DIGITAL FORENSICS

Corso di Sicurezza II

Dipartimento dI Informatica

Paolo Dal Checco

CHI SONO

- **Dottorato in Informatica**, gruppo di Sicurezza, @unito
- Per alcuni anni ricerca, poi **CTO** in ambito **crittografia**
- Ora **consulente Informatico Forense** per Procure, Tribunali, Aziende e Privati in ambito penale e civile
- Esperto di aspetti investigativi delle criptomonete, ransomware, computer/mobile/web/network forensics, perizie audio e video
- Tra i fondatori dell'Osservatorio Nazionale di Informatica Forense (**ONIF**), sviluppatore DEFT Linux fino al 2018
- Socio Tech & Law, Clusit, AIP, AssobIT
- paolo@dalchecco.it - @forensico
- dalchecco.it, bitcoinforensics.it, ransomware.it

PROGRAMMA 3 GIORNATA

- Verifica e apertura delle immagini forensi
- Virtualizzazione delle immagini forensi
- Recupero dei dati cancellati
- Analisi dei metadati

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

VERIFICA IMMAGINE FORENSE

- Garantisce che la copia del device sia inalterata ed identica all'originale
- Si utilizzano funzioni hash
- Gli algoritmi più utilizzati sono MD5 e SHA-1, ma ne esistono altri
- E' possibile ripetere la verifica sulle copie forensi o sui supporti originali in qualsiasi momento per dimostrare che i dati non sono stati alterati

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

ALGORITMI DI HASHING: COSA SONO?

- L'algoritmo restituisce una stringa di numeri e lettere (detto digest) a partire da un qualsiasi flusso di bit di qualsiasi dimensione finita
- La stringa di output è univoca per ogni documento identificandolo. Perciò, l'algoritmo è utilizzabile per la firma digitale
- La lunghezza del digest varia a seconda degli algoritmi utilizzati
- L'algoritmo non è invertibile, cioè non si può ricavare la sequenza di bit in ingresso a partire dal digest

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

ALGORITMI DI HASHING: I PIÙ UTILIZZATI

- **MD5** (RFC 1321)
  Prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 128 bit (con lunghezza fissa di 32 valori esadecimali, indipendentemente dalla stringa di input)

- **SHA-1** (RFC 3174)
  Prende in input una stringa di lunghezza arbitraria e ne produce in output un'altra a 160 bit (con lunghezza fissa di 40 valori esadecimali, indipendentemente dalla stringa di input)

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

ALGORITMI DI HASHING: PROBLEMI DI COLLISIONE

- Quando due sequenze di bit differenti generano lo stesso hash si parla di collisione
- La qualità di una funzione di hash è misurata direttamente in base alla difficoltà nell'individuare due testi che generino una collisione
- Si è riusciti a generare una collisione negli algoritmi HAVAL, RIPEMD, MD2, MD4, MD5 e SHA-1 dimostrando che non sono sicuri

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

ALGORITMI DI HASHING: PROBLEMI DI COLLISIONE

Per ovviare a problemi di collisione si devono:

- Usare algoritmi più sofisticati
- Validare i risultati con due algoritmi diversi Impossibile generare una collisione per entrambi gli hash contemporaneamente

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

VERIFICA IMMAGINI FORENSI

- Nel caso in cui si sia salvato in formato raw, con conseguente creazione del checksum, utilizziamo **md5sum** o **sha1sum**:

```
# md5sum -c image.dd.md5
# sha1sum -c image.dd.sha1
```

- **EWF:** # ewfverify image.E01

- **AFF:** # afinfo -v image.aff

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

VERIFICA IMMAGINE FORENSE

E’ possibile verificare l’hash delle immagini anche con Dhash importando il file contenente l’hash da verificare e indicando il file immagine o il device.

In alternativa per il controllo dell’hash posso usare anche FTK Imager sia in ambiente Windows, ma anche direttamente in DEFT tramite wine.

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

APERTURA DI UN'IMMAGINE FORENSE

- In base alla modalità con cui sono state eseguite le copie forensi (raw, split raw, ewf, aff, clone) vi sono diverse alternative per l'accesso in fase di analisi

- Il fine è quello di poter accedere al contenuto (filesystem, aree allocate e non) dell'immagine acquisita per poter eseguire le analisi del caso

- Alcuni formati lo prevedono come default, l'accesso va eseguito in sola lettura (read only) per ovvi motivi…

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

ACCESSO A IMMAGINI EWF/AFF

```
xmount --in ewf --out dd image.E?? /mnt/raw
xmount --in aff --out dd image.aff /mnt/raw
```

(per smontare il volume **`umount /mnt/raw`**)

- In /mnt/raw si vedranno due file “virtuali”, uno contenente l’intera immagine in formato raw, l’altro contenente le informazioni relative all’immagine stessa (ad es. nel caso di ewf le info memorizzate in fase di acquisizione)
- Il passo successivo è analizzare il partizionamento del file raw e montarne eventuali partizioni o accedere al raw content per avviare strumenti di analisi e ricupero dati (photorec, autopsy, scalpel, foremost, ecc.)

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

ACCESSO A IMMAGINI EWF

`ewfmount image.E01 /mnt/raw`

(per smontare il volume **`umount /mnt/raw`**)

- In /mnt/raw si vedranno due file “virtuali”, uno contenente l’intera immagine in formato raw, l’altro contenente le informazioni relative all’immagine stessa (ad es. nel caso di ewf le info memorizzate in fase di acquisizione)
- Il passo successivo è analizzare il partizionamento del file raw e montarne eventuali partizioni o accedere al raw content per avviare strumenti di analisi e ricupero dati (photorec, autopsy, scalpel, foremost, ecc.)

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

ACCESSO A IMMAGINI AFF/SPLIT RAW

```
affuse image.aff /mnt/raw
affuse image.001 /mnt/raw
```

(per smontare il volume "**fusermount -u /mnt/raw**")

- In /mnt/raw si vedranno due file "virtuali", uno contenente l'intera immagine in formato raw, l'altro contenente le informazioni relative all'immagine stessa (ad es. nel caso di ewf le info memorizzate in fase di acquisizione)
- Il passo successivo è analizzare il partizionamento del file raw e montarne eventuali partizioni o accedere al raw content per avviare strumenti di analisi e ricupero dati (photorec, autopsy, scalpel, foremost, ecc.)

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

ANALISI DELLE PARTIZIONI

mmls /mnt/raw/image.dd

```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

Slot Start End Length Description
00: Meta 0000000000 0000000000 0000000001 Primary Table
(#0) 01: -- 0000000000 0000000062 0000000063 Unallocated
02: 00:00 0000000063 0083859299 0083859237 NTFS (0×07)
03: -- 0083859300 0083886079 0000026780 Unallocated
```

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

ANALISI DELLE PARTIZIONI

mmls /mnt/raw/image.dd

```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

Slot Start End Length Description
00: Meta 0000000000 0000000000 0000000001 Primary Table
(#0) 01: -- 0000000000 0000000062 0000000063 Unallocated
02: 00:00 0000000063 0083859299 0083859237 NTFS (0×07)
03: -- 0083859300 0083886079 0000026780 Unallocated
```

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

MOUNT DELLE PARTIZIONI

```
deft ~ % mount -o ro,show_sys_files,streams_interface=windows /dev/sda1 /mnt/c
deft ~ % ls -al /mnt/c
totale 853110
drwxrwxrwx 1 root root      8192 2010-03-18 17:45 .
drwxr-xr-x 3 root root        60 2012-03-20 23:11 ..
drwxrwxrwx 1 root root     16384 2009-08-08 01:12 4928cbe0584148074357
-rwxrwxrwx 1 root root      2560 2005-06-11 18:23 $AttrDef
-rwxrwxrwx 1 root root         0 2005-06-11 16:46 AUTOEXEC.BAT
-rwxrwxrwx 1 root root         0 2005-06-11 18:23 $BadClus
-rwxrwxrwx 1 root root    435512 2005-06-11 18:23 $Bitmap
-rwxrwxrwx 1 root root      8192 2005-06-11 18:23 $Boot
-rwxrwxrwx 1 root root      4952 2001-08-31 11:00 Bootfont.bin
-rwxrwxrwx 1 root root       211 2005-06-11 17:28 boot.ini
```

- Si notano alcuni file di metadati NTFS ($Boot, $MFTMirr, ecc.)
- Alcuni metafile non si vedono ma si possono accedere direttamente ($MFT, $UsnJrnl:$J)

VERIFICA E APERTURA DELLE IMMAGINI FORENSI

MOUNT DELLE PARTIZIONI

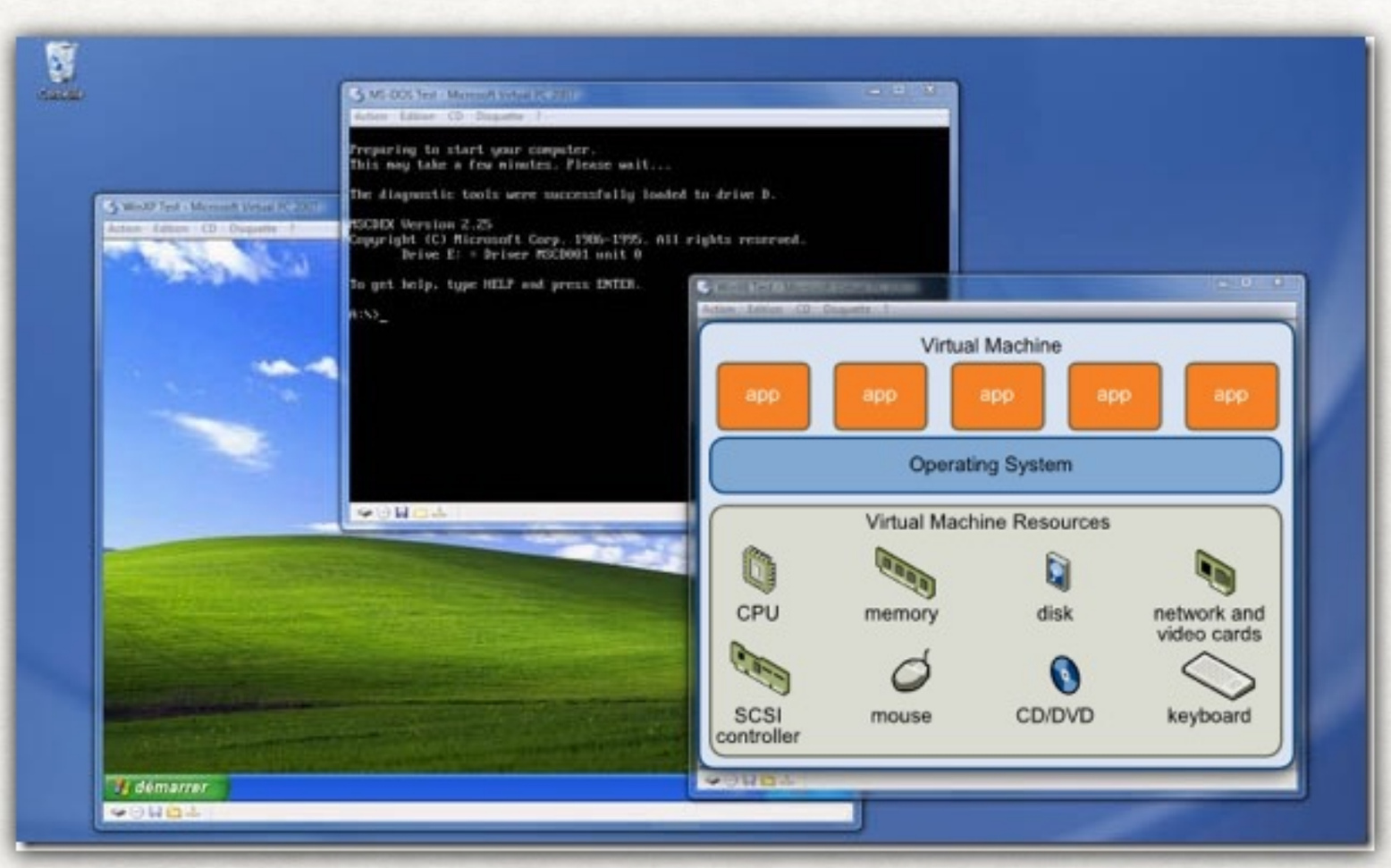
```
# mount -o ro,loop,show_sys_files,streams_interface=windows,
        offset=$((512*63)) /mnt/raw/image.dd /mnt/c
```

- Ulteriore forzatura read-only, in realtà superflua
- Importanti i parametri **show_sys_files** e **streams_interface=windows**
- Questi parametri permettono di accedere direttamente anche ai file di sistema come $MFT, $Boot, ecc… (seppur alcuni non visualizzabili da un ‘ls’) e agli Alternate Data Streams (ad es. il poco famoso $UsnJrnl:$J il Journaling definito “Update Sequence Number” che permette di rilevare attività sui file, compresa la cancellazione)

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

DEFINIZIONE DI VIRTUALIZZAZIONE

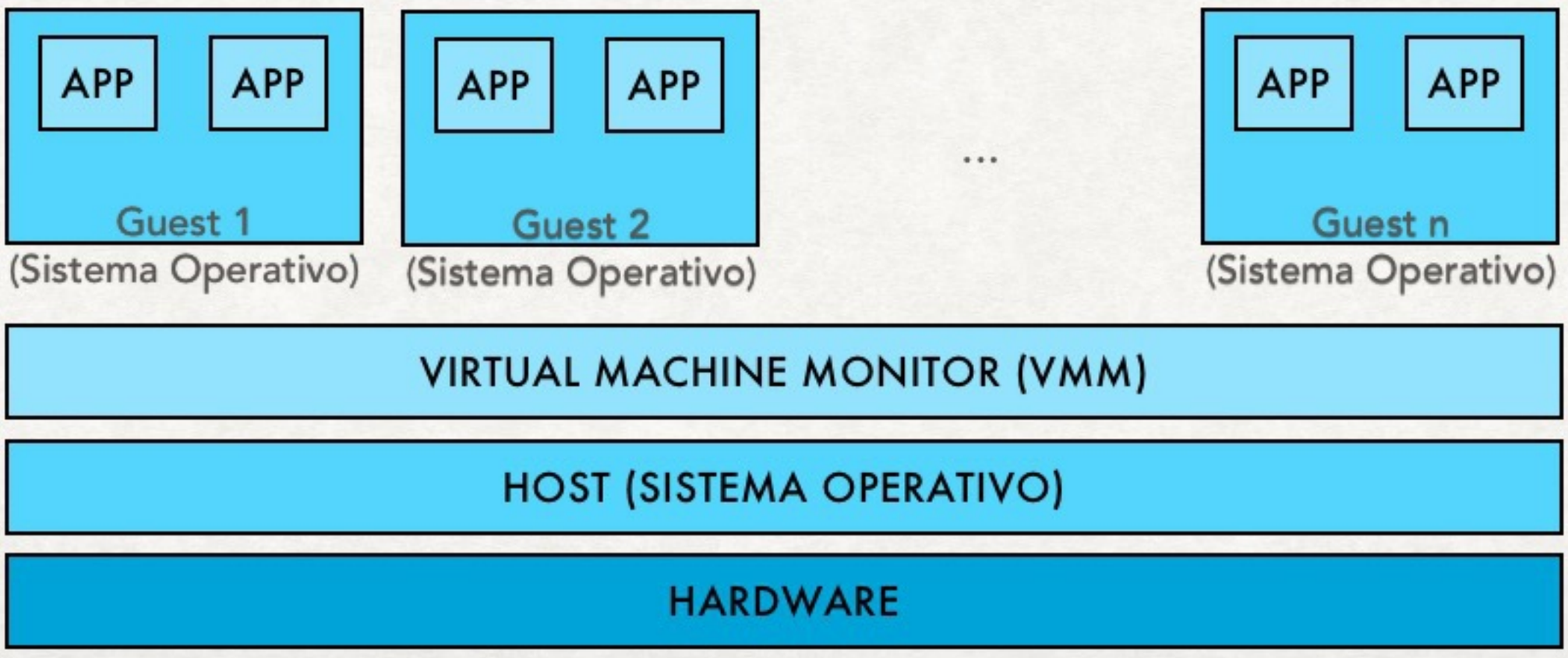
- Implementazione software di un computer che “esegue” come se fosse una macchina fisica
- "Duplicato efficiente e isolato di una macchina reale" (Popek e Goldberg, 1974)



VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

HOST E GUEST

- Host: macchina fisica (esterna)
- Guest: macchina virtuale (interna)
- VMM: Virtual Machine Monitor (hypervisor)
- Collegamenti di rete: bridge, NAT, host o custom)



VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

MACCHINE VIRTUALI E COMPUTER FORENSICS

Diversi punti di vista e di contatto:

- Test software in ambiente isolato
- virtualizzazione di immagini forensi
- acquisizione di macchine virtuali

- acquisizione di macchine fisiche
- formati proprietari, software proprietario gestionali, database, script, macro
- utilizzo di live distro su workstation Win (DEFT viene fornito anche come macchina virtuale)
- questioni legate sicurezza o crittografia

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ESEGUIRE IN VM UN'IMMAGINE FORENSE

Tre alternative:

1. Conversione del disco da immagine forense a disco virtuale
    - Richiede tempo e spazio, è necessario partire da DD/RAW
    - Portabile al 100%
2. Creazione di un disco virtuale che referenzia l'immagine forense
    - Non occupa spazio aggiuntivo, pochi file
    - E' portabile se si parte da un DD/RAW
3. Mount dell'IMG come disco virtuale
    - Immediato e non occupa spazio
    - Non è portabile

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

- disabilitare scheda di rete
- disabilitare scheda di rete
- disabilitare scheda di rete
- disabilitare scheda di rete
- disabilitare scheda di rete
- disabilitare scheda di rete

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

1: CONVERSIONE DEL DISCO DA RAW IMG A DISCO VIRTUALE

- La conversione produce un file non che non è necessariamente grande quanto l'immagine RAW
- Ok se l'immagine forense è in DD, altrimenti si converte in DD richiedendo quindi un passaggio ulteriore. Tool più usati:
  - **Virtual Box** (Windows, Linux, Mac OS)
    - "VBoxManage convertfromraw imagefile.dd vmdkname.vmdk --format VMDK"
  - **qemu** (Linux)
    - "qemu-img convert imagefile.dd -O vmdk vmdkname.vmdk"
- Una volta creato il disco, si crea una nuova macchina virtuale che utilizza il disco appena creato

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

2: CREAZIONE DISCO VIRTUALE CHE REFERENZIA IMG

- Si crea un disco virtuale (VMDK, etc...) che referenzia, al suo interno, l'immagine forense
- Si può fare a mano [dd2vm] impostando nel file di configurazione del disco virtuale la geometria del disco contenuto nell'immagine forense
- Se non si dispone di un'immagine RAW, usare FTK Imager per montare una raw device (per Live View) o eventualmente xmount per emulare un RAW
- Esistono tool gratuiti e a pagamento per creare il disco virtuale:
  - **Live View** (per Win) [livevw]
  - **dd2vmdk** (in C per Win, Linux, Mac) [dd2vmdk]
  - **raw2vmdk** (in Java per Win, Linux, Mac) [raw2vmdk]
  - **ProDiscover** Basic Edition [pdisc]
  - **EnCase** Physical Disk Emulator (PDE) [ecpdm]
  - **Virtual Forensic Computing** (VFC) [gdvfc]

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

LIVE VIEW

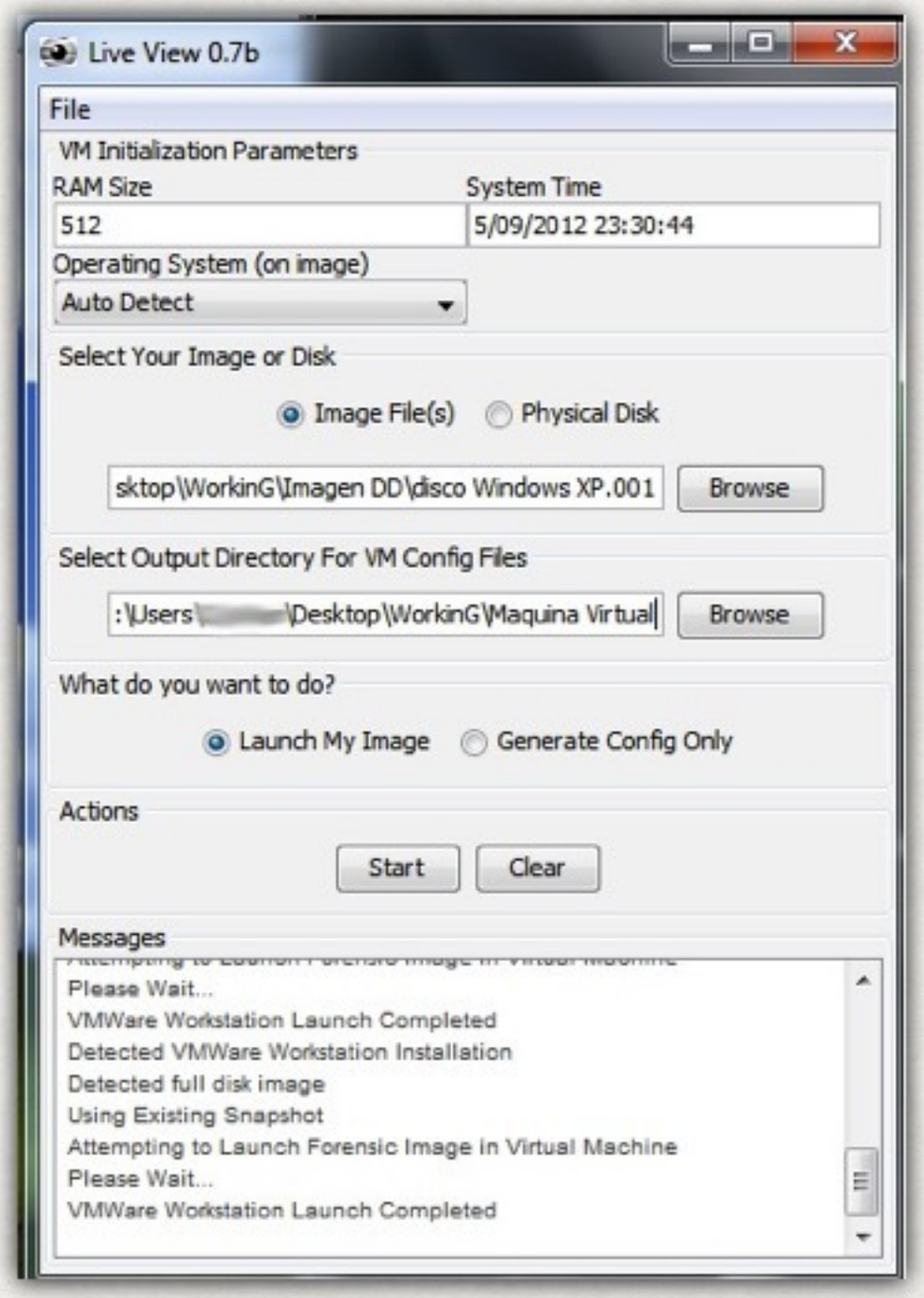
- Sviluppato da Carnegie Mellon University
- Basato su Java, non più aggiornato
- Può virtualizzare:
  - immagini raw di dischi
  - immagini raw di partizioni
  - dischi fisici (connessi via USB o firewire)
  - immagini in formati proprietari (tramite software di terze parti come FTK Imager)
- Ottimo per Windows, in parte anche Linux, tool molto usato
- In parte risolve anche i conflitti hardware legati alla virtualizzazione

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

LIVE VIEW

Necessita di:

- VMware Server 1.x Full Install
  - o VMware Workstation 5.5+
- Java Runtime Environment
- VMware Disk Mount Utility



VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

3: MOUNT DI IMMAGINE FORENSE COME VIRTUAL DISK

- In tempo reale, tramite FUSE, l'immagine forense viene vista dal sistema operativo come un file di un filesystem virtuale (VMDK, VHD o VDI) permettendo anche la scrittura su un file di cache

- Si può utilizzare **xmount** (Linux/Mac), gratuito e Open Source

xmount --in ewf --out vmdk --cache mycache.bin img.e?? /mnt/vmdk

fusermount -u /mnt/vmdk

- Una volta che abbiamo il disco virtuale, possiamo creare e lanciare la macchina virtuale che lo utilizza. Cosa otteniamo?

A problem has been detected and windows has been shut down to prevent damage
to your computer.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to be sure you have adequate disk space. If a driver is
identified in the Stop message, disable the driver or check
with the manufacturer for driver updates. Try changing video
adapters.

Check with your hardware vendor for any BIOS updates. Disable
BIOS memory options such as caching or shadowing. If you need
to use Safe Mode to remove or disable components, restart your
computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x0000007E (0xC0000005,0xF88FF190,0x0xF8975BA0,0xF89758A0)

*** EPUSBDSK.sys - Address F88FF190 base at FF88FE000, datestamp 3b9f3248

Beginning dump of physical memory

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

BSOD

- Con Windows, ma anche con Mac OS, l'avvio di una VM nata da una macchina fisica non va sempre liscio, così come quando si cambia l'hardware di una macchina lasciando il disco
- Sia su VMware sia su VirtualBox possono verificarsi problemi con i driver IDE, HAL, estensioni kernel, etc... che impediscono il boot.
- Si possono risolvere a mano [vbxwin] o utilizzare gli script OpenGates e OpenJobs [pinguinhq] di Gillen Dan
- Sono ISO che vanno avviate (OpenGates va prima creata) come LiveCD all'interno della virtual machine (guest) in modo che possano patchare il disco virtuale VMDK/VHD

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

OPENGATES

- Patch del registro per abilitare i legacy IDE drivers
- Azzera le password degli utenti (chntpw)
- Rimuove i driver che possono andare in conflitto con l'hw

- Determina gli HAL utilizzati (importante quando si migra su VirtualBox)
- "Risolve" i problemi di licenza/convalida che emergono quando Windows si "sveglia" su un altro hardware
- Stampa informazioni utili per configurare la VM

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

OPENJOBS

- Installa un bootloader per rendere il disco avviabile (v10.5 e v10.6).

- Installa le estensioni per il kernel Hackintosh

- Rimuove estensioni del kernel che possono andare in conflitto con il nuovo hardware (v10.7 e 10.8).

- Azzera le password degli utenti

- Stampa informazioni utili per configurare la VM

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

LO SAPEVATE?

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

LO SAPEVATE?

- Sembrerà ovvio, ma un guest a 64 bit non gira su hardware a 32bit...
- Un software è in grado di capire se è dentro una VM o fuori (ScoopyNG [scoopyng], VMDetect [vmdetect], Red Pill [rdpill])
- Per forzare un delay sul BIOS e avere tempo di lanciare OpenGates, aggiungere nel file di configurazione .vmx la riga **bios.bootDelay = "xxxx"** (xxxx in milli secondi)
- Per forzare l'entrata nel BIOS al boot aggiungere **bios.forceSetupOnce = "TRUE"** oppure utilizzare l'apposita voce nel menu
- Se Windows richiede l'attivazione:
  - La modalità provvisoria funziona sempre
  - (XP) tool di dubbia provenienza o legalità...
  - (XP) rundll32.exe syssetup | SetupOobeBnk
  - (7) sysprep /generalize | slmgr.vbs rearm | rundll32 slc.dll,SLReArmWindows | slmgr /rearm

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

- Le scatole nere spesso non sono che dei computer con Sistema Operativo proprietario o anche standard, hard disk tradizionali ide/sata (magari protetti e isolati per salvaguardarne l'integrità) con filesystem proprietari/standard
- Caso reale nel quale la virtualizzazione è stata di capitale importanza: scatola nera con hardware molto vecchio, software e formato proprietario
- Si è proceduto con i seguenti passi:
  - Copia forense del disco
  - Verifiche integrità e coerenza dati con ausilio di (super)timeline
  - Virtualizzazione tramite Live View
  - Avvio in ambiente virtuale
  - Elaborazione dei tracciati storici precedenti l'incidente
  - Esportazione delle informazioni rilevanti (se non è disponibile funzione di esportazione, si può operare con screenshot)

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

- Le scatole nere spesso non sono che dei computer con Sistema Operativo proprietario o anche standard
- I dati sono memorizzati su supporti di archiviazione, se possibile SSD (protetti e isolati) e con filesystem proprietari
- Es. QNX, OS/FS application critical e real time utilizzato in centrali nucleari, auto, navi, etc.. [osqnx]) o anche semplicemente FAT 16/32...

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

ARTICOLI

QNX, quando un crash sarebbe mortale

DI PAOLO ATTIVISSIMO

25 GIU 2003

A quale sistema operativo si affidano reattori nucleari, il controllo del traffico aereo, e altre situazioni in cui un crash semplicemente non è tollerabile?

Siete sul tavolo operatorio, decisi a farvi sistemare la vista con uno di quei fantastici interventi al laser. La macchina che incombe sui vostri occhi spalancati in stile *Arancia meccanica* è completamente robotizzata: la mano del chirurgo, per queste cose, è troppo imprecisa. Quel laser che può rendervi ciechi o ridarvi dieci decimi è gestito da un sistema operativo che comanda impulsi la cui durata si misura in millisecondi. Che cosa succede se gli capita un *crash*, o semplicemente un momento di esitazione?

Benvenuti nel mondo dei *sistemi operativi estremi*, quelli ai quali il *crash* non è concesso. Abituati come siamo ai frequenti collassi dei computer che usiamo quotidianamente, viene spontaneo pensare che sia nel naturale ordine delle cose che i sistemi operativi vadano in tilt, e che quando non si impallano ogni tanto si fermino a rimuginare prima di rispondere ai comandi. Non è così, e lo potete provare di persona.

- Sistema Operativo real-time Unix-like POSIX-compliant commerciale
- Esistono driver per Linux

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

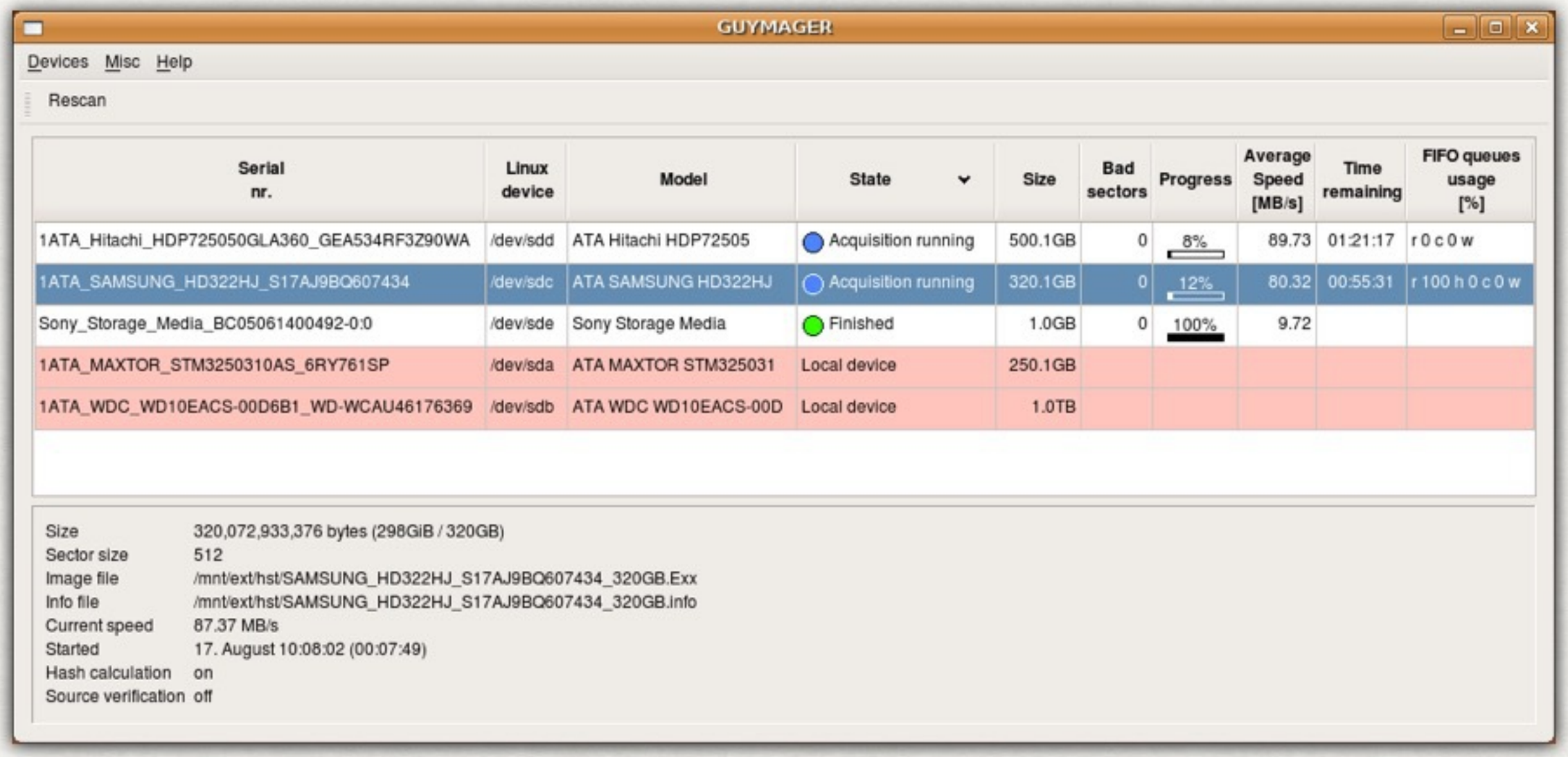
ANALISI DI UNA "SCATOLA NERA"

- Caso reale nel quale ci si può imbattere è quello di una scatola nera con hardware obsoleto, software e formato proprietari
- Cosa fare se non si hanno alternative? Virtualizzare...

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

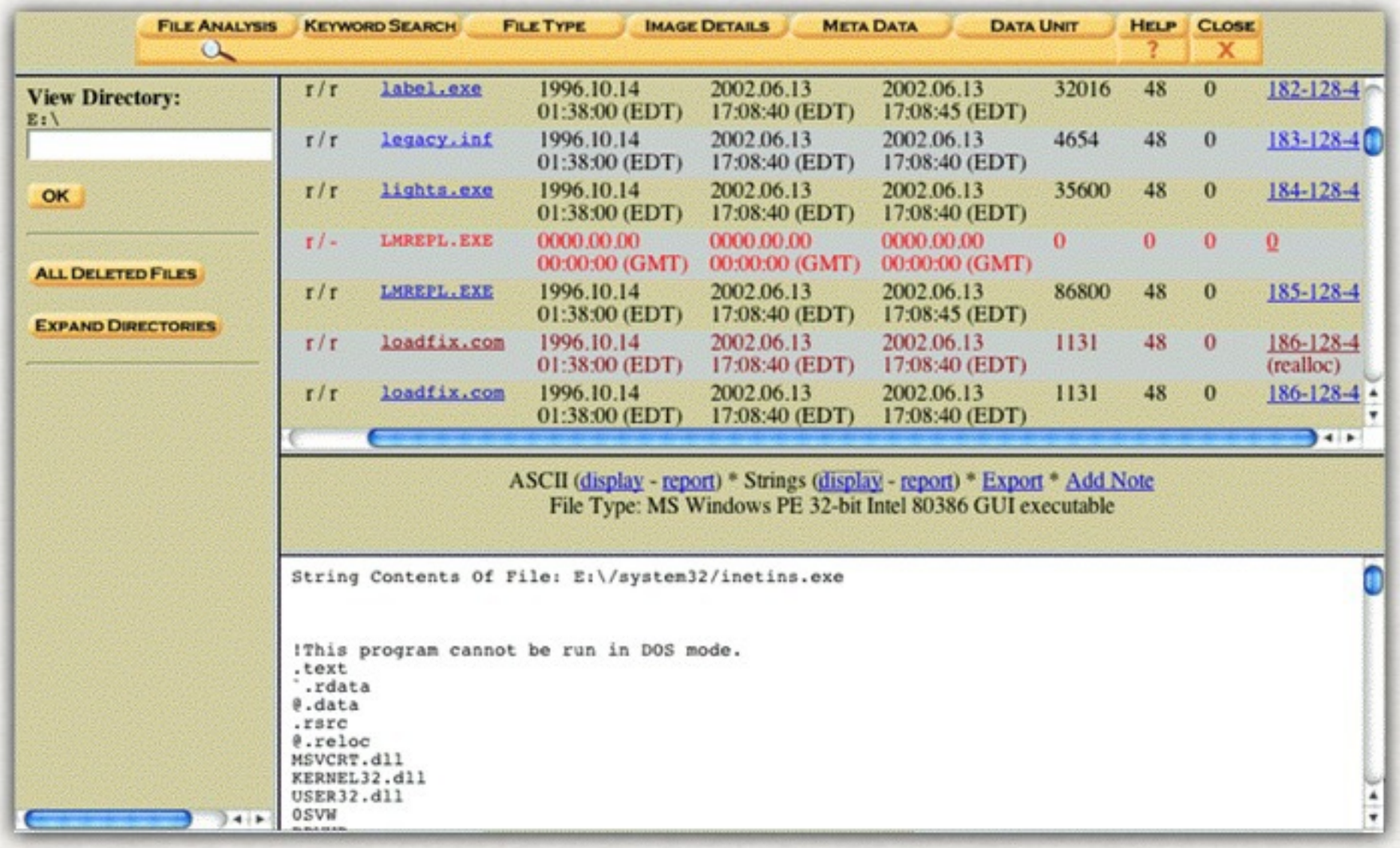
- Copia forense del disco con Guymager (DEFT)



VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

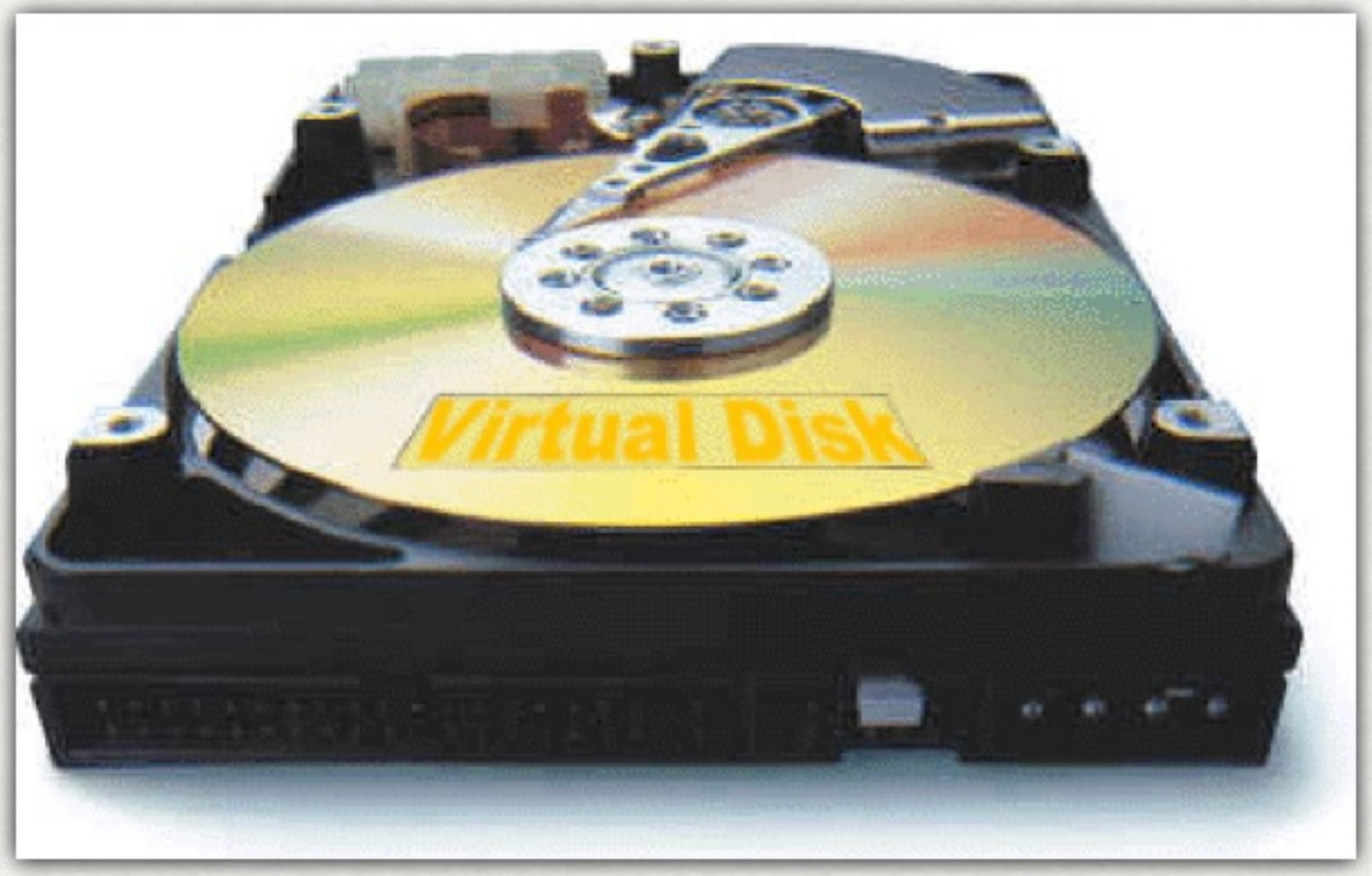
- Verifiche integrità e coerenza dati con ausilio di (super)timeline e log2timeline, TSK o Autopsy (DEFT)



VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

- Virtualizzazione disco tramite Live View oppure dd2vmdk o raw2vmdk (DEFT8) o con gli altri metodi descritti



VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

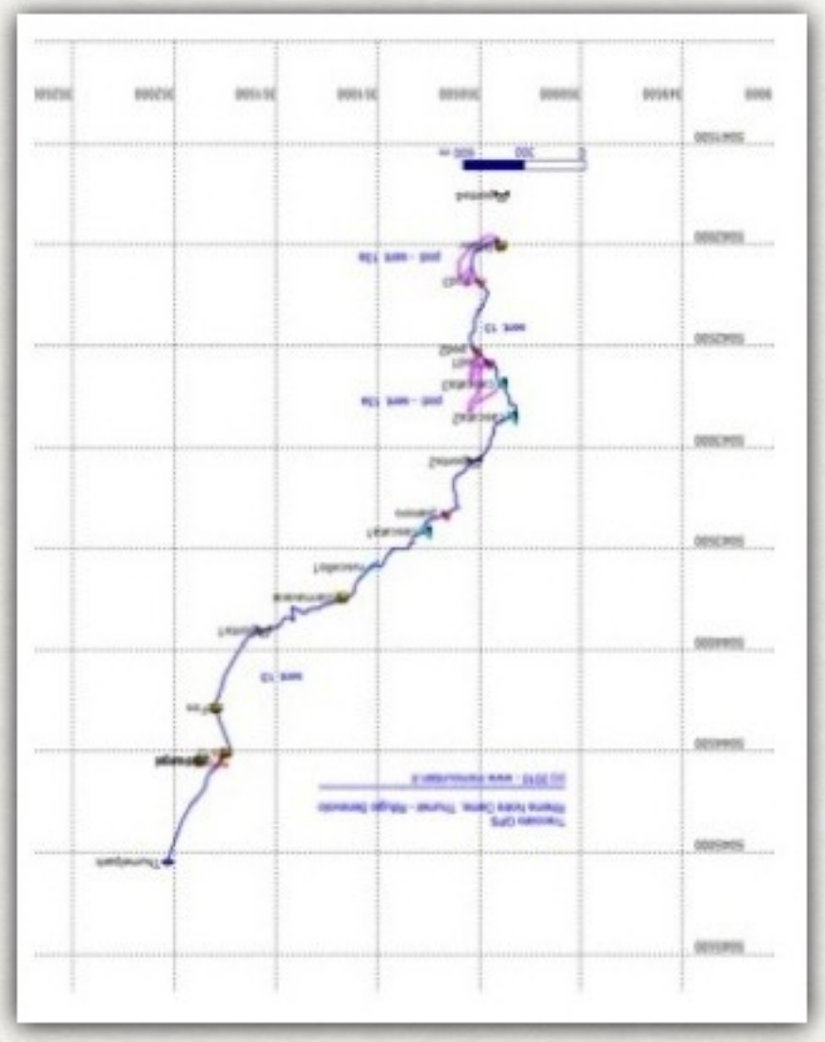
ANALISI DI UNA "SCATOLA NERA"

- Avvio in ambiente virtuale tramite VMware o Virtualbox (installabile in DEFT)

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

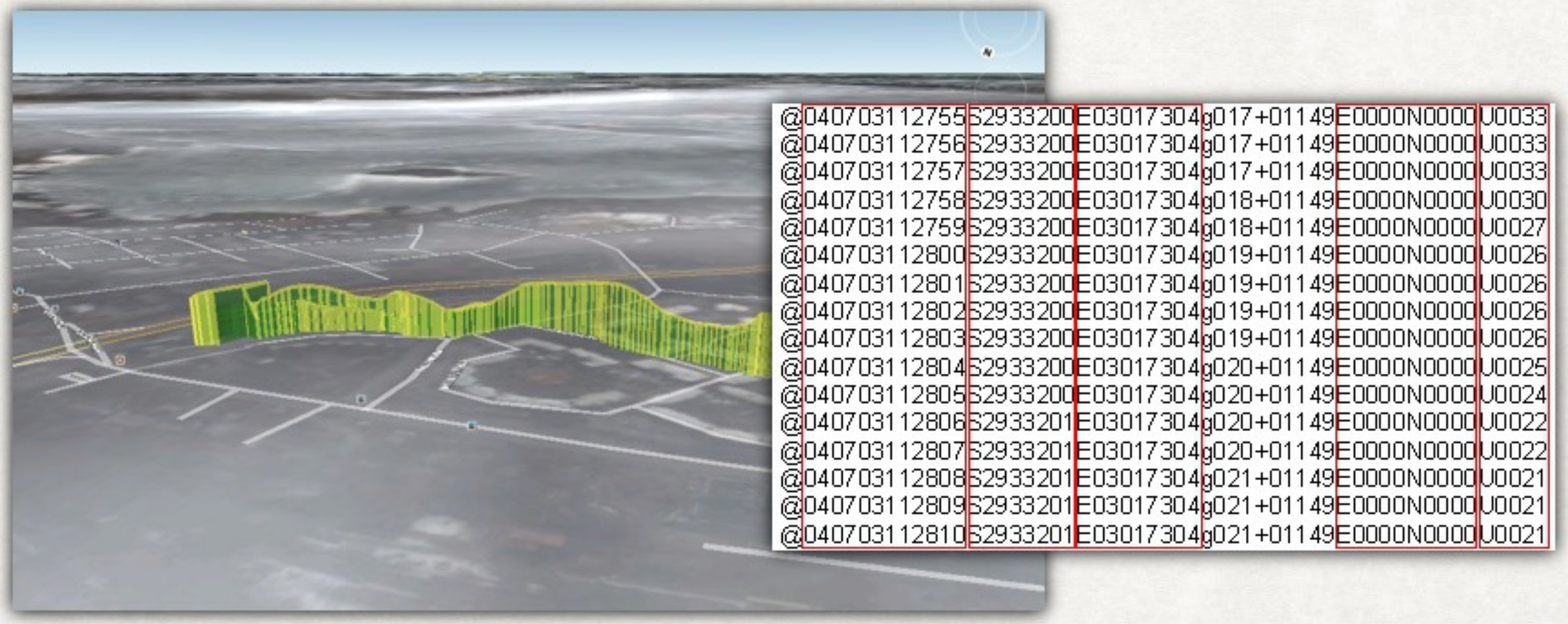
- Elaborazione dei tracciati storici precedenti l'incidente



VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

- Esportazione delle informazioni rilevanti (se non è disponibile funzione di esportazione, si può operare con screenshot)



```
@040703112755S2933200E03017304g017+01149E0000N0000U0033
@040703112756S2933200E03017304g017+01149E0000N0000U0033
@040703112757S2933200E03017304g017+01149E0000N0000U0033
@040703112758S2933200E03017304g018+01149E0000N0000U0030
@040703112759S2933200E03017304g018+01149E0000N0000U0027
@040703112800S2933200E03017304g019+01149E0000N0000U0026
@040703112801S2933200E03017304g019+01149E0000N0000U0026
@040703112802S2933200E03017304g019+01149E0000N0000U0026
@040703112803S2933200E03017304g019+01149E0000N0000U0026
@040703112804S2933200E03017304g020+01149E0000N0000U0025
@040703112805S2933200E03017304g020+01149E0000N0000U0024
@040703112806S2933201E03017304g020+01149E0000N0000U0022
@040703112807S2933201E03017304g020+01149E0000N0000U0022
@040703112808S2933201E03017304g021+01149E0000N0000U0021
@040703112809S2933201E03017304g021+01149E0000N0000U0021
@040703112810S2933201E03017304g021+01149E0000N0000U0021
```

RECUPERO DEI DATI CANCELLATI

- Quando viene cancellato un file, i dati non sono azzerati, ma soltanto **dereferenziati**
- I dati, di conseguenza, sono ancora sul disco ma lo spazio precedentemente occupato risulta ora **deallocato**
- Anche i metadati potrebbero essere ancora presenti in maniera analoga
- Per il recupero sono possibili due modalità:
    - Analisi dei metadati
    - File carving

RECUPERO DEI DATI CANCELLATI

RECUPERO TRAMITE ANALISI DEI METADATI

- Strettamente dipendente dal file system
- Consentono di ricostruire anche i file frammentati
- E' possibile recuperare altre informazioni tra cui il nome del file, data di creazione, data di modifica, ecc.

RECUPERO DEI DATI CANCELLATI

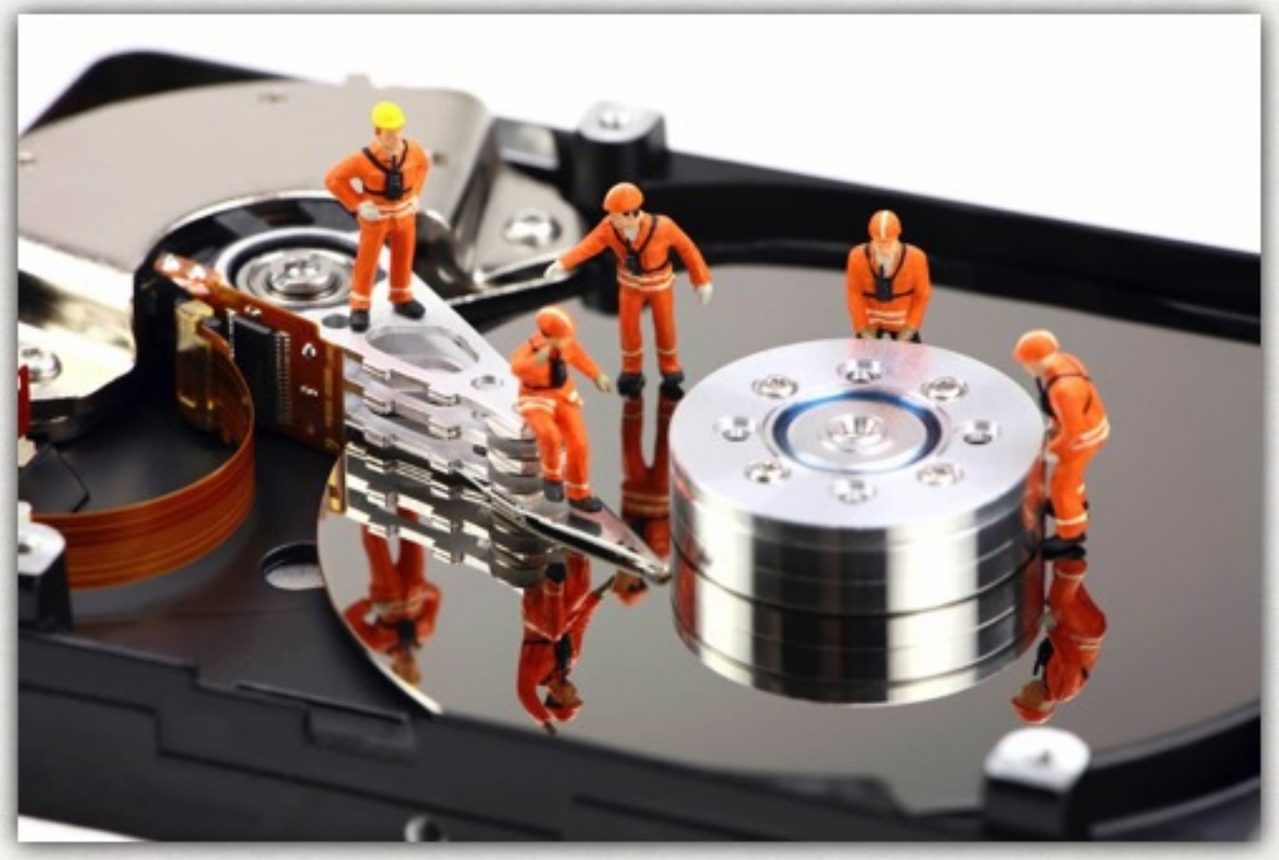
RECUPERO TRAMITE FILE CARVING

- Se il dato è completamente dereferenziato, l'unico recupero possibile è tramite la scansione del Binary Large Object
- Vengono ricercate le intestazioni (header o magic number) identificative di specifici formati di file
- Si cerca di interpretare quello che segue come parte integrante del file (se esiste viene cercato anche un footer)
- Funziona bene nel caso in cui i file siano allocati su cluster contigui ma non in caso di frammentazione
- Non recupera informazioni come nome e posizione originaria del file

RECUPERO DEI DATI CANCELLATI

SOFTWARE RECUPERO DATI

- Photorec
- Foremost
- Bulk Extractor
- Undelete360
- Recuva
- Ontrack Easy Recovery
- R-Studio
- ma ce ne sono altri ancora…



ANALISI DEI METADATI

- I metadati sono dati riguardanti altri dati. Spesso i metadati hanno un ruolo fondamentale nelle indagini digitali
- Possono fornire informazioni fondamentali riguardanti il documento stesso
- Possono rivelare informazioni che si è tentato di oscurare, nascondere o cancellare
- Possono utilizzati per correlare documenti alla loro fonte

ANALISI DEI METADATI

I più comuni tipi di metadati sono:

- Metadati del file system
- Metadati nei documenti (office, PDF, ecc.)
- Metadati nelle immagini
- Metadati nei file audio/video
- Metadati nelle email
- Metadati applicazioni
- …

ANALISI DEI METADATI

ALCUNI TIPI DI METADATI

- Nome del file
- Estensione del file
- Dimensione del file
- Data di creazione del file
- Data di ultimo accesso
- Data di ultima modifica
- Dati EXIF
- Ed altri dati…

ANALISI DEI METADATI

ALCUNI ESEMPI

Vediamo qualche esempio di metadati:

- Metadati nei documenti
- Metadati nelle immagini

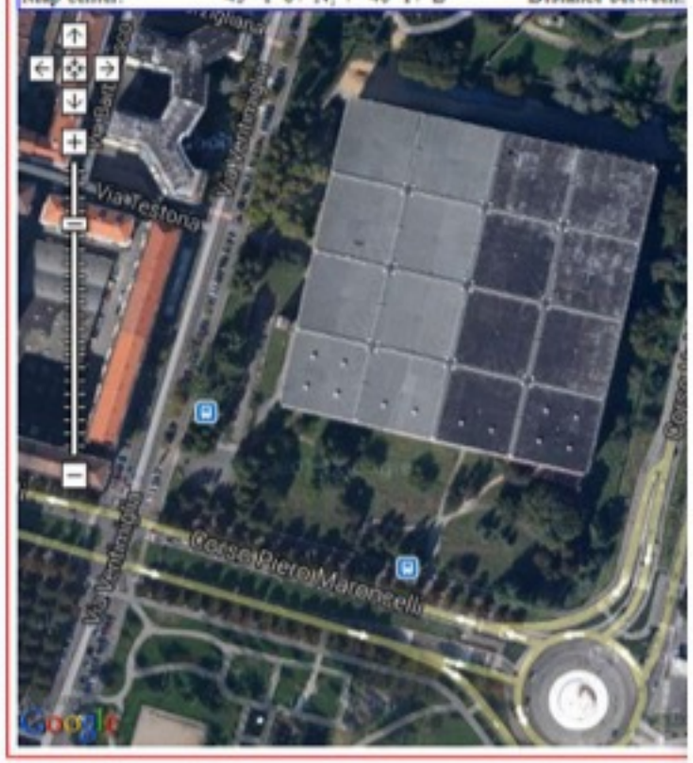
ANALISI DEI METADATI

ESEMPIO: METADATI NELLE IMMAGINI

Basic Image Information

Camera:	Apple iPhone 4
Lens:	3.9 mm
Exposure:	Auto exposure, Program AE, 1/40 sec, f/2.4, ISO
Flash:	No flash function
Date:	**July 14, 2011** 1:13:43PM (timezone not specified) (2 years, 1 month, 29 days, 1 hour, 57 minutes, 26 seconds of 1 hour ahead of GMT)
Location:	Latitude/longitude: **45°** 1' 7.2" North, **7°** 40' 16. (45.018667, 7.671333) Map via embedded coordinates at: Google, Yahoo, WikiM (also see the Google Maps pane below) Timezone guess from earthtools.org: 1 hour ahead of GMT
File:	**200** × **200** JPEG 14,773 bytes (0.014 megabytes) Image compression: 8 13% crop of the 480 × 640 (0.3 megapixel) origina
Color Encoding:	Embedded color profile: "sRGB"
Image URL:	http://0.academia-photos.com/638646/424198/523323/s200 Apply other tools to this image via ImgOps.com.

GPS-encoded location: 45° 1' 07"N, 7° 40' 17"E Display area:
Map center: 45° 1' 07"N, 7° 40' 17"E Distance between:



Here's the full data:

EXIF — this group of metadata is encoded in 712 bytes (0.7k)

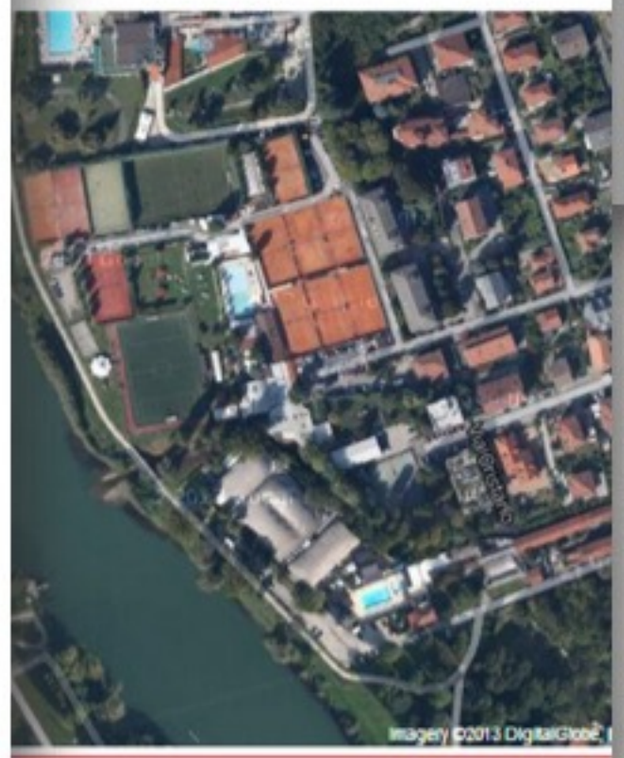
Exif Image Size	480 × 640
Make	Apple
Camera Model Name	iPhone 4
Orientation	Horizontal (normal)
Software	4.3.3
Modify Date	**2011:07:14** 13:13:43 2 years, 1 month, 28 days, 17 hours, 57 minutes, 26 seconds ago
Exposure Time	1/40
F Number	2.40
Exposure Program	Program AE
ISO	160
Exif Version	0221
Date/Time Original	**2011:07:14** 13:13:43 2 years, 1 month, 28 days, 17 hours, 57 minutes, 26 seconds ago
Create Date	**2011:07:14** 13:13:43 2 years, 1 month, 28 days, 17 hours, 57 minutes, 26 seconds ago
Components Configuration	-, -, -, Y
Shutter Speed Value	1/40
Aperture Value	2.40
Metering Mode	Multi-segment
Flash	No flash function
Focal Length	3.9 mm
Flashpix Version	0100
Color Space	sRGB
Sensing Method	One-chip color area
Exposure Mode	Auto
White Balance	Auto
Scene Capture Type	Standard
Sharpness	Normal
GPS Latitude Ref	North
GPS Latitude	45.018667 degrees
GPS Longitude Ref	East
GPS Longitude	7.671333 degrees
GPS Time Stamp	13:20:40
GPS Img Direction Ref	True North
GPS Img Direction	292.1517241
Resolution	72 pixels/inch

JFIF

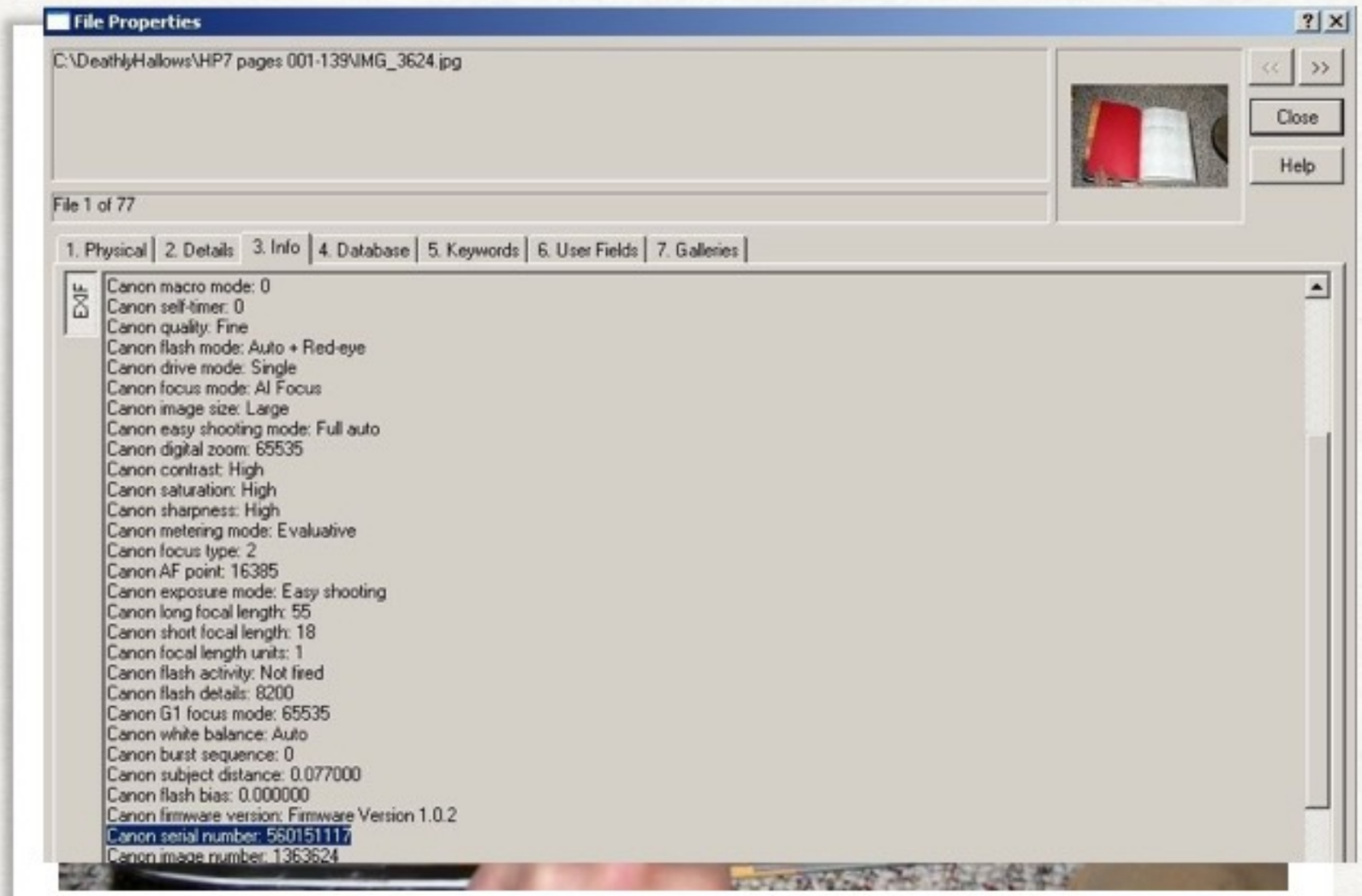
JFIF Version	1.01
Resolution	72 pixels/inch

http://regex.info/exif.cgi?imgurl=http%3A%2F%2F0.academia-photos.com%2F638646%2F424198%2

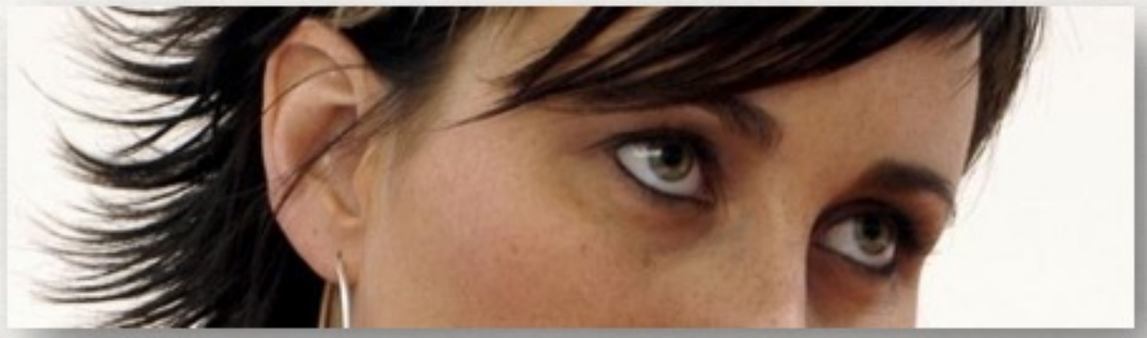
200% (400% the area of the original)



EXIF: UN CASO FAMOSO



EXIF TRADITORI



- Cat Schwartz
- &
- PhotoShop "crop"

full metadata intact, revealing not just that it was captured using an iPhone 4S, but the exact

CNET › News › Politics and Law › McAfee: Photo 'location' leak meant to mislead cops

McAfee: Photo 'location' leak meant to mislead cops

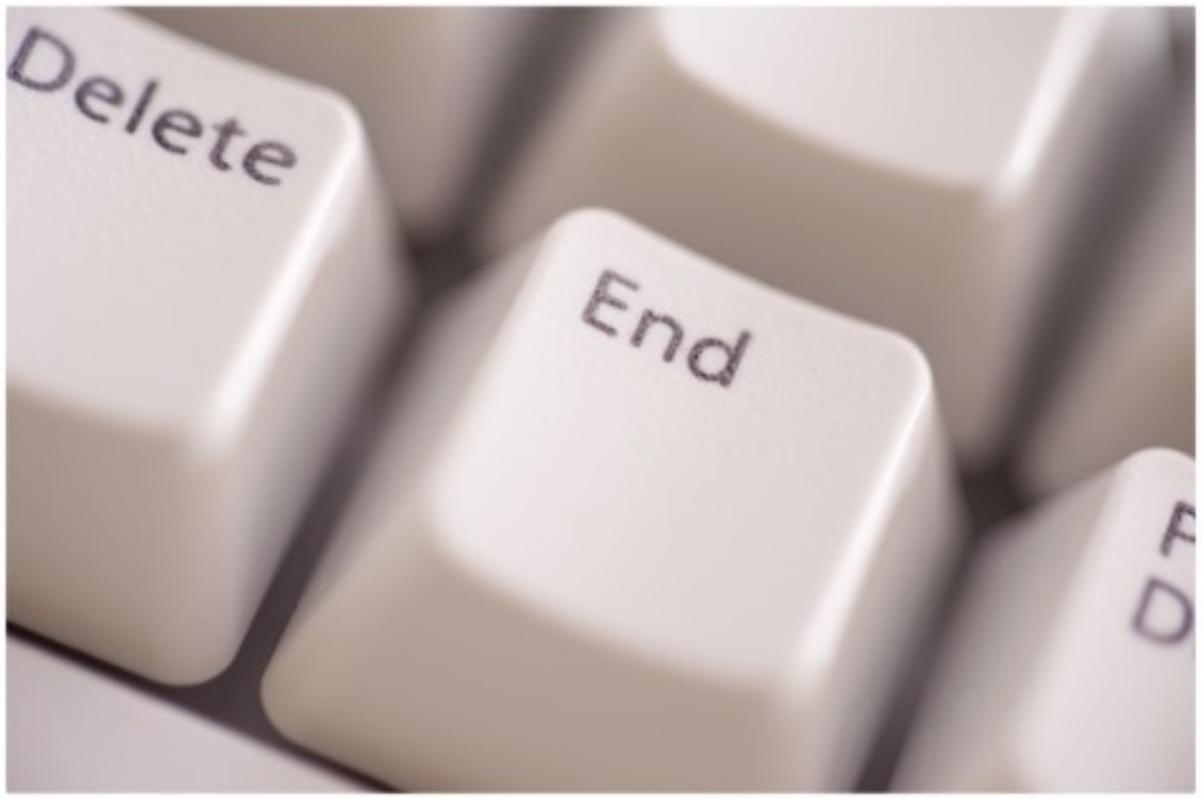
Antivirus pioneer John McAfee, on the run from police, appears to reveal his location through metadata posted on a magazine's website. Then he says it was intentional disinformation. Then he changes his story again.


by Declan McCullagh and Greg Sandoval | December 3, 2012 3:52 PM PST

Immagini: www.pcworld.com

THUMBNAIL EXIF

GRAZIE PER L'ATTENZIONE



LABORATORIO