Claudio Ballicu

Intercettazioni telefoniche e analisi dei "tabulati"

nell'attività peritale del Consulente Tecnico di Parte

Elaborazione grafica: *Simon Mago*

Intercettazioni telefoniche e analisi dei “tabulati”

nell’attività peritale del Consulente Tecnico di Parte

Progetto grafico, copertina, ricerche iconografiche, disegni e foto di Claudio Ballicu

Finito di stampare nell'ottobre2016

Indice

		Pag.
	Profilo biografico dell'autore	
	Prefazione	1
	Introduzione	2
1.	Quanto è privata la nostra *privacy*	5
2.	La conservazione dei dati o "Data Retention"	6
3.	Gli Enti coinvolti nell'intercettazione legale	9
4.	I "tabulati" richiesti dall'Autorità Giudiziaria	11
4.1	Ottenere i "tabulati" della propria linea telefonica	14
5.	Come funziona la telefonia cellulare	16
5.1	Il codice IMEI	19
5.2	Il codice IMSI	20
5.3	Il PIN e il PUK	21
5.4	Il codice MSISDN	22
6.	L'architettura della rete cellulare	24
6.1	Le reti di seconda generazione: il GPRS	29
6.2	Le reti di seconda generazione: l'EDGE	30
6.3	Le reti di terza generazione: l'UMTS	31
6.4	L'HSDPA	31
6.5	Le reti di quarta generazione: LTE	32
7.	La portata delle celle telefoniche	33

8. Il “Timing Advance” 35
9. La triangolazione 39
9.1 L’angulation 40
9.2 La lateration 42
9.3 Altri metodi di misura 44
10. A cosa serve l’acquisizione dei tabulati telefonici 47
10.1 L’interpretazione dei “tabulati telefonici” 49
11. I software per l’analisi dei “tabulati” 53
11.1 Phone Log 53
11.2 Sfera 54
11.3 Ultra 54
11.4 Tetras 55
12. Le “App” Android per l’individuazione delle celle 56
12.1 Info Segnale Rete Pro 56
12.2 G-net track Pro 57
12.3 Antennas 57
12.4 Cell Mapper 58
12.5 Antenna Pointer 58
12.6 Open Signal 58
13. Interpretare i dati presenti nei “tabulati telefonici” 59
13.1 La gestione della mobilità o “cell selection” 66
13.2 L’handover 66
13.3 Il Soft handover 70
13.4 L’indicazione LAI-CI 71
13.5 I siti “tricellulari” 78

13.6 Un semplice esperimento 82
14. La “Cell Site Analysis” 85
15. L’analisi della memoria del terminale 87
16. La digital forensics e i “forensic tools” 91
17. La catena di custodia 95
18. L’evoluzione tecnologica delle comunicazioni telefoniche e informatiche e i problemi delle intercettazioni 97
18.1 “Skype” e i servizi “VOIP” nelle intercettazioni 98
18.2 Le comunicazioni telefoniche satellitari nelle intercettazioni 101
18.3 Gli “Anonymous remailer” nelle indagini informatiche 103
19. Il GSM box nelle intercettazioni 105
20. Il GSM-R 107
21. Il sistema di posizionamento satellitare GPS 109
21.1 Il pedinamento elettronico mediante GPS 110
21.2 L’inquadramento giuridico del pedinamento GPS 114
21.3 I limiti tecnici dei tracker GPS 116
21.4 I limiti tecnici della comunicazione GSM nei trackers 119
21.5 Le contromisure anti-pedinamento/anti-intercettazione 121
21.6 Le schede SIM anonime e l’“IMSI Catcher” 123
22. La “chip-off” forensics nell’analisi di dispositivi senza interfacce o distrutti 127
22.1 L’acquisizione dei dati attraverso le porte JTAG 129

22.2 L’acquisizione dei dati da un hard-disk danneggiato 130
23 L’attività peritale del Consulente di Parte e le indagini difensive 132
- Indice analitico 135
- Bibliografia, sitografia, convegni 140

Profilo biografico dell'autore

Claudio Ballicu è nato a Roma nel 1949, dove vive e lavora. È perito in elettronica industriale e telecomunicazioni e laureato in Scienze dell'Investigazione all'Università di L'Aquila.

Autore di pubblicazioni nel campo della meccanica serraturiera e delle casseforti, del misterioso settore dello spionaggio elettronico e dell'indagine sulle cause di incendio, sulla rivista del settore "Force-Security", ha tenuto seminari sul tema della ricerca di tracce forensi nelle serrature sottoposte ad apertura clandestina nelle università di Aquila e Camerino e sulle tecniche di bonifica da microspie, presso la Facoltà di Giurisprudenza e presso la Facoltà di Informatica dell'Università di Camerino.

Effettua perizie forensi e consulenze nel campo serraturiero-casseforti e dei dispositivi elettronici anticrimine per il Tribunale di Roma, ove è iscritto dal 2005 nelle liste dei Consulenti Tecnici del Giudice, e per privati e compagnie assicurative.

Si occupa, inoltre, di tecnologie di ricerca e bonifica da microspie ambientali e/o telefoniche e localizzatori satellitari GPS e di tutto quanto concerne la sicurezza della vita privata.

È autore e curatore del sito internet www.perizieforensi.com, ricco di notizie sul mondo delle microspie, della sicurezza anticrimine e della protezione da intrusioni negli archivi dei dati digitali aziendali.

Collabora, su tutto il territorio nazionale, con importanti Studi Legali effettuando consulenze tecniche e indagini difensive (art.11, legge 7 dicembre 2000, n. 397).

Il presente lavoro si pone l'obiettivo di analizzare e riorganizzare le informazioni tecniche riguardanti le intercettazioni telefoniche sulle reti cellulari, richieste dall'Autorità Giudiziaria.

Queste informazioni, di natura decisamente specialistica, sono già reperibili da chiunque, anche se con qualche difficoltà, nel web. Tuttavia sono presenti in modo lacunoso e disarticolato, rendendole di fatto difficilmente comprensibili ai non addetti al settore.

Ulteriore finalità di queste pagine è descrivere nel dettaglio gli aspetti concernenti l'attività di analisi dei cosiddetti "tabulati telefonici", soprattutto dal punto di vista del Legale della Difesa e del Consulente Tecnico di Parte.

Lo studio dei tabulati evidenzia, non di rado, discrepanze anche macroscopiche relativamente alla posizione geografica dell'utenza nel segmento temporale della chiamata effettuata o ricevuta, dovute a peculiarità tecniche e funzionali scarsamente conosciute sull'organizzazione progettuale dei ponti radio cellulari, nonché a più generali fenomeni legati alla radiopropagazione.

Le contestazioni che ne derivano offrono valide argomentazioni al collegio difensivo, nell'oralità del contraddittorio, evidenziando le diverse legittime interpretazioni.

La capillare diffusione dei telefoni cellulari e le numerose possibilità di utilizzo degli stessi, che travalicano la semplice comunicazione vocale, integrando anche lo scambio di dati (SMS, navigazione internet e altro), hanno portato le indagini giudiziarie a fare largo uso tanto dei terminali stessi quanto delle tracce che questi lasciano nelle reti degli operatori telefonici.

Infatti, è oramai fortemente radicato l'uso, da parte degli organi inquirenti, dei CDR (*Call Detail Records*) ossia la registrazione dei dettagli delle chiamate, comunemente conosciuti come "tabulati", forniti, a richiesta, dai gestori di telefonia, per stabilire a posteriori la posizione geografica di un determinato utente in un preciso ritaglio temporale, nonché i suoi spostamenti e lo "stato" del suo terminale mobile (telefonino), se spento o acceso e collegato alla rete telefonica cellulare.

Ciò che mi preme sottolineare è che l'architettura di tale sistema di telecomunicazione mobile è ingegnerizzata al fine dell'individuazione approssimativa della posizione di ogni singolo terminale, allo scopo di metterlo in comunicazione con la cella che risulta avere, in un preciso istante, il segnale radio più forte. Questa "cella" è tecnicamente definita "miglior servente".

Attenzione! Non sto parlando della SRB (*Stazione Radio Base*, detta anche, nell'acronimo anglosassone, BTS, *Base Transceiver Station*) geograficamente più vicina.

Infatti, per le peculiari caratteristiche di propagazione delle onde radio nelle gamme di frequenza usate dalla telefonia mobile, che ricadono nella banda delle microonde, il segnale radio più forte non necessariamente coincide con la trasmittente geograficamente più prossima. Questo fenomeno è particolarmente rilevante negli ambienti urbani.

In realtà, uno o più ostacoli, quali possono essere edifici, formazioni orografiche collinari e/o montuose e, più in generale, qualunque struttura schermante la radiofrequenza, possono

rendere momentaneamente “miglior servente” anche una cella posta a distanze rilevanti, a discapito di un’altra posta, magari, a poche centinaia di metri.

A complicare un quadro già di per sé complesso, dobbiamo tener conto delle riflessioni, diffrazioni, attenuazioni, cui è soggetto il segnale radio in questa gamma di frequenze, il che rende quasi impossibile determinarne a priori il reale comportamento, anche tenendo conto delle innumerevoli variabili in gioco.

Quanto sopra, per affermare, in scienza e coscienza, come l’architettura di funzionamento delle SRB, implementata per scopi e con funzioni diverse da quelle cui, a volte, vorrebbero piegarla gli organi inquirenti, mal si presti all’uso forense della ricerca di “elementi di prova”.

Le troppe e imprevedibili variabili, insite in questo genere di approccio, possono generare risultati impropri, lacunosi e fuorvianti, potenzialmente capaci di distorcere la ricerca della verità influendo negativamente sulla formazione della prova stessa e sulla costruzione del libero convincimento del Giudice.

Lo studio della posizione geografica di un telefono cellulare mediante l’analisi delle SRB e delle celle si fonda, in realtà, su una valutazione di tipo probabilistico e non deterministico, per cui è fondamentale comprendere quali siano i fattori da tenere in considerazione per stimare l’affidabilità dei risultati sul piano tecnico, ancor prima che su quello giuridico.

Tuttavia, non ho la presunzione di contestare *in toto* la pratica dell’esame forense dei cosiddetti “tabulati telefonici” anzi, riconosco che spesso hanno portato alla soluzione di complessi casi giudiziari.

Semplicemente ritengo fondamentale evidenziare come, sotto il profilo criminologico-investigativo, si debba tener conto, a tutela degli inviolabili diritti della difesa, garantiti fra l’altro dall’art.111 Cost. delle summenzionate numerose ed inevitabili

variabili, tolleranze e persino aggiornamenti tecnici dei ponti telefonici, insite in un sistema progettato per scopi peculiari e, non da ultimo, delle diverse interpretazioni che le parti, legittimamente, offriranno nel successivo dibattimento.

Ovviamente, quanto sopra si riferisce esclusivamente all'analisi dei "tabulati telefonici". Cosa ben diversa è l'intercettazione delle conversazioni, effettuata in "tempo reale", la cui validità sul piano probatorio si pone su un diverso livello, sempre che siano state osservate le disposizioni previste dagli artt. 266, 267 e 268 commi 1 e 3 c.p.p.

Quanto è privata la nostra *privacy*

La principale fonte di tutela dei dati personali è il Codice della Privacy, ossia il Decreto Legislativo 196/03, che ha, fra l'altro, l'obiettivo di garantire i diritti che ogni persona ha sui dati che la riguardano, stabilendo alcuni limiti al loro trattamento, (art.1 di tale Codice).

Periodicamente il Garante rilascia delle indicazioni di carattere generale in relazione al trattamento dei dati personali nei vari ambiti, garantendo in tal modo la corretta applicazione dei principi stabiliti dal Codice.

Alcune delle deliberazioni che sono state emesse e che hanno particolare attinenza con il tema di questo libro sono la 46/20084 (*trattamento dei dati ad opera dei consulenti tecnici*) e la 60/2008 (*trattamento dei dati durante lo svolgimento di investigazioni*).

Tuttavia, vi sono persone si dicono favorevoli alle misure di sorveglianza generalizzata sostenendo che: "*m'intercettino pure, se non sto facendo niente di male, non ho nulla da nascondere*", rispondendo in tal modo a chi sostiene l'inviolabilità del diritto alla privacy. A costoro basterebbe ricordare l'art. 15 della Costituzione Italiana, gli artt. 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea e l'art. 12 della Dichiarazione Universale dei Diritti dell'Uomo.

Inoltre, basti pensare alle intercettazioni abusive telematiche e/o informatiche, capaci di fornire a criminali molto ben organizzati, dati sensibili sulle nostre carte di credito o sui codici delle nostre transazioni bancarie effettuate al computer o alle intercettazioni connesse con lo spionaggio industriale, capaci di vanificare in un attimo anni di ricerche e investimenti per arrivare a un brevetto o di insinuarsi, fraudolentemente, nelle offerte di gare d'appalto, per comprendere la necessità, degli appositi articoli del Codice Penale che perseguono gli autori di simili reati.

La conservazione dei dati o "Data Retention"

Fino all'entrata in vigore del "Codice della Privacy" (01/01/2004) l'ordinamento italiano non prevedeva alcun obbligo di conservazione dei dati di traffico, da parte dei gestori dei servizi telefonici e telematici, né un limite massimo temporale. La questione era demandata alla discrezionalità dei singoli operatori che la interpretavano ai soli fini commerciali e di fatturazione.

Successivamente, il Codice in materia di protezione dei dati personali, all'art. 123, stabilì un divieto generale di conservazione di dati relativi al traffico telefonico e telematico, con due eccezioni; Il trattamento di tali dati fu consentito per esigenze di fatturazione dell'abbonato o di commercializzazione consensuale di servizi, mentre la "conservazione" dei dati fu resa obbligatoria per finalità di accertamento e repressione dei reati (art. 132 del Codice).

La disciplina attuale in materia di conservazione dei dati di traffico delle comunicazioni telefoniche e telematiche, necessaria per il buon esito delle indagini, è un obbligo a cui sono tenuti i fornitori di tali servizi ed è la (sofferta) ricerca di equilibrio fra due opposti interessi; quello pubblico alla prevenzione e repressione dei reati e quello individuale alla tutela della riservatezza della sfera personale.

Dopo vari decreti, leggi e provvedimenti del garante, succedutisi negli anni, che hanno causato non poche perplessità in ambito forense, dove molti ritengono che non risolvano, ma anzi complichino alcuni aspetti relativi alla "*data retention"*, sono state inserite misure di conservazione dei dati di traffico telematico, oltre alle preesistenti norme relative a quello telefonico (art. 132 *Codice in materia di protezione dei dati personali*), con esclusione del contenuto delle comunicazioni, in ossequio anche ai principi di pertinenza e non eccedenza stabiliti dagli artt. 3 e 11 del Codice.

Infatti, non vengono registrate le conversazioni, né il contenuto dei messaggi SMS/MMS e non è neppure previsto nulla in merito dalle direttive europee e/o italiane, oltre che dal codice della privacy (D.L. 30/05/2008 n 109, per l'attuazione della direttiva 2006/24/CE e D. Lgs. 196/2003).

Il contenuto della comunicazione stessa quindi, non può essere intercettato né conservato senza una specifica disposizione dell'Autorità giudiziaria.

Pertanto non è possibile, *ex post*, risalire al contenuto di una qualsiasi comunicazione telefonica. La conservazione è limitata alle sole informazioni che consentono la tracciabilità degli accessi ossia: il numero telefonico del chiamante, del chiamato, la data, l'ora, la durata della conversazione, la cella utilizzata, l'IMEI, l'IMSI.

Il termine di conservazione, per i dati di traffico telematico, è stabilito in 12 mesi, prolungabile di altri 12 mesi nei casi dei delitti più gravi, mentre per i dati relativi al traffico telefonico i termini sono di 24 mesi (per le chiamate senza risposta il termine è di trenta giorni), prolungabili di altri 24 mesi per i delitti di cui all'articolo 407, comma 2, lett. a del Codice di Procedura Penale, nonché per i delitti in danno di sistemi informatici o telematici.

Tutto questo a smentire la cosiddetta "sindrome del Grande Fratello", secondo cui alcuni provano la sgradevole sensazione che i nostri dati telefonici, o addirittura le conversazioni, siano oggetto, di continuo, delle attenzioni degli operatori e dell'Autorità.

È vero piuttosto il contrario, stante il limitato tempo di permanenza dei "cartellini di traffico storico", normato dal già citato D.L. 30/05/2008, oltre alle cogenti disposizioni del Codice di Procedura Penale. Eppure, potrebbe dire qualcuno, la cronaca nera, le riviste di gossip o le trasmissioni televisive a tema criminalistico, ci deliziano con i testi degli SMS scambiati fra gli indagati o con le trascrizioni delle loro più private conversazioni.

Come si spiega tutto ciò?

Semplicemente, l'utenza di interesse era stata posta sotto intercettazione fin dall'inizio delle indagini, quando il soggetto non sospettava queste attività nei suoi confronti e ciò ha permesso la registrazione dei dialoghi e l'acquisizione dei testi dei "messaggini". Che poi questi dati siano sottoposti al segreto istruttorio o investigativo[1], come atti d'indagine compiuti dal P.M. o dalla P.G. (art. 329 c.p.p.) e non debbano essere portati a conoscenza pubblica… è un'altra storia.

In alternativa (ma solo riguardo agli SMS e/o alle eventuali foto e altri dati digitali) c'è il sequestro del telefonino che li ha inviati/ricevuti e l'estrazione dei testi memorizzati, fatta salva la creazione di una copia digitale di valore forense[2] e la regolarità della "catena di custodia[3]". A certe condizioni è anche possibile tentare il recupero dei messaggi eventualmente cancellati dal proprietario a mezzo di appositi software

1) Il segreto istruttorio proibisce la diffusione di informazioni per tutta la durata dell'istruttoria, ovvero sino al termine delle indagini. Il segreto investigativo, invece, perdura fin quando il P.M. ritiene che vi sia interesse dell'indagine a nascondere all'indagato la procedura nei suoi confronti.
Il segreto investigativo decade, ovviamente, quando il P.M. notifica l'accusa attraverso un avviso di garanzia, un'ordinanza di sequestro ecc.

2) La copia di valore forense, deve essere effettuata, alla presenza dell'indagato e/o del suo difensore e/o del consulente Tecnico di Parte, tramite l'utilizzo di speciali dispositivi hardware o software che impediscano qualunque modifica nei supporti originali durante la copia (*write blocker*), eseguendo una copia "*bit per bit*" degli hard-disk o altri supporti di memorizzazione, seguiti dal calcolo dell'"*hash*" dell'intero contenuto di ogni supporto acquisito, in modo da garantire l'assoluta conformità all'originale e quindi la non ripudiabilità dei dati acquisiti, sui quali svolgere gli accertamenti necessari.

3) La catena di custodia è il documento che contiene le informazioni su ciò che è stato fatto con la prova originale e con le copie forensi a partire dall'acquisizione, dalla conservazione e fino al momento del processo, garantendo in tal modo la genuinità della prova. Si vedano a questo proposito, anche i disposti degli artt. 191, 244 comma 2, 247 comma 1-bis, 254-bis, 352 comma 1-bis, 354 comma 2, del c.p.p.

(…)

I “tabulati” telefonici richiesti dall’Autorità Giudiziaria

A differenza delle intercettazioni telefoniche vere e proprie, l’acquisizione e l'analisi dei tabulati telefonici è sottoposta a una normativa diversa, e meno restrittiva.

In proposito, esistono diversi orientamenti giurisprudenziali, a chi ritiene essere questa un’attività di indagine fortemente invasiva della sfera privata, si contrappone chi giudica i tabulati, “*dati esterni identificativi delle comunicazioni”,* ossia uno strumento di riconoscimento dell’utenza, anche se comprende contatti telefonici tra soggetti.

Non sarebbe necessaria l’autorizzazione del Giudice per le Indagini Preliminari (GIP) per ottenere questo documento, ma sarebbe sufficiente un decreto formale del Pubblico Ministero[8] come ribadito dalle Sezioni Semplici della Corte di Cassazione, che si sono pronunciate sull’acquisizione di tabulati contenenti l’indicazione di comunicazioni telefoniche intervenute tra soggetti, che non necessiterebbero del decreto del Giudice per le indagini preliminari (ex art. 267 c.p.p.), essendo sufficiente il decreto motivato del pubblico ministero[9].

Infatti, l'analisi dei tabulati, mostra semplicemente una tabella di dati (spesso, ma non sempre, in formato Excel) che elenca tutto il traffico in entrata e in uscita dal telefono dell'indagato, con indicati data e orario di inizio chiamata, la sua durata, il numero di telefono dell’interlocutore, l’identificativo delle celle agganciate, (LAI-CI, c.f.r. cap.13) l’identificativo del telefono e della SIM del chiamante e del chiamato (IMEI – IMSI, c.f.r. capp. 5.1 e 5.2) ecc.

Facile intuire come questi dati possano risultare altrettanto decisivi rispetto alle intercettazioni vere e proprie poiché individuano l'indagato in una certa posizione geografica, pur con le inevitabili e rilevanti tolleranze, e in un certo segmento

temporale, oltre a palesare frequenza e intensità di eventuali rapporti con un sodalizio criminoso.

Il d.d.l. 1415, nel recepire integralmente l'orientamento della Corte di Legittimità, tende a ricomprendere in questo statuto processuale anche l'acquisizione dei tabulati delle utenze telefoniche.

Ciononostante, il requisito della motivazione, in relazione ai tabulati, è a volte sottovalutato nel decreto del P. M. ricorrendo a espressioni stereotipate quali "*gravi indizi di reato, necessari alla prosecuzione delle indagini*", ecc. non dando in tal modo il giusto rilievo alle ragioni che fanno prevalere l'interesse pubblico di perseguire i reati sul diritto alla privacy.

Va infine ricordato l'art. 132 comma 3 cod. privacy, che consente al difensore dell'imputato o della persona sottoposta alle indagini o alle altre parti private di chiedere direttamente i dati al fornitore, con le modalità indicate nell'art. 391-quater c.p.p.

Il pubblico ministero, in tal caso, non sarebbe più l'unica figura preposta all'acquisizione dei tabulati.

L'art. 8, comma 2, lett. f del Codice della privacy, che norma i diritti di ogni persona ad accedere alle informazioni che la riguardano, quando queste siano detenute da terzi "*non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397*".

Altrove si sostiene invece che l'esecuzione del provvedimento autorizzativo all'acquisizione dei dati spetterebbe al Giudice, anche avvalendosi della sezione di P.G. presso la Procura della Repubblica.

Tuttavia, un'esecuzione da parte del Giudice comporterebbe

il conferimento automatico nel fascicolo per il dibattimento, anche contro la volontà e l'interesse della difesa che, al contrario, deve essere lasciata in condizione di valutare se versare o meno nel processo i dati richiesti[10].

8) Cass. n. 8458/2000; "*Ai fini dell'acquisizione dei tabulati contenenti i dati esterni identificativi delle comunicazioni telefoniche (...) è sufficiente il decreto motivato dell'autorità giudiziaria, non essendo necessaria, per il diverso livello di intrusione nella sfera di riservatezza che ne deriva, l'osservanza delle disposizioni relative alla intercettazione di conversazioni o comunicazioni di cui all'art. 266 ss. c.p.p.*"
Inoltre; Cass. Sez. Un. n. 16/2000; "*Per l'acquisizione dei dati esterni relativi al traffico telefonico concernenti gli autori, il tempo, il luogo, il volume e la durata della comunicazione, fatta esclusione del contenuto di questa (...) è sufficiente, in considerazione della limitata invasività dell'atto, (...) il decreto del pubblico ministero con il quale si dia conto delle ragioni che fanno prevalere sul diritto alla privacy l'interesse pubblico di perseguire i reati. (...)*".

9) (Cass. sez. II, 25/11/2003).

10) (S. Perelli*, Le modalità di acquisizione dei tabulati*, in Diritto e Giustizia, 2004, n. 24, p. 117).

Il codice IMEI

L'IMEI è un codice univoco composto da 15 cifre contenente informazioni fondamentali sul dispositivo cui è associato. Il codice IMEI è così strutturato:

AAAAAA-BB-CCCCCC-D

Le prime 6 cifre sono il TAC (*Type Allocation Code*) e identificano la casa costruttrice e il modello del telefonino;

Le due successive rappresentano il FAC (*Final Assembly Code*) e fino all'aprile 2004 indicavano il luogo di costruzione o di assemblaggio del prodotto. Successivamente a questa data sono state sostituite da 00.

Seguono sei cifre che indicano il numero di serie del cellulare;

L'ultima cifra, detta "*Spare*", è riservata al controllo della correttezza del codice IMEI, calcolato con la formula di Luhn.

(In alcuni codici IMEI potremmo trovare 16 cifre anziché 15. In questo caso, la cifra finale di controllo (*Spare*) è sostituita da due cifre, dette SV (*Software Version*) che indicano la versione del firmware dell'apparecchio).

In caso di furto, è importante citare, nella denuncia alle autorità, il codice IMEI del proprio telefono cellulare e comunicarlo al proprio gestore (Per conoscerlo basta digitare: *#06#). In tal modo potrà essere inserito in una banca-dati, detta "*blacklist*", condivisa fra gli operatori, consentendo di bloccarne l'accesso alla rete telefonica. Tuttavia, operatori di altri paesi potrebbero non applicare la blacklist italiana.

Si può controllare l'IMEI di un telefono attraverso il sito International Numbering Plans, digitandolo nell'apposita finestra e cliccando poi su "analyse":

http://www.numberingplans.com/?page=analysis&sub=imeinr

L'immagine che segue (fig.1), ne è un esempio:

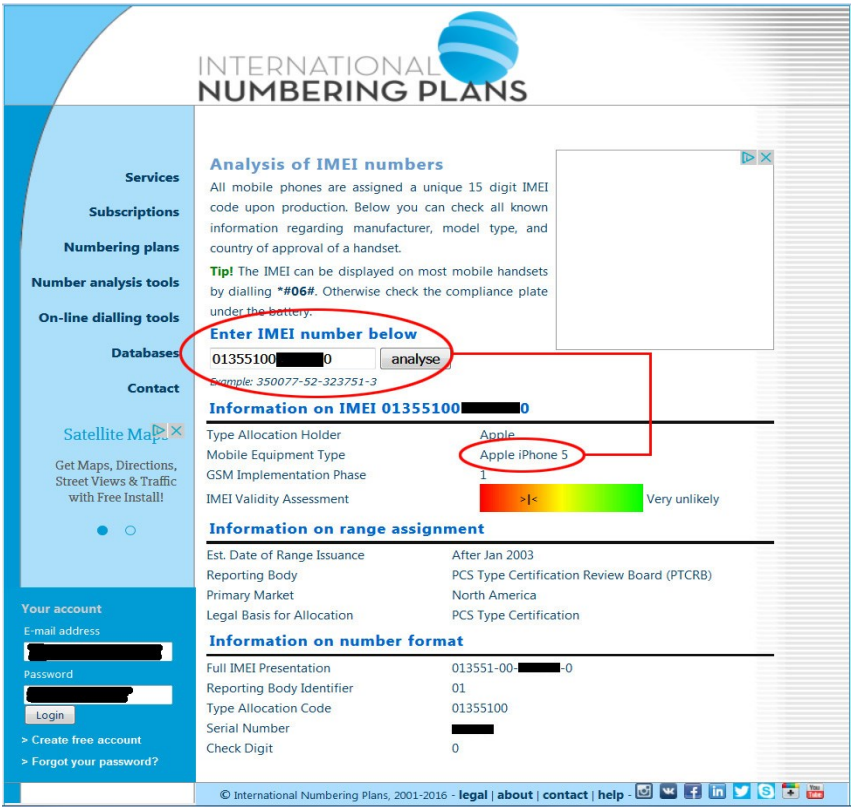

Fig.1

Il codice IMSI

L'IMSI, (International Mobile Subscriber Identity) è un codice seriale univoco che identifica una determinata SIM all'interno della rete di un operatore telefonico ed è composto da 18 cifre così strutturate:

AAA-BB-CCCCCCCCCCCCC

Le prime tre cifre, dette "*Mobile Country Code*" individuano il paese di appartenenza della SIM; le successive 2 cifre, dette MNC "*Mobile Network Code*" indicano l'operatore telefonico; i

numeri restanti servono a identificare univocamente l'utente e sono chiamate "*Mobile Subscriber Identification Number*" (MSIN).

Secondo questa codifica, i primi tre numeri dell'IMSI di un telefonino italiano saranno: 222 seguiti dal codice dell'operatore:

- 01 per Telecom Italia
- 10 per Omnitel
- 88 per Wind
- 99 per Tre
- 30 per GSM-R (rete GSM delle ferrovie italiane).

Nei tabulati telefonici troveremo sempre, insieme ad altre informazioni, anche i codici IMEI e IMSI dell'abbonato. È ovvio che, se ad un certo punto leggeremo, negli appositi campi, un cambiamento di IMSI pur con il medesimo IMEI, starà a significare che l'utente sta usando una diversa SIM nello stesso terminale, forse nell'illusorio tentativo di non essere intercettato.

L'IMEI e l'IMSI sono i codici principali trasmessi dal telefono al momento dell'accensione, per identificarsi nella rete e all'inizio di ogni comunicazione. Ovviamente la cosa non poteva essere così semplice; viene infatti trasmessa anche la "*Chiave d'Autenticazione*", il "*Local-Area Identity"*, il numero del centro servizi per gli SMS, il "*Service Provider Name"* e altra robaccia che, fortunatamente, ai nostri fini, possiamo tralasciare.

Il PIN e il PUK

Coraggio! Qui andiamo sul facile! Questa la sanno tutti!

Prima di poter utilizzare una qualsiasi SIM card, è necessario inserire un codice di sicurezza composto da 4 cifre che sblocca tutte le funzioni della scheda stessa. Stiamo parlando del PIN (*Personal Identity Number*), assegnato dall'operatore telefonico,

che l'utente può successivamente modificare oppure disattivare del tutto. Ad ogni accensione del telefono, dovremo digitare nuovamente il codice per accedere alle funzioni del terminale.

Per sbloccare la scheda SIM tramite questo codice, si hanno a disposizione un massimo di tre tentativi; nel caso di tre inserimenti errati del PIN, sarà necessario ricorrere al codice di sblocco PUK (*Personal Unblocking Key*). Per quest'ultimo codice sono disponibili 10 tentativi, dopodiché la SIM viene disattivata.

Troviamo entrambi i codici stampati sul supporto che contiene la scheda SIM quando ci viene consegnata dal rivenditore, nascosti da una vernice dorata da grattare con una monetina.

Il codice MSISDN

Ciascun utente radiomobile, tanto della rete GSM quanto della UMTS, è identificato dalla numerazione telefonica, univocamente associata al suo contratto, chiamata MSISDN (*Mobile Subscriber ISDN Number*). Si tratta semplicemente del numero che viene digitato per chiamare il suo terminale.

La numerazione, può essere composta da un massimo di 15 o 16 cifre ed è così strutturata:

AAA-BBB-CCCCCCCCCCC

Le prime tre cifre, chiamate "Country Code" identificano il prefisso internazionale della nazione di appartenenza. Ad esempio, per l'Italia è +39.

Seguono le cifre che identificano la rete radiomobile (*National Destination Code*) e le cifre che individuano l'abbonato (Subscriber Number).

Esempio: +39-380-1234567.

Vediamo, sinteticamente, le fasi di una chiamata:

- Il chiamante compone il numero telefonico dell'utente che vuole chiamare;

- La centrale di rete che gestisce il chiamante analizza i primi due campi del MSISDN (+39-380) e instrada il traffico verso la centrale GMSC (vedi capitolo seguente) a cui appartiene il chiamato, interrogando il database HLR (vedi capitolo seguente) che ha in memoria le sue informazioni personali;

- Il chiamante è oramai localizzato e le BSC chiedono alle loro BTS di lanciare un messaggio di "paging" alle celle appartenenti alle aree dove l'utente è geograficamente circoscritto;

- Il telefonino del chiamato risponde al "paging" con una richiesta di accesso alla rete che gli assegna un canale per l'autenticazione, conclusa positivamente la quale gli accorda un canale di traffico.

La connessione è completata e i due possono finalmente parlare… e non si dica che avrebbero fatto prima usando un piccione viaggiatore!

L’architettura della rete cellulare GSM

Eccoci ad un altro capitolo decisamente “difficile” ma nondimeno importante dal punto di vista tecnico.

Sebbene questo capitolo non proponga una descrizione esaustiva, non si tratta infatti di un testo di elettronica e telecomunicazioni, i concetti affrontati costituiscono la base per comprendere ciò che seguirà, quando entreremo nel dettaglio delle tecniche di intercettazione o di localizzazione dell’utenza o dell’analisi dei tabulati telefonici (CDR) usate per l'analisi forense.

La telefonia “cellulare” è una tipologia di accesso alla rete telefonica realizzata per mezzo terminali radio ricetrasmittenti; i telefonini sono appunto tali, in definitiva.

Trattandosi quindi di sistemi basati sulle onde radio e non potendo disporre di potenze elevate, la portata dei telefoni cellulari risulta, giocoforza, limitata.

Per tale ragione si è reso necessario installare, sul territorio, un gran numero di stazioni ripetitrici in grado di rilanciare il segnale radio generato dal telefonino, ad altre stazioni limitrofe, dette BSC (Base Station Controller) e così via, fino alla stazione “capomaglia”.

Insomma, il sistema telefonico mobile, suddivide vaste aree geografiche in settori più piccoli chiamati “celle”, di qui il nome “cellulare” ognuno controllato da una “Stazione Radio Base” (SRB) o *Base Transceiver Station* (BTS) nell’acronimo anglosassone.

Ogni comunicazione occupa un canale e richiede una coppia di frequenze dedicate, una per la trasmissione dal dispositivo mobile alla SRB, detta frequenza uplink, e una per la trasmissione dalla SRB al dispositivo mobile, detta frequenza downlink.

Le frequenze utilizzabili, non sono certo illimitate e nascerebbe presto il problema delle interferenze fra celle adiacenti che usassero lo stesso canale. In realtà, la portata del segnale radio

di ogni cella decresce con l'aumentare della distanza e le celle stesse sono raggruppate in "cluster" (insieme di celle).

Ad ogni "cluster" viene assegnata tutta la banda disponibile e ogni cella utilizza frequenze diverse (fra le sette disponibili) rispetto ad ogni altra cella adiacente, appartenente al medesimo cluster. Inoltre, il sistema è organizzato in modo che le celle che utilizzano la stessa frequenza siano separate da una distanza chiamata "*distanza di riuso*" necessaria, come ho già detto, ad evitare interferenze.

A questo punto si rende necessario ricorrere ad un disegno esplicativo, tanto per mettere ordine e fare chiarezza in un discorso che va facendosi sempre più intricato. In fig. 2 sono raffigurati tre diversi cluster. La linea rossa rappresenta la distanza di riuso fra due celle aventi la stessa frequenza.

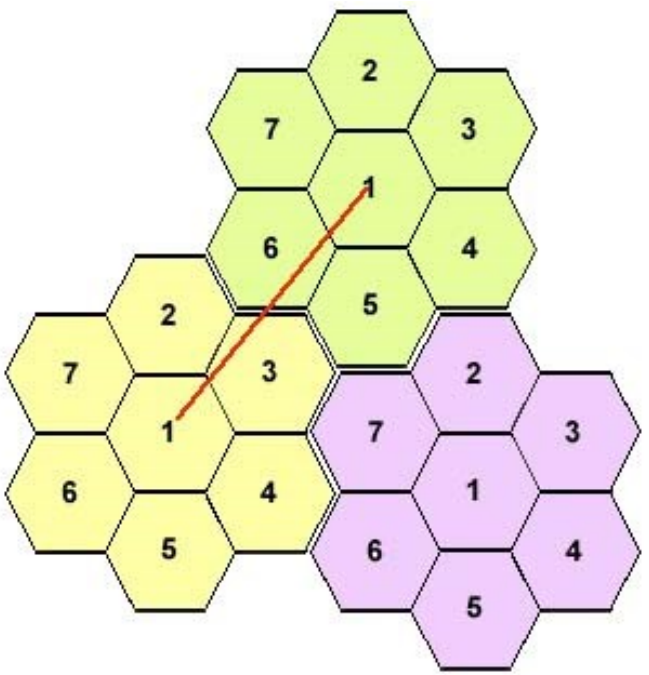

Fig.2

Le celle mostrate nel disegno della pagina precedente, rappresentano le aree di territorio idealmente coperte da ciascuna di esse. Ovviamente, nella realtà le cose sono molto diverse; la conformazione orografica della zona, pianeggiante o con rilievi montuosi, rurale o in centri abitati, la presenza di ostacoli di natura antropica, edifici ecc. alterano in modo determinante la geometria delle aree coperte dal segnale radio.

Esattamente ciò che ho affermato, fra l'altro, nella premessa di questo libro.

Ma torniamo al tema di questo capitolo, per tentare di chiarire nel modo più lineare possibile, l'architettura della rete cellulare GSM, partendo dal basso, ossia dal telefonino che aggancia il proprio ripetitore e, a seguire, gli altri elementi necessari al corretto funzionamento del sistema e all'instradamento delle chiamate:

- MS; (*Mobile Station*) Il telefonino, ma anche qualunque apparecchiatura in grado di comunicare, tramite onde radio, con le stazioni della rete cellulare. Dispone di uno "slot" in cui inserire la SIM, senza la quale non è possibile autenticarsi e accedere alla rete.

- BTS; (*Base Transceiver Station*) stazione radio che riceve e ritrasmette i segnali dei telefoni cellulari. La zona che copre con il suo segnale è detta cella e il luogo in cui è installata è chiamato sito della cella;

- BSC; (*Base Station Controller*) elemento della rete che effettua l'assegnazione del canale (la coppia di frequenze uplink e downlink) e fa da ponte tra il Mobile Switching Center e la Base Transceiver Station, coordinando gruppi di BTS;

- MSC; (Mobile Switching Center) sistema di commutazione che interconnette un elevato numero di BSC con l'interfaccia GMSC

- GMSC; (*Gateway MSC*) interfaccia con la rete telefonica pubblica, tecnicamente chiamata PSTN (*Public Switched Telephone Network*).

Per concludere, si osservi il disegno di fig.3 che cerca di semplificare e rendere "visualizzabile" quanto appena detto.

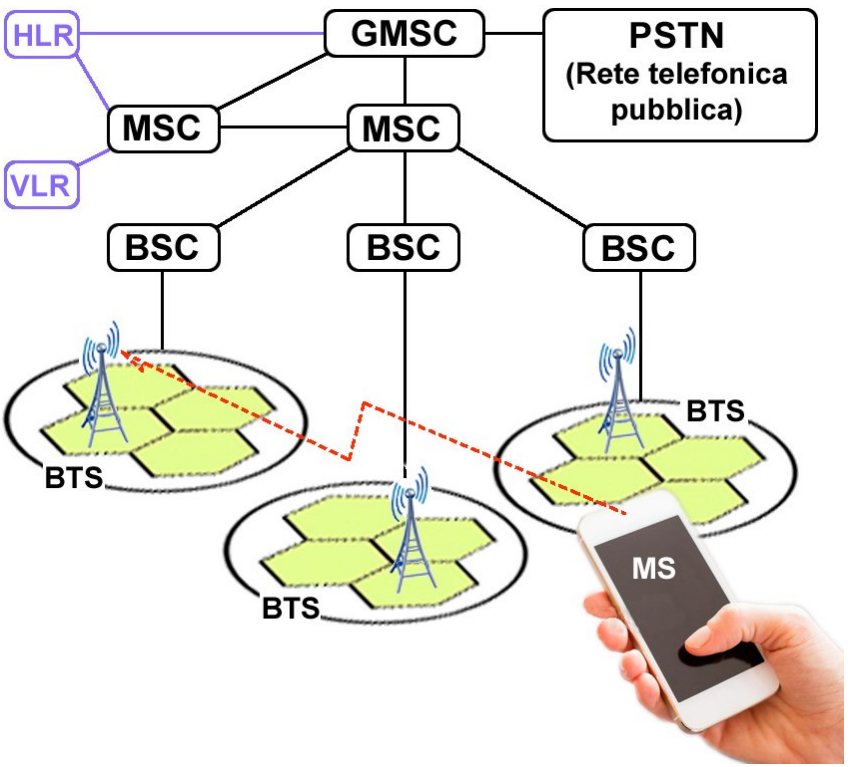

Fig.3

Avrete notato che, nell'elenco precedente, mancano due elementi che sono invece presenti nel disegno schematico; l'HLR e il VLR.

In realtà si tratta di una scelta voluta, per semplificare una trattazione già di per sé complessa, tralasciando elementi che, seppur essenziali al corretto funzionamento della rete telefonica cellulare, non sono tuttavia determinanti per la comprensione dei temi di questo libro.

Nonostante ciò, per completezza espositiva, li elenco di seguito;

- HLR (*Home Location Register*) database centrale condiviso con la rete GPRS, che memorizza i dati personali degli utenti, i servizi attivati, l'ultima posizione rilevata sulla rete e li autorizza ad usare la rete GSM;

- VLR (*Visitor Location Register*) database a supporto dei dispositivi mobili che sono in roaming, a cui fornisce un numero telefonico temporaneo (MSRN; *Mobile Station Roaming Number*) utilizzato solo fino a quando la comunicazione in atto non è conclusa;

Ogni registro supervisiona un gruppo di "*location areas*" e memorizza sia dati permanenti che temporanei.

Ci sono ancora altri elementi, come ad esempio l'AUC (*Authentication Center*), che genera e memorizza le chiavi di autenticazione e cifratura o l'EIR (*Equipment Identity Register)*, un database preposto alla conservazione dati relativi ai dispositivi degli utenti), ma evito di mettere nel calderone questi ulteriori dati per le ragioni già esposte. Basti sapere che, nel complesso universo delle telecomunicazioni mobili, ci sono anche loro.

Per quel che riguarda le reti GPRS (vedi 6.1), che usano la maggior parte delle componenti GSM e le reti UMTS (vedi 6.3), che sfruttano componenti sia GSM che GPRS, evito di entrare in dettagli tecnici che esulano da questa trattazione. Chi fosse interessato potrà trovare testi specifici per gli approfondimenti.

Le reti di seconda generazione: il GPRS

Il GPRS, acronimo di "*General Packet Radio Service*" consiste in un modo di trasferimento dei dati definito "commutazione a pacchetto", perché i dati, in formato digitale, vengono divisi per essere spediti separatamente sotto forma di "pacchetti" per poi essere ricongiunti una volta a destinazione. Viene anche definito "generazione 2.5 G" essendo il passaggio intermedio tra la seconda generazione (GSM) e la terza (3G).

Si tratta di una tecnologia datata (è solo un GSM migliorato) che comporta una navigazione internet piuttosto lenta, limitandola di fatto ai soli siti in versione mobile. È in grado di mantenere una connessione permanente ad Internet e questo fatto ha avuto la sua importanza nell'esame forense di alcuni tabulati telefonici.

La rete GPRS è utilizzata solo dal gestore Vodafone che, ovviamente, dispone anche delle tecnologie più veloci, basate sulle reti di terza generazione.

(…)

La portata delle celle telefoniche

Eccoci, finalmente, a uno dei capitoli più importanti di questo libro, assolutamente fondamentale per iniziare a comprendere il nesso funzionale tra rete cellulare, terminali telefonici e dati presenti nei tabulati.

Nei sistemi di trasmissione non cellulare, TV, radio, le comunicazioni sono di tipo “broadcast” e utilizzano stazioni di elevata potenza per coprire aree notevolmente estese.

Il sistema telefonico cellulare non è tecnicamente in grado di coprire un territorio vasto come un'intera regione attraverso un’unica stazione radio base, a causa delle caratteristiche di propagazione delle frequenze usate, nel campo delle microonde, che non permettono il superamento di rilievi orografici anche se di altezza contenuta e dell'enorme potenza che sarebbe necessaria per la trasmissione, in questo ipotetico scenario.

Ci sarebbe poi il problema dell’inquinamento elettromagnetico: anche nella situazione attuale, dove le potenze radio in gioco sono molto contenute, sia da parte dei ripetitori che da quella dei terminali, le persone temono le conseguenze sulla salute delle radioonde e non vedono di buon occhio l’installazione delle stazioni radio base.

Infine, si dovrebbe affrontare il problema della saturazione dello spettro elettromagnetico, certo non infinito, dedicato a tale servizio e proporzionale al numero degli utenti serviti.

Per questi e altri motivi, l’architettura progettuale del sistema telefonico mobile è basata su numerose unità elementari di ricetrasmissione, le stazioni radio base, appunto, ognuna di potenza ridotta e tuttavia sufficiente a coprire in modo più o meno omogeneo l'area interessata dalla cella stessa, consentendo il riutilizzo delle frequenze. Da qui il nome di “telefonia cellulare”.

Quando la cella è di tipo GSM e omnidirezionale, ossia dispone di antenne che irradiano su 360° possiamo assimilarne l'area di copertura, teorica, ad un cerchio.

Ovviamente, nell'ipotesi la cella abbia una determinata apertura angolare (quasi sempre di 120°) il risultato sarà un settore di corona circolare.

Nel caso della rete UMTS, invece, le celle hanno dimensioni che variano in funzione del traffico in atto e del numero di utenti.

Infatti, spesso la distribuzione della potenza del segnale irradiato viene ottimizzata nelle aree più critiche, a volte registrando il terminale mobile in più d'una cella contigua.

In questi casi, denominati di "*soft handover*" la posizione geografica reale del telefonino è rappresentata dalla zona in cui si sovrappongono le aree di copertura di celle contigue.

Nel prossimo capitolo, vedremo quale è la portata massima di una BTS e per quale ragione non può essere superata, al di là dei limiti costituiti da ostacoli di natura orografica o antropica.

(…)

La triangolazione,

La localizzazione topografica del terminale mobile usato da un soggetto al momento della commissione di un reato riveste fondamentale importanza per correlare la sua posizione al crimine stesso, ovviamente nella presunzione che il telefonino fosse effettivamente nelle sue mani, individuando in certi casi anche chi avesse eventualmente concorso nella realizzazione dell'evento criminoso.

Ottenere questa informazione è possibile tramite l'analisi puntuale dei tabulati richiesti dagli inquirenti, pur con tutte le limitazioni ed approssimazioni legate a questo strumento tecnico, come ho già precisato nell'introduzione a queste pagine.

Vedremo infatti, nei capitoli successivi, che questo genere di analisi è tutt'altro che semplice e può ingenerare errori, specialmente quando condotta da persone non sufficientemente competenti e preparate.

Naturalmente, esistono altre metodologie per ottenere la localizzazione di un terminale. In questo capitolo esaminiamo la procedura che va sotto il nome di "triangolazione", oltre ad alcune tecniche basate sulla velocità di propagazione delle onde elettromagnetiche.

La differenza macroscopica con l'analisi dei tabulati è che, mentre l'indagine su questi ultimi può essere effettuata anche in tempi successivi al reato e può esaminarne periodi antecedenti e/o posteriori, la localizzazione mediante la triangolazione non si può fare *ex post*, né sui tabulati ma va fatta mentre la chiamata è in corso, agendo sui radiosegnali. Ciò richiede l'attivazione di speciali procedure, basate anche sulla trigonometria, da parte dei gestori di telefonia mobile Quindi può essere richiesta solo quando si hanno già uno o più sospettati da inquisire.

Fondamentalmente si usano due proprietà geometriche della triangolazione; l'*angulation* e la *lateration* e una misura di distanza radiale, usando il "Timing Advance".

L’angulation

La tecnica di localizzazione topografica denominata “*angulation*” si fonda, come il nome stesso suggerisce, sulla misura degli angoli, attraverso equazioni trigonometriche.

Nel caso di posizionamenti bidimensionali, ove è secondario il dato della quota, come nel caso dell’individuazione di un telefono cellulare, è sufficiente conoscere una distanza (ad esempio quella fra due celle) e due angoli, rispetto ad un riferimento fisso (ad esempio, il nord) come illustrato nella fig.5, per individuare la posizione topografica del punto incognito, ossia del telefono cellulare cercato.

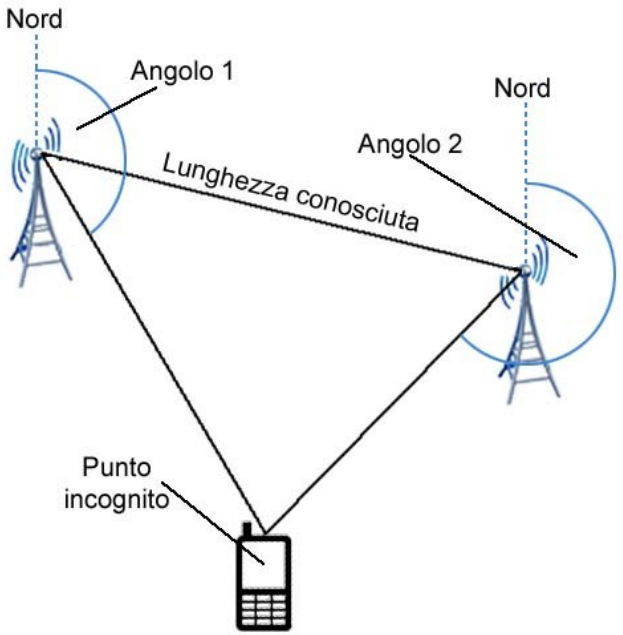

fig.5

Questo in teoria. Nella realtà, purtroppo, le cose non sono mai così nettamente determinate; si devono infatti fare i conti con segnali spuri derivanti da fenomeni di rifrazione e/o riflessione del vettore radio, nonché con tolleranze nella precisione della misura degli angoli. Conseguentemente, la posizione stimata sarà affetta da un margine di incertezza, come descritto nella fig.6.

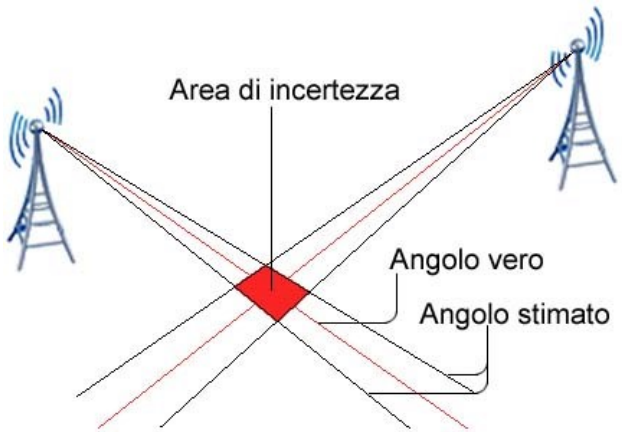

Fig.6

Ad esempio, uno dei problemi di cui tener conto è quello del cosiddetto "Multipath Fading". Quando esistono ostacoli fra il terminale mobile e il ripetitore, in situazioni dette "*Non Direct Line Of Sight*" (tipicamente in situazioni *indoor* o, nei centri abitati, fra gli edifici), la presenza di percorsi multipli dal trasmettitore al ricevitore, introduce distorsioni nel segnale ricevuto. Il risultato è l'arrivo a destinazione affetto da un certo numero di repliche, avendo subito riflessioni su superfici diverse, incontrate lungo il cammino, con attenuazioni diverse ed avendo percorso distanze differenti, che sfasano il segnale nel dominio del tempo. Il segnale diretto, tuttavia, esiste sempre, ma può essere così debole da non essere rilevabile.

Vi sono certamente delle situazioni ottimali nelle quali possiamo avere il cosiddetto "*Direct Line Of Sight*" ossia il contatto "visuale" fra trasmettitore e ricevitore che elimina, almeno teoricamente, le riflessioni e i relativi sfasamenti.

Tuttavia, i fenomeni di propagazione legati alle comunicazioni cellulari, sono spesso imprevedibili, tanto da non poterli racchiudere tutti e con esattezza in un modello matematico capace di fornirci indicazioni di *positioning* non affette da margini di errore.

La lateration

La localizzazione del terminale mobile tramite la "*lateration*" è basata sulla misura di distanze relative rispetto a punti noti, anche se non allineati.

Nel caso di sistemi automatici di rilevazione, come sono i ripetitori cellulari, vengono utilizzati fenomeni fisici mediante i quali è possibile, attraverso lo studio di appositi modelli, determinare la distanza fra trasmittente e ricevente.

Ad esempio, l'attenuazione della potenza del segnale: come è noto, per il fenomeno dell'attenuazione, l'intensità di un segnale decresce all'aumento della distanza dall'emittente.

Usando un algoritmo tale che, nota la potenza di emissione, possa correlare l'attenuazione con la distanza, è possibile risalire al percorso relativo fra ponte radio e terminale mobile.

Avendo a disposizione più elementi noti (celle) e la loro area di copertura, sarà possibile approssimare, mediante la "*lateration*", la posizione geografica dell'oggetto (fig.7).

Ovviamente, stiamo parlando della solita "situazione ideale". In ambienti *indoor* o in scenari urbani, affetti da "Multipath Fading" avremo un inevitabile peggioramento del margine di errore, dovuto anche al rumore elettronico che si somma al segnale utile (fig.8).

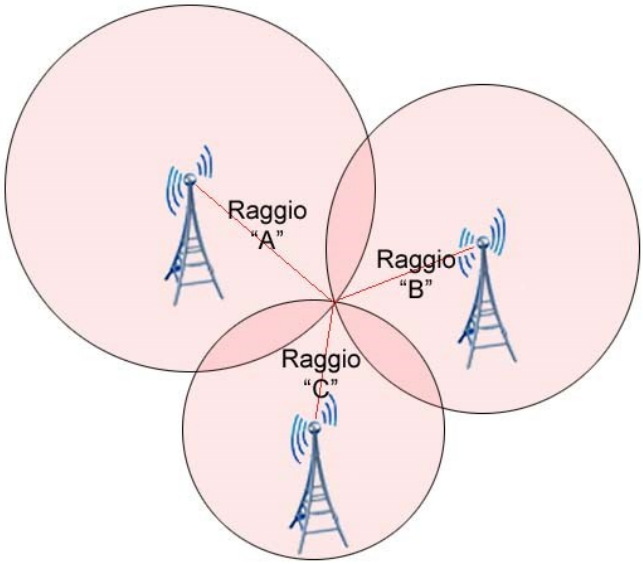
Raggio
"A"
Raggio
"B"
Raggio
"C"

Fig.7

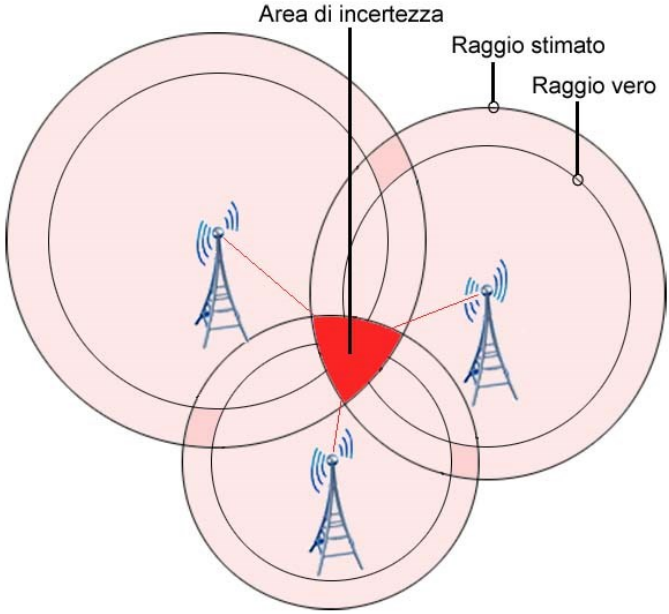
Area di incertezza
Raggio stimato
Raggio vero

Fig.8

A cosa serve l'acquisizione dei tabulati telefonici

Quando il PM, nel corso di un'indagine, chiede l'acquisizione dei tabulati relativi a una o più utenze, essenzialmente mira a stabilire dove si trovava l'indagato in un dato segmento temporale, a individuare con chi comunicava e l'esito della chiamata, se andata a buon fine o priva di risposta e se si trattava di comunicazione voce o di SMS/MMS (anche se è fallita la consegna) o altro.

Infatti, i tabulati consegnati all'Autorità di Polizia Giudiziaria, contengono fra l'altro, come vedremo nei prossimi capitoli, gli identificativi di ingresso e di uscita delle torri radio per la telefonia cellulare.

Attraverso questi identificativi, a volte addirittura completi della via e località dove è ubicato il ripetitore, è possibile stabilire, anche se in modo molto approssimativo, dove si trovavano gli interlocutori al momento della telefonata.

Se il telefono non genera traffico, ossia non effettua né riceve chiamate, ma è acceso, risulta invisibile (o meglio, non risulta nulla nel relativo tabulato telefonico).

È tuttavia possibile, in simili casi, ricorrere ad un'altra metodologia nota come "*Cell Site Analysis*" che permette di "vedere" un telefonino anche quando non è attivo.

Questa tecnica si basa sul fatto che, quando un telefono cellulare si sposta fra una cella e la successiva, deve *rinegoziare* la connessione con la rete telefonica, diventando quindi visibile anche se non sta generando traffico.

Inoltre, ogni sei minuti circa, il telefono *rinegozia* comunque la connessione anche se permane all'interno del raggio d'azione della stessa cella, perché il sistema telefonico ha necessità di sapere dove recapitare eventuali richieste di connessione o SMS/MMS, nonché di conoscerne lo stato del terminale, se acceso e raggiungibile o se *fuori campo*.

Alla luce di quanto appena detto, sembrerebbe esistere la possibilità di seguire gli spostamenti di un telefono anche se non fa e non riceve chiamate, purché sia acceso e ci sia una SIM attiva inserita, andando a leggere i "*log file*" delle celle.

In Italia, però, la registrazione di questi *log* è disattivata per default, trattandosi di un processo molto gravoso per l'hardware e in grado di produrre una enorme quantità di dati che dovrebbero essere memorizzati, con i relativi costi.

Per queste ragioni, l'attivazione dei "*log file*" avviene solo a seguito della richiesta di un magistrato, al fine di pedinare un indagato usando il suo cellulare.

Si tratta quindi, ancora una volta, di un'operazione che si svolge "*in tempo reale*" e impossibile da realizzare in tempi successivi.

Attenzione: quando, poco sopra, ho parlato della necessità della rete di conoscere lo stato del terminale se acceso e raggiungibile o se *fuori campo*, non ho nominato la situazione di *terminale spento* poiché, in tal caso, il telefono, durante la procedura di spegnimento, invia alla rete una informazione detta "*Detach*" che segnala al sistema l'irraggiungibilità del terminale.

Allo stesso modo, quando un telefonino viene acceso, invia l'informazione detta "*Attach*", insieme alle altre notifiche atte a registrarsi correttamente in rete, segnalando in tal modo al sistema cellulare la propria disponibilità.

Solo nei casi di perdita di campo o di scarica della batteria o di improvvisa avaria del terminale mobile, il segnale di "*Detach*" potrebbe non essere correttamente inviato e la rete non ne sarebbe informata fino alla prossima mancata *rinegoziazione.*

Questo particolare potrebbe rivestire notevole importanza in alcune indagini, ad esempio quando si ipotizza uno spegnimento volontario del telefonino da parte di un indagato, al fine di sottrarsi ad un'eventuale intercettazione o pedinamento elettronico.

In simili casi, la preventiva attivazione dei "*log file*" sarebbe in grado di dirimere il dubbio, cosa che l'esame dei tabulati non è in grado di fare.

Ancora una volta, quindi, l'analisi *ex post* si scontra con i limiti imposti dalla realtà; se l'indagato viene individuato in tempi successivi al reato, quando è tardi per l'intercettazione, alcune informazioni essenziali tanto per l'accusa quanto per la difesa, saranno irrimediabilmente perdute.

L'interpretazione dei "tabulati telefonici"

Come abbiamo visto nel capitolo 7, la copertura di ogni ponte ripetitore varia fra qualche centinaio di metri e diversi chilometri, in funzione delle caratteristiche orografiche del posto o dell'ubicazione fisica, se in zone rurali o fra i palazzi di una città.

Insomma, se l'intercettazione dei contenuti delle telefonate, fatta in tempo reale, consente agli inquirenti l'ascolto diretto e la registrazione delle conversazioni fra gli indagati, la documentazione del traffico prodotto dalle telecomunicazioni, (i soliti tabulati, insomma) rende possibile la ricostruzione *ex post*, di situazioni che oramai non è più possibile intercettare.

I cosiddetti "tabulati telefonici" sono più correttamente definiti, nel campo dell'analisi forense, "CDR"; *Call Detail Records*.

L'appellativo "tabulato" risale a quando era effettivamente composto da uno o più fogli stampati, contenenti righe e colonne divisi in appositi campi. I "diversamente giovani" come me, ricorderanno le stampanti ad aghi, antenate delle moderne laser o a getto d'inchiostro. A quei tempi i computer funzionavano a carbonella, scrivevano i dati su "floppy-disk" con capacità di memorizzazione di 1,44 MB, mentre i modem a 56Kbps accompagnavano le nostre navigazioni con la loro indimenticabile musichetta, alla vertiginosa velocità della Messa Cantata.

Al giorno d'oggi i CDR vengono inviati, sotto forma di files, mediante la posta elettronica o sono registrati su CD.

Tuttavia, a dispetto di ogni progresso, non esiste ancora uno standard comune a tutti gli operatori, che definisca quali e quanti "campi", in che ordine e con quali denominazioni, debbano essere presenti nel CDR.

Esistono, per la verità, alcuni accordi europei per uno standard detto "ETSI"[14], ma i vari Governi, succedutisi in Italia, non si sono mai presi l'onere di emanare i relativi decreti attuativi e quindi ognuno si regola come meglio crede.

Il risultato di quest'anarchia digitale complica non poco la vita degli inquirenti o dei periti della difesa che devono interpretare i CDR, spesso rilasciati in formato .CVS (*Comma Separated Values*) un formato utilizzato per l'importazione/esportazione di tabelle di dati, basato su file di testo che, come dice il nome stesso, hanno i campi separati da virgola o punto e virgola.

Altre volte, quando va bene, vengono rilasciati in .XLS (formato nativo di MS Excel, dedicato alla produzione ed alla gestione dei fogli elettronici) o in .TXT, un formato contenente solo caratteri di scrittura semplici che compongono un testo leggibile senza bisogno di installare appositi programmi.

Alla fine della storia, l'operatore di Polizia o il Consulente Tecnico della Difesa, debbono possedere la pazienza di un amanuense e mettere le cose in ordine a colpi di "convertitori" tipo SQL (*Structured Query Language*), un linguaggio di programmazione utilizzato per creare, trasformare e recuperare informazioni da un database quale è, appunto, Exel, o sapersi destreggiare con script Python, Visual Basic, ecc. Insomma, non proprio una passeggiata.

Si deve tener presente inoltre che, in un normale CDR, i "campi" sono spesso diverse centinaia o addirittura migliaia. Dover cercare a mano in quale l'utente del 380/123456 ha chiamato il numero 06/123456 è un'impresa sconfortante.

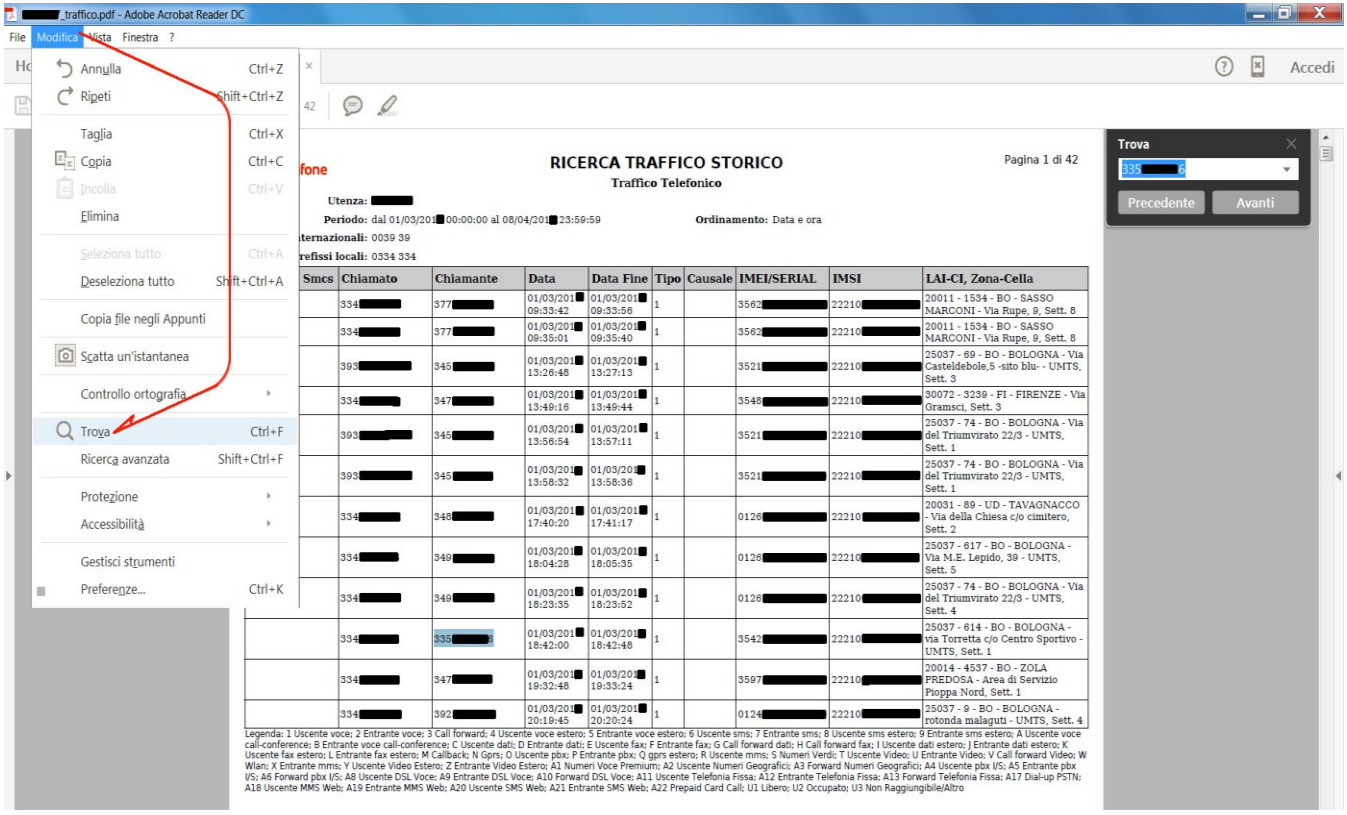
[redacted]_traffico.pdf - Adobe Acrobat Reader DC
File
Modifica
Vista
Finestra
?
Annulla Ctrl+Z
Ripeti Shift+Ctrl+Z
Taglia Ctrl+X
Copia Ctrl+C
Incolla Ctrl+V
Elimina
Seleziona tutto Ctrl+A
Deseleziona tutto Shift+Ctrl+A
Copia file negli Appunti
Scatta un'istantanea
Controllo ortografia
Trova Ctrl+F
Ricerca avanzata Shift+Ctrl+F
Protezione
Accessibilità
Gestisci strumenti
Preferenze... Ctrl+K
Accedi
Trova
Precedente
Avanti
fone
RICERCA TRAFFICO STORICO
Traffico Telefonico
Pagina 1 di 42
Utenza: [redacted]
Periodo: dal 01/03/201[redacted] 00:00:00 al 08/04/201[redacted] 23:59:59
Ordinamento: Data e ora
ternazionali: 0039 39
refissi locali: 0334 334
Smcs | Chiamato | Chiamante | Data | Data Fine | Tipo | Causale | IMEI/SERIAL | IMSI | LAI-CI, Zona-Cella
334[redacted] | 377[redacted] | 01/03/201[redacted] 09:33:42 | 01/03/201[redacted] 09:33:56 | 1 | | 3562[redacted] | 22210[redacted] | 20011 - 1534 - BO - SASSO MARCONI - Via Rupe, 9, Sett. 8
334[redacted] | 377[redacted] | 01/03/201[redacted] 09:35:01 | 01/03/201[redacted] 09:35:40 | 1 | | 3562[redacted] | 22210[redacted] | 20011 - 1534 - BO - SASSO MARCONI - Via Rupe, 9, Sett. 8
393[redacted] | 345[redacted] | 01/03/201[redacted] 13:26:48 | 01/03/201[redacted] 13:27:13 | 1 | | 3521[redacted] | 22210[redacted] | 25037 - 69 - BO - BOLOGNA - Via Casteldebole,5 -sito blu- - UMTS, Sett. 3
334[redacted] | 347[redacted] | 01/03/201[redacted] 13:49:16 | 01/03/201[redacted] 13:49:44 | 1 | | 3548[redacted] | 22210[redacted] | 30072 - 3239 - FI - FIRENZE - Via Gramsci, Sett. 3
393[redacted] | 345[redacted] | 01/03/201[redacted] 13:56:54 | 01/03/201[redacted] 13:57:11 | 1 | | 3521[redacted] | 22210[redacted] | 25037 - 74 - BO - BOLOGNA - Via del Triumvirato 22/3 - UMTS, Sett. 1
393[redacted] | 345[redacted] | 01/03/201[redacted] 13:58:32 | 01/03/201[redacted] 13:58:36 | 1 | | 3521[redacted] | 22210[redacted] | 25037 - 74 - BO - BOLOGNA - Via del Triumvirato 22/3 - UMTS, Sett. 1
334[redacted] | 348[redacted] | 01/03/201[redacted] 17:40:20 | 01/03/201[redacted] 17:41:17 | 1 | | 0126[redacted] | 22210[redacted] | 20031 - 89 - UD - TAVAGNACCO - Via della Chiesa c/o cimitero, Sett. 2
334[redacted] | 349[redacted] | 01/03/201[redacted] 18:04:28 | 01/03/201[redacted] 18:05:35 | 1 | | 0126[redacted] | 22210[redacted] | 25037 - 617 - BO - BOLOGNA - Via M.E. Lepido, 39 - UMTS, Sett. 5
334[redacted] | 349[redacted] | 01/03/201[redacted] 18:23:35 | 01/03/201[redacted] 18:23:52 | 1 | | 0126[redacted] | 22210[redacted] | 25037 - 74 - BO - BOLOGNA - Via del Triumvirato 22/3 - UMTS, Sett. 4
334[redacted] | 335[redacted] | 01/03/201[redacted] 18:42:00 | 01/03/201[redacted] 18:42:48 | 1 | | 3542[redacted] | 22210[redacted] | 25037 - 614 - BO - BOLOGNA - via Torretta c/o Centro Sportivo - UMTS, Sett. 1
334[redacted] | 347[redacted] | 01/03/201[redacted] 19:32:48 | 01/03/201[redacted] 19:33:24 | 1 | | 3597[redacted] | 22210[redacted] | 20014 - 4537 - BO - ZOLA PREDOSA - Area di Servizio Pioppa Nord, Sett. 1
334[redacted] | 392[redacted] | 01/03/201[redacted] 20:19:45 | 01/03/201[redacted] 20:20:24 | 1 | | 0124[redacted] | 22210[redacted] | 25037 - 9 - BO - BOLOGNA - rotonda malaguti - UMTS, Sett. 4
Legenda: 1 Uscente voce; 2 Entrante voce; 3 Call forward; 4 Uscente voce estero; 5 Entrante voce estero; 6 Uscente sms; 7 Entrante sms; 8 Uscente sms estero; 9 Entrante sms estero; A Uscente voce call-conference; B Entrante voce call-conference; C Uscente dati; D Entrante dati; E Uscente fax; F Entrante fax; G Call forward dati; H Call forward fax; I Uscente dati estero; J Entrante dati estero; K Uscente fax estero; L Entrante fax estero; M Callback; N Gprs; O Uscente pbx; P Entrante pbx; Q gprs estero; R Uscente mms; S Numeri Verdi; T Uscente Video; U Entrante Video; V Call forward Video; W Wlan; X Entrante mms; Y Uscente Video Estero; Z Entrante Video Estero; A1 Numeri Voce Premium; A2 Uscente Numeri Geografici; A3 Forward Numeri Geografici; A4 Uscente pbx I/S; A5 Entrante pbx I/S; A6 Forward pbx I/S; A8 Uscente DSL Voce; A9 Entrante DSL Voce; A10 Forward DSL Voce; A11 Uscente Telefonia Fissa; A12 Entrante Telefonia Fissa; A13 Forward Telefonia Fissa; A17 Dial-up PSTN; A18 Uscente MMS Web; A19 Entrante MMS Web; A20 Uscente SMS Web; A21 Entrante SMS Web; A22 Prepaid Card Call; U1 Libero; U2 Occupato; U3 Non Raggiungibile/Altro

Fig.9

Nel caso, invece, di un CDR in formato .TXT o Excel o PDF, è possibile utilizzare le apposite finestre di ricerca per raggiungere istantaneamente il dato ricercato, come si può vedere nell'esempio della pagina precedente, un file in PDF (Fig.9). Cliccando su "Modifica", poi su "Trova" e infine digitando nella finestra in alto a destra, il dato ricercato. Nel mio caso il numero 335/xxxxx6, che viene evidenziato in un riquadro azzurro.

Ovviamente, trattandosi di un CDR riferito ad un caso reale, ho oscurato tutti i dati sensibili.

Per far fronte alla mancanza di standardizzazione nei tabulati telefonici e rendere più rapide ed efficaci le indagini in questo particolare settore, sono stati elaborati diversi software in grado di importare i files nel formato in cui si trovano rimettendo ordine nelle informazioni contenute e, soprattutto, correlandoli e georeferenziandoli fra loro e con altre fonti investigative quali, ad esempio, note sul traffico autostradale o informazioni estratte da telefoni cellulari o smartphone, tramite gli appositi dispositivi di copia forense dei dati.

Nel prossimo capitolo esamineremo alcuni fra i più conosciuti software professionali, che richiedono il pagamento della licenza d'uso, seguiti da alcune "app" per tablet e smartphone che, pur avendo non pochi limiti, nella loro semplicità, sono del tutto gratuite.

14) L'ETSI, *European Telecommunications Standards Institute*, è un organismo internazionale, indipendente e senza fini di lucro, responsabile europeo della definizione e dell'emissione di standard nel campo delle telecomunicazioni.

(…)

I software per l'analisi dei "tabulati"

Esistono alcuni programmi per PC e anche per tablet o per i moderni smartphone, progettati appositamente per individuare la posizione dei ponti radio cellulari a partire dai dati di LAI/CI presenti nei CDR. Sono altresì in grado di correlare molti dati eseguendo velocemente delle ricerche che, a mano, richiederebbero tempi improponibili.

Qui di seguito ne esaminiamo alcuni fra i più diffusi. Si tratta di software professionali di alto livello e, quindi, dal costo adeguato.

Le "App" Android per l'analisi dei "tabulati"

Esistono anche alcune "app" per tablet o per i moderni smartphone, gratuite o comunque acquistabili per pochi euro.

Occorre precisare che non sono in grado di importare i tabulati nei loro formati nativi, né sono in grado di svolgere il fondamentale compito di correlare i dati fra loro, sollevando l'operatore da questa lunghissima operazione.

Possono essere utili al consulente della difesa, solamente per una prima generica "scrematura" dei dati ricevuti, per individuare la posizione dei ponti cellulari a partire dai loro segnali radio o attraverso i dati LAI/CI, anche se, ovviamente, con un livello di precisione nettamente inferiore ai programmi professionali (e costosi) visti nel capitolo precedente.

Chi vuole operare in maniera tecnicamente ineccepibile, non può prescindere dal rivolgersi a tali software-house, specializzate in questo particolare settore. Qui di seguito esaminiamo alcune fra le più diffuse "app" progettate per il sistema operativo "Android", ma anche chi usa s.o. differenti potrà trovare in rete gli equivalenti adatti

(…)

L'analisi della memoria del terminale

Nel cap.2, a proposito della "data retention" si accennava al fatto che non è possibile, *ex post*, risalire al contenuto di una conversazione telefonica, né ai testi di eventuali "messaggini" SMS scambiati fra un indagato e i suoi contatti sociali o, peggio, il suo sodalizio criminale.

Sarebbe, infatti, del tutto irragionevole, sul piano tecnico/pratico, registrare i milioni di SMS scambiati fra gli utenti o le conversazioni intercorse, poiché questo, al di là delle norme di legge, comporterebbe l'utilizzo di un numero impressionante di *petabyte* di memoria.

La conservazione da parte del gestore è limitata, infatti, alle sole informazioni che consentono la tracciabilità degli accessi: numero telefonico chiamante/chiamato, data, ora e durata della conversazione, cella/celle utilizzata/e, IMEI e IMSI.

Tuttavia, molteplici soggetti potrebbero essere interessati all'utilizzo forense di una prova informatica. Si pensi ad esempio al Pubblico Ministero che deve utilizzare mezzi di ricerca della prova[18] a carico dell'imputato di un reato, in cui l'utilizzo dello strumento informatico, nel nostro caso il telefono cellulare, è mezzo o fine dell'attività criminale.

Sullo stesso piano, ma con finalità diametralmente opposte, il collegio difensivo deve fornire prove a favore del proprio assistito o alla persona fisica o giuridica che intende far valere in giudizio la lesione di un proprio diritto da parte di un soggetto terzo, magari con la richiesta di un risarcimento del danno in sede civilistica. Infatti, l'impiego della prova digitale non è limitato al solo ambito penale, ma sempre più spesso è usata in giudizi civili o giuslavoristici[19].

In simili casi, l'unica soluzione possibile per gli organi inquirenti per il recupero delle fonti di prova utilizzabili in sede processuale, è rappresentata dal sequestro del terminale e dalla successiva analisi della sua memoria, alla ricerca non solo degli

SMS scambiati e dell'elenco delle chiamate fatte o ricevute, ma anche, di eventuali immagini, indirizzi IP, localizzazioni GPS e altri dati digitali utili alle indagini.

A tal proposito, è utile ricordare che la cancellazione o l'occultamento intenzionale di files compromettenti o d'intere cartelle dalla memoria di un computer o di un telefono cellulare, non sempre impedisce che tali dati siano recuperati, mediante l'uso di appositi software, né che si possano ricostruire le attività compiute di recente con il dispositivo.

Infatti, la cancellazione di dati da un computer o telefono cellulare, tablet o, più in generale da qualsiasi dispositivo dotato di memoria, è un'operazione a livello logico che elimina solo i riferimenti a quei files, rimettendo a disposizione del sistema operativo le aree del supporto di memoria assegnate in precedenza.

In questo modo, la persistenza dei dati nella memoria di massa permette che vengano recuperati in modo più o meno integrale, salvo che non siano stati sovrascritti da files più recenti.

Qualsiasi sistema operativo è programmato in modo da registrare numerose informazioni, sotto forma di files, in posizioni note del disco di memoria.

Si tratta di dati di log, informazioni che si riferiscono alla configurazione del sistema, agli utenti, all'utilizzo delle applicazioni installate, alla memorizzazione di punti di ripristino del sistema, che consentono al tecnico in computer o mobile forensics la ricostruzione di una "time-line" dell'uso del dispositivo da parte dell'utente (o dei vari utenti, se sono più d'uno), di identificare quali periferiche esterne sono state collegate (hard-disk esterni, pennette di memoria ecc.), rilevare l'elenco dei files stampati e con quale stampante (e a volte anche il loro contenuto), le reti lan o wi-fi con le quali si è collegato e molte altre notizie utili ai fini probatori.

Ci sono poi numerose applicazioni che memorizzano "metadati", spesso all'insaputa dell'utente, in speciali files nascosti, prodotti in seguito al loro uso, che possono essere estratti ed esaminati tramite speciali software di analisi forense.

Persino una semplice foto digitale contiene, invisibili all'utente, una serie d'informazioni (ancora metadati) capaci di raccontare molte cose a chi parla "informatichese".

Quanto ho scritto sopra, può riferirsi tanto a un computer quanto ad un telefono cellulare, ma anche a molti altri generi di supporti di memoria.

Non dimentichiamo, inoltre, che i moderni smartphone sono forniti di un proprio sistema operativo e sono capaci di navigare in internet, lasciando inevitabilmente traccia dei siti visitati, delle e-mail scambiate ecc.

Si tratta però di elementi inseriti in un ambiente caratterizzato da elevata probabilità di alterazione, anche involontaria, dei dati registrati in memoria.

Basti dire che il semplice spegnimento di un computer acceso può modificarne alcuni dati o che lo spostamento di un telefonino, se collegato alla rete cellulare, comporta l'alterazione del contenuto al momento di un eventuale cambio di cella o in seguito alla ricezione di chiamate e/o SMS.

Per prevenire tali problemi, la prima azione da mettere in atto al momento del sequestro di un cellulare è il suo isolamento elettromagnetico o, se questo non è possibile, lo spegnimento (anche se questo potrebbe comportare, in fase di riattivazione, l'inserimento di un PIN), eseguendo successivamente copie forensi della memoria del terminale e della SIM.

Insomma, l'approccio con il dispositivo digitale deve essere realizzato in modo da escludere modificazioni improprie delle tracce informatiche. Questo è il compito della "digital forensics" che esaminiamo nel prossimo capitolo.

18) I mezzi di ricerca della prova sono strumenti d'indagine che consentono di acquisire la prova (perquisizioni, sequestri, intercettazione di comunicazioni). Ne consegue che le norme sui mezzi di ricerca della prova sono rivolte al Pubblico Ministero (e per quanto di competenza alla polizia giudiziaria), mentre i mezzi di prova sono di competenza del Giudice.

19) Si pensi, ad esempio, alla presenza di files attestanti il possesso illegittimo di dati coperti dal diritto di proprietà intellettuale o a evidenze digitali di attività con strumenti informatici aziendali, non permesse durante l'orario di lavoro o volte a inviare a terzi documenti e/o dati riservati.

La digital forensics e i "forensic tools"

Il numero di dispositivi elettronici/informatici che fanno parte, sempre più pervasivamente, della nostra vita quotidiana, è in costante crescita e, parallelamente, s'intensifica la richiesta di analisi dei dati digitali, a fini investigativi e di giustizia, sui reati commessi attraverso l'uso di dispositivi informatici o le cui tracce sono memorizzate in tali sistemi.

Questo tipo di analisi è compito specifico della "digital forensics", che deve operare attraverso corrette metodologie atte a individuare, acquisire, preservare e valutare le informazioni contenute.

In conformità a questi elementi di prova, la cui funzione principale è dunque quella di permettere la corretta ricostruzione e dimostrazione dei fatti affermati dalle parti durante il processo, il giudice, nel rispetto del principio del contraddittorio, fonderà la propria decisione.

Tuttavia, il processo di acquisizione dei dati forensi rappresenta una sfida tecnica importante per chi compie le indagini, in considerazione dell'elevato rischio di alterazione degli originali che minerebbe *ab origine* il valore probatorio del materiale acquisito.

La conservazione dei dati presenti sui supporti di memoria è estremamente importante così com'è fondamentale evitarne la benché minima alterazione. Infatti, tutte le analisi devono essere eseguite in "modalità ripetibile" ossia tutte le informazioni raccolte devono poter essere verificabili in qualsiasi momento.

Per questa ragione si deve lavorare su copie speculari dei supporti di memoria (le cosiddette immagini) piuttosto che sui dati originali[20].

In sintesi quindi, scopo fondamentale della digital forensics è trattare i dati in maniera da non alterarne l'integrità e la genuinità per non comprometterne la ripetibilità nell'eventuale futuro utilizzo in sede processuale, applicando specifiche e validate procedure per la loro acquisizione e conservazione[21].

Il primo fondamentale passo da compiere è la copia dei dati contenuti nelle memorie del dispositivo sequestrato (nel nostro caso, trattandosi di un telefono cellulare, è più corretto parlare di "mobile forensics").

Ovviamente tale copia va eseguita, tassativamente, attraverso l'uso di dispositivi hardware e software che escludano qualsiasi rischio di scrittura di dati, ancorché involontaria, nell'apparecchio in sequestro (write blocker).

Le modalità di acquisizione dei dati possono essere di tipo fisico o logico.

La prima è preferibile rispetto alla seconda perché consente il recupero di dati di qualsiasi tipo rimasti in memoria (memoria non allocata o spazio sul file system) per poi poterli analizzare.

L'acquisizione logica è più limitata rispetto all'acquisizione fisica, ma offre il vantaggio di recuperare i dati sotto forma di file e directory, facilmente utilizzabili nella successiva fase di analisi. Nulla impedisce, tuttavia, di usare entrambe le modalità.

Al termine della copia dovrà essere elaborato un algoritmo matematico che trasformi i dati trascritti in una stringa binaria di dimensione fissa chiamata "*valore di hash"*.

Quest'algoritmo crittografico produce, a partire da una sequenza di bit di lunghezza e contenuto arbitrari, una serie di caratteri alfanumerici che godono di alcune interessanti proprietà. Ad esempio, due sequenze di bit identiche, producono hash identici.

Quindi, per verificare l'assenza di alterazioni rispetto all'originale, è sufficiente ripetere il calcolo dell'hash.

Confrontando l'hash generato dalla copia con quello generato dall'originale, avremo la certezza, se i due risultati coincidono, dell'assoluta identicità dei dati e quindi del valore forense della copia.

La probabilità di generare il medesimo codice hash (detta "*probabilità di collisione*"), partendo da sequenze diverse è in pratica nulla, pur dipendendo dall'algoritmo di hashing usato.

Ad esempio, l'hash MD5 produce codici di trentadue caratteri ed ha una "probabilità di collisione" pari a $1/ 2^{64}$ ossia uno su diciotto miliardi di miliardi.

L'hash SH1 produce codici di quaranta caratteri ed ha una "probabilità di collisione" pari a $1/2^{80}$ ossia uno su milleduecento miliardi di miliardi.

Com'è evidente, la "digital forensics" e la "mobile forensics" richiedono un elevato livello di specializzazione e un costante aggiornamento tecnico, per rimanere al passo con tecnologie complesse e in rapida, continua evoluzione.

Per queste ragioni è necessario, in alcuni casi, rivolgersi a centri specializzati per certi tipi di analisi, tanto da parte delle Procure, quanto da parte del collegio difensivo.

Infine, per terminare questo capitolo, non dimentichiamo che la corretta interpretazione di un'evidenza digitale richiede l'analisi di più informazioni a essa relative di quanto non si creda. Non è sufficiente, ad esempio, aver recuperato materiale illecito nel computer o nel telefonino di un indagato, ma occorre anche accertare l'intenzionalità nel detenerlo, costatandone

l'allocazione in cartelle non di sistema quali, ad esempio, i cosiddetti "file temporanei di Internet", o verificandone l'organizzazione in cartelle o sottocartelle.

Occorre inoltre escludere che tale materiale non sia conseguenza della visualizzazione delle cosiddette "finestre di pop-up" aperte in modo automatico da alcuni siti internet durante la loro visita.

Le metodologie e gli strumenti usati in informatica forense, infatti, sono tutt'altro che perfetti e possono generare errori di varia natura, capaci di inficiare la valenza probatoria delle tracce digitali riscontrate. Ancora meno perfetto e ancora più soggetto a errori è l'elemento umano, posizionato dall'altro lato della tastiera, a volte soggetto all'innamoramento della propria tesi accusatoria o a interpretazioni poco imparziali dei fatti.

20) Di norma, sono generate più copie: una master e alcune di lavoro per tutte le parti coinvolte nel processo. Le cosiddette "immagini" sono ampiamente accettate nei tribunali, purché correttamente realizzate, come rappresentazioni dei dispositivi originali.
Inoltre, le copie forensi permettono la restituzione del dispositivo originale al proprietario che, in tal modo, può continuare il suo lavoro su quella risorsa.

21) Anche la semplice accensione di un computer spento comporta la scrittura e/o modifica di numerosi files nel suo disco fisso di sistema, mentre, viceversa, il suo spegnimento determina la perdita dei dati contenuti nella memoria volatile.
Addirittura, l'esplorazione del contenuto di un hard-disk, se non eseguita attraverso hardware e software opportuni, modifica le proprietà di alcuni files come, ad esempio, la data e l'ora dell'ultimo accesso.

La catena di custodia

Uno dei requisiti fondamentali perché una prova sia ammessa nel processo, civile o penale che sia, è la sua idoneità a dimostrare i fatti ai quali si riferisce, come abbiamo visto nel capitolo precedente.

A tali requisiti è sottoposta, ai fini della sua utilizzazione in sede processuale, anche la prova informatica, soprattutto dal punto di vista dell'integrità dell'elemento raccolto, allo scopo di evitare che venga ripudiata da una delle parti.

La "catena di custodia" (*chain of custody*) è quella serie di azioni tese a garantire la corretta ed ininterrotta continuità nella gestione e custodia del reperto, dal momento in cui viene sequestrato al momento in cui viene prodotto in giudizio.

L'integrità, specialmente in un contesto caratterizzato da elevato rischio di alterazione delle informazioni o dei dati conservati o scambiati fra dispositivi digitali, deve essere tale da escludere modificazioni indebite delle tracce informatiche, avvenute in epoca successiva alla creazione di una copia, su apposito supporto, detta "bit a bit".

Per tali ragioni è fondamentale che, nell'acquisizione degli elementi di prova, vengano utilizzate e rispettate le procedure proprie della digital forensics (la cosiddetta "chain of custody" o "catena di custodia") e che le stesse siano formalizzate in un verbale sottoscritto dai presenti, che costituirà la corretta documentazione cronologica delle operazioni effettuate**,** contenente l'identificazione e la descrizione dei supporti e le azioni intraprese per la custodia di ciascuno di essi, insieme al dispositivo originale, in apposita busta sigillata e firmata dalle parti.

Infatti, le evidenze informatiche raccolte senza adottare le idonee metodologie, anche in seguito alle modifiche apportate dalla legge n. 48/2008 al c.p.p. in relazione agli articoli

riguardanti i mezzi di ricerca della prova e in particolare le ispezioni, le perquisizioni e i sequestri, comporta loro inutilizzabilità in sede processuale, poiché considerate inidonee a garantire l'integrità e genuinità degli elementi raccolti e pertanto ad accertare i fatti di reato[22].

In ogni caso, è importante ricordare che le prove informatiche prodotte in giudizio, benché raccolte nel rispetto delle procedure e con le accurate e validate metodologie della digital forensics, sono pur sempre il risultato dell'attività peritale di una parte[23] e, pertanto, non hanno pieno valore probatorio, ma sono liberamente valutabili dal giudice.

(…)

Gli "Anonymous remailer" nelle indagini informatiche

Quando un utente si collega al proprio "*provider*" per ottenere la connessione alla rete internet, è identificato, attraverso l'invio del suo user-name e della password, come soggetto abilitato a ricevere i servizi.

Una volta riconosciuto dal sistema, gli viene assegnato un indirizzo IP dinamico (indirizzo di protocollo internet) che identificherà univocamente il suo computer (o smartphone, nel caso di navigazione tramite telefono cellulare) durante il collegamento.

Nel momento in cui l'utente si collega a un "*server"* di posta elettronica, viene nuovamente registrato l'accesso richiedendo user-name e password collegati all'indirizzo di posta stesso.

Sono altresì registrate data e ora del "*login*" e del "*logout*" e l'indirizzo dell'IP dinamico.

Grazie a questi elementi, sarà eventualmente possibile, in seguito, risalire all'utilizzatore della connessione, incrociando le informazioni derivanti dai cosiddetti "*file* di *log*", conservati presso il provider.

Nel caso d'intercettazione telematica, il flusso di dati è trasferito tramite linea dedicata ad alta velocità verso la postazione della P.G. ove è prima decodificato e poi memorizzato, tramite un software che interpreta i protocolli in maniera che l'addetto alla postazione possa distinguere tra i messaggi di posta elettronica inviati e/o ricevuti, le pagine web visitate, le chat e così via.

Tuttavia, l'utilizzo di *software* in grado di occultare l'identità della macchina dalla quale è stato compiuto un crimine informatico, nonostante che a ogni connessione ciascun utente sia contrassegnato da un indirizzo IP univoco, rende difficoltosa, o addirittura impossibile, l'identificazione e la localizzazione dell'elaboratore collegato alla rete internet.

Ad esempio, un sistema di mascheramento dell'identità di un computer o smartphone utilizzati per scopi illeciti è l'utilizzo di speciali server cosiddetti *"anonymous remailer"*.

L'*"anonymous remailer"* non appena riceve un messaggio di posta elettronica, lo re-invia seguendo le istruzioni incluse nel messaggio stesso, senza rivelare la loro provenienza originaria e nascondendo, per esempio, l'identità del mittente dell'e-mail mediante la rimozione dell'intestazione e la sostituzione con intestazioni fittizie.

Queste operazioni di ricezione/camuffamento/re-invio sono ripetute più volte fra diversi server anonimizzatori, rendendo di fatto impossibile l'identificazione del sistema informatico di partenza.

In altri casi, particolarmente inquietanti, possiamo vedere all'opera pirati informatici capaci di acquisire user-name e password di un ignaro utente, manipolandone fisicamente il computer o attraverso l'invio, in allegato a messaggi di posta elettronica, di specifici programmi spia accuratamente occultati, i cosiddetti *"trojan horses"*.

In seguito, il pirata informatico potrà collegarsi alla rete usando le credenziali della sua vittima, magari attraverso un punto di accesso Wi-Fi libero, commettendo ogni genere di reato, dal traffico di materiale pedopornografico alla frode commerciale.

22) La recente ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica, ha individuato la necessità di adottare specifiche cautele nella gestione delle evidenze digitali, adottando "*misure tecniche dirette ad assicurare la conservazione dei dati originali e a impedirne l'alterazione*" (art. 8 commi 1 e 2, art. 9 commi 1 e 3), specificando inoltre che "*la loro acquisizione avvenga mediante copia di essi su adeguato supporto con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità*" (art. 8 commi 5 ed 8, art. 9 comma 3)

23) Di norma è la Procura ad analizzare i dispositivi sequestrati durante le indagini, attraverso i suoi tecnici, mentre il Consulente della Difesa si limita a verificare la correttezza del lavoro svolto, in sua presenza, agendo sulle copie digitali degli stessi.

Bibliografia

- AA.VV. *Codice Penale, V edizione*, Maggioli, Santarcangelo di Romagna 2011
- AA.VV. *Codice di procedura penale, IV edizione,* Maggioli, Santarcangelo di Romagna 2011
- Baroggi R. *Elaborazione e trasmissione dei dati a distanza: tecniche e metodologie*, Angeli, Milano 1984
- Brescia G. *Manuale del perito e del consulente tecnico nel processo civile e penale,* Maggioli, Santarcangelo di Romagna 2007
- Bertoni L. *Le intercettazioni. Mezzo di ricerca della prova nel processo*, Nuova Giuridica, Macerata 2012
- Gasparini G. Ippolito C., *Consulenti tecnici e periti* , Ediz. Giuridiche Simone, Pozzuoli 2002
- Gleick J. *L'informazione. Una storia. Una teoria. Un diluvio*, Feltrinelli, Milano 2012
- Huber D.M. Runstein R. E. *Manuale della registrazione sonora: Concetti generali, tecnologia audio analogica e digitale, attrezzature, procedure*, Hoepli, Milano 1999
- Nazzaro G. *Le intercettazioni sulle reti cellulari*, Mattioli, Fidenza 2010
- Paoloni A. Zavattaro D. *Intercettazioni telefoniche e ambientali*, Centro Scientifico Editore, Torino 2007

- Rapetto U. Di Nunzio R. *L'atlante delle spie: dall'antichità al "Grande Gioco" a oggi*, Rizzoli, Milano 2002

- A. Rizzo, *Manuale pratico delle intercettazioni*, Experta, Forlì 2002

- Ruggiero G., *Compendio delle investigazioni difensive* (Giuffré, Milano 2003)

- Tessitore A. Marino C. *Intercettazioni elettroniche e informatiche, le tecniche*, Sandit, Albino (BG) 2011

Sitografia

- http://www.altalex.com/

- http://www.brocardi.it/codice-di-procedura-penale/

- https://nannib.files.wordpress.com/.../seg_iii_mmxiv_bassetti_reale5.pdf

- http://www.sicurezzaegiustizia.com

- http://www.carabinieri.it/editoria/rassegna-dell-arma/anno-2013, (Bovio Sergio *Videoriprese e pedinamento satellitare*, Rassegna dell'Arma dei Carabinieri, Studi, Ott. Dic. 2013)

Convegni

- Collegio Periti Italiani: 4° Convegno nazionale del consulente tecnico e del perito: *Importanza del Consulente Tecnico e del Perito nel processo civile e penale.* maggio 2009, Tribunale di Roma, Aula Occorsio, Piazzale Clodio

- Consiglio Superiore della Magistratura: *"Tecniche di indagine e rapporti tra p.m., polizia giudiziaria, consulenti tecnici e difensori"* Roma, 4-8 luglio 2011

- Scuola Superiore della Magistratura: "*I tabulati: tecniche di interpretazione e limiti epistemologici*" corso: "*Che c'è di nuovo in tema di intercettazioni*" Roma, 3-5 novembre 2014