



LE PROVE INFORMATICHE, TRA QUESTIONI CIVILI E PENALI

CAMERA CIVILE VENEZIANA

IL TRATTAMENTO DEI REPERTI INFORMATICI NELL'AMBITO DEI PROCEDIMENTI FAMILIARI: METODOLOGIA E CASI REALI

Informatica Forense

Informatica forense è la disciplina che concerne le attività di individuazione, conservazione, protezione, estrazione, documentazione ed ogni altra forma di trattamento ed interpretazione del dato memorizzato su supporto informatico, al fine di essere valutato come prova nel processo.

Informatica forense studia a fini probatori i processi, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici (memorie, hard disk, dischetti, nastri, cartaceo, etc.), nonché l'analisi forense di ogni sistema informatico e telematico (computer, rete di computer, ed ogni altro dispositivo per il trattamento di dati in formato digitale), l'esibizione della prova elettronica, l'esibizione del dato digitale, il recupero di dati e la loro esibizione, l'analisi ed esame del sistema informatico e telematico.

Cesare Maioli

Informatica Forense

"Noi abbiamo i fatti" dicono.

*Ma i fatti non sono tutto; almeno metà della
faccenda sta nel sapere come comportarsi coi
fatti!"*

"E tu ti sai comportare coi fatti?"

Da "delitto e castigo" di Fjodor Dostoevskij

Informatica Forense

"E tu ti sai comportare coi fatti?"

LA PROVA DI RESISTENZA ...

la "*forma mentis*" del tecnico ...

Informatica Forense



donato@informaticaforensi.it

5

Limiti dell'Informatica Forense

- Estrema alterazione dei reperti
- Facile creazione ad arte di elementi probatori
- Difficile riconducibilità dei reperti ai veri autori

Limiti dell'Informatica Forense

- È necessaria una profonda attività di autocritica
- Il reperto informatico è alquanto ingannevole
- Bisogna ricercare in maniera paranoica elementi di riscontro

Limiti dell'Informatica Forense

Diffidenza!

**Soprattutto su quanto
si è accertato**

Caso tipico

Indirizzo IP

- Individua univocamente in un preciso istante un sistema in una rete
- Declinazione Internet:
individua univocamente in un preciso istante una utenza telefonica

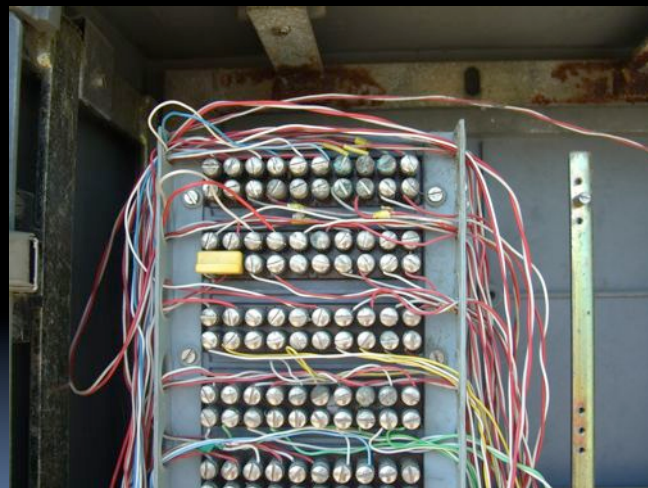
La realtà



La realtà



La realtà



Amarcord

- Un caso del 1994: un dischetto come alibi informatico
- Un altro caso sempre del 1994: il Notaio smemorato

L'effimero valore probatorio del bit

- Allorché viene generata la successione di bit, sussiste la possibilità che almeno un operatore possa in un preciso momento modificarne la successione
- Ugualmente, nel caso di bit registrati su supporti non scrivibili, una modifica è sempre possibile, atteso che prima che i bit vengano registrati sul supporto possono subire alterazioni

L'effimero valore probatorio del bit

- “analizzando il supporto su cui sono registrati i bit, non è possibile accertare ed individuare eventuali modifiche apportate in precedenza ai singoli bit”, non consentendo la successione di bit di capire se gli stessi in precedenza abbiano assunto valori diversi in seguito modificati

donato@informaticaforense.it

15

De dato informatico: presunzione di ripudio

- La possibilità della modifica di una successione di bit andrebbe presuntivamente considerata come avvenuta
- Se in un procedimento viene prodotto in giudizio un dato informatico, lo stesso andrebbe presuntivamente considerato come modificato ad arte, dovendo la parte interessata alla sua acquisizione nel processo dimostrarne l'attendibilità.

donato@informaticaforense.it

16

Tormentone “GARLASCO” e non solo...

Casistiche:

- Il reperto consegnato dal teste...
- Il reperto consegnato dal datore di lavoro

La fase di “valutazione” del reperto

- Ecco perché è necessario anche un momento di valutazione del reperto, anche se il bit può assumere solo il valore di 0 o 1

LA FASE DI “VALUTAZIONE” DEL REPERTO

Perché il reperto informatico può essere facilmente:

- alterato
- inquinato
- contraffatto

LA FASE DI “VALUTAZIONE” DEL REPERTO

Inoltre, bisogna verificare se le operazioni di acquisizione del reperto informatico sono state legittime

LA FASE DI “VALUTAZIONE” DEL REPERTO

Quindi vanno espressi giudizi di merito circa:

- l'attendibilità
- l'integrità
- l'autenticità

del reperto stesso

DE REPERTO INFORMATICO

5 fasi trattamento:

- individuazione
- acquisizione
- analisi
- valutazione
- presentazione

L'IMPORTANZA DI UN APPROCCIO METODOLOGICO

L'INDIVIDUAZIONE....





ACQUISIZIONE DEL REPERTO INFORMATICO:

va accuratamente documentata

per dare garanzia del rispetto dei principi esaminati, tutte le operazioni eseguite in fase di acquisizione vanno accuratamente documentate, meglio se si utilizzando dei dispositivi che registrano automaticamente quanto viene eseguito

© Donato Eugenio Caccavella

Acquisizione del reperto informatico:



donato@informaticaforense.it

Acquisizione del reperto informatico:



donato@informaticaforense.it

Acquisizione del reperto informatico:



donato@informaticaforensi.it

Acquisizione del reperto informatico:



donato@informaticaforensi.it

Acquisizione del reperto informatico:



donato@informaticaforense.it

Acquisizione del reperto informatico:



donato@informaticaforense.it

Acquisizione del reperto informatico:



donato@informaticaforense.it

Acquisizione del reperto informatico:



donato@informaticaforense.it

Caso “la scrittrice”

Marito incarica un investigatore
“PRIVATO” il quale:

Oltre a scattare foto...

Svolge anche un accertamento tecnico
sul PC Portatile utilizzato dalla
“controparte”

Caso “la scrittrice”

Marito incarica un investigatore “PRIVATO” il
quale:

Oltre a scattare foto...

Svolge anche un accertamento tecnico sul PC
Portatile utilizzato dalla “controparte”

Caso “la scrittrice”

Vengono estratte
alcune e-mail
considerate la prova del
“tradimento”

Caso “la scrittrice”

Si pongono in questo caso
diverse problematiche:

- Attendibilità dei reperti
prodotti da controparte

Caso “la scrittrice”

Diverse ipotesi di reato nei confronti dell'investigatore:

- Accesso abusivo a sistema informatico
- Violazione della corrispondenza

Caso “la scrittrice”

La strategia dell'Avvocato
Penale
Vs
Civile

Caso “la scrittrice”

Fu scelta la linea
“civilistica” di
disconoscimento della
corrispondenza prodotta
dalla controparte

De dato informatico: presunzione di ripudio

- La possibilità della modifica di una successione di bit andrebbe presuntivamente considerata come avvenuta
- Se in un procedimento viene prodotto in giudizio un dato informatico, lo stesso andrebbe presuntivamente considerato come modificato ad arte, dovendo la parte interessata alla sua acquisizione nel processo dimostrarne l'attendibilità.

De dato informatico: presunzione di ripudio

- Anche gli SMS possono essere modificati o creati ad arte sul dispositivo dove sono presenti
- E' possibile inviare degli SMS facendo risultare un altro mittente

Caso “monopoli”

Una signora lamenta
che il marito si è auto
inviato una mail
utilizzando l'account
della moglie...

Caso “monopoli”

In tale mail la moglie ammetteva l'accordo verbale di cedere al marito l'appartamento di “Via Cavour”

Caso “monopoli”

L'accertamento:

- Finalizzato a supportare la querela
- disconoscere a paternità della mail
- ricordiamo che in parallelo c'era una separazione giudiziale

Caso “monopoli”

L'accertamento:

- Web mail
- Disamina degli header
- Incongruenza della geo-localizzazione degli IP

Caso “monopoli”

L'accertamento:

Individuare elementi di riscontro che corroborino la querela

Caso “monopoli”

Riflessione:

Accertamento tecnico non particolarmente sofisticato, dove la componente divulgativa e di “presentazione” è fondamentale per l’efficacia alla relazione stessa

Caso "Galeotto fu Facebook"

La moglie accede al computer del marito:
legge e stampa tutti i messaggi amorosi
che lui aveva scambiato con altre donne

Caso "Galeotto fu Facebook"

Le "riproduzioni su carta" vengono prodotte
nella causa di separazione....

Caso "Galeotto fu Facebook"

Eccezioni:

non si ha garanzia di integrità

non si ha garanzia di autenticità

Caso "Galeotto fu Facebook"

Anche se viene coinvolto un ...

Notaio

Nuove fattispecie

Stalking
(cabine telefoniche e carte telefoniche)

Vs

Artefazione
(modifica ad arte di sms o di e-mail)

Nuove fattispecie

P2P per diffondere
materiale
"imbarazzante" per la
controparte

Nuove fattispecie

In questi casi è
fondamentale un
accertamento eseguito il
prima possibile, prima che il
materiale si diffonda nella
rete

Nuove fattispecie

Inoltre la attività di indagine è piuttosto difficoltosa poiché possono essere numerosi i potenziali diffusori "originari" del materiale.

Grazie
Donato Eugenio Caccavella

Università degli Studi di Bologna
Università degli Studi di Catania

donato@informaticaforense.it

www.periziainformatica.it

Q & A