

La professione dell'informatico forense: percorsi formativi e metodologie di intervento

Avv. Pierluigi Perri – Università degli Studi di Milano

Il corso di perfezionamento dell'Università degli Studi di Milano

- Nato nel 2006.
- Ogni edizione cura un aspetto particolare (mobile, antifoensics, case study).
- Ogni anno si iscrivono tra i 40 e i 50 partecipanti.
- Attira sia avvocati, sia forze dell'ordine sia tecnici.
- Si è rivelato un'ottima occasione per “fare rete”.

Altri percorsi formativi

- Università di Bologna
- LUMSA
- Università di Teramo

La formazione dell'informatico forense

- Trattandosi di materia “a cavallo” tra il tecnico e il giuridico, è richiesta la conoscenza di entrambe le materie (con ovvia predilezione di una di esse).
- Ogni percorso formativo sulle indagini informatiche, infatti, prevede sia moduli tecnico/informatici sia moduli giuridici.
- Non basta saper scovare, analizzare e conservare una fonte di prova, bisogna anche saperla **spiegare** ai giudici.
- Bisogna comprendere che la fonte di prova informatica, comunque, è immersa in un quadro probatorio complessivo.

Alcuni dei concetti giuridici alla
base della *computer forensics*

Cos' è una “prova” in senso lato?

- “Qualunque strumento, metodo, persona, cosa o circostanza che possa fornire informazioni utili per risolvere l'incertezza intorno alla verità o falsità degli enunciati fattuali” (Taruffo).

La “fonte di prova”

- Nel diritto processuale penale più che di “prova” in senso lato si parla di “fonte di prova”, consistente in “tutto ciò che è idoneo a fornire risultati apprezzabili per la decisione del giudice”. (Tonini).

Cos' è un "indizio"?

- “L'indizio è il procedimento mediante il quale, partendo da un fatto provato, si ricava, mediante massime di esperienza o leggi scientifiche, l'esistenza di un fatto storico da provare” (Tonini).

Lo “strumento di prova”

- Nell’impiego dei mezzi di prova potrebbe rendersi necessario utilizzare degli apparati conoscitivi (principi e metodologie scientifiche, tecnologie, apparecchiature) che non sono patrimonio del sapere comune e richiedono perciò il ricorso ad un esperto

Dalla “prova” alla “prova scientifica”



- Quando la prova verte su un fatto da leggi scientifiche e/o tecniche specialistiche per le quali è necessario ricorrere ad un esperto, si versa nel campo della prova scientifica

La “prova scientifica” digitale: la *computer forensics*

- La disciplina ha origine in ambienti giuridici di *common law* ad alta evoluzione tecnologica come gli USA e ha visto sorgere numerose agenzie specializzate che offrono formazione e certificano i *software* e gli strumenti adoperati per le indagini

Nascita della *computer forensics*

- La data di nascita “pratica” della *computer forensics* è il 1984, quando il laboratorio scientifico del FBI e altre agenzie investigative americane iniziarono a sviluppare programmi da utilizzare nell’esame dei dati presenti nei computer
- Nello stesso anno, per rispondere alla crescente richiesta di investigazioni in ambito informatico, fu creato, all’interno dell’FBI, il *Computer Analysis and Response Team (CART)* con il compito fondamentale di procedere nei casi in cui si rendeva necessaria l’analisi di un computer

Esempio di standardizzazione: il NIST



Ambito d' applicazione

- La *computer forensics* non riguarda solo i c.d. *computer crimes* ma può interessare:
 - i crimini realizzati con l' uso di un computer
 - diretti a un computer
 - in cui il computer può comunque rappresentare una fonte di prova

Alcuni fatti di cronaca



Cosa accomuna i 3 casi?

- Denominatore comune: il dato digitalizzato come oggetto di indagine
- Problema comune: come procedere nella raccolta di dati e informazioni a vocazione probatoria?

I problemi delle investigazioni informatiche

Casey individua tre problemi fondamentali:

- bisogno di **scientificità**, che si tradurrebbe anche nella definizione di diverse aree di specializzazione (ad es. tra *digital crime scene technicians* e *digital evidence examiners*);
- carenza di **sistematicità** nei metodi usati dagli investigatori;
- mancanza di **standard** accettati a livello nazionale e internazionale sia per la pratica che per la formazione.

In particolare, secondo Casey, bisogna investire sul lato **formativo** e **professionalizzante** del *computer forensics expert*.

Riassumendo

- I *device* elettronici sono immanenti nella vita di ogni individuo
- Questi dispositivi, spesso, contengono dati utili alla ricostruzione dei fatti
- La raccolta degli elementi di prova deve avvenire sempre secondo una metodologia rispettosa dei principi della scienza e del diritto

Le “recenti” prescrizioni del Legislatore

- Con la legge 4 aprile 2008 n. 48 sono stati introdotti all'interno del codice di procedura penale alcuni principi fondamentali per il trattamento dei dati digitali a fini probatori
- Restano molte zone d'ombra sui metodi per una corretta individuazione, raccolta, analisi e valutazione in giudizio delle *digital evidence* sono ancora molte

Alcuni esempi

- 244 c.p.p. (**Casi e forme delle ispezioni**).
- 1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.
- 2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, **anche in relazione a sistemi informatici o telematici**, adottando misure tecniche dirette ad assicurare la **conservazione** dei dati **originali** e ad impedirne l'**alterazione**.

- 247 c.p.p. (**Casi e forme delle perquisizioni**).
- 1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.
- **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.**
- 2. La perquisizione è disposta con decreto motivato.
- 3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.

- Art. 254-*bis* c.p.p. (**Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni**).
- 1. L' autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante **copia di essi su adeguato supporto**, con una procedura che assicuri la **conformità** dei dati acquisiti a quelli originali e la loro **immodificabilità**. In questo caso è, comunque, ordinato al fornitore dei servizi di **conservare e proteggere** adeguatamente i dati originali.

Elementi comuni

- Conservazione
- Non alterazione
- Non modificabilità
- Protezione
- Supporto “adeguato”

Problemi

- Come rispettare i requisiti indicati dal Legislatore?
- Quanto costa?
- Cos'è un dato “originale” e come lo distinguo da un dato “copiato”?
- Come faccio a garantire i diritti dell'indagato e dei terzi?

Le soluzioni

- Metodologie scientifiche di raccolta, analisi e gestione delle prove digitali
- Formazione specifica per gli attori processuali (magistrati, polizia giudiziari, avvocati, tecnici, operatori forensi)
- Osmosi tra mondo tecnico-informatico e mondo giuridico

Grazie per l' attenzione

Avv. Pierluigi Perri
Università degli Studi di Milano
Via Festa del Perdono, 7
20122 Milano
pierluigi.perri@unimi.it