The Sleuth Kit and Open Source Digital Forensics Conference

October 3, 2012
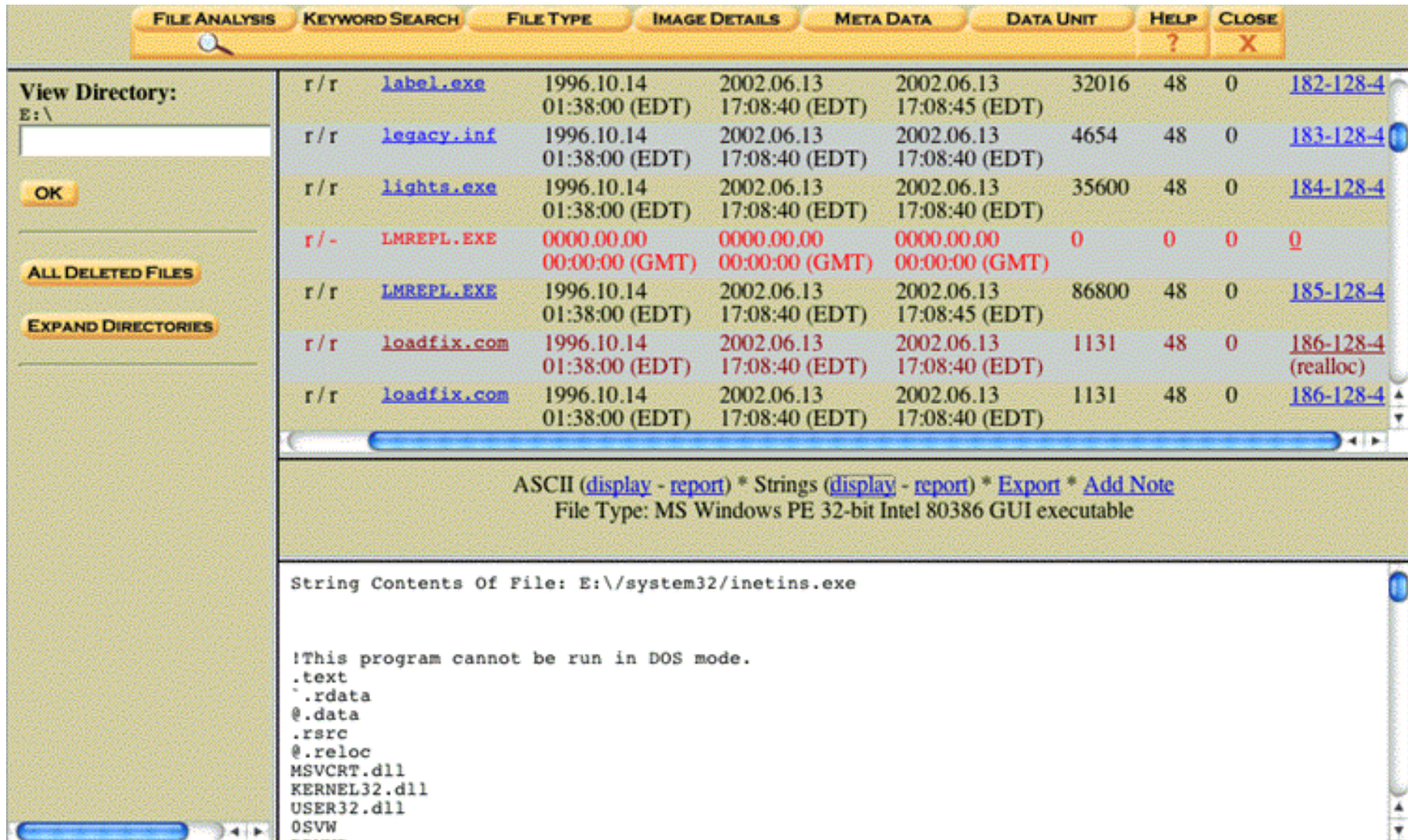
Autopsy 3.0

Brian Carrier

VP of Digital Forensics

Basis Technology

Autopsy 2

Why it had to go

- 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

xpinbox1 - Autopsy 3.0.0b3

File Edit View Tools Window Help

Close Case   Add Image   Generate Report   Keyword Lists   Search...

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

Directory Listing

\xp-sp3-v4.001\vol2

25 Results

Table View | Thumbnail View

Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
$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	Alloc
$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	Alloc
$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	Alloc
$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	Alloc
$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	Alloc
$Secure:$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	Alloc
$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	Alloc
$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	Alloc
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	Alloc
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	Alloc
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	Alloc
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	Alloc
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	Alloc
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	Alloc
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	Alloc
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	Alloc
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	Alloc
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	Alloc
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	Alloc
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	Alloc
$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	Alloc

Result View | Hex View | Media View | String View | Text View
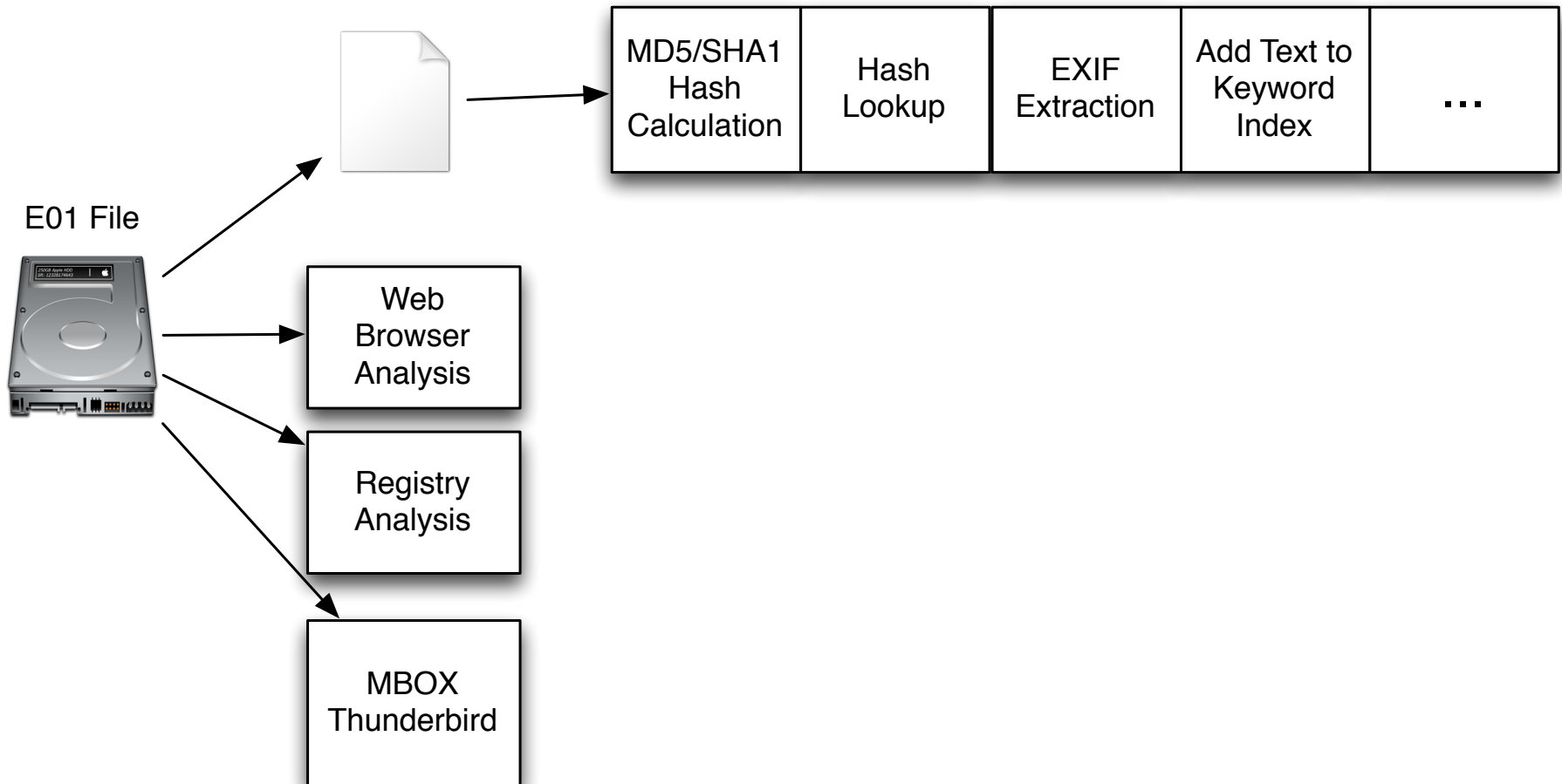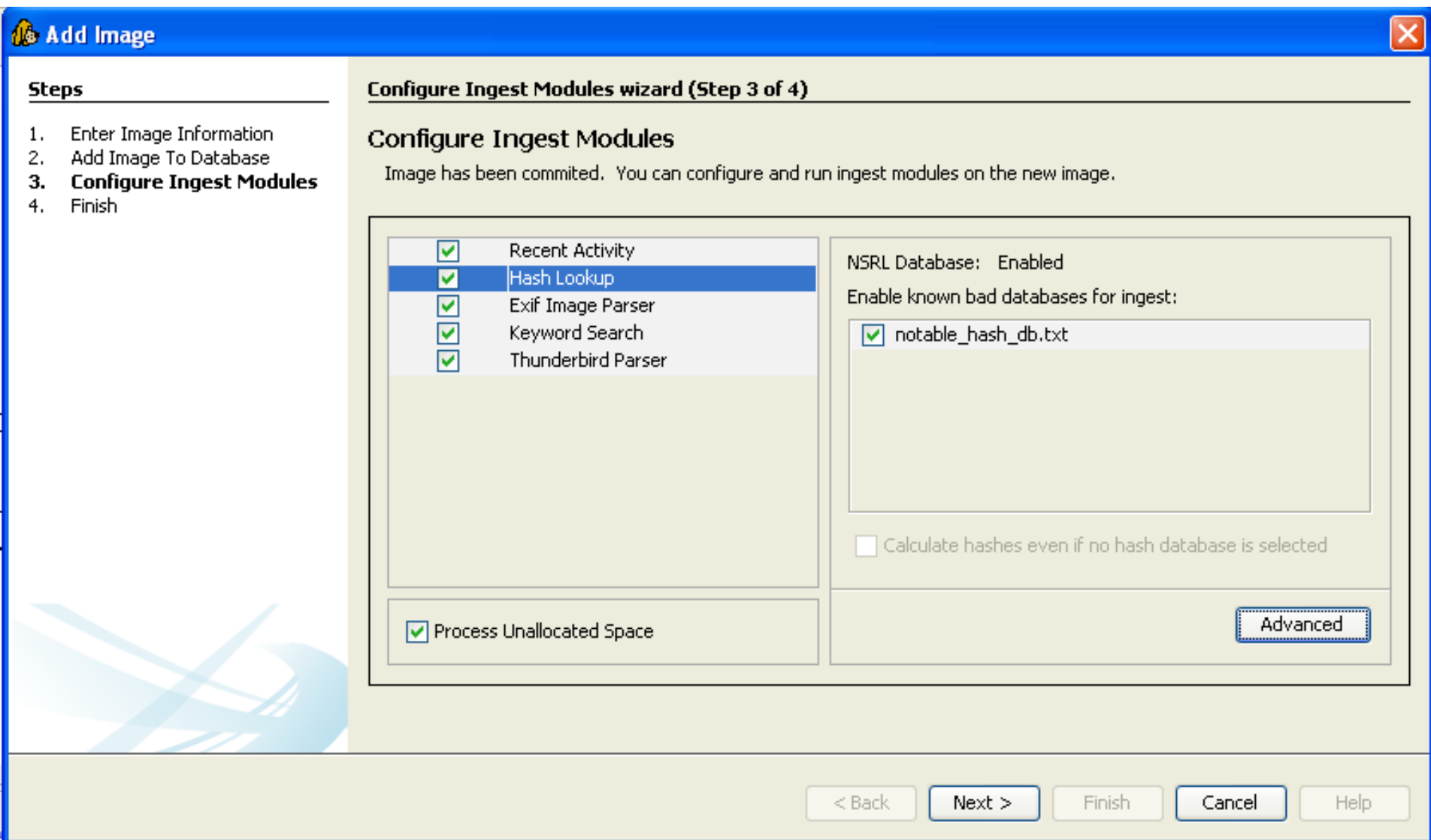
Page: 1 of 3   Page   Go to Page:

```
0x000000: 66 55 66 39 EC 66 FD E5   FF FF 00 00 1E 06 66 53   fUf..f........fS
0x000010: 66 56 66 57 B9 FD A4 C1   E9 04 52 C8 03 C1 7D D8   fVfW..........}.
0x000020: 7D C0 66 39 CC 66 30 0E   00 00 52 D1 30 0E 04 00   }.f.f.......0...
0x000030: 66 39 5E 08 66 39 4E 0C   66 39 76 10 66 39 7E 14   f.^.f.N.f.v.f.~.
0x000040: 66 39 56 18 66 39 6E 1C   7D D0 66 BC 06 10 00 00   f.V.f.n...f.....
0x000050: 66 55 66 52 66 57 66 56   66 51 66 53 66 33 C0 66   fUfRfWfVfQfSf3.f
0x000060: 33 F3 33 C9 66 33 D2   66 33 F6 66 33 FF E8 B7       3.f3.f3.f3...
0x000070: 02 66 0F B2 26 00 00 66   5F 66 5E 66 5B 07 1F 66   .f..&..f_f^f[..f
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 60 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

Ingest Modules

BASIS
TECHNOLOGY

E01 File

MD5/SHA1 Hash Calculation	Hash Lookup	EXIF Extraction	Add Text to Keyword Index	...

Web Browser Analysis

Registry Analysis

MBOX Thunderbird

Fast Results / Triage

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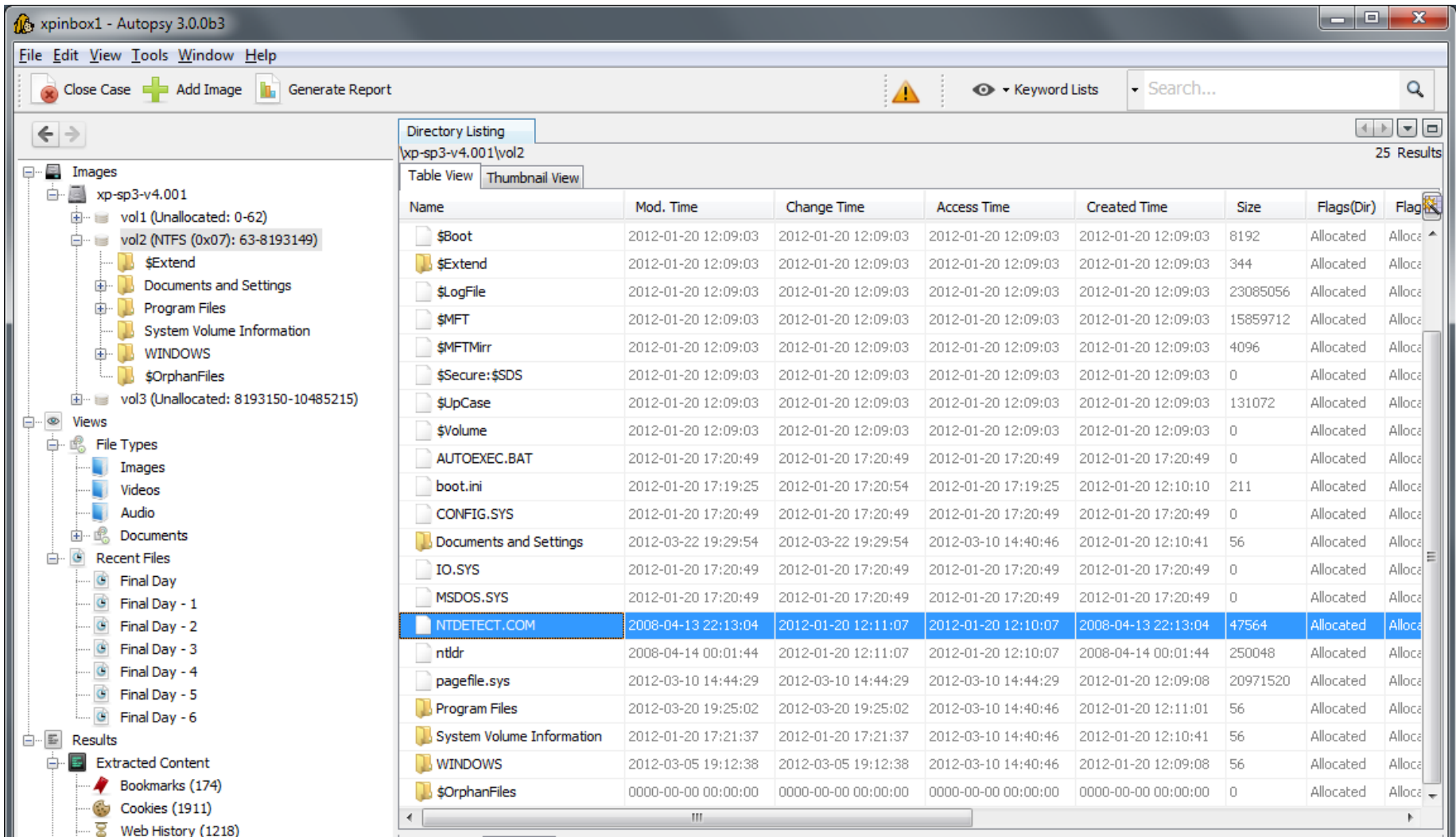
- Scheduler focuses on user content:
  1. User folders
  2. Program Files folder
  3. Windows folders
- Scheduler will be modular to allow for different approaches.

Easy To Use

- 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

Easy To Use

Appeal to Large Audience

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

Keyword Search Module

- 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.

Keyword List Manager

Keyword List Chooser

- 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.

Recent Activity Module

- 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

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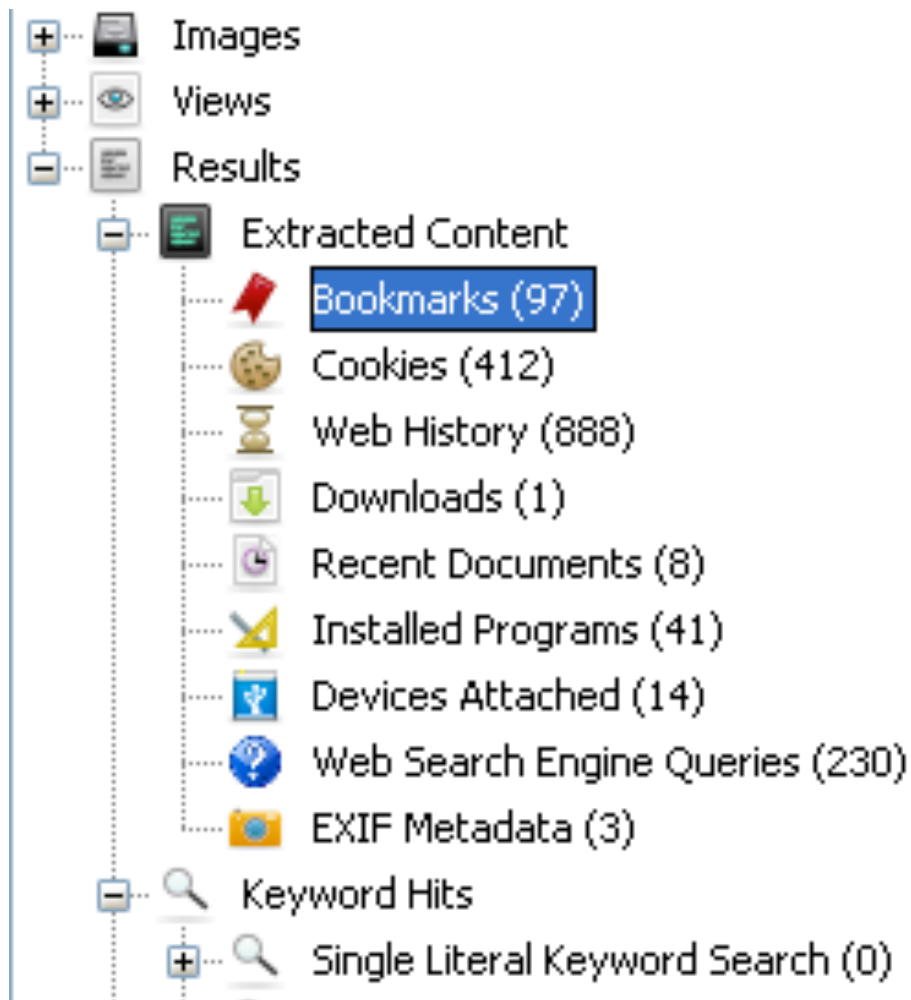
- MBOX / Thunderbird
    - Parses into individual messages
- Exif
    - Extracts dates, GPS, and device information
- More to come

Data Content Viewer Framework

- 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

Content Viewer: Strings

Content Viewer: Media

BASIS TECHNOLOGY

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

Reporting Framework

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

How do you get it?

- 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

Next Steps

- 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