Quick Preview of Drives Using Autopsy

Ann Priestman

Motivation

- You want 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 their system
  - At a location where there are lots of systems. Want to know which to analyze first (or which to image/grab)

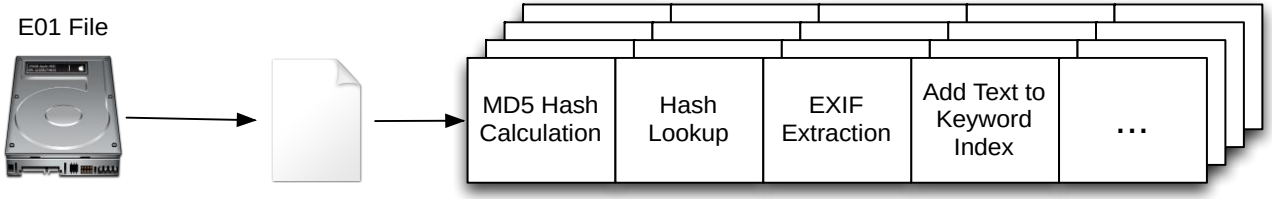
How We Solve It

1. Focus on files that are most likely to be relevant
2. Make a sparse image of the drive as we read it, which can later be opened and analyzed further
3. Allow Autopsy to run on a live computer from a USB drive

Focus on the Relevant Files

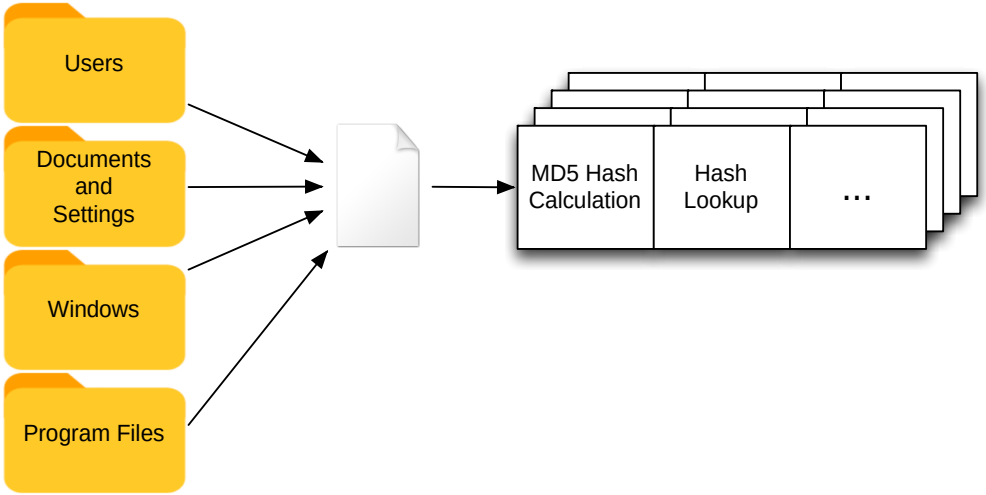
Short Time Requires Focus

- We want to get the most relevant files down the pipelines first
  1. User files have top priority
  2. Ingest filters can be used to ignore non-relevant files
  3. Ingest profiles combine an ingest filter and a subset of ingest modules to run



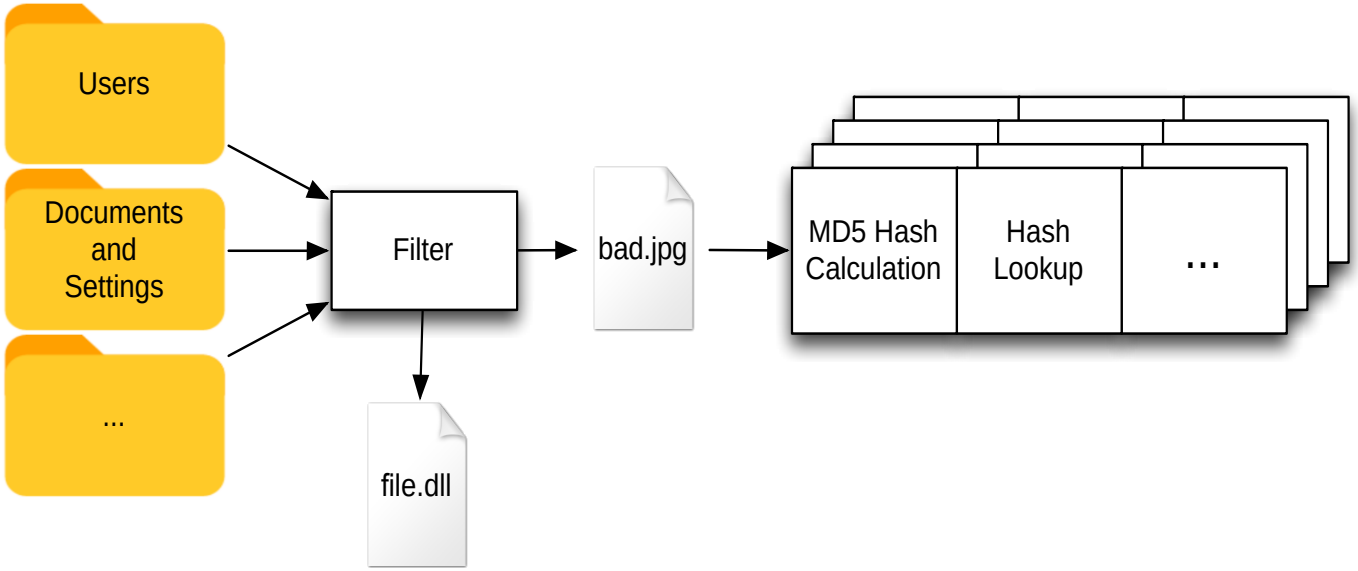
Schedule User Folders First

- Autopsy always run user folders through the pipeline first – that's often where the good stuff is located



Ingest Only a Subset of Files

- Skip files that are unlikely to be relevant based on file name, parent folder, or modified time



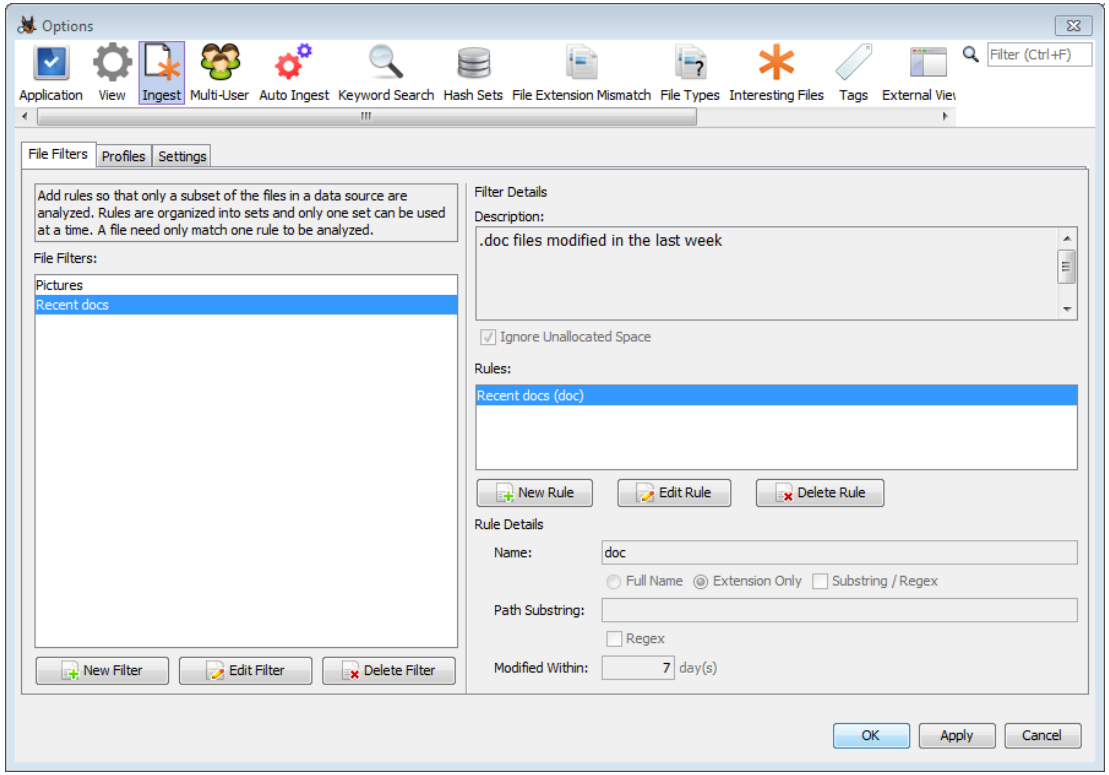
Ingest File Filters

- Set of rules that defines what passes
  - If any rule is true then the file passes
- Can ignore unallocated space
- Only one filter can be used at a time

Rules

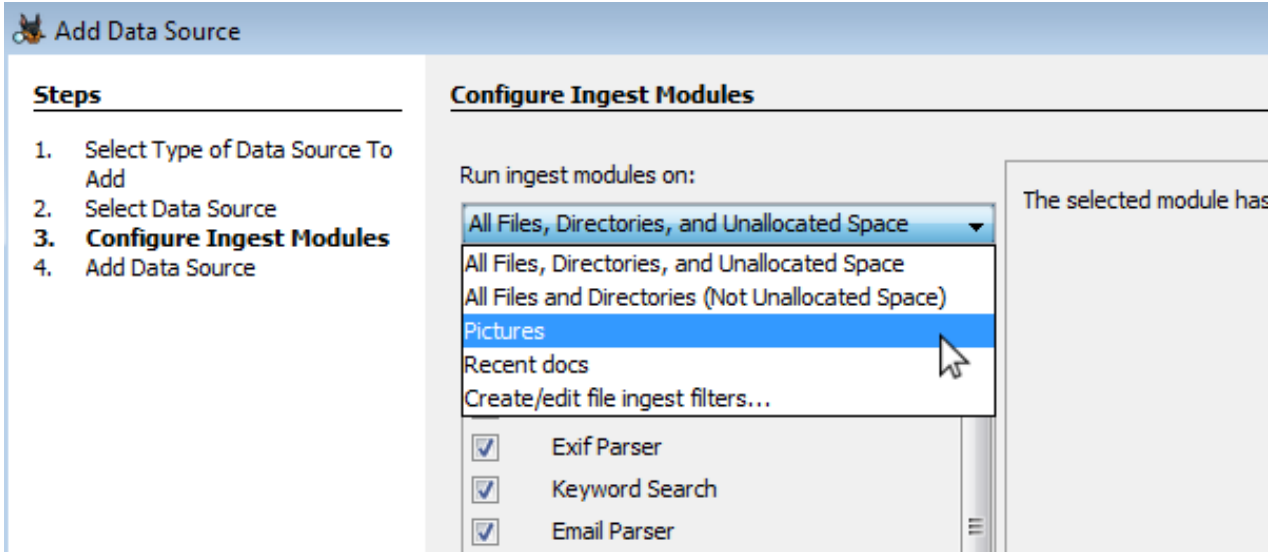
- Rules can be based on:
  - Name
    - Full name or extension only
  - Path
    - The value must be a substring in the full path
  - Date
    - Modified or created within the past X days

Making Ingest File Filters – Options Panel



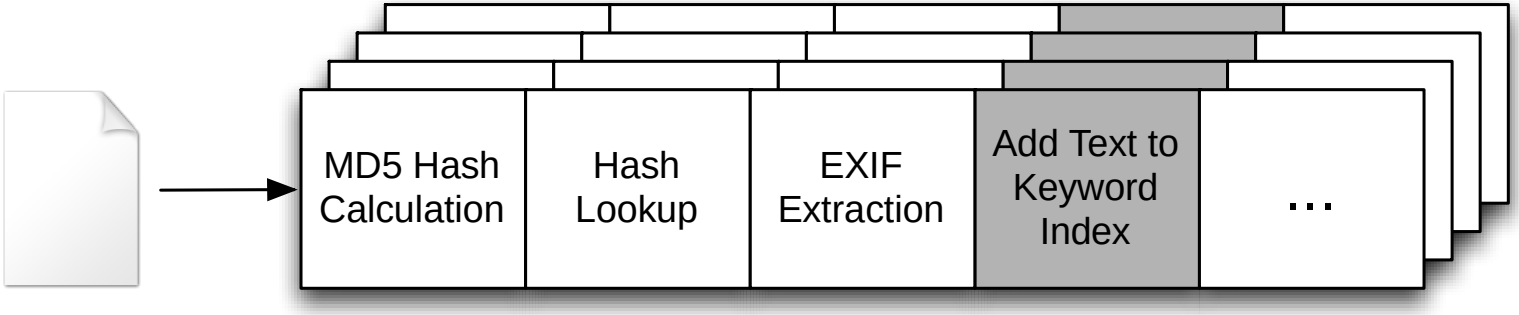
Choosing a File Filter

- Select your file filter to control which files the are processed by the 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

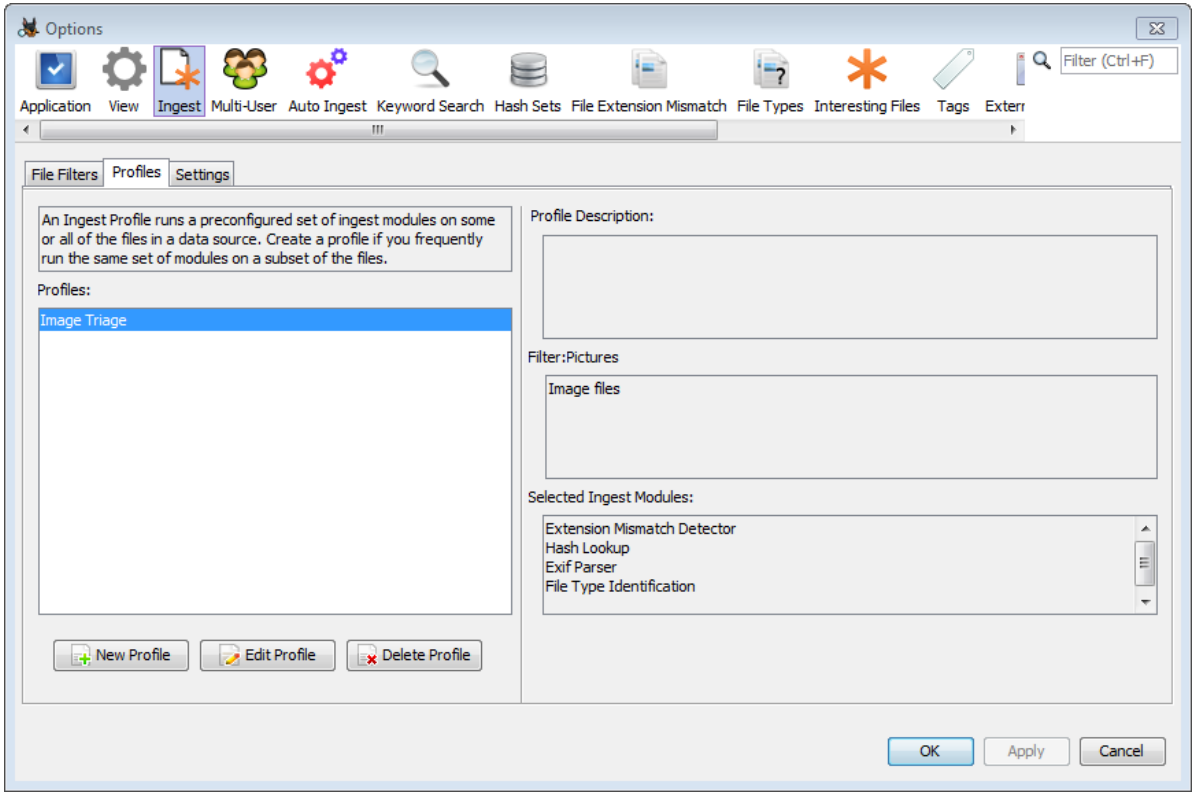


- You can manually do this, or…

Ingest Profiles

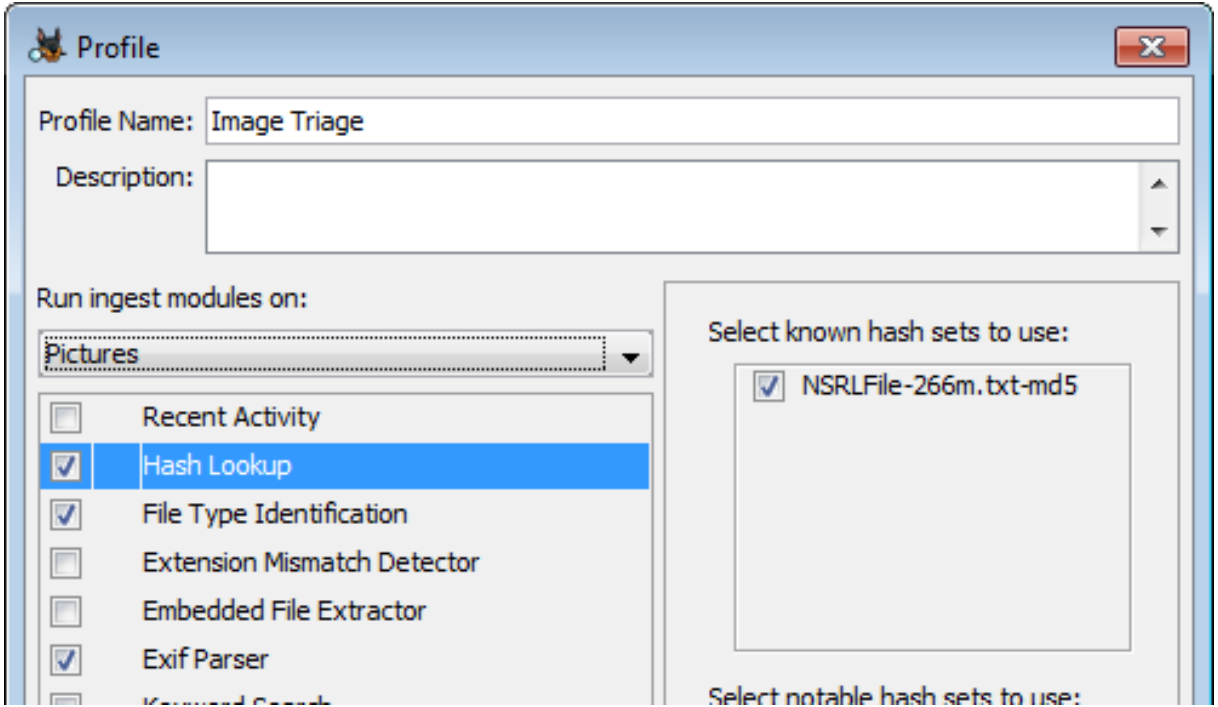
- Many triage sessions are similar
- Save time by configuring a profile that specifies:
  - Ingest filter to use
  - Ingest modules to use
- Example:
  - File filter that accepts .jpg, .png, etc. and Downloads
  - Ingest modules for hash lookups, EXIF, zip files, etc.

Making a Profile – Options Panel



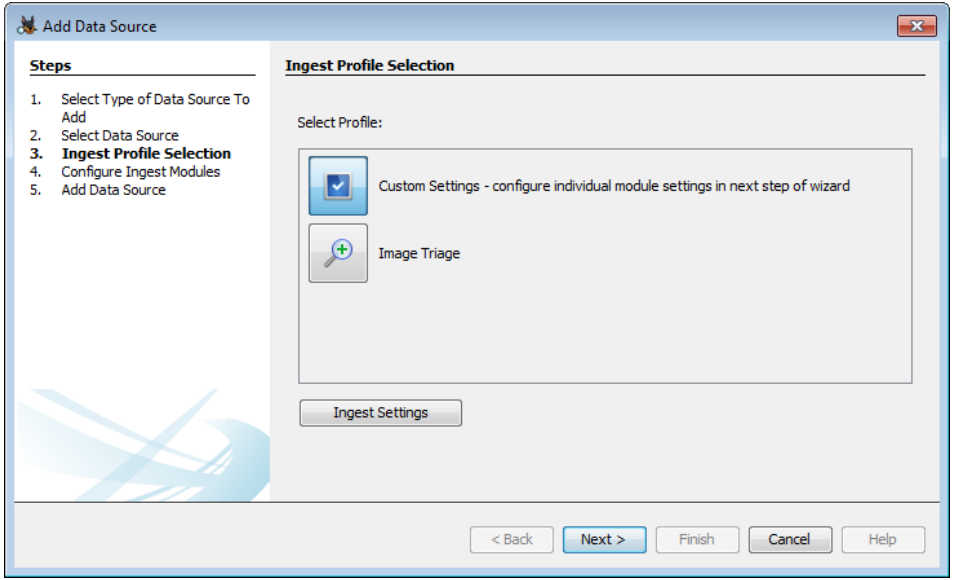
Making a New Profile

- Specify:
  - Name
  - Description
  - File Filter
  - Set of modules and their configuration



Selecting the Profile

- You will be able to select your profile after choosing your data source



Keep a Copy of Any Data You Read

Making an Image is Expensive

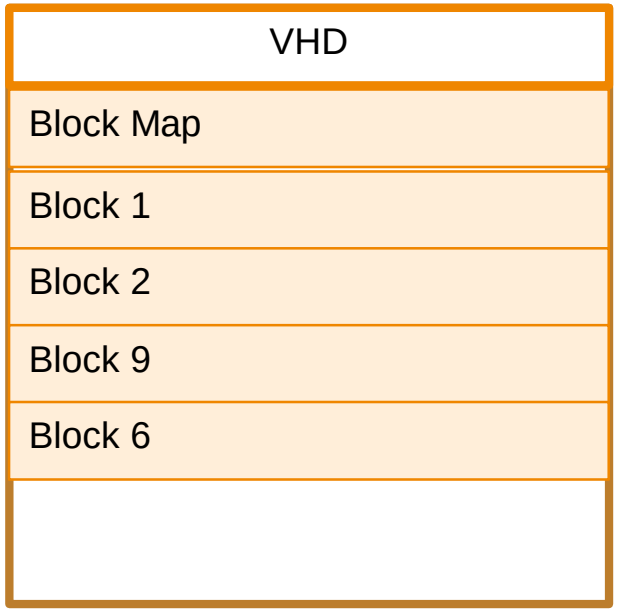
- Problem:
  - You want a record of what data was on the disk
  - Don't have time to make a full image
  - Ideally want more than just the notable files
- Solution:
  - Make an image as your analysis happens – each sector that is read in is also saved to a "sparse VHD file"

What is 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
  - Also known as “dynamic” or “expandable”
  - Efficient to write random sectors to
  - Readable by Windows and other forensic tools

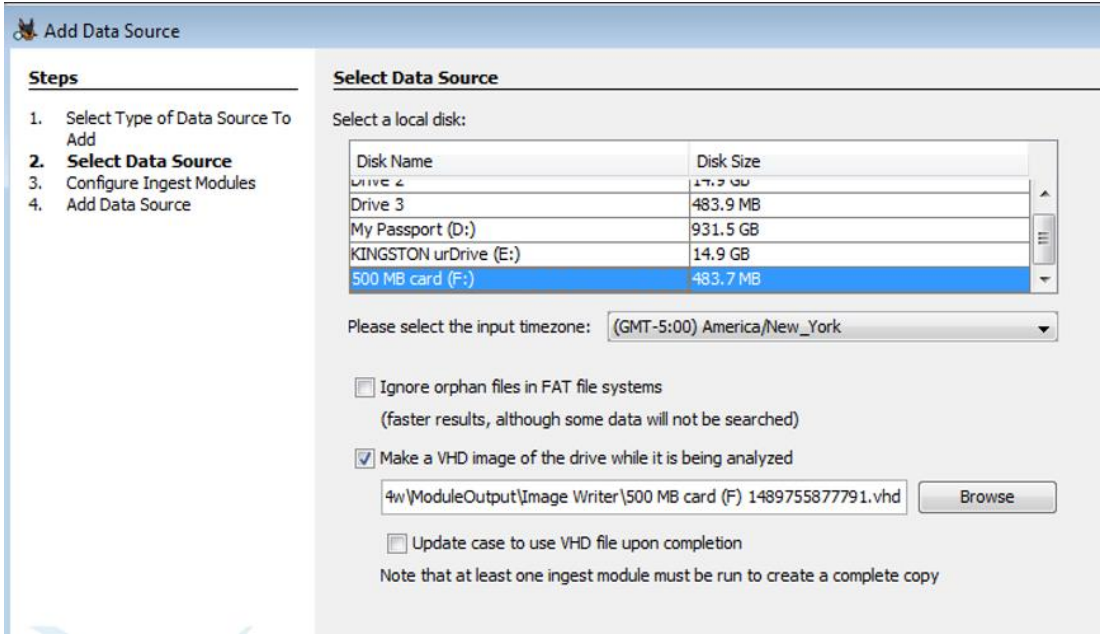
Sparse VHD Format

- Each block read by Autopsy is written to the sparse VHD
- The blocks may not be in order
- When normal analysis is complete, Autopsy will start filling in any missing blocks



Making a VHD with Autopsy

- Only possible when analyzing a local disk



VHD Limitations

- It is not compressed
  - VHD supports compression, but The Sleuth Kit/Autopsy do not yet
- At present, you need to have room to save the full image in your case folder

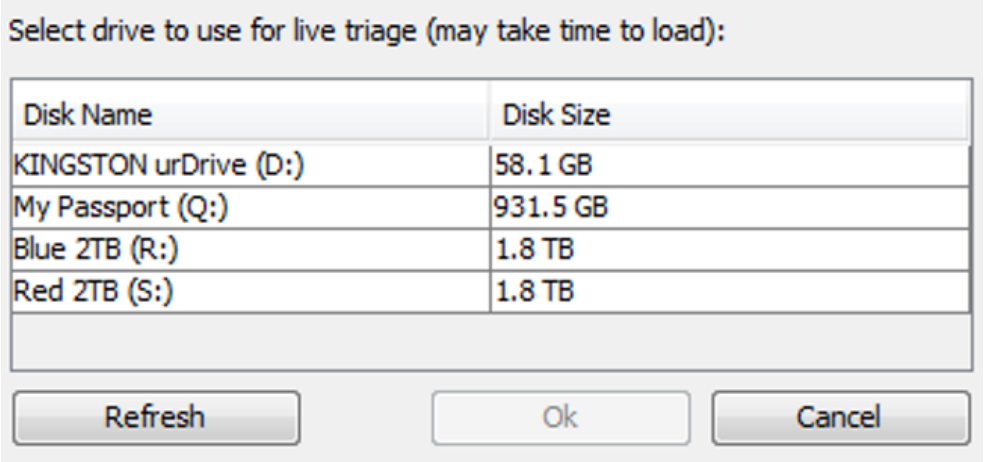
Creating and Using an Autopsy Live Triage Drive

Running Autopsy from USB

- Autopsy can be installed normally and run from a USB drive, but there are drawbacks:
  - It will write config data to the local AppData folder
  - You can't save your config settings between runs
- Creating a live triage drive solves these issues by saving all relevant data to the USB drive

Making a Live Triage Drive

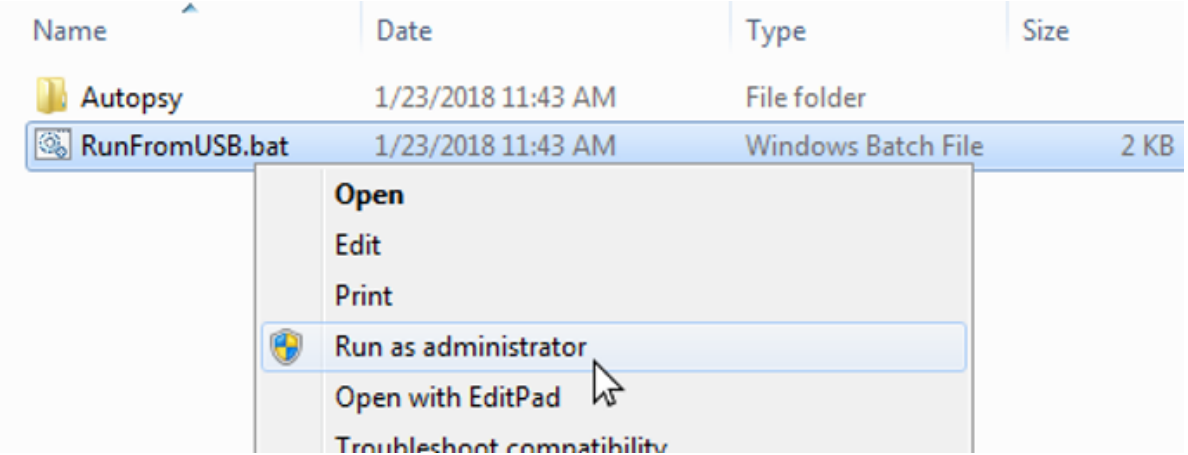
- Select Menu->Tools -> Make Live Triage Drive and pick the external drive to use



- This copies Autopsy and a ".bat" file to the USB

Running Autopsy

- Insert the USB drive into a live system
- Open file explorer and run “RunFromUSB.bat” file as Administrator

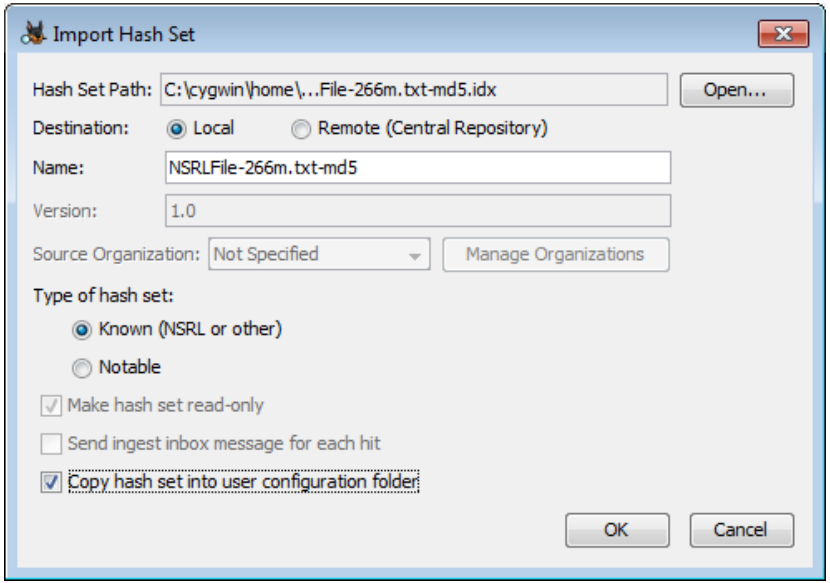


Configuration

- You can launch Autopsy from USB on your computer and preconfigure it
  - Set up ingest profiles
  - Configure keyword lists
  - Import hash sets

Importing Hash Sets

- Check the “Copy hash set into user configuration folder” box when importing the hash set
- Will copy it into the config folder on the USB drive



Using the Live Triage Drive

- Launch from “RunFromUSB.bat”
  - Create a case and save to the USB drive
  - Add local disk as data source, making a VHD image as the drive is analyzed

Putting It All Together

Scenario - Overview

- Knock and talk or probation situation
- Goal is to answer whether child exploitation images exist

Scenario - Preparation

- At the office:
  - Create a Live USB drive
  - Launch Autopsy from that USB and create an ingest profile that:
    - Runs on picture and ZIP extensions
    - Runs the Hash Lookup, EXIF, File Type, and Embedded File Extractor modules
    - Uses known child exploitation hash sets

Scenario – Launching Autopsy

- At the house:
  - Plug Live USB drive into their laptop
  - Launch Autopsy from .bat file
  - Create a case (saving to USB drive)
  - Add a local drive data source:
    - "C:"
    - Choose to make VHD and keep default location

Scenario – Analyzing the Drive

- As the automatic analysis continues:
  - Choose View->File Types -> Images and review the thumbnails
  - Wait for hash set hits
  - Review EXIF files
  - Tag any notable files found
- You can stop the analysis at any time. All data read so far will be in the VHD file.

Questions?

Ann Priestman
apriestman@basistech.com