# Práctica 3

# Analizando la RAM 3

Esta práctica implica el análisis de un volcado de memoria que se sospecha ha sido infectado de manera persistente por algún tipo de malware, posiblemente un dropper. Se nos encomienda la tarea de identificar el dominio malicioso utilizado por este malware.

Lo primero que haremos es utilizar el parámetro 'imageinfo' para obtener el perfil de esta imagen."

```
┌──(kali㉿kali)-[~/practica3]
└─$ vol.py -f memory.2244013c.img 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/kali/practica3/memory.2244013c.img)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x8054cf60L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-10-20 23:53:02 UTC+0000
     Image local date and time : 2018-10-21 01:53:02 +0200
```

Seguidamente, procederemos a verificar los procesos utilizando los comandos pslist, pstree, psscan y psxviewer."

```
┌──(kali㉿kali)-[~/practica3]
└─$ vol.py -f memory.2244013c.img --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x80eed020 System                    4      0     55      251 ------      0
0x80d42da0 smss.exe                368      4      3       19 ------      0 2018-10-20 22:45:17 UTC+0000
0x80d407e0 csrss.exe               592    368     12      497      0      0 2018-10-20 22:45:18 UTC+0000
0xffba6020 winlogon.exe            616    368     18      449      0      0 2018-10-20 22:45:18 UTC+0000
0x80dbe7e8 services.exe            660    616     16      260      0      0 2018-10-20 22:45:18 UTC+0000
0xffbd4228 lsass.exe               672    616     22      355      0      0 2018-10-20 22:45:18 UTC+0000
0x80d357e8 VBoxService.exe         828    660      8      105      0      0 2018-10-20 22:45:18 UTC+0000
0xffbbb578 svchost.exe             872    660     19      218      0      0 2018-10-20 23:45:19 UTC+0000
0x80d23938 svchost.exe             960    660     12      285      0      0 2018-10-20 23:45:19 UTC+0000
0xff9f5790 svchost.exe            1052    660     83     1431      0      0 2018-10-20 23:45:19 UTC+0000
0xff9edc10 svchost.exe            1112    660      6       62      0      0 2018-10-20 23:45:19 UTC+0000
0xffb98c20 svchost.exe            1192    660     11      164      0      0 2018-10-20 23:45:19 UTC+0000
0xff9c8c38 spoolsv.exe            1396    660     10      116      0      0 2018-10-20 23:45:19 UTC+0000
0xffba7890 explorer.exe           1608   1552      0 ------      0      0 2018-10-20 23:45:26 UTC+0000   2018-10-20 23:46:29 UTC+0000
0xffbb5da0 VBoxTray.exe           1760   1608     11      132      0      0 2018-10-20 23:45:27 UTC+0000
0x80d5e900 ctfmon.exe             1768   1608      1       79      0      0 2018-10-20 23:45:27 UTC+0000
0xffb9b7e8 cmd.exe                1976   1608      1       32      0      0 2018-10-20 23:45:48 UTC+0000
0xffb76a78 svchost.exe             944    660      5      104      0      0 2018-10-20 23:46:29 UTC+0000
0x80d26da0 explorer.exe           1868    616     21      733      0      0 2018-10-20 23:46:33 UTC+0000
0xff948b20 alg.exe                 248    660      6      105      0      0 2018-10-20 23:46:34 UTC+0000
0xff92c738 wscntfy.exe            1124   1052      1       39      0      0 2018-10-20 23:46:36 UTC+0000
0xff912438 msiexec.exe            1160    660      8      201      0      0 2018-10-20 23:47:01 UTC+0000
0xffbc5a78 msiexec.exe            1968   1160      0 ------      0      0 2018-10-20 23:47:04 UTC+0000   2018-10-20 23:47:07 UTC+0000
0xff8ff020 IEXPLORE.EXE           1624   1868     16      508      0      0 2018-10-20 23:47:12 UTC+0000
0x80e02bb8 msimn.exe               536   1868     11      323      0      0 2018-10-20 23:47:14 UTC+0000
0xff8f4020 msmsgs.exe              496    872      4      195      0      0 2018-10-20 23:47:14 UTC+0000
0xff8fbda0 msninst.exe            2256   1868     13      412      0      0 2018-10-20 23:47:33 UTC+0000
0xff956020 regedit.exe            2664   1868      1       53      0      0 2018-10-20 23:49:26 UTC+0000
0xff8db020 cmd.exe                3468   1868      1       30      0      0 2018-10-20 23:50:06 UTC+0000
0xff91e570 cmd.exe                1080   1868      1       32      0      0 2018-10-20 23:50:43 UTC+0000
0xffb82aa0 IEXPLORE.EXE           3728   1868     15      486      0      0 2018-10-20 23:52:15 UTC+0000
0xff913c98 cmd.exe                 300   1868      1       32      0      0 2018-10-20 23:52:27 UTC+0000
0xff9d37f0 Memoryze.exe           1896    300      1       69      0      0 2018-10-20 23:53:02 UTC+0000
```

```
└─$ vol.py -f memory.2244013c.img --profile=WinXPSP2x86 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x80eed020:System                                      4      0     55    251 1970-01-01 00:00:00 UTC+0000
. 0x80d42da0:smss.exe                                 368      4      3     19 2018-10-20 22:45:17 UTC+0000
.. 0x80d407e0:csrss.exe                               592    368     12    497 2018-10-20 22:45:18 UTC+0000
.. 0xffba6020:winlogon.exe                            616    368     18    449 2018-10-20 22:45:18 UTC+0000
... 0x80dbe7e8:services.exe                           660    616     16    260 2018-10-20 22:45:18 UTC+0000
.... 0xff912438:msiexec.exe                          1160    660      8    201 2018-10-20 23:47:01 UTC+0000
..... 0xffbc5a78:msiexec.exe                         1968   1160      0 ------ 2018-10-20 23:47:04 UTC+0000
.... 0xff9f5790:svchost.exe                          1052    660     83   1431 2018-10-20 23:45:19 UTC+0000
..... 0xff92c738:wscntfy.exe                         1124   1052      1     39 2018-10-20 23:46:36 UTC+0000
.... 0xffb98c20:svchost.exe                          1192    660     11    164 2018-10-20 23:45:19 UTC+0000
.... 0xffb76a78:svchost.exe                           944    660      5    104 2018-10-20 23:46:29 UTC+0000
.... 0x80d357e8:VBoxService.exe                       828    660      8    105 2018-10-20 22:45:18 UTC+0000
.... 0x80d23938:svchost.exe                           960    660     12    285 2018-10-20 23:45:19 UTC+0000
.... 0xffbbb578:svchost.exe                           872    660     19    218 2018-10-20 23:45:19 UTC+0000
..... 0xff8f4020:msmsgs.exe                           496    872      4    195 2018-10-20 23:47:14 UTC+0000
.... 0xff9edc10:svchost.exe                          1112    660      6     62 2018-10-20 23:45:19 UTC+0000
.... 0xff9c8c38:spoolsv.exe                          1396    660     10    116 2018-10-20 23:45:19 UTC+0000
.... 0xff948b20:alg.exe                               248    660      6    105 2018-10-20 23:46:34 UTC+0000
... 0xffbd4228:lsass.exe                              672    616     22    355 2018-10-20 22:45:18 UTC+0000
... 0x80d26da0:explorer.exe                          1868    616     21    733 2018-10-20 23:46:33 UTC+0000
.... 0xff956020:regedit.exe                          2664   1868      1     53 2018-10-20 23:49:26 UTC+0000
.... 0xff8db020:cmd.exe                              3468   1868      1     30 2018-10-20 23:50:06 UTC+0000
.... 0xffb82aa0:IEXPLORE.EXE                         3728   1868     15    486 2018-10-20 23:52:15 UTC+0000
.... 0xff8ff020:IEXPLORE.EXE                         1624   1868     16    508 2018-10-20 23:47:12 UTC+0000
.... 0x80e02bb8:msimn.exe                             536   1868     11    323 2018-10-20 23:47:14 UTC+0000
.... 0xff913c98:cmd.exe                               300   1868      1     32 2018-10-20 23:52:27 UTC+0000
..... 0xff9d37f0:Memoryze.exe                        1896    300      1     69 2018-10-20 23:53:02 UTC+0000
.... 0xff91e570:cmd.exe                              1080   1868      1     32 2018-10-20 23:50:43 UTC+0000
.... 0xff8fbda0:msninst.exe                          2256   1868     13    412 2018-10-20 23:47:33 UTC+0000
 0xffba7890:explorer.exe                             1608   1552      0 ------ 2018-10-20 23:45:26 UTC+0000
. 0xffb9b7e8:cmd.exe                                 1976   1608      1     32 2018-10-20 23:45:48 UTC+0000
. 0xffbb5da0:VBoxTray.exe                            1760   1608     11    132 2018-10-20 23:45:27 UTC+0000
. 0x80d5e900:ctfmon.exe                              1768   1608      1     79 2018-10-20 23:45:27 UTC+0000
```

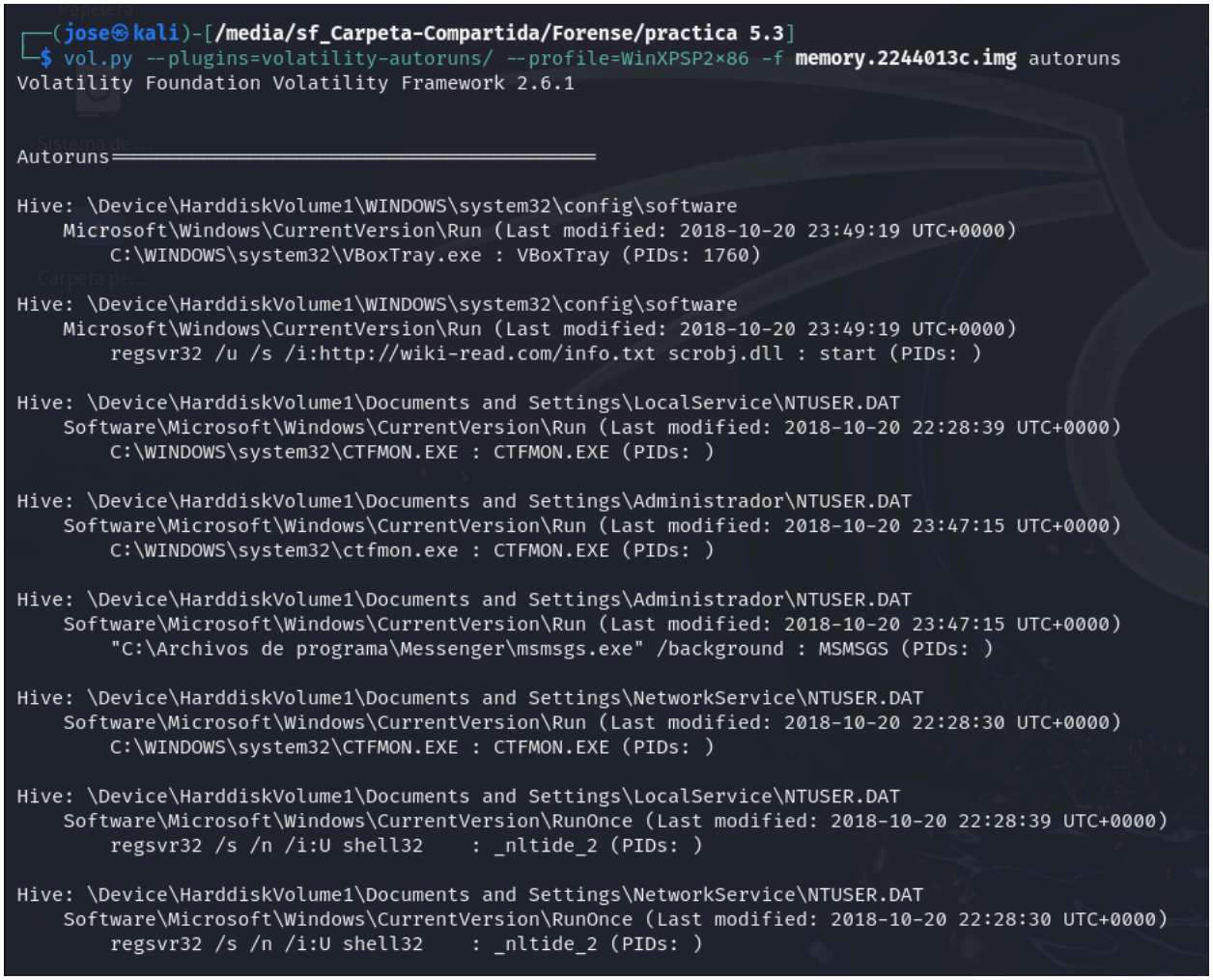
```
┌──(kali㉿kali)-[~/practica3]
└─$ vol.py -f memory.2244013c.img --profile=WinXPSP2x86 psscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------ ------------------------------
0x000000000086b020 msmsgs.exe          496    872 0x034e6000 2018-10-20 23:47:14 UTC+0000
0x0000000000bf3020 regedit.exe        2664   1868 0x04dfc000 2018-10-20 23:49:26 UTC+0000
0x000000000102b938 svchost.exe         960    660 0x07994000 2018-10-20 23:45:19 UTC+0000
0x000000000102eda0 explorer.exe       1868    616 0x0bf3b000 2018-10-20 23:46:33 UTC+0000
0x000000000103d7e8 VBoxService.exe     828    660 0x0730c000 2018-10-20 22:45:18 UTC+0000
0x00000000010487e0 csrss.exe           592    368 0x06770000 2018-10-20 22:45:18 UTC+0000
0x000000000104ada0 smss.exe            368      4 0x05a58000 2018-10-20 22:45:17 UTC+0000
0x0000000001066900 ctfmon.exe         1768   1608 0x0b2fb000 2018-10-20 23:45:27 UTC+0000
0x00000000010c67e8 services.exe        660    616 0x06ca9000 2018-10-20 22:45:18 UTC+0000
0x000000000110abb8 msimn.exe           536   1868 0x01ba3000 2018-10-20 23:47:14 UTC+0000
0x000000000011f5020 System               4      0 0x00039000
0x000000000181f020 IEXPLORE.EXE       1624   1868 0x0a7de000 2018-10-20 23:47:12 UTC+0000
0x0000000001ae9020 msmsgs.exe          496    872 0x034e6000 2018-10-20 23:47:14 UTC+0000
0x0000000004ade228 lsass.exe           672    616 0x06cb3000 2018-10-20 22:45:18 UTC+0000
0x0000000004c2da78 msiexec.exe        1968   1160 0x022f0000 2018-10-20 23:47:04 UTC+0000   2018-10-20 23:47:07 UTC+0000
0x0000000004cf7578 svchost.exe         872    660 0x07616000 2018-10-20 23:45:19 UTC+0000
0x0000000004d7dda0 VBoxTray.exe       1760   1608 0x0b1ab000 2018-10-20 23:45:27 UTC+0000
0x0000000004f0b890 explorer.exe       1608   1552 0x0a579000 2018-10-20 23:45:26 UTC+0000   2018-10-20 23:46:29 UTC+0000
0x0000000004f0c020 winlogon.exe        616    368 0x06935000 2018-10-20 22:45:18 UTC+0000
0x0000000004fd77e8 cmd.exe            1976   1608 0x02950000 2018-10-20 23:45:48 UTC+0000
0x000000000501ac20 svchost.exe        1192    660 0x08f3c000 2018-10-20 23:45:19 UTC+0000
0x0000000005230aa0 IEXPLORE.EXE       3728   1868 0x07449000 2018-10-20 23:52:15 UTC+0000
0x00000000052bca78 svchost.exe         944    660 0x0836b000 2018-10-20 23:46:29 UTC+0000
0x0000000005a41570 cmd.exe            1080   1868 0x068ff000 2018-10-20 23:50:43 UTC+0000
0x0000000007330020 cmd.exe            3468   1868 0x0808b000 2018-10-20 23:50:06 UTC+0000
0x0000000007b70790 svchost.exe        1052    660 0x07b5a000 2018-10-20 23:45:19 UTC+0000
0x0000000007d5bc10 svchost.exe        1112    660 0x07d71000 2018-10-20 23:45:19 UTC+0000
0x00000000083df020 cmd.exe            3468   1868 0x0808b000 2018-10-20 23:50:06 UTC+0000
0x000000000883ada0 msninst.exe        2256   1868 0x0535b000 2018-10-20 23:47:33 UTC+0000
0x0000000009093da0 msninst.exe        2256   1868 0x0535b000 2018-10-20 23:47:33 UTC+0000
0x00000000093f17f0 Memoryze.exe       1896    300 0x0616c000 2018-10-20 23:53:02 UTC+0000
0x00000000099a9c38 spoolsv.exe        1396    660 0x09981000 2018-10-20 23:45:19 UTC+0000
0x0000000009f19da0 msninst.exe        2256   1868 0x0535b000 2018-10-20 23:47:33 UTC+0000
0x000000000a0cb438 msiexec.exe        1160    660 0x01990000 2018-10-20 23:47:01 UTC+0000
0x000000000a409738 wscntfy.exe        1124   1052 0x02770000 2018-10-20 23:46:36 UTC+0000
0x000000000a988c98 cmd.exe             300   1868 0x082d9000 2018-10-20 23:52:27 UTC+0000
0x000000000b8deb20 alg.exe             248    660 0x01c83000 2018-10-20 23:46:34 UTC+0000
```

```
┌──(kali㉿kali)-[~/practica3]
└─$ vol.py -f memory.2244013c.img --profile=WinXPSP2x86 psxview
Volatility Foundation Volatility Framework 2.6.1
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ------ ------- -------- --------
0x01066900 ctfmon.exe             1768 True   True   False    True   True   True    True
0x07d5bc10 svchost.exe            1112 True   True   False    True   True   True    True
0x0a988c98 cmd.exe                 300 True   True   False    True   True   True    True
0x05230aa0 IEXPLORE.EXE           3728 True   True   False    True   True   True    True
0x0b8deb20 alg.exe                 248 True   True   False    True   True   True    True
0x04f0c020 winlogon.exe            616 True   True   False    True   True   True    True
0x05a41570 cmd.exe                1080 True   True   False    True   True   True    True
0x07330020 cmd.exe                3468 True   True   False    True   True   True    True
0x0501ac20 svchost.exe            1192 True   True   False    True   True   True    True
0x04ade228 lsass.exe               672 True   True   False    True   True   True    True
0x0883ada0 msninst.exe            2256 True   True   False    True   True   True    True
0x0a0cb438 msiexec.exe            1160 True   True   False    True   True   True    True
0x099a9c38 spoolsv.exe            1396 True   True   False    True   True   True    True
0x0102eda0 explorer.exe           1868 True   True   False    True   True   True    True
0x0181f020 IEXPLORE.EXE           1624 True   True   False    True   True   True    True
0x00bf3020 regedit.exe            2664 True   True   False    True   True   True    True
0x0a409738 wscntfy.exe            1124 True   True   False    True   True   True    True
0x04cf7578 svchost.exe             872 True   True   False    True   True   True    True
0x0086b020 msmsgs.exe              496 True   True   False    True   True   True    True
0x0102b938 svchost.exe             960 True   True   False    True   True   True    True
0x07b70790 svchost.exe            1052 True   True   False    True   True   True    True
0x04fd77e8 cmd.exe                1976 True   True   False    True   True   True    True
0x093f17f0 Memoryze.exe           1896 True   True   False    True   True   True    True
0x010c67e8 services.exe            660 True   True   False    True   True   True    True
0x0110abb8 msimn.exe               536 True   True   False    True   True   True    True
0x0103d7e8 VBoxService.exe         828 True   True   False    True   True   True    True
0x04d7dda0 VBoxTray.exe           1760 True   True   False    True   True   True    True
0x052bca78 svchost.exe             944 True   True   False    True   True   True    True
0x011f5020 System                    4 True   True   False    True   False False   False
0x0104ada0 smss.exe                368 True   True   False    True   False False   False
0x010487e0 csrss.exe               592 True   True   False    True   False True    True
0x04f0b890 explorer.exe           1608 True   True   False    True   False False   False    2018-10-20 23:46:29 UTC+0000
0x04c2da78 msiexec.exe            1968 True   True   False    True   False False   False    2018-10-20 23:47:07 UTC+0000
0x01ae9020 msmsgs.exe              496 False  True   False    False  False False   False
0x09093da0 msninst.exe            2256 False  True   False    False  False False   False
0x083df020 cmd.exe                3468 False  True   False    False  False False   False
0x09f19da0 msninst.exe            2256 False  True   False    False  False False   False
```

El siguiente paso consistirá en analizar la red utilizando el parámetro 'sockets'.

```
┌──(kali㉿kali)-[~/practica3]
└─$ vol.py -f memory.2244013c.img --profile=WinXPSP2x86 sockets
Volatility Foundation Volatility Framework 2.6.1
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ ------------ --------------- ---------------
0x80efe618         4    138     17 UDP          169.254.240.50  2018-10-20 23:46:20 UTC+0000
0xff93b508         4      0     47 GRE          0.0.0.0         2018-10-20 23:46:35 UTC+0000
0x80da0b98       672    500     17 UDP          0.0.0.0         2018-10-20 23:46:29 UTC+0000
0x80e3f2c8      1052   1025     17 UDP          127.0.0.1       2018-10-20 23:46:29 UTC+0000
0x80e44cb0      1052    123     17 UDP          169.254.240.50  2018-10-20 23:46:34 UTC+0000
0xff8b0430      2256   1033     17 UDP          127.0.0.1       2018-10-20 23:47:34 UTC+0000
0xffbb6e98         4    445      6 TCP          0.0.0.0         2018-10-20 22:45:17 UTC+0000
0xffb6fe98       960    135      6 TCP          0.0.0.0         2018-10-20 23:45:19 UTC+0000
0xff939360         4   1027      6 TCP          0.0.0.0         2018-10-20 23:46:35 UTC+0000
0x80df97e8       672      0    255 Reserved     0.0.0.0         2018-10-20 23:46:29 UTC+0000
0xff960320      1052    123     17 UDP          127.0.0.1       2018-10-20 23:46:34 UTC+0000
0xff93ea18      1192   1900     17 UDP          169.254.240.50  2018-10-20 23:46:35 UTC+0000
0xffbcfa78         4    139      6 TCP          169.254.240.50  2018-10-20 23:46:20 UTC+0000
0x80d3f748      1624   1031     17 UDP          127.0.0.1       2018-10-20 23:47:13 UTC+0000
0x80d806a8      1052     68     17 UDP          0.0.0.0         2018-10-20 23:52:45 UTC+0000
0xff949878       248   1026      6 TCP          127.0.0.1       2018-10-20 23:46:34 UTC+0000
0xff83d9d0      3728   1035     17 UDP          127.0.0.1       2018-10-20 23:52:15 UTC+0000
0xffb91e98         4    137     17 UDP          169.254.240.50  2018-10-20 23:46:20 UTC+0000
0xff93eca0      1192   1900     17 UDP          127.0.0.1       2018-10-20 23:46:35 UTC+0000
0xff9b8d70       672   4500     17 UDP          0.0.0.0         2018-10-20 23:46:29 UTC+0000
0xffb7cd00         4    445     17 UDP          0.0.0.0         2018-10-20 22:45:17 UTC+0000
```

Dado que se trata de un virus persistente, es fundamental verificar los procesos que se ejecutan al inicio del sistema. Mediante el uso del plugin de autoruns, podemos identificar si se está empleando '**regsvr32**'. Este proceso permite la descarga y ejecución de librerías y scripts de forma remota, eludiendo otros controles de seguridad. El dominio dañino asociado es '**http:/wiki-read.com/info.txt**'.



Al profundizar en la investigación, identificamos dos procesos asociados al navegador Internet Explorer. Utilizando el parámetro **'iehistory'**, podemos examinar el historial de navegación del usuario. Dentro de este historial, se encuentran algunas URLs sospechosas, caracterizadas por elementos inusuales como "**msni://**" y "**/xgi_regine.htm**"

```
┌──(jose㉿kali)-[/media/sf_Carpeta-Compartida/Forense/practica 5.3]
└─$ vol.py --plugins=volatility-autoruns/ --profile=WinXPSP2x86 -f memory.2244013c.img iehistory
Volatility Foundation Volatility Framework 2.6.1
**************************************************
Process: 1868 explorer.exe
Cache type "URL " at 0x2005000
Record length: 0x100
Location: Visited: Administrador@msni://install.mar@/xgl_engine.htm
Last modified: 2018-10-20 23:47:33 UTC+0000
Last accessed: 2018-10-20 23:47:33 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa4
**************************************************
Process: 1868 explorer.exe
Cache type "URL " at 0x2005100
Record length: 0x100
Location: Visited: Administrador@res://ieframe.dll/tabswelcome.htm
Last modified: 2018-10-20 23:47:36 UTC+0000
Last accessed: 2018-10-20 23:47:36 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa4
**************************************************
Process: 1868 explorer.exe
Cache type "URL " at 0x2005200
Record length: 0x100
Location: Visited: Administrador@res://ieframe.dll/tabswelcome.htm
Last modified: 2018-10-20 23:52:21 UTC+0000
Last accessed: 2018-10-20 23:52:21 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa4
**************************************************
Process: 2256 msninst.exe
Cache type "URL " at 0x10d5000
Record length: 0x100
Location: Visited: Administrador@msni://install.mar@/xgl_engine.htm
Last modified: 2018-10-20 23:47:33 UTC+0000
Last accessed: 2018-10-20 23:47:33 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0xa4
**************************************************
Process: 2256 msninst.exe
Cache type "URL " at 0x10d5100
Record length: 0x100
Location: Visited: Administrador@res://ieframe.dll/tabswelcome.htm
```

Es posible que el usuario haya descargado un archivo infectado. Al analizar el proceso del navegador identificado como **1624** utilizando el parámetro '**procdump**', podemos extraer una copia de la memoria del proceso para posteriormente enviarla a VirusTotal, un servicio de escaneo antivirus en línea, con el fin de identificar posibles amenazas.

```
┌──(jose㉿kali)-[/media/sf_Carpeta-Compartida/Forense/practica 5.3]
└─$ vol.py -f memory.2244013c.img --profile=WinXPSP2×86 procdump -p 1624 --dump-dir .
Volatility Foundation Volatility Framework 2.6.1
Process(V) ImageBase  Name                 Result
────────── ────────── ──────────────────── ──────
0×ff8ff020 0×00400000 IEXPLORE.EXE         OK: executable.1624.exe
```

Este análisis nos detecta que tenemos un troyano en el proceso 1624