

Smart & Cell Phone Forensics

Ra.C.I.S. – Reparto Tecnologie Informatiche

M. Mattiucci, R. Olivieri

ICT LAW – International Conference – Roma, 18 novembre 2006

Sintesi dell'intervento

La prima parte dell'intervento è stata dedicata alla presentazione del nuovo *Reparto Tecnologie Informatiche* che l'Arma dei Carabinieri ha recentemente attivato nell'ambito del RaCIS (Raggruppamento CC Investigazioni Scientifiche). Il RTI è prettamente dedicato alla formazione ed impiego di tecnici dell'Arma nel settore dei crimini ad alta tecnologia. La sua attività sul campo si esplica attraverso le indagini di laboratorio su sistemi digitali e nell'intervento informatico a supporto di investigatori e magistrati su quelle scene del crimine che risultino in condizioni critiche o particolarmente complesse dal punto di vista informatico o telematico.

Sia in relazione all'aggiornamento tecnico del personale che alla formazione dei nuovi specialisti il RTI si trova a collaborare, dal punto di vista della ricerca, con enti universitari, istituti di prestigio e ditte private. Fondamentale risulta l'inserimento del RTI (e del RaCIS in generale) nell'ENFSI (European Network of Forensic Science Institutes www.enfsi.org), rete di gabinetti scientifici che, in senso al workgroup per l'High Tech Crime, si scambia tool ed esercizi investigativi al fine di allineare le conoscenze e le metodologie.

La seconda parte dell'intervento si è quindi focalizzata sul *mobile forensics*, ossia su quella particolare branca forense che si occupa di studiare repertamento ed analisi di sistemi wireless. Si è premesso innanzitutto che lo studio sarebbe stato orientato solo sui sistemi cellulari GPRS ed UMTS (data la varietà dei sistemi wireless esistenti sul

commercio) e che non sarebbero stati considerati aspetti prettamente investigativi real time come *intercettazione* e *radiolocalizzazione*.

Il telefono cellulare è stato presentato come un sistema *embedded* ossia un sistema digitale dotato di microprocessore, memoria ed una serie di interfacce che a tutti gli effetti contiene gli elementi tipici di un computer se non fosse che lo scopo del sistema è predeterminato e ristretto quando lo si raffronta con sistemi *general purpose* quali i normali PC.

Nel cellulare vengono identificati i due elementi fondamentali: *SIM* e *terminale radiomobile*. Entrambi dotati di capacità elaborative e di memoria per cui soggetti al processo di analisi forense. In particolare, per il terminale radiomobile si hanno diverse informazioni quali:

- *Last Numbers dialled, Received & Missed.*
- *Phone book.*
- *IMEI, International Mobile Equipment Identity-Serial number.*
- *Fax's, Fax Journals, SMS Text Messages & Email.*
- *Audio recordings/memos and now MP3's*
- *Voice Mail (Held on Network).*
- *Map and position information.*
- *Images (pictures).*
- *Multimedia Messaging (MMS), Contain Images and Audio.*
- *Video.*
- *PDA Date, like reminders, calendar and documents.*

Mentre per la SIM:

- *Last Numbers Dialled (not really used these days).*
- *Phone book.*
- *IMSI, International Mobile System Identity, or the SIM Serial number, this identifies the subscriber.*
- *SMS Text Messages.*
- *Roaming Data, which countries the subscriber can make a call.*
- *New 3G SIM have the potential to store more data and applications.*
- *Location Area Code (LAC) the last paging area.*

I telefoni cellulari sono stati poi suddivisi in tre classi per comodità di studio:

- *Basic phone (SMS, voce);*
- *Advanced phone (+ EMS, SMS chat, WAP);*
- *High End phone (+ IM, MMS, POP, IMAP, SMTP, HTTP,...) + ...*
- *... + PDA = SMARTPHONE.*

In definitiva lo smartphone è “...un PDA che fornisce all’utente contemporaneamente alti servizi di telefonia cellulare, applicazioni PIM, gestione appuntamenti, contatti, documenti elettronici, ecc.”¹.

Volendo entrare nel mobile forensics è stato poi necessario evidenziare il parallelo con il *computer forensics*, settore ormai ampiamente studiato ed i cui risultati sono impiegati sul campo da anni. Le differenze che si determinano tra i due settori sono la ridotta dimensione dei sistemi mobili ma soprattutto le particolarità nella gestione dell’alimentazione elettrica, delle comunicazioni, delle memorie e delle applicazioni. I principi che si vogliono applicare sono invece gli stessi: *nessuna modifica ai dati durante l’analisi, controllabilità e documentazione delle attività di analisi, svolgimento di tali attività da parte esclusiva di personale specializzato*.

Il repertamento dei sistemi mobili è stato presentato assieme alle seguenti problematiche: mantenimento dell’alimentazione elettrica + isolamento radio dalle celle. A tale proposito sono state viste alcune soluzioni quali le *jamming device*, le *tende campali di Faraday* e le *valige autoalimentate per il repertamento*.

Riguardo invece l’analisi dei sistemi cellulari si è specificato che essa deve essere condotta separatamente su: memorie removibili eventualmente presenti, le SIM/USIM ed il terminale radiomobile. Quest’ultimo in assoluto è in grado di mantenere la maggior parte dei dati inerenti le comunicazioni digitali, per cui sono stati affrontati tre livelli di analisi possibili su di esso:

- (1) *non invasiva*: copia dei dati e ricostruzione mediante interfaccia specializzata, ottima per rilevare dati cancellati (es. SMS);
- (2) *semi-invasiva*: in camera schermata impiegando l’interfaccia del sistema mobile, sicura e veloce ma limitata riguardo la varietà dei dati estraibili;
- (3) *invasiva*: copia dei dati mediante estrazione fisica delle memorie, ottima e completa ma difficilmente ripetibile.

Al termine della conferenza è stato indicato il sito www.marcomattiucci.it come area web di riferimento in relazione agli argomenti trattati.

¹ R.Ayers, W.Jansen, N.Cilleros, R.Daniellou, (Oct 2005), “Computer Security – Cell Phone Forensic Tools: an overview and analysis”, NISTIR 7250, Computer Security Division, IT Laboratory, NIST, Gaithersburg, MD 20988-8930.