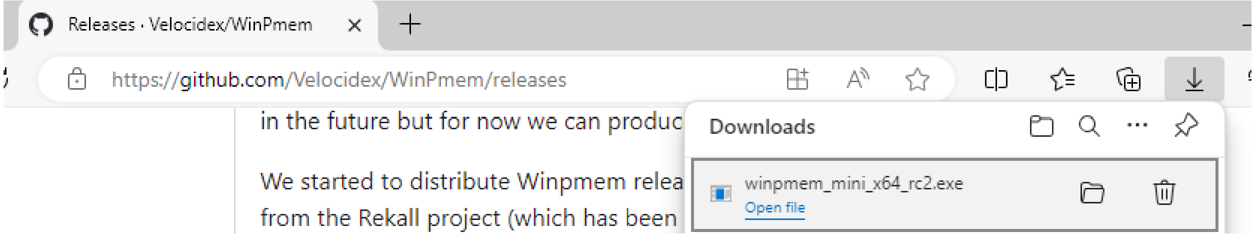
Task 1: Windows Memory Acquisition

Step 1: Tool Setup

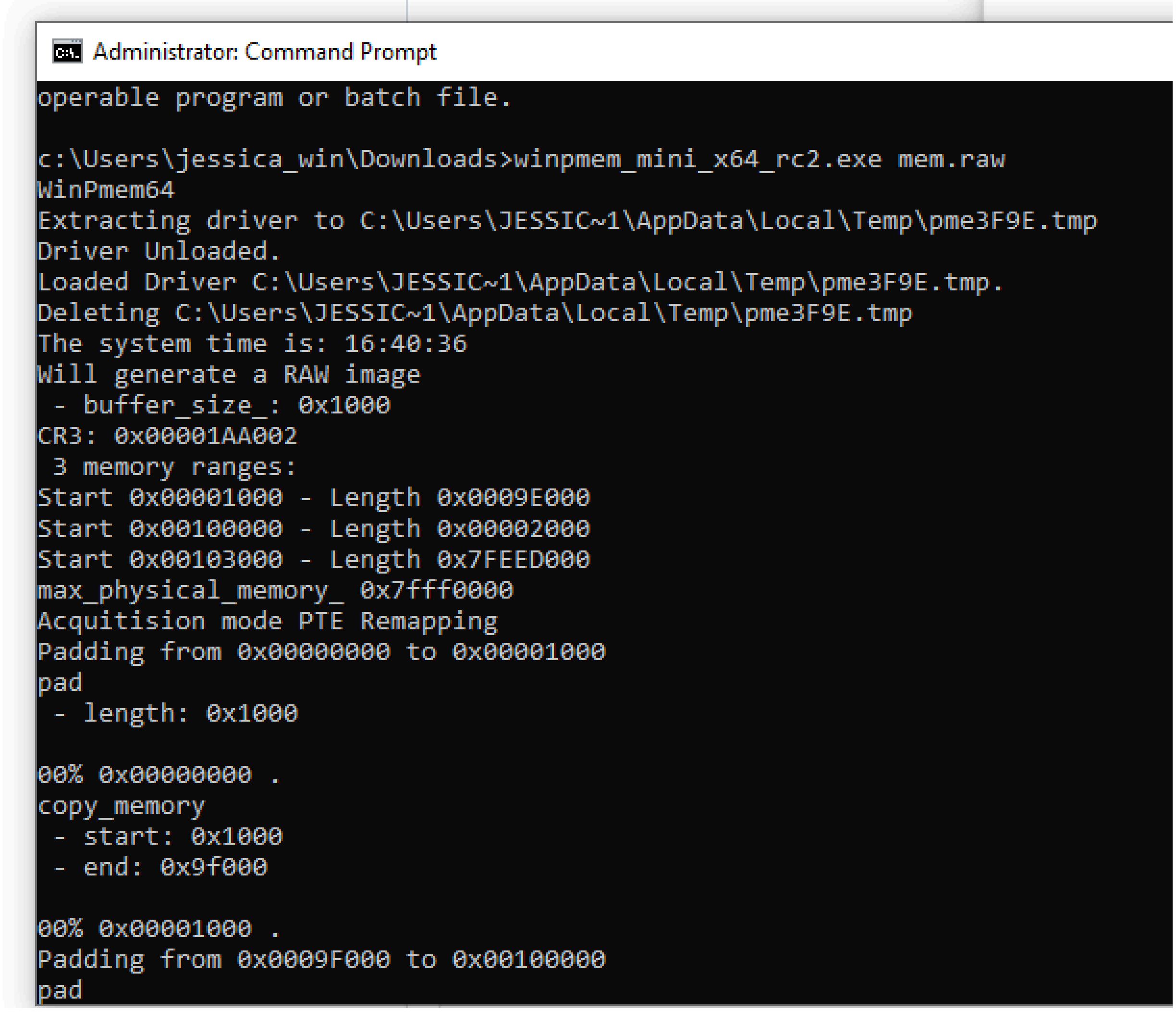

Releases · Velocidex/WinPmem
https://github.com/Velocidex/WinPmem/releases
Downloads
winpmem_mini_x64_rc2.exe
Open file

in the future but for now we can produc

We started to distribute Winpmem relea
from the Rekall project (which has been

Downloaded executable file.

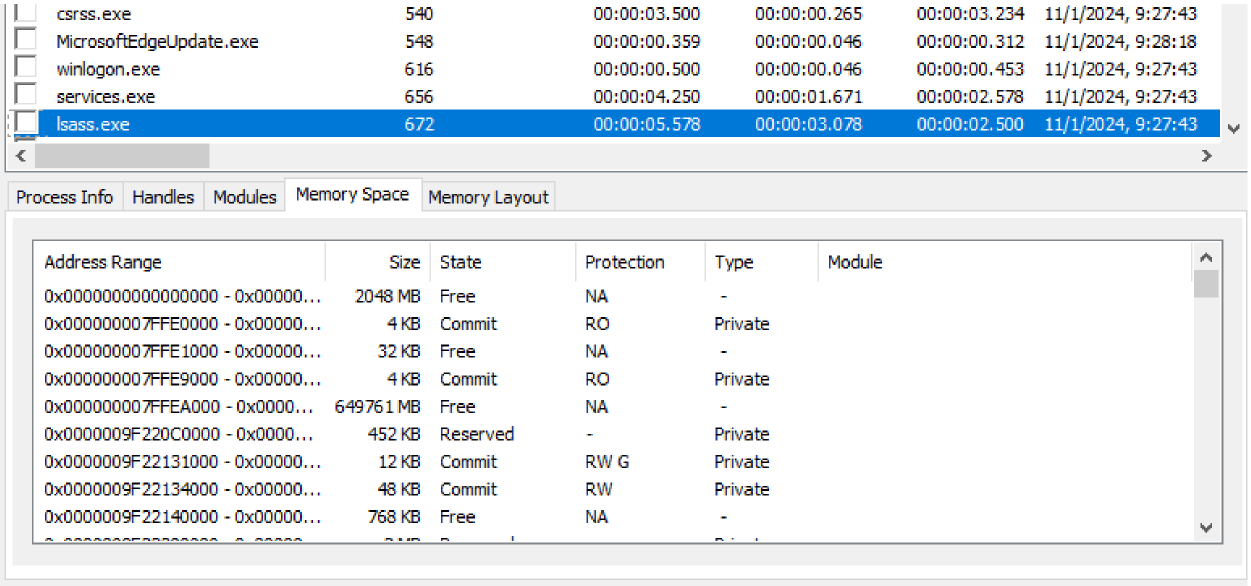
Step 2: Acquire Live Memory



```
operable program or batch file.

c:\Users\jessica_win\Downloads>winpmem_mini_x64_rc2.exe mem.raw
WinPmem64
Extracting driver to C:\Users\JESSIC~1\AppData\Local\Temp\pme3F9E.tmp
Driver Unloaded.
Loaded Driver C:\Users\JESSIC~1\AppData\Local\Temp\pme3F9E.tmp.
Deleting C:\Users\JESSIC~1\AppData\Local\Temp\pme3F9E.tmp
The system time is: 16:40:36
Will generate a RAW image
 - buffer_size_: 0x1000
CR3: 0x00001AA002
 3 memory ranges:
Start 0x00001000 - Length 0x0009E000
Start 0x00100000 - Length 0x00002000
Start 0x00103000 - Length 0x7FEED000
max_physical_memory_ 0x7fff0000
Acquitision mode PTE Remapping
Padding from 0x00000000 to 0x00001000
pad
 - length: 0x1000

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

00% 0x00001000 .
Padding from 0x0009F000 to 0x00100000
pad
```

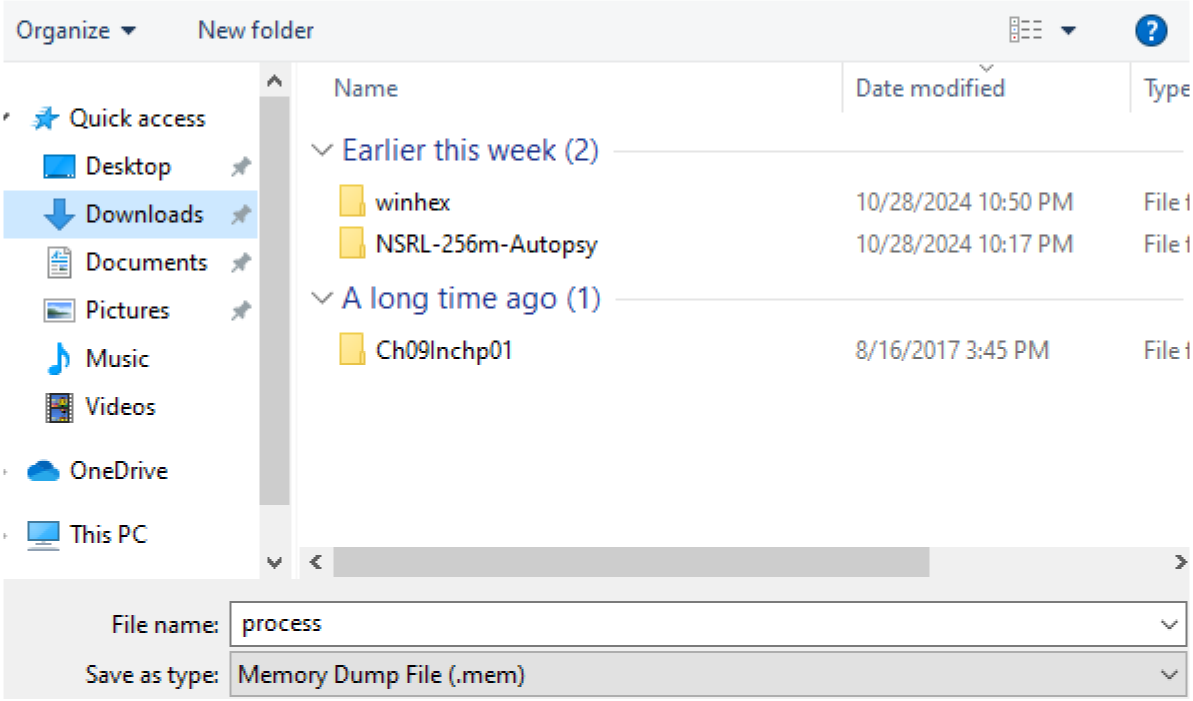
Successfully ran command.

Step 3: Live Memory Acquisition and Analysis



□ csrss.exe	540	00:00:03.500	00:00:00.265	00:00:03.234	11/1/2024, 9:27:43
□ MicrosoftEdgeUpdate.exe	548	00:00:00.359	00:00:00.046	00:00:00.312	11/1/2024, 9:28:18
□ winlogon.exe	616	00:00:00.500	00:00:00.046	00:00:00.453	11/1/2024, 9:27:43
□ services.exe	656	00:00:04.250	00:00:01.671	00:00:02.578	11/1/2024, 9:27:43
□ lsass.exe	672	00:00:05.578	00:00:03.078	00:00:02.500	11/1/2024, 9:27:43

Address Range	Size	State	Protection	Type	Module
0x0000000000000000 - 0x00000...	2048 MB	Free	NA	-	
0x000000007FFE0000 - 0x00000...	4 KB	Commit	RO	Private	
0x000000007FFE1000 - 0x00000...	32 KB	Free	NA	-	
0x000000007FFE9000 - 0x00000...	4 KB	Commit	RO	Private	
0x000000007FFEA000 - 0x0000...	649761 MB	Free	NA	-	
0x0000009F220C0000 - 0x0000...	452 KB	Reserved	-	Private	
0x0000009F22131000 - 0x00000...	12 KB	Commit	RW G	Private	
0x0000009F22134000 - 0x00000...	48 KB	Commit	RW	Private	
0x0000009F22140000 - 0x00000...	768 KB	Free	NA	-	



Name	Date modified	Type
Earlier this week (2)		
winhex	10/28/2024 10:50 PM	File f
NSRL-256m-Autopsy	10/28/2024 10:17 PM	File f
A long time ago (1)		
Ch09Inchp01	8/16/2017 3:45 PM	File f

File name: process

Save as type: Memory Dump File (.mem)

Successfully dumped onto disk.

Step 4: Static Memory Analysis

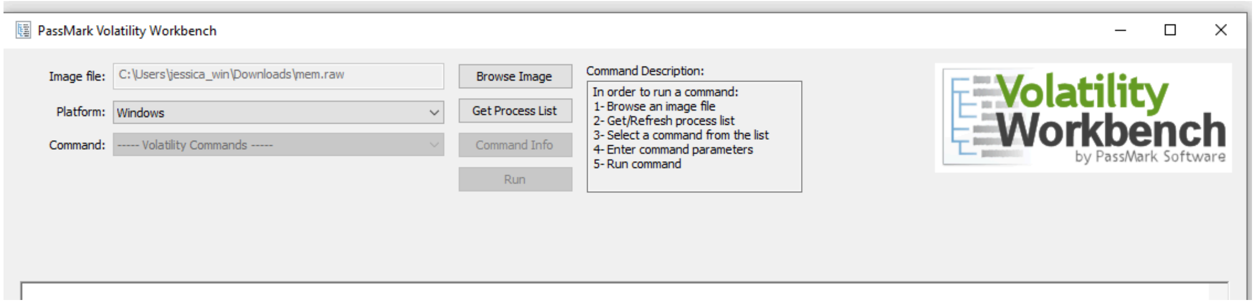


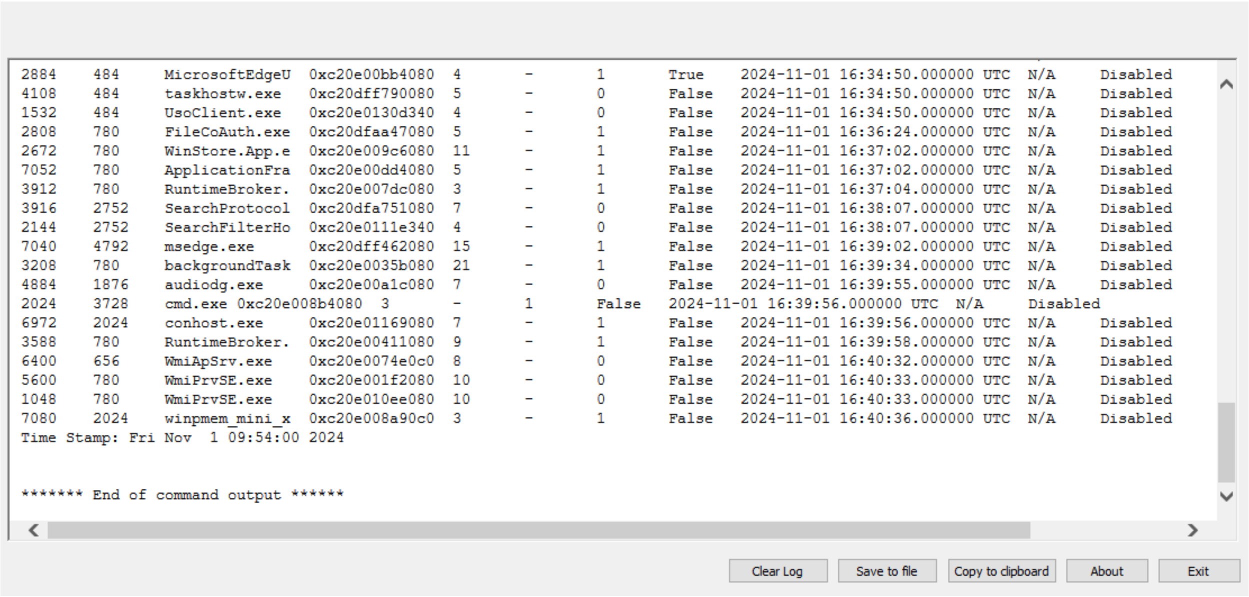
Image file: C:\Users\jessica_win\Downloads\mem.raw

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

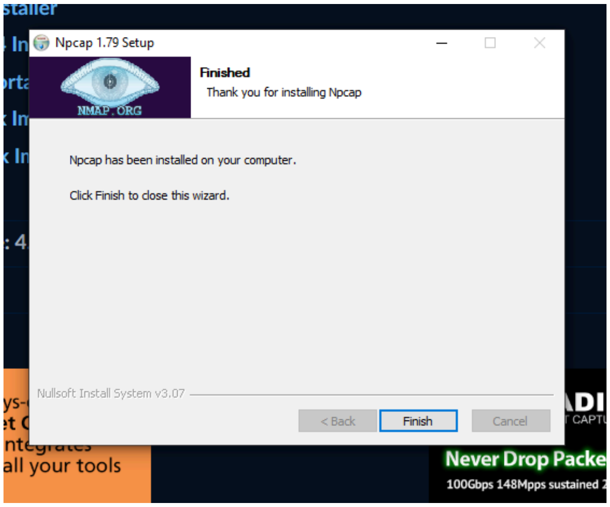


```
2884    484     MicrosoftEdgeU  0xc20e00bb4080  4       -       1       True    2024-11-01 16:34:50.000000 UTC  N/A     Disabled
4108    484     taskhostw.exe   0xc20dff790080  5       -       0       False   2024-11-01 16:34:50.000000 UTC  N/A     Disabled
1532    484     UsoClient.exe   0xc20e0130d340  4       -       0       False   2024-11-01 16:34:50.000000 UTC  N/A     Disabled
2808    780     FileCoAuth.exe  0xc20dfaa47080  5       -       1       False   2024-11-01 16:36:24.000000 UTC  N/A     Disabled
2672    780     WinStore.App.e  0xc20e009c6080  11      -       1       False   2024-11-01 16:37:02.000000 UTC  N/A     Disabled
7052    780     ApplicationFra  0xc20e00dd4080  5       -       1       False   2024-11-01 16:37:02.000000 UTC  N/A     Disabled
3912    780     RuntimeBroker.  0xc20e007dc080  3       -       1       False   2024-11-01 16:37:04.000000 UTC  N/A     Disabled
3916    2752    SearchProtocol  0xc20dfa751080  7       -       0       False   2024-11-01 16:38:07.000000 UTC  N/A     Disabled
2144    2752    SearchFilterHo  0xc20e0111e340  4       -       0       False   2024-11-01 16:38:07.000000 UTC  N/A     Disabled
7040    4792    msedge.exe      0xc20dff462080  15      -       1       False   2024-11-01 16:39:02.000000 UTC  N/A     Disabled
3208    780     backgroundTask  0xc20e0035b080  21      -       1       False   2024-11-01 16:39:34.000000 UTC  N/A     Disabled
4884    1876    audiodg.exe     0xc20e00a1c080  7       -       0       False   2024-11-01 16:39:55.000000 UTC  N/A     Disabled
2024    3728    cmd.exe 0xc20e008b4080  3       -       1       False   2024-11-01 16:39:56.000000 UTC  N/A     Disabled
6972    2024    conhost.exe     0xc20e01169080  7       -       1       False   2024-11-01 16:39:56.000000 UTC  N/A     Disabled
3588    780     RuntimeBroker.  0xc20e00411080  9       -       1       False   2024-11-01 16:39:58.000000 UTC  N/A     Disabled
6400    656     WmiApSrv.exe    0xc20e0074e0c0  8       -       0       False   2024-11-01 16:40:32.000000 UTC  N/A     Disabled
5600    780     WmiPrvSE.exe    0xc20e001f2080  10      -       0       False   2024-11-01 16:40:33.000000 UTC  N/A     Disabled
1048    780     WmiPrvSE.exe    0xc20e010ee080  10      -       0       False   2024-11-01 16:40:33.000000 UTC  N/A     Disabled
7080    2024    winpmem_mini_x  0xc20e008a90c0  3       -       1       False   2024-11-01 16:40:36.000000 UTC  N/A     Disabled
Time Stamp: Fri Nov  1 09:54:00 2024


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

Successfully analyzed the mem.raw file.

Task 2: Network Forensic Investigation

Step 1: Install Wireshark

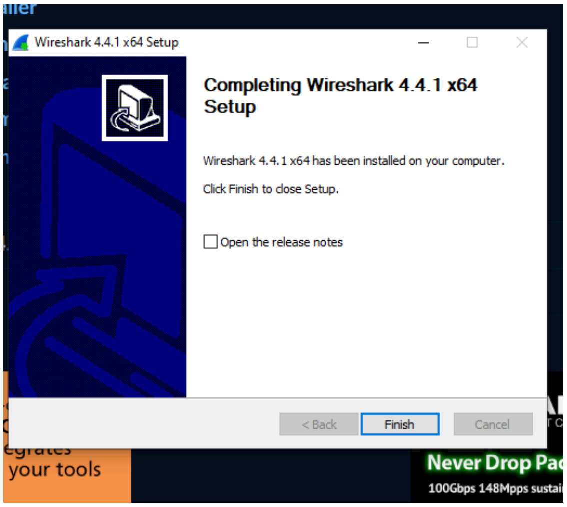


Finished

Thank you for installing Npcap

Npcap has been installed on your computer.

Click Finish to close this wizard.



Completing Wireshark 4.4.1 x64 Setup

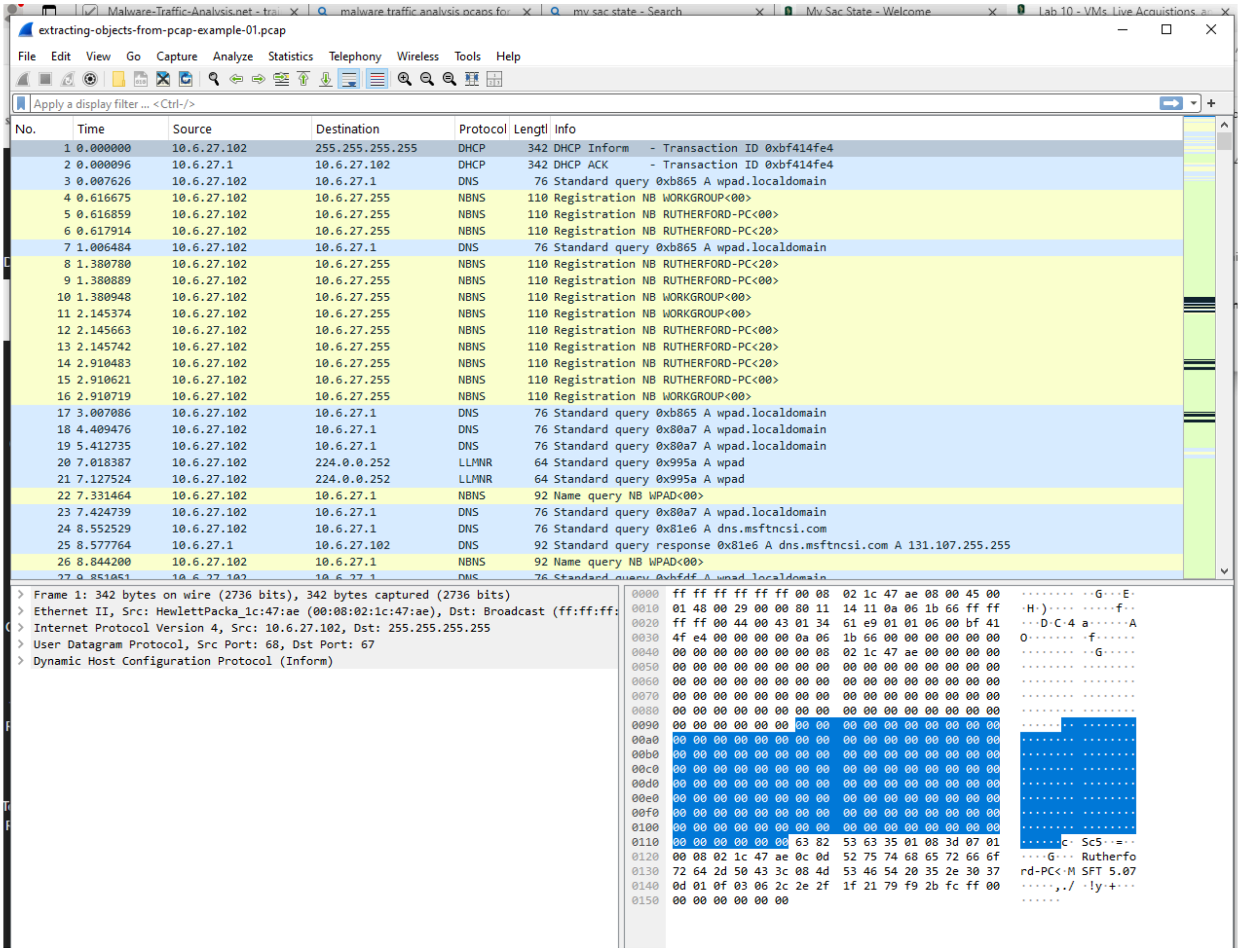
Wireshark 4.4.1 x64 has been installed on your computer.

Click Finish to close Setup.

□ Open the release notes

Successfully downloaded Wireshark.

Step 2: Download Sample PCAP


Malware-Traffic-Analysis.net - tra
malware traffic analysis pcaps for
my sac state - Search
My Sac State - Welcome
Lab 10 - VMs, Live Acquistions, a
extracting-objects-from-pcap-example-01.pcap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>

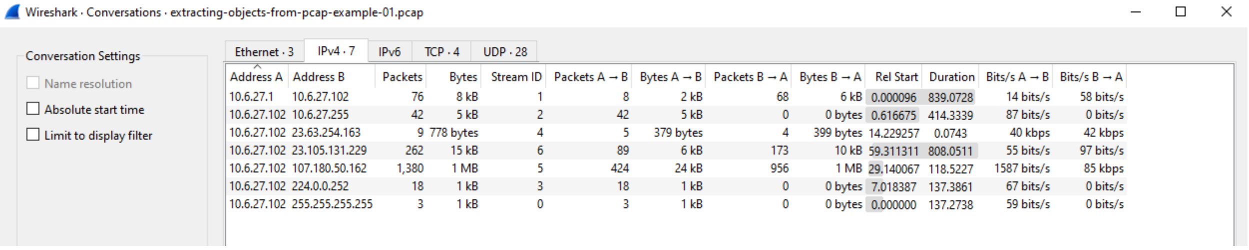
No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	10.6.27.102	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xbf414fe4
2	0.000096	10.6.27.1	10.6.27.102	DHCP	342	DHCP ACK - Transaction ID 0xbf414fe4
3	0.007626	10.6.27.102	10.6.27.1	DNS	76	Standard query 0xb865 A wpad.localdomain
4	0.616675	10.6.27.102	10.6.27.255	NBNS	110	Registration NB WORKGROUP<00>
5	0.616859	10.6.27.102	10.6.27.255	NBNS	110	Registration NB RUTHERFORD-PC<00>
6	0.617914	10.6.27.102	10.6.27.255	NBNS	110	Registration NB RUTHERFORD-PC<20>
7	1.006484	10.6.27.102	10.6.27.1	DNS	76	Standard query 0xb865 A wpad.localdomain
8	1.380780	10.6.27.102	10.6.27.255	NBNS	110	Registration NB RUTHERFORD-PC<20>
9	1.380889	10.6.27.102	10.6.27.255	NBNS	110	Registration NB RUTHERFORD-PC<00>
10	1.380948	10.6.27.102	10.6.27.255	NBNS	110	Registration NB WORKGROUP<00>
11	2.145374	10.6.27.102	10.6.27.255	NBNS	110	Registration NB WORKGROUP<00>
12	2.145663	10.6.27.102	10.6.27.255	NBNS	110	Registration NB RUTHERFORD-PC<00>
13	2.145742	10.6.27.102	10.6.27.255	NBNS	110	Registration NB RUTHERFORD-PC<20>
14	2.910483	10.6.27.102	10.6.27.255	NBNS	110	Registration NB RUTHERFORD-PC<20>
15	2.910621	10.6.27.102	10.6.27.255	NBNS	110	Registration NB RUTHERFORD-PC<00>
16	2.910719	10.6.27.102	10.6.27.255	NBNS	110	Registration NB WORKGROUP<00>
17	3.007086	10.6.27.102	10.6.27.1	DNS	76	Standard query 0xb865 A wpad.localdomain
18	4.409476	10.6.27.102	10.6.27.1	DNS	76	Standard query 0x80a7 A wpad.localdomain
19	5.412735	10.6.27.102	10.6.27.1	DNS	76	Standard query 0x80a7 A wpad.localdomain
20	7.018387	10.6.27.102	224.0.0.252	LLMNR	64	Standard query 0x995a A wpad
21	7.127524	10.6.27.102	224.0.0.252	LLMNR	64	Standard query 0x995a A wpad
22	7.331464	10.6.27.102	10.6.27.1	NBNS	92	Name query NB WPAD<00>
23	7.424739	10.6.27.102	10.6.27.1	DNS	76	Standard query 0x80a7 A wpad.localdomain
24	8.552529	10.6.27.102	10.6.27.1	DNS	76	Standard query 0x81e6 A dns.msftncsi.com
25	8.577764	10.6.27.1	10.6.27.102	DNS	92	Standard query response 0x81e6 A dns.msftncsi.com A 131.107.255.255
26	8.844200	10.6.27.102	10.6.27.1	NBNS	92	Name query NB WPAD<00>
27	9.851051	10.6.27.102	10.6.27.1	DNS	76	Standard query 0xbfdf A wpad.localdomain

```
> Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
> Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Broadcast (ff:ff:ff:
> Internet Protocol Version 4, Src: 10.6.27.102, Dst: 255.255.255.255
> 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 45 00   ········ ··G···E·
0010  01 48 00 29 00 00 80 11  14 11 0a 06 1b 66 ff ff   ·H·)···· ·····f··
0020  ff ff 00 44 00 43 01 34  61 e9 01 01 06 00 bf 41   ···D·C·4 a······A
0030  4f e4 00 00 00 00 0a 06  1b 66 00 00 00 00 00 00   O······· ·f······
0040  00 00 00 00 00 00 00 08  02 1c 47 ae 00 00 00 00   ········ ··G·····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 08 3d 07 01   ······c· Sc5··=··
0120  00 08 02 1c 47 ae 0c 0d  52 75 74 68 65 72 66 6f   ····G··· Rutherfo
0130  72 64 2d 50 43 3c 08 4d  53 46 54 20 35 2e 30 37   rd-PC<·M SFT 5.07
0140  0d 01 0f 03 06 2c 2e 2f  1f 21 79 f9 2b fc ff 00   ·····,./ ·!y·+···
0150  00 00 00 00 00 00                                  ······
```

Successfully downloaded and loaded onto Wireshark.

Step 3: Analyze the PCAP



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

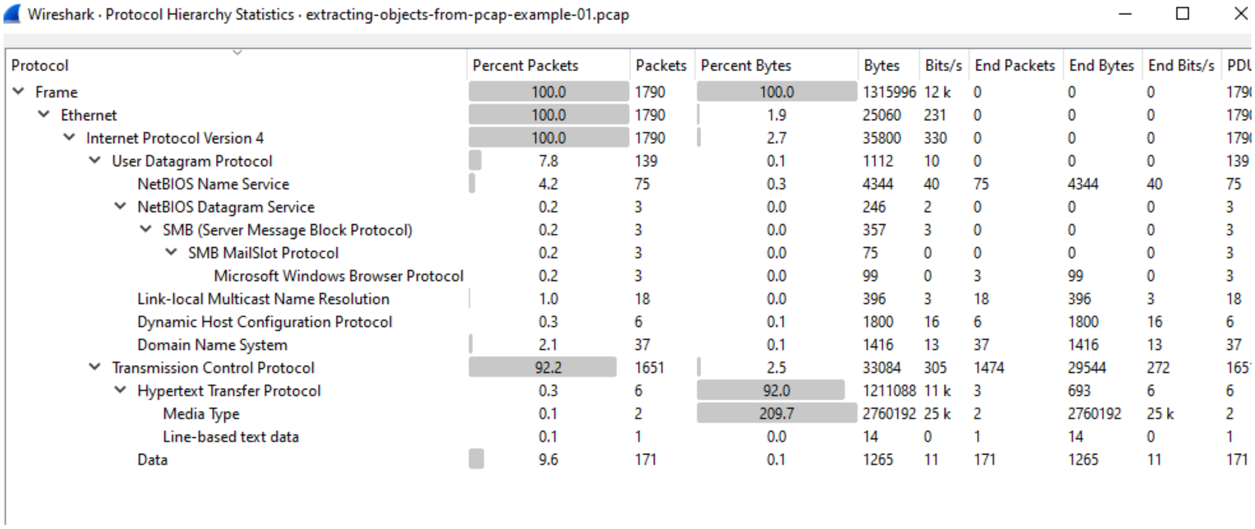
Conversation Settings

☐ Name resolution

☐ Absolute start time

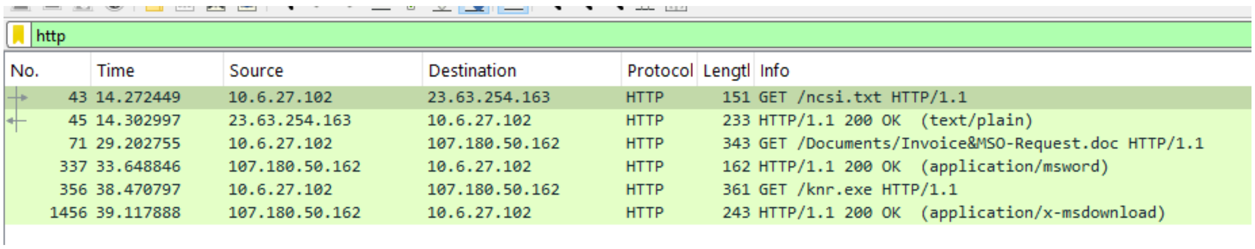
☐ Limit to display filter

Address A	Address B	Packets	Bytes	Stream ID	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	1	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	2	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	4	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	6	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	5	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	3	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	0	3	1 kB	0	0 bytes	0.000000	137.2738	59 bits/s	0 bits/s



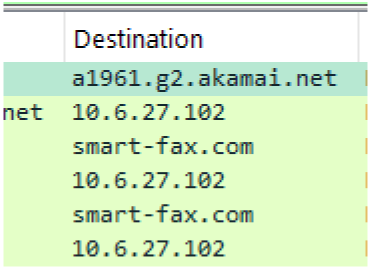
Wireshark · Protocol Hierarchy Statistics · extracting-objects-from-pcap-example-01.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDU
Frame	100.0	1790	100.0	1315996	12 k	0	0	0	179
Ethernet	100.0	1790	1.9	25060	231	0	0	0	179
Internet Protocol Version 4	100.0	1790	2.7	35800	330	0	0	0	179
User Datagram Protocol	7.8	139	0.1	1112	10	0	0	0	139
NetBIOS Name Service	4.2	75	0.3	4344	40	75	4344	40	75
NetBIOS Datagram Service	0.2	3	0.0	246	2	0	0	0	3
SMB (Server Message Block Protocol)	0.2	3	0.0	357	3	0	0	0	3
SMB MailSlot Protocol	0.2	3	0.0	75	0	0	0	0	3
Microsoft Windows Browser Protocol	0.2	3	0.0	99	0	3	99	0	3
Link-local Multicast Name Resolution	1.0	18	0.0	396	3	18	396	3	18
Dynamic Host Configuration Protocol	0.3	6	0.1	1800	16	6	1800	16	6
Domain Name System	2.1	37	0.1	1416	13	37	1416	13	37
Transmission Control Protocol	92.2	1651	2.5	33084	305	1474	29544	272	165
Hypertext Transfer Protocol	0.3	6	92.0	1211088	11 k	3	693	6	6
Media Type	0.1	2	209.7	2760192	25 k	2	2760192	25 k	2
Line-based text data	0.1	1	0.0	14	0	1	14	0	1
Data	9.6	171	0.1	1265	11	171	1265	11	171

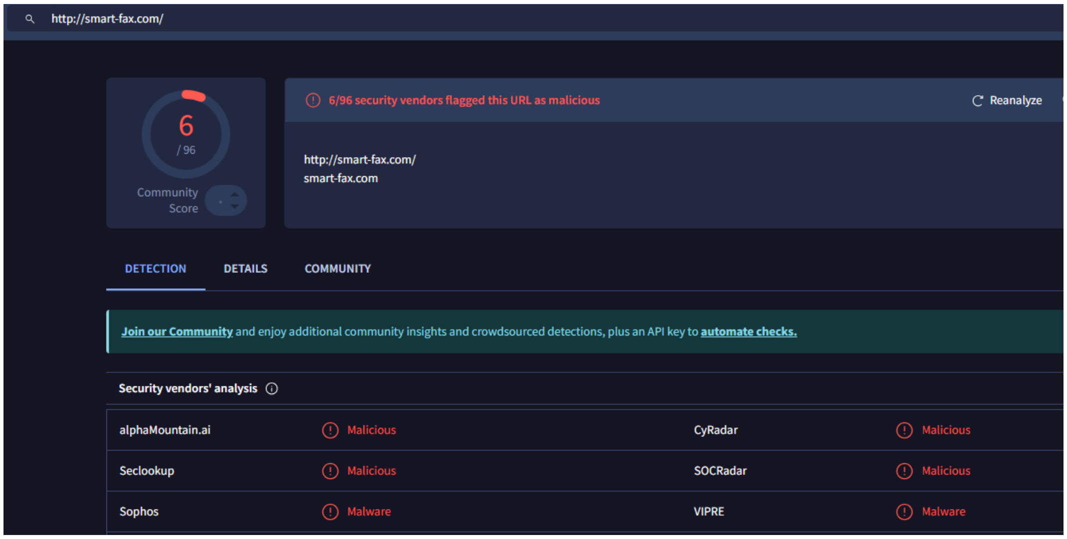


http

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/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)



Destination
a1961.g2.akamai.net
10.6.27.102
smart-fax.com
10.6.27.102
smart-fax.com
10.6.27.102



http://smart-fax.com/

6 / 96 Community Score

6/96 security vendors flagged this URL as malicious

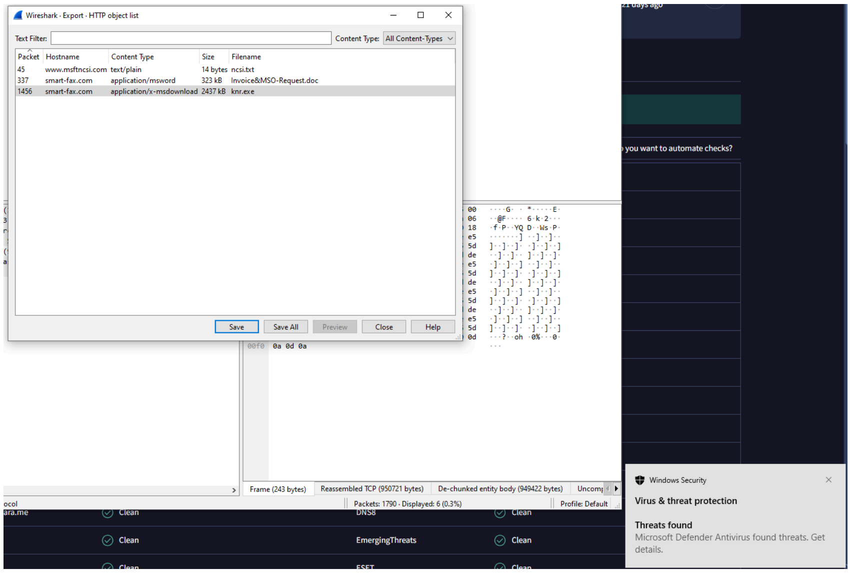
Reanalyze

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

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

Security vendors' analysis

alphaMountain.ai	Malicious	CyRadar	Malicious
Seclookup	Malicious	SOCRadar	Malicious
Sophos	Malware	VIPRE	Malware



Wireshark · Export · HTTP object list

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

Frame (243 bytes) | Reassembled TCP (950721 bytes) | De-chunked entity body (949422 bytes)

Packets: 1790 · Displayed: 6 (0.3%) | Profile: Default

	Clean	EmergingThreats	Clean

Windows Security

Virus & threat protection

Threats found

Microsoft Defender Antivirus found threats. Get details.

Successfully found malware through analysis. I recognized what looked like regular traffic through this network by observing the packets and their sizes. Through this, I noticed that a document was downloaded from one of the sites that the suspect visited. After further analysis, the site that the document was downloaded from was flagged as malicious by different outside sources. When attempting to download the said document, my machine flagged it as a threat. The suspect's machine had downloaded malware from a suspicious site called smart-fax.com.