Digital evidence e libertà fondamentali

Giuseppe Vaciago

Nexa Center for Internet & Society

12 giugno 2012

Agenda

① Introduzione
- *Definizione di digital evidence*
- *Classificazioni della digital evidence*
- *Definizione di digital forensics*
- *Digital forensics e prova scientifica*

② Best practices, aspetti processuali e problemi della digital forensics
- *Le cinque fasi della digital forensics*
- *Copia bit stream e funzione di hash*
- *La legge 48/08 di ratifica della Convenzione Cybercrime*
- *I due problemi della digital forensics: Cloud computing e crittografia*

③ Le cinque fasi della *digital forensics*
- *Individuazione della digital evidence*
- *Acquisizione della digital evidence*
- *Conservazione della digital evidence*
- *Analisi della digital evidence*
- *Presentazione della digital evidence*

④ Conclusioni

Cosa è la *digital evidence?*

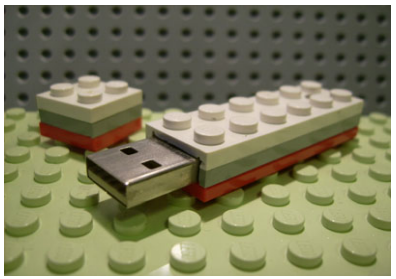
Digital evidence è una *qualsiasi informazione, con valore probatorio, che sia o meno memorizzata o trasmessa in un formato digitale* (Scientific Working Group on Digital Evidence - SWGDE).

Digital Evidence è *l'insieme di tutti quei dati inclusi quelli derivanti dalle risultanze registrate da apparati analogici e/o digitali creati, processati, memorizzati o trasmessi da qualsiasi apparecchio, elaboratore elettronico o sistema elettronico, o comunque disseminati a mezzo di una rete di comunicazione, rilevanti ai fini di un processo decisionale* (*Stephen Mason, Electronic Evidence. Discovery & Admissibility, LexisNexis Butterwoorths,* Londra, 2007)

Documento informatico è qualsiasi rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (l'art. 1 lett. p) del D.lgs. 82/05)

Cosa è la *digital evidence?*

Cosa è la *digital evidence?*

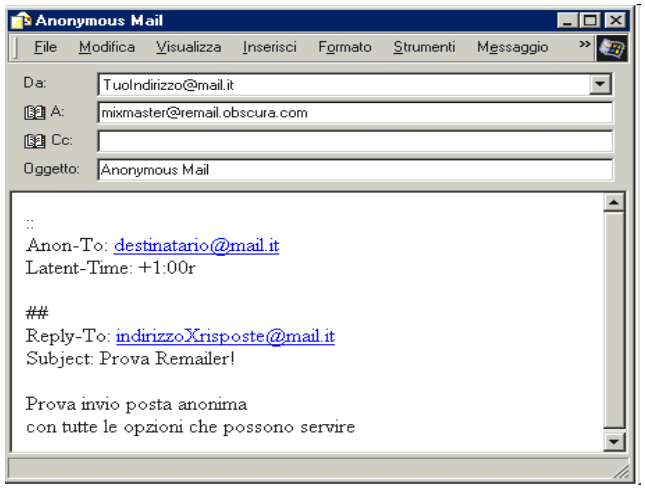


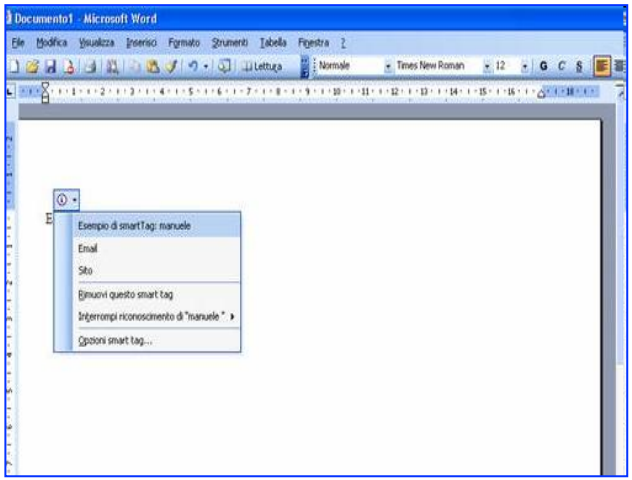
Le classificazioni della *digital evidence*

Si possono avere tre diverse tipologie di prova digitale:

Creata dall'uomo: ogni dato digitale che figuri come il risultato di un intervento o di un'azione umana e può essere di due tipi:

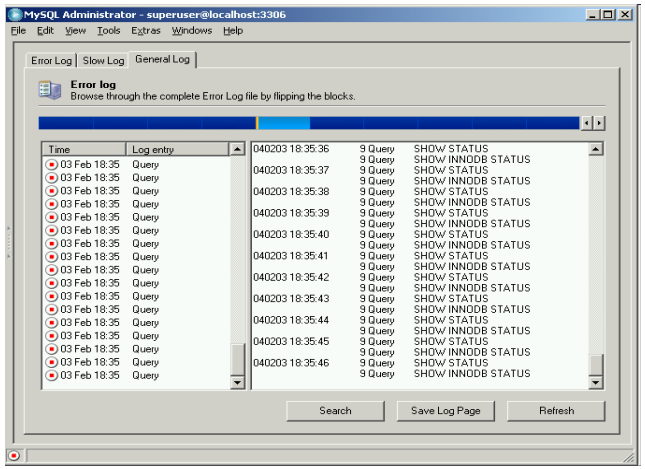
a) Human to human (mail)
b) Human to PC (documento word)

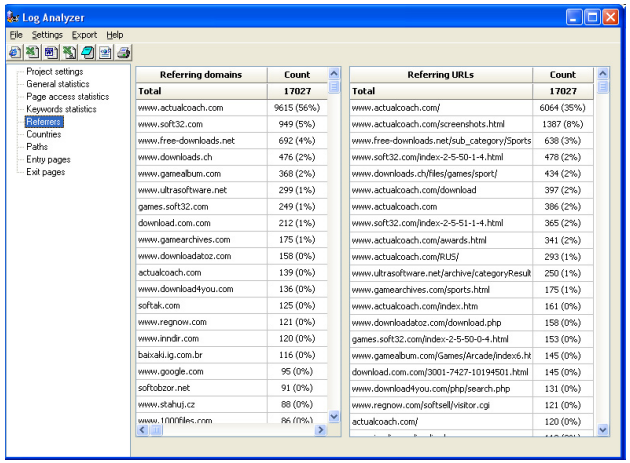




Le classificazioni della *digital evidence*

Creata autonomamente dal computer: ogni dato che figuri come il risultato di un processo su dei dati effettuato da un software secondo un preciso algoritmo e senza l'intervento umano (tabulati telefonici, file di log di un Internet Service Provider)





Le classificazioni della *digital evidence*

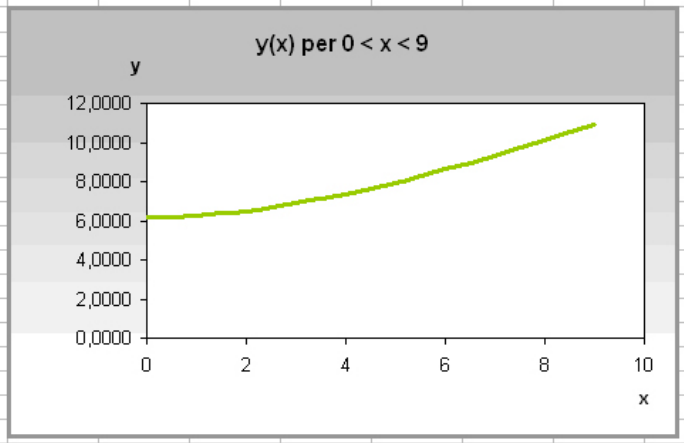
Creata sia dall'essere umano che dal computer: foglio di calcolo elettronico dove i dati vengono inseriti dall'essere umano, mentre il risultato viene effettuato dal computer

Calcolo del profilo di base

Condizioni iniziali

Incremento di x (cm)	0,5
Addendo	38,3

x	y^2	y
0	38,30	6,1887
0,5	38,55	6,2089
1	39,30	6,2690
1,5	40,55	6,3679
2	42,30	6,5038
2,5	44,55	6,6746
3	47,30	6,8775
3,5	50,55	7,1099
4	54,30	7,3689
4,5	58,55	7,6518
5	63,30	7,9561
5,5	68,55	8,2795
6	74,30	8,6197
6,5	80,55	8,9750
7	87,30	9,3434
7,5	94,55	9,7237
8	102,30	10,1143
8,5	110,55	10,5143
9	119,30	10,9225



Le prove atipiche e la digital forensics: prova scientifica

1923 *"I dati su cui si basa la deduzione devono avere raggiunto un tale giudizio di consenso da essere **generalmente accettati nello specifico campo scientifico**"*
(Frye v. US 293 F. 1013, 1014 – D.C. Cir. 1923)

1993 *"**Spetta al giudice** il ruolo di effettivo e diretto gatekeeper, per la formazione di ogni singola prova scientifica secondo i seguenti criteri*

1. ***Controllabilità** e falsificabilità della teoria scientifica*
2. ***Peer review** o revisione critica degli esperti del settore*
3. *Indicazione del margine di **errore conosciuto** o potenziale*
4. *Esistenza di **standards di applicazione** e*
5. *Accettazione generale da parte della **comunità scientifica***

(Daubert v. Merrel Dow Farmaceuticals Inc., 113 S. Ct. 2786 – 1993)

2012 In sostanza Le prove devono essere **rilevanti, idonee, utili, affidabili, attendibili**

Cosa è la *digital forensics ?*

Come Sherlock Holmes nel XIX secolo si serviva costantemente dei suoi apparecchi per l'analisi chimica, oggi nel XXI secolo egli non mancherebbe di effettuare un'accurata analisi di computer, di telefoni cellulari e di ogni tipo di apparecchiatura digitale (Ralph Losey).

Scopo della **digital forensics** *è quello di conservare, identificare, acquisire, documentare o interpretare i dati presenti in un computer. A livello generale si tratta di individuare le modalità migliori per:*

- acquisire le prove senza alterare il sistema informatico in cui si trovano;

- garantire che le prove acquisite su altro supporto siano identiche a quelle originarie;

- analizzare i dati senza alterarli (Cesare Maioli)

Le cinque fasi delle indagini digitali

Il fine ultimo di ogni investigazione digitale consiste nel recupero di tutti i dati che possano costituire una prova utilizzabile durante il processo. Per raggiungere tale fine è necessario:

1. **individuare il supporto informatico** che contiene il dato digitale utile all'indagine, al fine di identificare il potenziale criminale;
2. **acquisire tale dato** attraverso l'intercettazione nel caso di flussi di comunicazioni in Rete, ovvero attraverso il sequestro e la duplicazione del supporto di memorizzazione su cui è archiviato il dato;
3. **conservare in un luogo idoneo** tutti i dati digitali acquisiti e duplicati;
4. **effettuare**, esclusivamente sulla copia del supporto informatico, le **opportune analisi** che consentano di recuperare le informazioni utili al Pubblico Ministero e all'avvocato durante la fase delle indagini preliminari, e al Giudice durante la fase dibattimentale;
5. **presentare i risultati dell'indagine durante la fase dibattimentale** o nella relazione tecnica.

La legge 48/08 di ratifica della convenzione Cybercrime

- **Ispezione (244 c.p.p.) e Perquisizione (247 c.p.p.)**: la legge 48/2008 di ratifica della convenzione "Cybercrime" ha modificato l'articolo 244 c.p.p. sancendo che: "è disposta l'ispezione, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la **conservazione** dei dati originali e ad impedirne l'**alterazione**".

- **Accertamenti urgenti (354 c.p.p.)**: "in relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano **le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità**"

- **Sequestro presso provider (254-bis)**: "nel caso di sequestro di dati informatici presso fornitori di servizi telematici e di telecomunicazioni, l'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, **può disporre 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**.

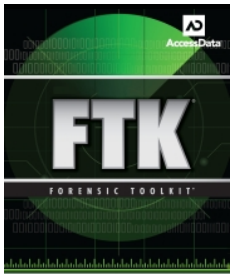
Copia Bit-Stream

Nel caso in cui si volesse validare il contenuto di una e-mail o dell'intero hard-disk è necessario procedere ad un particolare tipo di copia effettuando la *bit-stream image* in grado di "clonare" l'intero hard-disk.

La copia bitstream è un particolare tipo di duplicazione in cui il contenuto dell'unità fisica viene letto sequenzialmente caricando la minima quantità di memoria di volta in volta indirizzabile, per poi registrarla nella stessa sequenza su di un comune file binario generando un file di immagine fisico del supporto originale.

Algoritmo di Hash

L'Hash è una funzione univoca operante in un solo senso (ossia, che non può essere invertita), attraverso la quale viene trasformato un documento di lunghezza arbitraria in una stringa di lunghezza fissa, relativamente limitata.



I due problemi della digital forensics: Cloud Computing

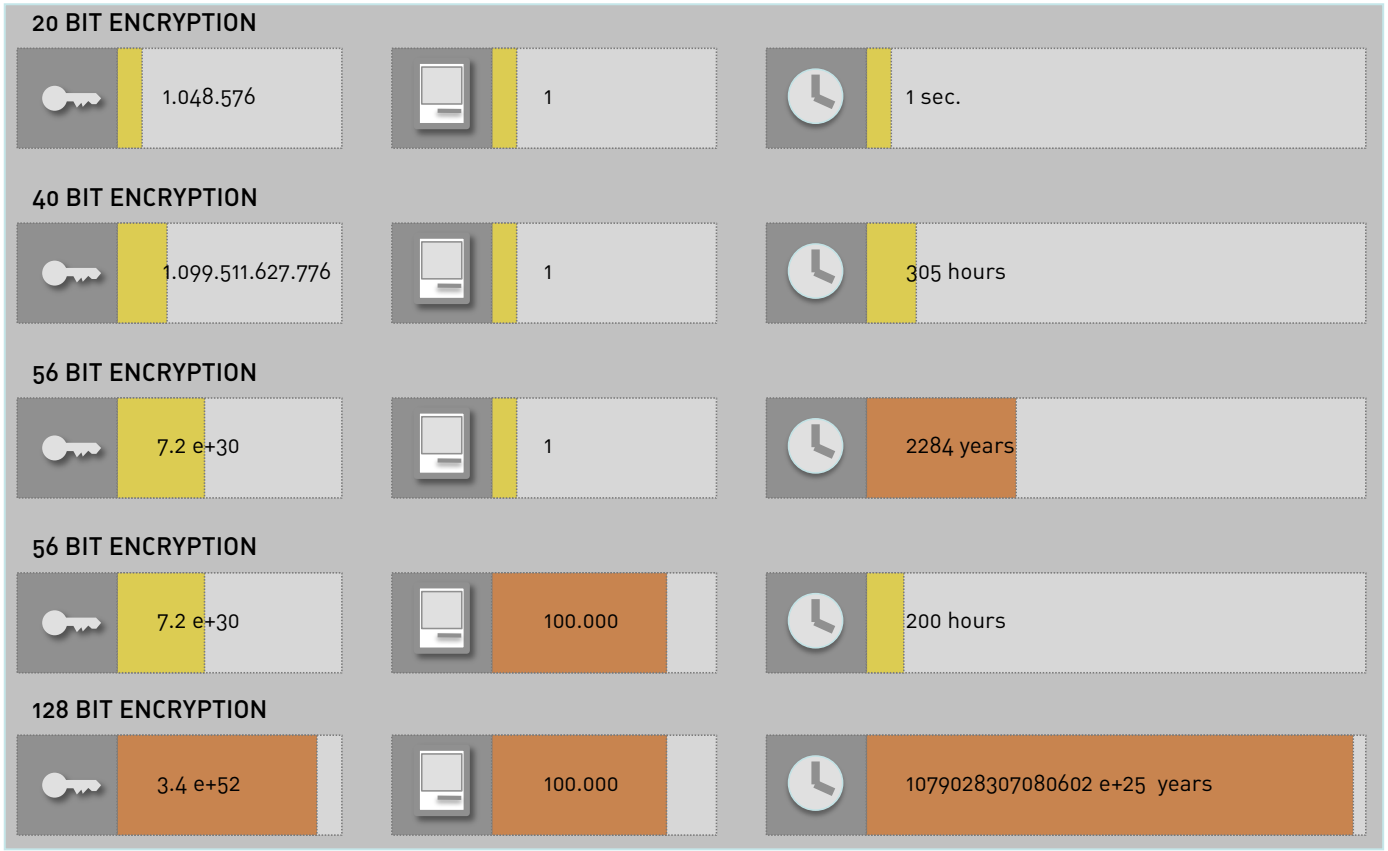
La nuova sfida della digital forensics derivante dal cloud computing è data dalla difficoltà di localizzare I dati:

- “Data at rest” non risiedono sul supporto
- “Data in transit” non possono essere analizzati a causa della cifratura
- “Data in execution” sono presenti solo in “cloud”

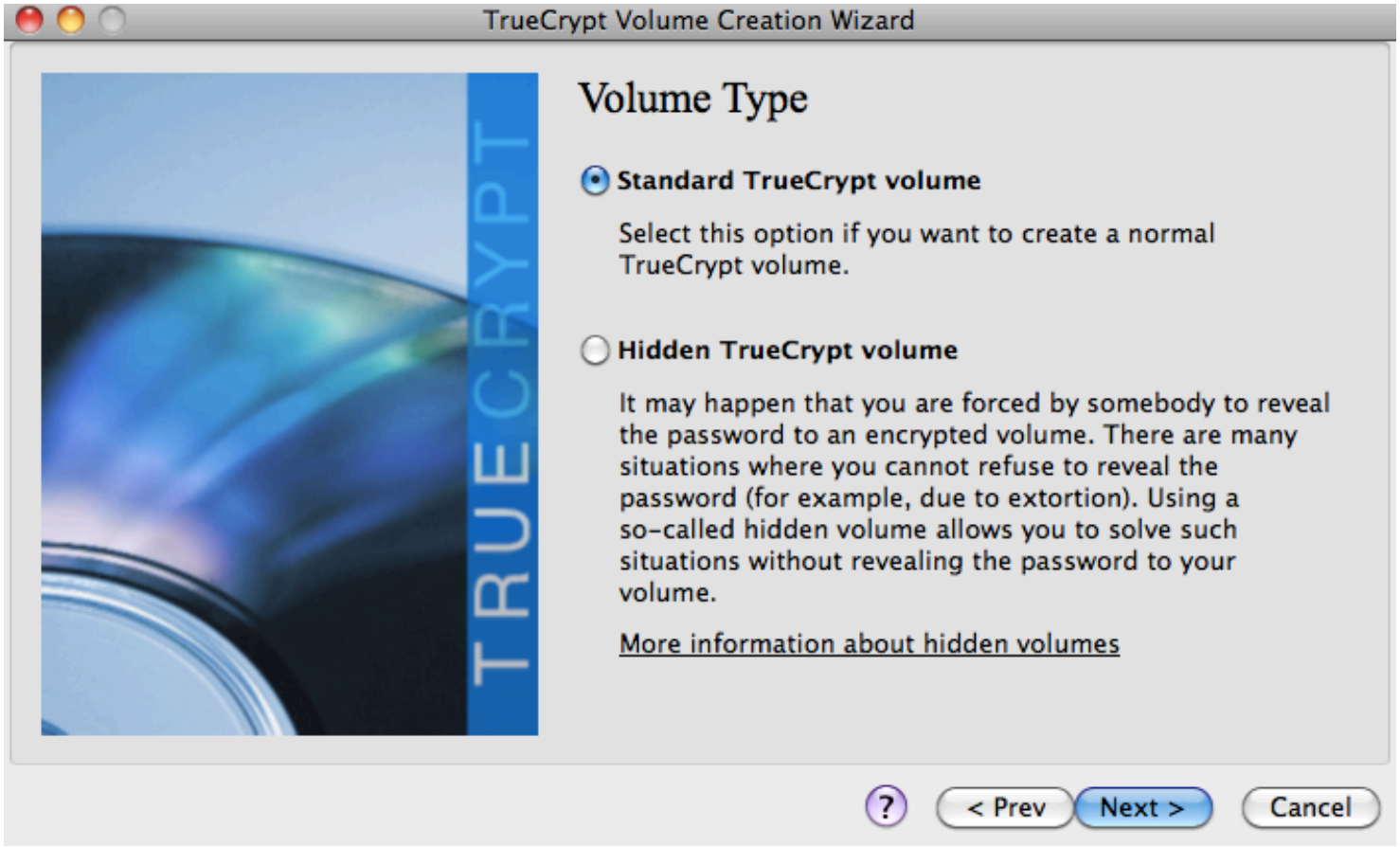
L’investigatore che vuole effettuare una copia forense dei dati (bit-stream image) riconducibili all’indagato si troverà nella stessa situazione di un soggetto che deve completare un complicato puzzle i cui pezzi sono sparsi in giro per il mondo.

Decifrare un testo crittografato è semplice.

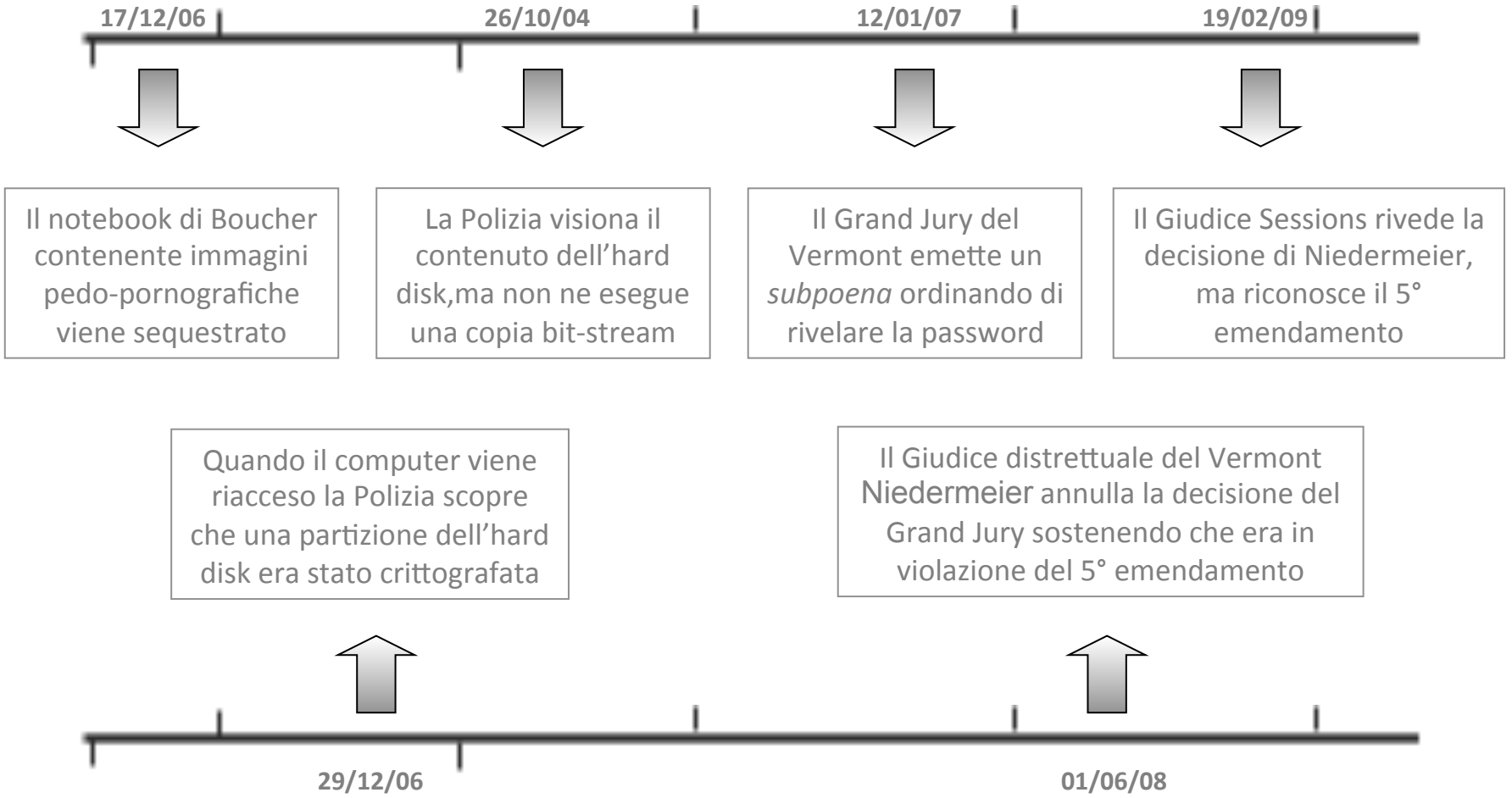
Il problema è: in questo tempo?



Indagini digitali: True Crypt



Indagini digitali: Il caso “Boucher”: la scansione temporale



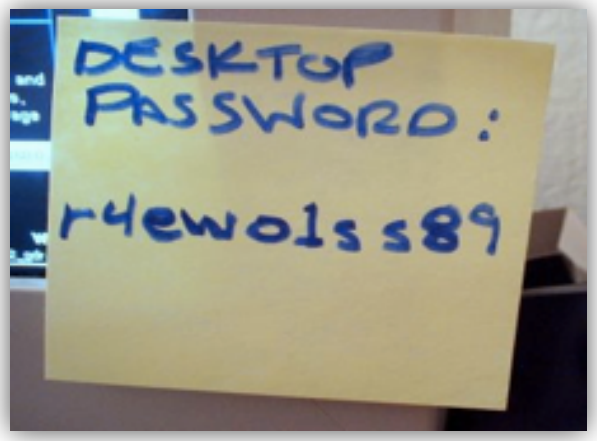
Indagini digitali: “Mandatory Key Disclosure Laws”

A livello internazionale alcuni Stati hanno previsto delle specifiche disposizioni normative che impongono di rivelare la chiave di cifratura alle forze di polizia.

In **Australia**, le forze dell’ordine hanno il potere di chiuedere a chiunque la chiave di cifratura.

In **Belgio** e in **Francia** invece è possibile ordinare solo a terzi (vedi fornitori di connettività e Internet Service Providers) di rivelare la chiave di cifratura.

L’**Italia** non ha un normativa in questo senso….forse perché non serve ?



Tali strumenti legislativi non funzionano. Perché?

1. **Ragioni tecniche**: un soggetto esperto può sempre trovare un metodo per nascondere un file.

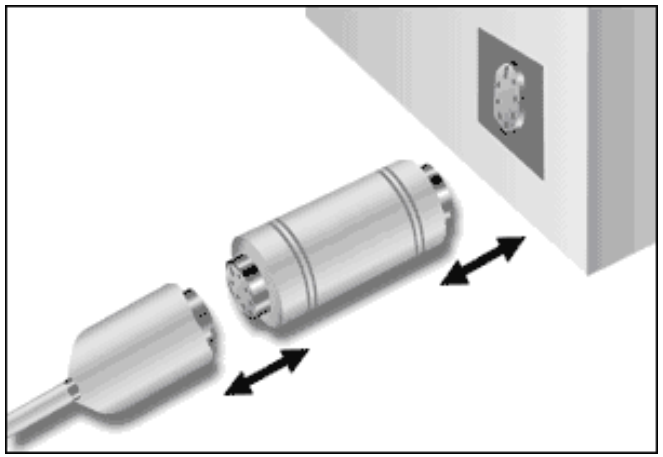
2. **Possibile violazione della Convenzione Europea sui Diritti dell'Uomo**: Articolo 6 *Ogni persona accusata di un reato è presunta innocente fino a quando la sua colpevolezza non sia stata legalmente accertata.*

Una soluzione di natura tecnica esiste ?

Un keylogger è, nel campo dell'informatica, uno strumento in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio computer. Esistono vari tipi di keylogger:

Hardware: vengono collegati al cavo di comunicazione tra la tastiera ed il computer o all'interno della tastiera.

Software: programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente.



Garanzie dell'indagato vs indagini digitali: Legge Nord Westfalia

- La Germania ha introdotto il 20 dicembre 2006 un emendamento alla legge sulla protezione della Costituzione nel Nord Reno-Westfalia che consentiva l'accesso segreto a sistemi informatici e il monitoraggio segreto della Rete attraverso sistemi *keylogger* installati in forma di *trojan horse.*

- La Corte Costituzionale tedesca il 27 febbraio 2008 ha dichiarato incostituzionale tale emendamento sostenendo che violava il **"diritto alla riservatezza ed alla integrità dei sistemi informatici".**

Risk of a wrong forensic analysis – Detecting Illegal Contents

German government accused of spying on citizens with state-sponsored Trojan

Facebook Backdoor Interception: FBI wants P2P and social media wiretap-friendly

The Telegraph

Ministers accused of retreat over internet surveillance plans

House approves CISPA despite last-minute push by opponents

II. Acquisizione della *digital evidence: remote forensics*

Cassazione Penale, Sez. V, 14 ottobre 2009, n. 16556

La giurisprudenza di legittimità ha ritenuto legittimo un decreto del Pubblico Ministero che, ai sensi dell'art. 234 c.p.p., disponeva l'acquisizione in copia attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel personal computer in uso all'imputato e installato presso un ufficio pubblico.

La Suprema Corte ha, infatti, evidenziato come il provvedimento del Pubblico Ministero non avesse riguardato un flusso di comunicazioni, ma **la semplice estrapolazione di dati già formati e contenuti nella memoria del "personal computer", ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer**.

II. Acquisizione della *digital evidence*: *remote forensics*

La Convenzione sul Cybercrime ha dettato alcune norme che potrebbero permettere un'attività investigativa da remoto:

L'art. 18 (**Production order**) ha introdotto la possibilità per l'Autorità Giudiziaria di ordinare a qualunque soggetto di fornire i dati digitali presenti all'interno di un sistema informatico in suo possesso o sotto il suo controllo.

L'art. 19 (**Search and seizure of stored computer data**) stabilisce che la Polizia Giudiziaria è autorizzata ad estendere la ricerca su dati che risiedono all'interno di un altro server, salvo che non si trovi al di fuori del territorio nazionale.

L'art. 20 (**Real-time collection of traffic data**), infine, prevede la possibilità di raccogliere in tempo reale i traffic data, che servono a monitorare in tempo reale l'attività dell'indagato in Rete.

II. Acquisizione della *digital evidence*: sequestro o copia bit-stream?

3 ragioni a favore del sequestro fisico dell'hard disk:

1. Molto spesso, si procede al sequestro di materiale informatico nell'ambito di indagini legate al contrasto della pirateria informatica (legge 633/41 e successive modifiche) o della pedo-ponografia (artt. 603-ter e quater c.p.): in entrambi i casi è prevista, in caso di condanna, la confisca degli strumenti e dei materiali utilizzati per compiere i relativi reati (art. 171-sexies legge 633/31 e art. 600-septies c.p.).

2. L'indagato, ai sensi dell'articolo 258 c.p.p., ha diritto di chiedere all'Autorità Giudiziaria che sia estratta gratuitamente la copia dei dati contenuti all'interno dell'hard disk, a condizione che sia in grado di dimostrare la legittimità del possesso del supporto.

3. La terza, già menzionata, è che un procedimento di copia forense di un hard disk può avere una durata incompatibile con l'esecuzione, in tempi ragionevoli, del mezzo di ricerca della prova.

II. Acquisizione della *digital evidence*: sequestro di corrispondenza

L'articolo 254 c.p.p., prevede che le carte e gli altri documenti sequestrati che **non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto** e non possono comunque essere utilizzati.

La legge 48/2008 ha assimilato la corrispondenza cartacea a quella telematica **consentendo all'autorità giudiziaria di disporre il sequestro presso il server che ospita la corrispondenza elettronica** dell'indagato ordinando una copia del contenuto presente all' interno del server.

II. Acquisizione della *digital evidence*: sequestro di corrispondenza

Tribunale di Brescia, 4 ottobre 2006

Il sequestro di un intero hard-disk consente certamente l'acquisizione di elementi probatori, ma implica anche l'**acquisizione di dati che esulano dal contesto per il quale l'atto e disposto**, sicché, come è immediatamente percepibile, tale genere di sequestro esige un ambito di corretta e ristretta operatività **per evitare connotazioni di spropositata afflittività e di lesione di beni costituzionalmente protetti**. Sotto questo profilo merita particolare segnalazione la compressione della **libertà e segretezza della corrispondenza conservata nel disco fisso**, con conoscenza dei messaggi tutti trasmessi e ricevuti, compresi quelli destinati a soggetti del tutto estranei alle indagini.

Tale decisione è stata confermata dalla **Corte di Cassazione** (*Cass. pen., sez. VI, 31 maggio 2007, n. 40380*).

II. Acquisizione della *digital evidence*: *L'esperienza US*

La Rule 41 Federal Rules of Criminal Procedure chiarisce che per ottenere un mandato (**warrant**) di perquisizione e sequestro **(search and seizure**), è necessario che l'agente che ha svolto le indagini sottoscriva una dichiarazione (**affidavit**) che dovrà essere sottoposta (**application**) al vaglio di un Giudice competente in materia (**magistrate**)

Le Corti statunitensi hanno ritenuto legittimo il sequestro qualora:

- la prova digitale sia inviata a una terza persona (Third-Party Possession) ;
- la prova digitale sia stata scoperta e comunicata all'Autorità Giudiziaria da parte di un privato (Private Search) ;
- vi sia il consenso dell'indagato, della moglie/marito dello stesso (Consent);
- un provider e la polizia trovino un accordo per lo scambio di informazioni (Exigent Circumstances);
- sia stato effettuato il legittimo arresto del soggetto indagato (Search after a lawful arrest);
- la prova digitale emerga *ictu oculi* (Plain View) ;
- la prova sia scoperta durante un controllo alla frontiera (Border Search) ;
- sia ricercata la prova all'interno di un ufficio pubblico (Public-Sector Workplace Searches) .

III. Conservazione della *digital evidence*: custodia e apposizione sigilli

Art. 259 c.p.p.: "Custodia delle cose sequestrate"

Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi.

Art. 260 c.p.p. "Apposizione dei sigilli alle cose sequestrate"

L'autorità giudiziaria fa estrarre copia dei documenti [...] Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata 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.

III. Conservazione della *digital evidence*: custodia e apposizione sigilli

Se il bit è eterno, il suo supporto non lo è affatto. I supporti digitali durano meno di quelli analogici e i dispositivi per leggere i supporti durano ancora meno.

Domesday Book (1086): Inchiostro su pergamena: leggibile dopo **oltre 900 anni.**

Domesday Book 2 (1983): LaserDisc: **illeggibile dopo 15 anni.**

A LaserDisc (left), compared with a DVD.

IV. Analisi della *digital evidence – atto ripetibile o irripetibile?*

ATTO RIPETIBILE

Cass. Pen. Sez. I, 5 marzo 2009, n. 14511; conformi Cass. Pen. Sez. I, 26 febbraio 2009, n. 11863 Cass. Pen. Sez. III, 02 luglio 2009, n. 38087; Cass. Pen. Sez. III, 25 febbraio 2009, n. 11503

Fatto: La Polizia Giudiziaria preleva (copia), ai sensi dell'art. 258 c.p.p. alcuni file dall'hard disk dell'indagato senza il rispetto di alcuna procedura di *digital forensics*.

La Corte ha affermato il principio secondo cui "*è da escludere che l'attività di estrazione di copia di file da un computer costituisca un atto irripetibile [...], atteso che non comporta alcuna attività di carattere valutativo su base tecnico-scientifica né determina alcuna alterazione dello stato delle cose, tale da recare pregiudizio alla genuinità del contributo conoscitivo nella prospettiva dibattimentale, essendo sempre comunque assicurata la riproducibilità di informazioni identiche a quelle contenute nell'originale*".

ATTO IRRIPETIBILE

Cass. Pen. Sez. III, 09 giugno 2009, n. 28524

Fatto: L'avvocato della difesa aveva richiesto di poter effettuare una copia bit-stream dell'hard disk ai sensi dell'art. 258 c.p.p. e non gli era stata concessa.

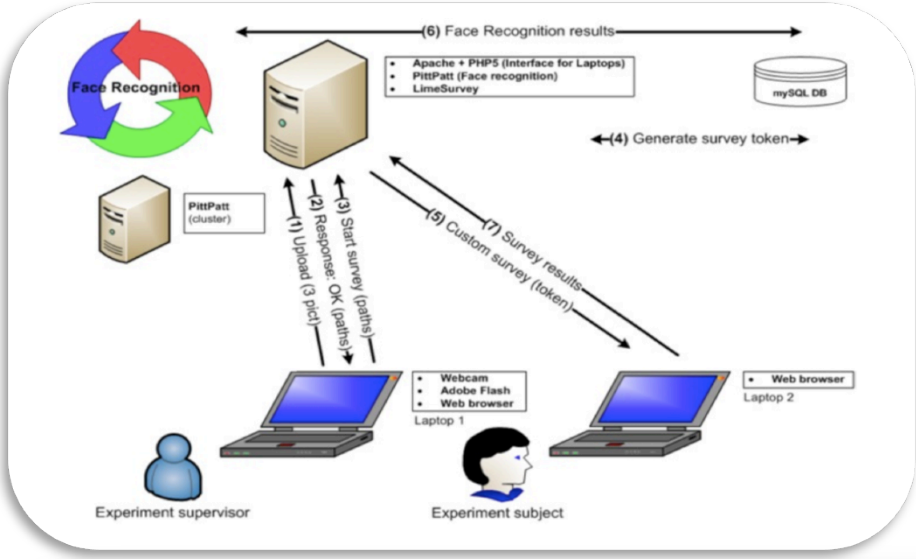
"*L'esame dell'hard disk di un computer in sequestro e la conseguente estrazione di copia dei dati ivi contenuti non sono attività che le parti possono compiere durante il termine per comparire all'udienza dibattimentale senza contraddittorio e alla sola presenza del custode, in quanto implicano accertamenti ed interventi di persone qualificate e l'utilizzo di appositi strumenti, sì che devono essere necessariamente svolti in dibattimento, nel contraddittorio e sotto la direzione del giudice*".

V. Presentazione della *digital evidence*: “Murtha Case”

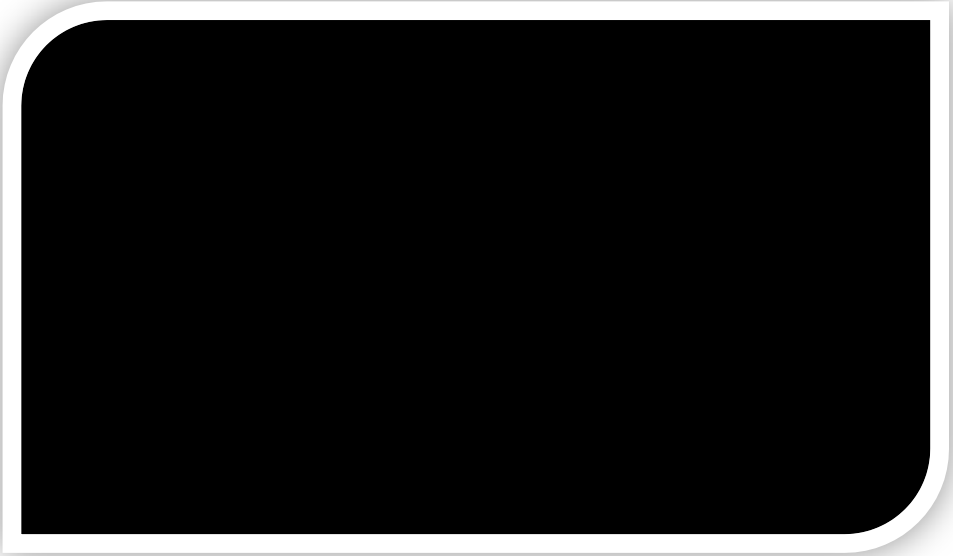
La cultura audiovisiva sta cambiando il mondo e la giustizia. È difficile dire se questo sia un bene, ma è sicuramente un dato di fatto. Stiamo assistendo, attraverso il computer, a una moltiplicazione del concetto d’immagine: abbiamo video e foto digitali, scene del crimine elaborate digitalmente, animazioni al computer, presentazioni multimediali, slides e molto di più.

Privacy vs Security

Face Recognition Project
Alessandro Acquisti



Date Check
Intelius



Grazie per l'attenzione

Giuseppe Vaciago

Mail: giuseppe.vaciago@htlaw.it
Blog: http://infogiuridica.blogspot.it
Linkedin: http://it.linkedin.com/in/vaciago