7th Annual

#OSDFCon

OPEN SOURCE DIGITAL FORENSICS CONFERENCE

BASIS TECHNOLOGY

What's New or Under Appreciated in Autopsy

Brian Carrier

October 26, 2016 | Westin Washington Dulles, Herndon, VA

Agenda

- Welcome back Hash
- What is Autopsy
- What’s new in Autopsy since last year
- What’s on the roadmap
- What’s under appreciated

Welcome Back Hash

Hash The Hound
(128-bit)

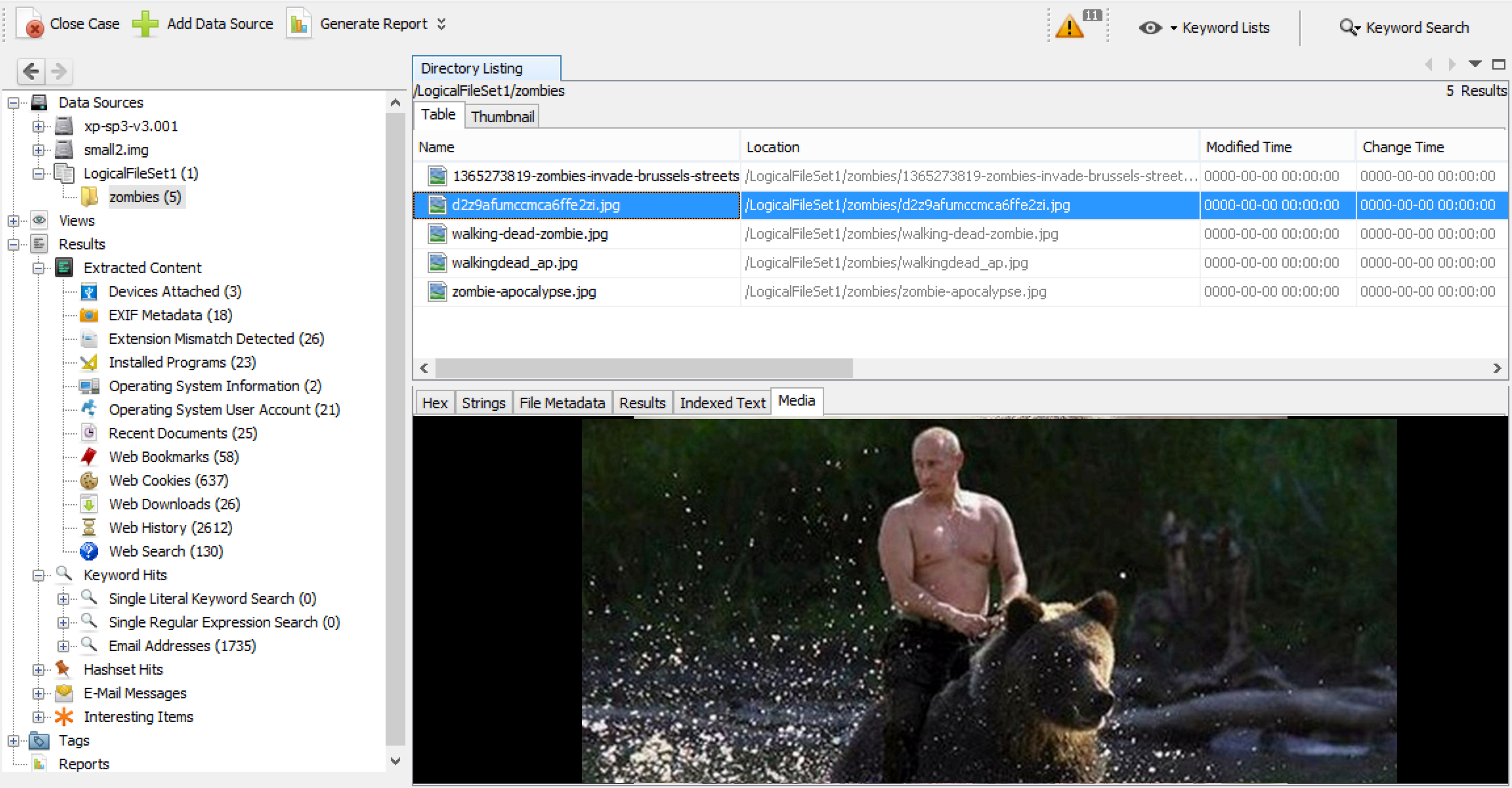
Renzik

Hash The Hound
(512-bit)

What is Autopsy?

Open Source Digital Forensics Platform

- **Open Source:** Reviewable, free, and customizable.
- **Digital Forensics:** Has the standard features you need and expect.
- **Platform:** Designed so that others can add functionality and plug-in modules.



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

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
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

Open Source Benefits

- Code is reviewable. Documented procedures for Daubert, etc.
- You are not tied into a vendor. Code lives on even if the vendor changes focus.
- Free. No cost to download or use. Many places will pay for training and support though.
  - Basis Technology provides both of them….

Digital Forensics Features

- Standard file systems for hard drives and smart phones
- Hash calculation and lookup
- Indexed keyword search
- Web activity
- Registry via RegRipper tool.
- File type identification & extension mismatch
- EXIF
- E-mail
- ZIP
- Carving
- Android
- Timeline ….

Extensibility

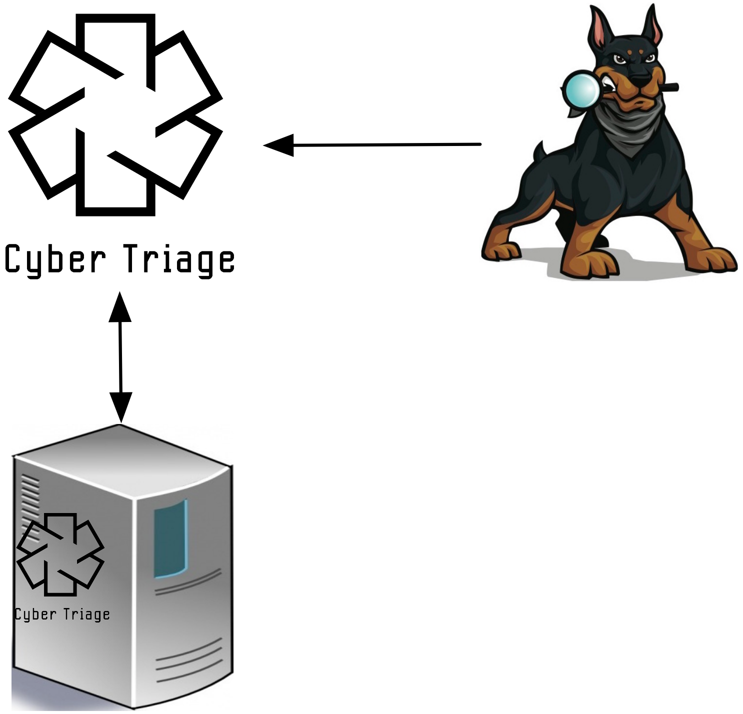
- Nearly everything is written as a module – even stuff we build.
- Examples:
  - Ingest modules analyze content from media
  - Content viewers display files in different ways
  - Report modules output data in different ways

- Can be written in Java or Python.

- We'll see lots of examples later with the module submissions.

Recent Example: Cyber Triage

1) Alert is generated from IDS / SIEM

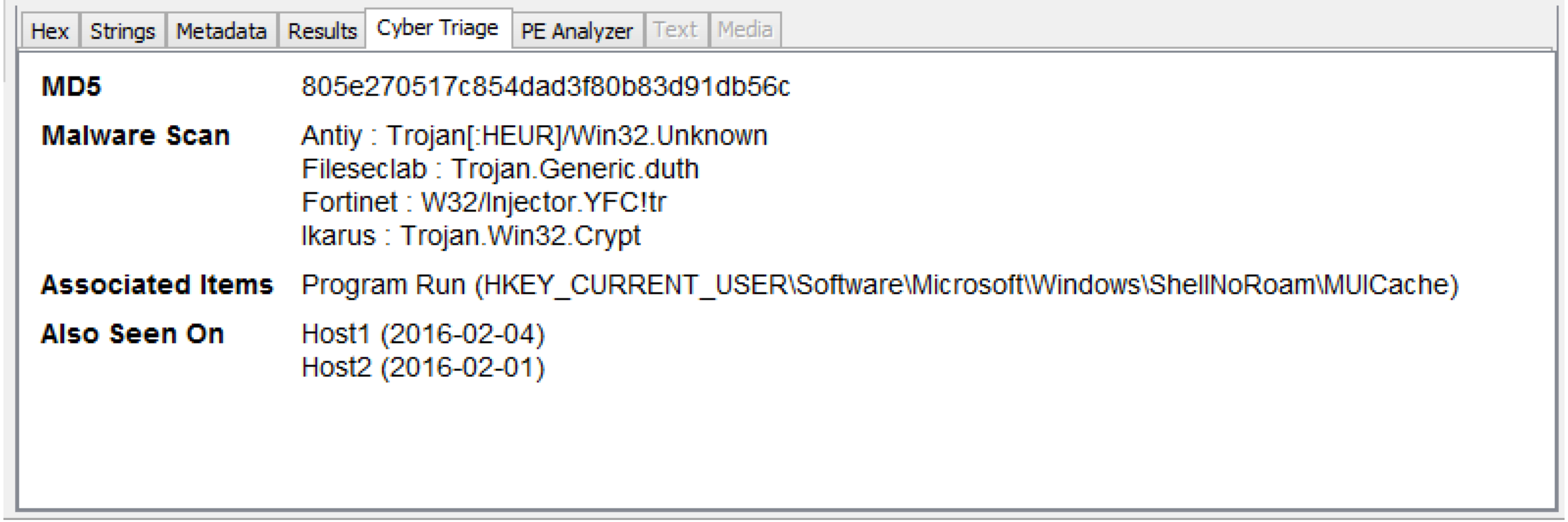


2) Cyber Triage is used on the live system to confirm & scope the alert.

3) If deep dive occurs, Autopsy can leverage Cyber Triage database contents.

Autopsy Module for Cyber Triage

- Custom content viewer queries Cyber Triage database.



MD5	805e270517c854dad3f80b83d91db56c
Malware Scan	Antiy : Trojan[:HEUR]/Win32.Unknown Fileseclab : Trojan.Generic.duth Fortinet : W32/Injector.YFC!tr Ikarus : Trojan.Win32.Crypt
Associated Items	Program Run (HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache)
Also Seen On	Host1 (2016-02-04) Host2 (2016-02-01)

- More info at: http://www.cybertriage.com

What's New Since Last Year

2016 in Summary

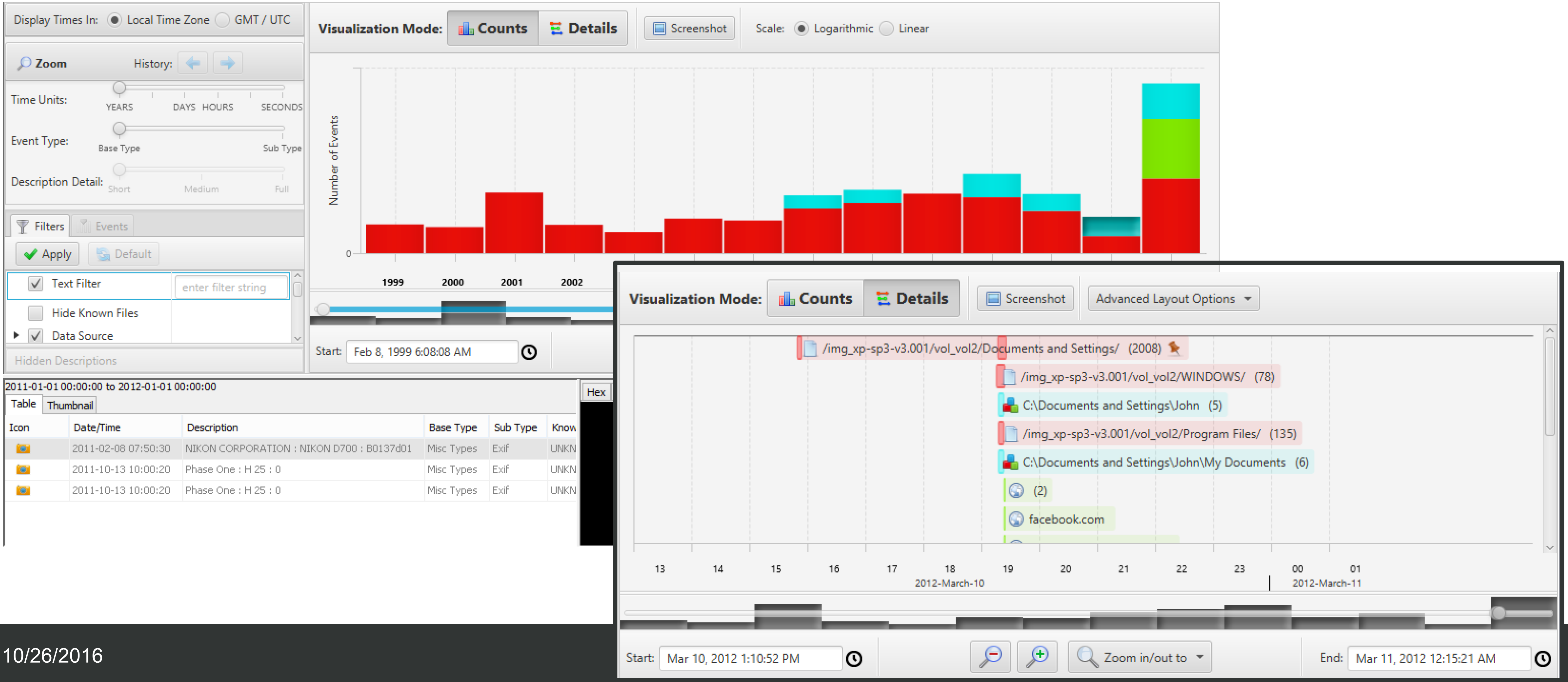
- A relatively quiet year
- Only 2 releases (4.1 and 4.2)!

- Features from DHS S&T funding
  - Timeline, Image Gallery, and Credit Card Searching
- Other smaller features
  - Virtual machines, indexing artifacts, etc.

- Let’s look at 2 highlights

Timeline: What Is It?

- Displays temporal data from a variety of places in a variety of ways.



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

Visualization Mode: Counts

Scale: ● Logarithmic ○ Linear

Time Units: YEARS

Event Type: Base Type

Description Detail: Short

☑ Text Filter

□ Hide Known Files

☑ Data Source

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

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

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

Visualization Mode: Details

/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)

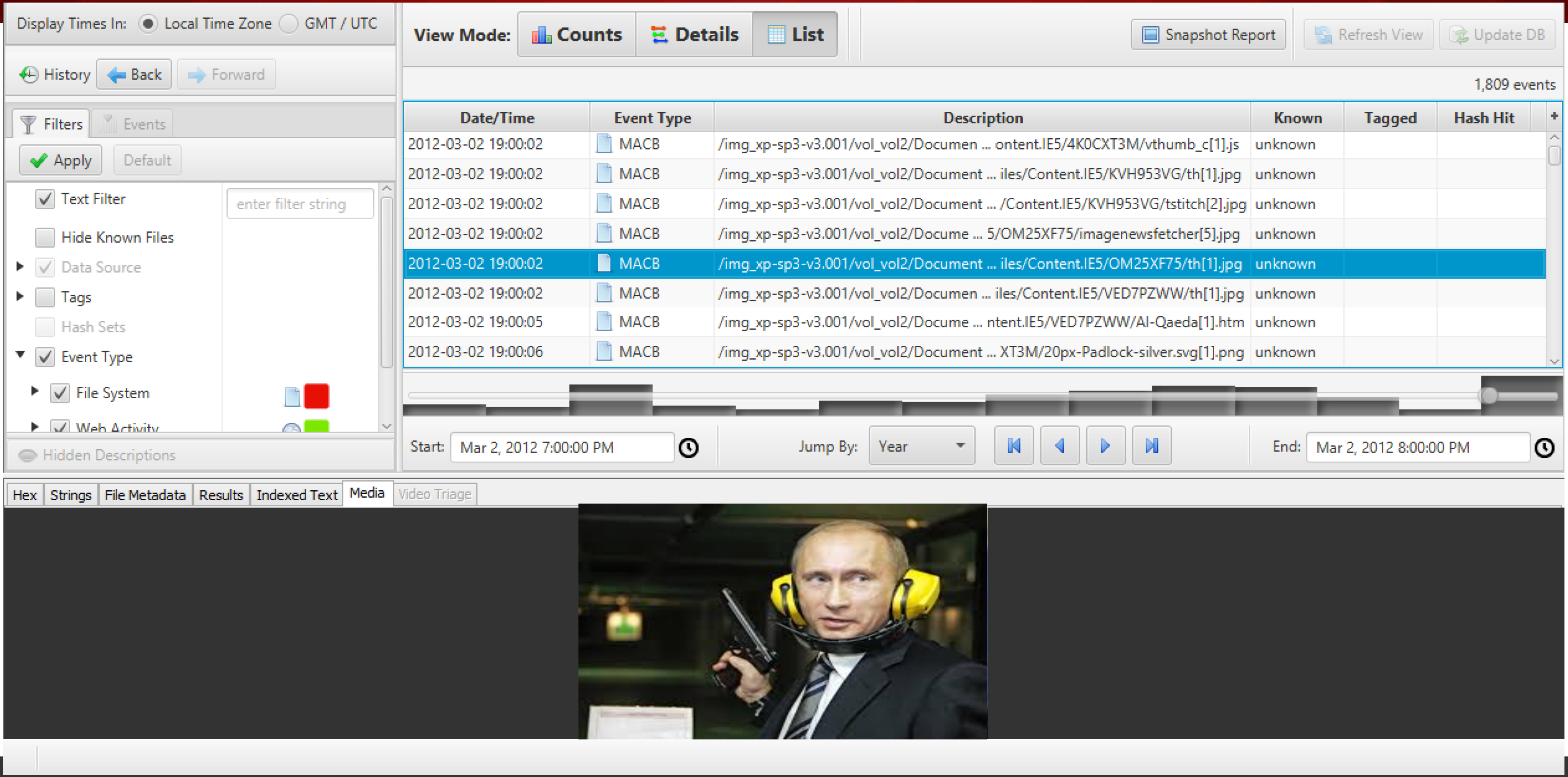
(2)

facebook.com

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

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

Timeline: New List View



1,809 events

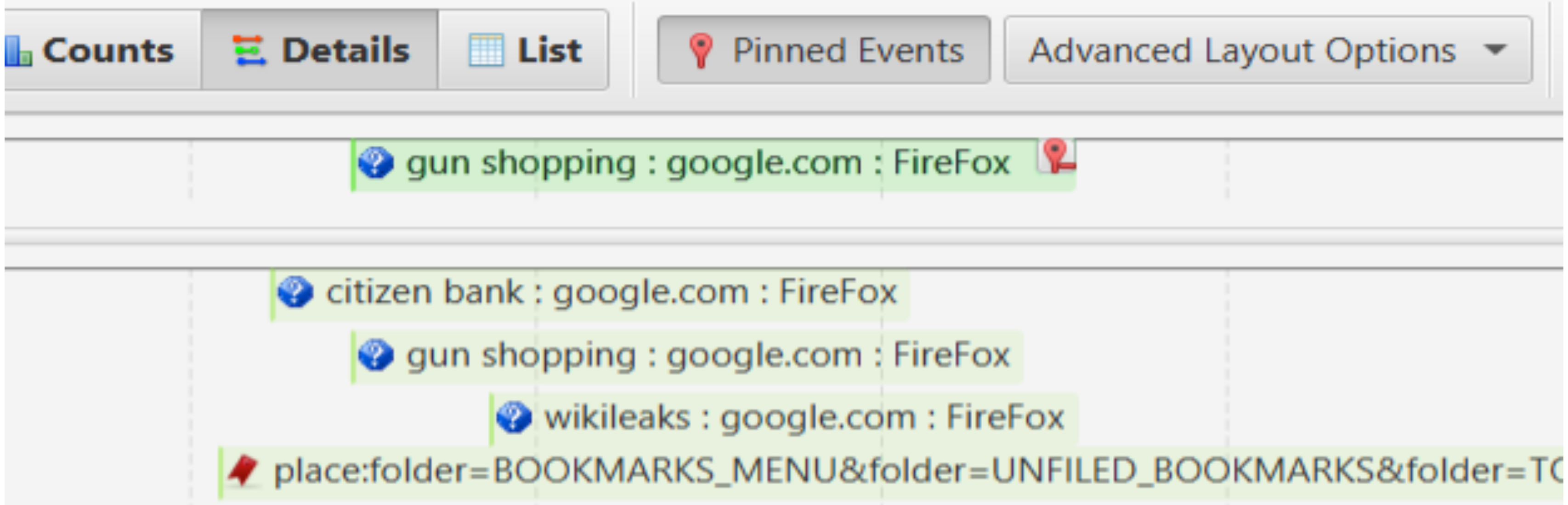
Date/Time	Event Type	Description	Known	Tagged	Hash Hit
2012-03-02 19:00:02	MACB	/img_xp-sp3-v3.001/vol_vol2/Documen ... ontent.IE5/4K0CXT3M/vthumb_c[1].js	unknown		
2012-03-02 19:00:02	MACB	/img_xp-sp3-v3.001/vol_vol2/Document ... iles/Content.IE5/KVH953VG/th[1].jpg	unknown		
2012-03-02 19:00:02	MACB	/img_xp-sp3-v3.001/vol_vol2/Document ... /Content.IE5/KVH953VG/tstitch[2].jpg	unknown		
2012-03-02 19:00:02	MACB	/img_xp-sp3-v3.001/vol_vol2/Docume ... 5/OM25XF75/imagenewsfetcher[5].jpg	unknown		
2012-03-02 19:00:02	MACB	/img_xp-sp3-v3.001/vol_vol2/Document ... iles/Content.IE5/OM25XF75/th[1].jpg	unknown		
2012-03-02 19:00:02	MACB	/img_xp-sp3-v3.001/vol_vol2/Documen ... iles/Content.IE5/VED7PZWW/th[1].jpg	unknown		
2012-03-02 19:00:05	MACB	/img_xp-sp3-v3.001/vol_vol2/Docume ... ntent.IE5/VED7PZWW/Al-Qaeda[1].htm	unknown		
2012-03-02 19:00:06	MACB	/img_xp-sp3-v3.001/vol_vol2/Document ... XT3M/20px-Padlock-silver.svg[1].png	unknown		

Start: Mar 2, 2012 7:00:00 PM

End: Mar 2, 2012 8:00:00 PM

Timeline: Pinning an Event

- Use Case: You want to know what happened before and after a specific event.
- The pinning feature lets you “pin” the event to the top and scroll around to see what happened before and after.



gun shopping : google.com : FireFox

citizen bank : google.com : FireFox

gun shopping : google.com : FireFox

wikileaks : google.com : FireFox

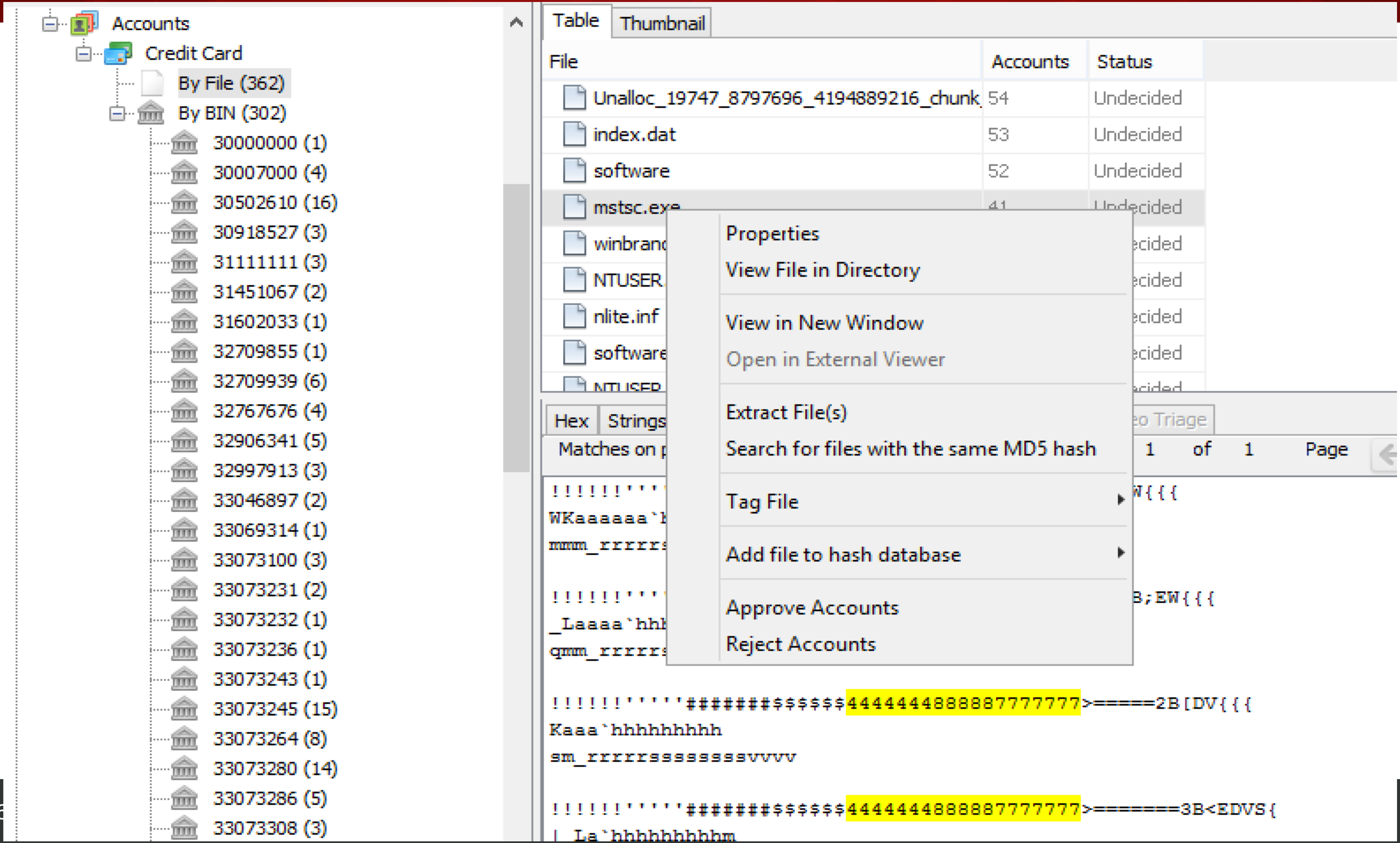
place:folder=BOOKMARKS_MENU&folder=UNFILED_BOOKMARKS&folder=TC

- See Jonathan’s talk for more details

Credit Card Searching

- Use Case: You need to search for credit card numbers on a drive and are getting a lot of false positives.
- How Does It Work:
  - Searches using regular expression.
  - Validates using Luhn check
  - Looks up Bank Identification Number (BIN) to provide bank details
  - Searches for additional track 1 & 2 data
  - User reviews results and can reject an entire file.
    - New concept into Autopsy – Rejected artifacts
- Thanks to those who helped.

Credit Card



- Accounts
  - Credit Card
    - By File (362)
    - By BIN (302)
      - 30000000 (1)
      - 30007000 (4)
      - 30502610 (16)
      - 30918527 (3)
      - 31111111 (3)
      - 31451067 (2)
      - 31602033 (1)
      - 32709855 (1)
      - 32709939 (6)
      - 32767676 (4)
      - 32906341 (5)
      - 32997913 (3)
      - 33046897 (2)
      - 33069314 (1)
      - 33073100 (3)
      - 33073231 (2)
      - 33073232 (1)
      - 33073236 (1)
      - 33073243 (1)
      - 33073245 (15)
      - 33073264 (8)
      - 33073280 (14)
      - 33073286 (5)
      - 33073308 (3)

File	Accounts	Status
Unalloc_19747_8797696_4194889216_chunk	54	Undecided
index.dat	53	Undecided
software	52	Undecided
mstsc.exe	41	Undecided
winbranc		cided
NTUSER.		cided
nlite.inf		cided
software		cided
NTUSER		cided

```
!!!!!!'''                         W{{{
WKaaaaaa`h
mmm_rrrrs

!!!!!!'''                         B;EW{{{
_Laaaa`hhh
qmm_rrrrs

!!!!!!'''''#######$$$$$$4444444888887777777>======2B[DV{{{
Kaaa`hhhhhhhhh
sm_rrrrrssssssssvvvv

!!!!!!'''''#######$$$$$$4444444888887777777>=======3B<EDVS{
| La`hhhhhhhhhm
```

What’s Coming in 2017

Experimental Module

- An add-on with features that can be enabled
- They were written for a specific use case and we want to get them out there, but they may not be ready for general use.
- They will be functionally stable, but may not yet have a stable programming API or general purpose interface.

Automated Ingest

- Use Case: You’ve got a pile of drives and want to get them analyzed quickly.
- How Does it Work:
  - You put images into a shared folder.
  - Autopsy Ingest Nodes (in a collaborative deployment) scan the folders, grab an image, and analyze it.
  - Autopsy Review Nodes allow users to see results from the analysis in real-time.
  - There are dashboards, shared configuration, and more.

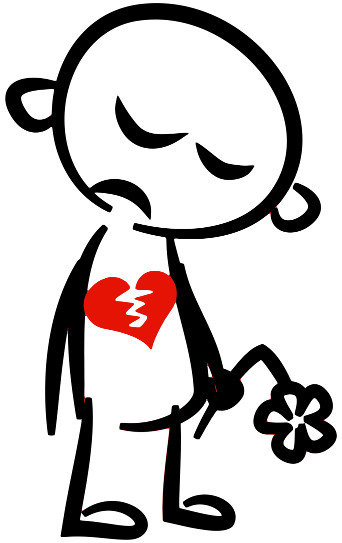
Search!

- Search in Autopsy has been ignored for too long.
- Right now, we are working on:
  - Performance improvements
  - Better (and faster) regular expression searches
    - Solr has evolved in the past 5 years!
  - Slack space
    - Database will have a row for slack space and it will be treated as a file.
- We are evaluating a change from Solr to Elastic.
  - If you have a strong opinion on why we should, please let us know.

Triage

- Use Case: You have limited time with an image / device and want to analyze a subset of the items.
- How Does It Work:
  - You add data source as usual.
  - You choose what files and folders to analyze.
    - Only those files will be hashed, keyword searched, etc.
    - All others will be ignored.
- You can focus on extensions, common folders, etc.

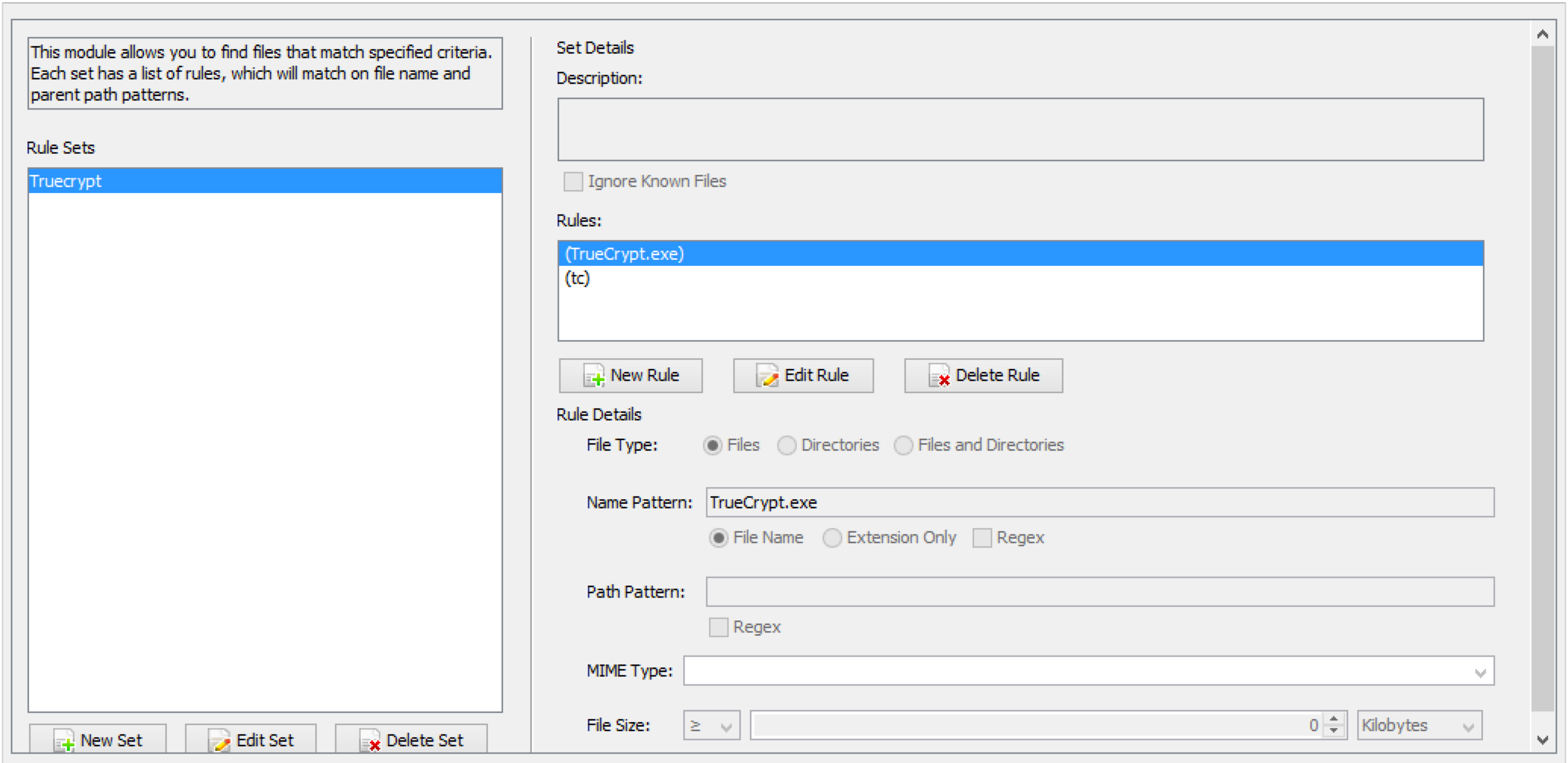
Under Appreciated Features (Less Understood)



Interesting Files

- What Is It: A module that flags files when they match a rule.
- Why Use It: To automate your checklist of things to look for.
- Examples:
  - True Crypt:
    - Files with .tc extension
    - Files named truecrypt.exe
    - Folder named TrueCrypt
  - iPhone Backup
    - Folder named “Backup” with “Apple Computer/MobileSync” in path

Using The Interesting Files Module



This module allows you to find files that match specified criteria. Each set has a list of rules, which will match on file name and parent path patterns.

Rule Sets

- Truecrypt

Set Details

Description:

□ Ignore Known Files

Rules:

- (TrueCrypt.exe)
- (tc)

Rule Details

File Type: ● Files ○ Directories ○ Files and Directories

Name Pattern: TrueCrypt.exe

● File Name ○ Extension Only □ Regex

Path Pattern:

□ Regex

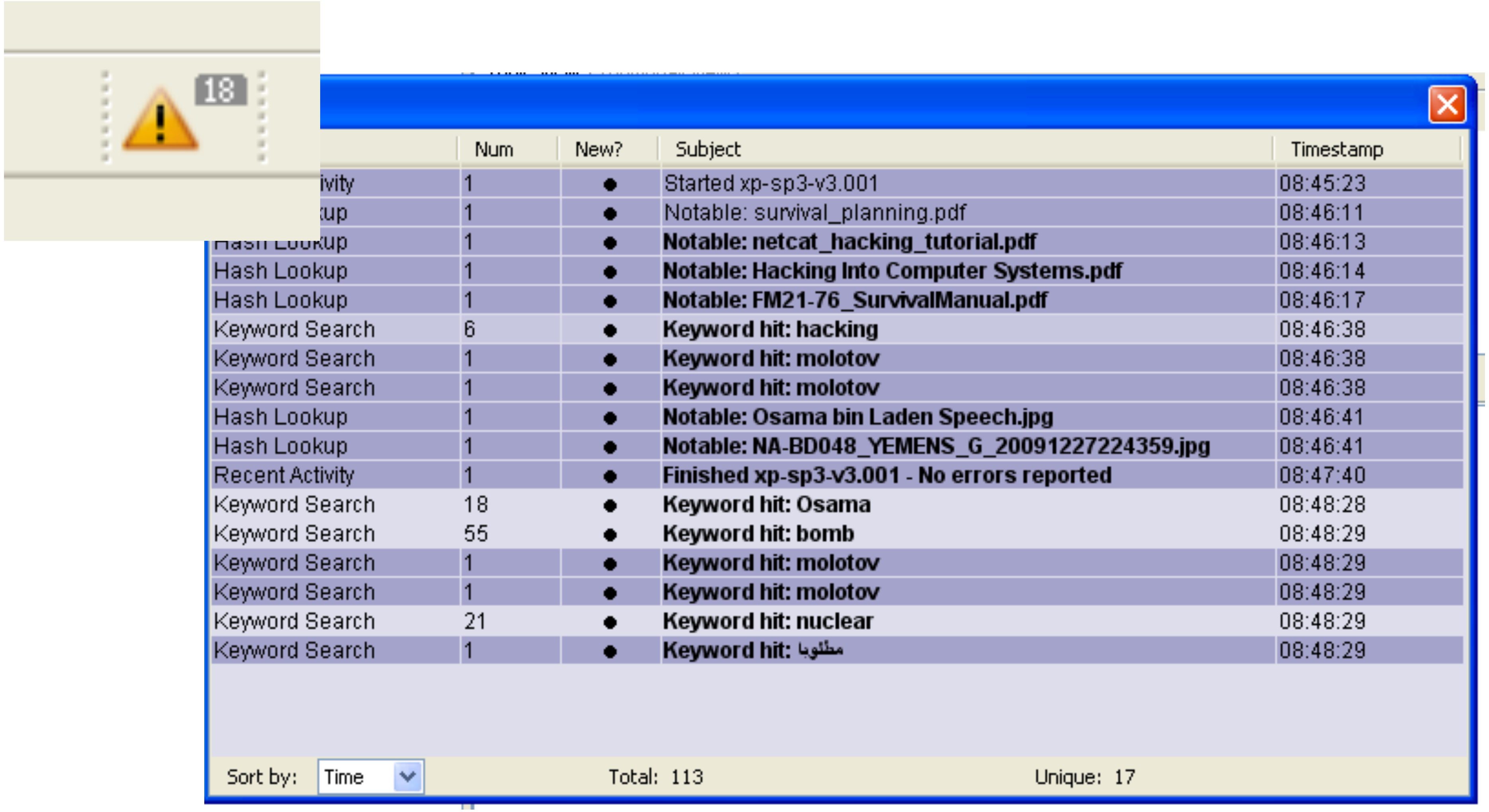
MIME Type:

File Size: ≥ 0 Kilobytes

Ingest Inbox

- What is It: Contains messages from modules that find data.
- Why Use It: Results are always being found in background and it’s hard to know when new things were found.
- Examples:
  - Each hashset hit sends a message.
  - You can be focused on something, such as web artifacts, for 10 minutes and then go to the inbox to see what was found during that 10 minutes.

Ingest Inbox



	Num	New?	Subject	Timestamp
ivity	1	●	Started xp-sp3-v3.001	08:45:23
up	1	●	Notable: survival_planning.pdf	08:46:11
Hash Lookup	1	●	**Notable: netcat_hacking_tutorial.pdf**	08:46:13
Hash Lookup	1	●	**Notable: Hacking Into Computer Systems.pdf**	08:46:14
Hash Lookup	1	●	**Notable: FM21-76_SurvivalManual.pdf**	08:46:17
Keyword Search	6	●	**Keyword hit: hacking**	08:46:38
Keyword Search	1	●	**Keyword hit: molotov**	08:46:38
Keyword Search	1	●	**Keyword hit: molotov**	08:46:38
Hash Lookup	1	●	**Notable: Osama bin Laden Speech.jpg**	08:46:41
Hash Lookup	1	●	**Notable: NA-BD048_YEMENS_G_20091227224359.jpg**	08:46:41
Recent Activity	1	●	**Finished xp-sp3-v3.001 - No errors reported**	08:47:40
Keyword Search	18	●	**Keyword hit: Osama**	08:48:28
Keyword Search	55	●	**Keyword hit: bomb**	08:48:29
Keyword Search	1	●	**Keyword hit: molotov**	08:48:29
Keyword Search	1	●	**Keyword hit: molotov**	08:48:29
Keyword Search	21	●	**Keyword hit: nuclear**	08:48:29
Keyword Search	1	●	**Keyword hit: مطلوبا**	08:48:29

Sort by: Time

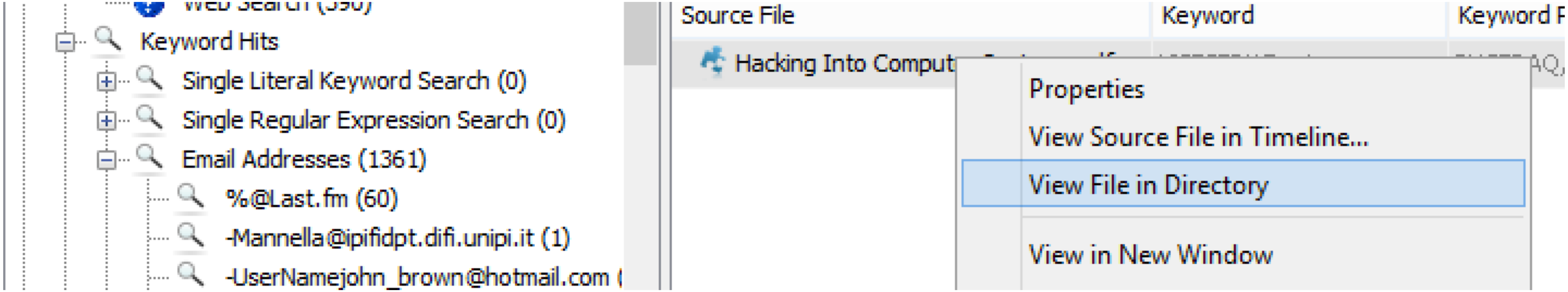
Total: 113

Unique: 17

View File in Directory

- What is It: Let’s you jump from a keyword or hash hit to its folder.
- Why Use It: Hashes and keywords get you some “bad stuff”, but there’s often more bad stuff in the same folder.
- Examples:
  - View the hash or keyword hits.
  - Verify it’s relevant.
  - Right click and choose “View File in Directory”.
  - It brings you to the folder.
  - Use the Back button to go back to the hash hits.

View File in Directory



Web Search (390)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (1361)
%@Last.fm (60)
-Mannella@ipifidpt.difi.unipi.it (1)
-UserNamejohn_brown@hotmail.com (
Source File
Keyword
Keyword P
Hacking Into Comput
Properties
View Source File in Timeline...
View File in Directory
View in New Window

Multi-user Cases

- What is It: Allow multiple examiners to work on the same case at the same time.
- Why Use It: Save time and make it easier to share results.
- Examples:
  - Large case comes into lab.
  - 3 examiners start working on different pieces of media.
  - Examiners can see either other’s tags and results to help their analysis.
  - Single report is generated at the end.

Try It Out!

- Download from www.sleuthkit.org
- Sign up for training at www.autopsy.com
- Get involved with the email lists and forum.
- Follow us on twitter: @sleuthkit