

DÍA D - EJERCICIO FINAL - CTF ANÁLISIS FORENSE

- Canal Slack: cs-ft-sep-23

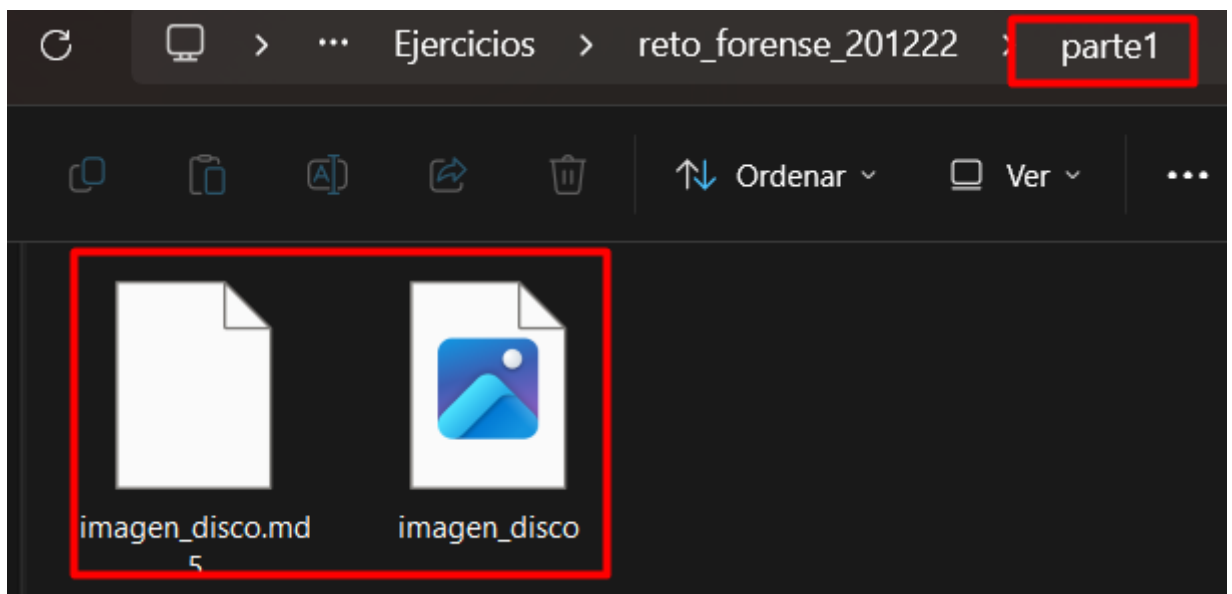
Prerrequisitos

- 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!).

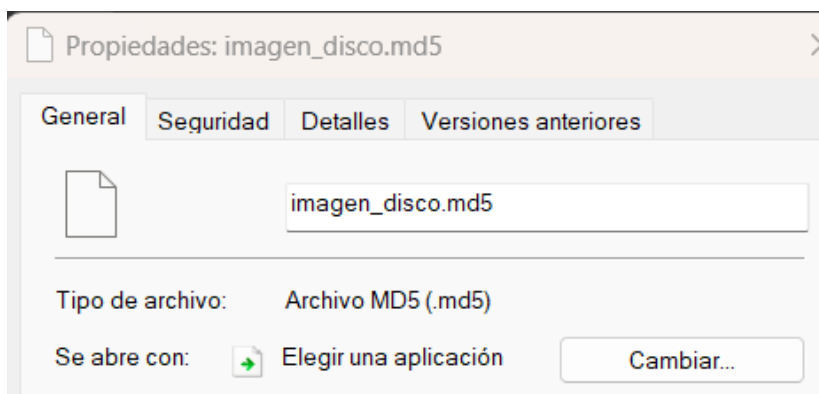
Cuestionario para el CSIRT

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

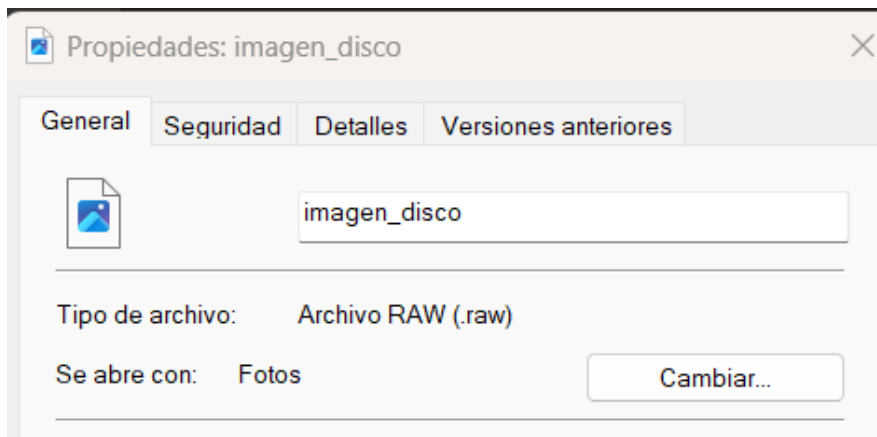
Una vez hemos descargado el archivo .zip descomprimos la carpeta y obtenemos los siguientes archivos



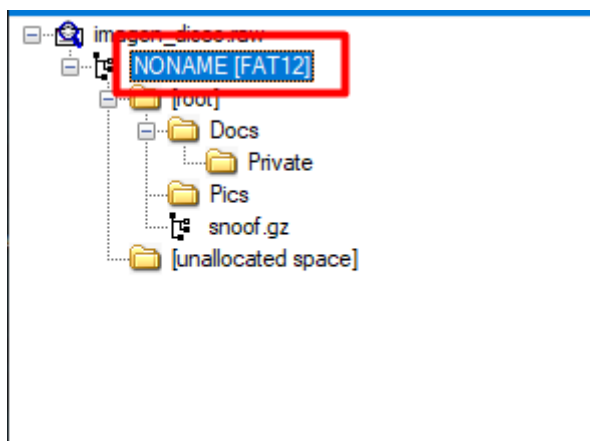
El primer archivo es un .MD5



Y el segundo es un .raw

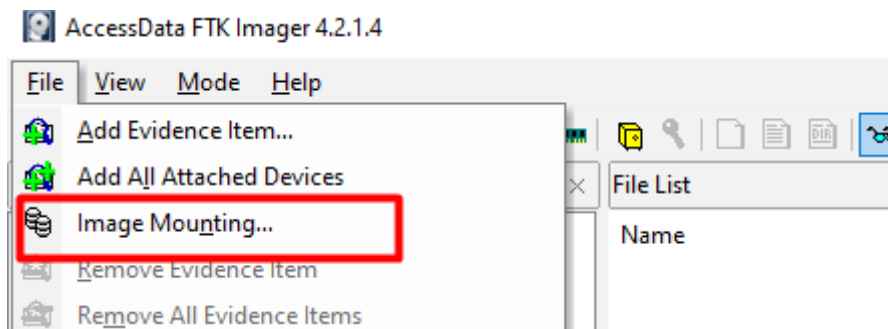


Una vez montada la imagen podemos observar que el sistema de ficheros es FAT

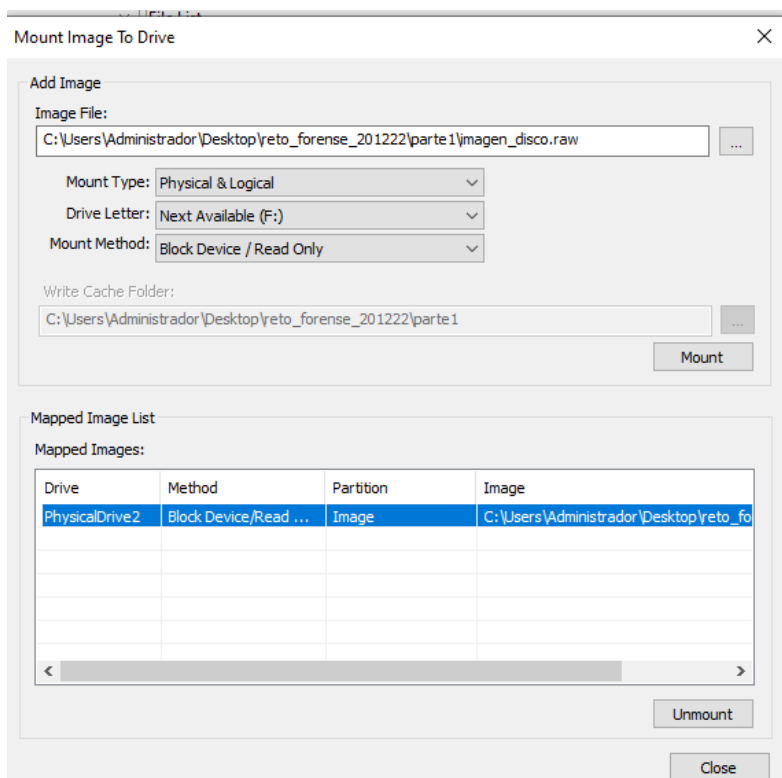


- 2.¿Cuandos directorios hay dentro de la imagen? - 10 puntos

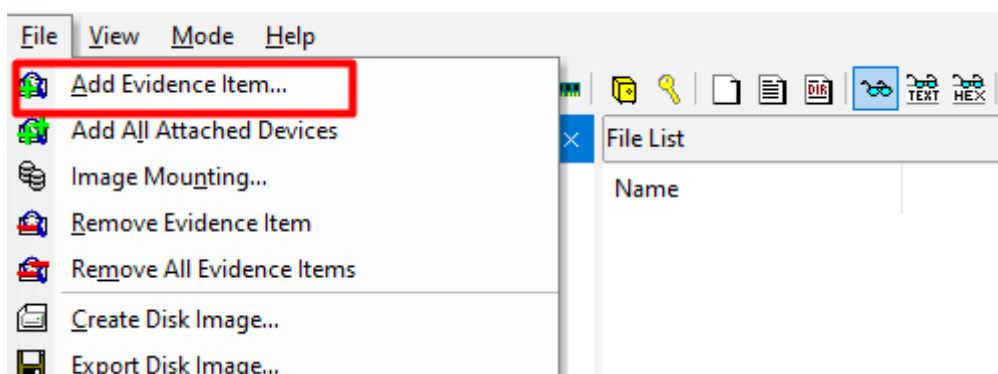
Para esto debemos montar la imagen con FTK



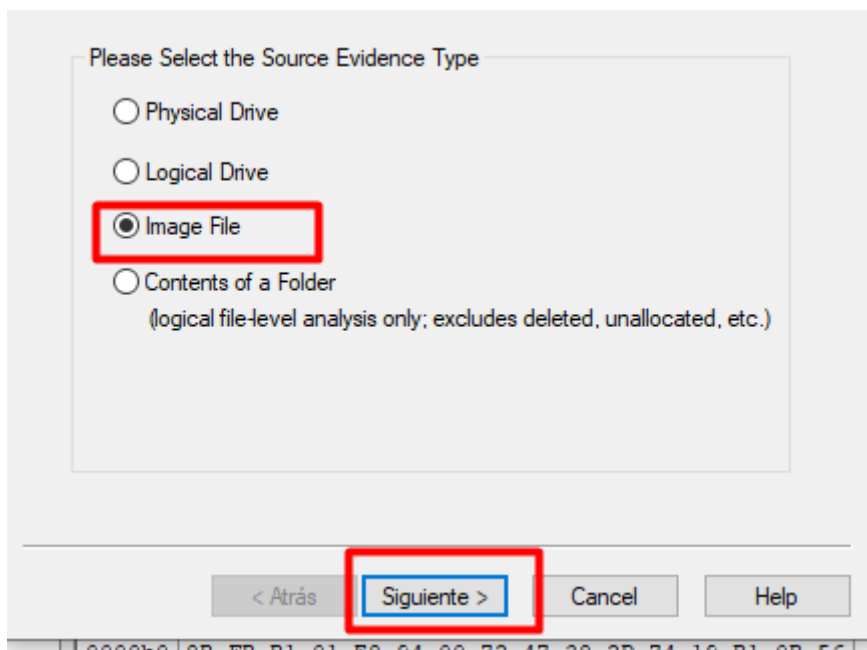
Seleccionamos la imagen y la montamos



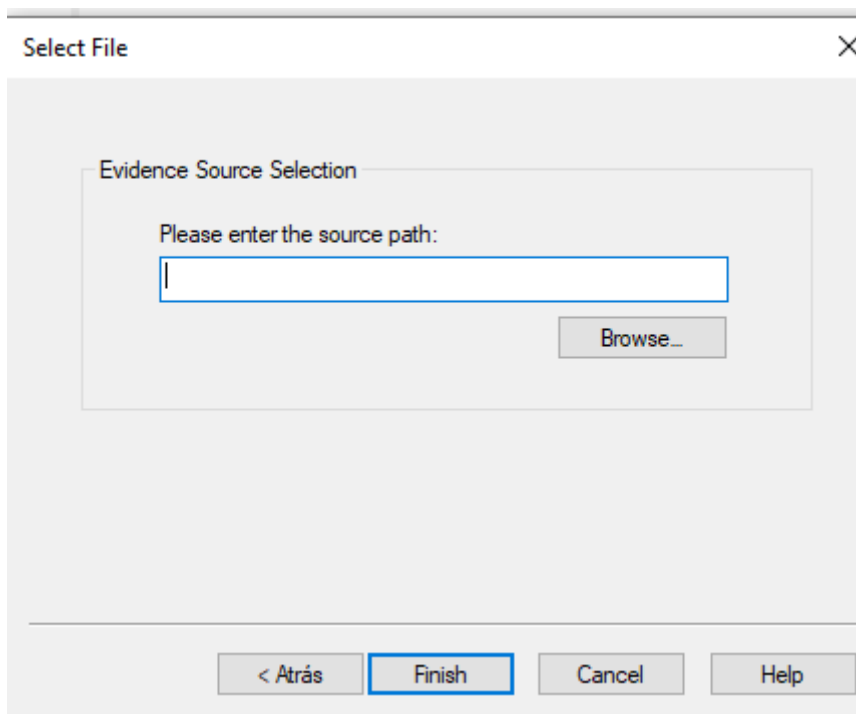
Una vez salimos hacemos lo siguiente



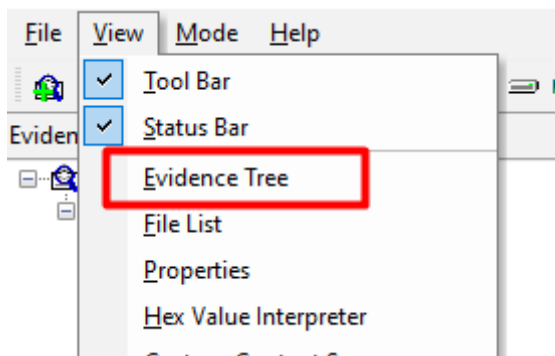
Seleccionamos Image file



Y después seleccionamos el archivo imagen



Finalizas y visualizamos el árbol de evidencias



Como resultado podemos observar los siguiente directorios y archivos

imagen_disco.raw

NONAME [FAT12]

[root]

[unallocated space]

Name	Size	Type	Date Modified
[root]	7	Directory	
[unallocated space]	0	Unallocated Sp...	
FAT1	5	Filesystem Met...	
FAT2	5	Filesystem Met...	
VBR	1	Filesystem Met...	

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

Hemos encontrado uno

imagen_disco.raw

NONAME [FAT12]

[root]

Docs

Private

Pics

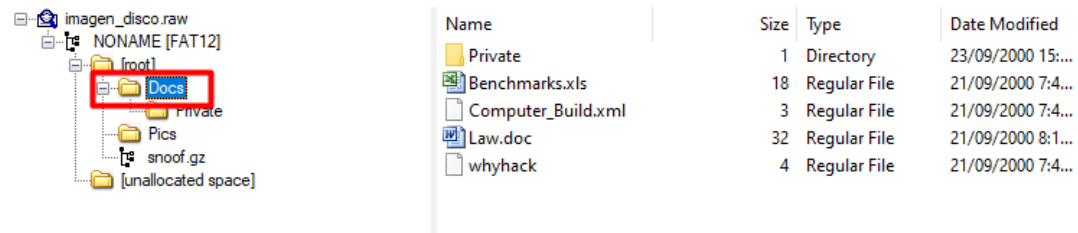
snoof.gz

[unallocated space]

Name	Size	Type	Date Modified
ReyHalif.doc	1	Regular File	23/09/2000 15:...

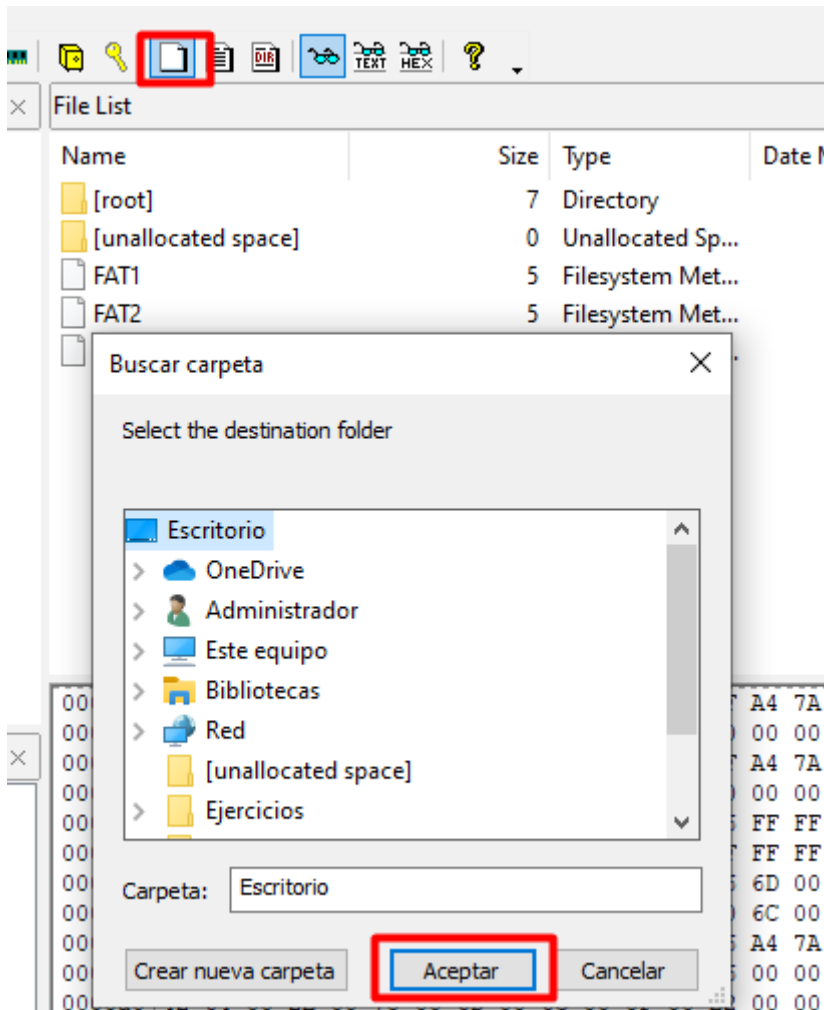
- 4. Monta la imagen para poder acceder a los ficheros. - 20 puntos

Este paso está explicado en el anterior prácticamente.

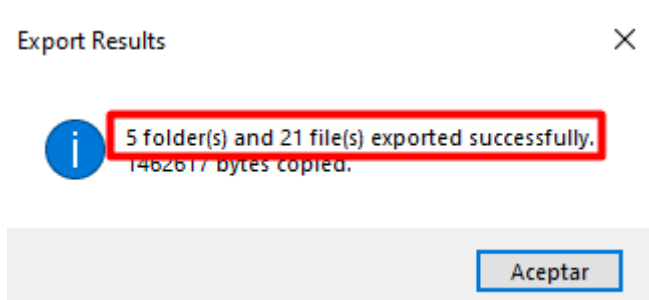


- 5. ¿Cuántos archivos hay en la imagen? - 20 puntos

Para esto exportamos la carpeta en el escritorio

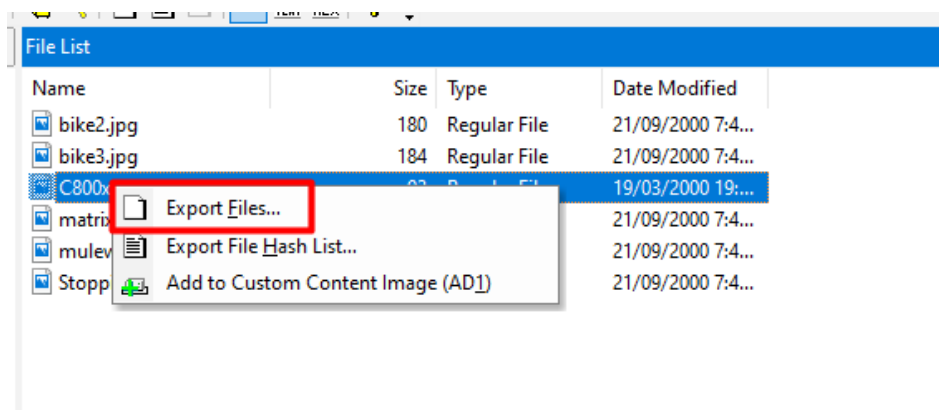


Y una vez le damos a aceptar nos sale la información que había dentro

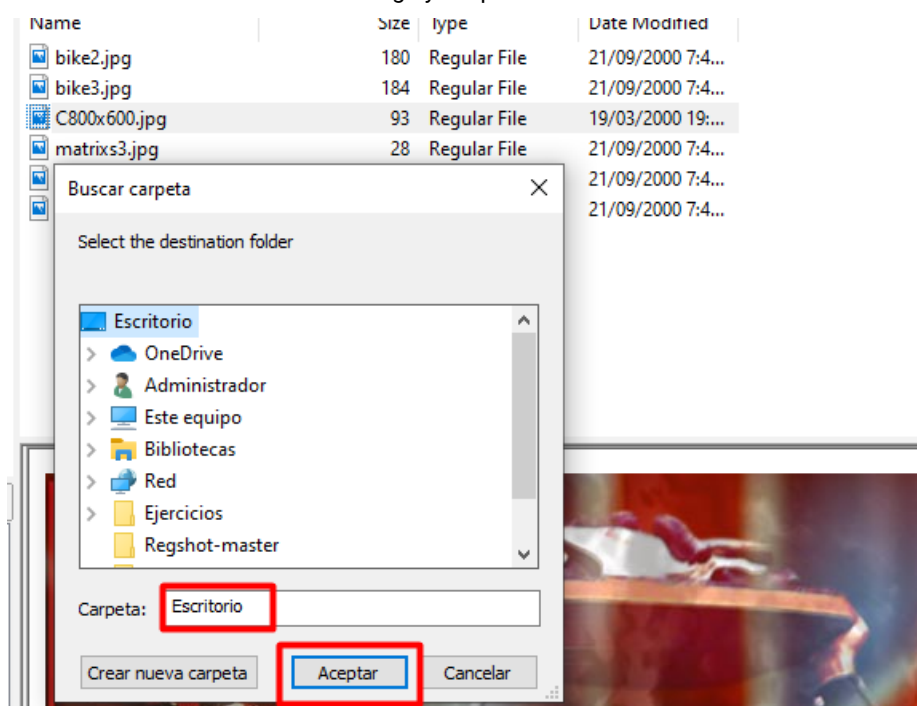


- 6. Descarga tres de las imágenes disponibles. - 30 puntos

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

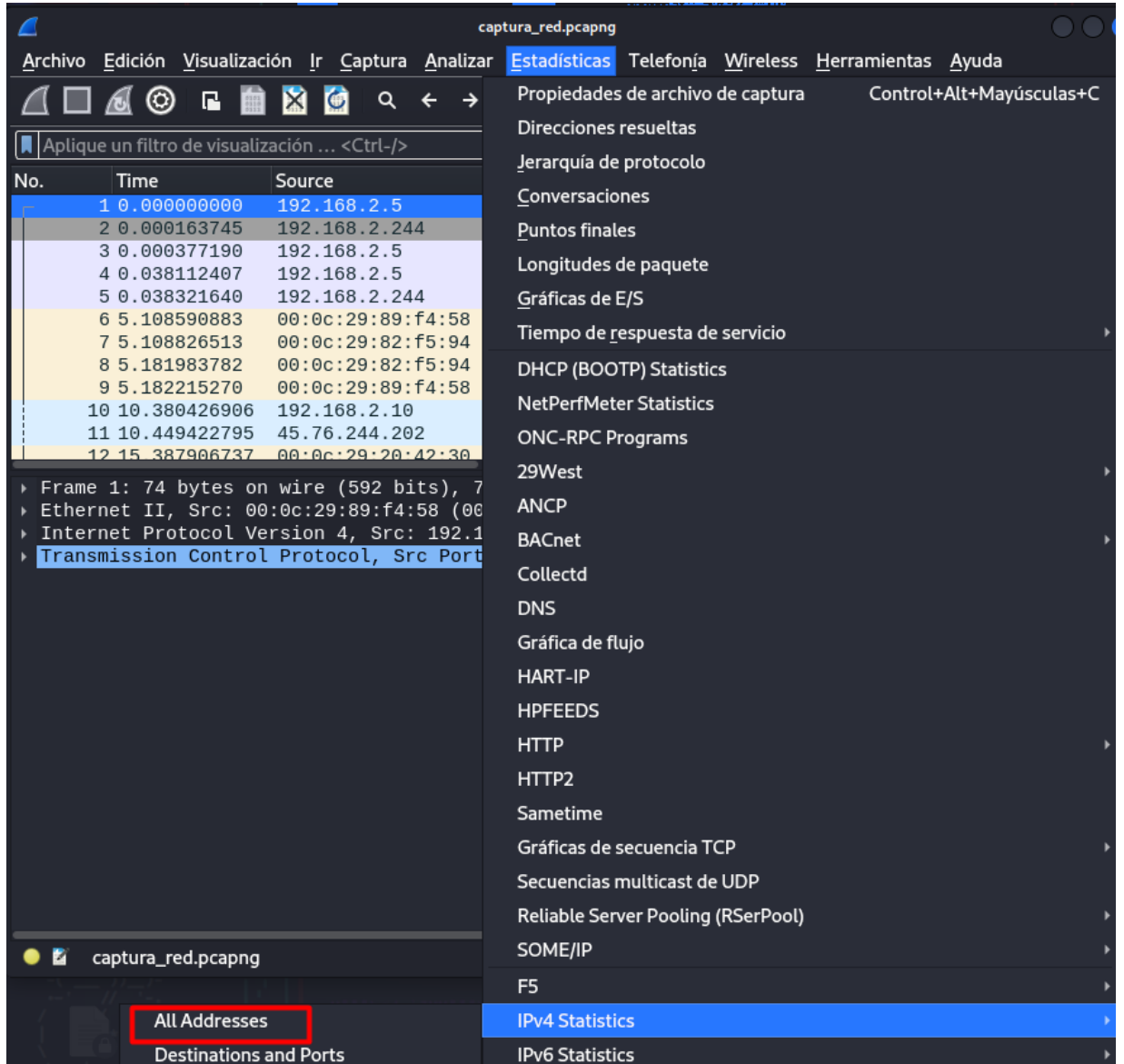


- PARTE 2. ANALISIS DE CAPTURA DE TRAFICO - 150 puntos
 - 1.¿Cuales son las dos IPs que estan en la comunicación? - 10 puntos

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

```
(root@kali)-[/home/kali/Escritorio/parte2]
# wireshark captura_red.pcapng
** (wireshark:1645) 10:22:51.476415 [GUI WARNING] -- QStandardPaths: runtime directory '/run/user/1000' is not owned by UID 0, but a directory permissions 0700 owned by UID 1000 GID 1000
1 0.000000000 192.168.2.244 TCP 98 52242 -> 4444
2 0.000163745 192.168.2.5 TCP 66 4444 -> 52242
3 0.000377190 192.168.2.5
4 0.038112407 192.168.2.5
5 0.038321640 192.168.2.244
6 5.108590883 00:0c:29:89:f4:58
7 5.108826513 00:0c:29:82:f5:94
8 5.181983782 00:0c:29:82:f5:94
9 5.182215270 00:0c:29:89:f4:58
10 10.380426906 192.168.2.10
11 10.449422795 45.76.244.202
12 15.387906737 00:0c:29:20:42:30
84 40.924512640 192.168.2.5 192.168.2.244 TCP 93 52242 -> 4444
```

Una vez dentro vamos a la pestaña de estadísticas

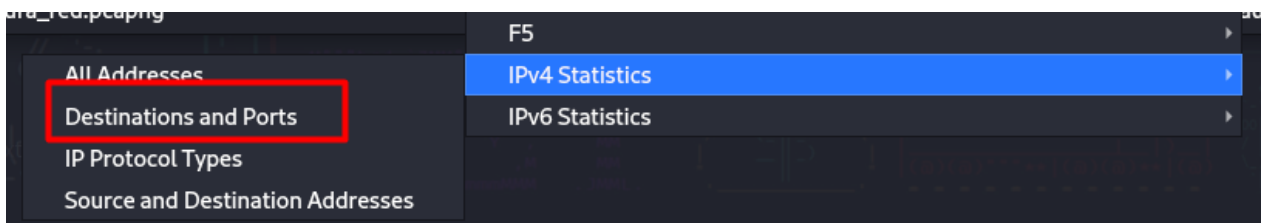


Una vez dentro vemos diferentes IP's pero las que concentran todo el trafico son principalmente dos

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	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

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ Destinations and Ports	240				0,0010	100%	0,5200	41,922
▼ 192.168.2.5	105				0,0004	43,75%	0,2600	41,922
▼ TCP	104				0,0004	99,05%	0,2600	41,922
52242	87				0,0004	83,65%	0,2600	41,922
36874	7				0,0000	6,73%	0,0600	23,654
9999	5				0,0000	4,81%	0,0300	219,409
36876	5				0,0000	4,81%	0,0500	41,421
▼ UDP	1				0,0000	0,95%	0,0100	23,640
45537	1				0,0000	100,00%	0,0100	23,640
▼ 192.168.2.244	93				0,0004	38,75%	0,2600	41,922
▼ TCP	92				0,0004	98,92%	0,2600	41,922
4444	84				0,0003	91,30%	0,2600	41,922
56398	5				0,0000	5,43%	0,0500	213,621
34972	3				0,0000	3,26%	0,0200	219,409
▼ UDP	1				0,0000	1,08%	0,0100	212,655
59042	1				0,0000	100,00%	0,0100	212,655
▶ 91.189.91.38	18				0,0001	7,50%	0,0800	41,408
▶ 35.224.99.156	5				0,0000	2,08%	0,0500	130,390

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

Para esto realizamos una búsqueda con filtros

ip.addr == 192.168.2.5 and ip.addr == 192.168.2.244							
No.	Time	Source	Destination	Protocol	Length	Info	
1	0.000000000	192.168.2.5	192.168.2.244	TCP	74	52242 → 4444	[SYN] Seq: 17
2	0.000163745	192.168.2.244	192.168.2.5	TCP	74	4444 → 52242	[SYN, ACK] Seq: 17, Win: 0
3	0.000377190	192.168.2.5	192.168.2.244	TCP	66	52242 → 4444	[ACK] Seq: 17, Win: 0
4	0.038112407	192.168.2.5	192.168.2.244	TCP	82	52242 → 4444	[PSH, ACK] Seq: 17, Win: 0
5	0.038321640	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242	[ACK] Seq: 17, Win: 0
15	23.421270737	192.168.2.244	192.168.2.5	TCP	107	4444 → 52242	[PSH, ACK] Seq: 17, Win: 0
16	23.421428769	192.168.2.5	192.168.2.244	TCP	66	52242 → 4444	[ACK] Seq: 17, Win: 0
17	23.421700149	192.168.2.5	192.168.2.244	TCP	106	52242 → 4444	[PSH, ACK] Seq: 17, Win: 0
18	23.421770769	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242	[ACK] Seq: 17, Win: 0
19	23.421783228	192.168.2.5	192.168.2.244	TCP	67	52242 → 4444	[PSH, ACK] Seq: 17, Win: 0
20	23.421823924	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242	[ACK] Seq: 17, Win: 0
21	23.438373893	192.168.2.5	192.168.2.244	TCP	67	52242 → 4444	[PSH, ACK] Seq: 17, Win: 0

▶ Frame 17: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface
 ▶ Ethernet II, Src: 00:0c:29:89:f4:58 (00:0c:29:89:f4:58), Dst: 00:0c:29:82:f5:94
 ▶ Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.244
 ▶ Transmission Control Protocol, Src Port: 52242, Dst Port: 4444, Seq: 17, Ack: 4
 ▶ Data (40 bytes)

```

0000  00 0c 29 82 f5 94 00 0c 29 89 f4 58 08 00 45 00  ..).X..).E.
0010  00 5c 56 9e 40 00 40 06 5d b4 c0 a8 02 05 c0 a8  .V.@.@.]....
0020  02 f4 cc 12 11 5c e0 50 4e e9 39 4a 91 49 80 18  .P.N.9J.I.
0030  01 f6 48 6b 00 00 01 01 08 0a 71 6e ec 76 11 9f  .Hk.....qn.v.
0040  be 3a 65 63 68 6f 20 22 2a 75 6d 52 40 51 25 34  .:echo " *umR@Q%4
0050  56 26 52 43 22 20 7c 20 73 75 64 6f 20 2d 53 20  V&RC" | sudo -S
0060  61 70 74 20 75 70 64 61 74 65                      apt upda te
  
```

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

ip.addr == 192.168.2.5 and ip.addr == 192.168.2.244							
No.	Time	Source	Destination	Protocol	Length	Info	
71	40.813279987	192.168.2.244	192.168.2.5	TCP	115	4444 → 52242	[PSH, ACK] Seq: 17, Win: 0
72	40.813843076	192.168.2.5	192.168.2.244	TCP	114	52242 → 4444	[PSH, ACK] Seq: 17, Win: 0

▶ Frame 71: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface
 ▶ Ethernet II, Src: 00:0c:29:89:f4:58 (00:0c:29:89:f4:58), Dst: 00:0c:29:82:f5:94
 ▶ Internet Protocol Version 4, Src: 192.168.2.244, Dst: 192.168.2.5
 ▶ Transmission Control Protocol, Src Port: 4444, Dst Port: 52242, Seq: 17, Ack: 4
 ▶ Data (49 bytes)

```

0000  00 0c 29 89 f4 58 00 0c 29 82 f5 94 08 00 45 00  ..).X..).E.
0010  00 65 0b 1d 40 00 40 06 a9 2c c0 a8 02 f4 c0 a8  .e..@.@.]....
0020  02 05 11 5c cc 12 39 4a 91 49 e0 50 51 13 80 18  .P.N.9J.I.PQ.
0030  01 fd 4d f8 00 00 01 01 08 0a 11 a0 02 2a 71 6e  .M.....*gn.
0040  f6 49 65 63 68 6f 20 22 2a 75 6d 52 40 51 25 34  .:echo " *umR@Q%4
0050  56 26 52 43 22 20 7c 20 73 75 64 6f 20 2d 53 20  V&RC" | sudo -S
0060  61 70 74 20 69 6e 73 74 61 6c 6c 20 6e 65 74 63  apt inst all netc
0070  61 74 0a                                         at.
  
```

En el 71 lo siguiente

ip.addr == 192.168.2.5 and ip.addr == 192.168.2.244							
No.	Time	Source	Destination	Protocol	Length	Info	
71	40.813279987	192.168.2.244	192.168.2.5	TCP	115	4444 → 52242	[PSH, ACK] Seq: 17, Win: 0
72	40.813843076	192.168.2.5	192.168.2.244	TCP	114	52242 → 4444	[PSH, ACK] Seq: 17, Win: 0

▶ Frame 71: 115 bytes on wire (920 bits), 115 bytes captured (920 bits) on interface
 ▶ Ethernet II, Src: 00:0c:29:89:f4:58 (00:0c:29:89:f4:58), Dst: 00:0c:29:82:f5:94
 ▶ Internet Protocol Version 4, Src: 192.168.2.244, Dst: 192.168.2.5
 ▶ Transmission Control Protocol, Src Port: 4444, Dst Port: 52242, Seq: 17, Ack: 4
 ▶ Data (49 bytes)

```

0000  00 0c 29 89 f4 58 00 0c 29 82 f5 94 08 00 45 00  ..).X..).E.
0010  00 65 0b 1d 40 00 40 06 a9 2c c0 a8 02 f4 c0 a8  .e..@.@.]....
0020  02 05 11 5c cc 12 39 4a 91 49 e0 50 51 13 80 18  .P.N.9J.I.PQ.
0030  01 fd 4d f8 00 00 01 01 08 0a 11 a0 02 2a 71 6e  .M.....*gn.
0040  f6 49 65 63 68 6f 20 22 2a 75 6d 52 40 51 25 34  .:echo " *umR@Q%4
0050  56 26 52 43 22 20 7c 20 73 75 64 6f 20 2d 53 20  V&RC" | sudo -S
0060  61 70 74 20 69 6e 73 74 61 6c 6c 20 6e 65 74 63  apt inst all netc
0070  61 74 0a                                         at.
  
```

Además en el 196

196	152.054787590	192.168.2.244	192.168.2.5	TCP	99 4444 → 52242 [PSH,
197	152.055423048	192.168.2.5	192.168.2.244	TCP	98 52242 → 4444 [PSH,
198	152.055427131	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242 [ACK]
199	152.055697037	192.168.2.5	192.168.2.244	TCP	67 52242 → 4444 [PSH,
200	152.055711745	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242 [ACK]
201	152.075098120	192.168.2.5	192.168.2.244	TCP	72 52242 → 4444 [PSH,
202	152.075207847	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242 [ACK]
203	152.075310160	192.168.2.5	192.168.2.244	TCP	113 52242 → 4444 [PSH,

Frame 196: 99 b	0000	00 0c 29 89 f4 58 00 0c	29 82 f5 94 08 00 45 00	..).X..).E.
Ethernet II, Sr	0010	00 55 0b 4c 40 00 40 06	a9 0d c0 a8 02 f4 c0 a8	.U.L@.
Internet Protoc	0020	02 05 11 5c cc 12 39 4a	91 7a e0 50 56 ed 80 18	.. \ .9J .z.PV..
Transmission Co	0030	01 fb e7 5f 00 00 01 01	08 0a 11 a1 b4 b4 71 6f	..f.k{qp
Data (33 bytes)	0040	3b 31 65 63 68 6f 20 22	2a 75 6d 52 40 51 25 34	..echo " *umR@Q%4
	0050	56 26 52 43 22 20 7c 20	73 75 64 6f 20 2d 53 20	V&RC" sudo -S
	0060	2d 69 0a		-i.

En el 225 tenemos este

225	198.845995213	192.168.2.244	192.168.2.5	TCP	124 4444 → 52242 [PSH, AC
226	198.846912992	192.168.2.5	192.168.2.244	TCP	123 52242 → 4444 [PSH, AC

Frame 225: 124	0000	00 0c 29 89 f4 58 00 0c	29 82 f5 94 08 00 45 00	..).X..).E.
Ethernet II, Sr	0010	00 6e 0b 57 40 00 40 06	a8 e9 c0 a8 02 f4 c0 a8	.n.W@.
Internet Protoc	0020	02 05 11 5c cc 12 39 4a	91 9c e0 50 57 b5 80 18	.. \ .9J .z.PW..
Transmission Co	0030	01 fb 66 ee 00 00 01 01	08 0a 11 a2 6b 7b 71 70	..f.k{qp
Data (58 bytes)	0040	f6 e7 65 63 68 6f 20 22	2a 75 6d 52 40 51 25 34	..echo " *umR@Q%4
	0050	56 26 52 43 22 20 7c 20	73 75 64 6f 20 2d 53 20	V&RC" sudo -S
	0060	6e 63 20 2d 6e 76 6c 70	20 39 39 39 39 20 3c 20	nc -nvlp 9999 <
	0070	2f 65 74 63 2f 70 61 73	73 77 64 0a	/etc/pas swd.

- 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

167	41.998641356	192.168.2.5	192.168.2.244	TCP	98 52242 → 4444 [PSH, AC
168	41.998689566	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242 [ACK] Se
169	41.998739250	192.168.2.5	192.168.2.244	TCP	68 52242 → 4444 [PSH, AC
170	41.998798059	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242 [ACK] Se
171	42.070031919	192.168.2.5	192.168.2.244	TCP	99 52242 → 4444 [PSH, AC

Frame 167: 98 b	0000	00 0c 29 82 f5 94 00 0c	29 89 f4 58 08 00 45 00	..).X..).E.
hernet II, Sr	0010	00 54 56 d7 40 00 40 06	5d 83 c0 a8 02 05 c0 a8	.TV.@.
Internet Protoc	0020	02 f4 cc 12 11 5c e0 50	56 98 39 4a 91 7a 80 18	.. \ .P V.9J .z..
ransmission Co	0030	01 f6 b1 e2 00 00 01 01	08 0a 71 6f 35 07 11 a0	..f.k{qp
ata (32 bytes)	0040	06 ca 55 6e 70 61 63 6b	69 6e 67 20 6e 65 74 63	..Unpack ing netc
	0050	61 74 20 28 31 2e 31 30	2d 34 31 2e 31 29 20 2e	at (1.10 -41.1) .
	0060	2e 2e		..

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

Un archivo swd en la carpeta /etc/pas

225	198.845995213	192.168.2.244	192.168.2.5	TCP	124 4444 → 52242 [PSH, AC
226	198.846912992	192.168.2.5	192.168.2.244	TCP	123 52242 → 4444 [PSH, AC
227	198.846918838	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242 [ACK] Se
228	198.846920194	192.168.2.5	192.168.2.244	TCP	67 52242 → 4444 [PSH, AC

Frame 225: 124	0000	00 0c 29 89 f4 58 00 0c	29 82 f5 94 08 00 45 00	..).X..).E.
Ethernet II, Sr	0010	00 6e 0b 57 40 00 40 06	a8 e9 c0 a8 02 f4 c0 a8	.n.W@.
Internet Protoc	0020	02 05 11 5c cc 12 39 4a	91 9c e0 50 57 b5 80 18	.. \ .9J .z.PW..
Transmission Co	0030	01 fb 66 ee 00 00 01 01	08 0a 11 a2 6b 7b 71 70	..f.k{qp
Data (58 bytes)	0040	f6 e7 65 63 68 6f 20 22	2a 75 6d 52 40 51 25 34	..echo " *umR@Q%4
	0050	56 26 52 43 22 20 7c 20	73 75 64 6f 20 2d 53 20	V&RC" sudo -S
	0060	6e 63 20 2d 6e 76 6c 70	20 39 39 39 39 20 3c 20	nc -nvlp 9999 <
	0070	2f 65 74 63 2f 70 61 73	73 77 64 0a	/etc/pas swd.

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

El usuario es jtomato

4	0.038112407	192.168.2.5	192.168.2.244	TCP	82 52242 → 4444	[PSH,
5	0.038321640	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	[ACK]
15	23.421270737	192.168.2.244	192.168.2.5	TCP	107 4444 → 52242	[PSH,
16	23.421428769	192.168.2.5	192.168.2.244	TCP	66 52242 → 4444	[ACK]
17	23.421700149	192.168.2.5	192.168.2.244	TCP	106 52242 → 4444	[PSH,
18	23.421770769	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	[ACK]
19	23.421783228	192.168.2.5	192.168.2.244	TCP	67 52242 → 4444	[PSH,
20	23.421823924	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	[ACK]
21	23.438373893	192.168.2.5	192.168.2.244	TCP	67 52242 → 4444	[PSH,

Frame 4: 82 bytes captured on interface eth0 (0.0000000000000000)	0000	00 0c 29 82 f5 94 00 0c 29 89 f4 58 08 00 45 00	..).....)..X..E..
Ethernet II, Src: VirtualBox__08:00:00:00:00:00, Dst: VirtualBox__08:00:00:00:00:00	0010	00 44 56 9c 40 00 40 06 5d ce c0 a8 02 05 c0 a8	..DV.@.@.].....
Internet Protocol Version 4, Src: 192.168.2.244, Dst: 192.168.2.5	0020	02 f4 cc 12 11 5c e0 50 4e d9 39 4a 91 20 80 18\P N-9J....
TCP, Src Port: 52242, Dst Port: 4444	0030	01 f6 f8 9c 00 00 01 01 08 0a 71 6e 91 20 11 9f\P N-9J....
Application Data (16 bytes)	0040	62 bd 6a 74 6f 6d 61 74 6f 40 6e 73 30 31 3a 7e	..b.jtomat o@ns01:~
Data: 6a746f6d61746f406e7330313a7e	0050	24 20	\$

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

197	152.055423048	192.168.2.5	192.168.2.244	TCP	98 52242 → 4444	[PSH,
198	152.055427131	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	[ACK]
199	152.055697037	192.168.2.5	192.168.2.244	TCP	67 52242 → 4444	[PSH,
200	152.055711745	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	[ACK]
201	152.075098120	192.168.2.5	192.168.2.244	TCP	72 52242 → 4444	[PSH,

Frame 197: 98 bytes captured on interface eth0 (0.0000000000000000)	0000	00 0c 29 82 f5 94 00 0c 29 89 f4 58 08 00 45 00	..).....)..X..E..
Ethernet II, Src: VirtualBox__08:00:00:00:00:00, Dst: VirtualBox__08:00:00:00:00:00	0010	00 54 56 dc 40 00 40 06 5d 7e c0 a8 02 05 c0 a8	..TV.@.@.]~.....
Internet Protocol Version 4, Src: 192.168.2.244, Dst: 192.168.2.5	0020	02 f4 cc 12 11 5c e0 50 56 ed 39 4a 91 9b 80 18\P V-9J....
TCP, Src Port: 52242, Dst Port: 4444	0030	01 f6 49 8a 00 00 01 01 08 0a 71 70 e2 ea 11 a1I.....qp....
Application Data (32 bytes)	0040	b4 b4 65 63 68 6f 20 22 2a 75 6d 52 40 51 25 34	..echo " *umR@Q%4
Data: 6563686f20222a756d5240512534	0050	56 26 52 43 22 20 7c 20 73 75 64 6f 20 2d 53 20	V&RC" sudo -S
[Length: 32]	0060	2d 69	-i

- 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

35	23.677439057	192.168.2.5	192.168.2.244	TCP	125 52242 → 4444	[PSH,
36	23.677798956	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	[ACK]
39	23.682908012	192.168.2.5	192.168.2.244	TCP	133 52242 → 4444	[PSH,

Checksum: 0000	00 0c 29 82 f5 94 00 0c 29 89 f4 58 08 00 45 00	..).....)..X..E..
Urgent: 0010	00 6f 56 a2 40 00 40 06 5d 9d c0 a8 02 05 c0 a8	..oV.@.@.].....
Options: 0020	02 f4 cc 12 11 5c e0 50 4f 64 39 4a 91 49 80 18\P Od9J.I..
TCP Options: 0030	01 f6 28 16 00 00 01 01 08 0a 71 6e ed 76 11 9f(.....)qn.v..
TCP Seq: 0040	be 4c 48 69 74 3a 31 20 68 74 74 70 3a 2f 2f 75	..LHit:1 http://u
TCP Len: 0050	73 2e 61 72 63 68 69 76 65 2e 75 62 75 6e 74 75	s.archiv e ubuntu
Kin: 0060	2e 63 6f 6d 2f 75 62 75 6e 74 75 20 62 69 6f 6e	.com/ubu ntu bion
Len: 0070	69 63 20 49 6e 52 65 6c 65 61 73 65 0a	ic InRel ease-

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

Para esto le damos click derecho en wireshark del paquete 252

252	219.409444784	192.168.2.5	192.168.2.244	TCP	1684 9999 → 34972	[PSH, A
253	219.409517998	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242	[ACK] S

[Checksum: 0000 00 0c 29 82 f5 94 00 0c 29 89 f4 58 08 00 45 00 ..).....)..X..E..

Urgent f 0010 06 86 42 74 40 00 40 06 6b b4 c0 a8 02 05 c0 a8 ..Bt@.@. k.....

Options: 0020 02 f4 27 0f 88 9c 3b 30 04 e3 0b 3b 97 e4 80 18!....;0....;

TCP O: 0030 01 fe 8c c2 00 00 01 01 08 0a 71 71 ea 01 11 a2(.....)qn.v..

TCP O: 0040 bb ce 72 6f 6f 74 3a 78 3a 30 3a 30 3a 72 6f 6f ..root:x :0:0:roo

TCP O: 0050 74 3a 2f 72 6f 6f 74 3a 2f 62 69 6e 2f 62 61 73 t:/root: /bin/bas

Kin: 0060 68 0a 64 61 65 6d 6f 6e 3a 78 3a 31 3a 31 3a 64 h-daemon :x:1:1:d

Len: 0070 61 65 6d 6f 6e 3a 2f 75 73 72 2f 73 62 69 6e 3a aemon:/u sr/sbin:

Tim: 0080 2f 75 73 72 2f 73 62 69 6e 2f 6e 6f 6c 6f 67 69 /usr/sbi n/nologi

Tim: 0090 6e 0a 62 69 6e 3a 78 3a 32 3a 32 3a 62 69 6e 3a n-bin:x :2:2:bin:

[Timestamp: 00a0 2f 62 69 6e 3a 2f 75 73 72 2f 73 62 69 6e 2f 6e /bin:/us r/sbin/n

[Time: 00b0 6f 6c 6f 67 69 6e 0a 73 79 73

[Time: 00c0 3a 73 79 73 3a 2f 64 65 76 3a

[Time: 00d0 62 69 6e 2f 6e 6f 6c 6f 67 69

[SEQ/ACK: 00e0 3a 78 3a 34 3a 36 35 35 33 34

[iRTT: 00f0 2f 62 69 6e 3a 2f 62 69 6e 2f

[Byte: 0100 61 6d 65 73 3a 78 3a 35 3a 36

[Byte: 0110 73 3a 2f 75 73 72 2f 67 61 6d

TCP pay: 0120 72 2f 73 62 69 6e 2f 6e 6f 6c

ata: (1618 0130 61 6e 3a 78 3a 36 3a 31 32 3a

✓ Allow hover highlighting

Copiar bytes como volcado hexadecimal + ASCII

...como volcado hexadecimal

...as Printable Text

...as a Hex Stream

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

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
lxd:x:105:65534:./var/lib/lxd:/bin/false
uidd:x:106:110:./run/uidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:./var/cache/pollinate:/bin/false
sshd:x:110:65534:./run/sshd:/usr/sbin/nologin
jtomato:x:1000:1000:Jim Tomamto:/home/jtomato:/bin/bash
bind:x:111:113:./var/cache/bind:/usr/sbin/nologin
```


- 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 : 0xffdf000L
      KUSER_SHARED_DATA : 0xffdf000L
      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 ejecución. - 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 0
0x82b1fda0 smss.exe 560 4 21 21 0 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 2016-06-24 10:22:49 UTC+0000
```

- 4. Podemos ver un proceso de sistema sospechoso por ser padre de varios procesos de sistema que no debería. ¿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:wsentfy.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        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        0 2016-06-24 10:29:05 UTC+0000
. 0x829d06c8:net.exe 1284   1716       0        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        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        0 2016-06-24 10:28:41 UTC+0000
. 0x82a3b900:cmd.exe 3988   1716       0        0 2016-06-24 10:28:42 UTC+0000
. 0x82a153a0:reg.exe 1712   1716       0        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        0 2016-06-24 10:28:52 UTC+0000
. 0x828bc628:game.exe 1044   1716       0        0 2016-06-24 10:20:25 UTC+0000
. 0x824d20f0:net1.exe 1432   1716       0        0 2016-06-24 10:28:45 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

SUMMARY DETECTION DETAILS BEHAVIOR COMMUNITY 1

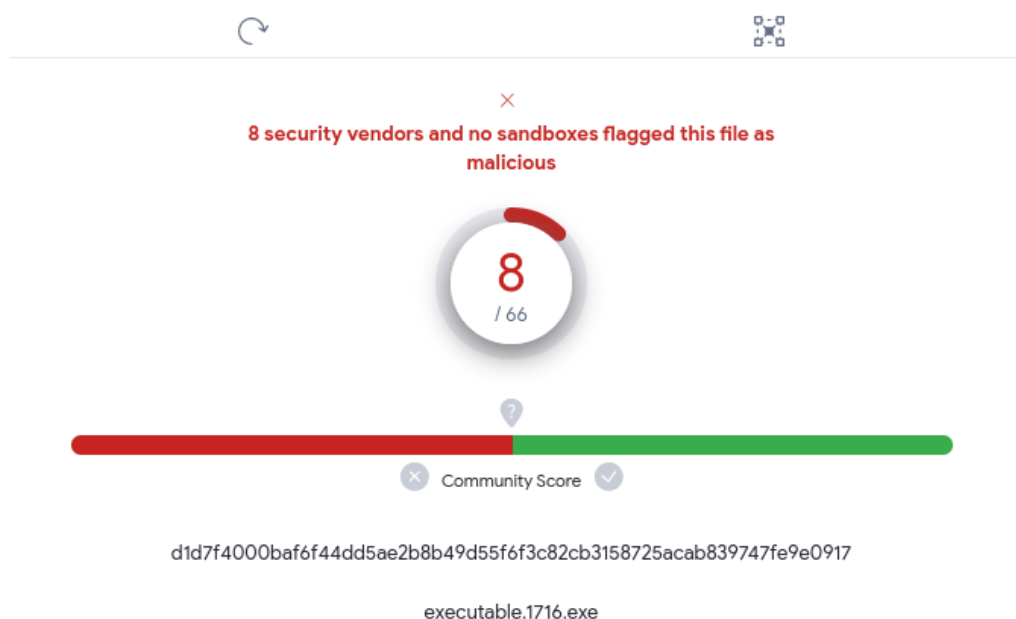
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label 🚨 pua.avax Threat categories pua virus Family labels avax

Security vendors' analysis ⓘ Do you want to automate checks?

AhnLab-V3	🚨 Malware/Gen.Generic.C1109330
Antiy-AVL	🚨 Trojan/Win32.AGeneric
CrowdStrike Falcon	🚨 Malicious_confidence_70% (W)
Cylance	🚨 Unsafe
Endgame	🚨 Malicious (moderate Confidence)
Kaspersky	🚨 Not-a-virus:RiskTool.Win32.Agent.avax
TrendMicro-HouseCall	🚨 Suspicious_GEN.F47V0124
ZoneAlarm by Check Point	🚨 Not-a-virus:RiskTool.Win32.Agent.avax

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/Analysisforens/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 \SystemRoot\System32\TSDDD.dll
0x000000000272f248 srv.sys 0xb21fd000 0x58000 \SystemRoot\system32\DRIVERS\srv.sys
0x000000000273ae38 vmemctl.sys 0xb274c000 0x3000 \??\C:\Program Files\Common Files\VMware\Drivers\memctl
\vmemctl.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 ndisui.sys 0xb29cc000 0x4000 \SystemRoot\system32\DRIVERS\ndisui.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.