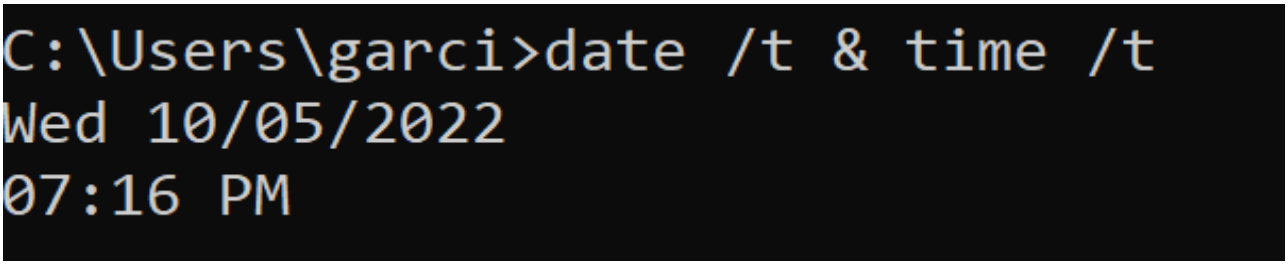
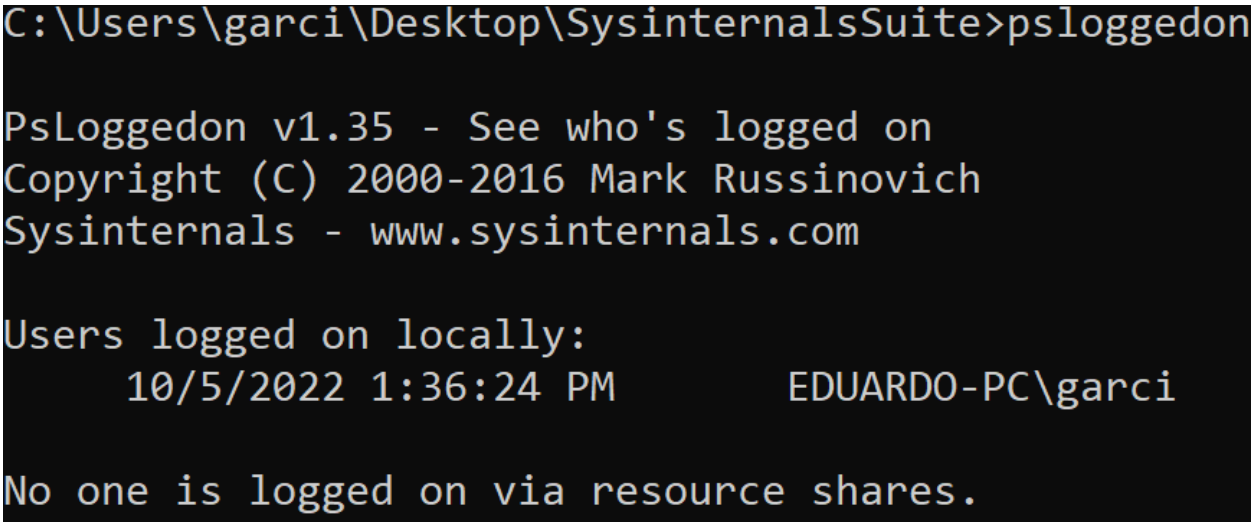
Report 6

For this week's lab, we used PowerShell to collect volatile information that was in our Microsoft Windows virtual machine. In my case, I used the host operating system since it was a Windows Operating system. The first task was to collect time and data. This can be done using the **date /t & time /t** command. The "&" executes the first command followed by the second one. Not using the **t/** parameter will result in you having to input a new date. Here below is the using the date and time commands for today's date.



The second task was listing the users who where had logged in. In order to do that, you need to use the **psloggedon** command**.** This command can only be utilized if you had previously installed the Sysinternals Suite package in your system. Since I had already installed this package, I changed my directory to access those tools by using **cd Desktop\SysinternalsSuite** Here below is the list of users that are logged on.



You can also list the number of logged-on sessions using the **logonsessions** command.

```
C:\Users\garci\Desktop\SysinternalsSuite>logonsessions

LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
    User name:    WORKGROUP\EDUARDO-PC$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   10/5/2022 1:36:22 PM
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:00015b44:
    User name:
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          (none)
    Logon time:   10/5/2022 1:36:22 PM
    Logon server:
    DNS Domain:
    UPN:

[2] Logon session 00000000:00015f2e:
    User name:    Font Driver Host\UMFD-0
    Auth package: Negotiate
    Logon type:   Interactive
    Session:      0
    Sid:          S-1-5-96-0-0
    Logon time:   10/5/2022 1:36:22 PM
    Logon server:
```

Using the **logonsessions | findstr "logon session"** command you list the logon session ID.

```
C:\Users\garci\Desktop\SysinternalsSuite>logonsessions | findstr "logon session"
LogonSessions v1.41 - Lists logon session information
[0] Logon session 00000000:000003e7:
[1] Logon session 00000000:00015b44:
[2] Logon session 00000000:00015f2e:
[3] Logon session 00000000:000003e4:
[4] Logon session 00000000:0001cbae:
[5] Logon session 00000000:0001d586:
[6] Logon session 00000000:0001d5ad:
[7] Logon session 00000000:000003e5:
[8] Logon session 00000000:0003530c:
[9] Logon session 00000000:00036058:
```

The **logonsessions -p** command displays the processes that are running in each session. Here below are the processes were running for the 9th logon session.

```
[9] Logon session 00000000:00036058:
    User name:    EDUARDO-PC\garci
    Auth package: CloudAP
    Logon type:   Interactive
    Session:      1
    Sid:          S-1-5-21-2061162394-2380904589-191770230-1001
    Logon time:   10/5/2022 1:36:23 PM
    Logon server:
    DNS Domain:
    UPN:
     4792: sihost.exe
     4832: svchost.exe
     4840: svchost.exe
     4892: svchost.exe
     5072: taskhostw.exe
     5244: ctfmon.exe
     5536: explorer.exe
     6568: svchost.exe
     7620: StartMenuExperienceHost.exe
     7648: SearchHost.exe
```

Below we are using the -c parameter to display the information below.

```
C:\Users\garci\Desktop\SysinternalsSuite> logonsessions -c

LogonSessions v1.41 - Lists logon session information
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

Logon Session,User Name,Auth Package,Logon Type,Session,Sid,Logon Time,Logon Server,DNS Domain,UPN,Processes
00000000:000003e7,WORKGROUP\EDUARDO-PC$,NTLM,(none),0,S-1-5-18,10/5/2022 1:36:22 PM,,,,
00000000:00015b44,,NTLM,(none),0,(none),10/5/2022 1:36:22 PM,,,,
00000000:00015f2e,Font Driver Host\UMFD-0,Negotiate,Interactive,0,S-1-5-96-0-0,10/5/2022 1:36:22 PM,,,,
00000000:000003e4,WORKGROUP\EDUARDO-PC$,Negotiate,Service,0,S-1-5-20,10/5/2022 1:36:22 PM,,,,
00000000:0001cbae,Font Driver Host\UMFD-1,Negotiate,Interactive,1,S-1-5-96-0-1,10/5/2022 1:36:22 PM,,,,
00000000:0001d586,Window Manager\DWM-1,Negotiate,Interactive,1,S-1-5-90-0-1,10/5/2022 1:36:22 PM,,,,
00000000:0001d5ad,Window Manager\DWM-1,Negotiate,Interactive,1,S-1-5-90-0-1,10/5/2022 1:36:22 PM,,,,
00000000:000003e5,NT AUTHORITY\LOCAL SERVICE,Negotiate,Service,0,S-1-5-19,10/5/2022 1:36:22 PM,,,,
00000000:0003530c,EDUARDO-PC\garci,CloudAP,Interactive,1,S-1-5-21-2061162394-2380904589-191770230-1001,10/5/2022 1:36:23 PM,,,,
00000000:00036058,EDUARDO-PC\garci,CloudAP,Interactive,1,S-1-5-21-2061162394-2380904589-191770230-1001,10/5/2022 1:36:23 PM,,,,
```

The next step was to collect information on network connections using the **netstat** command. To collect all the information, you can use the **netstat -a** command to display all the connections.

```
C:\Users\garci\Desktop\SysinternalsSuite>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:445            Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:554            Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:1042           Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:1043           Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:2869           Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:3389           Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:5040           Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:5357           Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:7680           Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:9012           Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:9013           Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:10243          Eduardo-PC:0           LISTENING
  TCP    0.0.0.0:17500          Eduardo-PC:0           LISTENING
```

Using the **netstat -p tcp** command will display a protocol that uses TCP. Here below are the active connections using TCP. You also select other protocols as well.

```
C:\Users\garci\Desktop\SysinternalsSuite>netstat -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1042         Eduardo-PC:49789       ESTABLISHED
  TCP    127.0.0.1:1042         Eduardo-PC:49795       ESTABLISHED
  TCP    127.0.0.1:1042         Eduardo-PC:49807       ESTABLISHED
  TCP    127.0.0.1:1042         Eduardo-PC:49866       ESTABLISHED
  TCP    127.0.0.1:9012         Eduardo-PC:49828       ESTABLISHED
  TCP    127.0.0.1:9013         Eduardo-PC:49808       ESTABLISHED
  TCP    127.0.0.1:9013         Eduardo-PC:49867       ESTABLISHED
  TCP    127.0.0.1:17532        Eduardo-PC:49818       ESTABLISHED
  TCP    127.0.0.1:27060        Eduardo-PC:57392       ESTABLISHED
```

The **netstat -r** command will display the routing table. Here below you can see the routing table.

```
C:\Users\garci\Desktop\SysinternalsSuite>netstat -r
===========================================================================
Interface List
 12...04 42 1a 06 2a 44 ......Realtek Gaming GbE Family Controller
 22...00 ff ed 1c 6a 65 ......TAP-NordVPN Windows Adapter V9
 23...0a 00 27 00 00 17 ......VirtualBox Host-Only Ethernet Adapter
 19...e8 f4 08 de 07 92 ......Intel(R) Wireless-AC 9260 160MHz
 15...e8 f4 08 de 07 93 ......Microsoft Wi-Fi Direct Virtual Adapter #3
  3...ea f4 08 de 07 92 ......Microsoft Wi-Fi Direct Virtual Adapter #4
  6...e8 f4 08 de 07 96 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.254    192.168.1.198     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link    192.168.1.198    281
    192.168.1.198  255.255.255.255         On-link    192.168.1.198    281
    192.168.1.255  255.255.255.255         On-link    192.168.1.198    281
     192.168.56.0    255.255.255.0         On-link     192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link     192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link     192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link    192.168.1.198    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.56.1    281
  255.255.255.255  255.255.255.255         On-link    192.168.1.198    281
===========================================================================
Persistent Routes:
  None
```

The netstat -b command will display an executable involved with the connection. Here below are the executables that are involved in my PC.

```
C:\Users\garci\Desktop\SysinternalsSuite>netstat -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1042         Eduardo-PC:49789       ESTABLISHED
 [asus_framework.exe]
  TCP    127.0.0.1:1042         Eduardo-PC:49795       ESTABLISHED
 [asus_framework.exe]
  TCP    127.0.0.1:1042         Eduardo-PC:49807       ESTABLISHED
 [asus_framework.exe]
  TCP    127.0.0.1:1042         Eduardo-PC:49866       ESTABLISHED
 [asus_framework.exe]
  TCP    127.0.0.1:9012         Eduardo-PC:49828       ESTABLISHED
 [ArmourySocketServer.exe]
  TCP    127.0.0.1:9013         Eduardo-PC:49808       ESTABLISHED
```

The **netstat -e** command will display the network statistics. You see my network stats below.

```
C:\Users\garci\Desktop\SysinternalsSuite>netstat -e
Interface Statistics

                           Received            Sent

Bytes                    1133807869      1073364033
Unicast packets            14895013         5071213
Non-unicast packets         1051050           50435
Discards                        469               0
Errors                            0               0
Unknown protocols                 0
```

The next task involved using the **tasklist**, **listdlls,** and **handle** commands to collect process information. The tasklist will display the list of tasks that are currently running. The information displayed is the Image name, PID number, Session name, Session#, and Memory Usage. You can see below the list of tasks on my PC.

```
C:\Users\garci\Desktop\SysinternalsSuite>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      3,732 K
Registry                       320 Services                   0     93,436 K
smss.exe                       792 Services                   0      1,368 K
csrss.exe                      988 Services                   0      6,676 K
wininit.exe                   1124 Services                   0      7,272 K
csrss.exe                     1132 Console                    1      7,164 K
services.exe                  1196 Services                   0     11,308 K
lsass.exe                     1204 Services                   0     14,640 K
svchost.exe                   1332 Services                   0     21,528 K
fontdrvhost.exe               1360 Services                   0         64 K
svchost.exe                   1424 Services                   0     13,228 K
svchost.exe                   1480 Services                   0      4,860 K
winlogon.exe                  1532 Console                    1      1,656 K
```

You can also filter tasks based on a specific parameter. You can use the **tasklist /FI "PID gt 320"** to display tasklists that are greater than 320. Note that you can specify the parameters that you want to filter out as well. Here below I display the list of tasks that contains a PID number less than 320.

```
C:\Users\garci\Desktop\SysinternalsSuite>tasklist /FI "PID lt 320"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      3,732 K
```

The **handle** command displays the information about open handles for any process in the system. Here below you can see some open handles for my PC.

```
backgroundTaskHost.exe pid: 3204 EDUARDO-PC\garci
   48: File  (RW-)   C:\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_18.2209.1071.0_x64__8wekyb3d8bbwe
  120: Section       \BaseNamedObjects\__ComCatalogCache__
  204: Section       \Sessions\1\AppContainerNamedObjects\S-1-15-2-930279079-3258969966-1203931420-3379063298-1496040207-3203565093-3038441310\Appli
cationService:c841d8d932b5a213d9
  2A4: File  (R-D)   C:\Windows\System32\en-US\KernelBase.dll.mui
---------------------------------------------------------------------------
RuntimeBroker.exe pid: 25064 EDUARDO-PC\garci
   50: File  (RW-)   C:\Windows\System32
  17C: Section       \BaseNamedObjects\__ComCatalogCache__
  1F0: Section       \BaseNamedObjects\__ComCatalogCache__
  1F4: File  (R--)   C:\Windows\Registration\R00000000000d.clb
  224: File  (R-D)   C:\Windows\System32\en-US\KernelBase.dll.mui
---------------------------------------------------------------------------
handle.exe pid: 28292 EDUARDO-PC\garci
   4C: File  (RW-)   C:\Windows
   A0: File  (RW-)   C:\Users\garci\Desktop\SysinternalsSuite
   E4: File  (RW-)   C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.22000.1_none_6ec7c6847ea94424
```

The **listdlls** command will display the DLLs loaded into processes. Here you can the processes that are loaded with DLLs below.

```
Listdlls64.exe pid: 26548
Command line: listdlls

Base               Size      Path
0x000000002d030000  0x38000   C:\Users\garci\Desktop\SysinternalsSuite\Listdlls64.exe
0x0000000022240000  0x209000  C:\WINDOWS\SYSTEM32\ntdll.dll
0x0000000021210000  0xbd000   C:\WINDOWS\System32\KERNEL32.DLL
0x000000001f9d0000  0x37c000  C:\WINDOWS\System32\KERNELBASE.dll
0x00000000207a0000  0x1f000   C:\WINDOWS\System32\imagehlp.dll
0x000000001ffb0000  0x111000  C:\WINDOWS\System32\ucrtbase.dll
0x0000000017640000  0xa000    C:\WINDOWS\SYSTEM32\VERSION.dll
0x0000000020d70000  0xa3000   C:\WINDOWS\System32\msvcrt.dll
0x000000001f7f0000  0x162000  C:\WINDOWS\System32\CRYPT32.dll
0x0000000020390000  0x1ad000  C:\WINDOWS\System32\USER32.dll
0x000000001f720000  0x26000   C:\WINDOWS\System32\win32u.dll
0x0000000021c20000  0x29000   C:\WINDOWS\System32\GDI32.dll
0x000000001fdd0000  0x119000  C:\WINDOWS\System32\gdi32full.dll
0x000000001f750000  0x9d000   C:\WINDOWS\System32\msvcp_win.dll
0x0000000020f10000  0xec000   C:\WINDOWS\System32\COMDLG32.dll
0x0000000021cc0000  0x379000  C:\WINDOWS\System32\combase.dll
0x00000000200d0000  0x120000  C:\WINDOWS\System32\RPCRT4.dll
0x0000000021000000  0xea000   C:\WINDOWS\System32\shcore.dll
0x00000000213f0000  0x5d000   C:\WINDOWS\System32\SHLWAPI.dll
0x0000000021460000  0x7b8000  C:\WINDOWS\System32\SHELL32.dll
0x000000000f840000  0x2a5000  C:\WINDOWS\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.22000.120_none_9d947278b86cc467\COMCTL3
2.dll
0x0000000020e20000  0xae000   C:\WINDOWS\System32\ADVAPI32.dll
0x0000000020cd0000  0x9e000   C:\WINDOWS\System32\sechost.dll
0x00000000201f0000  0xd6000   C:\WINDOWS\System32\OLEAUT32.dll
0x0000000020ed0000  0x31000   C:\WINDOWS\System32\IMM32.DLL
0x0000000016ba0000  0x221000  C:\WINDOWS\System32\dbghelp.dll
0x000000001fd50000  0x7f000   C:\WINDOWS\System32\bcryptPrimitives.dll
```

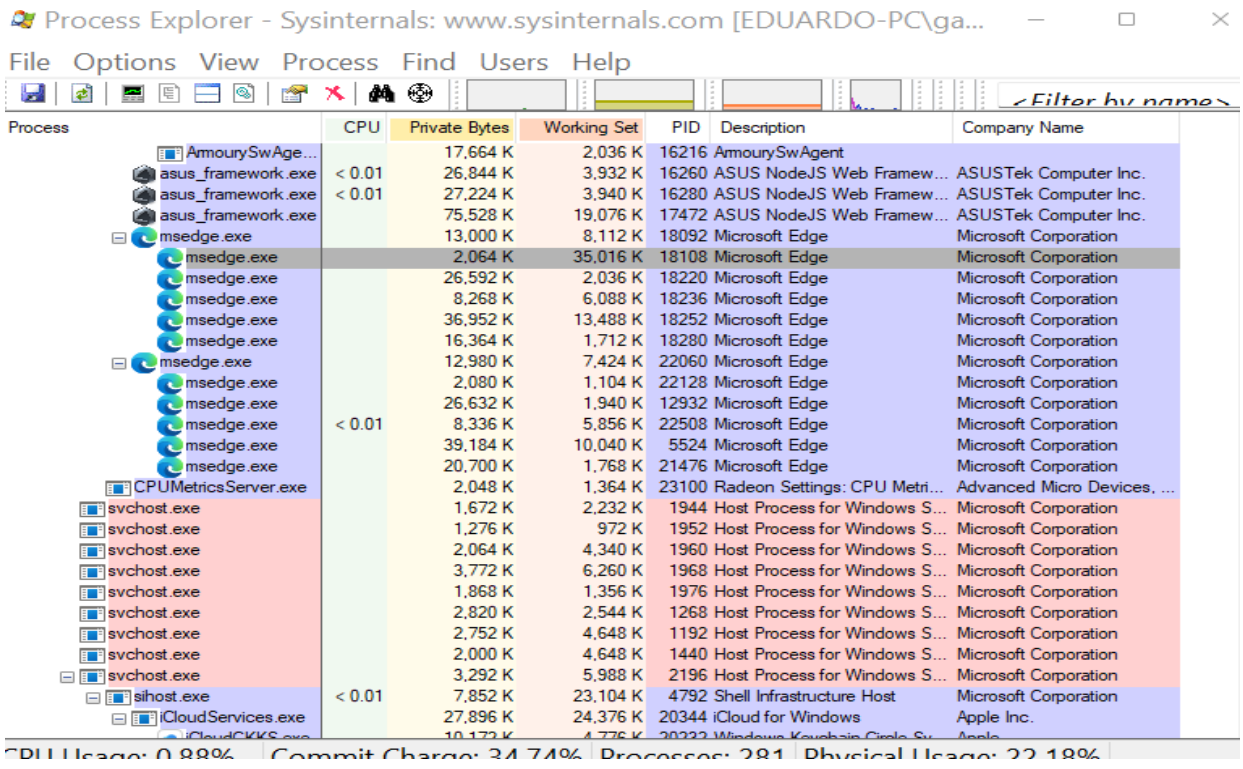
The **pslist** command displays the list of processes that are running in the system.

```
C:\Users\garci\Desktop\SysinternalsSuite>pslist

PsList v1.4 - Process information lister
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for EDUARDO-PC:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0  48    0     60   208:36:49.593     8:53:06.781
System                4   8 347 6750     44     0:17:14.328     8:53:06.781
Registry            320   8   4    0  11452     0:00:00.718     8:53:08.927
smss                792  11   2   57   1136     0:00:00.140     8:53:06.778
csrss               988  13  14  851   2456     0:00:01.781     8:53:03.725
wininit            1124  13   1  148   1432     0:00:00.078     8:53:01.671
csrss              1132  13  16  921  16828     0:00:04.203     8:53:01.668
services           1196   9   9  800   6228     0:00:12.671     8:53:01.625
lsass              1204   9  11 1935  11536     0:00:21.687     8:53:01.597
svchost            1332   8  19 1630  12468     0:00:19.015     8:53:01.470
fontdrvhost        1360   8   5   37   1680     0:00:00.015     8:53:01.461
svchost            1424   8  11 1619  10312     0:00:58.953     8:53:01.414
svchost            1480   8   4  386   3508     0:00:01.296     8:53:01.400
winlogon           1532  13   6  267   2752     0:00:00.140     8:53:01.379
fontdrvhost        1584   8   5   37   5216     0:00:00.625     8:53:01.362
```

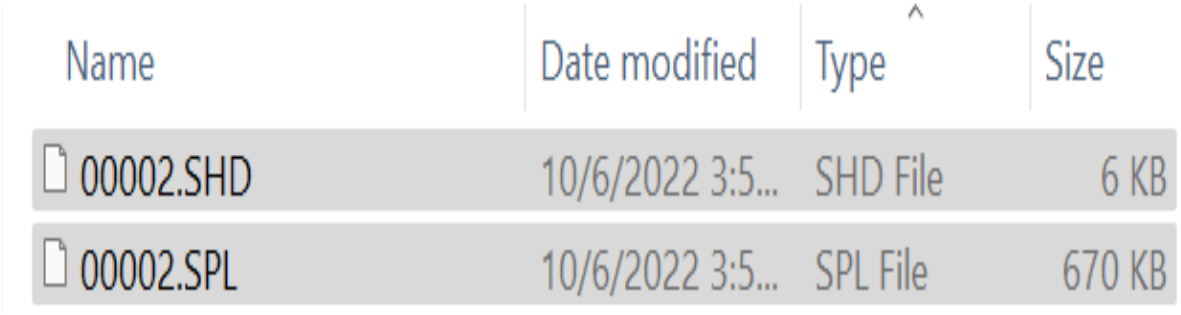
You can also use several other process information such as **pslist -d** command to view information on threads, the **pslist -m** command to view memory information, and the **pslist -x** command to view memory and thread information. Here below is the list meof mory and thread information.

```
C:\Users\garci\Desktop\SysinternalsSuite>pslist -x

PsList v1.4 - Process information lister
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Process and thread information for EDUARDO-PC:

Name                Pid      VM      WS    Priv Priv Pk   Faults   NonP Page
Idle                  0       8       8      60      60        9      0    0
 Tid Pri    Cswtch           State     User Time   Kernel Time   Elapsed Time
   0   0  53285434         Running  0:00:00.000  13:06:13.000    0:00:00.000
   0   0  47002688         Running  0:00:00.000  13:12:50.921    0:00:00.000
   0   0  39902171         Running  0:00:00.000  13:53:26.937    0:00:00.000
   0   0  34613532         Running  0:00:00.000  13:49:49.156    0:00:00.000
   0   0  54725460         Running  0:00:00.000  13:22:23.343    0:00:00.000
   0   0  48035495         Running  0:00:00.000  13:24:17.015    0:00:00.000
   0   0   7929835         Running  0:00:00.000  14:04:07.781    0:00:00.000
```

The another way to view processes by utilizing the **procexp** application. You can create dumps of a given process and analyzing the bits of that process. You can also perform malware analysis on any given processes.



The last task was to examine the print spool files that are located in the **c:\windows\system32\spool\PRINTERS folder.** Here below are the files



Below are the binary values for the SHD and SPL files.