DÍA D - EJERCICIO FINAL - CTF ANÁLISIS FORENSE

- Canal Slack: `cs-ft-sep-23`

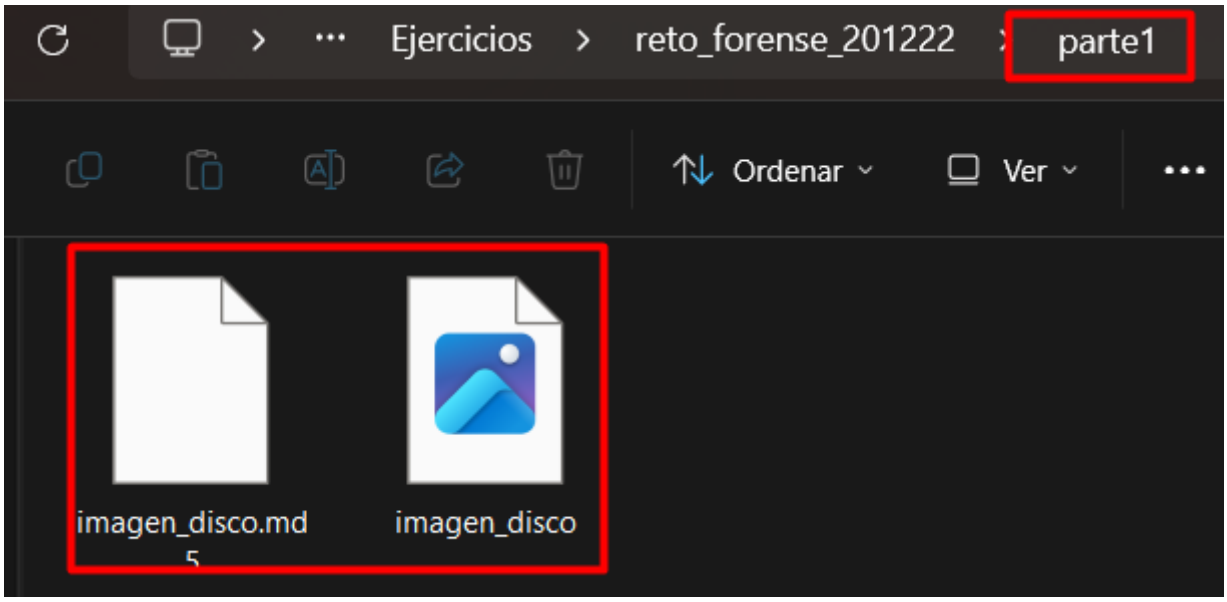
Prerrequisitos

- Descargar "reto_forense_201222.zip" de: Drive > Máquinas Virtuales > Blue Team
- Password: sleuth
- El reto forense consistente en 3 partes:
    - 1.Análisis de una imagen de disco
    - 2.Análisis de una captura de tráfico
    - 3.Análisis de un volcado de memoria
- Puntaje total: 450 puntos
- Son tres volcados de tres situaciones diferentes, sacar la siguiente información necesaria para el coordinador del CSIRT (tu profe!).

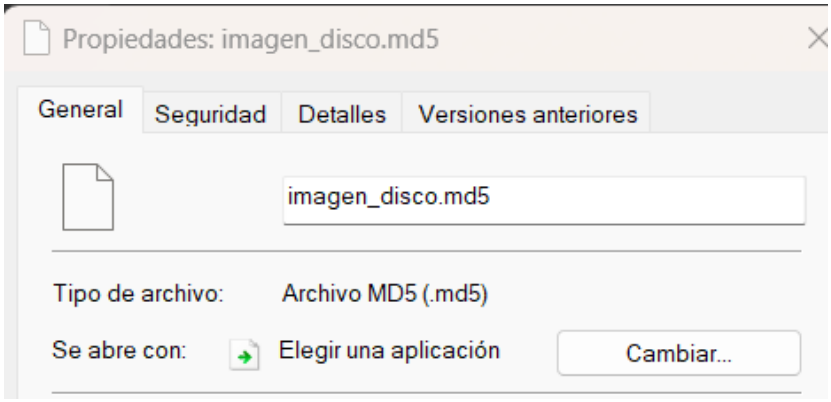
Cuestionario para el CSIRT

- PARTE 1. ANALISIS DE IMAGEN DE DISCO - 100 puntos
    - 1.¿Qué tipo de sistema de ficheros tiene la imagen? - 10 puntos

      Una vez hemos descargado el archivo .zip descomprimimos la carpeta y obtenemos los siguientes archivos

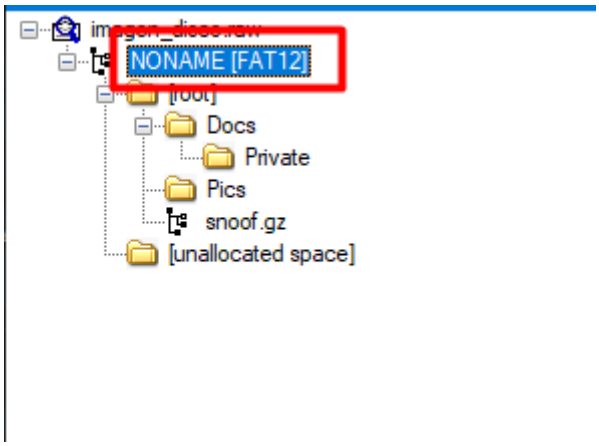


      El primer archivo es un .MD5



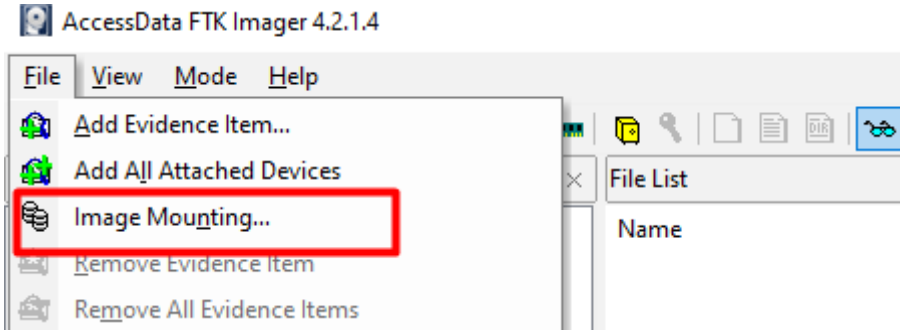
Y el segundo es un .raw

Una vez montada la imagen podemos observar que el sistema de ficheros es FAT

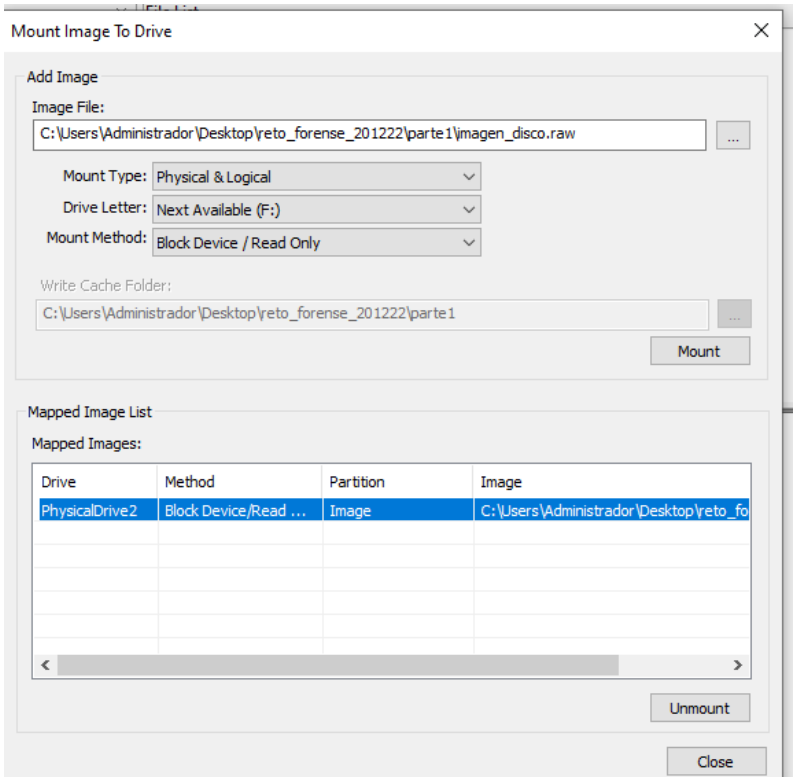


- 2.¿Cuandos directorios hay dentro de la imagen? - 10 puntos

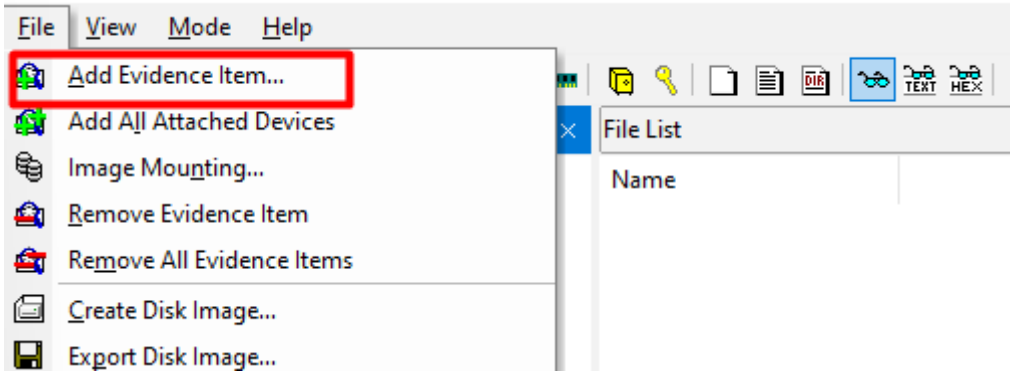
  Para esto debemos montar la imagen con FTK



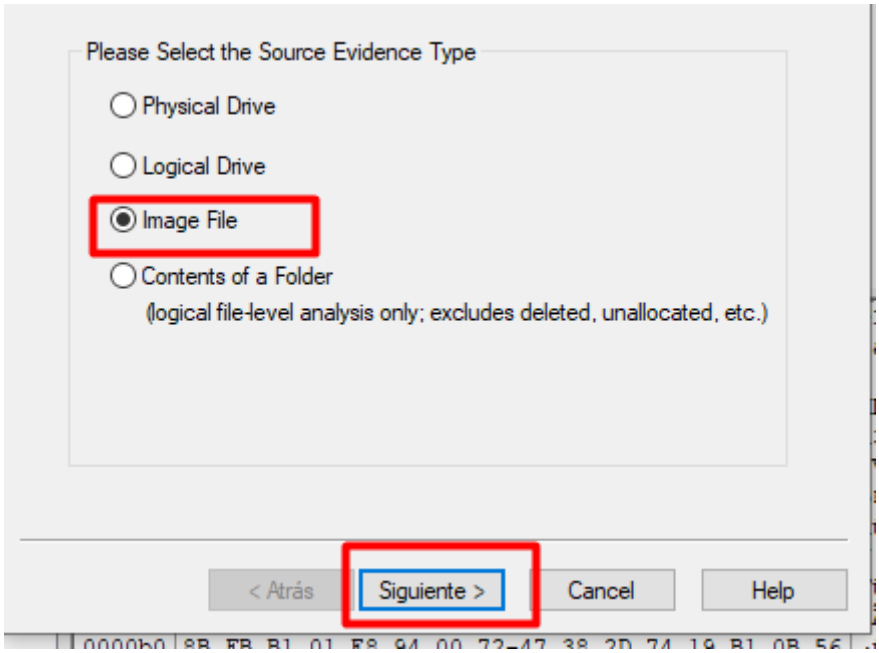
Seleccionamos la imagen y la montamos



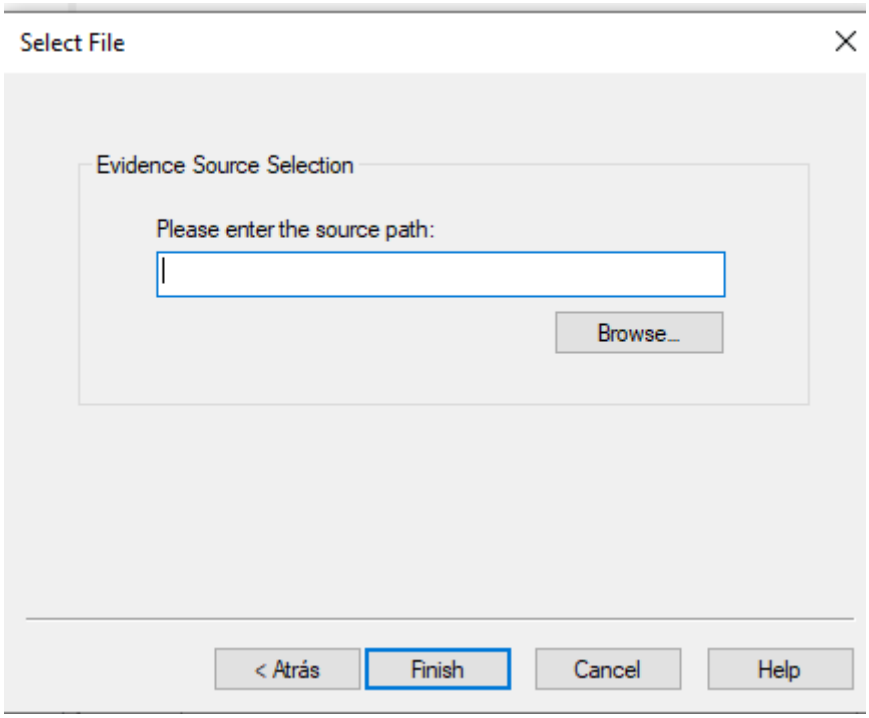
Una vez salimos hacemos lo siguiente



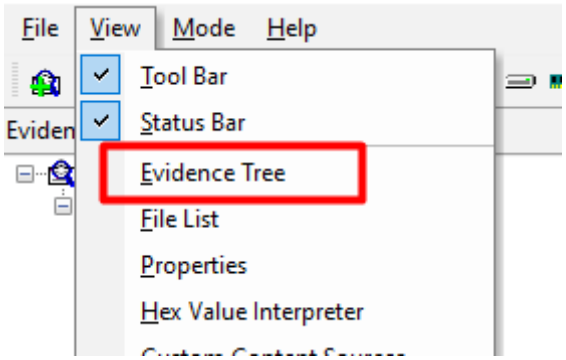
Seleccionamos Image file



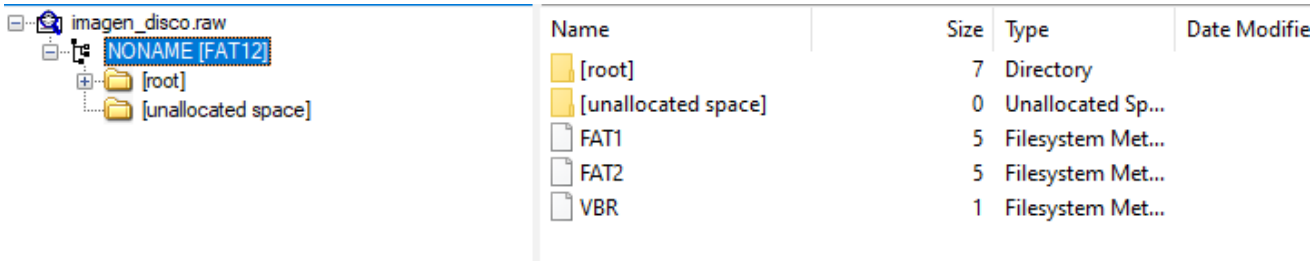
Y después seleccionamos el archivo imagen



Finalizas y visualizamos el árbol de evidencias

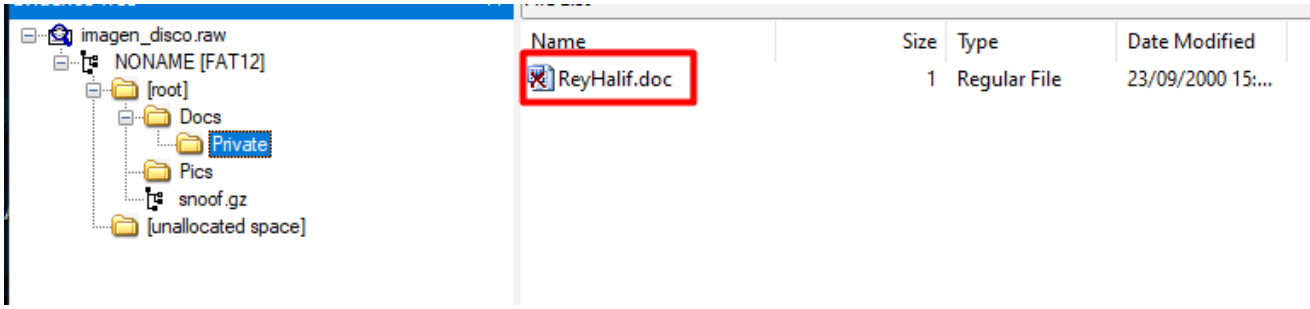


Como resultado podemos observar los siguiente directorios y archivos



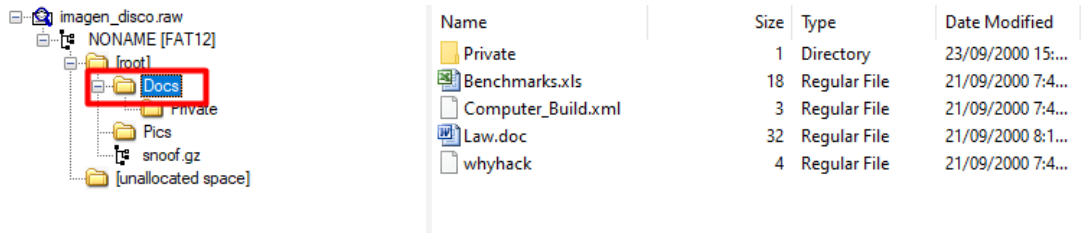
- 3.¿Cuantos archivos borrados hay? - 10 puntos

  Hemos encontrado uno



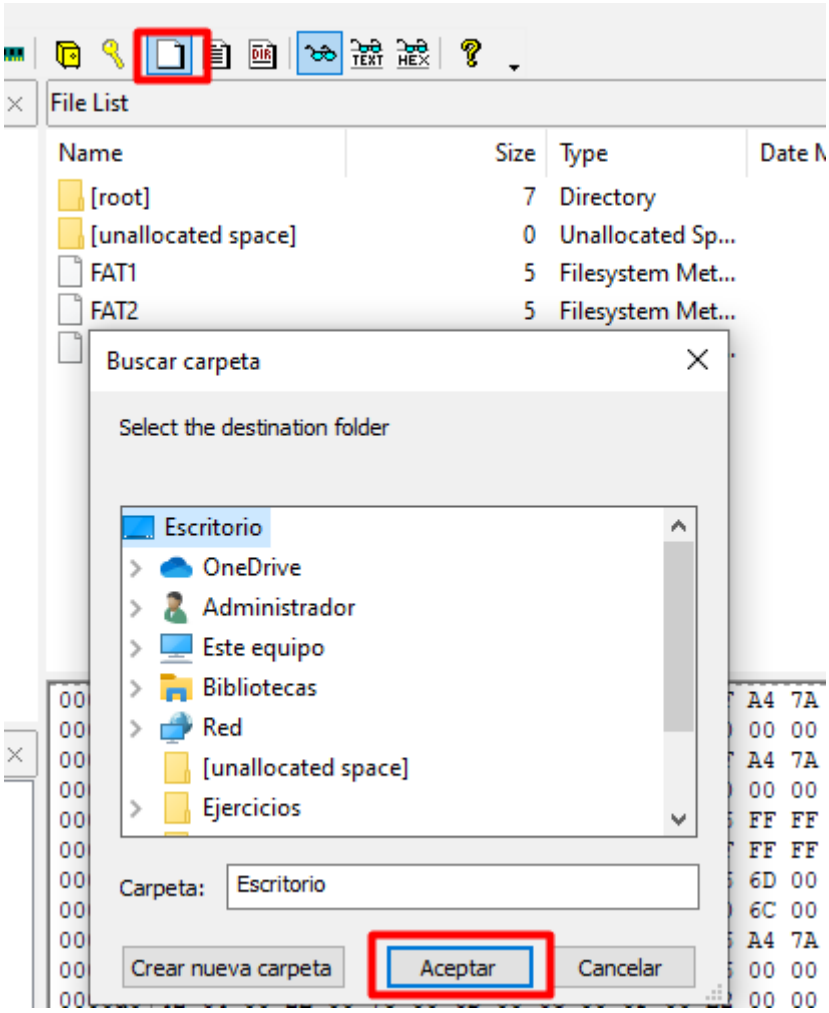
- 4.Monta la imagen para poder acceder a los ficheros. - 20 puntos

  Este paso está explicado en el anterior prácticamente.

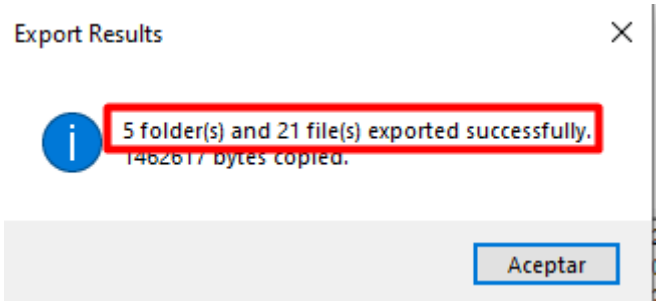


- 5. ¿Cuántos archivos hay en la imagen? - 20 puntos

  Para esto exportamos la carpeta en el escritorio

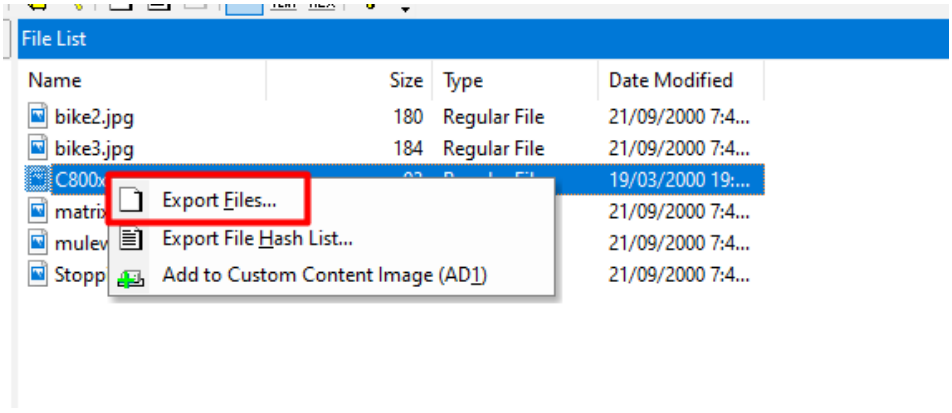


Y una vez le damos a aceptar nos sale la información que había dentro

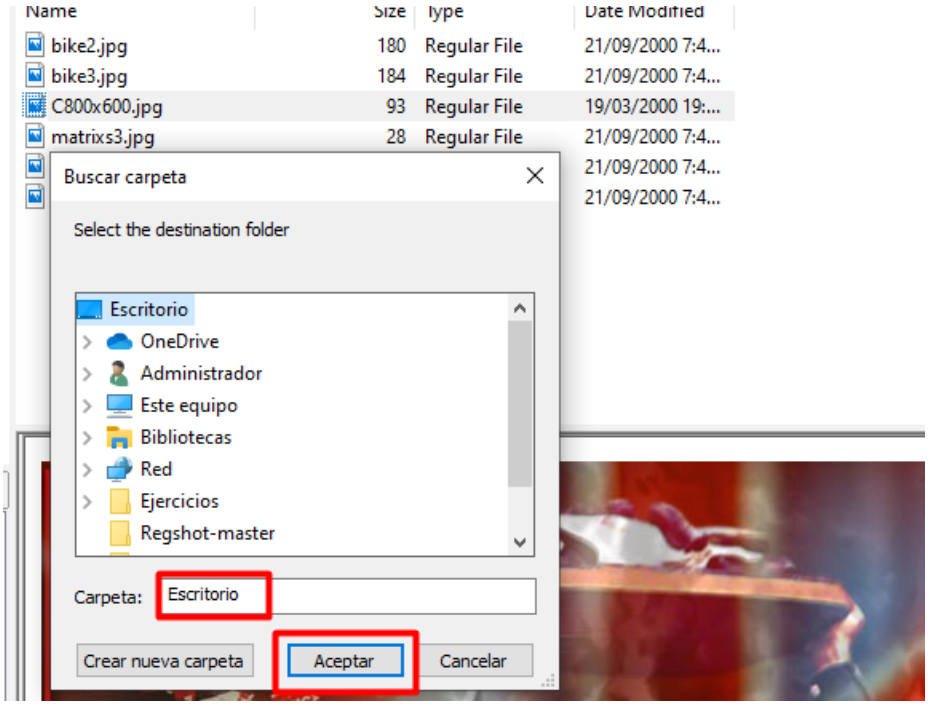


- 6.Descarga tres de las imágenes disponibles. - 30 puntos

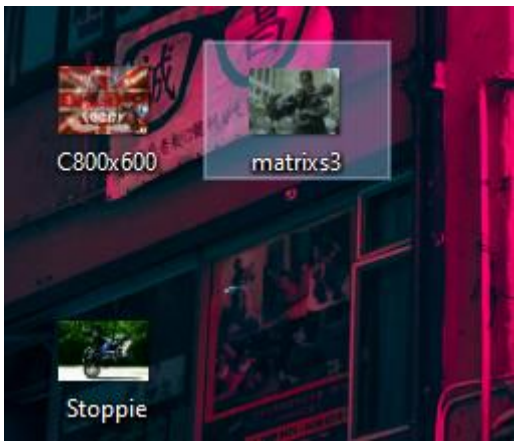
  Para poder hacer esto damos click derecho en la imagen que queremos descargar y exportamos el archivo



Seleccionamos el destino de descarga y aceptamos

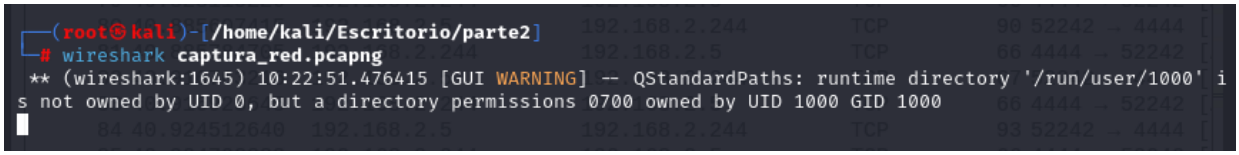


Este mismo procedimiento lo repetimos 3 veces y lo tendríamos

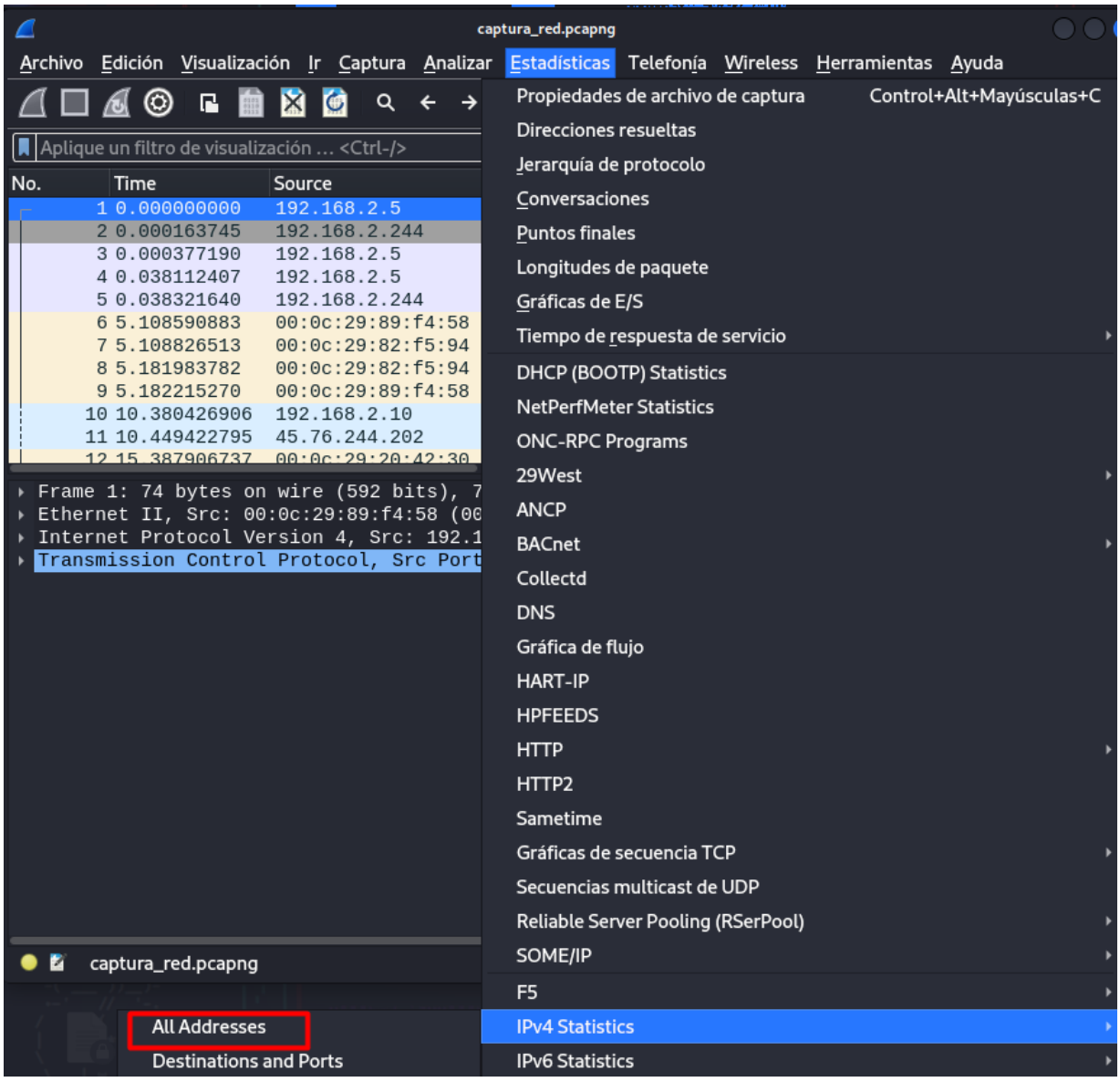


- PARTE 2. ANALISIS DE CAPTURA DE TRAFICO - 150 puntos
    - 1.¿Cuales son las dos IPs que estan en la comunicación? - 10 puntos

      Para poder hacer esto nos dirigimos a nuestra Kali y seleccionamos el archivo .pcapng



      Una vez dentro vamos a la pestaña de estadísticas

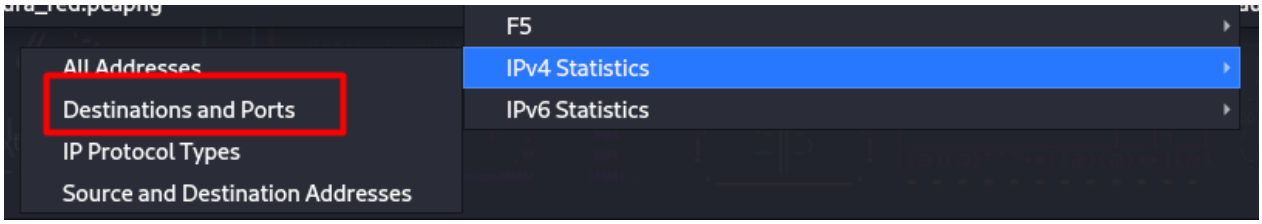


      Una vez dentro vemos diferentes IP’s pero las que concentran todo el trafico son principalmente dos

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percei	Burst Rate	Burst Start
All Addresses	240				0,0010	100%	0,5200	41,922
192.168.2.5	211				0,0009	87,92%	0,5200	41,922
192.168.2.244	191				0,0008	79,58%	0,5200	41,922
91.189.91.38	30				0,0001	12,50%	0,1300	23,641
35.224.99.156	10				0,0000	4,17%	0,0900	130,390
35.222.85.5	10				0,0000	4,17%	0,0900	213,575
192.168.2.243	10				0,0000	4,17%	0,0900	130,390
192.168.2.20	4				0,0000	1,67%	0,0200	52,122
192.168.2.1	4				0,0000	1,67%	0,0200	212,575
192.168.2.10	3				0,0000	1,25%	0,0200	10,380
45.76.244.202	2				0,0000	0,83%	0,0200	10,380
216.228.192.52	2				0,0000	0,83%	0,0200	165,543
171.66.97.126	2				0,0000	0,83%	0,0200	52,122
192.168.2.2	1				0,0000	0,42%	0,0100	23,052

- 2.¿A qué puerto se están conectando? - 10 puntos

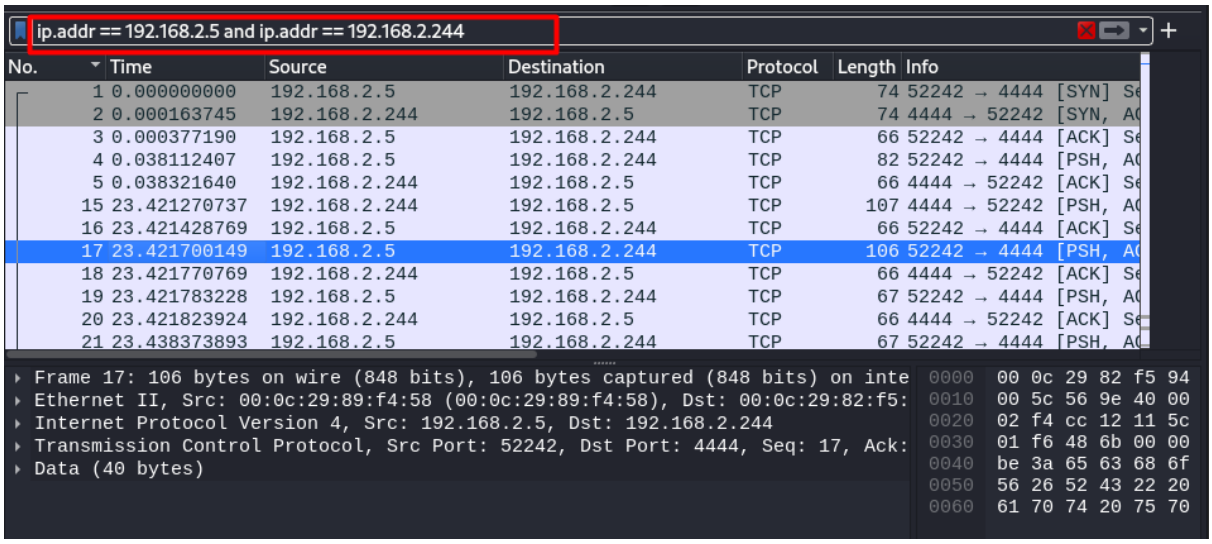
  Para esto volvemos a las estadísticas



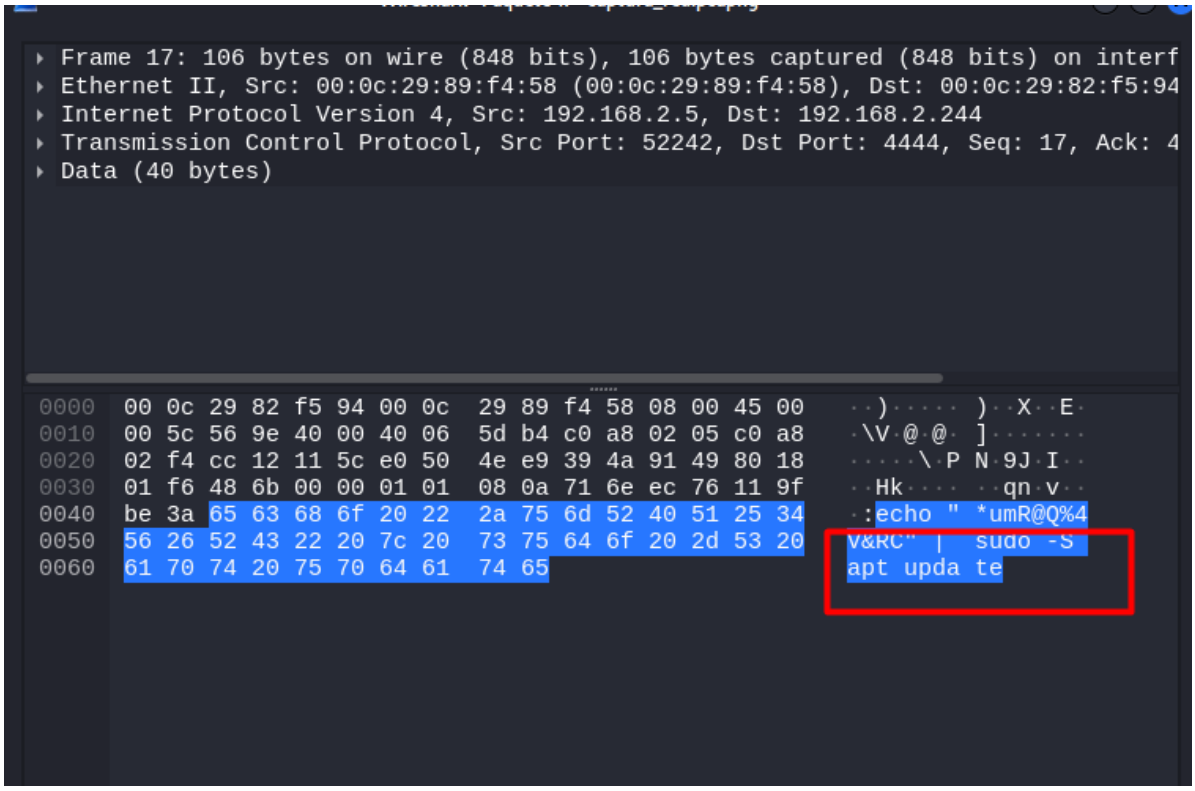
  Una vez dentro tenemos como resultado lo siguiente

- 3.¿Qué comando se ha realizado? - 10 puntos

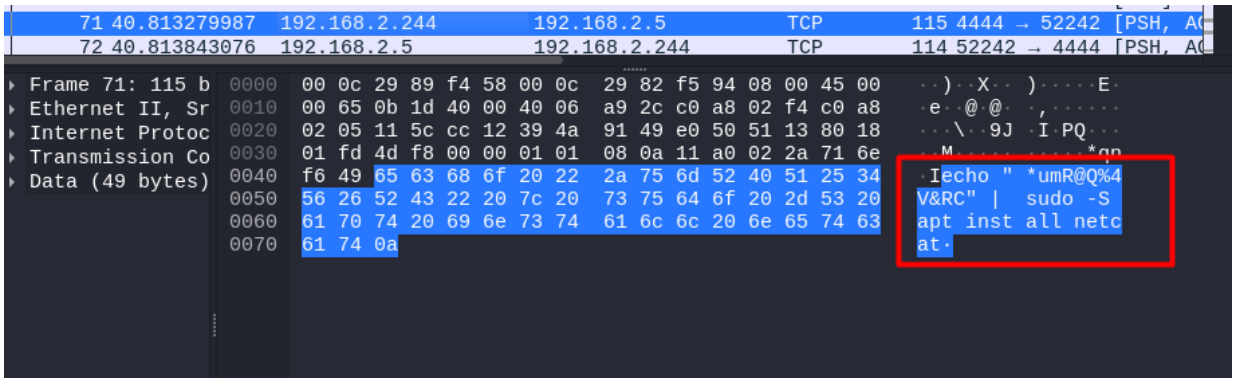
  Para esto realizamos una búsqueda con filtros



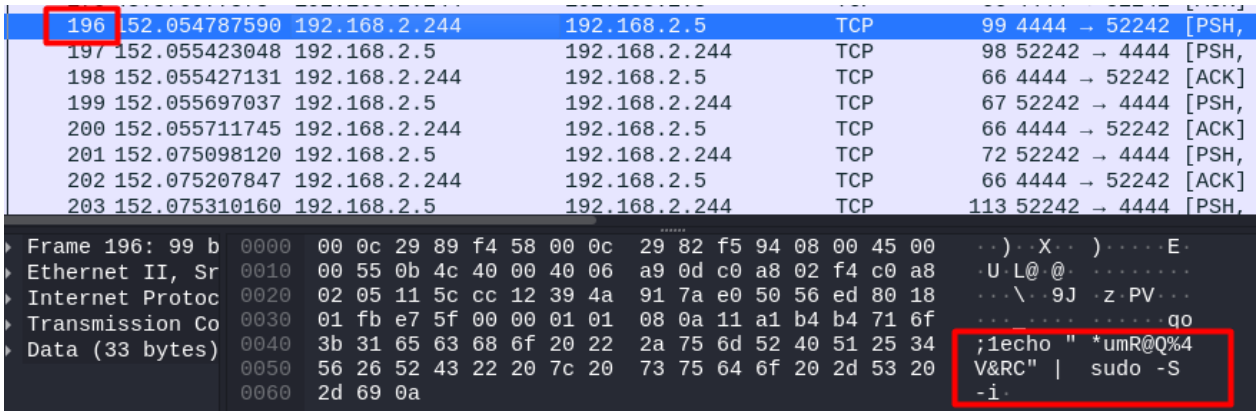
Luego nos movemos por los paquetes y obtenemos lo siguiente en el 17



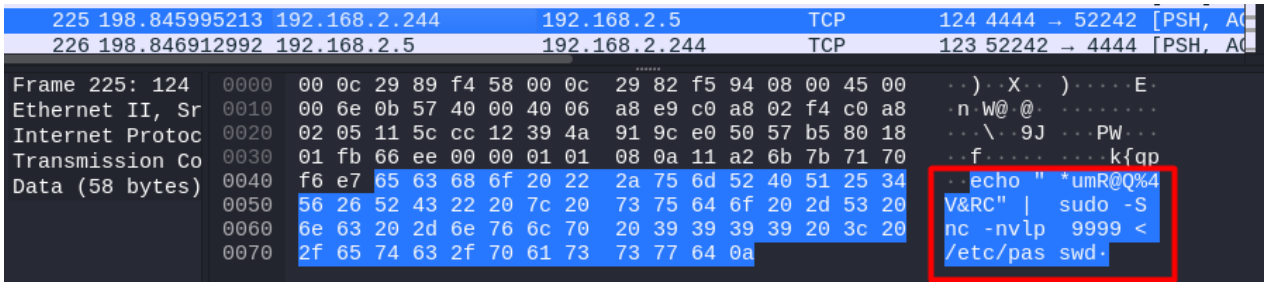
En el 71 lo siguiente



Además en el 196



En el 225 tenemos este

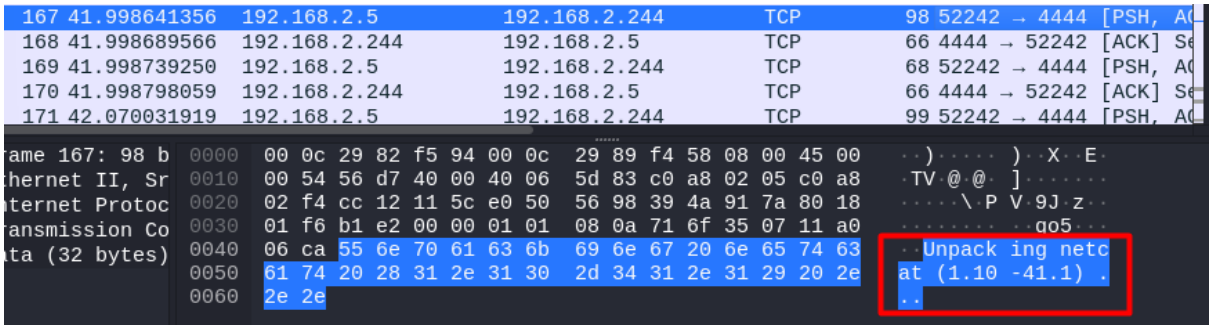


- 4.¿Qué servicio se ha levantado y en qué puerto? - 10 puntos

  Se ha levantado netcat y en el puerto 9999

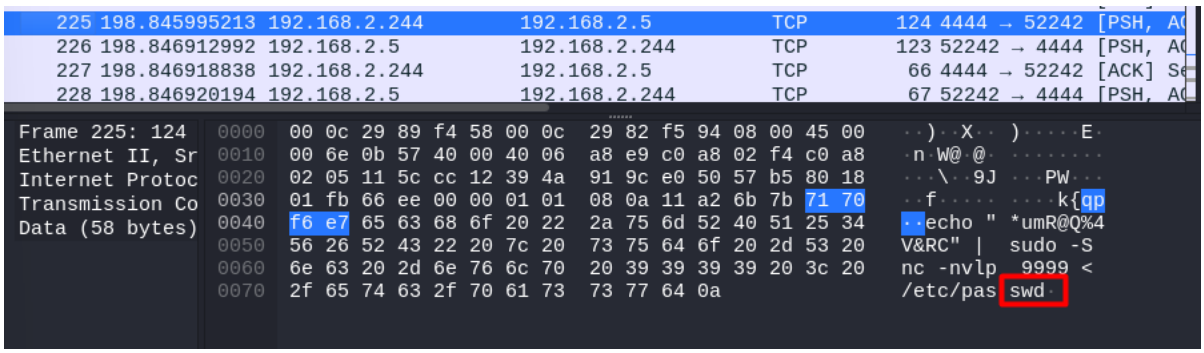
- 5.¿Qué versión del paquete se ha instalado? - 20 puntos

  se ha instalado la versión 1.10



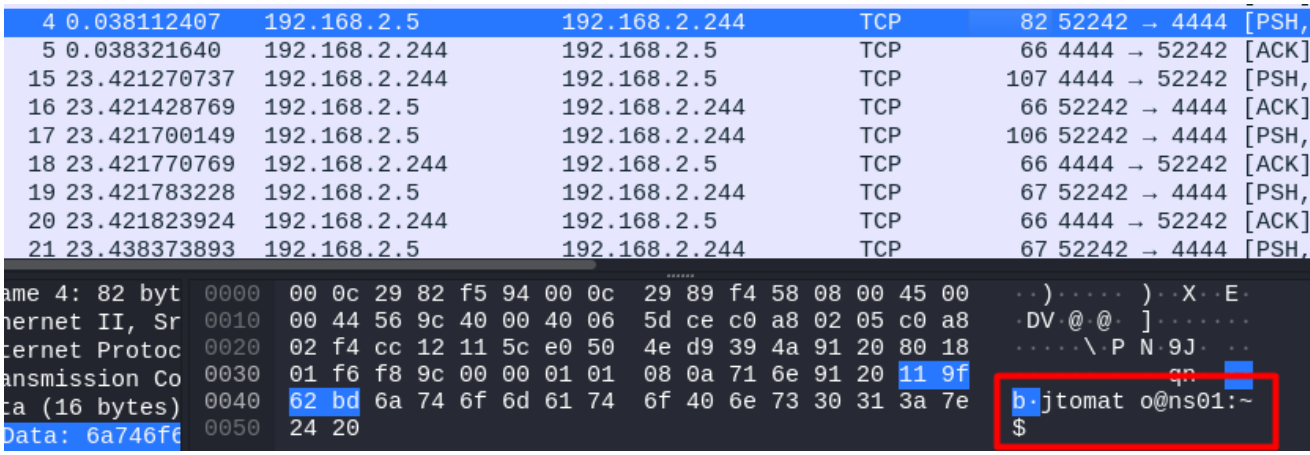
- 6.¿Qué archivo se ha enviado? - 20 puntos

  Un archivo swd en la carpeta /etc/pas

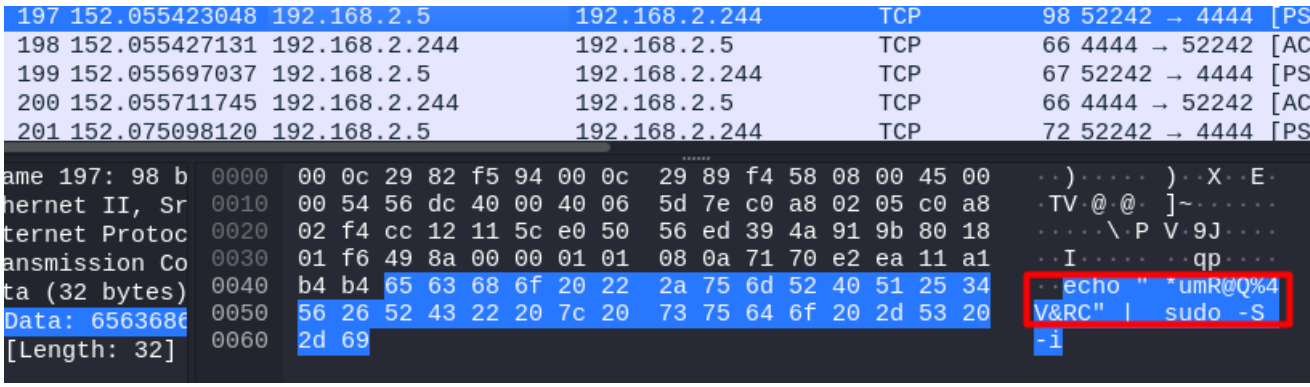


- 7.¿Qué usuario está en el equipo? ¿Qué password se ha utilizado para elevar la shell? - 20 puntos

El usuario es jtomato

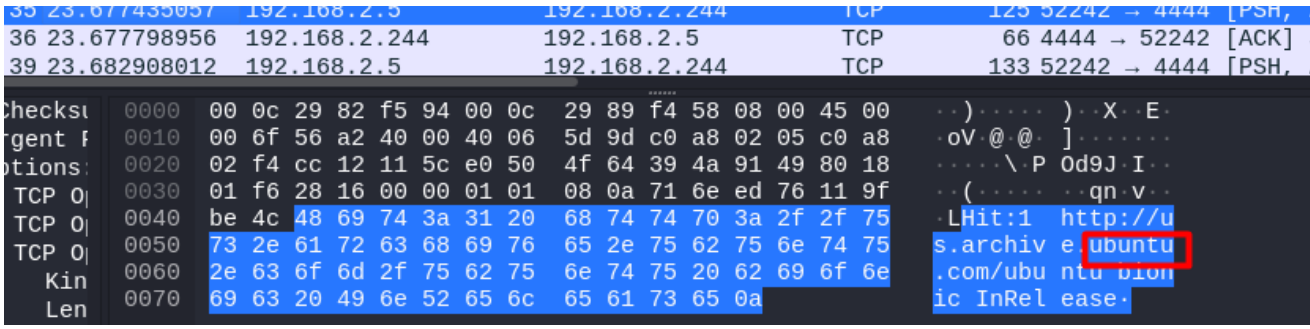


Y el password hemos observado que cada vez que utilizar el comando sudo escribe *umR@Q%4V&RC



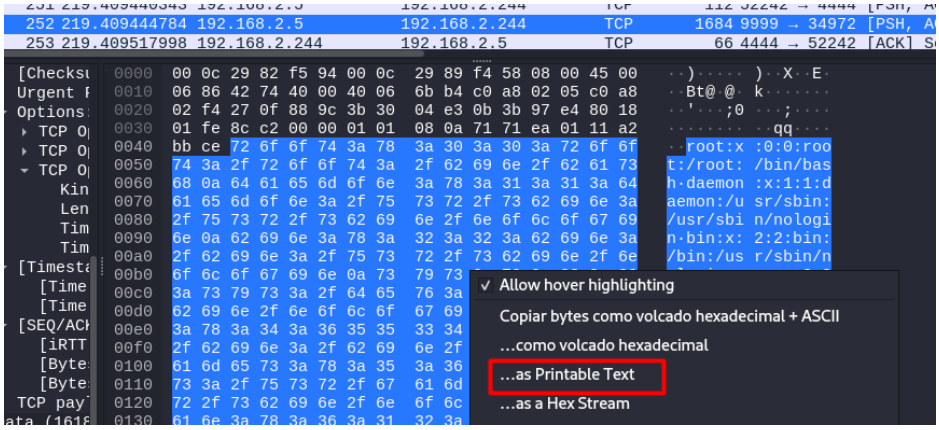
- 8.¿Qué distribución de Linux se está utilizando? - 20 puntos

  Buscamos en el paquete 35 y aparece información acerca del sistema operativo en este caso Ubuntu bionic

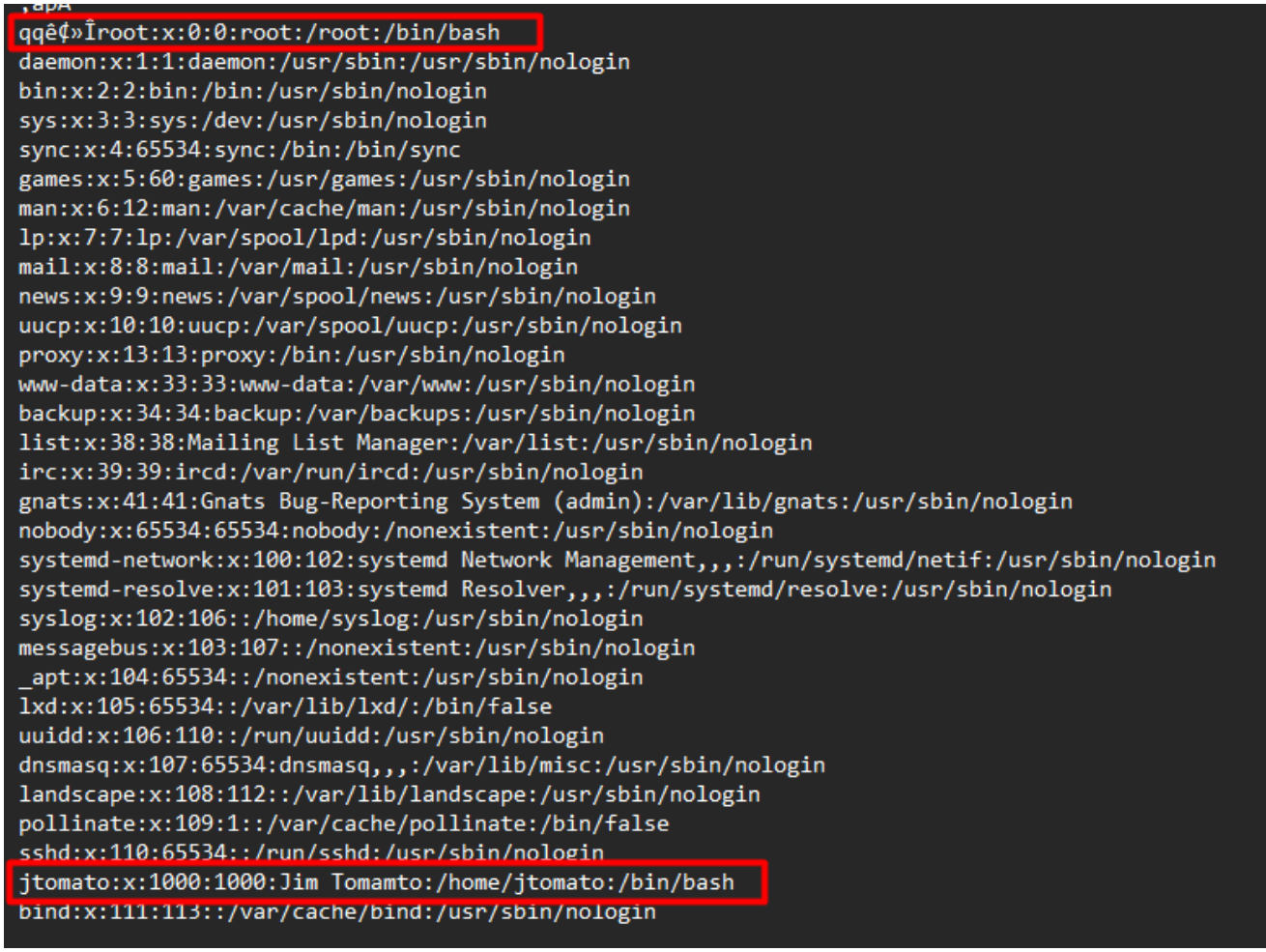


- 9.¿Cuantos usuarios hay en el sistema atacado? - 30 puntos

  Para esto le damos click derecho en wireshark del paquete 252



Y después de esto copiar en un archivo txt. Los únicos dos que tiene carpeta /bash son usuarios



- PARTE 3. ANALISIS DE MEMORIA - 200 puntos
  - 1.Identificar el tipo de sistema operativo de la máquina. - 10 puntos

```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility imageinfo -f memoria.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/memoria.vmem)
                      PAE type : PAE
                           DTB : 0x34c000L
                          KDBG : 0x80545ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2016-06-24 10:32:45 UTC+0000
     Image local date and time : 2016-06-24 16:02:45 +0530
```

  - 2.Identificar los procesos en ejecucion. - 10 puntos

```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility pslist -f memoria.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----------
0x82bc6660 System                    4      0     59      336 ------      0
0x82b1fda0 smss.exe                560      4      2       21 ------      0 2016-06-24 09:06:48 UTC+0000
0x829e4020 csrss.exe               676    560     12      421      0      0 2016-06-24 09:06:51 UTC+0000
0x82a7ada0 winlogon.exe            700    560     22      649      0      0 2016-06-24 09:06:53 UTC+0000
0x829e7960 services.exe            756    700     16      378      0      0 2016-06-24 09:07:02 UTC+0000
0x827b5990 lsass.exe               768    700     19      361      0      0 2016-06-24 09:07:07 UTC+0000
0x8293c3d8 vmacthlp.exe            924    756      1       38      0      0 2016-06-24 09:07:17 UTC+0000
0x825eb308 svchost.exe             984    756     23      235      0      0 2016-06-24 09:07:21 UTC+0000
0x827b4020 svchost.exe            1048    756     10      262      0      0 2016-06-24 09:07:23 UTC+0000
0x825d3958 svchost.exe            1192    756     73     1481      0      0 2016-06-24 09:07:23 UTC+0000
0x82595b20 svchost.exe            1404    756      4       73      0      0 2016-06-24 09:07:24 UTC+0000
0x82921020 svchost.exe            1544    756     12      183      0      0 2016-06-24 09:07:26 UTC+0000
0x825804b8 explorer.exe           1716   1700     14      559      0      0 2016-06-24 09:07:29 UTC+0000
0x828b0020 spoolsv.exe            1820    756     12      163      0      0 2016-06-24 09:07:32 UTC+0000
0x82547da0 rundll32.exe            660   1716      4       73      0      0 2016-06-24 09:07:39 UTC+0000
0x82546878 vmtoolsd.exe            732   1716      3      117      0      0 2016-06-24 09:07:39 UTC+0000
0x8287b020 svchost.exe            1984    756      4      105      0      0 2016-06-24 09:07:47 UTC+0000
```

  - 3.Podemos ver un proceso sospechoso por tener una duración de ejecución muy corta. ¿Puedes identificarlo?. - 20 puntos

    Se observa que este proceso es de corta duración

```
0x828bc628 game.exe            1044   1716      0 ------      0      0 2016-06-24 10:20:25 UTC+0000   2016-06-2
4 10:22:49 UTC+0000
```

  - 4.Podemos ver un proceso de sistema sospechoso por ser padre de varios procesos de sistema que no deberia. ¿Puedes identificarlo? ¿Incluye el proceso anterior como uno de sus hijos?. - 30 puntos

    Explorer.exe está ejecutando game.exe debido a que no tiene punto y por ende es el padre de los procesos

```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility pstree -f memoria.vmem
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x82bc6660:System                                      4      0     59    336 1970-01-01 00:00:00 UTC+0000
. 0x82b1fda0:smss.exe                                 560      4      2     21 2016-06-24 09:06:48 UTC+0000
.. 0x829e4020:csrss.exe                               676    560     12    421 2016-06-24 09:06:51 UTC+0000
.. 0x82a7ada0:winlogon.exe                            700    560     22    649 2016-06-24 09:06:53 UTC+0000
... 0x827b5990:lsass.exe                              768    700     19    361 2016-06-24 09:07:07 UTC+0000
... 0x829e7960:services.exe                           756    700     16    378 2016-06-24 09:07:02 UTC+0000
.... 0x82921020:svchost.exe                          1544    756     12    183 2016-06-24 09:07:26 UTC+0000
.... 0x827b4020:svchost.exe                          1048    756     10    262 2016-06-24 09:07:23 UTC+0000
.... 0x828b0020:spoolsv.exe                          1820    756     12    163 2016-06-24 09:07:32 UTC+0000
.... 0x825d3958:svchost.exe                          1192    756     73   1481 2016-06-24 09:07:23 UTC+0000
..... 0x824f2da0:wscntfy.exe                         1420   1192      1     36 2016-06-24 09:08:09 UTC+0000
..... 0x824d2020:wuauclt.exe                         2012   1192      3    111 2016-06-24 10:07:34 UTC+0000
.... 0x8293c3d8:vmacthlp.exe                          924    756      1     38 2016-06-24 09:07:17 UTC+0000
.... 0x8287b020:svchost.exe                          1984    756      4    105 2016-06-24 09:07:47 UTC+0000
.... 0x82871870:vmtoolsd.exe                          208    756      7    282 2016-06-24 09:07:47 UTC+0000
.... 0x825eb308:svchost.exe                           984    756     23    235 2016-06-24 09:07:21 UTC+0000
.... 0x8284b8f8:alg.exe                              1504    756      5    102 2016-06-24 09:08:10 UTC+0000
.... 0x8253a298:svchost.exe                          2020    756      4    100 2016-06-24 09:07:47 UTC+0000
.... 0x828375c0:TPAutoConnSvc.e                      1384    756      5    116 2016-06-24 09:08:09 UTC+0000
..... 0x828a2b88:TPAutoConnect.e                     2940   1384      1     78 2016-06-24 10:07:18 UTC+0000
.... 0x82595b20:svchost.exe                          1404    756      4     73 2016-06-24 09:07:24 UTC+0000
.. 0x825d03b0:csrss.exe                               836    560      0 ------ 2016-06-24 09:36:08 UTC+0000
 0x825804b8:explorer.exe                             1716   1700     14    559 2016-06-24 09:07:29 UTC+0000
. 0x827b6150:notepad.exe                             2816   1716      1     60 2016-06-24 09:08:38 UTC+0000
. 0x82547da0:rundll32.exe                             660   1716      4     73 2016-06-24 09:07:39 UTC+0000
. 0x824a4888:reg.exe                                 3232   1716      0 ------ 2016-06-24 10:29:05 UTC+0000
. 0x829d06c8:net.exe                                 1284   1716      0 ------ 2016-06-24 10:28:48 UTC+0000
. 0x82828620:cmd.exe                                 3508   1716      1     42 2016-06-24 10:27:51 UTC+0000
.. 0x82adc020:sc.exe                                 3316   3508      1     35 2016-06-24 10:28:22 UTC+0000
. 0x8250d8a8:netstat.exe                             3868   1716      0 ------ 2016-06-24 10:28:39 UTC+0000
. 0x829d18c8:cmd.exe                                 2632   1716      1     40 2016-06-24 10:26:05 UTC+0000
.. 0x82a75020:sc.exe                                 3120   2632      1     33 2016-06-24 10:27:32 UTC+0000
. 0x8250c020:netstat.exe                             2956   1716      0 ------ 2016-06-24 10:28:41 UTC+0000
. 0x82a3b900:cmd.exe                                 3988   1716      0 ------ 2016-06-24 10:28:42 UTC+0000
. 0x82a153a0:reg.exe                                 1712   1716      0 ------ 2016-06-24 10:29:00 UTC+0000
. 0x82546878:vmtoolsd.exe                             732   1716      3    117 2016-06-24 09:07:39 UTC+0000
. 0x828d7af0:cmd.exe                                 3068   1716      1     65 2016-06-24 10:30:19 UTC+0000
. 0x82a736d8:systeminfo.exe                          4008   1716      0 ------ 2016-06-24 10:28:52 UTC+0000
. 0x828bc628:game.exe                                1044   1716      0 ------ 2016-06-24 10:20:25 UTC+0000
```

- 5.Podemos ver diferentes conexiones en el equipo a IPs y puertos externos, de las cuales dos llaman sospechosamente la atención. ¿Cuáles son? ¿A que IP corresponden? ¿Qué tipo de software crees que se está utilizando?. - 30 puntos

  El proceso game.exe tiene el mismo pid de la conexión

```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility connections -f memoria.vmem
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x82a3bb68 192.168.78.135:1045       192.168.78.128:4444       1044
```

  Si observamos las conexiones ocultas aparecen las siguientes, la conexión con el pid 3696 es sospechosa ya que no aparece en el listado de procesos, lo que significa que el proceso ha terminado.

  En estas IP's la remote address es la ip del atacante y la local es el objetivo

```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility connscan -f memoria.vmem
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x028d1008 192.168.78.135:445        192.168.78.128:49072      4
0x02bcf2a0 192.168.78.135:445        192.168.78.128:49078      4
0x02bcfbe8 192.168.78.135:1046       192.168.78.128:4444       3696
0x02c3bb68 192.168.78.135:1045       192.168.78.128:4444       1044
```

  El tipo de programa es un archivo .exe y por ende es bastante probable que sea un troyano para que pueda ser ejecutado, además es bastante probable que se haya podido pasar por un juego a modo de ingeniería social

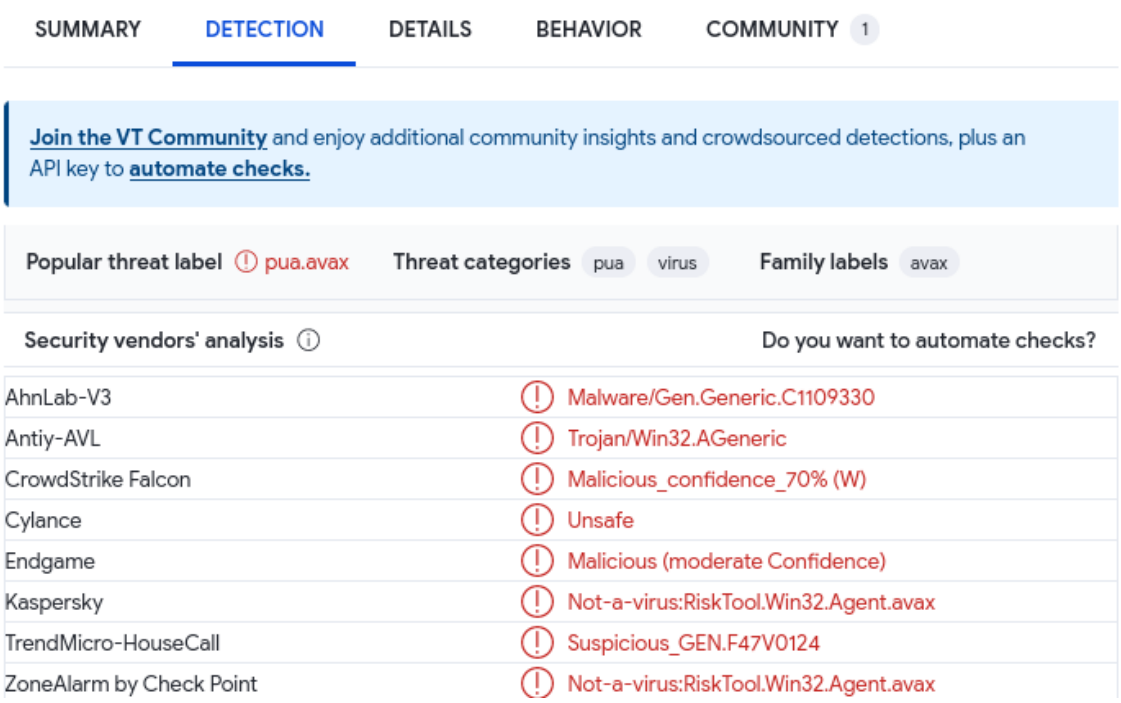
para ser descargado

- 6.Podemos comprobar si hay algún tipo de malware ejecutándose en la máquina. ¿En qué proceso? ¿Puedes volcar los registros del proceso y comprobar con alguna web externa si realmente es un malware y el tipo?. - 30 puntos

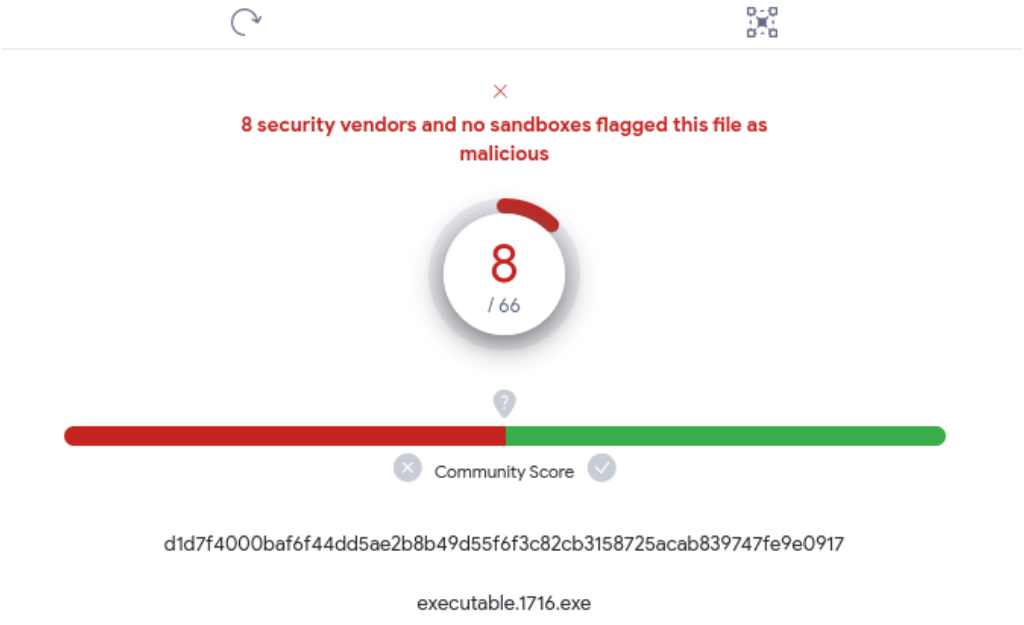
  Para esto realizamos un procdump

```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2x86 procdump -p 1716 -f memoria.vmem --dump-dir /home/kali/Escritorio
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x825804b8 0x01000000 explorer.exe         OK: executable.1716.exe
```

  Después de esto subimos el archivo a virus total



  Como resultado tenemos lo siguiente



- 7.¿Cual fué el último ejecutable que se lanzó por el usuario?. - 30 puntos

  Realizamos el siguiente comando

```
┌──(root㉿kali)-[~/Software/Analisisforense/volatility]
└─# ./volatility --profile=WinXPSP2x86 modscan -f memoria.vmem
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                Base             Size File
------------------ ------------------- ---------- ---------- ----
0x00000000026d1440 USBSTOR.SYS         0xf7e8d000     0x7000 .EXE-1CDAF90F.pfDRIVERQUERY.EXE-1CDAF90F
0x00000000026f8708 TSDDD.dll           0xbff50000     0x3000 ystemRoot\System32\TSDDD.dll
0x000000000272f248 srv.sys             0xb21fd000    0x58000 \SystemRoot\system32\DRIVERS\srv.sys
0x000000000273ae38 vmmemctl.sys        0xb274c000     0x3000 \??\C:\Program Files\Common Files\VMware\Drivers\memct
l\vmmemctl.sys
0x000000000277dbd8 Fastfat.SYS         0xb2724000    0x24000 \SystemRoot\System32\Drivers\Fastfat.SYS
0x0000000002829168 tcpip.sys           0xb2d74000    0x59000 \SystemRoot\system32\DRIVERS\tcpip.sys
0x0000000002881790 imapi.sys           0xf7b7d000     0xb000 \SystemRoot\system32\DRIVERS\imapi.sys
0x0000000002881c00 vmmouse.sys         0xf7fc7000     0x2000 \SystemRoot\system32\DRIVERS\vmmouse.sys
0x000000000288a288 ndisuio.sys         0xb29cc000     0x4000 \SystemRoot\system32\DRIVERS\ndisuio.sys
0x000000000288ac88 dxg.sys             0xbf9cb000    0x12000 \SystemRoot\System32\drivers\dxg.sys
0x0000000002891950 usbehci.sys         0xf7ded000     0x8000 \SystemRoot\system32\DRIVERS\usbehci.sys
```

  Y como resultado los últimos ejecutables son los siguiente

```
0x0000000002dfc338 hal.dll             0x806d1000    0x20380 \WINDOWS\system32\hal.dll
0x0000000002dfc3a0 ntoskrnl.exe        0x804d7000   0x1f9680 \WINDOWS\system32\ntkrnlpa.exe
```

- 8.¿Puedes resumir qué ha pasado en este equipo?. - 40 puntos

  Es bastante probable que el usuario de esta maquina haya descargado un archivo de un sitio poco seguro y al ejecutarlo ha abierto una puerta trasera para el atacante y por ende han infectado su dispositivo.