•**Titolo:** La computer fornsics: le nuove frontiere della legalitá.

•**Autore:** Giulio Giovinazzo

•**Istituzione**: Università degli Studi di Genova

•**Data di pubblicazione:** 18/11/2015

•**Riassunto:** Le nuove tecnologie stanno contribuendo in maniera decisiva alla reinvenzione della vita in un nuovo contesto globale rappresentato dalla rete. Questa sempre piú spesso si converte in un ambiente accessibile a diverse tipologie di reati e abusi. Dalla pedofilia informatica alle frodi di carattere economico sono giá innumerevoli i casi di illecito realizzati attraverso supporto informatico durante gli ultimi dieci anni. La computer foresics nasce come tentativo da parte delle istituzioni di combattere e impedire le infrazioni piú o meno gravi che vengono commesse in rete quotidianamente. Nel presente articolo si analizzeranno le principali attuazioni da parte del governo Italiano con la promulgazione di leggi orientate a tal fine e con la creazione di corpi speciali di polizia informatica durante il periodo compreso tra il 2008 e il 2012.

•**Parole chiave:** computer forensics, crimini online, informatica, diritto.

UNIVERSITÀ DEGLI STUDI
DI GENOVA

A.A.2011/2012

corso di laurea in:

Scienze della comunicazione

corso di:

FONDAMENTI DI DIRITTO DELLA COMUNICAZIONE ELETTRONICA

Prof.ssa Avv. Elena Bassoli

LA COMPUTER FORENSICS:

Le nuove frontiere della legalità

di

Giulio Giovinazzo

Università´degli Studi di Genova
Italia

Indice generale

INTRODUZIONE ALLA COMPUTER FORENSICS

La **Computer Forensics**, o informatica forense, è la disciplina che si occupa dell'identificazione, della conservazione, dell'analisi e della documentazione dei reperti informatici al fine di presentare prove digitali valide in procedure civili e penali.

Si tratta di una disciplina che ha origine negli ambienti giuridici degli Stati Uniti e della Gran Bretagna in seguito alla crescente diffusione degli strumenti digitali e che integra le competenze informatiche e tecniche con quelle giuridiche.

La ratifica della **Convezione di Budapest sui Cybercrime** nella **Legge 48/2008**[1] ha introdotto nel panorama normativo nazionale metodologie di Computer Forensics, con l'obiettivo di realizzare una politica comune con gli altri Stati membri dell'Unione Europea. Oggi la dottrina e la giurisprudenza in materia trattano tematiche delicate quali il riciclaggio di denaro e i reati tributari, i reati contro la persona, le frodi, l'uso a scopo personale di materiale aziendale, la violazione del diritto d'autore, lo spionaggio industriale, la pedopornografia, lo stalking e molti altri.

La figura professionale dell'informatico forense deve quindi garantire un livello di competenza tecnica e giuridica altamente qualificata e specializzata, al fine di analizzare sistemi digitali garantendo procedure conformi alle normative nazionali ed europee e alle best practices internazionali.

Oggigiorno i dati digitali sono il patrimonio più prezioso e la risorsa più strategica di ogni realtà aziendale, sia privata che pubblica. La Computer Forensics è la soluzione corretta per riuscire a prevenire il furto di dati, lo spionaggio industriale, l'accesso abusivo ai sistemi informatici aziendali, i danneggiamenti informatici e rispondere a tutte le potenziali controversie legali.

Si tratta di una disciplina di recente formazione (la sua nascita si colloca intorno al 1980 ad opera dei laboratori tecnici della FBI). Spesso viene erroneamente identificata come una

1 La Legge 18 marzo 2008, n. 48 promulgata dal Presidente della Repubblica (pubblicata in Gazzetta Ufficiale 4 aprile 2008, n. 80) reca la ratifica della Convenzione del Consiglio d'Europa di Budapest sulla criminalità informatica del 23 novembre 2001.

Il richiamo a tale fatto è determinante nell'ottica dell'intervento sulla scena del crimine per quanto riguarda i crimini ed i reperti ad alta tecnologia (digitali).

nuova "branca" della computer security.

In Italia, la legge di riferimento per l'informatica forense è la Legge n.48/2008, nota come "Legge di ratifica della Convenzione di Budapest".

ARTICOLI CHE REGOLANO LA COMPUTER FORENSICS

Art. 615 ter Accesso abusivo ad un sistema informatico o telematico

“Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volonta’ espressa o tacita di chi ha il diritto di escluderlo, e’ punito con la reclusione fino a tre anni. La pena e’ della reclusione da uno a cinque anni:

1) se il fatto e’ commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualita’ di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se e’ palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l’interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all’ordine pubblico o alla sicurezza pubblica o alla sanita’ o alla protezione civile o comunque di interesse pubblico, la pena e’, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto e’ punibile a querela della persona offesa; negli altri casi si procede d’ufficio”[2] .

Art. 615 quater: Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

“Chiunque, al fine di procurare a se’ o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all’accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, e’

2 Articolo aggiunto dall’art. 4, L. 23 dicembre 1993, n. 547.

punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni. La pena e' della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater"[3] .

Art. 615 quinquies: Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

"Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329"[4]

Art. 640 ter: Frode informatica

"Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalita' su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a se' o ad altri un ingiusto profitto con altrui danno, e' punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni. La pena e' della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto e' commesso con abuso della qualita' di operatore del sistema. Il delitto e' punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante"[5] .

3 Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.

4 Articolo così modificato dalla Legge 18 marzo 2008, n. 48.

5 Articolo aggiunto dall'art. 10, L. 23 dicembre 1993, n. 547.

LE 5 FASI DI FORMAZIONE DELLA PROVA DIGITALE

Così come in ogni scena criminis “tradizionale”, anche di fronte ad un presunto reato informatico, chi conduce le indagini (Polizia postale delle Comunicazioni, Guardia di Finanza, Corpo dei Carabinieri, tecnici specializzati nominati dal P.M.[6] ecc..) deve seguire un preciso iter di passaggi, per garantire una scientificità assoluta al processo di indagine e scongiurare così ogni possibile sospetto di inquinamento o comunque cattivo trattamento delle prove del reato.

Per questo motivo, la Computer Forensics basa le sue indagini su una serie di passaggi che sono:

1) IDENTIFICAZIONE: si tratta della ricerca vera e propria delle prove del reato, l' identificazione è quindi **fisica** quando si cercano i dispositivi (spesso molto piccoli e facilmente celabili come pc portatili, smarthphone, palmari, pennette usb, hard disk, schede micro sd ecc...) sparsi per la scena del reato, che sia una casa, un ufficio o una azienda intera. Oppure si parla di identificazione **logica** quando si compie una diagnosi preliminare del materiale hardware e software. Dal momento che non sono ammissibili errori durante le indagini, chi esegue le operazioni deve conoscere sufficientemente l'apparecchio informatico con cui si trova ad avere a che fare, per questo è necessaria da parte degli inquirenti una attenta fase di studio delle prove in vista del loro trattamento (di questo si parlerà maggiormente nel capitolo dell'elaborato “Competenze nell'informatica forense”).
2) ACQUISIZIONE: una volta trovati i dati da analizzare si procede alla fase di acquisizione, la quale deve essere effettuata in modo estremamente scrupoloso e deve fare si che i dati acquisiti vengano rilevati in modo da ricreare una copia identica. Per questo si fa una copia **bit to bit**, dal primo Kbit all' ultimo. Ad esempio in caso 4Gb di dati siano memorizzati in un Hard Disk da 500 Gb, si deve fare una copia dell'intero spazio di memoria del dispositivo, anche se 496 Gb risultano come spazio “vuoto”. Con questo processo si crea quella che i forensi chiamano una **Bit Stream Image**.

6 Art. 359 C.P.P. Consulenti tecnici del pubblico ministero.
“1. Il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di consulenti, che non possono rifiutare la loro opera.
2. Il consulente può essere autorizzato dal pubblico ministero ad assistere a singoli atti di indagine.”

Per garantire l'assoluta uguaglianza dei dati acquisiti, e dimostrare così che questi non sono

algoritmo di Hash[8], cioè un codice, una stringa alfanumerica di 128, 250 ecc. caratteri

(L'Hash è una chiave algoritmica, per cui se si modifica anche solo che un bit, questa chiave verrà completamente cambiata.)

L'acquisizione può essere:

- LIVE cioè ad apparecchio acceso, che non può essere spento per non perdere dati contenuti in memorie volatili come nella RAM. In questo caso il processo non è ripetibile più di una volta.

- POST MORTEM a macchina spenta, la si stacca e poi si acquisiscono i dati con il calcolo dell'Hash, per garantire la copia perfetta. Il dato originale andrà nell'archivio del tribunale come prova e la copia verrà utilizzata per le indagini.

3) ANALISI: si svolge sulla seconda copia di dati, si procede con la ricostruzione gerarchica delle cartelle e poi con la indicizzazione di ogni singola informazine. Si esegue l' analisi del File System e del registro di Windows in caso l'utente utilizzi questo sistema operativo, in modo da sapere quali programmi ha utilizzato, quali ha installato ecc..

   N.B. Il software **FTK**[9] è uno degli strumenti maggiormente usati dagli inquirenti in quanto rivela quali e quante conversazioni ha avuto un utente in un dato lasso di tempo.

---

8 L'algoritmo di hash elabora qualunque mole di bit (in informatica si dice che elabora dati "grezzi"). Si tratta di una famiglia di algoritmi che soddisfa questi requisiti:

1. L'algoritmo restituisce una stringa di numeri e lettere a partire da un qualsiasi flusso di bit di qualsiasi dimensione (può essere un file ma anche una stringa). L'output è detto digest.
2. La stringa di output è univoca per ogni documento e ne è un identificatore. Perciò, l'algoritmo è utilizzabile per la firma digitale.
3. L'algoritmo non è invertibile, ossia non è possibile ricostruire il documento originale a partire dalla stringa che viene restituita in output ovvero è una funzione unidirezionale. Definizione tratta da: http://it.wikipedia.org/wiki/Hash#Algoritmo_di_hash

9 FTK Imager è un programma di acquisizione dati che può essere utilizzato per fornire una rapida anteprima del contenuto di un hard disk e, se necessario, crearne un'immagine forense.
Per garantire l'integrità della copia questo software realizza una duplicazione bit-per-bit del dispositivo. L'immagine è in questo modo identica all'originale, incluso lo spazio non allocato e lo slack space.

Durante la fase di copia forense il programma verifica che l'hash dell'immagine realizzata e quello dell'hard disk coincidano.

Informazioni prese da: http://www.digital-forensics.it/acquisizione-con-ftk-imager

4) REPORT: dopo l'analisi delle prove del reato, si elabora una relazione tecnica, in cui si spiega dettagliatamente come è stata svolta l'indagine e quali sono i suoi risultati.

   L'intero lavoro del **digital forenser** deve essere costantemente documentato, a partire dall'inizio dell'investigazione fino al termine del processo. La documentazione prodotta comprende, oltre alla **catena di custodia**[10], un'analisi dei dati rinvenuti e del processo seguito. Un'accurata documentazione è di fondamentale importanza per minimizzare le obiezioni e spiegare come ripetere l'estrazione con un analogo processo sulla copia.

5) PRESENTAZIONI: dopo che l'investigatore ha **elaborato delle ipotesi** sul caso, e dopo averle presentate a chi ha la titolarità delle decisioni sulle azioni da compiere, ad esempio il pubblico ministero, è chiamato a **discutere le ipotesi trovate**, generalmente attraverso una discussione. Qualora suscitino delle perplessità, si dovrà procedere ad un ritorno alle fasi precedenti dell'indagine.

   I risultati di un'indagine vengono spesso **divulgati**, le notizie dovrebbero però essere filtrate in modo tale da non fornire particolari che potrebbero rendere più difficoltose analoghe investigazioni[11].

10 In materia di computer forensics per catena di custodia si intende l'identificazione di tutti i passaggi compiuti sull'evidenza digitale,dal suo rinvenimento fino al suo repertamento.
Definizione tratta da: Elena Bassoli, "Lezioni di diritto dell'informatica ed elementi di informatica giuridica" edizioni ECIG Universitas, Genova 2009.

11 Tratto da: Elena Bassoli, "Lezioni di diritto dell'informatica ed elementi di informatica giuridica" edizioni ECIG Universitas, Genova 2009.

COMPETENZE NELL' INFOMATICA FORENSE

L’informatica forense è una delle scienze ausiliarie del diritto penale (al pari della medicina legale o della balistica forense) strumentale all’accertamento dei fatti costituenti reato tipicamente informatico (ad esempio, accesso abusivo a sistema informatico), ovvero costituenti reato a condotta libera ma commesso con un sistema informatico e telematico (ad esempio, una diffamazione via Internet) ovvero un reato di qualsiasi tipo le cui prove siano contenute in un sistema informatico o telematico (ad esempio, geolocalizzazione del telefono cellulare per la ricostruzione dei movimenti di un indiziato di omicidio).

L’attività dell'indagine forense può avvenire sui sistemi informatici (computer forensics), su sistemi telematici (network forensics), su sistemi di comunicazione mobile (mobile forensics), nonché su tutti i nuovi dispositivi digitali che quotidianamente vengono immessi sul mercato.

L’obiettivo dell’informatica forense viene normalmente perseguito adottando tecniche e metodologie che consentono di acquisire tutti i dati registrati in un supporto digitale per riportarli inalterati su un supporto diverso. Talvolta, l’informatico forense è costretto a ricorrere a tecniche di hacking del sistema di protezione per poter acquisire i dati oggetto di acquisizione.

Lo svolgimento di tali operazioni richiede il rispetto di norme giuridiche e tecniche cosicché si impone la necessità di descrivere e documentare tutte le procedure tecniche, gli strumenti hardware e software utilizzati per l’ acquisizione ed analisi dei dati, al fine di consentire in ogni momento il controllo e la verifica tecnica e di legalità delle conclusioni. Si deduce quindi che ogni informatico forense, oltre ad una profonda preparazione tecnica, debba possedere anche una rilevante formazione giuridica, e in particolare del diritto pubblico, del diritto penale e del diritto processuale penale.

In questa disciplina, diritto e informatica si compenetrano con la massima evidenza. Inoltre, proprio la frequenza e la pervasività dell'innovazione tecnologica fanno si che non vi sia ormai processo senza prove digitali. Tale fenomeno impone a ogni operatore forense (magistrati, avvocati, polizia giudiziaria, cancellieri, custodi, consulenti, periti, ecc.) l'obbligo di informazione, formazione e aggiornamento in campo informatico e informatico-giuridico.

Gli informatici, dal canto loro, devono conoscere con precisione le implicazioni giuridiche delle loro attività e quindi i principi del diritto sostanziale, il diritto processuale ed in particolare il regime dei mezzi di prova e di ricerca della prova, per evitare errori in procedendo talvolta irrimediabili.

INFORMATICA FORENSE ALL'UNIVERSITÀ

Dal 2003 è stato attivato l'insegnamento di "Informatica Forense" nella Facoltà di Giurisprudenza dell'Università di Bologna, ed il Cirsfid[12] si è dotato di un laboratorio dedicato alla didattica delle tecniche di indagine forense in ambito informatico. Si tratta del primo corso coi contenuti sotto indicati attivato in Italia e, negli anni, varie sedi sia delle Facoltà di Giurisprudenza che delle Facoltà di Scienze Matematiche, Fisiche e Naturali hanno inserito tale insegnamento nei loro piani di studio. Dall'a.a. 2003-2004 al 2006-2007 e negli a.a. 2009-2010 e 2010-2011 è stato tenuto inoltre, nella Facoltà di Giurisprudenza, un Seminario affine (tre crediti, 24 ore di lezione frontale) dal titolo "Profili giuridici dell'Informatica Forense". Una versione del corso è stata tenuta al Master in Diritto delle nuove tecnologie e Informatica giuridica della Facoltà di Giurisprudenza dal2002-2003ad oggi.

Sono numerosi i contatti scientifici scaturiti dalle attività connesse al corso con le Forze di polizia,associazioni di avvocati, magistrati inquirenti e giudicanti, Istituzioni anche a livello internazionale. Attualmente alcuni dottorandi del Dottorato Interdisciplinare in Diritto e Nuove Tecnologie organizzato dal

Cirsfid svolgono la loro attività in relazione a tale disciplina.
In questo ambito, tra l'altro, è stata sviluppata DEFT (Digital Evidence & Forensics Toolkit), una distribuzione Linux live per le attività di analisi forense che da diversi anni è utilizzata non solo nei corsi ma anche da forze dell'ordine ed enti nazionali ed internazionali.

12 Cirsfid: Centro interdipartimentale di ricerca in storia del diritto, filosofia e sociologia del diritto e informatica giuridica. (Università di Bologna).

BIBLIOGRAFIA:

Per realizzare questo elaborato sono stati consultate le seguenti fonti:

- Elena Bassoli, "*Lezioni di diritto dell'informatica ed elementi di informatica giuridica*" edizioni ECIG Universitas, Genova 2009.

- slide e materiale informativo messo a disposizione dal Dott.Ing. Roberto Surlinelli (direttore tecnico principale della Polizia Postale di Genova).

- informazioni messe a disposizione da Fabio Massa (digital forenser, Vicepresidente *ANGIF* Nazionale, esperto nel settore della Digital Forensics, membro scelto del Corpo dei Carabinieri).

- appunti in materia di Digital Forensics riguardanti le lezioni di "Fondamenti di diritto della comunicazione elettronica" tenute dalla proff.ssa Avv. Elena Bassoli agli studenti di Scienze della Comunicazione A.A 2011-2012.

SITOGRAFIA:

cenni sulla computer forensics:

http://www.lawyersonweb.it/content/cenni-sulla-computer-forensics

articoli del codice penale:

http://www.altalex.com

http://www.crimine.info/public/crimineinfo/norme/615_ter.htm

http://it.wikisource.org/wiki/Codice_penale/Libro_II/Titolo_XII

http://www.crimine.info/public/crimineinfo/articoli/accesso_sistema_informatico.htm

nozioni sulla digital forensics:

http://www.digital-forensics.it

Legge di ratifica della Convenzione di Budapest, articolo di Marco Mattiucci:

http://www.marcomattiucci.it/l482008.php

algoritmo di Hash:

http://it.wikipedia.org/wiki/Algoritmo_di_Hash

CIRSFID, Università di Bologna:

http://www.cirsfid.unibo.it/CIRSFID/Centro/AreeDisciplinari/Informatica_Forense.htm

ANGIF associazione nazionale giuristi informatici e forensi:

http://www.angif.it/

Polizia postale e delle comuniazioni:

http://poliziadistato.it/articolo/982/