Assignment 4: RAM
Digital Forensics

Elisa Pioldi
ID 12305812

January 17, 2024

1 Factual part

1.1 Background

1.1.1 Case description

This analysis is divided into two parts:

1. Acquisition and analysis of a choosen RAM dump
2. Analysis of a RAM dump sent by an unknown source

1.1.2 Software and hardware specifications

For this analysis, I utilized the following software:

- **Volatility** [1] – version 2.5.2; to analyze the RAM dump.
- **WinPmem** [2] to acquire the RAM dump.

1.2 Analysis of the choosen RAM dump

1.2.1 Preprocessing and acquisition

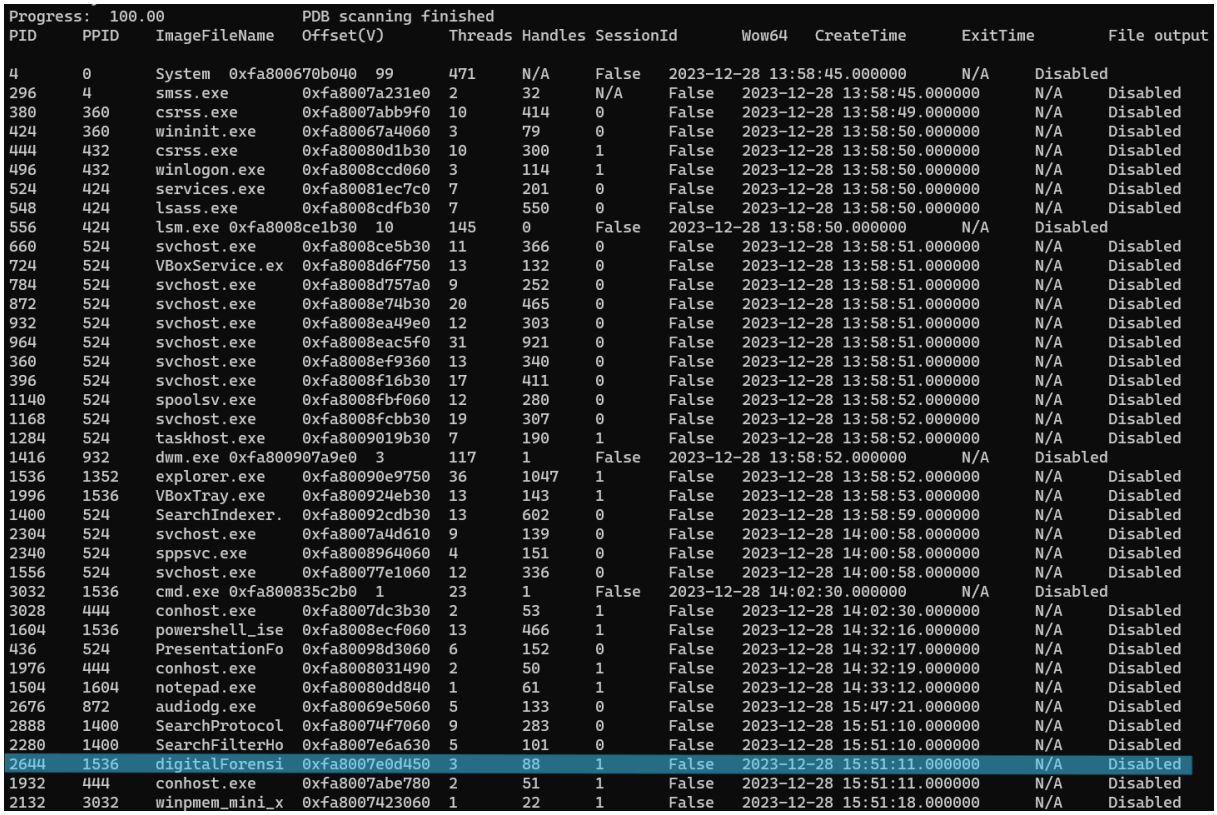
First, I created a virtual machine with Windows 7. To make the image unique, I created a simple application called *digitalForensic* in Powershell and I executed it.

Then I installed WinPmem and I acquired the RAM dump. The SHA-256 of `physmem.raw` is:
`32706ABA85866D8FA8726658B223AB497FD5BBFC1E42D53049567680A36078B7`

1.2.2 Analysis

Once I acquired the RAM dump, I used Volatility to analyze it. First I listed the processes running at the time of the dump. The results are shown in Figure 1. Then I scanned for processes, as shown in Figure 2.

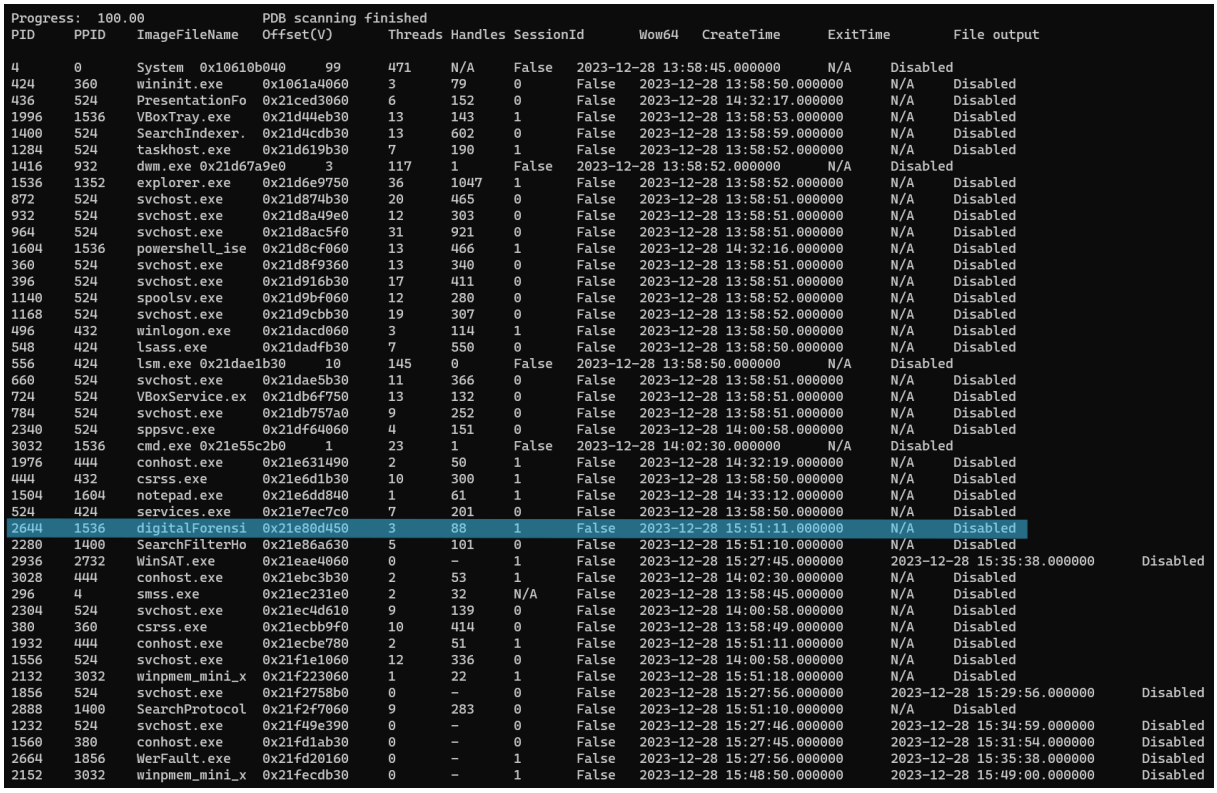
You can see highlighted in blue the process **digitalForensic.exe**, which is the one I created.



```
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xfa800670b040  99      471     N/A     False   2023-12-28 13:58:45.000000      N/A     Disabled
296     4       smss.exe        0xfa8007a231e0  2       32      N/A     False   2023-12-28 13:58:45.000000      N/A     Disabled
380     360     csrss.exe       0xfa8007abb9f0  10      414     0       False   2023-12-28 13:58:49.000000      N/A     Disabled
424     360     wininit.exe     0xfa80067a4060  3       79      0       False   2023-12-28 13:58:50.000000      N/A     Disabled
444     432     csrss.exe       0xfa80080d1b30  10      300     1       False   2023-12-28 13:58:50.000000      N/A     Disabled
496     432     winlogon.exe    0xfa8008ccd060  3       114     1       False   2023-12-28 13:58:50.000000      N/A     Disabled
524     424     services.exe    0xfa80081ec7c0  7       201     0       False   2023-12-28 13:58:50.000000      N/A     Disabled
548     424     lsass.exe       0xfa8008cdfb30  7       550     0       False   2023-12-28 13:58:50.000000      N/A     Disabled
556     424     lsm.exe 0xfa8008ce1b30  10      145     0       False   2023-12-28 13:58:50.000000      N/A     Disabled
660     524     svchost.exe     0xfa8008ce5b30  11      366     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
724     524     VBoxService.ex  0xfa8008d6f750  13      132     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
784     524     svchost.exe     0xfa8008d757a0  9       252     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
872     524     svchost.exe     0xfa8008e74b30  20      465     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
932     524     svchost.exe     0xfa8008ea49e0  12      303     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
964     524     svchost.exe     0xfa8008eac5f0  31      921     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
360     524     svchost.exe     0xfa8008ef9360  13      340     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
396     524     svchost.exe     0xfa8008f16b30  17      411     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
1140    524     spoolsv.exe     0xfa8008fbf060  12      280     0       False   2023-12-28 13:58:52.000000      N/A     Disabled
1168    524     svchost.exe     0xfa8008fcbb30  19      307     0       False   2023-12-28 13:58:52.000000      N/A     Disabled
1284    524     taskhost.exe    0xfa8009019b30  7       190     1       False   2023-12-28 13:58:52.000000      N/A     Disabled
1416    932     dwm.exe 0xfa800907a9e0  3       117     1       False   2023-12-28 13:58:52.000000      N/A     Disabled
1536    1352    explorer.exe    0xfa80090e9750  36      1047    1       False   2023-12-28 13:58:52.000000      N/A     Disabled
1996    1536    VBoxTray.exe    0xfa800924eb30  13      143     1       False   2023-12-28 13:58:53.000000      N/A     Disabled
1400    524     SearchIndexer.  0xfa80092cdb30  13      602     0       False   2023-12-28 13:58:59.000000      N/A     Disabled
2304    524     svchost.exe     0xfa8007a4d610  9       139     0       False   2023-12-28 14:00:58.000000      N/A     Disabled
2340    524     sppsvc.exe      0xfa8008964060  4       151     0       False   2023-12-28 14:00:58.000000      N/A     Disabled
1556    524     svchost.exe     0xfa80077e1060  12      336     0       False   2023-12-28 14:00:58.000000      N/A     Disabled
3032    1536    cmd.exe 0xfa800835c2b0  1       23      1       False   2023-12-28 14:02:30.000000      N/A     Disabled
3028    444     conhost.exe     0xfa8007dc3b30  2       53      1       False   2023-12-28 14:02:30.000000      N/A     Disabled
1604    1536    powershell_ise  0xfa8008ecf060  13      466     1       False   2023-12-28 14:32:16.000000      N/A     Disabled
436     524     PresentationFo  0xfa80098d3060  6       152     0       False   2023-12-28 14:32:17.000000      N/A     Disabled
1976    444     conhost.exe     0xfa8008031490  2       50      1       False   2023-12-28 14:32:19.000000      N/A     Disabled
1504    1604    notepad.exe     0xfa80080dd840  1       61      1       False   2023-12-28 14:33:12.000000      N/A     Disabled
2676    872     audiodg.exe     0xfa80069e5060  5       133     0       False   2023-12-28 15:47:21.000000      N/A     Disabled
2888    1400    SearchProtocol  0xfa80074f7060  9       283     0       False   2023-12-28 15:51:10.000000      N/A     Disabled
2280    1400    SearchFilterHo  0xfa8007e6a630  5       101     0       False   2023-12-28 15:51:10.000000      N/A     Disabled
2644    1536    digitalForensi  0xfa8007e0d450  3       88      1       False   2023-12-28 15:51:11.000000      N/A     Disabled
1932    444     conhost.exe     0xfa8007abe780  2       51      1       False   2023-12-28 15:51:11.000000      N/A     Disabled
2132    3032    winpmem_mini_x  0xfa8007423060  1       22      1       False   2023-12-28 15:51:18.000000      N/A     Disabled
```

Figure 1: List of processes.



```
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x10610b040     99      471     N/A     False   2023-12-28 13:58:45.000000      N/A     Disabled
424     360     wininit.exe     0x1061a4060     3       79      0       False   2023-12-28 13:58:50.000000      N/A     Disabled
436     524     PresentationFo  0x21ced3060     6       152     0       False   2023-12-28 14:32:17.000000      N/A     Disabled
1996    1536    VBoxTray.exe    0x21d44eb30     13      143     1       False   2023-12-28 13:58:53.000000      N/A     Disabled
1400    524     SearchIndexer.  0x21d4cdb30     13      602     0       False   2023-12-28 13:58:59.000000      N/A     Disabled
1284    524     taskhost.exe    0x21d619b30     7       190     1       False   2023-12-28 13:58:52.000000      N/A     Disabled
1416    932     dwm.exe 0x21d67a9e0     3       117     1       False   2023-12-28 13:58:52.000000      N/A     Disabled
1536    1352    explorer.exe    0x21d6e9750     36      1047    1       False   2023-12-28 13:58:52.000000      N/A     Disabled
872     524     svchost.exe     0x21d874b30     20      465     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
932     524     svchost.exe     0x21d8a49e0     12      303     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
964     524     svchost.exe     0x21d8ac5f0     31      921     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
1604    1536    powershell_ise  0x21d8cf060     13      466     1       False   2023-12-28 14:32:16.000000      N/A     Disabled
360     524     svchost.exe     0x21d8f9360     13      340     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
396     524     svchost.exe     0x21d916b30     17      411     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
1140    524     spoolsv.exe     0x21d9bf060     12      280     0       False   2023-12-28 13:58:52.000000      N/A     Disabled
1168    524     svchost.exe     0x21d9cbb30     19      307     0       False   2023-12-28 13:58:52.000000      N/A     Disabled
496     432     winlogon.exe    0x21dacd060     3       114     1       False   2023-12-28 13:58:50.000000      N/A     Disabled
548     424     lsass.exe       0x21dadfb30     7       550     0       False   2023-12-28 13:58:50.000000      N/A     Disabled
556     424     lsm.exe 0x21dae1b30     10      145     0       False   2023-12-28 13:58:50.000000      N/A     Disabled
660     524     svchost.exe     0x21dae5b30     11      366     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
724     524     VBoxService.ex  0x21db6f750     13      132     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
784     524     svchost.exe     0x21db757a0     9       252     0       False   2023-12-28 13:58:51.000000      N/A     Disabled
2340    524     sppsvc.exe      0x21df64060     4       151     0       False   2023-12-28 14:00:58.000000      N/A     Disabled
3032    1536    cmd.exe 0x21e55c2b0     1       23      1       False   2023-12-28 14:02:30.000000      N/A     Disabled
1976    444     conhost.exe     0x21e631490     2       50      1       False   2023-12-28 14:32:19.000000      N/A     Disabled
444     432     csrss.exe       0x21e6d1b30     10      300     1       False   2023-12-28 13:58:50.000000      N/A     Disabled
1504    1604    notepad.exe     0x21e6dd840     1       61      1       False   2023-12-28 14:33:12.000000      N/A     Disabled
524     424     services.exe    0x21e7ec7c0     7       201     0       False   2023-12-28 13:58:50.000000      N/A     Disabled
2644    1536    digitalForensi  0x21e80d450     3       88      1       False   2023-12-28 15:51:11.000000      N/A     Disabled
2280    1400    SearchFilterHo  0x21e86a630     5       101     0       False   2023-12-28 15:51:10.000000      N/A     Disabled
2936    2732    WinSAT.exe      0x21eae4060     0       -       1       False   2023-12-28 15:27:45.000000      2023-12-28 15:35:38.000000      Disabled
3028    444     conhost.exe     0x21ebc3b30     2       53      1       False   2023-12-28 14:02:30.000000      N/A     Disabled
296     4       smss.exe        0x21ec231e0     2       32      N/A     False   2023-12-28 13:58:45.000000      N/A     Disabled
2304    524     svchost.exe     0x21ec4d610     9       139     0       False   2023-12-28 14:00:58.000000      N/A     Disabled
380     360     csrss.exe       0x21ecbb9f0     10      414     0       False   2023-12-28 13:58:49.000000      N/A     Disabled
1932    444     conhost.exe     0x21ecbe780     2       51      1       False   2023-12-28 15:51:11.000000      N/A     Disabled
1556    524     svchost.exe     0x21f1e1060     12      336     0       False   2023-12-28 14:00:58.000000      N/A     Disabled
2132    3032    winpmem_mini_x  0x21f223060     1       22      1       False   2023-12-28 15:51:18.000000      N/A     Disabled
1856    524     svchost.exe     0x21f2758b0     0       -       0       False   2023-12-28 15:27:56.000000      2023-12-28 15:29:56.000000      Disabled
2888    1400    SearchProtocol  0x21f2f7060     9       283     0       False   2023-12-28 15:51:10.000000      N/A     Disabled
1232    524     svchost.exe     0x21f49e390     0       -       0       False   2023-12-28 15:27:46.000000      2023-12-28 15:34:59.000000      Disabled
1560    380     conhost.exe     0x21fd1ab30     0       -       0       False   2023-12-28 15:27:45.000000      2023-12-28 15:31:54.000000      Disabled
2664    1856    WerFault.exe    0x21fd20160     0       -       1       False   2023-12-28 15:27:56.000000      2023-12-28 15:35:38.000000      Disabled
2152    3032    winpmem_mini_x  0x21fecdb30     0       -       1       False   2023-12-28 15:48:50.000000      2023-12-28 15:49:00.000000      Disabled
```

Figure 2: Scanning for processes.

```
Progress:  100.00           PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0x831bc820      UDPv4   0.0.0.0 0       *       0               724     VBoxService.ex  2023-12-28 15:01:47.000000
0x138e23820     UDPv4   0.0.0.0 0       *       0               724     VBoxService.ex  2023-12-28 15:01:47.000000
0x21d41d690     UDPv4   0.0.0.0 5355    *       0               396     svchost.exe     2023-12-28 13:58:58.000000
0x21d41d690     UDPv6   ::      5355    *       0               396     svchost.exe     2023-12-28 13:58:58.000000
0x21d4b6b70     UDPv4   0.0.0.0 5355    *       0               396     svchost.exe     2023-12-28 13:58:58.000000
0x21d564c80     TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       548     lsass.exe       -
0x21d564c80     TCPv6   ::      49156   ::      0       LISTENING       548     lsass.exe       -
0x21d564ef0     TCPv4   0.0.0.0 49156   0.0.0.0 0       LISTENING       548     lsass.exe       -
0x21d571950     TCPv4   -       49157   84.53.184.185   80      CLOSED  396     svchost.exe     -
0x21d6b53f0     TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       524     services.exe    -
0x21d6b53f0     TCPv6   ::      49155   ::      0       LISTENING       524     services.exe    -
0x21d79ca10     TCPv4   0.0.0.0 49155   0.0.0.0 0       LISTENING       524     services.exe    -
0x21d7ad9f0     TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  -
0x21d7ad9f0     TCPv6   ::      445     ::      0       LISTENING       4       System  -
0x21d7c9200     TCPv4   10.0.2.15       139     0.0.0.0 0       LISTENING       4       System  -
0x21d7d49d0     UDPv4   10.0.2.15       138     *       0               4       System  2023-12-28 13:58:55.000000
0x21d85a8c0     TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       784     svchost.exe     -
0x21d85a8c0     TCPv6   ::      135     ::      0       LISTENING       784     svchost.exe     -
0x21d866d10     TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       424     wininit.exe     -
0x21d868ef0     TCPv4   0.0.0.0 49152   0.0.0.0 0       LISTENING       424     wininit.exe     -
0x21d868ef0     TCPv6   ::      49152   ::      0       LISTENING       424     wininit.exe     -
0x21d890010     UDPv4   127.0.0.1       1900    *       0               2304    svchost.exe     2023-12-28 14:00:58.000000
0x21d8a13b0     TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       872     svchost.exe     -
0x21d8a1be0     TCPv4   0.0.0.0 49153   0.0.0.0 0       LISTENING       872     svchost.exe     -
0x21d8a1be0     TCPv6   ::      49153   ::      0       LISTENING       872     svchost.exe     -
0x21d950610     UDPv4   0.0.0.0 0       *       0               396     svchost.exe     2023-12-28 13:58:55.000000
0x21d950610     UDPv6   ::      0       *       0               396     svchost.exe     2023-12-28 13:58:55.000000
0x21d9818a0     TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       964     svchost.exe     -
0x21d9845f0     TCPv4   0.0.0.0 49154   0.0.0.0 0       LISTENING       964     svchost.exe     -
0x21d9845f0     TCPv6   ::      49154   ::      0       LISTENING       964     svchost.exe     -
0x21dad90d0     UDPv6   fe80::88bd:4970:a919:4e32       546     *       0               872     svchost.exe     2023-12-28 15:45:53.000000
0x21db0ed90     UDPv4   10.0.2.15       1900    *       0               2304    svchost.exe     2023-12-28 14:00:58.000000
0x21dcad420     UDPv6   ::1     51627   *       0               2304    svchost.exe     2023-12-28 14:00:58.000000
0x21dd26400     TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       784     svchost.exe     -
0x21e671010     UDPv6   ::1     1900    *       0               2304    svchost.exe     2023-12-28 14:00:58.000000
0x21ebd91f0     UDPv4   0.0.0.0 0       *       0               724     VBoxService.ex  2023-12-28 15:52:05.000000
0x21ec11b80     UDPv6   fe80::88bd:4970:a919:4e32       1900    *       0               2304    svchost.exe     2023-12-28 14:00:58.000000
0x21ec949d0     UDPv4   127.0.0.1       51628   *       0               2304    svchost.exe     2023-12-28 14:00:58.000000
0x21ecbe2a0     UDPv4   10.0.2.15       137     *       0               4       System  2023-12-28 13:58:55.000000
```

Figure 3: List of network connections.

We can notice that scanning and listing processes gives different results. This is because `pslist` only lists processes that are in the *EPROCESS* structure, while `psscan` scans the physical memory for the *EPROCESS* structure. This means that `psscan` can find processes that are not in the *EPROCESS* structure, such as terminated processes.

Finally, I listed the network connections, as shown in Figure 3.

1.3 Analysis of the unknown RAM dump

I received a RAM dump from an unknown source. The SHA-256 of `physmem.raw` is: `fee4a87527509ed8a67c51a2b3e21a74ae52739e0d69020312180339cfd79e3b`

1.3.1 Basic information

First of all, I checked the basic information about the RAM dump, such as the operating system, the architecture, the profile, the time of the dump, etc. The results are shown in Table 1.

1.3.2 Processes

I looked for the processes running at the time of the dump (you can see some of them in Figure 4):

1. **System** (PID 4)
2. **Registry** (PID 88)
3. **smss.exe** (PID 384)

Property	Value
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

Table 1: Checksums of important files.

4. **csrss.exe** (PID 576, 652)
5. **wininit.exe** (PID 644)
6. **winlogon.exe** (PID 736)
7. **services.exe** (PID 772)
8. **lsass.exe** (PID 804)
9. **svchost.exe** (PID 908, 424, 536, 1088, 1100, 1208, 1252, 1300, 1324, 1336, 1420, 1452, 1496, 1540, 1752, 1856, 1916, 1924, 1936, 2036, 296, 1484, 2060, 2132, 2156, 2196, 2204, 2240, 2348, 2464, 2484, 2604, 2636, 2784, 2900, 2908, 2916, 2980, 2992, 3016, 3032, 3064)
10. **LogonUI.exe** (PID 852)
11. **dwm.exe** (PID 920)
12. **MemCompression** (PID 2020)
13. **Fontdrvhost.exe** (PID 924, 932)
14. **AggregatorHost** (PID 3456)
15. **sihost.exe** (PID 3584)
16. **SearchIndexer.exe** (PID 6076)
17. **explorer.exe** (PID 4108)
18. **VBoxTray.exe** (PID 6972)

```
Progress:  100.00           PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0x9f0f23ee6040  130     -       N/A     False   2023-01-09 21:47:13.000000      N/A     Disabled
88      4       Registry        0x9f0f23ede080  4       -       N/A     False   2023-01-09 21:47:12.000000      N/A     Disabled
384     4       smss.exe        0x9f0f24a75040  2       -       N/A     False   2023-01-09 21:47:13.000000      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
652     636     csrss.exe       0x9f0f27b1d140  14      -       1       False   2023-01-09 21:47:15.000000      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
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
424     772     svchost.exe     0x9f0f27b1b140  12      -       0       False   2023-01-09 21:47:16.000000      N/A     Disabled
536     772     svchost.exe     0x9f0f27c31080  5       -       0       False   2023-01-09 21:47:16.000000      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
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
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
1336    772     svchost.exe     0x9f0f27f0c080  5       -       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
1452    772     svchost.exe     0x9f0f27e9b0c0  5       -       0       False   2023-01-09 21:47:16.000000      N/A     Disabled
1496    772     svchost.exe     0x9f0f292540c0  9       -       0       False   2023-01-09 21:47:16.000000      N/A     Disabled
1540    772     svchost.exe     0x9f0f292aa0c0  9       -       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
1784    772     VBoxService.ex  0x9f0f23f7e080  10      -       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
1916    772     svchost.exe     0x9f0f23fcc080  4       -       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
1936    772     svchost.exe     0x9f0f23f0f080  3       -       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
2036    772     svchost.exe     0x9f0f23f2b080  2       -       0       False   2023-01-09 21:47:16.000000      N/A     Disabled
296     772     svchost.exe     0x9f0f27b49080  2       -       0       False   2023-01-09 21:47:16.000000      N/A     Disabled
1484    772     svchost.exe     0x9f0f29430080  8       -       0       False   2023-01-09 21:47:16.000000      N/A     Disabled
2060    772     svchost.exe     0x9f0f291820c0  8       -       0       False   2023-01-09 21:47:16.000000      N/A     Disabled
2132    772     svchost.exe     0x9f0f291dc080  11      -       0       False   2023-01-09 21:47:17.000000      N/A     Disabled
2156    772     svchost.exe     0x9f0f290450c0  3       -       0       False   2023-01-09 21:47:17.000000      N/A     Disabled
2196    772     svchost.exe     0x9f0f2918e080  7       -       0       False   2023-01-09 21:47:17.000000      N/A     Disabled
2204    772     svchost.exe     0x9f0f291e3080  3       -       0       False   2023-01-09 21:47:17.000000      N/A     Disabled
2240    772     svchost.exe     0x9f0f2906c080  3       -       0       False   2023-01-09 21:47:17.000000      N/A     Disabled
2348    772     svchost.exe     0x9f0f290f0080  2       -       0       False   2023-01-09 21:47:17.000000      N/A     Disabled
```

Figure 4: List of processes.

19. **OneDrive.exe** (PID 7056)
20. **SecurityHealth** (PID 6908, 6924)
21. **VBoxService.exe** (PID 1784)
22. **spoolsv.exe** (PID 2484)
23. **msedge.exe** (PID 4800, 6212, 5288, 5260, 2760)
24. **msteams.exe** (PID 7324)
25. **msedgewebview2** (PID 7492, 7508, 7636, 7788, 7800, 7816, 7920)
26. **dllhost.exe** (PID 8108, 9096)
27. **firefox.exe** (PID 7252, 6548, 8244, 8444, 8708, 9112, 9160, 9196, 3940, 4796, 4140, 2508)
28. **Notepad.exe** (PID 8944)
29. **NisSrv.exe** (PID 6004)
30. **ctfmon.exe** (PID 4828)
31. **SearchHost.exe** (PID 4588)
32. **LockApp.exe** (PID 5880)
33. **RuntimeBroker.exe** (PID 7492, 6924, 5012)

34. **taskhostw.exe** (PID 3908, 5184)
35. **userinit.exe** (PID 3820)
36. **RuntimeBroker.exe** (PID 5928)
37. **Widgets.exe** (PID 4684)

1.3.3 Network connections

I scanned for network connections: the results are shown in Figure **??**.

1.3.4 SID

I looked for the SIDs: you can see some of them in Figure 6.

2 Expert testimony

Observing the information about the RAM dump, we can retrieve the time of the dump, which is **2023-01-09 22:17:11**.

Taking a closer look to the running processes, we see that not all the browsers are the same. In fact, we have **msedge.exe** and **firefox.exe**. This means that the user was using two different browsers at the time of the dump.

I could also find the SID of the user, which is **S-1-5-21-2607170198-3457296929-47938352-1001**. This SID is associated to the user **Spongebob**.

2.1 User password

To retrieve the user password, I first got the hashes contained in the memory dump, then I used an online tool (hashes.com [3]) to crack the hash: this tool searches for the hash in a database of already cracked hashes.

The hash is `bcf8548eae42900beda0f150e16504b5` and the associated password is: `ThisIsPatrick`.

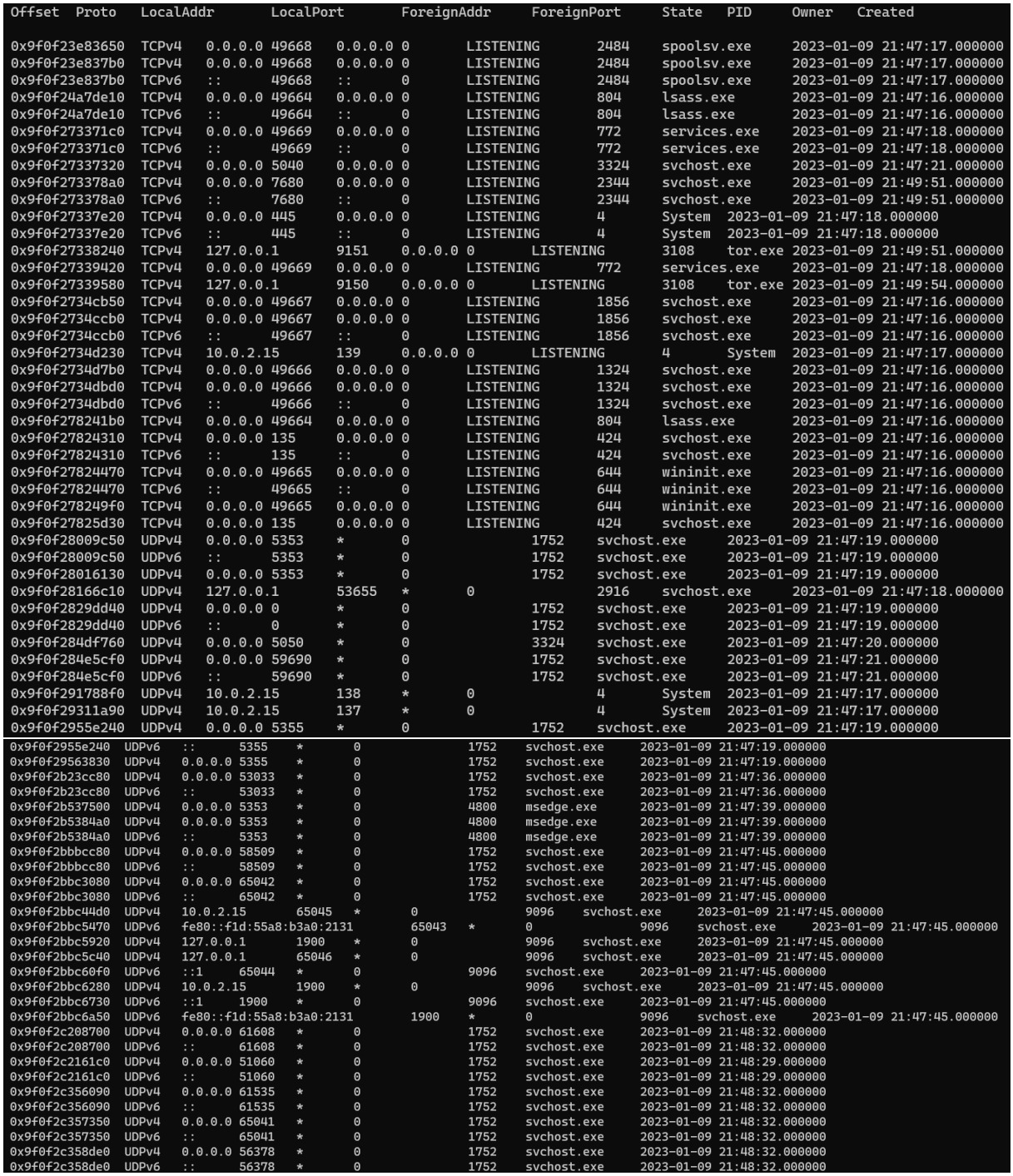
Given this, we can assume that who sent the RAM dump is **Patrick**.

References

[1] Volatility Foundation. *Volatility*. URL: `https://github.com/volatilityfoundation/volatility` (visited on 01/2023).

[2] Velocidex. *WinPmem*. URL: `https://github.com/Velocidex/WinPmem` (visited on 01/2023).

[3] *Hashes*. URL: `https://hashes.com/en/decrypt/hash` (visited on 01/2023).



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
0x9f0f2734ccb0	TCPv4	0.0.0.0	49667	0.0.0.0	0	LISTENING	1856	svchost.exe	2023-01-09 21:47:16.000000
0x9f0f2734ccb0	TCPv6	::	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
0x9f0f278249f0	TCPv4	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	
0x9f0f284df760	UDPv4	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	
0x9f0f291788f0	UDPv4	10.0.2.15	138	*	0	4	System	2023-01-09 21:47:17.000000	
0x9f0f29311a90	UDPv4	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	
0x9f0f2b23cc80	UDPv4	0.0.0.0	53033	*	0	1752	svchost.exe	2023-01-09 21:47:36.000000	
0x9f0f2b23cc80	UDPv6	::	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	
0x9f0f2bbbcc80	UDPv4	0.0.0.0	58509	*	0	1752	svchost.exe	2023-01-09 21:47:45.000000	
0x9f0f2bbbcc80	UDPv6	::	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	
0x9f0f2bbc5c40	UDPv4	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	
0x9f0f2bbc6a50	UDPv6	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	
0x9f0f2c2161c0	UDPv4	0.0.0.0	51060	*	0	1752	svchost.exe	2023-01-09 21:48:29.000000	
0x9f0f2c2161c0	UDPv6	::	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	
0x9f0f2c358de0	UDPv4	0.0.0.0	56378	*	0	1752	svchost.exe	2023-01-09 21:48:32.000000	
0x9f0f2c358de0	UDPv6	::	56378	*	0	1752	svchost.exe	2023-01-09 21:48:32.000000	

Figure 5: Network connections.

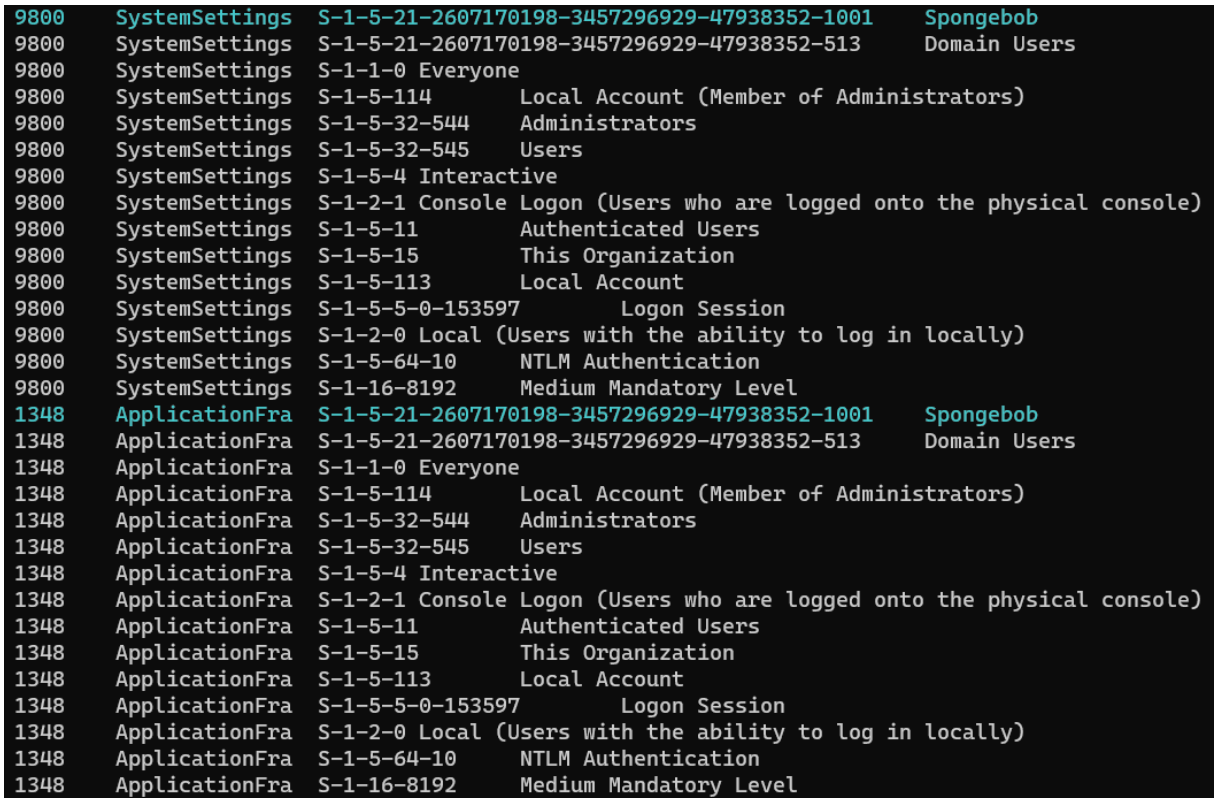


Figure 6: SID of the user.