Command Prompt

Objectives:

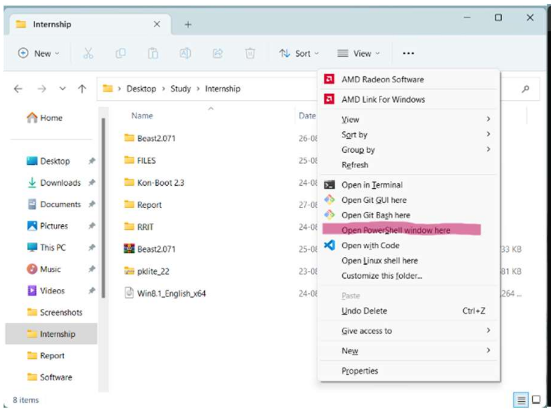
Executes the entered commands. Most of those commands automate tasks via scripts and batch files, perform advanced administrative functions, and troubleshoot or solve certain kinds of windows issues.

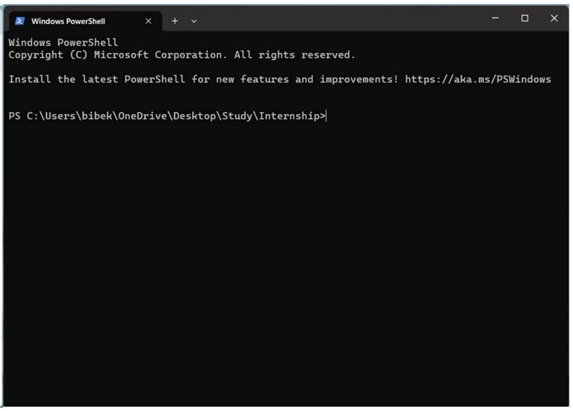
Command line Tips and Tricks:

1. To open power shell window from the current path-
   - Press *Shift and Right* lick on any folder to open a powershell window there.
2. Run command prompt as admin –
   - Many commands require you to open the Command window as in admin, instead of right clicking on the program and choosing the as administrator" we could simply press *Ctrl+Shift+Enter* to open it with admin privileges.
3. See command History-
   - We could use the command *doskey /history* to list all the commands in the command prompt itself.
4. Copy the command output to clipboard -
   - We could easily copy any commands output to the clipboard by using the *|clip* at the end of the command.
5. Run multiple commands-
   - We could also run multiple commands at a single time using the *'&&'* operator.
6. Get help for any command-
   - Whenever you don't know or remember any commands particular syntax, just suffix it with the */?* to view its usage.
7. View wifi passwords of all connected networks -
   - Use the command *"netsh wlan show profile"* to see all the connected networks from the device.
   - Use "*netsh wlan show profile <wifi-name> key=clear*" to view the password in the KEY CONTENT.
8. View the ip address of a network-
   - Use the command *"pconfig"* to see IPv4, IPv6 address.

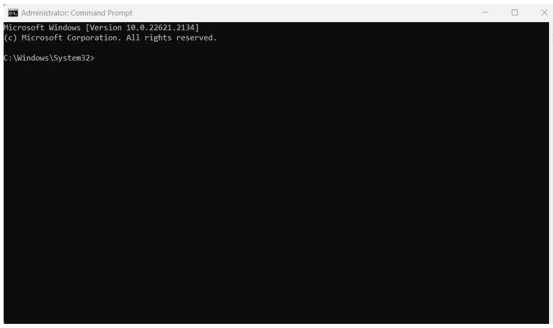
9. Find the list of servers of a websites and the packet movement from the pc to the server -
    - Use the command is “tracert site-name”
10. Find the list of TCP connection connected to the system-
    - Use the command “netstat” to see list of TCP connection connected to the system.

Proof of concept (POC):

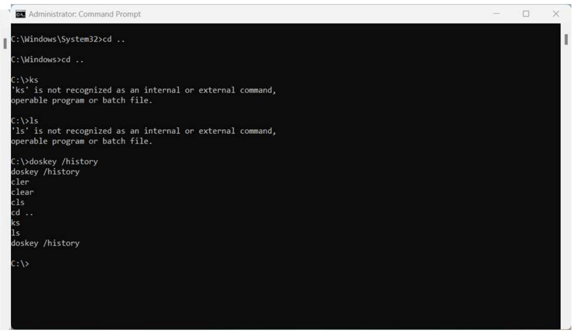




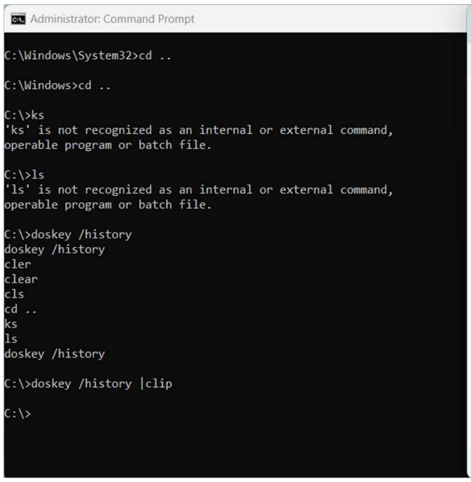
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\bibek\OneDrive\Desktop\Study\Internship>
```



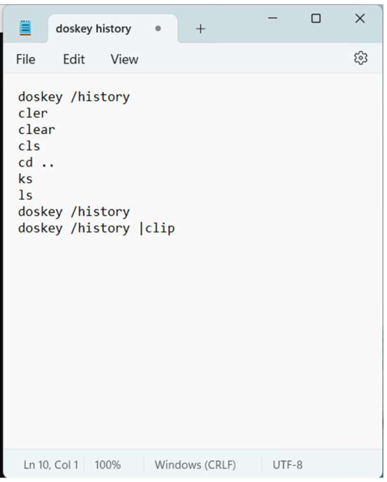
```
Microsoft Windows [Version 10.0.22621.2134]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>
```



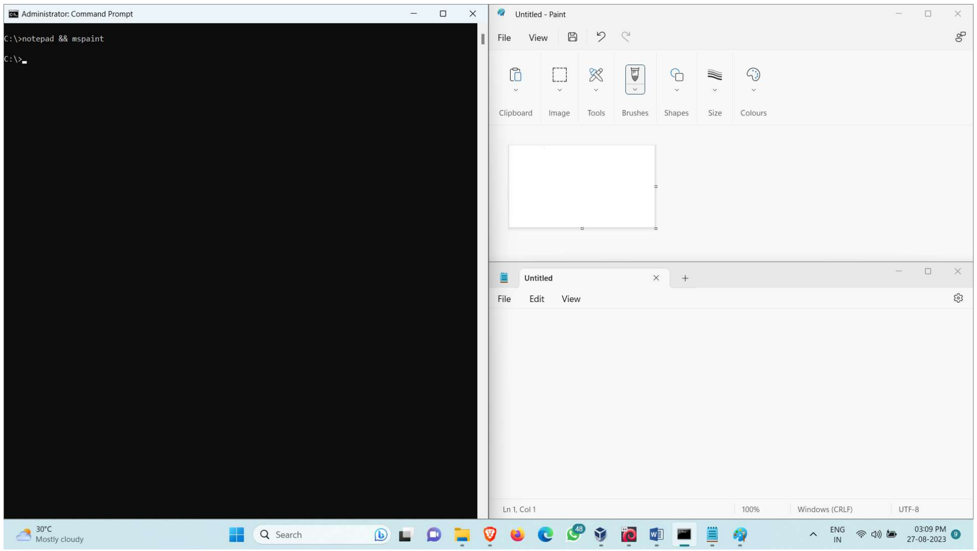
```
C:\Windows\System32>cd ..

C:\Windows>cd ..

C:\>ks
'ks' is not recognized as an internal or external command,
operable program or batch file.

C:\>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\>doskey /history
doskey /history
cler
clear
cls
cd ..
ks
ls
doskey /history

C:\>
```



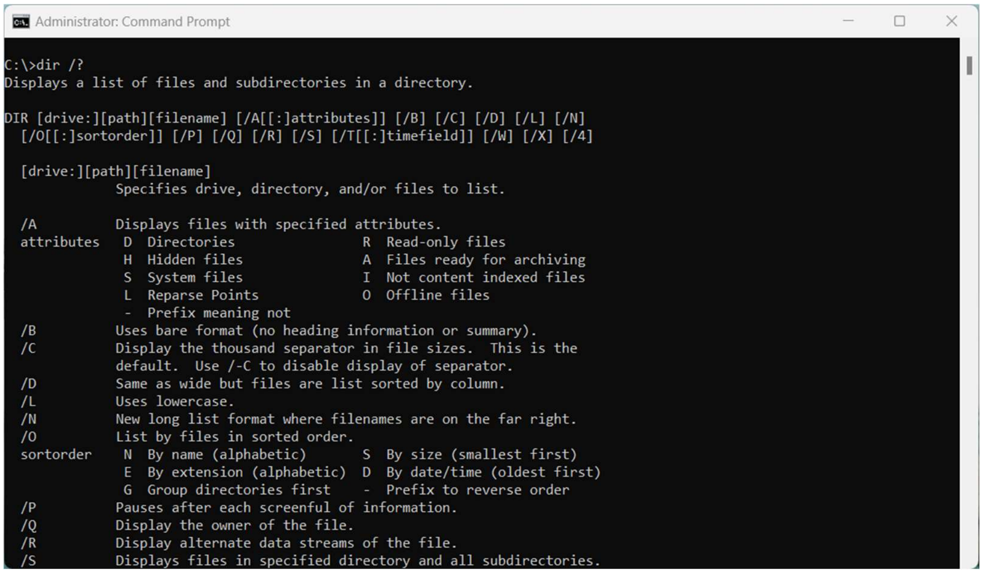
```
C:\Windows\System32>cd ..

C:\Windows>cd ..

C:\>ks
'ks' is not recognized as an internal or external command,
operable program or batch file.

C:\>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\>doskey /history
doskey /history
cler
clear
cls
cd ..
ks
ls
doskey /history

C:\>doskey /history |clip

C:\>
```



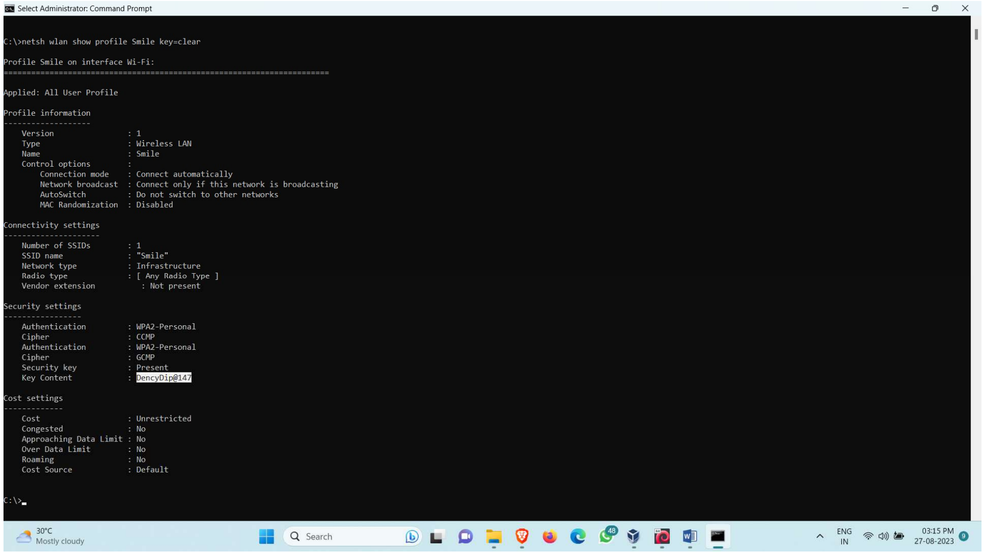
```
doskey /history
cler
clear
cls
cd ..
ks
ls
doskey /history
doskey /history |clip
```



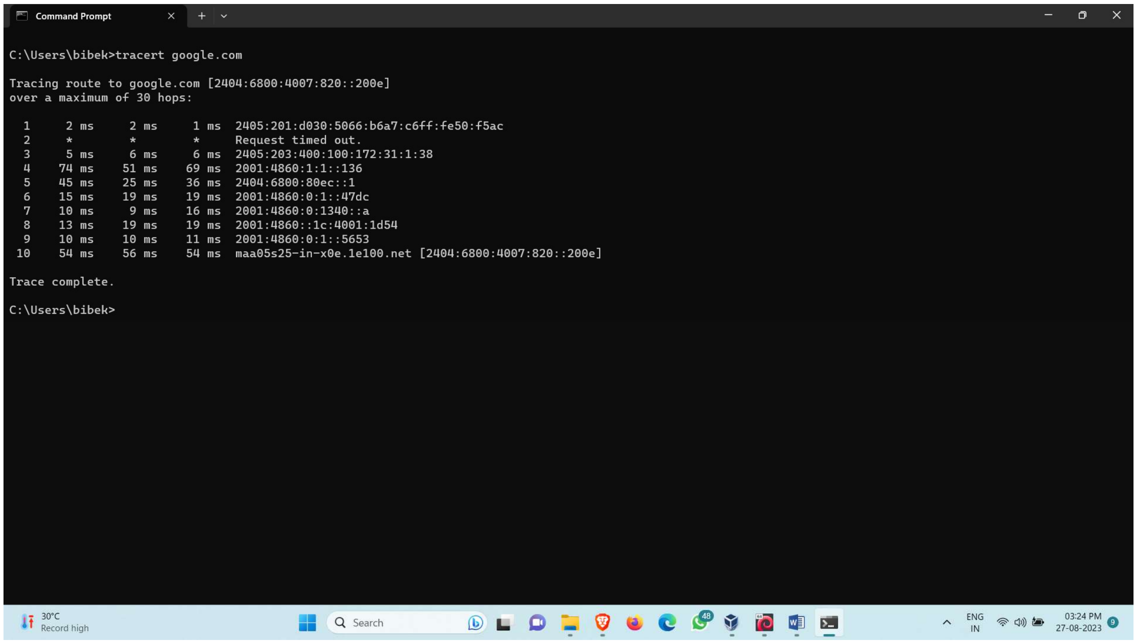
```
C:\>notepad && mspaint

C:\>
```



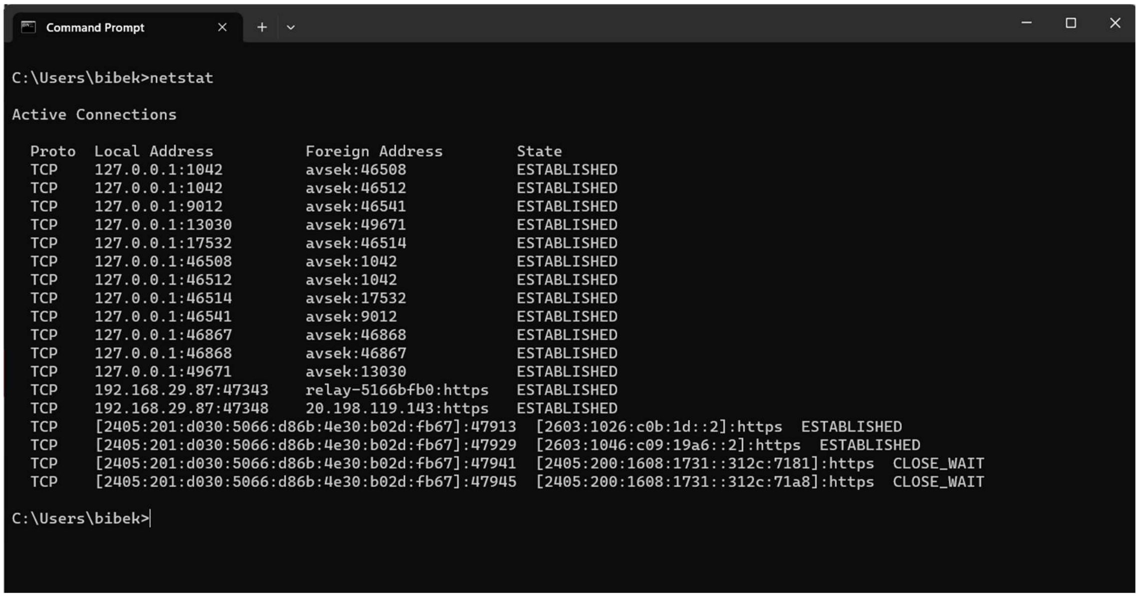
```
C:\>dir /?
Displays a list of files and subdirectories in a directory.

DIR [drive:][path][filename] [/A[[:]attributes]] [/B] [/C] [/D] [/L] [/N]
  [/O[[:]sortorder]] [/P] [/Q] [/R] [/S] [/T[[:]timefield]] [/W] [/X] [/4]

  [drive:][path][filename]
              Specifies drive, directory, and/or files to list.

  /A          Displays files with specified attributes.
  attributes   D  Directories                R  Read-only files
               H  Hidden files               A  Files ready for archiving
               S  System files               I  Not content indexed files
               L  Reparse Points             O  Offline files
               -  Prefix meaning not
  /B          Uses bare format (no heading information or summary).
  /C          Display the thousand separator in file sizes.  This is the
              default.  Use /-C to disable display of separator.
  /D          Same as wide but files are list sorted by column.
  /L          Uses lowercase.
  /N          New long list format where filenames are on the far right.
  /O          List by files in sorted order.
  sortorder    N  By name (alphabetic)       S  By size (smallest first)
               E  By extension (alphabetic)  D  By date/time (oldest first)
               G  Group directories first    -  Prefix to reverse order
  /P          Pauses after each screenful of information.
  /Q          Display the owner of the file.
  /R          Display alternate data streams of the file.
  /S          Displays files in specified directory and all subdirectories.
```



```
C:\>netsh wlan show profile Smile key=clear

Profile Smile on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : Smile
    Control options        :
        Connection mode    : Connect automatically
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "Smile"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Authentication         : WPA2-Personal
    Cipher                 : GCMP
    Security key           : Present
    Key Content            : DencyDip@147

Cost settings
-------------
    Cost                   : Unrestricted
    Congested              : No
    Approaching Data Limit : No
    Over Data Limit        : No
    Roaming                : No
    Cost Source            : Default


C:\>
```



```
C:\Users\bibek>tracert google.com

Tracing route to google.com [2404:6800:4007:820::200e]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  2405:201:d030:5066:b6a7:c6ff:fe50:f5ac
  2     *        *        *     Request timed out.
  3     5 ms     6 ms     6 ms  2405:203:400:100:172:31:1:38
  4    74 ms    51 ms    69 ms  2001:4860:1:1::136
  5    45 ms    25 ms    36 ms  2404:6800:80ec::1
  6    15 ms    19 ms    19 ms  2001:4860:0:1::47dc
  7    10 ms     9 ms    16 ms  2001:4860:0:1340::a
  8    13 ms    19 ms    19 ms  2001:4860::1c:4001:1d54
  9    10 ms    10 ms    11 ms  2001:4860:0:1::5653
 10    54 ms    56 ms    54 ms  maa05s25-in-x0e.1e100.net [2404:6800:4007:820::200e]

Trace complete.

C:\Users\bibek>
```



```
C:\Users\bibek>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1042         avsek:46508            ESTABLISHED
  TCP    127.0.0.1:1042         avsek:46512            ESTABLISHED
  TCP    127.0.0.1:9012         avsek:46541            ESTABLISHED
  TCP    127.0.0.1:13030        avsek:49671            ESTABLISHED
  TCP    127.0.0.1:17532        avsek:46514            ESTABLISHED
  TCP    127.0.0.1:46508        avsek:1042             ESTABLISHED
  TCP    127.0.0.1:46512        avsek:1042             ESTABLISHED
  TCP    127.0.0.1:46514        avsek:17532            ESTABLISHED
  TCP    127.0.0.1:46541        avsek:9012             ESTABLISHED
  TCP    127.0.0.1:46867        avsek:46868            ESTABLISHED
  TCP    127.0.0.1:46868        avsek:46867            ESTABLISHED
  TCP    127.0.0.1:49671        avsek:13030            ESTABLISHED
  TCP    192.168.29.87:47343    relay-5166bfb0:https   ESTABLISHED
  TCP    192.168.29.87:47348    20.198.119.143:https   ESTABLISHED
  TCP    [2405:201:d030:5066:d86b:4e30:b02d:fb67]:47913  [2603:1026:c0b:1d::2]:https  ESTABLISHED
  TCP    [2405:201:d030:5066:d86b:4e30:b02d:fb67]:47929  [2603:1046:c09:19a6::2]:https  ESTABLISHED
  TCP    [2405:201:d030:5066:d86b:4e30:b02d:fb67]:47941  [2405:200:1608:1731::312c:7181]:https  CLOSE_WAIT
  TCP    [2405:201:d030:5066:d86b:4e30:b02d:fb67]:47945  [2405:200:1608:1731::312c:71a8]:https  CLOSE_WAIT

C:\Users\bibek>
```

Conclusion:

If you are logging command line execution you will have visibility into executed processes. Once you have this visibility it opens a lot of doors for investigating alerts.