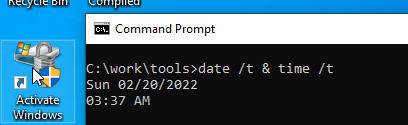
Windows Forensics

TASK 1: Collecting Volatile Information

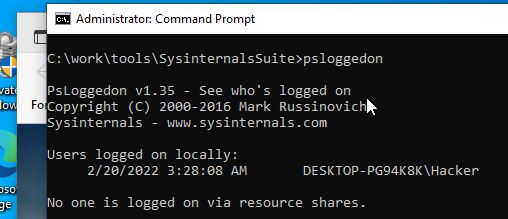
Part 1:



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

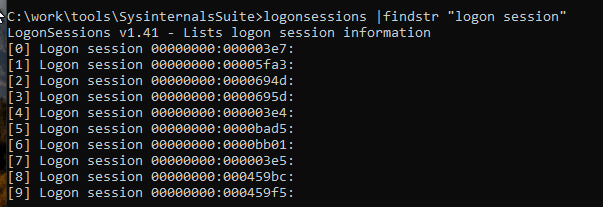
* **date** gives us date
* **/t** shifts to next line
* **&** is used to put another command
* **tim**e gives us current time

Part 2:



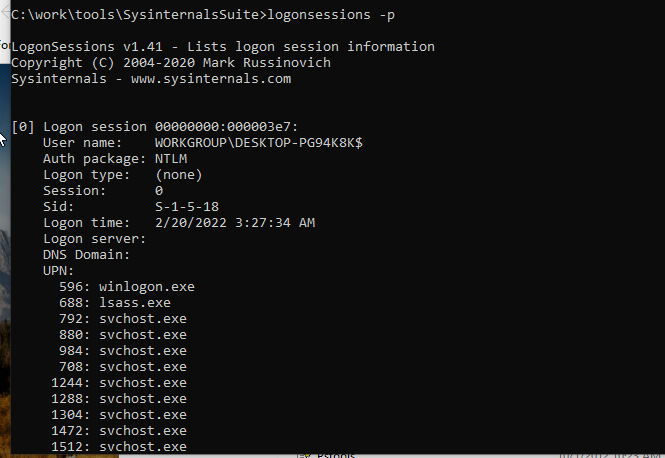
Okay so we have installed tools that are going to show us computer features. Here we are using psloggedon tool to see the current logged in user

Part 3:



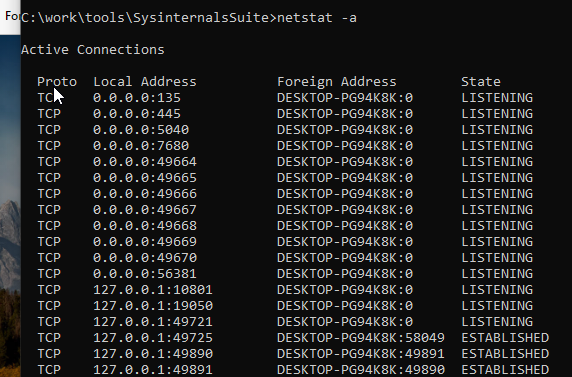
Here we are able to see how many active logon sessions are created and managed by Local Security Authority(**LSA**).

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

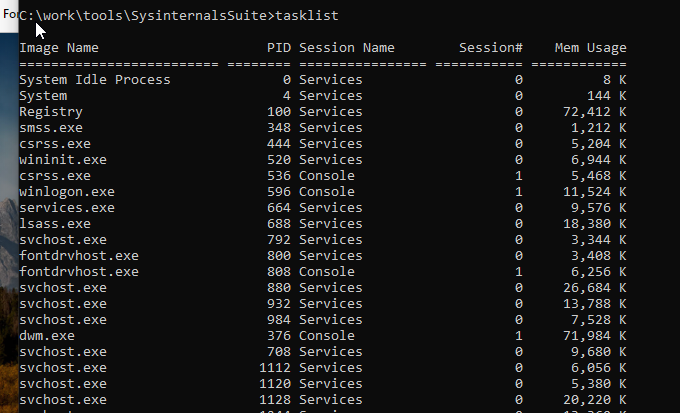


**-p** flag is used to list down all the processes running on each session.

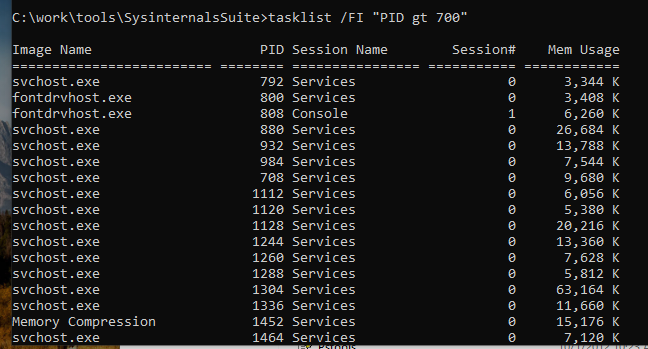
Part 4:



“**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

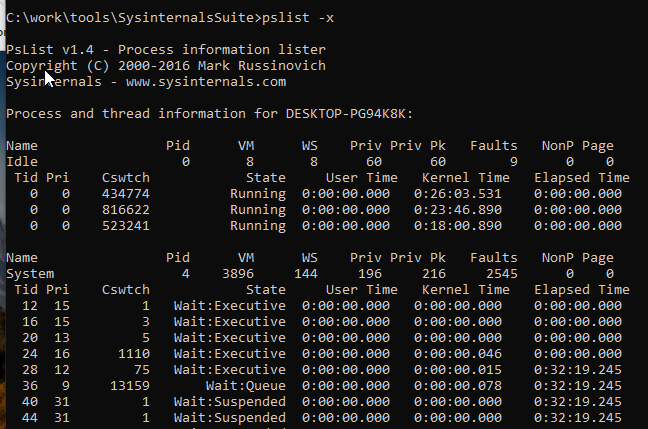


“**tasklist**” is a command line utility that displays running processes on a computer

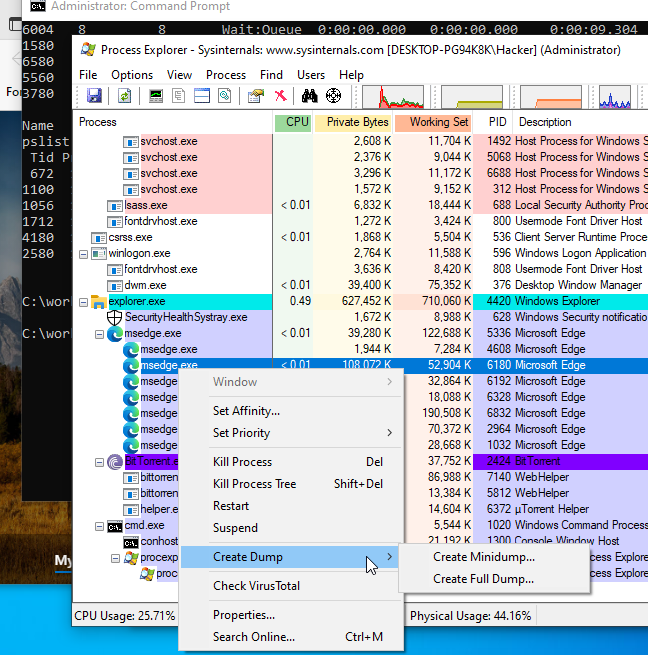


**/FI** flag is used to filter the processes, “**PID gt 700**” It is going to show processes having PID(process id) greater than 700

Task 5:

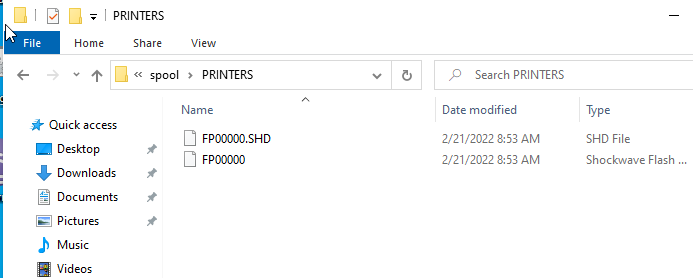


**Pslist** is a tool that is used to display information about CPU usage and the processes running on the computer



We can use the tool called **procexp** that can create full memory dump of a single process which can 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.