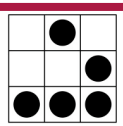
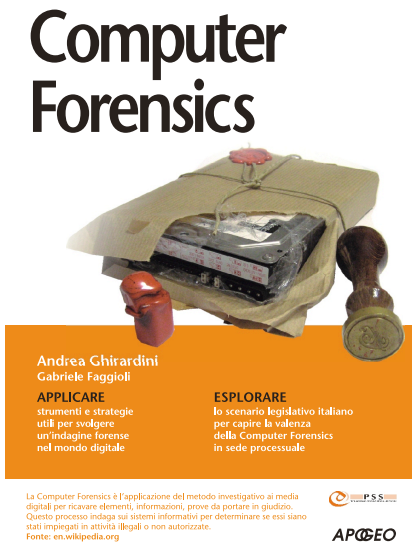
Tecniche di ricerca e tutela delle prove informatiche

Andrea “Pila” Ghirardini
founder @PSS srl



Andrea Ghirardini

- Titolare @PSS srl
- Consulente per Polizia, Carabinieri, Guardia di Finanza
- Perito per oltre 20 Procure in Italia
- Autore dell'unico manuale italiano riguardante la computer forensics
- CISSP
- Socio Clusit



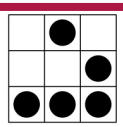
Computer Forensics

E’ quella branca della polizia scientifica, che si occupa del trattamento, gestione e presentazione delle evidenze digitali a fini probatori e di indagine

Computer Forensics: Il suo utilizzo - I

Fino a poco tempo fa la “computer forensics” era utilizzata solo per quanto riguarda i crimini tecnologici:

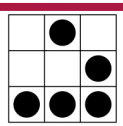
- Cracking
- Web defacement
- Danneggiamento/Furto di dati
- Pedofilia online



Computer Forensics: Il suo utilizzo - II

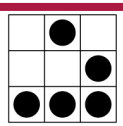
Negli ultimi due anni ci siamo occupati di: (in ordine di numero di casi trattati)

- Spionaggio Industriale
- Criminalità Eversiva
- Spaccio di droga
- Abusi sull'infanzia
- Reati connessi all'ambito lavorativo
- Furto/Abuso di dati



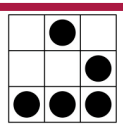
Computer Forensics: Il suo utilizzo - III

- La tecnologia pervade sempre più il nostro mondo
- E' normale per chiunque portare addosso uno o più dispositivi tecnologici
- La "digital life" profetizzata da Steve Jobs svariati anni fa è ora una realtà con la quale convivere



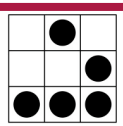
Computer Forensics: Il suo utilizzo - IV

- E' quindi assolutamente normale pensare che sia necessario dominare una disciplina che ci permetta di lavorare nella parte virtuale/digitale della vita delle persone
- In caso contrario si potrebbe rischiare di perdere una consistente parte di informazioni



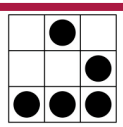
Computer Forensics: Il suo utilizzo - V

- Da sempre l'utilizzo di una qualunque tecnologia è scoperto prima dai criminali piuttosto che dalla giustizia
- E' un gioco di "guardie e ladri" dove le prime sono costantemente all'inseguimento e, quindi, dietro



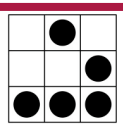
Computer Forensics: Il suo utilizzo - VI

- Dove agisce la computer forensics?
- In pratica ovunque vi sia l'utilizzo di tecnologia. Nata come tecnica di indagine per i computer si è estesa ai sistemi informativi, alle connessioni di rete, ai dispositivi portati dalle persone



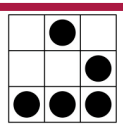
Computer Forensics: Il suo utilizzo - VII

- Dove si possono trovare le prove?
- Ovunque, da un computer ad un palmare, dallo smartphone al lettore MP3, dalla webmail al grande server dipartimentale



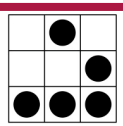
Computer Forensics
Aree di Influenza - I

- **In primis la computer forensics si occupa del trattamento, della raccolta e della preservazione delle prove digitali**
- Questo si rende necessario in quanto le prove digitali richiedono, per loro natura, un trattamento totalmente diverso da quello delle prove fisiche



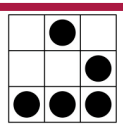
Computer Forensics
Aree di Influenza - II

- La prova digitale può essere copiata innumerevoli volte
- Non è possibile distinguere la prova dall'originale
- La prova è immateriale (non in tutti i casi!)
- E' facilmente alterabile e difficilmente si può dimostrare la sua alterazione



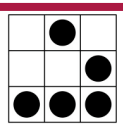
Computer Forensics
Aree di Influenza - III

- La prova digitale può essere estremamente difficile da trovare
- Può assumere forme diverse
- Può essere camuffata tramite steganografia, crittografia o altri metodi
- Può risiedere in luoghi dove non sia possibile effettuare l'acquisizione



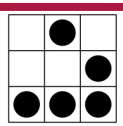
Computer Forensics
Aree di Influenza - IV

- La conservazione della prova digitale riveste un'importanza vitale nel processo d'indagine
- Una sua non corretta conservazione può rendere la prova inservibile oppure alterarla



Computer Forensics
Aree di Influenza - V

- Infine la Computer Forensics deve stabilire anche una metodologia per l'analisi delle evidenze raccolte
- Tale analisi deve avvenire in maniera da non alterare la prova stessa e deve essere legata ad una serie di dettami

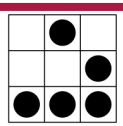


Computer Forensics
Aree di Influenza - VI

- Trasparenza
- Ripetitività
- Disponibilità
- Semplicità
- Esaustività

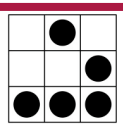
Computer Forensics
Aree di Influenza - VII

- **Trasparenza**
  - Non è possibile pensare di non documentare passo per passo ogni cosa si stia facendo
  - La controparte deve essere in grado non solo di svolgere una perizia in autonomia ma anche di **verificare il lavoro svolto dalla parte avversa**



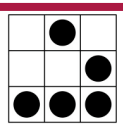
Computer Forensics
Aree di Influenza - VIII

- **Ripetitività**
  - Ogni passo compiuto durante l'analisi deve essere ponderato al fine di evitare di danneggiare la prova
  - Rispetto ad altre discipline, si ha il vantaggio di poter duplicare una prova un numero infinito di volte



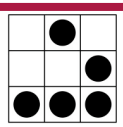
Computer Forensics
Aree di Influenza - IX

- **Disponibilità**
  - Dobbiamo poter porre la controparte nelle condizioni di poter ripetere quanto fatto da noi stessi
  - Essa deve quindi poter accedere non solo alla prova ma anche al software necessario al suo trattamento



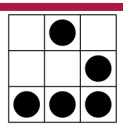
Computer Forensics
Aree di Influenza - X

- **Semplicità**
  - Il ragionamento può essere complesso, lo sforzo notevole, ma alla fine il risultato deve essere raggiunto con una serie di semplici passi che possano essere adeguatamente compresi
  - Non si può pretendere che in dibattimento siano tutti dei profondi esperti informatici



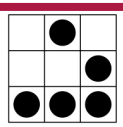
Computer Forensics
Aree di Influenza - X

- **Esaustività**
  - L'indagine deve essere completa.
  - Deve aver esaminato, nel limite del possibile, ogni fonte di prova nella sua globalità



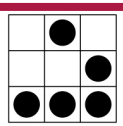
Computer Forensics
Software

- Software commerciale o open source?
- Il problema non è esclusivamente tecnico ma coinvolge anche una scelta filosofica e la legislazione del paese nel quale stiamo operando



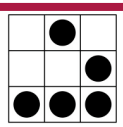
Computer forensics: Software Open Source - I

- L'open source è determinante per affrontare le nuove sfide poste dalla computer forensics (ma non è risolutivo in tutti i casi)
- L'open source ha due vantaggi fondamentali:
  - Ampia disponibilità
  - Apertura dei formati
- Velocità di sviluppo



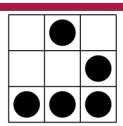
Computer forensics: Software Open Source - II

L'uso di programmi di analisi/controllo open source permette alla parte avversa di avere immediatamente a disposizione tutto quanto necessario per verificare il lavoro svolto dal perito e di effettuare le proprie considerazioni



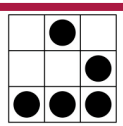
Computer forensics: Software Open Source - III

L'uso di formati dei archiviazione/file liberi ne preserva il valore nel corso del tempo.



Computer forensics: Software Open Source - IV

La velocità di sviluppo del software open source permette di poter essere sempre allineati con quanto è presente sul mercato. A volte la possibilità di accedere a programmi in Alpha/Beta Testing può essere vitale

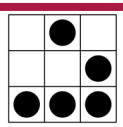


Computer forensics: Software Open Source - V

Linux è l'unico sistema operativo in grado di supportare oltre 40 file system differenti (altri 20 tramite il progetto FUSER) e fino a 18 tipi di partizionamento

Nell'anno scorso abbiamo incontrato:

- ✓Windows (in tutte le salse)
- ✓MacOSX (anche con crittografia)
- ✓Unix (Linux, *BSD, Irix e Solaris)
- ✓PalmOS, Symbian e PocketPC
- ✓VMS



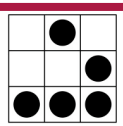
Computer forensics: Software Open Source - VI

Solo macchine Linux

(sia workstation di analisi sia file servers)*

*Con eccezione di due MAC

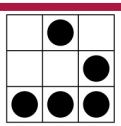
- Comportamento prevedibile
- Stabilità del sistema
- Supporto per formati di altri sistemi
- Possibilità di confinare Windows dove non faccia danni
- Supporto Hardware
- Ampia disponibilità di software
- Utility di sistema
- Ampia adattabilità



Computer forensics: Software Open Source - VII

Nei nostri laboratori utilizziamo:

- OpenSuSE
- Helix Knoppix
- The Sleuth Kit
- Autopsy Browser
- OpenOffice.org 2.2
- MacOSX



FINE

Per informazioni:

Andrea Ghirardini
andrea@atpss.net
+39-392-1101101

Q/A

Grazie per l'attenzione!

Ci sono domande?