



# PERU HACK

## Análisis Forense con Autopsy 3

Alonso Caballero Quezada  
ReYDeS - @Alonso\_ReYDeS  
[www.reydes.com](http://www.reydes.com)  
[reydes@gmail.com](mailto:reydes@gmail.com)

# ¿QUE ES AUTOPSY?

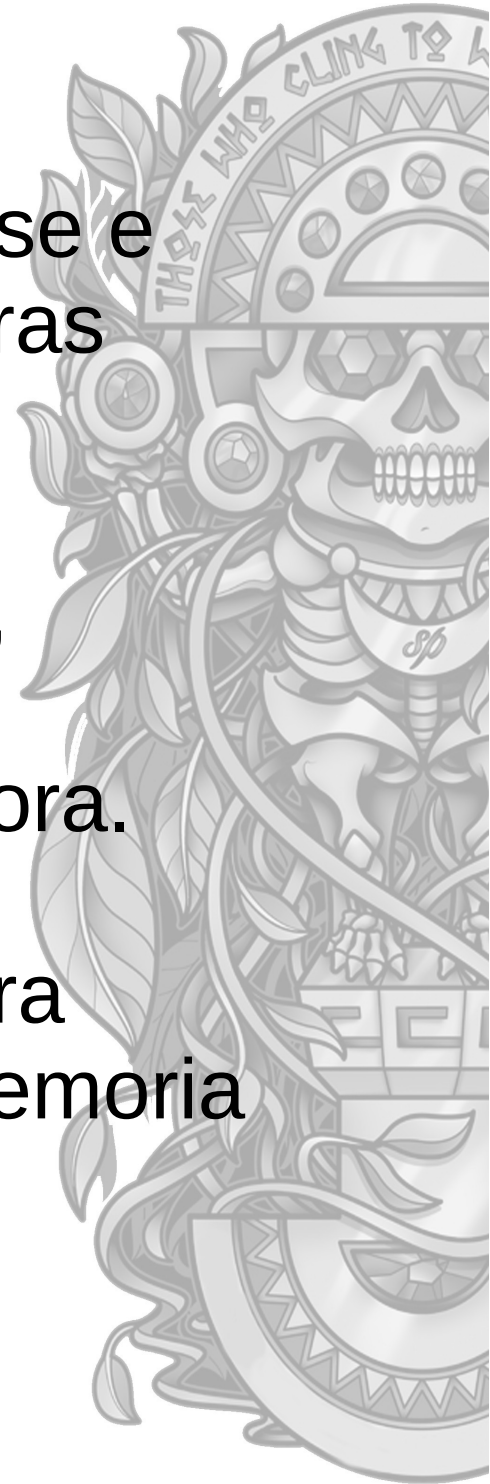
Autopsy es una plataforma digital forense e interfaz gráfica para The Sleuth Kit y otras herramientas forenses.

Puede ser utilizado por fuerzas legales, militares, y analistas corporativos para investigar lo ocurrido en una computadora.

Aunque también se le puede utilizar para recuperar fotos desde una tarjeta de memoria de una cámara digital.

\* <http://www.sleuthkit.org/autopsy/>

\* <http://www.sleuthkit.org/sleuthkit/>



# CARACTERÍSTICAS PARA EL ANÁLISIS

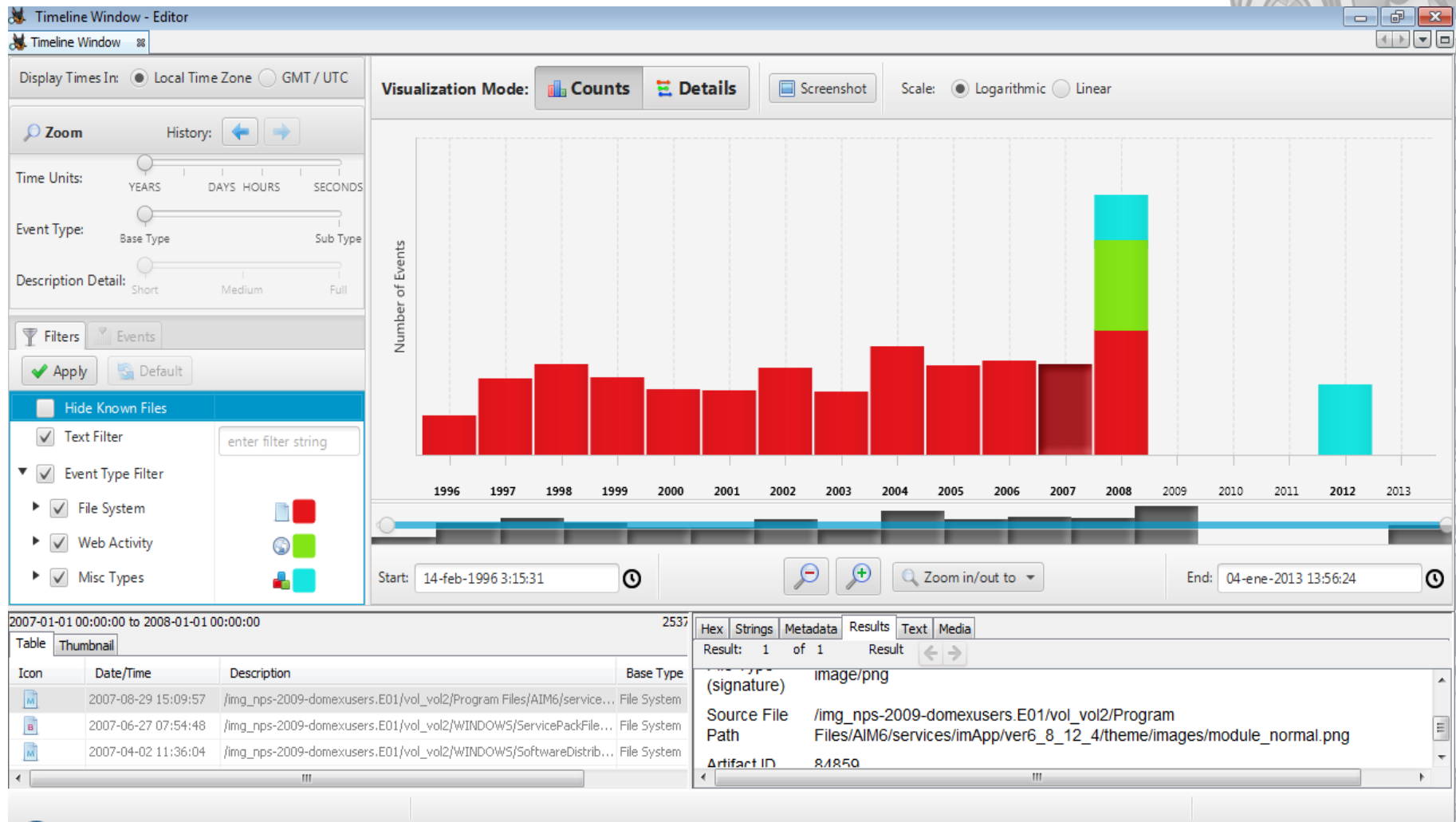
- Análisis por Cronología
- Búsqueda de Palabras Clave
- Artefactos Web
- Análisis del Registro
- Análisis de Archivos LNK
- Análisis de Correos Electrónicos
- EXIF
- Ordenamiento por Tipo de Archivo
- Reproducción de Medios
- Análisis Robusto de Sistemas de Archivos
- Filtrado por Conjunto de Hashes
- Etiquetas
- Extracción de Cadenas Unicode

\* <http://www.sleuthkit.org/autopsy/features.php>



# ANÁLISIS DE CRONOLOGÍA

Identificar archivos asociados con periodos activos de tiempo para enfocarse en su análisis



\* <http://www.sleuthkit.org/autopsy/timeline.php>

# BÚSQUEDA DE PALABRAS CLAVE

Autopsy 3 utiliza el poderoso motor para indexación de texto Apache SOLR.

Directory Listing  
/img\_nps-2009-domexusers.dd.raw/vol\_2

Name	Modified Time	Change Time	Access Time	Created Time	Size
\$Extend	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	344
\$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
\$Unalloc					
[current			10:56:39 COT	2008-10-20 09:26:07 COT	56
Docume			10:56:40 COT	2008-10-20 09:30:07 COT	56
MSOCad			11:47:12 COT	2008-10-28 11:40:03 COT	256
Program			11:39:40 COT	2008-10-20 09:30:51 COT	168
RECYCL			22:38:44 COT	2008-10-28 11:58:32 COT	600

**Ingest Modules**

- Recent Activity
- Hash Lookup
- File Type Identification
- Archive Extractor
- Exif Parser
- Keyword Search**
- Email Parser
- Extension Mismatch Detector
- E01 Verifier
- Android Analyzer

Select keyword lists to enable during ingest:

- Phone Numbers
- IP Addresses
- Email Addresses
- URLs

Scripts enabled for string extraction from unknown file types:

Latin - Basic

Encodings: UTF8, UTF16

Process Unallocated Space

Performs file indexing and periodic search... **Advanced**

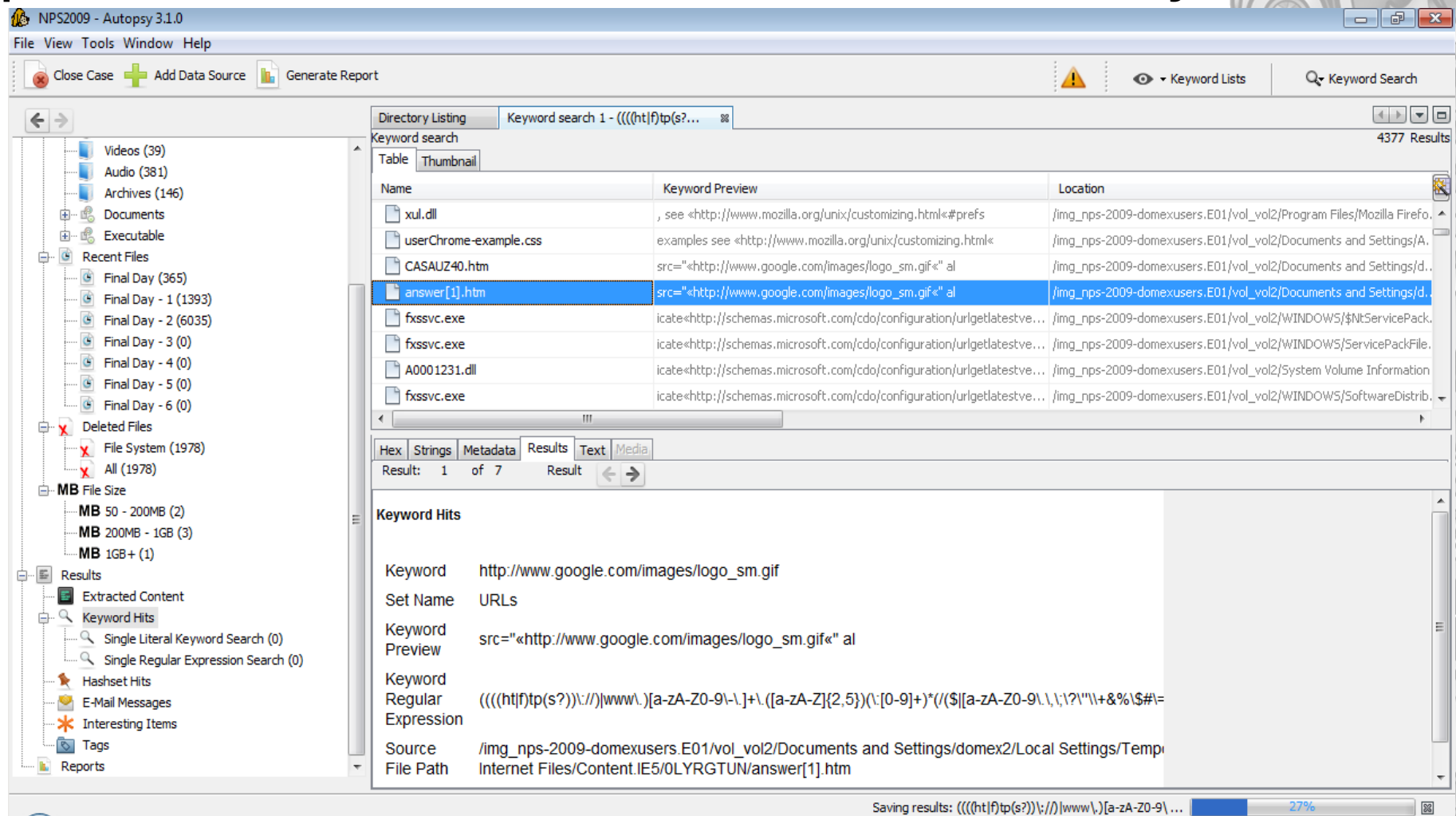
**Start** **Close**

\* <http://lucene.apache.org/solr/>

\* <http://www.sleuthkit.org/autopsy/keyword.php>

# BÚSQUEDA DE PALABRAS CLAVE (Cont.)

Autopsy 3 utiliza Apache Tika y otras librerías para extraer texto de HTML, M\$, PDF, y más.



Directory Listing Keyword search 1 - (((ht|f)tp(s)?... 88

Keyword search 4377 Results

Name	Keyword Preview	Location
xul.dll	, see <http://www.mozilla.org/unix/customizing.html#prefs	/img_nps-2009-domexusers.E01/vol_vol2/Program Files/Mozilla Firefo...
userChrome-example.css	examples see <http://www.mozilla.org/unix/customizing.html#	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/A...
CASAUZ40.htm	src="<http://www.google.com/images/logo_sm.gif" al	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...
answer[1].htm	src="<http://www.google.com/images/logo_sm.gif" al	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...
fxssvc.exe	icate<http://schemas.microsoft.com/cdo/configuration/urlgetlatestve...	/img_nps-2009-domexusers.E01/vol_vol2/WINDOWS/\$NtServicePack...
fxssvc.exe	icate<http://schemas.microsoft.com/cdo/configuration/urlgetlatestve...	/img_nps-2009-domexusers.E01/vol_vol2/WINDOWS/ServicePackFile...
A0001231.dll	icate<http://schemas.microsoft.com/cdo/configuration/urlgetlatestve...	/img_nps-2009-domexusers.E01/vol_vol2/System Volume Information...
fxssvc.exe	icate<http://schemas.microsoft.com/cdo/configuration/urlgetlatestve...	/img_nps-2009-domexusers.E01/vol_vol2/WINDOWS/SoftwareDistrib...

Hex Strings Metadata Results Text Media

Result: 1 of 7 Result < >

**Keyword Hits**

Keyword	http://www.google.com/images/logo_sm.gif
Set Name	URLs
Keyword Preview	src="<http://www.google.com/images/logo_sm.gif" al
Keyword Regular Expression	(((ht f)tp(s)?:// www\.)[a-zA-Z0-9\-\.\+]{2,5})(\.[a-zA-Z0-9\-\.\+]{0-9})*((/ [/\?!\ &%\\$\#]=
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex2/Local Settings/Temp... Internet Files/Content.IE5/OLYRGTUN/answer[1].htm

Saving results: (((ht|f)tp(s)?://|www\.)[a-zA-Z0-9\-\.\+]{2,5})(\.[a-zA-Z0-9\-\.\+]{0-9})\*((/|[/\?!\|&%\\$\#]= 27%

\* <http://tika.apache.org/>

\* <http://www.sleuthkit.org/autopsy/keyword.php>

# ARTEFACTOS WEB

Extrae información de Marcadores, Cookies, Historial, Descargas y Consultas de Búsqueda.

The screenshot displays the NPS2009 - Autopsy 3.1.0 interface. The left sidebar shows a tree view of data sources, including 'Final Day' folders, 'Deleted Files', 'File System', 'All', 'MB File Size', and 'Results'. The 'Results' section is expanded, showing 'Web History (2023)'. The main window displays a 'Directory Listing' for 'Keyword search 1 - (((ht|f|tp(s?...))'. Below this is a 'Web History' table with columns for 'Source File', 'URL', 'Date Accessed', and 'Referrer URL'. The table shows several entries, with one entry highlighted in blue. Below the table is a 'Text' view showing the details of the selected entry, including the URL, date accessed, referrer URL, title, program name, domain, source, and file path.

Source File	URL	Date Accessed	Referrer URL
places.sqlite	http://bl126w.blu126.mail.live.com/mail/EditMessageLight.aspx?Read...	2008-10-29 22:34:37 COT	http://news.bbc.co.uk/go/rss/-/2/hi/science/nature/7697482.stm
places.sqlite	http://bl126w.blu126.mail.live.com/mail/browsersupport.aspx?target...	2008-10-29 22:34:34 COT	http://news.bbc.co.uk/go/rss/-/2/hi/science/nature/7697482.stm
places.sqlite	http://bl126w.blu126.mail.live.com/mail/EditMessageLight.aspx?Read...	2008-10-29 22:34:43 COT	http://news.bbc.co.uk/go/rss/-/2/hi/middle_east/7697630.stm
index.dat	aim.com/	2008-10-20 22:43:31 COT	
index.dat	microsoftwga.112.2o7.net/	2008-10-20 22:40:22 COT	
index.dat	revsci.net/	2008-10-20 22:43:31 COT	
index.dat	m.webtrends.com/	2008-10-20 22:40:22 COT	
index.dat	update.microsoft.com/	2008-10-21 01:29:08 COT	

Result: 290 of 364

URL http://bl126w.blu126.mail.live.com/mail/EditMessageLight.aspx?ReadMessageId=f2b3b5fb-d1e0-4ef2-ac64-2dab6e908f31&FolderID=00  
Date Accessed 2008-10-29 22:34:43  
Referrer URL http://news.bbc.co.uk/go/rss/-/2/hi/middle\_east/7697630.stm  
Title Windows Live Hotmail  
Program Name Firefox  
Domain bl126w.blu126.mail.live.com  
Source /img\_nps-2009-domexusers.E01/vol\_vol2/Documents and Settings/domex2/Application Data/Mozilla/Firefox/Profiles/n2utfxqg.default/pla  
File Path

\* [http://www.sleuthkit.org/autopsy/web\\_artifacts.php](http://www.sleuthkit.org/autopsy/web_artifacts.php)

# ARTEFACTOS WEB (Cont.)

Para facilitar la ubicación de los datos, los resultados de los navegadores son mezclados.

Directory Listing: Keyword search 1 - (((ht|f)tp(s?...))

Web Cookies: 318 Results

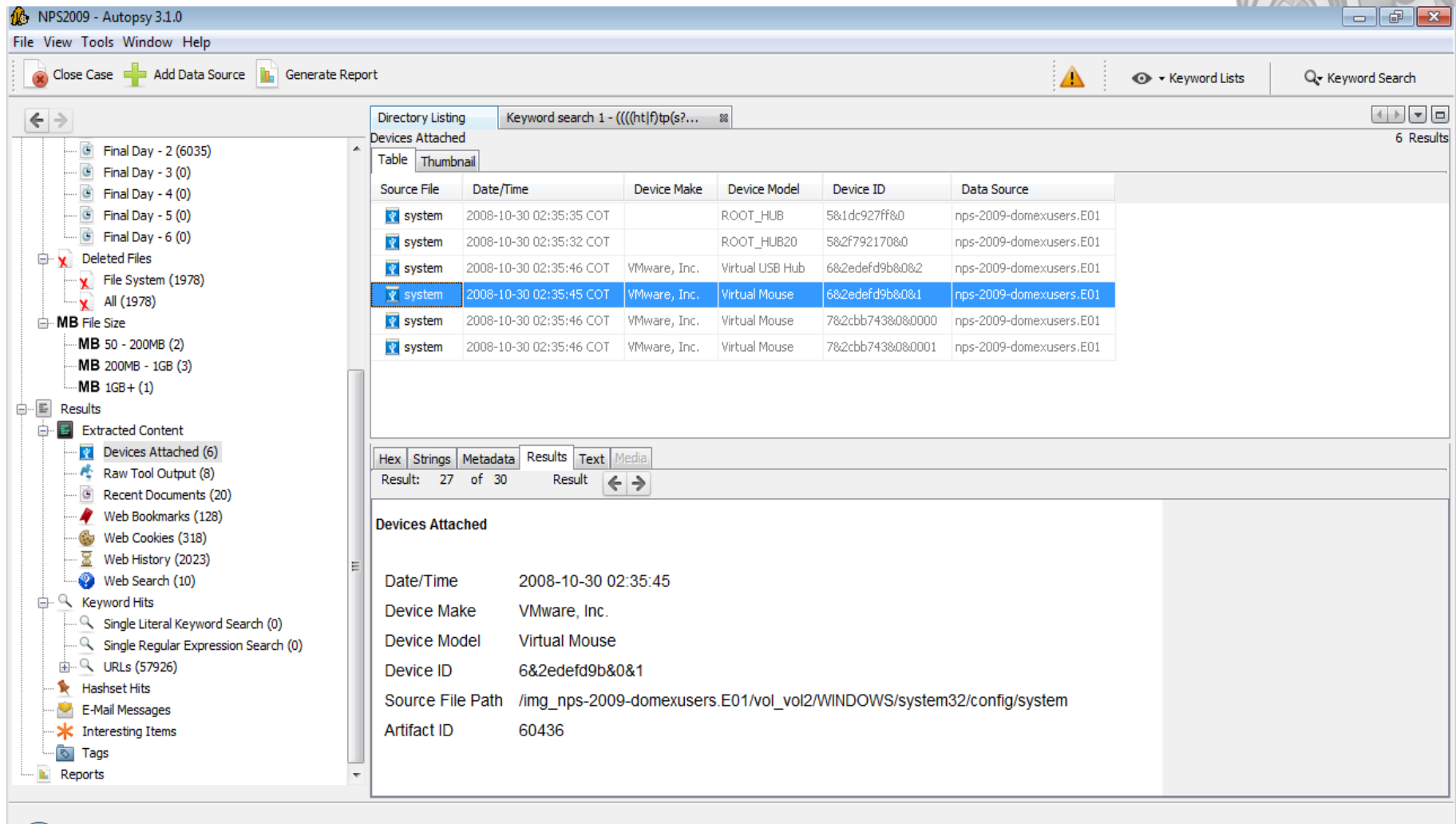
Source File	URL	Date/Time	Name	Value
cookies.sqlite	.atdmt.com	2008-10-29 22:34:16 COT	__qca	1225337594-92665847-43387892
cookies.sqlite	account.live.com	2008-10-29 22:33:59 COT	ANON	A=F2B96C89B05F2560B1E85829FFFFFFF&E=798&W=2
cookies.sqlite	account.live.com	2008-10-29 22:33:59 COT	NAP	V=1.6&E=735&C=4NT-ivRUS8QB8pTjBpMg4O855IRteA1zqr
cookies.sqlite	.advertising.com	2008-10-29 22:34:08 COT	C2	ws5CJlJFIy+FAH
administrator@live.com/	live.com/	2008-10-20 17:40:49 COT	wlidperf	throughput=15&latency=203
administrator@aim.com/	aim.com/	2008-10-20 17:43:31 COT	rsi_ct	2008_10_20:1
administrator@aol.com/	aol.com/	2008-10-20 17:43:04 COT	rsi_ct	2008_10_20:1
administrator@at.atwola.com/	at.atwola.com/	2008-10-20 17:43:12 COT	JEB2	48FCFF886E65181CCD9B41ECF0000622

Matches on page: - of - Match Page: 1 of 1 Page

```
wlidperf
throughput=15&latency=203
live.com/
1088
2189574144
32107986
3865074448
29963012
*
-----METADATA-----
Content-Encoding: ISO-8859-1
```

# ANÁLISIS DEL REGISTRO

Se utiliza RegRipper para identificar dispositivos USB y documentos accedidos.



The screenshot shows the NPS2009 - Autopsy 3.1.0 interface. The main window displays a directory listing of devices attached to a system. The table below shows the results of a keyword search for '(((ht|f)tp(s?...'. The table has 6 columns: Source File, Date/Time, Device Make, Device Model, Device ID, and Data Source. The selected row is highlighted in blue.

Source File	Date/Time	Device Make	Device Model	Device ID	Data Source
system	2008-10-30 02:35:35 COT		ROOT_HUB	5&1dc927ff&0	nps-2009-domexusers.E01
system	2008-10-30 02:35:32 COT		ROOT_HUB20	5&2f792170&0	nps-2009-domexusers.E01
system	2008-10-30 02:35:46 COT	VMware, Inc.	Virtual USB Hub	6&2edefd9b&0&2	nps-2009-domexusers.E01
system	2008-10-30 02:35:45 COT	VMware, Inc.	Virtual Mouse	6&2edefd9b&0&1	nps-2009-domexusers.E01
system	2008-10-30 02:35:46 COT	VMware, Inc.	Virtual Mouse	7&2cbb743&0&0000	nps-2009-domexusers.E01
system	2008-10-30 02:35:46 COT	VMware, Inc.	Virtual Mouse	7&2cbb743&0&0001	nps-2009-domexusers.E01

Below the table, the 'Results' tab is selected, showing a detailed view of the selected device. The details are as follows:

**Devices Attached**

- Date/Time: 2008-10-30 02:35:45
- Device Make: VMware, Inc.
- Device Model: Virtual Mouse
- Device ID: 6&2edefd9b&0&1
- Source File Path: /img\_nps-2009-domexusers.E01/vol\_vol2/WINDOWS/system32/config/system
- Artifact ID: 60436

\* <http://regripper.wordpress.com/>

\* <http://www.sleuthkit.org/autopsy/features.php>

# ANÁLISIS DEL REGISTRO (Cont.)

RegRipper permite la extracción de datos desde los archivos colmena de Windows.

The screenshot shows the Autopsy 3.1.0 interface. The left sidebar displays a tree view of the case, including 'Final Day' folders and 'Results' categories like 'Extracted Content' and 'Raw Tool Output'. The main window is titled 'Raw Tool Output' and shows a table with 8 results. The selected row is:

Source File	Program Name	Text	Data Source
NTUSER.DAT	RegRipper	acmru v.20080324- Gets contents of user's ACMru keySoftware\Micr...	nps-2009-domexusers.E01
NTUSER.DAT	RegRipper	acmru v.20080324- Gets contents of user's ACMru keySoftware\Micr...	nps-2009-domexusers.E01
NTUSER.DAT	RegRipper	acmru v.20080324- Gets contents of user's ACMru keySoftware\Micr...	nps-2009-domexusers.E01
NTUSER.DAT	RegRipper	acmru v.20080324- Gets contents of user's ACMru keySoftware\Micr...	nps-2009-domexusers.E01
NTUSER.DAT	RegRipper	acmru v.20080324- Gets contents of user's ACMru keySoftware\Micr...	nps-2009-domexusers.E01
NTUSER.DAT	RegRipper	acmru v.20080324- Gets contents of user's ACMru keySoftware\Micr...	nps-2009-domexusers.E01
ntuser.dat	RegRipper	acmru v.20080324- Gets contents of user's ACMru keySoftware\Micr...	nps-2009-domexusers.E01
system	RegRipper	ControlSet001\Control\Session Manager\AppCertDlls not found.-----...	nps-2009-domexusers.E01

Below the table, the 'Text' tab is selected, showing the following registry value details:

```
-----  
compname v.20090727  
(System) Gets ComputerName and Hostname values from System hive  
  
ComputerName = REALISTIC_XP  
TCP/IP Hostname = Realistic_XP  
  
-----  
crashcontrol v.20081212  
(System) Get crash control information  
  
CrashDumpEnabled = 3 [Small (64kb) memory dump]  
DumpFile = %SystemRoot%\MEMORY.DMP  
MinidumpDir = %SystemRoot%\Minidump
```

- \* <http://regripper.wordpress.com/>
- \* <http://www.sleuthkit.org/autopsy/features.php>

# ANÁLISIS DE ARCHIVOS LNK

Identifica atajos (accesos directos) y documentos accedidos.

The screenshot displays the NPS2009 - Autopsy 3.1.0 interface. The left sidebar shows a tree view with categories like 'Deleted Files', 'MB File Size', 'Results', 'Extracted Content', 'Web Bookmarks', 'Web Cookies', 'Web History', 'Web Search', 'Keyword Hits', 'Hashset Hits', 'E-Mail Messages', 'Interesting Items', 'Tags', and 'Reports'. The main window is divided into two panes. The top pane, titled 'Directory Listing', shows a table of 'Recent Documents' with columns for 'Source File', 'Path', 'Date/Time', and 'Data Source'. The file 'LicenseKey.lnk' is selected. The bottom pane shows a hex view of the selected file's content, with tabs for 'Hex', 'Strings', 'Metadata', 'Results', 'Text', and 'Media'. The hex view shows a sequence of bytes and their corresponding ASCII characters, including 'L...', '...F...', '.9...', '...O...', 'AA...', '1...', 'CE~1...', '...9...', 'i.c.e.2.0.0.7.E.', 'n.t.e.r.p.r.i.s.', 'e...P.2.O...e7', '...L.I.C.E.N.S~1.TXT', '...4...', '...L.i.c.e.n.', 's.e.K.e.y...t.x.', 't...', and '...'.

Source File	Path	Date/Time	Data Source
autorun.lnk	C:\Documents and Settings\Administrator\Desktop\Office2007Enterp...	2008-10-28 11:39:19 COT	nps-2009-domexusers.E01
LicenseKey.lnk	C:\Documents and Settings\Administrator\Desktop\Office2007Enterp...	2008-10-28 11:39:39 COT	nps-2009-domexusers.E01
Office2007Enterprise.lnk	C:\Documents and Settings\Administrator\Desktop\Office2007Enterp...	2008-10-28 11:39:20 COT	nps-2009-domexusers.E01
My Documents (2).LNK	C:\Documents and Settings\domex1\My Documents	2008-10-29 11:14:52 COT	nps-2009-domexusers.E01
My Documents.LNK	C:\Documents and Settings\domex1\My Documents	2008-10-29 11:14:52 COT	nps-2009-domexusers.E01
Templates.LNK	C:\Documents and Settings\domex1\Application Data\Microsoft\Temp...	2008-10-29 11:15:44 COT	nps-2009-domexusers.E01
This is a spreadsheet by domex user 1.LNK	C:\Documents and Settings\domex1\My Documents\This is a spreads...	2008-10-29 11:16:28 COT	nps-2009-domexusers.E01
This is a spreadsheet deleted by domex user 1.LNK	C:\Documents and Settings\domex1\My Documents\This is a spreads...	2008-10-29 11:17:24 COT	nps-2009-domexusers.E01

# EXIF

## Extrae información de geolocalización y de la cámara desde archivos JPEG.

The screenshot displays the Autopsy 3.1.0 interface. On the left, a tree view shows the file structure, including 'Final Day' folders and 'Results'. The main pane shows a 'Directory Listing' of EXIF Metadata with 14 results. A grid of image thumbnails is visible, with the last one (5AE35B40d01) selected. Below the thumbnails, the file path is shown: `/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Application Data/Mozilla/Firefox/Profiles/ngem72bk.default/Cache/5AE35B40d01`. The bottom pane displays the EXIF Metadata for the selected image:

Field	Value
Date Created	2008-08-22 21:28:40
Device Model	NIKON D2X
Device Make	NIKON CORPORATION
Source File Path	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/domex1/Local Settings/Application Data/Mozilla/Firefox/Profiles/ngem72bk.default/Cache/5AE35B40d01

\* [http://en.wikipedia.org/wiki/Exchangeable\\_image\\_file\\_format](http://en.wikipedia.org/wiki/Exchangeable_image_file_format)

\* <http://www.sleuthkit.org/autopsy/features.php>



# DETECTAR INCONGRUENCIA EN EXTENSIÓN

Detecta la no coincidencia de la extensión asignada a un archivo.

The screenshot shows the NPS2009 - Autopsy 3.1.0 interface. The main window displays a directory listing with a table of files. A message at the top of the listing area says "Extension Mismatch Detected". The table has columns for Source File, Extension, MIME Type, and Data Source. The file "copycd.wmv" is highlighted, showing a mismatch between its extension (.wmv) and its MIME type (text/html).

Source File	Extension	MIME Type	Data Source
nuskin.wmv	wmv	audio/x-ms-wma	nps-2009-domexusers.E01
mdlib.wmv	wmv	audio/x-ms-wma	nps-2009-domexusers.E01
ipp_util.inc	inc	text/html	nps-2009-domexusers.E01
copycd.wmv	wmv	audio/x-ms-wma	nps-2009-domexusers.E01
search.asp	asp	text/html	nps-2009-domexusers.E01
query.asp	asp	text/html	nps-2009-domexusers.E01
default.asp	asp	text/html	nps-2009-domexusers.E01
MSPUB.PUB	pub	application/x-msoffice	nps-2009-domexusers.E01
search.asp	asp	text/html	nps-2009-domexusers.E01
query.asp	asp	text/html	nps-2009-domexusers.E01
ipp_util.inc	inc	text/html	nps-2009-domexusers.E01

Below the table, there is a hex dump view showing the raw data of the selected file. The hex dump shows the file's content in hexadecimal and ASCII format.

\* [http://www.garykessler.net/library/file\\_sigs.html](http://www.garykessler.net/library/file_sigs.html)

\* <http://www.sleuthkit.org/autopsy/>

# REPRODUCTOR DE MEDIOS

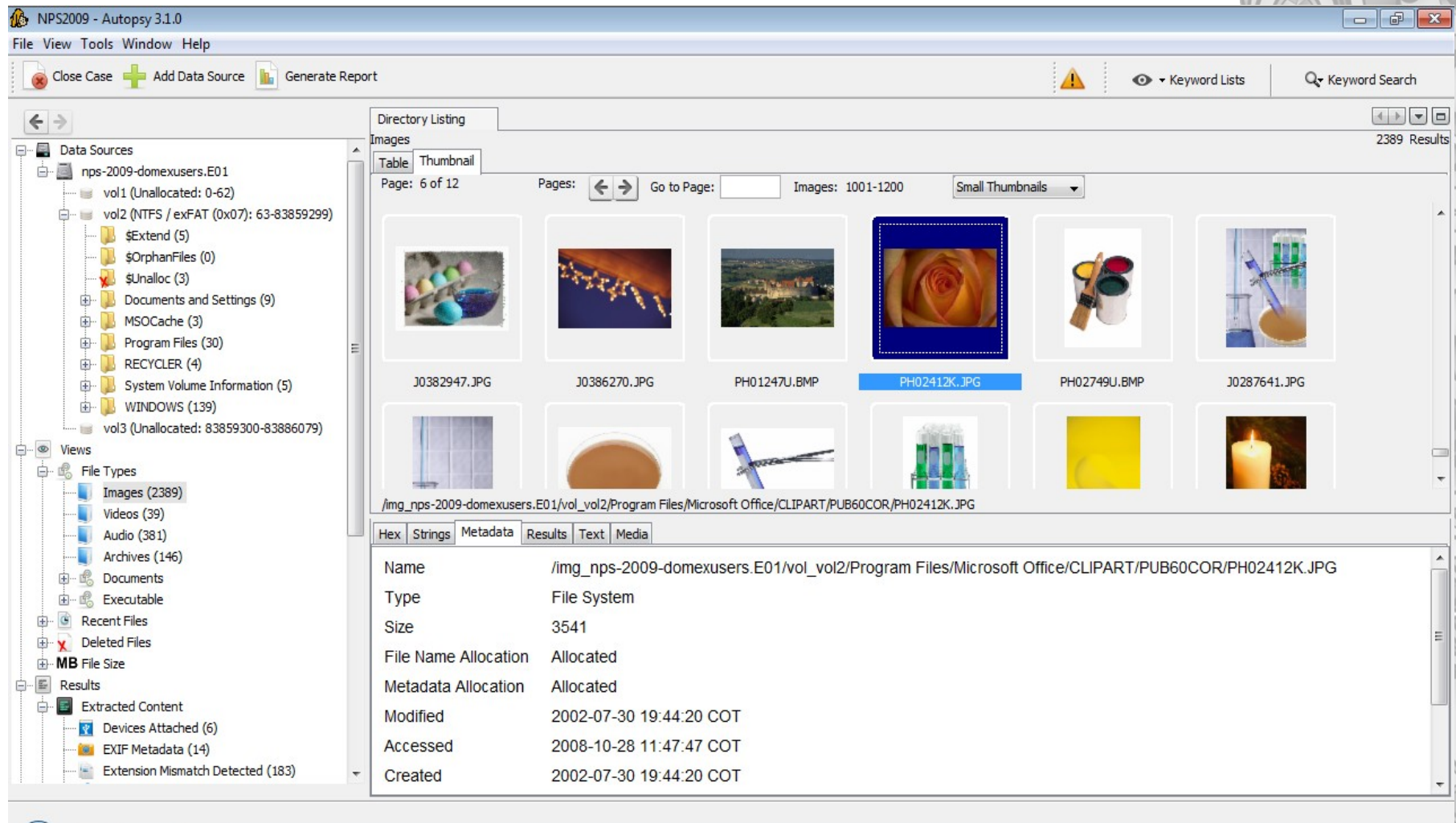
Visualizar videos e imágenes dentro de la aplicación, sin requerir un visor externo.

The screenshot displays the NPS2009 - Autopsy 3.1.0 application window. The interface includes a menu bar (File, View, Tools, Window, Help), a toolbar with buttons for 'Close Case', 'Add Data Source', and 'Generate Report', and a search bar for 'Keyword Lists' and 'Keyword Search'. The main area is divided into a left sidebar for 'Data Sources' and 'Views', and a central 'Directory Listing' pane. The 'Directory Listing' pane shows a table of audio files with columns for Name, Location, Modified Time, Change Time, and Access Time. The file 'New Stories (Highway Blues).wma' is selected. Below the table, a media player interface is visible, showing a play button, a progress bar, and the file path: '/img\_nps-2009-domexusers.E01/vol\_vol2/Documents and Settings/All Users/Documents/My Music/Sample Music/New Stories (Highway Blues).wma'. The media player shows a duration of 00:00:29/00:01:33.

Name	Location	Modified Time	Change Time	Access Time
sndrec.wav	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/A...	2004-08-04 07:00:00 COT	2008-10-20 16:58:34 COT	2008-10-2...
Beethoven's Symphony No. 9 (Scherzo).wma	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/All...	2004-08-04 07:00:00 COT	2008-10-20 16:36:02 COT	2008-10-2...
New Stories (Highway Blues).wma	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/All...	2004-08-04 07:00:00 COT	2008-10-20 16:36:02 COT	2008-10-2...
sndrec.wav	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/D...	2004-08-04 07:00:00 COT	2008-10-20 16:35:05 COT	2008-10-2...
sndrec.wav	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...	2004-08-04 07:00:00 COT	2008-10-21 14:12:18 COT	2008-10-2...
sndrec.wav	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...	2004-08-04 07:00:00 COT	2008-10-21 14:29:51 COT	2008-10-2...
Blip.wav	/img_nps-2009-domexusers.E01/vol_vol2/Program Files/NetMeeting/...	2004-08-04 07:00:00 COT	2008-10-20 16:36:00 COT	2008-10-2...
TestSnd.wav	/img_nps-2009-domexusers.E01/vol_vol2/Program Files/NetMeeting/...	2004-08-04 07:00:00 COT	2008-10-20 16:36:00 COT	2008-10-2...
IncomingCall.mp3	/img_nps-2009-domexusers.E01/vol_vol2/Program Files/AIM6/service...	2007-08-16 13:14:47 COT	2008-10-21 10:09:31 COT	2008-10-2...
PhoneRingInternal.mp3	/img_nps-2009-domexusers.E01/vol_vol2/Program Files/AIM6/service...	2007-08-10 14:55:23 COT	2008-10-21 10:09:31 COT	2008-10-2...

# VISOR DE MINIATURAS

Muestra las miniaturas de las imágenes para ayudar a visualizar rápidamente fotografías.



The screenshot displays the NPS2009 - Autopsy 3.1.0 interface. The main window shows a directory listing of images, with a thumbnail viewer displaying a grid of image thumbnails. The selected image is PH02412K.JPG, which is a close-up of a rose. The interface includes a menu bar (File, View, Tools, Window, Help), a toolbar with buttons for Close Case, Add Data Source, and Generate Report, and a search bar for Keyword Lists and Keyword Search. The left pane shows the Data Sources tree, including nps-2009-domexusers.E01 and its sub-directories. The bottom pane shows the metadata for the selected image.

Hex	Strings	Metadata	Results	Text	Media
Name	/img_nps-2009-domexusers.E01/vol_vol2/Program Files/Microsoft Office/CLIPART/PUB60COR/PH02412K.JPG				
Type	File System				
Size	3541				
File Name Allocation	Allocated				
Metadata Allocation	Allocated				
Modified	2002-07-30 19:44:20 COT				
Accessed	2008-10-28 11:47:47 COT				
Created	2002-07-30 19:44:20 COT				

\* <http://www.sleuthkit.org/autopsy/features.php>

# ANÁLISIS PARA SISTEMAS DE ARCHIVOS

Soporta los Sistemas de Archivos más comunes, NTFS, FAT12/16/32, Ext2/3, y otros.

The screenshot displays the NPS2009 - Autopsy 3.1.0 interface. The main window shows a directory listing for the path `/img_nps-2009-domexusers.E01/vol_vol2`. A dialog box titled "General Volume Information" is open, displaying the following details:

Property	Value
Volume ID:	2
Starting Sector:	63
Length in Sectors:	83859237
Description:	NTFS / exFAT (0x07)
Flags:	Allocated

The background interface shows a tree view of data sources, including `nps-2009-domexusers.E01` and `vol2 (NTFS / exFAT (0x07): 63-83859299)`. The main window also displays a table of file listings with columns for Name, Modified Time, Change Time, Access Time, Created Time, and Size. The bottom of the interface shows a list of extracted content, including `RSTR`, `NTFS`, `RSTR`, `NTFS`, `RCRD`, `Tahoma`, `ew Roman`, `Tahoma`, `ew Roman`, `Tahoma`, and `Serif`.

# FILTRAR POR CONJUNTO DE HASHS

Filtra archivos conocidos buenos utilizando NSRL (National Software Reference Library).

The screenshot shows the Autopsy 3.1.0 interface. A 'Hash Set Configuration' dialog box is open, showing the configuration for the 'NSRLFile' hash set. The dialog includes the following information:

- Hash Databases: NSRLFile
- Information:
  - Hash Set Name: NSRLFile
  - Type: Known
  - Database Path: \\Ryds\yds245\yds\_unified\NSRLFile.txt
  - Index Path: \\Ryds\yds245\yds\_unified\NSRLFile.txt-md5.idx
  - Index Status: Indexed
- Options:
  - Send ingest inbox message for each hit

Buttons at the bottom of the dialog include 'Create Database', 'Import Database', 'Delete Database', 'Re-Index', 'OK', and 'Cancel'.

The background shows a directory listing of data sources. The 'Results' pane at the bottom right displays a table with the following columns: 'Created Time' and 'Size'. The table contains 30 results, with the first few rows showing:

Created Time	Size
2008-10-20 09:26:07 COT	344
0000-00-00 00:00:00	0
0000-00-00 00:00:00	0
2008-10-20 09:26:07 COT	56
2008-10-20 09:30:07 COT	56
2008-10-28 11:40:03 COT	256
2008-10-20 09:30:51 COT	168
2008-10-28 11:58:32 COT	600
2008-10-20 09:30:07 COT	56
2008-10-20 09:26:16 COT	56
2008-10-20 09:26:07 COT	2560

\* <http://www.nsrل.nist.gov>

\* <http://www.sleuthkit.org/autopsy/features.php>

# FILTRAR POR CONJUNTO DE HASHS (Cont.)

Etiqueta archivos conocidos malos utilizando BDs de hashes HashKeeper, md5sum, EnCase.

The screenshot shows the Autopsy 3.1.0 interface. The main window displays a directory listing for the path `/img_nps-2009-domexusers.E01/vol_vol2/WINDOWS/system32/drivers/etc`. The 'hosts' file is selected, and its metadata is shown in the bottom pane.

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode
[current folder]	2008-10-20 09:26:56 COT	2008-10-20 09:26:56 COT	2008-10-30 02:35:30 COT	2008-10-20 09:26:16 COT	560	Allocated	Allocated	drwxrwxrwx 0
[parent folder]	2008-10-21 10:12:43 COT	2008-10-21 10:12:43 COT	2008-10-30 02:35:30 COT	2008-10-20 09:26:16 COT	56	Allocated	Allocated	drwxrwxrwx 0
hosts	2004-08-04 07:00:00 COT	2008-10-20 09:31:09 COT	2008-10-30 11:43:42 COT	2004-08-04 07:00:00 COT	734	Allocated	Allocated	rrwxrwxrwx 0
lmhosts.sam	2004-08-04 07:00:00 COT	2008-10-20 09:31:09 COT	2008-10-20 09:26:41 COT	2004-08-04 07:00:00 COT	3683	Allocated	Allocated	rrwxrwxrwx 0
networks	2004-08-04 07:00:00 COT	2008-10-20 09:31:09 COT	2008-10-20 09:26:45 COT	2004-08-04 07:00:00 COT	407	Allocated	Allocated	rrwxrwxrwx 0
protocol	2004-08-04 07:00:00 COT	2008-10-20 09:31:09 COT	2008-10-20 09:26:50 COT	2004-08-04 07:00:00 COT	799	Allocated	Allocated	rrwxrwxrwx 0
services	2004-08-04 07:00:00 COT	2008-10-20 09:31:09 COT	2008-10-20 09:26:56 COT	2004-08-04 07:00:00 COT	7116	Allocated	Allocated	rrwxrwxrwx 0

Hex	Strings	Metadata	Results	Text	Media
Metadata Allocation		Allocated			
Modified		2004-08-04 07:00:00 COT			
Accessed		2008-10-30 11:43:42 COT			
Created		2004-08-04 07:00:00 COT			
Changed		2008-10-20 09:31:09 COT			
MD5		de1cbfe6c3086010af115a1f00909b01			
Hash Lookup Results		KNOWN			
Internal ID		34307			

\* <http://www.nsrll.nist.gov>

\* <http://www.sleuthkit.org/autopsy/features.php>

# ETIQUETAS

Etiquetar archivos con nombre varios, como 'marcador' o 'sospechoso' y añadir comentarios

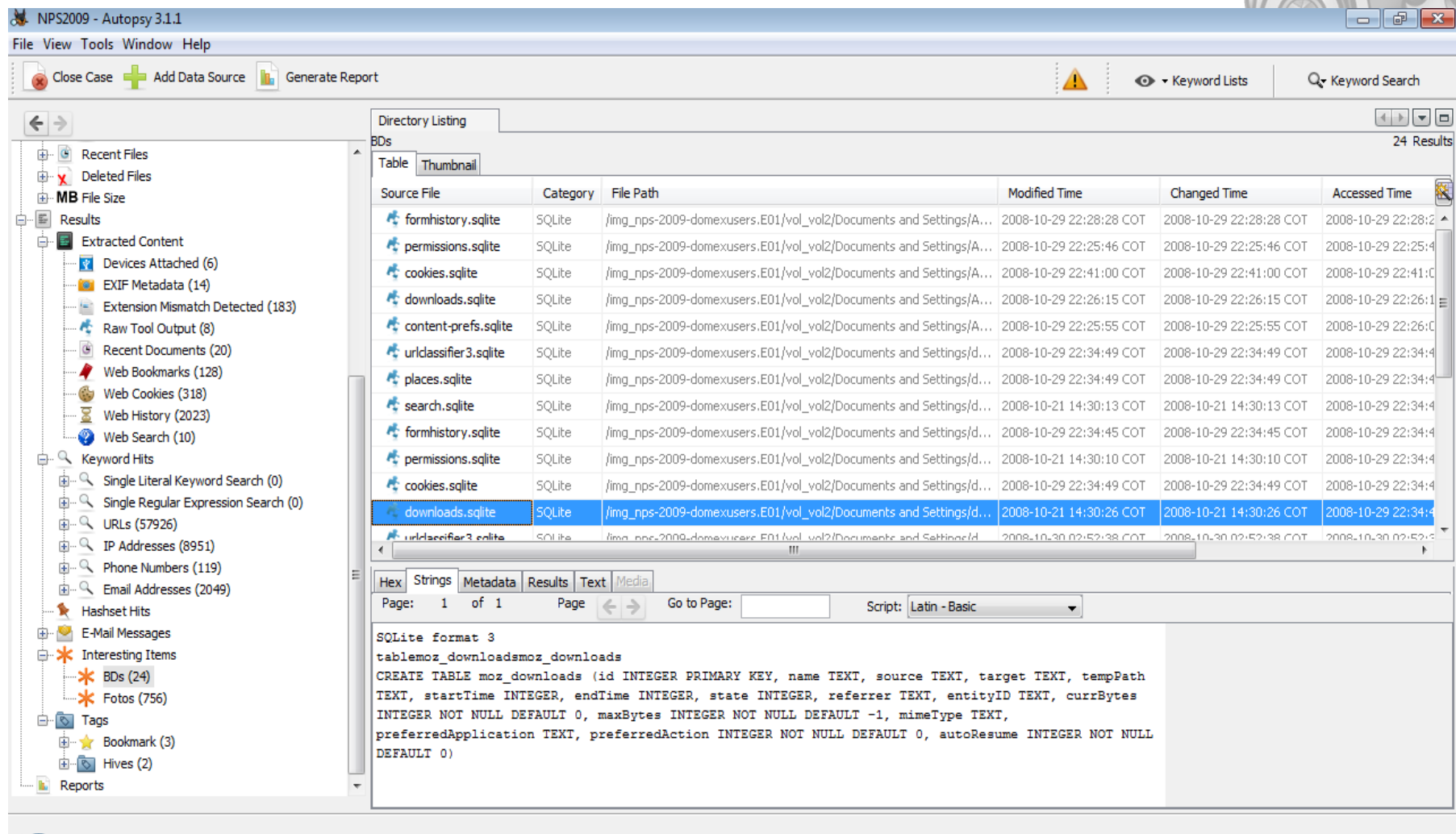
The screenshot shows the NPS2009 - Autopsy 3.1.0 interface. The main window displays a directory listing for the path `/img_nps-2009-domexusers.E01/vol_2/WINDOWS/system32/config`. The listing includes files such as `SAM`, `SAM.LOG`, `SecEvent.Evt`, `SECURITY`, `SECURITY.LOG`, `software`, `software.LOG`, `software.sav`, `SysEvent.Evt`, `system`, and `system.LOG`. A 'Create Tag' dialog box is open over the listing, with the 'Tag' field set to 'Hives' and the 'Comment' field set to 'Hive Security'. The dialog has 'New Tag', 'OK', and 'Cancel' buttons.

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode
SAM	2008-10-30 11:50:31 COT	2008-10-21 13:39:56 COT	2008-10-30 11:50:31 COT	2008-10-20 09:30:05 COT	262144	Allocated	Allocated	rrwxrw
SAM.LOG	2008-10-30 02:50:09 COT	2008-10-30 02:50:09 COT	2008-10-30 02:50:09 COT	2008-10-20 09:30:05 COT	1024	Allocated	Allocated	rr-xr-x
SecEvent.Evt	2008-10-20 09:30:17 COT	2008-10-20 09:31:09 COT	2008-10-20 09:30:17 COT	2008-10-20 09:30:17 COT	65536	Allocated	Allocated	rrwxrw
SECURITY	2008-10-30 11:50:31 COT	2008-10-29 21:33:59 COT	2008-10-30 11:50:31 COT	2008-10-20 09:30:05 COT	262144	Allocated	Allocated	rrwxrw
SECURITY.LOG	2008-10-30 02:50:09 COT	2008-10-30 02:50:09 COT	2008-10-30 02:50:09 COT	2008-10-20 09:30:05 COT	1024	Allocated	Allocated	rr-xr-x
software	2008-10-30 11:50:31 COT	2008-10-20 09:29:35 COT	2008-10-30 11:50:31 COT	2008-10-20 09:29:35 COT	18874368	Allocated	Allocated	rrwxrw
software.LOG	2008-10-30 02:50:24 COT	2008-10-30 02:50:24 COT	2008-10-30 02:50:24 COT	2008-10-20 09:29:35 COT	1024	Allocated	Allocated	rr-xr-x
software.sav	2008-10-30 09:29:38 COT	2008-10-30 09:29:38 COT	2008-10-30 09:29:38 COT	2008-10-20 09:29:38 COT	659456	Allocated	Allocated	rrwxrw
SysEvent.Evt	2008-10-30 02:50:13 COT	2008-10-30 02:50:13 COT	2008-10-30 02:50:13 COT	2008-10-20 09:30:17 COT	393216	Allocated	Allocated	rrwxrw
system	2008-10-30 11:50:31 COT	2008-10-20 09:29:35 COT	2008-10-30 11:50:31 COT	2008-10-20 09:29:35 COT	4194304	Allocated	Allocated	rrwxrw
system.LOG	2008-10-30 02:50:31 COT	2008-10-20 09:29:35 COT	2008-10-30 02:50:31 COT	2008-10-20 09:29:35 COT	1024	Allocated	Allocated	rr-xr-x

```
regf
Gyb:
emRoot\System32\Config\SECURITY
UNKNOWNNo error - symbol load deferredPdb read access denied
Cvinfo is corrupt
Unrecognized pdb formatImage header paged out
DBGHELP Out of memory
Error in load symbols
DBG not found
PDB not found
Unmatched PDB
```

# ARCHIVOS INTERESANTES

El módulo de archivos interesantes permite marcar archivos por nombres o extensión.



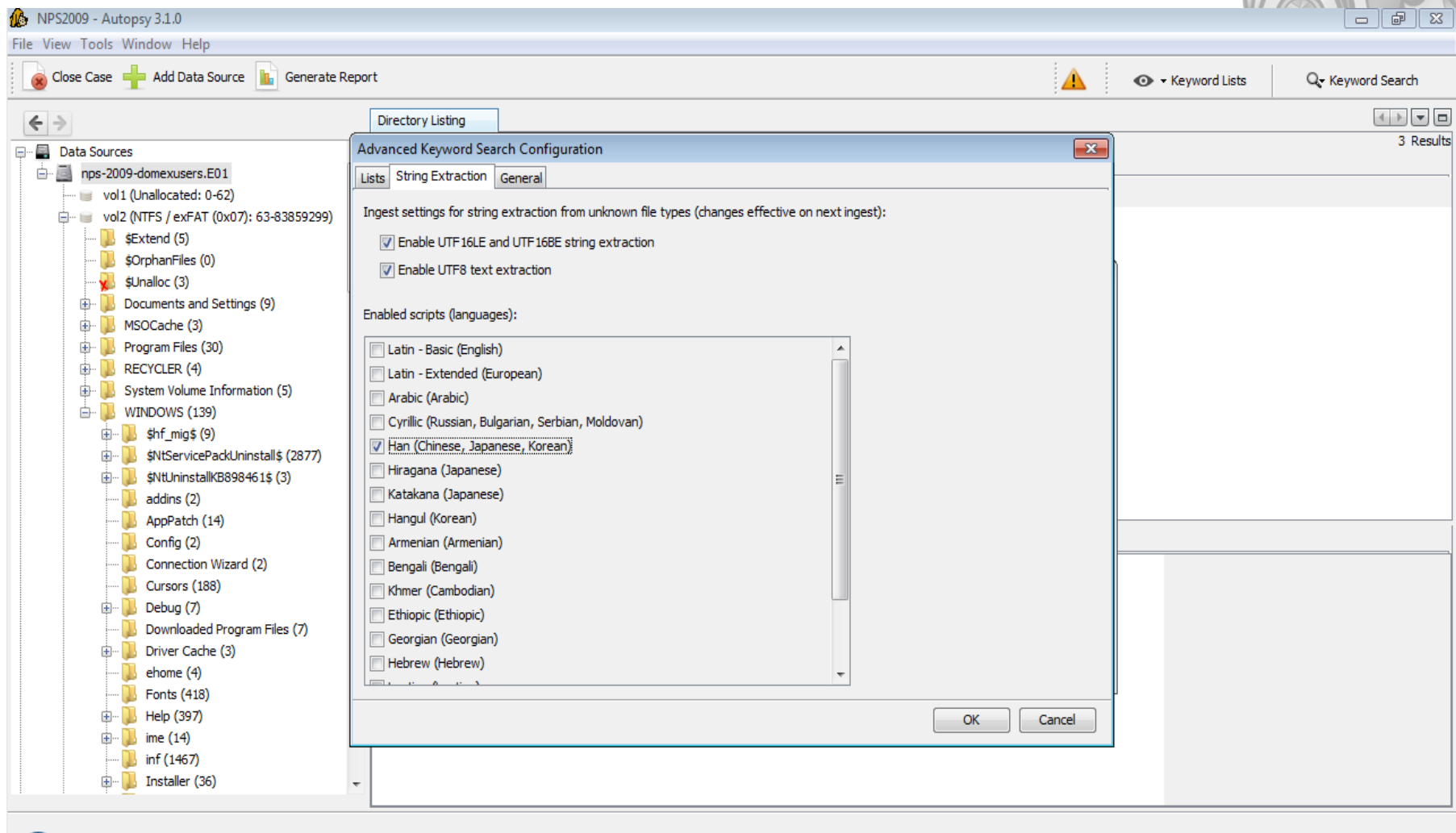
The screenshot displays the Autopsy 3.1.1 interface. On the left, a sidebar shows a tree view of results, including 'Interesting Items' with 24 'BDs' (Binary Data) marked. The main window shows a 'Directory Listing' of 24 results, all of which are SQLite files. The 'downloads.sqlite' file is highlighted in blue. Below the listing, the 'Text' tab is active, showing the SQLite database schema for 'moz\_downloads'.

Source File	Category	File Path	Modified Time	Changed Time	Accessed Time
formhistory.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/A...	2008-10-29 22:28:28 COT	2008-10-29 22:28:28 COT	2008-10-29 22:28:28 COT
permissions.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/A...	2008-10-29 22:25:46 COT	2008-10-29 22:25:46 COT	2008-10-29 22:25:46 COT
cookies.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/A...	2008-10-29 22:41:00 COT	2008-10-29 22:41:00 COT	2008-10-29 22:41:00 COT
downloads.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/A...	2008-10-29 22:26:15 COT	2008-10-29 22:26:15 COT	2008-10-29 22:26:15 COT
content-prefs.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/A...	2008-10-29 22:25:55 COT	2008-10-29 22:25:55 COT	2008-10-29 22:26:00 COT
urlclassifier3.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...	2008-10-29 22:34:49 COT	2008-10-29 22:34:49 COT	2008-10-29 22:34:49 COT
places.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...	2008-10-29 22:34:49 COT	2008-10-29 22:34:49 COT	2008-10-29 22:34:49 COT
search.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...	2008-10-21 14:30:13 COT	2008-10-21 14:30:13 COT	2008-10-29 22:34:49 COT
formhistory.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...	2008-10-29 22:34:45 COT	2008-10-29 22:34:45 COT	2008-10-29 22:34:49 COT
permissions.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...	2008-10-21 14:30:10 COT	2008-10-21 14:30:10 COT	2008-10-29 22:34:49 COT
cookies.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...	2008-10-29 22:34:49 COT	2008-10-29 22:34:49 COT	2008-10-29 22:34:49 COT
downloads.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...	2008-10-21 14:30:26 COT	2008-10-21 14:30:26 COT	2008-10-29 22:34:49 COT
urlclassifier3.sqlite	SQLite	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/d...	2008-10-30 02:52:38 COT	2008-10-30 02:52:38 COT	2008-10-30 02:52:38 COT

```
SQLite format 3
tablemoz_downloadsmoz_downloads
CREATE TABLE moz_downloads (id INTEGER PRIMARY KEY, name TEXT, source TEXT, target TEXT, tempPath TEXT, startTime INTEGER, endTime INTEGER, state INTEGER, referrer TEXT, entityID TEXT, currBytes INTEGER NOT NULL DEFAULT 0, maxBytes INTEGER NOT NULL DEFAULT -1, mimeType TEXT, preferredApplication TEXT, preferredAction INTEGER NOT NULL DEFAULT 0, autoResume INTEGER NOT NULL DEFAULT 0)
```

# EXTRACCIÓN DE CADENAS UNICODE

Extrae cadenas desde el espacio sin asignar y tipos de archivo desconocidos.



# ANÁLISIS DE CORREO ELECTRÓNICO

Interpreta mensajes en formato MBOX, como los del cliente Thunderbird.

Directory Listing  
Default  
267 Results

Date Received	Date Sent	Message (Plaintext)
2012-05-23 08:58:25 COT	2012-05-23 08:58:25 COT	Hello,Personnellement je suis restée à Finale 20
2012-05-23 09:01:22 COT	2012-05-23 09:01:22 COT	Bonjour,Suite à la demande toujours renouvelée
2012-05-23 09:30:43 COT	2012-05-23 09:30:43 COT	OK, ça me va, merci Frédéric.Continue à me me
2012-05-23 18:10:45 COT	2012-05-23 18:10:45 COT	David, Denis, etes vous presents a cette date?
2012-05-24 02:38:51 COT	2012-05-24 02:38:51 COT	Bonjour,J'ai reçu les bouchons de M PHAM et M
2012-05-24 07:31:00 COT	2012-05-24 07:31:00 COT	Quelles sont les dispo du studio d'ici là ?Le 23/0
2012-05-25 07:10:21 COT	2012-05-25 07:10:21 COT	
2012-05-25 11:17:40 COT	2012-05-25 11:17:40 COT	Bonsoir.das sûr d'avoir confirmé (studio et discu

Result: 24 of 267

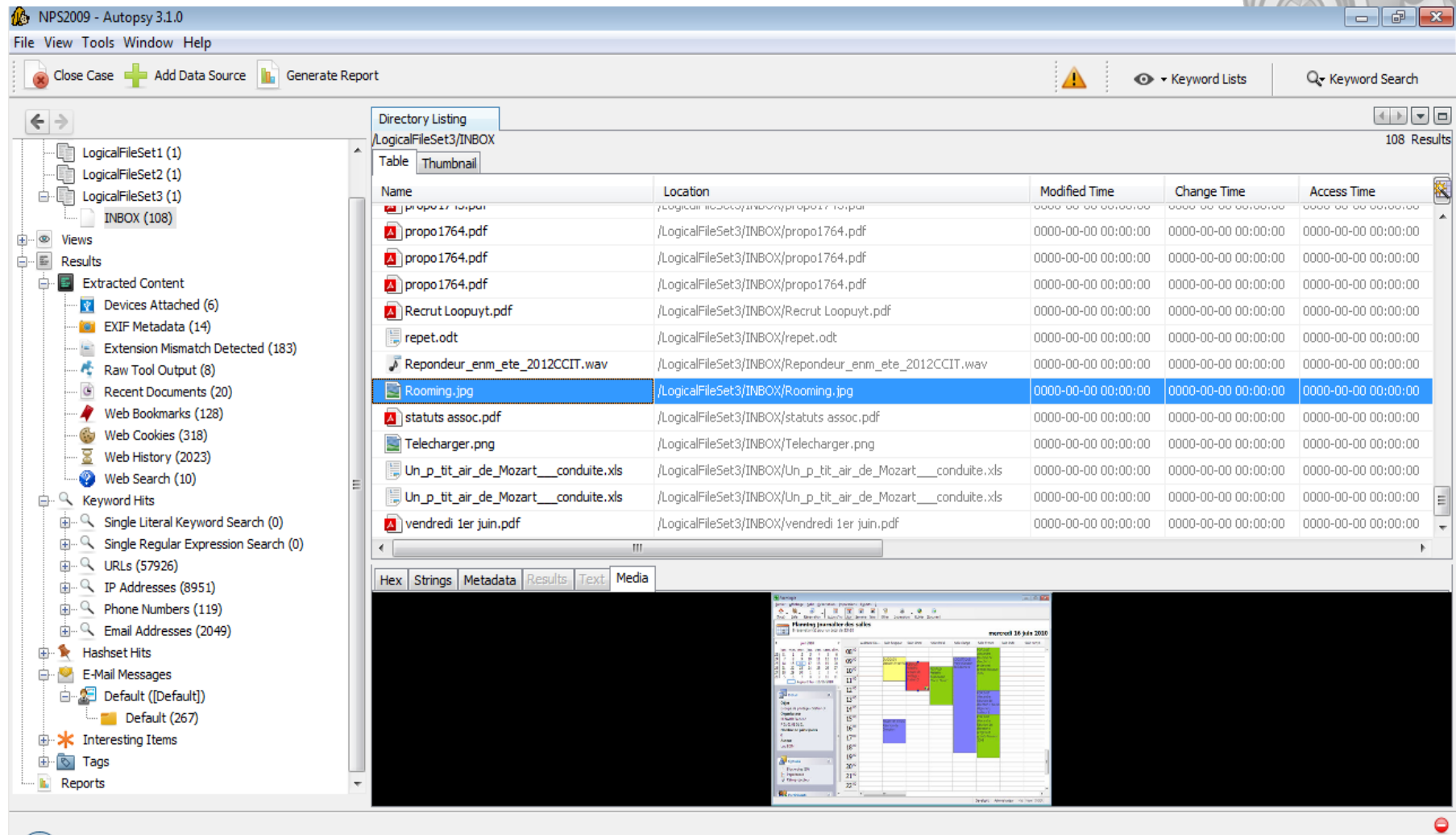
E-Mail To studioenregistrement@enm-villeurbanne.fr;  
E-Mail From directeurtechnique@enm-villeurbanne.fr;  
Date Received 2012-05-24 07:31:00  
Date Sent 2012-05-24 07:31:00  
Quelles sont les dispo du studio d'ici là ?  
Le 23/05/12 12:35, Studio Enregistrement ENMV a écrit :  
> Salut,  
> le piano du studio sonne vraiment "casserole", or je dois enregistrer  
> un projet de DEM.  
> Est-il envisageable de le faire accorder avant mercredi prochain  
> (30mai) 9h30 ?

\* <http://en.wikipedia.org/wiki/Mbox>

\* <http://www.sleuthkit.org/autopsy/features.php>

# ANÁLISIS DE CORREO ELECTRÓNICO (Cont.)

Mbox es un formato de archivo utilizado para manejar colecciones de mensajes de correo.



The screenshot displays the Autopsy 3.1.0 interface. The main window shows a directory listing for the path `/LogicalFileSet3/INBOX` containing 108 results. The table below lists the files and their metadata:

Name	Location	Modified Time	Change Time	Access Time
propo1764.pdf	/LogicalFileSet3/INBOX/propo1764.pdf	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
propo1764.pdf	/LogicalFileSet3/INBOX/propo1764.pdf	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
propo1764.pdf	/LogicalFileSet3/INBOX/propo1764.pdf	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Recrut Loopuyt.pdf	/LogicalFileSet3/INBOX/Recrut Loopuyt.pdf	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
repet.odt	/LogicalFileSet3/INBOX/repet.odt	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Repondeur_enm_ete_2012CCIT.wav	/LogicalFileSet3/INBOX/Repondeur_enm_ete_2012CCIT.wav	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Rooming.jpg	/LogicalFileSet3/INBOX/Rooming.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
statuts assoc.pdf	/LogicalFileSet3/INBOX/statuts assoc.pdf	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Telecharger.png	/LogicalFileSet3/INBOX/Telecharger.png	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Un_p_tit_air_de_Mozart__conduite.xls	/LogicalFileSet3/INBOX/Un_p_tit_air_de_Mozart__conduite.xls	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
Un_p_tit_air_de_Mozart__conduite.xls	/LogicalFileSet3/INBOX/Un_p_tit_air_de_Mozart__conduite.xls	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
vendredi 1er juin.pdf	/LogicalFileSet3/INBOX/vendredi 1er juin.pdf	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

The interface also shows a sidebar with various analysis categories like 'Extracted Content', 'Keyword Hits', and 'E-Mail Messages'. A preview window at the bottom right shows a calendar for June 16, 2010.

- \* <http://en.wikipedia.org/wiki/Mbox>
- \* <http://www.sleuthkit.org/autopsy/features.php>

# FORMATOS DE ENTRADA

Imagen de disco, unidad locales, archivos locales. Entradas en formato raw/dd o E01.

**Directory Listing**

Close Case + Add Data Source Generate Report

Keyword Lists Keyword Search

30 Results

Created Time	Size
2008-10-20 09:26:07 COT	344
0000-00-00 00:00:00	0
0000-00-00 00:00:00	0
2008-10-20 09:26:07 COT	56
2008-10-20 09:30:07 COT	56
2008-10-28 11:40:03 COT	256
2008-10-20 09:30:51 COT	168
2008-10-28 11:58:32 COT	600
2008-10-20 09:30:07 COT	56
2008-10-20 09:26:16 COT	56
2008-10-20 09:26:07 COT	2560

**Add Data Source**

**Steps**

1. Enter Data Source Information
2. Configure Ingest Modules
3. Add Data Source

**Enter Data Source Information wizard (Step 1 of 3)**

Select source type to add: Image File

Browse for an image file: \\RYDS\Images\_DD\NPS-2009-09-26-07\vol2

Please select the input timezone: (GMT-5:00) America/Bogota

Ignore orphan files in FAT file systems  
(faster results, although some data will not be searched)

Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

< Back Next > Finish Cancel Help

\* <http://sourceforge.net/projects/libewf/>

\* <http://www.sleuthkit.org/autopsy/features.php>

# REPORTAR

Infraestructura ampliable de reportes. Los tipos principales son HTML, XLS y Archivo "Body".

Directory Listing  
/img\_nps-2009-domexusers.E01/vol\_vol2  
30 Results

	Created Time	Size
26:07 COT	2008-10-20 09:26:07 COT	791400
26:07 COT	2008-10-20 09:26:07 COT	131072
26:07 COT	2008-10-20 09:26:07 COT	0
37:49 COT	2008-10-20 16:37:49 COT	0
48:42 COT	2008-10-20 09:29:40 COT	211
37:49 COT	2008-10-20 16:37:49 COT	0
37:49 COT	2008-10-20 16:37:49 COT	0
11:15 COT	2008-10-21 10:06:37 COT	385
37:49 COT	2008-10-20 16:37:49 COT	0
29:35 COT	2004-08-04 07:00:00 COT	47564
44:35 COT	2004-08-04 07:00:00 COT	250048
35:57 COT	2008-10-20 09:26:16 COT	805306368

**Generate Report**

**Select and Configure Report Modules**

Report Modules:

- Results - Excel  
A report about results and tagged items in Excel (XLS) format.
- Results - HTML
- Files - Text  
*This report will be configured on the next screen.*
- Google Earth/KML
- TSK Body File

< Back   Next >   Finish   Cancel   Help

# REPORTAR (Bug)

Bug en el código para la generación de reporte en algunos tipos de artefactos. Solución v 3.1.2


The screenshot shows the Autopsy 3.1.0 interface. The main window displays a directory listing for the path `/img_nps-2009-domexusers.E01/vol_vol2`. The listing includes columns for Name, Modified Time, Change Time, Access Time, Created Time, and Size. A table of files is shown below the directory listing. An error message dialog is open in the bottom right corner, indicating a bug in the report generation process.

Name	Modified Time	Change Time	Access Time	Created Time	Size
\$Secure:\$SDS	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	791400
\$UpCase	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	131072
\$Volume	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	2008-10-20 09:26:07 COT	0
AUTOEXEC.BAT	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	0
boot.ini	2008-10-20 16:33:39 COT	2008-10-20 16:38:02 COT	2008-10-30 11:48:42 COT	2008-10-20 09:29:40 COT	211
CONFIG.SYS	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	0
IO.SYS	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	0
IPH.PH	2008-10-21 10:11:15 COT	2008-10-21 10:11:15 COT	2008-10-21 10:11:15 COT	2008-10-21 10:06:37 COT	385
MSDOS.SYS	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	2008-10-20 16:37:49 COT	0
NTDETECT.COM	2004-08-04 07:00:00 COT	2008-10-20 09:31:05 COT	2008-10-20 09:29:35 COT	2004-08-04 07:00:00 COT	47564
ntldr	2008-10-20 19:44:35 COT	2008-10-20 19:44:35 COT	2008-10-20 19:44:35 COT	2004-08-04 07:00:00 COT	250048
pagefile.sys	2008-10-30 02:35:57 COT	2008-10-30 02:35:57 COT	2008-10-30 02:35:57 COT	2008-10-20 09:26:16 COT	805306368

Error generating report  
[Error generating report: java.lang.IndexOutOfBoundsException: Index: 0](#)  
Skipping artifact type TSK\_EMAIL\_MSG in reports  
[Unknown columns to report on](#)

# REPORTAR (Cont.)

Reportes HTML y Excel están completamente empaquetados y pueden ser compartidos.



The screenshot shows a web browser window with the address bar set to 'file:///E:'. The page title is 'Autopsy Forensic Report'. On the left, there is a 'Report Navigation' sidebar with the following items: Case Summary, Devices Attached (6), EXIF Metadata (14), Keyword Hits (69045), Recent Documents (20), Tagged Files (5), Tagged Results (0), Thumbnails (1), Web Bookmarks (128), Web Cookies (318), Web History (2023), and Web Search (10). The main content area displays the following report details:

Case: NPS2009  
Case Number: 003  
Examiner: Alonso Caballero  
Number of Images: 4

**Image Information:**

- nps-2009-domexusers.E01
  - Timezone: America/Bogota
  - Path: Images\_DD\NPS-2009-domexusers\nps-2009-domexusers.E01
- LogicalFile Set1
- LogicalFile Set2
- LogicalFile Set3

# MÁS SOBRE AUTOPSY 3

Sitio Web:



<http://www.sleuthkit.org/autopsy/>

Wiki:

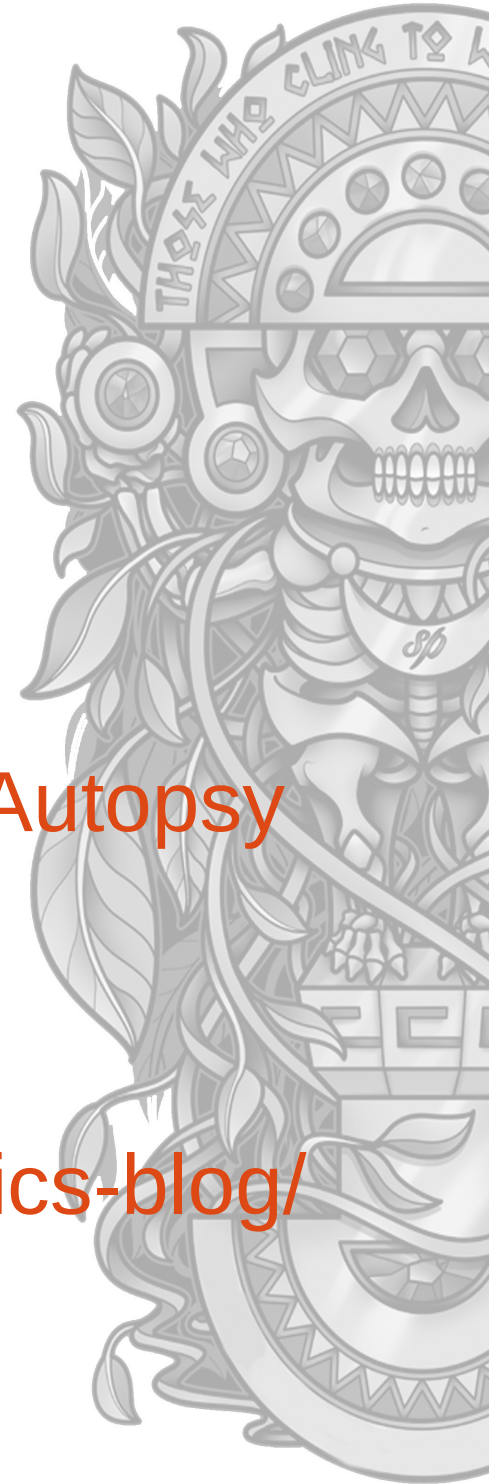


<http://wiki.sleuthkit.org/index.php?title=Autopsy>

Blog:

<http://www.basistech.com/digital-forensics-blog/>

\* Autopsy 3 en Español: <http://www.reydes.com/d/?q=node/2>



# MÁS SOBRE MI PERSONA

Sitio Web:

<http://www.reydes.com>



Twitter:

@Alonso\_ReYDeS

[https://twitter.com/Alonso\\_ReYDeS](https://twitter.com/Alonso_ReYDeS)



LinkedIn:

<http://pe.linkedin.com/in/alonsocaballeroquezada>



\* <http://www.reydes.com>





# PERU HACK

¡Muchas  
Gracias!

Alonso Caballero Quezada  
ReYDeS - @Alonso\_ReYDeS  
[www.reydes.com](http://www.reydes.com)  
[reydes@gmail.com](mailto:reydes@gmail.com)