Análisis de evidencias en memoria con Volatility.

Caso 1 : Archivo .dmp (dump memory) de un Windows 7

Este caso 1 se ha empezado a realizar con Volatility versión 2.7 por error, desde el ejercicio 1 hasta el 4. A partir del 5 incluido hasta el Caso 2 completo se ha cambiado a la versión 3 de Volatility.

1. ¿Cuál es el nombre del equipo?

Para saber el nombre del equipo, en el comando de volatility hay que utilizar el plugin de variables de entorno del proceso *envars*, tal y como indica la siguiente captura:

python2.7 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp --profile=Win7SP1x64 envars

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2.7 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp --profile=Win7SP1x64 envars
Volatility Foundation Volatility Framework 2.6.1
Pid      Process            Block              Variable                       Value
-------- ------------------ ------------------ ------------------------------ -----
     248 smss.exe           0x0000000000441320 Path                           C:\Windows\System32
     248 smss.exe           0x0000000000441320 SystemDrive                    C:
     248 smss.exe           0x0000000000441320 SystemRoot                     C:\Windows
     320 csrss.exe          0x0000000000411320 ComSpec                        C:\Windows\system32\cmd.exe
     320 csrss.exe          0x0000000000411320 FP_NO_HOST_CHECK               NO
     320 csrss.exe          0x0000000000411320 NUMBER_OF_PROCESSORS           1
     320 csrss.exe          0x0000000000411320 OS                             Windows_NT
     320 csrss.exe          0x0000000000411320 Path                           C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\
WindowsPowerShell\v1.0\
     320 csrss.exe          0x0000000000411320 PATHEXT                        .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
     320 csrss.exe          0x0000000000411320 PROCESSOR_ARCHITECTURE         AMD64
     320 csrss.exe          0x0000000000411320 PROCESSOR_IDENTIFIER           Intel64 Family 6 Model 158 Stepping 13, GenuineIntel
     320 csrss.exe          0x0000000000411320 PROCESSOR_LEVEL                6
     320 csrss.exe          0x0000000000411320 PROCESSOR_REVISION             9e0d
```

El nombre del equipo es **W7BASE**, el cual se recoge en la variable de entorno COMPUTERNAME.

```
Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\
    2464 iexplore.exe      0x0000000000471320 PATHEXT                        .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.M
    2464 iexplore.exe      0x0000000000471320 PROCESSOR_ARCHITECTURE         AMD64
    2464 iexplore.exe      0x0000000000471320 PROCESSOR_IDENTIFIER           Intel64 Family 6 Model 158 Stepping 13, GenuineInte
    2464 iexplore.exe      0x0000000000471320 PROCESSOR_LEVEL                6
    2464 iexplore.exe      0x0000000000471320 PROCESSOR_REVISION             9e0d
    2464 iexplore.exe      0x0000000000471320 ProgramData                    C:\ProgramData
    2464 iexplore.exe      0x0000000000471320 ProgramFiles                   C:\Program Files
    2464 iexplore.exe      0x0000000000471320 ProgramFiles(x86)              C:\Program Files (x86)
    2464 iexplore.exe      0x0000000000471320 ProgramW6432                   C:\Program Files
    2464 iexplore.exe      0x0000000000471320 PSModulePath                   C:\Windows\system32\WindowsPowerShell\v1.0\Modules\
    2464 iexplore.exe      0x0000000000471320 PUBLIC                         C:\Users\Public
    2464 iexplore.exe      0x0000000000471320 SESSIONNAME                    Console
    2464 iexplore.exe      0x0000000000471320 SystemDrive                    C:
    2464 iexplore.exe      0x0000000000471320 SystemRoot                     C:\Windows
    2464 iexplore.exe      0x0000000000471320 TEMP                           C:\Users\wadmin\AppData\Local\Temp
    2464 iexplore.exe      0x0000000000471320 TMP                            C:\Users\wadmin\AppData\Local\Temp
    2464 iexplore.exe      0x0000000000471320 USERDOMAIN                     w7base
    2464 iexplore.exe      0x0000000000471320 USERNAME                       wadmin
    2464 iexplore.exe      0x0000000000471320 USERPROFILE                    C:\Users\wadmin
    2464 iexplore.exe      0x0000000000471320 windir                         C:\Windows
    2464 iexplore.exe      0x0000000000471320 windows_tracing_flags          3
    2464 iexplore.exe      0x0000000000471320 windows_tracing_logfile        C:\BVTBin\Tests\installpackage\csilogfile.log
    2988 cmd.exe           0x0000000000371320 ALLUSERSPROFILE                C:\ProgramData
    2988 cmd.exe           0x0000000000371320 APPDATA                        C:\Users\wadmin\AppData\Roaming
    2988 cmd.exe           0x0000000000371320 CommonProgramFiles             C:\Program Files\Common Files
    2988 cmd.exe           0x0000000000371320 CommonProgramFiles(x86)        C:\Program Files (x86)\Common Files
    2988 cmd.exe           0x0000000000371320 CommonProgramW6432             C:\Program Files\Common Files
    2988 cmd.exe           0x0000000000371320 COMPUTERNAME                   W7BASE
```

2. El usuario tenía establecida una conexión FTP con un organismo público español. ¿Cuál es?

Para saberlo hay que utilizar el plugin *netscan*, el cual escanea estructuras de sockets y muestra todas las conexiones de red detectadas. Ejecutamos el comando siguiente:

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2.7 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x61dcc60          UDPv4    0.0.0.0:3702                   *:*                                   1408     svchost.exe    2020-12-07 18:19:24 UTC+0000
```

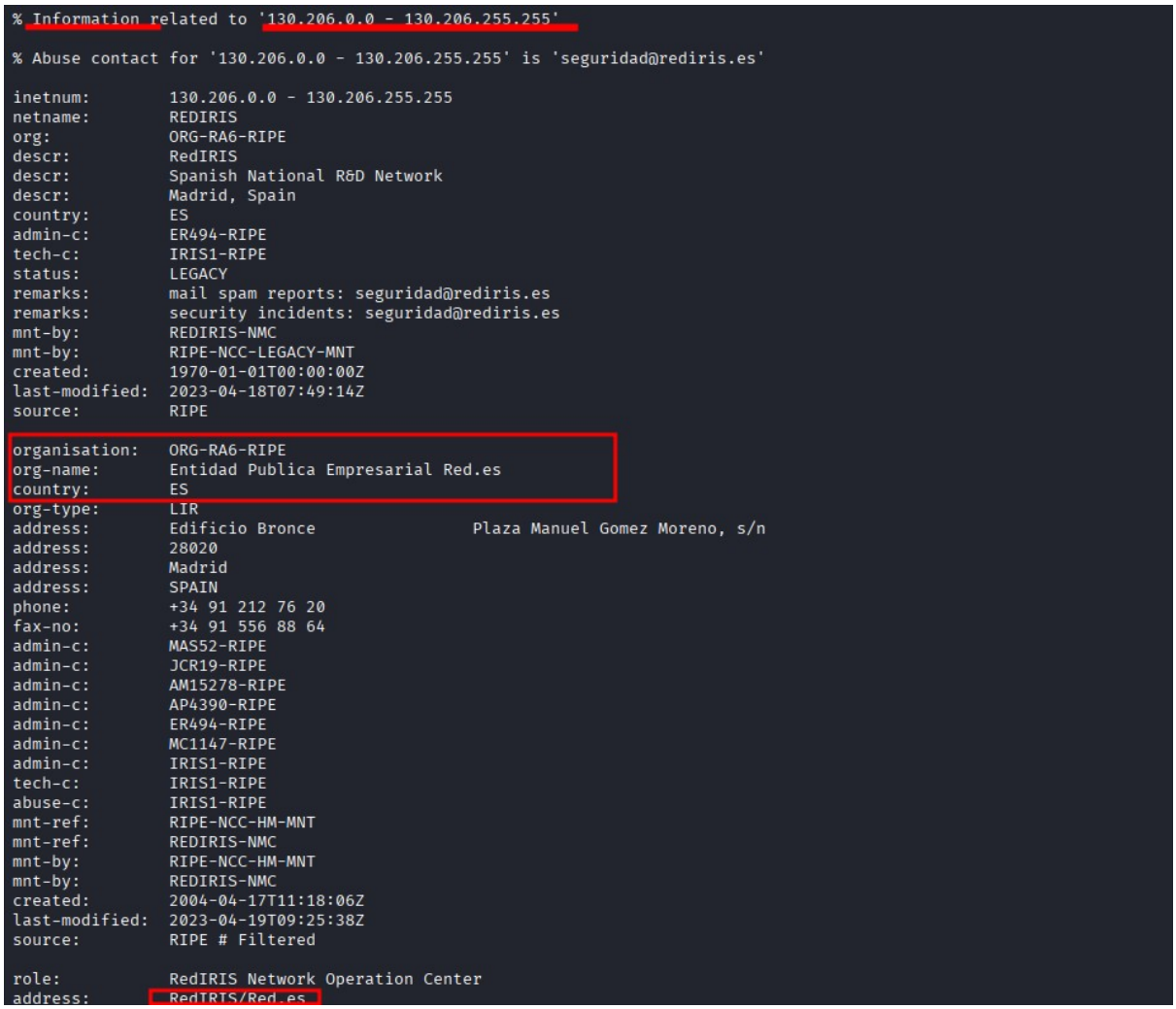
En todo el listado de conexiones de estado establecidas(con el campo State en ESTABLISHED) se va mirando por la columna Owner el proceso asociado a la conexión, el cual tenga un nombre que contenga algo como “ftp”, “*ftp.exe*” . Se localizan varias, con el mismo PID 2424, las cuales tienen como Foreign Address la IP 130.206.13.2.

```
  UDPv4    127.0.0.1:63917                *:*                                   2424     ftp.exe        2020-12-07 18:19:54 UTC+0000
  TCPv4    127.0.0.1:49233                127.0.0.1:49234      ESTABLISHED      1968     SearchFilterHo
  TCPv4    10.0.2.15:49171                130.206.13.2:21      ESTABLISHED      2424     ftp.exe
  TCPv4    0.0.0.0:5357                   0.0.0.0:0            LISTENING        4        System
  TCPv6    :::5357                        :::0                 LISTENING        4        System
  TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        472      lsass.exe
  TCPv6    :::49156                       :::0                 LISTENING        472      lsass.exe
  TCPv4    -:49285                        -:443                ESTABLISHED      1608     firefox.exe
  TCPv4    0.0.0.0:17448                  0.0.0.0:0            LISTENING        1028     haboer.exe
  UDPv4    127.0.0.1:1900                 *:*                                   1408     svchost.exe    2020-12-07 18:21:20 UTC+0000
  UDPv4    10.0.2.15:1900                 *:*                                   1408     svchost.exe    2020-12-07 18:21:20 UTC+0000
  TCPv4    127.0.0.1:49182                127.0.0.1:49183      ESTABLISHED      0
  UDPv4    10.0.2.15:137                  *:*                                   4        System         2020-12-07 18:19:21 UTC+0000
  UDPv4    127.0.0.1:63920                *:*                                   1408     svchost.exe    2020-12-07 18:21:20 UTC+0000
  UDPv6    ::1:63919                      *:*                                   1408     svchost.exe    2020-12-07 18:21:20 UTC+0000
  UDPv6    ::1:63918                      *:*                                   2424     ftp.exe        2020-12-07 18:19:54 UTC+0000
  UDPv4    0.0.0.0:62157                  *:*                                   1408     svchost.exe    2020-12-07 18:19:18 UTC+0000
  UDPv4    0.0.0.0:62158                  *:*                                   1408     svchost.exe    2020-12-07 18:19:18 UTC+0000
  UDPv6    :::62158                       *:*                                   1408     svchost.exe    2020-12-07 18:19:18 UTC+0000
  UDPv6    ::1:1900                       *:*                                   1408     svchost.exe    2020-12-07 18:52:25 UTC+0000
  UDPv4    127.0.0.1:63917                *:*                                   2424     ftp.exe        2020-12-07 18:19:54 UTC+0000
  UDPv4    10.0.2.15:1900                 *:*                                   1408     svchost.exe    2020-12-07 18:52:25 UTC+0000
  UDPv4    0.0.0.0:3702                   *:*                                   1408     svchost.exe    2020-12-07 18:52:26 UTC+0000
  UDPv6    :::3702                        *:*                                   1408     svchost.exe    2020-12-07 18:52:26 UTC+0000
  UDPv6    ::1:53399                      *:*                                   1408     svchost.exe    2020-12-07 18:52:26 UTC+0000
  UDPv4    0.0.0.0:3702                   *:*                                   1408     svchost.exe    2020-12-07 18:52:26 UTC+0000
  UDPv6    :::3702                        *:*                                   1408     svchost.exe    2020-12-07 18:52:26 UTC+0000
  UDPv4    127.0.0.1:1900                 *:*                                   1408     svchost.exe    2020-12-07 18:52:25 UTC+0000
  UDPv4    0.0.0.0:0                      *:*                                   1072     svchost.exe    2020-12-07 18:52:17 UTC+0000
  UDPv6    :::0                           *:*                                   1072     svchost.exe    2020-12-07 18:52:17 UTC+0000
  UDPv4    0.0.0.0:3702                   *:*                                   1408     svchost.exe    2020-12-07 18:52:26 UTC+0000
  TCPv4    0.0.0.0:5357                   0.0.0.0:0            LISTENING        4        System
  TCPv6    :::5357                        :::0                 LISTENING        4        System
  TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        464      services.exe
  TCPv6    :::49155                       :::0                 LISTENING        464      services.exe
  TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        472      lsass.exe
  TCPv6    :::49156                       :::0                 LISTENING        472      lsass.exe
  TCPv4    0.0.0.0:49156                  0.0.0.0:0            LISTENING        472      lsass.exe
  TCPv4    0.0.0.0:17448                  0.0.0.0:0            LISTENING        1028     haboer.exe
  TCPv4    0.0.0.0:17448                  0.0.0.0:0            LISTENING        1028     haboer.exe
  TCPv6    :::17448                       :::0                 LISTENING        1028     haboer.exe
  TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System
  TCPv6    :::445                         :::0                 LISTENING        4        System
  TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        368      wininit.exe
  TCPv6    :::49152                       :::0                 LISTENING        368      wininit.exe
  TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        780      svchost.exe
  TCPv6    :::49153                       :::0                 LISTENING        780      svchost.exe
  TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        464      services.exe
  TCPv4    10.0.2.15:49330                92.123.77.25:80      ESTABLISHED      2464     iexplore.exe
  TCPv6    -:0                            68c0:a402:80fa:ffff:68c0:a402:80fa:ffff:0 CLOSED          1028     haboer.exe
  TCPv6    -:0                            68c0:a402:80fa:ffff:68c0:a402:80fa:ffff:0 CLOSED          1028     haboer.exe
  TCPv4    10.0.2.15:49171                130.206.13.2:21      ESTABLISHED      2424     ftp.exe
```

Con esta IP encontrada ejecutamos un **whois 130.206.13.2** para saber información relativa a esta IP y obtener el organismo público a buscar:

```
    TCPv4    10.0.2.15:49171                130.206.13.2:21      ESTABLISHED      2424     ftp.exe

Session  Acciones  Editar  Vista  Ayuda
┌──(kali㉿kali)-[~]
└─$ whois 130.206.13.2
```

El organismo público español con el que el usuario tenía establecida una conexión FTP es la **Entidad Pública Empresarial** [Red.es](Red.es) , tal y como muestra la siguiente captura de pantalla:



```
% Information related to '130.206.0.0 - 130.206.255.255'

% Abuse contact for '130.206.0.0 - 130.206.255.255' is 'seguridad@rediris.es'

inetnum:        130.206.0.0 - 130.206.255.255
netname:        REDIRIS
org:            ORG-RA6-RIPE
descr:          RedIRIS
descr:          Spanish National R&D Network
descr:          Madrid, Spain
country:        ES
admin-c:        ER494-RIPE
tech-c:         IRIS1-RIPE
status:         LEGACY
remarks:        mail spam reports: seguridad@rediris.es
remarks:        security incidents: seguridad@rediris.es
mnt-by:         REDIRIS-NMC
mnt-by:         RIPE-NCC-LEGACY-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2023-04-18T07:49:14Z
source:         RIPE

organisation:   ORG-RA6-RIPE
org-name:       Entidad Publica Empresarial Red.es
country:        ES
org-type:       LIR
address:        Edificio Bronce                 Plaza Manuel Gomez Moreno, s/n
address:        28020
address:        Madrid
address:        SPAIN
phone:          +34 91 212 76 20
fax-no:         +34 91 556 88 64
admin-c:        MAS52-RIPE
admin-c:        JCR19-RIPE
admin-c:        AM15278-RIPE
admin-c:        AP4390-RIPE
admin-c:        ER494-RIPE
admin-c:        MC1147-RIPE
admin-c:        IRIS1-RIPE
tech-c:         IRIS1-RIPE
abuse-c:        IRIS1-RIPE
mnt-ref:        RIPE-NCC-HM-MNT
mnt-ref:        REDIRIS-NMC
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         REDIRIS-NMC
created:        2004-04-17T11:18:06Z
last-modified:  2023-04-19T09:25:38Z
source:         RIPE # Filtered

role:           RedIRIS Network Operation Center
address:        RedIRIS/Red.es
```

3. Hay por lo menos un proceso que contiene malware. ¿Cuál es su nombre y su PID?
Por su nombre tan sospechoso y con la extensión incompleta(.ex en vez de .exe) totalmente inusual a los procesos típicos esperados en Windows, el proceso que contiene malware es *AsustoMucho.ex* , con PID 1004. Además, el proceso fue lanzado por el explorer.exe(buscar el 896 en la columna PID), nada usual en para procesos del sistema que provienen de services.exe(ver 464 en la columna PID).

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2.7 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa80018c4040 System                    4      0     81      553 ------      0 2020-12-07 18:19:15 UTC+0000
0xfffffa80021017f0 smss.exe                248      4      2       29 ------      0 2020-12-07 18:19:15 UTC+0000
0xfffffa80028e1420 csrss.exe               320    312      9      357      0      0 2020-12-07 18:19:15 UTC+0000
0xfffffa80018cb060 wininit.exe             368    312      3       73      0      0 2020-12-07 18:19:16 UTC+0000
0xfffffa80018ccb30 csrss.exe               376    360      9      424      1      0 2020-12-07 18:19:16 UTC+0000
0xfffffa8002906230 winlogon.exe            404    360      3      109      1      0 2020-12-07 18:19:16 UTC+0000
0xfffffa8002941b30 services.exe            464    368      7      188      0      0 2020-12-07 18:19:16 UTC+0000
0xfffffa800294fb30 lsass.exe               472    368      6      582      0      0 2020-12-07 18:19:16 UTC+0000
0xfffffa80029517b0 lsm.exe                 480    368     10      141      0      0 2020-12-07 18:19:16 UTC+0000
0xfffffa800298fb30 svchost.exe             572    464      9      344      0      0 2020-12-07 18:19:16 UTC+0000
0xfffffa80029cc760 VBoxService.ex          632    464     12      110      0      0 2020-12-07 18:19:16 UTC+0000
0xfffffa80029eab30 svchost.exe             684    464      8      268      0      0 2020-12-07 18:19:16 UTC+0000
0xfffffa8002a24b30 svchost.exe             780    464     19      456      0      0 2020-12-07 18:19:16 UTC+0000
0xfffffa8002a45b30 svchost.exe             832    464     17      392      0      0 2020-12-07 18:19:16 UTC+0000
0xfffffa8002a4c060 svchost.exe             856    464     32     1003      0      0 2020-12-07 18:19:16 UTC+0000
0xfffffa8002a81b30 audiodg.exe             936    780      5      123      0      0 2020-12-07 18:19:17 UTC+0000
0xfffffa8002aa2b30 TrustedInstall          996    464      6      128      0      0 2020-12-07 18:19:17 UTC+0000
0xfffffa8002acd910 svchost.exe             276    464     10      258      0      0 2020-12-07 18:19:17 UTC+0000
0xfffffa8002b114e0 svchost.exe            1072    464     21      580      0      0 2020-12-07 18:19:17 UTC+0000
0xfffffa8002318b30 spoolsv.exe            1232    464     12      261      0      0 2020-12-07 18:19:18 UTC+0000
0xfffffa8002325590 taskhost.exe           1240    464      8      169      1      0 2020-12-07 18:19:18 UTC+0000
0xfffffa800234d450 svchost.exe            1308    464     19      325      0      0 2020-12-07 18:19:18 UTC+0000
0xfffffa8002ba2740 svchost.exe            1408    464     14      233      0      0 2020-12-07 18:19:18 UTC+0000
0xfffffa8002ddbb30 sppsvc.exe             1748    464      4      145      0      0 2020-12-07 18:19:18 UTC+0000
0xfffffa8002e777d0 dwm.exe                1436    832      3       82      1      0 2020-12-07 18:19:30 UTC+0000
0xfffffa8002e84b30 explorer.exe            896   1376     39     1207      1      0 2020-12-07 18:19:30 UTC+0000
0xfffffa8002f33340 VBoxTray.exe           2012    896      6      156      1      0 2020-12-07 18:19:31 UTC+0000
0xfffffa8002f3eb30 haboer.exe             1028    896     13     1071      1      1 2020-12-07 18:19:31 UTC+0000
0xfffffa8002f48b30 AsustoMucho.ex         1004    896      7      221      1      1 2020-12-07 18:19:31 UTC+0000
0xfffffa8002fb0400 SearchIndexer.         2112    464     13      669      0      0 2020-12-07 18:19:38 UTC+0000
0xfffffa80030b6b30 cmd.exe                2388    896      1       23      1      0 2020-12-07 18:19:41 UTC+0000
0xfffffa80030b7890 conhost.exe            2396    376      2       56      1      0 2020-12-07 18:19:41 UTC+0000
0xfffffa80030c8890 ftp.exe                2424   2388      2       75      1      0 2020-12-07 18:19:50 UTC+0000
0xfffffa8003135750 cmd.exe                2640    896      1       20      1      0 2020-12-07 18:20:04 UTC+0000
0xfffffa80030e3900 conhost.exe            2648    376      2       54      1      0 2020-12-07 18:20:04 UTC+0000
0xfffffa80022b2b30 notepad.exe            2732    896      4      291      1      0 2020-12-07 18:20:23 UTC+0000
0xfffffa800196eb30 firefox.exe            1608    896      0 ------      1      0 2020-12-07 18:22:18 UTC+0000 2020-12-07 18:54:49 UTC+0000
0xfffffa8001b53060 perfmon.exe            2216    896     17      320      1      0 2020-12-07 18:28:11 UTC+0000
0xfffffa80022fbb30 cmd.exe                2796   1668      2       77      1      1 2020-12-07 18:28:51 UTC+0000
0xfffffa80022bcb30 conhost.exe            2868    376      2       50      1      0 2020-12-07 18:28:51 UTC+0000
0xfffffa80028ddb30 cmd.exe                3428   3296      2       76      1      1 2020-12-07 18:29:33 UTC+0000
0xfffffa80028dc7d0 conhost.exe            3436    376      2       50      1      0 2020-12-07 18:29:33 UTC+0000
0xfffffa800297b060 7zFM.exe               1484    896      3      162      1      0 2020-12-07 18:53:53 UTC+0000
0xfffffa8001be42e0 firefox.exe            2996    852     33      446      1      1 2020-12-07 18:56:11 UTC+0000
0xfffffa80020f76a0 firefox.exe            2852   2996      9      184      1      1 2020-12-07 18:56:21 UTC+0000
0xfffffa8001dd2340 iexplore.exe           2948    896     16      432      1      1 2020-12-07 18:56:33 UTC+0000
0xfffffa8002dd3060 iexplore.exe           2464   2948     19      588      1      1 2020-12-07 18:56:35 UTC+0000
0xfffffa800232d060 cmd.exe                2988   3884      2       76      1      1 2020-12-07 18:57:12 UTC+0000
0xfffffa800232d630 conhost.exe            4076    376      2       50      1      0 2020-12-07 18:57:12 UTC+0000
0xfffffa8002eb1b30 pytcw.exe              3996   1640      9      255      1      1 2020-12-07 18:58:36 UTC+0000
0xfffffa80029db630 DumpIt.exe             3556   2640      5       90      1      0 2020-12-07 18:58:45 UTC+0000
0xfffffa8001b08b30 WmiPrvSE.exe           2100    572      6      115      0      0 2020-12-07 18:58:48 UTC+0000
```

También son malware los procesos haboer.exe y pytcw.exe por las siguientes razones:

- *haboer.exe*: El nombre no corresponde a ningún software conocido ni a algún proceso del sistema de Windows y tiene 6 caracteres aleatorios, una práctica común en archivos de malware de 5 a 8 caracteres. El proceso proviene de explorer.exe como AsustoMucho.ex. El número de handles es muy raro para un proceso sin nombre conocido, de hecho tiene 1071 en columna Hnds, y los malware que interactúan con el sistema se suelen detectar por tener muchos handles. Solo apps complejas como por ejemplo navegadores (véase el valor de explorer.exe en la columna Hnds a 1207) llegan a esos valores.
- *pytcw.exe*: Del mismo modo que *haboer.exe*, el nombre tiene un patrón muy aleatorio de 5 letras que sigue el patrón de los procesos maliciosos de 5 a 8 caracteres. Un binario desconocido con más de 250 handles(ver en la captura que tiene 255 handles) sugiere que está abriendo múltiples recursos del sistema (claves de registro, archivos,etc.), lo que coincide con patrones típicos de malware activo.

Recomendación: confirmar que el proceso es malicioso calculando un hash del ejecutable y pegarlo en VirusTotal para comprobarlo.Lo mismo para el siguiente ejercicio 4.

4. Hay un proceso infectado que tiene establecida una conexión HTTPS. ¿Cuál es la dirección IP a la que está conectado?

El plugin indicado a usar es *netscan*, buscando el proceso conectado al puerto 443 predeterminado para tráfico HTTPS. Para ello filtramos la salida con grep -i 443:

```
┌──(kali㉿kali)-[~/volatility]
└─$ python2.7 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp --profile=Win7SP1×64 netscan | grep -i 443
Volatility Foundation Volatility Framework 2.6.1
0×36281010         TCPv4    10.0.2.15:49262                216.58.213.3:443     ESTABLISHED      1608     firefox.e
xe
0×3aab7010         TCPv4    -:49284                        33.161.122.39:443    ESTABLISHED      1608     firefox.e
xe
0×3abc2010         TCPv4    -:49263                        188.165.205.194:443  CLOSED           1608     firefox.e
xe
0×464ebcf0         TCPv4    -:49286                        118.45.153.189:443   ESTABLISHED      1608     firefox.e
xe
0×62341010         TCPv4    -:49285                        -:443                ESTABLISHED      1608     firefox.e
xe
0×7fa7ecf0         TCPv4    10.0.2.15:49325                2.19.61.200:443      ESTABLISHED      2464     iexplore.
exe
0×7fdf0580         TCPv4    10.0.2.15:49326                2.19.61.200:443      ESTABLISHED      2464     iexplore.
exe
0×7fe0f450         TCPv4    10.0.2.15:49525                160.153.75.34:443    ESTABLISHED      3996     pytcw.exe


┌──(kali㉿kali)-[~/volatility]
└─$
```

De todos los ejecutables que se muestran en el resultado, el proceso anormal en Windows 7 es pytcw.exe., que tiene un nombre aleatorio típico de malware (como se explicó en el ejercicio anterior). Otra razón por la que el proceso pytcw.exe es un proceso infectado es que es el único proceso no conocido con una conexión HTTPS directa como el resto, que corresponden a los navegadores web como aparece en la captura el firefox.exe (proceso del navegador Firefox). Además las IPs remotas asociadas a los navegadores son de organizaciones legítimas, tales como las de las dos siguientes capturas:

```
┌──(kali㉿kali)-[~/volatility]
└─$ whois 216.58.213.3

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


NetRange:       216.58.192.0 - 216.58.223.255
CIDR:           216.58.192.0/19
NetName:        GOOGLE
NetHandle:      NET-216-58-192-0-1
Parent:         NET216 (NET-216-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2012-01-27
Updated:        2012-01-27
Ref:            https://rdap.arin.net/registry/ip/216.58.192.0



OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are located in the following links.
Comment:
Comment:        To report abuse and illegal activity: https://www.google.com/contact/
Comment:
Comment:        For legal requests: http://support.google.com/legal
Comment:
Comment:        Regards,
Comment:        The Google Team
Ref:            https://rdap.arin.net/registry/entity/GOGL
```

```
┌──(kali㉿kali)-[~/volatility]
└─$ whois 33.161.122.39

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#



# start

NetRange:       33.0.0.0 - 33.255.255.255
CIDR:           33.0.0.0/8
NetName:        DISN-IP-LEGACY
NetHandle:      NET-33-0-0-0-1
Parent:          ()
NetType:        Direct Allocation
OriginAS:
Organization:   United States Department of Defense (DoD) (USDDD)
RegDate:        1991-01-01
Updated:        2025-09-05
Ref:            https://rdap.arin.net/registry/ip/33.0.0.0



OrgName:        United States Department of Defense (DoD)
OrgId:          USDDD
Address:        3990 E. Broad Street
City:           Columbus
StateProv:      OH
PostalCode:     43218
Country:        US
RegDate:        2007-01-12
Updated:        2025-03-13
Ref:            https://rdap.arin.net/registry/entity/USDDD
```

La IP asociada al proceso no es usada típicamente por procesos legítimos de Windows sino que se corresponde con un servicio de hosting compartido llamado GoDaddy, se puede comprobar su origen con el comando *whois*:

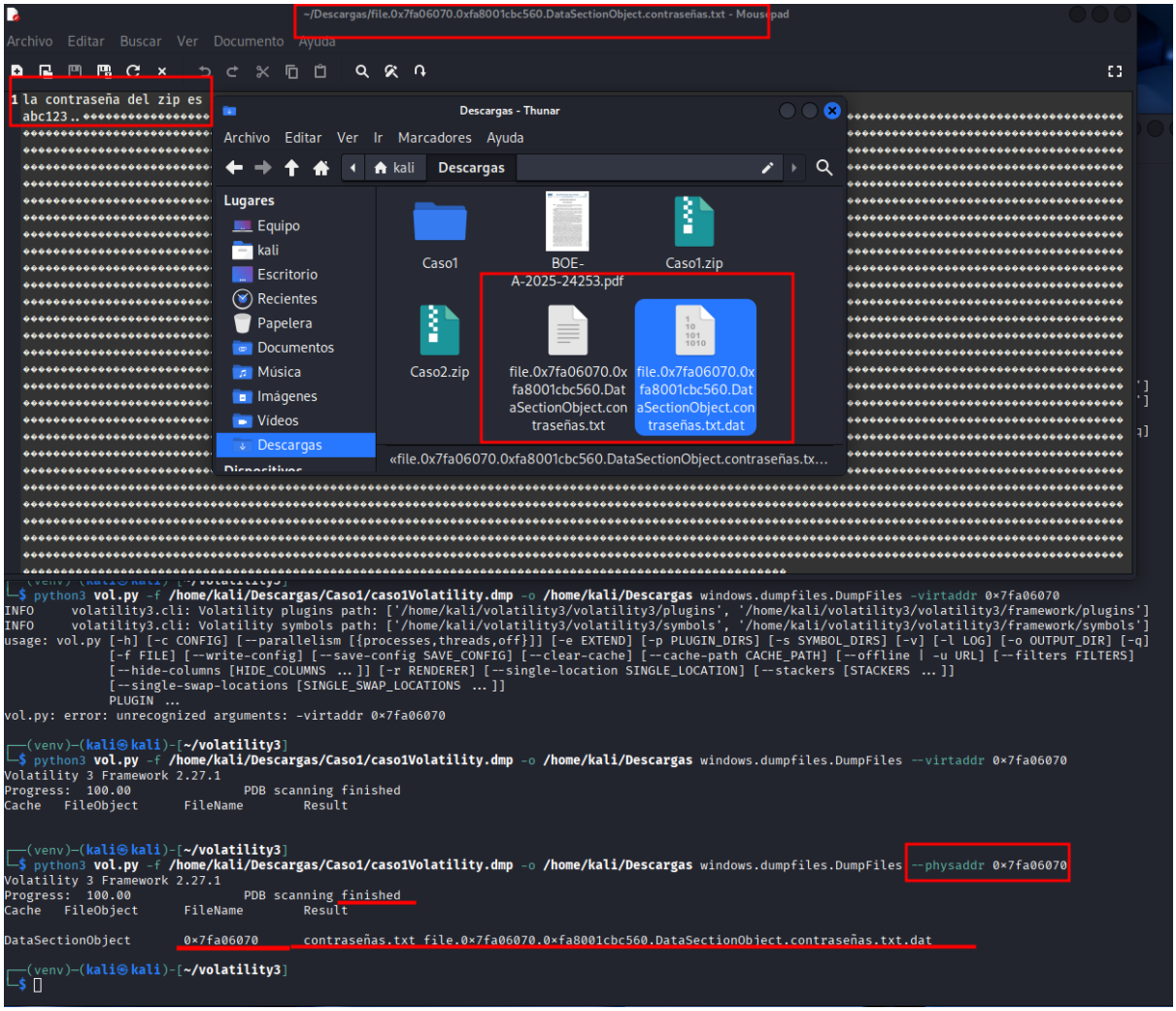
```
┌──(kali㉿kali)-[~/volatility]
└─$ whois 160.153.75.34

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


NetRange:       160.153.0.0 - 160.153.255.255
CIDR:           160.153.0.0/16
NetName:        GO-DADDY-COM-LLC
NetHandle:      NET-160-153-0-0-1
Parent:         NET160 (NET-160-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   GoDaddy.com, LLC (GODAD)
RegDate:        2011-09-01
Updated:        2014-02-25
Comment:        Please send abuse complaints to abuse@godaddy.com
Ref:            https://rdap.arin.net/registry/ip/160.153.0.0



OrgName:        GoDaddy.com, LLC
OrgId:          GODAD
Address:        2155 E GoDaddy Way
City:           Tempe
StateProv:      AZ
PostalCode:     85284
Country:        US
RegDate:        2007-06-01
Updated:        2024-11-25
Comment:        Please send abuse complaints to abuse@godaddy.com
Ref:            https://rdap.arin.net/registry/entity/GODAD
```

5. Hay una contraseña de un fichero comprimido escrita en el bloc de notas. ¿Cuál es?
A partir de este ejercicio se ha cambiado a la versión 3 de Volatility.

Los ficheros que se crean en el bloc de notas suelen tener la extensión .txt así que se realiza una búsqueda por este tipo de archivo, y se prueba por fuerza bruta que el fichero se llame “contraseñas.txt”, tal y como se muestra en la captura usando el plugin windows.filescan.FileScan:
python2.7 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp --profile=Win7SP1x64 filescan | grep -i "contraseñas.txt"

```
┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp windows.filescan.FileScan | grep -i "contraseñas.txt"
0x7fa06070 100.0\Users\wadmin\Desktop\contraseñas.txt
```

La prueba tuvo éxito: se encuentra un archivo en el escritorio del usuario *wadmin* con el nombre *contraseñas.txt*.
Ahora toca realizar una extracción del txt para ver su contenido con el plugin *windows.dumpfiles.DumpFiles*, indicando la dirección FÍSICA en memoria del fichero *contraseñas.txt* que muestra el comando de la captura anterior:



Se decide hacer una copia del archivo resultante .dat quitando dicha extensión para que solo quede la extensión .txt y se vea el contenido al abrirlo. Tal y como se indica en un cuadro rojo de la captura, la contraseña del zip es **abc123..** .

6. Existe un fichero ZIP accesible en la memoria RAM. ¿Qué animal se encuentra dentro?

Utilizamos el mismo comando que antes con el plugin *windows.filescan.FileScan* pero en este caso filtrando la búsqueda con .zip:

python3 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp windows.filescan.FileScan | grep -i ".zip"

Hay un fichero llamado *fichero.zip* accesible en la carpeta */Documents* del usuario *wadmin*, con la dirección en memoria 0x7f52e070:

```
┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp windows.filescan.FileScan | grep -i ".zip"
0x4150e690 100.0\Program Files\7-Zip\7zG.exe
0x42df6860      \Program Files\7-Zip\descript.ion
0x43c1c9a0      \Program Files\7-Zip\7-zip.dll
0x50223f20      \Windows\System32\es-ES\zipfldr.dll.mui
0x5675bdb0      \Windows\System32\zipfldr.dll
0x587a4430      \Program Files\7-Zip\7zFM.exe
0x6b7fccc0      \Program Files\7-Zip\7z.dll
0x7eff3db0      \Windows\System32\zipfldr.dll
0x7f4ff9c0      \ProgramData\Microsoft\Windows\Start Menu\Programs\7-Zip
0x7f52e070      \Users\wadmin\Documents\fichero.zip
0x7faddcc0      \Program Files\7-Zip\7z.dll
0x7fb2f690      \Program Files\7-Zip\7zG.exe
0x7fb45430      \Program Files\7-Zip\7zFM.exe
0x7fb7d9a0      \Program Files\7-Zip\7-zip.dll
0x7fb84f20      \Windows\System32\es-ES\zipfldr.dll.mui
0x7fd54860      \Program Files\7-Zip\descript.ion

┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$
```

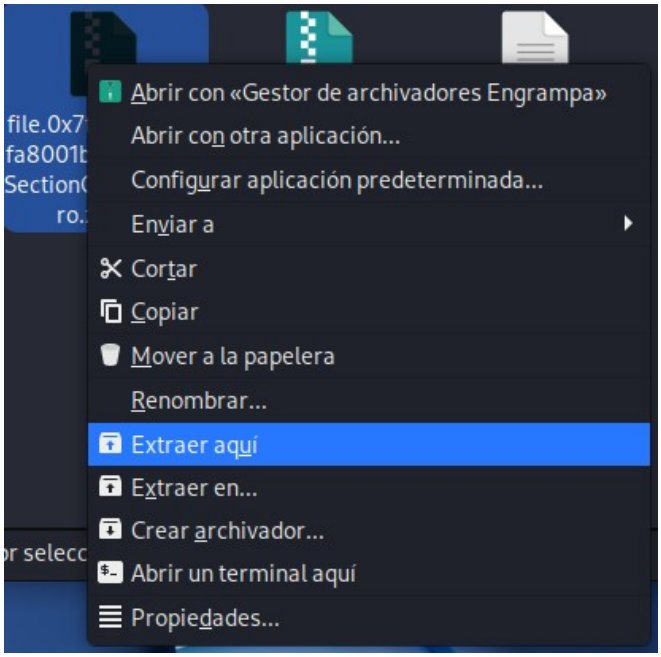
Ahora se realiza una extracción del ZIP para ver su contenido con el plugin *windows.dumpfiles.DumpFiles*, indicando la dirección FÍSICA en memoria del fichero que muestra la captura anterior:

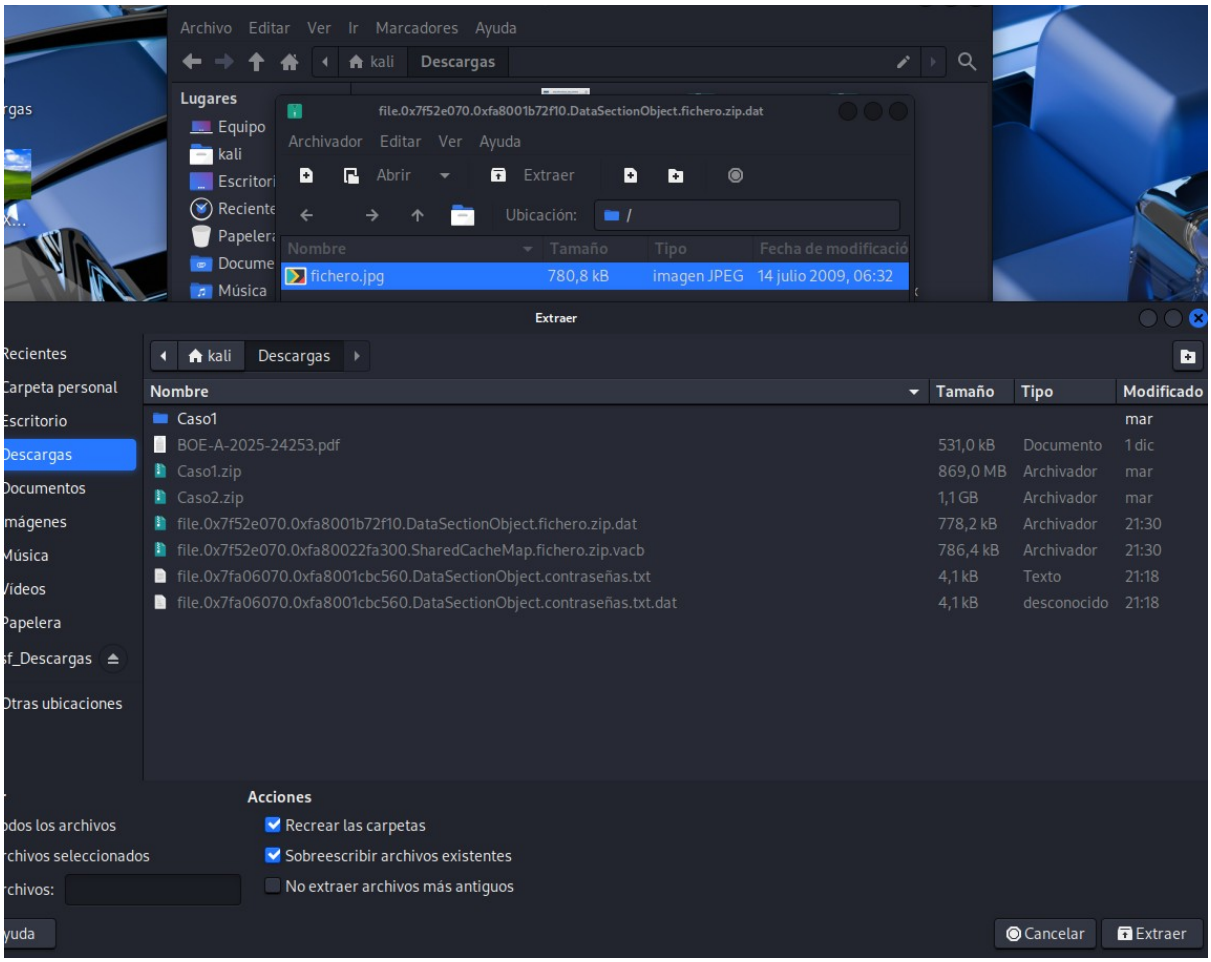
```
┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp windows.filescan.FileScan | grep -i ".zip"
0x4150e690 100.0\Program Files\7-Zip\7zG.exe
0x42df6860      \Program Files\7-Zip\descript.ion
0x43c1c9a0      \Program Files\7-Zip\7-zip.dll
0x50223f20      \Windows\System32\es-ES\zipfldr.dll.mui
0x5675bdb0      \Windows\System32\zipfldr.dll
0x587a4430      \Program Files\7-Zip\7zFM.exe
0x6b7fccc0      \Program Files\7-Zip\7z.dll
0x7eff3db0      \Windows\System32\zipfldr.dll
0x7f4ff9c0      \ProgramData\Microsoft\Windows\Start Menu\Programs\7-Zip
0x7f52e070      \Users\wadmin\Documents\fichero.zip
0x7faddcc0      \Program Files\7-Zip\7z.dll
0x7fb2f690      \Program Files\7-Zip\7zG.exe
0x7fb45430      \Program Files\7-Zip\7zFM.exe
0x7fb7d9a0      \Program Files\7-Zip\7-zip.dll
0x7fb84f20      \Windows\System32\es-ES\zipfldr.dll.mui
0x7fd54860      \Program Files\7-Zip\descript.ion

┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp -o /home/kali/Descargas windows.dumpfiles.DumpFiles --physaddr 0x7f52e070
```

Resultado: se ha extraído el fichero con éxito.

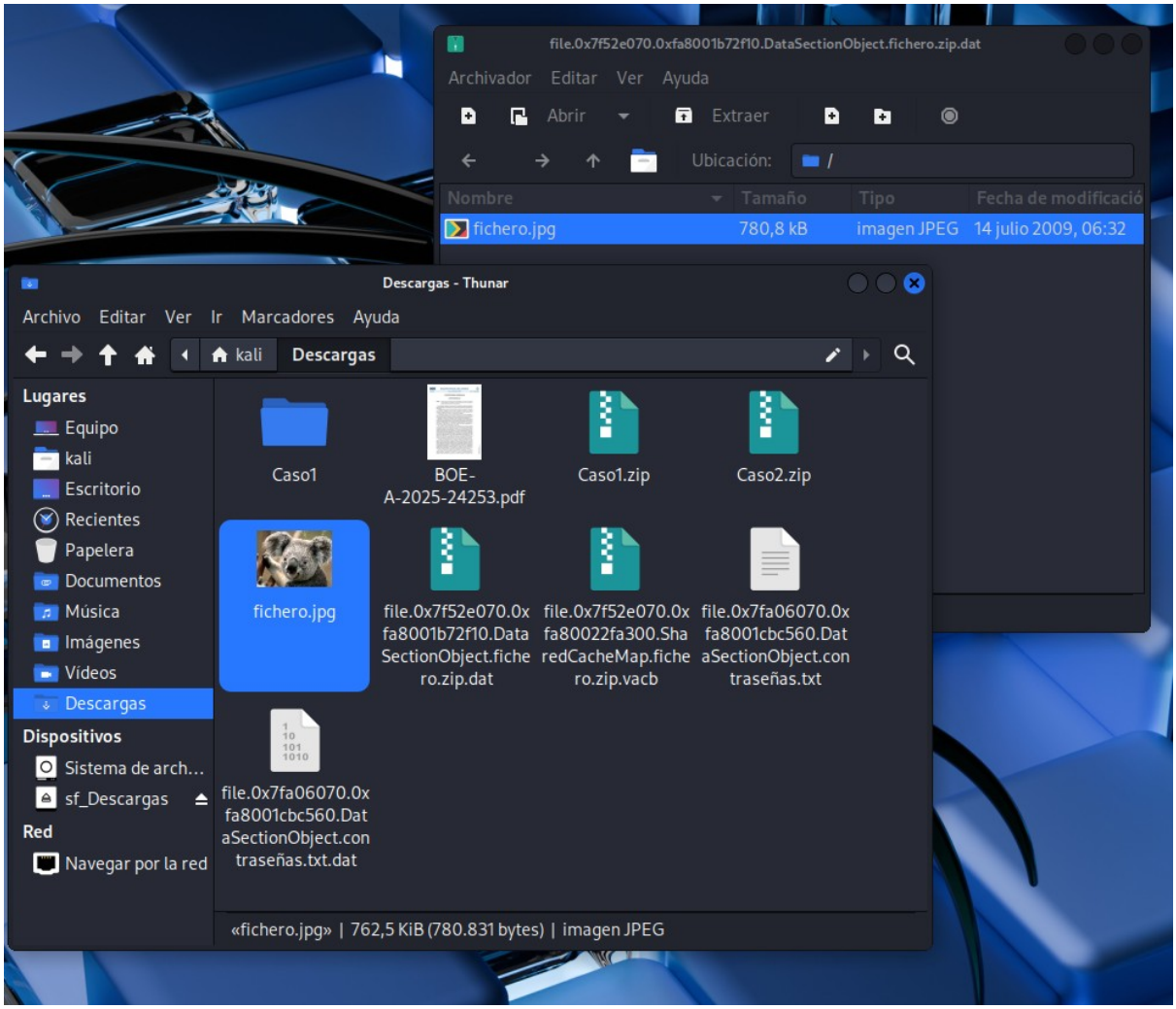
```
┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Descargas/Caso1/caso1Volatility.dmp -o /home/kali/Descargas windows.dumpfiles.DumpFiles --physaddr 0x7f52e070
Volatility 3 Framework 2.27.1
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0x7f52e070      fichero.zip     file.0x7f52e070.0x fa8001b72f10.DataSectionObject.fichero.zip.dat
SharedCacheMap  0x7f52e070      fichero.zip     file.0x7f52e070.0x fa80022fa300.SharedCacheMap.fichero.zip.vacb

┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$
```

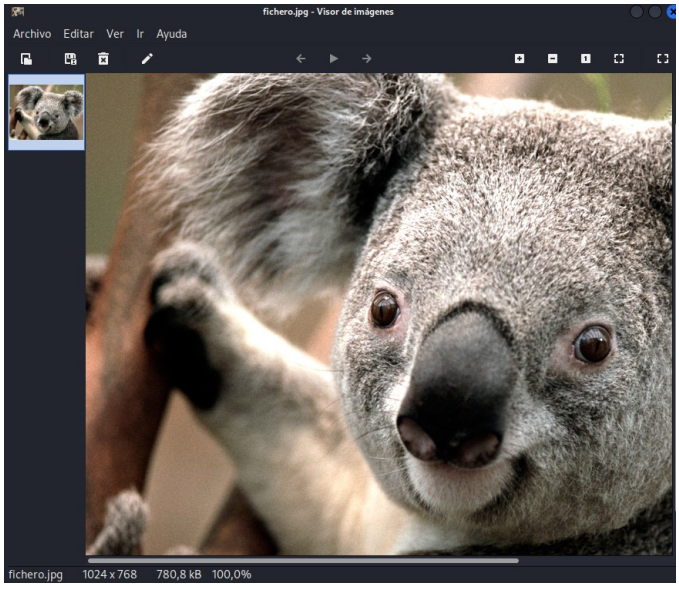
Vamos a la carpeta */Descargas* de nuestro equipo ya que es la ruta destino que hemos indicado y extraemos el fichero:





Ahí vemos el animal que se encuentra dentro del zip, es un **koala.**



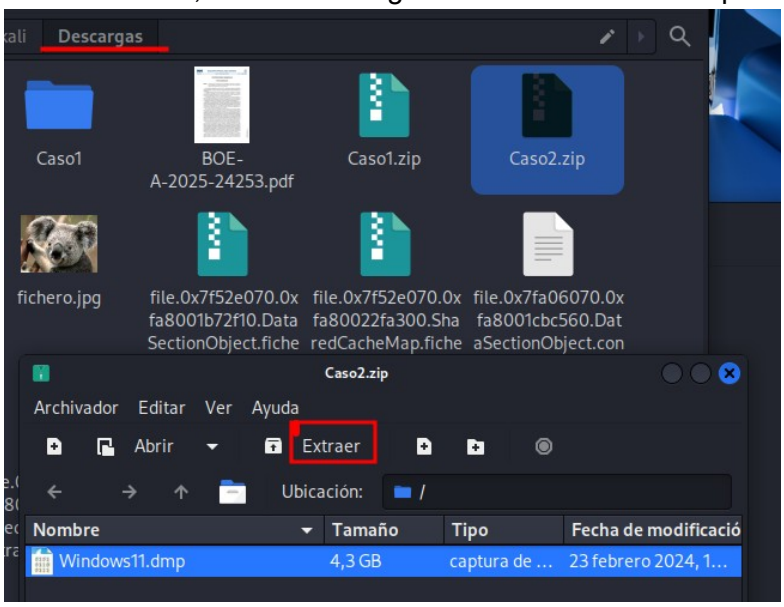


Caso 2 : Volcado de memoria RAM de un sistema Windows 11

El hash SHA256 del volcado de memoria de este caso es:
a1d84fe21f42cd8073b8630c91494992303b84061b493f91ccf28333cecc7040

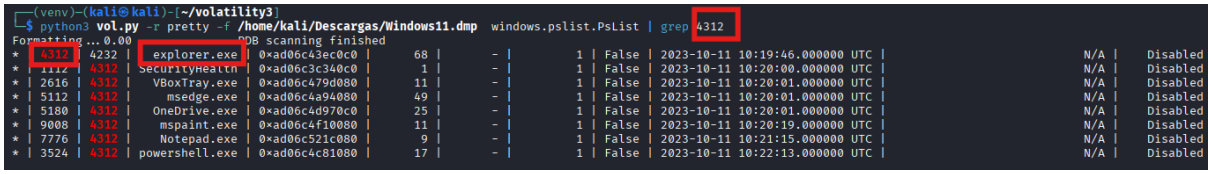
1. ¿Cuál es el PID del proceso del Microsoft Paint? ¿Cuál es el nombre de su proceso padre?

Antes de nada, extraer la imagen de Windows 11 del zip.



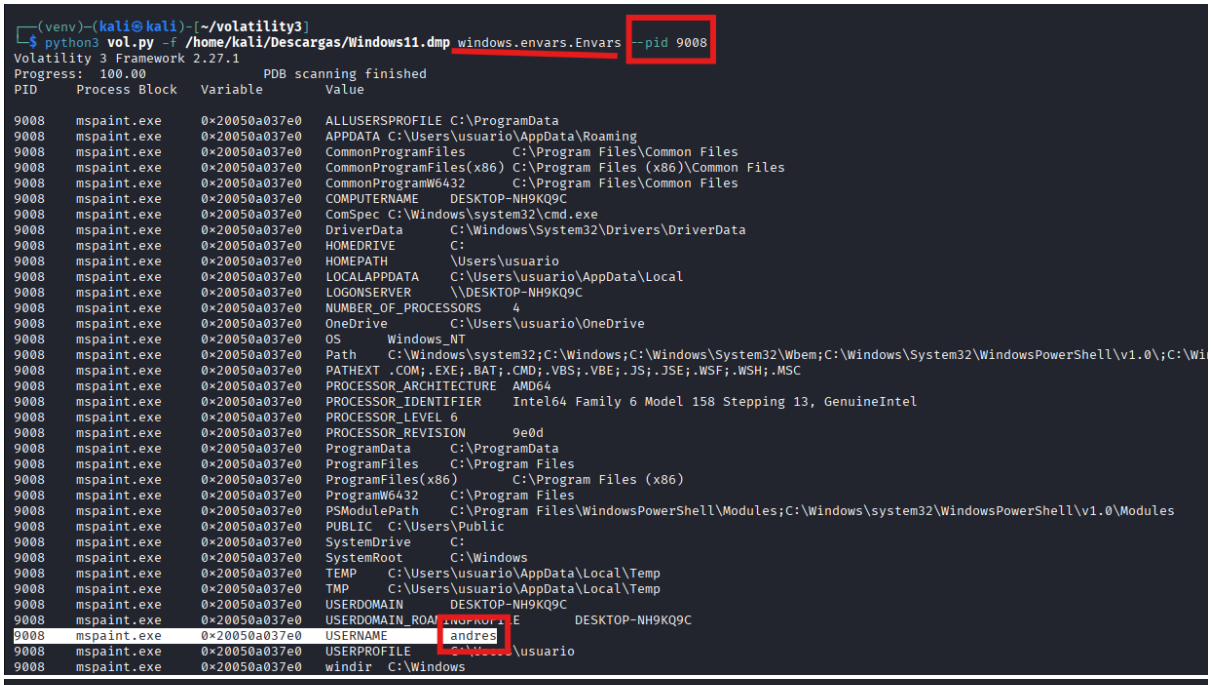
Usando el plugin *PsList* y *grep* obtenemos que el PID del proceso del Microsoft Paint es 9008.

Con el PID de su proceso padre que lo creó(PPID) que es 4312 vamos a filtrar con *grep* para saber el nombre. El nombre del proceso es **explorer.exe.**

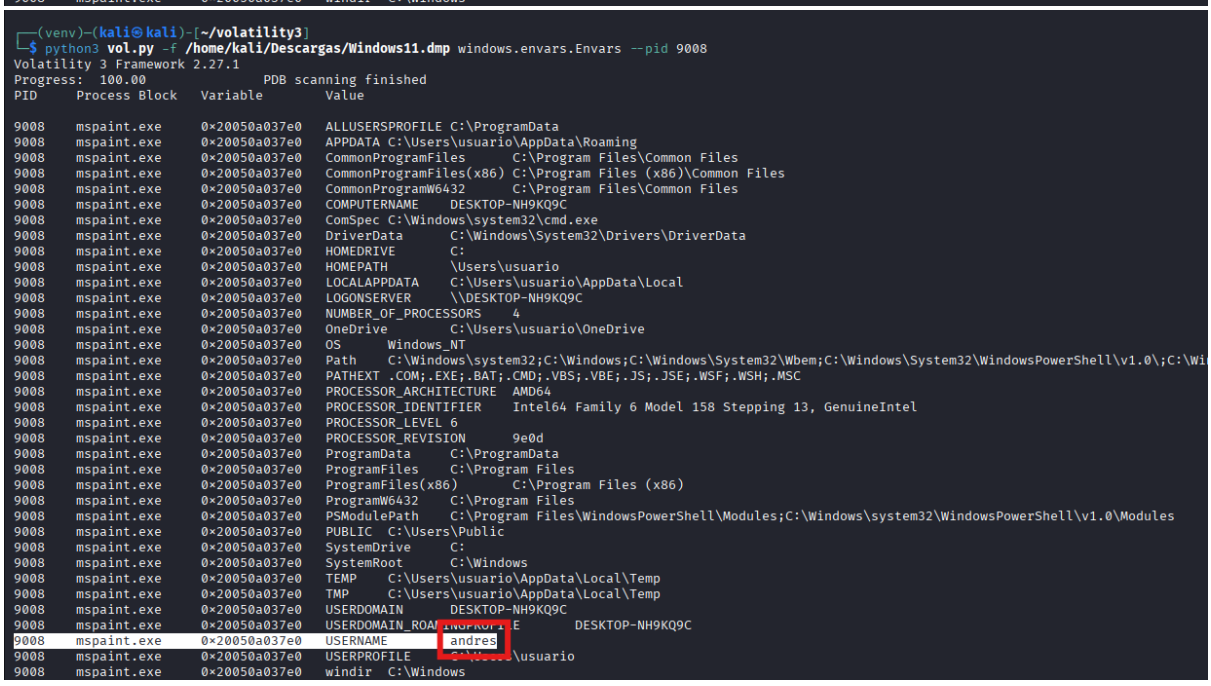


2. ¿Cuál es el nombre del usuario (es un nombre de persona) que está ejecutando el Microsoft Paint?

El nombre del usuario que está ejecutando el Microsoft Paint es **andres**. Una vez ubicado el PID de Microsoft Paint en el ejercicio anterior (PID=9008), hay que usar el plugin *windows.envars.Envars* indicando a mayores dicho PID 9008. En la captura se ve en la variable USERNAME andres , lo que confirma al 100% que el paint fue ejecutado por el usuario andres.

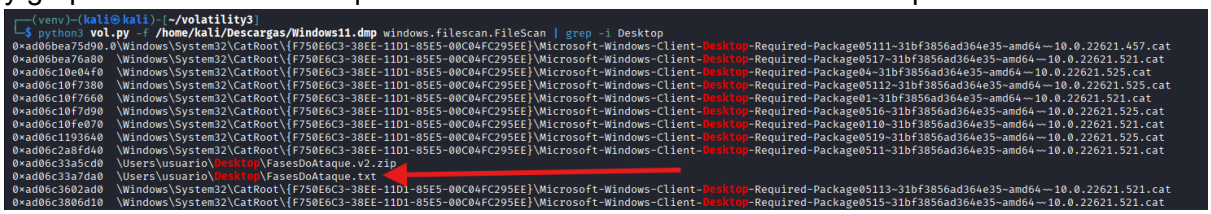


```
┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Descargas/Windows11.dmp windows.envars.Envars --pid 9008
Volatility 3 Framework 2.27.1
Progress:  100.00               PDB scanning finished
PID     Process Block   Variable        Value

9008    mspaint.exe     0×20050a037e0   ALLUSERSPROFILE C:\ProgramData
9008    mspaint.exe     0×20050a037e0   APPDATA C:\Users\usuario\AppData\Roaming
9008    mspaint.exe     0×20050a037e0   CommonProgramFiles      C:\Program Files\Common Files
9008    mspaint.exe     0×20050a037e0   CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
9008    mspaint.exe     0×20050a037e0   CommonProgramW6432      C:\Program Files\Common Files
9008    mspaint.exe     0×20050a037e0   COMPUTERNAME    DESKTOP-NH9KQ9C
9008    mspaint.exe     0×20050a037e0   ComSpec C:\Windows\system32\cmd.exe
9008    mspaint.exe     0×20050a037e0   DriverData      C:\Windows\System32\Drivers\DriverData
9008    mspaint.exe     0×20050a037e0   HOMEDRIVE       C:
9008    mspaint.exe     0×20050a037e0   HOMEPATH        \Users\usuario
9008    mspaint.exe     0×20050a037e0   LOCALAPPDATA    C:\Users\usuario\AppData\Local
9008    mspaint.exe     0×20050a037e0   LOGONSERVER     \\DESKTOP-NH9KQ9C
9008    mspaint.exe     0×20050a037e0   NUMBER_OF_PROCESSORS    4
9008    mspaint.exe     0×20050a037e0   OneDrive        C:\Users\usuario\OneDrive
9008    mspaint.exe     0×20050a037e0   OS      Windows_NT
9008    mspaint.exe     0×20050a037e0   Path    C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Wi
9008    mspaint.exe     0×20050a037e0   PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
9008    mspaint.exe     0×20050a037e0   PROCESSOR_ARCHITECTURE  AMD64
9008    mspaint.exe     0×20050a037e0   PROCESSOR_IDENTIFIER    Intel64 Family 6 Model 158 Stepping 13, GenuineIntel
9008    mspaint.exe     0×20050a037e0   PROCESSOR_LEVEL 6
9008    mspaint.exe     0×20050a037e0   PROCESSOR_REVISION      9e0d
9008    mspaint.exe     0×20050a037e0   ProgramData     C:\ProgramData
9008    mspaint.exe     0×20050a037e0   ProgramFiles    C:\Program Files
9008    mspaint.exe     0×20050a037e0   ProgramFiles(x86)       C:\Program Files (x86)
9008    mspaint.exe     0×20050a037e0   ProgramW6432    C:\Program Files
9008    mspaint.exe     0×20050a037e0   PSModulePath    C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
9008    mspaint.exe     0×20050a037e0   PUBLIC  C:\Users\Public
9008    mspaint.exe     0×20050a037e0   SystemDrive     C:
9008    mspaint.exe     0×20050a037e0   SystemRoot      C:\Windows
9008    mspaint.exe     0×20050a037e0   TEMP    C:\Users\usuario\AppData\Local\Temp
9008    mspaint.exe     0×20050a037e0   TMP     C:\Users\usuario\AppData\Local\Temp
9008    mspaint.exe     0×20050a037e0   USERDOMAIN      DESKTOP-NH9KQ9C
9008    mspaint.exe     0×20050a037e0   USERDOMAIN_ROAMINGPROFILE       DESKTOP-NH9KQ9C
9008    mspaint.exe     0×20050a037e0   USERNAME        andres
9008    mspaint.exe     0×20050a037e0   USERPROFILE     C:\Users\usuario
9008    mspaint.exe     0×20050a037e0   windir  C:\Windows
```

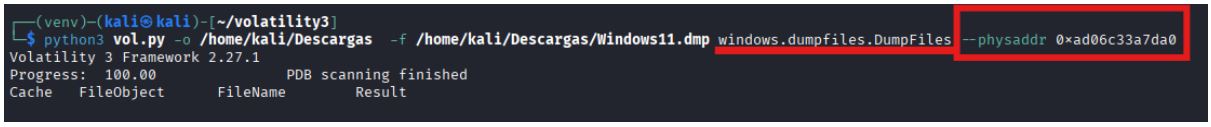


```
┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Descargas/Windows11.dmp windows.envars.Envars --pid 9008
Volatility 3 Framework 2.27.1
Progress:  100.00               PDB scanning finished
PID     Process Block   Variable        Value

9008    mspaint.exe     0×20050a037e0   ALLUSERSPROFILE C:\ProgramData
9008    mspaint.exe     0×20050a037e0   APPDATA C:\Users\usuario\AppData\Roaming
9008    mspaint.exe     0×20050a037e0   CommonProgramFiles      C:\Program Files\Common Files
9008    mspaint.exe     0×20050a037e0   CommonProgramFiles(x86) C:\Program Files (x86)\Common Files
9008    mspaint.exe     0×20050a037e0   CommonProgramW6432      C:\Program Files\Common Files
9008    mspaint.exe     0×20050a037e0   COMPUTERNAME    DESKTOP-NH9KQ9C
9008    mspaint.exe     0×20050a037e0   ComSpec C:\Windows\system32\cmd.exe
9008    mspaint.exe     0×20050a037e0   DriverData      C:\Windows\System32\Drivers\DriverData
9008    mspaint.exe     0×20050a037e0   HOMEDRIVE       C:
9008    mspaint.exe     0×20050a037e0   HOMEPATH        \Users\usuario
9008    mspaint.exe     0×20050a037e0   LOCALAPPDATA    C:\Users\usuario\AppData\Local
9008    mspaint.exe     0×20050a037e0   LOGONSERVER     \\DESKTOP-NH9KQ9C
9008    mspaint.exe     0×20050a037e0   NUMBER_OF_PROCESSORS    4
9008    mspaint.exe     0×20050a037e0   OneDrive        C:\Users\usuario\OneDrive
9008    mspaint.exe     0×20050a037e0   OS      Windows_NT
9008    mspaint.exe     0×20050a037e0   Path    C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Wi
9008    mspaint.exe     0×20050a037e0   PATHEXT .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
9008    mspaint.exe     0×20050a037e0   PROCESSOR_ARCHITECTURE  AMD64
9008    mspaint.exe     0×20050a037e0   PROCESSOR_IDENTIFIER    Intel64 Family 6 Model 158 Stepping 13, GenuineIntel
9008    mspaint.exe     0×20050a037e0   PROCESSOR_LEVEL 6
9008    mspaint.exe     0×20050a037e0   PROCESSOR_REVISION      9e0d
9008    mspaint.exe     0×20050a037e0   ProgramData     C:\ProgramData
9008    mspaint.exe     0×20050a037e0   ProgramFiles    C:\Program Files
9008    mspaint.exe     0×20050a037e0   ProgramFiles(x86)       C:\Program Files (x86)
9008    mspaint.exe     0×20050a037e0   ProgramW6432    C:\Program Files
9008    mspaint.exe     0×20050a037e0   PSModulePath    C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
9008    mspaint.exe     0×20050a037e0   PUBLIC  C:\Users\Public
9008    mspaint.exe     0×20050a037e0   SystemDrive     C:
9008    mspaint.exe     0×20050a037e0   SystemRoot      C:\Windows
9008    mspaint.exe     0×20050a037e0   TEMP    C:\Users\usuario\AppData\Local\Temp
9008    mspaint.exe     0×20050a037e0   TMP     C:\Users\usuario\AppData\Local\Temp
9008    mspaint.exe     0×20050a037e0   USERDOMAIN      DESKTOP-NH9KQ9C
9008    mspaint.exe     0×20050a037e0   USERDOMAIN_ROAMINGPROFILE       DESKTOP-NH9KQ9C
9008    mspaint.exe     0×20050a037e0   USERNAME        andres
9008    mspaint.exe     0×20050a037e0   USERPROFILE     C:\Users\usuario
9008    mspaint.exe     0×20050a037e0   windir  C:\Windows
```

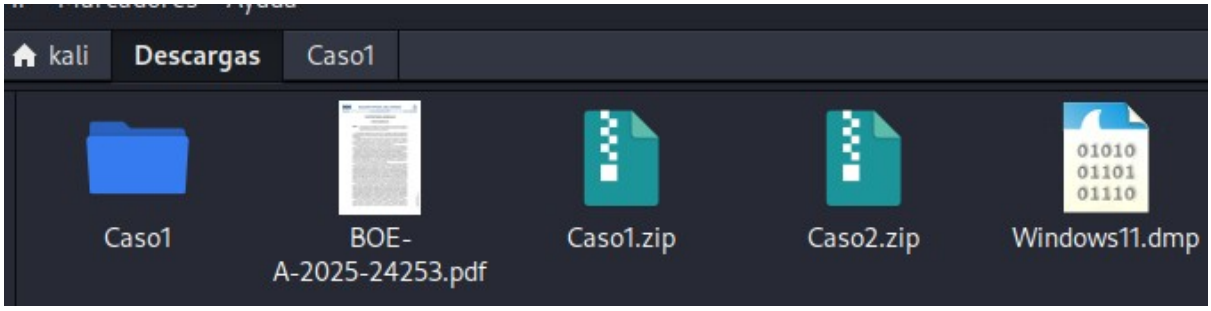
3. En el Escritorio del usuario usuario existe un fichero de texto con las instrucciones para llevar a cabo unas gamberradas. ¿De qué barrio de Ferrol es el cómplice del organizador?
Lo primero a realizar es localizar archivos en el Escritorio del usuario usuario, con FileScan y grep. El fichero de texto que llama la atención es este: FasesDoAtaque.txt



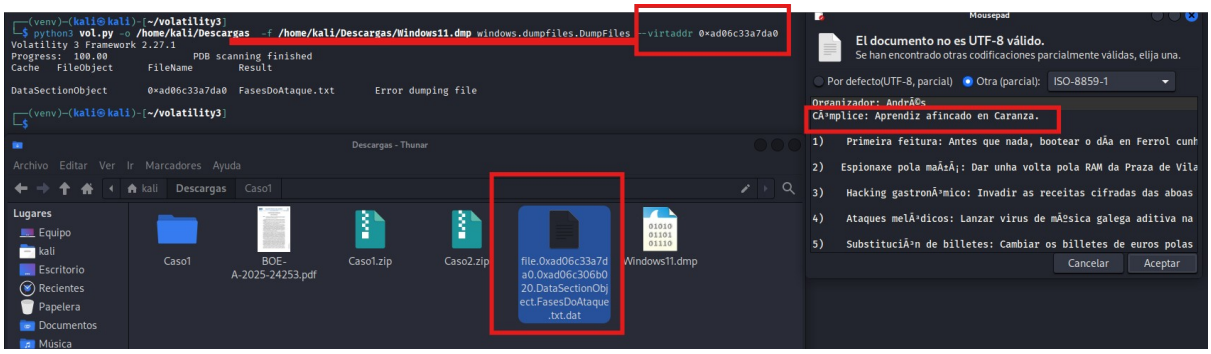
Seguidamente extrae el archivo para leerlo, con el plugin DumpFiles e indicando el offset físico del fichero de texto sospechoso, que es 0xad06c33a7da0.



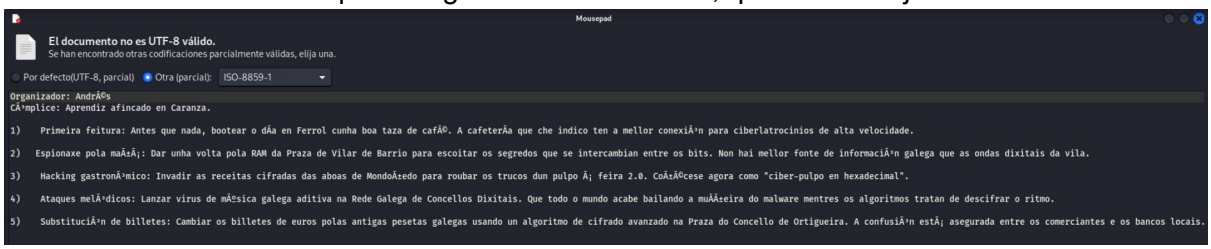
Debería aparecer debajo de la última línea el nombre del fichero, lo que ocurre es que esa dirección física no debe ser un fichero válido y por ello no aparece en la carpeta de Descargas.



Probamos la siguiente alternativa: igual la dirección correcta que indica FileScan es la virtual, y efectivamente se extrae con éxito el fichero.

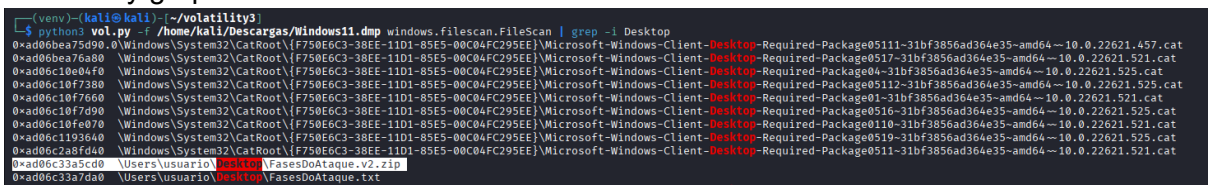


Lo abrimos y ahí está el barrio de Ferrol del que es el cómplice del organizador, el barrio de **Caranza.** Además se ve que el organizador es Andrés, quien antes ejecutó Microsoft Paint.

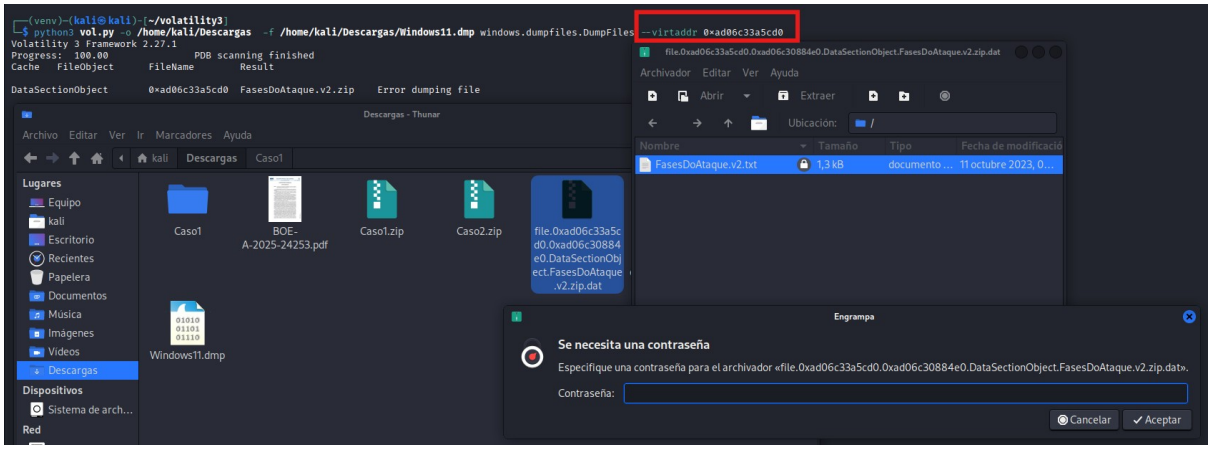


4. La última versión del plan, que incluye el último paso a realizar, se encuentra en un fichero ZIP cifrado en el Escritorio del usuario. No es posible encontrar la clave de descifrado en la memoria pero, ¿eres capaz de descifrar el contenido y saber cuál será el último de los pasos que piensan dar?

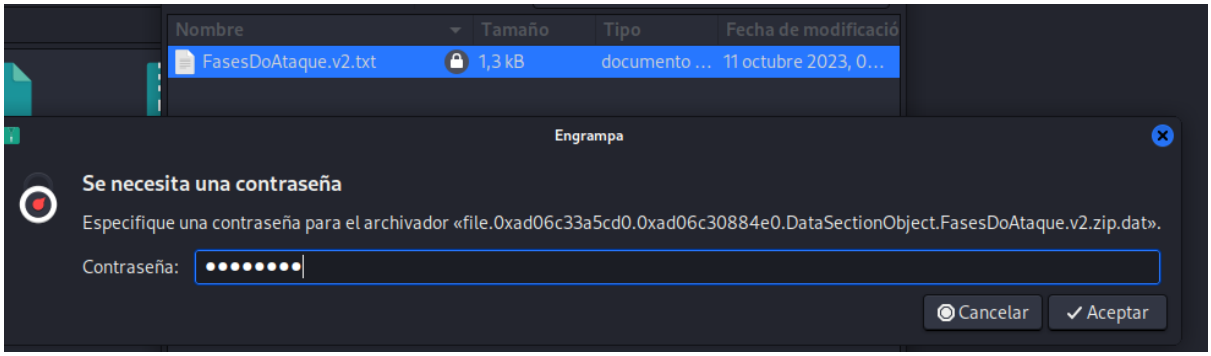
Primero se localiza el ZIP cifrado y su PID en el Escritorio del usuario, como antes con FileScan y grep:

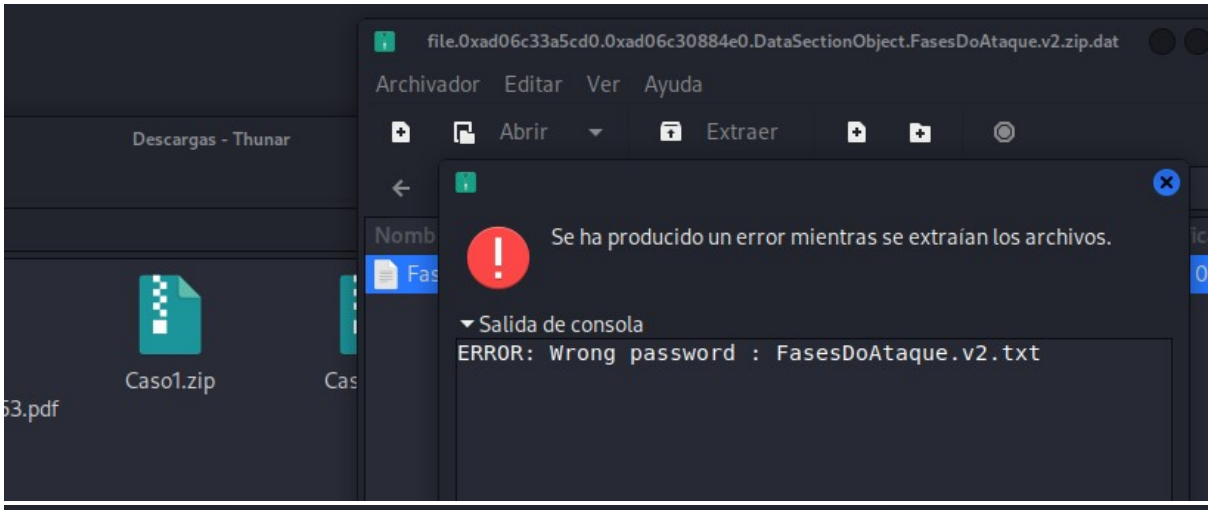


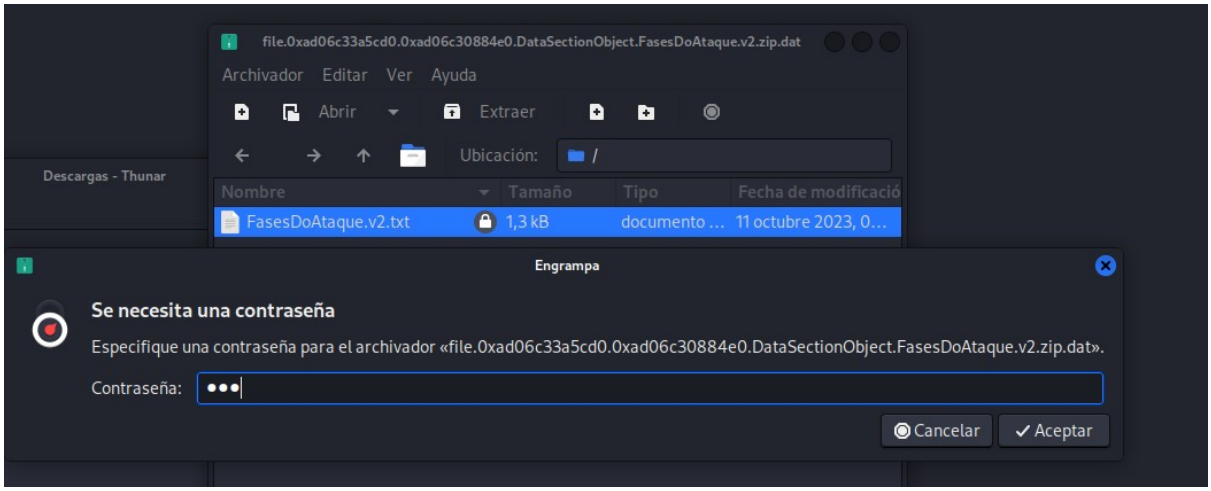
Seguidamente extrae el archivo para leerlo, con el plugin DumpFiles e indicando su offset virtual 0xad06c33a5cd0. Aunque aparece “Error dumping file” puede verse que sí se extrae correctamente.



Se prueba a fuerza bruta manualmente con las contraseñas abc123, abc123., abc123..,123abc, abc1…y se finaliza habiendo probado la combinación abc, la contraseña del fichero.







Aquí vemos todo el plan con los últimos pasos que piensan dar: