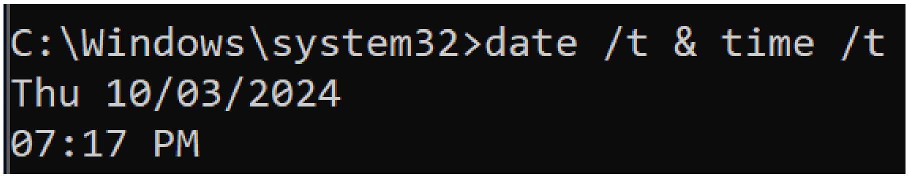
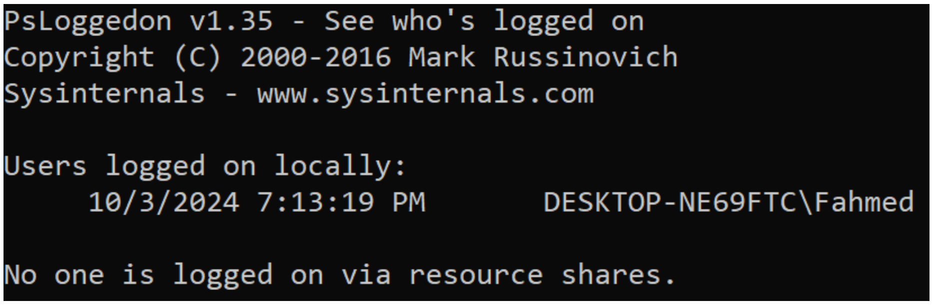


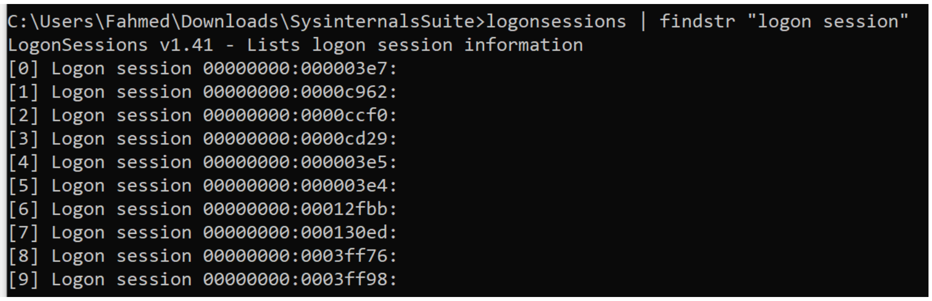
```
C:\Windows\system32>date /t & time /t
Thu 10/03/2024
07:17 PM
```

In the first step, the command date /t & time /t was used to grab the system's current date and time. The screenshot should show something simple, like the date ("Tue 02/15/2022") and the time ("12:41 PM"). This is important in forensics because it sets the timeline for everything else. When you're looking at logs or system events later on, you can match them to this time and date. By getting the time right at the start, investigators make sure they know exactly when everything they do happens.



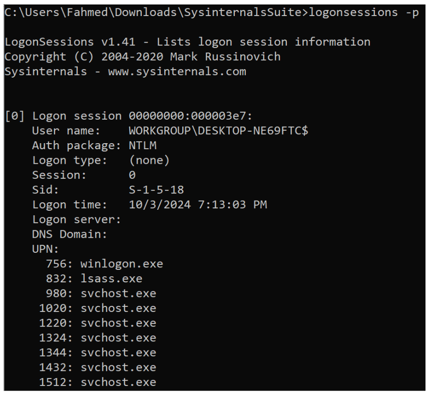
```
PsLoggedon v1.35 - See who's logged on
Copyright (C) 2000-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
     10/3/2024 7:13:19 PM       DESKTOP-NE69FTC\Fahmed

No one is logged on via resource shares.
```

The second command, psloggedon, was used to show all the users currently logged into the system, either locally or remotely. The screenshot should list the user accounts and their login times. This command helps because it tells investigators who's currently using the system, which is key to figuring out if someone's been on there without permission. If you see unexpected users in the output, that's a sign something's wrong, like someone gaining unauthorized access.



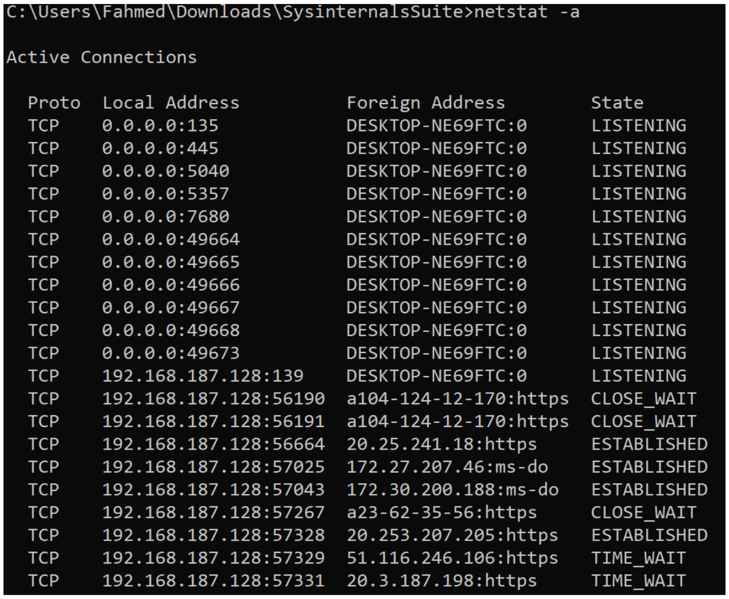
```
C:\Users\Fahmed\Downloads\SysinternalsSuite>logonsessions | findstr "logon session"
LogonSessions v1.41 - Lists logon session information
[0] Logon session 00000000:000003e7:
[1] Logon session 00000000:0000c962:
[2] Logon session 00000000:0000ccf0:
[3] Logon session 00000000:0000cd29:
[4] Logon session 00000000:000003e5:
[5] Logon session 00000000:000003e4:
[6] Logon session 00000000:00012fbb:
[7] Logon session 00000000:000130ed:
[8] Logon session 00000000:0003ff76:
[9] Logon session 00000000:0003ff98:
```

This time, the logonsessions | findstr "logon session" command was run to show all the active logon sessions on the machine. The screenshot should display multiple session IDs and details about who's logged in and what they're doing. The purpose here is to double-check all current sessions to make sure nothing suspicious is going on. Investigators can compare these sessions to normal user activity, and if they find any unexpected ones, that could mean unauthorized access or some sneaky stuff happening.



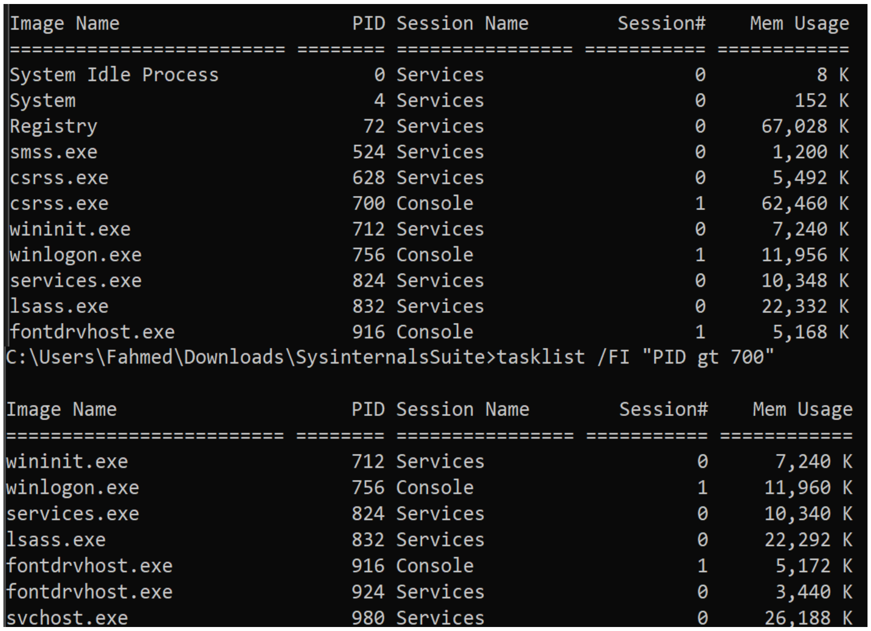
```
C:\Users\Fahmed\Downloads\SysinternalsSuite>logonsessions -p

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\DESKTOP-NE69FTC$
    Auth package: NTLM
    Logon type:   (none)
    Session:      0
    Sid:          S-1-5-18
    Logon time:   10/3/2024 7:13:03 PM
    Logon server:
    DNS Domain:
    UPN:
      756: winlogon.exe
      832: lsass.exe
      980: svchost.exe
     1020: svchost.exe
     1220: svchost.exe
     1324: svchost.exe
     1344: svchost.exe
     1432: svchost.exe
     1512: svchost.exe
```

The command logonsessions -p takes this a step further by adding details about the processes running in each session. The screenshot here would show which programs or services are running under each session, giving you a clearer picture of what each user is doing. This is especially helpful for spotting suspicious processes tied to a user session, like a hidden malware process. It provides a deeper look into each session, making it easier to tell if something abnormal is happening in the background.



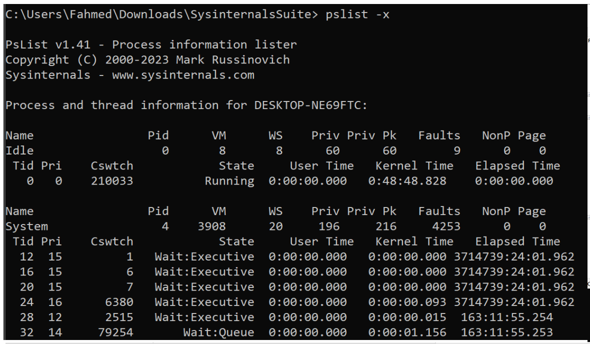
```
C:\Users\Fahmed\Downloads\SysinternalsSuite>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-NE69FTC:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-NE69FTC:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-NE69FTC:0      LISTENING
  TCP    0.0.0.0:5357           DESKTOP-NE69FTC:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-NE69FTC:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-NE69FTC:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-NE69FTC:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-NE69FTC:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-NE69FTC:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-NE69FTC:0      LISTENING
  TCP    0.0.0.0:49673          DESKTOP-NE69FTC:0      LISTENING
  TCP    192.168.187.128:139    DESKTOP-NE69FTC:0      LISTENING
  TCP    192.168.187.128:56190  a104-124-12-170:https  CLOSE_WAIT
  TCP    192.168.187.128:56191  a104-124-12-170:https  CLOSE_WAIT
  TCP    192.168.187.128:56664  20.25.241.18:https     ESTABLISHED
  TCP    192.168.187.128:57025  172.27.207.46:ms-do    ESTABLISHED
  TCP    192.168.187.128:57043  172.30.200.188:ms-do   ESTABLISHED
  TCP    192.168.187.128:57267  a23-62-35-56:https     CLOSE_WAIT
  TCP    192.168.187.128:57328  20.253.207.205:https   ESTABLISHED
  TCP    192.168.187.128:57329  51.116.246.106:https   TIME_WAIT
  TCP    192.168.187.128:57331  20.3.187.198:https     TIME_WAIT
```

Next, the netstat -a command was used to get a list of all the active network connections. The screenshot will show things like local and foreign addresses, and the state of the connections (e.g., ESTABLISHED, LISTENING). This step is super useful because it helps you figure out if the system is talking to any weird or unapproved servers. If the output shows connections to IP addresses you don’t recognize, it could be a sign of malware communicating with its command and control server, or worse, someone stealing data.

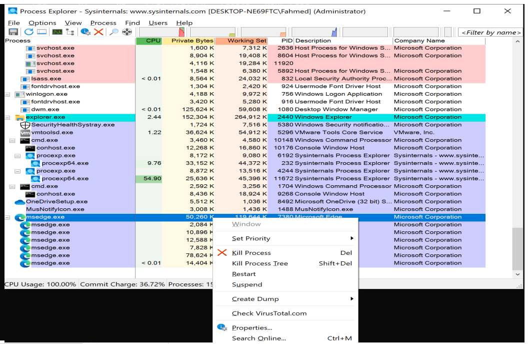


```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        152 K
Registry                        72 Services                   0     67,028 K
smss.exe                       524 Services                   0      1,200 K
csrss.exe                      628 Services                   0      5,492 K
csrss.exe                      700 Console                    1     62,460 K
wininit.exe                    712 Services                   0      7,240 K
winlogon.exe                   756 Console                    1     11,956 K
services.exe                   824 Services                   0     10,348 K
lsass.exe                      832 Services                   0     22,332 K
fontdrvhost.exe                916 Console                    1      5,168 K
C:\Users\Fahmed\Downloads\SysinternalsSuite>tasklist /FI "PID gt 700"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
wininit.exe                    712 Services                   0      7,240 K
winlogon.exe                   756 Console                    1     11,960 K
services.exe                   824 Services                   0     10,340 K
lsass.exe                      832 Services                   0     22,292 K
fontdrvhost.exe                916 Console                    1      5,172 K
fontdrvhost.exe                924 Services                   0      3,440 K
svchost.exe                    980 Services                   0     26,188 K
```

For this step, the tasklist command was used to list all the running processes, their PIDs, and how much memory each one is using. The screenshot will show a table with the active processes, including important system services and other applications. This helps investigators see what’s currently running on the machine, which is crucial when looking for malicious software. Any unknown or sketchy processes can be a red flag, especially if they’re using a lot of memory or CPU. Filtering the processes with tasklist /FI "PID gt 700" helps narrow it down and makes it easier to focus on important ones.



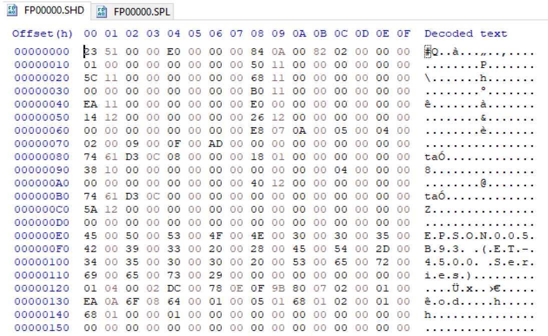
```
C:\Users\Fahmed\Downloads\SysinternalsSuite> pslist -x

PsList v1.41 - Process information lister
Copyright (C) 2000-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Process and thread information for DESKTOP-NE69FTC:

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    210033          Running  0:00:00.000   0:48:48.828    0:00:00.000

Name                Pid      VM     WS    Priv Priv Pk   Faults   NonP Page
System                4    3908     20     196     216     4253      0    0
 Tid Pri    Cswtch            State     User Time   Kernel Time   Elapsed Time
  12  15         1   Wait:Executive  0:00:00.000   0:00:00.000 3714739:24:01.962
  16  15         6   Wait:Executive  0:00:00.000   0:00:00.000 3714739:24:01.962
  20  15         7   Wait:Executive  0:00:00.000   0:00:00.000 3714739:24:01.962
  24  16      6380   Wait:Executive  0:00:00.000   0:00:00.093 3714739:24:01.962
  28  12      2515   Wait:Executive  0:00:00.000   0:00:00.015  163:11:55.254
  32  14     79254       Wait:Queue  0:00:00.000   0:00:01.156  163:11:55.253
```



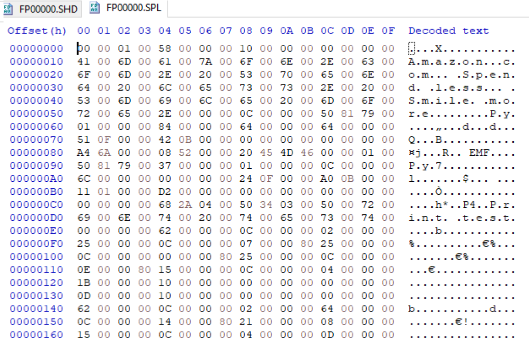
Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-NE69FTC\Fahmed] (Administrator)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		1,600 K	7,312 K	2636	Host Process for Windows S...	Microsoft Corporation
svchost.exe		8,904 K	19,408 K	8604	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,116 K	19,284 K	11920		
svchost.exe		1,548 K	6,380 K	5892	Host Process for Windows S...	Microsoft Corporation
lsass.exe	< 0.01	8,564 K	24,032 K	832	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe		1,304 K	2,420 K	924	Usermode Font Driver Host	Microsoft Corporation
winlogon.exe		4,188 K	9,972 K	756	Windows Logon Application	Microsoft Corporation
fontdrvhost.exe		3,420 K	5,280 K	916	Usermode Font Driver Host	Microsoft Corporation
dwm.exe	< 0.01	125,624 K	59,608 K	1080	Desktop Window Manager	Microsoft Corporation
explorer.exe	2.44	152,304 K	264,912 K	2440	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,724 K	7,516 K	5380	Windows Security notificatio...	Microsoft Corporation
vmtoolsd.exe	1.22	36,624 K	54,912 K	5296	VMware Tools Core Service	VMware, Inc.
cmd.exe		3,460 K	4,580 K	10148	Windows Command Processor	Microsoft Corporation
conhost.exe		12,268 K	16,860 K	10176	Console Window Host	Microsoft Corporation
procexp.exe		8,172 K	9,080 K	6192	Sysinternals Process Explorer	Sysinternals - www.sysinte...
procexp64.exe	9.76	33,152 K	44,372 K	232	Sysinternals Process Explorer	Sysinternals - www.sysinte...
procexp.exe		8,872 K	13,516 K	4244	Sysinternals Process Explorer	Sysinternals - www.sysinte...
procexp64.exe	54.90	25,636 K	45,396 K	11672	Sysinternals Process Explorer	Sysinternals - www.sysinte...
cmd.exe		2,592 K	3,256 K	1704	Windows Command Processor	Microsoft Corporation
conhost.exe		8,436 K	18,924 K	9268	Console Window Host	Microsoft Corporation
OneDriveSetup.exe		5,512 K	1,036 K	8492	Microsoft OneDrive (32 bit) S...	Microsoft Corporation
MusNotifyIcon.exe		3,008 K	1,436 K	1488	MusNotifyIcon.exe	Microsoft Corporation
msedge.exe		50,260 K	119,644 K	7380	Microsoft Edge	Microsoft Corporation
msedge.exe		2,084 K				Microsoft Corporation
msedge.exe		10,896 K				Microsoft Corporation
msedge.exe		12,588 K				Microsoft Corporation
msedge.exe		7,828 K				Microsoft Corporation
msedge.exe		78,624 K				Microsoft Corporation
msedge.exe	< 0.01	14,404 K				Microsoft Corporation

CPU Usage: 100.00% Commit Charge: 36.72% Processes: 15



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  23 51 00 00 E0 00 00 00 84 0A 00 82 02 00 00 00  #Q..à...„..‚....
00000010  01 00 00 00 00 00 00 00 50 11 00 00 00 00 00 00  ........P.......
00000020  5C 11 00 00 00 00 00 00 68 11 00 00 00 00 00 00  \.......h.......
00000030  00 00 00 00 00 00 00 00 B0 11 00 00 00 00 00 00  ........°.......
00000040  EA 11 00 00 00 00 00 00 E0 00 00 00 00 00 00 00  ê.......à.......
00000050  14 12 00 00 00 00 00 00 26 12 00 00 00 00 00 00  ........&.......
00000060  00 00 00 00 00 00 00 00 E8 07 0A 00 05 00 04 00  ........è.......
00000070  02 00 09 00 0F 00 AD 00 00 00 00 00 00 00 00 00  ................
00000080  74 61 D3 0C 08 00 00 00 18 01 00 00 00 00 00 00  taÓ.............
00000090  38 10 00 00 00 00 00 00 00 00 00 00 04 00 00 00  8...............
000000A0  00 00 00 00 00 00 00 00 40 12 00 00 00 00 00 00  ........@.......
000000B0  74 61 D3 0C 00 00 00 00 00 00 00 00 00 00 00 00  taÓ.............
000000C0  5A 12 00 00 00 00 00 00 00 00 00 00 00 00 00 00  Z...............
000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000E0  45 00 50 00 53 00 4F 00 4E 00 30 00 30 00 35 00  E.P.S.O.N.0.0.5.
000000F0  42 00 39 00 33 00 20 00 28 00 45 00 54 00 2D 00  B.9.3. .(.E.T.-.
00000100  34 00 35 00 30 00 30 00 20 00 53 00 65 00 72 00  4.5.0.0. .S.e.r.
00000110  69 00 65 00 73 00 29 00 00 00 00 00 00 00 00 00  i.e.s.).........
00000120  01 04 00 02 DC 00 78 0E 0F 9B 80 07 02 00 01 00  ....Ü.x..›€.....
00000130  EA 0A 6F 08 64 00 01 00 05 01 68 01 02 00 01 00  ê.o.d.....h.....
00000140  68 01 00 00 01 00 00 00 00 00 00 00 00 00 00 00  h...............
00000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  00 00 01 00 58 00 00 00 10 00 00 00 00 00 00 00  ....X...........
00000010  41 00 6D 00 61 00 7A 00 6F 00 6E 00 2E 00 63 00  A.m.a.z.o.n...c.
00000020  6F 00 6D 00 2E 00 20 00 53 00 70 00 65 00 6E 00  o.m... .S.p.e.n.
00000030  64 00 20 00 6C 00 65 00 73 00 73 00 2E 00 20 00  d. .l.e.s.s... .
00000040  53 00 6D 00 69 00 6C 00 65 00 20 00 6D 00 6F 00  S.m.i.l.e. .m.o.
00000050  72 00 65 00 2E 00 00 00 0C 00 00 00 50 81 79 00  r.e.........P.y.
00000060  01 00 00 00 84 00 00 00 64 00 00 00 64 00 00 00  ....„...d...d...
00000070  51 0F 00 00 42 0B 00 00 00 00 00 00 00 00 00 00  Q...B...........
00000080  A4 6A 00 00 08 52 00 00 20 45 4D 46 00 00 01 00  ¤j...R.. EMF....
00000090  50 81 79 00 37 00 00 00 01 00 00 00 0C 00 00 00  P.y.7...........
000000A0  6C 00 00 00 00 00 00 00 24 0F 00 00 A0 0B 00 00  l.......$... ...
000000B0  11 01 00 00 D2 00 00 00 00 00 00 00 00 00 00 00  ....Ò...........
000000C0  00 00 00 00 68 2A 04 00 50 34 03 00 50 00 72 00  ....h*..P4..P.r.
000000D0  69 00 6E 00 74 00 20 00 74 00 65 00 73 00 74 00  i.n.t. .t.e.s.t.
000000E0  00 00 00 00 62 00 00 00 0C 00 00 00 02 00 00 00  ....b...........
000000F0  25 00 00 00 0C 00 00 00 07 00 00 80 25 00 00 00  %..........€%...
00000100  0C 00 00 00 00 00 00 80 25 00 00 00 0C 00 00 00  .......€%.......
00000110  0E 00 00 80 15 00 00 00 0C 00 00 00 04 00 00 00  ...€............
00000120  1B 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
00000130  0D 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
00000140  62 00 00 00 0C 00 00 00 02 00 00 00 64 00 00 00  b...........d...
00000150  0C 00 00 00 14 00 00 80 21 00 00 00 08 00 00 00  .......€!.......
00000160  15 00 00 00 0C 00 00 00 04 00 00 00 0D 00 00 00  ................
```

In Step 6, I used the pslist -x command to check out more detailed info about the running processes, like how much memory they were using, how many threads they had, and how long they'd been running. The screenshot showed a table listing each process's ID, memory usage, and thread details, along with how long each process had been active. This was super helpful for spotting anything weird, like processes using too much memory or having a lot of threads, which could mean something suspicious was going on. I used pslist -x to get a deeper look at what each process was doing, so I could catch anything that might be hiding in the system. Along with that, I used HxD, a hex editor, to dive into the raw memory data of a process. The screenshot from HxD showed the contents of a process's memory, letting me look for hidden malware, encryption keys, or other suspicious stuff. HxD was really useful for checking out the memory itself, where I could see things like passwords or malware signatures that wouldn't show up in a regular process list. By using both pslist -x and HxD together, I was able to get a really detailed look at the processes and figure out if any of them were hiding something bad or using too many system resources. This was a key part of my forensic work, helping me spot malware or sneaky processes trying to avoid detection.

Executive Summary: In this lab, we worked on collecting information from a Windows system to check for any suspicious activity or unauthorized access. We used various commands to gather details like the current time and date, who was logged in, what network connections were active, and what processes were running. This helped us get a clear picture of who was using the system, what they were doing, and whether anything unusual was happening with the processes or connections. I also used a tool called HxD to dig deeper into the system's memory, which allowed us to search for hidden data or malware that might not be obvious just by looking at the process list. The goal of all these steps was to create a snapshot of the system while it was running, which is important for investigating potential security issues. By looking at who was logged in, what programs were running, and how the system was connected to the network, we could spot anything out of place. Overall, this lab helped us understand how to gather and analyze system data, which is key for figuring out if something suspicious or harmful is happening.