

Computer Forensics e Ethical Hacking

Nuove frontiere della sicurezza informatica

Dott. Mattia Epifani
01/04/2009
DISI – Genova

*La **Computer Forensics (Informatica Forense)** è la scienza che studia l'**individuazione**, la **conservazione**, la **protezione**, l'**estrazione**, la **documentazione** e ogni altra forma di trattamento del dato informatico per essere valutato in un processo giuridico e studia, ai fini probatori, le **tecniche e gli strumenti per l'esame metodologico dei sistemi informatici** (Wikipedia)*

Computer Forensics



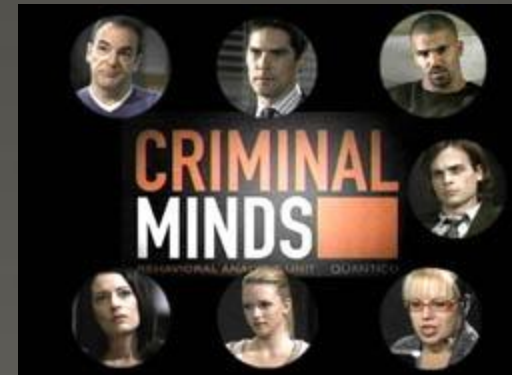
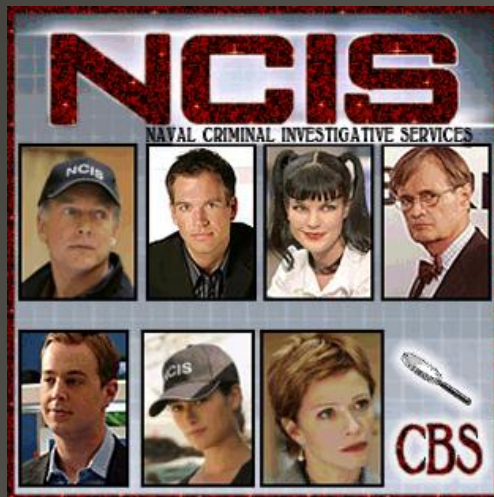
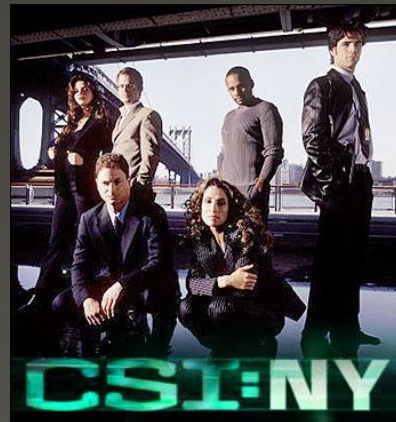
IT

SECURITY

INCIDENT RESPONSE

FORENSICS

Computer Forensics



Computer Forensics NON è...

- Informatici
- Avvocati
- Magistrati
- Forze dell'Ordine
- Investigatori
- Assicurazioni
- Aziende (Corporate Forensics)

CF – chi se ne occupa?

- Computer forensics (elaboratori)
- Digital forensics (strumenti digitali)
- Network forensics (reti informatiche)
- Mobile forensics (dispositivi mobili)
 - SIM forensics (SIM di telefoni cellulari)
 - Smartphone forensics
 - PDA forensics
- GPS forensics (navigatori satellitari)
- ...

CF – categorie

- 1984: L'FBI crea il CART (Computer Analysis and Response Team)
- 1993: Prima conferenza internazionale su "Computer Evidence"
- 1994: Dipartimento di Giustizia USA pubblica le prime linee guida
- **11/9/2001**: Twin Towers
- 26/10/2001: Patrioct Act USA
- 23/11/2001: **Convenzione di Budapest su Cybercrime**

CF – storia

- **Legge 633/41** (Diritto d'autore)
- **Legge 547/93** (Reati informatici)
- **Legge 231/2001** (Responsabilità società)
- **D.Lvo 196/2003** (Codice sulla Privacy)
- **Legge 155/2005** (Decreto Pisanu Antiterrorismo)
- **Legge 38/2006** (Pedopornografia)
- **Legge 48/2008** (Ratifica convenzione di Budapest) ha introdotto i **cybercrime** e ha fissato le linee guida nazionali
- **D.Lvo 109/2008** (Data retention)
- Linee guida e disposizioni del Garante

CF – e in Italia?

- **Computers crimes**

- Accesso abusivo a sistema informatico
- Cessione o detenzione abusiva di codici di accesso
- Invio di programmi diretti a danneggiare un sistema informatico
- Intercettazioni o impedimento abusivi di comunicazioni informatiche
- Cracking
- Spamming
- Frode informatica
- Danneggiamenti informatici
- Pedopornografia
- Ingiurie, minacce, diffamazione
- Diritto di autore
- Phising e truffe
- Riciclaggio e contraffazione
- Spionaggio industriale

CF – ambito penale

- ***Diritti della persona***

- Diritto al nome e nomi di dominio;
- Diritto alla riservatezza;
- Tutela del consumatore;

- ***Licenze e diritto di autore***

- ***Obbligazioni e contratti***

- Firma elettronica e documento informatico;
- Contratti telematici e digitali;

- ***Impresa e lavoro***

- Marchi e nomi a dominio;
- Lavoratori e strumenti informatici (telecontrollo, privacy...)

CF – ambito civile

- Codice dell'amministrazione digitale;
- E-governament;
- E-democracy;
- E-partecipation;
- Rete Unitaria della P.A.;
- Accessibilità;
- Internet e libertà di stampa e di pensiero;
- Altre libertà digitali.

CF – ambito amministrativo e costituzionale

- Gli strumenti elettronici ed informatici sono fonte di prova (e lo saranno sempre di più) in tutti gli ambiti
- La crescente diffusione della tecnologia li renderà quindi protagonisti sulla scena di crimini più diversi (terrorismo, traffico di stupefacenti, omicidi, rapine, aggressioni, ...)
- Ma anche in questioni civilistiche, fiscali, amministrative ...

CF – ma più in generale...

- Identificazione
- Acquisizione
- Conservazione
- Analisi
- Valutazione
- Presentazione

CF – passi operativi

- **Identificazione**
- Acquisizione
- Conservazione
- Analisi
- Valutazione
- Presentazione

CF – passi operativi

- Una **“prova”** é qualcosa che fornisce la dimostrazione di una **“teoria”**
- Senza prove si hanno solo **“sospetti”**

CF – individuare le prove

**Scena del
crimine**

Prova

Sospetto

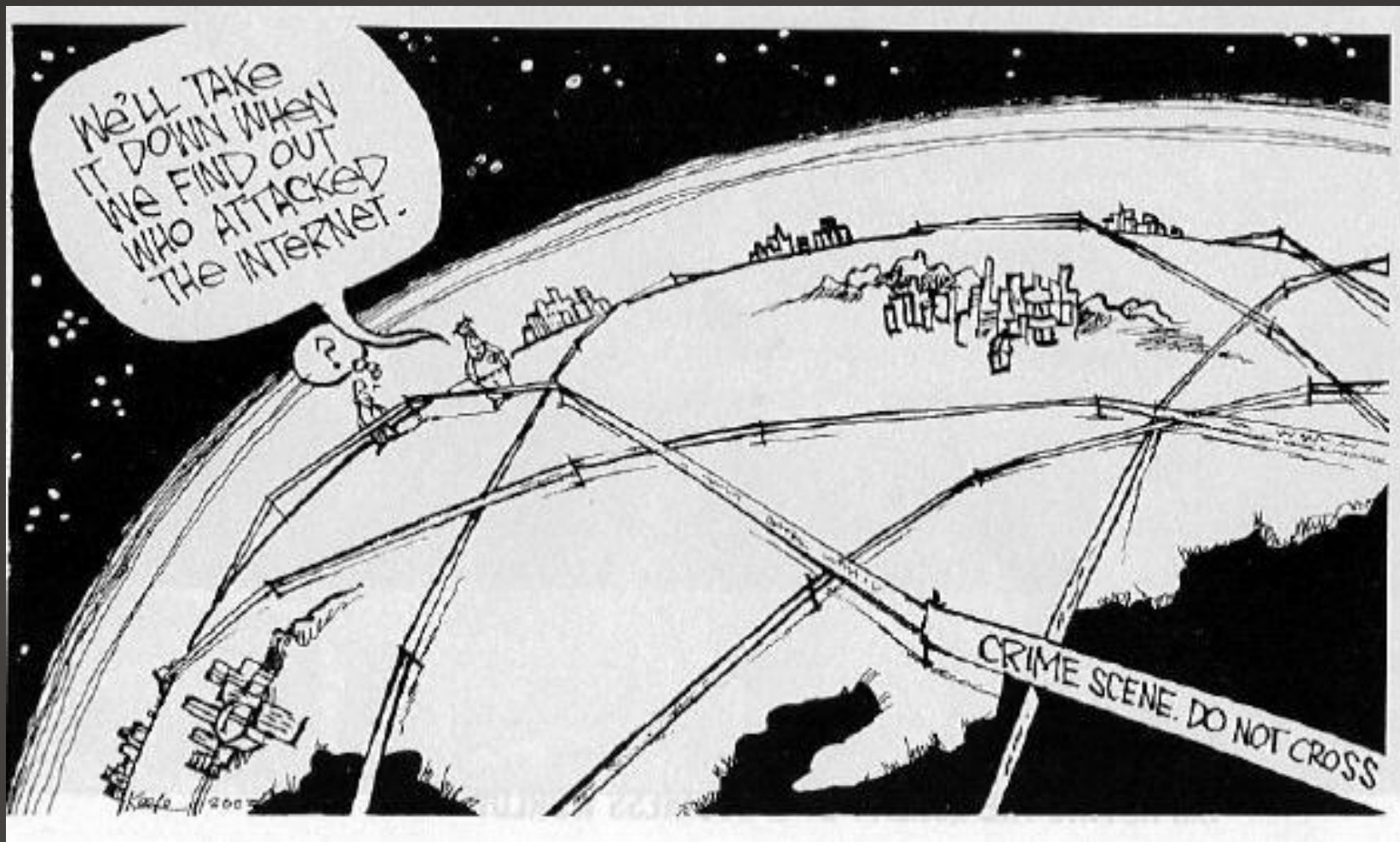
Vittima

CF – individuare le prove



- Isolare la scena del crimine per evitare l'accesso alle persone non autorizzate
- Ricercare impronte digitali
- Effettuare una descrizione accurata dell'ambiente unitamente a fotografie e filmati
- Cercare appunti, diari, note dai quali si possano eventualmente ricavare password chiavi di cifratura o altri elementi utili all'indagine
- Individuare i supporti che potrebbero contenere **prove digitali** (computer, telefoni, PDA, fotocamere, videocamere, memorie USB, navigatori satellitari, MP3, ...)

CF – individuare le prove



CF – e se la prova e su Internet?!?

- Identificazione
- **Acquisizione**
- Conservazione
- Analisi
- Valutazione
- Presentazione

CF – passi operativi

- Come tutte le prove, anche quella digitale deve essere:
 - Ammissibile
 - Autentica
 - Accurata
 - Completa
 - Convincente per il giudice
- Prove raccolte in maniera illegale o modificate dopo la raccolta NON SONO ACCETTABILI IN AULA

CF – acquisire la prova

- Necessità di un supporto per contenere il dato
- Riproducibilità in numero infinito di copie
- Ordine di volatilità
- Modificabilità (quasi) anonima dei dati
- Deteriorabilità dei dati e dei supporti

CF – il dato digitale

- Come NON si fa:
 - Accendo il computer sequestrato
 - Aspetto che il SO si sia caricato
 - Faccio un giro nelle impostazioni del sistema
 - Apro qualche documento e immagine sospetta
 - Mi collego ad Internet, già che ci sono, e leggo la mia mail
 - Collego un disco esterno
 - Faccio Copia e Incolla di quello che trovo
 - Spengo il computer

CF – acquisizione del dato

La migliore modalità di acquisizione è (ove possibile), effettuare una

copia bit per bit

dell'intero supporto digitale, verificando
l'integrità della copia con funzioni di Hash

CF – copia forense

- Identificare l'hard disk
 - Marca
 - Modello
 - Dati tecnici
 - Serial Number
- Documentare la modalità di estrazione e le precauzioni da adottare
 - Antistatica
 - Prevenire shock fisici (superficie di lavoro)
 - Alimentazione

CF – Caso pratico: un hard disk

- Montare l'hard disk
 - Prevenire la scrittura
 - Creare una immagine del disco
 - Provare l'integrità delle copie
 - Calcolare l'hash dell'hard disk originale
 - Calcolare l'hash dell'immagine
 - Confrontarli
 - Utilizzare solo strumenti dei quali si ha l'assoluta certezza che non inquinino le prove (permettendo, ad esempio, la scrittura su essa)

CF – Caso pratico: un hard disk

- Montare il volume in read only (blocco software)
 - Pro: economico
 - Contro:
 - Concetto difficile da accettare per l'utente medio (es. IL GIUDICE)
 - Errori di mounting
- Write blockers (blocco hardware)
 - Pro: efficace e "fisico"
 - Contro: costoso...

CF – prevenire la scrittura

- Si deve garantire una copia integrale (bit-per-bit) dell'intero supporto
- Soluzioni hardware
 - Pro: rapidità e efficacia
 - Contro: costo e tipologie di supporti e di connessioni (es. IDE, SCSI, SATA)
- Soluzioni software
 - Pro: economicità (es. comando dd in Linux)
 - Contro: skill tecnici e ATTENZIONE

CF – creazione dell'immagine

- Come verificare la **conformità** e la successiva **integrità** della copia?
 - **Verifica bit a bit**: Richiede tempi molto lunghi ed è possibile solo disponendo dell'originale
 - Usando **funzioni di hash** (MD5, SHA1, SHA-256, SHA-512, ...)

CF – verifica dell'integrità

- Una funzione di hash è una funzione one-way che, dato un input di **lunghezza arbitraria**, fornisce un output (hash) di **lunghezza fissa**
 - Non è possibile risalire al dato originario
 - Una piccola variazione nel dato originario si traduce in una grande variazione del risultato
 - È raro che due dati presi a caso diano il medesimo risultato (collisioni)
- Queste proprietà le rendono adatte per verificare integrità e errori di trasmissione

CF – funzioni di hash

- Se sulla scena del crimine il dato digitale si trova su un sistema acceso?
- Se il sistema non può essere spento per motivi di sicurezza? (es. strumenti medicali, militari, videosorveglianza, ecc.)
- Se lo spegnimento del computer creasse danno anche a terzi? (es. server di posta elettronica, database server, ecc,)

CF – e se il sistema è acceso?

- Ma anche se ...
- Il disco è cifrato
- La “prova” si trova in una memoria temporanea
- L’accesso al sistema è biometrico (impronta, retina, ecc.)

CF – e se il sistema è acceso?

- In questi casi si procede ad un analisi “live” del sistema
- Si utilizzano tool specifici
- Si devono identificare tutte le operazioni svolte
- Si tiene conto dell'**ordine di volatilità**

CF – e se il sistema è acceso?

- Registri di sistema
- Memoria cache
- Memoria delle periferiche (es. tabelle di routing)
- Processi in esecuzione
- Dischi
- Dati di log remoto e dati di controllo rilevanti per il sistema in esame
- Configurazione fisica del sistema informatico
- Topologia della rete
- Floppy
- CD/DVD e supporti ottici

CF – ordine di volatilità

- Identificazione
- Acquisizione
- **Conservazione**
- Analisi
- Valutazione
- Presentazione

CF – passi operativi

- Una volta in possesso della copia forense e dell'originale, occorre documentare come questi vengono conservati
 - Dove è memorizzata?
 - Chi ha avuto accesso?
 - Che operazioni sono state effettuate?
- 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

CF – conservazione della prova

- Identificazione
- Acquisizione
- Conservazione
- **Analisi**
- Valutazione
- Presentazione

CF – passi operativi

- L'analisi sarà effettuata sulla copia forense
- Oggetto dell'analisi sono:
 - Documenti (DOC, XLS, PDF, ...)
 - Immagini
 - Posta elettronica, navigazione web, chat
 - Database
 - File di Log
 - Registri di sistema e Active Data Stream
 - File cancellati
 - File nascosti
 - Slack Space
 - Bad Blocks
 - Steganografia
 - File cifrati
 - Partizioni nascoste

CF – analisi della prova

- Si utilizzano diversi tool, come:
 - Sistemi di virtualizzazione (Vmware, Parallels, Qemu)
 - Programmi e tecniche di password cracking per il SO e gli applicativi (John The Ripper, Ophcrack)
 - Analizzatori di pacchetti di rete (Wireshark, Ethereal)
 - Tool per la conversione dei formati
 - Player video e audio (VLC, Winamp, XMMS, iTunes)
 - File viewer (Quickview)
 - Editor esadecimale (WinHex, Hexedit)
 - Toolkit forensi (Autopsy, Encase, FTK)
 - Data recovery software (R-Studio, PC Inspector, Stellar)
 - File carver (Foremost, Scalpel)

CF – analisi della prova

- Forte contrapposizione

opensource vs proprietario

- Come in ogni altro settore dell'informatica il compromesso sta nel mezzo, ovvero utilizzare opensource finché si può, ma anche tool proprietari per non rovinarsi la vita!

CF – toolkit forensi

- I principali toolkit forensi commerciali sono:
 - Encase (Guidance Software)
 - Forensic Toolkit (Access Data)
 - X-Ways Forensic (X-Ways)
 - P2 Commander (Paraben Corporation)
 - Pro Discover (Technology Pathways)
 - Macintosh Forensic (Blackbag)

CF – toolkit forensi COMMERCIALI

- I tool opensource sono tutte distribuzioni Live (su CD o USB) di Linux con all'interno tool specifici per l'analisi forense
- Le principali distro disponibili sono:
 - Helix Knoppix (E-Fense, basato su Knoppix)
 - Helix 2008 (E-Fense, basato su Ubuntu)
 - DEFT 4.0 (Fratepietro, basato su Ubuntu)
 - Caine 0.5 (Giustini, basato su Ubuntu)
 - ForLex (Guerrieri)
 - IRIItaly Live CD (Forte, basato su Knoppix, chiuso)

CF – toolkit forensi OPENSOURCE

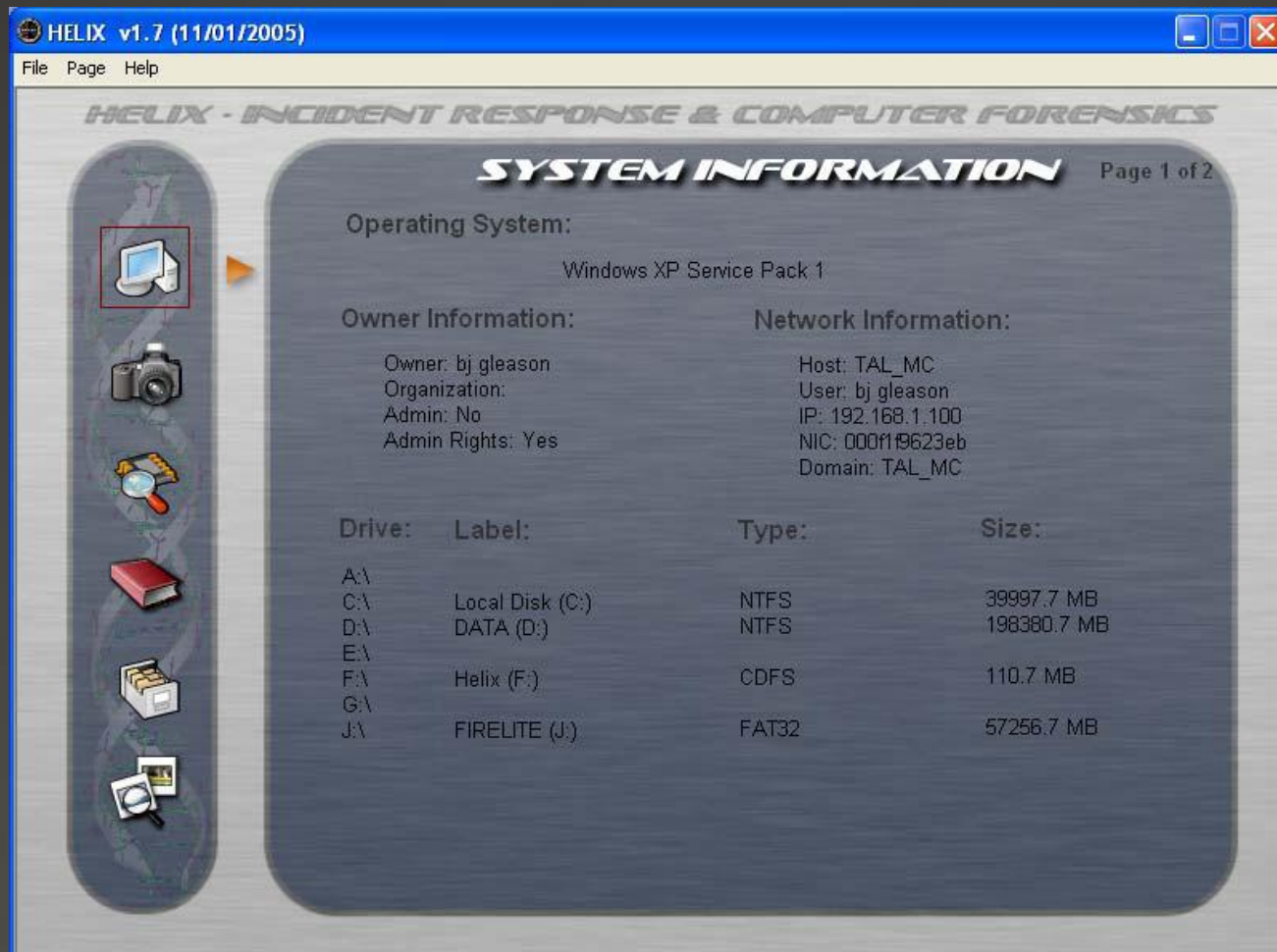
- E' la distribuzione di riferimento per i forenser
- Oltre alla distribuzione Live di Linux, ha anche un interfaccia grafica Windows
- Costruito per non modificare il sistema su cui viene eseguito
- Non monta in automatico i dischi
- Supporta molti filesystem (Ext, Fat, Ntfs, Reiser,...)

CF – Helix





CF – Helix



CF – Helix



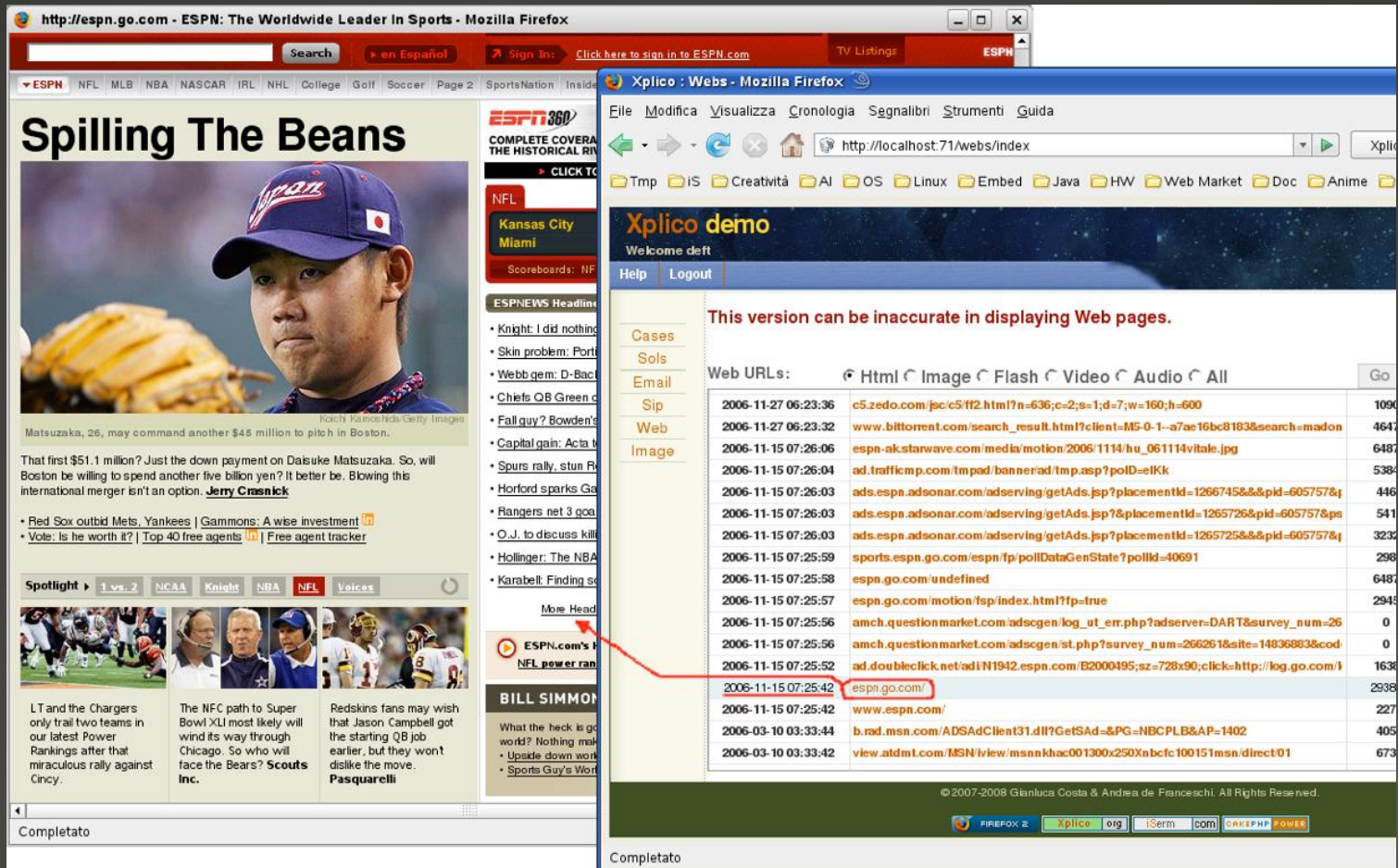
CF – Helix

- E' una distribuzione italiana
- E' **realmente** gratuito
- Ha un eccellente team di sviluppatori
- Basato su Xubuntu 8.10
- Ha una parte Windows
- Molto più performante di tutte le attuali distribuzioni dedicate alla Computer Forensics
- Include Xplico 0.6 (analisi su IP)

CF – Deft 4.0

The logo for DEFT Linux features the text "DEFT Linux" in a large, bold, white sans-serif font. Below it, in a smaller white sans-serif font, is the text "Computer Forensics live cd". To the right of the text is a stylized white fingerprint graphic on a dark, textured background.

DEFT Linux
Computer Forensics live cd



CF – Deft 4.0 (Xplico)

Xplico v0.5

Welcome deft

[Help](#) [Logout](#)

[Cases](#)

[Sols](#)

[Email](#)

[Sip](#)

[Web](#)

[Image](#)

Image Size:

☐ >50kb ☒ >25kb ☐ >12kb ☐ >6kb ☐ All

[Go](#)

28 images.



© 2007-2008 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.



FIREFOX 2

[Xplico](#) [org](#)

[iSerm](#) [com](#)

[CAKEPHP](#) [POWER](#)

CF – Deft 4.0 (Xplico)

- E' una distribuzione italiana
- Include i principali tool di CF
- Ha una compilazione semi-automatica ed incrementale del rapporto
- Adattabile alle diverse realtà legali (USA vs. Italy)



CF – Caine 0.5



- La cancellazione di un file è un'operazione **logica**
 - il sistema operativo cancella solamente i riferimenti al file
 - le aree del supporto ad esso assegnate sono rimesse a disposizione del sistema operativo
 - i dati veri e propri non sono cancellati finché non sono sovrascritti da altri file
- La persistenza dei dati sul dispositivo permette spesso di recuperare (in toto o in parte) il contenuto dei file cancellati

CF – recupero di file cancellati

- Tracciare l'uso del computer da parte dei diversi utenti definiti
- Individuare se e quando determinati file sono stati aperti da un certo utente
- Identificare le periferiche che sono state collegate (ad esempio, penne USB o dischi esterni)
- Individuare l'elenco (e spesso anche il contenuto) dei file stampati e su quale stampante
- Identificare le reti (tradizionali o WiFi) cui il computer è stato collegato

CF – analisi a livello di SO

- Molte applicazioni memorizzano, spesso all'insaputa dell'utente, informazioni di varia natura (*metadati*) nei file prodotti mediante di esse
- Questi medatati non sono normalmente visibili all'utente, ma possono essere estratti dai programmi di analisi forense e fornire molte informazioni utili ai fini probatori
- File di Office, file di immagine, file PDF

CF – metadati applicativi

- Il 30/1/03, il governo inglese pubblicò su un proprio sito web un dossier sulla struttura delle organizzazioni di intelligence e sicurezza irachene, che fu citato da Colin Powell nella sua relazione all'Assemblea delle Nazioni Unite il 5/2/2003
- Il Dr. G. Rangwala (U. Cambridge) si accorse che il dossier era stato in larghissima parte copiato da un articolo di un ricercatore del Monterey Institute of International Studies in California (e pubblicato su una rivista scientifica) senza citare la fonte

CF – metadati applicativi

*** WordDocument ***

Flags: +fExtChar+fWord97Saved

Locale identifier: 0x409 English (United States)

wMagicCreated: 6A62

Product created: 82198

cbMac: 39996

FileTime: 03/02/2003 12.18.31

Paul Hamill, Foreign Office

Communication Information Center
UK Government Office

Last authors (up to 10):

cic22 C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd

cic22 C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd

cic22 C:\DOCUME~1\phamill\LOCALS~1\Temp\AutoRecovery save of Iraq - security.asd

John Pratt, Downing Street

JPratt C:\TEMP\Iraq - security.doc

JPratt A:\Iraq - security.doc

Alison Blackshaw, uff. stampa
Primo Ministro

ablackshaw C:\ABlackshaw\Iraq - security.doc

ablackshaw C:\ABlackshaw\A\Iraq - security.doc

ablackshaw A:\Iraq - security.doc

Murthaza Khan, uff. stampa

MKhan C:\TEMP\Iraq - security.doc

MKhan C:\WINNT\Profiles\mkhan\Desktop\Iraq.doc

Copia da hard disk
a floppy disk

CF – metadati applicativi

Rif. Prof. Cosimo Anglano – Università degli Studi del Piemonte Orientale - "Informatica Forense ed Investigazioni Digitali" - http://digitalforensics.di.unipmn.it/Seminario_Ivrea.pdf

- I browser web memorizzano le informazioni di navigazione in appositi files
- Le informazioni che si possono recuperare sono:
 - indirizzo dei siti visitati e data ed ora della visita
 - ricerche effettuate su motori di ricerca
 - copie temporanee delle pagine visitate (cache)
 - cookies impostati dai siti visitati
- L'interpretazione di questi file consente di ricostruire l'attività di navigazione degli utenti

CF – navigazione su Internet

NetAnalysis - Forensic Internet History Analysis

File Filter Searching Sorting Tools Reports View Column Help

Record URL: 9

Last Visited [+0100]	Secondary Date	User	URL	Web Page Title	Search Engine Criteria
25/08/2004 17.12.52 mer	15/08/2004 17.53.28 dom		http://fok.ural.net/site.html		
25/08/2004 17.12.50 mer	01/11/2002 17.10.26 ven		http://fok.ural.net/		
25/08/2004 17.08.02 mer	25/08/2004 16.08.02 mer	Mr. Evil	http://www.whatsmyip.com	Your ip is 216.62.23.121 WhatIsMyIP.co	
25/08/2004 17.08.02 mer		mr. evil	http://www.whatsmyip.com/		
25/08/2004 17.08.02 mer	25/08/2004 11.08.02 mer	Mr. Evil	http://www.whatsmyip.com		
25/08/2004 17.07.57 mer	25/08/2004 11.07.57 mer	Mr. Evil	host: www.whatsmyip.com		
25/08/2004 17.07.51 mer		mr. evil	http://www.google.com/search?q=what+is+my+ip&hl=en&lr=&ie=UTF-8		
25/08/2004 17.07.51 mer	22/07/2004 23.05.08 gio	mr. evil	http://www.google.com/images/toolbar_promo.gif		
25/08/2004 17.07.51 mer	22/03/2004 23.05.03 lun	mr. evil	http://www.google.com/hav_next.gif		
25/08/2004 17.07.51 mer	22/03/2004 23.05.03 lun	mr. evil	http://www.google.com/hav_page.gif		
25/08/2004 17.07.51 mer	22/03/2004 23.05.03 lun	mr. evil	http://www.google.com/hav_current.gif		
25/08/2004 17.07.51 mer	22/03/2004 23.05.03 lun	mr. evil	http://www.google.com/hav_first.gif		
25/08/2004 17.07.51 mer	24/08/2004 02.40.46 mar	mr. evil	http://www.google.com/logos/summer2004_syndro_results.gif		
25/08/2004 17.07.51 mer	25/08/2004 16.07.51 mer	Mr. Evil	http://www.google.com/search?q=what+is+my+ip&hl=en&lr=&ie=UTF-8	Google Search: what is my ip	what is my ip
25/08/2004 17.07.51 mer			http://www.google.com/search?q=what+is+my+ip&hl=en&lr=&ie=UTF-8		what is my ip
25/08/2004 17.07.51 mer	25/08/2004 11.07.51 mer	Mr. Evil	http://www.google.com/search?q=what+is+my+ip&hl=en&lr=&ie=UTF-8		what is my ip
25/08/2004 17.07.32 mer		mr. evil	http://www.google.com/search?hl=en&ie=UTF-8&q=who+am+I		who am i
25/08/2004 17.07.32 mer			http://www.google.com/search?hl=en&ie=UTF-8&q=who+am+I		who am i
25/08/2004 17.07.32 mer	25/08/2004 16.07.32 mer	Mr. Evil	http://www.google.com/search?hl=en&ie=UTF-8&q=who+am+I	Google Search: who am i	who am i
25/08/2004 17.07.32 mer	25/08/2004 11.07.32 mer	Mr. Evil	http://www.google.com/search?hl=en&ie=UTF-8&q=who+am+I		who am i

www.digital-defective.co.uk

Type: Cache

Content: IES/index.dat

Offset: 336,688

URL Records: 9/45

CF – navigazione su Internet

Rif. Prof. Cosimo Anglano – Università degli Studi del Piemonte Orientale - "Informatica Forense ed Investigazioni Digitali" - http://digitalforensics.di.unipmn.it/Seminario_Ivrea.pdf

- I messaggi di posta elettronica salvati localmente possono essere estratti e decodificati dal formato proprietario dell'applicazione
- Ogni applicazione utilizza un formato proprietario quindi sono necessari tool in grado di interpretare i vari formati
- L'analisi delle intestazioni può rivelare il computer da cui il messaggio è stato spedito e la relativa data

CF – posta elettronica

- Molti reati sono compiuti utilizzando applicativi di Instant Messaging e Chat
 - Questi programmi memorizzano varie informazioni aventi valore probatorio sul computer su cui sono utilizzate:
 - log delle conversazioni (data, ora e contenuto)
 - file scambiati
 - lista dei contatti
 - Ci sono molte difficoltà dovute a un elevato numero di programmi e uso di **tecniche crittografiche** sui dati
- ## **CF – instant messaging e chat**

- Identificazione
- Acquisizione
- Conservazione
- Analisi
- **Valutazione**
- Presentazione

CF – passi operativi

- Durante la fase di analisi dei dati è necessario creare delle correlazioni tra essi, al fine di ricostruire gli eventi
- In questa fase si crea quindi una **Timeline Activity** del sistema, ovvero l'elenco completo delle caratteristiche dei file e dei metadati acquisiti in base ai loro MAC times (modified, access, created)

CF – valutazione dei dati

- Identificazione
- Acquisizione
- Conservazione
- Analisi
- Valutazione
- **Presentazione**

CF – passi operativi

- I risultati devono essere presentati in forma facilmente comprensibile
- I destinatari (giudici, avvocati, amministratori) non hanno di solito competenze informatiche approfondite
- Tuttavia è probabile che la relazione venga esaminata da un tecnico della controparte
- Semplicità e chiarezza, non superficialità e approssimazione

CF – reporting

- Computer potenti (l'analisi di tanti dati richiede elevata potenza di calcolo)
- Hard disk esterni firewire/usb2/ata/sata
- Write blocker HW o SW
- Software O.S. o proprietario
- Scheda di rete (alta velocità)
- Masterizzatore DVD
- Lettori di schede di memoria
- Lettori di SIM Card

CF – il laboratorio forense

- La crescente diffusione di dispositivi digitali, li rende fonte di potenziali prove. In particolare:

- Telefoni cellulari di (pen)ultima generazione
- Smart Phones
- Personal Digital Assistants
- Navigatori satellitari
- iPod ed iPhone
- Lettori MP3/MP4
- Videogame (PS2/3, Xbox, Nintendo, ecc.)

Forensics su altri media

- Questi dispositivi pongono nuove problematiche di non facile soluzione per le quali esistono soluzioni solo parziali
 - mancanza di standard per l'accesso e l'acquisizione (telefoni cellulari, navigatori satellitari, riproduttori MP3)
 - impiego di sole memorie volatili (PDA)
 - scarsa conoscenza del funzionamento dei sistemi operativi (di tipo proprietario)
 - scarsa conoscenza del formato dei file generati da applicazioni e sistemi operativi

Forensics su altri media

- Spesso è necessario ricostruire fatti analizzando il traffico di rete
 - Traffic capture and Packet analysis (Wireshark, NetIntercept, Netwitness)
 - Router/Switch Log analysis
 - Intrusion Detection/Intrusion Prevention (Snort)
 - Denial of Service
 - Analisi delle tracce di navigazione
 - Analisi di posta elettronica
 - P2P
 - Social Network (Facebook, Myspace, Linkedin)

Network Forensic

- Il NIST ha creato il **CFTT (Computer Forensics Tool Testing)** per la validazione degli strumenti (hardware e software) di computer forensic

<http://www.cftt.nist.gov>



CF – standardizzazione

- Alcuni stati hanno definito delle linee guida tecniche dettagliate con le corrette metodologie di analisi
 - RFC3227 - Guidelines for Evidence Collection and Archiving (2002)
 - USA – Department of Justice - Searching and Seizing Computers (2002)
 - USA – IACP - Best Practices for Seizing Electronic Evidence (2006)
 - USA – DoJ – Electronic Crime Scene Investigation v. 2 (2008)
 - UK – ACPO – Computer Based Evidence Guidelines v.4 (2008)

CF – standardizzazione

- In Italia esiste un'associazione di "Informatici Forensi", **IISFA** (**International Information Systems Forensics Association**) – Italian Chapter

<http://www.iisfa.it>

CF – IISFA Italian Chapter

- In Italia stanno nascendo i primi corsi di specializzazione in Informatica Forense
 - **Università Statale di Milano** - "Corso di perfezionamento in Computer Forensics e investigazioni digitali"
 - **Università di Teramo** - "Master in Sicurezza informatica e computer forensic"
 - **Università di Bologna** - "Corso di laurea di Operatore informatico giuridico"

Formazione e Certificazioni

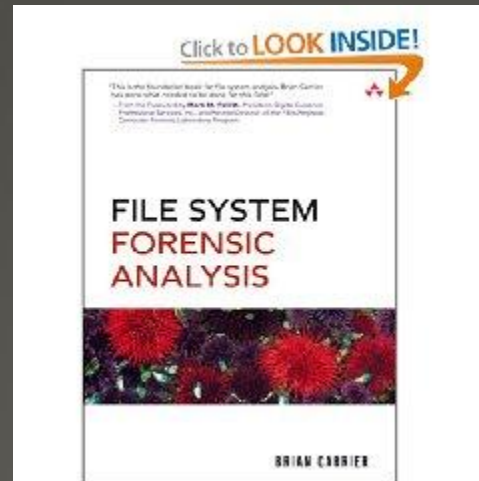
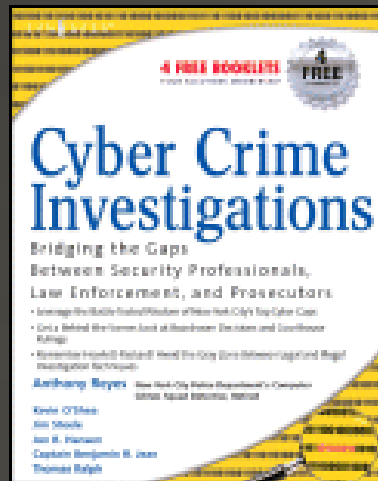
- In USA esistono corsi di laurea e diverse certificazioni riconosciute da ministero della Difesa e di Giustizia
- Le principali sono:
 - **Ec-Council CHFI** (Computer Hacking Forensic Investigator)
 - **Sans GCFA** (Giasec Certified Forensic Analyst)
 - **IISFA CIFI** (Certified Information Forensics Investigator)

Formazione e Certificazioni

- La Computer Forensics sta assumendo un ruolo sempre più importante in questioni legali (penali, civili ed amministrative)
- E' necessaria una maggior comprensione delle sue potenzialità e problematiche da parte degli "operatori del diritto" (magistratura, avvocati, p.g.)
- Esistono molti consulenti informatici e periti che improvvisano e spesso mancano di una formazione specifica
- Non esiste un criterio selettivo per diventare consulente e perito del tribunale (es. la laurea)

Conclusioni

- “File System Forensic Analysis” (Carrier) – Wesley – 2002
- “Cyber Crime Investigations (AA.VV.)” – Syngress – 2007
- “Computer Forensics” (Ghirardini, Faggioli) – Apogeo – 2007 (**Maggio 2009 nuova edizione**)



Riferimenti

- <http://www.cftt.nist.gov/>
- <http://www.iisfa.it/>
- <http://www.cybercrimes.it/>
- <http://www.marcomattiucci.it/>
- <http://www.cfitaly.net/>
- <http://www.ictlex.net/>
- <http://www.computerforensics.unimi.it/>
- <http://www.eccouncil.org/>
- <http://www.caine-live.net/>
- <http://www.deftlinux.net/>
- <http://www.e-evidence.info/>
- <http://www.forensicswiki.org/>

Riferimenti

- Queste slides sono rilasciate con licenza Creative Commons "Attribuzione-Non commerciale-Condividi allo stesso modo 2.5", il cui testo e' disponibile sul sito <http://creativecommons.org/licenses/by-nc-sa/2.5/it/legalcode>
- I contenuti di queste slide sono stati elaborati anche grazie a:
 - "Informatica Forense ed Investigazioni Informatiche"
Prof. Cosimo Anglano - Università del Piemonte Orientale
http://digitalforensics.di.unipmn.it/Seminario_Ivrea.pdf
 - "Computer Forensics" – Ing. Gianlugi Me
<http://gauguin.info.uniroma2.it/~italiano/Teaching/Security/forensics-b.pdf>
 - "Computer Forensics – Un'introduzione informale" – Gabriele Biondo
http://www.webbitcon.org/filemanager/download/2548/5927_biondo.ppt

Disponibilità slides



mattia.epifani@digital-forensics.it