

## Task 1:

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

c:\Users\timothyd\Downloads>dir
Volume in drive C has no label.
Volume Serial Number is 96A4-C332

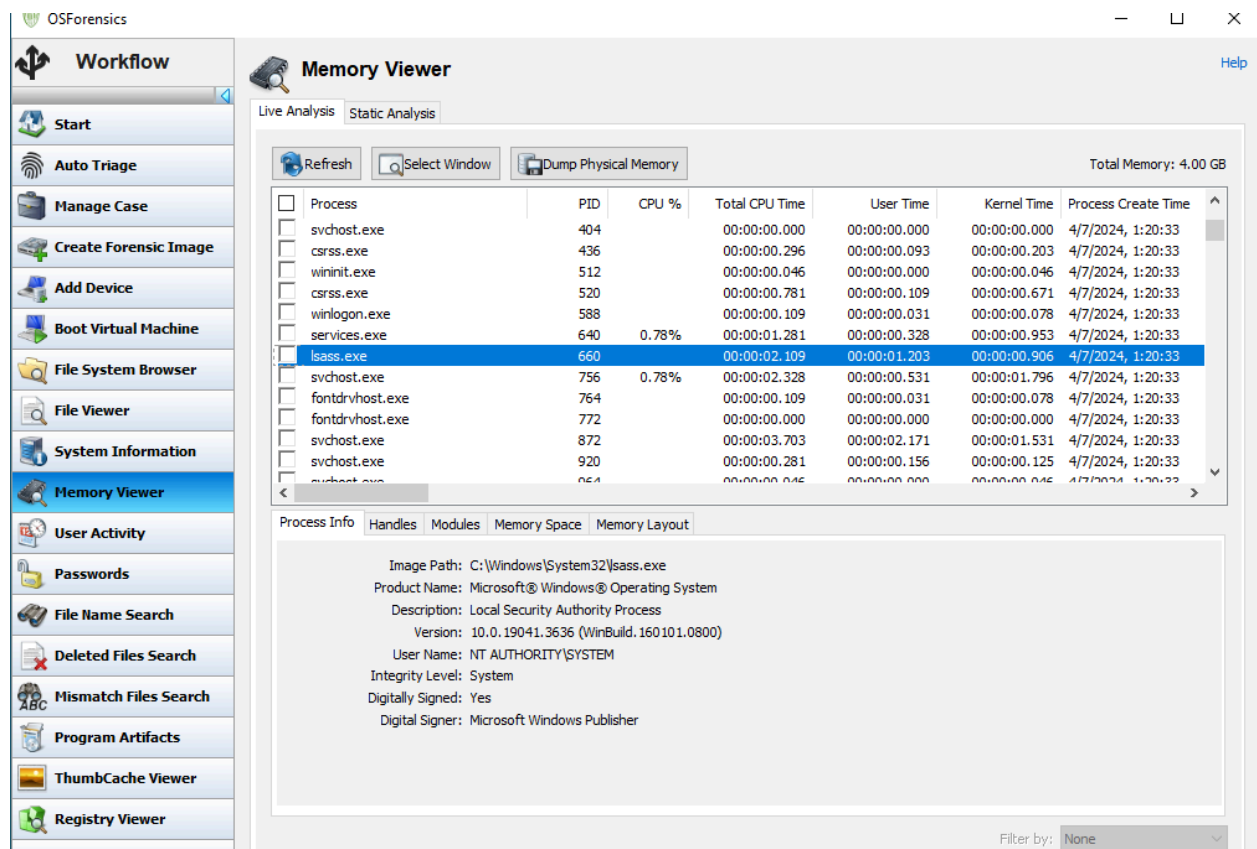
Directory of c:\Users\timothyd\Downloads

04/07/2024  12:15 AM    <DIR>          .
04/07/2024  12:15 AM    <DIR>          ..
03/24/2024  02:58 PM       1,188,695,040 autopsy-4.21.0-64bit.msi
03/01/2024  12:56 AM    <DIR>          Case Report
08/16/2017  03:45 PM    <DIR>          Ch09Inchp01
04/02/2024  01:57 PM       19,809,721 Ch09Inchp01.exe
02/22/2024  10:15 PM       33,499,203 chapter04-Terry_work_usb.E01
04/02/2024  02:58 PM        9,691 demo 9.docx
03/02/2024  03:17 PM       18,864,464 hw_v680.exe
03/24/2024  03:20 PM        3,348,102 HxDPortableSetup.zip
03/01/2024  12:30 AM    <DIR>          InCh05
03/01/2024  12:22 AM       11,051,005 InCh05.zip
04/02/2024  01:49 PM    <DIR>          NSRL-256m-Autopsy
04/02/2024  01:48 PM       773,217,105 NSRL-256m-Autopsy.zip
02/22/2024  10:10 PM       285,718,008 osf.exe
02/29/2024  11:59 PM    <DIR>          winhex
04/02/2024  02:57 PM    <DIR>          winhex (1)
04/02/2024  02:57 PM        4,143,160 winhex (1).zip
02/29/2024  11:59 PM        4,143,160 winhex.zip
04/07/2024  12:15 AM        527,640 winpmem_mini_x64_rc2.exe
               12 File(s)  2,343,026,299 bytes
               8 Dir(s)   7,413,846,016 bytes free
```

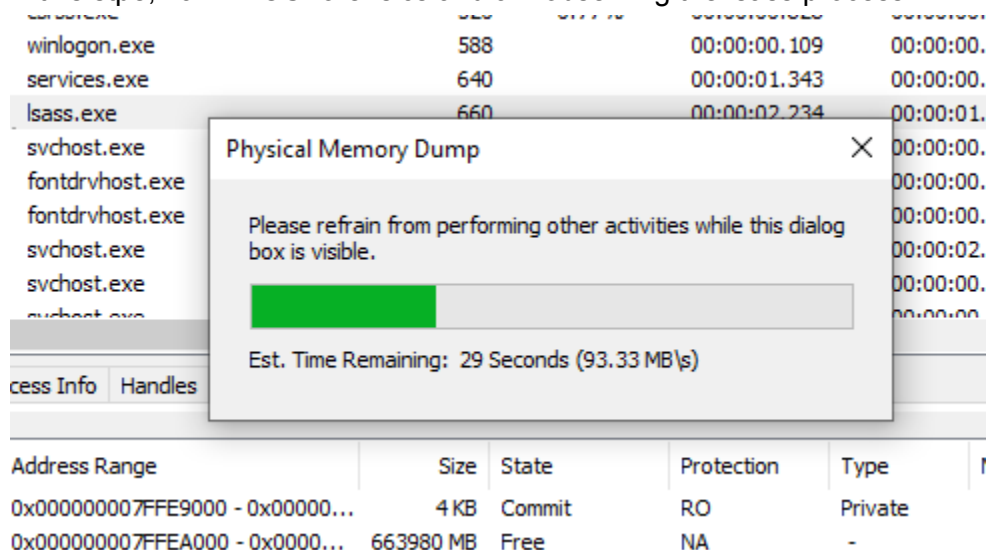
In this step, I have downloaded winpmem\_mini\_x64\_rc2.exe. Now I am in cmd as an admin and displaying my downloads folder.

```
c:\Users\timothyd\Downloads>winpmem_mini_x64_rc2.exe mem.raw
WinPmem64
Extracting driver to C:\Users\timothyd\AppData\Local\Temp\pmeC6A8.tmp
Driver Unloaded.
Loaded Driver C:\Users\timothyd\AppData\Local\Temp\pmeC6A8.tmp.
Deleting C:\Users\timothyd\AppData\Local\Temp\pmeC6A8.tmp
The system time is: 07:18:30
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 0x10000000 - Length 0x00000000
```

Here I am running winpmem and outputting it to mem.raw.

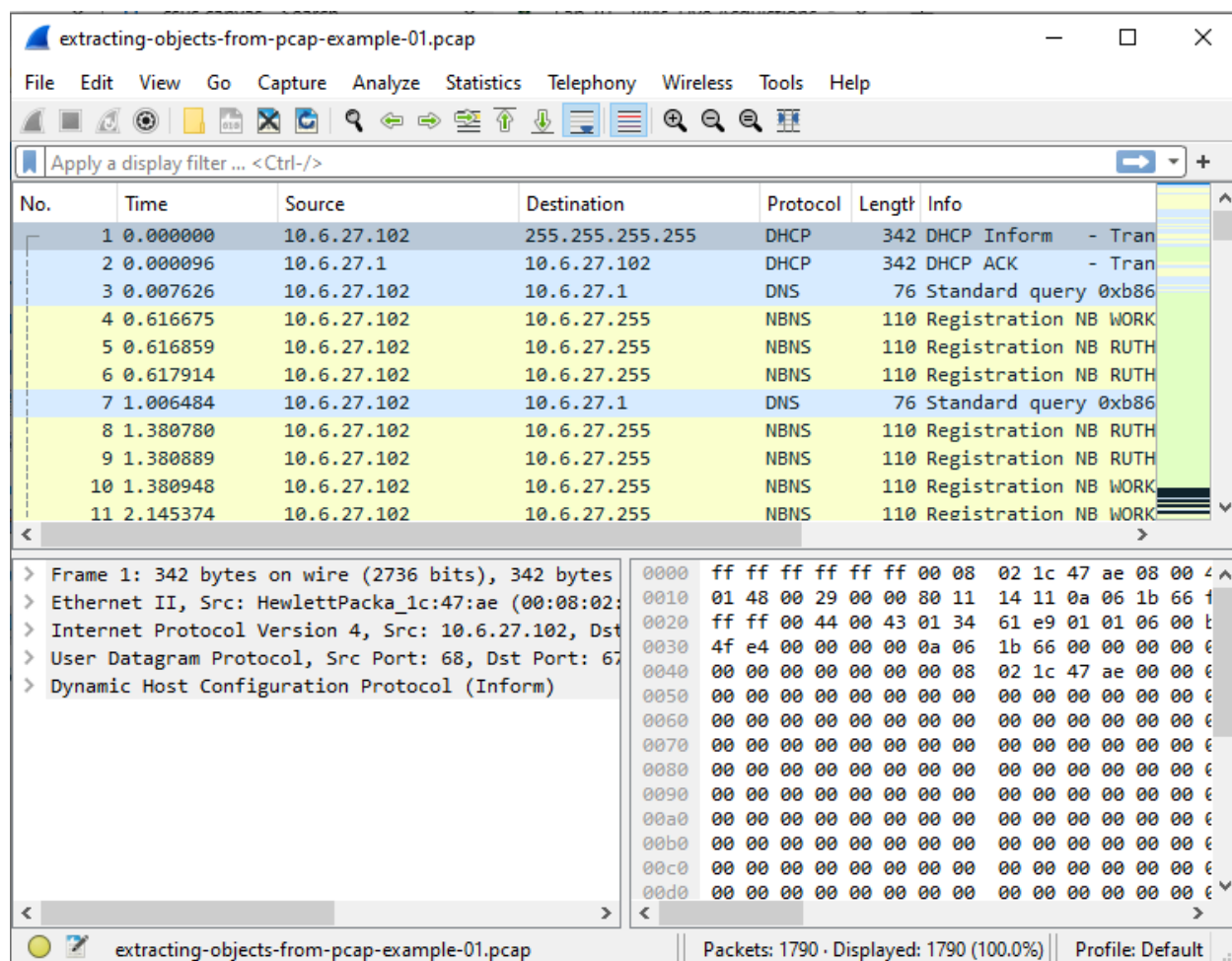


In this step, I am in OSForensics and am observing the lsass process.

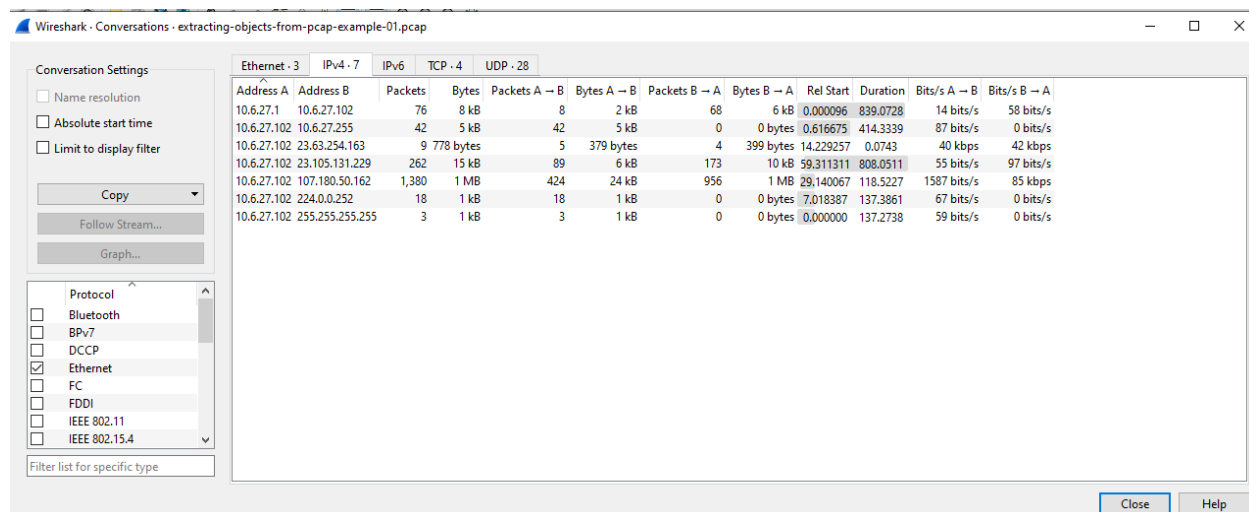


Now, I am dumping the physical memory.





In this step, I downloaded the zip file and opened it in wireshark.



Here I am observing the statistics.

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/s
▼ Frame	100.0	1790	100.0	1315996	12 k	0	0	0	1790
▼ Ethernet	100.0	1790	1.9	25060	231	0	0	0	1790
▼ Internet Protocol Version 4	100.0	1790	2.7	35800	330	0	0	0	1790
▼ 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	603	5	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	94.6	1245465	11 k	1474	1239491	11 k	1651
▼ Hypertext Transfer Protocol	0.3	6	92.0	1211102	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

No display filter.

Close Copy Protocols Help

Here we can see that http traffic is included.

extracting-objects-from-pcap-example-01.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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)

I have applied the http filter and can see that a word doc was downloaded.

extracting-objects-from-pcap-example-01.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	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/plain)
71	29.202755	10.6.27.102	smart-fax.com	HTTP	343	GET /Documents/Invoice&MSO-Request.doc HTTP/1.1
337	33.648846	smart-fax.com	10.6.27.102	HTTP	162	HTTP/1.1 200 OK (application/msword)
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 (application/x-msdownload)

Upon setting the IP resolution, we can see smart-fax.com.

smart-fax.com

7/90

Community Score

7/90 security vendors flagged this domain as malicious

Similar Graph API

smart-fax.com

Creation Date: 8 months ago

Last Analysis Date: 3 days ago

Malicious (alphaMountain.ai) porn spyware and malware

DETECTION DETAILS RELATIONS COMMUNITY

Join the VT 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?

Criminal IP	Phishing	CyRadar	Malicious
Gridinsoft	Malicious	Seclookup	Malicious
SOCradar	Malicious	Sophos	Malware

Here I can see that smart-fax.com has been flagged as malicious.

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

Here I am going to export the knr.exe file.



Here we can see that Windows detected that it is malware.