



universidade
de aveiro

Computer Systems Forensic Analysis AFSC

Autopsy

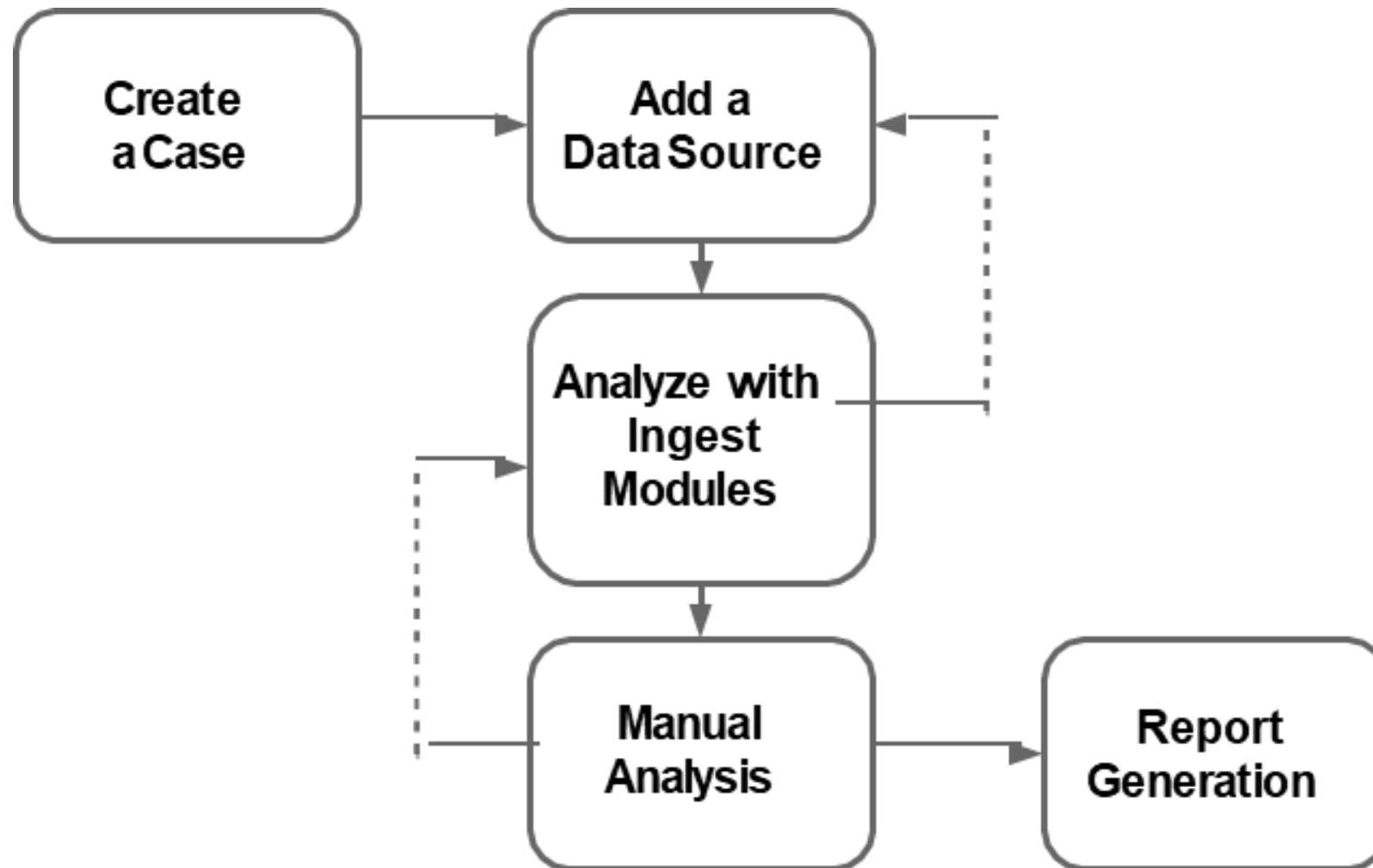
Artur Varanda

School Year 2023-2024

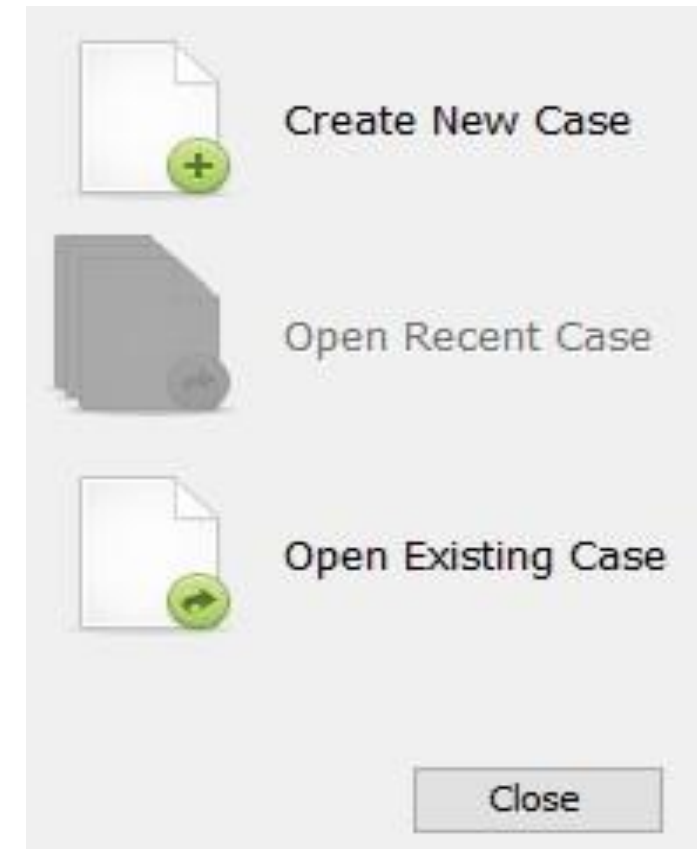
url: <https://www.autopsy.com>



- *Autopsy* is a graphical tool aimed at the digital investigation of images of storage media
- It is developed in Java, mainly for *Windows*
- It is expandable (supports modules developed in *Python* for Java)
- It has limited support for *Android*



1 - Create a Case



1 - Create a Case

- Case Information

Enter New Case Information:

Case Name:

Base Directory:

Case Type: ☒ Single-user ☐ Multi-user

Case data will be stored in the following directory:

1 - Create a Case

- Case Information
- Case number, examiner

Optional Information

Case

Number: NUIPC xxxxxxxx

Examiner

Name: MF

Phone:

Email:

Notes: Test

Organization

Organization analysis is being done f...

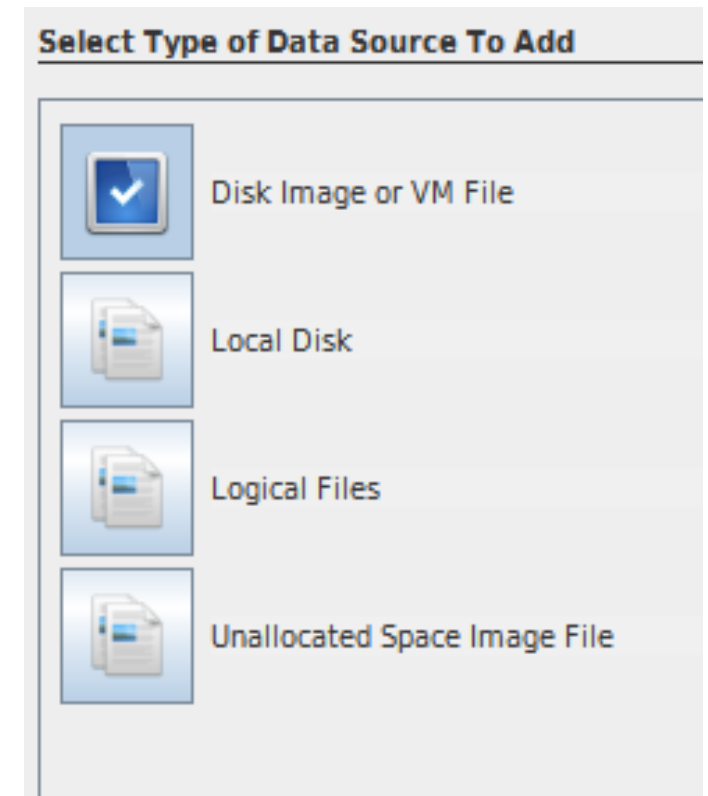
< Back Next > Finish

1 - Create a Case

- Case Information
- Case number, examiner

2 - Add a data source

- *Raw* (dd) or EnCase (E01) image
- Drives, files or local folders
- Virtual machine drives (vmdk, vhd)



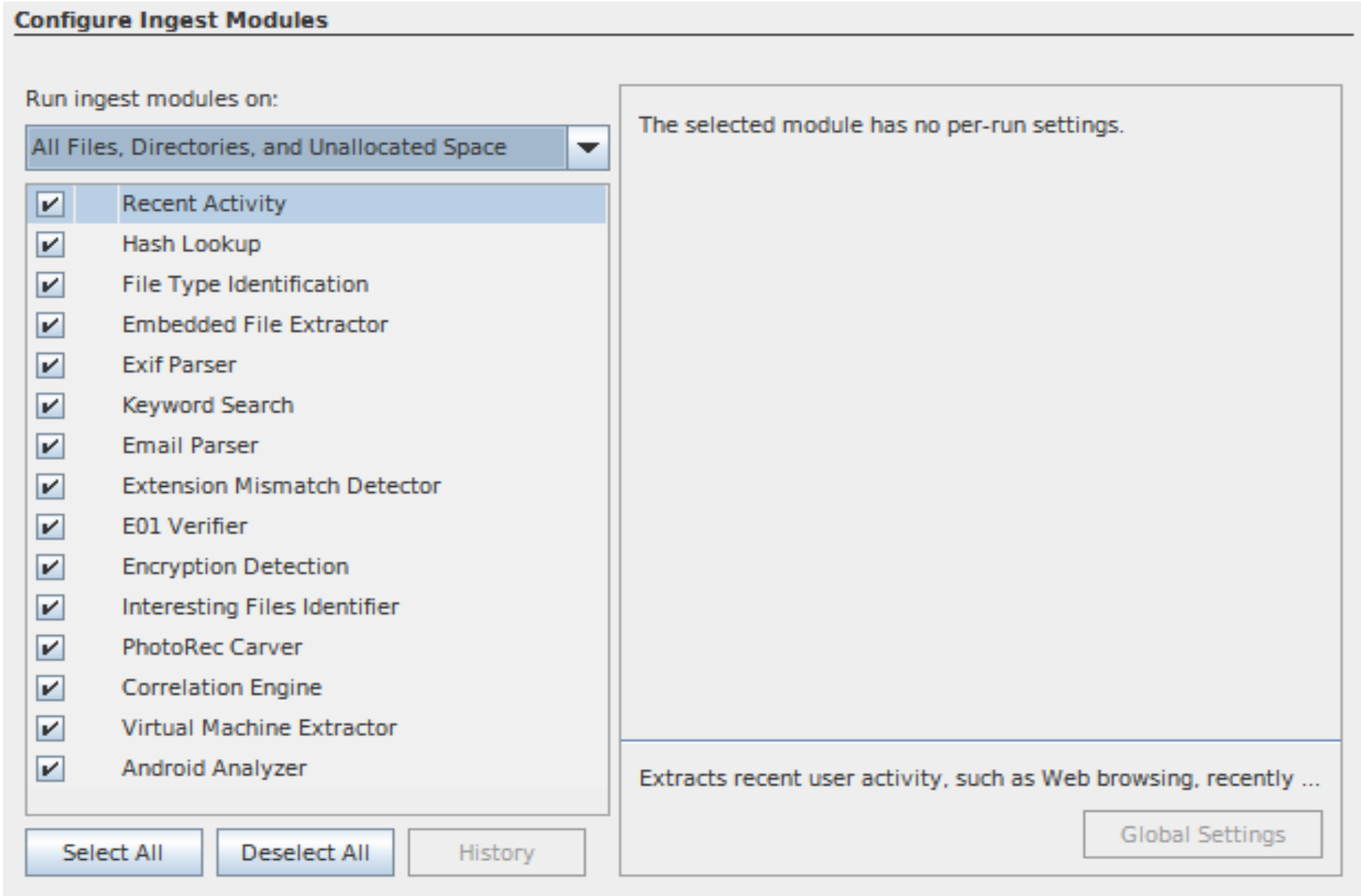
1 - Create a Case

- Case Information
- Case number, examiner

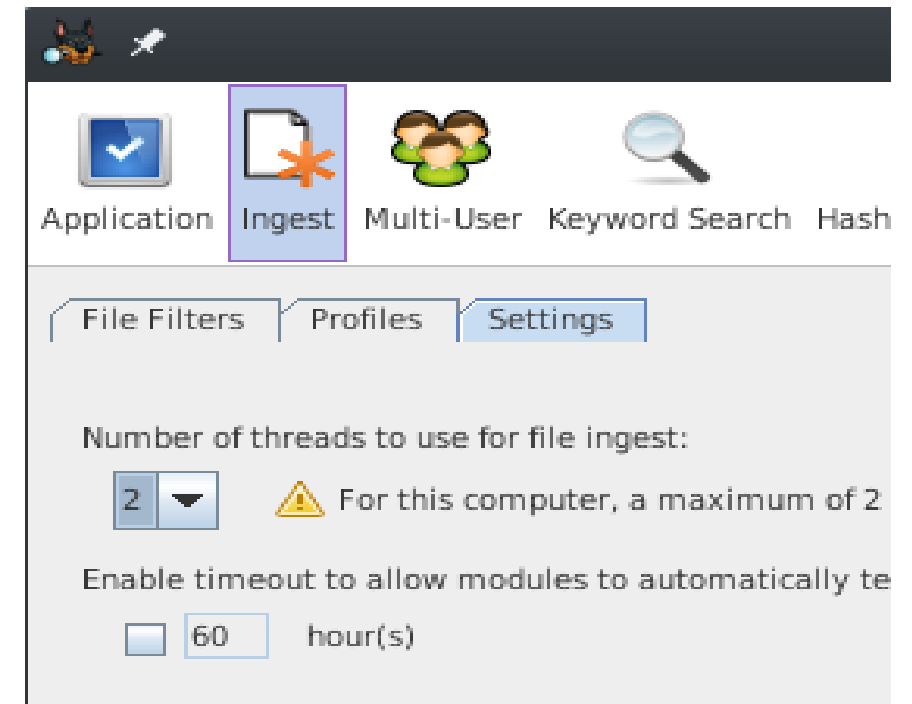
2 - Add a data source

- *Raw* (dd) or EnCase (E01) image
- Drives, files or local folders
- Virtual machine drives (vmdk, vhd)

The screenshot shows a 'Select Data Source' dialog box. It has a title bar with the text 'Select Data Source'. Below the title bar, there is a label 'Browse for an image file:' followed by a text input field containing the path '/home/mfrade/04-Local/01-LabCIF/M57-Jean/nps-2008-jean.E01'. To the right of the input field is a 'Browse' button. Below this, there is a label 'Please select the input timezone:' followed by a dropdown menu showing '(GMT+0:00) Europe/Lisbon'. Below the dropdown menu is a checkbox labeled 'Ignore orphan files in FAT file systems' with the text '(faster results, although some data will not be searched)' underneath it. At the bottom, there is a label 'Sector size:' followed by a dropdown menu showing 'Auto Detect'. A mouse cursor is visible in the bottom right corner of the dialog box.



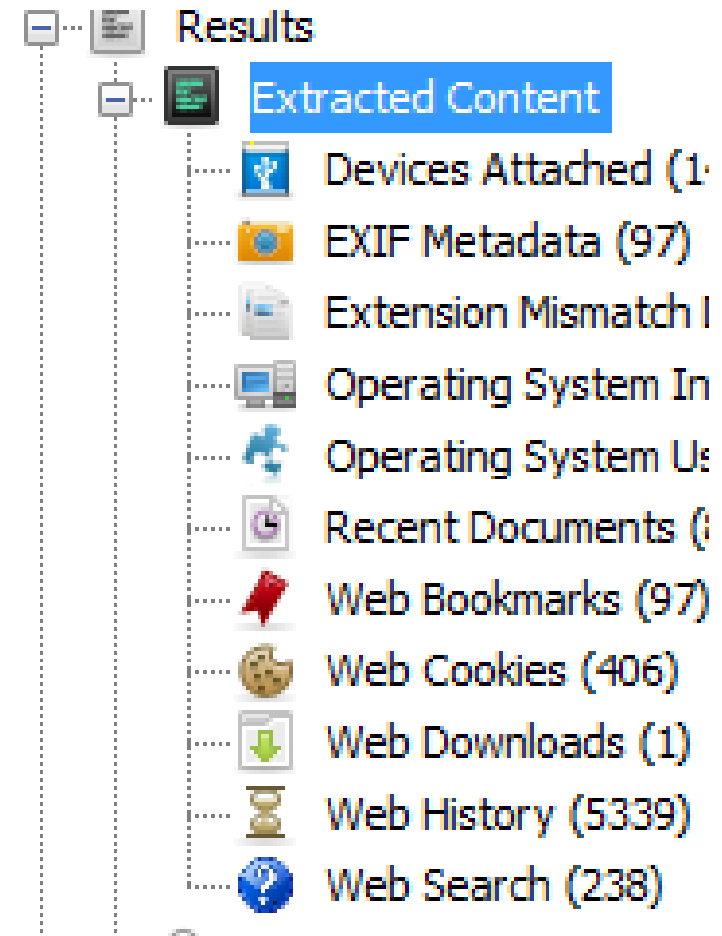
- *Autopsy* supports *multi-thread* execution of *file ingest*
- Aims to reduce the processing time
- Requires setting of the number of *threads* to use
- **Tools** → **Options** → **Ingest** → **Settings**



Extracts information from the last 7 days

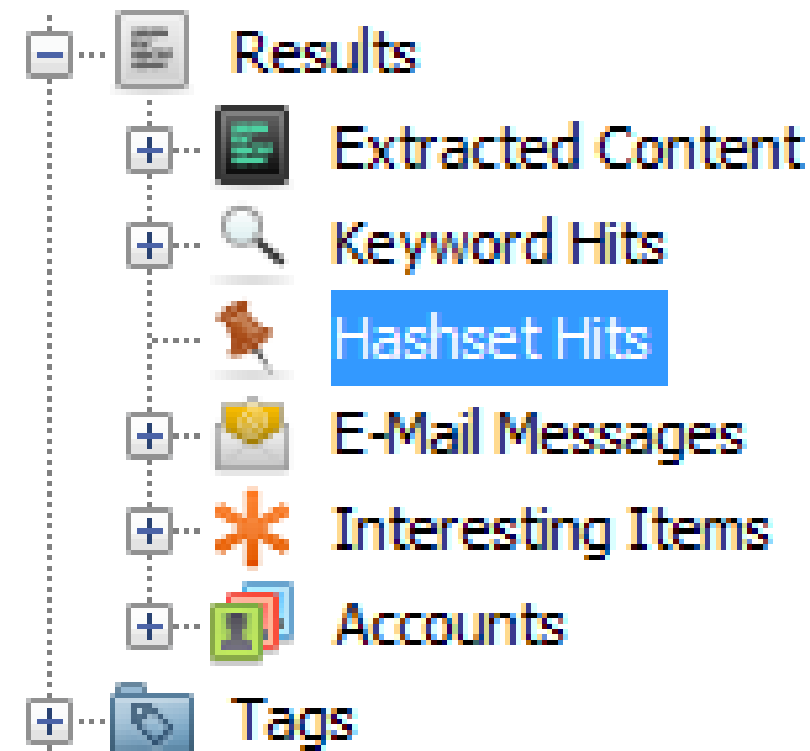
- Internet usage (including searches)
- Installed programs
- Connected devices (USB)
- Processes the *Registry hive*

The information is displayed in
Results → **Extracted Content**



Computes hash values of all found files and compares them with an existing database of *MD5* hashes

- Known bad hashsets
 - ✓ Files that must be validated
- Known good hashsets
 - ✓ Files that can be ignored
- Known hashsets
 - ✓ Files that can be good or bad (depending on the context)



Mainly available only for police forces (*i.e. hash sets* of child pornography pictures)

List of hash can be *good, bad* or just *known*







National Software Reference Library (NSRL) from NIST

URL: <https://www.nsrl.nist.gov/>

URL: <https://sourceforge.net/projects/autopsy/files/NSRL/>

VirusShare


URL: <https://virusshare.com/hashes.4n6>



itopsy Multi-user Keyword Search Hash Databases File Extension Mismatch File Types Inte

Hash Databases:

VirusShare

 Import Hash Database

Database Path:

Hash Set Name:

Type of database:

☐ Known (NSRL or other)

☒ Known Bad

☒ Send ingest inbox message for each hit

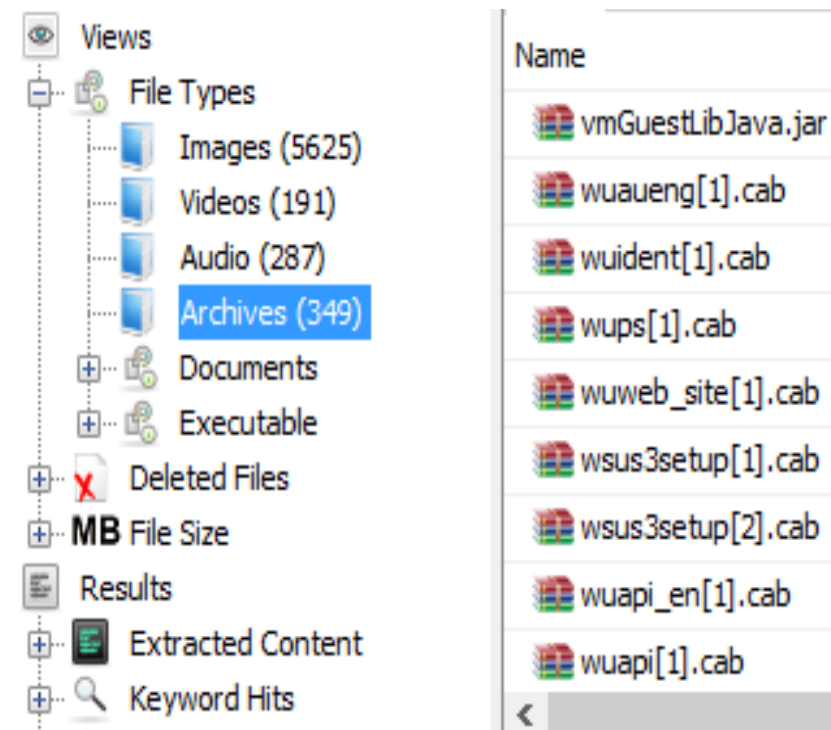
OK

Checks the file type according to its characteristics and collects meta data

- Uses *Tika* (<https://tika.apache.org/>)
- Indexing module without its own *output*
- Generates information for other modules
 - ✓ Extension Mismatch Detector
 - ✓ Keyword Search





Uncompress files (ZIP, RAR) or embedded files (DOC, DOCX, PPT, PPTX, XLS and XLSX), processing them again.

- Enables analysis of files included in these files
- Results are displayed in **File types** → **Archives**



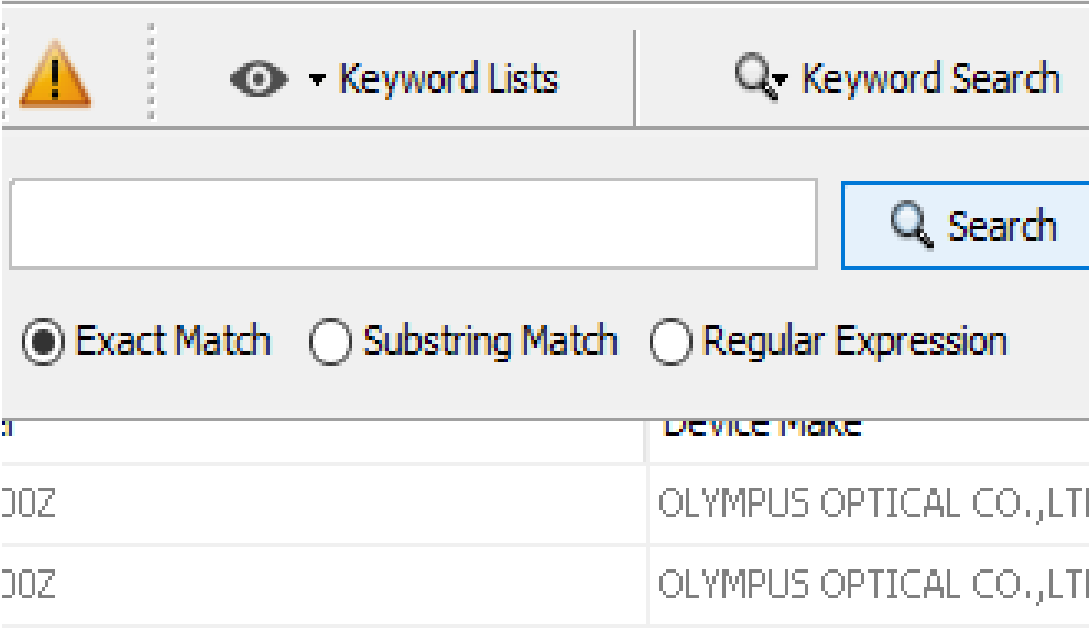
Extracts EXIF (*Exchangeable Image File Format*) information stored on images

- Geolocation, date and time
- Camera model, setup (exposure, resolution, . . .)
- Results are displayed in **Extracted content** → **EXIF Metadata**

Results			
Extracted Content			
Devices Attached (14)			
EXIF Metadata (97)			
Extension Mismatch Detection			
Operating System Information			
	 yhst-39930517073039_2007_147143019[1].j	0002-11-30 00:00:00 GMT	C4100Z,C4000Z
	 yhst-39930517073039_2007_267809[1].jpg	0002-11-30 00:00:00 GMT	C4100Z,C4000Z
	 HPIM1361[1].jpg	2008-06-15 22:17:02 BST	Photosmart M525
	 HPIM1360[1].jpg	2008-06-15 22:16:52 BST	Photosmart M525

Search by keywords during initial or on-demand processing

- Extracts text from the files being processed and adds them to an index (Solr)
- Supports several formats (Text, MS Office, PDF, Emails)

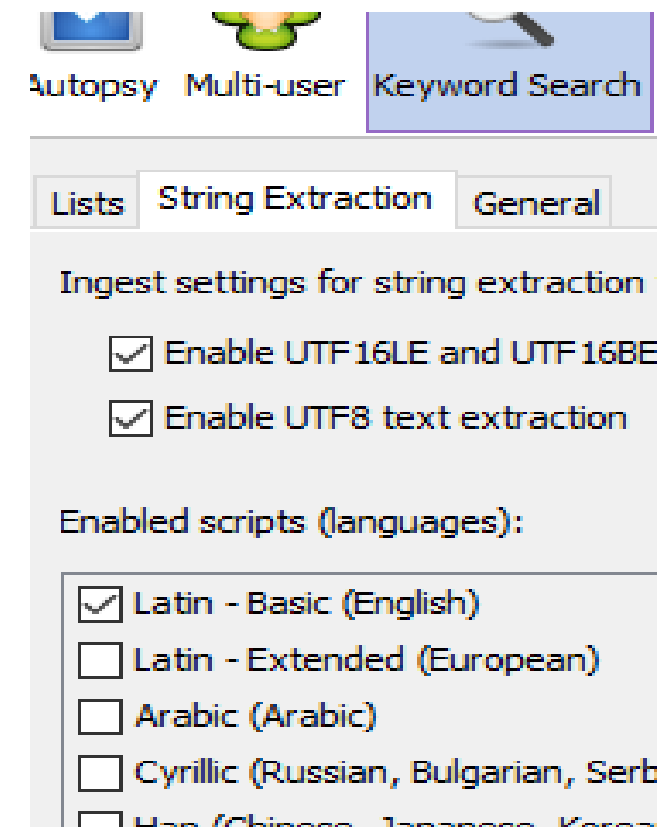


The screenshot shows a web-based keyword search interface. At the top, there is a navigation bar with a warning icon, a 'Keyword Lists' dropdown, and a 'Keyword Search' button. Below this is a search input field and a 'Search' button. Under the search field are three radio buttons: 'Exact Match' (selected), 'Substring Match', and 'Regular Expression'. Below the radio buttons is a table with two columns: 'ID' and 'DEVICE MAKE'. The table contains two rows of data.

ID	DEVICE MAKE
102	OLYMPUS OPTICAL CO.,LTI
102	OLYMPUS OPTICAL CO.,LTI

Search by keywords during initial or on-demand processing

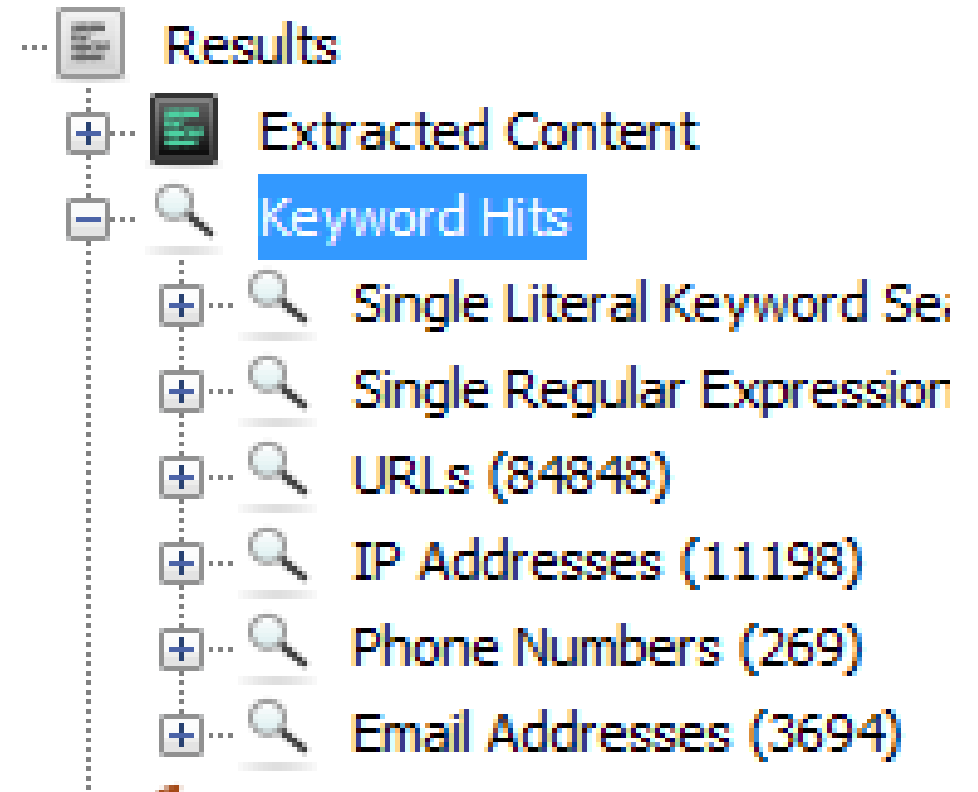
- Extracts text from the files being processed and adds them to an index (Solr)
- Supports several formats (Text, MS Office, PDF, Emails)
- For non-supported formats
 - ✓ String Extraction algorithm
 - ✓ Is able to identify encodings and languages



Autopsy includes a set of predefined lists of common expressions

- Web addresses (URLs)
- IP addresses
- Phone numbers E-mail addresses

Unfortunately, they generate a huge amount of false positives



Identifies and processes e-mail program files (MBOX, PST)

- Extract contained e-mails
- Processes its attachments

Results

Extracted Content

Keyword Hits

Hashset Hits

E-Mail Messages

Default ([Default])

Default (261)

outlook.pst	jean@m57.biz	Google Alerts: googlealerts-noreply@google
outlook.pst	jean@m57.biz	Google Alerts: googlealerts-noreply@google
outlook.pst	jean@m57.biz	alex: alex@m57.biz
outlook.pst	jean@m57.biz	alex: alex@m57.biz
outlook.pst	jean@m57.biz	alex: alex@m57.biz
outlook.pst	jean@m57.biz	alex: alex@m57.biz
outlook.pst	jean@m57.biz	alex: alex@m57.biz
outlook.pst	jean@m57.biz	alex: alex@m57.biz

Identifies files that have a file pattern that doesn't matches the filename extension

- Attempts to identify camouflaged files
 - ✓ may generate some false positives

Results			
Extracted Content			
Devices Attached (14)			
EXIF Metadata (97)			
Extension Mismatch Detected (118)			
Operating System Information (2)			
Envelope Wizard.wiz		wiz	application/msword
WEBPAGE.WIZ		wiz	application/msword
A0003824.rbf		rbf	application/pdf
GR8GALRY.GRA		gra	application/vnd.ms-excel

Verifies the hash value of the data stored in EWF files

- Calculates the hash and compares it with the values stored in the E01 metadata
- Aims to identify corrupted EWF files and prevents its automated process

Generate alerts when it detects files and folders with certain characteristics

- Type (file / folder)
- Size, extension
- Name, path
- MIME type

Interesting Files Set

Enter information about files that you want to find.

Type: ☐ Files ☒ Directories ☐ Files and Directories

☒ Name Pattern: Backup

☒ Full Name ☐ Extension Only ☐ Regex

☒ Path Pattern: Apple Computer/MobileSync

☐ Regex Use / as path separator

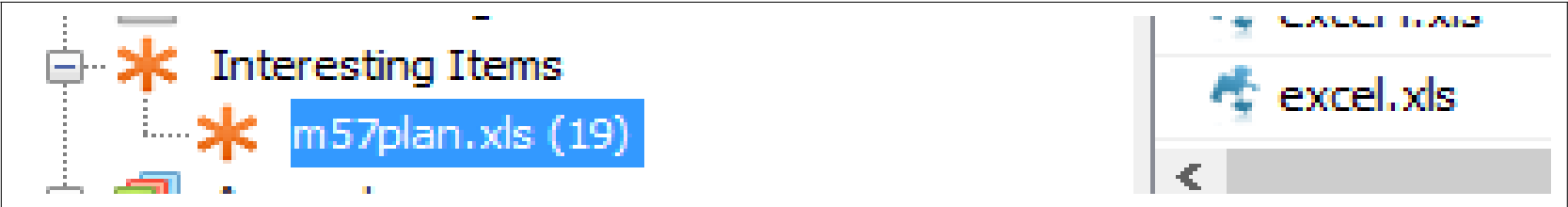
☐ MIME Type:

☐ File Size: Kilobytes

Rule Name (Optional):

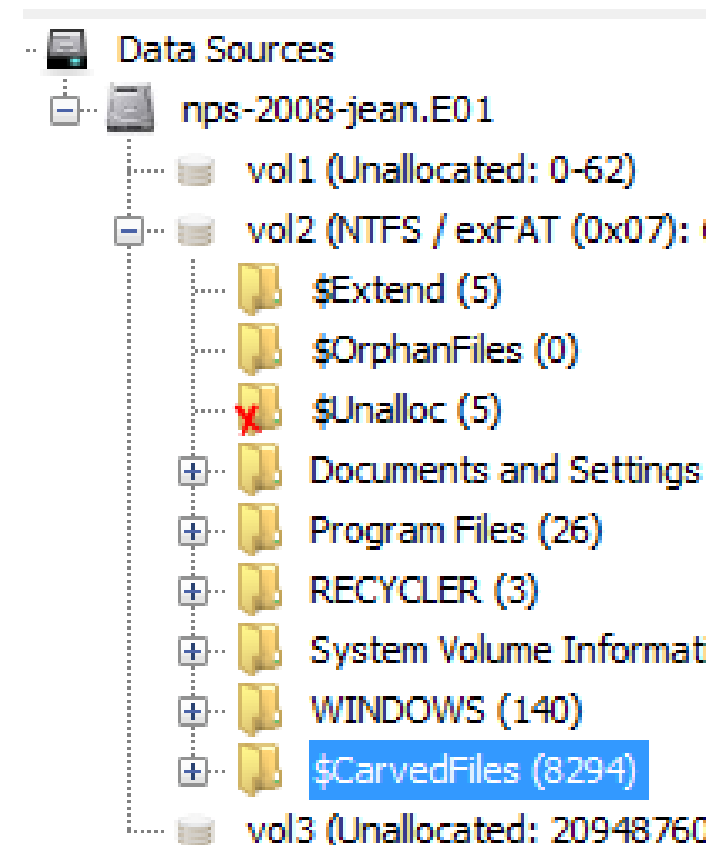
OK

Cancel



Extract files from unallocated spaces

- Supports multiple file types
- Allows the discovery of recently deleted files
- Allows custom addition of file patterns
- “Process Unallocated Space” option must be selected

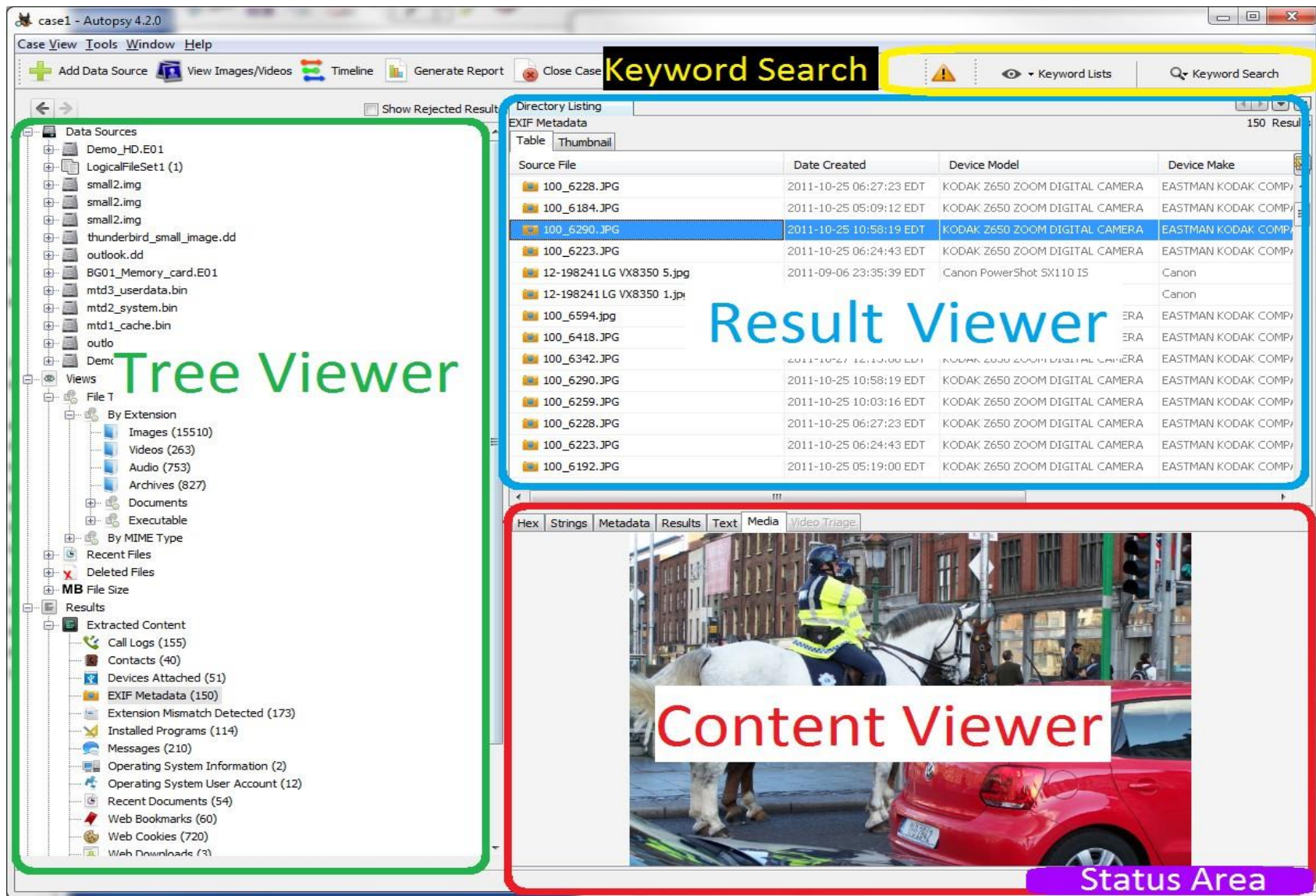


Identifies virtual machine disks and adds them directly as new data sources

- ✓ Supports VMWare (vmdk) and Microsoft Virtual Hard Drives (vhd) files

FTK Imager can read also virtual disks files and convert them to E01

AUTOPSY GRAPHIC INTERFACE



Tree viewer indexes information resulting from automated processing and gives access to four large areas:

- **Data sources:** Indicates the data source, allowing navigation within the respective file systems
- **Views:** Shows the found files under multiple views (type, size, state). The same file can appear here several times (in different views).
- **Results:** Shows the results found by the several modules.
- **Reports:** Indicates the several produced reports, either manually or automatically by the modules.

The **Views** area has:

- **File type:** Sorts files by extension or MIME type.
- **Recent files:** Files accessed in the last 7 days.
- **Deleted files:** Deleted files deleted, it tries to recover their original name.
- **File size:** Sorts files by size.

Useful when image analysis is relevant to the case under consideration. It is available in the *Tools*

- Group images by folder, compressed file
- Allows viewing of images when detected
- Functionality can be activated /deactivated in the options
- Allows cataloging of images (for child pornography and similar tasks)

Useful when searching for a file with specific characteristics.

It is available in the *Tools* menu

- Name
- Size
- MIME type
- Date
- Good/Bad

File Search by Attributes ✕

Search for files that match the following criteria:

☒ Name:

*Note: Name match is case insensitive and matches any part of the file name. Regular expressions are not currently supported.

☒ Size:

☒ MIME Type:

*Note: Multiple MIME types can be selected

☒ Date:

*Empty fields mean "No Limit" *The date format is mm/dd/yyyy

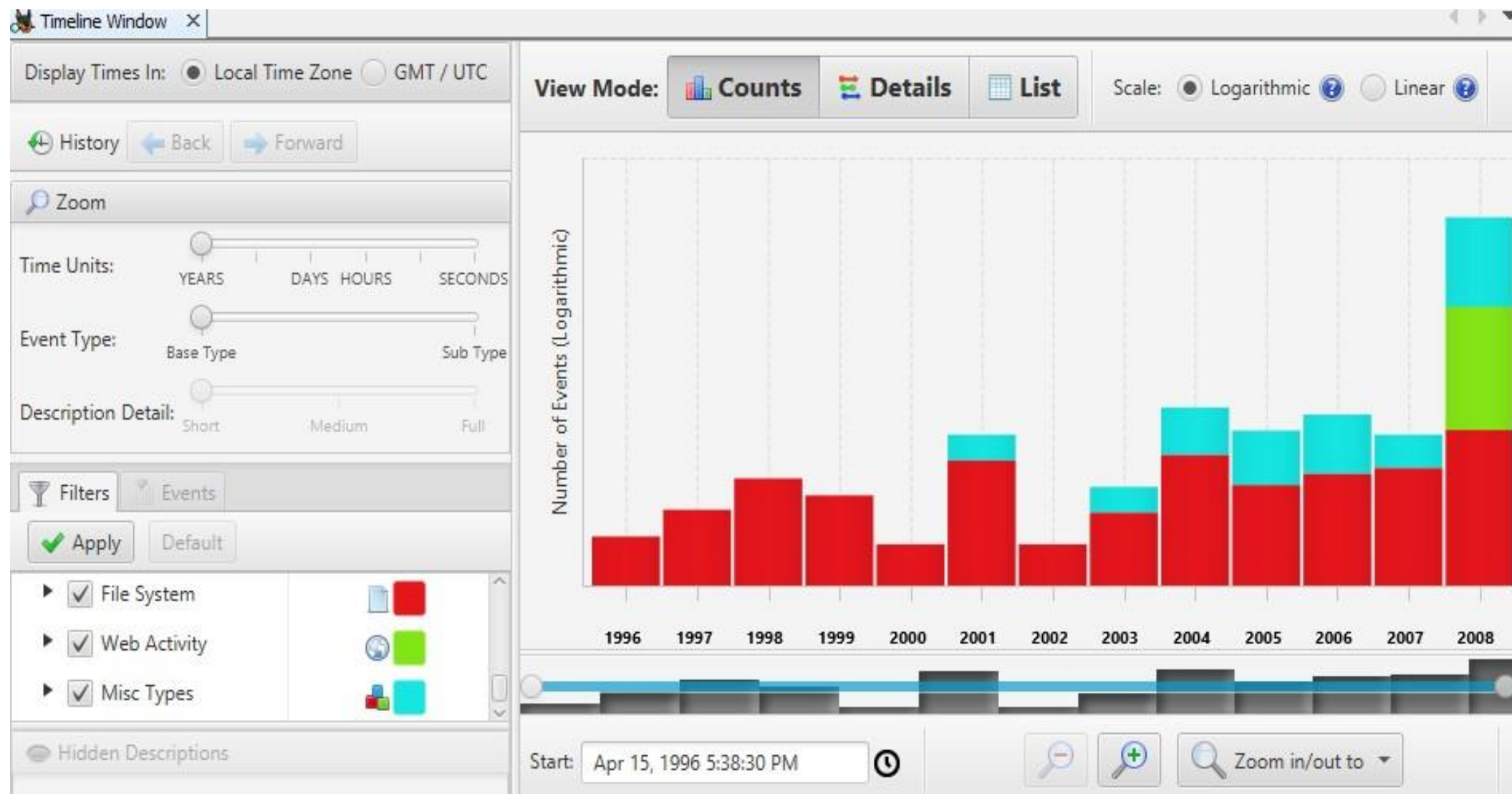
Timezone:

☒ Modified ☒ Accessed ☒ Created ☒ Changed

☒ Known Status:

☒ Unknown ☒ Known (NSRL or other) ☒ Known bad

After indexing events, Autopsy allows you to create timelines based on the dates on which such events occurred

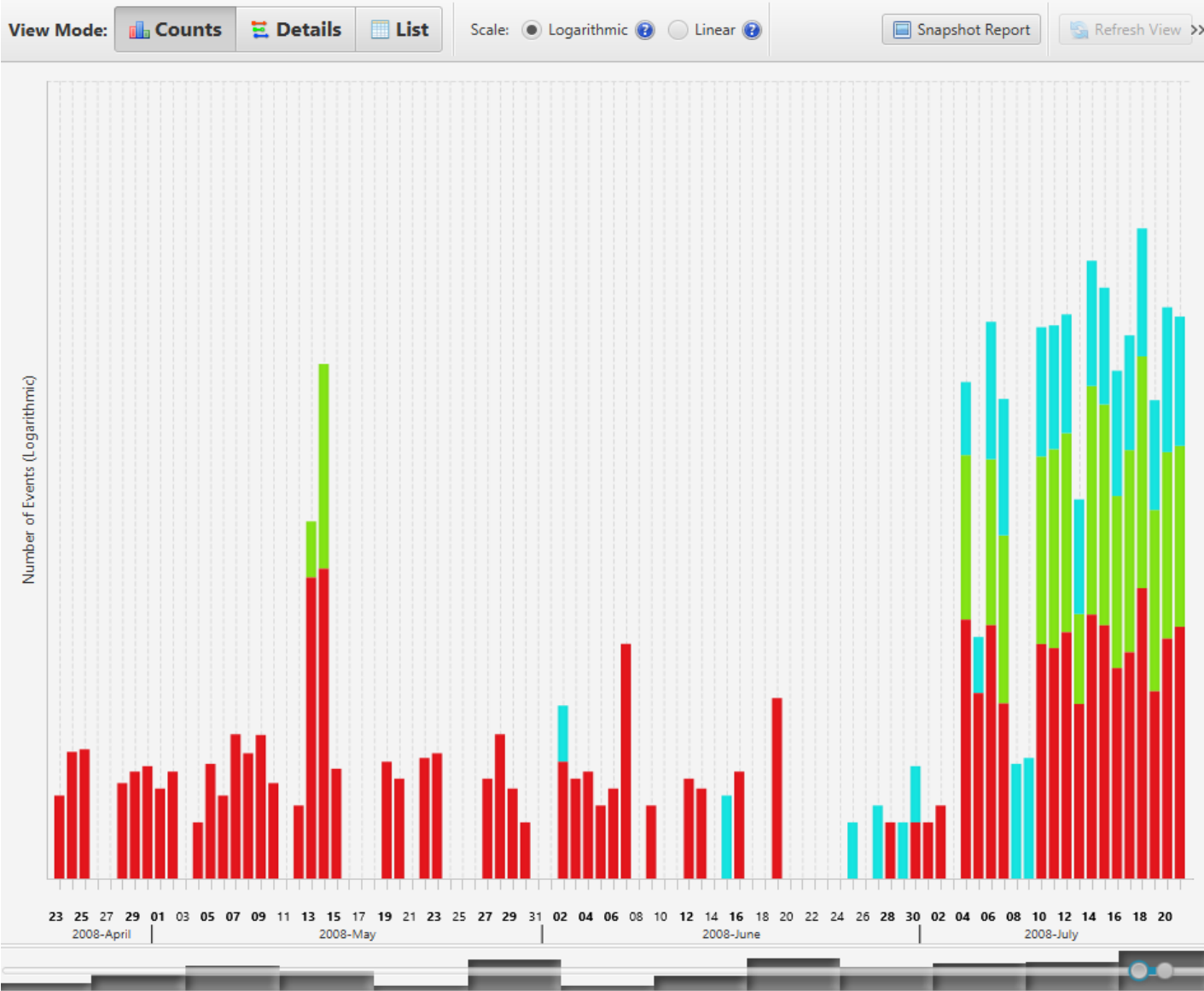


Autopsy recognizes events, such as

- Files (modification, access, creation, change)
- Internet access (downloads, cookies, bookmarks, searches, browser history)
- Others (messages, phone calls, e-mails, GPS tracks, . . .)

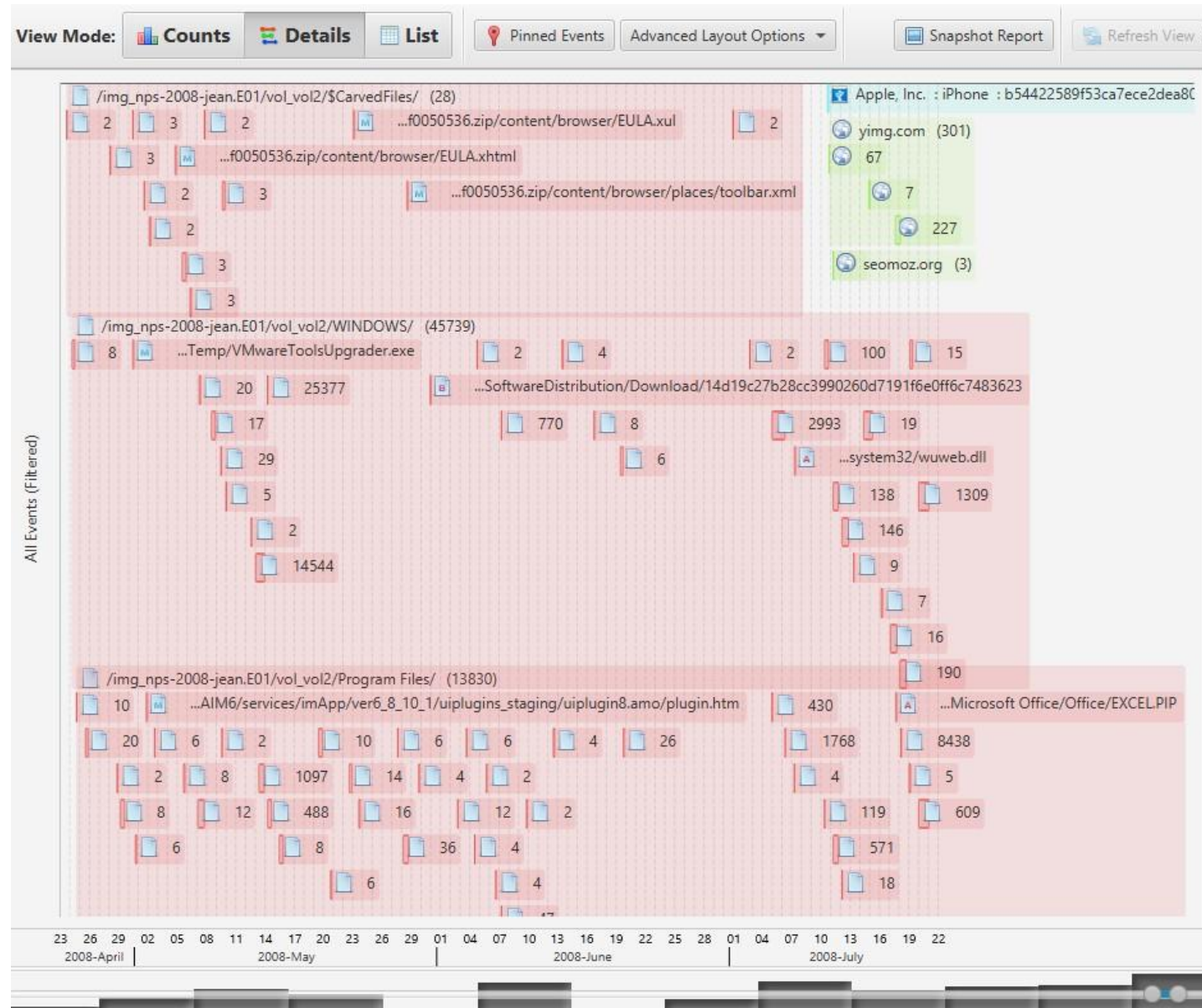
TIMELINE VISUALIZATION

HISTOGRAM



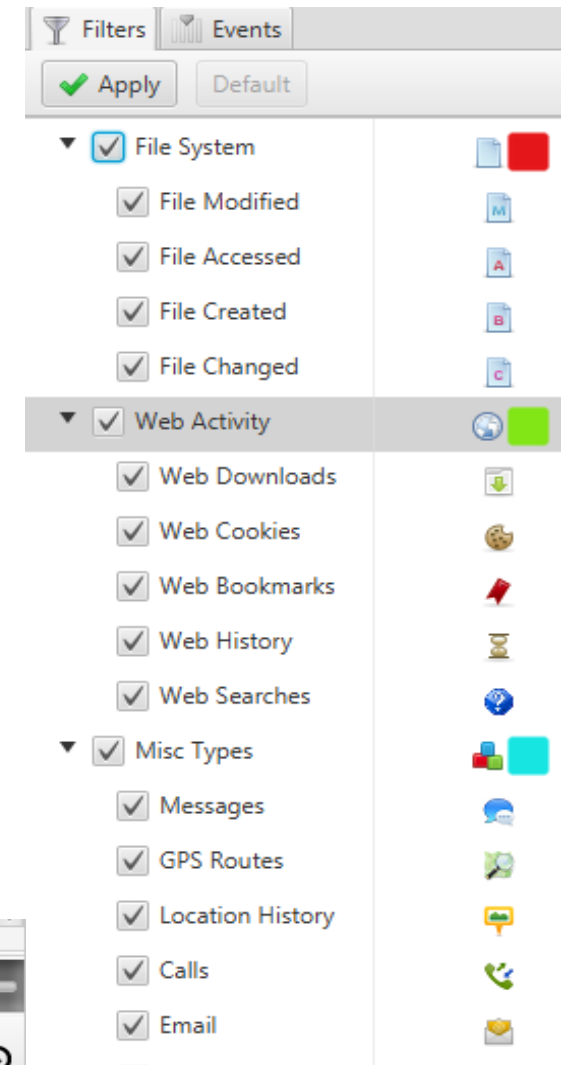
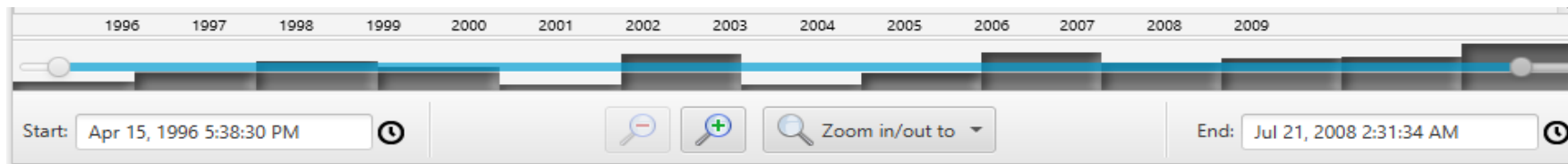
TIMELINE VISUALIZATION

DETAILED VIEW

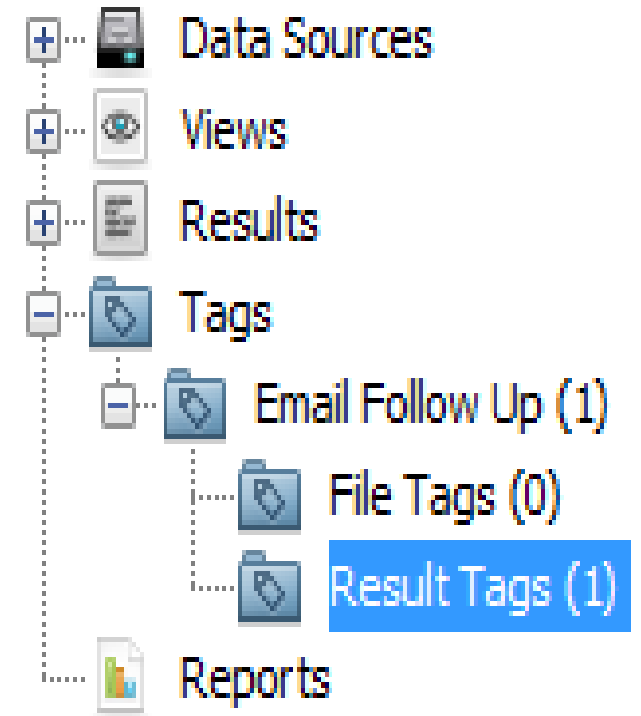


Autopsy allows to reduce the number of elements in a timeline using filters

- Filter known files
- Filter by text
- Event type
- Time windows



- Tag results with labels
- Items for future reference
- Enables the marking of files or results
- Tag name set by investigator
- Tags appear as a sub-area of **Results**



Several types of reports are available

Results: Applies to the items of the results view,

 Generate Report

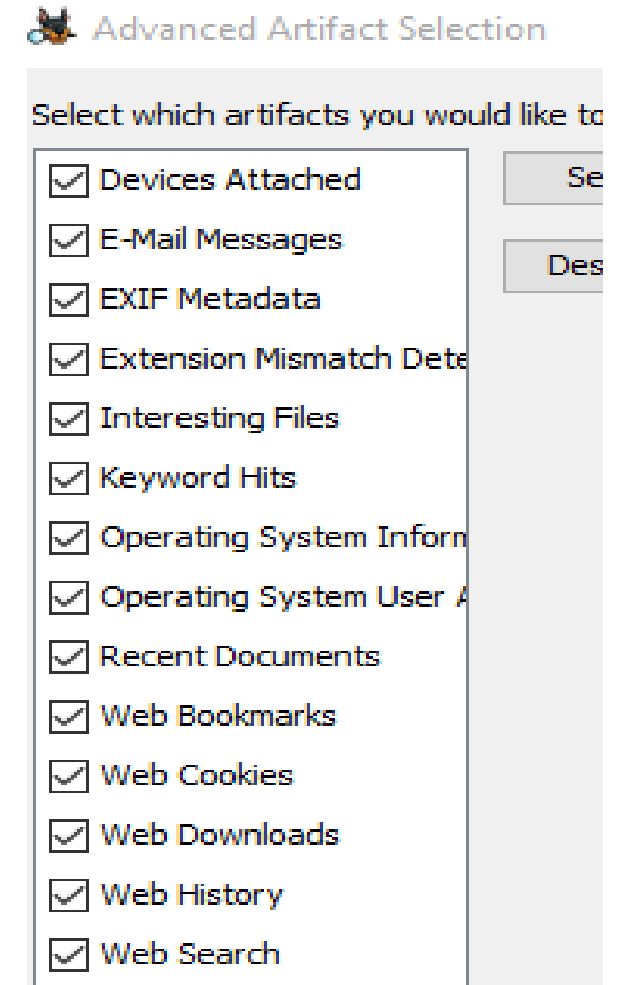
Select and Configure Report

Report Modules:

- ☒ Results - HTML
- ☐ Results - Excel
- ☐ Add Tagged Hashes
- ☐ Files - Text
- ☐ Google Earth/KML
- ☐ STIX
- ☐ TSK Body File

Several types of reports are available

Results: Applies to the items of the results view, can be filtered



The image shows a screenshot of a software interface titled "Advanced Artifact Selection". It features a list of 15 artifacts, each with a checked checkbox. To the right of the list are two buttons: "Select" and "Description".

Advanced Artifact Selection

Select which artifacts you would like to

- ☒ Devices Attached
- ☒ E-Mail Messages
- ☒ EXIF Metadata
- ☒ Extension Mismatch Detection
- ☒ Interesting Files
- ☒ Keyword Hits
- ☒ Operating System Information
- ☒ Operating System User Activity
- ☒ Recent Documents
- ☒ Web Bookmarks
- ☒ Web Cookies
- ☒ Web Downloads
- ☒ Web History
- ☒ Web Search

Select

Description

Several types of reports are available

Results: Applies to the items of the results view, can be filtered

Tagged: Applies to the tagged items

Configure Artifact Reports

Select which data to report on:

☐ All Results

☒ Tagged Results

☒ Email Follow Up

Several types of reports are available

Results: Applies to the items of the results view, can be filtered

Tagged: Applies to the tagged items

Files: List of files under analysis

Configure File Report

Select items to include in File Report:

- ☐ Name
- ☐ File Extension
- ☐ File Type
- ☐ Is Deleted
- ☐ Last Accessed
- ☐ File Created
- ☐ Last Modified
- ☐ Size
- ☐ Address
- ☐ Hash Value
- ☐ Known Status
- ☐ Permissions
- ☐ Full Path

Select All Deselect All

Several types of reports are available

Results: Applies to the items of the results view, can be filtered

Tagged: Applies to the tagged items

Files: List of files under analysis

KML: List of GPS coordinates in *Google Earth* format

 Generate Report

Select and Configure Report Mo

Report Modules:

- ☐ Results - HTML
- ☐ Results - Excel
- ☐ Add Tagged Hashes
- ☐ Files - Text
- ☒ Google Earth/KML
- ☐ STIX
- ☐ TSK Body File

Several types of reports are available

Results: Applies to the items of the results view, can be filtered

Tagged: Applies to the tagged items

Files: List of files under analysis

KML: List of GPS coordinates in *Google Earth* format

TSK: MAC timeline list of all files

Select and Configure Report

Report Modules:

- ☐ Results - HTML
- ☐ Results - Excel
- ☐ Add Tagged Hashes
- ☐ Files - Text
- ☐ Google Earth/KML
- ☐ STIX
- ☒ TSK Body File

Several types of reports are available

Results: Applies to the items of the results view, can be filtered

Tagged: Applies to the tagged items

Files: List of files under analysis

KML: List of GPS coordinates in *Google Earth* format

TSK: MAC timeline list of all files

STIX: Compares the results obtained with a threat file

Select and Configure Report Modules

Report Modules:

- ☐ Results - HTML
- ☐ Results - Excel
- ☐ Add Tagged Hashes
- ☐ Files - Text
- ☐ Google Earth/KML
- ☒ STIX
- ☐ TSK Body File

- Structured language for describing cyber threat information so it can be shared (XML)
- Accepts indicators like:
 - ✓ IP address, URL, Names
 - ✓ TCP, UDP connections
 - ✓ Filenames, *hashs*
 - ✓ . . .
- More information: <https://stix.mitre.org/>
<https://stix.mitre.org/language/version1.0.1/samples.html>
<https://oasis-open.github.io/cti-documentation/stix/examples.html>

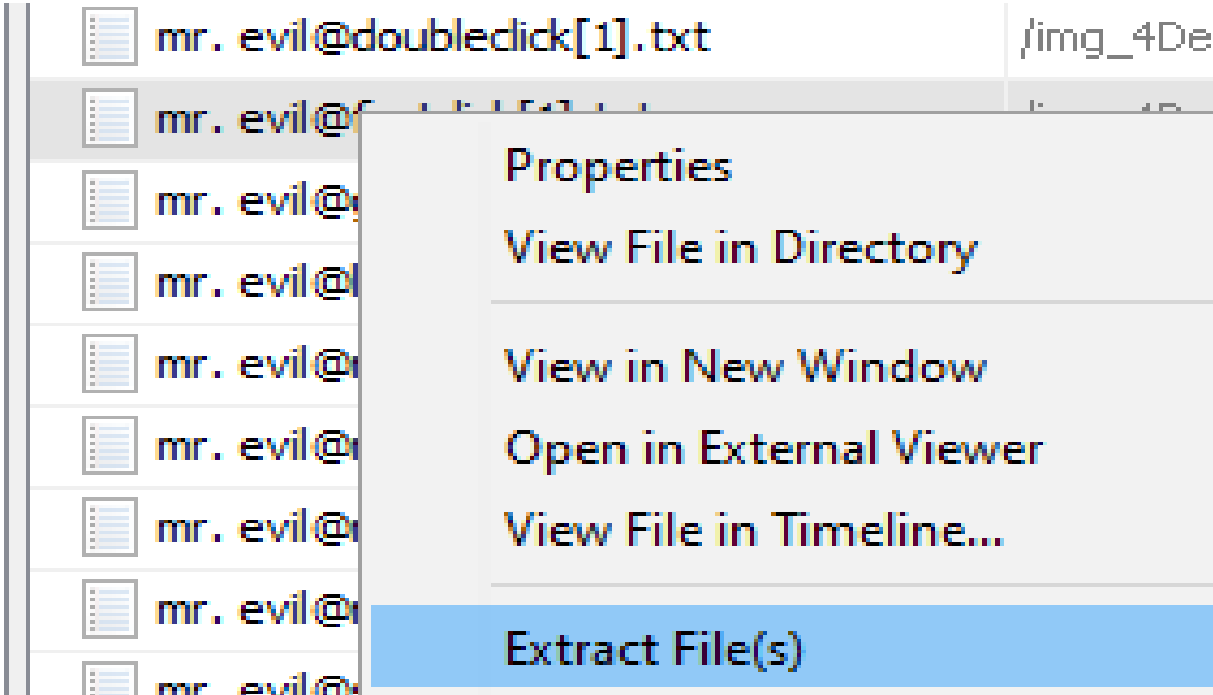
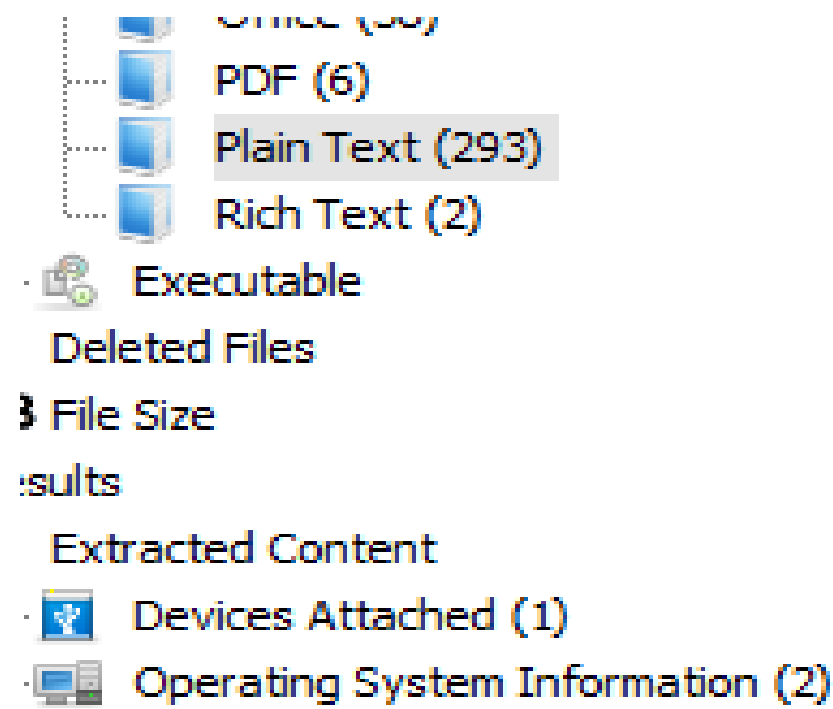
```

...
<stix:Indicators>
  <stix:Indicator xsi:type="indicator:IndicatorType" id="apinto:Indicator-83f51b6a-8512-4194-84bb-65744ad6604f"
    timestamp="2017-01-13T00:00:00.000000Z">
    <indicator:Title>Known IP address</indicator:Title>
    <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">IP Watchlist</indicator:Type>
    <indicator:Observable id="apinto:Observable-7b9e4a6f-513a-407d-9456-62f078cfd0b">
      <cybox:Object id="apinto:Object-de674b6f-a5f4-4ee4-9360-1b65877354d7">
        <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
          <AddressObject:Address_Value condition="Equals">192.168.1.111</AddressObject:Address_Value>
        </cybox:Properties>
      </cybox:Object>
    </indicator:Observable>
  </stix:Indicator>
</stix:Indicators>
<stix:TTPs>
  <stix:TTP xsi:type="ttp:TTPType" id="apinto:TTP-83fe262c-0f34-4178-be3f-e96328fa1ee6" timestamp="2017-01-13T00:00:00.000000Z">
    <ttp:Title>Potentially dangerous equipment!</ttp:Title>
  </stix:TTP>
</stix:TTPs>
...

```

Autopsy allows to export files to:

- Analyse with other tools
- Compare
- Archive



Bibliography

Autopsy User's Guide, Autopsy User Documentation (version 4.19.2)

<https://github.com/sleuthkit/autopsy/tree/develop/docs/doxygen-user>

Autopsy User Documentation

<https://sleuthkit.org/autopsy/docs/user-docs/4.19.2>

Credits

The original author of these slides is António Pinto, adapted and updated by Miguel Frade, Baltazar Rodrigues and Artur Varanda

On 20-09-2004 a computer was found abandoned and it is suspected that this computer was used for hacking purposes. The suspect, Greg Schardt, uses the nickname "Mr. Evil" and some of his associates have said that he would park his vehicle within range of Wireless Access Points where he would then intercept Internet traffic, attempting to get credit card numbers, usernames & passwords.

Class 05 - LAB01 – Image Analysis with Autopsy

1. Download the PC drive images from link available on *Moodle*
2. Create a new case in Autopsy and start automated processing
3. Answer the questions
4. Generate a report by running the STIX sample file against the data sources

