**Memory Forensics**

Download the memory dump attached with the assignment. The file is protected with a password popular among the malware community. Analyze the memory dump using

‘vol.py’ [volatility] and answer the following questions. For each of the following questions, provide screenshots [with big enough font size] of the executed commands:

a. On which platform was the memory dump taken?

b. Save all unique web domains captured in the memory dump to a .txt file. Did you find any suspicious websites? [Name the output file with “rollnumber\_7\_b.txt”]

c. List the unique ip addresses captured in the dump. [The command can just list all ips, not necessarily unique ips]

d. What were the processes running at the time?

e. Which 4 processes have the same parent?

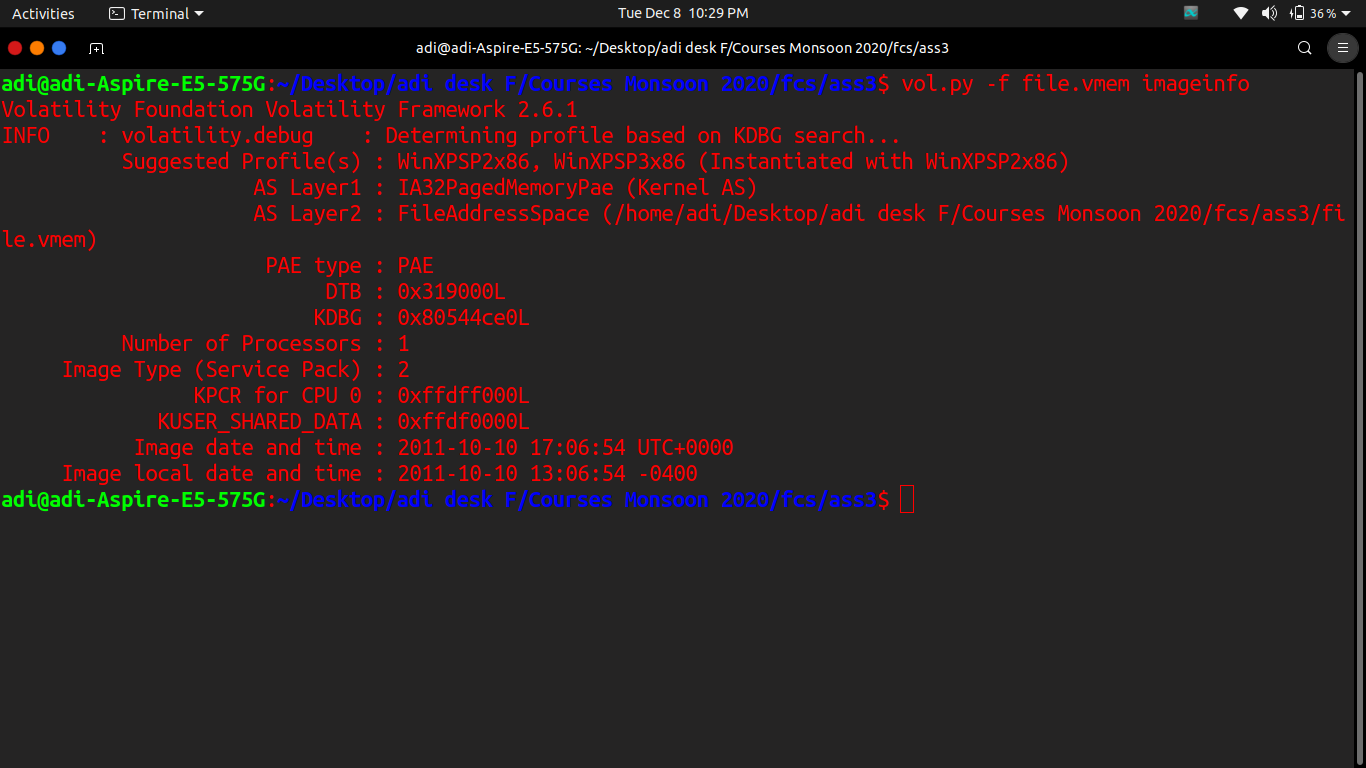
f. What commands invoked the above 4 processes?

g. One process is suspicious. Why?

h. Take the process dump of the suspicious process. Save the “strings” output of the process to a .txt file. Did you find any suspicious activity? Discuss?

The memory dump can be found here: https://drive.google.com/file/d/1vI-hV96yhJBH4ST3r3bzJK2cbGk5umZq/view?usp=sharing

0zapftis

a. vol.py -f 0zapftis.vmem imageinfo 

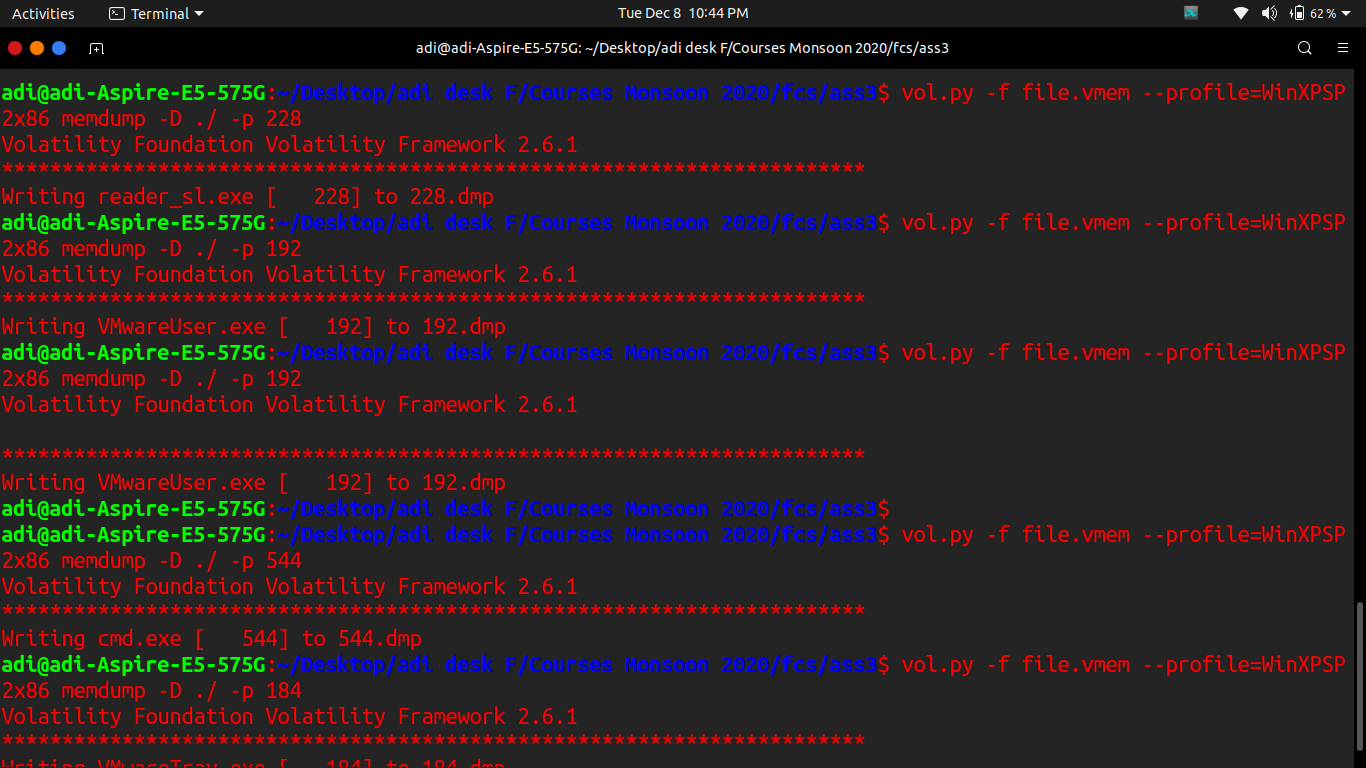
b. vol.py -f 0zapftis.vmem --profile=WinXPSP2x86 memdump -D ./ -p 228

vol.py -f 0zapftis.vmem --profile=WinXPSP2x86 memdump -D ./ -p 192

vol.py -f 0zapftis.vmem --profile=WinXPSP2x86 memdump -D ./ -p 184

vol.py -f 0zapftis.vmem --profile=WinXPSP2x86 memdump -D ./ -p 544

strings 228.dmp 184.dmp 544.dmp 192.dmp > 2017325\_7\_b.txt

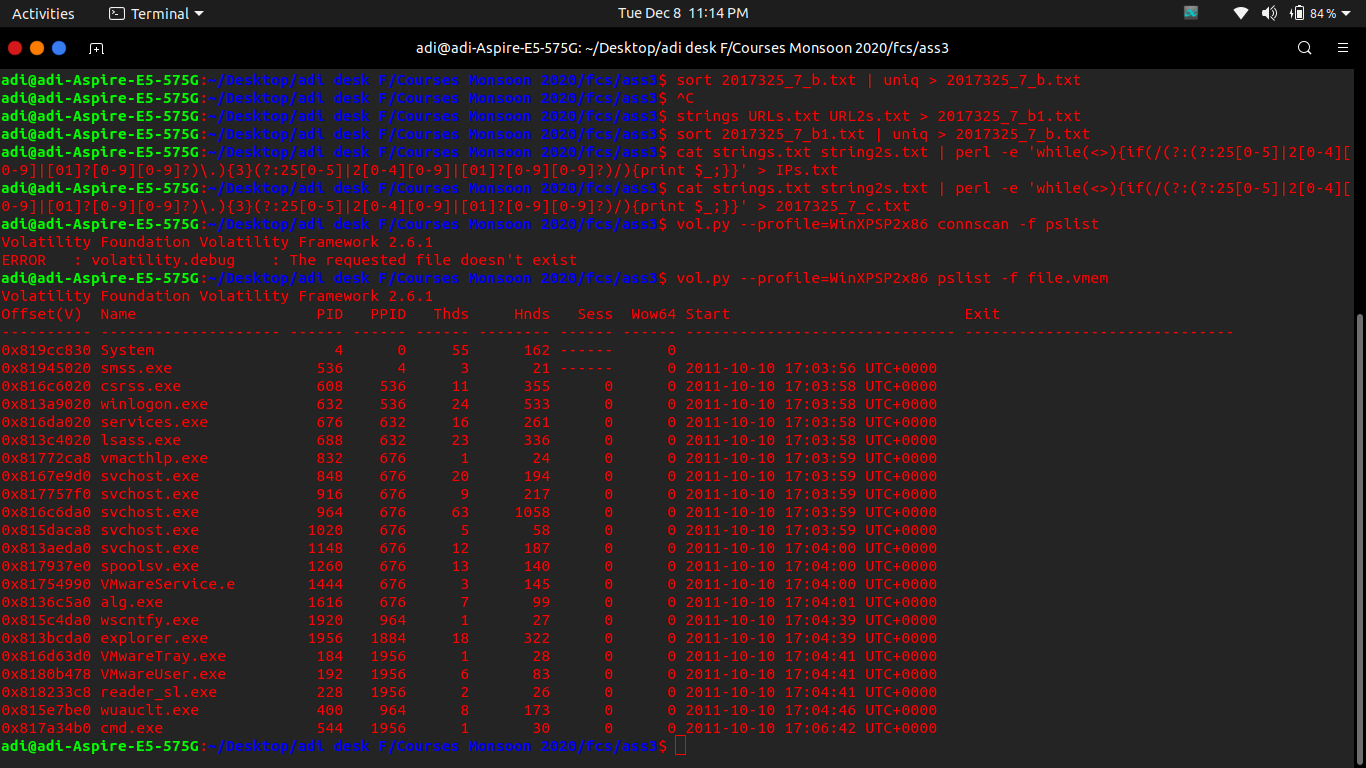




c. cat strings.txt string2s.txt | perl -e 'while(<>){if(/(?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9] [0-9]?)/){print $\_;}}' > 2017325\_7\_c.txt



d. vol.py --profile=WinXPSP2x86 pslist -f 0zapftis.vmem



e. vol.py --profile=WinXPSP2x86 pstree -f 0zapftis.vmem

192, 184, 544, 228 have the same parent.

0x813bcda0:explorer.exe 1956 1884 18 322 2011-10-10 17:04:39 UTC+0000

. 0x8180b478:VMwareUser.exe 192 1956 6 83 2011-10-10 17:04:41 UTC+0000

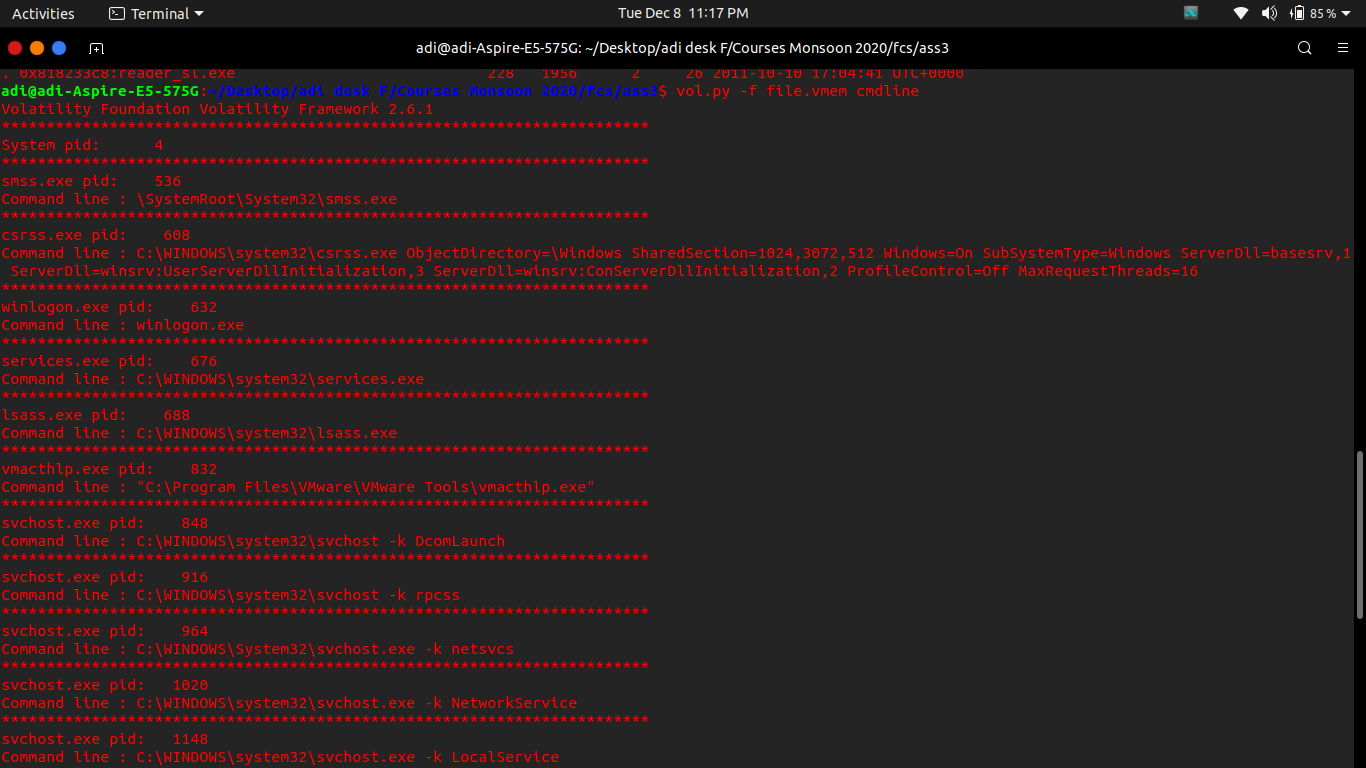
. 0x817a34b0:cmd.exe 544 1956 1 30 2011-10-10 17:06:42 UTC+0000

. 0x816d63d0:VMwareTray.exe 184 1956 1 28 2011-10-10 17:04:41 UTC+0000

. 0x818233c8:reader\_sl.exe 228 1956 2 26 2011-10-10 17:04:41 UTC+0000



f. vol.py -f 0zapftis.vmem cmdline

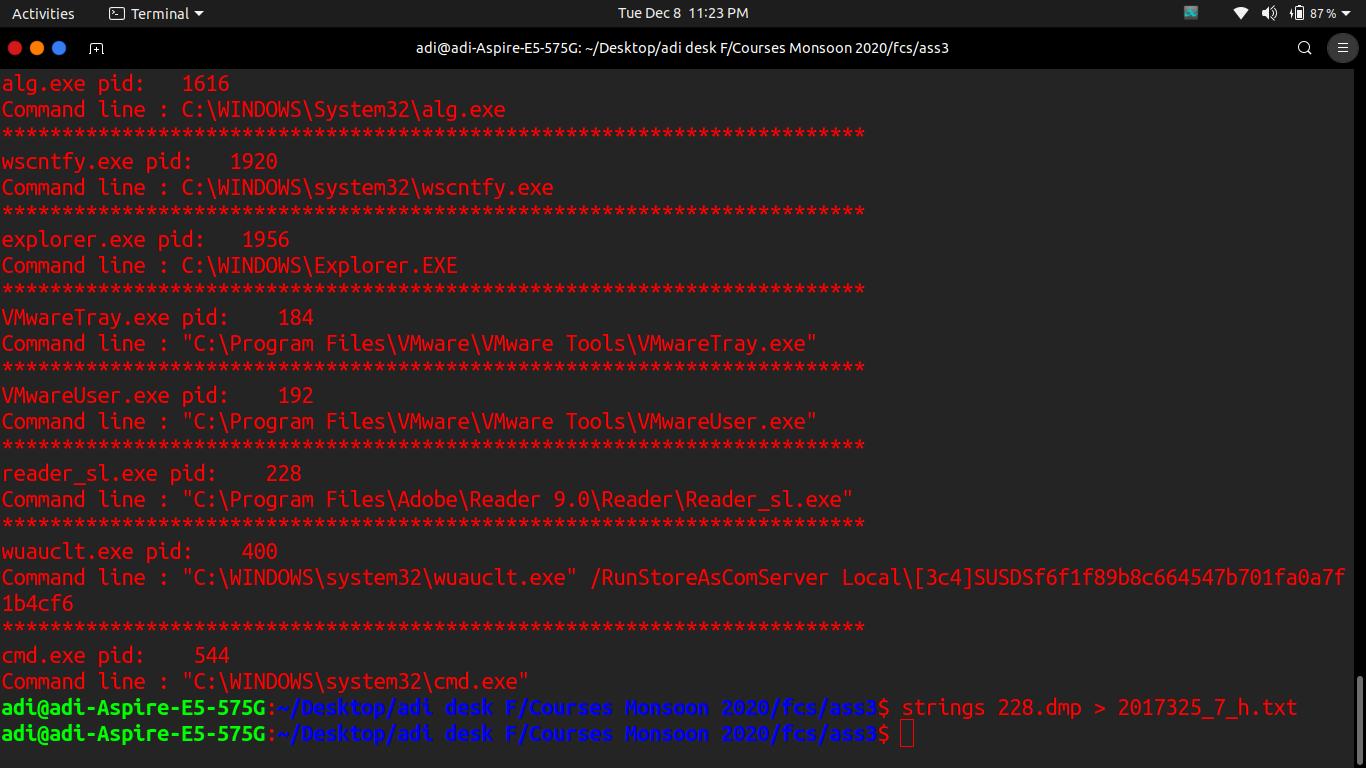


g. As discussed in class, any other process reaching the internet that is undefined for the resource usage at that time is suspicious. So here the process 228 is suspicious as it connected to the explorer.exe and did not have a defined use at that time, whereas others that did connect to the same parent had a defined usage. Process name - reader\_sl.exe:

. 0x818233c8:reader\_sl.exe 228 1956 2 26 2011-10-10 17:04:41 UTC+0000

h. vol.py -f file.vmem --profile=WinXPSP2x86 procdump -D ./ -p 228

strings 228.dmp > 2017325\_7\_h.txt



\*\*\*\*\*\* If you didnt get the password by yourself, it is - "infected"