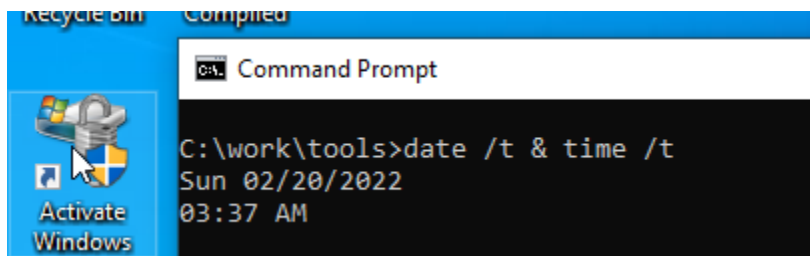


TASK 1: COLLECTING VOLATILE INFORMATION

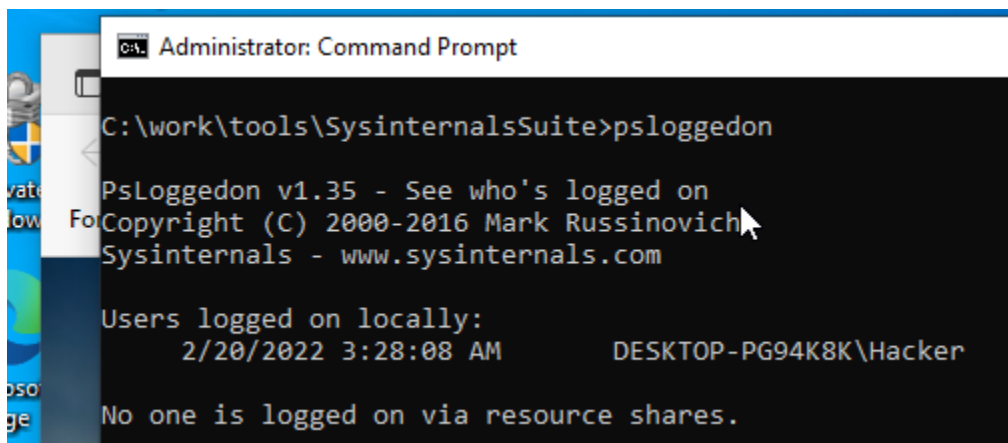
Part 1:



To see the date and time of our machine we use this command ***"date /t & time /t"***

- ➔ ***date*** gives us date
- ➔ ***/t*** shifts to next line
- ➔ ***&*** is used to put another command
- ➔ ***time*** gives us current time

Part 2:



Okay so we have installed tools that are going to show us computer features. Here we are using *psloggedon* tool to see the current logged in user

Part 3:

```
C:\work\tools\SysinternalsSuite>logonsessions |findstr "logon session"
LogonSessions v1.41 - Lists logon session information
[0] Logon session 00000000:000003e7:
[1] Logon session 00000000:00005fa3:
[2] Logon session 00000000:0000694d:
[3] Logon session 00000000:0000695d:
[4] Logon session 00000000:000003e4:
[5] Logon session 00000000:0000bad5:
[6] Logon session 00000000:0000bb01:
[7] Logon session 00000000:000003e5:
[8] Logon session 00000000:000459bc:
[9] Logon session 00000000:000459f5:
```

Here we are able to see how many active logon sessions are created and managed by Local Security Authority(LSA).

We have used findstr to only show us the IDS of the sessions

```
C:\work\tools\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-PG94K8K$
    Auth package:   NTLM
    Logon type:     (none)
    Session:        0
    Sid:            S-1-5-18
    Logon time:     2/20/2022 3:27:34 AM
    Logon server:
    DNS Domain:
    UPN:
        596: winlogon.exe
        688: lsass.exe
        792: svchost.exe
        880: svchost.exe
        984: svchost.exe
        708: svchost.exe
        1244: svchost.exe
        1288: svchost.exe
        1304: svchost.exe
        1472: svchost.exe
        1512: svchost.exe
```

-p flag is used to list down all the processes running on each session.

Part 4:

```
For C:\work\tools\SysinternalsSuite>netstat -a
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	DESKTOP-PG94K8K:0	LISTENING
TCP	0.0.0.0:445	DESKTOP-PG94K8K:0	LISTENING
TCP	0.0.0.0:5040	DESKTOP-PG94K8K:0	LISTENING
TCP	0.0.0.0:7680	DESKTOP-PG94K8K:0	LISTENING
TCP	0.0.0.0:49664	DESKTOP-PG94K8K:0	LISTENING
TCP	0.0.0.0:49665	DESKTOP-PG94K8K:0	LISTENING
TCP	0.0.0.0:49666	DESKTOP-PG94K8K:0	LISTENING
TCP	0.0.0.0:49667	DESKTOP-PG94K8K:0	LISTENING
TCP	0.0.0.0:49668	DESKTOP-PG94K8K:0	LISTENING
TCP	0.0.0.0:49669	DESKTOP-PG94K8K:0	LISTENING
TCP	0.0.0.0:49670	DESKTOP-PG94K8K:0	LISTENING
TCP	0.0.0.0:56381	DESKTOP-PG94K8K:0	LISTENING
TCP	127.0.0.1:10801	DESKTOP-PG94K8K:0	LISTENING
TCP	127.0.0.1:19050	DESKTOP-PG94K8K:0	LISTENING
TCP	127.0.0.1:49721	DESKTOP-PG94K8K:0	LISTENING
TCP	127.0.0.1:49725	DESKTOP-PG94K8K:58049	ESTABLISHED
TCP	127.0.0.1:49890	DESKTOP-PG94K8K:49891	ESTABLISHED
TCP	127.0.0.1:49891	DESKTOP-PG94K8K:49890	ESTABLISHED

“**netstat**” is a command line utility used to see network statistics, for example list down all the connections that have been established by the user

```
For C:\work\tools\SysinternalsSuite>tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	144 K
Registry	100	Services	0	72,412 K
smss.exe	348	Services	0	1,212 K
csrss.exe	444	Services	0	5,204 K
wininit.exe	520	Services	0	6,944 K
csrss.exe	536	Console	1	5,468 K
winlogon.exe	596	Console	1	11,524 K
services.exe	664	Services	0	9,576 K
lsass.exe	688	Services	0	18,380 K
svchost.exe	792	Services	0	3,344 K
fontdrvhost.exe	800	Services	0	3,408 K
fontdrvhost.exe	808	Console	1	6,256 K
svchost.exe	880	Services	0	26,684 K
svchost.exe	932	Services	0	13,788 K
svchost.exe	984	Services	0	7,528 K
dwm.exe	376	Console	1	71,984 K
svchost.exe	708	Services	0	9,680 K
svchost.exe	1112	Services	0	6,056 K
svchost.exe	1120	Services	0	5,380 K
svchost.exe	1128	Services	0	20,220 K

"tasklist" is a command line utility that displays running processes on a computer

```
C:\work\tools\SysinternalsSuite>tasklist /FI "PID gt 700"
```

Image Name	PID	Session Name	Session#	Mem Usage
svchost.exe	792	Services	0	3,344 K
fontdrvhost.exe	800	Services	0	3,408 K
fontdrvhost.exe	808	Console	1	6,260 K
svchost.exe	880	Services	0	26,684 K
svchost.exe	932	Services	0	13,788 K
svchost.exe	984	Services	0	7,544 K
svchost.exe	708	Services	0	9,680 K
svchost.exe	1112	Services	0	6,056 K
svchost.exe	1120	Services	0	5,380 K
svchost.exe	1128	Services	0	20,216 K
svchost.exe	1244	Services	0	13,360 K
svchost.exe	1260	Services	0	7,628 K
svchost.exe	1288	Services	0	5,812 K
svchost.exe	1304	Services	0	63,164 K
svchost.exe	1336	Services	0	11,660 K
Memory Compression	1452	Services	0	15,176 K
svchost.exe	1464	Services	0	7,120 K

/FI flag is used to filter the processes, "PID gt 700" It is going to show processes having PID(process id) greater than 700

Task 5:

```
C:\work\tools\SysinternalsSuite>pslist -x
```

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

Process and thread information for DESKTOP-PG94K8K:

Name	Pid	VM	WS	Priv	Priv	Pk	Faults	NonP	Page
Idle	0	8	8	60	60	60	9	0	0
Tid Pri	Cswtch	State	User Time	Kernel Time	Elapsed Time				
0 0	434774	Running	0:00:00.000	0:26:03.531	0:00:00.000				
0 0	816622	Running	0:00:00.000	0:23:46.890	0:00:00.000				
0 0	523241	Running	0:00:00.000	0:18:00.890	0:00:00.000				

Name	Pid	VM	WS	Priv	Priv	Pk	Faults	NonP	Page
System	4	3896	144	196	216	2545		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	0:00:00.000				
16 15	3	Wait:Executive	0:00:00.000	0:00:00.000	0:00:00.000				
20 13	5	Wait:Executive	0:00:00.000	0:00:00.000	0:00:00.000				
24 16	1110	Wait:Executive	0:00:00.000	0:00:00.046	0:00:00.000				
28 12	75	Wait:Executive	0:00:00.000	0:00:00.015	0:32:19.245				
36 9	13159	Wait:Queue	0:00:00.000	0:00:00.078	0:32:19.245				
40 31	1	Wait:Suspended	0:00:00.000	0:00:00.000	0:32:19.245				
44 31	1	Wait:Suspended	0:00:00.000	0:00:00.000	0:32:19.245				

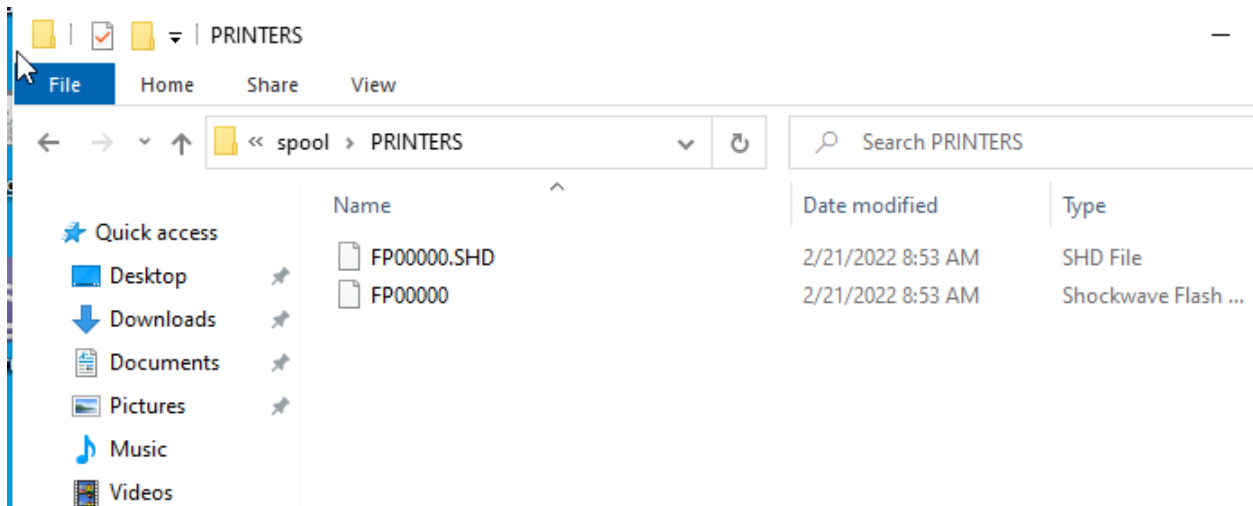
***Pslist** is a tool that is used to display information about CPU usage and the processes running on the computer*

The screenshot shows the Windows Task Manager interface. The 'Process Explorer' window is open, displaying a list of processes. The 'Create Dump' menu is open, showing options like 'Create Minidump...', 'Create Full Dump...', 'Kill Process', 'Kill Process Tree', 'Restart', 'Suspend', 'Properties...', and 'Search Online...'. The CPU usage is 25.71% and Physical Usage is 44.16%.

Name	Tid	P	Process	CPU	Private Bytes	Working Set	PID	Description
6004	8	8	Wait:Queue	0:00:00.000	0:00:00.000	0:00:09.304		
1580			svchost.exe		2,608 K	11,704 K	1492	Host Process for Windows S
6580			svchost.exe		2,376 K	9,044 K	5068	Host Process for Windows S
5560			svchost.exe		3,296 K	11,172 K	6688	Host Process for Windows S
For3780			svchost.exe		1,572 K	9,152 K	312	Host Process for Windows S
			lsass.exe	< 0.01	6,832 K	18,444 K	688	Local Security Authority Proc
			fontdrvhost.exe	< 0.01	1,272 K	3,424 K	800	Usemode Font Driver Host
			csrss.exe	< 0.01	1,868 K	5,504 K	536	Client Server Runtime Proce
			winlogon.exe		2,764 K	11,588 K	596	Windows Logon Application
			fontdrvhost.exe		3,636 K	8,420 K	808	Usemode Font Driver Host
			dwm.exe	< 0.01	39,400 K	75,352 K	376	Desktop Window Manager
			explorer.exe	0.49	627,452 K	710,060 K	4420	Windows Explorer
			SecurityHealthSystray.exe		1,672 K	8,988 K	628	Windows Security notificatio
			msedge.exe	< 0.01	39,280 K	122,688 K	5336	Microsoft Edge
			msedge.exe		1,944 K	7,284 K	4608	Microsoft Edge
			msedge.exe	< 0.01	108,072 K	52,904 K	6180	Microsoft Edge
			msedge			32,864 K	6192	Microsoft Edge
			msedge			18,088 K	6328	Microsoft Edge
			msedge			190,508 K	6832	Microsoft Edge
			msedge			70,372 K	2964	Microsoft Edge
			msedge			28,668 K	1032	Microsoft Edge
			BitTorrent.exe		37,752 K		2424	BitTorrent
			bittorrent		86,988 K		7140	WebHelper
			bittorrent		13,384 K		5812	WebHelper
			helper.e		14,604 K		6372	µTorrent Helper
			cmd.exe		5,544 K		1020	Windows Command Process
			conhost		21,192 K		1300	Console Window Host
			procexp					Process Explorer
			proc					Process Explorer

*We can use the tool called **procexp** that can create full memory dump of a single process which can be used further in Malware Analysis*

Task 6:



In this step we only saw that printer's files are stored at this specific location

SUMMARY

This whole lab was about collecting volatile information. First of all, we saw how to check date and time and the user connected to the computer. After that we saw the network connections that are established with our computer using "netstat" command. We also got to know about "tasklist", "pslist" commands that gave us information related to tasks and processes running on our Windows, At last we saw where our printer files are stored once they are printed.