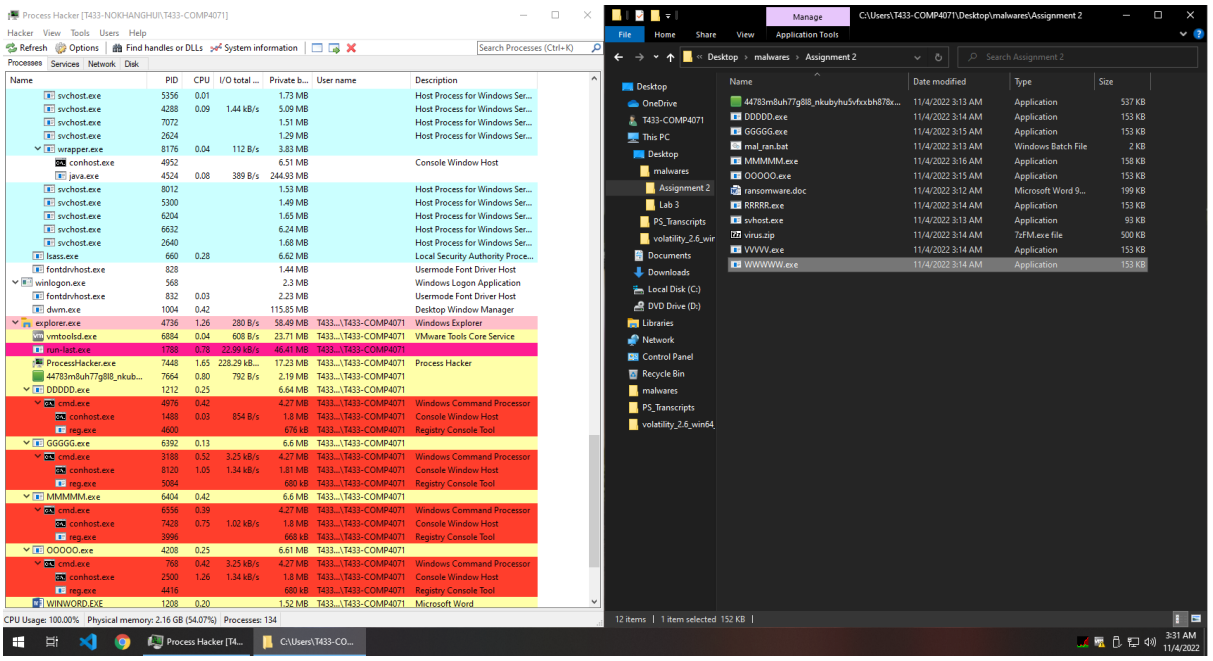
# Forensics Lab

**Author Name: Hui Nok Hang**

## Downloading and running the malwares

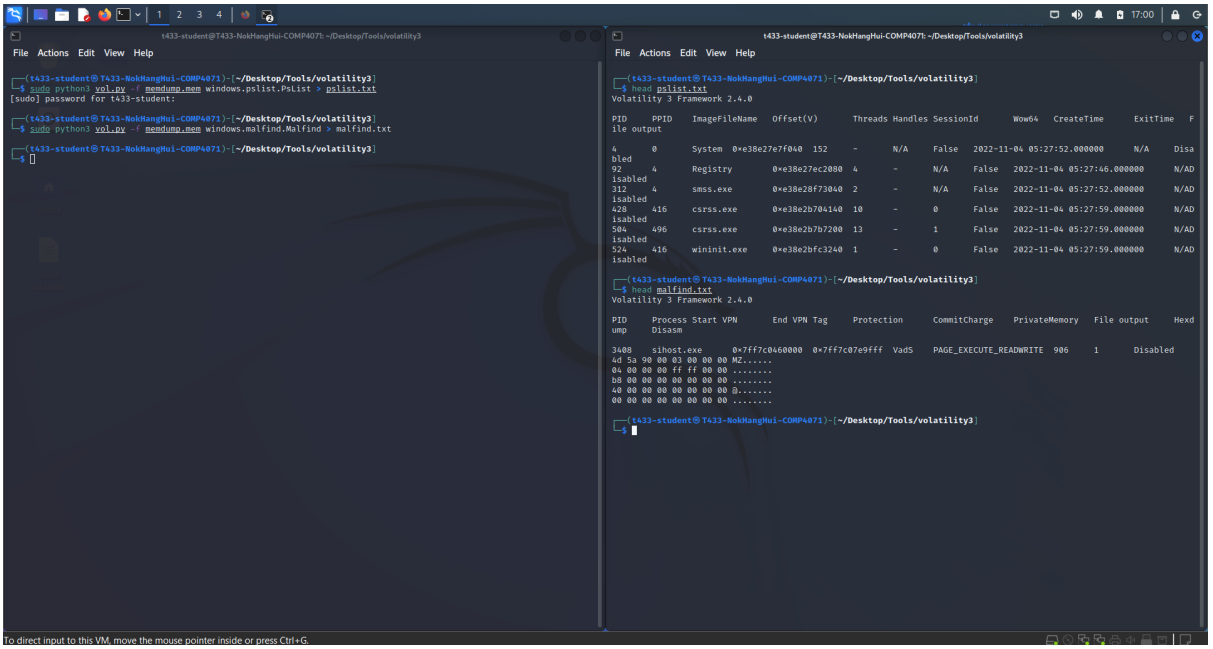
The malware executables from https://app.box.com/s/btzloulf1f82ql4io5d4spbmy19i1ror are downloaded into the Windows VM and run. They can be seen below in process hacker.

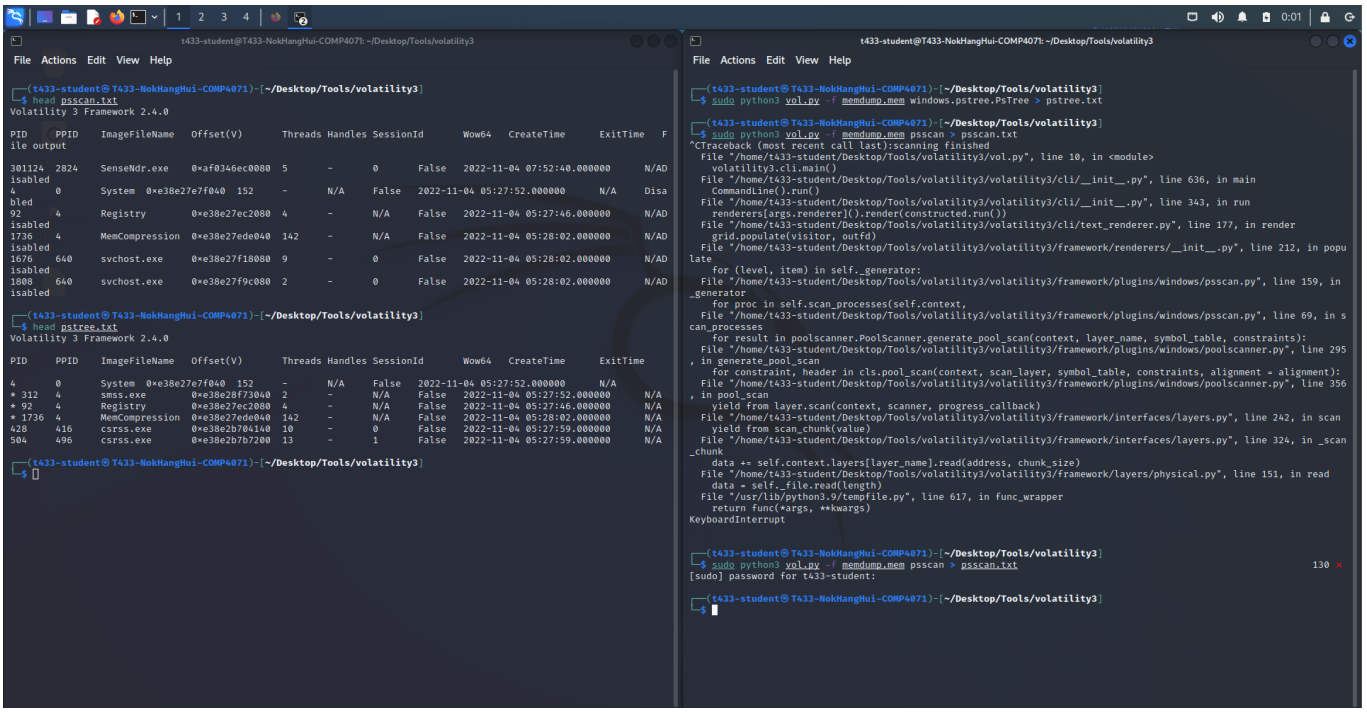


Memdump was then created and transferred to Kali Machine for investigation.

## Volatility Analysis

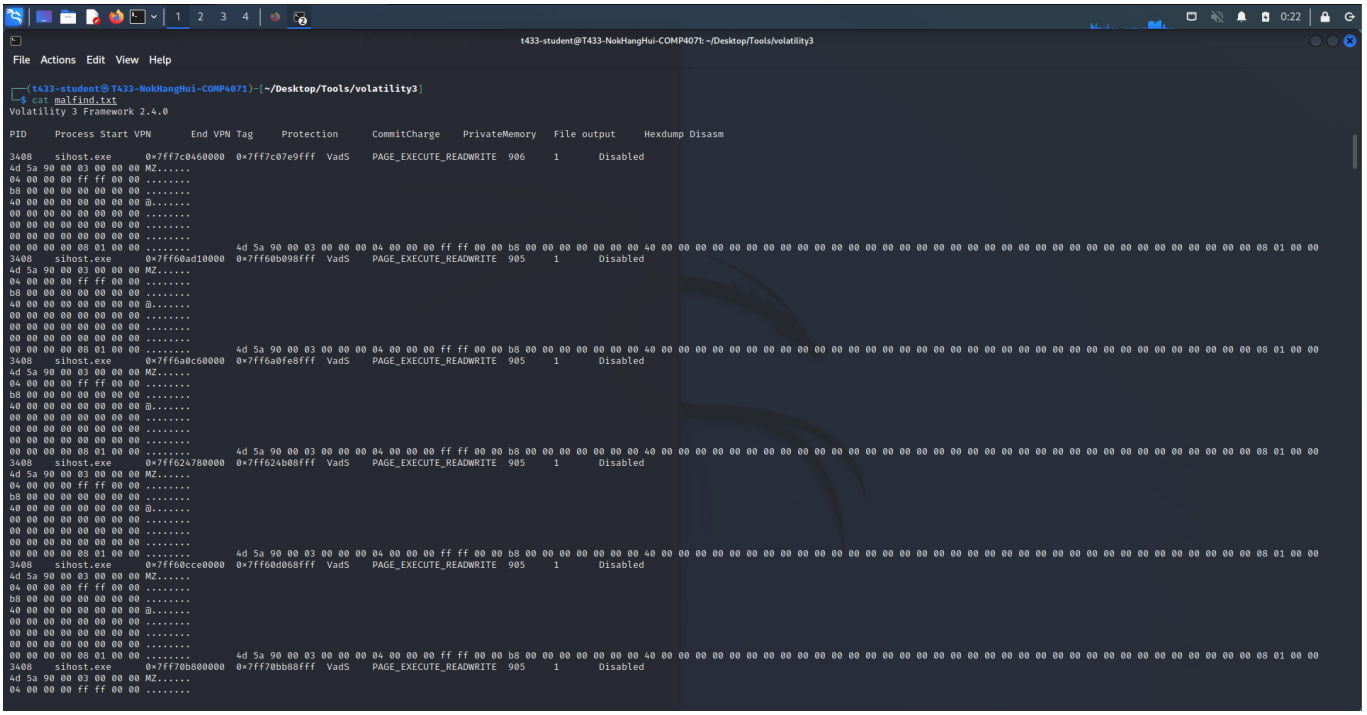
In Kali, volatility 3 modules pslist, pstree, psscan and malfind are run on the memdump we just created.



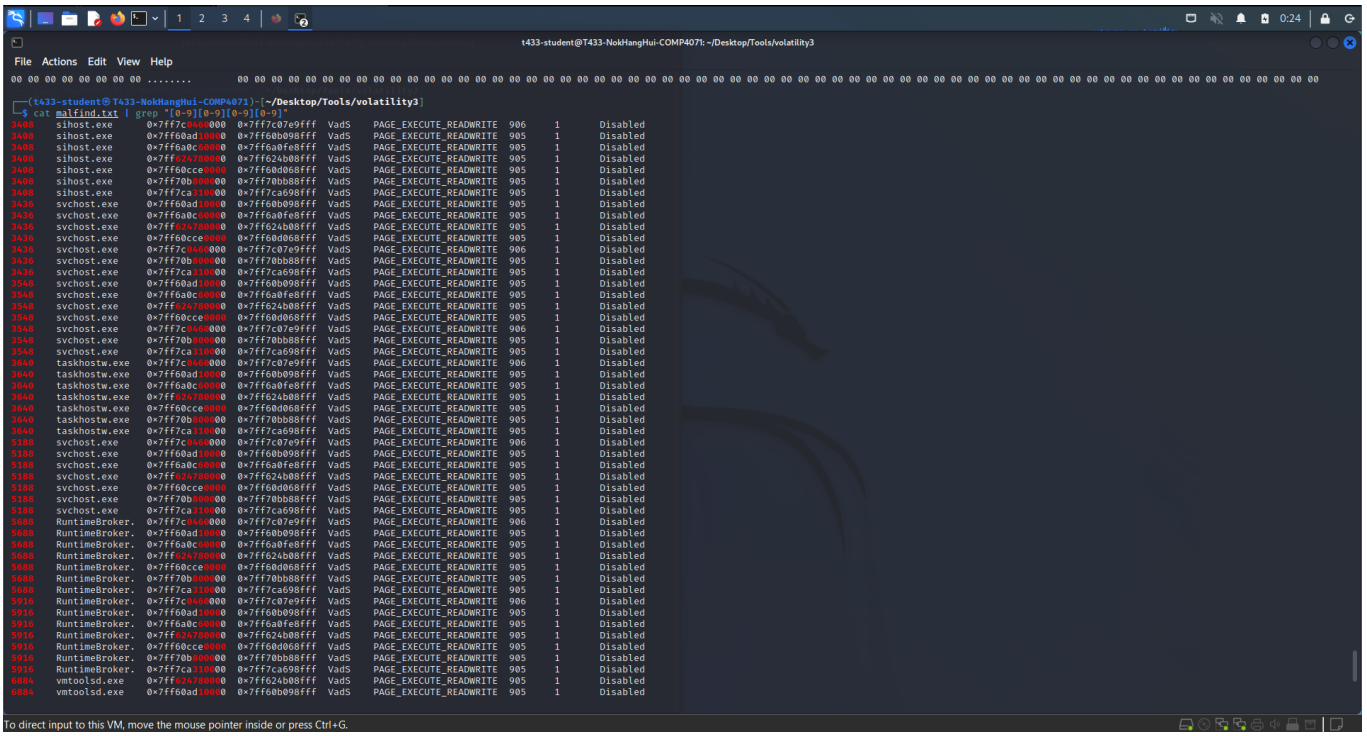



## Malfind

Malfind has a long list of outputs of potentially suspicious processes.




Trimming down the file with grep and simple regex, their process ID and names are:



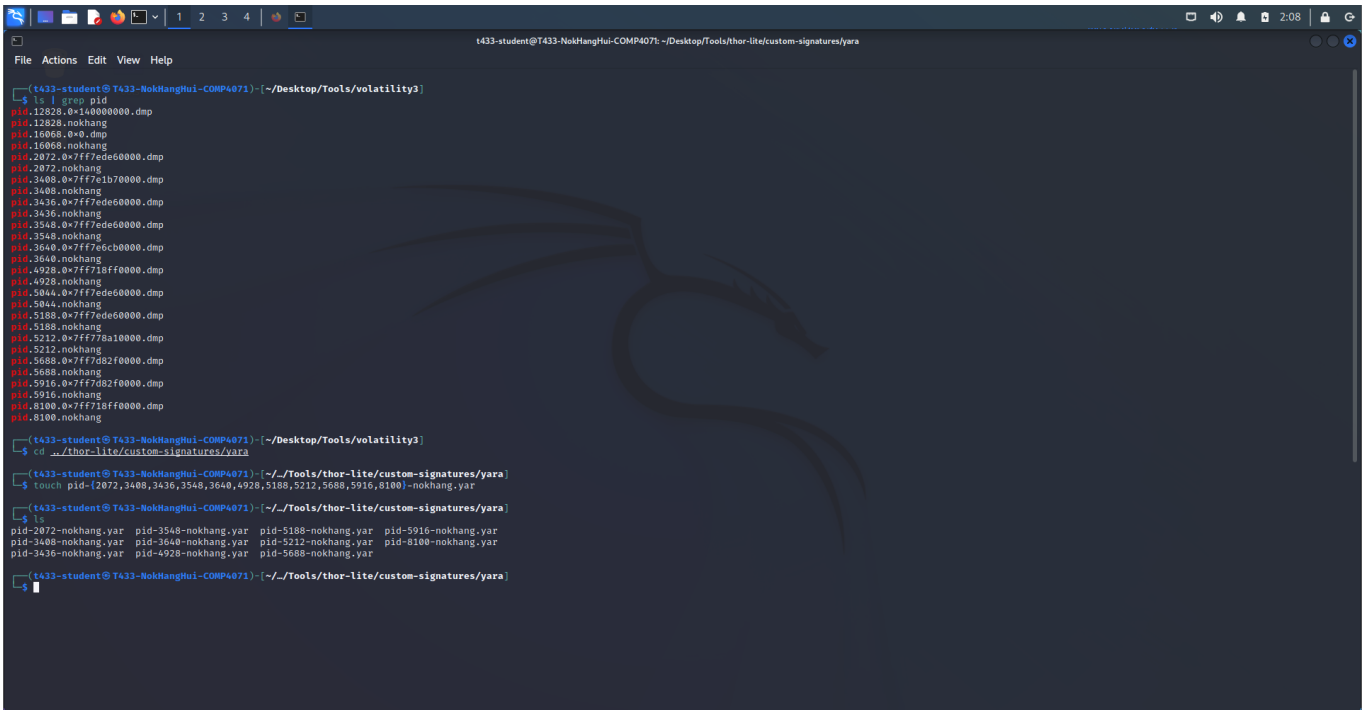

3408 sihost.exe
3436 svchost.exe
3548 svchost.exe
3640 taskhostw.exe
5188 svchost.exe
5688 RuntimeBroker.
5916 RuntimeBroker.
6884 vmtoolsd.exe (Eliminated)
2072 svchost.exe
4928 dllhost.exe
5212 ApplicationFra
8100 dllhost.exe
5044 svchost.exe
7448 ProcessHacker. (Eliminated)
12828 svchost.exe
16068 SearchApp.exe

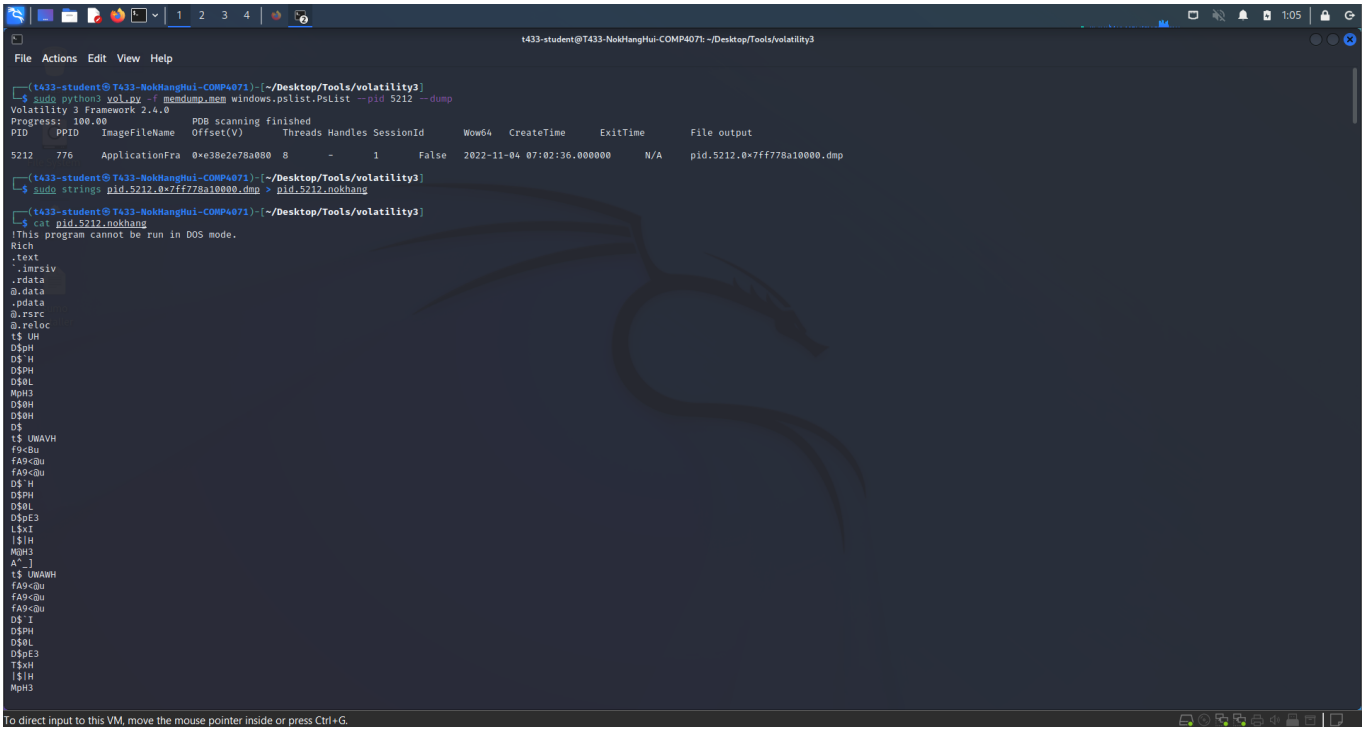
All of these processes are named after legit processes in the windows environments. However, malwares are known to disguise themselves as legit process names, so we definitely cannot dismiss these findings. However, we can reasonably conclude that vmtoolsd.exe and ProcessHacker. are false positives, since these are most likely related to the assignment and virtual machine and they are too niche to be used as a disguise.

**Strings analysis**

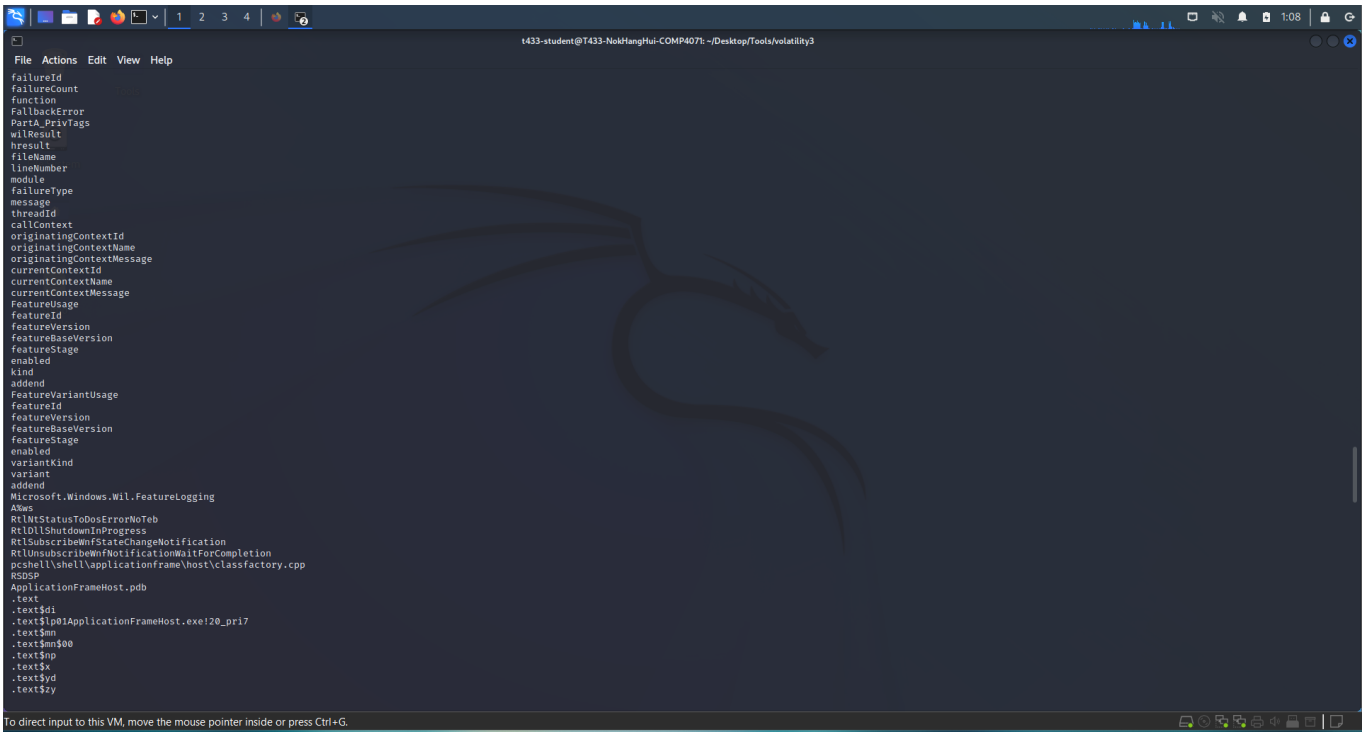
After getting a list of our target processes, now is the time to create the memory dump for these specific processes and doing strings analysis on them.

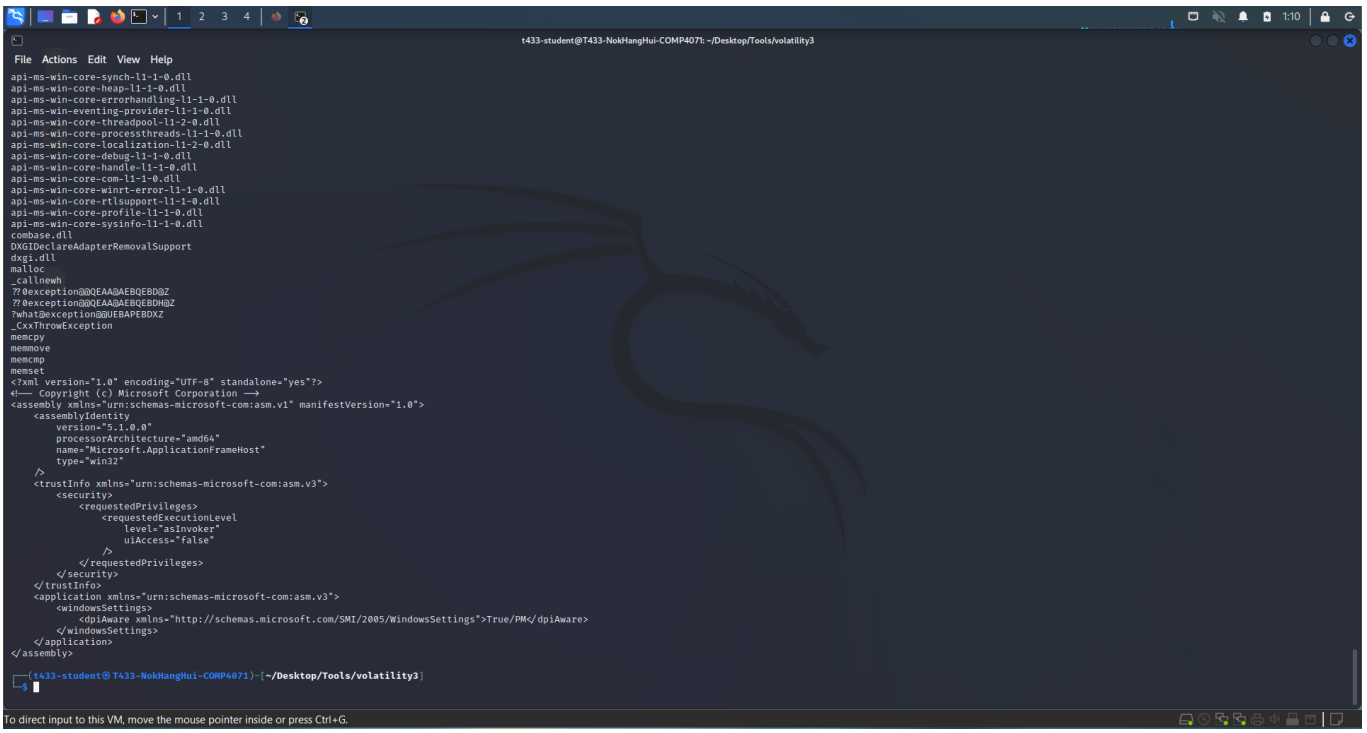
First, create yara rules in the thor-lite/custom-signatures/yara directory.



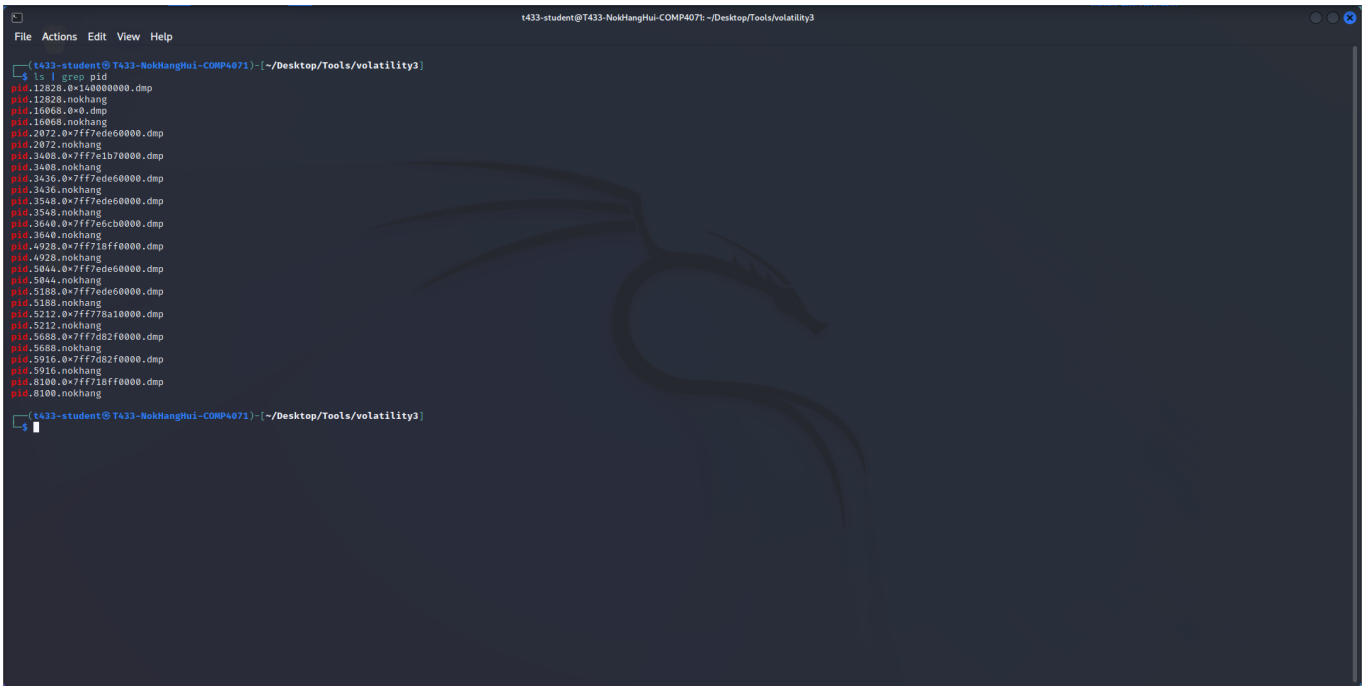

As we can see below, there are some interesting strings output in some of the processes. However, not every process outputs meaningful results.



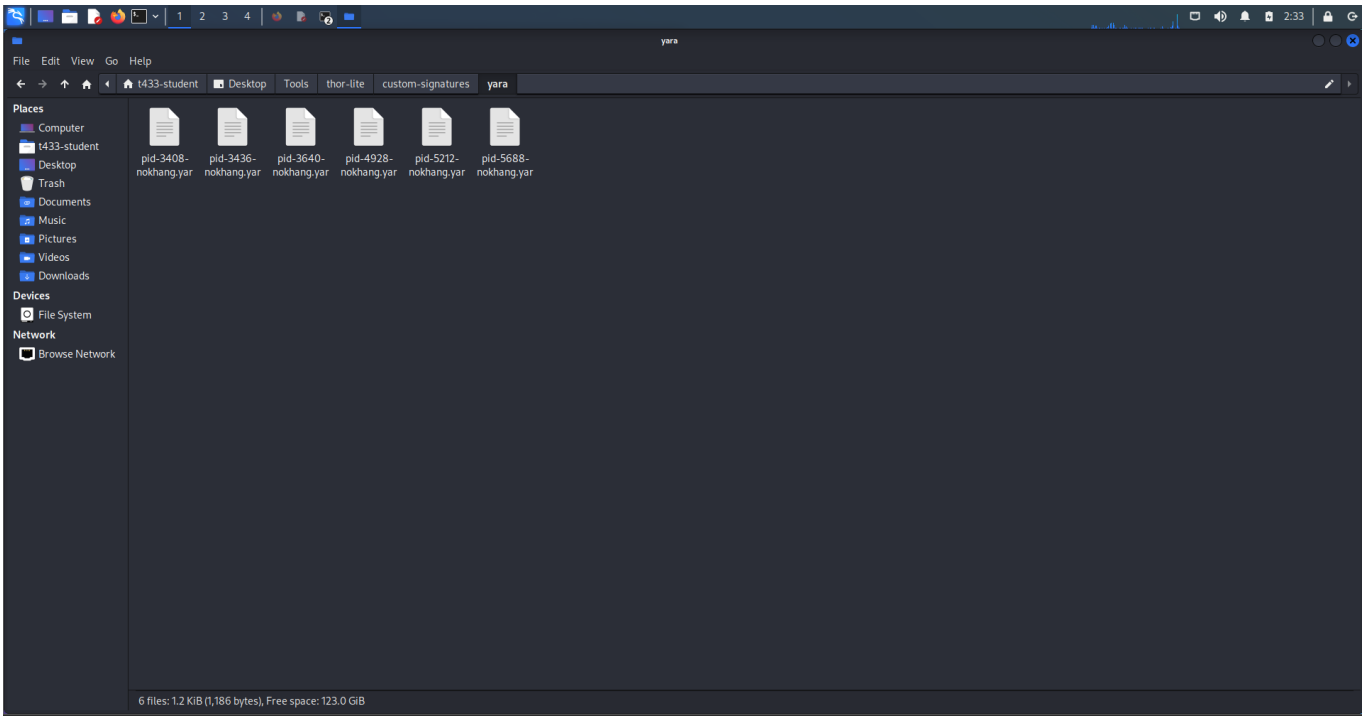

I repeated the steps for all of the listed processes above. Process 5044, 12828, 16068 yield no result from strings, therefore they are being excluded from having a yara rule created for them.

Since svchost.exe, RunTimeBroker and dllhost.exe have multiple instances in the list, which all yield the same strings result, I am only keeping the first instance of each of these processes in the list.

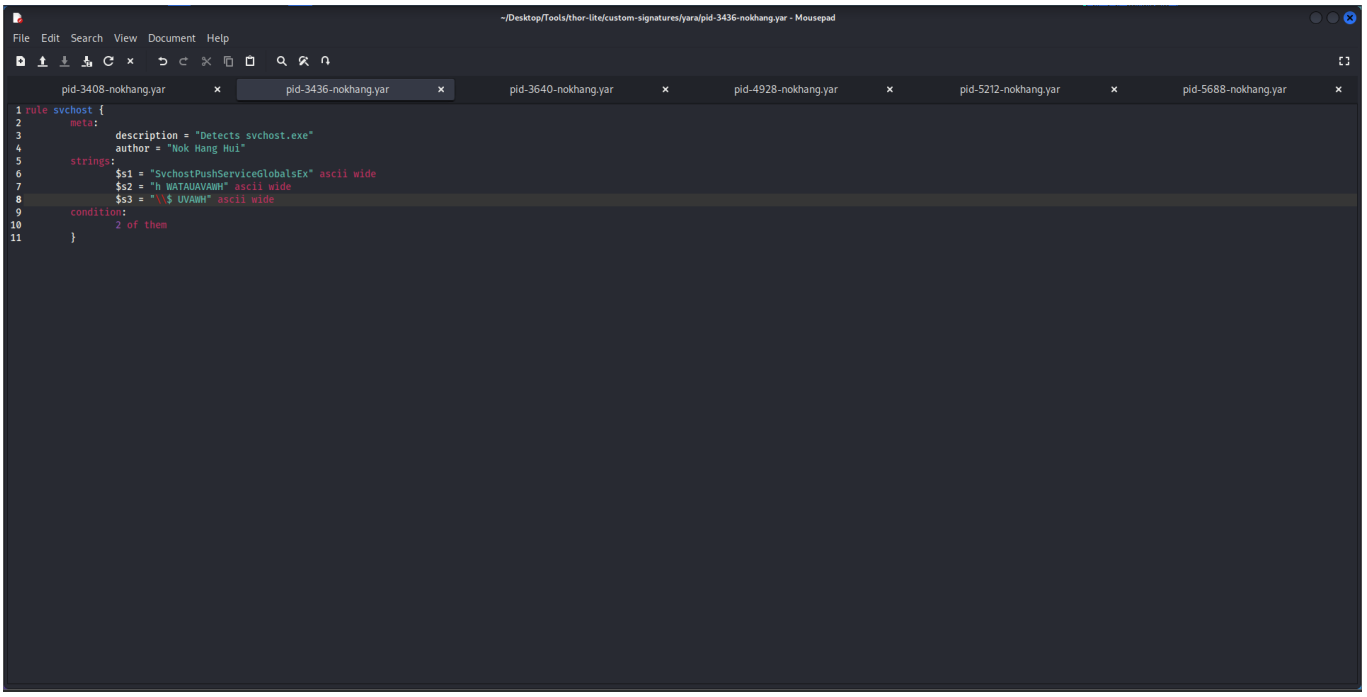



## Yara rules

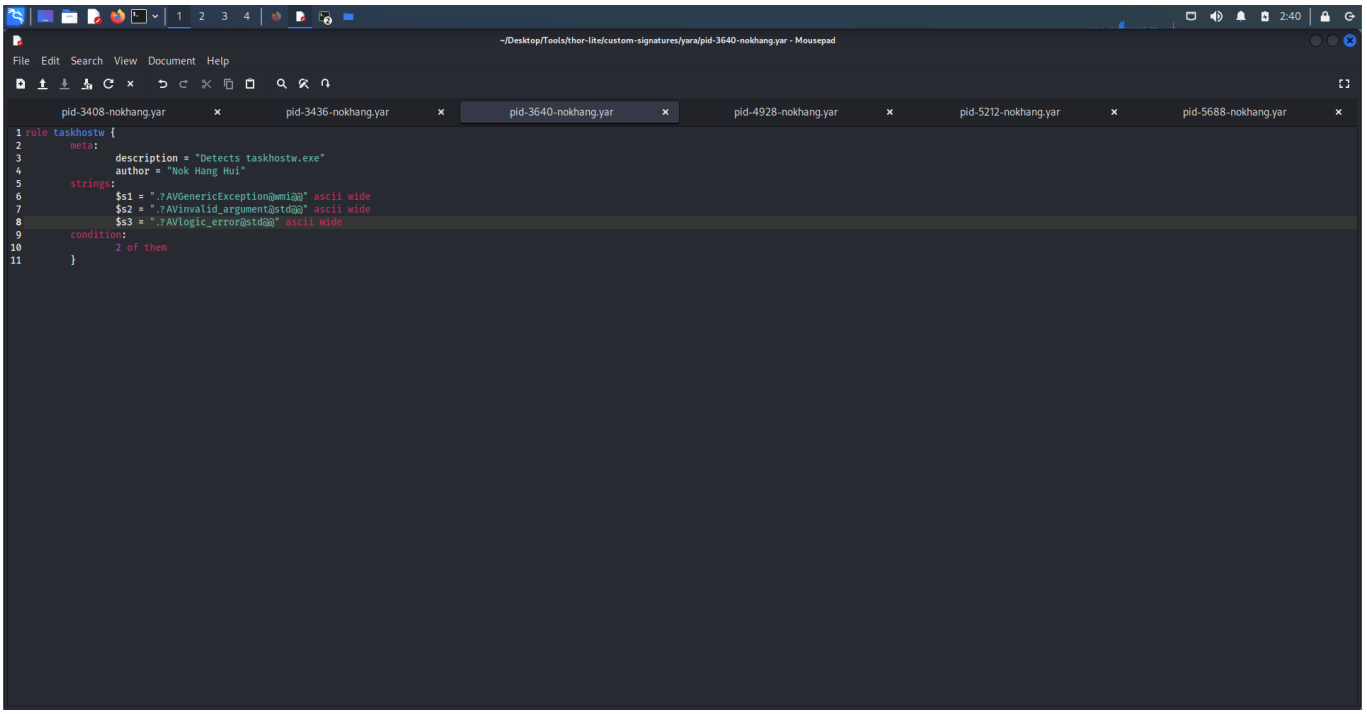
Now that we have readable strings from every suspicious process we flagged, it is time to create yara rules to detect them in thor lite.



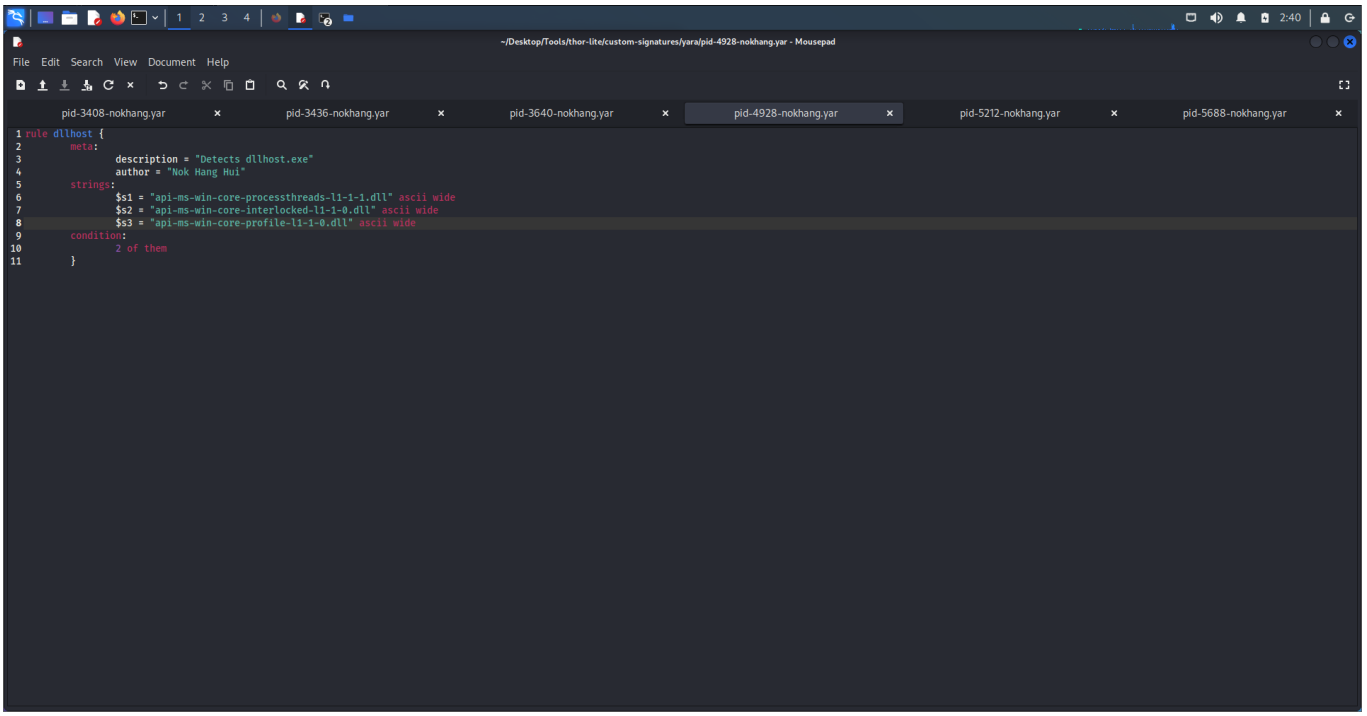

svchost.exe:



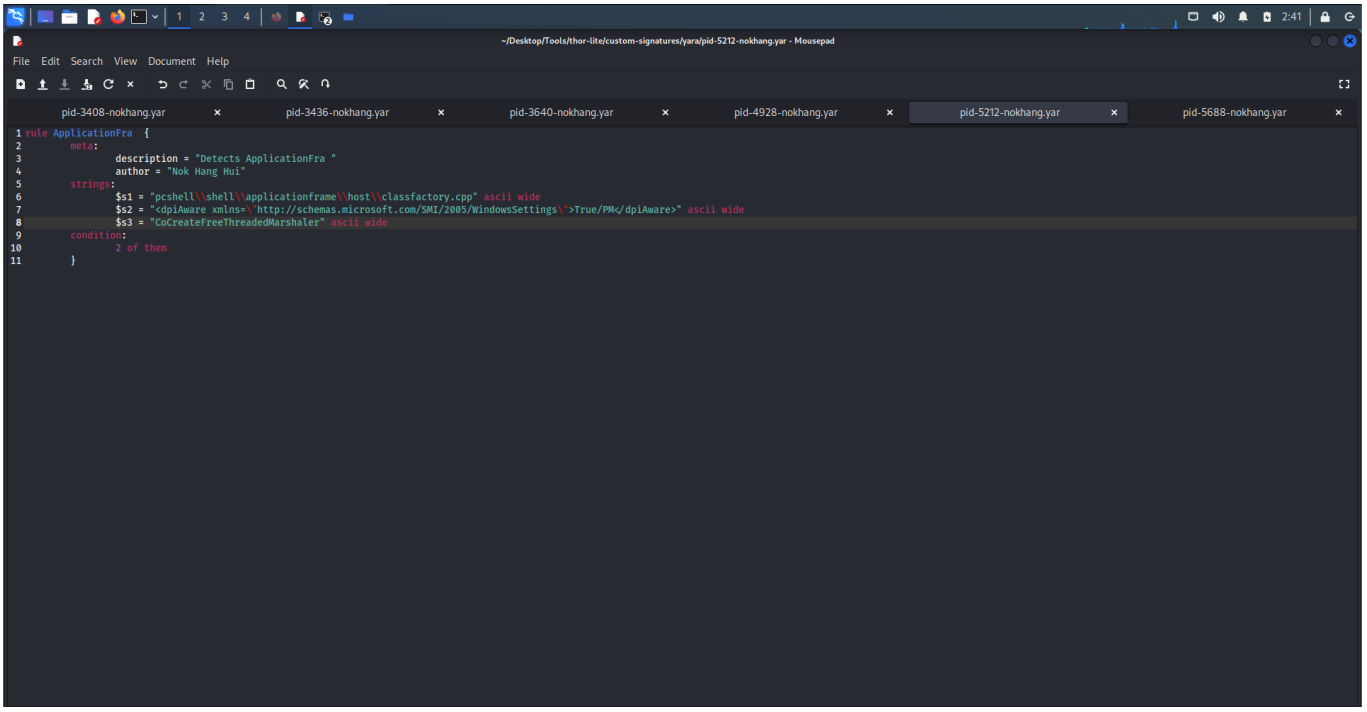

taskhostw.exe



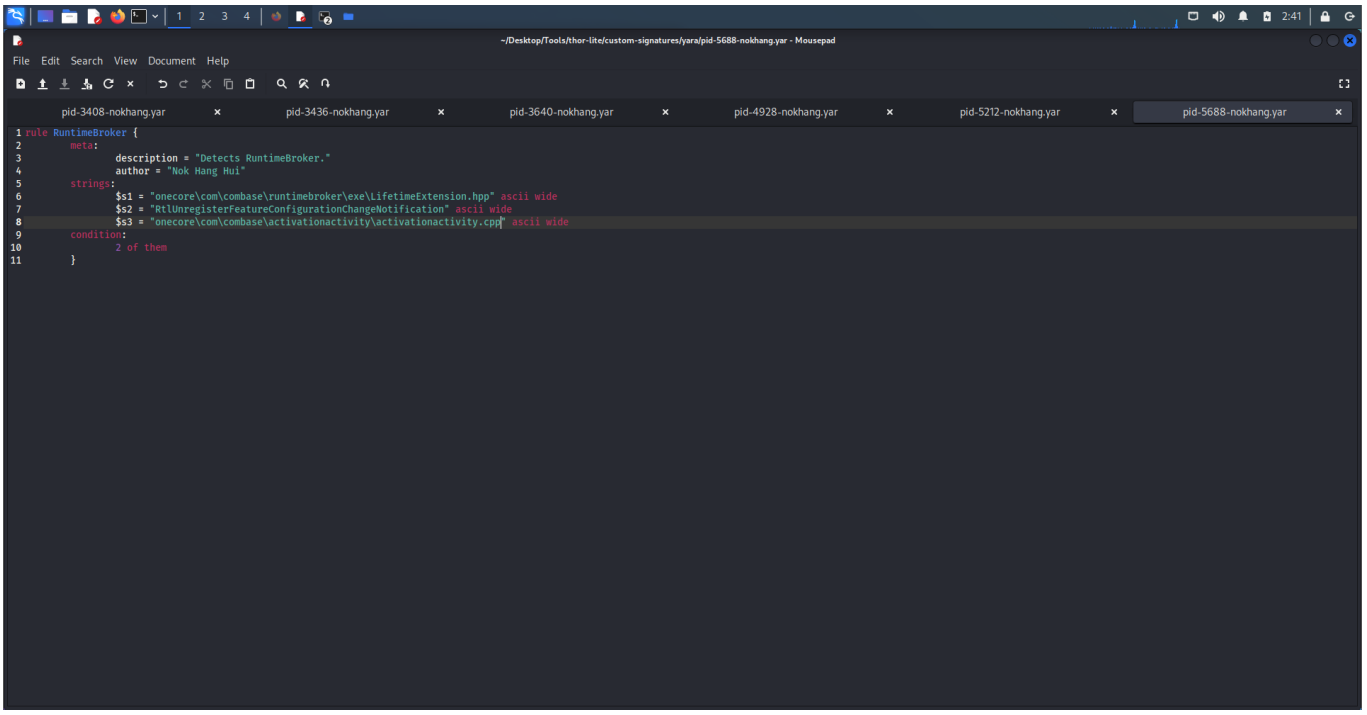

dllhost.exe:




ApplicationFra:

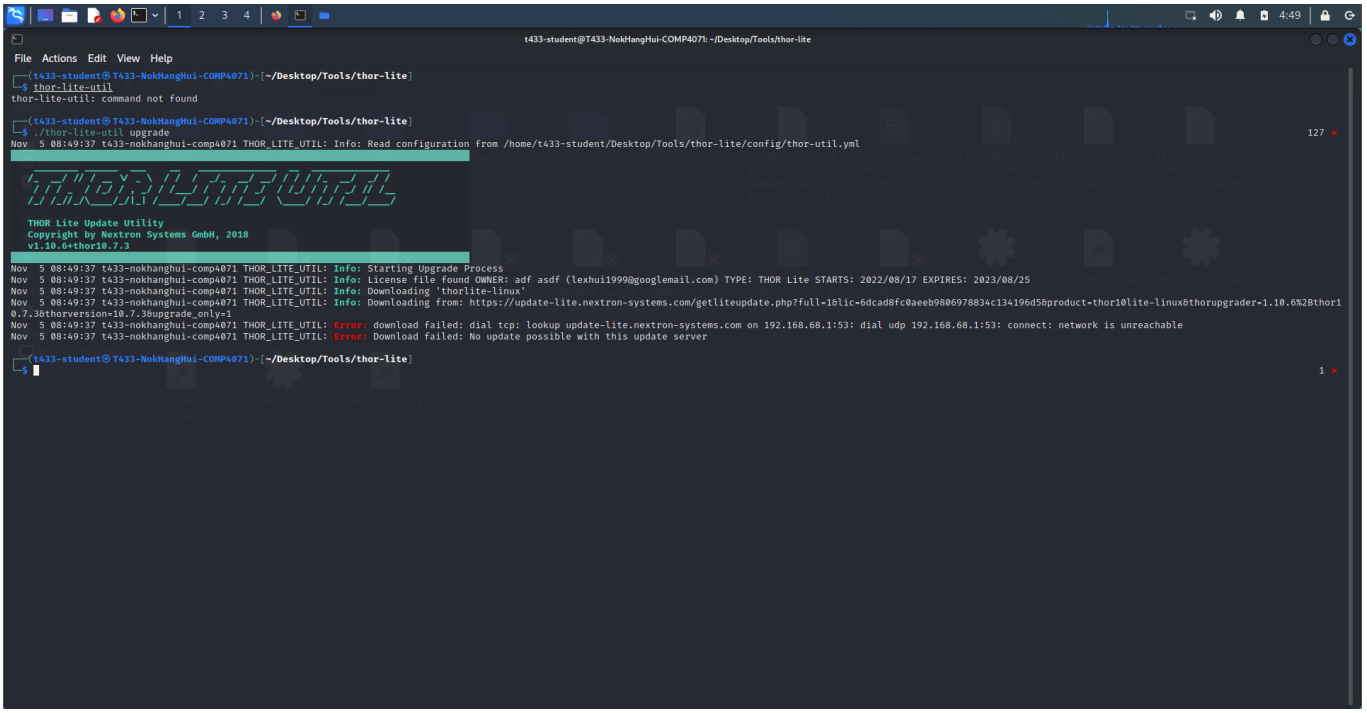


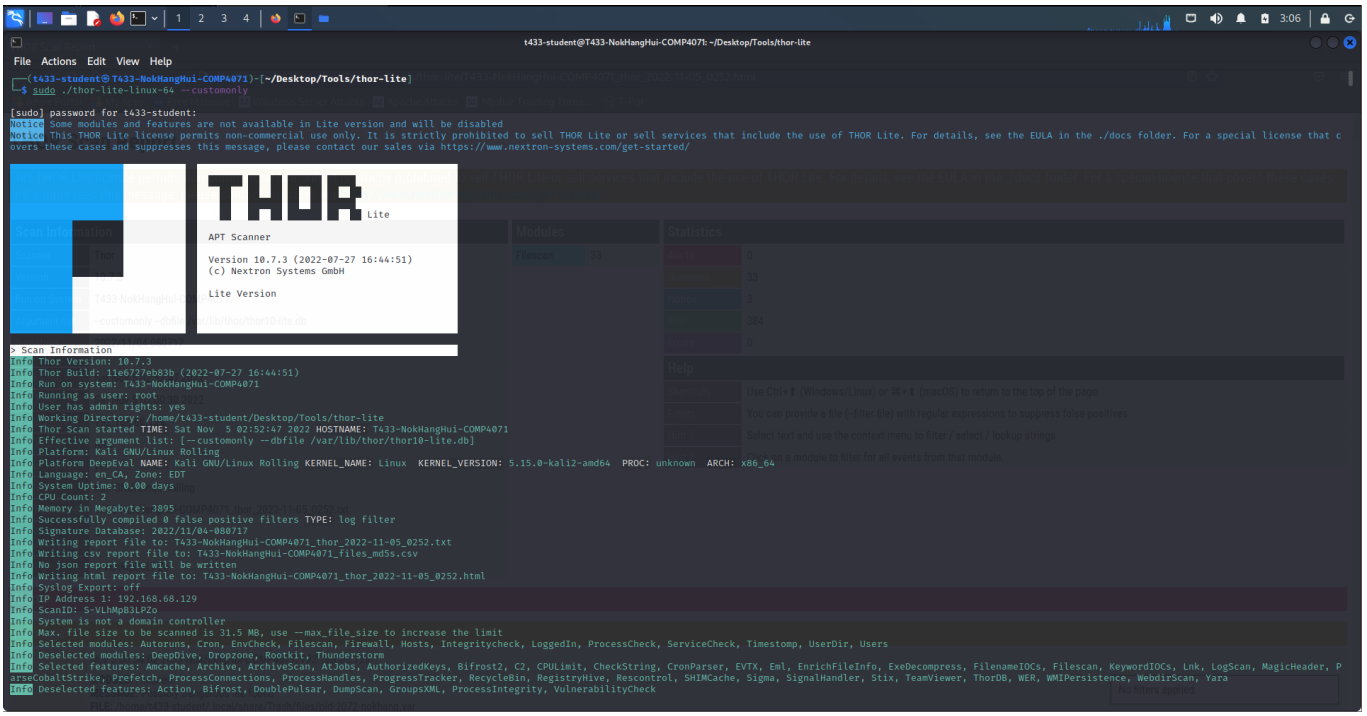

RunTimeBroker:



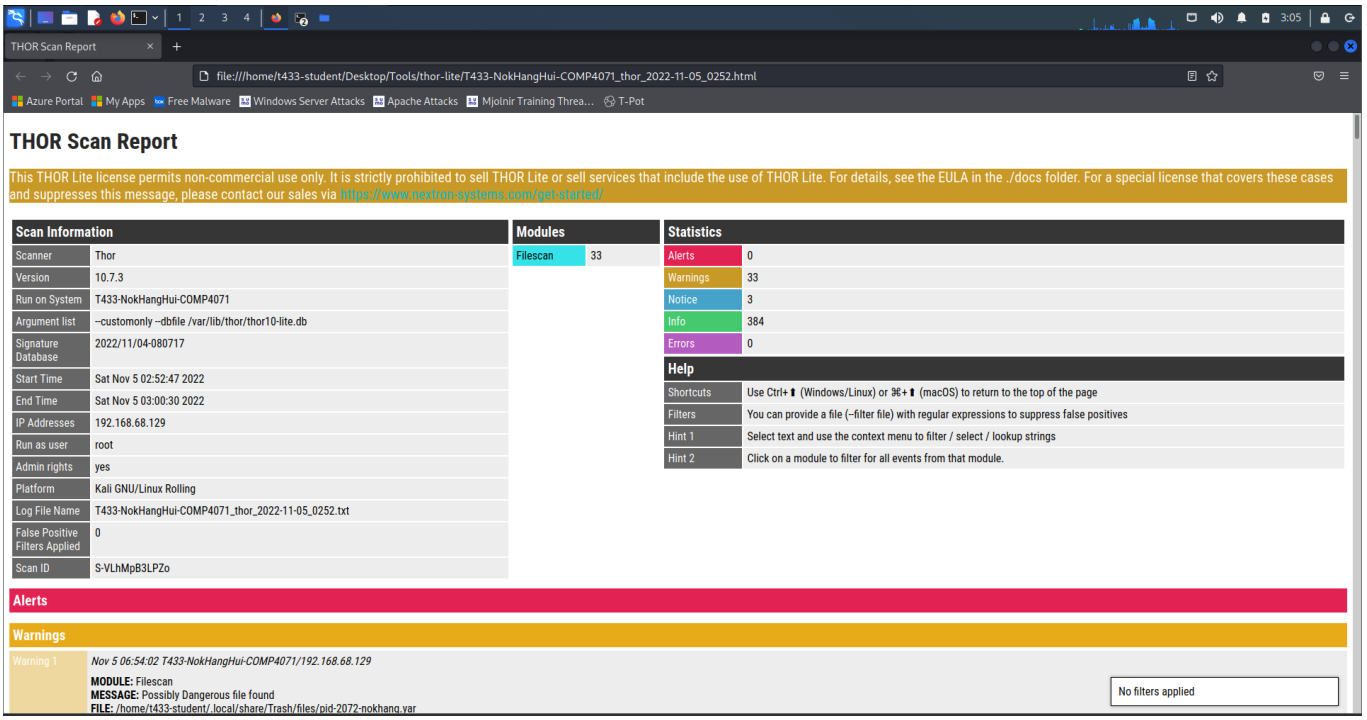

## THOR lite

After creating all the respective yara rules, it is time to test it on our Kali machine.

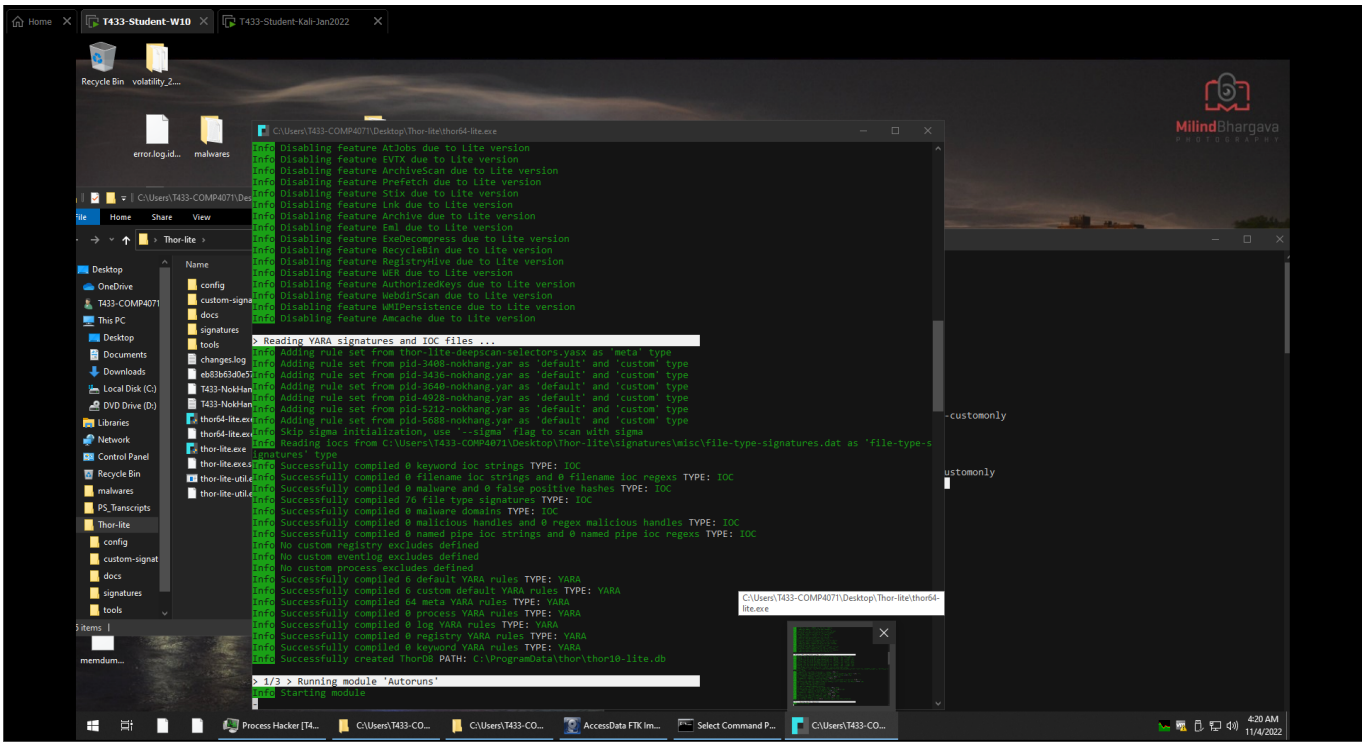


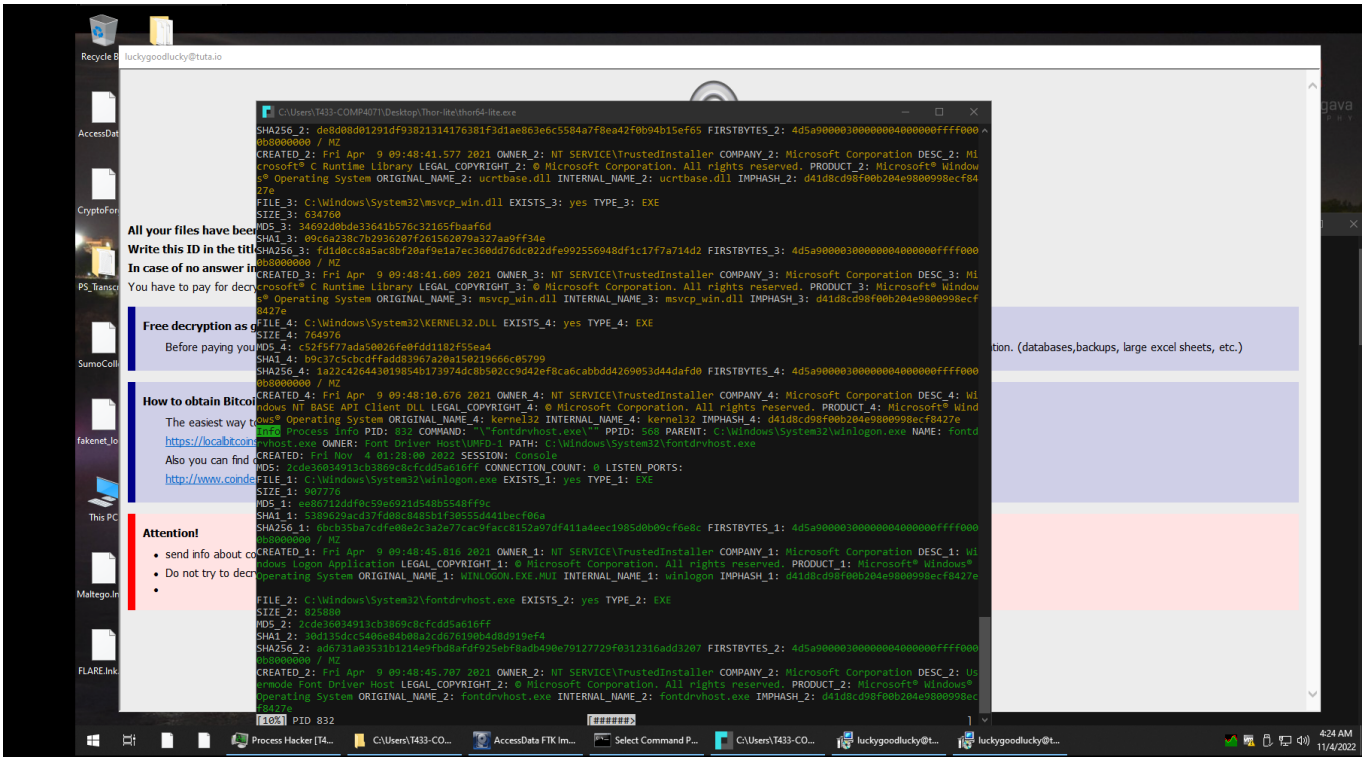



Below is the HTML report. It confirmed the detection of multiple rules and gave 33 warnings.

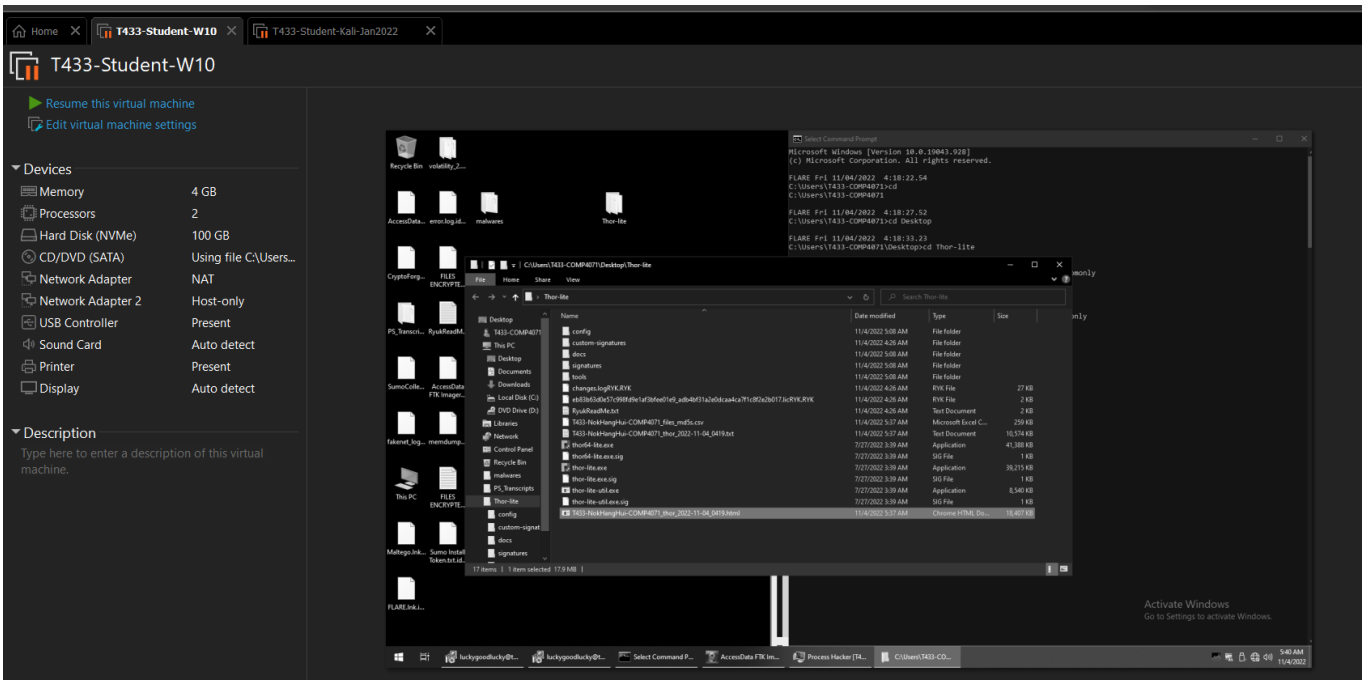


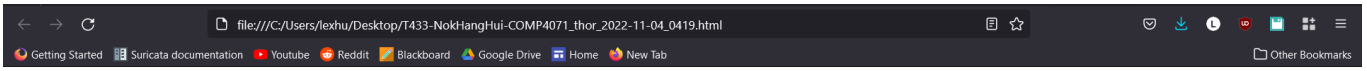

Running thor-lite in the infected Windows VM.





HTML report is generated.




# THOR Scan Report

This THOR Lite license permits non-commercial use only. It is strictly prohibited to sell THOR Lite or sell services that include the use of THOR Lite. For details, see the EULA in the ./docs folder. For a special license that covers these cases and suppresses this message, please contact our sales via https://www.nextron-systems.com/get-started/

| Scan Information | |
|---|---|
| Scanner | Thor |
| Version | 10.7.3 |
| Run on System | T433-NokHangHui-COMP4071 |
| Argument list | --customonly --dbfile %ProgramData%\thor\thor10-lite.db |
| Signature Database | 2022/11/04-080717 |
| Start Time | Fri Nov 4 04:19:49 2022 |
| End Time | Fri Nov 4 05:37:09 2022 |
| IP Addresses | 192.168.171.128 |
| Run as user | T433-NOKHANGHUI\T433-COMP4071 |
| Admin rights | yes |
| Platform | Windows 10 Enterprise |
| Log File Name | T433-NokHangHui-COMP4071_thor_2022-11-04_0419.txt |
| False Positive Filters Applied | 0 |
| Scan ID | S-aL2xeJKPfDk |

| Modules | |
|---|---|
| Filescan | 3195 |
| ProcessCheck | 412 |

| Statistics | |
|---|---|
| Alerts | 0 |
| Warnings | 2861 |
| Notice | 749 |
| Info | 996 |
| Errors | 0 |

| Help | |
|---|---|
| Shortcuts | Use Ctrl+↑ (Windows/Linux) or ⌘+↑ (macOS) to return to the top of the page |
| Filters | You can provide a file (--filter file) with regular expressions to suppress false positives |
| Hint 1 | Select text and use the context menu to filter / select / lookup strings |
| Hint 2 | Click on a module to filter for all events from that module. |

## Alerts

## Warnings

| | |
|---|---|
| Warning 1 | *Nov 4 08:22:32 T433-NokHangHui-COMP4071/192.168.171.128* |

No filters applied