

Acquisizione di elementi di indagine per l'autorità

Stefano Fratepietro



Argomenti trattati

- ✦ Cenni sull'informatica Forense
- ✦ Il dato informatico
- ✦ Strumenti per l'acquisizione e l'analisi di sistemi informatici (DEFT Linux)

Informatica Forense I

- L'Informatica forense (Computer Forensic in inglese) 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 II

- ✦ Informatica forense studia a fini probatori i processi, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici, nonché l'analisi forense di ogni sistema informatico e telematico, 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.
- ✦ L'insieme dei processi e delle tecniche più accreditate vengono definite "pratiche migliori".

Crescita della domanda

- ✦ All'aumento del trattamento dei dati con sistemi informatici consegue l'incremento della domanda di analisi dei dati digitali ai fini di investigazione e giustizia per:
 - ✦ reati informatici e telematici (es. L. 547/93)
 - ✦ reati non informatici ma commessi con sistemi informatici
 - ✦ reati di cui si rinvencono tracce o indizi nei sistemi

Problemi metodologici nel trattamento dei dati

- ✦ Completezza dell'acquisizione
- ✦ Integrità dei dati acquisiti
- ✦ Paternità e provenienza dei dati
- ✦ Esaminabilità dei dati acquisiti
- ✦ Verificabilità delle procedure seguite
- ✦ Riproducibilità dei processi eseguiti

Il dato digitale oggetto di indagine - I

- ✦ Il reperto informatico si esamina tenendo presente la volatilità del dato informatico
- ✦ Le fasi del trattamento sono:
 - ✦ Individuazione
 - ✦ Acquisizione
 - ✦ Analisi
 - ✦ Valutazione.

Il dato digitale oggetto di indagine - II

- ✦ L'acquisizione dei dati deve essere fatta eseguendo una "bit stream image" memorizzando la copia integrale dello storage su un altro supporto
- ✦ Calcolare l'hash del disco sorgente e del disco copia e confrontarli
- ✦ Effettuare l'analisi dei dati acquisiti solo dalle copie dei reperti.

Il dato digitale oggetto di indagine - III

- ✦ Le memorie di massa e ogni dispositivo di memorizzazione devono essere “congelati” il più presto possibile; cioè i reperti vanno raccolti nel tempo più prossimo all'accadere di un evento di interesse e senza che i contenuti dei dispositivi di memoria vengano alterati
- ✦ Tutte le procedure utilizzate durante l'esame dei reperti devono essere controllabili e ripetibili; cioè un esperto indipendente deve essere in grado, leggendo i documenti di ripetere tutte le operazioni che sono state eseguite durante le indagini

Documentazione

- ✦ Documentare con più dettagli possibili le rilevanze riscontrate con:
 - ✦ Relazioni
 - ✦ Verbali
 - ✦ Fotografie
 - ✦ Filmati

Strumenti del mercato

- ✦ Strumenti a codice chiuso (spesso a pagamento)
 - ✦ Encase
 - ✦ FTK
 - ✦ X-Way Forensics
- ✦ Strumenti a codice aperto (spesso gratuiti)
 - ✦ DEFT Linux
 - ✦ Helix

DEFT Linux - Caratteristiche

- ✦ Progetto 100% “Made in Italy”
- ✦ Stabilità e sicurezza dei dati durante l’elaborazione
- ✦ Raccolta dei migliori tool per le indagini informatiche
- ✦ Semplicità d’uso
- ✦ In continua evoluzione



DEFT Linux - What i can do?

- ✦ Acquisizione dei reperti
- ✦ Analisi dei dati
- ✦ Recupero file cancellati
- ✦ Cracking di password
- ✦ Intercettazioni telematiche



Dimostrazione

