IFS4102 LAB
WEEK 5

REMINDER: WEEK 5 GRADED LAB TASKS #3
SATURDAY, 18 FEBRUARY 2023, 23:59 SGT
USE THE GIVEN SAMPLE FILE

OBJECTIVES

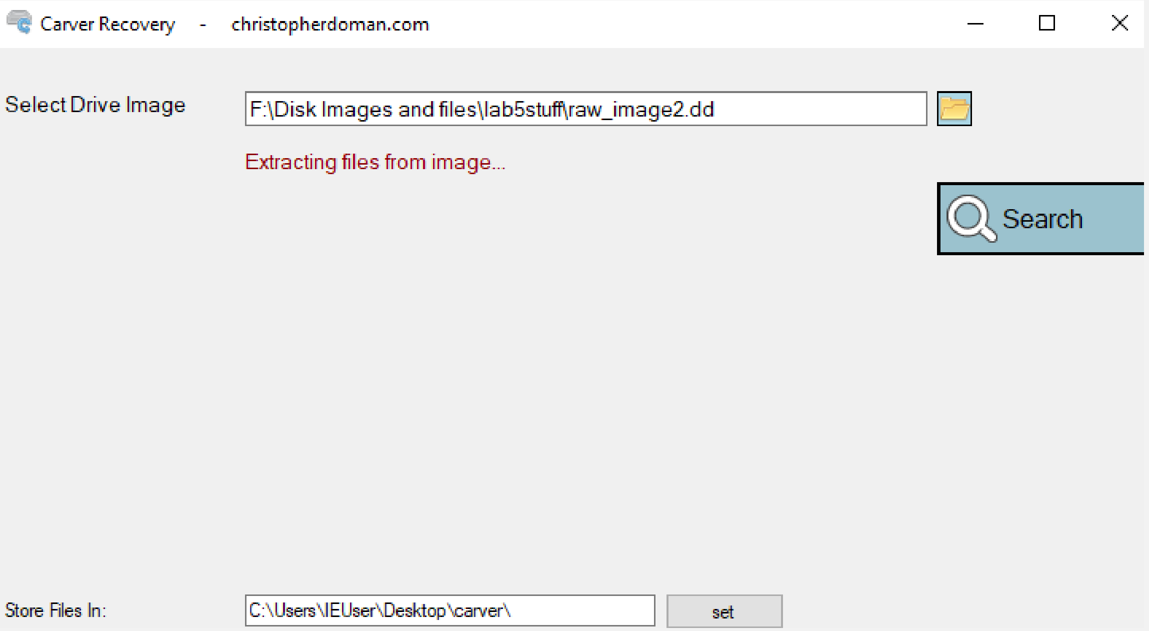
1. Perform automated file carving **(Task 1)**
2. Use Autopsy to find interesting files & find keywords **(Task 3-A&B)**
3. Extraction and analysis of windows registry files **(Task 4-A&B)**

1. AUTOMATED FILE CARVING **(TASK 1)**

- Recall last week's lecture, file carving is a process to extract data from a disk drive without the assistance from the file system
- Commonly performed on unallocated space because there is no metadata structure pointing to them
- Usually done by searching for signatures that corresponds to start and end known file type. Sounds familiar?
    - Your lab 4 Task 2.
- Live demo, use raw_image2.dd

1. AUTOMATED FILE CARVING (**TASK 1**)

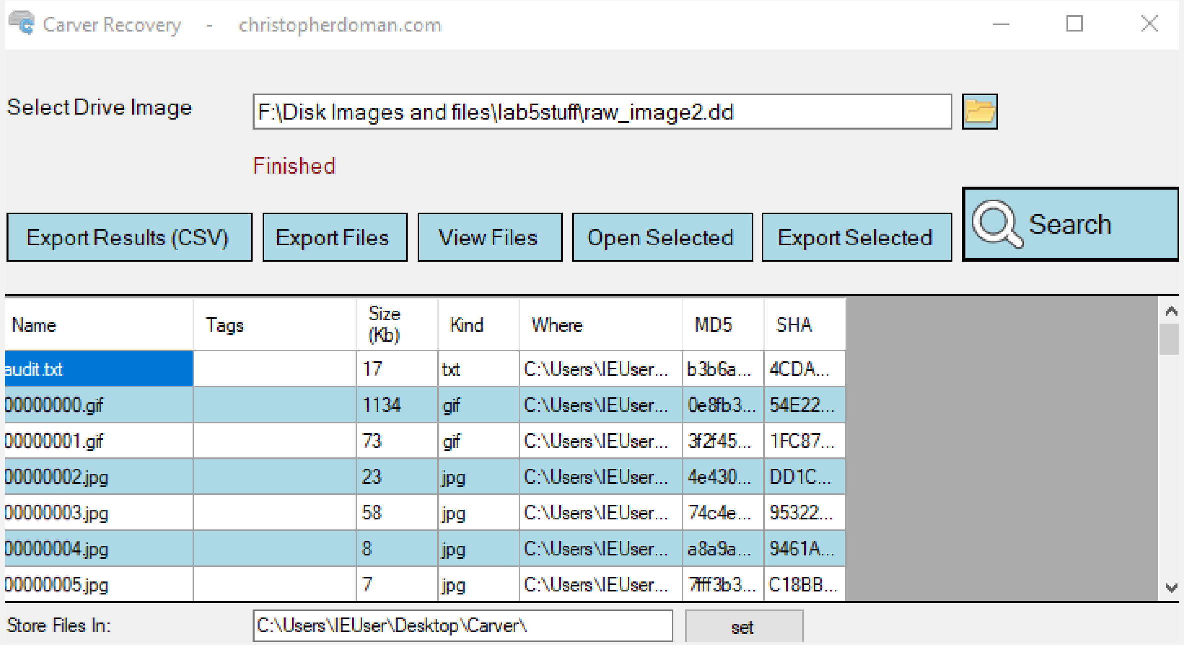
Carver Recover



Select Drive Image: F:\Disk Images and files\lab5stuff\raw_image2.dd

Extracting files from image...

Store Files In: C:\Users\IEUser\Desktop\carver\



Select Drive Image: F:\Disk Images and files\lab5stuff\raw_image2.dd

Finished

Name	Tags	Size (Kb)	Kind	Where	MD5	SHA
audit.txt		17	txt	C:\Users\IEUser...	b3b6a...	4CDA...
00000000.gif		1134	gif	C:\Users\IEUser...	0e8fb3...	54E22...
00000001.gif		73	gif	C:\Users\IEUser...	3f2f45...	1FC87...
00000002.jpg		23	jpg	C:\Users\IEUser...	4e430...	DD1C...
00000003.jpg		58	jpg	C:\Users\IEUser...	74c4e...	95322...
00000004.jpg		8	jpg	C:\Users\IEUser...	a8a9a...	9461A...
00000005.jpg		7	jpg	C:\Users\IEUser...	7fff3b3...	C18BB...

Store Files In: C:\Users\IEUser\Desktop\Carver\

1. AUTOMATED FILE CARVING **(TASK 1)**

- **Bulk Extractor Viewer**
- bulk_extractor-x.y.z-windowsinstaller.exe
  - Latest version is 1.5.5 but feel free to use older versions
- Java 6+ (But Java 8 not compatible)
  - https://drive.google.com/file/d/1yxG0JXUMUcKtsj-i9MoTGtRCMrAPcNyi/view?usp=sharing

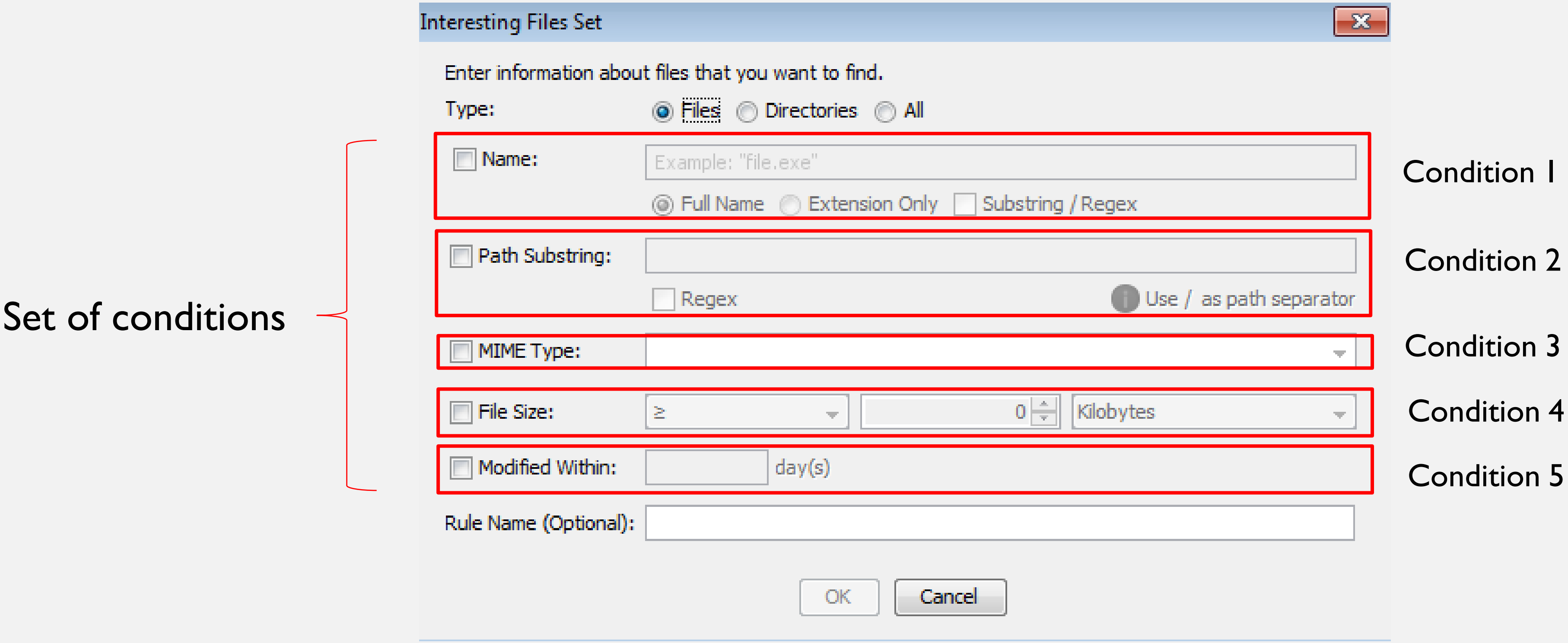
2. USE AUTOPSY TO FIND INTERESTING FILES & FIND KEYWORDS **(TASK 3-A&B)**

- Introduce 2 more ingest modules:
  - Interesting Files Identifier
  - Keyword search
- Interesting Files Identifier check **file/directory names, paths or certain type**
- Keyword search **looks inside the file** and search for strings

2. USE AUTOPSY TO FIND INTERESTING FILES & FIND KEYWORDS **(TASK 3-A&B)**

- **Interesting File Identifier Module**
- A rule is a set of conditions that must be true about a file to match the rule
- All conditions in the rule must be true
  - If conditions set "file size >1MB" and "file extension = txt", only file that matches both condition will display

2. USE AUTOPSY TO FIND INTERESTING FILES & FIND KEYWORDS **(TASK 3-A&B)**



Interesting Files Set

Enter information about files that you want to find.

Type: ● Files ○ Directories ○ All

□ Name: Example: "file.exe"
● Full Name ○ Extension Only □ Substring / Regex

□ Path Substring:
□ Regex — Use / as path separator

□ MIME Type:

□ File Size: ≥ 0 Kilobytes

□ Modified Within: day(s)

Rule Name (Optional):

Set of conditions

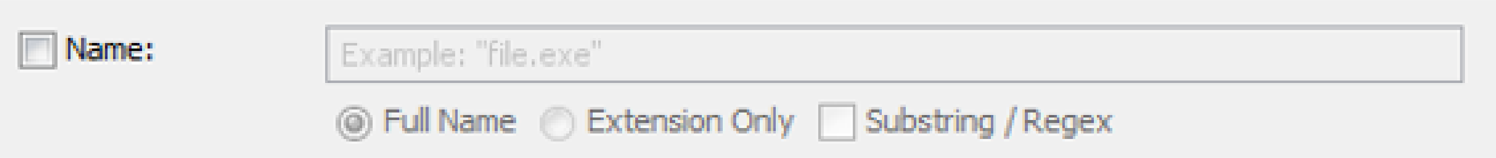
Condition 1

Condition 2

Condition 3

Condition 4

Condition 5



□ Name: Example: "file.exe"

● Full Name ○ Extension Only □ Substring / Regex

Type	Substring/Regex	Text	Description	Sample match
Full Name	false	test.txt	Will match files named "test.txt"	text.txt
Full Name	true	bomb	Will match files with "bomb" anywhere their name	Pipe bomb.png
Full Name	true	virus.*\.exe	Will match files with "virus" followed by ".exe" anywhere their name	bad_virus.exe
Extension Only	false	zip	Will match .zip files	myArchive.zip
Extension Only	false	zip,rar,7z	Will match .zip, .rar, and .7z files	anotherArchive.rar
Extension Only	true	jp	Will match .jpg, .jpeg files, and any others with "jp" in the extension	myImage.jpg

http://sleuthkit.org/autopsy/docs/user-docs/4.12.0/interesting_files_identifier_page.html

2. USE AUTOPSY TO FIND INTERESTING FILES & FIND KEYWORDS **(TASK 3-A&B)**

- **Keyword search module**
- Extract text from files and search keywords
- Comes with built in list for searching phone numbers, IP addresses, URLs and Emails.
- http://sleuthkit.org/autopsy/docs/user-docs/3.1/keyword_search.html

3. EXTRACTION AND ANALYSIS OF WINDOWS REGISTRY FILES (**TASK 4-A&B**)

Task 4A

- Manual using regedit
- Powerful but time consuming
- You need to know what keys you to look for

Task 4B

- Regripper
- Control-F

3. EXTRACTION AND ANALYSIS OF WINDOWS REGISTRY FILES (**TASK 4-A&B**)

Extra (Task 4C?)

- Reg Explorer
- https://ericzimmerman.github.io/#!index.md

QUESTIONS?

REMINDER: WEEK 5 GRADED LAB TASKS #3

SATURDAY, 18 FEBRUARY 2023, 23:59 SGT

USE THE GIVEN SAMPLE FILE