Report on Assignment 3: RAM

Student ID:

Course: Digital Forensics

Date: May 29, 2025

1 INTRODUCTION

Memory forensics plays a vital role in digital investigations by allowing forensic analysts to retrieve critical information from a system's volatile memory. This process helps uncover details about system operations, user activities, and security events that might not be accessible through traditional methods. In this assignment, I will showcase my forensic skills through two key tasks: RAM acquisition and RAM analysis.

For the RAM acquisition task, I will capture a RAM dump from a selected operating system and include a unique artifact to demonstrate my proficiency. This will be accomplished using the WinPMem tool, ensuring an accurate and complete memory capture.

In the RAM analysis task, I will examine a provided RAM dump using Volatility 3, a robust memory forensics tool. This analysis will address specific questions about the system, such as its operating system, active processes, network connections, and user details, highlighting my ability to interpret memory data effectively.

This report offers a straightforward summary of these tasks, the tools employed, and the resulting insights.

2 PERSONAL RAM

For the first task, I acquired and analyzed a RAM dump from a personally controlled system to demonstrate forensic techniques.

I used a **Windows 10 virtual machine** (hosted on VirtualBox, allocated 2GB RAM) as the target.

The dump was captured with **WinPMem (v4.0)** via the command:

```
winpmem_mini_x64.exe -o my_ram_dump.raw
```

After obtaining the RAM dump, we analyzed it using Volatility 3 (v2.5.2) to answer the questions in section 3 of the assignment. Accurate analysis requires downloading and integrating Windows symbol tables into Volatility. The initial step involves running a command to retrieve basic Windows information.

```
python3 vol.py -f ../ram-dump.raw windows.info
```

```
     Kernel Base    0xf80002607000 DTB  0x187000
     Symbols   jar:file:/home/imitxtion/Documents/Digital
Forensics/A4/

     volatility3/volatility3/symbols/windows.zip!windows/ntkrn
lmp.pdb/  3844DBB920174967BE7AA4A2C20430FA-2.json.xz
     Is64Bit        True
     IsPAEFalse
     layer_name0 WindowsIntel32e
     memory_layer        1 FileLayer
     KdDebuggerDataBlock 0xf800027f80a0
     NTBuildLab7601.17514.amd64fre.win7sp1_rtm.
     CSDVersion1
     KdVersionBlock      0xf800027f8068
     Major/Minor    15.7601
     MachineType    34404
     KeNumberProcessors  1
     SystemTime 2025-05-29  13:31:02
     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
```

The next step involved obtaining information about the running processes. That was done by executing a listing and scanning of processes:

```
python3 vol.py -f ../ram-dump.raw windows.pslist.PsList
```

Result:

```
PID   PPID  ImageFileName    Offset(V)       Threads  Handles  SessionId  Wow64  CreateTime                    ExitTime  File

4     0     System           0xfa8000cb8040  68       526      N/A        False  2025-05-29 14:18:39.000000    N/A       Disabled
216   4     smss.exe         0xfa8001c36180  4        29       N/A        False  2025-05-29 14:18:39.000000    N/A       Disabled
288   272   csrss.exe        0xfa8001bc79e0  9        445      0          False  2025-05-29 14:18:39.000000    N/A       Disabled
336   272   wininit.exe      0xfa8000cc28c0  7        86       0          False  2025-05-29 14:18:39.000000    N/A       Disabled
344   328   csrss.exe        0xfa80023b3320  9        399      1          False  2025-05-29 14:18:39.000000    N/A       Disabled
372   328   winlogon.exe     0xfa80023bdb30  6        120      1          False  2025-05-29 14:18:39.000000    N/A       Disabled
428   336   services.exe     0xfa80023f7420  28       237      0          False  2025-05-29 14:18:40.000000    N/A       Disabled
444   336   lsass.exe        0xfa80023fcb30  11       837      0          False  2025-05-29 14:18:40.000000    N/A       Disabled
452   336   lsm.exe          0xfa80023fb060  11       155      0          False  2025-05-29 14:18:40.000000    N/A       Disabled
540   428   svchost.exe      0xfa8002469690  15       360      0          False  2025-05-29 14:18:40.000000    N/A       Disabled
616   428   svchost.exe      0xfa800243c2f0  10       255      0          False  2025-05-29 14:18:40.000000    N/A       Disabled
680   428   svchost.exe      0xfa80024cbb30  26       516      0          False  2025-05-29 14:18:40.000000    N/A       Disabled
748   428   svchost.exe      0xfa80024f5060  29       474      0          False  2025-05-29 14:18:40.000000    N/A       Disabled
780   428   svchost.exe      0xfa80025025f0  52       880      0          False  2025-05-29 14:18:40.000000    N/A       Disabled
868   680   audiodg.exe      0xfa8002541b30  6        127      0          False  2025-05-29 14:18:40.000000    N/A       Disabled
944   428   svchost.exe      0xfa8002568b30  30       446      0          False  2025-05-29 14:18:40.000000    N/A       Disabled
244   428   svchost.exe      0xfa800256d710  21       422      0          False  2025-05-29 14:18:40.000000    N/A       Disabled
276   372   userinit.exe     0xfa80025f9570  0        44       1          False  2025-05-29 14:18:40.000000    N/A       Disabled
1028  748   dwm.exe          0xfa80025fe060  3        73       1          False  2025-05-29 14:18:40.000000    N/A       Disabled
1052  276   explorer.exe     0xfa8002605630  41       966      1          False  2025-05-29 14:18:40.000000    N/A       Disabled
1108  428   spoolsv.exe      0xfa8002649710  6        76       0          False  2025-05-29 14:18:40.000000    N/A       Disabled
1152  428   svchost.exe      0xfa8002664710  23       335      0          False  2025-05-29 14:18:41.000000    N/A       Disabled
1176  428   taskhost.exe     0xfa800266f530  12       182      1          False  2025-05-29 14:18:41.000000    N/A       Disabled
1304  428   svchost.exe      0xfa80026b8b30  23       262      0          False  2025-05-29 14:18:41.000000    N/A       Disabled
2028  1540  opera.exe        0xfa8002900b30  45       991      1          True   2025-05-29 14:18:42.000000    N/A       Disabled
1664  2028  opera_crashrep   0xfa800275bb30  10       126      1          True   2025-05-29 14:18:42.000000    N/A       Disable
696   2028  opera.exe        0xfa8002a4f060  15       242      1          True   2025-05-29 14:18:43.000000    N/A       Disabled
1540  2028  opera.exe        0xfa8002bc5060  8        171      1          True   2025-05-29 14:18:43.000000    N/A       Disabled
2276  2028  opera.exe        0xfa800270e7e0  16       245      1          True   2025-05-29 14:18:44.000000    N/A       Disabled
2536  2028  opera.exe        0xfa80028bc7b0  16       246      1          True   2025-05-29 14:18:45.000000    N/A       Disabled
2596  2028  opera.exe        0xfa800288f060  16       247      1          True   2025-05-29 14:18:45.000000    N/A       Disabled
2656  2028  opera.exe        0xfa80028eab30  16       249      1          True   2025-05-29 14:18:45.000000    N/A       Disabled
2664  2028  opera.exe        0xfa80028ec060  16       247      1          True   2025-05-29 14:18:45.000000    N/A       Disabled
2716  2028  opera.exe        0xfa8002a45b30  16       245      1          True   2025-05-29 14:18:46.000000    N/A       Disabled
2724  2028  opera.exe        0xfa80026b0670  12       203      1          True   2025-05-29 14:18:46.000000    N/A       Disabled
2216  780   taskeng.exe      0xfa80029a6390  6        85       1          False  2025-05-29 14:18:48.000000    N/A       Disabled
```

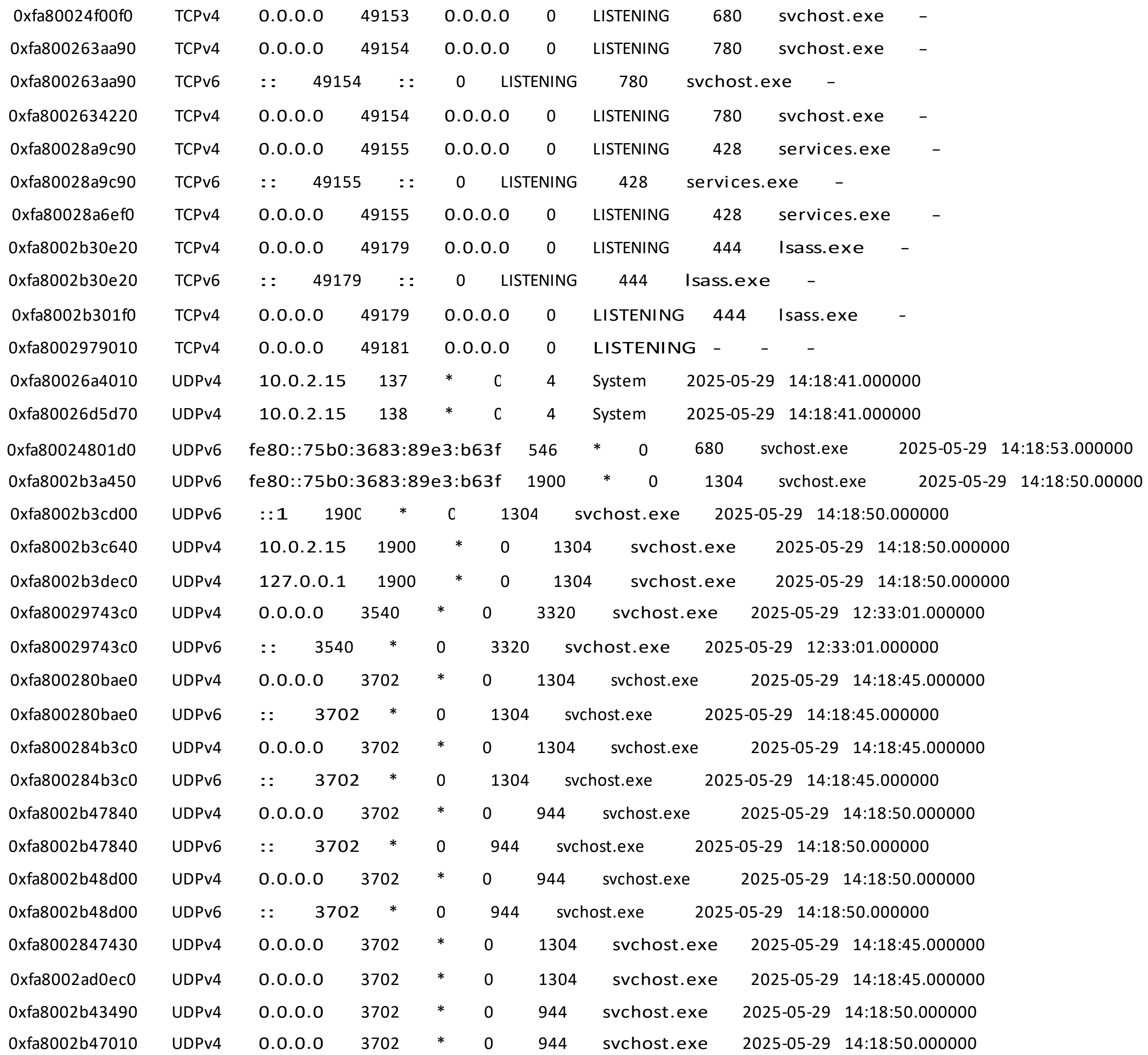
```
python3 vol.py -f ../ram-dump.raw windows.psscan.PsScan

PID   PPID   ImageFileName   Offset(V)   Threads   Handles   SessionId   Wow64   CreateTime   ExitTime   File

4     0      System          0x5d8040    68    526    N/A   False   2025-05-29  14:18:39.000000   N/A   Disabled
336   272    wininit.exe     0x5e28c0    7     86     0     False   2025-05-29  14:18:39.000000   N/A   Disabled
336   272    wininit.exe     0x76c58c0   7     86     0     False   2025-05-29  14:18:39.000000   N/A   Disabled
336   272    wininit.exe     0xc6fe8c0   7     86     0     False   2025-05-29  14:18:39.000000   N/A   Disabled
2716  2028   opera.exe       0x3e045b30  16    245    1     True    2025-05-29  14:18:46.000000   N/A   Disabled
696   2028   opera.exe       0x3e04f060  15    242    1     True    2025-05-29  14:18:43.000000   N/A   Disabled
3060  2484   SearchProtocol  0x3e06b430  8     278    0     False   2025-05-29  14:18:49.000000   N/A   Disabled
2200  540    WmiPrvSE.exe    0x3e092b30  8     188    0     F lse   2025-05-29  14:18:49.000000   N/A   Disabled
3696  1052   cmd.exe         0x3e09b9e0  1     22     1     False   2025-05-29  14:18:51.000000   N/A   Disabled
2260  428    wmpnetwk.exe    0x3e0b23e0  15    225    0     False   2025-05-29  14:18:49.000000   N/A   Disabled
3664  540    dllhost.exe     0x3e0d9540  0     -      0     False   2025-05-29  14:18:51.000000   2025-05-29  14:18:56.0000
3116  2484   SearchFilterHo  0x3e0e3630  5     95     0     False   2025-05-29  14:18:49.000000   N/A   Disabled
3320  428    svchost.exe     0x3e157060  10    341    0     False   2025-05-29  14:18:50.000000   N/A   Disabled
3704  344    conhost.exe     0x3e177b30  2     55     1     False   2025-05-29  14:18:51.000000   N/A   Disabled
1540  2028   opera.exe       0x3e1c5060  8     171    1     True    2025-05-29  14:18:43.000000   N/A   Disabled
2432  2028   opera.exe       0x3e242b30  1     7733353  1   True    2025-05-29  12:33:08.000000   N/A   Disabled
2596  2028   opera.exe       0x3e28f060  16    247    1     True    2025-05-29  14:18:45.000000   N/A   Disabled
2536  2028   opera.exe       0x3e2bc7b0  16    246    1     True    2025-05-29  14:18:45.000000   N/A   Disabled
2656  2028   opera.exe       0x3e2eab30  16    249    1     True    2025-05-29  14:18:45.000000   N/A   Disabled
2664  2028   opera.exe       0x3e2ec060  16    247    1     True    2025-05-29  14:18:45.000000   N/A   Disabled
2028  1540   opera.exe       0x3e300b30  45    991    1     True    2025-05-29  14:18:42.000000   N/A   Disabled
2216  780    taskeng.exe     0x3e3a6390  6     85     1     False   2025-05-29  14:18:48.000000   N/A   Disabled
3984  2028   opera.exe       0x3e3ae3c0  12    109    1     True    2025-05-29  12:33:07.000000   N/A   Disabled
2484  428    SearchIndexer.  0x3e3df800  13    583    0     False   2025-05-29  14:18:49.000000   N/A   Disabled
1052  276    explorer.exe    0x3e405630  41    966    1     False   2025-05-29  14:18:40.000000   N/A   Disabled
```

Same thing we can do to get network information, by executing a listing and scanning of networks:

```
python3 vol.py -f ../ram-dump.raw windows.netstat.NetStat
```



```
0xfa80024f00f0   TCPv4   0.0.0.0   49153   0.0.0.0   0   LISTENING   680   svchost.exe   -
0xfa800263aa90   TCPv4   0.0.0.0   49154   0.0.0.0   0   LISTENING   780   svchost.exe   -
0xfa800263aa90   TCPv6   ::   49154   ::   0   LISTENING   780   svchost.exe   -
0xfa8002634220   TCPv4   0.0.0.0   49154   0.0.0.0   0   LISTENING   780   svchost.exe   -
0xfa80028a9c90   TCPv4   0.0.0.0   49155   0.0.0.0   0   LISTENING   428   services.exe   -
0xfa80028a9c90   TCPv6   ::   49155   ::   0   LISTENING   428   services.exe   -
0xfa80028a6ef0   TCPv4   0.0.0.0   49155   0.0.0.0   0   LISTENING   428   services.exe   -
0xfa8002b30e20   TCPv4   0.0.0.0   49179   0.0.0.0   0   LISTENING   444   lsass.exe   -
0xfa8002b30e20   TCPv6   ::   49179   ::   0   LISTENING   444   lsass.exe   -
0xfa8002b301f0   TCPv4   0.0.0.0   49179   0.0.0.0   0   LISTENING   444   lsass.exe   -
0xfa8002979010   TCPv4   0.0.0.0   49181   0.0.0.0   0   LISTENING  -   -   -
0xfa80026a4010   UDPv4   10.0.2.15   137   *   C   4   System   2025-05-29  14:18:41.000000
0xfa80026d5d70   UDPv4   10.0.2.15   138   *   C   4   System   2025-05-29  14:18:41.000000
0xfa80024801d0   UDPv6   fe80::75b0:3683:89e3:b63f   546   *   0   680   svchost.exe   2025-05-29  14:18:53.000000
0xfa8002b3a450   UDPv6   fe80::75b0:3683:89e3:b63f   1900   *   0   1304   svchost.exe   2025-05-29  14:18:50.00000
0xfa8002b3cd00   UDPv6   ::1   190C   *   C   1304   svchost.exe   2025-05-29  14:18:50.000000
0xfa8002b3c640   UDPv4   10.0.2.15   1900   *   0   1304   svchost.exe   2025-05-29  14:18:50.000000
0xfa8002b3dec0   UDPv4   127.0.0.1   1900   *   0   1304   svchost.exe   2025-05-29  14:18:50.000000
0xfa80029743c0   UDPv4   0.0.0.0   3540   *   0   3320   svchost.exe   2025-05-29  12:33:01.000000
0xfa80029743c0   UDPv6   ::   3540   *   0   3320   svchost.exe   2025-05-29  12:33:01.000000
0xfa800280bae0   UDPv4   0.0.0.0   3702   *   0   1304   svchost.exe   2025-05-29  14:18:45.000000
0xfa800280bae0   UDPv6   ::   3702   *   0   1304   svchost.exe   2025-05-29  14:18:45.000000
0xfa800284b3c0   UDPv4   0.0.0.0   3702   *   0   1304   svchost.exe   2025-05-29  14:18:45.000000
0xfa800284b3c0   UDPv6   ::   3702   *   0   1304   svchost.exe   2025-05-29  14:18:45.000000
0xfa8002b47840   UDPv4   0.0.0.0   3702   *   0   944   svchost.exe   2025-05-29  14:18:50.000000
0xfa8002b47840   UDPv6   ::   3702   *   0   944   svchost.exe   2025-05-29  14:18:50.000000
0xfa8002b48d00   UDPv4   0.0.0.0   3702   *   0   944   svchost.exe   2025-05-29  14:18:50.000000
0xfa8002b48d00   UDPv6   ::   3702   *   0   944   svchost.exe   2025-05-29  14:18:50.000000
0xfa8002847430   UDPv4   0.0.0.0   3702   *   0   1304   svchost.exe   2025-05-29  14:18:45.000000
0xfa8002ad0ec0   UDPv4   0.0.0.0   3702   *   0   1304   svchost.exe   2025-05-29  14:18:45.000000
0xfa8002b43490   UDPv4   0.0.0.0   3702   *   0   944   svchost.exe   2025-05-29  14:18:50.000000
0xfa8002b47010   UDPv4   0.0.0.0   3702   *   0   944   svchost.exe   2025-05-29  14:18:50.000000
```

```
python3 vol.py -f ../ram-dump.raw windows.netscan.NetScan
```

```
0x3e2a9c90   TCPv6    ::      49155    ::      0     LISTENING    428     services.exe     -
0x3e2b0bb0   UDPv4    0.0.0.0      61038     *     0      1304     svchost.exe      2025-05-29  14:18:41.000000
0x3e2b0bb0   UDPv6    ::      61038     *     0      1304     svchost.exe      2025-05-29  14:18:41.000000
0x3e2e68a0   UDPv4    0.0.0.0     52662     *     0      696     opera.exe      2025-05-29  14:18:45.000000
0x3e364220   TCPv4    10.0.2.15     49181    142.251.5.188     5228    ESTABLISHED     696     opera.exe     N/A
0x3e3743c0   UDPv4    0.0.0.0     3540     *     0      3320     svchost.exe      2025-05-29  12:33:01.000000
0x3e3743c0   UDPv6    ::     3 40     *     0      3320     svchost.exe      2025-05-29  12:33:01.000000
0x3e37acf0   TCPv6    -     0     38cb:3f02:80fa:ffff:a070:780 2:80fa:ffff          0     CLOSED     696     opera.exe     N/A
0x3e3e06c0   TCPv4    10.0.2.15     49178     82.145.216.16      443     CLOSED     696     opera.exe      -
0x3e400590   TCPv4    10.0.2.15     139     0.0.0.0     0     LISTENING    4     System    -
0x3e434220   TCPv4    0.0.0.0     49154     0.0.0.0     0     LISTENING     780     svchost.exe      -
0x3e43aa90   TCPv4    0.0.0.0     49154     0.0.0.0     0     LISTENING     780     svchost.exe      -
0x3e43aa90   TCPv6    ::      49154     ::     0     LISTENING     780     svchost.exe   -
0x3e4a4010   UDPv4    10.0.2.15     137     *     0      4     System      2025-05-29  14:18:41.000000
0x3e4d5d70   UDPv4    10.0.2.15     138     *     0      4     System      2025-05-29  14:18:41.000000
0x3e4f8df0   TCPv4    0.0.0.0     5357     0.0.0.0     0     LISTENING     4     System      -
0x3e4f8df0   TCPv6    ::      5357     ::     0     LISTENING     4     System      -
0x3e590ec0   UDPv4    0.0.0.0      0     *     0      244     svchost.exe      2025-05-29  14:18:42.000000
0x3e590ec0   UDPv6    ::     0     *     0      244     svchost.exe     2025-05-29  14:18:42.000000
0x3e6801d0   UDPv6    fe80::75b0:3683:89e3:b63f       546     *     0      680     svchost.exe      2025-05-29  14:18:53.000000
0x3e6a5920   TCPv4    0.0.0.0     135     0.0.0.0     0     LISTENING     616     svchost.exe      -
```

3 PROVIDED RAM

To begin the second part of the assignment, download the provided RAM dump. Subsequently, compute its hash to ensure it corresponds with the value given in the assignment.

```
sha256sum physmem.raw > mem-hash.txt cat mem-hash.txt

fee4a87527509ed8a67c51a2b3e21a74ae52739e0d69020312180339c
```

Following our procedure from the previous RAM dump, we will now analyze the operating system details by executing the command below. The successful operation of the Volatility plugin indicates that the RAM originated from a Windows system. Additionally, the output provides the system's timestamp at the time of the RAM dump's creation.

```
python3 vol.py -f ../physmem.raw windows.info
```

```
Volatility 3 Framework 2.5.2
Progress:         100.00 PDB scanning finished Variable Value

Kernel Base 0xf80420a00000 DTB 0x1ae000
Symbols file:///home/imitxtion/Documents/Digital%20Forensics/A4/volatility3/volatili

Is64Bit True
 IsPAE False
layer_name 0 WindowsIntel32e
memory_layer 1 FileLayer
 KdVersionBlock 0xf804216099a0 Major/Minor 15.22621
MachineType 34404
KeNumberProcessors 2
SystemTime 2023-01-09 22:17:11
NtSystemRoot C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion  0
PE  MajorOperatingSystemVersion  10
PE  MinorOperatingSystemVersion  0
PE Machine 34404
PE TimeDateStamp Mon Jul  5  20:20:35  2100
```

Next, we can search for processes and networks active at the time by employing the scanning commands utilized in the previous RAM dump.

```
python3 vol.py -f ../physmem.raw windows.psscan.PsScan
```

```
PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime File output
88 4 Registry 0x9f0f23ede080 4 -N/A False 2023-01-09 21:47:12.000000 N/A Disabled
1936 772 svchost.exe 0x9f0f23f0f080 3 -0 False 2023-01-09 21:47:16.000000 N/A Disabled
2036 772 svchost.exe 0x9f0f23f2b080 2 -0 False 2023-01-09 21:47:16.000000 N/A Disabled
1856 772 svchost.exe 0x9f0f23f36080 7 -0 False 2023-01-09 21:47:16.000000 N/A Disabled
2020 4 MemCompression 0x9f0f23f6f040 18 -N/A False 2023-01-09 21:47:16.000000 N/A Disabled

1784 772 VBoxService.ex 0x9f0f23f7e080 10 -0 False 2023-01-09 21:47:16.000000 N/A Disabled
1752 772 svchost.exe 0x9f0f23fa4080 9 -0 False 2023-01-09 21:47:16.000000 N/A Disabled
1924 772 svchost.exe 0x9f0f23fca080 5 -0 False 2023-01-09 21:47:16.000000 N/A Disabled
1916 772 svchost.exe 0x9f0f23fcc080 4 -0 False 2023-01-09 21:47:16.000000 N/A Disabled
9176 772 svchost.exe 0x9f0f247c9080 7 -0 False 2023-01-09 21:49:19.000000 N/A Disabled
384 4 smss.exe 0x9f0f24a75040 2 -N/A False 2023-01-09 21:47:13.000000 N/A Disabled
5796 772 svchost.exe 0x9f0f24bd40c0 10 -0 False 2023-01-09 22:07:48.000000 N/A Disabled
7652 7300 firefox.exe 0x9f0f24c460c0 0 -1 False 2023-01-09 21:49:49.000000 2023-01-09 21:49:49.000000 Disabled
11220 7300 firefox.exe 0x9f0f24cc80c0 12 -1 False 2023-01-09 21:50:47.000000 N/A Disabled
472 7300 firefox.exe 0x9f0f275e6080 16 -1 False 2023-01-09 21:49:50.000000 N/A Disabled
9980 7300 firefox.exe 0x9f0f275ed080 12 -1 False 2023-01-09 21:50:40.000000 N/A Disabled
672 7252 firefox.exe 0x9f0f276400c0 15 -1 False 2023-01-09 21:48:47.000000 N/A Disabled
1348 908 ApplicationFra 0x9f0f276d50c0 2 -1 False 2023-01-09 21:54:11.000000 N/A Disabled
3640 7300 firefox.exe 0x9f0f276da080 16 -1 False 2023-01-09 21:49:48.000000 N/A Disabled
6472 7300 firefox.exe 0x9f0f276e60c0 16 -1 False 2023-01-09 21:50:04.000000 N/A Disabled
10188 7252 firefox.exe 0x9f0f2777a0c0 15 -1 False 2023-01-09 21:48:47.000000 N/A Disabled
7780 7252 firefox.exe 0x9f0f27787080 18 -1 False 2023-01-09 21:53:37.000000 N/A Disabled
576 508 csrss.exe 0x9f0f27977140 10 -0 False 2023-01-09 21:47:15.000000 N/A Disabled
644 508 wininit.exe 0x9f0f27b13080 2 -0 False 2023-01-09 21:47:15.000000 N/A Disabled
424 772 svchost.exe 0x9f0f27b1b140 12 -0 False 2023-01-09 21:47:16.000000 N/A Disabled
652 636 csrss.exe 0x9f0f27b1d140 14 -1 False 2023-01-09 21:47:15.000000 N/A Disabled
296 772 svchost.exe 0x9f0f27b49080 2 -0 False 2023-01-09 21:47:16.000000 N/A Disabled
736 636 winlogon.exe 0x9f0f27b81080 7 -1 False 2023-01-09 21:47:15.000000 N/A Disabled
```

```
772 644 services.exe 0x9f0f27b8d080 9 -0 False 2023-01-09 21:47:15.000000  N/A Disabled
804 644 lsass.exe 0x9f0f27ba3080 11 -0 False 2023-01-09 21:47:15.000000  N/A Disabled
2708 7252 firefox.exe 0x9f0f27bef0c0 15 -1 False 2023-01-09 22:15:01.000000  N/A Disabled
536 772 svchost.exe 0x9f0f27c31080 5 -0 False 2023-01-09 21:47:16.000000  N/A Disabled
8348 7252 firefox.exe 0x9f0f27c8a080 15 -1 False 2023-01-09 21:48:24.000000  N/A Disabled
852 736 LogonUI.exe 0x9f0f27caf080 0 -1 False 2023-01-09 21:47:16.000000  2023-01-09
21:47:33.000000  Disabled
920 736 dwm.exe 0x9f0f27cb1080 16 -1 False 2023-01-09 21:47:16.000000  N/A Disabled
1088 772 svchost.exe 0x9f0f27ccf0c0 9 -0 False 2023-01-09 21:47:16.000000  N/A Disabled
1100 772 svchost.exe 0x9f0f27cdb080 2 -0 False 2023-01-09 21:47:16.000000  N/A Disabled
908 772 svchost.exe 0x9f0f27d33080 23 -0 False 2023-01-09 21:47:16.000000  N/A Disabled
924 644 fontdrvhost.ex 0x9f0f27d56140 5 -0 False 2023-01-09 21:47:16.000000  N/A Disabled
932 736 fontdrvhost.ex 0x9f0f27d58140 5 -1 False 2023-01-09 21:47:16.000000  N/A Disabled
6584 10640 msedgewebview2 0x9f0f27dc50c0 7 -1 False 2023-01-09 22:03:17.000000 N/A
Disabled
1208 772 svchost.exe 0x9f0f27e30080 5 -0 False 2023-01-09 21:47:16.000000  N/A Disabled
1252 772 svchost.exe 0x9f0f27e43080 1 -0 False 2023-01-09 21:47:16.000000  N/A Disabled
1452 772 svchost.exe 0x9f0f27e9b0c0 5 -0 False 2023-01-09 21:47:16.000000  N/A Disabled
1300 772 svchost.exe 0x9f0f27eaa080 3 -0 False 2023-01-09 21:47:16.000000  N/A Disabled
1324 772 svchost.exe 0x9f0f27f07080 13 -0 False 2023-01-09 21:47:16.000000  N/A Disabled
2180    7252  firefox.exe  0x9f0f2934b080  11  -1  False  2023-01-09  21:53:42.000000    N/A
Disabled
2464    772     svchost.exe     0x9f0f293560c0      4       -0      False   2023-01-09
21:47:17.000000         N/A     Disabled
2484    772     spoolsv.exe     0x9f0f293670c0      7       -0      False   2023-01-09
21:47:17.000000         N/A     Disabled
2604 772 svchost.exe 0x9f0f293d3080 13 -0 False 2023-01-09 21:47:17.000000  N/A Disabled
2636    772     svchost.exe     0x9f0f293f10803     -0      False   2023-01-09
21:47:17.000000         N/A     Disabled
1484    772     svchost.exe     0x9f0f29430080      8       -0      False   2023-01-09
21:47:16.000000         N/A     Disabled
1420    772     svchost.exe     0x9f0f294ed080      4       -0      False   2023-01-09
21:47:16.000000         N/A     Disabled
2784    772     svchost.exe     0x9f0f29574080      3       -0      False   2023-01-09
21:47:17.000000         N/A     Disabled
2900 772 svchost.exe 0x9f0f295cc0c0 10 -0 False 2023-01-09 21:47:17.000000  N/A Disabled
2908 772 svchost.exe 0x9f0f295cd080 14 -0 False 2023-01-09 21:47:17.000000  N/A Disabled
```

```
2916	772	svchost.exe	0x9f0f295d1080		5	-0	False	2023-01-09
21:47:17.000000		N/A	Disabled
2980	772	svchost.exe	0x9f0f295da080		5	-0	False	2023-01-09
21:47:17.000000		N/A	Disabled
2992	772	svchost.exe	0x9f0f295e6080		3	-0	False	2023-01-09
21:47:17.000000		N/A	Disabled
3016 772 svchost.exe 0x9f0f295f6080 10 -0 False 2023-01-09 21:47:17.000000  N/A Disabled
3032 772 svchost.exe 0x9f0f295fc080 7 -0 False 2023-01-09 21:47:17.000000  N/A Disabled
3836 772 svchost.exe 0x9f0f2985c080 0 -0 False 2023-01-09 21:47:36.000000  2023-01-09
21:50:43.000000  Disabled
9988 7252 firefox.exe 0x9f0f2992d0c0 14 -1 False 2023-01-09 21:48:45.000000  N/A Disabled
3652 7300 firefox.exe 0x9f0f29969080 16 -1 False 2023-01-09 21:49:50.000000  N/A Disabled
2140 772 svchost.exe 0x9f0f2996a080 8 -0 False 2023-01-09 21:49:19.000000  N/A Disabled
4800  4108  msedge.exe  0x9f0f29975080  31  -1  False  2023-01-09  21:47:37.000000   N/A
Disabled
6212 4800 msedge.exe 0x9f0f29976080 7 -1 False 2023-01-09 21:47:37.000000  N/A Disabled
5540 7300 firefox.exe 0x9f0f29b860c0 20 -1 False 2023-01-09 21:49:48.000000  N/A Disabled
9916 7252 firefox.exe 0x9f0f29b970c0 15 -1 False 2023-01-09 21:48:45.000000  N/A Disabled
11212  7300  firefox.exe  0x9f0f29b98080  15  -1  False  2023-01-09  21:50:31.000000   N/A
Disabled

2660    7252  firefox.exe  0x9f0f29ba9080  15  -1  False  2023-01-09  21:48:32.000000   N/A
Disabled
5288    4800  msedge.exe  0x9f0f29bb90c0  10  -1  False  2023-01-09  21:47:38.000000   N/A
Disabled
7412    908 RuntimeBroker. 0x9f0f29bba080  1  -1  False  2023-01-09  21:47:39.000000   N/A
Disabled

5260  4800  msedge.exe  0x9f0f29bca0c0  13  -1  False  2023-01-09  21:47:38.000000   N/A
Disabled
9112 7252 firefox.exe 0x9f0f29bdc080 19 -1 False 2023-01-09 21:47:45.000000  N/A Disabled
10640 4684 msedgewebview2 0x9f0f29bdf080 25 -1 False 2023-01-09 22:03:17.000000 N/A
Disabled

9196    7252 firefox.exe 0x9f0f29c96080 15 -1 False 2023-01-09 21:47:45.000000         N/A
Disabled
```

```
        9160    7252 firefox.exe 0x9f0f29cb8080 16 -1 False 2023-01-09 21:47:45.000000      N/A
Disabled
        5192    7252 firefox.exe 0x9f0f29cbe0c0 15 -1 False 2023-01-09 21:48:29.000000      N/A
Disabled
        7492    7324    msedgewebview2  0x9f0f2b4db080  33  -1  False  2023-01-09  21:47:40.000000
N/A Disabled
        7508    7492    msedgewebview2  0x9f0f2b4f2080  7  -1  False  2023-01-09  21:47:40.000000
N/A Disabled
        7636    772  svchost.exe  0x9f0f2b4f7080  12  -0  False  2023-01-09  21:47:40.000000   N/A
Disabled
        3004    10640 msedgewebview2  0x9f0f2b86e080  11  -1  False  2023-01-09  22:03:17.000000
N/A Disabled
        7816    7492 msedgewebview2 0x9f0f2b891080 7 -1 False 2023-01-09 21:47:40.000000 N/A
Disabled
        7788    7492 msedgewebview2 0x9f0f2b892080 12 -1 False 2023-01-09 21:47:40.000000 N/A
Disabled
        7800    7492 msedgewebview2 0x9f0f2b893080 10 -1 False 2023-01-09 21:47:40.000000 N/A
Disabled
        7920    7492 msedgewebview2 0x9f0f2b9020c0 14 -1 False 2023-01-09 21:47:40.000000 N/A
Disabled
        8108    908 dllhost.exe 0x9f0f2ba130c0 3 -1 False 2023-01-09 21:47:41.000000  N/A Disabled
        8244    7252  firefox.exe  0x9f0f2ba450c0  5  -1  False  2023-01-09  21:47:42.000000   N/A
Disabled
        7252    7528  firefox.exe  0x9f0f2ba560c0  64  -1  False  2023-01-09  21:47:41.000000   N/A
Disabled

        9476    7252    firefox.exe     0x9f0f2bb8b080      15      -1      False   2023-01-09
        21:48:40.000000         N/A     Disabled
        9456    7252    firefox.exe     0x9f0f2bb8c080      15      -1      False   2023-01-09
        21:48:40.000000         N/A     Disabled
        9420    7252    firefox.exe     0x9f0f2bb8d080      15      -1      False   2023-01-09
        21:48:39.000000         N/A     Disabled
        6888    7252    firefox.exe     0x9f0f2bb8e080      15      -1      False   2023-01-09
        21:48:38.000000         N/A     Disabled
        3028    7252    firefox.exe     0x9f0f2bb8f08015    -1      False   2023-01-09
        21:48:38.000000         N/A     Disabled
```

python3 vol.py -f ../physmem.raw windows.netscan.NetScan

```
Volatility 3 Framework 2.5.2
Progress:  100.00 PDB scanning finished
Offset Proto LocalAddr LocalPort ForeignAddr ForeignPort State PID Owner Created
0x9f0f23e83650 TCPv4 0.0.0.0 49668 0.0.0.0 0 LISTENING 2484 spoolsv.exe 2023-01-09 21:47:17.000000
0x9f0f23e837b0 TCPv4 0.0.0.0 49668 0.0.0.0 0 LISTENING 2484 spoolsv.exe 2023-01-09 21:47:17.000000
0x9f0f23e837b0 TCPv6 :: 49668 :: 0 LISTENING 2484 spoolsv.exe 2023-01-09 21:47:17.000000
0x9f0f24a7de10 TCPv4 0.0.0.0 49664 0.0.0.0 0 LISTENING 804 lsass.exe 2023-01-09 21:47:16.000000
0x9f0f24a7de10 TCPv6 :: 49664 :: 0 LISTENING 804 lsass.exe 2023-01-09 21:47:16.000000
0x9f0f273371c0 TCPv4 0.0.0.0 49669 0.0.0.0 0 LISTENING 772 services.exe 2023-01-09 21:47:18.000000
0x9f0f273371c0 TCPv6 :: 49669 :: 0 LISTENING 772 services.exe 2023-01-09 21:47:18.000000
0x9f0f27337320 TCPv4 0.0.0.0 5040 0.0.0.0 0 LISTENING 3324 svchost.exe 2023-01-09 21:47:21.000000


0x9f0f273378a0 TCPv4 0.0.0.0 7680 0.0.0.0 0 LISTENING 2344 svchost.exe 2023-01-09 21:49:51.000000
0x9f0f273378a0 TCPv6 :: 7680 :: 0 LISTENING 2344 svchost.exe 2023-01-09 21:49:51.000000
0x9f0f27337e20 TCPv4 0.0.0.0 445 0.0.0.0 0 LISTENING 4 System 2023-01-09 21:47:18.000000
0x9f0f27337e20 TCPv6 :: 445 :: 0 LISTENING 4 System 2023-01-09 21:47:18.000000
0x9f0f27338240 TCPv4 127.0.0.1 9151 0.0.0.0 0 LISTENING 3108 tor.exe 2023-01-09 21:49:51.000000
0x9f0f27339420 TCPv4 0.0.0.0 49669 0.0.0.0 0 LISTENING 772 services.exe 2023-01-09 21:47:18.000000
```

```
0x9f0f27339580 TCPv4 127.0.0.1 9150 0.0.0.0 0 LISTENING 3108 tor.exe 2023-01-09 21:49:54.000000
0x9f0f2734cb50 TCPv4 0.0.0.0 49667 0.0.0.0 0 LISTENING 1856 svchost.exe 2023-01-09 21:47:16.000000
0x9f0f2734ccb0TCPv4 0.0.0.0 49667 0.0.0.0 0 LISTENING 1856 svchost.exe 2023-01-09 21:47:16.000000
0x9f0f2734ccb0TCPv6 :: 49667 :: 0 LISTENING 1856 svchost.exe 2023-01-09 21:47:16.000000
0x9f0f2734d230 TCPv4 10.0.2.15 139 0.0.0.0 0 LISTENING 4 System 2023-01-09 21:47:17.000000
0x9f0f2734d7b0 TCPv4 0.0.0.0 49666 0.0.0.0 0 LISTENING 1324 svchost.exe 2023-01-09 21:47:16.000000
0x9f0f2734dbd0 TCPv4 0.0.0.0 49666 0.0.0.0 0 LISTENING 1324 svchost.exe 2023-01-09 21:47:16.000000
0x9f0f2734dbd0 TCPv6 :: 49666 :: 0 LISTENING 1324 svchost.exe 2023-01-09 21:47:16.000000
0x9f0f278241b0 TCPv4 0.0.0.0 49664 0.0.0.0 0 LISTENING 804 lsass.exe 2023-01-09 21:47:16.000000
0x9f0f27824310 TCPv4 0.0.0.0 135 0.0.0.0 0 LISTENING 424 svchost.exe 2023-01-09 21:47:16.000000
0x9f0f27824310 TCPv6 :: 135 :: 0 LISTENING 424 svchost.exe 2023-01-09 21:47:16.000000
0x9f0f27824470 TCPv4 0.0.0.0 49665 0.0.0.0 0 LISTENING 644 wininit.exe 2023-01-09 21:47:16.000000
0x9f0f27824470 TCPv6 :: 49665 :: 0 LISTENING 644 wininit.exe 2023-01-09 21:47:16.000000
0x9f0f278249f0TCPv4 0.0.0.0 49665 0.0.0.0 0 LISTENING 644 wininit.exe 2023-01-09 21:47:16.000000
0x9f0f27825d30 TCPv4 0.0.0.0 135 0.0.0.0 0 LISTENING 424 svchost.exe 2023-01-09 21:47:16.000000
0x9f0f28009c50 UDPv4 0.0.0.0 5353 * 0 1752 svchost.exe 2023-01-09 21:47:19.000000
0x9f0f28009c50 UDPv6 :: 5353 * 0 1752 svchost.exe 2023-01-09 21:47:19.000000
0x9f0f28016130 UDPv4 0.0.0.0 5353 * 0 1752 svchost.exe 2023-01-09 21:47:19.000000
0x9f0f28166c10 UDPv4 127.0.0.1 53655 * 0 2916 svchost.exe 2023-01-09 21:47:18.000000
```

```
        0x9f0f2829dd40          UDPv4 0.0.0.0 0 * 0 1752 svchost.exe 2023-01-09 21:47:19.000000
        0x9f0f2829dd40          UDPv6 :: 0 * 0 1752 svchost.exe 2023-01-09 21:47:19.000000
        0x9f0f284df760UDPv4 0.0.0.0 5050 * 0 3324 svchost.exe 2023-01-09 21:47:20.000000
        0x9f0f284e5cf0 UDPv4 0.0.0.0 59690 * 0 1752 svchost.exe 2023-01-09 21:47:21.000000
        0x9f0f284e5cf0 UDPv6 :: 59690 * 0 1752 svchost.exe 2023-01-09 21:47:21.000000
        0x9f0f291788f0UDPv4 10.0.2.15 138 * 0 4 System 2023-01-09 21:47:17.000000
        0x9f0f29311a90UDPv4 10.0.2.15 137 * 0 4 System 2023-01-09 21:47:17.000000
        0x9f0f2955e240          UDPv4 0.0.0.0    5355    *    0    1752    svchost.exe    2023-01-09
21:47:19.000000
        0x9f0f2955e240          UDPv6 :: 5355 * 0 1752 svchost.exe 2023-01-09 21:47:19.000000
        0x9f0f29563830          UDPv4 0.0.0.0    5355    *    0    1752    svchost.exe    2023-01-09
21:47:19.000000
        0x9f0f2b23cc80UDPv4 0.0.0.0 53033 * 0 1752 svchost.exe 2023-01-09 21:47:36.000000
        0x9f0f2b23cc80UDPv6 :: 53033 * 0 1752 svchost.exe 2023-01-09 21:47:36.000000
        0x9f0f2b537500          UDPv4 0.0.0.0    5353    *    0    4800    msedge.exe    2023-01-09
21:47:39.000000
        0x9f0f2b5384a0          UDPv4 0.0.0.0    5353    *    0    4800    msedge.exe    2023-01-09
21:47:39.000000
        0x9f0f2b5384a0          UDPv6 :: 5353 * 0 4800 msedge.exe 2023-01-09 21:47:39.000000
        0x9f0f2bbbcc80UDPv4 0.0.0.0 58509 * 0 1752 svchost.exe 2023-01-09 21:47:45.000000


        0x9f0f2bbbcc80UDPv6 :: 58509 * 0 1752 svchost.exe 2023-01-09 21:47:45.000000
        0x9f0f2bbc3080          UDPv4 0.0.0.0    65042    *    0    1752    svchost.exe    2023-01-09
21:47:45.000000
        0x9f0f2bbc3080          UDPv6 :: 65042 * 0 1752 svchost.exe 2023-01-09 21:47:45.000000
        0x9f0f2bbc44d0          UDPv4 10.0.2.15    65045    *    0    9096    svchost.exe    2023-01-09
21:47:45.000000
        0x9f0f2bbc5470          UDPv6 fe80::f1d:55a8:b3a0:2131 65043 * 0 9096 svchost.exe 2023-
01-09 21:47:45.000000
        0x9f0f2bbc5920          UDPv4 127.0.0.1    1900    *    0    9096    svchost.exe    2023-01-09
21:47:45.000000
        0x9f0f2bbc5c40UDPv4 127.0.0.1 65046 * 0 9096 svchost.exe 2023-01-09 21:47:45.000000
        0x9f0f2bbc60f0 UDPv6 ::1 65044 * 0 9096 svchost.exe 2023-01-09 21:47:45.000000
        0x9f0f2bbc6280          UDPv4 10.0.2.15    1900    *    0    9096    svchost.exe    2023-01-09
21:47:45.000000
        0x9f0f2bbc6730          UDPv6 ::1 1900 * 0 9096 svchost.exe 2023-01-09 21:47:45.000000
```

```
0x9f0f2bbc6a50UDPv6 fe80::f1d:55a8:b3a0:2131 1900 * 0 9096 svchost.exe 2023-01-09 21:47:45.000000
0x9f0f2c208700 UDPv4 0.0.0.0 61608 * 0 1752 svchost.exe 2023-01-09 21:48:32.000000
0x9f0f2c208700 UDPv6 :: 61608 * 0 1752 svchost.exe 2023-01-09 21:48:32.000000
0x9f0f2c2161c0UDPv4 0.0.0.0 51060 * 0 1752 svchost.exe 2023-01-09 21:48:29.000000
0x9f0f2c2161c0UDPv6 :: 51060 * 0 1752 svchost.exe 2023-01-09 21:48:29.000000
0x9f0f2c356090 UDPv4 0.0.0.0 61535 * 0 1752 svchost.exe 2023-01-09 21:48:32.000000
0x9f0f2c356090 UDPv6 :: 61535 * 0 1752 svchost.exe 2023-01-09 21:48:32.000000
0x9f0f2c357350 UDPv4 0.0.0.0 65041 * 0 1752 svchost.exe 2023-01-09 21:48:32.000000
0x9f0f2c357350 UDPv6 :: 65041 * 0 1752 svchost.exe 2023-01-09 21:48:32.000000
0x9f0f2c358de0UDPv4 0.0.0.0 56378 * 0 1752 svchost.exe 2023-01-09 21:48:32.000000
0x9f0f2c358de0UDPv6 :: 56378 * 0 1752 svchost.exe 2023-01-09 21:48:32.000000
```

The next step is to examine the Security Identifiers (SIDs) of process owners to pinpoint the user's SID. While the output is extensive, several processes clearly show the user "Spongebob," as seen in the snippet below.

```
python3 vol.py -f ../physmem.raw windows.getsids.GetSIDs
```

```
1760    firefox.exe    S-1-5-113 Local Account
1760    firefox.exe    S-1-5-5-0-153597 Logon Session
1760    firefox.exe    S-1-2-0 Local (Users with the ability to log in locally)
1760    firefox.exe    S-1-5-64-10 NTLM Authentication
1760    firefox.exe    S-1-16-4096 Low Mandatory Level
7780    firefox.exe    S-1-5-21-2607170198-3457296929-47938352-1001  Spongebob

7780 firefox.exe S-1-5-21-2607170198-3457296929-47938352-513 Domain Users
7780 firefox.exe S-1-1-0 Everyone
...
```

To conclude, we extracted the user's password hash from the RAM dump using the hashdump Volatility plugin. This yielded the NTLM hash BCF8548EAE42900BEDA0F150E16504B5 (the format Windows uses for passwords [1]). The next logical step is to attempt to crack this password via a dictionary attack.

```
python3 vol.py -f ../physmem.raw windows.hashdump.Hashdump
```

ANALYSIS

RAM Dump from Owned System

1. List all the Running Processes and Network Connections

As outlined in section 2, the windows.pslist.PsList plugin of Volatility 3 was employed to list all processes. The provided output furnishes details for each visible running program, encompassing process IDs (and parent's IDs), file names, memory information, creation times, etc. The list includes instances of Windows processes, the file explorer, and user programs like web browsers.

A similar approach was adopted for network information using the windows.netstat.NetStat plugin of Volatility 3. This analysis reveals details such as protocol, state (listening, estab- lished, etc.), addresses, ports, process IDs, memory information, and the program account- able for initiating the network.

2. Differences Between Scanning and Listing Processes and Networks

Similarly to the listing process, section 2 presents the results of scanning processes and networks using the windows.psscan.PsScan and windows.netscan.NetScan Volatility plug- ins. Despite the visual similarity in output, the distinction lies in how listing from memory operates akin to the task manager, rendering it unable to detect processes or networks con- cealed by rootkits. In contrast, the PsScan and NetScan modules conduct a comprehensive scan of the entire memory for process and network structures, enabling the discovery of both hidden and terminated entities [2].

3. Verify the Existence of a Unique Artefact

During the retrieval of RAM from the Windows 7 image, an instance of the Opera (v95.0.4635.90) browser was active, with two tabs open. Consequently, an examination of the output from

the processes' listing/scanning reveals several processes initiated by the opera.exe exe- cutable. Additionally, a network created by the browser is evident, serving as a distinctive artifact within the memory dump.

Unknown RAM Dump

1. What Information can you Extract about the Operating System?

The details obtained regarding the operating system are available in section 2. Examples include the Windows layer name (WindowsIntel32e), major and minor versions (15.22621), the number of processors (2), the product type (NtProductWinNt), among others.

2. What Happened at the Time of the RAM Dump?

In section 2, the timestamp of the RAM extraction, along with the operating system details, reveals that the dump was obtained on 2023-01-09 at 22:17:11.

The section also provides a comprehensive overview of currently active processes and network connections, employing scanning tools to uncover potentially concealed elements. Notable processes include:

- Essential Windows services like svchost, desktop, and session manager.
- VirtualBox (VBoxService.exe).
- Web browsers such as Firefox (firefox.exe), Microsoft Edge (msedge.exe), and Tor (tor.exe).
- Notepad (Notepad.exe).

- A strange process named winpmem mini x, which might be related to the WinPMem memory extraction tool.

The presence of three distinct browsers concurrently running—Edge, Firefox, and Tor—raises considerations. While Edge and Firefox are standard choices for general web tasks, Tor is typically utilized by individuals seeking anonymity or navigating around censorship. This behavior could be perceived as suspicious, or it might simply reflect a concern for online privacy.

Regarding network activity, numerous networks are active, with many initiated by a Windows service, while others are associated with the aforementioned browsers.

3. What is the user SID?

Upon scrutinizing the results from the windows.getsids.GetSIDs plugin in section 2, the user's SID is identified as S-1-5-21-2607170198-3457296929-47938352-1001, and the corresponding username is Spongebob. The extraction of the SID is possible due to its association with various active processes, including Firefox.

4. Can you Find/Crack the User Password?

Following the execution of the windows.hashdump.Hashdump plugin in section 2, the hash of the user's password is retrievable: BCF8548EAE42900BEDA0F150E16504B5. Utilizing an online tool like hashes.com, it becomes feasible to conduct a dictionary attack and unveil the original password: ThisIsPatrick. Consequently, confirming the user's identity as Patrick.