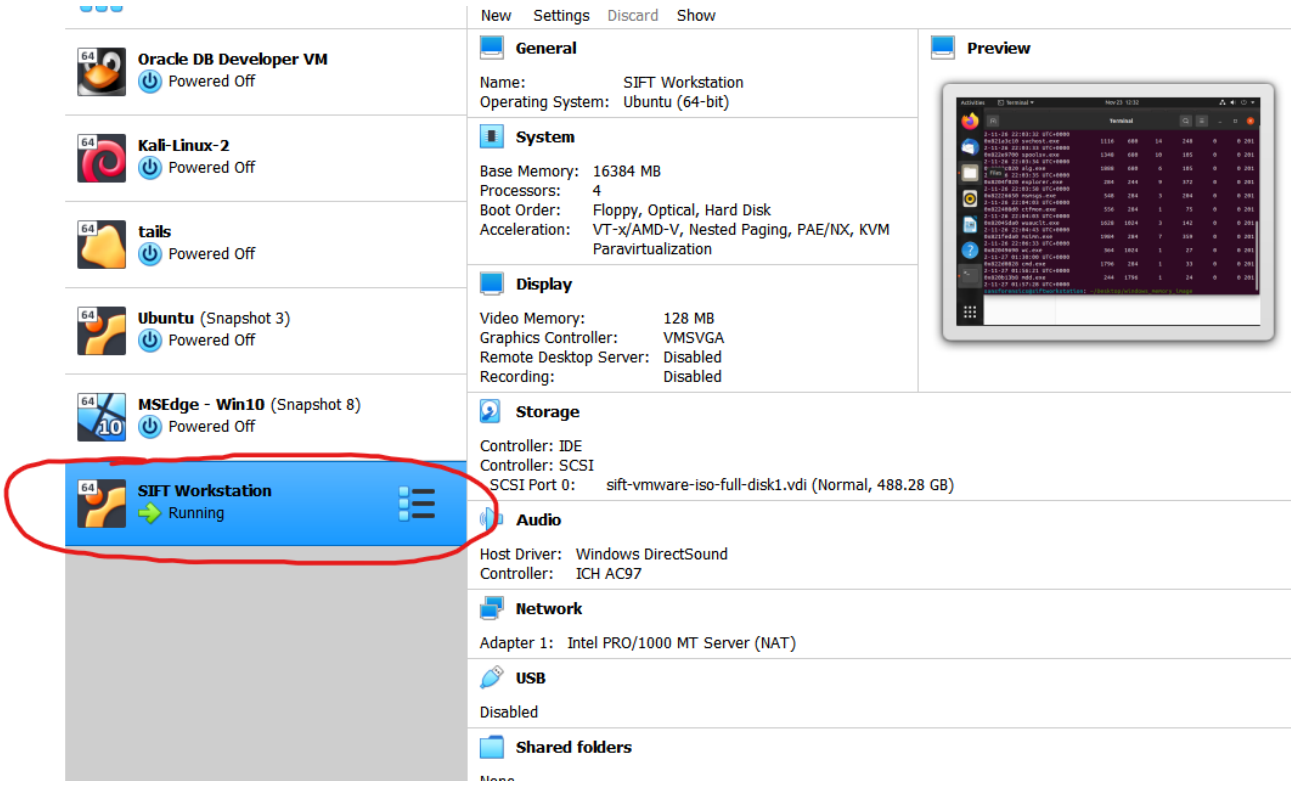
1) Download SIFT VM



General

Name: SIFT Workstation
Operating System: Ubuntu (64-bit)

System

Base Memory: 16384 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
Controller: SCSI
SCSI Port 0: sift-vmware-iso-full-disk1.vdi (Normal, 488.28 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

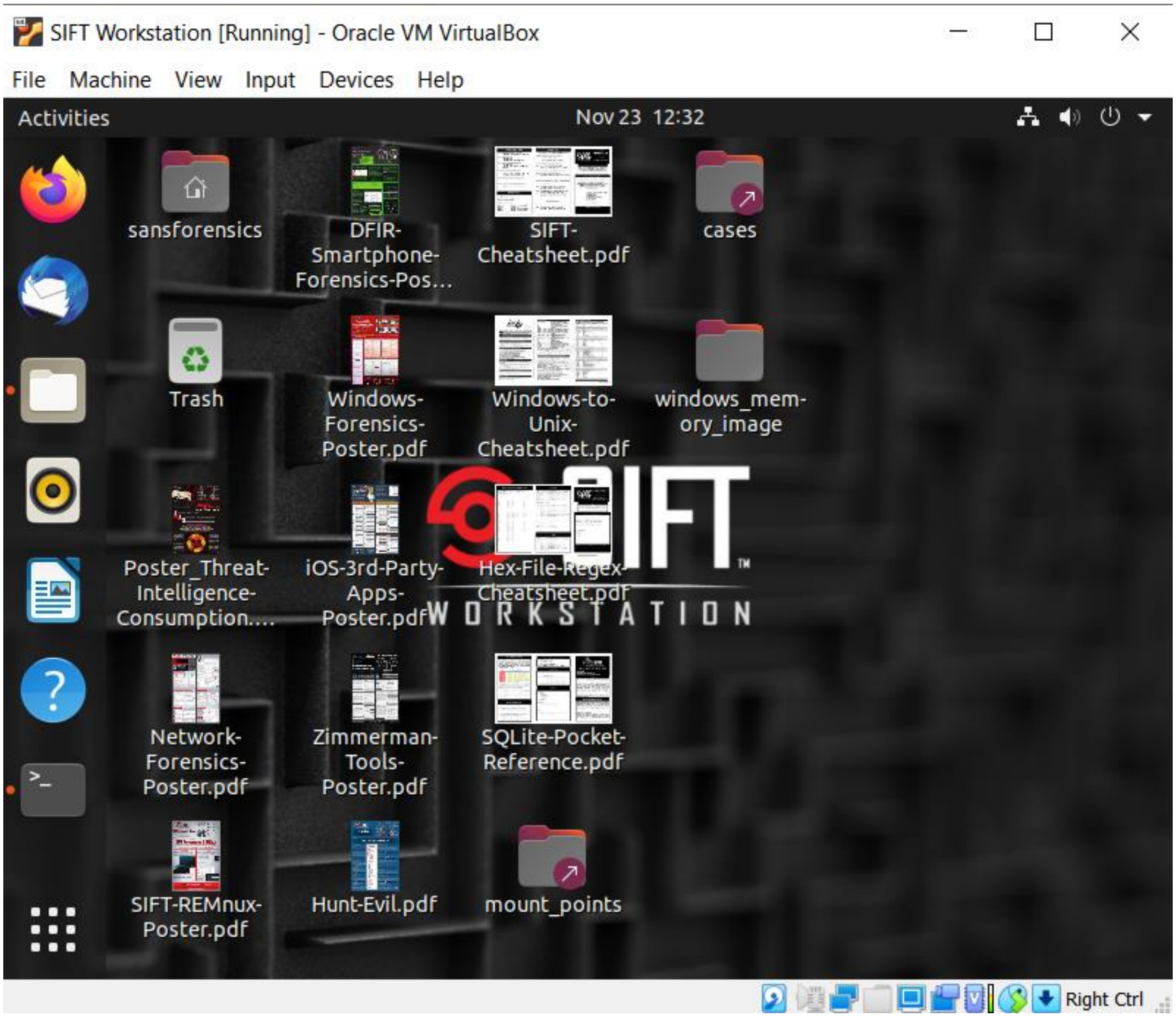
Adapter 1: Intel PRO/1000 MT Server (NAT)

USB

Disabled

Shared folders

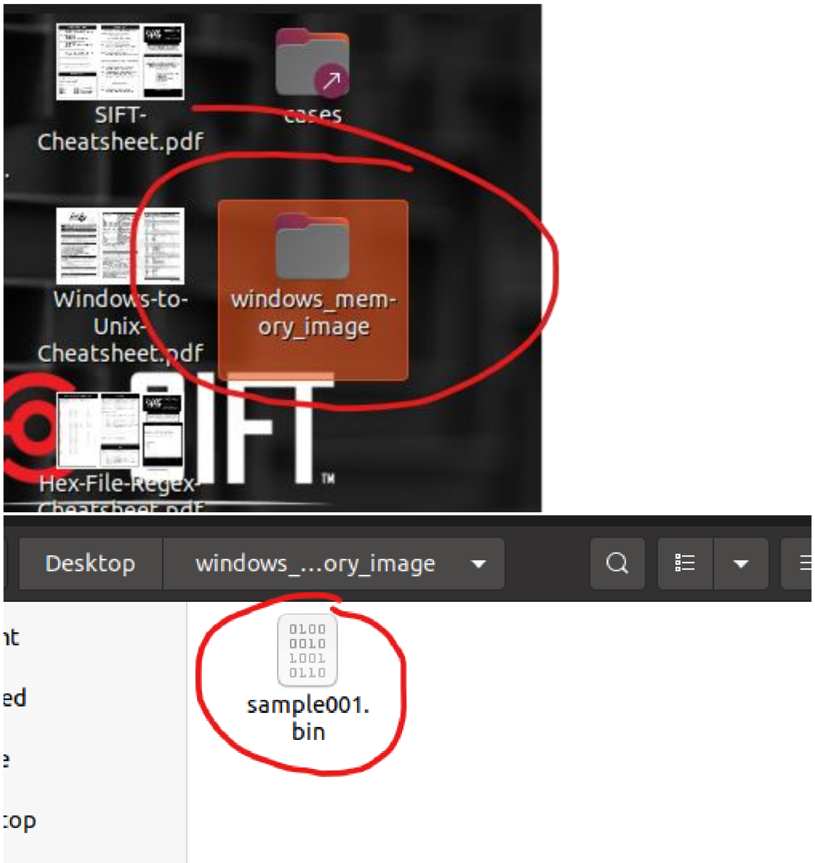
None

2) 

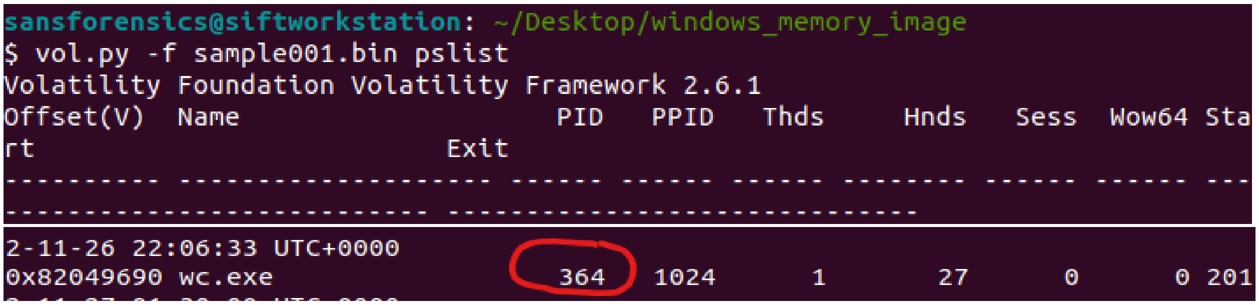
SIFT Workstation [Running] - Oracle VM VirtualBox

File
Machine
View
Input
Devices
Help
Activities
Nov 23 12:32
sansforensics
DFIR-Smartphone-Forensics-Pos…
SIFT-Cheatsheet.pdf
cases
Trash
Windows-Forensics-Poster.pdf
Windows-to-Unix-Cheatsheet.pdf
windows_memory_image
Poster_Threat-Intelligence-Consumption.…
iOS-3rd-Party-Apps-Poster.pdf
Hex-File-Regex-Cheatsheet.pdf
SIFT WORKSTATION
Network-Forensics-Poster.pdf
Zimmerman-Tools-Poster.pdf
SQLite-Pocket-Reference.pdf
SIFT-REMnux-Poster.pdf
Hunt-Evil.pdf
mount_points
Right Ctrl

3) Unzip the attached file to the VM



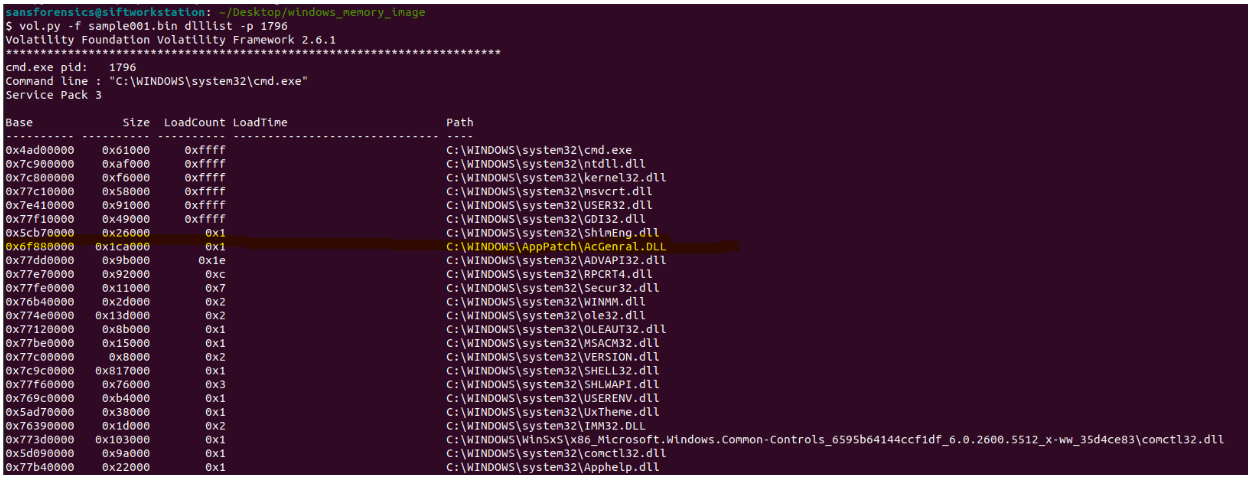
4) 1. What is the process ID of the wc.exe process?



```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Sta
rt                            Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ---
--------------------------- ------------------------------
2-11-26 22:06:33 UTC+0000
0x82049690 wc.exe                  364   1024      1       27      0      0 201
```

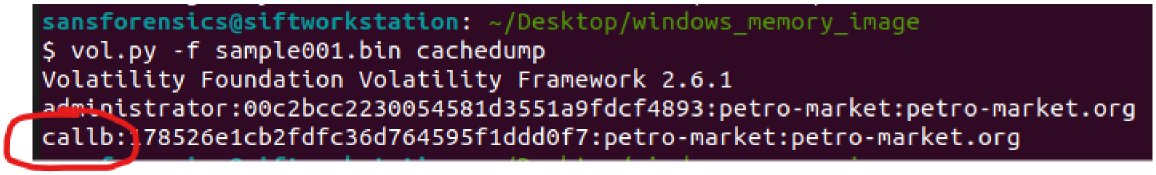
5) 2. How many DLL files does cmd.exe have loaded?

There are **23** files with “dll” in them; but only **1** with a capital “DLL” (screenshot below)



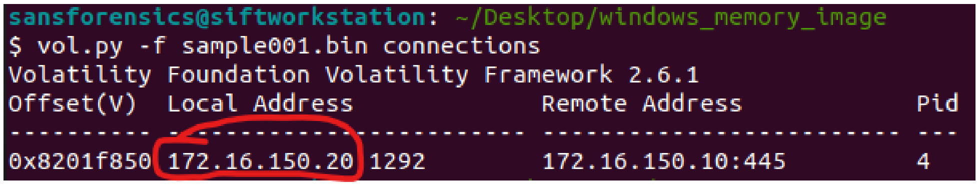
```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin dlllist -p 1796
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
cmd.exe pid:   1796
Command line : "C:\WINDOWS\system32\cmd.exe"
Service Pack 3

Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x4ad00000    0x61000     0xffff                                C:\WINDOWS\system32\cmd.exe
0x7c900000    0xaf000     0xffff                                C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf6000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x77c10000    0x58000     0xffff                                C:\WINDOWS\system32\msvcrt.dll
0x7e410000    0x91000     0xffff                                C:\WINDOWS\system32\USER32.dll
0x77f10000    0x49000     0xffff                                C:\WINDOWS\system32\GDI32.dll
0x5cb70000    0x26000        0x1                                C:\WINDOWS\system32\ShimEng.dll
0x6f880000   0x1ca000        0x1                                C:\WINDOWS\AppPatch\AcGenral.DLL
0x77dd0000    0x9b000       0x1e                                C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x92000        0xc                                C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000    0x11000        0x7                                C:\WINDOWS\system32\Secur32.dll
0x76b40000    0x2d000        0x2                                C:\WINDOWS\system32\WINMM.dll
0x774e0000   0x13d000        0x2                                C:\WINDOWS\system32\ole32.dll
0x77120000    0x8b000        0x1                                C:\WINDOWS\system32\OLEAUT32.dll
0x77be0000    0x15000        0x1                                C:\WINDOWS\system32\MSACM32.dll
0x77c00000     0x8000        0x2                                C:\WINDOWS\system32\VERSION.dll
0x7c9c0000   0x817000        0x1                                C:\WINDOWS\system32\SHELL32.dll
0x77f60000    0x76000        0x3                                C:\WINDOWS\system32\SHLWAPI.dll
0x769c0000    0xb4000        0x1                                C:\WINDOWS\system32\USERENV.dll
0x5ad70000    0x38000        0x1                                C:\WINDOWS\system32\UxTheme.dll
0x76390000    0x1d000        0x2                                C:\WINDOWS\system32\IMM32.DLL
0x773d0000   0x103000        0x1                                C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
0x5d090000    0x9a000        0x1                                C:\WINDOWS\system32\comctl32.dll
0x77b40000    0x22000        0x1                                C:\WINDOWS\system32\Apphelp.dll
```

6) 3. What is the username of the non-default user account?



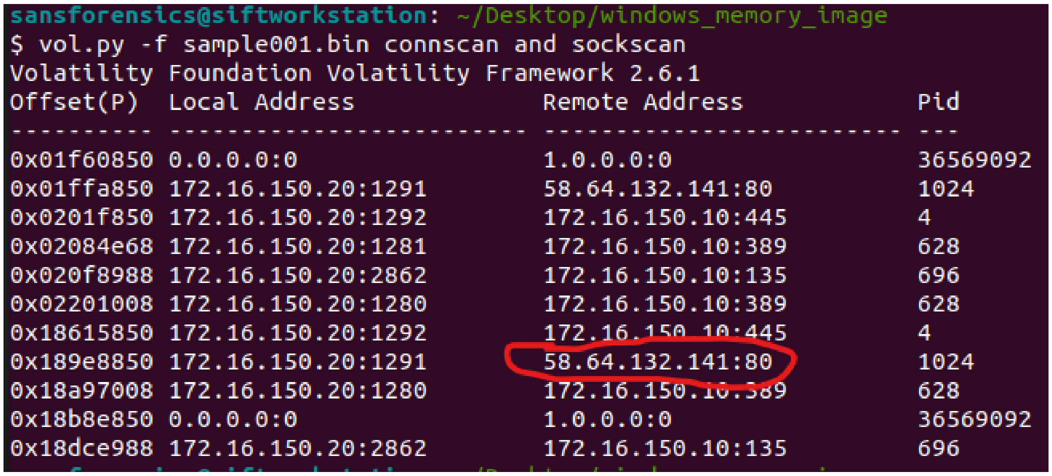
```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin cachedump
Volatility Foundation Volatility Framework 2.6.1
administrator:00c2bcc2230054581d3551a9fdcf4893:petro-market:petro-market.org
callb:178526e1cb2fdfc36d764595f1ddd0f7:petro-market:petro-market.org
```

7) 4. What is the machine's IP address?



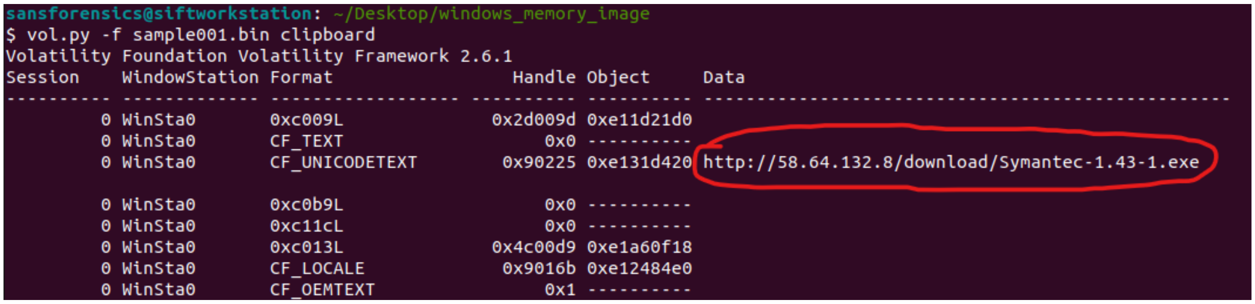
```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin connections
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x8201f850 172.16.150.20:1292        172.16.150.10:445         4
```

8) 5. What is the IP address of the web server the machine was connected to on port 80?



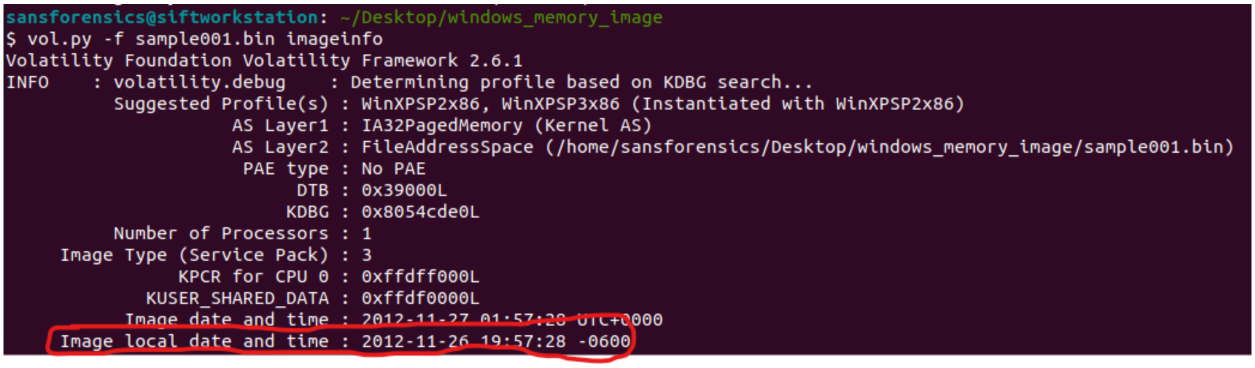
```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin connscan and sockscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x01f60850 0.0.0.0:0                 1.0.0.0:0                 36569092
0x01ffa850 172.16.150.20:1291        58.64.132.141:80          1024
0x0201f850 172.16.150.20:1292        172.16.150.10:445         4
0x02084e68 172.16.150.20:1281        172.16.150.10:389         628
0x020f8988 172.16.150.20:2862        172.16.150.10:135         696
0x02201008 172.16.150.20:1280        172.16.150.10:389         628
0x18615850 172.16.150.20:1292        172.16.150.10:445         4
0x189e8850 172.16.150.20:1291        58.64.132.141:80          1024
0x18a97008 172.16.150.20:1280        172.16.150.10:389         628
0x18b8e850 0.0.0.0:0                 1.0.0.0:0                 36569092
0x18dce988 172.16.150.20:2862        172.16.150.10:135         696
```

9) 6. What is the URL in the current user's clipboard?



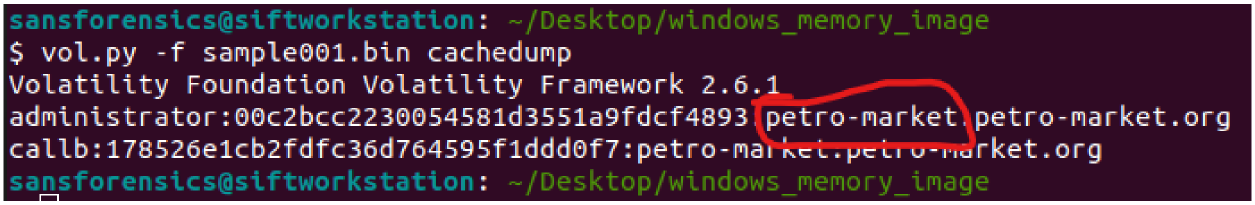
```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin clipboard
Volatility Foundation Volatility Framework 2.6.1
Session    WindowStation Format                 Handle Object     Data
---------- ------------- ------------------ ---------- ---------- --------------------------------------------------
         0 WinSta0       0xc009L              0x2d009d 0xe11d21d0
         0 WinSta0       CF_TEXT                   0x0 ----------
         0 WinSta0       CF_UNICODETEXT        0x90225 0xe131d420 http://58.64.132.8/download/Symantec-1.43-1.exe

         0 WinSta0       0xc0b9L                   0x0 ----------
         0 WinSta0       0xc11cL                   0x0 ----------
         0 WinSta0       0xc013L              0x4c00d9 0xe1a60f18
         0 WinSta0       CF_LOCALE             0x9016b 0xe12484e0
         0 WinSta0       CF_OEMTEXT                0x1 ----------
```

10) 7. What does the clock say on the user's desktop?



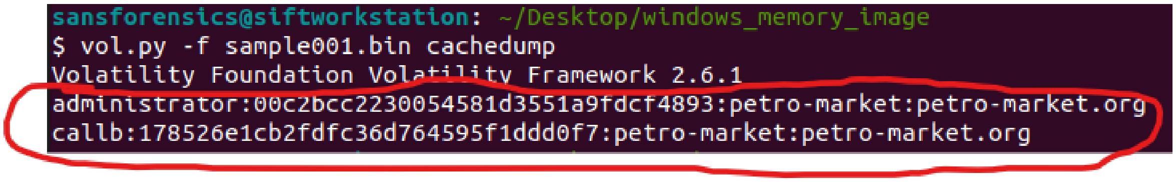
```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/sansforensics/Desktop/windows_memory_image/sample001.bin)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054cde0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2012-11-27 01:57:28 UTC+0000
     Image local date and time : 2012-11-26 19:57:28 -0600
```

11) 8. What windows domain is the computer one?



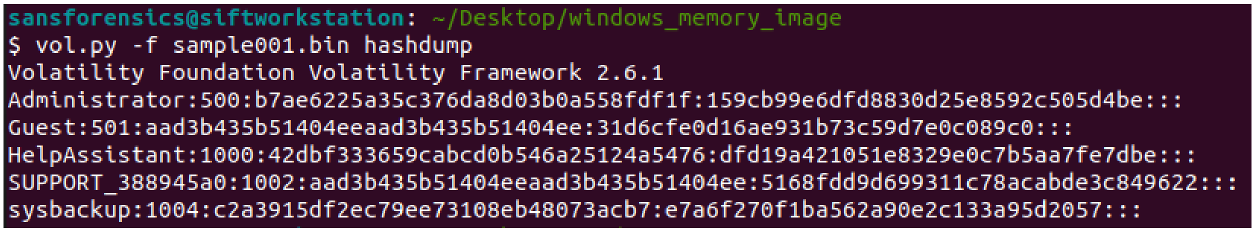
```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin cachedump
Volatility Foundation Volatility Framework 2.6.1
administrator:00c2bcc2230054581d3551a9fdcf4893:petro-market:petro-market.org
callb:178526e1cb2fdfc36d764595f1ddd0f7:petro-market:petro-market.org
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
```

12) 9. What are the cached domain authentication hashes for any available users?



```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin cachedump
Volatility Foundation Volatility Framework 2.6.1
administrator:00c2bcc2230054581d3551a9fdcf4893:petro-market:petro-market.org
callb:178526e1cb2fdfc36d764595f1ddd0f7:petro-market:petro-market.org
```

13) 10. What are the local password hashes for non-domain users?

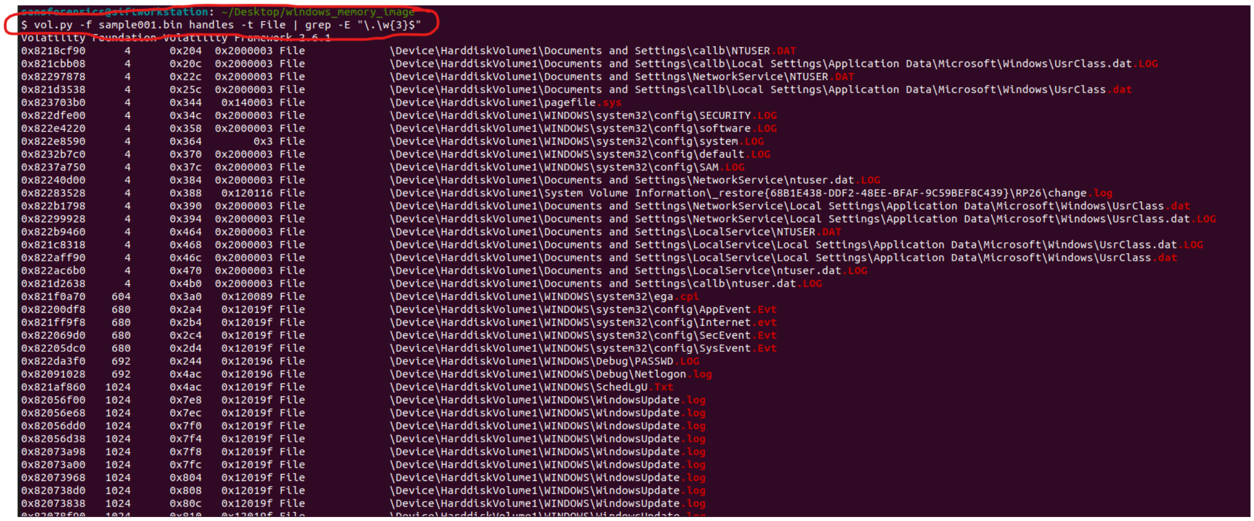


```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:b7ae6225a35c376da8d03b0a558fdf1f:159cb99e6dfd8830d25e8592c505d4be:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:42dbf333659cabcd0b546a25124a5476:dfd19a421051e8329e0c7b5aa7fe7dbe:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:5168fdd9d699311c78acabde3c849622:::
sysbackup:1004:c2a3915df2ec79ee73108eb48073acb7:e7a6f270f1ba562a90e2c133a95d2057:::
```

14) 11. How many open file handles point to files with three letter file extensions?

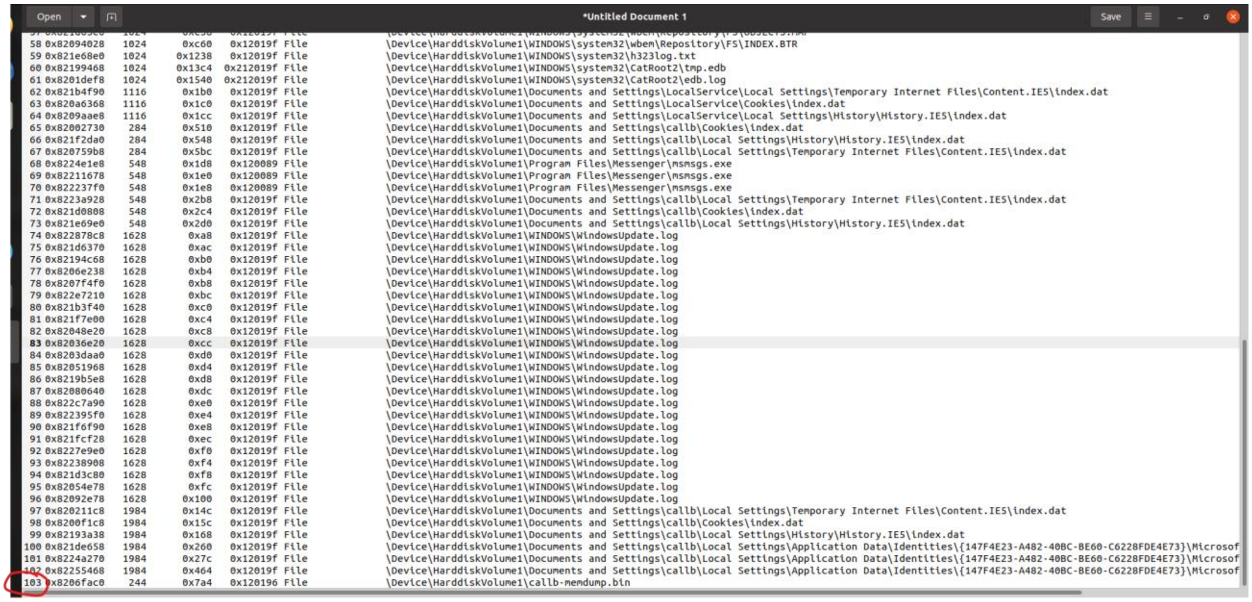
There are a **total of 103** open file handles point to files with three letter file extensions:

Used the command “vol.py -f sample001.bin -t File | grep -E "\.\w{3}$" as this prints out all the 3 letter extenstions under the file type option.



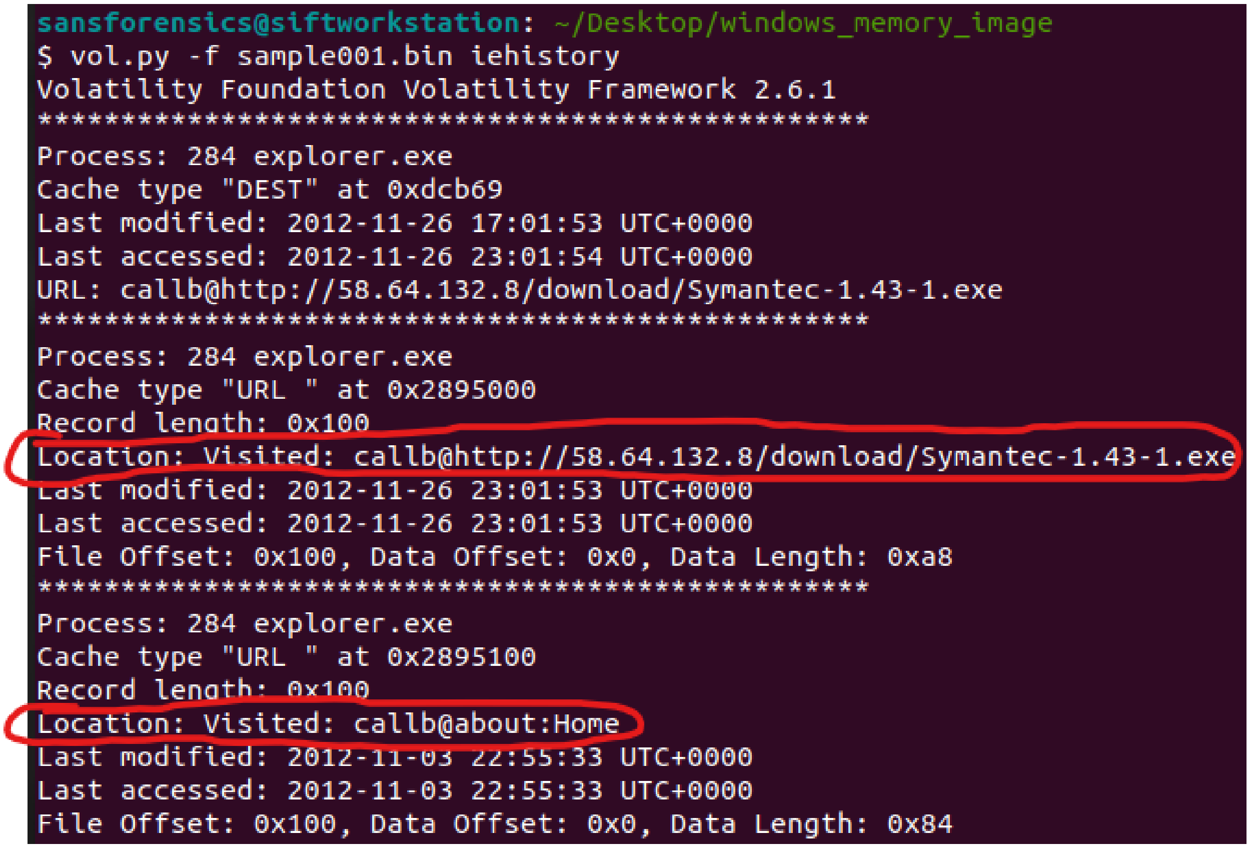
```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin handles -t File | grep -E "\.\w{3}$"
Volatility Foundation Volatility Framework 2.6.1
0x8218cf90      4    0x204  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\callb\NTUSER.DAT
0x821cbb08      4    0x20c  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\callb\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat.LOG
0x82297878      4    0x22c  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0x821d3538      4    0x25c  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\callb\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0x823703b0      4    0x344   0x140003 File           \Device\HarddiskVolume1\pagefile.sys
0x822dfe00      4    0x34c  0x2000003 File           \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY.LOG
0x822e4220      4    0x358  0x2000003 File           \Device\HarddiskVolume1\WINDOWS\system32\config\software.LOG
0x822e8590      4    0x364        0x3 File           \Device\HarddiskVolume1\WINDOWS\system32\config\system.LOG
0x8232b7c0      4    0x370  0x2000003 File           \Device\HarddiskVolume1\WINDOWS\system32\config\default.LOG
0x8237a750      4    0x37c  0x2000003 File           \Device\HarddiskVolume1\WINDOWS\system32\config\SAM.LOG
0x82240d00      4    0x384  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\NetworkService\ntuser.dat.LOG
0x82283528      4    0x388   0x120116 File           \Device\HarddiskVolume1\System Volume Information\_restore{68B1E438-DDF2-48EE-BFAF-9C59BEF8C439}\RP26\change.log
0x822b1798      4    0x390  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0x82299928      4    0x394  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat.LOG
0x822b9460      4    0x464  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0x821c8318      4    0x468  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat.LOG
0x822aff90      4    0x46c  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0x822ac6b0      4    0x470  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\LocalService\ntuser.dat.LOG
0x821d2638      4    0x4b0  0x2000003 File           \Device\HarddiskVolume1\Documents and Settings\callb\ntuser.dat.LOG
0x821f0a70    604    0x3a0   0x120089 File           \Device\HarddiskVolume1\WINDOWS\system32\ega.cpi
0x82200df8    680    0x2a4   0x12019f File           \Device\HarddiskVolume1\WINDOWS\system32\config\AppEvent.Evt
0x821ff9f8    680    0x2b4   0x12019f File           \Device\HarddiskVolume1\WINDOWS\system32\config\Internet.evt
0x822069d0    680    0x2c4   0x12019f File           \Device\HarddiskVolume1\WINDOWS\system32\config\SecEvent.Evt
0x82205dc0    680    0x2d4   0x12019f File           \Device\HarddiskVolume1\WINDOWS\system32\config\SysEvent.Evt
0x822da3f0    692    0x244   0x120196 File           \Device\HarddiskVolume1\WINDOWS\Debug\PASSWD.LOG
0x82091028    692    0x4ac   0x120196 File           \Device\HarddiskVolume1\WINDOWS\Debug\Netlogon.log
0x821af860   1024    0x4ac   0x12019f File           \Device\HarddiskVolume1\WINDOWS\SchedLgU.Txt
0x82056f00   1024    0x7e8   0x12019f File           \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x82056e68   1024    0x7ec   0x12019f File           \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x82056dd0   1024    0x7f0   0x12019f File           \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x82056d38   1024    0x7f4   0x12019f File           \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x82073a98   1024    0x7f8   0x12019f File           \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x82073a00   1024    0x7fc   0x12019f File           \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x82073968   1024    0x804   0x12019f File           \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x820738d0   1024    0x808   0x12019f File           \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x82073838   1024    0x80c   0x12019f File           \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
```

After this I put it into a note pad and counted the lines which lead to 103



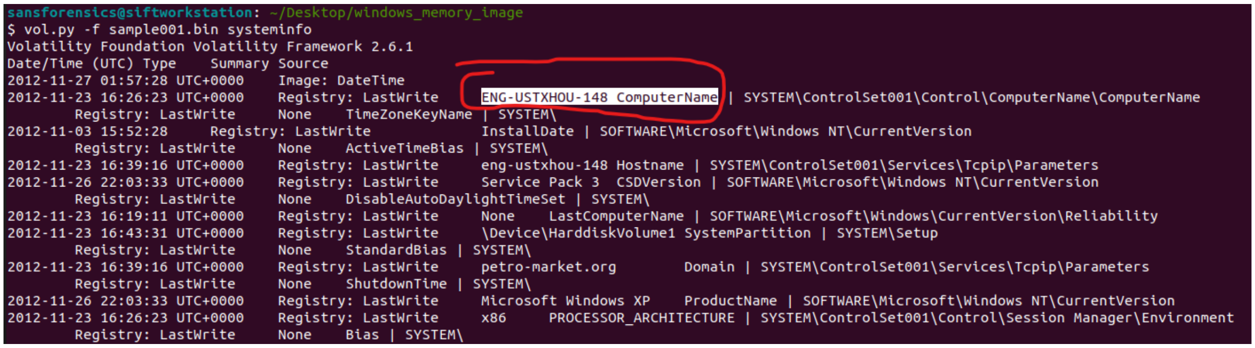
```
 58 0x82094028   1024     0xc60   0x12019f File          \Device\HarddiskVolume1\WINDOWS\system32\wbem\Repository\FS\INDEX.BTR
 59 0x821e68e0   1024    0x1238   0x12019f File          \Device\HarddiskVolume1\WINDOWS\system32\h323log.txt
 60 0x82199468   1024    0x13c4  0x212019f File          \Device\HarddiskVolume1\WINDOWS\system32\CatRoot2\tmp.edb
 61 0x8201def8   1024    0x1540  0x212019f File          \Device\HarddiskVolume1\WINDOWS\system32\CatRoot2\edb.log
 62 0x821b4f90   1116     0x1b0   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
 63 0x820a6368   1116     0x1c0   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\LocalService\Cookies\index.dat
 64 0x8209aae8   1116     0x1cc   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\History\History.IE5\index.dat
 65 0x82002730    284     0x510   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Cookies\index.dat
 66 0x821f2da0    284     0x548   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Local Settings\History\History.IE5\index.dat
 67 0x820759b8    284     0x5bc   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Local Settings\Temporary Internet Files\Content.IE5\index.dat
 68 0x8224e1e8    548     0x1d8   0x120089 File          \Device\HarddiskVolume1\Program Files\Messenger\msmsgs.exe
 69 0x82211678    548     0x1e0   0x120089 File          \Device\HarddiskVolume1\Program Files\Messenger\msmsgs.exe
 70 0x822237f0    548     0x1e8   0x120089 File          \Device\HarddiskVolume1\Program Files\Messenger\msmsgs.exe
 71 0x8223a928    548     0x2b8   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Local Settings\Temporary Internet Files\Content.IE5\index.dat
 72 0x821d0808    548     0x2c4   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Cookies\index.dat
 73 0x821e69e0    548     0x2d0   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Local Settings\History\History.IE5\index.dat
 74 0x822878c8   1628      0xa8   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 75 0x821d6370   1628      0xac   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 76 0x82194c68   1628      0xb0   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 77 0x8206e238   1628      0xb4   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 78 0x8207f4f0   1628      0xb8   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 79 0x822e7210   1628      0xbc   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 80 0x821b3f40   1628      0xc0   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 81 0x821f7e00   1628      0xc4   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 82 0x82048e20   1628      0xc8   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 83 0x82036e20   1628      0xcc   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 84 0x8203daa0   1628      0xd0   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 85 0x82051968   1628      0xd4   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 86 0x8219b5e8   1628      0xd8   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 87 0x82080640   1628      0xdc   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 88 0x822c7a90   1628      0xe0   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 89 0x822395f0   1628      0xe4   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 90 0x821f6f90   1628      0xe8   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 91 0x821fcf28   1628      0xec   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 92 0x8227e9e0   1628      0xf0   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 93 0x82238908   1628      0xf4   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 94 0x821d3c80   1628      0xf8   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 95 0x82054e78   1628      0xfc   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 96 0x82092e78   1628     0x100   0x12019f File          \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
 97 0x820211c8   1984     0x14c   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Local Settings\Temporary Internet Files\Content.IE5\index.dat
 98 0x8200f1c8   1984     0x15c   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Cookies\index.dat
 99 0x82193a38   1984     0x168   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Local Settings\History\History.IE5\index.dat
100 0x821de658   1984     0x260   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Local Settings\Application Data\Identities\{147F4E23-A482-40BC-BE60-C6228FDE4E73}\Microsof
101 0x8224a270   1984     0x27c   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Local Settings\Application Data\Identities\{147F4E23-A482-40BC-BE60-C6228FDE4E73}\Microsof
102 0x82255468   1984     0x464   0x12019f File          \Device\HarddiskVolume1\Documents and Settings\callb\Local Settings\Application Data\Identities\{147F4E23-A482-40BC-BE60-C6228FDE4E73}\Microsof
103 0x8206fac0    244     0x7a4   0x120196 File          \Device\HarddiskVolume1\callb-memdump.bin
```

15) 12. What two websites did the logged-in user visit?



```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin iehistory
Volatility Foundation Volatility Framework 2.6.1
**************************************************
Process: 284 explorer.exe
Cache type "DEST" at 0xdcb69
Last modified: 2012-11-26 17:01:53 UTC+0000
Last accessed: 2012-11-26 23:01:54 UTC+0000
URL: callb@http://58.64.132.8/download/Symantec-1.43-1.exe
**************************************************
Process: 284 explorer.exe
Cache type "URL " at 0x2895000
Record length: 0x100
Location: Visited: callb@http://58.64.132.8/download/Symantec-1.43-1.exe
Last modified: 2012-11-26 23:01:53 UTC+0000
Last accessed: 2012-11-26 23:01:53 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa8
**************************************************
Process: 284 explorer.exe
Cache type "URL " at 0x2895100
Record length: 0x100
Location: Visited: callb@about:Home
Last modified: 2012-11-03 22:55:33 UTC+0000
Last accessed: 2012-11-03 22:55:33 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x84
```

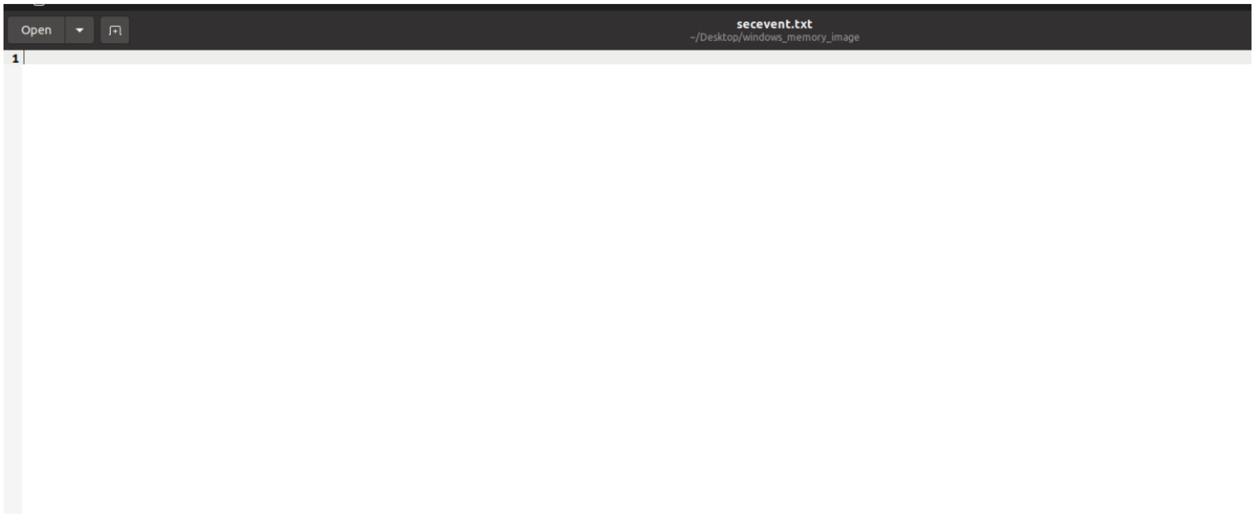
16) 13. What is the machine name?



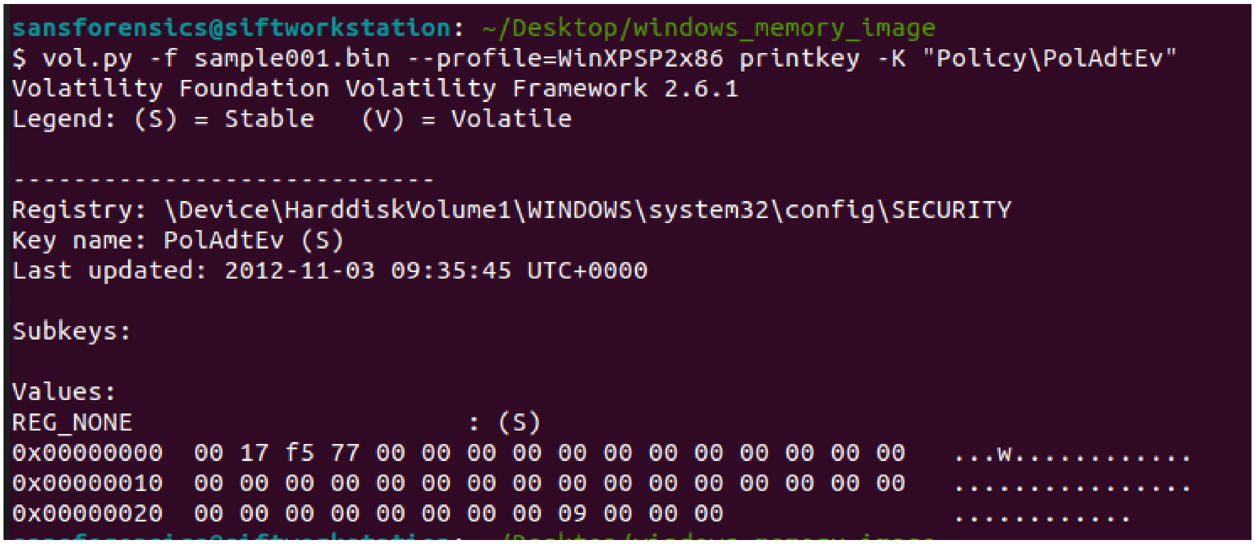
```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin systeminfo
Volatility Foundation Volatility Framework 2.6.1
Date/Time (UTC) Type    Summary Source
2012-11-27 01:57:28 UTC+0000    Image: DateTime
2012-11-23 16:26:23 UTC+0000    Registry: LastWrite     ENG-USTXHOU-148 ComputerName | SYSTEM\ControlSet001\Control\ComputerName\ComputerName
        Registry: LastWrite     None    TimeZoneKeyName | SYSTEM\
2012-11-03 15:52:28     Registry: LastWrite             InstallDate | SOFTWARE\Microsoft\Windows NT\CurrentVersion
        Registry: LastWrite     None    ActiveTimeBias | SYSTEM\
2012-11-23 16:39:16 UTC+0000    Registry: LastWrite     eng-ustxhou-148 Hostname | SYSTEM\ControlSet001\Services\Tcpip\Parameters
2012-11-26 22:03:33 UTC+0000    Registry: LastWrite     Service Pack 3  CSDVersion | SOFTWARE\Microsoft\Windows NT\CurrentVersion
        Registry: LastWrite     None    DisableAutoDaylightTimeSet | SYSTEM\
2012-11-23 16:19:11 UTC+0000    Registry: LastWrite     None    LastComputerName | SOFTWARE\Microsoft\Windows\CurrentVersion\Reliability
2012-11-23 16:43:31 UTC+0000    Registry: LastWrite     \Device\HarddiskVolume1 SystemPartition | SYSTEM\Setup
        Registry: LastWrite     None    StandardBias | SYSTEM\
2012-11-23 16:39:16 UTC+0000    Registry: LastWrite     petro-market.org        Domain | SYSTEM\ControlSet001\Services\Tcpip\Parameters
        Registry: LastWrite     None    ShutdownTime | SYSTEM\
2012-11-26 22:03:33 UTC+0000    Registry: LastWrite     Microsoft Windows XP    ProductName | SOFTWARE\Microsoft\Windows NT\CurrentVersion
2012-11-23 16:26:23 UTC+0000    Registry: LastWrite     x86     PROCESSOR_ARCHITECTURE | SYSTEM\ControlSet001\Control\Session Manager\Environment
        Registry: LastWrite     None    Bias | SYSTEM\
```

17) 14. How many entries are in the security event log?

There are None (screenshot below):

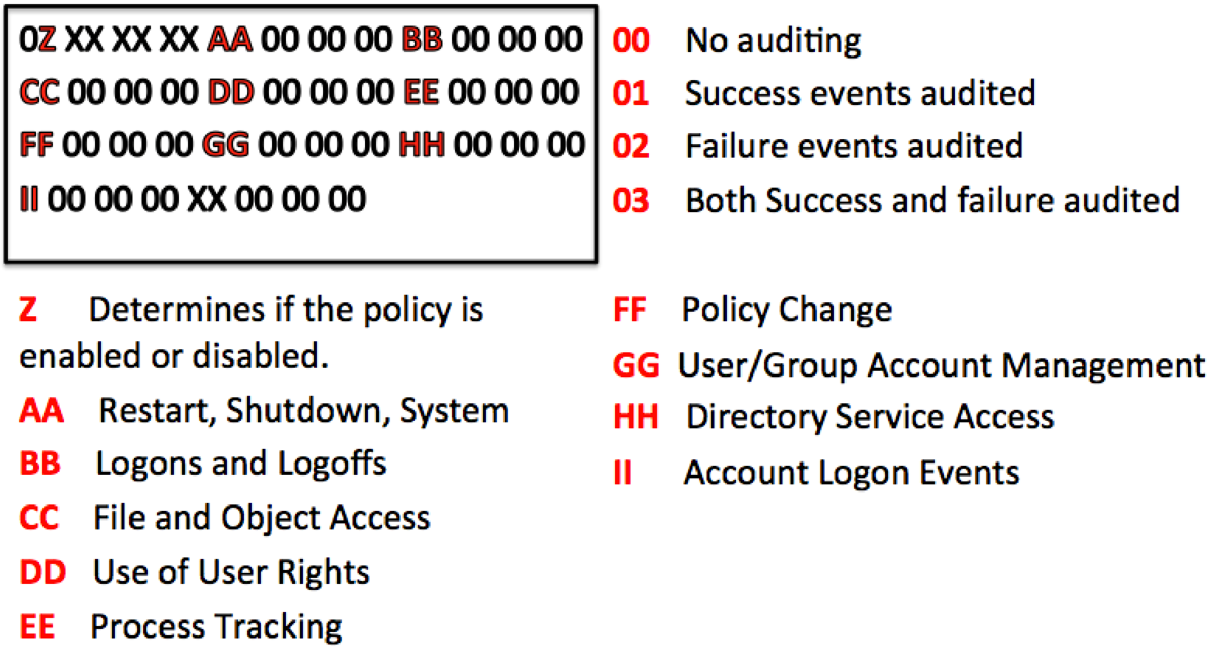


To confirm if this is truly the results, I ran the following command:



```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin --profile=WinXPSP2x86 printkey -K "Policy\PolAdtEv"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
Key name: PolAdtEv (S)
Last updated: 2012-11-03 09:35:45 UTC+0000

Subkeys:

Values:
REG_NONE                      : (S)
0x00000000  00 17 f5 77 00 00 00 00 00 00 00 00 00 00 00 00   ...w............
0x00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000020  00 00 00 00 00 00 00 00 09 00 00 00               ............
```

Using the grahic below, we can confirm or not by looking at the binary values with the below reference (https://volatility-labs.blogspot.com/2012/09/movp-23-event-logs-and-servicesids.html):



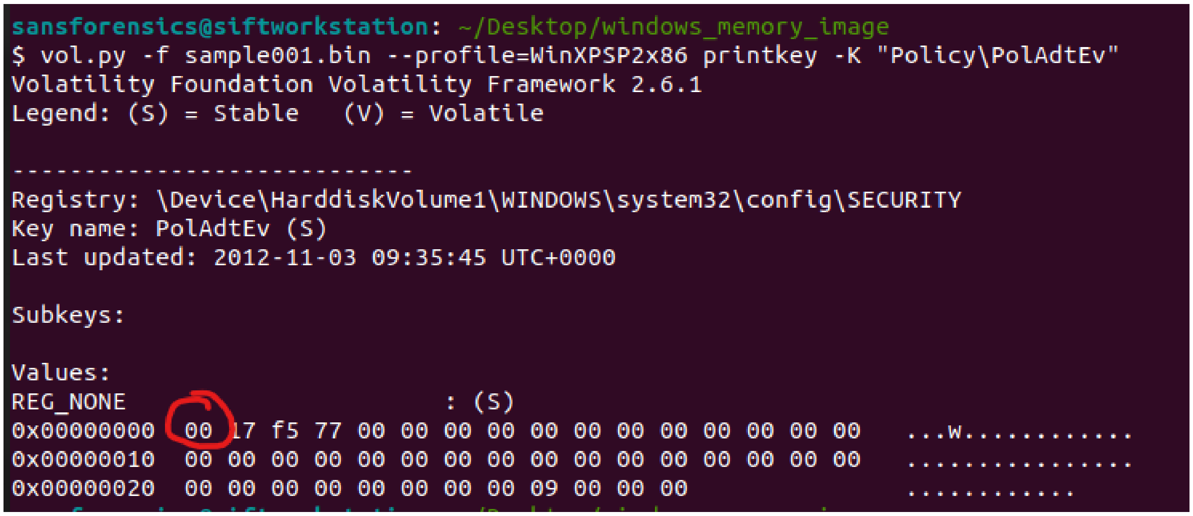
```
0Z XX XX XX AA 00 00 00 BB 00 00 00
CC 00 00 00 DD 00 00 00 EE 00 00 00
FF 00 00 00 GG 00 00 00 HH 00 00 00
II 00 00 00 XX 00 00 00
```

00	No auditing
01	Success events audited
02	Failure events audited
03	Both Success and failure audited

Z	Determines if the policy is enabled or disabled.
AA	Restart, Shutdown, System
BB	Logons and Logoffs
CC	File and Object Access
DD	Use of User Rights
EE	Process Tracking

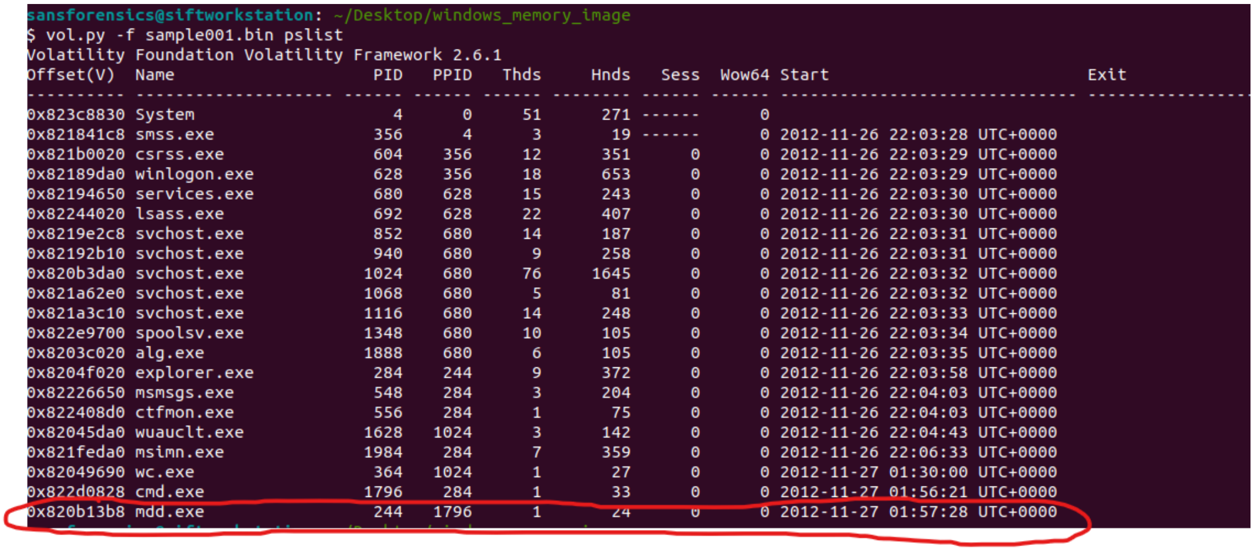
FF	Policy Change
GG	User/Group Account Management
HH	Directory Service Access
II	Account Logon Events

As you can see, the first two binary data are marked as “**00**” thus this shows that the policy is **disabled and no auditing was available**



```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin --profile=WinXPSP2x86 printkey -K "Policy\PolAdtEv"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
Key name: PolAdtEv (S)
Last updated: 2012-11-03 09:35:45 UTC+0000

Subkeys:

Values:
REG_NONE                          : (S)
0x00000000  00 17 f5 77 00 00 00 00 00 00 00 00 00 00 00 00   ...w............
0x00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000020  00 00 00 00 00 00 00 00 09 00 00 00               ............
```

18) 15. What was the name of the most recently started scheduled task?

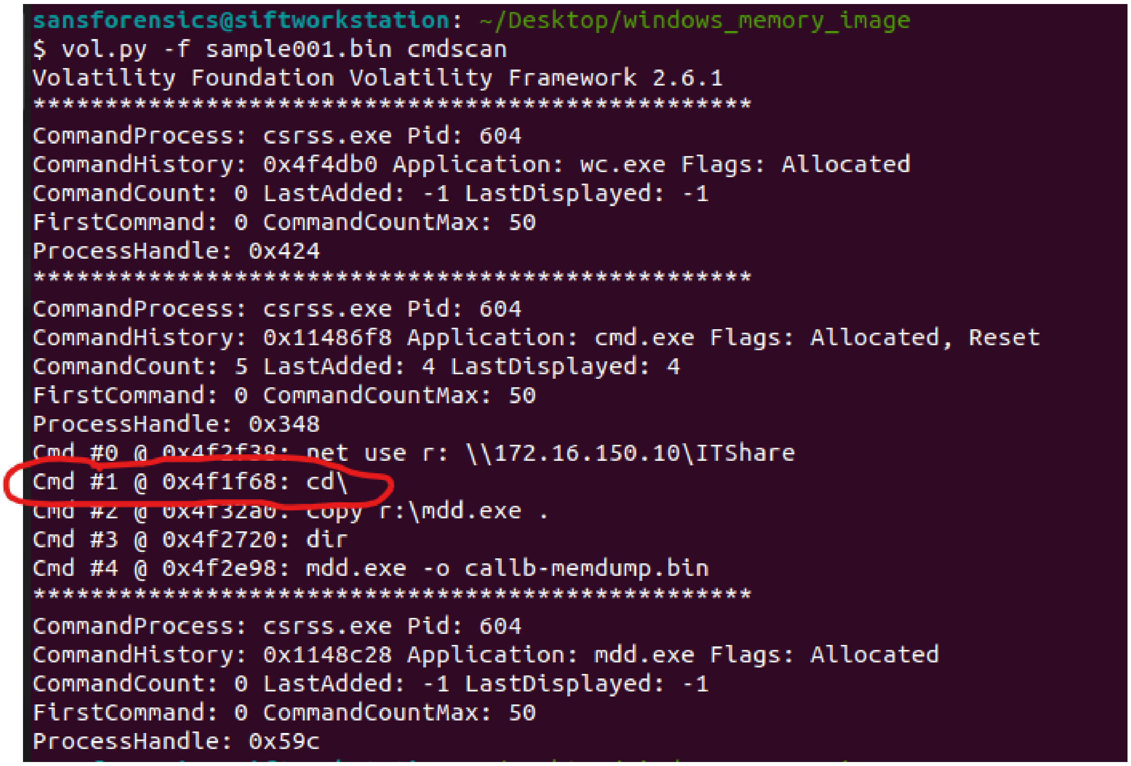


```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ---------------
0x823c8830 System                    4      0     51      271 ------      0
0x821841c8 smss.exe                356      4      3       19 ------      0 2012-11-26 22:03:28 UTC+0000
0x821b0020 csrss.exe               604    356     12      351      0      0 2012-11-26 22:03:29 UTC+0000
0x82189da0 winlogon.exe            628    356     18      653      0      0 2012-11-26 22:03:29 UTC+0000
0x82194650 services.exe            680    628     15      243      0      0 2012-11-26 22:03:30 UTC+0000
0x82244020 lsass.exe               692    628     22      407      0      0 2012-11-26 22:03:30 UTC+0000
0x8219e2c8 svchost.exe             852    680     14      187      0      0 2012-11-26 22:03:31 UTC+0000
0x82192b10 svchost.exe             940    680      9      258      0      0 2012-11-26 22:03:31 UTC+0000
0x820b3da0 svchost.exe            1024    680     76     1645      0      0 2012-11-26 22:03:32 UTC+0000
0x821a62e0 svchost.exe            1068    680      5       81      0      0 2012-11-26 22:03:32 UTC+0000
0x821a3c10 svchost.exe            1116    680     14      248      0      0 2012-11-26 22:03:33 UTC+0000
0x822e9700 spoolsv.exe            1348    680     10      105      0      0 2012-11-26 22:03:34 UTC+0000
0x8203c020 alg.exe                1888    680      6      105      0      0 2012-11-26 22:03:35 UTC+0000
0x8204f020 explorer.exe            284    244      9      372      0      0 2012-11-26 22:03:58 UTC+0000
0x82226650 msmsgs.exe              548    284      3      204      0      0 2012-11-26 22:04:03 UTC+0000
0x822408d0 ctfmon.exe              556    284      1       75      0      0 2012-11-26 22:04:03 UTC+0000
0x82045da0 wuauclt.exe            1628   1024      3      142      0      0 2012-11-26 22:04:43 UTC+0000
0x821feda0 msimn.exe              1984    284      7      359      0      0 2012-11-26 22:06:33 UTC+0000
0x82049690 wc.exe                  364   1024      1       27      0      0 2012-11-27 01:30:00 UTC+0000
0x822d0828 cmd.exe                1796    284      1       33      0      0 2012-11-27 01:56:21 UTC+0000
0x820b13b8 mdd.exe                 244   1796      1       24      0      0 2012-11-27 01:57:28 UTC+0000
```

It is mdd.exe because it has the latest start time

19) 16. Where was mdd.exe copied from?

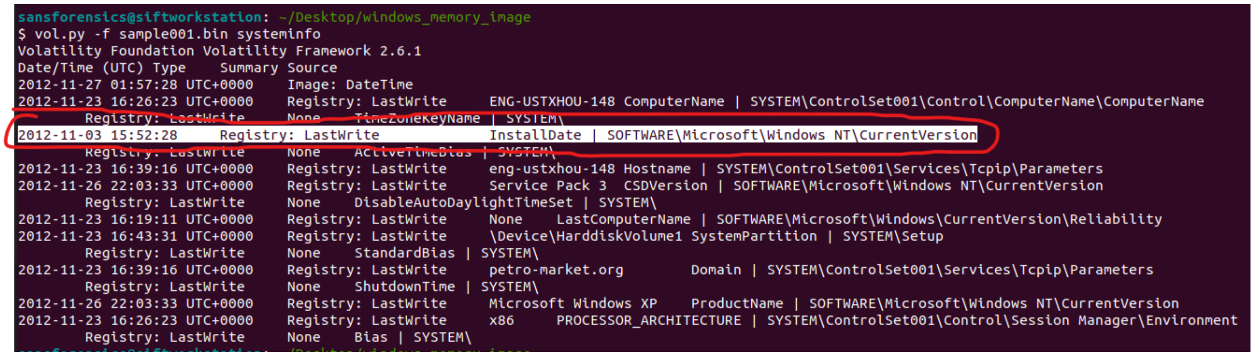
From the **root directory**



```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin cmdscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
CommandProcess: csrss.exe Pid: 604
CommandHistory: 0x4f4db0 Application: wc.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x424
**************************************************
CommandProcess: csrss.exe Pid: 604
CommandHistory: 0x11486f8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 5 LastAdded: 4 LastDisplayed: 4
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x348
Cmd #0 @ 0x4f2f38: net use r: \\172.16.150.10\ITShare
Cmd #1 @ 0x4f1f68: cd\
Cmd #2 @ 0x4f32a0: copy r:\mdd.exe .
Cmd #3 @ 0x4f2720: dir
Cmd #4 @ 0x4f2e98: mdd.exe -o callb-memdump.bin
**************************************************
CommandProcess: csrss.exe Pid: 604
CommandHistory: 0x1148c28 Application: mdd.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x59c
```

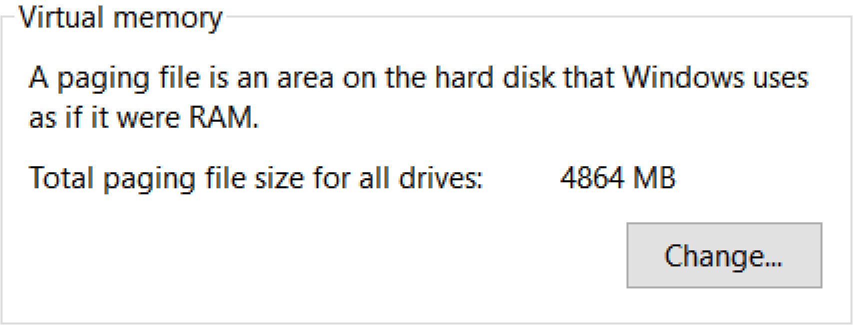
20) 17. What year and month did Windows Update last run?

Windows update was last run on 2012/Nov/3rd. We know this is the register key to the current build as “HKLM\Software\Microsoft\Windows NT\CurrentVersion” thus the user would’ve last run to update their system on that date.



```
sansforensics@siftworkstation: ~/Desktop/windows_memory_image
$ vol.py -f sample001.bin systeminfo
Volatility Foundation Volatility Framework 2.6.1
Date/Time (UTC) Type    Summary Source
2012-11-27 01:57:28 UTC+0000    Image: DateTime
2012-11-23 16:26:23 UTC+0000    Registry: LastWrite     ENG-USTXHOU-148 ComputerName | SYSTEM\ControlSet001\Control\ComputerName\ComputerName
        Registry: LastWrite     None    TimeZoneKeyName | SYSTEM\
2012-11-03 15:52:28     Registry: LastWrite             InstallDate | SOFTWARE\Microsoft\Windows NT\CurrentVersion
        Registry: LastWrite     None    ActiveTimeBias | SYSTEM\
2012-11-23 16:39:16 UTC+0000    Registry: LastWrite     eng-ustxhou-148 Hostname | SYSTEM\ControlSet001\Services\Tcpip\Parameters
2012-11-26 22:03:33 UTC+0000    Registry: LastWrite     Service Pack 3  CSDVersion | SOFTWARE\Microsoft\Windows NT\CurrentVersion
        Registry: LastWrite     None    DisableAutoDaylightTimeSet | SYSTEM\
2012-11-23 16:19:11 UTC+0000    Registry: LastWrite     None    LastComputerName | SOFTWARE\Microsoft\Windows\CurrentVersion\Reliability
2012-11-23 16:43:31 UTC+0000    Registry: LastWrite     \Device\HarddiskVolume1 SystemPartition | SYSTEM\Setup
        Registry: LastWrite     None    StandardBias | SYSTEM\
2012-11-23 16:39:16 UTC+0000    Registry: LastWrite     petro-market.org        Domain | SYSTEM\ControlSet001\Services\Tcpip\Parameters
        Registry: LastWrite     None    ShutdownTime | SYSTEM\
2012-11-26 22:03:33 UTC+0000    Registry: LastWrite     Microsoft Windows XP    ProductName | SOFTWARE\Microsoft\Windows NT\CurrentVersion
2012-11-23 16:26:23 UTC+0000    Registry: LastWrite     x86     PROCESSOR_ARCHITECTURE | SYSTEM\ControlSet001\Control\Session Manager\Environment
        Registry: LastWrite     None    Bias | SYSTEM\
```

21) Make sure your VM has paging file is configured



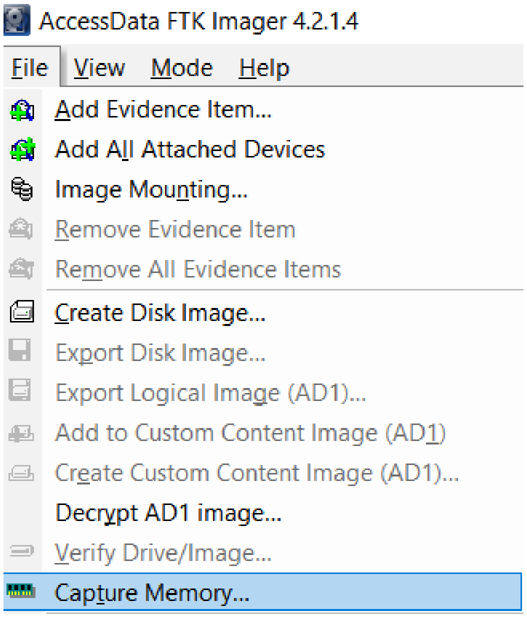
Virtual memory

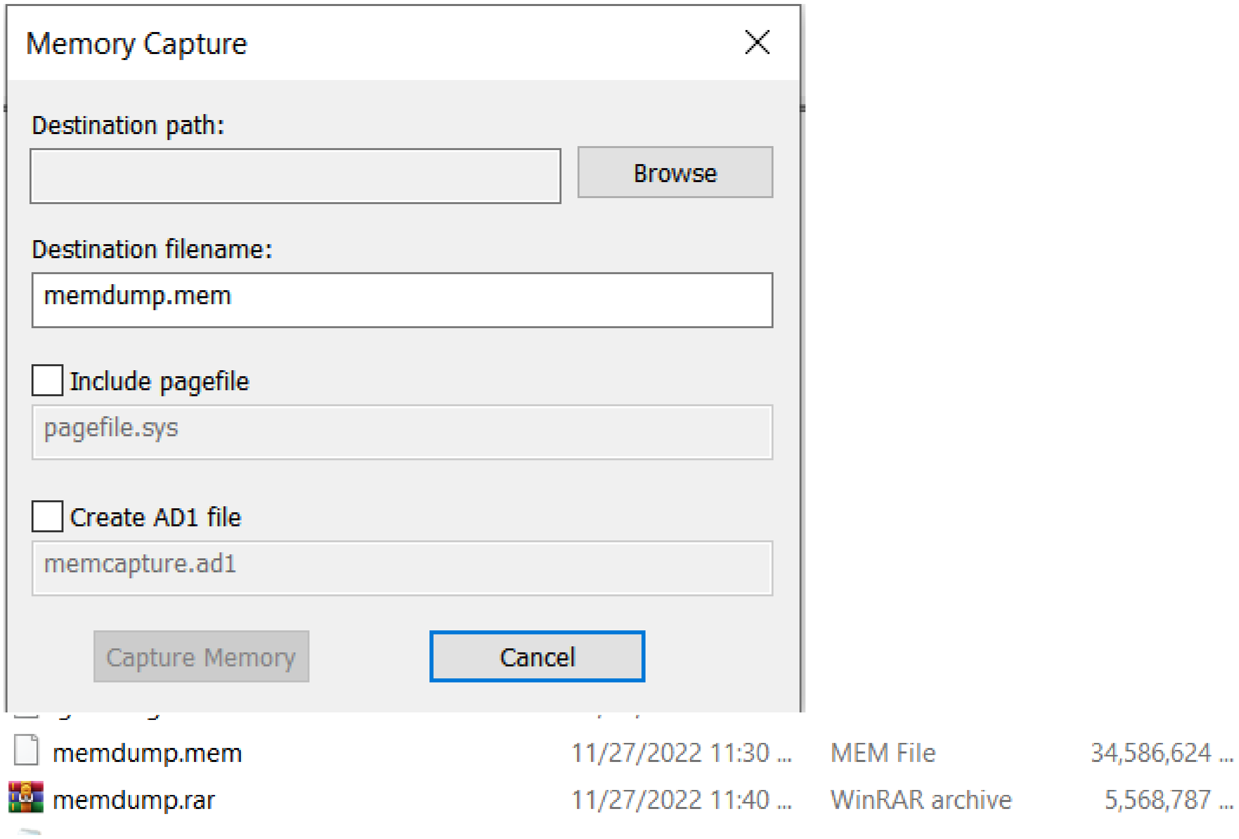
A paging file is an area on the hard disk that Windows uses as if it were RAM.

Total paging file size for all drives: 4864 MB

22) Create a dump file from your windows VM using one of the tools discussed in class

- Used FTK Imager and ran the memory collection process:





Destination path:

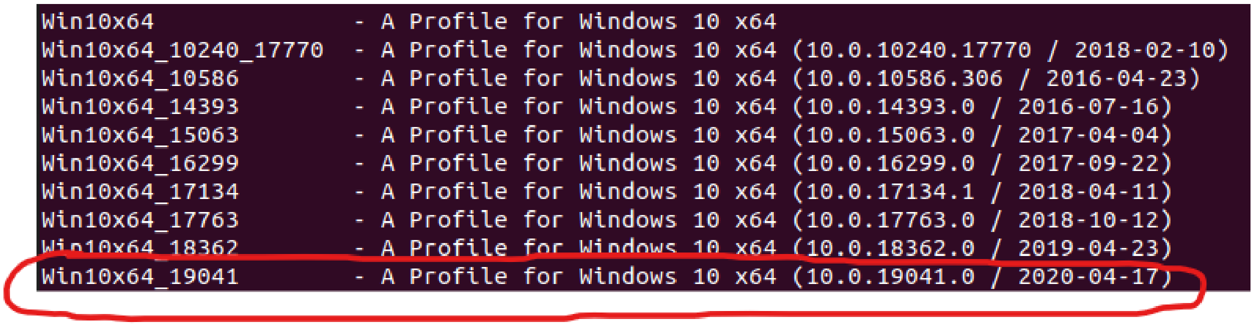
Destination filename: memdump.mem

□ Include pagefile
pagefile.sys

□ Create AD1 file
memcapture.ad1

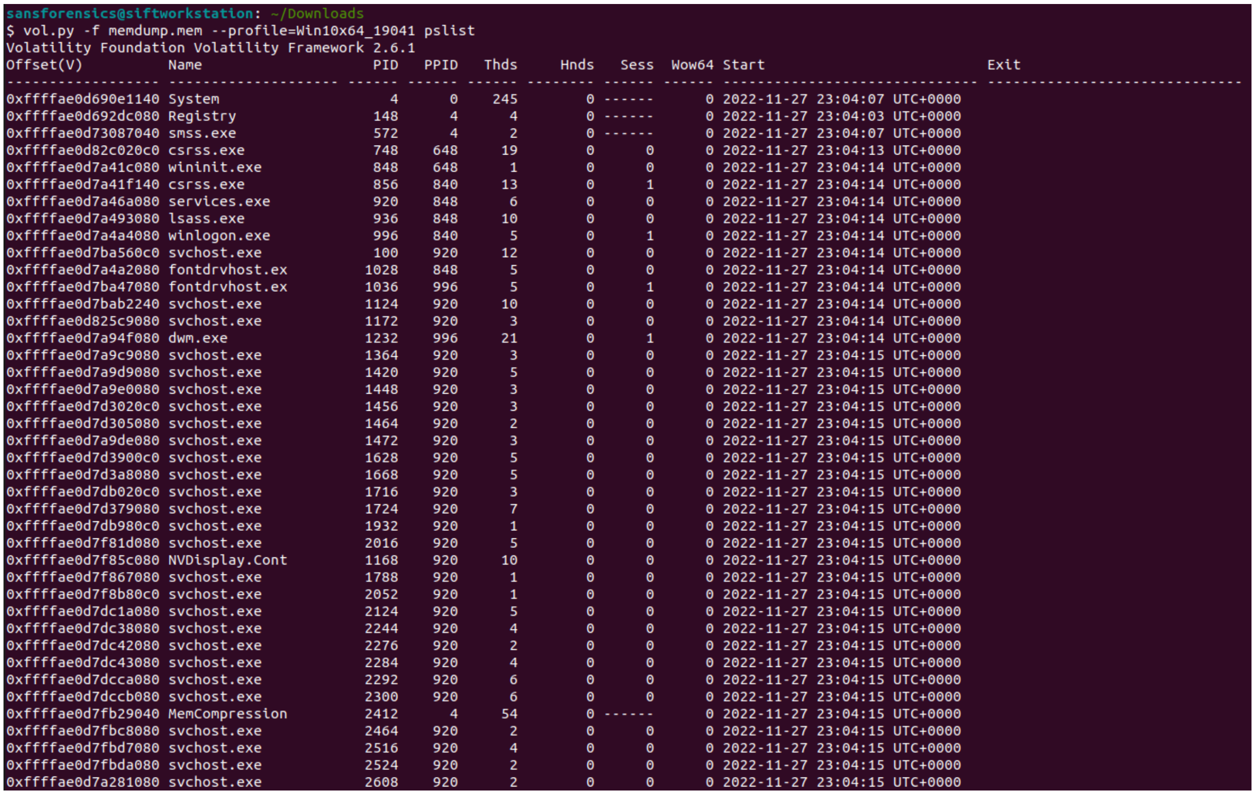
```
memdump.mem    11/27/2022 11:30 ...    MEM File          34,586,624 ...
memdump.rar    11/27/2022 11:40 ...    WinRAR archive     5,568,787 ...
```

23) Find the matching profile for your VM – This was the best solution since it's the latest release

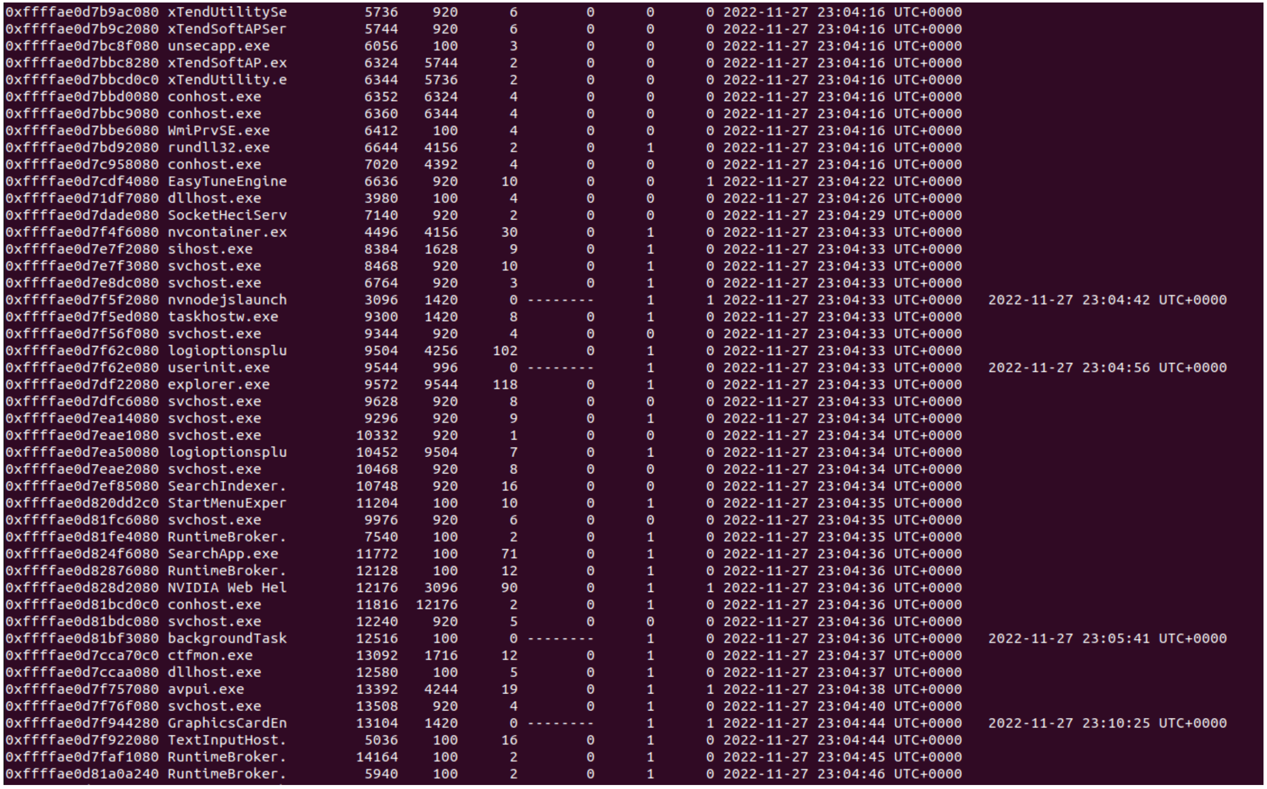


```
Win10x64                - A Profile for Windows 10 x64
Win10x64_10240_17770    - A Profile for Windows 10 x64 (10.0.10240.17770 / 2018-02-10)
Win10x64_10586          - A Profile for Windows 10 x64 (10.0.10586.306 / 2016-04-23)
Win10x64_14393          - A Profile for Windows 10 x64 (10.0.14393.0 / 2016-07-16)
Win10x64_15063          - A Profile for Windows 10 x64 (10.0.15063.0 / 2017-04-04)
Win10x64_16299          - A Profile for Windows 10 x64 (10.0.16299.0 / 2017-09-22)
Win10x64_17134          - A Profile for Windows 10 x64 (10.0.17134.1 / 2018-04-11)
Win10x64_17763          - A Profile for Windows 10 x64 (10.0.17763.0 / 2018-10-12)
Win10x64_18362          - A Profile for Windows 10 x64 (10.0.18362.0 / 2019-04-23)
Win10x64_19041          - A Profile for Windows 10 x64 (10.0.19041.0 / 2020-04-17)
```

24) Extract the list of all processes

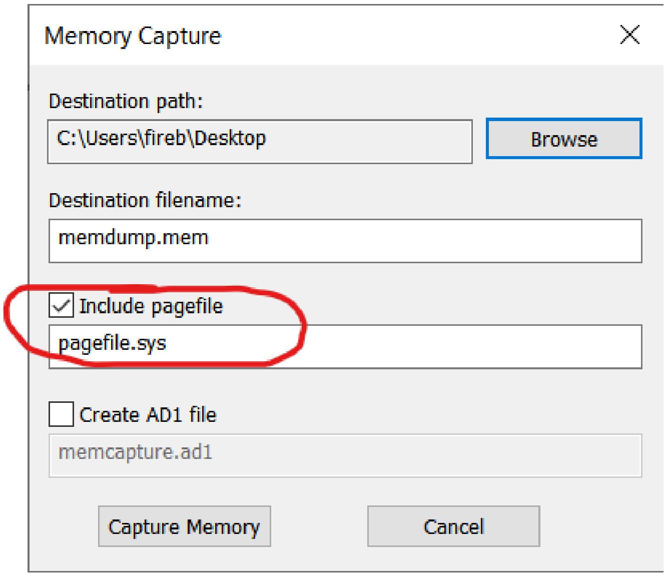


```
sansforensics@siftworkstation: ~/Downloads
$ vol.py -f memdump.mem --profile=Win10x64_19041 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xffffae0d690e1140 System                    4      0    245        0 ------      0 2022-11-27 23:04:07 UTC+0000
0xffffae0d692dc080 Registry                148      4      4        0 ------      0 2022-11-27 23:04:03 UTC+0000
0xffffae0d73087040 smss.exe                572      4      2        0 ------      0 2022-11-27 23:04:07 UTC+0000
0xffffae0d82c020c0 csrss.exe               748    648     19        0      0      0 2022-11-27 23:04:13 UTC+0000
0xffffae0d7a41c080 wininit.exe             848    648      1        0      0      0 2022-11-27 23:04:14 UTC+0000
0xffffae0d7a41f140 csrss.exe               856    840     13        0      1      0 2022-11-27 23:04:14 UTC+0000
0xffffae0d7a46a080 services.exe            920    848      6        0      0      0 2022-11-27 23:04:14 UTC+0000
0xffffae0d7a493080 lsass.exe               936    848     10        0      0      0 2022-11-27 23:04:14 UTC+0000
0xffffae0d7a4a4080 winlogon.exe            996    840      5        0      1      0 2022-11-27 23:04:14 UTC+0000
0xffffae0d7ba560c0 svchost.exe             100    920     12        0      0      0 2022-11-27 23:04:14 UTC+0000
0xffffae0d7a4a2080 fontdrvhost.ex         1028    848      5        0      0      0 2022-11-27 23:04:14 UTC+0000
0xffffae0d7ba47080 fontdrvhost.ex         1036    996      5        0      1      0 2022-11-27 23:04:14 UTC+0000
0xffffae0d7bab2240 svchost.exe            1124    920     10        0      0      0 2022-11-27 23:04:14 UTC+0000
0xffffae0d825c9080 svchost.exe            1172    920      3        0      0      0 2022-11-27 23:04:14 UTC+0000
0xffffae0d7a94f080 dwm.exe                1232    996     21        0      1      0 2022-11-27 23:04:14 UTC+0000
0xffffae0d7a9c9080 svchost.exe            1364    920      3        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7a9d9080 svchost.exe            1420    920      5        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7a9e0080 svchost.exe            1448    920      3        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7d3020c0 svchost.exe            1456    920      3        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7d305080 svchost.exe            1464    920      2        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7a9de080 svchost.exe            1472    920      3        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7d3900c0 svchost.exe            1628    920      5        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7d3a8080 svchost.exe            1668    920      5        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7db020c0 svchost.exe            1716    920      3        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7d379080 svchost.exe            1724    920      7        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7db980c0 svchost.exe            1932    920      1        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7f81d080 svchost.exe            2016    920      5        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7f85c080 NVDisplay.Cont         1168    920     10        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7f867080 svchost.exe            1788    920      1        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7f8b80c0 svchost.exe            2052    920      1        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7dc1a080 svchost.exe            2124    920      5        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7dc38080 svchost.exe            2244    920      4        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7dc42080 svchost.exe            2276    920      2        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7dc43080 svchost.exe            2284    920      4        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7dcca080 svchost.exe            2292    920      6        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7dccb080 svchost.exe            2300    920      6        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7fb29040 MemCompression         2412      4     54        0 ------      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7fbc8080 svchost.exe            2464    920      2        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7fbd7080 svchost.exe            2516    920      4        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7fbda080 svchost.exe            2524    920      2        0      0      0 2022-11-27 23:04:15 UTC+0000
0xffffae0d7a281080 svchost.exe            2608    920      2        0      0      0 2022-11-27 23:04:15 UTC+0000
```



```
0xffffae0d7b9ac080 xTendUtilitySe         5736    920      6        0      0      0 2022-11-27 23:04:16 UTC+0000
0xffffae0d7b9c2080 xTendSoftAPSer         5744    920      6        0      0      0 2022-11-27 23:04:16 UTC+0000
0xffffae0d7bc8f080 unsecapp.exe           6056    100      3        0      0      0 2022-11-27 23:04:16 UTC+0000
0xffffae0d7bbc8280 xTendSoftAP.ex         6324   5744      2        0      0      0 2022-11-27 23:04:16 UTC+0000
0xffffae0d7bbcd0c0 xTendUtility.e         6344   5736      2        0      0      0 2022-11-27 23:04:16 UTC+0000
0xffffae0d7bbd0080 conhost.exe            6352   6324      4        0      0      0 2022-11-27 23:04:16 UTC+0000
0xffffae0d7bbc9080 conhost.exe            6360   6344      4        0      0      0 2022-11-27 23:04:16 UTC+0000
0xffffae0d7bbe6080 WmiPrvSE.exe           6412    100      4        0      0      0 2022-11-27 23:04:16 UTC+0000
0xffffae0d7bd92080 rundll32.exe           6644   4156      2        0      1      0 2022-11-27 23:04:16 UTC+0000
0xffffae0d7c958080 conhost.exe            7020   4392      4        0      0      0 2022-11-27 23:04:16 UTC+0000
0xffffae0d7cdf4080 EasyTuneEngine         6636    920     10        0      0      1 2022-11-27 23:04:22 UTC+0000
0xffffae0d71df7080 dllhost.exe            3980    100      4        0      0      0 2022-11-27 23:04:26 UTC+0000
0xffffae0d7dade080 SocketHeciServ         7140    920      2        0      0      0 2022-11-27 23:04:29 UTC+0000
0xffffae0d7f4f6080 nvcontainer.ex         4496   4156     30        0      1      0 2022-11-27 23:04:33 UTC+0000
0xffffae0d7e7f2080 sihost.exe             8384   1628      9        0      1      0 2022-11-27 23:04:33 UTC+0000
0xffffae0d7e7f3080 svchost.exe            8468    920     10        0      1      0 2022-11-27 23:04:33 UTC+0000
0xffffae0d7e8dc080 svchost.exe            6764    920      3        0      1      0 2022-11-27 23:04:33 UTC+0000
0xffffae0d7f5f2080 nvnodejslaunch         3096   1420      0 --------      1      1 2022-11-27 23:04:33 UTC+0000   2022-11-27 23:04:42 UTC+0000
0xffffae0d7f5ed080 taskhostw.exe          9300   1420      8        0      1      0 2022-11-27 23:04:33 UTC+0000
0xffffae0d7f56f080 svchost.exe            9344    920      4        0      0      0 2022-11-27 23:04:33 UTC+0000
0xffffae0d7f62c080 logioptionsplu         9504   4256    102        0      1      0 2022-11-27 23:04:33 UTC+0000
0xffffae0d7f62e080 userinit.exe           9544    996      0 --------      1      0 2022-11-27 23:04:33 UTC+0000   2022-11-27 23:04:56 UTC+0000
0xffffae0d7df22080 explorer.exe           9572   9544    118        0      1      0 2022-11-27 23:04:33 UTC+0000
0xffffae0d7dfc6080 svchost.exe            9628    920      8        0      0      0 2022-11-27 23:04:33 UTC+0000
0xffffae0d7ea14080 svchost.exe            9296    920      9        0      1      0 2022-11-27 23:04:34 UTC+0000
0xffffae0d7eae1080 svchost.exe           10332    920      1        0      0      0 2022-11-27 23:04:34 UTC+0000
0xffffae0d7ea50080 logioptionsplu        10452   9504      7        0      1      0 2022-11-27 23:04:34 UTC+0000
0xffffae0d7eae2080 svchost.exe           10468    920      8        0      0      0 2022-11-27 23:04:34 UTC+0000
0xffffae0d7ef85080 SearchIndexer.        10748    920     16        0      0      0 2022-11-27 23:04:34 UTC+0000
0xffffae0d820dd2c0 StartMenuExper        11204    100     10        0      1      0 2022-11-27 23:04:35 UTC+0000
0xffffae0d81fc6080 svchost.exe            9976    920      6        0      0      0 2022-11-27 23:04:35 UTC+0000
0xffffae0d81fe4080 RuntimeBroker.         7540    100      2        0      1      0 2022-11-27 23:04:35 UTC+0000
0xffffae0d824f6080 SearchApp.exe         11772    100     71        0      1      0 2022-11-27 23:04:36 UTC+0000
0xffffae0d82876080 RuntimeBroker.        12128    100     12        0      1      0 2022-11-27 23:04:36 UTC+0000
0xffffae0d828d2080 NVIDIA Web Hel        12176   3096     90        0      1      1 2022-11-27 23:04:36 UTC+0000
0xffffae0d81bcd0c0 conhost.exe           11816  12176      2        0      1      0 2022-11-27 23:04:36 UTC+0000
0xffffae0d81bdc080 svchost.exe           12240    920      5        0      0      0 2022-11-27 23:04:36 UTC+0000
0xffffae0d81bf3080 backgroundTask        12516    100      0 --------      1      0 2022-11-27 23:04:36 UTC+0000   2022-11-27 23:05:41 UTC+0000
0xffffae0d7cca70c0 ctfmon.exe            13092   1716     12        0      1      0 2022-11-27 23:04:37 UTC+0000
0xffffae0d7ccaa080 dllhost.exe           12580    100      5        0      1      0 2022-11-27 23:04:37 UTC+0000
0xffffae0d7f757080 avpui.exe             13392   4244     19        0      1      1 2022-11-27 23:04:38 UTC+0000
0xffffae0d7f76f080 svchost.exe           13508    920      4        0      1      0 2022-11-27 23:04:40 UTC+0000
0xffffae0d7f944280 GraphicsCardEn        13104   1420      0 --------      1      1 2022-11-27 23:04:44 UTC+0000   2022-11-27 23:10:25 UTC+0000
0xffffae0d7f922080 TextInputHost.         5036    100     16        0      1      0 2022-11-27 23:04:44 UTC+0000
0xffffae0d7faf1080 RuntimeBroker.        14164    100      2        0      1      0 2022-11-27 23:04:45 UTC+0000
0xffffae0d81a0a240 RuntimeBroker.         5940    100      2        0      1      0 2022-11-27 23:04:46 UTC+0000
```

25) Copy pagefile.sys (from your VM) to SIFT and load it to volatility. Show the information stored in pagefile.sys?



Memory Capture

Destination path: C:\Users\fireb\Desktop

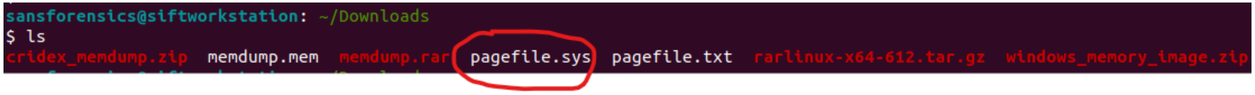
Destination filename: memdump.mem

☑ Include pagefile

pagefile.sys

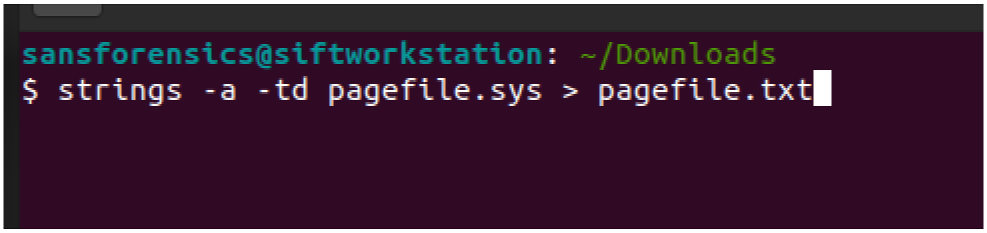
□ Create AD1 file

memcapture.ad1

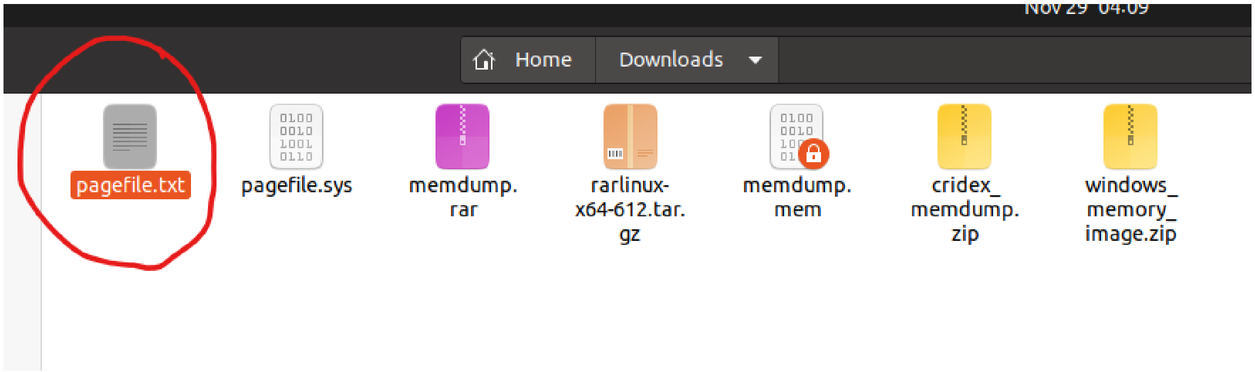


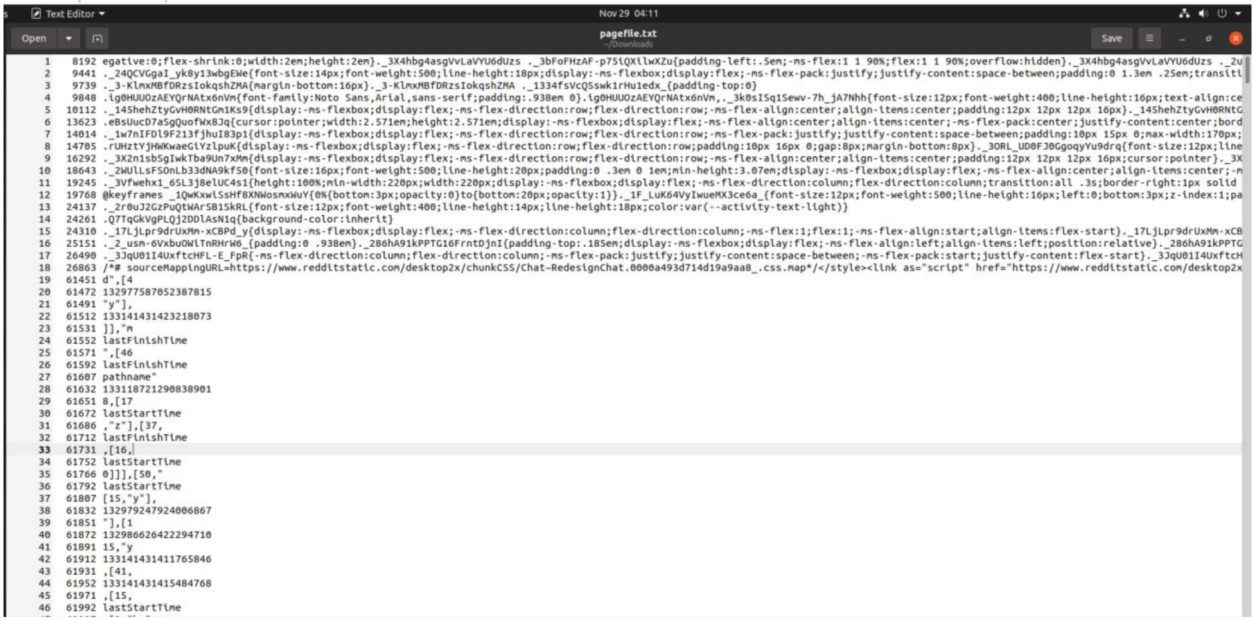
```
sansforensics@siftworkstation: ~/Downloads
$ ls
cridex_memdump.zip  memdump.mem  memdump.rar  pagefile.sys  pagefile.txt  rarlinux-x64-612.tar.gz  windows_memory_image.zip
```

Writing it to a text file to see what is inside pagefile.sys:



```
sansforensics@siftworkstation: ~/Downloads
$ strings -a -td pagefile.sys > pagefile.txt
```





```
 8192 egative:0;flex-shrink:0;width:2em;height:2em}._3X4hbg4asgVvLaVYU6dUzs ._3bFoFHzAF-p75iQXilwXZu{padding-left:.5em;-ms-flex:1 1 90%;flex:1 1 90%;overflow:hidden}._3X4hbg4asgVvLaVYU6dUzs ._2u
 9441 ._24QCVGgaI_yk8y13wbgEWe{font-size:14px;font-weight:500;line-height:18px;display:-ms-flexbox;display:flex;-ms-flex-pack:justify;justify-content:space-between;padding:0 1.3em .25em;transiti
 9739 ._3-KlmxMBfDRzsIokqshZMA{margin-bottom:16px}._3-KlmxMBfDRzsIokqshZMA ._1334fsVcQSswk1rHu1edx_{padding-top:0}
 9848 .ig0HUUOzAEYQrNAtx6nVm{font-family:Noto Sans,Arial,sans-serif;padding:.938em 0}.ig0HUUOzAEYQrNAtx6nVm,._3k0sISq1Sewv-7h_jA7Nhh{font-size:12px;font-weight:400;line-height:16px;text-align:ce
10112 ._145hehZtyGvH0RNtGm1Ks9{display:-ms-flexbox;display:flex;-ms-flex-direction:row;flex-direction:row;-ms-flex-align:center;align-items:center;padding:12px 12px 12px 16px}._145hehZtyGvH0RNtG
13623 .eBsUucD7aSgQuofWx8Jq{cursor:pointer;width:2.571em;height:2.571em;display:-ms-flexbox;display:flex;-ms-flex-align:center;align-items:center;-ms-flex-pack:center;justify-content:center;bord
14014 ._1w7nIFDl9F213fjhuI83p1{display:-ms-flexbox;display:flex;-ms-flex-direction:row;flex-direction:row;-ms-flex-pack:justify;justify-content:space-between;padding:10px 15px 0;max-width:170px;
14705 .rUHztYjHWKwaeGiYzlpuK{display:-ms-flexbox;display:flex;-ms-flex-direction:row;flex-direction:row;padding:10px 16px 0;gap:8px;margin-bottom:8px}._3ORL_UD0FJ0GgoqyYu9drq{font-size:12px;line
16292 ._3X2n1sbSgIwkTba9Un7xMm{display:-ms-flexbox;display:flex;-ms-flex-direction:row;flex-direction:row;-ms-flex-align:center;align-items:center;padding:12px 12px 12px 16px;cursor:pointer}._3X
18643 ._2WUlLsFSOnLb33dNA9kf50{font-size:16px;font-weight:500;line-height:20px;padding:0 .3em 0 1em;min-height:3.07em;display:-ms-flexbox;display:flex;-ms-flex-align:center;align-items:center;-m
19245 ._3Vfwehx1_6SL3j8elUC4s1{height:100%;min-width:220px;width:220px;display:-ms-flexbox;display:flex;-ms-flex-direction:column;flex-direction:column;transition:all .3s;border-right:1px solid
19768 @keyframes _1QwKxwiSsHf8XNWosmxWuY{0%{bottom:3px;opacity:0}to{bottom:20px;opacity:1}}._1F_LuK64VyIwueMX3ce6a_{font-size:12px;font-weight:500;line-height:16px;left:0;bottom:3px;z-index:1;pa
24137 ._2r0uJ2GzPuQtWArSB1SkRL{font-size:12px;font-weight:400;line-height:14px;line-height:18px;color:var(--activity-text-light)}
24261 .Q7TqGkVgPLQj2DDlAsN1q{background-color:inherit}
24310 ._17LjLpr9drUxMm-xCBPd_y{display:-ms-flexbox;display:flex;-ms-flex-direction:column;flex-direction:column;-ms-flex:1;flex:1;-ms-flex-align:start;align-items:flex-start}._17LjLpr9drUxMm-xCB
25151 ._2_usm-6VxbuOWiTnRHrW6_{padding:0 .938em}._286hA91kPPTG16FrntDjnI{padding-top:.185em;display:-ms-flexbox;display:flex;-ms-flex-align:left;align-items:left;position:relative}._286hA91kPPTG
26490 ._3JqU01I4UxftcHFL-E_FpR{-ms-flex-direction:column;flex-direction:column;-ms-flex-pack:justify;justify-content:space-between;-ms-flex-pack:start;justify-content:flex-start}._3JqU01I4UxftcH
26863 /*# sourceMappingURL=https://www.redditstatic.com/desktop2x/chunkCSS/Chat~RedesignChat.0000a493d714d19a9aa8_.css.map*/</style><link as="script" href="https://www.redditstatic.com/desktop2x
61451 d",[4
61472 132977587052387815
61491 "y"],
61512 133141431423218073
61531 ]],"m
61552 lastFinishTime
61571 ",[46
61592 lastFinishTime
61607 pathname"
61632 133118721290838901
61651 8,[17
61672 lastStartTime
61686 ,"z"],[37,
61712 lastFinishTime
61731 ,[16,
61752 lastStartTime
61766 0]]],[50,"
61792 lastStartTime
61807 [15,"y"],
61832 132979247924006867
61851 "],[1
61872 132986626422294710
61891 15,"y
61912 133141431411765846
61931 ,[41,
61952 133141431415484768
61971 ,[15,
61992 lastStartTime
```