1 Необходимо определить хэш-сумму файла дампа памяти

Команда ‘`certutil -hashfile C:\Users\briso\volatility3\Workstation.mem SHA256`’

```
C:\Users\briso>certutil -hashfile C:\Users\briso\volatility3\Workstation.mem SHA256
Хэш SHA256 C:\Users\briso\volatility3\Workstation.mem:
a18602964abfbc54e1c83ebdaa61638ff3c2251485e4ad684fc9b59d43dd04a8
CertUtil: -hashfile — команда успешно выполнена.
```

Какая хэш-сумма (SHA-256) у файла Workstation.mem ?

Ответ: хэш сумма файла a18602964abfbc54e1c83ebdaa61638ff3c2251485e4ad684fc9b59d43dd04a8

2 Определить самый подходящий профиль

Команда ‘`python vol.py -f Workstation.mem windows.info`’

```
Variable        Value

Kernel Base     0xf80002808000
DTB     0x187000
Symbols file:///C:/Users/briso/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/2E37F962D699492CAAF3F9F4E9770B1D-2.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdDebuggerDataBlock     0xf800029f80a0
NTBuildLab      7601.18741.amd64fre.win7sp1_gdr.
CSDVersion      1
KdVersionBlock  0xf800029f8068
Major/Minor     15.7601
MachineType     34404
KeNumberProcessors      2
SystemTime      2019-03-22 05:46:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  6
NtMinorVersion  1
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  1
PE Machine      34404
PE TimeDateStamp        Tue Feb  3 02:25:01 2015
```

Какой профиль приложения больше всего подходит для анализа дампа памяти?

‘`NTMajorVersion`’ и ‘`NTMinorVersion`’ указывают на основную и минорную версии операционной системы, которые составляют 6 и 1 соответственно. Это соответствует версии Windows 7 и Windows Server

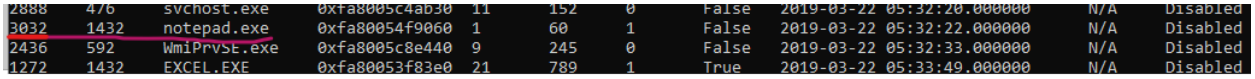
2008 R2. `'Is64Bit True'` указывает, является ли операционная система 64-разрядной.

Ответ: соответственно подходящий профиль - это `'Win7SP1x64'`. Это подтверждает строка

```
'NTBuildLab       7601.18741.amd64fre.win7sp1_gdr.'
```

3 Определить идентификатор процесса

Команда `'python vol.py -f Workstation.mem windows.pslist'`



2888	476	svchost.exe	0xfa8005c4ab30	11	152	0	False	2019-03-22 05:32:20.000000	N/A	Disabled
3032	1432	notepad.exe	0xfa80054f9060	1	60	1	False	2019-03-22 05:32:22.000000	N/A	Disabled
2436	592	WmiPrvSE.exe	0xfa8005c8e440	9	245	0	False	2019-03-22 05:32:33.000000	N/A	Disabled
1272	1432	EXCEL.EXE	0xfa80053f83e0	21	789	1	True	2019-03-22 05:33:49.000000	N/A	Disabled

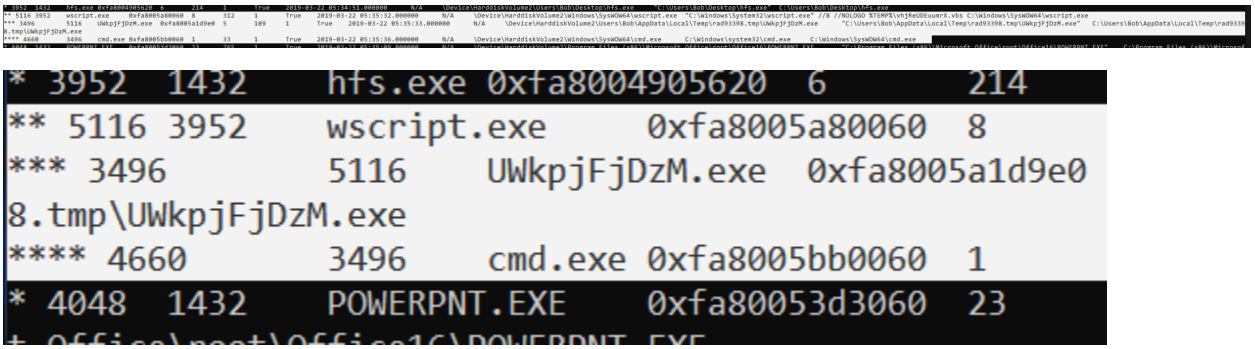
Какой идентификатор был у процесса notepad.exe ?

Ответ: идентификатора процесса (PID) в дампе памяти у процесса notepad.exe - 3032

4 Определить дочерний процесс

Команда `'python vol.py -f Workstation.mem windows.pstree'`

Какой дочерний процесс создан процессом wscript.exe ?

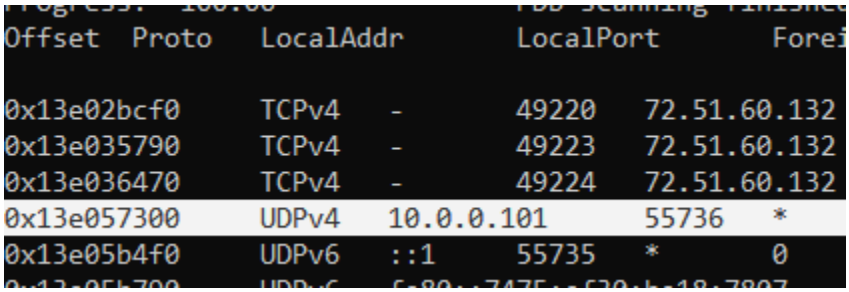


```
* 3952  1432    hfs.exe 0xfa8004905620  6       214
** 5116 3952    wscript.exe     0xfa8005a80060  8
*** 3496        5116    UWkpjFjDzM.exe  0xfa8005a1d9e0
8.tmp\UWkpjFjDzM.exe
**** 4660       3496    cmd.exe 0xfa8005bb0060  1
* 4048  1432    POWERPNT.EXE    0xfa80053d3060  23
```

Ответ: процессом wscript.exe создан дочерний процесс UWkpjFjDzM.exe, далее процессом UWkpjFjDzM.exe был создан дочерний процесс cmd.exe

5 Определить IP-адрес компьютера жертвы

Команда 'python vol.py -f Workstation.mem windows.netscan'



Offset	Proto	LocalAddr	LocalPort	Forei
0x13e02bcf0	TCPv4	-	49220	72.51.60.132
0x13e035790	TCPv4	-	49223	72.51.60.132
0x13e036470	TCPv4	-	49224	72.51.60.132
0x13e057300	UDPv4	10.0.0.101	55736	*
0x13e05b4f0	UDPv6	::1	55735	* 0

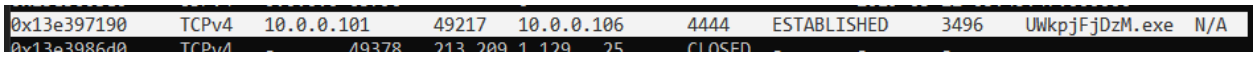
Какой IP-адрес был настроен на рабочей станции во время снятия дамп памяти?

Ответ: эта строка указывает на UDP-соединение с локальным адресом 10.0.0.101, что, вероятно, является IP-адресом компьютера-жертвы.

6 Определить IP-адрес злоумышленника

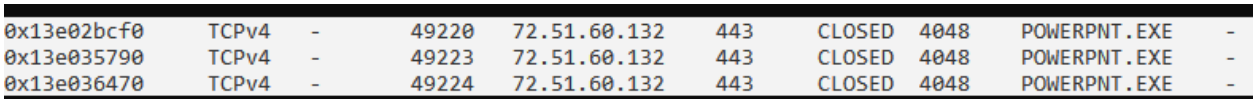
Команда 'python vol.py -f Workstation.mem windows.netscan'

На основе данных об идентификаторе зараженного процесса, можно ли определить IP злоумышленника?



0x13e397190	TCPv4	10.0.0.101	49217	10.0.0.106	4444	ESTABLISHED	3496	UWkpjFjDzM.exe	N/A

Ответ: Процесс с идентификатором PID 3496 (UWkpjFjDzM.exe) устанавливает соединение с IP-адресом 10.0.0.106 на порт 4444(Обратная оболочка Meterpreter). Это может указывать на потенциально подозрительную активность, поскольку процесс устанавливает связь с внешним IP-адресом и использует непривычный порт.



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	-

Также соединение с IP-адресом 72.51.60.132 на порт 443 (HTTP и HTTPS–протоколы web) установлено процессом POWERPNT.EXE (PID

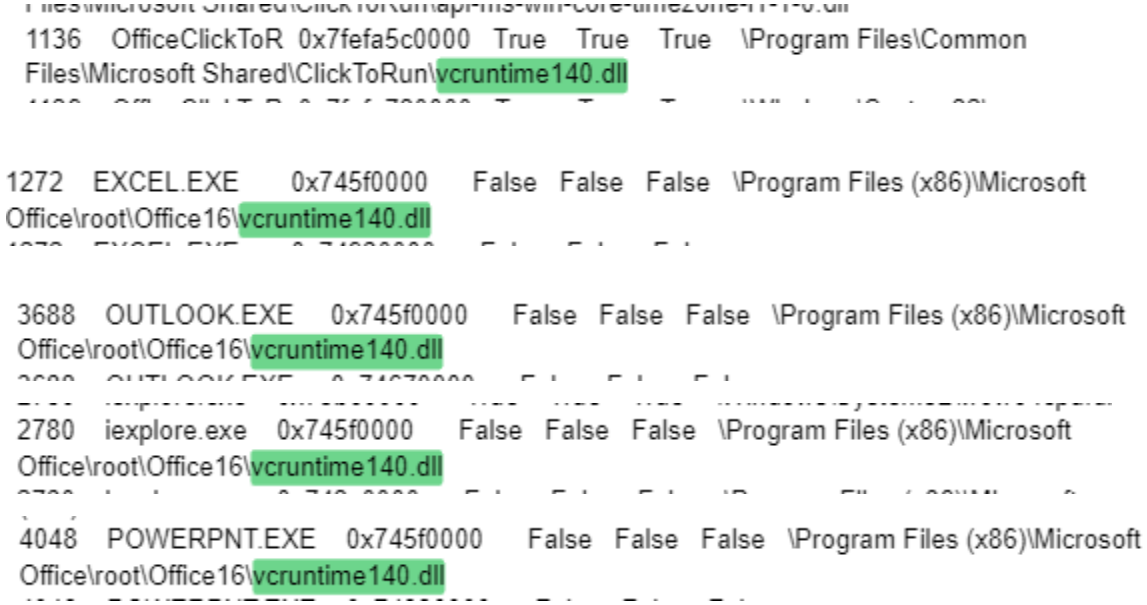
4048), что также может быть потенциально подозрительным, особенно если пользователь не ожидал такой сетевой активности.

7 Построение дерева процессов

Команда ‘`python vol.py -f Workstation.mem ldrmodules`’

С каким количеством процессов есть связь с библиотекой VCRUNTIME140.dll ?

Ответ: 5 процессов



8 Необходимо определить хэш-сумму файла зараженного процесса

Определить какую хэш-сумму (SHA1) имеет дамп зараженного процесса?

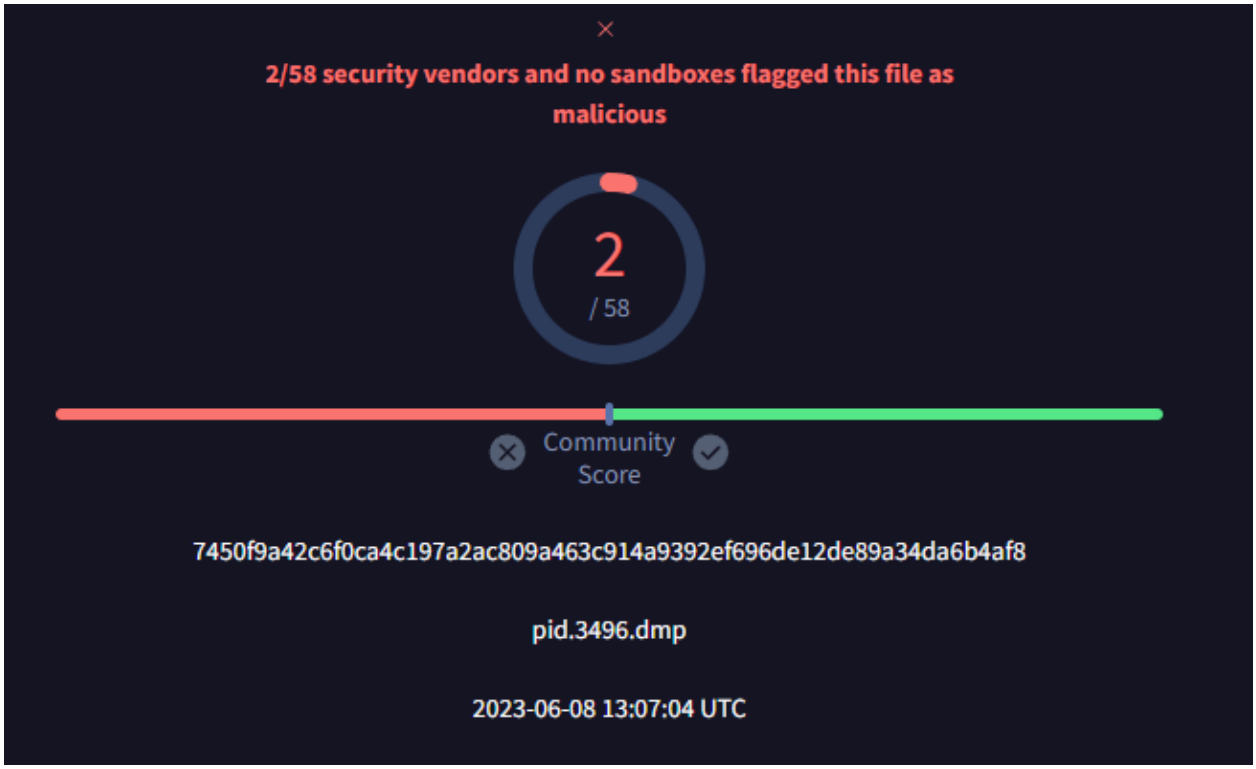
Команда ‘`python vol.py -f Workstation.mem --output-dir=procdump/ windows.memmap --pid 3496 --dump`’ создает файл с процессом под индексом 3496, так как есть подозрения, что этот процесс является зараженным

Команда ‘certutil -hashfile C:\Users\briso\volatility3\procdump\pid.3496.dmp SHA1’

```
C:\Users\briso>certutil -hashfile C:\Users\briso\volatility3\procdump\pid.3496.dmp SHA1
Хэш SHA1 C:\Users\briso\volatility3\procdump\pid.3496.dmp:
f36d4d3136174e9e3e2a80584607ef963b805f77
CertUtil: -hashfile — команда успешно выполнена.
```

Ответ: хэш-сумма f36d4d3136174e9e3e2a80584607ef963b805f77

Проверка файла VirusTotal подтверждает что он вредоносен



9 Определить учетную запись, от которой запустился зараженный процесс

Команда ‘python vol.py -f Workstation.mem cmdline’

На основе данных о заражённом процессе, можно ли узнать учетную запись потенциального злоумышленника?

```
3496   UWkpjFjDzM.exe  "C:\Users\Bob\AppData\Local\Temp\rad93398.tmp\UWkpjFjDzM.exe"
```

Ответ: Нашего хакера зовут Боб

10 Определить хэш учетной записи злоумышленника

Команда ‘‘`python vol.py -f Workstation.mem windows.hashdump`’

Каков LM-хэш учетной записи злоумышленника?

```
C:\Users\briso\volatility3>python vol.py -f Workstation.mem windows.hashdump
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
User    rid     lmhash  nthash

Administrator   500     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Guest   501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Bob     1000    aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
```

Ответ: aad3b435b51404eeaad3b435b51404ee

11 Работа с памятью

Команда ‘`python vol.py -f Workstation.mem vadinfo >> vadinfo.txt`’

Определить константы защиты памяти блока VAD по адресу 0xfffffa800577ba10 ?

```
0xfffffa800577ba10      0x30000 0x33fff Vad     PAGE_READONLY
0xfffffa8005776ea0      0x50000 0x50fff VadS    PAGE_READWRITE
0xfffffa800577cbc0      0x220000        0x286fff        Vad
```

Ответ: PAGE_READONLY

12 Работа с памятью

Команда ‘`python vol.py -f Workstation.mem vadinfo >> vadinfo.txt`’

Определить защиту памяти для блока VAD, со следующей адресацией: начало – 0x00000000033c0000 и конец – 0x00000000033dffff .

```
VAD node @ 0xfffffa80052652b0 Start 0x00000000033c0000 End 0x00000000033dffff Tag VadS
Flags: CommitCharge: 32, PrivateMemory: 1, Protection: 24
Protection: PAGE_NOACCESS
Vad Type: VadNone
```

Ответ: PAGE_NOACCESS

13 Поиск скриптов

Команда 'python vol.py -f Workstation.mem cmdline'

Какое имя имеет VBS скрипт, запущенный на хосте?

```
5116   wscript.exe    "C:\Windows\System32\wscript.exe" //B //NOLOGO
%TEMP%\vhjReUDEuumrX.vbs
```

Ответ: vhjReUDEuumrX.vbs

14 Анализ метаданных

Команда 'python vol.py -f Workstation.mem shimcache >> shimcache.txt'

Приложение было запущено 8 марта 2019 года в 02:06:58 (GMT +3). Как называется программа?

```
2019-03-22 01:21:05 UTC+0000   \??\C:\Users\Bob\Downloads\AccessData_FTK_Imager_3.4.3_x64.exe
2019-03-07 23:06:58 UTC+0000   \??\C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe
```

Ответ: Skype.exe

15 Поиск в блокноте

Команда 'python vol.py -f Workstation.mem memdump --dump-dir C:\ -p 3032'

Что было написано в блокноте в момент снятия дампа памяти? Требуется добраться до флага.

```
x3x
flag<REDBULL_IS_LIFE>
t.wi
```

Ответ: REDBULL_IS_LIFE

16 Работа с главной файловой таблицей

Команда `'python vol.py -f Workstation.mem mftparser >> MFT.txt'`

Определить какой файл расположен по адресу с номером записи 59045?

```
MFT entry found at offset 0x2193d400
Attribute: In Use & File
Record Number: 59045
Link count: 2


$STANDARD_INFORMATION
Creation                       Modified                       MFT Altered                    Access Date                    Type
------------------------------ ------------------------------ ------------------------------ ------------------------------ ----
2019-03-17 06:50:07 UTC+0000 2019-03-17 07:04:43 UTC+0000   2019-03-17 07:04:43 UTC+0000   2019-03-17 07:04:42 UTC+0000   Archive

$FILE_NAME
Creation                       Modified                       MFT Altered                    Access Date                    Name/Path
------------------------------ ------------------------------ ------------------------------ ------------------------------ ---------
2019-03-17 06:50:07 UTC+0000 2019-03-17 07:04:43 UTC+0000   2019-03-17 07:04:43 UTC+0000   2019-03-17 07:04:42 UTC+0000   Users\Bob\DOCUME~1\EMPLOY~1\EMPLOY~1.XLS

$FILE_NAME
Creation                       Modified                       MFT Altered                    Access Date                    Name/Path
------------------------------ ------------------------------ ------------------------------ ------------------------------ ---------
2019-03-17 06:50:07 UTC+0000 2019-03-17 07:04:43 UTC+0000   2019-03-17 07:04:43 UTC+0000   2019-03-17 07:04:42 UTC+0000   Users\Bob\DOCUME~1\EMPLOY~1\EmployeeInformation.xlsx
```

17 Определить идентификатор процесса

Какой идентификатор процесса соответствует meterpreter ?

Ответ: исходя из вопроса 8 PID зараженного процесса 3496