Introduction to Autopsy

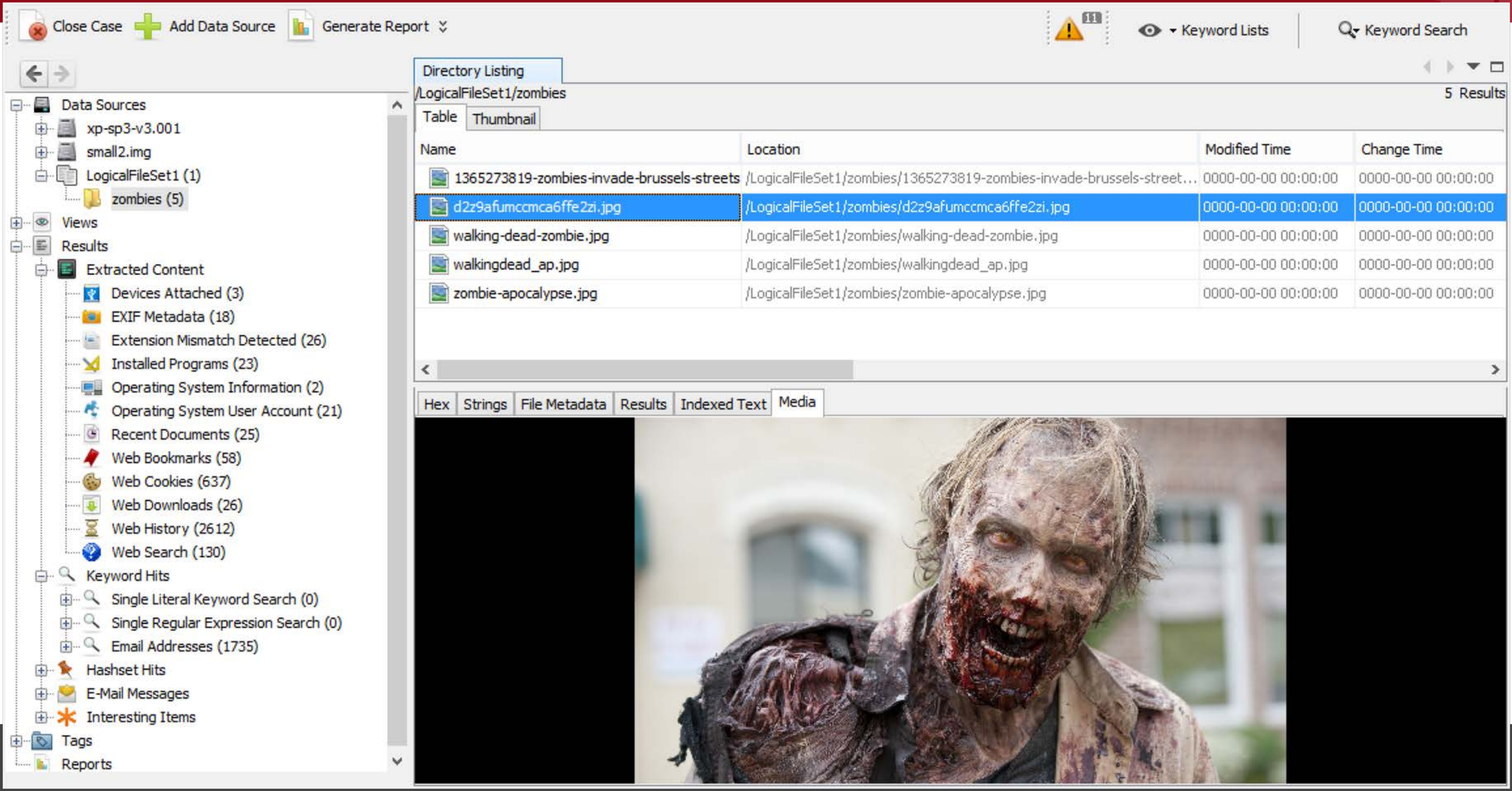
Brian Carrier

October 16, 2019 | Herndon, VA | Hosted by BASIS TECHNOLOGY

What is Autopsy?

- Open source digital forensics platform.
- Has been designed for:
  - Ease of use
  - Fast results
  - Extensibility (many plug-in frameworks)
- Has the features you need (and more).
- Free to download
- Has commercial support and development backing.
- Let’s take a quick tour

Main Interface



- Data Sources
  - xp-sp3-v3.001
  - small2.img
  - LogicalFileSet1 (1)
    - zombies (5)
- Views
- Results
  - Extracted Content
    - Devices Attached (3)
    - EXIF Metadata (18)
    - Extension Mismatch Detected (26)
    - Installed Programs (23)
    - Operating System Information (2)
    - Operating System User Account (21)
    - Recent Documents (25)
    - Web Bookmarks (58)
    - Web Cookies (637)
    - Web Downloads (26)
    - Web History (2612)
    - Web Search (130)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (1735)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
- Tags
- Reports

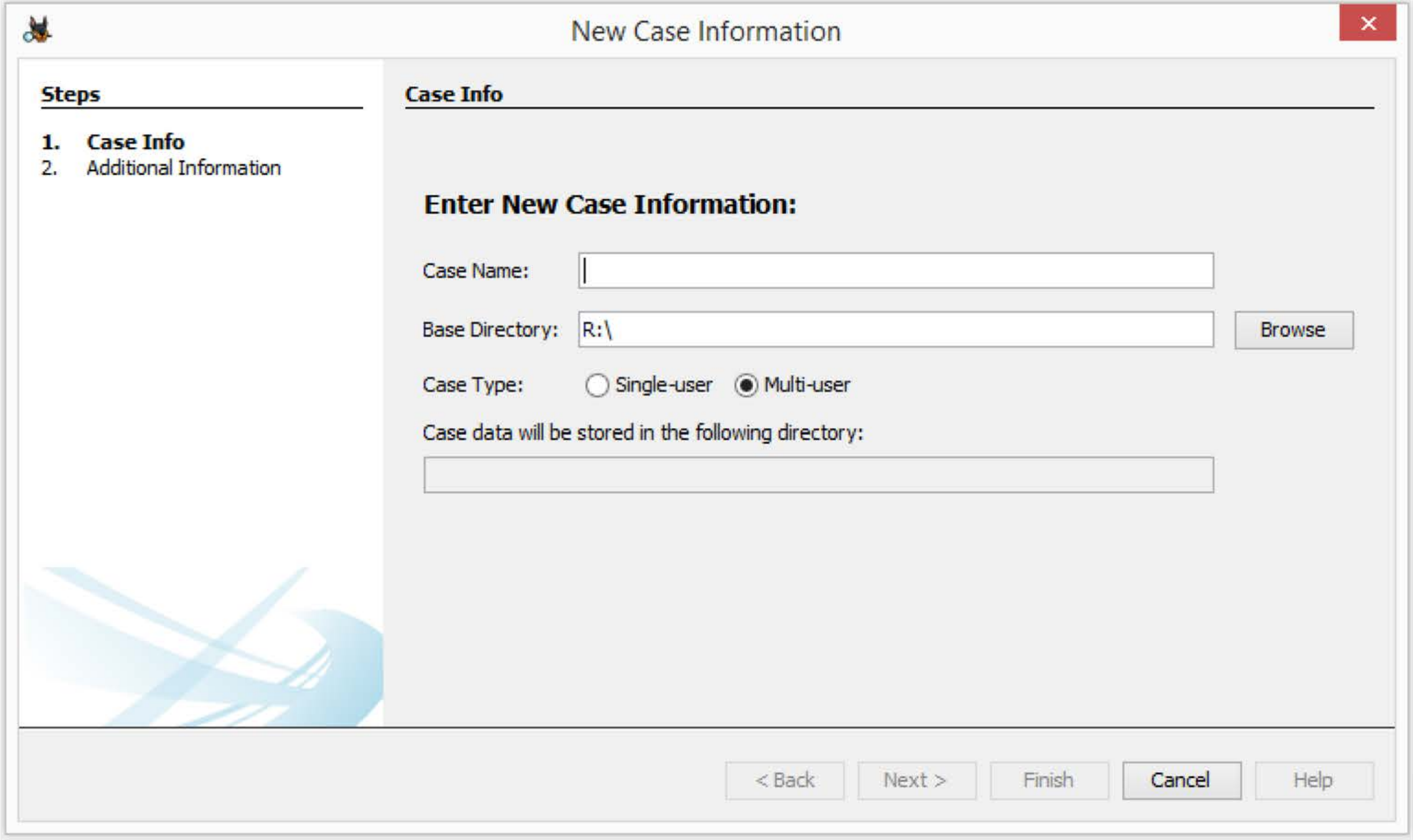
/LogicalFileSet1/zombies

5 Results

Name	Location	Modified Time	Change Time
1365273819-zombies-invade-brussels-streets	/LogicalFileSet1/zombies/1365273819-zombies-invade-brussels-street…	0000-00-00 00:00:00	0000-00-00 00:00:00
d2z9afumccmca6ffe2zi.jpg	/LogicalFileSet1/zombies/d2z9afumccmca6ffe2zi.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00
walking-dead-zombie.jpg	/LogicalFileSet1/zombies/walking-dead-zombie.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00
walkingdead_ap.jpg	/LogicalFileSet1/zombies/walkingdead_ap.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00
zombie-apocalypse.jpg	/LogicalFileSet1/zombies/zombie-apocalypse.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00

Standard Features

Make A Case



New Case Information

Steps

1. **Case Info**
2. Additional Information

Case Info

Enter New Case Information:

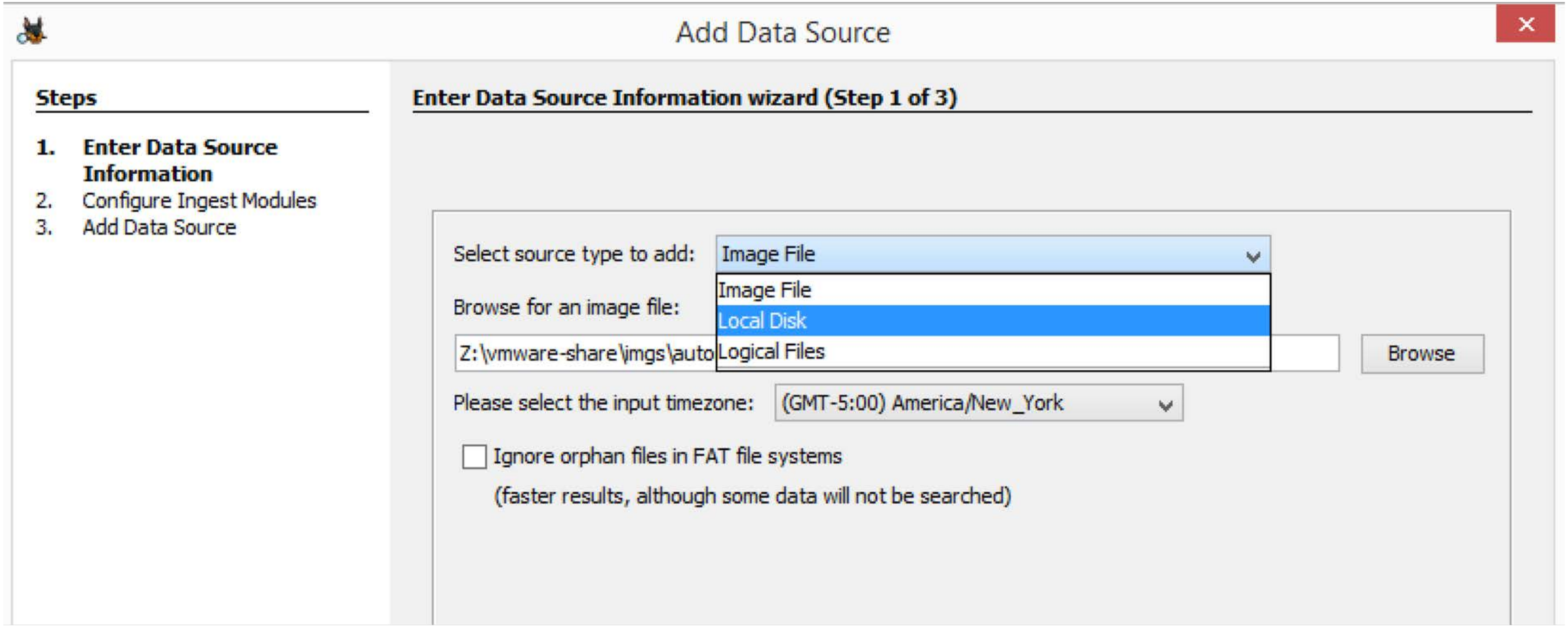
Case Name:

Base Directory: R:\

Case Type: ○ Single-user ● Multi-user

Case data will be stored in the following directory:

Add A Data Source



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: Z:\vmware-share\imgs\auto

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

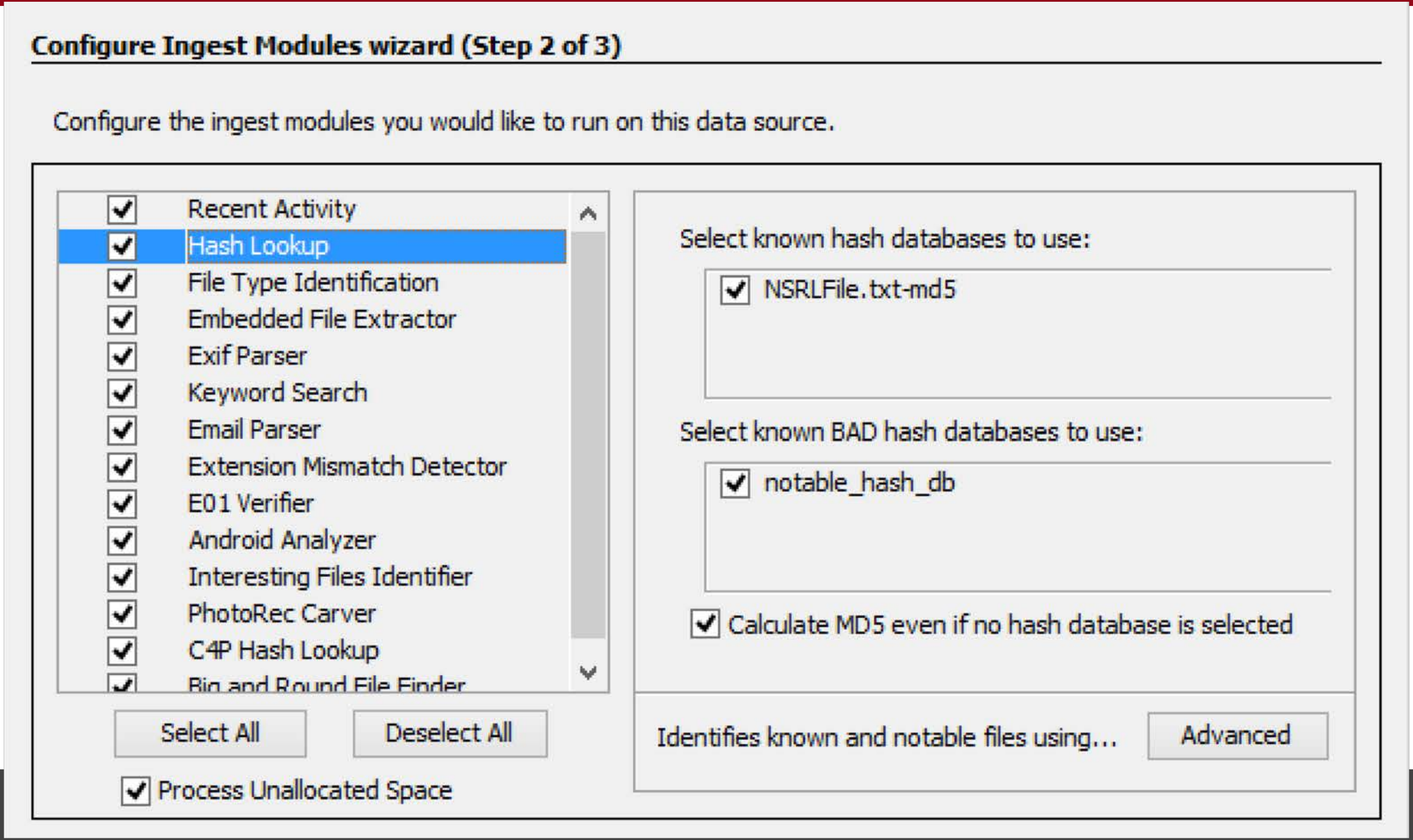
□ Ignore orphan files in FAT file systems

(faster results, although some data will not be searched)

Data Source Support

- All common file systems supported via The Sleuth Kit:
  - NTFS, FAT, ExFAT, HFS+, Ext2/Ext3/Ext4, YAFFS2, etc.
  - Covers common computers and smart phones
- Supports raw, E01, VMDK, and VHDI formats.
- Can also analyze:
  - Local drives (USB attached)
  - Local files

Choose Analysis Techniques



Configure Ingest Modules wizard (Step 2 of 3)

Configure the ingest modules you would like to run on this data source.

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round File Finder

☑ Process Unallocated Space

Select known hash databases to use:

☑ NSRLFile.txt-md5

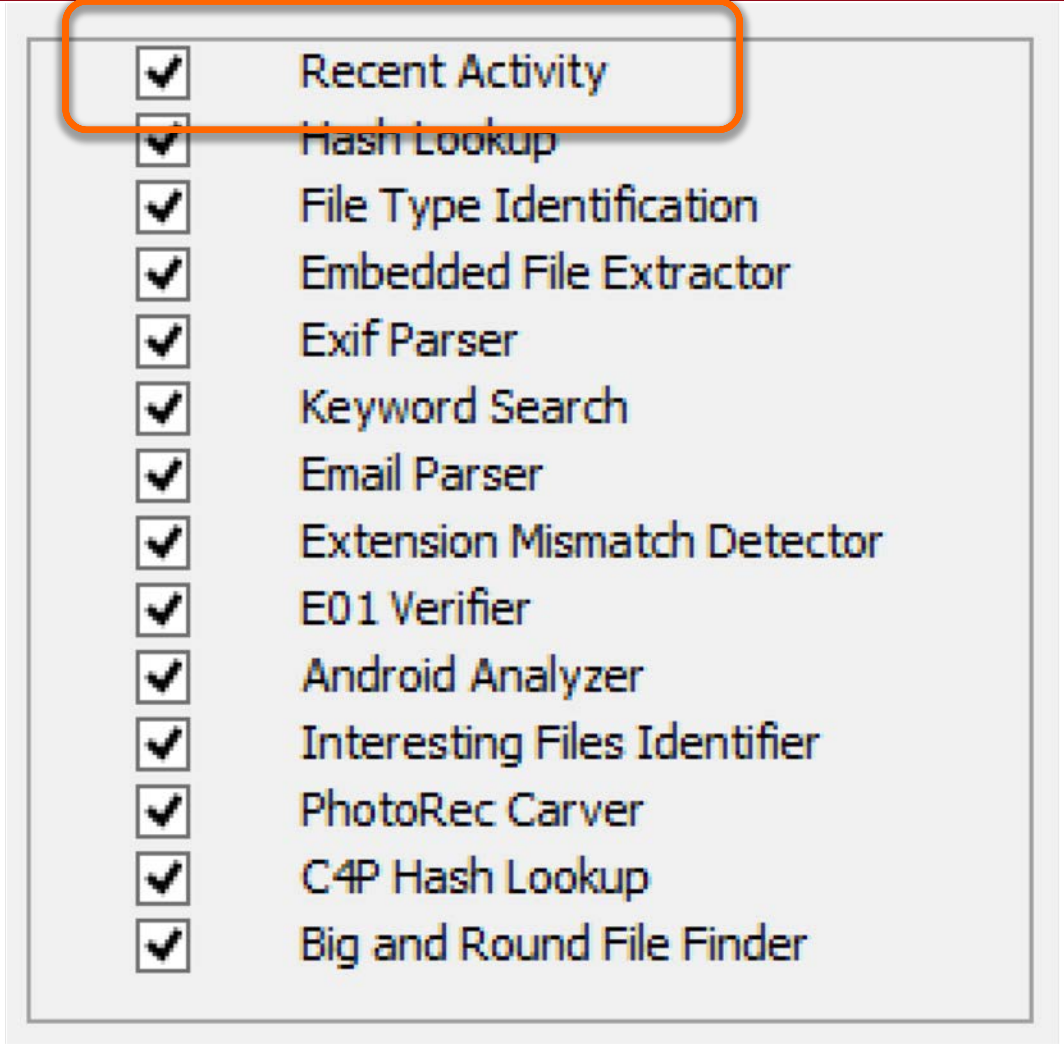
Select known BAD hash databases to use:

☑ notable_hash_db

☑ Calculate MD5 even if no hash database is selected

Identifies known and notable files using...

Standard Features

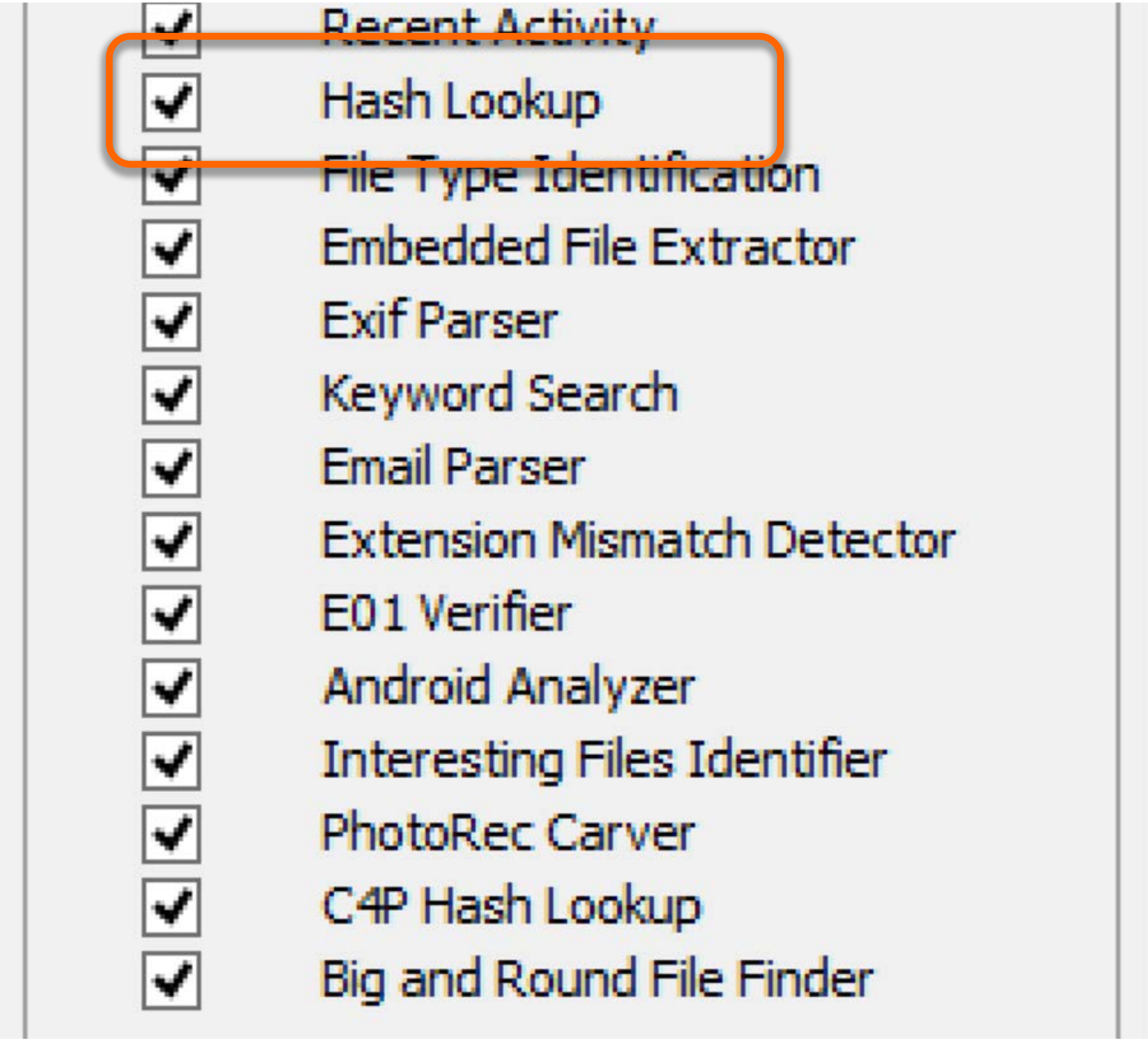


☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Android Analyzer
☑ Interesting Files Identifier
☑ PhotoRec Carver
☑ C4P Hash Lookup
☑ Big and Round File Finder

Recent Activity

- Web artifacts from Firefox, Chrome, and IE.
- Registry analysis using RegRipper.

Standard Features

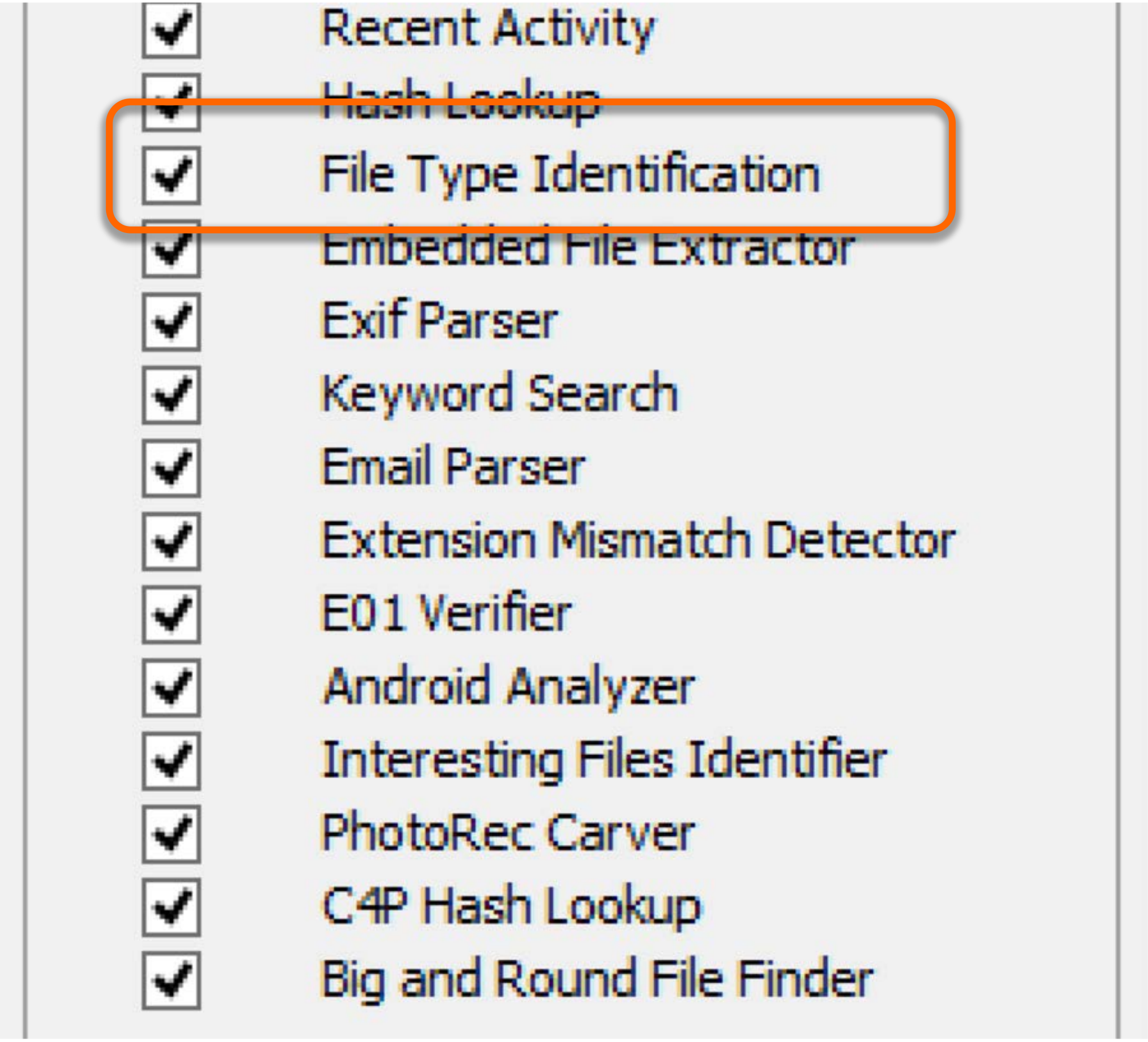


- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round File Finder

Hash Lookup

- Flags known and known bad files
- Supports:
  - NIST NSRL
  - EnCase format
  - Autopsy SQLite
  - Project Vic (with add-on)

Standard Features

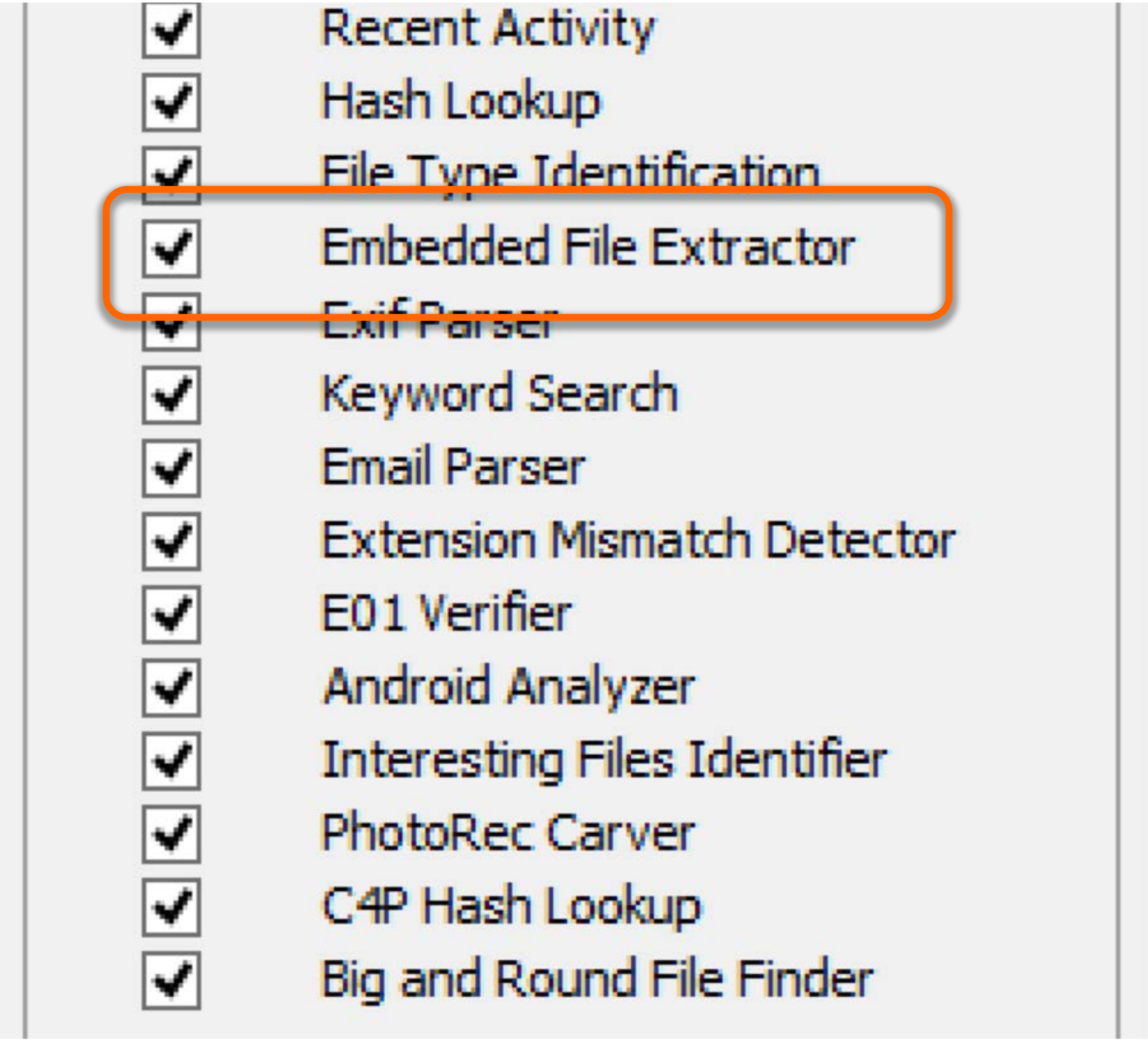


- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round File Finder

File Type Identification

- Detects files based on signatures.
- Supports user specified signatures.
  - Can raise alerts when they are found.

Standard Features



☑ Recent Activity

☑ Hash Lookup

☑ File Type Identification

☑ Embedded File Extractor

☑ Exif Parser

☑ Keyword Search

☑ Email Parser

☑ Extension Mismatch Detector

☑ E01 Verifier

☑ Android Analyzer

☑ Interesting Files Identifier

☑ PhotoRec Carver

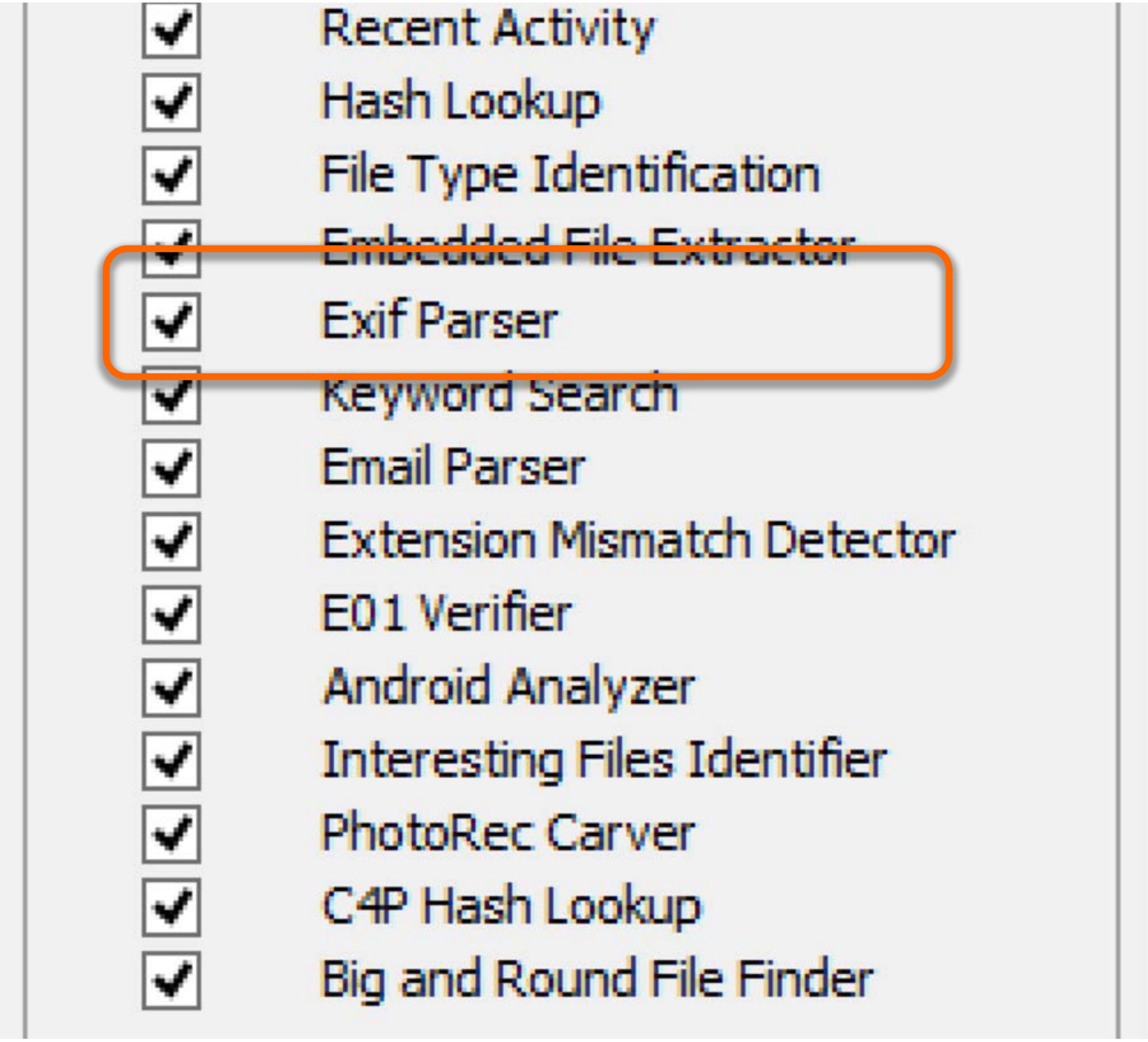
☑ C4P Hash Lookup

☑ Big and Round File Finder

Embedded File Extractor

- Opens ZIP, RAR, and many other archive files.
- Extracts images from office documents.

Standard Features

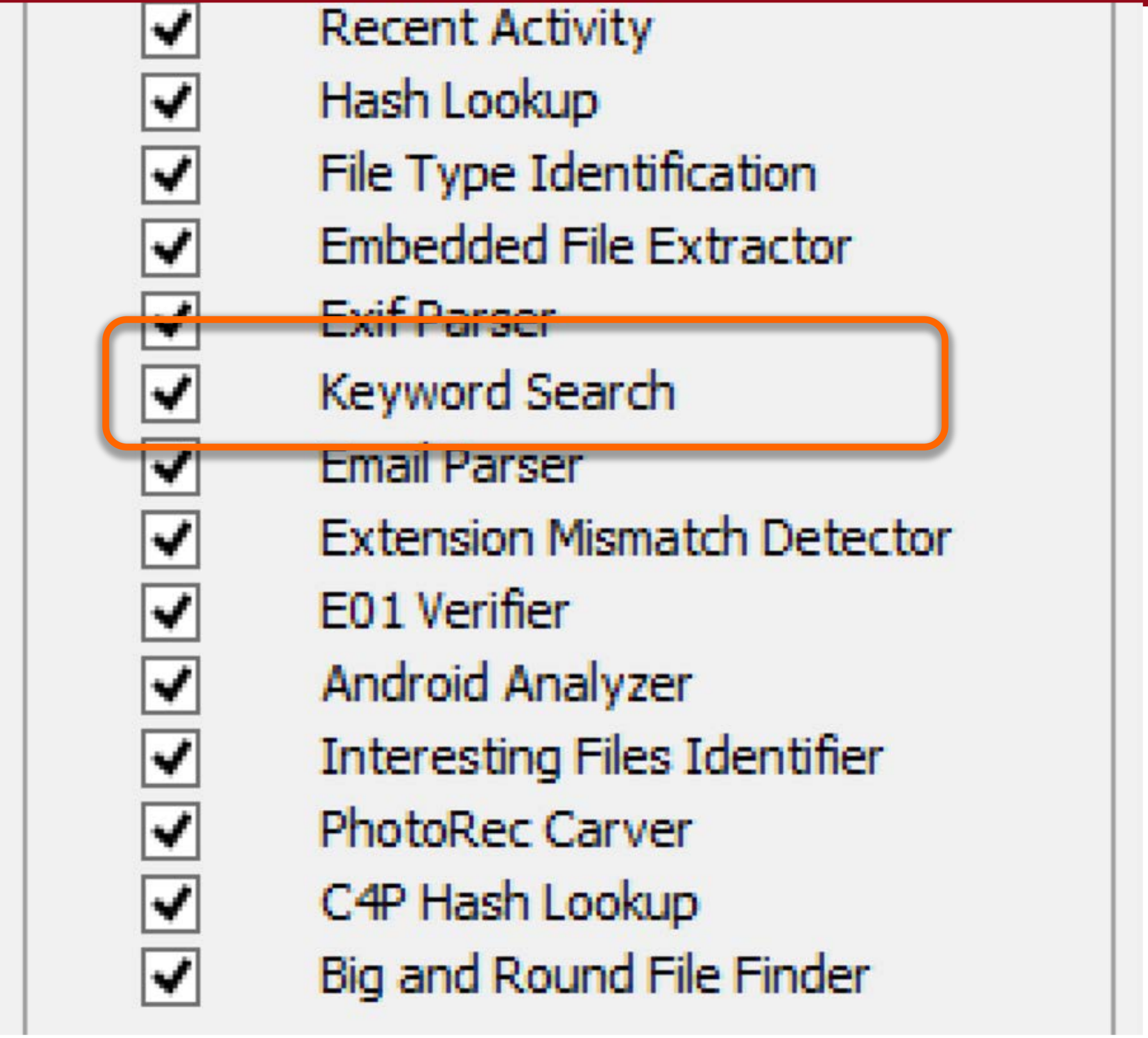


☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Android Analyzer
☑ Interesting Files Identifier
☑ PhotoRec Carver
☑ C4P Hash Lookup
☑ Big and Round File Finder

Exif Parser

- Finds JPEG images with Exif.
- Extracts device information, dates, and Geo-location.

Standard Features

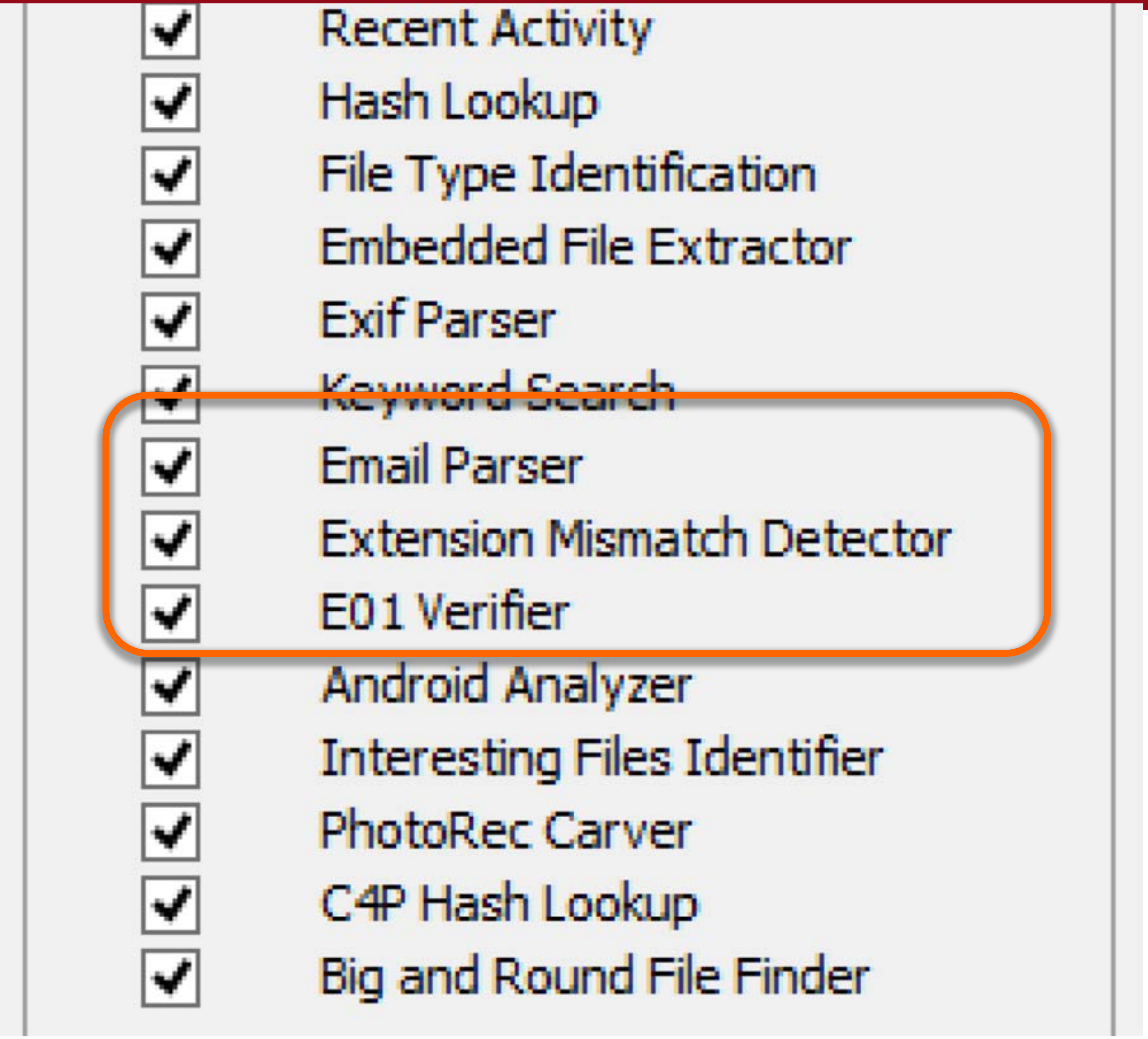


☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Android Analyzer
☑ Interesting Files Identifier
☑ PhotoRec Carver
☑ C4P Hash Lookup
☑ Big and Round File Finder

Keyword Search

- Indexed search using Solr.
- Performs periodic searches.
- Supports terms and regular expressions.

Standard Features



- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round File Finder

Email Parser

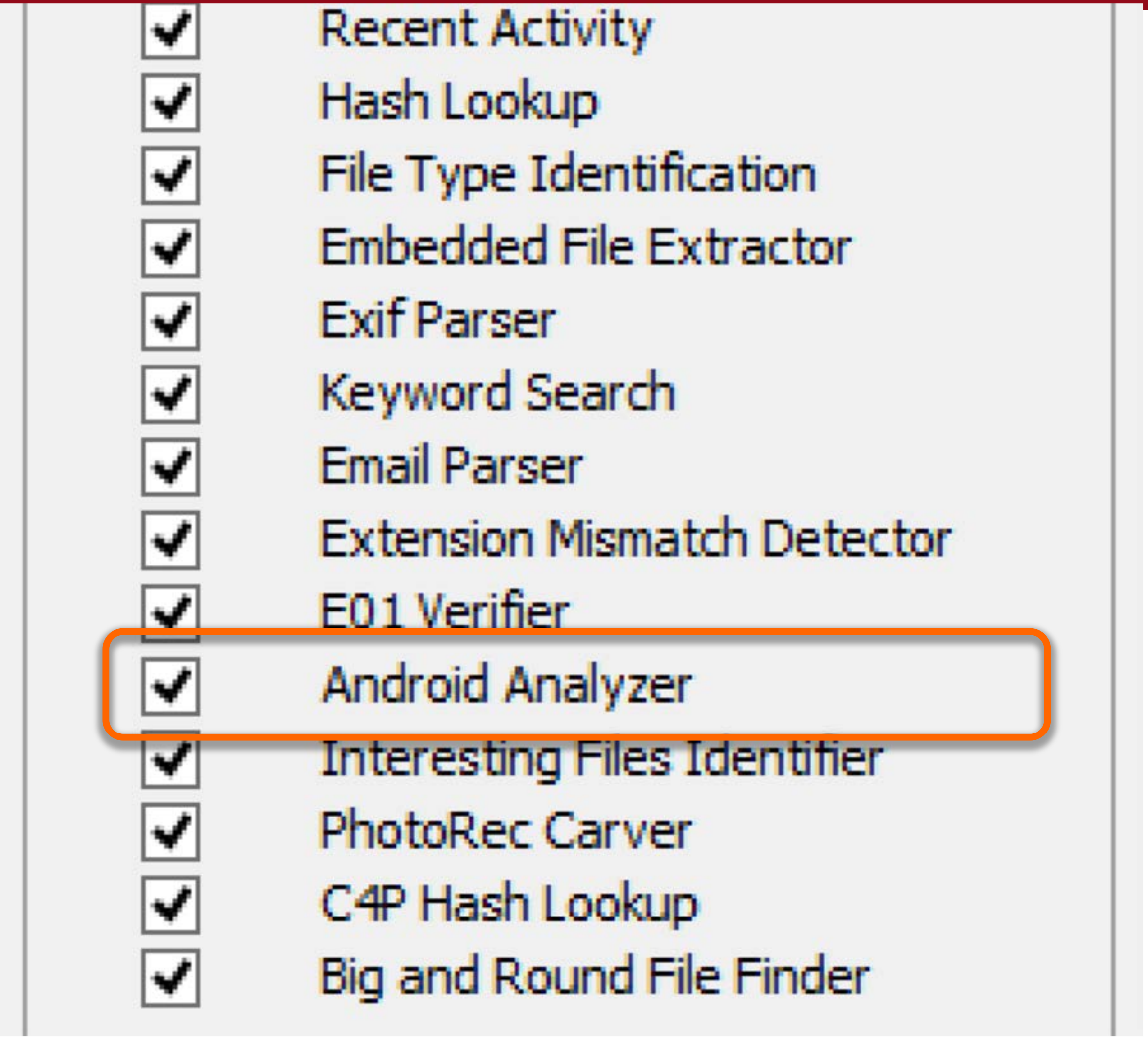
- Supports MBOX and PST.

Extension Mismatch

- Users can specify rules

E01 Verifier

Standard Features

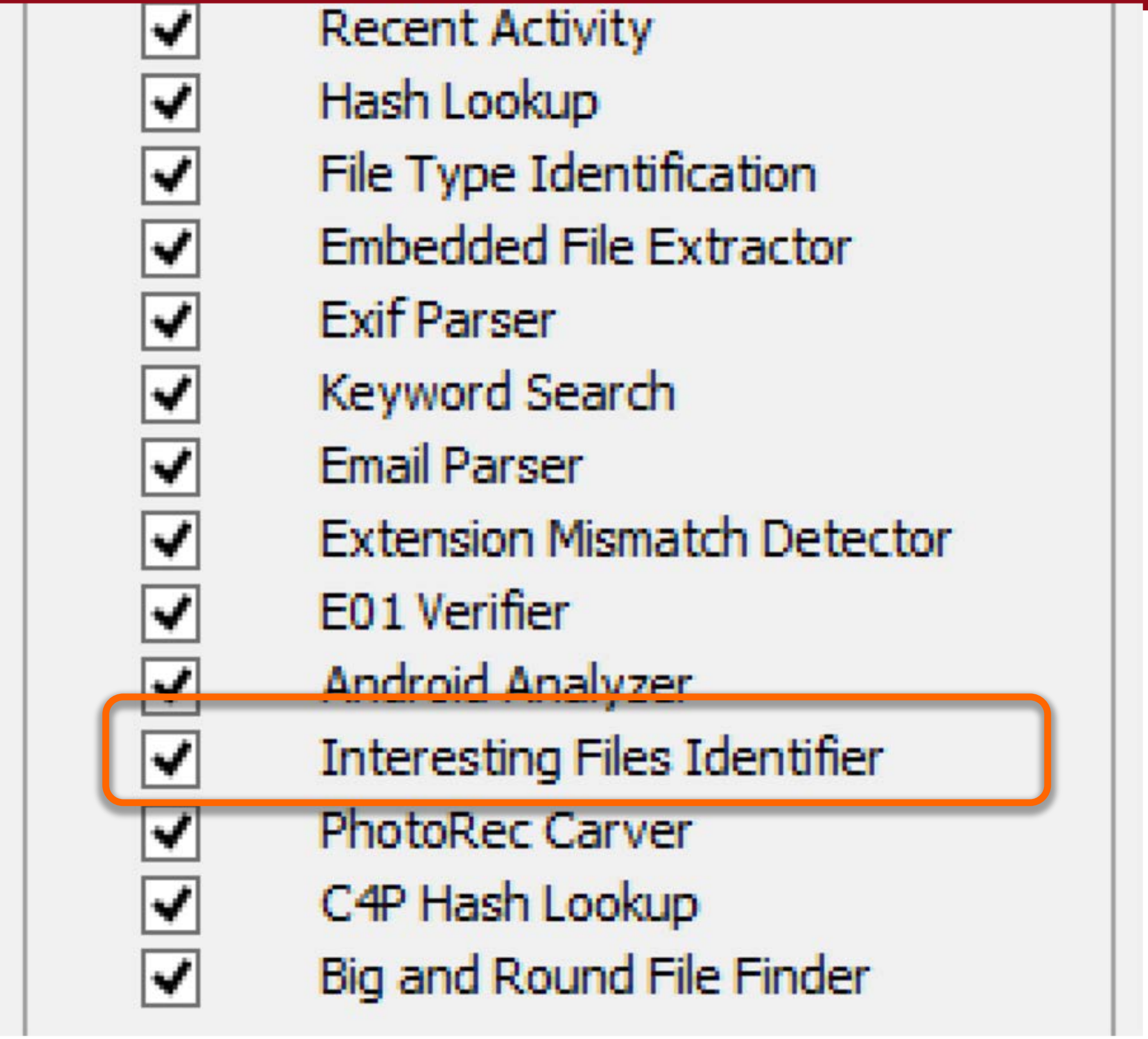


☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Android Analyzer
☑ Interesting Files Identifier
☑ PhotoRec Carver
☑ C4P Hash Lookup
☑ Big and Round File Finder

Android Analyzer

- SMS, Call logs, Contacts
- Tango
- Words With Friends
- ...

Standard Features

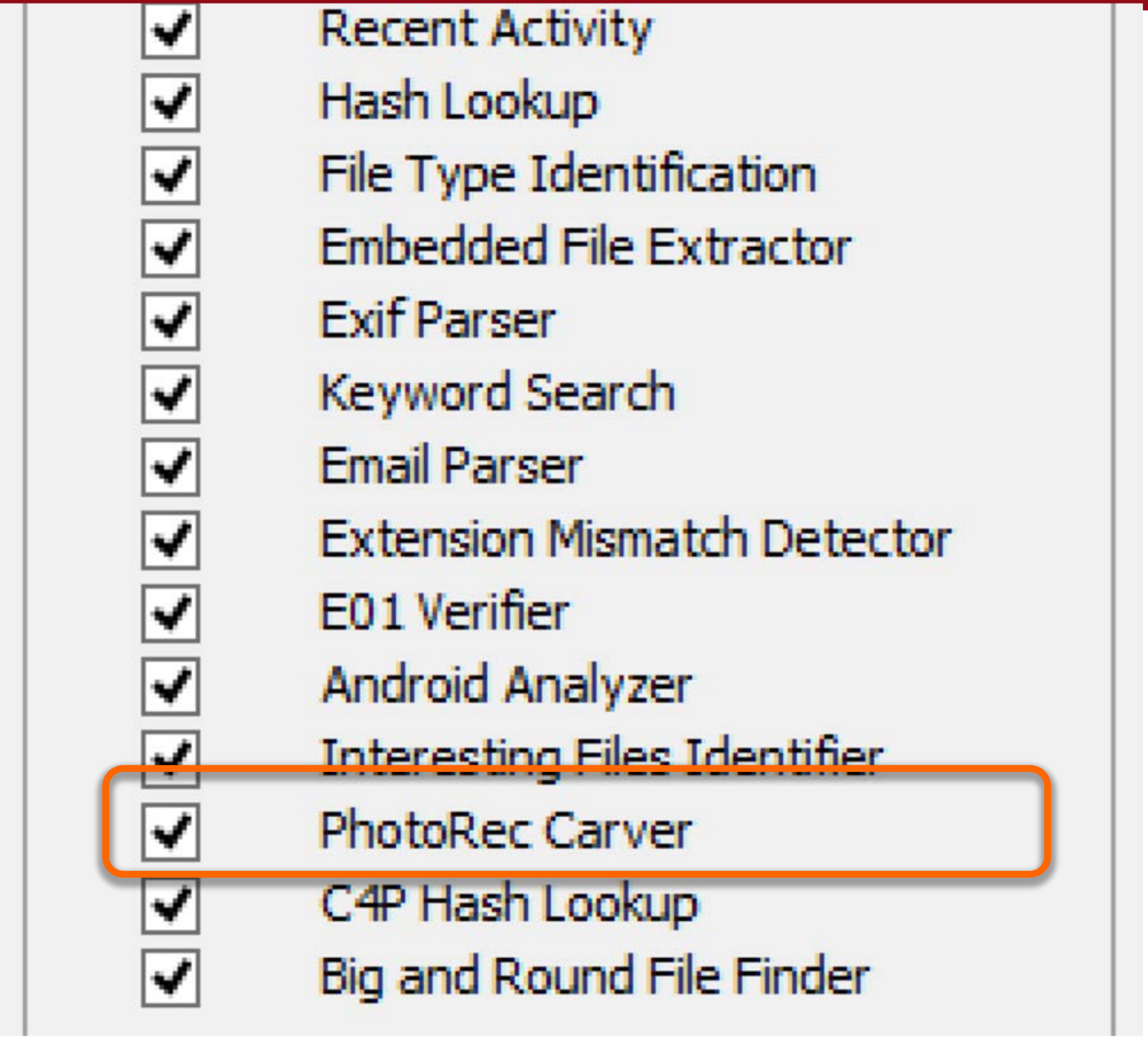


- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round File Finder

Interesting Files Module

- Flags files based on name.
- Allows you to automate your investigation checklist.
- Always look for:
  - iPhone Backup files
  - True Crypt
  - Virtual machines
  - …

Standard Features

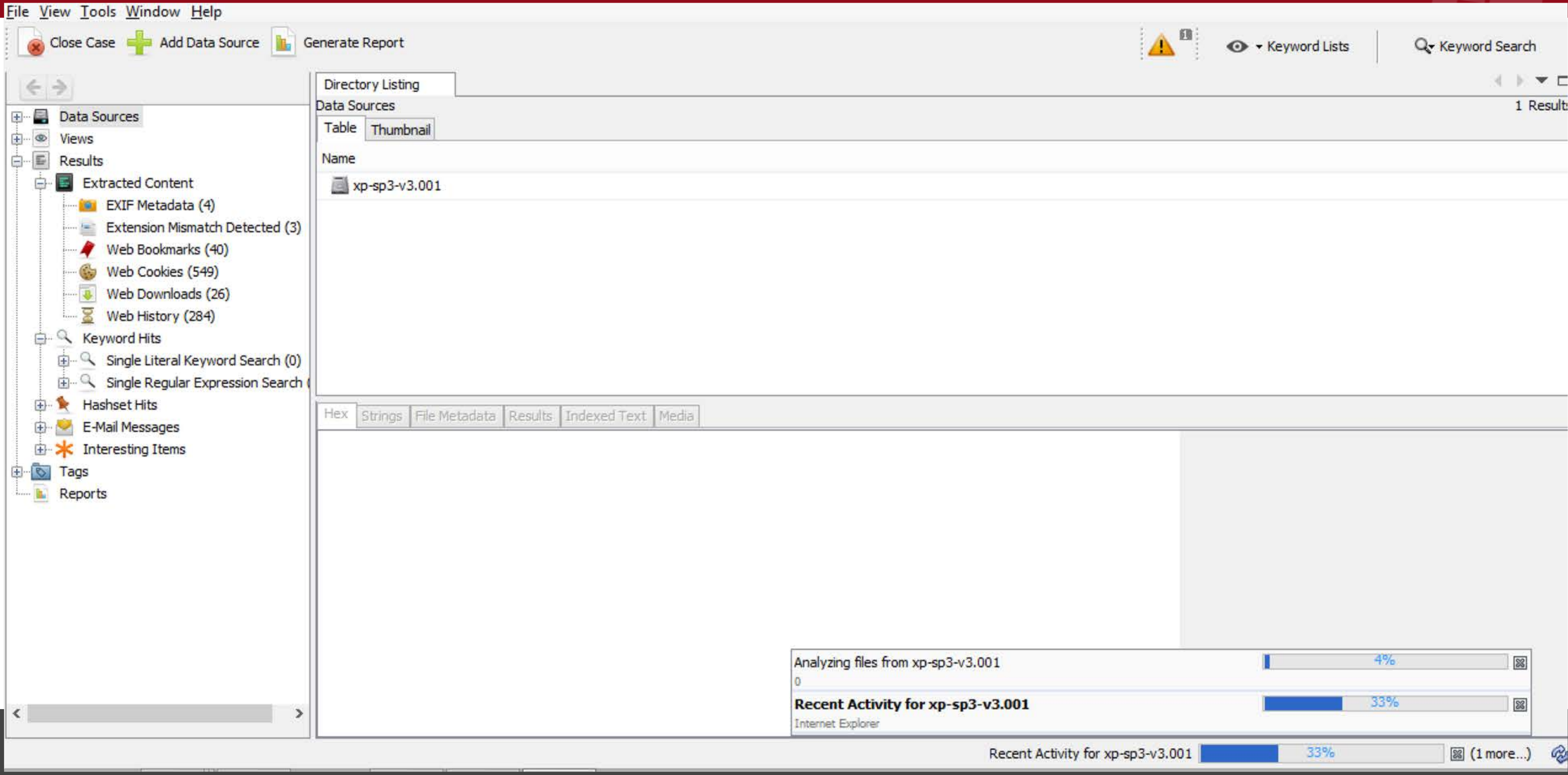


- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round File Finder

PhotoRec Carver

- Uses PhotoRec tool to carve unallocated space.
- Files are fed back through.

Review the Results During Analysis

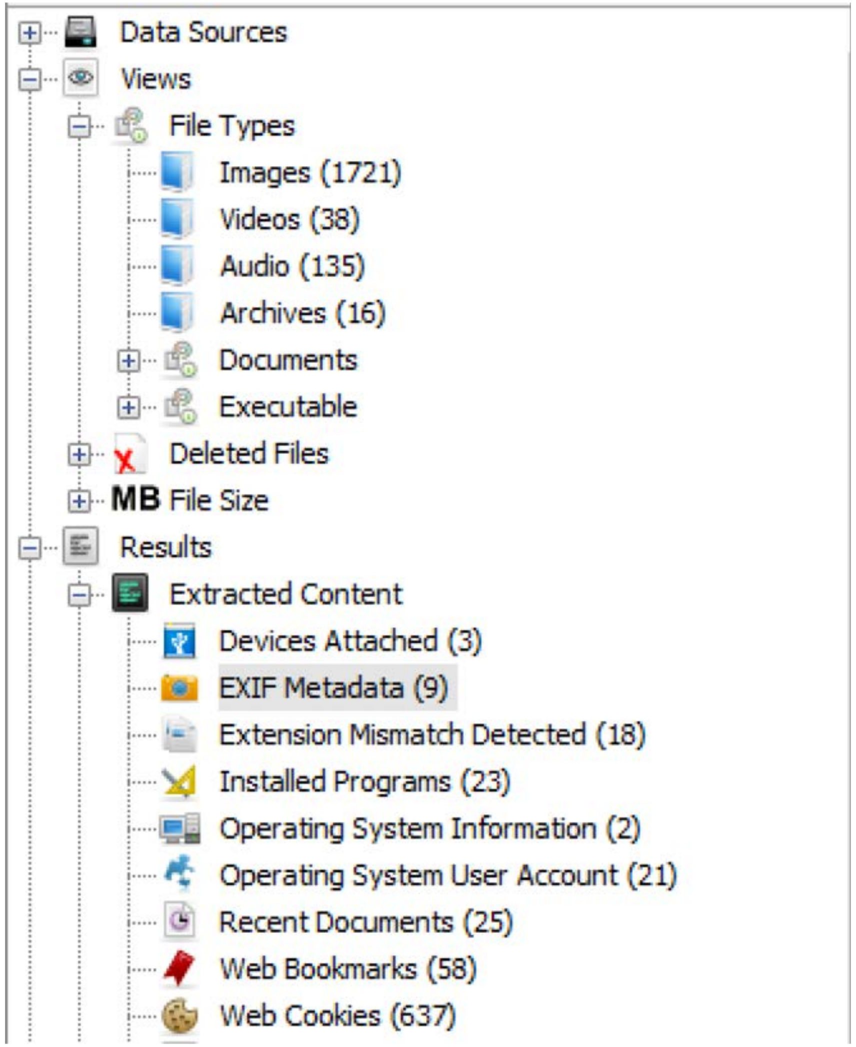


Analyzing files from xp-sp3-v3.001 4%
0

Recent Activity for xp-sp3-v3.001 33%
Internet Explorer

Recent Activity for xp-sp3-v3.001 33% (1 more...)

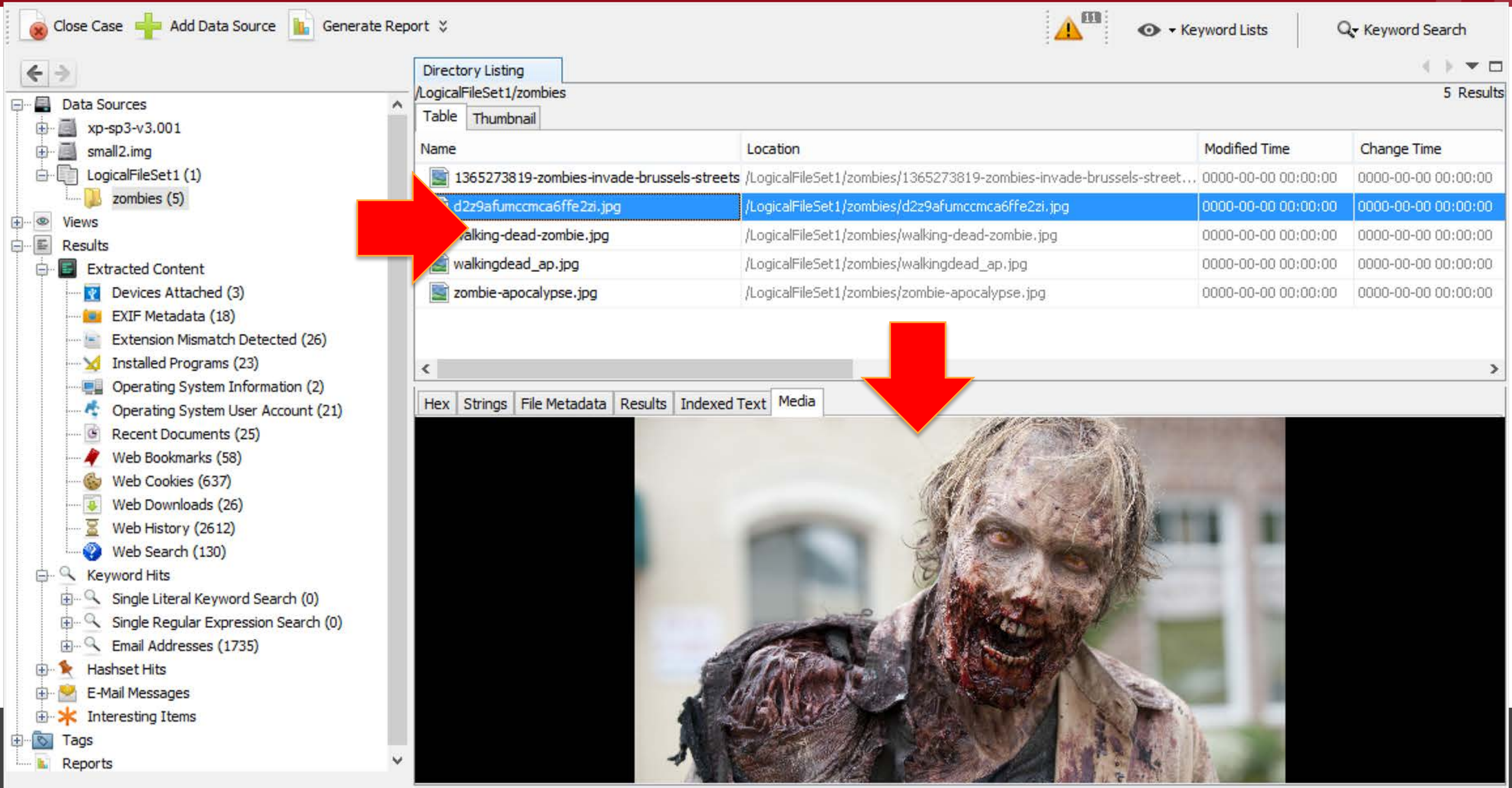
The Tree



- Data Sources
- Views
  - File Types
    - Images (1721)
    - Videos (38)
    - Audio (135)
    - Archives (16)
    - Documents
    - Executable
  - Deleted Files
  - MB File Size
- Results
  - Extracted Content
    - Devices Attached (3)
    - EXIF Metadata (9)
    - Extension Mismatch Detected (18)
    - Installed Programs (23)
    - Operating System Information (2)
    - Operating System User Account (21)
    - Recent Documents (25)
    - Web Bookmarks (58)
    - Web Cookies (637)

- The tree has all of the results.
- Updated in real-time.
- Find:
  - Files of a given type
  - Web artifacts
  - Registry results
  - ….

Workflow



- Data Sources
  - xp-sp3-v3.001
  - small2.img
  - LogicalFileSet1 (1)
    - zombies (5)
- Views
- Results
  - Extracted Content
    - Devices Attached (3)
    - EXIF Metadata (18)
    - Extension Mismatch Detected (26)
    - Installed Programs (23)
    - Operating System Information (2)
    - Operating System User Account (21)
    - Recent Documents (25)
    - Web Bookmarks (58)
    - Web Cookies (637)
    - Web Downloads (26)
    - Web History (2612)
    - Web Search (130)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (1735)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
- Tags
- Reports

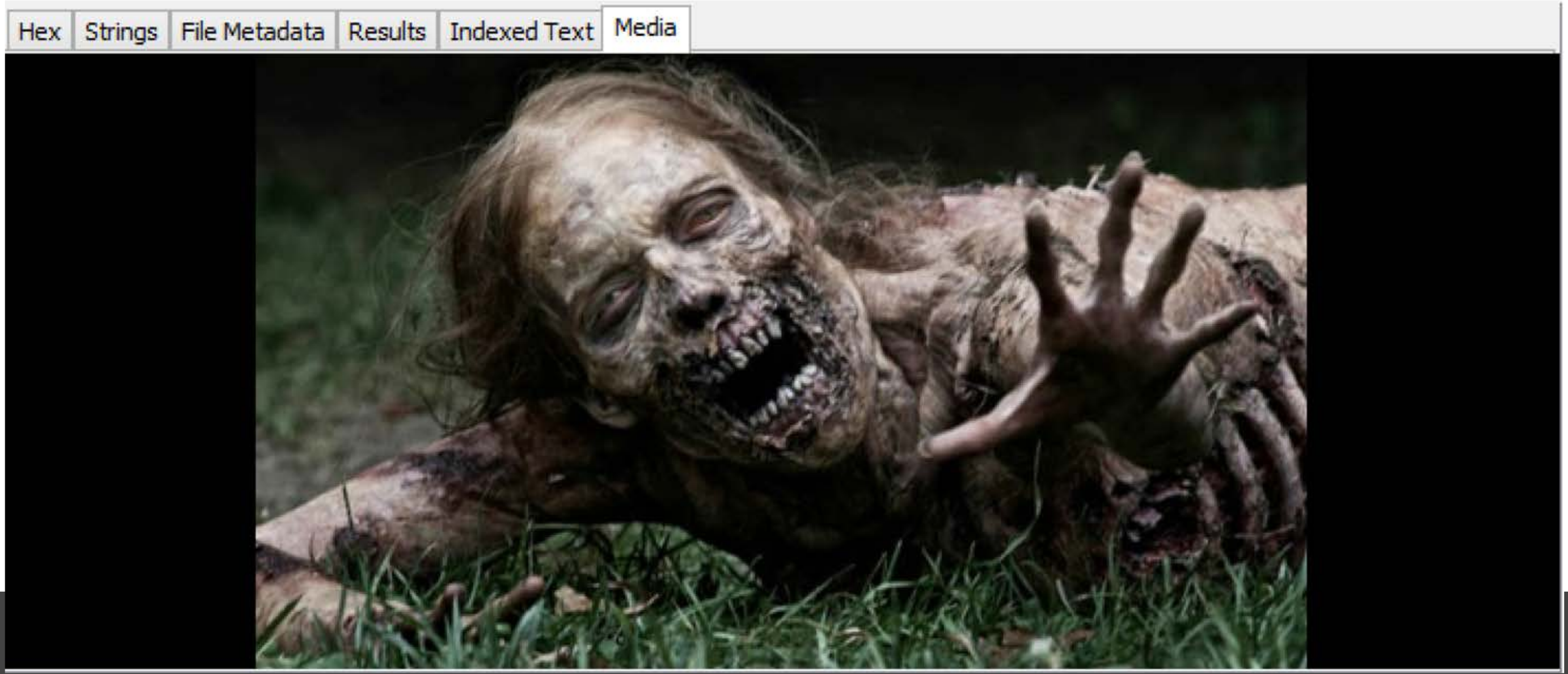
/LogicalFileSet1/zombies

5 Results

Name	Location	Modified Time	Change Time
1365273819-zombies-invade-brussels-streets	/LogicalFileSet1/zombies/1365273819-zombies-invade-brussels-street…	0000-00-00 00:00:00	0000-00-00 00:00:00
d2z9afumccmca6ffe2zi.jpg	/LogicalFileSet1/zombies/d2z9afumccmca6ffe2zi.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00
alking-dead-zombie.jpg	/LogicalFileSet1/zombies/walking-dead-zombie.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00
walkingdead_ap.jpg	/LogicalFileSet1/zombies/walkingdead_ap.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00
zombie-apocalypse.jpg	/LogicalFileSet1/zombies/zombie-apocalypse.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00

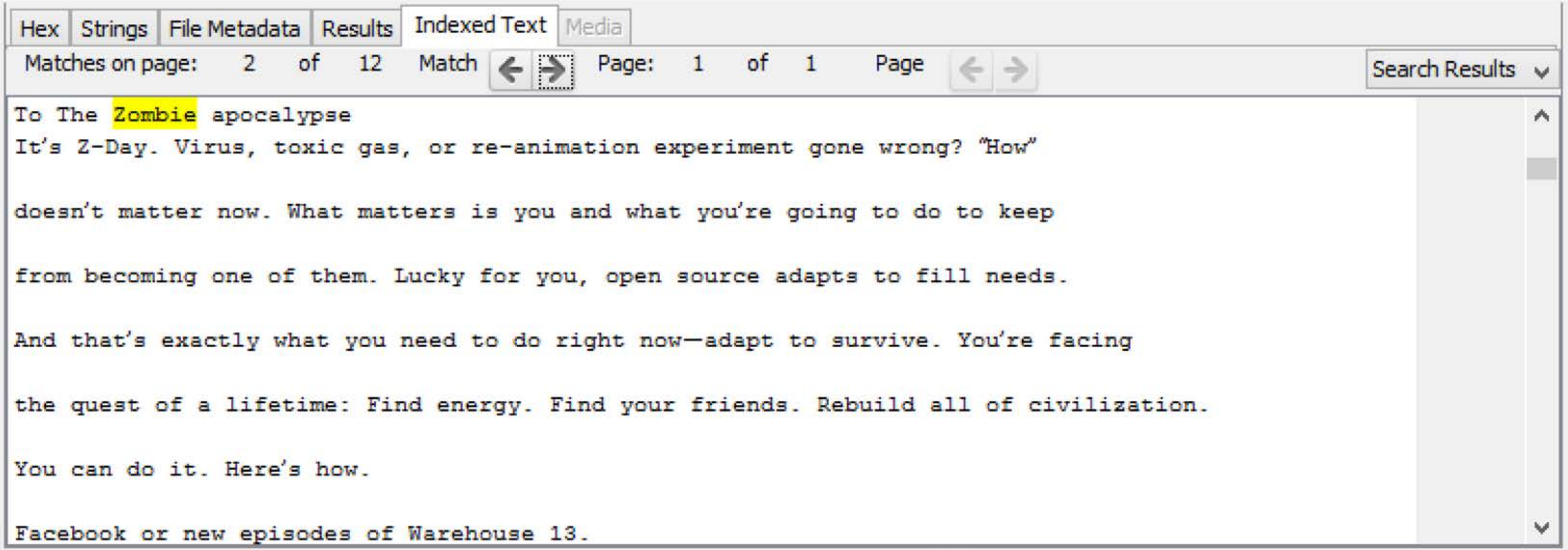
File Viewers

- View a file in the most relevant way.
- Images and video playback.



File Viewers

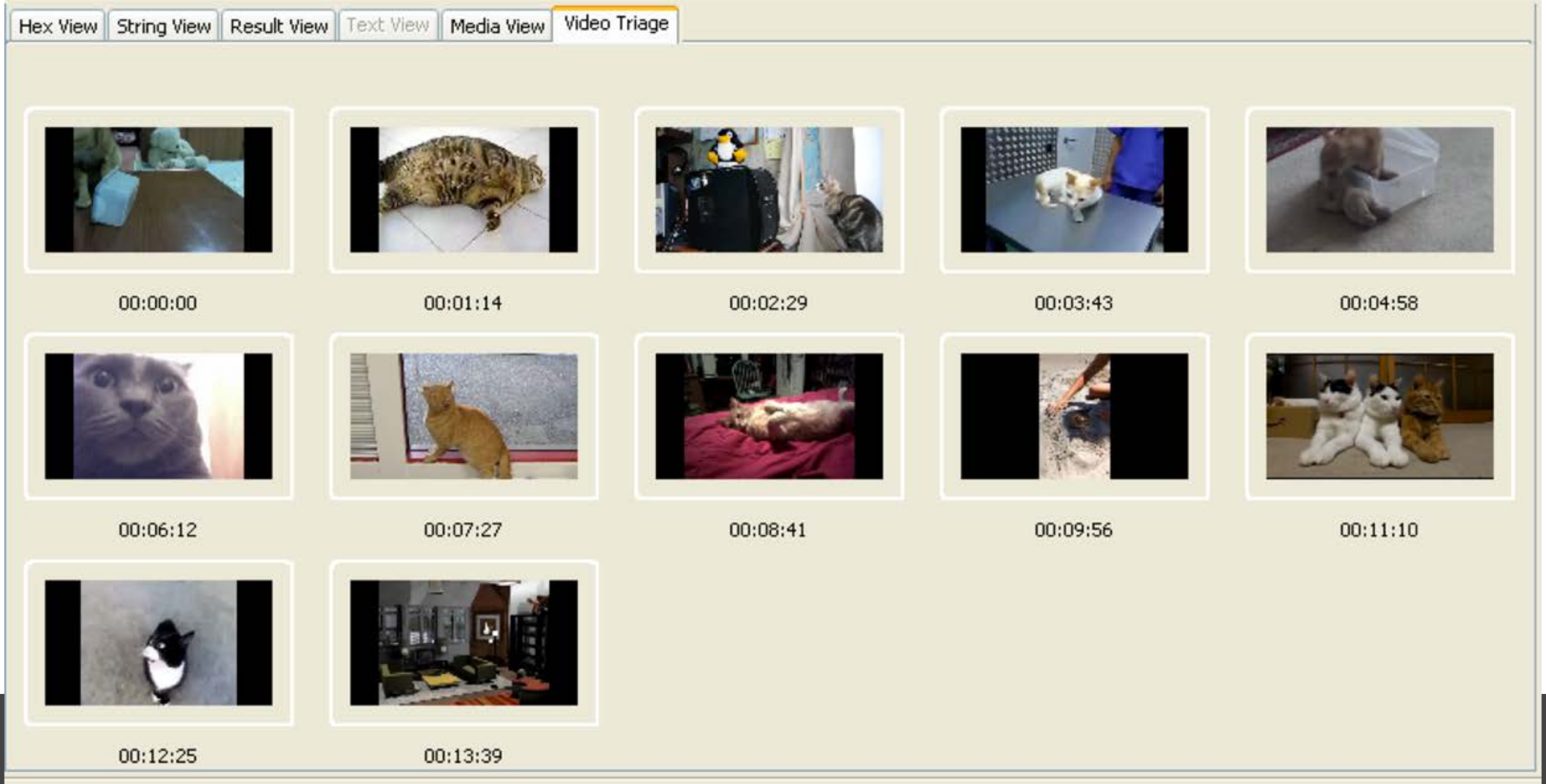
- View a file in the most relevant way.
- Text:



```
To The Zombie apocalypse
It's Z-Day. Virus, toxic gas, or re-animation experiment gone wrong? "How"

doesn't matter now. What matters is you and what you're going to do to keep

from becoming one of them. Lucky for you, open source adapts to fill needs.

And that's exactly what you need to do right now—adapt to survive. You're facing

the quest of a lifetime: Find energy. Find your friends. Rebuild all of civilization.

You can do it. Here's how.

Facebook or new episodes of Warehouse 13.
```

File Viewers

- View a file in the most relevant way.
- Long video as sequence of frames:



Unique Features

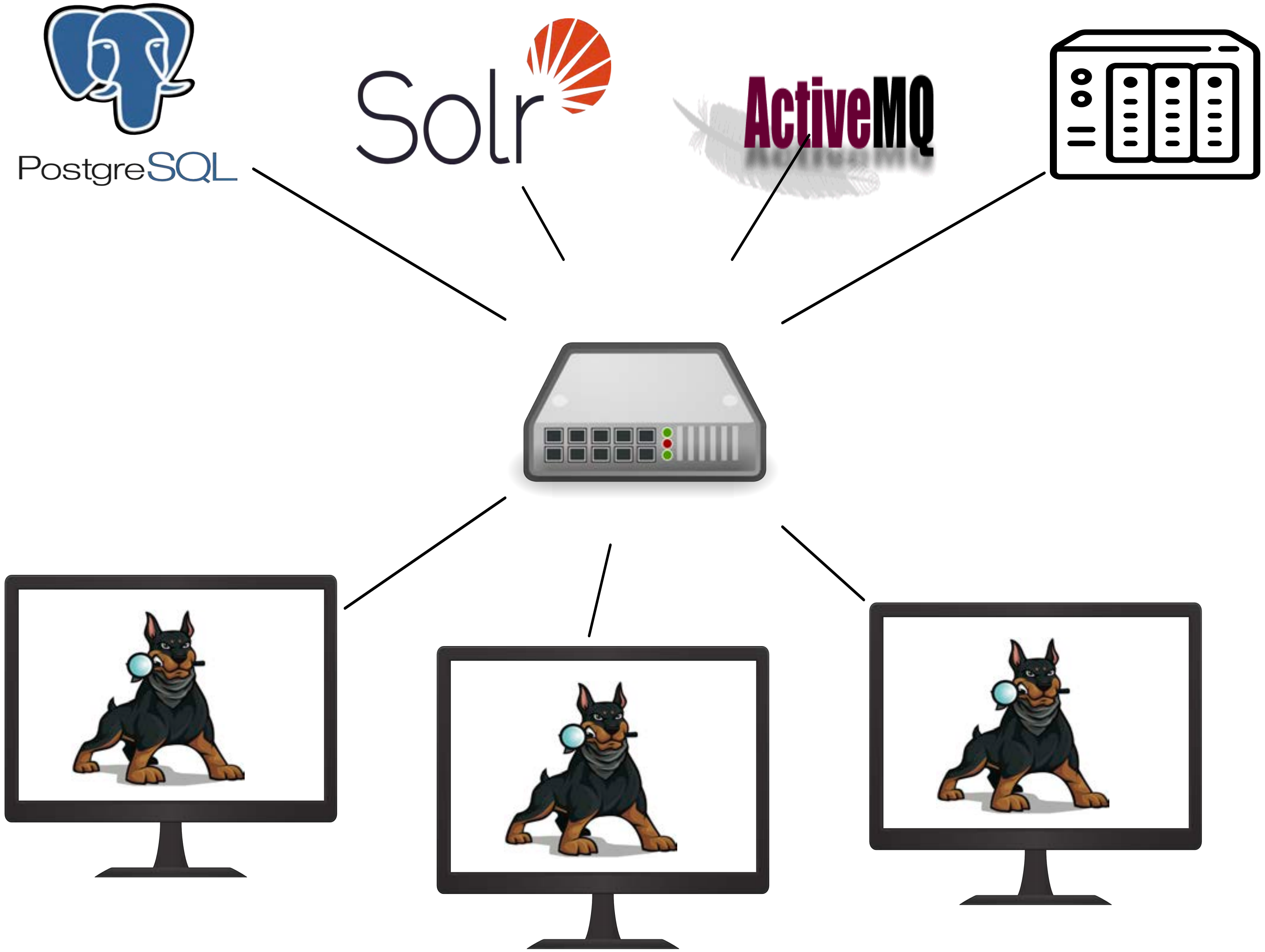
Triage

- User folders are analyzed first.
- Ingest filters allow you to focus on only certain file types and folders.
- A sparse VHD image can be created during analysis if you are reading from the raw device.
- Can run from USB or a booted OS.

Multi-User Cases

- Examiners can collaborate on the same case at the same time.
- Central database, text index, and storage.
- Users can see each others tags and generate single reports on big cases.
- Automatically analyze media 24x7.

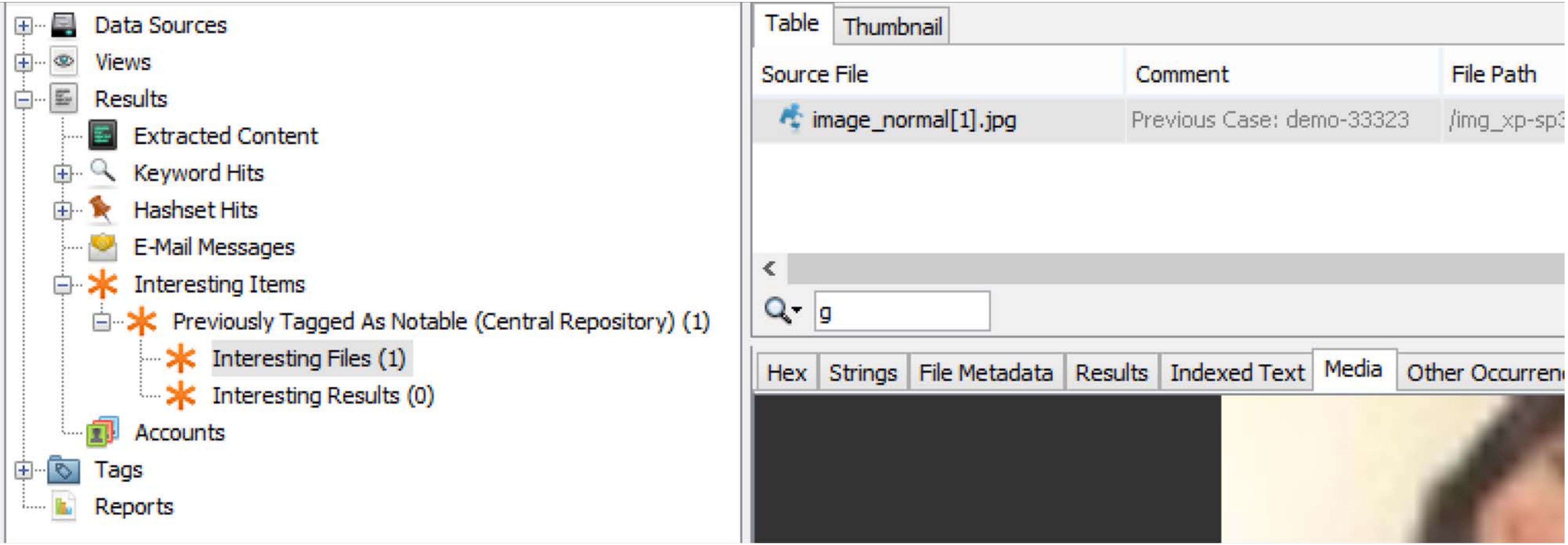
Multi-User Cases



Past Case Correlation

- The Central Repository database stores:
  - When each MD5, email, etc. has been seen
  - What files and attributes were tagged as notable
- You can make connections with past cases that had common files or phone numbers.
- When a previously notable item is seen again, it is automatically flagged.

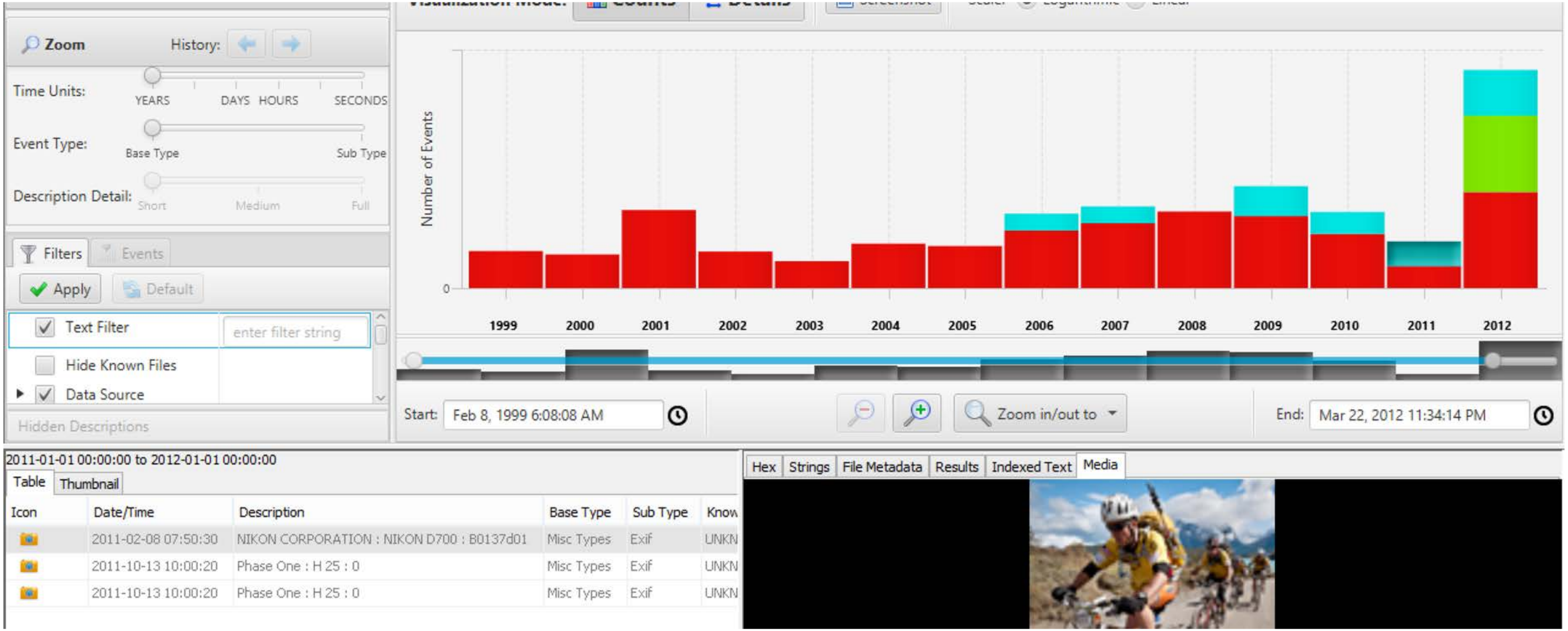
Past Case Correlation



Source File	Comment	File Path
image_normal[1].jpg	Previous Case: demo-33323	/img_xp-sp3

g

Timeline



Time Units: YEARS DAYS HOURS SECONDS

Event Type: Base Type Sub Type

Description Detail: Short Medium Full

☑ Text Filter enter filter string

□ Hide Known Files

☑ Data Source

Start: Feb 8, 1999 6:08:08 AM

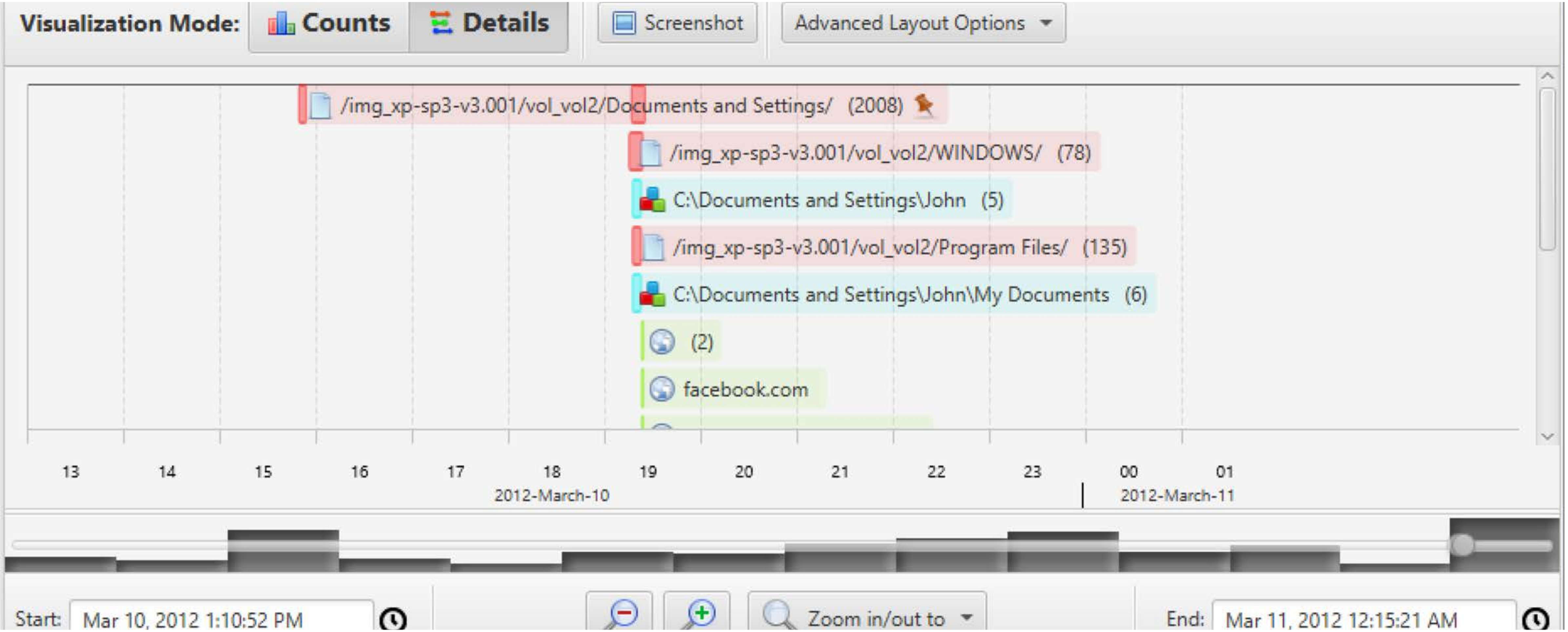
End: Mar 22, 2012 11:34:14 PM

2011-01-01 00:00:00 to 2012-01-01 00:00:00

Table Thumbnail

Icon	Date/Time	Description	Base Type	Sub Type	Know
	2011-02-08 07:50:30	NIKON CORPORATION : NIKON D700 : B0137d01	Misc Types	Exif	UNKN
	2011-10-13 10:00:20	Phase One : H 25 : 0	Misc Types	Exif	UNKN
	2011-10-13 10:00:20	Phase One : H 25 : 0	Misc Types	Exif	UNKN

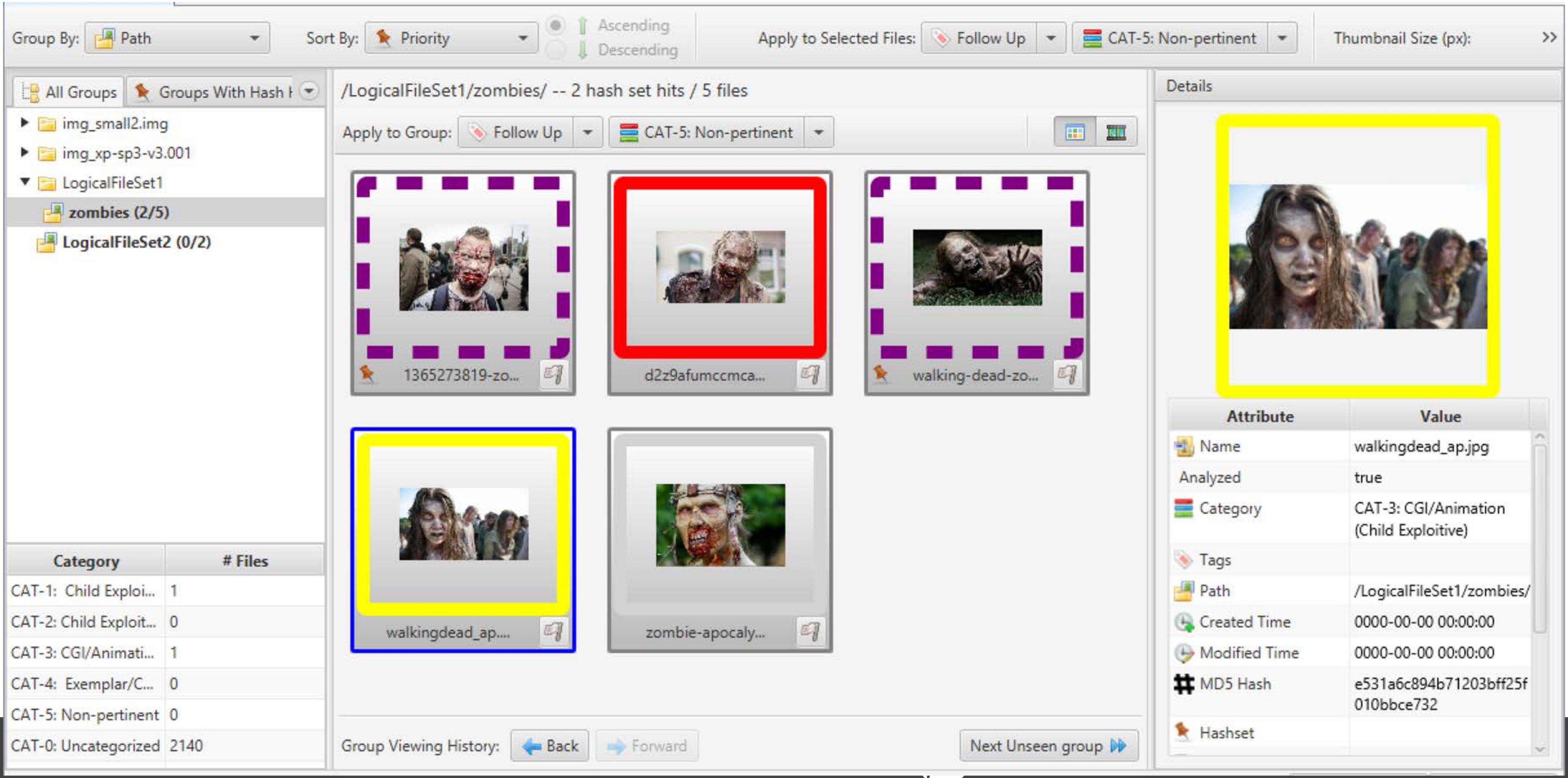
Timeline


Visualization Mode:
Counts
Details
Screenshot
Advanced Layout Options
/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/ (2008)
/img_xp-sp3-v3.001/vol_vol2/WINDOWS/ (78)
C:\Documents and Settings\John (5)
/img_xp-sp3-v3.001/vol_vol2/Program Files/ (135)
C:\Documents and Settings\John\My Documents (6)
(2)
facebook.com
13
14
15
16
17
18
19
20
21
22
23
00
01
2012-March-10
2012-March-11
Zoom in/out to

Start: Mar 10, 2012 1:10:52 PM

End: Mar 11, 2012 12:15:21 AM

Image Gallery



Group By: Path

Sort By: Priority

○ Ascending

○ Descending

Apply to Selected Files: Follow Up | CAT-5: Non-pertinent

Thumbnail Size (px):

All Groups | Groups With Hash I

- img_small2.img
- img_xp-sp3-v3.001
- LogicalFileSet1
  - **zombies (2/5)**
- **LogicalFileSet2 (0/2)**

Category	# Files
CAT-1: Child Exploi...	1
CAT-2: Child Exploit...	0
CAT-3: CGI/Animati...	1
CAT-4: Exemplar/C...	0
CAT-5: Non-pertinent	0
CAT-0: Uncategorized	2140

/LogicalFileSet1/zombies/ -- 2 hash set hits / 5 files

Apply to Group: Follow Up | CAT-5: Non-pertinent

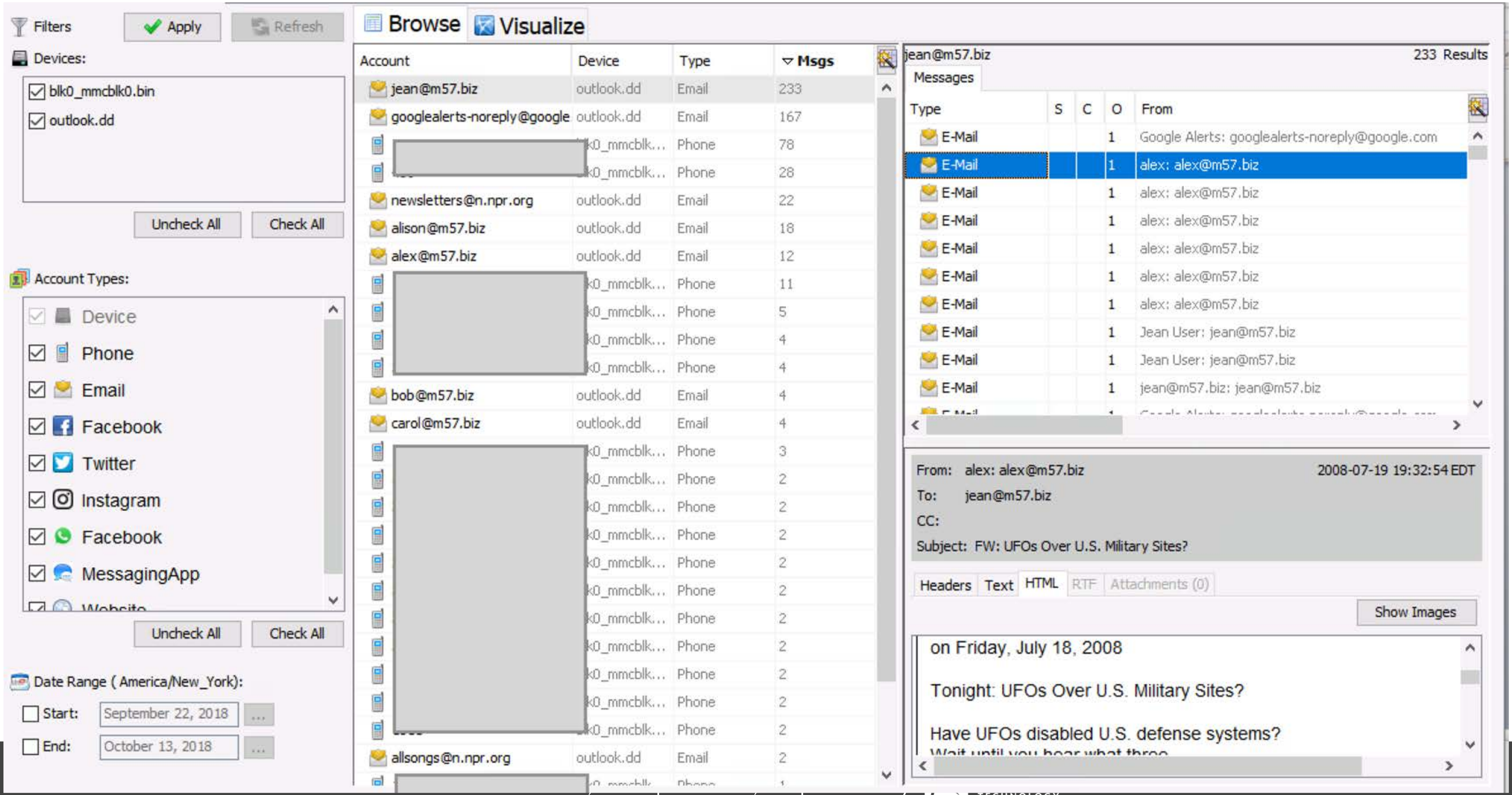
Group Viewing History: Back | Forward

Next Unseen group

Details

Attribute	Value
Name	walkingdead_ap.jpg
Analyzed	true
Category	CAT-3: CGI/Animation (Child Exploitive)
Tags	
Path	/LogicalFileSet1/zombies/
Created Time	0000-00-00 00:00:00
Modified Time	0000-00-00 00:00:00
MD5 Hash	e531a6c894b71203bff25f010bbce732
Hashset	

Communications



Filters ✓ Apply Refresh

Devices:

☑ blk0_mmcblk0.bin
☑ outlook.dd

Uncheck All Check All

Account Types:

☑ Device
☑ Phone
☑ Email
☑ Facebook
☑ Twitter
☑ Instagram
☑ Facebook
☑ MessagingApp
☑ Website

Uncheck All Check All

Date Range (America/New_York):

☐ Start: September 22, 2018
☐ End: October 13, 2018

Browse Visualize

Account	Device	Type	Msgs
jean@m57.biz	outlook.dd	Email	233
googlealerts-noreply@google	outlook.dd	Email	167
[redacted]	k0_mmcblk…	Phone	78
[redacted]	k0_mmcblk…	Phone	28
newsletters@n.npr.org	outlook.dd	Email	22
alison@m57.biz	outlook.dd	Email	18
alex@m57.biz	outlook.dd	Email	12
[redacted]	k0_mmcblk…	Phone	11
[redacted]	k0_mmcblk…	Phone	5
[redacted]	k0_mmcblk…	Phone	4
[redacted]	k0_mmcblk…	Phone	4
bob@m57.biz	outlook.dd	Email	4
carol@m57.biz	outlook.dd	Email	4
[redacted]	k0_mmcblk…	Phone	3
[redacted]	k0_mmcblk…	Phone	2
[redacted]	k0_mmcblk…	Phone	2
[redacted]	k0_mmcblk…	Phone	2
[redacted]	k0_mmcblk…	Phone	2
[redacted]	k0_mmcblk…	Phone	2
[redacted]	k0_mmcblk…	Phone	2
[redacted]	k0_mmcblk…	Phone	2
[redacted]	k0_mmcblk…	Phone	2
[redacted]	k0_mmcblk…	Phone	2
[redacted]	k0_mmcblk…	Phone	2
allsongs@n.npr.org	outlook.dd	Email	2
[redacted]	k0_mmcblk…	Phone	1

jean@m57.biz 233 Results

Messages

Type	S	C	O	From
E-Mail			1	Google Alerts: googlealerts-noreply@google.com
E-Mail			1	alex: alex@m57.biz
E-Mail			1	alex: alex@m57.biz
E-Mail			1	alex: alex@m57.biz
E-Mail			1	alex: alex@m57.biz
E-Mail			1	alex: alex@m57.biz
E-Mail			1	alex: alex@m57.biz
E-Mail			1	Jean User: jean@m57.biz
E-Mail			1	Jean User: jean@m57.biz
E-Mail			1	jean@m57.biz: jean@m57.biz

From: alex: alex@m57.biz 2008-07-19 19:32:54 EDT
To: jean@m57.biz
CC:
Subject: FW: UFOs Over U.S. Military Sites?

Headers Text HTML RTF Attachments (0)

Show Images

on Friday, July 18, 2008

Tonight: UFOs Over U.S. Military Sites?

Have UFOs disabled U.S. defense systems?

Python Modules

- It’s “easy” to write your own ingest modules in Python.
- Autopsy takes care of:
  - **Input Types:** File systems, image formats, logical files, ZIP file contents, file carving, etc.
  - **User Interaction:** interfaces, reports, etc.
- You just need to focus on finding the files and parsing them.
- We have tutorials and sample files to copy.

What Can You Do?

- To Learn More:
  - Attend the other sessions this afternoon
  - Attend a 1-day Training course
  - Try it out!
- Can try the standalone first:
  - Use it for validation.

Support

- Community:
  - Email list
  - Forum.sleuthkit.org
  - Github Issues
- Basis Technology:
  - Commercial support
  - Access to engineers who can fix any issues.

Questions?

brianc <at> basistech.com

Connect on LinkedIn