universidade
de aveiro

Computer Systems Forensic Analysis
AFSC

Autopsy

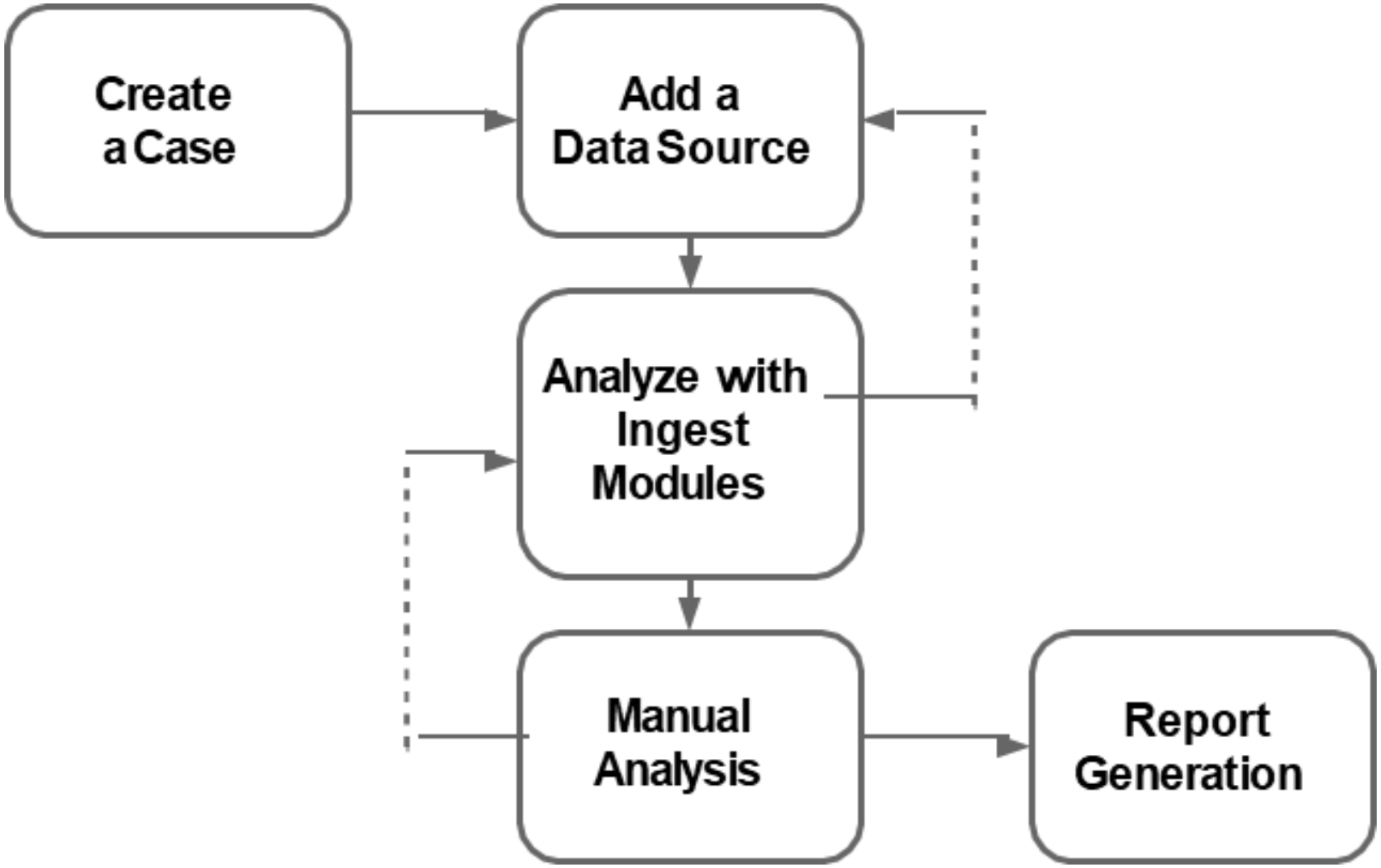
Artur Varanda

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*

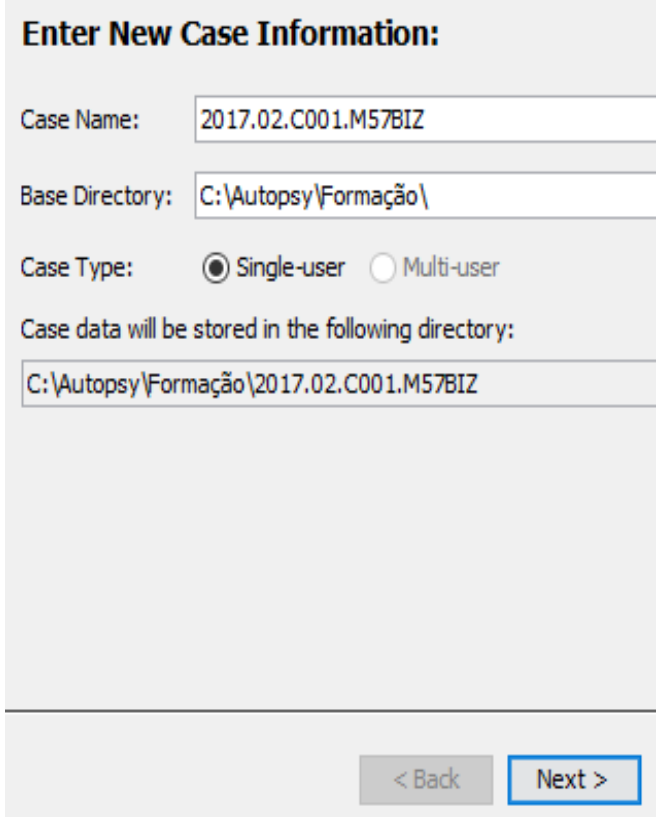
AUTOPSY WORKFLOW



1 - Create a Case

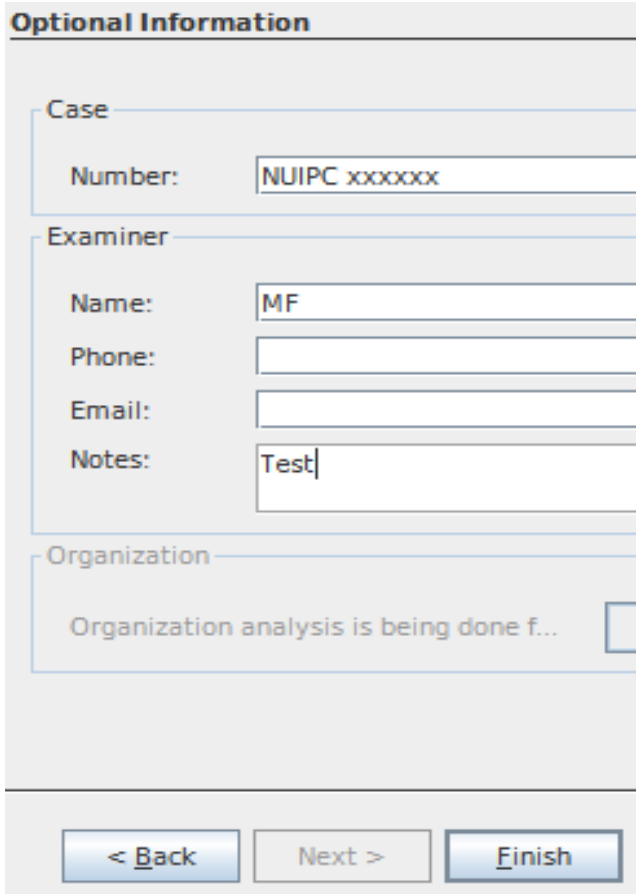
1 - Create a Case

- Case Information



1 - Create a Case

- Case Information
- Case number, examiner

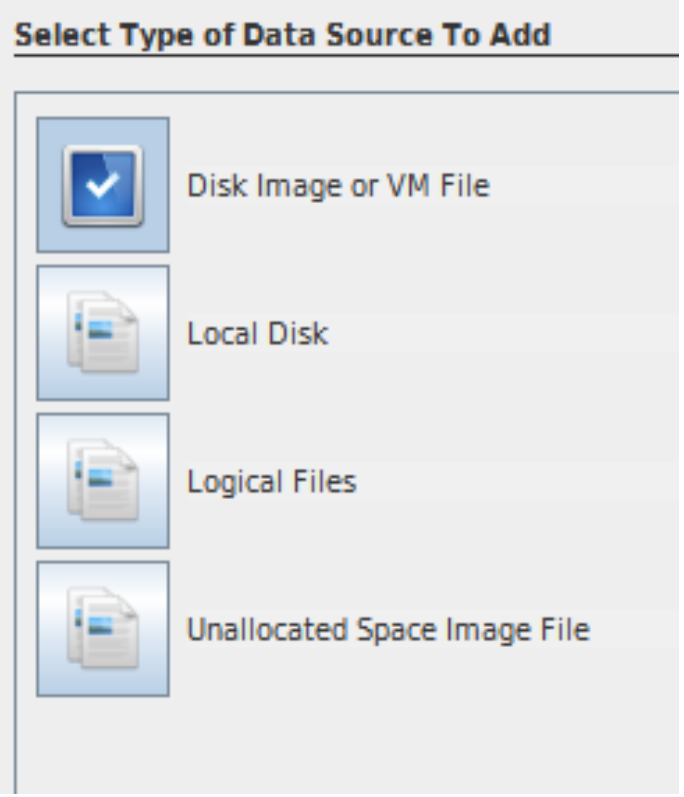


1 - Create a Case

- 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)

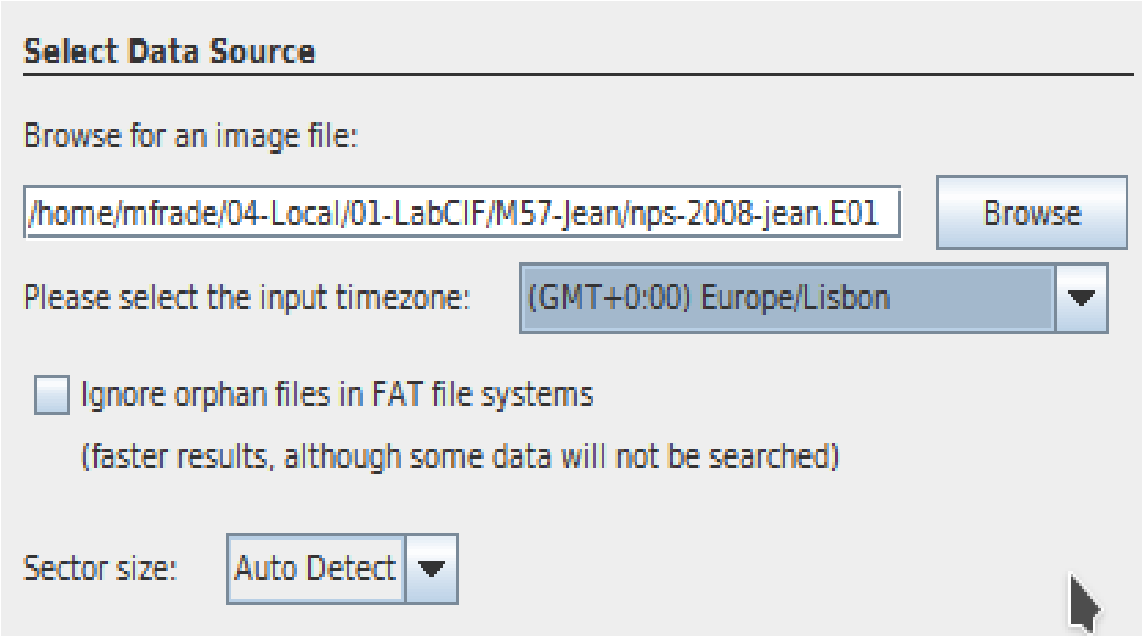


1 - Create a Case

- 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)



AUTOMATED PROCESSING – WITH INGEST MODULES

Configure Ingest Modules

Run ingest modules on:

All Files, Directories, and Unallocated Space

- [x] Recent Activity
- [x] Hash Lookup
- [x] File Type Identification
- [x] Embedded File Extractor
- [x] Exif Parser
- [x] Keyword Search
- [x] Email Parser
- [x] Extension Mismatch Detector
- [x] E01 Verifier
- [x] Encryption Detection
- [x] Interesting Files Identifier
- [x] PhotoRec Carver
- [x] Correlation Engine
- [x] Virtual Machine Extractor
- [x] Android Analyzer

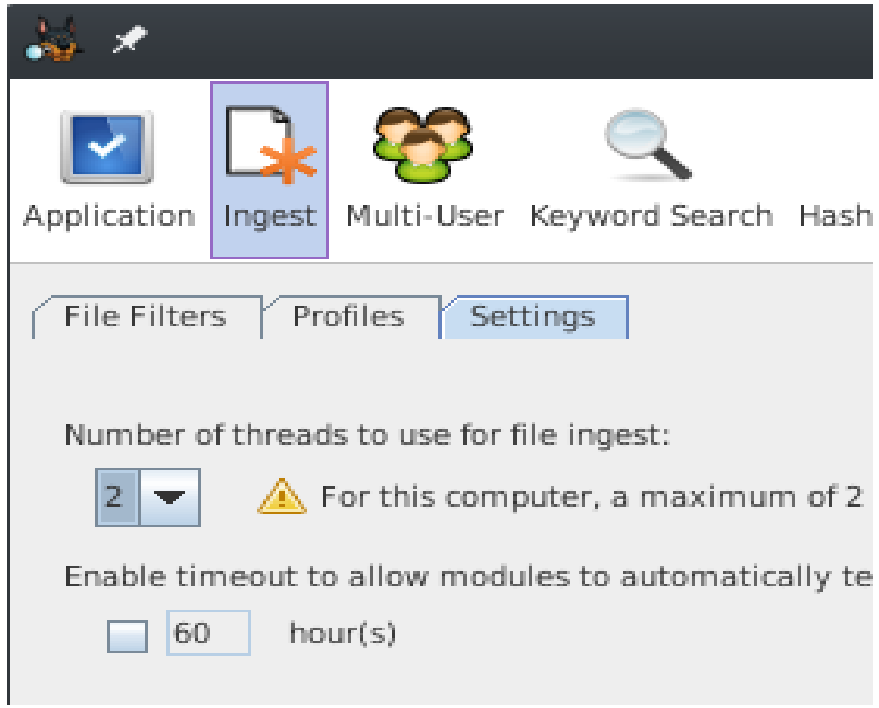
Select All | Deselect All | History

The selected module has no per-run settings.

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

Global Settings

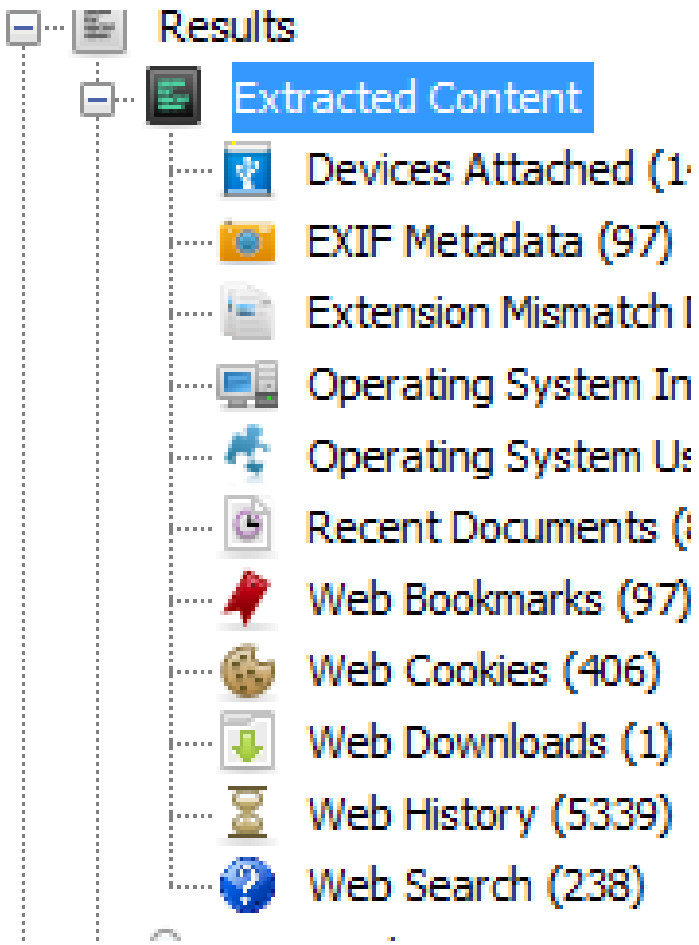
- *Autopsy* supports *multi-thread* execution of *file ingest*
- Aims to reduce the processing time
- Requires setting of the number of *threads* to use
- **Tools → Options → Ingest → Settings**



Extracts information from the last 7 days

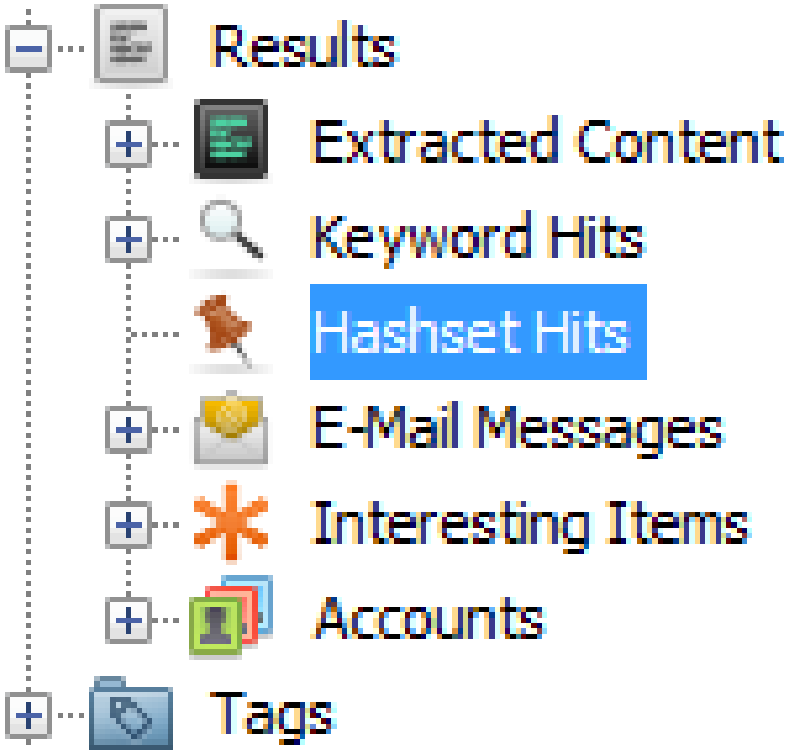
- Internet usage (including searches)
- Installed programs
- Connected devices (USB)
- Processes the *Registry hive*

The information is displayed in
Results → Extracted Content



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

- 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

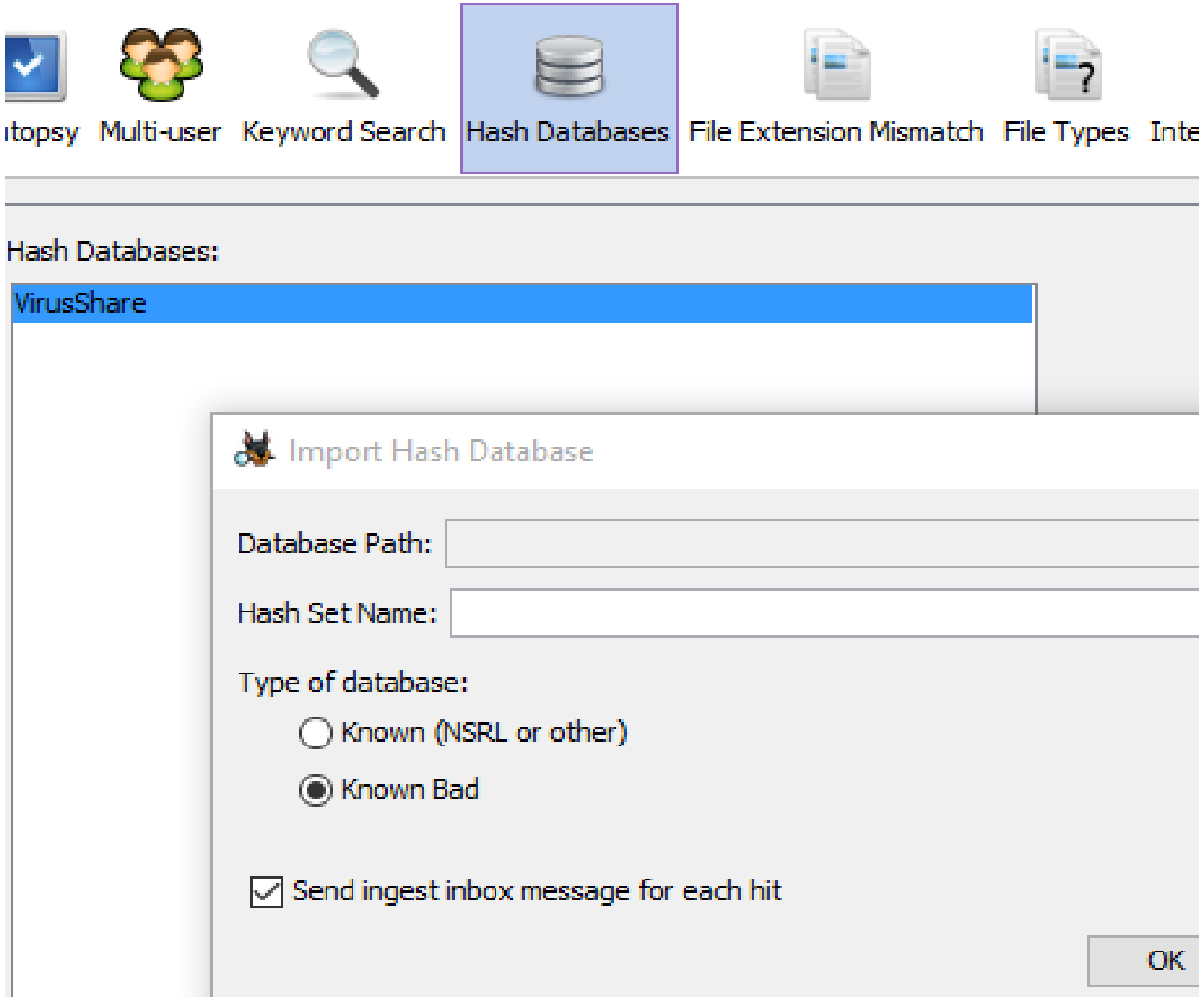
URL: https://www.nsrl.nist.gov/

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

VirusShare

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

MODULE: HASH LOOKUP – HASH SETS



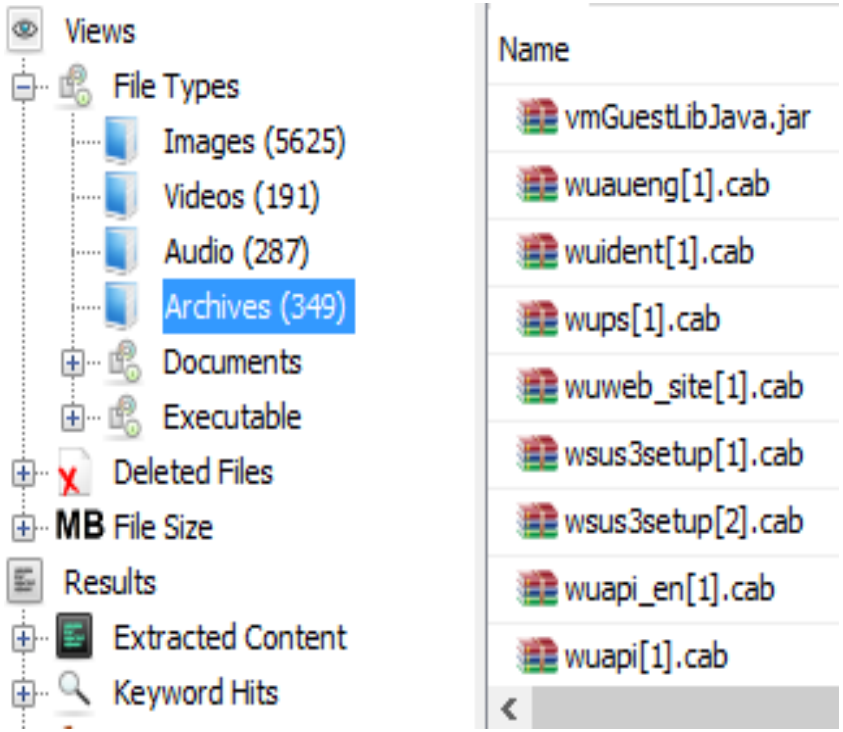
MODULE: FILE TYPE IDENTIFICATION

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

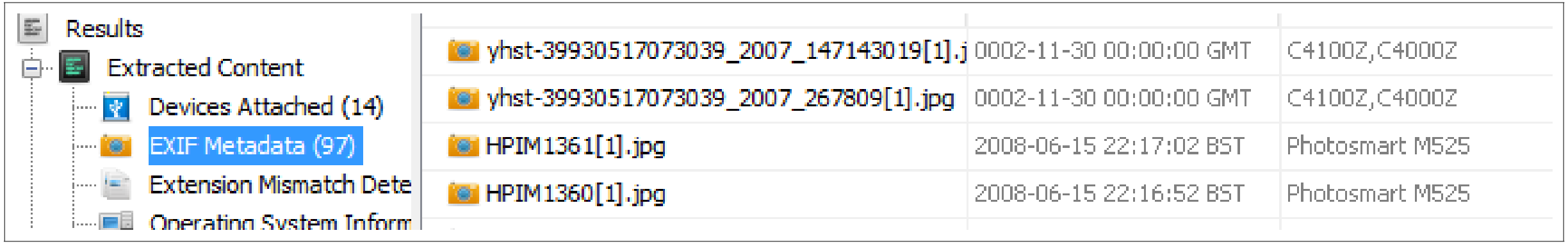
Uncompress files (ZIP, RAR) or embedded files (DOC, DOCX, PPT, PPTX, XLS and XLSX), processing them again.

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



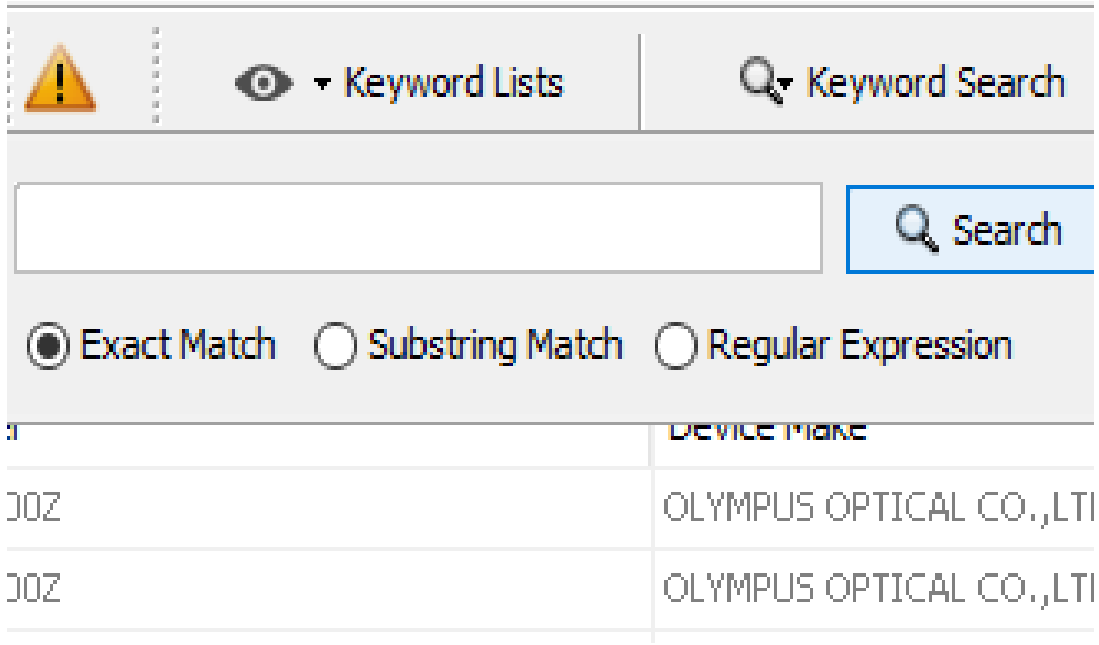
Extracts EXIF (*Exchangeable Image File Format*) information stored on images

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



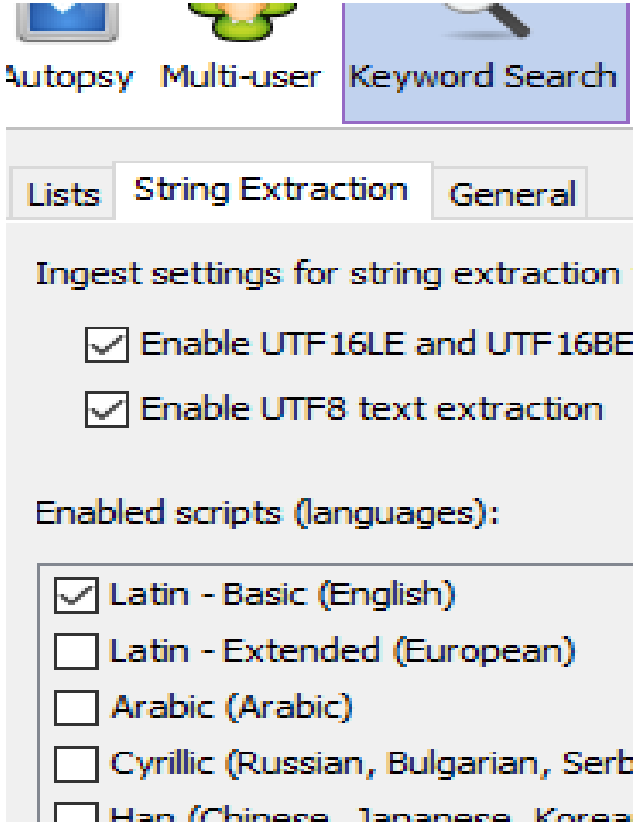
Search by keywords during initial or on-demand processing

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



Search by keywords during initial or on-demand processing

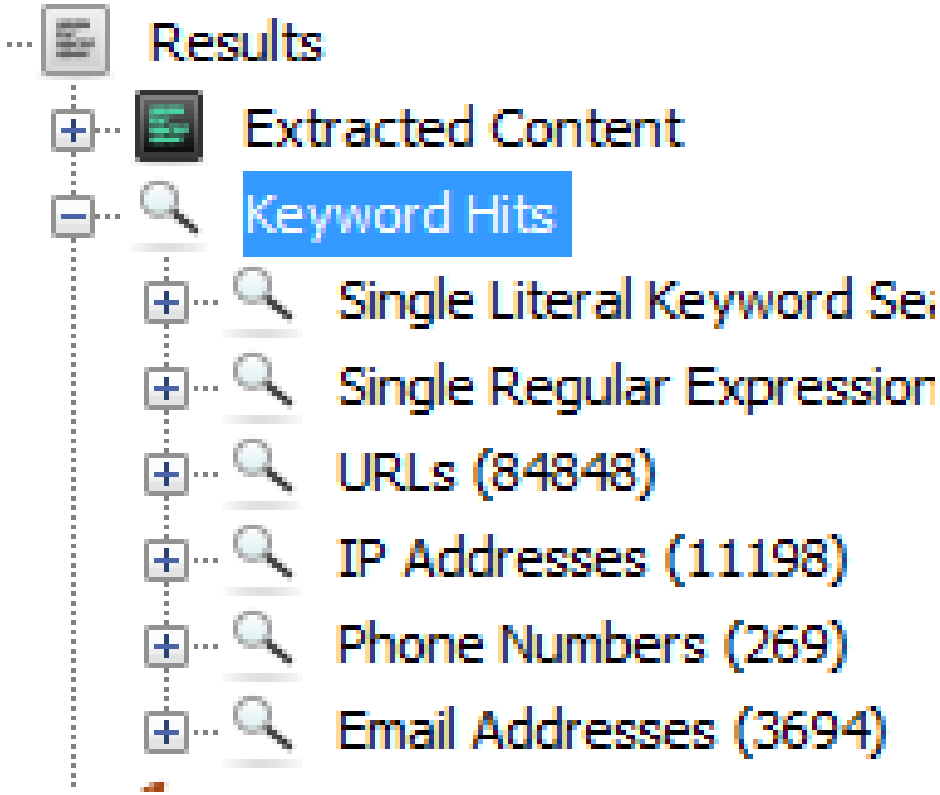
- Extracts text from the files being processed and adds them to an index (Solr)
- Supports several formats (Text, MS Office, PDF, Emails)
- For non-supported formats
  - ✓ String Extraction algorithm
  - ✓ Is able to identify encodings and languages



Autopsy includes a set of predefined lists of common expressions

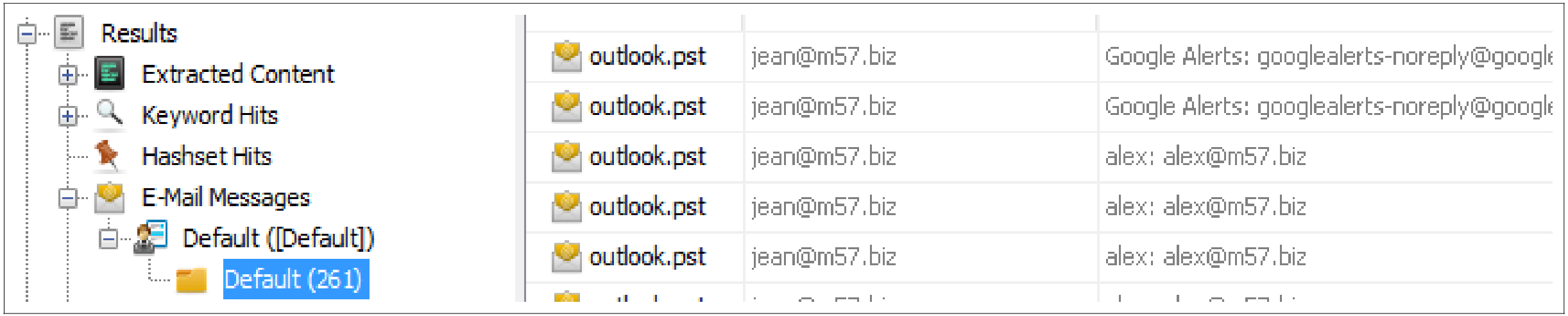
- Web addresses (URLs)
- IP addresses
- Phone numbers E-mail addresses

Unfortunately, they generate a huge amount of false positives



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

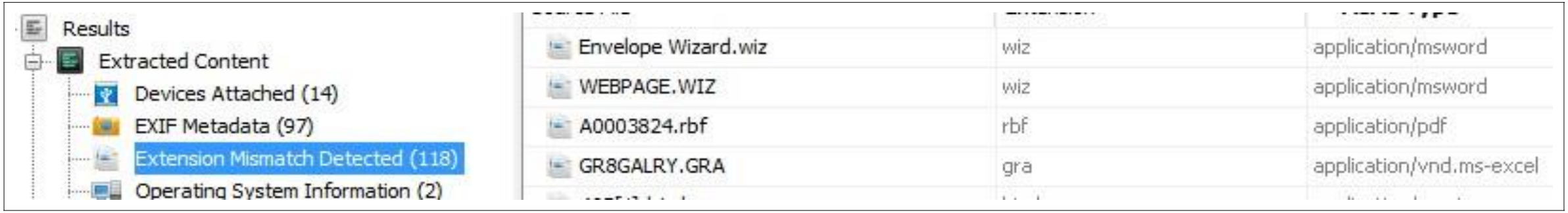
- Extract contained e-mails
- Processes its attachments



MODULE: EXTENSION MISMATCH DETECTOR

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

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



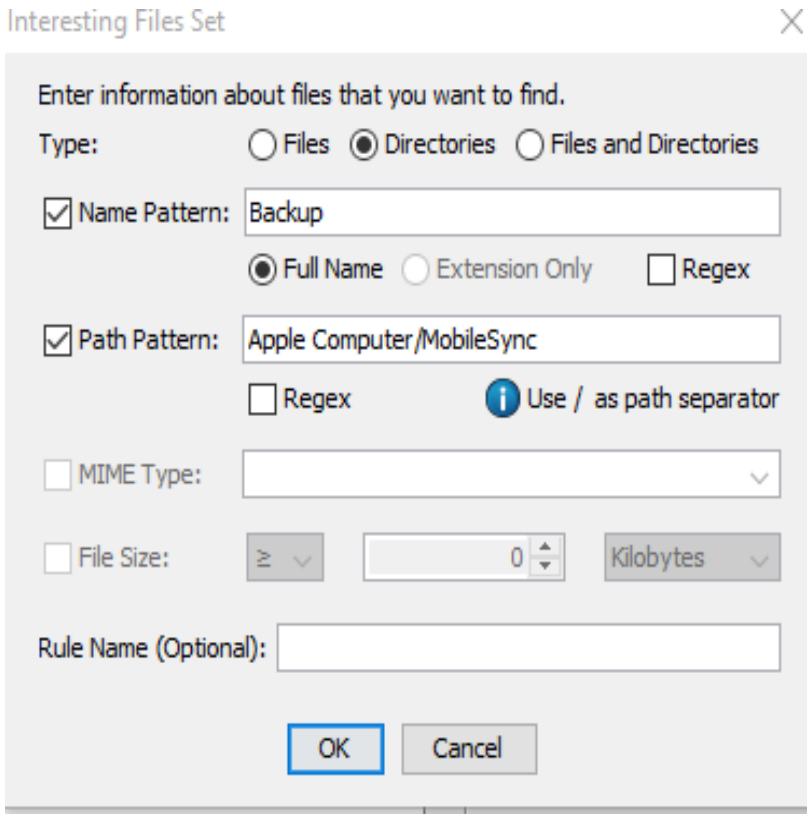
MODULE: E01 VERIFIER

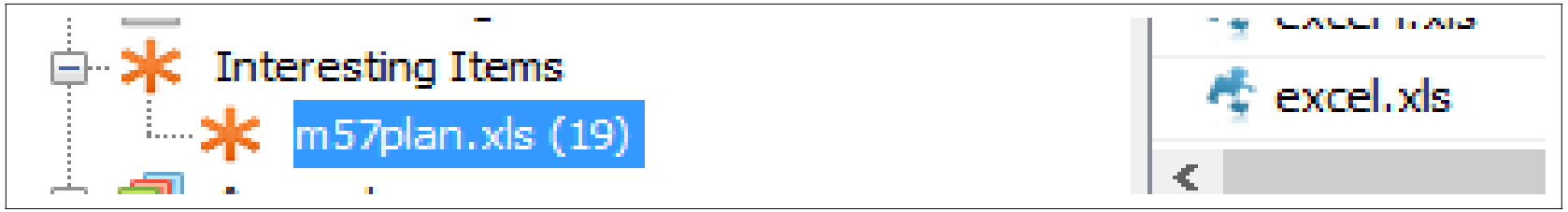
Verifies the hash value of the data stored in EWF files

- 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

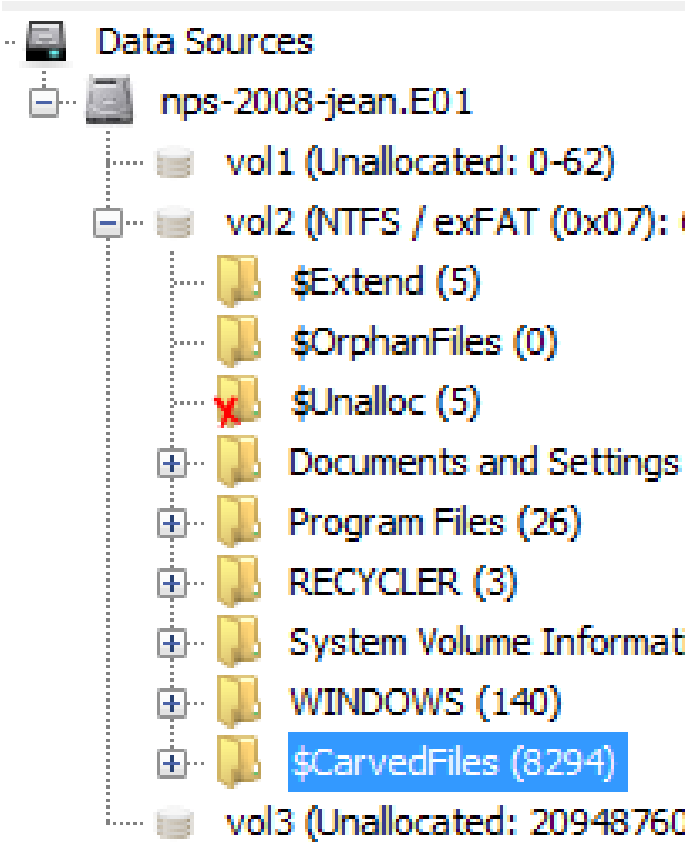
- Type (file / folder)
- Size, extension
- Name, path
- MIME type





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



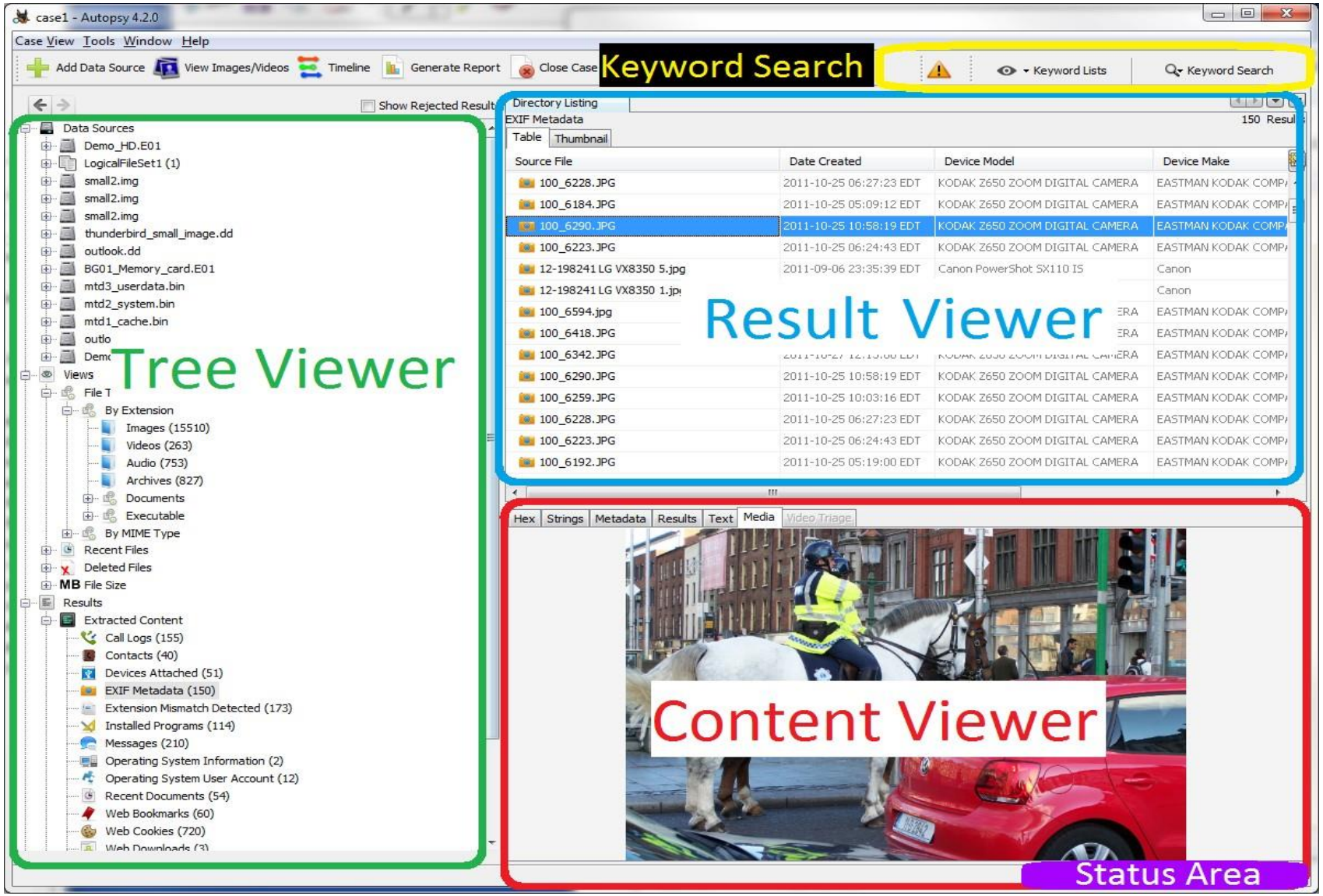
MODULE: VIRTUAL MACHINE EXTRACTOR

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.

IMAGE GALLERY

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

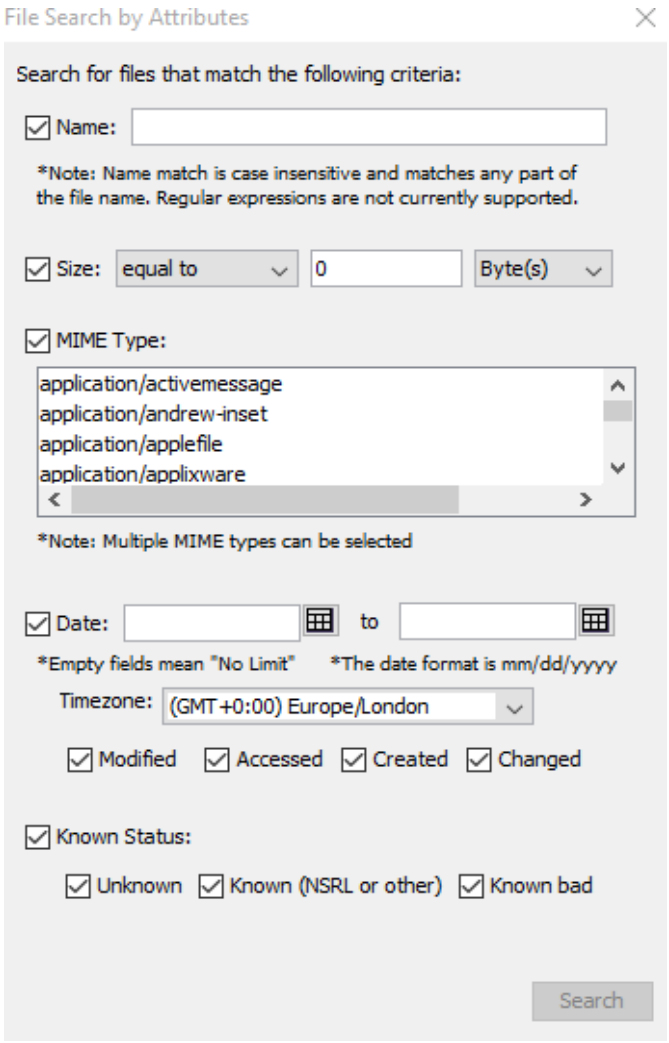
- Group images by folder, compressed file
- Allows viewing of images when detected
- Functionality can be activated /deactivated in the options
- Allows cataloging of images (for child pornography and similar tasks)

FILE SEARCH

Useful when searching for a file with specific characteristics.

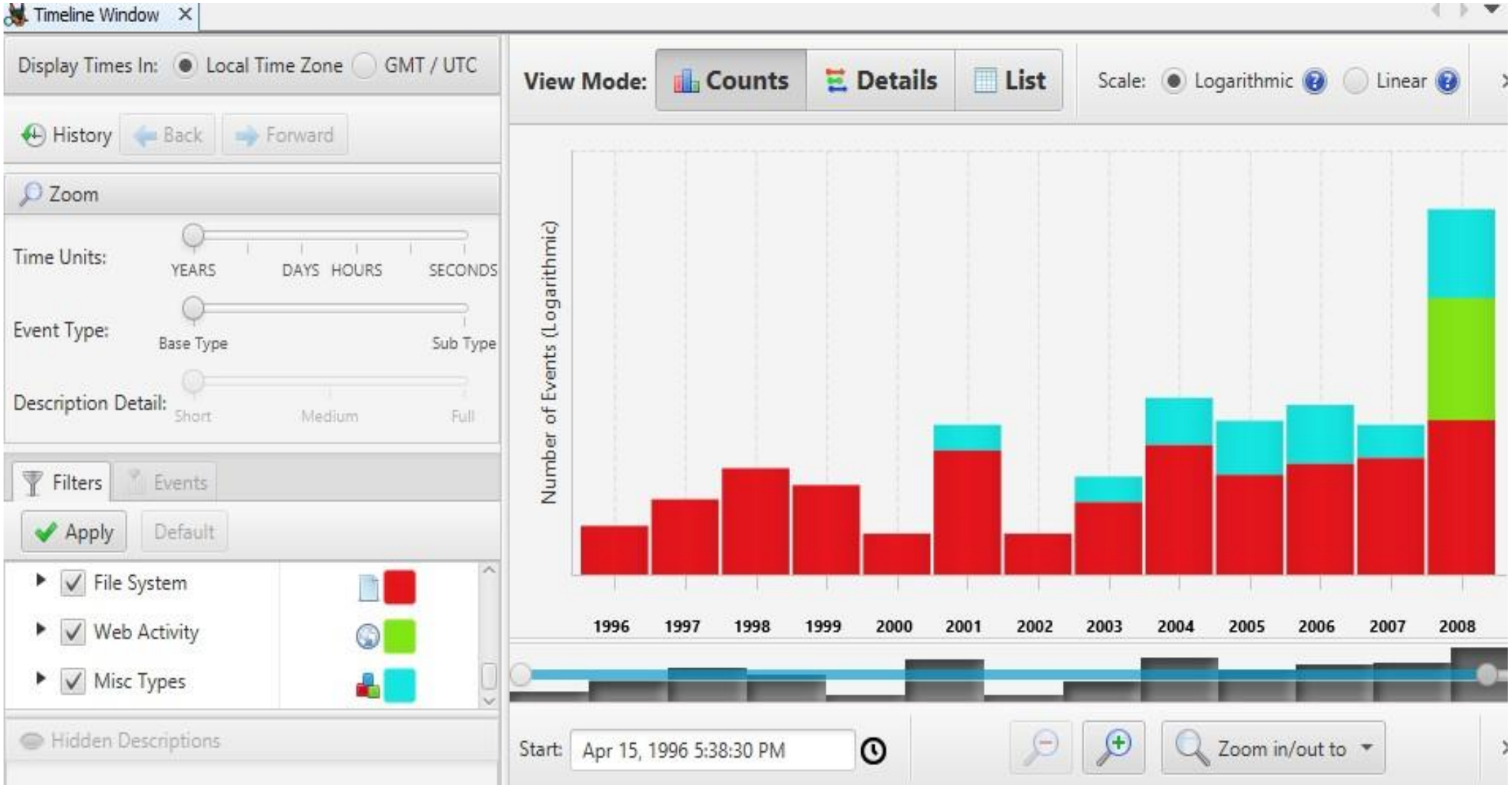
It is available in the *Tools* menu

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



TIMELINES

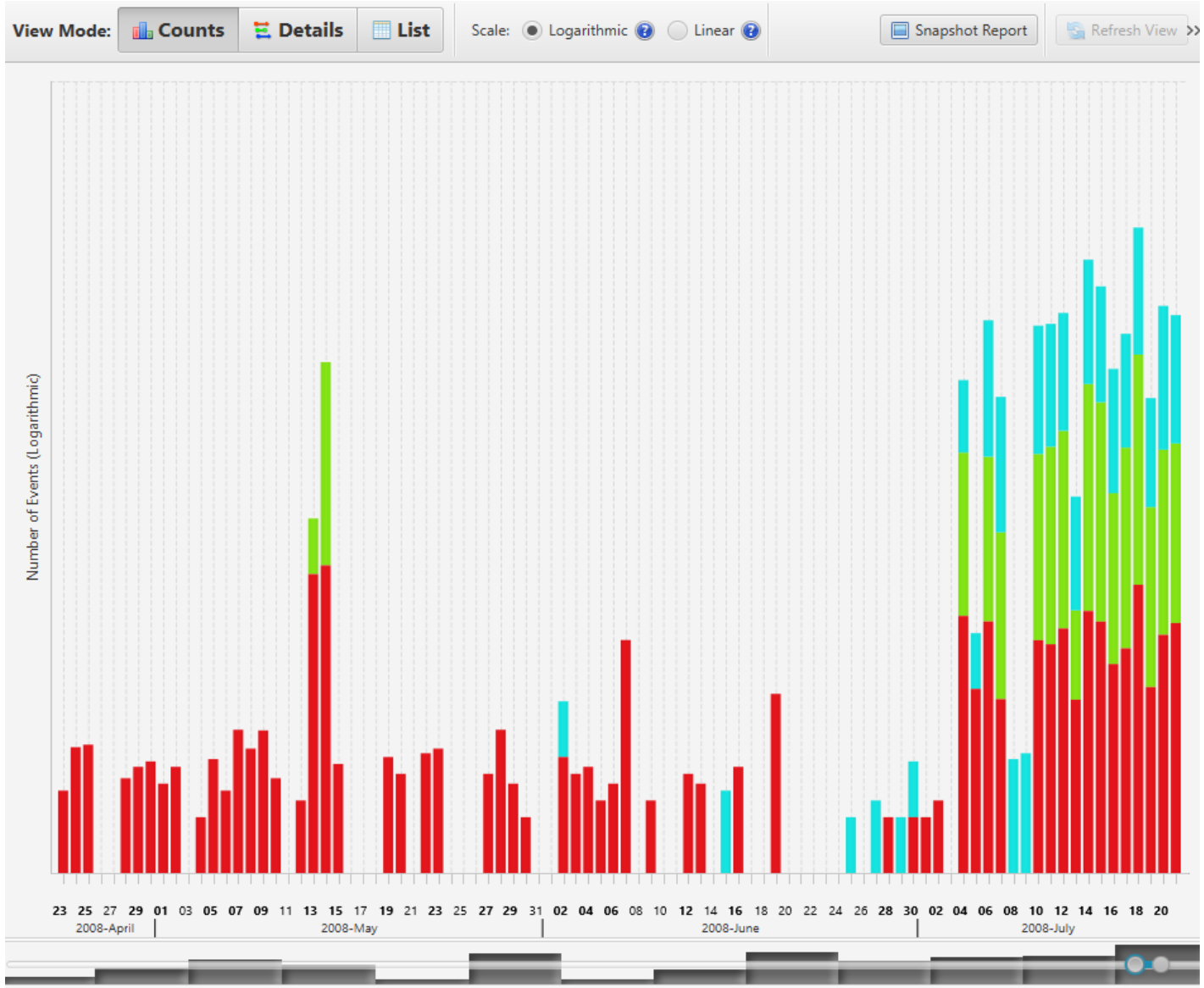
After indexing events, Autopsy allows you to create timelines based on the dates on which such events occurred



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

View Mode: Counts | Details | List | Pinned Events | Advanced Layout Options | Snapshot Report | Refresh View

All Events (Filtered)

/img_nps-2008-jean.E01/vol_vol2/$CarvedFiles/ (28)

...f0050536.zip/content/browser/EULA.xul

...f0050536.zip/content/browser/EULA.xhtml

...f0050536.zip/content/browser/places/toolbar.xml

Apple, Inc. : iPhone : b54422589f53ca7ece2dea8(

yimg.com (301)

seomoz.org (3)

/img_nps-2008-jean.E01/vol_vol2/WINDOWS/ (45739)

...Temp/VMwareToolsUpgrader.exe

...SoftwareDistribution/Download/14d19c27b28cc3990260d7191f6e0ff6c7483623

...system32/wuweb.dll

/img_nps-2008-jean.E01/vol_vol2/Program Files/ (13830)

...AIM6/services/imApp/ver6_8_10_1/uiplugins_staging/uiplugin8.amo/plugin.htm

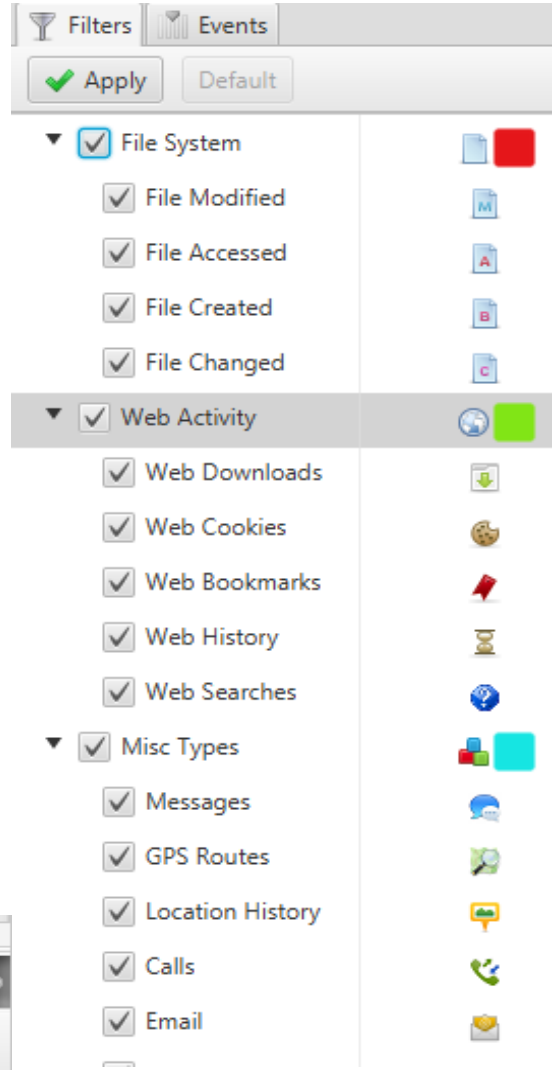
...Microsoft Office/Office/EXCEL.PIP

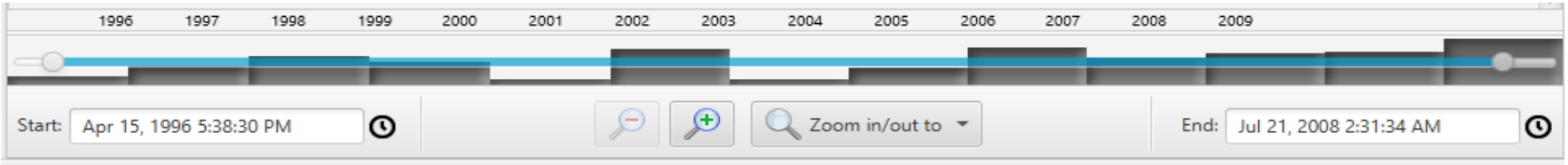
23 26 29 02 05 08 11 14 17 20 23 26 29 01 04 07 10 13 16 19 22 25 28 01 04 07 10 13 16 19 22

2008-April | 2008-May | 2008-June | 2008-July

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

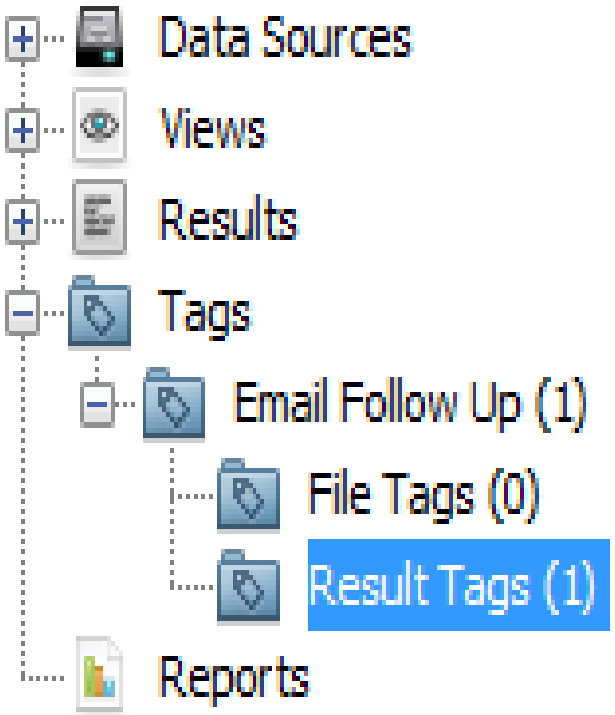
- Filter known files
- Filter by text
- Event type
- Time windows





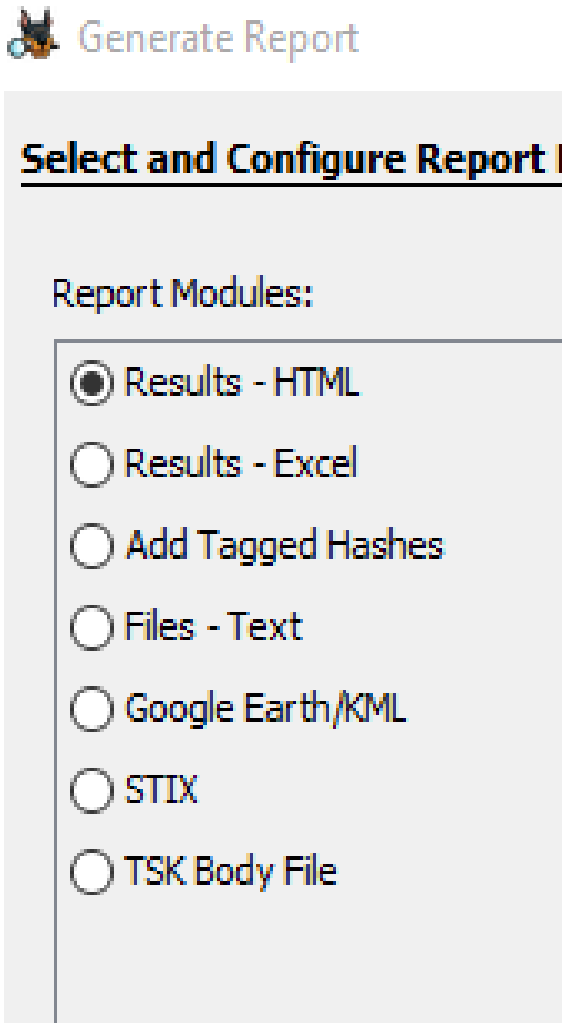
LABELING

- 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**



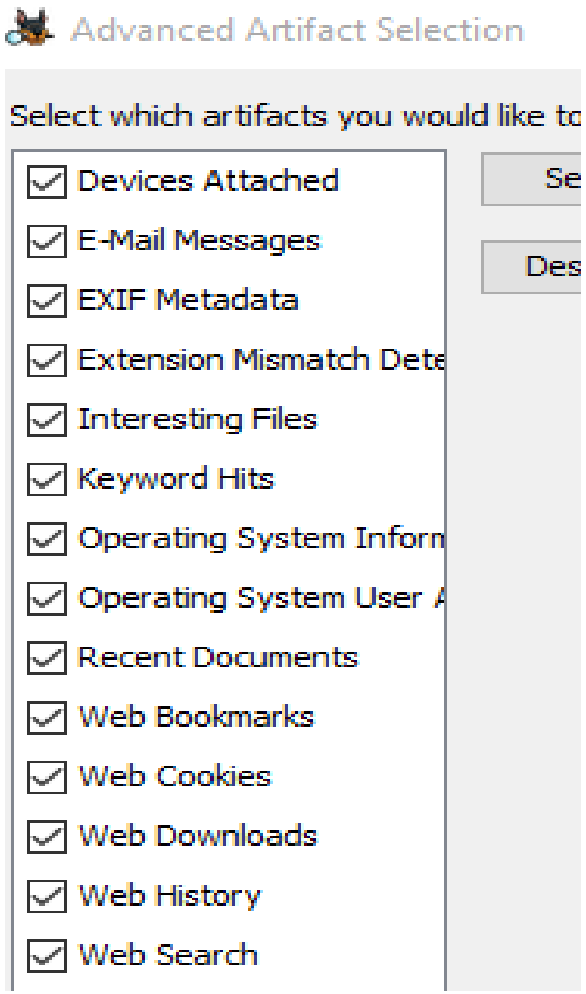
Several types of reports are available

Results: Applies to the items of the results view,



Several types of reports are available

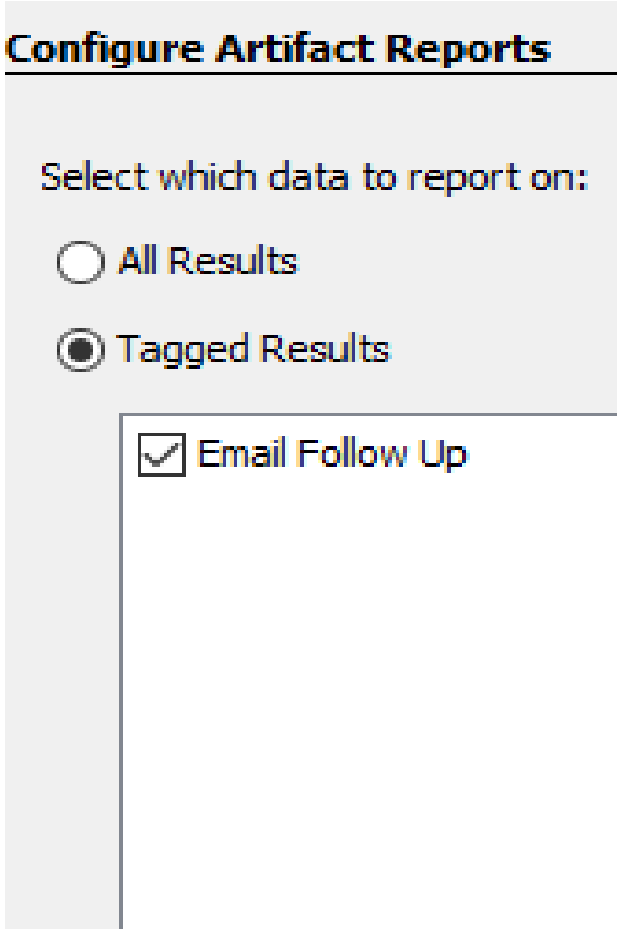
Results: Applies to the items of the results view, can be filtered



Several types of reports are available

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

Tagged: Applies to the tagged items

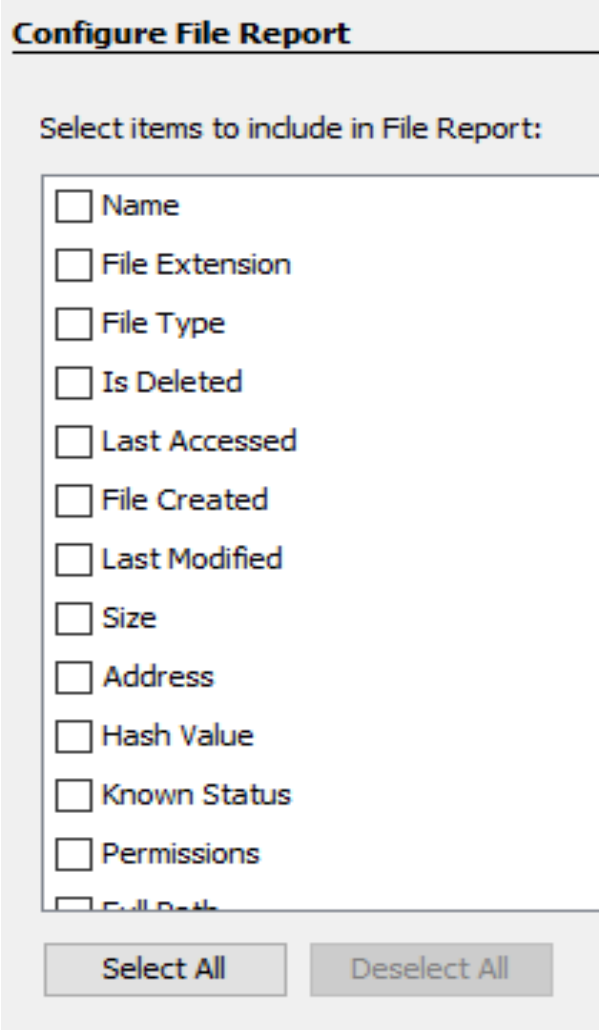


Several types of reports are available

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

Tagged: Applies to the tagged items

Files: List of files under analysis



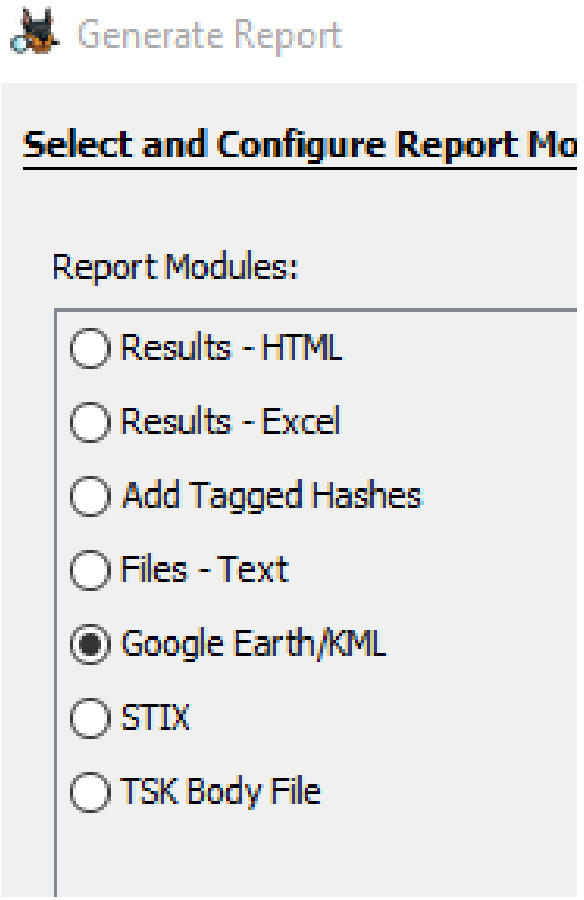
Several types of reports are available

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



Several types of reports are available

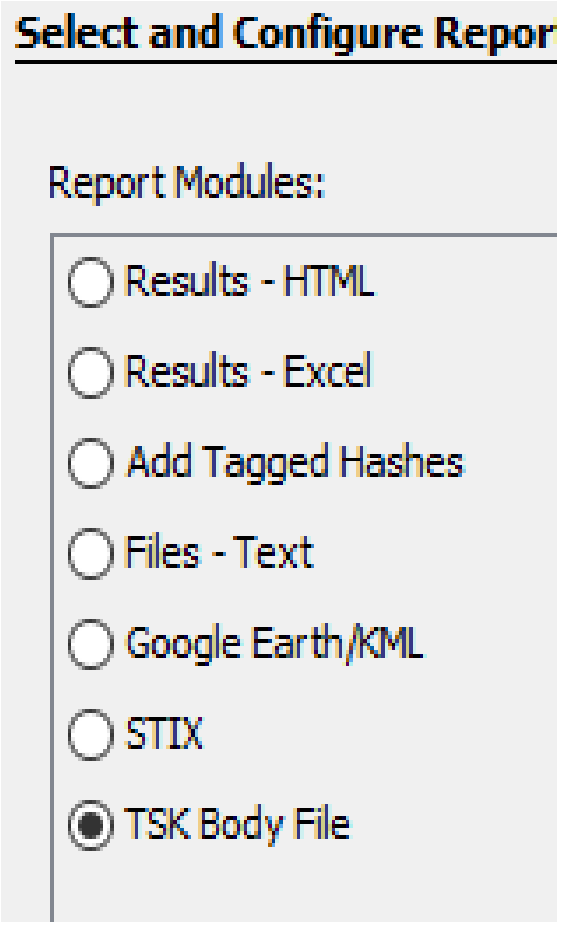
Results: Applies to the items of the results view, can be filtered

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



Several types of reports are available

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

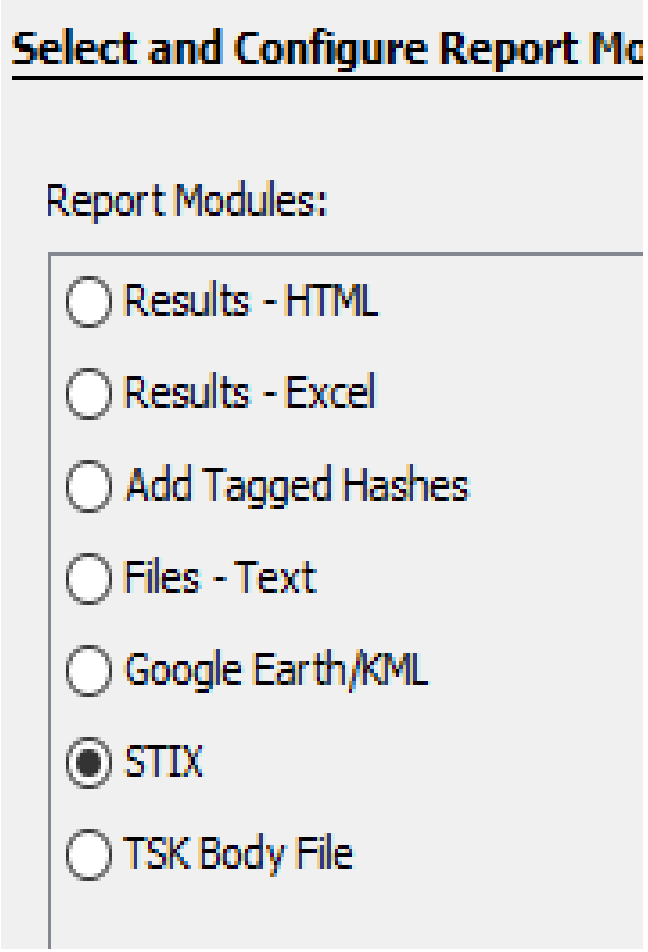
Tagged: Applies to the tagged items

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



STRUCTURED THREAT INFORMATION EXCHANGE (STIX)

- 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

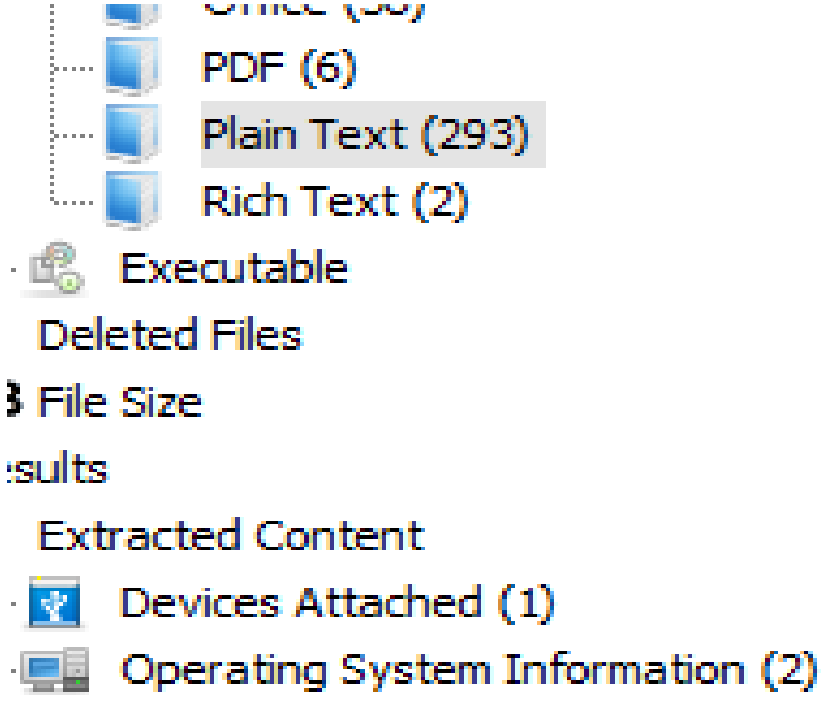
STRUCTURED THREAT INFORMATION EXCHANGE (STIX)

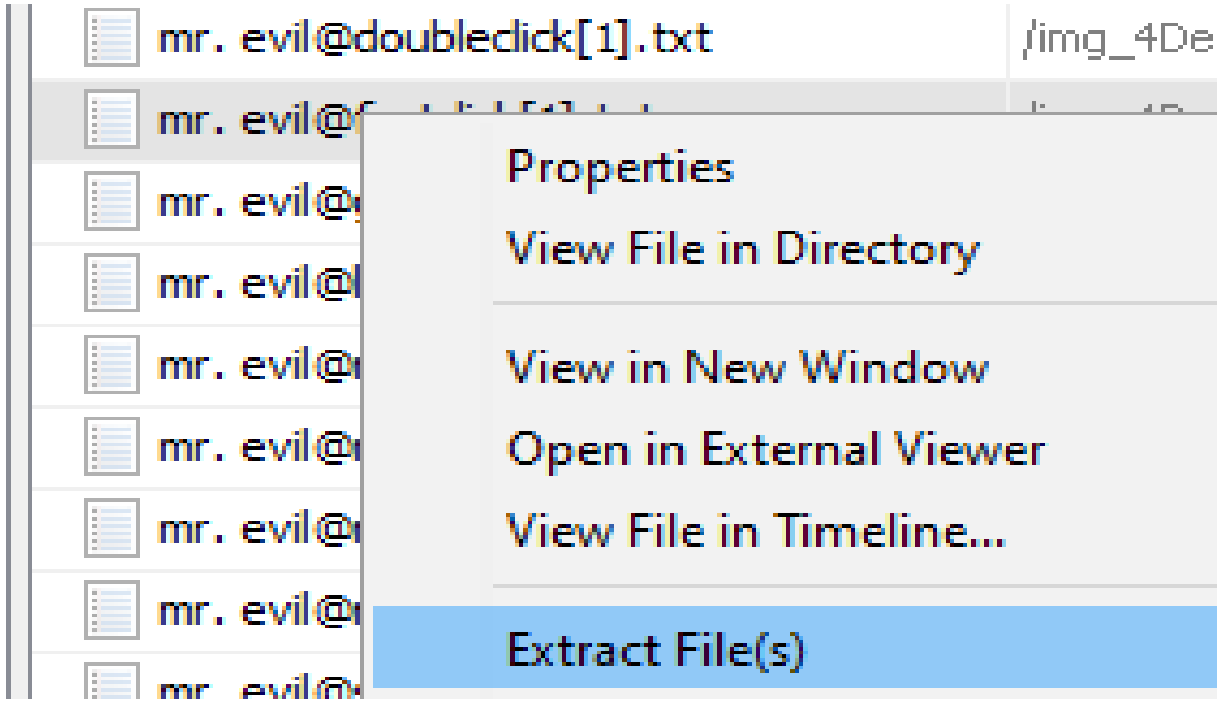
Example: IP address

```
...
<stix:Indicators>
    <stix:Indicator xsi:type="indicator:IndicatorType" id="apinto:Indicador-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-9456-62f078cfdf0b">
            <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

ANY QUESTIONS?