

DÍA D - EJERCICIO FINAL - CTF FORENSE

Prerrequisitos

No hay flags en este CTF.

El reto forense consistente en 3 partes:

- 1- Análisis de una imagen de disco (6 preguntas)
- 2- Análisis de una captura de tráfico (9 preguntas)
- 3- Análisis de un volcado de memoria (8 preguntas)

El .zip está en Drive: Máquinas Virtuales Nombre: reto_forense_201222.zip Password: sleuth

Puntaje total: 450 puntos

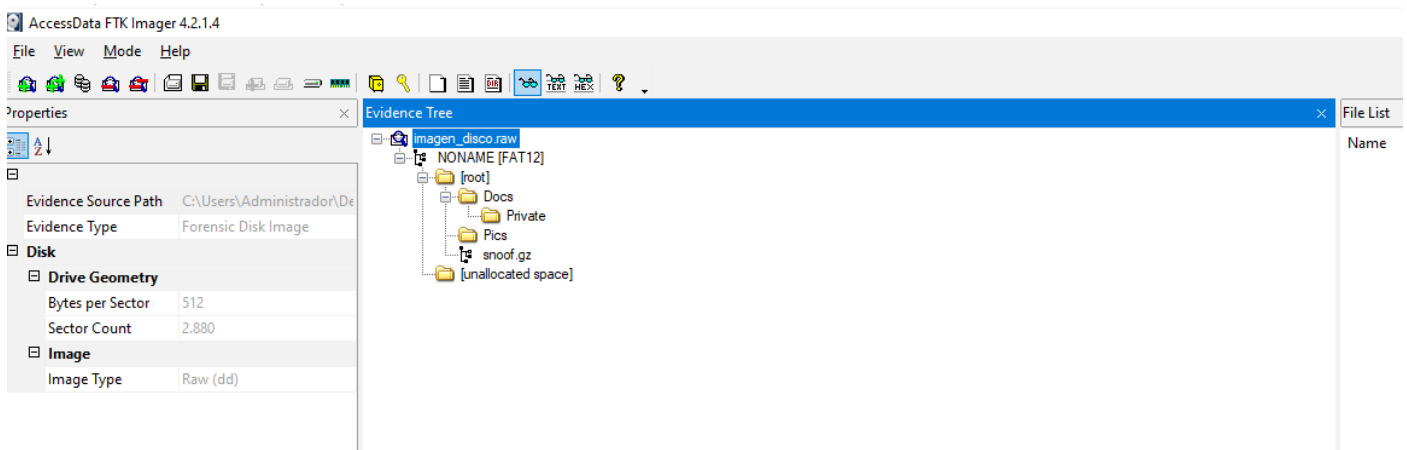
Son tres volcados de tres situaciones diferentes, no es necesario informe, si no sacar la siguiente información necesaria para el coordinador del CSIRT:

Cuestionario a rellenar

RETO FORENSE PARTE 1 - ANALISIS DE IMAGEN DE DISCO

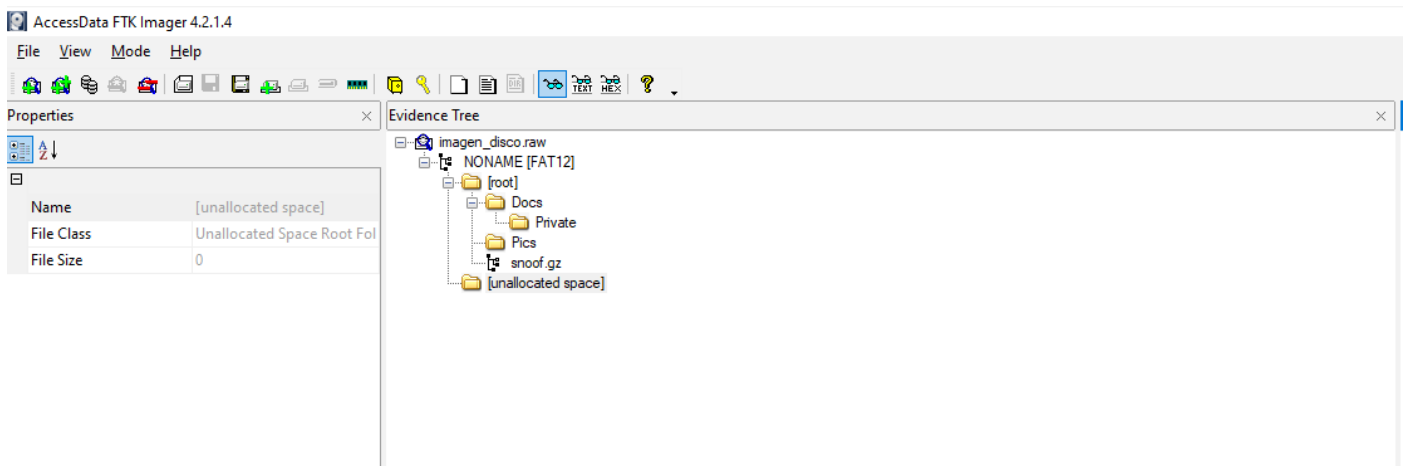
1. ¿Qué tipo de sistema de ficheros tiene la imagen?

El tipo de sistema de fichero es FAT12 según lo dice la herramienta FTK IMAGER



2. ¿Cuántos directorios hay dentro de la imagen?

El disco posee 5 directorios,



3. ¿Cuántos archivos borrados hay?

Se hallo un solo archivo aparentemente borrado

Evidence Tree

imagen_disco.raw

NO NAME (FAT12)

[root]

Docs

Private

Pics

snoof.gz

[unallocated space]

File List

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

Reynolds-Halifax

101 East Main St.

Somewhere, Ohio 43999

Septemper 21, 2000

To whom it may concearn:

I have the keys to your network. Unless you do what I say, I will hold you and your entire business ransom.

This is not a joke.

I have had enough of your mindless corporate piracy and will no longer stand for it. You will recieve another letter next week. It will have a single bank account number and bank name. I want you

Don't try anything, and dont contact the cops. If you do, I will unleash a virus that will bring down your whole network and destroy your consumer's confidence.

Don't mess with me on this!

your W0r3T N1ghTMar3EE

4. Monta la imagen para poder acceder a los ficheros.

Mount Image To Drive

Add Image

Image File:
C:\Users\Administrador\Desktop\parte1\imagen_disco.raw

Mount Type: Physical Only

Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

Write Cache Folder:
C:\Users\Administrador\Desktop\parte1

Mount

Mapped Image List

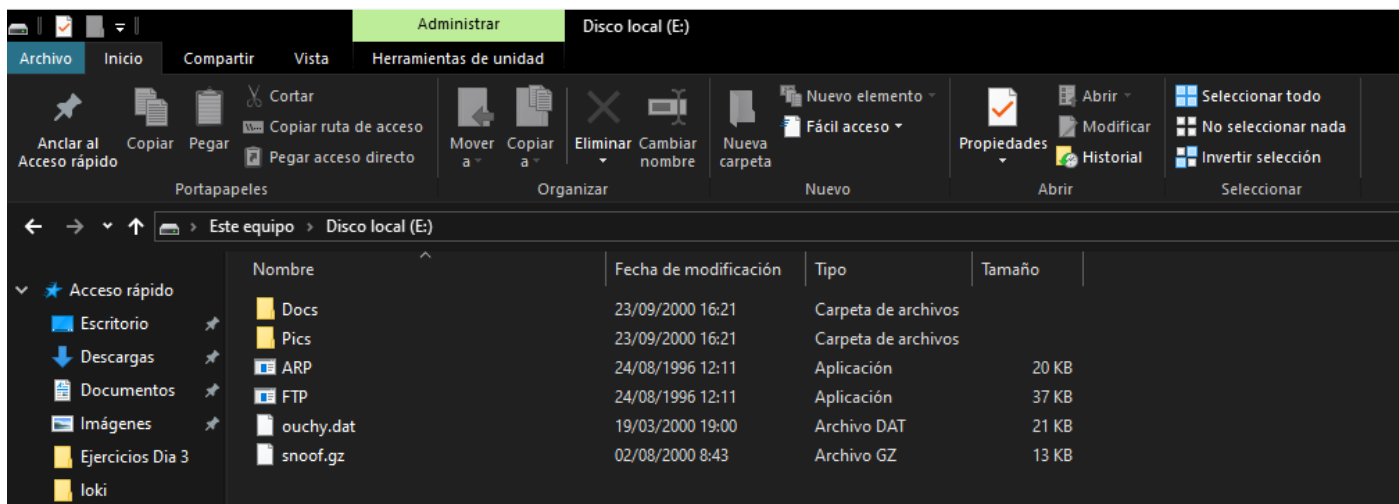
Mapped Images:

Drive	Method	Partition	Image
PhysicalDrive 1	Block Device/Read ...	Image	C:\Users\Administrador\Desktop\parte1\

< >

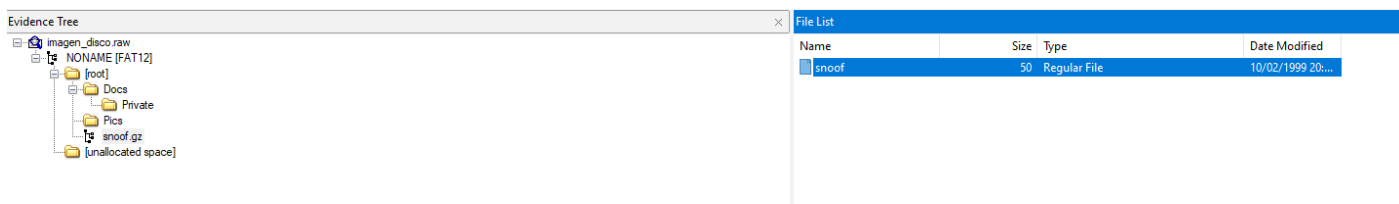
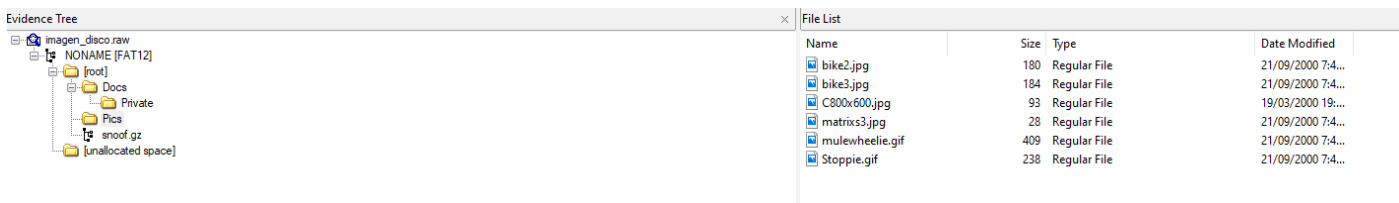
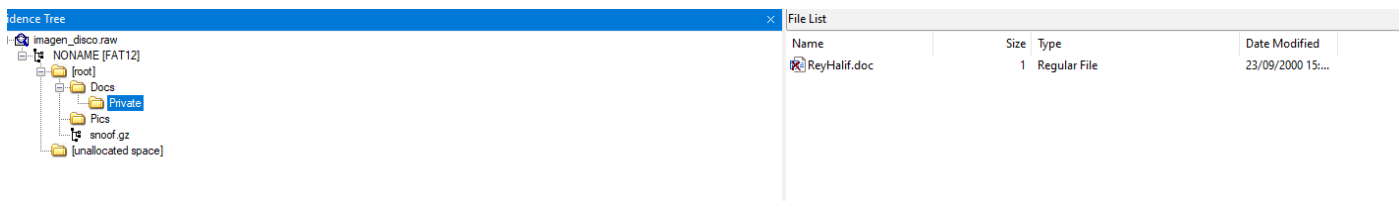
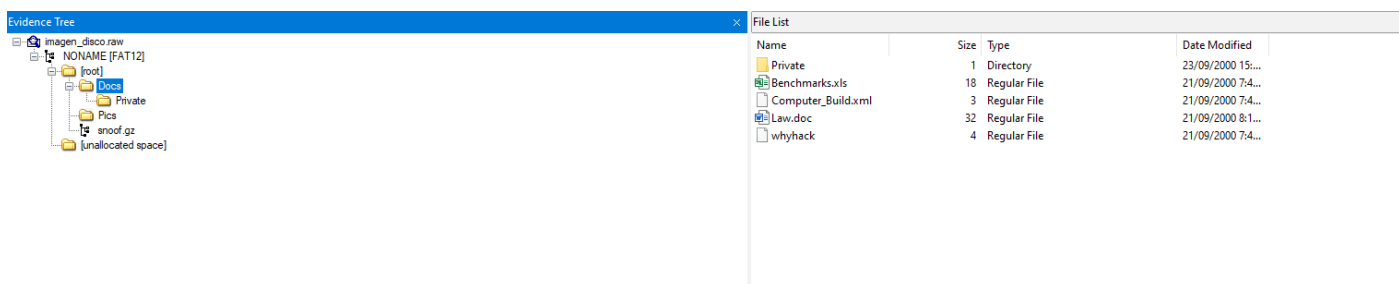
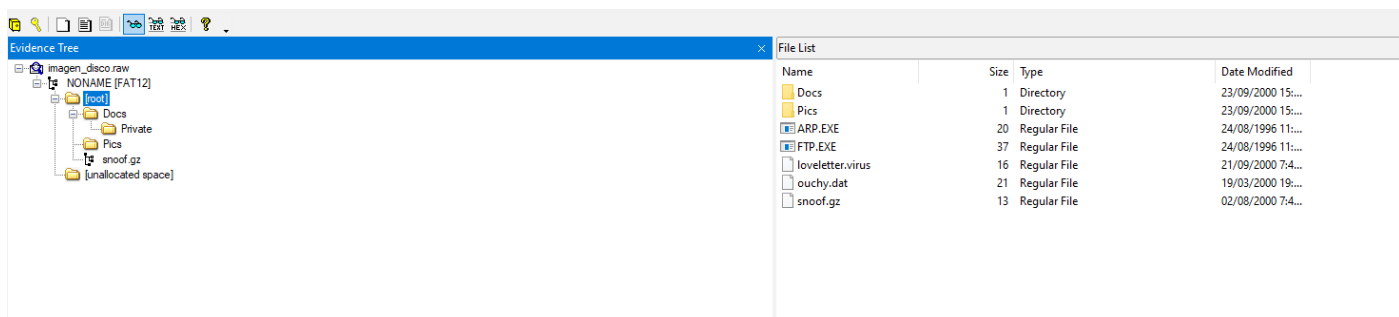
Unmount

Close



5. ¿Cuántos archivos hay en la imagen?

En la imagen hay 16 archivos visibles y un archivo borrado, en total 17, se componen de documentos Word, Excel, aplicaciones ARP Y FTP, archivos gif y jpg, además de otros archivos con formato DAT Y GZ.



6. Descarga tres de las imagenes disponibles.

Se exportaron con éxito.



RETO FORENSE PARTE 2 - ANALISIS DE CAPTURA DE TRAFICO

1. ¿Cuáles son las dos IPs que estan en la comunicacion?

Las IPs que se están comunicando son 192.168.2.244 y 192.168.2.5, estas son las que mas se comunican luego hay trafico de red hacia otras IPs.

captura_red.pcapng									
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda									
6									
No.	Time	Source	Destination	Protocol	Length	Info			
248	219.408686970	192.168.2.244	192.168.2.5	TCP	74	34972 → 9999 [SYN, Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=295877582 TSecr=0 WS=12			
249	219.409048569	192.168.2.5	192.168.2.244	TCP	74	9999 → 34972 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=1903290880 T			
250	219.409109184	192.168.2.244	192.168.2.5	TCP	66	34972 → 9999 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=295877582 TSecr=1903290880			
251	219.409440343	192.168.2.5	192.168.2.244	TCP	112	52242 → 4444 [PSH, ACK] Seq=2372 Ack=183 Win=64256 Len=46 TSval=1903290881 TSecr=29585703			
252	219.409444784	192.168.2.5	192.168.2.244	TCP	1684	9999 → 34972 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=1618 TSval=295877582 TSecr=1903290881			
253	219.409517998	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242 [ACK] Seq=183 Ack=2418 Win=64896 Len=0 TSval=295877583 TSecr=1903290881			
254	219.409519692	192.168.2.244	192.168.2.5	TCP	66	34972 → 9999 [ACK] Seq=1 Ack=1619 Win=64128 Len=0 TSval=295877583 TSecr=1903290881			
255	235.284704649	192.168.2.244	192.168.2.5	TCP	66	34972 → 9999 [FIN, ACK] Seq=1 Ack=1619 Win=64128 Len=0 TSval=295893458 TSecr=1903290881			
256	235.285018280	192.168.2.5	192.168.2.244	TCP	66	9999 → 34972 [FIN, ACK] Seq=1619 Ack=2 Win=65280 Len=0 TSval=1903306756 TSecr=295893458			
257	235.285622140	192.168.2.244	192.168.2.5	TCP	66	34972 → 9999 [ACK] Seq=2 Ack=1620 Win=64128 Len=0 TSval=295893458 TSecr=1903306756			
258	235.286610310	192.168.2.5	192.168.2.244	TCP	82	52242 → 4444 [PSH, ACK] Seq=2418 Ack=183 Win=64256 Len=16 TSval=1903306757 TSecr=29587758			
259	235.286682057	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242 [ACK] Seq=183 Ack=2434 Win=64896 Len=0 TSval=295893460 TSecr=1903306757			
260	243.021223918	192.168.2.244	192.168.2.5	TCP	71	4444 → 52242 [PSH, ACK] Seq=183 Ack=2434 Win=64896 Len=5 TSval=295901194 TSecr=1903306757			
261	243.021446553	192.168.2.5	192.168.2.244	TCP	70	52242 → 4444 [PSH, ACK] Seq=2434 Ack=188 Win=64256 Len=4 TSval=295901194 TSecr=295901194			
262	243.021579548	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242 [ACK] Seq=188 Ack=2438 Win=64896 Len=0 TSval=295901195 TSecr=1903314492			
263	243.021634919	192.168.2.5	192.168.2.244	TCP	72	52242 → 4444 [PSH, ACK] Seq=2438 Ack=188 Win=64256 Len=6 TSval=1903314492 TSecr=295901195			
264	243.021780577	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242 [ACK] Seq=188 Ack=2444 Win=64896 Len=0 TSval=295901195 TSecr=1903314492			
265	243.022062328	192.168.2.5	192.168.2.244	TCP	66	52242 → 4444 [FIN, ACK] Seq=2444 Ack=188 Win=64256 Len=0 TSval=1903314492 TSecr=295901195			
266	243.022203458	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242 [FIN, ACK] Seq=188 Ack=2445 Win=64896 Len=0 TSval=295901195 TSecr=1903314492			
267	243.022298881	192.168.2.5	192.168.2.244	TCP	66	52242 → 4444 [ACK] Seq=2445 Ack=189 Win=64256 Len=0 TSval=1903314493 TSecr=295901195			

2. ¿A qué puerto se están conectando?

Se conectan mayormente a los puertos 52242 y 4444

196	152.054787590	192.168.2.244	192.168.2.5	TCP	99	4444 → 52242 [PSH, ACK] Seq=91 Ack=2069 Win=64896 Len=33 TSval=295810228 TSecr=1903115057			
197	152.055423048	192.168.2.5	192.168.2.244	TCP	98	52242 → 4444 [PSH, ACK] Seq=2069 Ack=124 Win=64256 Len=32 TSval=1903223530 TSecr=295810228			
198	152.055427131	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242 [ACK] Seq=124 Ack=2101 Win=64896 Len=0 TSval=295810229 TSecr=1903223530			
199	152.055697037	192.168.2.5	192.168.2.244	TCP	67	52242 → 4444 [PSH, ACK] Seq=2101 Ack=124 Win=64256 Len=1 TSval=1903223530 TSecr=295810229			
200	152.055711745	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242 [ACK] Seq=124 Ack=2102 Win=64896 Len=0 TSval=295810229 TSecr=1903223530			
201	152.075098120	192.168.2.5	192.168.2.244	TCP	72	52242 → 4444 [PSH, ACK] Seq=2102 Ack=124 Win=64256 Len=6 TSval=1903223550 TSecr=295810229			
202	152.075207847	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242 [ACK] Seq=124 Ack=2108 Win=64896 Len=0 TSval=295810248 TSecr=1903223550			
203	152.075310160	192.168.2.5	192.168.2.244	TCP	113	52242 → 4444 [PSH, ACK] Seq=2108 Ack=124 Win=64256 Len=47 TSval=1903223550 TSecr=295810248			
204	152.075356959	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242 [ACK] Seq=124 Ack=2155 Win=64896 Len=0 TSval=295810249 TSecr=1903223550			
205	152.076048943	192.168.2.5	192.168.2.244	TCP	103	52242 → 4444 [PSH, ACK] Seq=2155 Ack=124 Win=64256 Len=37 TSval=1903223551 TSecr=295810249			
206	152.076099203	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242 [ACK] Seq=124 Ack=2192 Win=64896 Len=0 TSval=295810249 TSecr=1903223551			
207	152.077759590	192.168.2.5	192.168.2.244	TCP	82	52242 → 4444 [PSH, ACK] Seq=2192 Ack=124 Win=64256 Len=16 TSval=1903223552 TSecr=295810249			
208	152.077785170	192.168.2.244	192.168.2.5	TCP	66	4444 → 52242 [ACK] Seq=124 Ack=2208 Win=64896 Len=0 TSval=295810251 TSecr=1903223552			

3. ¿Qué comando se ha realizado?

Se realizo una consulta o query. El registro SRV es un registro de recursos del Sistema de nombres de dominio (DNS) . Se utiliza para identificar equipos que alojan servicios específicos. Los registros de recursos SRV se utilizan para localizar controladores de dominio para Active Directory

STANDARD QUERY 0X4805 SRV _HTTP._TCP.US.ARCHIVE.UBUNTU.COM OPT

25	23.514987554	192.168.2.5	192.168.2.1	DNS	103 Standard query 0x4805 SRV _http._tcp.us.archive.ubuntu.com OPT
26	23.639809648	192.168.2.1	192.168.2.5	DNS	183 Standard query response 0x4805 SRV _http._tcp.us.archive.ubuntu.c

```
Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.1
User Datagram Protocol, Src Port: 45537, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x4805
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  Queries
    _http._tcp.us.archive.ubuntu.com: type SRV, class IN
  Additional records
    <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 512
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
      Z: 0x0000
      Data length: 0
    [Response in: 26]
```

```
Answer RRs: 2
Authority RRs: 0
Additional RRs: 1
Queries
  _http._tcp.us.archive.ubuntu.com: type SRV, class IN
Answers
  _http._tcp.us.archive.ubuntu.com: type SRV, class IN, priority 0, weight 0, port 80, target banjo.canonical.com
    Service: _http
    Protocol: _tcp
    Name: us.archive.ubuntu.com
    Type: SRV (Server Selection) (33)
    Class: IN (0x0001)
    Time to live: 600 (10 minutes)
    Data length: 27
    Priority: 0
    Weight: 0
    Port: 80
    Target: banjo.canonical.com
  _http._tcp.us.archive.ubuntu.com: type SRV, class IN, priority 0, weight 0, port 80, target kazooie.canonical.com
    Service: _http
    Protocol: _tcp
```

```
_http._tcp.us.archive.ubuntu.com: type SRV, class IN, priority 0, weight 0, port 80, target kazooie.canonical.com
  Service: _http
  Protocol: _tcp
  Name: us.archive.ubuntu.com
  Type: SRV (Server Selection) (33)
  Class: IN (0x0001)
  Time to live: 600 (10 minutes)
  Data length: 29
  Priority: 0
  Weight: 0
  Port: 80
  Target: kazooie.canonical.com
```

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

Se ha levantado el servicio NTP, en el puerto 123

5	0.038321640	192.168.2.244	192.168.2.5	TCP	66 4444 → 52242 [ACK] Seq=1 Ack=17 Win=65152 Len=0 TSval=295658211 TSecr=1903071520
6	5.108590883	VMware_89:f4:58	VMware_82:f5:94	ARP	60 Who has 192.168.2.244? Tell 192.168.2.5
7	5.108826513	VMware_82:f5:94	VMware_89:f4:58	ARP	60 192.168.2.244 is at 00:0c:29:82:f5:94
8	5.181983782	VMware_82:f5:94	VMware_89:f4:58	ARP	60 Who has 192.168.2.5? Tell 192.168.2.244
9	5.182215270	VMware_89:f4:58	VMware_82:f5:94	ARP	60 192.168.2.5 is at 00:0c:29:89:f4:58
10	10.380426906	192.168.2.10	45.76.244.202	NTP	90 NTP Version 4, client
11	10.449422795	45.76.244.202	192.168.2.10	NTP	90 NTP Version 4, server
12	15.387906737	VMware_20:42:30	VMware_88:1d:63	ARP	60 Who has 192.168.2.1? Tell 192.168.2.10
13	15.387928302	VMware_88:1d:63	VMware_20:42:30	ARP	60 192.168.2.1 is at 00:0c:29:88:1d:63
14	23.052072590	192.168.2.10	192.168.2.2	TCP	66 139 → 43926 [ACK] Seq=1 Ack=1 Win=361 Len=0 TSval=4143298560 TSecr=101216154
15	23.421270737	192.168.2.244	192.168.2.5	TCP	107 4444 → 52242 [PSH, ACK] Seq=1 Ack=17 Win=65152 Len=41 TSval=295681594 TSecr=1903071520
16	23.421420769	192.168.2.5	192.168.2.244	TCP	66 52242 → 4444 [ACK] Seq=17 Ack=42 Win=64256 Len=0 TSval=1903094902 TSecr=295681594

```

User Datagram Protocol, Src Port: 39418, Dst Port: 123
  Source Port: 39418
  Destination Port: 123
  Length: 56
  Checksum: 0x3cff [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Timestamps]
  UDP payload (48 bytes)

```

5. ¿Qué versión del paquete se ha instalado?

Se instalo la versión 4

Time	Source	Destination	Protocol	Length	Info
10	10.380426906	192.168.2.10	NTP	90	NTP Version 4, client
11	10.449422795	45.76.244.202	NTP	90	NTP Version 4, server

6. ¿Qué archivo se ha enviado?

Se ha descargado el archivo Request URI: /ubuntu/pool/universe/n/netcat/netcat_1.10-41.1_all.deb,

```

Hypertext Transfer Protocol
  GET /ubuntu/pool/universe/n/netcat/netcat_1.10-41.1_all.deb HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /ubuntu/pool/universe/n/netcat/netcat_1.10-41.1_all.deb HTTP/1.1\r\n]
  [GET /ubuntu/pool/universe/n/netcat/netcat_1.10-41.1_all.deb HTTP/1.1\r\n]
  [Severity level: Chat]
  [Group: Sequence]
  Request Method: GET
  Request URI: /ubuntu/pool/universe/n/netcat/netcat_1.10-41.1_all.deb
  Request Version: HTTP/1.1
  Host: us.archive.ubuntu.com\r\n
  User-Agent: Debian APT-HTTP/1.3 (1.6.12)\r\n
  \r\n
  [Full request URI: http://us.archive.ubuntu.com/ubuntu/pool/universe/n/netcat/netcat_1.10-41.1_all.deb]
  [HTTP request 1/1]

```

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

8. ¿Qué distribución de Linux se está utilizando?

Esta utilizando linux y la distribución debian.

```

Host: us.archive.ubuntu.com\r\n
User-Agent: Debian APT-HTTP/1.3 (1.6.12)\r\n
\r\n

```

Debian APT-HTTP/1.3 (1.0.1ubuntu2)

browser:

operating system: Debian linux

primarily used on: -

9. ¿Cuántos usuarios hay en el sistema atacado?

RETO FORENSE PARTE 3 - ANALISIS DE MEMORIA

1. Identificar el tipo de sistema operativo de la máquina.

El sistema operativo utilizado es Windows XPSP2x86 / WindowsXPS3x86

```
(root@kali)-[/home/veronica/Documentos/blue_team/volatility_2.6_lin64_standalone]
# ./volatility_2.6_lin64_standalone 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 (/home/veronica/Documentos/blue_team/volatility_2.6_lin64_standalone/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.

```
(root@kali)-[/home/veronica/Documentos/blue_team/volatility_2.6_lin64_standalone]
# ./volatility_2.6_lin64_standalone --profile=WinXPSP3x86 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     0 2016-06-24 09:06:48 UTC+0000
0x82b1fda0 smss.exe            560   4      2    21   0     0     0 2016-06-24 09:06:51 UTC+0000
0x829e4020 csrss.exe            676  560    12   421   0     0     0 2016-06-24 09:06:53 UTC+0000
0x82a7ada0 winlogon.exe         700  560    22   649   0     0     0 2016-06-24 09:07:02 UTC+0000
0x829e7960 services.exe       756  700    16   378   0     0     0 2016-06-24 09:07:07 UTC+0000
0x827b5990 lsass.exe           768  700    19   361   0     0     0 2016-06-24 09:07:17 UTC+0000
0x8293c3d8 vmacthlp.exe         924  756     1    38   0     0     0 2016-06-24 09:07:21 UTC+0000
0x825eb308 svchost.exe          984  756    23   235   0     0     0 2016-06-24 09:07:23 UTC+0000
0x827b4020 svchost.exe         1048  756    10   262   0     0     0 2016-06-24 09:07:23 UTC+0000
0x825d3958 svchost.exe         1192  756    73  1481   0     0     0 2016-06-24 09:07:24 UTC+0000
0x82595b20 svchost.exe         1404  756     4    73   0     0     0 2016-06-24 09:07:26 UTC+0000
0x82921020 svchost.exe         1544  756    12   183   0     0     0 2016-06-24 09:07:29 UTC+0000
0x825804b8 explorer.exe        1716 1700    14   559   0     0     0 2016-06-24 09:07:32 UTC+0000
0x828b0020 spoolsv.exe          1820  756    12   163   0     0     0 2016-06-24 09:07:39 UTC+0000
0x82547da0 rundll32.exe         660 1716     4    73   0     0     0 2016-06-24 09:07:39 UTC+0000
0x82546878 vmtoolsd.exe         732 1716     3   117   0     0     0 2016-06-24 09:07:39 UTC+0000
0x8287b020 svchost.exe         1984  756     4   105   0     0     0 2016-06-24 09:07:47 UTC+0000
0x8253a298 svchost.exe         2020  756     4   100   0     0     0 2016-06-24 09:07:47 UTC+0000
0x82871870 vmtoolsd.exe         208  756     7   282   0     0     0 2016-06-24 09:08:09 UTC+0000
0x828375c0 TPAutoConnSvc.e     1384  756     5   116   0     0     0 2016-06-24 09:08:09 UTC+0000
0x824f2da0 wscntfy.exe         1420 1192     1    36   0     0     0 2016-06-24 09:08:10 UTC+0000
0x8284b8f8 alg.exe           1504  756     5   102   0     0     0 2016-06-24 09:08:38 UTC+0000
0x827b6150 notepad.exe          2816 1716     1    60   0     0     0 2016-06-24 09:09:38 UTC+0000
0x82a92da0 ctfmon.exe          3748 3396     1    88   0     0     0 2016-06-24 09:36:08 UTC+0000
0x825d03b0 csrss.exe            836  560     0     0   3     0     0 2016-06-24 10:07:18 UTC+0000
0x828a2b88 TPAutoConnect.e     2940 1384     1    78   0     0     0 2016-06-24 10:07:34 UTC+0000
0x824d2020 wuauclt.exe          2012 1192     3   111   0     0     0 2016-06-24 10:20:25 UTC+0000
0x828bc628 game.exe      1044 1716     0     0   0     0     0 2016-06-24 10:26:05 UTC+0000
0x829d18c8 cmd.exe             2632 1716     1    40   0     0     0 2016-06-24 10:27:32 UTC+0000
0x82a75020 sc.exe             3120 2632     1    33   0     0     0 2016-06-24 10:27:51 UTC+0000
0x82828620 cmd.exe             3508 1716     1    42   0     0     0 2016-06-24 10:28:22 UTC+0000
0x82adc020 sc.exe             3316 3508     1    35   0     0     0 2016-06-24 10:28:39 UTC+0000
0x8250d8a8 netstat.exe          3868 1716     0     0   0     0     0 2016-06-24 10:28:40 UTC+0000
0x8250c020 netstat.exe          2956 1716     0     0   0     0     0 2016-06-24 10:28:42 UTC+0000
0x82a3b900 cmd.exe             3988 1716     0     0   0     0     0 2016-06-24 10:28:42 UTC+0000
0x82a3b020 net1.exe            3292 3900     0     0   0     0     0 2016-06-24 10:28:43 UTC+0000
0x824d39f8 net1.exe            1412 1240     0     0   0     0     0 2016-06-24 10:28:45 UTC+0000
0x828a2020 net1.exe            620  2256     0     0   0     0     0 2016-06-24 10:28:45 UTC+0000
0x829d06c8 net.exe         1284 1716     0     0   0     0     0 2016-06-24 10:28:46 UTC+0000
0x82a3c3c0 net1.exe            3776 3964     0     0   0     0     0 2016-06-24 10:28:47 UTC+0000
0x824b67b8 net1.exe            948  3888     0     0   0     0     0 2016-06-24 10:28:48 UTC+0000
0x82a736d8 systeminfo.exe    4008 1716     0     0   0     0     0 2016-06-24 10:28:49 UTC+0000
0x82a153a0 reg.exe             1712 1716     0     0   0     0     0 2016-06-24 10:28:50 UTC+0000
0x824a4888 reg.exe             3232 1716     0     0   0     0     0 2016-06-24 10:28:52 UTC+0000
0x828d7af0 cmd.exe             3068 1716     1    65   0     0     0 2016-06-24 10:29:01 UTC+0000
```

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

Parece extraño el proceso sgame.exe, sospechoso, por su corta duración, y se busca alguna referencia acerca de este proceso, en internet se encontró,

0x824d2020 wuauclt.exe	2012	1192	3	111	0	0	2016-06-24 10:07:34 UTC+0000	
0x828bc628 game.exe	1044	1716	0		0	0	2016-06-24 10:20:25 UTC+0000	2016-06-24 10:22:49 UTC+0000
0x829d18c8 cmd.exe	2632	1716	1	40	0	0	2016-06-24 10:26:05 UTC+0000	

game.exe es un proceso que se coloca como W32.Gaze@mm worm. Este virus se distribuye vía el Internet a través del email y viene bajo la forma de correo electrónico, con la esperanza de que usted abra su conexión hostil. El gusano tiene su propio motor del smtp que los medios él recolecte los emails de su ordenador local y los redistribuyan sí mismo. En peores casos este gusano puede permitir que los atacantes tengan acceso a su ordenador, robando palabras de paso y datos personales. Este proceso es un riesgo para la seguridad y se debe quitar de su sistema. Ver por favor los detalles adicionales con respecto a este proceso.

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?.

```
(root@kali)-[/home/veronica/Documentos/blue_team/volatility_2.6_lin64_standalone]
# ./volatility_2.6_lin64_standalone --profile=WinXPSP3x86 pstree -f memoria.vmem
Volatility Foundation Volatility Framework 2.6
```

Name	Time	Source	Pid	PPid	Thds	Hnds	Time
0x82bc6660:System	192.168.2.244	192.168.2.5	4	0	59	336	1970-01-01 00:00:00 UTC+0000
0x82b1fda0:smss.exe	192.168.2.5	192.168.2.5	560	4	2	21	2016-06-24 09:06:48 UTC+0000
0x829e4020:csrss.exe	192.168.2.244	192.168.2.5	676	560	12	421	2016-06-24 09:06:51 UTC+0000
0x82a7ada0:winlogon.exe	192.168.2.5	192.168.2.5	700	560	22	649	2016-06-24 09:06:53 UTC+0000
0x827b5990:lsass.exe	192.168.2.244	192.168.2.5	768	700	19	361	2016-06-24 09:07:07 UTC+0000
0x829e7960:services.exe	192.168.2.5	192.168.2.5	756	700	16	378	2016-06-24 09:07:02 UTC+0000
0x82921020:svchost.exe	192.168.2.244	192.168.2.5	1544	756	12	183	2016-06-24 09:07:26 UTC+0000
0x827b4020:svchost.exe	192.168.2.5	192.168.2.5	1048	756	10	262	2016-06-24 09:07:23 UTC+0000
0x828b0020:spoolsv.exe	192.168.2.244	192.168.2.5	1820	756	12	163	2016-06-24 09:07:32 UTC+0000
0x825d3958:svchost.exe	192.168.2.5	192.168.2.5	1192	756	73	1481	2016-06-24 09:07:23 UTC+0000
0x824f2da0:wscntfy.exe	192.168.2.244	192.168.2.5	1420	1192	1	36	2016-06-24 09:08:09 UTC+0000
0x824d2020:wuauclt.exe	192.168.2.5	192.168.2.5	2012	1192	3	111	2016-06-24 10:07:34 UTC+0000
0x8293c3d8:vmacthlp.exe	192.168.2.244	192.168.2.5	924	756	1	38	2016-06-24 09:07:17 UTC+0000
0x8287b020:svchost.exe	192.168.2.5	192.168.2.5	1984	756	4	105	2016-06-24 09:07:47 UTC+0000
0x82871870:vmtoolsd.exe	192.168.2.244	192.168.2.5	208	756	7	282	2016-06-24 09:07:47 UTC+0000
0x825eb308:svchost.exe	192.168.2.5	192.168.2.5	984	756	23	235	2016-06-24 09:07:21 UTC+0000
0x8284b8f8:alg.exe	192.168.2.244	192.168.2.5	1504	756	5	102	2016-06-24 09:08:10 UTC+0000
0x8253a298:svchost.exe	192.168.2.5	192.168.2.5	2020	756	4	100	2016-06-24 09:07:47 UTC+0000
0x828375c0:TPAutoConnSvc.e	192.168.2.244	192.168.2.5	1384	756	5	116	2016-06-24 09:08:09 UTC+0000
0x828a2b88:TPAutoConnect.e	192.168.2.5	192.168.2.5	2940	1384	1	78	2016-06-24 10:07:18 UTC+0000
0x82595b20:svchost.exe	192.168.2.244	192.168.2.5	1404	756	4	73	2016-06-24 09:07:24 UTC+0000
0x825d03b0:csrss.exe	192.168.2.5	192.168.2.5	836	560	0		2016-06-24 09:36:08 UTC+0000
0x825804b8:explorer.exe	192.168.2.244	192.168.2.5	1716	1700	14	559	2016-06-24 09:07:29 UTC+0000
0x827b6150:notepad.exe	192.168.2.5	192.168.2.5	2816	1716	1	60	2016-06-24 09:08:38 UTC+0000
0x82547da0:rundll32.exe	192.168.2.244	192.168.2.5	660	1716	4	73	2016-06-24 09:07:39 UTC+0000
0x824a4888:reg.exe	192.168.2.5	192.168.2.5	3232	1716	0		2016-06-24 10:29:05 UTC+0000
0x829d06c8:net.exe	192.168.2.244	192.168.2.5	1284	1716	0		2016-06-24 10:28:48 UTC+0000
0x82828620:cmd.exe	192.168.2.5	192.168.2.5	3508	1716	1	42	2016-06-24 10:27:51 UTC+0000
0x82adc020:sc.exe	192.168.2.244	192.168.2.5	3316	3508	1	35	2016-06-24 10:28:22 UTC+0000
0x8250d8a8:netstat.exe	192.168.2.5	192.168.2.5	3868	1716	0		2016-06-24 10:28:39 UTC+0000
0x829d18c8:cmd.exe	192.168.2.244	192.168.2.5	2632	1716	1	40	2016-06-24 10:26:05 UTC+0000
0x82a75020:sc.exe	192.168.2.5	192.168.2.5	3120	2632	1	33	2016-06-24 10:27:32 UTC+0000
0x8250c020:netstat.exe	192.168.2.244	192.168.2.5	2956	1716	0		2016-06-24 10:28:41 UTC+0000
0x82a3b900:cmd.exe	192.168.2.5	192.168.2.5	3988	1716	0		2016-06-24 10:28:42 UTC+0000
0x82a153a0:reg.exe	192.168.2.244	192.168.2.5	1712	1716	0		2016-06-24 10:29:00 UTC+0000
0x82546878:vmtoolsd.exe	192.168.2.5	192.168.2.5	732	1716	3	117	2016-06-24 09:07:39 UTC+0000
0x828d7af0:cmd.exe	192.168.2.244	192.168.2.5	3068	1716	1	65	2016-06-24 10:30:19 UTC+0000
0x82a736d8:systeminfo.exe	192.168.2.5	192.168.2.5	4008	1716	0		2016-06-24 10:28:52 UTC+0000
0x828bc628:game.exe	192.168.2.244	192.168.2.5	1044	1716	0		2016-06-24 10:20:25 UTC+0000
0x824d39f8:net1.exe	192.168.2.5	192.168.2.5	1412	1240	0		2016-06-24 10:28:45 UTC+0000
0x824b67b8:net1.exe	192.168.2.244	192.168.2.5	948	3888	0		2016-06-24 10:28:51 UTC+0000
0x82a3b020:net1.exe	192.168.2.5	192.168.2.5	3292	3900	0		2016-06-24 10:28:44 UTC+0000
0x82a92da0:ctfmon.exe	192.168.2.244	192.168.2.5	3748	3396	1	88	2016-06-24 09:09:38 UTC+0000
0x828a2020:net1.exe	192.168.2.5	192.168.2.5	620	2256	0		2016-06-24 10:28:47 UTC+0000
0x82a3c3c0:net1.exe	192.168.2.244	192.168.2.5	3776	3964	0		2016-06-24 10:28:50 UTC+0000

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

```
(root@kali)-[/home/veronica/Documentos/blue_team/volatility_2.6_lin64_standalone]
# ./volatility_2.6_lin64_standalone 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
```

```
(root@kali)-[/home/veronica/Documentos/blue_team/volatility_2.6_lin64_standalone]
# ./volatility_2.6_lin64_standalone 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
0x02bcb2a0 192.168.78.135:445 192.168.78.128:49078 4
0x02bcbfe8 192.168.78.135:1046 192.168.78.128:4444 3696
0x02c3bb68 192.168.78.135:1045 192.168.78.128:4444 1044
```

Puede que sean sospechosas las conexiones de la IP 192.168.78.135:1046 A 192.168.78.128:4444 PID 1044 que corresponde a game.exe y que se encuentra activo y el otro podría ser 192.168.78.135:1046 a 192.168.78.128:4444 PID 3696 correspondiente a ctfmon.exe, parece un software de aplicación.

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?.

El malware aparentemente es game.exe, aquí se puede ver la ruta del ejecutable.

```
REG_BINARY  UEME_RUNPATH:C:\Documents and Settings\Administrator\Desktop\game.exe :
ID:          1
Count:       2
Last updated: 2016-06-24 10:21:18 UTC+0000
Raw Data:
0x00000000  01 00 00 00 07 00 00 00 d0 94 6d 25 02 ce d1 01  ....m%....
```

game.exe es un proceso que se coloca como W32.Gaze@mm worm. Este virus se distribuye vía el Internet a través del email y viene bajo la forma de correo electrónico, con la esperanza de que usted abra su conexión hostil. El gusano tiene su propio motor del smtp que los medios él recolecten los email de su ordenador local y los redistribuyan sí mismo. En peores casos este gusano puede permitir que los atacantes tengan acceso a su ordenador, robando palabras de paso y datos personales. Este proceso es un riesgo para la seguridad y se debe quitar de su sistema. Ver por favor los detalles adicionales con respecto a este proceso.

Los procesos no relacionados con el sistema como game.exe se originan a partir del software que ha instalado en sus sistema. Como la mayoría de las aplicaciones almacenan datos en el disco duro y en el registro del sistema, es probable que su ordenador haya sufrido una fragmentación y entradas no válidas acumuladas que pueden afectar el rendimiento de su PC.

En Windows Task Manager, puede ver qué CPU, memoria, disco y utilización de red está provocando el proceso W32.Gaze@mm worm. Para acceder al Task Manager, mantén pulsadas las teclas Ctrl + Mayúsculas + Esc al mismo tiempo. Estos tres botones están situados en el extremo izquierdo del teclado.

El game.exe es un archivo ejecutable en el disco duro de tu ordenador. El archivo contiene un código máquina. Si inicia el software W32.Gaze@mm worm en tu PC, el comando que contiene game.exe se ejecutará en tu PC. Para este fin, el archivo se carga en la memoria principal (RAM) y funciona ahí como un proceso de W32.Gaze@mm worm (también denominado una tarea).

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

El ultimo ejecutable lanzado fue un cmd

```
(root@kali)-[/home/veronica/Documentos/blue_team/volatility_2.6_lin64_standalone]
# ./volatility_2.6_lin64_standalone --profile=WinXPSP3x86 pslist -f memoria.vmem
```

Volatility Foundation Volatility Framework 2.6	Offset(V)	Name	PPID	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x82bc6660	System	4387	192.168.2.2	44	0	59	168	336	0	0	2016-06-24 09:06:44 UTC+0000
0x82b1fda0	smss.exe	4388	192.168.2.2	560	4	2	168	21	0	0	2016-06-24 09:06:48 UTC+0000
0x829e4020	csrss.exe	4387	192.168.2.2	676	560	12	168	421	0	0	2016-06-24 09:06:51 UTC+0000
0x82a7ada0	winlogon.exe	4388	192.168.2.2	700	560	22	168	649	44	0	2016-06-24 09:06:53 UTC+0000
0x829e7960	services.exe	4388	192.168.2.2	756	700	16	168	378	0	0	2016-06-24 09:07:02 UTC+0000
0x827b5990	lsass.exe	4388	192.168.2.2	768	700	19	168	361	44	0	2016-06-24 09:07:07 UTC+0000
0x8293c3d8	vmacthlp.exe	4388	192.168.2.2	924	756	1	168	38	0	0	2016-06-24 09:07:17 UTC+0000
0x825eb308	svchost.exe	4388	192.168.2.2	984	756	23	168	235	0	0	2016-06-24 09:07:21 UTC+0000
0x827b4020	svchost.exe	4388	192.168.2.2	1048	756	10	168	262	44	0	2016-06-24 09:07:23 UTC+0000
0x825d3958	svchost.exe	4388	192.168.2.2	1192	756	73	168	1481	0	0	2016-06-24 09:07:23 UTC+0000
0x82595b20	svchost.exe	4388	192.168.2.2	1404	756	4	168	73	44	0	2016-06-24 09:07:24 UTC+0000
0x82921020	svchost.exe	4388	192.168.2.2	1544	756	12	168	183	0	0	2016-06-24 09:07:26 UTC+0000
0x825804b8	explorer.exe	4388	192.168.2.2	1716	1700	14	168	559	44	0	2016-06-24 09:07:29 UTC+0000
0x828b0020	spoolsv.exe	4388	192.168.2.2	1820	756	12	168	163	0	0	2016-06-24 09:07:32 UTC+0000
0x82547da0	rundll32.exe	4388	192.168.2.2	660	1716	4	168	73	44	0	2016-06-24 09:07:39 UTC+0000
0x82546878	vmtoolsd.exe	4388	192.168.2.2	732	1716	3	168	117	0	0	2016-06-24 09:07:39 UTC+0000
0x8287b020	svchost.exe	4388	192.168.2.2	1984	756	4	168	105	0	0	2016-06-24 09:07:47 UTC+0000
0x8253a298	svchost.exe	4388	192.168.2.2	2020	756	4	168	100	44	0	2016-06-24 09:07:47 UTC+0000
0x82871870	vmtoolsd.exe	4388	192.168.2.2	208	756	17	168	282	0	0	2016-06-24 09:07:47 UTC+0000
0x828375c0	TPAutoConnSvc.e	4388	192.168.2.2	1384	756	5	68	116	20	0	2016-06-24 09:08:09 UTC+0000
0x824f2da0	wscntfy.exe	4388	192.168.2.2	1420	1192	1	168	36	0	0	2016-06-24 09:08:09 UTC+0000
0x8284b8f8	alg.exe	4388	192.168.2.2	1504	756	5	68	102	0	0	2016-06-24 09:08:10 UTC+0000
0x827b6150	notepad.exe	4388	192.168.2.2	2816	1716	1	68	60	0	0	2016-06-24 09:08:38 UTC+0000
0x82a92da0	ctfmon.exe	4388	192.168.2.2	3748	3396	1	88	0	0	0	2016-06-24 09:09:38 UTC+0000
0x825d03b0	csrss.exe	4388	192.168.2.2	836	560	0	0	3	0	0	2016-06-24 09:36:08 UTC+0000
0x828a2b88	TPAutoConnect.e	4388	192.168.2.2	2940	1384	1	78	0	0	0	2016-06-24 10:07:18 UTC+0000
0x824d2020	wuauclt.exe	4388	192.168.2.2	2012	1192	3	111	0	0	0	2016-06-24 10:07:34 UTC+0000
0x828bc628	game.exe	4388	192.168.2.2	1044	1716	0	0	0	0	0	2016-06-24 10:20:25 UTC+0000
0x829d18c8	cmd.exe	4388	192.168.2.2	2632	1716	1	40	0	0	0	2016-06-24 10:26:05 UTC+0000
0x82a75020	sc.exe	4388	192.168.2.2	3120	2632	1	33	0	0	0	2016-06-24 10:27:32 UTC+0000
0x82828620	cmd.exe	4388	192.168.2.2	3508	1716	1	42	0	0	0	2016-06-24 10:27:51 UTC+0000
0x82adc020	sc.exe	4388	192.168.2.2	3316	3508	1	35	0	0	0	2016-06-24 10:28:22 UTC+0000
0x8250d8a8	netstat.exe	4388	192.168.2.2	3868	1716	0	0	0	0	0	2016-06-24 10:28:39 UTC+0000
0x8250c020	netstat.exe	4388	192.168.2.2	2956	1716	0	0	0	0	0	2016-06-24 10:28:41 UTC+0000
0x82a3b900	cmd.exe	4388	192.168.2.2	3988	1716	0	0	0	0	0	2016-06-24 10:28:42 UTC+0000
0x82a3b020	net1.exe	4388	192.168.2.2	3292	3900	0	0	0	0	0	2016-06-24 10:28:44 UTC+0000
0x824d39f8	net1.exe	4388	192.168.2.2	1412	1240	0	0	0	0	0	2016-06-24 10:28:45 UTC+0000
0x828a2020	net1.exe	4388	192.168.2.2	620	2256	0	0	0	0	0	2016-06-24 10:28:47 UTC+0000
0x829d06c8	net.exe	4388	192.168.2.2	1284	1716	0	0	0	0	0	2016-06-24 10:28:48 UTC+0000
0x82a3c3c0	net1.exe	4388	192.168.2.2	3776	3964	0	0	0	0	0	2016-06-24 10:28:50 UTC+0000
0x824b67b8	net1.exe	4388	192.168.2.2	948	3888	0	0	0	0	0	2016-06-24 10:28:51 UTC+0000
0x82a736d8	systeminfo.exe	4388	192.168.2.2	4008	1716	0	0	0	0	0	2016-06-24 10:28:52 UTC+0000
0x82a153a0	reg.exe	4388	192.168.2.2	1712	1716	0	0	0	0	0	2016-06-24 10:29:00 UTC+0000
0x824a4888	reg.exe	4388	192.168.2.2	3232	1716	0	0	0	0	0	2016-06-24 10:29:05 UTC+0000
0x828d7af0	cmd.exe	4388	192.168.2.2	3068	1716	1	65	0	0	0	2016-06-24 10:30:19 UTC+0000

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

Teniendo en cuenta la cronología de los hechos, a las 10:07 se termino finalizo una tarea importante que no debe finalizarse el csrss, a partir de allí se procedió a realizar varios movimientos, entre estos la ejecución de game.exe considerado malicioso. Se abrió un cmd, se hizo consultas, se escaneo la red, se ejecuto el archivo net1.exe varias veces por cortos periodos de tiempo y se consultó información de sistema.

Lo que se considera pudo haber pasado a este equipo fue que a través del ejecutable se robo información del ordenador y se pudo acceder a directorios con privilegios, ya que este proceso como se mostro mas arriba posee privilegios para realizar muchas acciones, abajo se detallan, como ser realizar backups de files y direcotorios, debug programs, apagar el sistema, entre otros.

```

(root@kali)-[/home/veronica/Documents/blue_team/volatility_2.6_lin64_standalone]
# ./volatility_2.6_lin64_standalone --pid=1044 privs -f memoria.vmem
Volatility Foundation Volatility Framework 2.6

```

Pid	Process	Value	Privilege	Attributes	Description
1044	game.exe	23	SeChangeNotifyPrivilege	Present,Enabled,Default	Receive notifications of changes to files or directories
1044	game.exe	8	SeSecurityPrivilege	Present	Manage auditing and security log
1044	game.exe	17	SeBackupPrivilege	Present	Backup files and directories
1044	game.exe	18	SeRestorePrivilege	Present	Restore files and directories
1044	game.exe	12	SeSystemtimePrivilege	Present	Change the system time
1044	game.exe	19	SeShutdownPrivilege	Present	Shut down the system
1044	game.exe	24	SeRemoteShutdownPrivilege	Present	Force shutdown from a remote system
1044	game.exe	9	SeTakeOwnershipPrivilege	Present	Take ownership of files/objects
1044	game.exe	20	SeDebugPrivilege	Present,Enabled	Debug programs
1044	game.exe	22	SeSystemEnvironmentPrivilege	Present	Edit firmware environment values
1044	game.exe	11	SeSystemProfilePrivilege	Present	Profile system performance
1044	game.exe	13	SeProfileSingleProcessPrivilege	Present	Profile a single process
1044	game.exe	14	SeIncreaseBasePriorityPrivilege	Present	Increase scheduling priority
1044	game.exe	10	SeLoadDriverPrivilege	Present,Enabled	Load and unload device drivers
1044	game.exe	15	SeCreatePagefilePrivilege	Present	Create a pagefile
1044	game.exe	5	SeIncreaseQuotaPrivilege	Present	Increase quotas
1044	game.exe	25	SeUndockPrivilege	Present,Enabled	Remove computer from docking station
1044	game.exe	28	SeManageVolumePrivilege	Present	Manage the files on a volume
1044	game.exe	29	SeImpersonatePrivilege	Present,Enabled,Default	Impersonate a client after authentication
1044	game.exe	30	SeCreateGlobalPrivilege	Present,Enabled,Default	Create global objects