



**INTRODUZIONE ALLA
COMPUTER FORENSIC**

CORRADO GIUSTOZZI



 28 maggio 2010 Sapienza Università di Roma 1

Argomenti che tratteremo

- Cos'è la computer forensic
- Ambiti di applicazione
- Principi fondamentali
- Modalità di azione
- Problemi aperti
- Linee guida
- Anti-forensic

 28 maggio 2010 Sapienza Università di Roma 2

COMPUTER FORENSICS

*INFORMAZIONI GENERALI
E CONCETTI DI BASE*

 28 maggio 2010 Sapienza Università di Roma 3

Perché l'informatica forense?

- Della nostra vita di tutti i giorni fanno parte:
 - computer fissi e portatili
 - PlayStation, Xbox, ...
 - cellulari, PDA, ...
 - lettori MP3, iPod, fotocamere digitali, ...
 - Internet, reti fisse, reti Wi-Fi, ...
 - Web, blog, e-mail, chat, IM, SMS, VoIP, ...
- Tutti possono partecipare a crimini come:
 - armi, strumenti di offesa
 - vittime
 - complici
 - testimoni

 28 maggio 2010 Sapienza Università di Roma 4

Rapporti tra sistemi e crimine

- Armi, strumenti di offesa:
 - sorgenti di attacchi informatici, intrusioni, spam, ...
 - mittenti di messaggi (e-mail, IM) minatori, diffamatori, ...
- Vittime:
 - oggetto di attacco, tentativi di intrusione, ...
 - oggetto di intercettazione, spionaggio, sabotaggio, ...
- Complici:
 - nascondiglio per informazioni clandestine o illecite, ...
 - veicolo di rivendicazioni, richieste estorsive, ...
- Testimoni:
 - depositari di informazioni di stato, di tracce, di log, ...

 28 maggio 2010 Sapienza Università di Roma 5

Computer forensics: cos'è?

- Termine piuttosto ampio (ed abusato!)
- Possibili definizioni (tutte imprecise):
 - disciplina che si occupa di acquisire, preservare, identificare, documentare, estrarre, analizzare dati o eventi informatici al fine di evidenziare l'esistenza di prove nello svolgimento dell'attività investigativa
 - uso dell'informatica per rispondere a domande che sorgono nell'ambito di procedimenti legali
 - studio delle evidenze digitali come elementi di prova
- In ogni caso va considerata una disciplina della polizia scientifica come la grafologia, la medicina legale, la balistica, ...

 28 maggio 2010 Sapienza Università di Roma 6

Computer forensics: ambiti

- Non riguarda solo illeciti informatici:
 - oramai tutti usano computer e posta elettronica
- Non riguarda solo la sfera penale:
 - reati tributari
 - contenziosi aziendali / giuslavoristici
 - contenziosi contrattuali / commerciali
- Importanti differenziazioni:
 - reati informatici in senso stretto
 - reati comuni commessi per mezzo delle tecnologie informatiche
 - reati comuni le cui tracce o indizi si rinvenivano in sistemi informatici o telematici

28 maggio 2010

Sapienza Università di Roma

7

La situazione attuale (1/2)

- La computer forensic è una disciplina relativamente recente, ancora non del tutto consolidata anche a livello internazionale:
 - viene tuttora considerata la “cenerentola” delle discipline di indagine, e percepita come “meno nobile” rispetto alle altre discipline forensi
- I giudici, i PM e gli avvocati molto spesso non posseggono neppure le nozioni più elementari di informatica (e addirittura se ne vantano!...):
 - è difficile spiegare ad un giudice concetti a lui estranei
 - per un giudice è difficile poter stabilire la bravura e la professionalità di un perito, sia d'ufficio che di parte, e di conseguenza valutare l'attendibilità di una perizia

28 maggio 2010

Sapienza Università di Roma

8

La situazione attuale (2/2)

- Servono conoscenze e strumenti che non si possono improvvisare sul campo:
 - purtroppo chiunque si sente in grado di “mettere le mani” su un'evidenza informatica, con conseguenze spesso devastanti per l'indagine
 - gli investigatori, a parte alcune unità specializzate, non sono di solito formati sulle corrette modalità di repertamento, analisi e conservazione delle evidenze
 - la qualità media dei consulenti in questo campo lascia davvero a desiderare...
- La cultura generale si sta innalzando abbastanza rapidamente, ma è ancora comune che in fase di indagine si commettano errori banali i quali vanificano il lavoro (invalidazione delle prove)

28 maggio 2010

Sapienza Università di Roma

9

LINEE GUIDA

PRINCIPI FONDAMENTALI

28 maggio 2010

Sapienza Università di Roma

10

La scena del crimine



28 maggio 2010

Sapienza Università di Roma

11

Le evidenze digitali

- Documento informatico (L. 18/03/2008, n. 48):
 - non più “il supporto informatico contenente dati o informazioni aventi efficacia probatoria” (ex L. 547/93)
 - bensì “la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti” (ex DPR 513/97 e CodAmmDig)
- Caratteristiche delle evidenze digitali:
 - contro: estremamente labili, volatili, facilmente alterabili
 - il solo start-up di un sistema Windows modifica irreversibilmente lo stato di circa 200 file
 - pro: “clonabili” in modo perfetto, completo, ripetibile
 - è quasi sempre possibile (e fondamentale) assicurare l'integrità dell'evidenza originale e la ripetibilità della prova
- Occorre agire secondo protocolli precisi

28 maggio 2010

Sapienza Università di Roma

12

Principi fondamentali (1/2)

- Primum non nocere:
 - i computer spenti non vanno accesi!
 - i computer accesi non vanno toccati senza necessità
- Cosa si sta facendo?
 - accertamento *ripetibile* (art. 359 c.p.p.)
 - accertamento *irripetibile* (art. 360 c.p.p.)
- Documentare tutto con estrema cura:
 - assicurarsi che l'orario sia corretto!
 - prendere appunti passo passo
 - fotografare tutto ciò che si fa
 - redigere un verbale accurato, e possibilmente farlo controfirmare ai presenti

28 maggio 2010

Sapienza Università di Roma

13

Principi fondamentali (2/2)

- Lavorare sempre su una **seconda** copia:
 - lasciare l'originale dove si trova (*chain of custody*)
 - predisporre una copia forense master dei dati (clone)
 - verificare il master (*hash*) e conservarlo intatto!
 - dal master ricostruire una copia conforme dell'originale
 - svolgere l'analisi usando idonei strumenti di indagine
- Rispettare la catena di custodia:
 - acquisizione
 - analisi
 - conservazione
 - restituzione
 - documentazione!

28 maggio 2010

Sapienza Università di Roma

14

Problemi aperti (1/2)

- Ancora scarsa cultura sul tema, sia da parte dei magistrati che delle forze dell'ordine:
 - mancano esperienza e prassi comuni
 - si preferisce solitamente il sequestro all'acquisizione
- La legislazione non aiuta:
 - non esistono norme specifiche o principi consolidati
 - magistrati diversi richiedono metodi di indagine diversi
- Presenza di consulenti tecnici improvvisati:
 - non basta essere bravi tecnici e/o bravi avvocati!
 - spesso i danni maggiori li fanno le forze dell'ordine...
- Oggettive difficoltà tecniche:
 - si va dai PDA ai mainframe!

28 maggio 2010

Sapienza Università di Roma

15

Problemi aperti (2/2)

- Mancano protocolli tecnici comuni e condivisi:
 - forze dell'ordine diverse utilizzano metodi d'indagine, strumenti d'analisi e know-how diversi e spesso non interoperabili
- Scarsa attenzione nell'operare:
 - non si usano metodi "aperti" e formati interoperabili
 - non si garantisce la ripetibilità delle operazioni
 - non si garantisce la preservazione della prova
- Problemi tecnico-filosofici:
 - strumenti proprietari o open source?

28 maggio 2010

Sapienza Università di Roma

16

SW: Open Source o proprietario?

Caratteristica	Open Source	EnCase
Formato di acquisizione	Aperto (raw)	Proprietario
Modalità di verifica	Varietà di hash	Solo hash interno
Numero di file system gestiti	>40	<10
Numero di schemi di partizionamento	>18	<10
Velocità di sviluppo	Elevata	Bassa
Verificabilità del codice	Completa	Nessuna
Costo	Basso / Nullo	Elevato

28 maggio 2010

Sapienza Università di Roma

17

Linee guida

- Sequestro o acquisizione?:
 - cosa sequestrare e come farlo?
 - cosa acquisire e come farlo?
 - come comportarsi con gli oggetti fisici e coi dati digitali?
- Catena di custodia:
 - imballaggio, documentazione
 - gestione della prova
- Documentazione delle operazioni:
 - azioni effettuate
 - strumenti utilizzati
- Presentazione della prova:
 - supporti da usare
 - integrità ed autenticità dei dati (hash, firma digitale)

28 maggio 2010

Sapienza Università di Roma

18

Legge 18/03/2008, n. 48 (1/2)

- Art. 8 comma 5:
 - Dopo l'articolo 254 del codice di procedura penale è inserito il seguente: «Art. 254-bis. –1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».

28 maggio 2010

Sapienza Università di Roma

19

Legge 18/03/2008, n. 48 (2/2)

- Art. 9 comma 3:
 - All'articolo 354, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente: «In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità».

28 maggio 2010

Sapienza Università di Roma

20

PROBLEMATICHE TIPICHE***ESIGENZE COMUNI***

28 maggio 2010

Sapienza Università di Roma

21

Richieste tipiche

- Stabilire attività svolte dal soggetto o da terzi:
 - in caso di intrusione
 - in caso di contestazioni
 - come pura e semplice verifica di alibi
- Ricostruire profili personali:
 - contatti di posta elettronica, chat, ...
 - siti visitati, azioni svolte
 - contenuti delle comunicazioni
- Ricercare e repertare informazioni specifiche:
 - documenti significativi (email, log, testi, spreadsheet, ...)
 - materiale illecitamente detenuto (diritto d'autore)
 - materiale illegale (pedoporno), tipicamente nascosto

28 maggio 2010

Sapienza Università di Roma

22

Problematiche tipiche (1/3)

- Stabilire l'esatta cronologia delle azioni svolte:
 - accesso a sistemi esterni, connessioni ad Internet
 - accesso a documenti locali o remoti, scambio di e-mail
 - sessioni di lavoro in locale
- Recuperare informazioni inaccessibili:
 - file nascosti o occultati (slack space, steganografia, ...)
 - file di sistema o di servizio (log, cache, ...)
 - file cancellati
 - file cifrati
- Accedere a sistemi o documenti protetti:
 - recuperare o ricostruire password di accesso
 - forzare l'accesso a sistemi protetti

28 maggio 2010

Sapienza Università di Roma

23

Problematiche tipiche (2/3)

- Recuperare informazioni da sistemi "strani":
 - cellulari, palmari, PDA, ...
 - fotocamere digitali, lettori MP3, telecamere IP, ...
 - computer particolari (AS/400, Macintosh, ...)
 - sistemi specializzati (PlayStation, Xbox, multimedia, ...)
 - computer "vintage" (Amiga, Atari, Commodore, ...)
 - mainframe!
- Recuperare informazioni da supporti obsoleti:
 - floppy disk da 5,25" o 8", cartucce di nastro, ...
 - hard disk d'antiquariato...

28 maggio 2010

Sapienza Università di Roma

24

Problematiche tipiche (3/3)

- Recuperare informazioni da sistemi guasti (!):
 - hard disk rotti o malfunzionanti
 - palmari, PDA, cellulari rotti
- Analizzare archivi di posta elettronica:
 - selezione ed estrazione di messaggi per keyword
- Analizzare e repertare centinaia di file:
 - immagini pedopornografiche
 - audio/video “piratati”
 - copie illegali di libri (tipografie universitarie clandestine!)

28 maggio 2010

Sapienza Università di Roma

25

Computer forensic “in casa” (1/2)

- Sempre più spesso le aziende vorrebbero investigare direttamente su incidenti interni:
 - spionaggio industriale, fuga di informazioni
 - infedeltà aziendale
 - sabotaggio, estorsione
 - attività sospette
- A volte è la magistratura a chiedere alle aziende informazioni su determinate attività tecniche svolte al proprio interno:
 - navigazione Web
 - invio/ricezione di e-mail
 - corrispondenza tra account di posta e/o IP address

28 maggio 2010

Sapienza Università di Roma

26

Computer forensic “in casa” (2/2)

- Non sempre/tutto si può fare!!!
 - controllo della postazione di lavoro
 - controllo della posta
 - controllo della navigazione in Rete
 - videosorveglianza interna
- I diritti (dei lavoratori) sono inviolabili:
 - L. 300/1970: Statuto dei lavoratori
 - Legge 23/12/1993, n. 547: Criminalità informatica
 - Art. 616 CP: Violazione della corrispondenza
 - D. Lgs. 196/2003: Tutela dei dati personali
- Alcune azioni sono possibili con determinate accortezze, altre sono inevitabilmente reato!

28 maggio 2010

Sapienza Università di Roma

27

IL PROCESSO DI INVESTIGAZIONE DIGITALE

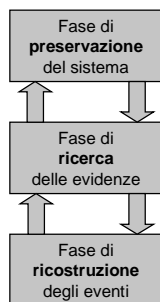
MODALITÀ DI ANALISI DELLE EVIDENZE INFORMATICHE

28 maggio 2010

Sapienza Università di Roma

28

La scena del crimine digitale



- L'approccio metodologico più corretto per svolgere l'indagine della scena del crimine digitale segue quello usato per la scena del crimine tradizionale
- L'analisi procede lungo tre fasi, non necessariamente sequenziali:
 - preservazione del sistema
 - ricerca delle evidenze
 - ricostruzione degli eventi
- Ogni fase può influenzare le altre!

28 maggio 2010

Sapienza Università di Roma

29

Approccio PICL (Carrier, 2005)

- **Preservation:** evitare ogni modifica alle evidenze
 - copiare e conservare con cura le evidenze importanti
 - lavorare esclusivamente su copie conformi
- **Isolation:** eliminare interferenze ed interazioni
 - separare il sistema sotto esame dal mondo esterno
 - lavorare in ambienti “stagni” (virtualizzazione, ...)
- **Correlation:** cercare conferme ai risultati ottenuti
 - confrontare i dati ricavati con altre fonti indipendenti
 - verificare la consistenza delle conclusioni raggiunte
- **Logging:** documentare tutte le azioni svolte
 - giustificare le modalità di azione e i risultati ottenuti
 - permettere ad altri la verifica/ricostruzione delle attività

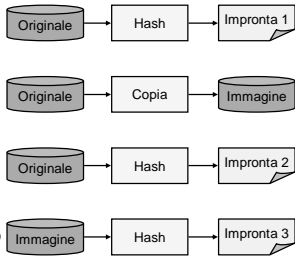
28 maggio 2010

Sapienza Università di Roma

30

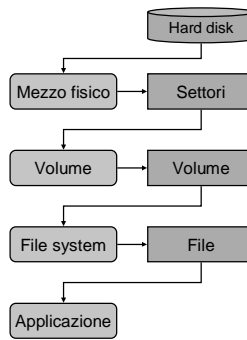
Il processo di acquisizione fisica

- È tassativo evitare di modificare l'evidenza originale durante la copia:
 - usare un *write blocker*
 - montare il disco in R/O
- Per dimostrare che l'evidenza originale non è stata modificata durante la copia, e che l'immagine è identica all'originale:
 - si calcolano gli *hash* dell'originale prima e dopo la copia, e dell'immagine
 - tutti e tre gli *hash* devono coincidere tra loro



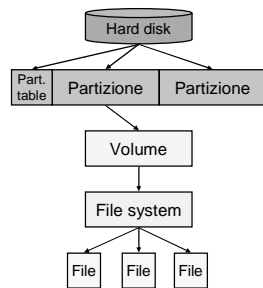
Livelli di analisi dei dati

- I dati digitali sono strutturati su vari livelli di astrazione
- Ogni livello richiede un tipo di analisi appropriata per passare al successivo:
 - livello fisico:
 - dai settori al volume
 - livello di volume
 - dal volume al file system
 - livello di file system
 - dal file system ai file
 - livello dell'applicazione
 - dai file all'applicazione
- Ogni livello è importante!

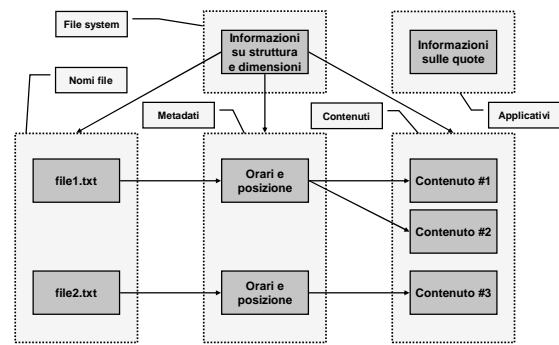


Struttura logica dei dati su disco

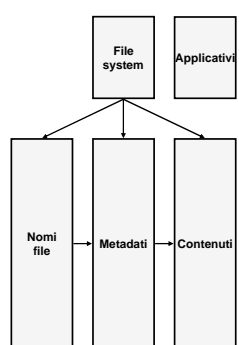
- Un hard disk è organizzato in varie strutture logiche:
 - ogni disco fisico è suddiviso in una o più **partizioni** indipendenti
 - una o più partizioni formano un **volume**
 - ciascun volume contiene un **file system**
 - il file system contiene ed organizza i **file** e i relativi **metadati** mediante apposite strutture dati di sistema, diverse per ogni tipo di file system



Categorie di dati nel file system (1/2)



Categorie di dati nel file system (2/2)



- File system:
 - informazioni generali sulla struttura del file system
- Contenuti:
 - dati che costituiscono l'effettivo contenuto dei file
- Metadati:
 - dati che descrivono i file (posizione, attributi, ...)
- Nomi file:
 - dati relativi ai nomi dei file
- Applicativi:
 - dati di servizio per funzioni speciali

Metadati temporali

- Fra i metadati più importanti ai fini investigativi vi sono le registrazioni di momenti chiave (*timestamp*)
 - tutti i SO ed i FS moderni associano ad ogni file almeno:
 - l'orario di **creazione originale**
 - l'orario di **ultima modifica**
 - l'orario di **ultimo accesso**
- Attenzione però all'effettiva attendibilità di tali orari:
 - l'orologio di sistema potrebbe non essere impostato bene
 - i timestamp potrebbero essere stati modificati ad arte
 - la risoluzione temporale non è uguale tra i vari timestamp
- Attenzione al confronto tra orari di sistemi diversi!
 - stessi timestamp hanno talvolta semantiche diverse
 - l'orario può essere espresso in tempo locale o in UTC

Dimensione e posizione dei file

- I metadati essenziali al sistema per la gestione dei file sono quelli di dimensione e di posizione
 - **dimensione**: solitamente in byte
 - **posizione iniziale**: nell'unità locale (settore, cluster, ...)
- La cancellazione di un file non cancella lo spazio occupato ma lo rende solo nuovamente disponibile:
 - nei settori non (più) allocati le informazioni sono intatte!
- Tra la fine logica del file e la fine dell'ultima unità di allocazione occupata c'è dello spazio allocato al file ma non utilizzato dal sistema (*slack space*):
 - vi si possono trovare tracce di memoria o dati precedenti
 - è possibile usarlo per nascondervi dei dati

28 maggio 2010

Sapienza Università di Roma

37

UN CASO DI STUDIO

LA CORRETTA ACQUISIZIONE DI UN HARD DISK

28 maggio 2010

Sapienza Università di Roma

38

Ricognizione iniziale (1/2)



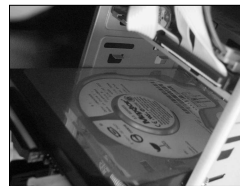
- Effettuare una ricognizione esterna dell'hardware
- Descrivere accuratamente il sistema annotando marca, modello, caratteristiche
- Annotare lo stato di preservazione del tutto
- Se il sistema è sigillato, rompere i sigilli solo alla fine dell'operazione

28 maggio 2010

Sapienza Università di Roma

39

Ricognizione iniziale (2/2)



- Effettuare una ricognizione interna dell'hardware
- Descrivere accuratamente l'hard disk annotando marca, modello, caratteristiche
- Solitamente non c'è bisogno di estrarre l'hard disk dalla propria sede

28 maggio 2010

Sapienza Università di Roma

40

Collegamento all'hard disk



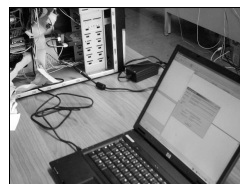
- Scollegare l'hard disk dai suoi cavi di collegamento
- Collegare all'hard disk un *write blocker* esterno possibilmente certificato dal DoJ USA
- Assicurarsi che il blocco (se escludibile) sia effettivamente attivo
- Collegare il *blocker* al PC di acquisizione

28 maggio 2010

Sapienza Università di Roma

41

Acquisizione e verifica (1/2)



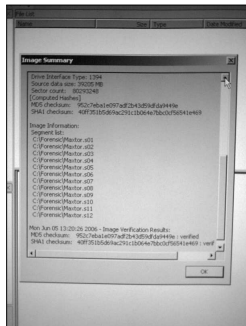
- Calcolare l'hash del disco originale **prima** della copia usando algoritmi standard (MD5, SHA1)
- Effettuare la copia forense mediante software apposito
- Calcolare l'hash del disco originale **dopo** la copia usando gli stessi algoritmi
- Verificare che i due hash coincidano (integrità!)
- Documentare nel verbale le azioni svolte riportando il valore dell'hash calcolato

28 maggio 2010

Sapienza Università di Roma

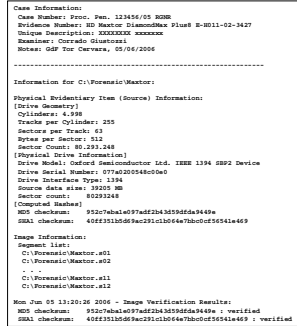
42

Acquisizione e verifica (2/2)



- Calcolare l'hash della copia forense usando i medesimi algoritmi
- Verificare che l'hash della copia forense coincida con quello del disco originale
- Documentare nel verbale le azioni svolte

Log di acquisizione



- Molti programmi di acquisizione forense sono in grado di produrre in modo automatico il log dell'operazione di copia
- Tale log di solito riporta anche le informazioni tecniche sul disco acquisito (geometria, dimensioni, ...) nonché i valori degli hash prima e dopo la copia
- Se si usa un programma che non lo produce, tutto ciò va riportato a mano!

In alternativa...

- Avviare il computer in esame dal CD di una *live distro* di Linux specifica per utilizzo forense:
 - Helix, Deft, Caine, ...
- Calcolare l'hash dell'hard disk interno da copiare
- Collegare al computer un disco esterno USB
- Effettuare la copia con un idoneo tool forense
- Calcolare gli hash dopo la copia, verificarli e riportarli nel verbale

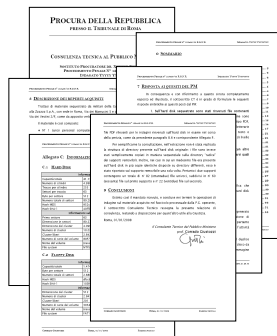


La fase di analisi

- L'immagine si può analizzare direttamente (con appositi tool) oppure la si può utilizzare per creare un disco clone
- Non si deve mai accedere direttamente all'immagine per evitare di alterarla accidentalmente
 - montarla in modo R/O
 - utilizzare tool forensi
 - usare un write blocker
- Anche "guardare" un file ne altera le date significative!
- Categorie di tool forensi:
 - sistemi di virtualizzazione
 - tool di cracking/hacking
 - tool di conversione
 - tool di file analysis
 - tool di data recovery
- Può capitare di doversi scrivere dei tool *ad hoc*!
- Un annoso problema: è meglio utilizzare strumenti commerciali o aperti?

La stesura della relazione tecnica

- La relazione deve riportare:
 - un frontespizio con i dati rilevanti del procedimento
 - un indice completo
 - l'antefatto e i quesiti posti
 - la descrizione della metodologia seguita e delle azioni svolte
 - le evidenze ricavate ed i risultati oggettivi stabiliti
 - le conclusioni raggiunte e le relative motivazioni
 - le risposte ai quesiti
 - eventuali considerazioni utili e pertinenti allo scopo



DIGITAL FORENSICS E TECNICHE DI ANTI-FORENSICS

VERSO UNA ULTERIORE SPECIALIZZAZIONE

Specializzazione della materia

- La “computer forensics” è in realtà solo una parte di una disciplina più ampia che si potrebbe definire *digital forensics*
- La *digital forensics* abbraccia temi diversi ed estremamente ampi, e si sta già specializzando in discipline più specifiche:
 - computer forensics:
 - analisi dei singoli sistemi, siano essi client o server
 - mobile forensics:
 - tutto quanto concerne i dispositivi ad uso personale
 - network forensics:
 - cattura ed analisi dei flussi di dati in transito

28 maggio 2010

Sapienza Università di Roma

49

Le branche della digital forensics

- Computer forensics:
 - media analysis
 - memory analysis
 - process analysis
 - data recovery
- Mobile forensics:
 - telefoni cellulari, smartphone, palmari
 - console portatili per videogiochi
 - personal multimedia...
- Network forensics:
 - { PAN, LAN, WAN, MAN } analysis
 - interception, wiretapping

28 maggio 2010

Sapienza Università di Roma

50

Anti-forensics

- Insieme di tecniche che mirano a confondere i tool di analisi forense, o ad usare i tool e i loro risultati per confondere l'analista forense
- Alcune sono “fantascientifiche”, altre però sono già state implementate in semplici strumenti
- Obiettivi principali dell'anti-forensics:
 - confondere la scala dei tempi
 - rendere inutilizzabili o inaffidabili i file di log
 - impedire il recupero di file cancellati
 - impedire l'identificazione di file ed eseguibili
 - nascondere i dati

28 maggio 2010

Sapienza Università di Roma

51

Le tecniche di anti-forensic (1/2)

- Cancellazione sicura:
 - dei dati e dello slack space (*wiping*)
 - dei metadati
- Alterazione dei metadati:
 - timestamp dei file
 - partition table
 - allocation table
- Boot esterno:
 - uso di *distro live* per bypassare il SO locale
- Steganografia:
 - nascondere i dati dentro un “carrier” insospettabile

28 maggio 2010

Sapienza Università di Roma

52

Le tecniche di anti-forensic (2/2)

- Pulizia delle tracce:
 - cancellazione di log, cache, cookies, ...
 - cancellazione dei file di swap, hibernation, ...
- Produzione di false tracce:
 - introduzione di voci spurie nei log
- Subversion:
 - creazione di partizioni estese, nascoste, disallineate, ...
 - inserimento di dati nelle strutture di controllo (metadati)
 - inserimento di dati in posti inattesi (slack space, ...)
- Plausible deniability:
 - file cifrati nei quali non si può dimostrare l'esistenza di contenuti

28 maggio 2010

Sapienza Università di Roma

53



 Dipartimento di Cibernetica e Informatica

FINE

**INTRODUZIONE ALLA
COMPUTER FORENSIC**

master universitario di secondo livello
Master in Gestione della Sicurezza
 Informatica per l'Impresa e la Pubblica Amministrazione



28 maggio 2010 Sapienza Università di Roma 54