Secure Coding Lab - 3

Name: Tejeswar Allaka

Reg No: 18BCN7033

1) where

```
C:\Users\allak>where
The syntax of this command is:

WHERE [/R dir] [/Q] [/F] [/T] pattern...

Description:
    Displays the location of files that match the search pattern.
    By default, the search is done along the current directory and
    in the paths specified by the PATH environment variable.

Parameter List:
    /R       Recursively searches and displays the files that match the
             given pattern starting from the specified directory.

    /Q       Returns only the exit code, without displaying the list
             of matched files. (Quiet mode)

    /F       Displays the matched filename in double quotes.

    /T       Displays the file size, last modified date and time for all
             matched files.

    pattern  Specifies the search pattern for the files to match.
             Wildcards * and ? can be used in the pattern. The
             "$env:pattern" and "path:pattern" formats can also be
             specified, where "env" is an environment variable and
             the search is done in the specified paths of the "env"
             environment variable. These formats should not be used
             with /R. The search is also done by appending the
             extensions of the PATHEXT variable to the pattern.

     /?      Displays this help message.

  NOTE: The tool returns an error level of 0 if the search is
        successful, of 1 if the search is unsuccessful and
        of 2 for failures or errors.

Examples:
    WHERE /?
    WHERE myfilename1 myfile????.*
    WHERE $windir:*.*
    WHERE /R c:\windows *.exe *.dll *.bat
    WHERE /Q ??.???
    WHERE "c:\windows;c:\windows\system32:*.dll"
    WHERE /F /T *.dll
```

```
C:\Users\allak>where /R c:\ Windows
c:\Users\allak\AppData\Roaming\discord\0.0.309\modules\discord_utils\node_modules\isexe\windows.js
c:\Users\allak\AppData\Roaming\discord\0.0.309\modules\discord_voice\node_modules\isexe\windows.js

C:\Users\allak>
```

2) Diskpart

```
Command Prompt - diskpart
Microsoft Windows [Version 10.0.19042.804]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\allak>diskpart

C:\windows\system32\diskpart.exe
Copyright (C) Microsoft Corporation.
On computer: LAPTOP-MO96SVVG

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          119 GB  6144 KB        *
  Disk 1    Online          931 GB  1024 KB        *
```

```
DISKPART> select disk0

Microsoft DiskPart version 10.0.19041.610

DISK        - Shift the focus to a disk. For example, SELECT DISK.
PARTITION   - Shift the focus to a partition. For example, SELECT PARTITION.
VOLUME      - Shift the focus to a volume. For example, SELECT VOLUME.
VDISK       - Shift the focus to a virtual disk. For example, SELECT VDISK.

DISKPART> select disk 0

Disk 0 is now the selected disk.

DISKPART> list partition

  Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
  Partition 1    System             260 MB  1024 KB
  Partition 2    Reserved            16 MB   261 MB
  Partition 3    Primary            118 GB   277 MB
```

3)File replication

Experiment - File Replication.

- Assume your computer got infected with some virus.
- Virus exhibits the property of replication with the same file name.
  - For example. File1 is replicated as File1(1) -> Initial infection
  - File1(2) -> Second infection, likewise it replicates File1 for 50 times.
- Now, How will you find all the replicated files.
- Task to experiment: Use the cmd prompt to identify and locate the files and delete the same.

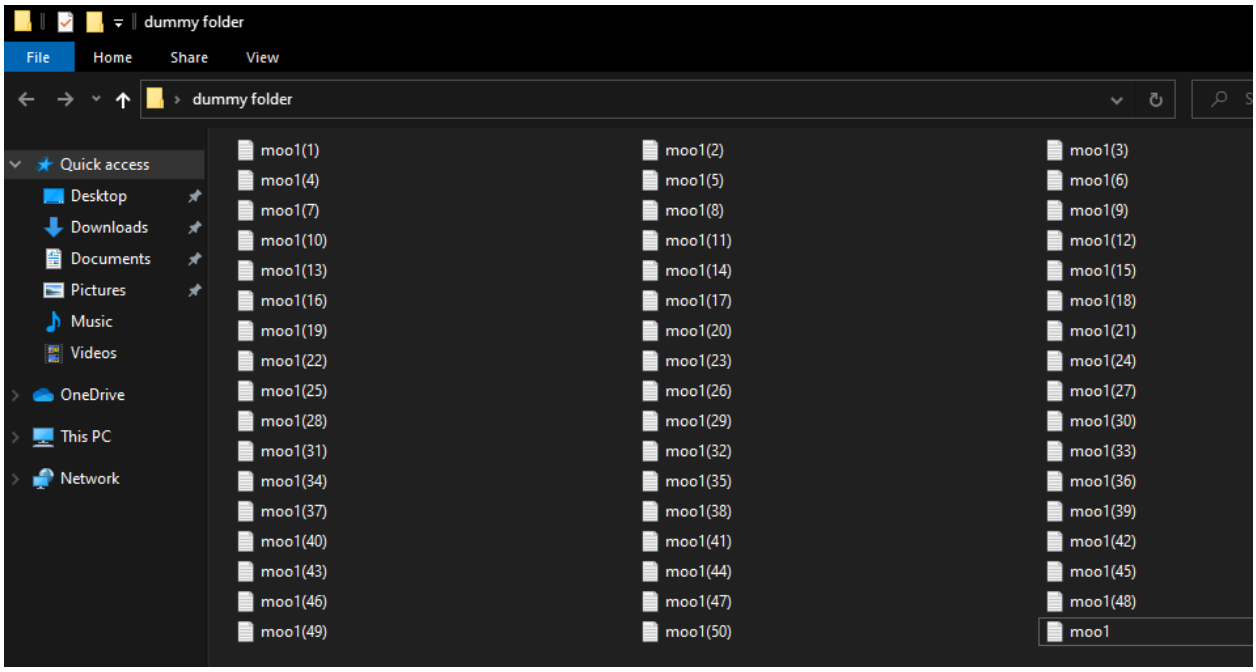
```
C:\Users\allak>where /R c:\ moo1*
c:\Users\allak\Desktop\dummy folder\moo1(1).txt
c:\Users\allak\Desktop\dummy folder\moo1(10).txt
c:\Users\allak\Desktop\dummy folder\moo1(11).txt
c:\Users\allak\Desktop\dummy folder\moo1(12).txt
c:\Users\allak\Desktop\dummy folder\moo1(13).txt
c:\Users\allak\Desktop\dummy folder\moo1(14).txt
c:\Users\allak\Desktop\dummy folder\moo1(15).txt
c:\Users\allak\Desktop\dummy folder\moo1(16).txt
c:\Users\allak\Desktop\dummy folder\moo1(17).txt
c:\Users\allak\Desktop\dummy folder\moo1(18).txt
c:\Users\allak\Desktop\dummy folder\moo1(19).txt
c:\Users\allak\Desktop\dummy folder\moo1(2).txt
c:\Users\allak\Desktop\dummy folder\moo1(20).txt
c:\Users\allak\Desktop\dummy folder\moo1(21).txt
c:\Users\allak\Desktop\dummy folder\moo1(22).txt
c:\Users\allak\Desktop\dummy folder\moo1(23).txt
c:\Users\allak\Desktop\dummy folder\moo1(24).txt
c:\Users\allak\Desktop\dummy folder\moo1(25).txt
c:\Users\allak\Desktop\dummy folder\moo1(26).txt
c:\Users\allak\Desktop\dummy folder\moo1(27).txt
c:\Users\allak\Desktop\dummy folder\moo1(28).txt
c:\Users\allak\Desktop\dummy folder\moo1(29).txt
c:\Users\allak\Desktop\dummy folder\moo1(3).txt
```

```
C:\Users\allak\Desktop>cd "dummy folder"

C:\Users\allak\Desktop\dummy folder>del moo*

C:\Users\allak\Desktop\dummy folder>dir
 Volume in drive C is WINDOWS
 Volume Serial Number is E681-94E2

 Directory of C:\Users\allak\Desktop\dummy folder

20-02-2021  19:20    <DIR>          .
20-02-2021  19:20    <DIR>          ..
               0 File(s)              0 bytes
               2 Dir(s)  71,922,450,432 bytes free

C:\Users\allak\Desktop\dummy folder>
```

4)

Classwork

- Write a file replication code to copy the same file for 50 times on the same directory.




```
import shutil

org= r'C:\Users\allak\Desktop\dummy folder\mool.txt'

for i in range(1,51):
    target = r'C:\Users\allak\Desktop\dummy folder\mool('+str(i)+').txt'
    shutil.copyfile(org,target)
```

5)

Process/Tasks/Jobs/

- A **process** is the **instance** of a **computer program** that is being **executed**. It contains the program code and its activity.
  - Depending on the operating system (**OS**), a **process** may be made up of multiple threads of execution that execute instructions concurrently.
- A **task** represents the execution of a single process or multiple processes on a compute node.
- A collection of **tasks** that is used to perform a computation is known as a **job**.

Basics

- Create a task name "Reg.no_Task1" to run on a specific time
- Change the time of the scheduled task
- Delete the scheduled task
- Schedule an another task to run only on Weekdays
- Schedule an another task to run only on Weekends

```
C:\WINDOWS\system32>schtasks

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
GoogleUpdateTaskMachineCore              21-02-2021 03:05:11    Ready
GoogleUpdateTaskMachineUA                20-02-2021 20:05:11    Ready
HPAudioSwitch                            N/A                    Running
HPEA3JOBS                                N/A                    Ready
HPJumpStartLaunch                        N/A                    Running
McAfee Remediation (Prepare)             N/A                    Ready
McAfeeLogon                              N/A                    Running
MicrosoftEdgeUpdateTaskMachineCore       21-02-2021 02:57:28    Ready
MicrosoftEdgeUpdateTaskMachineCore1d6fbb 21-02-2021 01:13:01    Ready
MicrosoftEdgeUpdateTaskMachineUA         20-02-2021 19:43:01    Ready
npcapwatchdog                            N/A                    Ready
NvBatteryBoostCheckOnLogon_{B2FE1952-018 N/A                    Ready
NvDriverUpdateCheckDaily_{B2FE1952-0186- 21-02-2021 12:25:35    Ready
NVIDIA GeForce Experience SelfUpdate_{B2 N/A                    Ready
NvNodeLauncher_{B2FE1952-0186-46C3-BAEC- N/A                    Ready
NvProfileUpdaterDaily_{B2FE1952-0186-46C 21-02-2021 12:25:29    Ready
NvProfileUpdaterOnLogon_{B2FE1952-0186-4 N/A                    Ready
NvTmRep_CrashReport1_{B2FE1952-0186-46C3 21-02-2021 12:25:35    Ready
NvTmRep_CrashReport2_{B2FE1952-0186-46C3 21-02-2021 18:25:35    Ready
NvTmRep_CrashReport3_{B2FE1952-0186-46C3 21-02-2021 00:25:35    Ready
NvTmRep_CrashReport4_{B2FE1952-0186-46C3 21-02-2021 06:25:35    Ready
OneDrive Standalone Update Task v2       21-02-2021 15:10:58    Ready
OneDrive Standalone Update Task-S-1-5-21 21-02-2021 00:40:23    Ready

Folder: \Agent Activation Runtime
```

Creating the task

```
C:\WINDOWS\system32>schtasks /create /SC DAILY /TN "Tasks\18BCN7033_Task1" /TR "C:\Windows\System32\Notepad.exe" /ST 21:30
SUCCESS: The scheduled task "Tasks\18BCN7033_Task1" has successfully been created.
```

Display the task

```
Folder: \Tasks
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
18BCN7033_Task1                          20-02-2021 21:30:00    Ready
```

Update the task

```
C:\WINDOWS\system32>schtasks /CHANGE /TN "Tasks\18BCN7033_Task1" /ST 21:40
Please enter the run as password for allak: ***********

SUCCESS: The parameters of scheduled task "Tasks\18BCN7033_Task1" have been changed.

C:\WINDOWS\system32>
```

Delete the task

```
C:\WINDOWS\system32>schtasks /DELETE /TN "Tasks\18BCN7033_Task1"
WARNING: Are you sure you want to remove the task "Tasks\18BCN7033_Task1" (Y/N)? Y
SUCCESS: The scheduled task "Tasks\18BCN7033_Task1" was successfully deleted.
```