9<sup>th</sup> Annual

### #OSDFCon

OPEN SOURCE DIGITAL FORENSICS CONFERENCE

#### Quick Preview of Drives Using Autopsy

Ann Priestman



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)



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



# 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

bad.jpg





Hash

Lookup

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 Ο
  - Modified or created within the past X days



#### Making Ingest File Filters – Options Panel

A Options	8
🖸 🗘 🛃 🚱 🗳 🔍 🛛	
Application Vew Ingest Multi-User Auto Ingest Keyword Search Ha	sh Sets. File Extension Mismatch. File Types. Interesting Files. Tags. External Ver
File Filters Profiles Settings 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. Pile Pilers: Pictures Discort docs	Piter Details Description:    doc files modified in the last week
	Image: New Rule     Image: Bdit Rule     Image: Delete Rule       Rule Details     Image: Image: Delete Rule       Name:     Image: Image: Image: Delete Rule       Full Name:     Image: Ima
New Pilar 2 Edit Pilar	Madfied Within: 7 day(s)
	OK Apply Canod



#### Choosing a File Filter

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

🖌 Add Data Source			
Steps	Configure Ingest Modules		
<ol> <li>Select Type of Data S Add</li> <li>Select Data Source</li> <li>Configure Ingest M</li> <li>Add Data Source</li> </ol>	All Files, Directories, and Unallocated Space All Files, Directories, and Unallocated Space All Files and Directories (Not Unallocated Space) Recent docs Create/edit file ingest filters Exif Parser Keyword Search E Email Parser E mail Parser E		



Process more files by spending less time on each

Don't run the modules you don't need



You can manually do this, or...





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

😹 Options	8
Appication View Ingest Multi-User Auto Ingest Keyword Search Had	File Extension Mamatch File Types Interesting Files Tags Extern
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.	Profile Description:
Profiles: Insige Triage	
	PiterPictures
	Drage files
	Selected Ingest Modules:
	Extension Monatch Detector A Hish Lookup Exif Parser E He Type Identification
New Profie	
	OK Apply Cancel



### Making a New Profile

Specify:

- o Name
- Description
- File Filter
- Set of modules and their configuration

😹 Pro	file		×
Profile	Name: Image Triage		
Descr	iption:		
			+
Run ing Picture	est modules on:	Select known hash sets to use:	
	Recent Activity	V NSRLPIE-245m. DC-md5	
	Hash Lookup		
	File Type Identification		
	Embedded File Extractor		
	Exif Parser		
	Keyword Search		_
	Email Darcer	Select notable hash sets to use:	



#### Selecting the Profile

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

😹 Add Data Source		
Steps   Select Type of Data Source To Add  Select Data Source  A Ingest Pholie Selection  Configure Ingest Modules  Add Data Source	Impest Profile Selection           Select Profile           Custom Settings - configure individual module settings in next step of staard           Image Triage	
	Ingest Settings	
	Klack Next > Finish Cancel H	tip



## 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"



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

Steps	Select Data Source		
<ol> <li>Select Type of Data Source To Add</li> </ol>	Select a local disk:		
2. Select Data Source	Disk Name	Disk Size	
<ol><li>Configure Ingest Modules</li></ol>	LAINE 4	17.2 00	
<ol> <li>Add Data Source</li> </ol>	Drive 3	483.9 MB	_
	My Passport (D:)	931.5 GB	
	KINGSTON urDrive (E:)	14.9 G8	
	500 M8 card (F:)	483.7 M8	-
	Ignore orphan files in FAT f (faster results, although so Make a VHD image of the di 4w WoduleOutput/Jimage V Update case to use VH Note that at least one income	le systems me data will not be searched) ivre while it is being analyzed inter\\$00 MB card (F) 1489755877791.vhd Bro D file upon completion at module must be sur to create a complete conv	wse



#### **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





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

Select drive to use for live triage (may take time to load):

	Disk Name	Disk Size		
	KINGSTON urDrive (D:)	58.1 GB		
	My Passport (Q:)	931.5 GB		
	Blue 2TB (R:)	1.8 TB		
	Red 2TB (S:)	1.8 TB		
This copies				JSB
	Refresh	Ok	Cancel	



#### Insert the USB drive into a live system

#### Open file explorer and run "RunFromUSB.bat" file as Administrator

Name	Date	Туре	Size
퉬 Autopsy	1/23/2018 11:43 AM	File folder	
RunFromUSB.bat	1/23/2018 11:43 AM	Windows Batch File	2 KB
	Open		
	Edit		
	Print		
	Run as administrator		
	Open with EditPad		
	Troubleshoot compatibility		

#### 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

😹 Import Hash	s Set		
Hash Set Path:	Hash Set Path: C:\cygwin\homeFile-245m.bxt-md5.idx Open		
Destination:	Local     O Remote (Central Repository)		
Name:	NSRLFile-245m.txt-md5		
Version:	1.0		
Source Organiza	ation: Not Specified + Manage Organizations		
Type of hash set:			
Known (NSRL or other)			
Notable			
✓ Make hash set read-only			
Send ingest inbox message for each hit			
Copy hash set into user configuration folder			
	OK Cancel		



#### 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









#### 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.



9<sup>th</sup> Annual

### #OSDFCon

OPEN SOURCE DIGITAL FORENSICS CONFERENCE

### **Questions?**

#### Ann Priestman apriestman@basistech.com

October 17, 2018 | Herndon, VA | Hosted by

