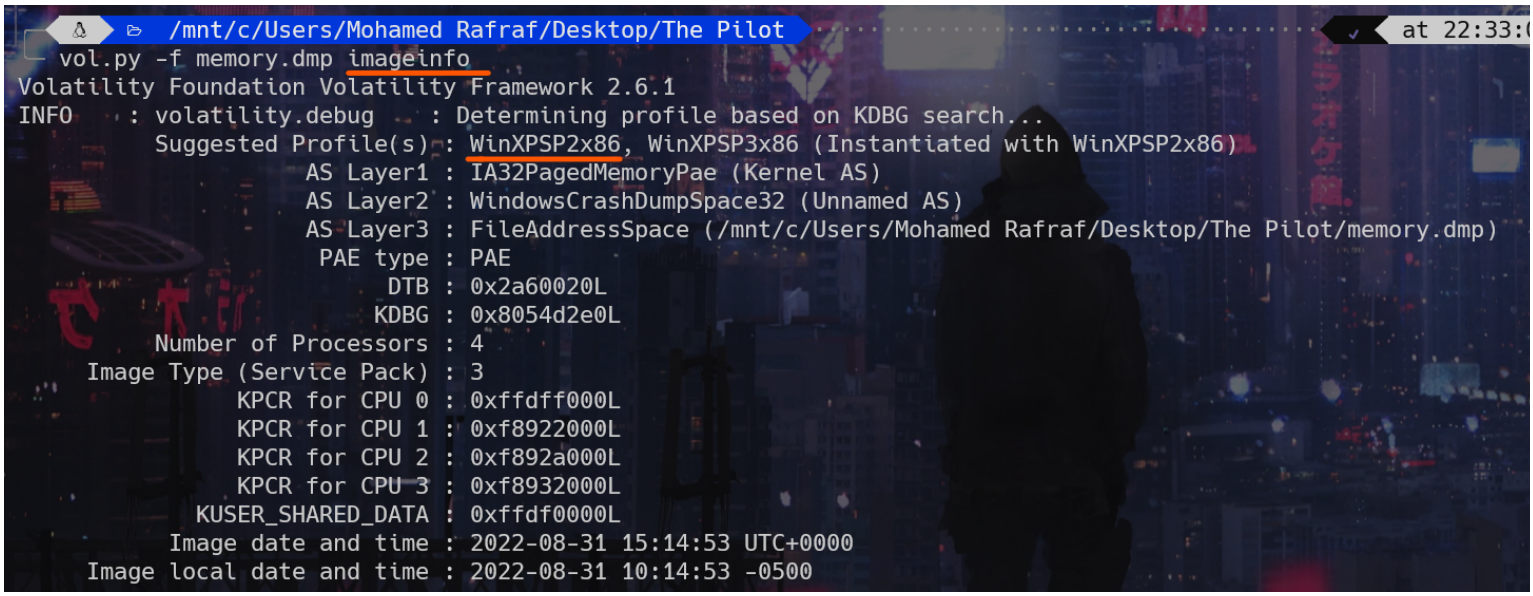
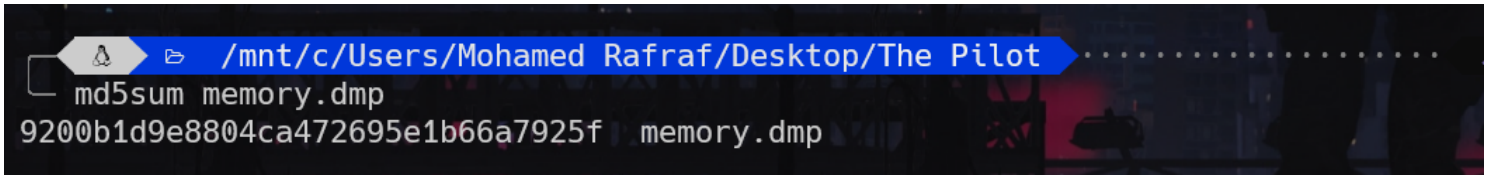
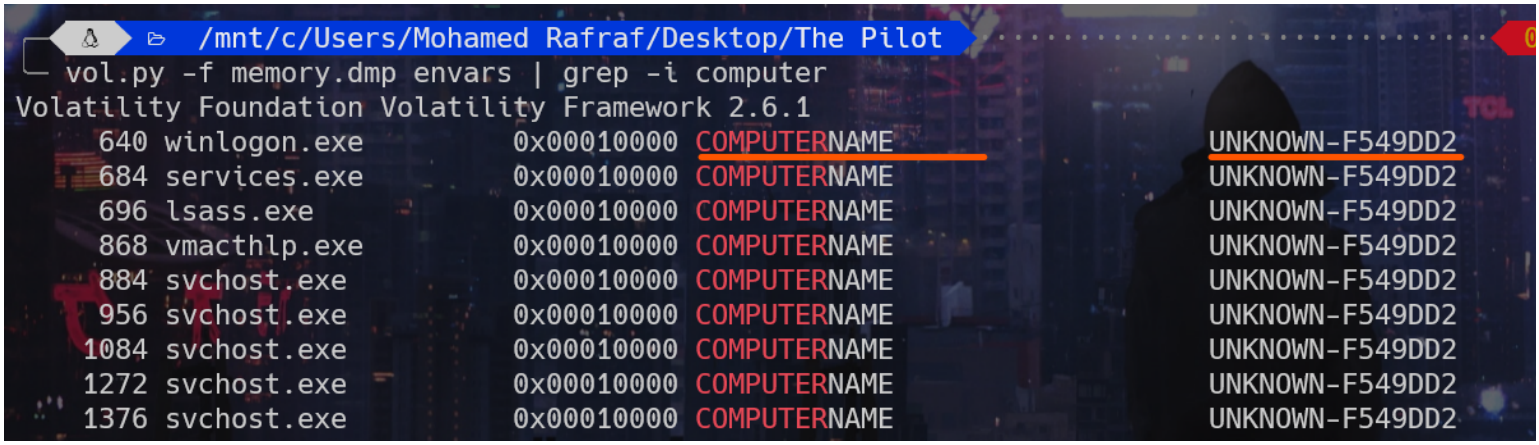
What volatility profile is the most appropriate for this machine? | Weight: +25



What is the MD5 hash of the memory dump? | Weight: +25



What is the hostname? | Weight: +25



What is the PID of the Notepad process? | Weight: +25

```
/mnt/c/Users/Mohamed Rafraf/Desktop/The Pilot ..... took 35s ⧗ at 22:4
└─ vol.py -f memory.dmp pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c6830:System                                      4      0     69    259 1970-01-01 00:00:00 UTC+0000
. 0x81e16550:smss.exe                                 552      4      3     19 2022-08-31 15:03:46 UTC+0000
.. 0x8202e2c0:winlogon.exe                            640    552     16    292 2022-08-31 15:03:49 UTC+0000
... 0x81fdb458:services.exe                           684    640     15    301 2022-08-31 15:03:50 UTC+0000
.... 0x81e9d948:alg.exe                              1680    684      7    113 2022-08-31 15:04:38 UTC+0000
.... 0x81e11a78:svchost.exe                          1292    684      4    112 2022-08-31 15:04:15 UTC+0000
.... 0x822507e8:svchost.exe                           816    684     21    432 2022-08-31 15:04:16 UTC+0000
.... 0x81e16808:svchost.exe                          1084    684     73   1199 2022-08-31 15:03:54 UTC+0000
..... 0x81ea1550:wscntfy.exe                         1344   1084      1     43 2022-08-31 15:04:35 UTC+0000
..... 0x81f31020:wuauclt.exe                         2924   1084      7    141 2022-08-31 15:09:55 UTC+0000
.... 0x821f3228:svchost.exe                          1376    684     13    190 2022-08-31 15:03:56 UTC+0000
.... 0x82041da0:vmacthlp.exe                          868    684      1     26 2022-08-31 15:03:52 UTC+0000
.... 0x81ef3b20:VGAuthService.e                      1768    684      2     60 2022-08-31 15:04:19 UTC+0000
.... 0x81e09020:svchost.exe                           956    684     11    310 2022-08-31 15:03:53 UTC+0000
.... 0x81a75770:spoolsv.exe                          1520    684     10    142 2022-08-31 15:03:59 UTC+0000
.... 0x8225c8a0:vmtoolsd.exe                          168    684      8    279 2022-08-31 15:04:27 UTC+0000
..... 0x820ae020:cmd.exe                             2732    168      0 ------ 2022-08-31 15:14:52 UTC+0000
.... 0x81e263e8:svchost.exe                           884    684     22    235 2022-08-31 15:03:52 UTC+0000
..... 0x81ebc8c8:wmiprvse.exe                         496    884     13    283 2022-08-31 15:04:33 UTC+0000
.... 0x820f6da0:svchost.exe                          1272    684      4     81 2022-08-31 15:03:55 UTC+0000
... 0x81e1da70:lsass.exe                              696    640     27    394 2022-08-31 15:03:50 UTC+0000
.. 0x821fb020:csrss.exe                               616    552     12    475 2022-08-31 15:03:47 UTC+0000
 0x81f10158:explorer.exe                             1308   1216     17    493 2022-08-31 15:04:15 UTC+0000
. 0x81a50020:cmd.exe                                 3904   1308      1     30 2022-08-31 15:07:25 UTC+0000
. 0x81fbe3c0:ctfmon.exe                              1164   1308      1     94 2022-08-31 15:04:23 UTC+0000
. 0x81e82508:clipbrd.exe                             3048   1308      1     64 2022-08-31 15:05:51 UTC+0000
. 0x82023228:vmtoolsd.exe                            1972   1308      5    151 2022-08-31 15:04:23 UTC+0000
. 0x81e27da0:notepad.exe                              584   1308      1     61 2022-08-31 15:05:02 UTC+0000
. 0x820b9da0:iexplore.exe                             312   1308     14    593 2022-08-31 15:05:15 UTC+0000
```

What is the PID of the Explorer process? | Weight: +25 : 1308

What is the parent process start time of notepad.exe? | Weight: +50 : 2022-08-31 15:04:15

```
 0x81f10158:explorer.exe                             1308   1216     17    493 2022-08-31 15:04:15 UTC+0000
. 0x81a50020:cmd.exe                                 3904   1308      1     30 2022-08-31 15:07:25 UTC+0000
. 0x81fbe3c0:ctfmon.exe                              1164   1308      1     94 2022-08-31 15:04:23 UTC+0000
. 0x81e82508:clipbrd.exe                             3048   1308      1     64 2022-08-31 15:05:51 UTC+0000
. 0x82023228:vmtoolsd.exe                            1972   1308      5    151 2022-08-31 15:04:23 UTC+0000
. 0x81e27da0:notepad.exe                              584   1308      1     61 2022-08-31 15:05:02 UTC+0000
```

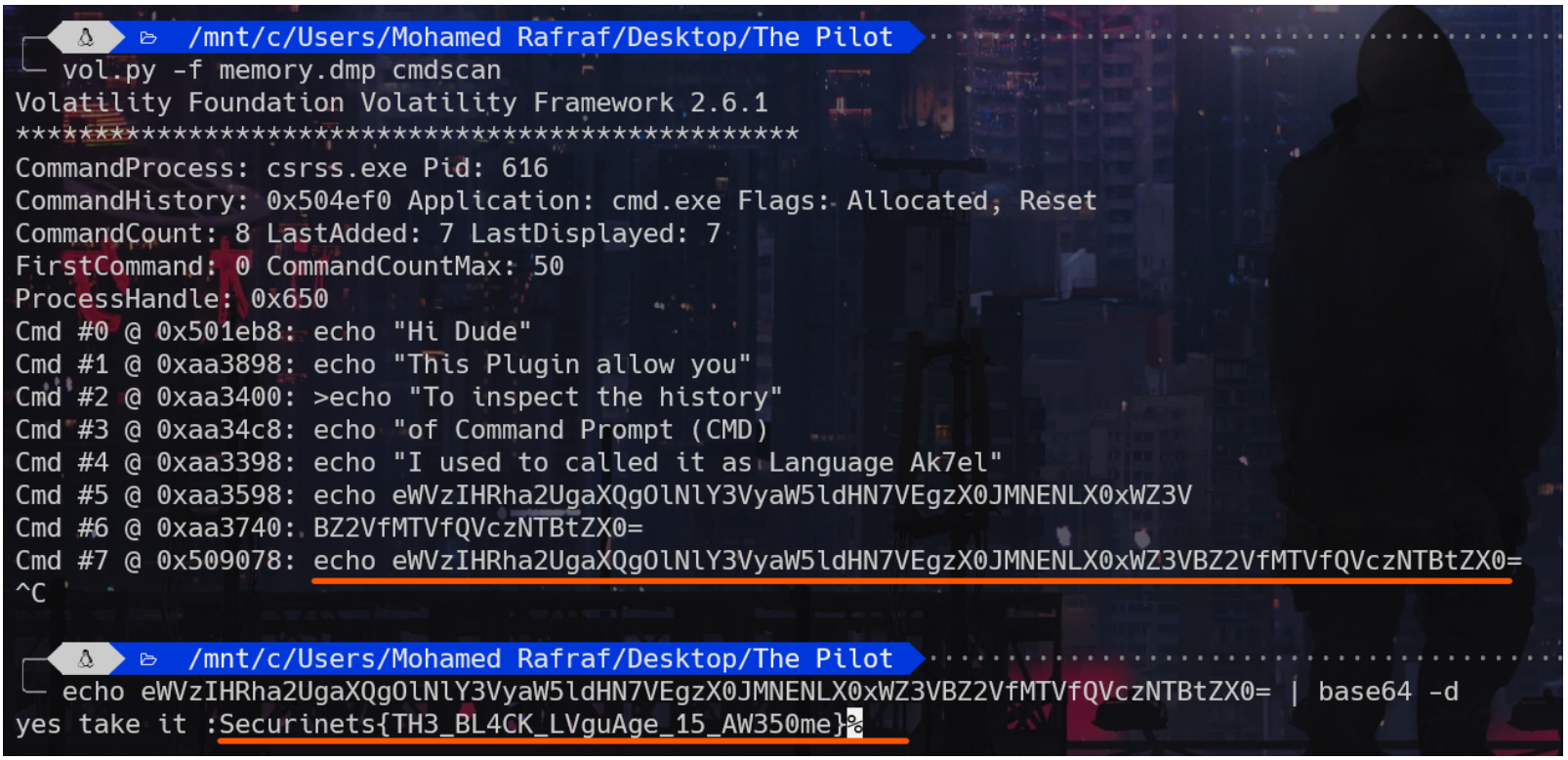
What is the IP Address used by the machine? | Weight: +50

```
/mnt/c/Users/Mohamed Rafraf/Desktop/The Pilot
└─ vol.py -f memory.dmp connscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x01c2d6e0 192.168.1.130:1121       52.97.201.226:443         312
0x01c30638 192.168.1.130:1090       104.20.67.143:443         564
0x01c69e68 192.168.1.130:1113       41.231.245.24:443         564
0x01c77008 192.168.1.130:1098       92.123.112.145:443        564
0x01c9d008 192.168.1.130:1124       20.190.159.5:443          564
0x02039420 37.0.0.0:0               42.0.0.0:8192             23
```

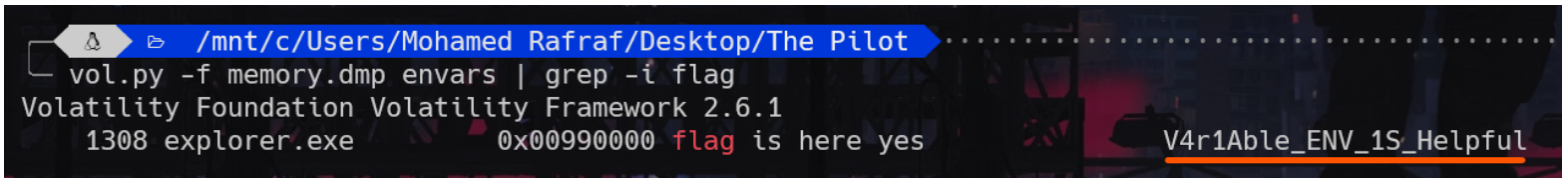
What is the executable path for process ID 1164? | Weight: +75

```
/mnt/c/Users/Mohamed Rafraf/Desktop/The Pilot
└─ vol.py -f memory.dmp cmdline | grep 1164 -C 1
Volatility Foundation Volatility Framework 2.6.1
**************************************************
ctfmon.exe pid:   1164
Command line : "C:\WINDOWS\system32\ctfmon.exe"
```

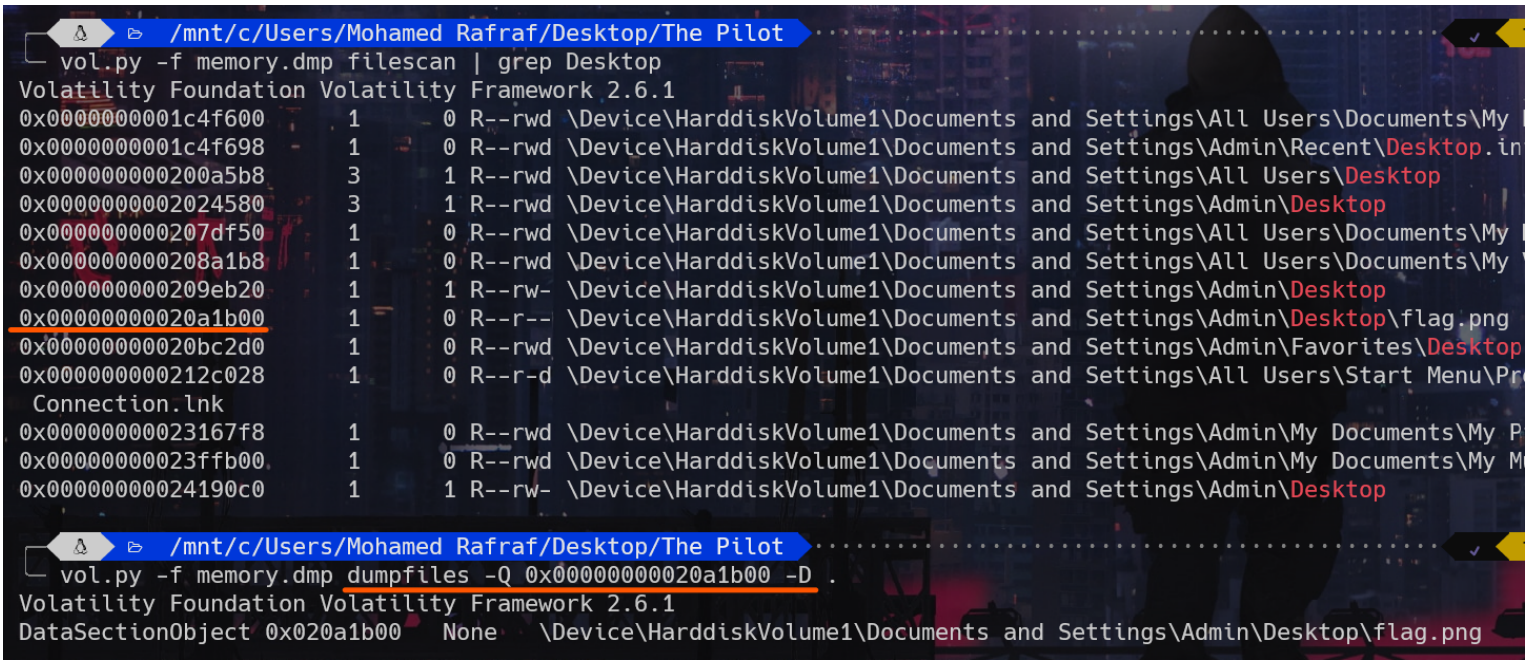
My Grandfather calls CMD, the Black Language, can you find the flag there? | Weight: +50



My Grandfather is environmental, can you find the flag? | Weight: +75 (it's hint about variable env)

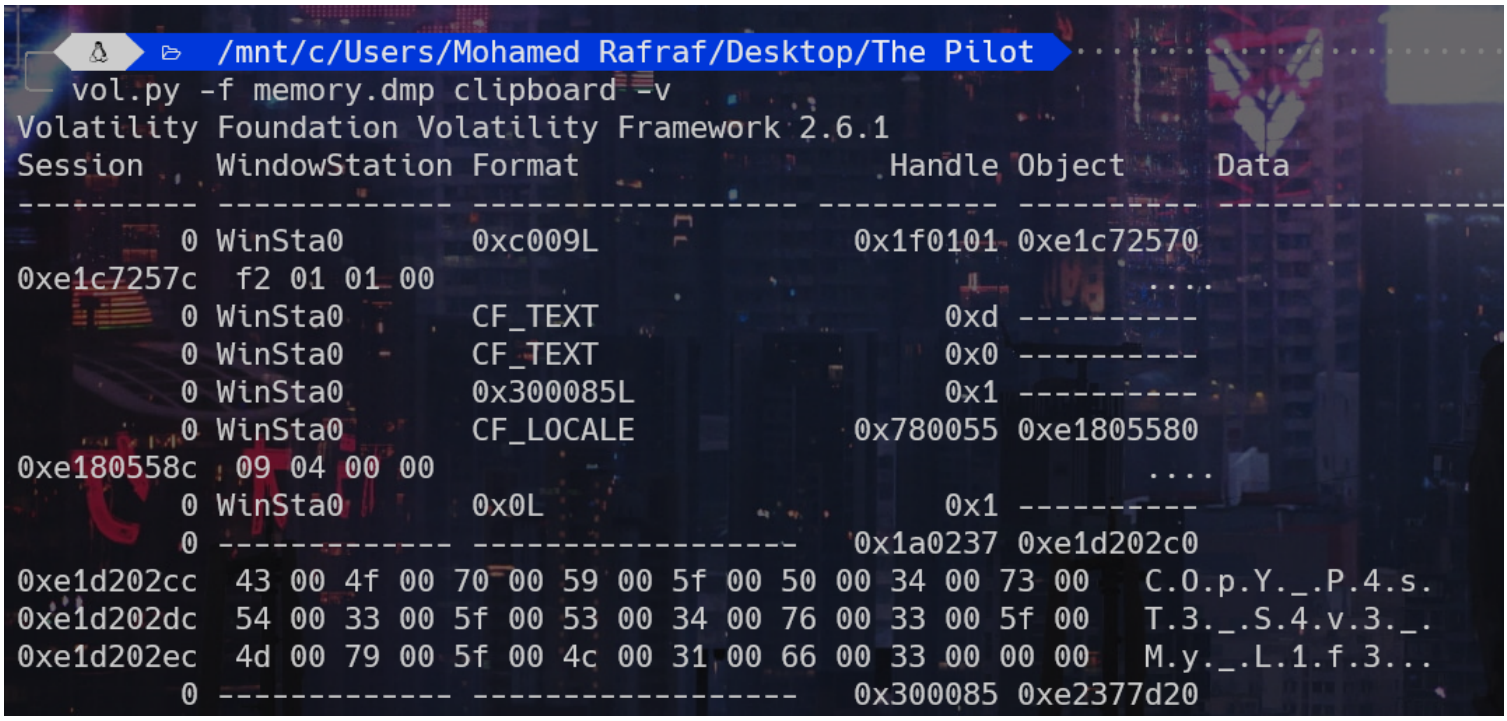


My Grandfather left something in the Desktop, can you find it? | Weight: +100

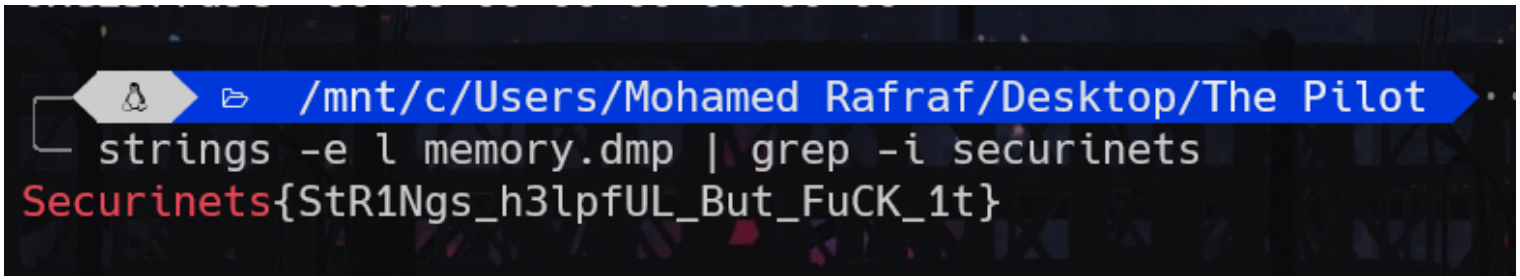


Securinets{Dump_F1L3S_1S_My_Be5t_PLuG1N}

My Grandfather copied his password, can you find it? | Weight: +100



Just one more mysterious flag, can you find it? | Weight: +200:
Mmm just i wrote the flag in notepad , strings -e l (little endian) will be helpful to get the flag



My grandfather had saved some senetive information in a sepecific website. Can you find what's been hidden in the history of his default browser

Run Vol.py -f memory.dmp iehistory