

The Sleuth Kit and Open Source Digital Forensics Conference



October 3, 2012

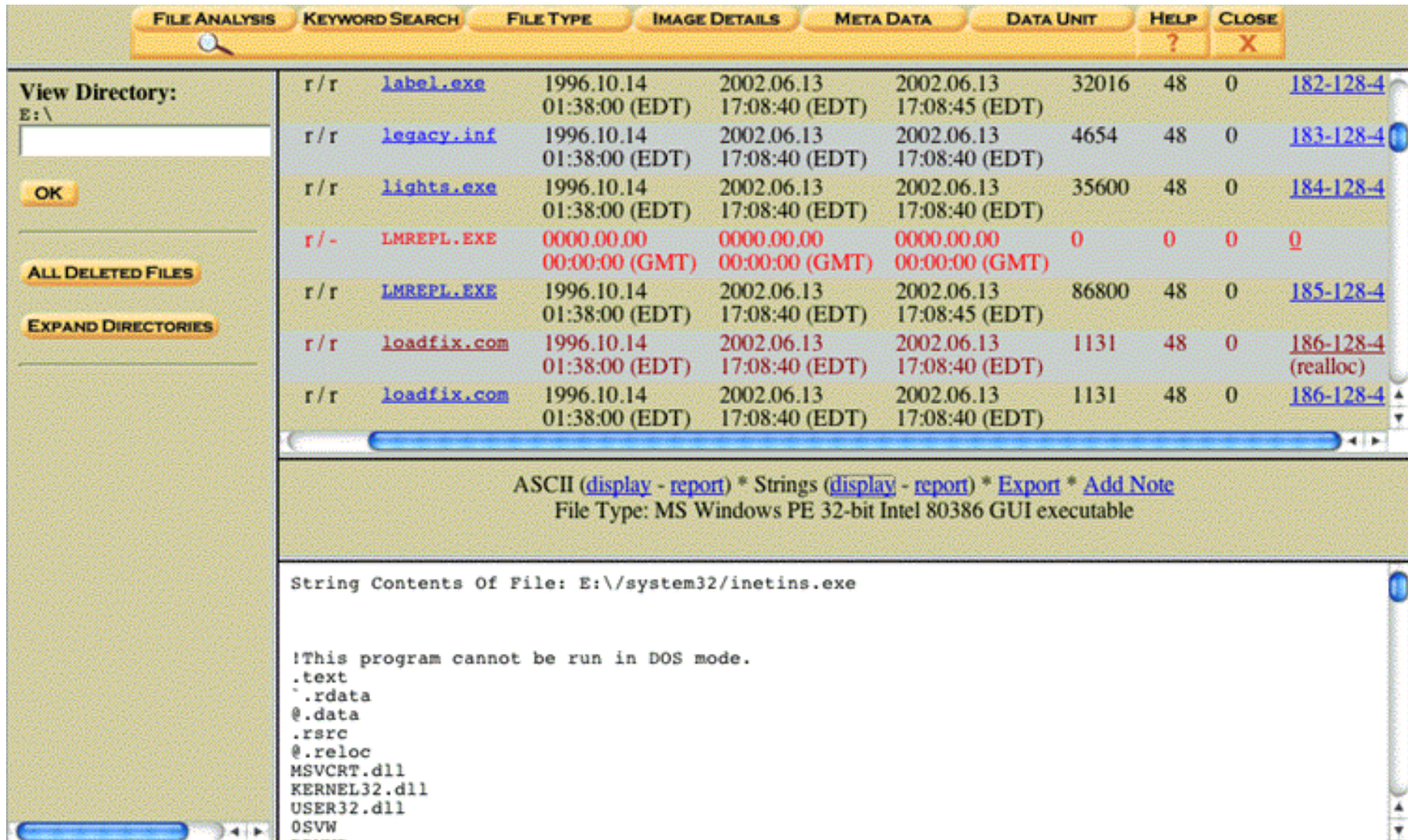
Autopsy 3.0

Brian Carrier

VP of Digital Forensics

Basis Technology

Autopsy 2



The screenshot shows the Autopsy 2 interface. At the top, there are tabs for FILE ANALYSIS, KEYWORD SEARCH, FILE TYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. Below the tabs is a search bar. On the left side, there is a 'View Directory:' section with a text input field containing 'E:\', an 'OK' button, and buttons for 'ALL DELETED FILES' and 'EXPAND DIRECTORIES'. The main area displays a table of files with columns for permissions, filename, creation/modification times, file size, and other attributes. The file 'loadfix.com' is selected, and the bottom pane shows its string contents.

Permissions	Filename	Creation Time	Modification Time	File Size	Other Attributes
r/r	label.exe	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	32016	48 0 182-128-4
r/r	legacy.inf	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	4654	48 0 183-128-4
r/r	lights.exe	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	35600	48 0 184-128-4
r/-	LMREPL.EXE	0000.00.00 00:00:00 (GMT)	0000.00.00 00:00:00 (GMT)	0	0 0 0 0
r/r	LMREPL.EXE	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	86800	48 0 185-128-4
r/r	loadfix.com	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	1131	48 0 186-128-4 (realloc)
r/r	loadfix.com	1996.10.14 01:38:00 (EDT)	2002.06.13 17:08:40 (EDT)	1131	48 0 186-128-4

ASCII ([display - report](#)) * Strings ([display - report](#)) * [Export](#) * [Add Note](#)
File Type: MS Windows PE 32-bit Intel 80386 GUI executable

String Contents Of File: E:\system32/inetins.exe

```
!This program cannot be run in DOS mode.  
.text  
.rdata  
@.data  
.rsrc  
@.reloc  
MSVCRT.dll  
KERNEL32.dll  
USER32.dll  
OSVW
```

- Didn't run natively on Windows
- Slow UI and analytics
- Old-school HTML
 - Couldn't right click
- Didn't allow much at the application level

- Open Source Graphical Platform / Framework
- Automation
- Fast Results / Triage
- Easy to use
- Appeal to large audience

Directory Listing

xp-sp3-v4.001\vol2

25 Results

Table View Thumbnail View

Images

- xp-sp3-v4.001
 - vol1 (Unallocated: 0-62)
 - vol2 (NTFS (0x07): 63-8193149)
 - \$Extend
 - Documents and Settings
 - Program Files
 - System Volume Information
 - WINDOWS
 - \$OrphanFiles
 - vol3 (Unallocated: 8193150-10485215)
- Views
 - File Types
 - Images
 - Videos
 - Audio
 - Documents
 - Recent Files
 - Final Day
 - Final Day - 1
 - Final Day - 2
 - Final Day - 3
 - Final Day - 4
 - Final Day - 5
 - Final Day - 6
- Results
 - Extracted Content
 - Bookmarks (174)
 - Cookies (1911)
 - Web History (1218)
 - Downloads (30)
 - Recent Documents (72)
 - Installed Programs (72)
 - Device Attached (9)
 - Keyword Hits
 - Single Literal Keyword Search (0)
 - Single Regular Expression Search (0)
 - Hashset Hits

Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags
\$boot	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	8192	Allocated	Allocated
\$Extend	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	344	Allocated	Allocated
\$LogFile	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	23085056	Allocated	Allocated
\$MFT	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	15859712	Allocated	Allocated
\$MFTMirr	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	4096	Allocated	Allocated
\$Secure:\$SDS	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Allocated
\$UpCase	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	131072	Allocated	Allocated
\$Volume	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Allocated
AUTOEXEC.BAT	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
boot.ini	2012-01-20 17:19:25	2012-01-20 17:20:54	2012-01-20 17:19:25	2012-01-20 12:10:10	211	Allocated	Allocated
CONFIG.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
Documents and Settings	2012-03-22 19:29:54	2012-03-22 19:29:54	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Allocated
IO.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
MSDOS.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
NTDETECT.COM	2008-04-13 22:13:04	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-13 22:13:04	47564	Allocated	Allocated
ntldr	2008-04-14 00:01:44	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-14 00:01:44	250048	Allocated	Allocated
pagefile.sys	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-01-20 12:09:08	20971520	Allocated	Allocated
Program Files	2012-03-20 19:25:02	2012-03-20 19:25:02	2012-03-10 14:40:46	2012-01-20 12:11:01	56	Allocated	Allocated
System Volume Information	2012-01-20 17:21:37	2012-01-20 17:21:37	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Allocated
WINDOWS	2012-03-05 19:12:38	2012-03-05 19:12:38	2012-03-10 14:40:46	2012-01-20 12:09:08	56	Allocated	Allocated
\$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	Allocated	Allocated

Result View Hex View Media View String View Text View

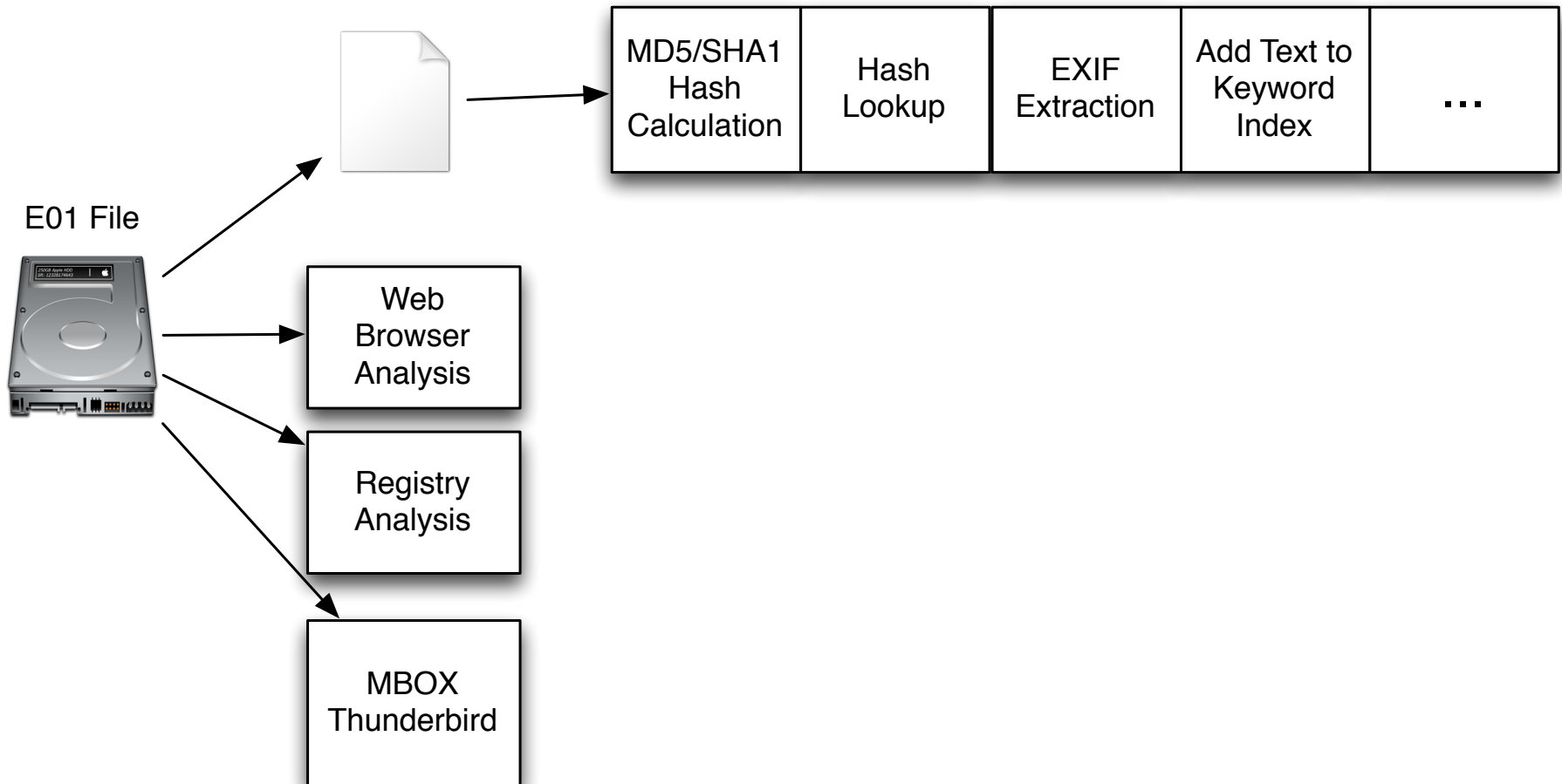
Page: 1 of 3 Page Go to Page:

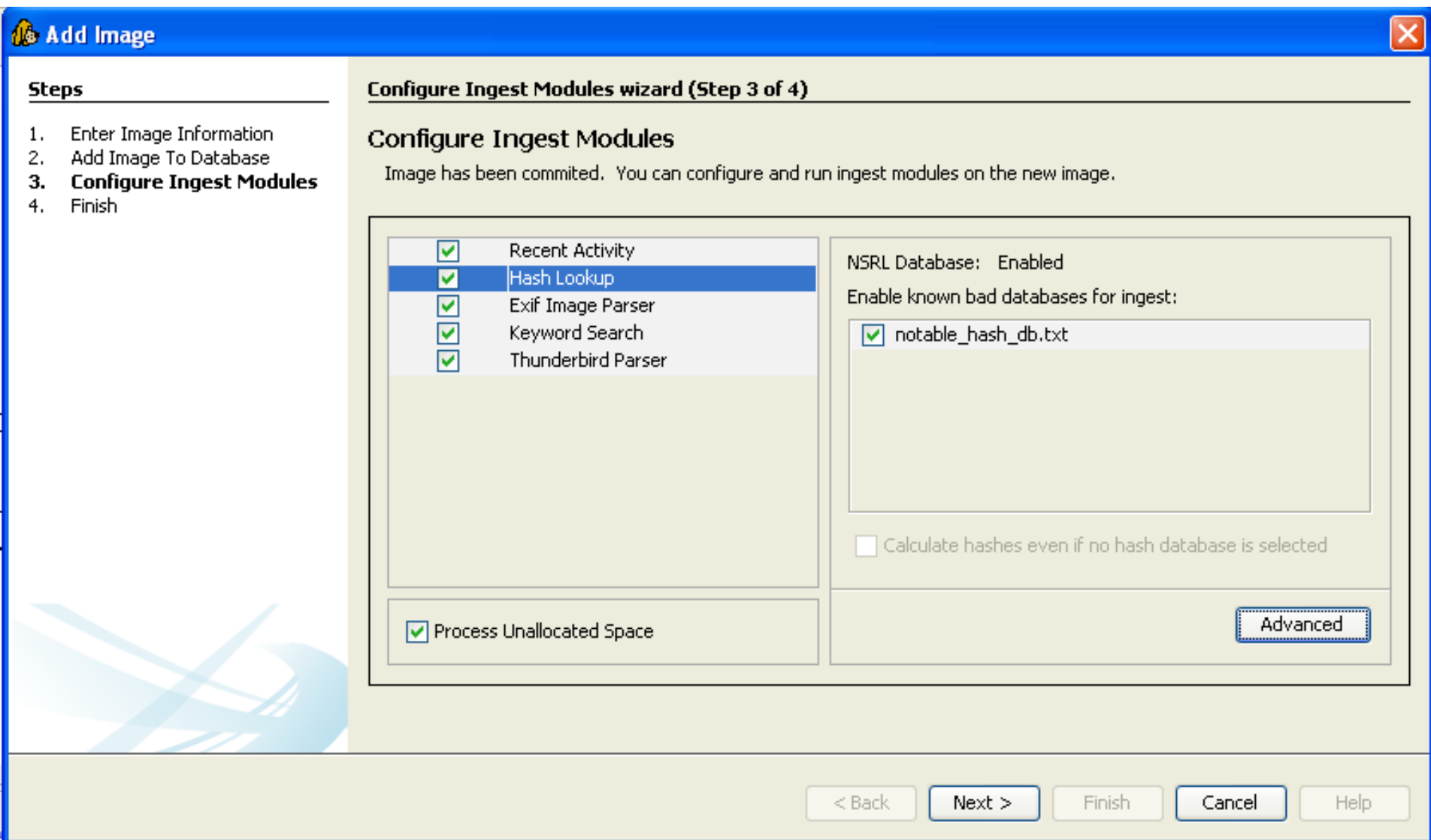
```

0x000000: 66 55 66 39 EC 66 FD E5 FF FF 00 00 1E 06 66 53 EUE...E...E$
0x000010: 66 56 66 57 B9 FD A4 C1 E9 04 52 C8 03 C1 7D D8 EVIEW...
0x000020: 7D C0 66 39 CC 66 30 0E 00 00 52 D1 30 0E 04 00 ..E..E..E..E..E
0x000030: 66 39 5E 08 66 39 4E 0C 66 39 76 10 66 39 7E 14 E..E..N..E..V..E..~
0x000040: 66 39 56 18 66 39 6E 1C 7D D0 66 BC 06 10 00 00 E..V..E..n...E...
0x000050: 66 55 66 52 66 57 66 56 66 51 66 53 66 33 C0 66 EUEFEWEVEFESE$E
0x000060: 33 DB 66 33 C9 66 33 D2 66 33 F6 66 33 FF E8 B7 3..E3..E3..E3...
0x000070: 02 66 0F B2 26 00 00 66 5F 66 5E 66 5B 07 1F 66 ..E..E..E..E^E[...E
0x000080: 5D CB 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ].....
0x000090: 55 39 EC 56 57 53 60 4E 06 B8 00 D8 CD 15 53 39 U..VWS..N.....S
0x0000a0: 5E 04 C6 27 C6 47 01 58 C6 67 02 C6 47 03 30 4F ^...G.X.g..G..O
0x0000b0: 04 C6 77 06 C6 57 07 30 7F 08 30 77 0A 5B 5F 5E ].w..W.....w[^
0x0000c0: 5D C3 55 39 EC 56 B8 01 D8 08 4E 06 60 6E 08 39 ].U..V...N..n..
0x0000d0: 76 04 CD 15 60 C4 5E 5D C3 06 53 B8 00 F0 7D C0 v.....^]..S.....
    
```

- Started with the Netbeans Platform
 - Java.
 - Designed to build apps like this.
- Designed with lots of internal frameworks.
 - Places where modules can be dropped in.
- Writing lots of docs to help developers build modules.

- Ingest Modules
- Run on each image as it is added.
 - In background
 - In parallel
 - Saves previous settings





Add Image

Steps

1. Enter Image Information
2. Add Image To Database
3. **Configure Ingest Modules**
4. Finish

Configure Ingest Modules wizard (Step 3 of 4)

Configure Ingest Modules

Image has been committed. You can configure and run ingest modules on the new image.

<input checked="" type="checkbox"/>	Recent Activity
<input checked="" type="checkbox"/>	Hash Lookup
<input checked="" type="checkbox"/>	Exif Image Parser
<input checked="" type="checkbox"/>	Keyword Search
<input checked="" type="checkbox"/>	Thunderbird Parser

Process Unallocated Space

NSRL Database: Enabled

Enable known bad databases for ingest:

- notable_hash_db.txt

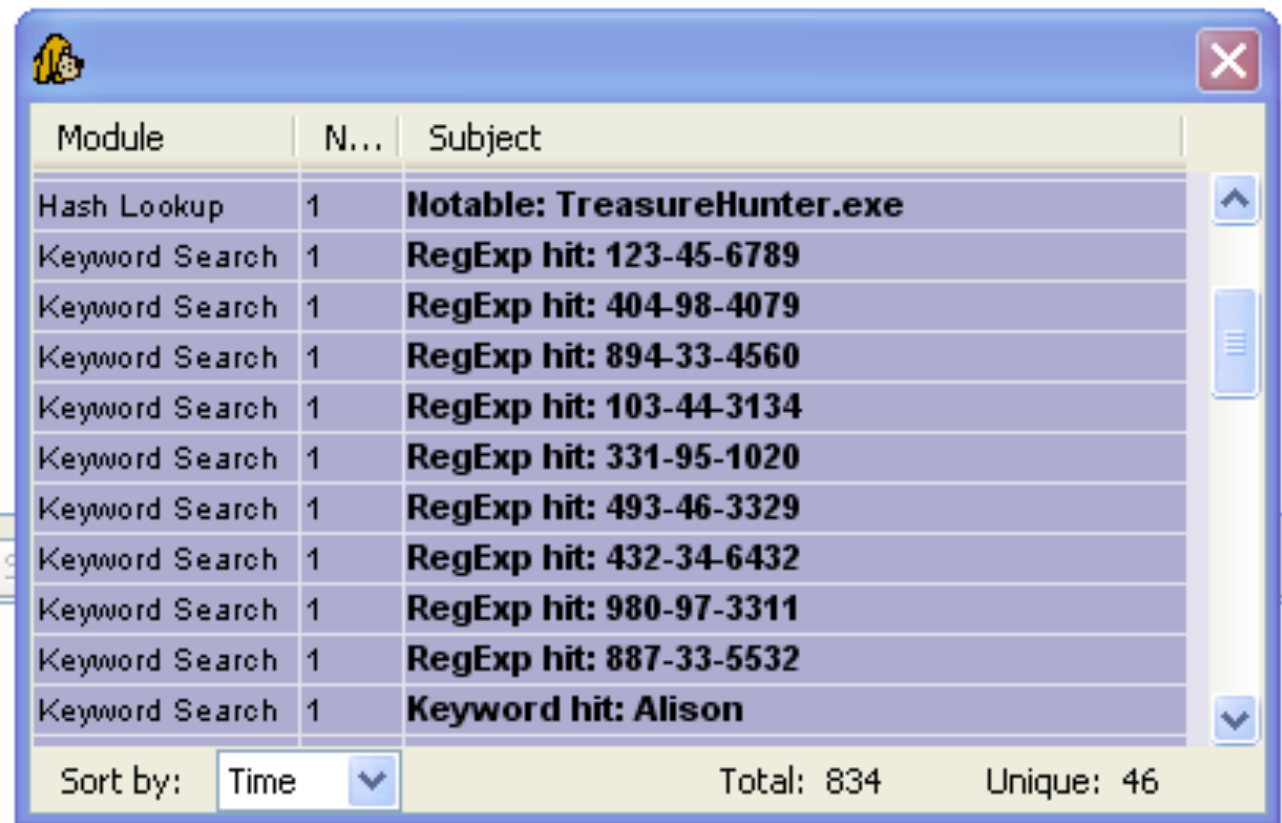
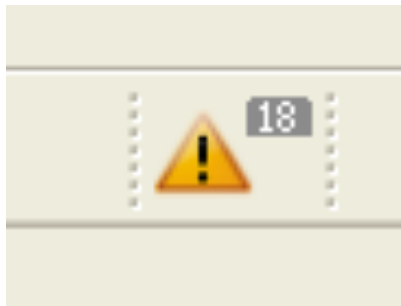
Calculate hashes even if no hash database is selected

Advanced

< Back **Next >** Finish Cancel Help

- Can configure ingest modules based on available time:
 - Process unallocated space?
 - Search for orphan files?
 - English-only strings extraction?
- Results from Ingest modules are shown as they are found.
 - Ingest Inbox gives updates.

Ingest Inbox Screen Shot

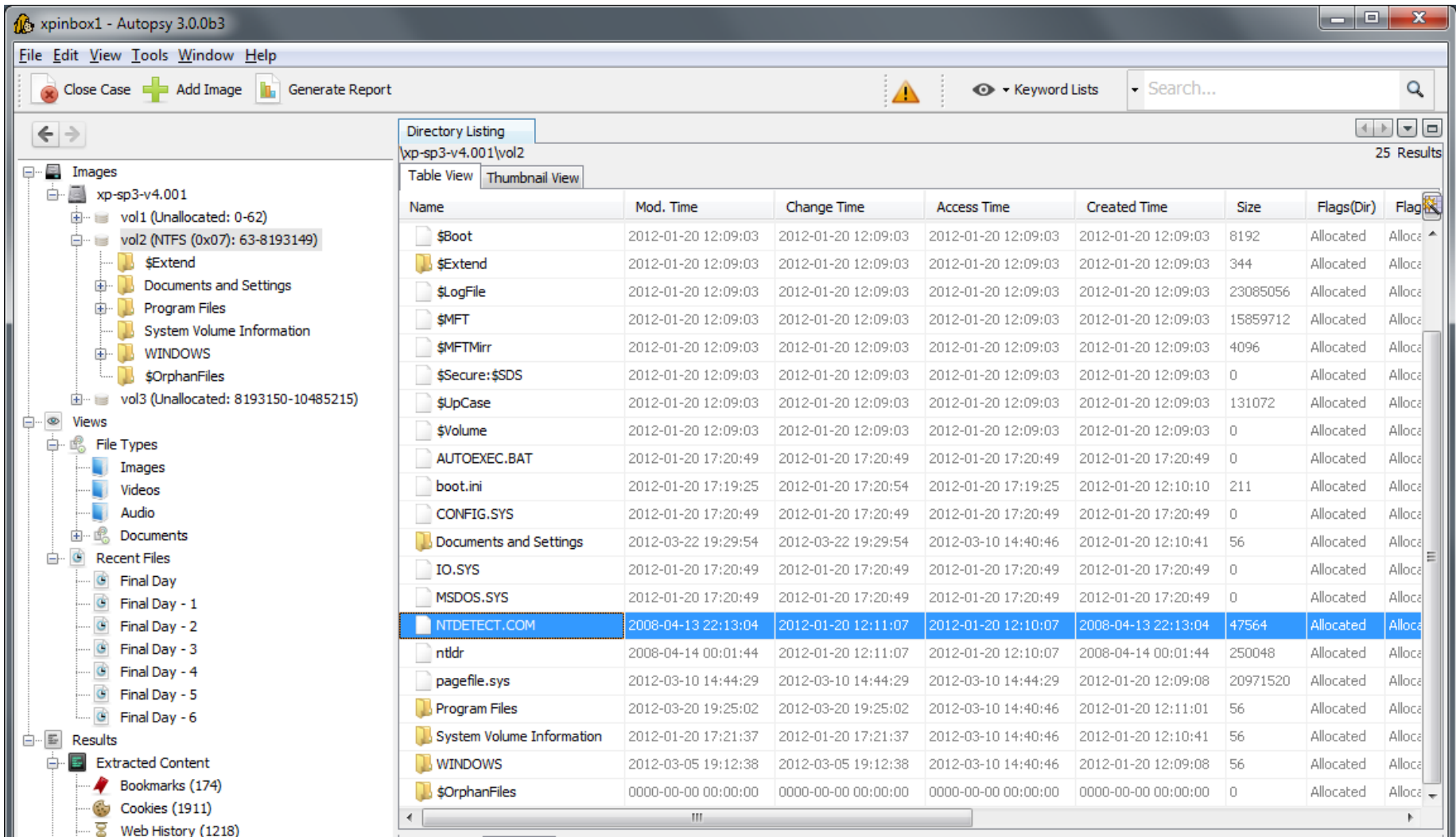


Module	N...	Subject
Hash Lookup	1	Notable: TreasureHunter.exe
Keyword Search	1	RegExp hit: 123-45-6789
Keyword Search	1	RegExp hit: 404-98-4079
Keyword Search	1	RegExp hit: 894-33-4560
Keyword Search	1	RegExp hit: 103-44-3134
Keyword Search	1	RegExp hit: 331-95-1020
Keyword Search	1	RegExp hit: 493-46-3329
Keyword Search	1	RegExp hit: 432-34-6432
Keyword Search	1	RegExp hit: 980-97-3311
Keyword Search	1	RegExp hit: 887-33-5532
Keyword Search	1	Keyword hit: Alison

Sort by: Time Total: 834 Unique: 46

- Scheduler focuses on user content:
 1. User folders
 2. Program Files folder
 3. Windows folders
- Scheduler will be modular to allow for different approaches.

- Wizards to create cases and import data.
- Single navigation tree to find ingest module results.
 - Modules post results to blackboard.
 - More details will be given in the framework talk.
- Common navigation concepts:
 - Back and Forward buttons
 - Search bar in upper right

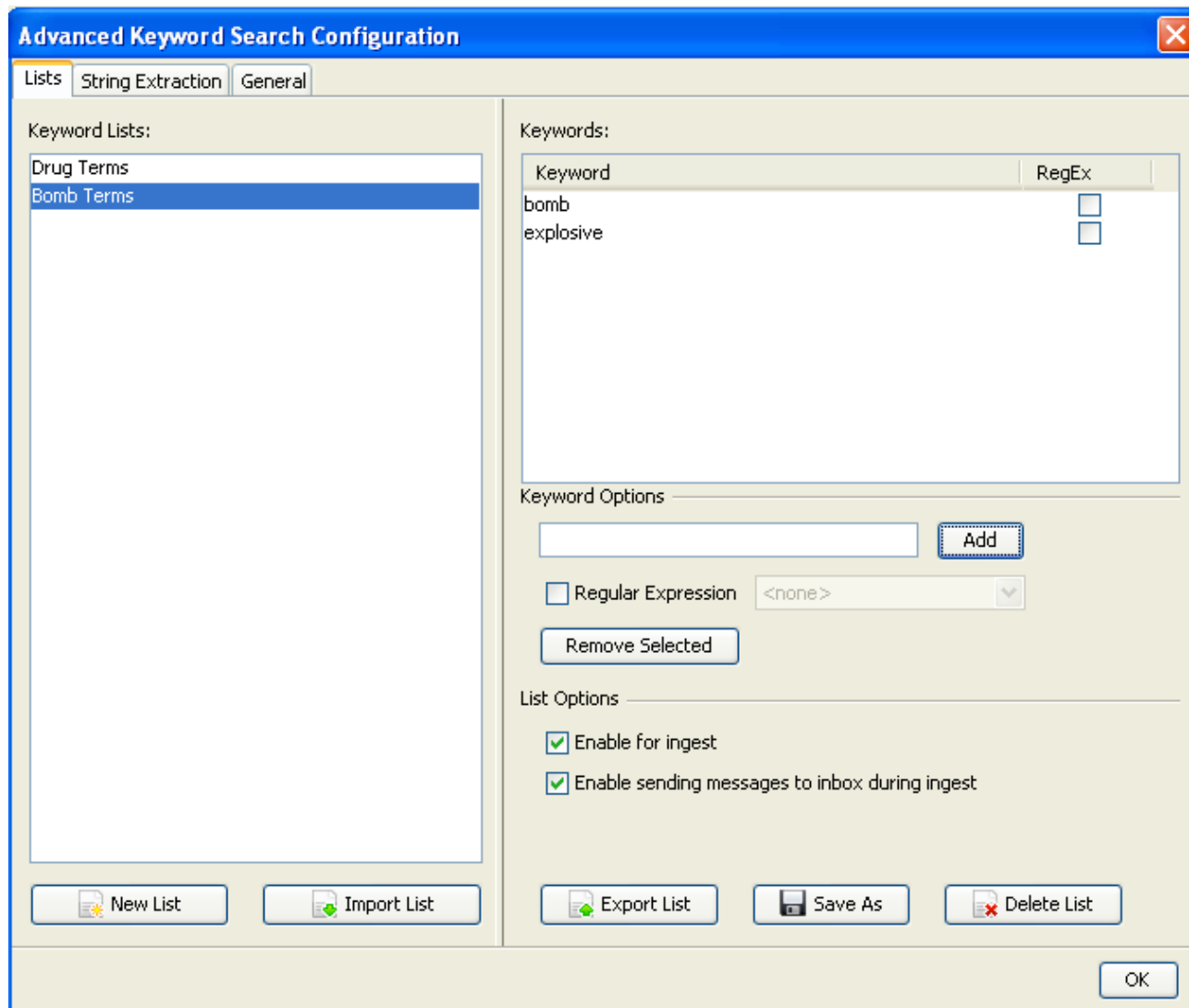


The screenshot shows the Autopsy 3.0.0b3 interface. The left pane displays a tree view of the file system structure, including folders like 'Images', 'Views', 'Recent Files', and 'Results'. The main pane shows a 'Directory Listing' for the path 'xp-sp3-v4.001\vol2'. The listing is in 'Table View' and shows 25 results. The file 'NTDETECT.COM' is highlighted in blue.

Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags
\$Boot	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	8192	Allocated	Allocated
\$Extend	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	344	Allocated	Allocated
\$LogFile	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	23085056	Allocated	Allocated
\$MFT	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	15859712	Allocated	Allocated
\$MFTMirr	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	4096	Allocated	Allocated
\$Secure:\$SDS	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Allocated
\$UpCase	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	131072	Allocated	Allocated
\$Volume	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Allocated
AUTOEXEC.BAT	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
boot.ini	2012-01-20 17:19:25	2012-01-20 17:20:54	2012-01-20 17:19:25	2012-01-20 12:10:10	211	Allocated	Allocated
CONFIG.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
Documents and Settings	2012-03-22 19:29:54	2012-03-22 19:29:54	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Allocated
IO.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
MSDOS.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Allocated
NTDETECT.COM	2008-04-13 22:13:04	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-13 22:13:04	47564	Allocated	Allocated
ntldr	2008-04-14 00:01:44	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-14 00:01:44	250048	Allocated	Allocated
pagefile.sys	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-01-20 12:09:08	20971520	Allocated	Allocated
Program Files	2012-03-20 19:25:02	2012-03-20 19:25:02	2012-03-10 14:40:46	2012-01-20 12:11:01	56	Allocated	Allocated
System Volume Information	2012-01-20 17:21:37	2012-01-20 17:21:37	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Allocated
WINDOWS	2012-03-05 19:12:38	2012-03-05 19:12:38	2012-03-10 14:40:46	2012-01-20 12:09:08	56	Allocated	Allocated
\$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	Allocated	Allocated

- Focused first on Windows.
- Installer
- Auto-update
- Basic features
 - Keyword Search
 - Hash Databases
 - File System Browsing
 - Registry Analysis
 - E-mail Analysis

- Index-based search
- Extracts text from documents:
 - Better for non-English PDF and HTML files
- Uses Lucene SOLR (open source)
- Can support more advanced text analytics.
- Searches are done as image is indexed.
- Can save and export keyword lists.



Configure Ingest Modules

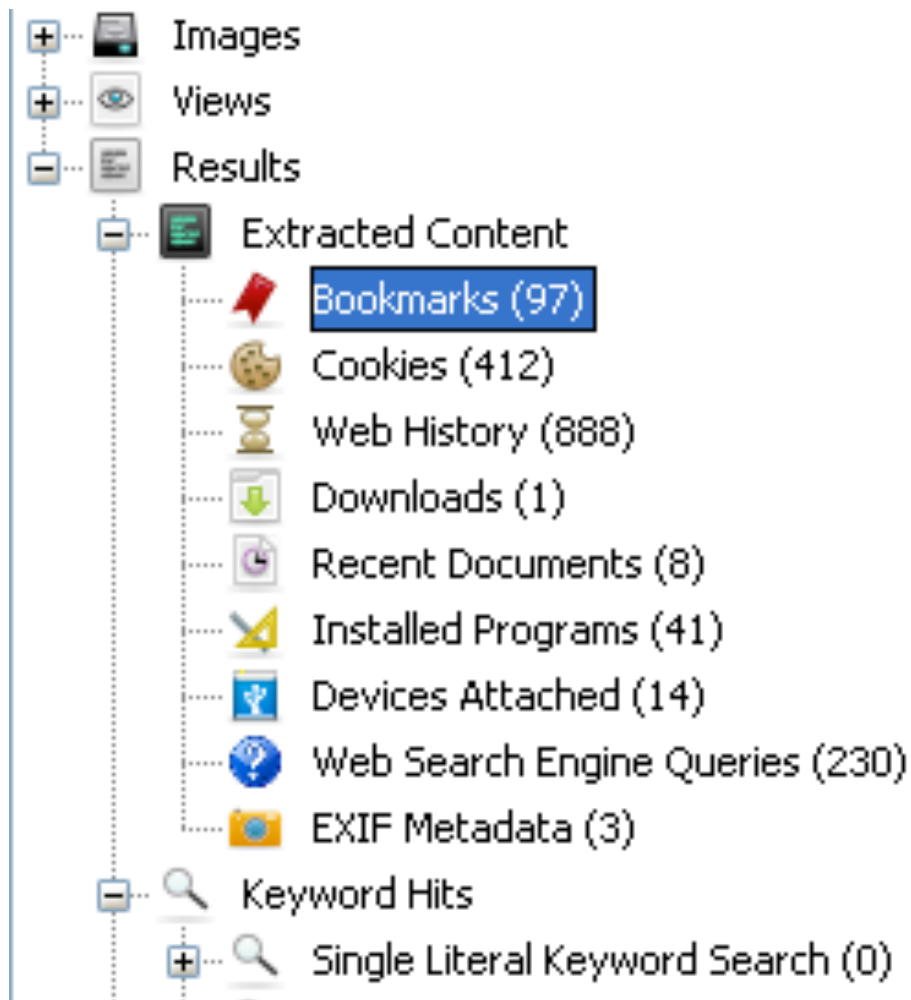
Image has been committed. You can configure and run ingest modules on the new image.

<input checked="" type="checkbox"/> Recent Activity <input checked="" type="checkbox"/> Hash Lookup <input checked="" type="checkbox"/> Exif Image Parser <input checked="" type="checkbox"/> Keyword Search <input checked="" type="checkbox"/> Thunderbird Parser	<p>Select keyword lists to enable during ingest:</p> <table border="1"><tr><td><input type="checkbox"/> Phone Numbers</td><td>▲</td></tr><tr><td><input type="checkbox"/> IP Addresses</td><td>☰</td></tr><tr><td><input checked="" type="checkbox"/> Email Addresses</td><td>▼</td></tr><tr><td><input checked="" type="checkbox"/> URLs</td><td></td></tr><tr><td><input checked="" type="checkbox"/> Drug Terms</td><td></td></tr><tr><td><input checked="" type="checkbox"/> Bank Terms</td><td></td></tr></table> <p>Scripts enabled for string extraction from unknown file types: Latin - Basic</p> <p>Encodings: UTF8, UTF16</p> <p>Advanced</p>	<input type="checkbox"/> Phone Numbers	▲	<input type="checkbox"/> IP Addresses	☰	<input checked="" type="checkbox"/> Email Addresses	▼	<input checked="" type="checkbox"/> URLs		<input checked="" type="checkbox"/> Drug Terms		<input checked="" type="checkbox"/> Bank Terms	
<input type="checkbox"/> Phone Numbers	▲												
<input type="checkbox"/> IP Addresses	☰												
<input checked="" type="checkbox"/> Email Addresses	▼												
<input checked="" type="checkbox"/> URLs													
<input checked="" type="checkbox"/> Drug Terms													
<input checked="" type="checkbox"/> Bank Terms													
<input checked="" type="checkbox"/> Process Unallocated Space													

- Can calculate MD5 and SHA-1 hashes of all files.
- Looks up hashes in:
 - NSRL (known files)
 - EnCase hashsets (notable / known bad)
 - Md5 hashsets (notable / known bad)
- Identifies known bad files as they are found.

- Focuses on user activity
- Browser artifacts:
 - History, cookies, downloads, bookmarks
 - Firefox, Chrome, Safari, IE
- Recent user docs
- Recent devices
- Uses:
 - RegRipper
 - Pasco2

Recent Activity Results



- MBOX / Thunderbird
 - Parses into individual messages
- Exif
 - Extracts dates, GPS, and device information
- More to come

- Allows for different file types to be viewed differently.
- Standard modules:
 - Hex
 - Strings extraction (4 or more printable characters)
 - Extracted Text from index
 - Media (pictures / video)
 - gstreamer

Content Viewer: Hex



Hex View	String View	Result View	Text View	Media View
Page: 1 of 1	Page	←	→	Go to Page: <input type="text"/>
0x000000:	FF D8 FF E0 00 10 4A 46	49 46 00 01 01 01 00 48JFIF.....H	
0x000010:	00 48 00 00 FF DB 00 43	00 0A 07 07 08 07 06 0A	.H.....C.....	
0x000020:	08 08 08 0B 0A 0A 0B 0E	18 10 0E 0D 0D 0E 1D 15	
0x000030:	16 11 18 23 1F 25 24 22	1F 22 21 26 2B 37 2F 26	...#.*\$".!&+7/&	
0x000040:	29 34 29 21 22 30 41 31	34 39 3B 3E 3E 3E 25 2E)4)!"0A149;>>>%.	
0x000050:	44 49 43 3C 48 37 3D 3E	3B FF DB 00 43 01 0A 0B	DIC<H7=>;...C...	
0x000060:	0B 0E 0D 0E 1C 10 10 1C	3B 28 22 28 3B 3B 3B 3B;(" (;;;	
0x000070:	3B 3B 3B 3B 3B 3B 3B 3B	3B 3B 3B 3B 3B 3B 3B 3B	;;;;;;;;;;;;;;;;	
0x000080:	3B 3B 3B 3B 3B 3B 3B 3B	3B 3B 3B 3B 3B 3B 3B 3B	;;;;;;;;;;;;;;;;	
0x000090:	3B 3B 3B 3B 3B 3B 3B 3B	3B 3B 3B 3B 3B 3B FF C0	;;;;;;;;;;;;;;;;..	
0x0000a0:	00 11 08 00 64 00 C0 03	01 11 00 02 11 01 03 11d.....	
0x0000b0:	01 FF C4 00 1F 00 00 01	05 01 01 01 01 01 01 00	
0x0000c0:	00 00 00 00 00 00 00 01	02 03 04 05 06 07 08 09	
0x0000d0:	0A 0B FF C4 00 B5 10 00	02 01 03 03 02 04 03 05	
0x0000e0:	05 04 04 00 00 01 7D 01	02 03 00 04 11 05 12 21}.....!	
0x0000f0:	31 41 06 13 51 61 07 22	71 14 32 FD 18 A1 08 23	lA..Qa."q.2....#	
0x000100:	42 B1 C1 15 52 D1 F0 24	33 62 72 1A 09 0A 16 17	B...R..\$3br.....	

Content Viewer: Strings



Hex View String View Result View Text View Media View

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

```
JFIF
    
+7/ )4)!"0A149;>>>% .DIC<H7=>;
;("(:;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
 3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
      #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
r1'8
the
I +H
z1Ei'
<8#4
#|.bi
F9@Z
`n#4
(i04
```

Hex View String View Result View Text View **Media View**



أكتوبر/ تشرين الأول 2001 : فر **al-Zarqawi** إلى **Iran** بعد أن فقدت **Taliban** سيطرتها على **Afghanistan**، ومن هناك جند فلسطينيين اثنين وأردنيا دخلوا **Turkey** وكان من المفترض أن يذهبوا إلى **Israel** للقيام بهجمات بالفتائل هناك .

15 فبراير/ شباط 2002 : إلغاء القبض على الثلاثة الذين أرسلهم **al-Zarqawi** في **Turkey** .

مايو/ أيار 2002 : سافر **al-Zarqawi** إلى **Iraq** حيث فقد إحدى رجليه واستبدل بها أخرى صناعية .

مايو/ أيار- يوليو/ تموز 2002 : تعافى من إصابته في **Baghdad** والتقى بعض المقاتلين هناك حيث أقام قاعدة عمليات .

نهاية صيف 2002 : سافر **al-Zarqawi** إلى **Lebanon** لمقابلة قادة من **Hizballah** ومجموعة مسلحة أخرى .

بداية 2003 : عاد **al-Zarqawi** إلى معسكر أنصار الإسلام في **Iraq**، وقام شخص آخر تدرّب في هذا المعسكر بالتخطيط لهجمات كيميائية باستخدام سموم مختلفة في **Britain France Georgia Chechnya** .

يناير/ كانون الثاني 2003 : القبض على بعض "الإرهابيين" في **Britain** بتهمة التخطيط لوضع ريسين في أغذية الجيش، ومرة أخرى يربط بين "الإرهابيين" **Wa'alzzarqawi** .

5 فبراير/ شباط 2003 : وزير الخارجية الأميركي **Colin Powell** تحدث أمام **Majlis al-Amn** مشيراً إلى معلومات لديه عن علاقات **al-Zarqawi** بتنظيم **al-Qa'idah** في **Iraq** .

- Finds names of people and places.
- Translates from Arabic to Latin Characters
- Looks names up in watch lists.

- Results can be saved to HTML or XML.
- Other modules can be created in the future.

- Available from sleuthkit.org:

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

- Writing modules will make your life easier:
 - We deal with file access.
 - We deal with displaying results
 - ...
- We're polishing up the module writer's guide:
www.sleuthkit.org/autopsy/docs/api-docs

- Give us feedback.
- Bug the developers of your favorite tools to write them as modules.

- Partly funded by US Army Intelligence Center of Excellence (USAICoE).
 - Partnered with 42Six Solutions



- Framework Enhancements
- Linux / OS X support
- More modules
- Tighter integration with TSK Framework.



Thank you!

For more information:

Visit www.basistech.com

Write to conference@basistech.com

Call 617-386-2090 or 800-697-2062