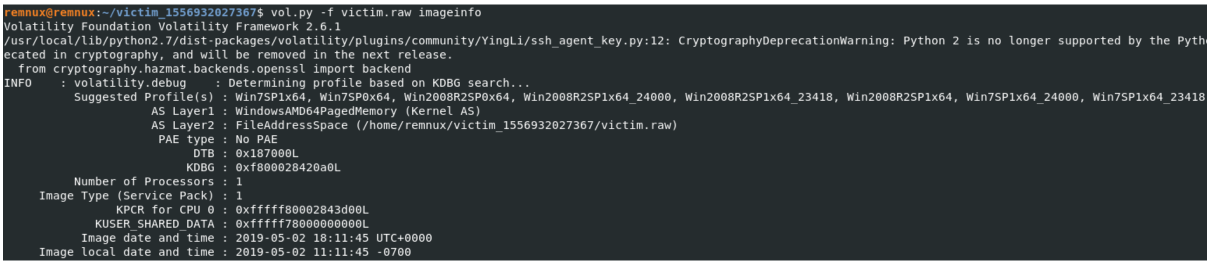
TryHackMe: Forensics

The following writeup is for Forensics, a room hosted on TryHackMe. This room is rated as hard difficulty, and involves analysing a memory dump of a compromised system using volatility. The room rating is farfetched, in my opinion, this room should be rated as medium difficulty, and maybe even easy. I have participated in medium difficulty rooms that were far more difficult than this. Nonetheless, this is a really fun room and I highly recommend it for those who enjoy memory forensics.

What is the Operating System of this Dump file? (OS name)

To determine the Operating System of this Dump file, we can use the imageinfo plugin like as follows:



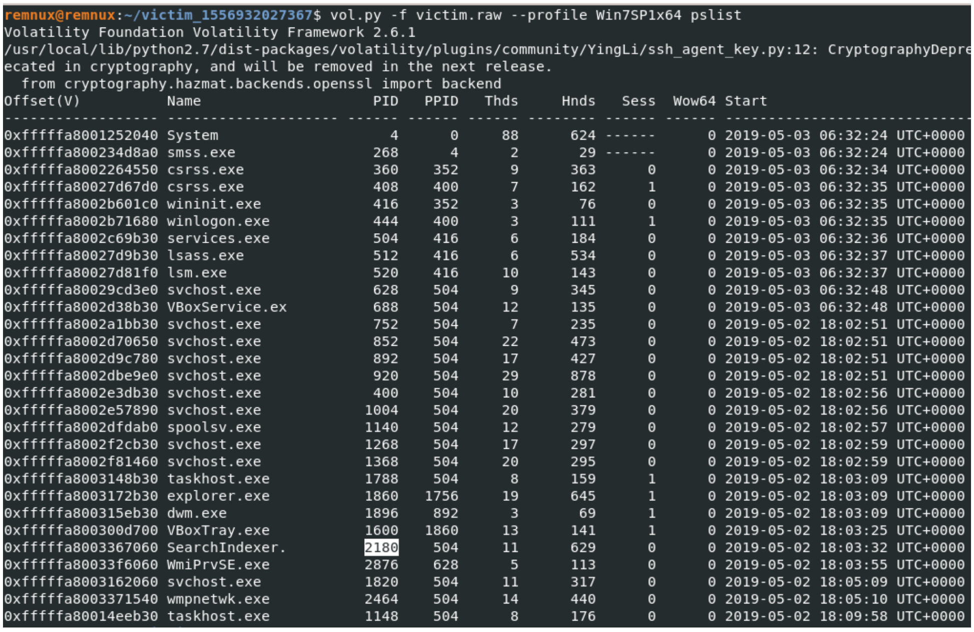
```
remnux@remnux:~/victim_1556932027367$ vol.py -f victim.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Pyth
ecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/remnux/victim_1556932027367/victim.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800028420a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002843d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-05-02 18:11:45 UTC+0000
     Image local date and time : 2019-05-02 11:11:45 -0700
```

Based on this, it is pretty obvious that the OS is Windows.

Answer: Windows

What is the PID of SearchIndexer?

To list all the running processes, we can use a series of plugins including pslist:



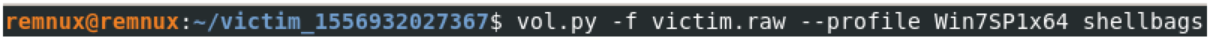
```
remnux@remnux:~/victim_1556932027367$ vol.py -f victim.raw --profile Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyDepre
ecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
0xfffffa8001252040 System                    4      0     88      624 ------      0 2019-05-03 06:32:24 UTC+0000
0xfffffa800234d8a0 smss.exe                268      4      2       29 ------      0 2019-05-03 06:32:24 UTC+0000
0xfffffa8002264550 csrss.exe               360    352      9      363      0      0 2019-05-03 06:32:34 UTC+0000
0xfffffa80027d67d0 csrss.exe               408    400      7      162      1      0 2019-05-03 06:32:35 UTC+0000
0xfffffa8002b601c0 wininit.exe             416    352      3       76      0      0 2019-05-03 06:32:35 UTC+0000
0xfffffa8002b71680 winlogon.exe            444    400      3      111      1      0 2019-05-03 06:32:35 UTC+0000
0xfffffa8002c69b30 services.exe            504    416      6      184      0      0 2019-05-03 06:32:36 UTC+0000
0xfffffa80027d9b30 lsass.exe               512    416      6      534      0      0 2019-05-03 06:32:37 UTC+0000
0xfffffa80027d81f0 lsm.exe                 520    416     10      143      0      0 2019-05-03 06:32:37 UTC+0000
0xfffffa80029cd3e0 svchost.exe             628    504      9      345      0      0 2019-05-03 06:32:48 UTC+0000
0xfffffa8002d38b30 VBoxService.ex          688    504     12      135      0      0 2019-05-03 06:32:48 UTC+0000
0xfffffa8002a1bb30 svchost.exe             752    504      7      235      0      0 2019-05-02 18:02:51 UTC+0000
0xfffffa8002d70650 svchost.exe             852    504     22      473      0      0 2019-05-02 18:02:51 UTC+0000
0xfffffa8002d9c780 svchost.exe             892    504     17      427      0      0 2019-05-02 18:02:51 UTC+0000
0xfffffa8002dbe9e0 svchost.exe             920    504     29      878      0      0 2019-05-02 18:02:51 UTC+0000
0xfffffa8002e3db30 svchost.exe             400    504     10      281      0      0 2019-05-02 18:02:56 UTC+0000
0xfffffa8002e57890 svchost.exe            1004    504     20      379      0      0 2019-05-02 18:02:56 UTC+0000
0xfffffa8002dfdab0 spoolsv.exe            1140    504     12      279      0      0 2019-05-02 18:02:57 UTC+0000
0xfffffa8002f2cb30 svchost.exe            1268    504     17      297      0      0 2019-05-02 18:02:59 UTC+0000
0xfffffa8002f81460 svchost.exe            1368    504     20      295      0      0 2019-05-02 18:02:59 UTC+0000
0xfffffa8003148b30 taskhost.exe           1788    504      8      159      1      0 2019-05-02 18:03:09 UTC+0000
0xfffffa8003172b30 explorer.exe           1860   1756     19      645      1      0 2019-05-02 18:03:09 UTC+0000
0xfffffa800315eb30 dwm.exe                1896    892      3       69      1      0 2019-05-02 18:03:09 UTC+0000
0xfffffa800300d700 VBoxTray.exe           1600   1860     13      141      1      0 2019-05-02 18:03:25 UTC+0000
0xfffffa8003367060 SearchIndexer.         2180    504     11      629      0      0 2019-05-02 18:03:32 UTC+0000
0xfffffa80033f6060 WmiPrvSE.exe           2876    628      5      113      0      0 2019-05-02 18:03:55 UTC+0000
0xfffffa8003162060 svchost.exe            1820    504     11      317      0      0 2019-05-02 18:05:09 UTC+0000
0xfffffa8003371540 wmpnetwk.exe           2464    504     14      440      0      0 2019-05-02 18:05:10 UTC+0000
0xfffffa80014eeb30 taskhost.exe           1148    504      8      176      0      0 2019-05-02 18:09:58 UTC+0000
```

Answer: 2180

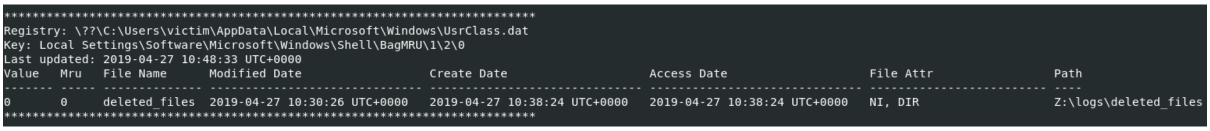
What is the last directory accessed by the user?

(The last folder name as it is?)

To find the last directory accessed by the user, we can use a forensic artifact known as Shellbags. Shellbags are registry keys for which store information about how users view folders in Windows. This is forensically important because it provides an investigator with information about the browsing history of the victim. Fortunately for us, Volatility has a shellbags plugin:



```
remnux@remnux:~/victim_1556932027367$ vol.py -f victim.raw --profile Win7SP1x64 shellbags
```

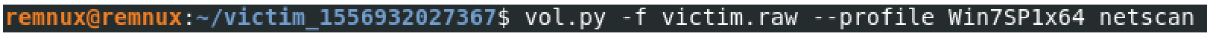


```
***************************************************************************
Registry: \??\C:\Users\victim\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\2\0
Last updated: 2019-04-27 10:48:33 UTC+0000
Value   Mru   File Name      Modified Date                  Create Date                    Access Date                    File Attr                Path
------- ----- -------------- ------------------------------ ------------------------------ ------------------------------ ------------------------ ----
0       0     deleted_files  2019-04-27 10:30:26 UTC+0000   2019-04-27 10:38:24 UTC+0000   2019-04-27 10:38:24 UTC+0000   NI, DIR                  Z:\logs\deleted_files
***************************************************************************
```

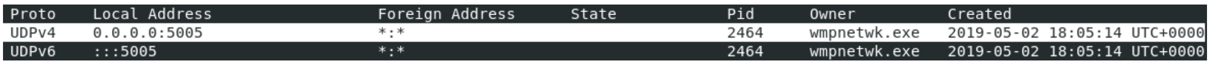
Answer: deleted_files

There are many suspicious open ports; which one is it? (ANSWER format: protocol:port)

To find any suspicious open ports, we can use the netscan plugin:



```
remnux@remnux:~/victim_1556932027367$ vol.py -f victim.raw --profile Win7SP1x64 netscan
```

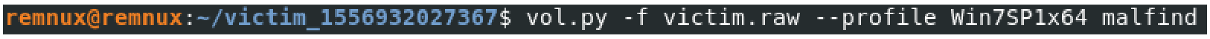


```
 Proto    Local Address                    Foreign Address      State            Pid      Owner          Created
 UDPv4    0.0.0.0:5005                     *:*                                   2464     wmpnetwk.exe   2019-05-02 18:05:14 UTC+0000
 UDPv6    :::5005                          *:*                                   2464     wmpnetwk.exe   2019-05-02 18:05:14 UTC+0000
```

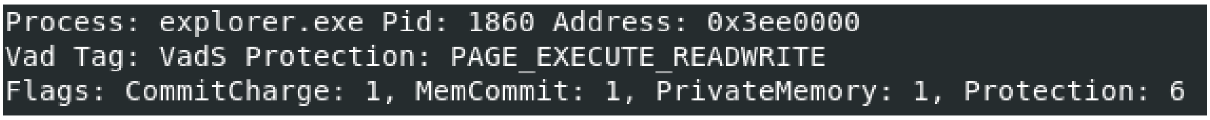
Answer: UDP:5005

Vads tag and execute protection are strong indicators of malicious processes; can you find which they are? (ANSWER format: Pid1;Pid2;Pid3)

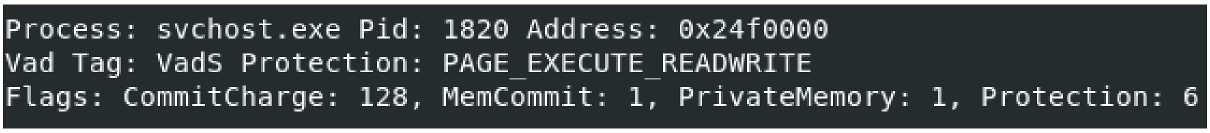
Vad tags can be analysed by using the malfind plugin, enabling analysts to identify memory regions that contain permissions such as EXECUTE_READWRITE.



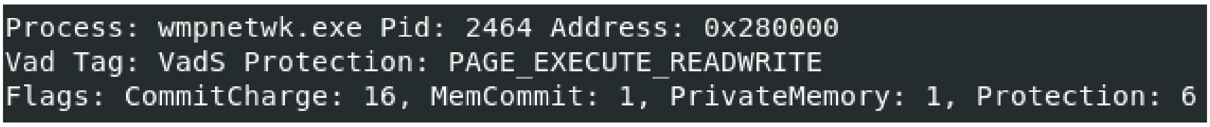
```
remnux@remnux:~/victim_1556932027367$ vol.py -f victim.raw --profile Win7SP1x64 malfind
```



```
Process: explorer.exe Pid: 1860 Address: 0x3ee0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6
```



```
Process: svchost.exe Pid: 1820 Address: 0x24f0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 128, MemCommit: 1, PrivateMemory: 1, Protection: 6
```



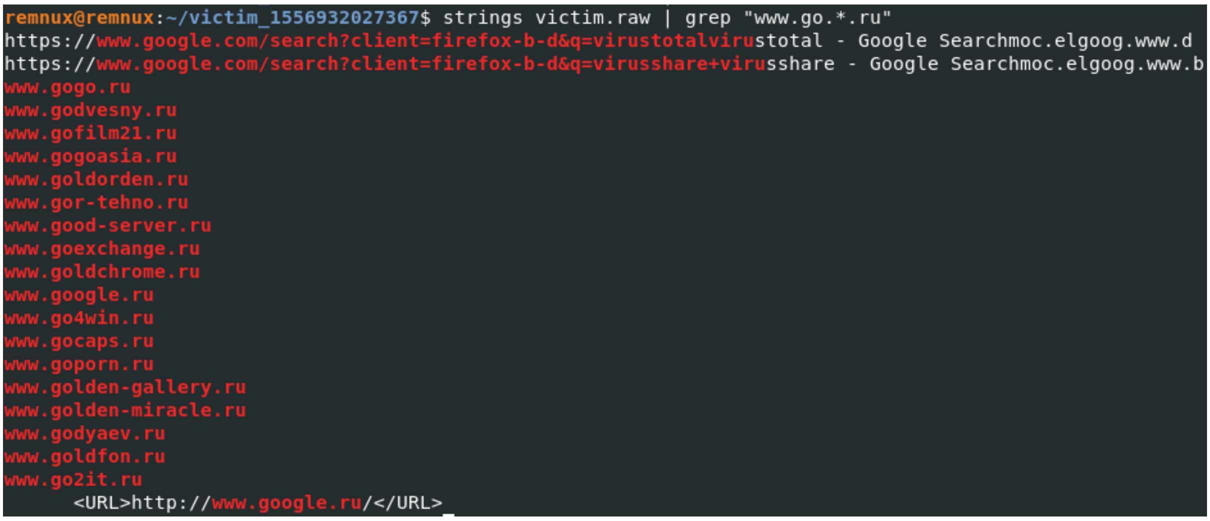
```
Process: wmpnetwk.exe Pid: 2464 Address: 0x280000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 16, MemCommit: 1, PrivateMemory: 1, Protection: 6
```

Answer: 1860;1820;2464

In the previous task, you identified malicious processes, so let's dig into them and find some Indicator of Compromise (IOC). You just need to find them and fill in the blanks (You may search for them on VirusTotal to discover more details).

'www.go**.ru' (write full url without any quotation marks)**

To find the full link, we can simply run strings against the file, and pipe the output to grep like as follows:

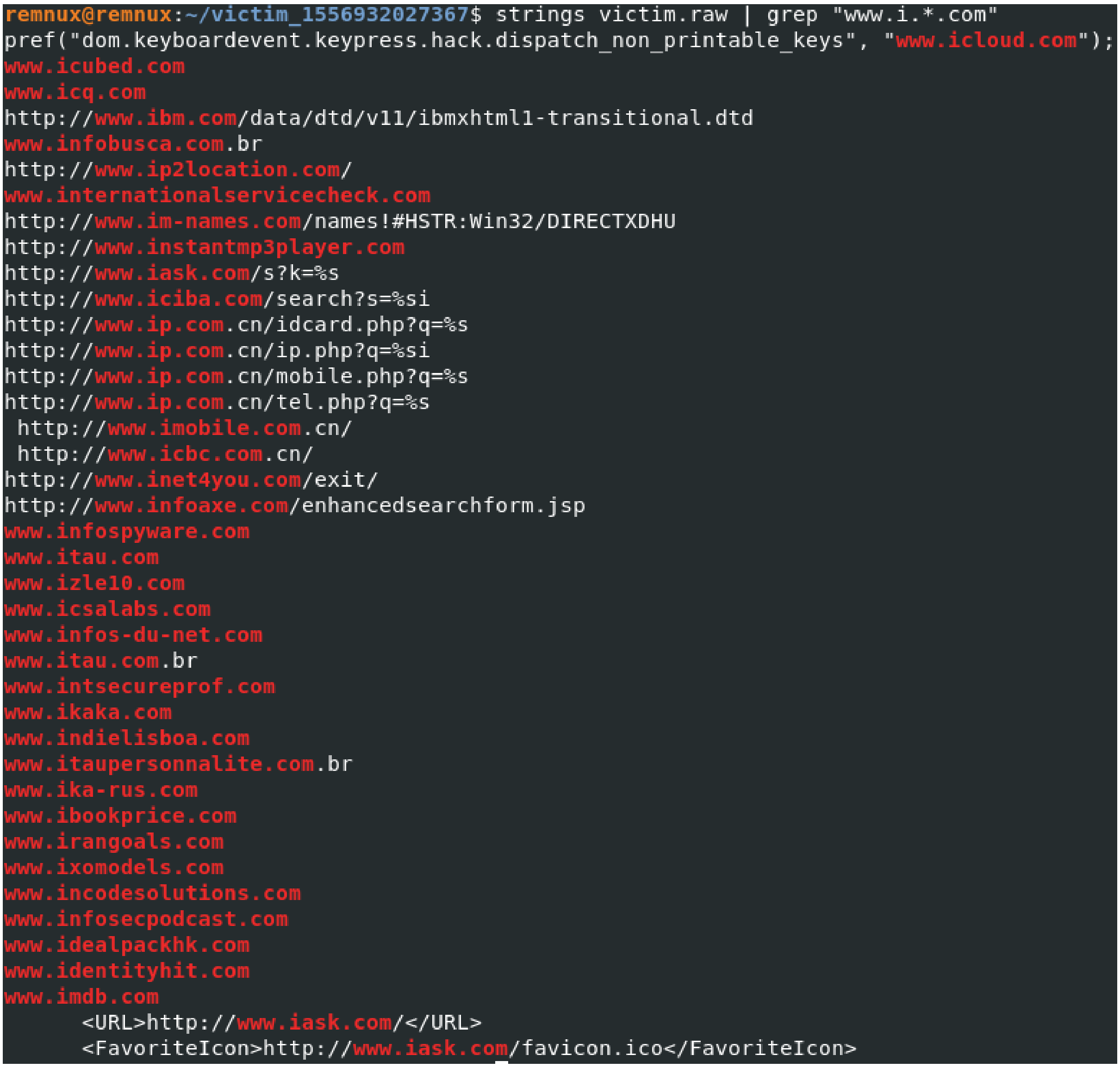


```
remnux@remnux:~/victim_1556932027367$ strings victim.raw | grep "www.go.*.ru"
https://www.google.com/search?client=firefox-b-d&q=virustotalvirustotal - Google Searchmoc.elgoog.www.d
https://www.google.com/search?client=firefox-b-d&q=virusshare+virusshare - Google Searchmoc.elgoog.www.b
www.gogo.ru
www.godvesny.ru
www.gofilm21.ru
www.gogoasia.ru
www.goldorden.ru
www.gor-tehno.ru
www.good-server.ru
www.goexchange.ru
www.goldchrome.ru
www.google.ru
www.go4win.ru
www.gocaps.ru
www.goporn.ru
www.golden-gallery.ru
www.golden-miracle.ru
www.godyaev.ru
www.goldfon.ru
www.go2it.ru
      <URL>http://www.google.ru/</URL>
```

Answer: www.goporn.ru

'www.i**.com' (write full url without any quotation marks)**

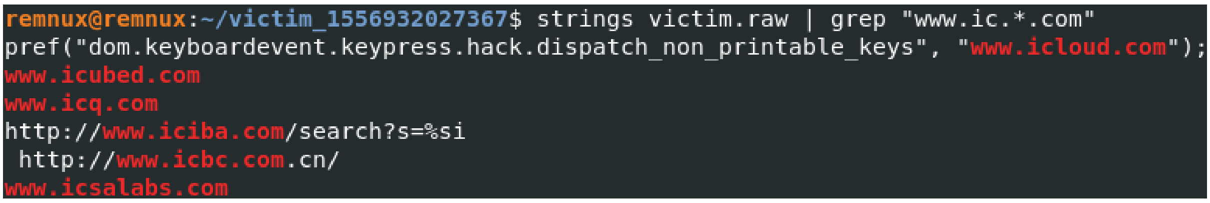
Follow the same process as done previously:



```
remnux@remnux:~/victim_1556932027367$ strings victim.raw | grep "www.i.*.com"
pref("dom.keyboardevent.keypress.hack.dispatch_non_printable_keys", "www.icloud.com");
www.icubed.com
www.icq.com
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd
www.infobusca.com.br
http://www.ip2location.com/
www.internationalservicecheck.com
http://www.im-names.com/names!#HSTR:Win32/DIRECTXDHU
http://www.instantmp3player.com
http://www.iask.com/s?k=%s
http://www.iciba.com/search?s=%si
http://www.ip.com.cn/idcard.php?q=%s
http://www.ip.com.cn/ip.php?q=%si
http://www.ip.com.cn/mobile.php?q=%s
http://www.ip.com.cn/tel.php?q=%s
 http://www.imobile.com.cn/
 http://www.icbc.com.cn/
http://www.inet4you.com/exit/
http://www.infoaxe.com/enhancedsearchform.jsp
www.infospyware.com
www.itau.com
www.izle10.com
www.icsalabs.com
www.infos-du-net.com
www.itau.com.br
www.intsecureprof.com
www.ikaka.com
www.indielisboa.com
www.itaupersonnalite.com.br
www.ika-rus.com
www.ibookprice.com
www.irangoals.com
www.ixomodels.com
www.incodesolutions.com
www.infosecpodcast.com
www.idealpackhk.com
www.identityhit.com
www.imdb.com
      <URL>http://www.iask.com/</URL>
      <FavoriteIcon>http://www.iask.com/favicon.ico</FavoriteIcon>
```

Answer: www.ikaka.com

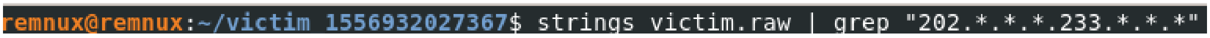
'www.ic****.com'**



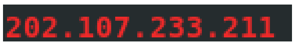
```
remnux@remnux:~/victim_1556932027367$ strings victim.raw | grep "www.ic.*.com"
pref("dom.keyboardevent.keypress.hack.dispatch_non_printable_keys", "www.icloud.com");
www.icubed.com
www.icq.com
http://www.iciba.com/search?s=%si
 http://www.icbc.com.cn/
www.icsalabs.com
```

Answer: www.icsalabs.com

202.*.233.*** (Write full IP)**



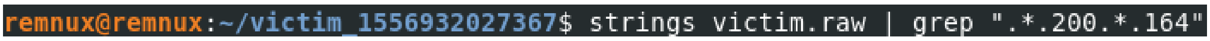
```
remnux@remnux:~/victim 1556932027367$ strings victim.raw | grep "202.*.*.*.233.*.*.*"
```



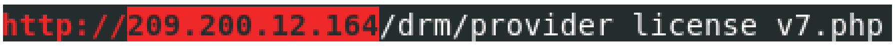
```
202.107.233.211
```

Answer: 202.107.233.211

*****.200.**.164 (Write full IP)**



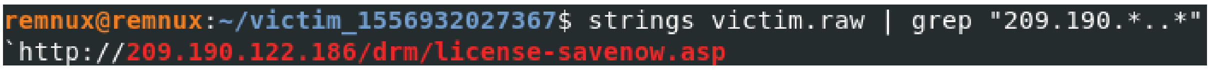
```
remnux@remnux:~/victim_1556932027367$ strings victim.raw | grep ".*.200.*.164"
```



```
http://209.200.12.164/drm/provider license v7.php
```

Answer: 209.200.12.164

209.190.*.*****

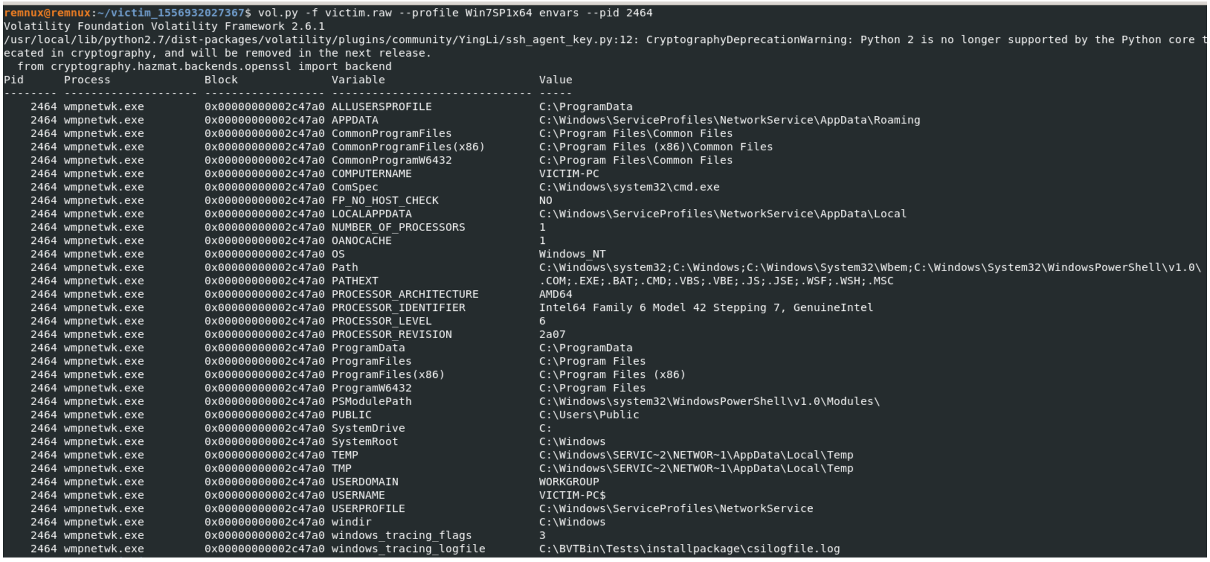


```
remnux@remnux:~/victim_1556932027367$ strings victim.raw | grep "209.190.*..*"
`http://209.190.122.186/drm/license-savenow.asp
```

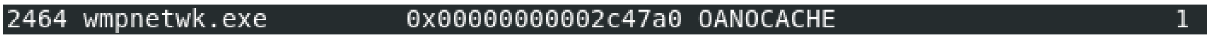
Answer: 209.190.122.186

What is the unique environmental variable of PID 2464?

You can use the envars plugin and the --pid option to find the unique environmental variable of PID 2464:



```
remnux@remnux:~/victim_1556932027367$ vol.py -f victim.raw --profile Win7SP1x64 envars --pid 2464
Volatility Foundation Volatility Framework 2.6.1
/usr/local/lib/python2.7/dist-packages/volatility/plugins/community/YingLi/ssh_agent_key.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core t
ecated in cryptography, and will be removed in the next release.
  from cryptography.hazmat.backends.openssl import backend
Pid      Process              Block              Variable                       Value
-------- -------------------- ------------------ ------------------------------ -----
    2464 wmpnetwk.exe         0x00000000002c47a0 ALLUSERSPROFILE                C:\ProgramData
    2464 wmpnetwk.exe         0x00000000002c47a0 APPDATA                        C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming
    2464 wmpnetwk.exe         0x00000000002c47a0 CommonProgramFiles             C:\Program Files\Common Files
    2464 wmpnetwk.exe         0x00000000002c47a0 CommonProgramFiles(x86)        C:\Program Files (x86)\Common Files
    2464 wmpnetwk.exe         0x00000000002c47a0 CommonProgramW6432             C:\Program Files\Common Files
    2464 wmpnetwk.exe         0x00000000002c47a0 COMPUTERNAME                   VICTIM-PC
    2464 wmpnetwk.exe         0x00000000002c47a0 ComSpec                        C:\Windows\system32\cmd.exe
    2464 wmpnetwk.exe         0x00000000002c47a0 FP_NO_HOST_CHECK               NO
    2464 wmpnetwk.exe         0x00000000002c47a0 LOCALAPPDATA                   C:\Windows\ServiceProfiles\NetworkService\AppData\Local
    2464 wmpnetwk.exe         0x00000000002c47a0 NUMBER_OF_PROCESSORS           1
    2464 wmpnetwk.exe         0x00000000002c47a0 OANOCACHE                      1
    2464 wmpnetwk.exe         0x00000000002c47a0 OS                             Windows_NT
    2464 wmpnetwk.exe         0x00000000002c47a0 Path                           C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
    2464 wmpnetwk.exe         0x00000000002c47a0 PATHEXT                        .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
    2464 wmpnetwk.exe         0x00000000002c47a0 PROCESSOR_ARCHITECTURE         AMD64
    2464 wmpnetwk.exe         0x00000000002c47a0 PROCESSOR_IDENTIFIER           Intel64 Family 6 Model 42 Stepping 7, GenuineIntel
    2464 wmpnetwk.exe         0x00000000002c47a0 PROCESSOR_LEVEL                6
    2464 wmpnetwk.exe         0x00000000002c47a0 PROCESSOR_REVISION             2a07
    2464 wmpnetwk.exe         0x00000000002c47a0 ProgramData                    C:\ProgramData
    2464 wmpnetwk.exe         0x00000000002c47a0 ProgramFiles                   C:\Program Files
    2464 wmpnetwk.exe         0x00000000002c47a0 ProgramFiles(x86)              C:\Program Files (x86)
    2464 wmpnetwk.exe         0x00000000002c47a0 ProgramW6432                   C:\Program Files
    2464 wmpnetwk.exe         0x00000000002c47a0 PSModulePath                   C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
    2464 wmpnetwk.exe         0x00000000002c47a0 PUBLIC                         C:\Users\Public
    2464 wmpnetwk.exe         0x00000000002c47a0 SystemDrive                    C:
    2464 wmpnetwk.exe         0x00000000002c47a0 SystemRoot                     C:\Windows
    2464 wmpnetwk.exe         0x00000000002c47a0 TEMP                           C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
    2464 wmpnetwk.exe         0x00000000002c47a0 TMP                            C:\Windows\SERVIC~2\NETWOR~1\AppData\Local\Temp
    2464 wmpnetwk.exe         0x00000000002c47a0 USERDOMAIN                     WORKGROUP
    2464 wmpnetwk.exe         0x00000000002c47a0 USERNAME                       VICTIM-PC$
    2464 wmpnetwk.exe         0x00000000002c47a0 USERPROFILE                    C:\Windows\ServiceProfiles\NetworkService
    2464 wmpnetwk.exe         0x00000000002c47a0 windir                         C:\Windows
    2464 wmpnetwk.exe         0x00000000002c47a0 windows_tracing_flags          3
    2464 wmpnetwk.exe         0x00000000002c47a0 windows_tracing_logfile        C:\BVTBin\Tests\installpackage\csilogfile.log
```



```
2464 wmpnetwk.exe         0x00000000002c47a0 OANOCACHE                      1
```

Answer: OANOCACHE