DIGITAL FORENSICS

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 Trusugi Linux fino al 2018
- Socio Tech & Law, Clusit, AIP, AssobIT
- paolo@dalchecco.it - @forensico
- dalchecco.it, bitcoinforensics.it, ransomware.it

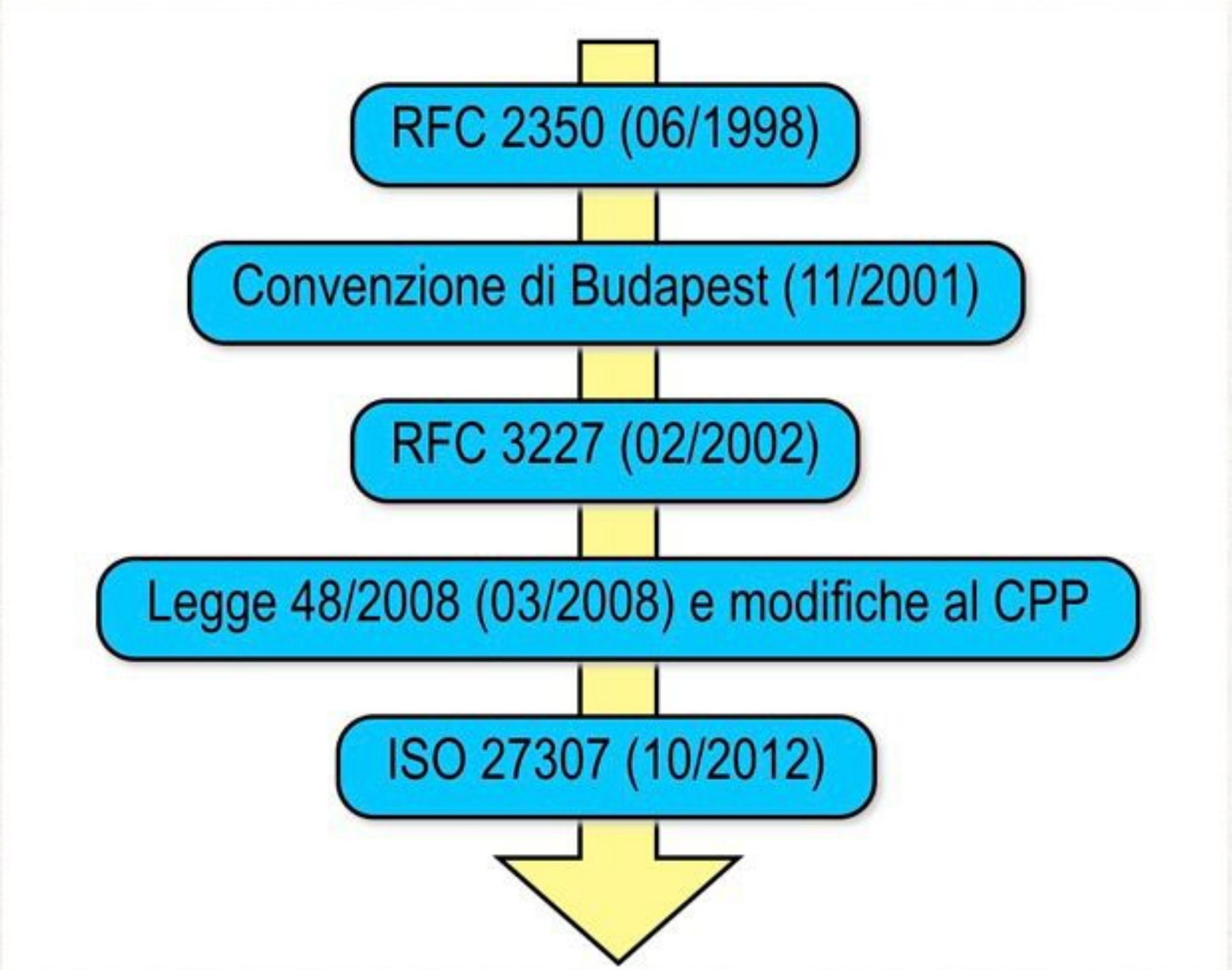
INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

COS'È LA COMPUTER FORENSICS?

L'informatica forense è la scienza che studia, in ambito giuridico, l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione, l'impiego ed ogni altra forma di trattamento del dato informatico al fine di essere valutato in un processo

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

NORMATIVE E BEST PRACTICES



INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

BEST PRACTICES – ACQUISIZIONE DELLE PROVE (RFC3227)

La RFC3227: Guidelines for Evidence Collection and Archiving

Pubblicata nel febbraio 2002, è ancora un punto di riferimento internazionale. Tra le altre cose consiglia di:

- Documentare dettagliatamente ogni operazione svolta (chiari riferimenti temporal indicando eventuali discrepanze)
- Evitare tecniche invasive o limitarne l'impatto, preferendo strumenti ben documentabili
- Isolare il sistema da fattori esterni che possono modificarlo (attenzione: l'attività potrebbe essere rilevata)
- Nella scelta tra acquisizione e analisi, **PRIMA** si acquisisce e **POI** si analizza
- Essere metodici e implementare automatismi (attenzione: arma a doppio taglio)
- Procedere dalle fonti più volatili alle meno volatili
- Eseguire copie bit-level (bit stream image) e lavorare su esse

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

- ISO **27037**: ""Guidelines for identification, collection, acquisition and preservation of digital evidence"
- La ISO/IEC 27037:2012 si limita alle fasi iniziali del processo di gestione della prova informatica, non arriva all'analisi, non si occupa di aspetti legali, strumenti, reportistica, trattamento dei dati
- Integrità della prova informatica e metodologia al fine di rendere ammissibile la prova in giudizio
- Si occupa di trattamento del reperto informatico e **identifica 4 fasi**:
  - 1)Identificazione (ispezione),
  - 2) Raccolta (sequestro)
  - 3) Acquisizione (copia o sequestro virtuale)
  - 4) Conservazione (conservazione e sigillo)

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

49016-17

In caso di diffusione del presente provvedimento omettere le generalità e gli altri dati identificativi, a norma dell'art. 52 d.lgs. n. 196/03 in quanto:
☐ disposto d'ufficio
☐ a richiesta di parte
☐ imposto dalla legge

REPUBBLICA ITALIANA

In nome del Popolo Italiano

LA CORTE SUPREMA DI CASSAZIONE

QUINTA SEZIONE PENALE

Composta da:

PUBBLICA UDIENZA
DEL 19/06/2017

MARIA VESSICHELLI - Presidente -
CATERINA MAZZITELLI
SERGIO GORJAN
GIUSEPPE DE MARZO
IRENE SCORDAMAGLIA - Rel. Consigliere -

Sent. n. sez.
1660/2017

REGISTRO GENERALE
N.9109/2017

http://www.processopenaleegiustizia.it/materiali/49016.pdf

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

2. Va giudicata ineccepibile la decisione della Corte territoriale di non acquisire la trascrizione delle conversazioni svoltesi sul canale informatico denominato '*whatsapp*', tra l'imputato e la parte offesa il 2 gennaio 2014, che la difesa dell'imputato avrebbe voluto versare agli atti del processo a riprova della inattendibilità della persona offesa, che aveva sostenuto che la relazione con l'imputato si era interrotta nell'ottobre 2013.

Deve, infatti, osservarsi che, per quanto la registrazione di tali conversazioni, operata da uno degli interlocutori, costituisca una forma di memorizzazione di un fatto storico, della quale si può certamente disporre legittimamente ai fini probatori, trattandosi di una prova documentale, atteso

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

l'utilizzabilità della stessa è, tuttavia, condizionata dall'acquisizione del supporto – telematico o figurativo - contenente la menzionata registrazione, svolgendo la relativa trascrizione una funzione meramente riproduttiva del contenuto della principale prova documentale (Sez. 2, n. 50986 del 06/10/2016, Rv. 268730; Sez. 5, n. 4287 del 29/09/2015 – dep. 2/02/2016, Pepi, Rv. 265624): tanto perché occorre controllare l'affidabilità della prova medesima mediante l'esame diretto del supporto onde verificare con certezza sia la paternità delle registrazioni sia l'attendibilità di quanto da esse documentato.

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

CONSIGLI UTILI

- Se il sistema è accesso, non spegnere il sistema prima di aver completato tutte le necessarie acquisizioni
- Valutare la modalità di spegnimento più idonea
- L'attaccante può aver alterato le normali procedure di shutdown
- Con uno spegnimento improvviso alcune informazione potrebbero andare perse
- Se il sistema è spento, non accenderlo
- Non fidarsi del sistema: utilizzare tool propri, compilati staticamente e su supporto in sola lettura
- Non usare programmi che possono alterare la timeline dei file
- La corretta profilazione dell'utente è importante per calibrare le modalità di intervento

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

CATENA DI CUSTODIA

Procedura che consente di tracciare lo stato di un reperto e la relativa responsabilità in qualsiasi momento della sua esistenza

Deve documentare in modo chiaro:

- Dove, quando e da chi il reperto è stato rinvenuto e acquisito
- Dove, quando e da chi è stato custodito e/o analizzato
- Chi ha avuto il reperto in custodia e in quale periodo
- Come è stato conservato
- Ad ogni passaggio di consegna, bisogna indicare dove e come è stato trasferito

Gli accessi ai reperti devono essere estremamente ristretti e documentati.

INTRODUZIONE ALLE PROBLEMATICHE DI COMPUTER FORENSICS

WRITE BLOCKER

- Il write blocker è un dispositivo hardware che:
  - Inibisce la scrittura sul dispositivo a cui è collegato in modo da non alterarlo
  - Fa credere al sistema operativo che ha accesso anche in scrittura (ma non è vero)
- Esistono anche write blocker software in particolare sono molto diffusi quelli per bloccare la scrittura su dispositivi USB

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

Il processo di investigazione forense prevede le seguenti fasi:

- Identificazione
- Preservazione
- Acquisizione
- Analisi
- Presentazione dei risultati

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

IDENTIFICAZIONE

- Individuare le informazioni o le fonti di informazione disponibili prestando attenzione in quanto i dati potrebbero essere nascosti (fisicamente o logicamente) oppure essere altrove

- Rilevare elementi ambientali può essere utile per reperire informazioni sugli usi e la disponibilità dei sistemi, soprattutto per individuare responsabilità personali

- Simili informazioni, se non annotate con precisione, potrebbero andar perse

- Potrebbe capitare che chi esegue l'acquisizione non è la stessa persona che effettuerà l'analisi

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI

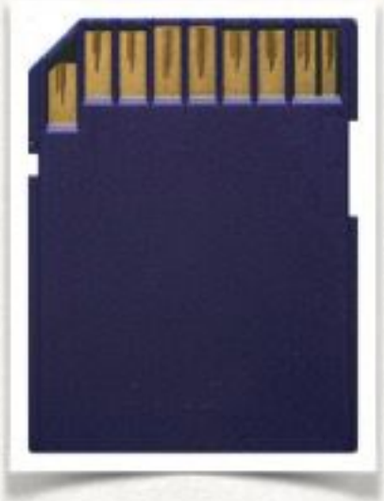
- Computer (hard disk interno)
- Dispositivi di storage comuni (hard disk esterni, chiavette USB, schede di memoria)
- Dispositivi di storage non comuni (orologi con memoria, coltellini svizzeri, ecc.)
- Floppy, CD, DVD o Blue-Ray
- Macchine fotografiche digitali
- Console
- Cellulari, Palmari, iPod, Smartphone, Tablet, Smartwatch

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI

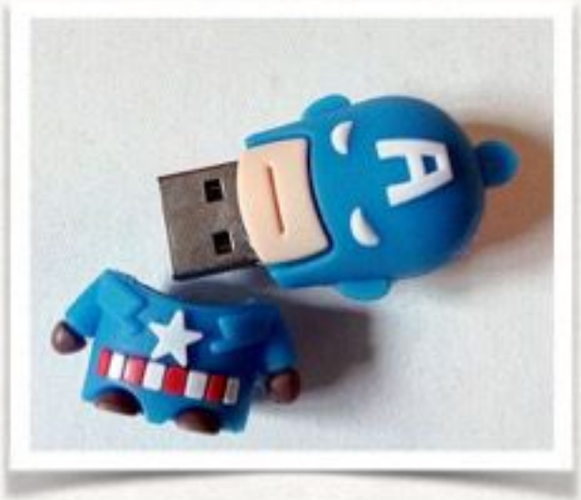


LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI



LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ALCUNE TIPOLOGIE DI MEDIA ACQUISIBILI

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

IDENTIFICAZIONE

Una volta identificato cosa acquisire bisogna:

- Saper valutare cosa va acquisito e cosa è trascurabile
- Essere in grado di acquisire tutto quello che è necessario
- "Etichettare" univocamente ogni supporto
- Assegnare un identificativo associato alla descrizione (marca, modello, seriale, ubicazione, stato ecc.)
- Stabilire il piano di acquisizione efficace

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ACQUISIZIONE

Bisogna rispettare un ordine di volatilità:

- Registri, cache
- Memorie RAM
- Stato della rete (connessioni stabilite, socket in ascolto, applicazioni coinvolte, cache ARP, routing table, DNS cache ecc.)
- Processi attivi
- Memorie di massa (hard disk, pendrive USB, ecc.)
- Log remoti
- Floppy, nastri e altri dispositivi di backup
- Supporti ottici

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ACQUISIZIONE

- Le copie eseguite devono essere identiche all'originale (integrità e non ripudiabilità)
- Le procedure devono essere documentate e attuate secondo metodi e tecnologie conosciute, così da essere verificabili dalla controparte

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

PRESERVAZIONE

- Non bisogna alterare il reperto originale (Write blocker / Distro Forense)

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

ANALISI

- Estrarre i dati e processarli per ricostruire informazioni
- Interpretare le informazioni per individuare elementi utili alle indagini
- Comprendere e correlare, in modo da affinare le ricerche e poterne trarre le conclusioni
- E' sicuramente la fase più laboriosa di tutto il processo e richiede conoscenze disparate

LE FASI DELL'ACCERTAMENTO FORENSE SU DATI DIGITALI

PRESENTAZIONE

Alla fine dell'attività di analisi, si deve presentare quanto elaborato, in una relazione tecnica:

- I risultati devono essere presentati in forma facilmente comprensibile a tutti
- I destinatari non hanno di solito competenze informatiche approfondite
- Tuttavia è probabile che la relazione venga esaminata da un tecnico della controparte
- Essere semplici e chiari, non bisogna essere superficiali e approssimati

PRINCÌPI, PREPARAZIONE, PRECAUZIONI E UTILIZZO DEI SISTEMI LIVE

- Un sistema live è un sistema operativo – Tsurugi Linux nel nostro caso- che per essere eseguito viene caricato nella memoria RAM in modo parziale o integrale (tramiteil parametro **toram**)
- NON scrive nulla sul disco rigido per poter essere eseguito
- Allo spegnimento del computer NON restano tracce del sistema live eseguito e le eventuali personalizzazioni al sistema verrano perse
- Un sistema live ad uso forense NON fa il mount automatico delle memorie di massa ad esso collegate

PRINCÌPI, PREPARAZIONE, PRECAUZIONI E UTILIZZO DEI SISTEMI LIVE

- Assicurarsi che venga fatto il boot da CD (o da USB) utilizzando gli appositi tasti (CANC, F2, F8, F12, ESC, ecc.) in modo da selezionare il corretto dispositivo di boot
- In caso contrario il boot verrebbe fatto dal sistema residente sull'hard disk con rischio di alterazione dei dati
- Nel caso di dubbio sul tasto di boot da utilizzare, scollegare temporaneamente il disco fisso a PC **SPENTO**

PRINCÌPI, PREPARAZIONE, PRECAUZIONI E UTILIZZO DEI SISTEMI LIVE

E' possibile selezionare tre modalità di avvio di Trusugi:

- Utilizzando interfaccia grafica
- Tramite la modalità testuale utile nel caso in cui per qualsiasi motivo (es. risorse hardware limitare che non permettono l'avvio della GUI, scheda video non supportata, ecc.) non si possa utilizzare l'interfaccia grafica
- Modalità “To RAM” passando il parametro **toram** in fase di boot (già presente nel menu di boot in Trusugi Acquire)
- Tramite interfaccia grafica è possibile montare in sola lettura le immagini o i dispositivi da analizzare direttamente utilizzando "Disk utility” o il file manager, mentre tramite interfaccia testuale bisogna prestare attenzione ad inserire l'opzione di "sola lettura" durante l'operazione di mount

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

Cos'è Trusugi?

- DFIR Linux distribution. *A Tsurugi (剣) is a legendary Japanese double-bladed sword used by ancient Japan monks*

Chi c'è dietro Tsurugi?

- Giovanni 'sug4r' Rattaro: Tsurugi Linux and Tsurugi Acquire core Developer
- Marco 'blackmoon' Giorgi: Tsurugi Linux and Tsurugi Acquire core Developer
- Davide 'rebus' Gabrini: Bento DFIR toolkit project leader
- Francesco 'dfirfpi' Picasso: New staff 2019! Tsurugi Linux and Tsurugi Acquire core Developer

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

- Distribuzione basata su Lubuntu Mate LTS
- Deve essere avviata al boot via DVD o USB, ma può essere installata o eseguita in virtual machine (attenzione ala protezione dei dispositivi attraverso la VM)
- Ideale per eseguire copie forensi o triage
- Toolkit per acquisizione e analisi (timeline, metadati, supertimeline, registro, ecc.)

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

- Minimale, solo per acquisizioni e mount di img

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

DOVE È POSSIBILE USARE TRUSUGI?

Trusugi Linux: su tutte le architetture x86
e su architetture a 64 bit

Bento: su tutti i computer con Microsoft Windows
...ma non solo

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

QUANDO PUÒ ESSERE UTILE?

Clonare un hard disk senza dover smontare lo schermo

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

DOVE NON POSSO USARE TRUSUGI?

Mainframe

Architetture non x86

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

OLTRE ALLE ACQUISIZIONI?

- Analisi di memorie di massa
- Analisi di traffico di rete
- Analisi di dispositivi mobile
- Analisi di backup di iPhone e Black Berry
- Analisi dei database che compongono parte della app, sia per iOS che per Android
- Incident Response e Live Forensics
- Attività di analisi in contesti di Cyber Intelligence
- Organizzazione delle evidence

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

TRUSUGI IN MACCHINA VIRTUALE: VANTAGGI E SVANTAGGI

- Trusugi mette a disposizione una virtual appliance, scaricabile dal sito ufficiale, già pronta per essere eseguita in una macchina virtuale

- Trusugi infatti può essere utilizzato come un sistema per workstation atte all'analisi

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

TRUSUGI IN MACCHINA VIRTUALE: VANTAGGI E SVANTAGGI

Vantaggi:

- Non si necessita di una macchina fisica dedicata
- Sulla stessa macchina fisica è possibile installare più macchina per l'analisi (se l'hardware lo permette)
- Possibilità di aggiungere software
- Possibilità di salvare le personalizzazioni in modo persistente
- Possibilità di spostare il sistema virtualizzato da una macchina fisica all'altra
- Possibilità di condividere i file tra host e guest (anche diversi) ed eventualmente tra le varie macchine virtuali

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

TRUSUGI IN MACCHINA VIRTUALE: VANTAGGI E SVANTAGGI

Svantaggi:

- Necessita di hardware performante
- Il sistema host potrebbe scrivere su un eventuale device collegato per essere analizzato o acquisito (necessario write blocker), ma di ma solitamente non si collegano mai in questa modalità i device da acquisire

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

BENTO

- Raccolta di applicativi ottimizzati, liberamente re-distribuibili per licenza d'uso, per eseguire attività di Incident Response e Live Forensics
- Alto livello di personalizzazione, senza l'obbligo di ricompilare codice sorgente
- Controllo dell'integrità dell'applicativo prima dell'avvio
- Binari dei principali sistemi operativi Windows, Linux e OS X

INTRODUZIONE AL SISTEMA TRUSUGI E BENTO

BENTO: POTENZIALITÀ

- Acquisizione memorie di massa
- Dump memoria RAM
- Calcolo di hash
- Analisi processi
- Analisi traffico di rete
- Analisi registro di Windows
- Antimalware e antirootkit
- Time line degli eventi del sistema
- Analisi navigazione internet e posta elettronica
- Password cracking
- E molto altro...

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

MICROSOFT WINDOWS

- Il sistema operativo Windows 1.0 di Microsoft viene sviluppato per la prima volta nel 1985, era molto immaturo e non aveva il supporto per le reti.

- Vengono rilasciate nuove versioni fino ad arrivare alla attuale versione 10: progressivamente si introducono nuove feature e le varie versioni diventano sempre più affidabili

- Ricordiamo alcune feature:
  Obbligo utilizzo filesystem NTFS (da Windows XP)
  Active Directory
  Windows Update
  Multiutenza
  Disponibile per architetture a 64-bit (Win XP / più diffusamente con Vista)
  Bitlocker
  …

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

MS WINDOWS: CARTELLE DI INTERESSE

- La cartella utente:
  - **C:\Document and settings\NOME-UTENTE** (Win XP/Vista)
  - **C:\Users\NOME-UTENTE** (da Win 7)
  - NOTA: Nella cartella utente troviamo anche il file **NTUSER.DAT** che contiene i dati del registro relativi all'utente
    Inoltre fare riferimento alle altre sotto cartelle, le quali possono contenere altri file utili.
- Cartella con file del registro configurazione:
  - **C:\Windows\System32\Config**
- Cartella con il registro eventi:
  - **C:\Windows\System32\Config\Events**

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

MS WINDOWS: ALTRI PUNTI INTERESSANTI DEL SISTEMA

- Registro di sistema
- File di swap e di ibernazione (pagefile.sys, hiberfil.sys)
- Eventi di sistema (estensione .evt relativi a: Applicazione, Protezione, Sistema, …)
- Cestino, file recenti, thumbs.db, spooler di stampa
- Punti di ripristino
- Dati applicazioni e Impostazioni locali (Browser, e-mail, chat, software P2P)

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

LINUX

- Il sistema operativo GNU/Linux nasce nel 1991 partendo da un'idea di Linus Torvalds
- Sistema basato su Kernel "Unix-like" open source e gratuito
- Nascono le prime aziende e progetti senza scopo di lucro tra cui Red Hat, SuSe, Mandrake, Slackware, Debian, ecc.
- Arrivando ai giorni nostri, cresce il numero di distribuzioni. Nascono, muoiono diversi progetti, interessante è la distribuzione Ubuntu (e le sue derivate), sulla quale si base Trusugi Linux

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

LINUX: CARTELLE DI INTERESSE

Il sistema Linux utilizza standard per i file e le cartelle (LSB) ma in alcuni sistemi si hanno delle piccole differenze. In ogni caso, possiamo fare riferimento a quanto segue:

- Cartella utente: **/home/NOME-UTENTE**
- Cartella con i log di sistema: **/var/log**
- Cartella con le configurazioni di sistema: **/etc**
  In questa cartella troviamo le varie configurazioni tra cui le impostazioni di rete, impostazioni globali del terminale ed altre configurazioni varie, tra cui il file con le password di sistema

Prestiamo particolare attenzione ai "file nascosti" in Linux iniziano con il carattere "." se accediamo a questo filesystem da un sistema Linux che ha disabilitato la visualizzazione dei file nascosti, NON saranno mostrati a video

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

LINUX: ALTRI PUNTI INTERESSANTI DEL SISTEMA

- Generalmente la struttura del filesystem è ordinata come segue:

  /bin contiene i file binari comuni
  /boot contiene il kernel e i file di avvio
  /dev contiene la mappatura dei device
  /etc contiene il i file di configurazione del sistema
  /home contiene i profili utente
  /mnt o **/media** contiene i punti di mount
  /root contiene il profilo dell'amministratore
  /sbin contiene i binari riservati a root
  /tmp contiene il i file temporanei
  /usr contiene gli applicativi non di sistema
  /var contiene i dati degli applicativi (log, mail, spool di stampa, database, sorgenti web, ecc.)

- Il filesystem può essere distribuito su più partizioni

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

LINUX: ALTRI PUNTI INTERESSANTI DEL SISTEMA

Non dimentichiamo che:

- La partizione di swap può contenere dati interessanti
- Le shell mantengono una history: **/home/NOME-UTENTE/.bash_history**
- Nella cartella /home dell'utente dobbiamo controllare:
    - Configurazioni personali
    - Dati delle applicazioni dell'utente
    - Dati dell'utente
    - Ricordandoci che generalmente i file o le cartelle contenenti le configurazioni iniziano con il carattere "." (es. ~/.config)

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

APPLE MAC OS

- Il sistema operativo Mac OS di Apple nasce nel 1984, il nome è l'acronimo di Macintosh Operating System
- Aveva la caratteristica di essere un sistema operativo completamente grafico. Questa novità favorì molto la popolarità delle GUI
- L'attuale Mac OS X ("10" in numeri romani) è stato completamente riscritto e migliorato (commercializzato dal 2001)

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

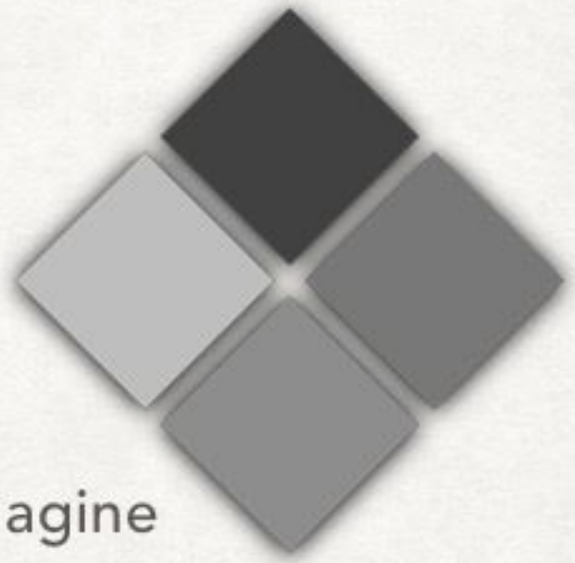
APPLE MAC OS X: CARTELLE DI INTERESSE

Le principali cartelle di interesse di OS X sono le seguenti:

- Cartella utente: **/Users/NOME-UTENTE**
- Cartella con i log di sistema: **/var/log**
- Cartella con le configurazioni di sistema: **/etc**
- Anche in questo caso, prestiamo particolare attenzione ai "file nascosti" in Linux iniziano con il carattere "." se accediamo a questo filesystem da un sistema Linux che ha disabilitato la visualizzazione dei file nascosti, NON saranno mostrati a video

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

APPLE MAC OS X: BOOT CAMP



Boot Camp è una tecnologia sviluppata da Apple che consente di installare un sistema Windows o Linux in una partizione del disco Macintosh. Il partizionamento avviene in modo non distruttivo e contestualmente viene fornito un immagine CD con i driver per far funzionare il sistema Windows installato

- Non dimentichiamo di verificare la presenza di tale partizione ed in caso positivo di fare un'analisi anche di quest'area

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

CARTELLE DI INTERESSE

Le cartelle indicate in precedenza sono cartelle particolari che potrebbero fornire materiale di interesse, tuttavia **NON** dobbiamo focalizzarci solo su queste, ma prendere una visione completa di tutto il sistema

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

COS'È UN FILESYSTEM?

In informatica, un file system è il metodo con il quale i file sono immagazzinati e organizzati su un dispositivo di archiviazione, come ad esempio un hard disk, una pendrive o un CD-ROM.

Più formalmente, un file system è l'insieme dei tipi di dati astratti necessari per la memorizzazione, l'organizzazione gerarchica, la manipolazione, la navigazione, l'accesso e la lettura dei dati.

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

COS'È UN FILESYSTEM?

I file system generalmente usano dispositivi di archiviazione che offrono l'accesso ad un array di blocchi di dimensione fissa, generalmente in settori di 512 byte l'uno.

Il file system è responsabile dell'organizzazione di questi settori e tiene traccia di quali settori appartengono a quali file, e quali invece non sono utilizzati.

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

TIPI DI FILESYSTEM

- Amiga FileSystems - OFS, FFS1 e 2, International, PFS, SFS usati su Amiga
- BFS (Beos File System) - file system nativo di BeOS
- DFS , ADFS - file system della Acorn
- EFS (IRIX) - un vecchio file system a blocchi usato su IRIX
- Ext2 - Extended File System 2, diffuso su sistemi GNU/Linux
- Ext3/Ext4 - Extended File System 3, diffuso su sistemi GNU/Linux (ext2+journaling)
- FAT - Usato su DOS, Microsoft Windows e su molti dispositivi dedicati, dispone di tabelle a 12 e 16 bit
- FAT32 - versione con tabelle a 32 bit di FAT
- FFS - Fast File System, usato in vecchi sistemi BSD
- HFS - Hierarchal File System, usato su vecchie versioni di Mac OS
- HFS+ - Hierarchal File System Plus, usato su Mac OS X

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

TIPI DI FILESYSTEM

- HPFS - High Performance File System, usato su OS/2
- ISO 9660 - Usato su dischi CD-ROM e DVD-ROM (anche con estensioni Rock Ridge e Joliet)
- JFS – Journaling File System, disponibile su sistemi GNU/Linux, OS/2, e AIX
- LFS - Log-structured File System
- Minix - Usato su sistemi Minix
- NTFS - New Technology File System. Usato su sistemi Windows (NT, 2000, XP, Vista, 7, 8, 10)
- ReiserFS - File system journaling diffuso su sistemi GNU/Linux
- UDF - File system a pacchetti usato su supporti WORM/RW, CD-RW e DVD
- UFS/UFS2 - Unix File System, usato su vecchi sistemi BSD
- UMSDOS - File system FAT esteso con permessi e metadata, usato su GNU/Linux
  XFS - Usato su sistemi IRIX
- ZFS - Creato dalla Sun
- APFS -

UTILIZZO DI TRUSUGI CON I PRINCIPALI O.S. E FILESYSTEM

NETWORK FILESYSTEM

- AFS (Andrew File System)
- AppleShare
- CIFS (conosciuto anche come SMB o Samba)
- Coda
- GFS
- InterMezzo
- Lustre
- NFS

TIPOLOGIE DI ACQUISIZIONE FORENSE E FORMATI

COS'É LA COPIA FORENSE

- La copia forense è un duplicato fedele all'originale in ogni sua parte
- Le duplicazioni eseguite a basso livello vengono anche dette bit stream image

TIPOLOGIE DI ACQUISIZIONE FORENSE E FORMATI

TIPI DI ACQUISIZIONE FORENSE

- **Post mortem (dopo lo spegnimento del sistema)**
  Si smonta il dispositivo e lo si collega ad un PC dedicato all'acquisizione

- **On the fly (direttamente sul sistema posto ad analisi)**
  Nel caso di sistemi RAID l'acquisizione "al volo" è quasi obbligatoria

- **Su network**
  Sia nel caso di acquisizione post mortem, sia nel caso di acquisizione on the fly è possibile salvare l'output direttamente durante la fase di acquisizione in altri PC o dischi della LAN appositamente configurati

  Gli strumenti utilizzati sono:

  - netcat
  - ssh

TIPOLOGIE DI ACQUISIZIONE FORENSE E FORMATI

I formati utilizzati per l'acquisizione forense sono:

- RAW (dd)
- EWF
- AFF

TIPOLOGIE DI ACQUISIZIONE FORENSE E FORMATI

RAW (DD)

- Copia bit a bit del device da acquisire
- E' supportato da tutti i tools di analisi forense (mount diretto)
- Nessuna compressione (occupa lo stesso spazio del dispositivo da acquisire)
- Non supporta i metadati all'interno dell'immagine forense

TIPOLOGIE DI ACQUISIZIONE FORENSE E FORMATI

EWF (EXPERT WITNESS COMPRESSION)

- Standard de facto per le analisi forensi
- E' supportato dai software di analisi open source (Autopsy, PyFlag, ecc.)
- E' supportato dai software commerciali (EnCase, Ftk, ecc.)
- E' possibile includere metadati (anche se in modo limitato) nell'immagine acquisita:
  - Data/ora acquisizione
  - Nome esaminatore
  - Note extra
  - Password
  - Hash MD5 dell'intera immagine
- Supporta la compressione dell'immagine
- Ricerca all'interno dell'immagine acquisita
- Immagini divisibili e "montabili" al volo
- Formato proprietario (la compatibilità è ottenuta tramite il reverse engineering) :-(

TIPOLOGIE DI ACQUISIZIONE FORENSE E FORMATI

AFF (ADVANCED FORENSICS FORMAT)

- E' supportato dai software open source
- Supporta la compressione dell'immagine
- Supporta la cifratura dell'immagine
- Dimensione immagine illimitata (non è necessario splittare)
- Immagini divisibili
- E' possibile includere un numero illimitato di metadati (anche in un file xml separato)
- Formato open source

ATTIVITÀ DI PREVIEW E TRIAGE SICURO CON TSURUGI

E' necessario montare il disco in sola lettura in modo da **non alterare** nessun dato.

Questo può essere utile nel caso in cui, durante le operazioni on-site:

- Si desidera avere risposte immediate (es. verificare se è presente un determinato dato)
- Evidenziare subito informazioni rilevanti
- Si vuole individuare subito responsabilità in caso di risorse condivise
- Gestire al meglio le operazioni di perquisizione
- Creare una timeline (es. per verificare se e quando è stato inserito un determinato pen drive su una determinata macchina)

ATTIVITÀ DI PREVIEW E TRIAGE SICURO CON TSURUGI

Un’ analisi di preview fatta durante le operazioni on-site, può confermare la presenza di una prova individuata, ma il fatto di non individuarla, non ne conferma l'assenza con assoluta certezza.

ACQUISIZIONE DI MEMORIE DI MASSA

- La copia forense è un duplicato fedele all'originale in ogni sua parte che soddisfa i requisiti di **integrità** e **non ripudiabilititità**
- Le duplicazioni eseguite a basso livello vengono anche dette bit stream image
- Le interfacce con cui si ha più spesso a che fare sono ATA, SATA e USB
- Esistono anche altri tipi di interfacce: SCSI, SAS, Firewire, Thunderbolt

ACQUISIZIONE DI MEMORIE DI MASSA

TIPI DI COPIA FORENSE

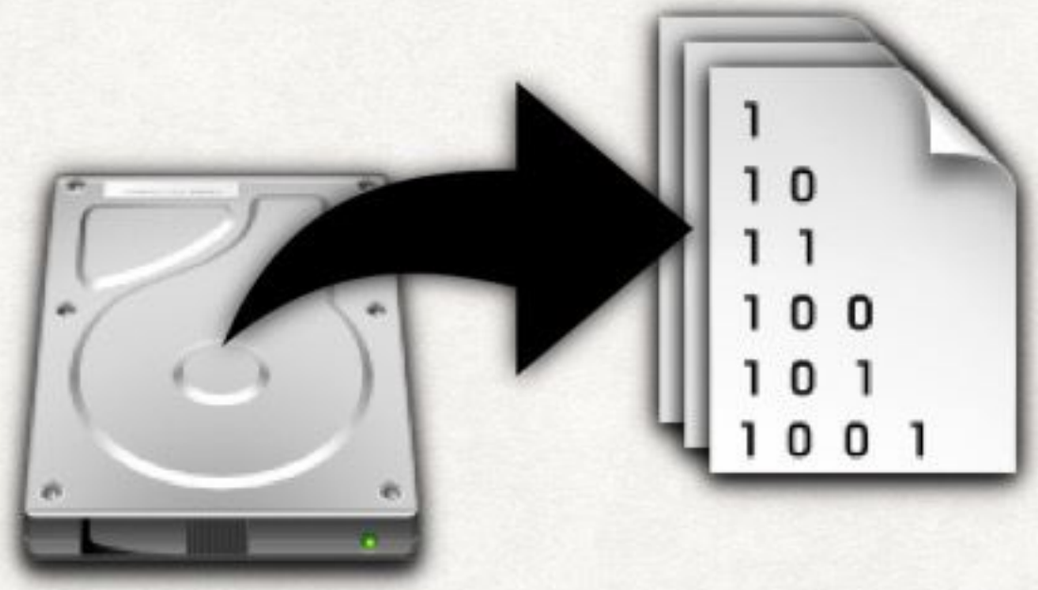
Esistono due modalità di copia forense di un dispositivo:

- Device to file
- Device to device

ACQUISIZIONE DI MEMORIE DI MASSA

DEVICE TO FILE

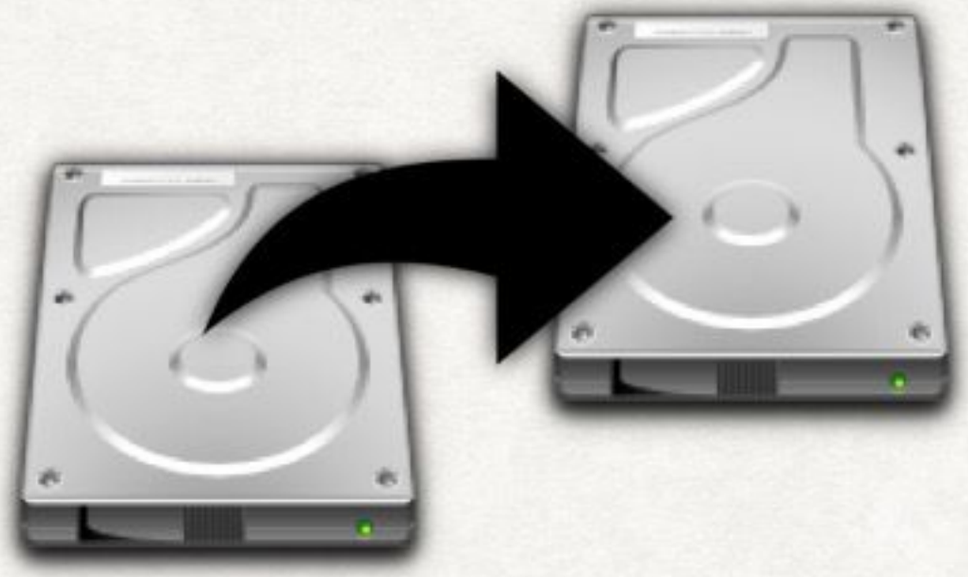
- Consente maggiore flessibilità
- Scelta del formato: RAW (dd), EWF, AFF
- Split su più file
- Compressione
- Cifratura
- Metadati
- Calcolo degli hash facilitato
- Non è indispensabile un write blocker per accedere al file in sola lettura
- Più device possono essere acquisiti sulla stessa unità di destinazione



ACQUISIZIONE DI MEMORIE DI MASSA

DEVICE TO DEVICE

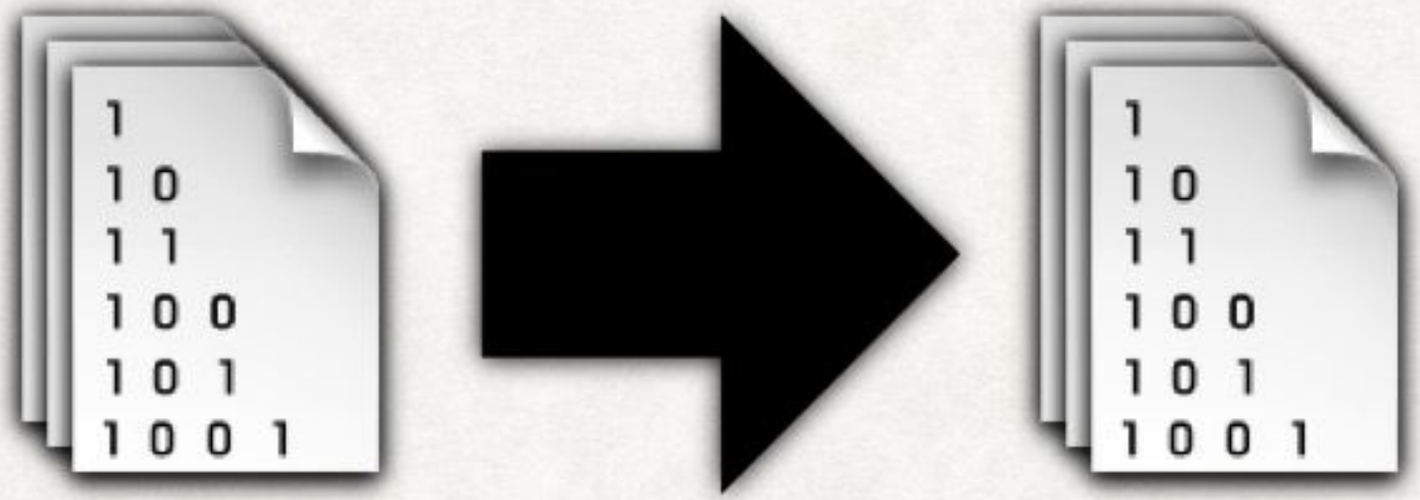
- Richiede un disco di destinazione di capacità uguale o superiore rispetto all'originale
- Richiede un disco di destinazione per ogni disco originale da copiare
- Richiede il wiping del disco di destinazione (per evitare cross contaminazione)
- Richiede che anche le copie vengano trattate con write blocker



ACQUISIZIONE DI MEMORIE DI MASSA

COPIA MULTIPLA

Una volta fatta l'acquisizione e verificati gli hash, si deve fare una seconda copia lavoro mettendo la prima copia al sicuro



ACQUISIZIONE DI MEMORIE DI MASSA

DUPLICATORI

- Hardware
- Live CD Tsurugi
- Workstation dedicata con Tsurugi installata(laboratorio)

ACQUISIZIONE DI MEMORIE DI MASSA

WRITE BLOCKER

- Esistono write blocker hardware ma se utilizziamo Tsurugi non sono necessari

ACQUISIZIONE DI MEMORIE DI MASSA

SOFTWARE DI ACQUISIZIONE

Riga di comando

- dd
- dcfldd
- dc3dd
- ddrescue
- dd_rescue
- ewfaquire
- aimage
- cyClone
- FTK Imager (CLI Linux/Mac)

GUI

- guymager
- dhash
- FTK Imager (GUI Windows)

ACQUISIZIONE DI MEMORIE DI MASSA

DD

- dd è il capostipite di tutti i tools di acquisizione, consente di acquisire i dati bit a bit in formato raw.
- Nativamente non supporta la compressione dei dati, ma è possibile comprimere il data stream tramite l'uso delle pipe

```
# dd if=/dev/sda - | bzip2 > /mnt/image.dd.bz2
```

```
# dd if=/dev/sda of=/mnt/acq/img.dd conv=noerror,sync bs=512
# dd if=/dev/hda conv=noerror,sync bs=512 | split –b 2000m – image.dd
```

ACQUISIZIONE DI MEMORIE DI MASSA

DDRESCUE

- Evoluzione di dd
- Permette di riversare il contenuto di un disco direttamente su di un'altro
- Permette l'acquisizione di memorie di massa che presentano errori durante l'accesso a determinati settori del disco impostando su zero i bit non leggibili
- Durante l'acquisizione della memoria l'applicazione fornisce aggiornamenti su quanti byte sono stati letti e scritti, quanti errori di lettura sono stati riscontrati e la velocità di acquisizione calcolata per byte/s.

ACQUISIZIONE DI MEMORIE DI MASSA

DD_RESCUE

- Evoluzione di dd
- Non è legato allo sviluppo di ddrescue
- Non salta semplicemente il blocco danneggiato, ma tenta di leggerlo ricorrendo a tecniche diverse (es. variando dinamicamente la lunghezza dei blocchi)
- Durante l'acquisizione della memoria l'applicazione fornisce informazioni sullo stato delle operazioni correnti.

ACQUISIZIONE DI MEMORIE DI MASSA

DCFLDD

- dcfldd è una versione avanzata di dd sviluppata dal Dipartimento della Difesa degli U.S.A.
- Calcolo al volo degli hash (MD5, SHA-1) dell'immagine
- Indicatore di avanzamento sui dati acquisiti
- Output simultaneo su più file (o dischi)
- Output divisibile in più file
- Log


```
# dcfldd if=/dev/sda hash=md5,sha256 md5log=image.md5
                    sha256log=image.sha256  of=/mnt/image.dd
```

ACQUISIZIONE DI MEMORIE DI MASSA

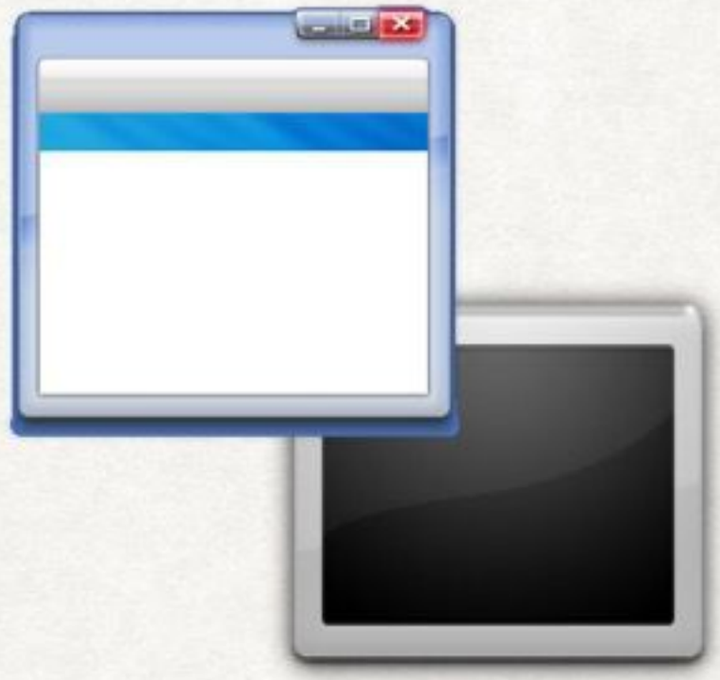
CYCLONE

- Wizard per l'acquisizione guidata, sviluppato team Tsurugi, che permette di effettuare l'acquisizione delle immagini rispondendo a semplici domande visualizzate a video
- Acquisizione in diversi formati
- (raw, ewf, aff)
- Compressione (ewf, aff)
- Calcolo hash
- Log

ACQUISIZIONE DI MEMORIE DI MASSA

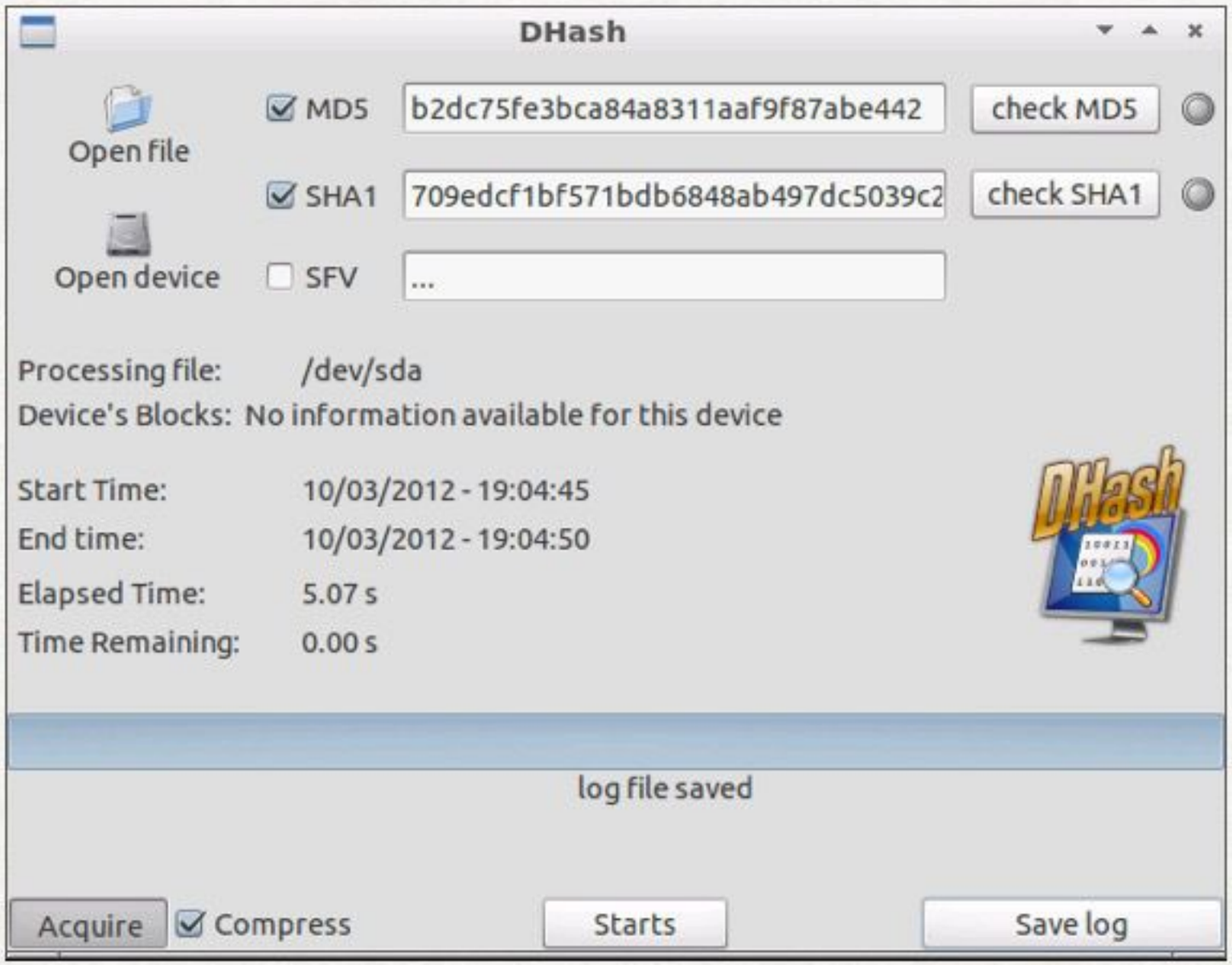
DHASH

- Tool per l'acquisizione in formato raw, sviluppato dal team Tsurugi sia per riga di comando sia per interfaccia grafica
- Consente compressione (bz2)
- Calcolo hash
  - MD5
  - SHA-1
  - SFV
- Calcolo del tempo residuo di acquisizione
- 10% più veloce nel calcolo degli hash rispetto a gli altri tools
- Log



ACQUISIZIONE DI MEMORIE DI MASSA

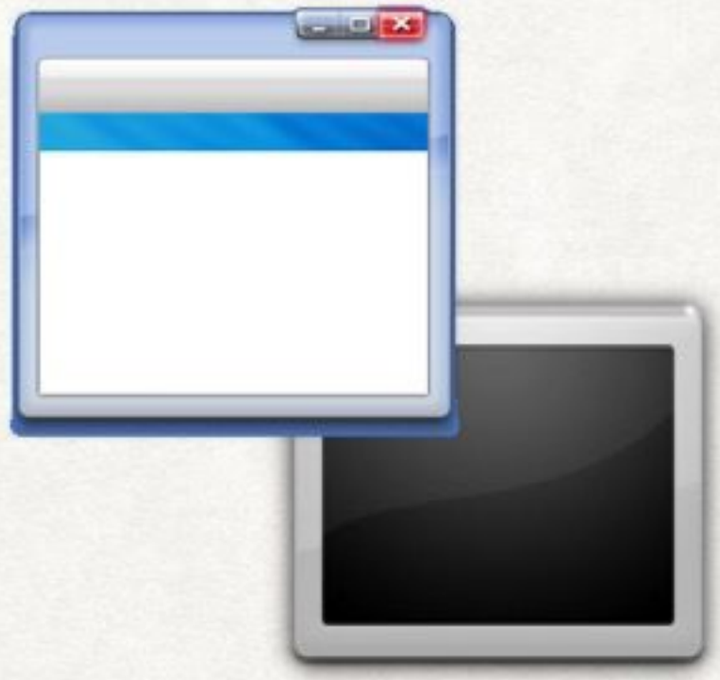
DHASH



ACQUISIZIONE DI MEMORIE DI MASSA

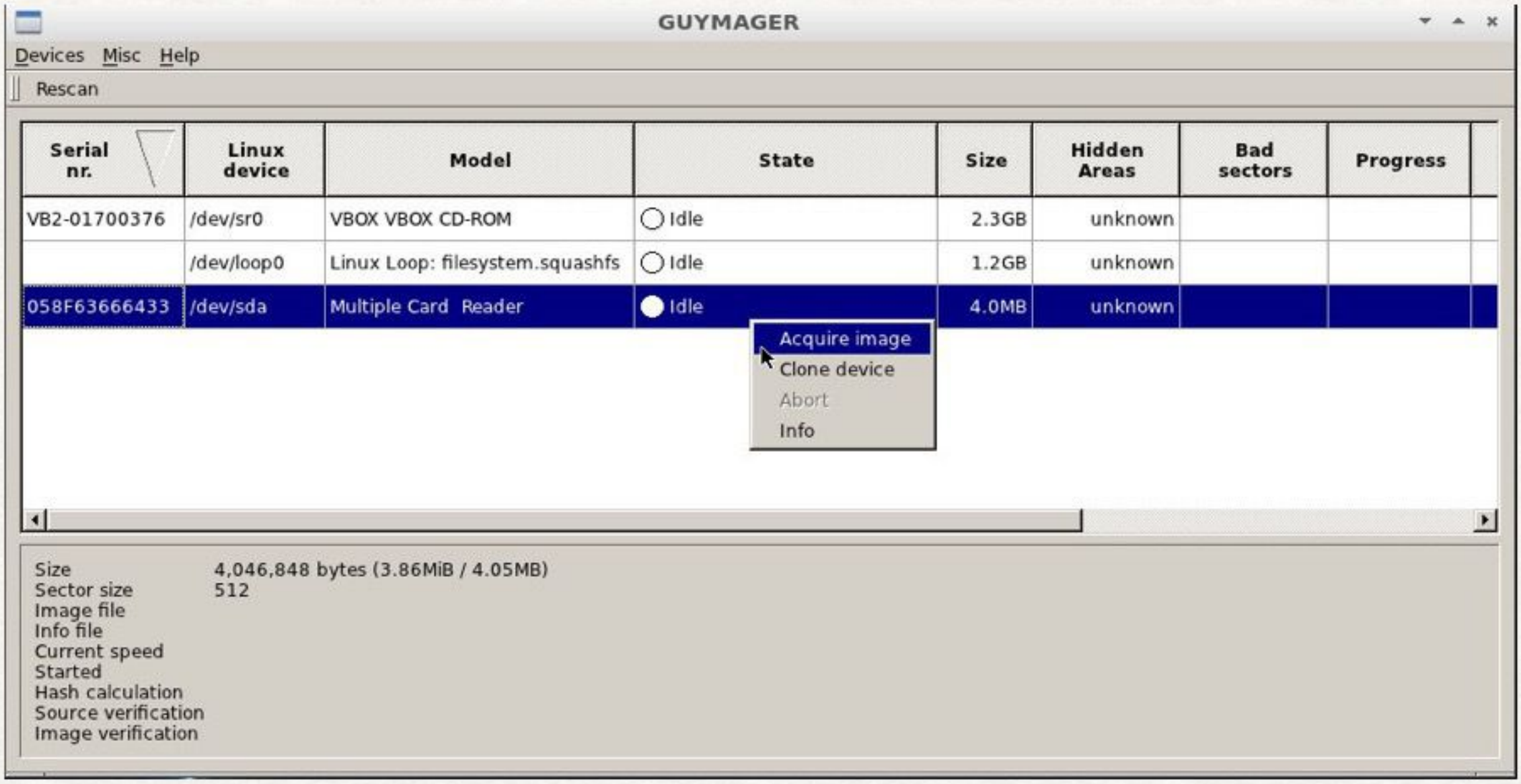
GUYMAGER

- Acquisizione in diversi formati:
  - raw
  - ewf
  - aff
- Calcolo hash:
  - MD5
  - SHA-1 / SHA-256
- Inserimento metadati per formato ewf
- Split per formato ewf
- Utile nel caso in cui si debba fare più di un'acquisizione contemporaneamente
- Personalizzabile tramite file di configurazione
- Log



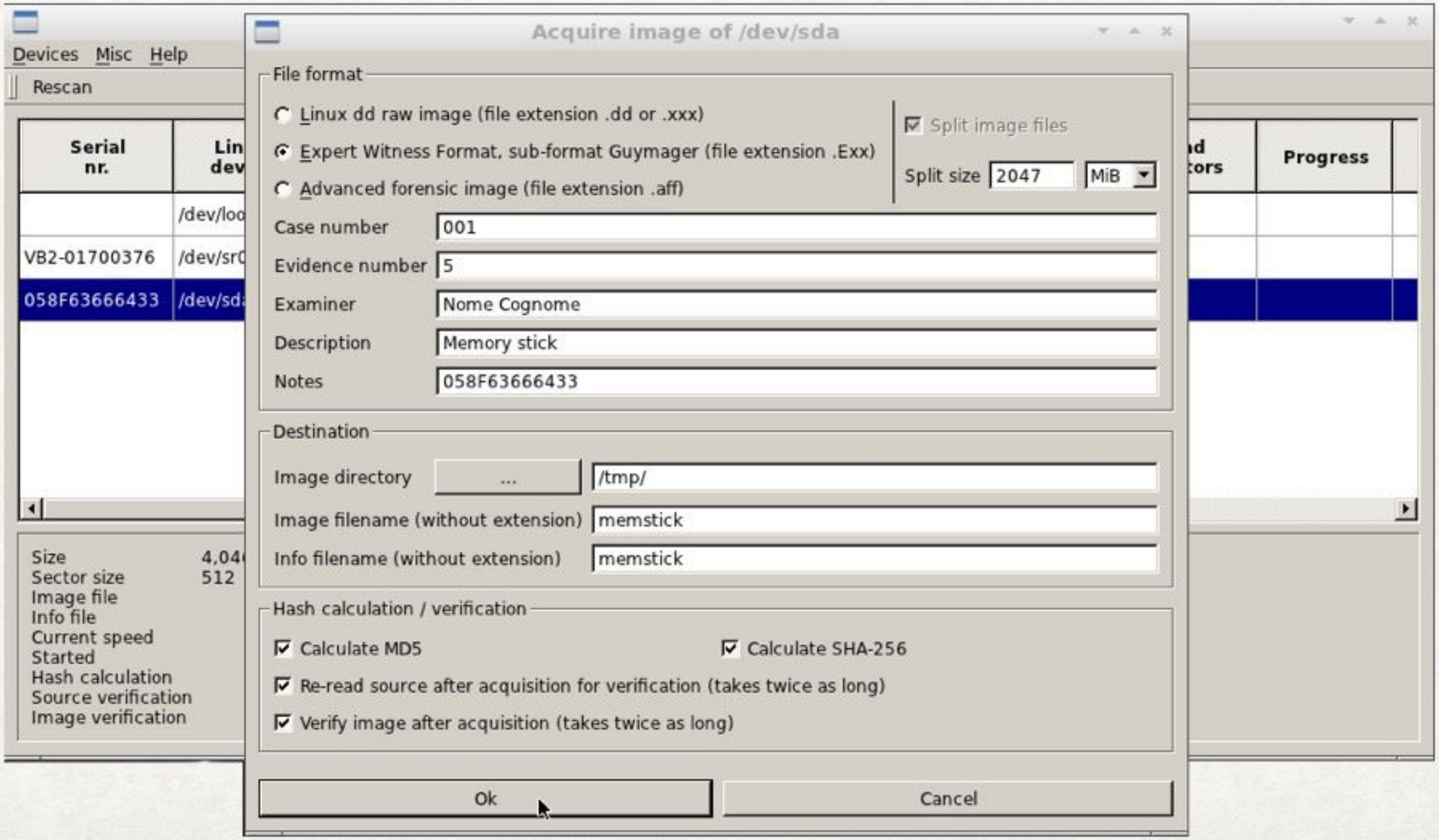
ACQUISIZIONE DI MEMORIE DI MASSA

GUYMAGER



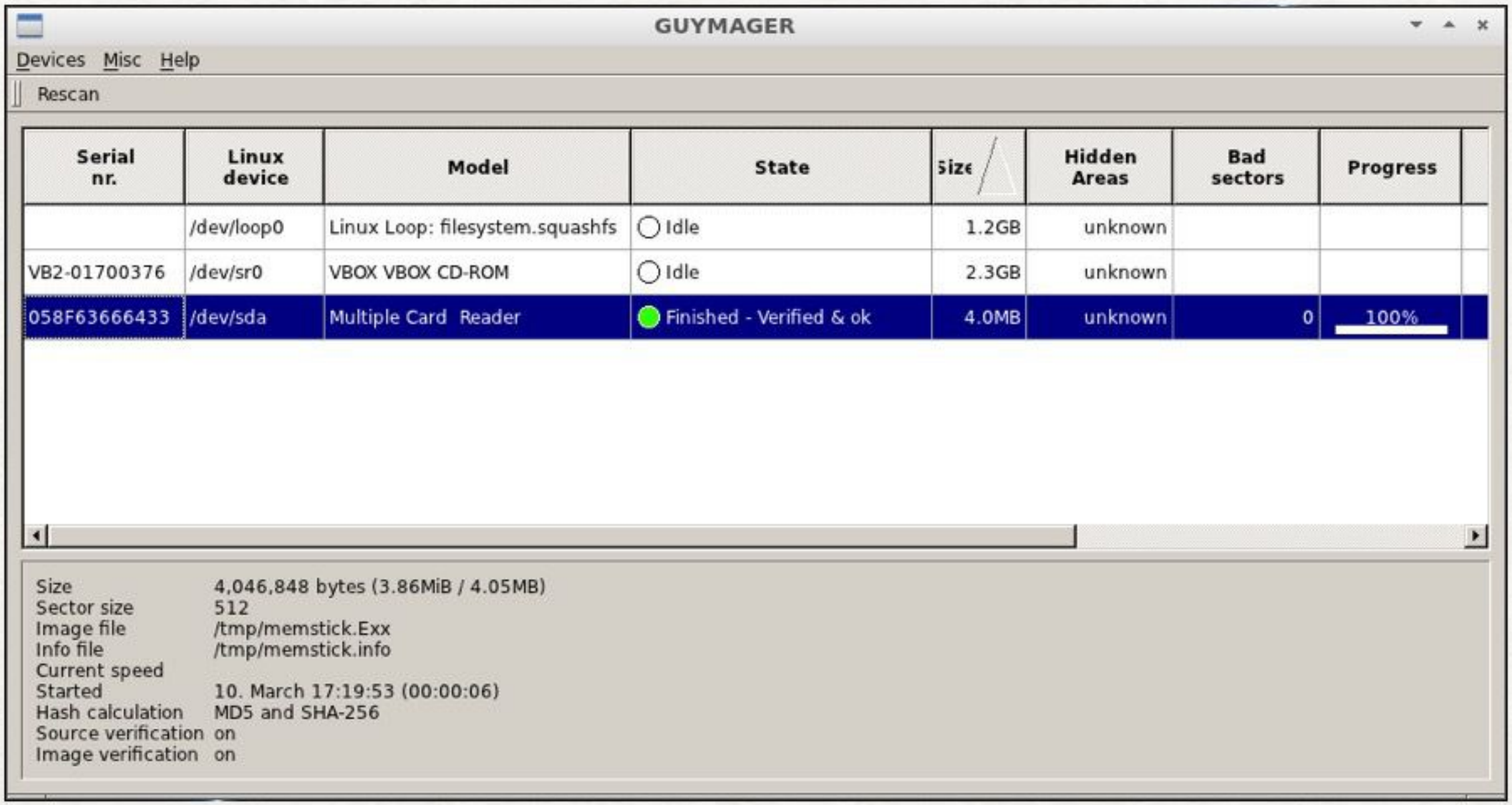
ACQUISIZIONE DI MEMORIE DI MASSA

GUYMAGER



ACQUISIZIONE DI MEMORIE DI MASSA

GUYMAGER



ACQUISIZIONE DI MEMORIE DI MASSA

COPIA LOGICA

- Oltre alla copia dell'intero dispositivo, potrebbe essere necessario eseguire una copia parziale, magari limitata ad alcuni file, cartelle o porzioni di quest'ultime

- Le funzioni di copia standard dei sistemi operativi non danno sufficienti garanzie (conservazione dei metadati, verifica di integrità, log dell'acquisizione, ecc.)

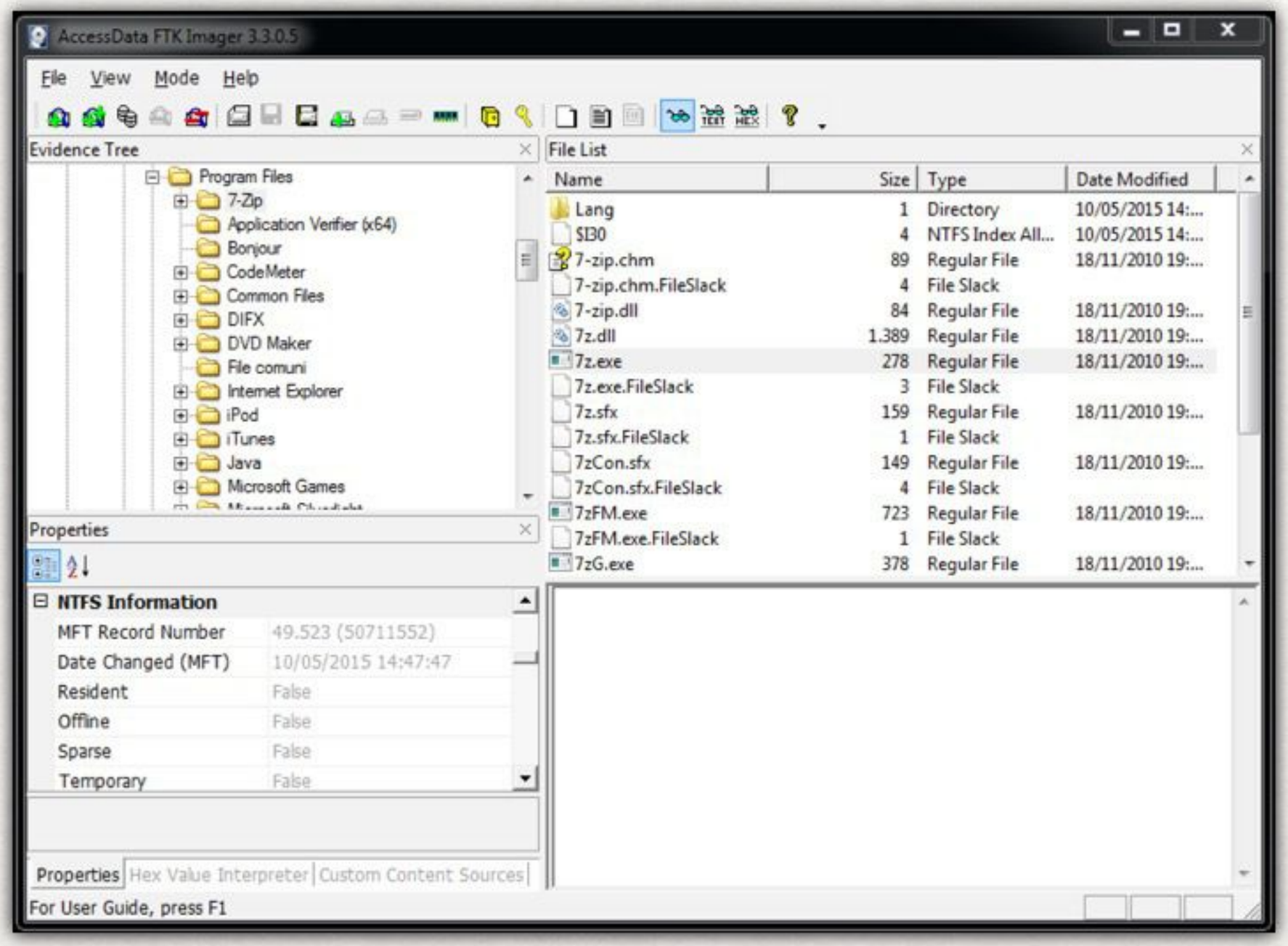
ACQUISIZIONE DI MEMORIE DI MASSA

COPIA LOGICA DA LINUX

- Nell'esempio seguente, il contenuto della cartella /var [illegible] un disco in esame (montato in /mnt/origine) viene copiato [illegible]lla di destinazione /mnt/evidence
- Prima di calcolano gli hash originali:
- # find /mnt/origine/var/log -type f -exec sha1sum {} + > /mnt/evidence/var_log.sha1
- Poi si copiano i file all'interno di un unico archivio compresso, in modo da preservarne gli attributi:
  # tar -czpvf /mnt/evidence/var_log.tgz /mnt/origine/var/log
  Avere come risultato dell'acquisizione un unico file agevola tutti i trasferimenti e le manipolazioni successive. Consente p.e. di calcolare un unico hash da riportare a verbale
- # sha1sum /mnt/evidence/var_log.tgz > /mnt/evidence/var_log.tgz.sha1
- Infine si possono salvare altre informazioni utili alla documentazione, come ad esempio il log dei comandi eseguiti: # history > /mnt/evidence/history.log

ACQUISIZIONE DI MEMORIE DI MASSA

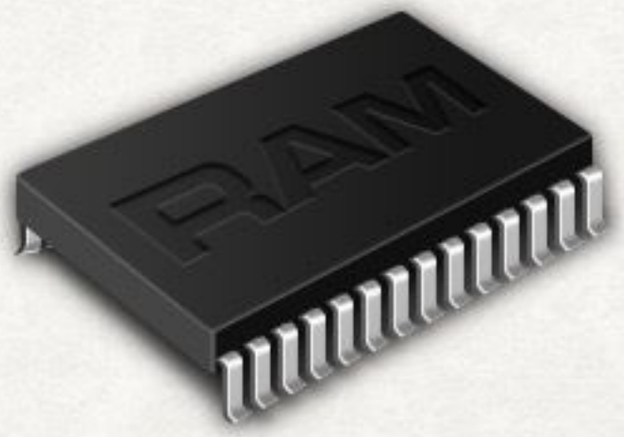
COPIA LOGICA TRAMITE FTK IMAGER



ACQUISIZIONE DI MEMORIA VOLATILE

RAM

- La RAM (Random Access Memory) è una memoria di tipo volatile, che permettere l'accesso diretto a qualunque indirizzo di memoria con lo stesso tempo di accesso.
- I dati vanno persi allo spegnimento del dispositivo
- L'acquisizione della RAM va fatta a sistema acceso



ACQUISIZIONE DI MEMORIA VOLATILE

QUANDO È UTILE ACQUISIRE LA RAM?

- Recuperare password o informazioni presenti in memoria (Es. quando sono attivi software di cifratura)
- Per tenere traccia dei processi attivi ed analizzarli successivamente
- Per recuperare informazioni da quei software che sono stati creati con lo scopo di non lasciare tracce o almeno il meno possibile
- Nel caso di analisi malware e rootkit

ACQUISIZIONE DI MEMORIA VOLATILE

PRECAUZIONI

- Eseguire i tool di acquisizione da dispositivo esterno (pendrive USB, DVD)
- Se devo dumpare la RAM di una VM posso fare: snapshot, pause, clone
- Salvare il dump su pendrive esterno, su hard disk USB, via rete, ecc. ma **NON** sul disco locale

ACQUISIZIONE DI MEMORIA VOLATILE

SOFTWARE PER ACQUISIRE/ANALIZZARE LA RAM

- Volatility
- Rekall
- Mandiant Memoryze
- AccessData FTK Imager
- Windows Memory Reader
- Mac Memory Reader
- MoonSols Windows Memory Toolkit
- Belcasoft RAM capture
- Fmem (Linux)
- e altri ancora…

ACQUISIZIONE DI MEMORIA VOLATILE

VOLATILITY

Volatility è un software open source multi piattaforma (Windows, Linux, Mac) che consente di effettuare analisi delle RAM dumpata.

Il vantaggio di questo software è che è "modulare" ovvero espandibile tramite l'ausilio di plugin che variano in base all'evenienza.

Periodicamente vengono rilasciati diversi plugin che ci vengono incontro per le evenienze più disparate.

ACQUISIZIONE DI MEMORIA VOLATILE

VOLATILITY

Per verificare il sistema di provenienza della nostra acquisizione di memoria, utilizziamo il comando:

```
vol.py -f win-mem-image.bin imageinfo
```

Questo ci serve per poter essere utilizzato come profilo durante l'analisi per esecuzione dei vari plugin

ACQUISIZIONE DI MEMORIA VOLATILE

VOLATILITY

```
vol.py [comando] -f win-mem-image.bin --profile=WinXPSP3x86
```

Alcuni comandi supportati da volatility:

- **connscan** Scansiona oggetti di connessione
- **files** Elenca file aperti
- **imagecopy** Converte il file di ibernazione (hiberfil.sys)
- **procdump** Fa il dump dei processi
- **pslist** Elenca processi in esecuzione
- **sockscan** Scansiona oggetti sul socket
- **screenshot** Salva dei pseudo screenshot del desktop

CENNI SU ACQUISIZIONE DI SMARTPHONE

MEDOTOLOGIE DI ACQUISIZIONE

- Logica
- Filesystem
- Fisica
- Chip-off

CENNI SU ACQUISIZIONE DI SMARTPHONE

MEDOTOLOGIE DI ACQUISIZIONE

Logica

- Accesso diretto ai “record” memorizzati dal telefono all’interno delle diverse aree di interesse (es. Rubrica, messaggi, registro chiamate, ecc.)
- Problemi di accesso con passcode
- Metodo veloce

CENNI SU ACQUISIZIONE DI SMARTPHONE

MEDOTOLOGIE DI ACQUISIZIONE

Filesystem

- Copia dei file del file system
- Recupero di maggiori informazioni
- Possibilità di recuperare record cancellati all'interno di file (es. SQLite deleted records, thumbnails)
- Problemi di accesso con passcode
- Richiede più tempo

CENNI SU ACQUISIZIONE DI SMARTPHONE

MEDOTOLOGIE DI ACQUISIZIONE

Fisica

- Copia bit-a-bit del dispositivo
- Possibilità di superare i blocchi con il codice
- Possibilità di recuperare record e interi file cancellati

CENNI SU ACQUISIZIONE DI SMARTPHONE

MEDOTOLOGIE DI ACQUISIZIONE

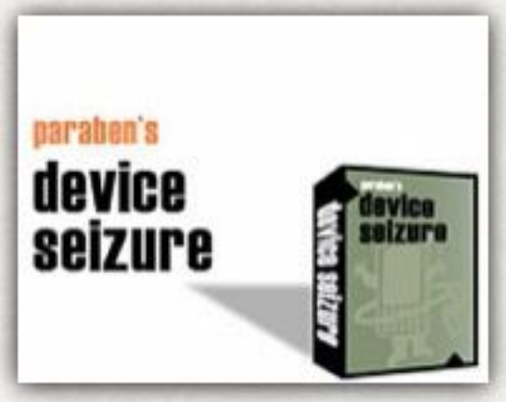
Chip-off

- Distruttiva e rischiosa
- Intero dump del chip di memoria
- Estrazione di tutti i files e cartelle
- E’ possibile fare carving

CENNI SU ACQUISIZIONE DI SMARTPHONE

STRUMENTI DI ACQUISIZIONE

Strumenti commerciali



CENNI SU ACQUISIZIONE DI SMARTPHONE

STRUMENTI DI ACQUISIZIONE
Strumenti di backup

CENNI SU ACQUISIZIONE DI SMARTPHONE

STRUMENTI DI ACQUISIZIONE

Strumenti open

- ADB
- libidevicemobile
- Bitpim
- iPBA 2 (iPhone Backup Analyzer)
- Sql Lite database browser
- Bulk extractor
- Strings
- Foremost
- pySIM and TULP2G
- Editor esadecimali come XXD e Ghex2

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 Tsurugi 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

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

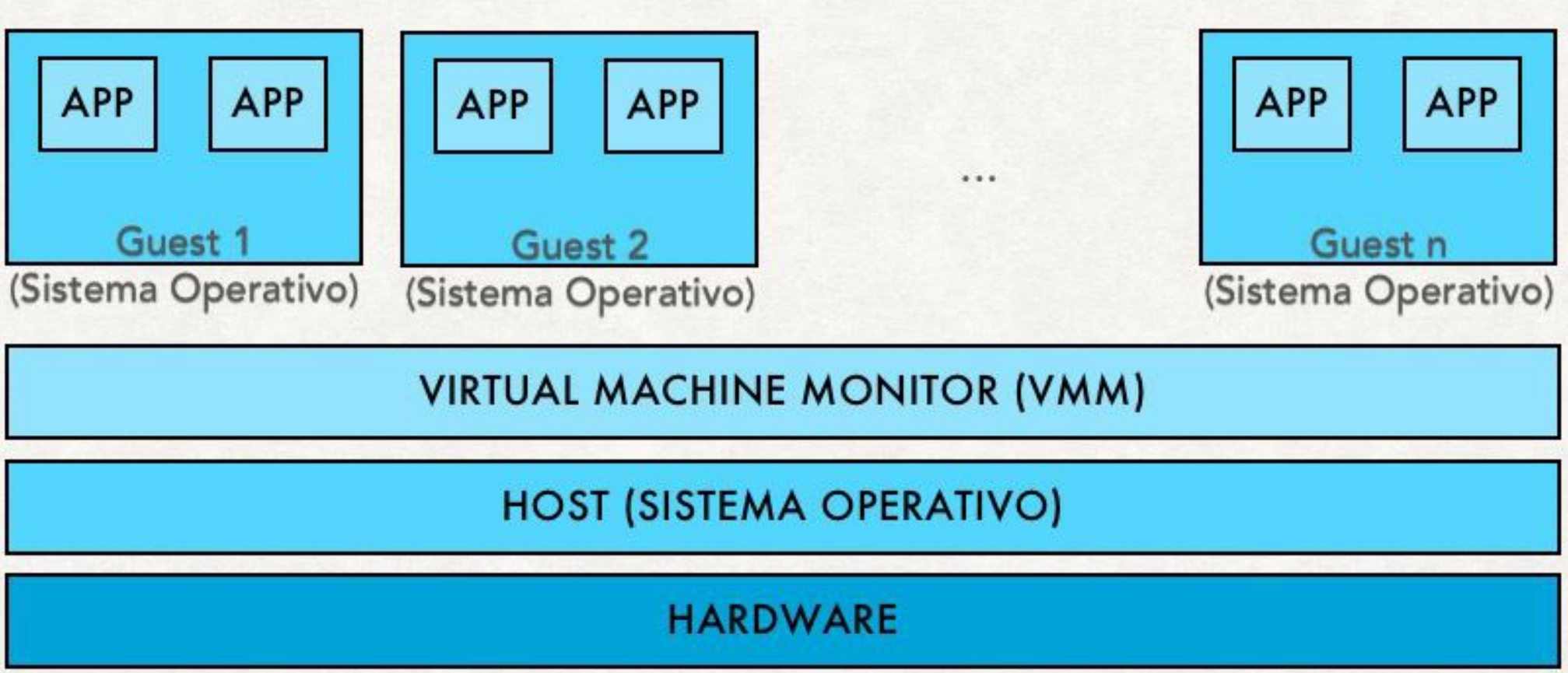
DEFINIZIONE DI VIRTUALIZZAZIONE

- 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 (Tsurugi 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
- 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

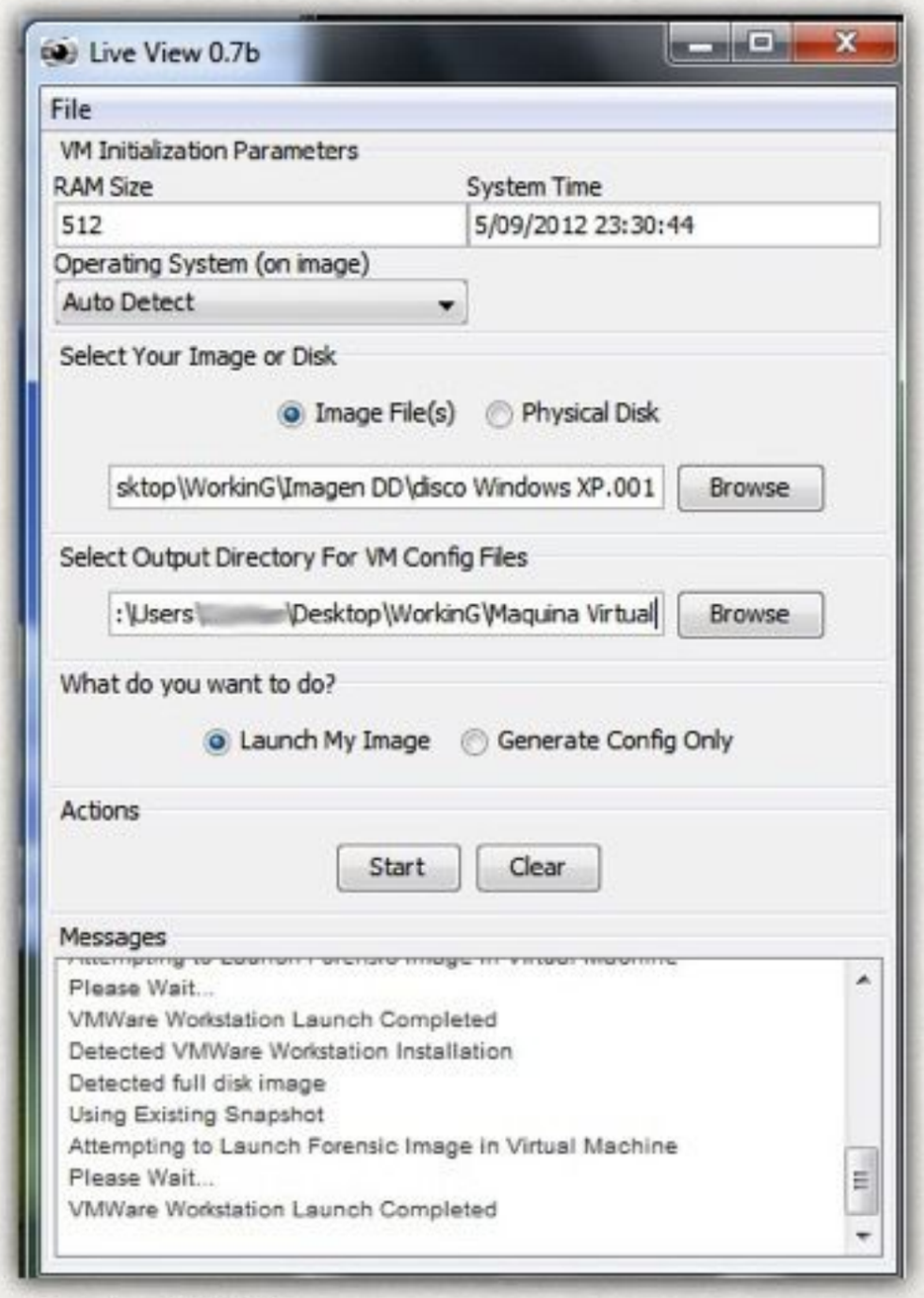
- Sviluppato da Carnegie Mellon University
- Basato su Java, non più aggiornato
- Può virtualizzare:
    - immagini raw di dischi
    - immagini raw di partizioni
    - dischi fisici (connessi via USB o firewire)
    - immagini in formati proprietari (tramite software di terze parti come FTK Imager)
- 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

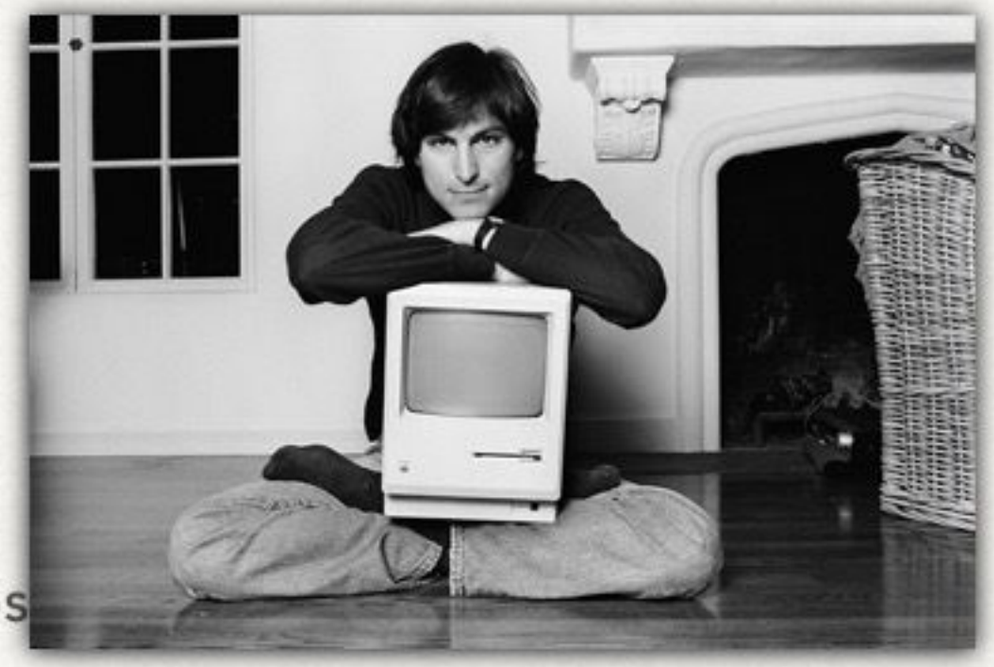
- Patch del registro per abilitare i legacy IDE drivers
- Azzera le password degli utenti (chntpw)
- Rimuove i driver che possono andare in conflitto con l'hw

- 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 pos 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 (Tsurugi)

GUYMAGER

Devices Misc Help

Rescan

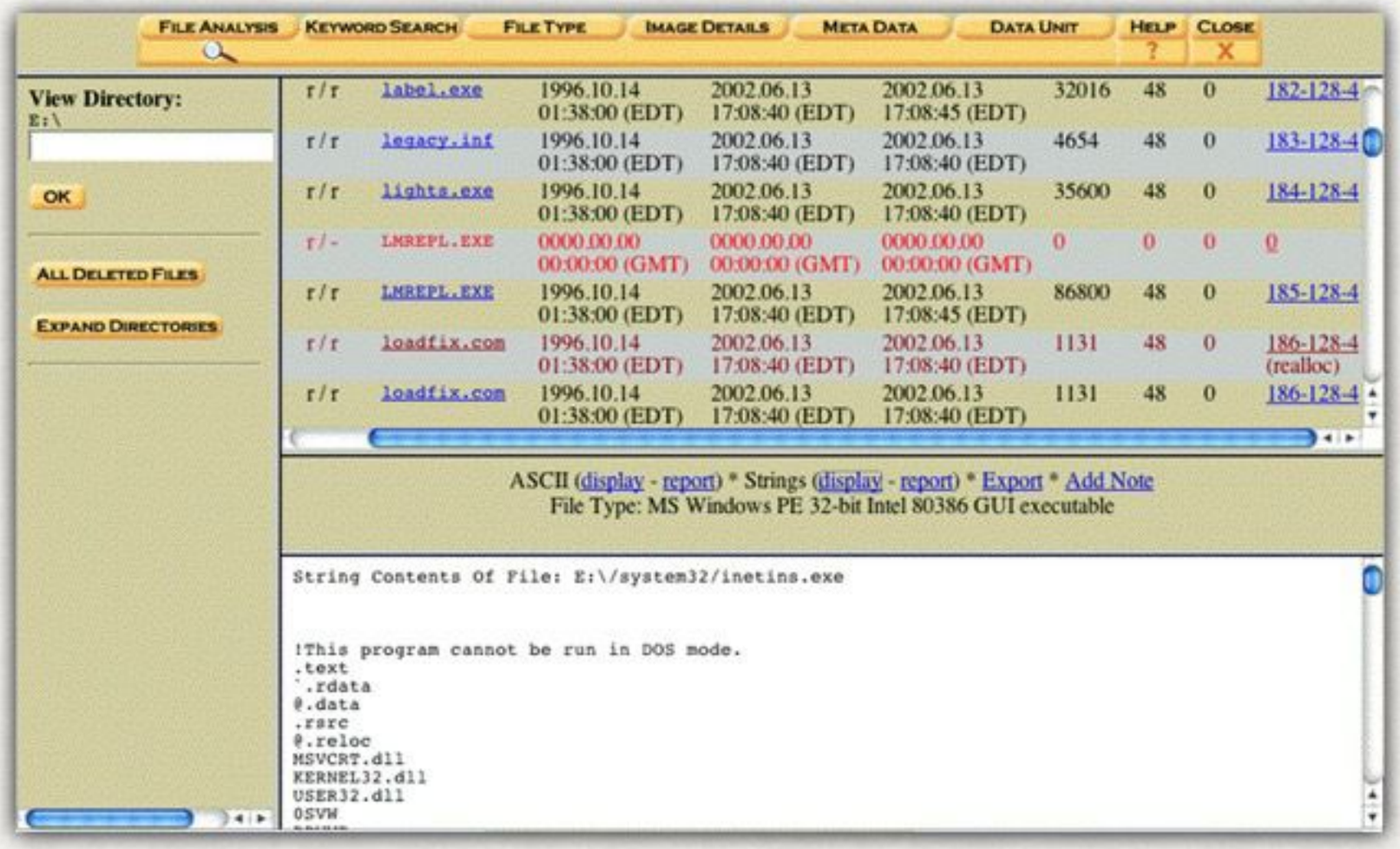
Serial nr.	Linux device	Model	State	Size	Bad sectors	Progress	Average Speed [MB/s]	Time remaining	FIFO queues usage [%]
1ATA_Hitachi_HDP725050GLA360_GEA534RF3Z90WA	/dev/sdd	ATA Hitachi HDP72505	Acquisition running	500.1GB	0	8%	89.73	01:21:17	r 0 c 0 w
1ATA_SAMSUNG_HD322HJ_S17AJ9BQ607434	/dev/sdc	ATA SAMSUNG HD322HJ	Acquisition running	320.1GB	0	12%	80.32	00:55:31	r 100 h 0 c 0 w
Sony_Storage_Media_BC05061400492-0:0	/dev/sde	Sony Storage Media	Finished	1.0GB	0	100%	9.72		
1ATA_MAXTOR_STM3250310AS_6RY761SP	/dev/sda	ATA MAXTOR STM325031	Local device	250.1GB					
1ATA_WDC_WD10EACS-00D6B1_WD-WCAU46176369	/dev/sdb	ATA WDC WD10EACS-00D	Local device	1.0TB					

Size	320,072,933,376 bytes (298GiB / 320GB)
Sector size	512
Image file	/mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.Exx
Info file	/mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.info
Current speed	87.37 MB/s
Started	17. August 10:08:02 (00:07:49)
Hash calculation	on
Source verification	off

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

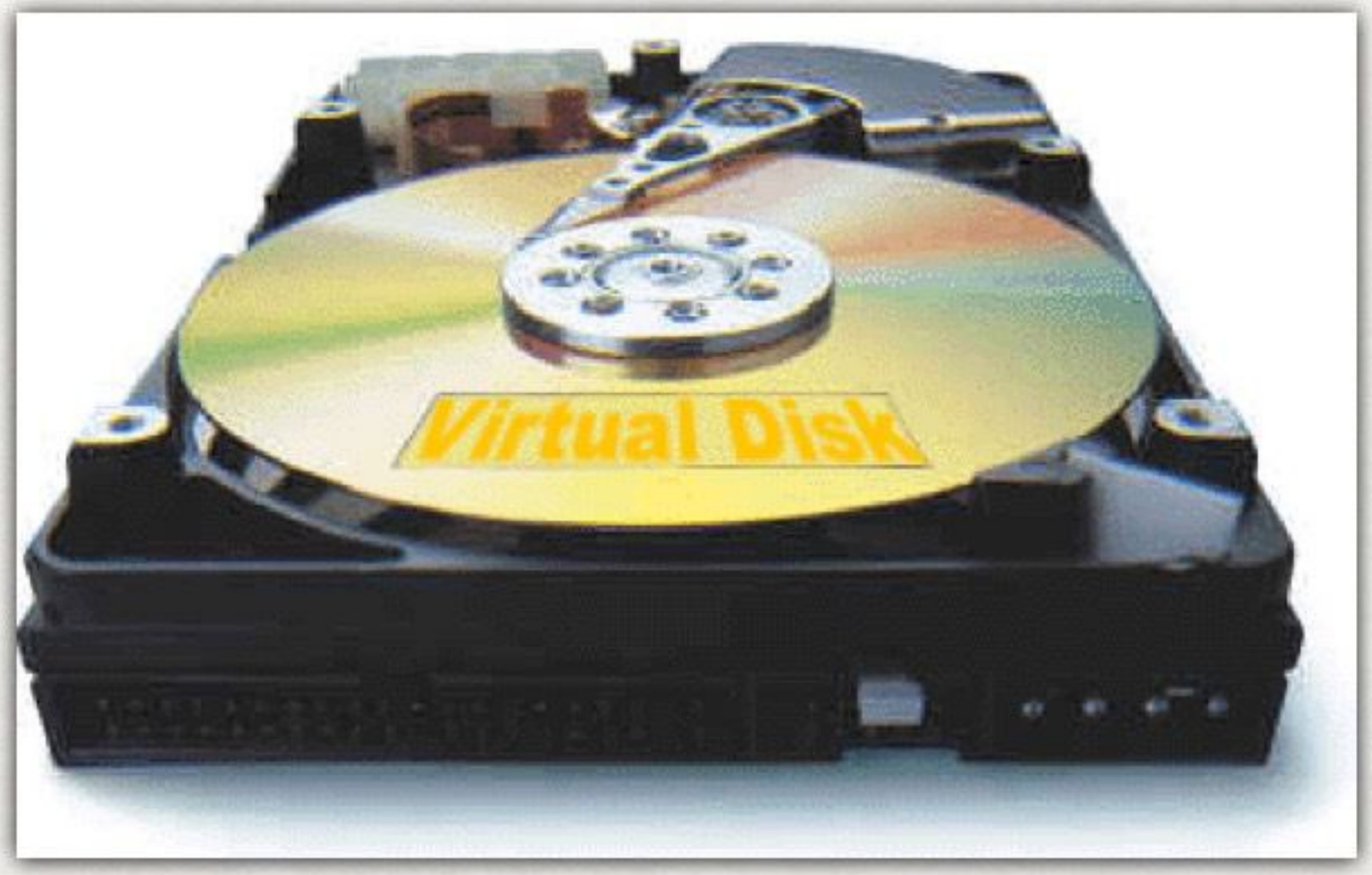
- Verifiche integrità e coerenza dati con ausilio di (super)timeline e log2timeline, TSK o Autopsy (Tsurugi)



VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

- Virtualizzazione disco tramite Live View oppure dd2vmdk o raw2vmdk (Tsurugi8) o con gli altri metodi descritti



VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

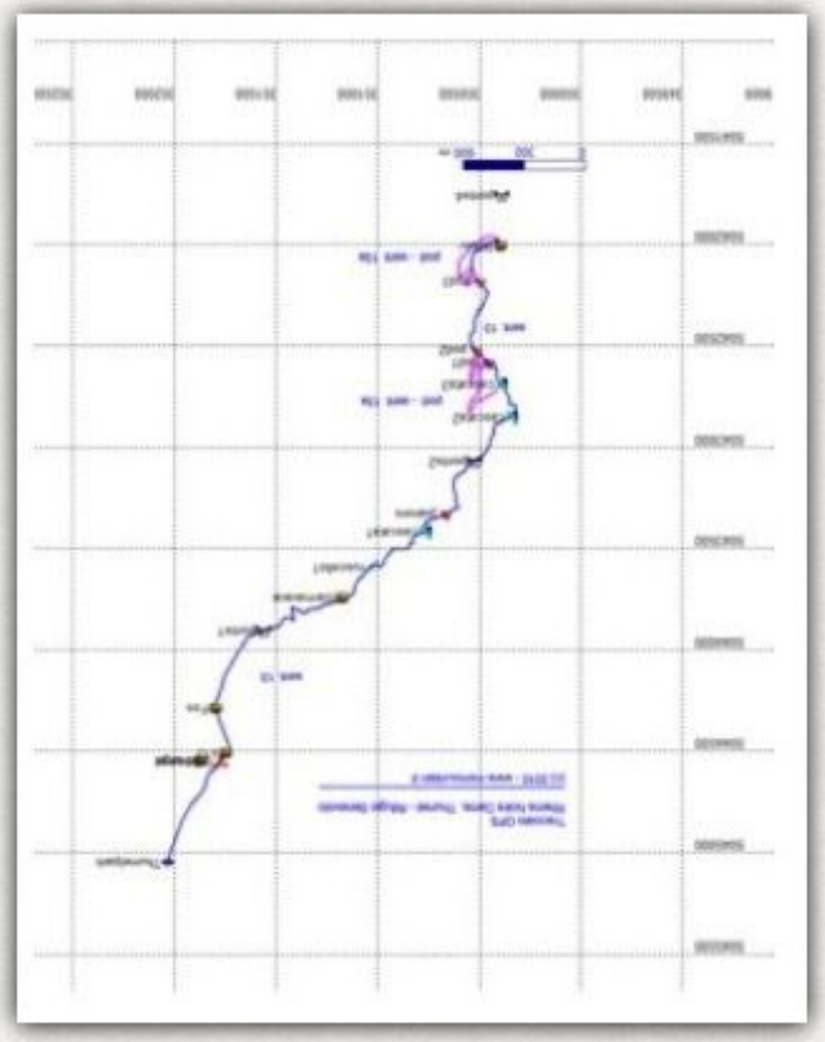
ANALISI DI UNA "SCATOLA NERA"

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

VIRTUALIZZAZIONE DELLE IMMAGINI FORENSI

ANALISI DI UNA "SCATOLA NERA"

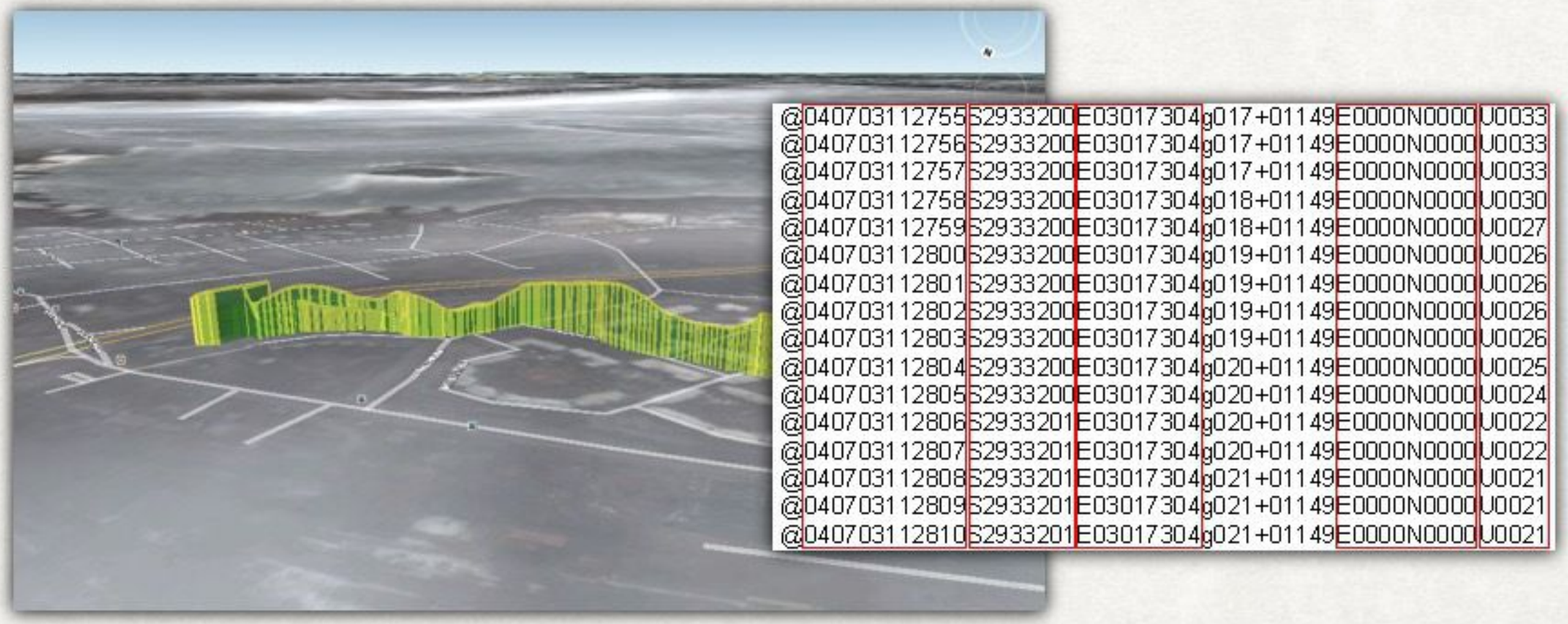
- Elaborazione dei tracciati storici precedenti l'incidente



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

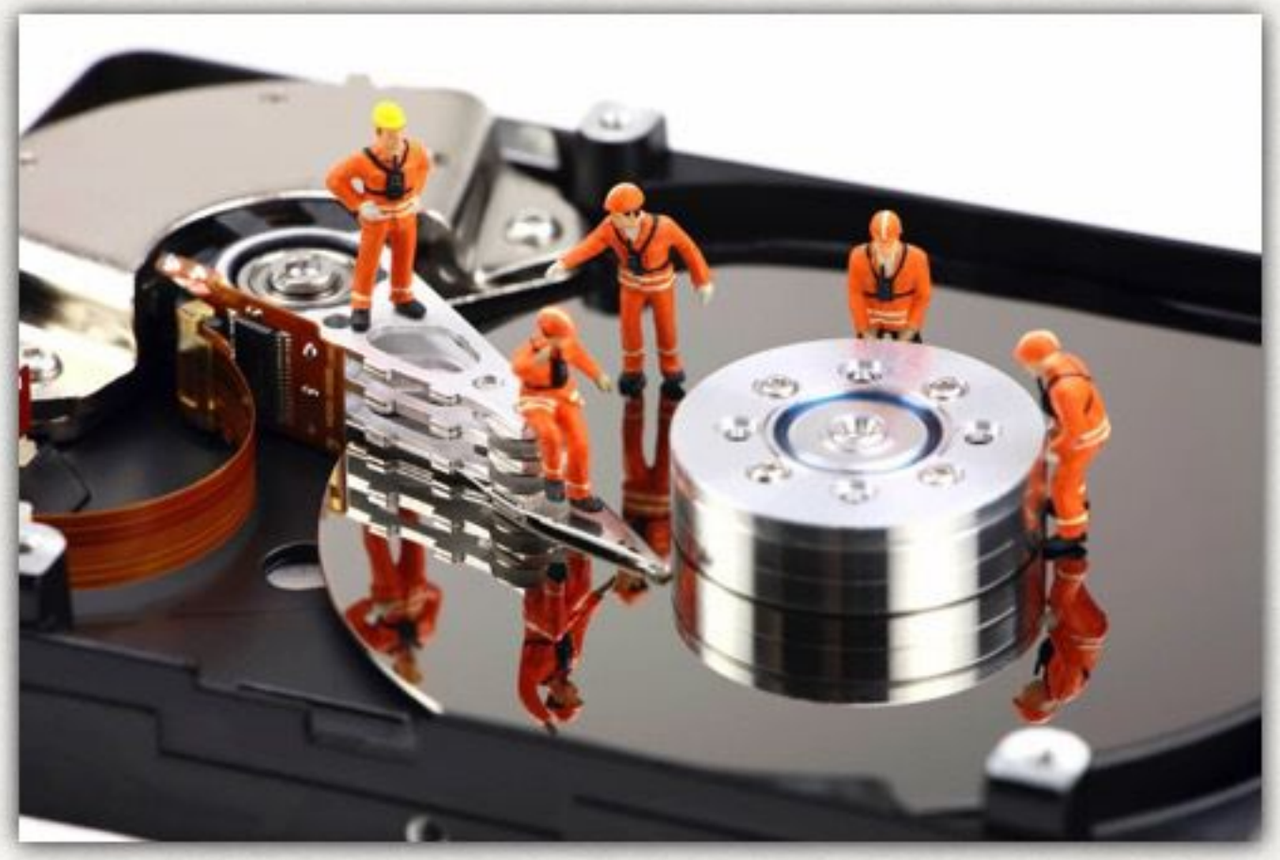
RECUPERO TRAMITE FILE CARVING

- 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

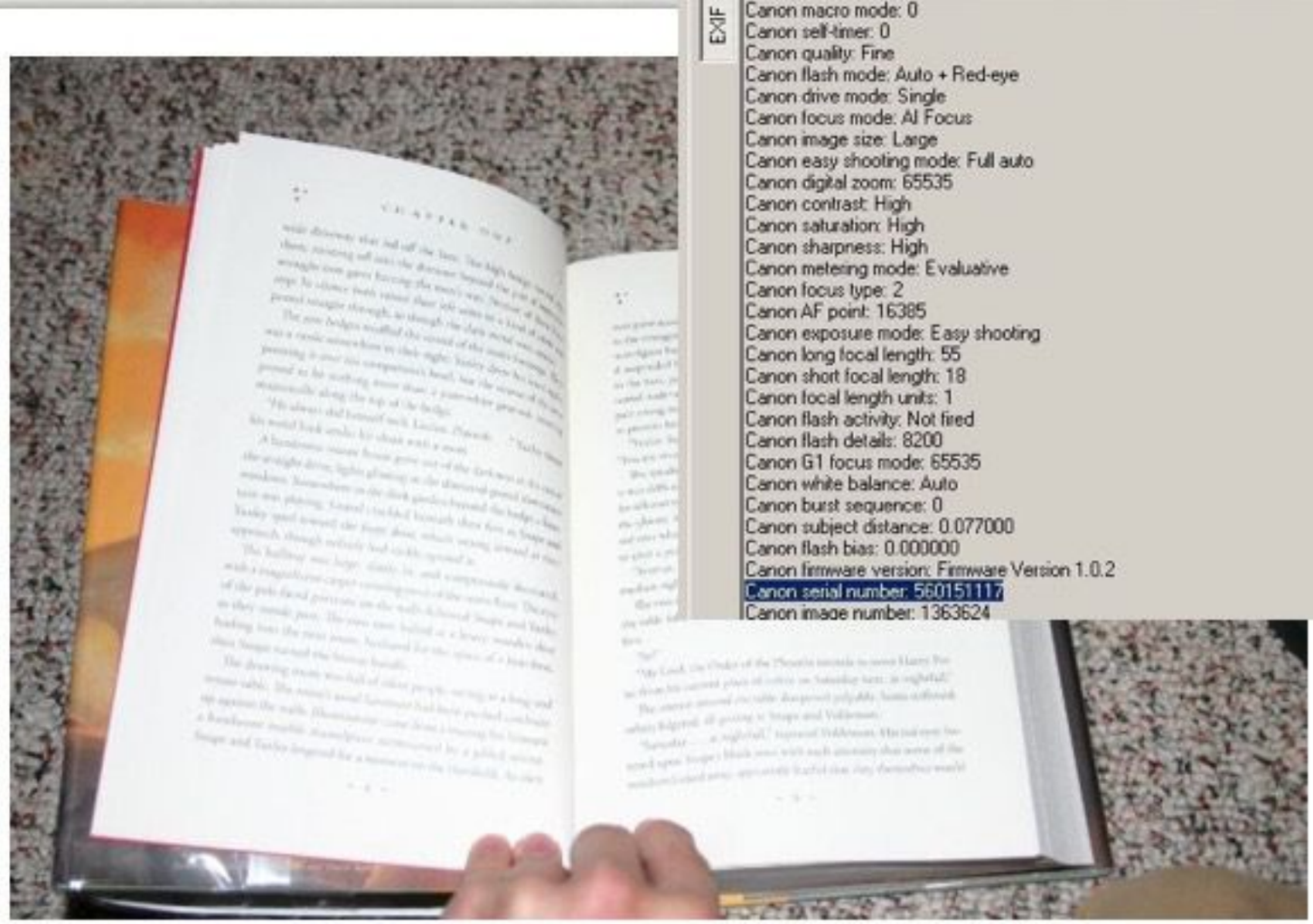
Vediamo qualche esempio di metadati:

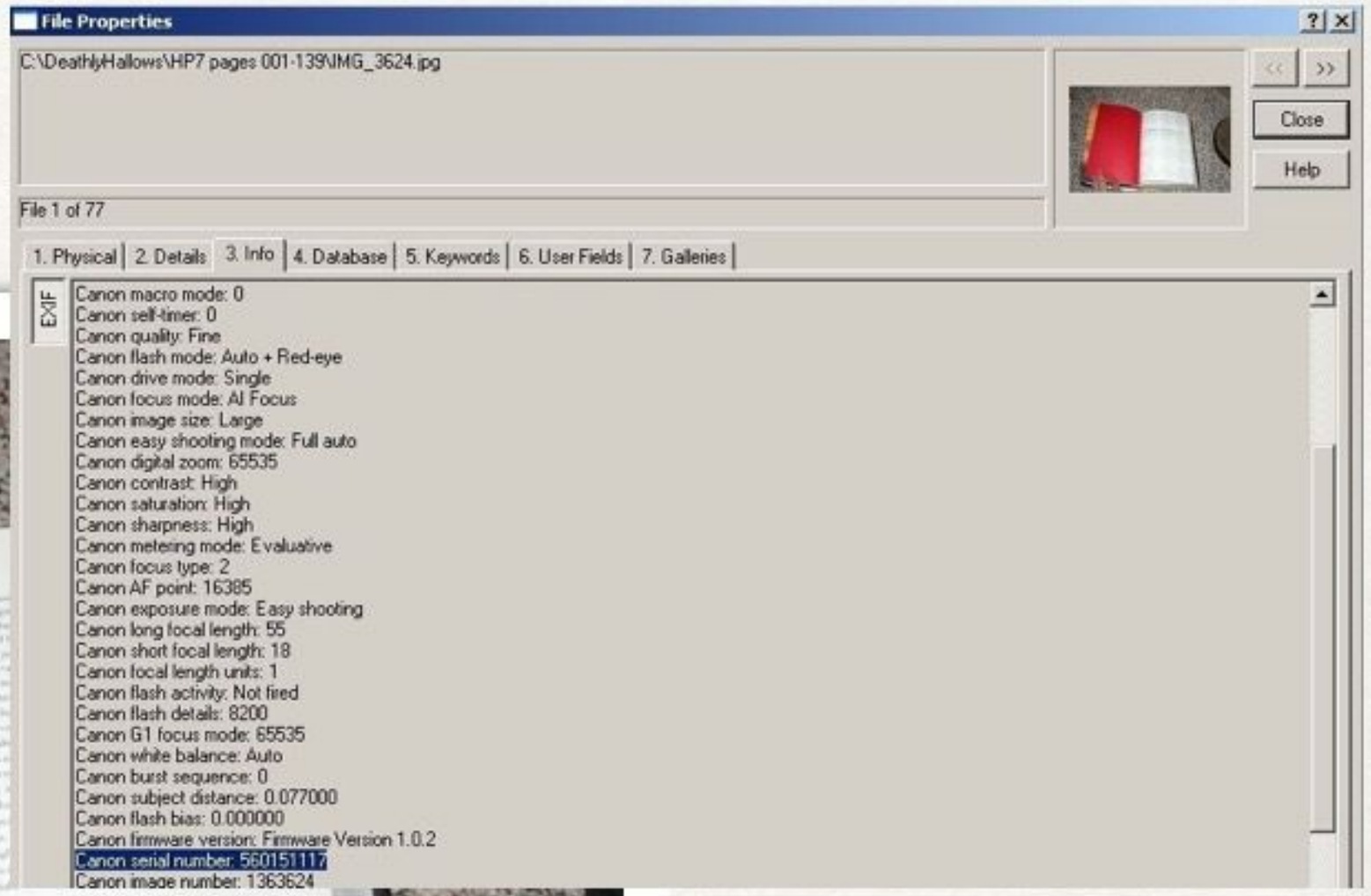
- Metadati nei documenti
- Metadati nelle immagini

METADATA DELLE IMMAGINI

- Embedded Metadata
  - EXIF data
    - brand, model, numero seriale, firmware version …
    - Timestamp
    - Thumbnail
    - GPS, ecc. ecc.
  - IPTC (International Press Telecommunications Council)
  - XMP (Extensible Metadata Platform)
  - Camera Raw, History Log, DICOM ecc.

EXIF: UN CASO FAMOSO





EXIF TRADITORI

- Cat Schwartz
- &
- PhotoShop "crop"

EXIF TRADITORI: UN ALTRO CASO FAMOSO

Webpage Screenshot

EXIF Data May Have Revealed Location of Fugitive Software Tycoon John McAfee

About Subscribe Contact

Michael Zhang · Dec 03, 2012

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

Here are some **screenshots from regex.info** showing the geotag info baked into the photo:

GPS-encoded location:	15° 39' 29"N, 88° 59' 32"W	Display area:	832 m × 517 m	Click on map to measure distance from GPS-encoded location
Map center:	15° 39' 29"N, 88° 59' 32"W	Distance between:	0 m	

Camera:	Apple iPhone 4S
Lens:	4.3 mm
Exposure:	Auto exposure, Program AE, 1/20 sec, f/2.4, ISO 125

Main image displayed here at 7

/data-may-have-revealed-location-of-fugitive-billionaire-john-mcafee/ Fri Sep 13 2013 00:50:34 GMT+0200 (W. Europe Summer Time)

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.

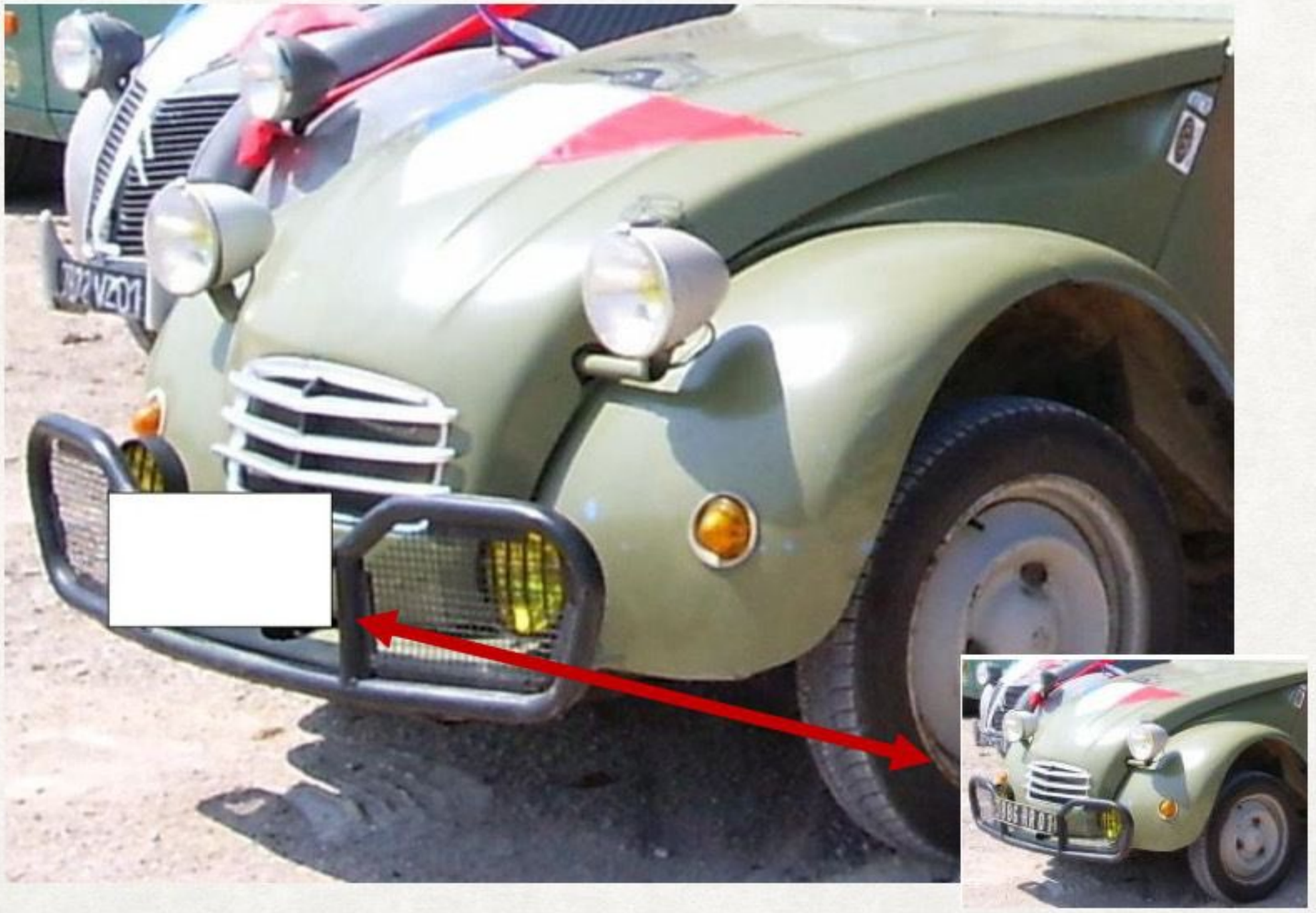

by Declan McCullagh and Greg Sandoval | December 3, 2012 3:52 PM PST

John McA
l' John M
McAfee
GMT+0200

56914-38/mcafee-photo-location-leak-meant-to-mislead-cops/ Fri Sep 13 2013 00:52:06 GMT+0200 (W. Europe Summer Time)

Immagini: www.pcworld.com

THUMBNAIL EXIF



RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

TIMELINE

- Una timeline è una rappresentazione di eventi ordinati cronologicamente
- Gli eventi possono provenire da un'unica fonte o da una più fonti
- Metodo rapido e intuitivo per rendersi conto di quanto è accaduto in un sistema in un determinato arco temporale

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPER TIMELINE

SUPER TIMELINE

- La super timeline si intende la creazione di un file in cui sono memorizzate su scala temporale analogamente a quanto descritto per la timeline tradizionale
- Consente di restituire in risultato molto più esaustivo ed accurato facendo uso dei metadati

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

USI DELLA TIMELINE E SUPER TIMELINE

- Ricostruire le attività di un utente
- Ricostruire le fasi di un attacco o l'analisi di un malware
- Individuare le cause di un incidente informatico
- Evidenziare incongruenze che siano sintomo di attività illecite o tentativi di occultamento tracce
- Per avere una rappresentazione lineare della creazione di file, chiavi di registro, installazione di servizi, ecc.

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

VERIFICA DELLE FONTI TEMPORALI

E' molto importante individuare la fonte dei riferimenti temporali:

- Locale (orologio CMOS)
    - La data locale è corretta?
- Esterna (NTP)
    - Configurazione Timezone
    - Frequenza di aggiornamento
    - Ultimo aggiornamento
- L'applicazione che ha registrato l'evento usa un timestamp particolare?

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

DOVE TROVIAMO I RIFERIMENTI TEMPORALI

- Nel filesystem guardando gli attributi MAC(B) di ogni file e cartella
- File di log e registro eventi del sistema operativo
- Registro di Windows
- Feature proprie del sistema operativo (Prefetch, Restore Points, Link, Cestino, thumbs.db, ShellBag, Volume Shadow Copy)
- Cronologia, Cache e Cookies dei browser
- Cache e database applicativi
- Metadati interni ai documenti (Office, Mail, dati EXIF, ecc.)
- Eventi temporali recuperabili tramite carving da aree deallocate, slack space, dump di memoria, partizioni di swap, file di ibernazione (record $MFT, chiavi di registro, chat, password)

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

MAC(B)

- In un filesystem gli attributi riguardano gli eventi:
  - **M**odified (modifica dei dati)
  - **A**ccessed (lettura dei dati)
  - **C**hanged (modifica dei metadati)
  - **B**irth (creazione del file)
- Non tutti i filesystem registrano le stesse informazioni
- Non tutti i sistemi operativi sfruttano le possibilità del filesystem

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

Significato degli attributi MAC(B) per i vari filesystem:

Tipo FS	Modified	Accessed	Changed	Birth
Ext2/3	Modified	Accessed	Changed	-
Ext4	Modified	Accessed	Changed	Created
FAT	Written	Accessed	N/A	Created
NTFS	File Modified	Accessed	MFT Modified	Created
HFS	Modified	Accessed	Changed	-

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

FILESYSEM E OS

- **FAT** registra gli attributi MAC in localtime
- **NTFS** registra 2 serie di attributi MACB in UTC
- In Windows l'aggiornamento dell'attributo **Access** è gestito tramite la chiave di registro:
  - **HKLM\SYSTEM\CurrentSet\Control\FileSystem\NtfsDisableLastAccessUpdate**
    Il valore **1**: aggiornamento del tempo di accesso è disattivato (default da Win Vista +)
    Il valore **0**: aggiornamento del tempo di accesso è attivato (default Win XP e prec.)
- Linux registra in **Unix time** (secondi trascorsi dal 1/1/1970 00:00:00 UTC) gli attributi MAC su Ext2/3. Con l'avvento di Ext4 viene introdotto l'attributo **Birth**
- In Linux l'aggiornamento degli attributi può essere inibito in fase di mount (**noatime**)
- HFS+ registra i secondi trascorsi da 1/1/1904 00:00:00 GMT

WINDOWS: ACCESS TIME DISABILITATO

Quando disabilitato, l'attributo di **Accesso**, viene solitamente inizializzato alla data in cui il file è stato scritto sul disco, seguendo le regole indicate in tabella:

Condizione	Modified	Accessed	Changed
Rinomina file	Attrib. conservato	Attrib. conservato	Attrib. conservato
Spostamento file tra cartelle	Attrib. conservato	Attrib. conservato	Attrib. conservato
Spostamento di file tra partizioni o dischi	Attrib. conservato	Data spostamento	Attrib. conservato
Copia file	Attrib. conservato	Data copia	Data copia
Creazione nuovo file	Data creazione	Data creazione	Data creazione
Modifica file esistente	Data modifica	Attrib. conservato	Attrib. conservato
Accesso file esisitente	Attrib. conservato	Aggiornato entro un'ora se abilitato, altrimenti conservato	Attrib. conservato

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

Le regole sulla modifica o preservazione dei timestamp nel casi di copia e spostamento di file che risiedono su filesystem **FAT** e **NTFS** sono riportate alla seguente pagina web:

http://support.microsoft.com/kb/299648/en-us

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ATTENZIONE

Singole applicazioni possono adottare timestamp alternativi:

- Nel registro di Windows, i valori FILETIME riportano il numero di intervalli da 100 nanosecondi trascorsi dal 1/1/1601 00:00:00 UTC

- da Mac OS X v10 le applicazioni (es. Safari) possono usare il Mac Absolute Time, o CFDate: secondi trascorsi dal 1/1/2001 00:00:00 GMT

Pertanto è necessario verificare ogni fonte e uniformare tra loro i diversi timestamp

UNIFORMARE I TIMESTAMP

- Conversione del fuso orario
- Compensazione eventuali discrepanze temporali
- Normalizzazione del formato data-ora
- Ricorso a formati standardizzati:
  - Body file
  - TLN

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

INFORMAZIONI DAL REGISTRO

Prima di procedere con la creazione della (super)timeline possiamo estrarre alcune informazioni utili dal registro di sistema:

- Versione del sistema operativo
- Time zone

Per recuperare queste informazioni, dopo aver montato in R/O il disco, facciamo uso del tool registry ripper presente in Tsurugi:

```
# cd /opt/regripper
# rip -r /mnt/C/Windows/system32/config/software -p winver
# rip -r /mnt/C/Windows/system32/config/system -p timezone
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

STRUMENTI

- Useremo i tool fls/mactime della suite TSK, The Sleuth Kit e log2timeline.
- Esistono diverse alternative, più o meno scomode, open/gratuite/commerciali
- fls è la più usata, anche perchè utilizzata dal frontend Autopsy

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

STRUMENTI ALTERNATIVI MA SCOMODI

- FTK Imager (AccessData)
- NTFSwalk (TzWorks)
- AnalyzeMFT
- mft.pl
- MFTView
- Encase
- X-Ways Forensics

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE TIMELINE CON DAILY SUMMARY

- Suite TSK, con fls credo file in formato bodyfile
- Converto il bodyfile in CSV
- Creo daily summary con attività giornaliera

fls -o 63 -r -m C: /mnt/raw/image.dd > c-timeline.body

mactime -y -m -d -i day c-timeline-daily.csv -z Europe/Rome -b c-timeline.body > c-timeline.csv

oppure

mactime -y -m -d -i hour c-timeline-hourly.csv -z Europe/Rome -b c-timeline.body > c-timeline.csv

CREAZIONE TIMELINE CON DAILY SUMMARY

- Il daily summary serve per rilevare anomalie sui giorni
- Nell'esempio, cominceremo ad esaminare il giorno 4 marzo 2010, dove rileviamo 62.239 movimentazioni di file
- Possibile anche hourly summary, con analisi oraria, nell'esempio rileviamo pesante attività tra le ore 11 e 12

```
Tue 03 02 2010, 6616
Wed 03 03 2010, 3990
Thu 03 04 2010, 62239
Fri 03 05 2010, 315
Sat 03 06 2010, 5
Sun 03 07 2010, 178
```

```
Wed 03 03 2010 17:00:00, 63
Wed 03 03 2010 18:00:00, 94
Thu 03 04 2010 01:00:00, 2
Thu 03 04 2010 02:00:00, 1
Thu 03 04 2010 09:00:00, 294
Thu 03 04 2010 10:00:00, 46
Thu 03 04 2010 11:00:00, 13874
Thu 03 04 2010 12:00:00, 44408
Thu 03 04 2010 13:00:00, 3478
Thu 03 04 2010 16:00:00, 3
Thu 03 04 2010 17:00:00, 98
Thu 03 04 2010 18:00:00, 1
Thu 03 04 2010 19:00:00, 2
Thu 03 04 2010 20:00:00, 3
Thu 03 04 2010 23:00:00, 29
Fri 03 05 2010 01:00:00, 6
Fri 03 05 2010 06:00:00, 1
Fri 03 05 2010 08:00:00, 10
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

CREAZIONE TIMELINE CON DAILY SUMMARY

- Otteniamo (i dati provengono dall'$MFT) data di creazione/accesso/salvataggio/entry modified, dimensione, numero di inode e percorso sul filesystem quando disponibile

- Sappiamo se un file esisteva ma è stato cancellato e in tal caso anche se l'area disco è stata riscritta

```
2004 08 04 Wed 05:00:00,629,m..b,r/rrwxrwxrwx,0,0,1010-128-1,"C:/WINDOWS/inf/minioc.inf"
2004 08 04 Wed 05:00:00,1688,m...,r/rrwxrwxrwx,0,0,10109-128-3,"C:/WINDOWS/repair/autoexec.nt"
2004 08 04 Wed 05:00:00,673088,m..b,r/rrwxrwxrwx,0,0,1011-128-3,"C:/WINDOWS/system32/mlang.dat"
2004 08 04 Wed 05:00:00,3584,m..b,r/rrwxrwxrwx,0,0,1012-128-3,"C:/WINDOWS/system32/mll_hp.dll"
2004 08 04 Wed 05:00:00,7680,m..b,r/rrwxrwxrwx,0,0,1013-128-3,"C:/WINDOWS/system32/mll_mtf.dll"
2004 08 04 Wed 05:00:00,5632,m..b,r/rrwxrwxrwx,0,0,1014-128-3,"C:/WINDOWS/system32/mll_qic.dll"
2004 08 04 Wed 05:00:00,17135,m..b,r/rrwxrwxrwx,0,0,1015-128-3,"C:/WINDOWS/Help/mls_trb.chm"
2004 08 04 Wed 05:00:00,37298,m..b,r/rrwxrwxrwx,0,0,1016-128-3,"C:/WINDOWS/Help/mmc_dlg.hlp"
2004 08 04 Wed 05:00:00,1492,m..b,r/rrwxrwxrwx,0,0,1017-128-3,"C:/WINDOWS/system32/mmdriver.inf"
.
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESPORTO $MFT PER L'ANALISI LABORATORIO

- Utile se non si ha tempo di fare timeline/supertimeline
- log2timeline lo elabora in automatico
- Si può elaborare in laboratorio con diversi tool, compreso log2timeline
- Se non si ha tempo di usare fls/autopsy, acquisire MFT e parsificare in laboratorio

```
cat -c /mnt/c/\$MFT > mft.bin
(oppure)
icat -o 63 /dev/sda 0 > mft.bin
```

ESPORTAZIONE DEL JOURNAL NTFS

- Se il journaling è attivo, il file contiene timestamp di creazione, modifica e cancellazione dei file presenti sul disco
- Si può elaborare in laboratorio con diversi tool, commerciali e non e integrare tramite apposito plugin nella super timeline

```
cat /mnt/c/\$Extend/\$UsnJrnl:\$J > usnjrnl.bin
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

INTEGRAZIONE DI FILE RECUPERATI NELLA SUPERTIMELINE

- Prassi poco nota ma dagli ottimi risultati
- Estrarre tramite carving e applicare log2timeline su quanto ricuperato
- Verranno parsificati registro, eventi, immagini, documenti, link, navigazione Internet e molti altri metadati che altrimenti non sarebbero stati inclusi nella supertimeline

```
log2timeline -r -z Europe/Rome ./carving -m C: -w c-log2t-carve.csv
cat *.csv > supertimeline-unsorted.csv
l2t_process -i -b supertimeline-unsorted.csv -y > supertimeline.csv
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESEMPIO: NAVIGAZIONE WEB

- 10/20/2014,15:42:24,PST8PDT,.ACB,WEBHIST,**Internet Explorer**,time1,Administrator,-,visited http://www.google.com/search?hl=en&**q=pidgin**&aq=f [...]

- 10/20/2014,15:42:55,PST8PDT,M...,WEBHIST,**Internet Explorer**,time2,Administrator,-,visited http://sourceforge.net/project/downloading.php?groupname=pidgin&filename=**pidgin-2.5.2.exe**&use_mirror=internap [...]

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESEMPIO: FILESYSTEM

- 10/21/2014,11:13:04,PST8PDT,.A..,FILE,NTFS $MFT,$FN [.**A**..] time,-,-,C:/Documents and Settings/All Users/Documents/**pidgin-2.5.2.exe** [...]

- 10/21/2014,11:04:08,PST8PDT,.A..,FILE,NTFS $MFT,$FN [.**A**..] time,-,-,C:/Documents and Settings/All Users/Documents/**Thunderbird Setup 2.0.0.17.exe** [...]

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESEMPIO: ESECUZIONE PROGRAMMI

- 10/29/2014,19:44:34,,MACB,REG,UserAssist key,Time of Launch,domex2,REALISTIC_XP,UEME_RUNPATH:C:/Program Files/Mozilla Thunderbird/**thunderbird.exe**, [**Count: 2**] [...]

- 10/30/2014,00:50:43,PST8PDT,MACB,PRE,XP Prefetch,Last run,-,REALISTIC_XP,AIM6.EXE-34DC5725.pf: AIM6.EXE was executed,**AIM6.EXE-34DC5725.pf** - [AIM6.EXE] was executed - run **count [5]** [...]

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESEMPIO: AVVIO E SPEGNIMENTO PC

- 10/29/2014,19:44:34,,MACB,REG,UserAssist key,Time of Launch,domex2,REALISTIC_XP,UEME_RUNPATH:C:/Program Files/Mozilla Thunderbird/**thunderbird.exe**, [**Count: 2**] [...]

- 10/30/2014,00:50:43,PST8PDT,MACB,PRE,XP Prefetch,Last run,-,REALISTIC_XP,AIM6.EXE-34DC5725.pf: AIM6.EXE was executed,**AIM6.EXE-34DC5725.pf** - [AIM6.EXE] was executed - run **count [5]** [...]

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ESEMPIO: AVVIO E SPEGNIMENTO PC

```
03/16/2010,07:42:40,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6009;Info;5.01. - 2600 - Service Pack 3 - Uniprocessor Free,EventLog/6009;Info;5.01. -
2600 - Service Pack 3 - Uniprocessor Free,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,
3266,URL: http://eventid.net/display.asp?eventid=6009&source=EventLog,Log2t::input::evt,u
id: unknown size: 524288
03/16/2010,07:42:40,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6005;Info;,EventLog/6005;Info;,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,3266,URL:
 http://eventid.net/display.asp?eventid=6005&source=EventLog,Log2t::input::evt,uid: unkno
wn size: 524288
03/16/2010,10:55:43,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6006;Info;,EventLog/6006;Info;,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,3266,URL:
 http://eventid.net/display.asp?eventid=6006&source=EventLog,Log2t::input::evt,uid: unkno
wn size: 524288
03/16/2010,10:56:53,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6009;Info;5.01. - 2600 - Service Pack 3 - Uniprocessor Free,EventLog/6009;Info;5.01. -
2600 - Service Pack 3 - Uniprocessor Free,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,
3266,URL: http://eventid.net/display.asp?eventid=6009&source=EventLog,Log2t::input::evt,u
id: unknown size: 524288
03/16/2010,10:56:53,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6005;Info;,EventLog/6005;Info;,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,3266,URL:
 http://eventid.net/display.asp?eventid=6005&source=EventLog,Log2t::input::evt,uid: unkno
wn size: 524288
03/16/2010,11:54:36,Europe/Rome,MACB,EVT,Event Log,Time generated/written,-,FRAPC,EventLo
g/6005;Info;,EventLog/6005;Info;,2,/mnt/c/WINDOWS/system32/config//SysEvent.Evt,3266,URL:
 http://eventid.net/display.asp?eventid=6005&source=EventLog,Log2t::input::evt,uid: unkno
wn size: 524288
```

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

ELABORAZIONE TIMELINE SUPER TIMELINE

Una volta creata la (super)timeline, per visionarla, filtrarla o fare ricerche, si consiglia l'uso di un foglio di calcolo o eventualmente un DBMS

RICOSTRUZIONE DELLE ATTIVITÀ TRAMITE TIMELINE E SUPERTIMELINE

POSSIBILI PROBLEMATICHE

- Programmi che eseguono scansioni di file (antivirus, antispyware), software di indicizzazione, deframmentazione, ecc. spesso alterano la data di accesso, rendendo l'informazione poco significativa

- Alcuni antivirus ci vengono incontro a tal proposito (es. "Preserve Filetime" in Norton Anti Virus Corporate)

RILEVAMENTO DI COMPROMISSIONI

Per verificare se un sistema è stato compromesso o se c'è stato un utilizzo non autorizzato, possiamo effettuare questi controlli:

- Creazione (super)timeline
- Registro di sistema
    - Verifica orari accensione/spegnimento del sistema
    - Verifica dei file recenti (recents su filesystem o da registro)
        - Verifica file recenti all'interno delle varie applicazioni
        - Verifica connessione dispositivi USB
        - Verifica comandi eseguiti
- Verifica processi attivi
- Registro eventi
- …

RILEVAMENTO DI COMPROMISSIONI

Una vasta serie di informazioni la possiamo estrarre dal registro di Windows utilizzando **regripper**. Regripper funziona sia in ambiente Linux ma è possibile eseguirlo anche da Windows.

E' un programma che funziona tramite l'ausilio di plugin e di conseguenza le sue potenzialità sono espandibili.

I file di registro che andremo a leggere si trovano in:

- /Users/NOME-Utente/**NTUSER.DAT**
- /Windows/System32/config/**SOFTWARE**
- /Windows/System32/config/**SAM**
- /Windows/System32/config/**SECURITY**
- /Windows/System32/config/**SYSTEM**

RILEVAMENTO DI COMPROMISSIONI

I plugin di regripper sono contenuti all'interno della cartella **plugins** di regripper ed essendo in formato testuale, possono essere letti per avere una descrizione sul plugin e soprattutto per comprendere quale chiave di registro utilizzare come file di input.

ANALISI DELLE PERIFERICHE USB UTILIZZATE

Il collegamento di periferiche USB viene tracciato nel registro di sistema di Windows, pertanto estraiamo tali informazioni tramite regripper:

- **# rip -r /mnt/c/Windows/system32/config/system -p usbstor2**
- PC-402,Disk&Ven_&Prod_USB_DISK&Rev_1.04,**0738015025AC&0**,1127776426,USB DISK USB Device,7&2713a8a1&0,\DosDevices\H:

Dove i vari paramentri sono:

- Nome del sistema
- ID classe dispositivo
- Numero di serie
- Ultima scrittura nel registro (inserimento usb), 'normalizzato' in Unix time
- Nome dispositivo
- ID dispositivo
- Lettera dell'unità

ANALISI DEI DOCUMENTI APERTI E UTILIZZATI

- Per effettuare un controllo sui file aperti di recente, oltre a fare riferimento alle informazioni presenti nel registro di sistema, è possibile analizzare i file nella cartella dei dati recenti.
- Tale cartella contiene dei link ai documenti recenti pertanto utilizzando il software **lnkinfo** (link info), possiamo ottenere informazioni dettagliate relative a quel link.
- Tra queste informazioni ricordiamo:
- Data di creazione
- Data apertura
- Percorso sorgente

ESTRAZIONE DI EVIDENZE TRAMITE BULK EXTRACTOR E AUTOPSY

BULK EXTRACTOR

Bulk Extractor è un software scritto da Simson Garfinkel l'autore di AffLib

- Parsifica il disco a livello raw estraendo:
  - numeri di carte di credito
  - indirizzi
  - telefoni
  - email
  - url
  - ricerche su Google
  - indirizzi IP
  - zip file
  - ecc.

ESTRAZIONE DI EVIDENZE TRAMITE BULK EXTRACTOR E AUTOPSY

AUTOPSY

- Interfaccia grafica alla suite TSK
- Possiamo creare un caso, impostare una timezone, inserire immagini forensi e/o dischi (es. /dev/sda)
- Utile per fare preview di file anche cancellati (ricavati da MFT)
- Utile per fare ricerca di parole chiavi su raw disk, estrazione stringhe, estrazione dello spazio non allocato, organizzazione file per tipo, ricupero di tutti i file cancellati (a livello MFT)
- Preview raw a livello di settore