

IL DIGITAL FORENSICS E L'ARMA DEI CARABINIERI: SULLA SCENA DEL CRIMINE ED IN LABORATORIO

Gennaio 2010

Intervento del Magg. Marco Mattiucci

Sezione Telematica (Indagini Informatiche e Telematiche - Roma)

Reparto tecnologie Informatiche (Roma)

Raggruppamento Carabinieri Investigazioni Scientifiche (Roma)



ABSTRACT

La presentazione ha come obiettivo inquadrare la materia del Digital Forensics, sia sulla scena del crimine che in laboratorio, questo contestualmente alla presentazione del Reparto Tecnologie Informatiche dell'Arma dei Carabinieri e dei protocolli ed approcci posti in atto dall'Istituzione per garantire la massima affidabilità ed efficacia agli accertamenti tecnici in questo delicato, avveniristico e fondamentale settore.

TESTO ESPLICATIVO DELL'INTERVENTO

Alla crescente rilevanza dei fenomeni criminali di carattere informatico, le Forze di polizia hanno risposto in modo differenziato, mediante l'ampliamento e qualificazione dei compiti assegnati ai vari uffici e/o istituendo reparti specializzati nello specifico settore, così da ottenere un'adeguata attività di contrasto di questa emergente forma di criminalità, sia su Internet, sia nel mondo reale (personal computer, cellulari, software, ecc.).

Nell'Arma, oltre alla Sezione Telematica del Raggruppamento Operativo Speciale (Terrorismo e grandi organizzazioni criminali – istituita nel 2002 nell'ambito del Reparto Tecnico), che si occupa principalmente dei crimini informatici e delle intercettazioni digitali su Internet, è stato istituito (novembre 2006) - nell'ambito del Ra.C.I.S. - il Reparto Tecnologie Informatiche (che ha assorbito i compiti della Sezione Telematica del RIS di Roma, già operativa dal 2001).

Il predetto Reparto è strutturato su:

- una Sezione Telematica che si occupa di svolgere indagini tecnico scientifiche nei settori delle memorie di massa digitali, dei telefoni cellulari, di Internet e delle reti di computer nonché dei sistemi elettronici;
- una Sezione "Informatizzazione e Ricerca scientifica" che cura la ricerca scientifica inerente strumenti e metodologie per lo svolgimento delle indagini tecniche e tratta delle varie problematiche inerenti l'informatizzazione dei Reparti del Ra.C.I.S. nel rispetto della normativa concernente il trattamento dei dati personali, nonché le banche dati scientifiche.

Il Reparto Tecnologie Informatiche oltre all'attività di contrasto al "computer crime", cioè ai reati introdotti nel C.P. dalla legge 23 dicembre 1993, n. 547 ("Modifica ed integrazione alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica") che potrebbe definirsi compito eccezionale, riceve una notevole mole di richieste di indagini tecniche (IT) da parte dei reparti dell'Arma per accertamenti, anche di grande complessità, su memorie di massa, sui telefoni cellulari, sulle fotocamere digitali e su quant'altro di tecnologico, utilizzato dalla vittima o dall'autore di un reato, che come "reperto" deve essere sottoposto ad un'accurata analisi per scoprire elementi utili alle indagini (rif. la L. 48/2008 che ha recentemente modificato il Codice di Procedura Penale riguardo il reperimento delle fonti di prova da sistemi ad alta tecnologia).

In modo particolare quest'ultima attività tende costantemente ad aumentare, raddoppiando mediamente su base annua, in quanto non solo legata al numero di delitti su cui l'Arma indaga, ma soprattutto alla diffusione delle apparecchiature elettroniche ed alla presenza, in molte di queste, di componenti di memorizzazione di dati che hanno capacità sempre maggiore a fronte di un costo ormai alla portata di tutti.

Altra attività in crescita costante è quella relativa agli interventi sulla scena del crimine, richiesti dai reparti territoriali e speciali dell'Arma per le indagini più complesse (occorre ricordare la competenza della sezione telematica estesa su tutto il territorio nazionale).

Oggi l'accertamento tecnico non si limita alla sola estrazione del dato contenuto (ad es. in una scheda di memoria), ma si spinge anche a valutare l'informazione ed il suo significato (ad es. immagini pedo-pornografiche). Questa seconda attività che richiede tempi lunghi, conoscenza del caso e solo una semplice manualità nell'impiego dei programmi di visualizzazione, rimane generalmente a carico degli investigatori classici. Il RTI, invece, si occupa di rendere disponibili tali dati (anche magari recuperati da aree cancellate) per una pronta consultazione e navigazione da parte di personale non necessariamente tecnico.

Le aree del digital forensics che negli anni la Sezione Telematica del RTI ha approfondito e rese altamente operative sono, in sintesi, le seguenti:

- **COMPUTER FORENSICS:** le indagini tecniche si svolgono soprattutto su memorie di massa (hard disk, Usbkey, DVD, ecc.) isolate o facente parte di sistemi digitali computerizzati.
- **MOBILE FORENSICS:** indagini tecniche su cellulari, Personal Digital Assistance (palmari), ed altri sistemi di comunicazione digitali senza fili;
- **NETWORK FORENSICS:** le indagini tecniche si svolgono su reti di computer (LAN, WAN, ...) di tipo wired o wireless. Il sub-settore dell'Internet forensics è talmente rilevante a livello investigativo che spesso viene considerato come un settore a se stante nel digital forensics;
- **DEBIT&CREDIT CARD FRAUDS:** Sistemi di natura hardware che software che possono essere impiegati x frodi sulle carte plastificate di pagamento, siano esse di debito (es. pagobancomat), di credito e prepagate (es. moneta elettronica).
- **SOFTWARE FORENSICS:** analisi di originalità /alterazione del software, violazioni di copyright, identificazione ed analisi di software di intrusione, malware, virus, trojan, ecc.
- **ELECTRONIC (EMBEDDED SYSTEM) FORENSICS:** indagini tecniche sui sistemi elettronici speciali (inneschi a distanza, rilevatori, video-camere, ecc.).

Lo sforzo costante del Ra.C.I.S. e quindi di tutti i RIS e del RTI è elevare con continuità l'efficacia del servizio offerto e quindi studi e risorse sono stati orientati verso l'implementazione di un sistema per la qualità totale che regoli tutta l'attività di indagine tecnico-scientifico dell'Arma nei vari settori previsti (dattiloscopia, chimica, biologia, telematica, ecc.).

In particolare, la Sezione Telematica del RTI ha da anni abbracciato l'orientamento internazionale di seguire esclusivamente standard metodologici ben assestati e garantiti da istituti di provata esperienza, nonché di acquisire tool forense impiegati da centinaia di altre Forze di Polizia e Centri di ricerca.

La continua collaborazione con i laboratori di altre Forze di Polizia europee, americane e giapponesi concorre al perenne aggiornamento dei tecnici forensi del RTI ed i vari protocolli di intesa in atto consentono ai direttori di laboratorio di verificare con continuità efficacia e dispendiosità dei diversi metodi di gestione del forensics industriale (accertamenti tecnici a fini legali su larga scala).