

8th Annual

##OSDFCon

OPEN SOURCE DIGITAL FORENSICS CONFERENCE

October 17, 2017 | Herndon, VA | Hosted by  BASIS
TECHNOLOGY

Triaging Media with Autopsy

Richard Cordovano
Basis Technology

What Problem Are We Trying to Solve?

- You need to be able to make a quick decision when faced with a lot of data.
 - Doing a knock and talk. Want to know if there is notable data on the system in question.
 - At a location where there are lots of systems. Want to know which to analyze first (or which to image / grab).

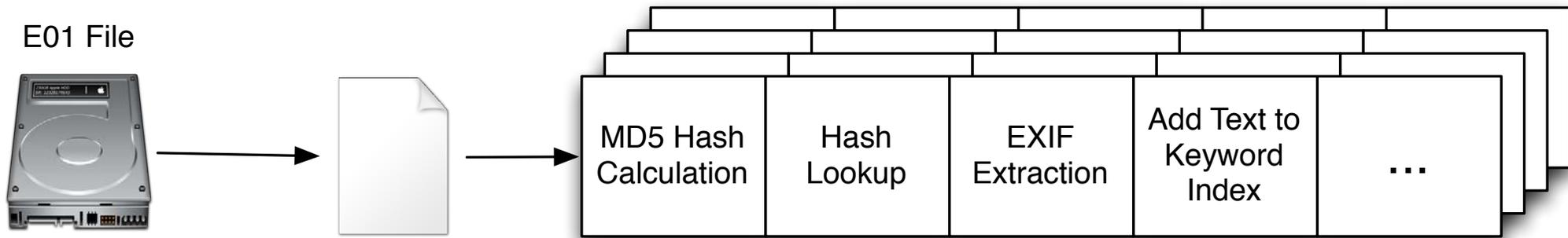
- Focus on files and locations that are most likely to be relevant.
- Make a partial image of the drive as we read it that can be later opened and analyzed.

1. Plug drive into laptop via write blocker.
2. Run Autopsy and choose an “Ingest Profile”
3. Autopsy focuses on a subset of files and looks at hashes, keywords, etc.
4. VHD image file is made as the analysis is happening.
5. You see the results in real time and navigate the system at will.
6. Unplug external drive when done (or press Cancel).

Triaging Feature: Focus on The Relevant Files

Short Time Requires Focus

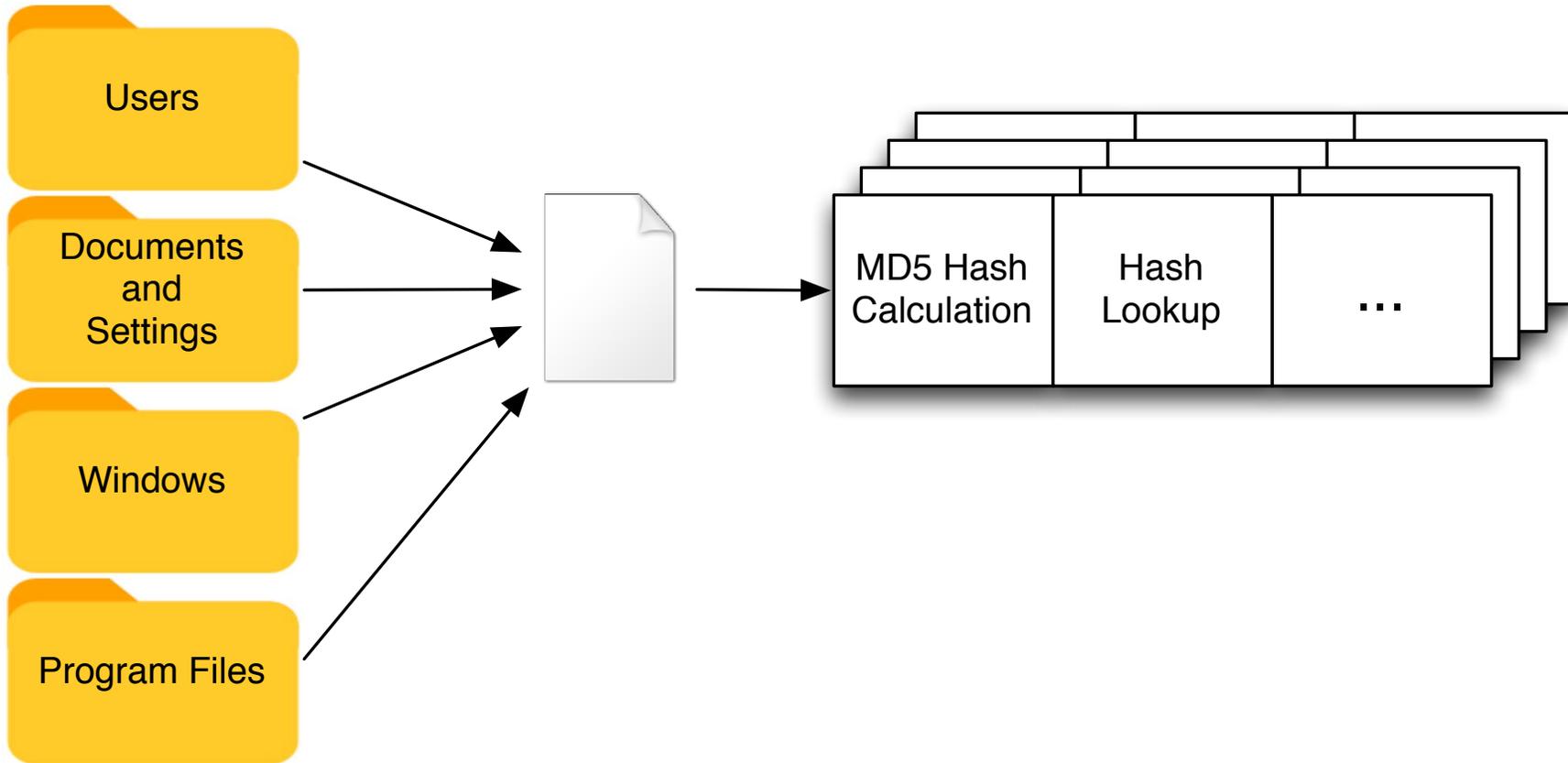
- We want to get the most relevant files down the pipelines first.



- Autopsy does this three ways:
 - User files are scheduled first
 - Filtering reduces files that are processed
 - Run predetermined modules with a single button click

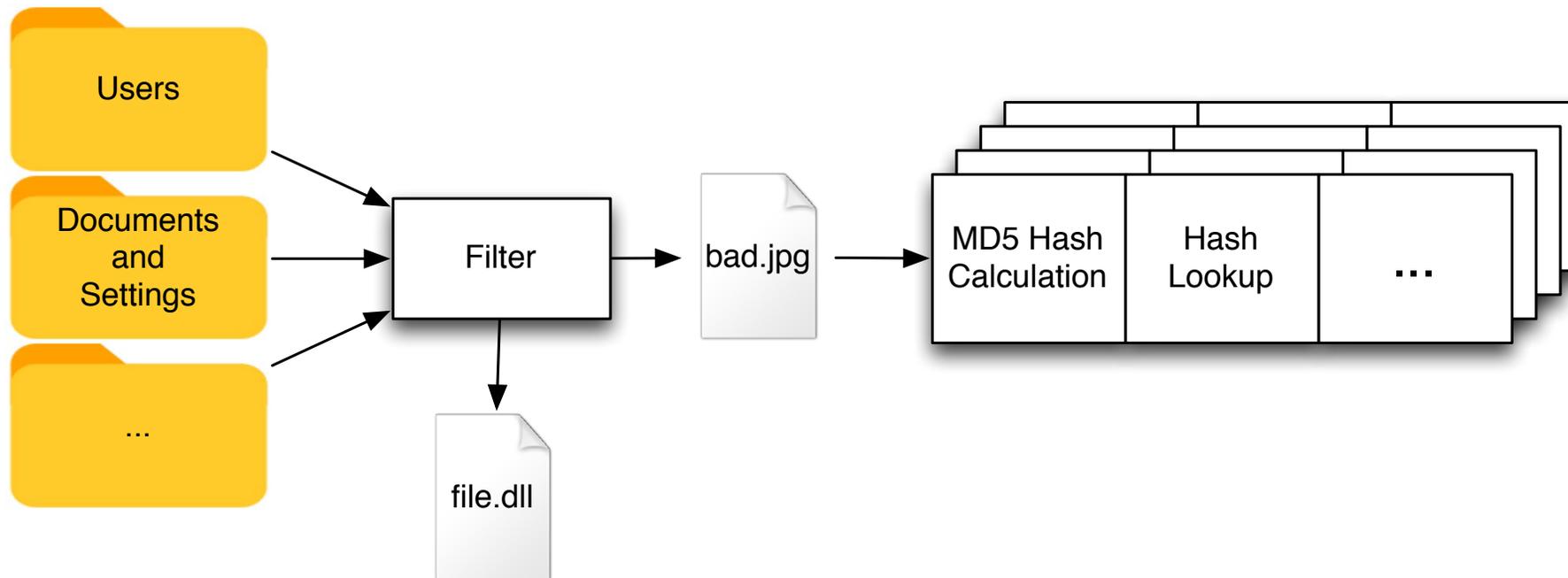
Schedule User Folders First

- Autopsy always runs user folders through the pipeline first.
- That's often where the good stuff is.



Subset of Files

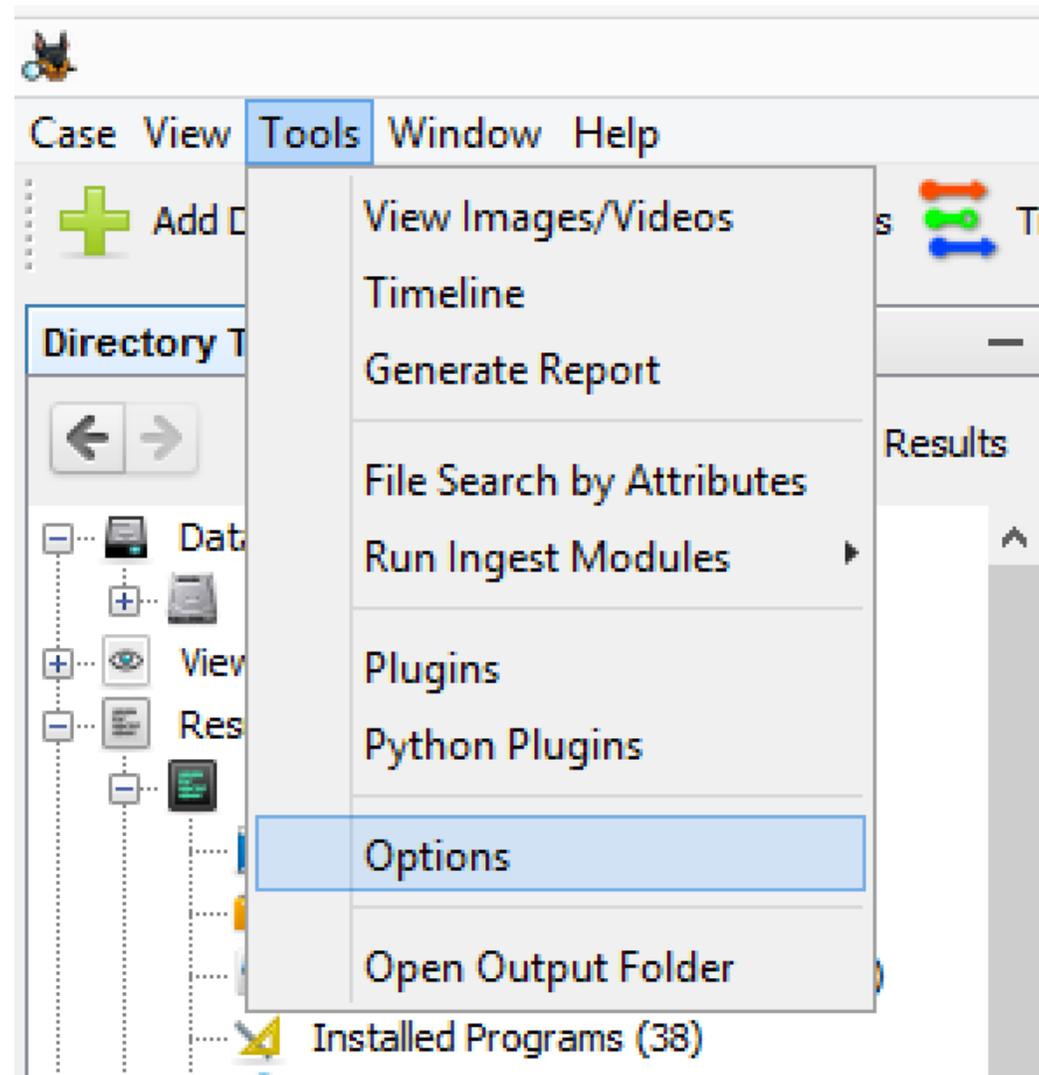
- Skip the files that are unlikely to be relevant.
- Filter based on: file name, parent folder.



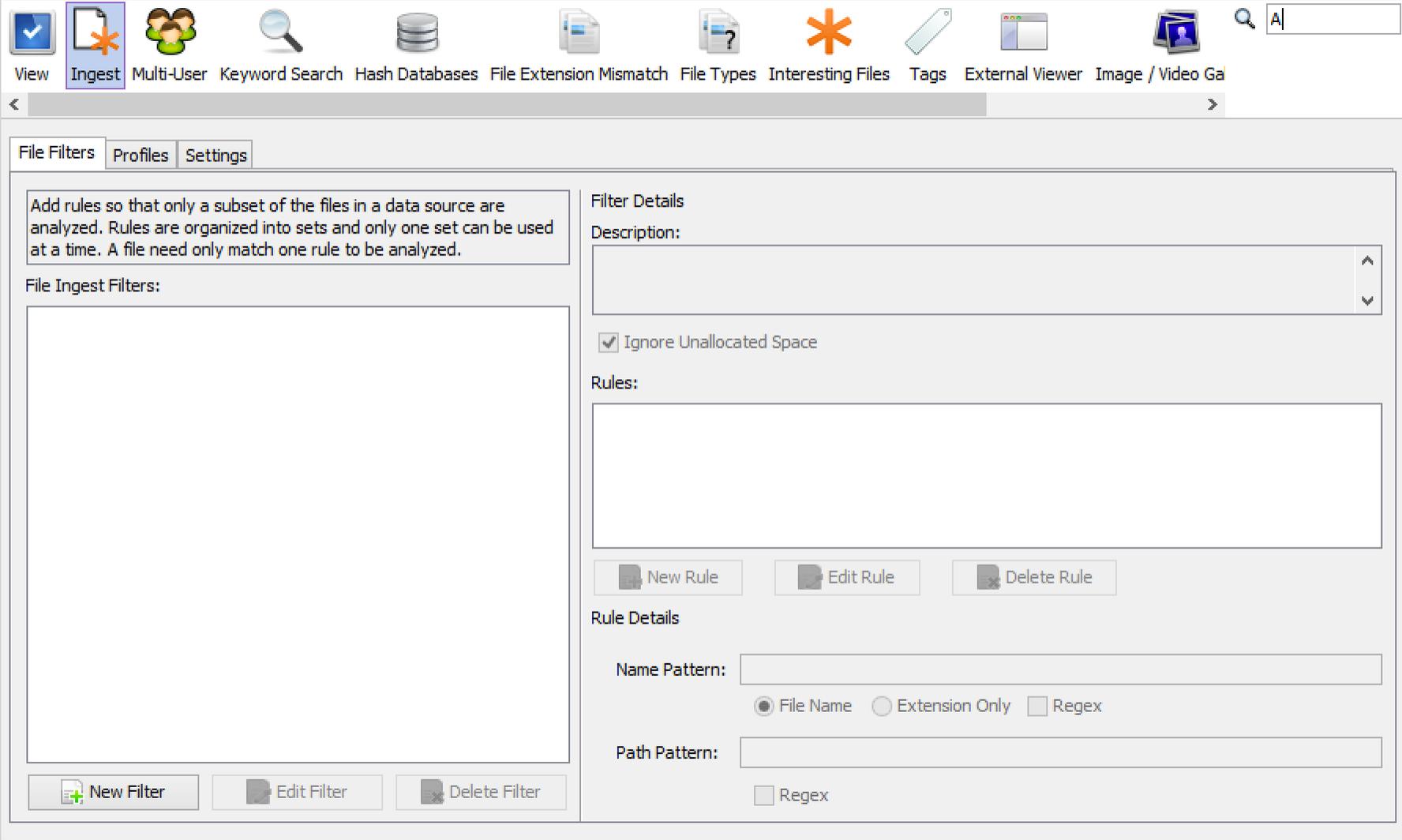
Subset of Files Examples

- Process all files with jpg, png, avi, mov, mp3, and mp4 extensions. Skip unallocated space.
- Process all files in the Desktop or My Documents Folder.
- Other ideas?

Making File Filters: Open Options Panel



Making File Filters: The Ingest Options Panel



The screenshot shows a software interface with a top navigation bar containing icons for View, Ingest, Multi-User, Keyword Search, Hash Databases, File Extension Mismatch, File Types, Interesting Files, Tags, External Viewer, and Image / Video Ga. Below the navigation bar is a breadcrumb trail: File Filters > Profiles > Settings.

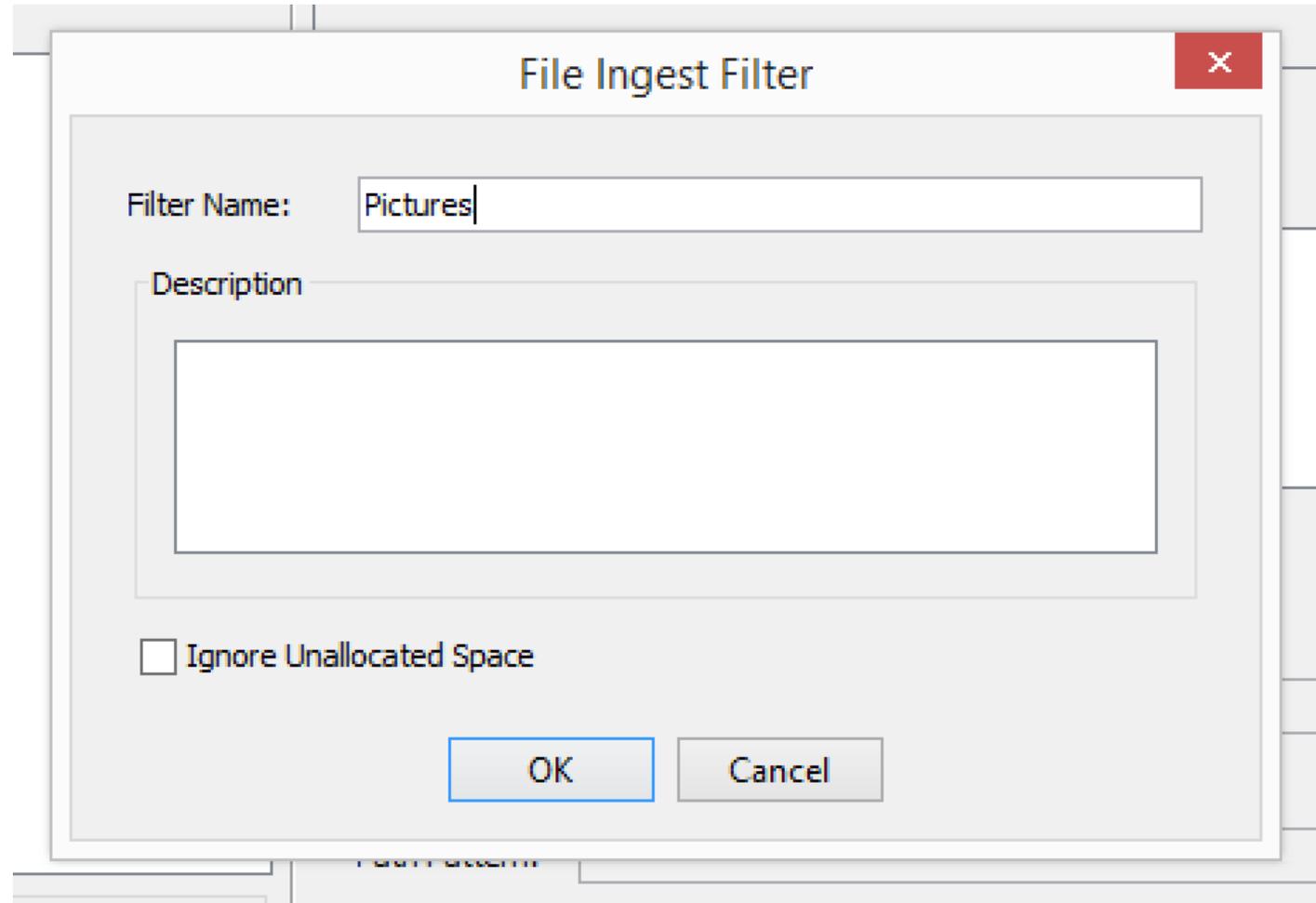
The main content area is divided into two columns. The left column contains a text box with the instruction: "Add rules so that only a subset of the files in a data source are analyzed. Rules are organized into sets and only one set can be used at a time. A file need only match one rule to be analyzed." Below this is a section titled "File Ingest Filters:" with a large empty rectangular area. At the bottom of this column are three buttons: "New Filter", "Edit Filter", and "Delete Filter".

The right column is titled "Filter Details" and contains a "Description:" text area with up and down arrow controls. Below the description is a checked checkbox labeled "Ignore Unallocated Space". Underneath is a "Rules:" section with a large empty rectangular area. Below the rules area are three buttons: "New Rule", "Edit Rule", and "Delete Rule".

At the bottom of the right column is a "Rule Details" section with two text input fields: "Name Pattern:" and "Path Pattern:". Below the "Name Pattern:" field are three radio buttons: "File Name" (selected), "Extension Only", and "Regex". Below the "Path Pattern:" field is a checkbox labeled "Regex".

Making a File Filter

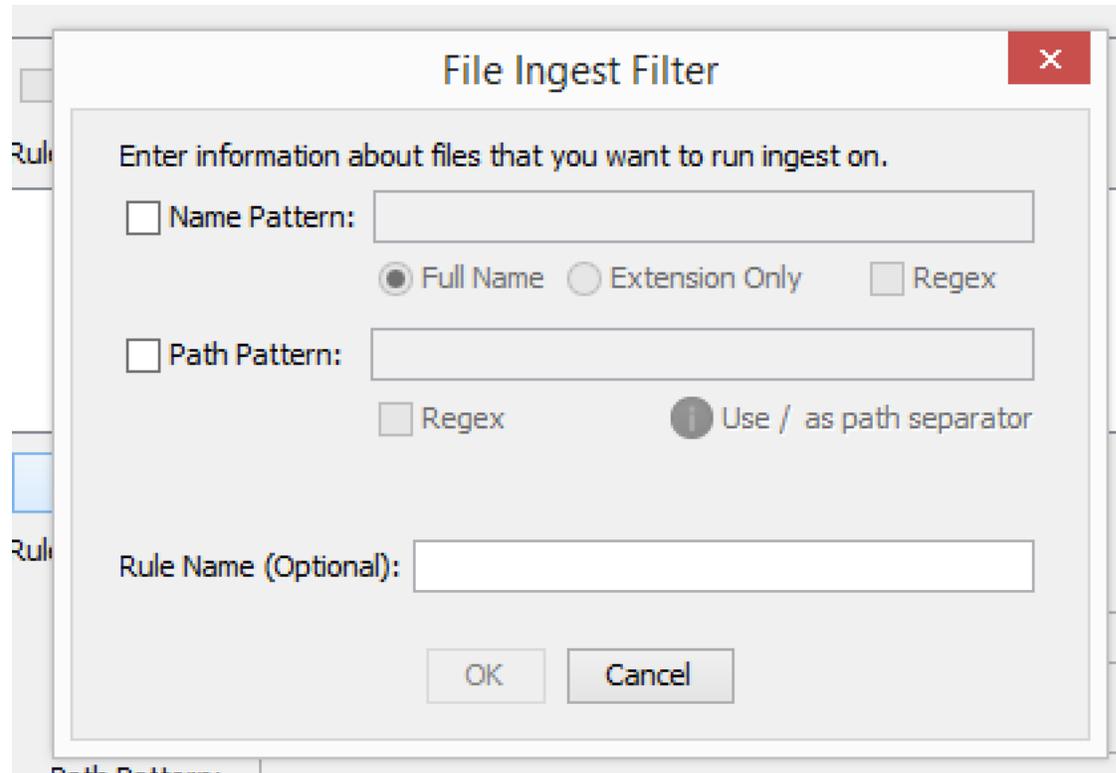
- Press “New Filter” button
- File Filter:
 - Set of rules that defines what passes.
 - Has a name and optional description.
 - Can ignore unallocated space.
 - Only one filter can be used a time.



The screenshot shows a dialog box titled "File Ingest Filter". It has a close button (X) in the top right corner. The "Filter Name:" label is followed by a text input field containing the word "Pictures". Below this is a "Description" label followed by a large, empty text area. At the bottom left, there is a checkbox labeled "Ignore Unallocated Space" which is currently unchecked. At the bottom right, there are two buttons: "OK" and "Cancel".

- Filters have a set of rules that are ORed together
- Rules can specify:
 - File name
 - Full name
 - Extension only
 - File path
 - The value must be a substring in the full path for the file to be analyzed.

- Press “New Rule” button



File Ingest Filter

Enter information about files that you want to run ingest on.

Name Pattern:

Full Name Extension Only Regex

Path Pattern:

Regex Use / as path separator

Rule Name (Optional):

Example Rule: .jpg

File Ingest Filter [X]

Enter information about files that you want to run ingest on.

Name Pattern:

Full Name Extension Only Regex

Path Pattern:

Regex Use / as path separator

Rule Name (Optional):

Path Pattern:

Example Rule: Desktop folder

File Ingest Filter

Enter information about files that you want to run ingest on.

Name Pattern:

Full Name Extension Only Regex

Path Pattern:

Regex Use / as path separator

Rule Name (Optional):

Example Rule: jpgs in Downloads

File Ingest Filter ✕

Enter information about files that you want to run ingest on.

Name Pattern:

Full Name Extension Only Regex

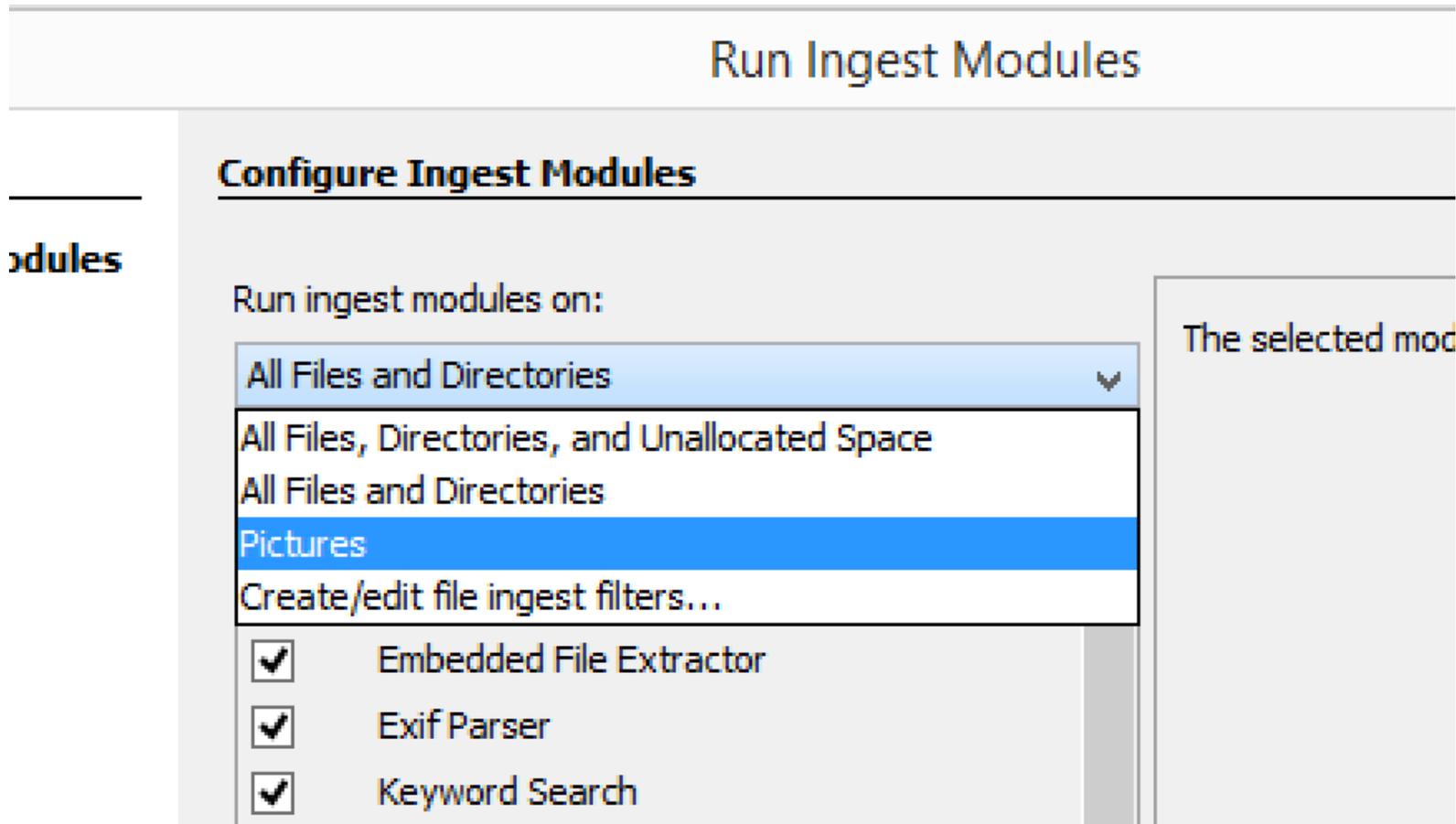
Path Pattern:

Regex  Use / as path separator

Rule Name (Optional):

Choosing a File Filter

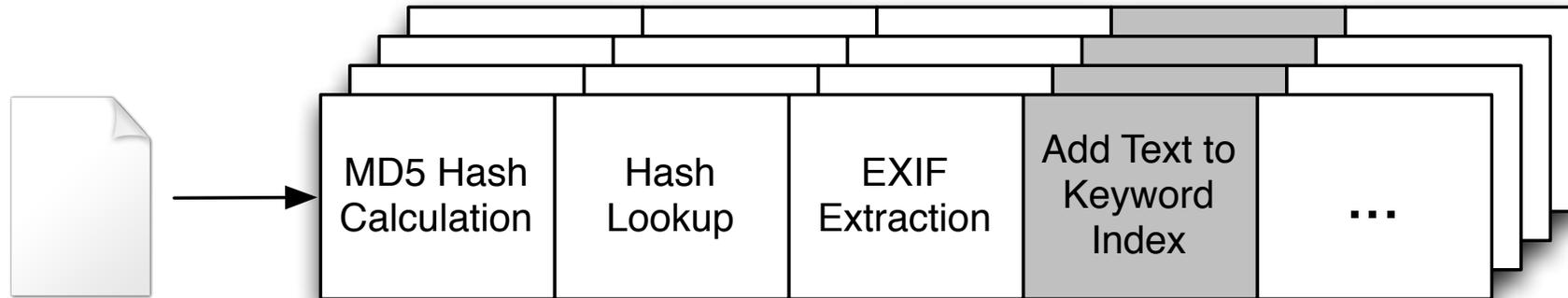
- When you pick the ingest modules to run, you can pick the filter.



Triaging Feature: Run Predetermined, Preconfigured Ingest Modules

Reduce the Modules You Run

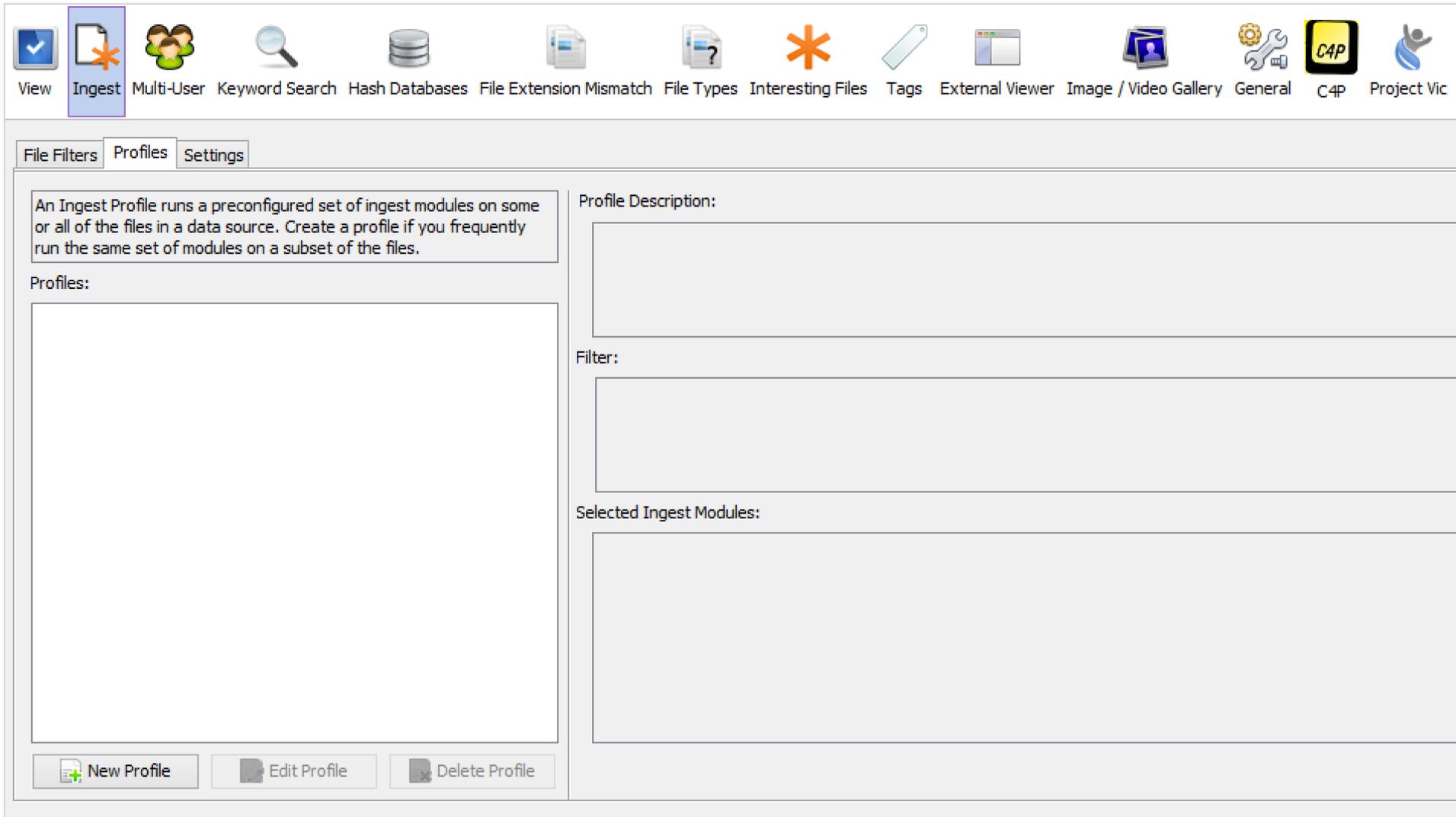
- Process more files by spending less time on each.
- Don't run the modules you don't need the results for.



- You can manually do this. Or....

- Many triage sessions are similar and use the same settings.
- Save time by configuring a profile that specifies:
 - File filter to use (what files to process)
 - Ingest modules to use and their settings
- Example:
 - File filter that passes only .jpg, .png, .avi, .mov, etc. and all Downloads
 - Ingest modules for hash lookups, EXIF, open zip files

Making a Profile: Ingest Options Panel



View Ingest Multi-User Keyword Search Hash Databases File Extension Mismatch File Types Interesting Files Tags External Viewer Image / Video Gallery General C4P Project Vic

File Filters Profiles Settings

An Ingest Profile runs a preconfigured set of ingest modules on some or all of the files in a data source. Create a profile if you frequently run the same set of modules on a subset of the files.

Profiles:

Profile Description:

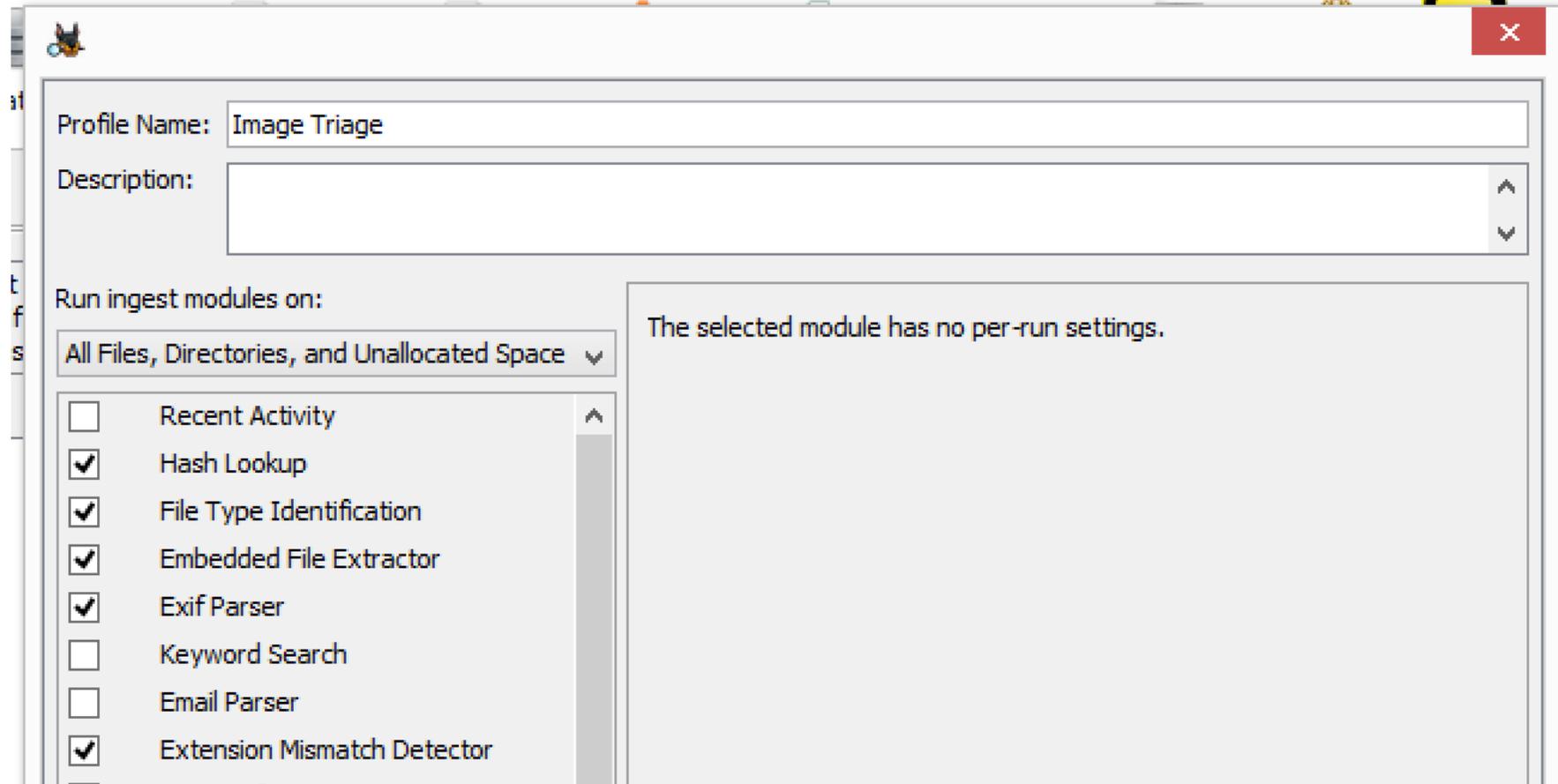
Filter:

Selected Ingest Modules:

New Profile Edit Profile Delete Profile

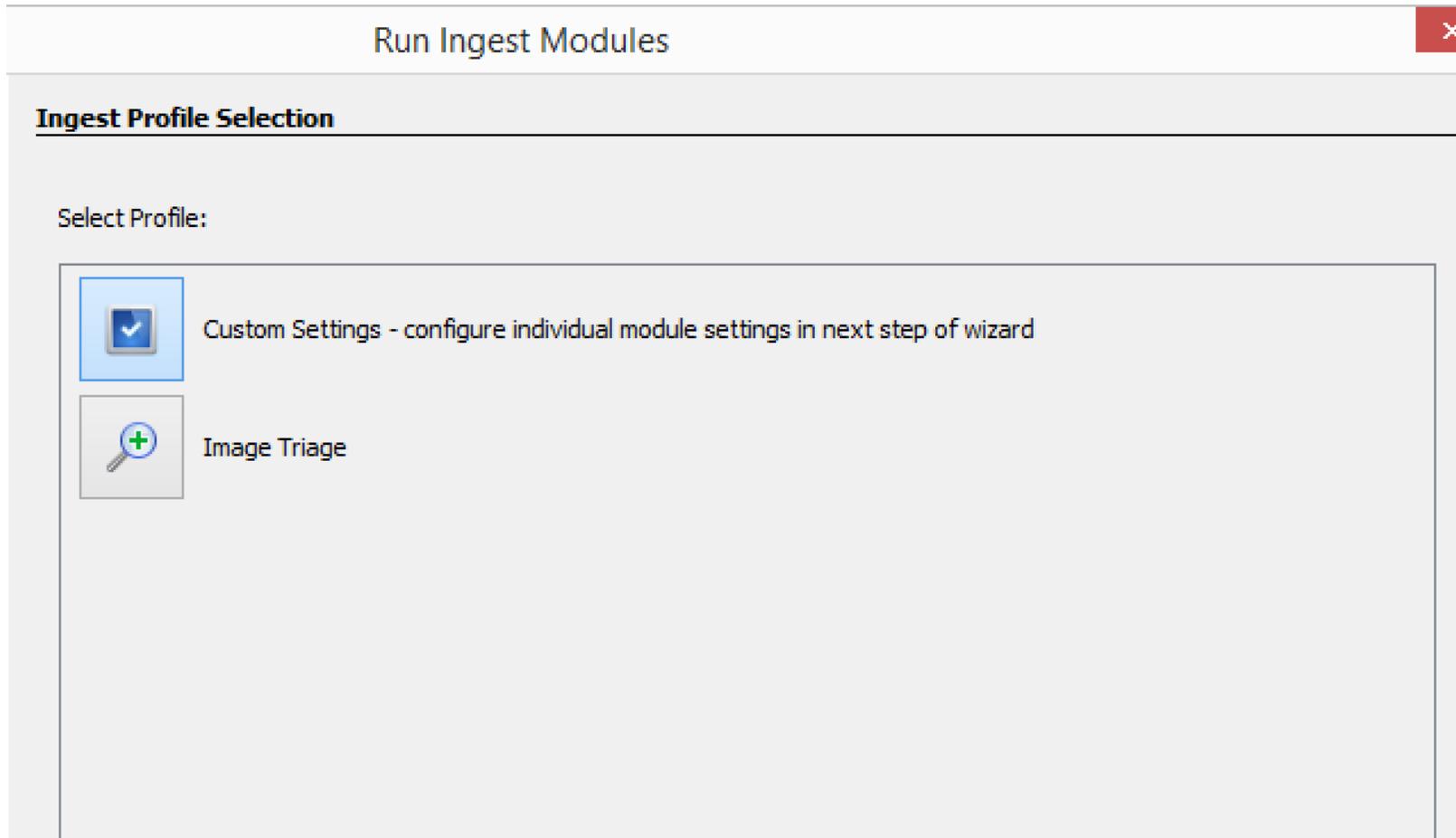
Making a Profile

- Specify:
 - Name
 - Optional description
 - Set of modules and their configuration.



Picking the Profile

- You will see the profiles before you run the ingest modules.



Triaging Features:

Keep a Copy of Any Data You Read

Making An Image Is Expensive

- Problem:
 - You want some record of what data was on the image.
 - Don't have time to make a full image.
 - Ideally you want more than just the notable files.
- Solution:
 - Make an image as your analysis happens
- Basic Idea:
 - Use the previously described triage techniques.
 - When a sector is read for the first time, a copy is made.
 - Save the sectors to a “sparse” VHD file.

What's a Sparse VHD?

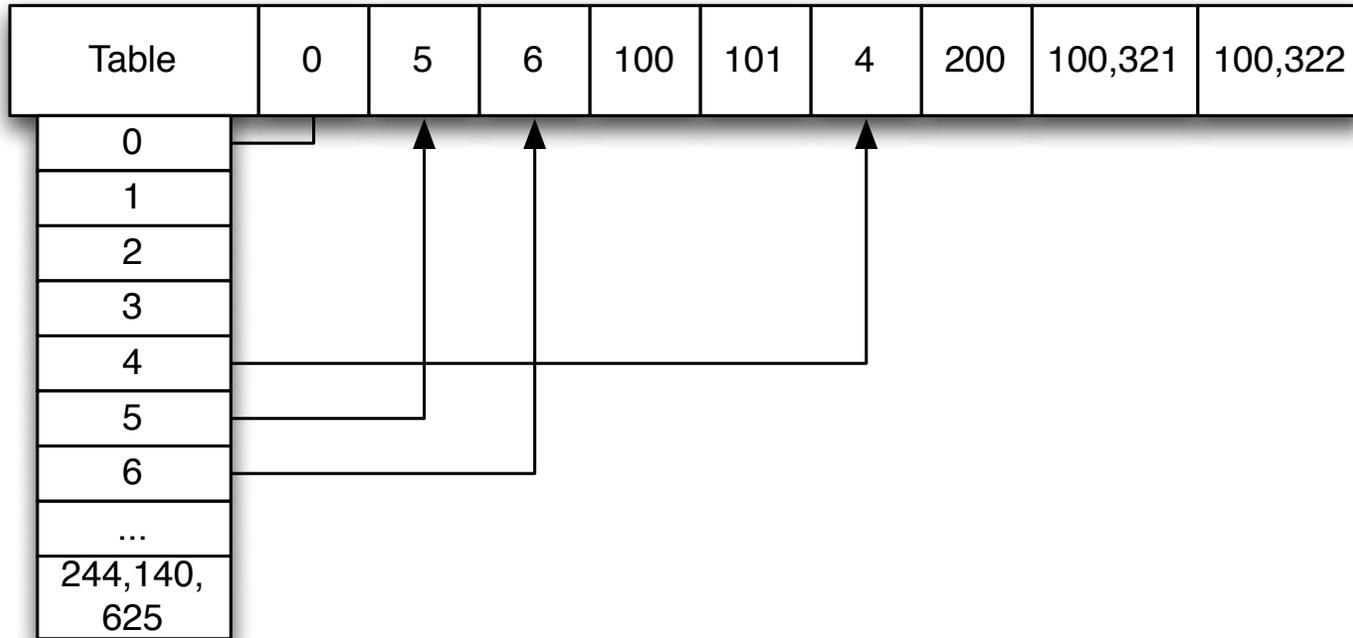
- File format used by Microsoft Virtual Machines.
- “Sparse” because the file size is based on how much data has been written to it.
- Efficient to write random sectors to (versus traditional formats)
- Readable by Windows (double click it) and other forensics tools.
- A VHD file from Autopsy will contain file system data (master boot record, master file table, etc.)

Normal Raw vs. VHD Images

Normal Raw

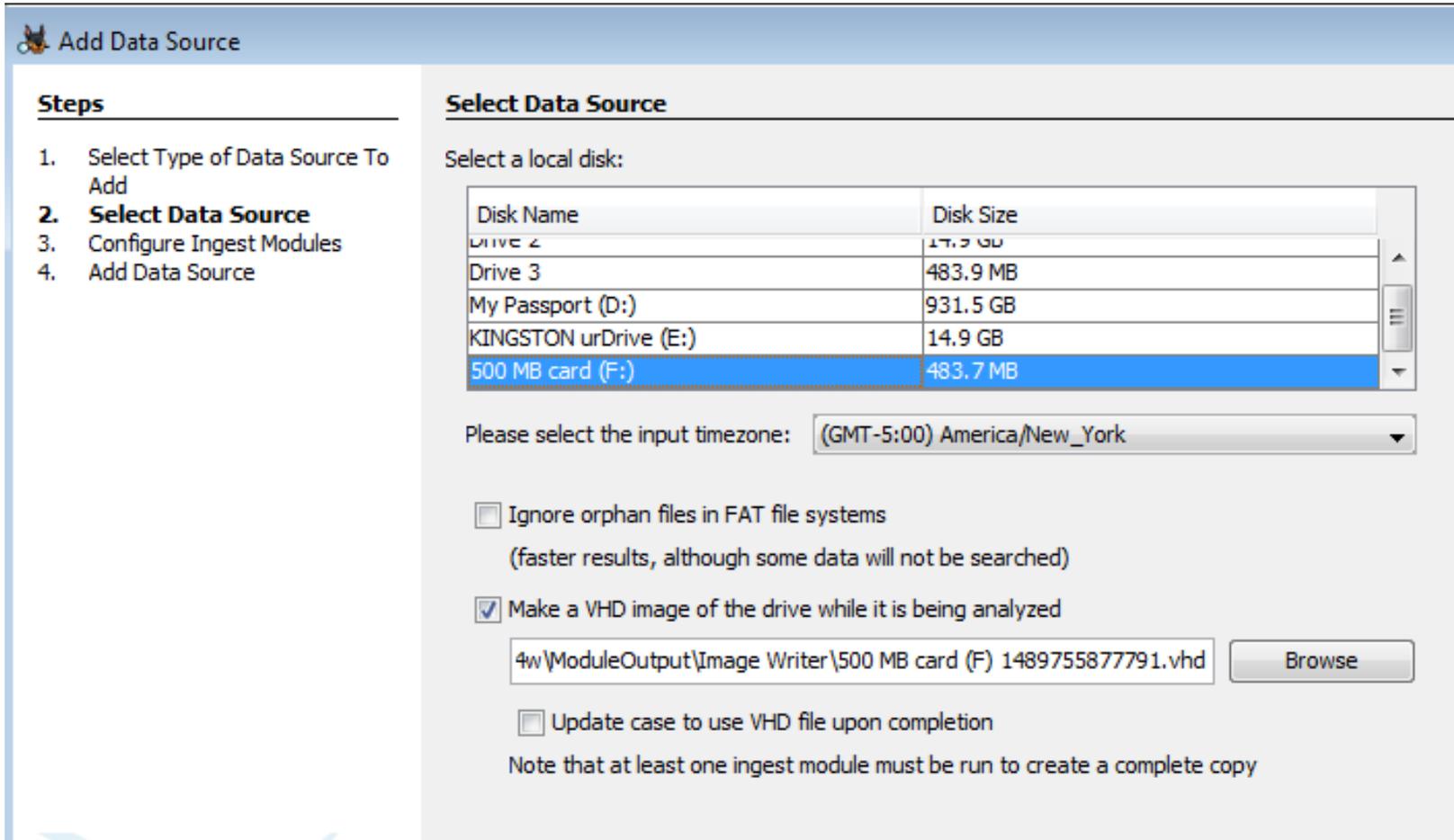


Sparse VHD



Making a VHD with Autopsy

- Only possible when analyzing a local drive.



Add Data Source

Steps

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

Select Data Source

Select a local disk:

Disk Name	Disk Size
DRIVE 2	17.2 GB
Drive 3	483.9 MB
My Passport (D:)	931.5 GB
KINGSTON urDrive (E:)	14.9 GB
500 MB card (F:)	483.7 MB

Please select the input timezone: (GMT-5:00) America/New_York

Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

Make a VHD image of the drive while it is being analyzed

4w\ModuleOutput\Image Writer\500 MB card (F) 1489755877791.vhd

Update case to use VHD file upon completion

Note that at least one ingest module must be run to create a complete copy

- Choose “Make a VHD...” option
- By default it will pick a file name in the case folder
- Choose the “Update Database...” option if you want Autopsy to update the case database to refer to the VHD file after it is complete.
 - Otherwise, it will have a reference to [\\.\E:](#) (or something)
- The remaining analysis is the same. Pick your profiles, modules, etc.

Sample VHD Layout

- Data will be saved in the order that it was read:
 - Partition table to determine disk layout
 - File system data to determine FS layout
 - Root and user directories to focus on user files
 - Files that were processed first and passed filters

VHD Header	Partition Table	Boot Sector	MFT	\	\Users	\Users\Jdoe	file1.jpg	file2.jpg	Desktop	file1.docx
------------	-----------------	-------------	-----	---	--------	-------------	-----------	-----------	---------	------------

- It is not compressed.
 - VHD supports compression, but The Sleuth Kit / Autopsy do not yet.
- There are no cryptographic checksums.

Triaging Features: Putting It All Together

- Knock and talk or probation situation.
- Goal is to answer question about if child exploitation images exist.
- Subject has a desktop computer.
- You plug in a USB write blocker to subject's drive and connect it to your laptop.
- You turn on Autopsy.

- Make a case
- Add a local drive data source:
 - “E:”
 - Choose to make VHD and keep default location
- Choose an ingest profile that:
 - Runs on image and ZIP extensions
 - Runs hash lookup, EXIF, file type, and embedded file extraction modules
 - Hash lookup configured to use known child exploitation hash sets

- As the analysis continues:
 - Choose View -> File Types -> Images and review the thumbnails
 - Wait for hash set hits
 - Review EXIF files
- Tag the notable files (if any).
- Stop the analysis at any time.
 - You'll have the data read so far in the VHD file.

- There are times when you want quick answers and can't focus on everything.
- Autopsy allows you to:
 - Focus on the relevant files first.
 - Make an image copy of the data you analyzed