

9th Annual

#OSDFCon

OPEN SOURCE DIGITAL FORENSICS CONFERENCE

Introduction to Autopsy

Brian Carrier

October 17, 2018 | Herndon, VA | Hosted by



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


Close Case + Add Data Source Generate Report

Directory Listing

LogicalFileSet1/zombies 5 Results

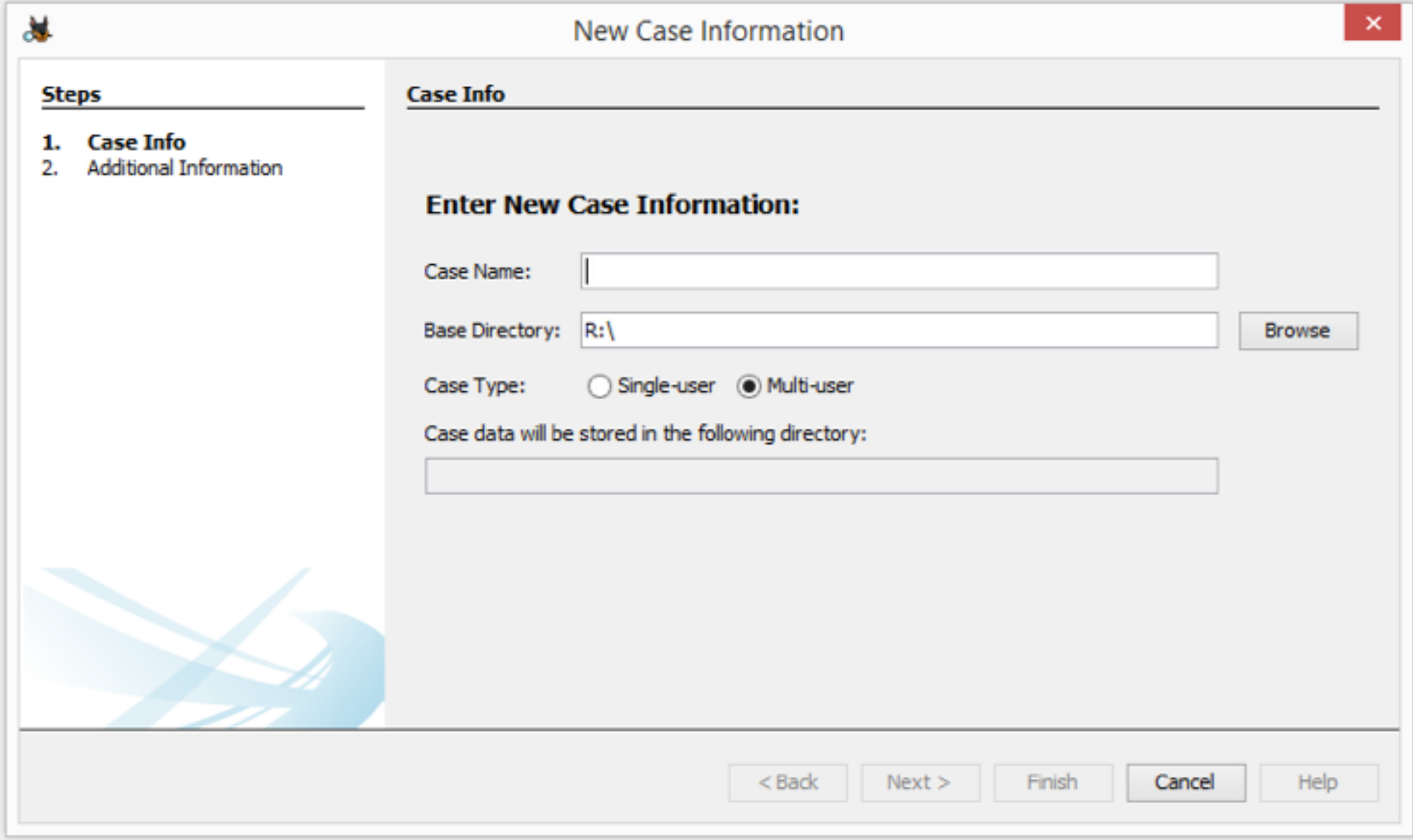
Name	Location	Modified Time	Change Time
1365273819-zombies-invade-brussels-streets	/LogicalFileSet1/zombies/1365273819-zombies-invade-brussels-street...	0000-00-00 00:00:00	0000-00-00 00:00:00
d2z9afumccmca6ffe2zi.jpg	/LogicalFileSet1/zombies/d2z9afumccmca6ffe2zi.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00
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

Hex Strings File Metadata Results Indexed Text Media



Standard Features

Make A Case



The image shows a Windows-style dialog box titled "New Case Information". It has a standard title bar with a close button (X) in the top right corner. The dialog is divided into two main sections. On the left is a "Steps" sidebar with a list: "1. Case Info" (which is selected and bolded) and "2. Additional Information". The main area on the right is titled "Case Info" and contains the heading "Enter New Case Information:". Below this heading are four input fields: "Case Name:" with an empty text box; "Base Directory:" with a text box containing "R:\", followed by a "Browse" button; "Case Type:" with two radio buttons, "Single-user" (unselected) and "Multi-user" (selected); and "Case data will be stored in the following directory:" followed by an empty text box. At the bottom of the dialog is a row of five buttons: "< Back", "Next >", "Finish", "Cancel", and "Help".

New Case Information

Steps

- 1. Case Info**
2. Additional Information

Case Info

Enter New Case Information:

Case Name:

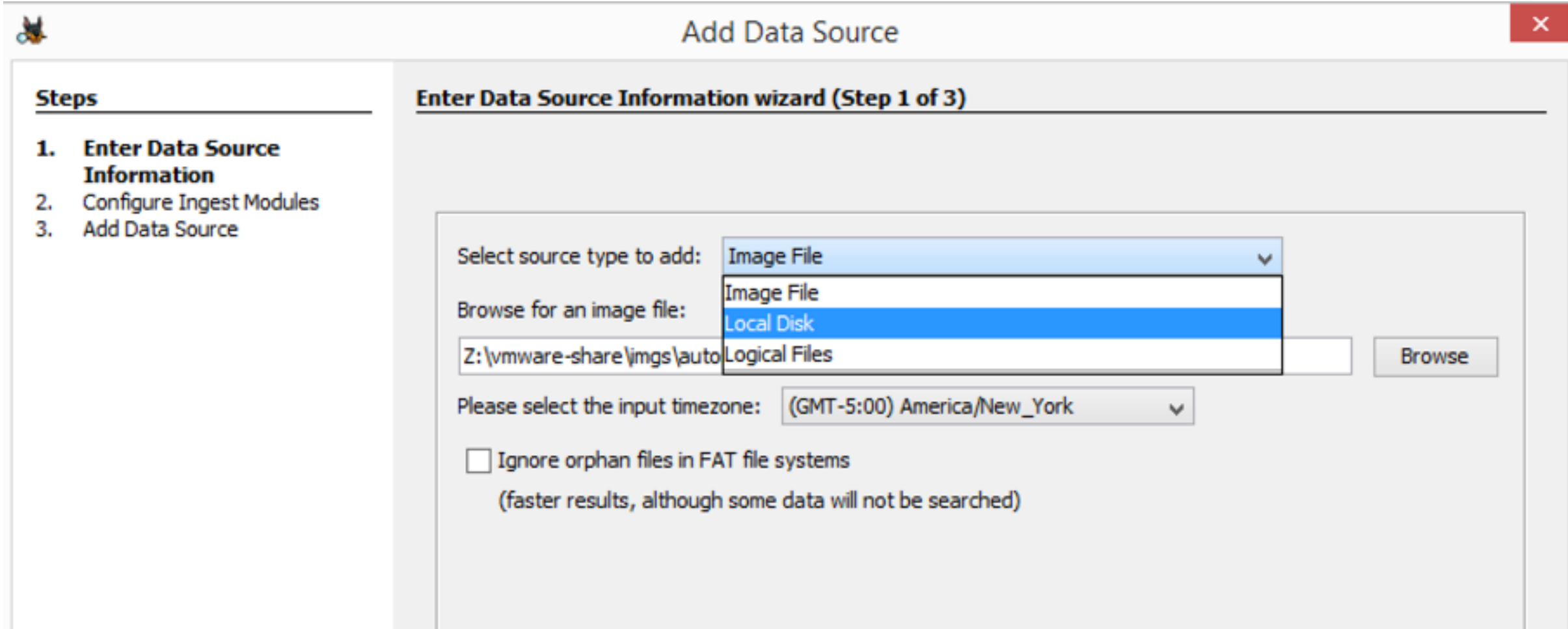
Base Directory:

Case Type: ☐ Single-user ☒ Multi-user

Case data will be stored in the following directory:

< Back Next > Finish Cancel Help

Add A Data Source



The screenshot shows a software window titled "Add Data Source" with a close button in the top right corner. On the left is a "Steps" sidebar with three items: "1. Enter Data Source Information" (highlighted), "2. Configure Ingest Modules", and "3. Add Data Source". The main area is titled "Enter Data Source Information wizard (Step 1 of 3)". It contains a dropdown menu "Select source type to add:" with "Image File" selected and open, showing options "Image File", "Local Disk", and "Logical Files". Below this is a text field "Browse for an image file:" containing "Z:\vmware-share\imgs\auto" and a "Browse" button. Further down is a dropdown "Please select the input timezone:" set to "(GMT-5:00) America/New_York". At the bottom is an unchecked checkbox "Ignore orphan files in FAT file systems" with the text "(faster results, although some data will not be searched)" below it.

Steps

- 1. Enter Data Source Information**
2. Configure Ingest Modules
3. Add Data Source

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)

Browse

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, VMDDK, 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
- ☒ Bin and Round File Finder

Select All

Deselect All

☒ Process Unallocated Space

Select known hash databases to use:

☒ NSRLFile.txt-md5

Select known BAD hash databases to use:

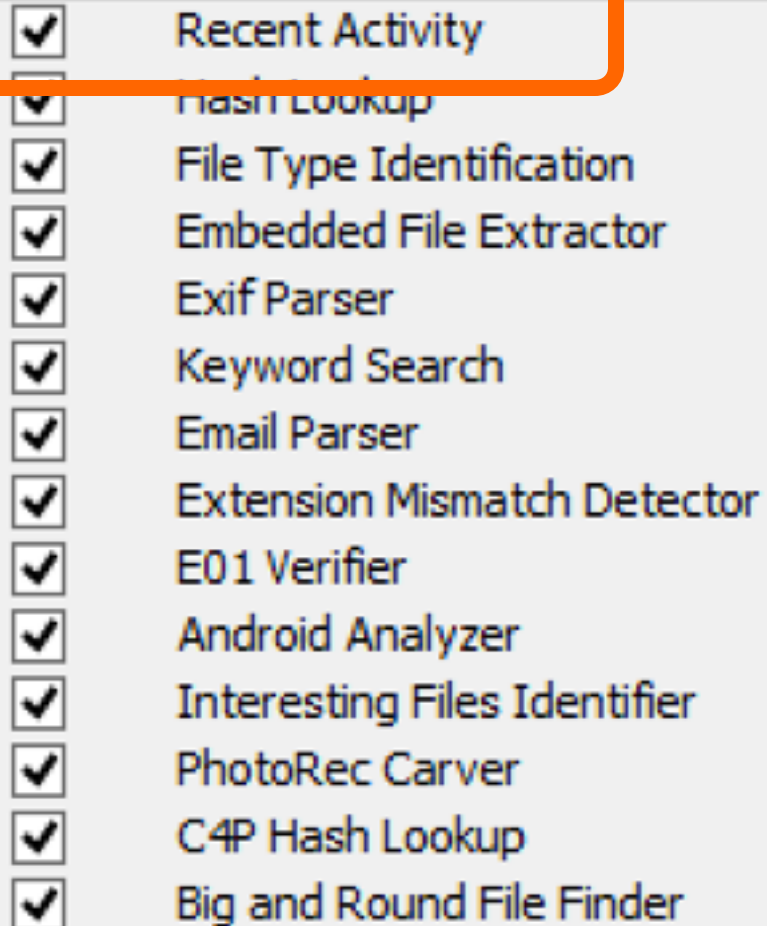
☒ notable_hash_db

☒ Calculate MD5 even if no hash database is selected

Identifies known and notable files using...

Advanced

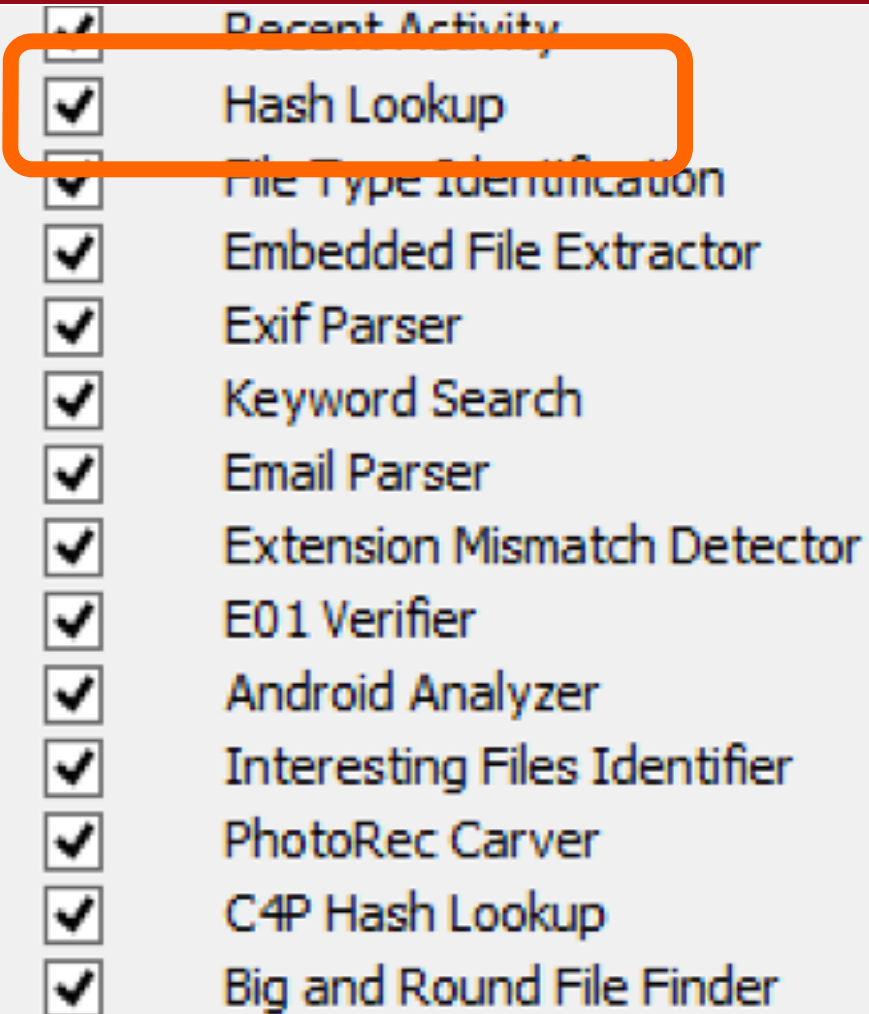
Standard Features

- 
- | | |
|-------------------------------------|------------------------------|
| <input checked="" type="checkbox"/> | Recent Activity |
| <input checked="" type="checkbox"/> | Hash Lookup |
| <input checked="" type="checkbox"/> | File Type Identification |
| <input checked="" type="checkbox"/> | Embedded File Extractor |
| <input checked="" type="checkbox"/> | Exif Parser |
| <input checked="" type="checkbox"/> | Keyword Search |
| <input checked="" type="checkbox"/> | Email Parser |
| <input checked="" type="checkbox"/> | Extension Mismatch Detector |
| <input checked="" type="checkbox"/> | E01 Verifier |
| <input checked="" type="checkbox"/> | Android Analyzer |
| <input checked="" type="checkbox"/> | Interesting Files Identifier |
| <input checked="" type="checkbox"/> | PhotoRec Carver |
| <input checked="" type="checkbox"/> | C4P Hash Lookup |
| <input checked="" type="checkbox"/> | Big and Round File Finder |

Recent Activity

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

Standard Features



Hash Lookup

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

Standard Features

<input checked="" type="checkbox"/>	Recent Activity
<input checked="" type="checkbox"/>	Hash Lookup
<input checked="" type="checkbox"/>	File Type Identification
<input checked="" type="checkbox"/>	Embedded File Extractor
<input checked="" type="checkbox"/>	Exif Parser
<input checked="" type="checkbox"/>	Keyword Search
<input checked="" type="checkbox"/>	Email Parser
<input checked="" type="checkbox"/>	Extension Mismatch Detector
<input checked="" type="checkbox"/>	E01 Verifier
<input checked="" type="checkbox"/>	Android Analyzer
<input checked="" type="checkbox"/>	Interesting Files Identifier
<input checked="" type="checkbox"/>	PhotoRec Carver
<input checked="" type="checkbox"/>	C4P Hash Lookup
<input checked="" type="checkbox"/>	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

<input checked="" type="checkbox"/>	Recent Activity
<input checked="" type="checkbox"/>	Hash Lookup
<input checked="" type="checkbox"/>	File Type Identification
<input checked="" type="checkbox"/>	Embedded File Extractor
<input checked="" type="checkbox"/>	Exif Parser
<input checked="" type="checkbox"/>	Keyword Search
<input checked="" type="checkbox"/>	Email Parser
<input checked="" type="checkbox"/>	Extension Mismatch Detector
<input checked="" type="checkbox"/>	E01 Verifier
<input checked="" type="checkbox"/>	Android Analyzer
<input checked="" type="checkbox"/>	Interesting Files Identifier
<input checked="" type="checkbox"/>	PhotoRec Carver
<input checked="" type="checkbox"/>	C4P Hash Lookup
<input checked="" type="checkbox"/>	Big and Round File Finder

Embedded File Extractor

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

Standard Features

<input checked="" type="checkbox"/>	Recent Activity
<input checked="" type="checkbox"/>	Hash Lookup
<input checked="" type="checkbox"/>	File Type Identification
<input checked="" type="checkbox"/>	Embedded File Extractor
<input checked="" type="checkbox"/>	Exif Parser
<input checked="" type="checkbox"/>	Keyword Search
<input checked="" type="checkbox"/>	Email Parser
<input checked="" type="checkbox"/>	Extension Mismatch Detector
<input checked="" type="checkbox"/>	E01 Verifier
<input checked="" type="checkbox"/>	Android Analyzer
<input checked="" type="checkbox"/>	Interesting Files Identifier
<input checked="" type="checkbox"/>	PhotoRec Carver
<input checked="" type="checkbox"/>	C4P Hash Lookup
<input checked="" type="checkbox"/>	Big and Round File Finder

Exif Parser

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

Standard Features

<input checked="" type="checkbox"/>	Recent Activity
<input checked="" type="checkbox"/>	Hash Lookup
<input checked="" type="checkbox"/>	File Type Identification
<input checked="" type="checkbox"/>	Embedded File Extractor
<input checked="" type="checkbox"/>	Exif Parser
<input checked="" type="checkbox"/>	Keyword Search
<input checked="" type="checkbox"/>	Email Parser
<input checked="" type="checkbox"/>	Extension Mismatch Detector
<input checked="" type="checkbox"/>	E01 Verifier
<input checked="" type="checkbox"/>	Android Analyzer
<input checked="" type="checkbox"/>	Interesting Files Identifier
<input checked="" type="checkbox"/>	PhotoRec Carver
<input checked="" type="checkbox"/>	C4P Hash Lookup
<input checked="" type="checkbox"/>	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
- ✓ F01 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

The screenshot displays a digital forensics analysis application. The interface includes a menu bar (File, View, Tools, Window, Help) and a toolbar with buttons for 'Close Case', 'Add Data Source', and 'Generate Report'. A left-hand sidebar contains a tree view with categories: Data Sources, Views, Results, Extracted Content (with sub-items like EXIF Metadata, Extension Mismatch Detected, Web Bookmarks, Web Cookies, Web Downloads, Web History), Keyword Hits, Hashset Hits, E-Mail Messages, Interesting Items, Tags, and Reports. The main pane is titled 'Directory Listing' and shows a table of 'Data Sources'. The table has columns for 'Table' and 'Thumbnail', and lists a single entry: 'xp-sp3-v3.001'. Below the table, there are tabs for 'Hex', 'Strings', 'File Metadata', 'Results', 'Indexed Text', and 'Media'. At the bottom right, a status bar shows progress for 'Analyzing files from xp-sp3-v3.001' at 4% and 'Recent Activity for xp-sp3-v3.001' at 33%.

File View Tools Window Help

Close Case Add Data Source Generate Report

Keyword Lists Keyword Search

Directory Listing

Data Sources

Table Thumbnail

Name

xp-sp3-v3.001

1 Result

Hex Strings File Metadata Results Indexed Text Media

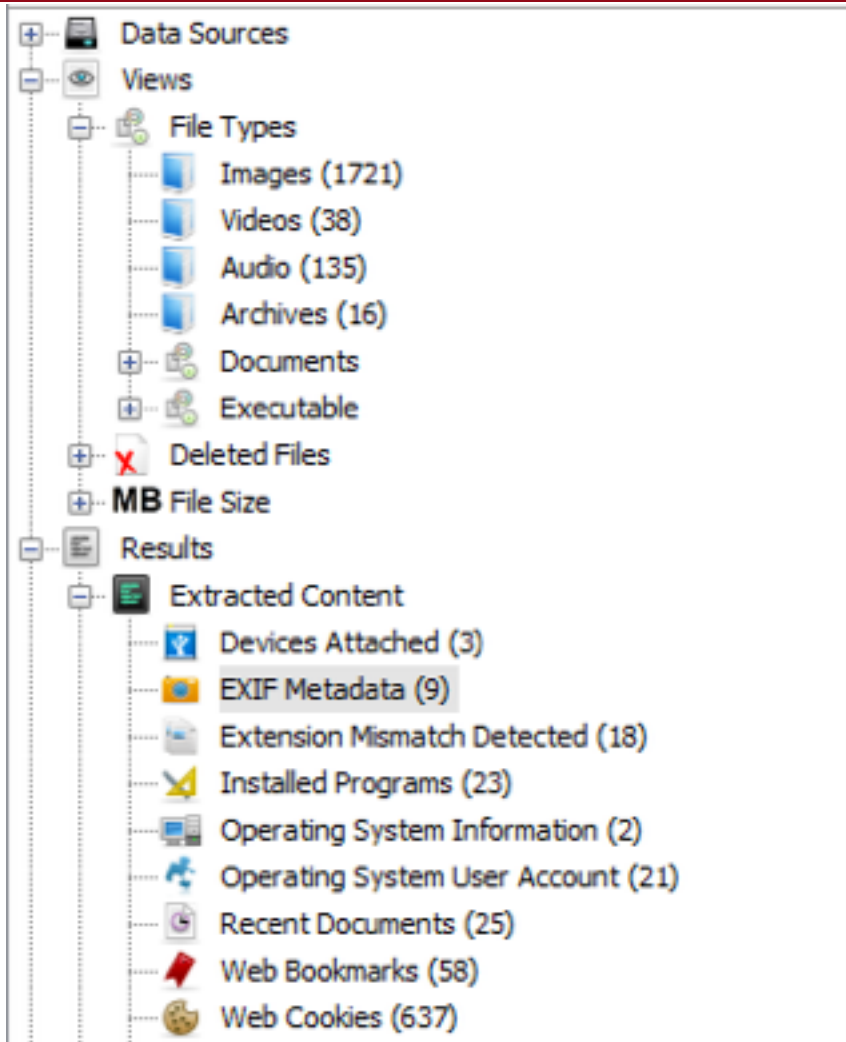
Analyzing files from xp-sp3-v3.001 4%

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

Internet Explorer

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

The Tree



The tree has all of the results.

Updated in real-time.

Find:

- Files of a given type
- Web artifacts
- Registry results
-

Workflow

Close Case Add Data Source Generate Report

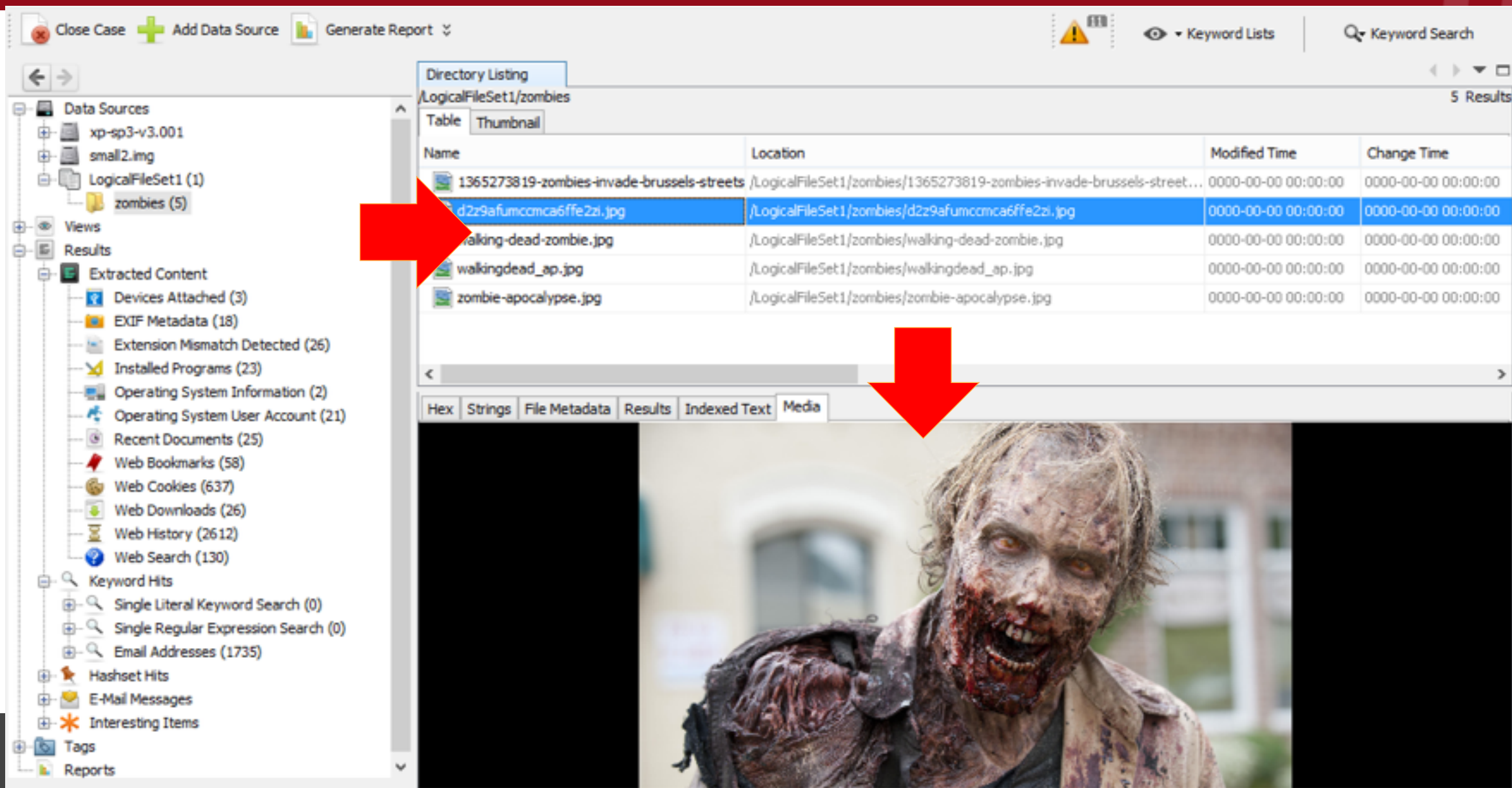
Directory Listing

LogicalFileSet1/zombies 5 Results

Table Thumbnail

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
d2z9afumcmca6ffe2zi.jpg	/LogicalFileSet1/zombies/d2z9afumcmca6ffe2zi.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

Hex Strings File Metadata Results Indexed Text Media



The image shows a forensic analysis tool interface. The left sidebar contains a tree view of data sources and results. The main pane displays a directory listing of files in a 'zombies' folder. A red arrow points from the 'd2z9afumcmca6ffe2zi.jpg' file in the table to a large image viewer at the bottom, which shows a zombie character from 'The Walking Dead'.

File Viewers

View a file in the most relevant way.

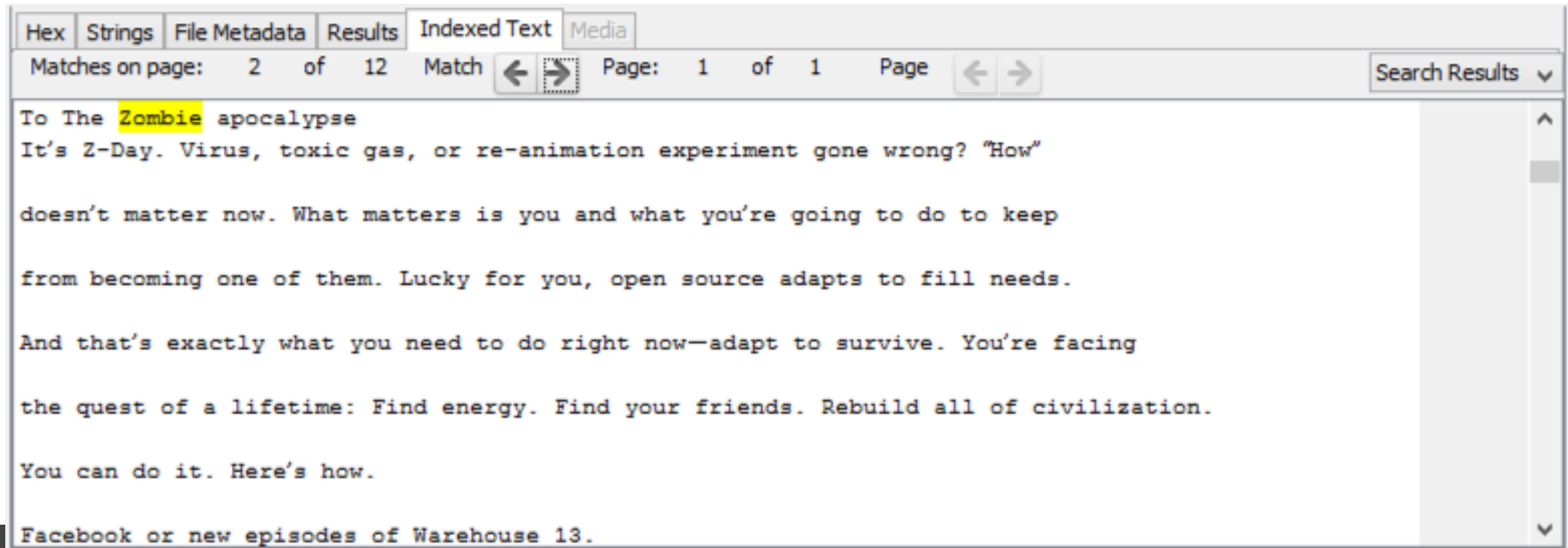
Images and video playback.



File Viewers

View a file in the most relevant way.

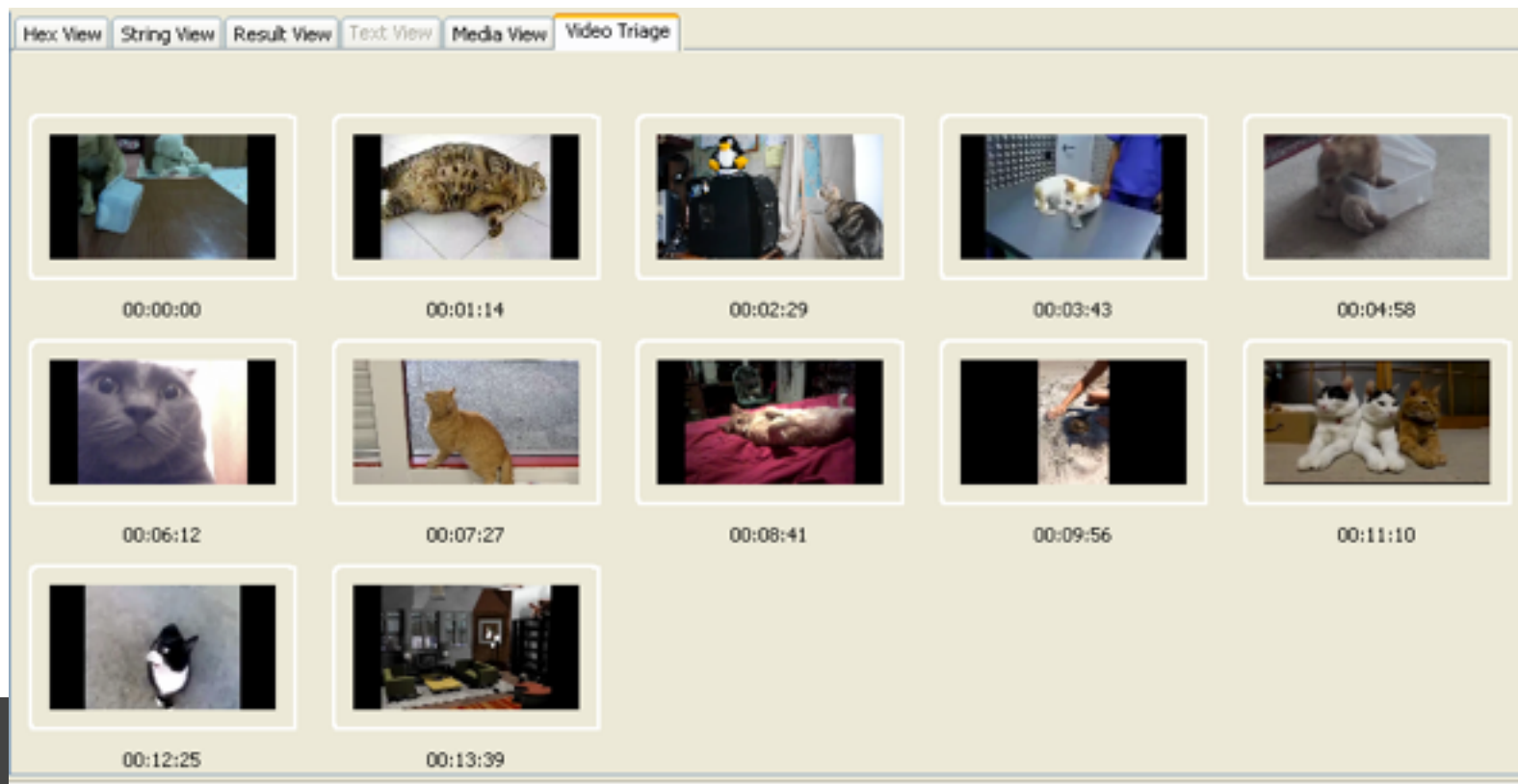
Text:



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

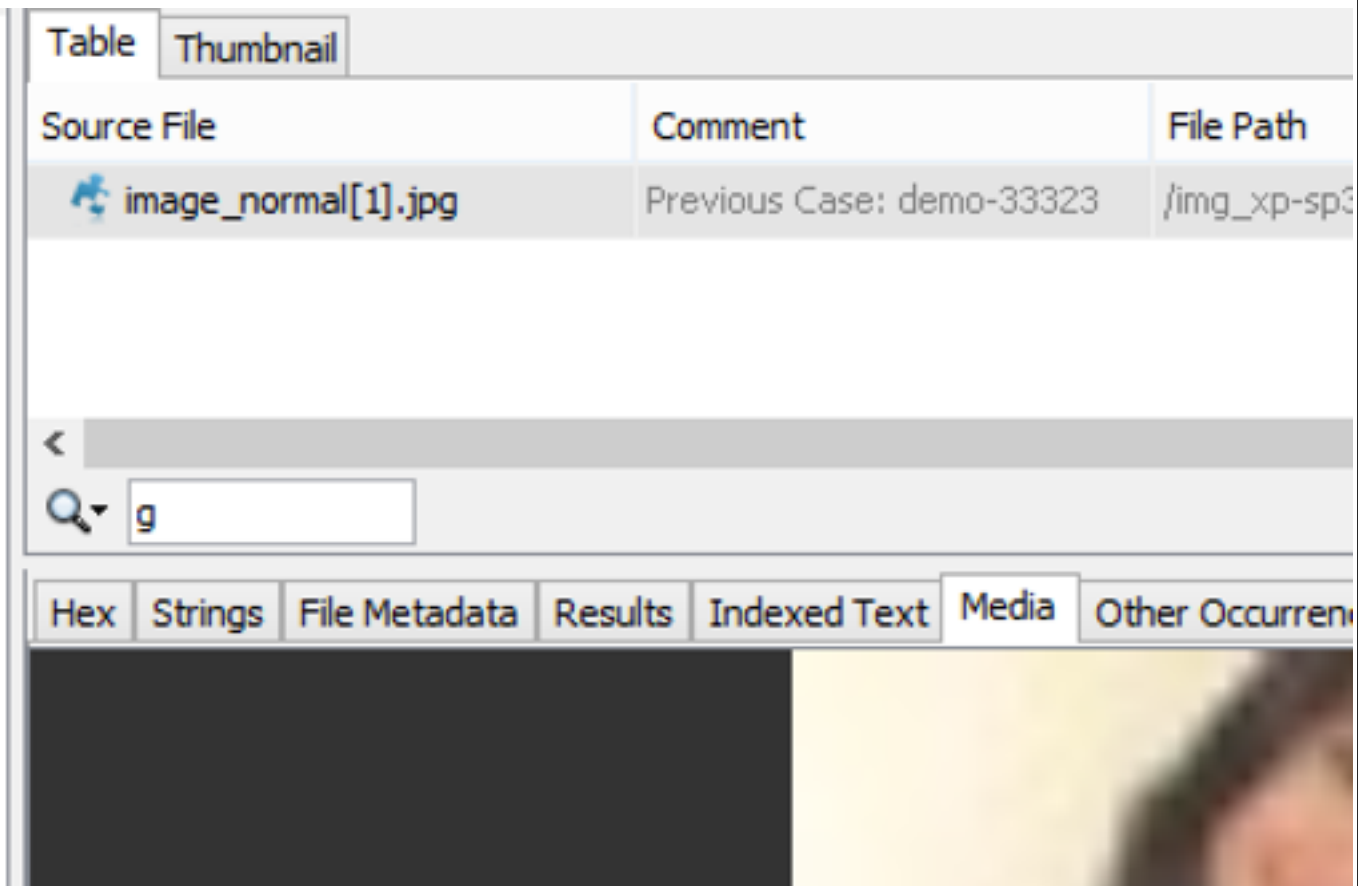
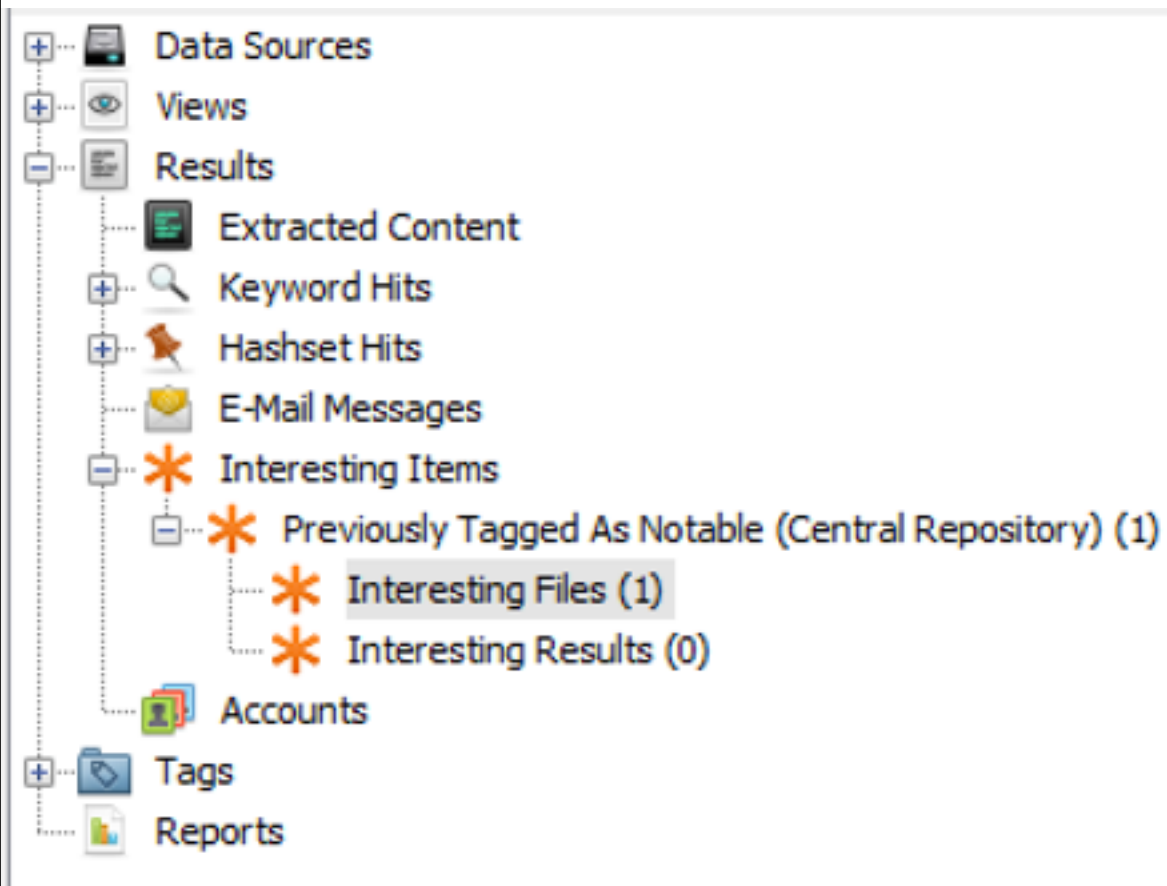
The Central Repository database stores:

- When each MD5, email, etc. has been seen
- What files and attributes were tagged as notable

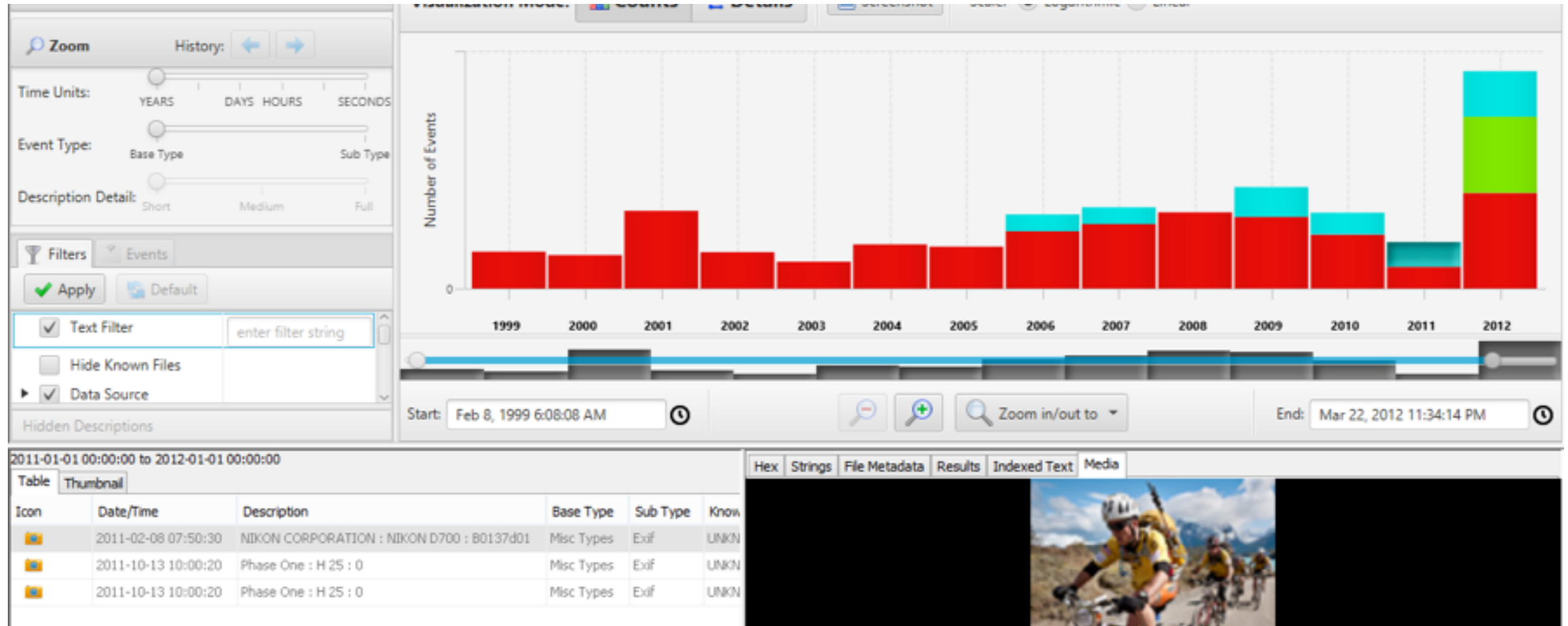
You can make connections with past cases that had common files or phone numbers.

When a previously notable item is seen again, it is automatically flagged.

Past Case Correlation



Timeline



Timeline

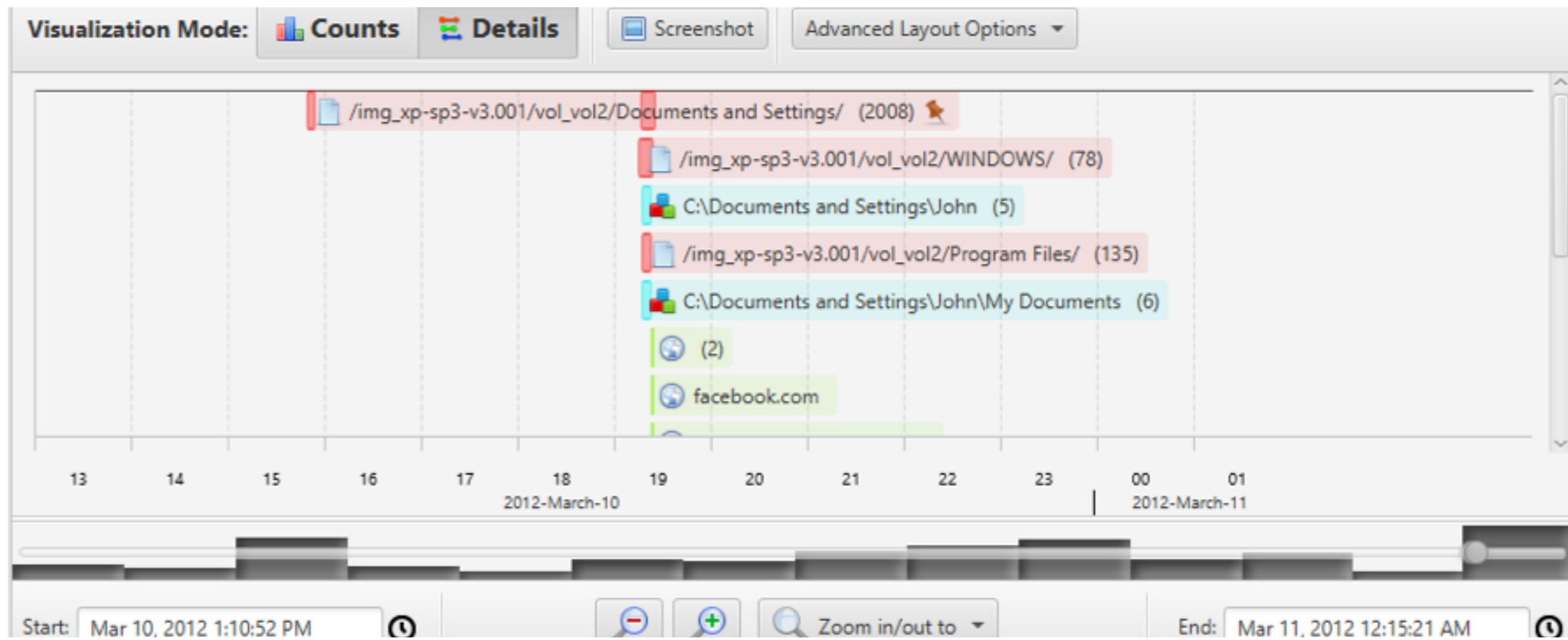


Image Gallery

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)

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

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

1365273819-zo...
d2z9afumccmca...
walking-dead-zo...
walkingdead_ap...
zombie-apocaly...

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

Group Viewing History: Back Forward Next Unseen group >>

Details

walkingdead_ap.jpg

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

The screenshot displays a software interface for analyzing mobile communications. It is divided into several sections:

- Filters:** Includes 'Devices' with checkboxes for 'biko_mmcbk0.bin' and 'outlook.dd', and 'Account Types' with checkboxes for Device, Phone, Email, Facebook, Twitter, Instagram, Facebook, MessagingApp, and Website. There are 'Uncheck All' and 'Check All' buttons for both sections.
- Date Range:** Labeled 'Date Range (America/New_York):', it has 'Start' and 'End' date pickers. The 'Start' date is 'September 22, 2018' and the 'End' date is 'October 13, 2018'.
- Account List:** A table with columns 'Account', 'Device', 'Type', and 'Msgs'. It lists various accounts including 'jean@m57.biz', 'googlealerts-noreply@google', 'newsletters@n.npr.org', 'alson@m57.biz', 'alex@m57.biz', 'bob@m57.biz', 'carol@m57.biz', and 'allsongs@n.npr.org'. Some device names are redacted with grey boxes.
- Message Details:** On the right, a pane shows details for a selected message from 'alex: alex@m57.biz'. It includes a header section with 'From', 'To', 'CC', and 'Subject' (FW: UFOs Over U.S. Military Sites?), a 'Show Images' button, and the message body text starting with 'on Friday, July 18, 2008' and 'Tonight: UFOs Over U.S. Military Sites?'.

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
- Github Issues

Basis Technology:

- Commercial support
- Access to engineers who can fix any issues.

Questions?

brianc <at> basistech.com

Connect on LinkedIn