



COMPUTER FORENSICS
CORSO DI LAUREA IN INFORMATICA
ANNO ACCADEMICO 2012- 2013
CATANIA 11 MARZO 2013

TECNICHE DI TRATTAMENTO DEI REPERTI INFORMATICI

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

Il ruolo del consulente tecnico

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 Fjòdor Dostoevskij

Informatica Forense

- I fatti di oggi…


Innovazione | Uomini & Mezzi | Attività Internazion
link | contatti | pubblicità

sabato 3 marzo 2012, ore 08.23

Enrica Lexie: cancellati i dati nella scatola nera

I dati con la posizione nel giorno dell'incidente non sarebbero stati salvati nel

www.italiavela.it
il cantiere delle idee per la nautica

ARTICOLI CORRE

Pirateria: prolungata la missi EuNavFor Atalanta

Pirateria, Somalia: sequestra Italiana

Pirateria: Confitarma accusa

Pirati attaccano nave italiana

Pirati, attaccata nave italiana

Pirateria: liberata la motonav Valle di Cordoba

Pirateria: Nave Bersagliere ri golfo di Aden

www.ilcorrieredellasicurezza.it

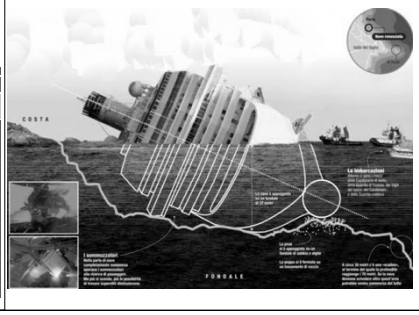
Informatica Forense

- I fatti di oggi…

Concordia, integra la scatola nera sei progetti per rimuovere il relitto

10 marzo 2012 — pagina 7 sezione: FIRENZE

E' COMINCIATA l' analisi da parte dei periti della scatola nera della Costa Concordia, la grande nave da crociera naufragata il 13 gennaio davanti alle coste dell' isola del Giglio. L' integrità del Vdr è stata accertata, primo passo importante nell' inchiesta. Sia secondo la procura, sia in base ai quesiti posti dal gip Valeria Montesarchio, nell' ambito dell' incidente probatorio sulla scatola nera il Vdr è



www.repubblicat.it

Informatica forense

"E tu ti sai comportare coi fatti?"

LA PROVA DI RESISTENZA …

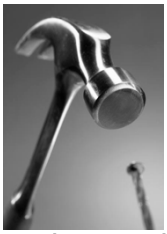
la "*forma mentis"* del tecnico …

Informatica Forense

Informatica Forense

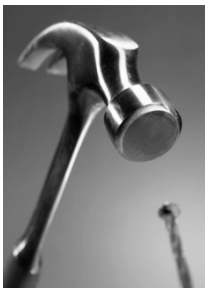
Informatica Forense

Bisogna avere un approccio metodologico….perché?
Il destino di chi esegue l'accertamento tecnico…



Il chiodo, non il martello

Informatica Forense



Solo supportando la attività di accertamento con un rigoroso percorso metodologico il tecnico, il "chiodo" il consulente tecnico potrà confermare le proprie conclusioni attraverso la prova di resistenza "giudiziaria"

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!

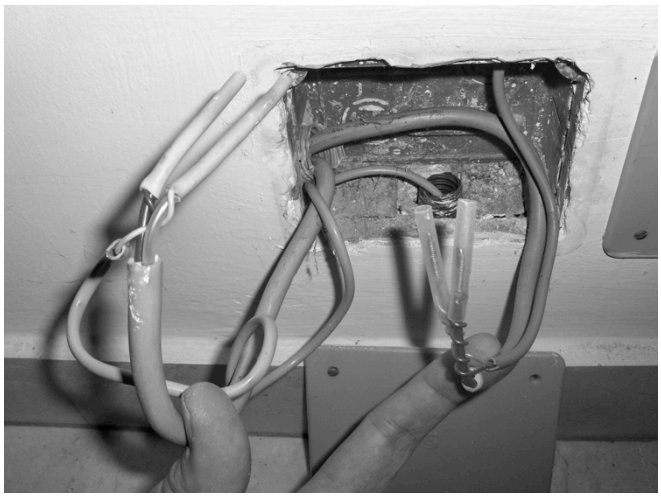
Soprattutto su quanto si è accertato

Caso tipico

Indirizzo IP

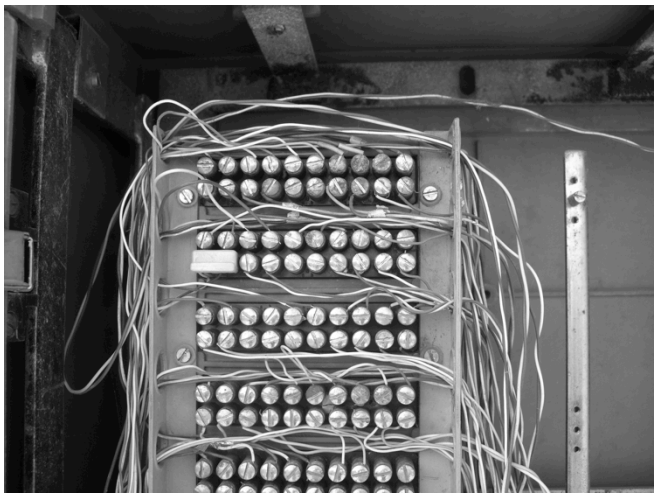
- Individua univocamente in un preciso istante un sistema in una rete
- Declinazione Internet:
  individua univocamente in un preciso istante una utenza telefonica

La realtà



La realtà

La realtà



Ruoli

L'investigatore deve rimanere il dominus dell'indagine e deve governare le tecnologie forensi come meri strumenti di ausilio e non risolutori,

Ruoli

il consulente tecnico deve rimanere nel suo ruolo di tecnico e non sostituirsi al giurista

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

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.

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 operazione 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

LA FASE DI "VALUTAZIONE" DEL REPERTO

integrità

autenticità

Computer Forensics

PROGRAMMA DEL CORSO

Programma del Corso

prima parte metodologica…

- ma operativa fornendo agli studenti un KIT "professionale"
- svolta in laboratorio
- declinare i principi metodologici sul "campo", ossia nella realtà

Programma del Corso

seconda parte simulazione pre-dibattimentale e dibattimentale

- con il supporto di giuristi: avvocati, magistrati e polizia giudiziaria,
- creando gruppi di 4 – 5 studenti che saranno i CT delle diverse parti

Grazie
Dott. Donato Eugenio Caccavella

Q & A