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 2 GIORNATA

- Tipologie di acquisizione forense e formati
- Attività di preview e triage sicuro con DEFT
- Acquisizione di memorie di massa
- Acquisizione di memoria volatile
- Cenni su acquisizione di smartphone

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 DEFT

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 DEFT

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 ripudiabilitità**
- 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

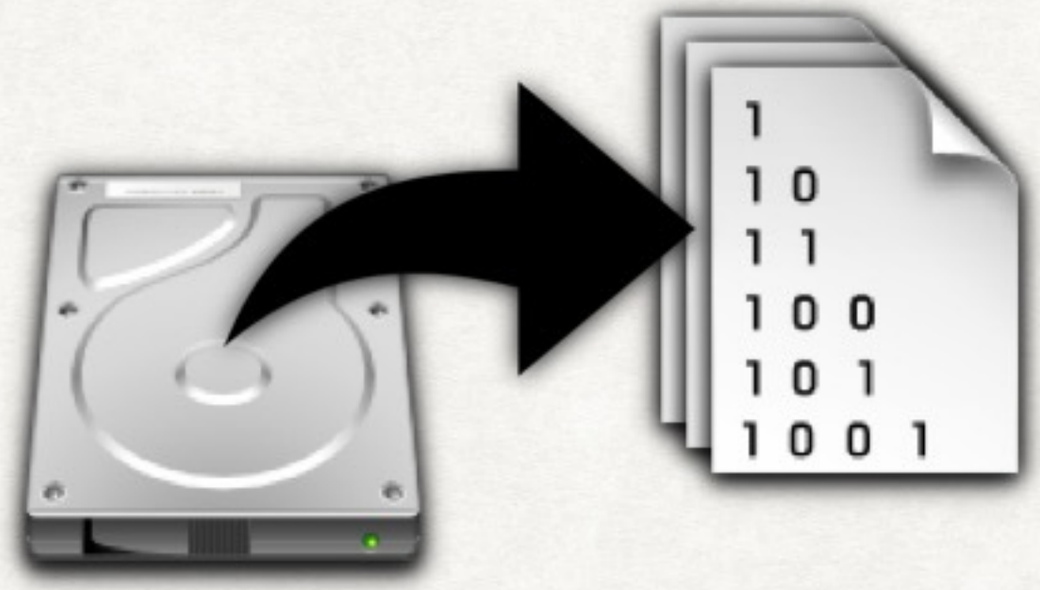
Esistono due modalità di copia forense di un dispositivo:

- 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

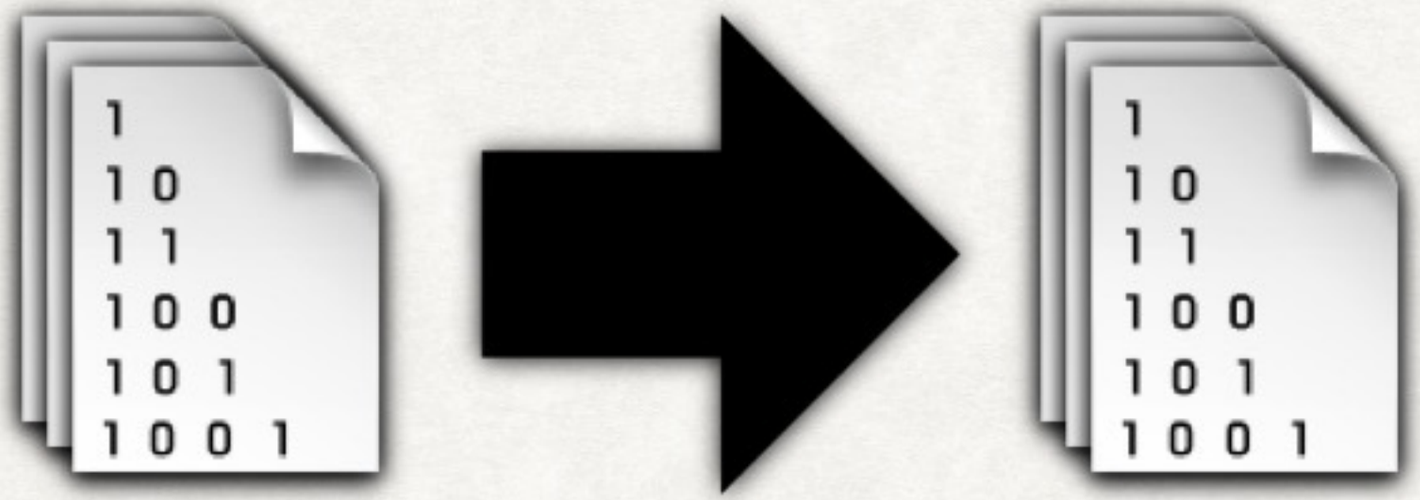
DEVICE TO DEVICE

- Richiede un disco di destinazione di capacità uguale o superiore rispetto all'originale
- Richiede un disco di destinazione ogni disco originale da copiare
- Richiede il wiping dis destinazione (per 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 DEFT
- Workstation dedicata con DEFT installata(laboratorio)

ACQUISIZIONE DI MEMORIE DI MASSA

WRITE BLOCKER

- Esistono write blocker hardware ma se utilizziamo DEFT 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 DEFT, 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

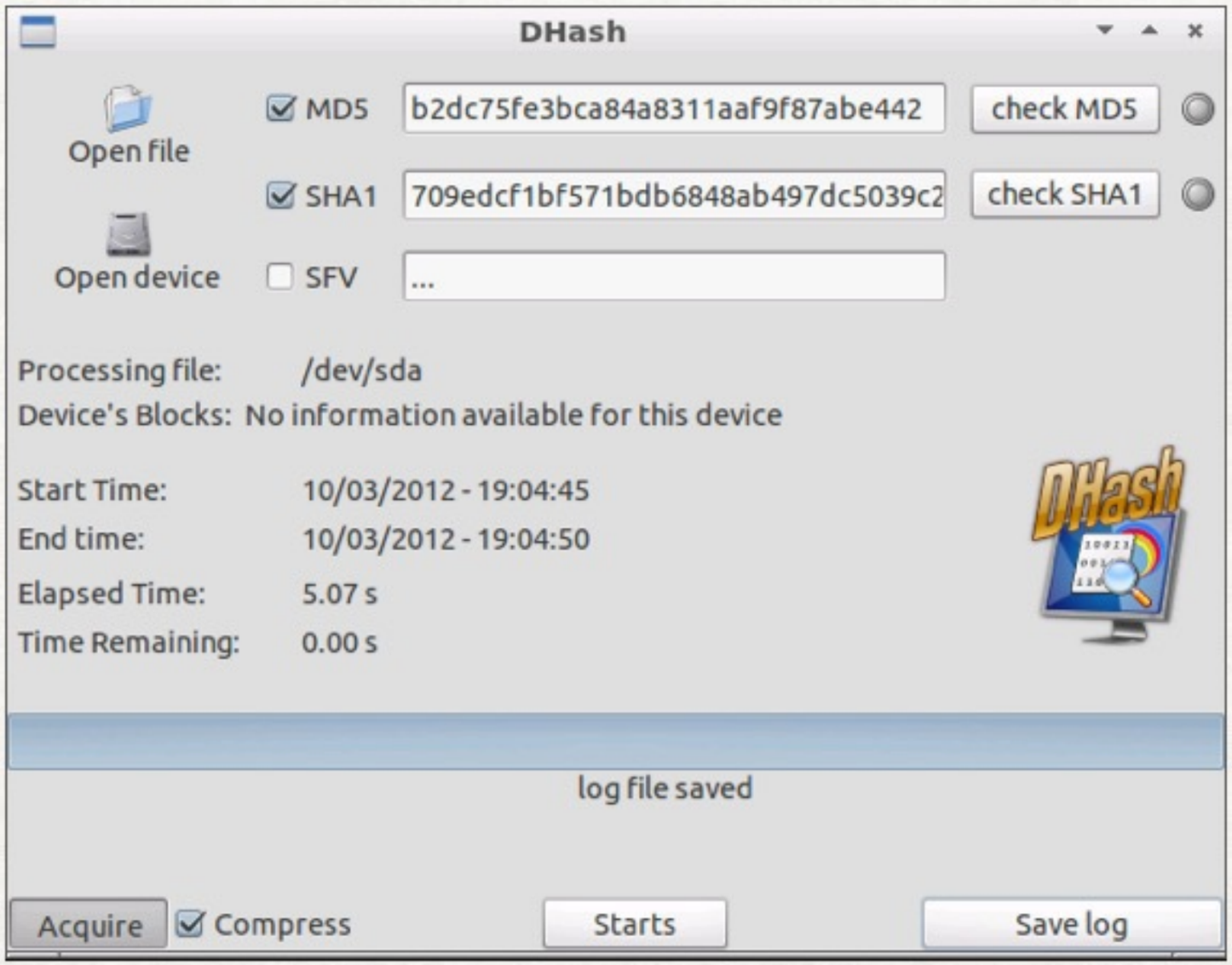
ACQUISIZIONE DI MEMORIE DI MASSA

DHASH

- Tool per l'acquisizione in formato raw, sviluppato dal team DEFT 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



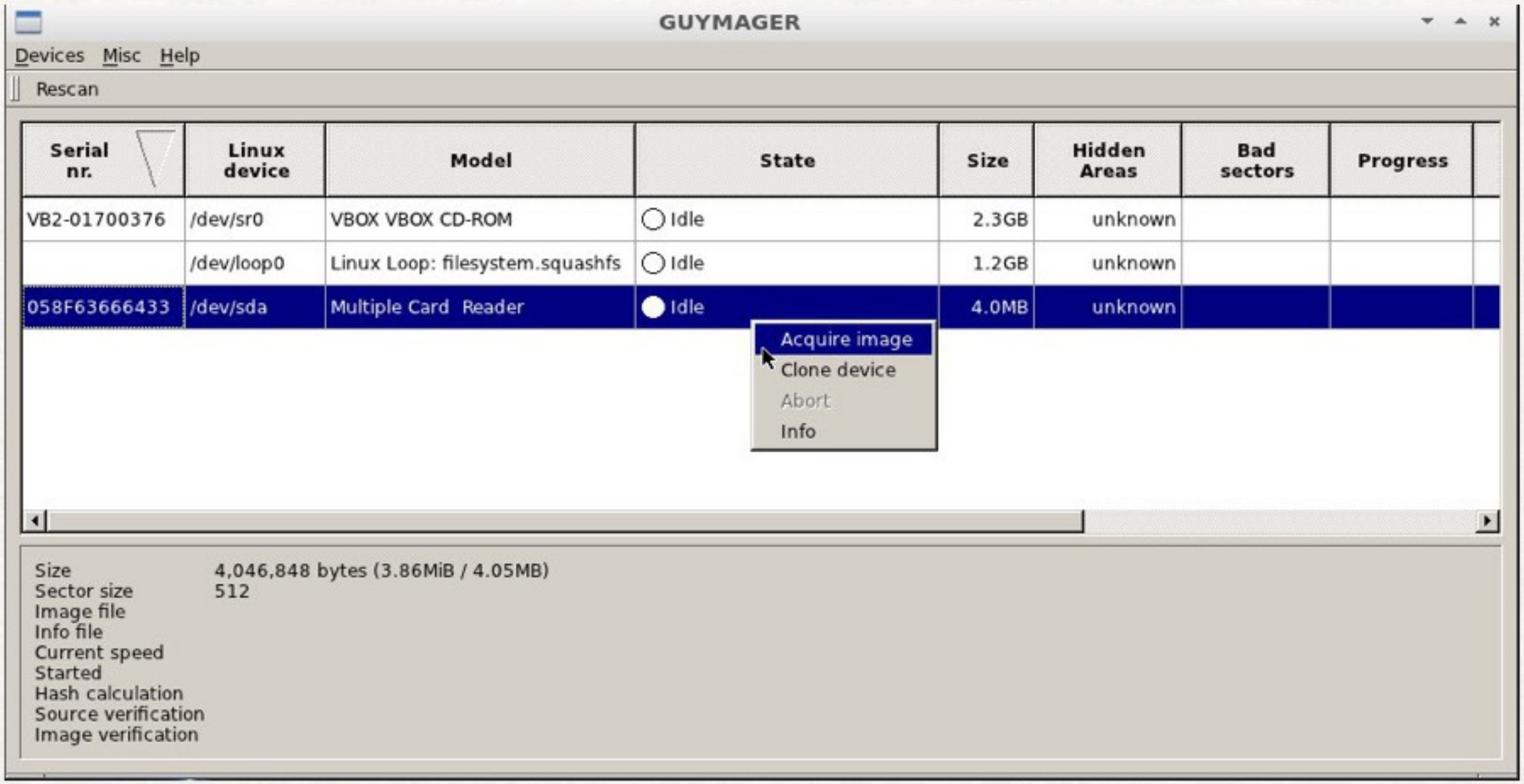
ACQUISIZIONE DI MEMORIE DI MASSA

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

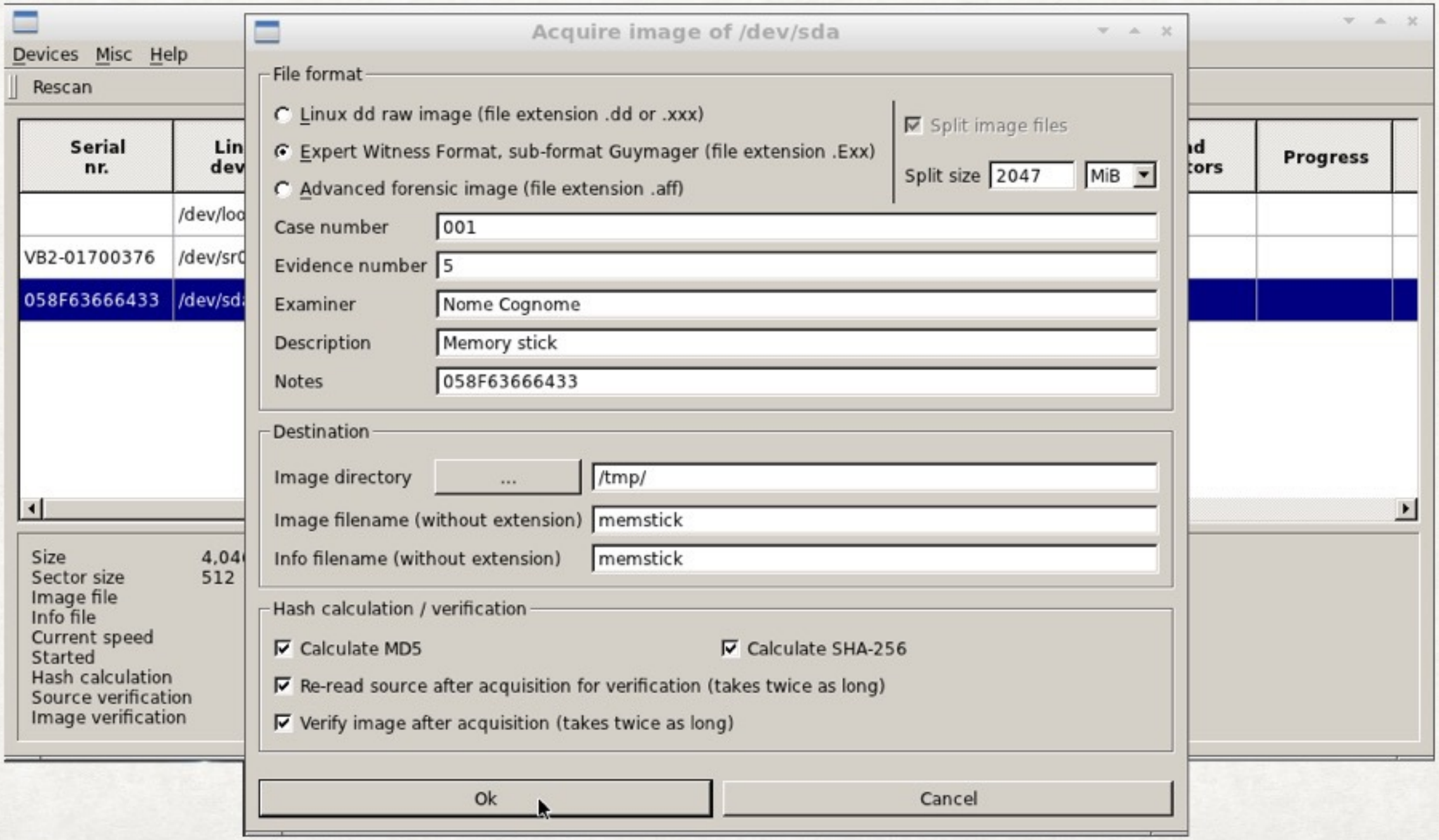
ACQUISIZIONE DI MEMORIE DI MASSA

GUYMAGER



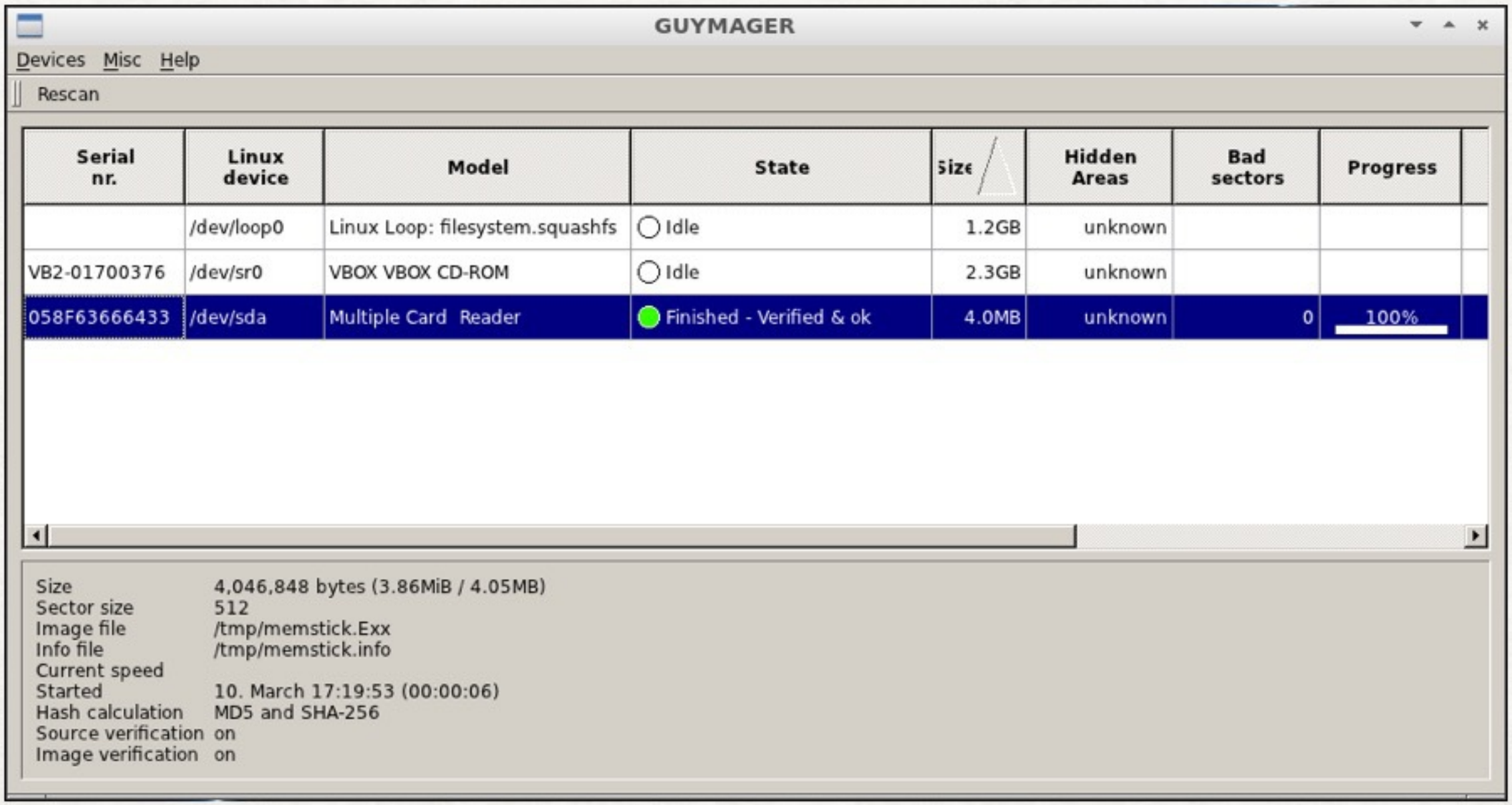
ACQUISIZIONE DI MEMORIE DI MASSA

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.)

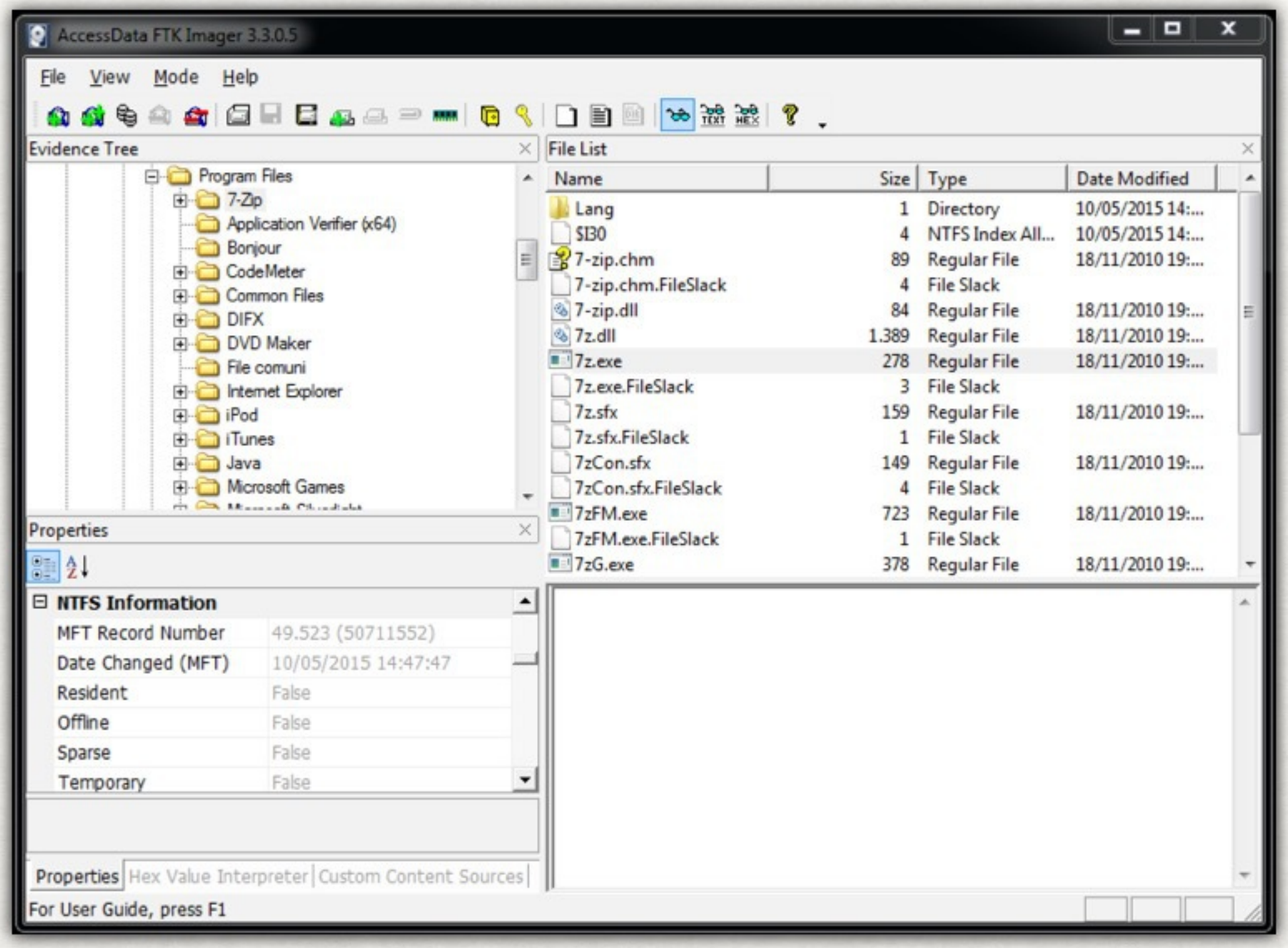
ACQUISIZIONE DI MEMORIE DI MASSA

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

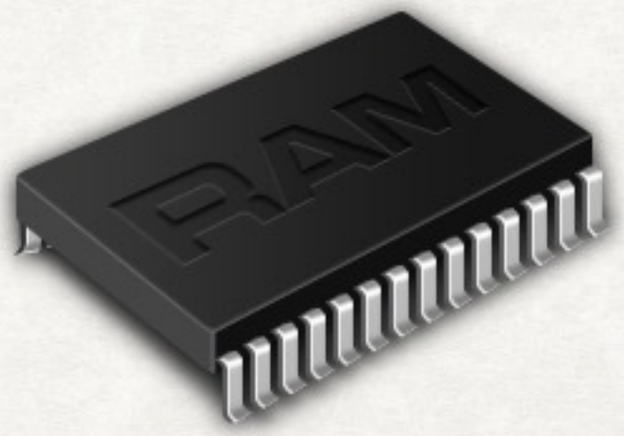
COPIA LOGICA TRAMITE FTK IMAGER



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

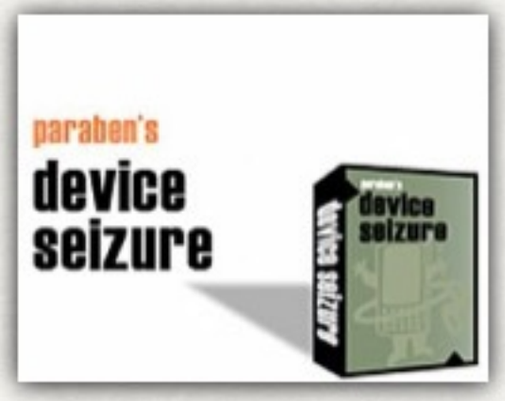
- Distruttiva e rischiosa
- Intero dump del chip di memoria
- Estrazione di tutti i files e cartelle
- E’ possibile fare carving

CENNI SU ACQUISIZIONE DI SMARTPHONE

STRUMENTI DI ACQUISIZIONE

Strumenti commerciali

MOBILedit



CENNI SU ACQUISIZIONE DI SMARTPHONE

STRUMENTI DI ACQUISIZIONE

Strumenti di backup

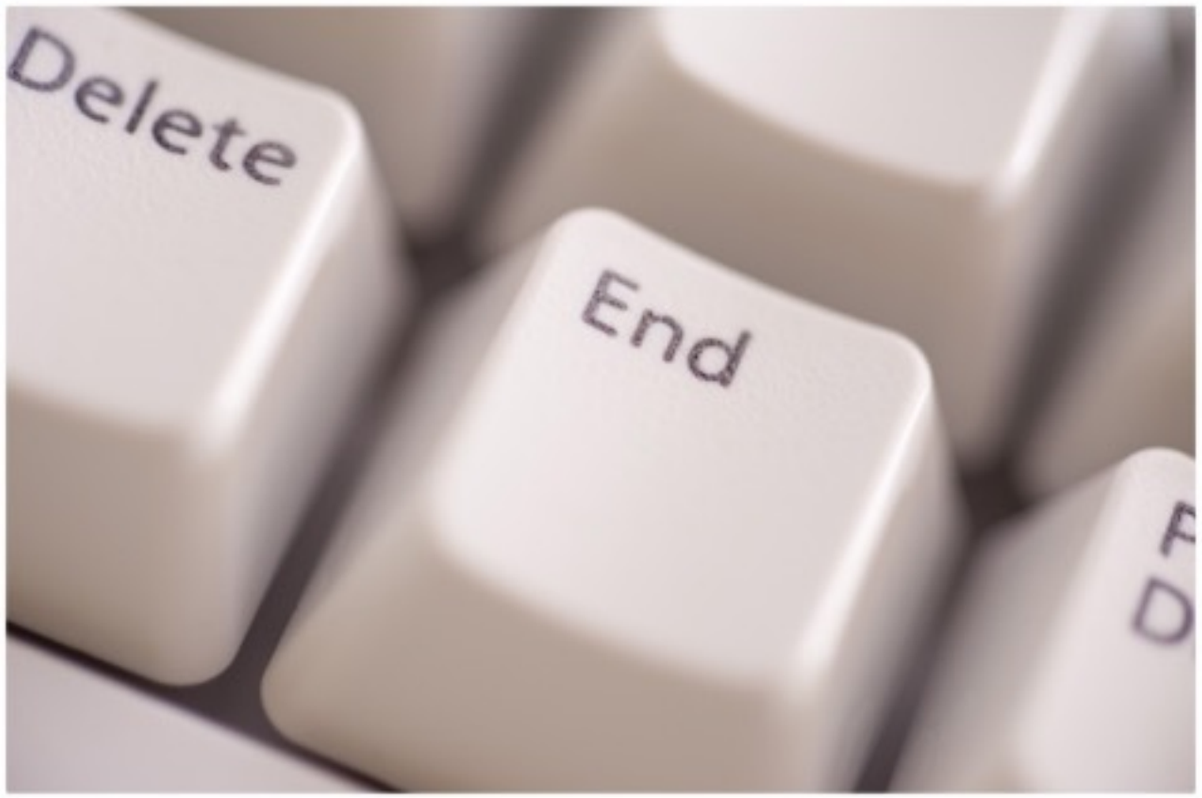
CENNI SU ACQUISIZIONE DI SMARTPHONE

STRUMENTI DI ACQUISIZIONE

Strumenti open

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

GRAZIE PER L'ATTENZIONE



LABORATORIO