Computer forensics

Laboratorio

Michele Ferrazzano

8 aprile 2013

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

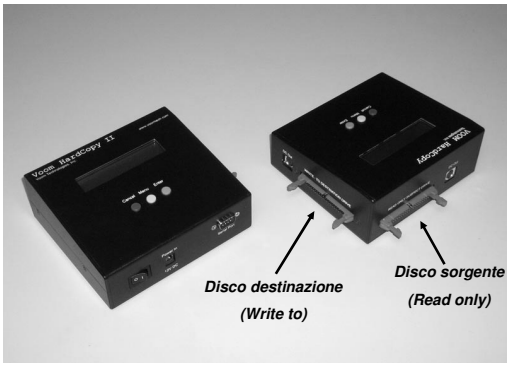
Software per l'attività di laboratorio

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

Acquisizione

DISK FORENSICS

Copiatore hardware

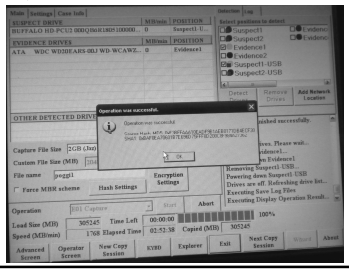


Copiatore hardware (es: Logicube Talon)

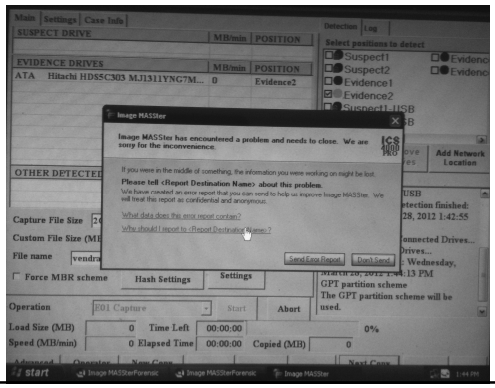
Copiatore hardware (es: ICS Image Master)

IM Solo-4 IT Hard Drive Duplicator - Non Expandable
Our Price: $2,900.00 ADD TO CART

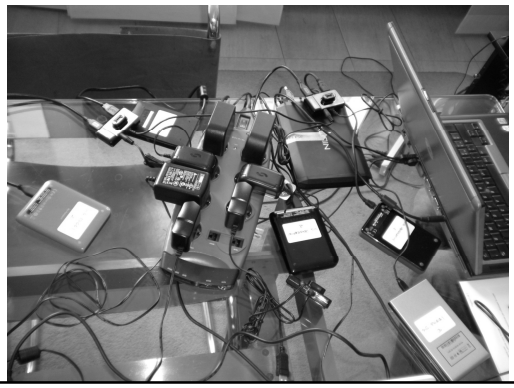
Image MASSter Solo-4 IT unit (designed exclusively for IT applications) is a versatile light weight, portable, high speed data duplication device. Capable of copying/duplicating/cloning/imaging two Source drives simultaneously or duplicating from one Source drive to 3 Target drives. Source drive's data can be copied at speeds exceeding 7GB per minute and is designed to support up to 18GB/min transfer rates for tomorrow's advanced drives. Test using Solid State Drives produced transfer rate as high as 12GB/min. The unit offers flexible Copy Mode formats known as "IQCopy" and "Image Copy". The IQCopy format provides an "intelligent" method of copying and scaling partitions. Only used clusters are copied, greatly reducing the time to copy. IQCopy supports the FAT16, FAT32, exFAT and NTFS File Systems. The IQCopy-Linux Option can be purchased separately to add Linux support. The unit has a built-in Gigabit Ethernet port which can be used to copy data to or from Shared Network Folders. More info



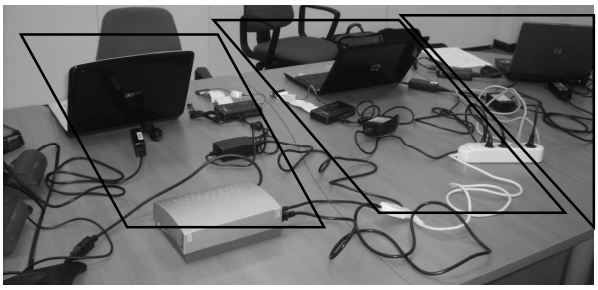
Copiatore hardware (es: ICS Image Master)



Il consulente tecnico frettoloso



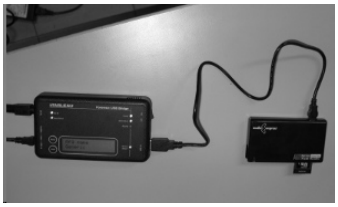
Il consulente tecnico ordinato



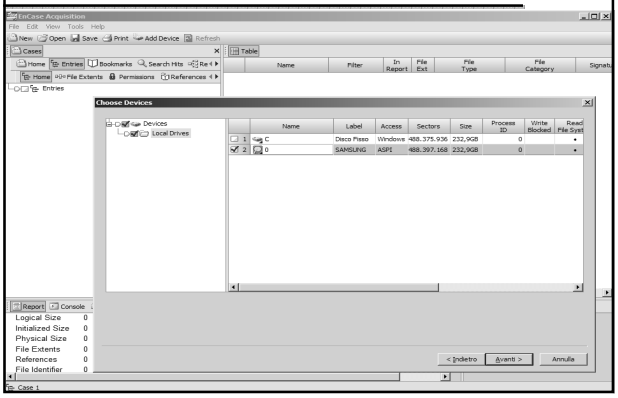
Write blocker

- 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

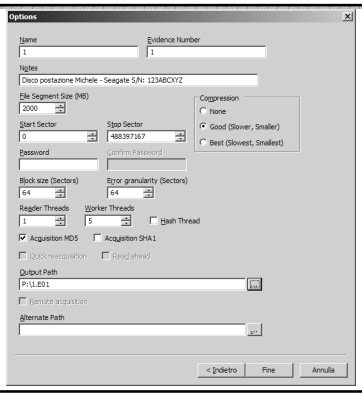
Write blocker



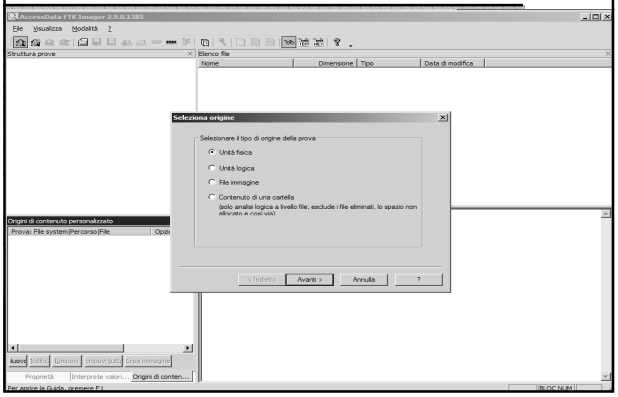
Acquisizione – Encase



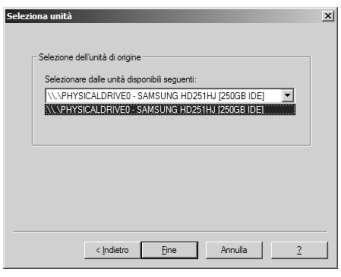
Acquisizione - Encase



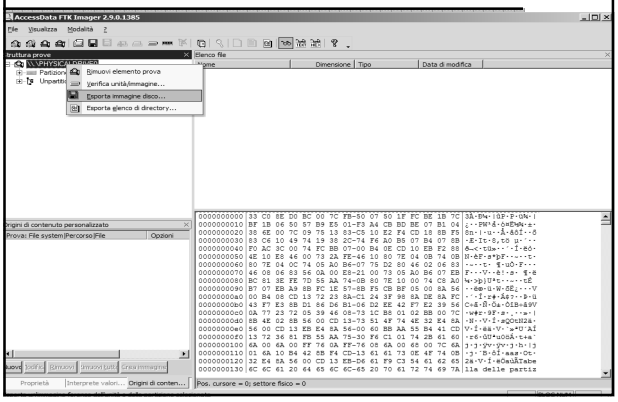
Acquisizione - FTK Imager



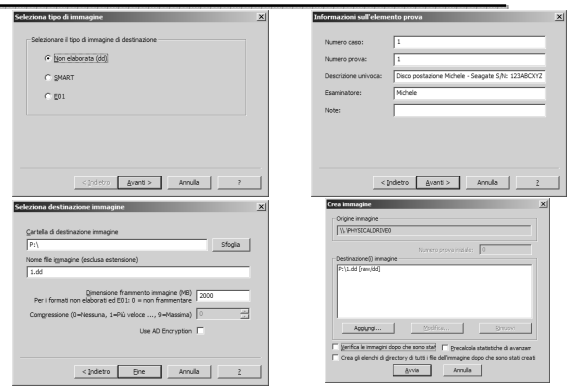
Acquisizione - FTK Imager



Acquisizione - FTK Imager

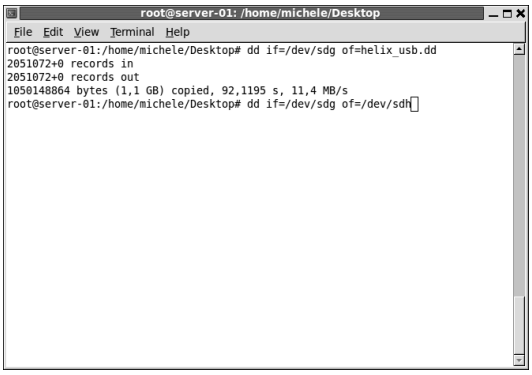


Acquisizione – FTK Imager



Acquisizione – Dispositivi *mobile*

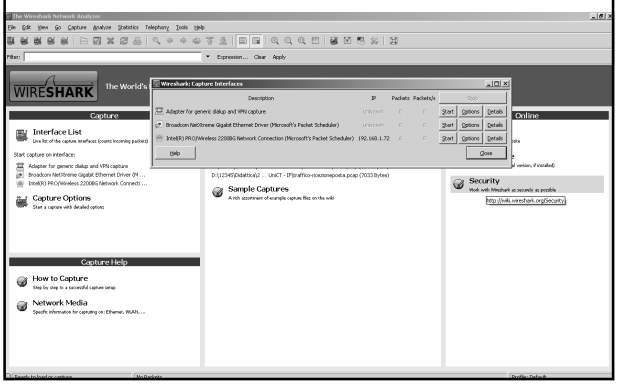
Acquisizione – dd



Analisi

NETWORK FORENSICS

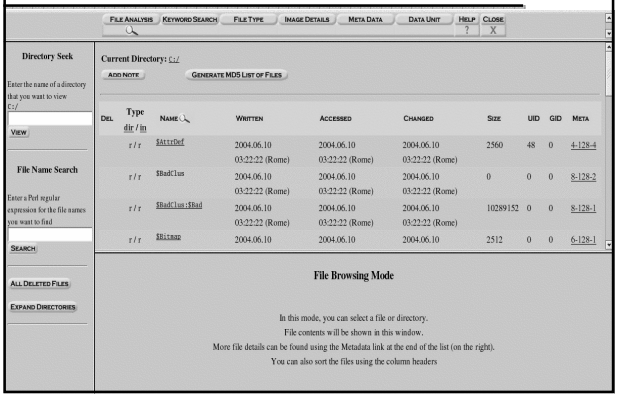
Wireshark



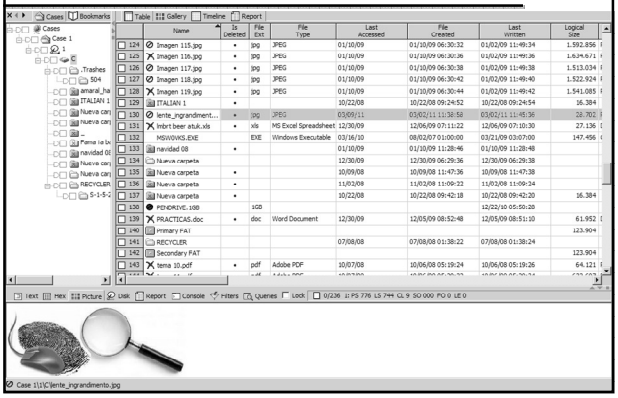
Analisi

DISK FORENSICS

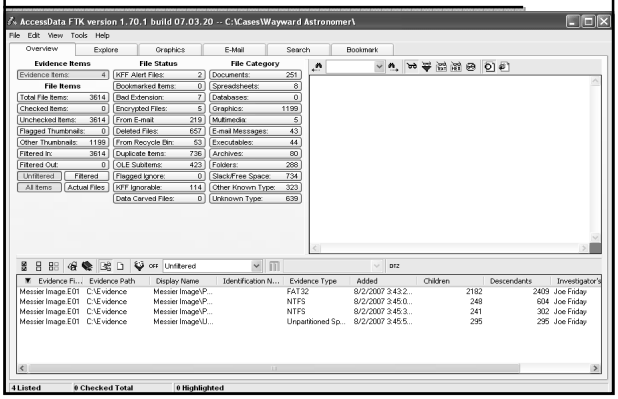
Analisi - Autopsy



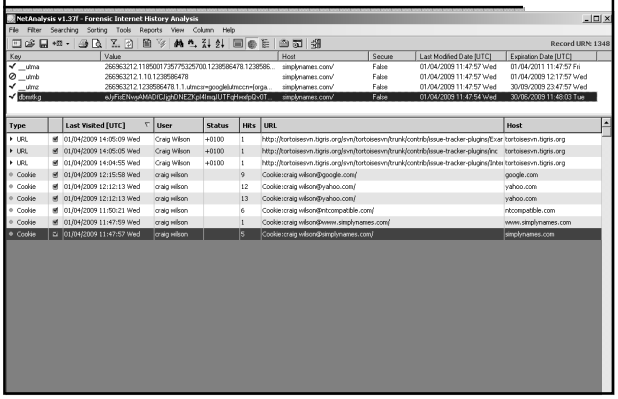
Analisi - Encase



Analisi - FTK (Forensic ToolKit)

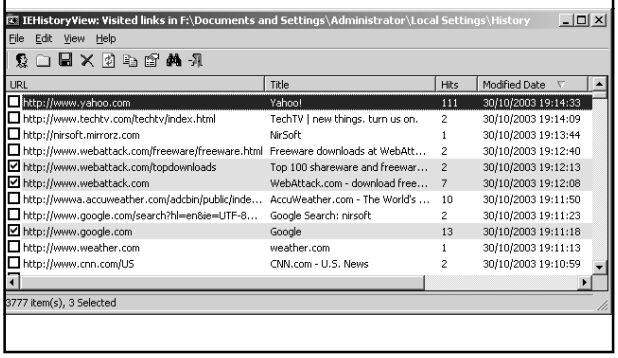


Analisi - NetAnalysis



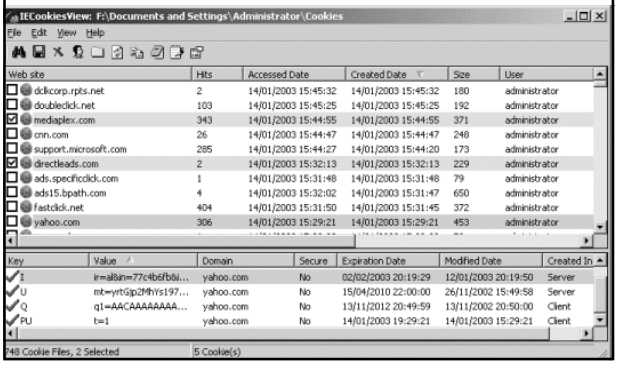
IEHistoryView

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



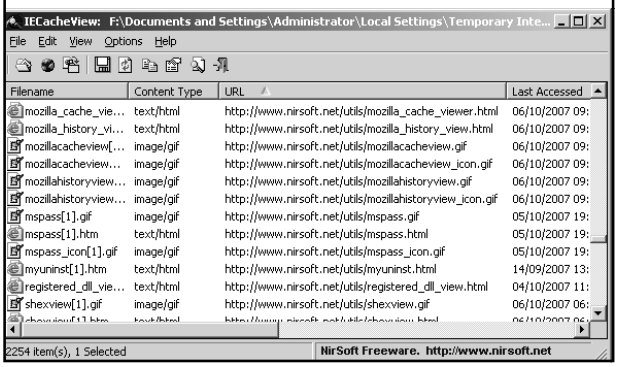
IECookieView

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



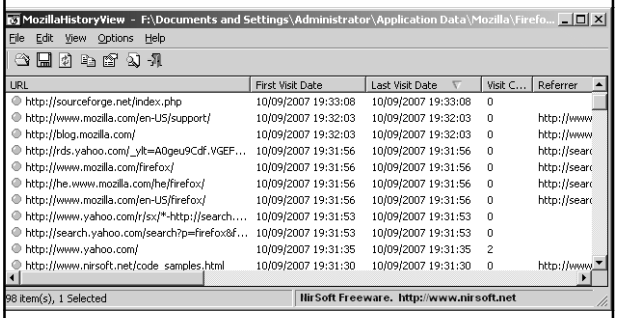
IECacheView

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



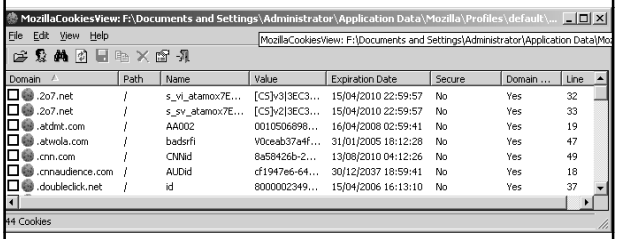
MozillaHistoryView

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



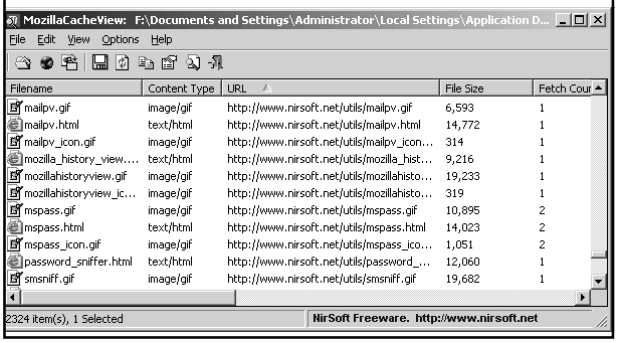
MozillaCookieView

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



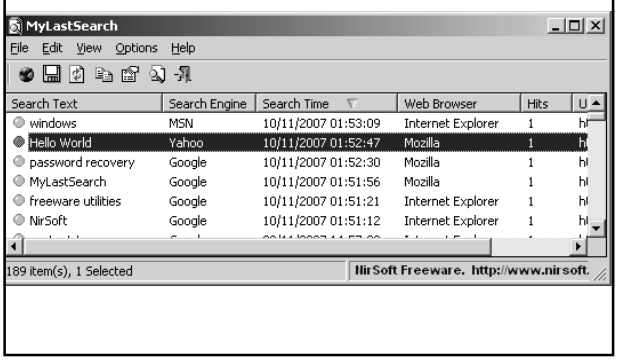
MozillaCacheView

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

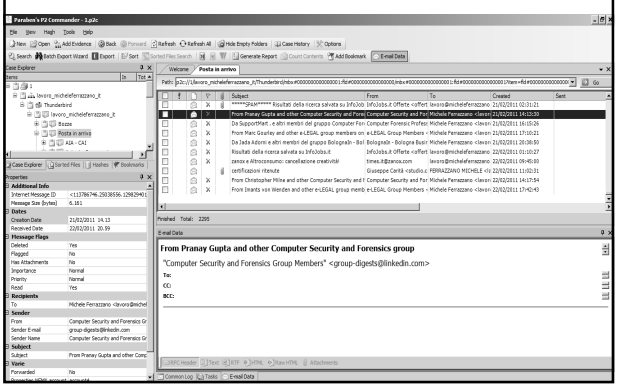


MyLastSearch

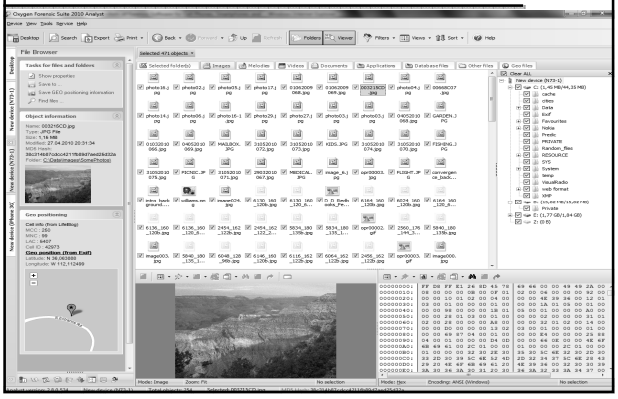
http://www.nirsoft.net/utils/my_last_search.html



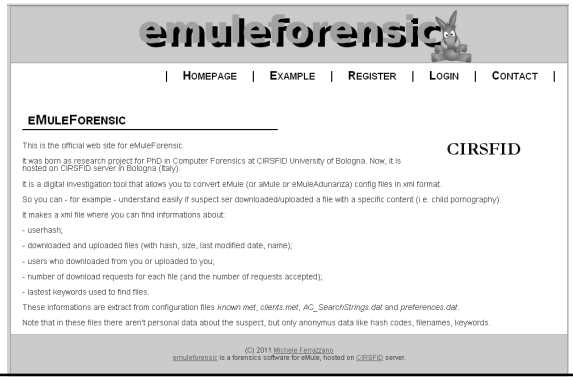
Analisi - P2Commander



Analisi - Oxygen forensics



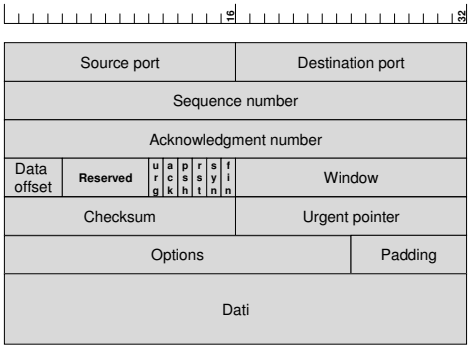
Analisi - emuleforensic



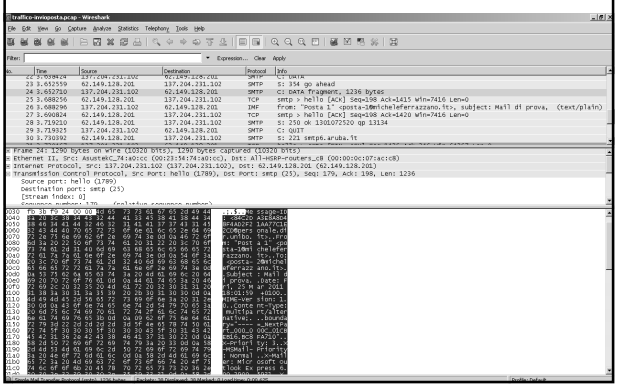
Analisi

NETWORK FORENSICS

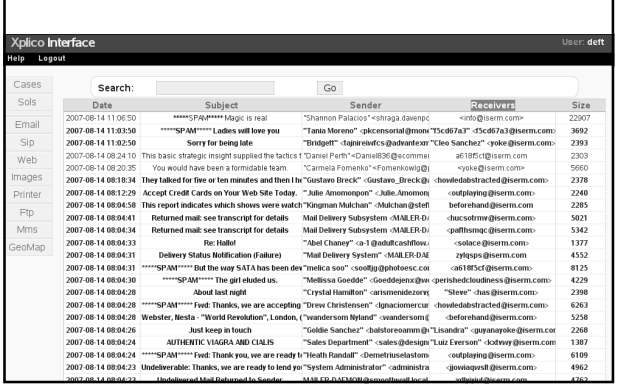
Pacchetto TCP



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, dcfldd	**0 €**
Software per acquisizione (NF)	
Wireshark	**0 €**

Investimento iniziale minimo: 0 €

Software per l'attività di laboratorio

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

Investimento iniziale minimo: 0 €