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).

How We Solve It

- 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.

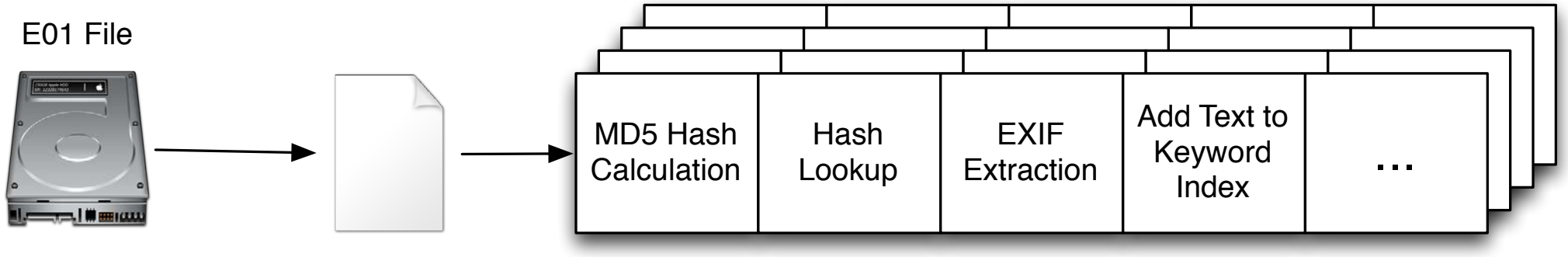
Basic Scenario

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

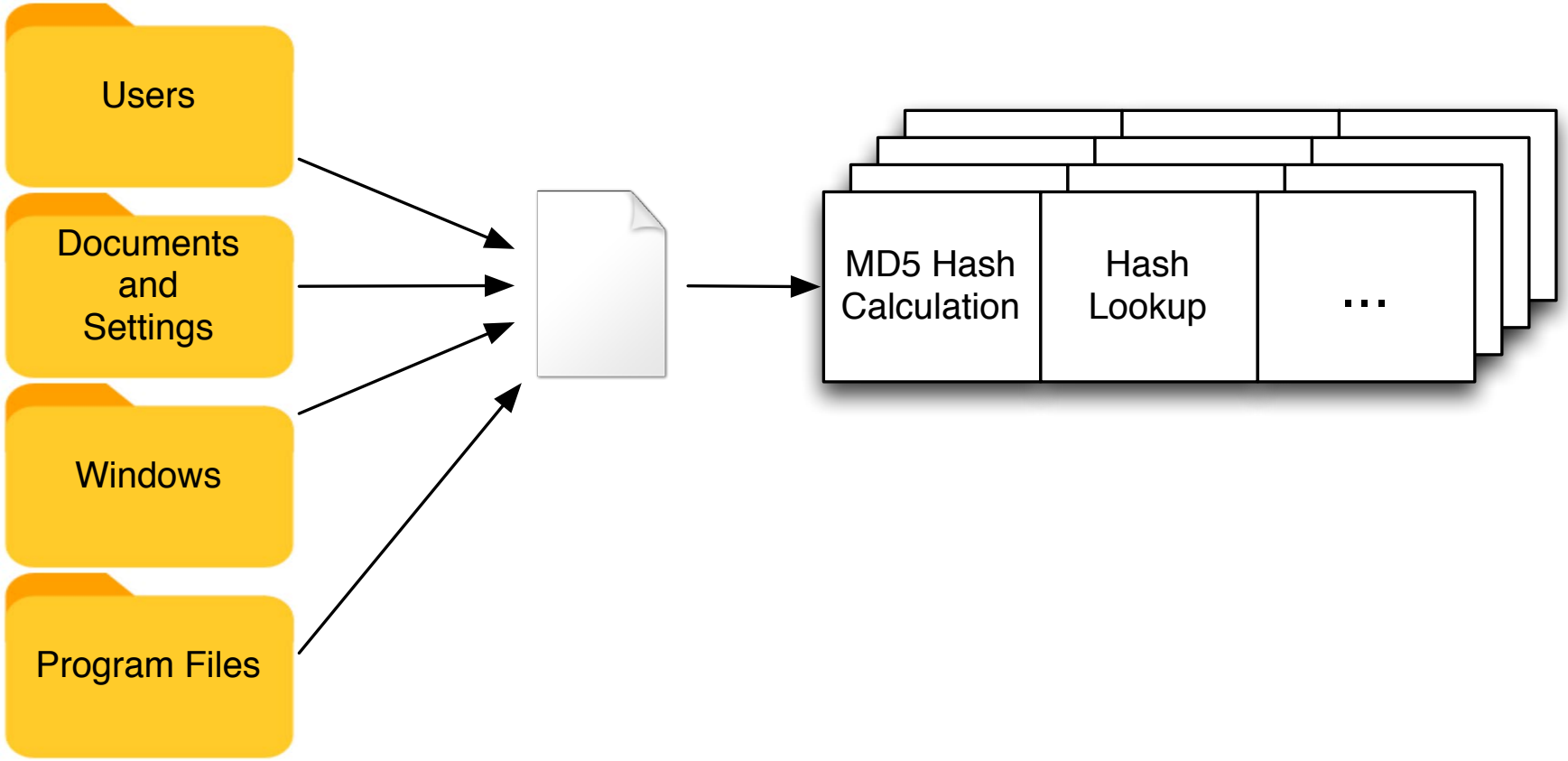
- We want to get the most relevant files down the pipelines first.



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

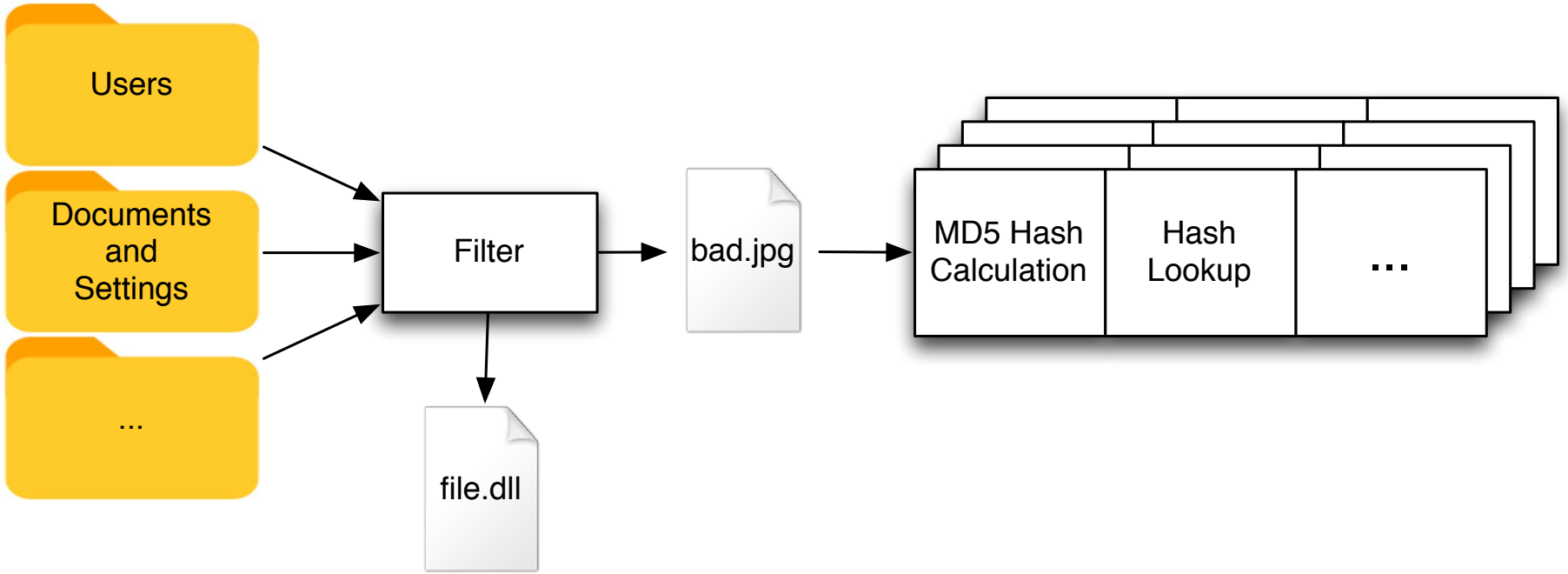
Schedule User Folders First

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



Subset of Files

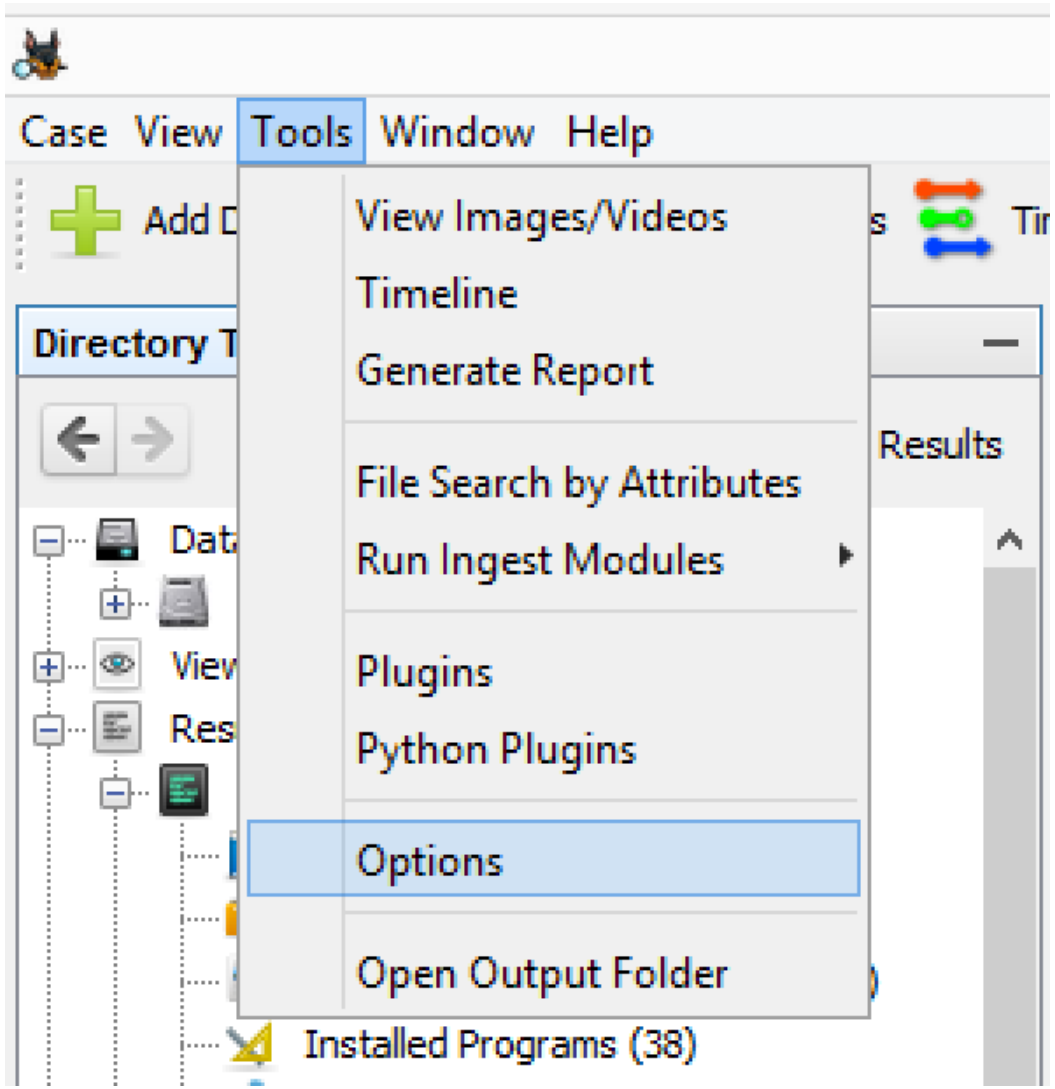
- Skip the files that are unlikely to be relevant.
- Filter based on: file name, parent folder.



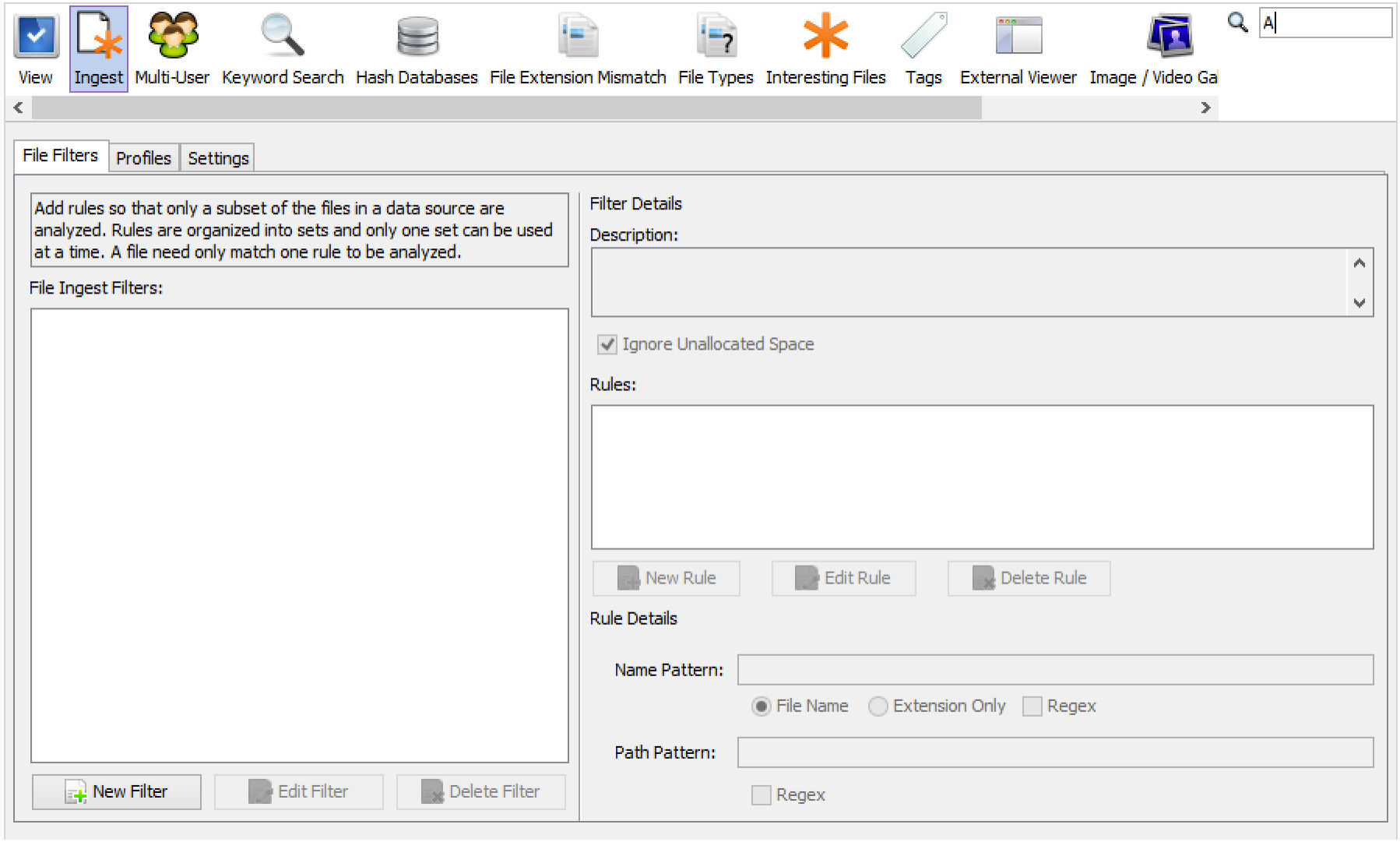
Subset of Files Examples

- 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

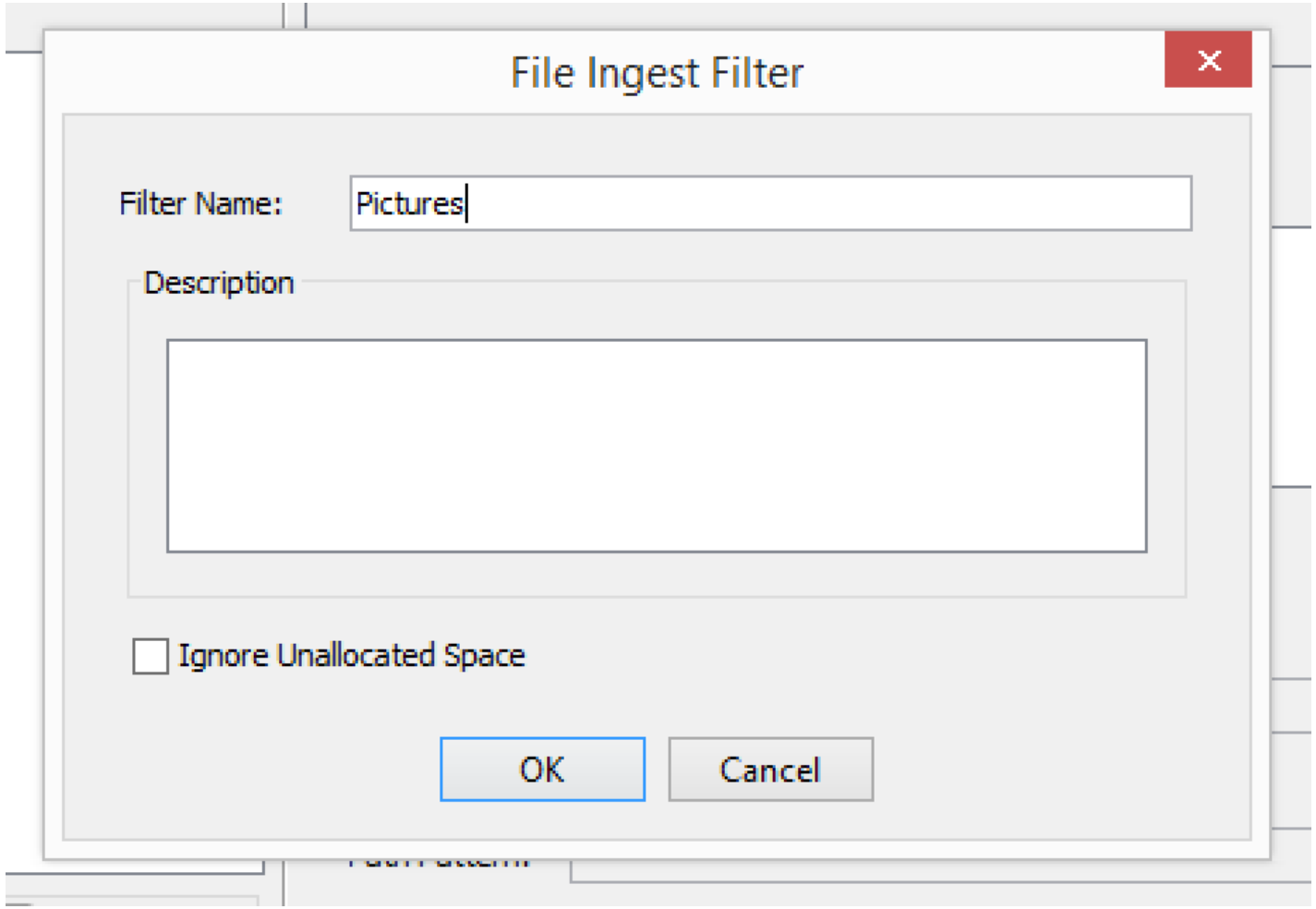


Making File Filters: The Ingest Options Panel



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.

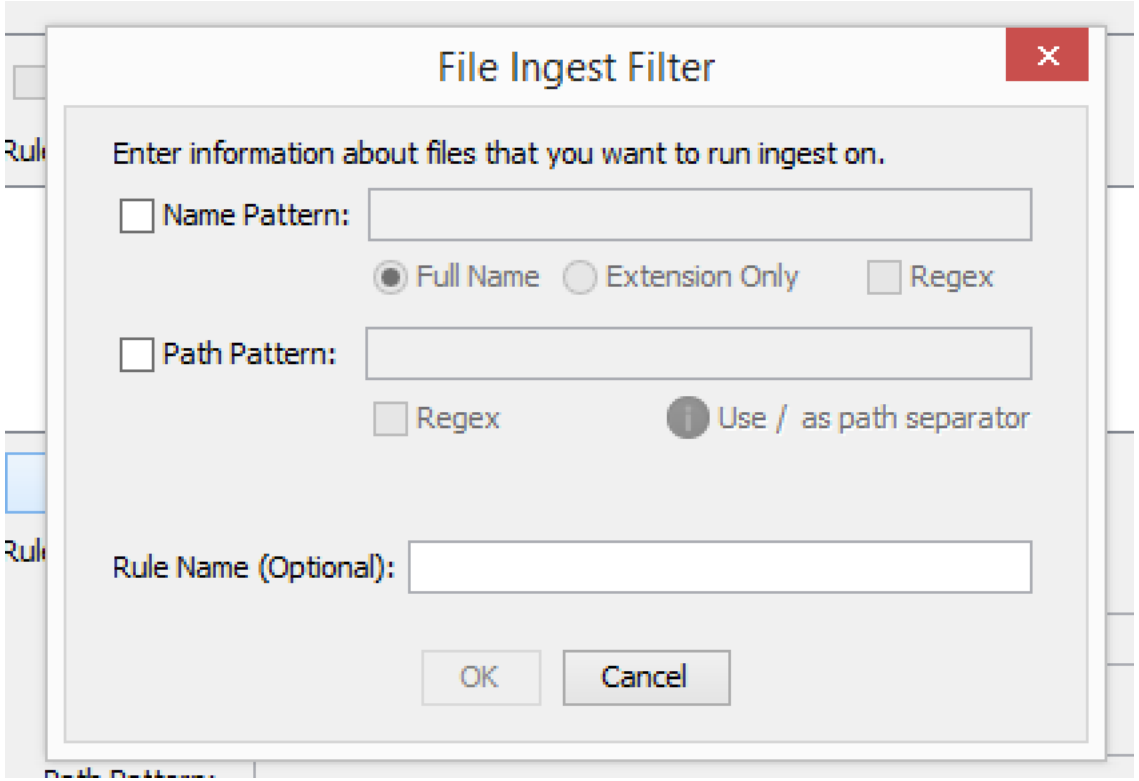


Add Rules

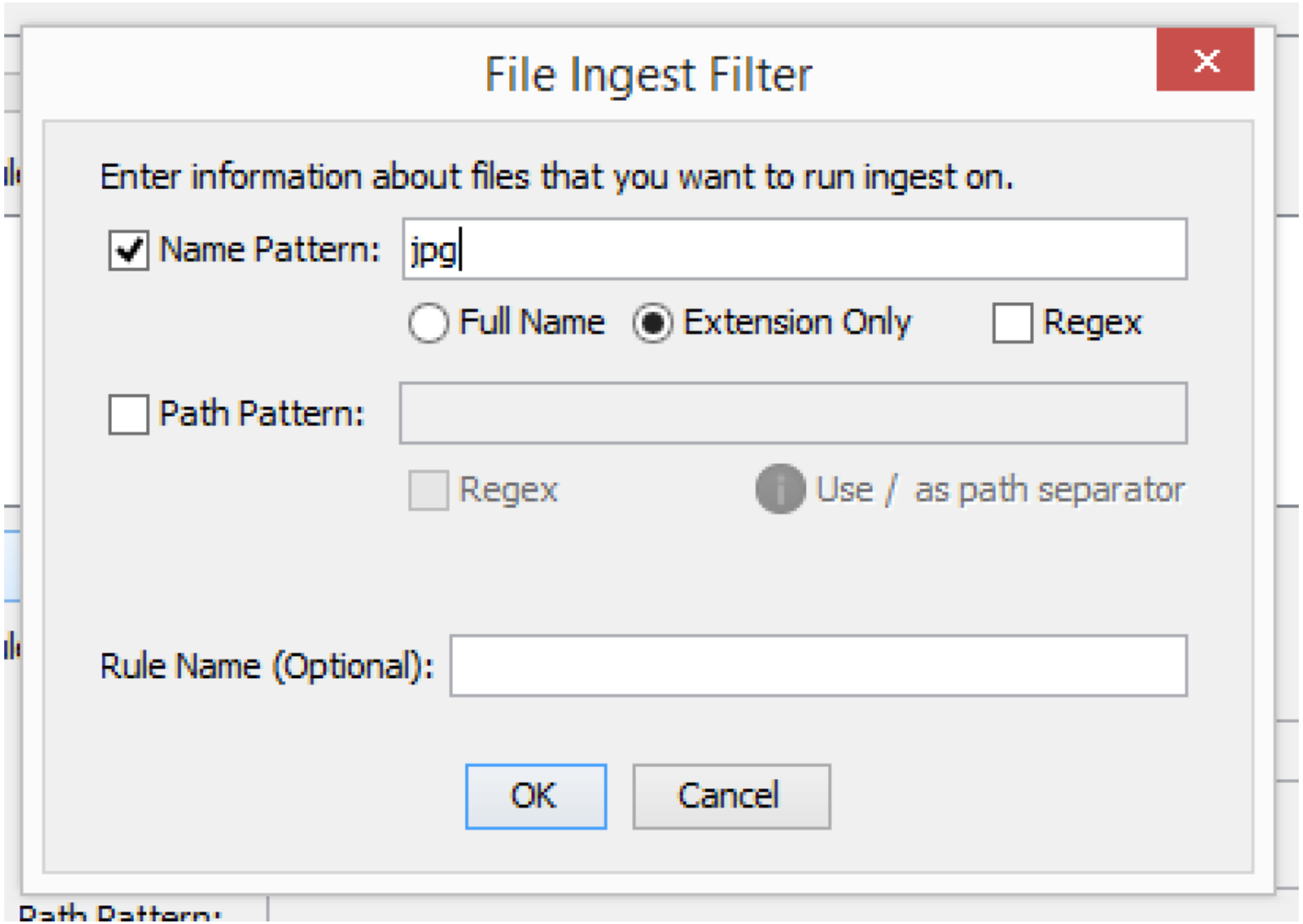
- Filters have a set of rules that are ORed together
- Rules can specify:
  - File name
    - Full name
    - Extension only
  - File path
    - The value must be a substring in the full path for the file to be analyzed.

Add Rules

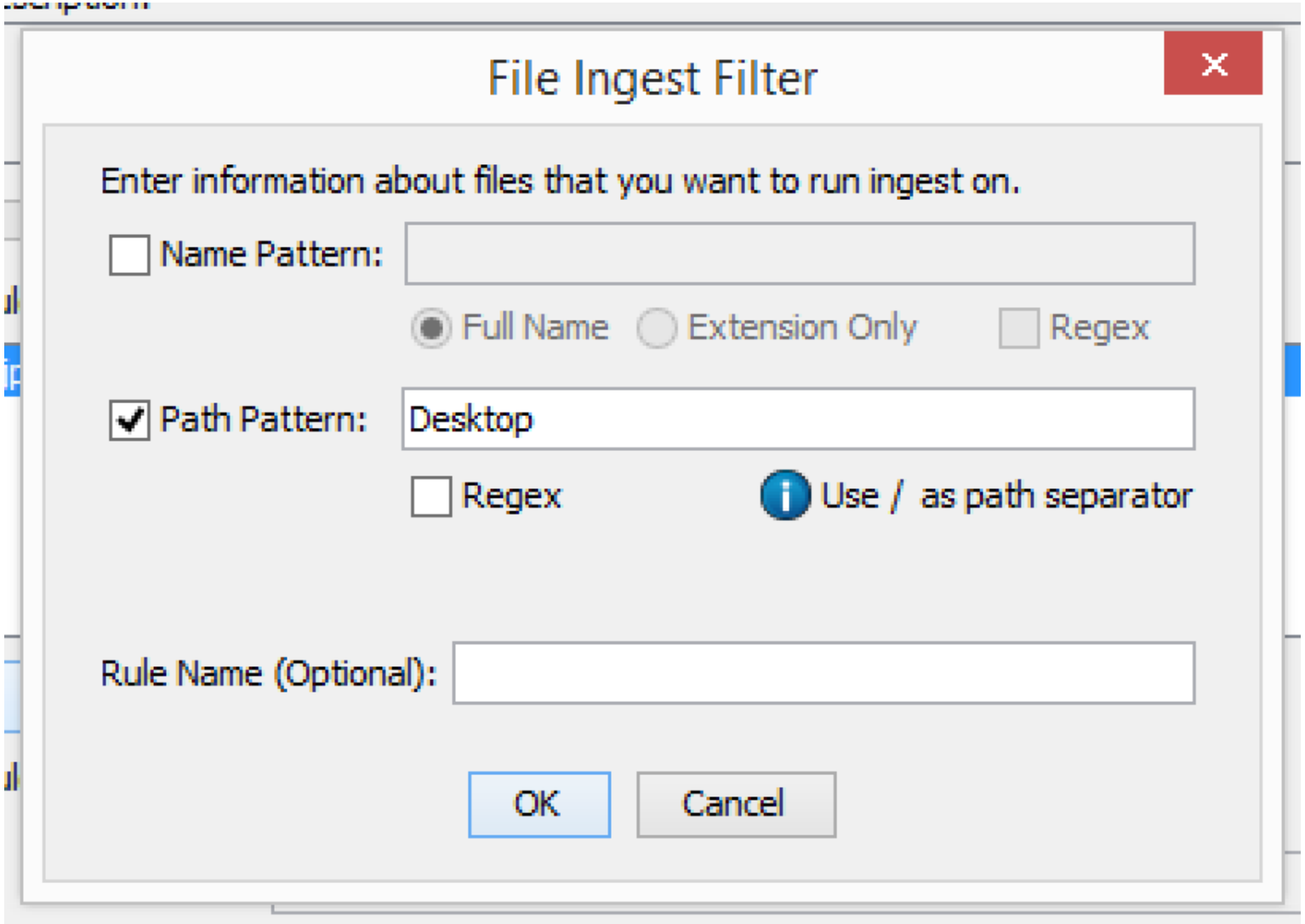
- Press “New Rule” button



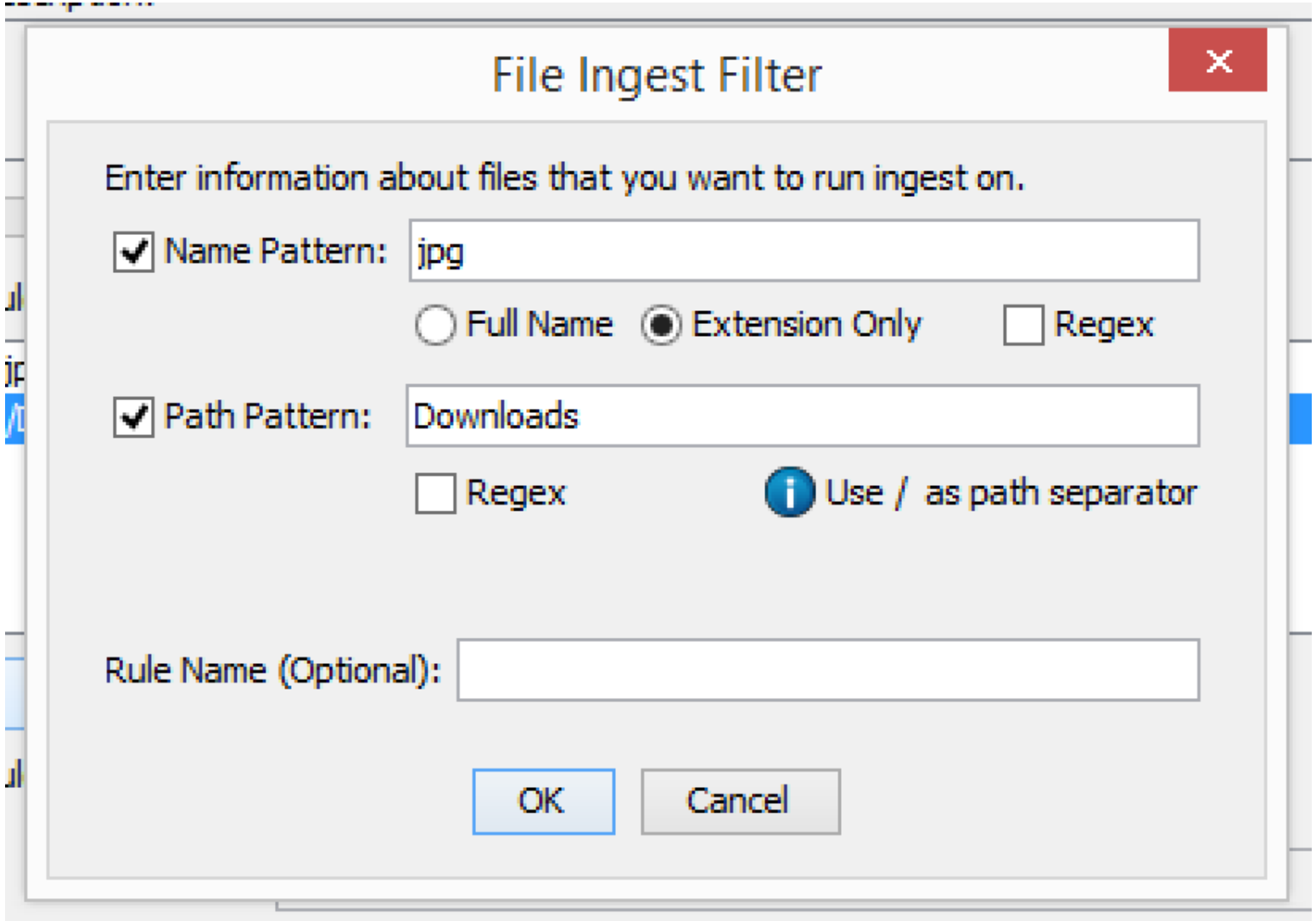
Example Rule: .jpg



Example Rule: Desktop folder

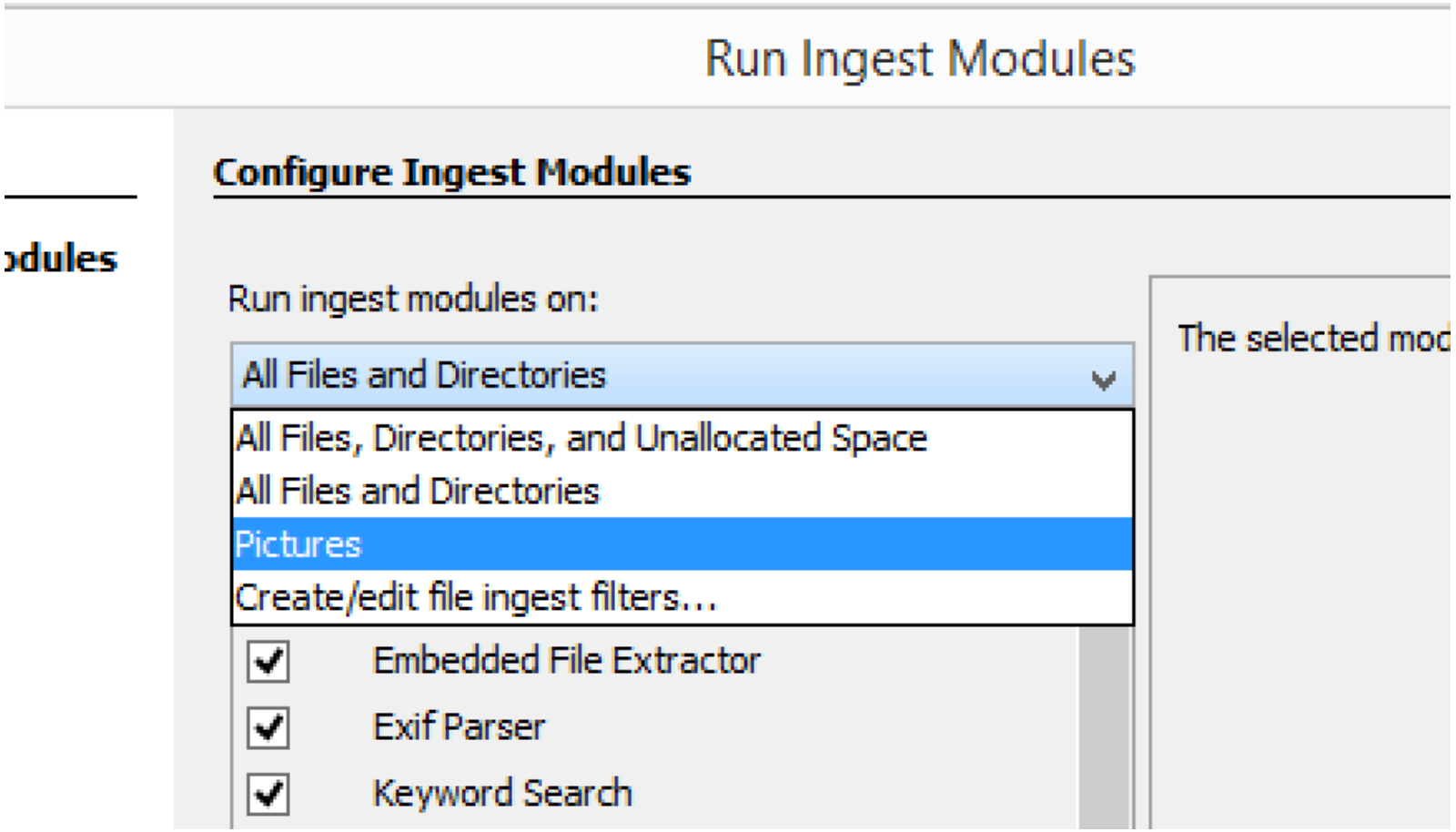


Example Rule: jpgs in Downloads



Choosing a File Filter

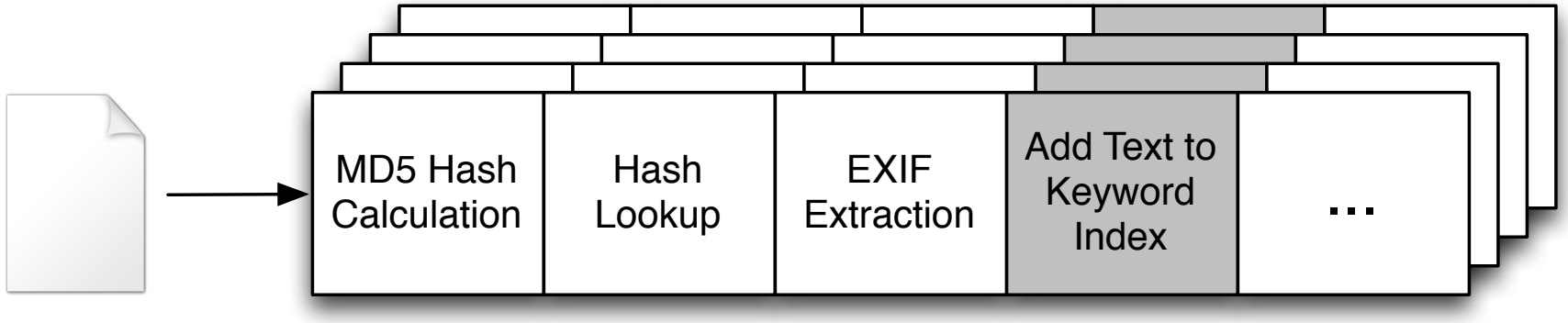
- When you pick the ingest modules to run, you can pick the filter.



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.

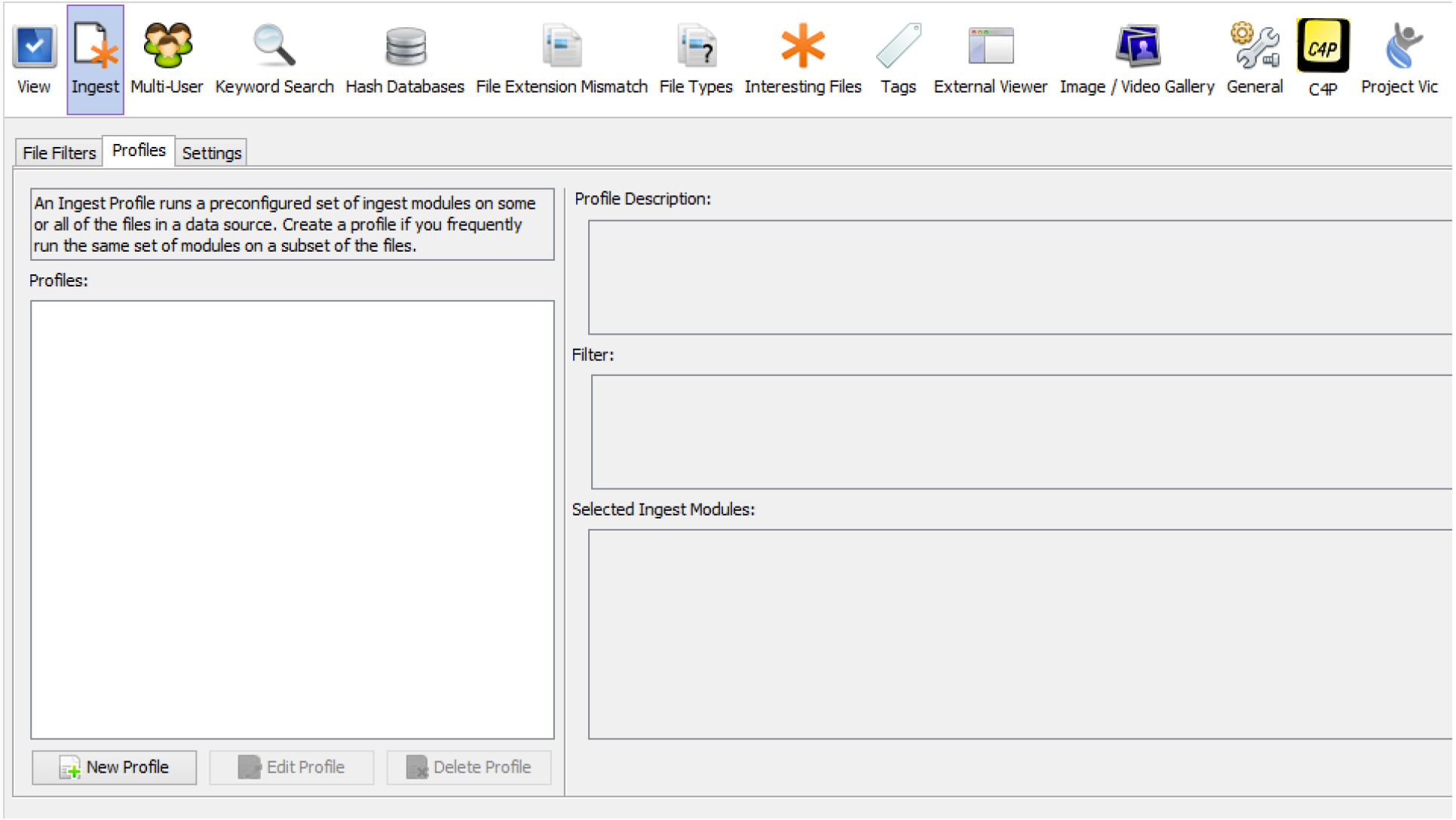


- You can manually do this. Or….

Ingest Profiles

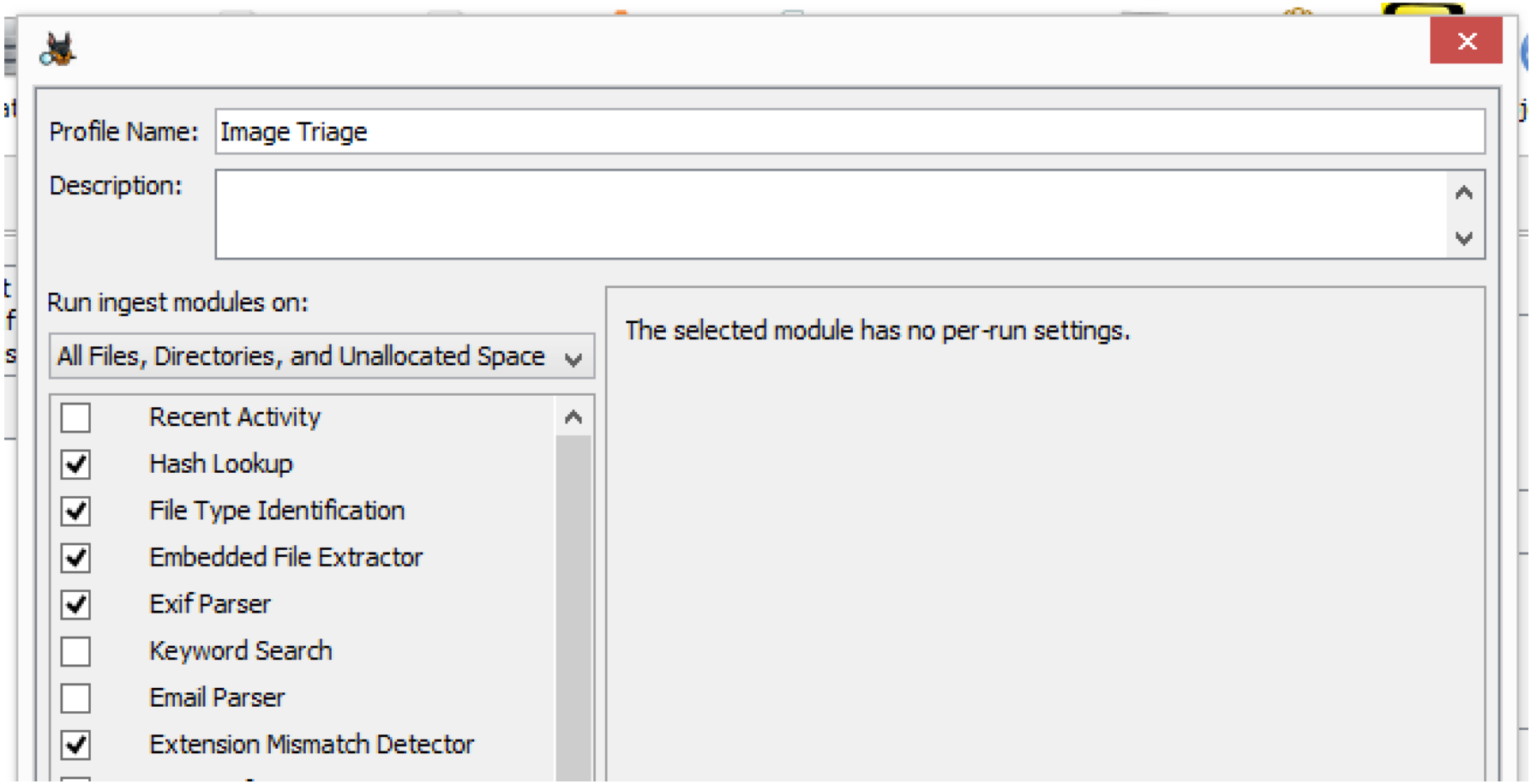
- Many triage sessions are similar and use the same settings.
- Save time by configuring a profile that specifies:
  - File filter to use (what files to process)
  - Ingest modules to use and their settings
- Example:
  - File filter that passes only .jpg, .png, .avi, .mov, etc. and all Downloads
  -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

Making a Profile: Ingest Options Panel



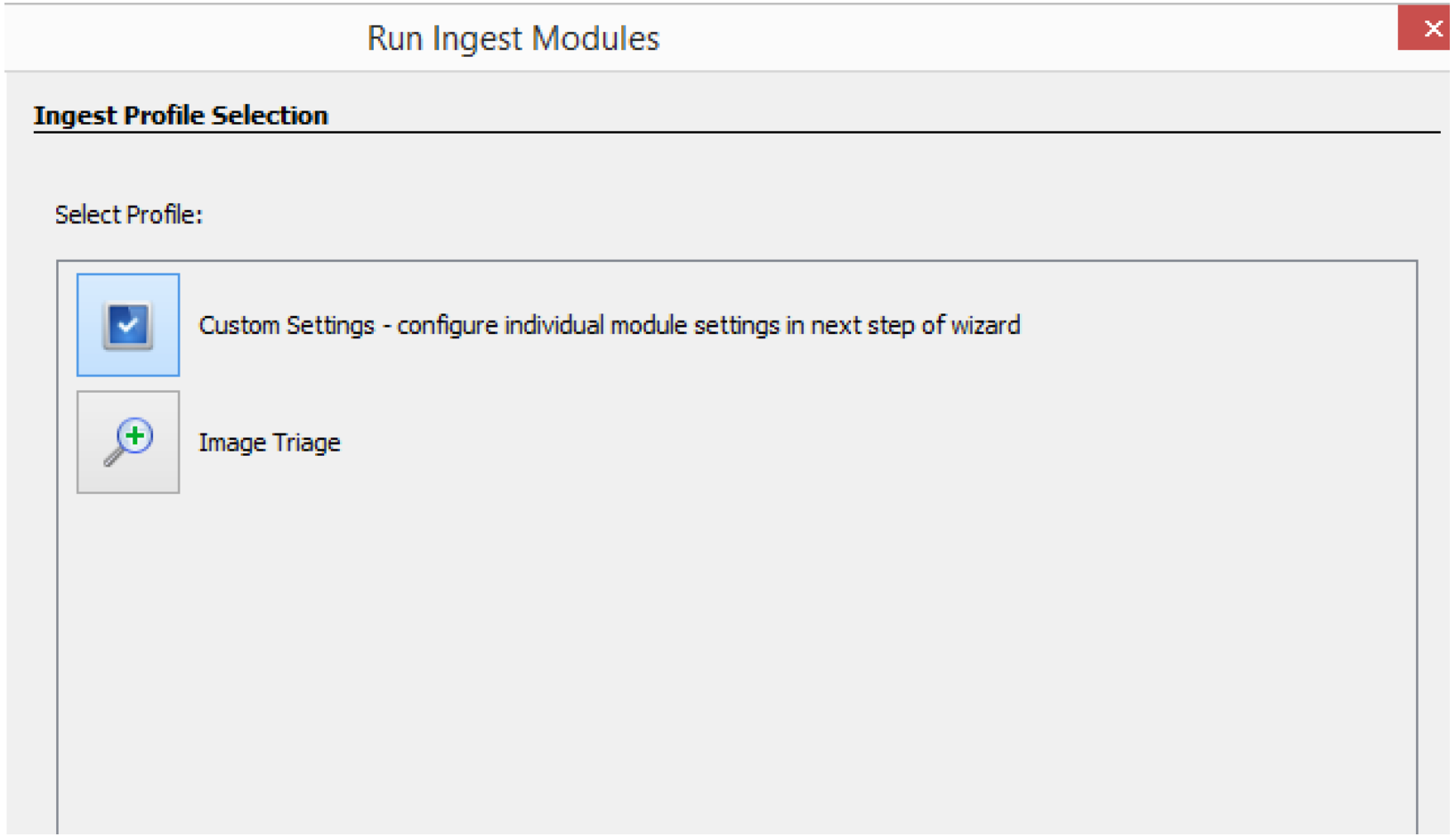
Making a Profile

- 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

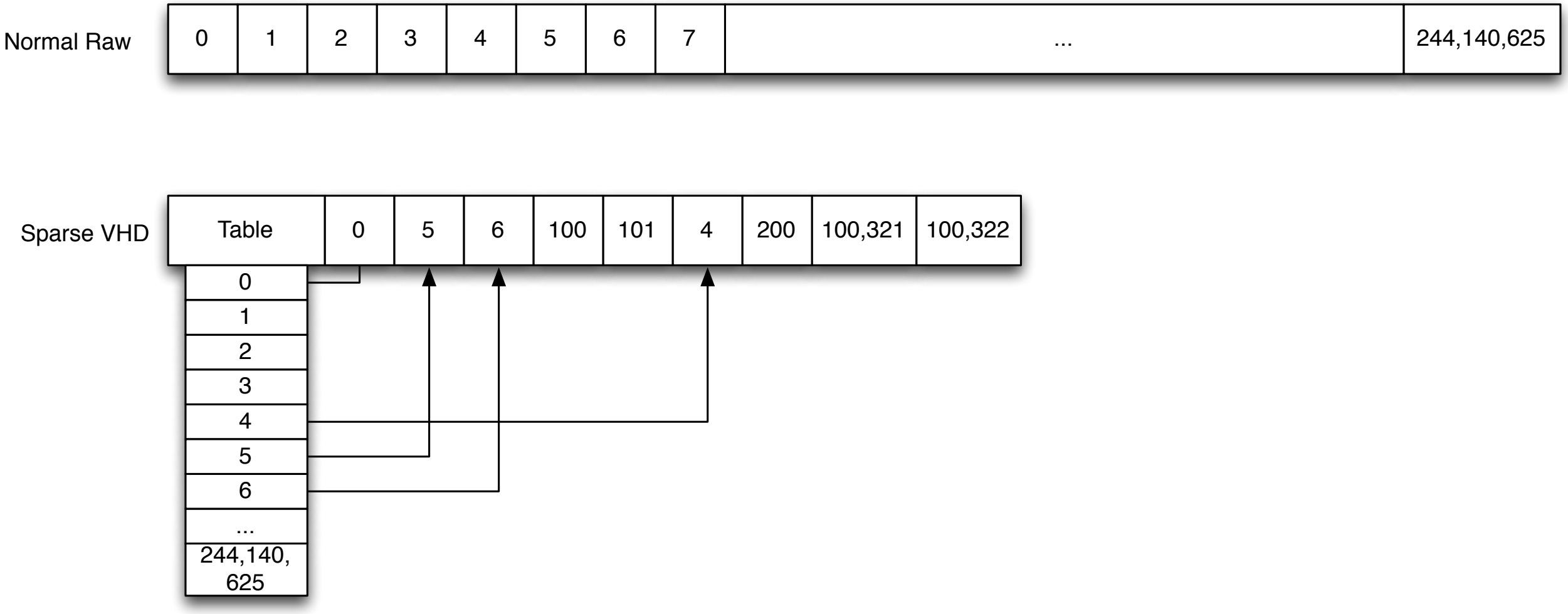
Making An Image Is Expensive

- 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?

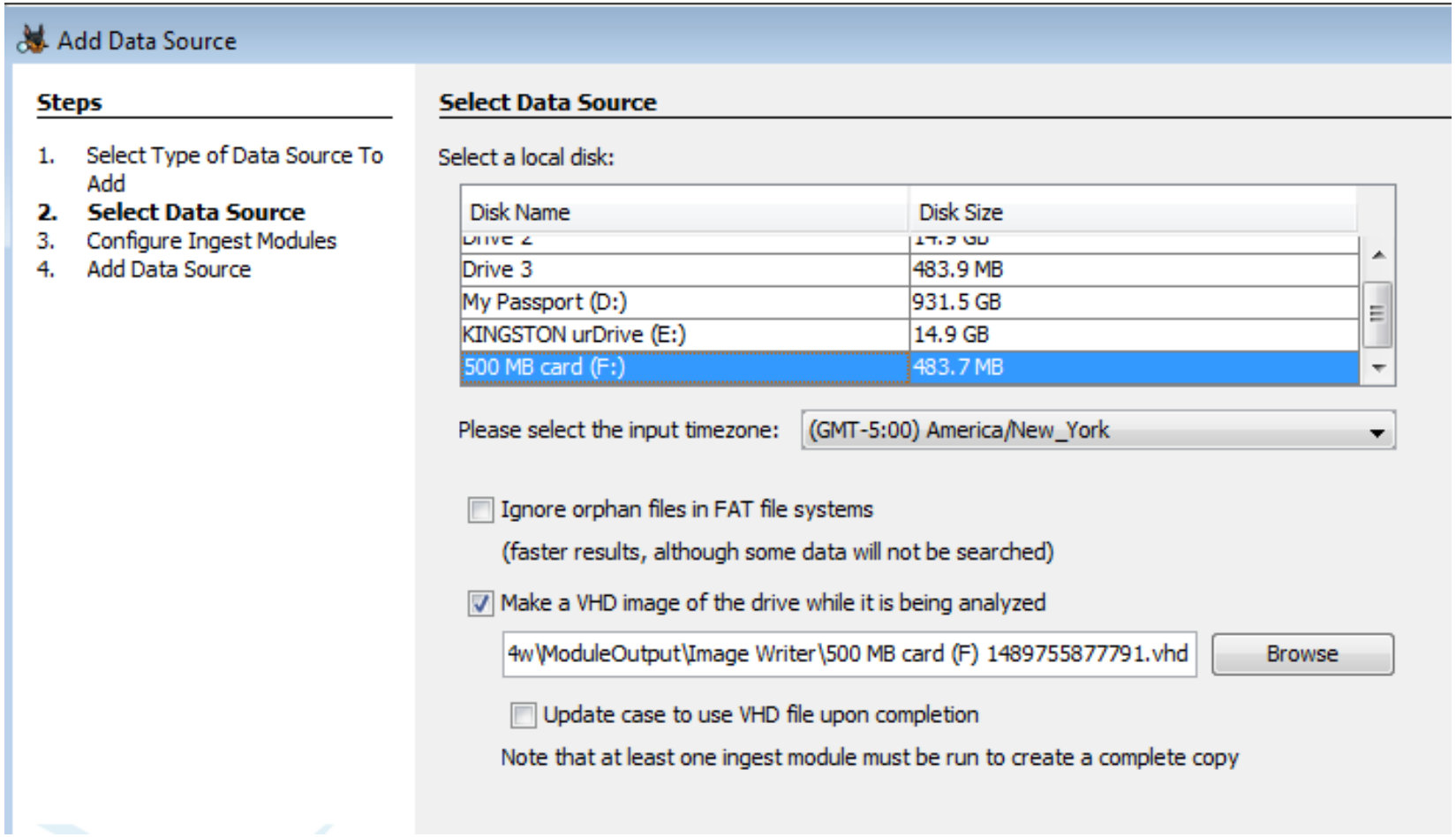
- File format used by Microsoft Virtual Machines.
- "Sparse" because the file size is based on how much data has been written to it.
- Efficient to write random sectors to (versus traditional formats)
- Readable by Windows (double click it) and other forensics tools.
- A VHD file from Autopsy will contain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

Normal Raw vs. VHD Images



Making a VHD with Autopsy

- Only possible when analyzing a local drive.

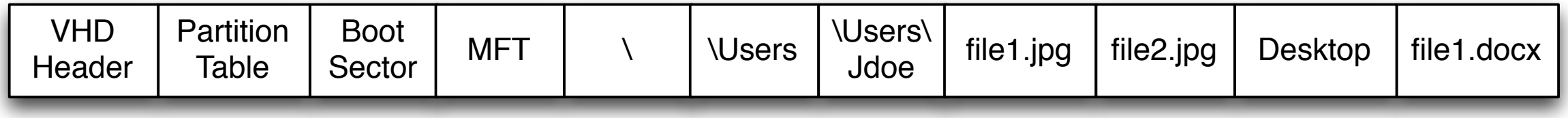


Making a VHD with Autopsy

- 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 Limitations

- 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

Scenario

- 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.

Scenario (continued)

- 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

Scenario (continued)

- 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.

Triage Summary

- 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