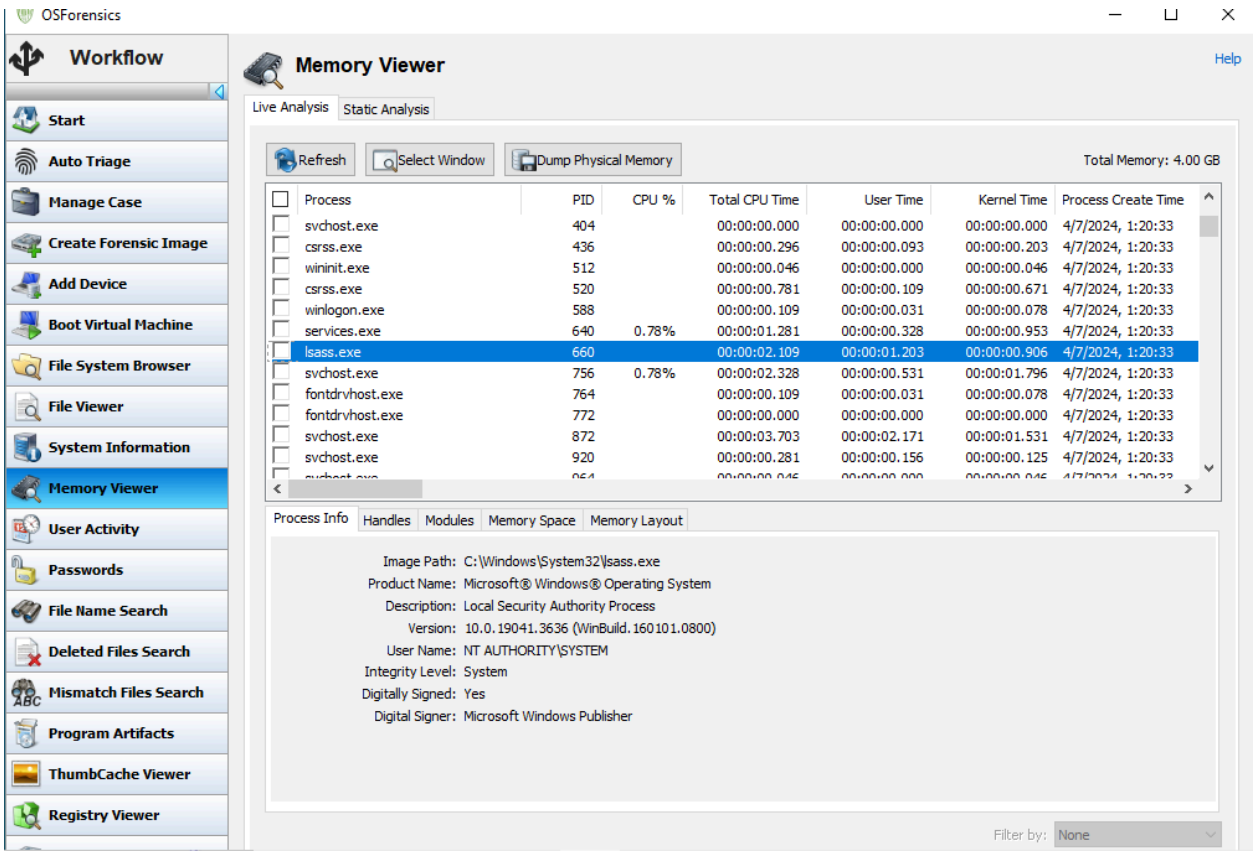
Task 1:

```
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
```

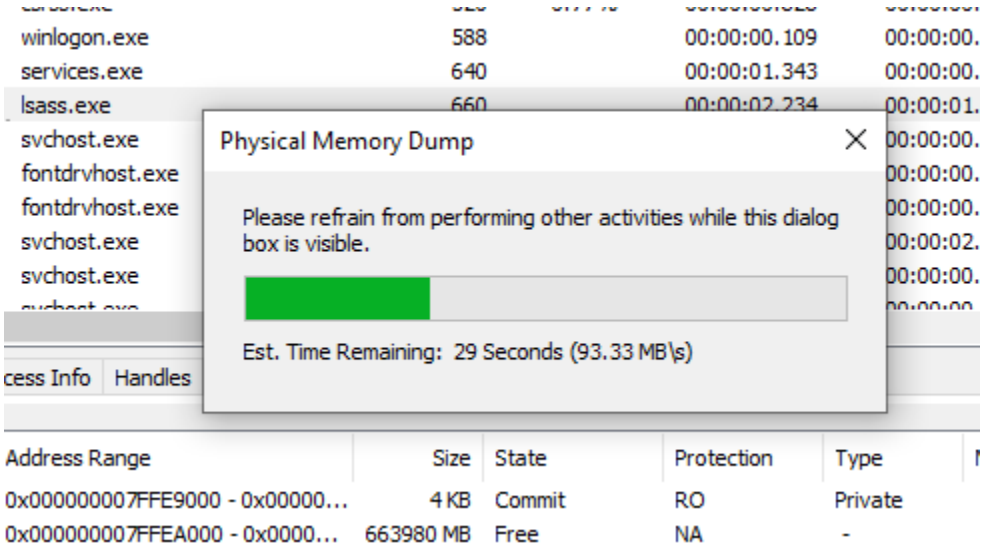
In this step, I have downloaded winpmem_mini_x64_rc2.exe. Now I am in cmd as an admin and displaying my downloads folder.

```
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
```

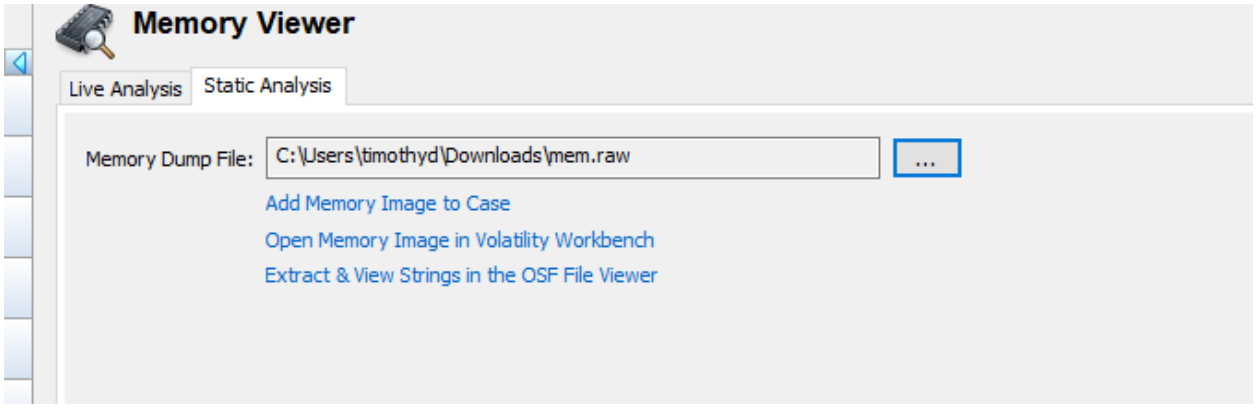
Here I am running winpmem and outputting it to mem.raw.



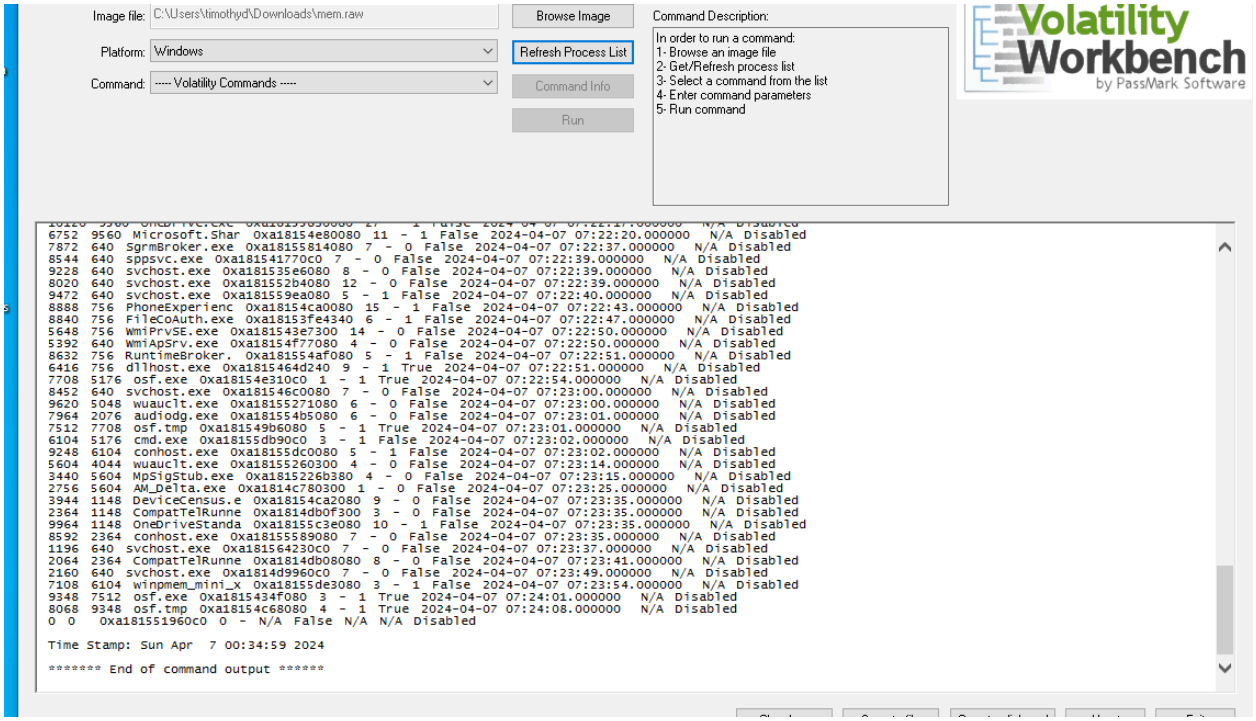
In this stpe, I am in OSForensics and am observing the isass process.



Now, Iam dumping the physical memory.

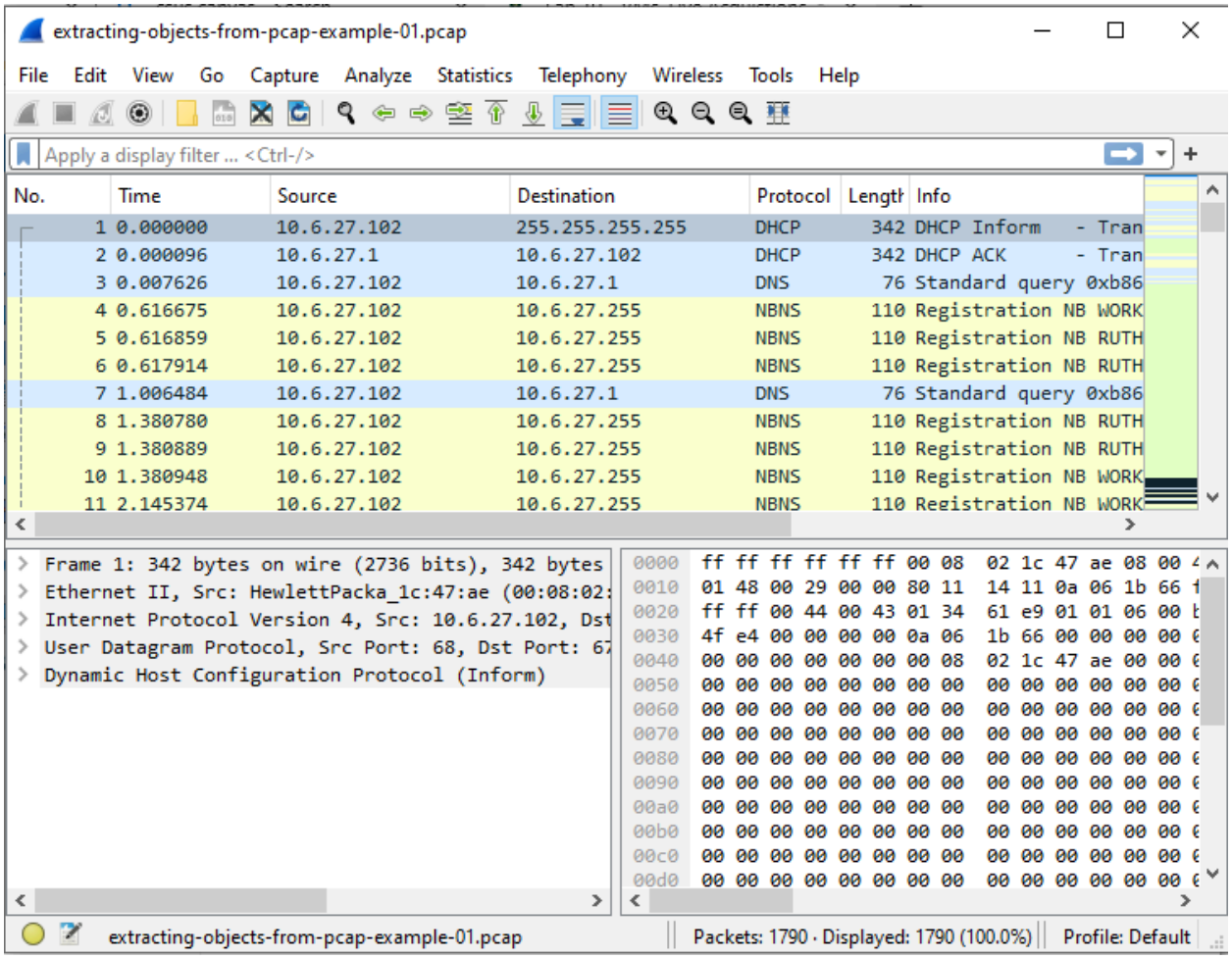


Here I have the mem.raw file selected.

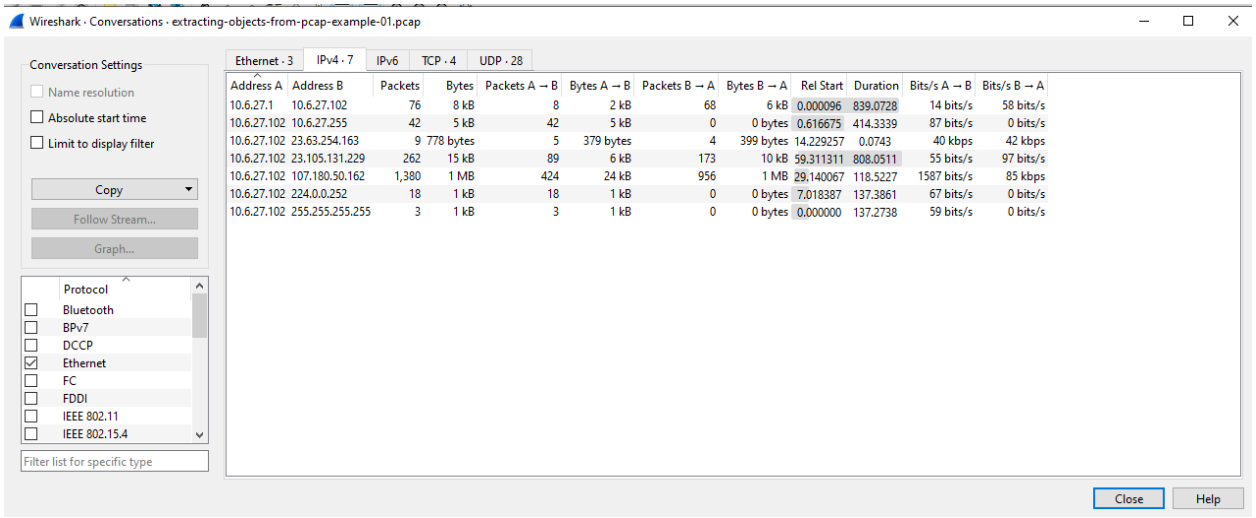


In this step, I clicked the “Open Memory Image in Volatility WorkBench” and then the “Get Process List” button.

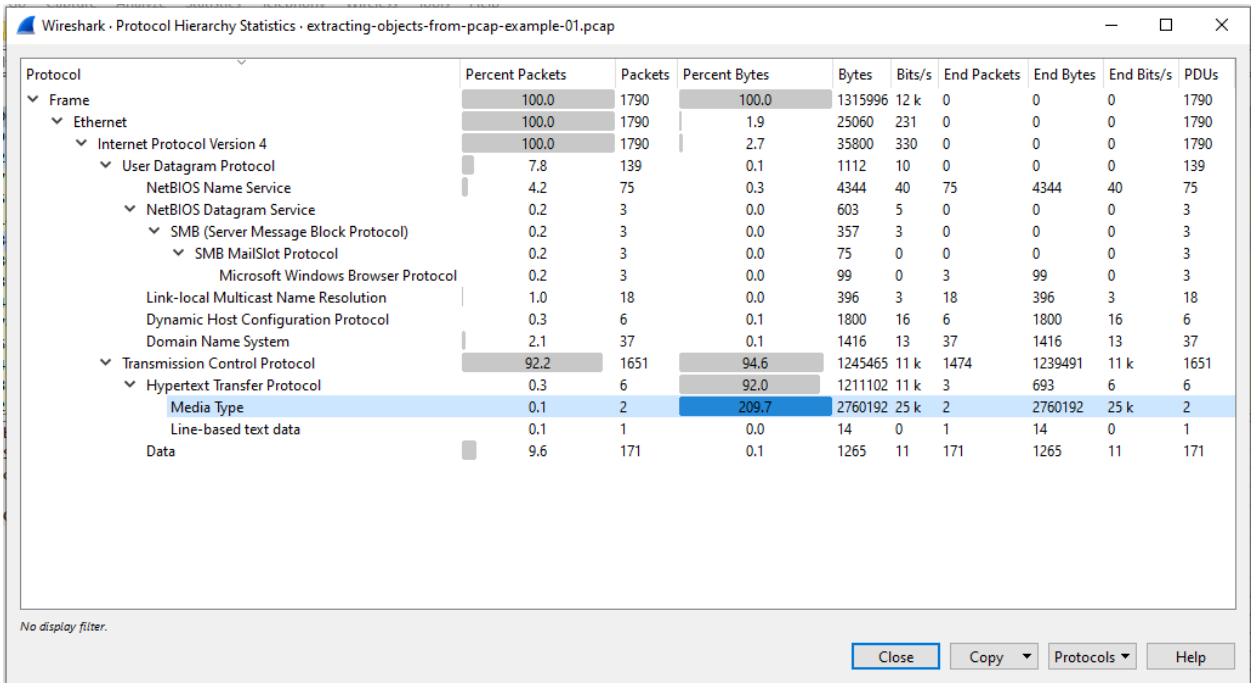
Task 2:



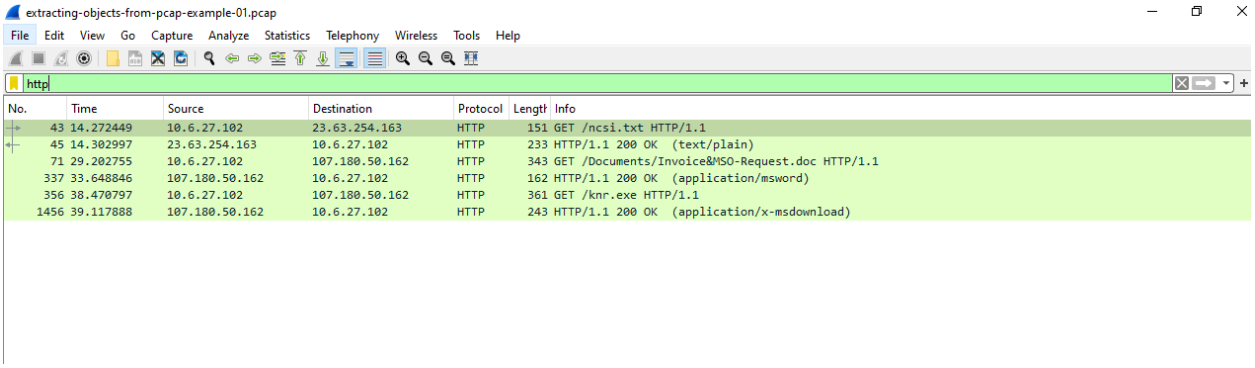
In this step, I downloaded the zip file and opened it in wireshark.



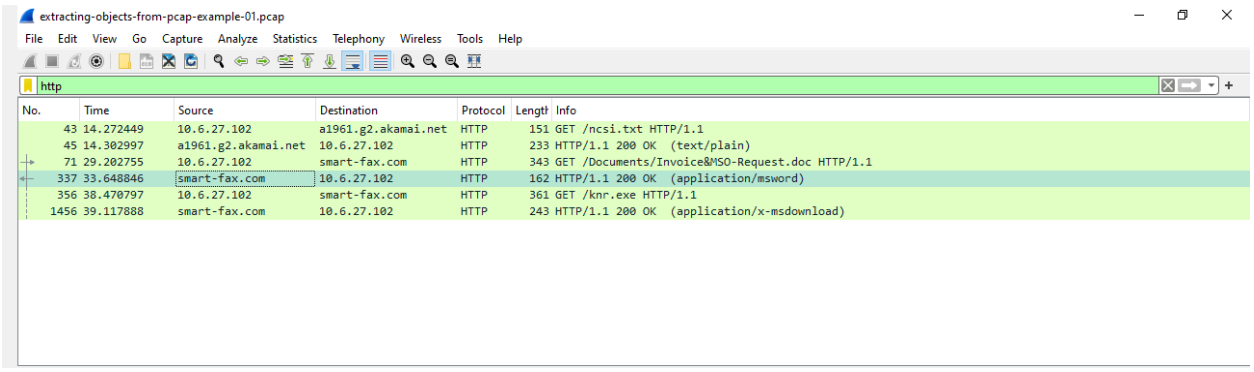
Here I am observing the statistics.



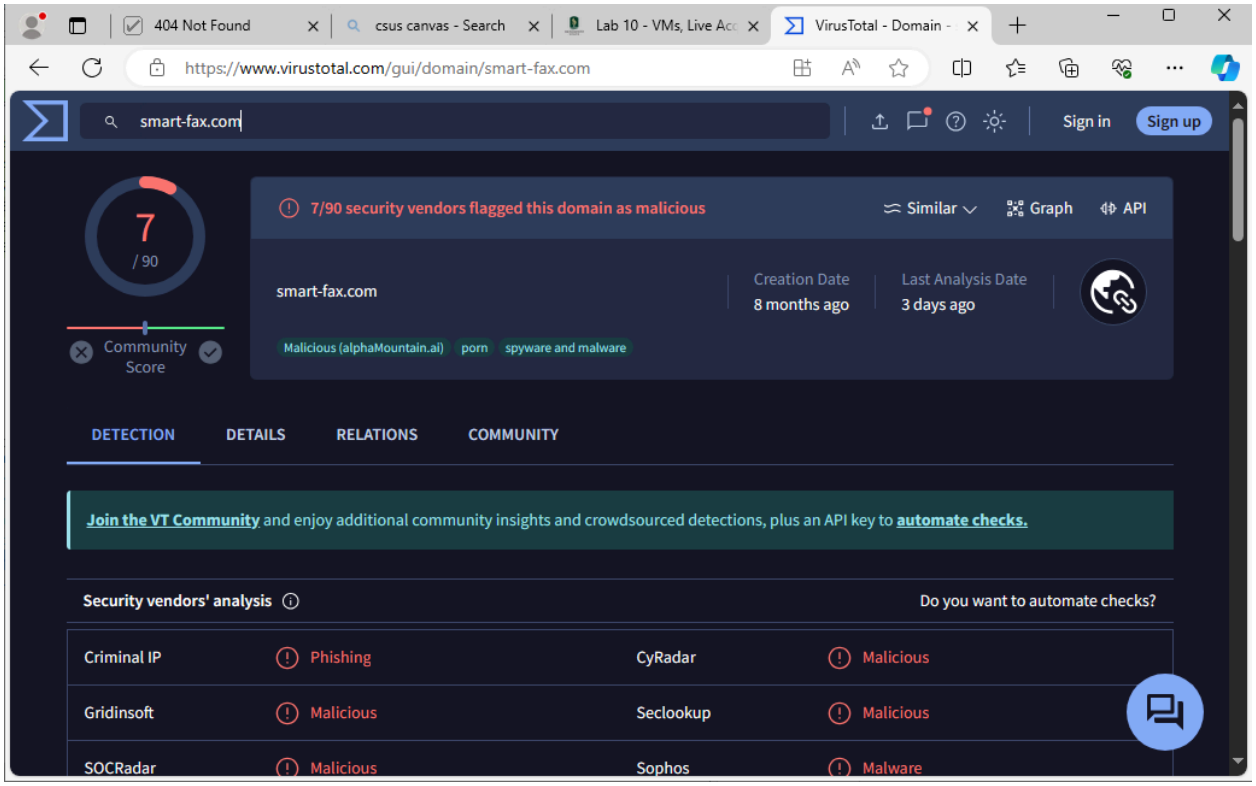
Here we can see that http traffic is included.



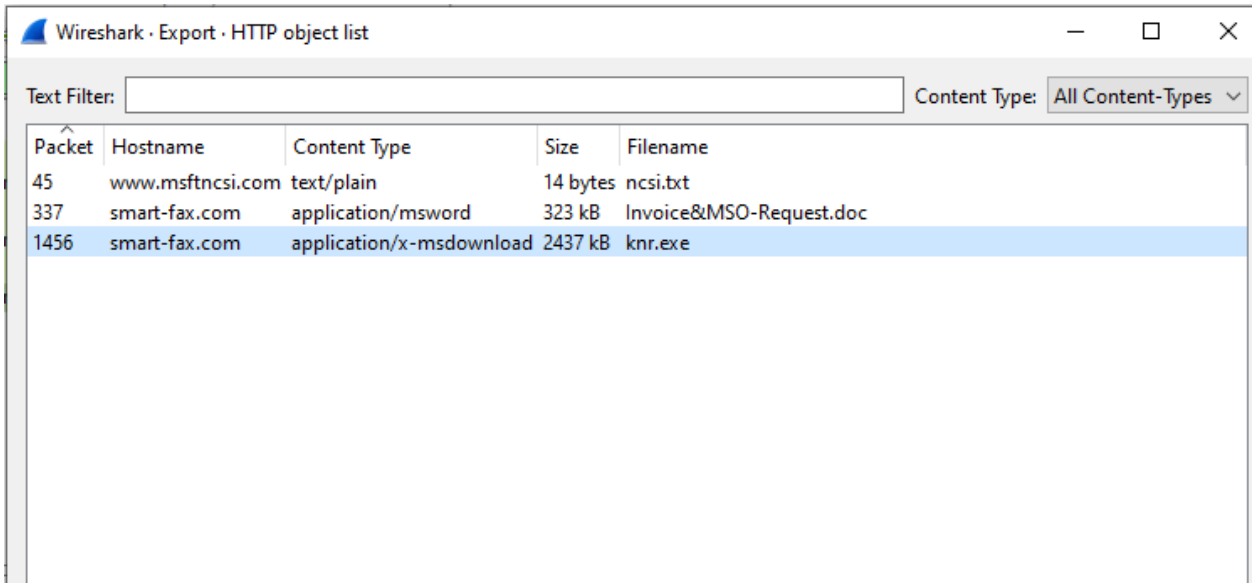
I have applied the http filter and can see that a word doc was downloaded.



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



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



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

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