Maria Valencia

CSC 153

Lab 10

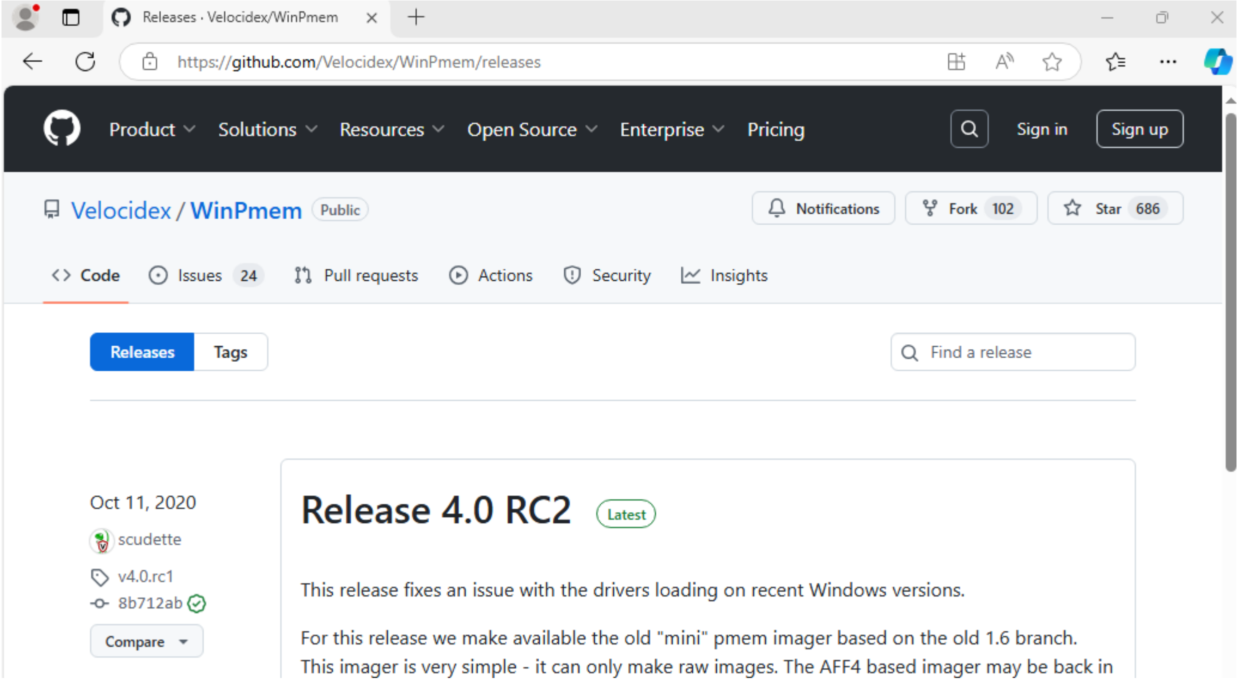
Lab 10 - VMs, Live Acquisitions, and Network Forensics

Task 1 – Windows Memory Acquistion

In this task, i will collect RAM data from a running Windows system and analyze it using OSForensics.

Step 1: Tool Setup

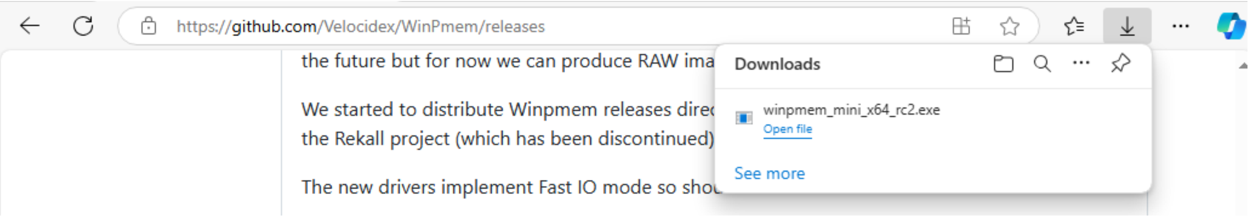
I launched my Windows VM, opened a browser and navigated to https://github.com/Velocidex/WinPmem/releases and downloaded winpmem_mini_x64_rc2.exe.



Release 4.0 RC2

This release fixes an issue with the drivers loading on recent Windows versions.

For this release we make available the old "mini" pmem imager based on the old 1.6 branch. This imager is very simple - it can only make raw images. The AFF4 based imager may be back in



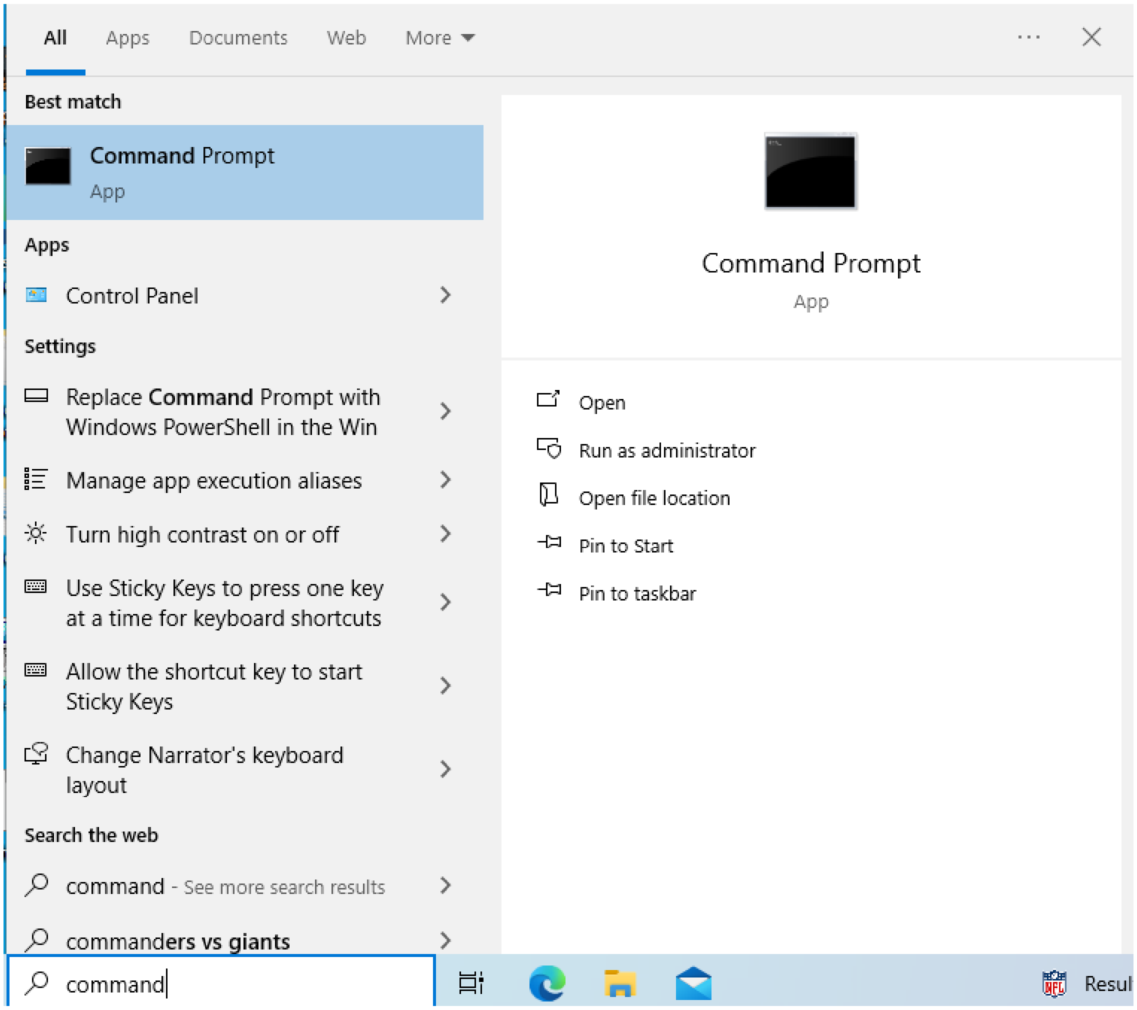
the future but for now we can produce RAW ima

We started to distribute Winpmem releases direc
the Rekall project (which has been discontinued)

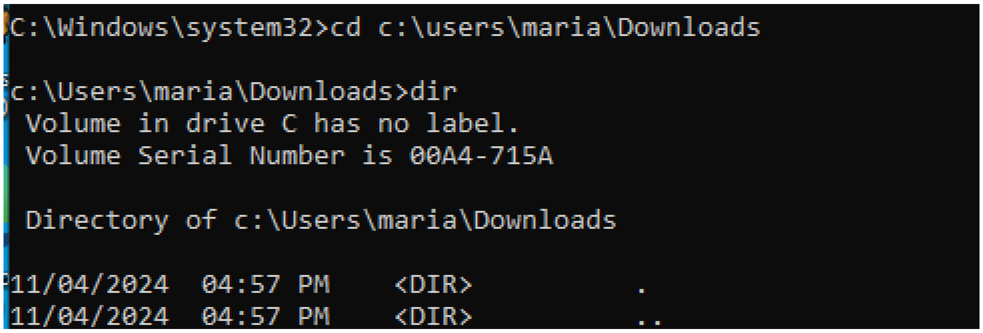
The new drivers implement Fast IO mode so shou

Step 2: Acquire Live Memory

From within the Windows VM, launch a command prompt as administrator accepting any UAC prompt.

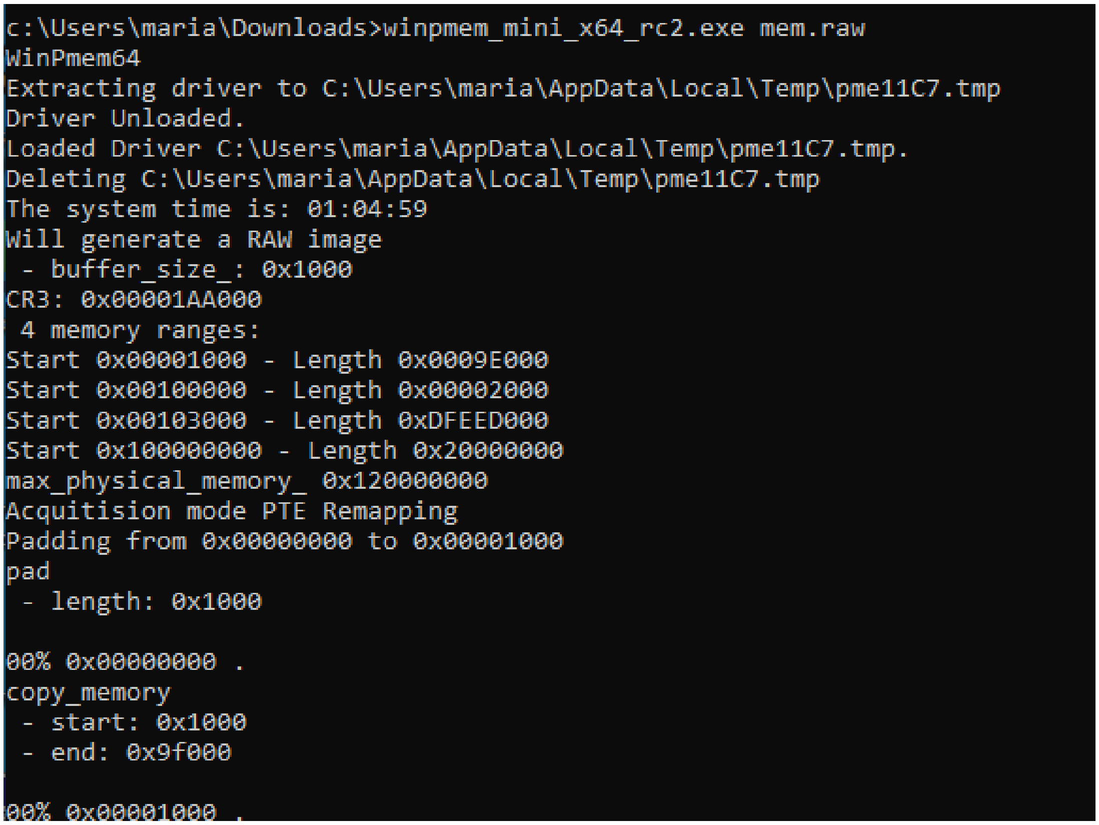

All
Apps
Documents
Web
More
Best match
Command Prompt
App
Apps
Control Panel
Settings
Replace Command Prompt with Windows PowerShell in the Win
Manage app execution aliases
Turn high contrast on or off
Use Sticky Keys to press one key at a time for keyboard shortcuts
Allow the shortcut key to start Sticky Keys
Change Narrator's keyboard layout
Search the web
command - See more search results
commanders vs giants
Command Prompt
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
command
Resul

I changed the directory to my user's downloads folder where winpmem was downloaded to.



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

c:\Users\maria\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is 00A4-715A

 Directory of c:\Users\maria\Downloads

11/04/2024  04:57 PM    <DIR>          .
11/04/2024  04:57 PM    <DIR>          ..
```

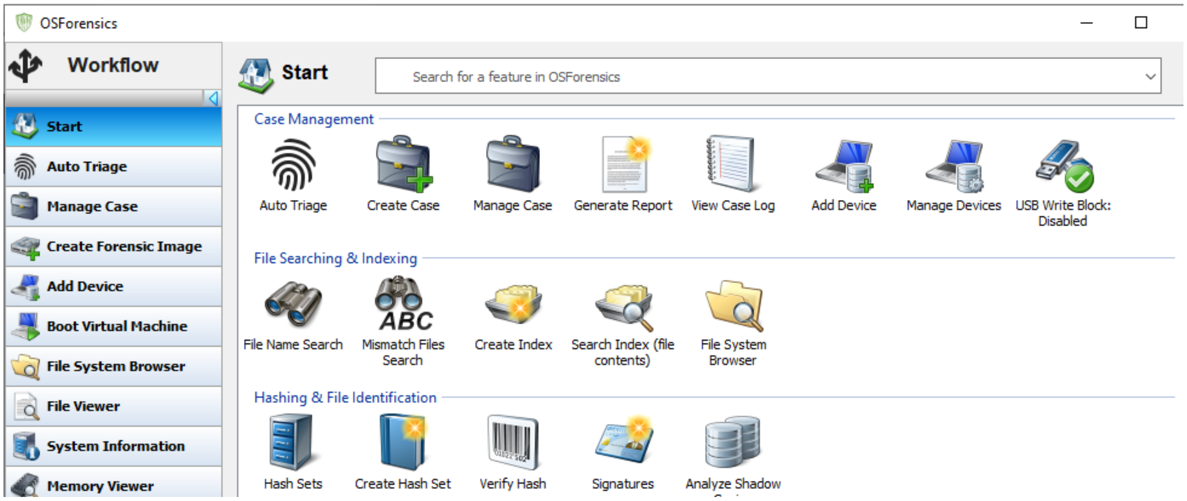
I ran winpmem and output to a mem.raw file to collect all the data in memory on the live system. This command took a few minutes to complete.



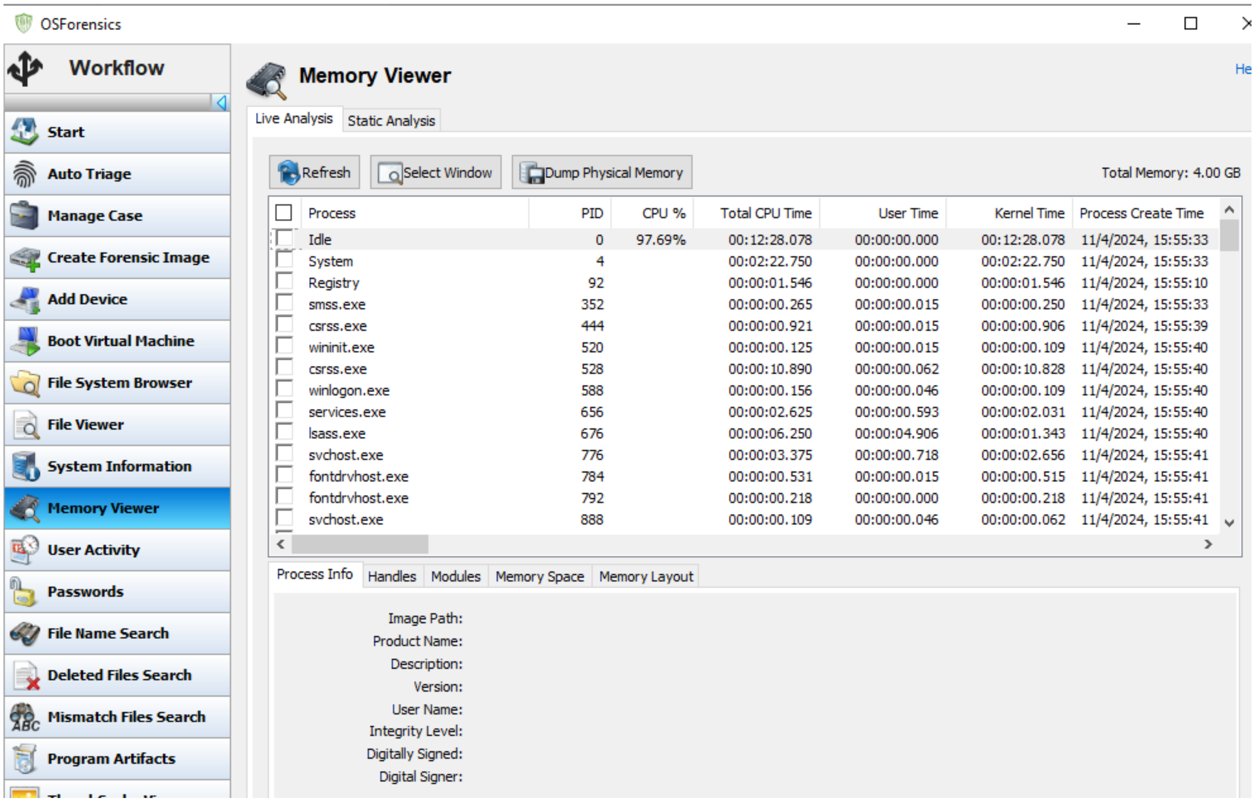
```
c:\Users\maria\Downloads>winpmem_mini_x64_rc2.exe mem.raw
WinPmem64
Extracting driver to C:\Users\maria\AppData\Local\Temp\pme11C7.tmp
Driver Unloaded.
Loaded Driver C:\Users\maria\AppData\Local\Temp\pme11C7.tmp.
Deleting C:\Users\maria\AppData\Local\Temp\pme11C7.tmp
The system time is: 01:04:59
Will generate a RAW image
 - buffer_size_: 0x1000
CR3: 0x00001AA000
 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

00% 0x00000000 .
copy_memory
 - start: 0x1000
 - end: 0x9f000

00% 0x00001000 .
```

Step 3: Live Memory Acquisition and Analysis

I launched OSForensics on the Windows VM accepting any UAC prompts. (I had to download it from https://www.osfornensics.com/download.html)



I selected the “Memory Viewer” from the left navigation pane. I observed live system processes are displayed.

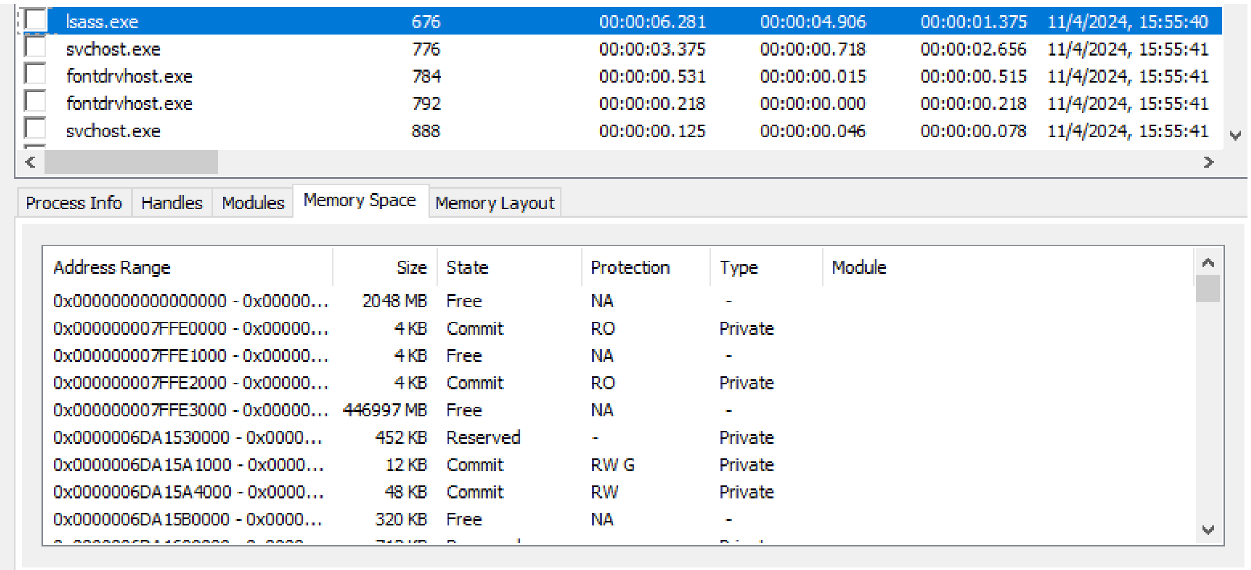


Total Memory: 4.00 GB

□ Process	PID	CPU %	Total CPU Time	User Time	Kernel Time	Process Create Time
□ Idle	0	97.69%	00:12:28.078	00:00:00.000	00:12:28.078	11/4/2024, 15:55:33
□ System	4		00:02:22.750	00:00:00.000	00:02:22.750	11/4/2024, 15:55:33
□ Registry	92		00:00:01.546	00:00:00.000	00:00:01.546	11/4/2024, 15:55:10
□ smss.exe	352		00:00:00.265	00:00:00.015	00:00:00.250	11/4/2024, 15:55:33
□ csrss.exe	444		00:00:00.921	00:00:00.015	00:00:00.906	11/4/2024, 15:55:39
□ wininit.exe	520		00:00:00.125	00:00:00.015	00:00:00.109	11/4/2024, 15:55:40
□ csrss.exe	528		00:00:10.890	00:00:00.062	00:00:10.828	11/4/2024, 15:55:40
□ winlogon.exe	588		00:00:00.156	00:00:00.046	00:00:00.109	11/4/2024, 15:55:40
□ services.exe	656		00:00:02.625	00:00:00.593	00:00:02.031	11/4/2024, 15:55:40
□ lsass.exe	676		00:00:06.250	00:00:04.906	00:00:01.343	11/4/2024, 15:55:40
□ svchost.exe	776		00:00:03.375	00:00:00.718	00:00:02.656	11/4/2024, 15:55:41
□ fontdrvhost.exe	784		00:00:00.531	00:00:00.015	00:00:00.515	11/4/2024, 15:55:41
□ fontdrvhost.exe	792		00:00:00.218	00:00:00.000	00:00:00.218	11/4/2024, 15:55:41
□ svchost.exe	888		00:00:00.109	00:00:00.046	00:00:00.062	11/4/2024, 15:55:41

Image Path:
Product Name:
Description:
Version:
User Name:
Integrity Level:
Digitally Signed:
Digital Signer:

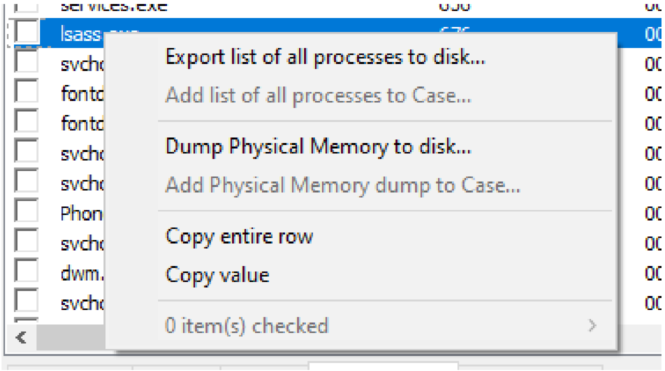
I selected the lsass process and review the Process Info and Memory Space tabs in the lower pane.

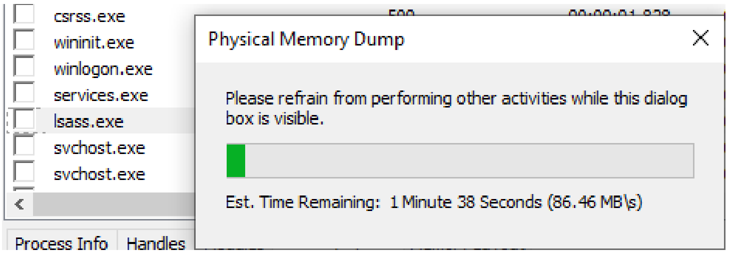


□ lsass.exe	676	00:00:06.281	00:00:04.906	00:00:01.375	11/4/2024, 15:55:40
□ svchost.exe	776	00:00:03.375	00:00:00.718	00:00:02.656	11/4/2024, 15:55:41
□ fontdrvhost.exe	784	00:00:00.531	00:00:00.015	00:00:00.515	11/4/2024, 15:55:41
□ fontdrvhost.exe	792	00:00:00.218	00:00:00.000	00:00:00.218	11/4/2024, 15:55:41
□ svchost.exe	888	00:00:00.125	00:00:00.046	00:00:00.078	11/4/2024, 15:55:41

Address Range	Size	State	Protection	Type	Module
0x0000000000000000 - 0x00000...	2048 MB	Free	NA	-	
0x000000007FFE0000 - 0x00000...	4 KB	Commit	RO	Private	
0x000000007FFE1000 - 0x00000...	4 KB	Free	NA	-	
0x000000007FFE2000 - 0x00000...	4 KB	Commit	RO	Private	
0x000000007FFE3000 - 0x00000...	446997 MB	Free	NA	-	
0x0000006DA1530000 - 0x0000...	452 KB	Reserved	-	Private	
0x0000006DA15A1000 - 0x0000...	12 KB	Commit	RW G	Private	
0x0000006DA15A4000 - 0x0000...	48 KB	Commit	RW	Private	
0x0000006DA15B0000 - 0x0000...	320 KB	Free	NA	-	

I right-clicked the selected process and select “Dump Physical Memory to disk”. Name the file “process” and hit save noting the location. This takes a couple minutes to complete.


lsass
svchc
fontc
fontc
svchc
svchc
Phon
svchc
dwm.
svchc
Export list of all processes to disk...
Add list of all processes to Case...
Dump Physical Memory to disk...
Add Physical Memory dump to Case...
Copy entire row
Copy value
0 item(s) checked



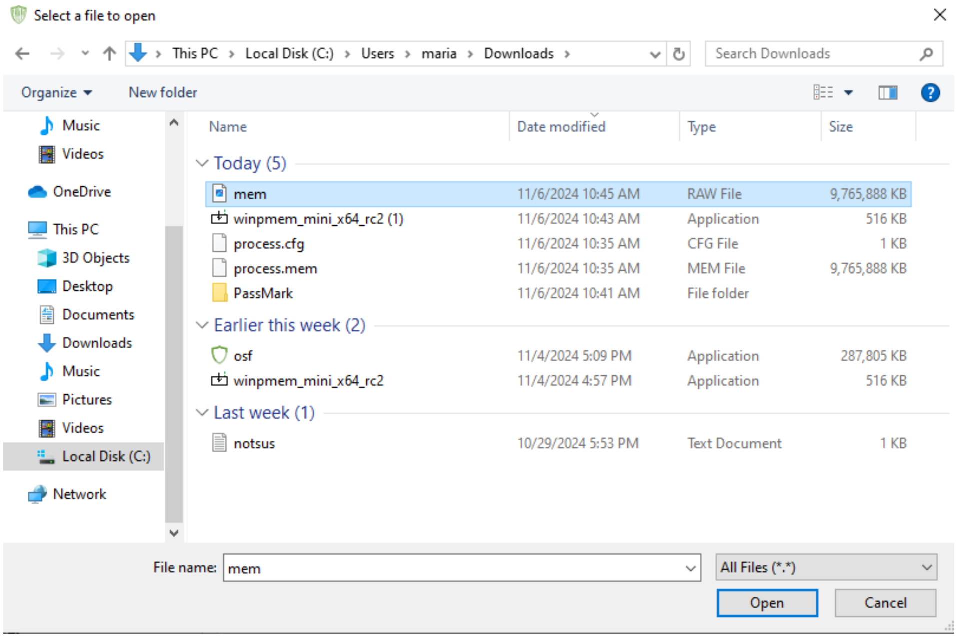
Physical Memory Dump

Please refrain from performing other activities while this dialog box is visible.

Est. Time Remaining: 1 Minute 38 Seconds (86.46 MB\s)

Step 4: Static Memory Analysis

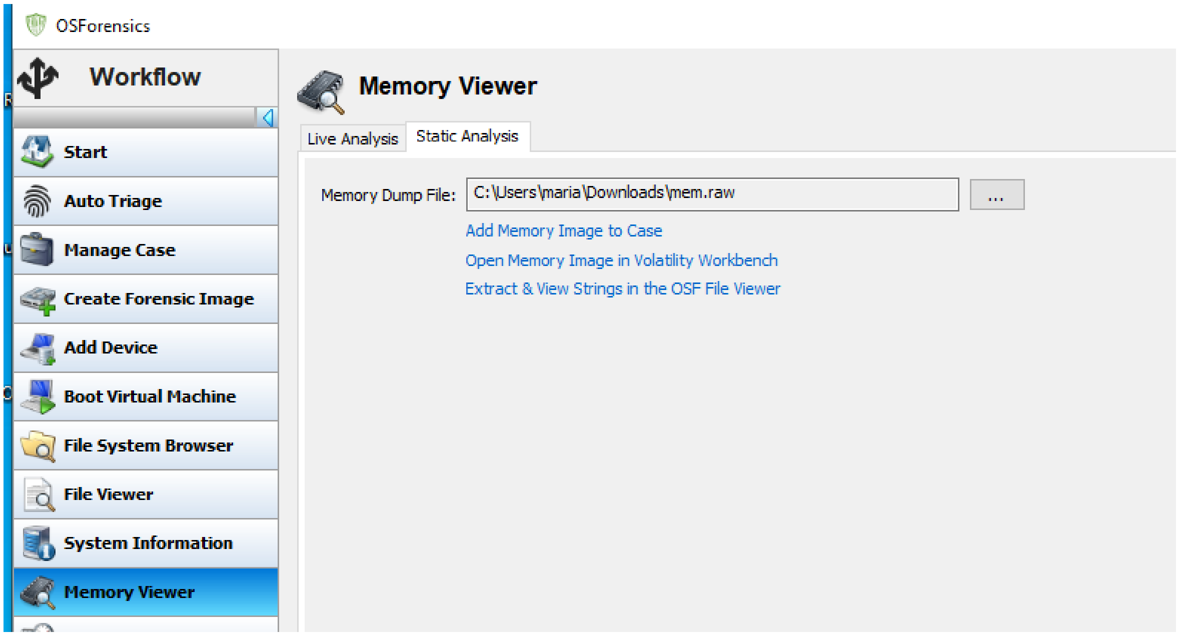
With OSForensics running on the Window VM, I navigated to the memory viewer on the left navigation menu. Selected the static analysis tab and chose the mem.raw dump file from the Downloads folder that was created with the winpmem utility.



Name	Date modified	Type	Size
Today (5)			
mem	11/6/2024 10:45 AM	RAW File	9,765,888 KB
winpmem_mini_x64_rc2 (1)	11/6/2024 10:43 AM	Application	516 KB
process.cfg	11/6/2024 10:35 AM	CFG File	1 KB
process.mem	11/6/2024 10:35 AM	MEM File	9,765,888 KB
PassMark	11/6/2024 10:41 AM	File folder	
Earlier this week (2)			
osf	11/4/2024 5:09 PM	Application	287,805 KB
winpmem_mini_x64_rc2	11/4/2024 4:57 PM	Application	516 KB
Last week (1)			
notsus	10/29/2024 5:53 PM	Text Document	1 KB

File name: mem

All Files (*.*)



Memory Dump File: C:\Users\maria\Downloads\mem.raw

With the mem.raw file selected, I pressed the “Open Memory Image in Volatility Workbench” to launch Volatility.

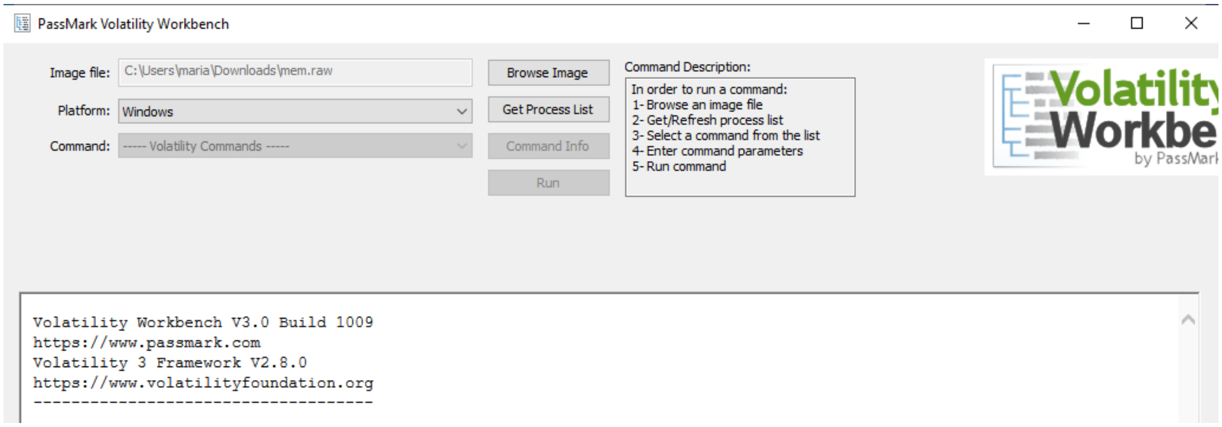


Image file: C:\Users\maria\Downloads\mem.raw

Platform: Windows

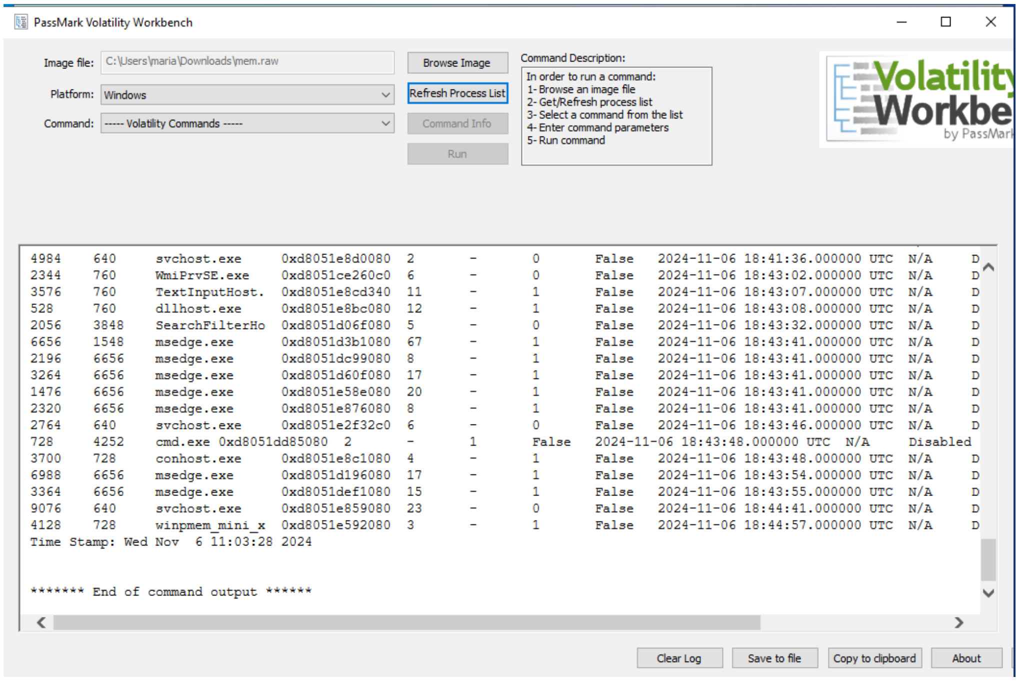
Command: ----- Volatility Commands -----

Command Description:

In order to run a command:
1- Browse an image file
2- Get/Refresh process list
3- Select a command from the list
4- Enter command parameters
5- Run command

```
Volatility Workbench V3.0 Build 1009
https://www.passmark.com
Volatility 3 Framework V2.8.0
https://www.volatilityfoundation.org
------------------------------------
```

I pressed the “Get Process List” button in Volatility Workbench and observe the command’s progress at the bottom of the window.


PassMark Volatility Workbench
Image file: C:\Users\maria\Downloads\mem.raw
Platform: Windows
Command: ----- Volatility Commands -----
Browse Image
Refresh Process List
Command Info
Run
Command Description:
In order to run a command:
1- Browse an image file
2- Get/Refresh process list
3- Select a command from the list
4- Enter command parameters
5- Run command
Volatility Workbe
by PassMar
Clear Log
Save to file
Copy to clipboard
About

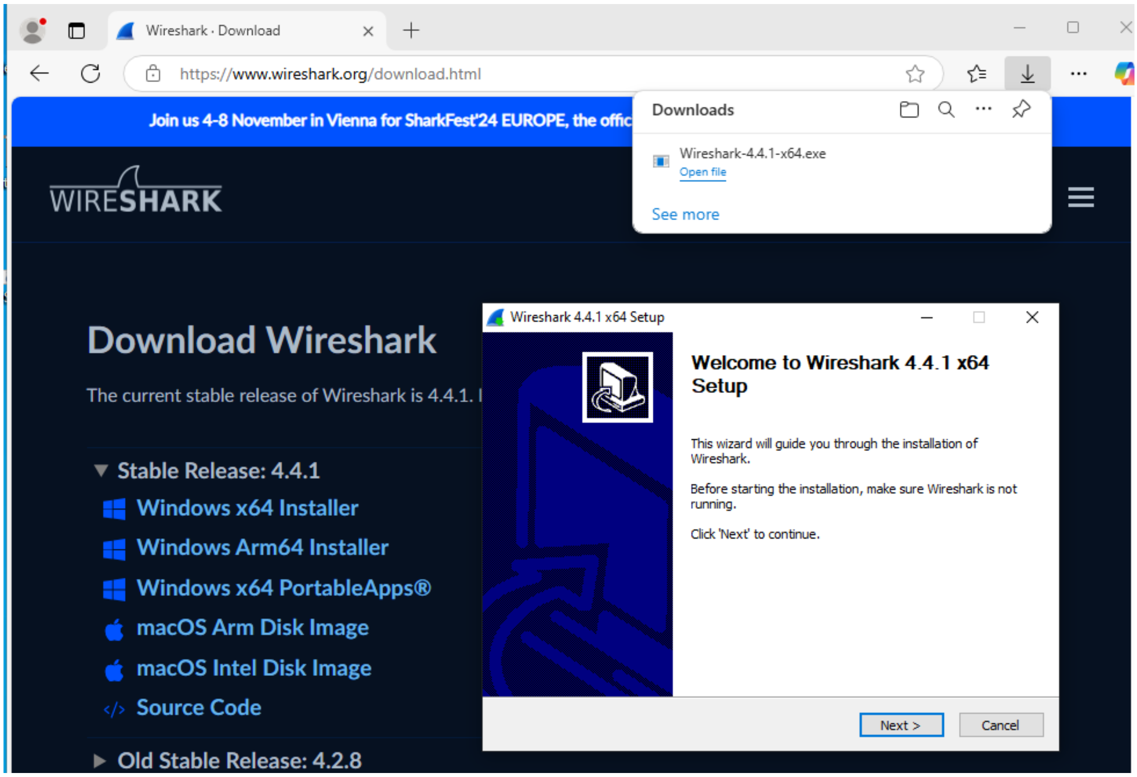
```
4984    640     svchost.exe     0xd8051e8d0080  2       -       0       False   2024-11-06 18:41:36.000000 UTC  N/A     D
2344    760     WmiPrvSE.exe    0xd8051ce260c0  6       -       0       False   2024-11-06 18:43:02.000000 UTC  N/A     D
3576    760     TextInputHost.  0xd8051e8cd340  11      -       1       False   2024-11-06 18:43:07.000000 UTC  N/A     D
528     760     dllhost.exe     0xd8051e8bc080  12      -       1       False   2024-11-06 18:43:08.000000 UTC  N/A     D
2056    3848    SearchFilterHo  0xd8051d06f080  5       -       0       False   2024-11-06 18:43:32.000000 UTC  N/A     D
6656    1548    msedge.exe      0xd8051d3b1080  67      -       1       False   2024-11-06 18:43:41.000000 UTC  N/A     D
2196    6656    msedge.exe      0xd8051dc99080  8       -       1       False   2024-11-06 18:43:41.000000 UTC  N/A     D
3264    6656    msedge.exe      0xd8051d60f080  17      -       1       False   2024-11-06 18:43:41.000000 UTC  N/A     D
1476    6656    msedge.exe      0xd8051e58e080  20      -       1       False   2024-11-06 18:43:41.000000 UTC  N/A     D
2320    6656    msedge.exe      0xd8051e876080  8       -       1       False   2024-11-06 18:43:41.000000 UTC  N/A     D
2764    640     svchost.exe     0xd8051e2f32c0  6       -       0       False   2024-11-06 18:43:46.000000 UTC  N/A     D
728     4252    cmd.exe 0xd8051dd85080  2       -       1       False   2024-11-06 18:43:48.000000 UTC  N/A     Disabled
3700    728     conhost.exe     0xd8051e8c1080  4       -       1       False   2024-11-06 18:43:48.000000 UTC  N/A     D
6988    6656    msedge.exe      0xd8051d196080  17      -       1       False   2024-11-06 18:43:54.000000 UTC  N/A     D
3364    6656    msedge.exe      0xd8051def1080  15      -       1       False   2024-11-06 18:43:55.000000 UTC  N/A     D
9076    640     svchost.exe     0xd8051e859080  23      -       0       False   2024-11-06 18:44:41.000000 UTC  N/A     D
4128    728     winpmem_mini_x  0xd8051e592080  3       -       1       False   2024-11-06 18:44:57.000000 UTC  N/A     D
Time Stamp: Wed Nov  6 11:03:28 2024


******* End of command output ******
```

Task 2 – Network Forensic Investigation

I will now analyze packet captures using Wireshark in my Windows VM in this task.

Step 1: Install Wireshark

I launched my windows VM and downloaded the Wireshark x64 installer from https://www.wireshark.org/download.html .



Join us 4-8 November in Vienna for SharkFest'24 EUROPE, the offic

Download Wireshark

The current stable release of Wireshark is 4.4.1.

▼ Stable Release: 4.4.1
- Windows x64 Installer
- Windows Arm64 Installer
- Windows x64 PortableApps®
- macOS Arm Disk Image
- macOS Intel Disk Image
- Source Code

▶ Old Stable Release: 4.2.8

Wireshark 4.4.1 x64 Setup

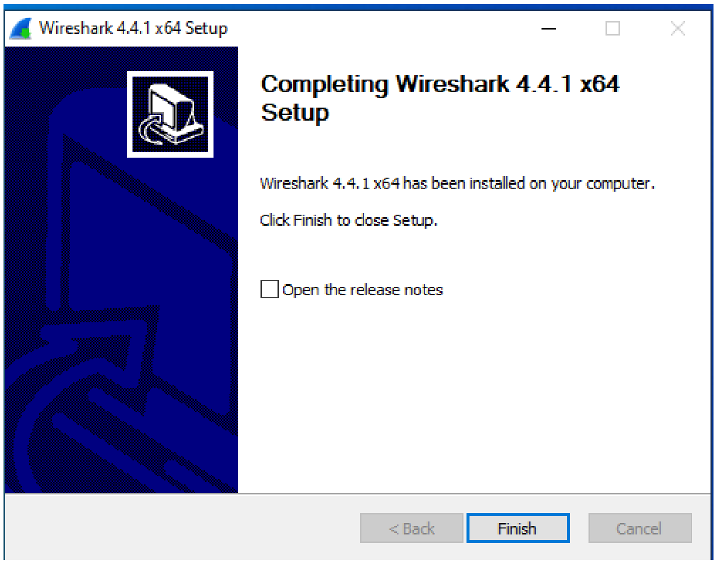
Welcome to Wireshark 4.4.1 x64 Setup

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

I kept the default settings.



Wireshark 4.4.1 x64 Setup

Completing Wireshark 4.4.1 x64 Setup

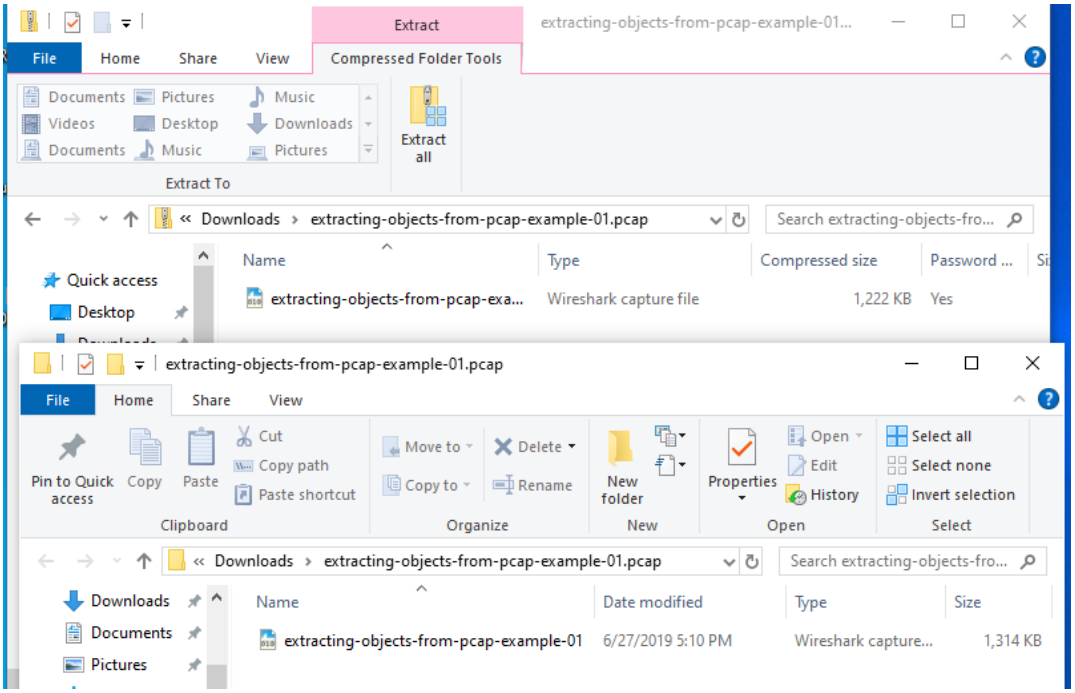
Wireshark 4.4.1 x64 has been installed on your computer.

Click Finish to close Setup.

□ Open the release notes

Step 2: Download Sample PCAP

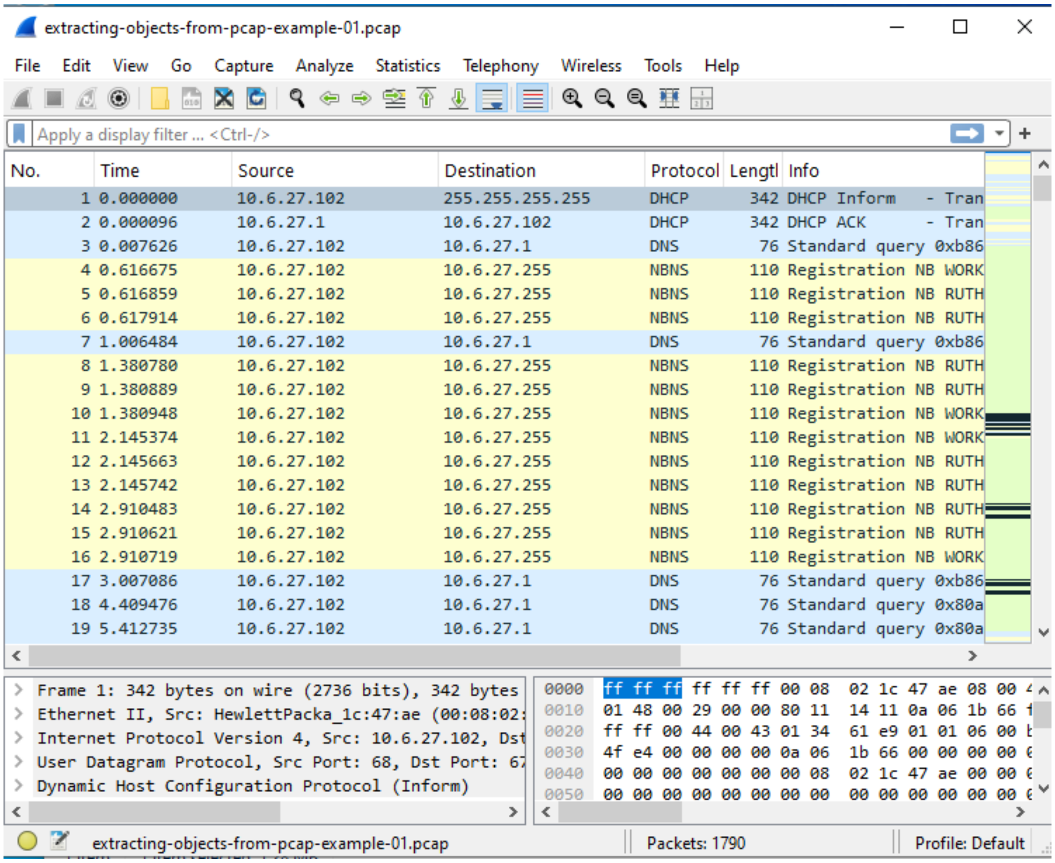
With wireshark installed, I opened the windows VM browser and navigated to https://www.malware-traffic-analysis.net/training/exporting-objects.html and download the “extracting-objects-from-pcap-example-01.pcap.zip” file. (my browser didn't allow me to do so) However, I downloaded it from canvas.



Name	Type	Compressed size	Password ...	Si
extracting-objects-from-pcap-exa...	Wireshark capture file	1,222 KB	Yes	

Name	Date modified	Type	Size
extracting-objects-from-pcap-example-01	6/27/2019 5:10 PM	Wireshark capture...	1,314 KB

I double clicked the extracted PCAP file which automatically opened in Wireshark.


extracting-objects-from-pcap-example-01.pcap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

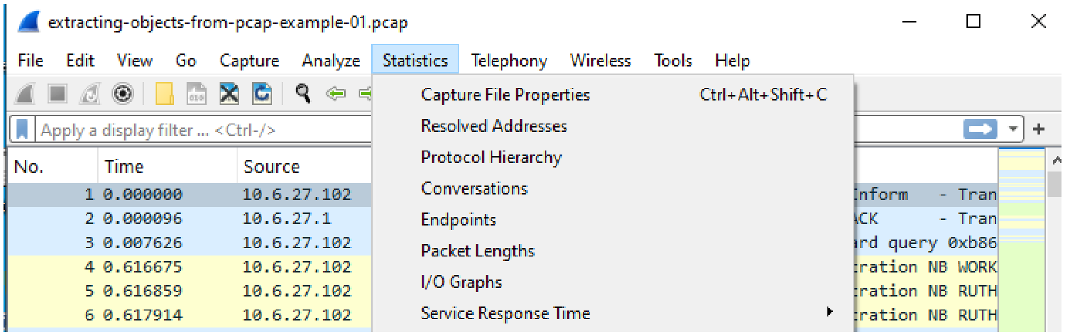
```
No.  Time        Source        Destination      Protocol Lengtl Info
   1 0.000000    10.6.27.102   255.255.255.255  DHCP      342 DHCP Inform   - Tran
   2 0.000096    10.6.27.1     10.6.27.102      DHCP      342 DHCP ACK      - Tran
   3 0.007626    10.6.27.102   10.6.27.1        DNS        76 Standard query 0xb86
   4 0.616675    10.6.27.102   10.6.27.255      NBNS      110 Registration NB WORK
   5 0.616859    10.6.27.102   10.6.27.255      NBNS      110 Registration NB RUTH
   6 0.617914    10.6.27.102   10.6.27.255      NBNS      110 Registration NB RUTH
   7 1.006484    10.6.27.102   10.6.27.1        DNS        76 Standard query 0xb86
   8 1.380780    10.6.27.102   10.6.27.255      NBNS      110 Registration NB RUTH
   9 1.380889    10.6.27.102   10.6.27.255      NBNS      110 Registration NB RUTH
  10 1.380948    10.6.27.102   10.6.27.255      NBNS      110 Registration NB WORK
  11 2.145374    10.6.27.102   10.6.27.255      NBNS      110 Registration NB WORK
  12 2.145663    10.6.27.102   10.6.27.255      NBNS      110 Registration NB RUTH
  13 2.145742    10.6.27.102   10.6.27.255      NBNS      110 Registration NB RUTH
  14 2.910483    10.6.27.102   10.6.27.255      NBNS      110 Registration NB RUTH
  15 2.910621    10.6.27.102   10.6.27.255      NBNS      110 Registration NB RUTH
  16 2.910719    10.6.27.102   10.6.27.255      NBNS      110 Registration NB WORK
  17 3.007086    10.6.27.102   10.6.27.1        DNS        76 Standard query 0xb86
  18 4.409476    10.6.27.102   10.6.27.1        DNS        76 Standard query 0x80a
  19 5.412735    10.6.27.102   10.6.27.1        DNS        76 Standard query 0x80a
```

```
> Frame 1: 342 bytes on wire (2736 bits), 342 bytes
> Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:
> Internet Protocol Version 4, Src: 10.6.27.102, Dst
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Inform)
```

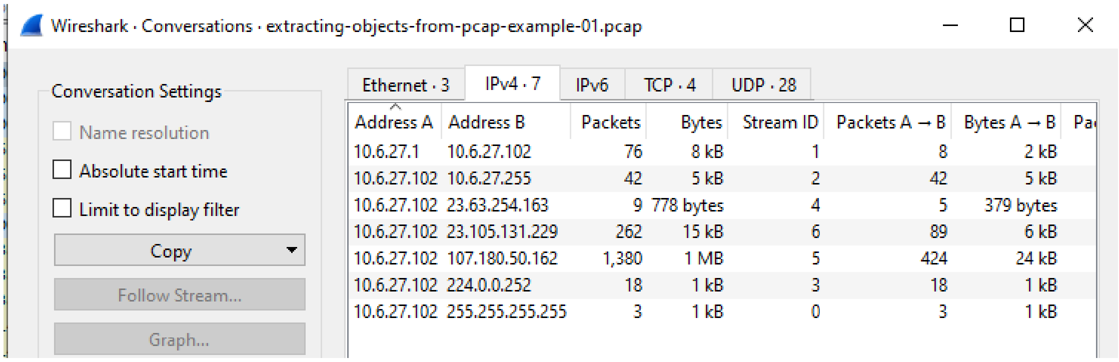
```
0000  ff ff ff ff ff ff 00 08  02 1c 47 ae 08 00 4
0010  01 48 00 29 00 00 80 11  14 11 0a 06 1b 66 f
0020  ff ff 00 44 00 43 01 34  61 e9 01 01 06 00 b
0030  4f e4 00 00 00 00 0a 06  1b 66 00 00 00 00 0
0040  00 00 00 00 00 00 00 08  02 1c 47 ae 00 00 0
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 0
```

Step 3: Analyze the PCAP

With Wireshark launched and the sample PCAP file loaded, I selected Statistics from the menu bar and Conversations. I selected the IPv4 and observed the addresses, packet counts and byte sizes of the PCAP.

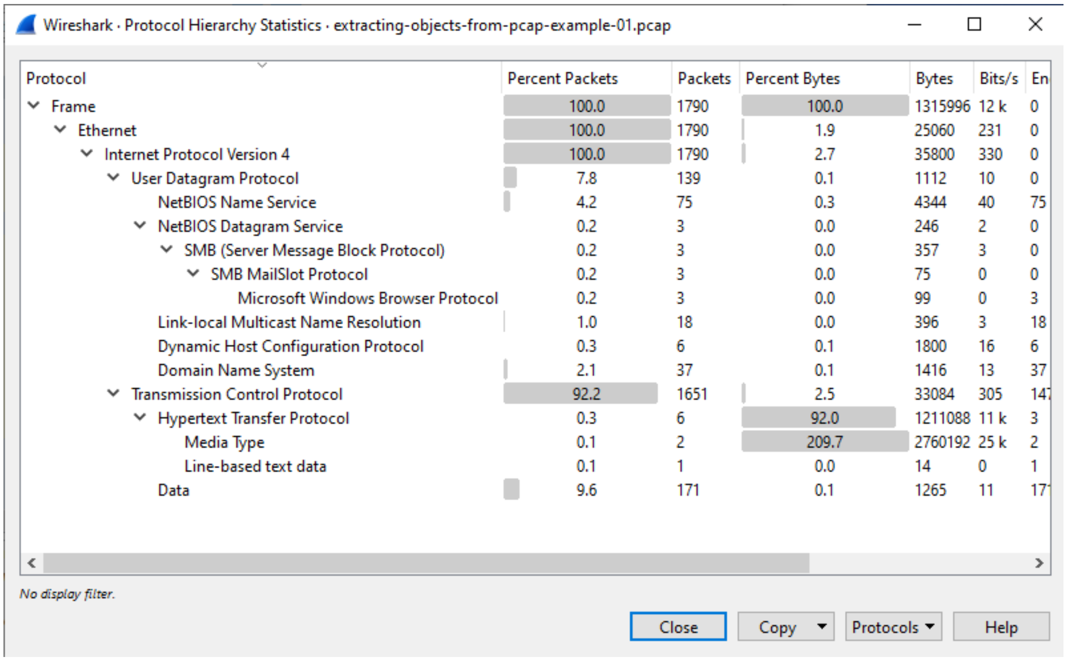


```
No.  Time        Source           Info
   1 0.000000    10.6.27.102      Inform   - Tran
   2 0.000096    10.6.27.1        CK       - Tran
   3 0.007626    10.6.27.102      rd query 0xb86
   4 0.616675    10.6.27.102      ration NB WORK
   5 0.616859    10.6.27.102      ration NB RUTH
   6 0.617914    10.6.27.102      ration NB RUTH
```



Address A	Address B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Pa
10.6.27.1	10.6.27.102	76	8 kB	1	8	2 kB	
10.6.27.102	10.6.27.255	42	5 kB	2	42	5 kB	
10.6.27.102	23.63.254.163	9	778 bytes	4	5	379 bytes	
10.6.27.102	23.105.131.229	262	15 kB	6	89	6 kB	
10.6.27.102	107.180.50.162	1,380	1 MB	5	424	24 kB	
10.6.27.102	224.0.0.252	18	1 kB	3	18	1 kB	
10.6.27.102	255.255.255.255	3	1 kB	0	3	1 kB	

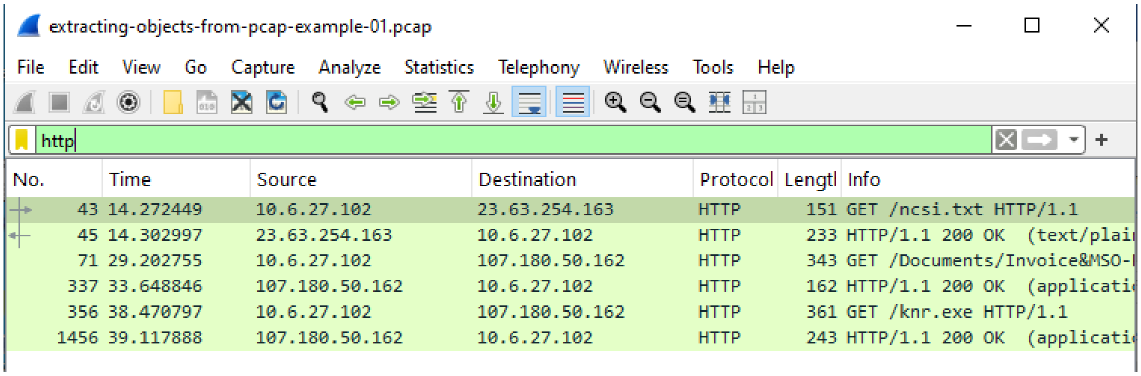
I selected statistics from the menu and chose Protocol Hierarchy. I observed the protocol statistics summary includes HTTP traffic and closed the summary window.


Wireshark · Protocol Hierarchy Statistics · extracting-objects-from-pcap-example-01.pcap
Close
Copy
Protocols
Help

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	En
Frame	100.0	1790	100.0	1315996	12 k	0
Ethernet	100.0	1790	1.9	25060	231	0
Internet Protocol Version 4	100.0	1790	2.7	35800	330	0
User Datagram Protocol	7.8	139	0.1	1112	10	0
NetBIOS Name Service	4.2	75	0.3	4344	40	75
NetBIOS Datagram Service	0.2	3	0.0	246	2	0
SMB (Server Message Block Protocol)	0.2	3	0.0	357	3	0
SMB MailSlot Protocol	0.2	3	0.0	75	0	0
Microsoft Windows Browser Protocol	0.2	3	0.0	99	0	3
Link-local Multicast Name Resolution	1.0	18	0.0	396	3	18
Dynamic Host Configuration Protocol	0.3	6	0.1	1800	16	6
Domain Name System	2.1	37	0.1	1416	13	37
Transmission Control Protocol	92.2	1651	2.5	33084	305	147
Hypertext Transfer Protocol	0.3	6	92.0	1211088	11 k	3
Media Type	0.1	2	209.7	2760192	25 k	2
Line-based text data	0.1	1	0.0	14	0	1
Data	9.6	171	0.1	1265	11	17

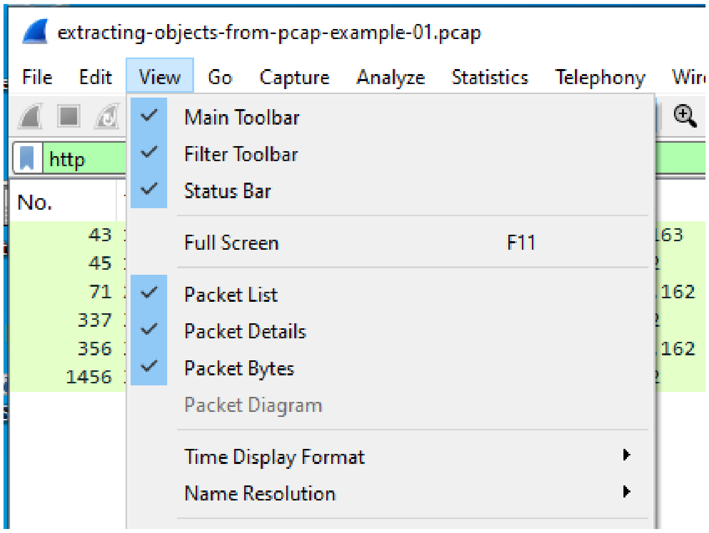
No display filter.

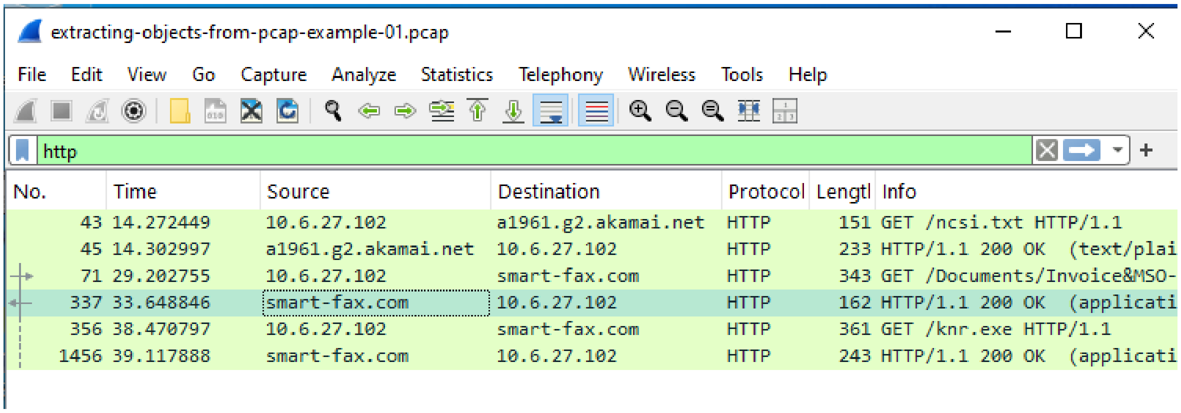
I displayed only HTTP traffic by using the HTTP filter. I observed that a word document appears to have been downloaded from 107.180.50.162 to 10.6.27.102.



No.	Time	Source	Destination	Protocol	Lengtl	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/plai
71	29.202755	10.6.27.102	107.180.50.162	HTTP	343	GET /Documents/Invoice&MSO-I
337	33.648846	107.180.50.162	10.6.27.102	HTTP	162	HTTP/1.1 200 OK (applicati
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 (applicati

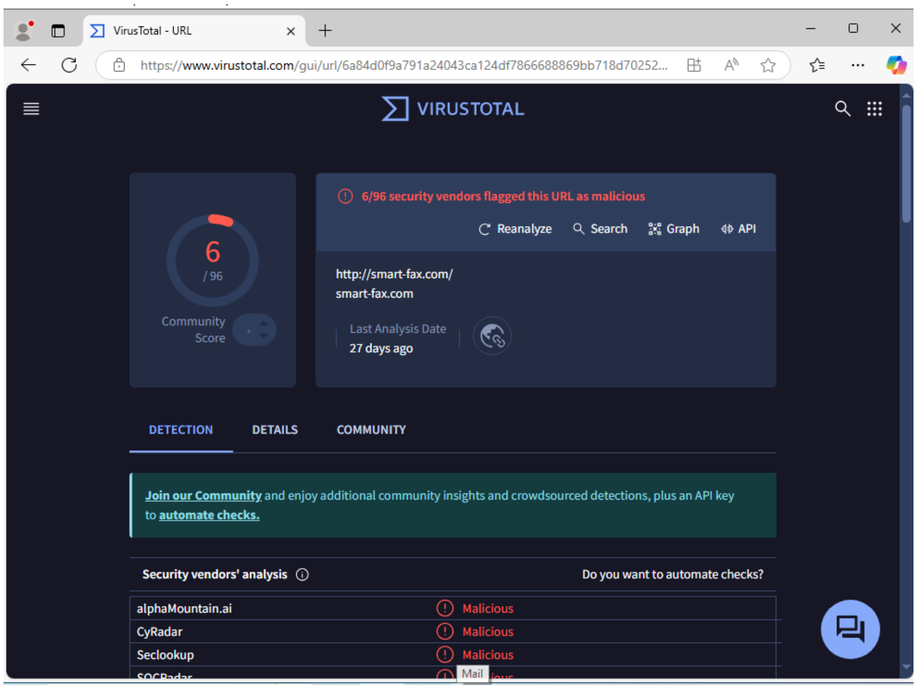
I set the IP resolution by selecting View from the menu bar, Name resolution, and then Resolve Network Addresses. I observed that the 107.180.50.162 address was resolved to “smart-fax.com”!





No.	Time	Source	Destination	Protocol	Lengtl	Info
43	14.272449	10.6.27.102	a1961.g2.akamai.net	HTTP	151	GET /ncsi.txt HTTP/1.1
45	14.302997	a1961.g2.akamai.net	10.6.27.102	HTTP	233	HTTP/1.1 200 OK (text/plai
71	29.202755	10.6.27.102	smart-fax.com	HTTP	343	GET /Documents/Invoice&MSO-
337	33.648846	smart-fax.com	10.6.27.102	HTTP	162	HTTP/1.1 200 OK (applicati
356	38.470797	10.6.27.102	smart-fax.com	HTTP	361	GET /knr.exe HTTP/1.1
1456	39.117888	smart-fax.com	10.6.27.102	HTTP	243	HTTP/1.1 200 OK (applicati

I returned to my Windows VM web browser and navigated to virustotal.com, select URL, enter “smart-fax.com” and press enter. I observed several vendors flagged this domain as malicious!



6/96 security vendors flagged this URL as malicious

http://smart-fax.com/
smart-fax.com

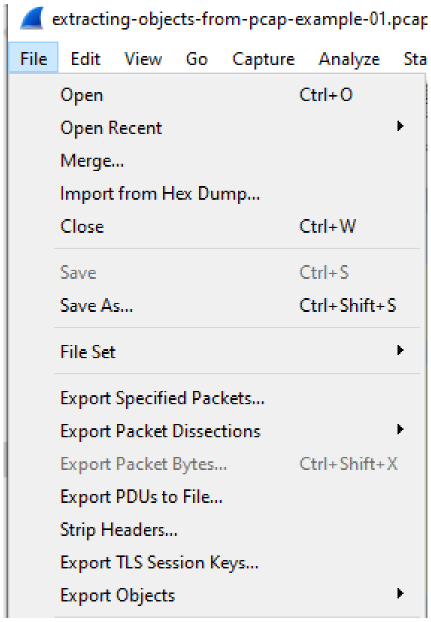
Last Analysis Date
27 days ago

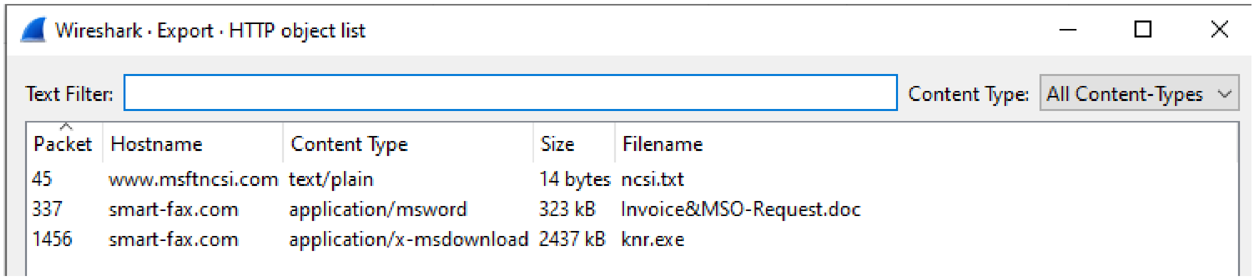
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis | Do you want to automate checks?

alphaMountain.ai	Malicious
CyRadar	Malicious
Seclookup	Malicious
SOCRadar	

I returned to Wireshark to extract the suspected malware. I selected file from the menu bar, Export Objects, and then HTTP. I observed that there are two interesting files, one is a DOC and the other an EXE.



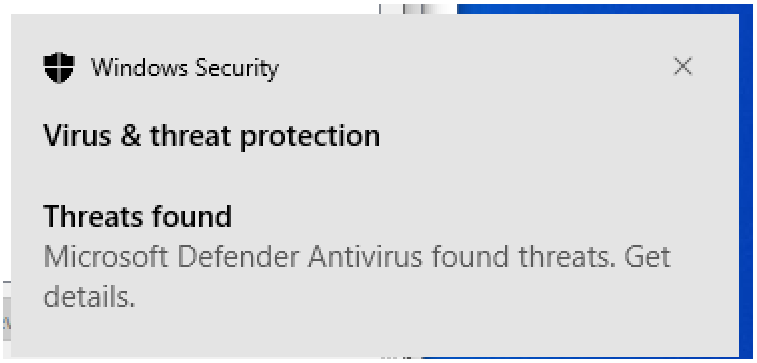


Text Filter:

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
45	www.msftncsi.com	text/plain	14 bytes	ncsi.txt
337	smart-fax.com	application/msword	323 kB	Invoice&MSO-Request.doc
1456	smart-fax.com	application/x-msdownload	2437 kB	knr.exe

While in the Export dialog window, selected the “knr.exe” file, pressed Save, and chose a location. I observed that Windows Defender detected this file as malware and blocked its writing to disc!



Virus & threat protection

Threats found

Microsoft Defender Antivirus found threats. Get details.