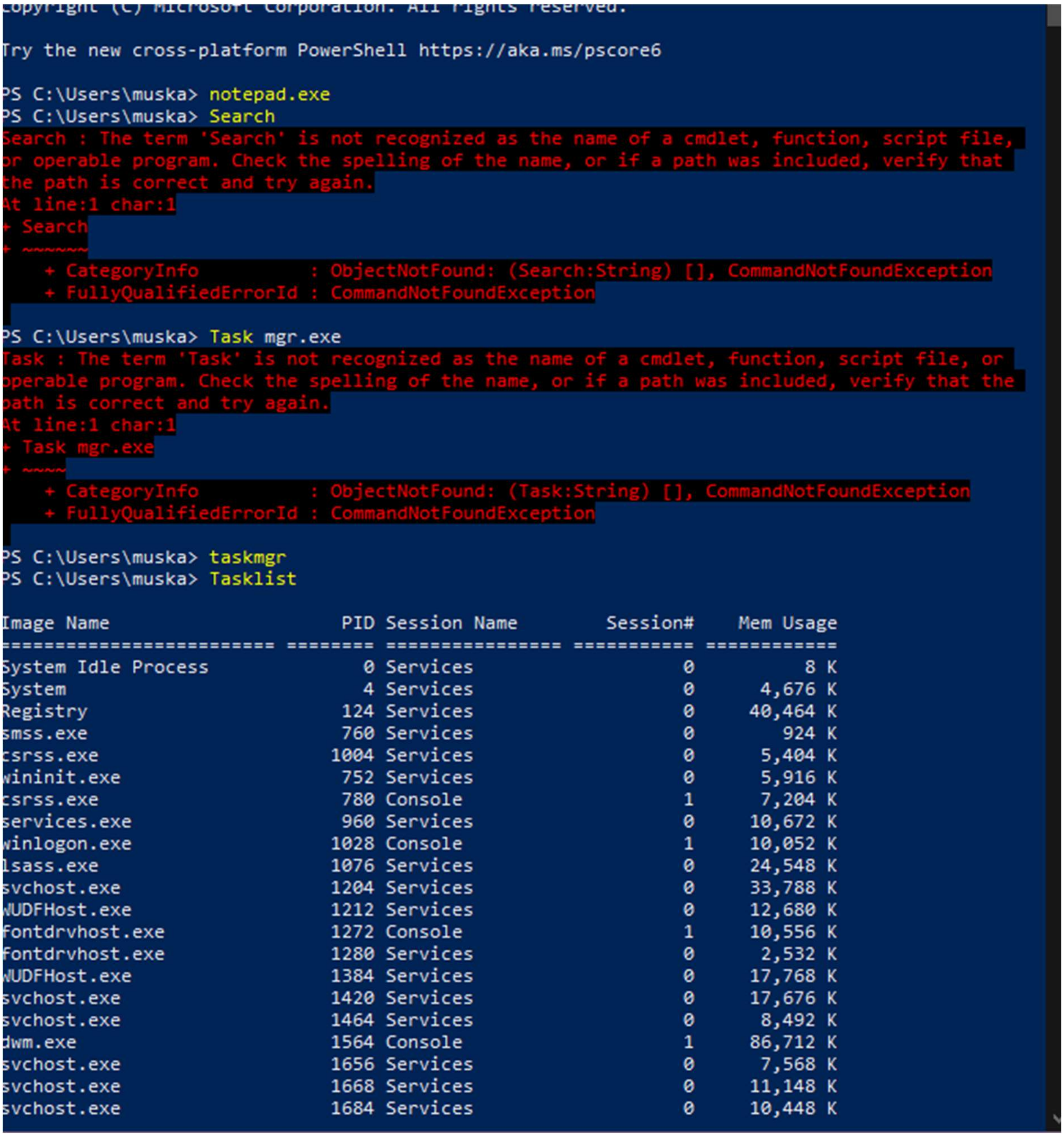
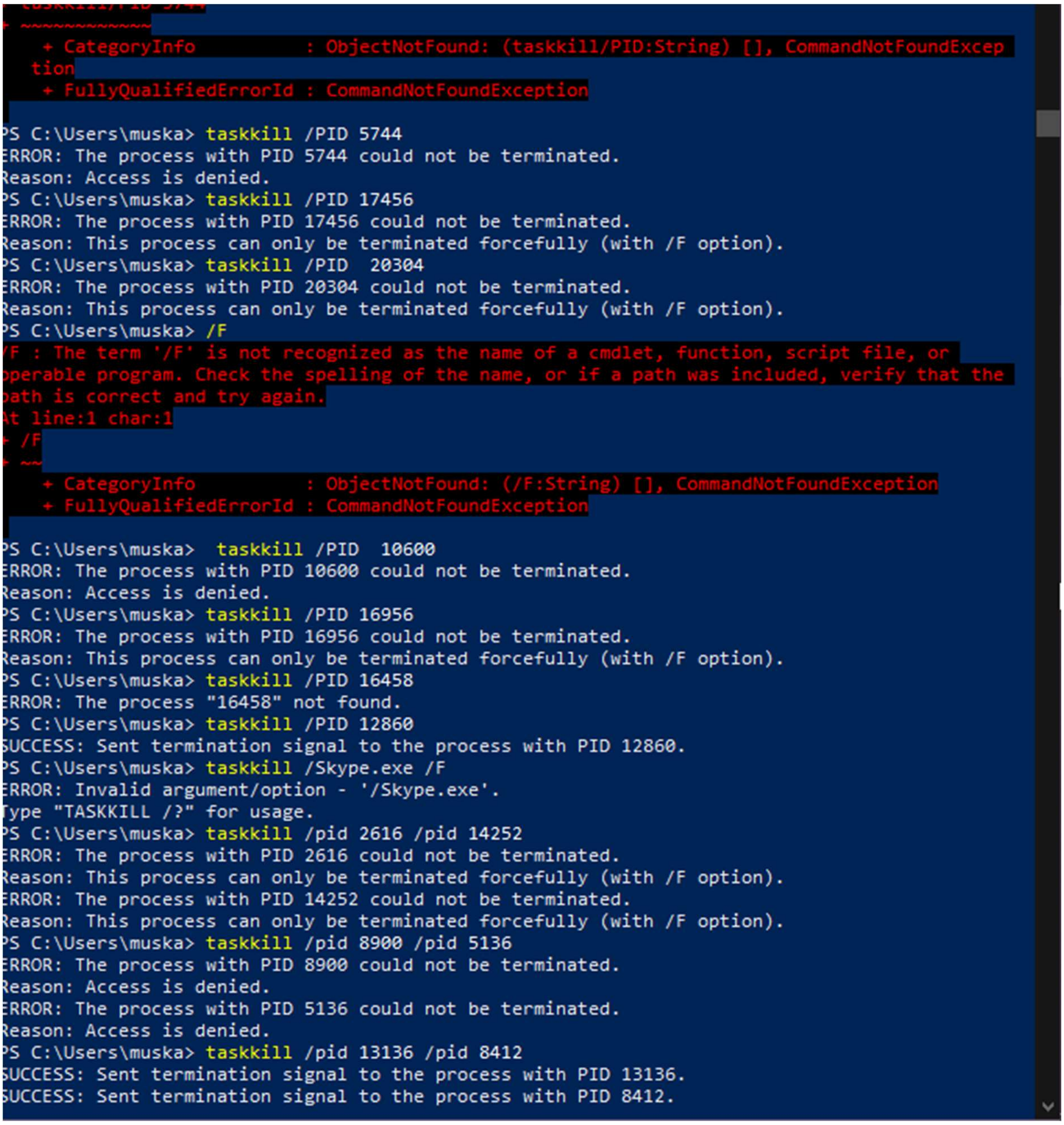
Module 2

Submitted by – Muskaan Sharma RA1811033010008

ASSIGNMENT 2 - Using Logs to Help You Track Down an Issue in Windows



```
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\muska> notepad.exe
PS C:\Users\muska> Search
Search : The term 'Search' is not recognized as the name of a cmdlet, function, script file,
or operable program. Check the spelling of the name, or if a path was included, verify that
the path is correct and try again.
At line:1 char:1
+ Search
+ ~~~~~~
    + CategoryInfo          : ObjectNotFound: (Search:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\muska> Task mgr.exe
Task : The term 'Task' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the
path is correct and try again.
At line:1 char:1
+ Task mgr.exe
+ ~~~~
    + CategoryInfo          : ObjectNotFound: (Task:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\muska> taskmgr
PS C:\Users\muska> Tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      4,676 K
Registry                       124 Services                   0     40,464 K
smss.exe                       760 Services                   0        924 K
csrss.exe                     1004 Services                   0      5,404 K
wininit.exe                    752 Services                   0      5,916 K
csrss.exe                      780 Console                    1      7,204 K
services.exe                   960 Services                   0     10,672 K
winlogon.exe                  1028 Console                    1     10,052 K
lsass.exe                     1076 Services                   0     24,548 K
svchost.exe                   1204 Services                   0     33,788 K
WUDFHost.exe                  1212 Services                   0     12,680 K
fontdrvhost.exe               1272 Console                    1     10,556 K
fontdrvhost.exe               1280 Services                   0      2,532 K
WUDFHost.exe                  1384 Services                   0     17,768 K
svchost.exe                   1420 Services                   0     17,676 K
svchost.exe                   1464 Services                   0      8,492 K
dwm.exe                       1564 Console                    1     86,712 K
svchost.exe                   1656 Services                   0      7,568 K
svchost.exe                   1668 Services                   0     11,148 K
svchost.exe                   1684 Services                   0     10,448 K
```



```
+ taskkill/PID 5744
+ ~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (taskkill/PID:String) [], CommandNotFoundExcep
   tion
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\muska> taskkill /PID 5744
ERROR: The process with PID 5744 could not be terminated.
Reason: Access is denied.
PS C:\Users\muska> taskkill /PID 17456
ERROR: The process with PID 17456 could not be terminated.
Reason: This process can only be terminated forcefully (with /F option).
PS C:\Users\muska> taskkill /PID  20304
ERROR: The process with PID 20304 could not be terminated.
Reason: This process can only be terminated forcefully (with /F option).
PS C:\Users\muska> /F
/F : The term '/F' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the
path is correct and try again.
At line:1 char:1
+ /F
+ ~~
    + CategoryInfo          : ObjectNotFound: (/F:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\muska>  taskkill /PID  10600
ERROR: The process with PID 10600 could not be terminated.
Reason: Access is denied.
PS C:\Users\muska> taskkill /PID 16956
ERROR: The process with PID 16956 could not be terminated.
Reason: This process can only be terminated forcefully (with /F option).
PS C:\Users\muska> taskkill /PID 16458
ERROR: The process "16458" not found.
PS C:\Users\muska> taskkill /PID 12860
SUCCESS: Sent termination signal to the process with PID 12860.
PS C:\Users\muska> taskkill /Skype.exe /F
ERROR: Invalid argument/option - '/Skype.exe'.
Type "TASKKILL /?" for usage.
PS C:\Users\muska> taskkill /pid 2616 /pid 14252
ERROR: The process with PID 2616 could not be terminated.
Reason: This process can only be terminated forcefully (with /F option).
ERROR: The process with PID 14252 could not be terminated.
Reason: This process can only be terminated forcefully (with /F option).
PS C:\Users\muska> taskkill /pid 8900 /pid 5136
ERROR: The process with PID 8900 could not be terminated.
Reason: Access is denied.
ERROR: The process with PID 5136 could not be terminated.
Reason: Access is denied.
PS C:\Users\muska> taskkill /pid 13136 /pid 8412
SUCCESS: Sent termination signal to the process with PID 13136.
SUCCESS: Sent termination signal to the process with PID 8412.
```