HackerFrogs Afterschool Memory File Forensics Part 1

Class:
Digital Forensics

Workshop Number:
AS-FOR-07

Document Version:
1.75

Special Requirements:
- Registered account at tryhackme.com

Welcome to HackerFrogs Afterschool!

This workshop is the seventh class for digital forensics.

In the last workshop, we learned about the following digital forensics concepts:

Autopsy Forensics Software

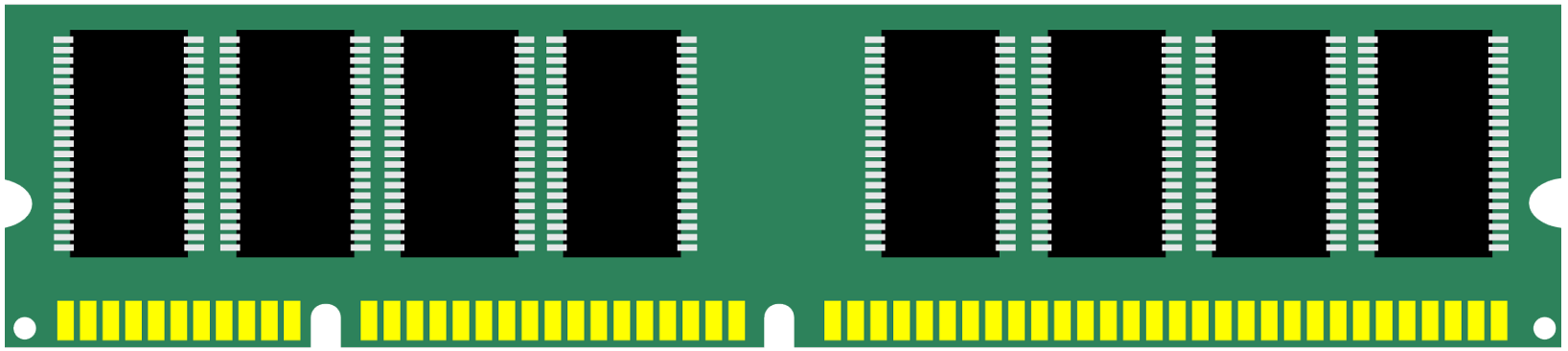
Autopsy is the GUI Implementation of the Sleuthkit, and it allows users to view the contents of disk image files in a much more intuitive manner

This Workshop's Topics

- Device Memory Forensics with Volatility

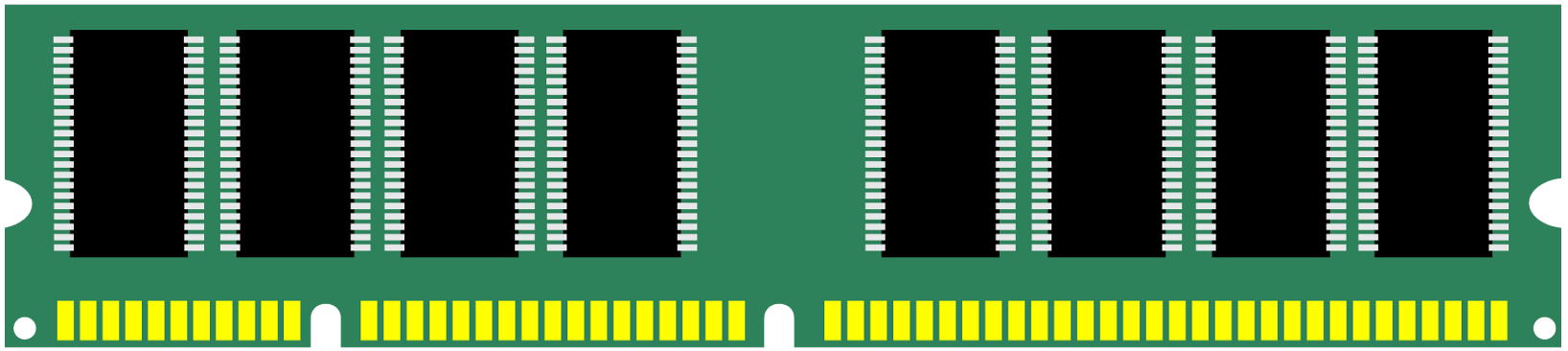
- Advent of Cyber 2022: Day 11 Challenge (Pt 1)

What is Memory Forensics?



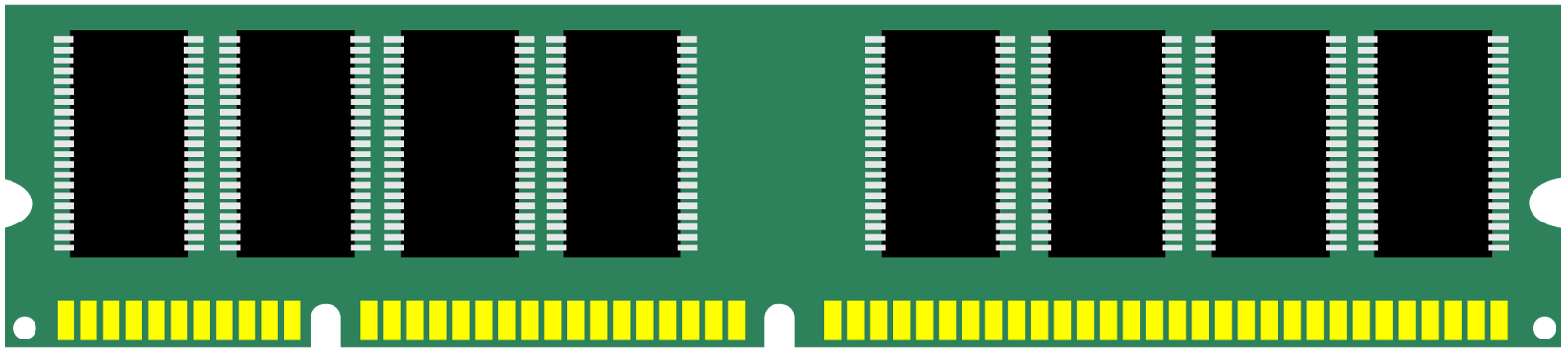
Digital memory forensics is the examination of data in computer memory

Advantages of Memory Forensics



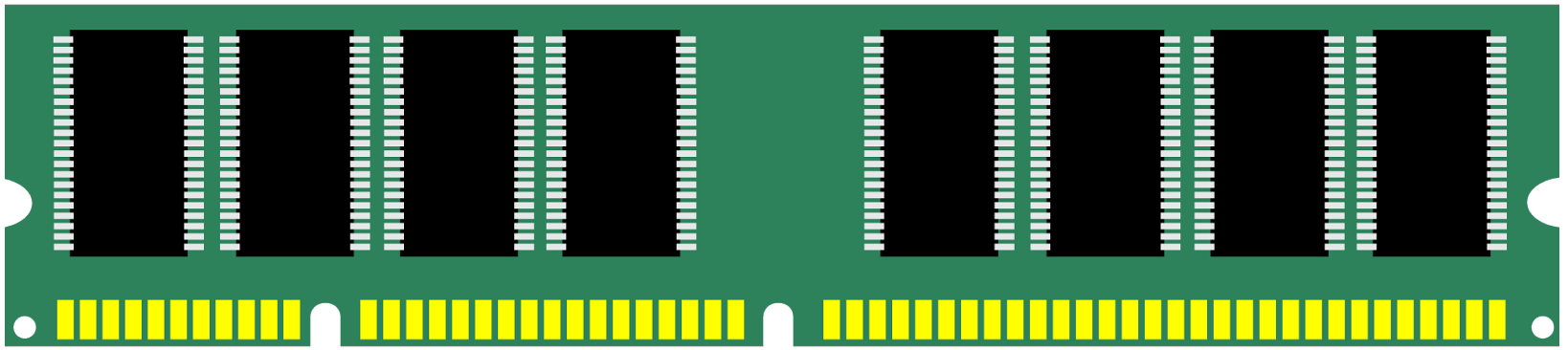
Volatile memory can contain the decrypted versions of encrypted files, passwords and encryption keys

Advantages of Memory Forensics



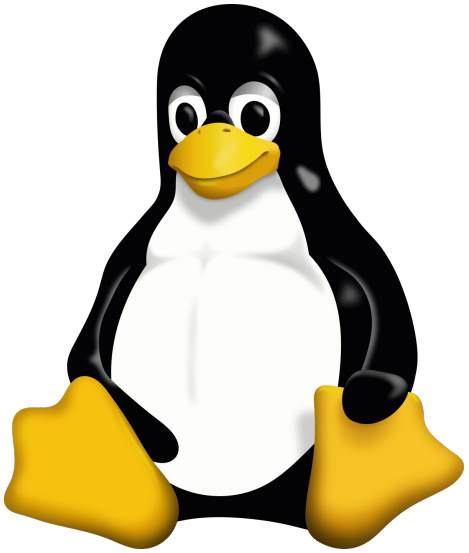
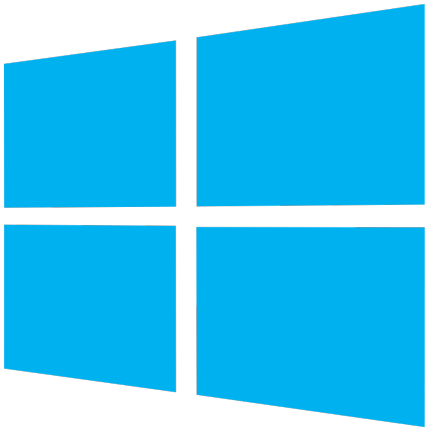
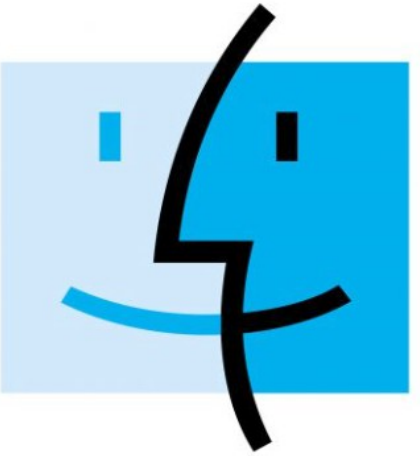
Volatile memory also contains data about all processes running on the system, which can include malicious processes, i.e., malware

Advantages of Memory Forensics



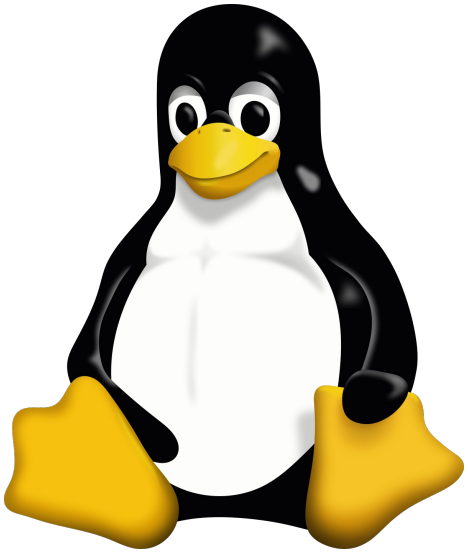
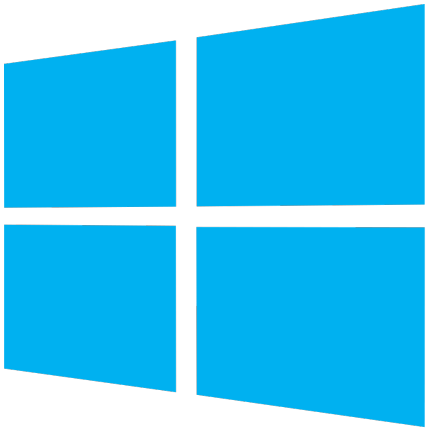
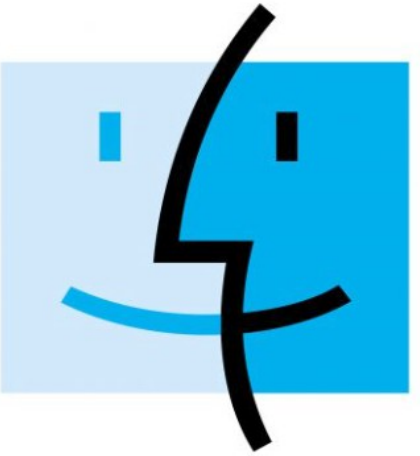
Memory forensics can also provide insight to process creation and termination times, and network connections, which can help investigators track the sequence of events in an incident

Memory Forensics File Creation

The software used for the creation of memory forensics files differs depending on the OS of the system to be dumped

Memory Forensics File Creation

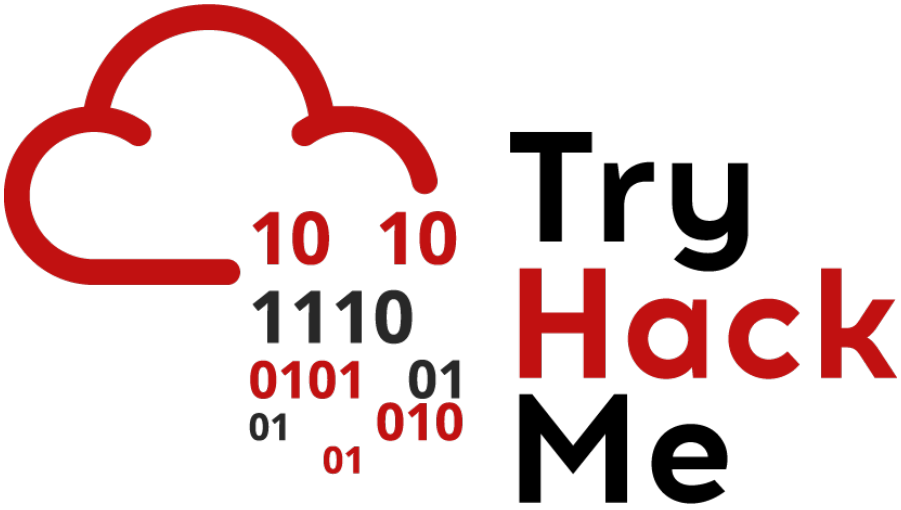
Some popular options include LiME (Linux), Winpmem (Windows), and OSXPmem (MacOS)

Volatility Memory Forensics Software

Volatility is a powerful, free tool used for memory forensics, written in Python.

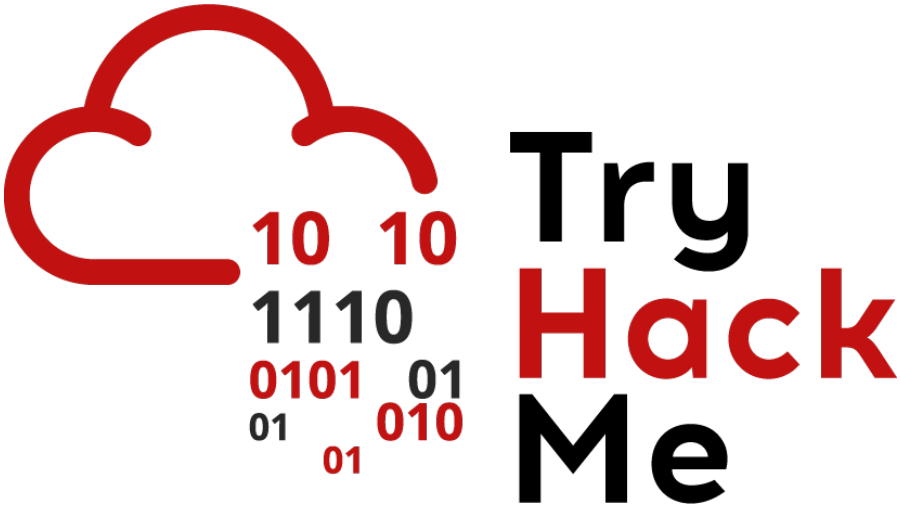
TryHackMe: Advent Modules

TryHackMe runs an event every December which covers a lot of different cybersecurity topics, including digital memory forensics.



TryHackMe: Advent Modules

We'll be looking at a TryHackMe Advent module to learn about memory forensics.

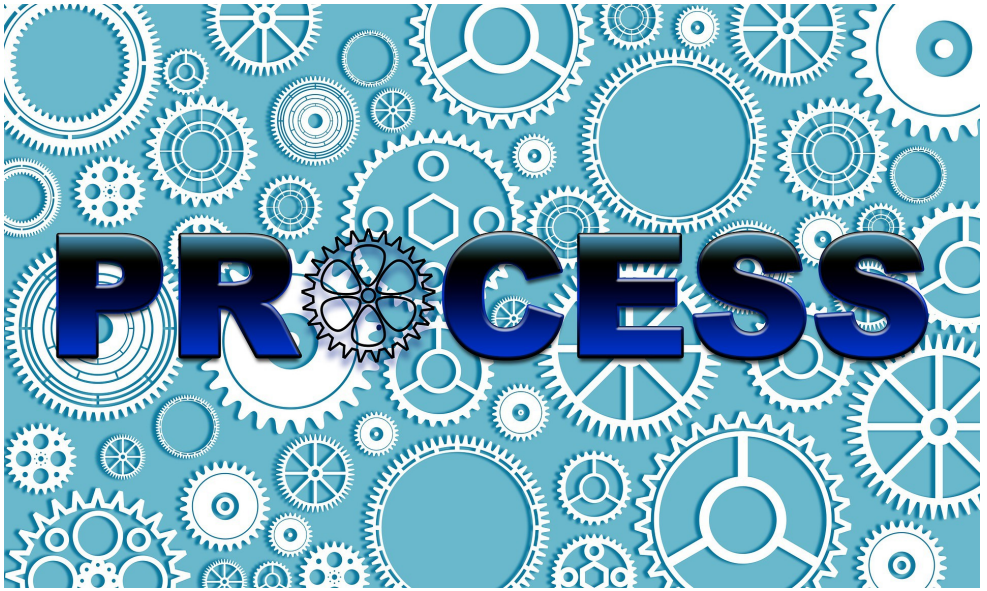


TryHackMe: Advent 2022 – Task 16

The module we'll be looking at is the Advent of Cyber 2022 module:

https://tryhackme.com/r/room/adventofcyber4

System Processes



One of the biggest advantages of memory forensics over other forensic methods is the ability to examine system process information. But what are processes?

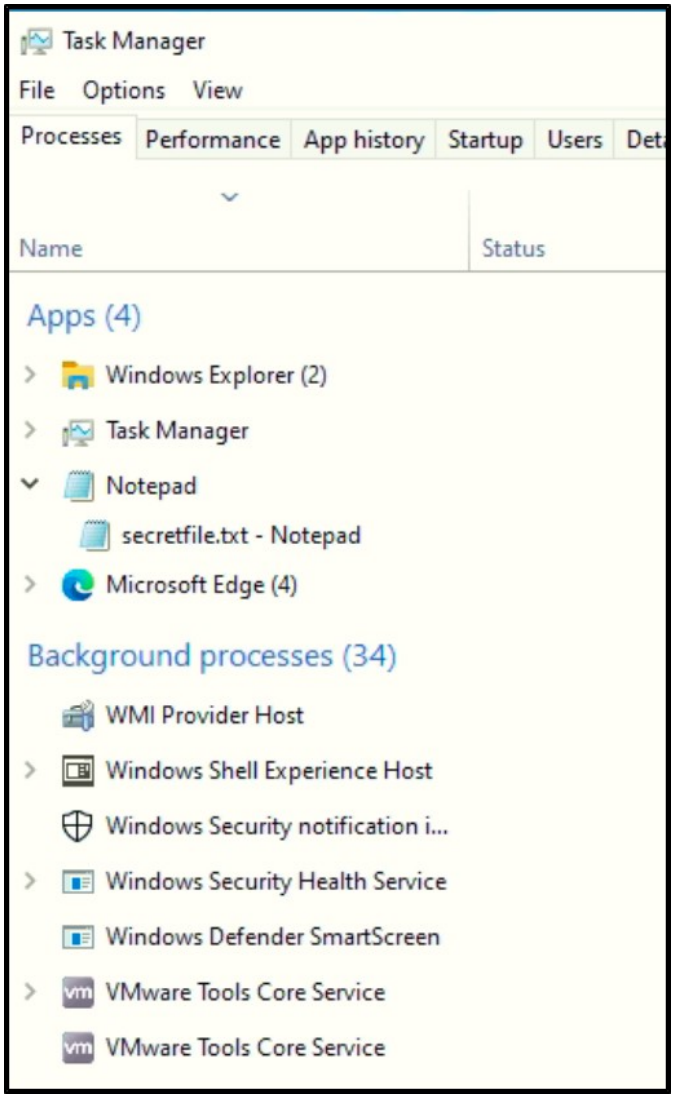
System Processes

```
PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
1814  0.0  0.0   8016  4608 pts/1    S+   12:57   0:00 nano test.txt
```

Put simply, processes are programs running on the system. E.g., if you run a text editor program, that program becomes a process until the program is closed.

System Processes

On Windows OS, the Task Manger app lets us observe which processes are running on the system

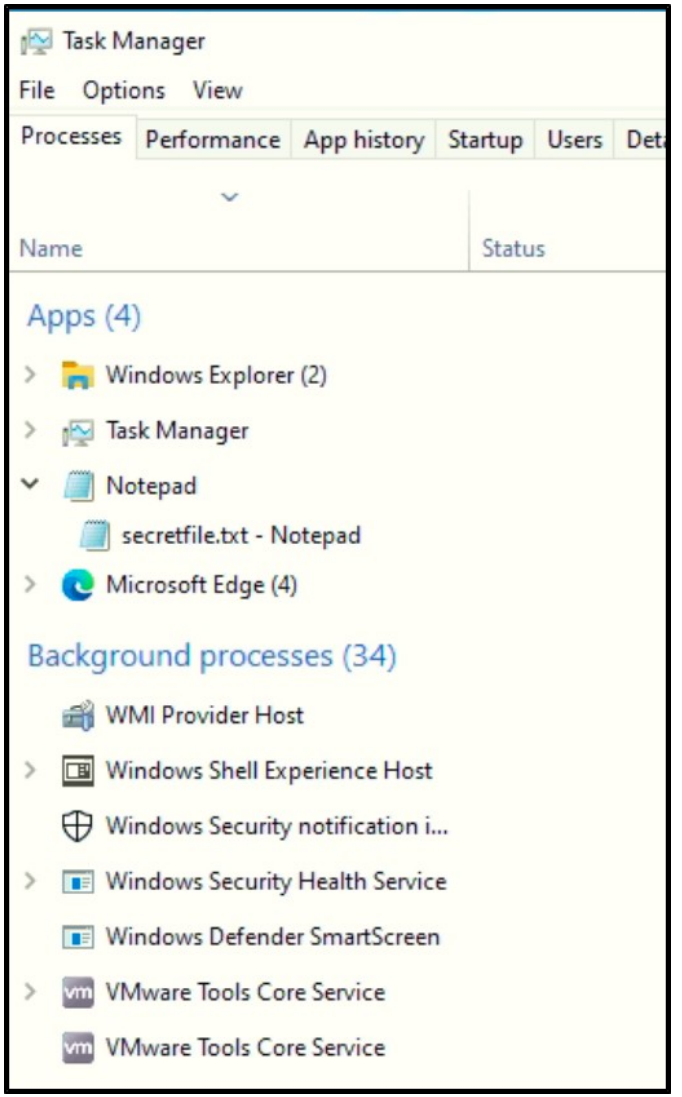


System Processes

Processes are divided into two categories

User processes, which are programs started by users

Background processes, which are run and managed by the OS



Volatility Memory Forensics Software

Volatility is a powerful, free tool used for memory forensics, written in Python

There are two major versions of Volatility currently in use, Volatility 2 and Volatility 3

Version 2 versus Version 3

This workshop uses Volatility 3, but keep in mind that Volatility 2 is still used regularly, since there are many plugins and modules exclusive to Volatility 2

Version 2 versus Version 3

As a consequence, we will need to be careful when looking up Volatility commands

As a rule of thumb, all Volatility 2 commands include the `--profile` argument

And Volatility 3 commands often include an <OS_type>.<module> argument, such as `windows.pslist`

Version 2 versus Version 3

Example Volatility 2 command

```
vol.py -f linux.mem --profile="LinuxUbuntu_5_4_0-163-generic_profilex64" linux_pslist
```

Example Volatility 3 command

```
vol.py -f workstation.vmem windows.pslist
```

Save Time With Output Redirection

Some of the Volatility commands take a long time to complete, it's a good idea to output each of our commands to a file so we can look at those outputs later

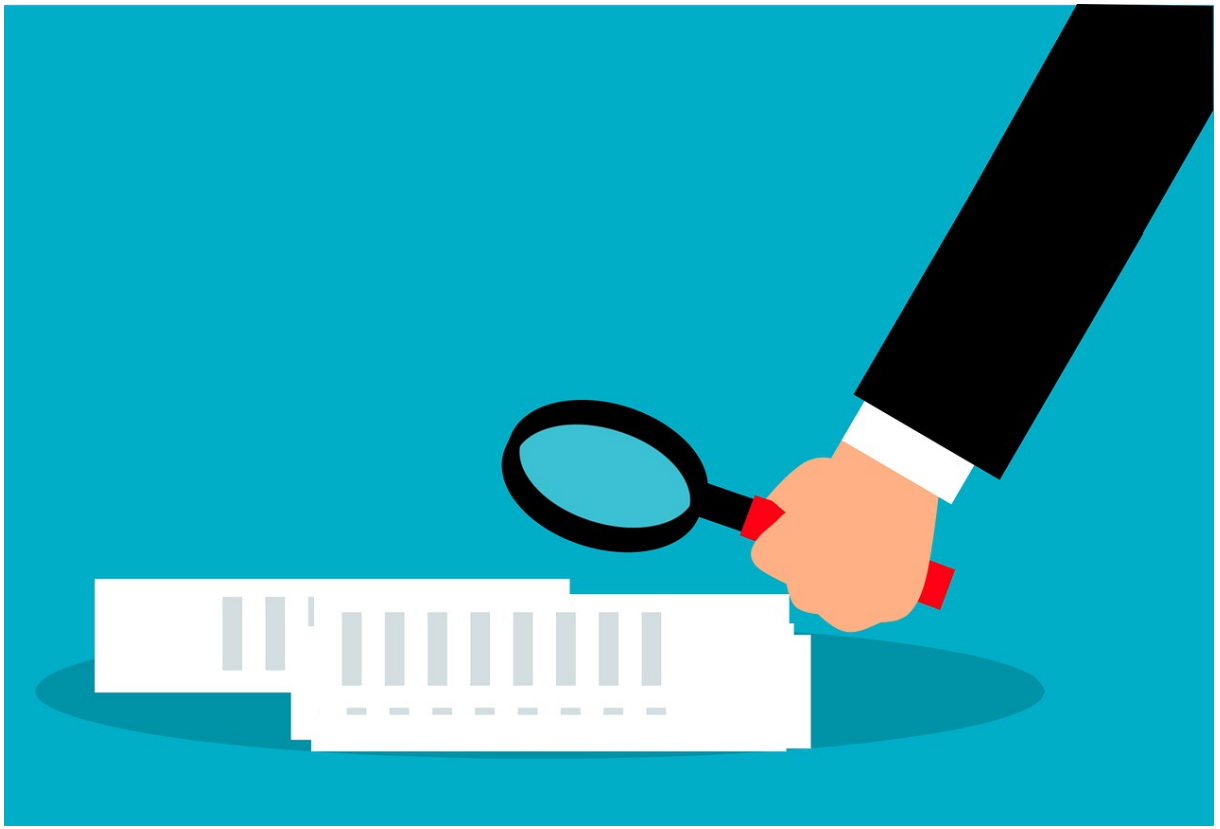
```
python Vol.py windows.someModule > someModule.txt
```

Let's Answer the THM Questions!

If we get stuck, we can always look at a cheatsheet!

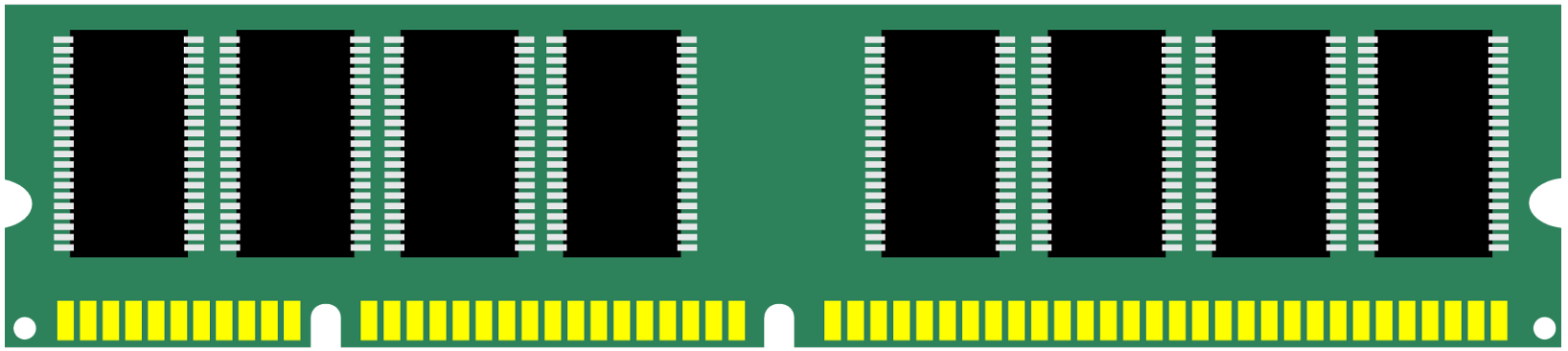
https://blog.onfvp.com/post/volatility-cheatsheet/

Summary



Let's review the digital forensics concepts we learned in this workshop:

Memory Forensics



Digital memory forensics is the examination of data in computer memory. It can give forensics investigators a view into processes running on the system

Volatility Memory Forensics Software

Volatility is a powerful, free tool used for memory forensics, written in Python.

There's two versions currently used, Vol 2 and Vol3

What's Next?

In the next HackerFrogs Afterschool digital forensics workshop, we'll come back to Volatility and discover some functions and methods to discover memory file secrets!

Extra Credit

Looking for more study material on this workshop's topics?

See this video's description for links to supplemental documents and exercises!

Until Next Time, HackerFrogs!