Ordine degli Ingegneri di Pisa
Talent Garden Pisa
Via Umberto Forti 6, Montacchiello (PI)
26 Maggio 2017 – 09:00-19:00

Computer Forensics e Sicurezza Informatica

Dalla costruzione di una timeline alla rilevazione e ricostruzione di un attacco informatico

Marco A. CALAMARI – marco.calamari@ordineingegneripisa.it
IISFA - Information Systems Forensics Association: Italian Chapter

Igor Falcomatà – ifalcomata@enforcer.it
Enforcer Network Security

Copyleft 2017, Marco A. Calamari

Questo materiale e' rilasciato sotto licenza Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo 3.0 Italia (CC BY-NC-SA 3.0 IT)

https://creativecommons.org/licenses/by-nc-sa/3.0/it/deed.it

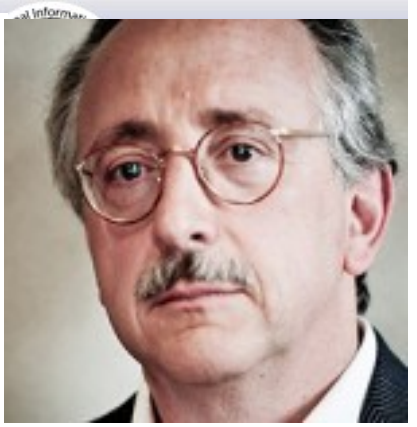
Alcune immagini della presentazione sono citazioni o "fair use" di opere protette da copyright dei legittimi proprietari.

Tutti i marchi citati appartengono ai legittimi proprietari

Un particolare ringraziamento all'amico e collega Paolo Giardini per il materiale gentilmente messo a disposizione

Il vostro anfitrione

https://www.linkedin.com/in/marcocalamari/



- **Marco Calamari, classe 1955, ingegnere nucleare, si cimenta a rotazione tra attivita' di consulenza tecnica informatica, editoriali e di formazione.**
- **Qualche sigla: IISFA, AIP, Opsi, HERMES, PWS.**
- **Appassionato di privacy e crittografia, ha contribuito ai progetti FOSS Freenet, Mixmaster, Mixminion, Tor e Globaleaks.**
- **Fondatore del Progetto Winston Smith e del Centro Hermes per la Trasparenza ed i diritti digitali.**
- **In concorrenza con i veri giornalisti, dal 2003 scrive su Punto Informatico ed altre riviste la rubrica settimanale "Cassandra Crossing", che dal 2005 a oggi e' quasi arrivata alla 400ma puntata … (www.cassandracrossing.org)**

Quindi parleremo di ...

La computer forensics (autopsia informatica) e' una disciplina tecnica come tante altre affrontate quotidianamente da ingegneri, sia come tecnici che come consulenti di parte o del Giudice.

Affrontata a livelli ordinari puo' essere ripulita dalla patina di irraggiungibilita' e rivelarsi tranquillamente alla nostra portata.

Questo secondo corso affrontera’ in maniera molto piu’ dettagliata (e quindi anche meno divertente) gli stessi argomenti del primo, estendendoli fino alla generazione di una timeline.

Saranno inoltre trattati estesamente i problemi di sicurezza informatica che possono portare a danneggiamenti tali da richiedere l’uso di tecniche di CF per scoprirne le tracce, ricostruire gli eventi e tentare il recupero delle informazioni con le tecniche di CF.

Quindi parleremo di ...

IISFA European Chapter

Prima parte

- Organizzazione delle informazioni su disco e su scheda SD: boot block, tavola delle partizioni e filesystem
- Elementi del protocollo TCP/IP
- Crittografia
-

Seconda parte

- Utilizzo di distribuzioni Linux live
- Caine/Kali forensic distribution
- Carving di una immagine
- Creazione di una timeline
- Utilizzo di macchine virtuali

Terza parte

Incidenti informatici: Attacchi alle postazioni di lavoro

- falsificazione email (mail spoofing)
- phishing e spear phishing
- social engineering / OSINT
- accesso fisico
- malware
- attacchi "client-side"

Quindi parleremo di ...

IISFA European Chapter

Quarta parte

Incidenti informatici: Attacchi alle reti e ai server

- **arp poisoning**
- **spoofing**
- **denial of service**
- **MITM su SSL**
- **partizionamento delle reti**
- **filtri sul traffico e firewalling**
- **esempi di vulnerabilità e misconfigurazioni più diffuse**
- **network/service discovery**
- **vulnerabilità note / software obsoleto**
- **password guessing**
- **esempi di vulnerabilità e misconfigurazioni più diffuse**

Standard Disclaimer

IISFA European Chapter

Le informazioni contenute in questa presentazione, se male utilizzate, possono produrre effetti negativi come, ma non limitati a:

- **Perdita di dati**
- **Cancellazione di file**
- **Blocco del computer**
- **Distruzione di informazioni**
- **Scongelamento del frigorifero**
- **Rottura di relazioni sentimentali**

(aggiungete altri vostri incubi a piacere...)

QUINDI, OCCHIO!

Io, comunque, vi avevo avvertito

Zeresima parte

Test di qualche prerequisito

Hardware e software necessari

TEST:
Prerequisiti ad un corso di computer forensics?

1)I file messi nel cestino sono cancellati?
2)I file messi nel cestino svuotato sono cancellati?
3)I file di un computer reinstallato sono cancellati?
4)I file di un hard disk formattato sono cancellati?
5)I file di un disco formattato a basso livello sono cancellati?
6)I file di un hard disk portato sopra il punto di Curie sono cancellati? (Non chiedetemi cos'e' il punto di Curie per favore)
7)I file di un hard disk tritato in pezzi cosi fini che passino tutti da un setaccio di 3 mm. sono cancellati? (non e' uno scherzo ma uno standard DoD)

Prima parte

dischi e filesystem

L'ambito della computer forensics

- Non pensate solo ai computer
  - Penne USB
  - Dischi esterni
  - Tablet
  - Navigatori
  - Lettori mp3
  - Cellulari
  - Smartphone
  - Macchine fotografiche
  - In futuro, non tanto lontano: *automobili*

NB: tutti apparati anche connessi ad Internet...

Ma non solo...

Oltre alle cose che possiamo fisicamente “avere fra le mani” l'investigatore si dovrà confrontare con sistemi Cloud ed allora le cose si complicano...

La normativa nella CF

- Non esistono norme di legge, a parte quanto stabilito dalla convenzione di Budapest del 2001 sulle modalità di preservazione delle prove informatiche.
- Ci sono però Best Practices che suggeriscono le regole fondamentali per l'acquisizione delle copie valide sia nell'analisi investigativa che per il recupero di file cancellati dal computer di casa.
- Si basano sulla RFC 3227 “Guidelines for Evidence Collection and Archiving” del 2002, Vecchia ma sempre valida (anche se specificatamente riferita ad “incidenti di sicurezza”).
- Esistono anche altre norme, come la ISO 27037 e la ISO/IEC 27037-2012.

Il codice di procedura penale

- L'art. 244 CPP “Casi e forme delle ispezioni” modificato a seguito del recepimento della convenzione di Budapest (legge 18/3/2008 n. 48) recita:

«L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l’alterazione».

Best practices

- Non utilizzare il sistema. Spegnere anche brutalmente e non riaccenderlo (punto controverso; secondo voi perche')
- Calcolare hash ms5 e sha del supporto per poter successivamente determinare la corrispondenza delle copie con l'originale
- Procedere alla copia fisica del supporto, calcolare hash della copia e confrontarlo con l'originale
- Non utilizzare mai l'originale. Etichettarlo e riporlo in luogo protetto
- Se necessario accedere al disco originale, effettuare un mount con l'opzione "read only" o tramite block writer
- Documentare tutto e mantenere intatta la catena di custodia

La regola fondamentale

- Data l'assoluta necessità di non alterare il contenuto del supporto in esame è indispensabile utilizzare strumenti che impediscano qualsiasi operazione di scrittura sul supporto informatico in esame, cosa che potrebbe invalidare la prova.

Hardware e software

Per fortuna nella CF i lavori “semplici” sono frequenti, e per questi i prezzi stracciati dell’elettronica cinese, l’e-commerce ed il software libero (FOSS) ci vengono in aiuto; i numeri allora cambiano molto.

Ribadiamo pero’ un concetto ben noto: si impara a camminare e poi a volare, dal semplice al complesso.

L’uso esclusivo che faremo di software libero non significa che per il fini dell’analisi forense sia migliore o peggiore di quello proprietario, ne’ e’ ispirato a considerazioni filosofiche.

Il motivo banale e’ che il suo uso abbassa, anzi quasi azzera la soglia di ingresso economica per chi vuol crescere in questa direzione … e non e’ poco!

Cavo SATA-EIDE to USB3

IISFA
European Chapter

Cavo SATA-EIDE to USB3

IDE 44Pin for 2.5"HDD

IDE 40Pin for 3.5"HDD

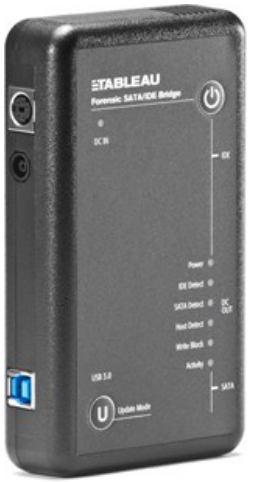
IDE 40Pin for CD-ROM

For 3.5" SATA HDD

For 2.5" SATA HDD

Strumenti hardware

- I Block writer sono strumenti che interposti fra supporto in esame e computer intercettano e bloccano le richieste di scrittura.
- I Disk Duplicator permettono di effettuare una copia speculare di un disco (clone) senza necessità di collegarlo ad un computer.



Un caso di studio

Quale potrebbe essere un caso tipico ma non banale di analisi forense alla nostra portata?

Analisi di un laptop alla ricerca di documenti riservati che potrebbero essere stati inviate per posta e/o cancellati

Step da eseguire

- **Documentazione fotografica del laptop**
- **Creazione dell'immagine forense del disco**
- **Estrazione dei file di interesse**
- **Elaborazione di file particolari (posta elettronica)**
- **Carving alla ricerca di file cancellati**
- **Creazione di una Timeline degli eventi**

Acquisizione immagine forense

IISFA
European Chapter

Acquisizione immagine forense

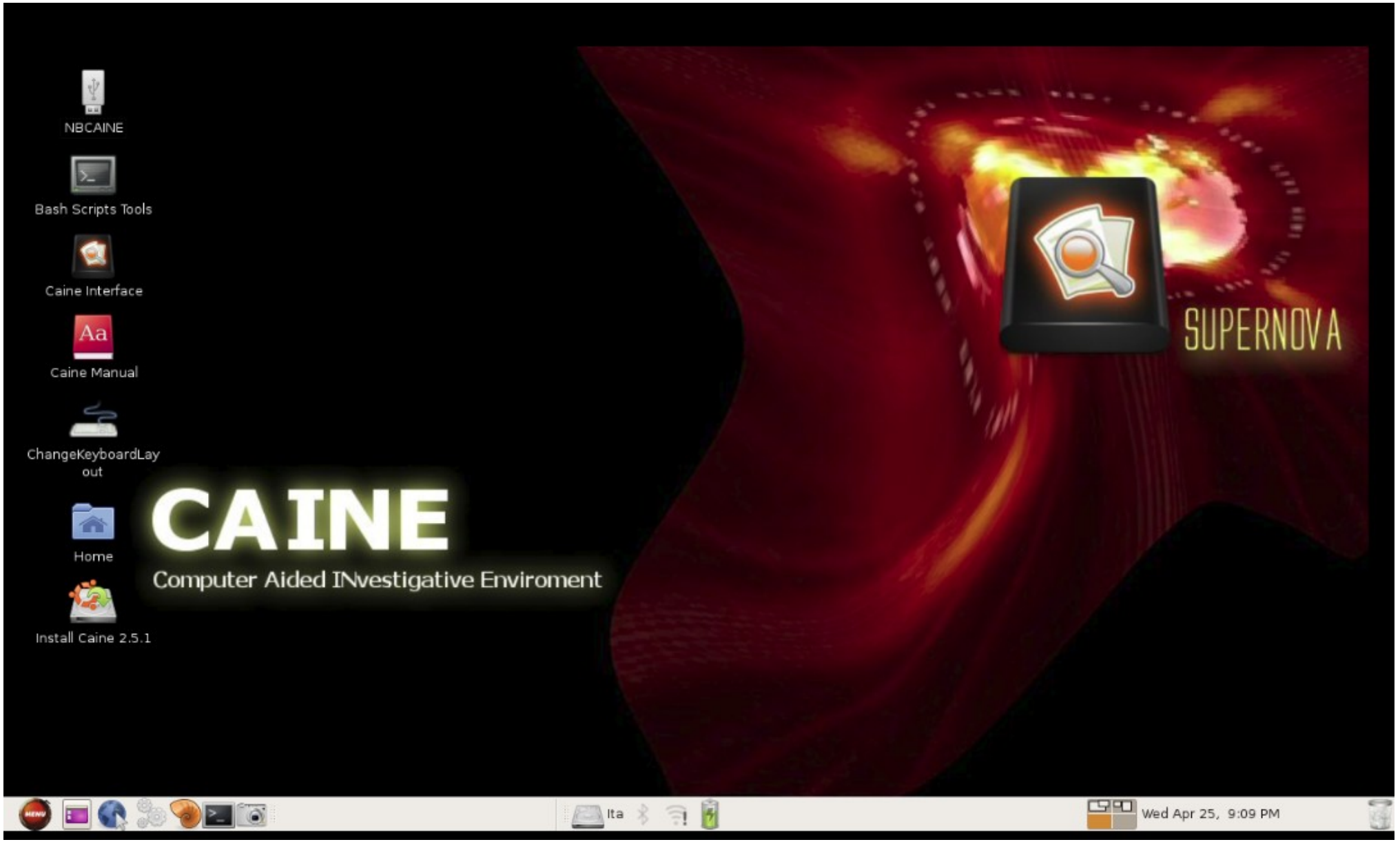
IISFA European Chapter

Acquisizione immagine forense

IISFA
European Chapter

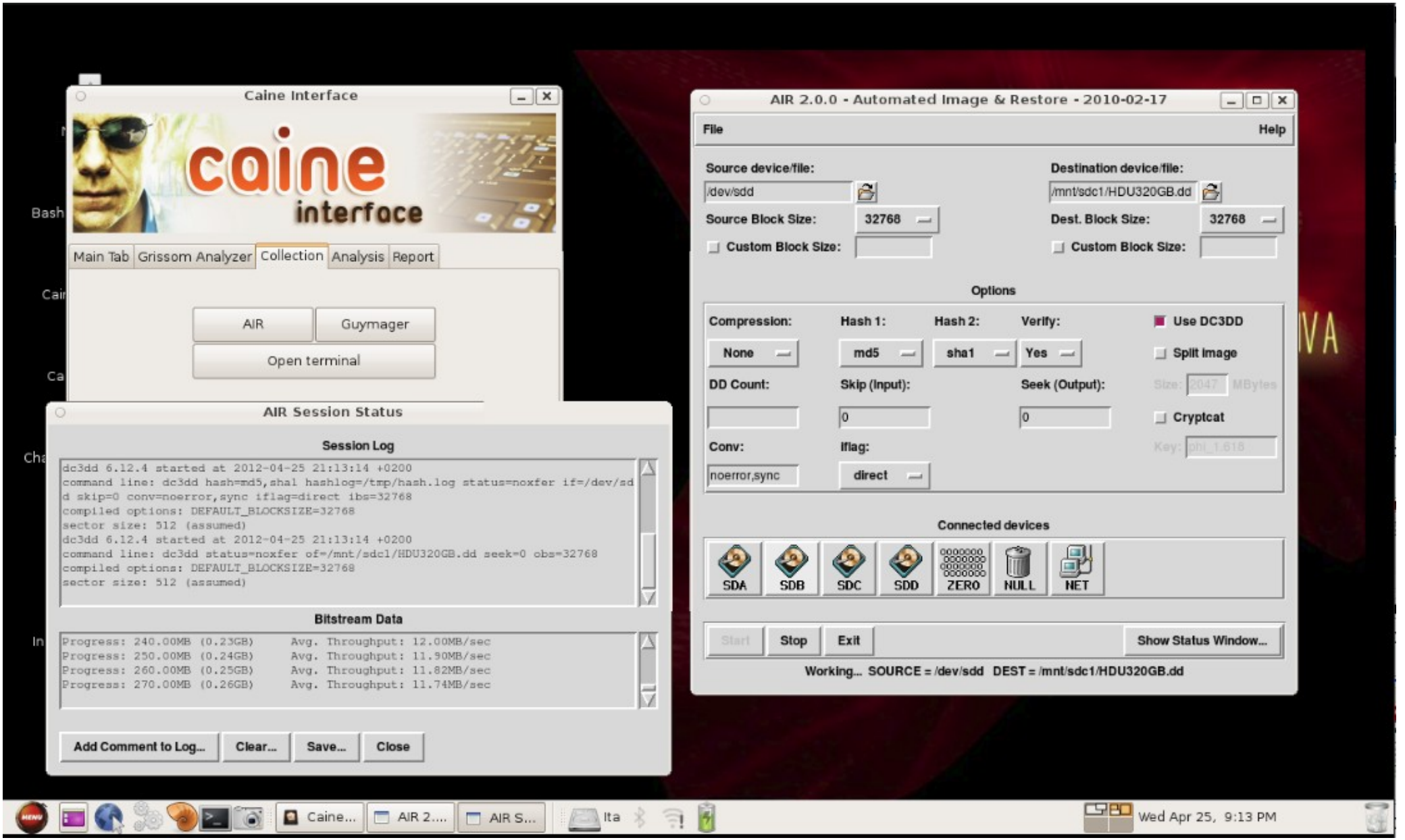
Acquisizione immagine forense

IISFA European Chapter



Acquisizione immagine forense

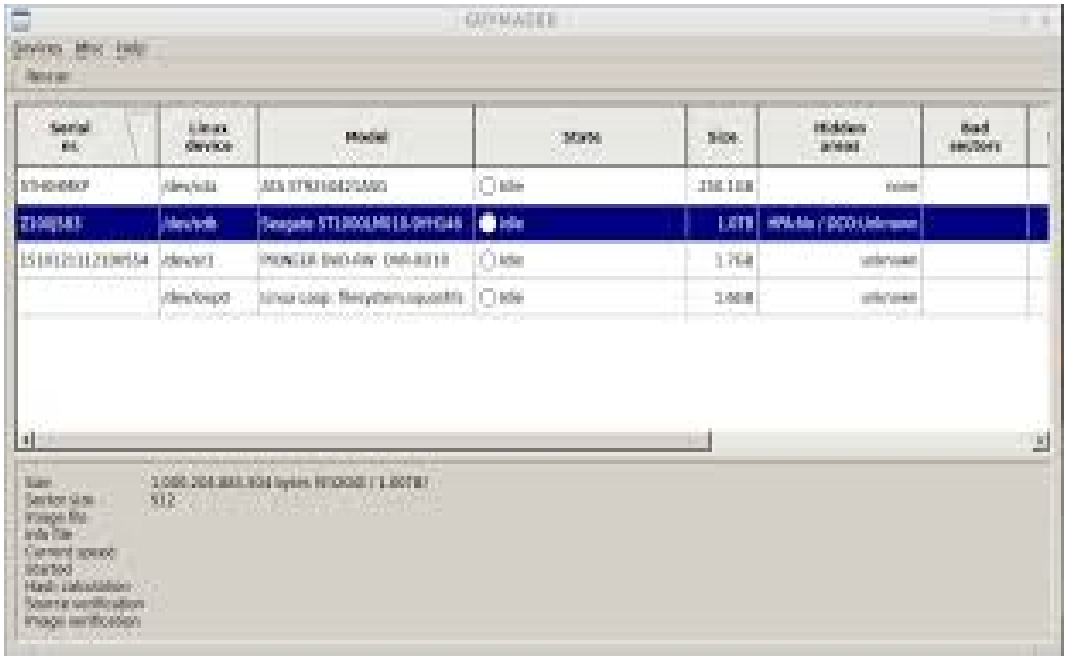
IISFA European Chapter



Distribuzioni GNU/Linux forensi

Software per copia forense

- **Il classico dd e la sua versione speciale per recupero di supporti con settori danneggiati ddrescue e dd_rescue**
- **Guymager, interfaccia grafica per il cloning dei device in vari formati (EWF, AFF, RAW)**
- **Cyclone, tool a linea di comando per copie in formato EWF e RAW**



Software per Analisi e Carving

Sono programmi che analizzano il contenuto del disco sia via file system sia accedendo direttamente al supporto senza usareil file system):

1) **Tool generici per l'esame del contenuto dei supporti informatici**
   - **The Sleuth Kit + Autopsy**
   - **Bulk extractor**
2) **Tool specifici per tipo di analisi**
   - **Analisi della navigazione internet**
   - **Analisi della posta elettronica**
   - **Analisi chat, immagini, …**
3) **Tool per il recovery di file e partizioni**
   - **Testdisk**
   - **Photorec**
   - **Foremost**
   - **Scalpel**

Formati standard dei file immagine

Raw format (.dd)
Copia bit a bit dell'originale. E' possibile spezzare il file immagine in file gestibili dal S.O.
Advanced Forensic Format (.AFF)
Le specifiche del formato sono open source. Il file immagine è compresso ed occupa molto meno spazio dell'originale. All'interno del file immagine vengono memorizzate le informazioni relative all'evidenza (data, modello del disco, serial numer, hash, ecc.).
Expert Witness Format (. E01)
E' un formato proprietario ma molto diffuso, divenuto standard di fatto. Tramite reverse engineering è stato possibile individuare le specifiche e fare si che tutti i software per forensics riconoscano e possano utilizzare questo formato. L'immagine del disco viene spezzata e salvata in file numerati (E01, E02,...) e contiene le informazioni sul supporto originale e sul caso in esame.

Altri formati: esistono numerosi altri formati di uso meno comune. Il formato AFF non è più supportato, secondo una dichiarazione riportata sul sito di Guymager.

Esempio con formato RAW

- Effettuare la copia

```
# dd if=/dev/.... of=/temp/file.dd
```

- Individuare l'offset della partizione

```
# mmls /temp/file.dd (oppure con fdisk /dev/...)
```

- Calcolare offset e montare la partizione in sola lettura

```
# mount -o ro,offset=$((512*2048)) /temp/file.dd /mnt/mountpoint
```

- Smontare l'immagine

```
# umount /mnt/mountpoint
```

Esempio con formato AFF

- Effettuare la copia con Guymager
- Montare il disco in formato RAW

affuse file.aff /mnt/mountpoint

- Individuare l'offset della partizione

mmls /mnt/mountpoint/file.aff.raw

(oppure mmls /dev/device, oppure mmls file.aff od anche usare fdisk)

- Calcolare offset e montare la partizione in sola lettura

mount -o ro,offset=$((512*2048)) /mnt/mountpoint/file.aff.raw /mnt/partizione

Esempio con formato AFF
(smontare)

- Per rimuovere il device è necessario prima smontare la partizione logica e poi smontare il disco RAW. Notare i diversi comandi utilizzati.

- Smontare partizione

```
# umount /mnt/partizione
```

- Smontare immagine RAW

```
# fusermount -u /mnt/mountpoint
```

Esempio con formato EWF

- Effettuare la copia con Guymager
- Montare il disco in formato RAW

```
#  xmount --in ewf file.E0* /mnt/disk1
```

- Individuare l'offset della partizione

```
# mmls /mnt/mountpoint/file.dd
```

```
(oppure mmls /dev/device, oppure mmls file.aff od
anche usare fdisk)
```

- Calcolare offset e montare la partizione in sola lettura

```
# mount -o ro,offset=$((512*2048))
/mnt/mountpoint/file.dd /mnt/partizione
```

Esempio con formato EWF
(smontare)

- Per rimuovere il device è necessario prima smontare la partizione logica e poi smontare il disco RAW. Notare i diversi comandi utilizzati.

- Smontare partizione

```
# umount /mnt/partizione
```

- Smontare immagine RAW

```
# fusermount -u /mnt/mountpoint
```

Software per l'analisi

- Dal punto di vista software, sono utilizzati programmi che analizzano il contenuto del supporto sia attraverso il file system sia accedendo direttamente al supporto a prescindere dalla logica della sua organizzazione (dipendente dal file system). Un elenco non esaustivo:
  - Tool generici per l'esame del contenuto dei supporti informatici
    - The Sleuth Kit + Autopsy
    - Bulk extractor
    - Tool classici della shell (grep, hex editor, text editor, find, shell script)
  - Tool specifici per tipo di analisi
    - Analisi della navigazione internet
    - Analisi della posta elettronica
    - Analisi chat, immagini, …
  - Tool per il recovery di file e partizioni
    - Testdisk
    - Photorec
    - Foremost
    - Scalpel

The Sleuth Kit e Autopsy

- The Sleuth Kit (TSK) è una suite di programmi per analisi delle immagini di dischi e file system. Può essere utilizzata a linea di comando oppure tramite la sua interfaccia grafica.

- Autopsy è l'interfaccia grafica di TSK.

Passiamo alla pratica

Caso pratico

Ho cancellato le foto delle vacanze!

E adesso?

Basta armarsi pazienza e degli strumenti di base per il file carving

File Carving è l'operazione di ricerca (e recupero) di file basato sul contenuto e non sui metadati

Proveremo photorec, foremost, scalpel, testdisk.

Ovviamente sono tutti software open source, e non sono i soli programmi di questo tipo disponibili :-)

Qualche nozione di base

- I file system memorizzano i file in piccole unità di allocazione chiamate “cluster” registrando la posizione del file, il nome ed altre informazioni definite metadati (data creazione, proprietario, permessi, data modifica...) in speciali strutture che cambiano a seconda del tipo di file system
- Un file sarà scritto su più cluster, creando una “*catena*” di cluster e una “*mappa*” che identifica quali cluster appartengono al file.
- All'inizio ed alla fine della “*catena*” di cluster sono posti delle sequenze di caratteri che identificano il tipo di file: header e footer

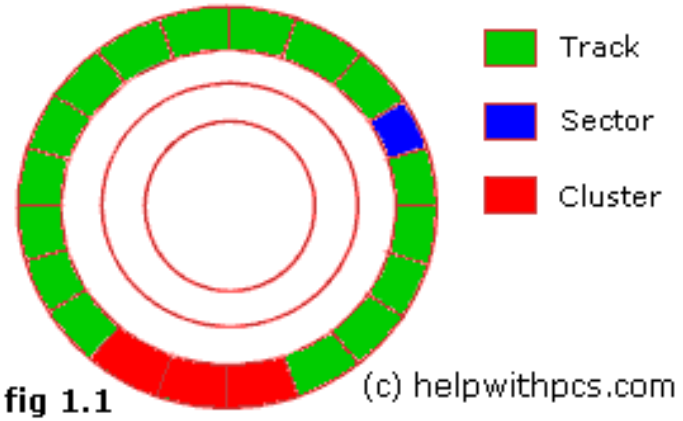


fig 1.1

Master boot record, partition table, boot sector

- Il settore zero del disco contiene il Master Boot Record (MBR) lungo 512 byte.
- Il programma contenuto nell'MBR legge la Partition Table e lancia il sistema operativo.
- La Partition Table (PT) è memorizzata negli ultimi 66 byte del MBR.
- Gli ultimi 2 byte della PT contengono il codice AA55H che indica la fine del MBR.
- La PT contiene le informazioni sulle suddivisioni logiche del disco dette partizioni e indica quale di queste è quella di boot.
- All'inizio di ciascuna partizione si trova il Boot Sector che contiene il programma di avvio del sistema operativo installato.

Master Boot Record

All'offset 00001b8 si trova l'ID del disco in formato little endian

```
#fdisk -lu
Disk /dev/sda: 750.2 GB, 750156374016 bytes
255 testine, 63 settori/tracce, 91201 cilindri, totale 1465149168 settori
Unità = settori di 1 * 512 = 512 byte
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Identificativo disco: 0x0004e447
...

#hexdump -n 512 /dev/sdb
...
0000190 6d6 f 4800 7261 2064 6944 6b73 5200 6165
00001a0 0064 4520 7272 726f 0a0d bb00 0001 0eb4
00001b0 10cd 3cac 7500 c3f4 e447 0004 0000 2000
00001c0 0021 4b82 0a81 0800 0000 0000 0080 4b80
...
```

Marcatore fine MBR

Alla fine del blocco di 512 byte si trova il marcatore di fine MBR costituito dai caratteri AA55

```
00001b0 10cd 3cac 7500 c3f4 e447 0004 0000 2000
00001c0 0021 4b82 0a81 0800 0000 0000 0080 4b80
00001d0 0a82 fe83 ffff 0800 0080 0000 0c35 fe00
00001e0 ffff fe83 ffff 0800 0cb5 5800 4a9f 0000
00001f0 0000 0000 0000 0000 0000 0000 0000 aa55
```

Partition Table

La Partition Table è composta da 4 record di 16 byte che contengono tutte le informazioni relative alle partizioni create sul disco.
I record delle 4 partizioni possibili sono così posizionati:

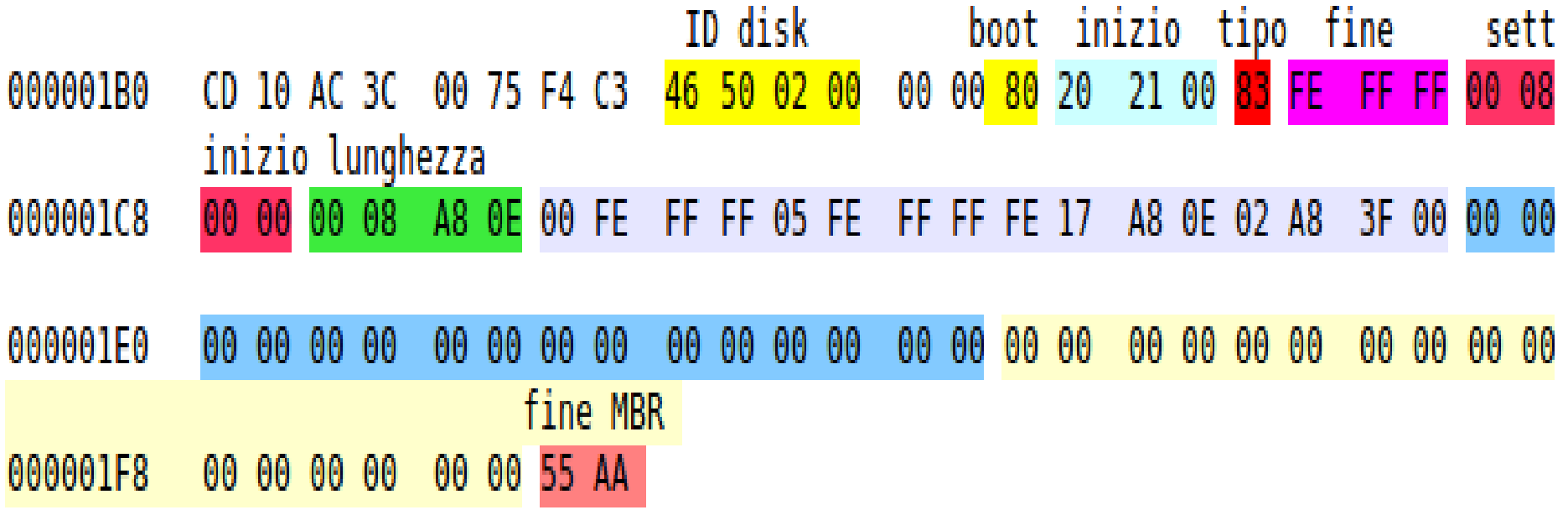
Offset 1be - 1cd	prima partizione
Offset 1ce - 1dd	seconda partizione
Offset 1de - 1ed	terza partizione
Offset 1ee - 1fd-	quarta partizione

Partition Table

Il significato di ciascun byte di ogni record è il seguente:

Byte	Descrizione
0	Indicatore del boot: 0 non bootabile, 80h bootabile
1-3	Testina, Settore, Cilindro inizio partizione
4	Tipo di partizione
5-7	Testina, Settore, Cilindro fine partizione
8-11	Settore inizio partizione
12-15	Numero di settori della partizione

Partition table

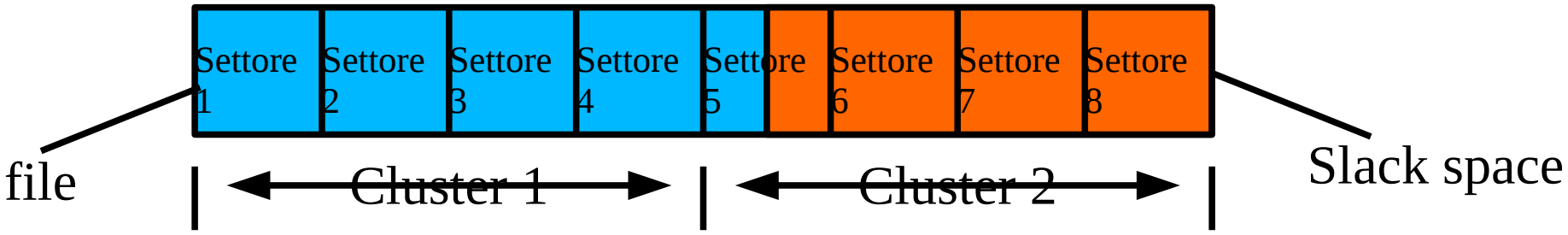



```
# fdisk -lu
Disk /dev/sda: 128.0 GB, 128035676160 bytes
255 testine, 63 settori/tracce, 15566 cilindri, 250069680 ettori
Unità = settori di 1 * 512 = 512 byte
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Identificativo disco: 0x00025046

Dispositivo Boot      Start         End      Blocks   Id  System
/dev/sda1   *        2048   245895167   122946560   83  Linux
/dev/sda2       245897214   250068991     2085889    5  Esteso
/dev/sda5       245897216   250068991     2085888   82  Linux swap
```

La cancellazione di un file

- Quando viene cancellato un file viene solo apposto un flag (l'operazione effettiva è diversa in base ai file system) per indicare che il file è "*deleted*" ed i cluster utilizzati dal file cancellato vengono resi nuovamente disponibili per altri file.
- L'operazione di cancellazione di un file non ripulisce i cluster del loro contenuto permettendo così il recupero dei file cancellati se non sono stati sovrascritti.
- Se il contenuto di un file non riempie completamente un cluster, possono rimanere parti del file che occupava precedentemente quel cluster. Si parla di Slack Space.



Attenzione!

- E' fondamentale non utilizzare il supporto originale per evitare di sovrascrivere i cluster contenenti i dati da recuperare.
- Tutto questo non funziona su dischi SSD se è attivata la funzione TRIM. In questo caso il cluster viene immediatamente cancellato perché sia disponibile per altri file. In generale, un file cancellato su un disco SSD è irrecuperabile.

Lavoriamo sulla copia

- Procurarsi un supporto di capacità adeguata dove scrivere i file recuperati
- Assicurarsi di utilizzare una distribuzione specifica per la forensic, ovvero, che almeno non effettui il montaggio automatico di partizioni e dispositivi (es. chiavette USB)
- Le distribuzioni “Forensics” Deft e Caine sono configurate di default in questo modo, altre (p.e. backtrack) possono essere avviate in modalità “forensic”
- Utilizzare “dd” od un sw equivalente per creare una immagine bit to bit del supporto originale

Passiamo alla pratica

- Abbiamo una scheda MMC da 65 MB (per questioni di tempo...)
- La prepariamo per la demo.
  - Azzerare il contenuto riempiendo il device di zero
  - Creare nuova tabella delle partizioni
  - Creare nuovo file system; utilizzeremo FAT32, il FS utilizzato da molte fotocamere
  - Montare la MMC preparata, copiare alcune immagini e verificarne la presenza
  - Cancellare i file
- Riusciremo a recuperare i nostri file?

Pronti? Via

- Verifica del nome del dispositivo

```
fdisk -lu
Dispositivo Boot      Start         End      Blocks   Id  System
/dev/sdb1            2048      124927       61440    b  W95 FAT32
```

- Riempiamolo di zeri ! (carattere null)

```
dd if=/dev/zero of=/dev/sdb
```

Piccolo trucco

- dd non da alcuna indicazione dell'avanzamento del lavoro
- Un trucco per non farsi prendere dalle paranoie tipo “si sarà bloccato?” è usare il comando kill
- Apriamo un'altra shell e digitiamo:

```
#ps fax | grep dd
2948 … sudo dd if=/dev/zero of=/dev/sdb  <<< il processo lanciato
2949 ...\ dd if=/dev/zero of=/dev/sdb   <<<< il processo figlio
```

Diamo il comando:

```
#kill -USR1 2949    <<< usiamo il process ID  figlio!
```

Piccolo trucco

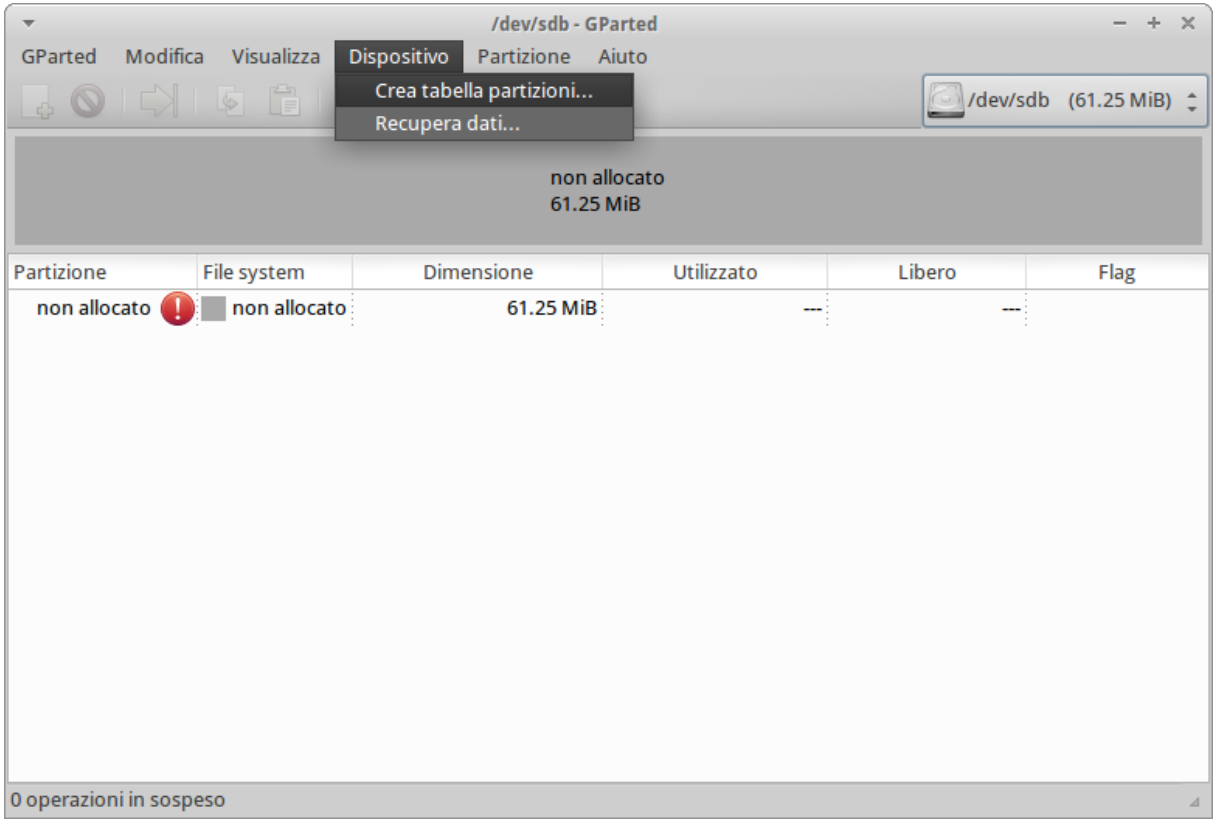
- Sulla shell dove gira dd vedremo qualcosa di simile:

```
100537+0 record dentro
100537+0 record fuori
51474944 byte (51 MB) copiati, 33,0879 s, 1,6 MB/s
125441+0 record dentro
125440+0 record fuori
64225280 byte (64 MB) copiati, 81,9182 s, 784 kB/s
```

- Con fdisk possiamo verificare che non esiste più la tabella delle partizioni, la scheda MMC non contiene più nulla

Creiamo un file system nuovo

- Utilizziamo gparted per creare una nuova tavola delle partizioni e file system FAT32 (potremmo usare altro, come fdisk)



Avanti!

- Montiamo la scheda
- Copiamo alcuni file nella scheda
- Verifichiamo che sia tutto ok
- Cancelliamo i file !

#root@/recovery# mount /dev/sdb1 ../mountpoint/

#root@/recovery# cd ../mountpoint/

#root@/mountpoint# ls -la

-rwxr-xr-x 1 root root 47457 ott 22 19:25 2013-10-22-192559.jpg

-rwxr-xr-x 1 root root 57916 ott 22 19:27 2013-10-22-192721.jpg

-rwxr-xr-x 1 root root 58688 ott 22 19:29 2013-10-22-192919.jpg

#root@/mountpoint# rm *

Copia fisica del dispositivo

- Prima di operare, assicuriamoci di non danneggiare il dispositivo originale con le nostre operazioni. Facciamone una copia da usare per i test
- Usiamo ancora dd nella forma standard

```
#dd if=/dev/sdb of=scheda.dd
```

Abbiamo quindi un file raw (grezzo) “scheda.dd” contenente l'immagine speculare del nostro dispositivo in esame.

Possiamo mettere via la scheda MMC. Ed operare sulla immagine come se fosse il dispositivo originale, montandola come se fosse un disco

```
#mount -o ro,loop,offset=1048576 ./scheda.dd ./mountpoint/
```

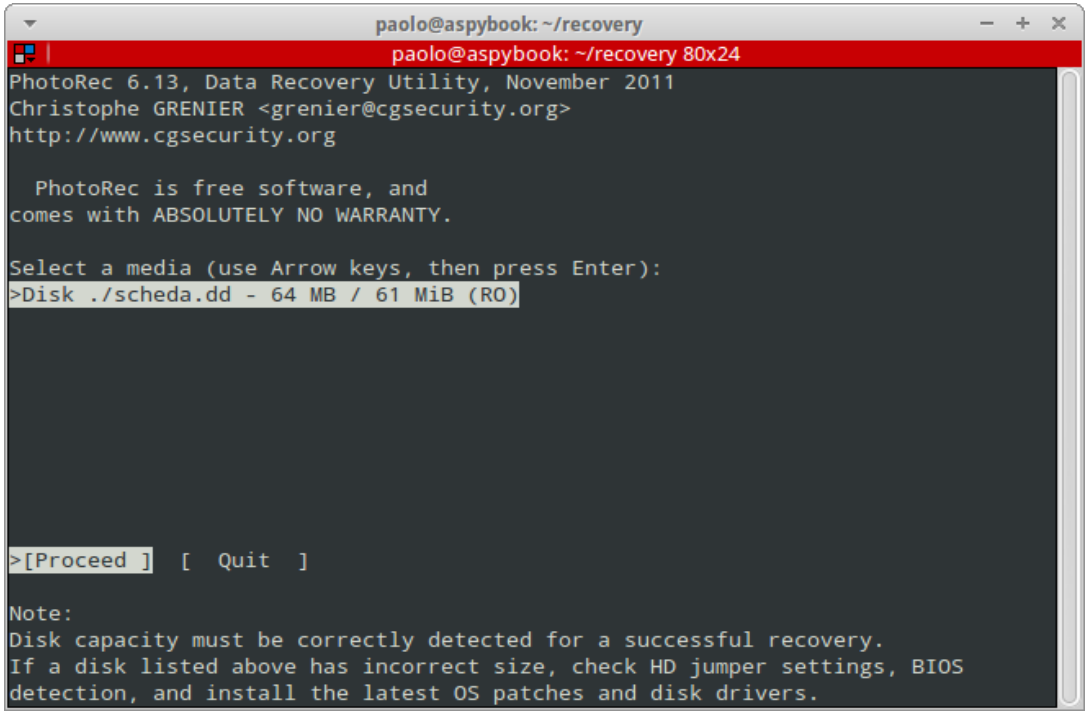
PS: l'offset si calcola moltiplicando il n. del settore di inizio della partizione per dimensione in byte del settore (info recuperate con fdisk o mmls)

Recupero con photorec

- Il comando da dare è:

```
#Photorec scheda.dd
```

Viene mostrato un menu dal quale effettuare le scelte del tipo di file system, ecc. I file recuperati vengono memorizzati in cartelle chiamate recup_dir.1, 2, 3...



Recupero con scalpel

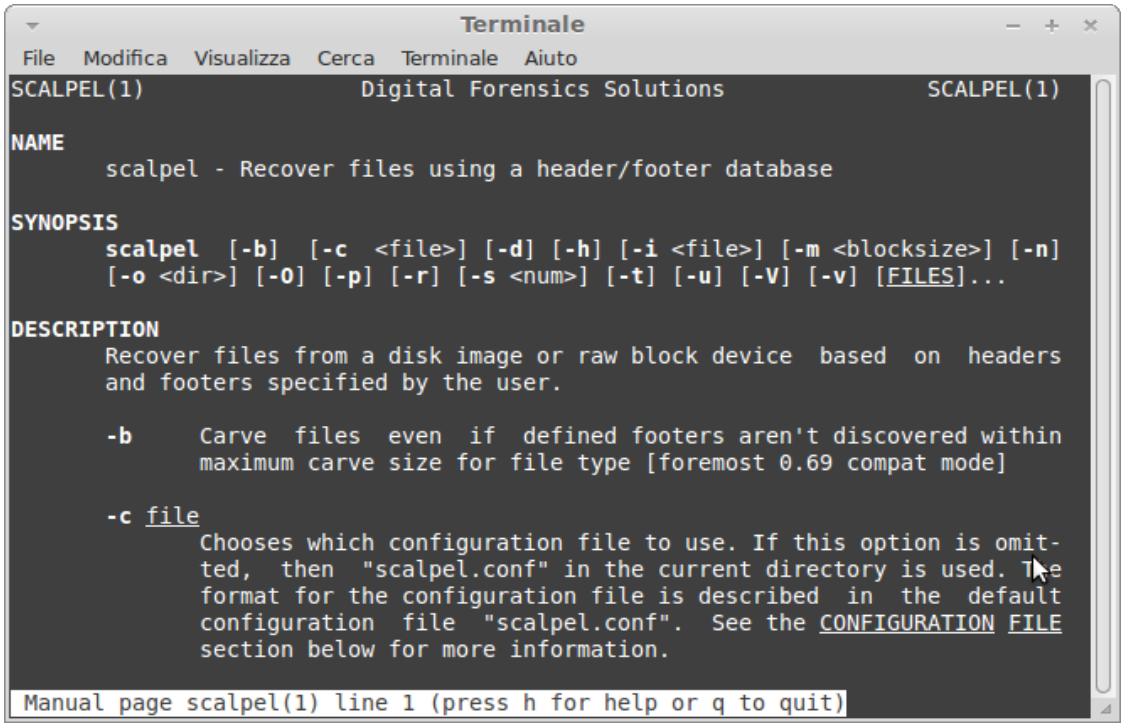
- Scalpel effettua la ricerca di file mediante il riconoscimento degli header e dei footer
- Si può usare scalpel direttamente sul device ma è bene non rischiare ed operare sulla copia
- Deve essere impostato il file di configurazione /etc/scalpel/scalpel.conf per indicare il tipo di file da recuperare decommentando le righe relative.

Recupero con scalpel

```
#Scalpel /dev/sdb

oppure

#Scalpel ./scheda.dd
```



I file recuperati sono salvati nella cartella specificata dal parametro “-o” oppure scalpel-output insieme ad un file di log

Attenzione agli header!

- **Ad esempio, i file JPG hanno vari header**
  - **JPEG EXIF: FF D8 FF E1**
  - **JPEG JFIF: FF D8 FF E0**

```
Esemnpio di Scalpel.conf
# GIF and JPG files (very common)
#  gif   y  5000000    \x47\x49\x46\x38\x37\x61 \x00\x3b
#  gif   y  5000000    \x47\x49\x46\x38\x39\x61 \x00\x3b
#  jpg   y  200000000  \xff\xd8\xff\xe0\x00\x10 \xff\xd9
   jpg   y  200000000  \xff\xd8\xff\xe1         \xff\xd9

http://filesignatures.net
```

Recupero con foremost

- Foremost si basa sulla ricerca di header e footer. Può lavorare sia sul device che sulla sua immagine ed è indipendente dal tipo di file system.
- Deve essere impostato il file di configurazione /etc/foremost.conf decommentando le righe contenenti la definizione relativa al tipo di file che desideriamo recuperare.
- I file recuperati vengono salvati in una cartella chiamata output ma è possibile indicare posizioni alternative
- Il comando da dare è:

```
#foremost ./scheda.dd
```

Caso di studio

- Cancelliamo la partizione con fdisk
- Ovviamente la nostra scheda MMC diventa inutilizzabile
- Tentiamo il recupero con testdisk, un programma in grado di analizzare il disco alla ricerca degli identificativi delle partizioni rimosse.

Caso di studio

- Formattiamo la MMC!
  - Cancelliamo la partizione
  - Ricreiamo la partizione FAT32 e formattiamo la scheda MMC
  - Ovviamente non troviamo nulla dentro la nostra schedina...
  - O no?
- Tentiamo il recupero delle nostre immagini con photorec

Caso di studio

- Si tratta di un hard disk esterno da 320 GB
- Durante l'aggiornamento del sistema operativo da WinXP a Win8 il disco è scomparso =:-|
- Per risolvere questo caso avremo bisogno di un po di teoria...

Analisi di un hdu danneggiato

- Colleghiamo il disco (la copia!) e vediamo cosa succede con dmesg
- Proviamo a vedere cosa ci dice fdisk
- Primo tentativo con photorec (sulla partizione)
- Secondo tentativo con photorec (sull'intero disco)
- Analisi del MBR
- Soluzione del caso

Seconda parte

La timeline

Per usare il linguaggio di Perry Mason, il computer forenser va alla ricerca di dati sul computer oggetto in modo da rispondera ad un quesito, esplicito od implicito, postogli da un soggetto.

Sia che il soggetto sia un giudice, un avvocato di parte od una parte in causa che vuole cepure cosa e' successo e/o recuperare dati e/o ripristinare un'operativita', il computer forenser va alla ricerca di fatti (dati, log, etc.) nel computer oggetto.

Se una ricostruzione dell'accaduto e' richiesta (caso tipico della CTU) la raccolta di evidenze (fatti=evidenze) e' il primo passo.

La timeline

Quasi sempre, talvolta in maniera semplice, talaltra in maniera complessa, esse devono essere confrontate con la dimensione “tempo”.

L’organizzazione delle evidenze, spesso di piu’ ripi diversi, lungo l’asse dei tempi e’ chiamata “Timeline”.

Non esistono programmi che costruiscono una timeline gia’ colorata e con una freccia rossa sui fatti salienti.

Esistono magari programmi assai costosi che dicono cose del genere nella pubblicita. E’, appunto, pubblicita’...

La timeline

Il nostro scopo e' di costruire una timeline utile (che non vuol dire necessariamente bella, completa o onnicomprensiva) con poche operazioni manuali ed utilizzando strumenti gratuiti ed open source.

Normalmente la costruzione di una timeline non triviale si svolge in due fasi.

Nella prima fase si estraggono una o piu' serie di eventi, spesso fa fonti diverse (ad esempio date dei file di un disco, date di messaggi di posta, date da un file di log.

In una seconda fase si importano in uno strumento adatto (Excel nell'80% dei casi) uniformandone i formati.

La timeline

Nella fase finale si elaborano i dati (senza cancellarne nessuno, mettendo in evidenza quelli che costituiscono fatti salienti.

Si costruisce poi in maniera discorsiva una timeline sintetica che interpreta le evidenze salienti e le organizza in una ricostruzione dei fatti.

E' molto importante documentare e giustificare nella relazione finale sia gli strumenti utilizzati che il metodo usato per costruire la timeline.

Link: strumenti ed approfondimenti

- http://www.cgsecurity.org/wiki/TestDisk
- http://www.cgsecurity.org/wiki/PhotoRec_Step_By_Step
- http://www.ubuntugeek.com/recover-deleted-files-with-foremostscalpel-in-ubuntu.html
- http://www.deftlinux.org/
- http://www.forensicswiki.org/wiki/File_Carving
- http://www.caine-live.net/
- http://computer-forensics.sans.org/community/downloads
- http://www.forensicswiki.org/wiki/Main_Page
- http://thestarman.pcministry.com/asm/mbr/PartTables.htm
- http://www.dban.org/

IISFA European Chapter

Grazie per l'attenzione

Q&A time

+ Marco A. Calamari marco.calamari@ordineingegneripisa.it --+
| |
| PGP RSA: ED84 3839 6C4D 3FFE 389F 209E 3128 5698 |
| DSS/DH: 8F3E 5BAE 906F B416 9242 1C10 8661 24A9 BFCE 822B |
| Tel: (+39) 050 576031 Cell: (+39) 347 8530279 |
| Fax: (+39) 050 7849817 Skype-Twitter: calamarim |
| |
+ P.E.C.: marcoanselmoluca.calamari@ingpec.eu -------------+