PERUHACK

Análisis Forense con Autopsy 3

Alonso Caballero Quezada
ReYDeS - @Alonso_ReYDeS
www.reydes.com
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/

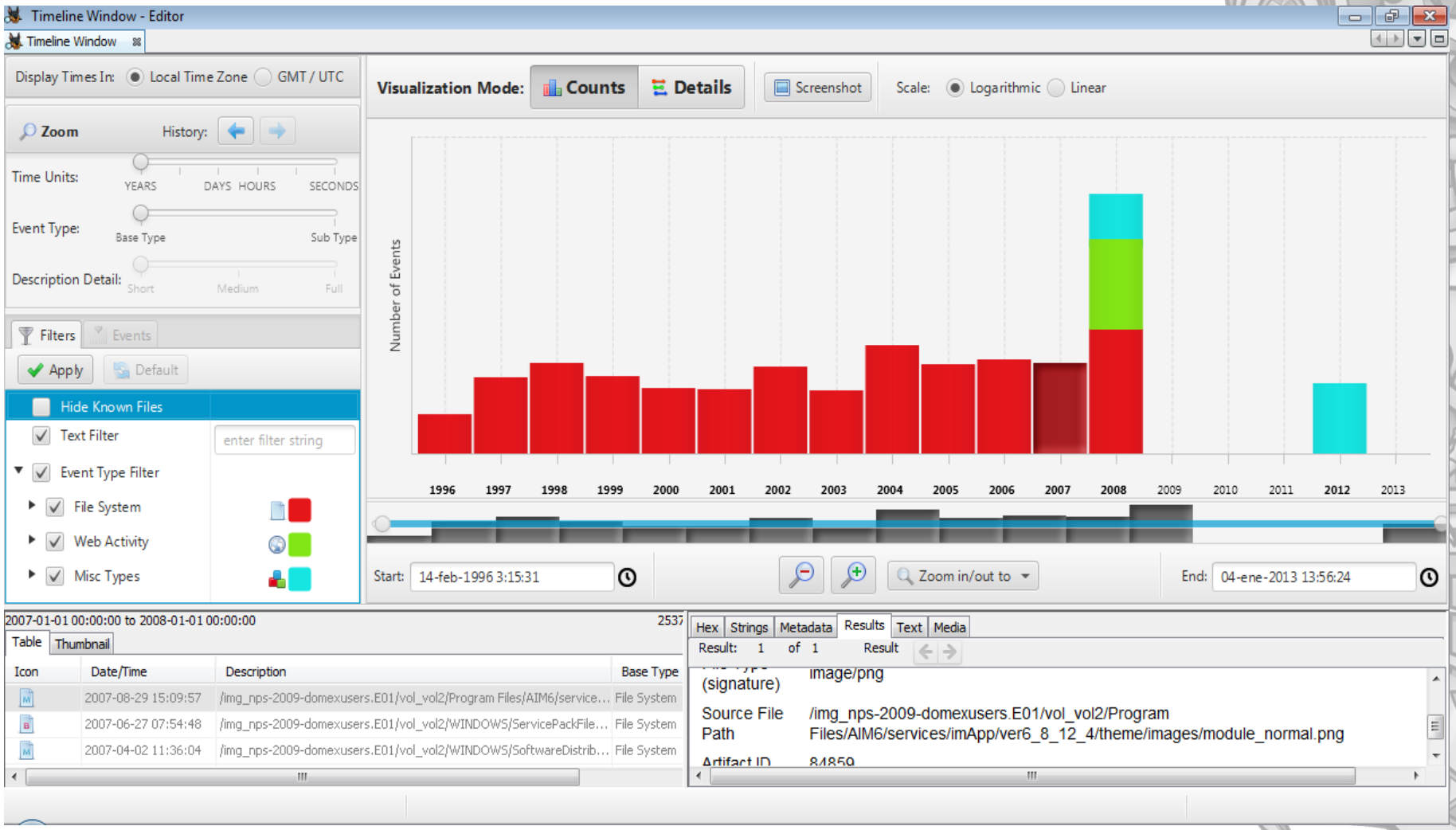
CARACTERÍSTICAS PARA EL ANÁLISIS

- 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

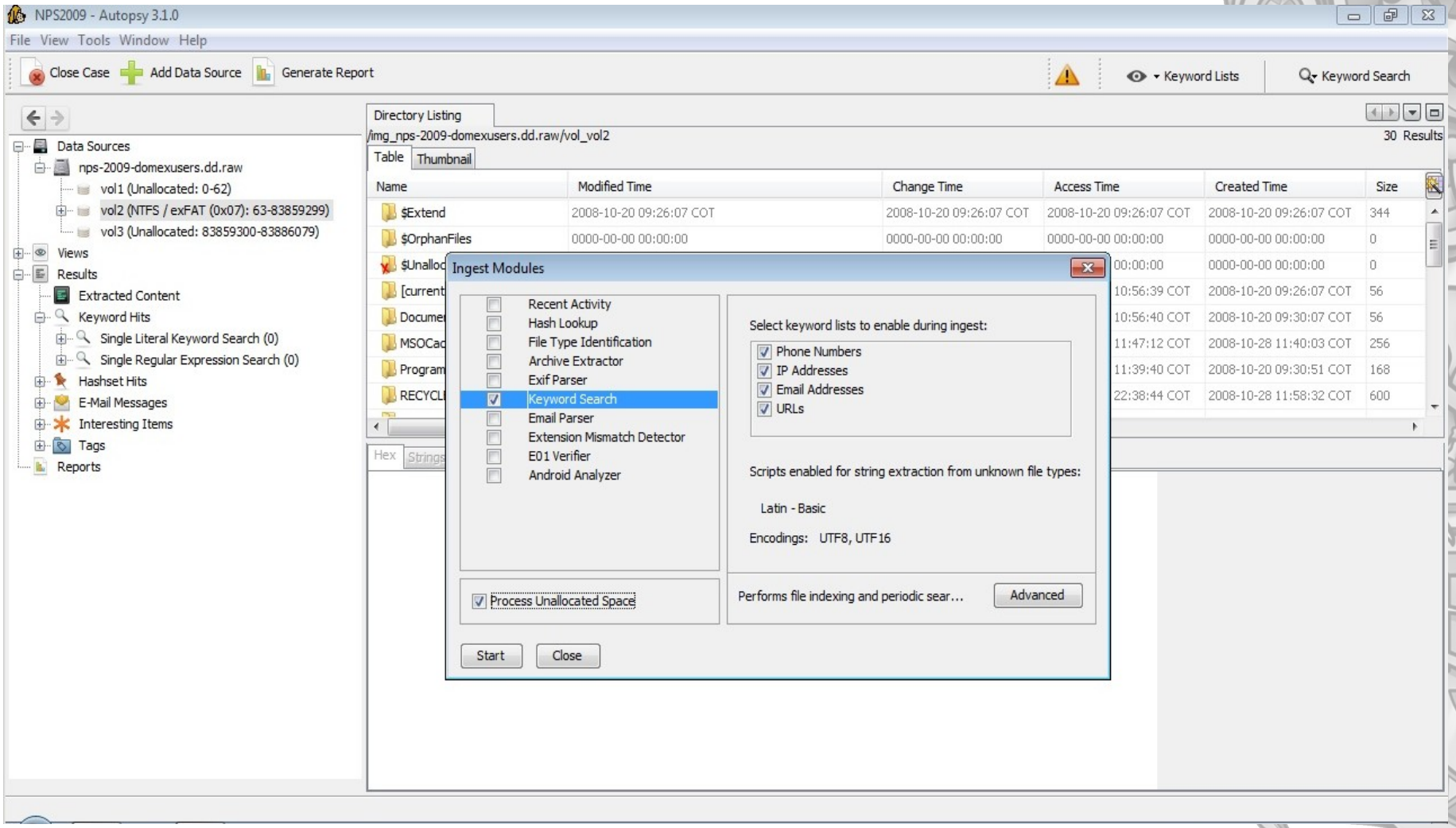
Identificar archivos asociados con periodos activos de tiempo para enfocarse en su análisis



* http://www.sleuthkit.org/autopsy/timeline.php

BÚSQUEDA DE PALABRAS CLAVE

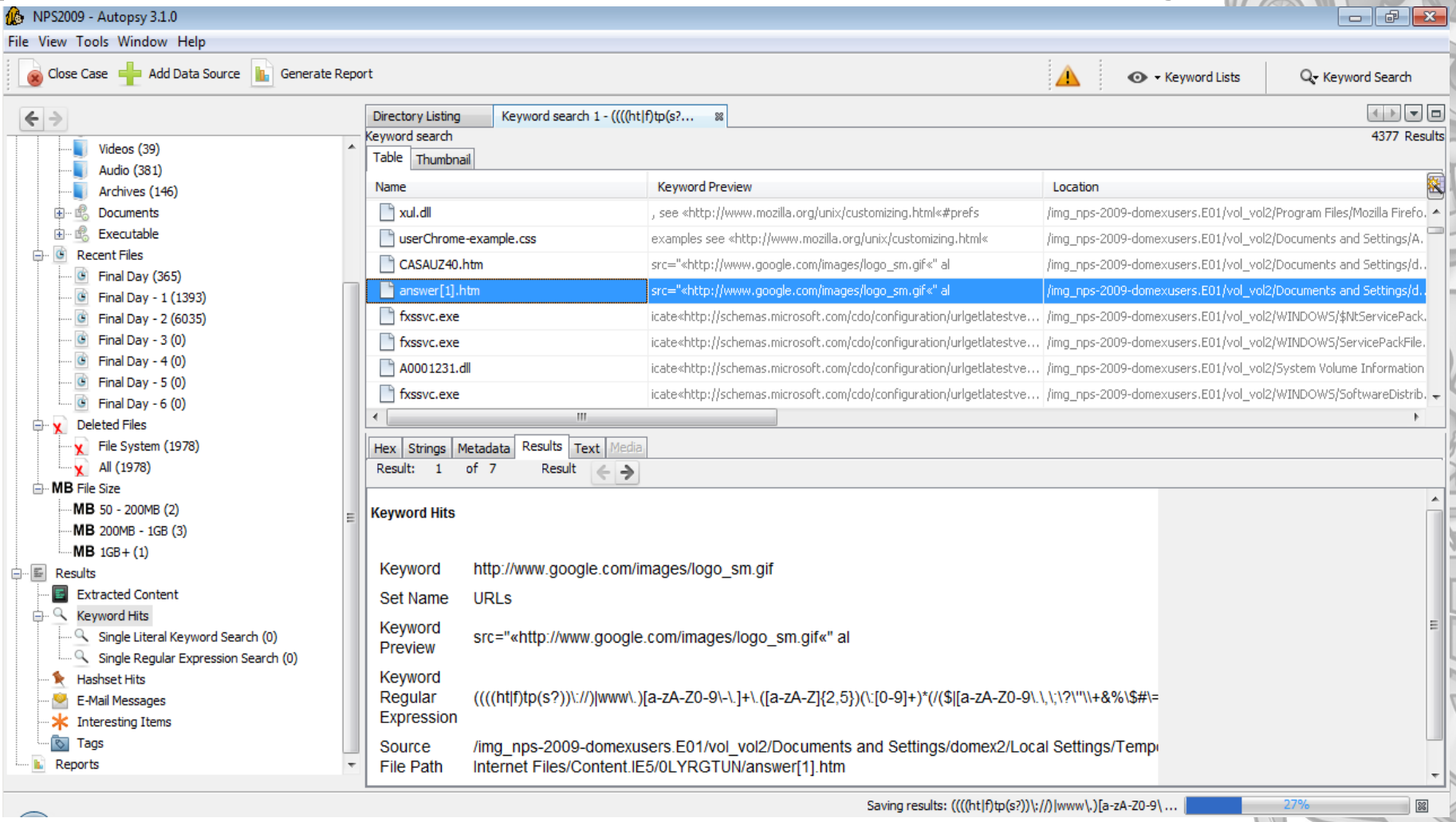
Autopsy 3 utiliza el poderoso motor para indexación de texto Apache SOLR.



* http://lucene.apache.org/solr/
* http://www.sleuthkit.org/autopsy/keyword.php

BÚSQUEDA DE PALABRAS CLAVE (Cont.)

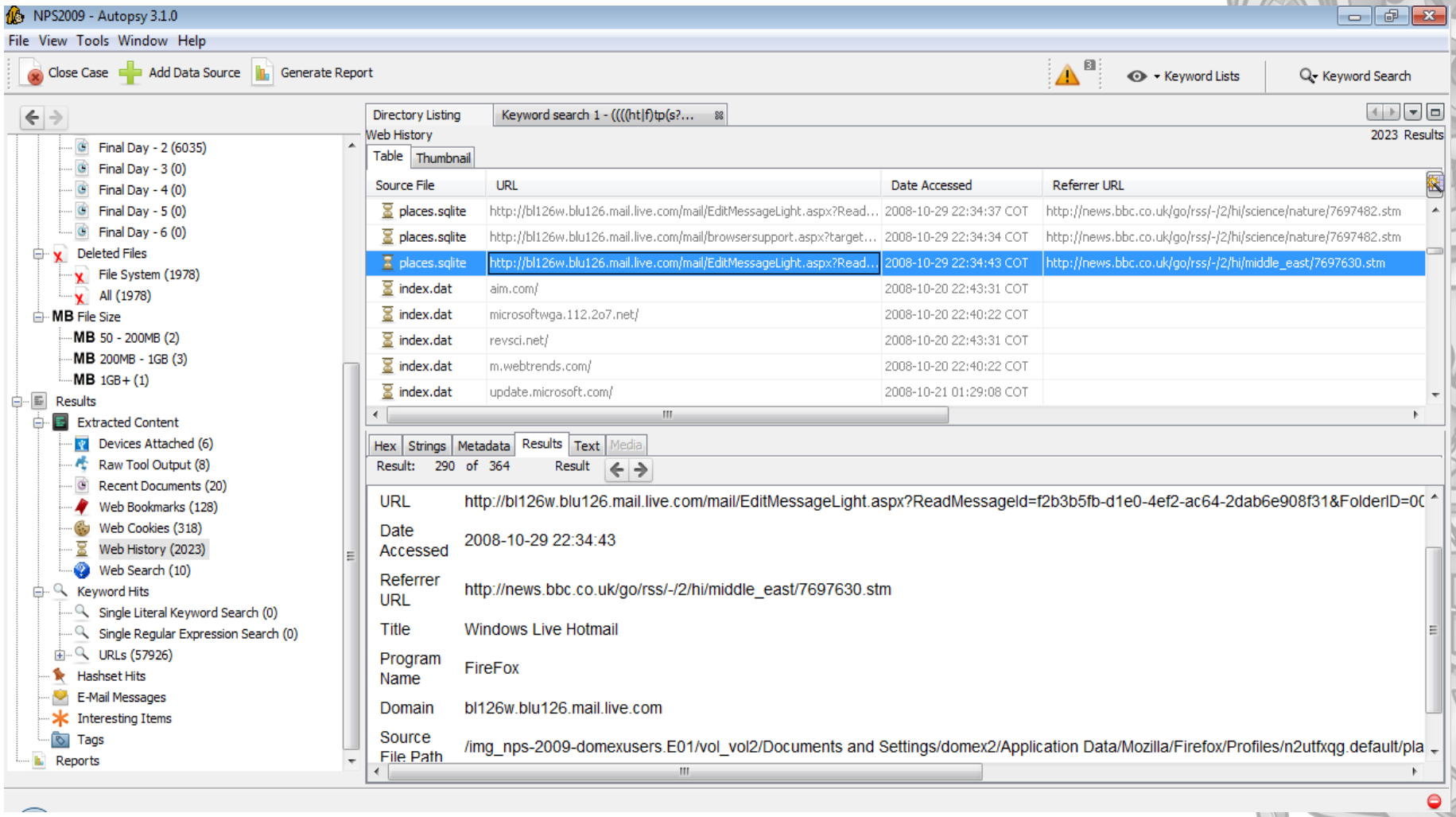
Autopsy 3 utiliza Apache Tika y otras librerías para extraer texto de HTML, M$, PDF, y más.



* http://tika.apache.org/
* http://www.sleuthkit.org/autopsy/keyword.php

ARTEFACTOS WEB

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



* 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.

NPS2009 - Autopsy 3.1.0

File View Tools Window Help

Close Case | Add Data Source | Generate Report | Keyword Lists | Keyword Search

- Final Day - 2 (6035)
- Final Day - 3 (0)
- Final Day - 4 (0)
- Final Day - 5 (0)
- Final Day - 6 (0)
- Deleted Files
  - File System (1978)
  - All (1978)
- MB File Size
  - MB 50 - 200MB (2)
  - MB 200MB - 1GB (3)
  - MB 1GB+ (1)
- Results
  - Extracted Content
    - Devices Attached (6)
    - Raw Tool Output (8)
    - Recent Documents (20)
    - Web Bookmarks (128)
    - Web Cookies (318)
    - Web History (2023)
    - Web Search (10)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - URLs (57926)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Tags
- Reports

Directory Listing | Keyword search 1 - ((((ht|f)tp(s?... | 318 Results

Web Cookies

Table | Thumbnail

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=F2B96C89B05F2560B1E85829FFFFFFFF&E=798&W=2
cookies.sqlite	account.live.com	2008-10-29 22:33:59 COT	NAP	V=1.6&E=735&C=4NT-ivRUS8QB8pTjBCpMg4O85SIRteA1zqr
cookies.sqlite	.advertising.com	2008-10-29 22:34:08 COT	C2	wsSCJlJFIIy+FAH
administrator@liv	live.com/	2008-10-20 17:40:49 COT	wlidperf	throughput=15&latency=203
administrator@ai	aim.com/	2008-10-20 17:43:31 COT	rsi_ct	2008_10_20:1
administrator@ac	aol.com/	2008-10-20 17:43:04 COT	rsi_ct	2008_10_20:1
administrator@at	at.atwola.com/	2008-10-20 17:43:12 COT	JEB2	48FCFF8B6E65181CCD9B41ECF0000622

Hex | Strings | Metadata | Results | Text | Media

Matches on page: - of - Match | Page: 1 of 1 Page | Extracted Text

```
wlidperf
throughput=15&latency=203
live.com/
1088
2189574144
32107986
3865074448
29963012
*



-----------------------------METADATA-----------------------------

Content-Encoding: ISO-8859-1
```

* http://www.sleuthkit.org/autopsy/web_artifacts.php

ANÁLISIS DEL REGISTRO

Se utiliza RegRipper para identificar dispositivos USB y documentos accedidos.

NPS2009 - Autopsy 3.1.0

File View Tools Window Help

Close Case | Add Data Source | Generate Report | Keyword Lists | Keyword Search

- Final Day - 2 (6035)
- Final Day - 3 (0)
- Final Day - 4 (0)
- Final Day - 5 (0)
- Final Day - 6 (0)
- Deleted Files
  - File System (1978)
  - All (1978)
- MB File Size
  - MB 50 - 200MB (2)
  - MB 200MB - 1GB (3)
  - MB 1GB+ (1)
- Results
  - Extracted Content
    - Devices Attached (6)
    - Raw Tool Output (8)
    - Recent Documents (20)
    - Web Bookmarks (128)
    - Web Cookies (318)
    - Web History (2023)
    - Web Search (10)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - URLs (57926)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Tags
- Reports

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

Devices Attached — 6 Results

Table | Thumbnail

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&2f7921708&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

Hex | Strings | Metadata | Results | Text | Media

Result: 27 of 30 Result

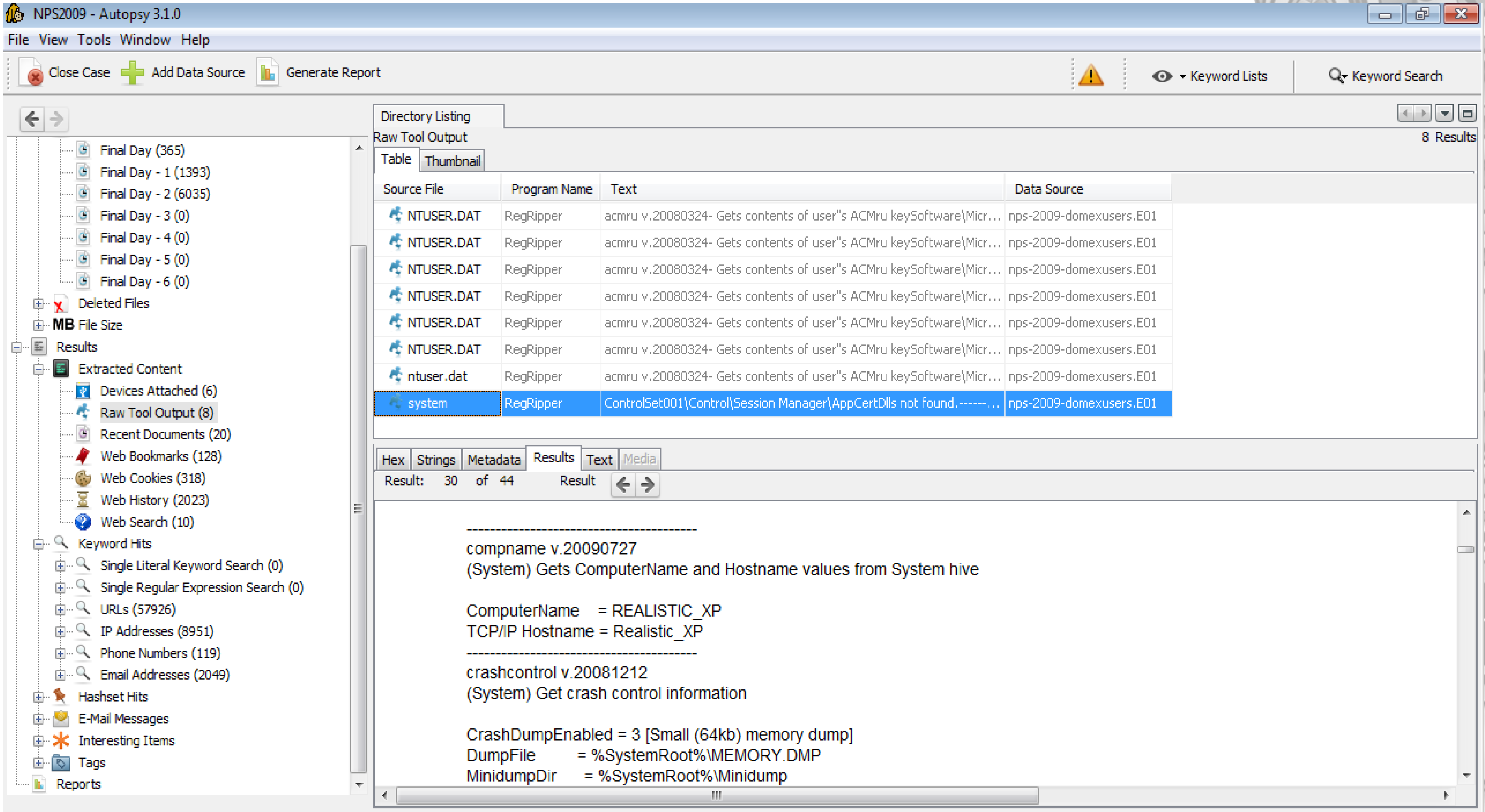
Devices Attached

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.



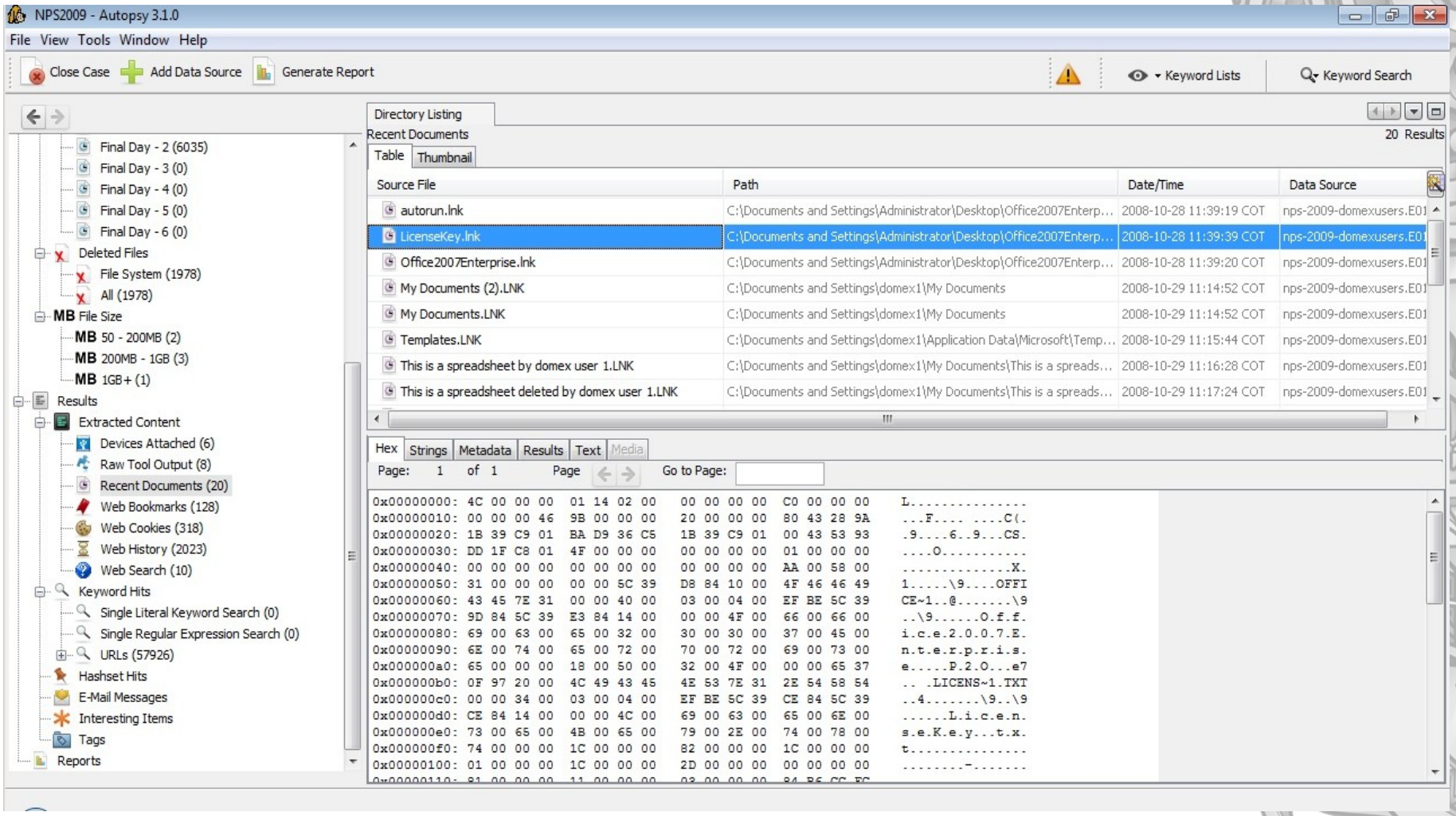
Source File	Program Name	Text	Data Source
NTUSER.DAT	RegRipper	acmru v.20080324- Gets contents of user''s ACMru keySoftware\Micr…	nps-2009-domexusers.E01
NTUSER.DAT	RegRipper	acmru v.20080324- Gets contents of user''s ACMru keySoftware\Micr…	nps-2009-domexusers.E01
NTUSER.DAT	RegRipper	acmru v.20080324- 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

```
----------------------------------------
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

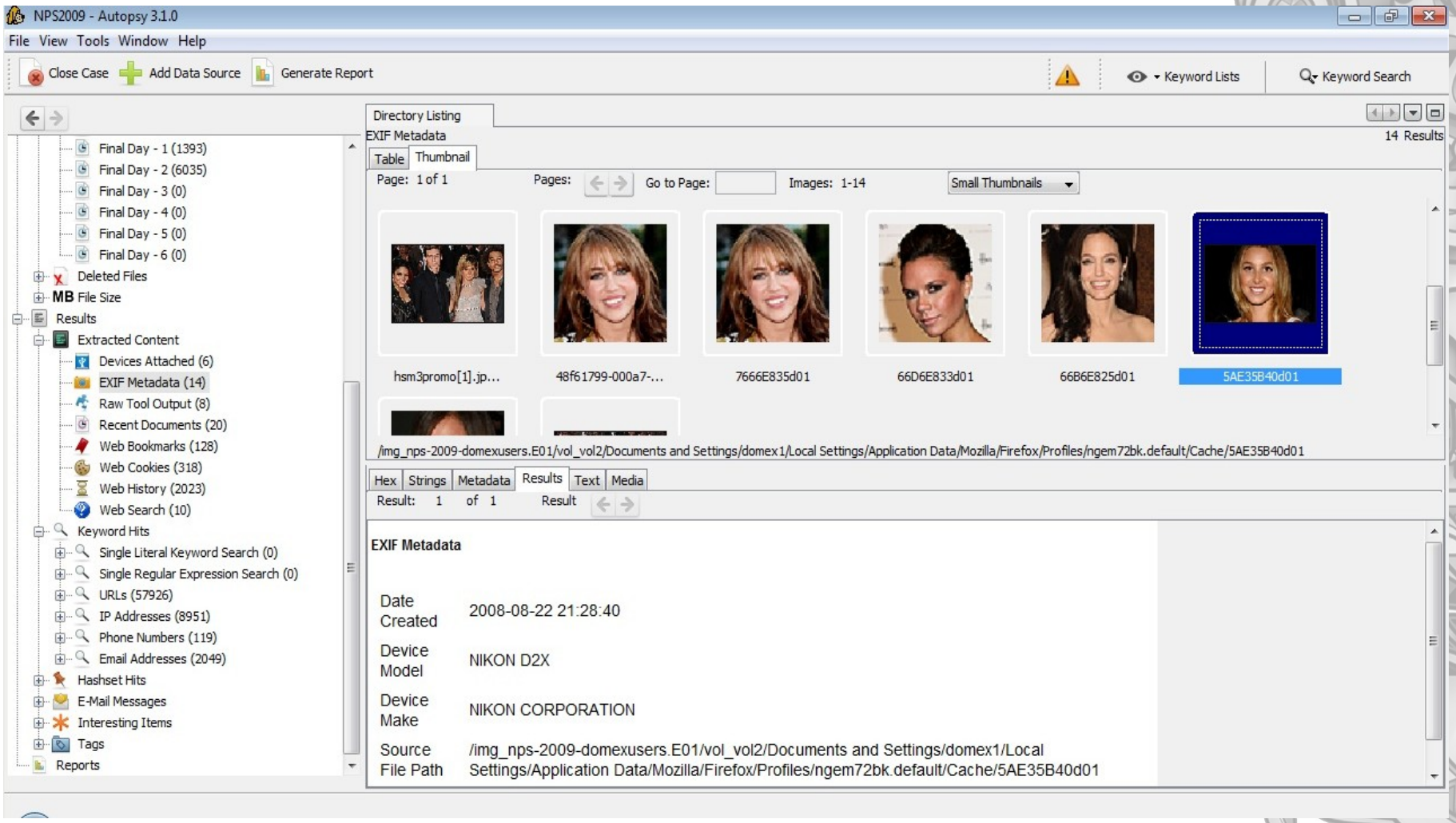
Identifica atajos (accesos directos) y documentos accedidos.



* http://www.sleuthkit.org/autopsy/features.php

EXIF

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



* http://en.wikipedia.org/wiki/Exchangeable_image_file_format
* http://www.sleuthkit.org/autopsy/features.php

Ordenar por Tipo de Archivo

Agrupar los archivos por su tipo para encontrar todas las imágenes o documentos.

NPS2009 - Autopsy 3.1.0

File View Tools Window Help

Close Case | Add Data Source | Generate Report | Keyword Lists | Keyword Search

- File Types
  - Images (2389)
  - Videos (39)
  - Audio (381)
  - Archives (146)
  - Documents
    - HTML (953)
    - Office (40)
    - PDF (2)
    - Plain Text (214)
    - Rich Text (0)
  - Executable
- Recent Files
  - Final Day (365)
  - Final Day - 1 (1393)
  - Final Day - 2 (6035)
  - Final Day - 3 (0)
  - Final Day - 4 (0)
  - Final Day - 5 (0)
  - Final Day - 6 (0)
- Deleted Files
- MB File Size
- Results
  - Extracted Content
    - Devices Attached (6)
    - EXIF Metadata (14)
    - Raw Tool Output (8)
    - Recent Documents (20)
    - Web Bookmarks (128)
    - Web Cookies (318)

Directory Listing

Office — 40 Results

Table | Thumbnail

Name	Location	Modified Time	Change Time	Access Ti
excel.xls	/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
excel4.xls	/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
powerpnt.ppt	/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
winword.doc	/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
winword2.doc	/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
excel.xls	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/D...	2004-08-04 07:00:00 COT	2008-10-20 16:35:04 COT	2008-10-2
excel4.xls	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/D...	2004-08-04 07:00:00 COT	2008-10-20 16:35:04 COT	2008-10-2
powerpnt.ppt	/img_nps-2009-domexusers.E01/vol_vol2/Documents and Settings/D...	2004-08-04 07:00:00 COT	2008-10-20 16:35:04 COT	2008-10-2
winword.doc	/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

Hex | Strings | Metadata | Results | Text | Media

Page: 1 of 1 Page Go to Page:

```
0x000003d0: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF  ................
0x000003e0: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF  ................
0x000003f0: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF  ................
0x00000400: 52 00 6F 00  6F 00 74 00  20 00 45 00  6E 00 74 00  R.o.o.t. .E.n.t.
0x00000410: 72 00 79 00  00 00 FF FF  FF FF FF FF  FF FF FF FF  r.y.............
0x00000420: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF  ................
0x00000430: FF FF FF FF  FF FF FF FF  FF FF FF FF  FF FF FF FF  ................
0x00000440: 16 00 05 00  FF FF FF FF  FF FF FF FF  01 00 00 00  ................
0x00000450: 00 09 02 00  00 00 00 00  C0 00 00 00  00 00 00 46  ...............F
0x00000460: 00 00 00 00  FF FF FF FF  FF FF FF FF  00 B9 EA 31  ................1
0x00000470: 40 D9 B9 01  03 00 00 00  C0 09 00 00  FF FF FF FF  @...............
0x00000480: 57 00 6F 00  72 00 64 00  44 00 6F 00  63 00 75 00  W.o.r.d.D.o.c.u.
0x00000490: 6D 00 65 00  6E 00 74 00  00 00 FF FF  01 00 00 00  m.e.n.t.........
0x000004a0: A4 08 9F 82  00 00 00 00  FD FF FF FF  00 00 00 00  ................
0x000004b0: 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  ................
0x000004c0: 1A 00 02 01  02 00 00 00  FF FF FF FF  FF FF FF FF  ................
```

* http://www.sleuthkit.org/autopsy/features.php

DETECTAR INCONGRUENCIA EN EXTENSIÓN

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

NPS2009 - Autopsy 3.1.0

File View Tools Window Help

Close Case | Add Data Source | Generate Report | Keyword Lists | Keyword Search

- .cmd (8)
- .com (34)
- Recent Files
  - Final Day (365)
  - Final Day - 1 (1393)
  - Final Day - 2 (6035)
  - Final Day - 3 (0)
  - Final Day - 4 (0)
  - Final Day - 5 (0)
  - Final Day - 6 (0)
- Deleted Files
- MB File Size
- Results
  - Extracted Content
    - Devices Attached (6)
    - EXIF Metadata (14)
    - Extension Mismatch Detected (183)
    - Raw Tool Output (8)
    - Recent Documents (20)
    - Web Bookmarks (128)
    - Web Cookies (318)
    - Web History (2023)
    - Web Search (10)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - URLs (57926)
    - IP Addresses (8951)
    - Phone Numbers (119)
    - Email Addresses (2049)

Directory Listing

Extension Mismatch Detected — 183 Results

Table | Thumbnail

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

Hex | Strings | Metadata | Results | Text | Media

Page: 1 of 24 Page Go to Page:

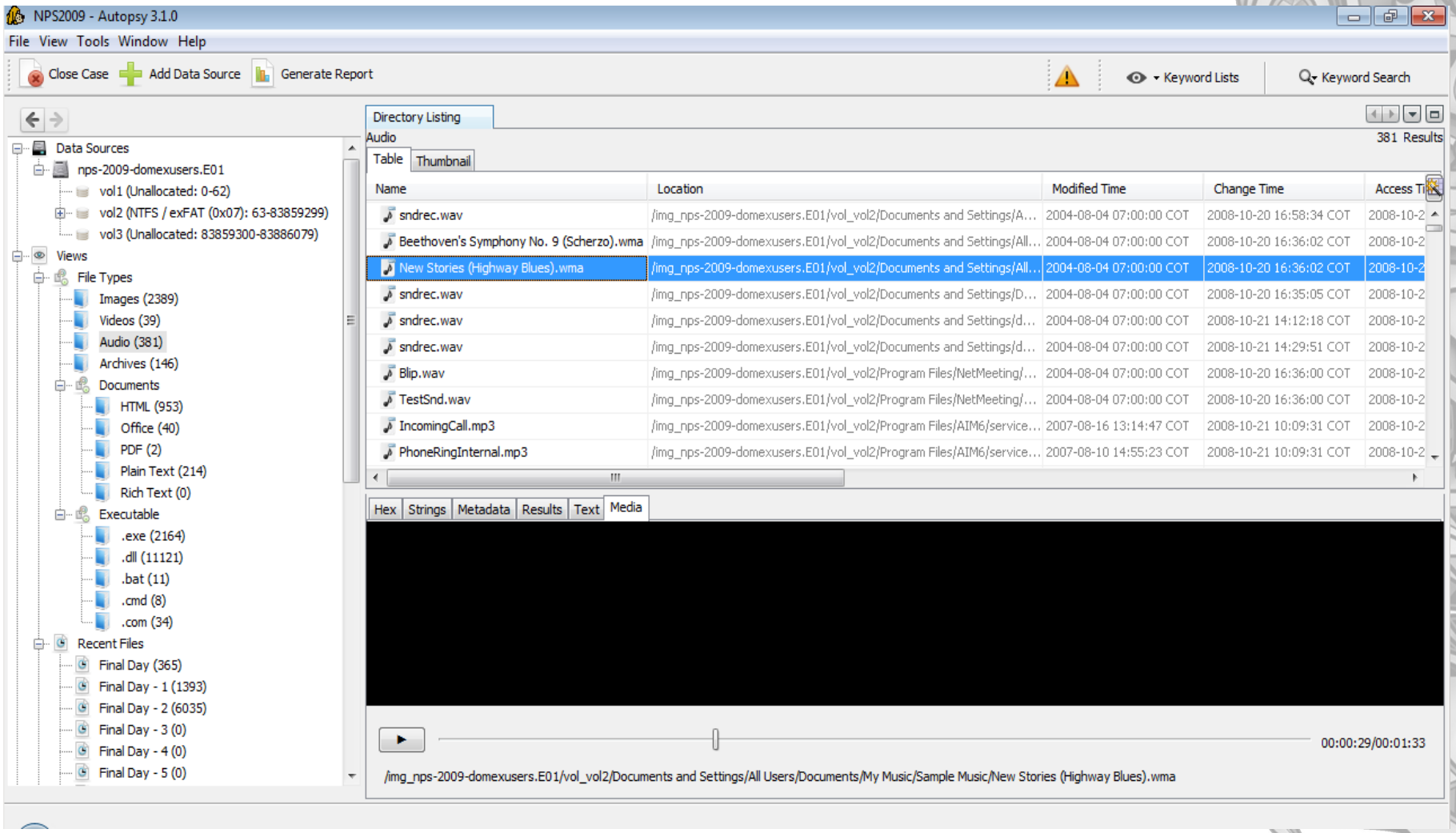
```
0x00000000: 30 26 B2 75  8E 66 CF 11  A6 D9 00 AA  00 62 CE 6C   0&.u.f.......b.l
0x00000010: 89 06 00 00  00 00 00 00  08 00 00 00  01 02 33 26   ..............3&
0x00000020: B2 75 8E 66  CF 11 A6 D9  00 AA 00 62  CE 6C 2C 00   .u.f.......b.l,.
0x00000030: 00 00 00 00  00 00 02 00  02 00 02 00  02 00 02 00   ................
0x00000040: 00 00 00 00  00 00 00 00  00 00 CE 75  F8 7B 8D 46   ...........u.{.F
0x00000050: D1 11 8D 82  00 60 97 C9  A2 B2 26 00  00 00 00 00   .....`....&.....
0x00000060: 00 00 02 00  01 00 B7 28  00 00 02 00  B6 78 01 00   .......(.....x..
0x00000070: A1 DC AB 8C  47 A9 CF 11  8E E4 00 C0  0C 20 53 65   ....G........ Se
0x00000080: 68 00 00 00  00 00 00 00  D7 D2 64 6D  96 74 1F 45   h.........dm.t.E
0x00000090: 84 E2 29 F8  1D B8 54 7C  F1 D1 05 00  00 00 00 00   ..)...T|........
0x000000a0: 20 F4 D8 C7  25 B3 C0 01  1C 01 00 00  00 00 00 00    ...%...........
0x000000b0: 50 04 87 15  00 00 00 00  E0 50 AC 13  00 00 00 00   P........P......
0x000000c0: 1C 0C 00 00  00 00 00 00  02 00 00 00  38 05 00 00   ............8...
0x000000d0: 38 05 00 00  6D A1 01 00  B5 03 BF 5F  2E A9 CF 11   8...m......_....
```

* http://www.garykessler.net/library/file_sigs.html

* http://www.sleuthkit.org/autopsy/

REPRODUCTOR DE MEDIOS

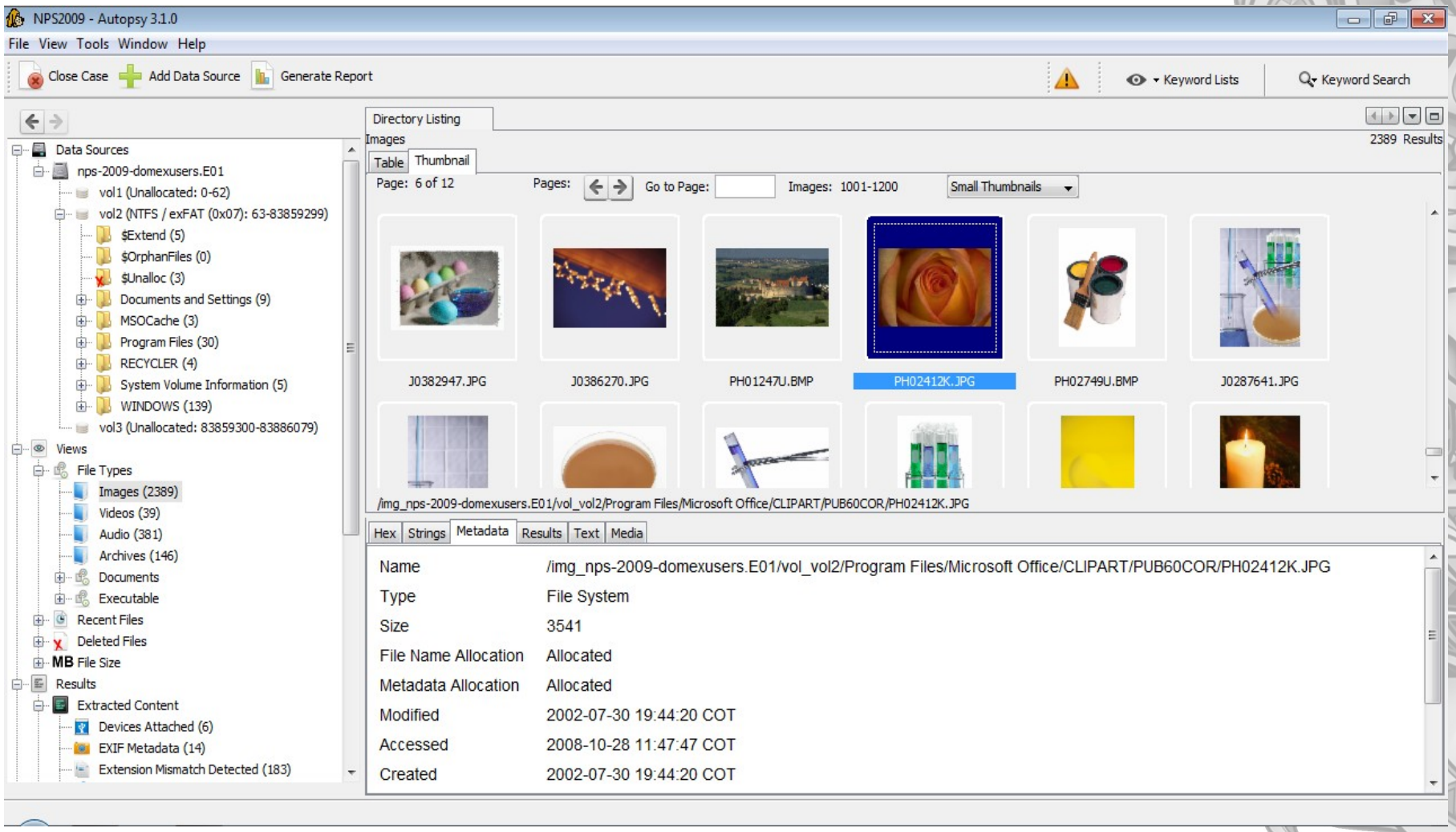
Visualizar videos e imágenes dentro de la aplicación, sin requerir un visor externo.



* http://www.sleuthkit.org/autopsy/features.php

VISOR DE MINIATURAS

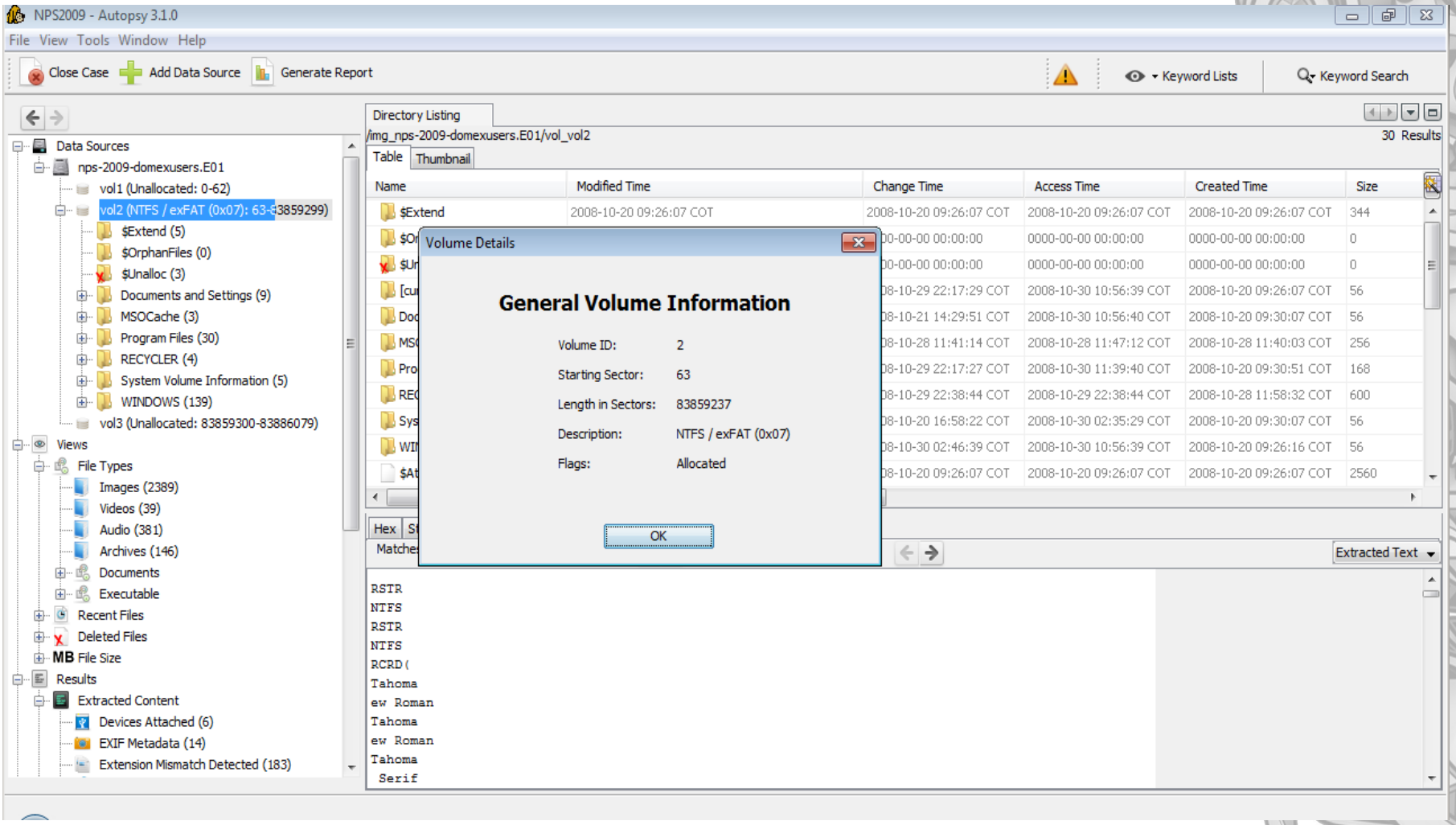
Muestra las miniaturas de las imágenes para ayudar a visualizar rápidamente fotografías.



* http://www.sleuthkit.org/autopsy/features.php

ANÁLISIS PARA SISTEMAS DE ARCHIVOS

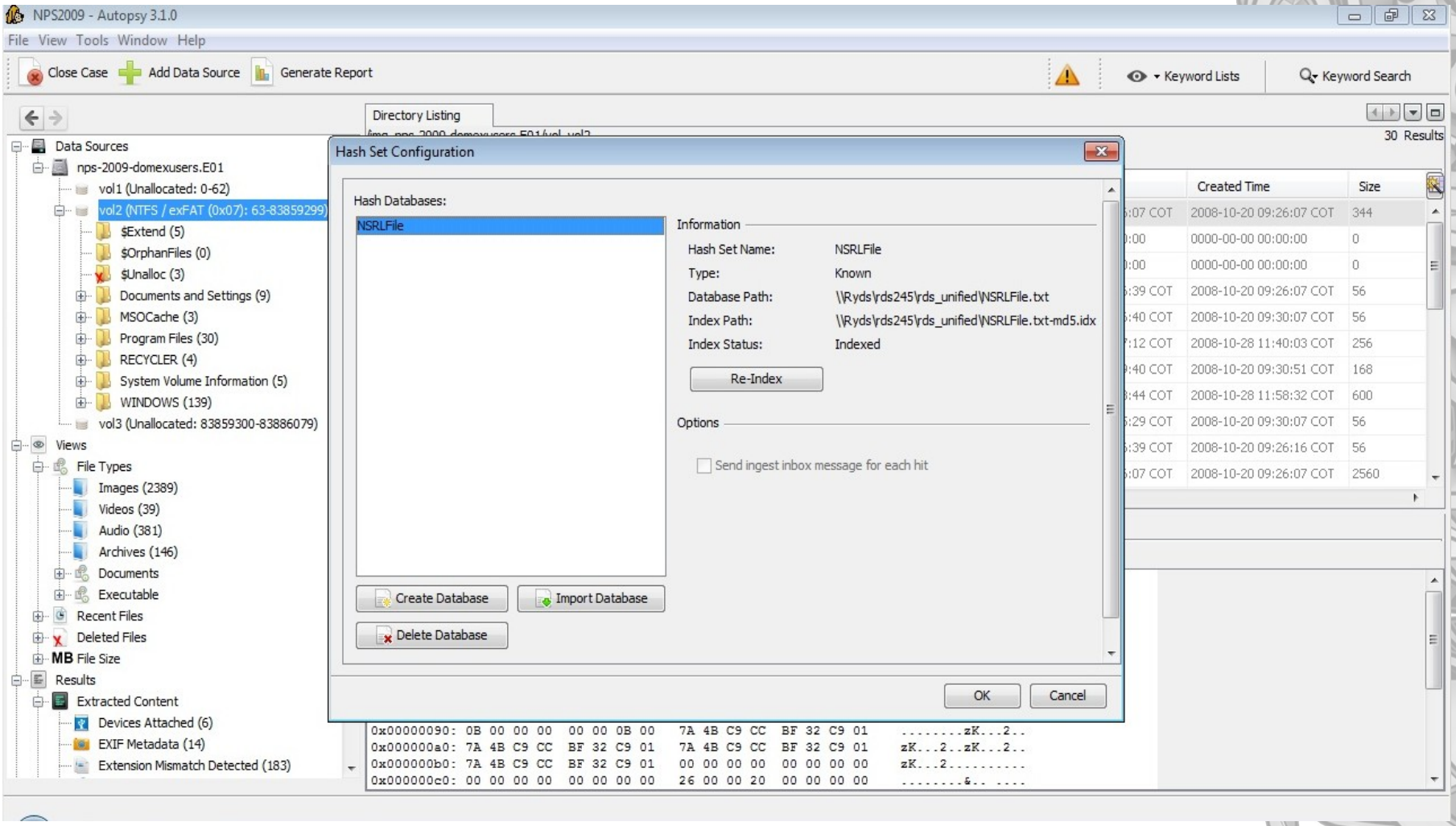
Soporta los Sistemas de Archivos más comunes, NTFS, FAT12/16/32, Ext2/3, y otros.



* http://www.sleuthkit.org/autopsy/features.php

FILTRAR POR CONJUNTO DE HASHS

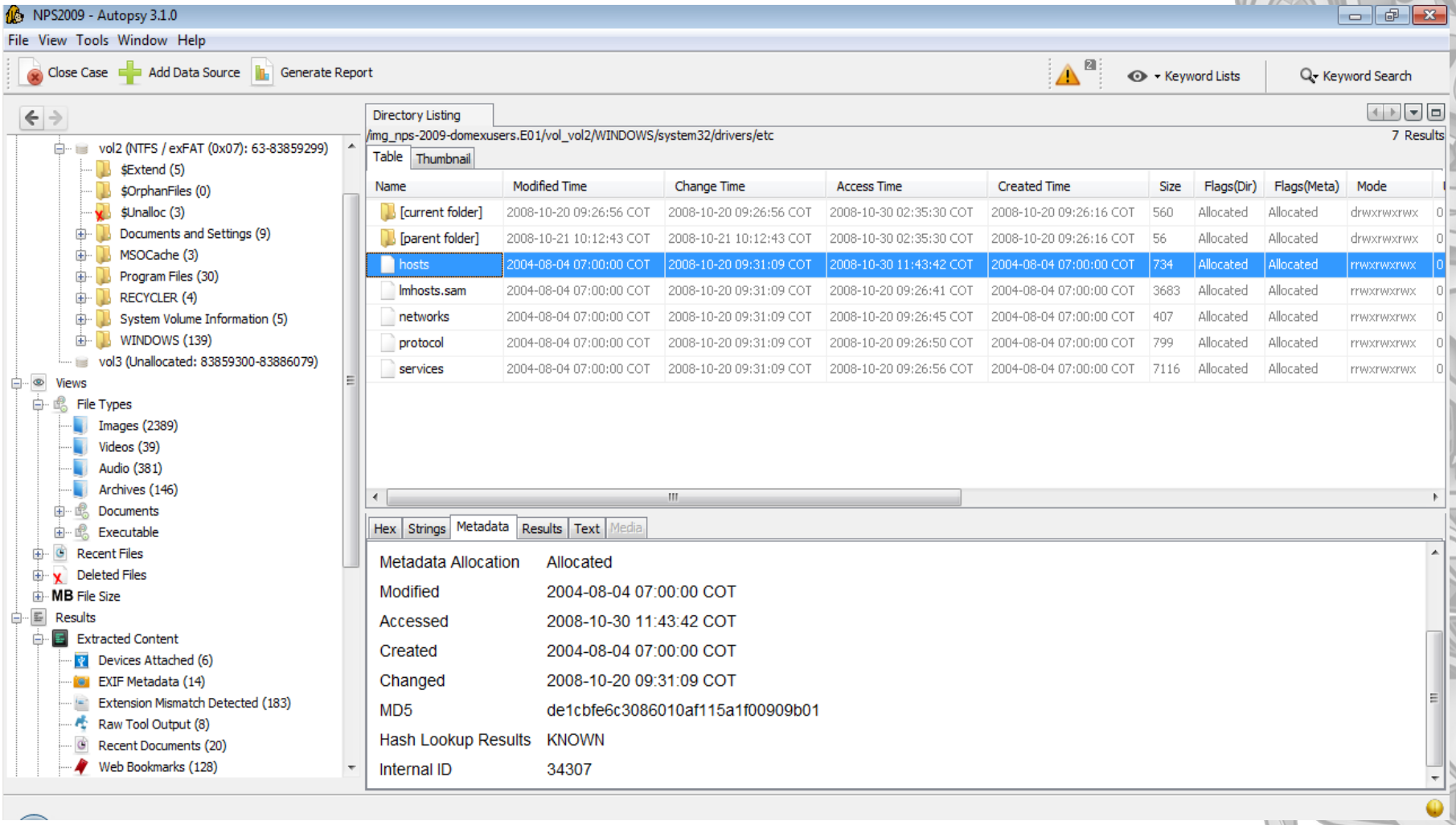
Filtra archivos conocidos buenos utilizando NSRL (National Software Reference Library).



* http://www.nsrl.nist.gov
* http://www.sleuthkit.org/autopsy/features.php

FILTRAR POR CONJUNTO DE HASHS (Cont.)

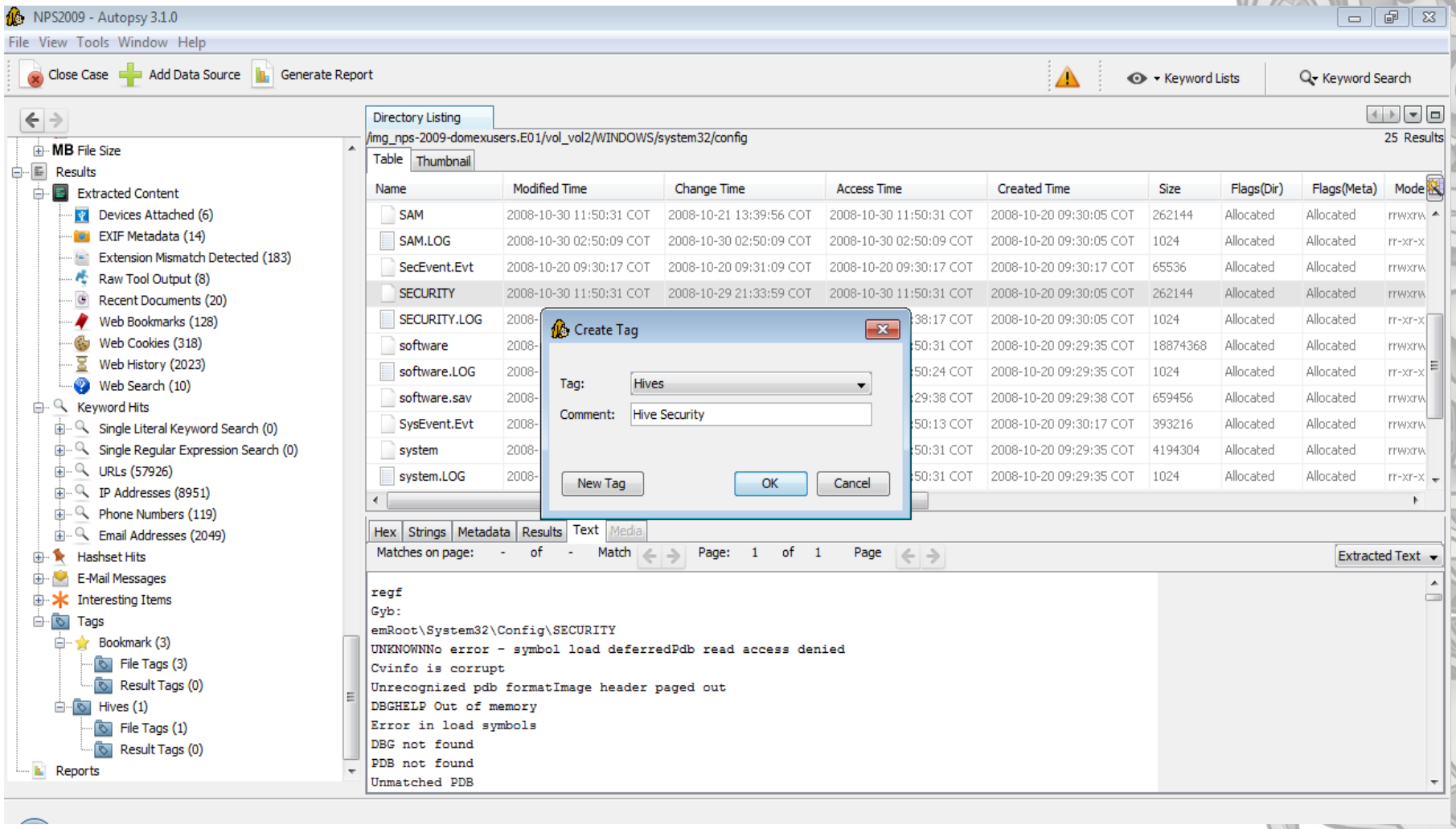
Etiqueta archivos conocidos malos utilizando BDs de hashs HashKeeper, md5sum, EnCase.



* http://www.nsrl.nist.gov
* http://www.sleuthkit.org/autopsy/features.php

ETIQUETAS

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



* http://www.sleuthkit.org/autopsy/features.php

ARCHIVOS INTERESANTES

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

NPS2009 - Autopsy 3.1.1

File View Tools Window Help

Close Case | Add Data Source | Generate Report | Keyword Lists | Keyword Search

- Recent Files
- Deleted Files
- MB File Size
- Results
  - Extracted Content
    - Devices Attached (6)
    - EXIF Metadata (14)
    - Extension Mismatch Detected (183)
    - Raw Tool Output (8)
    - Recent Documents (20)
    - Web Bookmarks (128)
    - Web Cookies (318)
    - Web History (2023)
    - Web Search (10)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - URLs (57926)
    - IP Addresses (8951)
    - Phone Numbers (119)
    - Email Addresses (2049)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
    - BDs (24)
    - Fotos (756)
  - Tags
    - Bookmark (3)
    - Hives (2)
- Reports

Directory Listing

BDs — 24 Results

Table | Thumbnail

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 22:28:2
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 22:25:4
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 22:41:0
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 22:26:1
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 22:26:0
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 22:34:4
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 22:34:4
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 22:34:4
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 22:34:4
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 22:34:4
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 22:34:4
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 22:34:4

Hex | Strings | Metadata | Results | Text | Media

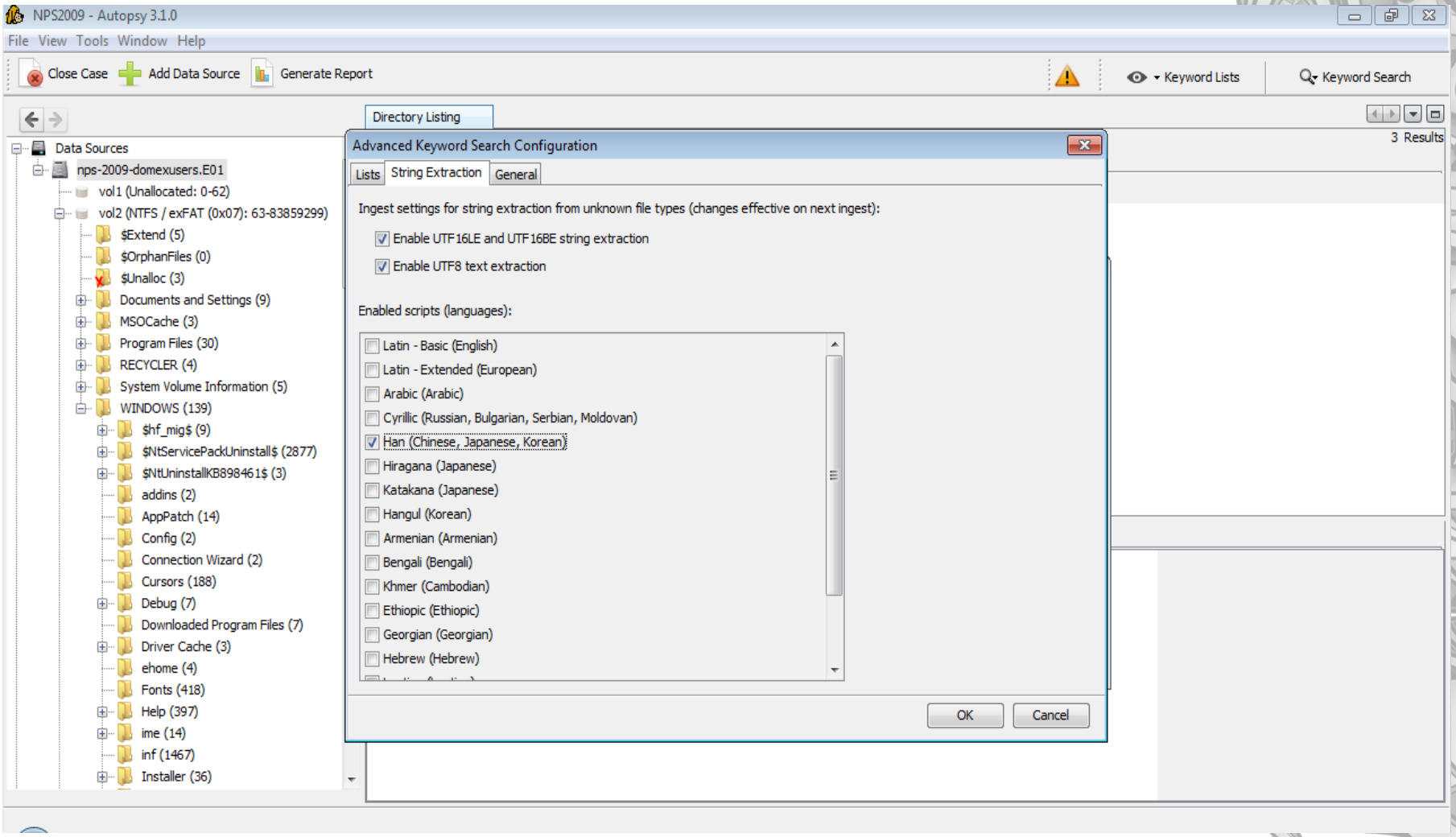
Page: 1 of 1 Page Go to Page: Script: Latin - Basic

```
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)
```

* http://www.sleuthkit.org/autopsy/features.php

EXTRACCIÓN DE CADENAS UNICODE

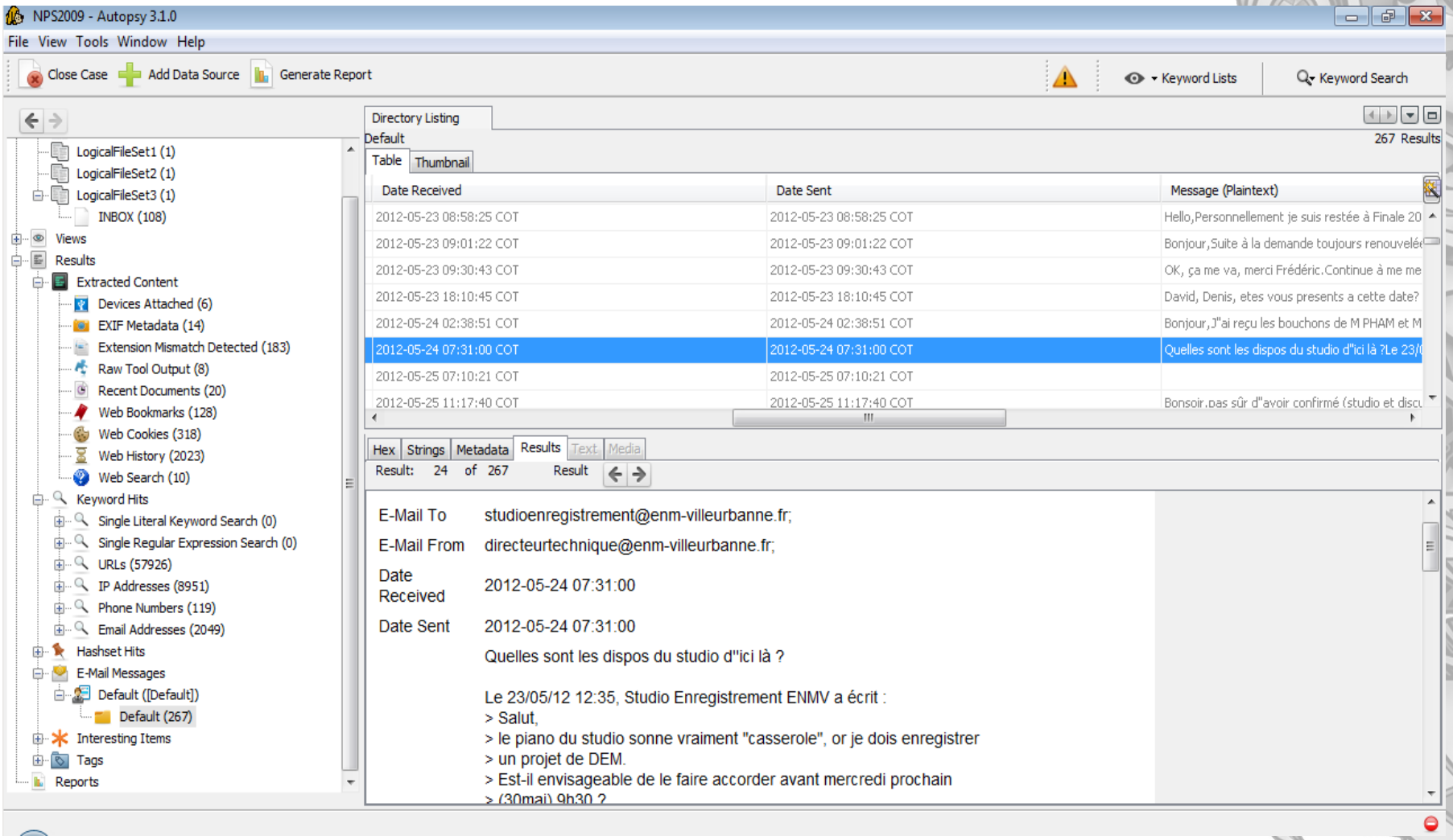
Extrae cadenas desde el espacio sin asignar y tipos de archivo desconocidos.



URL

ANÁLISIS DE CORREO ELECTRÓNICO

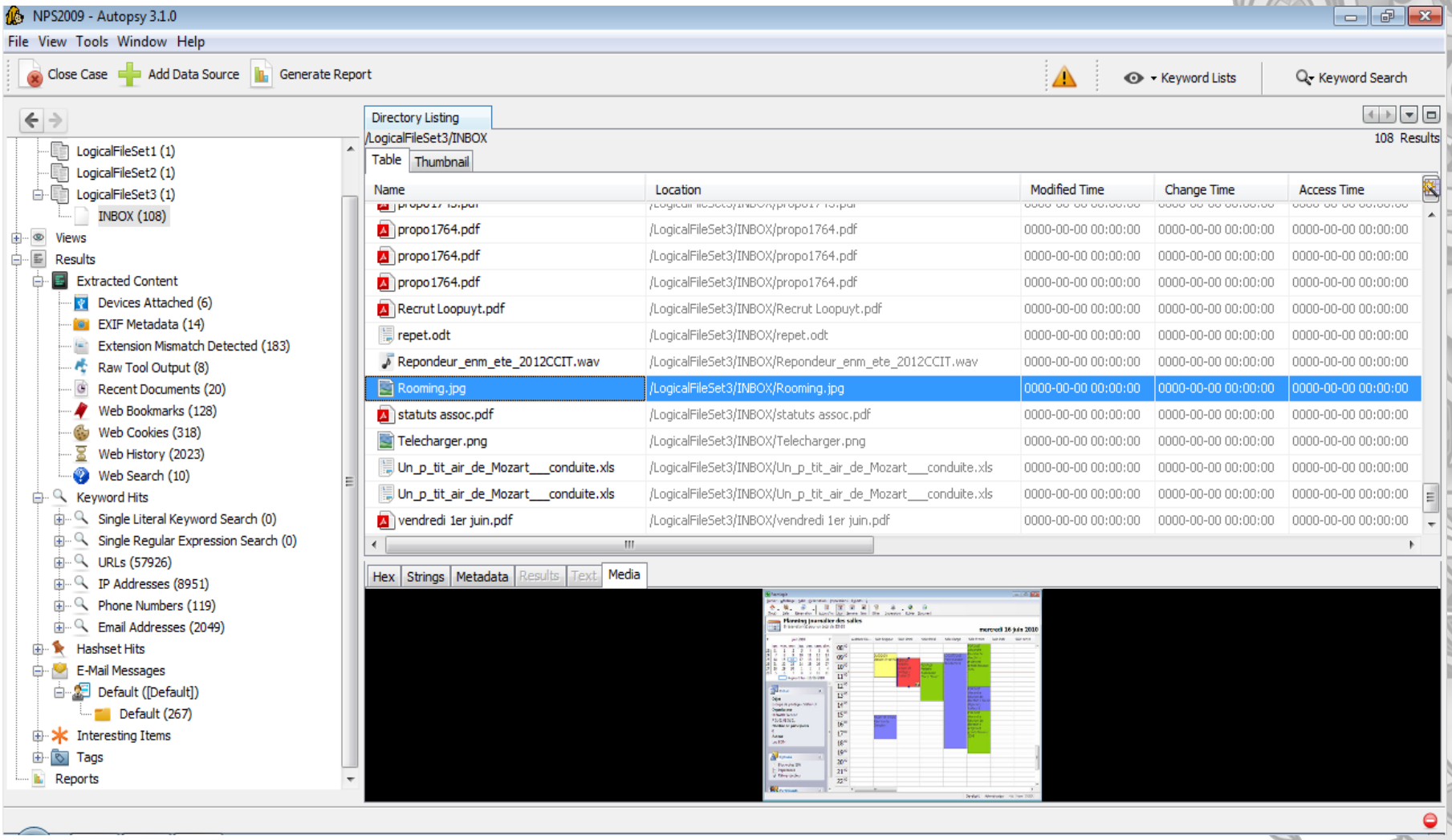
Interpreta mensajes en formato MBOX, como los del cliente Thunderbird.



* http://en.wikipedia.org/wiki/Mbox
* http://www.sleuthkit.org/autopsy/features.php

ANÁLISIS DE CORREO ELECTRÓNICO (Cont.)

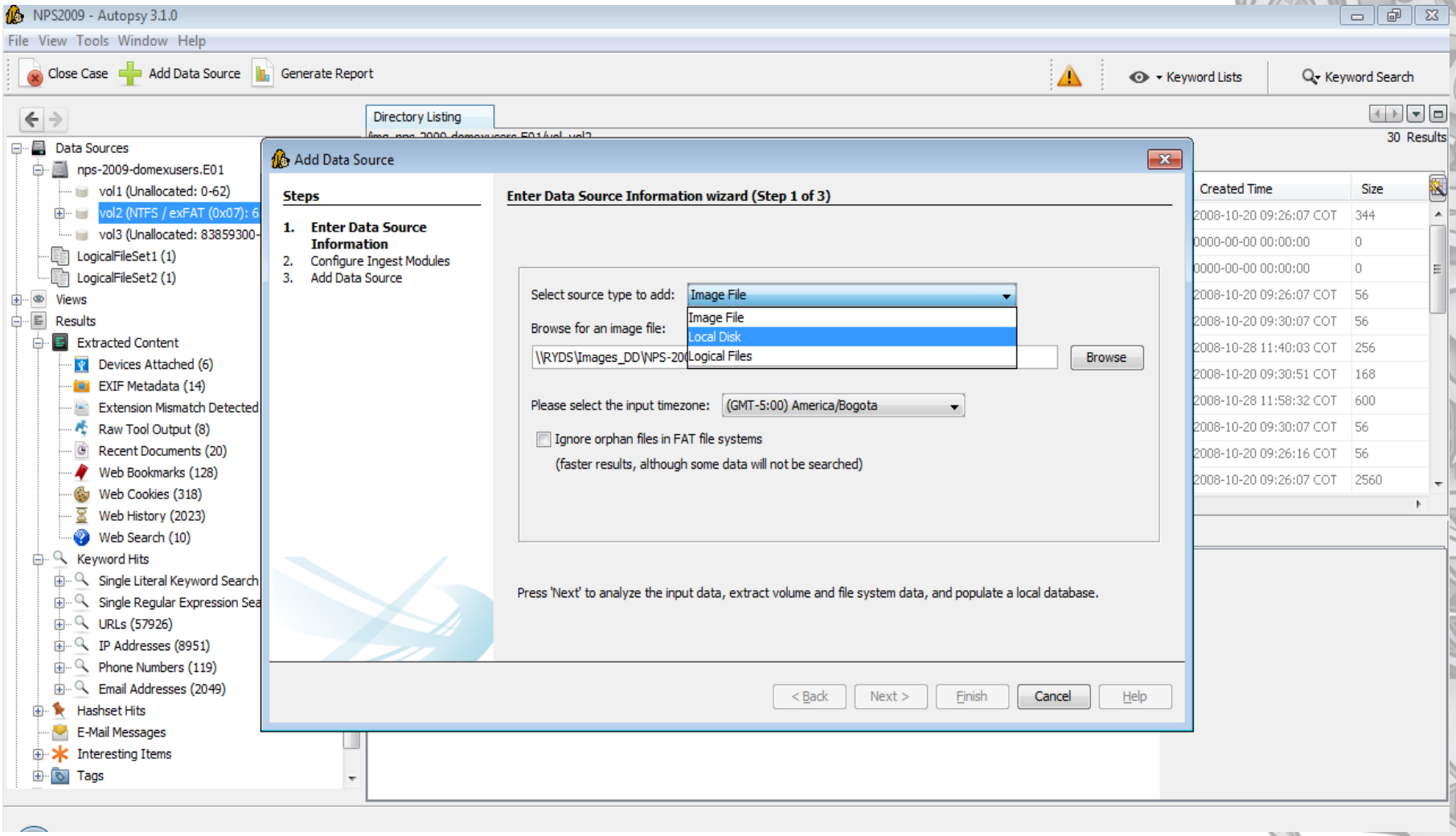
Mbox es un formato de archivo utilizado para manejar colecciones de mensajes de correo.



* http://en.wikipedia.org/wiki/Mbox
* http://www.sleuthkit.org/autopsy/features.php

FORMATOS DE ENTRADA

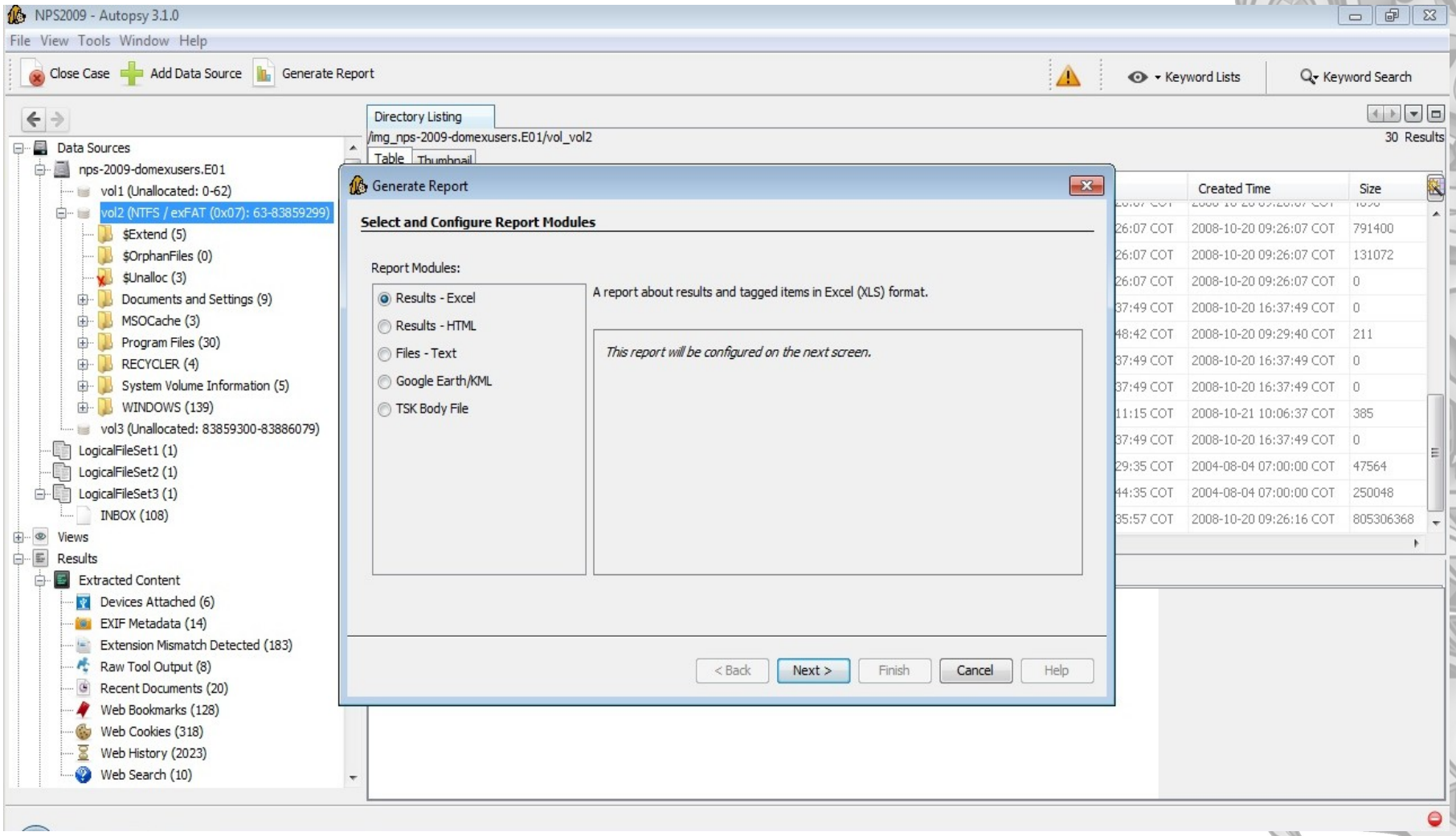
Imagen de disco, unidad locales, archivos locales. Entradas en formato raw/dd o E01.



* http://sourceforge.net/projects/libewf/
* http://www.sleuthkit.org/autopsy/features.php

REPORTAR

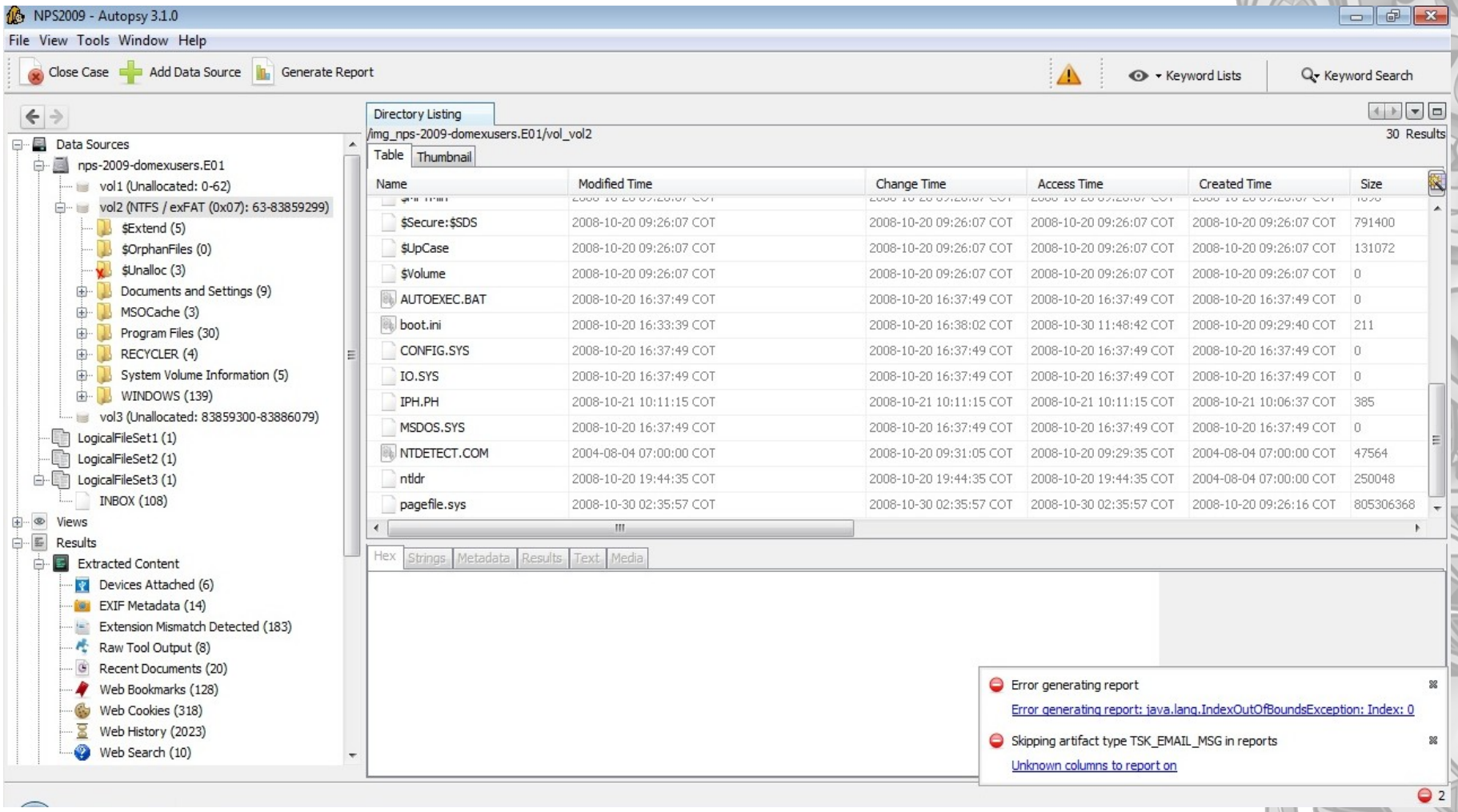
Infraestructura ampliable de reportes. Los tipos principales son HTML, XLS y Archivo “Body”.



* www.sleuthkit.org/autopsy/features.php

REPORTAR (Bug)

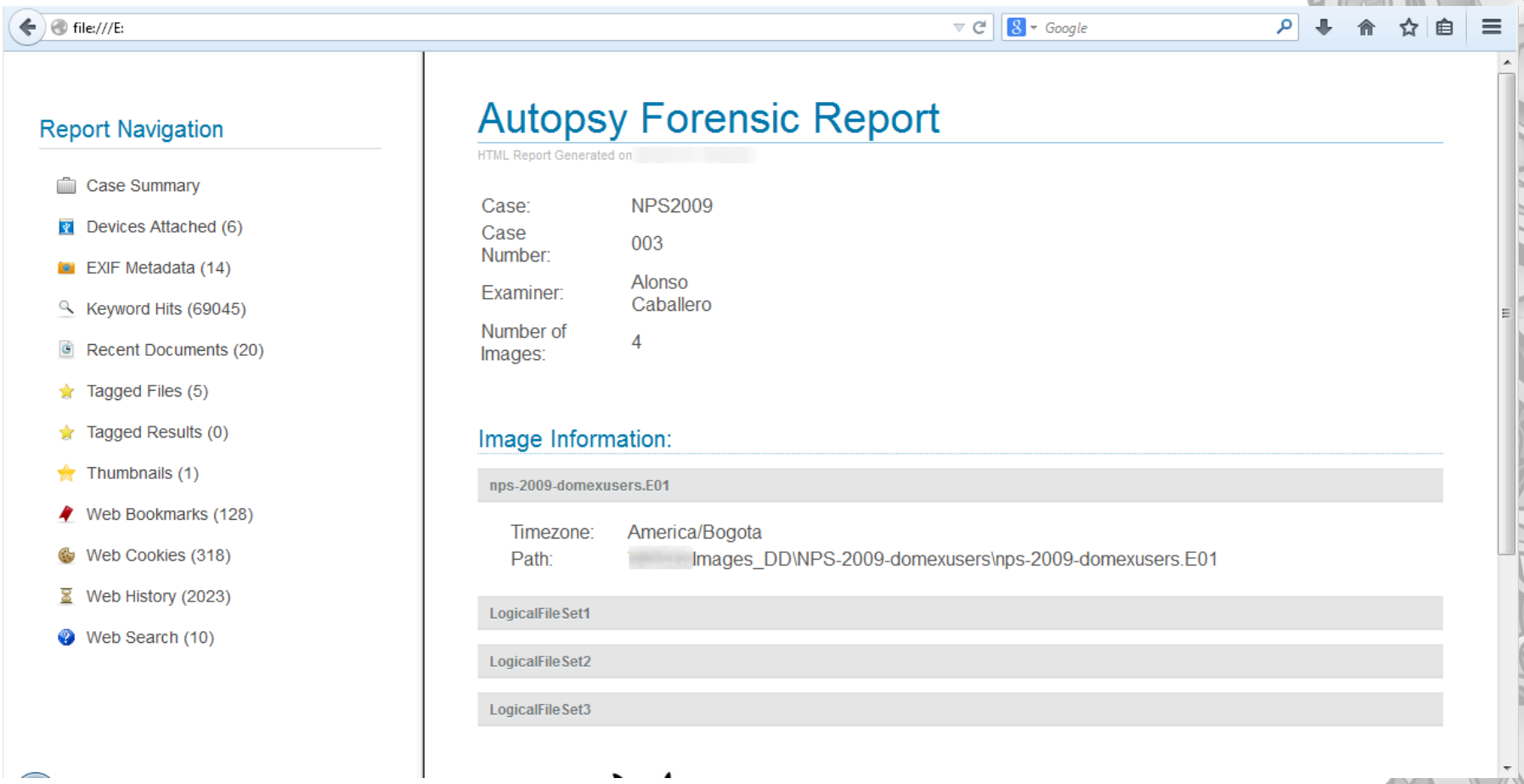
Bug en el código para la generación de reporte en algunos tipos de artefactos. Solución v 3.1.2



* www.sleuthkit.org/autopsy/features.php

REPORTAR (Cont.)

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



* www.sleuthkit.org/autopsy/features.php

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

LinkedIn:

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

* http://www.reydes.com

PERUHACK

¡Muchas Gracias!

Alonso Caballero Quezada
ReYDeS - @Alonso_ReYDeS
www.reydes.com
reydes@gmail.com