LNJN National Institute Of Criminology And Forensic Science

National Forensics Science University

Python And Scripting

Subject Code: CTMSDFIS S1 P4

Submitted By

Shubhang Gupta

Roll No. :

M.Sc. Digital Forensics And Information Security

LAB 01 25-08-2022

AIM: To study basics and user status powershell commands.

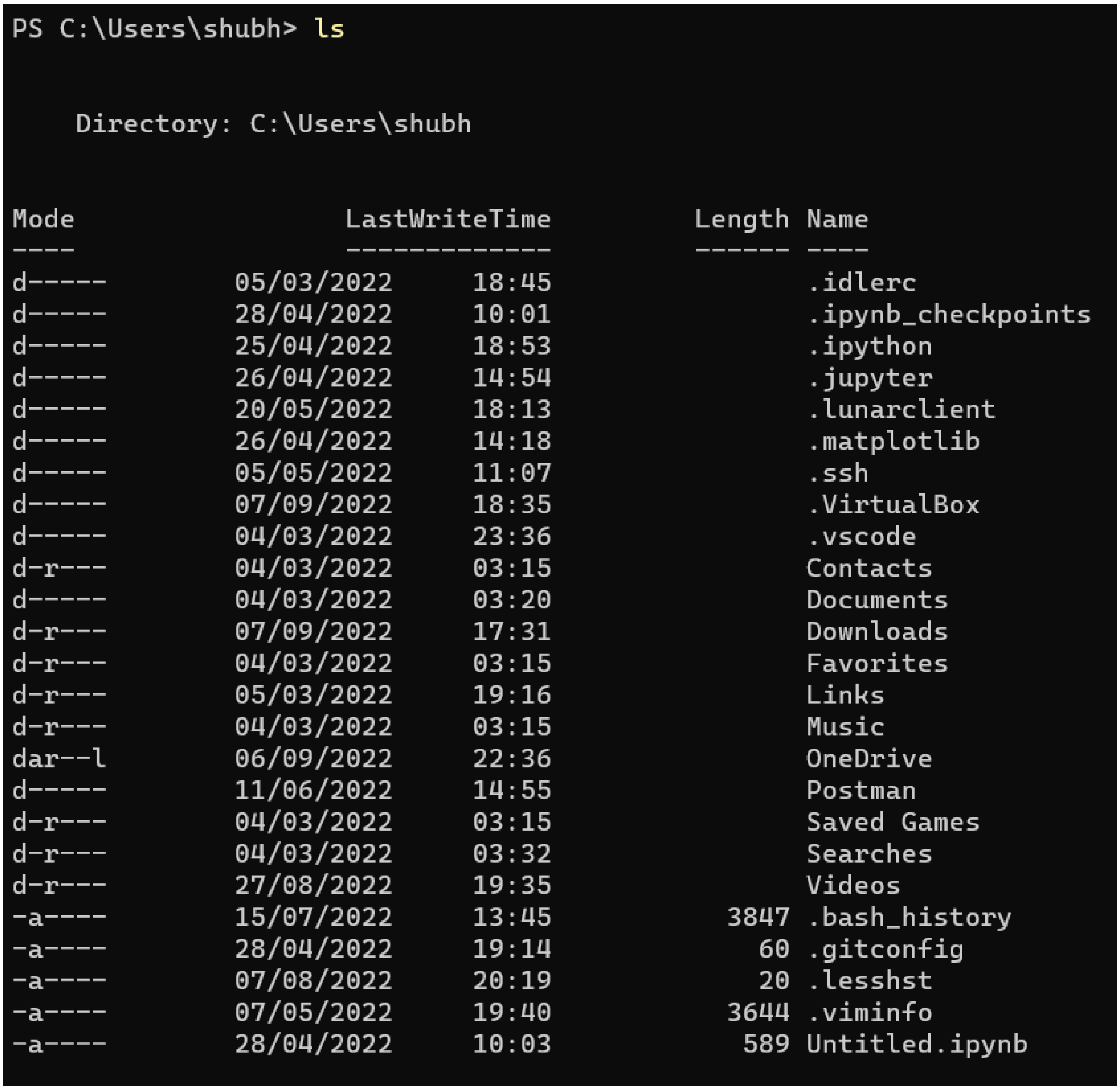
SOFTWARE REQUIRED: A personal desktop with powershell.

INTRODUCTION: Windows PowerShell is a Microsoft framework for automating tasks using a command-line shell and an associated scripting language. When it was released in 2006, this powerful tool essentially replaced Command Prompt as the default way to automate batch processes and create customized system management tools. Many system administrators, including managed services providers (MSPs) rely on the 130+ command-line tools within PowerShell to streamline and scale tasks in both local and remote systems.

“Windows PowerShell is an interactive object-oriented command environment with scripting language features that utilizes small programs called cmdlets to simplify configuration, administration, and management of heterogeneous environments in both standalone and networked typologies by utilizing standards-based remoting protocols.”

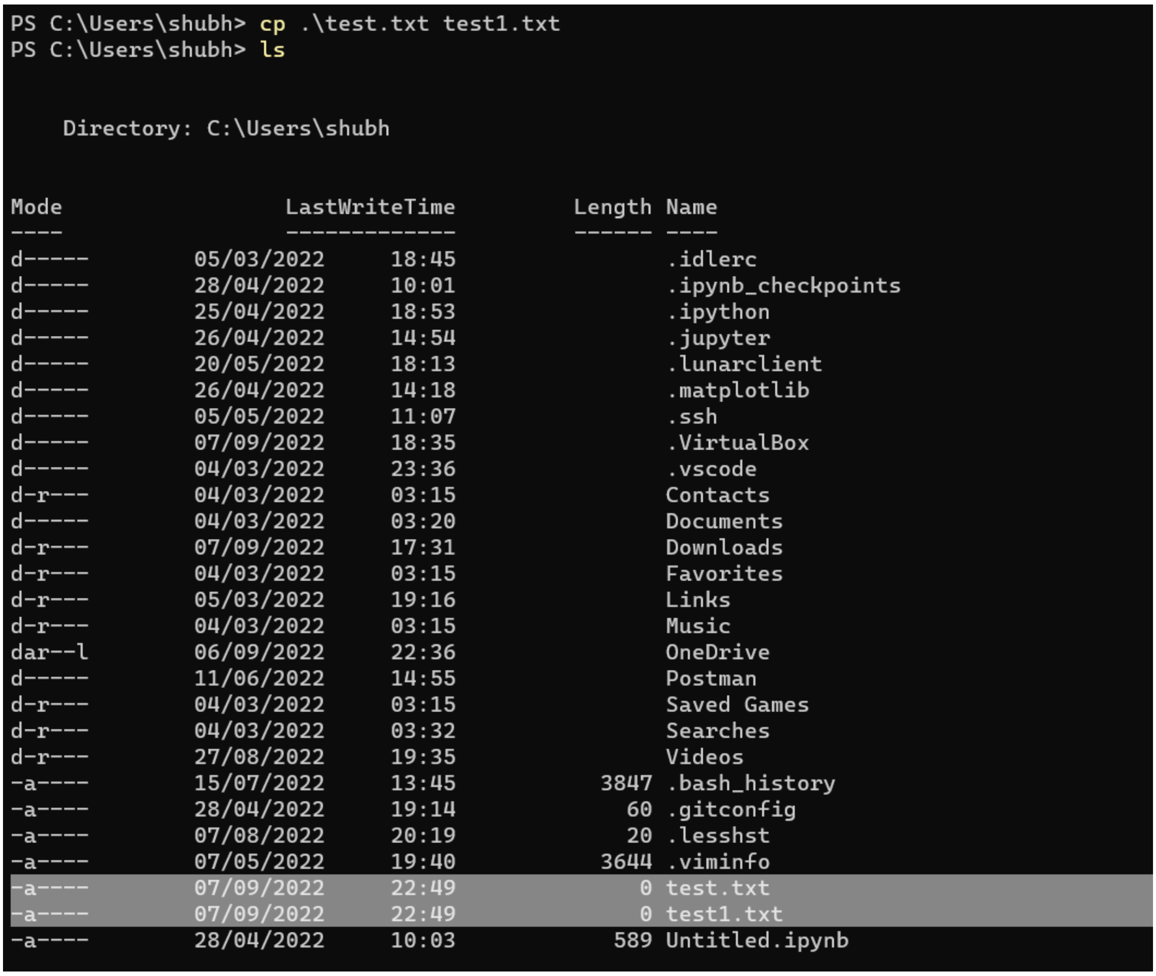
POWERSHELL COMMANDS

1. ‘**ls**’ command – This command is used to list all the files and directories in the current directory.



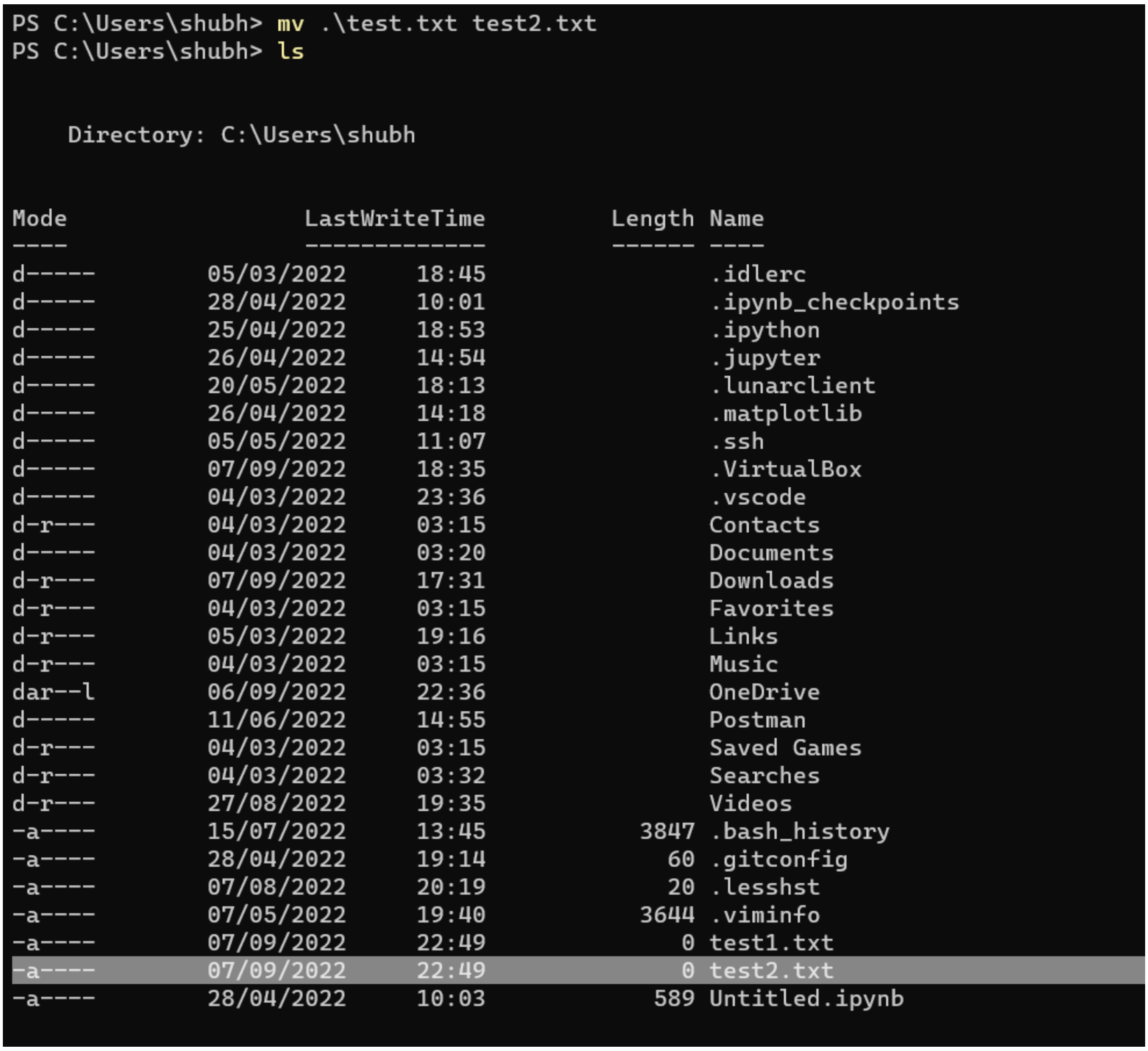
```
PS C:\Users\shubh> ls


    Directory: C:\Users\shubh


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        05/03/2022     18:45                .idlerc
d-----        28/04/2022     10:01                .ipynb_checkpoints
d-----        25/04/2022     18:53                .ipython
d-----        26/04/2022     14:54                .jupyter
d-----        20/05/2022     18:13                .lunarclient
d-----        26/04/2022     14:18                .matplotlib
d-----        05/05/2022     11:07                .ssh
d-----        07/09/2022     18:35                .VirtualBox
d-----        04/03/2022     23:36                .vscode
d-r---        04/03/2022     03:15                Contacts
d-----        04/03/2022     03:20                Documents
d-r---        07/09/2022     17:31                Downloads
d-r---        04/03/2022     03:15                Favorites
d-r---        05/03/2022     19:16                Links
d-r---        04/03/2022     03:15                Music
dar--l        06/09/2022     22:36                OneDrive
d-----        11/06/2022     14:55                Postman
d-r---        04/03/2022     03:15                Saved Games
d-r---        04/03/2022     03:32                Searches
d-r---        27/08/2022     19:35                Videos
-a----        15/07/2022     13:45           3847 .bash_history
-a----        28/04/2022     19:14             60 .gitconfig
-a----        07/08/2022     20:19             20 .lesshst
-a----        07/05/2022     19:40           3644 .viminfo
-a----        28/04/2022     10:03            589 Untitled.ipynb
```

2. ‘**cp**’ command - This command is used to copy a file from one location to another.



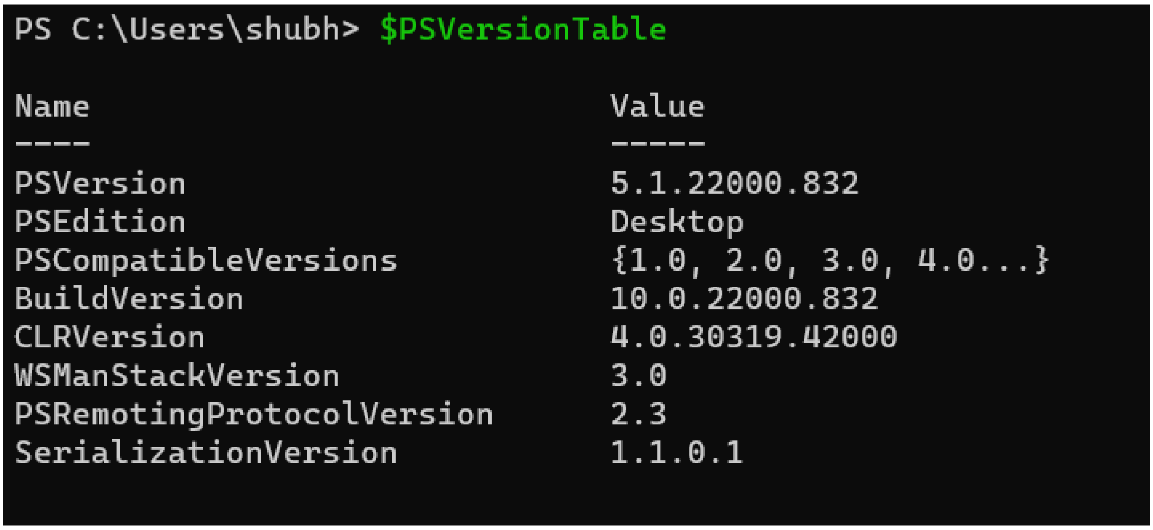
```
PS C:\Users\shubh> cp .\test.txt test1.txt
PS C:\Users\shubh> ls


    Directory: C:\Users\shubh


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        05/03/2022     18:45                .idlerc
d-----        28/04/2022     10:01                .ipynb_checkpoints
d-----        25/04/2022     18:53                .ipython
d-----        26/04/2022     14:54                .jupyter
d-----        20/05/2022     18:13                .lunarclient
d-----        26/04/2022     14:18                .matplotlib
d-----        05/05/2022     11:07                .ssh
d-----        07/09/2022     18:35                .VirtualBox
d-----        04/03/2022     23:36                .vscode
d-r---        04/03/2022     03:15                Contacts
d-----        04/03/2022     03:20                Documents
d-r---        07/09/2022     17:31                Downloads
d-r---        04/03/2022     03:15                Favorites
d-r---        05/03/2022     19:16                Links
d-r---        04/03/2022     03:15                Music
dar--l        06/09/2022     22:36                OneDrive
d-----        11/06/2022     14:55                Postman
d-r---        04/03/2022     03:15                Saved Games
d-r---        04/03/2022     03:32                Searches
d-r---        27/08/2022     19:35                Videos
-a----        15/07/2022     13:45           3847 .bash_history
-a----        28/04/2022     19:14             60 .gitconfig
-a----        07/08/2022     20:19             20 .lesshst
-a----        07/05/2022     19:40           3644 .viminfo
-a----        07/09/2022     22:49              0 test.txt
-a----        07/09/2022     22:49              0 test1.txt
-a----        28/04/2022     10:03            589 Untitled.ipynb
```

3. ‘**mv**’ command – The command is used to move one directory or file from one location to another location. We can also give the location as the parameters for the “mv”



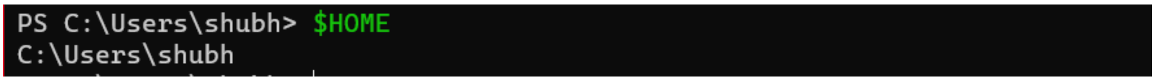
```
PS C:\Users\shubh> mv .\test.txt test2.txt
PS C:\Users\shubh> ls


    Directory: C:\Users\shubh


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        05/03/2022     18:45                .idlerc
d-----        28/04/2022     10:01                .ipynb_checkpoints
d-----        25/04/2022     18:53                .ipython
d-----        26/04/2022     14:54                .jupyter
d-----        20/05/2022     18:13                .lunarclient
d-----        26/04/2022     14:18                .matplotlib
d-----        05/05/2022     11:07                .ssh
d-----        07/09/2022     18:35                .VirtualBox
d-----        04/03/2022     23:36                .vscode
d-r---        04/03/2022     03:15                Contacts
d-----        04/03/2022     03:20                Documents
d-r---        07/09/2022     17:31                Downloads
d-r---        04/03/2022     03:15                Favorites
d-r---        05/03/2022     19:16                Links
d-r---        04/03/2022     03:15                Music
dar--l        06/09/2022     22:36                OneDrive
d-----        11/06/2022     14:55                Postman
d-r---        04/03/2022     03:15                Saved Games
d-r---        04/03/2022     03:32                Searches
d-r---        27/08/2022     19:35                Videos
-a----        15/07/2022     13:45           3847 .bash_history
-a----        28/04/2022     19:14             60 .gitconfig
-a----        07/08/2022     20:19             20 .lesshst
-a----        07/05/2022     19:40           3644 .viminfo
-a----        07/09/2022     22:49              0 test1.txt
-a----        07/09/2022     22:49              0 test2.txt
-a----        28/04/2022     10:03            589 Untitled.ipynb
```

4. **'$PSversiontable**' command – The command contains a read-only hash table (Constant, AllScope) that displays details about the version of PowerShell that is running in the current session.



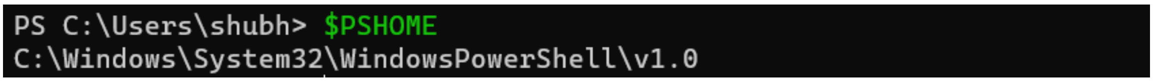
```
PS C:\Users\shubh> $PSVersionTable

Name                           Value
----                           -----
PSVersion                      5.1.22000.832
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.22000.832
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1
```

5. '**$HOME**' command – The command gives the path of the home directory.



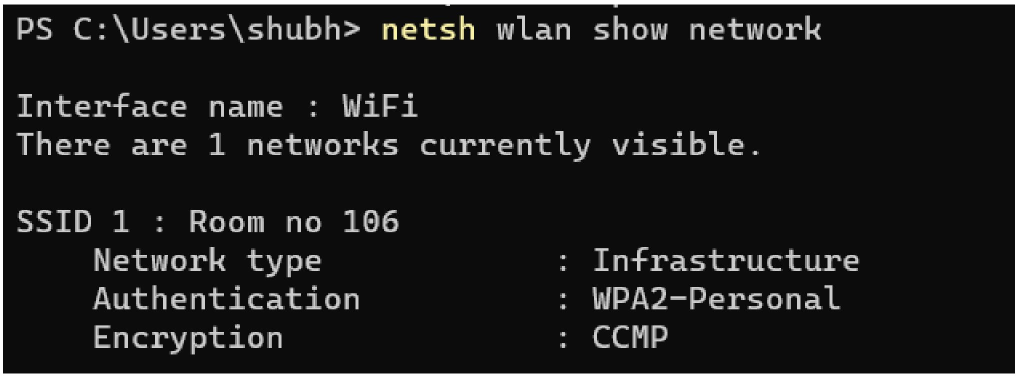
```
PS C:\Users\shubh> $HOME
C:\Users\shubh
```

6. '**$PSHOME**' command – The command gives the



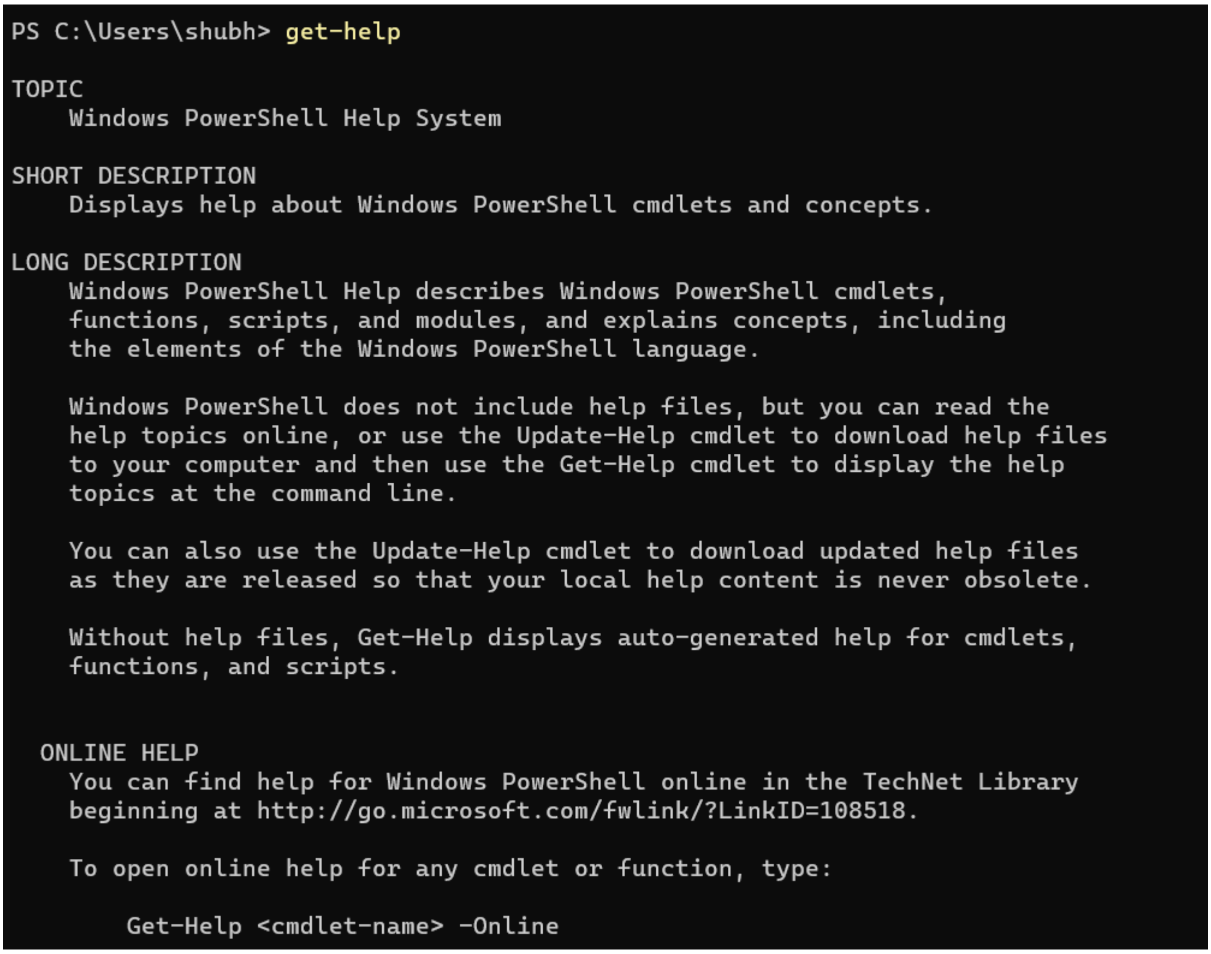
```
PS C:\Users\shubh> $PSHOME
C:\Windows\System32\WindowsPowerShell\v1.0
```

7. ‘**netsh**’ command - Netsh is a command-line scripting utility that allows you to, either locally or remotely, display or modify the network configuration of a currently running computer. Used without parameters, netsh opens the Netsh.exe command prompt (that is, netsh>).



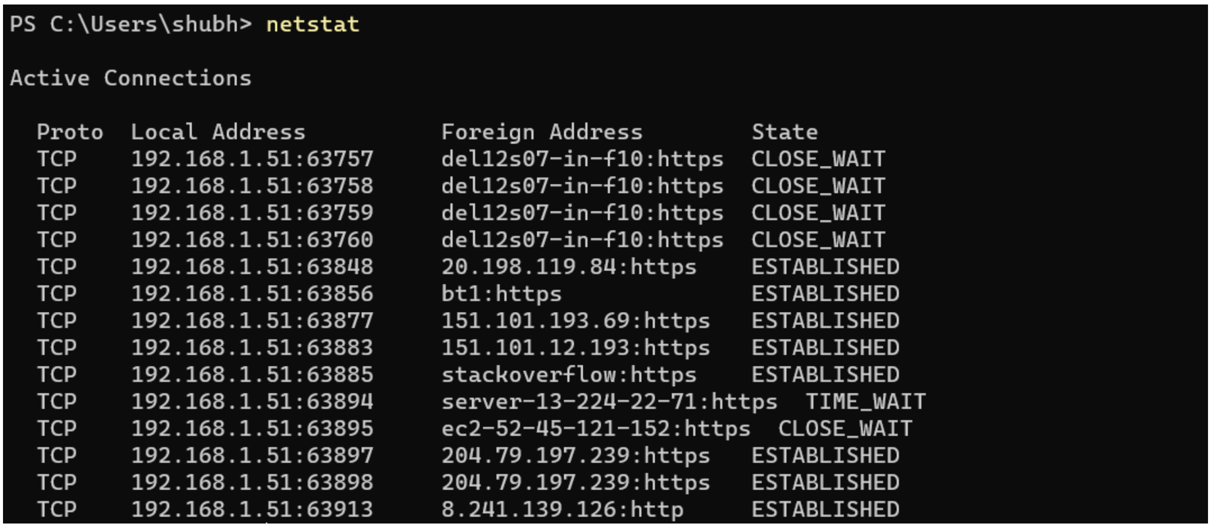
```
PS C:\Users\shubh> netsh wlan show network

Interface name : WiFi
There are 1 networks currently visible.

SSID 1 : Room no 106
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP
```

8. ‘**get-help**’ command – This cmdlet displays information about PowerShell concepts and commands, including cmdlets, functions, Common Information Model (CIM) commands, workflows, providers, aliases, and scripts.



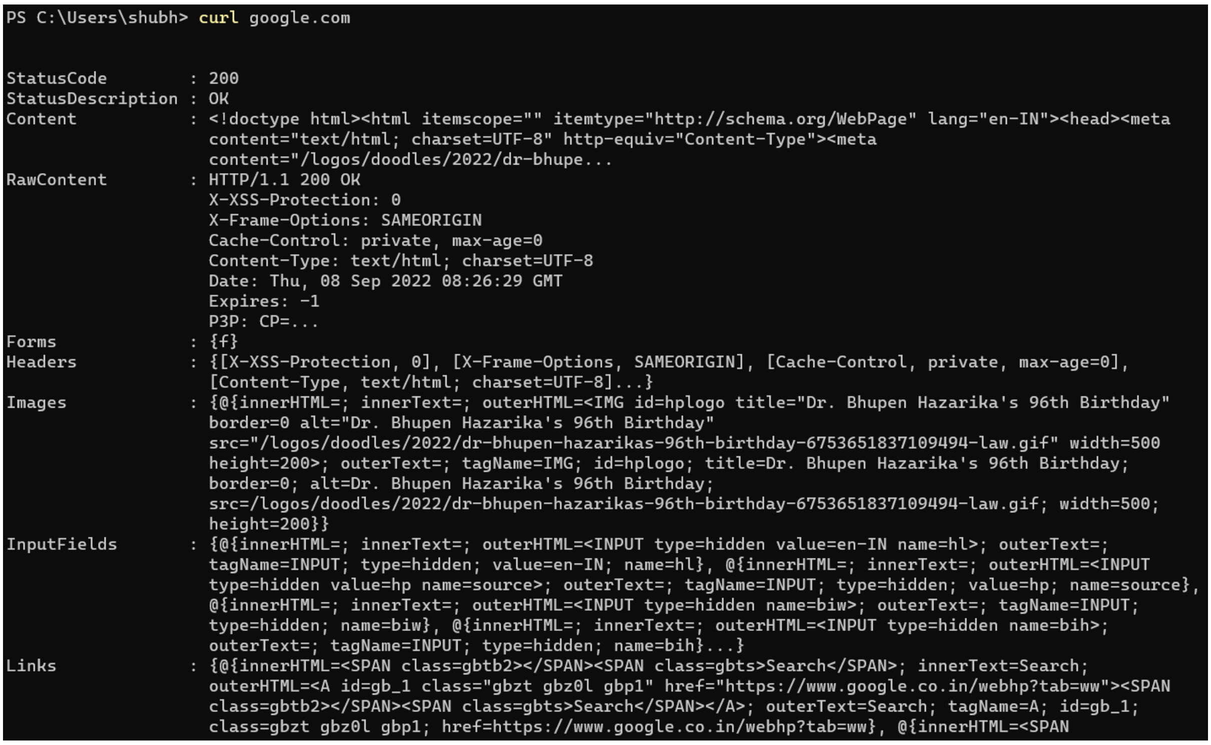
```
PS C:\Users\shubh> get-help

TOPIC
    Windows PowerShell Help System

SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.

LONG DESCRIPTION
    Windows PowerShell Help describes Windows PowerShell cmdlets,
    functions, scripts, and modules, and explains concepts, including
    the elements of the Windows PowerShell language.

    Windows PowerShell does not include help files, but you can read the
    help topics online, or use the Update-Help cmdlet to download help files
    to your computer and then use the Get-Help cmdlet to display the help
    topics at the command line.

    You can also use the Update-Help cmdlet to download updated help files
    as they are released so that your local help content is never obsolete.

    Without help files, Get-Help displays auto-generated help for cmdlets,
    functions, and scripts.


  ONLINE HELP
    You can find help for Windows PowerShell online in the TechNet Library
    beginning at http://go.microsoft.com/fwlink/?LinkID=108518.

    To open online help for any cmdlet or function, type:

        Get-Help <cmdlet-name> -Online
```

9. ‘**netstat**’ command - command produces tab-delimited, fixed-width tables. The following example converts the active connections that list active TCP connections as well as listening TCP and UDP ports to an object.



```
PS C:\Users\shubh> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.51:63757     del12s07-in-f10:https  CLOSE_WAIT
  TCP    192.168.1.51:63758     del12s07-in-f10:https  CLOSE_WAIT
  TCP    192.168.1.51:63759     del12s07-in-f10:https  CLOSE_WAIT
  TCP    192.168.1.51:63760     del12s07-in-f10:https  CLOSE_WAIT
  TCP    192.168.1.51:63848     20.198.119.84:https    ESTABLISHED
  TCP    192.168.1.51:63856     bt1:https              ESTABLISHED
  TCP    192.168.1.51:63877     151.101.193.69:https   ESTABLISHED
  TCP    192.168.1.51:63883     151.101.12.193:https   ESTABLISHED
  TCP    192.168.1.51:63885     stackoverflow:https    ESTABLISHED
  TCP    192.168.1.51:63894     server-13-224-22-71:https  TIME_WAIT
  TCP    192.168.1.51:63895     ec2-52-45-121-152:https  CLOSE_WAIT
  TCP    192.168.1.51:63897     204.79.197.239:https   ESTABLISHED
  TCP    192.168.1.51:63898     204.79.197.239:https   ESTABLISHED
  TCP    192.168.1.51:63913     8.241.139.126:http     ESTABLISHED
```

10. ‘**curl**’ command - command-line tool for transferring data from or to a server with any of the supported protocols including HTTP, HTTPS, FTP, and IMAP. The tool provides numerous options like resume transfer, limit bandwidth, and proxy support.



```
PS C:\Users\shubh> curl google.com


StatusCode        : 200
StatusDescription : OK
Content           : <!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en-IN"><head><meta
                    content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta
                    content="/logos/doodles/2022/dr-bhupe...
RawContent        : HTTP/1.1 200 OK
                    X-XSS-Protection: 0
                    X-Frame-Options: SAMEORIGIN
                    Cache-Control: private, max-age=0
                    Content-Type: text/html; charset=UTF-8
                    Date: Thu, 08 Sep 2022 08:26:29 GMT
                    Expires: -1
                    P3P: CP=...
Forms             : {f}
Headers           : {[X-XSS-Protection, 0], [X-Frame-Options, SAMEORIGIN], [Cache-Control, private, max-age=0],
                    [Content-Type, text/html; charset=UTF-8]...}
Images            : {@{innerHTML=; innerText=; outerHTML=<IMG id=hplogo title="Dr. Bhupen Hazarika's 96th Birthday"
                    border=0 alt="Dr. Bhupen Hazarika's 96th Birthday"
                    src="/logos/doodles/2022/dr-bhupen-hazarikas-96th-birthday-6753651837109494-law.gif" width=500
                    height=200>; outerText=; tagName=IMG; id=hplogo; title=Dr. Bhupen Hazarika's 96th Birthday;
                    border=0; alt=Dr. Bhupen Hazarika's 96th Birthday;
                    src=/logos/doodles/2022/dr-bhupen-hazarikas-96th-birthday-6753651837109494-law.gif; width=500;
                    height=200}}
InputFields       : {@{innerHTML=; innerText=; outerHTML=<INPUT type=hidden value=en-IN name=hl>; outerText=;
                    tagName=INPUT; type=hidden; value=en-IN; name=hl}, @{innerHTML=; innerText=; outerHTML=<INPUT
                    type=hidden value=hp name=source>; outerText=; tagName=INPUT; type=hidden; value=hp; name=source},
                    @{innerHTML=; innerText=; outerHTML=<INPUT type=hidden name=biw>; outerText=; tagName=INPUT;
                    type=hidden; name=biw}, @{innerHTML=; innerText=; outerHTML=<INPUT type=hidden name=bih>;
                    outerText=; tagName=INPUT; type=hidden; name=bih}...}
Links             : {@{innerHTML=<SPAN class=gbtb2></SPAN><SPAN class=gbts>Search</SPAN>; innerText=Search;
                    outerHTML=<A id=gb_1 class="gbzt gbz0l gbp1" href="https://www.google.co.in/webhp?tab=ww"><SPAN
                    class=gbtb2></SPAN><SPAN class=gbts>Search</SPAN></A>; outerText=Search; tagName=A; id=gb_1;
                    class=gbzt gbz0l gbp1; href=https://www.google.co.in/webhp?tab=ww}, @{innerHTML=<SPAN
```

THE END