

## Informatica forense

---

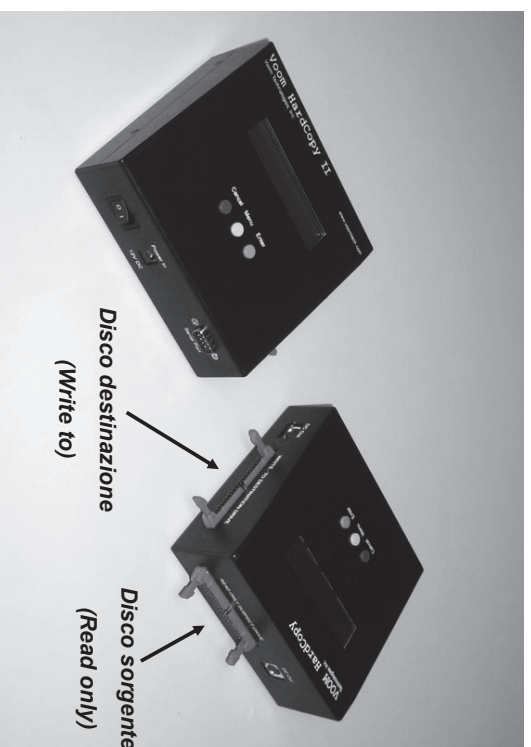
### Laboratorio

*Michele Ferrazzano*

15 marzo 2011

## Copiatore hardware

---



## Cosa occorre per fare analisi forense?

---

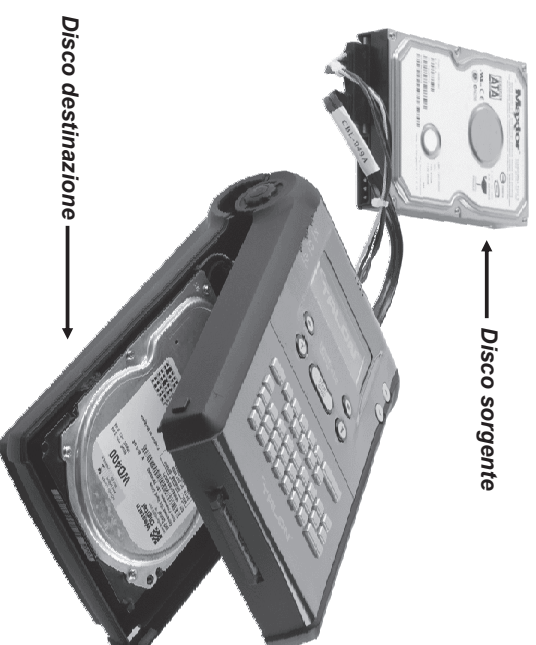
### Hardware

### Software

- PC e notebook
- Lettori di supporti e cavi (di tutti i tipi)
  - BluRay, DVD, CD, hard-disk, floppy 3,5", floppy 5,25", DAT...
  - Cavi per telefoni cellulari
- Copiatori
- Write blocker
- Cacciaviti
- Sistema operativo
  - Windows, Linux
- Software per acquisizione
  - Encase, FTK Imager, dd...
- Software per analisi
  - Generico
    - Encase, FTK, autopsy...
  - Ad hoc
    - NetAnalysis, DNA, P2Commander, Distributed Network Attack (DNA), Password Recovery Toolkit (PRTK), Oxygen Forensics...
- Conversione tra formati

## Copiatore hardware (es: Logicube Talon)

---



## Write blocker

- Un write blocker è un dispositivo usato per prevenire scritture (anche accidentali) su hard disk oggetto di investigazioni
- Il write blocker è posto tra il disco esaminato e il computer utilizzato per esaminarlo o acquisirlo



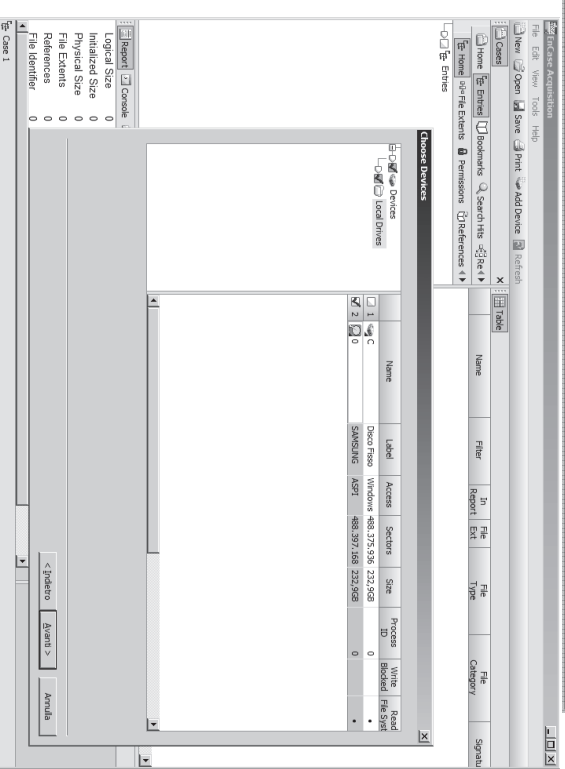
## Write blocker



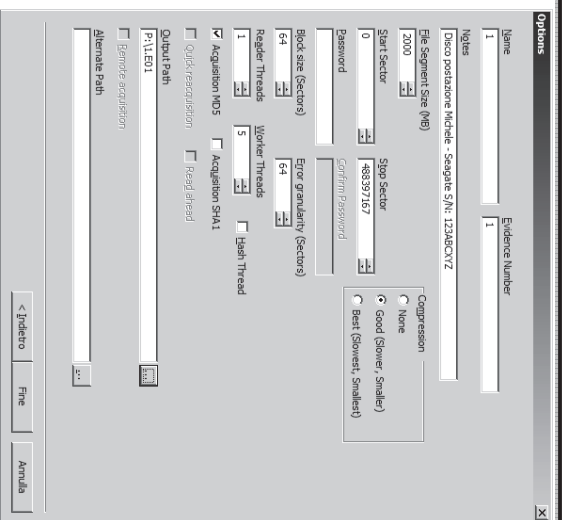
## Cacciaviti



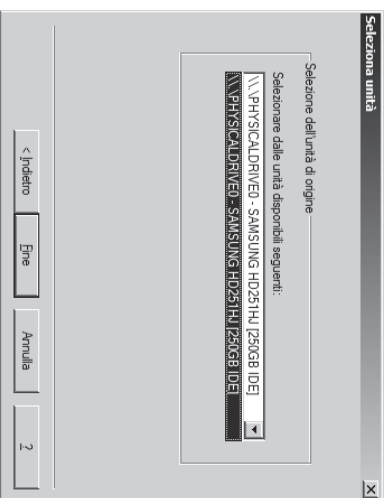
## Acquisizione – Encase



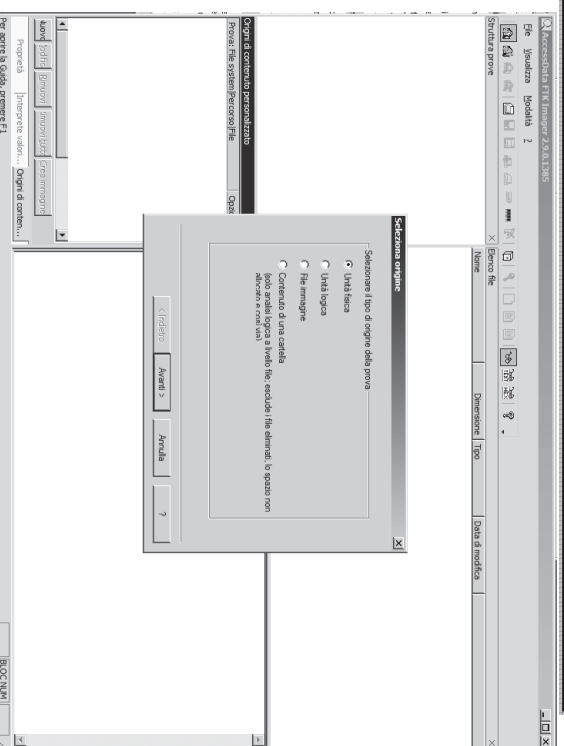
## Acquisizione - Encase



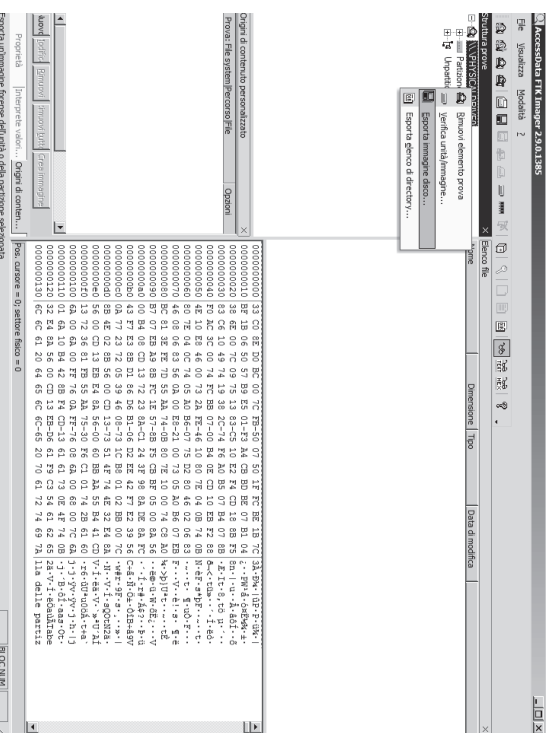
## Acquisizione - FTK Imager



## Acquisizione - FTK Imager



# Acquisizione - FTK Imager



# Acquisizione – FTK Imager

Seleziona tipo di immagine

Seleziona il tipo di immagine di destinazione

☒ Non elaborata (dd)

☐ SMART

☐ E01

< Indietro

Avanti >

Annulla

?

Seleziona destinazione immagine

Carica il file di destinazione immagine

Pr1

Scegli

Nome file immagine (estensione)

1.dd

Dimensione massima per immagine (MB)

2000

Per i formati non elaborati nel E01.0 = non formattare

Compressione (0=nessuna, 1=lu, reduce ... , 9=massima)

0

Use AD Encryption

☐

< Indietro

Fine

Annulla

2

Informazioni sull'elemento prova

Numero caso:

1

Numero prova:

1

Descrizione ultima:

Disco portatile Michiel - Samsung S/N: 12345678

Esaminatore:

Michiel

Note:

< Indietro

Avanti >

Annulla

2

Crea immagine

Oggetto immagine

\\.\PR1SCARD\PR1

Destinazione immagine

Numero prova 115865

0

Pr1.1.dd (raw.dd)

Aggiungi...

03/01/2011

Browse

☒ Verifica le immagini dopo che sono stati

☐ Creare le statistiche e avanzare

☐ Crea gli elenchi di backup e di tutti file dell'immagine dopo che sono stati creati

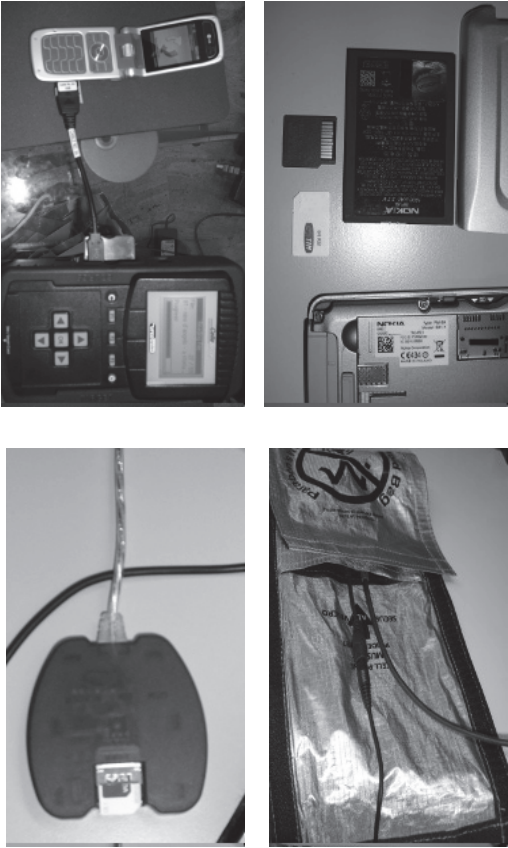
Avvia

Annulla

# Acquisizione – dd

```
stresslinux_32bit-686-0.5.113.raw: dd
File Modifica Visualizza Scorrimento Segnalibri Impostazioni Auto
bash-3.1# dd if=stresslinux_32bit-686-0.5.113.raw of=/dev/sdb bs=4k
21401540 records in
21401540 records out
876609336 bytes (877 MB) copied, 146.317 s, 6.0 MB/s
bash-3.1#
```

# Acquisizione – Dispositivi mobile



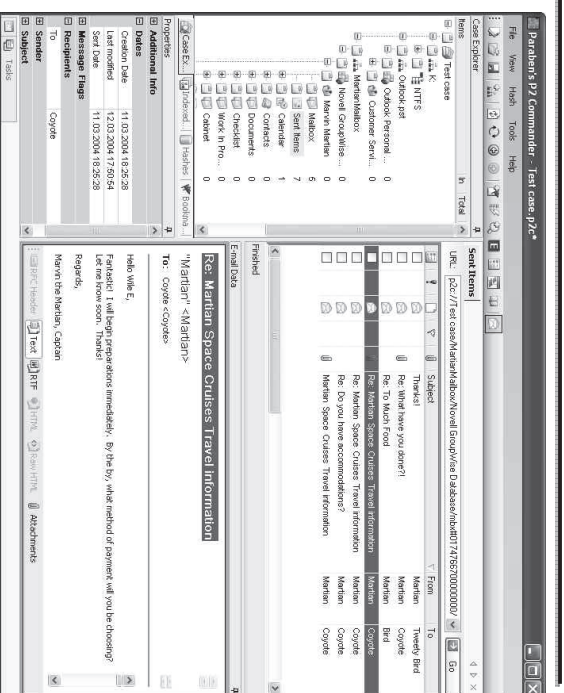
# Analisi – Autopsy







## Analisi - P2Commander



## Analisi - Oxygen forensics

