Il *DIGITAL FORENSICS*: DAL COMPUTER AL CELLULARE, AD INTERNET FINO ALL'ELETTRONICA PURA

di Marco Mattiucci

Il *Digital Forensics* (DF) è una scienza di recente costituzione che è risultata pervasiva e trasversale rispetto alle altre discipline scientifico forensi. In questo lavoro introduttivo ci si pone lo scopo di percorrere in generale la strada del DF in Italia da 15 anni a questa parte evidenziando alcuni dei filoni di studio che ha aperto, le problematiche tecniche (risolte ed irrisolte) nonché gli aspetti teorici cui ha dato vita formalmente a livello accademico e legale, ciò ovviamente senza pretesa di esaustività.

Il digital forensics: definizione ed ambito italiano

Il DF si è sviluppato con ampio anticipo in zone quali il Nord Europa, il Nord America, il Giappone e l'Australia. Si può stimare, in base agli strumenti utilizzati e all'evoluzione dei corsi accademici attualmente presenti in Italia, che la nostra penisola segua l'*iter* di sviluppo della materia con almeno 6-8 anni di distanza rispetto a quanto accade in tali paesi. Una comparazione effettiva basata su metodi quantitativi non è completamente realizzabile a causa della natura "anche legale" e non solo tecnica del DF. La definizione ad oggi maggiormente accettata ed aggiornata a livello internazionale è la seguente: "…*the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions*…" (IFIP ACT 306 - 2009). Tale definizione va però contestualizzata al nostro codice di procedura penale ed alla realtà operativa della polizia giudiziaria, questo soprattutto per chiarificare quale sia la situazione in Italia a riguardo di questo delicato settore.

Sembra ovvio che si debbano impiegare "metodi scientificamente derivati" per svolgere esami di apparecchiature elettroniche digitali, ma per anni (e forse molte volte ancora oggi) l'esperienza del consulente tecnico o perito ha sostituito l'applicazione pedissequa di metodologie rigorose trascritte su documenti ufficiali. A chi vuole entrare nel mondo professionale del DF e chiede (giustamente) quale siano le procedure ufficiali del DF da seguire nel repertamento ed analisi dei reperti, si può rispondere che in Italia non ne esistono di ufficiali, quindi stabilire quale metodo sia scientificamente derivato o meno è a carico della capacità del consulente tecnico.

La situazione peggiora quando il discorso si allarga poi ai "metodi provati" ossia soggetti a *test* puntuali ed esaustivi, definiti formalmente da una commissione. Più studi del NIST (*National Institute of Standards and Technology*) hanno purtroppo dimostrato la quasi impossibilità di testare esaustivamente metodi e strumenti per le indagini tecniche elettronico/digitali. Questo non toglie però che il NIST stesso abbia emanato decine di documenti ufficiali sulle prove fatte che dovrebbero sempre essere impiegate come riferimento dagli specialisti nel settore.

Di seguito si vanno ad analizzare i principali filoni tecnici cui storicamente il DF ha dato origine, al fine di creare un'immagine più dettagliata della materia, delle sue problematiche e dei suoi risultati.

❶ *Computer Forensics (CF)*

Il macro settore di maggior rilievo del *digital forensics* è il CF, che internazionalmente muove i primi passi, segnalati accademicamente con articoli ufficiali, nel periodo 1985-87. Si trattava del recupero di un *file* di *data base* opportunamente o inavvertitamente cancellato a livello di *file system*. In Italia le prime attività di alto profilo nel settore risalgono al periodo 1990-95 e coinvolgono sostanzialmente lo stesso tipo di attività tecnica prima citata, ossia il *data recovery*. Il recupero di dati cancellati logicamente e/o la loro ristrutturazione da frammenti sparsi diviene un obiettivo determinante in quegli anni, tanto che oggi il *data recovery* è un settore a se stante ed una notevole fetta del *business IT* di nicchia. Ben presto si notò che era necessario separare il *data recovery* dal *forensic data recovery,* per le garanzie da dare agli indagati, e ciò ha determinato il fiorire di svariate *best practices* nei periodi iniziali. Dato che il CF si concentrava sulla singola macchina, *post mortem* ed in condizioni controllate di laboratorio, furono stabilite delle procedure ineccepibili alla ricerca di quella che sembrava la definizione perfetta della materia. L'evolvere dei sistemi ha ovviamente dato torto a tutto questo. I *file system* sempre più complessi hanno reso praticamente impossibile svolgere il *data recovery* senza l'intervento di *tool* specialistici molto complessi (si pensi che le prime attività di *recovery* venivano effettuate sostanzialmente "a mano" dall'esperto, il quale ispezionava direttamente il contenuto esadecimale della memoria di massa). L'attuale impiego delle macchine soprattutto in rete e su Internet ha poi cambiato totalmente l'approccio all'analisi dei contenuti della memoria, generando la differenza tra *live* e *dead forensics*. Per chiarificare, sebbene il *forensics* rimanga attività *post mortem,* intendendo con ciò "dopo il fatto" (nel caso penale dopo il reato), esso può svilupparsi mentre la macchina è ancora operativa (a breve distanza temporale dal fatto, nell'ipotesi che non sia stata spenta – *live forensics*) o quando la stessa sia stata spenta e

repertata fisicamente (*dead forensics*). I settori di studio che ne sono venuti fuori sono sostanzialmente diversi tra loro sia in termini di strumenti impiegati che di teorie e condizioni di lavoro di cui tener conto. La più attuale spinta alla ricerca nel CF è poi venuta dalle tecniche di virtualizzazione in cui interi elaboratori vengono incapsulati in *file,* assieme sia ai loro dati che alle loro elaborazioni anche temporanee.

❷ *Network & Internet Forensics (NF)*

Dal 1993/95 inizia l'esplosione dei casi di pedopornografia e per quanto possa sembrare assurdo pornografia e pedopornografia costituiranno una spinta commerciale senza pari per lo sviluppo di Internet. Non tutti sanno che, purtroppo, la quantità di materiale pedo e porno su Internet è una fetta percentuale molto alta del totale, ma ancora meno sanno che una delle principali spinte all'ampliamento delle bande di trasmissione e quindi alla velocizzazione delle connessioni è stato proprio il mercato porno. Sono partite quindi anche in Italia le prime attività di indagine su Internet e sulle reti di computer. Dal 1997 al 2000 le unità delle Forze di Polizia dedite all'indagine telematica sono state rafforzate ed hanno iniziato ad acquisire una loro forte identità. Si tratta sempre di attività *post mortem* ma questa volta inevitabilmente *live* in quanto la rete è una entità distribuita (formata da più parti geograficamente distanti e generalmente indipendenti) e tempo-variante. Le prime attività di indagine si appoggiavano fortemente al CF e, quindi, ci si limitava ad usare la rete per individuare i "*peer*" responsabili di attività illegali per poi intervenire fisicamente e prelevare/analizzare le singole macchine. Negli anni la stessa Internet è divenuta un mezzo per supportare comunicazioni di profilo più alto (es. *subnet cripto*, P2P, *social networks*, VoIP, ecc.) ed il concetto di indagine tecnica tradizionale sulla rete ha subito un enorme stravolgimento. La frontiera attuale è l'indagine sui "*cloud system*" ossia su sistemi che risultano dalla virtualizzazione di intere federazioni di *server* collegati tra loro indipendentemente dalla posizione geografica e dalla tipologia, cosa che rende praticamente irrealizzabile l'identificazione degli autori delle azioni.

❸ *Mobile Forensics (MF)*

L'anno 2000 vede l'inizio della crescita inarrestabile della proliferazione e pervasività dei sistemi mobili in Italia. Dal dimenticato ETACS ai digitali GSM, GPRS, UMTS ed alle loro varie evoluzioni, il mercato dei cellulari ha visto il nostro paese come uno dei fulcri a livello mondiale. La corsa all'arricchimento delle funzioni e dei servizi ha spinto a miscelare i concetti di cellulare, modem e personal computer determinando l'attuale concetto di *smartphone*. Le ridotte dimensioni e la risultante portabilità di questi sistemi, nonché l'enormità delle loro funzioni e l'integrazione con i computer e le reti attuali determina in essi un *target* fondamentale nelle indagini di polizia giudiziaria. È ben noto agli investigatori che nulla fornisce informazioni di valore come uno *smartphone*. Il MF è diviso in tre aree di studio: ***SIM forensics***, settore che è totalmente esplorato ed i cui risultati sono deterministici; ***Handset forensics***, differente a seconda della casa produttrice che si considera e quindi non deterministico in linea generale nei risultati; ***Removable Media forensics***, riconducibile al CF applicato alle memorie ausiliarie che è possibile inserire nell'*handset* (settore anch'esso ampiamente studiato). Allo stato attuale il MF vede nell'iPhone e nei sistemi Android la punta dell'impegno di ricerca e studio, ciò per quanto riguarda gli *smartphone*. Al contrario si vede anche un problema tecnico importante nell'affrontare l'analisi di cellulari a limitate funzionalità e scarsa memoria, costruiti secondo canoni non *standard* proprio allo scopo di non lasciare tracce (*basic phone*).

❹ *Embedded System Forensics o Electronic Forensics (EF)*

Accanto ai sistemi di elaborazioni standard, come computer e cellulari, si sono affiancati negli ultimi 10 anni sistemi elettronici che potevano avere una rilevante importanza investigativa, sebbene non seguissero schemi di realizzazione noti e non fossero classificabili unicamente come computer, cellulari o reti. I primi casi hanno riguardato sistemi di innesco di esplosivi, come ad es. gli attuatori elettronici basati su cellulari modificati. Numerosi altri casi hanno poi interessato il settore delle clonazioni e delle frodi, tramite carte di credito (sistemi di *skimming*). Più recentemente si è iniziato a parlare di ***black box forensics*** sia in relazione a scatole nere di velivoli che di auto. Si è quindi pervenuti alla necessità di analizzare Xbox, iPod, iPad, ecc. determinando una miriade di micro settori del DF che necessitano di una enorme specializzazione e di strumentazione sofisticata e molto costosa. La frontiera del EF è nel *chip removal*, ossia nella possibilità di estrarre direttamente i *chip* di memoria da qualsiasi sistema elettronico digitale, per poi leggerne ed interpretarne il contenuto e poter così recuperare grandi quantità di dati anche non più evidenti.

Conclusioni

Il DF è una materia molto complessa e variegata che coinvolge direttamente l'informatica, l'elettronica ed il codice di procedura penale e vede i suoi *target* fondamentali nel CF (memorie di massa di computer), NF (reti ed Internet), MF (cellulari) e EF (sistemi elettronici speciali). Oltre alle attività di frontiera già citate, è bene sottolineare alcune attività di ricerca che hanno prodotto negli ultimi anni importanti risultati anche dal punto di vista investigativo: la ricostruzione di memorie danneggiate (soggette a fuoco, liquidi, agenti meccanici, ecc.), le indagini *live* sui cellulari (intercettazione telematica, radiolocalizzazione, ecc.) ed il *cracking*, ossia le tecniche di attacco delle protezioni *cripto software* ed *hardware* dei sistemi digitali. L'evidente multidisciplinarietà ed ampiezza del DF trova poi un esatto corrispondente nella sua velocità di evoluzione, la quale impone un incessante aggiornamento tecnico. ©