6th Annual

#OSDFCon

OPEN SOURCE DIGITAL FORENSICS CONFERENCE

BASIS TECHNOLOGY

# Autopsy: Wait, there are still more features?

Brian Carrier

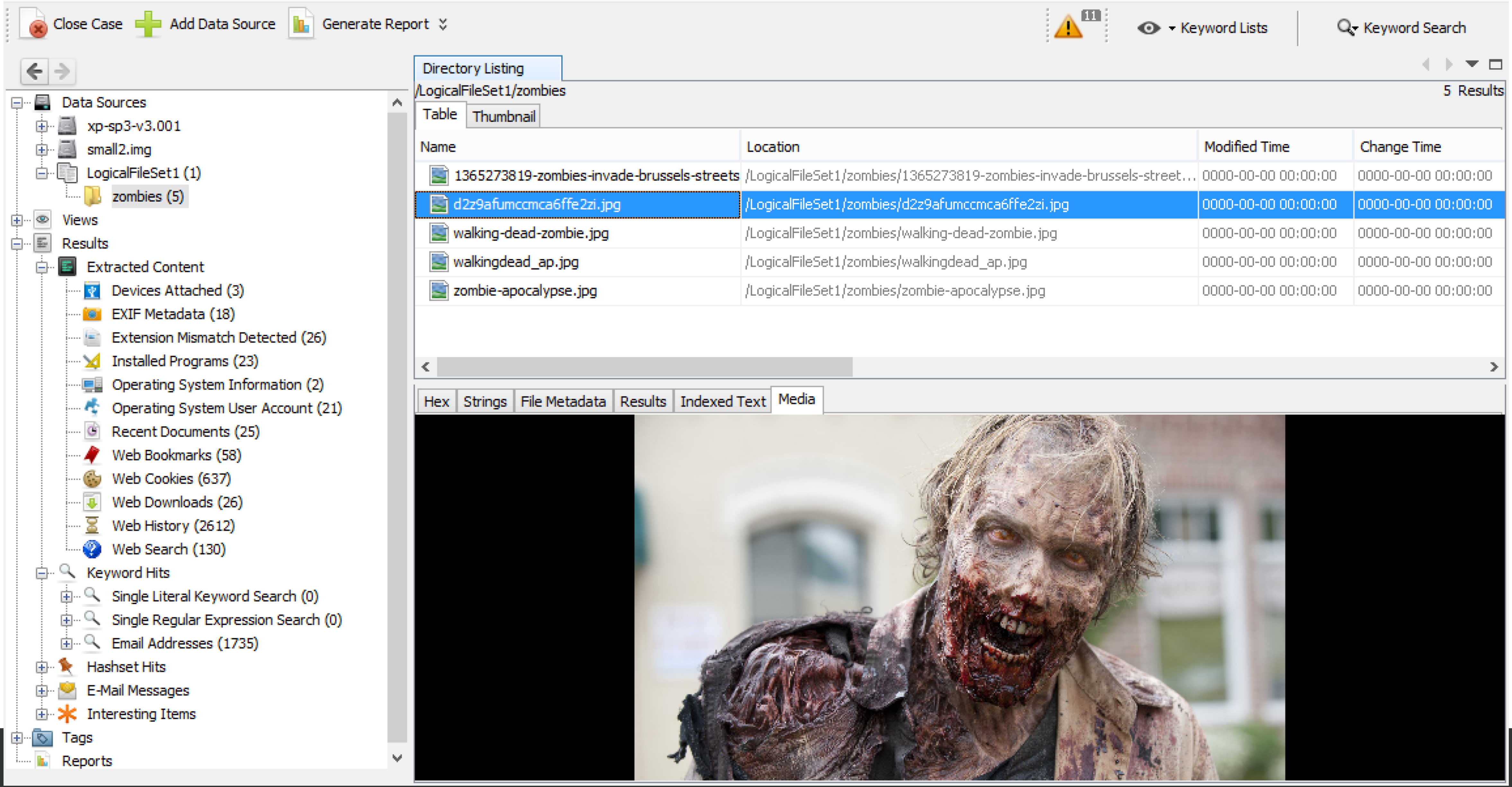
Basis Technology

October 28, 2015 | Westin Washington Dulles, Herndon, VA

# What is Autopsy?

- Open source digital forensics platform.
- Has been designed for:
    - Ease of use
    - Fast results
    - Extensibility (many plug-in frameworks)

# 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 |

# Why Should You Care?

- Has the features you need (and more).
- Will reduce your licensing costs.
- Will reduce errors because:
  - It is easy to use
  - Can automate your investigations
- Has commercial support and development backing.

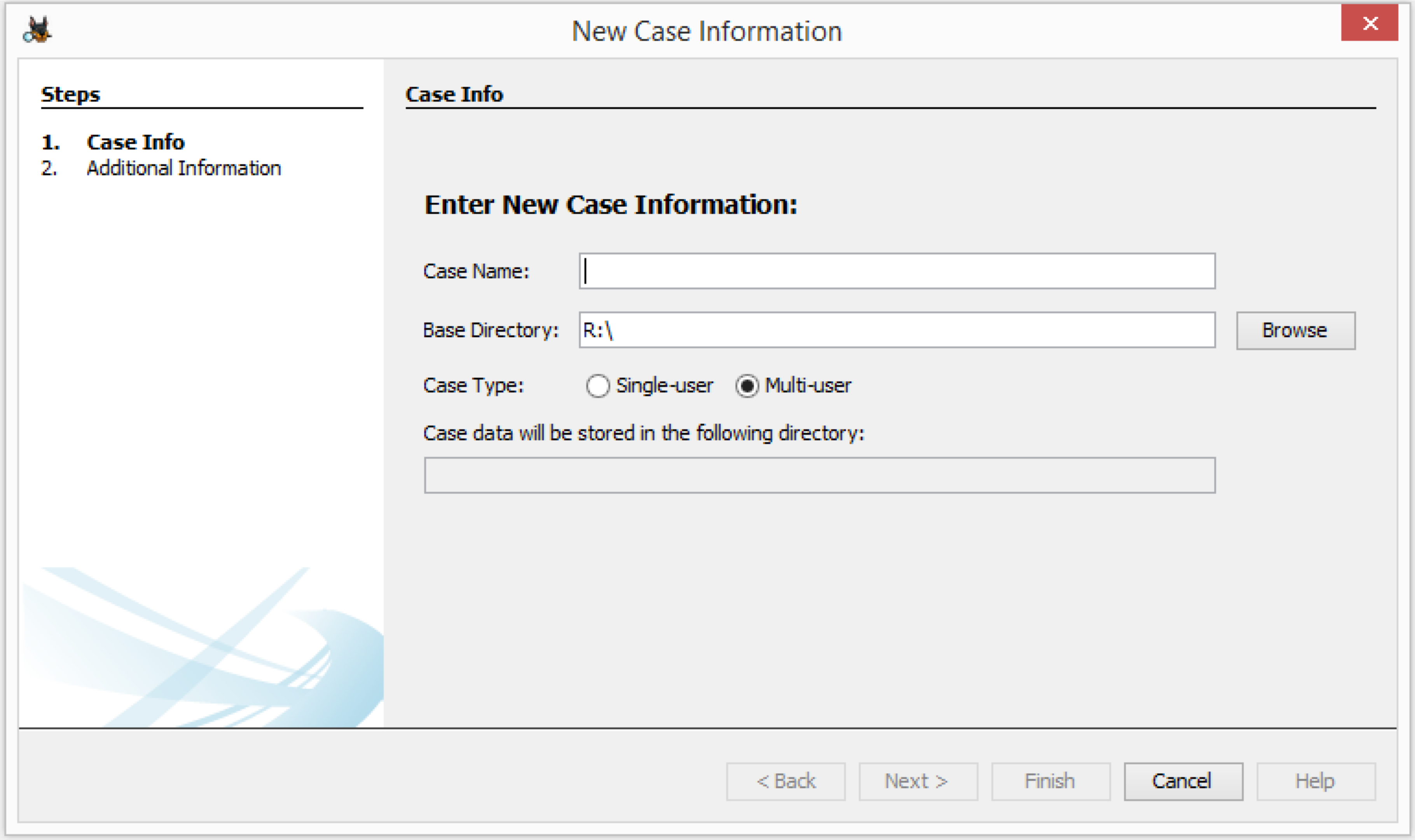
# Summary of Past Year

- 3 Releases.
  - Version 4.0 released next week.
- New Features:
  - Multi-user cases
  - New modules
  - Lots of improvements to existing features.

# Autopsy Tour

## With Highlights of New Features

# New Case Wizard



New Case Information

**Steps**

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

**Case Info**

**Enter New Case Information:**

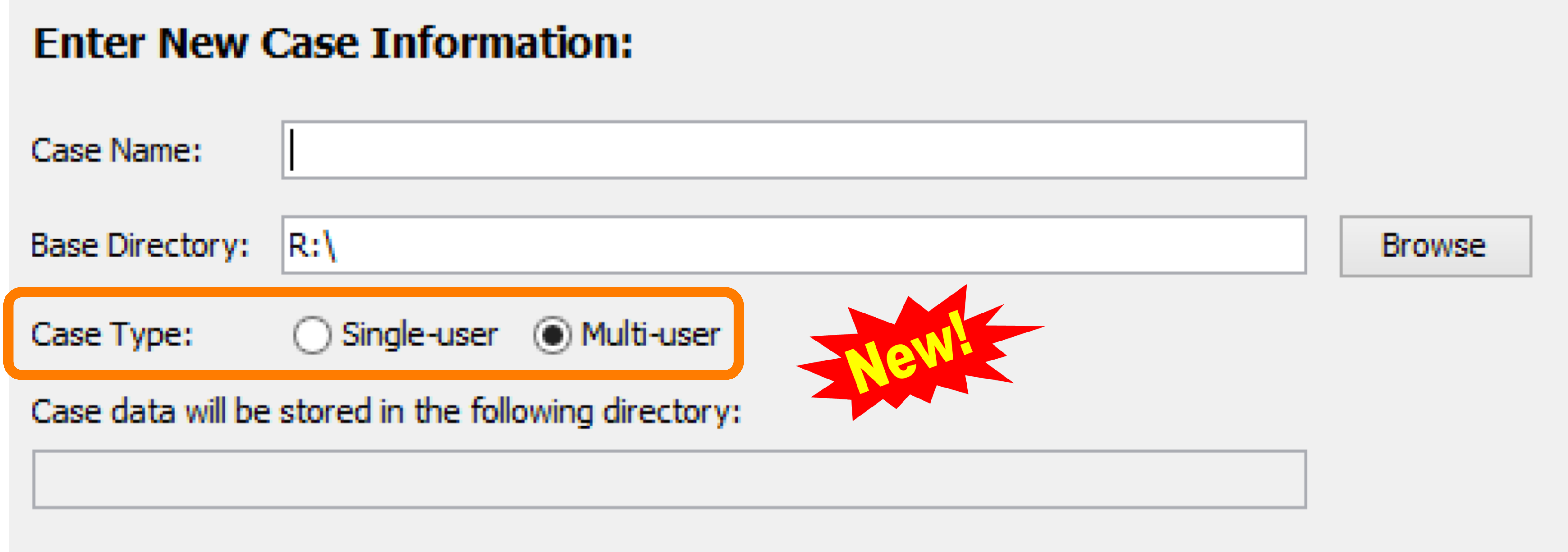
Case Name:

Base Directory: R:\

Case Type: ○ Single-user ● Multi-user

Case data will be stored in the following directory:

# New Case Wizard: What’s New



**Enter New Case Information:**

Case Name:

Base Directory: R:\

Case Type: ○ Single-user ● Multi-user

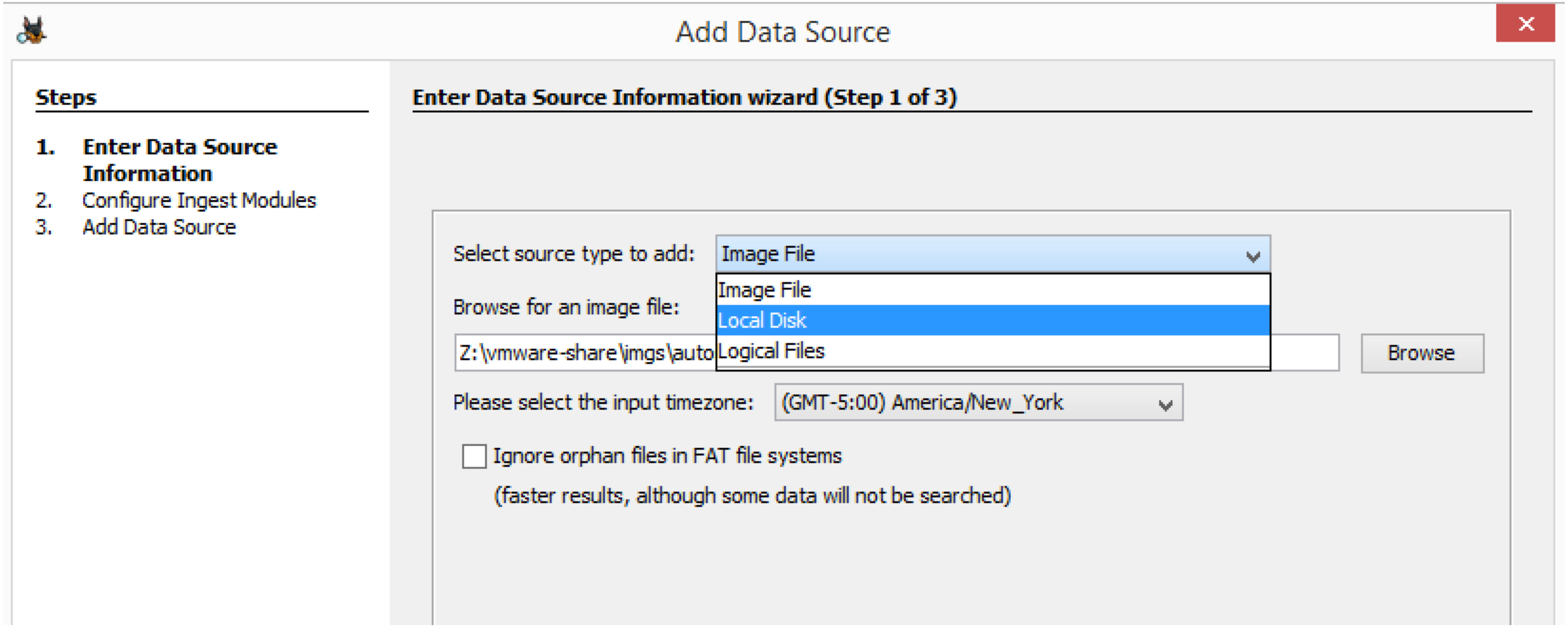
New!

Case data will be stored in the following directory:

# Multi-User Cases

- Analyze large cases faster by enabling collaboration.
  - Multiple users can work on the same case at the same time.
  - Real-time updates from each user.
- All infrastructure software is free and open source:
  - Database server: PostgreSQL
  - Text index server: Apache Solr
  - Messaging server: ActiveMQ
- See Richard’s talk after lunch for more details.

# Add Data Source Wizard



**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

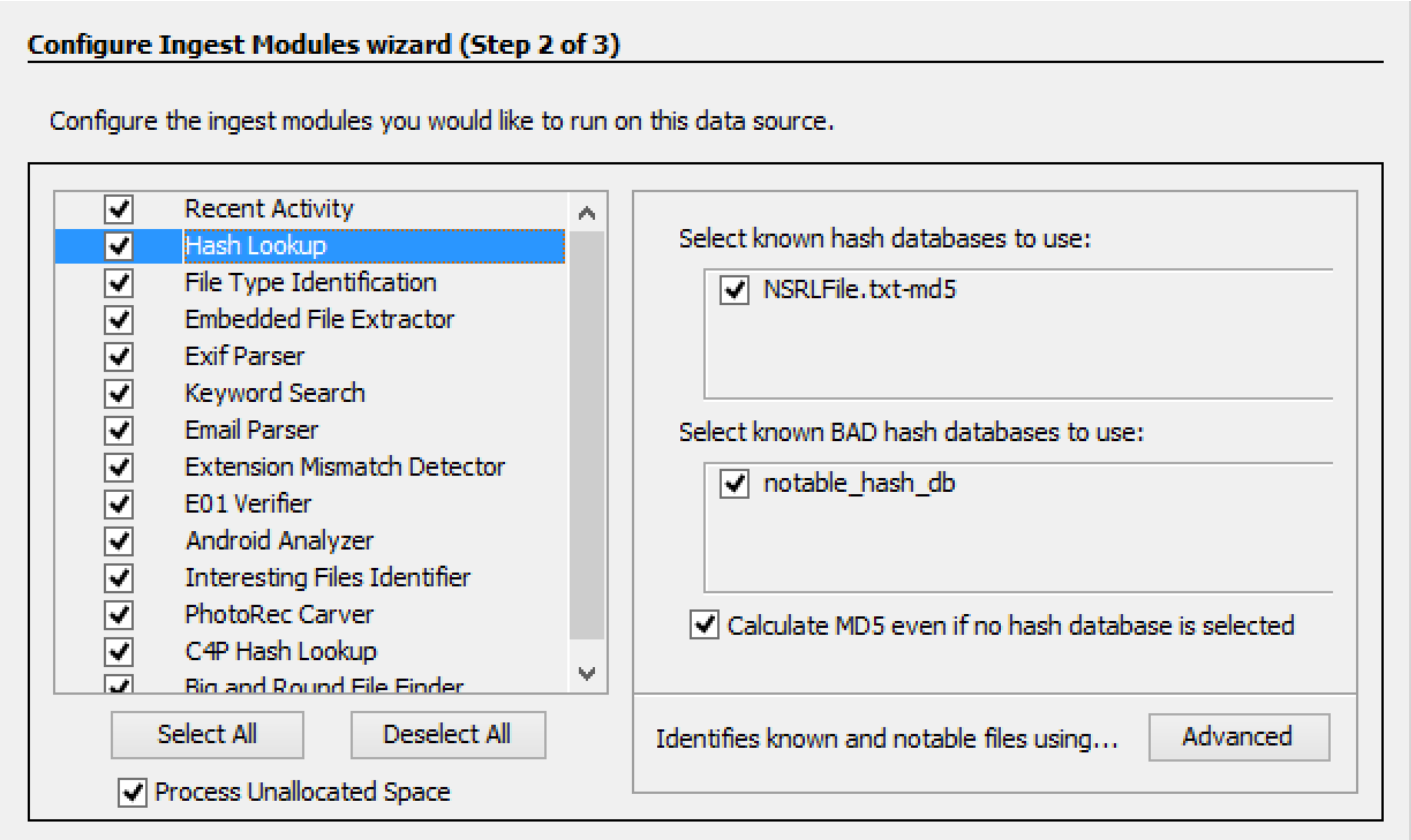
(faster results, although some data will not be searched)

# Data Source Support

- The Sleuth Kit is used to support all common file systems:
  - NTFS, FAT, ExFAT, HFS+, Ext2/Ext3/Ext4, etc.
  - Covers common computers and smart phones
- Can also analyze:
  - Local drives (USB attached)
  - Local files
- What's New: Bug fixes to underlying code in The Sleuth Kit

New!

# Configure Ingest Modules



**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

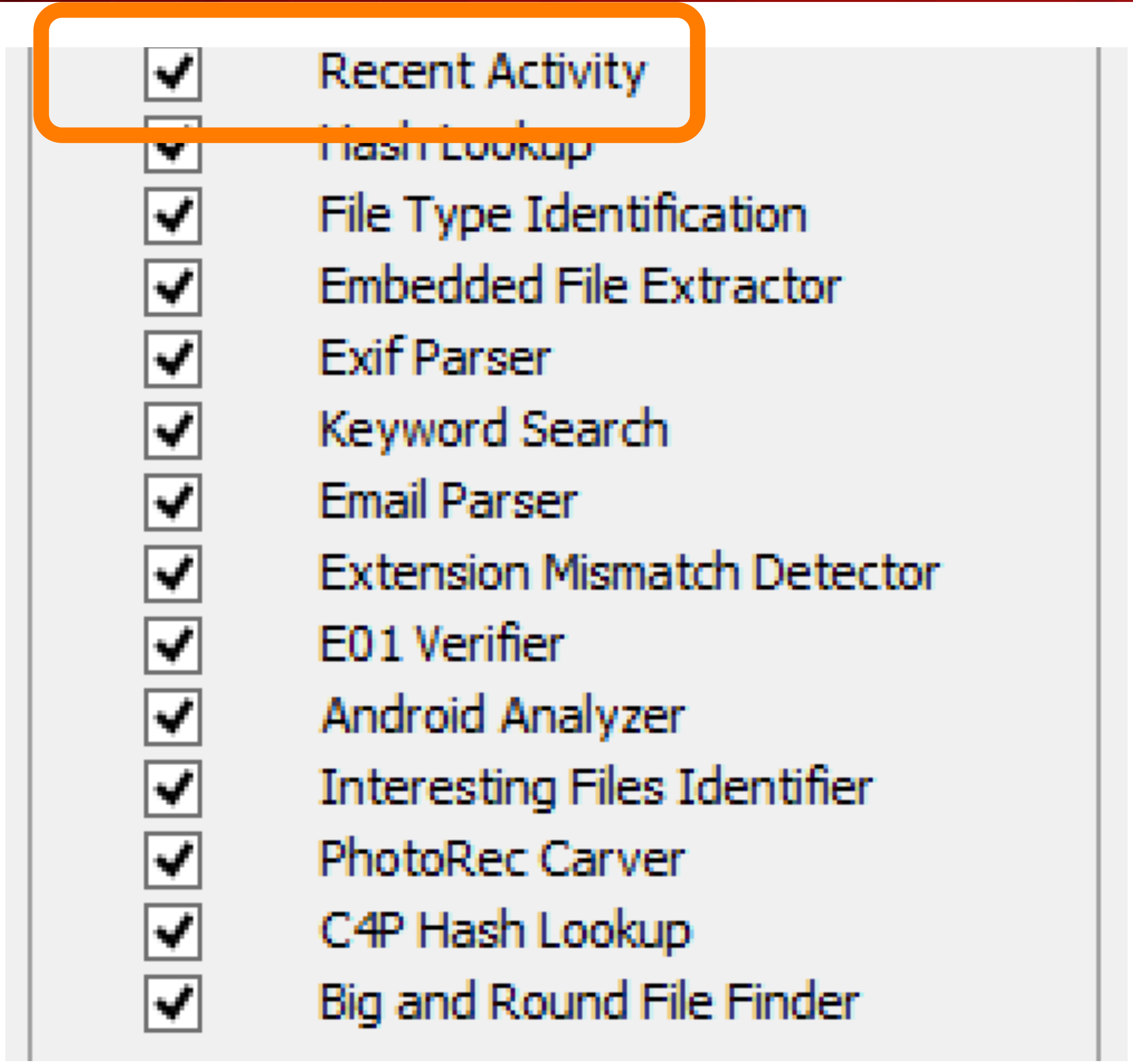
Select known BAD hash databases to use:

☑ notable_hash_db

☑ Calculate MD5 even if no hash database is selected

Identifies known and notable files using...

# Standard Features

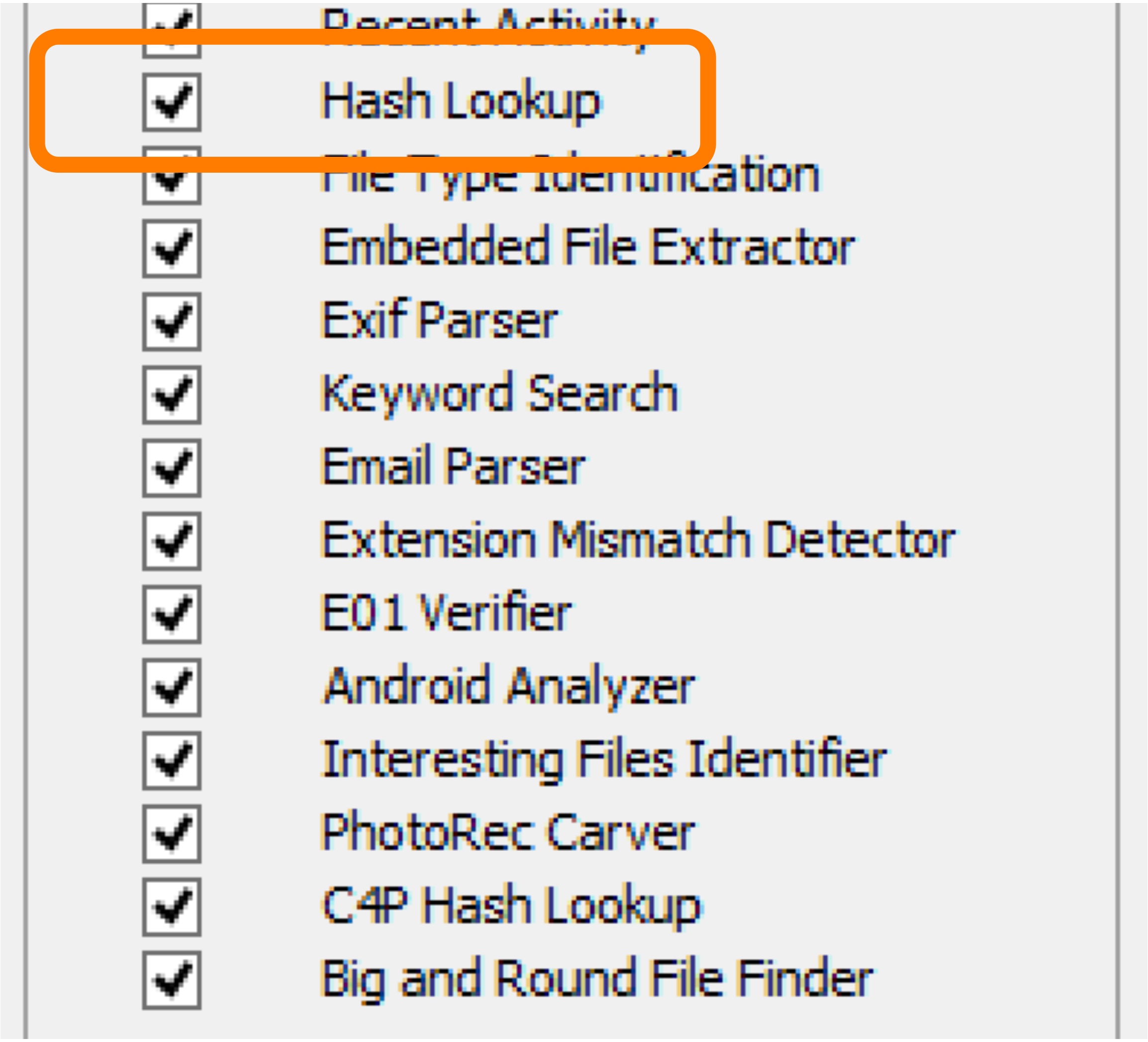


☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Android Analyzer
☑ Interesting Files Identifier
☑ PhotoRec Carver
☑ C4P Hash Lookup
☑ Big and Round File Finder

## Recent Activity

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

# Standard Features

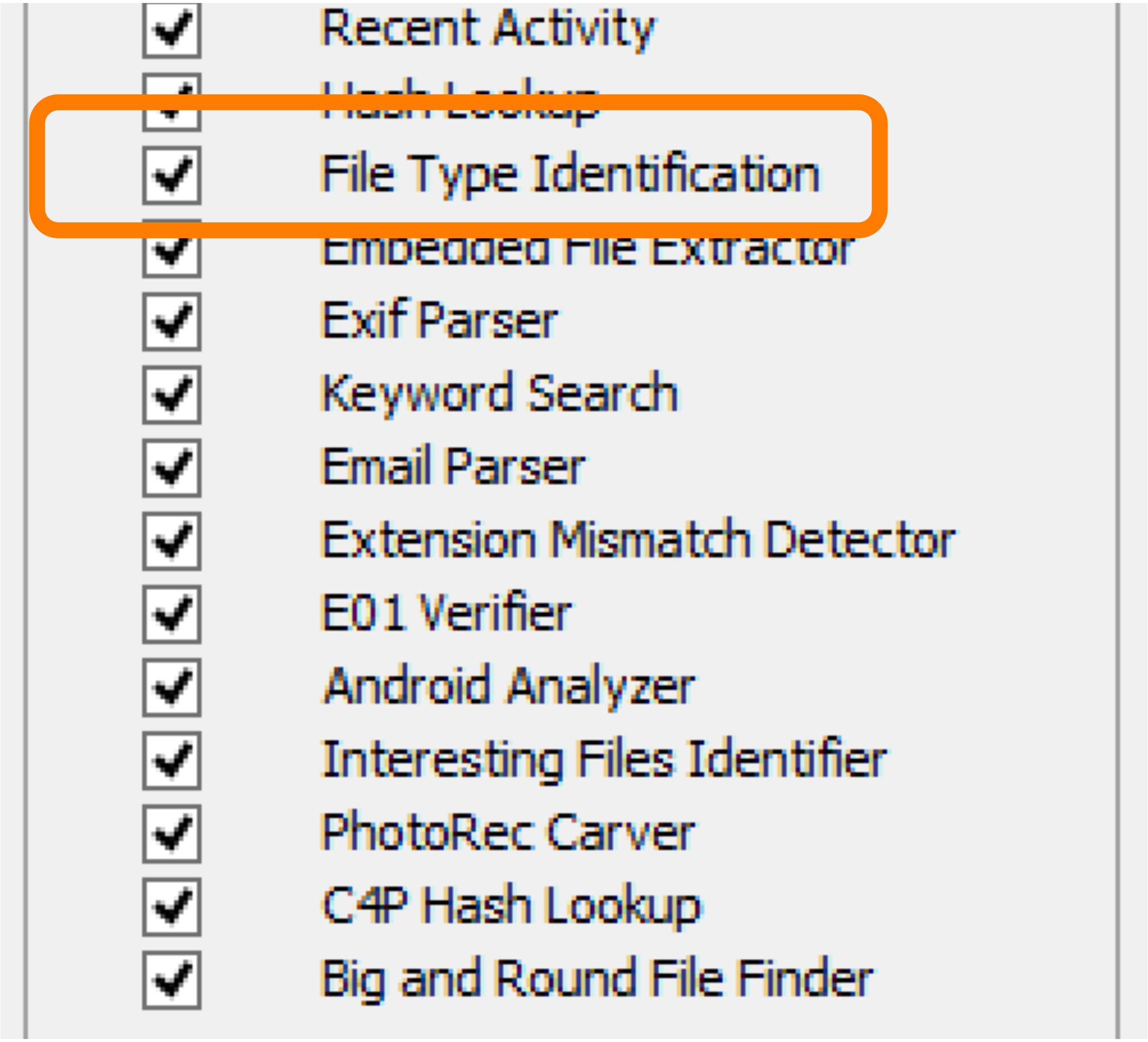


- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round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

## Hash Lookup

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

# Standard Features

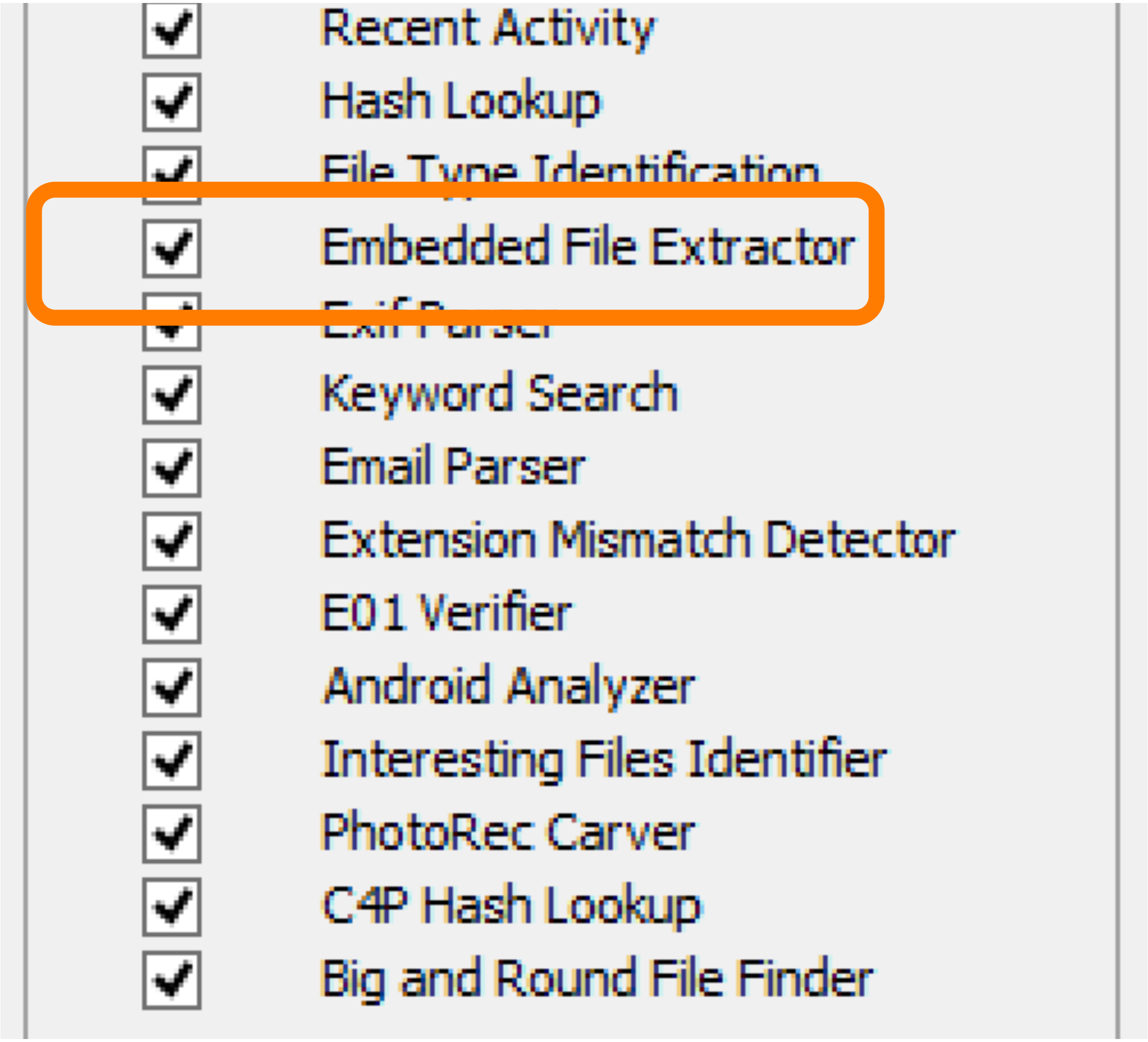


☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Android Analyzer
☑ Interesting Files Identifier
☑ PhotoRec Carver
☑ C4P Hash Lookup
☑ Big and Round File Finder

## File Type Identification

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

# Standard Features



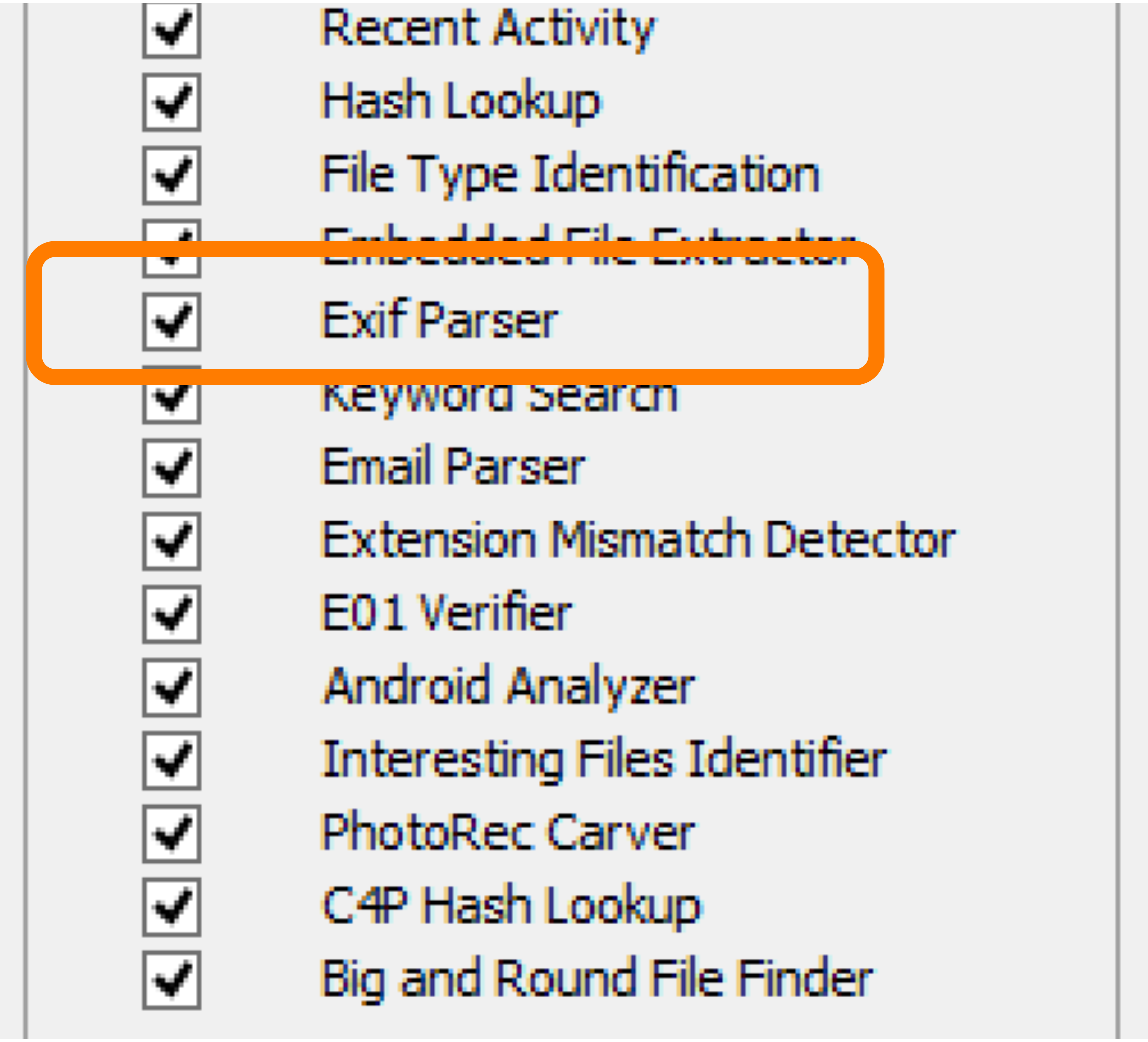
- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round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

## Embedded File Extractor

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

New!

# Standard Features

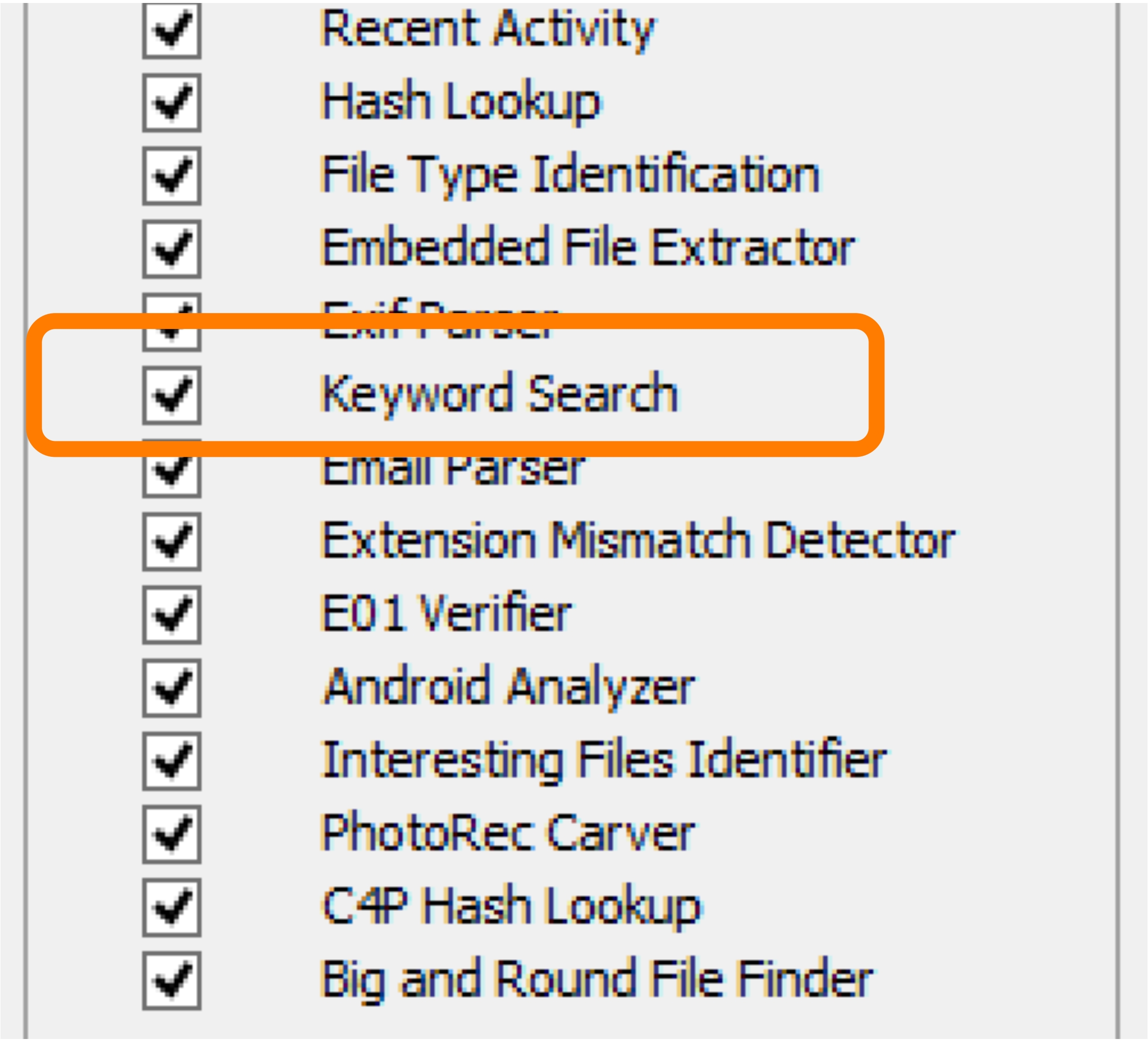


- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round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

## Exif Parser

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

# Standard Features

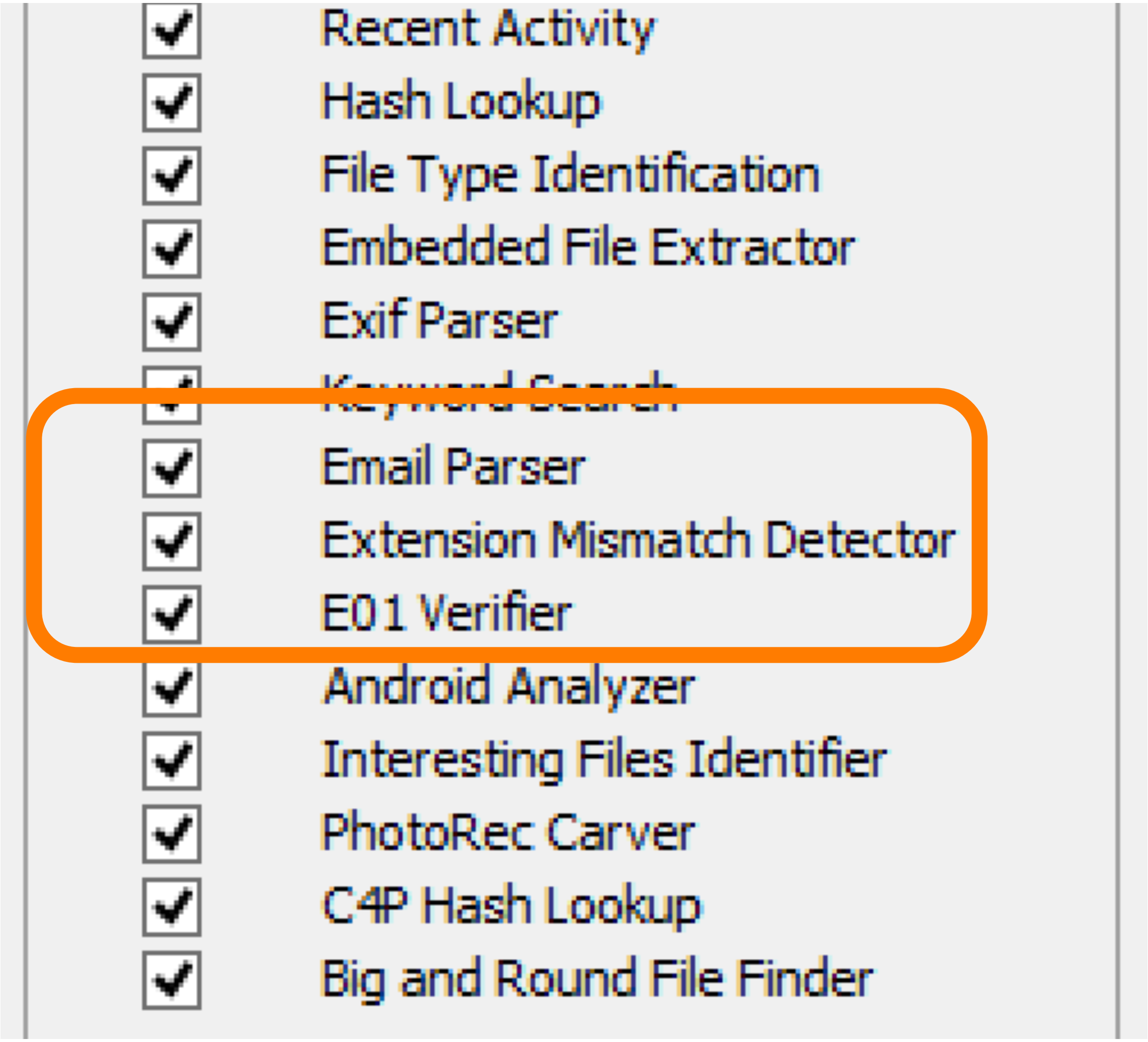


- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round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

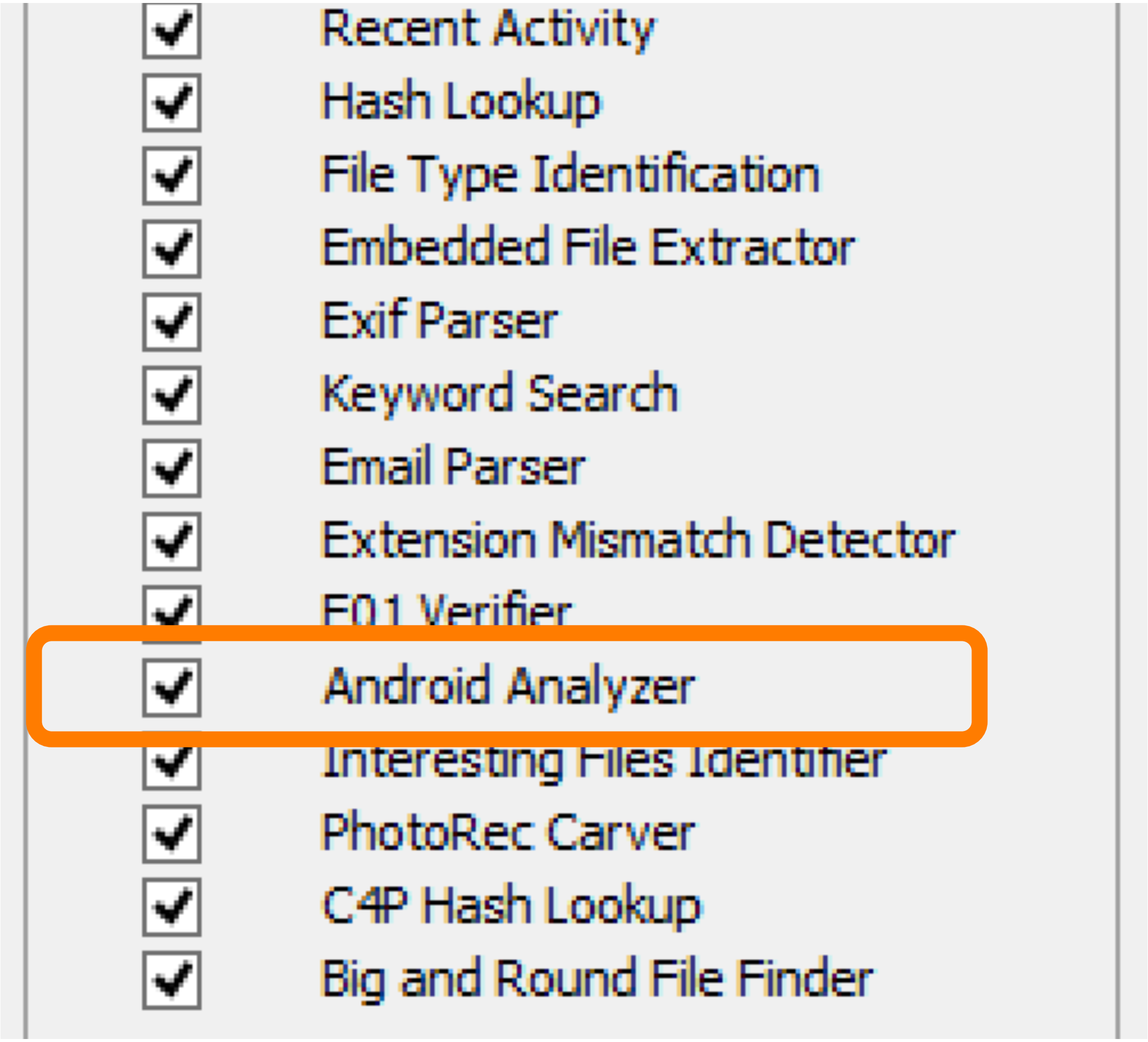
- Supports MBOX and PST.

## Extension Mismatch

- Users can specify rules

## E01 Verifier

# Standard Features

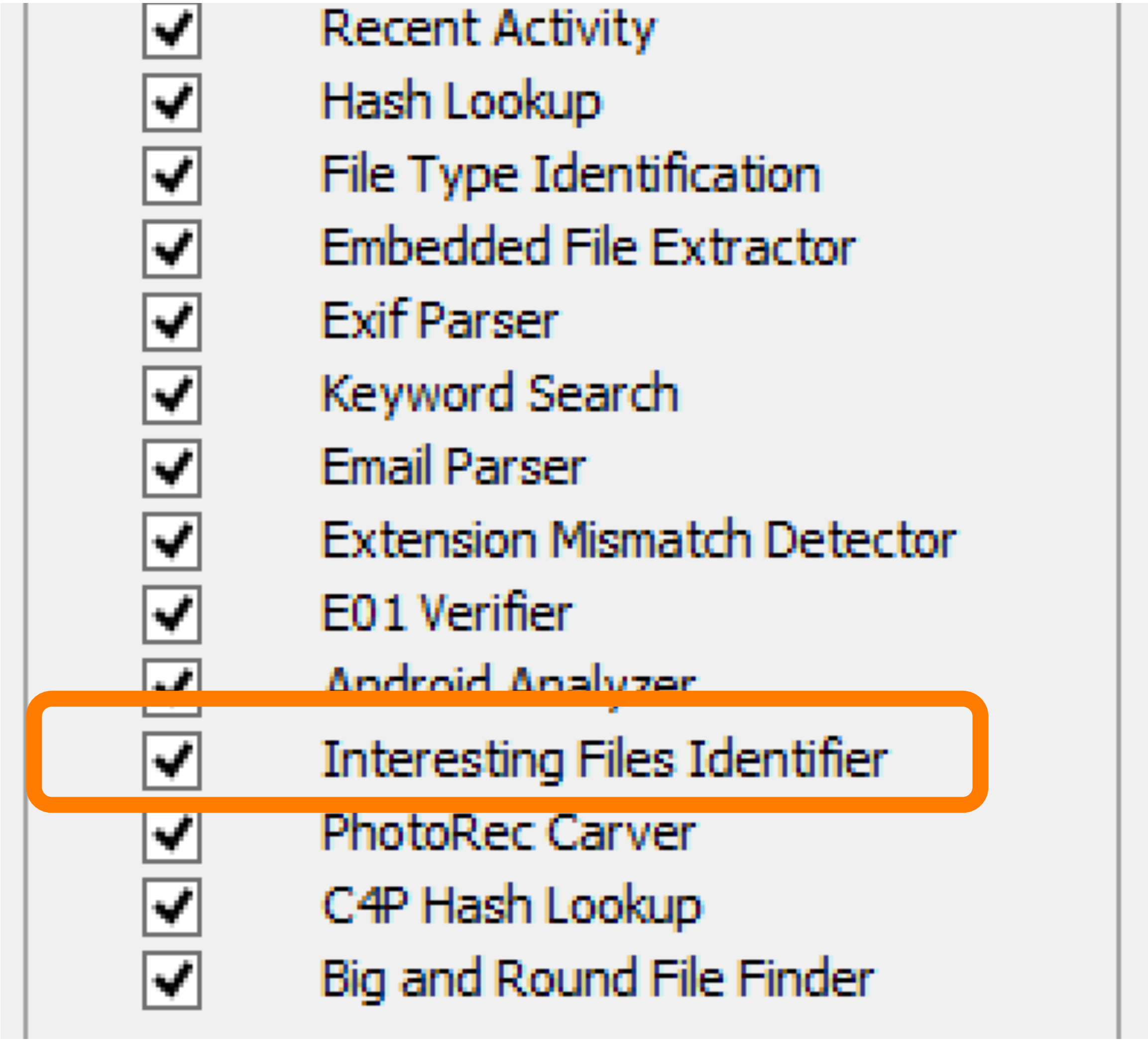


- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round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

## Android Analyzer

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

# Standard Features



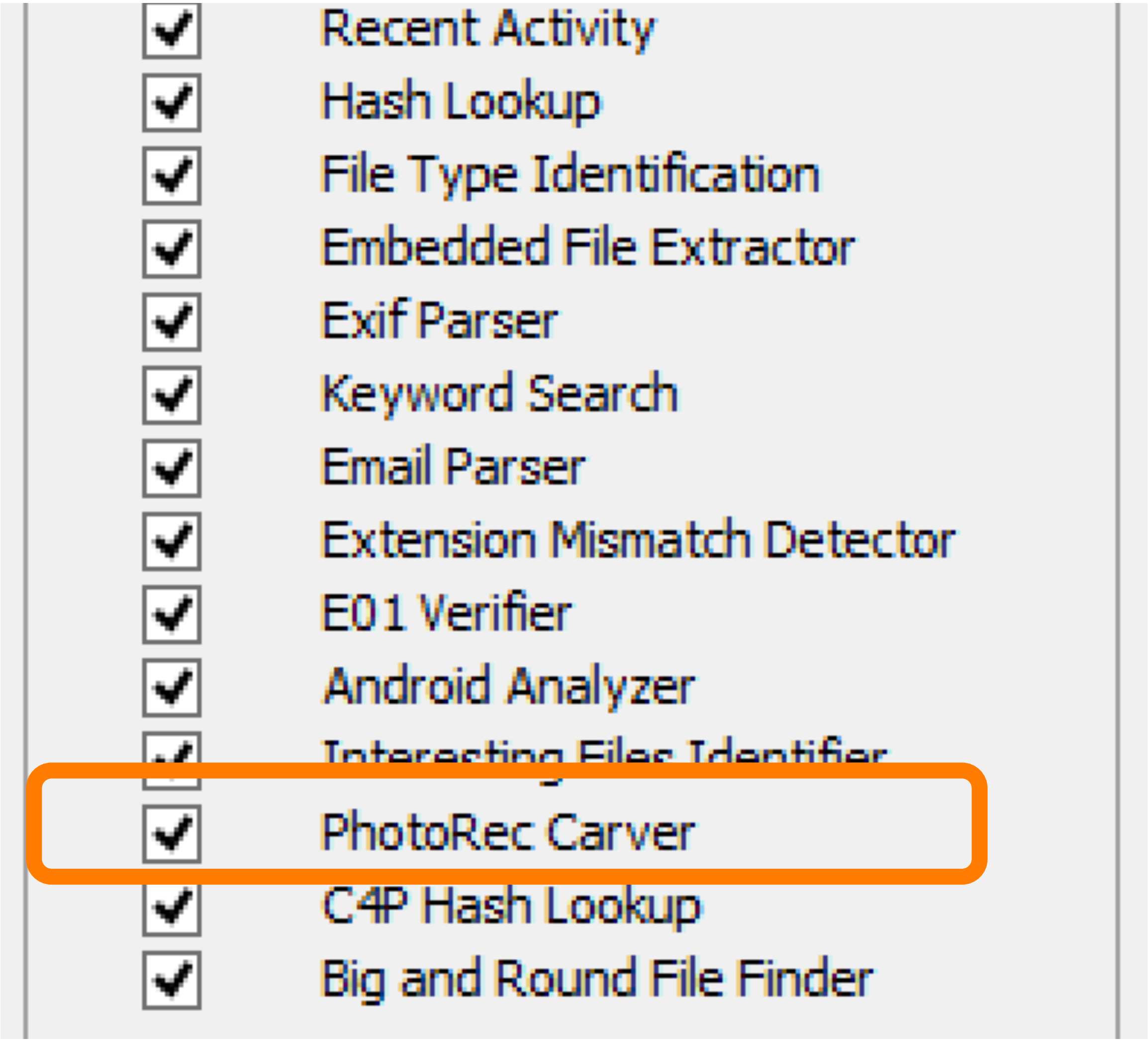
☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Android Analyzer
☑ Interesting Files Identifier
☑ PhotoRec Carver
☑ C4P Hash Lookup
☑ Big and Round File Finder

## 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
  - …

New!

# Standard Features



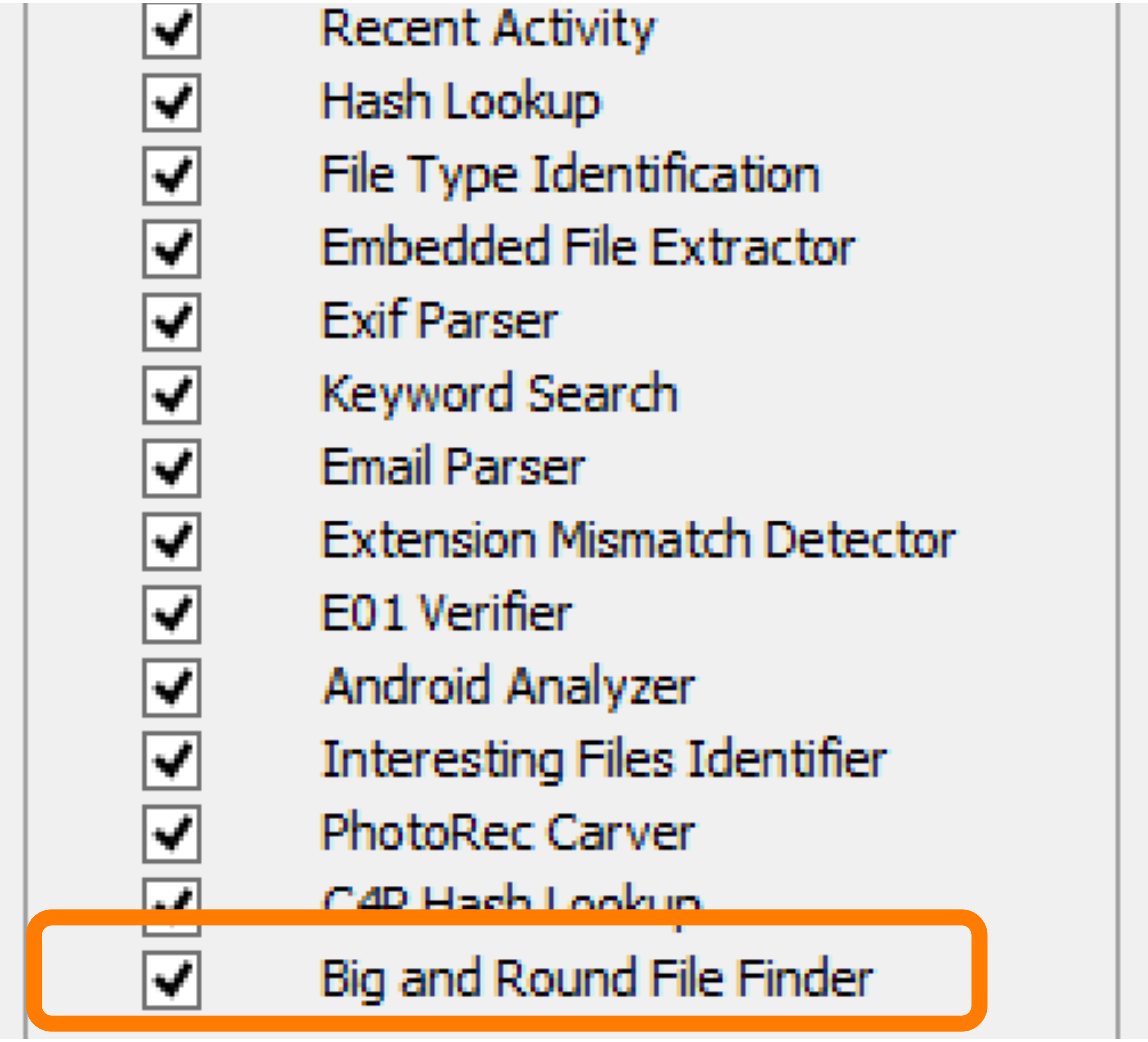
- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver
- ☑ C4P Hash Lookup
- ☑ Big and Round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

## PhotoRec Carver

New!

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

# Standard Features



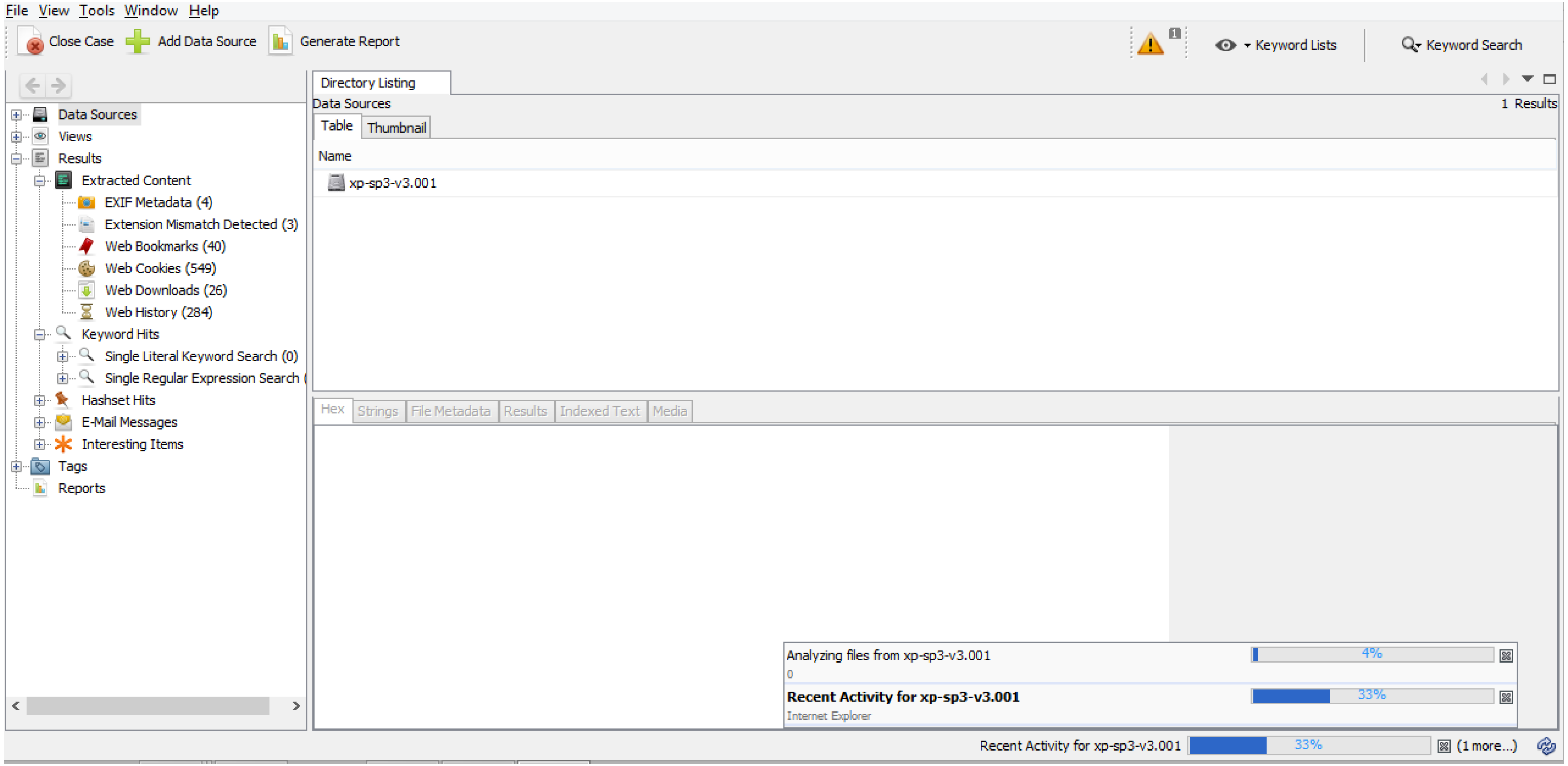
☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Embedded File Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Android Analyzer
☑ Interesting Files Identifier
☑ PhotoRec Carver
☑ C4P Hash Lookup
☑ Big and Round File Finder

## Big and Round File Finder

New!

- ????
- We did a lot of work on Python support.
- You'll learn more about this later.

# Review the Results



- Data Sources
- Views
- Results
  - Extracted Content
    - EXIF Metadata (4)
    - Extension Mismatch Detected (3)
    - Web Bookmarks (40)
    - Web Cookies (549)
    - Web Downloads (26)
    - Web History (284)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
- Tags
- Reports

Data Sources 1 Results

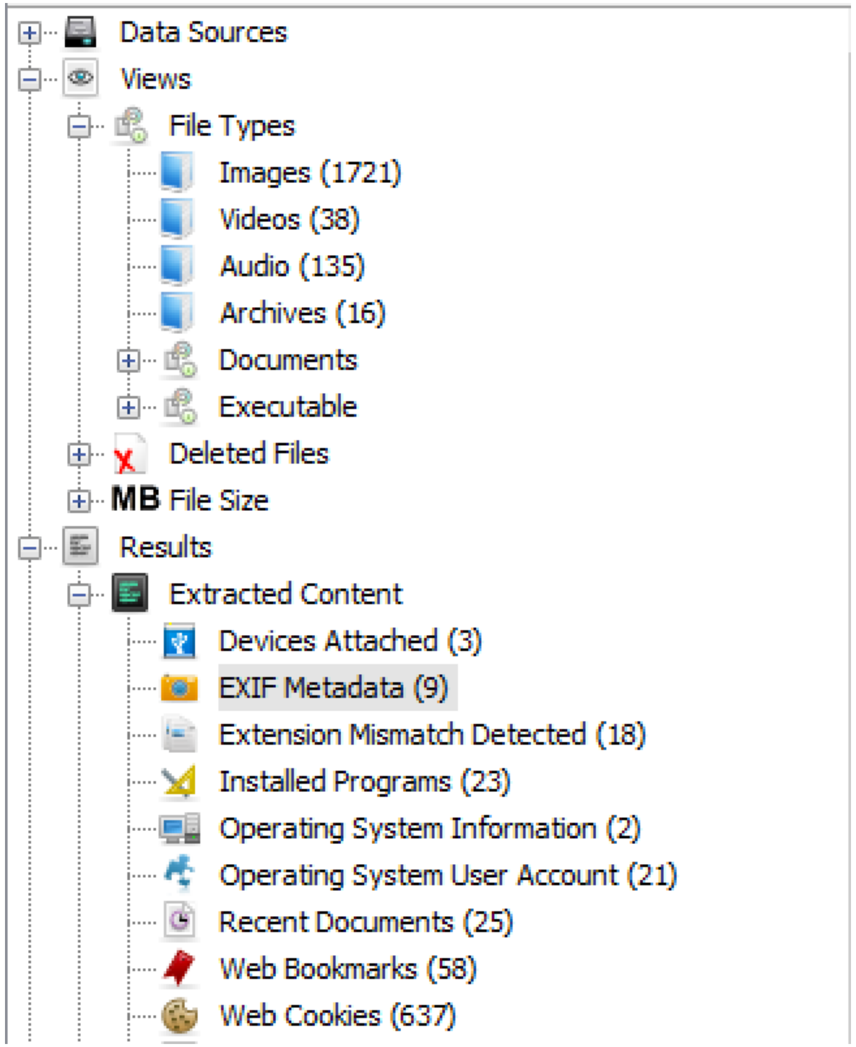
| Name |
|---|
| xp-sp3-v3.001 |

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

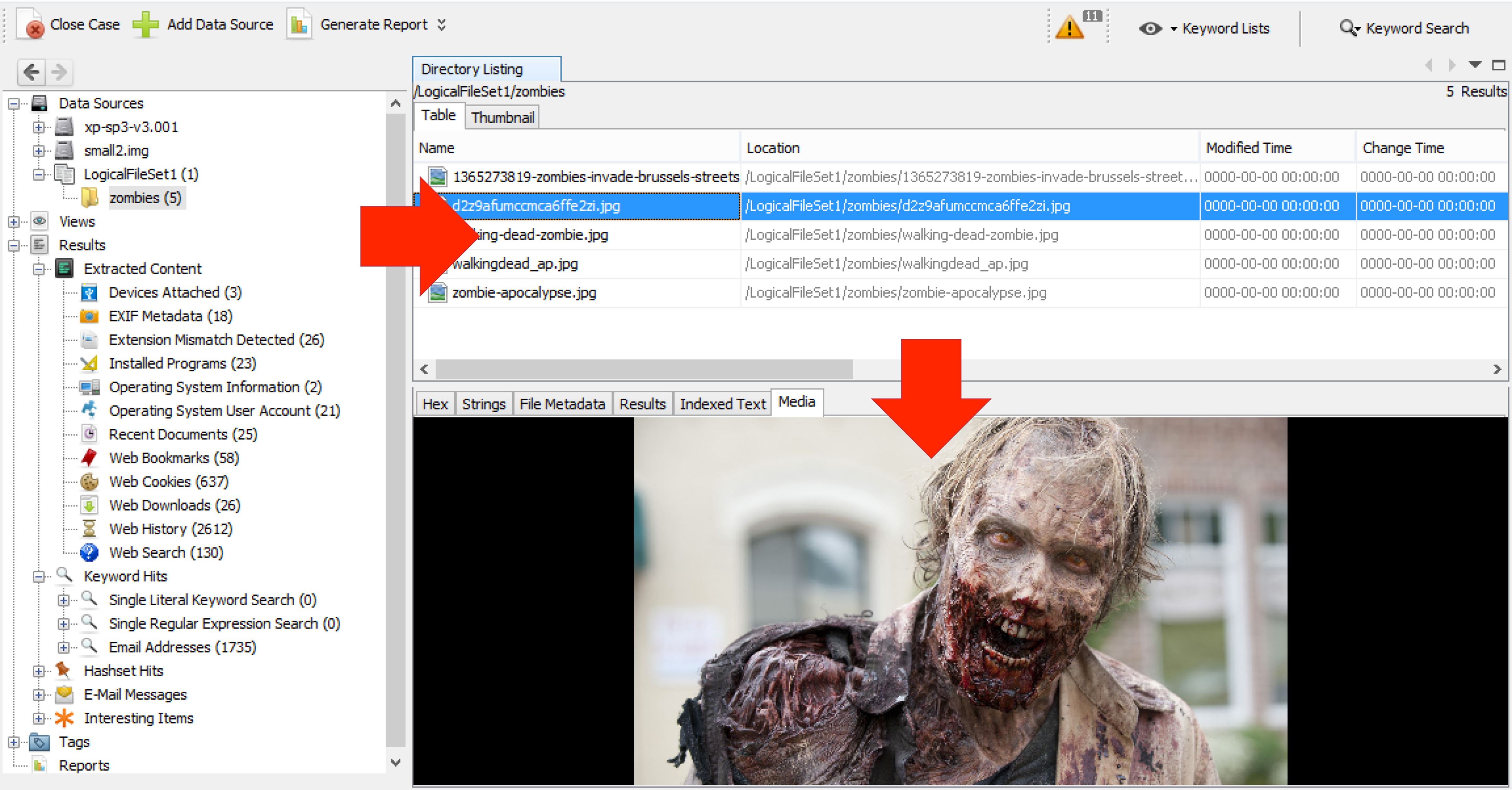


- Data Sources
- Views
  - File Types
    - Images (1721)
    - Videos (38)
    - Audio (135)
    - Archives (16)
    - Documents
    - Executable
  - Deleted Files
  - MB File Size
- Results
  - Extracted Content
    - Devices Attached (3)
    - EXIF Metadata (9)
    - Extension Mismatch Detected (18)
    - 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
  - ....
- New: Refreshes better when ZIP files are expanded behind the scenes.

New!

# Workflow



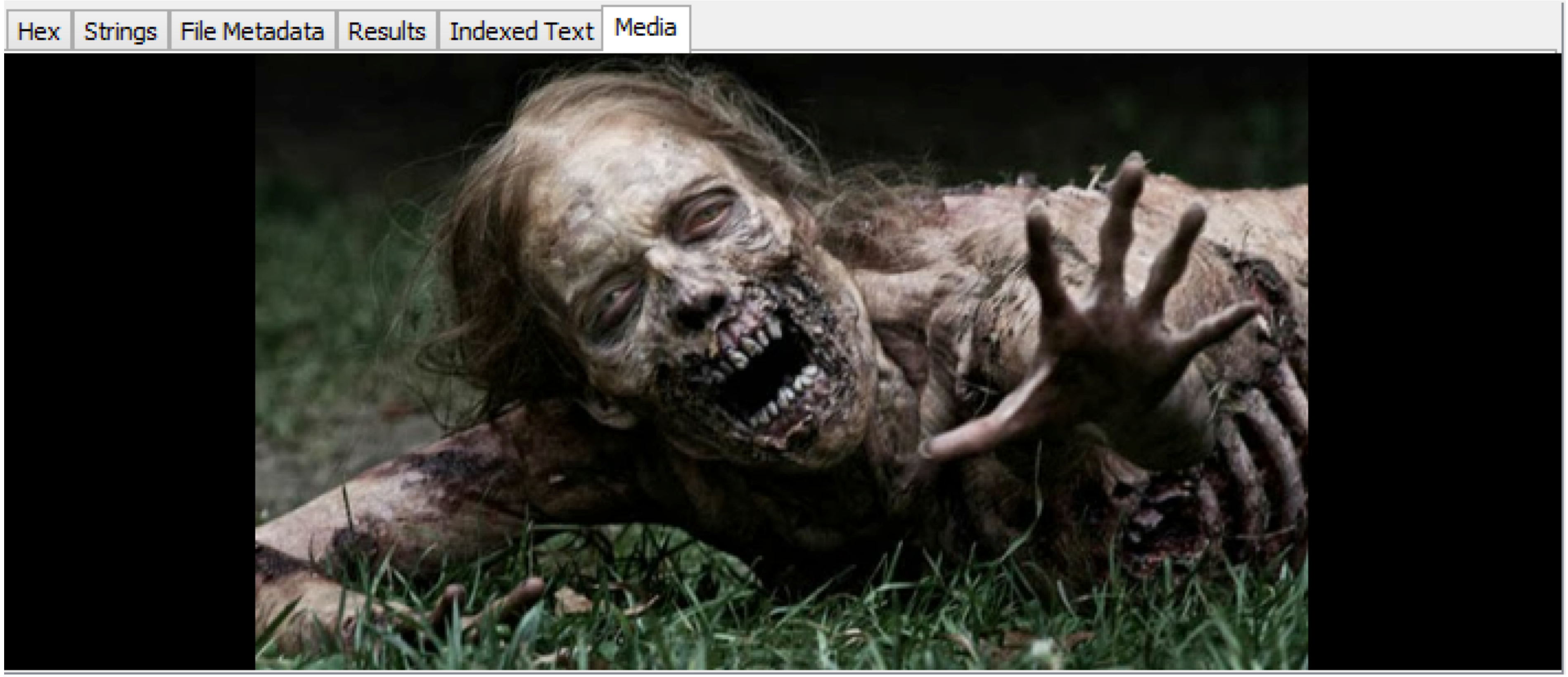
/LogicalFileSet1/zombies

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 |
| king-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 |

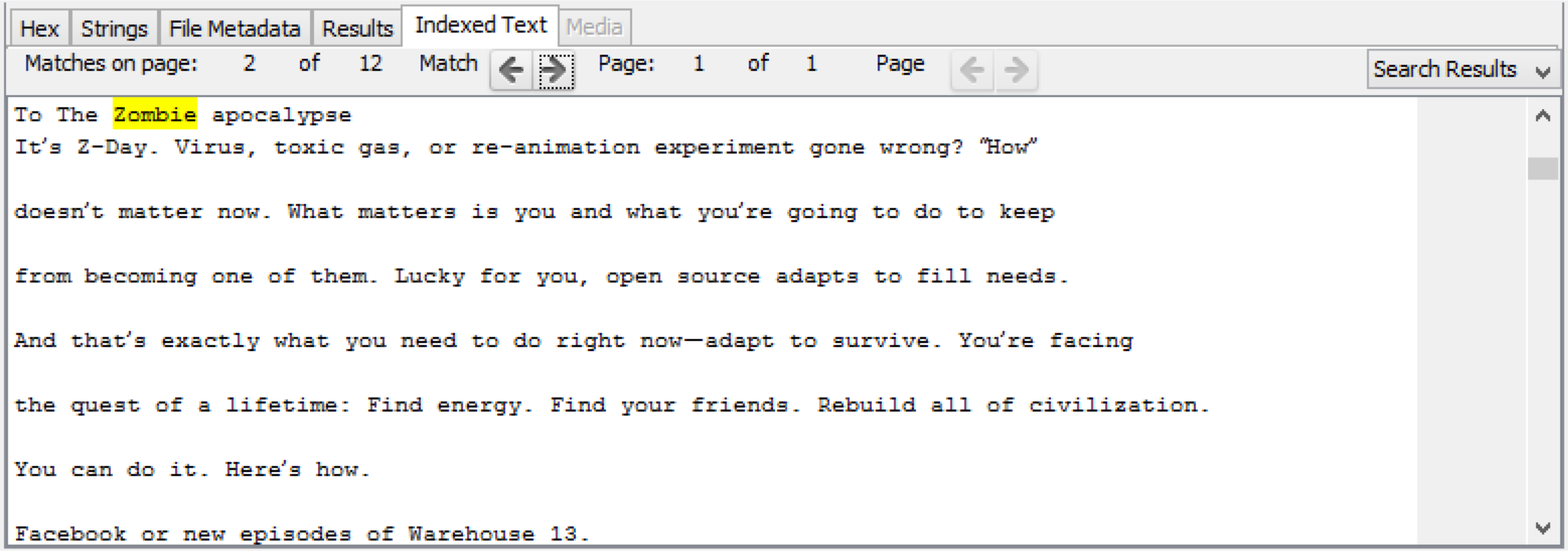
# File Viewers

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



# File Viewers

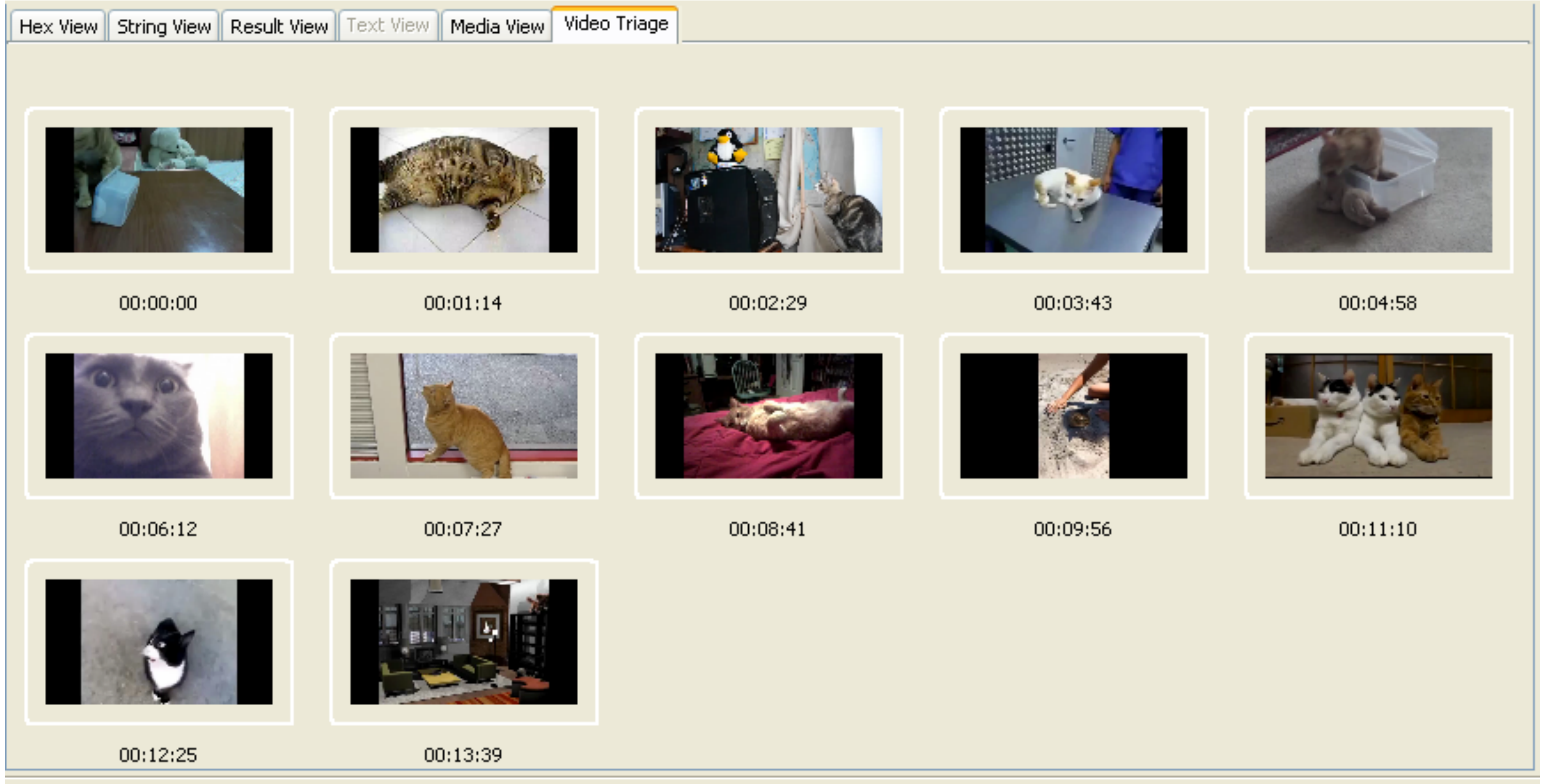
- View a file in the most relevant way.
- Text:



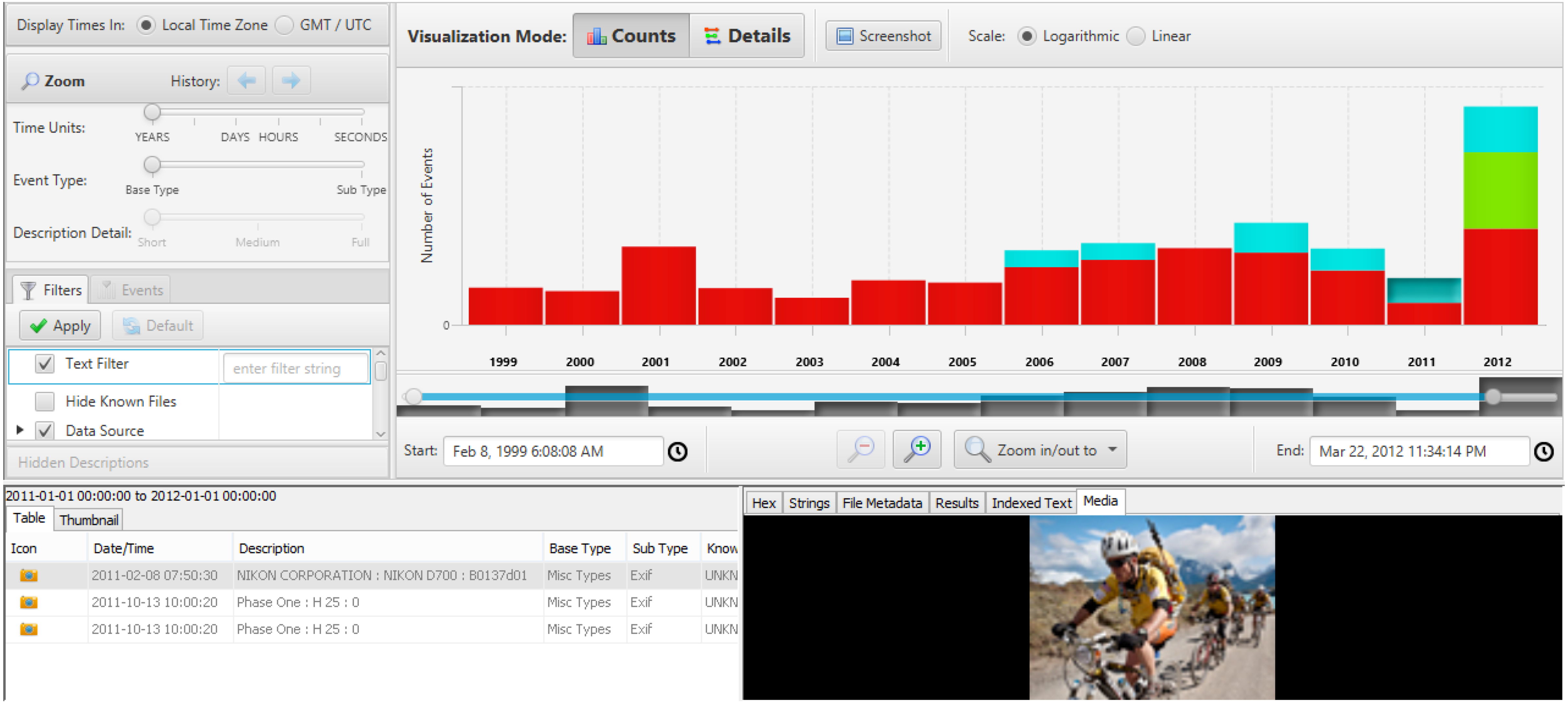
```
To The Zombie apocalypse
It's Z-Day. Virus, toxic gas, or re-animation experiment gone wrong? "How"

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:



# Timeline



Display Times In: ● Local Time Zone ○ GMT / UTC

Scale: ● Logarithmic ○ Linear

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

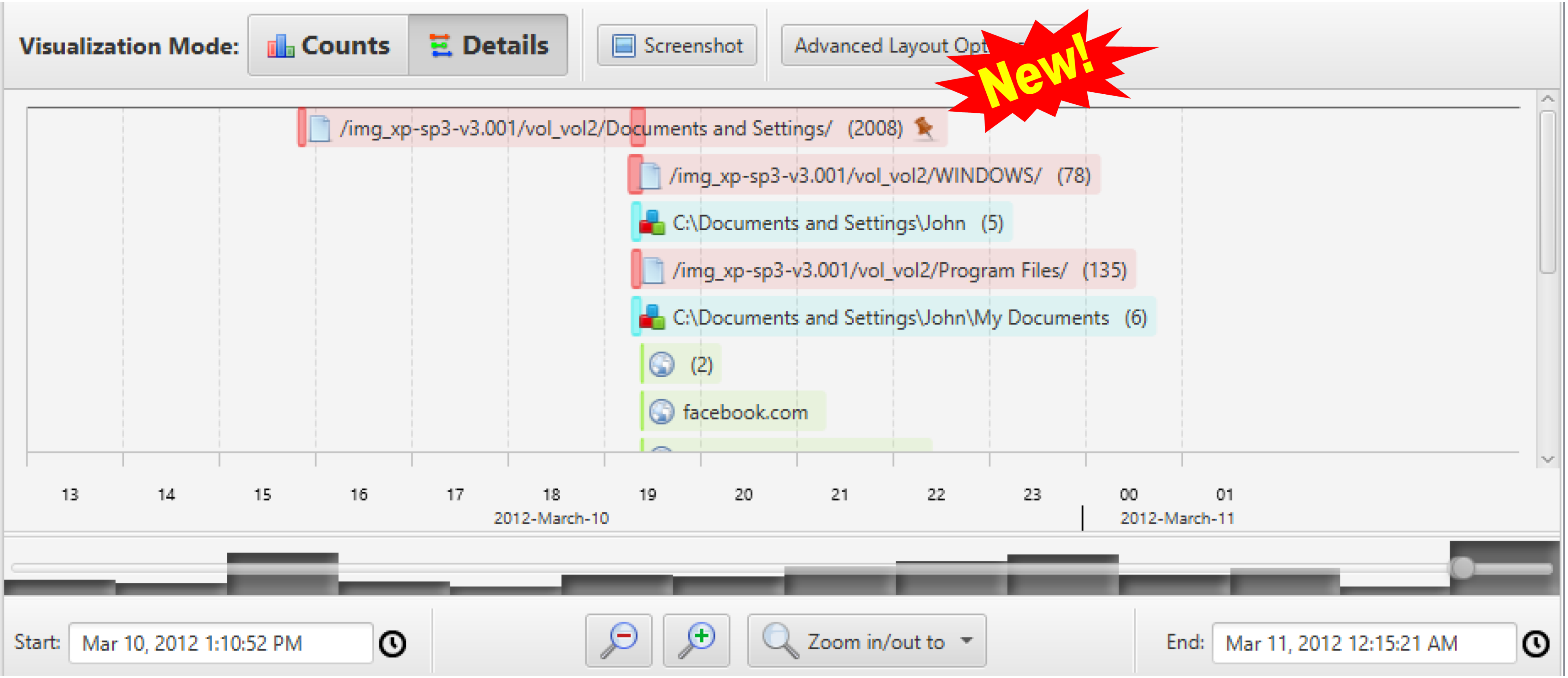
End: Mar 22, 2012 11:34:14 PM

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



/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)

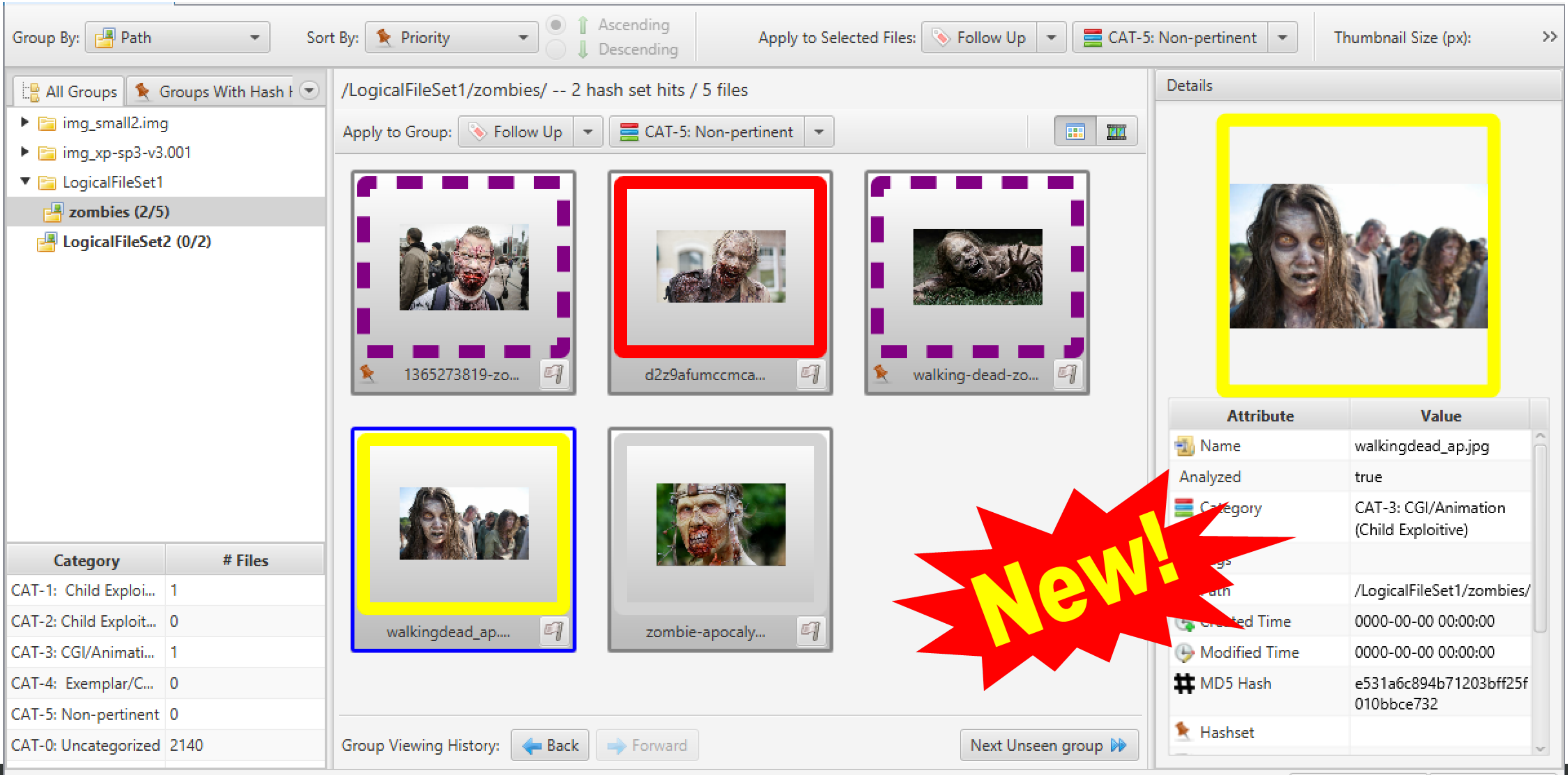
(2)

facebook.com

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

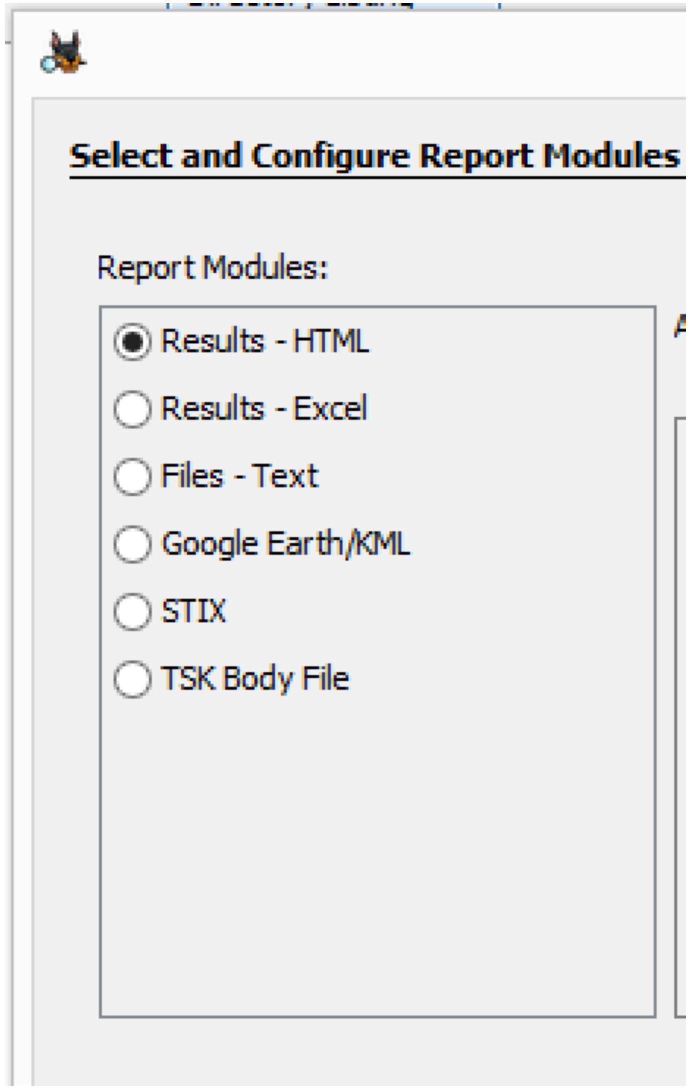
Apply to Group: Follow Up | CAT-5: Non-pertinent

Group Viewing History: Back | Forward | Next Unseen group

Details

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

# Generate A Report



Select and Configure Report Modules

Report Modules:

- ● Results - HTML
- ○ Results - Excel
- ○ Files - Text
- ○ Google Earth/KML
- ○ STIX
- ○ TSK Body File

- Standard reports:
  - HTML
  - Excel
  - CSV
  - KML
- STIX module looks for indicators of compromise.

# Impact

- Download Statistics:
  - May 1 to Oct 26 (2014 vs 2015).
  - One release during each time period.
- 2014: 45,232 total downloads  (253 per day)
- 2015: 59,718 total downloads (334 per day)
- Increase of 32%.

- Does not include Linux users on Sumuri Paladin.

# Platform Usage: Cyber Triage

- We continue to build our Cyber Triage application on it.
- Enables incident responders to:
  - Collect data from live system (or dead) by pushing agents as needed.
  - Applies heuristics to collected data
  - Guides responder through other data that requires manual review
- Stop by the table outside for more information.
  - Get a free "Cyber First Responder" T-shirt.

# What’s Next This Year?

- More work on collaboration features.
- More support for Python.
- More timeline and image gallery work.
- New feature to help search for account numbers and more easily review false positives.
- ….

# What Can You Do?

- If you are using it:
  - Spread the word to your friends.
  - Provide us some quotes and stories for www.sleuthkit.org.
  - Let us know what else you want.
- If you aren't using it:
  - Try it out.
  - Especially if your existing software is up for renewal.

- Send me an e-mail: brianc@basistech.com

# Support

- Community:
  - E-mail list and web forum
- Basis Technology:
  - Commercial support
  - Access to engineers who can fix any issues.

# Training

- Basis offers public training courses.
- Next one will be next March.
  - Besides the one tomorrow.
- We also offer private training courses.

# Contact

Brian Carrier

brianc@basistech.com

Download It Today

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