



Cybercrimes.it

Computer Forensics & Crimine Informatico

Dario Scalea

Computer Forensics

Metodologia, Eziologia ed Etica

I

Definizione

È ora di (de)finirla.

L'incognita primaria che ogni forma di conoscenza si trova ad affrontare è la propria definizione. Definire significa cercare con un metodo condiviso un'insieme di proprietà differenziali che soddisfino i criteri di unicità del fine e relazionabilità dei concetti. Anche la computer forensics, per assumere una determinazione gnoseologica, si affanna in questa doverosa ricerca con alterne fortune tipiche della stadio iniziale di una disciplina. In verità, l'informatica forense è sì giovane, ma non come mendacemente si ritiene. Le prime testimonianze d'interesse risalgono all'inizio degli anni '80 quando negli Stati Uniti d'America nacquero i primi algoritmi sperimentali di ceas (computer evidence analysis software) sviluppati da diversi laboratori di ricerca universitari e federali. Un quarto di secolo abbondante, considerando che la velocità dello scambio informativo nell'intervallo temporale considerato è aumentata in modo esponenziale, dovrebbe essere più che sufficiente per consentire alla maggior parte degli studiosi di convenire su di una definizione. Invece, questo tanto agognato traguardo sembra ripercorrere il tortuoso cammino denotazionale che si originò dal "Mengenlehre" di Cantor: ancora oggi il termine "insieme" resta privo di una delimitazione logico-formale universalmente accettata. Ritornando alla computer forensics, assistiamo scontenti ad un proliferare divergente di tentativi più o meno autorevoli. Personalmente ho letto circa sessanta definizioni che propongono soluzioni a carattere includente od escludente ma nessuna originata da una semplice

operazione inferenziale delle precedenti. Questa situazione antitetica ad ogni canone scientifico (Bacone e Galilei, perdonateci) è stata generata essenzialmente da due fattori:

1) Fattore ontologico.

La computer forensics è, per la propria natura interdisciplinare, una materia ad alto rischio di contraddizione in quanto nata dall'intersezione tra la giurisprudenza e l'informatica ovvero tra l'ente conoscitivo fondato sull'esclusione di ogni ragionevole dubbio (di alterazione) e quello che ogni ragionevole dubbio (di alterazione) include. Geometricamente sarebbe come voler trovare il punto d'intersezione di due rette parallele. La soluzione è una sola: piegarle. Tradotto nei meno rigidi schemi umani significa trovare un equilibrato compromesso che consente l'ormai ineludibile istanza d'ingresso della prova informatica nei tribunali.

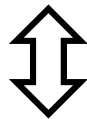
2) Fattore antropologico.

In internet si trova tutto e il contrario di tutto. L'ausilio delle tecnologie che in teoria avrebbe dovuto consentire una più rapida evoluzione del sapere ha avuto un effetto egotrofico nell'animo umano che ha portato i "passanti" della Rete, tra una foto porno e l'altra, a sentirsi in grado di confutare teorie di premi Nobel, frutto di decenni di studio e riconosciute dalla comunità scientifica internazionale. Questo perché l'equidisponibilità delle risorse, che di per sé è un bene, è stata confusa con l'equivalenza delle risorse annullando in molti navigatori la consapevolezza dei propri limiti che, evidentemente, in precedenza, questi stessi soggetti identificavano con l'inaccessibilità a determinati luoghi. D'altronde è proprio dell'ignorante ritenersi onnisciente. Oltretutto, la facilità di comunicazione ha avuto un effetto negativo anche su chi ha la preparazione per affrontare determinate tematiche perché ha esasperato la

naturale propensione al primato (meglio sarebbe una tensione all'eccellenza) nell'anteporre l'interesse personale a quello scientifico. Conseguenze più o meno accentuate di questo fenomeno sono un notevole inquinamento ed una diffusa frammentazione della conoscenza con labirintite assicurata per chi vede la Rete come luogo di formazione.

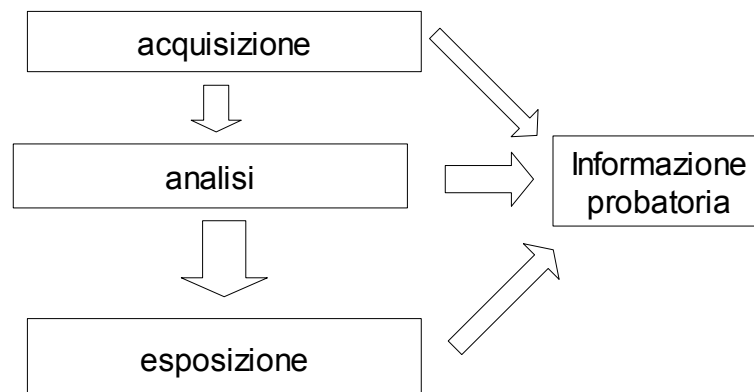
Dopo aver filtrato per mezzo di procedure logiche-formali (con cui non vi tedierò, almeno in questa occasione) tutte le principali definizioni di computer forensics sono giunte a questa conclusione:

$$C_f = \sum_{k=1}^3 \varphi_k(x) \quad \forall x_{(svt)_2} \in \Pi$$



La computer forensics è una disciplina scientifica finalizzata all'acquisizione, all'analisi ed all'esposizione in sede processuale di ogni genere d'informazione probatoria memorizzata o trasmessa in formato binario.

N.b. (per estensione e sostituzione si può ricavare la definizione di digital forensics)



Teoria assiomatica

Che Peano mi assista.

A quanti tra voi che, alla vista dell'equazione precedente, hanno pensato di accendere la televisione, ricordo quanto segue:

Matematica \Rightarrow Informatica

(Informatica \cap Giurisprudenza) \Leftrightarrow Computer forensics

L'informatica (crasi di informazione automatica) è una branca della matematica (anche se non ho mai visto nessuno entrare in un negozio di "informatica" e chiedere il teorema di De Morgan) e la *c.f.* è un settore specialistico dell'informatica: capirete bene la stretta correlazione esistente con la matematica, senza contare che, al di sopra di ogni altra considerazione, una disciplina scientifica degna di questo nome necessita di una formalizzazione logica. Quell'accozzaglia di plastica e silicio scadente che molti venerano come una divinità sa fare un'unica azione (calcolare) e il suo unico pregio (di grande utilità) è che la sa fare ad una velocità incrementale di gran lunga superiore a qualsiasi essere umano. Ho sentito dire che il calcolo e la matematica hanno una certa affinità, ma non chiedetemi quale.

Sperando di avervi persuaso, procediamo. Tramite operazioni di riduzioni logiche ricorsive, sono arrivato a costruire la *c.f.* a partire da cinque assiomi fondamentali: formazione tecnico-scientifica, inalterabilità della prova, completezza procedurale, coerenza probatoria, conformità legislativa.

Di seguito riporto la relativa formalizzazione logico-matematica.

1) Formazione tecnico-scientifica

$$F = \{ \varphi_{k=[1,3]} \} \subset \mathbb{C}$$

2) Inalterabilità della prova

$$\{ [X_{(svt)_2}] \in \Phi_1 \} = \{ [X_{(svt)_2}] \in \Phi_2 \} = \{ [X_{(svt)_2}] \in \Phi_3 \}$$

3) Completezza procedurale

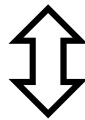
$$C_f \Rightarrow \{ \varphi_{k=[1,3]} \} \Rightarrow \{ \varphi_1 \Rightarrow \varphi_2 \Rightarrow \varphi_3 \}$$

4) Coerenza probatoria

$$[X_{(svt)_2}] \subset \Pi$$

5) Conformità legislativa

$$\sum_{k=1}^3 \varphi_k \subset L$$



① Formazione tecnico-scientifica

Ogni fase del processo di computer forensics deve essere costruita su solide fondamenta tecnico-scientifiche.

② Inalterabilità della prova

La prova informatica deve essere uguale a se stessa dall'acquisizione all'esposizione in sede processuale.

③ Completezza procedurale

La c.f. è costituita da un macroprocesso indivisibile in cui ogni fase implica la successiva.

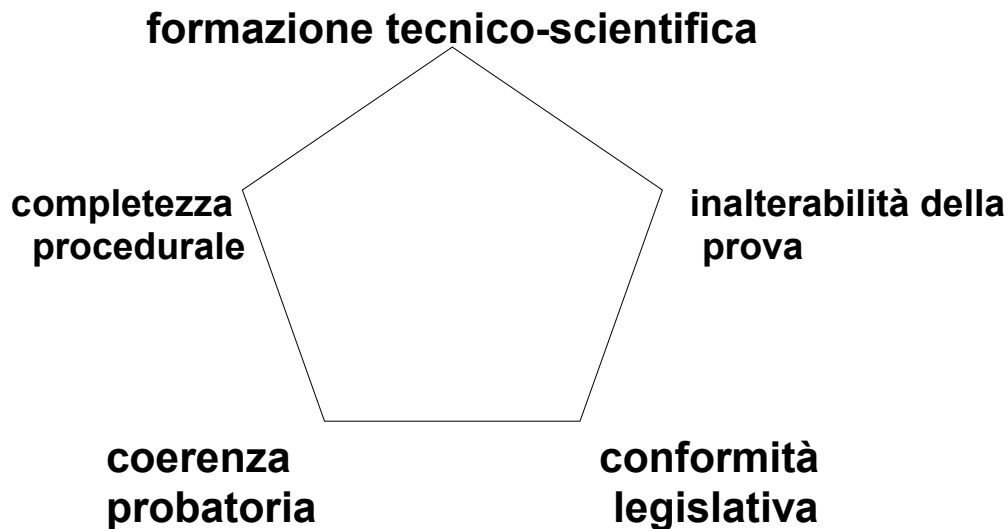
④ Coerenza probatoria

Ogni dato informativo ha valore quando è funzionale allo stato d'innocenza o colpevolezza dell'imputato.

⑤ Conformità legislativa

Ogni azione dell'analista informatico-forense non deve essere contraria alle relative disposizioni di legge.

Pentagono assiomatico



N.B.(La teoria assiomatica della digital forensics è equipollente)

Principia nova methodo exposita

L'impostazione analitica è una pratica sconosciuta a molti sedicenti informatici. Il virus dello strumentalismo si è diffuso in modo pervasivo fino a far ritenere che memorizzare una sequenza di “click” del dispositivo di puntamento, nell'utilizzo di tools come toys, o saper digitare comandi parametrici di Unix equivalga a conoscere. Ma l'unica cosa che conoscerete sarà lo studio di uno specialista per la sindrome del tunnel carpale. La conoscenza implica la comprensione e la comprensione è la risposta al perchè, non al come. Avete mai visto una casa costruita a partire dal tetto? Quindi, per evitare di pensare che i multivibratori bistabili siano oggetti da sexy-shop, lancio un appello rivolto a me in prima persona e poi a tutti voi: spegniamo un po' di più il monitor e “accendiamo” un po' di più i libri. Ora siamo pronti a partire per questo lungo ed affascinante viaggio.

Dario Scalea

digitalforensics@cryptomail.org