Informe de Análisis Forense con Volatility 3

Asunto: OSINT – Inteligencia de Fuentes Abiertas: Análisis Forense con Volatility 3
Autor: Giampiero Castillo
Fecha: Septiembre 2025

1. Objetivo del Análisis

El propósito de este análisis forense es investigar posibles actividades maliciosas o sospechosas dentro de la imagen de memoria capturada (*Challenge.raw*).
Mediante el uso de Volatility 3, se examinaron procesos, actividad de red y archivos ejecutables con el fin de detectar signos de compromiso o de actividad no autorizada.

2. Resumen de Hallazgos

2.1 DumpIt.exe (PID 4084)

- **Ruta:** C:\Users\Jaffa\Desktop\DumpIt.exe
- **Motivo de sospecha:**
    - Herramienta de adquisición de memoria.
    - Su ejecución solo se justifica en un análisis forense controlado.
    - Indica que alguien con conocimientos avanzados intentaba recolectar datos de la memoria.

2.2 WinRAR.exe (PID 3716)

- **Ruta:** C:\Users\Jaffa\Desktop\pr0t3ct3d\flag.rar
- **Motivo de sospecha:**
    - Archivo llamado *flag.rar*, común en retos CTF o entornos de pruebas de hacking.
    - El uso de WinRAR sugiere intento de compresión y posible exfiltración.

2.3 GoogleCrashHandler.exe (PIDs: 1292, 924, 1192, 864)

- **Rutas:**
    - "C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler.exe"
    - "C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler64.exe"
- **Motivo de sospecha:**
    - Ejecución de múltiples instancias simultáneas.
    - Aunque son procesos legítimos, pueden usarse como camuflaje de malware.
    - Necesario verificar integridad mediante *hashes*.

---

3. Pasos y Detalles del Análisis

3.1 Información de la Imagen

Comando utilizado:
vol -f '/home/csi/Downloads/Challenge.raw' windows.info

- **Hallazgos clave:**
    - Sistema: Windows 7 SP1 (Build 7601.17514.amd64fre).
    - Fecha/hora: 19/08/2019 – 14:41:58 UTC.
    - Arquitectura: 64 bits.
    - Dirección base del kernel: 0xf80002609000.
    - Equivalente Volatility 2: imageinfo.

03:28:44 csi@csi ~/Downloads

❯ vol -f '/home/csi/Downloads/Challenge.raw' windows.info
Volatility 3 Framework 2.26.0
Progress: 100.00 PDB scanning finished
Variable Value

Kernel Base 0xf80002609000
DTB 0x187000

Symbols file:///home/csi/.local/lib/python3.10/site-packages/volatility3/symbols/windows/ntkrnlmp.pdb/3844DBB920174967BE7AA4A2C20430FA-2.json.xz
Is64Bit True
IsPAE False
layer_name 0 WindowsIntel32e
memory_layer 1 FileLayer
KdDebuggerDataBlock 0xf800027fa0a0
NTBuildLab 7601.17514.amd64fre.win7sp1_rtm.
CSDVersion 1
KdVersionBlock 0xf800027fa068
Major/Minor 15.7601
MachineType 34404
KeNumberProcessors 1
SystemTime 2019-08-19 14:41:58+00:00
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 6
NtMinorVersion 1
PE MajorOperatingSystemVersion 6
PE MinorOperatingSystemVersion 1
PE Machine 34404
PE TimeDateStamp Sat Nov 20 09:30:02 2010

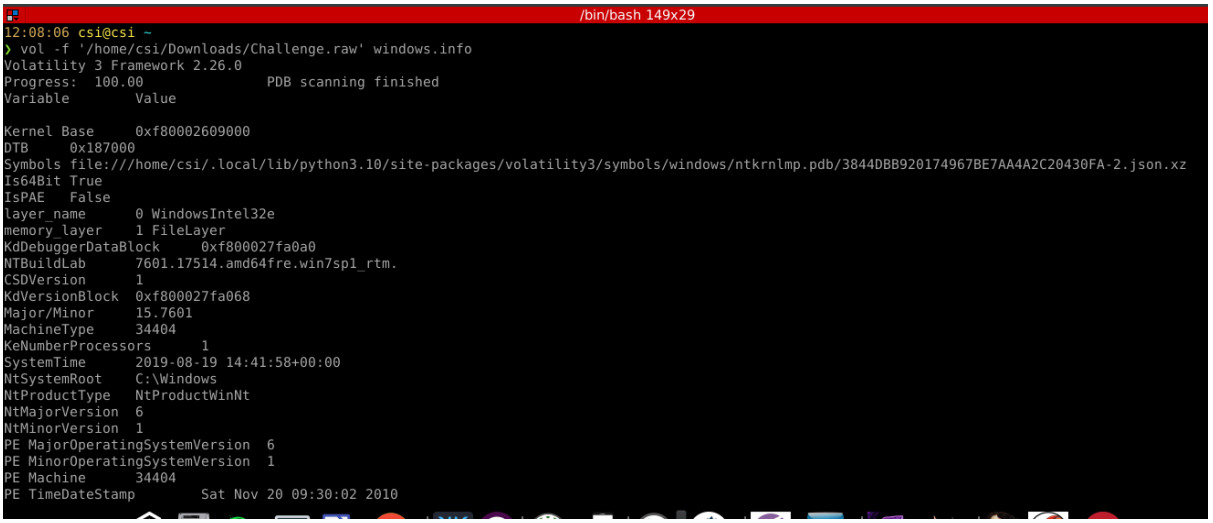

Imagen 1

3.2 Listado de Procesos

Comando utilizado:
vol -f '/home/csi/Downloads/Challenge.raw' windows.pslist

- **Hallazgos clave:**
    - DumpIt.exe (PID 4084) → indica volcado de memoria.
    - WinRAR.exe (PID 3716) → vinculado a *flag.rar*.
    - GoogleCrashHandler.exe → múltiples instancias.
    - Equivalente Volatility 2: pslist.

```
04:01:38 csi@csi ~/Downloads
❯ vol -f '/home/csi/Downloads/Challenge.raw' windows.pslist
Volatility 3 Framework 2.26.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads         Handles         SessionId
        Wow64           CreateTime      ExitTime        File output

4       0       System          0xfa80012a5040  78      495     N/A     False
2019-08-19 14:40:07.000000 UTC  N/A     Disabled
264     4       smss.exe        0xfa8002971470  2       29      N/A     False
2019-08-19 14:40:07.000000 UTC  N/A     Disabled
336     328     csrss.exe       0xfa800234cb30  10      415     0       False
2019-08-19 14:40:10.000000 UTC  N/A     Disabled
384     328     wininit.exe     0xfa8002aae910  3       74      0       False
2019-08-19 14:40:11.000000 UTC  N/A     Disabled
396     376     csrss.exe       0xfa8002ab7060  9       499     1       False
2019-08-19 14:40:11.000000 UTC  N/A     Disabled
436     376     winlogon.exe    0xfa8002b66560  6       116     1       False
2019-08-19 14:40:11.000000 UTC  N/A     Disabled
480     384     services.exe    0xfa8002b99200  9       194     0       False
2019-08-19 14:40:11.000000 UTC  N/A     Disabled
496     384     lsass.exe       0xfa8002bb4600  7       513     0       False
2019-08-19 14:40:11.000000 UTC  N/A     Disabled
504     384     lsm.exe         0xfa80022ff910  10      152     0       False
2019-08-19 14:40:11.000000 UTC  N/A     Disabled
608     480     svchost.exe     0xfa8002ce8740  10      358     0       False
2019-08-19 14:40:11.000000 UTC  N/A     Disabled
668     480     VBoxService.ex  0xfa8002d13060  13      136     0       False
2019-08-19 14:40:11.000000 UTC  N/A     Disabled
724     480     svchost.exe     0xfa8002d4bb30  6       257     0       False
2019-08-19 14:40:11.000000 UTC  N/A     Disabled
780     480     svchost.exe     0xfa8002d4fb30  19      405     0       False
2019-08-19 14:40:11.000000 UTC  N/A     Disabled
896     480     svchost.exe     0xfa8002dcf5f0  22      452     0       False
2019-08-19 14:40:12.000000 UTC  N/A     Disabled
948     480     svchost.exe     0xfa8002de1b30  35      893     0       False
2019-08-19 14:40:12.000000 UTC  N/A     Disabled
```

1008 780 audiodg.exe 0xfa8002e0b1c0 7 132 0 False
2019-08-19 14:40:12.000000 UTC N/A Disabled
400 480 svchost.exe 0xfa8002e645f0 13 275 0 False
2019-08-19 14:40:12.000000 UTC N/A Disabled
1052 480 svchost.exe 0xfa8002eac740 17 368 0 False
2019-08-19 14:40:12.000000 UTC N/A Disabled
1176 480 spoolsv.exe 0xfa8002e76b30 14 279 0 False
2019-08-19 14:40:13.000000 UTC N/A Disabled
1212 480 svchost.exe 0xfa8002f4d780 21 311 0 False
2019-08-19 14:40:13.000000 UTC N/A Disabled
1308 480 svchost.exe 0xfa8002f79b30 17 253 0 False
2019-08-19 14:40:13.000000 UTC N/A Disabled
1812 480 taskhost.exe 0xfa8003144250 9 147 1 False
2019-08-19 14:40:18.000000 UTC N/A Disabled
1868 896 dwm.exe 0xfa8003160120 4 70 1 False
2019-08-19 14:40:18.000000 UTC N/A Disabled
1876 948 taskeng.exe 0xfa8003164b30 5 81 0 False
2019-08-19 14:40:18.000000 UTC N/A Disabled
1944 1844 explorer.exe 0xfa800319a060 35 894 1 False
2019-08-19 14:40:19.000000 UTC N/A Disabled
1292 1928 GoogleCrashHan 0xfa8003227060 7 105 0 True
2019-08-19 14:40:19.000000 UTC N/A Disabled
924 1928 GoogleCrashHan 0xfa8003219060 6 93 0 False
2019-08-19 14:40:19.000000 UTC N/A Disabled
1108 1944 VBoxTray.exe 0xfa8003277810 14 139 1 False
2019-08-19 14:40:20.000000 UTC N/A Disabled
880 1944 cmd.exe 0xfa8002324b30 1 21 1 False
2019-08-19 14:40:26.000000 UTC N/A Disabled
916 396 conhost.exe 0xfa800231e370 3 50 1 False
2019-08-19 14:40:26.000000 UTC N/A Disabled
856 480 SearchIndexer. 0xfa8003315060 13 689 0 False
2019-08-19 14:40:27.000000 UTC N/A Disabled
2124 1944 chrome.exe 0xfa800234eb30 27 662 1 False
2019-08-19 14:40:46.000000 UTC N/A Disabled
2132 2124 chrome.exe 0xfa800234f780 9 75 1 False
2019-08-19 14:40:46.000000 UTC N/A Disabled
2168 2124 chrome.exe 0xfa800314fab0 3 55 1 False
2019-08-19 14:40:49.000000 UTC N/A Disabled
2292 608 WmiPrvSE.exe 0xfa80032d9060 13 288 0 False
2019-08-19 14:40:52.000000 UTC N/A Disabled
2340 2124 chrome.exe 0xfa80032f9a70 12 282 1 False
2019-08-19 14:40:52.000000 UTC N/A Disabled
2440 2124 chrome.exe 0xfa8003741b30 13 263 1 False
2019-08-19 14:40:54.000000 UTC N/A Disabled
2452 2124 chrome.exe 0xfa800374bb30 14 167 1 False
2019-08-19 14:40:54.000000 UTC N/A Disabled
2800 480 WmiApSrv.exe0xfa8002b74060 6 115 0 False
2019-08-19 14:40:57.000000 UTC N/A Disabled

2896 608 WmiPrvSE.exe 0xfa8002d9eab0 7 124 0 False
2019-08-19 14:40:57.000000 UTC N/A Disabled
2940 2124 chrome.exe 0xfa80032d4380 9 172 1 False
2019-08-19 14:41:06.000000 UTC N/A Disabled
2080 3060 firefox.exe 0xfa8003905b30 59 970 1 True
2019-08-19 14:41:08.000000 UTC N/A Disabled
2860 2080 firefox.exe 0xfa80021fa630 11 210 1 True
2019-08-19 14:41:09.000000 UTC N/A Disabled
3016 2080 firefox.exe 0xfa80013a4580 31 413 1 True
2019-08-19 14:41:10.000000 UTC N/A Disabled
2968 2080 firefox.exe 0xfa8001415b30 22 323 1 True
2019-08-19 14:41:11.000000 UTC N/A Disabled
3316 2080 firefox.exe 0xfa8001454b30 21 307 1 True
2019-08-19 14:41:13.000000 UTC N/A Disabled
3716 1944 WinRAR.exe 0xfa80035e71e0 7 201 1 False
2019-08-19 14:41:43.000000 UTC N/A Disabled
4084 1944 DumpIt.exe 0xfa800156e400 5 46 1 True
2019-08-19 14:41:55.000000 UTC N/A Disabled
4092 396 conhost.exe 0xfa80014c1060 2 50 1 False
2019-08-19 14:41:55.000000 UTC N/A Disabled
1224 480 sppsvc.exe 0xfa80014aa060 5 0 0 False
2019-08-19 14:42:39.000000 UTC N/A Disabled
2256 2396 GoogleUpdate.e 0xfa800157eb30 3 118 0 True
2019-08-19 14:42:40.000000 UTC N/A Disabled
1192 2256 GoogleCrashHan 0xfa80014f9060 3 46 0 True
2019-08-19 14:42:41.000000 UTC N/A Disabled
864 2256 GoogleCrashHan 0xfa80035e3700 1 1279459345 0
False 2019-08-19 14:42:41.000000 UTC N/A Disabled

```
12:15:47 csi@csi ~
❯ vol -f '/home/csi/Downloads/Challenge.raw' windows.pslist
Volatility 3 Framework 2.26.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xfa80012a5040  78      495     N/A     False   2019-08-19 14:40:07.000000 UTC  N/A     Disabled
264     4       smss.exe        0xfa8002971470  2       29      N/A     False   2019-08-19 14:40:07.000000 UTC  N/A     Disabled
336     328     csrss.exe       0xfa800234cb30  10      415     0       False   2019-08-19 14:40:10.000000 UTC  N/A     Disabled
384     328     wininit.exe     0xfa8002aae910  3       74      0       False   2019-08-19 14:40:11.000000 UTC  N/A     Disabled
396     376     csrss.exe       0xfa8002ab7060  9       499     1       False   2019-08-19 14:40:11.000000 UTC  N/A     Disabled
436     376     winlogon.exe    0xfa8002b66560  6       116     1       False   2019-08-19 14:40:11.000000 UTC  N/A     Disabled
480     384     services.exe    0xfa8002b99200  9       194     0       False   2019-08-19 14:40:11.000000 UTC  N/A     Disabled
496     384     lsass.exe       0xfa8002bb4600  7       513     0       False   2019-08-19 14:40:11.000000 UTC  N/A     Disabled
504     384     lsm.exe 0xfa80022ff910  10      152     0       False   2019-08-19 14:40:11.000000 UTC  N/A     Disabled
608     480     svchost.exe     0xfa8002ce8740  10      358     0       False   2019-08-19 14:40:11.000000 UTC  N/A     Disabled
668     480     VBoxService.ex  0xfa8002d13060  13      136     0       False   2019-08-19 14:40:11.000000 UTC  N/A     Disabled
724     480     svchost.exe     0xfa8002d4bb30  6       257     0       False   2019-08-19 14:40:11.000000 UTC  N/A     Disabled
780     480     svchost.exe     0xfa8002d4fb30  19      405     0       False   2019-08-19 14:40:11.000000 UTC  N/A     Disabled
896     480     svchost.exe     0xfa8002dcf5f0  22      452     0       False   2019-08-19 14:40:12.000000 UTC  N/A     Disabled
948     480     svchost.exe     0xfa8002de1b30  35      893     0       False   2019-08-19 14:40:12.000000 UTC  N/A     Disabled
1008    780     audiodg.exe     0xfa8002e0b1c0  7       132     0       False   2019-08-19 14:40:12.000000 UTC  N/A     Disabled
400     480     svchost.exe     0xfa8002e645f0  13      275     0       False   2019-08-19 14:40:12.000000 UTC  N/A     Disabled
1052    480     svchost.exe     0xfa8002eac740  17      368     0       False   2019-08-19 14:40:12.000000 UTC  N/A     Disabled
1176    480     spoolsv.exe     0xfa8002e76b30  14      279     0       False   2019-08-19 14:40:13.000000 UTC  N/A     Disabled
1212    480     svchost.exe     0xfa8002f4d780  21      311     0       False   2019-08-19 14:40:13.000000 UTC  N/A     Disabled
1308    480     svchost.exe     0xfa8002f79b30  17      253     0       False   2019-08-19 14:40:13.000000 UTC  N/A     Disabled
1812    480     taskhost.exe    0xfa8003144250  9       147     1       False   2019-08-19 14:40:18.000000 UTC  N/A     Disabled
```

Imagen 2

```
1868    896     dwm.exe 0xfa8003160120  4       70      1       False   2019-08-19 14:40:18.000000 UTC  N/A     Disabled
1876    948     taskeng.exe     0xfa8003164b30  5       81      0       False   2019-08-19 14:40:18.000000 UTC  N/A     Disabled
1944    1844    explorer.exe    0xfa800319a060  35      894     1       False   2019-08-19 14:40:19.000000 UTC  N/A     Disabled
1292    1928    GoogleCrashHan  0xfa8003227060  7       105     0       True    2019-08-19 14:40:19.000000 UTC  N/A     Disabled
924     1928    GoogleCrashHan  0xfa8003219060  6       93      0       False   2019-08-19 14:40:19.000000 UTC  N/A     Disabled
1108    1944    VBoxTray.exe    0xfa8003277810  14      139     1       False   2019-08-19 14:40:20.000000 UTC  N/A     Disabled
880     1944    cmd.exe 0xfa8002324b30  1       21      1       False   2019-08-19 14:40:26.000000 UTC  N/A     Disabled
916     396     conhost.exe     0xfa800231e370  3       50      1       False   2019-08-19 14:40:26.000000 UTC  N/A     Disabled
856     480     SearchIndexer.  0xfa8003315060  13      689     0       False   2019-08-19 14:40:27.000000 UTC  N/A     Disabled
2124    1944    chrome.exe      0xfa800234eb30  27      662     1       False   2019-08-19 14:40:46.000000 UTC  N/A     Disabled
2132    2124    chrome.exe      0xfa800234f780  9       75      1       False   2019-08-19 14:40:46.000000 UTC  N/A     Disabled
2168    2124    chrome.exe      0xfa800314fab0  3       55      1       False   2019-08-19 14:40:49.000000 UTC  N/A     Disabled
2292    608     WmiPrvSE.exe    0xfa80032d9060  13      288     0       False   2019-08-19 14:40:52.000000 UTC  N/A     Disabled
2340    2124    chrome.exe      0xfa80032f9a70  12      282     1       False   2019-08-19 14:40:52.000000 UTC  N/A     Disabled
2440    2124    chrome.exe      0xfa8003741b30  13      263     1       False   2019-08-19 14:40:54.000000 UTC  N/A     Disabled
2452    2124    chrome.exe      0xfa800374bb30  14      167     1       False   2019-08-19 14:40:54.000000 UTC  N/A     Disabled
2800    480     WmiApSrv.exe    0xfa8002b74060  6       115     0       False   2019-08-19 14:40:57.000000 UTC  N/A     Disabled
2896    608     WmiPrvSE.exe    0xfa8002d9eab0  7       124     0       False   2019-08-19 14:40:57.000000 UTC  N/A     Disabled
2940    2124    chrome.exe      0xfa80032d4380  9       172     1       False   2019-08-19 14:41:06.000000 UTC  N/A     Disabled
2080    3060    firefox.exe     0xfa8003905b30  59      970     1       True    2019-08-19 14:41:08.000000 UTC  N/A     Disabled
2860    2080    firefox.exe     0xfa80021fa630  11      210     1       True    2019-08-19 14:41:09.000000 UTC  N/A     Disabled
3016    2080    firefox.exe     0xfa80013a4580  31      413     1       True    2019-08-19 14:41:10.000000 UTC  N/A     Disabled
2968    2080    firefox.exe     0xfa8001415b30  22      323     1       True    2019-08-19 14:41:11.000000 UTC  N/A     Disabled
3316    2080    firefox.exe     0xfa8001454b30  21      307     1       True    2019-08-19 14:41:13.000000 UTC  N/A     Disabled
3716    1944    WinRAR.exe      0xfa80035e71e0  7       201     1       False   2019-08-19 14:41:43.000000 UTC  N/A     Disabled
4084    1944    DumpIt.exe      0xfa800156e400  5       46      1       True    2019-08-19 14:41:55.000000 UTC  N/A     Disabled
4092    396     conhost.exe     0xfa80014c1060  2       50      1       False   2019-08-19 14:41:55.000000 UTC  N/A     Disabled
```

Imagen 3

```
916     396     conhost.exe     0xfa800231e370  3       50      1       False   2019-08-19 14:40:26.000000 UTC  N/A     Disabled
856     480     SearchIndexer.  0xfa8003315060  13      689     0       False   2019-08-19 14:40:27.000000 UTC  N/A     Disabled
2124    1944    chrome.exe      0xfa800234eb30  27      662     1       False   2019-08-19 14:40:46.000000 UTC  N/A     Disabled
2132    2124    chrome.exe      0xfa800234f780  9       75      1       False   2019-08-19 14:40:46.000000 UTC  N/A     Disabled
2168    2124    chrome.exe      0xfa800314fab0  3       55      1       False   2019-08-19 14:40:49.000000 UTC  N/A     Disabled
2292    608     WmiPrvSE.exe    0xfa80032d9060  13      288     0       False   2019-08-19 14:40:52.000000 UTC  N/A     Disabled
2340    2124    chrome.exe      0xfa80032f9a70  12      282     1       False   2019-08-19 14:40:52.000000 UTC  N/A     Disabled
2440    2124    chrome.exe      0xfa8003741b30  13      263     1       False   2019-08-19 14:40:54.000000 UTC  N/A     Disabled
2452    2124    chrome.exe      0xfa800374bb30  14      167     1       False   2019-08-19 14:40:54.000000 UTC  N/A     Disabled
2800    480     WmiApSrv.exe    0xfa8002b74060  6       115     0       False   2019-08-19 14:40:57.000000 UTC  N/A     Disabled
2896    608     WmiPrvSE.exe    0xfa8002d9eab0  7       124     0       False   2019-08-19 14:40:57.000000 UTC  N/A     Disabled
2940    2124    chrome.exe      0xfa80032d4380  9       172     1       False   2019-08-19 14:41:06.000000 UTC  N/A     Disabled
2080    3060    firefox.exe     0xfa8003905b30  59      970     1       True    2019-08-19 14:41:08.000000 UTC  N/A     Disabled
2860    2080    firefox.exe     0xfa80021fa630  11      210     1       True    2019-08-19 14:41:09.000000 UTC  N/A     Disabled
3016    2080    firefox.exe     0xfa80013a4580  31      413     1       True    2019-08-19 14:41:10.000000 UTC  N/A     Disabled
2968    2080    firefox.exe     0xfa8001415b30  22      323     1       True    2019-08-19 14:41:11.000000 UTC  N/A     Disabled
3316    2080    firefox.exe     0xfa8001454b30  21      307     1       True    2019-08-19 14:41:13.000000 UTC  N/A     Disabled
3716    1944    WinRAR.exe      0xfa80035e71e0  7       201     1       False   2019-08-19 14:41:43.000000 UTC  N/A     Disabled
4084    1944    DumpIt.exe      0xfa800156e400  5       46      1       True    2019-08-19 14:41:55.000000 UTC  N/A     Disabled
4092    396     conhost.exe     0xfa80014c1060  2       50      1       False   2019-08-19 14:41:55.000000 UTC  N/A     Disabled
1224    480     sppsvc.exe      0xfa80014aa060  5       0       0       False   2019-08-19 14:42:39.000000 UTC  N/A     Disabled
2256    2396    GoogleUpdate.e  0xfa800157eb30  3       118     0       True    2019-08-19 14:42:40.000000 UTC  N/A     Disabled
1192    2256    GoogleCrashHan  0xfa80014f9060  3       46      0       True    2019-08-19 14:42:41.000000 UTC  N/A     Disabled
864     2256    GoogleCrashHan  0xfa80035e3700  1       1279459345      0       False   2019-08-19 14:42:41.000000 UTC  N/A     Disabled
```

Imagen 4

3.3 Actividad de Red

Comando utilizado:
vol -f '/home/csi/Downloads/Challenge.raw' windows.netscan

- **Hallazgos clave:**
    - DumpIt.exe → sin conexiones detectadas.
    - WinRAR.exe → sin conexiones detectadas.
    - Firefox.exe (PID 2080) → conexiones externas (ej. 172.217.163.100:443).

- Equivalente Volatility 2: connscan y sockets.

```
04:12:22 csi@csi ~/Downloads
❯ vol -f '/home/csi/Downloads/Challenge.raw' windows.netscan
Volatility 3 Framework 2.26.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID
Owner Created

0x53f2010       TCPv4   127.0.0.1       49171   127.0.0.1       49170   ESTABLISHED
2968    firefox.exe     N/A
0x53f2a90       TCPv4   127.0.0.1       49170   127.0.0.1       49171   ESTABLISHED
2968    firefox.exe     N/A
0x5d80d9f0      UDPv4   127.0.0.1       58500   *       0               1308    svchost.exe
2019-08-19 14:42:39.000000 UTC
0x5d8c3360      UDPv4   0.0.0.0 5353    *       0               2124    chrome.exe
2019-08-19 14:40:55.000000 UTC
0x5d8c3360      UDPv6   ::      5353    *       0               2124    chrome.exe
2019-08-19 14:40:55.000000 UTC
0x5d8c3ec0      UDPv4   0.0.0.0 5353    *       0               2124    chrome.exe
2019-08-19 14:40:55.000000 UTC
0x5d8d8500      TCPv4   10.0.2.15       49232   172.217.160.131         80      ESTABLISHED
        2080    firefox.exe     N/A
0x5d8e7b90      TCPv4   127.0.0.1       49166   127.0.0.1       49165   ESTABLISHED
2080    firefox.exe     N/A
0x5d8e9010      TCPv4   10.0.2.15       49235   172.217.194.189         443     ESTABLISHED
        2080    firefox.exe     N/A
0x5d9705f0      TCPv4   10.0.2.15       49196   172.217.160.133         443     ESTABLISHED
        2080    firefox.exe     N/A
0x5dadd860      TCPv4   10.0.2.15       49198   216.58.197.67   443     ESTABLISHED
2080    firefox.exe     N/A
0x5daeb850      TCPv4   127.0.0.1       49165   127.0.0.1       49166   ESTABLISHED
2080    firefox.exe     N/A
0x5dafccf0      TCPv4   10.0.2.15       49224   172.217.163.205         443     ESTABLISHED
        2080    firefox.exe     N/A
0x5dde8680      TCPv4   10.0.2.15       49234   172.217.163.106         443     ESTABLISHED
        2080    firefox.exe     N/A
0x5ddf9010      TCPv4   10.0.2.15       49202   216.58.196.163          443     ESTABLISHED
        2080    firefox.exe     N/A
0x5de48b50      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       496     lsass.exe       -
0x5e0663e0      TCPv4   0.0.0.0 5357    0.0.0.0 0       LISTENING       4       System  -
0x5e0663e0      TCPv6   ::      5357    ::      0       LISTENING       4       System  -
0x5e06b010      UDPv4   0.0.0.0 64930   *       0               1308    svchost.exe
2019-08-19 14:40:13.000000 UTC
0x5e06b620      UDPv4   0.0.0.0 64931   *       0               1308    svchost.exe
2019-08-19 14:40:13.000000 UTC
```

```
0x5e06b620  UDPv6  ::          64931  *           0                1308  svchost.exe
2019-08-19 14:40:13.000000 UTC
0x5e07c670  UDPv4  0.0.0.0     3702   *           0                1308  svchost.exe
2019-08-19 14:40:17.000000 UTC
0x5e07c670  UDPv6  ::          3702   *           0                1308  svchost.exe
2019-08-19 14:40:17.000000 UTC
0x5e08e2d0  TCPv4  0.0.0.0     445    0.0.0.0     0       LISTENING  4     System       -
0x5e08e2d0  TCPv6  ::          445    ::          0       LISTENING  4     System       -
0x5e0a85d0  TCPv4  0.0.0.0     49155  0.0.0.0     0       LISTENING  480   services.exe -
0x5e0a85d0  TCPv6  ::          49155  ::          0       LISTENING  480   services.exe -
0x5e0dbcb0  UDPv4  127.0.0.1   56645  *           0                1052  svchost.exe
2019-08-19 14:40:17.000000 UTC
0x5e109890  TCPv4  10.0.2.15   139    0.0.0.0     0       LISTENING  4     System
        -
0x5e10ab80  UDPv4  10.0.2.15   137    *           0                4     System
2019-08-19 14:40:17.000000 UTC
0x5e10baa0  UDPv4  10.0.2.15   138    *           0                4     System
2019-08-19 14:40:17.000000 UTC
0x5e114010  UDPv4  0.0.0.0     3702   *           0                1308  svchost.exe
2019-08-19 14:40:17.000000 UTC
0x5e12c5d0  UDPv4  0.0.0.0     0      *           0                1052  svchost.exe
2019-08-19 14:40:17.000000 UTC
0x5e12c5d0  UDPv6  ::          0      *           0                1052  svchost.exe
2019-08-19 14:40:17.000000 UTC
0x5e135c40  UDPv4  0.0.0.0     3702   *           0                1308  svchost.exe
2019-08-19 14:40:17.000000 UTC
0x5e135c40  UDPv6  ::          3702   *           0                1308  svchost.exe
2019-08-19 14:40:17.000000 UTC
0x5e135dc0  UDPv4  0.0.0.0     3702   *           0                1308  svchost.exe
2019-08-19 14:40:17.000000 UTC
0x5e1379c0  UDPv4  0.0.0.0     5355   *           0                1052  svchost.exe
2019-08-19 14:40:20.000000 UTC
0x5e1379c0  UDPv6  ::          5355   *           0                1052  svchost.exe
2019-08-19 14:40:20.000000 UTC
0x5e2be2e0  UDPv4  0.0.0.0     5355   *           0                1052  svchost.exe
2019-08-19 14:40:20.000000 UTC
0x5e2beb30  TCPv4  0.0.0.0     49154  0.0.0.0     0       LISTENING  948   svchost.exe  -
0x5e2fc550  TCPv4  10.0.2.15   49231  172.217.160.131     80        ESTABLISHED
        2080  firefox.exe  N/A
0x5e3037b0  TCPv4  0.0.0.0     49154  0.0.0.0     0       LISTENING  948   svchost.exe  -
0x5e3037b0  TCPv6  ::          49154  ::          0       LISTENING  948   svchost.exe  -
0x5e31f900  TCPv4  0.0.0.0     49155  0.0.0.0     0       LISTENING  480   services.exe -
0x5e51fd20  TCPv4  0.0.0.0     49152  0.0.0.0     0       LISTENING  384   wininit.exe  -
0x5e559ef0  TCPv4  0.0.0.0     135    0.0.0.0     0       LISTENING  724   svchost.exe  -
0x5e55cef0  TCPv4  0.0.0.0     135    0.0.0.0     0       LISTENING  724   svchost.exe  -
0x5e55cef0  TCPv6  ::          135    ::          0       LISTENING  724   svchost.exe  -
0x5e56a3c0  TCPv4  0.0.0.0     49152  0.0.0.0     0       LISTENING  384   wininit.exe  -
0x5e56a3c0  TCPv6  ::          49152  ::          0       LISTENING  384   wininit.exe  -
```

```
0x5e5add20    TCPv4 0.0.0.0 49156 0.0.0.0 0       LISTENING   496   lsass.exe       -
0x5e5add20    TCPv6 ::      49156 ::      0       LISTENING   496   lsass.exe       -
0x5e5d2e30    TCPv4 0.0.0.0 49153 0.0.0.0 0       LISTENING   780   svchost.exe     -
0x5e5d3950    TCPv4 0.0.0.0 49153 0.0.0.0 0       LISTENING   780   svchost.exe     -
0x5e5d3950    TCPv6 ::      49153 ::      0       LISTENING   780   svchost.exe     -
0x5ee7fcf0    TCPv4 10.0.2.15     49240 172.217.167.138     443     ESTABLISHED
        2080    firefox.exe     N/A
0x5fc0dcf0    TCPv4 10.0.2.15     49172 54.149.112.164      443     ESTABLISHED
        2080    firefox.exe     N/A
0x5fc13010    TCPv4 10.0.2.15     49182 117.18.237.29 80      ESTABLISHED
2080    firefox.exe     N/A
0x5fc13cf0    TCPv4 10.0.2.15     49241 52.24.89.101  443     ESTABLISHED
2080    firefox.exe     N/A
0x5fc24010    TCPv4 10.0.2.15     49200 172.217.163.33      443     ESTABLISHED
        2080    firefox.exe     N/A
0x5fc2e300    TCPv4 127.0.0.1     49167 127.0.0.1     49168 ESTABLISHED
3016    firefox.exe     N/A
0x5fc303d0    TCPv4 127.0.0.1     49168 127.0.0.1     49167 ESTABLISHED
3016    firefox.exe     N/A
0x5fc3a010    TCPv4 10.0.2.15     49169 23.195.74.19  80      ESTABLISHED
2080    firefox.exe     N/A
0x5fc43640    TCPv6 -         0     381b:de02:80fa:ffff:381b:de02:80fa:ffff     0
CLOSED      2080    firefox.exe     N/A
0x5fc49700    TCPv4 -         0     56.27.222.2 0       CLOSED      2080    firefox.exe
        N/A
0x5fc4e810    TCPv4 10.0.2.15     49178 117.18.237.29 80      ESTABLISHED
2080    firefox.exe     N/A
0x5fc52940    TCPv4 10.0.2.15     49179 117.18.237.29 80      ESTABLISHED
2080    firefox.exe     N/A
0x5fc81810    TCPv4 127.0.0.1     49186 127.0.0.1     49185 ESTABLISHED
3316    firefox.exe     N/A
0x5fc869e0    TCPv4 127.0.0.1     49185 127.0.0.1     49186 ESTABLISHED
3316    firefox.exe     N/A
0x5fc94770    TCPv4 10.0.2.15     49195 172.217.160.131     80      ESTABLISHED
        2080    firefox.exe     N/A
0x5fc989d0    TCPv4 10.0.2.15     49193 172.217.160.131     80      ESTABLISHED
        2080    firefox.exe     N/A
0x5fca7cf0    TCPv4 10.0.2.15     49191 172.217.163.100     443     ESTABLISHED
        2080    firefox.exe     N/A
0x5fcbe5b0    TCPv4 10.0.2.15     49214 172.217.160.131     80      FIN_WAIT2
2080    firefox.exe     N/A
0x5fcbeb30    TCPv4 10.0.2.15     49228 172.217.163.106     443     ESTABLISHED
        2080    firefox.exe     N/A
0x5fccd010    TCPv4 10.0.2.15     49203 172.217.160.131     80      ESTABLISHED
        2080    firefox.exe     N/A
0x5fccd5e0    TCPv4 10.0.2.15     49225 172.217.163.110     443     ESTABLISHED
        2080    firefox.exe     N/A
```

0x5fcceb30 TCPv4 10.0.2.15 49239 172.217.167.138 443 ESTABLISHED 2080 firefox.exe N/A
0x5fcdb460 TCPv4 10.0.2.15 49216 172.217.167.142 443 ESTABLISHED 2080 firefox.exe N/A
0x5fcebcf0 TCPv4 10.0.2.15 49218 216.58.200.142 443 ESTABLISHED 2080 firefox.exe N/A
0x5fcf5cf0 TCPv4 10.0.2.15 49217 216.58.200.142 443 ESTABLISHED 2080 firefox.exe N/A
0x5fcf6010 UDPv6 fe80::6dfd:18d9:71ed:3522 1900 * 0 1308 svchost.exe 2019-08-19 14:42:39.000000 UTC
0x5fcf8010 TCPv4 10.0.2.15 49226 172.217.163.170 443 ESTABLISHED 2080 firefox.exe N/A
0x5fcfe010 TCPv4 10.0.2.15 49209 172.217.163.67 443 ESTABLISHED 2080 firefox.exe N/A
0x5fd03010 TCPv4 10.0.2.15 49219 172.217.163.110 443 ESTABLISHED 2080 firefox.exe N/A
0x5fd039d0 TCPv4 10.0.2.15 49213 172.217.160.131 80 FIN_WAIT2 2080 firefox.exe N/A
0x5fd03cf0 TCPv4 10.0.2.15 49227 172.217.163.170 443 ESTABLISHED 2080 firefox.exe N/A
0x5fd058d0 TCPv4 10.0.2.15 49222 172.217.31.206 443 ESTABLISHED 2080 firefox.exe N/A
0x5fd0eec0 UDPv4 0.0.0.0 0 * 0 668 VBoxService.ex 2019-08-19 14:42:51.000000 UTC
0x5fd6a010 UDPv4 0.0.0.0 0 * 0 668 VBoxService.ex 2019-08-19 14:42:43.000000 UTC
0x5fe17550 UDPv4 127.0.0.1 1900 * 0 1308 svchost.exe 2019-08-19 14:42:39.000000 UTC
0x5fe18270 UDPv4 10.0.2.15 1900 * 0 1308 svchost.exe 2019-08-19 14:42:39.000000 UTC
0x5fe4f490 UDPv6 ::1 58499 * 0 1308 svchost.exe 2019-08-19 14:42:39.000000 UTC
0x5fe4fcf0 TCPv4 10.0.2.15 49177 13.224.25.60 443 ESTABLISHED 2080 firefox.exe N/A
0x5fe61010 TCPv4 10.0.2.15 49174 35.167.81.14 443 CLOSED 2080 firefox.exe -
0x5fe67cf0 TCPv4 10.0.2.15 49181 117.18.237.29 80 ESTABLISHED 2080 firefox.exe N/A
0x5ff6b6d0 UDPv6 ::1 1900 * 0 1308 svchost.exe 2019-08-19 14:42:39.000000 UTC

```
/bin/bash 149x29
12:31:48 csi@csi ~
❯ vol -f '/home/csi/Downloads/Challenge.raw' windows.netscan
Volatility 3 Framework 2.26.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0x53f2010       TCPv4   127.0.0.1       49171   127.0.0.1       49170   ESTABLISHED     2968    firefox.exe     N/A
0x53f2a90       TCPv4   127.0.0.1       49170   127.0.0.1       49171   ESTABLISHED     2968    firefox.exe     N/A
0x5d80d9f0      UDPv4   127.0.0.1       58500   *       0               1308    svchost.exe     2019-08-19 14:42:39.000000 UTC
0x5d8c3360      UDPv4   0.0.0.0 5353    *       0               2124    chrome.exe      2019-08-19 14:40:55.000000 UTC
0x5d8c3360      UDPv6   ::      5353    *       0               2124    chrome.exe      2019-08-19 14:40:55.000000 UTC
0x5d8c3ec0      UDPv4   0.0.0.0 5353    *       0               2124    chrome.exe      2019-08-19 14:40:55.000000 UTC
0x5d8d8500      TCPv4   10.0.2.15       49232   172.217.160.131 80      ESTABLISHED     2080    firefox.exe     N/A
0x5d8e7b90      TCPv4   127.0.0.1       49166   127.0.0.1       49165   ESTABLISHED     2080    firefox.exe     N/A
0x5d8e9010      TCPv4   10.0.2.15       49235   172.217.194.189 443     ESTABLISHED     2080    firefox.exe     N/A
0x5d9705f0      TCPv4   10.0.2.15       49196   172.217.160.133 443     ESTABLISHED     2080    firefox.exe     N/A
0x5dadd860      TCPv4   10.0.2.15       49198   216.58.197.67   443     ESTABLISHED     2080    firefox.exe     N/A
0x5daeb850      TCPv4   127.0.0.1       49165   127.0.0.1       49166   ESTABLISHED     2080    firefox.exe     N/A
0x5dafccf0      TCPv4   10.0.2.15       49224   172.217.163.205 443     ESTABLISHED     2080    firefox.exe     N/A
0x5dde8680      TCPv4   10.0.2.15       49234   172.217.163.106 443     ESTABLISHED     2080    firefox.exe     N/A
0x5ddf9010      TCPv4   10.0.2.15       49202   216.58.196.163  443     ESTABLISHED     2080    firefox.exe     N/A
0x5de48b50      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       496     lsass.exe       -
0x5e0663e0      TCPv4   0.0.0.0 5357    0.0.0.0 0       LISTENING       4       System  -
0x5e0663e0      TCPv6   ::      5357    ::      0       LISTENING       4       System  -
0x5e06b010      UDPv4   0.0.0.0 64930   *       0               1308    svchost.exe     2019-08-19 14:40:13.000000 UTC
0x5e06b620      UDPv4   0.0.0.0 64931   *       0               1308    svchost.exe     2019-08-19 14:40:13.000000 UTC
0x5e06b620      UDPv6   ::      64931   *       0               1308    svchost.exe     2019-08-19 14:40:13.000000 UTC
0x5e07c670      UDPv4   0.0.0.0 3702    *       0               1308    svchost.exe     2019-08-19 14:40:17.000000 UTC
0x5e07c670      UDPv6   ::      3702    *       0               1308    svchost.exe     2019-08-19 14:40:17.000000 UTC
```

Imagen 5

```
0x5e08e2d0      TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  -
0x5e08e2d0      TCPv6   ::      445     ::      0       LISTENING       4       System  -
0x5e0a85d0      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       480     services.exe    -
0x5e0a85d0      TCPv6   ::      49155   ::      0       LISTENING       480     services.exe    -
0x5e0dbcb0      UDPv4   127.0.0.1       56645   *       0               1052    svchost.exe     2019-08-19 14:40:17.000000 UTC
0x5e109890      TCPv4   10.0.2.15       139     0.0.0.0 0       LISTENING       4       System  -
0x5e10ab80      UDPv4   10.0.2.15       137     *       0               4       System  2019-08-19 14:40:17.000000 UTC
0x5e10baa0      UDPv4   10.0.2.15       138     *       0               4       System  2019-08-19 14:40:17.000000 UTC
0x5e114010      UDPv4   0.0.0.0 3702    *       0               1308    svchost.exe     2019-08-19 14:40:17.000000 UTC
0x5e12c5d0      UDPv4   0.0.0.0 0       *       0               1052    svchost.exe     2019-08-19 14:40:17.000000 UTC
0x5e12c5d0      UDPv6   ::      0       *       0               1052    svchost.exe     2019-08-19 14:40:17.000000 UTC
0x5e135c40      UDPv4   0.0.0.0 3702    *       0               1308    svchost.exe     2019-08-19 14:40:17.000000 UTC
0x5e135c40      UDPv6   ::      3702    *       0               1308    svchost.exe     2019-08-19 14:40:17.000000 UTC
0x5e135dc0      UDPv4   0.0.0.0 3702    *       0               1308    svchost.exe     2019-08-19 14:40:17.000000 UTC
0x5e1379c0      UDPv4   0.0.0.0 5355    *       0               1052    svchost.exe     2019-08-19 14:40:20.000000 UTC
0x5e1379c0      UDPv6   ::      5355    *       0               1052    svchost.exe     2019-08-19 14:40:20.000000 UTC
0x5e2be2e0      UDPv4   0.0.0.0 5355    *       0               1052    svchost.exe     2019-08-19 14:40:20.000000 UTC
0x5e2beb30      TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       948     svchost.exe     -
0x5e2fc550      TCPv4   10.0.2.15       49231   172.217.160.131 80      ESTABLISHED     2080    firefox.exe     N/A
0x5e3037b0      TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       948     svchost.exe     -
0x5e3037b0      TCPv6   ::      49154   ::      0       LISTENING       948     svchost.exe     -
0x5e31f900      TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       480     services.exe    -
0x5e51fd20      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       384     wininit.exe     -
0x5e559ef0      TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       724     svchost.exe     -
0x5e55cef0      TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       724     svchost.exe     -
0x5e55cef0      TCPv6   ::      135     ::      0       LISTENING       724     svchost.exe     -
0x5e56a3c0      TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       384     wininit.exe     -
0x5e56a3c0      TCPv6   ::      49152   ::      0       LISTENING       384     wininit.exe     -
```

Imagen 6

```
0x5e5add20      TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       496     lsass.exe       -
0x5e5add20      TCPv6   ::      49156   ::      0       LISTENING       496     lsass.exe       -
0x5e5d2e30      TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       780     svchost.exe     -
0x5e5d3950      TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       780     svchost.exe     -
0x5e5d3950      TCPv6   ::      49153   ::      0       LISTENING       780     svchost.exe     -
0x5ee7fcf0      TCPv4   10.0.2.15       49240   172.217.167.138 443     ESTABLISHED     2080    firefox.exe     N/A
0x5fc0dcf0      TCPv4   10.0.2.15       49172   54.149.112.164  443     ESTABLISHED     2080    firefox.exe     N/A
0x5fc13010      TCPv4   10.0.2.15       49182   117.18.237.29   80      ESTABLISHED     2080    firefox.exe     N/A
0x5fc13cf0      TCPv4   10.0.2.15       49241   52.24.89.101    443     ESTABLISHED     2080    firefox.exe     N/A
0x5fc24010      TCPv4   10.0.2.15       49200   172.217.163.33  443     ESTABLISHED     2080    firefox.exe     N/A
0x5fc2e300      TCPv4   127.0.0.1       49167   127.0.0.1       49168   ESTABLISHED     3016    firefox.exe     N/A
0x5fc303d0      TCPv4   127.0.0.1       49168   127.0.0.1       49167   ESTABLISHED     3016    firefox.exe     N/A
0x5fc3a010      TCPv4   10.0.2.15       49169   23.195.74.19    80      ESTABLISHED     2080    firefox.exe     N/A
0x5fc43640      TCPv6   -       0       381b:de02:80fa:ffff:381b:de02:80fa:ffff 0       CLOSED  2080    firefox.exe     N/A
0x5fc49700      TCPv4   -       0       56.27.222.2     0       CLOSED  2080    firefox.exe     N/A
0x5fc4e810      TCPv4   10.0.2.15       49178   117.18.237.29   80      ESTABLISHED     2080    firefox.exe     N/A
0x5fc52940      TCPv4   10.0.2.15       49179   117.18.237.29   80      ESTABLISHED     2080    firefox.exe     N/A
0x5fc81810      TCPv4   127.0.0.1       49186   127.0.0.1       49185   ESTABLISHED     3316    firefox.exe     N/A
0x5fc869e0      TCPv4   127.0.0.1       49185   127.0.0.1       49186   ESTABLISHED     3316    firefox.exe     N/A
0x5fc94770      TCPv4   10.0.2.15       49195   172.217.160.131 80      ESTABLISHED     2080    firefox.exe     N/A
0x5fc989d0      TCPv4   10.0.2.15       49193   172.217.160.131 80      ESTABLISHED     2080    firefox.exe     N/A
0x5fca7cf0      TCPv4   10.0.2.15       49191   172.217.163.100 443     ESTABLISHED     2080    firefox.exe     N/A
0x5fcbe5b0      TCPv4   10.0.2.15       49214   172.217.160.131 80      FIN_WAIT2       2080    firefox.exe     N/A
0x5fcbeb30      TCPv4   10.0.2.15       49228   172.217.163.106 443     ESTABLISHED     2080    firefox.exe     N/A
0x5fccd010      TCPv4   10.0.2.15       49203   172.217.160.131 80      ESTABLISHED     2080    firefox.exe     N/A
0x5fccd5e0      TCPv4   10.0.2.15       49225   172.217.163.110 443     ESTABLISHED     2080    firefox.exe     N/A
0x5fcceb30      TCPv4   10.0.2.15       49239   172.217.167.138 443     ESTABLISHED     2080    firefox.exe     N/A
0x5fcdb460      TCPv4   10.0.2.15       49216   172.217.167.142 443     ESTABLISHED     2080    firefox.exe     N/A
0x5fcebcf0      TCPv4   10.0.2.15       49218   216.58.200.142  443     ESTABLISHED     2080    firefox.exe     N/A
```

Imagen 7

3.4 Argumentos de Línea de Comandos

Comando utilizado:
vol -f '/home/csi/Downloads/Challenge.raw' windows.cmdline

- **Hallazgos clave:**
    - **DumpIt.exe (PID 4084):** Los argumentos confirman su ejecución como herramienta de adquisición de memoria.
    - **WinRAR.exe (PID 3716):** Los argumentos muestran interacción con *flag.rar*, lo que refuerza la sospecha de posible exfiltración de datos.
    - **GoogleCrashHandler.exe:** No se observan argumentos inusuales, pero la ejecución de múltiples instancias sigue siendo sospechosa.

Procesos sospechosos identificados

DumpIt.exe (PID 4084)

- **Ruta:** "C:\Users\Jaffa\Desktop\DumpIt.exe"
- **Motivos de sospecha:**
    - Herramienta forense específica utilizada para generar volcados de memoria en formato *.raw* (como el que se analiza).
    - Un usuario común nunca ejecutaría esta aplicación.
    - Su ejecución implica que alguien —ya sea un investigador forense, un analista de incidentes o un atacante con conocimientos avanzados— estaba capturando la memoria del sistema.
    - En el contexto de la investigación, constituye la prueba definitiva que muestra claramente la recolección de evidencias en curso.

WinRAR.exe (PID 3716)

- **Ruta:** "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\Jaffa\Desktop\pr0t3ct3d\flag.rar"
- **Motivo de sospecha:**

- La interacción con el archivo *flag.rar* en el escritorio resulta inusual en un sistema estándar.

- El término *flag* se asocia frecuentemente a competiciones CTF (*Capture The Flag*) o actividades relacionadas con hacking.

- Si esta acción no fue iniciada por el usuario legítimo, podría indicar un intento de comprimir o manipular datos sensibles para su exfiltración.

GoogleCrashHandler.exe / GoogleCrashHandler64.exe (PIDs: 1292, 924, 1192, 864)

- **Rutas:**

  - "C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler.exe"

  - "C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler64.exe"

- **Motivo de sospecha:**

  - Ejecución simultánea de múltiples instancias, lo cual no es habitual.

  - Estos procesos suelen encargarse de enviar reportes de fallos a Google.

  - Atacantes pueden camuflar malware bajo nombres de procesos legítimos.

  - El número de instancias detectadas aumenta el nivel de sospecha y requiere verificación adicional (p. ej. comprobación de integridad mediante *hashes*).

  - Sin embargo, VirusTotal no reporta estos binarios como maliciosos, lo que obliga a un análisis más profundo antes de emitir un juicio definitivo.

```
❯ vol -f '/home/csi/Downloads/Challenge.raw' windows.cmdline
Volatility 3 Framework 2.26.0
Progress:  100.00               PDB scanning finished
PID     Process         Args

4       System          -
264     smss.exe        \SystemRoot\System32\smss.exe
336     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,20480,768 Windows=On SubSystemType=Windows
ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3
ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off
MaxRequestThreads=16
384     wininit.exe     wininit.exe
```

396 csrss.exe %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
436 winlogon.exe winlogon.exe
480 services.exe C:\Windows\system32\services.exe
496 lsass.exe C:\Windows\system32\lsass.exe
504 lsm.exe C:\Windows\system32\lsm.exe
608 svchost.exe C:\Windows\system32\svchost.exe -k DcomLaunch
668 VBoxService.ex C:\Windows\System32\VBoxService.exe
724 svchost.exe C:\Windows\system32\svchost.exe -k RPCSS
780 svchost.exe C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
896 svchost.exe C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
948 svchost.exe C:\Windows\system32\svchost.exe -k netsvcs
1008 audiodg.exe C:\Windows\system32\AUDIODG.EXE 0x2ac
400 svchost.exe C:\Windows\system32\svchost.exe -k LocalService
1052 svchost.exe C:\Windows\system32\svchost.exe -k NetworkService
1176 spoolsv.exe C:\Windows\System32\spoolsv.exe
1212 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
1308 svchost.exe C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
1812 taskhost.exe "taskhost.exe"
1868 dwm.exe "C:\Windows\system32\Dwm.exe"
1876 taskeng.exe taskeng.exe {54DBC692-AE6C-4620-B58A-A05704950172}
1944 explorer.exe C:\Windows\Explorer.EXE
1292 GoogleCrashHan "C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler.exe"
924 GoogleCrashHan "C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler64.exe"
1108 VBoxTray.exe "C:\Windows\System32\VBoxTray.exe"
880 cmd.exe "C:\Windows\system32\cmd.exe"
916 conhost.exe \??\C:\Windows\system32\conhost.exe
856 SearchIndexer. C:\Windows\system32\SearchIndexer.exe /Embedding
2124 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
2132 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-dir=C:\Users\Jaffa\AppData\Local\Google\Chrome\User Data" /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\Jaffa\AppData\Local\Google\Chrome\User Data\Crashpad" "--metrics-dir=C:\Users\Jaffa\AppData\Local\Google\Chrome\User Data" --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=76.0.3809.100 --initial-client-data=0x38,0x3c,0x40,0x34,0x44,0x7fef693ef08,0x7fef693ef18,0x7fef693ef28
2168 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=watcher --main-thread-id=2128 --on-initialized-event-handle=12 --parent-handle=164 /prefetch:6
2292 WmiPrvSE.exe C:\Windows\system32\wbem\wmiprvse.exe

2340 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --field-trial-handle=912,6904440883533218926,14009848578096020689,131072 --lang=en-US --service-sandbox-type=network --service-request-channel-token=7087325372642059998 --mojo-platform-channel-handle=1404 /prefetch:8
2440 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=912,6904440883533218926,14009848578096020689,131072 --lang=en-US --instant-process --enable-auto-reload --device-scale-factor=1 --num-raster-threads=1 --service-request-channel-token=30920957510107878 --renderer-client-id=6 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=1956 /prefetch:1
2452 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=912,6904440883533218926,14009848578096020689,131072 --lang=en-US --enable-auto-reload --device-scale-factor=1 --num-raster-threads=1 --service-request-channel-token=8732891429699623721 --renderer-client-id=7 --no-v8-untrusted-code-mitigations --mojo-platform-channel-handle=2148 /prefetch:1
2800 WmiApSrv.exeC:\Windows\system32\wbem\WmiApSrv.exe
2896 WmiPrvSE.exe C:\Windows\system32\wbem\wmiprvse.exe
2940 chrome.exe "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=gpu-process --field-trial-handle=912,6904440883533218926,14009848578096020689,131072 --gpu-preferences=IAAAAAAAAADgAAAwAAAAAAAAYAAAAAAACAAAAAAAAAAoAAAAB AAAACAAAAAAAAAAKAAAAAAAAAAwAAAAAAAAADgAAAAAAAAAEAAAAAAAAAAAAA AABQAAABAAAAAAAAAAAAAAAAYAAAAQAAAAAAAAAEAAAAFAAAAEAAAAAAAAAA BAAAABgAAAA== --use-gl=swiftshader-webgl --service-request-channel-token=8183290027954516201 --mojo-platform-channel-handle=2724 --ignored=" --type=renderer " /prefetch:2
2080 firefox.exe "C:\Program Files (x86)\Mozilla Firefox\firefox.exe"
2860 firefox.exe "C:\Program Files (x86)\Mozilla Firefox\firefox.exe" -contentproc --channel="2080.0.1430399655\1507561340" -parentBuildID 20190813150448 -greomni "C:\Program Files (x86)\Mozilla Firefox\omni.ja" -appomni "C:\Program Files (x86)\Mozilla Firefox\browser\omni.ja" -appdir "C:\Program Files (x86)\Mozilla Firefox\browser" - 2080 "\\.\pipe\gecko-crash-server-pipe.2080" 1096 gpu
3016 firefox.exe "C:\Program Files (x86)\Mozilla Firefox\firefox.exe" -contentproc --channel="2080.3.1961766982\1524136179" -childID 1 -isForBrowser -prefsHandle 1596 -prefMapHandle 1652 -prefsLen 1 -prefMapSize 190550 -parentBuildID 20190813150448 -greomni "C:\Program Files (x86)\Mozilla Firefox\omni.ja" -appomni "C:\Program Files (x86)\Mozilla Firefox\browser\omni.ja" -appdir "C:\Program Files (x86)\Mozilla Firefox\browser" - 2080 "\\.\pipe\gecko-crash-server-pipe.2080" 764 tab
2968 firefox.exe "C:\Program Files (x86)\Mozilla Firefox\firefox.exe" -contentproc --channel="2080.13.820371489\1898621292" -childID 2 -isForBrowser -prefsHandle 2684 -prefMapHandle 2688 -prefsLen 5982 -prefMapSize 190550 -parentBuildID 20190813150448 -greomni "C:\Program Files (x86)\Mozilla Firefox\omni.ja" -appomni "C:\Program Files (x86)\Mozilla Firefox\browser\omni.ja" -appdir "C:\Program Files (x86)\Mozilla Firefox\browser" - 2080 "\\.\pipe\gecko-crash-server-pipe.2080" 2700 tab

3316 firefox.exe "C:\Program Files (x86)\Mozilla Firefox\firefox.exe" -contentproc --channel="2080.20.122820616\259359170" -childID 3 -isForBrowser -prefsHandle 3252 -prefMapHandle 3728 -prefsLen 6704 -prefMapSize 190550 -parentBuildID 20190813150448 -greomni "C:\Program Files (x86)\Mozilla Firefox\omni.ja" -appomni "C:\Program Files (x86)\Mozilla Firefox\browser\omni.ja" -appdir "C:\Program Files (x86)\Mozilla Firefox\browser" - 2080 "\\.\pipe\gecko-crash-server-pipe.2080" 3740 tab
3716 WinRAR.exe "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\Jaffa\Desktop\pr0t3ct3d\flag.rar"
4084 DumpIt.exe "C:\Users\Jaffa\Desktop\DumpIt.exe"
4092 conhost.exe \??\C:\Windows\system32\conhost.exe
1224 sppsvc.exe -
2256 GoogleUpdate.e -
1192 GoogleCrashHan -
864 GoogleCrashHan -

```
12:56:18 csi@csi ~
❯ vol -f '/home/csi/Downloads/Challenge.raw' windows.cmdline
Volatility 3 Framework 2.26.0
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  -
264     smss.exe        \SystemRoot\System32\smss.exe
336     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
384     wininit.exe     wininit.exe
396     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
436     winlogon.exe    winlogon.exe
480     services.exe    C:\Windows\system32\services.exe
496     lsass.exe       C:\Windows\system32\lsass.exe
504     lsm.exe C:\Windows\system32\lsm.exe
608     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch
668     VBoxService.ex  C:\Windows\System32\VBoxService.exe
724     svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS
780     svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
896     svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
```

Imagen 8

```
948     svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs
1008    audiodg.exe     C:\Windows\system32\AUDIODG.EXE 0x2ac
400     svchost.exe     C:\Windows\system32\svchost.exe -k LocalService
1052    svchost.exe     C:\Windows\system32\svchost.exe -k NetworkService
1176    spoolsv.exe     C:\Windows\System32\spoolsv.exe
1212    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
1308    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
1812    taskhost.exe    "taskhost.exe"
1868    dwm.exe "C:\Windows\system32\Dwm.exe"
1876    taskeng.exe     taskeng.exe {54DBC692-AE6C-4620-B58A-A05704950172}
1944    explorer.exe    C:\Windows\Explorer.EXE
1292    GoogleCrashHan  "C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler.exe"
924     GoogleCrashHan  "C:\Program Files (x86)\Google\Update\1.3.34.11\GoogleCrashHandler64.exe"
1108    VBoxTray.exe    "C:\Windows\System32\VBoxTray.exe"
880     cmd.exe "C:\Windows\system32\cmd.exe"
916     conhost.exe     \??\C:\Windows\system32\conhost.exe
856     SearchIndexer.  C:\Windows\system32\SearchIndexer.exe /Embedding
2124    chrome.exe      "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe"
2132    chrome.exe      "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-dir=C:\Users\Jaffa\AppData\Local\Google\Chrome\User Data" /prefetch:7 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\Jaffa\AppData\Local\Google\Chrome\User Data\Crashpad" "--metrics-dir=C:\Users\Jaffa\AppData\Local\Google\Chrome\User Data" --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=76.0.3809.100 --initial-client-data=0x38,0x3c,0x40,0x34,0x44,0x7fef693ef08,0x7fef693ef18,0x7fef693ef28
2168    chrome.exe      "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=watcher --main-thread-id=2128 --on-initialized-event-handle=12 --parent-handle=164 /prefetch:6
2292    WmiPrvSE.exe    C:\Windows\system32\wbem\wmiprvse.exe
2340    chrome.exe      "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=utility --field-trial-handle=912,6904440883533218926,14009848578096020689,131072 --lang=en-US --service-sandbox-type=network --service-request-channel-token=7087325372642059998 --mojo-platform-channel-hand
```

Imagen 9

Imagen 10

Imagen 11

4. Volcado de Archivos Sospechosos

Comandos Utilizados:

vol -f '/home/csi/Downloads/Challenge.raw' -o '/home/csi/Downloads/Extractions' windows.memmap --pid 4084 --dump para obtener rangos de memoria virtual en bruto.

vol -f '/home/csi/Downloads/Challenge.raw' -o '/home/csi/Downloads/Extractions' windows.dumpfiles --pid 4084 para obtener módulos ejecutables y archivos mapeados

Hallazgos Clave:

El ejecutable **DumpIt.exe** fue extraído con éxito:

- **Ruta del archivo:**

  /home/csi/Downloads/Extractions/file.0xfa8001436520.0xfa8001407010.DataSection Object.DumpIt.exe.dat

Análisis en VirusTotal: virustotal.com Imagen 13 e Imagen 14 se observan distintos proveedores que señalan este archivo como malicioso, por ejemplo, Google, CrowdStrike Falcon AI y Cynet entre otros.

vol -f '/home/csi/Downloads/Challenge.raw' -o '/home/csi/Downloads/Extractions' windows.memmap --pid 4084 --dump

01:43:11 csi@csi ~/Downloads/Extractions
❯ ls
file.0xfa8001436520.0xfa8001407010.DataSectionObject.DumpIt.exe.dat

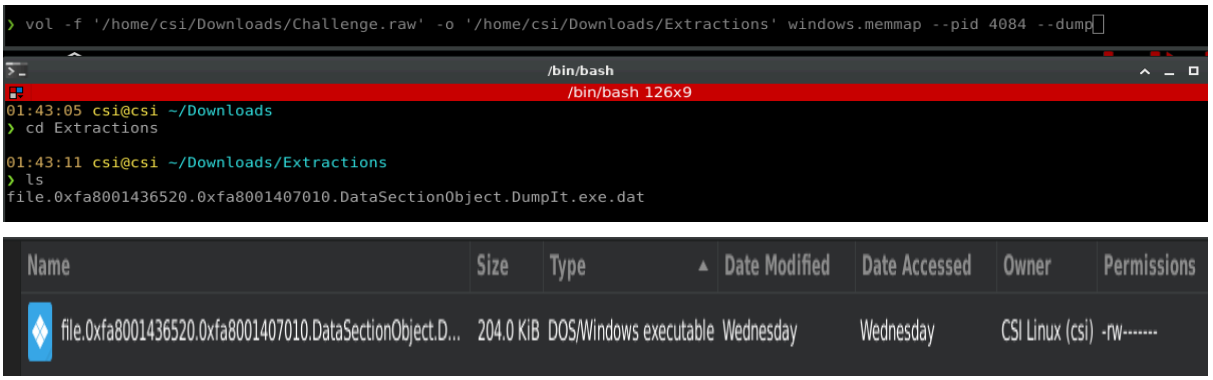

Imagen 12

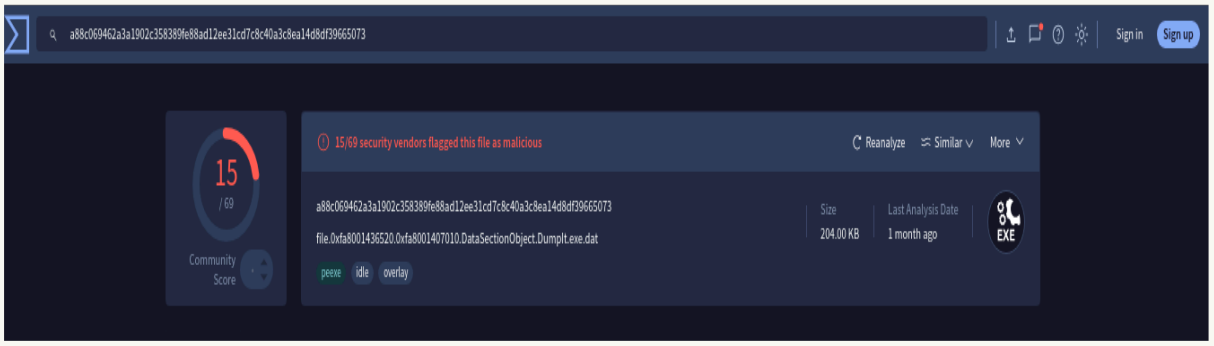

Imagen 13

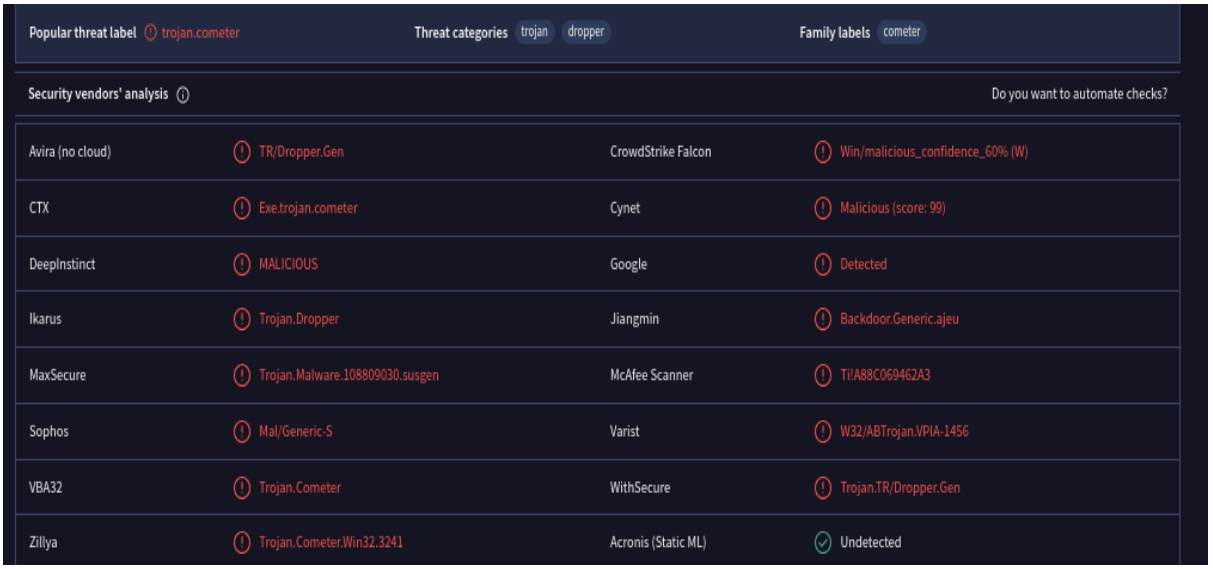

Imagen 14

```
❯ vol -f '/home/csi/Downloads/Challenge.raw' -o '/home/csi/Downloads/Extractions'
windows.dumpfiles --pid 4084
Volatility 3 Framework 2.26.0
Progress:  100.00               PDB scanning finished
Cache FileObject      FileName        Result

ImageSectionObject  0xfa8002a61f20      kernel32.dll
file.0xfa8002a61f20.0xfa8002a558a0.ImageSectionObject.kernel32.dll.img
ImageSectionObject  0xfa800292c2c0      apisetschema.dll
file.0xfa800292c2c0.0xfa8002970250.ImageSectionObject.apisetschema.dll.img
DataSectionObject   0xfa8001436520      DumpIt.exe
file.0xfa8001436520.0xfa8001407010.DataSectionObject.DumpIt.exe-1.dat
ImageSectionObject  0xfa8001436520      DumpIt.exe
file.0xfa8001436520.0xfa8003895010.ImageSectionObject.DumpIt.exe.img
ImageSectionObject  0xfa8003205710      wow64cpu.dll
file.0xfa8003205710.0xfa800320d830.ImageSectionObject.wow64cpu.dll.img
ImageSectionObject  0xfa80031fc850      wow64win.dll
file.0xfa80031fc850.0xfa8003208c30.ImageSectionObject.wow64win.dll.img
ImageSectionObject  0xfa8003205470      wow64.dll
file.0xfa8003205470.0xfa8003205230.ImageSectionObject.wow64.dll.img
ImageSectionObject  0xfa8002a51c90      rpcrt4.dll
file.0xfa8002a51c90.0xfa8002a518f0.ImageSectionObject.rpcrt4.dll.img
ImageSectionObject  0xfa8002a52c20      sspicli.dll
file.0xfa8002a52c20.0xfa8002a528b0.ImageSectionObject.sspicli.dll.img
DataSectionObject   0xfa8002a52f20      cryptbase.dll
file.0xfa8002a52f20.0xfa8002d46010.DataSectionObject.cryptbase.dll-1.dat
ImageSectionObject  0xfa8002a52f20      cryptbase.dll
file.0xfa8002a52f20.0xfa8002a53d10.ImageSectionObject.cryptbase.dll.img
ImageSectionObject  0xfa8002a637c0      advapi32.dll
file.0xfa8002a637c0.0xfa8002a5dd00.ImageSectionObject.advapi32.dll.img
ImageSectionObject  0xfa8002a63ac0      usp10.dll
file.0xfa8002a63ac0.0xfa8002a5d870.ImageSectionObject.usp10.dll.img
ImageSectionObject  0xfa8002a5cd70      msctf.dll
file.0xfa8002a5cd70.0xfa8002a5c8b0.ImageSectionObject.msctf.dll.img
ImageSectionObject  0xfa8002a06a70      KernelBase.dll
file.0xfa8002a06a70.0xfa8002a60e60.ImageSectionObject.KernelBase.dll.img
ImageSectionObject  0xfa8002a60c10      sechost.dll
file.0xfa8002a60c10.0xfa8002a618b0.ImageSectionObject.sechost.dll.img
ImageSectionObject  0xfa8002a617c0      user32.dll
file.0xfa8002a617c0.0xfa8002a55bb0.ImageSectionObject.user32.dll.img
DataSectionObject   0xfa8002a60910      gdi32.dll
file.0xfa8002a60910.0xfa80022c9dc0.DataSectionObject.gdi32.dll-1.dat
ImageSectionObject  0xfa8002a60910      gdi32.dll
file.0xfa8002a60910.0xfa8002a61d10.ImageSectionObject.gdi32.dll.img
ImageSectionObject  0xfa8002a7ca90      imm32.dll
file.0xfa8002a7ca90.0xfa8002a7a820.ImageSectionObject.imm32.dll.img
```

ImageSectionObject 0xfa8002a7a5d0 shlwapi.dll
file.0xfa8002a7a5d0.0xfa8002a72290.ImageSectionObject.shlwapi.dll.img
ImageSectionObject 0xfa8002a7c940 msvcrt.dll
file.0xfa8002a7c940.0xfa8002a7a9d0.ImageSectionObject.msvcrt.dll.img
ImageSectionObject 0xfa8002268b00 ntdll.dll
file.0xfa8002268b00.0xfa80022a3010.ImageSectionObject.ntdll.dll.img
ImageSectionObject 0xfa80022ccaf0 ntdll.dll
file.0xfa80022ccaf0.0xfa80022d1bf0.ImageSectionObject.ntdll.dll.img
ImageSectionObject 0xfa8002a089b0 lpk.dll
file.0xfa8002a089b0.0xfa8002a60a00.ImageSectionObject.lpk.dll.img

```
02:07:08 csi@cs1 ~
❯ vol -f '/home/csi/Downloads/Challenge.raw' -o '/home/csi/Downloads/Extractions' windows.dumpfiles --pid 4084
Volatility 3 Framework 2.26.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

ImageSectionObject      0xfa8002a61f20  kernel32.dll    file.0xfa8002a61f20.0xfa8002a558a0.ImageSectionObject.kernel32.dll-1.img
ImageSectionObject      0xfa800292c2c0  apisetschema.dll        file.0xfa800292c2c0.0xfa8002970250.ImageSectionObject.apisetschema.dll-1.img
DataSectionObject       0xfa8001436520  DumpIt.exe      file.0xfa8001436520.0xfa8001407010.DataSectionObject.DumpIt.exe-2.dat
ImageSectionObject      0xfa8001436520  DumpIt.exe      file.0xfa8001436520.0xfa8003895010.ImageSectionObject.DumpIt.exe-1.img
ImageSectionObject      0xfa8003205710  wow64cpu.dll    file.0xfa8003205710.0xfa800320d830.ImageSectionObject.wow64cpu.dll-1.img
ImageSectionObject      0xfa80031fc850  wow64win.dll    file.0xfa80031fc850.0xfa8003208c30.ImageSectionObject.wow64win.dll-1.img
ImageSectionObject      0xfa8003205470  wow64.dll       file.0xfa8003205470.0xfa8003205230.ImageSectionObject.wow64.dll-1.img
ImageSectionObject      0xfa8002a51c90  rpcrt4.dll      file.0xfa8002a51c90.0xfa8002a518f0.ImageSectionObject.rpcrt4.dll-1.img
ImageSectionObject      0xfa8002a52c20  sspicli.dll     file.0xfa8002a52c20.0xfa8002a528b0.ImageSectionObject.sspicli.dll-1.img
DataSectionObject       0xfa8002a52f20  cryptbase.dll   file.0xfa8002a52f20.0xfa8002d46010.DataSectionObject.cryptbase.dll-1.dat
ImageSectionObject      0xfa8002a52f20  cryptbase.dll   file.0xfa8002a52f20.0xfa8002a53d10.ImageSectionObject.cryptbase.dll-1.img
ImageSectionObject      0xfa8002a637c0  advapi32.dll    file.0xfa8002a637c0.0xfa8002a5dd00.ImageSectionObject.advapi32.dll-1.img
ImageSectionObject      0xfa8002a63ac0  usp10.dll       file.0xfa8002a63ac0.0xfa8002a5d870.ImageSectionObject.usp10.dll-1.img
ImageSectionObject      0xfa8002a5cd70  msctf.dll       file.0xfa8002a5cd70.0xfa8002a5c8b0.ImageSectionObject.msctf.dll-1.img
ImageSectionObject      0xfa8002a06a70  KernelBase.dll  file.0xfa8002a06a70.0xfa8002a60e60.ImageSectionObject.KernelBase.dll-1.img
ImageSectionObject      0xfa8002a60c10  sechost.dll     file.0xfa8002a60c10.0xfa8002a618b0.ImageSectionObject.sechost.dll-1.img
ImageSectionObject      0xfa8002a617c0  user32.dll      file.0xfa8002a617c0.0xfa8002a55bb0.ImageSectionObject.user32.dll-1.img
DataSectionObject       0xfa8002a60910  gdi32.dll       file.0xfa8002a60910.0xfa80022c9dc0.DataSectionObject.gdi32.dll-1.dat
ImageSectionObject      0xfa8002a60910  gdi32.dll       file.0xfa8002a60910.0xfa8002a61d10.ImageSectionObject.gdi32.dll-1.img
ImageSectionObject      0xfa8002a7ca90  imm32.dll       file.0xfa8002a7ca90.0xfa8002a7a820.ImageSectionObject.imm32.dll-1.img
ImageSectionObject      0xfa8002a7a5d0  shlwapi.dll     file.0xfa8002a7a5d0.0xfa8002a72290.ImageSectionObject.shlwapi.dll-1.img
ImageSectionObject      0xfa8002a7c940  msvcrt.dll      file.0xfa8002a7c940.0xfa8002a7a9d0.ImageSectionObject.msvcrt.dll-1.img
ImageSectionObject      0xfa8002268b00  ntdll.dll       file.0xfa8002268b00.0xfa80022a3010.ImageSectionObject.ntdll.dll-1.img
ImageSectionObject      0xfa80022ccaf0  ntdll.dll       file.0xfa80022ccaf0.0xfa80022d1bf0.ImageSectionObject.ntdll.dll-1.img
ImageSectionObject      0xfa8002a089b0  lpk.dll file.0xfa8002a089b0.0xfa8002a60a00.ImageSectionObject.lpk.dll-1.img
```

5. Conclusiones

- La ejecución de **DumpIt.exe** indica extracción activa de memoria, actividad sospechosa si no es un análisis controlado.

- **WinRAR.exe** apunta a manipulación de un archivo sensible (*flag.rar*), lo que sugiere intento de compresión/exfiltración.

- La presencia de múltiples instancias de **GoogleCrashHandler.exe** requiere validación para descartar *malware enmascarado*.

- **Firefox.exe** mostró conexiones externas que podrían ser normales, aunque deben revisarse en contexto.

6. Anexo

Resumen sobre las diferencias entre Volatility 2.6 y Volatility 3

Durante el desarrollo del análisis forense de memoria, me encontré con una dificultad importante: la información proporcionada en el curso hacía referencia a Volatility 2.6, mientras que la versión actual y mantenida es Volatility 3. Esto generó una serie de retos, ya que muchos de los comandos, parámetros y plugins explicados en el material del curso han quedado obsoletos o han cambiado de forma significativa.

Una de las diferencias más notables es que en Volatility 2.6 se utilizaba el parámetro --profile para definir el perfil del sistema operativo (por ejemplo, Win7SP1x64). En Volatility 3, este parámetro ha desaparecido, ya que el framework incorpora un sistema de detección automática mediante el plugin windows.info. Esta modificación, aunque más moderna y flexible, supuso inicialmente un obstáculo, ya que obligó a replantear todos los procedimientos aprendidos.

Otro cambio relevante fue la ausencia de algunos comandos clásicos. Por ejemplo, el plugin memdump en Volatility 2.6 no tiene un equivalente directo en Volatility 3. En su lugar, deben emplearse varias alternativas como windows.memmap --dump, windows.vadump o windows.dumpfiles, dependiendo del tipo de información que se busque extraer (rangos de memoria en bruto, fragmentos del espacio de memoria del proceso o archivos ejecutables mapeados). Esto exige comprender en mayor profundidad cómo funciona la memoria y qué resultado se espera de cada plugin, lo que incrementa la complejidad del análisis.

En resumen, la transición de Volatility 2.6 a Volatility 3 ha supuesto una inversión considerable de tiempo en investigación y pruebas. Si bien esta situación ralentizó mi progreso, también me permitió adquirir un conocimiento mucho más profundo de las herramientas, los plugins y la lógica del framework. Este esfuerzo adicional ha sido valioso para mi aprendizaje, pero refleja claramente la brecha entre los materiales formativos disponibles y el estado actual de la herramienta.