

# Happy Holidays From Renzik

What Happened in Autopsy in the Past Year

Brian Carrier

# It's That Time Of Year.....

---

- We get to tell you about all of the great things that happened in the past year!



## Side Note: Our Dogs.....

---

Renzik



Hash

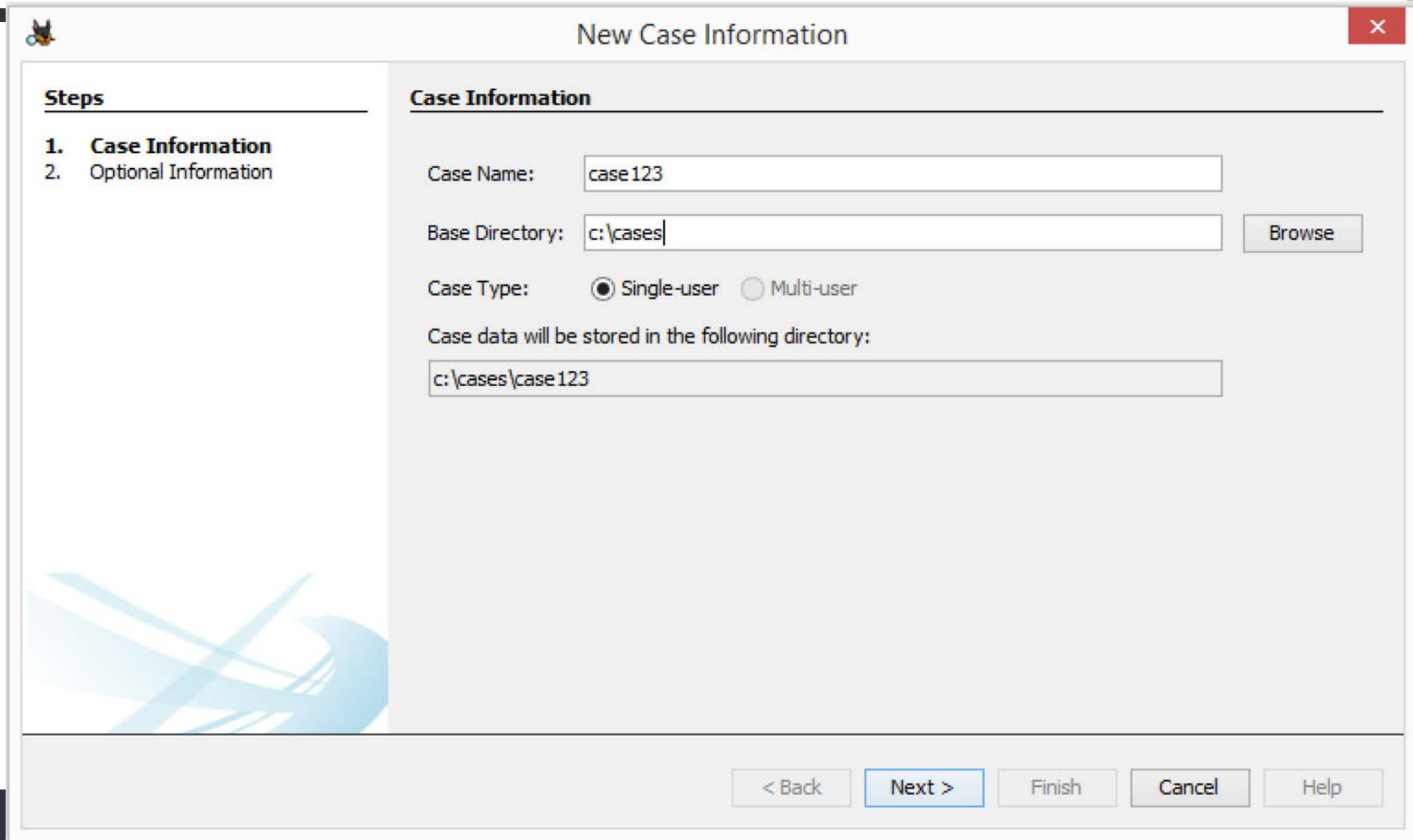


# What is Autopsy?

---

- Open source digital forensics platform.
- Designed to be:
  - Easy to use
  - Extensible with open plug-in frameworks
- Supports hard drives, media cards, and smart phone formats.
- Has all of the standard features, plus some unique features.
- Let's go through a typical workflow and point out the new features.
- “Intro to Autopsy” talk this afternoon will cover more of the basics.

# Make A Case



The image shows a 'New Case Information' dialog box with a title bar containing a small icon and a close button. The dialog is divided into two main sections: 'Steps' on the left and 'Case Information' on the right. The 'Steps' section lists two steps: '1. Case Information' and '2. Optional Information'. The 'Case Information' section contains several input fields and buttons. The 'Case Name' field is filled with 'case 123'. The 'Base Directory' field is filled with 'c:\cases' and has a 'Browse' button next to it. The 'Case Type' section has two radio buttons: 'Single-user' (selected) and 'Multi-user'. Below this, a text label states 'Case data will be stored in the following directory:', followed by a text field containing 'c:\cases\case 123'. At the bottom of the dialog, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

**Steps**

1. Case Information
2. Optional Information

**Case Information**

Case Name:

Base Directory:

Case Type: ☒ Single-user ☐ Multi-user

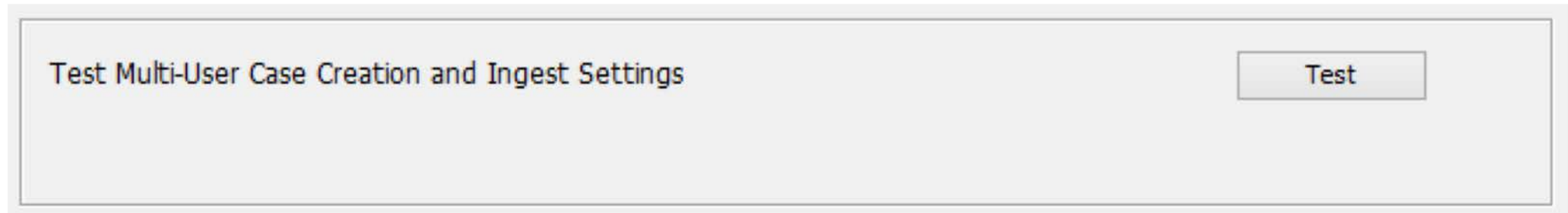
Case data will be stored in the following directory:

< Back   Next >   Finish   Cancel   Help


# Multi-user Case Documentation



- People were having trouble setting up multi-user clusters.
  - Usually because of user permissions and the Solr service.
- We updated the docs to help diagnose issues and added a test button to the “Auto Ingest” panel (i.e. running 24x7 and scanning for new images)



# Add A Data Source





Add Data Source


**Steps**


- 1. Select Type of Data Source To Add**
2. Select Data Source
3. Ingest Profile Selection
4. Configure Ingest Modules
5. Add Data Source


**Select Type of Data Source To Add**


 Disk Image or VM File

 Local Disk

 Logical Files

 Unallocated Space Image File

 Autopsy Logical Imager Results

OCTOBER 16, 2019 • HERNDON, VA • HOSTED BY  BASIS TECHNOLOGY






# Add A Data Source

**Add Data Source**

**Steps**

1. **Select Type of Data Source To Add**
2. Select Data Source
3. Ingest Profile Selection
4. Configure Ingest Modules
5. Add Data Source

**Select Type of Data Source To Add**

-  Disk Image or VM File
-  Local Disk
-  Logical Files
-  Unallocated Space Image File
-  Autopsy Logical Imager Results

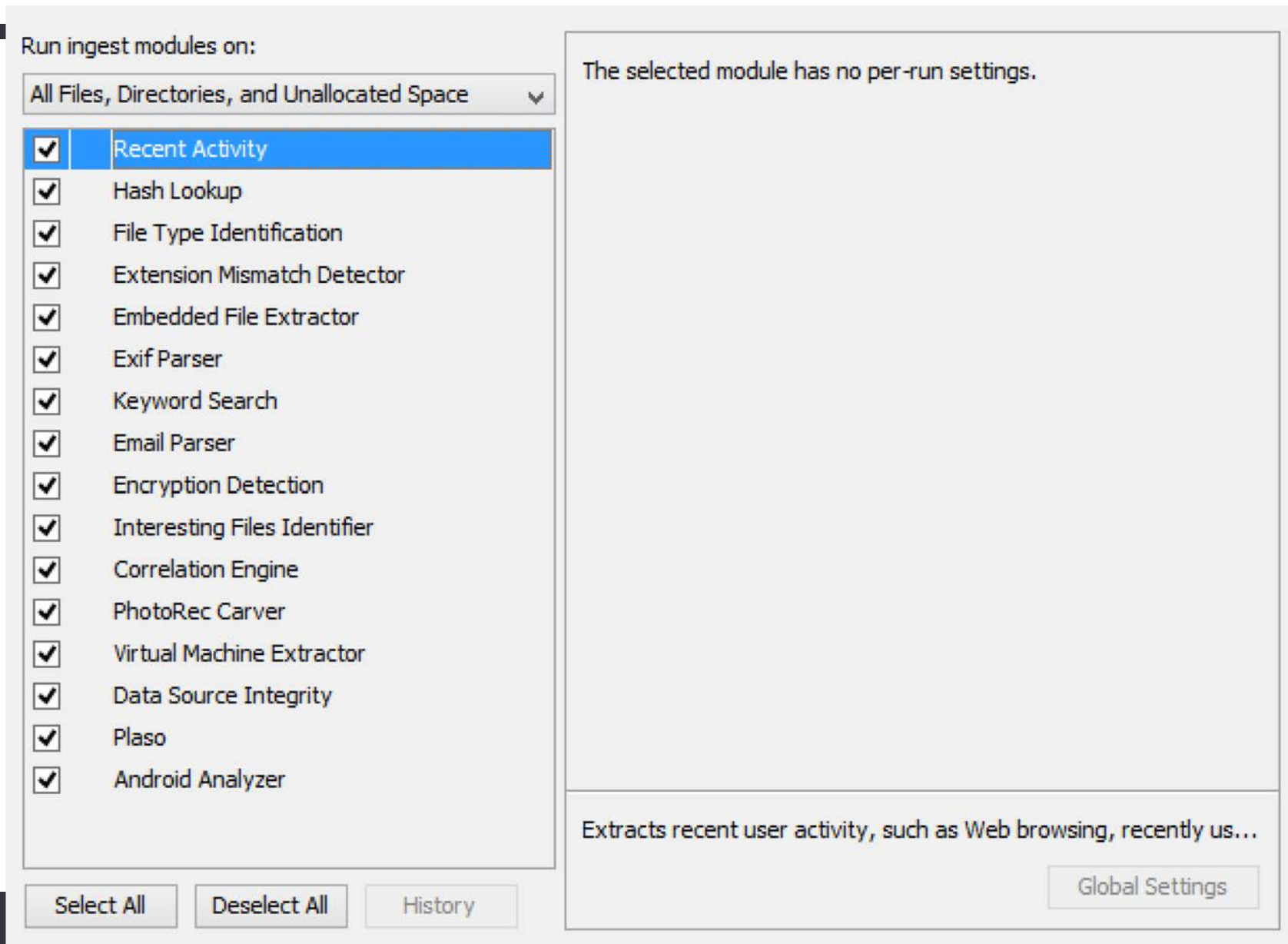


# Logical Imager



- Command line program that runs on target computer and collects:
  - Files (based on a set of rules)
  - System information (such as users)
- Parses raw drive data and the registry using The Sleuth Kit
- Unique Benefits:
  - Can access locked files and bypass rootkits that hide files
  - Does not update time stamps during search
  - Can access dual boot volumes (Linux for example)
  - Can create a full image if you keep it plugged in long enough.
- See Ann's talk later today for more details.

# Configure Ingest Modules to Analyze Data



Run ingest modules on:

All Files, Directories, and Unallocated Space ▼

- ☒ Recent Activity
- ☒ Hash Lookup
- ☒ File Type Identification
- ☒ Extension Mismatch Detector
- ☒ Embedded File Extractor
- ☒ Exif Parser
- ☒ Keyword Search
- ☒ Email Parser
- ☒ Encryption Detection
- ☒ Interesting Files Identifier
- ☒ Correlation Engine
- ☒ PhotoRec Carver
- ☒ Virtual Machine Extractor
- ☒ Data Source Integrity
- ☒ Plaso
- ☒ Android Analyzer

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Select All Deselect All History Global Settings

# Configure Ingest Modules

Run ingest modules on:

All Files, Directories, and Unallocated Space

- ☒ Recent Activity
- ☒ Hash Lookup
- ☒ File Type Identification
- ☒ Extension Mismatch Detector
- ☒ Embedded File Extractor
- ☒ Exif Parser
- ☒ Keyword Search
- ☒ Email Parser
- ☒ Encryption Detection
- ☒ Interesting Files Identifier
- ☒ Correlation Engine
- ☒ PhotoRec Carver
- ☒ Virtual Machine Extractor
- ☒ Data Source Integrity
- ☒ Plaso
- ☒ Android Analyzer

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...

Select All Deselect All History Global Settings

# Recent Activity Module

---

- Lots of features added from our DHS S&T contract.
- All of them came from “What’s Needed” and surveys from past OSDFCons.
- Web: Added Safari and Edge. Added form fill data to Firefox and Chrome. Added cache parsing to Chrome.
- Parse Zone.Identifiers to show source of downloaded files.
- Ported existing 3<sup>rd</sup> Party Modules (all from Mark McKinnon):
  - Recycle Bin: Make artifact and create file at original location.
  - ShellBag: Make artifacts (using RegRipper output)
  - Users: Parse more RegRipper output to simulate “Parse SAM” module

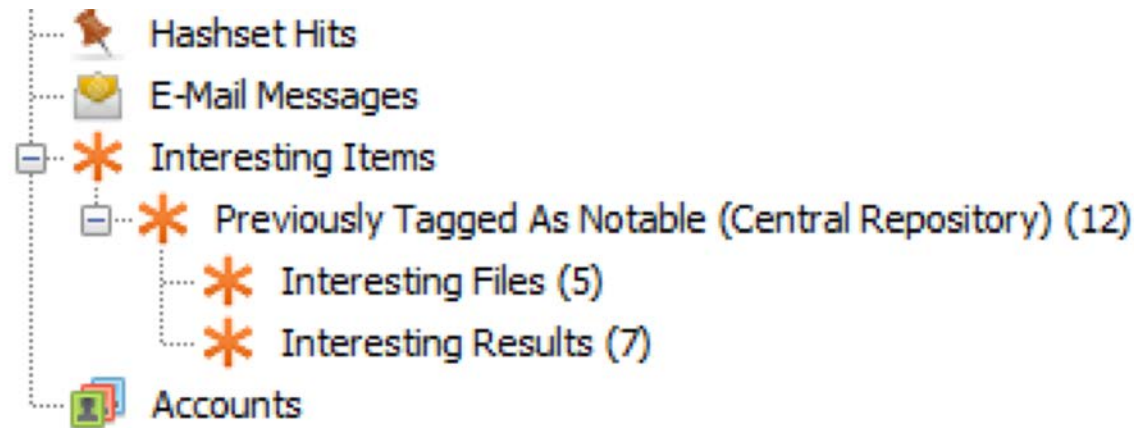
# Plaso & Email Modules

---

- Also from DHS S&T contract
- New Plaso module:
  - Creates events to be displayed in the timeline
- Updated Email module:
  - Added support for EML files. Based on Mark McKinnon's module.
  - Added support to make Contact Book Entries based on vCards

# Correlation Engine Module

- This module:
  - Saves artifacts to a central database for future correlation
  - Flags artifacts that were previously seen and marked as notable
- Updates:
  - More artifacts: SSID, MAC address, IMEI, IMSI, and ICCID



# Android Analyzer Module



---

- Added support for many more apps:
  - Browsers: Android browser, Opera, Samsung SBrowser
  - Messaging: Facebook Messenger, IMO, LINE, Skype, TextNow, Viber, WhatsApp
  - File Transfer: ShareIt, Xender, Zapy
  - ...
- Made it even easier to make 3<sup>rd</sup> party apps. 3 steps:
  - Find and open SQLite and associated WAL files with one call.
  - Query correct tables
  - Add artifacts for contacts, messages, etc. (one call each instead of 8 or 10).
- See talk later today for more details



# Case Opens Up

File View Tools Window Help

Close Case Add Data Source Generate Report

Keyword Lists Keyword Search


Directory Listing

Images

Table Thumbnail

Name	Location	Modified Time	Cl
buttonCenterFinished[1].png	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-01-20 18:13:32 EST	20
adobe.lpf.background-image.page-headlines.	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-01-20 17:29:47 EST	20
Ambox_content[1].png	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-03-02 19:00:06 EST	20
16px-Folder_Hexagonal_Icon.svg[1].png	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-03-02 18:57:16 EST	20
1C292392A3EB692F156893FF1C2DE[1].jpg	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-03-02 19:09:11 EST	20
220px-Hasib_Hussain_leaving_Boots_the_Ch	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-03-02 18:57:16 EST	20
22px-Flag_of_Libya.svg[1].png	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-03-02 19:00:06 EST	20

Hex Strings File Metadata Results Indexed Text Media





# Basic UI Flow

File View Tools Window Help

Close Case Add Data Source Generate Report

Keyword Lists Keyword Search

Directory Listing

Images

Table Thumbnail

Name	Location	Modified Time	Cl
buttonCenterFinished[1].png	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-01-20 18:13:32 EST	20
adobe.lpf.background-image.page-headlines.	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-01-20 17:29:47 EST	20
Ambox_content[1].png	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-03-02 19:00:06 EST	20
16px-Folder_Hexagonal_Icon.svg[1].png	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-03-02 18:57:16 EST	20
1C292392A3EB692F156893FF1C2DE[1].jpg	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-03-02 19:09:11 EST	20
220px-Hasib_Hussain_leaving_Boots_the_Ch	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-03-02 18:57:16 EST	20
22px-Flag_of_Libya.svg[1].png	/img_xp-sp3-v3.001/vol_vol2/Documents and Settings/John/Local Se...	2012-03-02 19:00:06 EST	20

Hex Strings File Indexes Indexed Text Media

Results

- Extracted Content
  - Devices Attached (3)
  - EXIF Metadata (11)
  - Extension Mismatch Detected (39)
  - 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 (444)

Images (2435)

Videos (39)

Audio (138)


Archives (16)

Documents

Executable

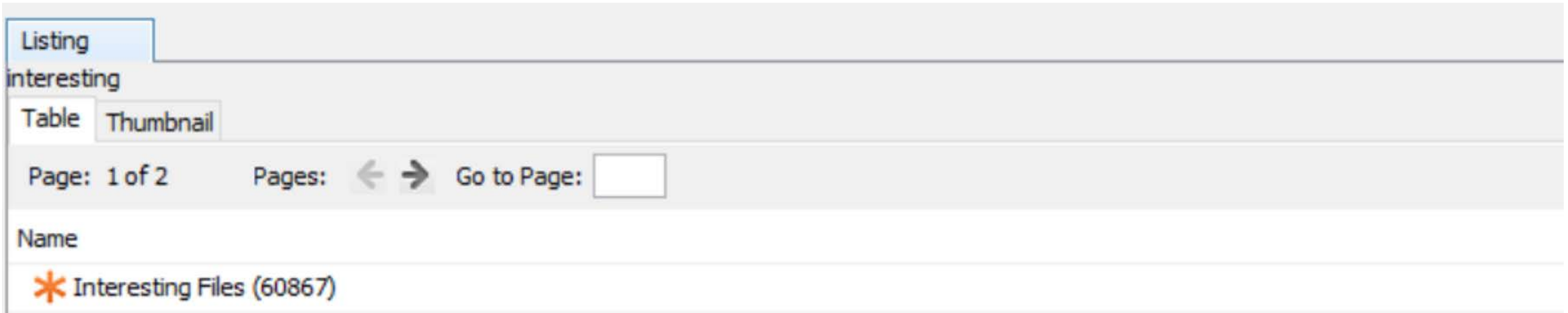
Deleted Files

MB File Size



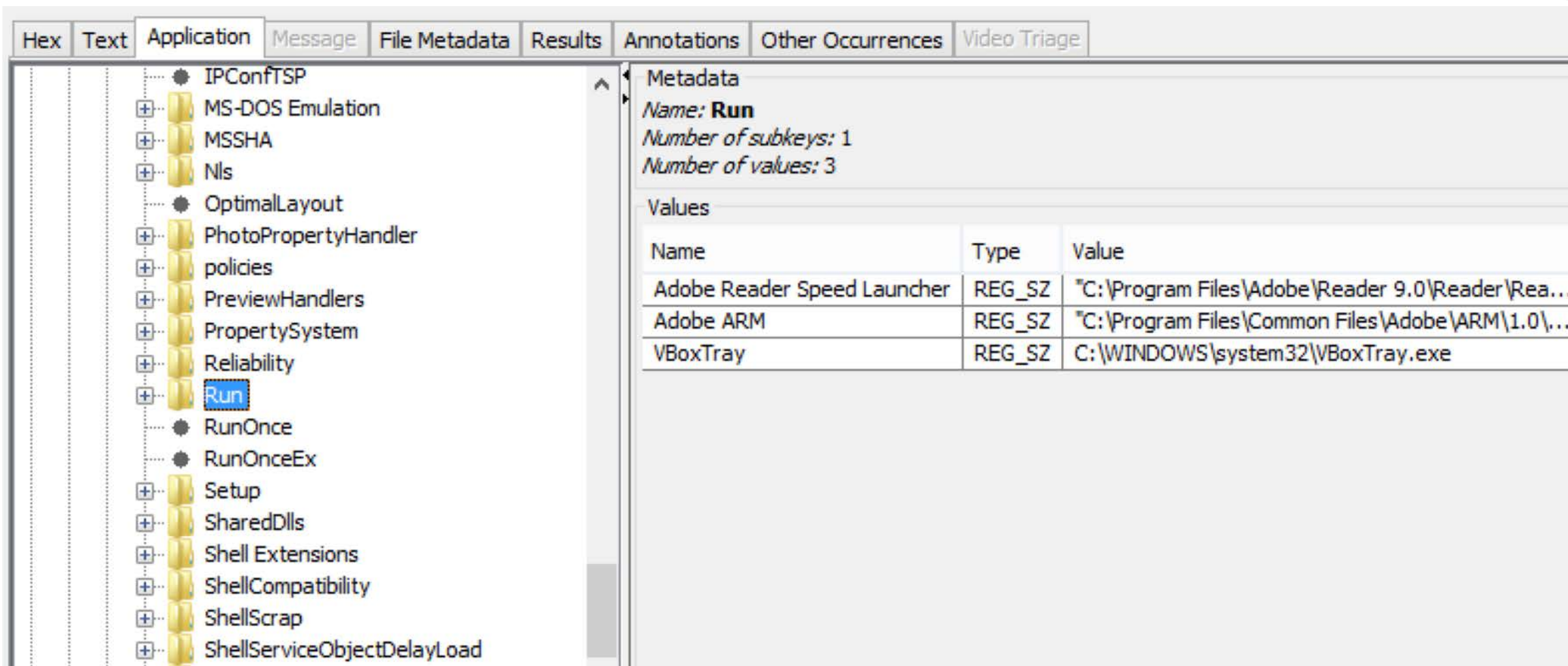
# Performance

- Several things were done to improve performance with large datasets
- Improved some backend queries
- Added paging everywhere



The screenshot shows a web application interface for a file listing. At the top, there is a tab labeled "Listing" and a sub-tab labeled "interesting". Below these, there are two buttons: "Table" and "Thumbnail". The "Table" button is currently selected. Below the buttons, there is a pagination section that includes the text "Page: 1 of 2", "Pages:", a left arrow, a right arrow, and "Go to Page:" followed by an input field. Below the pagination section, there is a section titled "Name" which contains a single entry: an orange asterisk icon followed by the text "Interesting Files (60867)".

# Content Viewer: Added Willi's Registry Viewer



The screenshot shows the Content Viewer application with the Registry Viewer tab selected. The left pane displays a tree of registry paths, with 'Run' selected. The right pane shows the metadata and values for the 'Run' registry key.

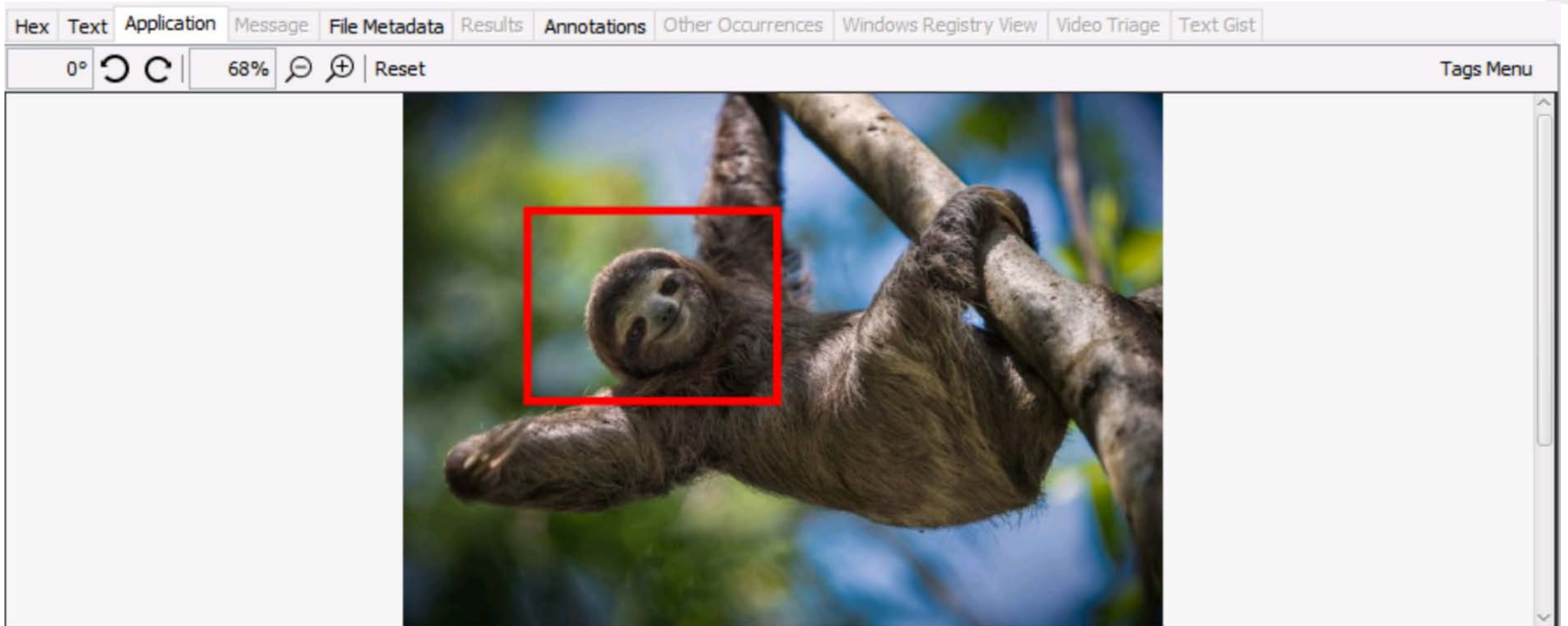
**Metadata**

- Name: **Run**
- Number of subkeys: 1
- Number of values: 3

**Values**

Name	Type	Value
Adobe Reader Speed Launcher	REG_SZ	"C:\Program Files\Adobe\Reader 9.0\Reader\Rea...
Adobe ARM	REG_SZ	"C:\Program Files\Common Files\Adobe\ARM\1.0\...
VBoxTray	REG_SZ	C:\WINDOWS\system32\VBoxTray.exe

# Content Viewer: Image Tags Can Have Boxes





# Content Viewer: Added HTML viewer

The screenshot displays a web-based Content Viewer interface. At the top, a table lists several files, with 'dsl\_b.htm' selected. Below the table, a tabbed interface shows the 'Application' view of the selected file. The content area displays an HTML form titled 'Setting up a high speed connection' with instructions for configuring DSL or cable modem settings. The form includes checkboxes for 'Obtain IP automatically' and 'Obtain DNS automatically', and input fields for 'Static IP address', 'Preferred DNS', and 'Alternate DNS'.

File Name	Path	Timestamp	Size
dsl_a.htm	/img_xp-sp3-v4.E01/vol_vol2/WINDOWS/system...	2008-04-13 21:16:40 EDT	2012-01-20
dsl_b.htm	/img_xp-sp3-v4.E01/vol_vol2/WINDOWS/system...	2008-04-13 21:16:40 EDT	2012-01-20
icntlast.htm	/img_xp-sp3-v4.E01/vol_vol2/WINDOWS/system...	2008-04-13 21:16:40 EDT	2012-01-20
icntlast.htm	/img_xp-sp3-v4.E01/vol_vol2/WINDOWS/system...	2008-04-13 21:16:40 EDT	2012-01-20

Hex Text Application Message File Metadata Results Annotations Other Occurrences

Download Images

Setting up a high speed connection

Enter the following settings to set up your DSL or cable modem Internet account. You can get these settings from your Internet services provider: Enter the following settings to set up your LAN connection. You can get these settings from your network administrator:  
Please enter a valid setting.

Obtain IP automatically : ☐ Obtain DNS automatically : ☐

Static IP address:  Preferred DNS:

Subnet mask:  Alternate DNS:

# Content Viewer: Other Occurrences

- Shows past cases where a file or other artifact was seen
- Changed layout to make it easier to see unique case names

The screenshot displays the 'Other Occurrences' tab in a software interface. It features a table with three columns: 'Case', 'Data Source Name', and 'File Name'. The table lists five cases, with 'Case 4' selected. To the right of the table, there are three sections: 'Common Properties', 'File Details', and 'Data Source Details', each displaying specific information about the selected case and file.

Case	Data Source Name	File Name
Case 1	LogicalFileSet1	bird2.jpg
Case 2	LogicalFileSet1	bird2.jpg
Case 3		
Case 4		
Case 5		

**Common Properties**

Type: Files  
Value: 17a1c6277804784dccdeed865f556ae8  
Known Status: notable

**File Details**

File Path: /test files/animals/birds/bird2.jpg

**Data Source Details**

Name: LogicalFileSet1






**Case Details**

Name: Case 4  
Created Date: 2019/06/27 08:47:02 (EDT)

Central Repository Starting Date: 2019/06/27 08:42:38 (EDT) Found 12 instances in 5 cases and 6 data sources.

# Content Viewer: Added Translation Viewer

- Uses Google or Microsoft API (requires credentials)

Hex	Text	Application	Message	File Metadata	Results	Annotations	Other Occurrences
Strings	Indexed Text	Translation					
Matches on page: - of - Match  				Page: 1 of 21 Page  		Text Source: File Text 	

## 概要 [編集]

東京都が管轄する領域は東京都区部(東京23区)、多摩地域(26市)とある。東京都区部(東京23区)は、一つの都市として「東京」道府県でもある。都公認の「東京都」の英語表記はTokyo Metrがある。


人口は13,843,403人(2018年10月1日現在)。これは日本の都道

人口密度も日本の都道府県のなかで最も大きい。東京を中心とする人口だけで、ポーランド、アルジェリア、カナダのそれぞれの国、インドの都市圏に人口規模において追いつかれるものと見られて

## 行政機関、首長 [編集]

行政機関の集合体も「東京都」と言う。

Hex	Text	Application	Message	File Metadata	Results	Annotations	Other Occurrences
Strings	Indexed Text	Translation					

 Up to the first 5KB of text will be translated










Show: Translated Text

General [Edit] The jurisdiction of Tokyo is comprised of the Tokyo metropolitan area (23 wards of Tokyo), the Tama area (26 Subbranch offices of the Tokyo Islands (Oshima, Miyake, Hachijo, Ogasawara) (2 towns, 7 villages). Tokyo-ku (Tokyo 23 wa e located at the southernmost and most eastern end Japan to include the Ogasawara Islands, including the Okinoshima Islar ognized official of the metropolitan government.

There are other Tokyo Prefecture and Tokyo Metropolitan Prefecture. The population is 13,843,403 people (as of October 1

This is the largest population in Japan prefectures, accounting for more than 10% of the Japan population. The population c s the largest metropolitan area in the world with more than 37 million population. 34 percent of the Japan population is conce olitan population, Poland, Algeria and Canada, each of which rivals the entire country's population. The second-largest Mum million [note 4].

# Translation: File Names Too

Listing					
/LogicalFileSet5/Test files/Translation Testing					
Table Thumbnail					
Name	Original Name	S	C	O	Location
 Spain	España				/LogicalFileSet5/Test files/Translation Testing/España
 test					/LogicalFileSet5/Test files/Translation Testing/test
 Greece	Ελλάδα				/LogicalFileSet5/Test files/Translation Testing/Ελλάδα
 Russia's Federation	Росси́йская...				/LogicalFileSet5/Test files/Translation Testing/Росс...
 Russia	Росси́я				/LogicalFileSet5/Test files/Translation Testing/Росси́я
 Bahrain	البحرين				/LogicalFileSet5/Test files/Translation Testing/البحرين
 Japan	日本				/LogicalFileSet5/Test files/Translation Testing/日本
 Korean	한국어				/LogicalFileSet5/Test files/Translation Testing/한국어
 Four.txt	أربعة.txt				/LogicalFileSet5/Test files/Translation Testing/أربعة.txt

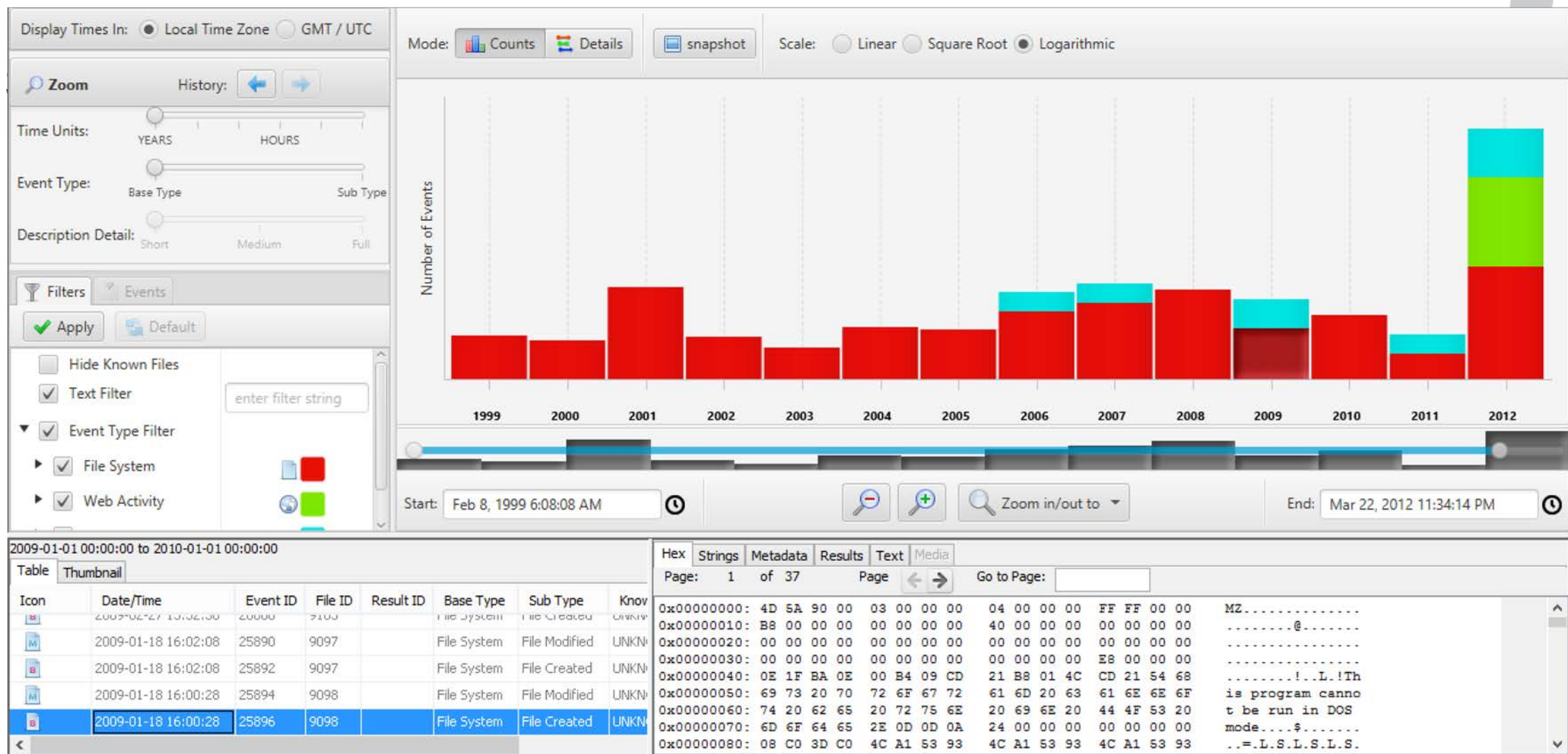


# Other Viewers

---

- Some data types need an interface more specific than the generic tree and table.
- All of those viewers received updates too:
  - Timeline
  - Image Gallery
  - Communications

# Timeline



# Timeline Enhancements

---

- No longer need to create timeline databases the first time it is opened.
  - It is now maintained as files and artifacts are created
- 3<sup>rd</sup> Party modules can now add events to the timeline.
- Users can manually create their own events.
  
- Nothing changed in the UI. Just backend changes.
- Timeline has been funded by DHS S&T

# Communications UI

The screenshot displays the 'Communications Visualization - Editor' application. The interface is divided into several sections:

- Filters:** Includes 'Devices' (target\_laptop.dd, target\_phone.bin) and 'Account Types' (Device, Phone, Email, Facebook, Twitter, Instagram, Facebook, MessagingApp, Website). Buttons for 'Apply', 'Refresh', 'Uncheck All', and 'Check All' are present.
- Account List:** A table with columns: Account, Device, Type, and Msgs. The 'example111@test.com' account is selected.
- Message List:** A table showing messages for the selected account. The selected message is an 'E-Mail' from 'example111@test.com' to 'example2@test.com' dated '2012-06-06 17:07:16'.
- Message Detail:** A detailed view of the selected message, showing the 'From', 'To', 'CC', and 'Subject' fields. The subject is 'Hi'.
- Date Range:** A section for filtering by date range, currently set to 'April 24, 2018' to 'May 15, 2018'.

The 'Messages' table data is as follows:

Type	From	To	Date
E-Mail	mail-noreply@google.com	example111@test.com	2012-06-06 17:06:19
E-Mail	mail-noreply@google.com	example111@test.com	2012-06-06 17:06:22
E-Mail	mail-noreply@google.com	example111@test.com	2012-06-06 17:06:22
E-Mail	example33333333@test.com	example111@test.com	2012-06-07 13:12:19
E-Mail	example111@test.com	example2@test.com	2012-06-06 17:07:16
E-Mail	example111@test.com	example2@test.com	2012-06-06 17:09:04
E-Mail	example111@test.com	example444@test.com	2012-06-07 12:50:39
E-Mail	example111@test.com	example2@test.com	2012-06-07 12:51:39
E-Mail	example111@test.com	example33333333@test.com	2012-06-07 18:46:52
E-Mail	example111@test.com	example2@test.com	2012-06-06 17:07:16
E-Mail	mail-noreply@google.com	example111@test.com	2012-06-06 17:06:19
E-Mail	mail-noreply@google.com	example111@test.com	2012-06-06 17:06:22
E-Mail	mail-noreply@google.com	example111@test.com	2012-06-06 17:06:22

The 'Account List' table data is as follows:

Account	Device	Type	Msgs
+12025551234	target_phone.bin	Phone	78
456	target_phone.bin	Phone	28
example111@test.com	target_laptop.dd	Email	13
12025551234	target_phone.bin	Phone	11
mail-noreply@google.com	target_laptop.dd	Email	6
+14105553456	target_phone.bin	Phone	5
example2@test.com	target_laptop.dd	Email	4
+14435550987	target_phone.bin	Phone	4
32665	target_phone.bin	Phone	4
130155555555	target_phone.bin	Phone	3
example33333333@test.com	target_laptop.dd	Email	2
example444@test.com	target_laptop.dd	Email	2
4435550987	target_phone.bin	Phone	2
12345009	target_phone.bin	Phone	2
	target_phone.bin	Phone	2
12345007	target_phone.bin	Phone	2
12345006	target_phone.bin	Phone	2
12345004	target_phone.bin	Phone	2
12345003	target_phone.bin	Phone	2
180	target_phone.bin	Phone	2
+15715556543	target_phone.bin	Phone	2
1511	target_phone.bin	Phone	2
12765552468	target_phone.bin	Phone	1

# Communications Updates

---

- Organize emails into threads and display messages by thread
- Added “Account Summary” tab to provide basics of an account (# of messages, other devices it was seen on, etc.)
- Added tab to show contact book entries
- Added tab to show image and video attachments
- Added filter to more easily focus on most recent messages
- Communications UI has been funded by DHS S&T


# Contacts


Summary

Messages

Contacts

Media Attachments

Name	Email	Phone Number
 Forrest Gump	forrestgump@example.com	(404) 555-1212



Forrest Gump

Properties

Source File	Forrest Gump
Name	Forrest Gump
Phone (Work)	(111) 555-1212
Phone (Voice)	(404) 555-1212
Phone Number (Home)	(404) 555-1212
Email (Pref)	forrestgump@example.com
Email (Internet)	forrestgump@example.com
Organization	Bubba Gump Shrimp Co.
Data Source	LogicalFileSet1
Name	Forrest Gump
Phone (Voice)	(404) 555-1212
Phone (Voice)	(111) 555-1212

# Common Property Search

---

- This feature matches files and other artifacts within a case or with past cases.
  - Finds patterns between devices and cases.
- Updates:
  - Updated the ways the results are shown
  - Can focus on certain file types when matching past cases
  - Can search past cases for specific artifact values (email, SSID, etc.)



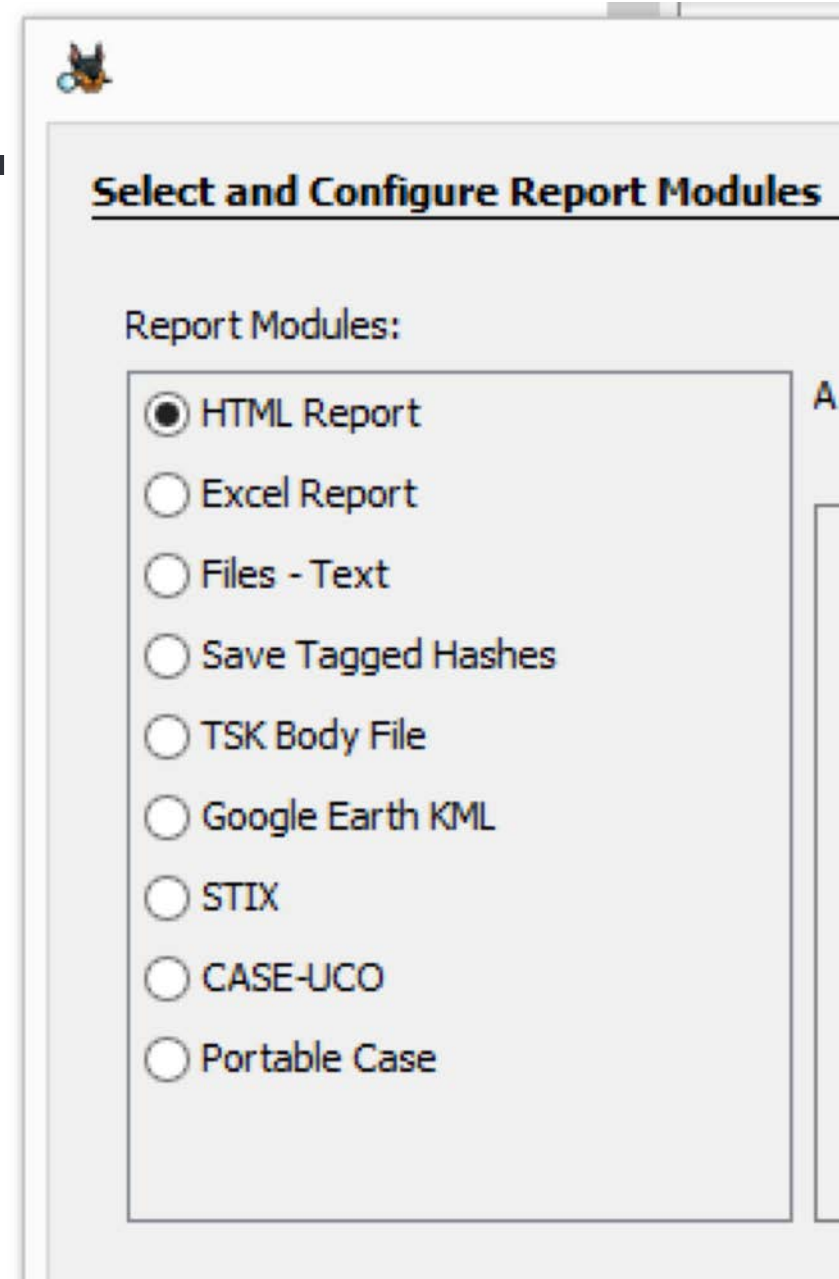
# New Past Case Matching Grouping

Listing Common Properties (All Central Repository Cases, All File Categories) ⌘					
Common Properties Results					
Table					
Name	Local Parent Path	MIME Type	Value	S	C
demo-case					
cr_test4.vhd1					
0002_s.txt	/0002/	text/plain	007cc81e9e06d4d0b582bf56406e967f		5
logs.db	/Android Folders/data/9333-com.sec....	application/x-sqlite3	031b467ac8306ecec08a493b80fd4b8		5
index.dat	logs.db RL testing/2/	application/octet-stream	0b0239d86b5fb7e47fe00cf148ffb45a		5
0004_e.txt	/0004/	text/plain	0cbf0ceab2335e54c8e4bb5e6b9ba30d		5
9223372034707292161	/Android Folders/data/12193-com.and...	text/xml	15d725172c2f54485ccb86e3f1883589		5
mmssms.db-shm	/Android Folders/data/12765-com.and...	application/octet-stream	16b4a62100ff96cd4dc0408610958233		5
\$TxfLogContainer00000000000000000001	/\$Extend/\$RmMetadata/\$TxfLog/	application/octet-stream	1a2183c9f6878c974b4693c15ebc2626		5
0000_x.txt	/0000/	text/plain	1a487c7525d23007763a22c50a8d0031		5



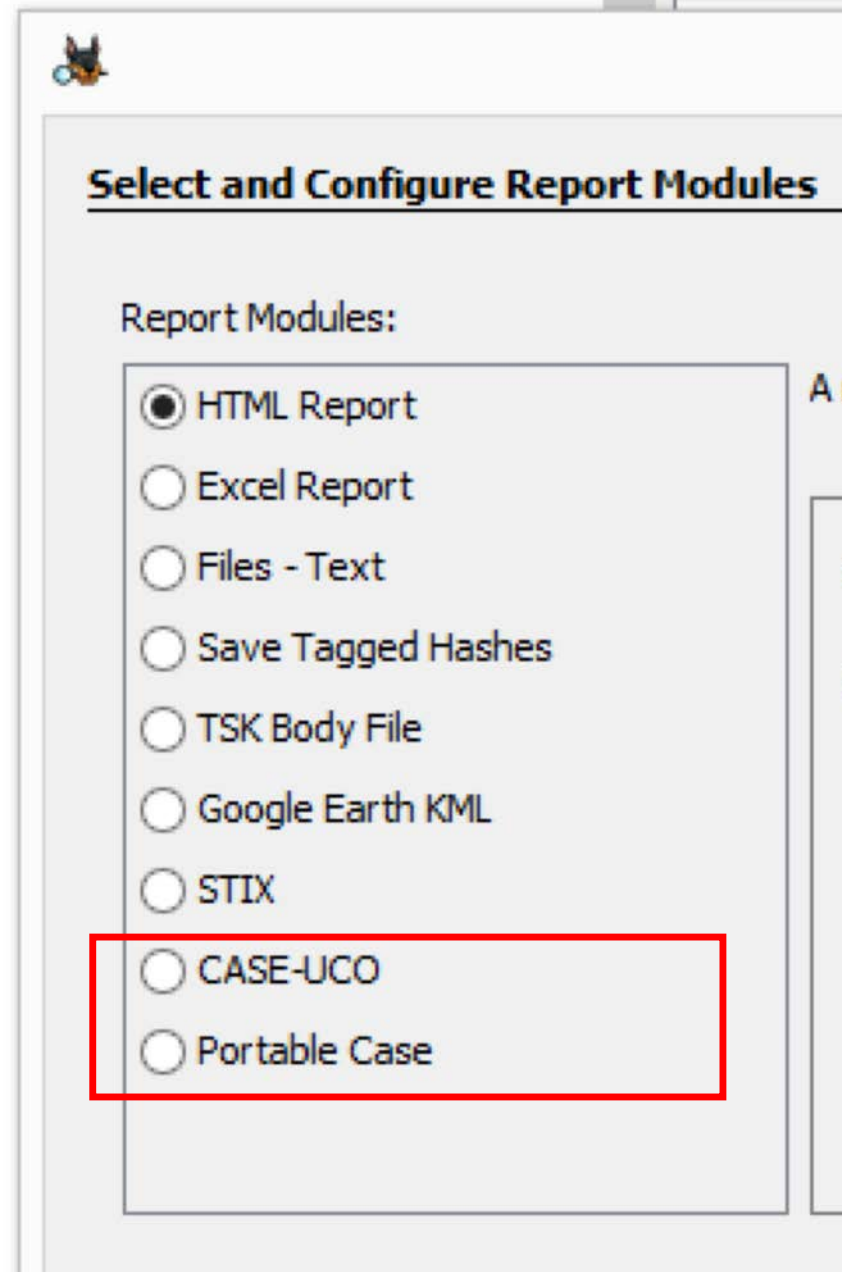
# Reporting

- At the end of the case, it's time to generate a report.



# Reporting

- At the end of the case, it's time to generate a report.



**Select and Configure Report Modules**

Report Modules:

- ☒ HTML Report
- ☐ Excel Report
- ☐ Files - Text
- ☐ Save Tagged Hashes
- ☐ TSK Body File
- ☐ Google Earth KML
- ☐ STIX
- ☐ CASE-UCO
- ☐ Portable Case

# CASE/UCO Report

---

- Is a manifest that contains information on all files in the case.
- CASE/UCO is a JSON format.
- Makes it easier to import into other tools.
- See the talk later today for more details.
  
- More CASE/UCO integrations coming this year.

# Portable Case

---

- Contains a subset of data from the original case.
  - Tagged files or others marked as “Interesting”
- Self contained folder with a SQLite case database and all relevant files.
- Resulting case can run ingest modules, tag files, etc.
- Can be compressed and split for easy transmission.
- Makes it easier to send data for review.

# Command Line



- You can now run Autopsy from the command line:

- Make Cases and Add Data Sources
- Run Ingest Modules
- Generate Reports

- Example:

```
> autopsy64.exe \  
    -createCase -caseName="case123" -caseBaseDir="C:\Cases" \  
    -addDataSource -dataSourcePath="C:\images\disk.bin" \  
    -runIngest -generateReports
```

- Requires you to preconfigure what modules to run.


# Linux / OS X

---

- Linux support stopped working this year because of Oracle's change to Java licensing.
- It now works again and we can use OpenJDK.
- It's just more complicated based on what distribution you use.

# http://forum.sleuthkit.org












- We setup a new forum site this year at Discourse (t.
- Thanks for the free hosting!
- It has had a lot of activity



Sign UpLog In

Q≡

all categories ▾LatestTopCategories

Topic		Replies	Views	Activity
<div>  <b>Welcome to the Autopsy and The Sleuth Kit Forum</b></div> <div>This site is for discussing the open source Autopsy and The Sleuth Kit tools. Users can ask questions here about using the tools. Developers can ask questions about building modules. Please submit any bug reports to t... <a href="#">read more</a></div>	 	1	4.7k	Apr 22
<b>7z (LZMA2 compression method) support : Embedded File Extraction Module</b>  Autopsy Help		0	11	18h
<b>How to access Linux partitions from Windows</b>  Autopsy Help	   	6	41	3d

# What's Coming

---

- New Search / Discovery UI
- Mobile and drones
- Updated keyword search
- REST APIs
- APFS / Logical Disk Management
- Updated Project Vic integration
- Online training
- ...



# We Need Your Support

---

- Nearly all of this was built with support for various organizations.
- It's always easier if we can point to increased usage and people who depend on this investment.
- If you are law enforcement, please reach out and let us know you are using this and what else you need.
  - We can then relay that to places like DHS S&T.

# Download and Contact

---

- Download the latest version from [autopsy.com](https://autopsy.com)
- You can get notifications from our email list or Twitter
- Basis Technology provides commercial support

Brian Carrier

brianc <at> basistech <dot> com

Connect on LinkedIn or Twitter  
(I'm low volume on both...)