Manvir Mann

01 November 2023

# Network Forensics

## ***Introduction***

For this project, we will be looking at memory acquisition and analysis, along with conducting network forensic analysis regarding a malware infection.

## ***Initial Setup***

We will be using OSForensics in order to acquire a live memory image and analyze it, as well as utilizing Wireshark in order to conduct a network forensic investigation.

## ***Task 1 - Step 1:***

To begin this project, we will need to open our Windows VM, and download a tool called "WinPmem".


***Step 2:***

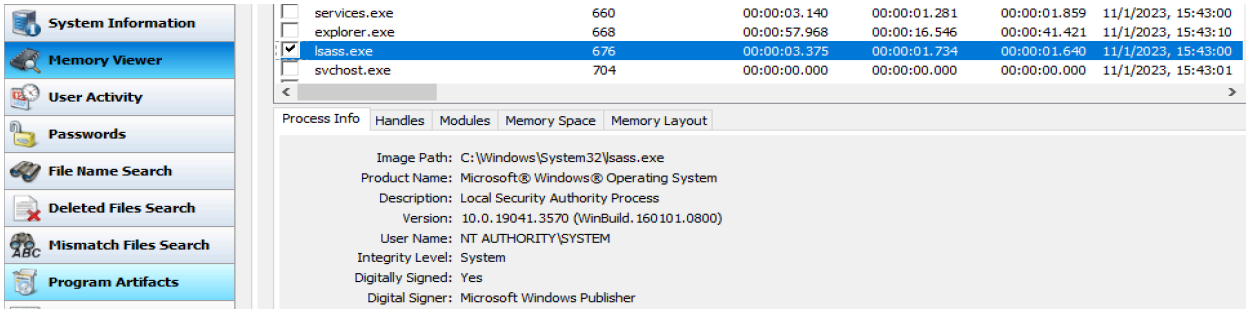
Next we will be opening a command prompt session as administrator, and changing directories to the downloads folder. From there, we can use the command “winpmem_mini_x64_rc2.exe mem.raw” to collect all of the data that we need regarding the memory on our system.

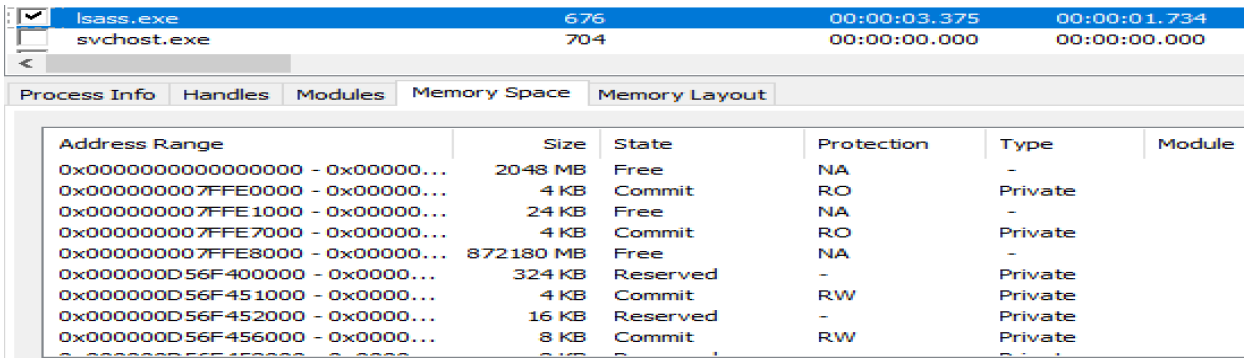
```
C:\Windows\system32>cd c:\users\manvir\Downloads

c:\Users\manvir\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is 6A2C-A1E1

 Directory of c:\Users\manvir\Downloads

11/01/2023  03:51 PM    <DIR>          .
11/01/2023  03:51 PM    <DIR>          ..
10/13/2023  03:01 PM        53,465,480 AccessData_FTK_Imager_4.7.1.exe
10/13/2023  03:16 PM        18,864,464 hw_v680.exe
10/18/2023  11:09 PM    <DIR>          HxDSetup
11/01/2023  03:50 PM     1,074,802,688 mem.raw
10/25/2023  01:55 PM    <DIR>          NSRL-256m-Autopsy
10/13/2023  03:06 PM       252,667,008 osf.exe
10/13/2023  03:11 PM    <DIR>          winhex
11/01/2023  03:44 PM           527,640 winpmem_mini_x64_rc2.exe
               5 File(s)  1,400,327,280 bytes
               5 Dir(s)   4,915,253,248 bytes free

c:\Users\manvir\Downloads>_
```

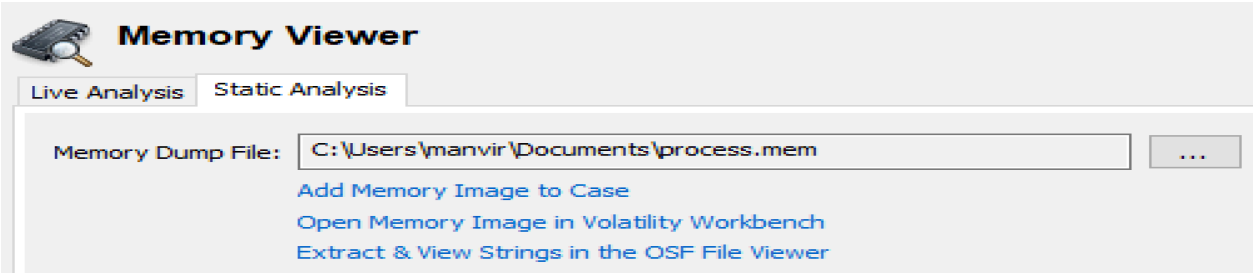
```
c:\Users\manvir\Downloads>winpmem_mini_x64_rc2.exe mem.raw
WinPmem64
Extracting driver to C:\Users\manvir\AppData\Local\Temp\pmeFDED.tmp
Driver Unloaded.
Loaded Driver C:\Users\manvir\AppData\Local\Temp\pmeFDED.tmp.
Deleting C:\Users\manvir\AppData\Local\Temp\pmeFDED.tmp
The system time is: 22:56:59
Will generate a RAW image
 - buffer_size_: 0x1000
CR3: 0x00001AA002
 4 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0xDFEED000
Start 0x100000000 - Length 0x20000000
max_physical_memory_ 0x120000000
Acquitision mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
 - length: 0x1000
```

***<u>Step 3:</u>***

Now that we have our data, we can open up OSForensics and head to the “Memory Viewer” section in the left hand pane. We want to then select the “lsass” process and analyze the information present in the process info and memory space tabs at the bottom of the screen. After viewing the present information, we can dump all the memory we want by right clicking on the process and selecting the appropriate dump button. We will save the file as “process”.

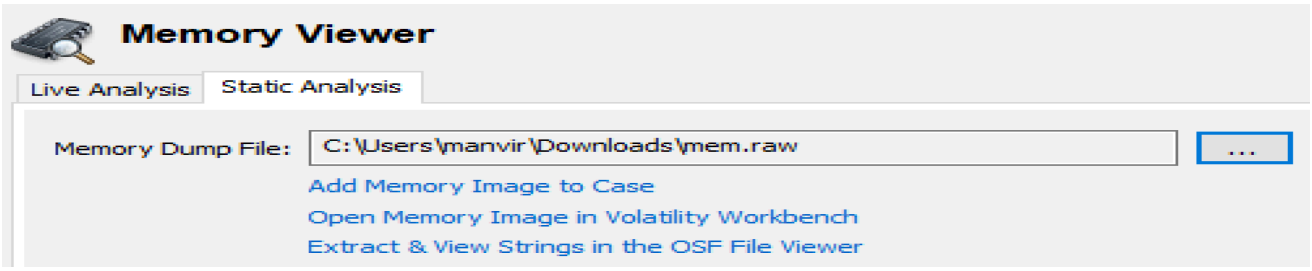


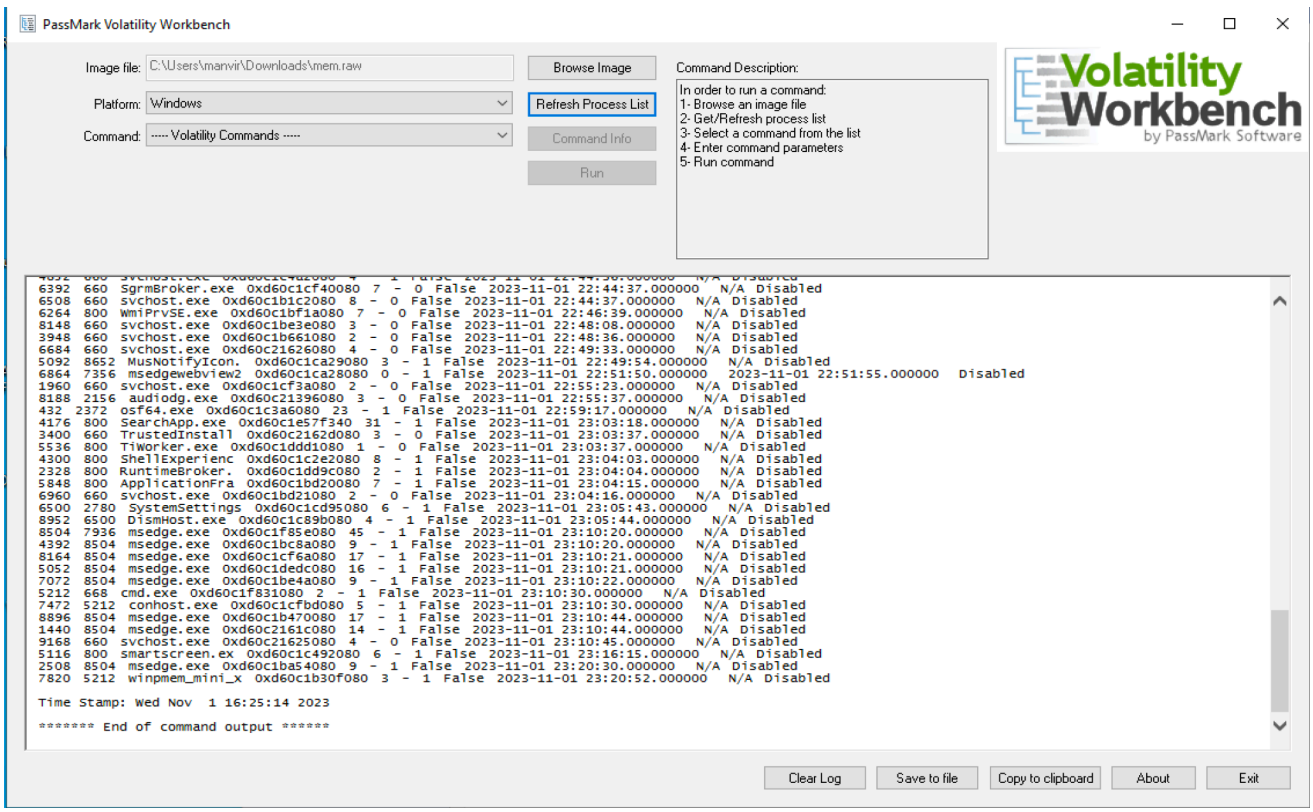




***Step 4:***

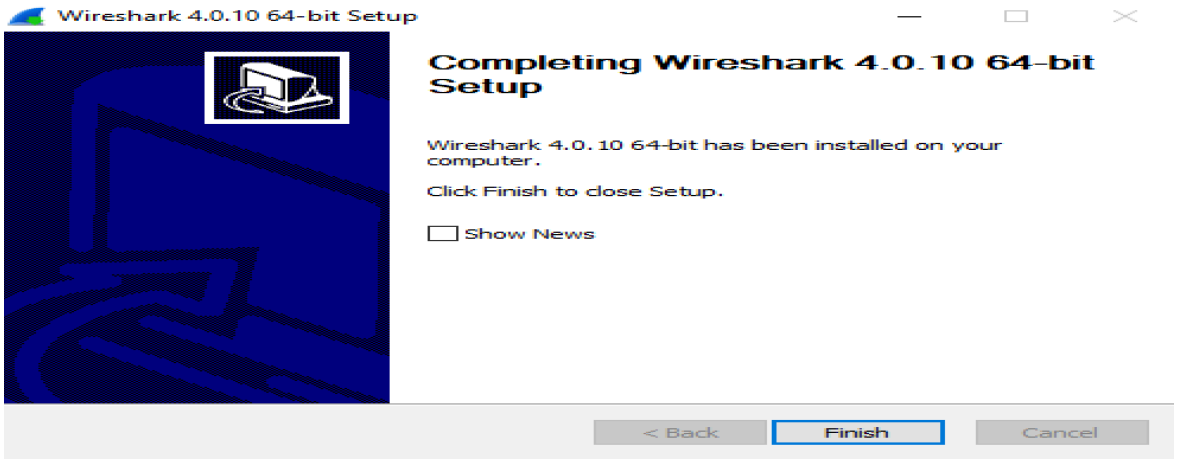
In the same tab, we want to change the directory to the previous mem.raw dump file we generated inside of our downloads folder using the winpmem tool. After that we can open ip Volatility Workbench by selecting the appropriate button, and then we can click on “Get Process List” in order to see all of the running processes at the time our snapshot was taken.



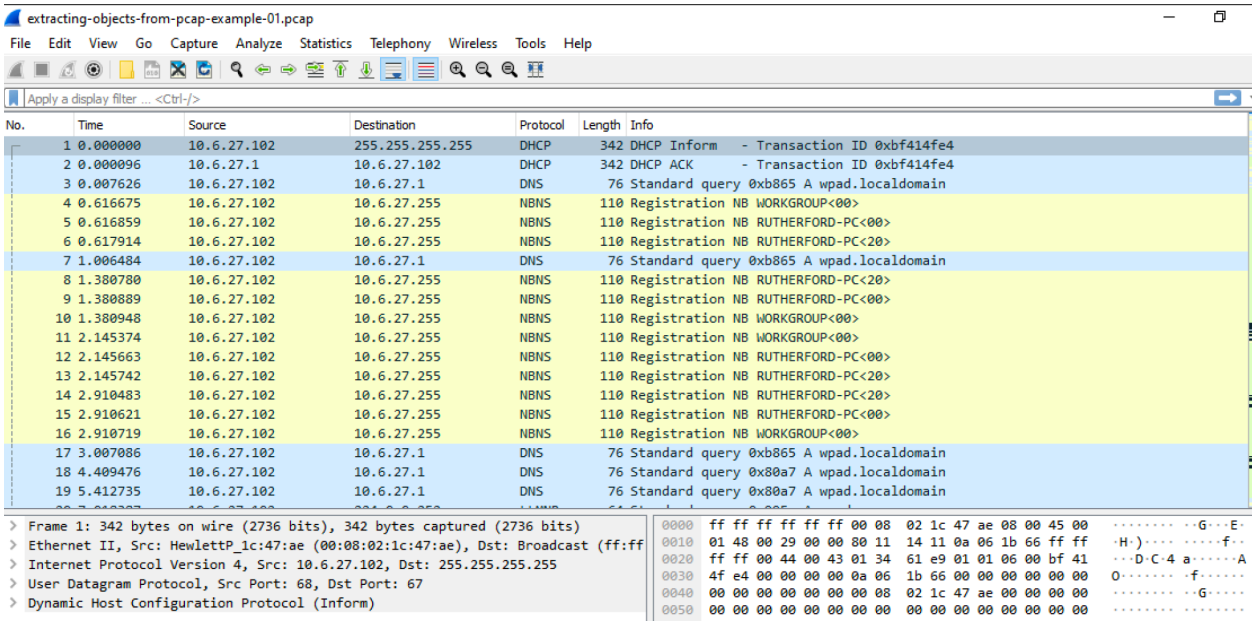

## ***Task 2 - Step 1:***

To start this step, we will first need to download Wireshark and make sure to select the Npcap settings.




***Step 2:***

From there, we will download an example pcap file from a website and extract all the files using the password “infected”. We will then launch the extracted file which will automatically launch inside of Wireshark where we are presented with a bunch of information containing IP addresses, protocols, etc.




***Step 3:***

We can then start to analyze the pcap file, one example being selecting the “Statistics” tab from the menu and selecting “Conversations”. If we then select the IPv4 - 7 tab, we can see various traffic information and addresses. If we close the tab and navigate to “Protocol Hierarchy” instead of “Conversations”, we can see various dropdowns and packet information, including that of HTTP. In Wireshark, we can further add filters such as “http” which shows that someone downloaded a word document from the IP address “107.180.50.162” to “10.6.27.102”. We can view the source address’ website link by selecting “View” in the menu, “Name Resolution” and finally “Resolve Network Addresses” which shows us that the host of the download came from “smart-fax.com”.

Wireshark · Conversations · extracting-objects-from-pcap-example-01.pcap

Conversation Settings
- Name resolution
- Absolute start time
- Limit to display filter

Ethernet · 3 | IPv4 · 7 | IPv6 | TCP · 4 | UDP · 28

| Address A | Address B | Packets | Bytes | Packets A → B | Bytes A → B | Packets B → A | Bytes B → A | Rel Start | Duration | Bits/s A → B | Bits/s B → A |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 10.6.27.1 | 10.6.27.102 | 76 | 8 kB | 8 | 2 kB | 68 | 6 kB | 0.000096 | 839.0728 | 14 bits/s | 58 bits/s |
| 10.6.27.102 | 10.6.27.255 | 42 | 5 kB | 42 | 5 kB | 0 | 0 bytes | 0.616675 | 414.3339 | 87 bits/s | 0 bits/s |
| 10.6.27.102 | 23.63.254.163 | 9 | 778 bytes | 5 | 379 bytes | 4 | 399 bytes | 14.229257 | 0.0743 | 40 kbps | 42 kbps |
| 10.6.27.102 | 23.105.131.229 | 262 | 15 kB | 89 | 6 kB | 173 | 10 kB | 59.311311 | 808.0511 | 55 bits/s | 97 bits/s |
| 10.6.27.102 | 107.180.50.162 | 1,380 | 1 MB | 424 | 24 kB | 956 | 1 MB | 29.140067 | 118.5227 | 1587 bits/s | 85 kbps |
| 10.6.27.102 | 224.0.0.252 | 18 | 1 kB | 18 | 1 kB | 0 | 0 bytes | 7.018387 | 137.3861 | 67 bits/s | 0 bits/s |
| 10.6.27.102 | 255.255.255.255 | 3 | 1 kB | 3 | 1 kB | 0 | 0 bytes | 0.000000 | 137.2738 | 59 bits/s | 0 bits/s |

Wireshark · Protocol Hierarchy Statistics · extracting-objects-from-pcap-example-01.pcap

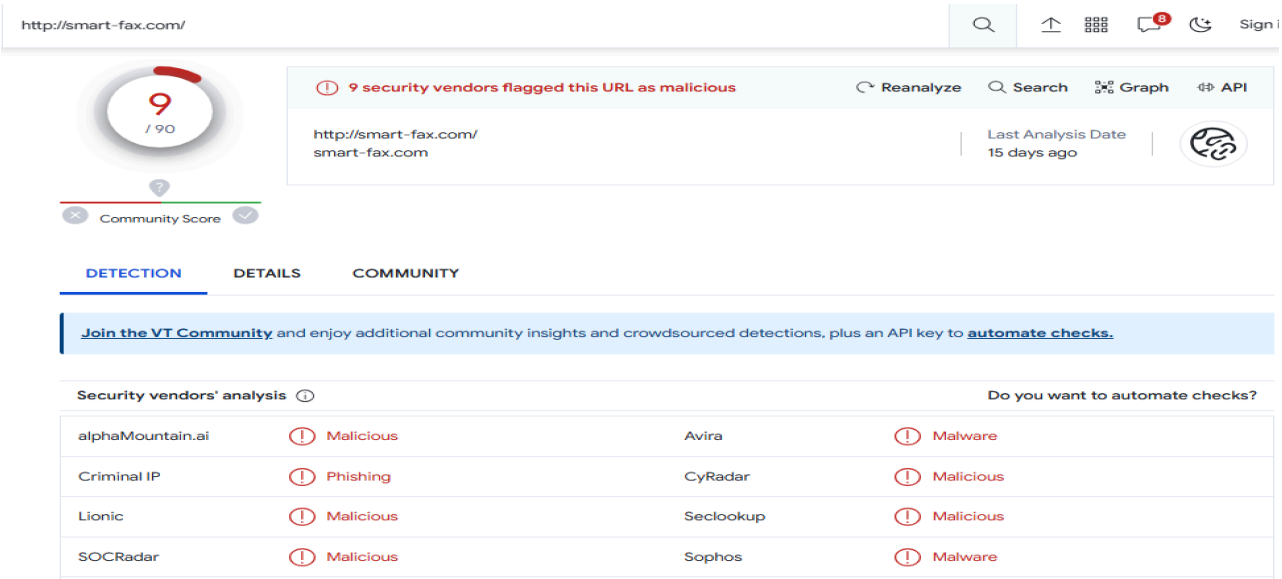
| Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets | End Bytes | Enc |
|---|---|---|---|---|---|---|---|---|
| Frame | 100.0 | 1790 | 100.0 | 1315996 | 12 k | 0 | 0 | 0 |
| Ethernet | 100.0 | 1790 | 1.9 | 25060 | 231 | 0 | 0 | 0 |
| Internet Protocol Version 4 | 100.0 | 1790 | 2.7 | 35800 | 330 | 0 | 0 | 0 |
| User Datagram Protocol | 7.8 | 139 | 0.1 | 1112 | 10 | 0 | 0 | 0 |
| NetBIOS Name Service | 4.2 | 75 | 0.3 | 4344 | 40 | 75 | 4344 | 40 |
| NetBIOS Datagram Service | 0.2 | 3 | 0.0 | 603 | 5 | 0 | 0 | 0 |
| SMB (Server Message Block Protocol) | 0.2 | 3 | 0.0 | 357 | 3 | 0 | 0 | 0 |
| SMB MailSlot Protocol | 0.2 | 3 | 0.0 | 75 | 0 | 0 | 0 | 0 |
| Microsoft Windows Browser Protocol | 0.2 | 3 | 0.0 | 99 | 0 | 3 | 99 | 0 |
| Link-local Multicast Name Resolution | 1.0 | 18 | 0.0 | 396 | 3 | 18 | 396 | 3 |
| Dynamic Host Configuration Protocol | 0.3 | 6 | 0.1 | 1800 | 16 | 6 | 1800 | 16 |
| Domain Name System | 2.1 | 37 | 0.1 | 1416 | 13 | 37 | 1416 | 13 |
| Transmission Control Protocol | 92.2 | 1651 | 94.6 | 1245465 | 11 k | 1474 | 1239491 | 11 |
| Hypertext Transfer Protocol | 0.3 | 6 | 92.0 | 1211102 | 11 k | 3 | 693 | 6 |
| Media Type | 0.1 | 2 | 209.7 | 2760192 | 25 k | 2 | 2760192 | 25 |
| Line-based text data | 0.1 | 1 | 0.0 | 14 | 0 | 1 | 14 | 0 |
| Data | 9.6 | 171 | 0.1 | 1265 | 11 | 171 | 1265 | 11 |

http

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 43 | 14.272449 | 10.6.27.102 | 23.63.254.163 | HTTP | 151 | GET /ncsi.txt HTTP/1.1 |
| 45 | 14.302997 | 23.63.254.163 | 10.6.27.102 | HTTP | 233 | HTTP/1.1 200 OK (text/plain) |
| 71 | 29.202755 | 10.6.27.102 | 107.180.50.162 | HTTP | 343 | GET /Documents/Invoice&MSO-Request.doc HTTP/1.1 |
| 337 | 33.648846 | 107.180.50.162 | 10.6.27.102 | HTTP | 162 | HTTP/1.1 200 OK (application/msword) |
| 356 | 38.470797 | 10.6.27.102 | 107.180.50.162 | HTTP | 361 | GET /knr.exe HTTP/1.1 |
| 1456 | 39.117888 | 107.180.50.162 | 10.6.27.102 | HTTP | 243 | HTTP/1.1 200 OK (application/x-msdownload) |

337 33.648846 smart-fax.com 10.6.27.102 HTTP 162 HTTP/1.1 200 OK (application/msword)

If we open up our browser and navigate to “virustotal.com”, we can enter the smart fax url which shows us the site is full of malware and malicious content.




If we select file, export objects, http, it opens up a popup that shows 2 files in which one is an .exe file, and the other a document. If we save the .exe file, Windows Defender will block it as it contains malware.