanzati** - strumenti che offrono caratteristiche aggiuntive rispetto ai modelli di base, solitamente legate ai servizi multimediali;
- **Smartphone** - strumenti che uniscono le funzionalità già menzionate a quelle di gestione di documenti elettronici; inoltre consentono l'esecuzione di un'ampia varietà di applicazioni specifiche.

Col passare del tempo le funzionalità proprie degli smartphone tendono a comparire nei telefoni cellulari avanzati, mentre gli smartphone vengono arricchiti da nuove tecnologie. Invece i cellulari di base, considerando che per la loro semplicità vengono utilizzati principalmente da utenti anziani, tendono ad arricchirsi di elementi che ne aumentino l'usabilità, come ad esempio tastiere e caratteri su schermo più grandi. A parte questo nuovo target in costante crescita, il loro uso è piuttosto limitato.

3.2.1 Panoramica sulle caratteristiche software

In Figura 3.1 è presentata una tabella riassuntiva delle caratteristiche generali di smartphone e cellulari avanzati (*feature phone*). I telefoni cellulari avanzati hanno tipicamente un sistema operativo chiuso di cui non sono state rese disponibili documentazioni: ciò complica particolarmente le eventuali operazioni di estrazione dei dati. Esistono numerose compagnie specializzate nello sviluppo di software *embedded* e i produttori di dispositivi avanzati

	Feature Phone	Smartphone
OS	Closed	Android, BlackBerry OS, iOS, Symbian, WebOS and Windows Phone
PIM (Personal Information Management)	Phonebook, Calendar and Reminder List	Enhanced Phonebook, Calendar and Reminder List
Applications	Minimal (e.g., games, notepad)	Applications (e.g., games, office productivity and social media)
Call	Voice	Voice, Video
Messaging	Text Messaging	Text, Enhanced Text, Full Multimedia Messaging
Chat	Instant Messaging	Enhanced Instant Messaging
Email	Via text messaging	Via POP or IMAP Server
Web	Via WAP Gateway	Direct HTTP

Figura 3.1: Comparazione caratteristiche software device. Fonte: [ABJ13]

spesso si fidelizzano con queste società per l'installazione del sistema operativo e di alcuni software generici (preinstallati) su date serie di dispositivi. Nei dispositivi smartphone è invece possibile avere sia sistemi operativi proprietari che aperti; attualmente i più diffusi sono: **Android** [Paragrafo 6.1.1], **iOS** [Paragrafo 6.2.1], **Windows Phone** e **BlackBerry OS**. Questi sistemi hanno molte più funzionalità rispetto alle controparti installate su cellulari avanzati, dato che sono spesso progettati su misura per un dato dispositivo. In alcuni casi i produttori forniscono la suite SDK¹ per lo sviluppo in quel determinato ambiente.

Entrambe le tipologie di dispositivi supportano l'inoltro di chiamate, messaggi (testuali e spesso anche multimediali) e hanno funzionalità per la gestione delle informazioni personali come ad esempio la rubrica e il calendario. In aggiunta gli smartphone hanno a disposizione un intero parco di applicazioni scaricabili da un *application store*.

¹Software Development Kit.

3.2.2 Panoramica sulle caratteristiche hardware

In Figura 3.2 proponiamo la comparazione di smartphone e cellulari avanzati (*feature phone*) a livello di caratteristiche hardware.

	Feature Phone	Smartphone
Processor	Limited Speed (~52Mhz)	Superior Speed (~1GHz dual-core)
Memory	Limited Capacity (~5MB)	Superior Capacity (~128GB)
Display	Small Size Color, 4k – 260k (12-bit to 18-bit)	Large size Color, 16.7 million (~24-bit)
Card Slots	None	MiniSDXC
Camera	Still	Still, Panoramic, and Video (HD)
Text Input	Numeric Keypad	Touch Screen, Handwriting Recognition, Built-in QWERTY-style Keyboard
Voice Input	None	Voice Recognition (Dialing and Control)
Cell Interface	Voice and Limited Data	Voice and High Speed Data (4G LTE)
Positioning	None	GPS receiver
Wireless	IrDA, Bluetooth	Bluetooth, WiFi, and NFC
Battery	Fixed/Removable, Li-Ion Polymer	Fixed/Removable, Rechargeable Li-Ion Polymer

Figura 3.2: Comparazione caratteristiche hardware device. Fonte: [ABJ13]

Esistono alcuni punti di contatto tra queste due categorie di prodotti, come ad esempio il fatto che siano dispositivi compatti, leggeri, ideati per garantire la mobilità. Inoltre le loro caratteristiche di base sono spesso confrontabili considerando che qualunque dispositivo è sicuramente dotato di [Ate11]:

- Un modulo di trasmissione radio per poter gestire i servizi di connessione alla rete cellulare [Capitolo 4];
- Un modulo per la lettura/scrittura della SIMcard;
- Un microprocessore e un processore di segnale digitale;

- Una memoria volatile RAM [Paragrafo 3.3] che contiene i dati generati durante l'utilizzo del dispositivo;
- Una memoria non volatile ROM [Paragrafo 3.3] che contiene il software di base, ossia il firmware o il sistema operativo;
- Una memoria non volatile per il salvataggio di dati e impostazioni dell'utente;
- Un microfono e uno speaker;
- Uno schermo a cristalli liquidi (LCD);
- Un qualche tipo di interfaccia hardware o meccanismo di input, come ad esempio tastiera o touchscreen);
- Una batteria ricaricabile e removibile.

I dispositivi più avanzati, che convergono verso gli smartphone, sono tipicamente più grandi rispetto a tutte le altre tipologie di telefono per supportare una maggiore risoluzione dello schermo e integrare touch-screen o tastiere QWERTY di dimensioni contenute. Dispongono di componenti ulteriori come ad esempio:

- Slot per l'utilizzo di memorie removibili in vari formati;
- Slot o interfacce per la connessione di periferiche esterne;
- Moduli per la comunicazione wireless a onde radio (WiFi, Bluetooth) o a infrarossi (IrDA);
- Un ricevitore GPS² e un giroscopio;
- Una o più fotocamere.

²Global Positioning System, sistema che consente il rilevamento della propria posizione tramite una triangolazione di più satelliti artificiali in orbita.

3.3 Memoria interna

I dispositivi mobili contengono al loro interno una combinazione di memorie volatili, i cui contenuti si perdono allo spegnimento del dispositivo, e non volatili. Un esempio di memoria non volatile è la RAM, che viene utilizzata dal sistema per caricare, eseguire e manipolare elementi del sistema operativo, applicazioni o dati. La RAM può contenere importanti informazioni, solitamente utilizzate dalle applicazioni per processare i dati, come ad esempio password, credenziali, chiavi di crittografia, dati riguardanti applicazioni e processi di sistema.

La memoria non volatile (ROM) invece è persistente e i dati in essa contenuti, solitamente file di sistema e porzioni significative dei dati dell'utente, permangono anche in mancanza di alimentazione. Esistono principalmente due tipologie di memorie flash:

- **Memorie NOR** - minimizzano il tempo di accesso per lettura/scrittura (che avviene mediante random access) e vengono utilizzate nel caso in cui si debba eseguire codice direttamente dalla memoria. Sono nate per sostituire le EEPROM [Paragrafo 4.2.1] e vengono impiegate ad esempio per contenere il firmware (che viene eseguito direttamente e non viene aggiornato frequentemente).
- **Memorie NAND** - tipologia molto diffusa, tant'è che la maggior parte degli attuali dispositivi flash (SD, MS, etc) ne fa uso. Offrono maggiori capacità di immagazzinamento e un aggiornamento rapido dei dati. Per contro sono meno stabili.

3.3.1 Configurazioni

La configurazione della memoria nei dispositivi di telefonia cellulare evolve nel tempo. Sono riconoscibili tre diverse generazioni.

Prima generazione I telefoni avanzati furono i primi dispositivi a contenere memorie flash di tipo NOR unitamente ad una memoria RAM. Questa

configurazione è nota come *di prima generazione*. I dati del sistema e dell'utente vengono conservati nella NOR e poi copiati in RAM durante l'avvio per un'esecuzione più celere del codice.

Seconda generazione Con l'avvento dei dispositivi smartphone si è giunti ad una nuova configurazione (*di seconda generazione*), la quale aggiunge una memoria flash di tipo NAND. In tale scenario i dati del file system vengono salvati nella NOR, i dati dell'utente nella NAND e la RAM è utilizzata per l'esecuzione del codice.

Terza generazione Esiste poi una configurazione *di terza generazione*, in rapida diffusione negli smartphone di più recente produzione. In questo caso si ha solo una memoria NAND e una RAM: ciò consente di aumentare la velocità e la densità dei dati, riducendo i costi.

In Figura 3.3 sono presentate le tre configurazioni.

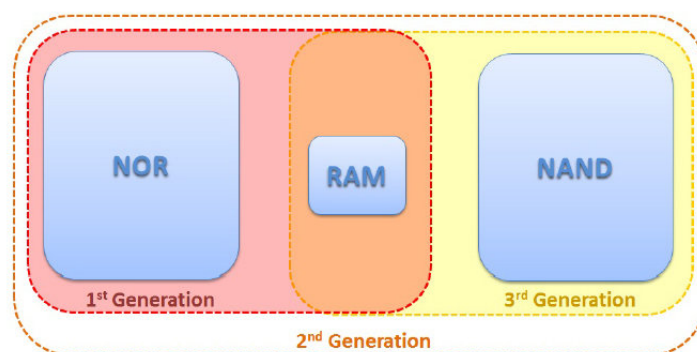


Figura 3.3: Tipologie di configurazione della memoria. Fonte: [ABJ13]

3.3.2 Dati acquisibili

La RAM è la componente più difficile da esaminare per via della sua natura volatile. Essendo utilizzata per l'esecuzione dei programmi, tipicamente si presta a contenere informazioni che potrebbero rivelarsi interessanti

in ambito di indagine. La memoria NOR contiene dati di sistema, come ad esempio il kernel, i driver del dispositivo, le librerie di sistema, informazioni relative all'esecuzione di applicazioni. Infine la memoria NAND contiene le informazioni personali (dati PIM³), elementi grafici, audio, video e altri file dell'utente.

Per i dispositivi con una configurazione della memoria di prima generazione la memoria NOR è certamente la principale fonte di evidenze digitali mentre nei dispositivi con configurazione di seconda e terza generazione si rivela fondamentale la memoria NAND.

3.4 Periferiche di memorizzazione

I telefoni cellulari avanzati e gli smartphone dispongono di slot in cui ospitare memorie aggiuntive removibili. Questa caratteristica di espandibilità della memoria è sempre più diffusa, e permette di moltiplicare notevolmente lo spazio a disposizione dell'utente per il salvataggio dei suoi dati. Rispetto ai cellulari basilari, con l'utilizzo di una memoria aggiuntiva si acquisisce oltre un ordine di grandezza in più di spazio, che solitamente è sfruttato per immagazzinare contenuti multimediali e documenti.

Le memorie aggiuntive sono di tipo flash, e sono principalmente:

- **SD card** (*Secure Digital card*) - vengono utilizzate nei formati *mini-SD* e *microSD*, facilmente interscambiabili mediante adattatori. Per tali formati la capacità massima è attualmente di 64GB; utilizzano connettori superficiali e sono molto resistenti agli urti.
- **MMC card** (*MultiMedia card*) - vengono utilizzate nei formati *Reduced Size* (RS-MMC), *MMCmobile* e *MMC Micro*. La capacità massima è attualmente di 2GB; utilizzano connettori superficiali e sono molto resistenti agli urti.

³Personal Information Management, dati relativi a calendario, agenda, rubrica, etc.

Le MMC card sono meno diffuse rispetto alle SD card, e sono probabilmente destinate a scomparire. La loro massima diffusione si è avuta grazie ad alcuni produttori come Nokia e Siemens che le hanno adottate per anni su specifiche linee di dispositivi. Alcuni formati come le MMC micro e le microSD sono molto simili ma sono fisicamente incompatibili.

3.4.1 Dati acquisibili

Le memorie aggiuntive vengono sfruttate principalmente per l'immagazzinamento di applicazioni, dati e contenuti multimediali. In particolar modo solo grazie al notevole incremento di spazio che deriva dal loro utilizzo, sui dispositivi di telefonia possono essere salvate numerose fotografie anche ad alta risoluzione. Quando poi a questi contenuti si aggiunge la possibilità, data oramai da qualunque smartphone, di utilizzare il GPS per salvare le coordinate geografiche nei metadati dell'immagine (Exif), l'acquisizione si può ritenere estremamente utile.

3.5 Cablaggi e connettori

Il discorso di assoluta eterogenità dei dispositivi esistenti si applica molto bene all'argomento cablaggi e connettori, dal momento che ogni dispositivo mobile ne ha tipicamente associati diversi. La varietà esistente è notevole e dato che esistono infiniti produttori, anche di materiale compatibile, molto spesso sui cavi non sono riportate indicazioni di marca e modello: questo fattore rende molto complesse le operazioni di riconducibilità dei cavi ad un dato reperto [Ate11].

I cavi si rivelano spesso di fondamentale importanza durante la fase di acquisizione. La maggior parte dei telefoni di base e di quelli avanzati ospita slot e connettori che dipendono strettamente dal modello e dalla marca del dispositivo: non è inusuale infatti trovare telefonini dello stesso produttore che necessitino di cavetteria molto diversa per l'alimentazione o la connessione dati (ove prevista). Negli smartphone invece si sta gradualmente convergen-



Figura 3.4: Connettori più diffusi: *micro USB*, *mini USB*, *30-pin dock* e *Lightning*

do ad una standardizzazione ed il fatto che le porte USB possano alimentarli ha eliminato la necessità di avere più di un cavo per dispositivo. Attualmente i principali connettori per gli smartphone sono i *mini USB* e i *micro USB*, invece per quanto riguarda l'ecosistema dei prodotti Apple si hanno i connettori *dock* e *Lightning* [Figura 3.4].

Capitolo 4

Architettura della rete cellulare

Sarà obiettivo di questo capitolo l'approfondimento di vari aspetti legati all'architettura della rete cellulare, con particolare riguardo per i sistemi GSM, GPRS e UMTS, che sono attualmente i più diffusi a livello europeo. In particolar modo ci si focalizzerà sugli aspetti legati alla mobilità degli utenti: queste reti permettono infatti agli utilizzatori di dispositivi cellulari di spostarsi liberamente sul territorio. Gli aspetti legati alla rintracciabilità degli utenti sono molto importanti a fini forensi.

4.1 Evoluzione dei sistemi di telefonia

I telefoni cellulari iniziarono ad essere commercializzati in Europa a partire dai primissimi anni '80, inizialmente nei soli Regno Unito e Scandinavia e a seguire in tutti gli altri Paesi europei. In Italia iniziarono a diffondersi solo nella seconda metà degli anni '90.

In questo primo periodo, ogni Paese finì col sviluppare uno specifico sistema di telefonia di 1^a generazione, che di conseguenza risultava inaccessibile a chiunque fosse dotato di tecnologie straniere. Gli svantaggi di tale scenario erano ovvi e numerosi: oltre a rimare contro all'idea di Europa unificata che si andava via via creando in quegli anni, così facendo si riduceva di molto il mercato di questi dispositivi cellulari, che erano di fatto limitati territo-

rialmente, e paradossalmente si limitava la loro penetrazione nel mercato nazionale, dal momento che si rendeva impossibile ai produttori mettere in atto economie di scala per ridurne i prezzi.

4.1.1 Nascita di GSM

Nel 1982 si compì un primo passo: la *Conference of European Posts and Telegraphs* (CEPT) formò un gruppo di studio, chiamato *Groupe Spécial Mobile* (GSM), con l'obiettivo di sviluppare ex novo un sistema di comunicazione europeo che:

- Garantisse una buona qualità vocale;
- Garantisse bassi costi di sviluppo e gestione di terminali e servizi;
- Garantisse la predisposizione di un range di nuovi servizi e strutture;
- Potesse gestire il roaming internazionale;
- Offerisse la piena compatibilità con alcune tecnologie esistenti.

Nel 1989 la responsabilità di definire GSM fu trasferita all'*European Telecommunication Standards Institute* (ETSI) e così l'anno seguente furono pubblicate le specifiche della prima versione di GSM. Il sistema fu avviato commercialmente nel 1991 e si diffuse molto rapidamente: al 1993 si contavano già 36 reti GSM in 22 Paesi, nonché il forte interesse di altri 25 Paesi che stavano valutando l'idea di adottarlo come standard. Anche se GSM nasce come standard europeo, non è in uso solo in Europa: reti di questo tipo sono infatti operative anche in Oriente e Medio Oriente, Africa, Sud America e Australia. Quindi l'acronimo GSM è stato col tempo adattato alle parole *Global System for Mobile communication*, sistema globale per la comunicazione mobile.

4.1.2 Nascita di UMTS

UMTS, ossia *Universal Mobile Telecommunications System*, è uno standard di telefonia mobile 3G (anche detto *di terza generazione*). Iniziò ad essere sviluppato a partire dagli anni 2000 e divenne operativo nel 2003, grazie della compagnia telefonica *Tre*. Nacque nel Regno Unito per estendersi poi, grazie all'intervento di altri gestori, ai Paesi dell'Europa continentale e poi agli Stati Uniti.

Lo standard UMTS mira a divenire l'erede di GSM, infatti è stato ideato partendo da una sua architettura rinforzata. Ha portato ad un aumento della qualità e della velocità di trasmissione delle informazioni, consentendo l'invio a banda larga di testo, voce, video, multimedia e dati.

4.1.3 Panoramica italiana

Attualmente GSM è la tecnologia cellulare dominante a livello europeo. Sul territorio italiano sono attivi diversi operatori telefonici, che gestiscono altrettante diverse reti mobili ad uso pubblico. I principali gestori italiani sono *Telecom Italia* (ex *Tim*), *Vodafone*, *Wind* e *Tre (H3G)*. I primi tre offrono servizi con tecnologia GSM (900MHz) e UMTS (2000 MHz), mentre *Tre* si occupa unicamente di servizi UMTS.

4.2 Funzionamento e componenti della rete

La scelta della rete di cui si serve un determinato dispositivo di telefonia mobile dipende strettamente dai termini di servizio sottoscritti con l'operatore telefonico e dalla tecnologia del dispositivo stesso. Nei dispositivi non vincolati ad uno specifico canale (generalmente definiti *unlocked* o sbloccati) la rete può essere modificata molto semplicemente sostituendo la SIM-card o USIM-card montata nel dispositivo.

4.2.1 Le stazioni mobili (MS)

Un dispositivo di telefonia mobile non è altro che una stazione mobile (MS - *Mobile Station*), composta da due componenti distinte:

- **UICC** (*Universal Integrated Circuit Card*) - una smart-card;
- **ME** (*Mobile Equipment*) - l'apparecchiatura vera e propria.

Caratteristiche delle UICC

La UICC è comunemente chiamata modulo di identità e può essere ad esempio una SIM-card¹ per la rete GSM o una USIM-card² per la rete UMTS. È una componente removibile indispensabile, che custodisce le informazioni essenziali sul sottoscrittore del contratto di telefonia. Il suo scopo principale è quello di autenticare l'utente alla rete, permettendogli l'accesso ai servizi che ha sottoscritto. La UICC inoltre offre servizi basilari di salvataggio delle informazioni personali, come ad esempio la rubrica telefonica, gli SMS o le informazioni sulle ultime chiamate ricevute o inoltrate.

Ad ogni UICC è associato un numero di telefono univoco, detto *MSISDN*³. Quando l'UICC è in roaming su un'altra rete gli viene associato un numero telefonico temporaneo detto *MSRN*⁴.

Spostando la UICC tra dispositivi compatibili si trasferiscono automaticamente anche l'identità dell'utente e le informazioni a lui associate.

Formati Le UICC sono disponibili in quattro differenti formati [Figura 4.1]:

- **Full-size** o **Standard SIM** di dimensioni 85,60x53,98x0,76mm. Questo formato è stato dismesso;

¹Subscriber Identity Module

²Universal Subscriber Identity Module

³Non si tratta di un vero e proprio acronimo ma può comunque essere interpretato come *Mobile Subscriber Integrated Services Digital Network-Number*

⁴Mobile Station Roaming Number

- **Mini SIM (2FF)** di dimensioni 25x15x0,76mm;
- **Micro SIM (3FF)** di dimensioni 15x12x0,76mm;
- **Nano SIM (4FF)** di dimensioni 12,30x8,80x0,67mm.

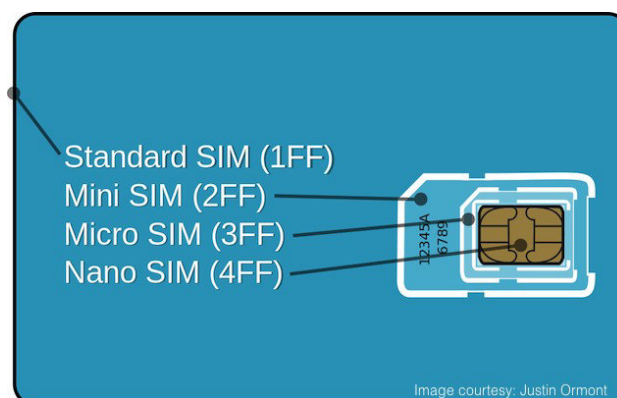


Figura 4.1: Formati delle UICC

Componenti Il cuore di una UICC è un particolare tipo di smart-card che contiene solitamente un processore e una memoria di dimensioni comprese tra i 16 e i 128KB. Tale memoria è di sola lettura, persistente, elettronicamente cancellabile e programmabile e per questo prende il nome di EEPROM⁵.

La UICC possiede una porzione di memoria RAM per i programmi in esecuzione e una di ROM che conserva principalmente le informazioni relative all'utente. In base alle caratteristiche del dispositivo che la ospita, la UICC può gestire le informazioni memorizzate in combinazione con la memoria del telefono. Talvolta è anche possibile che le informazioni risiedano unicamente sul dispositivo invece che sulla UICC.

Sicurezza L'accesso alle informazioni contenute nella UICC è protetto da un codice di identificazione personale (PIN, *Personal Identification Number*) assegnato all'utente in fase di sottoscrizione. È generalmente composto da

⁵dall'inglese *Persistent Electronically Erasable, Programmable Read Only Memory*

quattro cifre e può essere modificato dall'utente. L'inserimento del PIN ammette un predefinito numero massimo di tentativi, solitamente tre, superati i quali si va incontro al blocco della UICC. Per ripristinarla occorre inserire il codice di sblocco (PUK, *PIN Unblocking Key*): anche in questo caso esiste un numero massimo di tentativi, normalmente dieci, superati i quali la UICC si blocca permanentemente.

Caratteristiche delle ME

Una ME è una qualunque apparecchiatura in grado di comunicare, tramite una determinata frequenza, con le stazioni radio della rete cellulare. Dispone di un alloggiamento in cui collocare la UICC, senza la quale sarebbe impossibile accedere alla rete.

Identificazione sulla rete Ogni apparecchiatura che opera sulla rete è identificata da un codice univoco chiamato IMEI (*International Mobile Equipment Identifier*). Si tratta di un numero composto da 15 cifre che indica alcune informazioni fondamentali sul dispositivo, come ad esempio il produttore, il modello e il Paese in cui è stato abilitato alla rete. Le prime 8 cifre sono il TAC (*Type Allocation Code*) che indica il modello e la provenienza; le restanti sono invece le specifiche del produttore.

4.2.2 Componenti dell'architettura GSM

Le componenti principali [Figura 4.2] di una rete GSM sono:

- **BTS** (*Base Transceiver Station*) - sono delle stazioni radio, ossia degli impianti che ricevono e ritrasmettono i segnali dei dispositivi cellulari. Ognuno di essi è costituito da un'antenna e dai relativi dispositivi radio. La zona che riescono a coprire col loro segnale è detta cella. Il luogo in cui è installata la BTS è invece chiamato *sito della cella*;
- **BSC** (*Base Station Controller*) - sono dei controller che gestiscono e regolano l'emissione del segnale delle stazioni BTS a loro collegate. Si

occupano dell'instaurazione del canale radio, del frequency hopping e dell'handover;

- **MSC** (*Mobile Switching Center*) - sono sistemi di commutazione che interconnettono un elevato numero di BSC. Gestiscono l'instradamento delle chiamate in entrata e in uscita e assegnano i canali.

Esistono poi alcuni elementi (gateway e database) a supporto di quelli appena introdotti:

- **GMSC** (*Gateway MSC*) - gateway che si interfacciano con la rete telefonica pubblica (anche detta **PSTN**);
- **HLR** (*Home Location Register*) - un database centrale che contiene i dettagli di ogni sottoscrittore di contratto telefonico autorizzato ad usare la rete GSM. Memorizza sia dati permanenti che temporanei;
- **VLR** (*Visitor Location Register*) - database che conserva dati a supporto dei dispositivi mobili che sono in roaming al di fuori della loro area

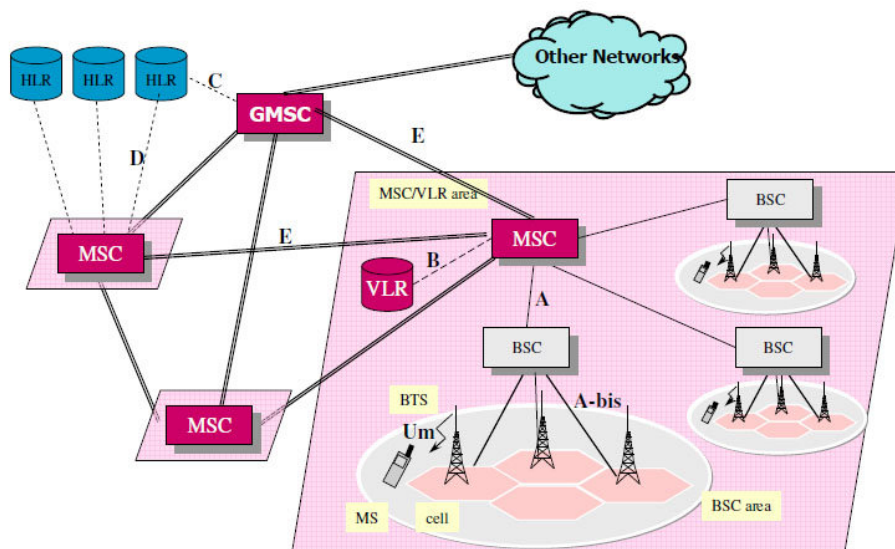


Figura 4.2: Architettura della rete GSM. Fonte: [D'A06]

di servizio [aspetto che verrà approfondito nel Paragrafo 4.3.3]. Ogni registro è responsabile di un gruppo di *location areas* e memorizza sia dati temporanei che permanenti;

- **AUC** (*Authentication Center*) - genera e memorizza dati relativi alla sicurezza, come ad esempio le chiavi di autenticazione e cifratura.
- **EIR** (*Equipment Identity Register*) - database che conserva dati relativi ai dispositivi degli utenti.

Interazione

Le MS riescono a collegarsi alla rete utilizzando i segnali radio trasmessi dalle BTS dislocate sul territorio. Queste sono coordinate a gruppi da una BSC (sulla rete ne esistono diverse) che si occupa di gestire correttamente la copertura territoriale delle celle. Le BSC fanno riferimento ad un MSC (sulla rete ne esistono diversi): ogni MSC controlla un set di BSC tramite i quali gestisce complessivamente le comunicazioni attraverso la rete cellulare, elaborando le chiamate e coordinandole. Gestisce anche i messaggi SMS e tiene traccia delle informazioni relative alle chiamate (CDS, *Call Detail Records*) e alla successione temporale delle chiamate (*logs*). Si interfaccia con lo switch della rete PSTN tramite un Gateway MSC (GMSC). Per svolgere le sue funzioni un MSC si serve di diversi database: uno dei più importanti è HLR che è un database centrale, condiviso con la rete GPRS, che conserva i dati relativi agli utenti, come ad esempio i dati personali, i servizi attivati e l'ultima posizione rilevata sulla rete. Vi è poi un altro database, VLR, che gestisce i dati relativi ai dispositivi in roaming. Infine vi sono l'AUC e l'EIR che conservano rispettivamente dati legati alla sicurezza e dati sulle MS.

Accesso alla rete

Il sistema GSM utilizza TDMA (*Time Division Multiple Access*) come algoritmo di accesso alla rete. Si tratta di un algoritmo ideato per permettere a

più dispositivi di condividere, tramite turni, un singolo canale di trasmissione. Operativamente, il canale trasmissivo viene utilizzato da un dispositivo X solo per un determinato intervallo di tempo, trascorso il quale il canale viene rilasciato per essere utilizzato da altri dispositivi.

4.2.3 Componenti dell'architettura GPRS

La maggior parte delle componenti di GSM sono utilizzate anche dalla rete GPRS. Abbiamo così due sistemi coesistenti attraverso i quali transitano dati di natura differente.

Le componenti condivise sono le **BTS** (Base Transceiver Station), i **BSC** (Base Station Controller) e il database **HLR** (Home Location Register). Vi sono poi alcune componenti simili ma specifiche per GPRS [Figura 4.3]:

- **SGSN** (*Service GPRS Support Node*) - sistemi che svolgono un ruolo simile agli MSC;
- **GGSN** (*Gateway GPRS Support Node*) - gateway simili agli GMSC ma che si interfacciano con Internet anzichè con la rete PSTN.

Accesso alla rete

GPRS utilizza CDMA (*Code Division Multiple Access*) come algoritmo di accesso alla rete. È un algoritmo basato sul principio che più dispositivi possano trasmettere contemporaneamente sullo stesso canale fisico. È compito della stazione ricevente occuparsi della decodifica di quanto ricevuto, e della conseguente estrazione dei soli dati che la riguardano. Il flusso dei dati è distinto grazie all'utilizzo di sequenze numeriche uniche.

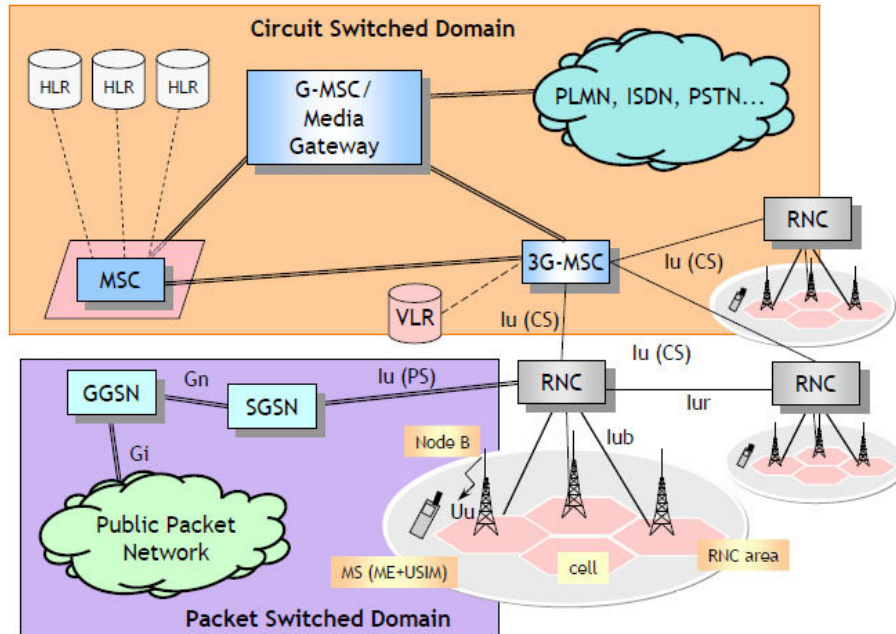


Figura 4.4: Architettura della rete UMTS. Fonte: [D'A06]

- Il **dominio CS** (*Circuit Switched*) è l'insieme di tutte le entità che offrono connessioni di tipo CS. Le sue componenti sono le stesse della rete GSM: i registri **HLR**, **VLR**, **AUC**, **EIR** e gli **MSC** e i **GMSC**, le cui funzionalità sono già state spiegate nei paragrafi precedenti.
- Il **dominio PS** (*Packet Switched*) è l'insieme di tutte le entità che offrono connessioni di tipo PS. Le sue componenti sono le stesse della rete GPRS, ossia i **SGSN** e i **GGSN**.

Accesso alla rete

UMTS, come GPRS, utilizza CDMA come algoritmo di accesso alla rete [Paragrafo 4.2.3].

4.3 Copertura e mobilità

Le reti cellulari garantiscono in generale un buon livello di mobilità ai loro utenti: ciò è reso possibile da un'attenta gestione della capacità di trasmissione di ogni antenna posizionata sul territorio. La rete è infatti strutturata in una serie di celle adiacenti [Figura 4.5], ognuna delle quali è gestita da una BTS. Questa disposizione garantisce una buona copertura del territorio e la non interruzione dei servizi erogati, anche per gli utenti in movimento.

Le BTS sono distribuite sul territorio in maniera capillare. Ampiezza e forma di ogni singola cella dipendono però da una serie di caratteristiche strettamente legate all'area da servire o all'antenna stessa, tra cui:

- la densità degli utenti da servire in quell'area;
- la tipologia di zona (ad esempio se siamo in contesto urbano o rurale) e la presenza di ostacoli;
- l'altezza delle installazioni;
- la tipologia di antenna utilizzata e la potenza impiegata.

Le BTS possono quindi essere distanziate tra loro da poche centinaia di metri, come nel caso delle grandi città, e fino a diversi chilometri nelle aree rurali. La potenza del segnale radio emesso, e quindi l'area di ogni cella, è

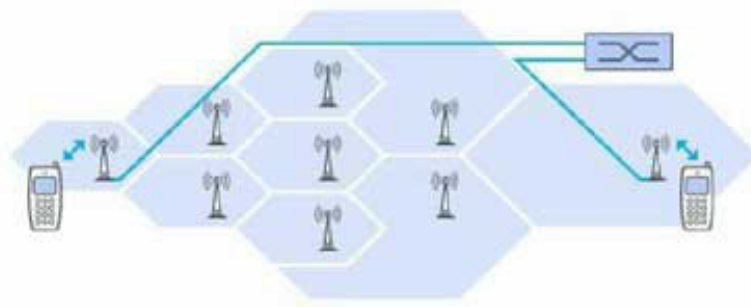


Figura 4.5: Suddivisione territoriale in celle. Fonte: [ERti]

accuratamente controllata dal sistema. Il sito della cella non è come si può pensare posto al centro della stessa, ma si trova invece nei pressi del confine tra le celle [Figura 4.5], in modo da facilitare le comunicazioni degli utenti in movimento. Solitamente ogni torre della cella ha tre pannelli per lato: quello centrale è il trasmettitore e quelli laterali sono i ricevitori, costantemente in ascolto dei segnali radio in arrivo.

4.3.1 Propagazione del segnale

La propagazione del segnale dalle BTS avviene tramite bande di frequenza diverse, comprese tra i 900 e i 2100 MHz a seconda del sistema implementato (GSM o UMTS). Le trasmissioni di telefonia mobile, diversamente ad esempio da quelle di diffusione radiotelevisiva, sono contraddistinte dalla caratteristica della bi-direzionalità: dalle stazioni BTS ai terminali degli utenti e viceversa.

Le antenne delle BTS tradizionali sono generalmente installate su sostegni posizionati sul terreno o fissati sulla sommità di edifici; le altezze di installazione sono normalmente comprese tra i 15 e i 50 metri. Ogni BTS può essere costituita da più sistemi di diversa tecnologia (GSM o UMTS); inoltre la stessa struttura può ospitare più BTS di diversi gestori (questo fenomeno è conosciuto come *co-siting*). In alcune zone nei centri urbani le BTS di tipo tradizionale lavorano in concomitanza con BTS micro o pico-cellulari⁶. Si tratta di sistemi con una portata minore, che sono visivamente più gradevoli o più facilmente mimetizzabili, che possono essere installati sulle pareti degli edifici anche a pochi metri dal suolo.

Le BSC implementano un controllo dinamico della potenza e possono quindi regolare, aumentandolo o diminuendolo, il potere di trasmissione delle BTS. Sono infatti implementati meccanismi tramite i quali le MS raccolgono e inviano valori relativi alla qualità del segnale. Ciò è reso possibile dalla tecnica di trasmissione: dentro ogni slot è infatti inclusa una sequenza fissata,

⁶estensori di copertura.

detta *bit di training*, che permette alla BTS ricevente di stimare la probabilità di errori nei bit.

4.3.2 Handover

La struttura a celle della rete di telefonia mobile garantisce ai dispositivi mobili (MS) collegati un buon grado di mobilità all'interno della rete. Il passaggio della connessione dalla BTS attuale ad un'altra BTS posta in condizioni più favorevoli è noto come *handover*⁷ o *handoff*⁸. Questo fenomeno deve essere gestito efficientemente, devono quindi essere implementati dei meccanismi che garantiscano che:

- Il passaggio venga eseguito rapidamente, in modo che l'utente non percepisca un'interruzione del servizio (*seamless*);
- Il numero di handover attuati rispetto alla distanza coperta sia minimo;
- L'handover sia attuato il più vicino possibile al confine delle celle;
- La cella di destinazione venga scelta correttamente;
- Siano limitati gli handover non necessari compiendo adeguate valutazioni del segnale.

Funzionamento

Nella pratica la realizzazione dell'handover è possibile grazie alla creazione di una lista, per ogni cella, che contenga le potenziali celle raggiungibili. Le celle potenziali sono di fatto quelle vicine, e per questo motivo la lista è denominata *neighbour list*; tramite essa è possibile individuare, quando richiesto, la migliore cella raggiungibile.

Le fasi tramite cui si attua un handover sono:

⁷Termine che deriva dall'inglese britannico.

⁸Termine che deriva dall'inglese americano.

1. **Inizializzazione** - in questa fase vengono raccolti diversi indicatori relativi alla qualità del collegamento. Solitamente questi sono la potenza ricevuta, il *bit error ratio*⁹ e il *block error ratio*¹⁰;
2. **Decisione** - gli indicatori raccolti vengono confrontati con determinate soglie;
3. **Preparazione** - dalla *neighbour list* della BTS attuale viene selezionata la migliore opzione, ossia un canale libero di qualità migliore rispetto a quello attuale.
4. **Esecuzione** - fase in cui finalmente la MS e la rete commutano simultaneamente.

L'handover non entra in funzione unicamente quando si attraversa il confine di una nuova cella, ma anche quando viene rilevata una perdita di qualità del segnale radio tale da essere necessaria una riconnessione (**handover per qualità**), oppure quando viene rilevata una cella che permetterebbe al dispositivo di consumare meno batteria durante la trasmissione (**handover per power-budget**).

Tipologie di handover

Esistono due principali tipologie di handover, che hanno funzionamenti leggermente diversi:

- **Hard handover** (HHO) - le risorse in uso di una cella vengono rilasciate prima di accedere ai servizi di una nuova. Per questo motivo è soprannominata *break-before-make*;
- **Soft handover** (SHO) - le risorse precedenti vengono mantenute durante il passaggio e rilasciate in seguito. È soprannominata *make-before-break*.

⁹Rapporto tra i bit ricevuti correttamente rispetto a quelli trasmessi. Viene valutato in base ai bit di training.

¹⁰Rapporto tra il numero di blocchi errati ricevuti rispetto a quelli trasmessi.

Sulla rete GSM, o meglio su TDMA, la tipologia di handover implementata è di tipo hard. Ne consegue che la qualità della trasmissione è strettamente legata alla velocità con cui avviene il passaggio tra celle (anche se solitamente il distacco non è percepibile). Sulla rete UMTS (CDMA) che offre invece la possibilità di ricevere contemporaneamente più segnali, è implementato il soft handover.

A seconda del soggetto che gestisce il meccanismo di handover abbiamo poi una ulteriore differenziazione:

- **Network Controlled HandOver** (NCHO) - completamente gestito dalla rete;
- **Mobile Assisted HandOver**(MAHO) - è gestito dalla rete, ma le misure di qualità vengono fornite sia dalla MS che dalla BTS;
- **Mobile Controlled HandOver** (MCHO) - completamente gestito dalla MS.

Problematiche da gestire

L'handover deve avvenire quanto l'MS si trova piuttosto vicino al confine della nuova cella, non prima, dal momento che ogni BTS riesce a supportare solo il carico di traffico previsto entro la sua cella. Inoltre, se si verificasse tale caso, i dispositivi mobili dovrebbero utilizzare maggiore potenza di trasmissione per comunicare con la BTS, fatto che accrescerebbe le interferenze nel sistema.

Quando i dispositivi si muovono lungo i confini delle celle, potrebbe essere necessario attuare l'handover diverse volte prima di trovare stabilità in una cella. Devono quindi essere implementati algoritmi che evitino gli handover ripetuti.

4.3.3 Roaming

Con il termine *roaming* si indica solitamente l'estensione della connettività di un servizio al di fuori della località in cui è stato registrato. Il roaming, come l'handover, assicura che le connessioni dei dispositivi alla rete siano mantenute. Il roaming venne inizialmente sviluppato per GSM e successivamente implementato anche su UMTS.

Funzionamento

La differenza tra la rete in cui un utente è registrato e quella in cui è ospite è tecnicamente data da una voce contenuta nei registri del sistema. Se le informazioni di un utente non sono contenute nel database HLR della rete devono essere richieste alla sua rete di appartenenza, così da poter autenticare o meno l'utente al sistema. Una volta che questi dati sono stati ricevuti dalla rete ospitante, essa si occupa di aggiungere una nuova voce temporanea all'interno del database VLR e di attivare i servizi a cui l'utente è abilitato.

I dettagli relativi al processo per contattare un dispositivo in roaming variano in base al tipo di rete, ma in generale i passaggi sono i seguenti:

1. L'utente chiamante digita il numero telefonico del dispositivo cellulare in roaming;
2. In base alle informazioni contenute nel numero di telefono (MSISDN) dell'utente da contattare la chiamata è direzionata al GMSC.
3. Il GMSC contatta l'HLR per individuare l'MS cercato.
4. L'HLR è a conoscenza delle ultime posizioni in cui l'MS è stato registrato, per cui conosce il VLR che attualmente gestisce il dispositivo in roaming.
5. Il VLR viene contattato e assegna all'MS un nuovo numero temporaneo (MSRN).

6. Disponendo dell'MSRN il GMSC è in grado instradare la chiamata all'MS.

4.4 Localizzazione a fini investigativi

Le informazioni relative al passaggio di un dispositivo da una cella all'altra o da una rete all'altra si rivelano spesso molto utili a fini investigativi. Questi dati tengono di fatto traccia degli spostamenti geografici di un dispositivo mobile, e di conseguenza degli spostamenti del suo utilizzatore. In particolar modo, note le posizioni delle BTS ed avendo a disposizione il log dei luoghi in cui l'MS è stato registrato, è possibile ricostruire il percorso effettuato, creando ad esempio una tabella spazio temporale degli eventi. Ovviamente questo tipo di analisi deve tenere conto di vari elementi esterni, quali ad esempio la viabilità stradale. È opportuno poi verificare tramite misurazioni manuali (utilizzando misuratori di campo), che le linee di handover siano effettivamente quelle note. Infine occorre ricordare che sia le UICC che i codici IMEI possono essere clonati.

Capitolo 5

Metodologie e strumenti per la mobile device forensics

L'approccio da utilizzare in fase di analisi deve essere tarato specificamente sul dispositivo che occorre esaminare, facendo considerazioni caso per caso sulle caratteristiche e sullo stato di integrità fisica del device. In questo capitolo analizzeremo le possibili opzioni di acquisizione dei dati, declinandone caratteristiche e limiti.

5.1 Livelli di analisi

Esistono numerose metodologie per l'acquisizione di dati da dispositivi di telefonia mobile: è possibile creare una classificazione [Figura 5.1] che tenga conto di criteri come invasività, complessità e *know-how* necessario.

Al primo livello di questa classificazione si trova l'estrazione manuale dei dati, che si attua mediante l'utilizzo diretto del device. Al secondo livello è collocata l'estrazione logica, che mira ad acquisire una rappresentazione logica della memoria e dei dati in essa contenuti. Al terzo livello si trova l'estrazione fisica, o *hex dump*, che riguarda l'acquisizione fisica della memoria del dispositivo tramite computer (*workstation*). Al quarto livello si hanno le tecniche di *chip-off*, ossia di esportazione fisica dei chip di memoria dal



Figura 5.1: Livelli di analisi per la mobile device forensics. Fonte: [ABJ13]

dispositivo e loro acquisizione mediante copie forensi. Infine al quinto livello si colloca la micro lettura, che utilizza sofisticate strumentazioni, come ad esempio microscopi elettronici, per esaminare le circuiterie dei chip di memoria.

È bene notare come i livelli dal terzo al quinto (estrazione fisica, *chip-off* e micro lettura) riguardino la creazione di una copia forense, ossia bit-a-bit del supporto fisico, mentre l'acquisizione logica al secondo livello serve per acquisire una copia logica, ossia una rappresentazione astratta¹, dei dati archiviati; l'acquisizione di primo livello opera invece su un livello di astrazione ancora più elevato. Il livello di astrazione si ripercuote anche sulle informazioni che è possibile raccogliere: l'acquisizione fisica permette di accedere a qualunque dato presente su disco, ivi compresi gli elementi che sono stati cancellati ma non ancora totalmente sovrascritti, come ad esempio i dati contenuti nello *slack space*; tali elementi risulterebbero inaccessibili mediante l'acquisizione logica. L'elevata astrazione dell'acquisizione logica rende però i dati di immediata comprensione mentre invece i risultati ottenuti a mezzo di acquisizione fisica necessitano di interpretazione: il passaggio da *raw data*, dati grezzi non ancora processati, ad informazioni comprensibili necessita ovviamente di ulteriori risorse.

¹Mediante oggetti logici, ossia file e cartelle

In base alle circostanze in cui si deve svolgere l'acquisizione (valutando cioè elementi come tempo, strumentazioni disponibili e condizioni del reperto) il tecnico forense deve decidere da quale livello iniziare ad operare. Dal momento che il ricorso a determinate metodologie può precludere lo svolgimento di altre, la scelta deve essere fatta con consapevolezza. Inoltre occorre sempre tenere in considerazione il grado di rischio delle procedure: esso aumenta proporzionalmente al livello di complessità.

5.2 Metodologie di acquisizione dei dati

5.2.1 Estrazione manuale

Collocata al livello più basso della classificazione, tale procedura non richiede conoscenze specialistiche, ma solo praticità col dispositivo in esame. Tale requisito può essere facilmente ovviato procurandosi il suo manuale d'uso del telefono.

L'estrazione manuale dei dati consiste nella visualizzazione degli stessi sul dispositivo che li contiene, procedura che solitamente viene documentata attuando delle riprese con una fotocamera esterna. Si attua mediante la manipolazione del reperto: si agisce sul dispositivo utilizzando la tastiera o il touchscreen in modo che i dati vengono conseguentemente visualizzati sul display. In questo contesto ovviamente il recupero delle informazioni cancellate non è possibile. Il metodo è solitamente veloce, funziona su qualunque dispositivo non danneggiato, non richiede cavi ed è di facile messa in opera. Il tempo richiesto dalla procedura è proporzionale alla mole di dati memorizzati sul dispositivo, al cui aumentare cresce anche il rischio di alterazione o cancellazione accidentale.

Questa tecnica non è solitamente la scelta preferenziale visto che con l'uso diretto del device il rischio di alterare involontariamente i dati è eleva-

to: pensiamo ad esempio ai messaggi di testo non ancora letti; inoltre non rende possibile il recupero delle informazioni cancellate. È però una tecnica possibile, validamente utilizzabile in sede processuale se opportunamente documentata.

5.2.2 Estrazione logica

L'estrazione logica si colloca al secondo livello della classificazione: è una metodologia di acquisizione mediamente tecnica che richiede un livello base di conoscenze informatiche, dal momento che si attua utilizzando un software dedicato. Il dispositivo da analizzare deve essere connesso alla workstation tramite un collegamento via cavo o wireless. Il tecnico forense opera sulla stazione di lavoro, generalmente un computer, dalla quale predispose l'operazione e sulla quale raccoglie i risultati.

L'acquisizione logica di un dispositivo mobile consente di estrarre le informazioni attualmente memorizzate utilizzando l'interfaccia messa a disposizione del produttore per effettuare i backup, oppure ricorrendo a software dedicato. A seconda del tipo di tool utilizzato l'informazione estratta può essere mostrata a livello di file system (mediante file e cartelle) o a livello applicativo (organizzazione di contatti, sms, etc). Questo metodo consente di raccogliere una buona varietà di informazioni sul dispositivo, anche in merito alle configurazioni adottate dall'utente. Esistono però alcune problematiche, come ad esempio l'impossibilità di recuperare le informazioni cancellate o la necessità di possedere la cavetteria adeguata.

Si tratta di una delle metodologie più diffuse; per i limiti che abbiamo appena illustrato solitamente nella pratica la si usa come strategia di partenza per l'esame preliminare del device, dal momento che la sua esecuzione non preclude alcuna azione successiva, per poi passare a livelli di analisi più approfonditi.

5.2.3 Estrazione fisica (hex dump)

Al terzo livello della classificazione si colloca l'estrazione fisica, anche detta analisi *hex dump*, attraverso la quale un tecnico forense può accedere ai *raw data* immagazzinati nella memoria del dispositivo. Anche questa modalità si attua mediante una workstation, che monta un apposito software, e il collegamento (cablato o wireless) della stessa al dispositivo.

Questa tipologia di acquisizione si attua creando una copia bit-a-bit della memoria permanente del device; successivamente, i tool impiegati per l'analisi e la decodifica dei contenuti lavoreranno sull'immagine forense così generata, fornendo all'operatore una vista logica della struttura del file system comprensiva dei dati cancellati e non ancora sovrascritti.

Tale metodologia, in combinazione con l'estrazione logica, è la più utilizzata nell'ambito delle indagini forensi poichè, ad un costo accettabile, consente di analizzare in maniera approfondita la stragrande maggioranza dei dispositivi. I software che si occupano di questa attività sono quelli che evolvono più velocemente e che necessitano di continui aggiornamenti per riuscire a supportare i nuovi device introdotti sul mercato. Malgrado il rapido avanzamento tecnologico esistono ancora diverse criticità, come ad esempio il fatto che sia necessaria la conversione dei dati, attuata dallo stesso software di estrazione. I più grossi limiti riguardano il fatto che non tutti i dispositivi siano supportati da un unico tool e che sia necessaria anche in questo caso cavetteria specifica.

5.2.4 Esportazione dei chip (chip-off)

La tecnica di *chip-off*, collocata al quarto livello della classificazione, consiste nella rimozione fisica dei chip di memoria dal device, e nella conseguente acquisizione e analisi dei dati in essi contenuti. L'asportazione dei chip viene eseguita solitamente nei casi in cui sia l'unica o l'ultima risorsa disponibile: in questo modo è possibile l'acquisizione dei dati anche se i dispositivi so-

no gravemente danneggiati, non più funzionanti, protetti da password/pin o bloccati da altri meccanismi di sicurezza. Si può attuare sulla maggior parte dei device che montano memorie flash di tipo NAND o NOR [Paragrafo 3.3].

La procedura si attua mediante una serie di fasi:

- Estrazione fisica dei chip, utilizzando il calore (de-saldatura) o prodotti chimici per sciogliere i collanti.
- Pulizia e riparazione dei chip, ove necessaria;
- Acquisizione dei *raw data* mediante la creazione copie forensi;
- Analisi delle copie forensi mediante software specializzato;

Questa metodologia è quella che presenta più analogie con la procedura di acquisizione in camera bianca di hard-disk nel contesto di indagini di *computer forensics*. È però utilizzata molto poco frequentemente, quasi per nulla in Italia, per via dell'alto costo di intervento, e nei soli casi che coinvolgono dispositivi gravemente danneggiati o bloccati. Si tratta di un'operazione che richiede una certa tecnica, dal momento che si deve operare con componenti estremamente delicate. Le principali criticità riguardano la varietà dei chip e dei formati di immagazzinamento dei *raw data* [Swa12].

5.2.5 Micro lettura

La tecnica della micro lettura si colloca all'ultimo livello della classificazione, e consiste nell'osservazione fisica delle circuiterie elettroniche che compongono i chip delle memorie NAND o NOR [Paragrafo 3.3] mediante l'ausilio di microscopi elettronici. La lettura avviene dopo l'asportazione fisica delle componenti dal device, quindi le sue fasi preliminari sono le stesse della tecnica di chip-off.

Questa tipologia di acquisizione è estremamente delicata e costosa e perciò può venire impiegata solo per indagini di alto profilo concernenti ad esempio questioni di sicurezza nazionale. Viene utilizzata solo se le metodologie

precedenti si sono rivelate inadeguate, per acquisire ad esempio dati da chip fisicamente danneggiati.

5.3 Strumenti per l'acquisizione dei dati

Esistono varie tipologie di strumenti e software per acquisire dati mediante le tecniche appena illustrate. Ogni diverso livello di analisi, ad eccezione del quinto (micro lettura), trova soluzioni disponibili commercialmente, che spaziano dall'hardware al software. Un esempio di attrezzatura hardware che può essere citata, è quella che riguarda l'acquisizione manuale, in cui non tanto la messa in opera della procedura, quanto la sua documentazione, necessita di una base di lavoro [Figura 5.2].

Per quanto riguarda le metodologie di estrazione logica e fisica sono invece disponibili soluzioni software, sia forensi che commerciali: le soluzioni forensi [ne verranno forniti esempi al Paragrafo 7.1.2] sono pensate specificamente per attuare acquisizioni di dati da memorie interne, esterne e UICC, senza provocare alterazioni; le soluzioni non forensi, come ad esempio iTunes, sono invece solitamente create e distribuite dai produttori dei device per consentire agli utenti la gestione dei dati e l'esecuzione di backup. Entrambe le categorie di software sono in genere specializzate su un range di dispositivi, supportando ad esempio device col medesimo sistema operativo o con date



Figura 5.2: Base di lavoro per acquisizioni manuali. Fonte: [Fer]



Figura 5.3: Programmatori per l'acquisizione di chip. Fonte: [Swa12]

caratteristiche hardware. È quindi buona norma che gli operatori tecnici si dotino di un ventaglio di strumenti che consenta loro di gestire, sperabilmente, ogni possibile contesto.

Infine per quanto riguarda le metodologie di chip-off sono disponibili strumenti hardware, di natura prettamente elettronica, come *chip programmer* [Figura 5.3] e relativi adattatori.

Capitolo 6

Procedure invasive per l'analisi forense di Android e iOS

The right to have root on your machine is the right to store things which operate on your behalf.

Tim Berners-Lee¹

Quando l'utilizzo di strumentazioni e procedure forensi non conduce ai risultati sperati si può decidere di proseguire le indagini “sperimentando”, ossia adottando metodologie alternative di estrazione e analisi dei dati. Tali procedure sono tipicamente non ripetibili ma rappresentano l'unica strada per acquisire il maggior numero di dati contenuti all'interno di dispositivi smartphone, andando ad alterare il sistema operativo del dispositivo al fine di avere accesso completo sui dati in esso memorizzati. Stiamo parlando del *rooting* per ambiente Android e del *jailbreaking* per sistemi iOS. Queste metodologie sono normalmente utilizzate dagli utenti per abbassare il livello di protezione del dispositivo, potendo così decidere in maniera completamente autonoma quali programmi, anche non autorizzati dal produttore o acquisiti senza legale licenza d'uso, installare. Tuttavia, ai fini forensi sono fondamentali per avere accesso completo sul file system.

¹Intervistato al Linux.conf.au 2013 [[Stiti](#)].

6.1 Acquisizione mediante rooting

6.1.1 Nozioni generali sul sistema operativo Android

Android² è un sistema operativo *open source* e *unix-based*, particolarmente versatile perché adatto a supportare famiglie di dispositivi molto diverse fra loro, come ad esempio telefoni cellulari, netbook, *smart TV*.

Il progetto è gestito dalla *Open Handset Alliance* (OHA), un consorzio di produttori e sviluppatori di tecnologie mobili a cui fa capo Google. È attualmente il sistema operativo per device portatili con la maggiore diffusione³, disponendo di una vastissima comunità di sviluppatori per la realizzazione di app dedicate.

Architettura di Android

Si tratta di un sistema operativo complesso, che presenta un'architettura a livelli. Partendo dal basso questi sono [Figura 6.1]:

- **Livello Linux Kernel** - vi risiedono le componenti necessarie alla gestione dell'hardware;
- **Livello Librerie** - ospita le librerie native del sistema;
- **Livello Application Framework** - implementa i vari servizi offerti dal sistema alle applicazioni;
- **Livello Applicazioni** - ospita sia le applicazioni native che quelle scaricate dall'utente.

Partizioni di sistema

Nei dispositivi che montano il sistema Android solitamente la memoria è partizionata in quattro diverse aree, che sono indicativamente:

²Per maggiori informazioni si veda <http://www.google.it/mobile/android/>.

³Con una quota di mercato del 79% ad agosto 2013 [Relti].



Figura 6.1: Architettura del sistema operativo Android.

- **Partizione di bootloader** - consente di avviare il sistema;
- **Partizione di recovery** - necessaria al ripristino del telefono alle condizioni di fabbrica;
- **Partizione di sistema** - ospita le cartelle del sistema operativo;
- **Partizione dati** - ospita i dati relativi all'utente.

Nei dispositivi Android la memorizzazione dei dati relativi all'utente e alle applicazioni avviene solitamente nella memoria flash interna⁴ o in quella esterna⁵. Avviene con modalità diverse: la maggior parte dei dati è organizzata all'interno del file system, mentre la parte concernente dati "elencabili" (come ad esempio contatti, sms, e-mail, etc.) è memorizzata all'interno di file database `SQLite` che a loro volta risiedono nel file system.

⁴La quale monta un file system di tipo `YAFFS2`.

⁵Ove presente, la quale monta un file system di tipo `FAT`.

Meccanismi di protezione del sistema

Sui sistemi Android sono implementati meccanismi di protezione che hanno impatto sulle tecniche di analisi forense. Parliamo della gestione dei privilegi utente e del *sand-boxing*.

Nei sistemi unix, *root* è l'utente amministratore con i privilegi più alti. Possedere i diritti di root offre in pratica la possibilità di accedere e di agire con permessi di scrittura su tutte le cartelle del sistema. Quest'azione solitamente è preclusa all'utente standard, che possiede permessi di scrittura sui soli file contenuti nella sua cartella utente, per preservare il sistema da qualunque rischio di cancellazione accidentale ad opera di un utente poco esperto.

Inoltre le applicazioni vengono eseguite all'interno di un ambiente protetto, detto *sand-box*: esse non possono accedere ai dati di altre applicazioni a meno che non ne venga richiesto esplicito consenso.

6.1.2 Ottenimento dei diritti di root

Sebbene i dispositivi Android vengano distribuiti con l'utenza di root disabilitata, la promozione ad utente con poteri di amministratore è comunque sempre possibile tramite una procedura che comporta alterazioni al sistema che in gergo è nota sotto il nome di *rooting*.

In riferimento alle partizioni di sistema precedentemente illustrate [Paragrafo 6.1.1], mediante la modifica della partizione di *recovery* e in taluni casi del *bootloader*, la procedura di rooting comporta l'installazione di un file binario di *SU* all'interno della partizione di sistema che sarà controllabile dall'utente mediante l'omonima applicazione *SuperUser*. Rispetto ai primi tentativi di hacking dei device mobili Android, la procedura è stata notevolmente semplificata con gli anni, e ora consiste nell'installazione ed esecuzione a mezzo terminale di un software specifico per il modello di cellulare da trattare. In dettaglio i passaggi che consentono di ottenere i diritti di root sono i seguenti:

1. Decidere opzionalmente, o espressamente ove richiesto, di sbloccare il `bootloader`;
2. Modificare la `recovery`, installando al posto di quella di fabbrica una versione modificata;
3. Installare tramite la nuova `recovery` i file necessari a compiere la modifica dei diritti, che andranno a collocarsi all'interno della partizione `system`.

6.1.3 Acquisizione

Dopo aver ottenuto i permessi di root sarà possibile accedere ad ogni cartella del sistema e quindi si potrà procedere ad un'acquisizione completa del dispositivo. La buona tecnica forense prevede che si proceda preventivamente alla creazione di una copia della memoria, anche detta immagine, su cui si andrà ad attuare l'analisi in modo da renderla perfettamente ripetibile. Esistono diversi possibili metodi per acquisire i dati conservati nel file system del sistema, ne verranno di seguito approfonditi due.

Accesso remoto tramite ADB

L'interazione con i dispositivi Android è possibile mediante l'interfaccia ADB⁶, previa abilitazione della modalità `debug USB` sul dispositivo. Lanciando il servizio ADB con i permessi di root sarà possibile esplorare l'intero file system senza limitazioni e scaricare sulla workstation i file di interesse.

Accesso remoto tramite ssh

È altrimenti possibile acquisire i file del device ricorrendo all'utilizzo del comando `dd` da eseguire mediante tastiera virtuale sul dispositivo (previa installazione di un'applicazione che emuli il terminale) oppure attraverso una

⁶*Android Debug Bridge*, strumento incluso nell'SDK di Android che consente la comunicazione device-computer tramite una shell Linux.

connessione `ssh`. In questo modo è possibile generare una copia forense che sarà memorizzata all'interno di una delle memorie riconosciute del dispositivo: quella flash interna o quella SD removibile. La clonazione dell'intera memoria non è possibile in una sola sessione, è quindi necessario eseguire il comando `dd` per ogni partizione montata dal dispositivo [[FRtt]].

6.1.4 Analisi dei file di interesse

Terminata l'acquisizione dell'intera memoria del device o delle sole directory di interesse, una copia dei dati sarà disponibile sulla workstation o su una periferica da essa leggibile e si potrà procedere all'analisi.

Su Android i dati di interesse come ad esempio sms, chiamate, cronologia di navigazione internet, sono contenuti all'interno di database memorizzati in file con estensione `.db` o simili. Solitamente tali file sono conservati in sotto-directory del percorso `/data`⁷; individuandoli sarà possibile procedere alla loro analisi tramite l'utilizzo di qualunque software in grado di gestire basi di dati.

Nel Capitolo 7 verrà illustrato un caso concreto, mostrando la procedura necessaria per ottenere i diritti di root su un dispositivo di marca *Huawei*. Sullo stesso saranno poi messi in atto alcuni dei metodi appena illustrati per acquisire e analizzare i dati.

6.2 Acquisizione mediante jailbreaking

6.2.1 Nozioni generali sul sistema operativo iOS

iOS⁸, sviluppato da Apple, è un sistema operativo per dispositivi portatili rilasciato originariamente per iPhone e poi esteso agli altri device dello stesso produttore. iOS deriva da Mac OS X e la sua interfaccia utente è basata sul

⁷Tale percorso può variare da cellulare a cellulare.

⁸Per maggiori informazioni si veda www.apple.com/it/ios/what-is/.

concetto di manipolazione diretta: gli oggetti di interesse sono ben visibili e ad ogni azione consegue sempre un feedback immediato. Si tratta del secondo sistema operativo per diffusione⁹, installato unicamente su hardware Apple.

Architettura di iOS

Partendo dal basso, l'architettura di iOS risulta essere così composta:

- **Livello Core OS** - interagisce direttamente con l'hardware e gestisce principalmente memoria, file system, networking e power management;
- **Livello Core Service** - composto dai servizi utilizzati dalle applicazioni durante la loro esecuzione;
- **Livello Media** - si occupa della gestione dei servizi collegati ad audio, video e immagini;
- **Livello Cocoa Touch** - offre un'interfaccia alle librerie necessarie allo sviluppo di applicazioni

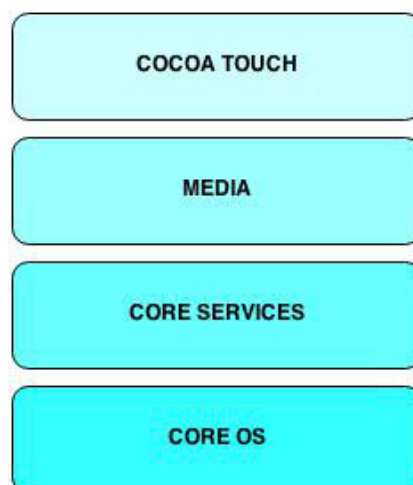


Figura 6.2: Architettura del sistema operativo iOS.

⁹Con una quota di mercato del 14% ad agosto 2013 [Relti].

Partizioni di sistema

Al fine di estrarre e analizzare i contenuti della memoria è necessario conoscere come sono organizzati i dati al suo interno. La memorizzazione dei dati avviene solitamente nella memoria flash interna [Paragrafo 3.3], il cui spazio è suddiviso nelle seguenti partizioni:

- **Partizione di sistema** - ospita i dati del sistema operativo e delle applicazioni native. Durante il normale funzionamento del device questa partizione è acceduta in sola lettura mentre durante gli aggiornamenti del sistema è acceduta in lettura e scrittura. Il contenuto di tale partizione è tipicamente di scarso interesse per gli operatori forensi, ma può essere utile verificare se siano state attuate modifiche al sistema operativo;
- **Partizione dati** - occupa il restante spazio della memoria e contiene i dati dell'utente nonché tutti i contenuti generati, scaricati e sincronizzati durante il normale utilizzo del device.

La memorizzazione dei dati dell'utente e delle applicazioni avviene con modalità diverse: una parte dei dati è organizzata all'interno del file system¹⁰ mentre la parte concernente le informazioni personali (come ad esempio contatti, sms, email, etc.) è memorizzata all'interno di file di database SQLite e altri file di tipo `.plist`, che sono a loro volta conservati nel file system.

Meccanismi di protezione del sistema

Su iOS sono implementati alcuni meccanismi di sicurezza, detti "di jail", per controllare l'accesso a funzionalità e dati del dispositivo. Tali protezioni possono essere disabilitate grazie alle tecniche di *jailbreaking* che, sfruttando alcune vulnerabilità della piattaforma, vanno a sostituire (temporaneamente o in via definitiva) il kernel originale con uno modificato e privo di protezioni. La procedura in questione non deve essere confusa con quella di *unlocking*

¹⁰Di tipo HFS.

[Paragrafo 4.2], altro meccanismo di “evasione” messo in atto per poter utilizzare il proprio iPhone con una SIM-card diversa da quella abbinata al dispositivo al momento dell’acquisto.

6.2.2 Rimozione dei meccanismi “di jail”

Con il termine *jailbreaking* ci si riferisce al processo attraverso il quale si possono rimuovere le limitazioni al sistema operativo imposte dalla casa produttrice, prima tra tutte la l’impossibilità di installare applicazioni non disponibili sullo store ufficiale (**App Store**). Il jailbreaking è una forma di *privilege escalation* ossia di superamento delle autorizzazioni, un meccanismo che sfrutta un bug del sistema per acquisire il controllo di risorse che altrimenti sarebbero precluse. Tale modifica permette infatti di disabilitare, in via permanente o meno, il controllo dei certificati di autenticità che impedisce l’esecuzione di codice sviluppato da terze parti. Solitamente la procedura di jailbreaking prevede l’utilizzo di un software di gestione pacchetti, ad esempio Cydia¹¹, che consente agli utenti di installare applicazioni che non fanno parte del *repository* ufficiale AppStore [Zdz12].

È comunque sempre possibile ripristinare un dispositivo *jailbroken* tramite l’utilizzo di iTunes.

Tipologie

Esistono diverse tipologie di jailbreaking [Guiti]:

- **Tethered** - dall’inglese *legato*, si tratta di una versione non effettiva, ossia non permanente: ogni volta che il dispositivo viene spento o riavviato si blocca. Questo avviene perchè la modifica avviene solo a livello di firmware, e quindi si annulla ogni volta che il device ricarica il boot di sistema. Per sbloccare il dispositivo, reso inutilizzabile dopo uno spegnimento, occorre connetterlo ad un computer e utilizzare lo stesso

¹¹Sito ufficiale: <https://cydia.saurik.com/>.

software con cui si era compiuta l'operazione di jailbreaking, altrimenti le uniche alternative sono il ripristino alle impostazioni di fabbrica o il ripristino tramite backup, entrambi da compiersi con iTunes. Il fatto che il dispositivo non possa essere spento non è solitamente un grave problema per l'utente medio dal momento che device come questi si prestano per loro natura a rimanere sempre accesi. È una versione ovviamente poco pratica, pensiamo ad esempio ad uno spegnimento accidentale dovuto allo scaricamento della batteria, ma più semplice da realizzare;

- **Untethered** - dall'inglese *slegato*, si tratta di una versione permanente, tramite la quale non si riscontrano problemi in caso di spegnimenti o riavvii del dispositivo. È resa possibile da una modifica che va ad agire a livello di **boot**;
- **Semi-tethered** - si tratta di un jailbreak quasi effettivo che consente di spegnere o riavviare il dispositivo ma inibisce l'utilizzo di alcune applicazioni native. È una versione più recente delle altre e quindi ancora poco diffusa.

6.2.3 Acquisizione

Per aver pieno accesso ai dati del sistema e quindi poter generare una copia forense dei contenuti del device occorre quindi:

1. Sostituire il kernel originale con uno modificato privo dei meccanismi di protezione che impedirebbero pieno accesso alla memoria;
2. Caricare e attivare sul dispositivo un *software agente* attraverso il quale operare l'estrazione dei contenuti. Questo programma rimarrà in attesa di comandi da parte della workstation;
3. Acquisire e inviare alla workstation l'immagine della memoria. Dato che questa viene generata in *live forensics* da un device con processi in esecuzione, potrebbe presentare delle inconsistenze.

6.2.4 Analisi dei file di interesse

Disponendo dell'immagine forense sulla workstation è possibile procedere all'analisi. Questa può essere fatta a livello logico o fisico [Paragrafi 5.2.2 e 5.2.3]: ricordiamo che l'analisi logica dei dati permette, attraverso la lettura del file system, l'accesso logico ai file memorizzati, mentre invece quella fisica effettua una scansione del contenuto grezzo della memoria e va a recuperare qualunque sequenza ammissibile di file conosciuti. Gli strumenti utilizzati solitamente per l'estrazione fisica sono detti di *carving*; ne sono un esempio `Foremost` e `Scalpel`. Essi operano scansionando interamente il file immagine alla ricerca di sequenze di byte che corrispondano a strutture note.

Nel Capitolo 7 verrà illustrato un caso concreto, mostrando la procedura necessaria a rendere *jailbroken* un dispositivo iPhone. Sullo stesso saranno poi messi in atto i metodi appena illustrati per acquisire e analizzare i dati.

Capitolo 7

Risultati ottenuti con metodologie finalizzate all'analisi forense

7.1 Presentazione dello studio

In questo capitolo si intende mettere a confronto i risultati ottenuti utilizzando vari strumenti software commercializzati con la dizione “forense”, software per la gestione dei contenuti (iTunes) e tecniche di analisi più invasive basate sull'alterazione del sistema del device al fine di procedere all'acquisizione completa dei dati memorizzati [Capitolo 6].

7.1.1 Device analizzati

I test sono stati condotti su uno smartphone con sistema operativo Android [Paragrafo 6.1.1] e uno smartphone con sistema operativo iOS [Paragrafo 6.2.1], nello specifico:

- **Device 1:** Vodafone 858 Smart, anche conosciuto come Huawei U8160, dispositivo con sistema operativo Android nella sua versione 2.2.1 [Figura 7.1]. Per lo svolgimento dei test è stato necessario attivare la



Figura 7.1: Device analizzati: *Vodafone 858 Smart* e *Apple iPhone 3GS*

modalità sviluppo (Debug USB) tramite il menu:

Impostazioni > Impostazioni applicazioni > Sviluppo;

- **Device 2:** Apple iPhone 3GS, con sistema operativo iOS nella sua versione 6.1.3 [Figura 7.1]. Per lo svolgimento dei test è stato necessario disabilitare il blocco automatico del display tramite il menu: Impostazioni > Generali > Blocco automatico.

Entrambi i dispositivi erano funzionanti e in buone condizioni, utilizzati in precedenza da un utente medio. I loro sistemi operativi non presentavano alterazioni di alcun tipo ed erano entrambi privi di UICC e memorie esterne.

7.1.2 Software utilizzati

Tutti i software sono stati eseguiti o installati su un computer con sistema operativo Windows 7 Professional (durante la trattazione ci si riferirà ad esso con il termine di *workstation*).

Software forensi

Per lo svolgimento dei test sono stati utilizzati quattro diversi software forensi, le cui caratteristiche e modalità sono illustrate di seguito:

- **Paraben's DDS (Deployable Device Seizure)**¹, nella versione 4.0 build 4891.29553.

Le modalità di acquisizione disponibili sono:

- **Textual data**, acquisizione di tipo logico che consente di ottenere i principali dati relativi all'utente;
- **All data**, acquisizione avanzata di tipo logico che consente di ottenere dati aggiuntivi rispetto a quelli della modalità precedente.

- **Paraben's Device Seizure**², nella versione 6.5 build 5078.1901. Le modalità di acquisizione disponibili sono:

- **Logical**, acquisizione di tipo logico che consente di ottenere i principali dati relativi all'utente;
- **Physical**, acquisizione di tipo fisico che include i file di sistema e i dati cancellati (compatibilmente con le restrizioni del dispositivo).

- **Oxygen Forensic Suite 2014**³, nella standard version 6.0.1.184. Le modalità di acquisizione disponibili sono:

- **Recommanded mode**, acquisizione di tipo logico che consente di ottenere i principali dati relativi all'utente;
- **Advanced mode with physical dump**, acquisizione che prevede la creazione di una copia bit-a-bit della memoria e la sua analisi (compatibilmente con le restrizioni del dispositivo).
- **Advanced mode with logical extraction (selected view)**, acquisizione di tipo logico che consente di ottenere, previa selezione, i principali dati dell'utente;
- **Advanced mode with logical extraction (complete view)**, acquisizione di tipo logico che consente di ottenere, previa selezione, i principali dati dell'utente e i file di sistema.

¹Sito ufficiale: www.paraben.com/dds.html

²Sito ufficiale: www.paraben.com/device-seizure.html

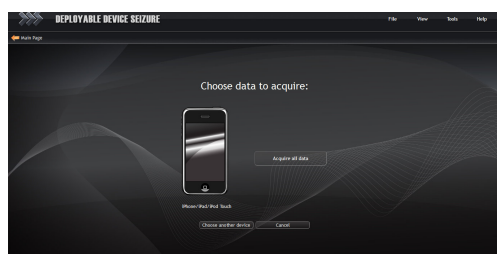
³Sito ufficiale: www.oxygen-forensic.com/en/features/standard

- **Compelson's MOBILedit!**⁴, nella versione lite 7.5.3.4200.

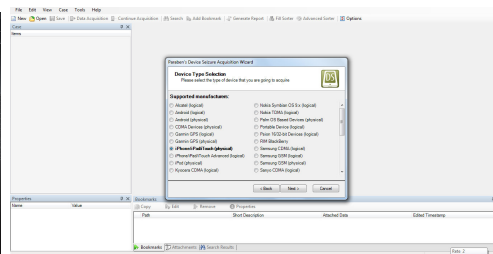
Dispone di un'unica modalità di acquisizione che consente di ottenere i dati dell'utente, delle applicazioni installate ed i file presenti nella memoria (compatibilmente con le restrizioni del dispositivo).

La disponibilità o meno di una data modalità è dipesa strettamente dal device analizzato: le modalità realmente utilizzate saranno illustrate in seguito [Paragrafo 7.3]. In Figura 7.2 vi sono alcune schermate dimostrative dei software menzionati: è stato possibile utilizzare i primi due in versione completa, il terzo in versione *freeware* (con licenza di sei mesi) e l'ultimo in versione ridotta. Le limitazioni di questi ultimi non hanno avuto ripercussioni sui test: *Oxygen* aveva funzionalità complete e *MOBILedit!* impediva soltanto il salvataggio dei risultati delle acquisizioni e l'accesso a funzionalità avanzate.

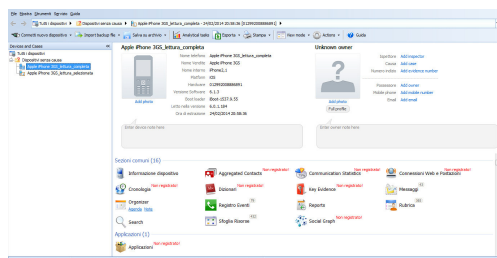
⁴Sito ufficiale: www.mobiledit.com/forensic



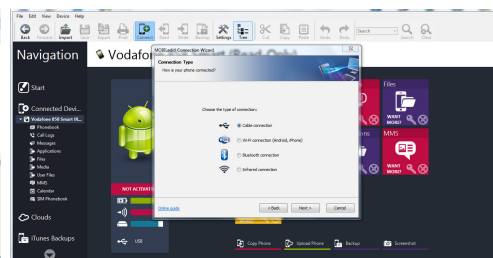
(a) Paraben's DDS



(b) Paraben's Device Seizure



(c) Oxygen Forensic suite



(d) Compelson's MOBILedit!

Figura 7.2: Software forensi utilizzati.

Software non forensi

I software utilizzati per mettere in atto le procedure “sperimentali” sono stati per il device 1 (Android):

- **SuperOneClick** nella versione 2.3.3, toolkit contenente diversi software per gestire Android, tra cui appunto **SuperOneClick.exe** per attuare il rooting;
- **ADB**, disponibile nell’SDK di Android e nel toolkit appena menzionato, per accedere da remoto al device;
- **SQLite Database Browser** nella sua versione 2.0b1, per la lettura dei file di database estratti.

I software utilizzati per la generazione e l’analisi dei backup del device 2 (iOS) sono stati:

- **iTunes** nell’ultima versione disponibile (11.1.4.62);
- **iPhone Backup Browser** nell’ultima versione disponibile (1.2.0.6), per la navigazione dei file di backup;
- **iBackupBot** nell’ultima versione disponibile (5.1.1.4), altro software per la navigazione dei file di backup.

Infine i software utilizzati per mettere in atto le procedure “sperimentali” su device 2 (iOS) sono stati:

- **Firmware originale** (in formato .ipsw) di iPhone 3GS nella ver 6.0;
- **Redsn0w** nella versione 0.9.15b3, per attuare il jailbreaking di tipo *tethered*;
- **Cydia**, installatore di pacchetti non ufficiali, automaticamente installato sul device durante il jailbreaking;

- **P0sixspwn** pacchetto scaricabile tramite Cydia (dopo aver effettuato il jailbreaking tethered del device) per rendere il jailbreaking *untethered*;
- **OpenSSH** nell'ultima versione disponibile (6.1), pacchetto scaricabile tramite Cydia, per rendere possibile l'accesso remoto al device, via protocollo SFTP;
- **WinSCP** nell'ultima versione disponibile (5.5.1), client FTP per effettuare la connessione al device da remoto;
- **SQLite Database Browser** nell'ultima versione disponibile (2.0b1), nuovamente per la lettura dei file di database estratti;
- **PlistEditor Pro** nell'ultima versione disponibile (2.1), per la lettura dei file `.plist`.

7.2 Attuazione dei test

7.2.1 Test su device1 (Android)

1) Acquisizione forense

Non saranno oggetto della trattazione i passaggi che hanno condotto, per ogni singolo software, all'acquisizione del device, per i quali si rimanda alle documentazioni ufficiali dei singoli prodotti. Saranno invece affrontate le problematiche riscontrate durante il loro utilizzo.

Note sull' utilizzo di Oxygen Forensic Le acquisizioni sono avvenute sul dispositivo non *rootato*, condizione che non ha consentito la corretta esecuzione delle attività del software **Oxygen Forensic**. Tutte le modalità di acquisizione previste da tale prodotto (*Recommended mode* e *Advanced mode* in tutte le sue declinazioni) sono fallite per l'impossibilità di installare l'agente **OxyAgent** sul dispositivo. Per completezza si è così deciso di eseguire nuovamente il test con il programma dopo aver acquisito i diritti di

root [Paragrafo 7.2.1]. Il test effettuato dopo il rooting del dispositivo ha dato comunque esito negativo per la *Recommended mode*, ma ha avuto esito parzialmente positivo (acquisizione completata ma con avvertimenti) per le *Advanced mode with logical extraction (selected view)* e *Advanced mode with logical extraction (complete view)*.

2) Acquisizione sperimentale

Fase 1 - Rooting Per ottenere il pieno accesso in lettura e scrittura a tutte le directory del file system del dispositivo è stato necessario attuare il rooting del device [Paragrafo 6.1].

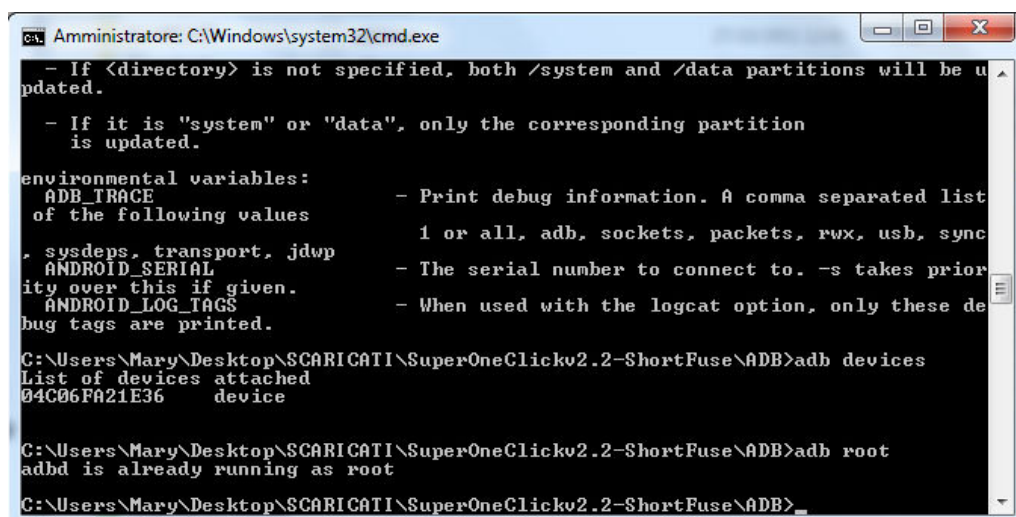
La prima via tentata è stata quella di utilizzare l'app **z4root**, compatibile col modello di cellulare in oggetto. Questa è stata installata tramite terminale remoto (shell di ADB) e poi avviata sul dispositivo: il rooting a livello di applicazione è stato eseguito propriamente (dal device, tramite l'app **RootBrowser**, era possibile accedere alle cartelle in precedenza protette), ma il demone del terminale remoto (**adbd**) non ha ottenuto i medesimi privilegi di root e quindi i comandi lanciati erano eseguiti come utente non privilegiato. Questa condizione è stata rilevata utilizzando il comando `getprop ro.secure` che ha restituito il valore `ro.secure=1` invece che `ro.secure=0` [Chuti]. Dal momento che tale valore non è modificabile da remoto, e che quindi tali privilegi non erano aggiornabili, si è deciso di cambiare approccio. Il cellulare è stato quindi *de-rootato* tramite **z4root** e ripristinato alla condizione di partenza.

La seconda via intrapresa si è rivelata corretta: utilizzando il software **SuperOneClick.exe** è stato possibile *rootare* il device 1, collegato alla workstation mediante cavo USB. È bastato eseguire il programma sulla workstation (non necessitando di installazione) e seguire le istruzioni fornite a video.

Fase 2 - Acquisizione tramite accesso remoto Successivamente, mantenendo lo stesso collegamento cablato, si è utilizzato ADB per accedere al device da remoto. Il cellulare è stato montato, è stata verificata la condizione di root [Figura 7.3] e infine si è proceduto all'acquisizione dei file di interesse (contenuti in questo caso specifico al percorso /data), mediante copia di tale directory e dei suoi contenuti sulla workstation. I comandi usati sono stati:

```
adb
adb devices
adb root
adb pull <remote> <local>
```

Fase 3 - Analisi dei file I file di nostro interesse sono in particolare quelli di database, nei formati .sqlitedb e .db; nel nostro caso sono stati rilevati 75 file .db. Successivamente i file in questione sono stati analizzati con il software SQLite Database Browser.



```
Administrator: C:\Windows\system32\cmd.exe
- If <directory> is not specified, both /system and /data partitions will be updated.
- If it is "system" or "data", only the corresponding partition is updated.

environmental variables:
  ADB_TRACE                - Print debug information. A comma separated list of the following values: adb, sockets, packets, rwx, usb, sync, sysdeps, transport, jdwp
  ANDROID_SERIAL           - The serial number to connect to. -s takes priority over this if given.
  ANDROID_LOG_TAGS         - When used with the logcat option, only these debug tags are printed.

C:\Users\Mary\Desktop\SCARICATI\SuperOneClickv2.2-ShortFuse\ADB>adb devices
List of devices attached
04C06FA21E36    device

C:\Users\Mary\Desktop\SCARICATI\SuperOneClickv2.2-ShortFuse\ADB>adb root
adb is already running as root

C:\Users\Mary\Desktop\SCARICATI\SuperOneClickv2.2-ShortFuse\ADB>
```

Figura 7.3: Shell di ADB

Alcune delle informazioni raccolte sono state ad esempio:

- Contatti e registro chiamate (`contacts.db`);
- Calendari ed eventi (`calendars.db`);
- Messaggi testuali e multimediali (`mmssms.db`);
- Preferiti (`browser.db`) e cronologia di navigazione (`qsb-history.db`);
- Parole aggiunte al dizionario (`User_dict`);

È stato inoltre possibile raccogliere i dati di alcune applicazioni: le principali sono state *Facebook*, *WhatsApp* e *Gmail*. Il dettaglio dei percorsi e file in cui è stato possibile leggere tali informazioni è riportato in Tabella 7.1.

In Figura 7.4 è presentato un esempio della struttura di una tabella di uno dei database, nello specifico quello contenente SMS e MMS (file `mmssms.db`).

7.2.2 Test su device2 (iOS)

1) Acquisizione forense

Non saranno oggetto della trattazione i passaggi che hanno condotto, per ogni singolo software, all'acquisizione del device, per i quali si rimanda alle

Field Name	Field Type	Table Name	Table Definition
_id	INTEGER PRIMARY KEY	sms	CREATE TABLE sms (_id INTEGER PRIMARY KEY, threa...
thread_id	INTEGER		
address	TEXT		
person	INTEGER		
date	INTEGER		
protocol	INTEGER		
read	INTEGER		
status	INTEGER		
type	INTEGER		
reply_path_present	INTEGER		
subject	TEXT		
body	TEXT		
service_center	TEXT		
locked	INTEGER		
error_code	INTEGER		
seen	INTEGER		
		raw	CREATE TABLE raw (id INTEGER PRIMARY KEY,date ...

Figura 7.4: Struttura di una tabella del database `mmssms.db`

documentazioni ufficiali dei singoli prodotti. Saranno invece affrontate le problematiche riscontrate nel loro uso.

Note sull' utilizzo dei prodotti Paraben Non è stato possibile attuare le acquisizioni del device, in tutte le modalità, con i due software della Paraben, DDS e Device Seizure. Vi sono stati problemi di compatibilità device-workstation che non hanno impedito l'avvio della procedura di acquisizione, nonostante fossero stati installati tutti i software e driver richiesti.

2) Acquisizione mediante iTunes

iTunes, oltre che come riproduttore musicale è utilizzato anche per la gestione dei device di Apple. Collegando (via WiFi o USB) ad esempio, un iPhone ad un computer, tramite tale software sarà possibile sincronizzare la maggior parte delle informazioni del device. Il protocollo utilizzato per il trasferimento dei dati è AFC⁵, attraverso il quale non vengono alterati i dati del device (ad eccezione di quelli relativi alle chiavi di crittografia) [Bti].

Connettendo il device alla workstation per la prima volta, si avvia automaticamente la sincronizzazione, attraverso la quale iTunes crea una directory dedicata al device (dandole il nome dell'UDID⁶ del dispositivo e salvandone all'interno i contenuti). Creato il nuovo percorso, tutte le volte che il device verrà connesso alla workstation avverrà la sincronizzazione e quindi l'aggiornamento di tali file. La directory viene salvata in un percorso specifico che varia a seconda del sistema operativo in uso, nel nostro caso lavorando su Windows 7, sono reperibili in:

C:\Users\[Utente]\AppData\Roaming\Apple Computer\MobileSync\Backup.

I file aggiunti automaticamente alla directory menzionata si presentano con estensione non leggibile [Figura 7.5]. Per poter analizzare i loro contenuti si è utilizzato il software iBackupBot tramite il quale è stato possibile raccogliere informazioni sull'utente e file multimediali:

⁵Apple File Connection

⁶Unique Device ID, un codice esadecimale lungo 40 caratteri.

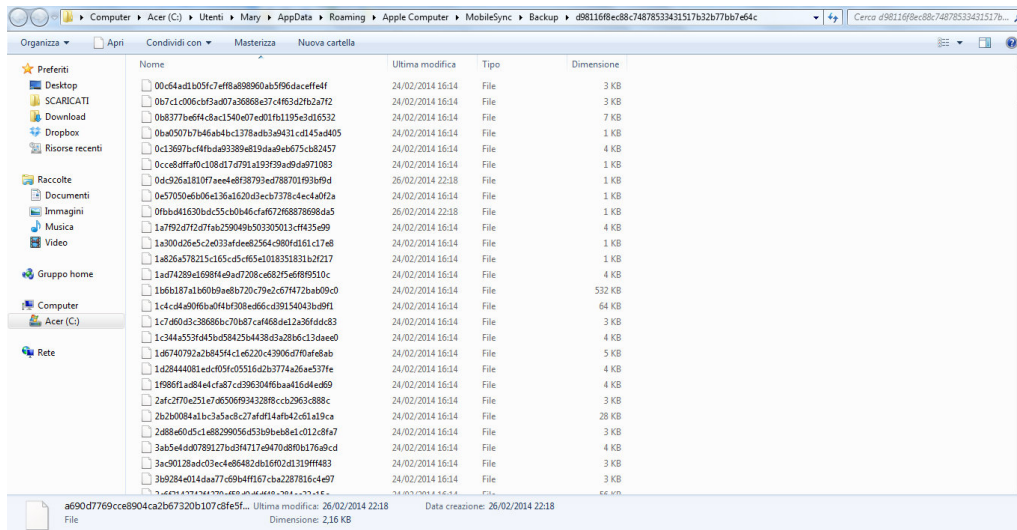


Figura 7.5: File contenuti nella cartella di backup

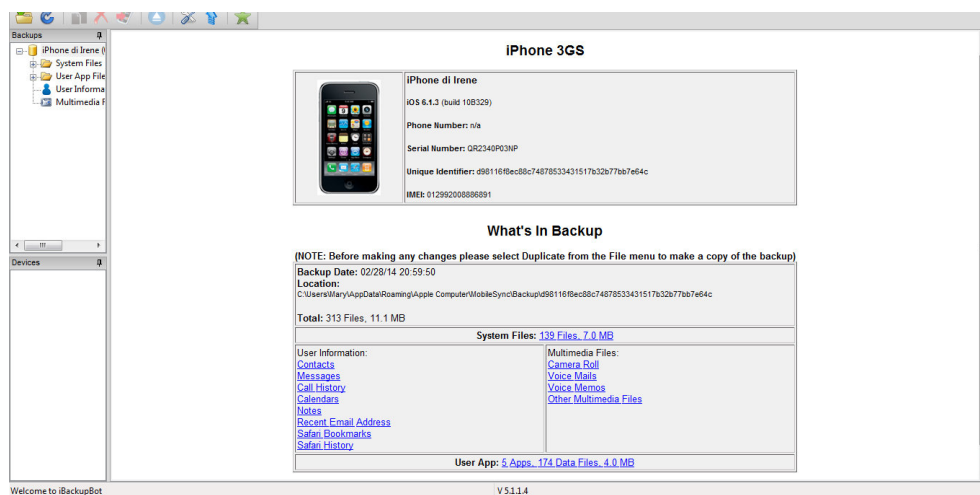
- Contatti (`AddressBook.sqlitedb`);
- Messaggi (`Sms.db`);
- Storico delle chiamate (`Call_history.db`);
- Calendari ed eventi (`Calendar.sqlitedb`);
- Note (`Notes.sqlite`);
- Indirizzi delle ultime mail inviate (`Recent.db`);
- Dati di Safari quali i preferiti `Safari/Bookmarks.db` e le cronologia di navigazione `Safari/History.plist`;
- Fotografie scattate.

Tali dati erano presentati all'interno di una vista logica fornita dal programma [Figura 7.6 (a)], ma veniva comunque data la possibilità di estrarre (e quindi poter esplorare) i file da cui tali informazioni erano state estrapolate.

Per completare l'analisi si è ricorso all'uso del software `iPhone Backup Browser` per navigare direttamente i file contenuti nella directory [Figura 7.6 (b)]: appresi i nomi reali si è potuto modificare manualmente le estensioni dei file per renderli

84 7. Risultati ottenuti con metodologie finalizzate all'analisi forense

leggibili. Quindi con i programmi SQLite Database Browser e plistEditor Pro sono stati letti i file di database e i file .plist.



(a) Vista del software iBackupBot

Display Name	Name	Files	Size	App Size
	System	138	1.962	
com.apple.weather	com.apple.weather	N/A	0	
com.apple.WebView.Service	com.apple.WebView.Service	N/A	0	
com.facebook.Facebook	com.facebook.Facebook	5	77.267	
com.vodafone.contacts	com.vodafone.contacts	8	59.788	
net.whatsapp.WhatsApp	net.whatsapp.WhatsApp	151	4.104.782	

Name	Size	Date	Domain	Key
keychain-backup.plist	34.429	29/02/2014 19:59:46	KeychainDomain	51e4616e5750d33c2dabedf8e5746b9f248f0e
Library/Accounts/Accounts2.sqlite	90.112	15/12/2013 07:38:03	HomeDomain	9432346112c7b3002c0d59e1110022356e365e
Library/AddressBook/AddressBook.sqlite	250.048	24/02/2014 20:39:49	HomeDomain	31bb_7ba931476644b40d56b5113a3b614be442
Library/AddressBook/AddressBook/images.sqlite	335.872	24/02/2014 20:39:49	HomeDomain	cd57020ee29e893f230a76794405ab17930ee
Library/BulletinBoard/BehaviorOverrides.plist	1.496	14/12/2013 17:39:55	HomeDomain	3418406efac25598db103ac505c1e1a3a35e4e36
Library/BulletinBoard/CleanedSections.plist	126	20/02/2014 19:57:17	HomeDomain	648652c3f74ed59a76b0ca2b6e79651e65c2b71d
Library/BulletinBoard/SectionInfo.plist	19.093	18/12/2013 06:37:24	HomeDomain	3d8e6530ca29c3835470e1c45a747e249f8584
Library/BulletinBoard/SectionOrder.plist	911	18/12/2013 06:37:24	HomeDomain	910e28e5a76cc77740ac5d51545e68ad59f9491
Library/Caches/com.apple.mobilesafari/Thumbnails/06F5CE4F-DF4D-4D8A-821...	9.594	15/12/2013 07:40:55	HomeDomain	540e77c072b53eb0c384344ec08a92779e058ad
Library/Caches/com.apple.mobilesafari/Thumbnails/71A4E464-C0C2-457E-8A2...	43.898	18/12/2013 06:42:26	HomeDomain	4e56f0e47e322472b54db0c0e081185199214f6
Library/Caches/locationd/clients.plist	2.220	20/02/2014 14:18:54	RootDomain	695947789e6994ca2b367f300b10793e8f9412
Library/Caches/locationd/consolidated.db	20.480	24/02/2014 15:12:26	RootDomain	4096c9ec57892847dc283405900e284a7c915836
Library/Calendar/Calendar.sqlite	393.216	24/02/2014 20:39:26	HomeDomain	204145105e04d39dab481178355d6f701e5858
Library/Calendar/Extras.db	28.672	24/02/2014 15:12:28	HomeDomain	Zb97b3c3890dfc0e0805c52392e0e0e0e9f8d
Library/CallHistory/call_history.db	28.672	21/12/2013 20:57:56	WirelessDomain	2b2b1094a1ac2ab5e0c270df4f14db42c51e18ca
Library/com.apple.iTunes/iTunesStore/private.sqlite	57.344	14/12/2013 17:34:53	HomeDomain	80c42a29a2b6877c49781e1ae246efc599c3c
Library/com.apple.iTunes/iTunesStore2.sqlite	49.152	14/12/2013 17:26:13	HomeDomain	9143d986a77ab8cf5878e4e9ac80627477eb6674
Library/com.apple.iTunes/iTunesStore/keys.sqlite	28.672	20/02/2014 15:59:38	HomeDomain	af0e461e0b53220c029e0c42e7841ec0b09f9
Library/Configuration/Profiles/ClientTrust.plist	181	14/12/2013 17:50:49	HomeDomain	8d4e080c746556c74f4f1e1b50595c3159d0a3d
Library/Configuration/Profiles/MCDataMigration.plist	288	14/12/2013 17:26:35	HomeDomain	01e4e944e4421c3053d117201ac5571e5236
Library/Configuration/Profiles/PayloadManifest.plist	263	14/12/2013 17:26:22	HomeDomain	45b1e3778ee198a9e2df128469e2e9e5403e6f
Library/Configuration/Profiles/ProfileTrust.plist	181	14/12/2013 17:26:24	HomeDomain	f7bbe53e1427d2ee89e4995720b811289d46a38
Library/Configuration/Profiles/PublicInfo/EffectiveUserSettings.plist	4.981	25/02/2014 23:36:58	HomeDomain	23461ac2b578f102d598e9e78e500600204a5
Library/Configuration/Profiles/PublicInfo/MCMeta.plist	243	14/12/2013 17:26:24	HomeDomain	10c305955e9f4e45eae05e74295797c5367305e
Library/Configuration/Profiles/UserSettings.plist	5.017	25/02/2014 23:36:58	HomeDomain	3432b051212e4311c705fa598c4db8c5ee8002

(b) Vista del software iPhone Backup Browser

Figura 7.6: Software utilizzati per navigare ed estrarre i file di backup

3) Acquisizione sperimentale

Fase 1 - Jailbreaking tethered Per attuare la prima fase di jailbreaking, quella *tethered* [Paragrafo 6.2.2] si è utilizzato `Redsn0w`. Si è avviato il programma sulla workstation, dopodichè il device è stato connesso (acceso) tramite cavo USB. È stato necessario caricare il firmware di iOS 6.0 (scaricato in precedenza) e seguire le istruzioni a video del programma, ossia lo spegnimento del device e l'avvio della `DFU mode`⁷. Successivamente, al riavvio del device è stato necessario selezionare nuovamente il firmware ed attuare la procedura di `boot`, sempre via cavo, per rendere il *jailbreaking tethered* effettivo.

Fase 2 - Jailbreaking untethered Dopo aver portato a termine la procedura della fase precedente, il device si presenta acceso e *jailbroken tethered*; il collegamento cablato con la workstation non è più richiesto. A questo punto è stato necessario attivare il WiFi del device (agendo tramite il menu impostazioni) e aprire l'app `Cydia` che si è automaticamente installata durante la fase precedente. L'applicazione ha dovuto eseguire alcuni aggiornamenti essenziali, dopodichè si è potuto utilizzarla per scaricare il pacchetto `P0sixspwn`, la cui installazione ha reso il *jailbreaking untethered*. Il successo dell'operazione è stato verificabile tramite spegnimento e successiva riaccensione, andata a buon fine, del device.

Fase 3 - Acquisizione tramite accesso remoto Dopo aver attuato il *jailbreaking* del device (la condizione di *untethering* non era obbligatoria ma è stata preferita per praticità), si può effettuare il backup manuale dei dati dell'utente, ossia un'acquisizione completa di tali dati sulla workstation. Tramite `Cydia` è stato necessario installare il pacchetto `OpenSSH` per poter utilizzare il protocollo SFTP e quindi accedere da remoto al device, tramite collegamento USB o connessione di entrambi alla stessa rete locale; si è preferito il secondo approccio. Come client FTP sulla workstation è stato utilizzato `WinSCP`.

⁷La modalità `Device Firmware Update` è una procedura tramite la quale è possibile aggiornare o ripristinare il firmware del device. Si attua collegando il device alla workstation e premendo una combinazione di tasti (per 3 secondi il tasto di `accensione`, poi senza rilasciarlo premere il tasto `home` per 10 secondi e infine rilasciare il tasto `accensione` mantenendo premuto quello `home` per altri 10 secondi).

86 7. Risultati ottenuti con metodologie finalizzate all'analisi forense

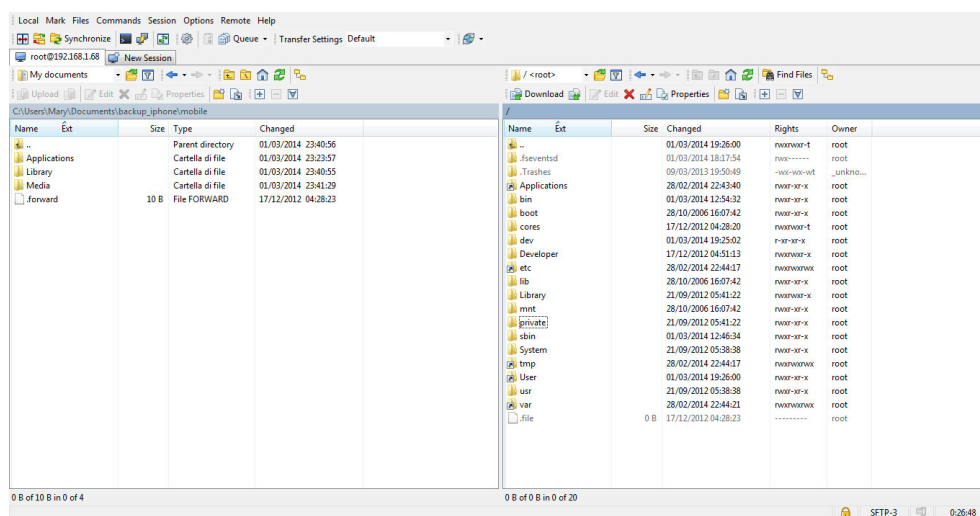


Figura 7.7: Directory di iOS copiate tramite SFTP

Per poter mettere in atto la connessione è stato necessario recuperare l'indirizzo IP del device tramite menu **Impostazioni > WiFi > rete connessa**. Successivamente si è configurata la connessione, tramite WinSCP, impostando i seguenti parametri:

Protocollo: SFTP

Nome Server: indirizzo IP device

Numero Porta: 22

Username: root

Password: alpine (di default)

Avviando la connessione creata è stato possibile copiare i file del device sulla workstation. Si è proceduto quindi all'acquisizione delle directory di interesse [Figura 7.7], quelle contenute all'interno del percorso `/private/var/mobile`, ossia:

- **Applications** - dati relativi alle applicazioni scaricate;
- **Library** - dati relativi alle applicazioni native;
- **Media** - contenuti multimediali generati o acquistati dall'utente.

Fase 4 - Analisi dei file Nelle cartelle appena citate si trovano diversi elementi di interesse, in particolar modo i file database (in formato `.sqlite` e `.sqllitedb`): ne sono stati rilevati 23 [Paragrafo 7.2.2]. Anche in questo caso per l'analisi è stato utilizzato il software `SQLite Database Browser`.

7.3 Presentazione dei risultati

7.3.1 Risultati acquisizione device 1 (Android)

Vengono presentati in Tabella 7.1 i risultati ottenuti dalle acquisizioni del device 1, in termini puramente quantitativi. Sulle righe sono riportate le tipologie di dato, mentre sulle colonne vi sono le modalità di acquisizione, da leggersi mediante la legenda riportata nella pagina seguente. I valori contrassegnati da * rappresentano i risultati che è stato possibile raccogliere tramite l'analisi dei file acquisiti (i cui percorsi sono specificati in Tabella 7.2 - la voce tra parentesi rappresenta la tabella specifica del database); gli altri valori sono invece stati raccolti mediante la lettura di una vista logica fornita dal software.

Occorre infine rilevare che per motivi di tempo non è stato possibile approfondire la ricerca dei contenuti multimediali (audio, video, foto) sul device; si è quindi preferito concentrare gli sforzi sulla ricerca di documenti, ottenendo i risultati riportati in Tabella 7.1.

Legenda

1. Software DDS con modalità *textual data*;
2. Software DDS con modalità *all data*;
3. Software Device Seizure con modalità *logical*;
4. Software Device Seizure con modalità *physical* - INCONSISTENTE;
5. Software MOBILedit! con l'unica modalità disponibile;
6. Software Oxygen con modalità *recommanded mode* - NON ESEGUITA;
7. Software Oxygen con modalità *advanced mode with physical dump* - NON ESEGUITA;
8. Software Oxygen con modalità *advanced mode with logical extraction (selected view)*, attuata previo rooting;
9. Software Oxygen con modalità *advanced mode with logical extraction (complete view)*, attuata previo rooting;
10. Estrazione sperimentale previo rooting.

Le modalità elencate erano quelle disponibili per il device in oggetto. Quelle contrassegnate dalla dicitura “non eseguita” sono state impossibili da attuare sul device: sono state avviate ma l’acquisizione si è conclusa con un messaggio di errore. Non avendo restituito alcun risultato, le voci sono presenti in legenda ma non in tabella. Inoltre la modalità contrassegnata con la dicitura “inconsistente” non è stata inclusa in tabella visto che non è stato possibile categorizzare correttamente i risultati ottenuti.

Tabella 7.1: Quantità dati estratti per modalità di acquisizione (Android)

	1	2	3	5	8	9	10
NATIVE APPS							
contacts	434	434	434	-	434*	434*	434*
calendars	-	5	-	-	5*	5*	5*
events	-	125	-	125	125*	125*	125*
events attendees	-	-	-	-	131*	131*	131*
call history	-	500	-	500	500*	500*	500*
mms history	-	2	-	2	2*	2*	2*
sms history	-	-	564	564	564*	564*	564*
(sms) canonical addresses	-	-	-	-	52*	52*	52*
(sms) threads	-	-	-	-	50*	50*	50*
(sms) words content	-	-	-	-	565*	565*	565*
bookmarks	-	106	-	-	106*	106*	106*
search history	-	1	-	-	1*	1*	1*
quick search box history	-	-	-	-	1*	1*	1*
auto dict	-	-	-	-	687*	687*	687*
user dictionary	-	-	-	-	25*	25*	25*
launcher favorites	-	-	-	-	20*	20*	20*
alarms	-	-	-	-	2*	2*	2*
INSTALLED APPS							
(Gmail) conversations	-	-	-	-	20*	20*	20*
(Gmail) messages	-	-	-	-	3*	3*	3*
(Gmail) downloads	-	-	-	-	4*	4*	4*
(Gmail) raw contacts	-	-	-	396	396*	396*	396*
(WhatsApp) raw contacts	-	-	-	165	166*	166*	166*
(WhatsApp) messages	-	-	-	-	12492*	12492*	12492*
(WhatsApp) chat list	-	-	-	-	61*	61*	61*
(WhatsApp) contacts	-	-	-	-	324*	324*	324*
(Facebook) search results	-	-	-	-	20*	20*	20*
(Facebook) photos	-	-	-	-	488*	488*	488*
(Facebook) albums	-	-	-	-	44*	44*	44*
(Facebook) notifications	-	-	-	-	18*	18*	18*
(Facebook) user statuses	-	-	-	-	25*	25*	25*
(Facebook) mailbox threads	-	-	-	-	35*	35*	35*
(Facebook) mailbox messages	-	-	-	-	140*	140*	140*
(Facebook) mailbox profiles	-	-	-	-	73*	73*	73*
(Facebook) friends	-	-	-	-	343*	343*	343*
(Facebook) info contacts	-	-	-	-	343*	343*	343*
CONTENTS							
documents (.txt)	-	-	-	-	27	27	27
documents (.log)	-	-	-	-	13	13	13
documents / downloads (.pdf)	-	-	-	-	1*	1*	1*
database (.db)	-	-	-	-	75	75	75

Tabella 7.2: Percorsi di estrazione dati (Android)

	PATH
NATIVE APPS	
contacts	com.android.providers.contacts/databases/contacts.db (contacts)
calendars	com.android.providers.calendar/databases/calendar.db (calendars)
events	com.android.providers.calendar/databases/calendar.db (events)
events attendees	com.android.providers.calendar/databases/calendar.db (attendees)
call history	com.android.providers.contacts/databases/contacts.db (calls)
mms history	com.android.providers.telephony/databases/mmssms.db (part)
sms history	com.android.providers.telephony/databases/mmssms.db (sms)
(sms) canonical addresses	com.android.providers.telephony/databases/mmssms.db (can_addresses)
(sms) threads	com.android.providers.telephony/databases/mmssms.db (threads)
(sms) words content	com.android.providers.telephony/databases/mmssms.db (words_content)
bookmarks	com.android.browser/databases/browser.db (bookmarks)
search history	com.android.browser/databases/browser.db (searches)
quick search box history	com.google.android.googlequicksearchbox/databases/qsbox-history.db (history)
auto dict	com.android.inputmethod.latin/databases/auto_dict.db (words)
user dictionary	com.android.providers.userdictionary/databases/user_dict.db (words)
launcher favorites	com.android.launcher/databases/launcher.db (favorites)
alarms	com.android.deskclock/databases/alarms.db (alarms)
downloads	com.android.providers.downloads/databases/downloads.db (downloads)
INSTALLED APPS	
(Gmail) conversations	com.google.android.gm/databases/mailstore[indirizzo].db (conversations)
(Gmail) messages	com.google.android.gm/databases/mailstore[indirizzo].db (messages)
(Gmail) downloads	com.google.android.gm/databases/mailstore[indirizzo].db (downloads)
(Gmail) raw contacts	com.android.providers.contacts/databases/contacts.db (raw_contacts)
(WhatsApp) raw contacts	com.android.providers.contacts/databases/contacts.db (raw_contacts)
(WhatsApp) messages	com.whatsapp/databases/msgstore.db (messages)
(WhatsApp) chat list	com.whatsapp/databases/msgstore.db (chat_list)
(WhatsApp) contacts	com.whatsapp/databases/wa (wa_contacts)
(Facebook) search results	com.facebook.katana/databases/fb.db (search_results)
(Facebook) photos	com.facebook.katana/databases/fb.db (photos)
(Facebook) albums	com.facebook.katana/databases/fb.db (albums)
(Facebook) notifications	com.facebook.katana/databases/fb.db (notifications)
(Facebook) user statuses	com.facebook.katana/databases/fb.db (user_statuses)
(Facebook) mail threads	com.facebook.katana/databases/fb.db (mailbox_threads)
(Facebook) mail messages	com.facebook.katana/databases/fb.db (mailbox_messages)
(Facebook) mail profiles	com.facebook.katana/databases/fb.db (mailbox_profiles)
(Facebook) friends	com.facebook.katana/databases/fb.db (friends)
(Facebook) info contacts	com.facebook.katana/databases/fb.db (info_contacts)

7.3.2 Risultati acquisizione device 2 (iOS)

Ad ultimo, vengono presentati in Tabella 7.3 i risultati ottenuti dalle acquisizioni device 2, in termini puramente quantitativi. Sulle righe sono riportate le tipologie di dato, mentre sulle colonne vi sono le modalità di acquisizione, da leggersi mediante la legenda riportata di seguito.

I valori contrassegnati da * rappresentano i risultati che è stato possibile raccogliere tramite l'analisi dei file acquisiti, i cui percorsi sono specificati in Tabella 7.4 (e in cui la voce tra parentesi rappresenta la tabella specifica del database); gli altri valori sono invece stati raccolti mediante la lettura di una vista logica fornita dal software.

Legenda

1. Software DDS con modalità *textual data* - NON ESEGUITA;
2. Software DDS con modalità *all data* - NON ESEGUITA;
3. Software Device Seizure con modalità *logical* - NON ESEGUITA;
4. Software Device Seizure con modalità *physical* - NON ESEGUITA;
5. Software MOBILedit! con l'unica modalità disponibile;
6. Software Oxygen con modalità *advanced mode with logical extraction (selected view)*;
7. Software Oxygen con modalità *advanced mode with logical extraction (complete view)*;
8. Estrazione sperimentale, previo jailbreaking;
9. Analisi dei file di backup di iTunes.

Le modalità elencate erano quelle disponibili per il device in oggetto. Quelle contrassegnate dalla dicitura “non eseguita” sono state impossibili da attuare sul device: sono state avviate ma l'acquisizione si è conclusa con un messaggio di errore. Non avendo restituito alcun risultato, le voci sono presenti in legenda ma non in tabella.

92 7. Risultati ottenuti con metodologie finalizzate all'analisi forense

Tabella 7.3: Quantità dati estratti per modalità di acquisizione (iOS)

	5	6	7	8	9
NATIVE APPS					
contacts	365	365	365	365*	365
(contacts) favorites	-	-	-	135*	135
call history	-	79	79	79*	79
sms history	43	43	43	43*	43
browser bookmarks	-	1*	1*	1*	1
browser history	-	18*	18*	18*	18
user dictionary entry	-	1*	1*	1*	1
recent emails	-	-	-	-	5
INSTALLED APPS					
(Facebook) person search	-	-	-	1995*	-
(Facebook) people	-	-	-	347*	-
(Facebook messenger) threads	-	-	-	22*	-
(Facebook messenger) messages	-	-	-	12*	-
(Facebook messenger) users	-	-	-	60*	-
(WhatsApp) messages	-	658*	658*	658*	658*
(WhatsApp) chat session	-	19*	19*	19*	19*
(WhatsApp) info groups	-	9*	9*	9*	9*
(WhatsApp) group member	-	38*	38*	38*	38*
(WhatsApp) media item	-	6*	6*	6*	6*
(WhatsApp) message word	-	4371*	4371*	4371*	4371*
FILES					
pictures (.jpg)	-	12	12	33	6
pictures (.png)	-	2	2	11	-
audio (.mp3)	-	-	-	1	-
audio (.aac)	-	1	1	4	-
audio (.m4a)	-	-	-	4	-
audio (.wav)	-	-	-	1	-
database (.sqlitedb)	-	10	10	14	-
database (.sqlite3)	-	2	2	-	-
database (.sqlite)	-	10	10	15	-
database (.db)	-	9	9	34	-
.log	-	5	5	7	-
.plist	-	91	91	189	-

Tabella 7.4: Percorsi di estrazione dati (iOS)

	PATH
NATIVE APPS	
contacts	Library/AddressBook/AddressBook.sqlitedb
(contacts) favorites	Documents/Contacts.sqlite (zwafavorite)
call history	Library/CallHistory/call_history.db (call)
sms history	Library/SMS/sms.db
browser bookmarks	Library/Safari/Bookmark.db
browser history	Library/Safari/History.plist
user dictionary entry	Library/Keyboard/UserDictionary.sqlite (zuserdictionaryentry)
recent emails	Library/Mail/Recents.sqlitedb
INSTALLED APPS	
(Facebook) person search	Library/Caches/fbsyncstore.db (person_search)
(Facebook) people	Library/Caches/fbsyncstore.db (people)
(Facebook messenger) threads	Library/Caches/orca2.db (threads)
(Facebook messenger) messages	Library/Caches/orca2.db (messages)
(Facebook messenger) users	Library/Caches/orca2.db (users)
(WhatsApp) messages	Documents/ChatStorage.sqlite (zwamessage)
(WhatsApp) chat session	Documents/ChatStorage.sqlite (zwachatsession)
(WhatsApp) info groups	Documents/ChatStorage.sqlite (zwagroupinfo)
(WhatsApp) group member	Documents/ChatStorage.sqlite (zwagroupmember)
(WhatsApp) media item	Documents/ChatStorage.sqlite (zwamediaitem)
(WhatsApp) message word	Documents/ChatStorage.sqlite (zwamessageword)

Conclusioni

Questo lavoro di tesi è stato intrapreso con l'obiettivo di approfondire le tematiche connesse alla *mobile device forensics*, con particolare riferimento all'analisi di dispositivi di telefonia cellulare. Inoltre, col progetto in essa documentato, si è voluto mettere a confronto le capacità estrattive di metodologie di "hacking" dei device, solitamente impiegate per altri fini, rispetto ai più tradizionali approcci forensi che prevedono l'utilizzo di software specifico.

Tale studio ha avuto esiti interessanti sotto molti punti di vista. Innanzitutto sono state assolutamente confermate le potenzialità delle metodologie volte ad ottenere il pieno controllo di tutte le funzionalità dei dispositivi: in entrambi gli ambienti testati si è potuto osservare come la rimozione delle limitazioni indirizzate all'utente medio permetta di analizzare più approfonditamente ogni contenuto del device. Queste tecniche infatti risultano essere attualmente l'unico modo per avere pieno accesso ad ogni directory del sistema operativo, quindi l'unico mezzo tramite cui acquisire tutte le informazioni registrate dall'interazione dell'utente con quel determinato strumento. Confrontando il numero di dati acquisiti dopo l'attuazione di tali procedure di sblocco rispetto a quelli derivanti dall'analisi di un ambiente "vincolato", si può osservare molto bene come la panoramica fornita all'operatore forense possa essere superficiale. Infatti, come si evince dai risultati presentati in Tabella 7.1 e Tabella 7.3, anche i tool specificamente ideati per acquisire le tipologie di dato che sono state oggetto della ricerca, risultano essere soggetti alle limitazioni imposte dal produttore di dispositivi di telefonia mobile. Senza attuare meccanismi di *rooting* o *jailbreaking* (in riferimento ai casi specifici studiati) la vista fornita dai tool forensi di acquisizione risulta essere superficiale, adatta sì alla raccolta delle classiche informazioni d'uso dei device (come ad esem-

pio il registro chiamate e i messaggi inoltrati e ricevuti) ma incapace di aggiungere ulteriori livelli di approfondimento.

Utilizzare le tecniche che sono state oggetto del Capitolo 6 non solo consente di mettere in atto un vero e proprio ulteriore filone di indagine sul device, ma anche di estendere le capacità operative dei tool propriamente forensi, peculiarità ovviamente nota alle case di produzione dei tool⁸. Le migliorate capacità estrattive di un software forense dopo la *privilege escalation* derivante dal rooting sono state ampiamente dimostrate in ambiente Android: si vedano ad esempio in Tabella 7.1 le nette differenze tra le prime cinque modalità di acquisizione (le quattro modalità dei software **Paraben** e l'unica disponibile di **MOBILedit!**, tutte attuate pre-rooting) rispetto alle numero 8 e 9 (le due modalità di **Oxygen** attuate post-rooting). Le ultime due hanno infatti avuto una performance pari soltanto a quella della numero 10 (metodologia sperimentale). Facendo tali considerazioni non si vuole in alcun modo mettere in dubbio la valenza dei tool utilizzati, come dimostrano i risultati essi infatti agiscono in maniera abbastanza simile [ancora una volta si faccia riferimento alle modalità di cui alle colonne dalla 1 alla 5] ma sono potenziati dall'accesso con diritti di amministratore sul sistema [colonne 8 e 9].

Per quanto riguarda l'ambiente iOS possiamo trarre conclusioni diverse. Innanzitutto è stato possibile provare la difficoltà di trovare software compatibili con quel dato dispositivo e sistema operativo. Infatti nonostante le installazioni dei tool fossero complete dei driver e dei software aggiuntivi (**iTunes** e **Quicktime** ad esempio, richiesti dopo l'avvenuto riconoscimento del device) non è stato in alcun modo possibile eseguire la maggior parte delle acquisizioni tramite tool forensi. Nonostante l'insuccesso delle prime quattro modalità estrattive (quelle dei software di **Paraben**), è stato possibile portare a termine le acquisizioni con **MOBILedit!** e con **Oxygen**: se tramite l'utilizzo del primo [Tabella 7.3, colonna 5] si denota una certa superficialità, lo stesso non può essere detto delle modalità seguenti [colonne 6 e 7] che risultano essere quasi allo stesso livello dell'acquisizione previo *jailbreaking* [colonna 8]. Possiamo quindi affermare che lo sblocco dei dispositivi

⁸A tal proposito si può ad esempio menzionare il fatto che durante l'utilizzo di uno dei software forensi oggetto dello studio, **Paraben's Device Seizure**, tra le indicazioni per la scelta di una determinata modalità d'uso si richiedesse esplicitamente il possesso dei pieni diritti di root.

iOS non è equiparabile, come risultati, allo sblocco dei device Android, ma si rivela indispensabile per poter installare applicazioni di terze parti utili ad un'analisi più approfondita.

È stato poi dimostrato, su entrambi i sistemi, che le acquisizioni che rendono disponibili all'operatore i file di database estratti (quelli da cui sono state attinte le informazioni mostrate) si rivelano maggiormente esaustive. Di fatto l'eterogeneità delle informazioni raccolte [Tabella 7.3] in modalità 6, 7 e 9 (rispettivamente Oxygen e analisi dei backup di iTunes) rispetto alla 8 (sperimentale) dipende solamente dalla presenza o meno di alcuni determinati file di database tra i risultati, ossia dalla capacità di raggiungere e riconoscere tali informazioni.

L'analisi post-sblocco dei dispositivi può certamente essere attuata con metodologie più sofisticate di quelle illustrate in questo progetto. Possono essere acquisite copie bit-a-bit delle memorie dei device, può essere calcolato l'hash prima e dopo per verificare la correttezza dell'acquisizione; possono infine essere utilizzati software di carving per raccogliere le informazioni cancellate ma non ancora sovrascritte. Le potenzialità sono infinite, e i risultati ottenibili sperimentando dipendono quasi unicamente dall'estro e dalle intuizioni degli operatori coinvolti. Nello scenario descritto la *privilege escalation* tramite tecniche di *hacking* parrebbe meritare il diritto di essere il primo step da intraprendere per attuare un'acquisizione. In realtà è una tecnica estremamente promettente, ma altrettanto rischiosa e invasiva: il suo uso deve essere attentamente ponderato.

Occorre premettere che lo studio è stato intrapreso partendo da conoscenze tecniche abbastanza limitate sull'argomento, via via migliorate in corso d'opera; durante il suo svolgimento sono state incontrate e affrontate diverse difficoltà operative che probabilmente un operatore con maggiore esperienza avrebbe potuto gestire in modo migliore. Si intende anche far presente che questo lavoro non ha potuto prendere in esame gli strumenti hardware e software della Cellebrite, sicuramente tra i più evoluti a livello sia tecnico che di usabilità, e di conseguenza anche tra i più costosi, nel campo delle indagini forensi su dispositivi di telefonia mobile. Ciò non toglie che, prese in esame le opportune cautele prescritte dal codice di procedura penale in tema di attività irripetibili ed ottenute le dovute autorizzazioni, tecniche più invasive che richiedono conoscenze tecniche approfondite, da utilizzare

nel campo della *mobile device forensics*, consentano di ottenere un risultato senza dubbio di livello superiore.

Bibliografia

Bibliografia

- [Vac12] Giuseppe Vaciago. *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*. Giappichelli Editore, 2012.
- [Ate11] Stefano Aterno. *Computer forensics e indagini digitali. Manuale tecnico-giuridico e casi pratici*. Experta, 2011.
- [O'C04] Thomas R. O'Connor. «Admissibility of Scientific Evidence Under Daubert». In: *North Carolina Wesleyan College* (2004).
- [DCN07] Luisella De Cataldo Neuburger. *La prova scientifica nel processo penale*. Cedam, 2007, pp. 71–72.
- [Ton12] Paolo Tonini. *Manuale di procedura penale*. Giuffrè Editore, 2012.
- [EUR01] COUNCIL OF EUROPE. *Convention on cybercrime, Budapest, 23*. 2001. URL: <http://tinyurl.com/owd7tpq>.
- [Cin11] Mariagrazia Cinti. «Quantificazione ed individuazione delle alterazioni dei dati nell'ambito di indagini di Informatica Forense». Tesi triennale in Informatica per il Management. Università di Bologna, 2011.
- [ABJ13] Rick Ayers, Sam Brothers e Wayne Jansen. *Guidelines on Mobile Device Forensics*. Ver. Special Publication 800-101 Revision 1 (Draft). National Institute of Standards e Technology. 2013.

- [D'A06] Luca D'Antonio. *Una panoramica su GSM, GPRS, EDGE e UMTS*. Seminario. UniRoma1, 2006. URL: <http://tinyurl.com/pjpltqb>.
- [Swa12] Jim Swauger. «Chip-off forensics, extracting a full bit-stream image from device containing embedded flash memory». In: *Digital Forensics Magazine* (2012).
- [FRtt] Stefano Fratepietro e Sandro Rossetti. «Android Forensics - Analisi di un dispositivo Android utilizzando strumenti freeware ed open source». In: (settembre 2011).
- [Zdz12] Jonathan Zdziarski. *Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It*. O'Reilly Media, 2012.
- [Sco95] John Scourias. «Overview of the global system for mobile communications». In: *University of Waterloo* (1995).
- [ZB10] Amjad Zareen e Shamim Baig. «Mobile Phone Forensics: Challenges, Analysis and Tools Classification». In: *Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on*. IEEE. 2010, pp. 47–55.
- [Hoo11] Andrew Hoog. *Android forensics: investigation, analysis and mobile security for Google Android*. Elsevier, 2011.

Sitografia

- [ERti] Arpa Emilia-Romagna. *Impianti per la telefonia mobile (Stazioni radio base)*. Ultima visita: dicembre 2013. URL: <http://tinyurl.com/ok8vjmx>.
- [Fer] *Fernico.com*. Ultima visita: febbraio 2013. URL: <http://www.fernico.com/>.

- [Stiti] Stilgherrian. *Apps? No root? Your device serves others: Berners-Lee*. A cura di ZDNet.com. Ultima visita: febbraio 2014. URL: <http://tinyurl.com/a8ev8t7>.
- [Relti] Press Release. *Gartner Says Smartphone Sales Grew 46.5 Percent in Second Quarter of 2013 and Exceeded Feature Phone Sales for First Time*. A cura di Gartner.com. Ultima visita: febbraio 2014. URL: <http://tinyurl.com/oug6tbk>.
- [Guiti] Guidaiphone.com. *Differenza tra Jailbreak Tethered e Untethered*. Ultima visita: febbraio 2013. URL: <http://tinyurl.com/p8wzcwt>.
- [Chuti] Ji Chuan. *How Rooting Works - A Technical Explanation of the Android Rooting Process*. A cura di Seasonofcode.com. Ultima visita: febbraio 2013. URL: <http://tinyurl.com/njz5ot6>.
- [Bti] Satish B. *Forensic analysis of iPhone backups*. Ultima visita: marzo 2013. URL: <http://tinyurl.com/k85vzgg>.
- [Broti] Sam Brothers. *iPhone Tool Classification*. A cura di The Apple Examiner. Ultima visita: febbraio 2014. URL: <http://tinyurl.com/ovjr2bq>.
- [Incti] Apple Inc. *iTunes: informazioni sui backup di iOS*. Ultima visita: febbraio 2013. URL: <http://tinyurl.com/nmzrt23>.

Ringraziamenti

Ringrazio anzitutto il mio relatore, professor Luciano Bononi, per l'infinita disponibilità avuta nei miei riguardi. Ringrazio il mio primo correlatore, professor Cesare Maioli, per avermi trasmesso, con i suoi insegnamenti, la passione per le tematiche della *computer forensics*. Ringrazio il mio secondo correlatore, il dottor Michele Ferrazzano, per le numerose ore dedicate alla mia tesi; ringrazio il dottor Donato Eugenio Caccavella per i preziosi spunti, ed infine ringrazio nuovamente entrambi per aver messo a mia disposizione la loro esperienza nonché le strumentazioni del loro studio di informatica forense.

Vorrei infine ringraziare, per il loro costante supporto, le persone a me più care: la mia famiglia, i miei amici e colleghi, ed infine Riccardo, per essere semplicemente il mio "tutto".