



---

# ANÁLISIS FORENSE

---

Unidad 1. Actividad 3



13 DE NOVIEMBRE DE 2023  
CARLOS DÍAZ MONTES  
ESPECIALIZACIÓN DE CIBERSEGURIDAD

## Índice

1. ¿Cuál es el hash SHA-1 del archivo memory-triage.mem?.....	2
2. ¿Cuál es el perfil más apropiado para la máquina? .....	2
3. ¿Cuál es el PID del proceso notepad.exe? .....	2
4. Nombre del proceso hijo de wscript.exe.....	2
5. ¿Cuál era la dirección IP de la máquina en el momento en el que se hizo la imagen de memoria? .....	2
6. Basándose en la respuesta relacionada con el PID infectado ¿Cuál es la IP del atacante? .....	3
7. ¿Cuál es el nombre del proceso relacionado con la librería VCRUNTIME140.dll? .....	3
8. ¿Cuál es el valor del hash MD5 del potencial malware en el sistema? .....	4
9. ¿Cuál es el hash LM de la cuenta de Bob? .....	4
10. ¿Qué protecciones tiene el nodo VAD en la dirección 0xfffffa800577ba10? .....	4
11. ¿Qué protecciones tenía el nodo VAD que empieza en la dirección 0x00000000033c0000 y 4 termina en la dirección 0x00000000033dffff? .....	4
12. Hubo un script VBS corriendo en la máquina. ¿Cuál es el nombre del script (sin extensión)? .....	5
13. Se ejecutó una aplicación el 2019-03-07 23:06:58 UTC. ¿Cuál es el nombre del programa? .5	
14. ¿Qué estaba escrito en el notepad.exe en el momento de la captura de memoria? .....	5
15. ¿Cuál es el nombre corto del archivo en el registro 59045? .....	6
16. Este equipo ha sido comprometido y tiene una sesión de meterpreter. ¿Qué PID ha sido .... infectado?.....	6

## 1. ¿Cuál es el hash SHA-1 del archivo memory-triage.mem?

Usamos el comando sha1sum (nombre del archivo):

```
(kali@kali)-[~/volatility]
$ sha1sum Triage-Memory-001.mem
c95e8cc8c946f95a109ea8e47a6800de10a27abd Triage-Memory-001.mem
```

## 2. ¿Cuál es el perfil más apropiado para la máquina?

Usamos el comando python2.7 vol.py -f (nombre del archivo) imageinfo y como vemos es Win7SP1X64Bits:

```
(kali@kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/volatility/Triage-Memory-001.mem)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80029f80a0L
Number of Processors : 2
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80029f9d00L
KPCR for CPU 1 : 0xfffff80009ee000L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2019-03-22 05:46:00 UTC+0000
Image local date and time : 2019-03-22 01:46:00 -0400
```

## 3. ¿Cuál es el PID del proceso notepad.exe?

Usamos el comando python2.7 vol.py -f (nombre del archivo) --profile=Win7SP1x64 pstree | grep "notepad", como vemos la respuesta es el 3032:

```
(kali@kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 pstree | grep "notepad"
Volatility Foundation Volatility Framework 2.6.1
. 0xfffffa80054f9060:notepad.exe 3032 1432 1 60 2019-03-22 05:32:22 UTC+0000
```

## 4. Nombre del proceso hijo de wscript.exe.

Usamos el comando python2.7 vol.py -f (nombre del archivo) --profile=Win7SP1x64 pstree | grep -A 2 "wscript.exe", como vemos se llama:

```
(kali@kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 pstree | grep -A 2 "wscript.exe"
Volatility Foundation Volatility Framework 2.6.1
.. 0xfffffa8005a80060:wscript.exe 5116 3952 8 312 2019-03-22 05:35:32 UTC+0000
... 0xfffffa8005a1d9e0:UwkpjFjDzM.exe 3496 5116 5 109 2019-03-22 05:35:33 UTC+0000
... 0xfffffa8005bb0060:cmd.exe 4660 3496 1 33 2019-03-22 05:35:36 UTC+0000
```

## 5. ¿Cuál era la dirección IP de la máquina en el momento en el que se hizo la imagen de memoria?

Para ver la ip que tenia en el momento de la imagen es 10.0.0.101:

```
(kali@kali)~/volatility
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P) Proto Local Address Foreign Address State Pid Owner Created
0x13e057300 UDPv4 10.0.0.101:55736 ** 2888 svchost.exe 2019-03-22 05:32:20 UTC+
0000
0x13e05b4f0 UDPv6 ::1:55735 ** 2888 svchost.exe 2019-03-22 05:32:20 UTC+
0000
0x13e05b790 UDPv6 fe80::7475:ef30:be18:7807:55734 ** 2888 svchost.exe 2019-03-22 05:32:20 UTC+
+0000
0x13e05d4b0 UDPv6 fe80::7475:ef30:be18:7807:1900 ** 2888 svchost.exe 2019-03-22 05:32:20 UTC+
0000
0x13e05dec0 UDPv4 127.0.0.1:55737 ** 2888 svchost.exe 2019-03-22 05:32:20 UTC+
0000
0x13e05e3f0 UDPv4 10.0.0.101:1900 ** 2888 svchost.exe 2019-03-22 05:32:20 UTC+
0000
0x13e05eab0 UDPv6 ::1:1900 ** 2888 svchost.exe 2019-03-22 05:32:20 UTC+
0000
0x13e064d70 UDPv4 127.0.0.1:1900 ** 2888 svchost.exe 2019-03-22 05:32:20 UTC+
0000
0x13e02bcf0 TCPv4 -:49220 72.51.60.132:443 CLOSED 4048 POWERPNT.EXE
0x13e035790 TCPv4 -:49223 72.51.60.132:443 CLOSED 4048 POWERPNT.EXE
0x13e036470 TCPv4 -:49224 72.51.60.132:443 CLOSED 4048 POWERPNT.EXE
0x13e258010 UDPv4 127.0.0.1:55560 ** 5116 wscript.exe 2019-03-22 05:35:32 UTC+
0000
0x13e305a50 UDPv4 0.0.0.0:5355 ** 232 svchost.exe 2019-03-22 05:32:09 UTC+
```

## 6. Basándose en la respuesta relacionada con el PID infectado ¿Cuál es la IP del atacante?

La ip del atacante es 10.0.0.106:

```
(kali@kali)~/volatility
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 netscan | grep UwpkjFjDzM.exe
Volatility Foundation Volatility Framework 2.6.1
0x13e397190 TCPv4 10.0.0.101:49217 10.0.0.106:4444 ESTABLISHED 3496 UwpkjFjDzM.exe
```

## 7. ¿Cuál es el nombre del proceso relacionado con la librería VCRUNTIME140.dll?

El nombre del proceso relacionado es officeclicktorun

```
(kali@kali)~/volatility
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 dlllist | grep -B 35 VCRUNTIME140.dll
Volatility Foundation Volatility Framework 2.6.1
0x000007fef5300000 0xd000 0x1 2019-03-22 05:32:14 UTC+0000 C:\Windows\system32\wdiasqmmodule.dll
0x000007fefcb90000 0x22000 0x1 2019-03-22 05:32:15 UTC+0000 C:\Windows\system32\bcrypt.dll
*****
OfficeClickToRun pid: 1136
Command line : "C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service
Service Pack 1

Base Size LoadCount LoadTime Path
0x000000013f420000 0xa9d000 0xffff 1970-01-01 00:00:00 UTC+0000 C:\Program Files\Common Files\Microsoft Shared\ClickToRun
\OfficeClickToRun.exe
0x0000000077260000 0x1a9000 0xffff 1970-01-01 00:00:00 UTC+0000 C:\Windows\SYSTEM32\ntdll.dll
0x0000000077040000 0x11f000 0xffff 2019-03-22 05:32:05 UTC+0000 C:\Windows\system32\kernel32.dll
0x000007fef3800000 0x6c000 0xffff 2019-03-22 05:32:05 UTC+0000 C:\Windows\system32\KERNELBASE.dll
0x000007fef9700000 0xdb000 0xffff 2019-03-22 05:32:05 UTC+0000 C:\Windows\system32\ADVAPI32.dll
0x000007fef6b00000 0x9f000 0xffff 2019-03-22 05:32:05 UTC+0000 C:\Windows\system32\msvcrt.dll
0x000007fef1600000 0x1f000 0xffff 2019-03-22 05:32:05 UTC+0000 C:\Windows\SYSTEM32\sechost.dll
0x000007fef7a00000 0x12d000 0xffff 2019-03-22 05:32:05 UTC+0000 C:\Windows\system32\RPCRT4.dll
0x000007fefef60000 0x67000 0xffff 2019-03-22 05:32:05 UTC+0000 C:\Windows\system32\GDI32.dll
0x0000000077160000 0xfa000 0xffff 2019-03-22 05:32:05 UTC+0000 C:\Windows\system32\USER32.dll
```

8. ¿Cuál es el valor del hash MD5 del potencial malware en el sistema?

Es el 3496:

```
(kali@kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 pstree | grep -A 2 "wscript.exe"
Volatility Foundation Volatility Framework 2.6.1
.. 0xfffffa8005a80060:wscript.exe          5116   3952    8   312 2019-03-22 05:35:32 UTC+0000
... 0xfffffa8005a1d9e0:UWkpfjDzM.exe       3496   5116    5   109 2019-03-22 05:35:33 UTC+0000
.... 0xfffffa8005bb0060:cmd.exe            4660   3496    1    33 2019-03-22 05:35:36 UTC+0000

(kali@kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 procdump -p 3496 -D .
Volatility Foundation Volatility Framework 2.6.1
Process(V)      ImageBase      Name              Result
-----
0xfffffa8005a1d9e0 0x0000000000040000 UWkpfjDzM.exe     OK: executable.3496.exe

(kali@kali)-[~/volatility]
$
```

```
(kali@kali)-[~/volatility]
$ md5sum executable.3496.exe
690ea20bc3bdfb328e23005d9a80c290  executable.3496.exe
```

9. ¿Cuál es el hash LM de la cuenta de Bob?

```
(kali@kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Bob:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
```

10. ¿Qué protecciones tiene el nodo VAD en la dirección 0xfffffa800577ba10?

```
(kali@kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 vadinfo | grep -A 5 0xfffffa800577ba10
Volatility Foundation Volatility Framework 2.6.1
VAD node @ 0xfffffa800577ba10 Start 0x000000000030000 End 0x000000000033fff Tag Vad
Flags: NoChange: 1, Protection: 1
Protection: PAGE_READONLY
Vad Type: VadNone
ControlArea @fffffa8005687a50 Segment fffff8a000c4f870
NumberOfSectionReferences: 1 NumberOfPfnReferences: 0
```

11. ¿Qué protecciones tenía el nodo VAD que empieza en la dirección 0x00000000033c0000 y termina en la dirección 0x00000000033dffff?

```
(kali@kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 vadinfo | grep -A 5 "Start 0x00000000033c0000 End 0x00000000033dffff"
Volatility Foundation Volatility Framework 2.6.1
VAD node @ 0xfffffa80052652b0 Start 0x00000000033c0000 End 0x00000000033dffff Tag VadS
Flags: CommitCharge: 32, PrivateMemory: 1, Protection: 24
Protection: PAGE_NOACCESS
Vad Type: VadNone

VAD node @ 0xfffffa8003f416d0 Start 0x00000000033a0000 End 0x00000000033bfff Tag VadS
```

12. Hubo un script VBS corriendo en la máquina. ¿Cuál es el nombre del script (sin extensión)?

```
(kali㉿kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 cmdline -p 5116
Volatility Foundation Volatility Framework 2.6.1
*****
wscript.exe pid: 5116
Command line : "C:\Windows\System32\wscript.exe" //B //NOLOGO %TEMP%\vhjReUDEuumrX.vbs
```

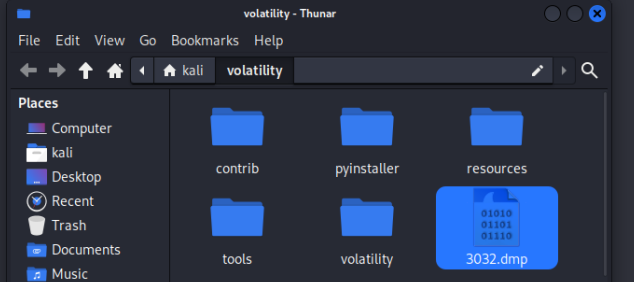
13. Se ejecutó una aplicación el 2019-03-07 23:06:58 UTC. ¿Cuál es el nombre del programa?

```
(kali㉿kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 shimcache | grep -A 5 "2019-03-07 23:06:58"
Volatility Foundation Volatility Framework 2.6.1
2019-03-07 23:06:58 UTC+0000 \??\C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe
2010-11-20 12:17:22 UTC+0000 \??\C:\Windows\syswow64\MsiExec.exe
2010-11-20 13:25:29 UTC+0000 \??\C:\Windows\system32\WFS.exe
2016-12-09 13:26:47 UTC+0000 \??\C:\Windows\syswow64\WindowsPowerShell\v1.0\PowerShell_ISE.exe
2016-12-09 19:45:10 UTC+0000 \??\C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
2016-12-09 01:35:04 UTC+0000 \??\C:\Windows\SysOW64\WindowsPowerShell\v1.0\powershell.exe
```

14. ¿Qué estaba escrito en el notepad.exe en el momento de la captura de memoria?

```
(kali㉿kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 memdump -p 3032 -D .
Volatility Foundation Volatility Framework 2.6.1
*****
Writing notepad.exe [ 3032] to 3032.dmp

(kali㉿kali)-[~/volatility]
$
```

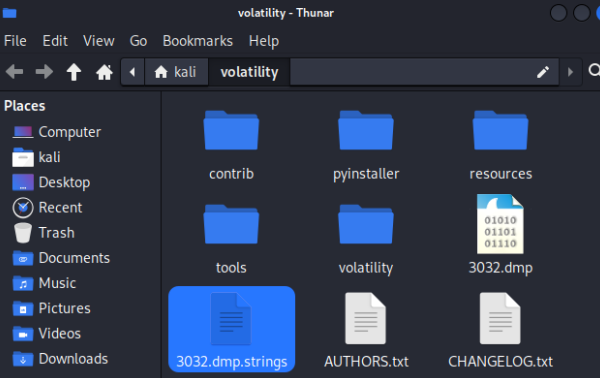
A screenshot of a Thunar file manager window titled 'volatility - Thunar'. The window shows a sidebar with 'Places' including Computer, kali, Desktop, Recent, Trash, Documents, and Music. The main pane displays the contents of the 'volatility' directory, which includes folders 'contrib', 'pyinstaller', 'resources', 'tools', and 'volatility', and a file '3032.dmp' with a binary icon. The file '3032.dmp' is selected and highlighted in blue.

15. ¿Cuál es el nombre corto del archivo en el registro 59045?

```
(kali㉿kali)-[~/volatility]
$ python2.7 vol.py -f Triage-Memory-001.mem --profile=Win7SP1x64 memdump -p 3032 -D .
Volatility Foundation Volatility Framework 2.6.1
*****
Writing notepad.exe [ 3032] to 3032.dmp

(kali㉿kali)-[~/volatility]
$ strings -e l 3032.dmp > 3032.dmp.strings

(kali㉿kali)-[~/volatility]
$
```



16. Este equipo ha sido comprometido y tiene una sesión de meterpreter. ¿Qué PID ha sido infectado?