HackerFrogs Afterschool Memory File Forensics Part 2

Class:
Digital Forensics

Workshop Number:
AS-FOR-08

Document Version:
1.75

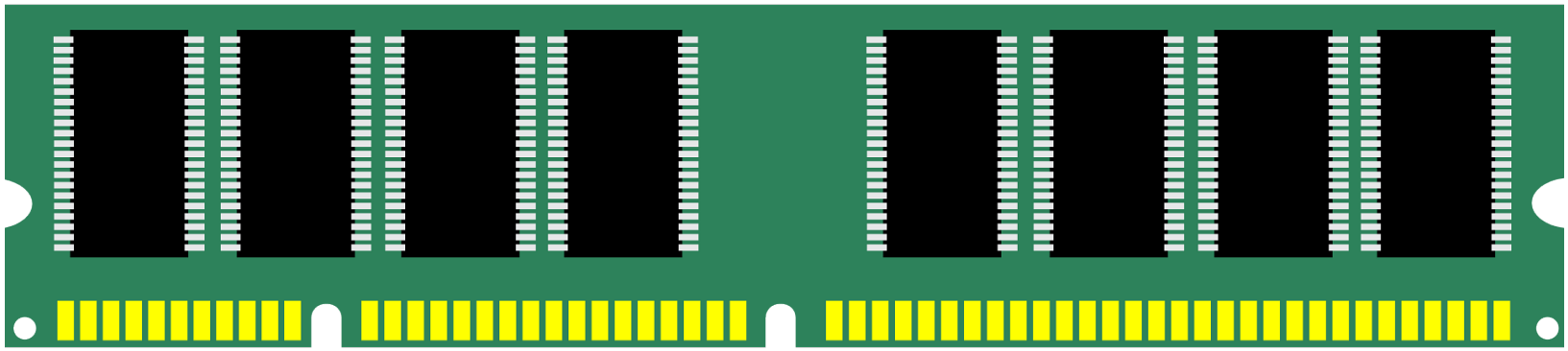
Special Requirements:
- Registered account at tryhackme.com

Welcome to HackerFrogs Afterschool!

This workshop is the eighth and final class for digital forensics.

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

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

This Workshop's Topics

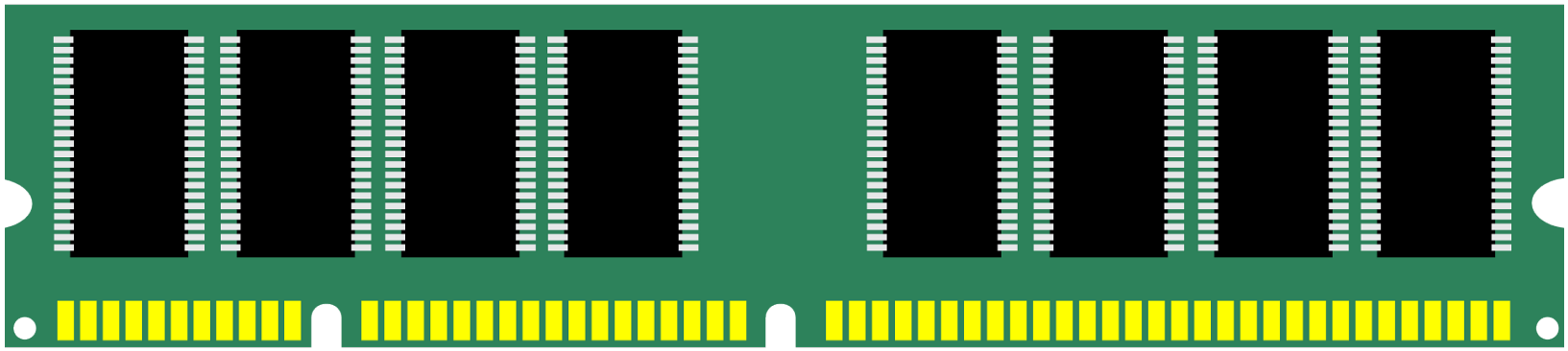
- Device Memory Forensics with Volatility
- Advent of Cyber 2022: Day 11 Challenge (Pt 2)

TryHackMe: Advent 2022 – Task 16

Let's go back to the Advent of Cyber 2022 module to learn more Volatility functions:

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

Let's Answer Some Different Questions Today!



We can find them at the following link:

https://github.com/theshyhat/DC604/blob/main/volatility_workshop/questions.md

What process created the mysterygift.exe file?

```
** 4064 4040     explorer.exe     0xc0091
09:44:05.000000          N/A
*** 5888          4064     cmd.exe 0xc0091
09:59:38.000000          N/A
**** 2040         5888     mysterygift.ex
2-11-23 10:15:19.000000          N/A
```

python 3 vol.py -f workstation.vmem windows.pstree

According to the memory dump command-line history, what suspicious file is opened by notepad.exe?

```
python3 vol.py -f workstation.vmem windows.cmdline.CmdLine | grep notepad
tem32\NOTEPAD.EXE" C:\Users\CMNatic\Desktop\secretfile.txt
```

python 3 vol.py -f workstation.vmem windows.cmdline.CmdLine | grep notepad

According to the memory dump file's networking information, what program is associated with the local and foreign port 80?

```
TCPv4   0.0.0.0 80      0.0.0.0 0       LISTENING       3108    python.exe
TCPv6   ::      80      ::      0       LISTENING       3108    python.exe
```

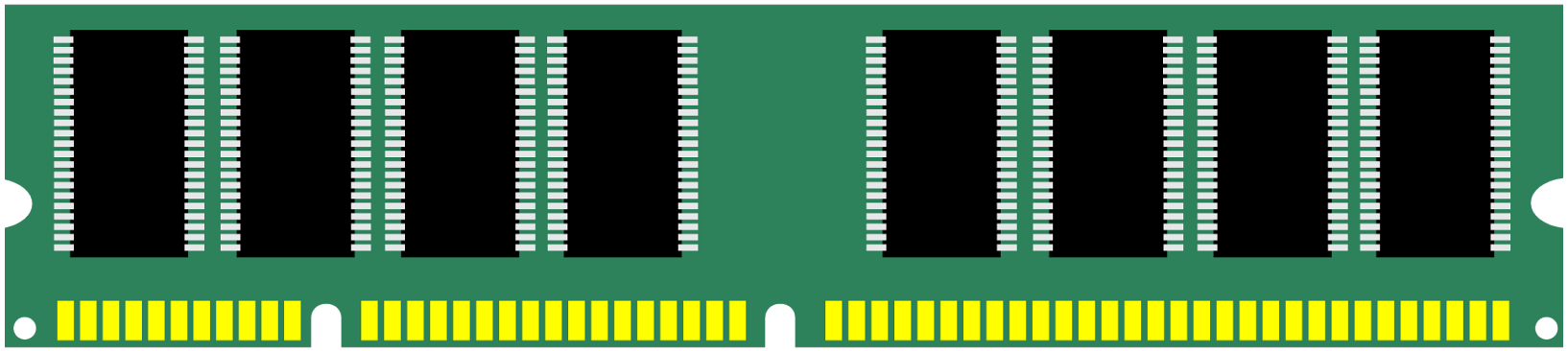
python3 vol.py -f workstation.vmem windows.netscan | grep 80

According to the Windows registry files, what is the name of the localhost?

```
(Default)          "mnmsrvc"          False
ComputerName       "DESKTOP-3SD2BNH"
```

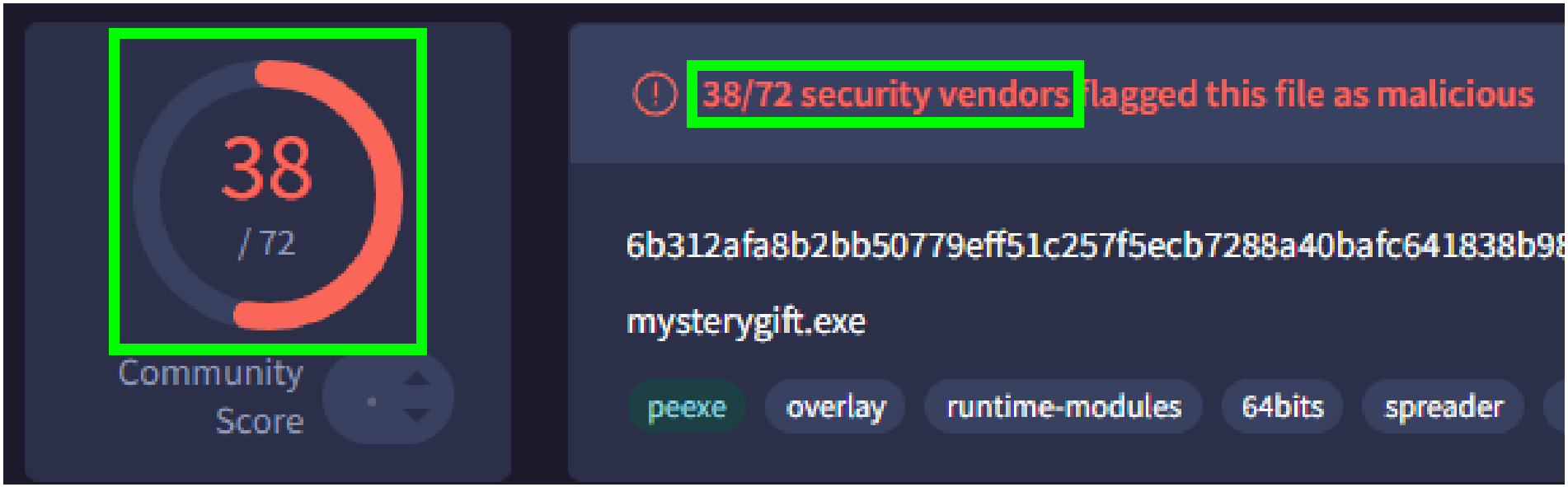
python3 vol.py -f workstation.vmem windows.registry.printkey --key "ControlSet001\\Control\\ComputerName\\ComputerName"

Let's Take Some Time to Answer the Advanced Questions – Part 2!



Let's take a bit of time answer the second set of advanced questions. We'll need to run md5sum on the mysterygift.exe file and submit it to VirusTotal to get the entry for the malware

How many security vendors flagged the file as malicious?



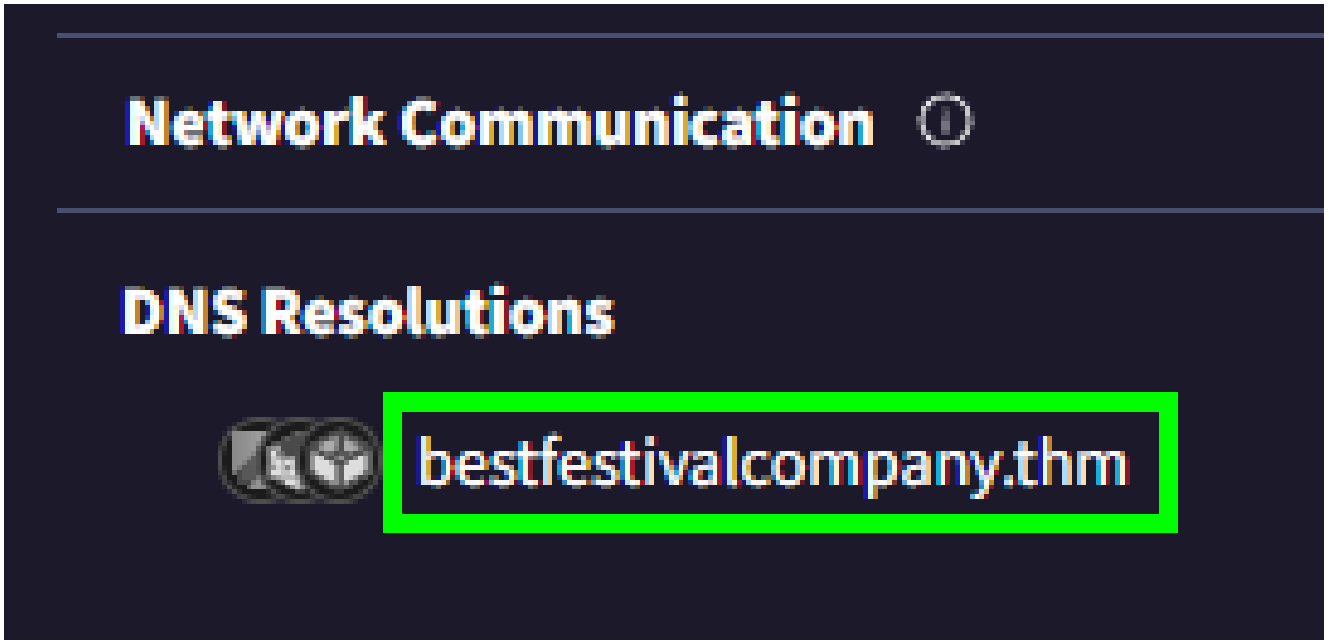
According to the file's history, what was the file creation time?

History

Creation Time	2022-11-04 13:23:22 UTC
First Submission	2022-12-11 18:49:35 UTC
Last Submission	2022-12-17 13:45:21 UTC
Last Analysis	2022-12-14 20:08:27 UTC

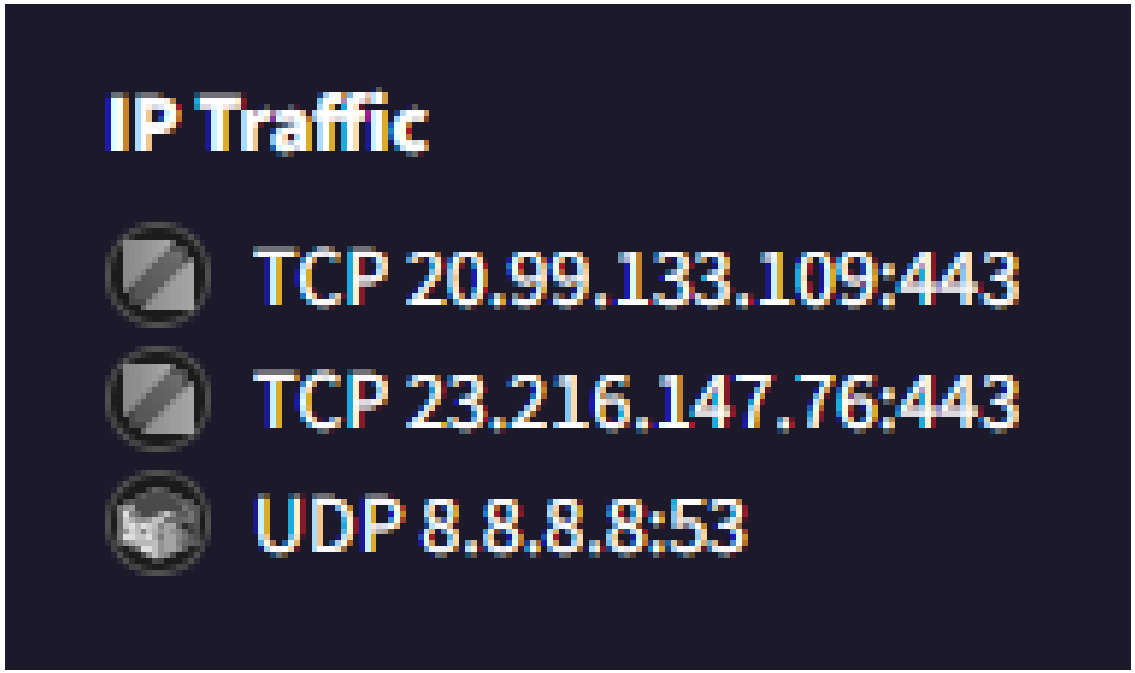
This can be found in the **DETAILS** tab

What domain name is associated with this file?



This can be found in the BEHAVIOR tab

What IP addresses are contacted by this file?



This is also found in the BEHAVIOR tab or RELATIONS tab

Aside from mysterygift.exe, what are the other two names of this file?

Names

mysterygift.exe

6b312afa8b2bb50779eff51c257f5ecb7288a40bafc641838b985d9798a1b3ce.sample

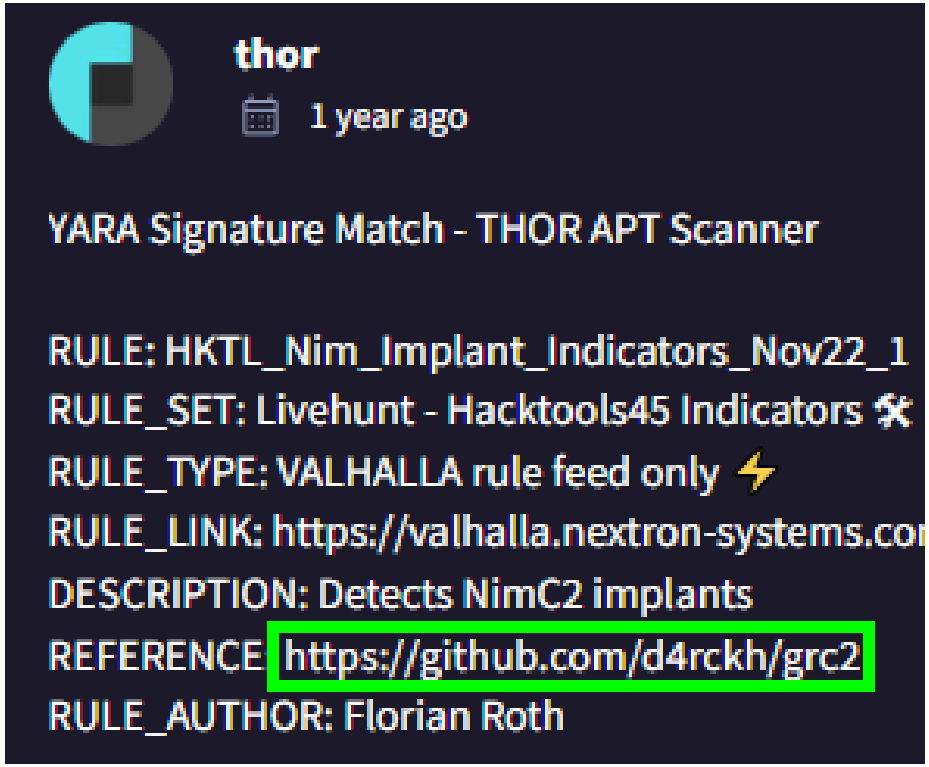
file.0xc00912e1f1f0.0xc009119ab9b0.ImageSectionObject.mysterygift.exe.img

This can be found in the DETAILS tab

Is this a signed file?

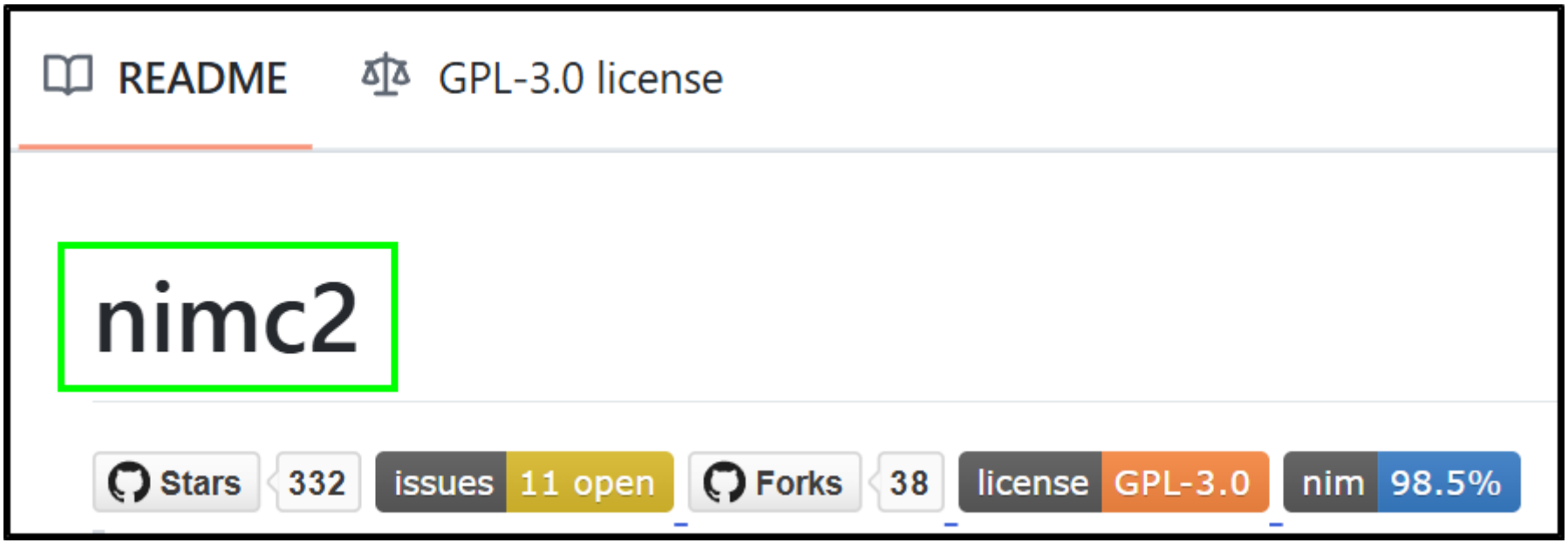
We can assume that this file is not signed, since it is malware

What Github repo (URL) is associated with this file?



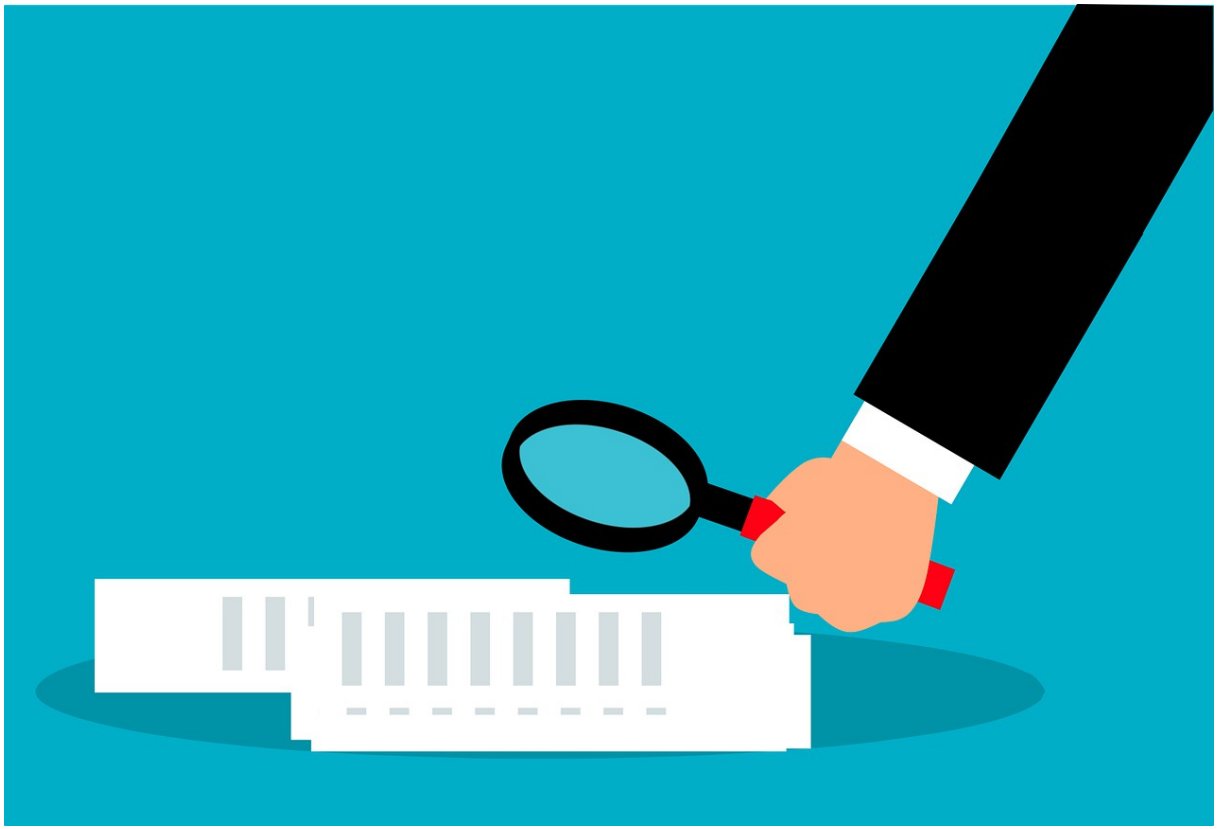
This can be found in the COMMUNITY tab

What is the name of this Github project?



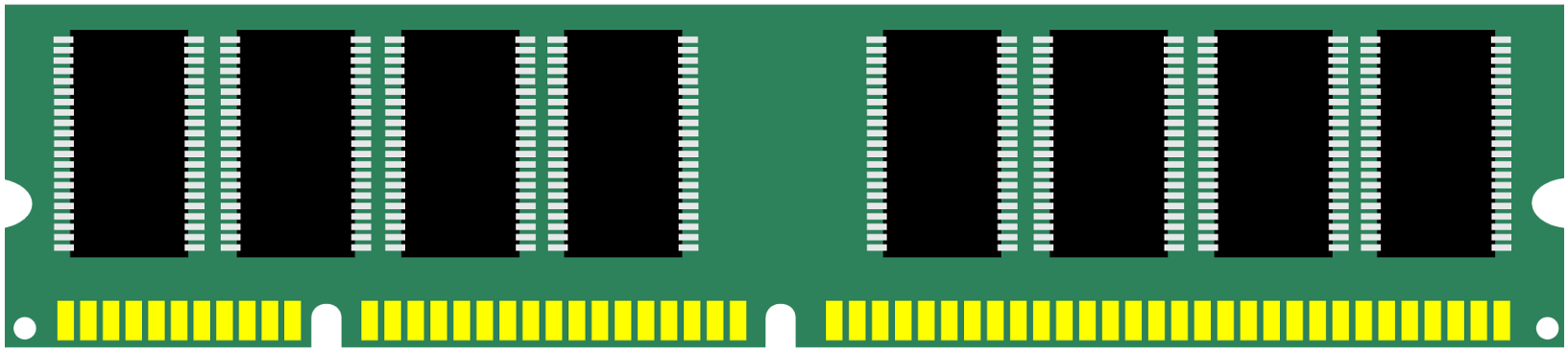
We find the name of the project on the Github page

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?

The digital forensics lessons are done, but in the next HackerFrogs Afterschool workshop, we'll start a new course: Cryptography!

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!