Informatica forense

Laboratorio

Michele Ferrazzano

28 marzo 2011

Sommario

- Hardware e software
- Acquisizione
  - Disk forensics
  - Network forensics
- Analisi
  - Disk forensics
  - Network forensics
- Laboratorio low-cost

Hardware per l'attività di laboratorio

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

Software per l'attività di laboratorio

- Sistema operativo
  - Windows, Linux
- Software per acquisizione (DF)
  - Encase, FTK Imager, dd…
- Software per analisi (DF)
  - Generico
    - Encase, FTK, autopsy…
  - Ad hoc
    - NetAnalysis, DNA, P2Commander, Distributed Network Attack (DNA), Password Recovery Toolkit (PRTK), Oxygen Forensics…
- Conversione tra formati
- Software per acquisizione (NF)
  - Wireshark…
- Software per analisi (NF)
  - Wireshark, XPlico…

Acquisizione

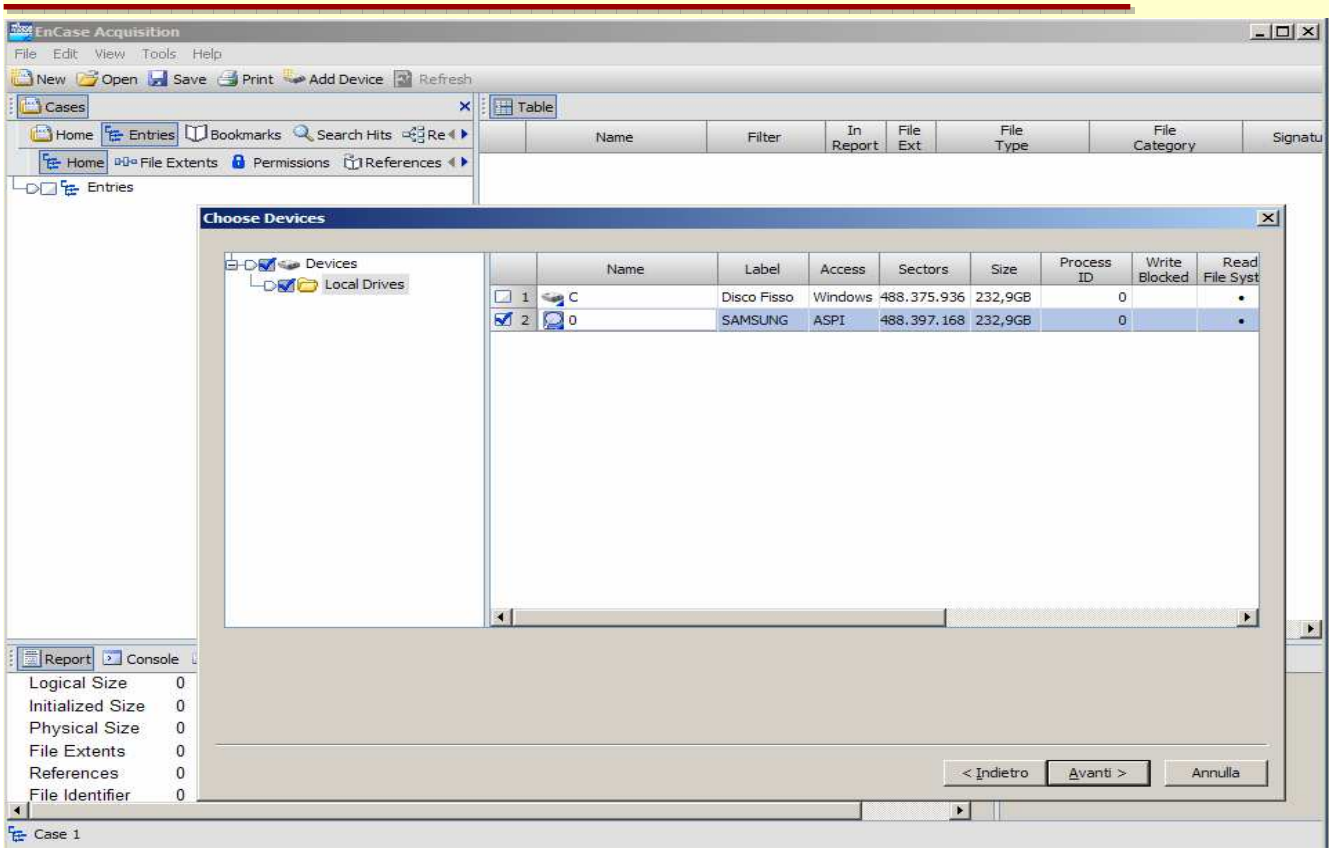
DISK FORENSICS

Copiatore hardware

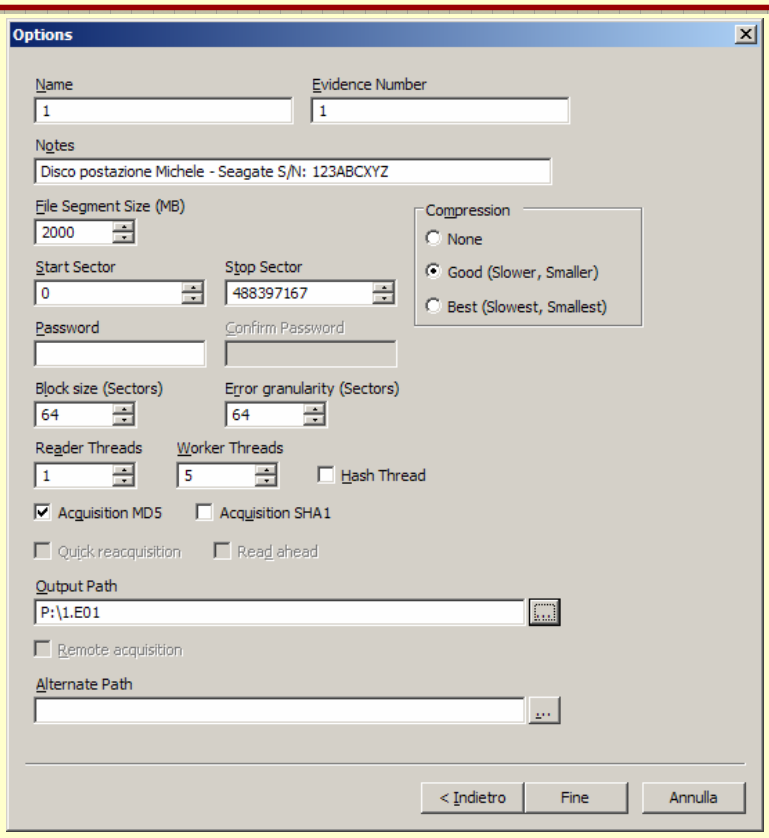
Copiatore hardware (es: Logicube Talon)

Write blocker

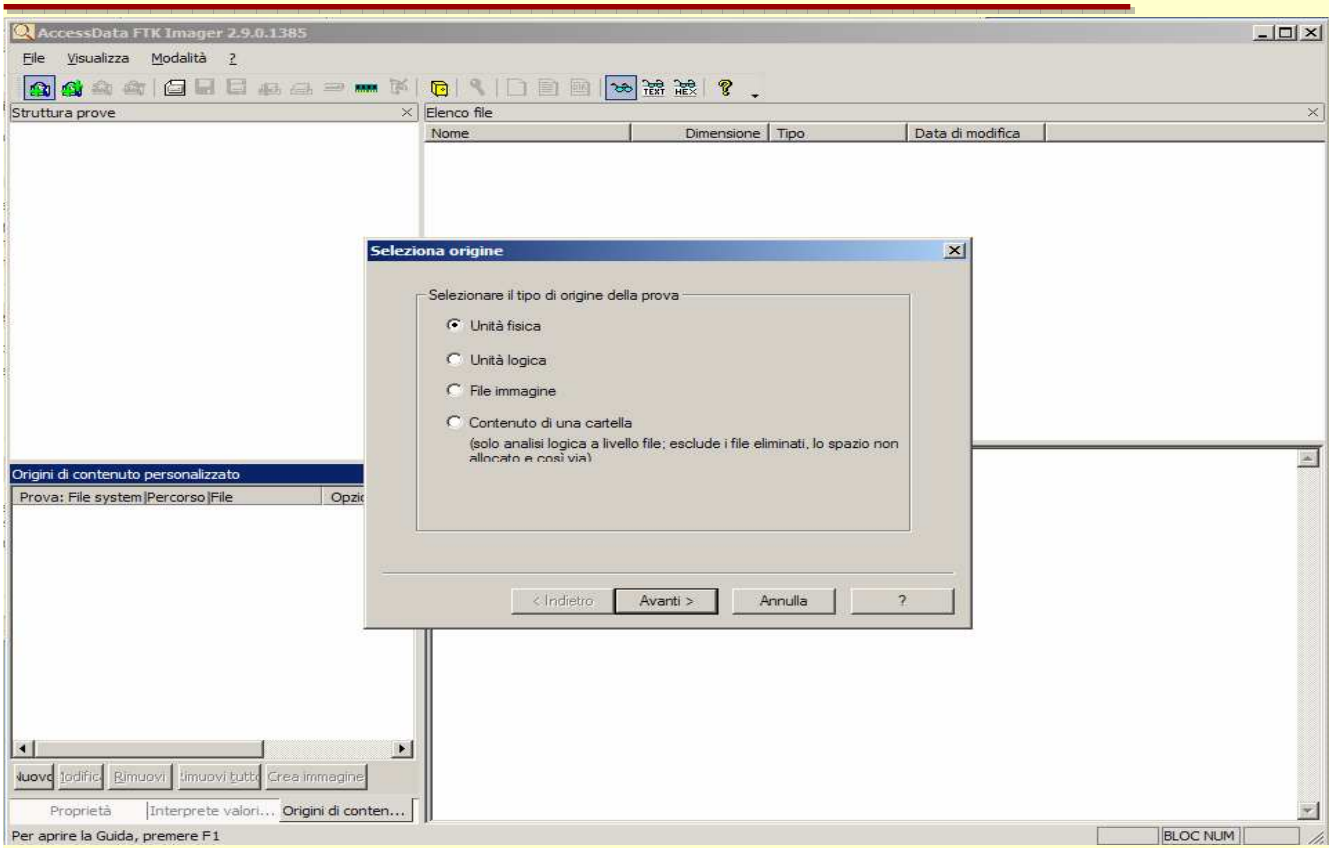
Acquisizione – Encase



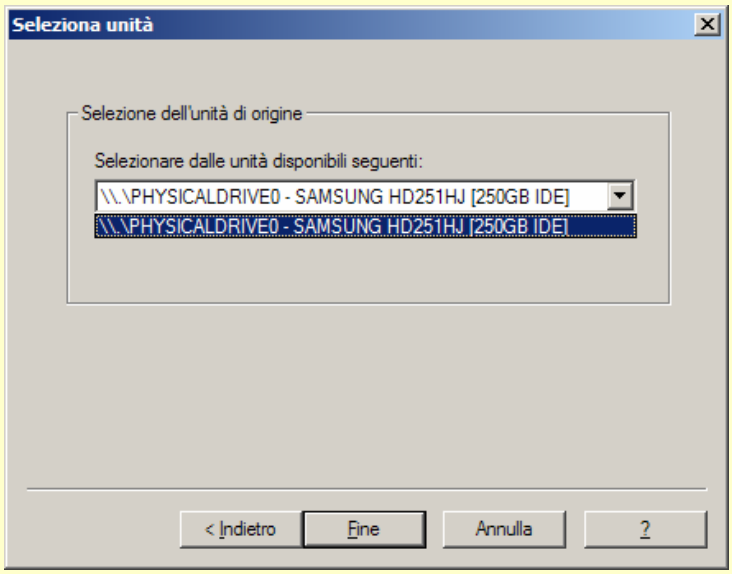
Acquisizione - Encase



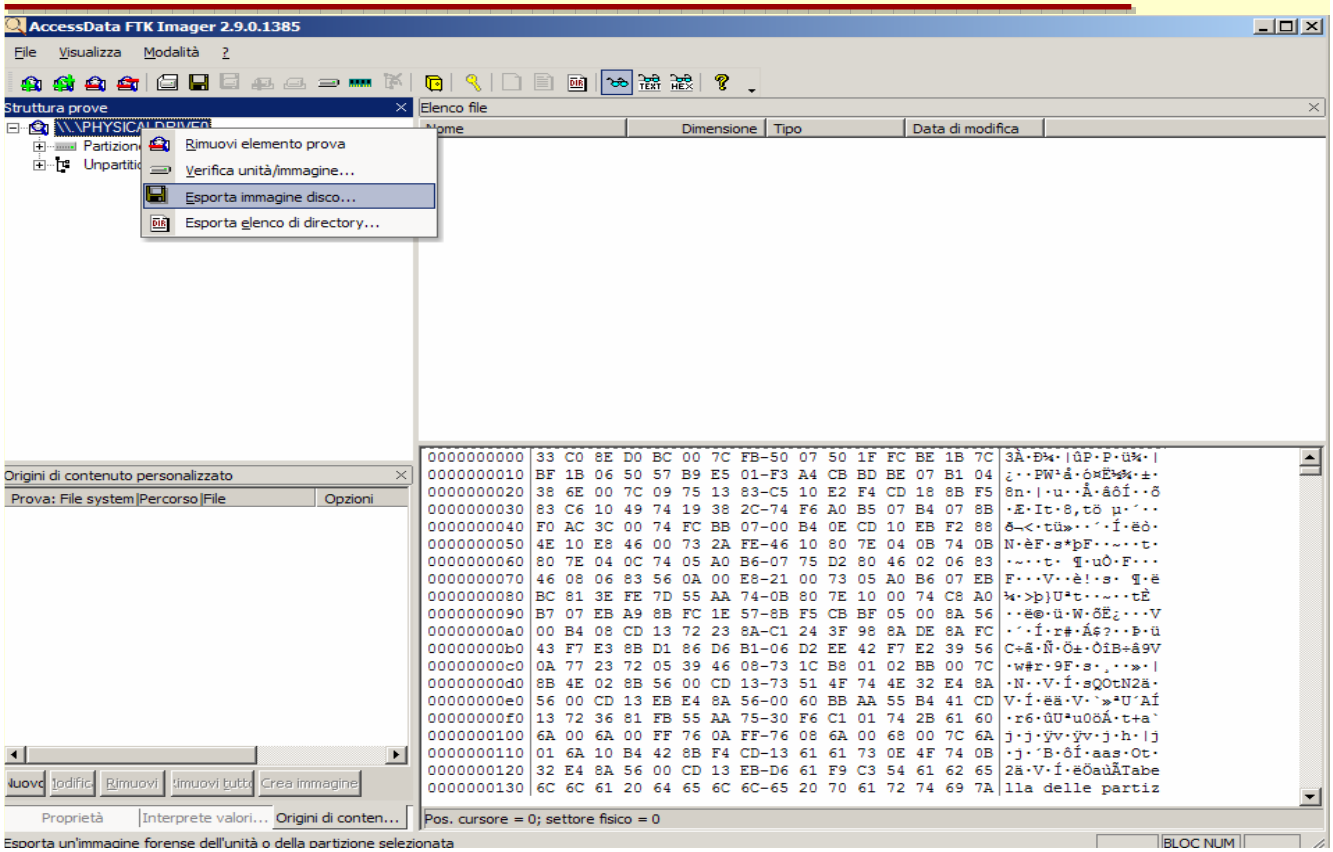
Acquisizione - FTK Imager



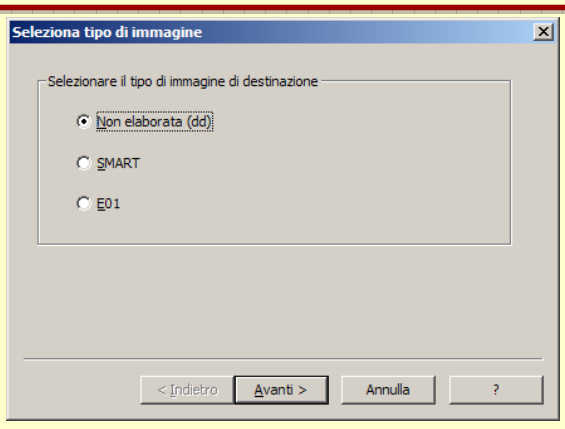
Acquisizione - FTK Imager

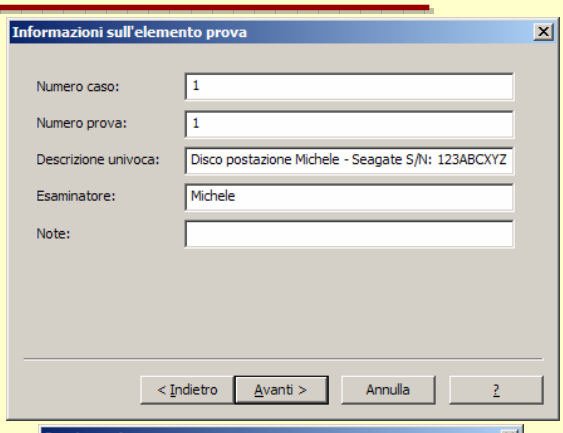


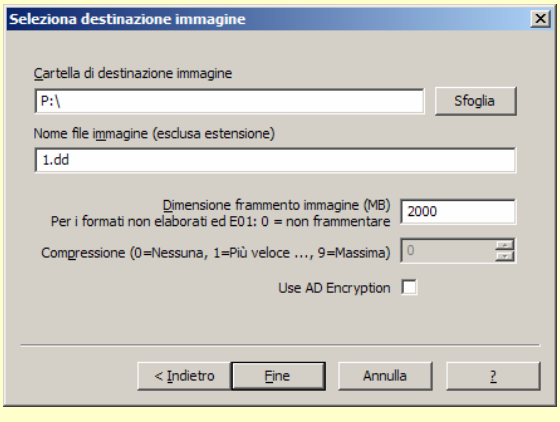
Acquisizione - FTK Imager

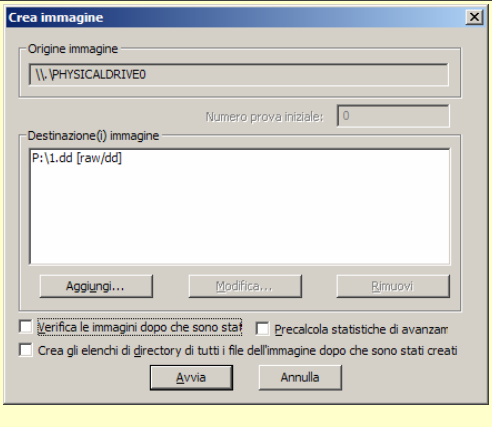


Acquisizione – FTK Imager

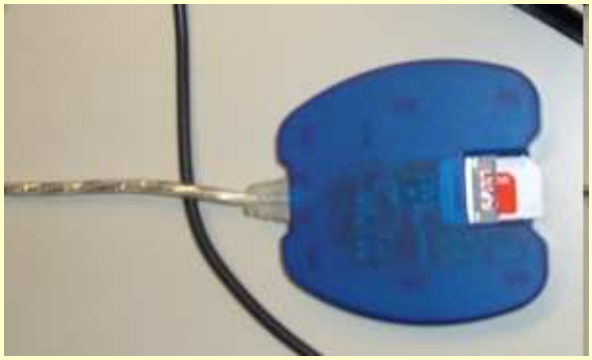




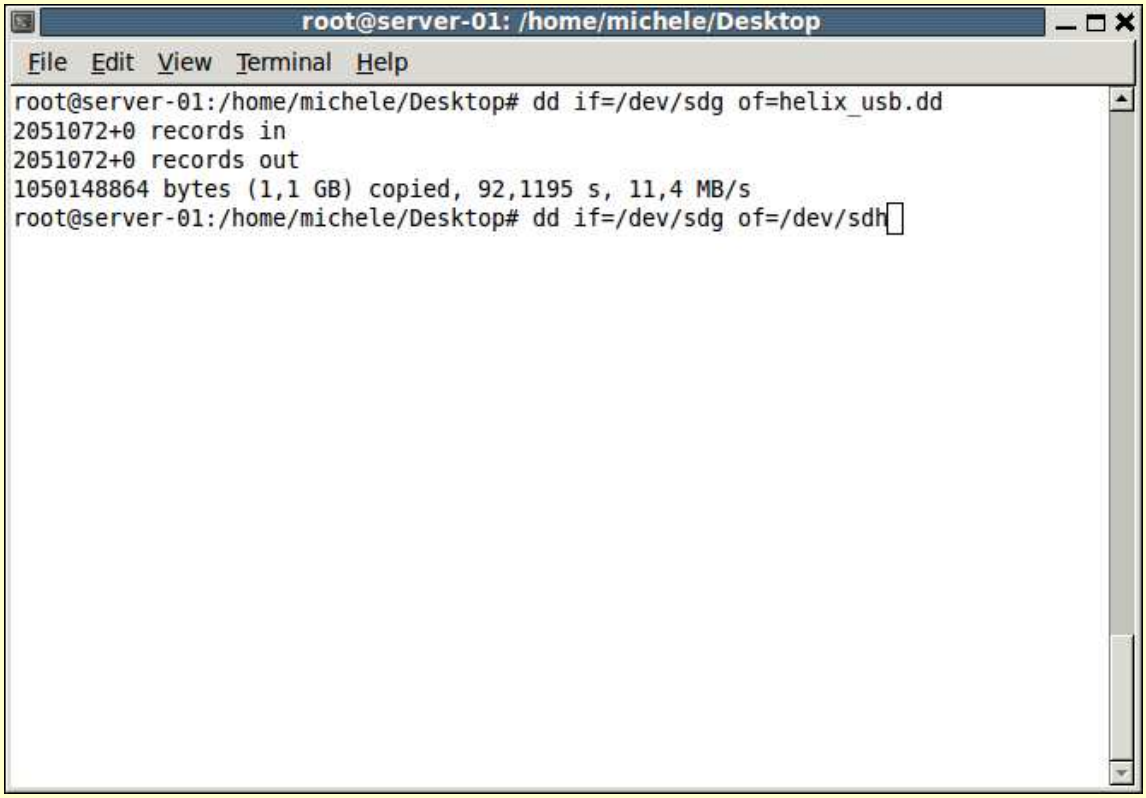




Acquisizione – Dispositivi *mobile*



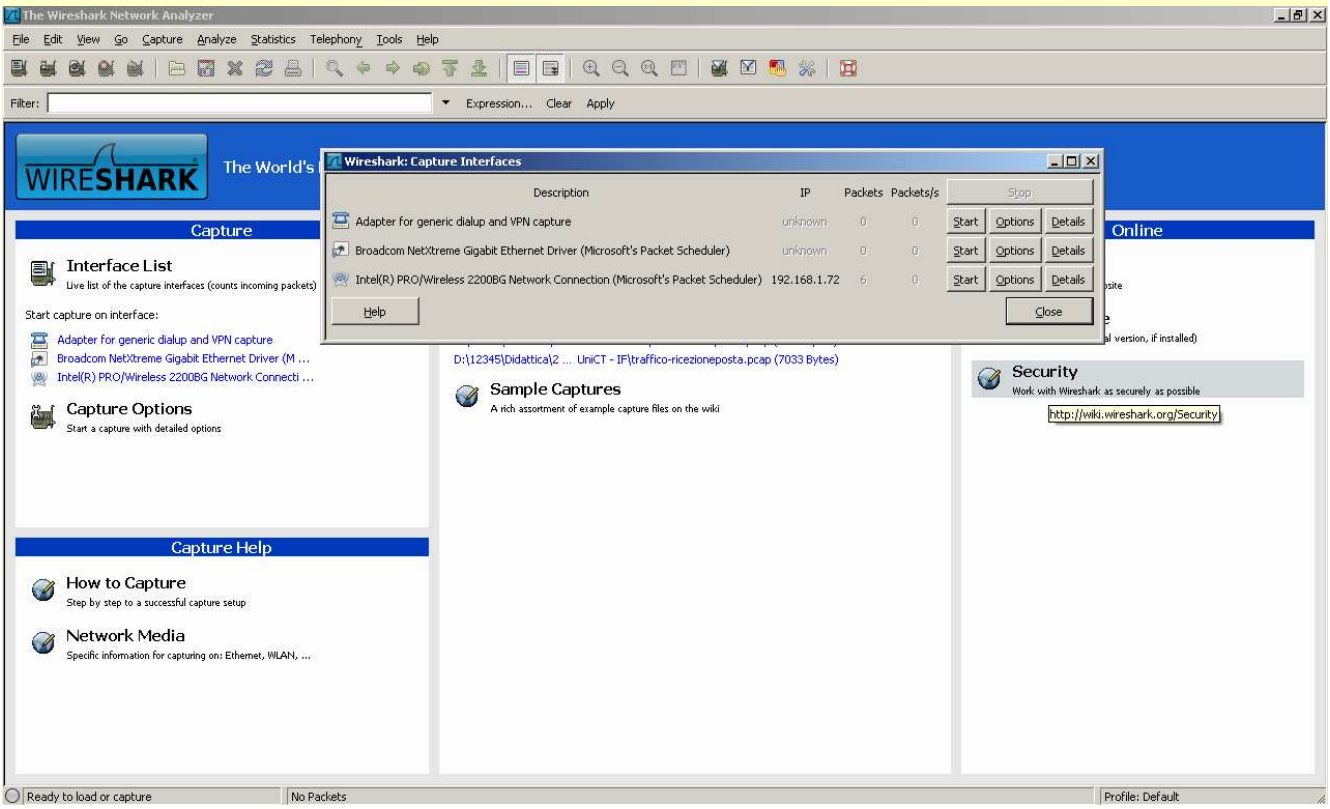
Acquisizione – dd



Analisi

NETWORK FORENSICS

Wireshark

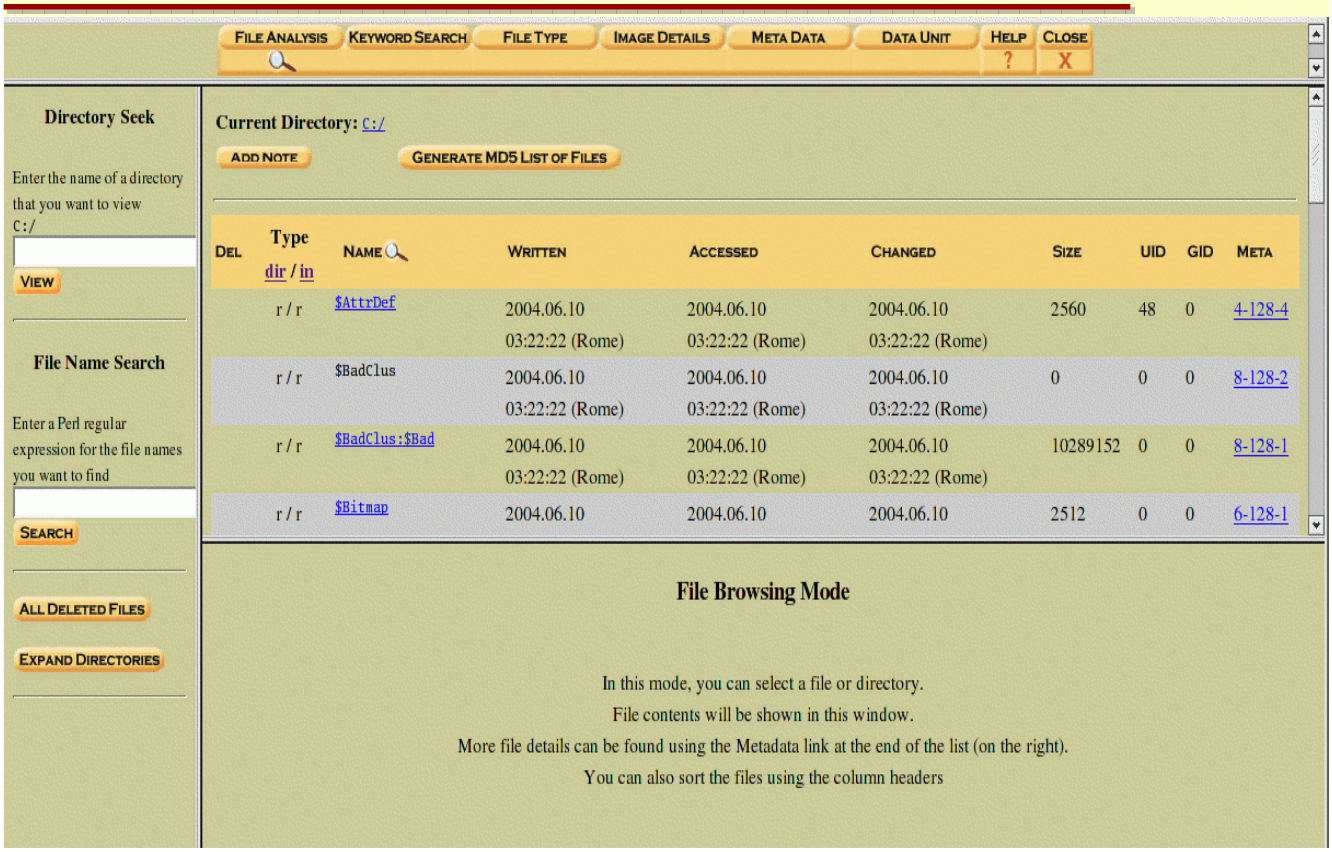


Analisi

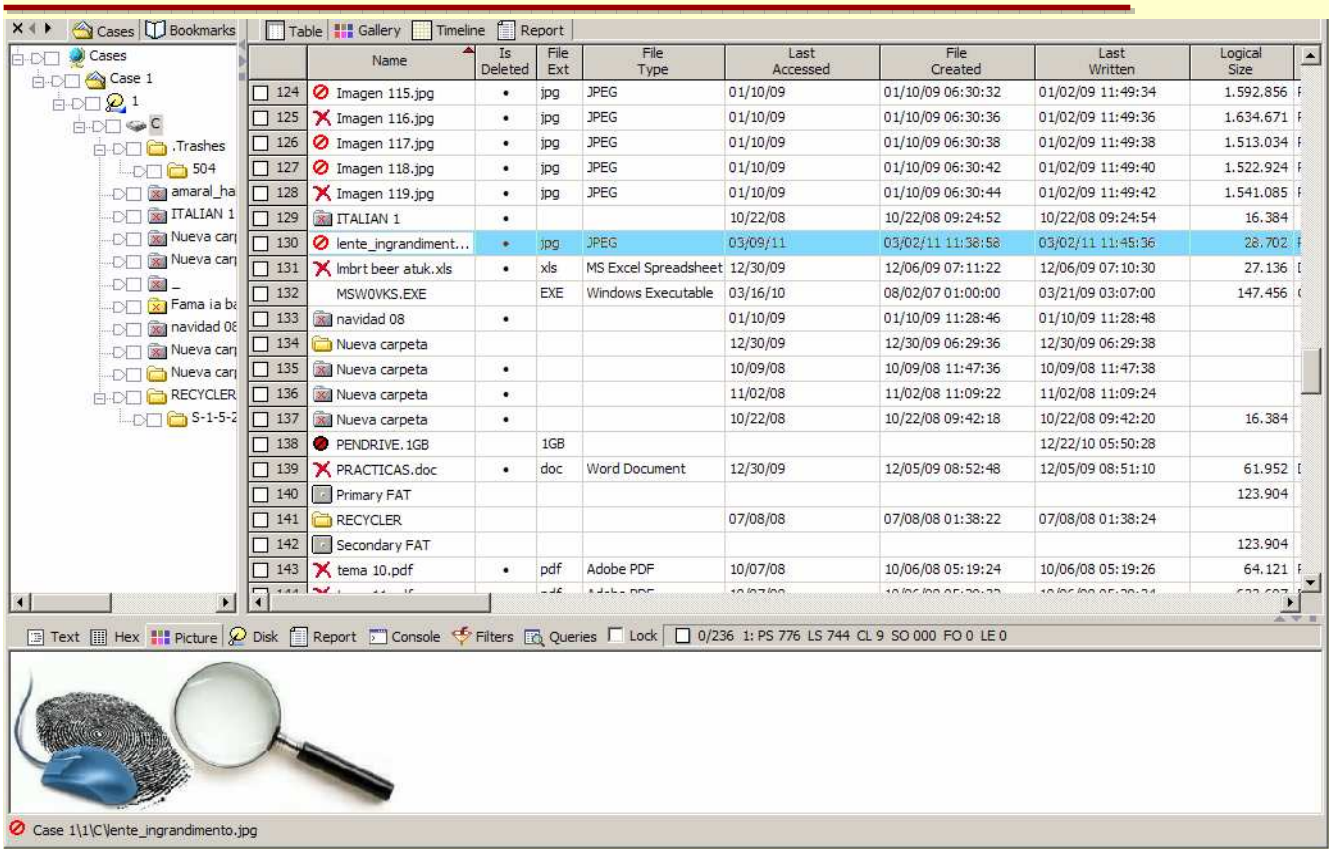
DISK FORENSICS

Analisi – Autopsy

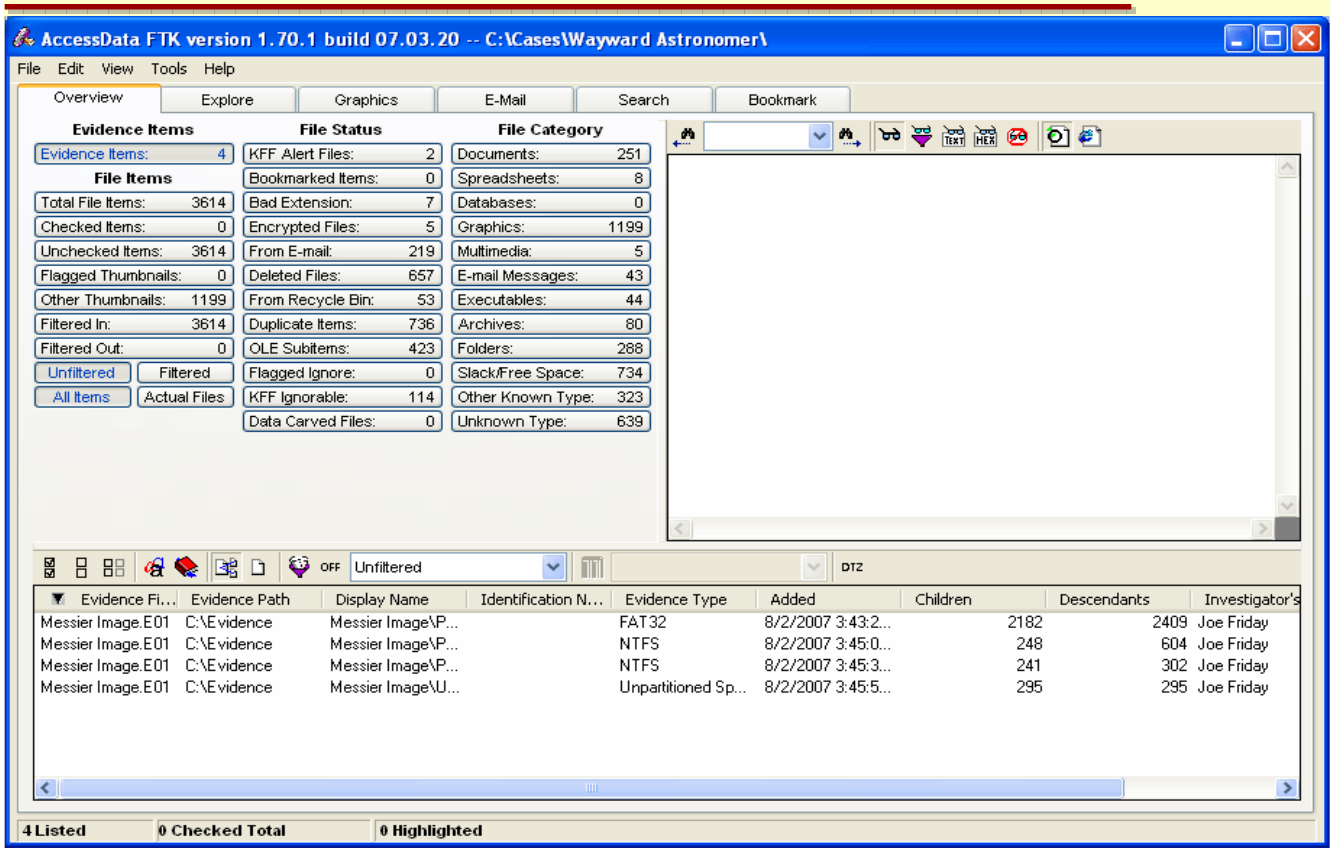
Analisi - Autopsy



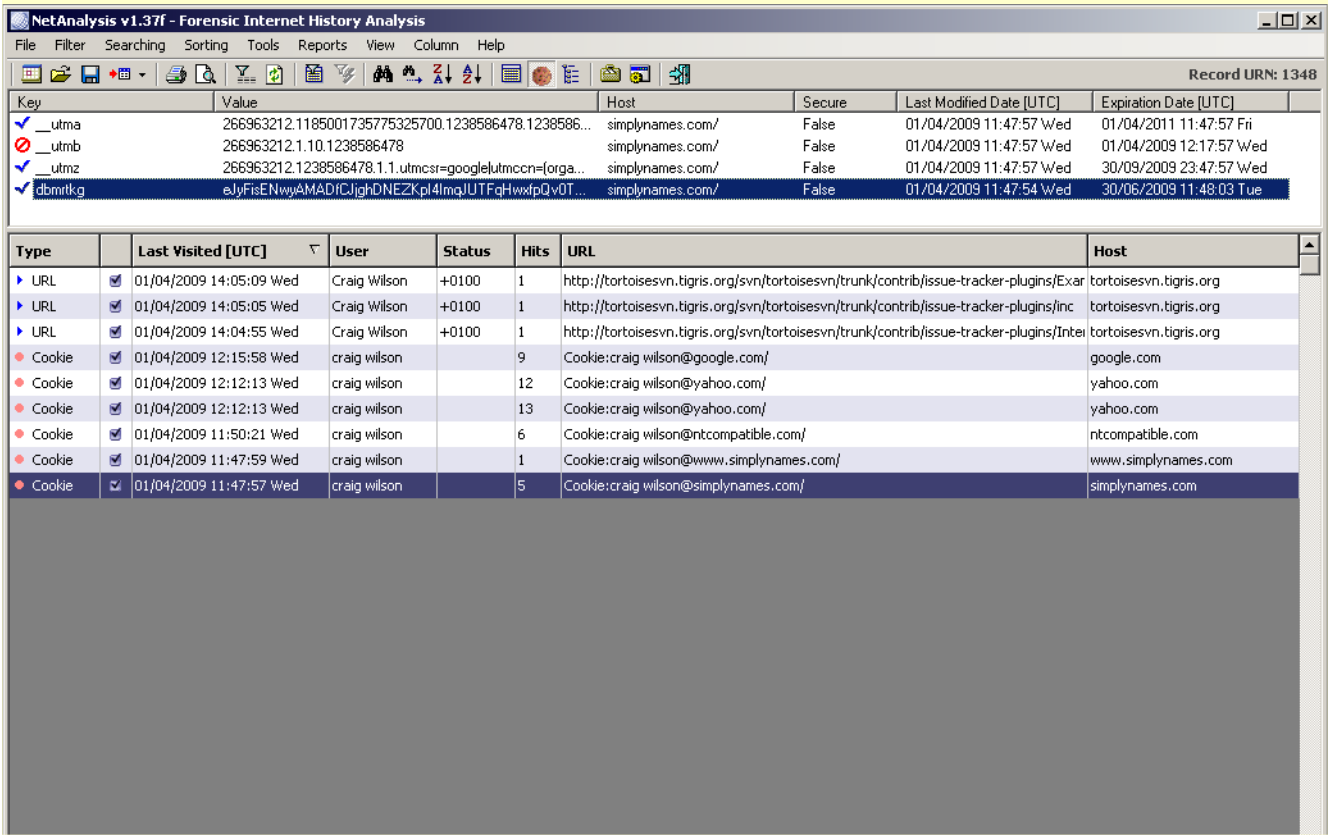
Analisi - Encase



Analisi - FTK (Forensic ToolKit)

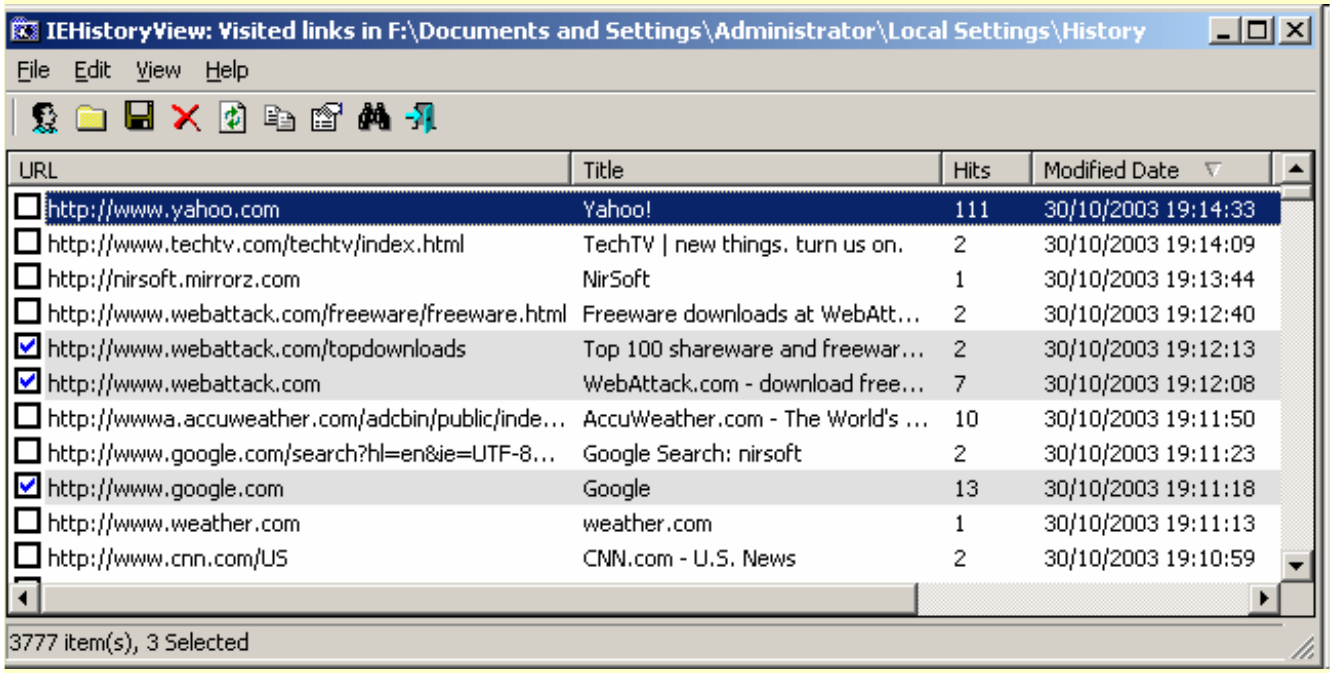


Analisi - NetAnalysis



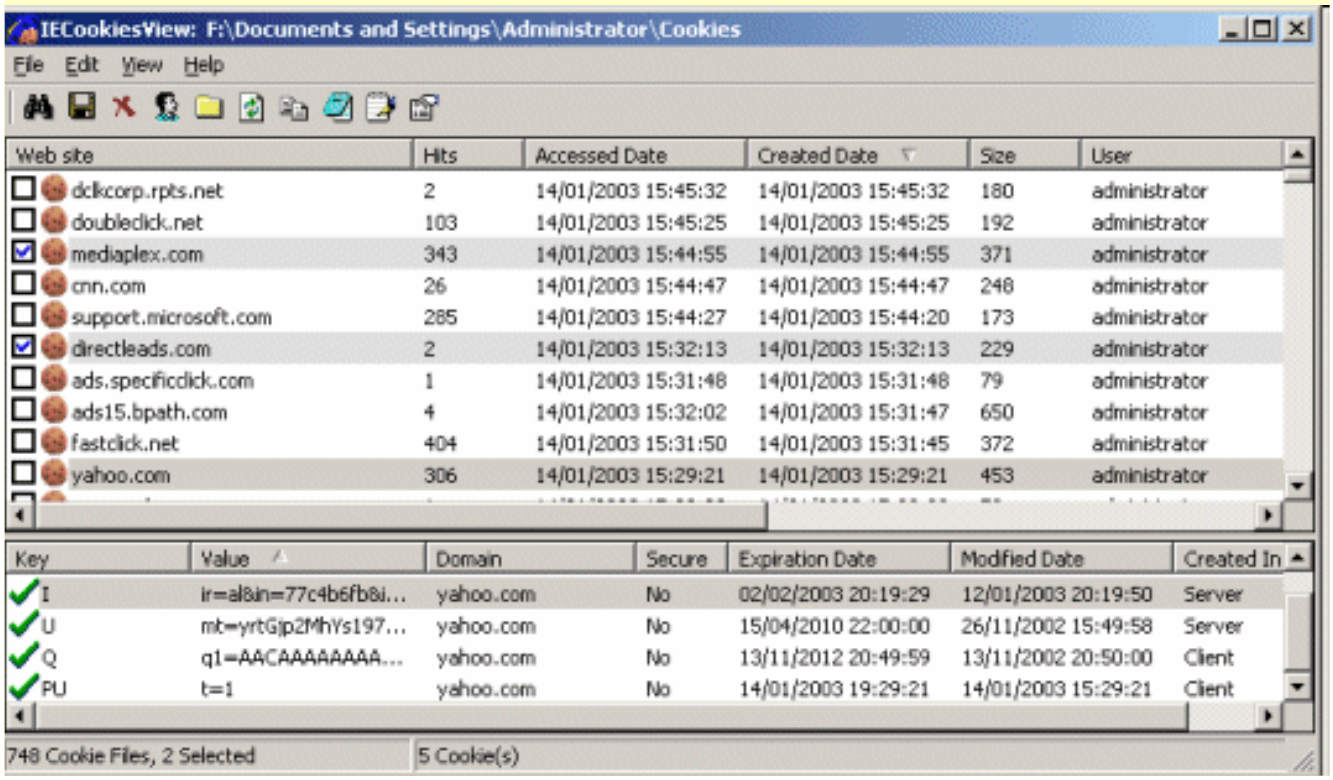
IEHistoryView

http://www.nirsoft.net/utils/iehv.html



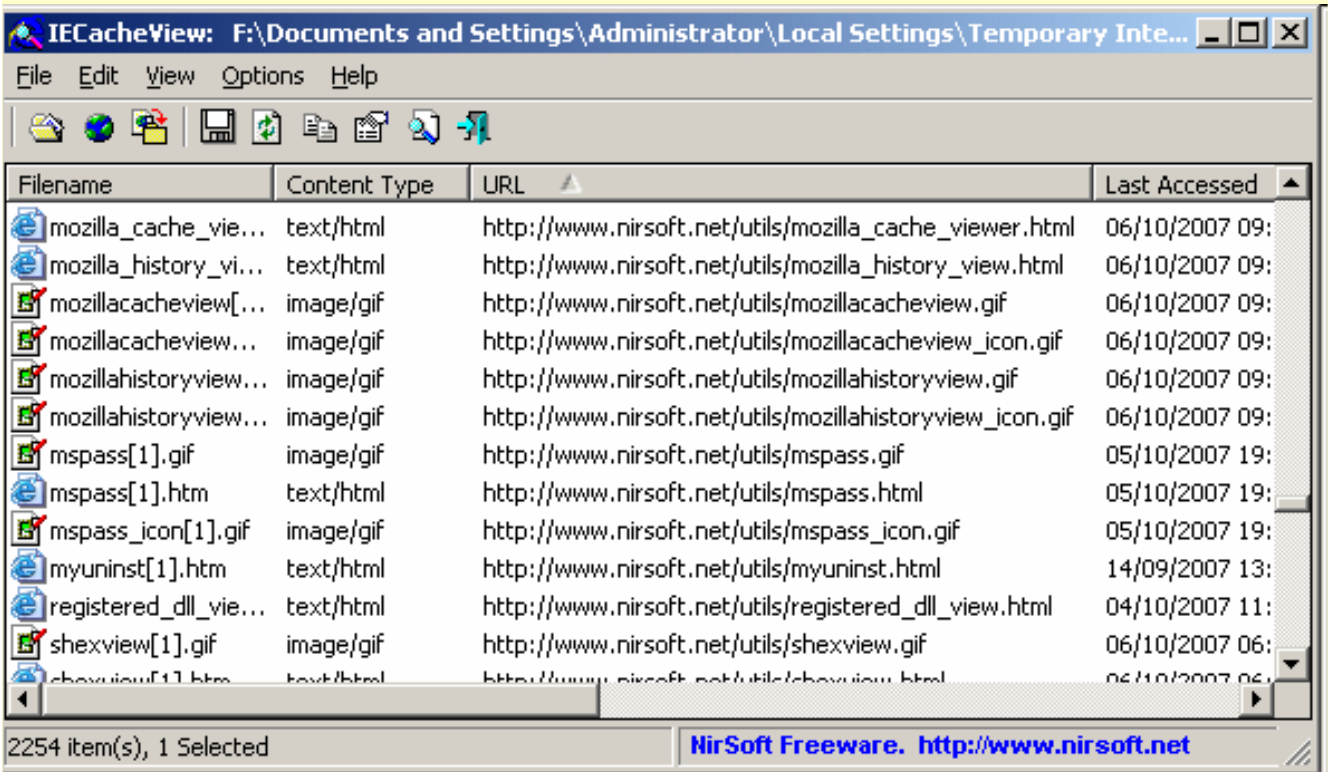
IECookieView

http://www.nirsoft.net/utils/iecookies.html



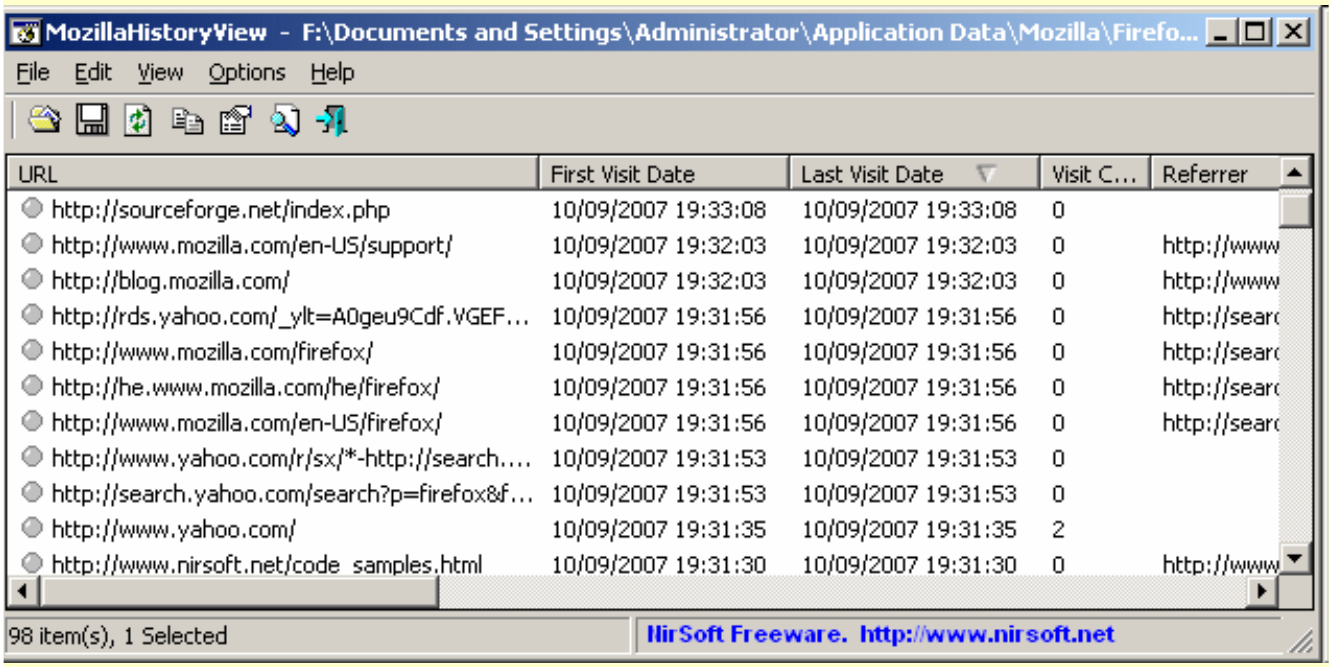
IECacheView

http://www.nirsoft.net/utils/ie_cache_viewer.html



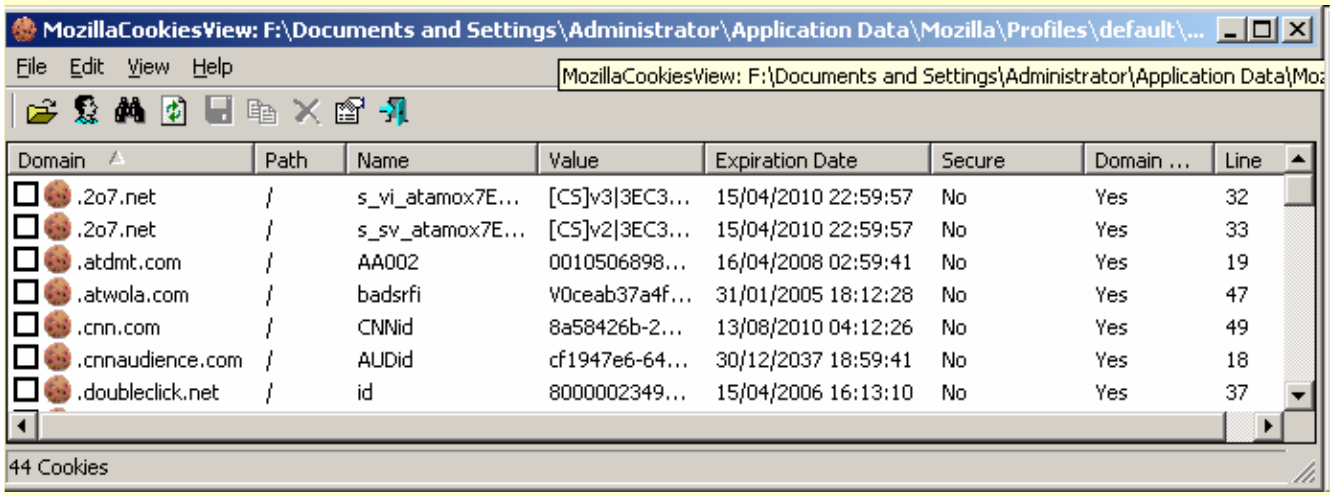
MozillaHistoryView

http://www.nirsoft.net/utils/mozilla_history_view.html



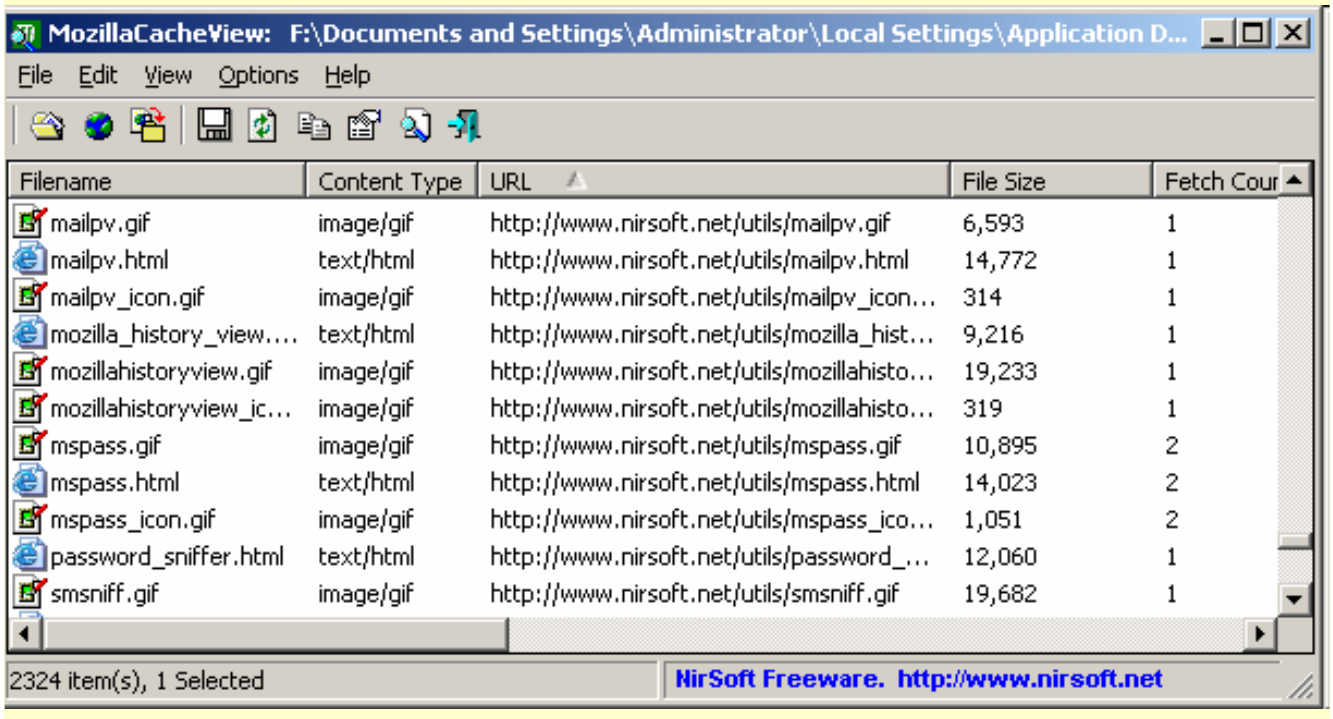
MozillaCookieView

http://www.nirsoft.net/utils/mozilla_cookie_view.html



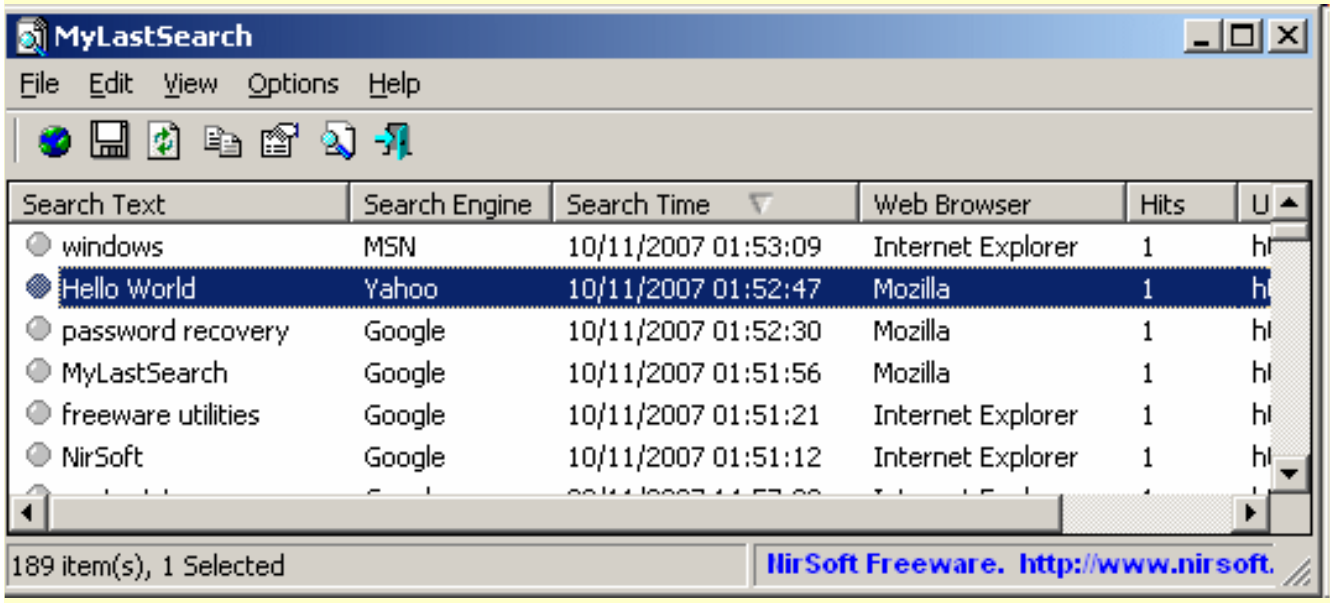
MozillaCacheView

http://www.nirsoft.net/utils/mozilla_cache_viewer.html

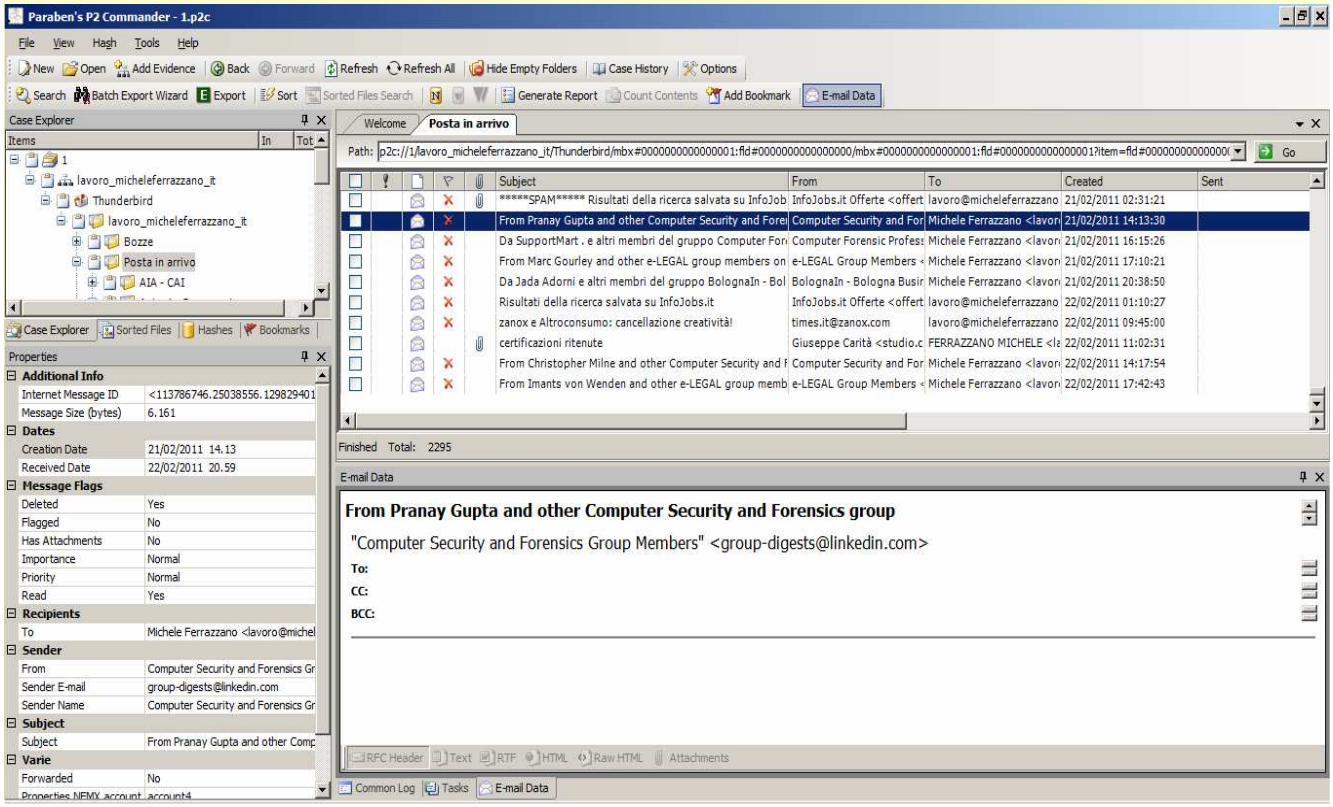


MyLastSearch

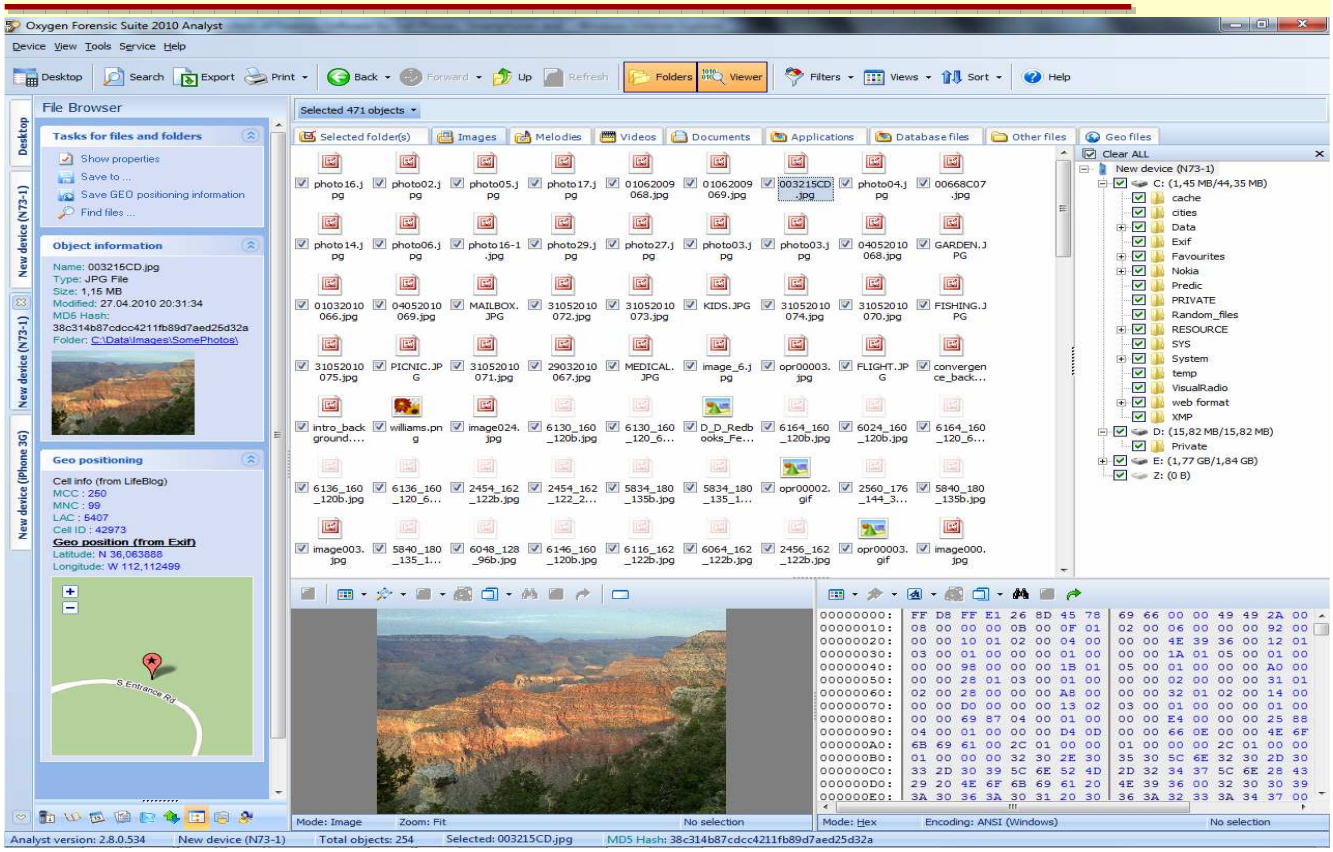
http://www.nirsoft.net/utils/my_last_search.html



Analisi - P2Commander



Analisi - Oxygen forensics

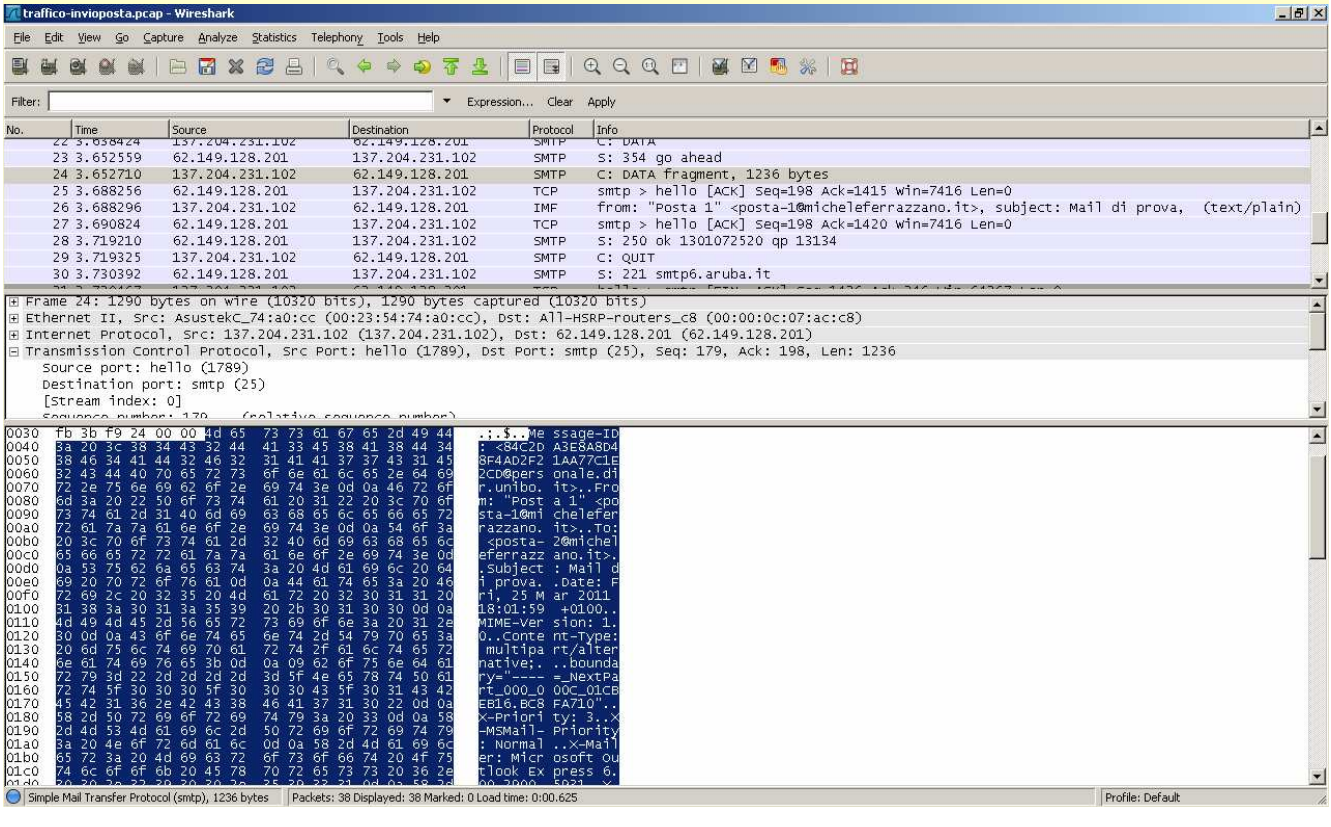


Analisi - emuleforensic

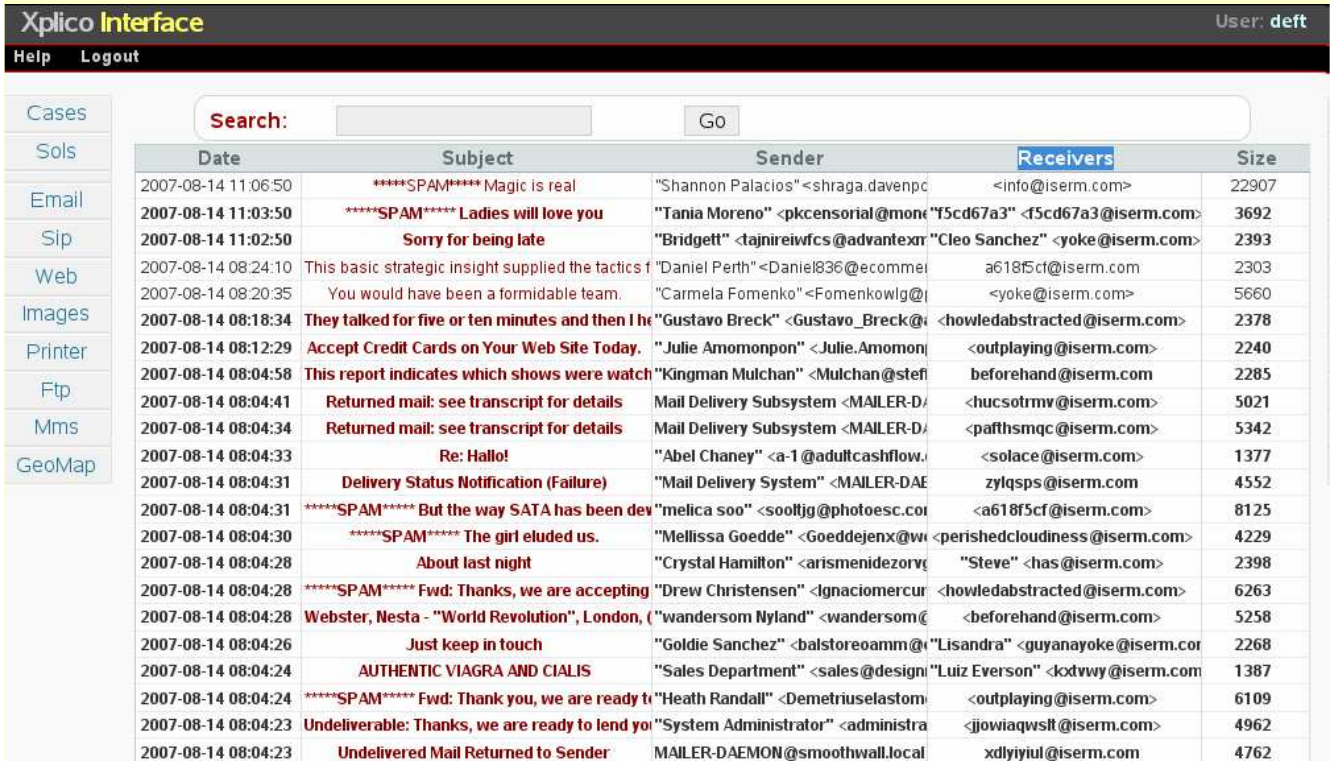
Analisi

NETWORK FORENSICS

Wireshark



Xplico



Xplico

Laboratorio

LABORATORIO INFORMATICA FORENSE LOW-COST

Hardware per l'attività di laboratorio

PC e notebook	**XXX €**
Lettori di supporti e cavi (di tutti i tipi)	
BluRay	XX €
DVD	**XX €**
CD	**XX €**
Hard-disk	**X – XX €**
Floppy 3,5''	X – XX €
Cavi per telefoni cellulari	X – XXX €
Copiatori	XXX – XXXX €
Write blocker	XXX – XXXX €

Investimento iniziale minimo: alcune centinaia di €

Software per l'attività di laboratorio

Sistema operativo	
Windows	XXX €
Linux (es: DEFT)	**0 €**
Software per acquisizione (DF)	
EnCase	XXXX €
FTK Imager	**0 €**
dd	**0 €**
Software per acquisizione (NF)	
Wireshark	**0 €**

Investimento iniziale minimo: 0 €

Software per l'attività di laboratorio

Software per analisi (DF)	
Encase	XXXX €
Autopsy	**0 €**
FTK Imager	**0 €**
NetAnalisyis	XXX €
FTK	XXXX €
P2Commander	XXX €
Software vari Nirsoft	**0 €**
Software per analisi (NF)	
Wireshark	**0 €**
Xplico	**0 €**

Investimento iniziale minimo: 0 €