

9th Annual

#OSDFCon

OPEN SOURCE DIGITAL FORENSICS CONFERENCE

Quick Preview of Drives Using Autopsy

Ann Priestman



Wifi: HyattMTG
Access Code: osdfcon

October 17, 2018 | Herndon, VA | Hosted by



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

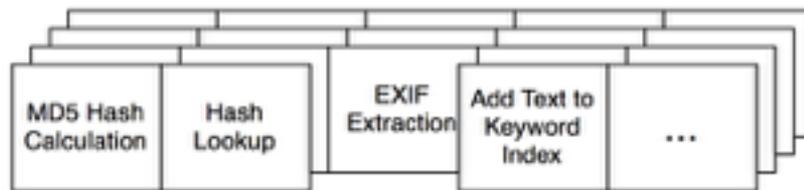


Focus on the Relevant Files

Short Time Requires Focus

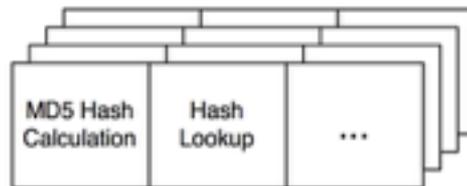
We want to get the most relevant files down the pipelines first

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



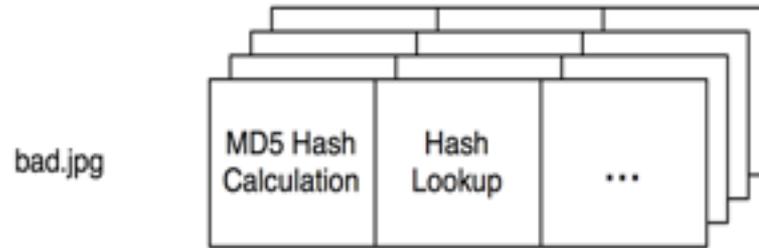
Schedule User Folders First

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

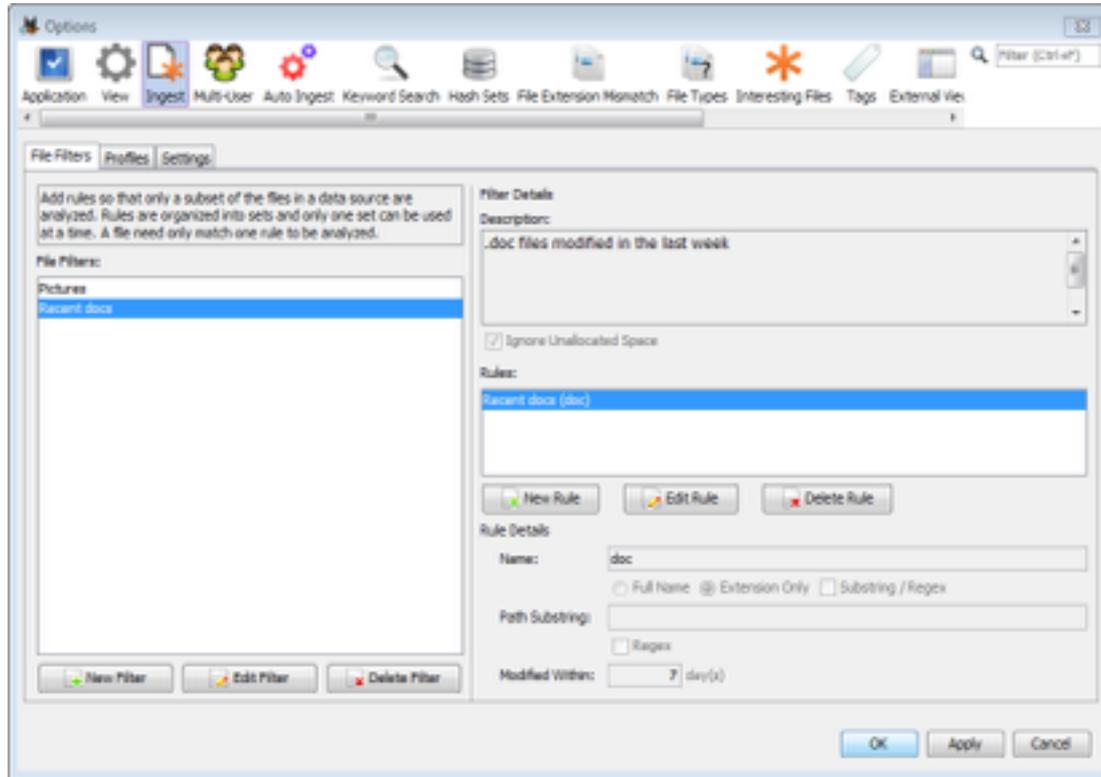
Rules



Rules can be based on:

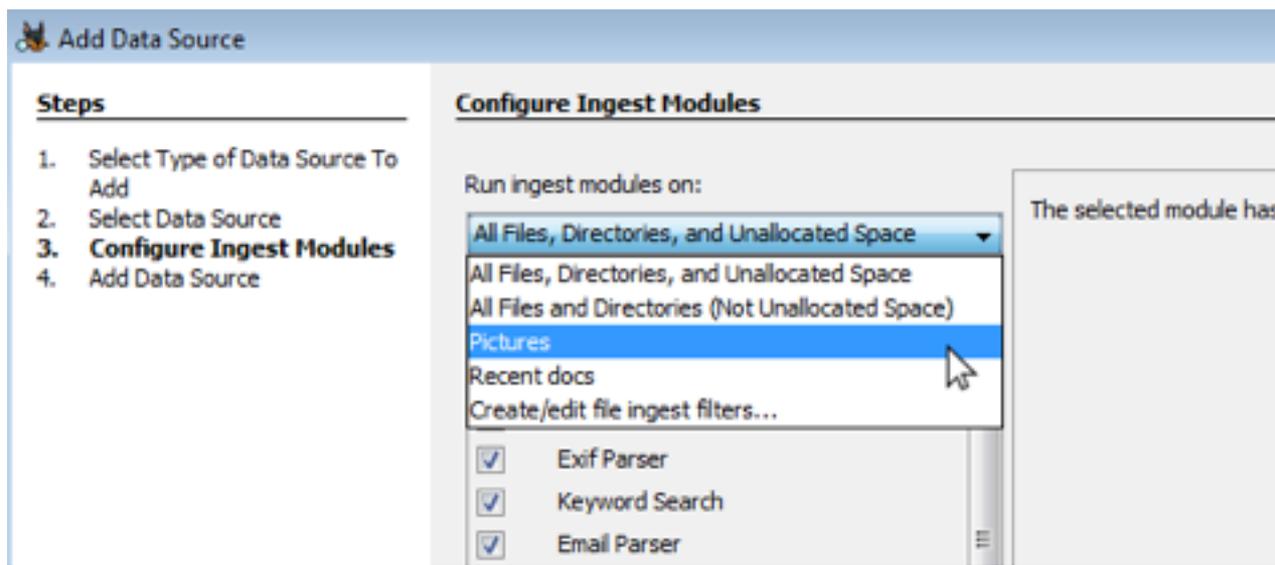
- Name
 - **Full name or extension only**
- Path
 - **The value must be a substring in the full path**
- Date
 - **Modified or created within the past X days**

Making Ingest File Filters – Options Panel



Choosing a File Filter

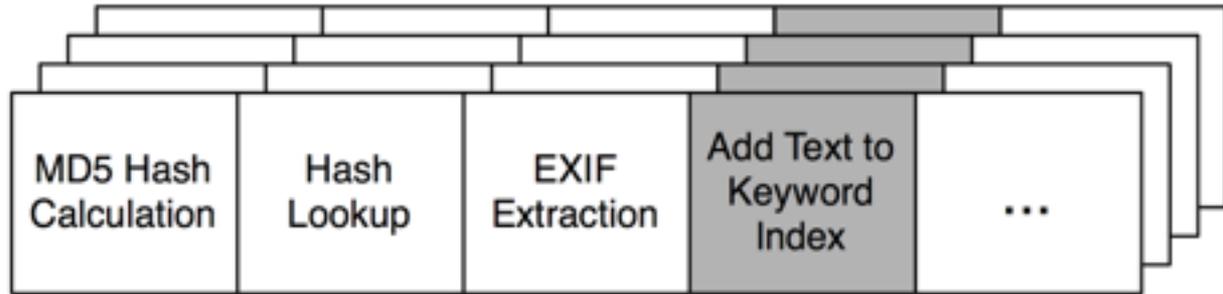
Select your file filter to control which files the are processed by the ingest modules



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

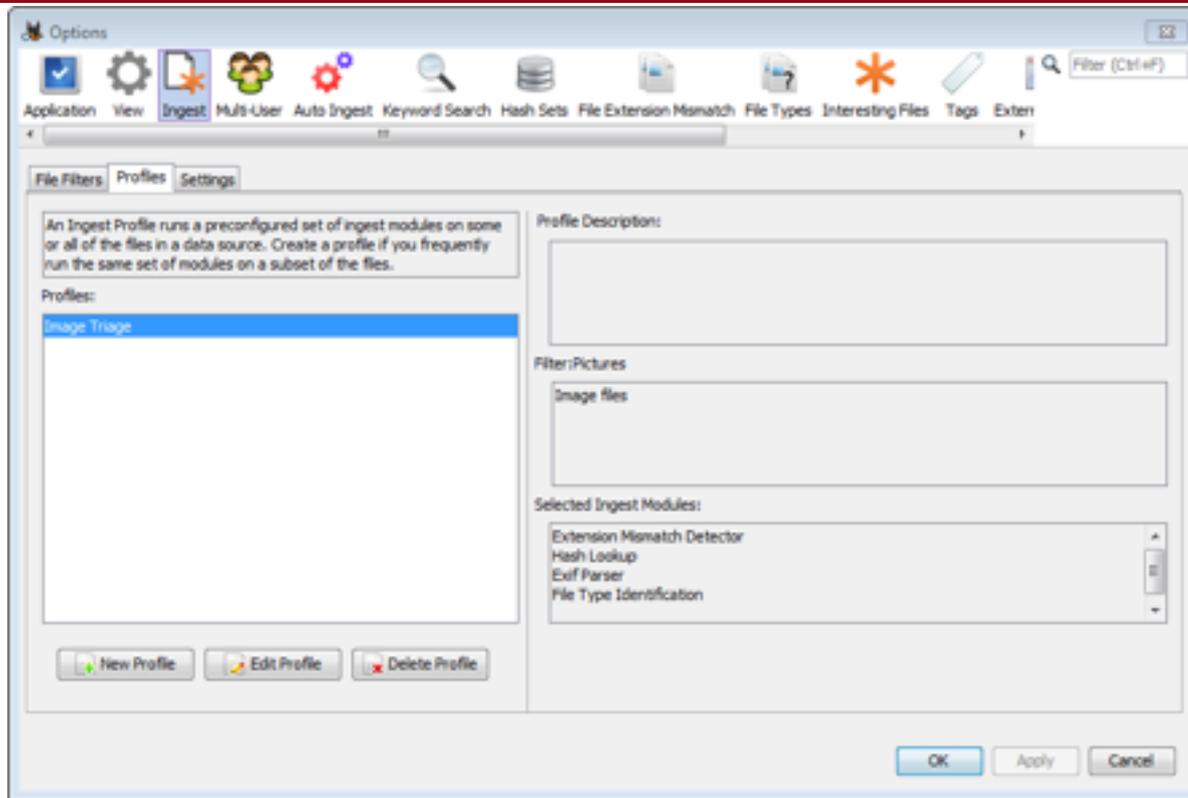
Save time by configuring a profile that specifies:

- 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

Profile

Profile Name: Image Triage

Description:

Run ingest modules on:

Pictures

- Recent Activity
- Hash Lookup
- File Type Identification
- Embedded File Extractor
- Exif Parser
- Keyword Search
- Email Parser

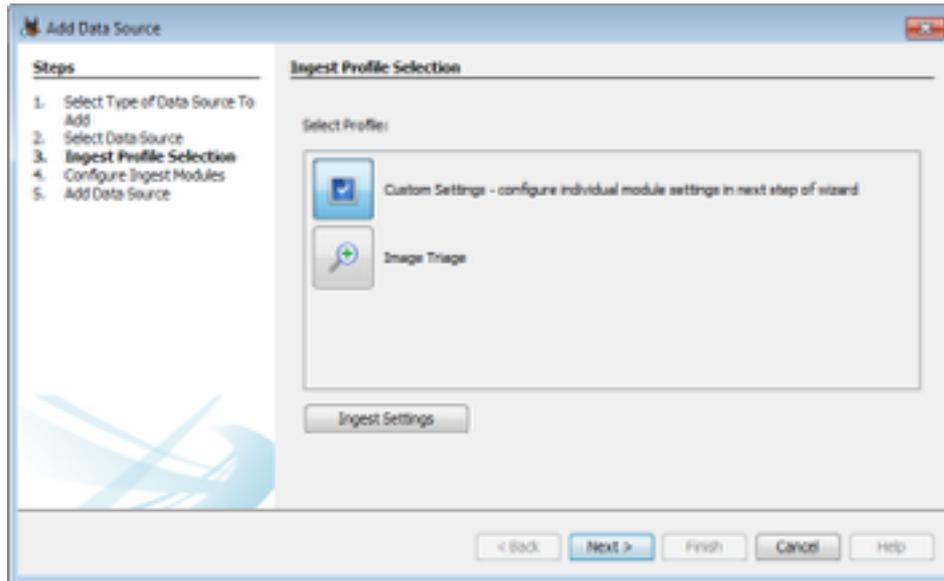
Select known hash sets to use:

- NSRFile-245m.txt-md5

Select notable hash sets to use:

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

Making a VHD with Autopsy

Only possible when analyzing a local disk

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 | 471.3 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

VHD Limitations

It is not compressed

- VHD supports compression, but The Sleuth Kit/Autopsy do not yet

There are no cryptographic checksums

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

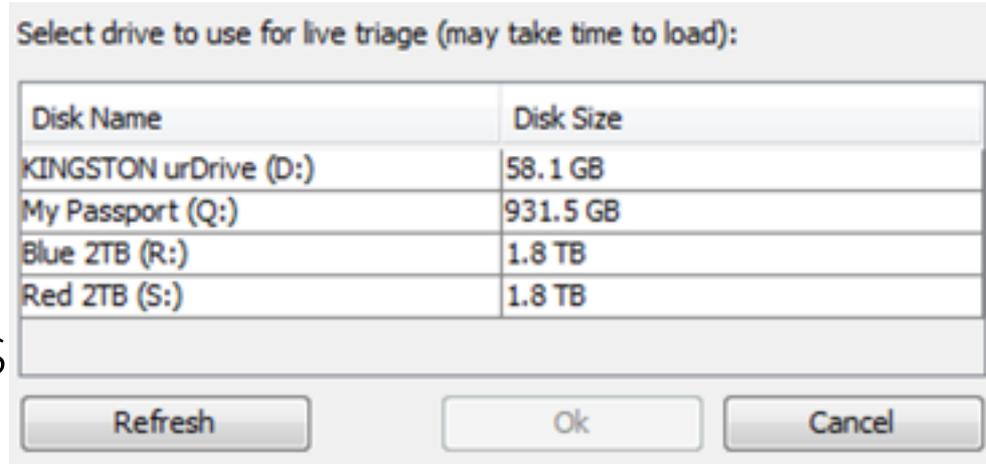
Autopsy can be installed normally and run from a USB drive, but there are drawbacks:

- 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



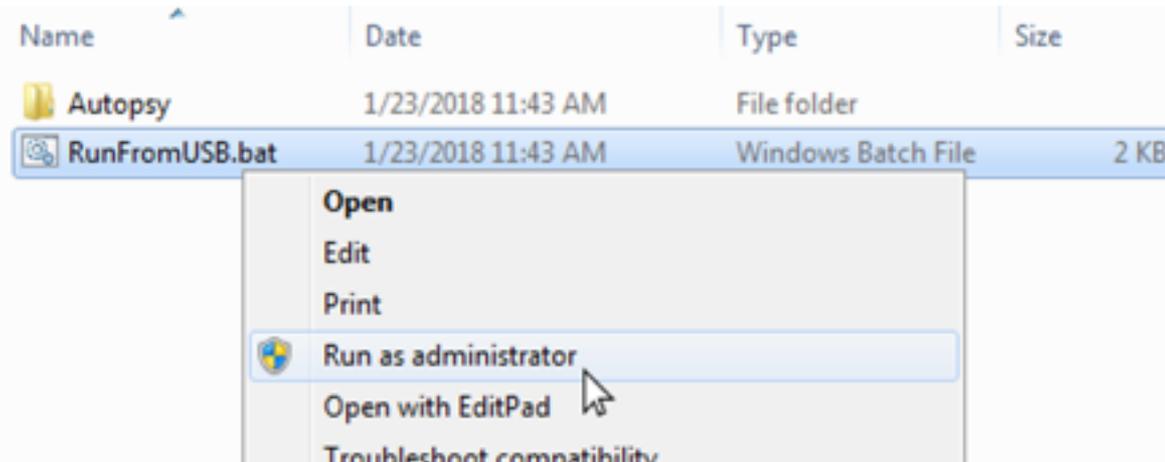
This copies

JSB

Running Autopsy

Insert the USB drive into a live system

Open file explorer and run “RunFromUSB.bat” file as Administrator



Configuration

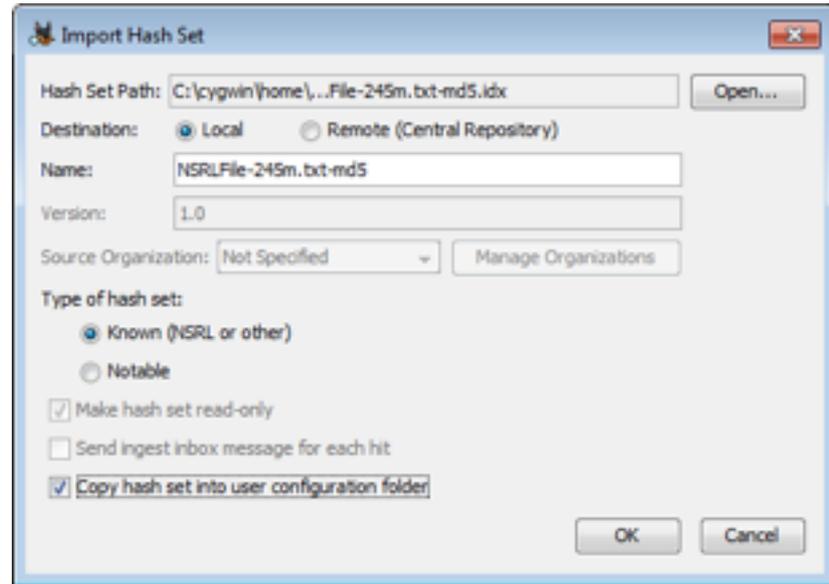
You can launch Autopsy from USB on your computer and preconfigure it

- 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.

9th Annual

#OSDFCon

OPEN SOURCE DIGITAL FORENSICS CONFERENCE

Questions?

Ann Priestman
apriestman@basistech.com