Informatica forense

Laboratorio

Michele Ferrazzano

15 marzo 2011

Cosa occorre per fare analisi forensi?

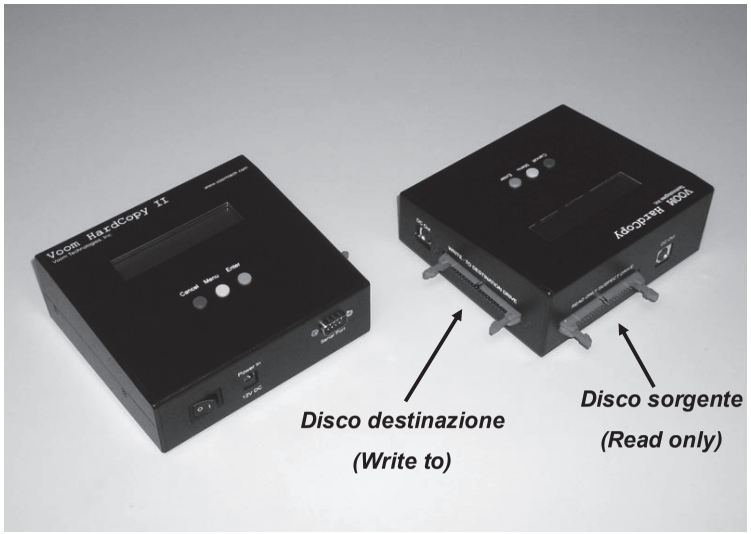
Hardware

- 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

Software

- 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

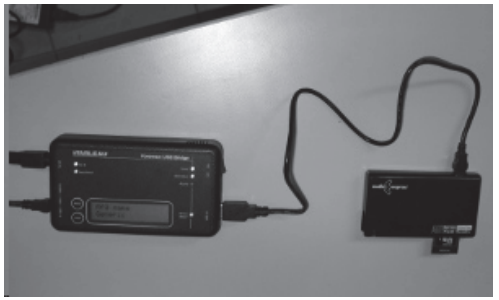


Copiatore hardware (es: Logicube Talon)

Write blocker

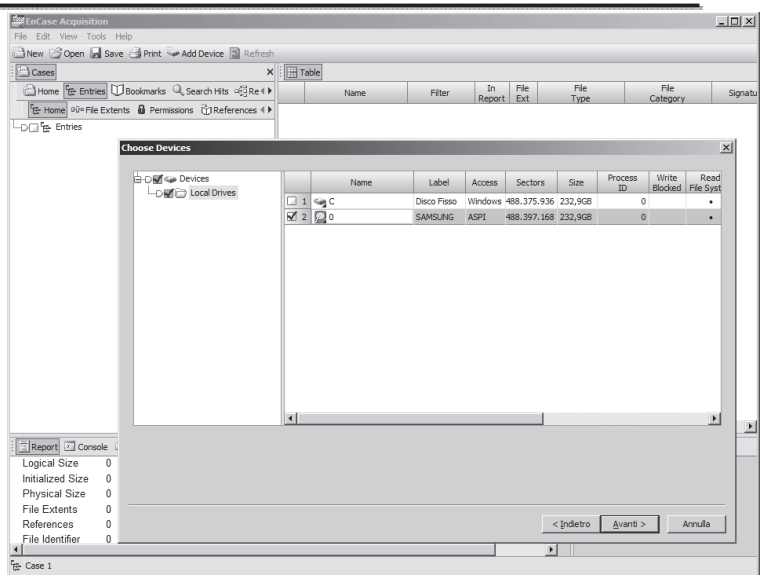
- Un write blocker è un dispositivo usato per prevenire scritture (anche accidentali) su hard disk oggetto di investigazioni
- Il write blocker è posto tra il disco esaminato e il computer utilizzato per esaminarlo o acquisirlo

Write blocker

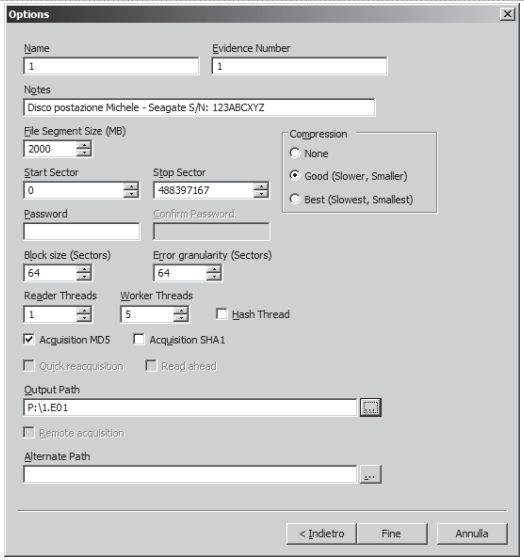


Cacciaviti

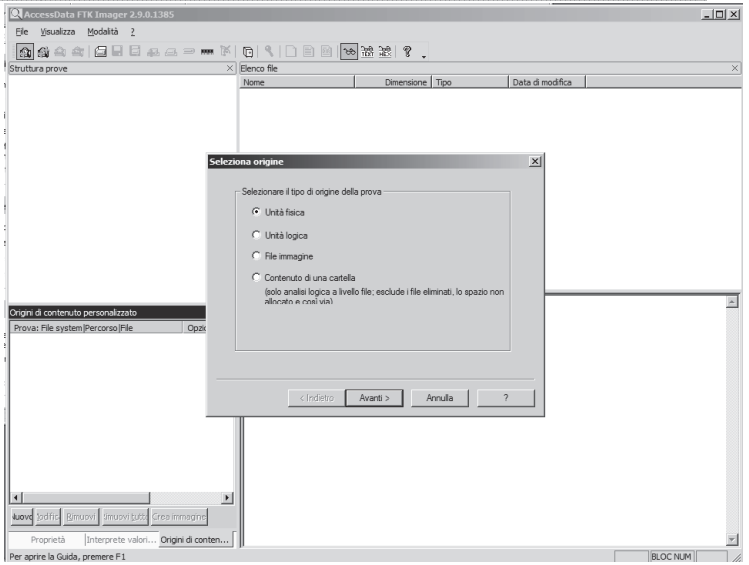
Acquisizione – Encase



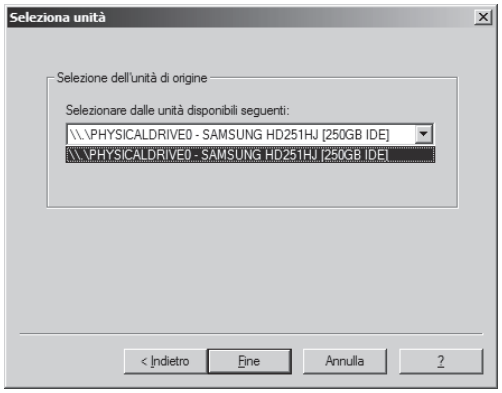
Acquisizione - Encase



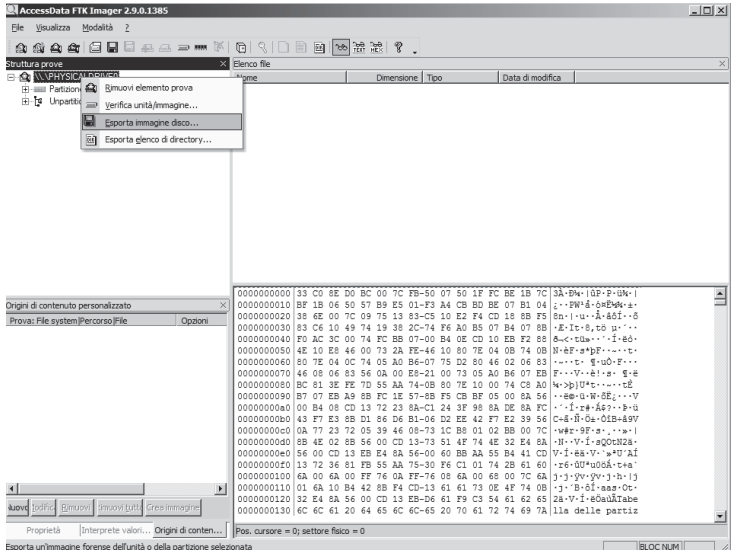
Acquisizione - FTK Imager



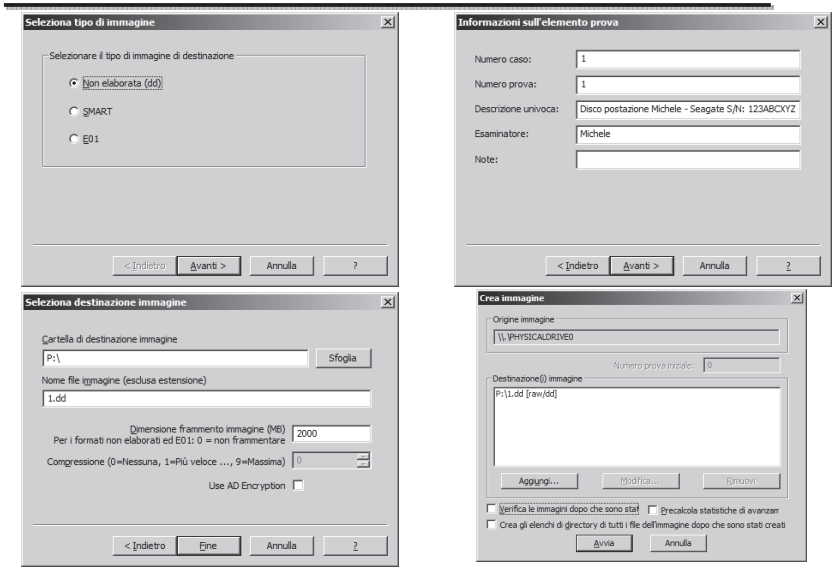
Acquisizione - FTK Imager



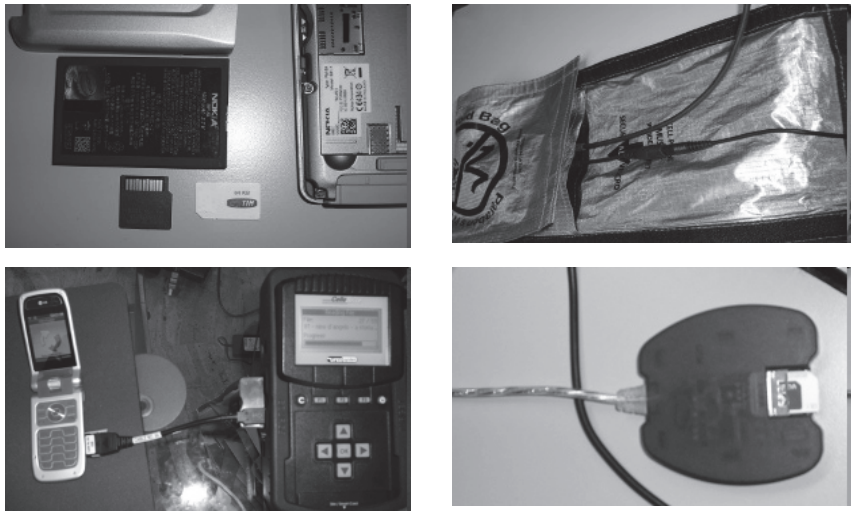
Acquisizione - FTK Imager



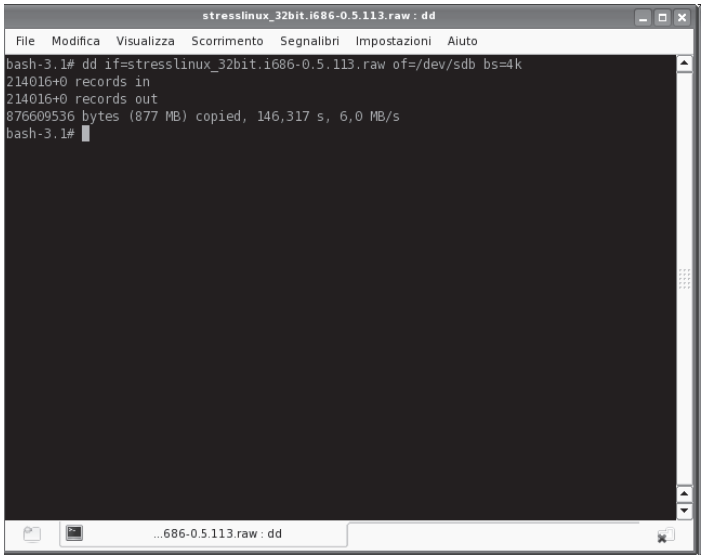
Acquisizione – FTK Imager



Acquisizione – Dispositivi *mobile*

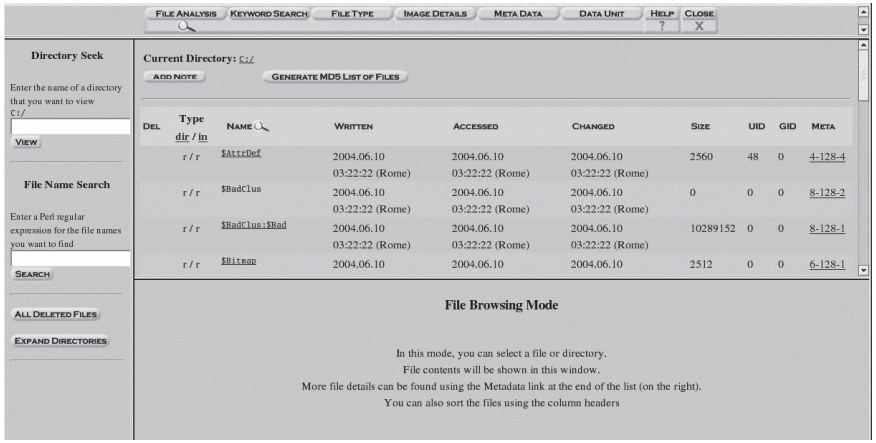


Acquisizione – dd

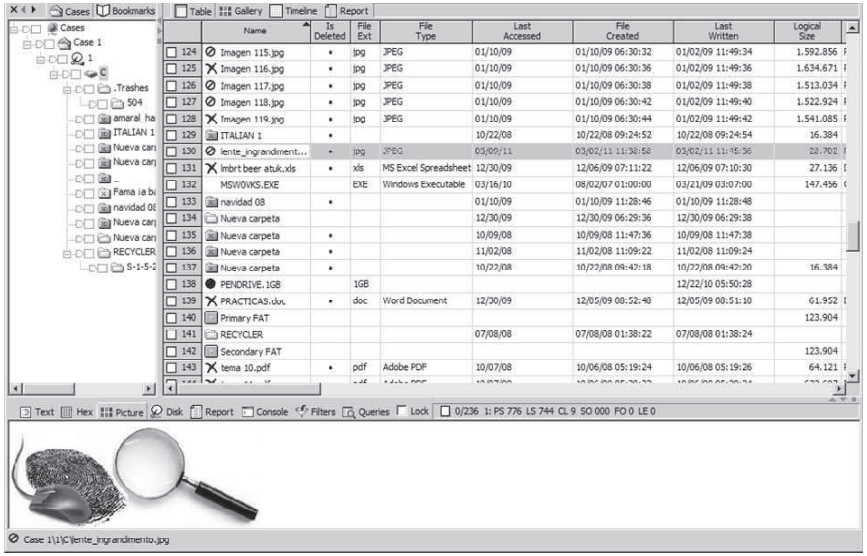


Analisi – Autopsy

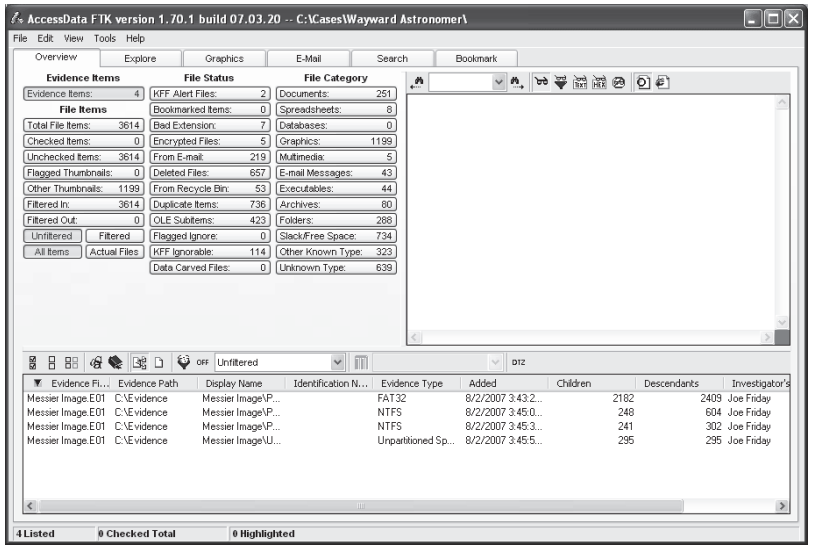
Analisi - Autopsy



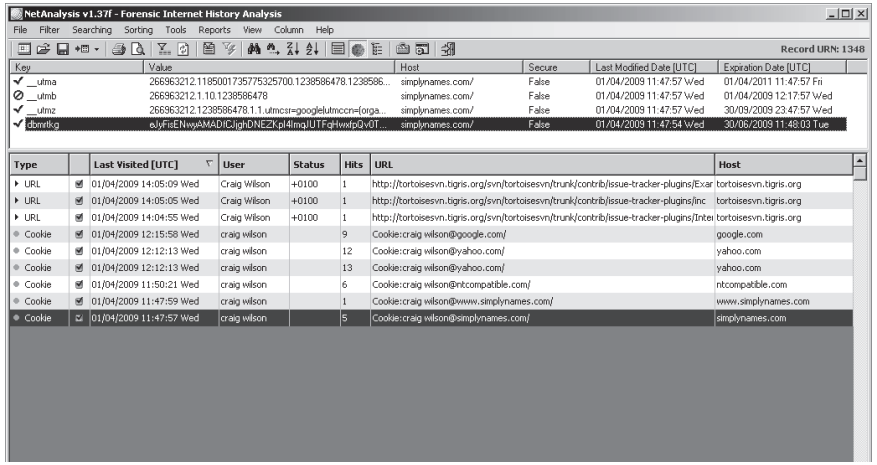
Analisi - Encase



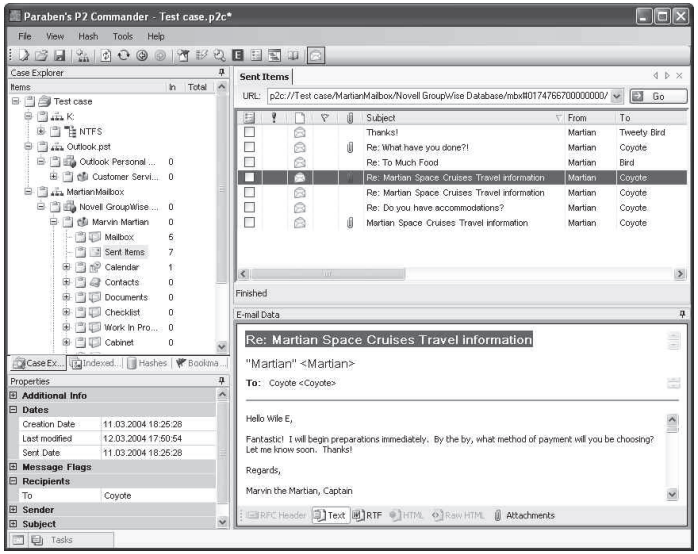
Analisi - FTK (Forensic ToolKit)



Analisi - NetAnalysis



Analisi - P2Commander



Analisi - Oxygen forensics