

universidade  
de aveiro

# Computer Systems Forensic Analysis AFSC

**Autopsy**

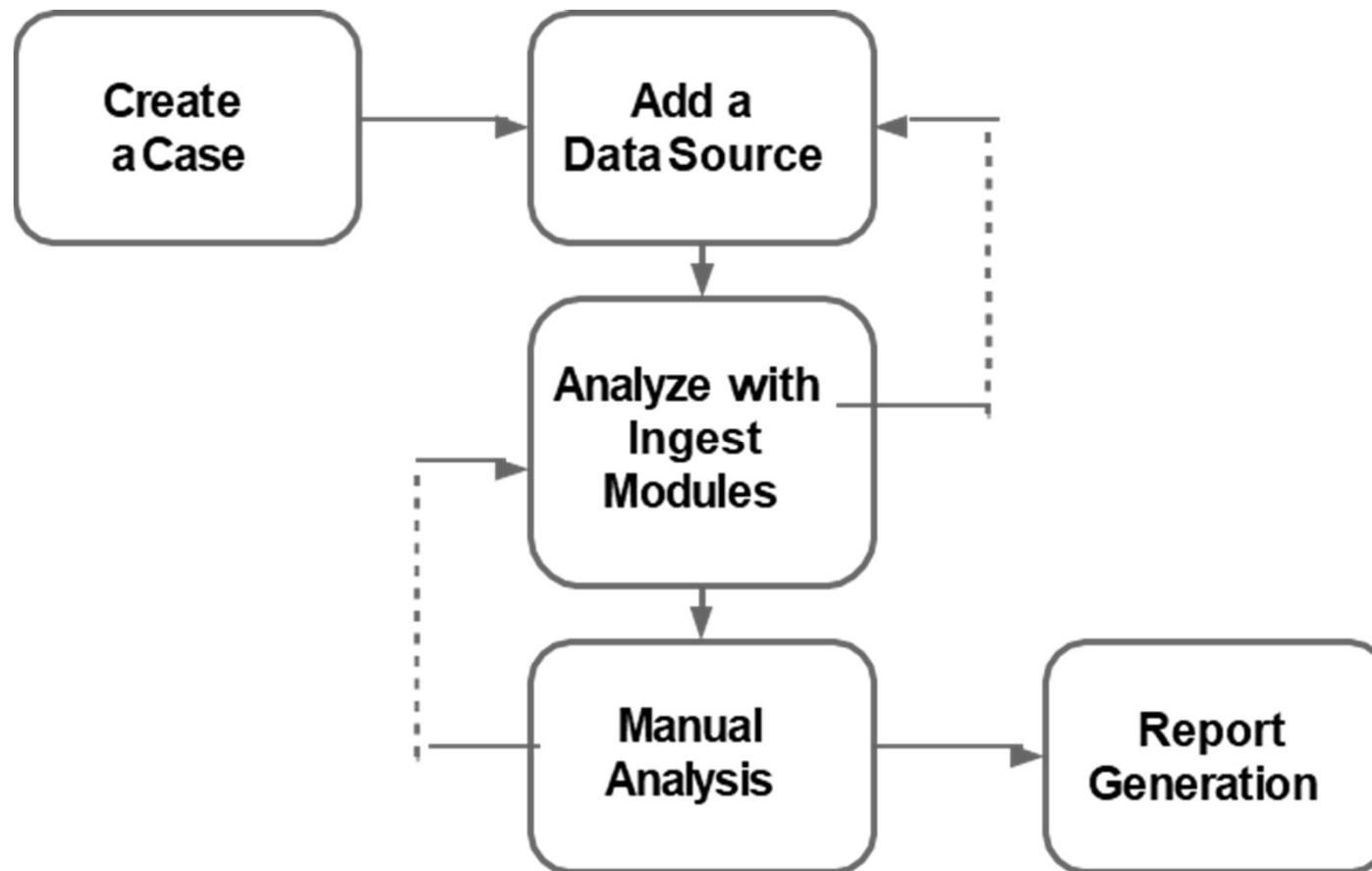
*Artur Varanda*

School Year 2021-2022

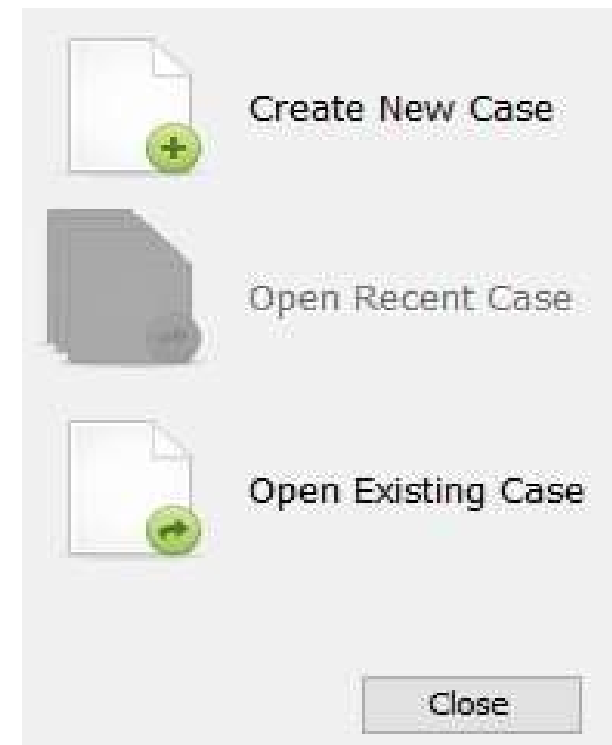
url: <https://www.autopsy.com>



- *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

The screenshot shows a web form titled "Optional Information". It contains three main sections: "Case", "Examiner", and "Organization".

- Case**: A single input field labeled "Number:" with the text "NUIPC xxxxxx" entered.
- Examiner**: Four input fields labeled "Name:", "Phone:", "Email:", and "Notes:". The "Name:" field contains "MF", and the "Notes:" field contains "Test".
- Organization**: A single input field with the text "Organization analysis is being done f..." entered.

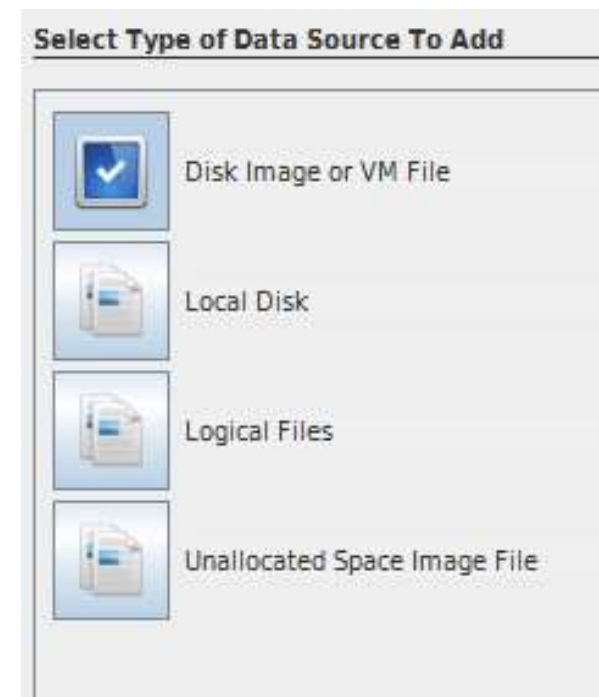
At the bottom of the form are three buttons: "< Back", "Next >", and "Finish".

### 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)



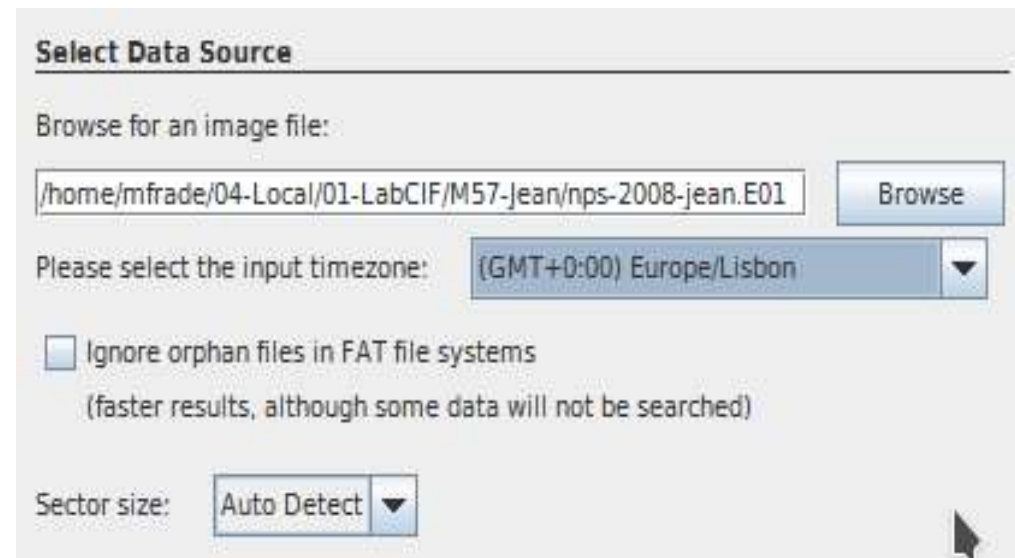
## CREATE A CASE

### 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)

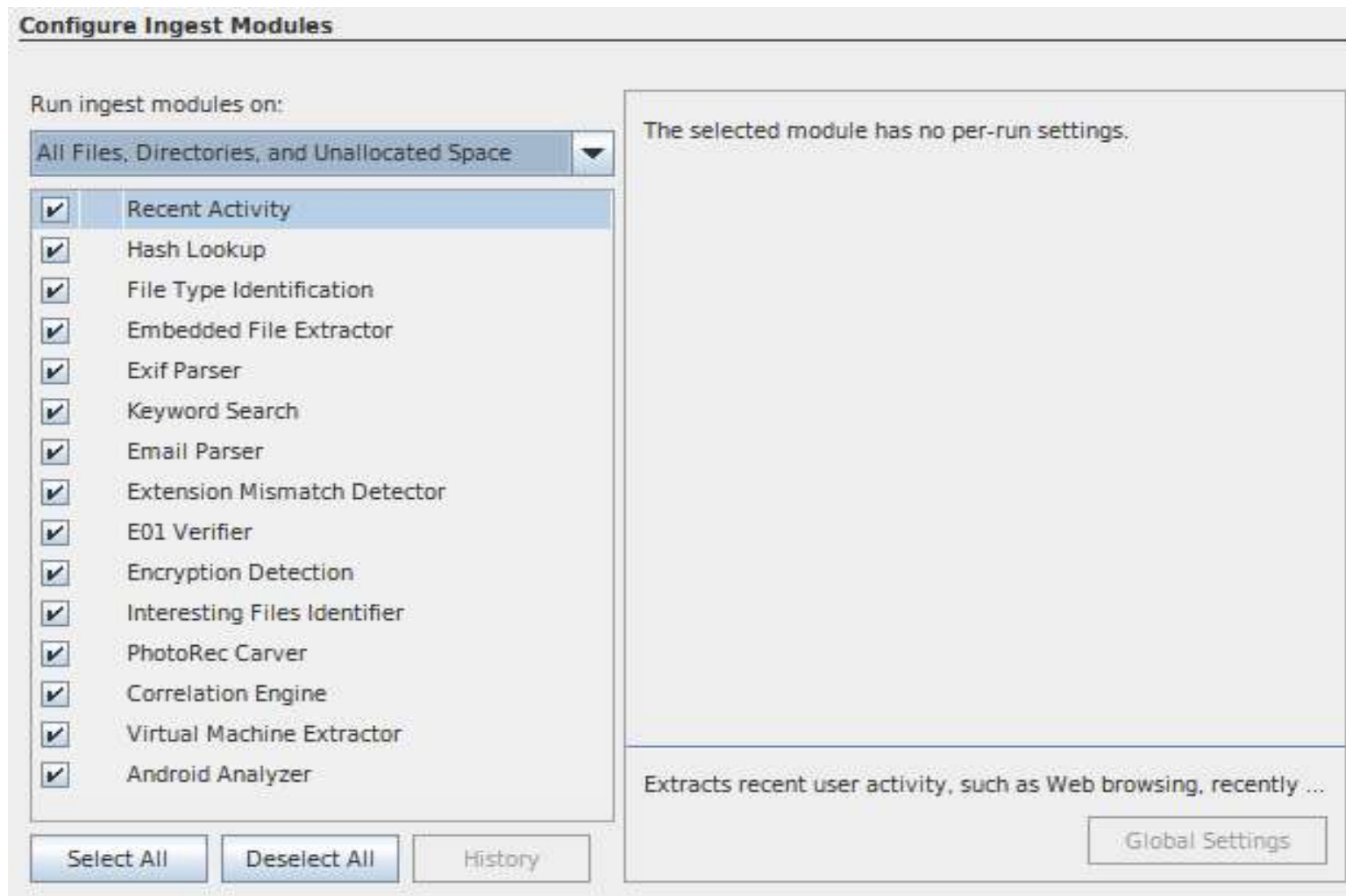


The screenshot shows a dialog box titled "Select Data Source". It contains the following elements:

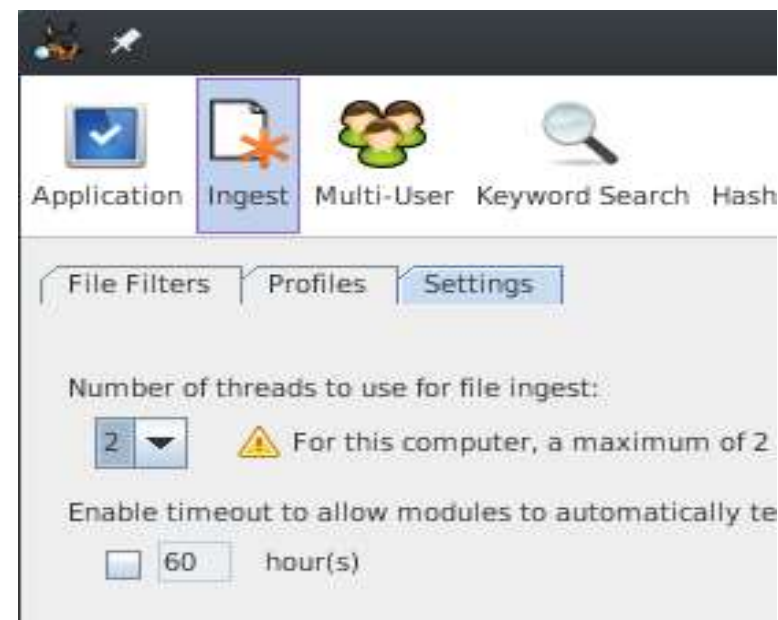
- A label "Browse for an image file:" followed by a text input field containing the path `/home/mfrade/04-Local/01-LabCIF/M57-jean/nps-2008-jean.E01` and a "Browse" button.
- A label "Please select the input timezone:" followed by a dropdown menu showing `(GMT+0:00) Europe/Lisbon`.
- A checkbox labeled "Ignore orphan files in FAT file systems" with the subtext "(faster results, although some data will not be searched)".
- A label "Sector size:" followed by a dropdown menu showing "Auto Detect".



## AUTOMATED PROCESSING – WITH INGEST MODULES



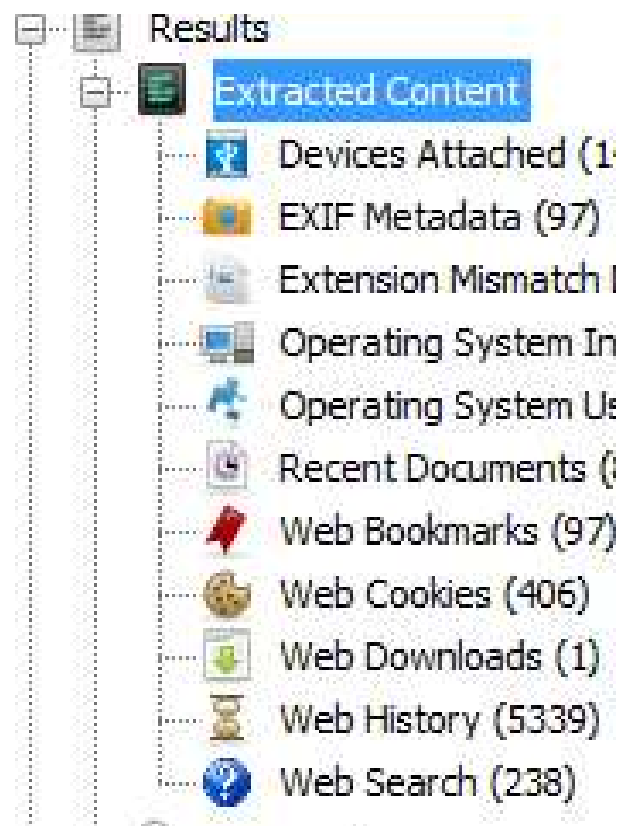
- *Autopsy* supports *multi-thread* execution of *file ingest*
- Aims to reduce the processing time
- Requires setting of the number of *threads* to use
- **Tools** → **Options** → **Ingest** → **Settings**



Extracts information from the last 7 days

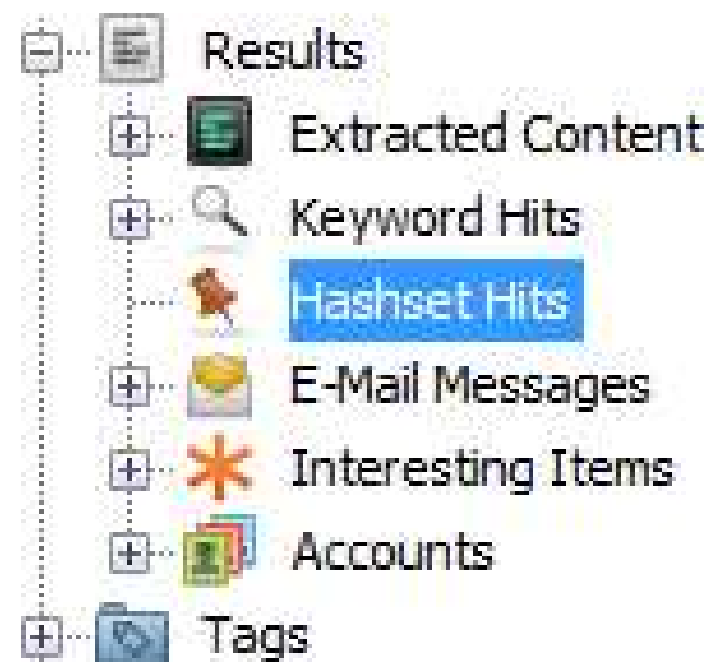
- Internet usage (including searches)
- Installed programs
- Connected devices (USB)
- Processes the *Registry hive*

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

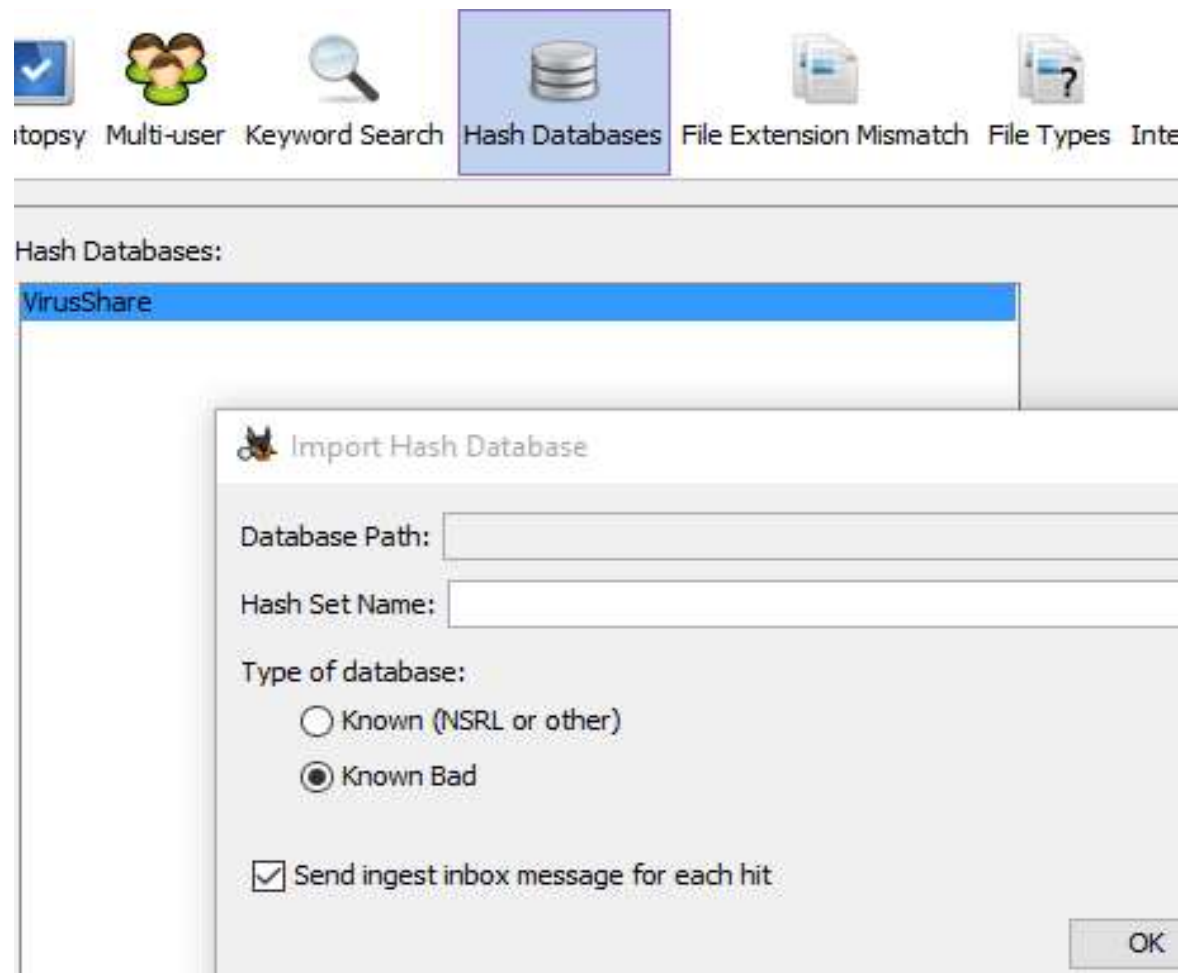
**URL:** <http://www.nsrl.nist.gov/>

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

VirusShare

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

## MODULE: HASH LOOKUP – HASH SETS

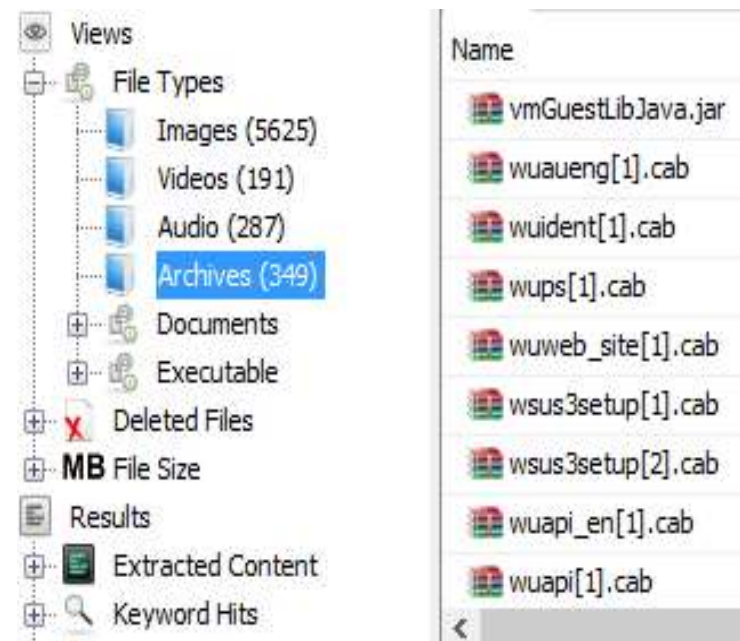


Checks the file type according to its characteristics and collects meta data

- Uses *Tika* (<http://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**





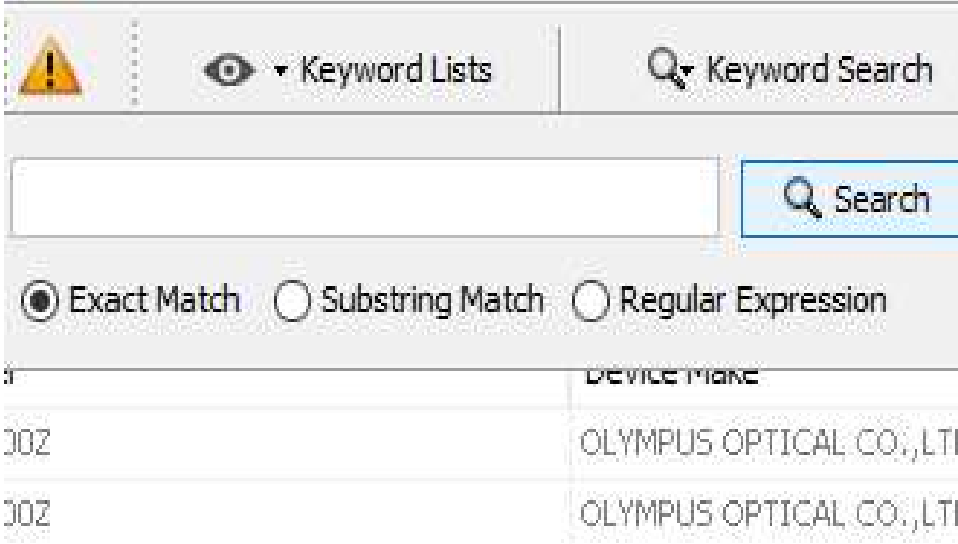
Extracts EXIF (*Exchangeable Image File Format*) information stored on images

- 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 Dete			
Operating System Inform			
	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 displays a user interface for keyword searching. At the top, there is a toolbar with a warning icon, a 'Keyword Lists' dropdown, and a 'Keyword Search' button. Below this is a search input field with a 'Search' button. Under the input field, three radio buttons are available: 'Exact Match' (selected), 'Substring Match', and 'Regular Expression'. At the bottom, a table shows search results with two columns: an identifier and 'DEVICE MAKE'.

	DEVICE MAKE
302	OLYMPUS OPTICAL CO.,LTI
302	OLYMPUS OPTICAL CO.,LTI

Search by keywords during initial or on-demand processing

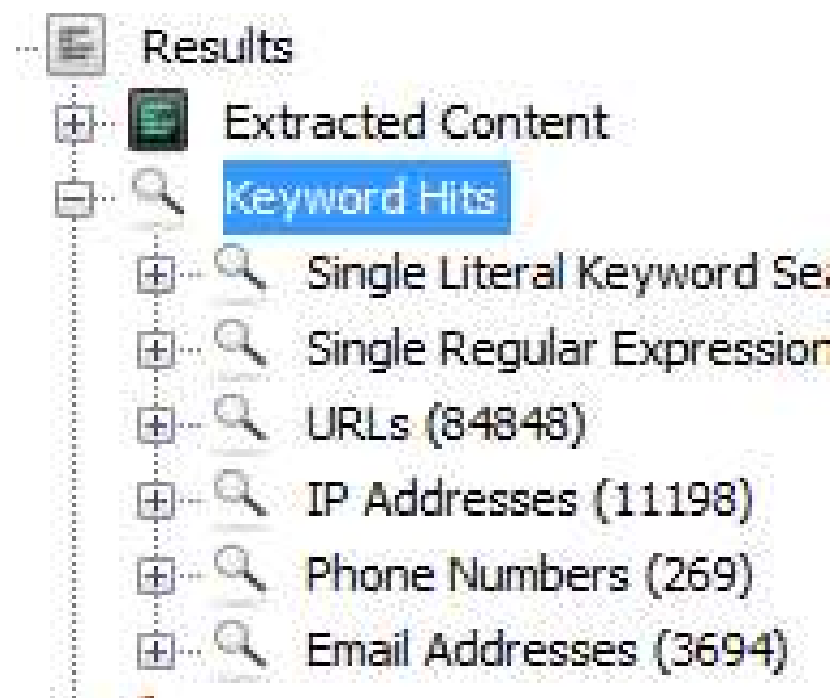
- Extracts text from the files being processed and adds them to an index (Solr)
- Supports several formats (Text, MS Office, PDF, Emails)
- For non-supported formats
  - ✓ String Extraction algorithm
  - ✓ Is able to identify encodings and languages



*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)

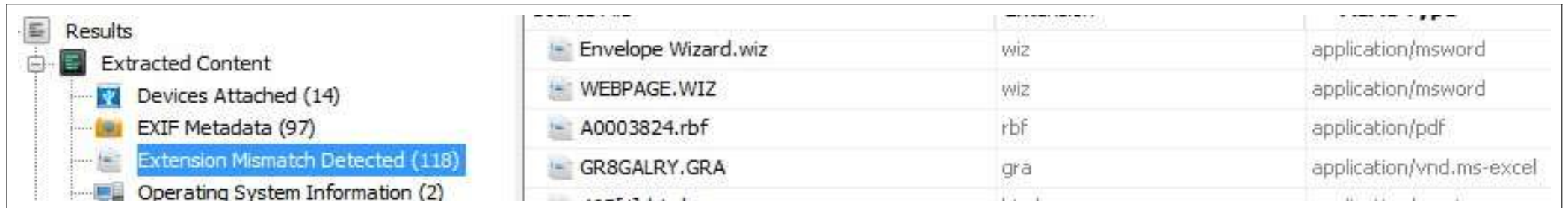
- Extract contained e-mails
- Processes its attachments

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

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

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



The screenshot shows a forensic analysis tool interface. On the left, a tree view under 'Results' includes 'Extracted Content', 'Devices Attached (14)', 'EXIF Metadata (97)', 'Extension Mismatch Detected (118)' (highlighted in blue), and 'Operating System Information (2)'. On the right, a table lists files with their extensions and detected MIME types.

File Name	Extension	MIME Type
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:   0  Kilobytes

Rule Name (Optional):

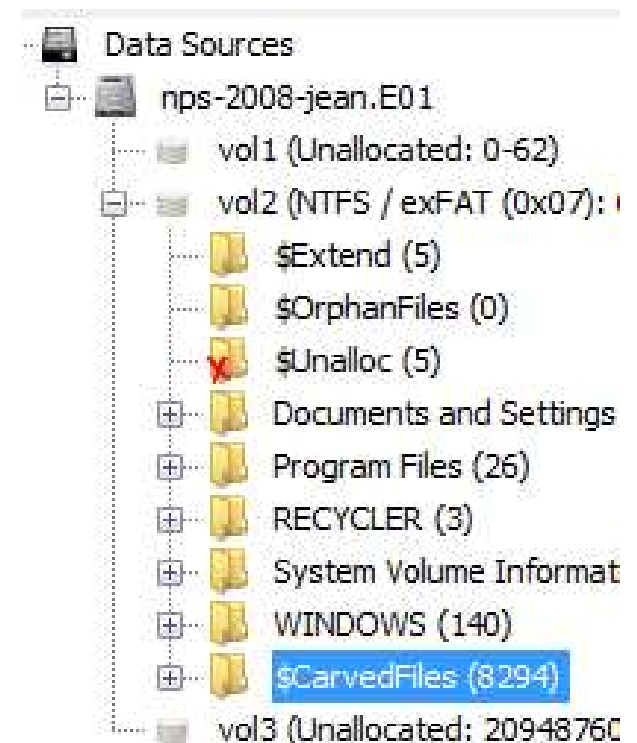
OK Cancel





## 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

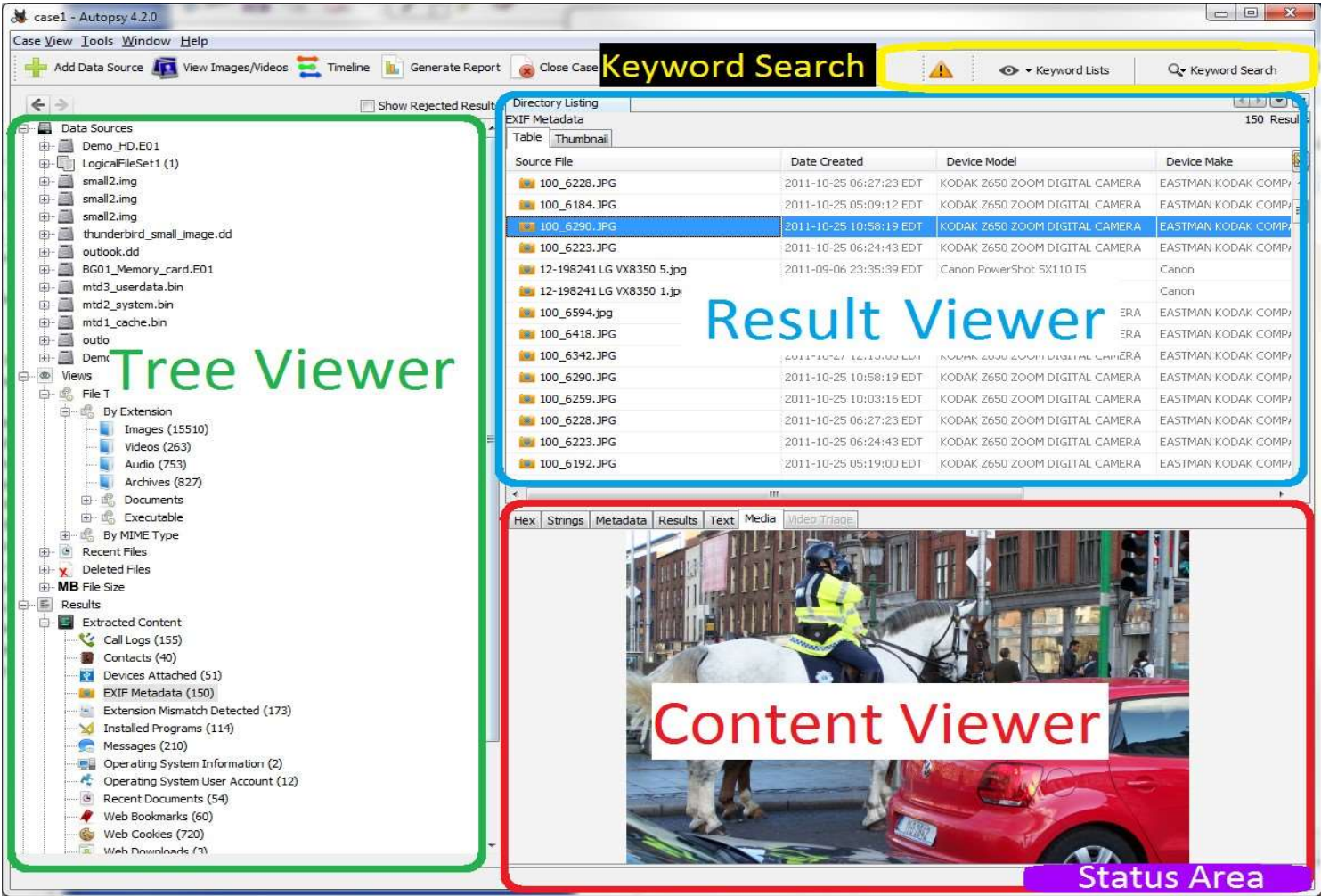


Identifies virtual machine disks and adds them directly as new data sources

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

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

MANUAL CONTENT ANALYSIS  
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)

## FILE SEARCH

Useful when searching for a file with specific characteristics.

It is available in the *Tools* menu

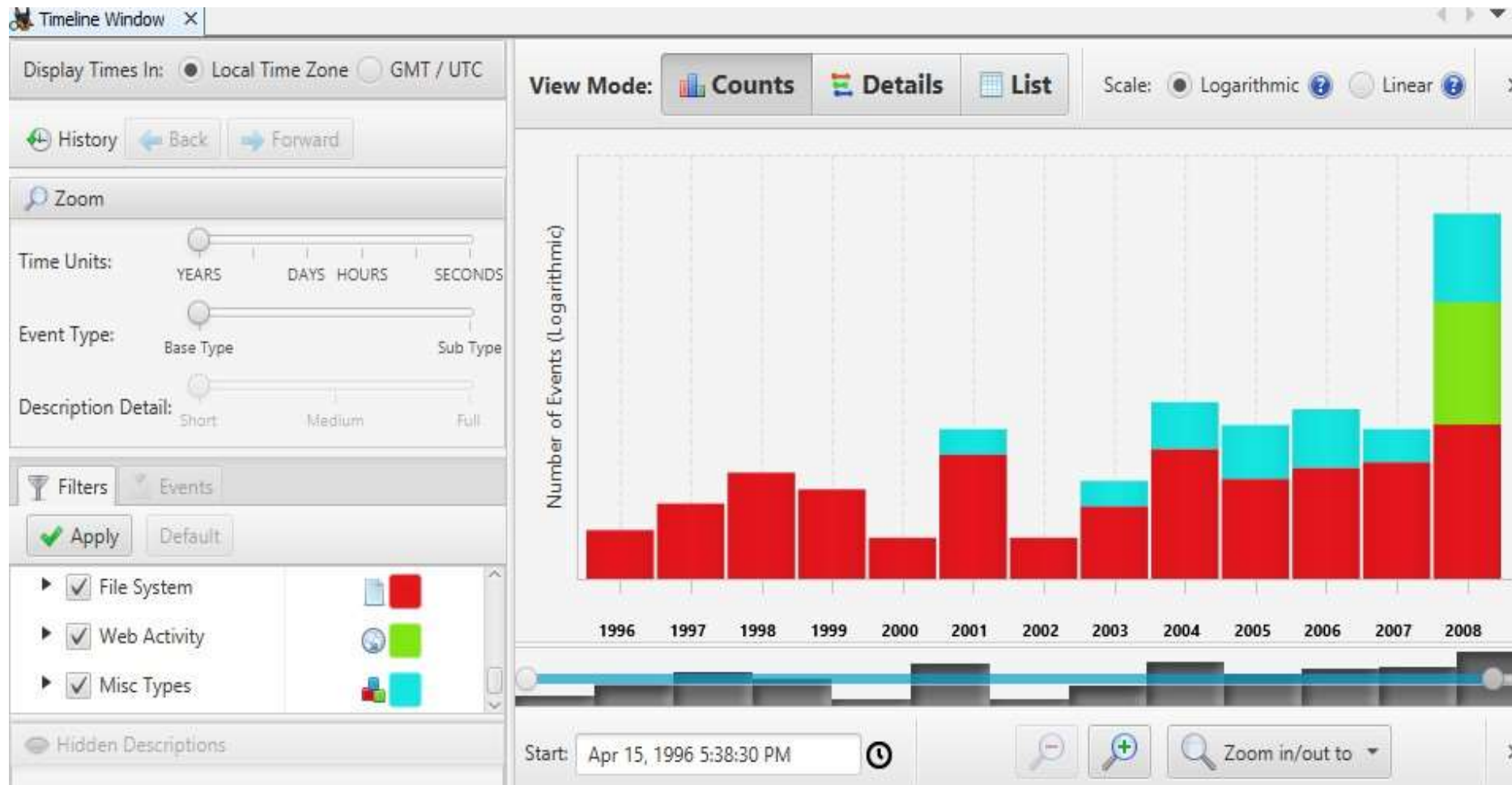
- Name
- Size
- MIME type
- Date
- Good/Bad

The screenshot shows a window titled "File Search by Attributes" with a close button (X) in the top right corner. The window contains the following elements:

- A label: "Search for files that match the following criteria:"
- A checked checkbox labeled "Name:" followed by a text input field.
- A note: "\*Note: Name match is case insensitive and matches any part of the file name. Regular expressions are not currently supported."
- A checked checkbox labeled "Size:" followed by a dropdown menu set to "equal to", a text input field containing "0", and another dropdown menu set to "Byte(s)".
- A checked checkbox labeled "MIME Type:" followed by a list box containing the following items: "application/activemessage", "application/andrew-inset", "application/applefile", and "application/appixware". There are scroll arrows on the right side of the list box.
- A note: "\*Note: Multiple MIME types can be selected"
- A checked checkbox labeled "Date:" followed by two date input fields separated by a "to" label. Below these fields are two notes: "\*Empty fields mean 'No Limit'" and "\*The date format is mm/dd/yyyy".
- A "Timezone:" dropdown menu set to "(GMT+0:00) Europe/London".
- Four checked checkboxes: "Modified", "Accessed", "Created", and "Changed".
- A checked checkbox labeled "Known Status:" followed by three checked checkboxes: "Unknown", "Known (NSRL or other)", and "Known bad".
- A "Search" button at the bottom right.

## TIMELINES

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



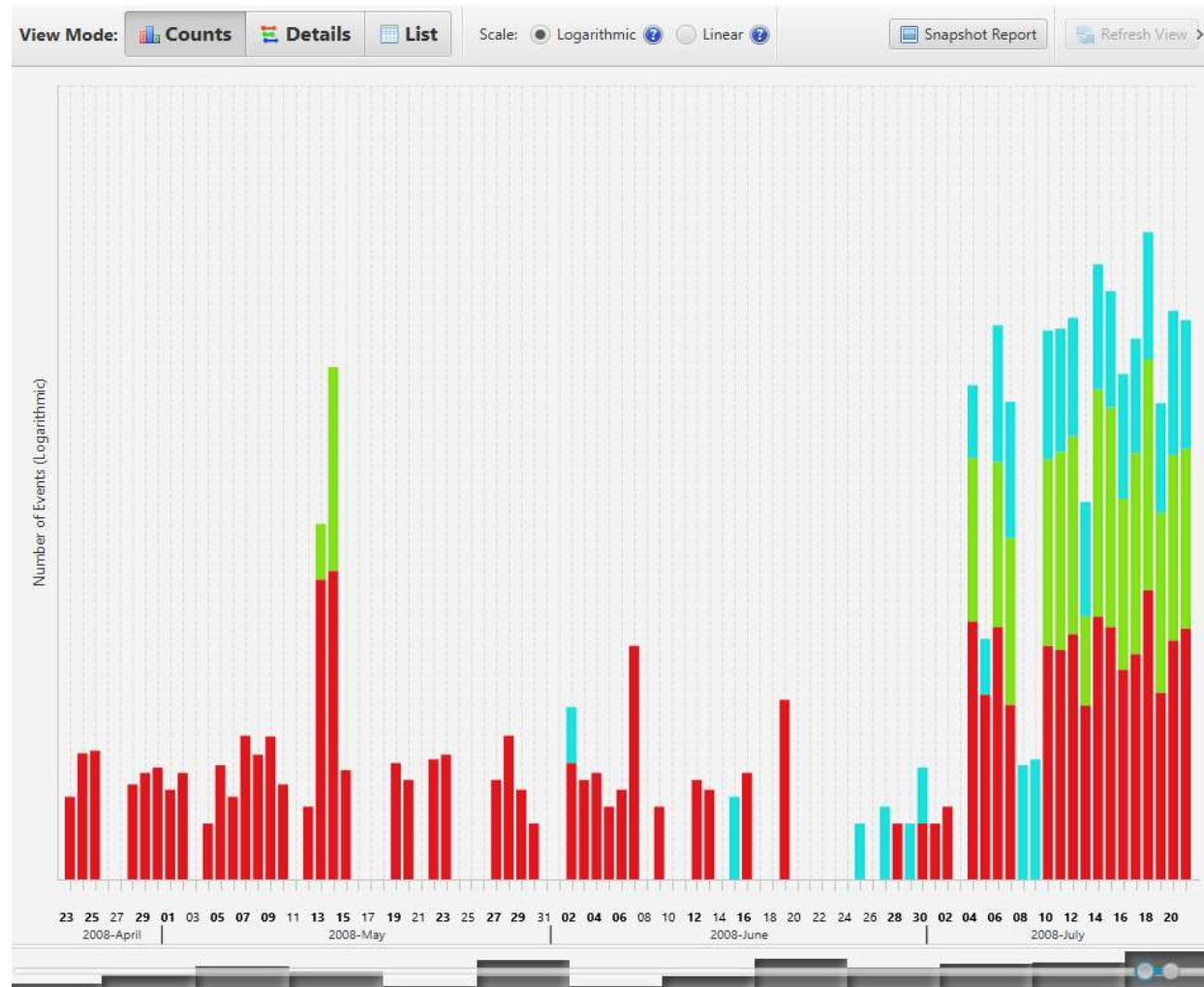


Autopsy recognizes events, such as

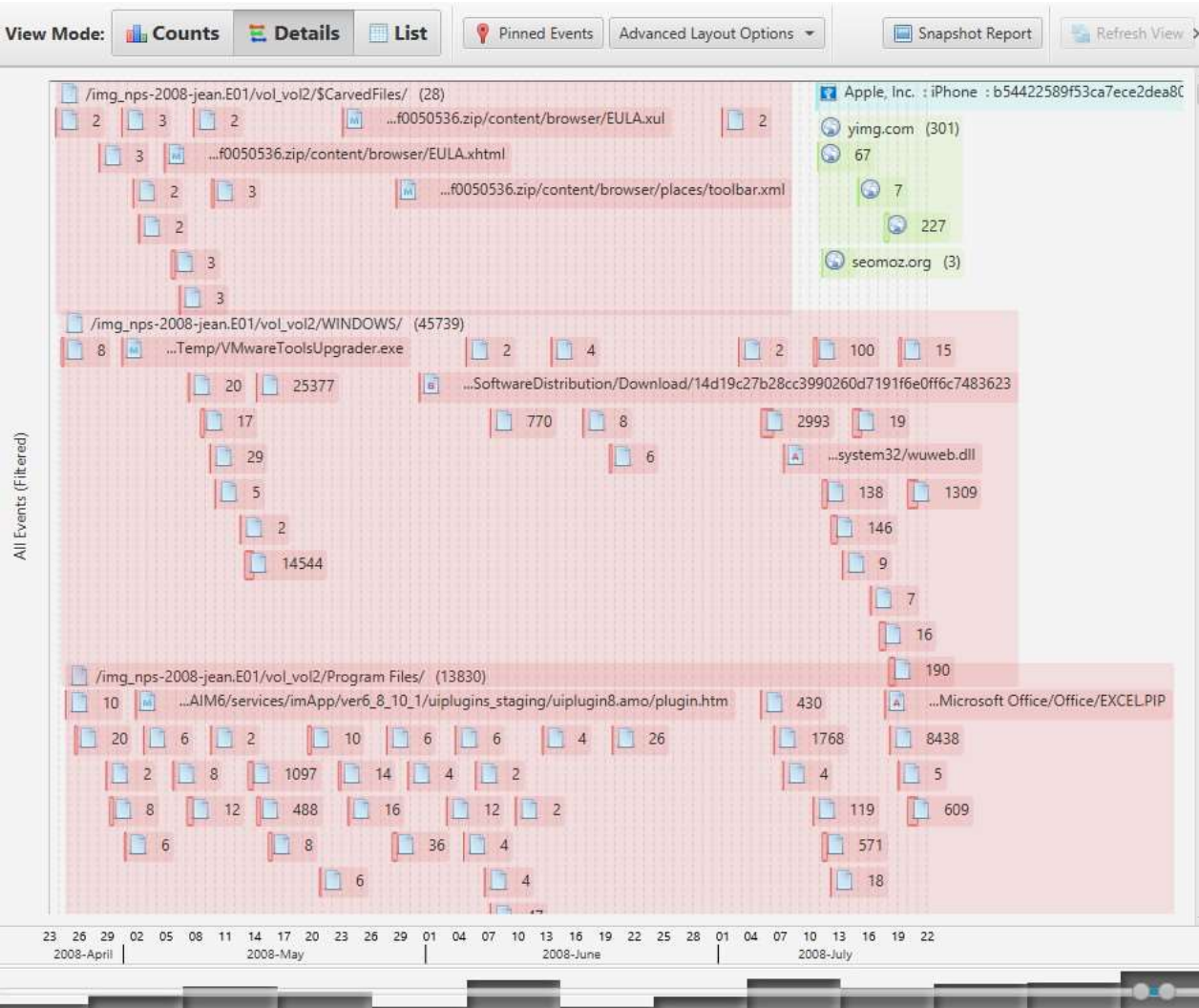
- Files (modification, access, creation, change)
- Internet access (downloads, cookies, bookmarks, searches, browser history)
- Others (messages, phone calls, e-mails, GPS tracks, . . . )

# TIMELINE VISUALIZATION

## HISTOGRAM



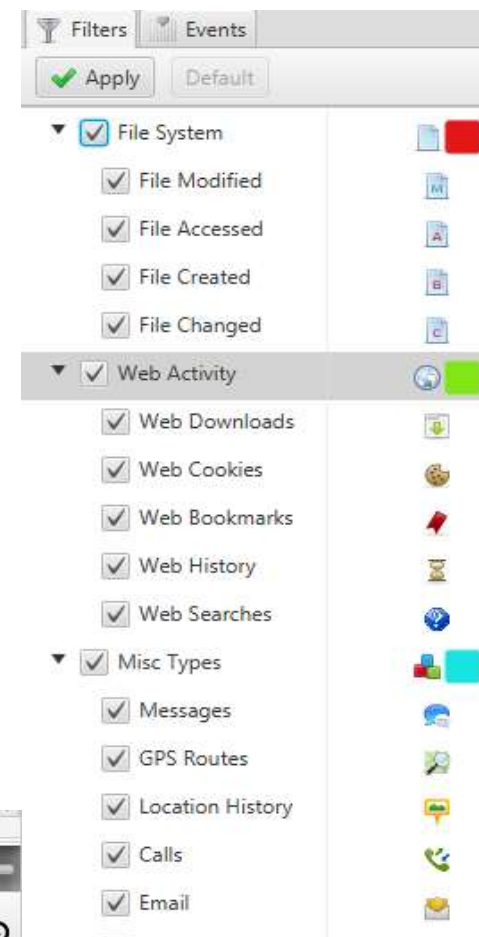
TIMELINE VISUALIZATION  
DETAILED VIEW



## TIMELINE VISUALIZATION FILTERS

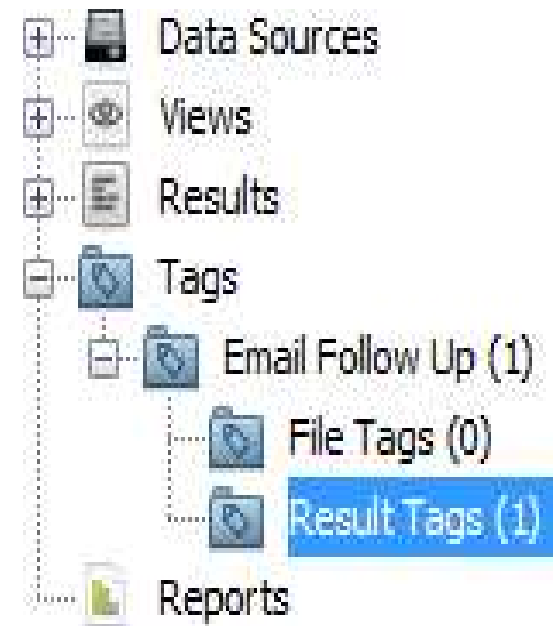
Autopsy allows to reduce the number of elements in a timeline using filters

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



## LABELING

- 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**



## REPORT GENERATION

Several types of reports are available

**Results:** Applies to the items of the results view,

 Generate Report

### Select and Configure Report

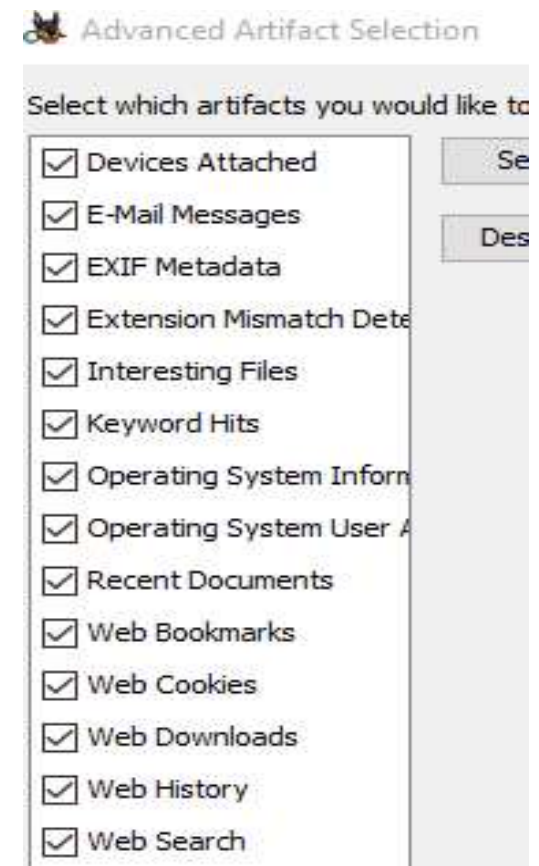
Report Modules:

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

## REPORT GENERATION

Several types of reports are available

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



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

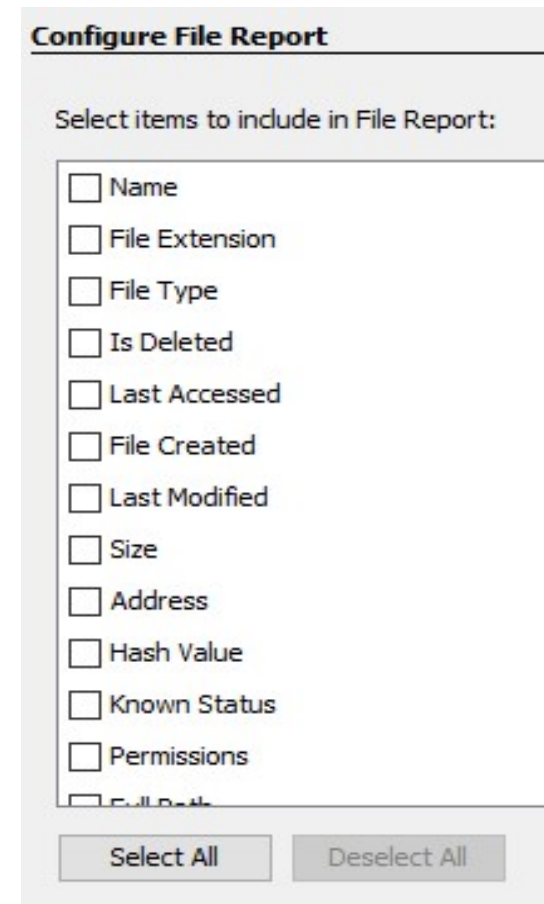


Several types of reports are available

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

**Tagged:** Applies to the tagged items

**Files:** List of files under analysis



The screenshot shows a dialog box titled "Configure File Report". Inside, there is a section labeled "Select items to include in File Report:" followed by a list of checkboxes. The items are: Name, File Extension, File Type, Is Deleted, Last Accessed, File Created, Last Modified, Size, Address, Hash Value, Known Status, Permissions, and Full Path. At the bottom of the dialog, there are two buttons: "Select All" and "Deselect All".

Item	Selected
Name	<input type="checkbox"/>
File Extension	<input type="checkbox"/>
File Type	<input type="checkbox"/>
Is Deleted	<input type="checkbox"/>
Last Accessed	<input type="checkbox"/>
File Created	<input type="checkbox"/>
Last Modified	<input type="checkbox"/>
Size	<input type="checkbox"/>
Address	<input type="checkbox"/>
Hash Value	<input type="checkbox"/>
Known Status	<input type="checkbox"/>
Permissions	<input type="checkbox"/>
Full Path	<input type="checkbox"/>

Select All Deselect All

## REPORT GENERATION

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>

## STRUCTURED THREAT INFORMATION EXCHANGE (STIX)

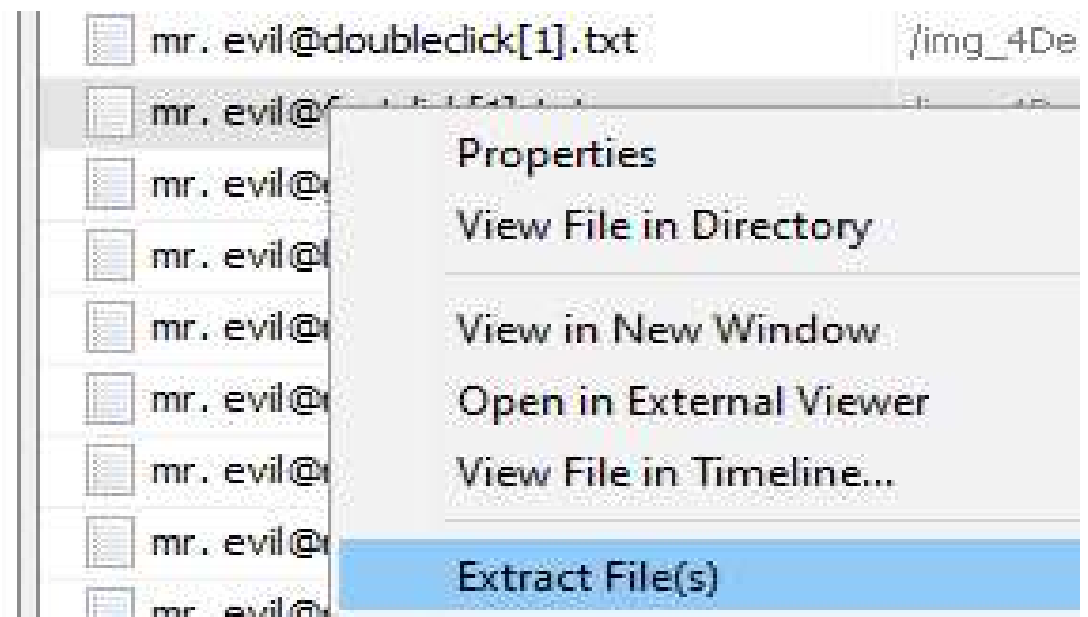
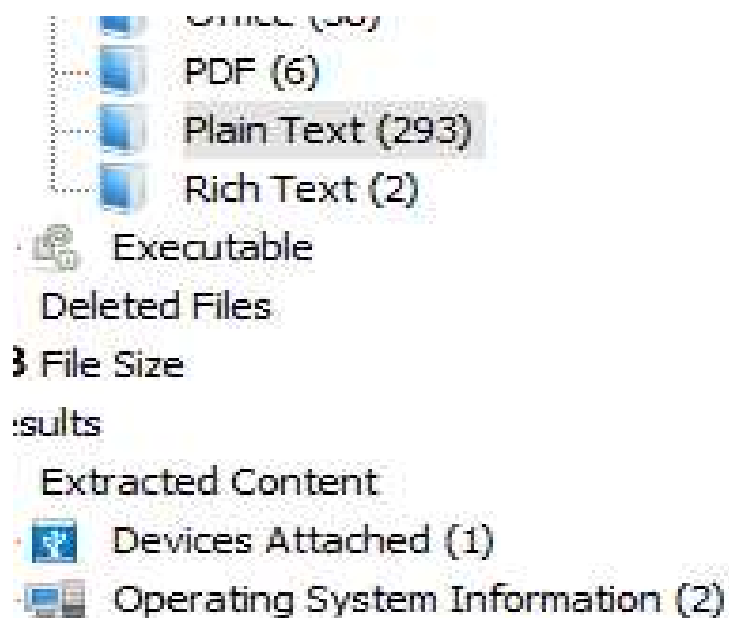
Example: IP address

```
...
<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>
...
```

## EXPORTING EVIDENCES

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

ANY QUESTIONS?

