IFS4102 LAB
WEEK 9

REMINDER: WEEK 7 GRADED LAB TASKS #4
SATURDAY, 18 MARCH 2023, 23:59 SGT
USE THE GIVEN SAMPLE FILES

REMINDER: WEEK 9 GRADED LAB TASKS #5
SATURDAY, 25 MARCH 2023, 23:59 SGT
USE YOUR OWN WINDOWS MACHINE/VM

OBJECTIVES

1. Use Autopsy's Plaso and timeline feature **(Task 1)**
2. Run various Windows' wmic commands **(Task 3)**
3. Use KAPE for incident response's evidence extraction and parsing **(Task 5)**

1. USE AUTOPSY'S PLASO AND TIMELINE FEATURE **(TASK 1)**

- Download NSRL hashset
  - https://sourceforge.net/projects/autopsy/files/NSRL/
  - Download the latest "computer-Autopsy".zip file and extract
  - Import the extracted contents in tools > options > Hash Sets > Import Hash Set

1. USE AUTOPSY'S PLASO AND TIMELINE FEATURE **(TASK 1)**

- Select ingest modules (at least):
  - Recent activities
  - Hash lookup with imported NSRL dataset
  - Picture analyzer
  - Any other modules that you need (file type identification, etc.)
- Plaso events **are not shown in the tree viewer**
  - Use Autopsy's timeline under Tools > Timeline
- https://www.sleuthkit.org/autopsy/timeline.php

2. RUN VARIOUS WINDOWS’ WMIC COMMANDS **(TASK 3)**

- WMI – Windows Management Instrumentation
- WMIC – WMI Command Line
- Powerful local & remote system management infrastructure
- Can be used to:
  - Obtained system information
    - Registry
    - File system
    - Etc.
  - Execute Commands
  - Subscribe to events.

2. RUN VARIOUS WINDOWS' WMIC COMMANDS **(TASK 3)**

- Operates more or less like a database would do
  - Offers you large and varied information useful for monitoring Windows based systems
- For the purpose of today's lab, only query machine information

2. RUN VARIOUS WINDOWS' WMIC COMMANDS **(TASK 3)**

- Get number of CPU cores
  - wmic cpu get numberofcores
- Get make/model, vendor of your PC
  - wmic csproduct get name,vendor
- Get product id of system
  - wmic os get serialnumber
  - systeminfo
- Get which user is logged on
  - wmic computersystem get username

2. RUN VARIOUS WINDOWS' WMIC COMMANDS **(TASK 3)**

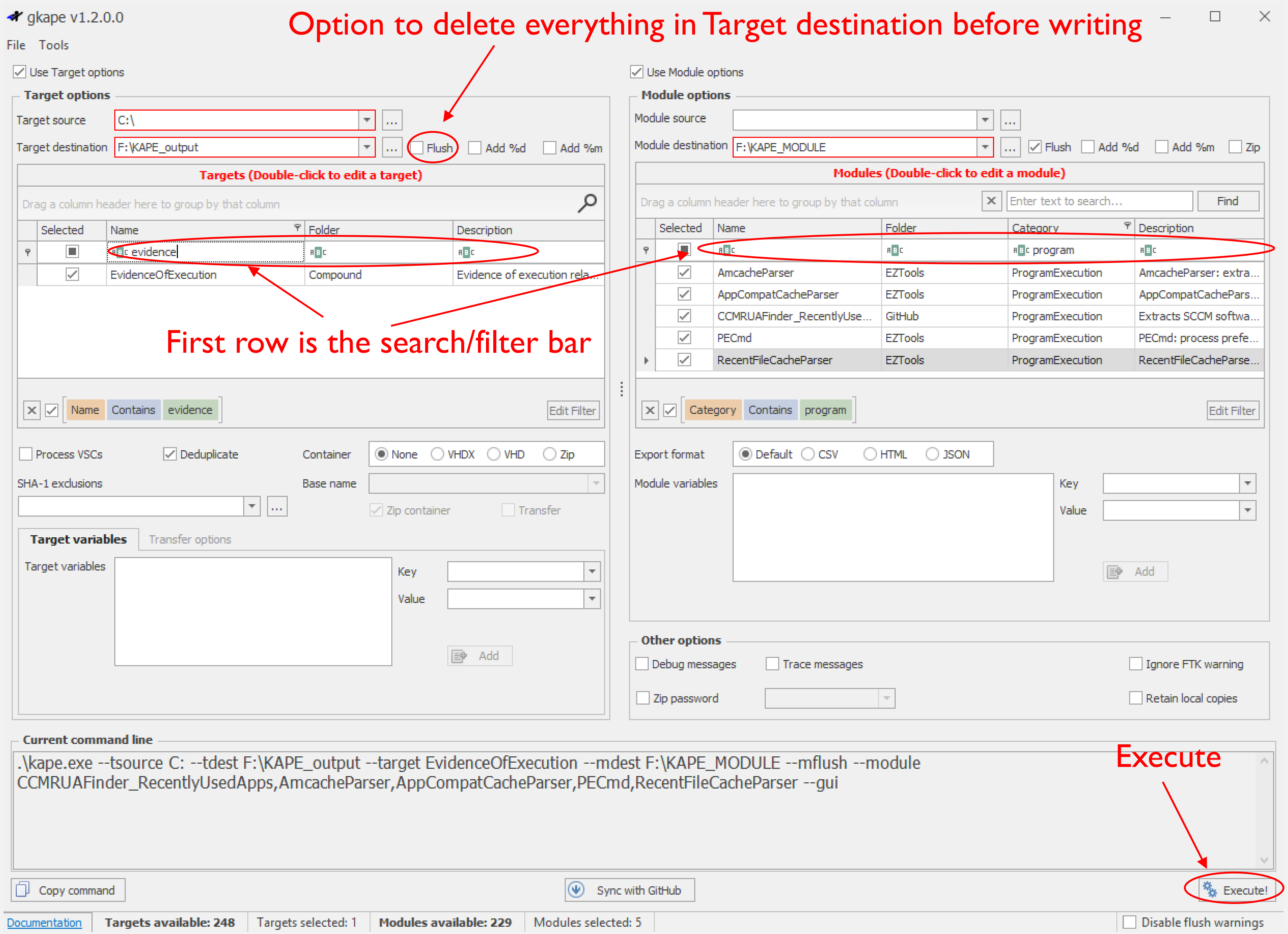
- https://www.sans.org/blog/wmic-for-incident-response/
- https://resources.infosecinstitute.com/topic/commandline-malware-and-forensics/

2. RUN VARIOUS WINDOWS' WMIC COMMANDS **(TASK 3)**

- All these are, command-line based monitoring
- Optional Task 4 introduces some GUI based monitoring tools
  - Procmon
  - Process Explorer
  - Autoruns
  - Regshot
- CS4238 also uses the above tools for malware analysis!

3. USE KAPE FOR INCIDENT RESPONSE'S EVIDENCE EXTRACTION AND PARSING **(TASK 5)**

- https://drive.google.com/file/d/1szDSh3fr6oXMpb63TX3fi63zs4BZWzdH/view?usp=sharing
- If you want to **use a disk image as a target source**, must **mount** it first
  - KAPE doesn't recommend using FTK
  - Use Arsenal Image Mounter
  - For demo, we will use 'C' drive



gkape v1.2.0.0
File
Tools
Targets (Double-click to edit a target)
Modules (Double-click to edit a module)
Drag a column header here to group by that column
Enter text to search...
Find
Edit Filter
Add
Copy command
Sync with GitHub
Execute!
Documentation

Option to delete everything in Target destination before writing

First row is the search/filter bar

Execute

☑ Use Target options

Target options

Target source: C:\

Target destination: F:\KAPE_output   □ Flush   □ Add %d   □ Add %m

Selected	Name	Folder	Description
■	evidence		
☑	EvidenceOfExecution	Compound	Evidence of execution rela...

☒ ☑ Name Contains evidence

□ Process VSCs   ☑ Deduplicate   Container: ● None ○ VHDX ○ VHD ○ Zip

SHA-1 exclusions   Base name

☑ Zip container   □ Transfer

Target variables | Transfer options

Target variables   Key   Value

☑ Use Module options

Module options

Module source:

Module destination: F:\KAPE_MODULE   ☑ Flush   □ Add %d   □ Add %m   □ Zip

Selected	Name	Folder	Category	Description
■			program	
☑	AmcacheParser	EZTools	ProgramExecution	AmcacheParser: extra...
☑	AppCompatCacheParser	EZTools	ProgramExecution	AppCompatCachePars...
☑	CCMRUAFinder_RecentlyUse...	GitHub	ProgramExecution	Extracts SCCM softwa...
☑	PECmd	EZTools	ProgramExecution	PECmd: process prefe...
☑	RecentFileCacheParser	EZTools	ProgramExecution	RecentFileCacheParse...

☒ ☑ Category Contains program

Export format: ● Default ○ CSV ○ HTML ○ JSON

Module variables   Key   Value

Other options

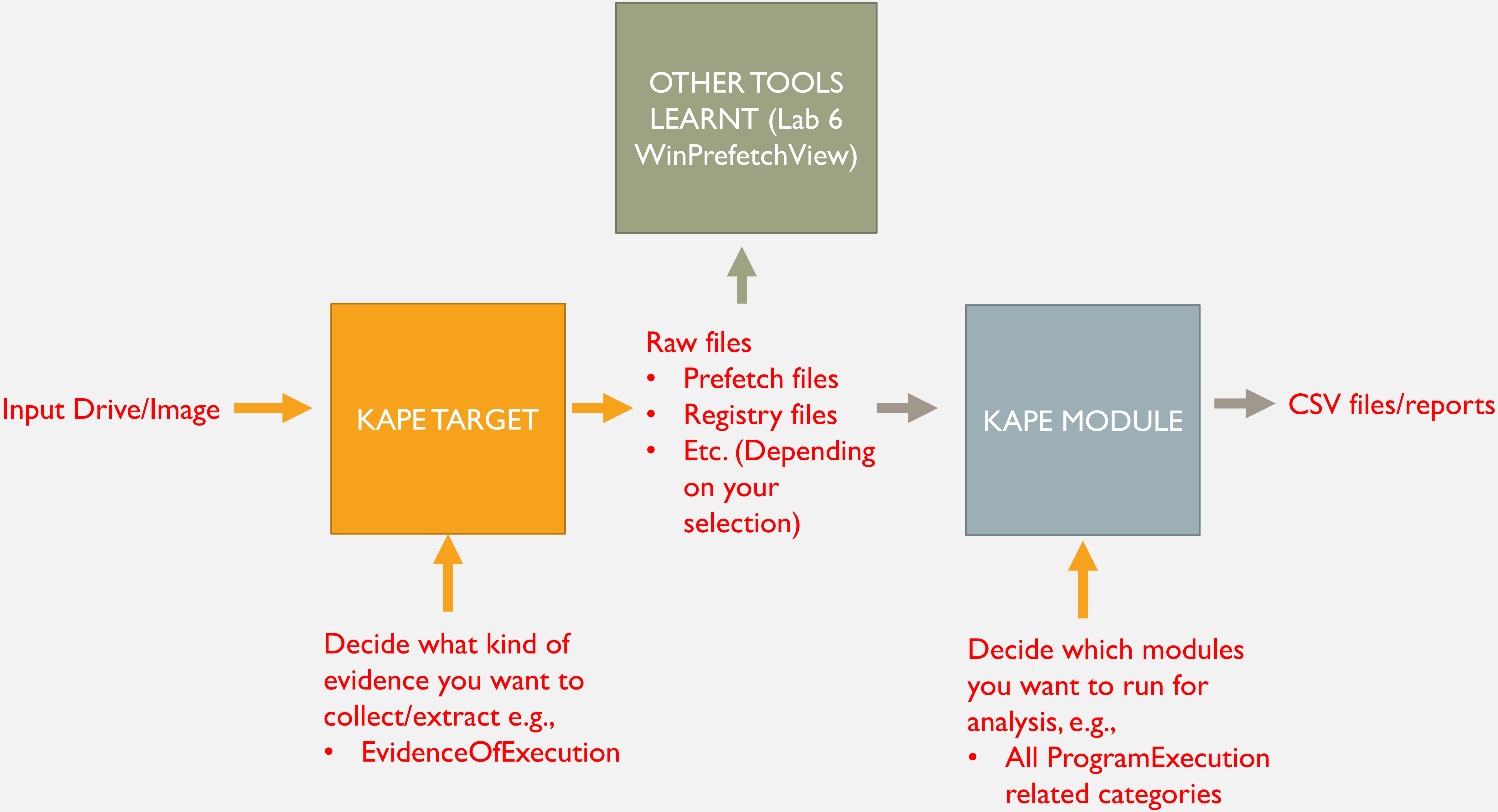
□ Debug messages   □ Trace messages   □ Ignore FTK warning

□ Zip password   □ Retain local copies

Current command line

```
.\kape.exe --tsource C: --tdest F:\KAPE_output --target EvidenceOfExecution --mdest F:\KAPE_MODULE --mflush --module
CCMRUAFinder_RecentlyUsedApps,AmcacheParser,AppCompatCacheParser,PECmd,RecentFileCacheParser --gui
```

Targets available: 248   Targets selected: 1   **Modules available: 229**   Modules selected: 5   □ Disable flush warnings



Input Drive/Image

KAPE TARGET

Decide what kind of evidence you want to collect/extract e.g.,

- EvidenceOfExecution

Raw files

- Prefetch files
- Registry files
- Etc. (Depending on your selection)

OTHER TOOLS LEARNT (Lab 6 WinPrefetchView)

KAPE MODULE

Decide which modules you want to run for analysis, e.g.,

- All ProgramExecution related categories

CSV files/reports

QUESTIONS?

TIMELINE?

- Confession :p : Back when I took this module I didn’t really use the plaso tool
- But it is a really good tool, can boast in your CV as well!

-
  ```
  fls –I <image_type> –f <file_system> –o <offset> –m / <image> | mactime –b
  ```