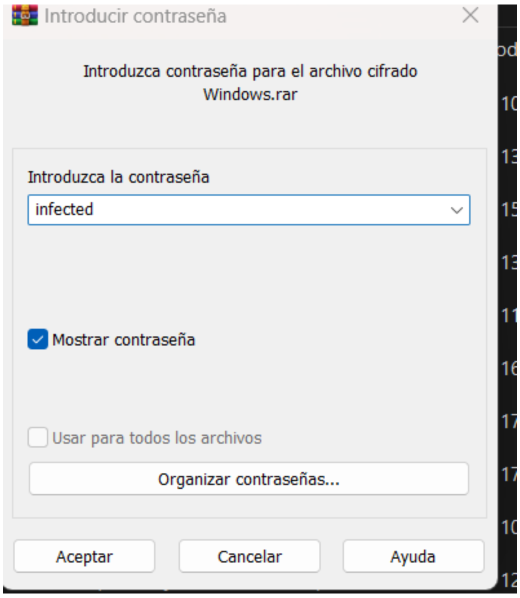
EJERCICIOS ANÁLISIS DE MEMORIA

Prerrequisitos

- Kali Linux
- Windows.rar > Password: infected > windows.vmem

Ejercicio - Volatility

Para esto descargamos el archivo.rar y lo descomprimimos, una vez hecho esto lo mandamos a la kali



Introducir contraseña

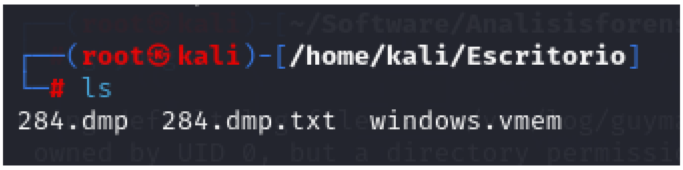
Introduzca contraseña para el archivo cifrado
Windows.rar

Introduzca la contraseña: infected

☑ Mostrar contraseña

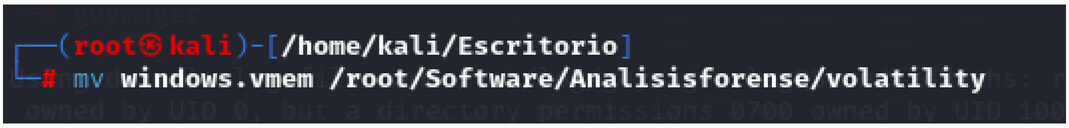
☐ Usar para todos los archivos

Dejamos el archivo en el escritorio



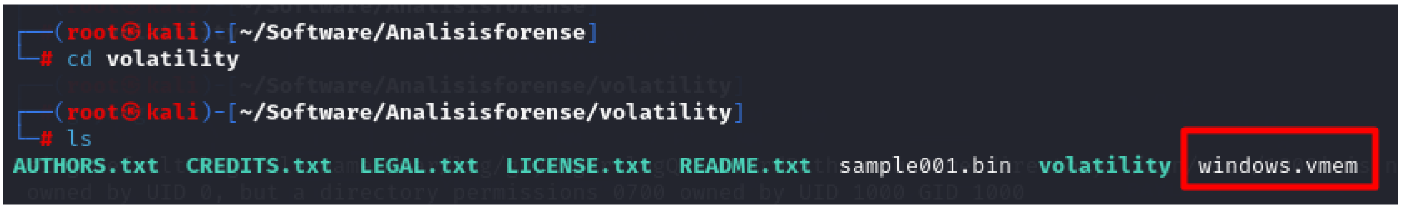
```
┌──(root㉿kali)-[/home/kali/Escritorio]
└─# ls
284.dmp  284.dmp.txt  windows.vmem
```

Y lo movemos a la carpeta de volatility para que sea más sencillo utilizarlo



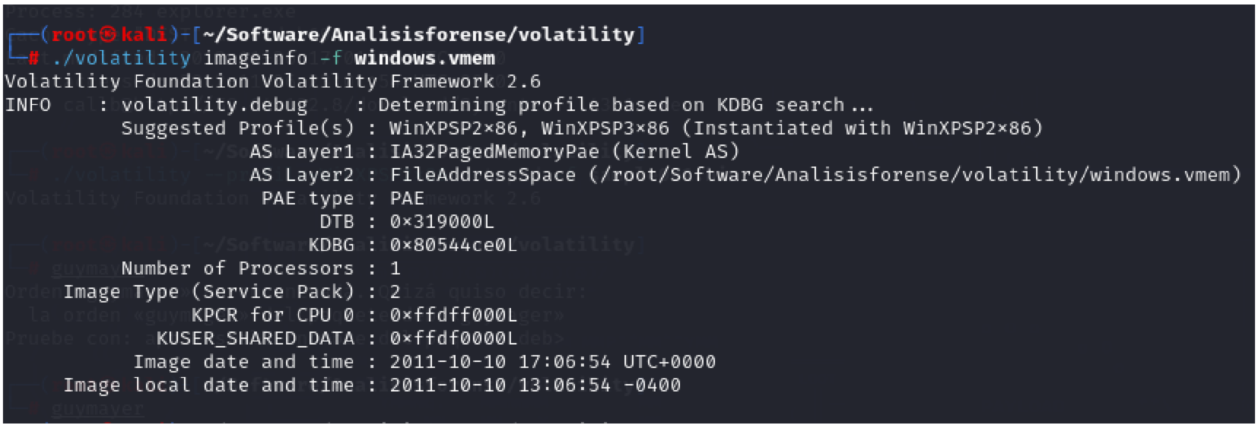
```
┌──(root㉿kali)-[/home/kali/Escritorio]
└─# mv windows.vmem /root/Software/Analisisforense/volatility
```

Habiendo realizado todo esto podemos empezar a listar los distintos valores que se nos piden



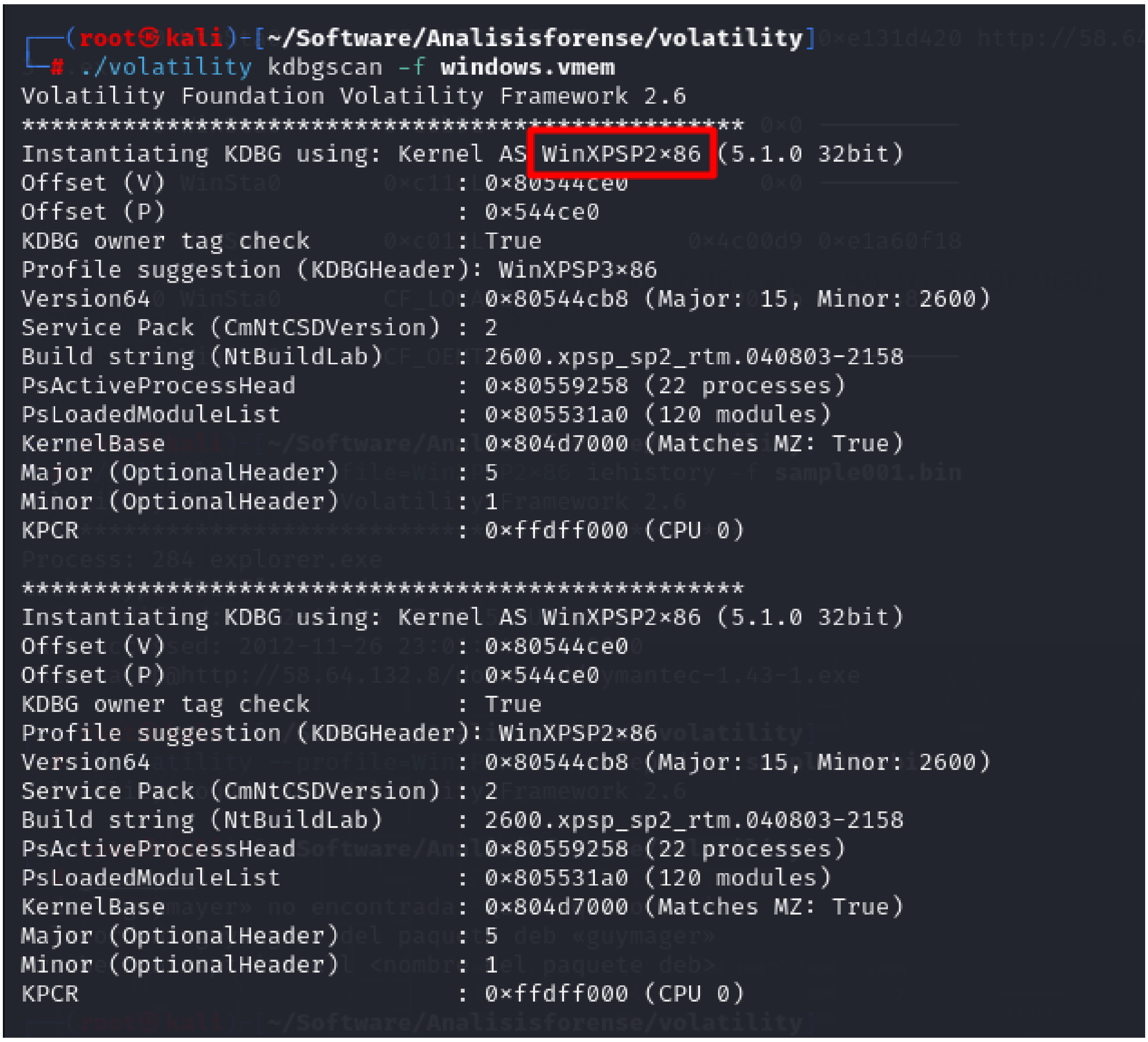
```
┌──(root㉿kali)-[~/Software/Analisisforense]
└─# cd volatility

┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ls
AUTHORS.txt  CREDITS.txt  LEGAL.txt  LICENSE.txt  README.txt  sample001.bin  volatility  windows.vmem
```

- El sistema operativo del que se realizó el volcado de la memoria proporcionado estaba infectado con malware. Realiza una investigación extrayendo la siguiente información:
    - El perfil recomendado para el análisis.



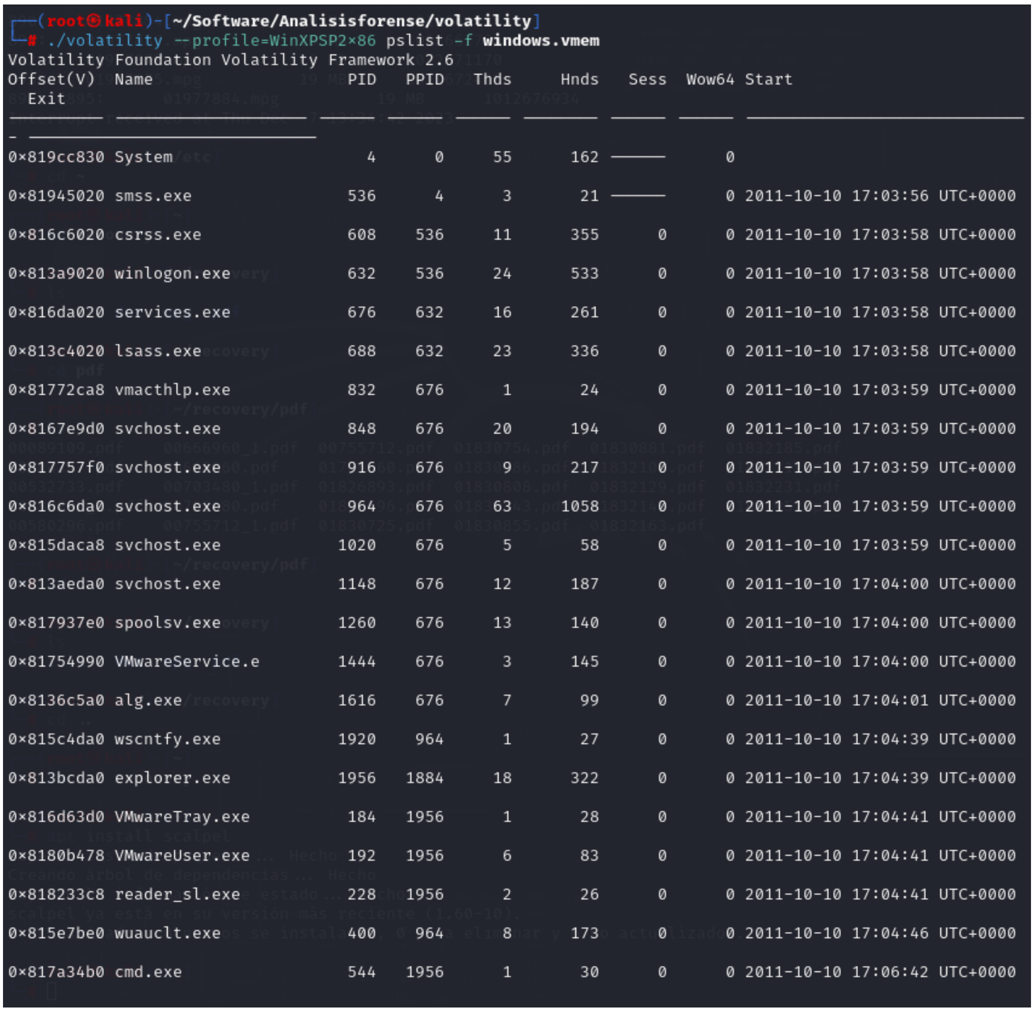
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility imageinfo -f windows.vmem
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Software/Analisisforense/volatility/windows.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2011-10-10 17:06:54 UTC+0000
     Image local date and time : 2011-10-10 13:06:54 -0400
```

- El detalle de los perfiles extraídos anteriormente.



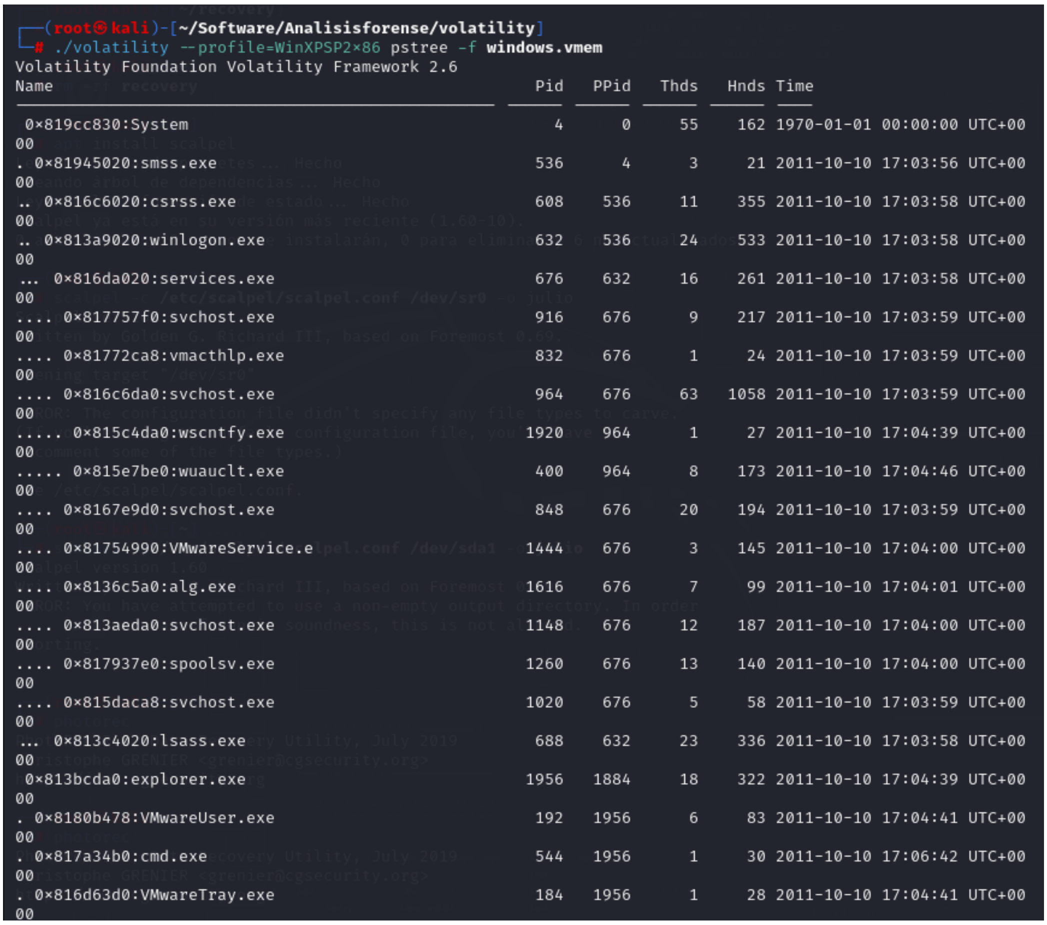
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility kdbgscan -f windows.vmem
Volatility Foundation Volatility Framework 2.6
**************************************************
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V)                    : 0x80544ce0
Offset (P)                    : 0x544ce0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP3x86
Version64                     : 0x80544cb8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 2
Build string (NtBuildLab)     : 2600.xpsp_sp2_rtm.040803-2158
PsActiveProcessHead           : 0x80559258 (22 processes)
PsLoadedModuleList            : 0x805531a0 (120 modules)
KernelBase                    : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)

**************************************************
Instantiating KDBG using: Kernel AS WinXPSP2x86 (5.1.0 32bit)
Offset (V)                    : 0x80544ce0
Offset (P)                    : 0x544ce0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): WinXPSP2x86
Version64                     : 0x80544cb8 (Major: 15, Minor: 2600)
Service Pack (CmNtCSDVersion) : 2
Build string (NtBuildLab)     : 2600.xpsp_sp2_rtm.040803-2158
PsActiveProcessHead           : 0x80559258 (22 processes)
PsLoadedModuleList            : 0x805531a0 (120 modules)
KernelBase                    : 0x804d7000 (Matches MZ: True)
Major (OptionalHeader)        : 5
Minor (OptionalHeader)        : 1
KPCR                          : 0xffdff000 (CPU 0)
```

- Un listado de los procesos con el fin de encontrar aquel/aquellos que pueda/n ser sospechoso/s.



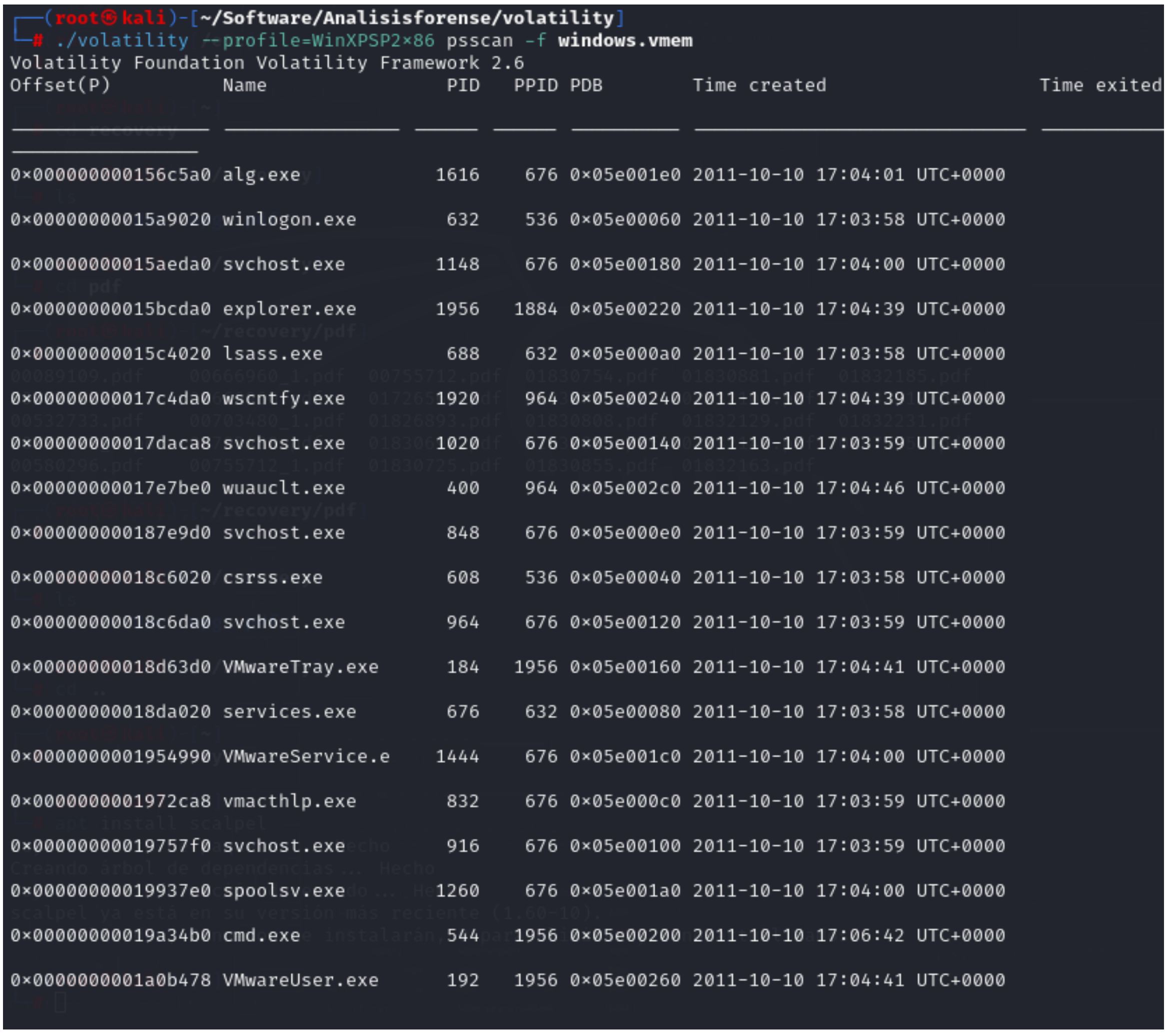
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2×86 pslist -f windows.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start
  Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------
- ------------------------------
0×819cc830 System                    4      0     55      162 ------      0

0×81945020 smss.exe                536      4      3       21 ------      0 2011-10-10 17:03:56 UTC+0000

0×816c6020 csrss.exe               608    536     11      355      0      0 2011-10-10 17:03:58 UTC+0000

0×813a9020 winlogon.exe            632    536     24      533      0      0 2011-10-10 17:03:58 UTC+0000

0×816da020 services.exe            676    632     16      261      0      0 2011-10-10 17:03:58 UTC+0000

0×813c4020 lsass.exe               688    632     23      336      0      0 2011-10-10 17:03:58 UTC+0000

0×81772ca8 vmacthlp.exe            832    676      1       24      0      0 2011-10-10 17:03:59 UTC+0000

0×8167e9d0 svchost.exe             848    676     20      194      0      0 2011-10-10 17:03:59 UTC+0000

0×817757f0 svchost.exe             916    676      9      217      0      0 2011-10-10 17:03:59 UTC+0000

0×816c6da0 svchost.exe             964    676     63     1058      0      0 2011-10-10 17:03:59 UTC+0000

0×815daca8 svchost.exe            1020    676      5       58      0      0 2011-10-10 17:03:59 UTC+0000

0×813aeda0 svchost.exe            1148    676     12      187      0      0 2011-10-10 17:04:00 UTC+0000

0×817937e0 spoolsv.exe            1260    676     13      140      0      0 2011-10-10 17:04:00 UTC+0000

0×81754990 VMwareService.e        1444    676      3      145      0      0 2011-10-10 17:04:00 UTC+0000

0×8136c5a0 alg.exe                1616    676      7       99      0      0 2011-10-10 17:04:01 UTC+0000

0×815c4da0 wscntfy.exe            1920    964      1       27      0      0 2011-10-10 17:04:39 UTC+0000

0×813bcda0 explorer.exe           1956   1884     18      322      0      0 2011-10-10 17:04:39 UTC+0000

0×816d63d0 VMwareTray.exe          184   1956      1       28      0      0 2011-10-10 17:04:41 UTC+0000

0×8180b478 VMwareUser.exe          192   1956      6       83      0      0 2011-10-10 17:04:41 UTC+0000

0×818233c8 reader_sl.exe           228   1956      2       26      0      0 2011-10-10 17:04:41 UTC+0000

0×815e7be0 wuauclt.exe             400    964      8      173      0      0 2011-10-10 17:04:46 UTC+0000

0×817a34b0 cmd.exe                 544   1956      1       30      0      0 2011-10-10 17:06:42 UTC+0000
```

- La jerarquía de los procesos.



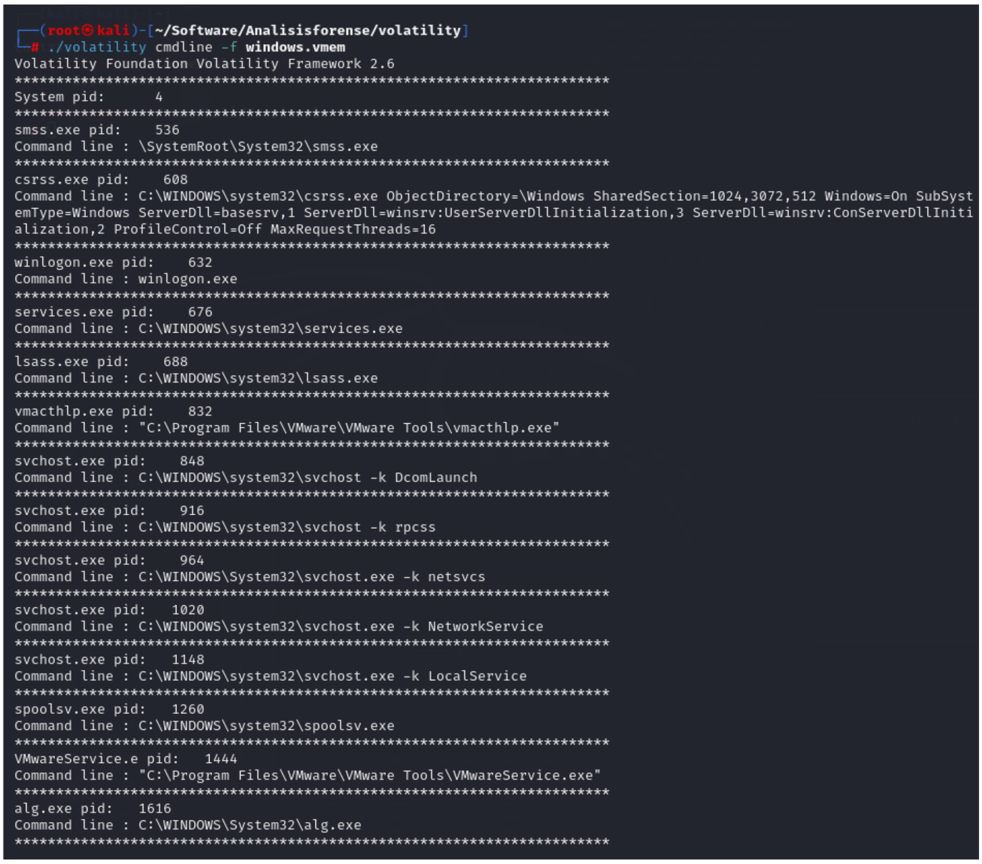
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2×86 pstree -f windows.vmem
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0×819cc830:System                                      4      0     55    162 1970-01-01 00:00:00 UTC+00
00
. 0×81945020:smss.exe                                 536      4      3     21 2011-10-10 17:03:56 UTC+00
00
.. 0×816c6020:csrss.exe                               608    536     11    355 2011-10-10 17:03:58 UTC+00
00
.. 0×813a9020:winlogon.exe                            632    536     24    533 2011-10-10 17:03:58 UTC+00
00
... 0×816da020:services.exe                           676    632     16    261 2011-10-10 17:03:58 UTC+00
00
.... 0×817757f0:svchost.exe                           916    676      9    217 2011-10-10 17:03:59 UTC+00
00
.... 0×81772ca8:vmacthlp.exe                          832    676      1     24 2011-10-10 17:03:59 UTC+00
00
.... 0×816c6da0:svchost.exe                           964    676     63   1058 2011-10-10 17:03:59 UTC+00
00
..... 0×815c4da0:wscntfy.exe                         1920    964      1     27 2011-10-10 17:04:39 UTC+00
00
..... 0×815e7be0:wuauclt.exe                          400    964      8    173 2011-10-10 17:04:46 UTC+00
00
.... 0×8167e9d0:svchost.exe                           848    676     20    194 2011-10-10 17:03:59 UTC+00
00
.... 0×81754990:VMwareService.e                      1444    676      3    145 2011-10-10 17:04:00 UTC+00
00
.... 0×8136c5a0:alg.exe                              1616    676      7     99 2011-10-10 17:04:01 UTC+00
00
.... 0×813aeda0:svchost.exe                          1148    676     12    187 2011-10-10 17:04:00 UTC+00
00
.... 0×817937e0:spoolsv.exe                          1260    676     13    140 2011-10-10 17:04:00 UTC+00
00
.... 0×815daca8:svchost.exe                          1020    676      5     58 2011-10-10 17:03:59 UTC+00
00
... 0×813c4020:lsass.exe                              688    632     23    336 2011-10-10 17:03:58 UTC+00
00
 0×813bcda0:explorer.exe                             1956   1884     18    322 2011-10-10 17:04:39 UTC+00
00
. 0×8180b478:VMwareUser.exe                           192   1956      6     83 2011-10-10 17:04:41 UTC+00
00
. 0×817a34b0:cmd.exe                                  544   1956      1     30 2011-10-10 17:06:42 UTC+00
00
. 0×816d63d0:VMwareTray.exe                           184   1956      1     28 2011-10-10 17:04:41 UTC+00
00
```

- Los posibles procesos ocultos.



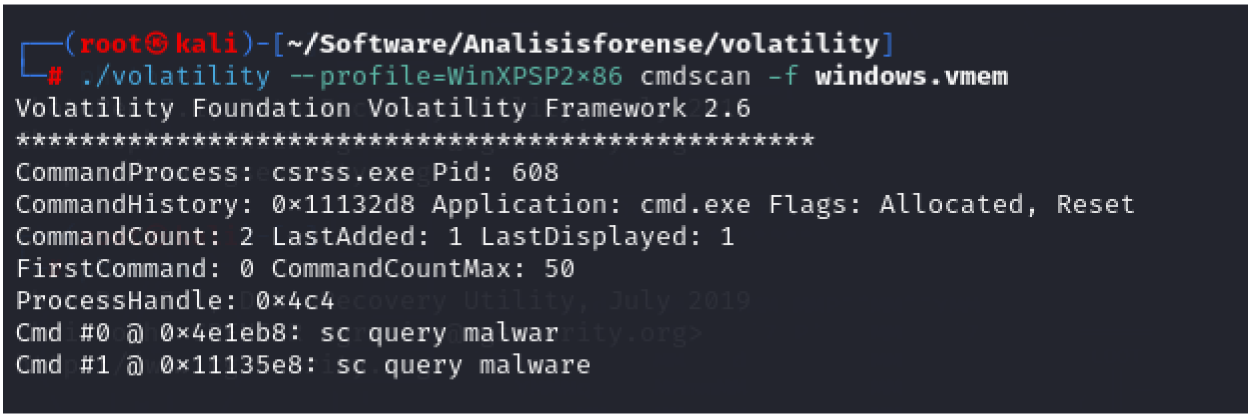
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2x86 psscan -f windows.vmem
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                PID   PPID PDB        Time created                   Time exited
------------------ ---------------- ------ ------ ---------- ------------------------------ ----------
0x000000000156c5a0 alg.exe            1616    676 0x05e001e0 2011-10-10 17:04:01 UTC+0000
0x00000000015a9020 winlogon.exe        632    536 0x05e00060 2011-10-10 17:03:58 UTC+0000
0x00000000015aeda0 svchost.exe        1148    676 0x05e00180 2011-10-10 17:04:00 UTC+0000
0x00000000015bcda0 explorer.exe       1956   1884 0x05e00220 2011-10-10 17:04:39 UTC+0000
0x00000000015c4020 lsass.exe           688    632 0x05e000a0 2011-10-10 17:03:58 UTC+0000
0x00000000017c4da0 wscntfy.exe        1920    964 0x05e00240 2011-10-10 17:04:39 UTC+0000
0x00000000017daca8 svchost.exe        1020    676 0x05e00140 2011-10-10 17:03:59 UTC+0000
0x00000000017e7be0 wuauclt.exe         400    964 0x05e002c0 2011-10-10 17:04:46 UTC+0000
0x00000000187e9d0 svchost.exe          848    676 0x05e000e0 2011-10-10 17:03:59 UTC+0000
0x00000000018c6020 csrss.exe           608    536 0x05e00040 2011-10-10 17:03:58 UTC+0000
0x00000000018c6da0 svchost.exe         964    676 0x05e00120 2011-10-10 17:03:59 UTC+0000
0x00000000018d63d0 VMwareTray.exe      184   1956 0x05e00160 2011-10-10 17:04:41 UTC+0000
0x00000000018da020 services.exe        676    632 0x05e00080 2011-10-10 17:03:58 UTC+0000
0x0000000001954990 VMwareService.e    1444    676 0x05e001c0 2011-10-10 17:04:00 UTC+0000
0x0000000001972ca8 vmacthlp.exe        832    676 0x05e000c0 2011-10-10 17:03:59 UTC+0000
0x00000000019757f0 svchost.exe         916    676 0x05e00100 2011-10-10 17:03:59 UTC+0000
0x00000000019937e0 spoolsv.exe        1260    676 0x05e001a0 2011-10-10 17:04:00 UTC+0000
0x00000000019a34b0 cmd.exe             544   1956 0x05e00200 2011-10-10 17:06:42 UTC+0000
0x0000000001a0b478 VMwareUser.exe      192   1956 0x05e00260 2011-10-10 17:04:41 UTC+0000
```

- Los procesos, su path y que comandos que se estaban ejecutando.



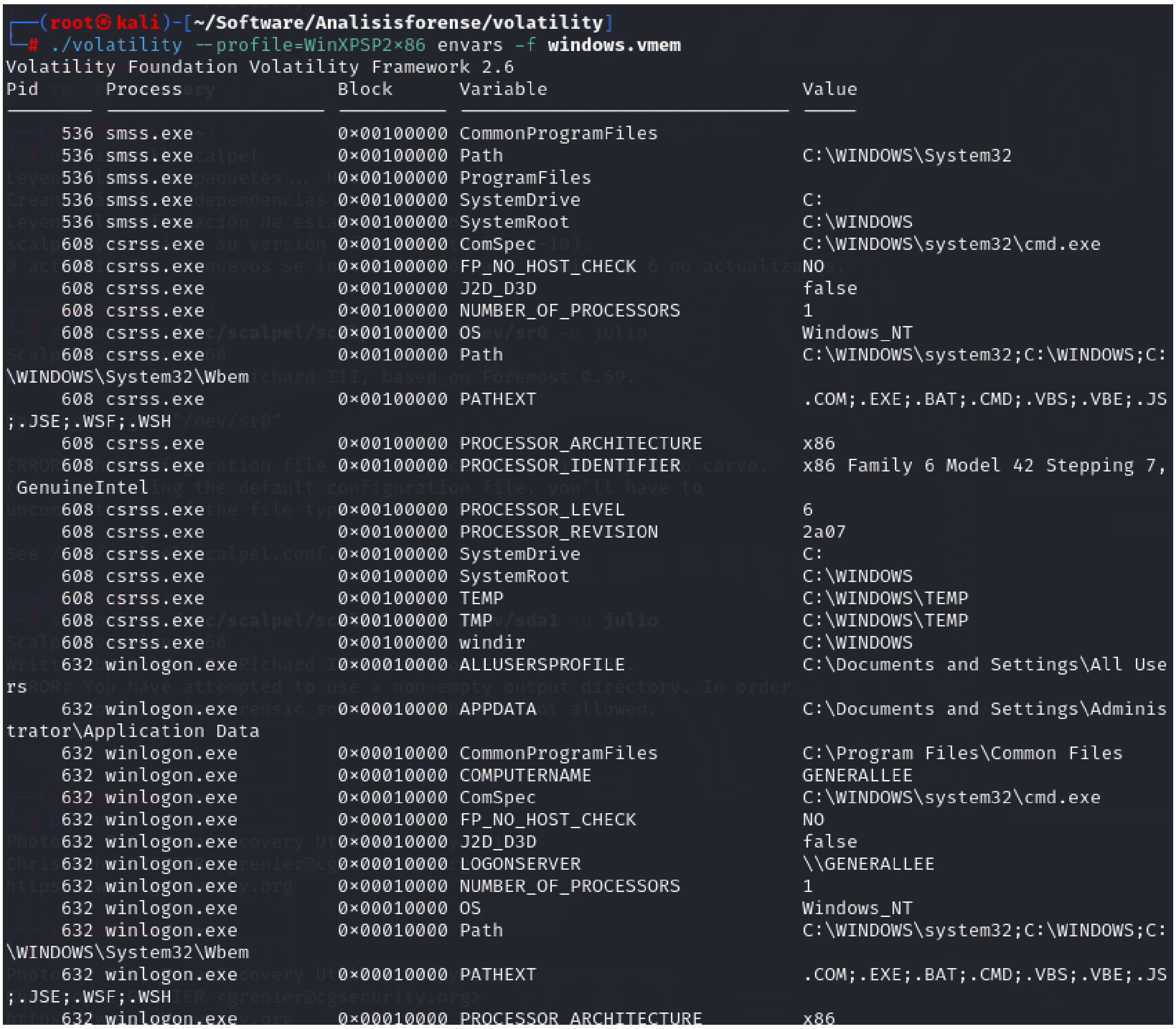
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility cmdline -f windows.vmem
Volatility Foundation Volatility Framework 2.6
************************************************************************
System pid:      4
************************************************************************
smss.exe pid:    536
Command line : \SystemRoot\System32\smss.exe
************************************************************************
csrss.exe pid:    608
Command line : C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows=On SubSyst
emType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllIniti
alization,2 ProfileControl=Off MaxRequestThreads=16
************************************************************************
winlogon.exe pid:    632
Command line : winlogon.exe
************************************************************************
services.exe pid:    676
Command line : C:\WINDOWS\system32\services.exe
************************************************************************
lsass.exe pid:    688
Command line : C:\WINDOWS\system32\lsass.exe
************************************************************************
vmacthlp.exe pid:    832
Command line : "C:\Program Files\VMware\VMware Tools\vmacthlp.exe"
************************************************************************
svchost.exe pid:    848
Command line : C:\WINDOWS\system32\svchost -k DcomLaunch
************************************************************************
svchost.exe pid:    916
Command line : C:\WINDOWS\system32\svchost -k rpcss
************************************************************************
svchost.exe pid:    964
Command line : C:\WINDOWS\System32\svchost.exe -k netsvcs
************************************************************************
svchost.exe pid:   1020
Command line : C:\WINDOWS\system32\svchost.exe -k NetworkService
************************************************************************
svchost.exe pid:   1148
Command line : C:\WINDOWS\system32\svchost.exe -k LocalService
************************************************************************
spoolsv.exe pid:   1260
Command line : C:\WINDOWS\system32\spoolsv.exe
************************************************************************
VMwareService.e pid:   1444
Command line : "C:\Program Files\VMware\VMware Tools\VMwareService.exe"
************************************************************************
alg.exe pid:   1616
Command line : C:\WINDOWS\System32\alg.exe
************************************************************************
```

- Los últimos comandos ejecutados.



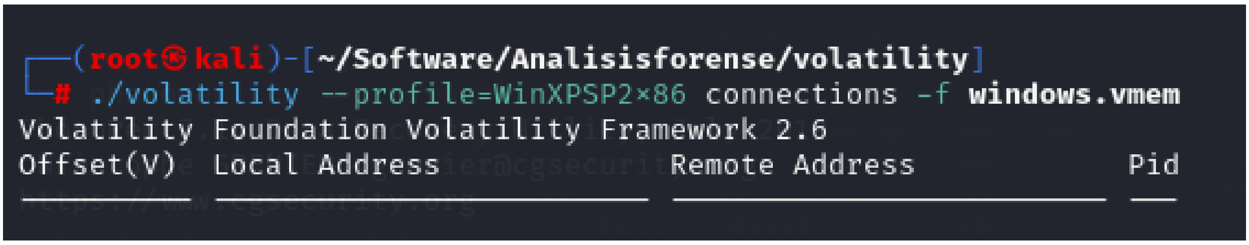
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2×86 cmdscan -f windows.vmem
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: csrss.exe Pid: 608
CommandHistory: 0×11132d8 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×4c4
Cmd #0 @ 0×4e1eb8: sc query malwar
Cmd #1 @ 0×11135e8: sc query malware
```

- Las variables de entorno del sistema.



```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2×86 envars -f windows.vmem
Volatility Foundation Volatility Framework 2.6
Pid      Process                  Block      Variable                       Value
-------- -------------------- ---------- ------------------------------ -----
     536 smss.exe             0×00100000 CommonProgramFiles
     536 smss.exe             0×00100000 Path                           C:\WINDOWS\System32
     536 smss.exe             0×00100000 ProgramFiles
     536 smss.exe             0×00100000 SystemDrive                    C:
     536 smss.exe             0×00100000 SystemRoot                     C:\WINDOWS
     608 csrss.exe            0×00100000 ComSpec                        C:\WINDOWS\system32\cmd.exe
     608 csrss.exe            0×00100000 FP_NO_HOST_CHECK               NO
     608 csrss.exe            0×00100000 J2D_D3D                        false
     608 csrss.exe            0×00100000 NUMBER_OF_PROCESSORS           1
     608 csrss.exe            0×00100000 OS                             Windows_NT
     608 csrss.exe            0×00100000 Path                           C:\WINDOWS\system32;C:\WINDOWS;C:
\WINDOWS\System32\Wbem
     608 csrss.exe            0×00100000 PATHEXT                        .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS
;.JSE;.WSF;.WSH
     608 csrss.exe            0×00100000 PROCESSOR_ARCHITECTURE         x86
     608 csrss.exe            0×00100000 PROCESSOR_IDENTIFIER           x86 Family 6 Model 42 Stepping 7,
 GenuineIntel
     608 csrss.exe            0×00100000 PROCESSOR_LEVEL                6
     608 csrss.exe            0×00100000 PROCESSOR_REVISION             2a07
     608 csrss.exe            0×00100000 SystemDrive                    C:
     608 csrss.exe            0×00100000 SystemRoot                     C:\WINDOWS
     608 csrss.exe            0×00100000 TEMP                           C:\WINDOWS\TEMP
     608 csrss.exe            0×00100000 TMP                            C:\WINDOWS\TEMP
     608 csrss.exe            0×00100000 windir                         C:\WINDOWS
     632 winlogon.exe         0×00010000 ALLUSERSPROFILE                C:\Documents and Settings\All Use
rs
     632 winlogon.exe         0×00010000 APPDATA                        C:\Documents and Settings\Adminis
trator\Application Data
     632 winlogon.exe         0×00010000 CommonProgramFiles             C:\Program Files\Common Files
     632 winlogon.exe         0×00010000 COMPUTERNAME                   GENERALLEE
     632 winlogon.exe         0×00010000 ComSpec                        C:\WINDOWS\system32\cmd.exe
     632 winlogon.exe         0×00010000 FP_NO_HOST_CHECK               NO
     632 winlogon.exe         0×00010000 J2D_D3D                        false
     632 winlogon.exe         0×00010000 LOGONSERVER                    \\GENERALLEE
     632 winlogon.exe         0×00010000 NUMBER_OF_PROCESSORS           1
     632 winlogon.exe         0×00010000 OS                             Windows_NT
     632 winlogon.exe         0×00010000 Path                           C:\WINDOWS\system32;C:\WINDOWS;C:
\WINDOWS\System32\Wbem
     632 winlogon.exe         0×00010000 PATHEXT                        .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS
;.JSE;.WSF;.WSH
     632 winlogon.exe         0×00010000 PROCESSOR_ARCHITECTURE         x86
```

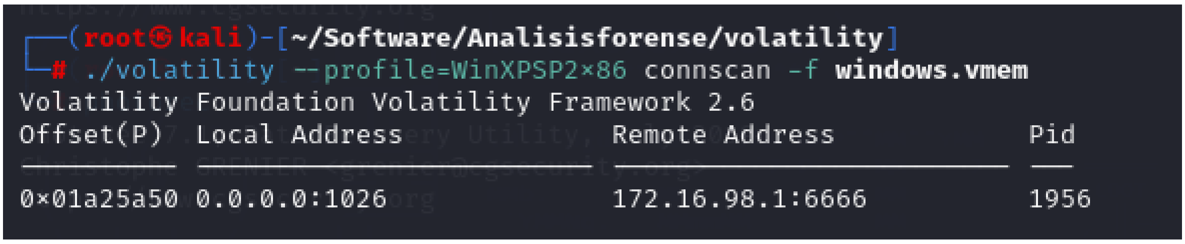
- Las conexiones del host.



```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2×86 connections -f windows.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
```

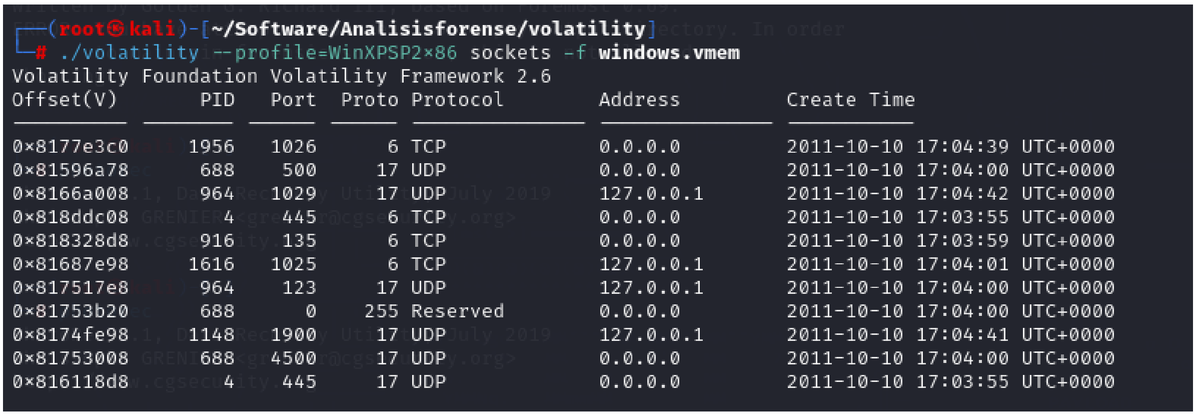
- Las posibles conexiones ocultas con IP remotas.

  En este tenemos el proceso 1956 oculto por tanto nos hace sospechar



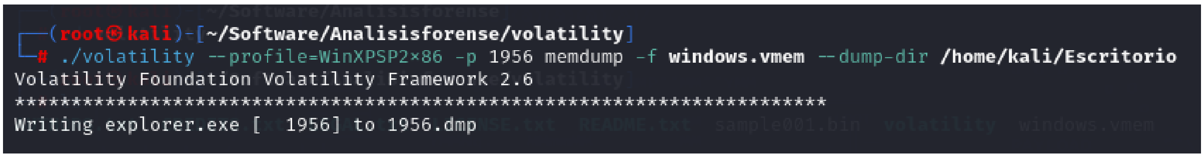
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2x86 connscan -f windows.vmem
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
────────── ───────────────────────── ───────────────────────── ───
0x01a25a50 0.0.0.0:1026              172.16.98.1:6666          1956
```

- Los sockets del host.



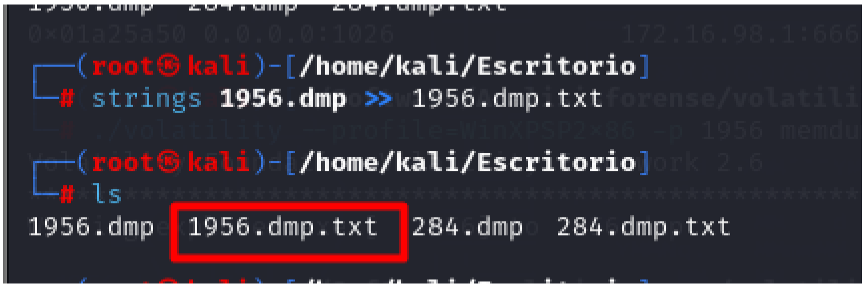
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2x86 sockets -f windows.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
────────── ──────── ────── ────── ─────────────── ─────────────── ───────────
0x8177e3c0     1956   1026      6 TCP             0.0.0.0         2011-10-10 17:04:39 UTC+0000
0x81596a78      688    500     17 UDP             0.0.0.0         2011-10-10 17:04:00 UTC+0000
0x8166a008      964   1029     17 UDP             127.0.0.1       2011-10-10 17:04:42 UTC+0000
0x818ddc08        4    445      6 TCP             0.0.0.0         2011-10-10 17:03:55 UTC+0000
0x818328d8      916    135      6 TCP             0.0.0.0         2011-10-10 17:03:59 UTC+0000
0x81687e98     1616   1025      6 TCP             127.0.0.1       2011-10-10 17:04:01 UTC+0000
0x817517e8      964    123     17 UDP             127.0.0.1       2011-10-10 17:04:00 UTC+0000
0x81753b20      688      0    255 Reserved        0.0.0.0         2011-10-10 17:04:00 UTC+0000
0x8174fe98     1148   1900     17 UDP             127.0.0.1       2011-10-10 17:04:41 UTC+0000
0x81753008      688   4500     17 UDP             0.0.0.0         2011-10-10 17:04:00 UTC+0000
0x816118d8        4    445     17 UDP             0.0.0.0         2011-10-10 17:03:55 UTC+0000
```

- Volcado/s del/de los proceso/s sospechoso/s.



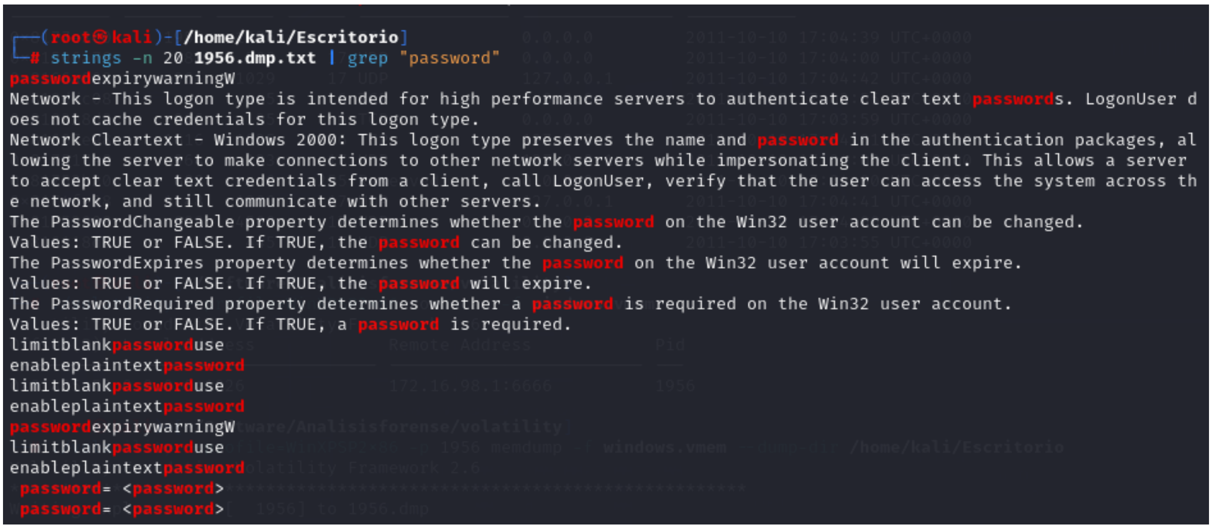
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2x86 -p 1956 memdump -f windows.vmem --dump-dir /home/kali/Escritorio
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing explorer.exe [  1956] to 1956.dmp
```

Una vez tenemos esto, nos dirigimos a la carpeta y cambiamos el formato a txt



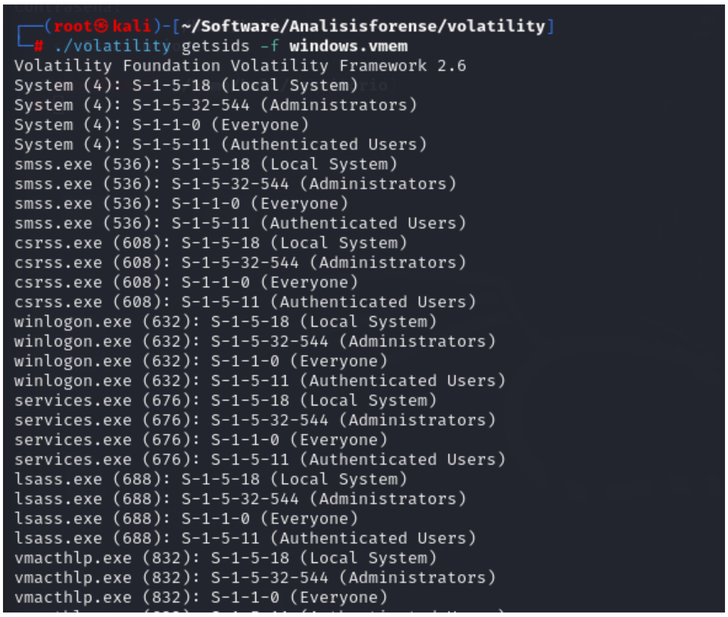
```
┌──(root㉿kali)-[/home/kali/Escritorio]
└─# strings 1956.dmp >> 1956.dmp.txt

┌──(root㉿kali)-[/home/kali/Escritorio]
└─# ls
1956.dmp  1956.dmp.txt  284.dmp  284.dmp.txt
```

- Sacar cadenas del/de los volcado/s para inspeccionarlo/s.

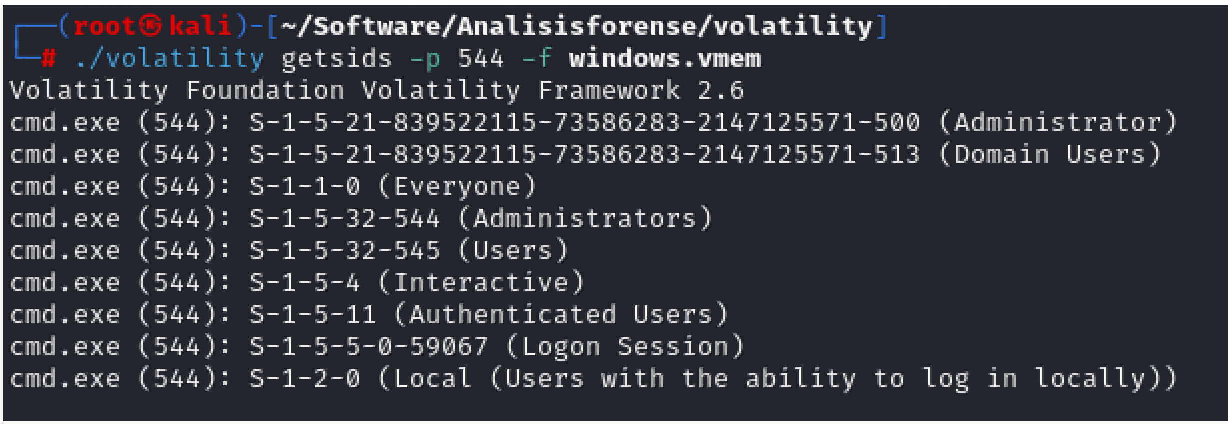


```
┌──(root㉿kali)-[/home/kali/Escritorio]
└─# strings -n 20 1956.dmp.txt | grep "password"
passwordexpirywarningW
Network - This logon type is intended for high performance servers to authenticate clear text passwords. LogonUser d
oes not cache credentials for this logon type.
Network Cleartext - Windows 2000: This logon type preserves the name and password in the authentication packages, al
lowing the server to make connections to other network servers while impersonating the client. This allows a server
to accept clear text credentials from a client, call LogonUser, verify that the user can access the system across th
e network, and still communicate with other servers.
The PasswordChangeable property determines whether the password on the Win32 user account can be changed.
Values: TRUE or FALSE. If TRUE, the password can be changed.
The PasswordExpires property determines whether the password on the Win32 user account will expire.
Values: TRUE or FALSE. If TRUE, the password will expire.
The PasswordRequired property determines whether a password is required on the Win32 user account.
Values: TRUE or FALSE. If TRUE, a password is required.
limitblankpassworduse
enableplaintextpassword
limitblankpassworduse
enableplaintextpassword
passwordexpirywarningW
limitblankpassworduse
enableplaintextpassword
 password= <password>
 password= <password>
```

- Los identificadores de sesión.

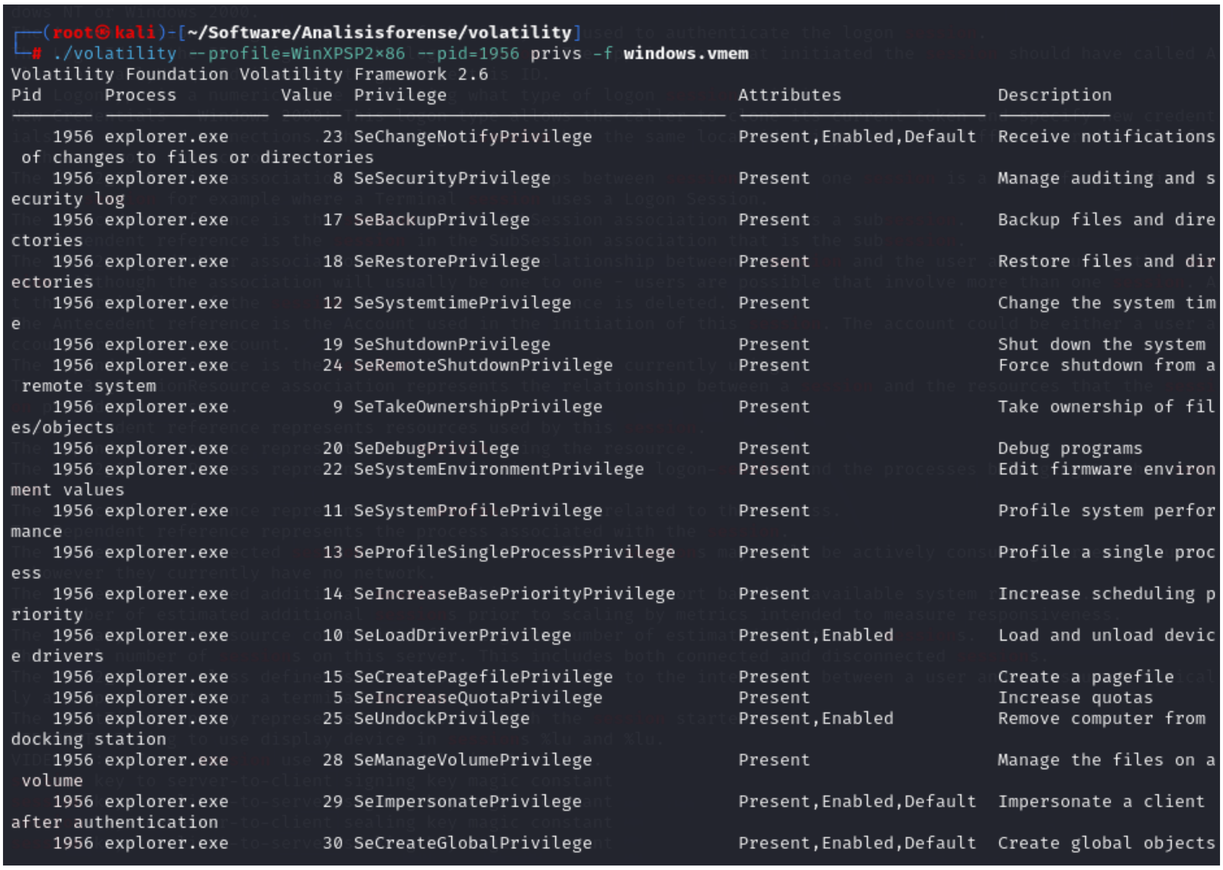


```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility getsids -f windows.vmem
Volatility Foundation Volatility Framework 2.6
System (4): S-1-5-18 (Local System)
System (4): S-1-5-32-544 (Administrators)
System (4): S-1-1-0 (Everyone)
System (4): S-1-5-11 (Authenticated Users)
smss.exe (536): S-1-5-18 (Local System)
smss.exe (536): S-1-5-32-544 (Administrators)
smss.exe (536): S-1-1-0 (Everyone)
smss.exe (536): S-1-5-11 (Authenticated Users)
csrss.exe (608): S-1-5-18 (Local System)
csrss.exe (608): S-1-5-32-544 (Administrators)
csrss.exe (608): S-1-1-0 (Everyone)
csrss.exe (608): S-1-5-11 (Authenticated Users)
winlogon.exe (632): S-1-5-18 (Local System)
winlogon.exe (632): S-1-5-32-544 (Administrators)
winlogon.exe (632): S-1-1-0 (Everyone)
winlogon.exe (632): S-1-5-11 (Authenticated Users)
services.exe (676): S-1-5-18 (Local System)
services.exe (676): S-1-5-32-544 (Administrators)
services.exe (676): S-1-1-0 (Everyone)
services.exe (676): S-1-5-11 (Authenticated Users)
lsass.exe (688): S-1-5-18 (Local System)
lsass.exe (688): S-1-5-32-544 (Administrators)
lsass.exe (688): S-1-1-0 (Everyone)
lsass.exe (688): S-1-5-11 (Authenticated Users)
vmacthlp.exe (832): S-1-5-18 (Local System)
vmacthlp.exe (832): S-1-5-32-544 (Administrators)
vmacthlp.exe (832): S-1-1-0 (Everyone)
```



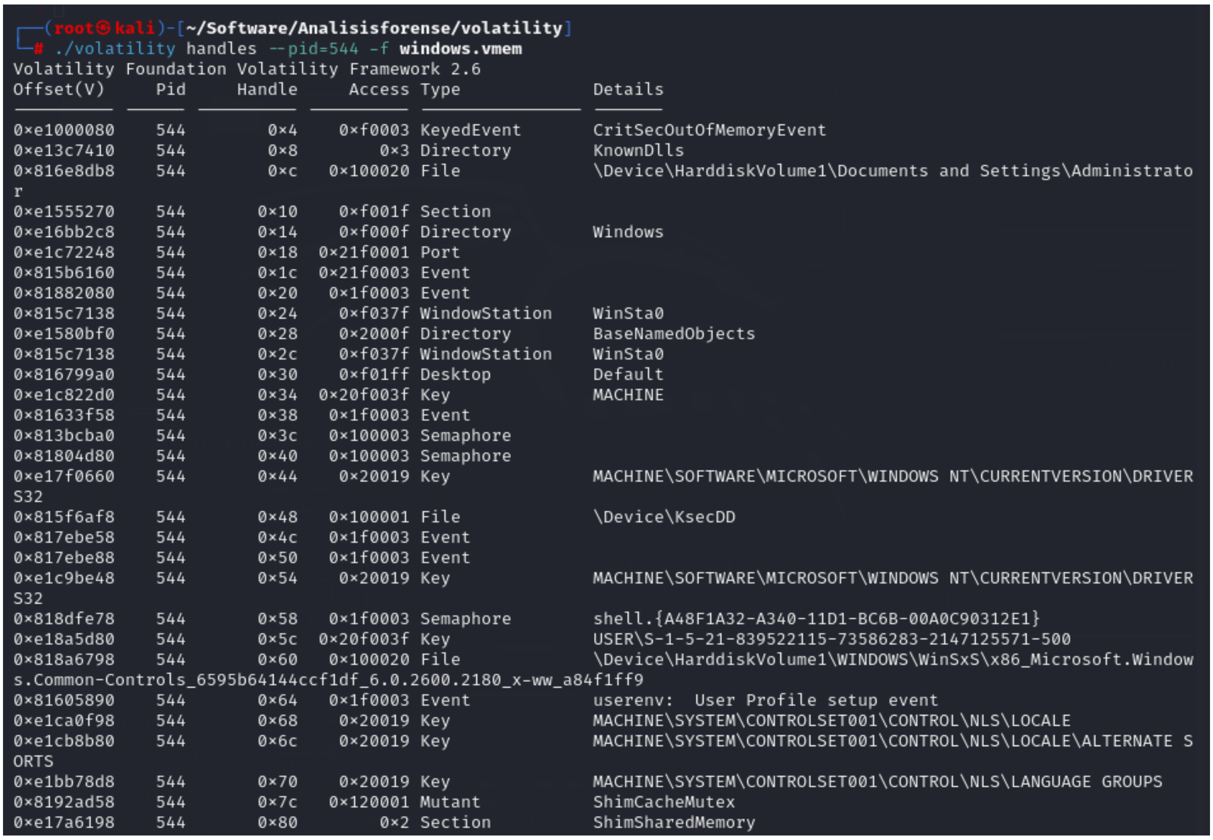
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility getsids -p 544 -f windows.vmem
Volatility Foundation Volatility Framework 2.6
cmd.exe (544): S-1-5-21-839522115-73586283-2147125571-500 (Administrator)
cmd.exe (544): S-1-5-21-839522115-73586283-2147125571-513 (Domain Users)
cmd.exe (544): S-1-1-0 (Everyone)
cmd.exe (544): S-1-5-32-544 (Administrators)
cmd.exe (544): S-1-5-32-545 (Users)
cmd.exe (544): S-1-5-4 (Interactive)
cmd.exe (544): S-1-5-11 (Authenticated Users)
cmd.exe (544): S-1-5-5-0-59067 (Logon Session)
cmd.exe (544): S-1-2-0 (Local (Users with the ability to log in locally))
```

- ○ Los privilegios con los que se ejecuta/n el/los proceso/s sospechoso/s.



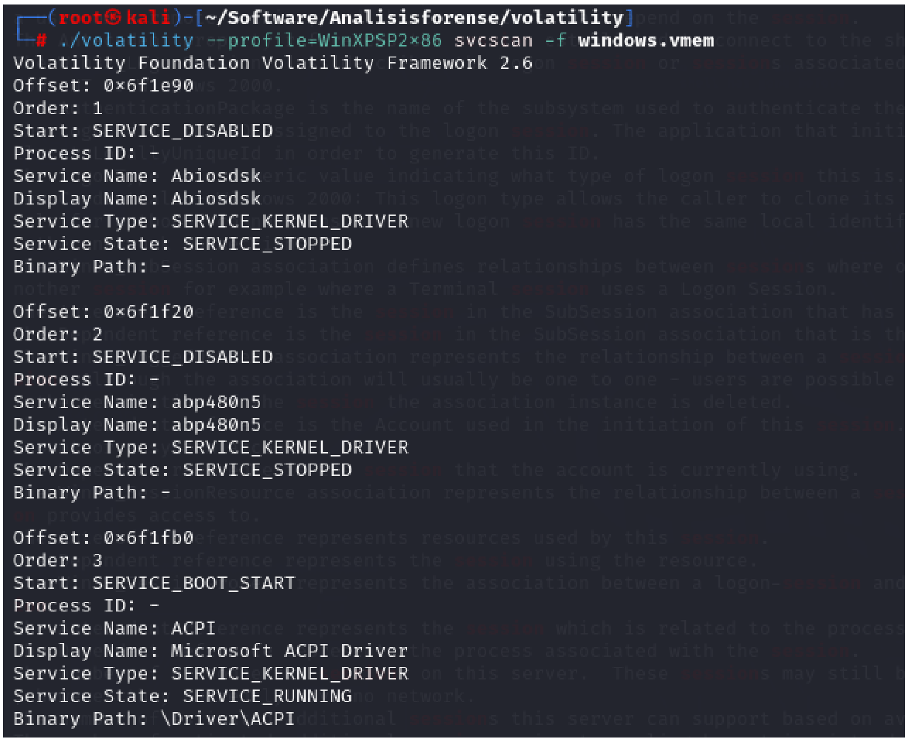
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2x86 --pid=1956 privs -f windows.vmem
Volatility Foundation Volatility Framework 2.6
Pid      Process          Value  Privilege                            Attributes               Description
-------- ---------------- ------ ------------------------------------ ------------------------ -----------
    1956 explorer.exe         23 SeChangeNotifyPrivilege              Present,Enabled,Default  Receive notifications
 of changes to files or directories
    1956 explorer.exe          8 SeSecurityPrivilege                  Present                  Manage auditing and s
ecurity log
    1956 explorer.exe         17 SeBackupPrivilege                    Present                  Backup files and dire
ctories
    1956 explorer.exe         18 SeRestorePrivilege                   Present                  Restore files and dir
ectories
    1956 explorer.exe         12 SeSystemtimePrivilege                Present                  Change the system tim
e
    1956 explorer.exe         19 SeShutdownPrivilege                  Present                  Shut down the system
    1956 explorer.exe         24 SeRemoteShutdownPrivilege            Present                  Force shutdown from a
 remote system
    1956 explorer.exe          9 SeTakeOwnershipPrivilege             Present                  Take ownership of fil
es/objects
    1956 explorer.exe         20 SeDebugPrivilege                     Present                  Debug programs
    1956 explorer.exe         22 SeSystemEnvironmentPrivilege         Present                  Edit firmware environ
ment values
    1956 explorer.exe         11 SeSystemProfilePrivilege             Present                  Profile system perfor
mance
    1956 explorer.exe         13 SeProfileSingleProcessPrivilege      Present                  Profile a single proc
ess
    1956 explorer.exe         14 SeIncreaseBasePriorityPrivilege      Present                  Increase scheduling p
riority
    1956 explorer.exe         10 SeLoadDriverPrivilege                Present,Enabled          Load and unload devic
e drivers
    1956 explorer.exe         15 SeCreatePagefilePrivilege            Present                  Create a pagefile
    1956 explorer.exe          5 SeIncreaseQuotaPrivilege             Present                  Increase quotas
    1956 explorer.exe         25 SeUndockPrivilege                    Present,Enabled          Remove computer from
docking station
    1956 explorer.exe         28 SeManageVolumePrivilege              Present                  Manage the files on a
 volume
    1956 explorer.exe         29 SeImpersonatePrivilege               Present,Enabled,Default  Impersonate a client
after authentication
    1956 explorer.exe         30 SeCreateGlobalPrivilege              Present,Enabled,Default  Create global objects
```

- Tipo de accesos que tiene/n el/los proceso/s sospechoso/s.



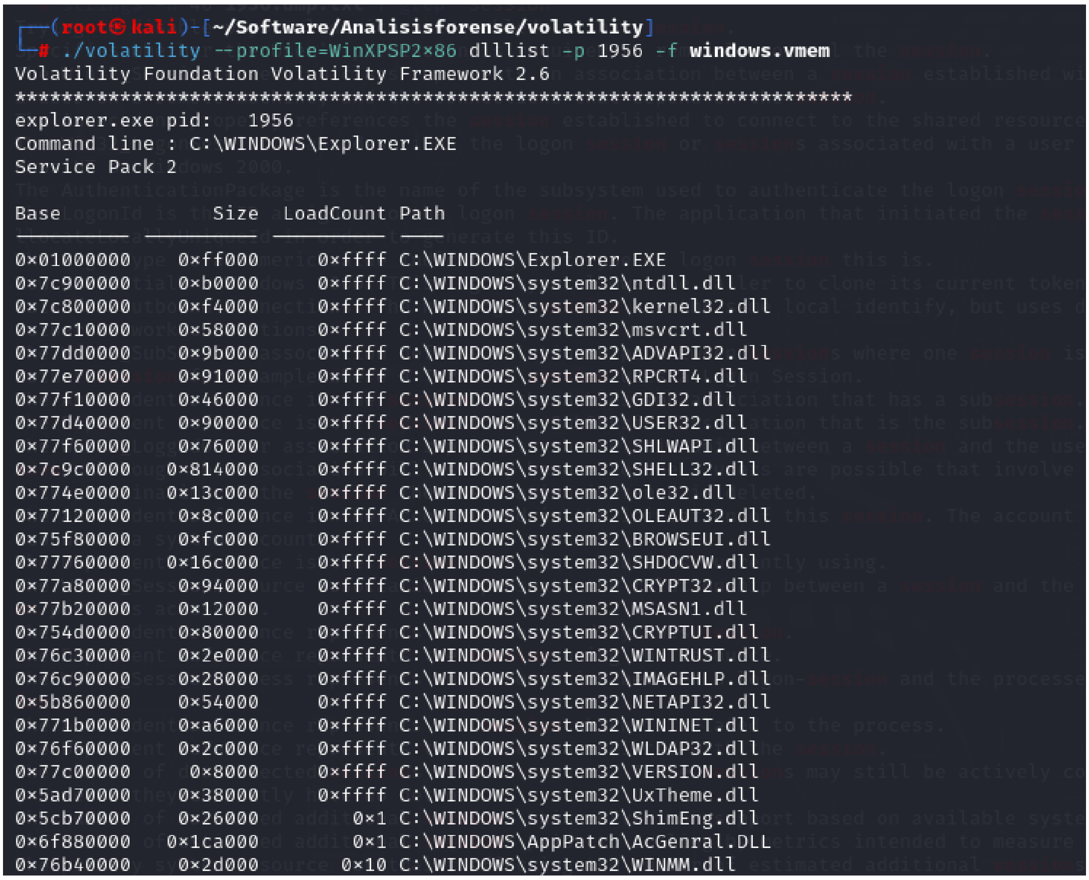
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility handles --pid=544 -f windows.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V)     Pid     Handle     Access Type             Details
──────────  ──────  ──────────  ────────── ──────────────  ───────
0xe1000080    544        0x4    0xf0003 KeyedEvent       CritSecOutOfMemoryEvent
0xe13c7410    544        0x8        0x3 Directory        KnownDlls
0x816e8db8    544        0xc   0x100020 File             \Device\HarddiskVolume1\Documents and Settings\Administrato
r
0xe1555270    544       0x10    0xf001f Section
0xe16bb2c8    544       0x14    0xf000f Directory        Windows
0xe1c72248    544       0x18  0x21f0001 Port
0x815b6160    544       0x1c  0x21f0003 Event
0x81882080    544       0x20   0x1f0003 Event
0x815c7138    544       0x24    0xf037f WindowStation    WinSta0
0xe1580bf0    544       0x28    0x2000f Directory        BaseNamedObjects
0x815c7138    544       0x2c    0xf037f WindowStation    WinSta0
0x816799a0    544       0x30    0xf01ff Desktop          Default
0xe1c822d0    544       0x34  0x20f003f Key              MACHINE
0x81633f58    544       0x38   0x1f0003 Event
0x813bcba0    544       0x3c   0x100003 Semaphore
0x81804d80    544       0x40   0x100003 Semaphore
0xe17f0660    544       0x44    0x20019 Key              MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\DRIVER
S32
0x815f6af8    544       0x48   0x100001 File             \Device\KsecDD
0x817ebe58    544       0x4c   0x1f0003 Event
0x817ebe88    544       0x50   0x1f0003 Event
0xe1c9be48    544       0x54    0x20019 Key              MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\DRIVER
S32
0x818dfe78    544       0x58   0x1f0003 Semaphore        shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
0xe18a5d80    544       0x5c  0x20f003f Key              USER\S-1-5-21-839522115-73586283-2147125571-500
0x818a6798    544       0x60   0x100020 File             \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Window
s.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9
0x81605890    544       0x64   0x1f0003 Event            userenv:  User Profile setup event
0xe1ca0f98    544       0x68    0x20019 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE
0xe1cb8b80    544       0x6c    0x20019 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE\ALTERNATE S
ORTS
0xe1bb78d8    544       0x70    0x20019 Key              MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LANGUAGE GROUPS
0x8192ad58    544       0x7c   0x120001 Mutant           ShimCacheMutex
0xe17a6198    544       0x80        0x2 Section          ShimSharedMemory
```

- El listado de servicios e inspeccionar concretamente aquel/aquellos que sean sospechoso/s.



```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2x86 svcscan -f windows.vmem
Volatility Foundation Volatility Framework 2.6
Offset: 0x6f1e90
Order: 1
Start: SERVICE_DISABLED
Process ID: -
Service Name: Abiosdsk
Display Name: Abiosdsk
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6f1f20
Order: 2
Start: SERVICE_DISABLED
Process ID: -
Service Name: abp480n5
Display Name: abp480n5
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_STOPPED
Binary Path: -

Offset: 0x6f1fb0
Order: 3
Start: SERVICE_BOOT_START
Process ID: -
Service Name: ACPI
Display Name: Microsoft ACPI Driver
Service Type: SERVICE_KERNEL_DRIVER
Service State: SERVICE_RUNNING
Binary Path: \Driver\ACPI
```

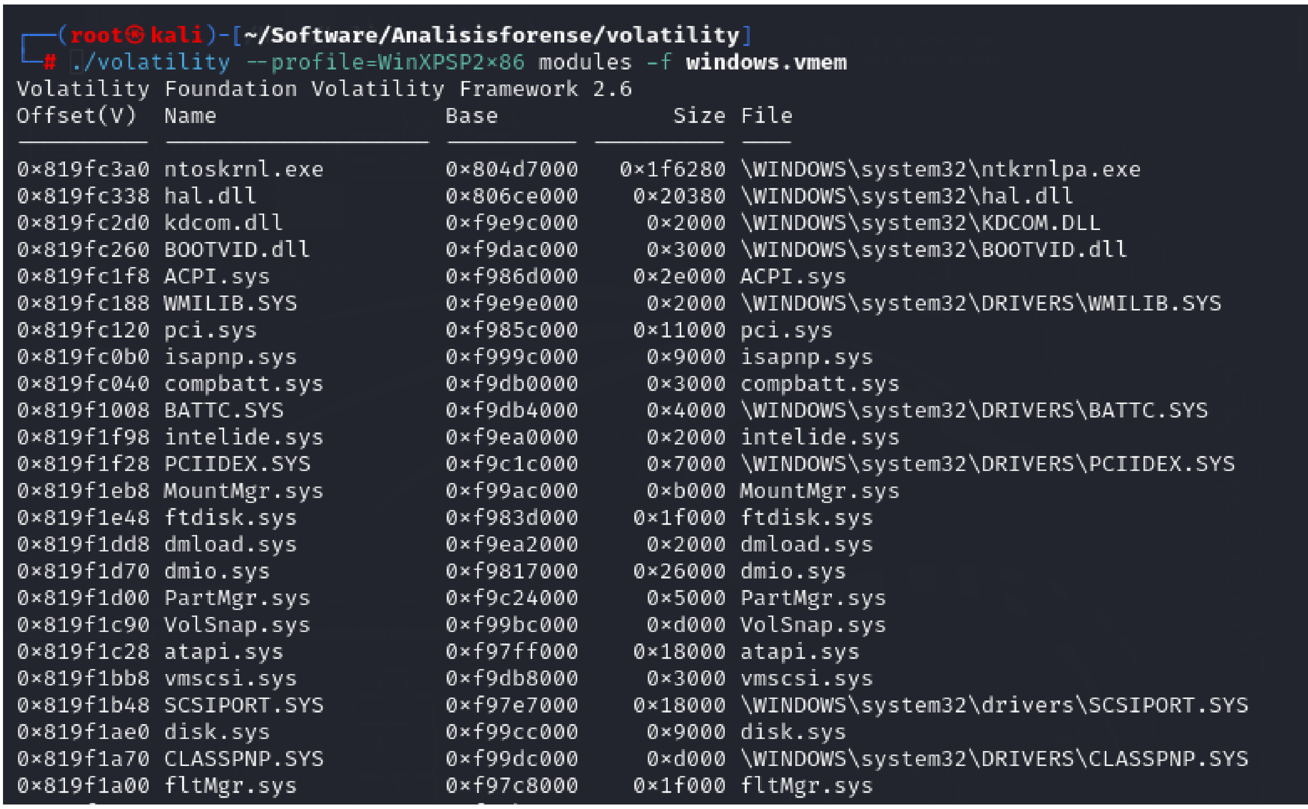
- Las librerías dinámicas del proceso/s sospechoso/s.



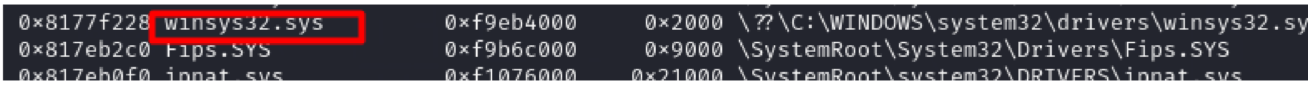
```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2x86 dlllist -p 1956 -f windows.vmem
Volatility Foundation Volatility Framework 2.6
************************************************************************
explorer.exe pid:   1956
Command line : C:\WINDOWS\Explorer.EXE
Service Pack 2

Base             Size  LoadCount Path
──────────── ──────────── ──────────── ────
0x01000000    0xff000     0xffff C:\WINDOWS\Explorer.EXE
0x7c900000    0xb0000     0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000    0xf4000     0xffff C:\WINDOWS\system32\kernel32.dll
0x77c10000    0x58000     0xffff C:\WINDOWS\system32\msvcrt.dll
0x77dd0000    0x9b000     0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x91000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77f10000    0x46000     0xffff C:\WINDOWS\system32\GDI32.dll
0x77d40000    0x90000     0xffff C:\WINDOWS\system32\USER32.dll
0x77f60000    0x76000     0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x7c9c0000   0x814000     0xffff C:\WINDOWS\system32\SHELL32.dll
0x774e0000   0x13c000     0xffff C:\WINDOWS\system32\ole32.dll
0x77120000    0x8c000     0xffff C:\WINDOWS\system32\OLEAUT32.dll
0x75f80000    0xfc000     0xffff C:\WINDOWS\system32\BROWSEUI.dll
0x77760000   0x16c000     0xffff C:\WINDOWS\system32\SHDOCVW.dll
0x77a80000    0x94000     0xffff C:\WINDOWS\system32\CRYPT32.dll
0x77b20000    0x12000     0xffff C:\WINDOWS\system32\MSASN1.dll
0x754d0000    0x80000     0xffff C:\WINDOWS\system32\CRYPTUI.dll
0x76c30000    0x2e000     0xffff C:\WINDOWS\system32\WINTRUST.dll
0x76c90000    0x28000     0xffff C:\WINDOWS\system32\IMAGEHLP.dll
0x5b860000    0x54000     0xffff C:\WINDOWS\system32\NETAPI32.dll
0x771b0000    0xa6000     0xffff C:\WINDOWS\system32\WININET.dll
0x76f60000    0x2c000     0xffff C:\WINDOWS\system32\WLDAP32.dll
0x77c00000     0x8000     0xffff C:\WINDOWS\system32\VERSION.dll
0x5ad70000    0x38000     0xffff C:\WINDOWS\system32\UxTheme.dll
0x5cb70000    0x26000        0x1 C:\WINDOWS\system32\ShimEng.dll
0x6f880000   0x1ca000        0x1 C:\WINDOWS\AppPatch\AcGenral.DLL
0x76b40000    0x2d000       0x10 C:\WINDOWS\system32\WINMM.dll
```

- Los módulos cargados.

  El proceso winsys32 carga desde la carpeta C:Windows

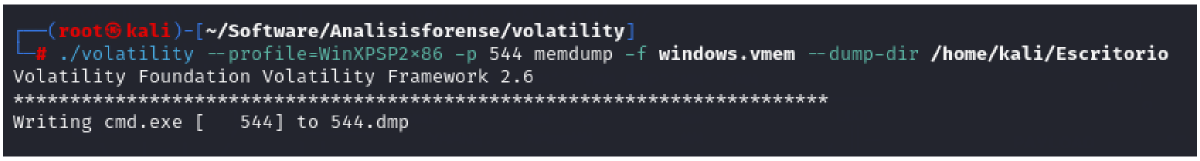


```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2x86 modules -f windows.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                 Base              Size File
────────── ──────────────────── ────────── ────────── ────
0x819fc3a0 ntoskrnl.exe         0x804d7000   0x1f6280 \WINDOWS\system32\ntkrnlpa.exe
0x819fc338 hal.dll              0x806ce000    0x20380 \WINDOWS\system32\hal.dll
0x819fc2d0 kdcom.dll            0xf9e9c000     0x2000 \WINDOWS\system32\KDCOM.DLL
0x819fc260 BOOTVID.dll          0xf9dac000     0x3000 \WINDOWS\system32\BOOTVID.dll
0x819fc1f8 ACPI.sys             0xf986d000    0x2e000 ACPI.sys
0x819fc188 WMILIB.SYS           0xf9e9e000     0x2000 \WINDOWS\system32\DRIVERS\WMILIB.SYS
0x819fc120 pci.sys              0xf985c000    0x11000 pci.sys
0x819fc0b0 isapnp.sys           0xf999c000     0x9000 isapnp.sys
0x819fc040 compbatt.sys         0xf9db0000     0x3000 compbatt.sys
0x819f1008 BATTC.SYS            0xf9db4000     0x4000 \WINDOWS\system32\DRIVERS\BATTC.SYS
0x819f1f98 intelide.sys         0xf9ea0000     0x2000 intelide.sys
0x819f1f28 PCIIDEX.SYS          0xf9c1c000     0x7000 \WINDOWS\system32\DRIVERS\PCIIDEX.SYS
0x819f1eb8 MountMgr.sys         0xf99ac000     0xb000 MountMgr.sys
0x819f1e48 ftdisk.sys           0xf983d000    0x1f000 ftdisk.sys
0x819f1dd8 dmload.sys           0xf9ea2000     0x2000 dmload.sys
0x819f1d70 dmio.sys             0xf9817000    0x26000 dmio.sys
0x819f1d00 PartMgr.sys          0xf9c24000     0x5000 PartMgr.sys
0x819f1c90 VolSnap.sys          0xf99bc000     0xd000 VolSnap.sys
0x819f1c28 atapi.sys            0xf97ff000    0x18000 atapi.sys
0x819f1bb8 vmscsi.sys           0xf9db8000     0x3000 vmscsi.sys
0x819f1b48 SCSIPORT.SYS         0xf97e7000    0x18000 \WINDOWS\system32\drivers\SCSIPORT.SYS
0x819f1ae0 disk.sys             0xf99cc000     0x9000 disk.sys
0x819f1a70 CLASSPNP.SYS         0xf99dc000     0xd000 \WINDOWS\system32\DRIVERS\CLASSPNP.SYS
0x819f1a00 fltMgr.sys           0xf97c8000    0x1f000 fltMgr.sys
```



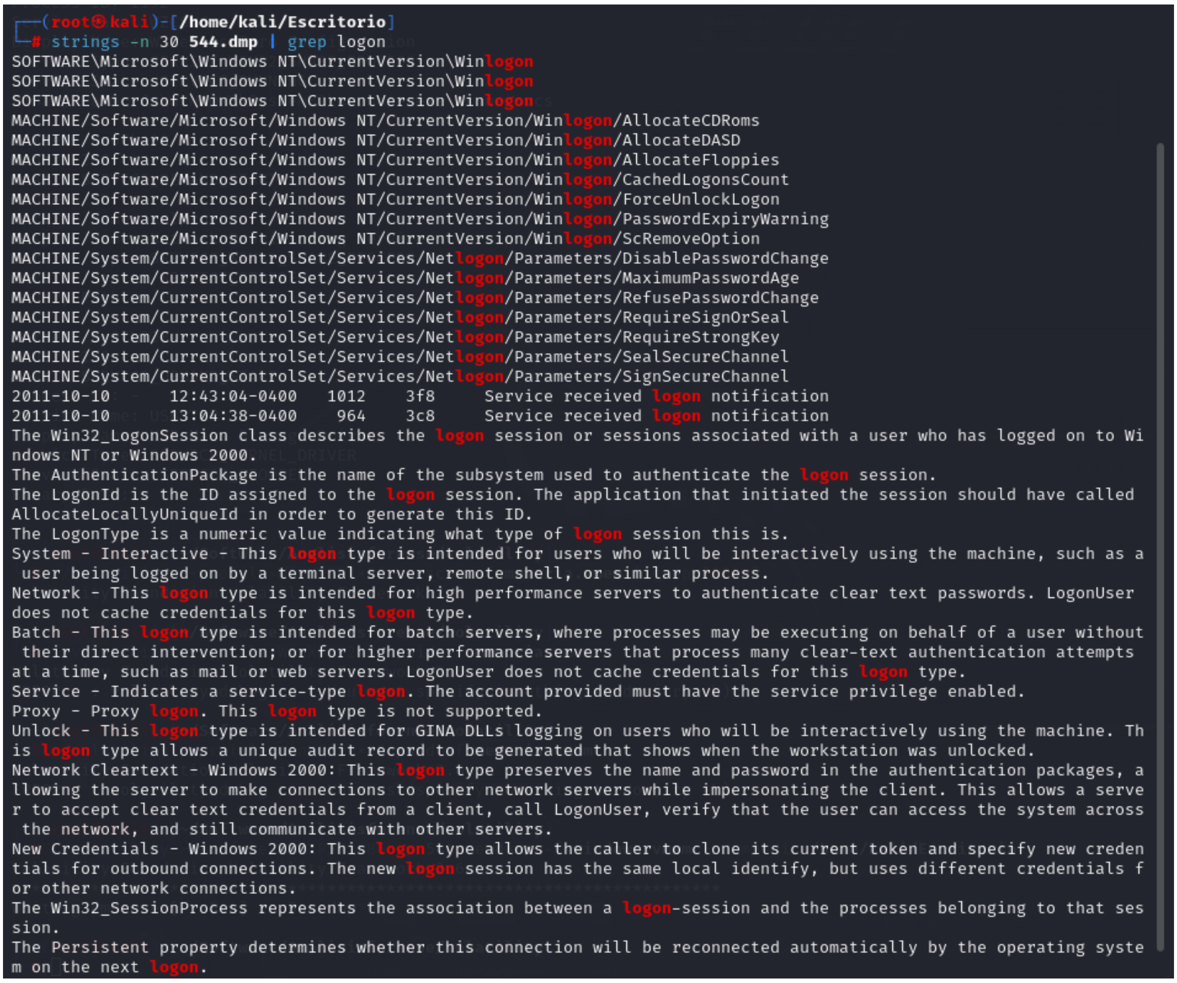
```
0x8177f228 winsys32.sys         0xf9eb4000     0x2000 \??\C:\WINDOWS\system32\drivers\winsys32.sy
0x817eb2c0 Fips.SYS             0xf9b6c000     0x9000 \SystemRoot\System32\Drivers\Fips.SYS
0x817eb0f0 ipnat.sys            0xf1076000    0x21000 \SystemRoot\system32\DRIVERS\ipnat.sys
```

- Un volcado en profundidad del/de los proceso/s sospechoso/s.



```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2x86 -p 544 memdump -f windows.vmem --dump-dir /home/kali/Escritorio
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing cmd.exe [   544] to 544.dmp
```

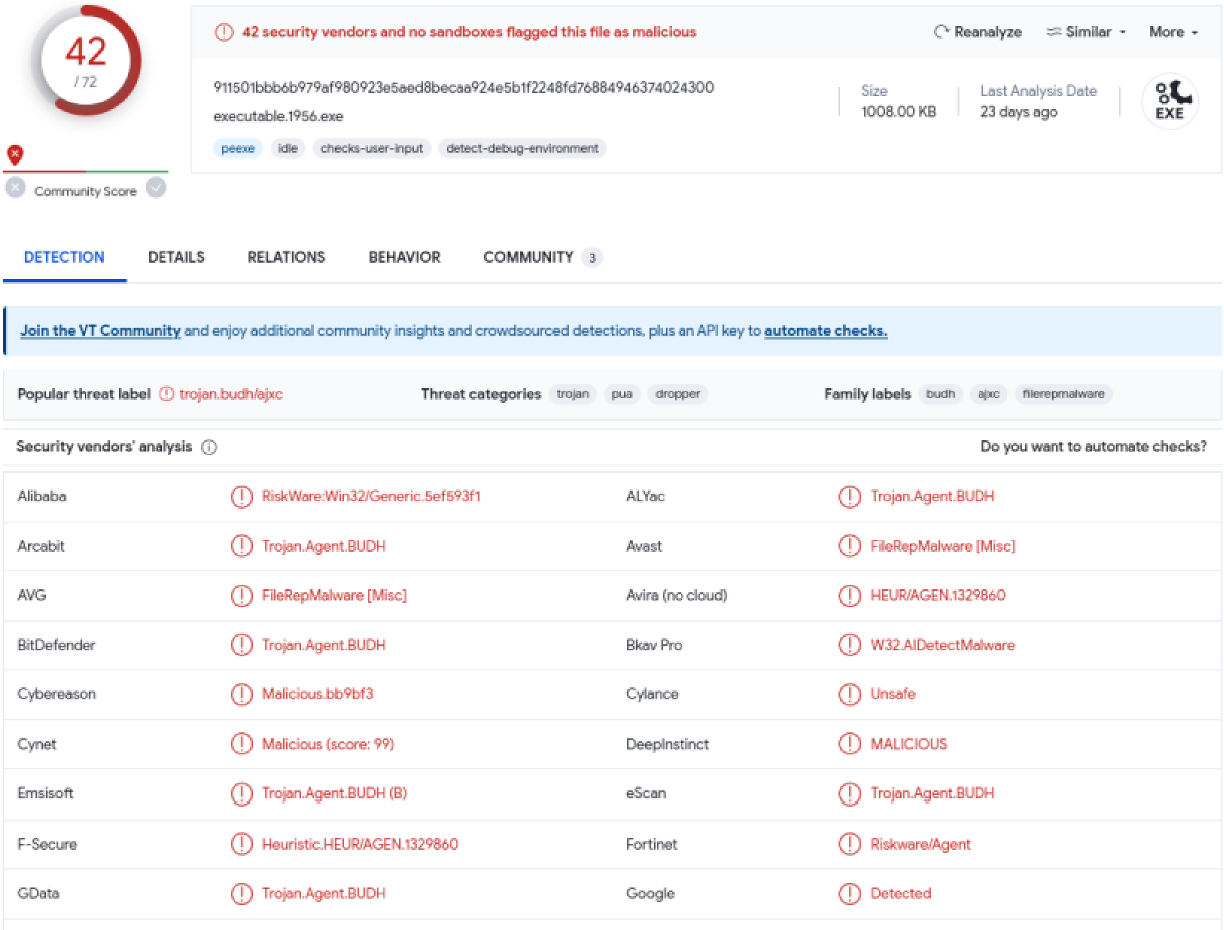
- Sacar cadenas del/de los volcado/s en profundidad para inspeccionarlo/s.



```
┌──(root㉿kali)-[/home/kali/Escritorio]
└─# strings -n 30 544.dmp | grep logon
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
MACHINE/Software/Microsoft/Windows NT/CurrentVersion/Winlogon/AllocateCDRoms
MACHINE/Software/Microsoft/Windows NT/CurrentVersion/Winlogon/AllocateDASD
MACHINE/Software/Microsoft/Windows NT/CurrentVersion/Winlogon/AllocateFloppies
MACHINE/Software/Microsoft/Windows NT/CurrentVersion/Winlogon/CachedLogonsCount
MACHINE/Software/Microsoft/Windows NT/CurrentVersion/Winlogon/ForceUnlockLogon
MACHINE/Software/Microsoft/Windows NT/CurrentVersion/Winlogon/PasswordExpiryWarning
MACHINE/Software/Microsoft/Windows NT/CurrentVersion/Winlogon/ScRemoveOption
MACHINE/System/CurrentControlSet/Services/Netlogon/Parameters/DisablePasswordChange
MACHINE/System/CurrentControlSet/Services/Netlogon/Parameters/MaximumPasswordAge
MACHINE/System/CurrentControlSet/Services/Netlogon/Parameters/RefusePasswordChange
MACHINE/System/CurrentControlSet/Services/Netlogon/Parameters/RequireSignOrSeal
MACHINE/System/CurrentControlSet/Services/Netlogon/Parameters/RequireStrongKey
MACHINE/System/CurrentControlSet/Services/Netlogon/Parameters/SealSecureChannel
MACHINE/System/CurrentControlSet/Services/Netlogon/Parameters/SignSecureChannel
2011-10-10      12:43:04-0400   1012    3f8     Service received logon notification
2011-10-10      13:04:38-0400    964    3c8     Service received logon notification
The Win32_LogonSession class describes the logon session or sessions associated with a user who has logged on to Wi
ndows NT or Windows 2000.
The AuthenticationPackage is the name of the subsystem used to authenticate the logon session.
The LogonId is the ID assigned to the logon session. The application that initiated the session should have called
AllocateLocallyUniqueId in order to generate this ID.
The LogonType is a numeric value indicating what type of logon session this is.
System - Interactive - This logon type is intended for users who will be interactively using the machine, such as a
 user being logged on by a terminal server, remote shell, or similar process.
Network - This logon type is intended for high performance servers to authenticate clear text passwords. LogonUser
does not cache credentials for this logon type.
Batch - This logon type is intended for batch servers, where processes may be executing on behalf of a user without
 their direct intervention; or for higher performance servers that process many clear-text authentication attempts
at a time, such as mail or web servers. LogonUser does not cache credentials for this logon type.
Service - Indicates a service-type logon. The account provided must have the service privilege enabled.
Proxy - Proxy logon. This logon type is not supported.
Unlock - This logon type is intended for GINA DLLs logging on users who will be interactively using the machine. Th
is logon type allows a unique audit record to be generated that shows when the workstation was unlocked.
Network Cleartext - Windows 2000: This logon type preserves the name and password in the authentication packages, a
llowing the server to make connections to other network servers while impersonating the client. This allows a serve
r to accept clear text credentials from a client, call LogonUser, verify that the user can access the system across
 the network, and still communicate with other servers.
New Credentials - Windows 2000: This logon type allows the caller to clone its current token and specify new creden
tials for outbound connections. The new logon session has the same local identify, but uses different credentials f
or other network connections.
The Win32_SessionProcess represents the association between a logon-session and the processes belonging to that ses
sion.
The Persistent property determines whether this connection will be reconnected automatically by the operating syste
m on the next logon.
```

- Llegar a una conclusión sobre el malware que se estaba ejecutando en la máquina proporcionando las evidencias recolectadas en el análisis e investigando en fuente abierta.

Para realizar esto, nos dirigimos a VirusTotal y pegamos el ejecutable adquirido para poder analizarlo.
En resumen, el troyano Win32 se destaca por su baja efectividad y alta facilidad de detección. Dentro de sus funcionalidades se encuentran capacidades como el seguimiento de las teclas presionadas, la captura de pantallas, el robo de datos personales, la descarga de archivos dañinos, el control remoto de sistemas, así como la habilidad de espiar y vigilar actividades.



42
/ 72

Community Score

42 security vendors and no sandboxes flagged this file as malicious

911501bbb6b979af980923e5aed8becaa924e5b1f2248fd76884946374024300

executable.1956.exe

peexe idle checks-user-input detect-debug-environment

Size
1008.00 KB

Last Analysis Date
23 days ago

EXE

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.budh/ajxc   Threat categories trojan pua dropper   Family labels budh ajxc filerepmalware

Security vendors' analysis   Do you want to automate checks?

Alibaba	RiskWare:Win32/Generic.5ef593f1	ALYac	Trojan.Agent.BUDH
Arcabit	Trojan.Agent.BUDH	Avast	FileRepMalware [Misc]
AVG	FileRepMalware [Misc]	Avira (no cloud)	HEUR/AGEN.1329860
BitDefender	Trojan.Agent.BUDH	Bkav Pro	W32.AIDetectMalware
Cybereason	Malicious.bb9bf3	Cylance	Unsafe
Cynet	Malicious (score: 99)	DeepInstinct	MALICIOUS
Emsisoft	Trojan.Agent.BUDH (B)	eScan	Trojan.Agent.BUDH
F-Secure	Heuristic.HEUR/AGEN.1329860	Fortinet	Riskware/Agent
GData	Trojan.Agent.BUDH	Google	Detected