

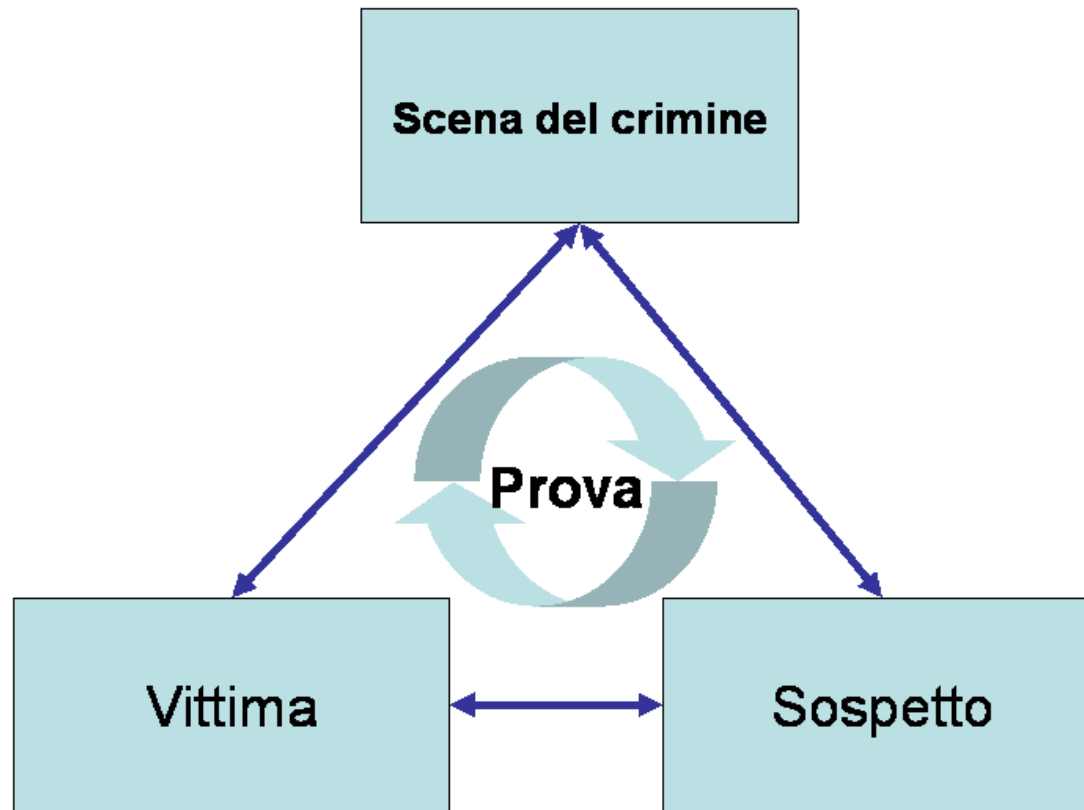
Ing. Gianluigi Me

Computer Forensics

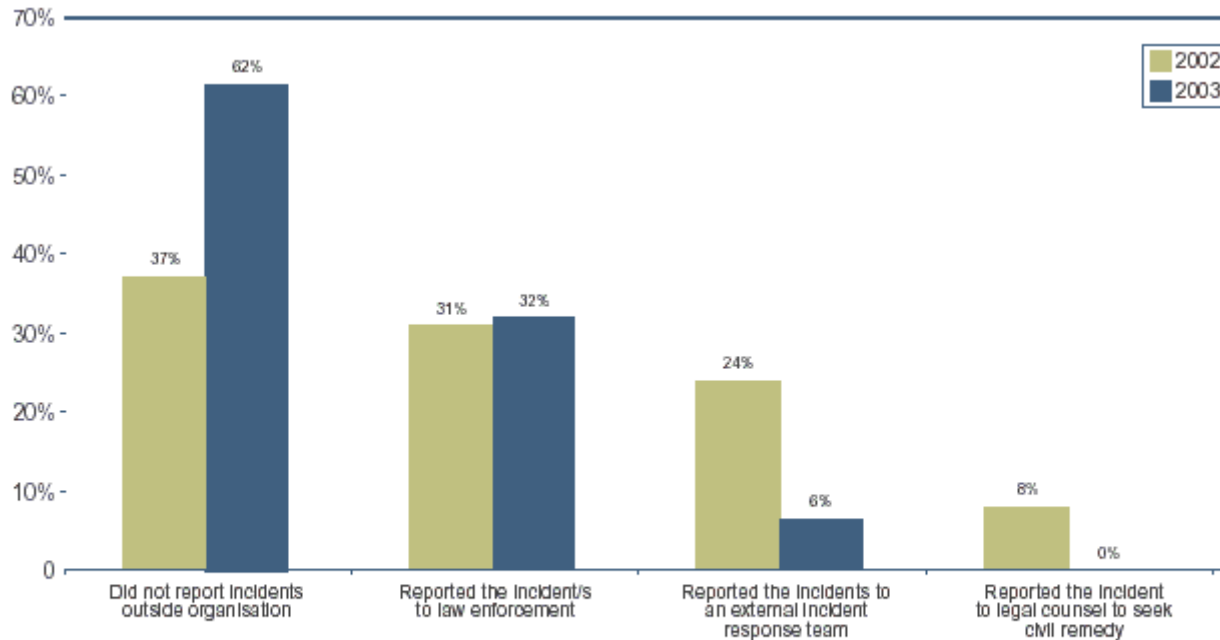
Cosa è Computer Forensics?

La Computer Forensics è l'applicazione di tecniche scientifiche ed analitiche ai Sistemi Operativi ed ai Filesystem al fine di recuperare prove utili (e valide) nell'attività processuale.

La prova secondo Locard



L'approccio aziendale



Source: 2003 Australian Computer Crime and Security Survey
2003: 94 respondents/43%, 2002: 59 respondents/62%

L'approccio aziendale



Source: 2003 Australian Computer Crime and Security Survey
2003: 107 respondents/50%, 2002: 27 respondents/28%

Note: Respondents were asked to give a ranking of 1 - 5 (1 for least important and 5 for most important) for each category.

PROCEDIMENTO A 4 PASSI

- **Acquisizione**
- **Identificazione**
- **Valutazione**
- **Presentazione**

Chi ha bisogno della Computer Forensics?

- La vittima
- Le forze di polizia
- Assicurazioni
- Le aziende
- Il sistema giudiziario

Chi sono le vittime?

- Aziende
- Governo
- Individui

Obiettivi della Analisi Forense

- Identificare il colpevole;
- Identificare il metodo/la vulnerabilità della rete della rete che ha consentito al colpevole di guadagnare l'accesso al sistema;
- Condurre un assessment del danno della rete colpita;
- Conservare correttamente la prova per l'azione giudiziaria;

Tipi di richieste forensi

- Analisi delle intrusioni
- Assessment del danno
- Esame del sospetto
- Tool Analysis
- Analisi dei file di log
- Ricerca della prova

Analisi delle intrusioni

- Chi si è introdotto?
- Cosa ha fatto?
- Quando è accaduto?
- Dove è andato?
- Perché ha scelto questa rete?
- Come ha fatto?

Assessment del danno

- Che cosa ha visto l'intrusore?
- Cosa ha preso?
- Che tracce ha lasciato?
- Dove è andato?

Computer Forensics

Caratteristiche della prova

La prova informatica deve essere...

...come ogni altra prova:

- ammissibile
- autentica
- accurata
- completa
- convincente per il giudice

La prova informatica deve essere...

CONVINCENTE

- Avere un valore probatorio
- Un test pratico di presentazione

Procedure Forensi

- “Congelare la scena del crimine”
 - Procedimento formale
 - imaging
- Mantenere la continuità della prova
 - controlled copying
 - controlled print-out
- Raccolta testimonianze
- ACPO

Catena di custodia

- Una volta in possesso della copia originale del dispositivo, occorre documentare come si conserva
 - Dove è memorizzata
 - Chi ne ha avuto accesso
 - Che operazioni sono state effettuate su di essa
- Questa è la catena di custodia, che fornisce la documentazione provante che l'integrità dei dati è stata preservata e non c'è stata alcuna modifica, seppur casuale.

Catena di custodia

Tecnicamente, si ottiene con

- documentazione,
- hashes,
- timestamps

Tipi di dispositivi

- CD-RWs
- DVD-RWs
- Floppies
- Hard drives
- Flash ram (smart media, memory stick, mmc, secure digital)
- PDA
- Telefoni cellulari

Computer Forensics

Analisi del disco

Richiami sul procedimento forense

- Preparazione
- Protezione
- Imaging
- Esame
- Documentazione

Estrarre, processare, interpretare

- Lavorare sull'immagine o sulla copia sicura
- I dati estratti possono essere in formato binario
- Convertire I dati in un formato comprensibile
 - Reverse-engineer per estrarre informazioni da partizioni di disco, file system, directory, file etc.
 - Software disponibile per questi scopi
- Interpretare I dati, cercare parole chiave, frasi etc.

Problemi aperti

- Problemi sull'uso di tool proprietari per forze di polizia
- disclosure del metodo
- Open source?
- “Parità di armi” con la difesa
- Es: Pedofilia rilascio del materiale alla difesa

Frutto dell'albero avvelenato

- Chiamata anche regola dell'esclusione *exclusionary rule*
- La prova ottenuta in violazione ai diritti di qualcuno non è ammissibile (spyware: Gator, Cydoor, SaveNow, eZula)
- I log sono tutto

Network Monitoring

- Consentito quando:
 - Il sistema è compromesso e si sta monitorando per localizzare ed indentificare un intrusore
 - Quando il monitoraggio è esplicitamente consentito dagli utenti (AUP)
 - Dove le leggi lo consentono

Sporcare le prove

- La prova informatica è “modificabile”
 - Un intrusore potrebbe aggiungere/rimuovere/modificare il contenuto dei log
 - Possono compromettere i componenti del sistema che ospita i log
 - Potresti modificare qualcosa durante l’investigazione

Recupero di file

- File cancellati
- File nascosti
- Slack Space
- Bad Blocks
- Steganografia
- File cifrati
- Partizioni nascoste

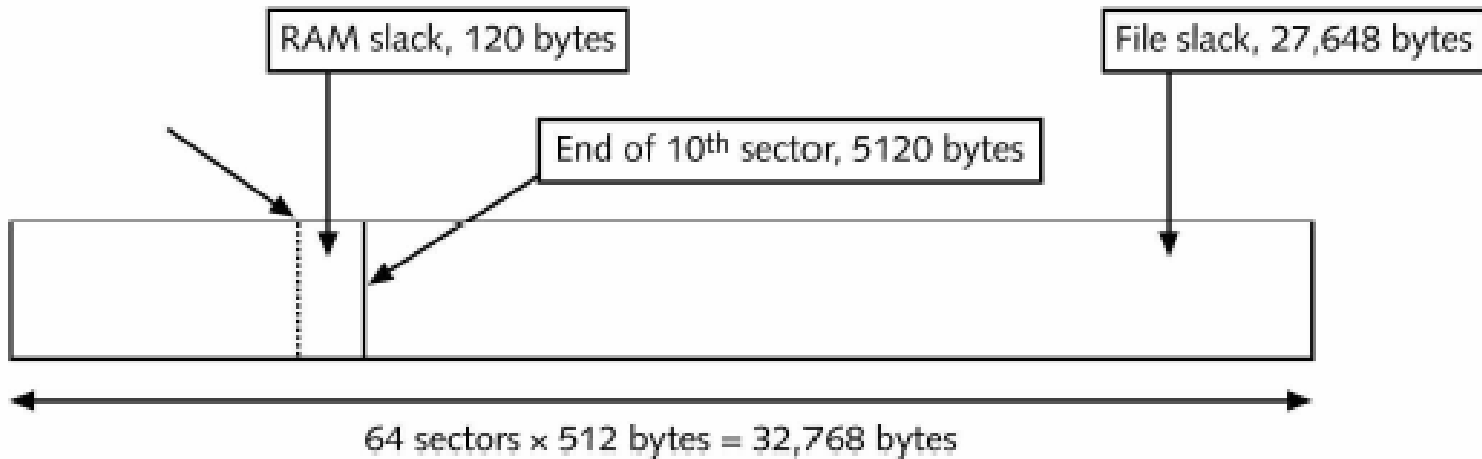
Bit Stream Backup

- Settore per settore
- Mappa il drive originale
- Recupera I file esistenti, RAM slack, file slack

Identificare la prova

- Hard disk nella forma di
 - Swap files
 - Temporary files
 - Unallocated Spazio del disco non allocato
 - Spazio del file slack
- Memoria e Processi in piedi
- Floppy Disks, CD-ROMS, DVDs, Zip e dischi Jaz, Nastri di backup
- File di Log
- RAID, Backup

RAM e File Slack

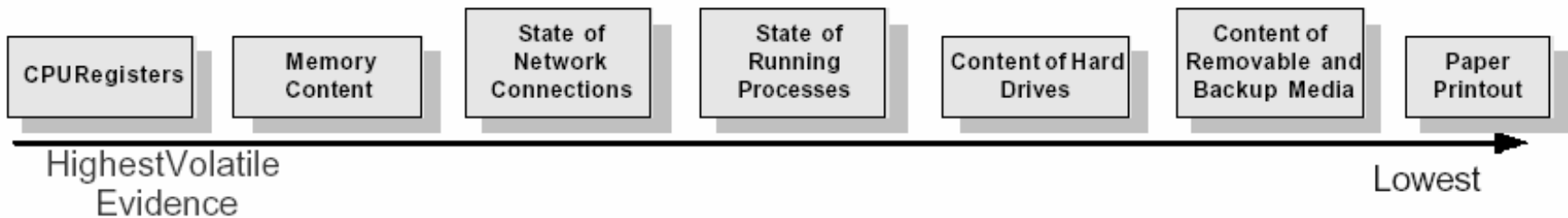


Come conservare

- Bypassare il Sistema operativo per creare backup bit-stream di tutta la prova
- Duplicati sono riportati su HD, CD-ROM, etc.
- Tutte le analisi sono fatte su queste immagini
- Documentare ogni cambiamento che comporta il cambiamento dell'immagine
- Autenticare le immagini rispetto agli originali usando CRC o hash MD5

Ordine di volatilità

- Registri, cache, memoria delle periferiche
- Memoria(kernel, fisica)
- Stato della rete
- Processi in esecuzione
- Dischi
- Floppy, backup media
- CD-ROM



Analisi dei File di Log

- Eventi
- Quali eventi sono monitorati?
- Cosa rivelano i record degli eventi?
- File di log di Firewall/IDS/Router/Server?
- TripWire Database?
- Modem/FTP/Telnet/RAS

Steganografia

- Creata per proteggere i diritti d'autore
- Usata, generalmente, per nascondere dati o file nella grafica
- Programmi per intercettarla
 - Stegdetect
 - Stegbreak
- Usata per proteggere le informazioni da persone in regime non libero.

Documenti utili

- RCMP Article on the Forensic Process. http://www.rcmp-grc.gc.ca/tsb/pubs/bulletins/bull41_3.htm
- Lance Spitzner's Page: Forensic Analysis, Building Honeypots <http://www.enteract.com/~lspitz/pubs.html>
- Fish.com Security's Forensic Page: The Coroner's Toolkit (Unix), Computer Forensic Class Handouts. <http://www.fish.com/forensics/>
- The Forensic Toolkit (NT). <http://www.ntobjectives.com/forensic.htm>
- Cryptcat. http://www.farm9.com/Free_Tools/Cryptcat
- Long Play Video Recorders. <http://www.pimall.com/nais/vrec.html>
- FBI Handbook of Forensic Services. <http://www.fbi.gov/programs/lab/handbook/intro.htm>
- Solaris Fingerprint Database for cryptographic comparison of system binaries. <http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl>
- Inspecting Your Solaris System and Network Logs for Evidence of Intrusion. <http://www.cert.org/security-improvement/implementations/i003.01.html>
- ONCTek List of possible Trojan/Backdoor Activity <http://www.onctek.com/trojanports.html>
- Sixteen Tips for Testifying in Court from the "PI Mall" <http://www.pimall.com/nais/n.testify.html>

Ing. Gianluigi Me

Computer Forensics

FINE