

Informatica forense

Laboratorio

Michele Ferrazzano

23 aprile 2012

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

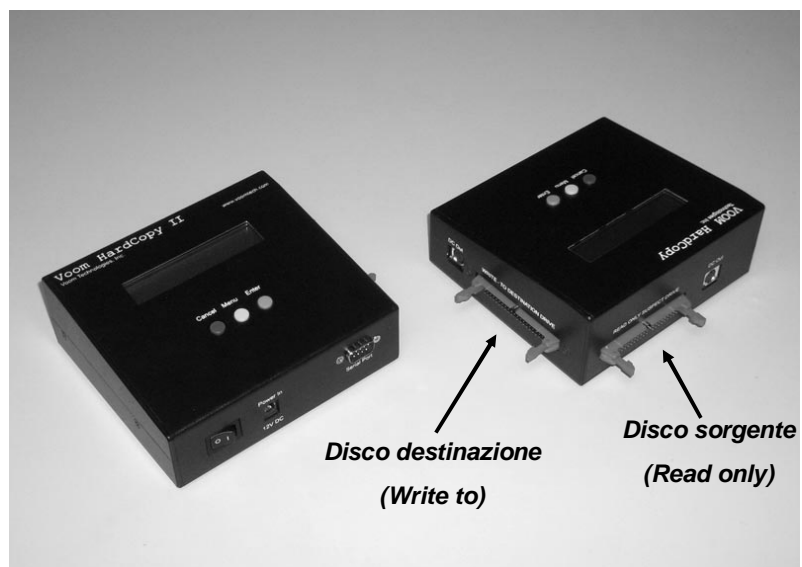
Software per l'attività di laboratorio

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

Acquisizione

DISK FORENSICS


Copiatore hardware



Copiatore hardware (es: Logicube Talon)

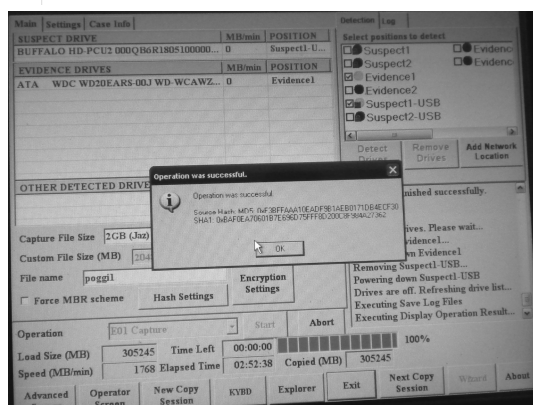


Copiatore hardware (es: ICS Image Master)



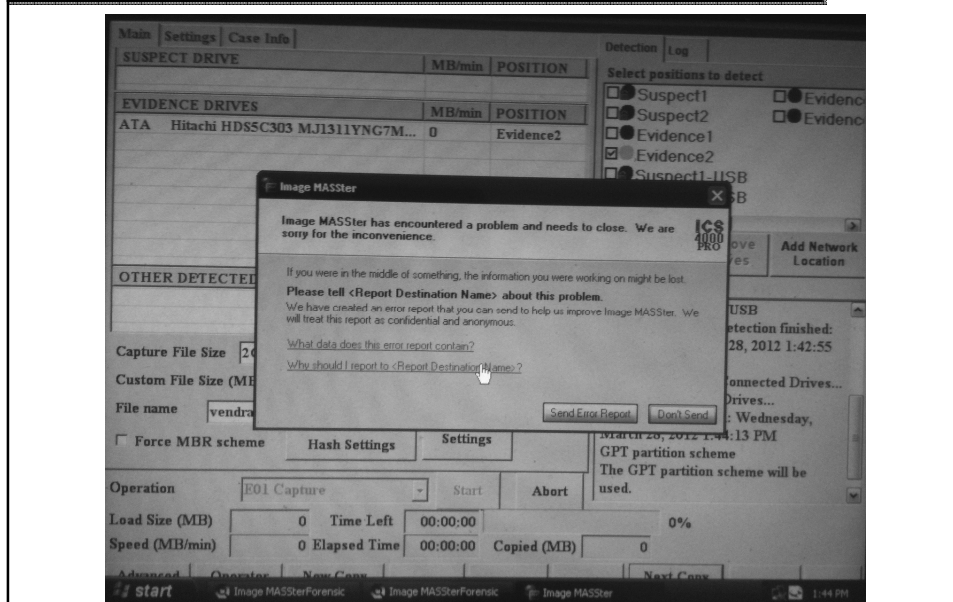
IM Solo-4 IT Hard Drive Duplicator - Non Expandable
 Our Price: \$2,900.00 [ADD TO CART](#) [»](#)

Image MASter 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 19GB/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 FAT15, 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](#)



The screenshot shows the ICS Image Master software interface. It includes a 'Main' menu with 'Settings' and 'Case Info'. The 'SUSPECT DRIVE' section shows a Buffalo HD-PCU2 000Q86R180S100000... drive. The 'EVIDENCE DRIVES' section shows an ATA WDC WD20EARS-00JWD-WCAWZ... drive. The 'OTHER DETECTED DRIVES' section shows a capture file size of 2GB (320) and a custom file size of 2048. The 'Operation' section shows a progress bar at 100% and a time left of 00:00:00. The 'Advanced Screen' shows the 'Operator' screen with a 'New Copy Session' button.

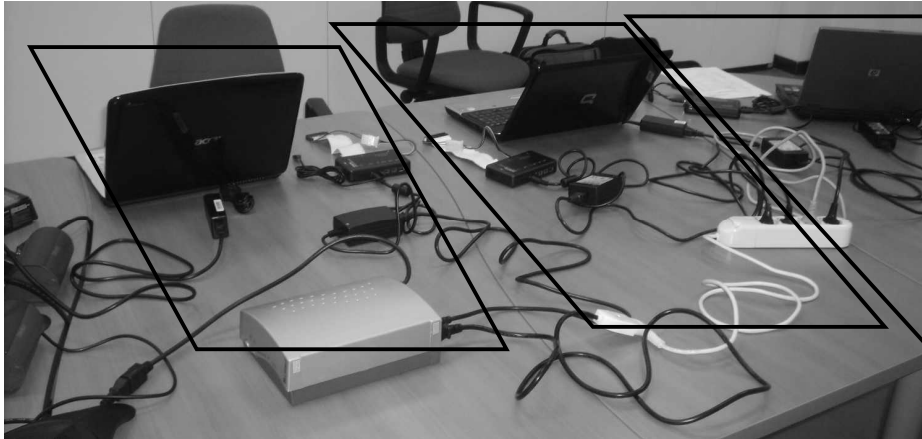
Copiatore hardware (es: ICS Image Master)



Il consulente tecnico frettoloso



Il consulente tecnico ordinato



Write blocker

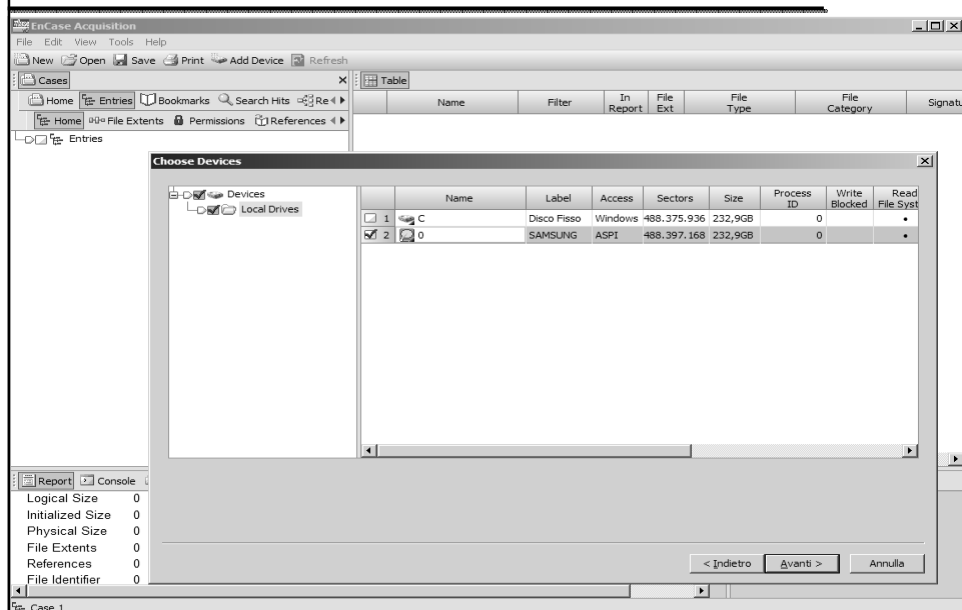
- Un write blocker è un dispositivo usato per prevenire scritture (anche accidentali) su hard disk oggetto di investigazioni
- Il write blocker è posto tra il disco esaminato e il computer utilizzato per esaminarlo o acquisirlo



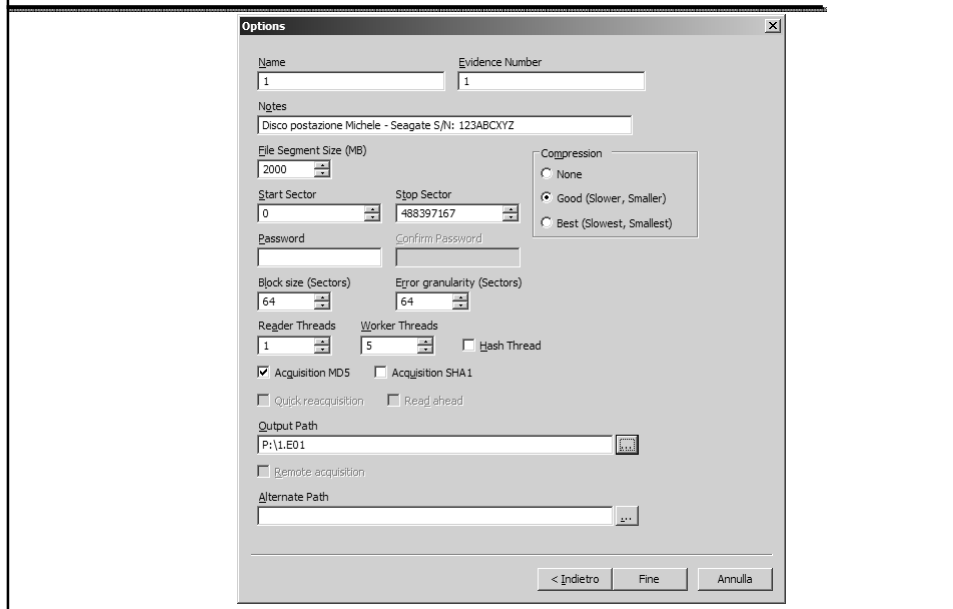
Write blocker



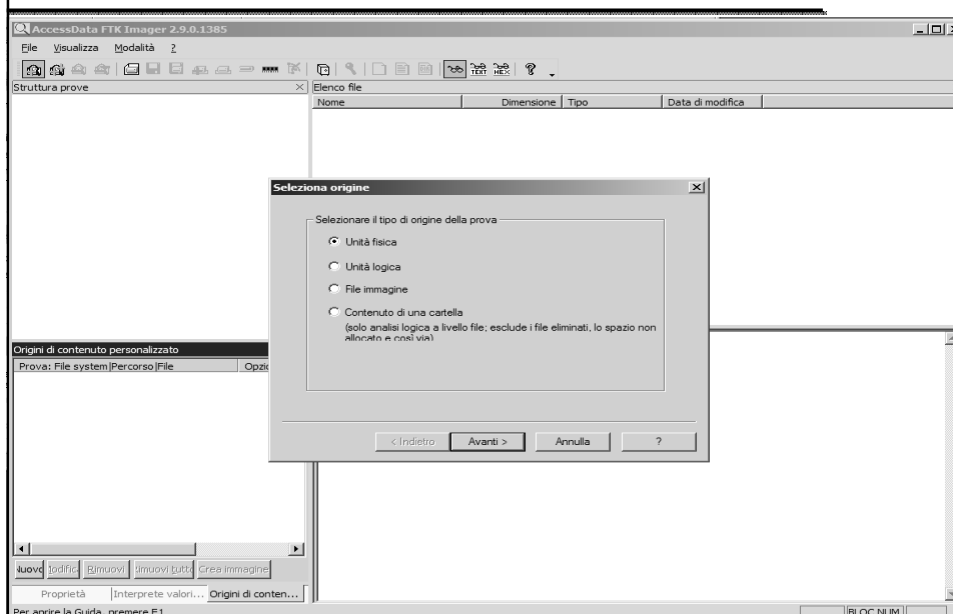
Acquisizione – Encase



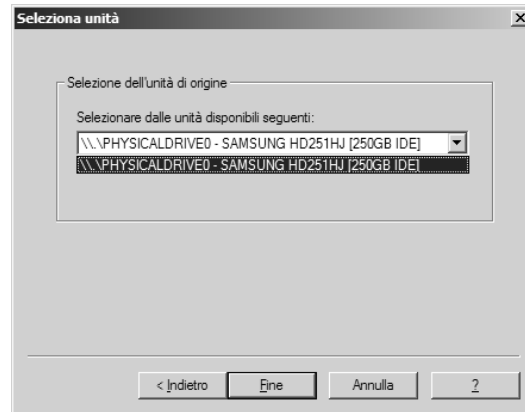
Acquisizione - Encase



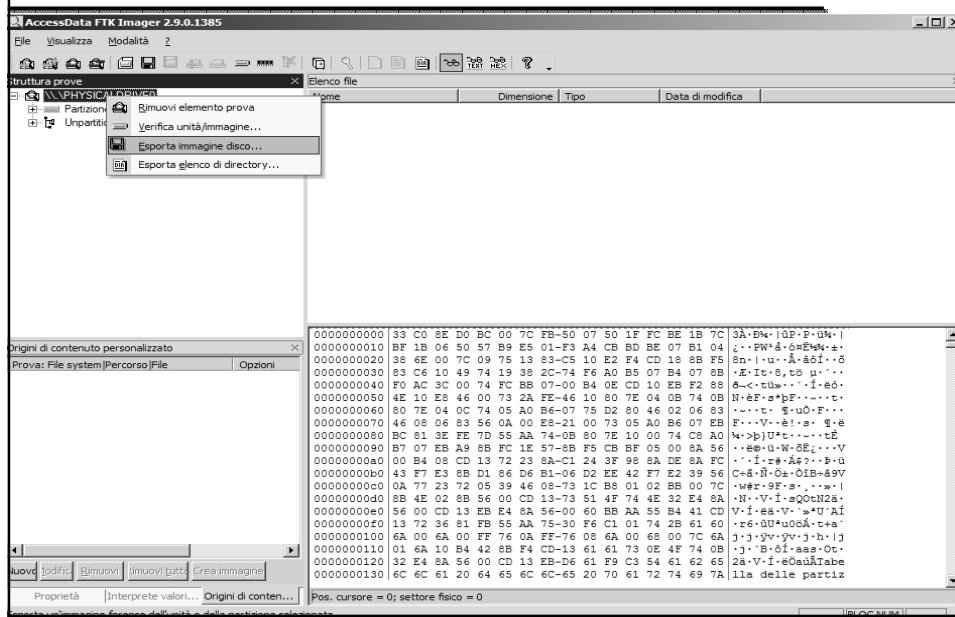
Acquisizione - FTK Imager



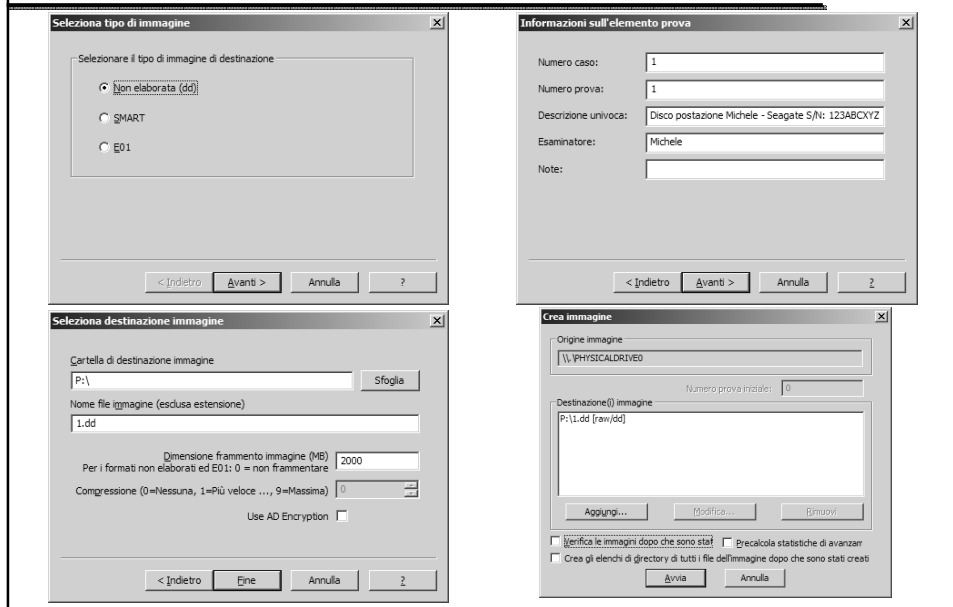
Acquisizione - FTK Imager



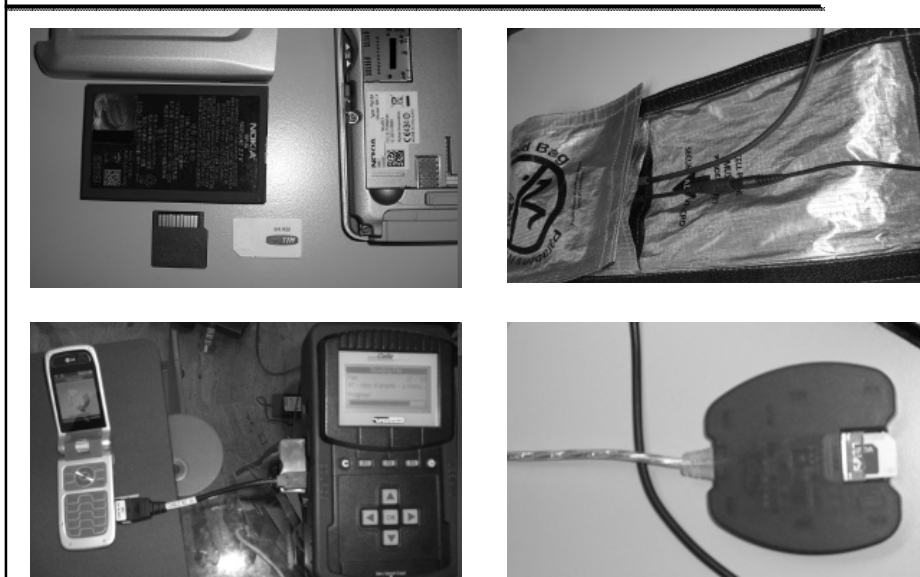
Acquisizione - FTK Imager



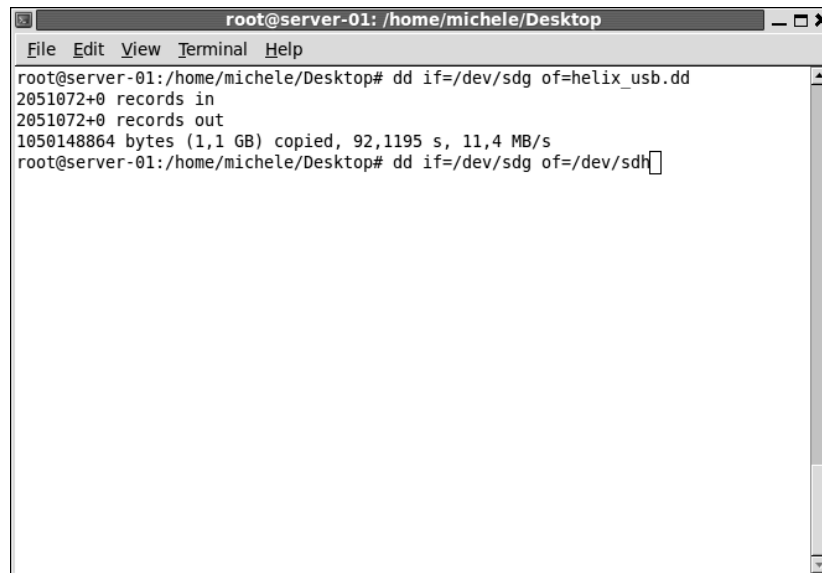
Acquisizione – FTK Imager



Acquisizione – Dispositivi *mobile*



Acquisizione – dd

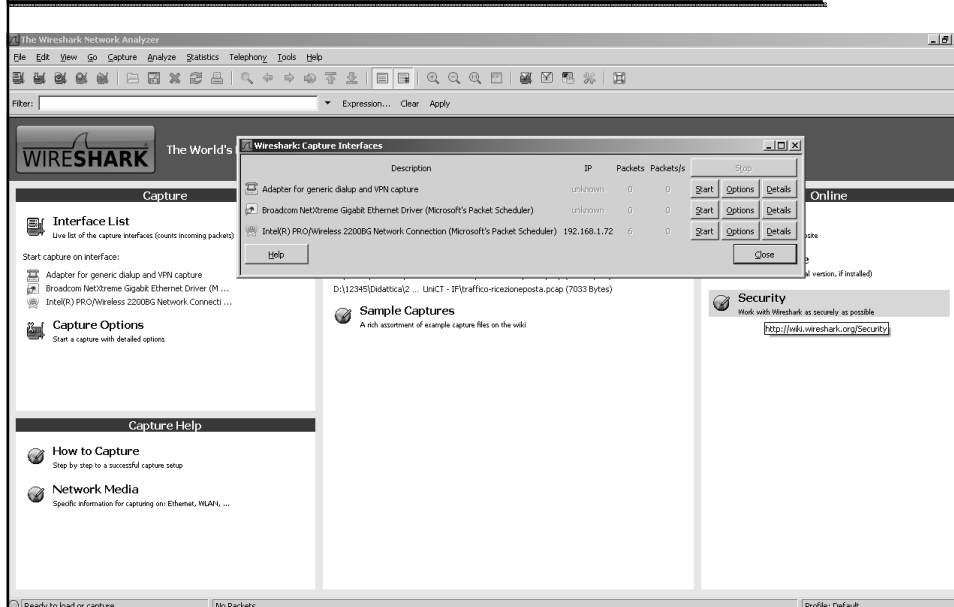


```
root@server-01: /home/michele/Desktop
File Edit View Terminal Help
root@server-01:/home/michele/Desktop# dd if=/dev/sdg of=helix_usb.dd
2051072+0 records in
2051072+0 records out
1050148864 bytes (1,1 GB) copied, 92,1195 s, 11,4 MB/s
root@server-01:/home/michele/Desktop# dd if=/dev/sdg of=/dev/sdh
```

Analisi

***NETWORK
FORENSICS***

Wireshark



Analisi

DISK FORENSICS

Analisi – Autopsy



Analisi - Autopsy

FILE ANALYSIS

KEYWORD SEARCH

FILE TYPE

IMAGE DETAILS

META DATA

DATA UNIT

HELP

CLOSE

Directory Seek

Enter the name of a directory that you want to view
C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

Current Directory: C:/

ADD NOTE

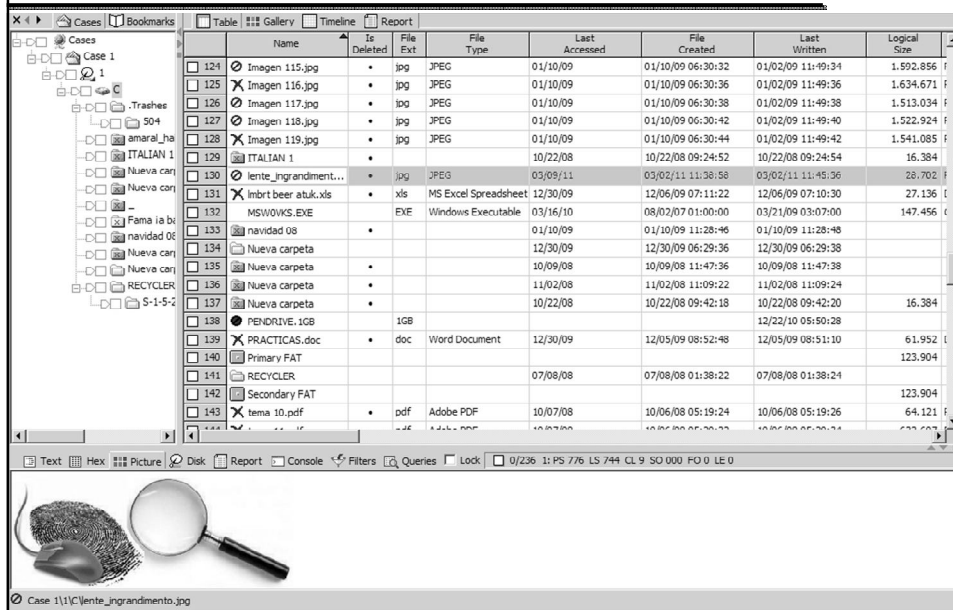
GENERATE MDS LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META
	r / r	\$AttrDef	2004.06.10 03:22:22 (Rome)	2004.06.10 03:22:22 (Rome)	2004.06.10 03:22:22 (Rome)	2560	48	0	4-128-4
	r / r	\$BadClus	2004.06.10 03:22:22 (Rome)	2004.06.10 03:22:22 (Rome)	2004.06.10 03:22:22 (Rome)	0	0	0	8-128-2
	r / r	\$BadClus:\$Bad	2004.06.10 03:22:22 (Rome)	2004.06.10 03:22:22 (Rome)	2004.06.10 03:22:22 (Rome)	10289152	0	0	8-128-1
	r / r	\$BitMap	2004.06.10	2004.06.10	2004.06.10	2512	0	0	6-128-1

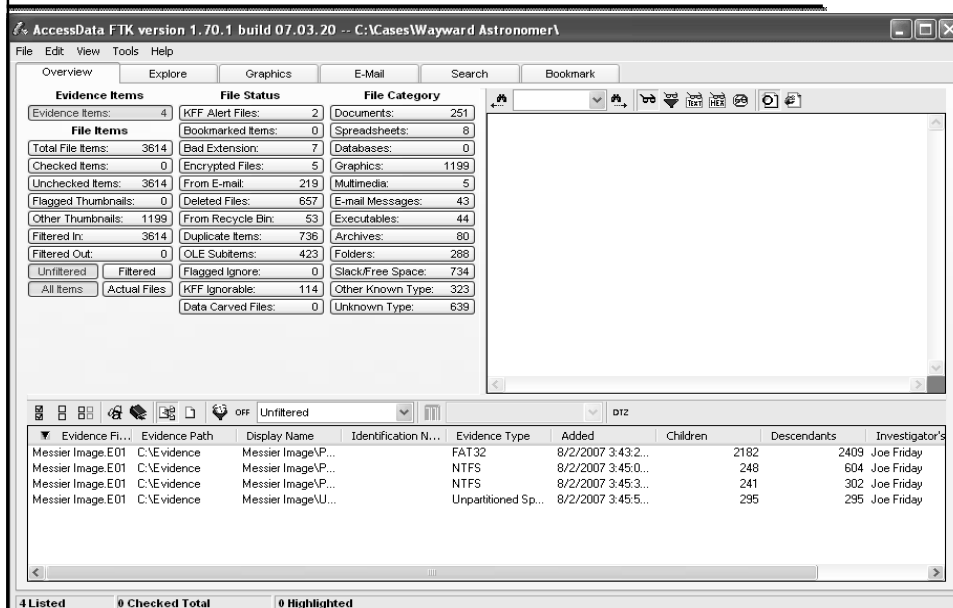
File Browsing Mode

In this mode, you can select a file or directory.
File contents will be shown in this window.
More file details can be found using the Metadata link at the end of the list (on the right).
You can also sort the files using the column headers

Analisi - Encase



Analisi - FTK (Forensic ToolKit)



Analisi - NetAnalysis

NetAnalysis v1.37f - Forensic Internet History Analysis

File Filter Searching Sorting Tools Reports View Column Help

Record URN: 1348

Key	Value	Host	Secure	Last Modified Date [UTC]	Expiration Date [UTC]
✓ _utma	266963212.1105001735775325700.1238586478.1238586...	simplynames.com/	False	01/04/2009 11:47:57 Wed	01/04/2011 11:47:57 Fri
✓ _utmb	266963212.1.10.1238586478	simplynames.com/	False	01/04/2009 11:47:57 Wed	01/04/2009 12:17:57 Wed
✓ _utmz	266963212.1238586478.1.1.utmcsr=googleutmccn=orga...	simplynames.com/	False	01/04/2009 11:47:57 Wed	30/09/2009 23:47:57 Wed
✓ dbmrtkg	6jYfIEENwAMADICjgIDNEZKp4ImglUTFGHwtpQV0T...	simplynames.com/	False	01/04/2009 11:47:54 Wed	30/06/2009 11:48:03 Tue

Type	Last Visited [UTC]	User	Status	Hits	URL	Host
▶ URL	01/04/2009 14:05:09 Wed	Craig Wilson	+0100	1	http://tortoisefvn.tigris.org/svn/tortoisefvn/trunk/contrib/issue-tracker-plugins/Exar	tortoisefvn.tigris.org
▶ URL	01/04/2009 14:05:05 Wed	Craig Wilson	+0100	1	http://tortoisefvn.tigris.org/svn/tortoisefvn/trunk/contrib/issue-tracker-plugins/Inc	tortoisefvn.tigris.org
▶ URL	01/04/2009 14:04:55 Wed	Craig Wilson	+0100	1	http://tortoisefvn.tigris.org/svn/tortoisefvn/trunk/contrib/issue-tracker-plugins/Inte	tortoisefvn.tigris.org
• Cookie	01/04/2009 12:15:58 Wed	craig wilson		9	Cookie:craig wilson@google.com/	google.com
• Cookie	01/04/2009 12:12:13 Wed	craig wilson		12	Cookie:craig wilson@yahoo.com/	yahoo.com
• Cookie	01/04/2009 12:12:13 Wed	craig wilson		13	Cookie:craig wilson@yahoo.com/	yahoo.com
• Cookie	01/04/2009 11:50:21 Wed	craig wilson		6	Cookie:craig wilson@ntcompatible.com/	ntcompatible.com
• Cookie	01/04/2009 11:47:59 Wed	craig wilson		1	Cookie:craig wilson@www.simplynames.com/	www.simplynames.com
• Cookie	01/04/2009 11:47:57 Wed	craig wilson		5	Cookie:craig wilson@simplynames.com/	simplynames.com

IEHistoryView

<http://www.nirsoft.net/utills/iehv.html>

IEHistoryView: Visited links in F:\Documents and Settings\Administrator\Local Settings\History

File Edit View Help

URL	Title	Hits	Modified Date
<input type="checkbox"/> http://www.yahoo.com	Yahoo!	111	30/10/2003 19:14:33
<input type="checkbox"/> http://www.techtv.com/techtv/index.html	TechTV new things. turn us on.	2	30/10/2003 19:14:09
<input type="checkbox"/> http://nirsoft.mirrorz.com	NirSoft	1	30/10/2003 19:13:44
<input type="checkbox"/> http://www.webattack.com/freeware/freeware.html	Freeware downloads at WebAtt...	2	30/10/2003 19:12:40
<input checked="" type="checkbox"/> http://www.webattack.com/topdownloads	Top 100 shareware and freewar...	2	30/10/2003 19:12:13
<input checked="" type="checkbox"/> http://www.webattack.com	WebAttack.com - download free...	7	30/10/2003 19:12:08
<input type="checkbox"/> http://www.accuweather.com/adcbn/public/inde...	AccuWeather.com - The World's ...	10	30/10/2003 19:11:50
<input type="checkbox"/> http://www.google.com/search?hl=en&ie=UTF-8...	Google Search: nirsoft	2	30/10/2003 19:11:23
<input checked="" type="checkbox"/> http://www.google.com	Google	13	30/10/2003 19:11:18
<input type="checkbox"/> http://www.weather.com	weather.com	1	30/10/2003 19:11:13
<input type="checkbox"/> http://www.cnn.com/US	CNN.com - U.S. News	2	30/10/2003 19:10:59

3777 item(s), 3 Selected

IECookieView

<http://www.nirsoft.net/utills/iecookies.html>

IECookiesView: F:\Documents and Settings\Administrator\Cookies

File Edit View Help

Web site	Hits	Accessed Date	Created Date	Size	User
<input type="checkbox"/> dclcorp.rpts.net	2	14/01/2003 15:45:32	14/01/2003 15:45:32	180	administrator
<input type="checkbox"/> doubledclick.net	103	14/01/2003 15:45:25	14/01/2003 15:45:25	192	administrator
<input checked="" type="checkbox"/> mediaplex.com	343	14/01/2003 15:44:55	14/01/2003 15:44:55	371	administrator
<input type="checkbox"/> cnn.com	26	14/01/2003 15:44:47	14/01/2003 15:44:47	248	administrator
<input type="checkbox"/> support.microsoft.com	285	14/01/2003 15:44:27	14/01/2003 15:44:20	173	administrator
<input checked="" type="checkbox"/> directleads.com	2	14/01/2003 15:32:13	14/01/2003 15:32:13	229	administrator
<input type="checkbox"/> ads.specificclick.com	1	14/01/2003 15:31:48	14/01/2003 15:31:48	79	administrator
<input type="checkbox"/> ads15.bpath.com	4	14/01/2003 15:32:02	14/01/2003 15:31:47	650	administrator
<input type="checkbox"/> fastclick.net	404	14/01/2003 15:31:50	14/01/2003 15:31:45	372	administrator
<input type="checkbox"/> yahoo.com	306	14/01/2003 15:29:21	14/01/2003 15:29:21	453	administrator

Key	Value	Domain	Secure	Expiration Date	Modified Date	Created In
<input checked="" type="checkbox"/> I	ir=a8in=77c4b6fb8u...	yahoo.com	No	02/02/2003 20:19:29	12/01/2003 20:19:50	Server
<input checked="" type="checkbox"/> U	mt=yrtGjp2MhYs197...	yahoo.com	No	15/04/2010 22:00:00	26/11/2002 15:49:58	Server
<input checked="" type="checkbox"/> Q	q1=AAACAAAAA...	yahoo.com	No	13/11/2012 20:49:59	13/11/2002 20:50:00	Client
<input checked="" type="checkbox"/> PU	t=1	yahoo.com	No	14/01/2003 19:29:21	14/01/2003 15:29:21	Client

748 Cookie Files, 2 Selected 5 Cookie(s)

IECacheView

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

IECacheView: F:\Documents and Settings\Administrator\Local Settings\Temporary Inte...

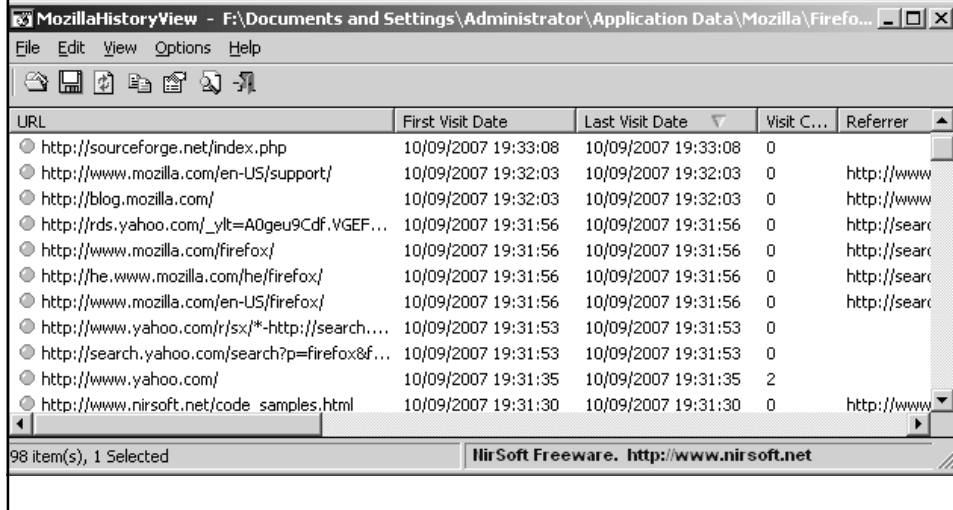
File Edit View Options Help

Filename	Content Type	URL	Last Accessed
mozilla_cache_vie...	text/html	http://www.nirsoft.net/utills/mozilla_cache_viewer.html	06/10/2007 09:
mozilla_history_vi...	text/html	http://www.nirsoft.net/utills/mozilla_history_view.html	06/10/2007 09:
mozillacacheview[...	image/gif	http://www.nirsoft.net/utills/mozillacacheview.gif	06/10/2007 09:
mozillacacheview[...	image/gif	http://www.nirsoft.net/utills/mozillacacheview_icon.gif	06/10/2007 09:
mozillahistoryview...	image/gif	http://www.nirsoft.net/utills/mozillahistoryview.gif	06/10/2007 09:
mozillahistoryview...	image/gif	http://www.nirsoft.net/utills/mozillahistoryview_icon.gif	06/10/2007 09:
mypass[1].gif	image/gif	http://www.nirsoft.net/utills/mypass.gif	05/10/2007 19:
mypass[1].htm	text/html	http://www.nirsoft.net/utills/mypass.html	05/10/2007 19:
mypass_icon[1].gif	image/gif	http://www.nirsoft.net/utills/mypass_icon.gif	05/10/2007 19:
myuninst[1].htm	text/html	http://www.nirsoft.net/utills/myuninst.html	14/09/2007 13:
registered_dll_vie...	text/html	http://www.nirsoft.net/utills/registered_dll_view.html	04/10/2007 11:
shexview[1].gif	image/gif	http://www.nirsoft.net/utills/shexview.gif	06/10/2007 06:
shexview[1].htm	text/html	http://www.nirsoft.net/utills/shexview.html	06/10/2007 06:

2254 item(s), 1 Selected NirSoft Freeware. <http://www.nirsoft.net>

MozillaHistoryView

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



MozillaHistoryView - F:\Documents and Settings\Administrator\Application Data\Mozilla\Firefo...

File Edit View Options Help

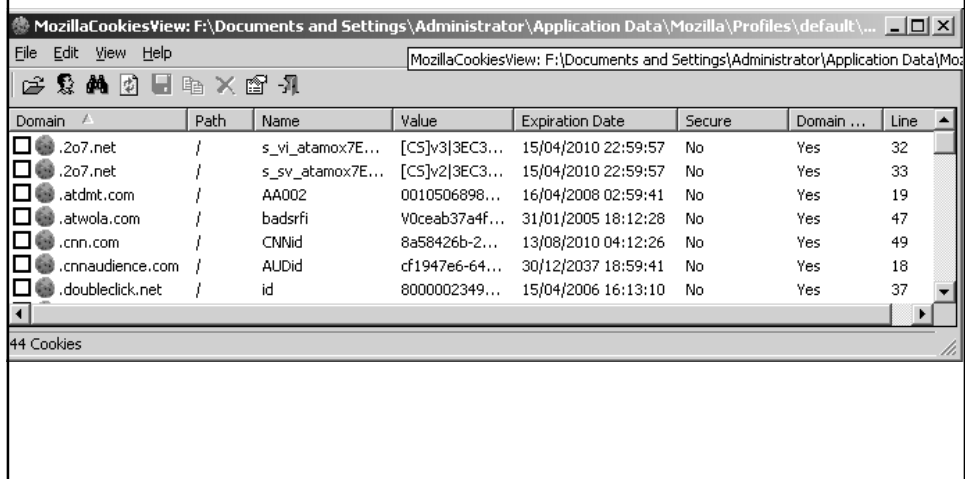
URL	First Visit Date	Last Visit Date	Visit C...	Referrer
http://sourceforge.net/index.php	10/09/2007 19:33:08	10/09/2007 19:33:08	0	
http://www.mozilla.com/en-US/support/	10/09/2007 19:32:03	10/09/2007 19:32:03	0	http://www
http://blog.mozilla.com/	10/09/2007 19:32:03	10/09/2007 19:32:03	0	http://www
http://rds.yahoo.com/_ylt=A0geu9Cdf.VGEF...	10/09/2007 19:31:56	10/09/2007 19:31:56	0	http://sear
http://www.mozilla.com/firefox/	10/09/2007 19:31:56	10/09/2007 19:31:56	0	http://sear
http://he.www.mozilla.com/he/firefox/	10/09/2007 19:31:56	10/09/2007 19:31:56	0	http://sear
http://www.mozilla.com/en-US/firefox/	10/09/2007 19:31:56	10/09/2007 19:31:56	0	http://sear
http://www.yahoo.com/r/sx/*-http://search...	10/09/2007 19:31:53	10/09/2007 19:31:53	0	
http://search.yahoo.com/search?p=firefox&f...	10/09/2007 19:31:53	10/09/2007 19:31:53	0	
http://www.yahoo.com/	10/09/2007 19:31:35	10/09/2007 19:31:35	2	
http://www.nirsoft.net/code_samples.html	10/09/2007 19:31:30	10/09/2007 19:31:30	0	http://www

98 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

MozillaCookieView

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



MozillaCookiesView - F:\Documents and Settings\Administrator\Application Data\Mozilla\Profiles\default\...

File Edit View Help

MozillaCookiesView: F:\Documents and Settings\Administrator\Application Data\Mo...

Domain	Path	Name	Value	Expiration Date	Secure	Domain ...	Line
.2o7.net	/	s_vi_atamox7E...	[CS]v3 3EC3...	15/04/2010 22:59:57	No	Yes	32
.2o7.net	/	s_sv_atamox7E...	[CS]v2 3EC3...	15/04/2010 22:59:57	No	Yes	33
.atdmt.com	/	AA002	0010506898...	16/04/2008 02:59:41	No	Yes	19
.atwola.com	/	badrfi	V0ceab37a4f...	31/01/2005 18:12:28	No	Yes	47
.cnn.com	/	CNNid	8a58426b-2...	13/08/2010 04:12:26	No	Yes	49
.cnnaudience.com	/	AUDid	cf1947e6-64...	30/12/2037 18:59:41	No	Yes	18
.doubleclick.net	/	id	8000002349...	15/04/2006 16:13:10	No	Yes	37

44 Cookies

MozillaCacheView

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

MozillaCacheView: F:\Documents and Settings\Administrator\Local Settings\Application D...

File Edit View Options Help

Filename	Content Type	URL	File Size	Fetch Cour
mailpv.gif	image/gif	http://www.nirsoft.net/utis/mailpv.gif	6,593	1
mailpv.html	text/html	http://www.nirsoft.net/utis/mailpv.html	14,772	1
mailpv_icon.gif	image/gif	http://www.nirsoft.net/utis/mailpv_icon...	314	1
mozilla_history_view...	text/html	http://www.nirsoft.net/utis/mozilla_hist...	9,216	1
mozillahistoryview.gif	image/gif	http://www.nirsoft.net/utis/mozillahisto...	19,233	1
mozillahistoryview_ic...	image/gif	http://www.nirsoft.net/utis/mozillahisto...	319	1
mypass.gif	image/gif	http://www.nirsoft.net/utis/mypass.gif	10,895	2
mypass.html	text/html	http://www.nirsoft.net/utis/mypass.html	14,023	2
mypass_icon.gif	image/gif	http://www.nirsoft.net/utis/mypass_ico...	1,051	2
password_sniffer.html	text/html	http://www.nirsoft.net/utis/password_...	12,060	1
smsniff.gif	image/gif	http://www.nirsoft.net/utis/smsniff.gif	19,682	1

2324 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

MyLastSearch

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

MyLastSearch

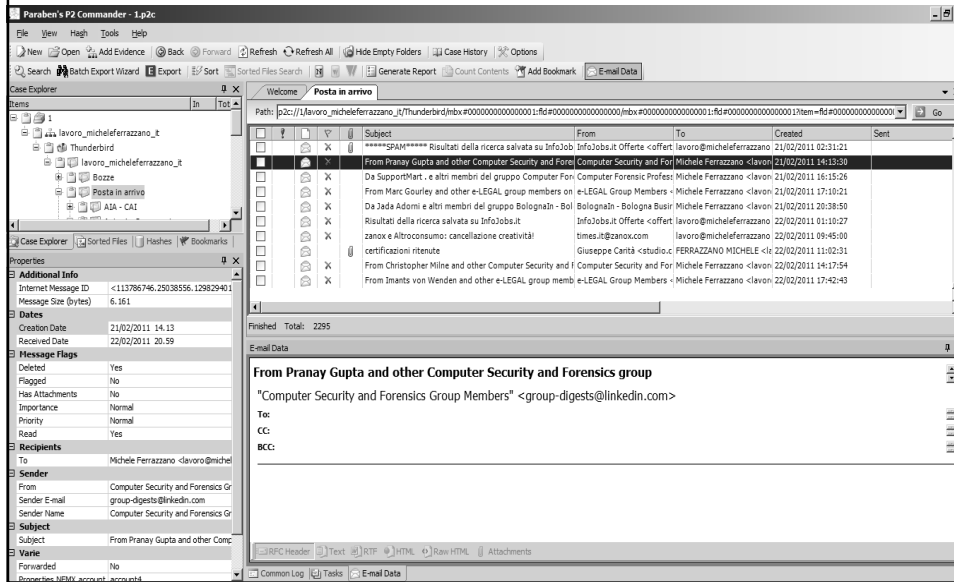
File Edit View Options Help

Search Text	Search Engine	Search Time	Web Browser	Hits	U
windows	MSN	10/11/2007 01:53:09	Internet Explorer	1	h
Hello World	Yahoo	10/11/2007 01:52:47	Mozilla	1	h
password recovery	Google	10/11/2007 01:52:30	Mozilla	1	h
MyLastSearch	Google	10/11/2007 01:51:56	Mozilla	1	h
freeware utilities	Google	10/11/2007 01:51:21	Internet Explorer	1	h
NirSoft	Google	10/11/2007 01:51:12	Internet Explorer	1	h

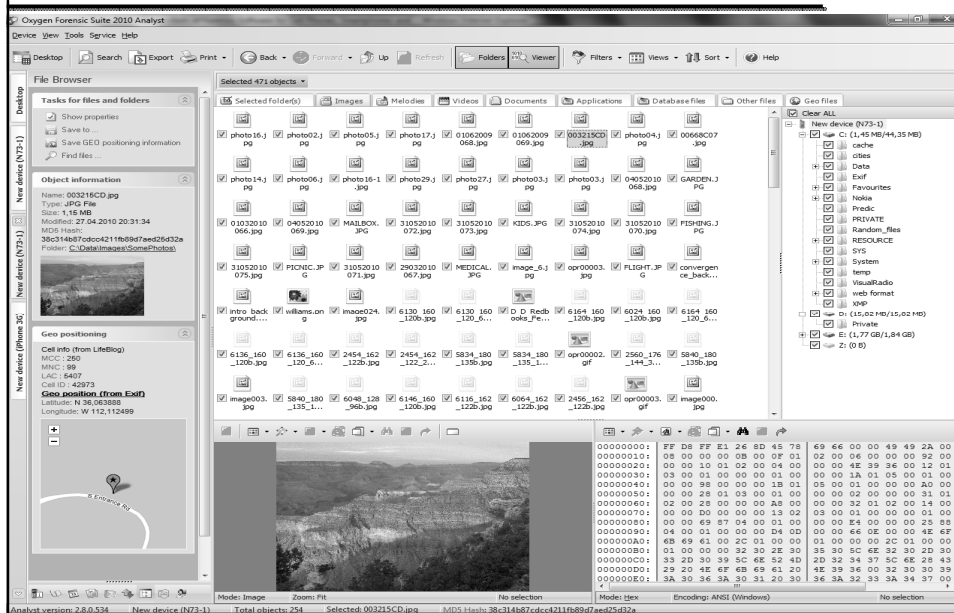
189 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>


Analisi - P2Commander



Analisi - Oxygen forensics



Analisi - emuleforensic



[| HOMEPAGE](#) | [EXAMPLE](#) | [REGISTER](#) | [LOGIN](#) | [CONTACT](#) |

EMULEFORENSIC

This is the official web site for eMuleForensic.

It was born as research project for PhD in Computer Forensics at CIRSFD University of Bologna. Now, it is hosted on CIRSFD server in Bologna (Italy).

It is a digital investigation tool that allows you to convert eMule (or aMule or eMuleAdunanza) config files in xml format.

So you can - for example - understand easily if suspect ser downloaded/uploaded a file with a specific content (i.e. child pornography).

It makes a xml file where you can find informations about:

- userhash;
- downloaded and uploaded files (with hash, size, last modified date, name);
- users who downloaded from you or uploaded to you;
- number of download requests for each file (and the number of requests accepted);
- latest keywords used to find files.

These informations are extract from configuration files *known.met*, *clients.met*, *AC_SearchStrings.dat* and *preferences.dat*.

Note that in these files there aren't personal data about the suspect, but only anonymus data like hash codes, filenames, keywords.

CIRSFD

(C) 2011 Michele Ferrazzano
emuleforensic is a forensics software for eMule, hosted on CIRSFD server.

Analisi

***NETWORK
FORENSICS***

Pacchetto TCP

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Wireshark

traffic-invoipa.pcap - Wireshark

FileEditViewGoCaptureAnalyzeStatisticsTelephonyToolsHelp

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
22	3.638424	137.204.231.102	62.149.128.201	SMTP	C: DATA
23	3.652559	62.149.128.201	137.204.231.102	SMTP	S: 354 go ahead
24	3.652710	137.204.231.102	62.149.128.201	SMTP	C: DATA Fragment, 1236 bytes
25	3.688256	62.149.128.201	137.204.231.102	TCP	smtp > hello [ACK] Seq=198 Ack=1415 Win=7416 Len=0
26	3.688296	137.204.231.102	62.149.128.201	IMF	From: "Posta 1" <posta-1@micheleferrazzano.it>, subject: Mail di prova, (text/plain)
27	3.690824	62.149.128.201	137.204.231.102	TCP	smtp > hello [ACK] Seq=198 Ack=1420 Win=7416 Len=0
28	3.719210	62.149.128.201	137.204.231.102	SMTP	S: 250 OK 1301072520 qp 13134
29	3.730325	137.204.231.102	62.149.128.201	SMTP	C: QUIT
30	3.730392	62.149.128.201	137.204.231.102	SMTP	S: 221 smtp6.aruba.it

Frame 24: 1290 bytes on wire (10320 bits), 1290 bytes captured (10320 bits)

Ethernet II, Src: AsustekC_74:aa:0c:00:23:54:74:aa:0c:cc, Dst: All-HSRP-routers_c8 (00:00:0c:07:ac:c8)

Internet Protocol, Src: 137.204.231.102 (137.204.231.102), Dst: 62.149.128.201 (62.149.128.201)

Transmission Control Protocol, Src Port: hello (1789), Dst Port: smtp (25), Seq: 179, Ack: 198, Len: 1236

Source port: hello (1789)

Destination port: smtp (25)

[Stream index: 0]

Sequence numbers: 179 (capture sequence number)

0030	fb 3b f9 24 00 00 4d 65	73 73 61 67 65 2d 49 44	:1355: message-ID
0040	8a 20 3c 38 34 43 32 44	41 33 45 38 41 38 44 34	: 88C2D A3E8A8d4
0050	38 46 34 41 44 32 46 32	32 41 41 37 37 43 31 45	: 88A0322 AA722C5
0060	32 43 44 40 70 65 72 73	6f 6e 61 6c 65 2e 64 69	: 2C00pers onale, di
0070	72 2e 75 6e 69 62 6f 2e	69 74 3e 0d 0a 46 72 6f	: P unibo. It>, PRO
0080	6d 3a 20 22 50 6f 73 74	65 20 31 22 20 3c 70 6a	: M "post a 1, sp
0090	73 74 61 2d 31 40 6d 69	63 68 65 6c 65 66 65 72	: sta-1@mi chelefer
00a0	72 61 7a 61 6e 6f 2e 69	74 3e 0d 0a 54 6f 3a	: ferrazzano. It>, To:
00b0	20 3c 70 6f 73 74 61 2d	32 40 6d 69 63 68 65 6c	: <posta- 2@michele
00c0	65 6e 65 72 72 61 7a 61	6e 6f 2e 69 74 3e 0d 0a	: ferrazzano. It>, From:
00d0	0a 33 71 62 68 65 63 74	38 20 4d 61 69 6c 20 64	: Subject : Mail di
00e0	69 20 70 72 6f 76 61 0d	0a 44 61 74 65 3a 20 46	: I prova, >date: F
00f0	72 69 20 22 3f 20 4d 61	61 72 20 31 32 20 32	: M "23 Mar 2011
0100	31 38 3a 30 31 3a 35 39	20 2b 30 31 30 30 0d 0a	: 18:01:59 +0100..
0110	4d 49 4d 43 29 36 65 72	73 69 6f 6e 3a 20 31 2e	: MIME-version: 1.
0120	50 0d 0a 0f 6e 74 65	6e 74 14 79 70 65 3a	: Content-type:
0130	20 6d 75 6c 74 69 70 61	72 74 2f 61 6c 6c 74 65 72	: multipart/alter
0140	62 61 69 65 63 69 6d	69 69 62 6f 72 70 61	: native; ..bounda
0150	72 72 30 22 2d 2d 2d 2d	3d 3f 4e 65 78 74 50 61	: <mailto:..NextPa
0160	72 74 5f 30 30 30 3f 30	30 30 43 3f 30 31 43 42	: <000.0 00c_01CB
0170	45 42 31 2b 2e 42 2b 2e	46 42 37 31 30 22 0d 0a	: 2016.068 24707
0180	58 2d 50 72 69 6f 72 69	74 79 3a 20 33 0d 0a 58	: X-Priori ty: 3..X
0190	2d 4d 32 4d 61 69 6c 2d	50 72 69 6f 72 69 74 79	: <Mail> Priority
01a0	38 20 44 6f 72 6d 6c 6c	0d 0a 18 2d 4d 61 69 6c	: Normal <X-Mail
01b0	65 72 3a 20 4d 69 63 72	6f 73 6f 66 74 20 4f 74	: <er: Microsoft ou
01c0	84 65 6f 72 6d 6c 6c	0d 0a 18 2d 4d 61 69 6c	: <look ex press o
01d0	2a 36 36 36 36 36 36 36	72 72 22 22 22 22 22 22	: <000.0 00c_01CB

Simple Mail Transfer Protocol (smtp), 1236 bytes

Packets: 38 Displayed: 38 Marked: 0 Load time: 0:00:0.655

Profile: Default

Xplico

Xplico Interface

User: deft

Help Logout

Cases
Sols
Email
Sip
Web
Images
Printer
Ftp
Mms
GeoMap

Search:

Go

Date	Subject	Sender	Receivers	Size
2007-08-14 11:06:50	*****SPAM***** Magic is real	"Shannon Palacios" <shraga.davenpc	<info@iserm.com>	22907
2007-08-14 11:03:50	*****SPAM***** Ladies will love you	"Tania Moreno" <pkcensorial@mon	<f5cd67a3" <f5cd67a3@iserm.com>	3692
2007-08-14 11:02:50	Sorry for being late	"Bridgett" <tajnireiwc@advantex	"Cleo Sanchez" <yoke@iserm.com>	2393
2007-08-14 08:24:10	This basic strategic insight supplied the tactics f	"Daniel Perth" <Daniel836@ecommel	a6185cf@iserm.com	2303
2007-08-14 08:20:35	You would have been a formidable team.	"Carmela Fomenko" <Fomenkowig@i	<yoke@iserm.com>	5660
2007-08-14 08:18:34	They talked for five or ten minutes and then I ht	"Gustavo Breck" <Gustavo_Breck@i	<howledabstracted@iserm.com>	2378
2007-08-14 08:12:29	Accept Credit Cards on Your Web Site Today.	"Julie Amomonpon" <Julie.Amomon	<outplaying@iserm.com>	2240
2007-08-14 08:04:58	This report indicates which shows were watch	"Kingman Mulchan" <Mulchan@stef	beforehand@iserm.com	2285
2007-08-14 08:04:41	Returned mail: see transcript for details	Mail Delivery Subsystem <MAILER-D	<hucsofmrw@iserm.com>	5021
2007-08-14 08:04:34	Returned mail: see transcript for details	Mail Delivery Subsystem <MAILER-D	<paftsmqc@iserm.com>	5342
2007-08-14 08:04:33	Re: Hallo!	"Abel Chaney" <a-1@adultcashflow.	<solace@iserm.com>	1377
2007-08-14 08:04:31	Delivery Status Notification (Failure)	"Mail Delivery System" <MAILER-DAE	zylqsp@iserm.com	4552
2007-08-14 08:04:31	*****SPAM***** But the way SATA has been dev	"melica soo" <sooltig@photoesc.co	<a6185cf@iserm.com>	8125
2007-08-14 08:04:30	*****SPAM***** The girl eluded us.	"Melissa Goedde" <Goeddejenx@wi	<perishedcloudiness@iserm.com>	4229
2007-08-14 08:04:28	About last night	"Crystal Hamilton" <arismenidezorv	"Steve" <has@iserm.com>	2398
2007-08-14 08:04:28	*****SPAM***** Fwd: Thanks, we are accepting	"Drew Christensen" <ignaciomercur	<howledabstracted@iserm.com>	6263
2007-08-14 08:04:28	Webster, Nesta - "World Revolution", London, ("	"wandersom Nyland" <wandersom@	<beforehand@iserm.com>	5258
2007-08-14 08:04:26	Just keep in touch	"Goldie Sanchez" <balstoreoamm@	"Lisandra" <guyanayoke@iserm.co	2268
2007-08-14 08:04:24	AUTHENTIC VIAGRA AND CIALIS	"Sales Department" <sales@designi	"Luiz Everson" <odvwy@iserm.com	1387
2007-08-14 08:04:24	*****SPAM***** Fwd: Thank you, we are ready to	"Heath Randall" <Demetriuselastom	<outplaying@iserm.com>	6109
2007-08-14 08:04:23	Undeliverable: Thanks, we are ready to lend yo	"System Administrator" <administra	<jjowiaqwsit@iserm.com>	4962
2007-08-14 08:04:23	Undelivered Mail Returned to Sender	MAILER-DAEMON@smoothwall.local	xdlyiyul@iserm.com	4762

Xplico

Xplico Interface

User: deft

Help Logout

Cases
Sols
Email
Sip
Web
Images
Printer
Ftp
Mms
GeoMap

Email to <info@iserm.com>

Subject:	*****SPAM***** Magic is real
Sender:	Shannon Palacios <shraga.davenport@armhule.dk>
Recipient:	
Date:	Tue, 14 Aug 2007 09:05:56 -0900
Username:	
Password:	
EML file:	email.eml
Info:	info.xml
Spam detection software, running on the system "mxavas14.fe.aruba.it", has identified this incoming email as possible spam. The original message has been attached to this so you can view it (if it isn't spam) or label similar future email. If you have any questions, see http://vadamecum.aruba.it/start/mail/antispam/ for details.	
Content preview: [...]	
Content analysis details: (5.1 points, 5.0 required)	
pts rule name	description
Attached message	
E-mail message	

Xplico org CRISPMP POWER Version 0.5

© 2007-2009 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

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 €
NetAnalysisis	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 €