

Indagini Digitali: Linux e l'Analisi Forense

Gianni Amato

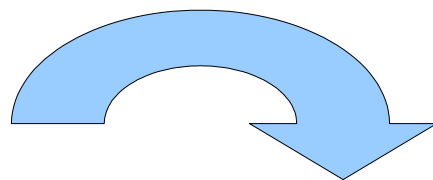


LinuxDay 2008
Reggio Calabria

CFI – Computer Forensics Italia

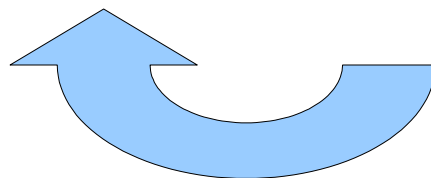
- Mailing list (..almeno finora)
- Si analizzano insieme i casi reali
- E' ispirata alla filosofia dell'Open Source
- Documentazione e sviluppo di forensics tools
- Corsi, convegni, rappresentanze
- Game

Security & Forensics



- Prepara
- Previene
- Riduce

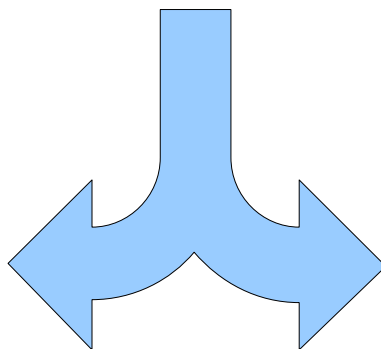
- Investiga
- Analizza
- Recupera



Security & Forensics

Incidente

Reazione



Ripristino

Computer Forensics

La disciplina che si occupa dell'identificazione, dello studio e della preservazione dei dati presenti su un computer al fine di evidenziare prove di reati informatici.

Quindi per le indagini giudiziarie (...e non solo).

Il computer come fonte di prova.

E' compito dell'Esaminatore Forense

- Studiare e ricostruire la scena del crimine informatico
- Analizzare le evidenze informatiche mediante metodologie scientifiche
- Presentare i risultati

Quindi: fornire risultanze che abbiano un valore legale e garantire che nulla abbia subito alterazioni in fase di analisi.

Perchè Linux?

- E' open source e questo comporta notevoli vantaggi:
 - il sorgente è visionabile da chiunque.
 - lunga vita alle vecchie versioni (facilmente reperibili).
- Linux supporta una enorme quantità di **filesystem** diversi.
- Linux dispone di numerosi **tools** per la forensics.
- Linux permette di montare le unità e i supporti removibili in modalità **solo lettura** (read-only).
- ...Bash è poesia.

Device

```
root@guelfoweb-laptop: ~  
File Modifica Visualizza Terminale Schede Ajuto  
root@guelfoweb-laptop:~# fdisk -l  
  
Disco /dev/sda: 120.0 GB, 120034123776 byte  
255 heads, 63 sectors/track, 14593 cylinders  
Units = cilindri of 16065 * 512 = 8225280 bytes  
Disk identifier: 0x8d231afa  
  
Dispositivo Boot      Start          End            Blocks      Id System  
/dev/sda1              1             1274          10233373+   27 Sconosciuto  
/dev/sda2 *           1275          7951          53627904    6  FAT16  
/dev/sda3              7952          14593         53351865    5  Estesio  
/dev/sda5              7952          9774          14643216    83  Linux  
/dev/sda6              9775          10260         3903763+    82  Linux swap / Solaris  
/dev/sda7             10261          14593         34804791    83  Linux  
  
Disco /dev/sdb: 4127 MB, 4127195136 byte  
16 heads, 32 sectors/track, 15744 cylinders  
Units = cilindri of 512 * 512 = 262144 bytes  
Disk identifier: 0xf0aa5dlc  
  
Dispositivo Boot      Start          End            Blocks      Id System  
/dev/sdb1              1             15744         4030448     c  W95 FAT32 (LBA)  
root@guelfoweb-laptop:~# █
```

hd = IDE
sd = SCSI

sda = 1° disco
sdb = 2° disco

sda1 = prima partizione logica del primo disco
sda2 = seconda partizione logica del primo disco

La Copia Forense

Non agire **mai** sul supporto originale

- Clonazione
- File immagine

esempi dd

```
# dd if /dev/hda of=/mnt/disk/immagine.dd bs 512 count=noerror sync
```

```
# dd if /dev/hda | nc 10.0.0.1 1234
```

```
# dd if=/dev/zero of=/dev/hda
```

Validazione

Confronto della copia con l'originale

L'Algoritmo di Hashing. Esiste ed è unico!

```
# md5sum /dev/hda
```

```
# sha1 /dev/hda
```

```
# md5sum /mnt/disk/immagine.dd
```

```
# sha1 /mnt/disk/immagine.dd
```

Hash collision?

Analisi

- Analisi Live
 - Live CD
 - device, ram, processi, history
- Analisi Post-Mortem
 - Copia forense
 - file, logs, images, registry

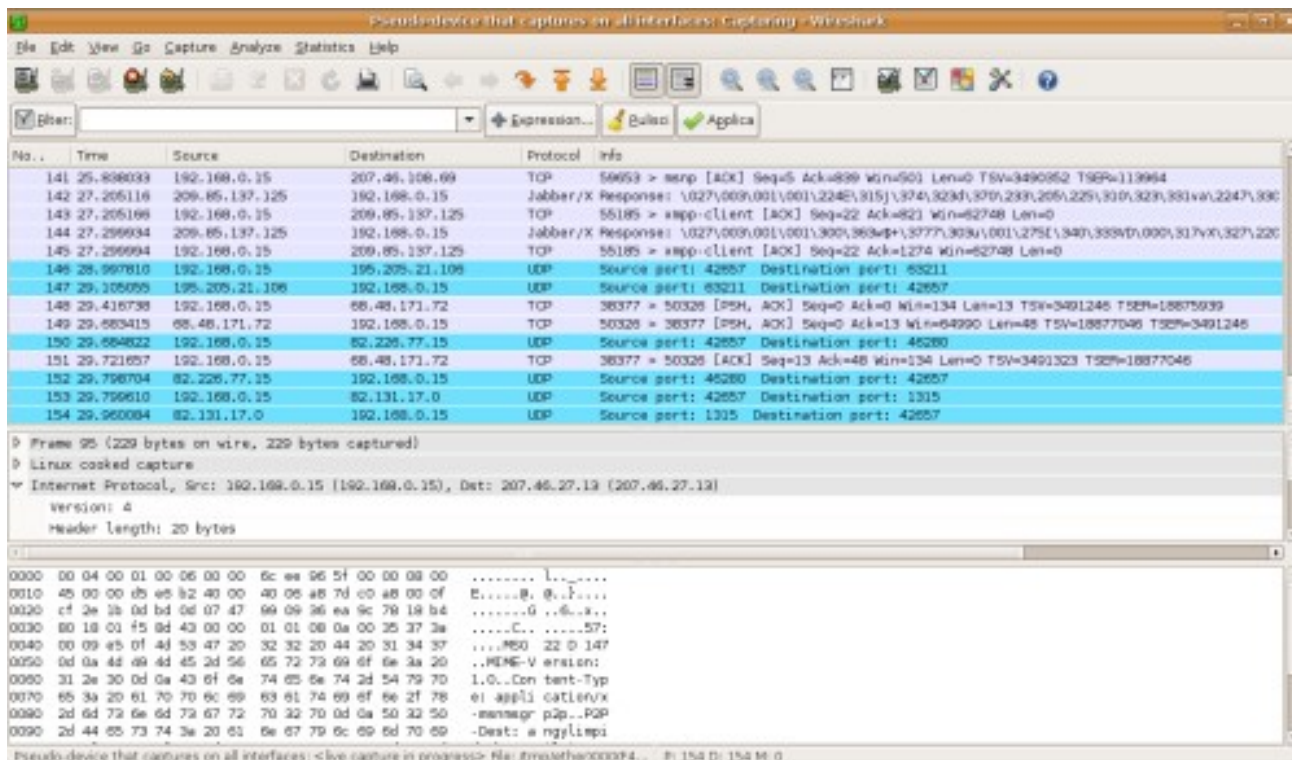
Alcune metodologie

- Timeline activity
- Caratteristiche del filesystem
- Registry Review
- File temporanei
- Ricerca delle keywords
- Ricerca immagini
- Contatti e conversazioni chat
- Carving (filetype / header)
- Cronologia e siti preferiti
- Recupero file eliminati
- Metadata e Active Data Stream
- Corrispondenza elettronica

Analisi protocolli

Wireshark

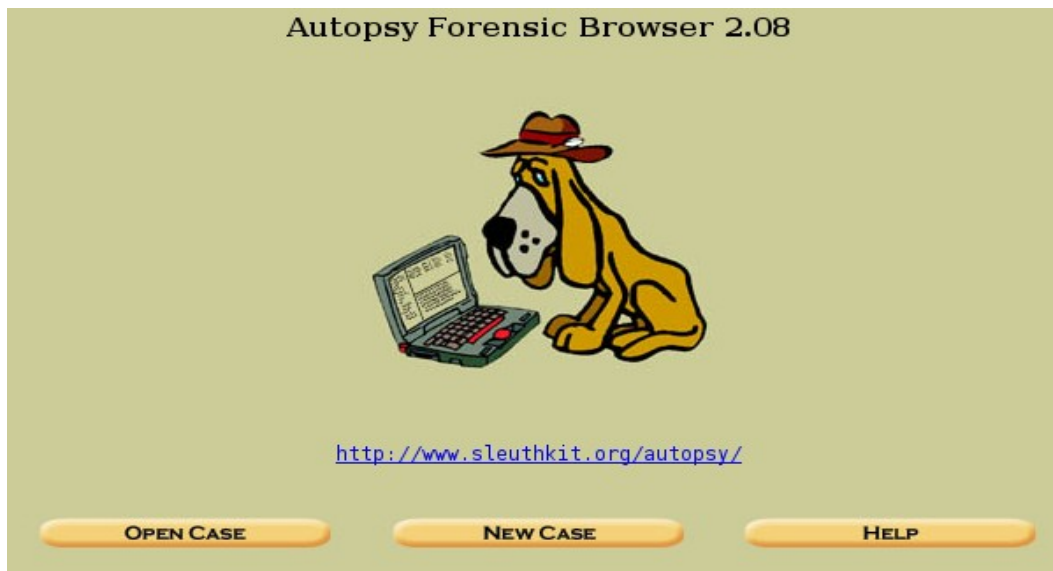
- cattura
- filtra
- ordina
- analizza



(libpcap)

L'Autopsia

Wikipedia: L'autopsia, chiamato anche esame post-mortem, è un esame medico dettagliato ed attento del corpo e dei relativi organi della persona dopo la morte per stabilirne le cause, le modalità ed eventualmente i mezzi che l'hanno prodotta



...l'autopsia di un disco non è poi così diversa da quella di un corpo umano

Recupero dei dati

Quando è possibile?

	FILE ANALYSIS	KEYWORD SEARCH	FILE TYPE	IMAGE DETAILS	META DATA	DATA UNIT	HELP ?	CLOSE X	
✓	r / r	Cartell.xls	2008.03.15 12:38:06 (CET)	2008.03.15 00:00:00 (CET)	2008.03.15 12:38:04 (CET)	0	0	0	86
✓	r / r	Cartell.xls	2008.03.15 12:38:16 (CET)	2008.03.26 00:00:00 (CET)	2008.03.15 12:38:04 (CET)	16896	0	0	89
✓	r / r	decreto-sicurezza-testo.doc	2008.03.17 17:03:08 (CET)	2008.08.08 00:00:00 (CEST)	2008.03.17 17:02:50 (CET)	864768	0	0	94
✓	r / r	documento.doc	2008.03.14 12:51:30 (CET)	2008.03.14 00:00:00 (CET)	2008.03.14 12:51:22 (CET)	46592	0	0	76
✓	r / r	documento.doc	2008.03.14 12:51:46 (CET)	2008.03.15 00:00:00 (CET)	2008.03.14 12:51:22 (CET)	46592	0	0	80
✓	r / r	documento.doc	2008.03.15 12:37:58 (CET)	2008.08.08 00:00:00 (CEST)	2008.03.14 12:51:22 (CET)	52736	0	0	84
	r / r	info	2008.10.13	2008.10.22	2008.10.13	1067	0	0	24

Carving

<header>

...

...

...

</footer>

```

audit.txt
Foremost version 1.5 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Fri Oct 24 22:50:35 2008
Invocation: foremost -s 1 -i /home/guelfoweb/Scrivania/p7300036.jpg
Output directory: /home/guelfoweb/output
Configuration file: /etc/foremost.conf
-----
File: /home/guelfoweb/Scrivania/p7300036.jpg
Start: Fri Oct 24 22:50:35 2008
Length: 61 KB (63150 bytes)
Skipping: 512 B (512 bytes)

Num      Name (bs=512)      Size      File Offset      Comment
0:       00000003.jpg      9 KB      1926
Finish: Fri Oct 24 22:50:35 2008


1 FILES EXTRACTED

jpg:= 1
-----

Foremost finished at Fri Oct 24 22:50:35 2008

```

Trova le differenze




Nome: gianniamato.jpg

Tipo: Immagine JPEG

Dimensione: 6,3 kB (6492 byte)

Posizione: /home/guelfoweb/Scrivania

Tipo MIME: image/jpeg



Nome: gianniamato (copia).jpg

Tipo: Immagine JPEG

Dimensione: 6,3 kB (6492 byte)

Posizione: /home/guelfoweb/Scrivania

Tipo MIME: image/jpeg

gianniamato.jpg - GHex

File Modifica Vista Finestre Aiuto

00000000	FF D8	FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 00JFIF.....
00000011	60 00 00 FF DB 00 43 00 03 02 02 03 02 02 03 03 03C.....	
00000022	03 04 03 03 04 05 08 05 05 04 04 05 0A 07 07 06 08		

gianniamato (copia).jpg - GHex

File Modifica Vista Finestre Aiuto

00000000	DD D8	FF E0 00 10 4A 46 49 46 00 01 01 01 00 60 00JFIF.....
00000011	60 00 00 FF DB 00 43 00 03 02 02 03 02 02 03 03 03C.....	
00000022	03 04 03 03 04 05 08 05 05 04 04 05 0A 07 07 06 08		

Risalire alla foto originale



EXIF && THUMBNAIL



Domande



Info & Contatti

Gianni Amato

Web: <http://www.gianniamato.it>
<http://www.securityside.it>

E-mail: gianni.amato@gmail.com
amato@securityside.it

Cell: +39 320 28 42 382