

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

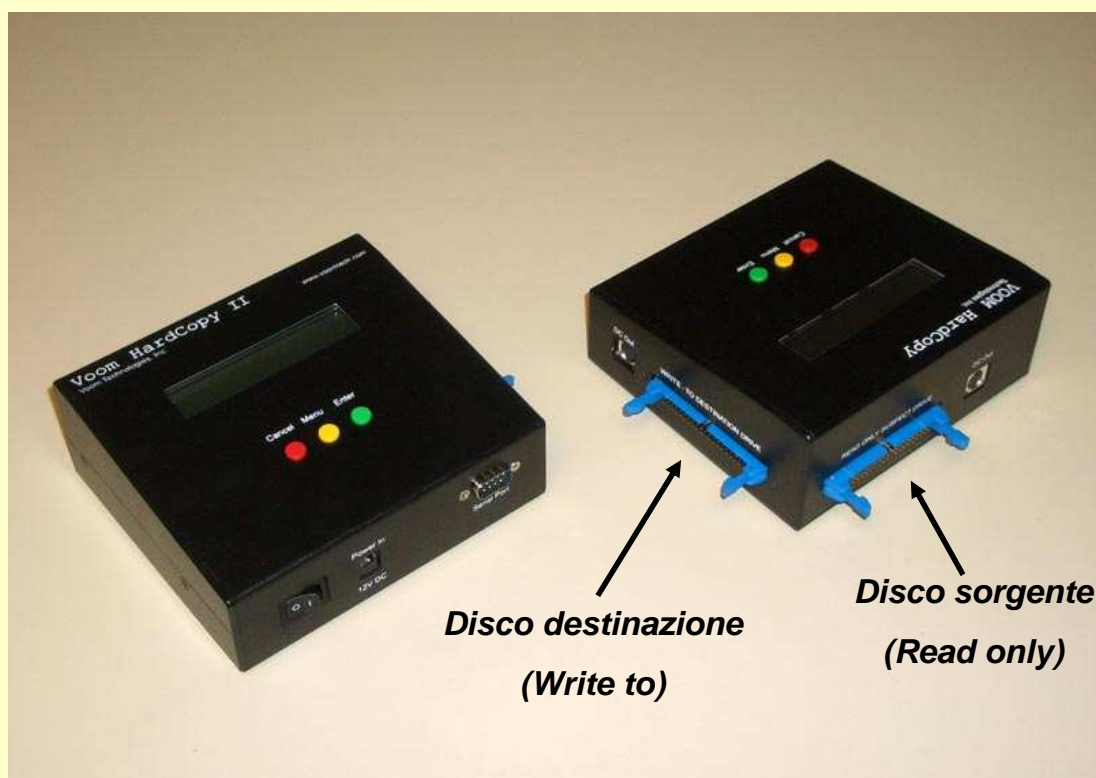
- PC e notebook
- Lettori di supporti e cavi (di tutti i tipi)
 - BluRay, DVD, CD, hard-disk, floppy 3,5", floppy 5,25", DAT...
 - Cavi per telefoni cellulari
- Copiatori
- Write blocker

Software per l'attività di laboratorio

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

DISK FORENSICS

Copiatore hardware



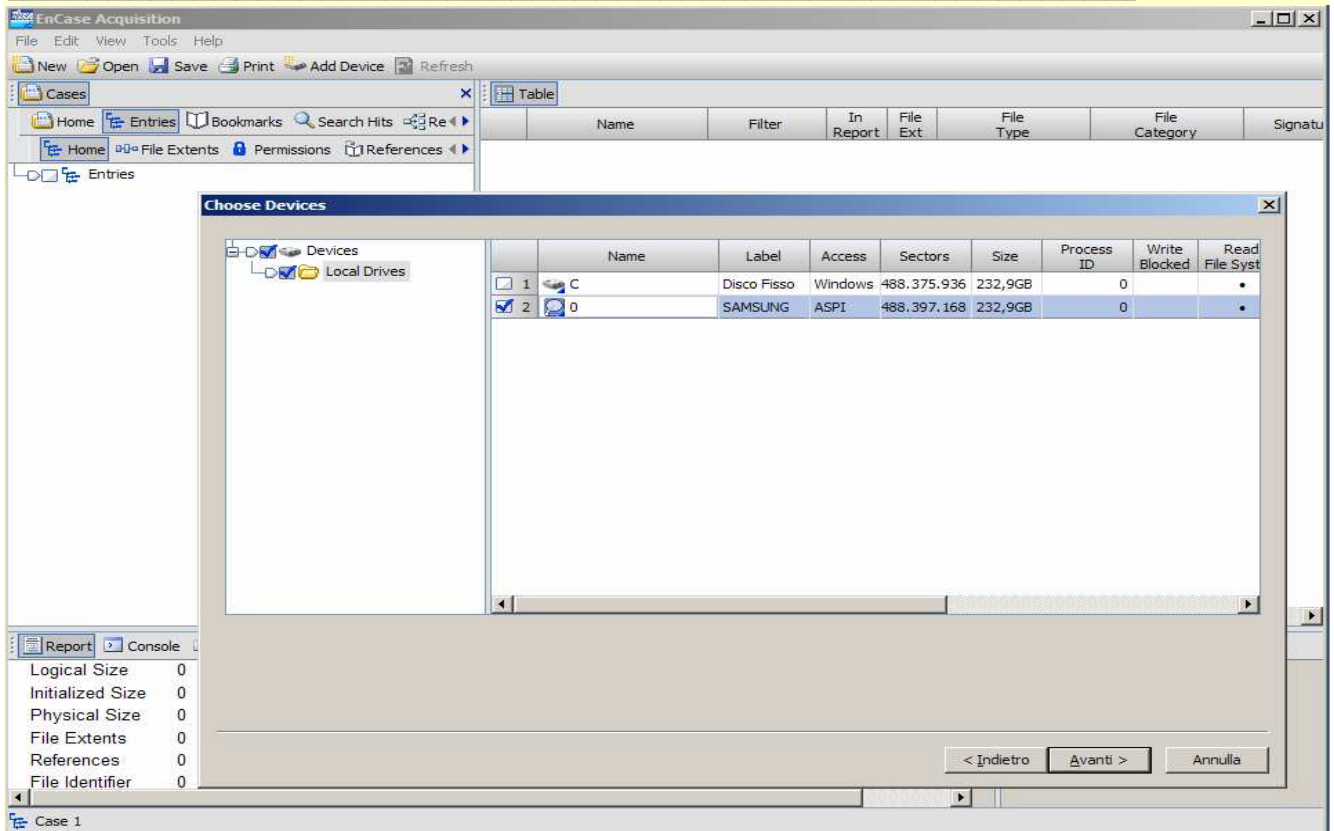
Copiatore hardware (es: Logicube Talon)



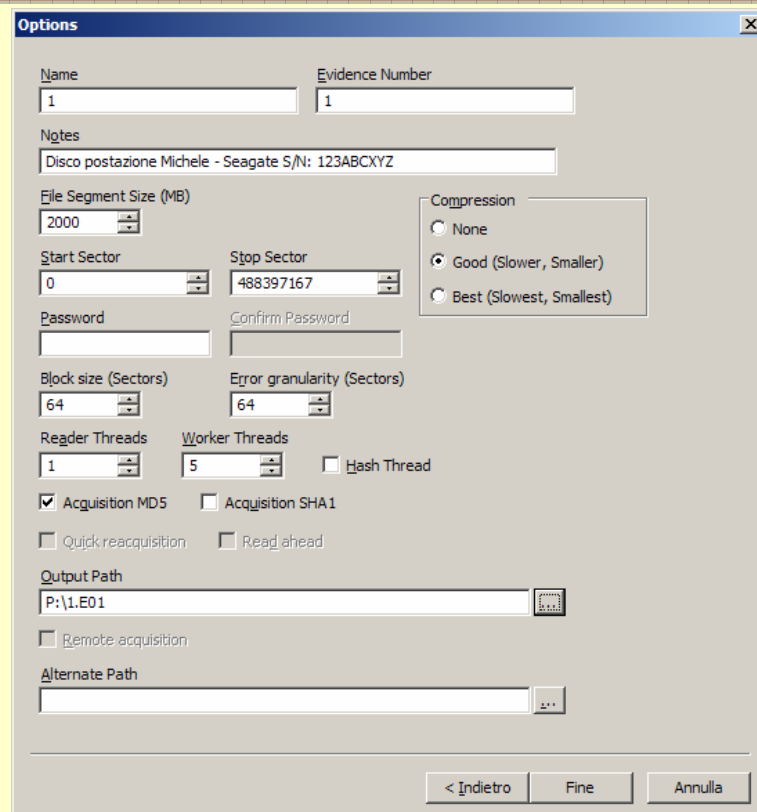
Write blocker



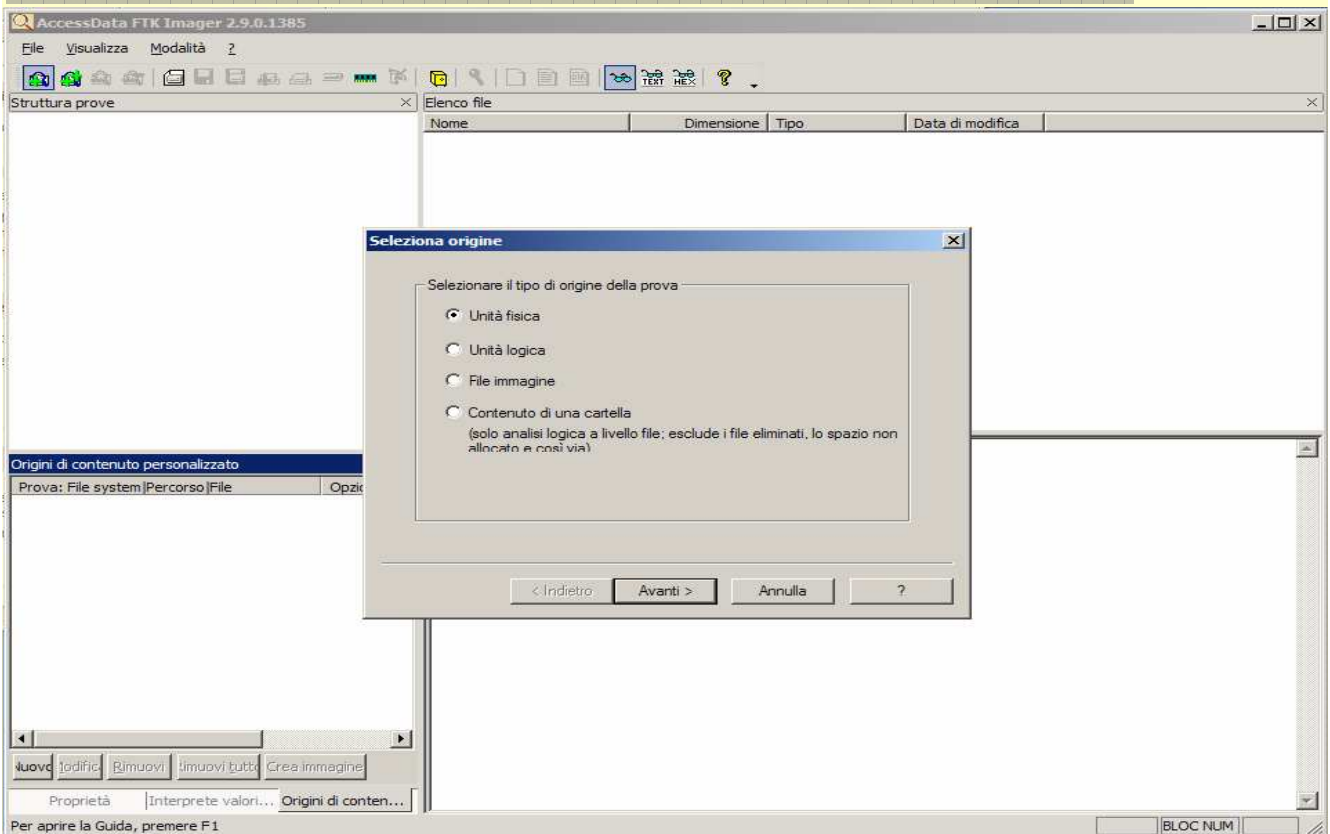
Acquisizione – Encase



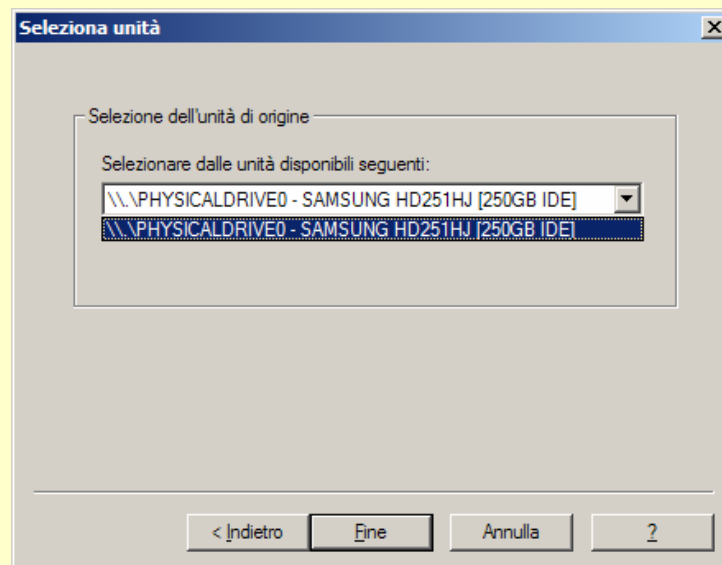
Acquisizione - Encase



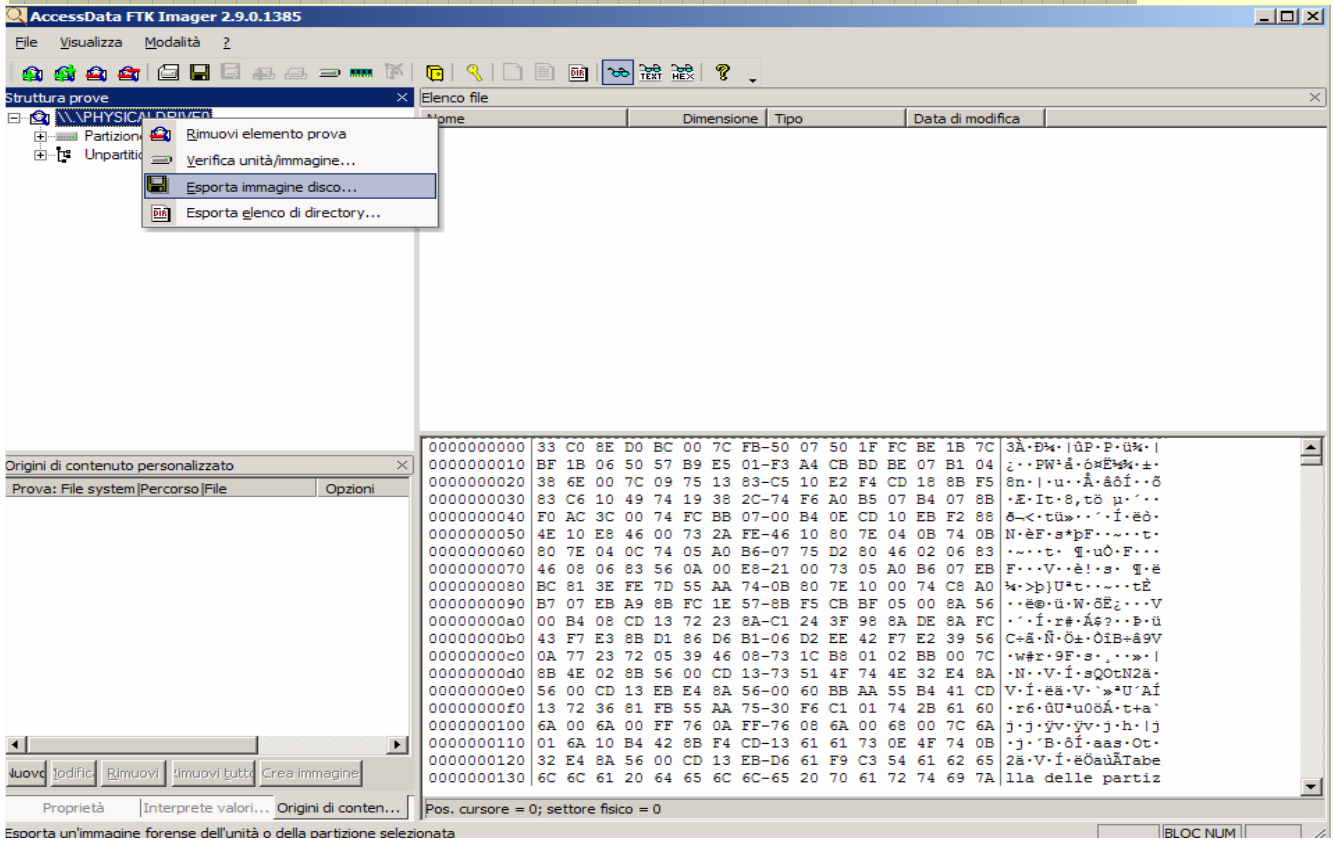
Acquisizione - FTK Imager



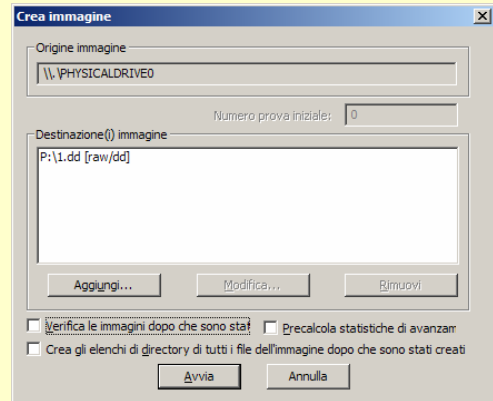
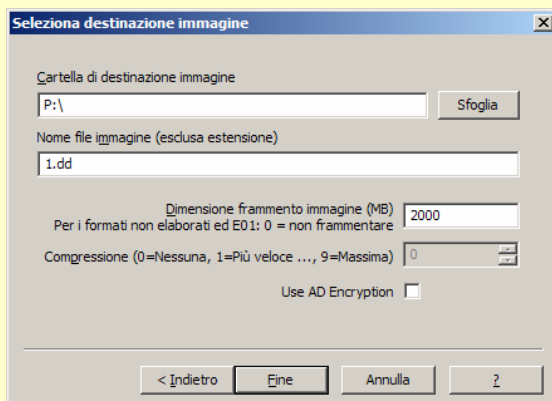
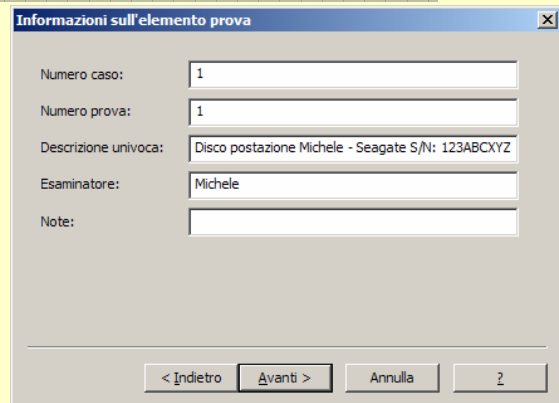
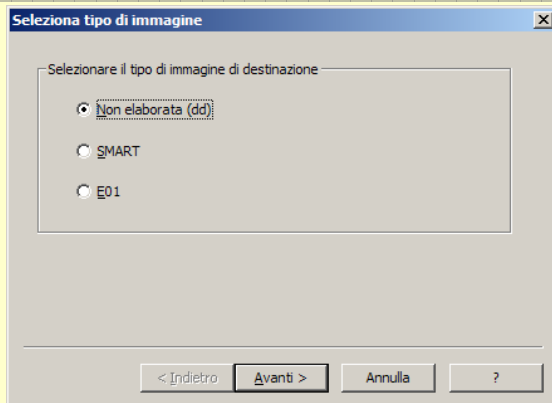
Acquisizione - FTK Imager



Acquisizione - FTK Imager



Acquisizione – FTK Imager



Acquisizione – Dispositivi *mobile*



Acquisizione – dd

```
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

The screenshot displays the Wireshark Network Analyzer interface. The main window is titled "The Wireshark Network Analyzer" and features a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Help) and a toolbar. A filter bar is visible above the main content area.

The "Capture" section is active, showing the "Interface List" and "Capture Options" panels. The "Interface List" panel displays a table of available capture interfaces:

Description	IP	Packets	Packets/s	Stop
Adapter for generic dialup and VPN capture	unknown	0	0	Start Options Details
Broadcom NetXtreme Gigabit Ethernet Driver (Microsoft's Packet Scheduler)	unknown	0	0	Start Options Details
Intel(R) PRO/Wireless 2200BG Network Connection (Microsoft's Packet Scheduler)	192.168.1.72	6	0	Start Options Details

The "Capture Options" panel is also visible, showing the "Start capture on interface:" section. The "Sample Captures" section is active, displaying a list of capture files, including "D:\{12345\Didattica\2 ... UniCT - IP\traffico-ricezioneposta.pcap (7033 Bytes)".

The "Security" section is also visible, with a link to "http://wiki.wireshark.org/Security".

The status bar at the bottom indicates "Ready to load or capture", "No Packets", and "Profile: Default".

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 MD5 LIST OF FILES**

DEL	Type	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

Table Gallery Timeline Report

Cases

- Case 1
 - 1
 - .Trashes
 - 504
 - amaral_ha
 - ITALIAN 1
 - Nueva carpeta
 - Nueva carpeta
 -
 - Fama ia be
 - navidad 08
 - Nueva carpeta
 - Nueva carpeta
 - RECYCLER
 - S-1-5-2

	Name	Is Deleted	File Ext	File Type	Last Accessed	File Created	Last Written	Logical Size	
<input type="checkbox"/>	124	<input checked="" type="checkbox"/>	Imagen 115.jpg	jpg	JPEG	01/10/09	01/10/09 06:30:32	01/02/09 11:49:34	1.592.856
<input type="checkbox"/>	125	<input checked="" type="checkbox"/>	Imagen 116.jpg	jpg	JPEG	01/10/09	01/10/09 06:30:36	01/02/09 11:49:36	1.634.671
<input type="checkbox"/>	126	<input checked="" type="checkbox"/>	Imagen 117.jpg	jpg	JPEG	01/10/09	01/10/09 06:30:38	01/02/09 11:49:38	1.513.034
<input type="checkbox"/>	127	<input checked="" type="checkbox"/>	Imagen 118.jpg	jpg	JPEG	01/10/09	01/10/09 06:30:42	01/02/09 11:49:40	1.522.924
<input type="checkbox"/>	128	<input checked="" type="checkbox"/>	Imagen 119.jpg	jpg	JPEG	01/10/09	01/10/09 06:30:44	01/02/09 11:49:42	1.541.085
<input type="checkbox"/>	129	<input type="checkbox"/>	ITALIAN 1			10/22/08	10/22/08 09:24:52	10/22/08 09:24:54	16.384
<input type="checkbox"/>	130	<input checked="" type="checkbox"/>	lente_ingrandiment...	jpg	JPEG	03/09/11	03/02/11 11:38:58	03/02/11 11:45:36	28.702
<input type="checkbox"/>	131	<input checked="" type="checkbox"/>	Imbrt beer atuk.xls	xls	MS Excel Spreadsheet	12/30/09	12/06/09 07:11:22	12/06/09 07:10:30	27.136
<input type="checkbox"/>	132	<input type="checkbox"/>	MSW0VKS.EXE	EXE	Windows Executable	03/16/10	08/02/07 01:00:00	03/21/09 03:07:00	147.456
<input type="checkbox"/>	133	<input type="checkbox"/>	navidad 08			01/10/09	01/10/09 11:28:46	01/10/09 11:28:48	
<input type="checkbox"/>	134	<input type="checkbox"/>	Nueva carpeta			12/30/09	12/30/09 06:29:36	12/30/09 06:29:38	
<input type="checkbox"/>	135	<input type="checkbox"/>	Nueva carpeta			10/09/08	10/09/08 11:47:36	10/09/08 11:47:38	
<input type="checkbox"/>	136	<input type="checkbox"/>	Nueva carpeta			11/02/08	11/02/08 11:09:22	11/02/08 11:09:24	
<input type="checkbox"/>	137	<input type="checkbox"/>	Nueva carpeta			10/22/08	10/22/08 09:42:18	10/22/08 09:42:20	16.384
<input type="checkbox"/>	138	<input checked="" type="checkbox"/>	PENDRIVE.1GB	1GB				12/22/10 05:50:28	
<input type="checkbox"/>	139	<input checked="" type="checkbox"/>	PRACTICAS.doc	doc	Word Document	12/30/09	12/05/09 08:52:48	12/05/09 08:51:10	61.952
<input type="checkbox"/>	140	<input type="checkbox"/>	Primary FAT						123.904
<input type="checkbox"/>	141	<input type="checkbox"/>	RECYCLER			07/08/08	07/08/08 01:38:22	07/08/08 01:38:24	
<input type="checkbox"/>	142	<input type="checkbox"/>	Secondary FAT						123.904
<input type="checkbox"/>	143	<input checked="" type="checkbox"/>	tema 10.pdf	pdf	Adobe PDF	10/07/08	10/06/08 05:19:24	10/06/08 05:19:26	64.121

Text Hex Picture Disk Report Console Filters Queries Lock 0/236 1: PS 776 LS 744 CL 9 SO 000 FO 0 LE 0

Case 1[C]Vente_ingrandimento.jpg

Analisi - FTK (Forensic ToolKit)

AccessData FTK version 1.70.1 build 07.03.20 -- C:\Cases\Wayward Astronomer\

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items	File Status	File Category
Evidence Items: 4	KFF Alert Files: 2	Documents: 251
File Items	Bookmarked Items: 0	Spreadsheets: 8
Total File Items: 3614	Bad Extension: 7	Databases: 0
Checked Items: 0	Encrypted Files: 5	Graphics: 1199
Unchecked Items: 3614	From E-mail: 219	Multimedia: 5
Flagged Thumbnails: 0	Deleted Files: 657	E-mail Messages: 43
Other Thumbnails: 1199	From Recycle Bin: 53	Executables: 44
Filtered In: 3614	Duplicate Items: 736	Archives: 80
Filtered Out: 0	OLE Subitems: 423	Folders: 288
Unfiltered	Flagged Ignore: 0	Slack/Free Space: 734
All Items	KFF Ignorable: 114	Other Known Type: 323
Actual Files	Data Carved Files: 0	Unknown Type: 639

Evidence Fi...	Evidence Path	Display Name	Identification N...	Evidence Type	Added	Children	Descendants	Investigator's
Messier Image.E01	C:\Evidence	Messier Image\P...		FAT32	8/2/2007 3:43:2...	2182	2409	Joe Friday
Messier Image.E01	C:\Evidence	Messier Image\P...		NTFS	8/2/2007 3:45:0...	248	604	Joe Friday
Messier Image.E01	C:\Evidence	Messier Image\P...		NTFS	8/2/2007 3:45:3...	241	302	Joe Friday
Messier Image.E01	C:\Evidence	Messier Image\U...		Unpartitioned Sp...	8/2/2007 3:45:5...	295	295	Joe Friday

4 Listed 0 Checked Total 0 Highlighted

Analisi - NetAnalysis

NetAnalysis v1.37f - Forensic Internet History Analysis

File Filter Searching Sorting Tools Reports View Column Help

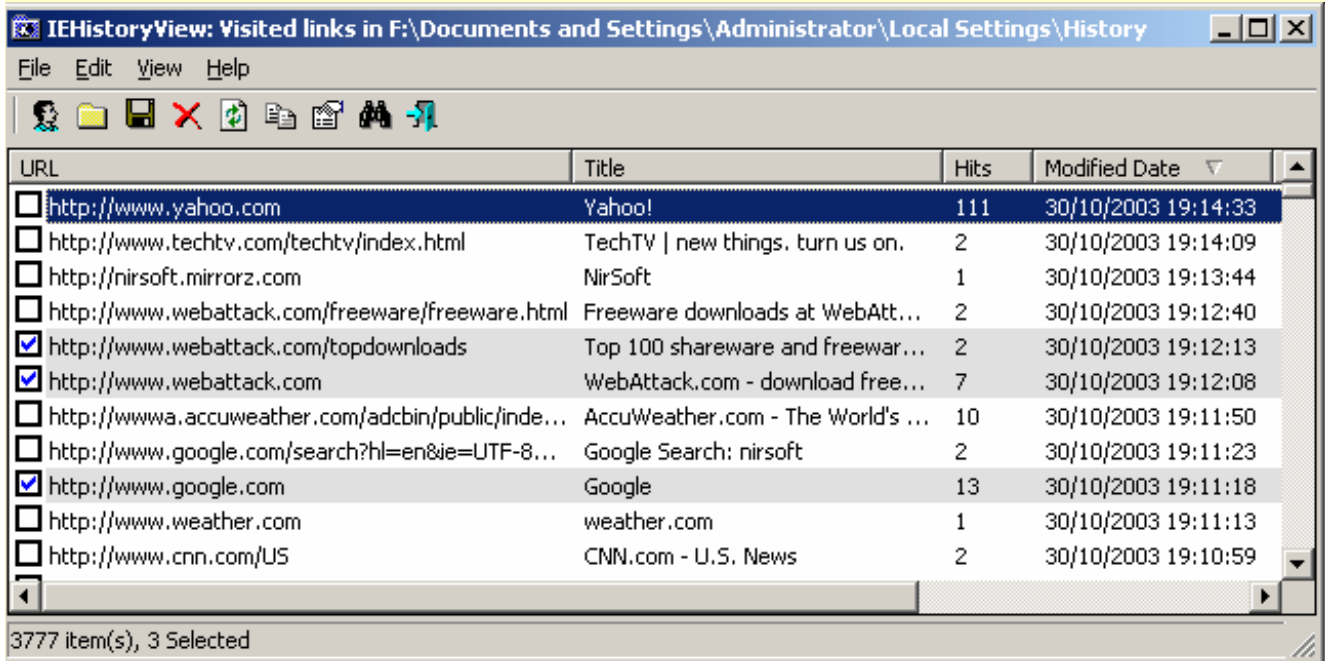
Record URN: 1348

Key	Value	Host	Secure	Last Modified Date [UTC]	Expiration Date [UTC]
✓ __utma	266963212.1185001735775325700.1238586478.1238586...	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=google utmccn=(orga...	simplynames.com/	False	01/04/2009 11:47:57 Wed	30/09/2009 23:47:57 Wed
✓ dbmrtkg	eJyFisENwyAMADiCjghDNEZKpl4lmqjUTFgHwxlpQv0T...	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>



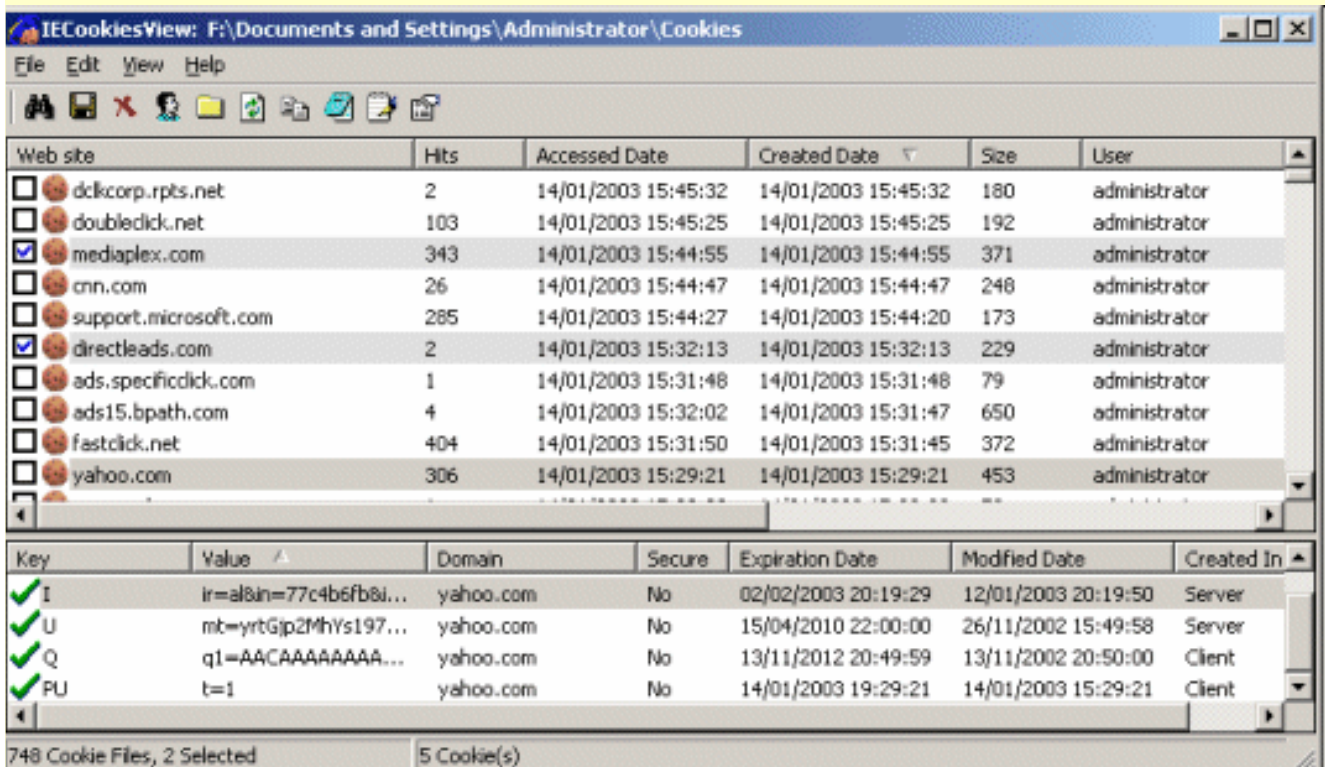
IEHistoryView: Visited links in F:\Documents and Settings\Administrator\Local Settings\History

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

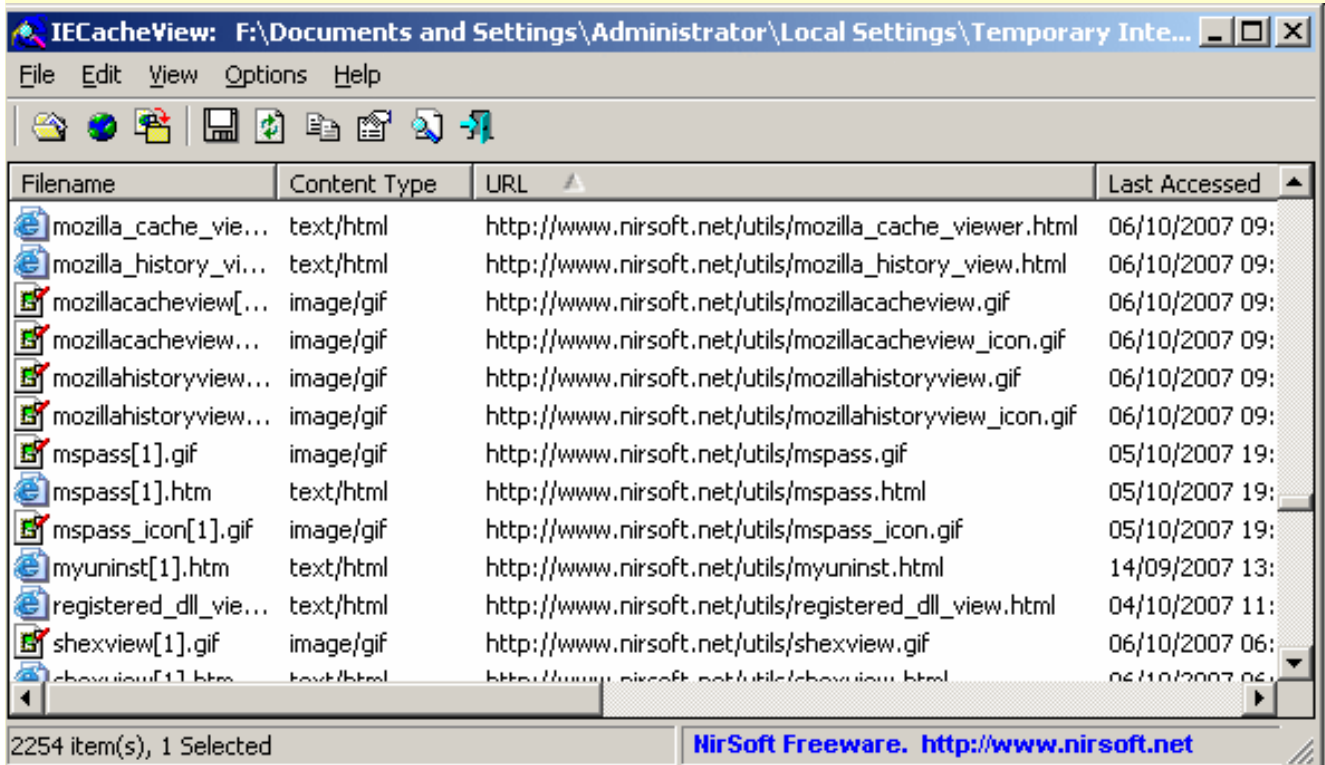
Web site	Hits	Accessed Date	Created Date	Size	User
<input type="checkbox"/> dckcorp.rpts.net	2	14/01/2003 15:45:32	14/01/2003 15:45:32	180	administrator
<input type="checkbox"/> doubledclick.net	103	14/01/2003 15:45:25	14/01/2003 15:45:25	192	administrator
<input checked="" type="checkbox"/> mediaplex.com	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.specifidick.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
I	ir=al&in=77c4b6fb&...	yahoo.com	No	02/02/2003 20:19:29	12/01/2003 20:19:50	Server
U	mt=yrtGjp2MhYs197...	yahoo.com	No	15/04/2010 22:00:00	26/11/2002 15:49:58	Server
Q	q1=AACAAAAAAAAA...	yahoo.com	No	13/11/2012 20:49:59	13/11/2002 20:50:00	Client
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/utis/ie_cache_viewer.html



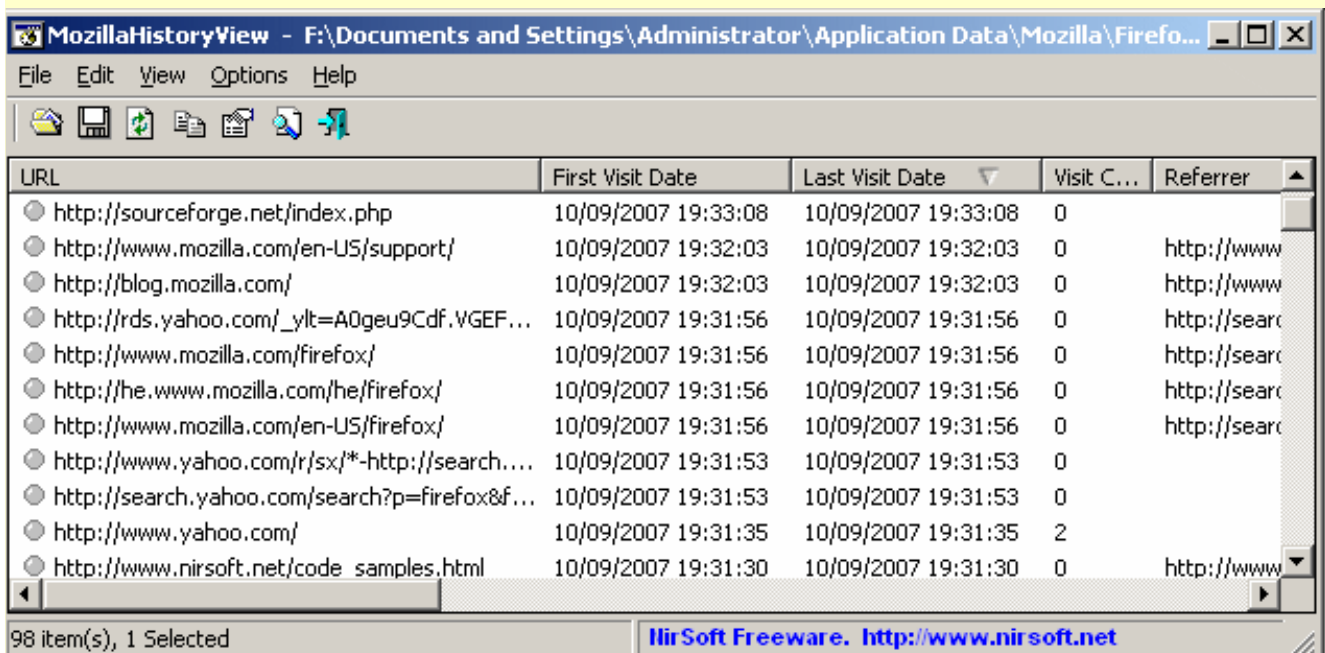
The screenshot shows the IECacheView application window. The title bar reads "IECacheView: F:\Documents and Settings\Administrator\Local Settings\Temporary Inte...". The menu bar includes "File", "Edit", "View", "Options", and "Help". The toolbar contains icons for file operations. The main area displays a table of cached files with columns for "Filename", "Content Type", "URL", and "Last Accessed".

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

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

MozillaHistoryView

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



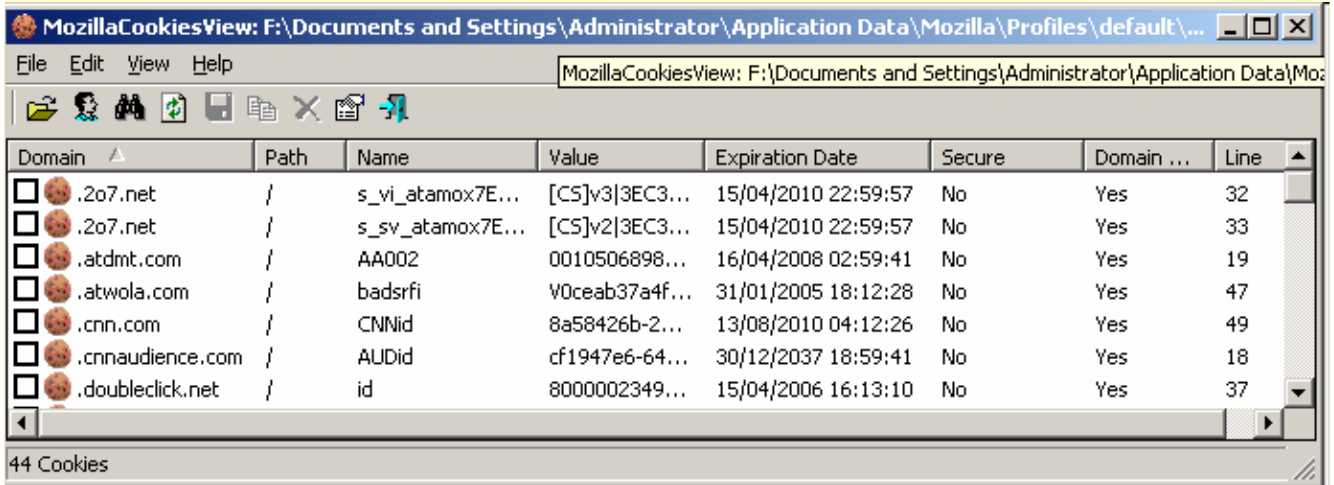
The screenshot shows the MozillaHistoryView application window. The title bar reads "MozillaHistoryView - F:\Documents and Settings\Administrator\Application Data\Mozilla\Firefo...". The menu bar includes "File", "Edit", "View", "Options", and "Help". The toolbar contains icons for file operations. The main area displays a table of browser history entries with columns for "URL", "First Visit Date", "Last Visit Date", "Visit C...", and "Referrer".

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://searc
http://www.mozilla.com/firefox/	10/09/2007 19:31:56	10/09/2007 19:31:56	0	http://searc
http://he.www.mozilla.com/he/firefox/	10/09/2007 19:31:56	10/09/2007 19:31:56	0	http://searc
http://www.mozilla.com/en-US/firefox/	10/09/2007 19:31:56	10/09/2007 19:31:56	0	http://searc
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



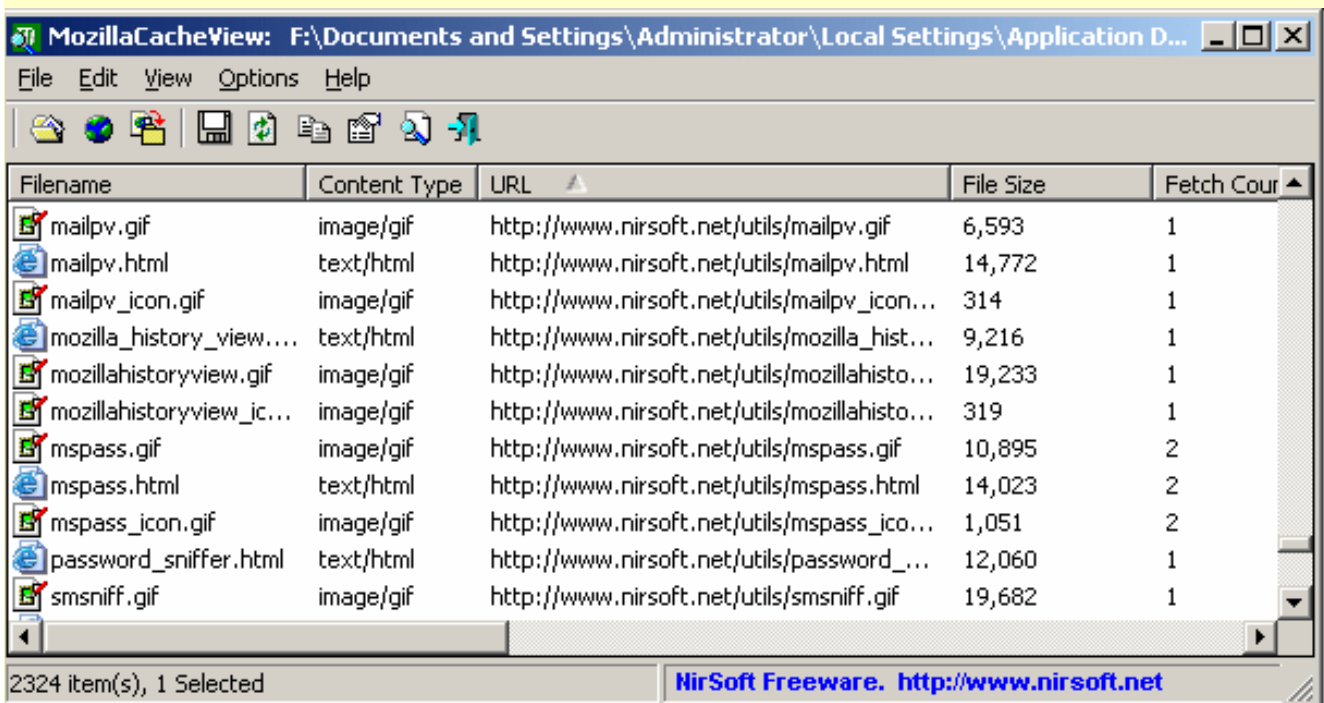
MozillaCookiesView: F:\Documents and Settings\Administrator\Application Data\Mozilla\Profiles\default\...

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	/	badsrfi	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/utills/mozilla_cache_viewer.html



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

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

2324 item(s), 1 Selected

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

MyLastSearch

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

The screenshot shows the MyLastSearch application window. The title bar reads "MyLastSearch". The menu bar includes "File", "Edit", "View", "Options", and "Help". Below the menu bar is a toolbar with icons for search, refresh, and other functions. The main area contains a table with the following columns: "Search Text", "Search Engine", "Search Time", "Web Browser", "Hits", and "U". The table lists several search results, with "Hello World" selected. At the bottom, it shows "189 item(s), 1 Selected" and a footer for "NirSoft Freeware. http://www.nirsoft.net".

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

Analisi - P2Commander

The screenshot shows the Paraben's P2 Commander application. The title bar reads "Paraben's P2 Commander - 1.p2c". The menu bar includes "File", "View", "High", "Tools", and "Help". The interface is divided into several panes. On the left is a "Case Explorer" showing a tree view of files and folders. Below it is a "Properties" pane with "Additional Info", "Dates", "Message Flags", "Recipients", "Sender", "Subject", and "Vari" sections. The main pane is titled "Posta in arrivo" and displays a list of emails. The selected email is from "Pranay Gupta and other Computer Security and Forensics group" with the subject "Computer Security and Forensics Group Members". The email content is visible in the bottom pane.

From: Pranay Gupta and other Computer Security and Forensics group
Subject: "Computer Security and Forensics Group Members" <group-digests@linkedin.com>

To:
CC:
BCC:

Analisi - Oxygen forensics

Oxygen Forensic Suite 2010 Analyst

Device View Tools Service Help

Desktop Search Export Print Back Forward Up Refresh Folders Viewer Filters Views Sort Help

File Browser

Tasks for files and folders

- Show properties
- Save to ...
- Save GEO positioning information
- Find files ...

Object information

Name: 003215CD.jpg
Type: JPG File
Size: 1,16 MB
Modified: 27.04.2010 20:31:34
MD5 Hash: 38c314b87cdcc4211fb89d7aed25d32a
Folder: C:\Data\Images\SomePhotos\

Geo positioning

Cell info (from LifeLog)

MCC : 250
MNC : 99
LAC : 5407
Cell ID : 42973

Geo position (from Exif)

Latitude: N 36.063888
Longitude: W 112.112499

Analyst version: 2.8.0.534 New device (N73-1) Total objects: 254 Selected: 003215CD.jpg MD5 Hash: 38c314b87cdcc4211fb89d7aed25d32a

Analisi - emuleforensic

emuleforensic

HOME PAGE | 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 CIRSFID University of Bologna. Now, it is hosted on CIRSFID 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.

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

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.davenport@armhule.dk>	<info@iserm.com>	22907
2007-08-14 11:03:50	****SPAM**** Ladies will love you	"Tania Moreno" <pkcensorial@montecarlo.com>	<f5cd67a3@iserm.com>	3692
2007-08-14 11:02:50	Sorry for being late	"Bridgett" <tajnireiwfcs@advantext.com>	"Cleo Sanchez" <yoke@iserm.com>	2393
2007-08-14 08:24:10	This basic strategic insight supplied the tactics for	"Daniel Perth" <Daniel836@ecommerce.com>	a618f5cf@iserm.com	2303
2007-08-14 08:20:35	You would have been a formidable team.	"Carmela Fomenko" <Fomenkowlg@iserm.com>	<yoke@iserm.com>	5660
2007-08-14 08:18:34	They talked for five or ten minutes and then I he	"Gustavo Breck" <Gustavo_Breck@iserm.com>	<howledabstracted@iserm.com>	2378
2007-08-14 08:12:29	Accept Credit Cards on Your Web Site Today.	"Julie Amomonpon" <Julie.Amomonpon@iserm.com>	<outplaying@iserm.com>	2240
2007-08-14 08:04:58	This report indicates which shows were watched	"Kingman Mulchan" <Mulchan@step.com>	beforehand@iserm.com	2285
2007-08-14 08:04:41	Returned mail: see transcript for details	Mail Delivery Subsystem <MAILER-DAEMON@iserm.com>	<hucsoftrmv@iserm.com>	5021
2007-08-14 08:04:34	Returned mail: see transcript for details	Mail Delivery Subsystem <MAILER-DAEMON@iserm.com>	<pafthsmqc@iserm.com>	5342
2007-08-14 08:04:33	Re: Hallo!	"Abel Chaney" <a-1@adulfcashflow.com>	<solace@iserm.com>	1377
2007-08-14 08:04:31	Delivery Status Notification (Failure)	"Mail Delivery System" <MAILER-DAEMON@iserm.com>	zylqsp@iserm.com	4552
2007-08-14 08:04:31	****SPAM**** But the way SATA has been dev	"melica soo" <sooftjg@photoesc.com>	<a618f5cf@iserm.com>	8125
2007-08-14 08:04:30	****SPAM**** The girl eluded us.	"Melissa Goedde" <Goeddejenx@wired.com>	<perishedcloudiness@iserm.com>	4229
2007-08-14 08:04:28	About last night	"Crystal Hamilton" <arismenidezorv@iserm.com>	"Steve" <has@iserm.com>	2398
2007-08-14 08:04:28	****SPAM**** Fwd: Thanks, we are accepting	"Drew Christensen" <Ignaciomercurio@iserm.com>	<howledabstracted@iserm.com>	6263
2007-08-14 08:04:28	Webster, Nesta - "World Revolution", London, ("wandersom Nyland" <wandersom@iserm.com>	<beforehand@iserm.com>	5258
2007-08-14 08:04:26	Just keep in touch	"Goldie Sanchez" <balstoreoamm@iserm.com>	"Lisandra" <guyanayoke@iserm.com>	2268
2007-08-14 08:04:24	AUTHENTIC VIAGRA AND CIALIS	"Sales Department" <sales@design.com>	"Luiz Everson" <koxvwy@iserm.com>	1387
2007-08-14 08:04:24	****SPAM**** Fwd: Thank you, we are ready to	"Heath Randall" <Demetriuselastom@iserm.com>	<outplaying@iserm.com>	6109
2007-08-14 08:04:23	Undeliverable: Thanks, we are ready to lend yo	"System Administrator" <administrator@iserm.com>	<jjowiaqwsft@iserm.com>	4962
2007-08-14 08:04:23	Undelivered Mail Returned to Sender	MAILER-DAEMON@smoothwall.local	xdlyiyiul@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			
<p>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://vademeccum.aruba.it/start/mail/antispam/ for details.</p> <p>Content preview: [...]</p> <p>Content analysis details: (5.1 points, 5.0 required)</p> <table border="1"><thead><tr><th>pts</th><th>rule name</th><th>description</th></tr></thead><tbody></tbody></table>		pts	rule name	description
pts	rule name	description		
Attached message				
E-mail message				

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 €
NetAnalysisis	XXX €
FTK	XXXX €
P2Commander	XXX €
Software vari Nirsoft	0 €
Software per analisi (NF)	
Wireshark	0 €
Xplico	0 €

Investimento iniziale minimo: 0 €