DC604 November Workshop
Memory Forensics /w TryHackMe

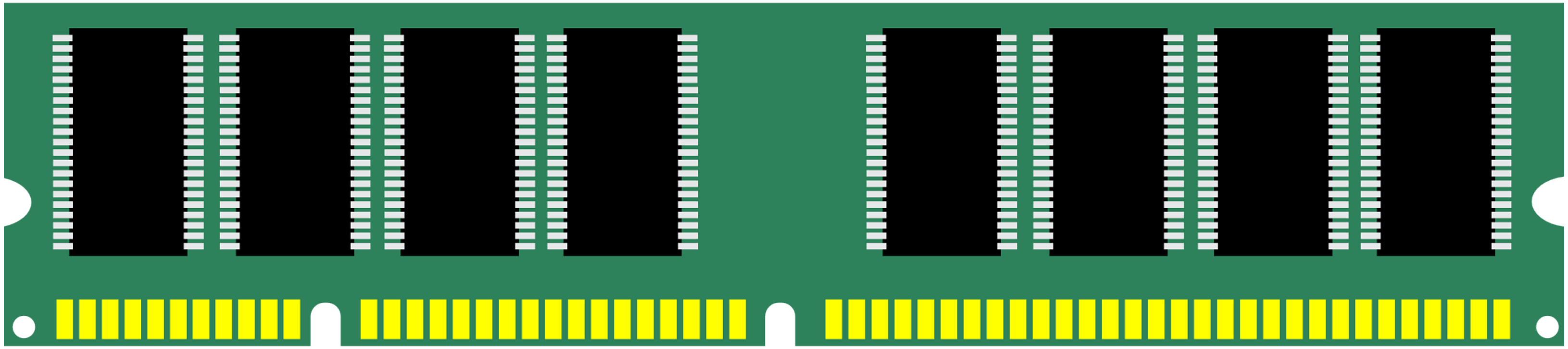
Subject:
Digital Forensics

Workshop ID:
DC604_NOV

Document Version:
1.0

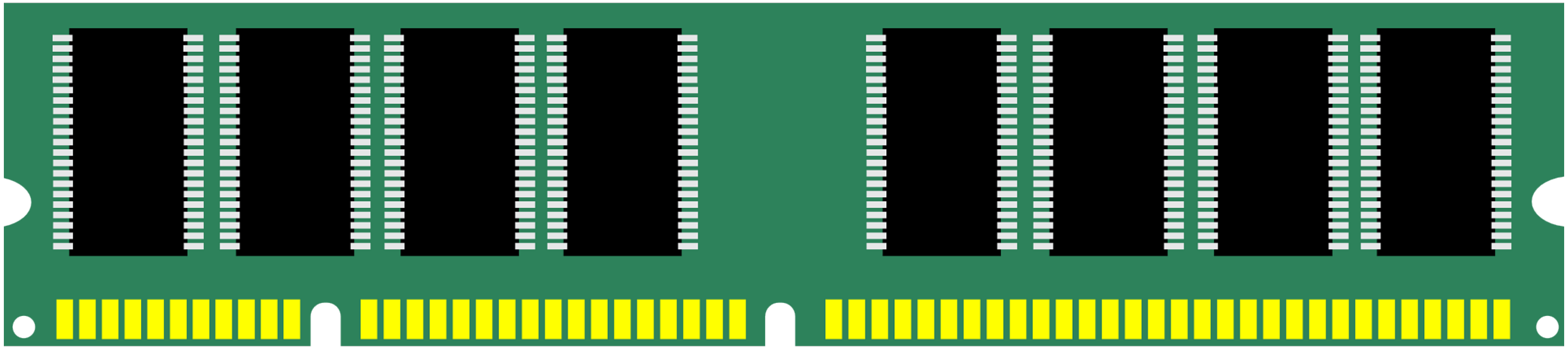
Special Requirements:
- Registered account at tryhackme.com

What is Memory Forensics?



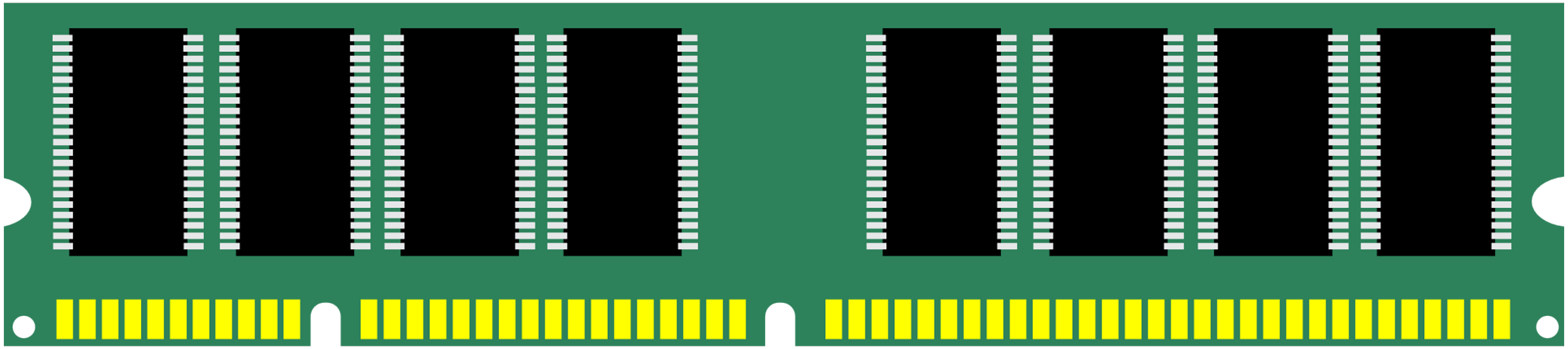
Digital memory forensics is the examination of data in computer memory

Advantages of Memory Forensics



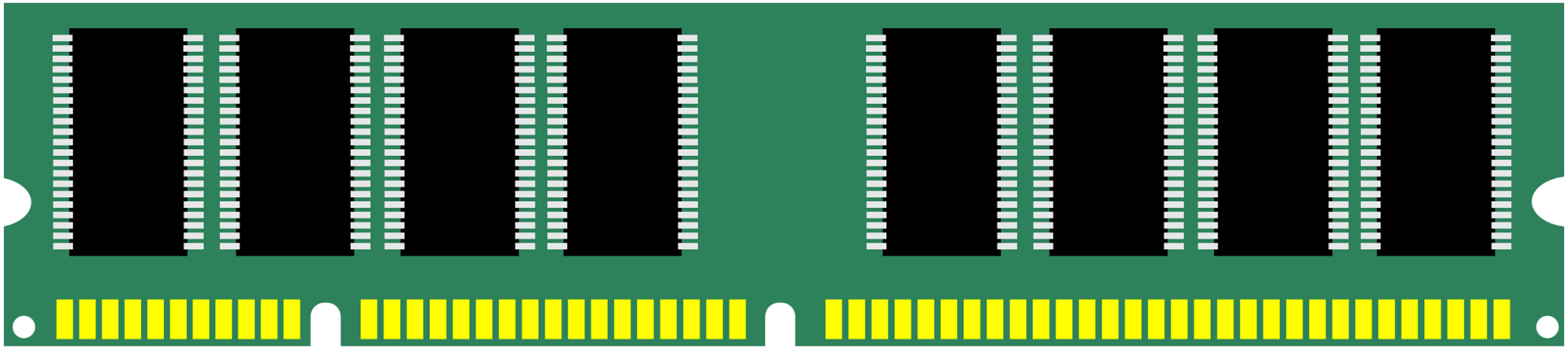
Volatile memory can contain the decrypted versions of encrypted files, passwords and encryption keys

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.

The Link with All the Links

All the links for this workshop can be found at this Github link:

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

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.

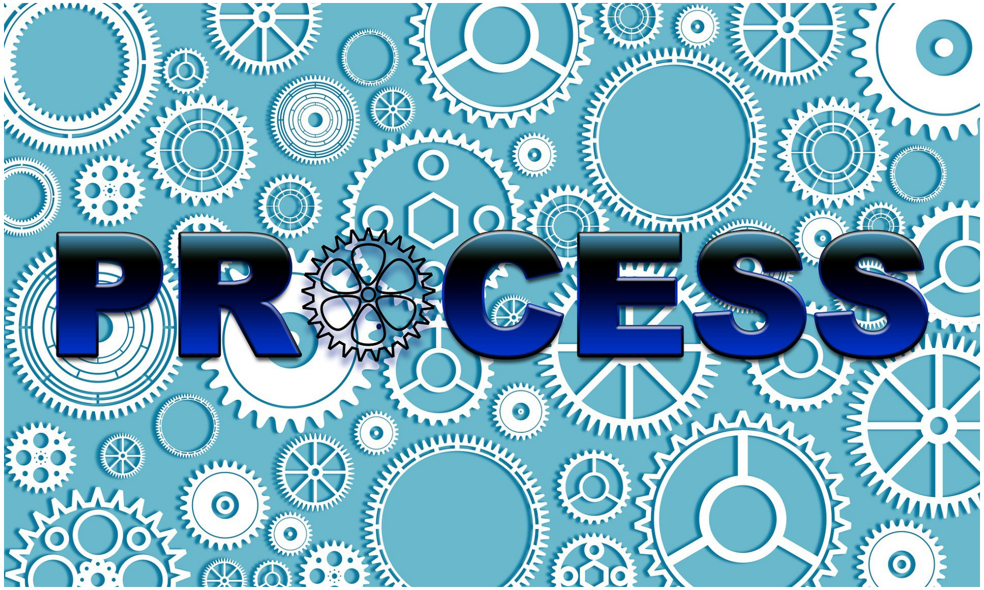
TryHackMe: Advent 2022 – Task 16

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

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

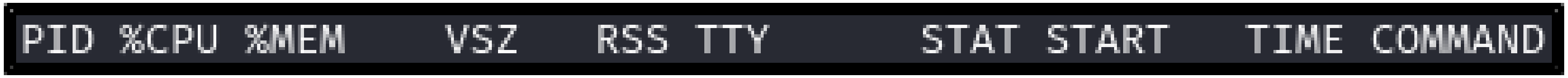
This link can found on the main.md page under section 1

System Processes

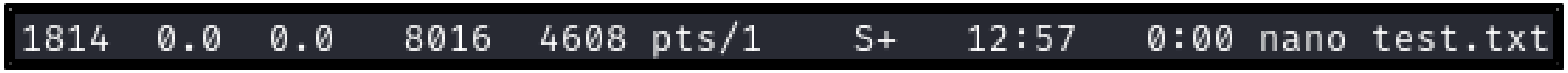


One of the biggest advantages of memory forensics over other forensic methods is the ability to examine system process information. But what are processes?

System Processes



```
PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
```

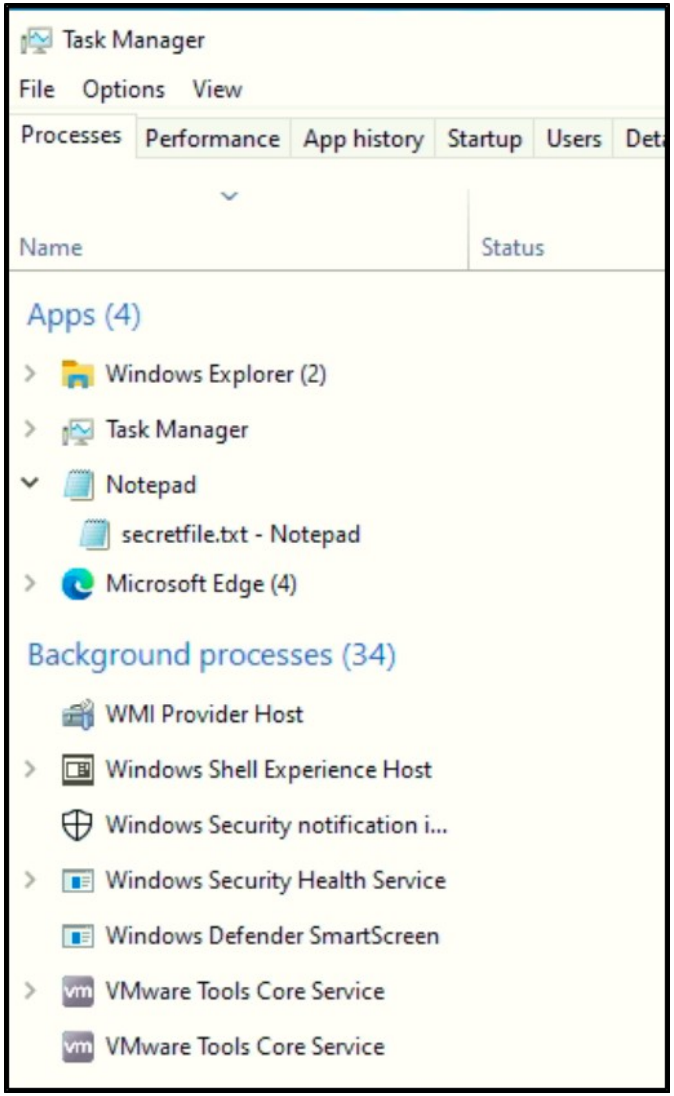


```
1814  0.0  0.0   8016  4608 pts/1    S+   12:57   0:00 nano test.txt
```

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



Task Manager

Apps (4)

- Windows Explorer (2)
- Task Manager
- Notepad
  - secretfile.txt - Notepad
- Microsoft Edge (4)

Background processes (34)

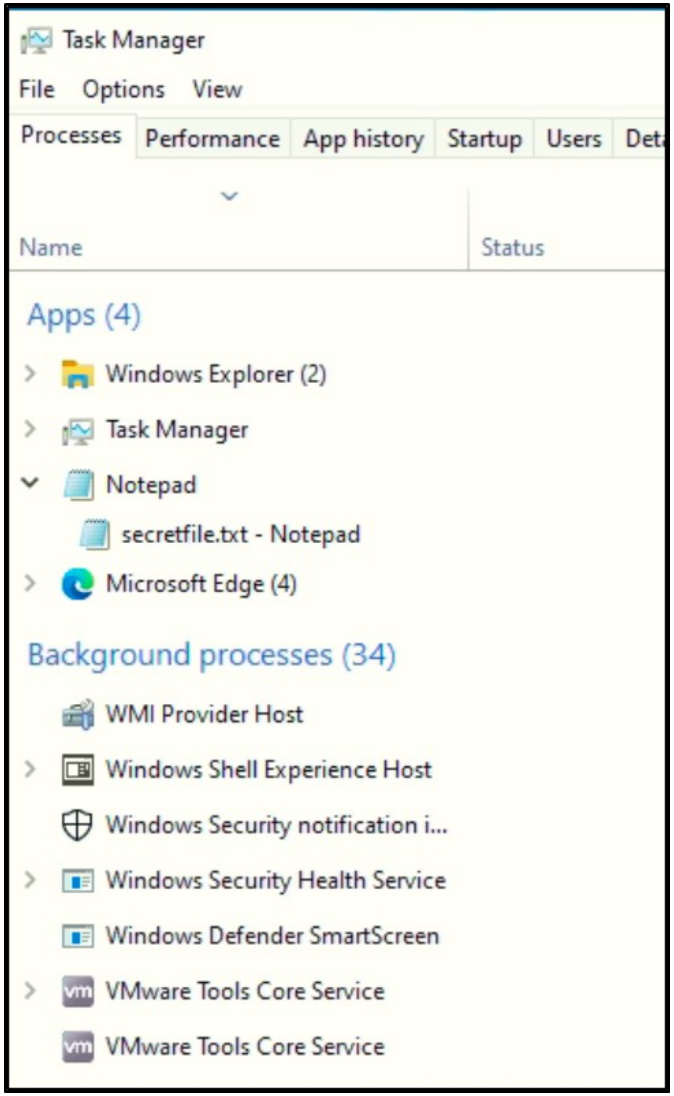
- WMI Provider Host
- Windows Shell Experience Host
- Windows Security notification i...
- Windows Security Health Service
- Windows Defender SmartScreen
- VMware Tools Core Service
- VMware Tools Core Service

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



Task Manager

File Options View

Processes Performance App history Startup Users Det

Name Status

Apps (4)

- Windows Explorer (2)
- Task Manager
- Notepad
  - secretfile.txt - Notepad
- Microsoft Edge (4)

Background processes (34)

- WMI Provider Host
- Windows Shell Experience Host
- Windows Security notification i...
- Windows Security Health Service
- Windows Defender SmartScreen
- VMware Tools Core Service
- VMware Tools Core Service

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!

Let's take a bit of time to play around with Volatility and answer the questions. The questions can be found in the main.md file under section 2

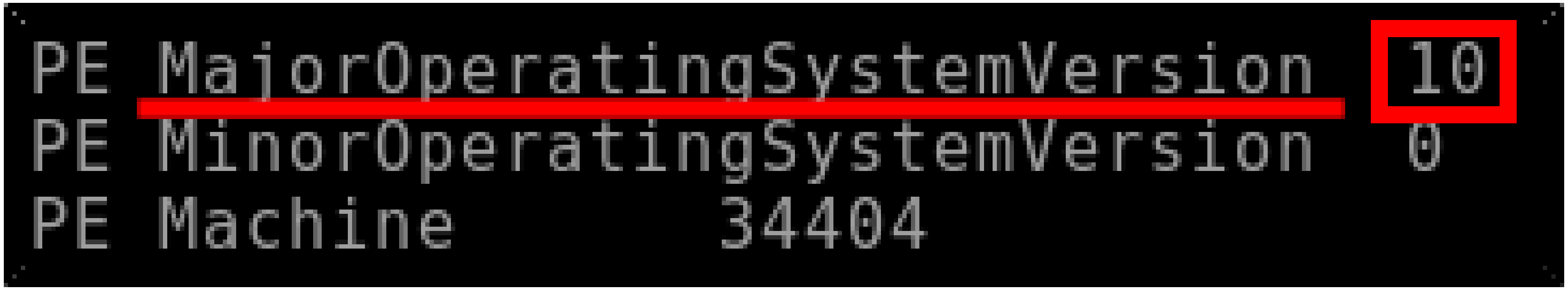
Before running any commands, we should move into the `volatility3` directory

We'll go over the answers together in about 15 minutes

Let's Go Over the THM Questions!

Don't forget to extend the time on your TryHackMe VM so it doesn't timeout

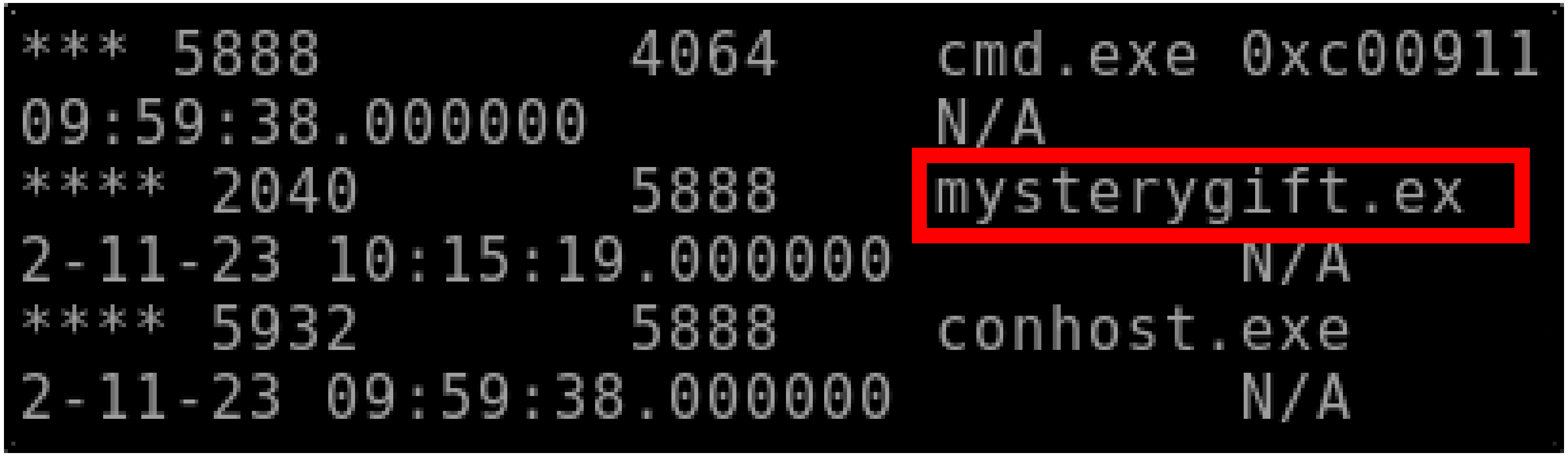
What is the Windows version number that the memory image captured?



```
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine       34404
```

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

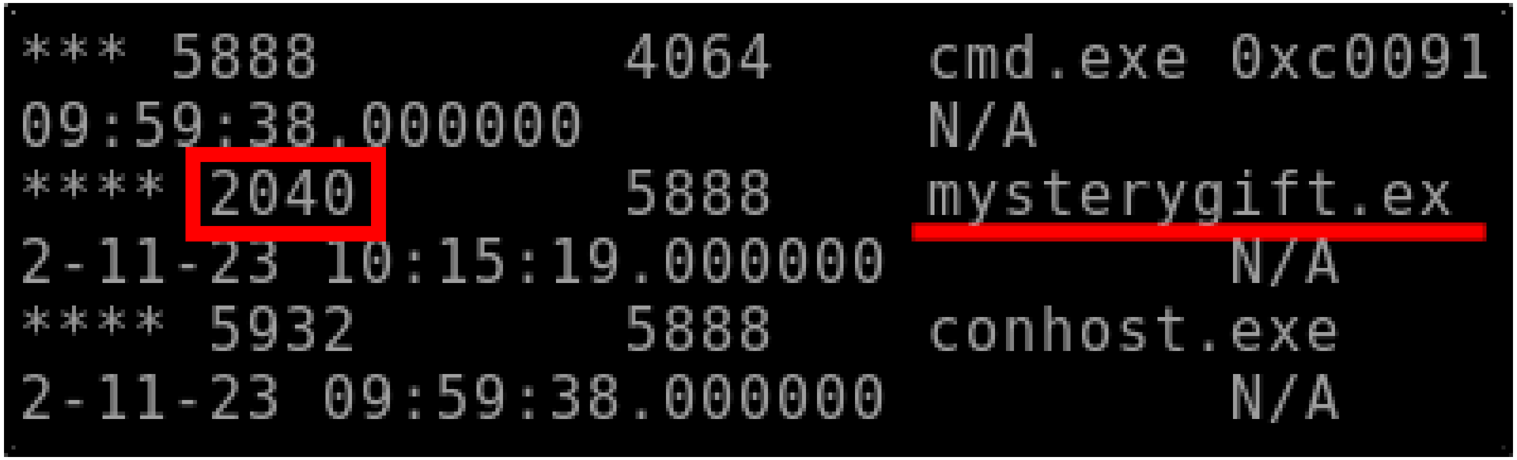
What is the name of the binary/gift that secret Santa left?



```
*** 5888        4064    cmd.exe 0xc00911
09:59:38.000000         N/A
**** 2040       5888    mysterygift.ex
2-11-23 10:15:19.000000         N/A
**** 5932       5888    conhost.exe
2-11-23 09:59:38.000000         N/A
```

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

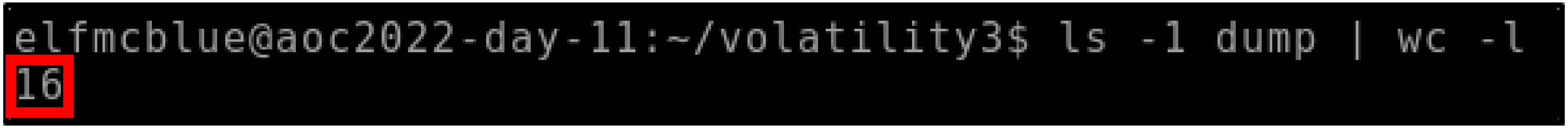
What is the Process ID (PID) of this binary?



```
*** 5888        4064    cmd.exe 0xc0091
09:59:38.000000         N/A
**** 2040       5888    mysterygift.ex
2-11-23 10:15:19.000000         N/A
**** 5932       5888    conhost.exe
2-11-23 09:59:38.000000         N/A
```

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

Dump the contents of this binary. How many files are dumped?



```
elfmcblue@aoc2022-day-11:~/volatility3$ ls -1 dump | wc -l
16
```

python3 vol.py -o ./dump -f workstation.vmem windows.dumpfiles --pid 2040

ls -1 dump | wc -l

It's time to Investigate and Answer the Advanced Questions (Part 1)!

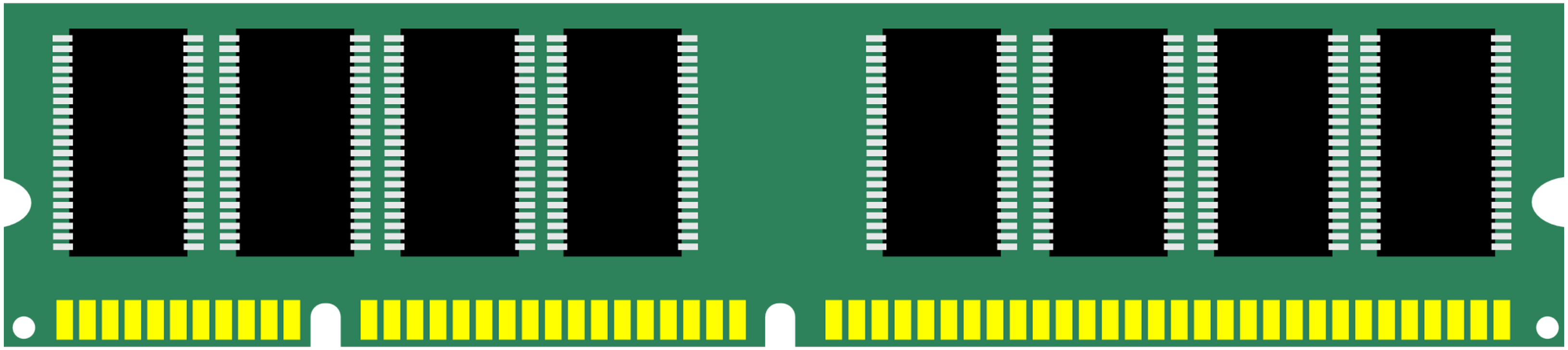
These questions may require you to search some additional functions and modules of Volatility 3

The questions can be found on the main.md page under section 3

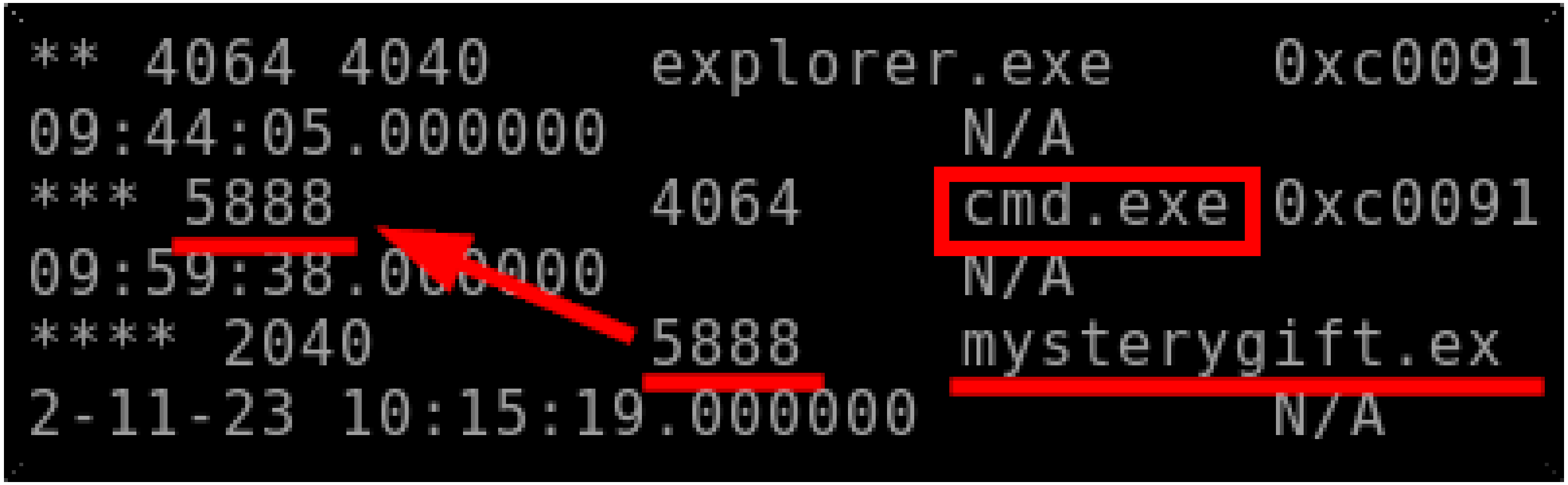
Volalatility command help can be found in section 5

We'll go over the answers in 20 minutes

Let's go over the answers to the Advanced Questions!



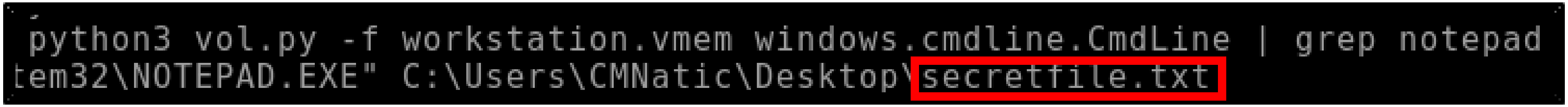
What process created the mysterygift.exe file?



```
** 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
```

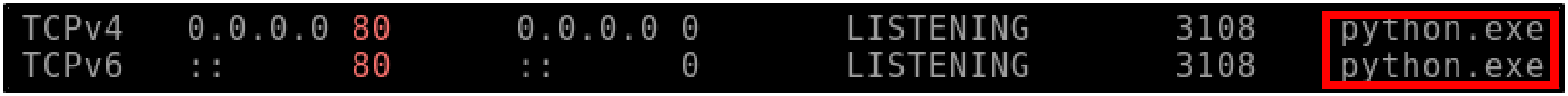
According to the memory dump command-line history, what suspicious file is opened by notepad.exe?



```
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

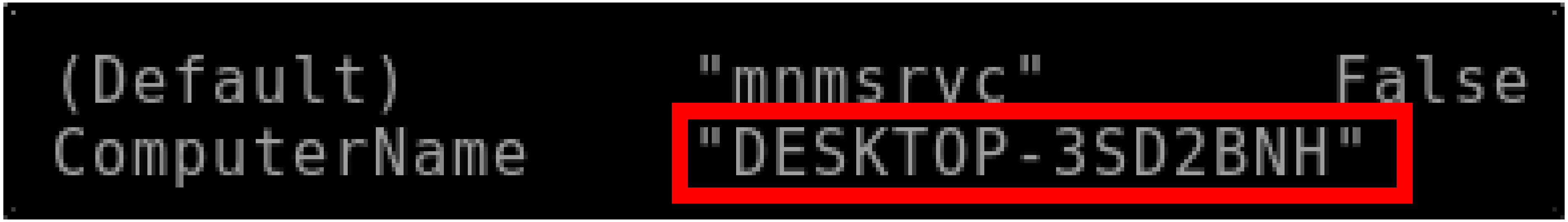
According to the memory dump file's networking information, what program is associated with the local and foreign port 80?



```
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"
```

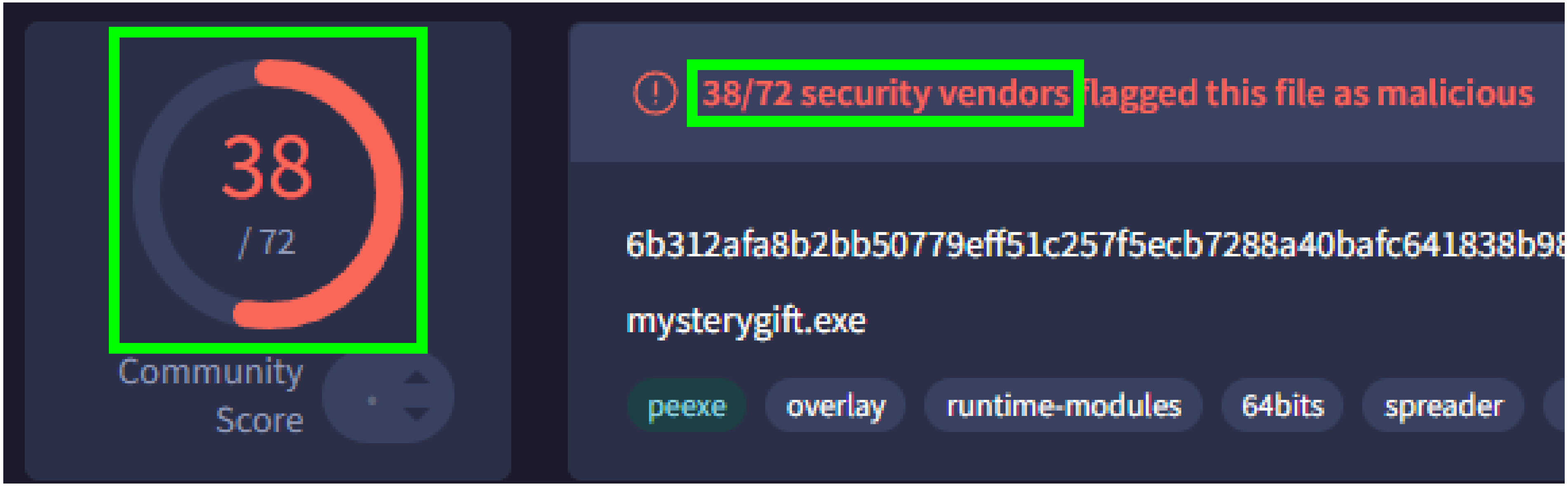
```
python3 vol.py -f workstation.vmem
windows.registry.printkey --key
"ControlSet001\\Control\\ComputerName
\\ComputerName"
```

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. They can found in the main.md file under section 4

We'll reconvene to go over the answers in 10 minutes

How many security vendors flagged the file as malicious?



38

/ 72

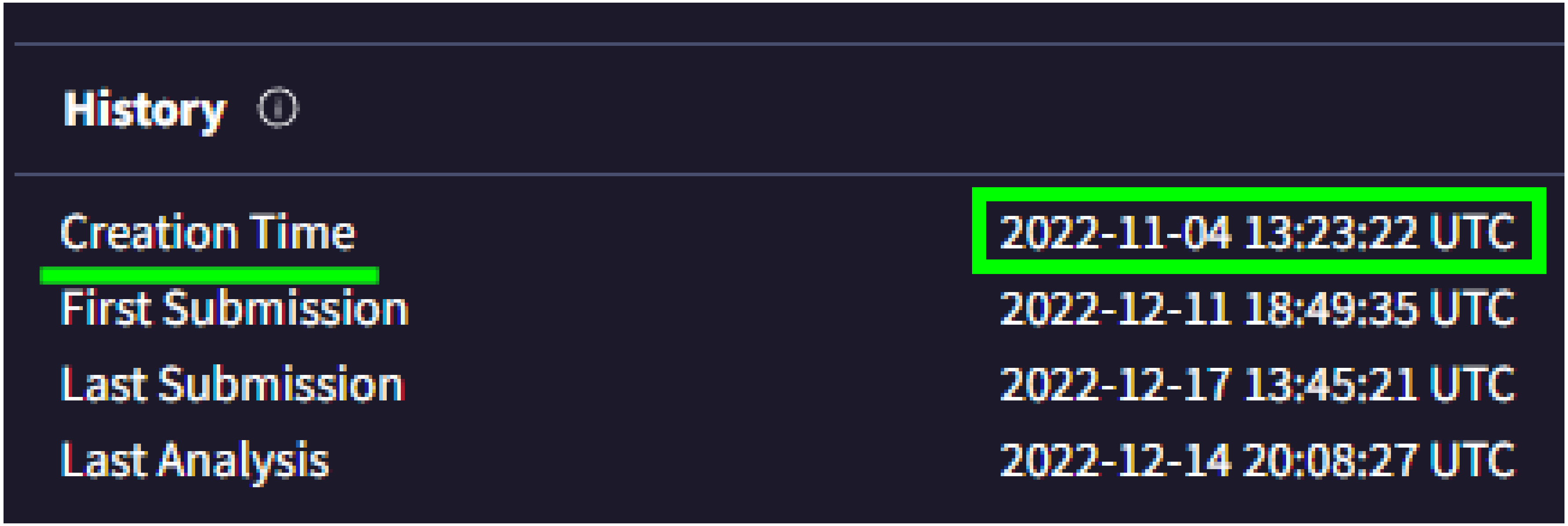
Community Score

38/72 security vendors flagged this file as malicious

6b312afa8b2bb50779eff51c257f5ecb7288a40bafc641838b98

mysterygift.exe

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

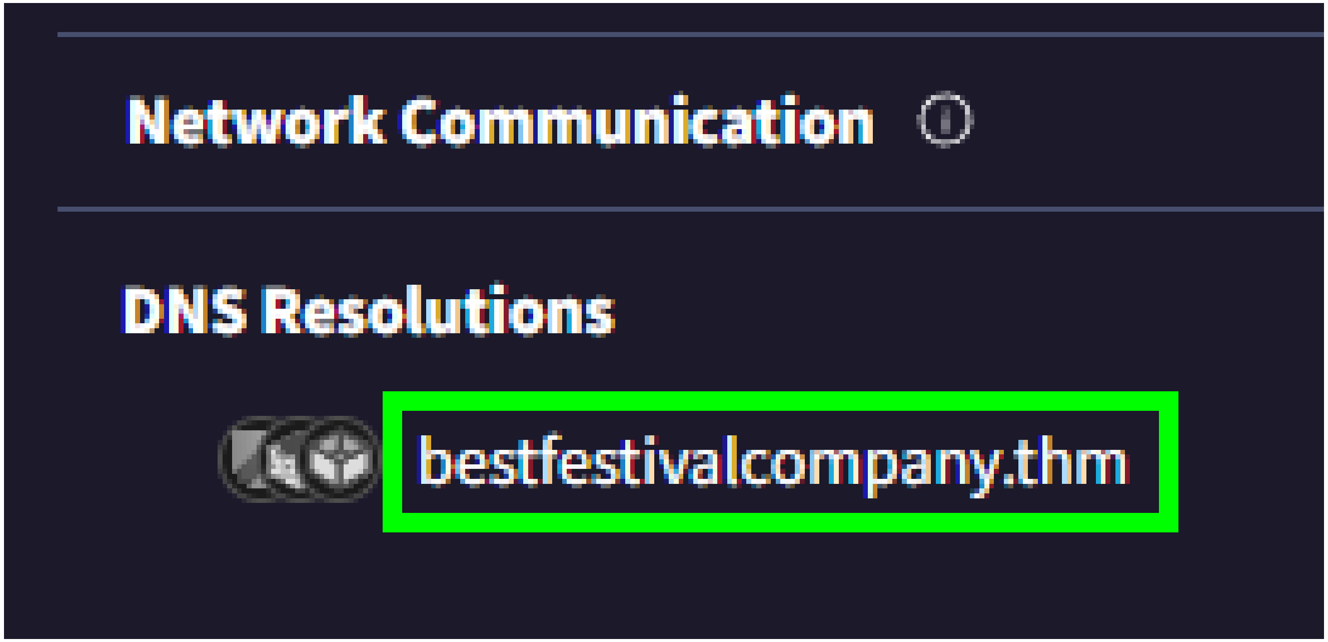


History

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?



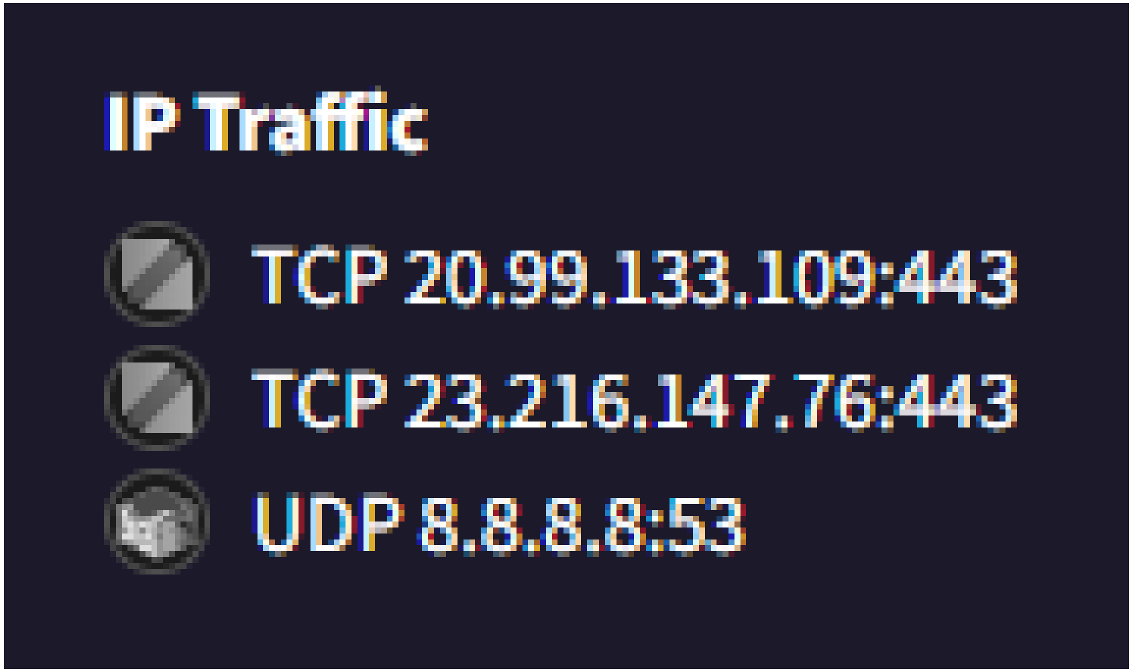
Network Communication

DNS Resolutions

bestfestivalcompany.thm

This can be found in the BEHAVIOR tab

What IP addresses are contacted by this file?



IP Traffic

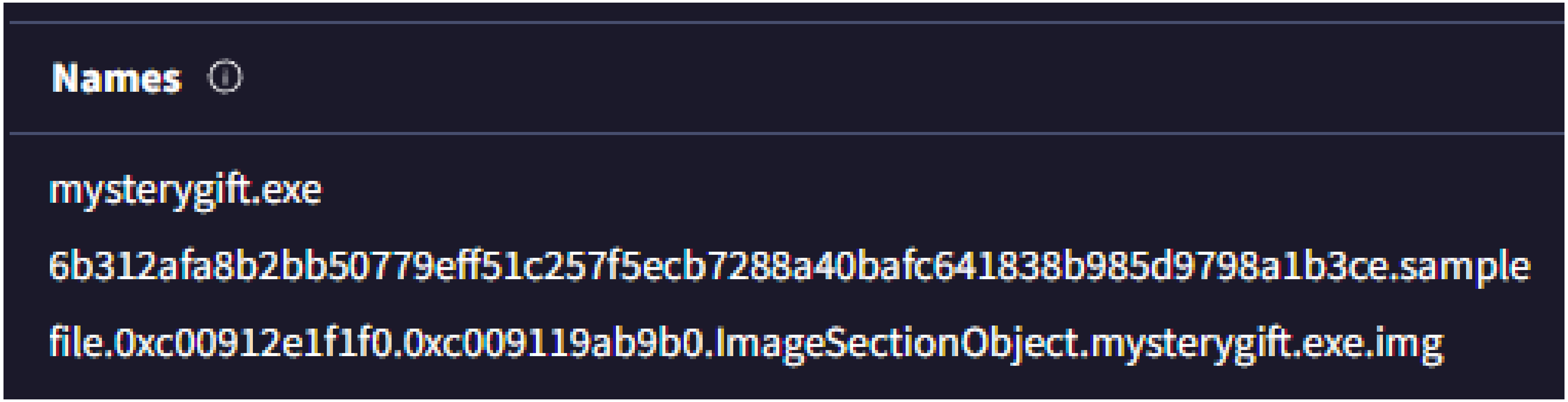
TCP 20.99.133.109:443

TCP 23.216.147.76:443

UDP 8.8.8.8:53

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

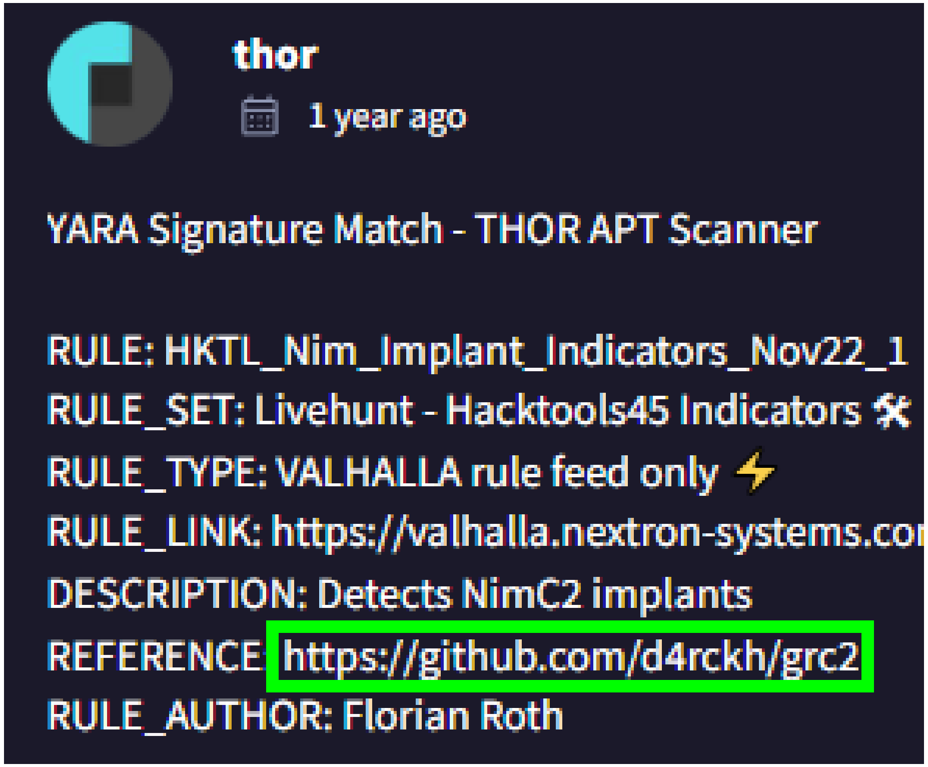
file.0xc00912e1f1f0.0xc009119ab9b0.ImageSectionObject.mysterygift.exe.img

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?



thor

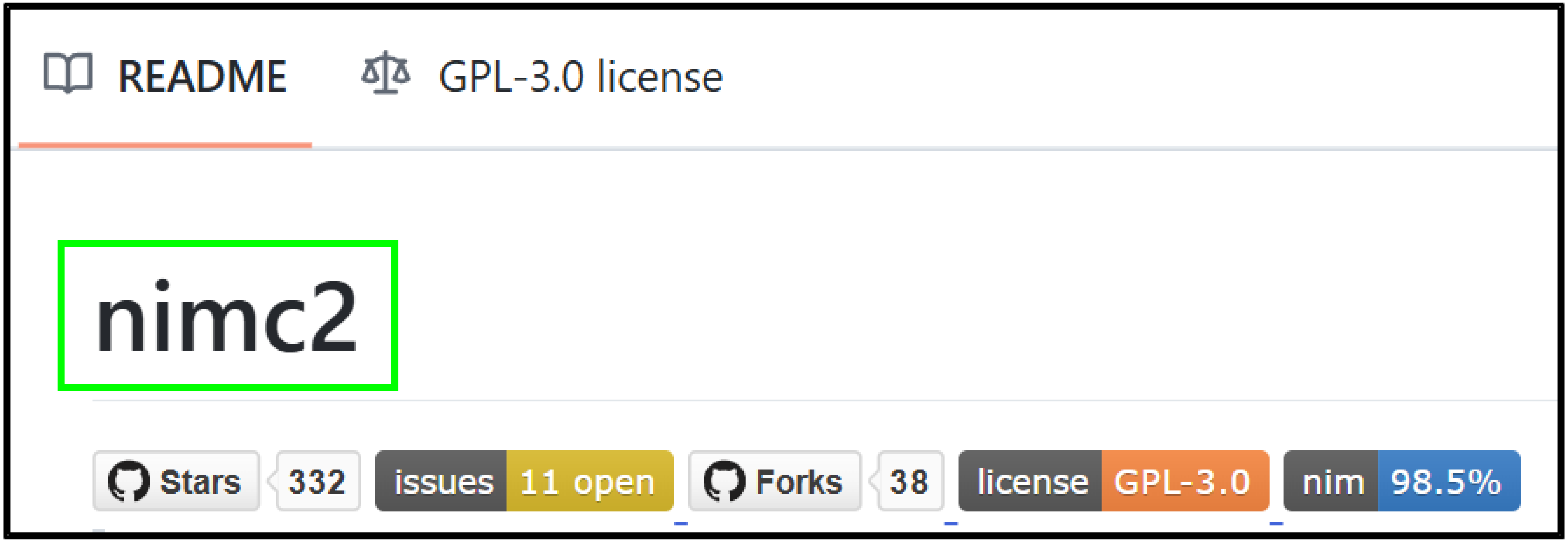
1 year ago

YARA Signature Match - THOR APT Scanner

RULE: HKTL_Nim_Implant_Indicators_Nov22_1
RULE_SET: Livehunt - Hacktools45 Indicators 🛠
RULE_TYPE: VALHALLA rule feed only ⚡
RULE_LINK: https://valhalla.nextron-systems.co
DESCRIPTION: Detects NimC2 implants
REFERENCE: https://github.com/d4rckh/grc2
RULE_AUTHOR: Florian Roth

This can be found in the COMMUNITY tab

What is the name of this Github project?

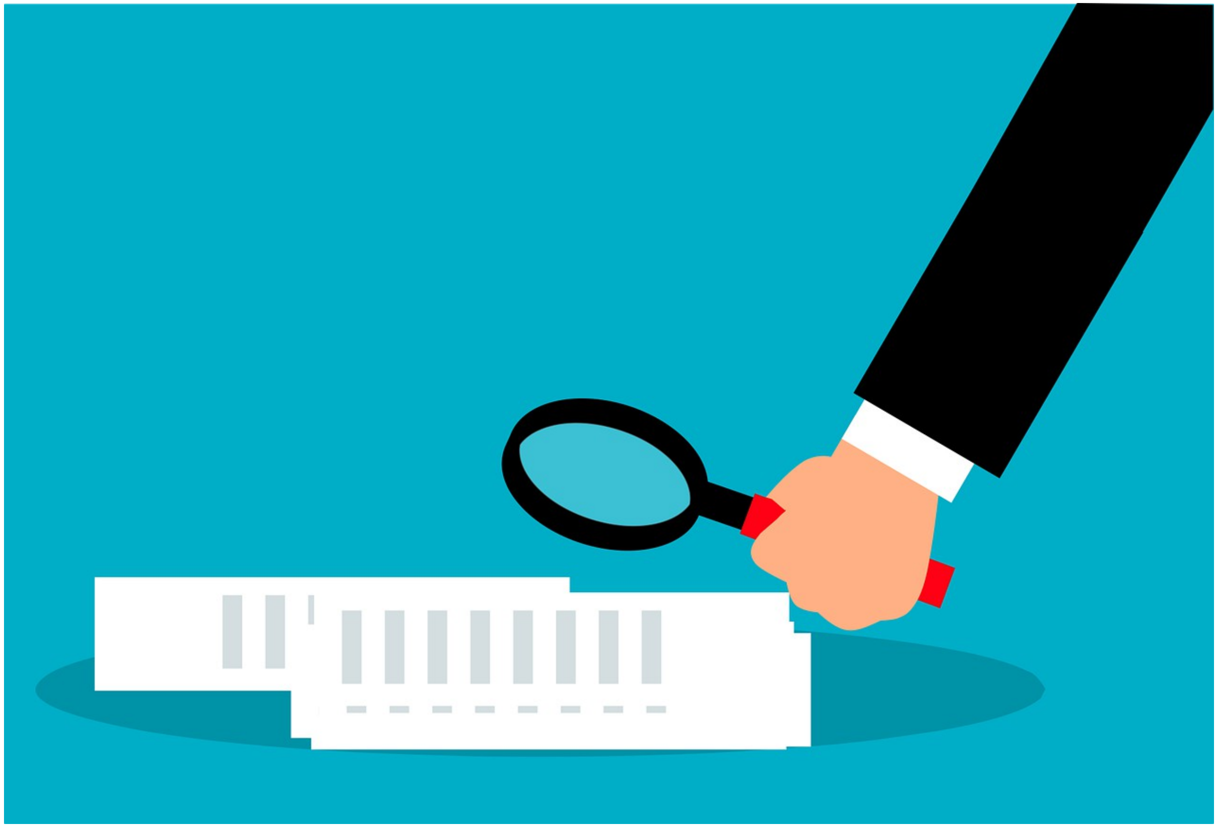


README GPL-3.0 license

nimc2

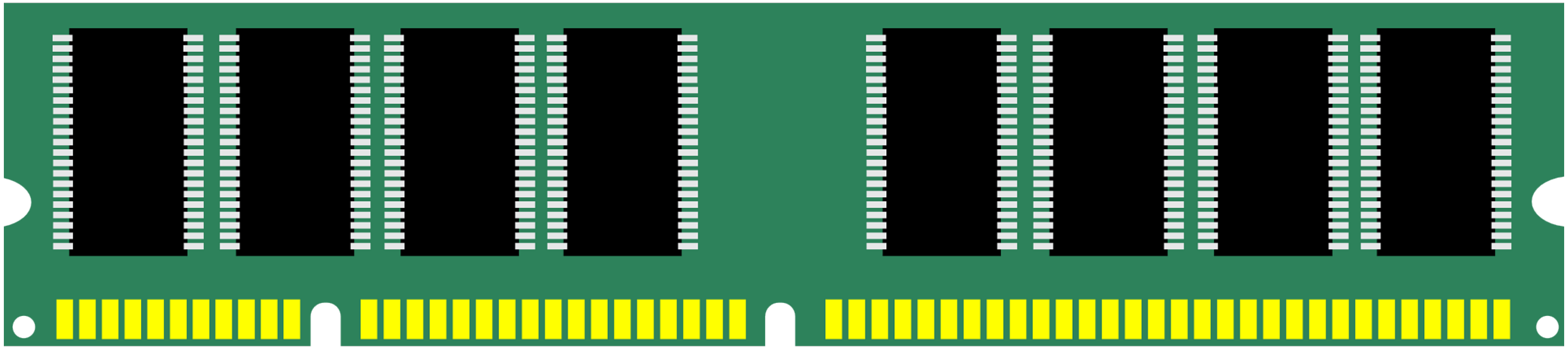
We find the name of the project on the Github page

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

More Volatility Modules?

If you want more Volatility education modules, you can some in the main.md file under section 6

Who Gave this Workshop Today?

Kevin Lee, learning cybersecurity since 2020, currently teaching beginner's cybersecurity skills through YouTube, Twitch, and the HackerFrogs program

Goes by “theShyHat”
on all platforms

Until Next Time, Hackers!