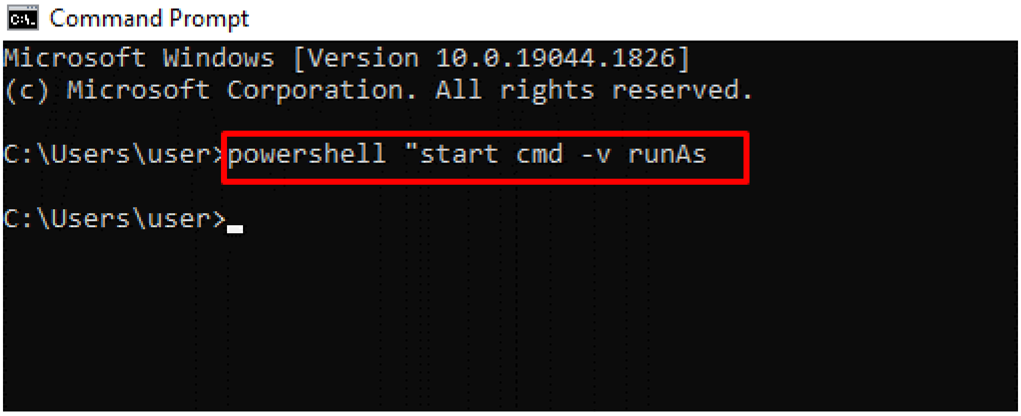
Command Line Hacking

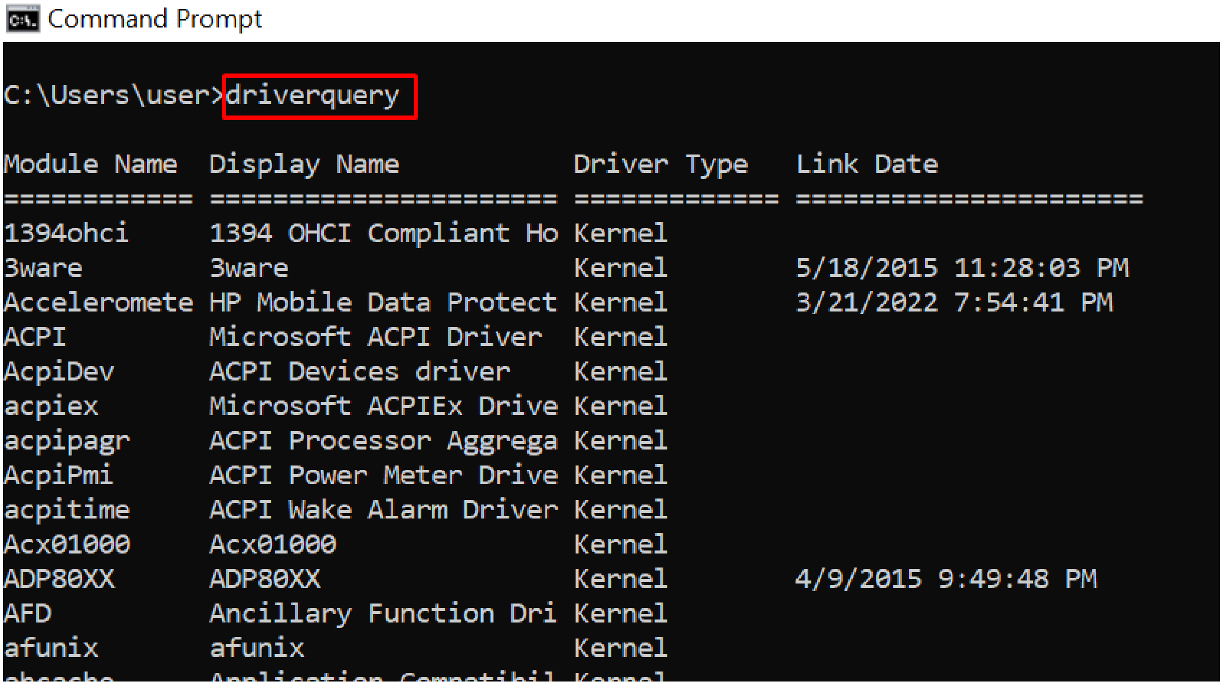
powershell start cmd -v runAs – Run the Command Prompt as an Administrator
Entering this command opens another command prompt window as an administrator:



```
Microsoft Windows [Version 10.0.19044.1826]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user>powershell "start cmd -v runAs

C:\Users\user>_
```

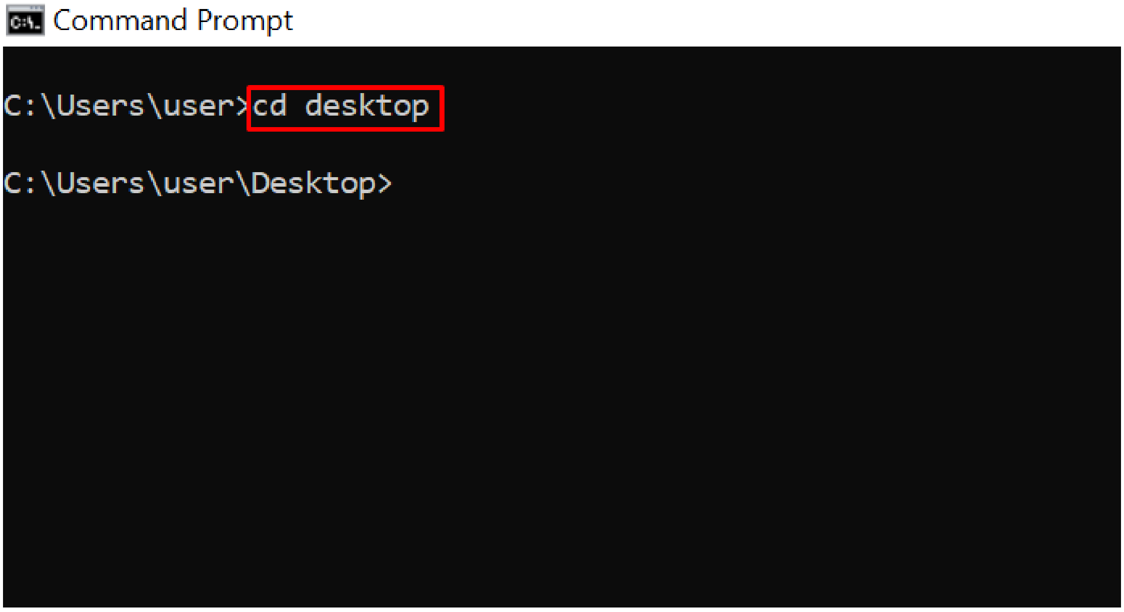
driverquery – Lists All Installed Drivers
It is important to have access to all drivers because they often cause problems.

That’s what this command does – it shows you even the drivers you won’t find in the device manager.



```
C:\Users\user>driverquery

Module Name  Display Name           Driver Type   Link Date
============ ====================== ============= ======================
1394ohci     1394 OHCI Compliant Ho Kernel
3ware        3ware                  Kernel        5/18/2015 11:28:03 PM
Acceleromete HP Mobile Data Protect Kernel        3/21/2022 7:54:41 PM
ACPI         Microsoft ACPI Driver  Kernel
AcpiDev      ACPI Devices driver    Kernel
acpiex       Microsoft ACPIEx Drive Kernel
acpipagr     ACPI Processor Aggrega Kernel
AcpiPmi      ACPI Power Meter Drive Kernel
acpitime     ACPI Wake Alarm Driver Kernel
Acx01000     Acx01000               Kernel
ADP80XX      ADP80XX                Kernel        4/9/2015 9:49:48 PM
AFD          Ancillary Function Dri Kernel
afunix       afunix                 Kernel
```

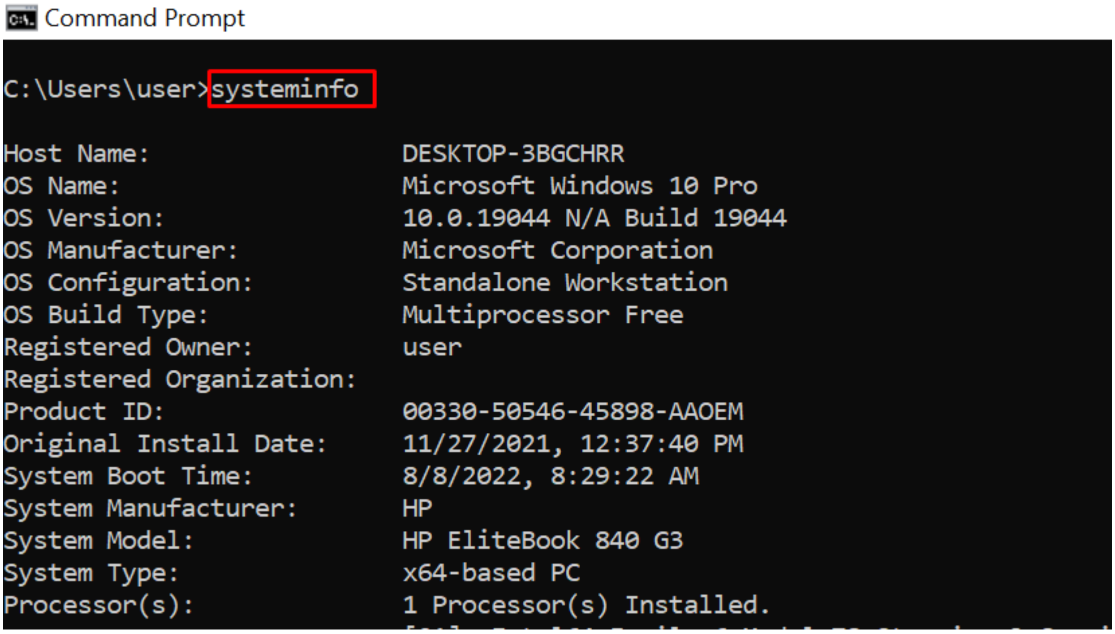
chdir or cd – Changes the Current Working Directory to the Specified Directory



```
C:\Users\user>cd desktop

C:\Users\user\Desktop>
```

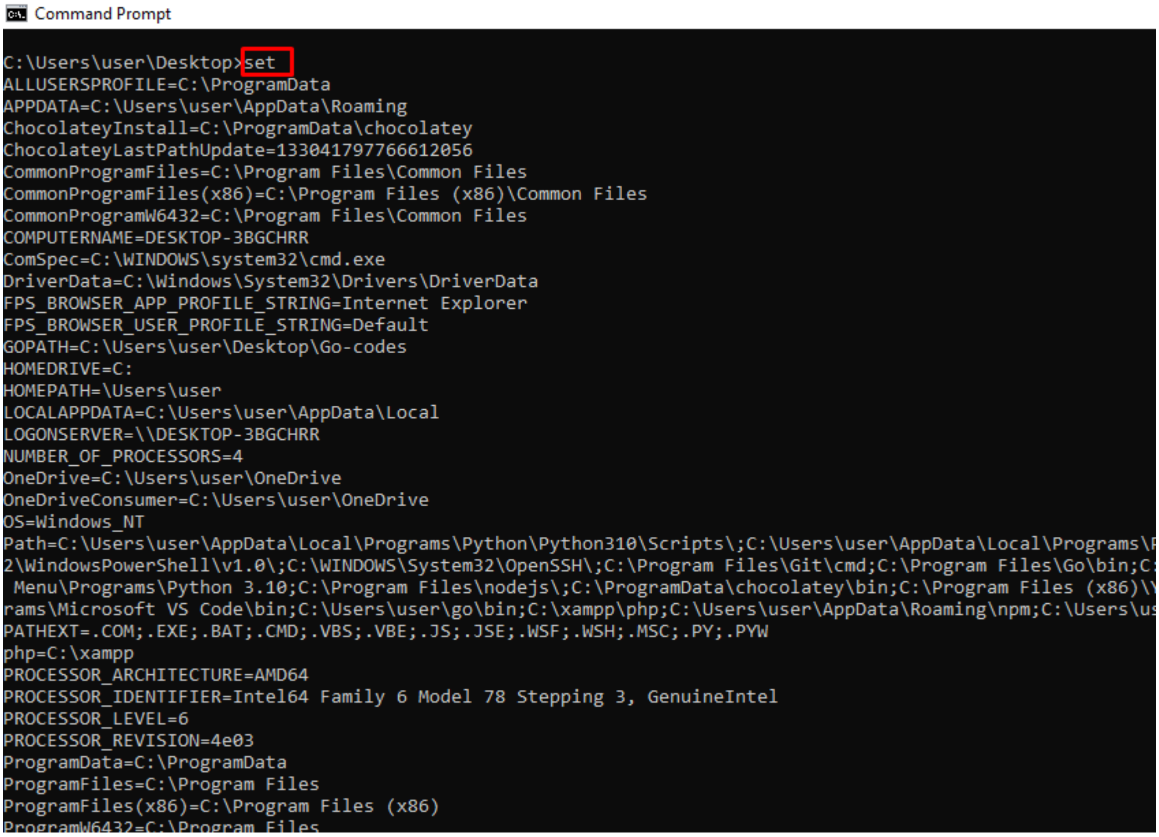
systeminfo – Shows Your PC's Details

If you want to see more detailed information about your system you won’t see in the GUI, this is the command for you.



```
C:\Users\user>systeminfo

Host Name:                 DESKTOP-3BGCHRR
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19044 N/A Build 19044
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          user
Registered Organization:
Product ID:                00330-50546-45898-AAOEM
Original Install Date:     11/27/2021, 12:37:40 PM
System Boot Time:          8/8/2022, 8:29:22 AM
System Manufacturer:       HP
System Model:              HP EliteBook 840 G3
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
```

set – Shows your PC’s Environment Variables

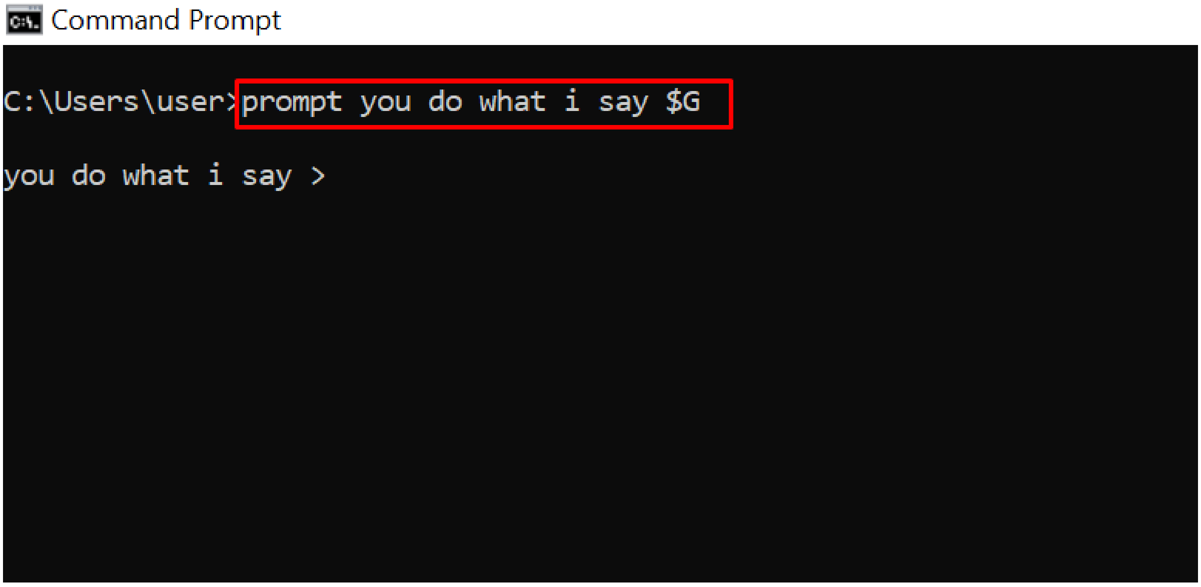


```
C:\Users\user\Desktop>set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\user\AppData\Roaming
ChocolateyInstall=C:\ProgramData\chocolatey
ChocolateyLastPathUpdate=133041797766612056
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=DESKTOP-3BGCHRR
ComSpec=C:\WINDOWS\system32\cmd.exe
DriverData=C:\Windows\System32\Drivers\DriverData
FPS_BROWSER_APP_PROFILE_STRING=Internet Explorer
FPS_BROWSER_USER_PROFILE_STRING=Default
GOPATH=C:\Users\user\Desktop\Go-codes
HOMEDRIVE=C:
HOMEPATH=\Users\user
LOCALAPPDATA=C:\Users\user\AppData\Local
LOGONSERVER=\\DESKTOP-3BGCHRR
NUMBER_OF_PROCESSORS=4
OneDrive=C:\Users\user\OneDrive
OneDriveConsumer=C:\Users\user\OneDrive
OS=Windows_NT
Path=C:\Users\user\AppData\Local\Programs\Python\Python310\Scripts\;C:\Users\user\AppData\Local\Programs\P
2\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Program Files\Git\cmd;C:\Program Files\Go\bin;C:
 Menu\Programs\Python 3.10;C:\Program Files\nodejs\;C:\ProgramData\chocolatey\bin;C:\Program Files (x86)\Y
rams\Microsoft VS Code\bin;C:\Users\user\go\bin;C:\xampp\php;C:\Users\user\AppData\Roaming\npm;C:\Users\us
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.PY;.PYW
php=C:\xampp
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 78 Stepping 3, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=4e03
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
```

prompt – Changes the Default Text Shown before Entering Commands

By default, the command prompt shows the C drive path to your user account.

You can use the prompt command to change that default text with the syntax prompt prompt_name $G:

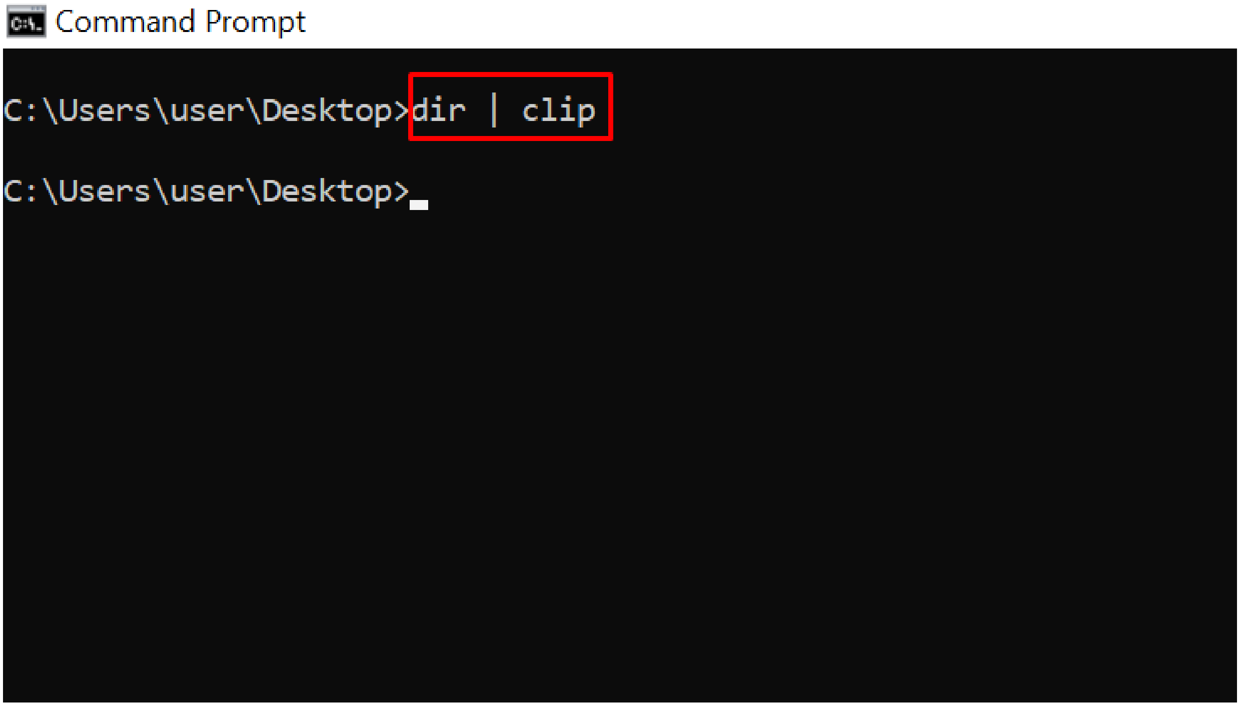


```
C:\Users\user>prompt you do what i say $G

you do what i say >
```

N.B: If you don't append $G to the command, you won't get the greater than symbol in front of the text.

clip – Copies an Item to the Clipboard

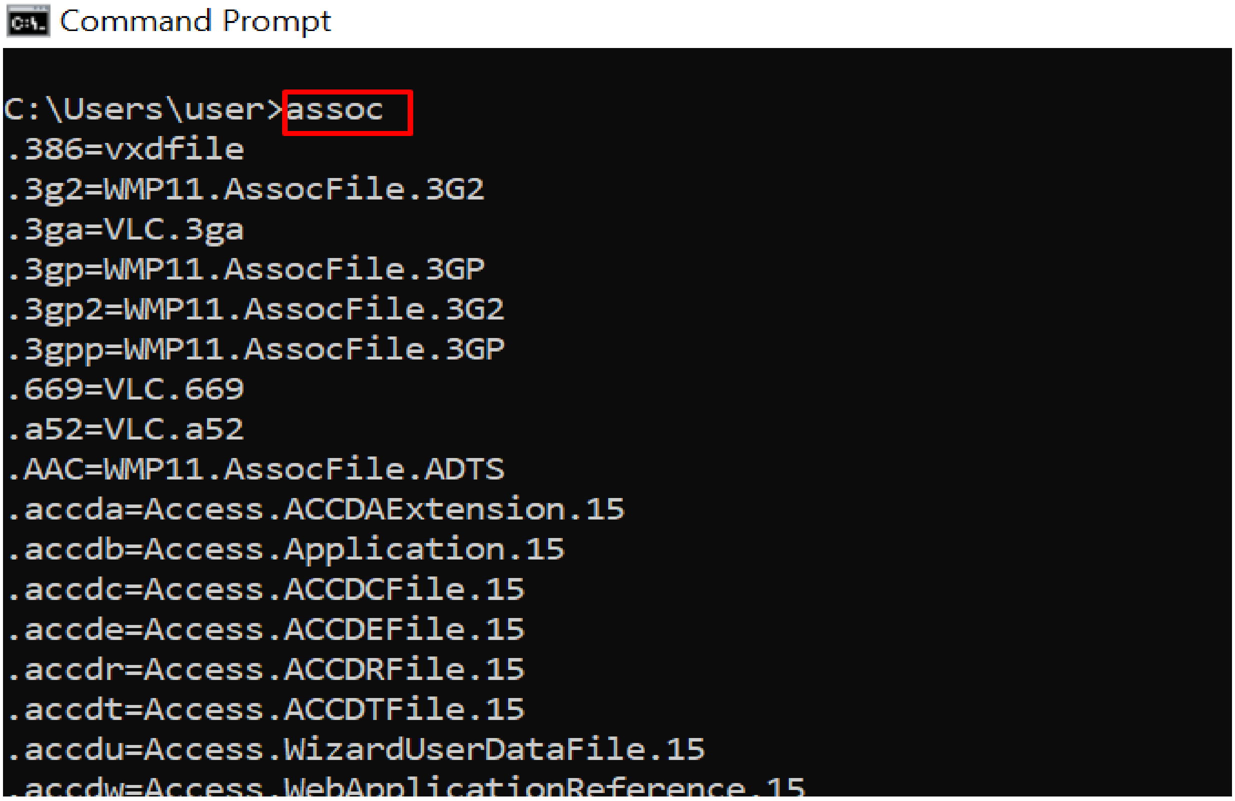
For example, dir | clip copies all the content of the present working directory to the clipboard.



```
C:\Users\user\Desktop>dir | clip

C:\Users\user\Desktop>_
```

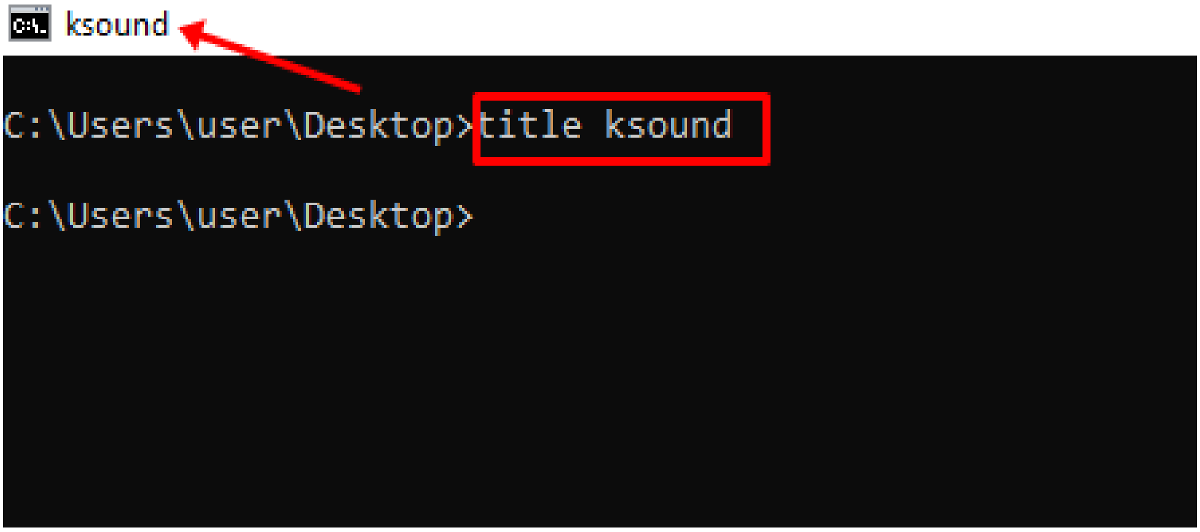
You can type clip /? and hit ENTER to see how to use it.

assoc – Lists Programs and the Extensions They are Associated With



```
C:\Users\user>assoc
.386=vxdfile
.3g2=WMP11.AssocFile.3G2
.3ga=VLC.3ga
.3gp=WMP11.AssocFile.3GP
.3gp2=WMP11.AssocFile.3G2
.3gpp=WMP11.AssocFile.3GP
.669=VLC.669
.a52=VLC.a52
.AAC=WMP11.AssocFile.ADTS
.accda=Access.ACCDAExtension.15
.accdb=Access.Application.15
.accdc=Access.ACCDCFile.15
.accde=Access.ACCDEFile.15
.accdr=Access.ACCDRFile.15
.accdt=Access.ACCDTFile.15
.accdu=Access.WizardUserDataFile.15
.accdw=Access.WebApplicationReference.15
```

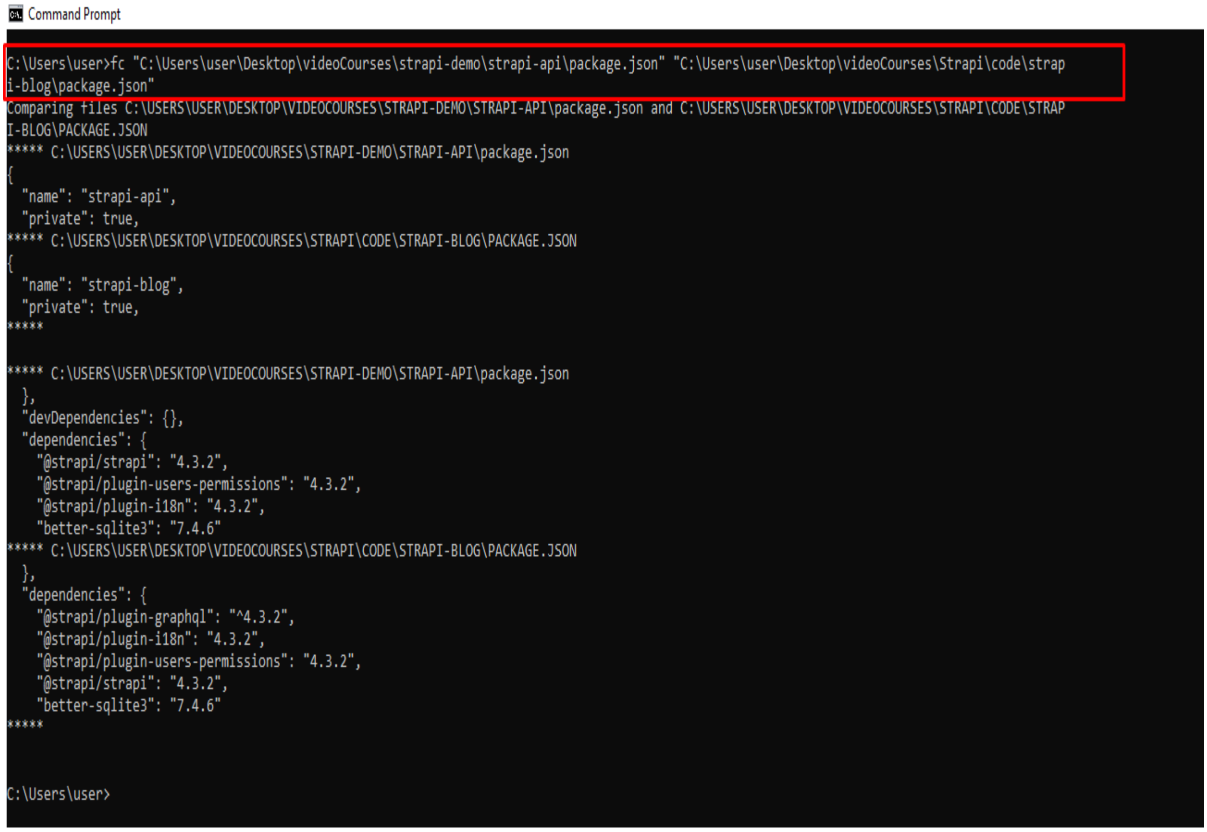
title – Changes the Command Prompt Window Title Using the Format title window-title-name



```
C:\Users\user\Desktop>title ksound

C:\Users\user\Desktop>
```

fc – Compares Two Similar Files

If you are a programmer or writer and you want to quickly see what differs between two files, you can enter this command and then the full path to the two files. For example fc “file-1-path” “file-2-path”.

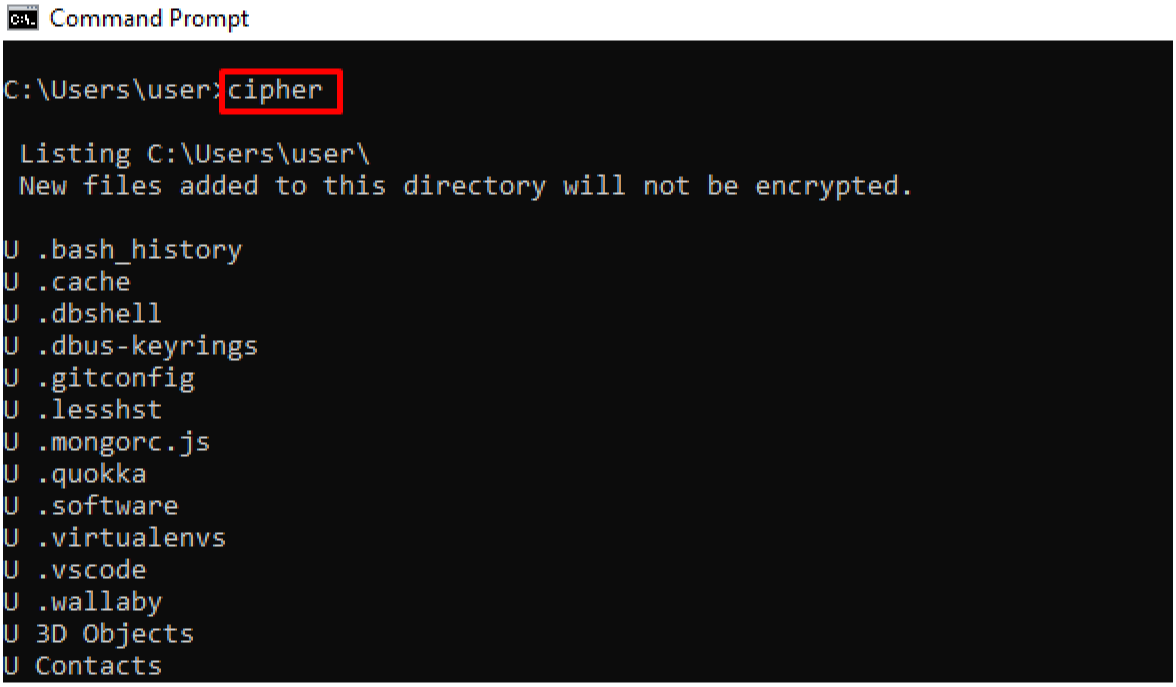


```
C:\Users\user>fc "C:\Users\user\Desktop\videoCourses\strapi-demo\strapi-api\package.json" "C:\Users\user\Desktop\videoCourses\Strapi\code\strap
i-blog\package.json"
Comparing files C:\USERS\USER\DESKTOP\VIDEOCOURSES\STRAPI-DEMO\STRAPI-API\package.json and C:\USERS\USER\DESKTOP\VIDEOCOURSES\STRAPI\CODE\STRAP
I-BLOG\PACKAGE.JSON
***** C:\USERS\USER\DESKTOP\VIDEOCOURSES\STRAPI-DEMO\STRAPI-API\package.json
{
  "name": "strapi-api",
  "private": true,
***** C:\USERS\USER\DESKTOP\VIDEOCOURSES\STRAPI\CODE\STRAPI-BLOG\PACKAGE.JSON
{
  "name": "strapi-blog",
  "private": true,
*****

***** C:\USERS\USER\DESKTOP\VIDEOCOURSES\STRAPI-DEMO\STRAPI-API\package.json
  },
  "devDependencies": {},
  "dependencies": {
    "@strapi/strapi": "4.3.2",
    "@strapi/plugin-users-permissions": "4.3.2",
    "@strapi/plugin-i18n": "4.3.2",
    "better-sqlite3": "7.4.6"
***** C:\USERS\USER\DESKTOP\VIDEOCOURSES\STRAPI\CODE\STRAPI-BLOG\PACKAGE.JSON
  },
  "dependencies": {
    "@strapi/plugin-graphql": "^4.3.2",
    "@strapi/plugin-i18n": "4.3.2",
    "@strapi/plugin-users-permissions": "4.3.2",
    "@strapi/strapi": "4.3.2",
    "better-sqlite3": "7.4.6"
*****


C:\Users\user>
```

cipher – Wipes Free Space and Encrypts Data

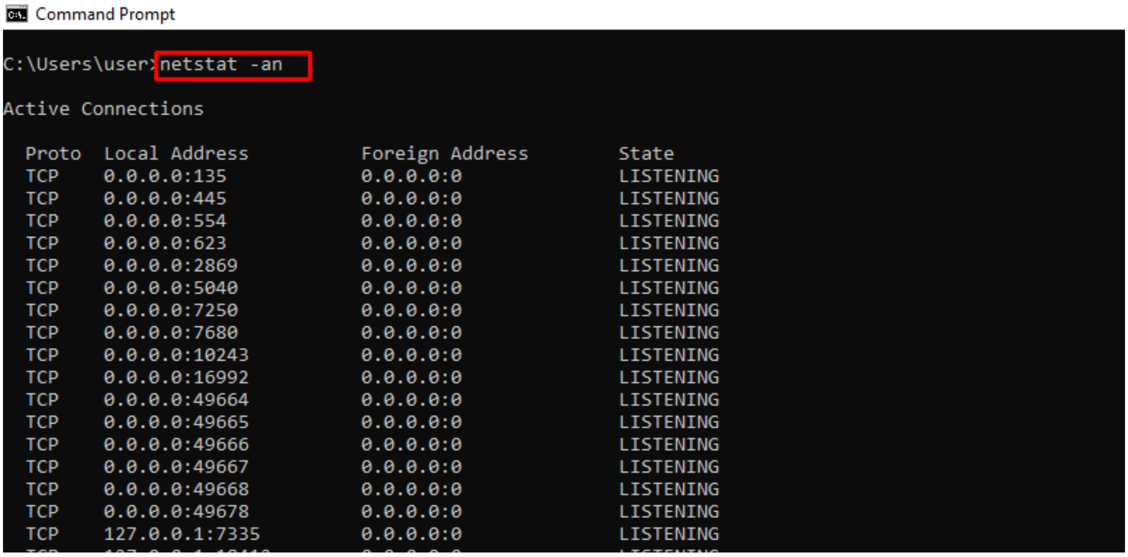
On a PC, deleted files remain accessible to you and other users. So, technically, they are not deleted under the hood.

You can use the cipher command to wipe the drive clean and encrypt such files.



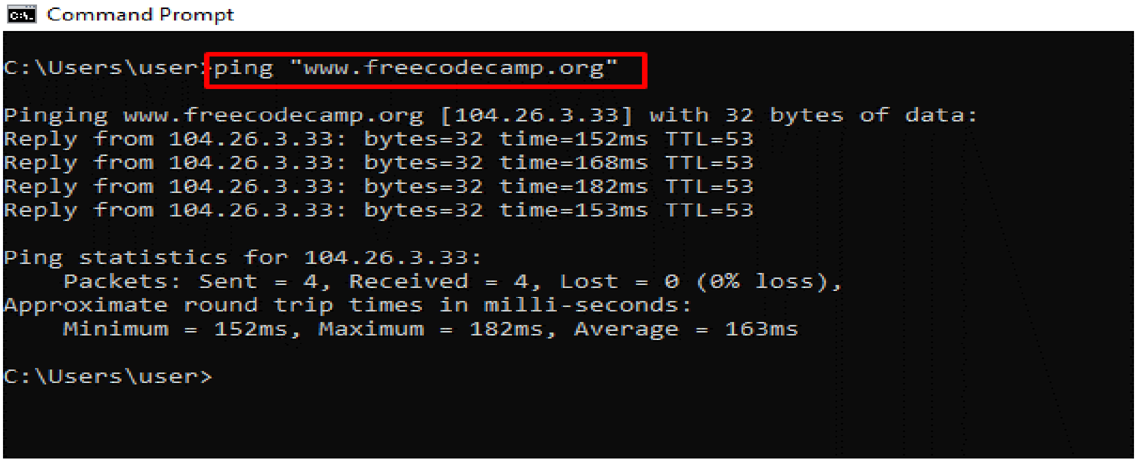
```
C:\Users\user>cipher

 Listing C:\Users\user\
 New files added to this directory will not be encrypted.

U .bash_history
U .cache
U .dbshell
U .dbus-keyrings
U .gitconfig
U .lesshst
U .mongorc.js
U .quokka
U .software
U .virtualenvs
U .vscode
U .wallaby
U 3D Objects
U Contacts
```

netstat -an – Shows Open Ports, their IP Addresses and States



```
C:\Users\user>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:554            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:623            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7250           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:10243          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:16992          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49678          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:7335         0.0.0.0:0              LISTENING
```

ping – Shows a Website IP Address, Lets you Know How Long it Takes to Transmit Data and a Get Response

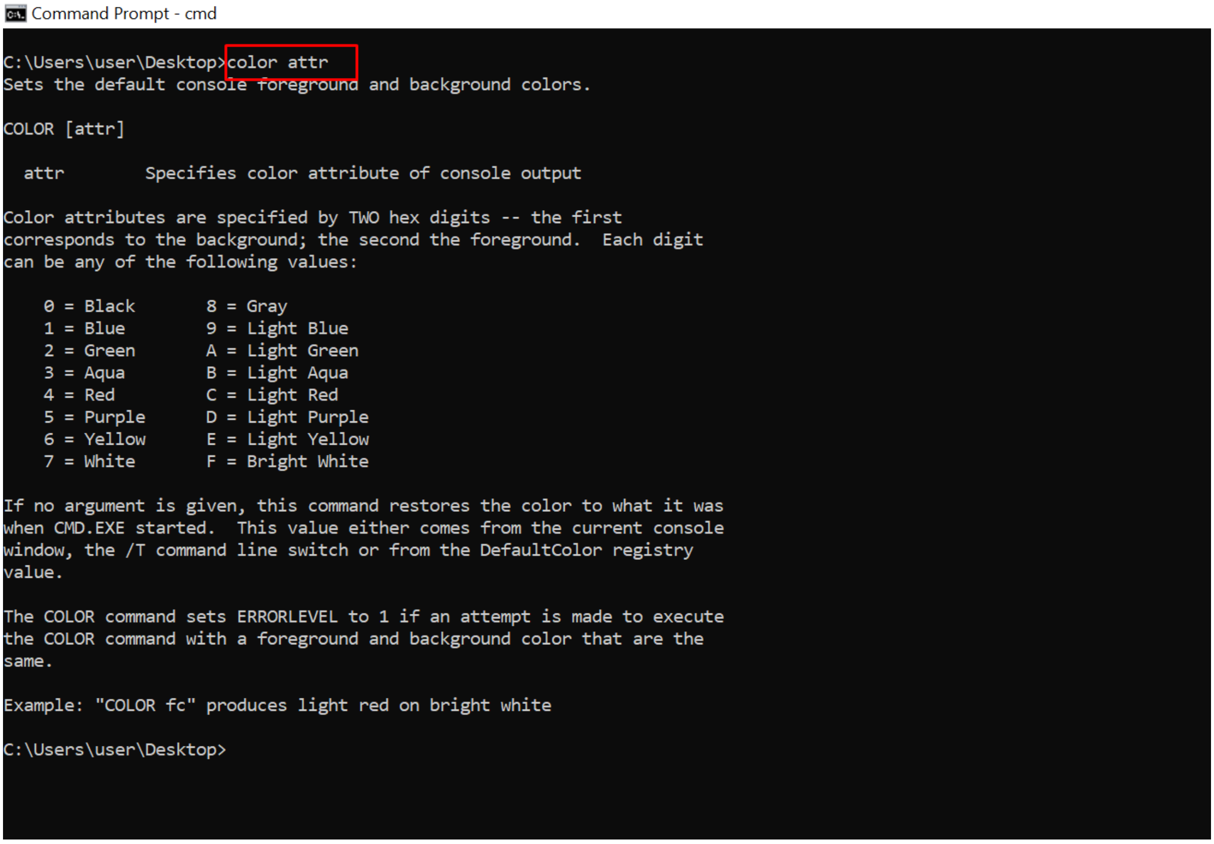


Command Prompt

```
C:\Users\user>ping "www.freecodecamp.org"

Pinging www.freecodecamp.org [104.26.3.33] with 32 bytes of data:
Reply from 104.26.3.33: bytes=32 time=152ms TTL=53
Reply from 104.26.3.33: bytes=32 time=168ms TTL=53
Reply from 104.26.3.33: bytes=32 time=182ms TTL=53
Reply from 104.26.3.33: bytes=32 time=153ms TTL=53

Ping statistics for 104.26.3.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 152ms, Maximum = 182ms, Average = 163ms

C:\Users\user>
```

color – Changes the Text Color of the Command Prompt

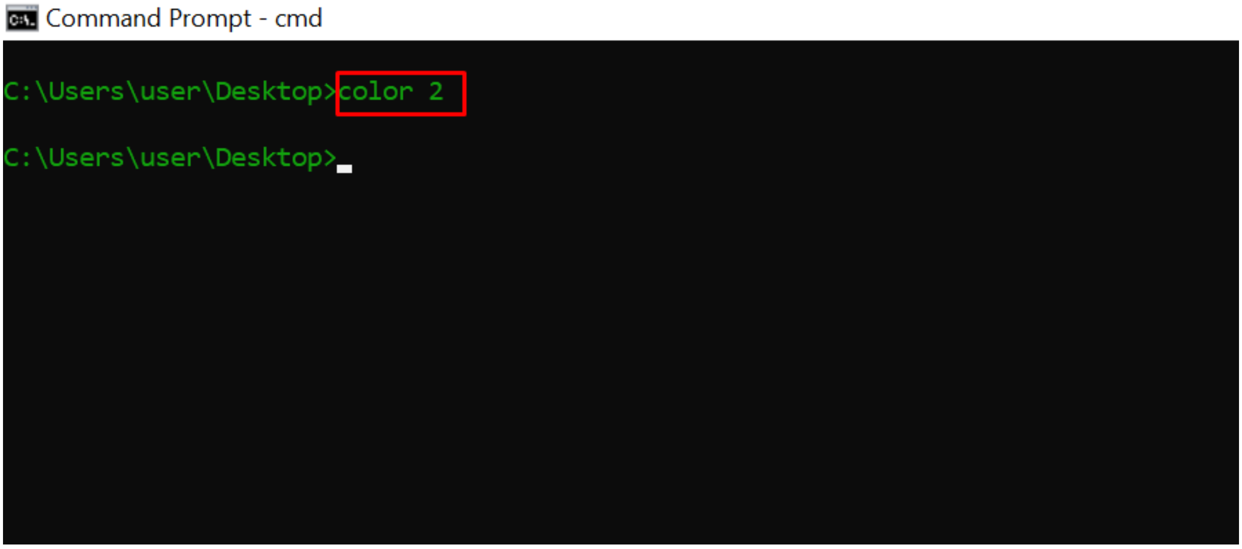
Enter color attr to see the colors you can change to:



Command Prompt - cmd

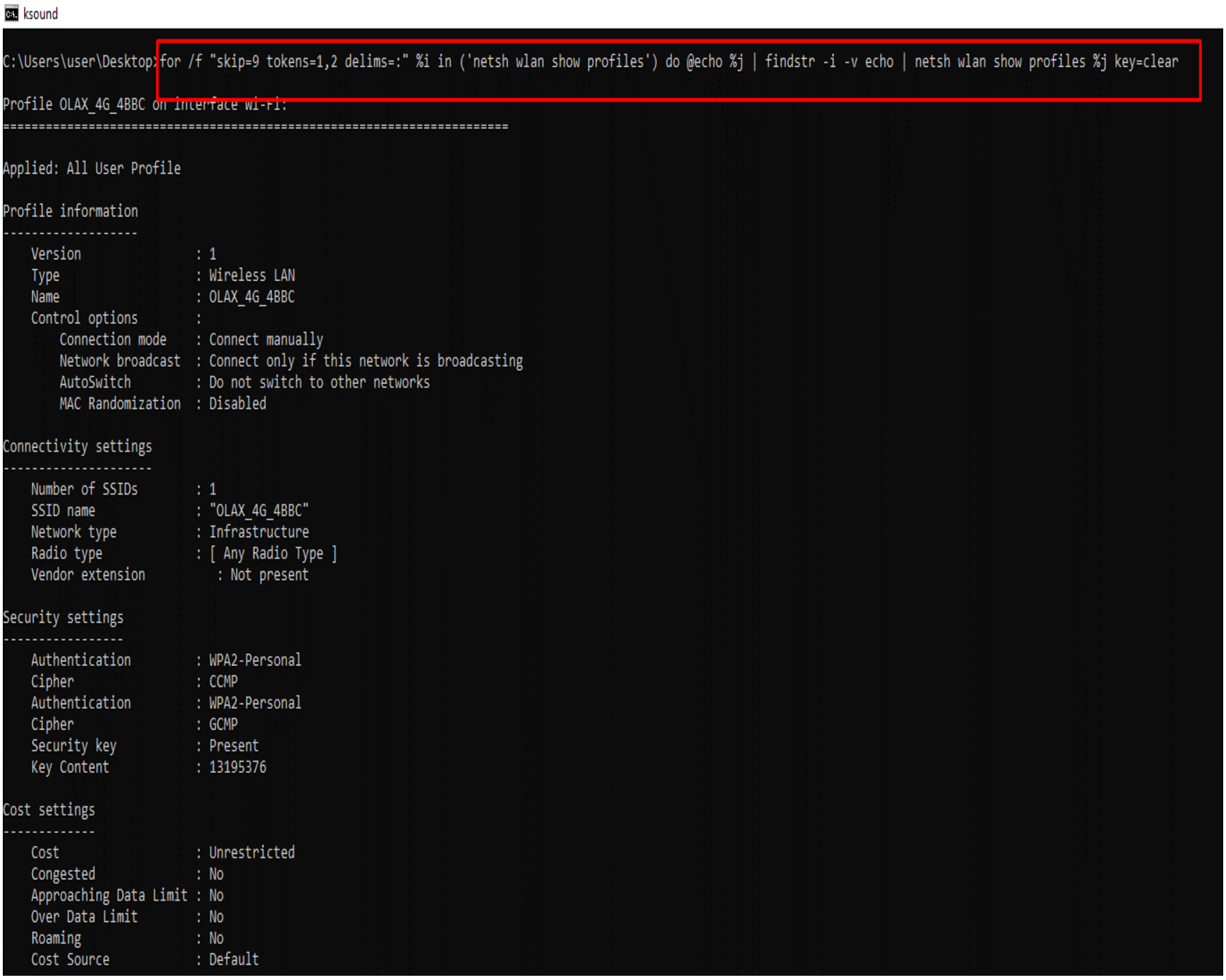
```
C:\Users\user\Desktop>color attr
Sets the default console foreground and background colors.

COLOR [attr]

  attr        Specifies color attribute of console output

Color attributes are specified by TWO hex digits -- the first
corresponds to the background; the second the foreground.  Each digit
can be any of the following values:

    0 = Black       8 = Gray
    1 = Blue        9 = Light Blue
    2 = Green       A = Light Green
    3 = Aqua        B = Light Aqua
    4 = Red         C = Light Red
    5 = Purple      D = Light Purple
    6 = Yellow      E = Light Yellow
    7 = White       F = Bright White

If no argument is given, this command restores the color to what it was
when CMD.EXE started.  This value either comes from the current console
window, the /T command line switch or from the DefaultColor registry
value.

The COLOR command sets ERRORLEVEL to 1 if an attempt is made to execute
the COLOR command with a foreground and background color that are the
same.

Example: "COLOR fc" produces light red on bright white

C:\Users\user\Desktop>
```

Entering color 2 changes the color of the terminal to green:


Command Prompt - cmd

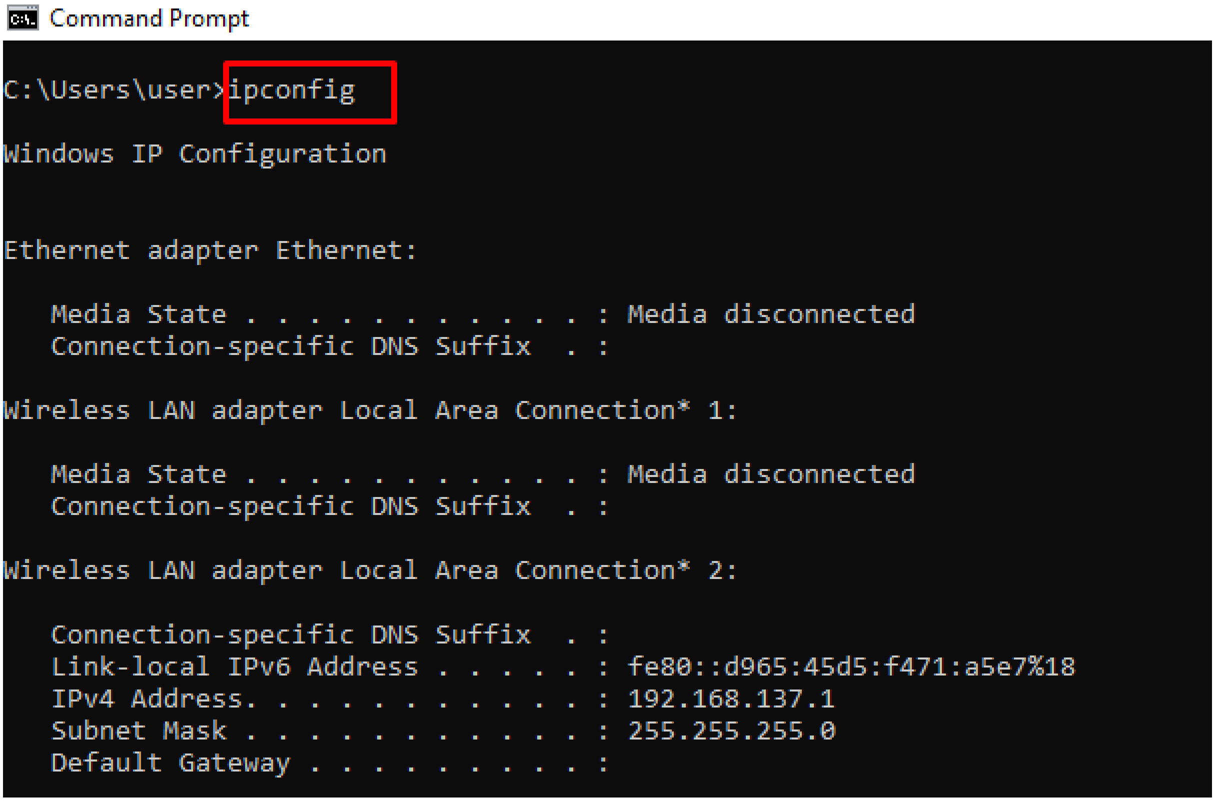
```
C:\Users\user\Desktop>color 2

C:\Users\user\Desktop>_
```

for /f "skip=9 tokens=1,2 delims=:" %i in ('netsh wlan show profiles') do @echo %j | findstr -i -v echo | netsh wlan show profiles %j key=clear – Shows All Wi-Fi Passwords


ksound

```
C:\Users\user\Desktop>for /f "skip=9 tokens=1,2 delims=:" %i in ('netsh wlan show profiles') do @echo %j | findstr -i -v echo | netsh wlan show profiles %j key=clear

Profile OLAX_4G_4BBC on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : OLAX_4G_4BBC
    Control options        :
        Connection mode    : Connect manually
        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              : "OLAX_4G_4BBC"
    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            : 13195376

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

ipconfig – Shows Information about PC IP Addresses and Connections



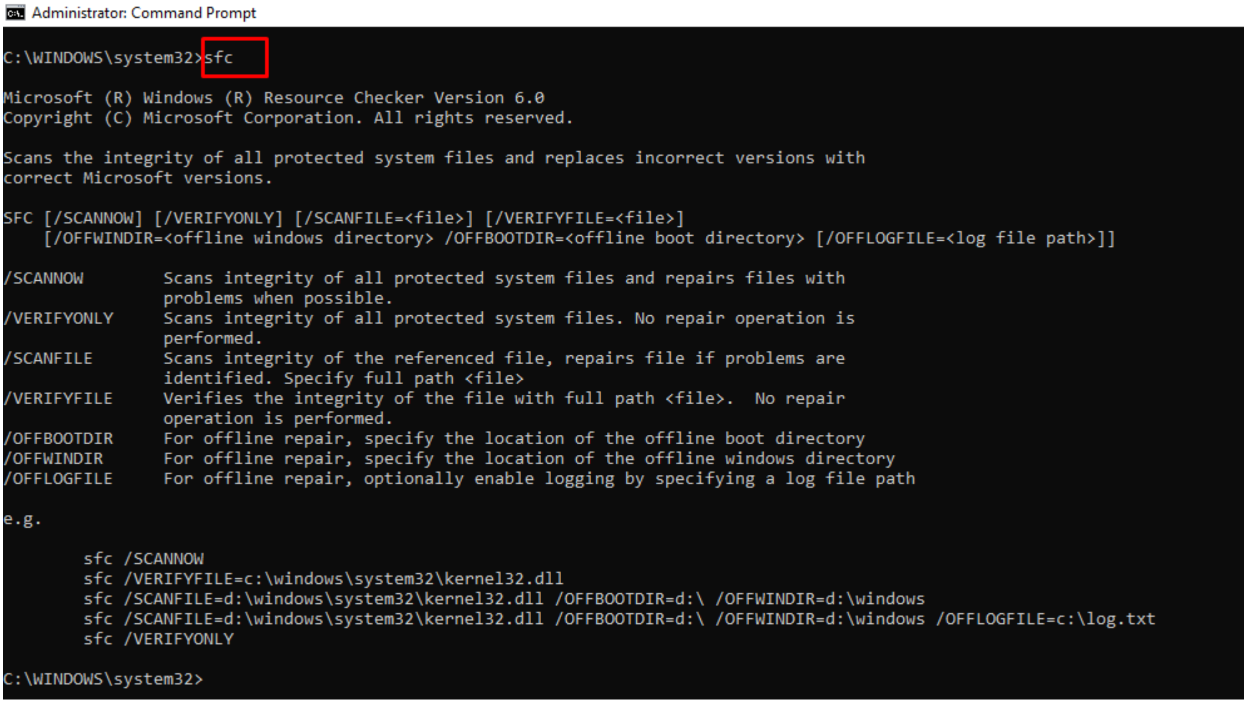
Command Prompt

```
C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d965:45d5:f471:a5e7%18
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

This command also has extensions such as ipconfig /release, ipconfig /renew, and ipconfig /flushdns which you can use to troubleshoot issues with internet connections.

sfc – System File Checker

This command scans your computer for corrupt files and repairs them. The extension of the command you can use to run a scan is /scannow.

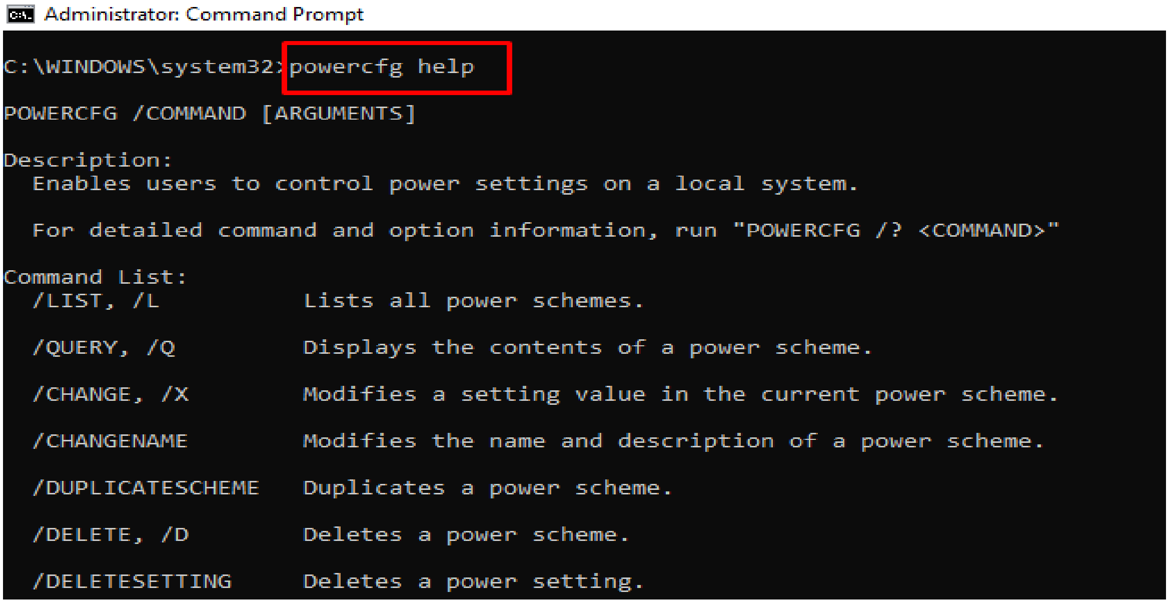


Administrator: Command Prompt

```
C:\WINDOWS\system32>sfc

Microsoft (R) Windows (R) Resource Checker Version 6.0
Copyright (C) Microsoft Corporation. All rights reserved.

Scans the integrity of all protected system files and replaces incorrect versions with
correct Microsoft versions.

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<file>] [/VERIFYFILE=<file>]
    [/OFFWINDIR=<offline windows directory> /OFFBOOTDIR=<offline boot directory> [/OFFLOGFILE=<log file path>]]

/SCANNOW        Scans integrity of all protected system files and repairs files with
                problems when possible.
/VERIFYONLY     Scans integrity of all protected system files. No repair operation is
                performed.
/SCANFILE       Scans integrity of the referenced file, repairs file if problems are
                identified. Specify full path <file>
/VERIFYFILE     Verifies the integrity of the file with full path <file>.  No repair
                operation is performed.
/OFFBOOTDIR     For offline repair, specify the location of the offline boot directory
/OFFWINDIR      For offline repair, specify the location of the offline windows directory
/OFFLOGFILE     For offline repair, optionally enable logging by specifying a log file path

e.g.

        sfc /SCANNOW
        sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
        sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows
        sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows /OFFLOGFILE=c:\log.txt
        sfc /VERIFYONLY

C:\WINDOWS\system32>
```

powercfg – Controls Configurable Power Settings
You can use this command with its several extensions to show information about the power state of your PC.

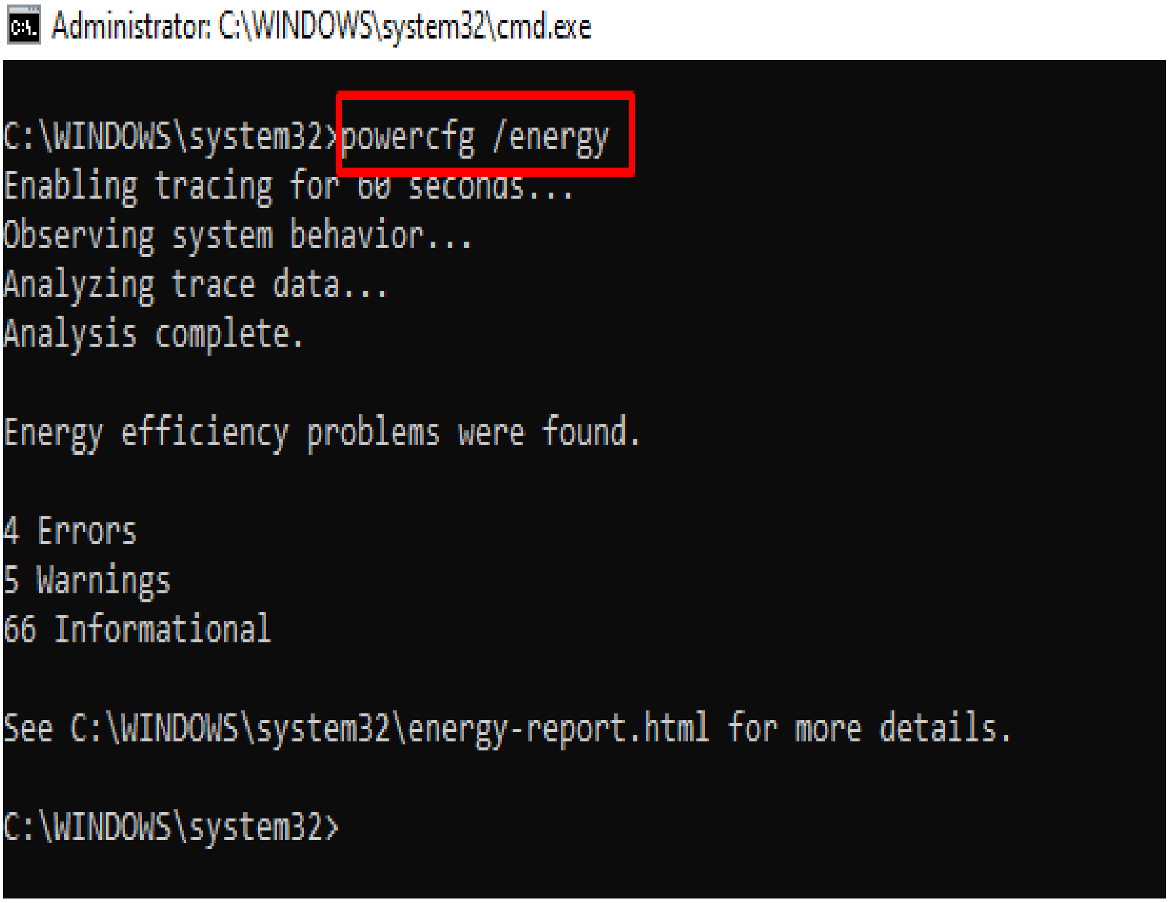
You can enter powercfg help to show those extensions.



Administrator: Command Prompt

```
C:\WINDOWS\system32>powercfg help

POWERCFG /COMMAND [ARGUMENTS]

Description:
  Enables users to control power settings on a local system.

  For detailed command and option information, run "POWERCFG /? <COMMAND>"

Command List:
  /LIST, /L            Lists all power schemes.

  /QUERY, /Q           Displays the contents of a power scheme.

  /CHANGE, /X          Modifies a setting value in the current power scheme.

  /CHANGENAME          Modifies the name and description of a power scheme.

  /DUPLICATESCHEME     Duplicates a power scheme.

  /DELETE, /D          Deletes a power scheme.

  /DELETESETTING       Deletes a power setting.
```

For example, you can use powercfg /energy to generate a battery health report.

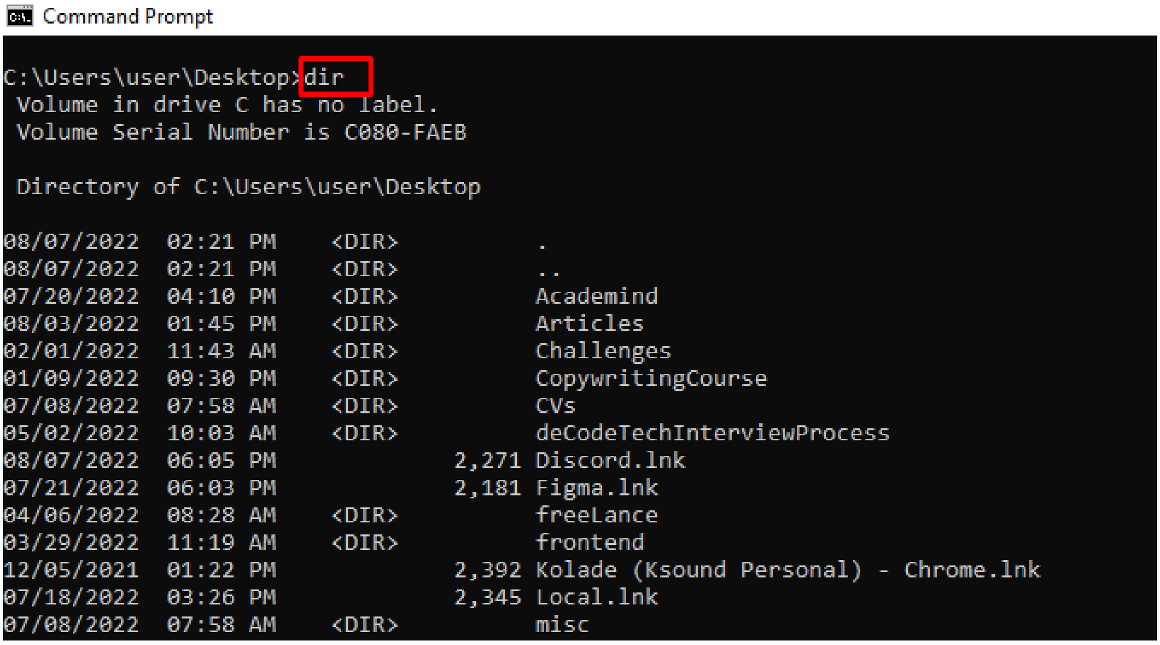


Administrator: C:\WINDOWS\system32\cmd.exe

```
C:\WINDOWS\system32>powercfg /energy
Enabling tracing for 60 seconds...
Observing system behavior...
Analyzing trace data...
Analysis complete.

Energy efficiency problems were found.

4 Errors
5 Warnings
66 Informational

See C:\WINDOWS\system32\energy-report.html for more details.

C:\WINDOWS\system32>
```

The powercfg /energy command will generate an HTML file containing the report. You can find the HTML file in C:\Windows\system32\energy-report.html.

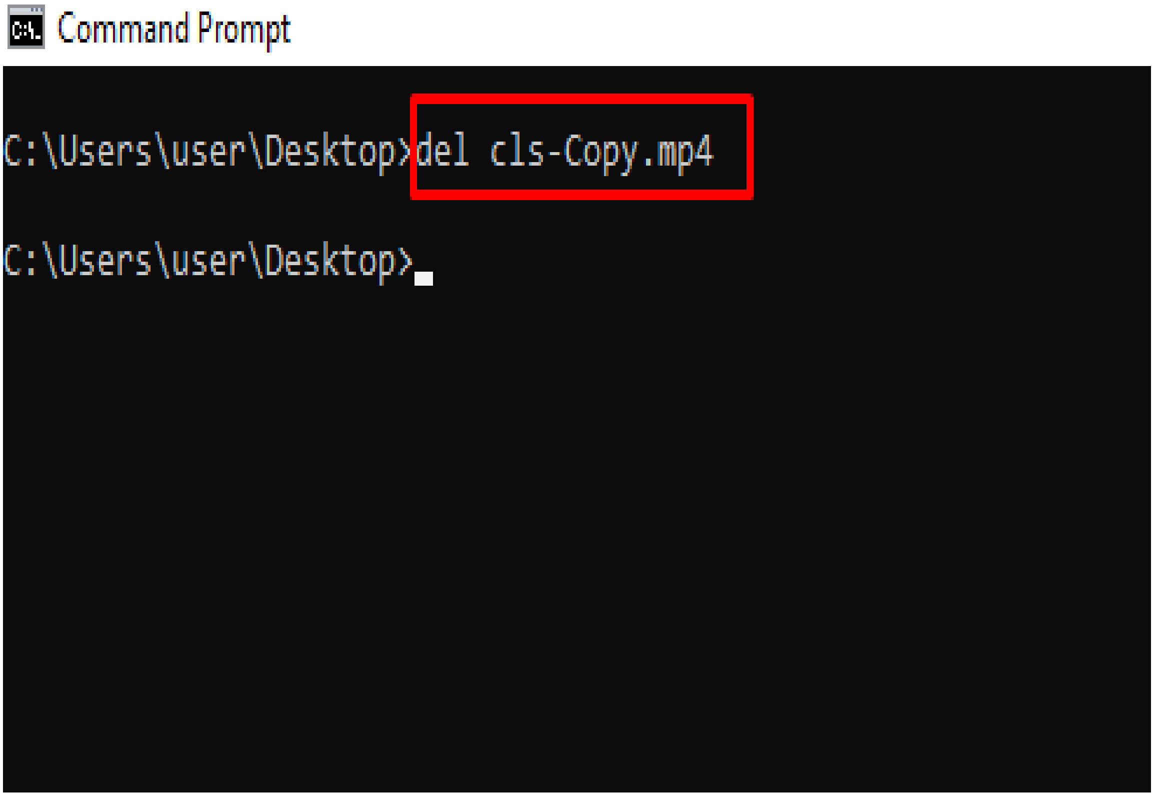
dir – Lists Items in a Directory



Command Prompt

```
C:\Users\user\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is C080-FAEB

 Directory of C:\Users\user\Desktop

08/07/2022  02:21 PM    <DIR>          .
08/07/2022  02:21 PM    <DIR>          ..
07/20/2022  04:10 PM    <DIR>          Academind
08/03/2022  01:45 PM    <DIR>          Articles
02/01/2022  11:43 AM    <DIR>          Challenges
01/09/2022  09:30 PM    <DIR>          CopywritingCourse
07/08/2022  07:58 AM    <DIR>          CVs
05/02/2022  10:03 AM    <DIR>          deCodeTechInterviewProcess
08/07/2022  06:05 PM             2,271 Discord.lnk
07/21/2022  06:03 PM             2,181 Figma.lnk
04/06/2022  08:28 AM    <DIR>          freeLance
03/29/2022  11:19 AM    <DIR>          frontend
12/05/2021  01:22 PM             2,392 Kolade (Ksound Personal) - Chrome.lnk
07/18/2022  03:26 PM             2,345 Local.lnk
07/08/2022  07:58 AM    <DIR>          misc
```

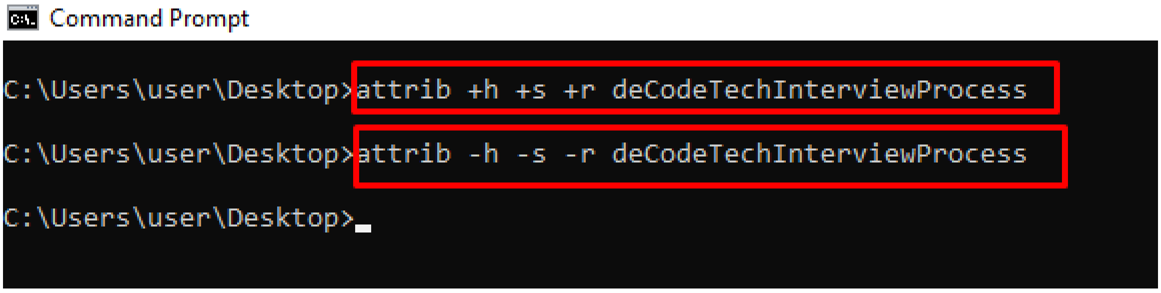
del – Deletes a File



Command Prompt

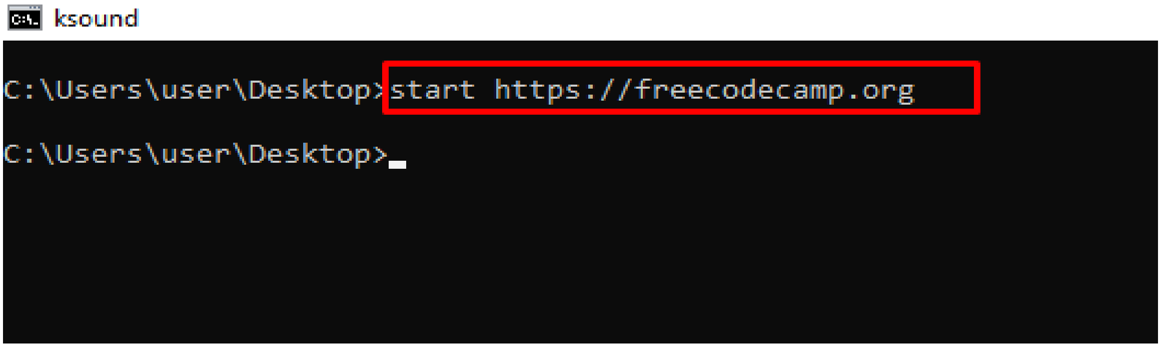
```
C:\Users\user\Desktop>del cls-Copy.mp4

C:\Users\user\Desktop>_
```

attrib +h +s +r folder_name – Hides a Folder
You can hide a folder right from the command line by typing in attrib +h +s +r folder_name and then pressing ENTER.
To show the folder again, execute the command – attrib -h -s -r folder_name.



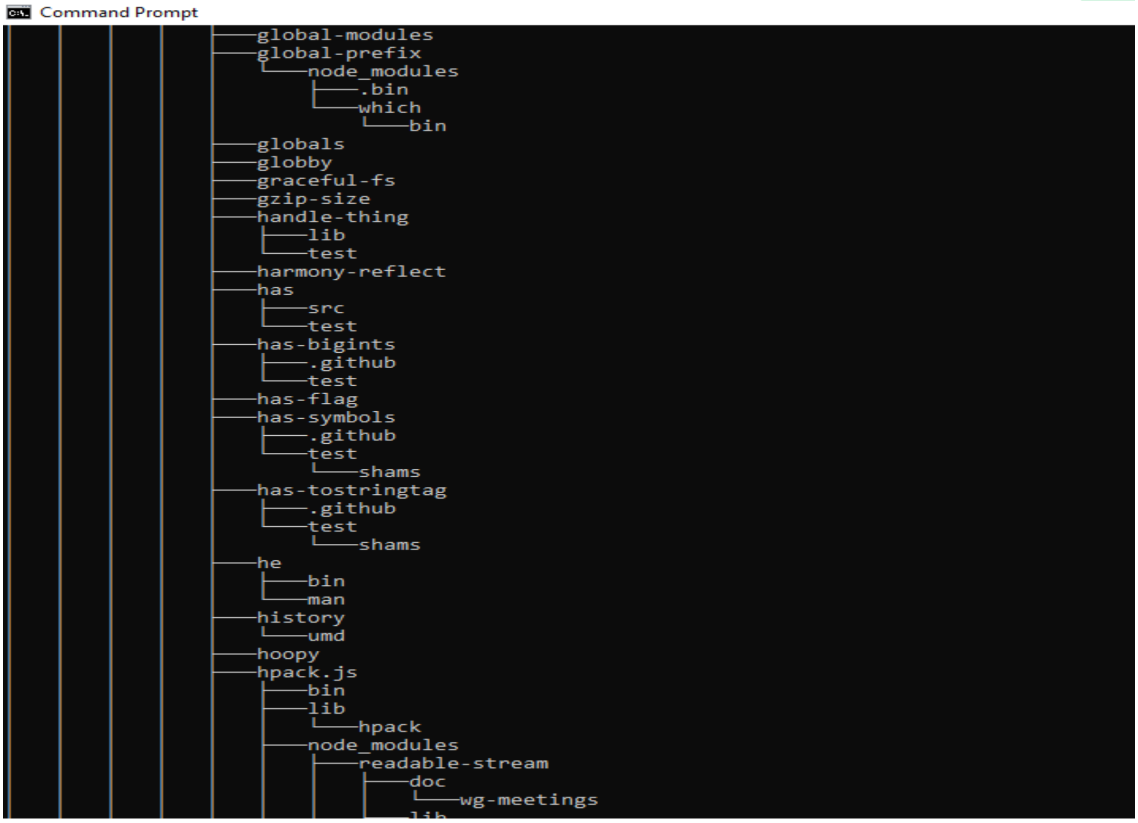
```
C:\Users\user\Desktop>attrib +h +s +r deCodeTechInterviewProcess

C:\Users\user\Desktop>attrib -h -s -r deCodeTechInterviewProcess

C:\Users\user\Desktop>_
```

start website-address – Logs on to a Website from the Command Line



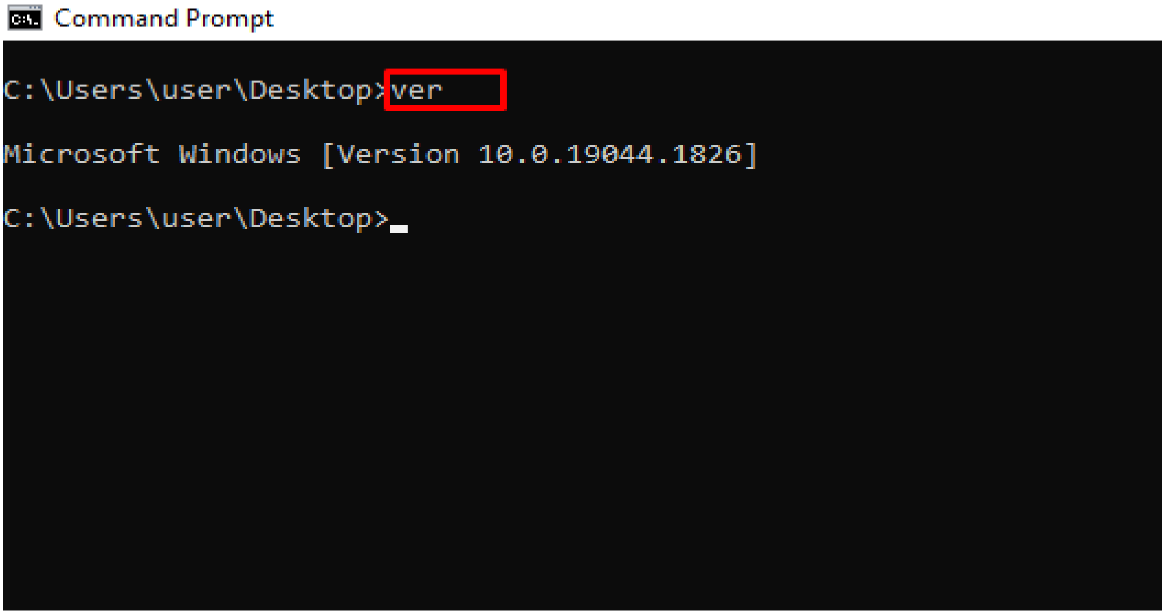
```
C:\Users\user\Desktop>start https://freecodecamp.org

C:\Users\user\Desktop>_
```

tree – Shows the Tree of the Current Directory or Specified Drive



```
│   │   │   │   ├───global-modules
│   │   │   │   ├───global-prefix
│   │   │   │   │   └───node_modules
│   │   │   │   │       ├───.bin
│   │   │   │   │       └───which
│   │   │   │   │           └───bin
│   │   │   │   ├───globals
│   │   │   │   ├───globby
│   │   │   │   ├───graceful-fs
│   │   │   │   ├───gzip-size
│   │   │   │   ├───handle-thing
│   │   │   │   │   ├───lib
│   │   │   │   │   └───test
│   │   │   │   ├───harmony-reflect
│   │   │   │   ├───has
│   │   │   │   │   ├───src
│   │   │   │   │   └───test
│   │   │   │   ├───has-bigints
│   │   │   │   │   ├───.github
│   │   │   │   │   └───test
│   │   │   │   ├───has-flag
│   │   │   │   ├───has-symbols
│   │   │   │   │   ├───.github
│   │   │   │   │   └───test
│   │   │   │   │       └───shams
│   │   │   │   ├───has-tostringtag
│   │   │   │   │   ├───.github
│   │   │   │   │   └───test
│   │   │   │   │       └───shams
│   │   │   │   ├───he
│   │   │   │   │   ├───bin
│   │   │   │   │   └───man
│   │   │   │   ├───history
│   │   │   │   │   └───umd
│   │   │   │   ├───hoopy
│   │   │   │   ├───hpack.js
│   │   │   │   │   ├───bin
│   │   │   │   │   ├───lib
│   │   │   │   │   │   └───hpack
│   │   │   │   │   ├───node_modules
│   │   │   │   │   │   ├───readable-stream
│   │   │   │   │   │   │   ├───doc
│   │   │   │   │   │   │   │   └───wg-meetings
│   │   │   │   │   │   │   ├───lib
```

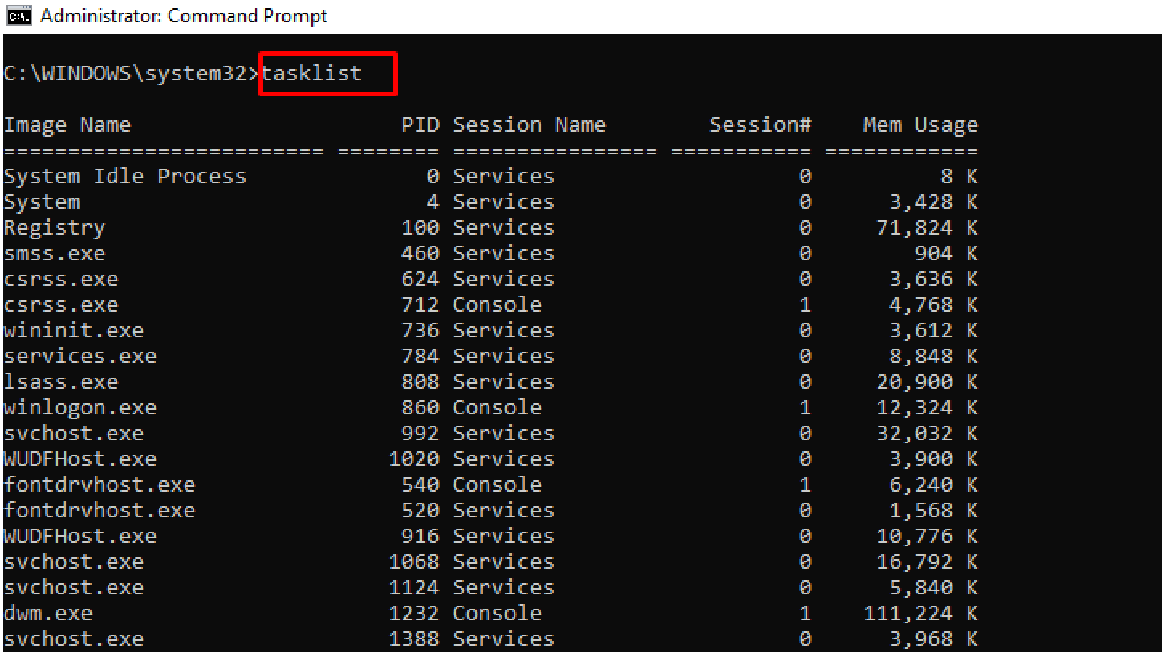
ver – Shows the Version of the OS



```
C:\Users\user\Desktop>ver

Microsoft Windows [Version 10.0.19044.1826]

C:\Users\user\Desktop>_
```

tasklist – Shows Open Programs

You can do the same thing you do with the task manager with this command:

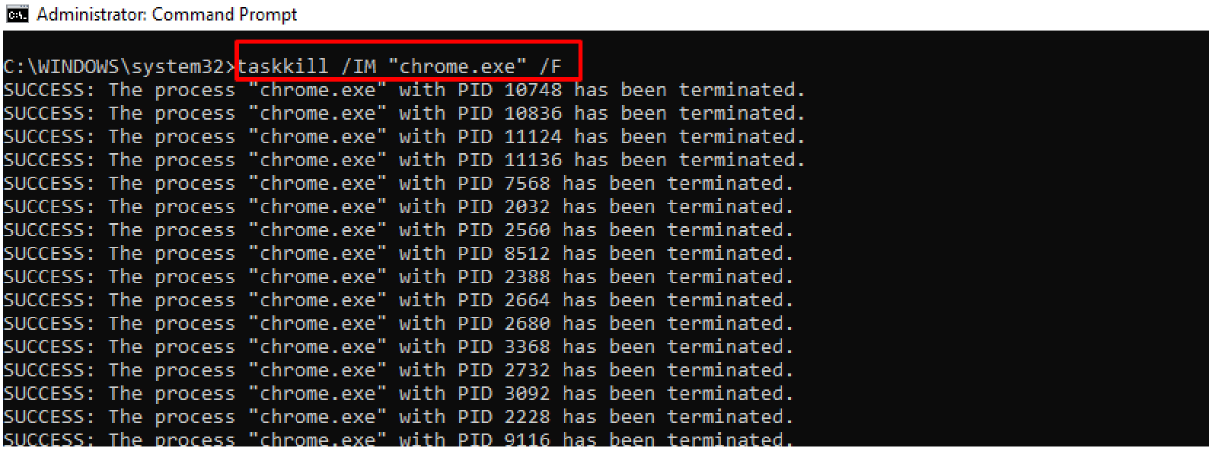


```
C:\WINDOWS\system32>tasklist

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      3,428 K
Registry                       100 Services                   0     71,824 K
smss.exe                       460 Services                   0        904 K
csrss.exe                      624 Services                   0      3,636 K
csrss.exe                      712 Console                    1      4,768 K
wininit.exe                    736 Services                   0      3,612 K
services.exe                   784 Services                   0      8,848 K
lsass.exe                      808 Services                   0     20,900 K
winlogon.exe                   860 Console                    1     12,324 K
svchost.exe                    992 Services                   0     32,032 K
WUDFHost.exe                  1020 Services                   0      3,900 K
fontdrvhost.exe                540 Console                    1      6,240 K
fontdrvhost.exe                520 Services                   0      1,568 K
WUDFHost.exe                   916 Services                   0     10,776 K
svchost.exe                   1068 Services                   0     16,792 K
svchost.exe                   1124 Services                   0      5,840 K
dwm.exe                       1232 Console                    1    111,224 K
svchost.exe                   1388 Services                   0      3,968 K
```

The next command shows you how to close an open task.

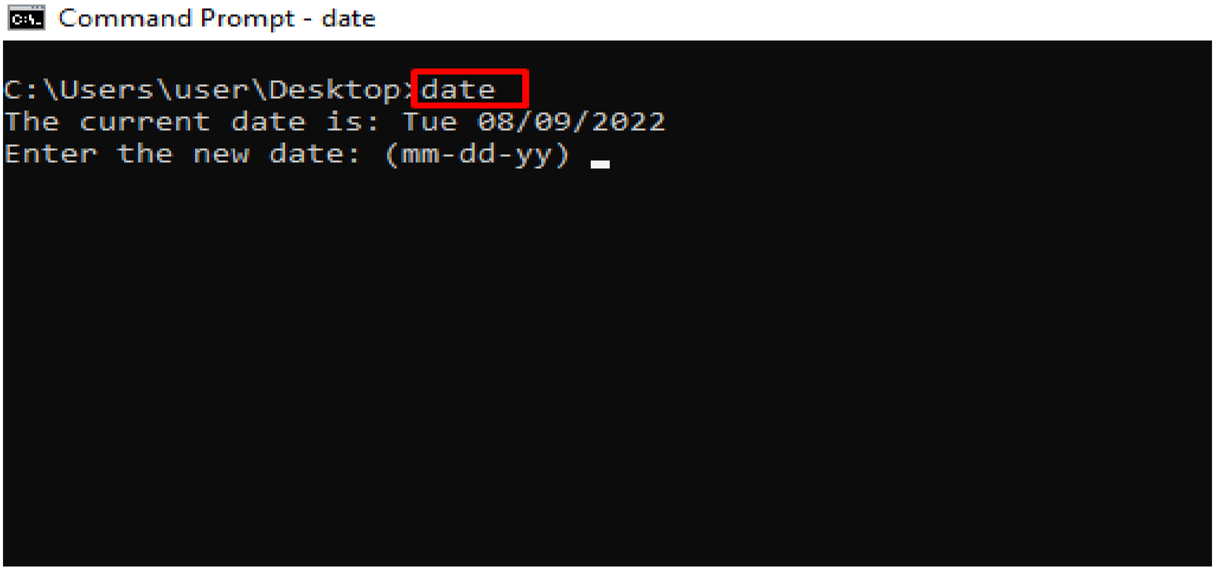
taskkill – Terminates a Running Task

To kill a task, run taskkill /IM "task.exe" /F. For example, taskkill /IM "chrome.exe" /F:



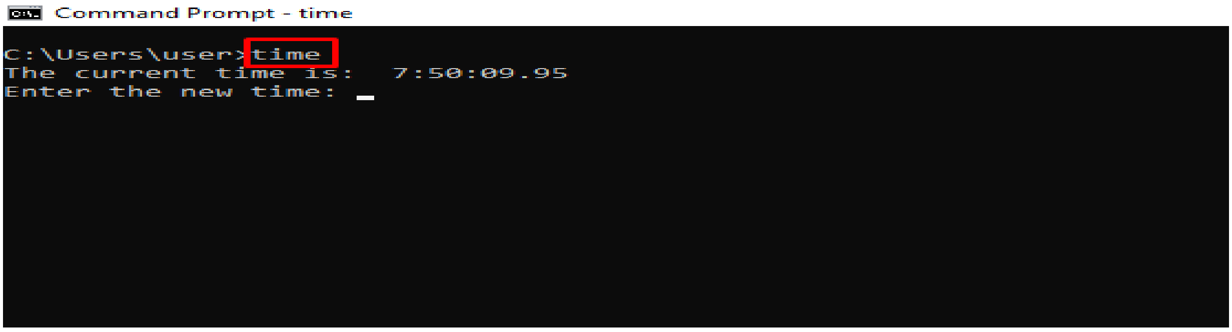
```
C:\WINDOWS\system32>taskkill /IM "chrome.exe" /F
SUCCESS: The process "chrome.exe" with PID 10748 has been terminated.
SUCCESS: The process "chrome.exe" with PID 10836 has been terminated.
SUCCESS: The process "chrome.exe" with PID 11124 has been terminated.
SUCCESS: The process "chrome.exe" with PID 11136 has been terminated.
SUCCESS: The process "chrome.exe" with PID 7568 has been terminated.
SUCCESS: The process "chrome.exe" with PID 2032 has been terminated.
SUCCESS: The process "chrome.exe" with PID 2560 has been terminated.
SUCCESS: The process "chrome.exe" with PID 8512 has been terminated.
SUCCESS: The process "chrome.exe" with PID 2388 has been terminated.
SUCCESS: The process "chrome.exe" with PID 2664 has been terminated.
SUCCESS: The process "chrome.exe" with PID 2680 has been terminated.
SUCCESS: The process "chrome.exe" with PID 3368 has been terminated.
SUCCESS: The process "chrome.exe" with PID 2732 has been terminated.
SUCCESS: The process "chrome.exe" with PID 3092 has been terminated.
SUCCESS: The process "chrome.exe" with PID 2228 has been terminated.
SUCCESS: The process "chrome.exe" with PID 9116 has been terminated.
```

date – Shows and Changes the Current Date



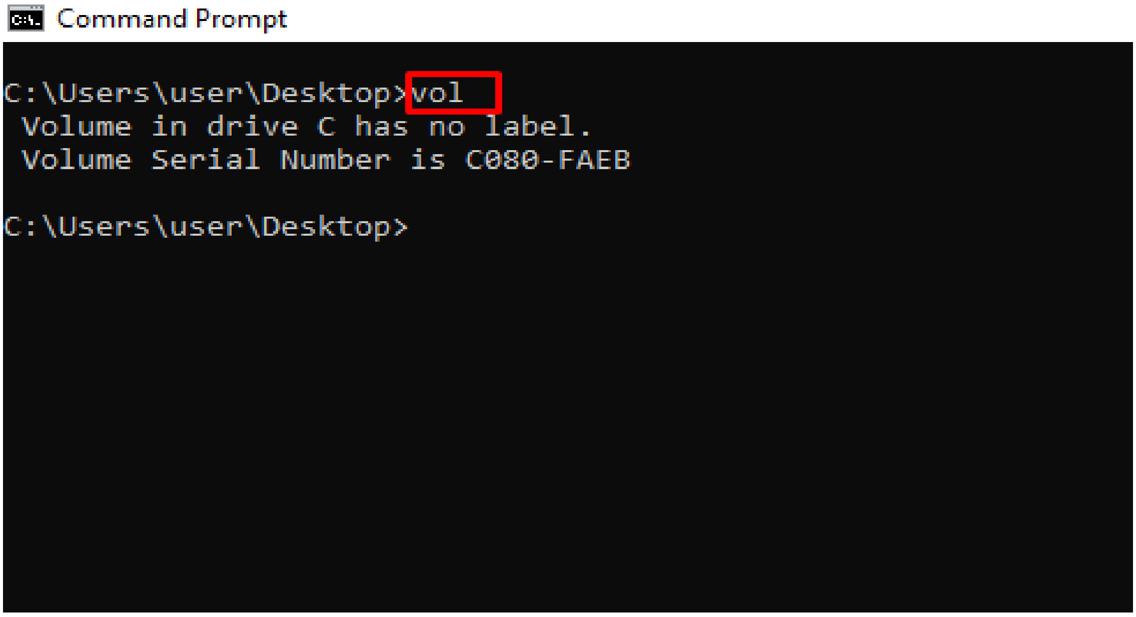
```
C:\Users\user\Desktop>date
The current date is: Tue 08/09/2022
Enter the new date: (mm-dd-yy) _
```

time – Shows and Changes the Current Time



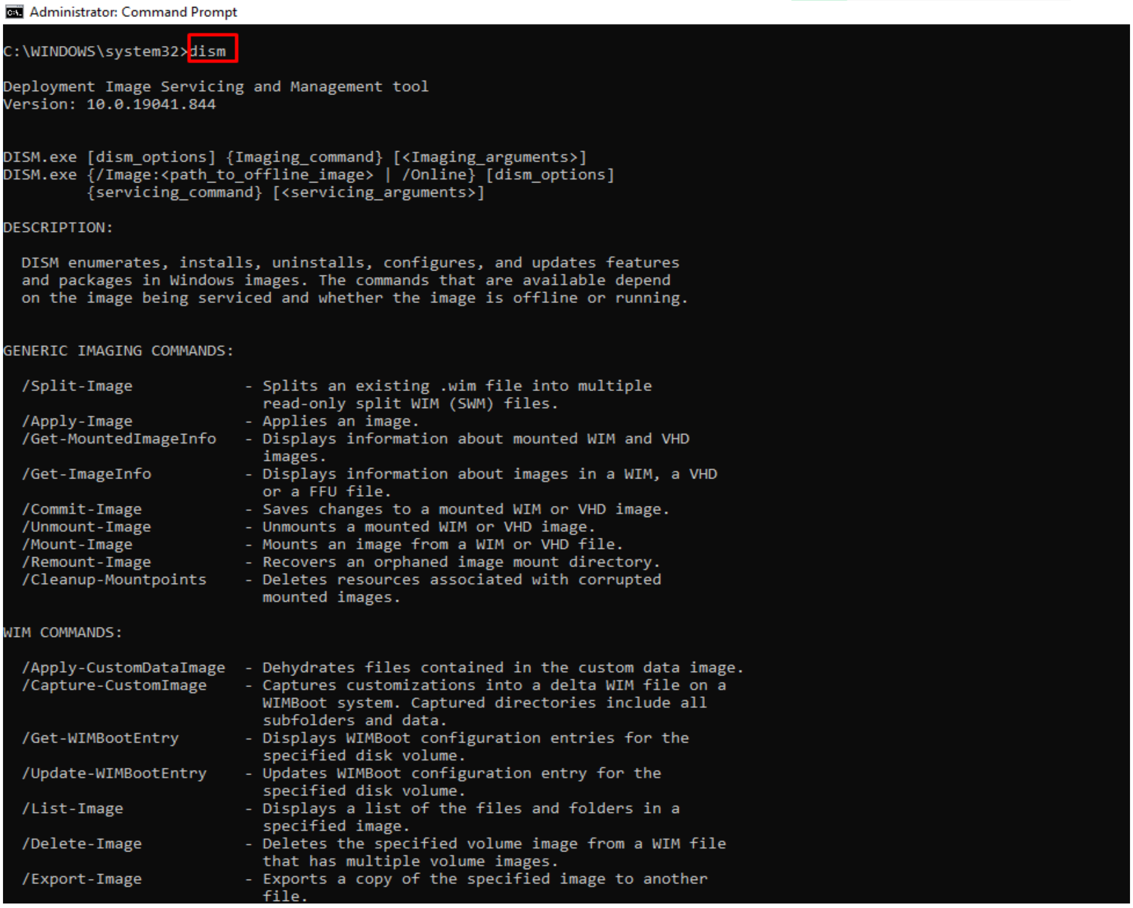
```
C:\Users\user>time
The current time is:  7:50:09.95
Enter the new time: _
```

vol – Shows the Serial Number and Label Info of the Current Drive



```
C:\Users\user\Desktop>vol
 Volume in drive C has no label.
 Volume Serial Number is C080-FAEB

C:\Users\user\Desktop>
```

dism – Runs the Deployment Image Service Management Tool

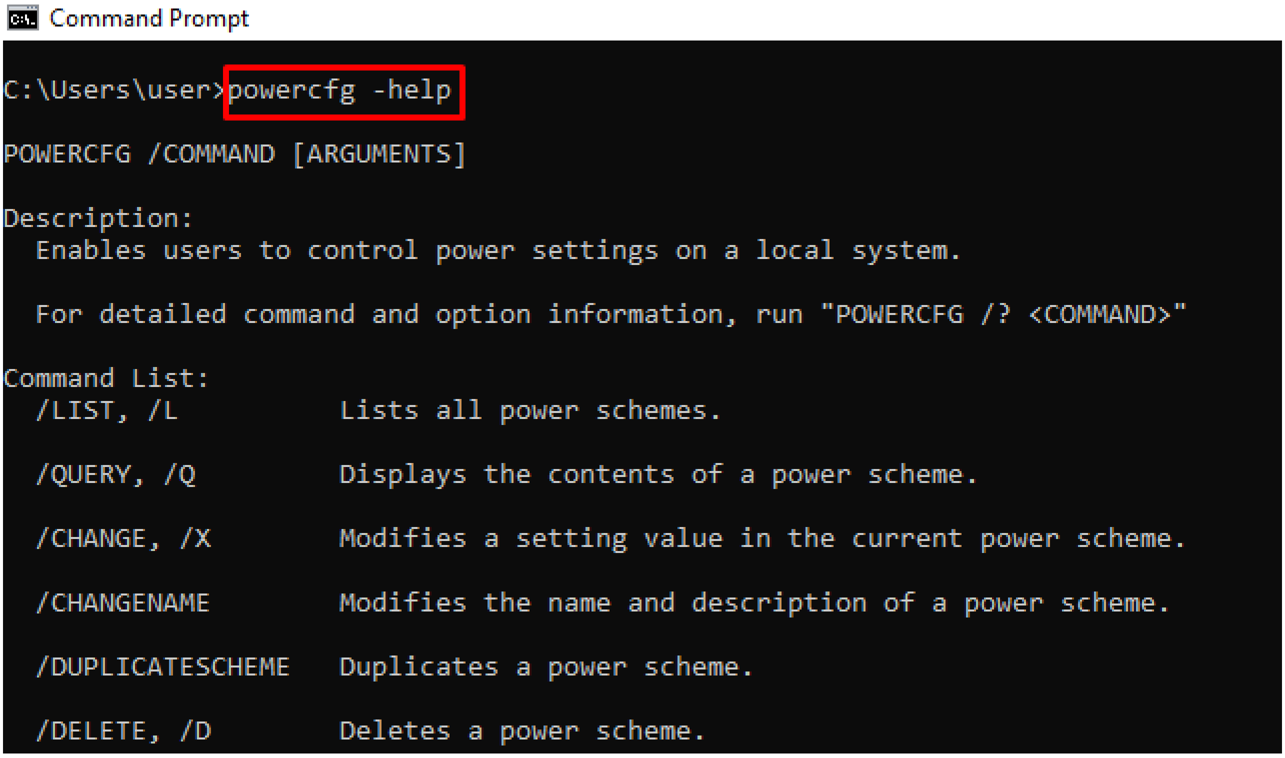


```
C:\WINDOWS\system32>dism

Deployment Image Servicing and Management tool
Version: 10.0.19041.844


DISM.exe [dism_options] {Imaging_command} [<Imaging_arguments>]
DISM.exe {/Image:<path_to_offline_image> | /Online} [dism_options]
         {servicing_command} [<servicing_arguments>]

DESCRIPTION:

  DISM enumerates, installs, uninstalls, configures, and updates features
  and packages in Windows images. The commands that are available depend
  on the image being serviced and whether the image is offline or running.


GENERIC IMAGING COMMANDS:

  /Split-Image            - Splits an existing .wim file into multiple
                            read-only split WIM (SWM) files.
  /Apply-Image            - Applies an image.
  /Get-MountedImageInfo   - Displays information about mounted WIM and VHD
                            images.
  /Get-ImageInfo          - Displays information about images in a WIM, a VHD
                            or a FFU file.
  /Commit-Image           - Saves changes to a mounted WIM or VHD image.
  /Unmount-Image          - Unmounts a mounted WIM or VHD image.
  /Mount-Image            - Mounts an image from a WIM or VHD file.
  /Remount-Image          - Recovers an orphaned image mount directory.
  /Cleanup-Mountpoints    - Deletes resources associated with corrupted
                            mounted images.

WIM COMMANDS:

  /Apply-CustomDataImage  - Dehydrates files contained in the custom data image.
  /Capture-CustomImage    - Captures customizations into a delta WIM file on a
                            WIMBoot system. Captured directories include all
                            subfolders and data.
  /Get-WIMBootEntry       - Displays WIMBoot configuration entries for the
                            specified disk volume.
  /Update-WIMBootEntry    - Updates WIMBoot configuration entry for the
                            specified disk volume.
  /List-Image             - Displays a list of the files and folders in a
                            specified image.
  /Delete-Image           - Deletes the specified volume image from a WIM file
                            that has multiple volume images.
  /Export-Image           - Exports a copy of the specified image to another
                            file.
```

CTRL + C – Stops the Execution of a Command

-help – Provides a Guide to other Commands

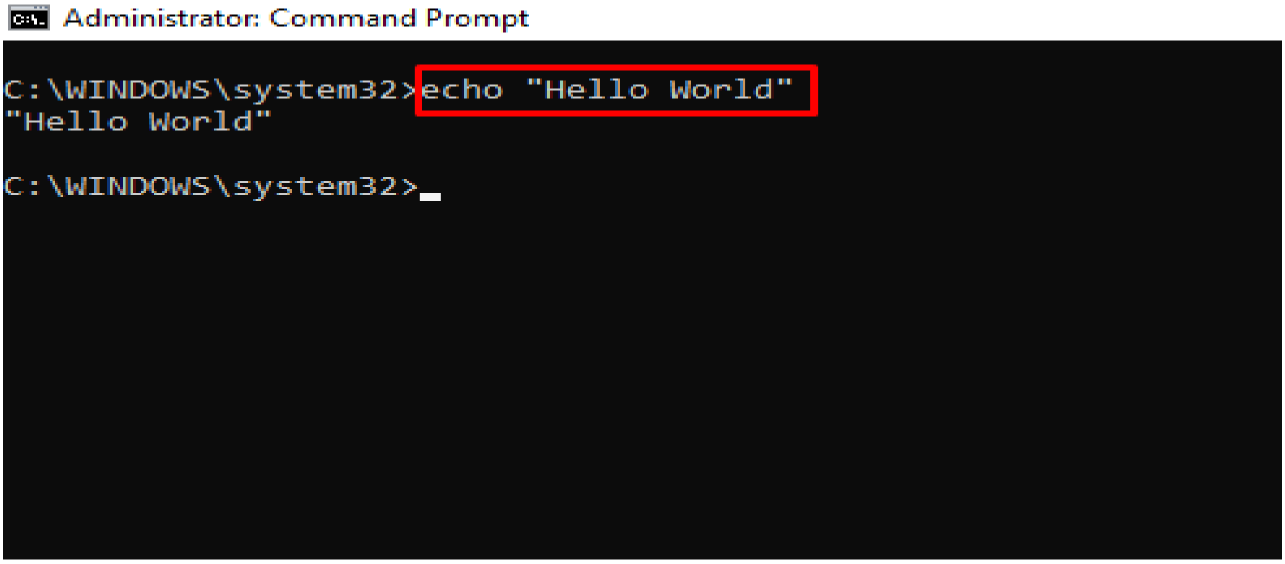
For example, powercfg -help shows how to use the powercfg command



Command Prompt

```
C:\Users\user>powercfg -help

POWERCFG /COMMAND [ARGUMENTS]

Description:
  Enables users to control power settings on a local system.

  For detailed command and option information, run "POWERCFG /? <COMMAND>"

Command List:
  /LIST, /L           Lists all power schemes.

  /QUERY, /Q          Displays the contents of a power scheme.

  /CHANGE, /X         Modifies a setting value in the current power scheme.

  /CHANGENAME         Modifies the name and description of a power scheme.

  /DUPLICATESCHEME    Duplicates a power scheme.

  /DELETE, /D         Deletes a power scheme.
```

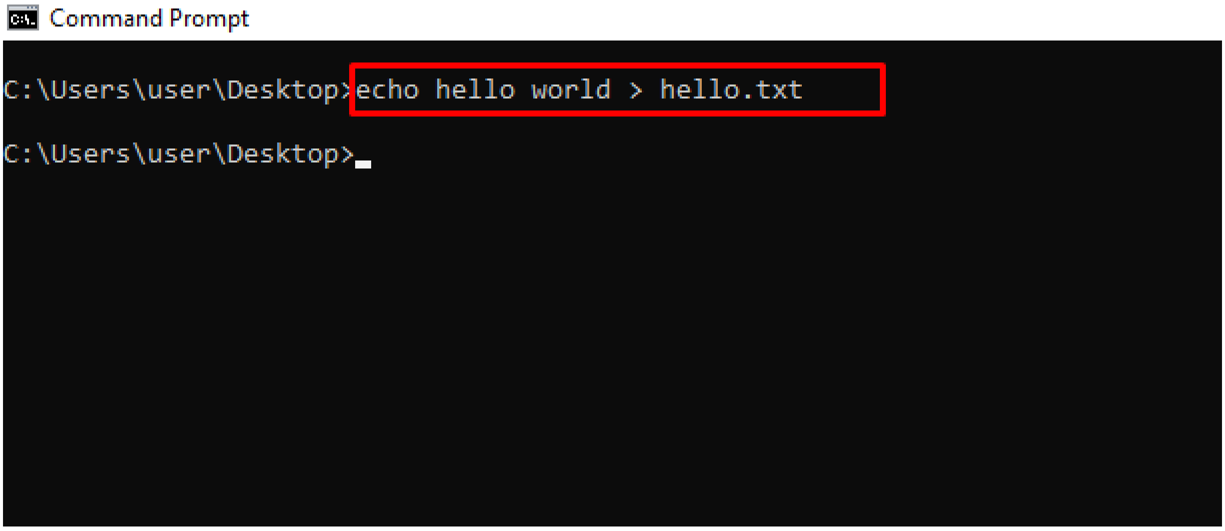
echo – Shows Custom Messages or Messages from a Script or File



Administrator: Command Prompt

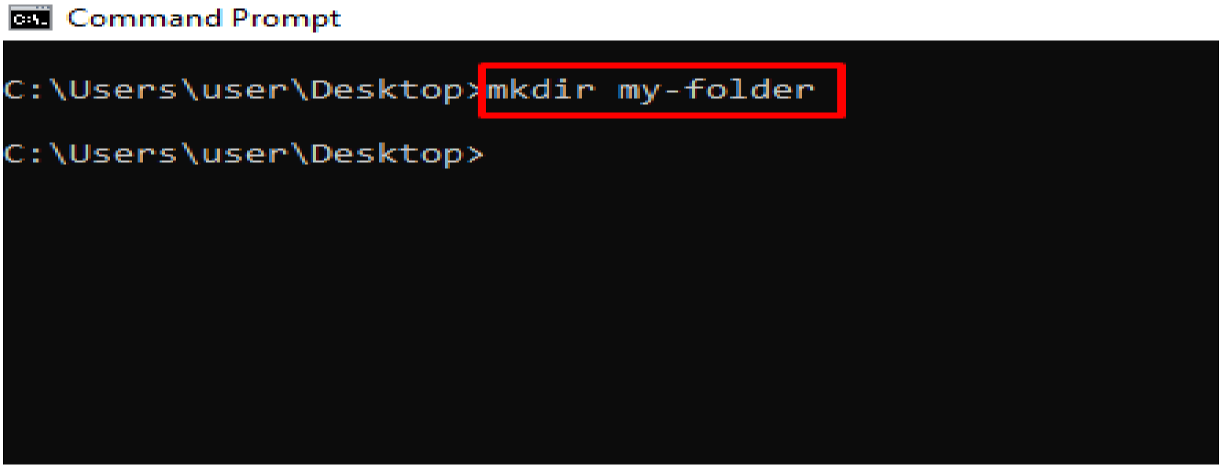
```
C:\WINDOWS\system32>echo "Hello World"
"Hello World"

C:\WINDOWS\system32>_
```

You can also use the echo command to create a file with this syntax echo file-content > filename.extension.



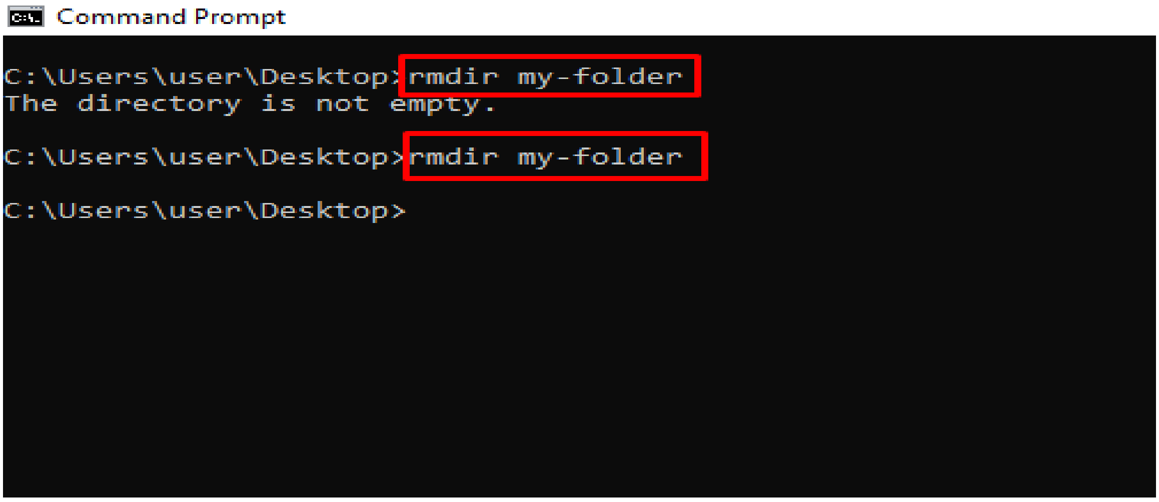
```
C:\Users\user\Desktop>echo hello world > hello.txt

C:\Users\user\Desktop>_
```

mkdir – Creates a Folder



```
C:\Users\user\Desktop>mkdir my-folder

C:\Users\user\Desktop>
```

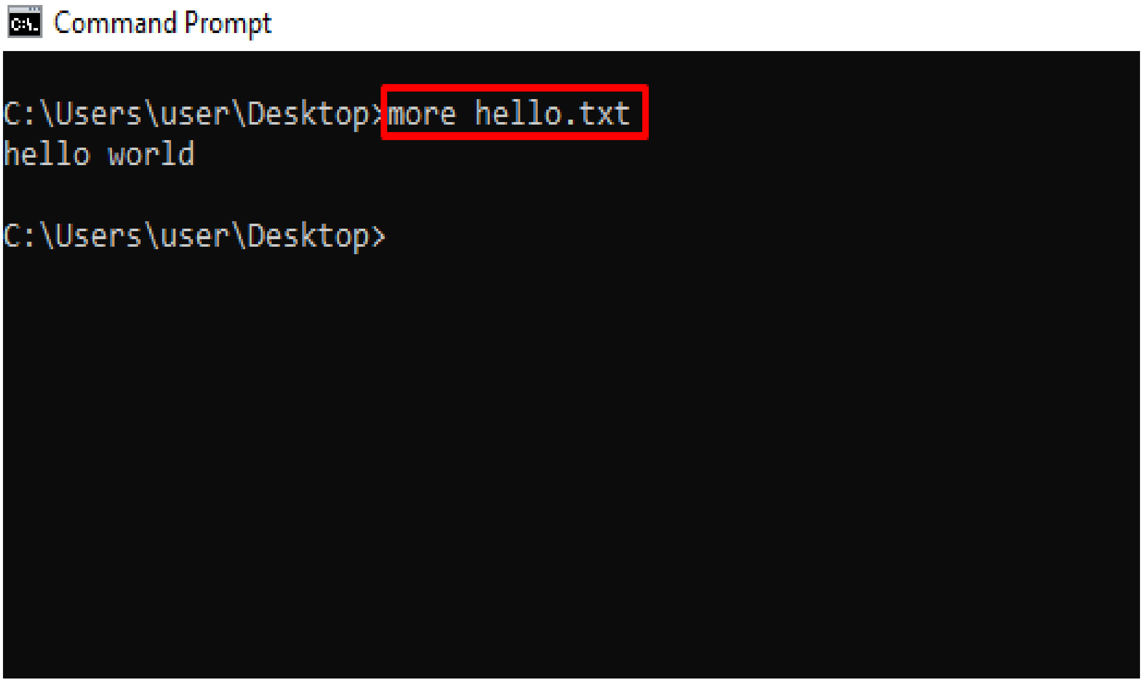
rmdir – Deletes a Folder



```
C:\Users\user\Desktop>rmdir my-folder
The directory is not empty.

C:\Users\user\Desktop>rmdir my-folder

C:\Users\user\Desktop>
```

N.B.: The folder must be empty for this command to work.

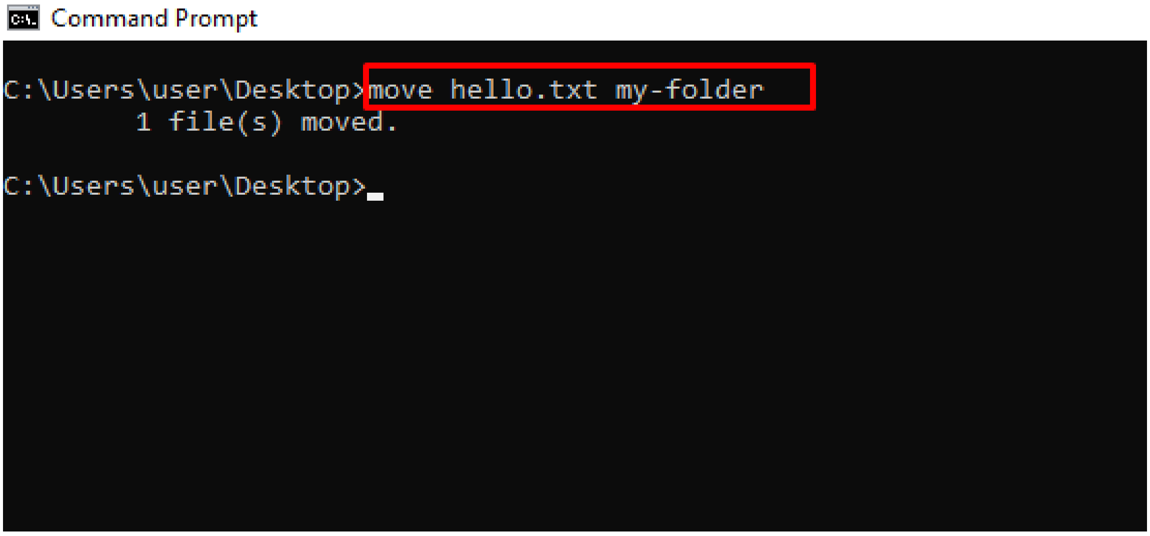
more – Shows More Information or the Content of a File



Command Prompt

```
C:\Users\user\Desktop>more hello.txt
hello world

C:\Users\user\Desktop>
```

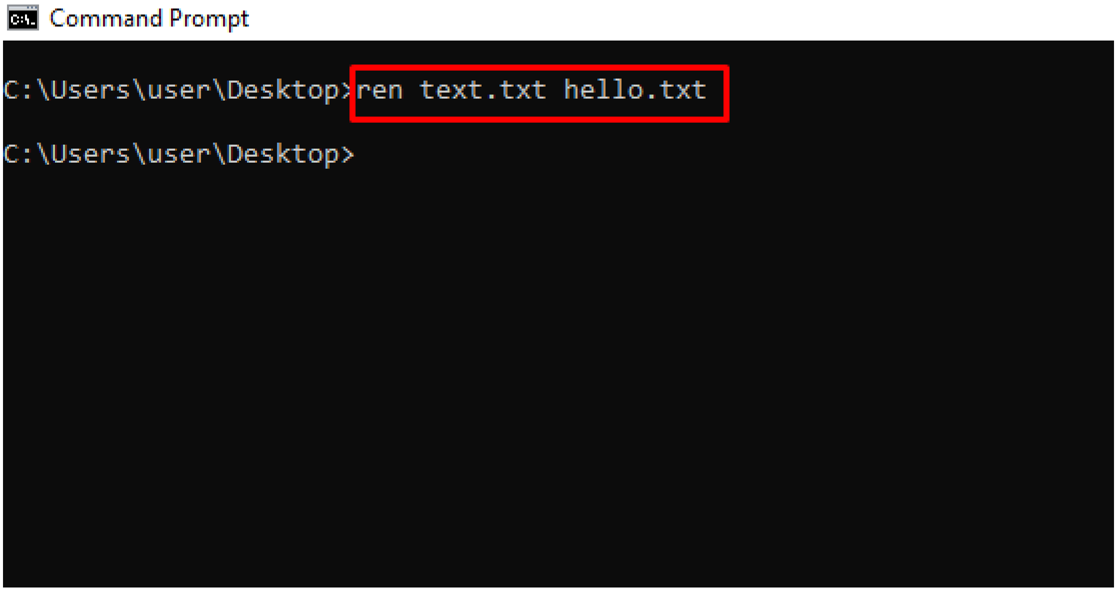
move – Moves a File or Folder to a Specified Folder



Command Prompt

```
C:\Users\user\Desktop>move hello.txt my-folder
        1 file(s) moved.

C:\Users\user\Desktop>_
```

ren – Renames a File with the Syntax ren filename.extension new-name.extension

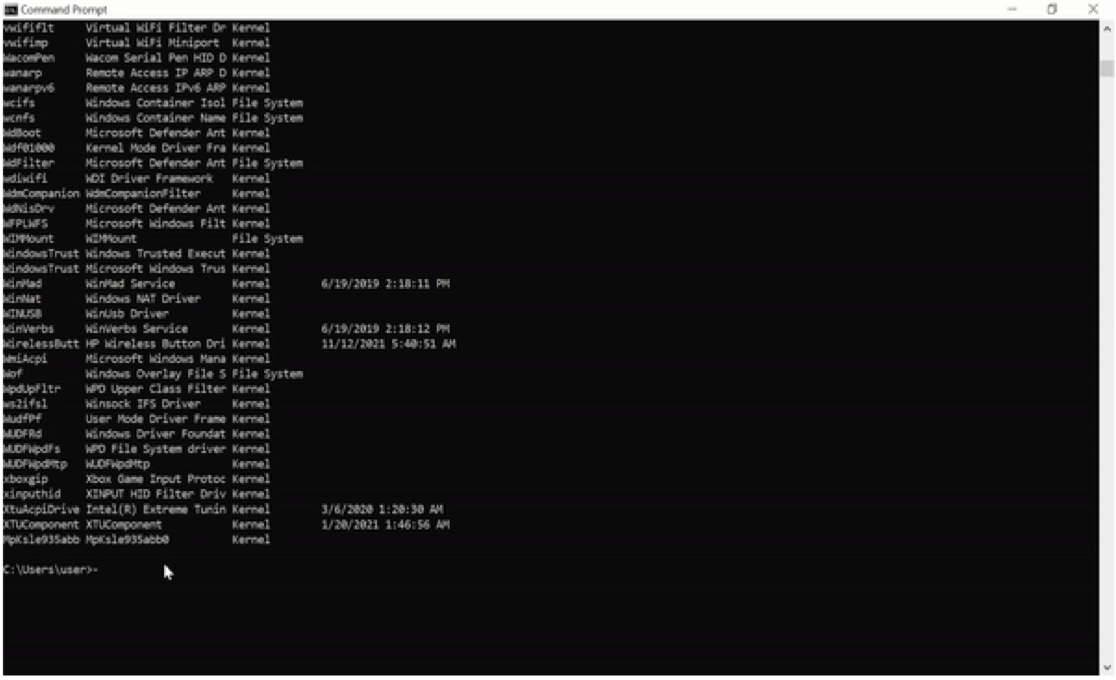


Command Prompt

```
C:\Users\user\Desktop>ren text.txt hello.txt

C:\Users\user\Desktop>
```

cls – Clears the Command Line

In case you enter several commands and the command line gets clogged up, you can use cls to clear all entries and their outputs.



Command Prompt

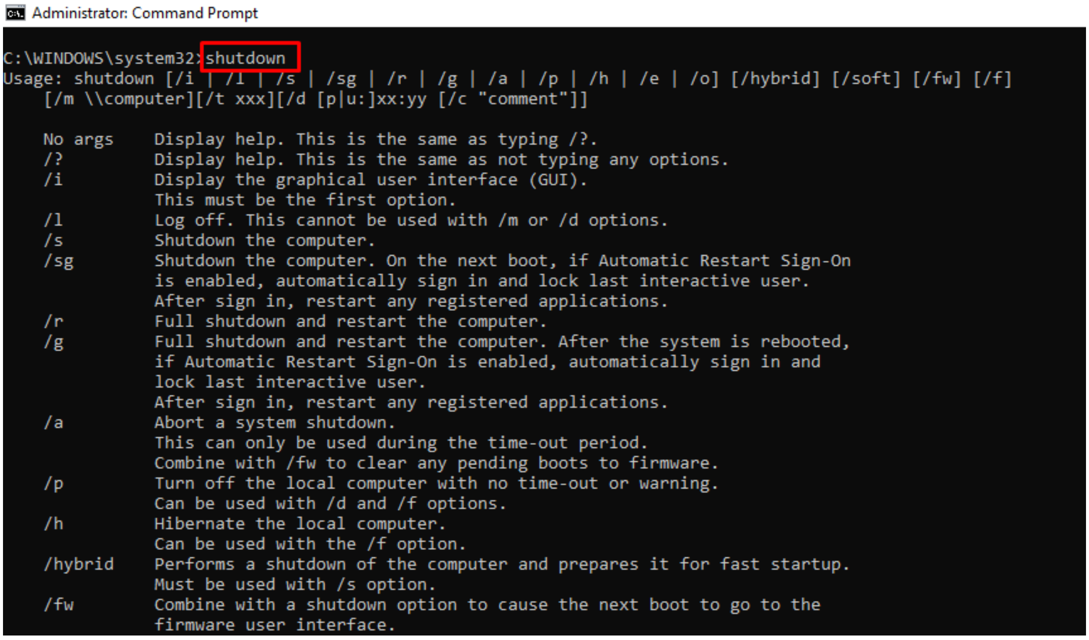
```
vwififlt     Virtual WiFi Filter Dr Kernel
vwifimp      Virtual WiFi Miniport  Kernel
WacomPen     Wacom Serial Pen HID D Kernel
wanarp       Remote Access IP ARP D Kernel
wanarpv6     Remote Access IPv6 ARP Kernel
wcifs        Windows Container Isol File System
wcnfs        Windows Container Name File System
WdBoot       Microsoft Defender Ant Kernel
Wdf01000     Kernel Mode Driver Fra Kernel
WdFilter     Microsoft Defender Ant File System
wdiwifi      WDI Driver Framework   Kernel
WdmCompanion WdmCompanionFilter     Kernel
WdNisDrv     Microsoft Defender Ant Kernel
WFPLWFS      Microsoft Windows Filt Kernel
WIMMount     WIMMount               File System
WindowsTrust Windows Trusted Execut Kernel
WindowsTrust Microsoft Windows Trus Kernel
WinMad       WinMad Service         Kernel         6/19/2019 2:18:11 PM
WinNat       Windows NAT Driver     Kernel
WINUSB       WinUsb Driver          Kernel
WinVerbs     WinVerbs Service       Kernel         6/19/2019 2:18:12 PM
WirelessButt HP Wireless Button Dri Kernel         11/12/2021 5:40:51 AM
WmiAcpi      Microsoft Windows Mana Kernel
Wof          Windows Overlay File S File System
WpdUpFltr    WPD Upper Class Filter Kernel
ws2ifsl      Winsock IFS Driver     Kernel
WudfPf       User Mode Driver Frame Kernel
WUDFRd       Windows Driver Foundat Kernel
WUDFWpdFs    WPD File System driver Kernel
WUDFWpdMtp   WUDFWpdMtp             Kernel
xboxgip      Xbox Game Input Protoc Kernel
xinputhid    XINPUT HID Filter Driv Kernel
XtuAcpiDrive Intel(R) Extreme Tunin Kernel         3/6/2020 1:20:30 AM
XTUComponent XTUComponent           Kernel         1/20/2021 1:46:56 AM
MpKsle935abb MpKsle935abb0          Kernel

C:\Users\user>-
```

exit – Closes the Command Line

shutdown – Shuts down, Restarts, Hibernates, Sleeps the Computer

You can shut down, restart, hibernate, and sleep your PC from the command line.

Enter shutdown in the command line so you can see the extensions you can use to perform the actions. For example, shutdown /r will restart your computer.



Administrator: Command Prompt

```
C:\WINDOWS\system32>shutdown
Usage: shutdown [/i | /l | /s | /sg | /r | /g | /a | /p | /h | /e | /o] [/hybrid] [/soft] [/fw] [/f]
    [/m \\computer][/t xxx][/d [p|u:]xx:yy [/c "comment"]]

    No args    Display help. This is the same as typing /?.
    /?         Display help. This is the same as not typing any options.
    /i         Display the graphical user interface (GUI).
               This must be the first option.
    /l         Log off. This cannot be used with /m or /d options.
    /s         Shutdown the computer.
    /sg        Shutdown the computer. On the next boot, if Automatic Restart Sign-On
               is enabled, automatically sign in and lock last interactive user.
               After sign in, restart any registered applications.
    /r         Full shutdown and restart the computer.
    /g         Full shutdown and restart the computer. After the system is rebooted,
               if Automatic Restart Sign-On is enabled, automatically sign in and
               lock last interactive user.
               After sign in, restart any registered applications.
    /a         Abort a system shutdown.
               This can only be used during the time-out period.
               Combine with /fw to clear any pending boots to firmware.
    /p         Turn off the local computer with no time-out or warning.
               Can be used with /d and /f options.
    /h         Hibernate the local computer.
               Can be used with the /f option.
    /hybrid    Performs a shutdown of the computer and prepares it for fast startup.
               Must be used with /s option.
    /fw        Combine with a shutdown option to cause the next boot to go to the
               firmware user interface.
```

Basic CMD Commands

Here are some basic CMD (Command Prompt) commands for Windows that can be useful in ethical hacking or penetration testing:

1. **ipconfig**: This command displays information about the current TCP/IP network configuration, including IP addresses, subnet masks, and default gateways.

   Example: `ipconfig /all` (displays detailed network configuration information)

2. **netstat**: This command displays active TCP connections, ports on which the computer is listening, and various network statistics.

   Example: `netstat -an` (shows all active connections and listening ports)

3. **nslookup**: This command is used to query DNS (Domain Name System) servers for information about domain names, IP addresses, and other DNS records.

   Example: `nslookup example.com` (queries DNS information for a specific domain)

4. **tracert**: This command traces the path that packets take from your system to a remote host, displaying all the intermediate routers/gateways along the way.

Example: `tracert example.com` (traces the route to a specific host)

5. **net**: This command is used to manage user accounts, groups, and network resources in Windows.

Example: `net user` (displays information about user accounts)

6. **whoami**: This command displays information about the current user, including the user's name, security identifiers (SIDs), and other details.

Example: `whoami /all` (displays detailed information about the current user)

7. **netsh**: This command-line utility is used to configure and monitor various network components, such as firewalls, interfaces, and routing tables.

Example: `netsh firewall show state` (shows the status of the Windows Firewall)

8. **arp**: This command is used to view and modify the Address Resolution Protocol (ARP) cache, which maps IP addresses to physical (MAC) addresses.

Example: `arp -a` (displays the ARP cache)

9. **tasklist**: This command displays a list of currently running processes on the system.

Example: `tasklist` (lists all running processes)

10. **reg**: This command is used to access and modify the Windows registry, which stores configuration settings for various system components and applications.

Example: `reg query HKEY_LOCAL_MACHINE\SOFTWARE` (queries the specified registry key)

Advanced CMD Commands

1. **net use**: This command is used to connect to a shared resource, such as a network drive or printer.
Example: `net use \\192.168.1.100\share /user:domain\username password`

2. **net view**: This command displays a list of available network resources and shares.
Example: `net view \\192.168.1.100`

3. **net share**: This command is used to create, manage, or delete shared resources on the local system.
Example: `net share share_name=C:\path /GRANT:domain\username,READ`

4. **runas**: This command is used to run a program or command with different credentials or

privileges.
Example: `runas /user:domain\username cmd.exe`

5. **sc**: This command is used to manage services and display information about their status.
Example: `sc query service_name`

6. **wmic**: This command-line tool is used to retrieve and modify system information through the Windows Management Instrumentation (WMI) interface.
Example: `wmic product get name, version`

7. **reg export/import**: These commands are used to export and import registry keys or values to and from a file.
Example: `reg export HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run backup.reg`

8. **schtasks**: This command is used to schedule commands or programs to run at a specific time or after a specific event.
Example: `schtasks /create /tn "TaskName" /tr "command.exe" /sc daily /st 00:00`

9. **netsh**: This command-line utility is used to configure various network components, including interfaces, routing tables, and firewalls.
Example: `netsh advfirewall firewall add rule name="Rule Name" dir=in action=allow protocol=TCP localport=80`

10. **powershell**: This command launches the PowerShell environment, which provides advanced scripting and automation capabilities.
Example: `powershell -c "Get-Process"`

Basic Linux Commands

Here are some basic Linux commands that are commonly used:

1. **ls**: This command is used to list files and directories in the current working directory.
Example: `ls` (lists files and directories)
Example: `ls -l` (lists files and directories with detailed information)
Example: `ls -a` (lists all files and directories, including hidden ones)

2. **cd**: This command is used to change the current working directory.
Example: `cd /path/to/directory` (changes the current directory to the specified path)
Example: `cd ..` (moves up one directory level)

3. **pwd**: This command displays the current working directory's full path.
Example: `pwd`

4. **mkdir**: This command is used to create a new directory.
Example: `mkdir directory_name`

5. **rm**: This command is used to remove (delete) files or directories.
Example: `rm file_name` (removes a file)
Example: `rm -r directory_name` (removes a directory and its contents recursively)

6. **cp**: This command is used to copy files or directories.
Example: `cp source_file destination_file` (copies a file)
Example: `cp -r source_directory destination_directory` (copies a directory and its contents recursively)

7. **mv**: This command is used to move or rename files or directories.
Example: `mv source_file destination_file` (moves a file)
Example: `mv source_directory destination_directory` (moves a directory)
Example: `mv file_name new_file_name` (renames a file)

8. **cat**: This command is used to display the contents of a file.
Example: `cat file_name`

9. **grep**: This command is used to search for patterns or text within files.
Example: `grep "pattern" file_name` (searches for the specified pattern in the file)

10. **sudo**: This command is used to execute a command with superuser (root) privileges.
Example: `sudo command` (runs the specified command with root privileges)

11. **man**: This command displays the manual page (documentation) for a given command.
Example: `man command_name` (shows the manual page for the specified command)

12. **apt** (or **apt-get**, **yum**, **dnf**): These commands are used to install, update, or remove packages (software) on different Linux distributions.
Example: `sudo apt update` (updates the package lists on Debian/Ubuntu-based systems)
Example: `sudo yum install package_name` (installs a package on RHEL/CentOS-based systems)

Networking Commands used for Ethical Hacking

- **Ipconfig:** This is your go-to command to view your IP address, subnet mask, default gateway, and DNS server information. You can also use ipconfig /all for more detailed information and ipconfig /renew (or /release) to renew or release your IP lease.
- **Ping:** The ping command is fundamental for checking connectivity to another device on a network or the internet. It sends test packets to the specified IP address or hostname and reports on the response time.
- **Nslookup:** This command helps with troubleshooting DNS (Domain Name System) resolution issues. You can use it to query DNS servers and see how they translate hostnames into IP addresses.
- **Tracert:** Ever wondered what route your data packets take to reach a website? Tracert visualizes the path (hops) taken by packets to reach a destination, aiding in diagnosing network latency and routing problems.

Advanced Configuration Commands:

- **Netstat:** While ipconfig shows network configuration, netstat offers a deeper look into active connections on your system. It can display details like listening and established connections, ports used, and foreign IP addresses. Use flags like -a (all connections), -b (program using the connection), or -f (fully qualified domain names) for more granular information.
- **ARP (Address Resolution Protocol):** ARP displays the Address Resolution Protocol cache, which maps MAC addresses (physical addresses) to IP addresses on your local network.
- **Route:** This command deals with routing tables, which dictate how your device forwards data packets. You can use route print to see the current routing table and potentially use route add or route delete for advanced configuration (use with caution!).