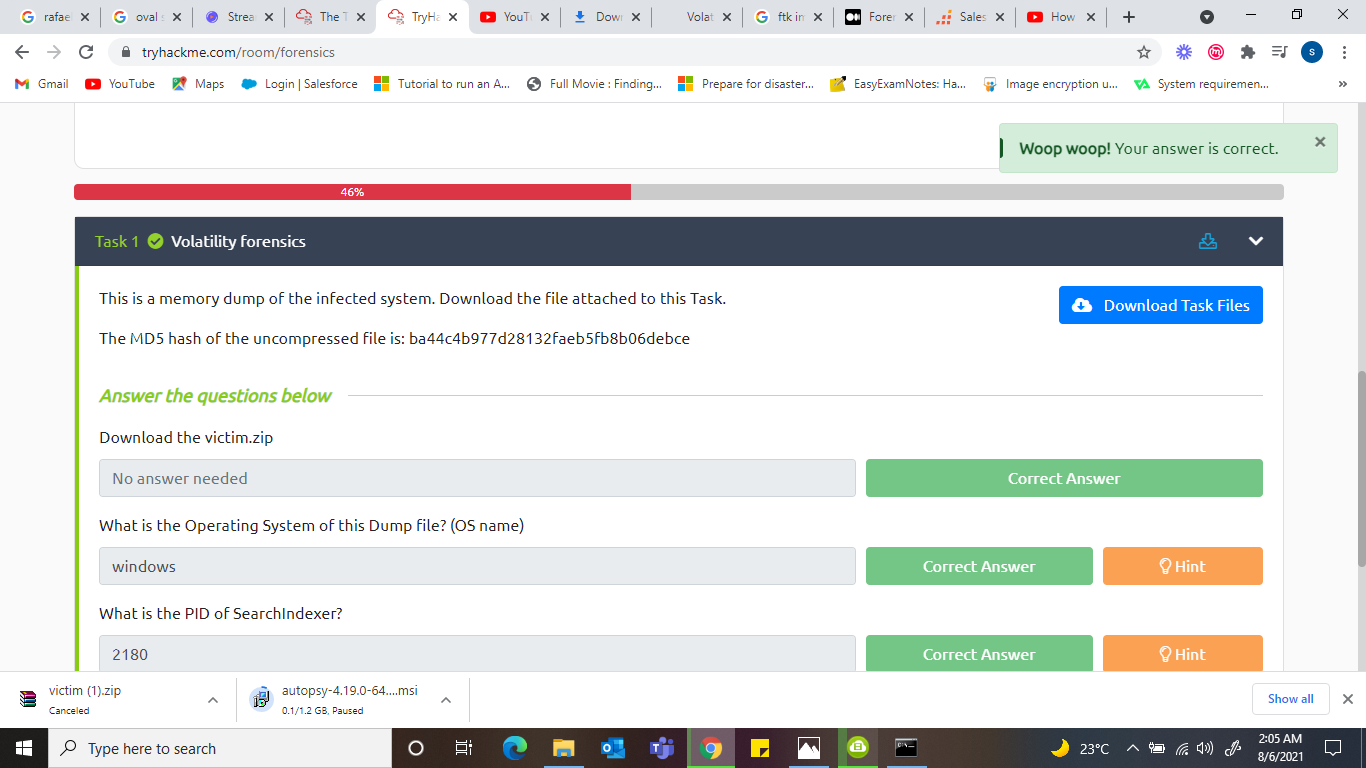
Sally Oketch.

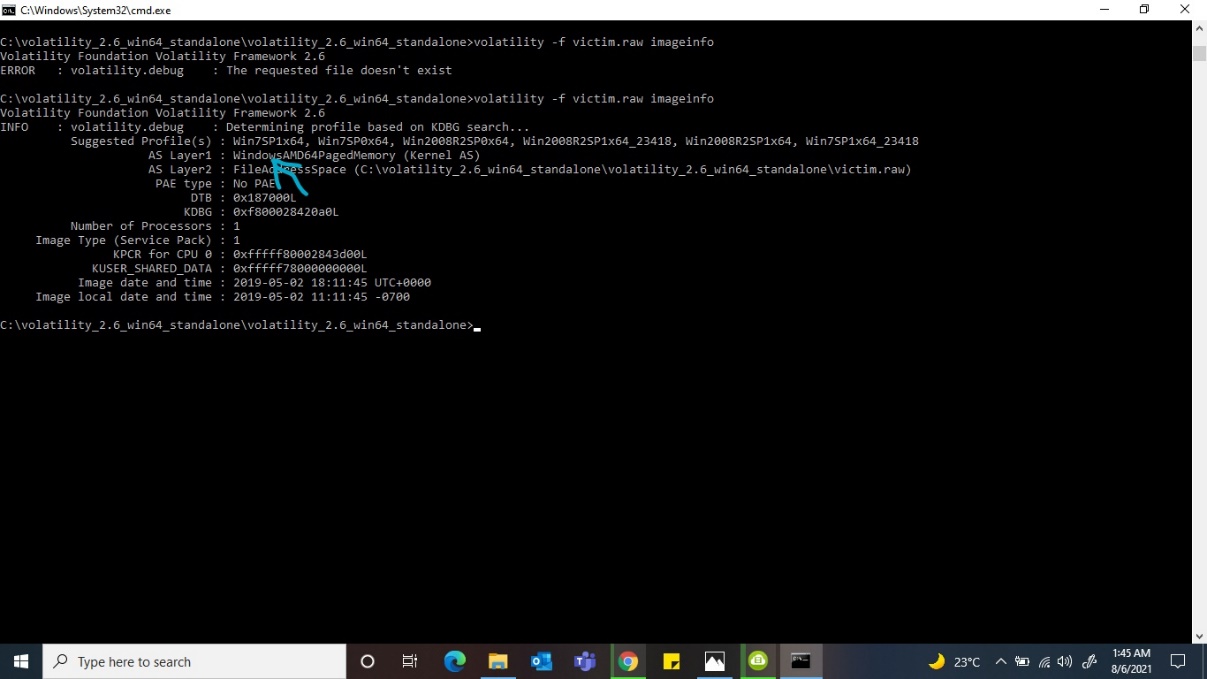
[Sally.oketch@womentechsters.org](mailto:Sally.oketch@womentechsters.org)

PRACTICAL ACTIVITY 9

**Task 1**

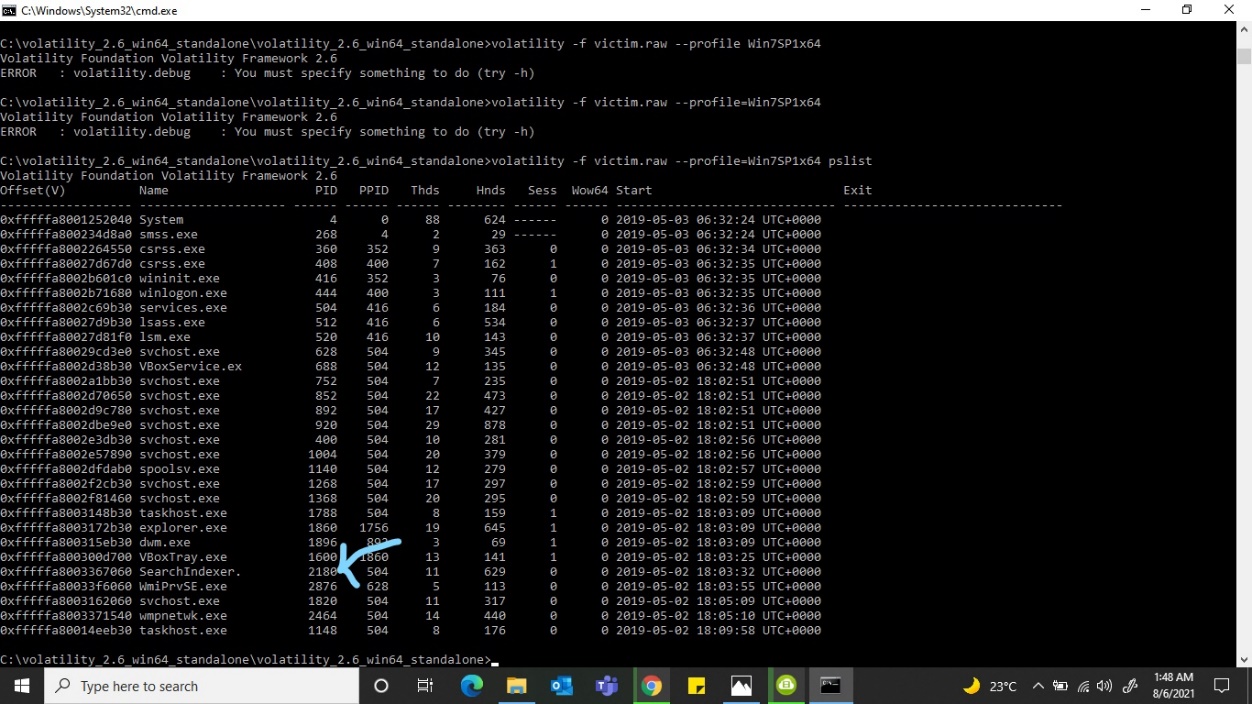


Operating system of dump file: ***windows***

***Volatility -f victim.raw imageinfo***

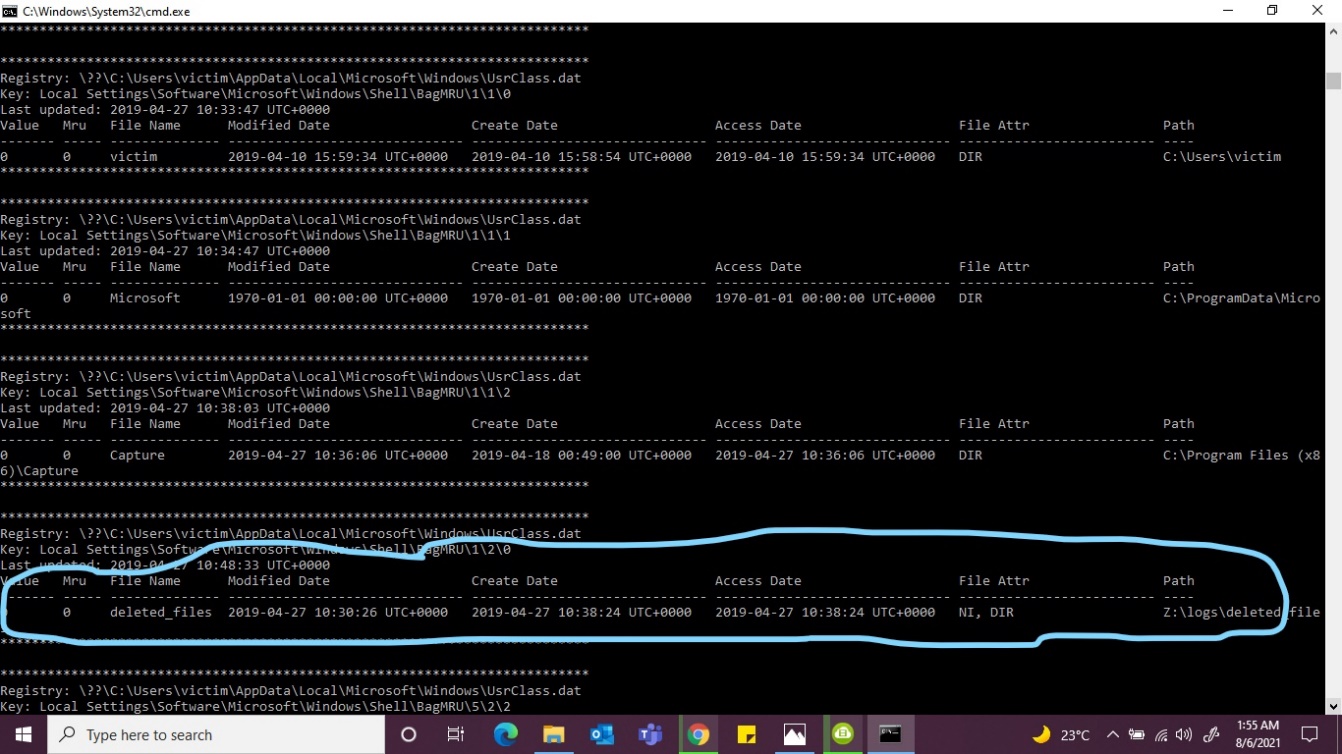
What is the PID of searchindexer***? 2180***

***Volatility -f victim.raw –profile=Win7SP1x64 pslist***

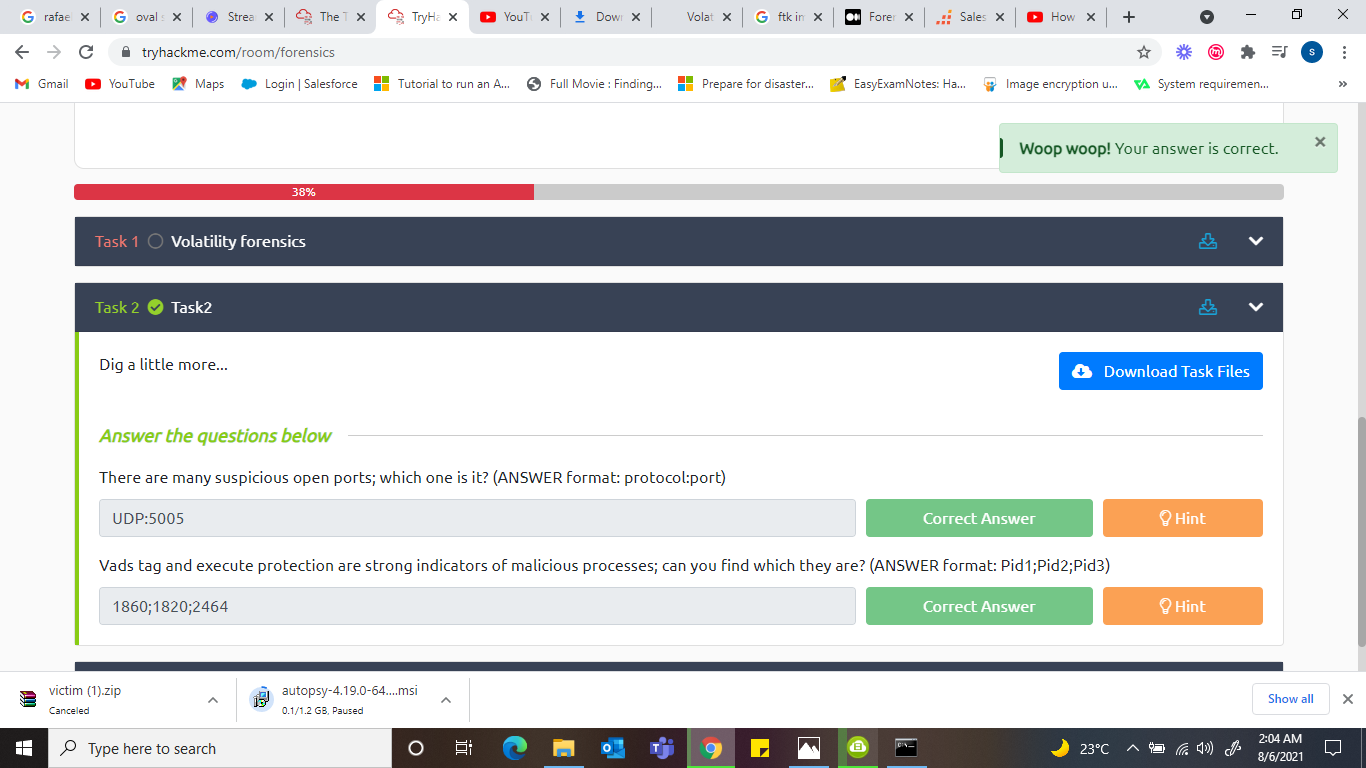
******

What is the last directory accessed by the user? deleted\_files

***Volatility -f victim.raw –profile=Win7SP1x64 shellbags***

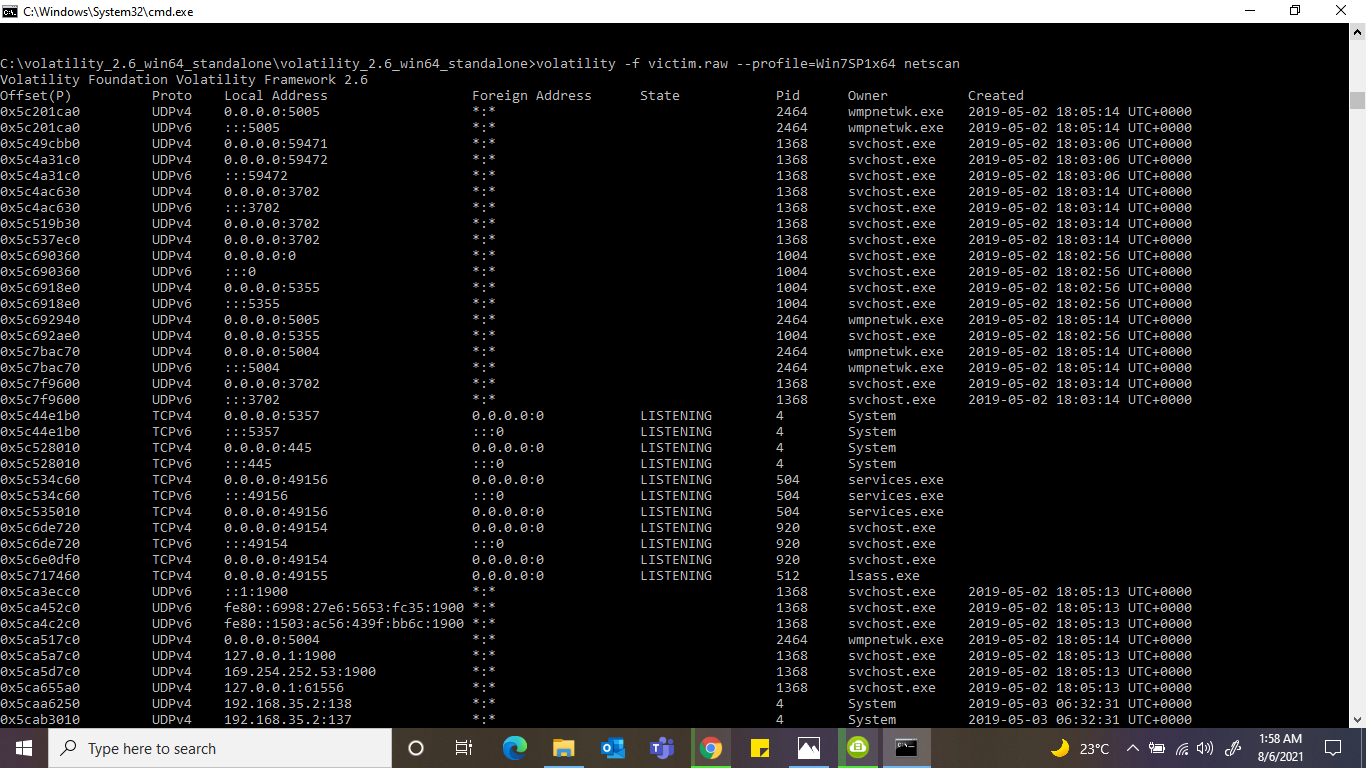
******

**Task 2**

****

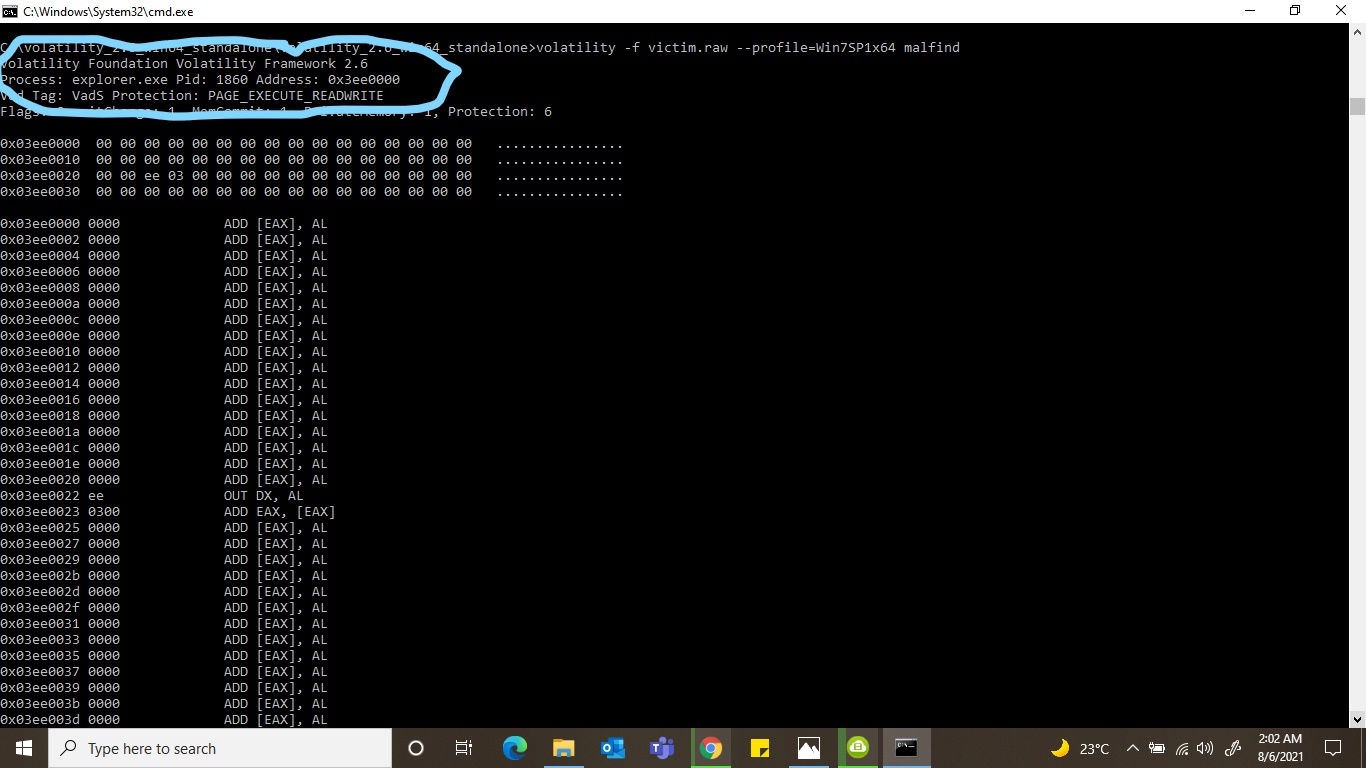
Suspicious open ports? ***UDP:5005***

***Volatility -f victim.raw –profile=Win7SP1x64 netscan***

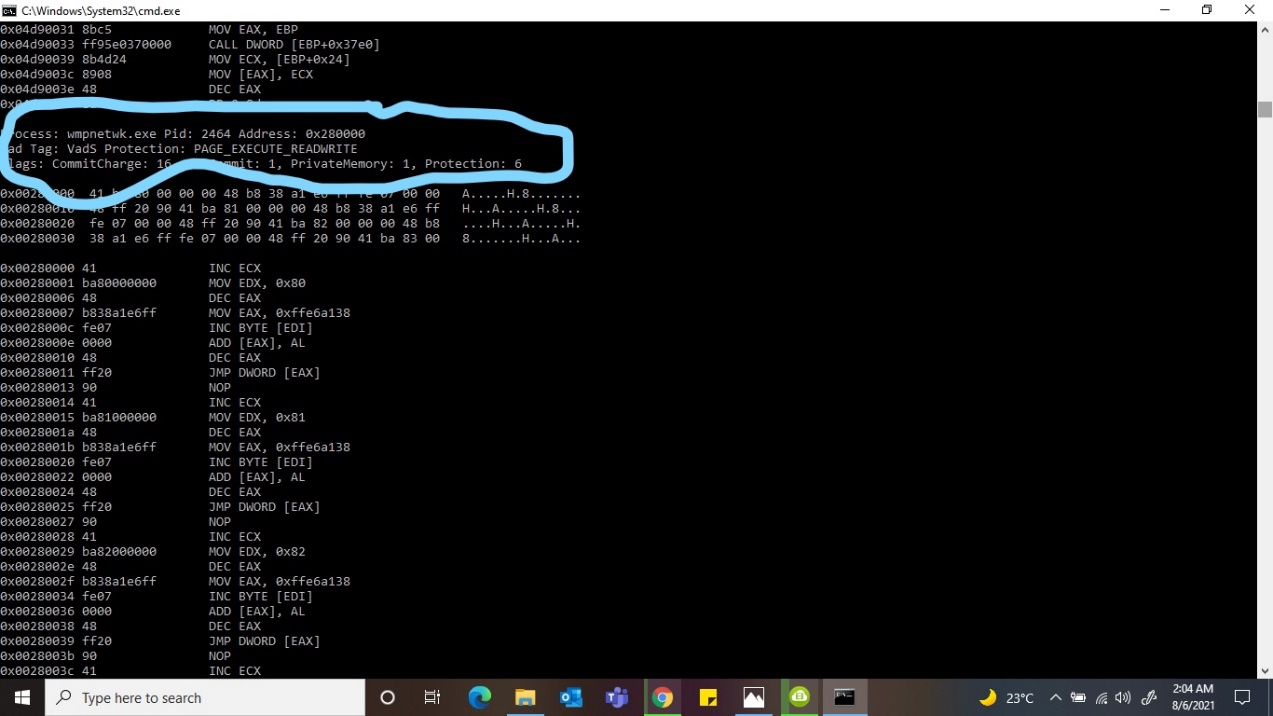


Vads tag and execute protection are strong indicators of malicious processes, which are they? ***1860;1820;2464***

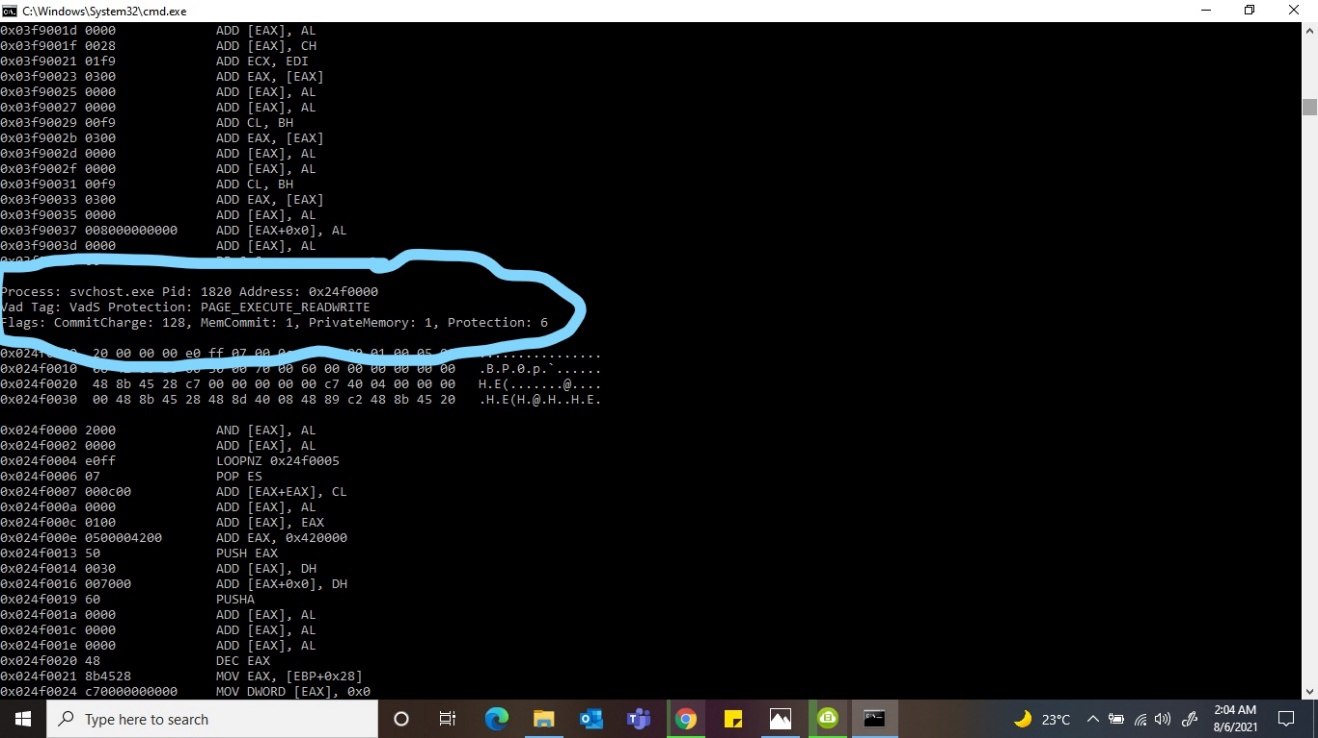
***1860***



**2464**



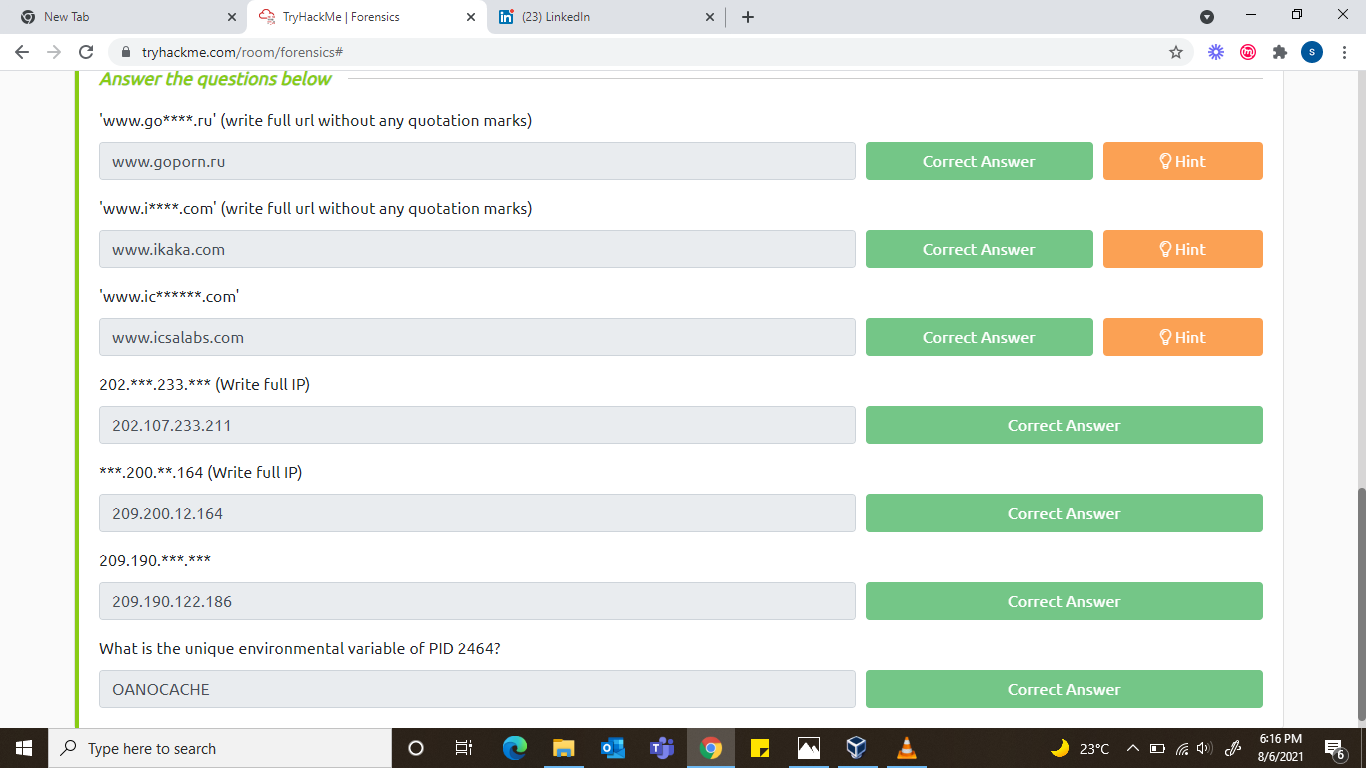
**1820**



**TASK 3**

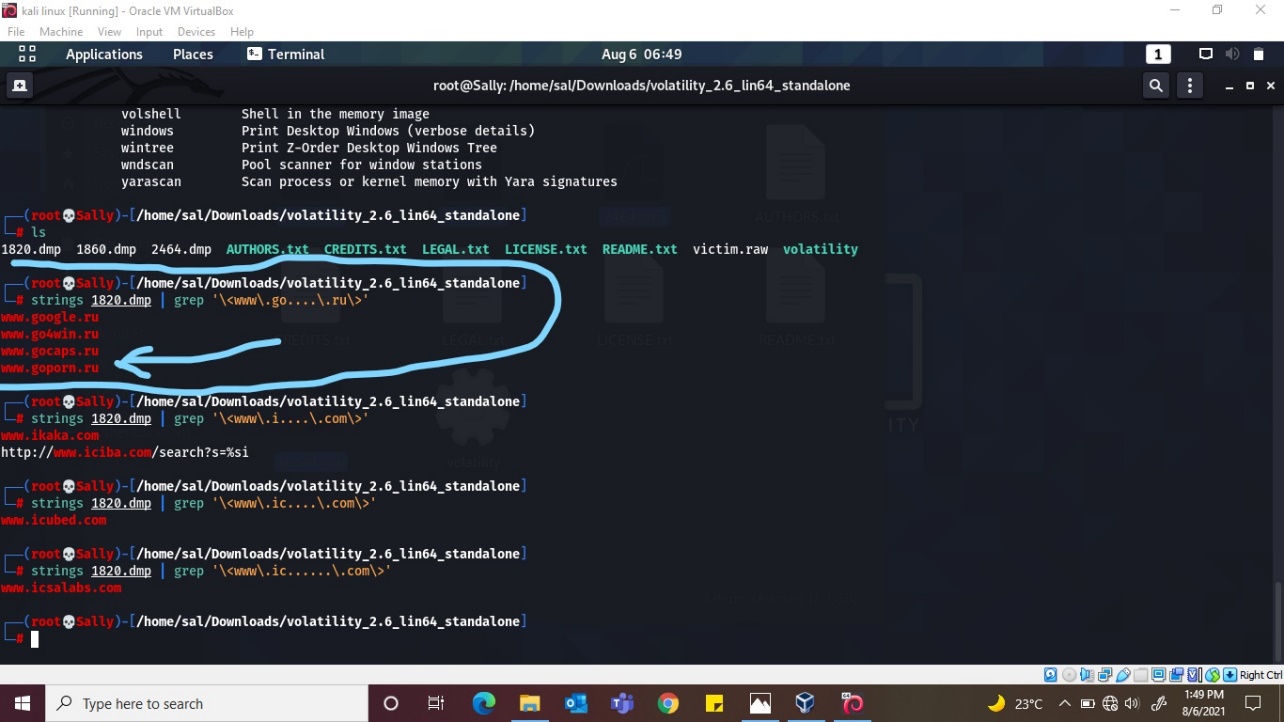
I went ahead and created 3 dump files using the memdump command.

**Volatility -f victim.raw –profile=Win7SP1x64 memdump -p 1860,1820,2464 -D**

****

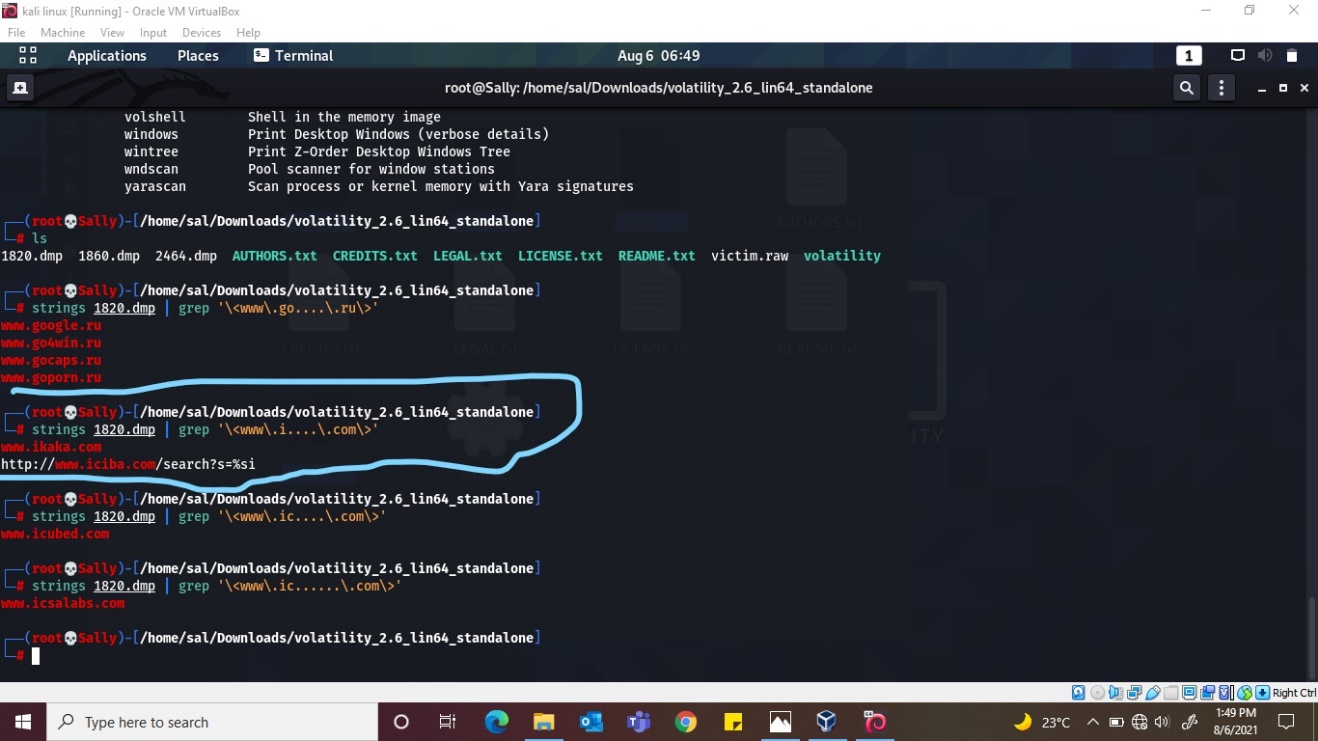
**‘www.go\*\*\*\*.ru’**

**Strings 1820.dmp | grep ‘<\www\.go….\.ru\>’**

****

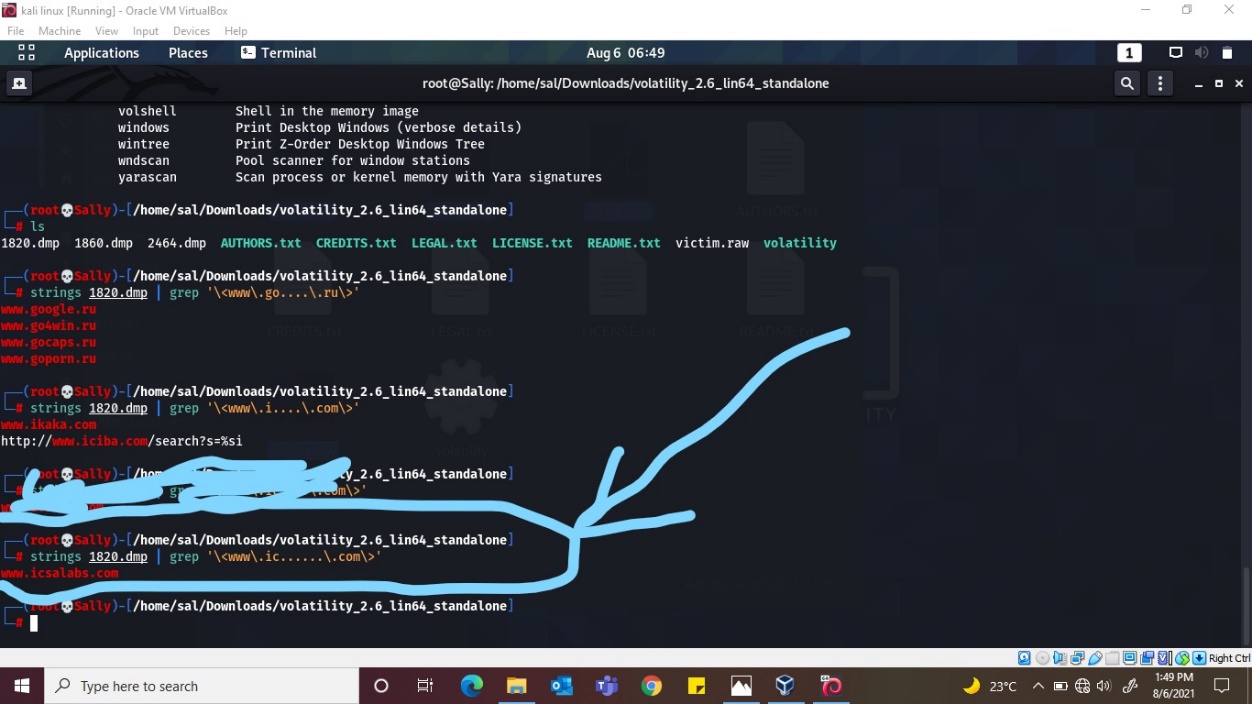
**‘www.i\*\*\*\*.com’**

**Strings 1820.dmp | grep ‘<\www\.i….\.com\>’**

****

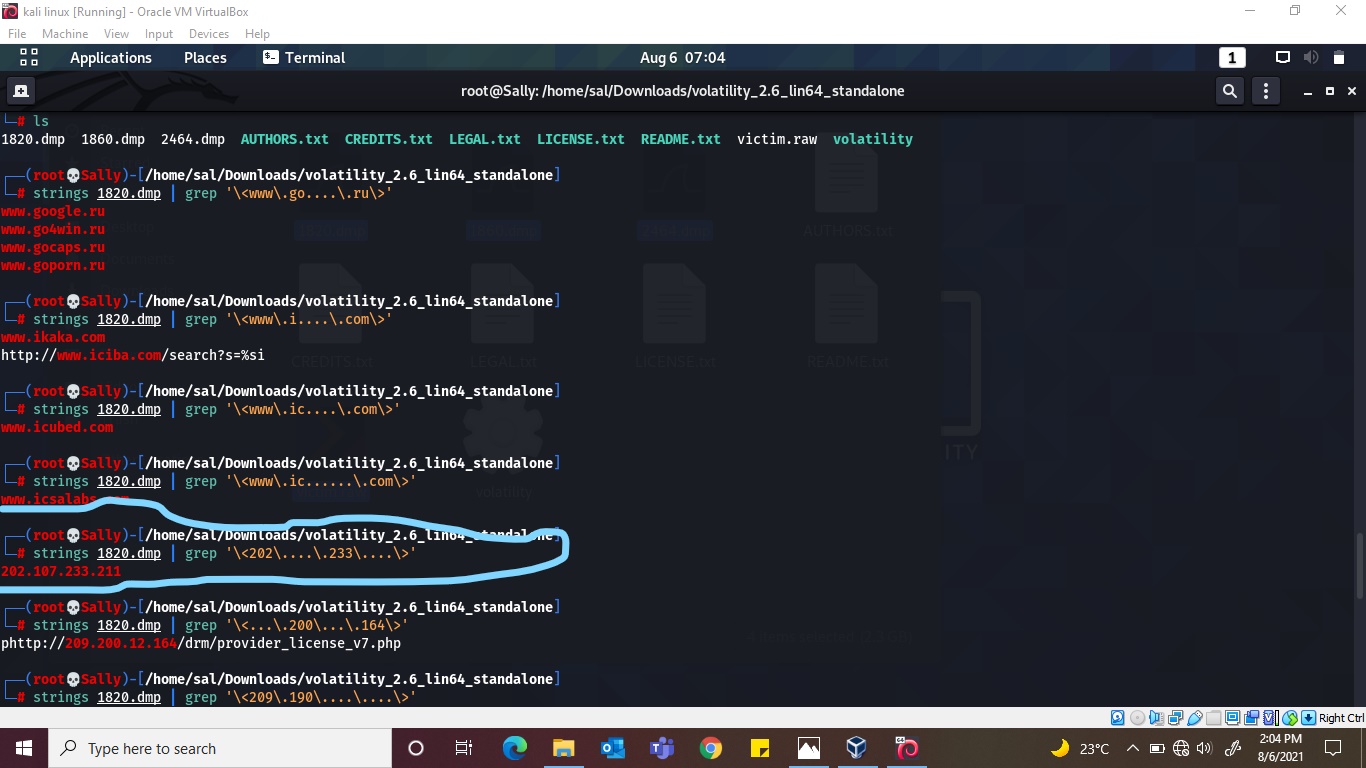
**‘www.ic\*\*\*\*\*\*.com’**

**Strings 1820.dmp | grep ‘<\www\.ic..….\.com\>’**

****

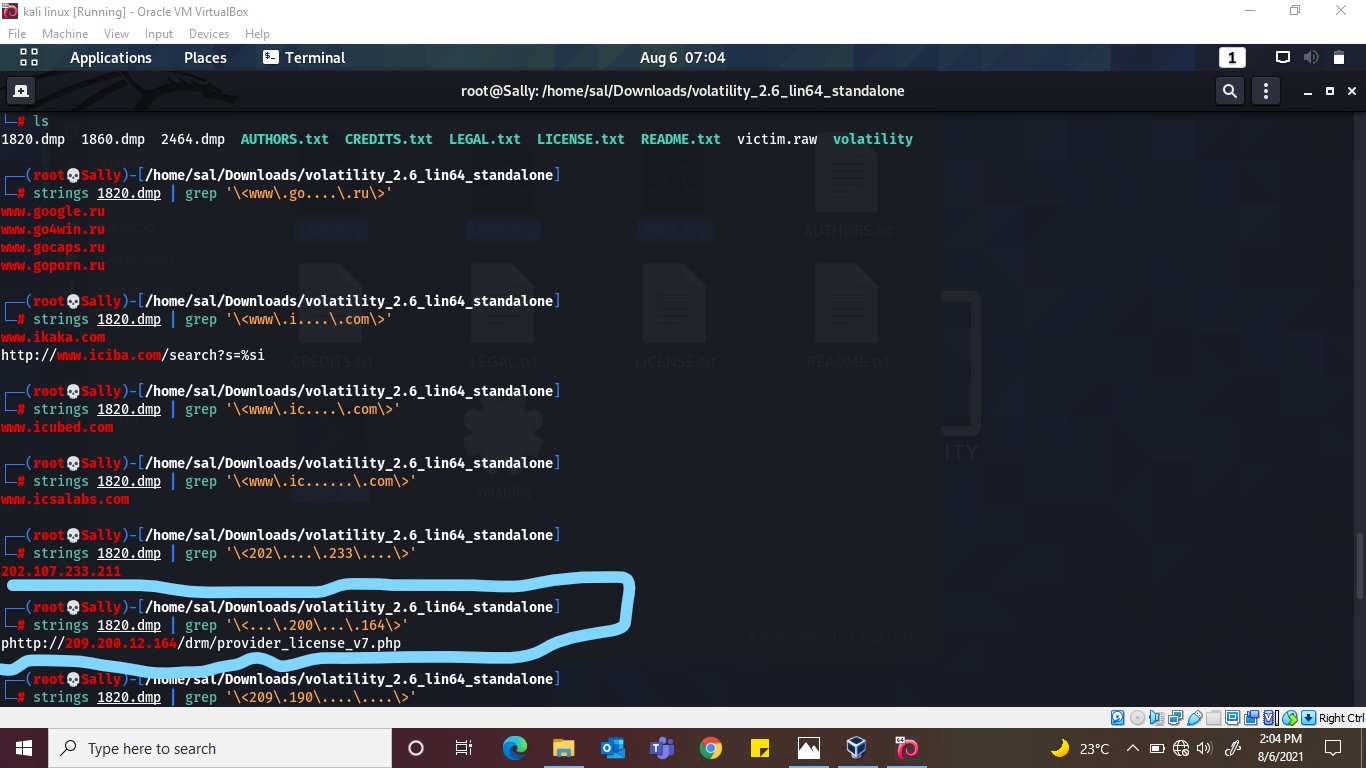
**202.\*\*\*.233.\*\*\***

**Strings 1820.dmp | grep ‘\<202\...\.233\....\>’**

****

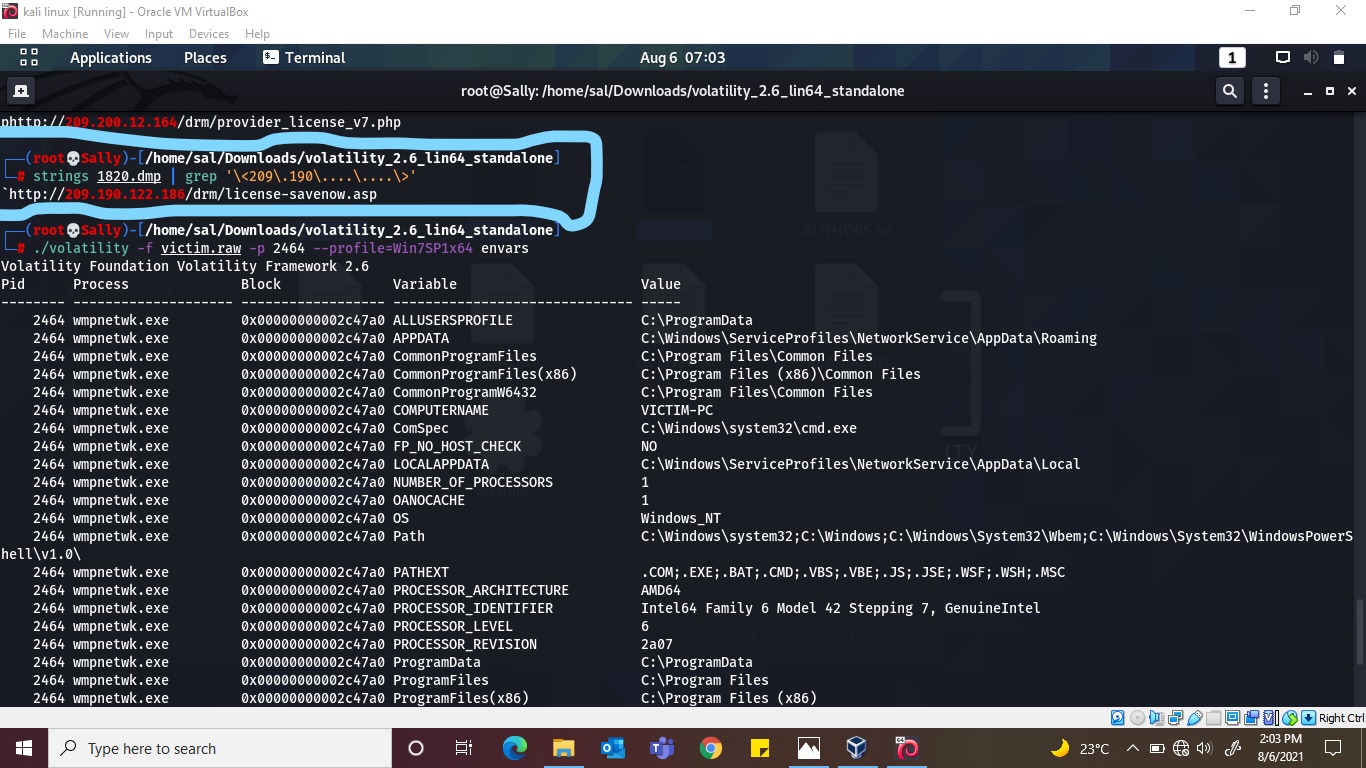
**\*\*\*.200.\*\*.164**

**Strings 1820.dmp | grep ‘\<…\.200\...\.104\>’**

****

**209.190.\*\*\*.\*\*\***

**Strings 1820.dmp | grep ‘\<209\.190\....\....\>’**

****

What is the unique environmental variable of PID 2464 ? **OANOCACHE**

**./volatility -f victim.raw -p 2464 –profile=Win7SP1x64 envars**

****