ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

Computer Forensic e investigazioni informatiche

Nicola Chemello, David D'Agostini, Antonio Piva

1. Introduzione

La tecnologia sviluppatasi negli ultimi anni ha portato a un notevole incremento delle fonti di prova a disposizione degli investigatori, ora sempre più derivanti dai nuovi strumenti di comunicazione disponibili. Indagini su impronte digitali, su tracce di scarpe o di pneumatici, sulla composizione del suolo rinvenuto sul luogo del delitto, sono procedure che negli anni sono entrate nella conoscenza comune, grazie anche a famose serie TV.

Oggi si potrebbe addirittura affermare che non esiste più reato che non utilizzi, direttamente o indirettamente, un dispositivo elettronico; basti pensare al telefono cellulare, sempre più connesso a internet anche attraverso reti senza fili: sono attivi circa 152 *mobile phone contracts* (contratti per telefonia mobile) ogni 100 abitanti[1].

Le indagini penali si stanno indirizzando sempre più verso i dispositivi digitali (computer, telefoni cellulari, GPS): facendo riferimento ai tabulati telefonici, alle informazioni memorizzate dalle microcelle per l'accesso alla rete di telefonia mobile GSM e agli eventuali dati memorizzati su questi dispositivi, è possibile stabilire, con discreta sicurezza, la correlazione tra il fatto accaduto e l'utilizzatore del dispositivo.

Più un dispositivo è ricco di funzionalità, più sarà in grado di memorizzare le azioni intraprese durante una normale giornata lavorativa, la sveglia impostata sul cellulare offre la possibilità di mettere in relazione particolari eventi accaduti, il percorso memorizzato sulla cronologia del navigatore dell'automobile delineerà, in maniera inequivocabile, i chilometri percorsi; le macchine fotografiche digitali, anch'esse con funzioni GPS legano ogni immagine a un determinato luogo; il programma di fitness sul cellulare tiene traccia sia delle calorie bruciate, che delle abitudini dell'utilizzatore; il computer e le reti memorizzano molti più dati di quanto si possa immaginare e rendono difficili la loro definitiva cancellazione (riquadro 1).

Recuperare le informazioni memorizzate su un computer o un dispositivo elettronico è un compito possibile, non sempre semplice, ma sicuramente molto utile per poter valutare la commissione di un reato ovvero per verificare un alibi. Esempi più specifici possono riguardare la correlazione di informazioni memorizzate nella RAM di un telefono, con un evento quale una rapina, uno scambio di messaggi via mail o sms, un accesso a un server remoto per cancellare dei dati scomodi. In particolare se i reati

Riquadro 1

"I dispositivi digitali memorizzano molti più dati di quanto si possa immaginare e rendono difficile la loro cancellazione. La sfida dell'investigatore forense consiste nella loro ricerca".

[1] Fonte Eurostat: ec.europa.eu/eurostat

vengono commessi utilizzando le nuove tecnologie, anche il loro accertamento dovrà inevitabilmente impiegare metodi, tecniche e strumenti idonei; ad esempio nel caso di diffamazione tramite Internet si rivela essenziale acquisire informazioni sulla connessione telematica attraverso i relativi file di log. Questi, e molti altri, sono alcuni degli ambiti di un'indagine forense su dispositivi elettronici.

2. Digital Forensic

La *Digital* o *Computer Forensic* prevede l'utilizzo delle tecnologie appropriate, in modo complementare con le metodologie di indagine tradizionali, allo scopo di individuare i responsabili degli illeciti. Il *Digital Forensic* è anche l'insieme delle attività, tecniche, procedure di indagine diretta all'analisi e alla soluzione dei casi legati alla criminalità informatica. Si tratta di una disciplina che si occupa dell'individuazione, della conservazione e protezione, della ricerca ed estrazione, della documentazione e di qualsiasi forma di trattamento del dato informatico per essere utilizzato in un'indagine e in un procedimento giudiziario.
L'Informatica Forense viene utilizzata ai fini probatori e richiede l'impiego di tecniche, strumenti e procedure per l'esame metodologico dei sistemi informatici.
Dalla nascita, circa 30 anni fa, per opera dei laboratori dell'FBI, la *Digital Forencic* ha avuto grande diffusione inizialmente negli Stati Uniti, e successivamente anche in Italia, in particolare a causa dell'aumento dei crimini informatici e conseguente presa di coscienza da parte di aziende, cittadini, consumatori e utenti della rete che hanno finalmente cominciato a denunciare i crimini dei quali sono vittime.
Il mondo delle investigazioni digitali è stato recentemente aggiornato da numerosi articoli di legge; la ratifica della convenzione di Budapest (Convenzione del Consiglio d'Europa di Budapest sulla criminalità informatica del 23 novembre 2001), avvenuta con la legge n.48 del 18 Marzo 2008, ha apportato importanti procedure e novità riguardanti i reati informatici al fine di poter trattare, in maniera congrua alla loro natura, i dati digitali.
Attraverso la Convenzione di Budapest e alcune normative italiane come la legge 23 dicembre 1993 n.547 riguardante il tema della criminalità informatica[2], sono stati introdotti nel nostro ordinamento giuridico il *danneggiamento informatico e l'accesso abusivo a un sistema informatico o telematico* (*artt.* 615 *quinquies*, 635 *bis*, 635 *ter*, 635 *quater*, 635 *quinquies* c.p.) la perquisizione informatica (*art.* 352 *c.p.p.*), modifiche del codice di cui al d.lgs. 30 giugno 2003 n.196 (noto come codice della Privacy), l'istituzione del fondo per il contrasto della pedopornografia su Internet e per la protezione delle infrastrutture informatiche di interesse nazionale.
La citata Convenzione di Budapest ha fornito una definizione unitaria delle infrazioni penali commesse contro o tramite le reti informatiche che possono essere suddivise in quattro gruppi:
- infrazioni riguardanti la riservatezza, l'integrità e disponibilità dei dati o dei sistemi informatici, per garantire la tutela delle comunicazioni elettroniche e delle informazioni contenute;
- infrazioni informatiche, come le frodi o falsi in ambiente elettronico;
- infrazioni relative ai contenuti, quali pornografia infantile;
- infrazioni contro i diritti d'autore come copie illegali protette dai diritti di proprietà intellettuali.

Con la Convenzione di Budapest è stato possibile apportare importanti modifiche al codice di procedura penale al fine di poter trattare, in maniera congrua alla loro natura, i dati informatici.
Di seguito vengono riportati alcuni degli articoli introdotti nel codice penale nel marzo 2008, che hanno diretta rilevanza per l'informatica forense:
- Art. 244 [...] l'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica (artt. 359-364), anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.
- Art. 247 1-bis: quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.
- Art. 260 al comma 2 è aggiunto il seguente periodo: quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere rea-

[2] Chiamata anche legge sui *Computer Crime*.

lizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria.
Risulta chiaro che la suscettibilità all'alterazione di molti dispositivi o supporti informatici sia il fulcro di una qualsiasi procedura di acquisizione o analisi dei dati digitali. Solo il rispetto delle procedure e specifiche norme può garantire lo svolgimento di un'adeguata perizia. Il recupero delle informazioni costituisce una delle sfide che quotidianamente le forze dell'ordine sono chiamate a vincere. A differenza delle normali prove di reato, i dati digitali sono per natura suscettibili di modifica, e persino la visualizzazione di un singolo file, se non eseguita con la dovuta cura, ne altera alcune caratteristiche fondamentali, rendendo contestabile l'analisi effettuata.
Le investigazioni digitali possono fornire la risposta, attraverso le prove, di dove o con chi era un indagato in un determinato intervallo di tempo, che tipo di file sono stati scambiati attraverso un particolare computer, con che modalità, dove e quando, è stato effettuato un accesso ad una risorsa in Internet.
La *digital forensic* è, pertanto, la scienza che analizza, secondo le modalità previste dalla legge, i dispositivi digitali al fine di portare in giudizio le informazioni recuperate.

3. Dati digitali contro dati cartacei o analogici

Anche se di primo acchito sembra compito più semplice il recupero di dati digitali, rispetto al rilevamento di un'impronta digitale, bisogna fare molta attenzione a non improvvisarsi investigatori, per non correre il rischio di inquinare le prove ed ottenere informazioni certe. Una formazione universitaria specifica, competenze adeguate e una o più certificazioni, sono necessarie per operare con efficacia nell'acquisizione di reperti così facilmente deperibili.
Non è ben chiaro se oggi sia più semplice ritrovare un foglietto o un documento cartaceo contenente delle frasi compromettenti oppure rinvenire la sua forma digitalizzata. Per quanto riguarda le informazioni cartacee la difficoltà di recuperare le informazioni può dipendere dal grado di conoscenza e attenzione di chi vuole nascondere tale documento: una persona inesperta potrebbe strapparlo e cestinarlo, senza considerare tutti i metodi per una distruzione efficace. Allo stesso modo vi sono diverse modalità per la cancellazione dei file da un computer, ma bisogna tenere ben presente che è molto più sicuro agire su ciò che si conosce a fondo piuttosto che su ciò che si presume di conoscere: pensando di saper cancellare i dati, magari utilizzando uno dei tanti software sul mercato, si lascerebbero evidenti tracce sia della cancellazione, sia di file e delle informazioni che si volevano cancellare[3].
Le parole scritte sul pezzo di carta, una volta ricucito lo strappo, possono essere lette abbastanza agevolmente. La struttura di un *filesystem* rende la semplice lettura delle stesse parole decisamente più complicata: l'organizzazione delle informazioni dipende dal dispositivo, dal suo sistema operativo, dalle scelte del suo progettista e sviluppatore spinto da motivazioni che solitamente non riguardano il recupero di dati per un giudizio. Spesso l'esperto è in grado di recuperare informazioni utili per le indagini forensi.
Un altro aspetto da considerare, è il tipo di informazioni che un dispositivo memorizza: in un navigatore GPS non si andranno a ricercare documenti di videoscrittura, ma solamente informazioni riguardanti la latitudine e la longitudine; altresì potrebbe essere interessante ed utile controllare anche con quali dispositivi è stato messo in comunicazione, per esempio con un computer piuttosto che con un telefono cellulare, per utilizzarne la funzionalità di vivavoce.
Oggi, sempre più spesso, azioni compiute con modalità tradizionali e senza l'ausilio di mezzi elettronici sono comunque soggette a investigazioni digitali, basti pensare agli innumerevoli dispositivi di videosorveglianza presenti sul territorio, alla posizione dell'automobile o cellulare con GPS. Altre azioni compiute con l'ausilio dei moderni mezzi di comunicazione, dallo spionaggio industriale, alla diffamazione *on line* posta in essere tramite un *blog* o *social network*, alla frode, truf-

[3] Nel caso sia installato un sistema operativo utilizzante *filesystem* NTFS, le posizioni dei file sono indicate in una particolare tabella chiamata *Master File Table* (MFT) che contiene il collegamento base ad ogni file e ad ogni cartella memorizzata. Il record associato nella tabella MFT viene segnato come *cancellato* e il *filesystem* renderà lo spazio libero (ma eliminando non vengono cancellati i byte con cui era composto il file). Apposite procedure e strumenti adeguati riescono quindi a recuperare questo file *pseudo cancellato*.

fa o furto commesso attraverso Internet[4], al trattamento illecito dei dati, all'accesso abusivo ai calcolatori, vengono altresì trattati dal *computer forensic examiner*[5] con metodologie adeguate al compito che deve svolgere. Esempi concreti, analizzati in maniera oggettiva, possono essere i log di un webserver oggetto di attacco informatico, tabulati telefonici di una particolare microcella, SMS cancellati inviati per mezzo di un telefono cellulare, verifica dell'esistenza di una determinata foto o informazione all'interno di un hard disk, accessi alla rete mediante l'uso di pseudonimi in apparenza anonimi o accessi effettuati attraverso account presunti tali.

4. Procedure generali per la raccolta probatoria, procedimenti ripetibili e irripetibili, analisi dei dati ed i sistemi di analisi

La disciplina della *computer forensic* si articola in diverse categorie:

- *computer media analysis* (verifica dei supporti di memorizzazione dei dati, delle periferiche ecc.);
- *imagery, audio and video enhancement* (verifica di immagini, audio, video generati dal computer);
- *data base visualization* (verifica delle basi di dati);
- *network and Internet control* (verifica della attività svolte in reti pubbliche o private).

Considerati i presupposti giuridici sopra delineati, si evince come un computer *forensic examiner* debba garantire un insieme di metodologie e procedure adeguate al compito che deve svolgere.
La natura dei dati digitali è suscettibile a facile modifica, pertanto l'investigatore ha la necessità di preservare il dato digitale così com'è, eliminando la possibilità di alterazione.
La semplice accensione di un sistema operativo, nella maggioranza dei casi, modifica alcuni dati memorizzati nel computer, con conseguente alterazione dei parametri di ultima modifica di taluni file. Tali alterazioni dell'originale possono, in sede di giudizio, far sì che le prove digitali non siano valutate come oggettive, screditando altresì l'operato del tecnico investigatore.
L'organizzazione della raccolta delle informazioni digitali atte a fornire prove oggettive prevede l'utilizzo di adeguati e certificati dispositivi che impediscano la scrittura, volontaria o meno, sui reperti oggetto di analisi. Pertanto, durante un'acquisizione forense, devono essere utilizzati i cd. *writeblock*, che impediscono tramite procedure software o mediante hardware, la scrittura sul dispositivo collegato per la duplicazione. Il processo di analisi forense, posto in essere su dati digitali, viene riassunto nella figura 1.

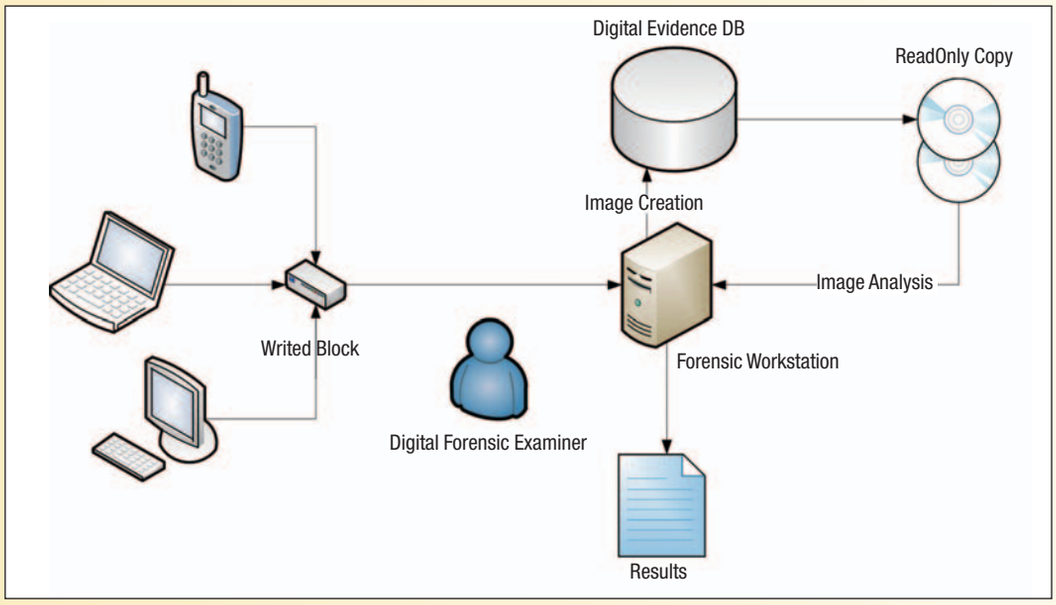

FIGURA 1
Processo di analisi forense su dati e dispositivi digitali

[4] Si pensi al *Phishing*, argomento trattato nell'articolo pubblicato in Mondo Digitale, n. 4, dicembre 2006.

[5] L'investigatore forense che si occupa di dispositivi digitali.

I dispositivi da analizzare, riportati sulla sinistra, vengono collegati, mediante apposito dispositivo, al computer adibito alla duplicazione e successiva analisi[6]. Un dispositivo *writeblock* esegue esattamente quello che il nome denota: blocca la possibilità di scrittura, quindi elimina la possibilità di modifica o alterazione dei file. Successivamente l'investigatore forense procede con la duplicazione integrale dei supporti, creando l'immagine forense memorizzata in apposita locazione di memoria (*Digital Evidence* DB), sottoposta preventivamente a processo di *disk sanitization*[7]. Al termine di questo processo, dopo verifica dei dati scritti, l'immagine viene trasferita su supporti ottici non riscrivibili. Solo dopo aver eseguito questi passaggi è possibile iniziare con l'analisi dei dati.

Questo tipo di dispositivi è fondamentale quando si deve operare nell'ambito di un procedimento che deve essere ripetibile (in altre parole, attuando le medesime procedure sugli stessi originali, si devono ottenere identici risultati). La ripetibilità delle azioni, in ambito forense, è di fondamentale importanza. Anche se non è una norma prescritta, l'utilizzo dei *writeblocker* è da consigliarsi non solo durante il processo di acquisizione, ma anche nel processo di analisi, per preservare il "nuovo originale" creato dalla duplicazione del reperto (riquadro 2).

L'effettuazione di un accertamento tecnico ripetibile non è però sempre possibile, in quanto in determinate occasioni può risultare necessario, al fine di recuperare le informazioni ricercate, alterare in maniera permanente un supporto; in tal caso, come disposto dall'art. 360[8] c.p.p, si utilizzano i procedimenti irripetibili.

Riquadro 2

La forza di un investigatore forense è la sua capacità di rispondere ai quesiti posti, garantendo oggettività e ripetibilità delle operazioni intraprese. Non importa il tipo di strumento utilizzato, ma è di fondamentale importanza esser certi del suo funzionamento.

Un tipico caso riguarda l'ispezione informatica di uno spazio virtuale: accedendo a una casella di posta su web vengono modificati tutti i log relativi all'ultimo accesso, compresi i riferimenti all'ultimo indirizzo IP da cui ci si è collegati. In queste particolari circostanze, come previsto dal sopra citato articolo 360 c.p.p., in ottemperanza a un fondamentale principio di garanzia e difesa, è necessario che siano invitate le parti e gli avvocati, che possono presenziare alle operazioni peritali con i propri eventuali consulenti.

Solo dopo aver creato l'immagine forense, è possibile iniziare il processo di analisi, inteso come la ricerca delle informazioni interessanti ai fini del particolare procedimento. Per quanto riguarda la fondamentale attività formale di analisi forense, è bene sottolineare che non esiste una procedura prestabilita per legge, in quanto non ci si può porre davanti un reperto sempre con lo stesso *modus procedendi*, sia per la natura del dispositivo, sia per il tipo di informazioni contenute. Pertanto si dovrà agire in maniera

---

6 In caso di dispositivi *writeblock* sofisticati, la copia forense viene eseguita direttamente da questi, senza la necessità di *workstation* forense. Nulla vieta che siano predisposte più postazioni, ognuna adibita a specifico compito (per esempio una macchina esegue le duplicazioni, mentre una seconda è utilizzata per l'analisi).

7 Processo che prevede la cancellazione in maniera sicura dei dispositivi di destinazione dell'immagine, al fine di evitare contaminazione e/o alterazione dei file creati.

8 Art.360 - Accertamenti tecnici non ripetibili (codice procedura penale).

1. Quando gli accertamenti previsti dall'art. 359 riguardano persone, cose o luoghi il cui stato è soggetto a modificazione (116, 117 att.), il pubblico ministero avvisa, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici (233).

2. Si applicano le disposizioni dell'art. 364 comma 2.

3. I difensori nonché i consulenti tecnici eventualmente nominati hanno diritto di assistere al conferimento dell'incarico, di partecipare agli accertamenti e di formulare osservazioni e riserve.

4. Qualora, prima del conferimento dell'incarico, la persona sottoposta alle indagini formuli riserva di promuovere incidente probatorio (392 s.), il pubblico ministero dispone che non si proceda agli accertamenti salvo che questi, se differiti, non possano più essere utilmente compiuti.

5. Se il pubblico ministero, nonostante l'espressa riserva formulata dalla persona sottoposta alle indagini e pur non sussistendo le condizioni indicate nell'ultima parte del comma 4, ha ugualmente disposto di procedere agli accertamenti, i relativi risultati non possono essere utilizzati nel dibattimento.

differente nel caso si cerchino immagini scambiate tramite supporto rimovibile, piuttosto che per la verifica degli accessi ad una determinata risorsa remota.
Si deve comunque utilizzare un metodo scientifico[9] nel procedere con l'analisi.
Un chiaro esempio, che denota la difficoltà di stabilire a priori una specifica procedura standard, può essere il caso di dover ricercare un'immagine di 1023 KB all'interno di un dispositivo sequestrato di dimensione di 2 TB. Le varie, e non esaustive, tecniche di ricerca potrebbero essere:

- ricerca in base a nome file;
- ricerca in base all'estensione file;
- ricerca in base all'*header* (firma del file che denota la sua natura) dell'immagine;
- ricerca in base al codice HASH dell'immagine da ritrovare;
- ricerca in base alla dimensione del file.

Tutte queste tecniche possono presentare dei limiti o dei pregi, relativamente all'obiettivo di ricerca: l'indagato potrebbe aver modificato il nome file, potrebbe aver copiato l'immagine all'interno di un altro documento, potrebbe aver inserito un messaggio nascosto tramite steganografia[10] o altro ancora.
Come esistono degli strumenti informatici che facilitano il compito degli ingegneri edili nel calcolo strutturale, così esistono programmi di supporto agli investigatori digitali per la ricerca delle informazioni. Sul mercato esistono molti software (sia commerciali, sia *open source*) che aiutano a svolgere l'analisi forense: tra quelli appartenenti alla prima famiglia bisogna sicuramente ricordare Encase, FTK, X-Way Forensic, mentre appartengono alla seconda categoria i progetti italiani DEFT, CAINE e i progetti esteri come Helix e FCCU.
Tali strumenti sono comunque solo un supporto al professionista, in quanto nessun software potrà eseguire un'analisi forense in maniera automatica[11]; inoltre il lavoro o il compito del *computer forensic examiner* non è limitato al cliccare il pulsante giusto, ma è quello di comprendere profondamente il contesto, per poter indirizzare e guidare il software nella direzione corretta, al fine di ottenere risultati oggettivi, coerenti e rispondenti allo scopo.
Il processo di analisi forense termina con la redazione di un documento scritto che evidenzi sia la procedura utilizzata, che i risultati ottenuti. Questo documento deve essere tanto preciso quanto semplice da leggere da parte di una persona non tecnica, che deve decidere su ciò che è stato trovato.

5. Conclusioni

Le indagini sui dispositivi digitali sono in aumento; per una miglior azione di prevenzione e repressione di tutti i reati, non solo dei *computer crimes*, servono nuove conoscenze, tecniche e metodologiche che riescano a preservare i dati informatici. Queste informazioni soffrono di problematiche legate alla loro facile modifica, circostanza che potrebbe compromettere l'esito di un intero procedimento giudiziario.
Non esiste la procedura esatta per effettuare un'analisi, non esiste il software perfetto per svolgere le ricerche, il cuore della *digital forensic* rimane l'esperienza certificata del *computer forensic examiner* che traduce i *bytes* in una risposta oggettiva ai quesiti degli investigatori.

Nicola Chemello è laureato in Ingegneria Informatica ed iscritto all'albo degli ingegneri della provincia di Treviso, membro della relativa commissione informatica ed informatizzazione e della commissione permanente di ingegneria dell'informazione della FOIV. In possesso della certificazione internazionale EnCE per l'analisi forense su dispositivi elettronici Collabora con le forze dell'ordine e con i Tribunali del Nord-est per consulente e perizie tecniche informatiche. Esperto in sicurezza informatica e certificatore di sistemi di sicurezza delle reti aziendali. Promotore del progetto di sensibilizzazione sul cyberbullismo.
E-mail: nicola@securcube.net

[9] Cioè con la modalità tipica con cui la scienza procede per raggiungere una conoscenza della realtà oggettiva, affidabile, verificabile e condivisibile. Consiste, da una parte, nella raccolta di evidenza empirica e misurabile attraverso l'osservazione e l'esperimento; dall'altra, nella formulazione di ipotesi e teorie da sottoporre nuovamente al vaglio dell'esperimento.

[10] Tecnica che si prefigge di nascondere la comunicazione tra due interlocutori.

[11] Notoriamente il software velocizza l'analisi: tutto quello che esegue un programma per l'analisi forense può essere replicato "a mano" da un capace investigatore. Non è sufficiente recuperare un'immagine, ma si deve descrivere dove è stata trovata, per non fuorviare il giudizio; per esempio indicare se è presente in uno *slack space* (spazio inutilizzato nei settori del supporto di memorizzazione) fornisce una serie di informazioni fondamentali in sede di dibattimento.