Editoriale

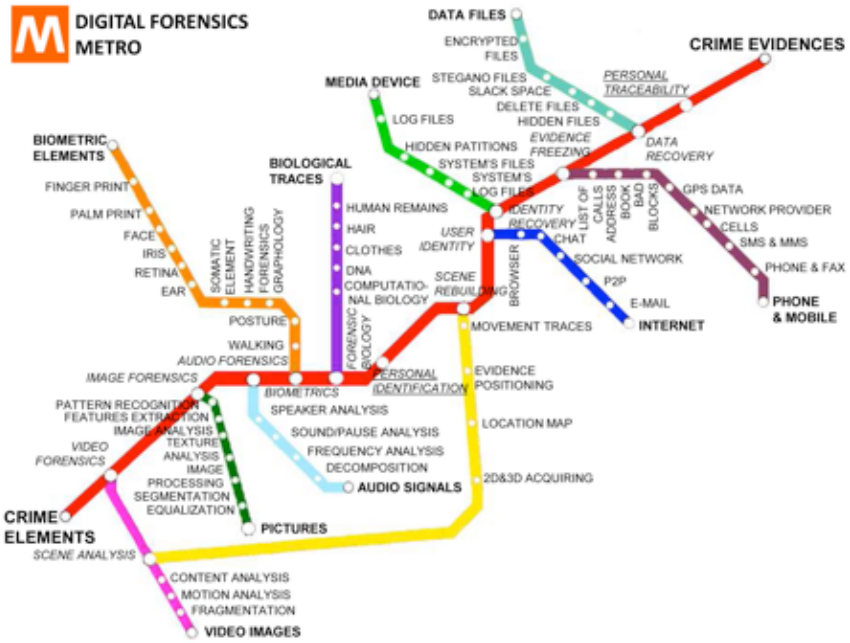
La Digital Forensics - Il metodo scientifico delle IT nelle attività investigative

Nelle attività investigative sono in crescente aumento le applicazioni di tecniche informatiche sempre più sofisticate finalizzate a supportare il compito di esperti impegnati nella ricerca della verità in vicende criminose il cui responsabile è spesso ignaro di lasciare tracce della sua presenza o della sua identità. A maggior ragione tali tecniche si applicano ai crimini informatici, ovvero a quei reati che si compiono mediante lo stesso mezzo informatico e vengono facilitati dall'uso di tutte le possibilità offerte dalla rete, ove è diventato sempre più praticabile il furto di identità e la frode di informazione. Infatti, la scala globale di diffusione delle informazioni fornisce l'occasione di incrementare i reati informatici. mettendo ovviamente in crisi preoccupante la tutela della privacy di tutti gli utenti. Oggi gli attuali terminali di comunicazione, dai computer ai cellulari, dagli ATM (Bancomat) al Telepass, si affacciano su una stessa grande rete, ma entrando in Internet, le informazioni che ogni navigatore lascia sono sufficienti per far catturare la sua identità, e non tutti sembrano essere consapevoli di questo rischio. Inoltre, il crescente uso delle TIC (tecnologie dell'informazione e della comunicazione) nelle diverse organizzazioni crea spesso la necessità di cercare la "prova del computer" (o "computer evidence"), composta da tracce lasciate in sistemi o programmi applicativi e accesso a banche dati, in modo da consentire attività investigative di diversa natura, sia all'interno delle imprese sia in ambito forense. Esistono, perciò, diversi tipi di indagini:

- *interne alle società, anche per valutare danni arrecati;*
- *per scoprire atti di spionaggio, terrorismo e frodi di diversa natura;*
- *per evidenziare violazioni dei diritti di accesso;*
- *scoprire le finalità di inoltro di posta malevola (spam e phishing);*
- *a sostegno di un pubblico ministero o della polizia investigativa;*
- *a supporto di indagati e imputati (consulenze tecniche di parte).*

Per poter procedere ad analisi valutative utili e ripetibili, è necessario esaminare reperti costituiti da elementi certi, che possono essere ottenuti mediante il "congelamento" della prova. In altri termini questi elementi non devono essere degradati da passaggi impropri ma soprattutto non devono perdere i riferimenti temporali e in certi casi anche spaziali (in informatica lo spazio è costituito dalla allocazione delle risorse, che possono essere fisiche e logiche).
Affinchè le prove di abusi o reati, a cui dare seguito con un'azione disciplinare o l'apertura di un procedimento civile o penale, siano utilizzabili è necessario che soddisfino criteri di conformità. Le prove raccolte con metodi tradizionali non sempre sono sufficienti a garantire la loro ammissibilità nei procedimenti giudiziari. Si evidenzia, quindi, la necessità di un nuovo approccio per garantire la corretta raccolta delle prove che corrisponde a verifiche di accettabilità, autenticità, completezza e affidabilità. L'esperto di computer-forensics, per offrire la sua opera nella computer-crime (criminalità informatica), è solito preservare, individuare, indagare e analizzare il contenuto memorizzato in qualsiasi supporto o dispositivo di memoria. Tuttavia, queste attività devono essere rivolte non solo ai diversi tipi di computer, ma a qualsiasi apparato elettronico dotato di memoria per archiviare dati. Considerata l'eterogeneità di questi dispositivi all'esperto è richiesto un più ampio spettro di competenze dall'acquisizione delle prove digitali (applicando algoritmi di hash crittografici) all'analisi dei file system, applicazioni e dati (documenti, immagini, e-mail, sms, mms, etc), dall'audio-forensics (trascrizione testuale di una conversazione, estrazione delle formanti per l'analisi parametrica a fini comparativi) alla video-forensics (estrazione di caratteristiche presenti in singole immagini e in sequenze di immagini), dall'analisi di impronte digitali (mediante AFIS) alla identificazione personale mediante confronto di voci e volti (analisi comparativa, sovrapposizione parametrizzata, valutazione del grado di compatibilità), da tecniche e strumenti di intercettazione dei flussi di comunicazione alla tracciabilità personale (mediante dispositivi mobili), dal confronto tra sequenze di DNA alla ricostruzione della scena del crimine e all'analisi dei comportamenti (firma, voce, movimenti).
Per meglio comprendere la complessa interazione tra i diversi settori propri delle tecnologie informatiche e le necessità evidenziate nell'ambito delle attività investigative si è ritenuto utile descrivere questo complesso scenario attraverso la seguente metafora del Metrò:

Scenario della Digital Forensics e dei necessari contributi delle TIC



Molti sono, quindi, i reati che possono usufruire delle tecnologie informatiche e fare ricorso alle diverse tecniche di analisi basate su metodi informatici dalla computer-graphics alla video analisi, dall'audio analisi ai confronti biometrici, dall'information-retrival al data-mining, tutte finalizzate a trasformare gli elementi del crimine, i "reperti", in evidenze del crimine, le "prove", attraverso la identificazione o la tracciabilità personale, poiché tutto deve portare al responsabile di un atto criminoso. Perciò, al fine di acquisire la prova legittima da un computer o desktop o laptop o smartphone o tablet, da un server o un gestore di telefonia o un impianto di videosorveglianza o da programmi che vengono eseguiti all'interno di questi sistemi, all'esperto in digital-forensics si richiede di:

- *acquisire una prova tempestivamente, prima che venga alterata o rimossa;*
- *definire la catena di custodia dei reperti da sottoporre a scansione;*
- *bloccare in scrittura i dispositivi per la protezione dei vari supporti (dati, audio, video);*
- *assicurarsi che i dati originali non possano essere alterati;*
- *eseguire l'hash del supporto originale (firma digitale con riferimento temporale);*
- *copiare bit a bit il flusso di informazioni su altro supporto;*
- *verificare l'hash della copia con l'hash originale;*
- *utilizzare tecniche e strumenti per garantire la ripetibilità del controllo;*
- *garantire la conservazione e l'accesso nel tempo.*

Ovviamente è necessario non ignorare l'alta volatilità delle evidenze in rete, poiché in Internet una informazione può durare un tempo molto breve, trovarsi in un qualunque punto del globo, e perciò può essere facilmente alterata, rimossa, sovrascritta o spostata in altro sito connesso.

Occorrono, quindi, competenze variegate e specifiche sia in ambito legale sia in settori squisitamente tecnici al fine di cercare la "prova" del reato o dell'illecito. I contributi di questo numero speciale di Mondo Digitale, scaturiti da alcune sessioni di Congressi Nazionali AICA (Roma 2009, Salerno 2013) e dal Workshop IT-STAR (Bari 2013), possono far comprendere la grande importanza dell'informatica nelle attività investigative e forensi. Attraverso questo insieme di saperi si è voluto prendere in considerazione alcuni aspetti frequenti dell'analisi forense, in modo da evidenziare tecniche e metodi informatici che caratterizzando la Digital Forensics, una scienza molto ampia che copre settori ancora più complessi rispetto alla Computer Forensics.

Giuseppe Mastronardi

Dipartimento di Ingegneria Elettrica e dell'Informazione

Politecnico di Bari