Itech Guides

40 POWERSHELL & CMD COMMANDS FOR ADMINISTRATORS

BY VICTOR ASHIEDU

40 Most Useful PowerShell and Command Prompt Commands for Windows Administrators

By Victor ASHIEDU

Sign up to my PowerShell mailing list.
To receive PowerShell Freebies from Itechguides.com, click this link:

Itechguides.com/powershell-list-amazon/

To get the best of this FREE PowerShell & CMD eBook, use the Table of Contents
(See next page).

Table of Contents

Introduction

This free eBook lists and explains the 40 most useful PowerShell commands and Command Prompt commands. Each command comes with examples.

The book is divided into 2 chapters. Chapter 1 covers the 20 most useful PowerShell commands. Chapter 2 covers the 20 most useful Command Prompt commands.

“40 Most Useful PowerShell and Command Prompt Commands for Windows Administrators” is for administrators that want to learn the skills to automate Windows tasks with PowerShell or Command Prompt commands.

Chapter 1: 20 Most Useful PowerShell Commands

This guide teaches you how to use the 20 most useful PowerShell commands for Systems Administrators.

In this guide, I will share commands required to perform common tasks in Windows. Most Windows administrators will find this tutorial both useful and handy.

1.0 PowerShell Commands to Find and Get Help with Cmdlets

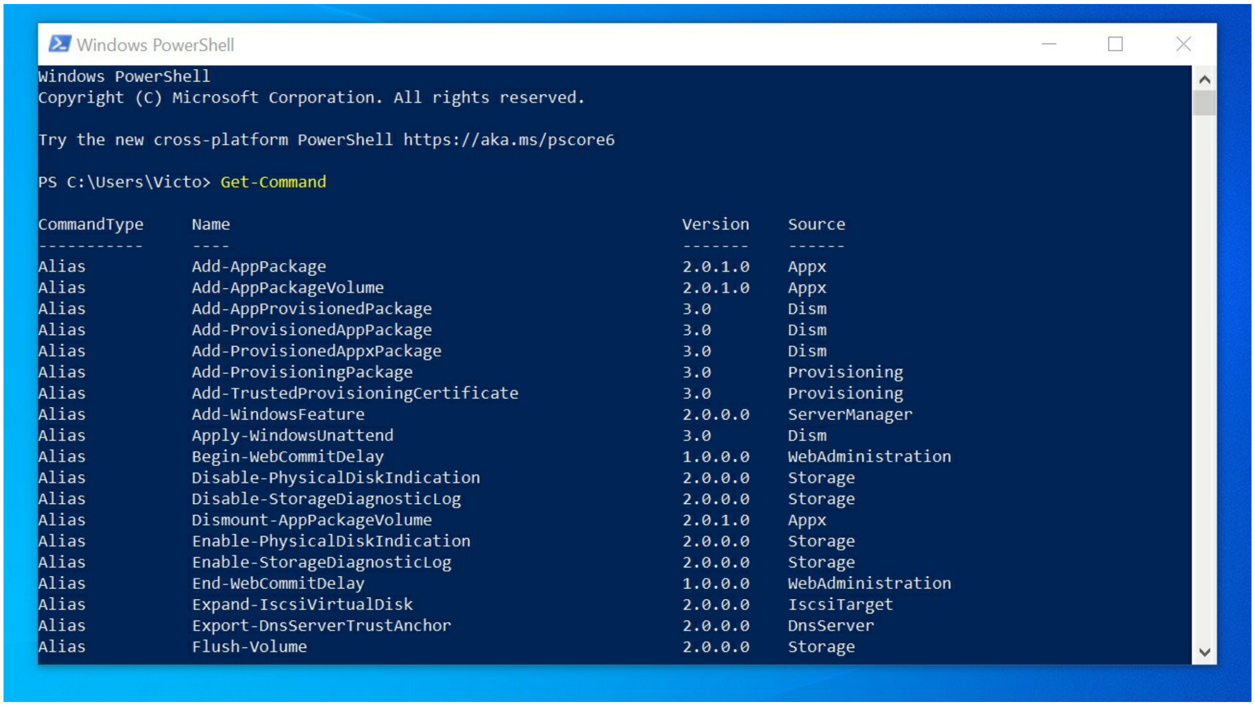
You cannot talk about the most useful PowerShell commands without learning how to find them. Below are the PowerShell commands that will help you find Cmdlets (Command Lets).

Get-Command

The Get-Command Cmdlet is the first and most important command a PowerShell newbie should learn and know how to use. Why? It helps you find other PowerShell Cmdlets. What command can be more important than a command that can do this?

To find all PS Commands in your computer, simply execute this command below:

```
Get-Command
```



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

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

PS C:\Users\Victo> Get-Command

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Alias           Add-AppPackage                                     2.0.1.0    Appx
Alias           Add-AppPackageVolume                               2.0.1.0    Appx
Alias           Add-AppProvisionedPackage                          3.0        Dism
Alias           Add-ProvisionedAppPackage                          3.0        Dism
Alias           Add-ProvisionedAppxPackage                         3.0        Dism
Alias           Add-ProvisioningPackage                            3.0        Provisioning
Alias           Add-TrustedProvisioningCertificate                 3.0        Provisioning
Alias           Add-WindowsFeature                                 2.0.0.0    ServerManager
Alias           Apply-WindowsUnattend                              3.0        Dism
Alias           Begin-WebCommitDelay                               1.0.0.0    WebAdministration
Alias           Disable-PhysicalDiskIndication                     2.0.0.0    Storage
Alias           Disable-StorageDiagnosticLog                       2.0.0.0    Storage
Alias           Dismount-AppPackageVolume                          2.0.1.0    Appx
Alias           Enable-PhysicalDiskIndication                      2.0.0.0    Storage
Alias           Enable-StorageDiagnosticLog                        2.0.0.0    Storage
Alias           End-WebCommitDelay                                 1.0.0.0    WebAdministration
Alias           Expand-IscsiVirtualDisk                            2.0.0.0    IscsiTarget
Alias           Export-DnsServerTrustAnchor                        2.0.0.0    DnsServer
Alias           Flush-Volume                                       2.0.0.0    Storage
```

Understanding the Results of the Get-Command Cmdlet

There are four columns in the results of the Get-Command Output

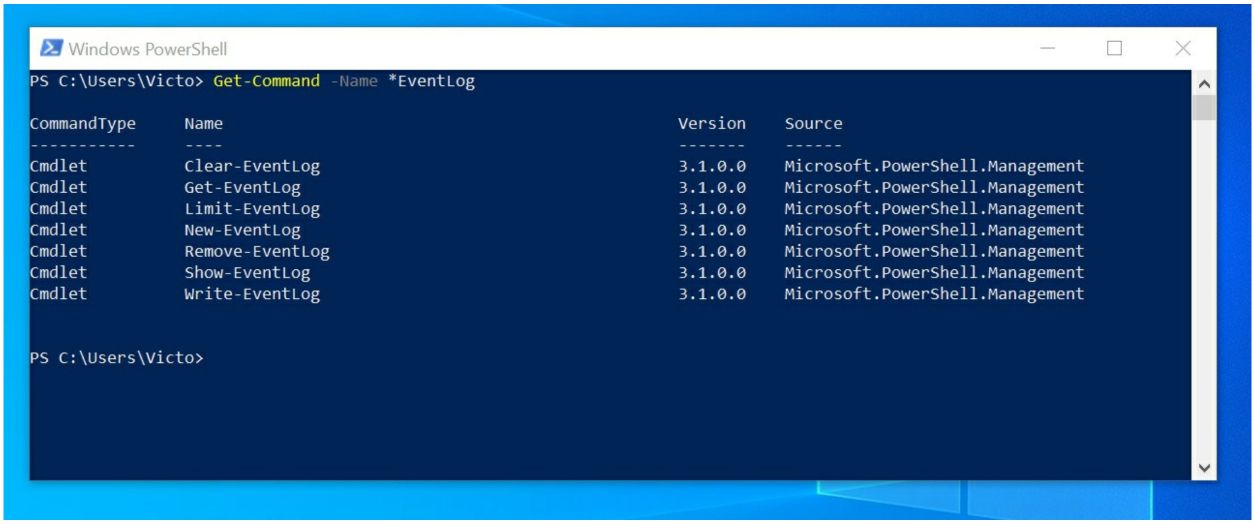
1. *CommandType*: This tells you whether a command is an Alias, a Cmdlet, or a Function.
2. *Name*: The name is the actual command you execute.
3. *Version*: This is the PowerShell version
4. *Source*: The module of the PS command.

With this information, you can filter the results from Get-Command. Say you want to see PowerShell commands containing the word "EventLog", running the command below will get the job done:

```
Get-Command -Name *EventLog
```

Notice where I added the asterisks. This is because I am aware that "EventLog" is the "Noun" part of the Cmdlets. However, if you don't even know you could try adding the asterisks at the beginning then try the end.

Below is the result of the previous command.



```
PS C:\Users\Victo> Get-Command -Name *EventLog

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Cmdlet          Clear-EventLog                                     3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Get-EventLog                                       3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Limit-EventLog                                     3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          New-EventLog                                       3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Remove-EventLog                                    3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Show-EventLog                                      3.1.0.0    Microsoft.PowerShell.Management
Cmdlet          Write-EventLog                                     3.1.0.0    Microsoft.PowerShell.Management


PS C:\Users\Victo>
```

Get-Command Parameters

Lastly, before we move on, let’s discuss the parameters of the Get-Command Cmdlet.

To get all the parameters and information about the Get-Command command, execute this command below:

```
Get-Help Get-Command -Full
```

This will give you all the information regarding the Get-Command Cmdlet. I will discuss the Get-Help Cmdlet next.

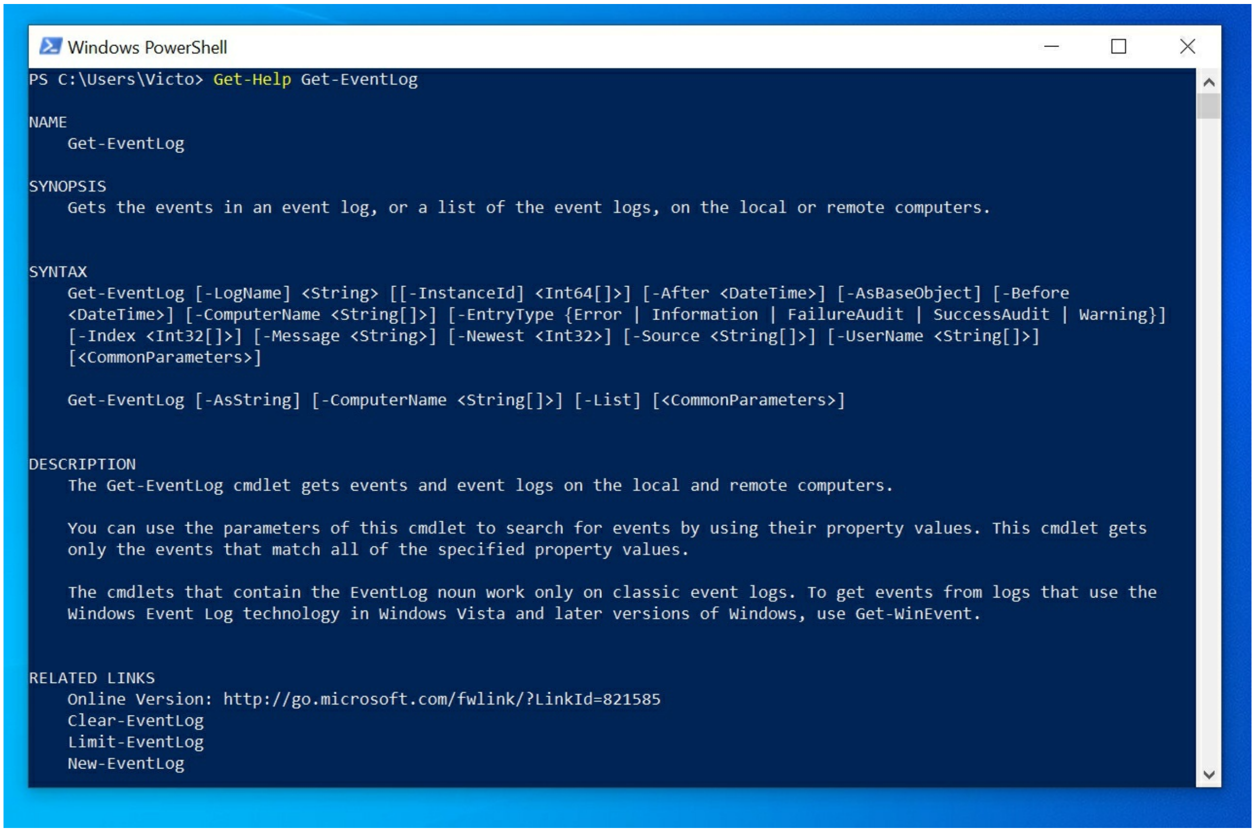
Get-Help

While the Get-Command Cmdlet finds the Cmdlets, the Get-Help PowerShell command gives you the information you need to use the command.

The easiest way to use the Get-Help Cmdlet is to enter Get-Help followed by the command you want information on. To find more information about the Get-EventLog Cmdlet, run the command below:

```
Get-Help Get-EventLog
```

This will give you the basic information about Get-EventLog PowerShell Command. See the result below:



```
PS C:\Users\Victo> Get-Help Get-EventLog

NAME
    Get-EventLog

SYNOPSIS
    Gets the events in an event log, or a list of the event logs, on the local or remote computers.


SYNTAX
    Get-EventLog [-LogName] <String> [[-InstanceId] <Int64[]>] [-After <DateTime>] [-AsBaseObject] [-Before
    <DateTime>] [-ComputerName <String[]>] [-EntryType {Error | Information | FailureAudit | SuccessAudit | Warning}]
    [-Index <Int32[]>] [-Message <String>] [-Newest <Int32>] [-Source <String[]>] [-UserName <String[]>]
    [<CommonParameters>]

    Get-EventLog [-AsString] [-ComputerName <String[]>] [-List] [<CommonParameters>]


DESCRIPTION
    The Get-EventLog cmdlet gets events and event logs on the local and remote computers.

    You can use the parameters of this cmdlet to search for events by using their property values. This cmdlet gets
    only the events that match all of the specified property values.

    The cmdlets that contain the EventLog noun work only on classic event logs. To get events from logs that use the
    Windows Event Log technology in Windows Vista and later versions of Windows, use Get-WinEvent.


RELATED LINKS
    Online Version: http://go.microsoft.com/fwlink/?LinkId=821585
    Clear-EventLog
    Limit-EventLog
    New-EventLog
```

Some Important Parameters of the Get-Help Command

Like any other PowerShell Cmdlet, the Get-Help Cmdlet has several parameters. Below are the most important parameters you will need.

1. -*Detailed*: The *Detailed* parameter gives you the command SYNTAX, PARAMETERS, ALIASES, and REMARKS.
2. -*Full*: The Full gives similar information provided by the *Detailed* parameter with more information about each parameter
3. -*Examples*: Gives examples of how to use the Cmdlet. This can be very useful if you have never used the Cmdlet before.
4. -*Online*: Opens the online help page of the Cmdlet.

To see the parameters of a PS Cmdlet, type the Cmdlet in PS, hit the space key, type hyphen "-" followed by the tab key. As you press the tab key you will scroll through available parameters.

1.1 PowerShell Commands to Manage Files and

Folders

Now that you know how to find PowerShell commands, let's get you in the hood. The next set of the most useful PowerShell commands are Cmdlets to help you manage files and folders.

Get-ChildItem

Gets items in a specified location. To list the folders in my drive C, I will run the command below:

```
Get-ChildItem c:/
```

This will list all the top-level folders. To list all files, folders include sub-folders use the -*Recurse* parameter.

Tip

You can combine the Get-ChildItem Cmdlet let with other Cmdlet to calculate the size of each folder in a specified directory.

Copy-Item and Move-Item

You could use the Get-ChildItem Cmdlet to list items in a folder, then pipe the result to Copy-Item Cmdlet to copy the items to a new location. The command below will do the job:

```
Get-ChildItem C:\Dropbox | Copy-Item -Destination C:\NewFolder
```

The above PowerShell command will only copy the top-level folders and files - it will NOT copy sub-folders and files. To copy all files and folders including sub-folders, include the -*Recurse* parameter in the Get-ChildItem command as shown below:

```
Get-ChildItem C:\Dropbox -Recurse | Copy-Item -Destination C:\NewFolder
```

While the Copy-Item Cmdlet copies items from one location to another the Move-Item Cmdlet moves the item.

Remove-Item

This Cmdlet deletes specified items. Like the Copy-Item and Move-Item Cmdlets, you could pipe the output of Get-ChildItem to Remove-Item.

Use the Remove-Item Cmdlet with caution as it can delete all files and folders in your computer including Windows files!

Tip

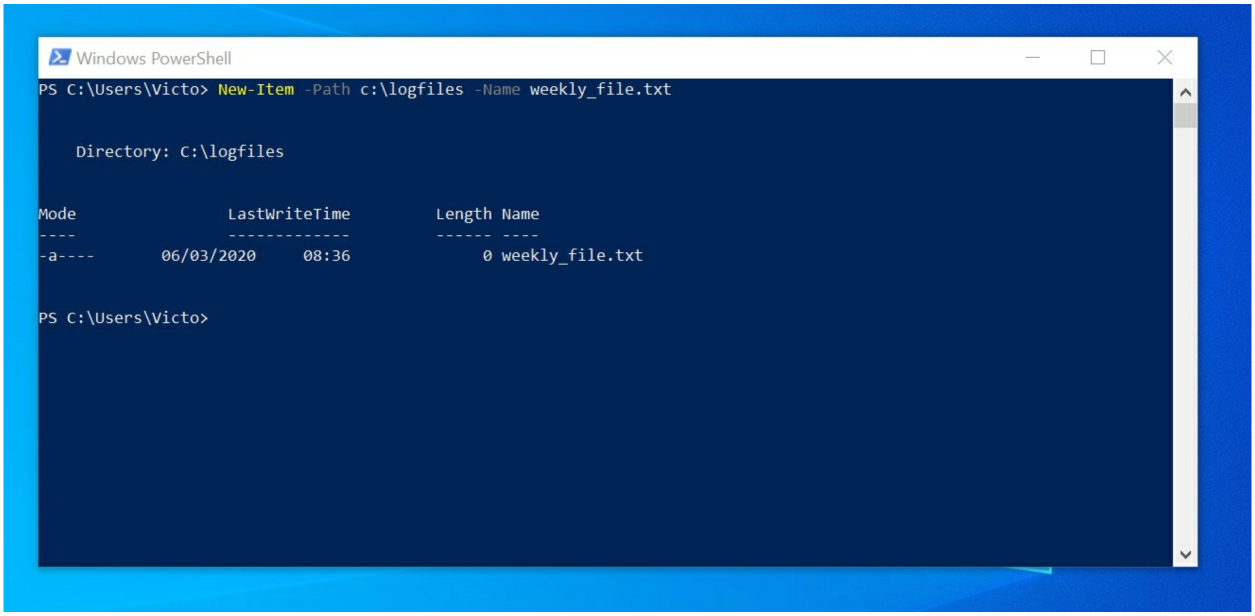
By piping the output of Get-ChildItem to Remove-Item, you could create a simple script that will delete some log files on regular bases. You could schedule the PS script to run at a specified time using Windows Scheduler.

New-Item

This Cmdlet creates a new item in Windows. New-Item can be used to create files, folders and registry keys and entries. The command below creates a text file called weekly_file.txt in c:\logfiles folder:

New-Item -Path c:\logfiles -Name weekly_file.txt

Here is the command in PowerShell



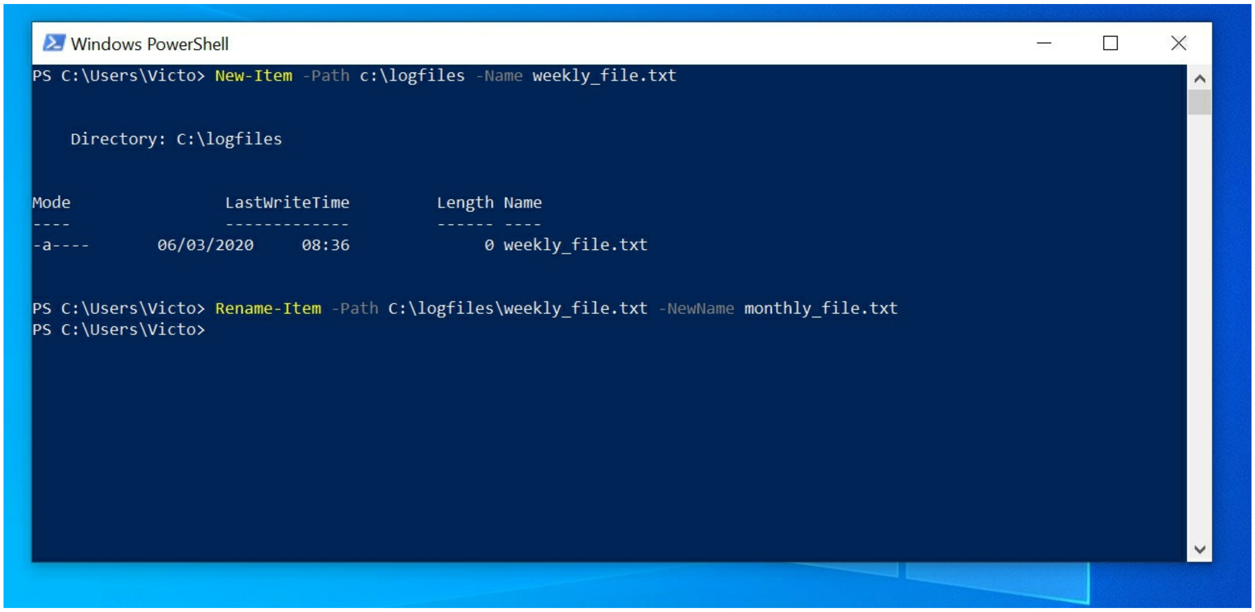
```
PS C:\Users\Victo> New-Item -Path c:\logfiles -Name weekly_file.txt


    Directory: C:\logfiles


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        06/03/2020     08:36              0 weekly_file.txt


PS C:\Users\Victo>
```

Rename-Item

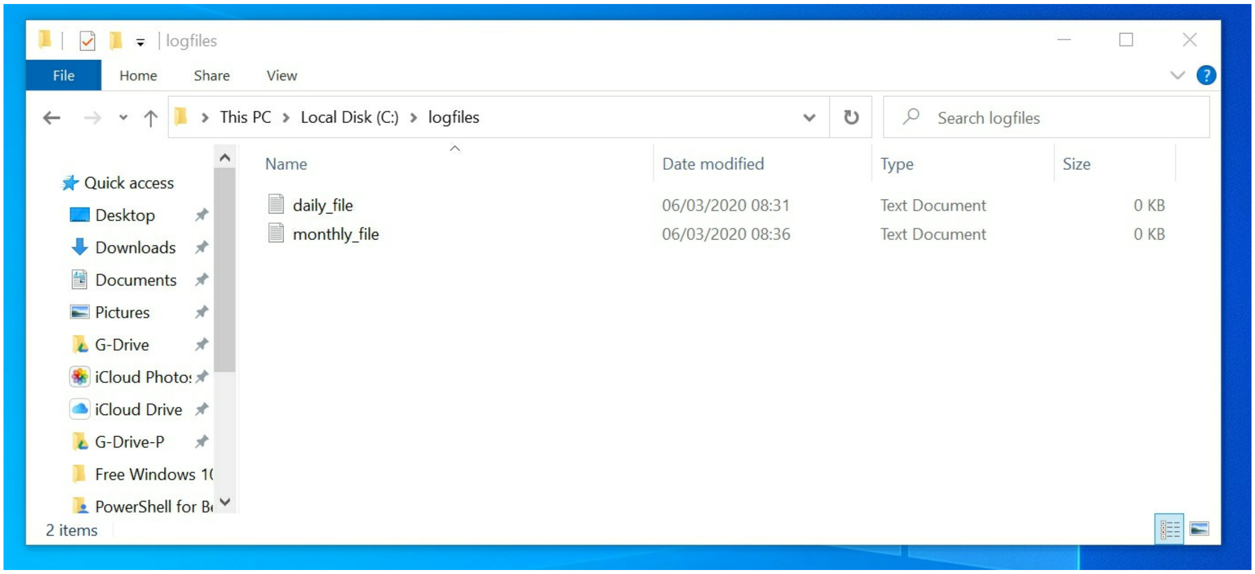
Rename-Item Cmdlet is used to rename things in Windows. This Cmdlet can rename files, folders and registry keys. This command will rename weekly_file.txt to monthly_file.txt

Rename-Item -Path C:\logfiles\weekly_file.txt -NewName monthly_file.txt

When you run the command, it appears that nothing happened, but when you check the folder, the text file has been renamed!



```
PS C:\Users\Victo> New-Item -Path c:\logfiles -Name weekly_file.txt


    Directory: C:\logfiles


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        06/03/2020     08:36              0 weekly_file.txt


PS C:\Users\Victo> Rename-Item -Path C:\logfiles\weekly_file.txt -NewName monthly_file.txt
PS C:\Users\Victo>
```



Name	Date modified	Type	Size
daily_file	06/03/2020 08:31	Text Document	0 KB
monthly_file	06/03/2020 08:36	Text Document	0 KB

1.2 PowerShell Commands for Reporting

There are 3 sets of PowerShell commands that you can use to export items to CVS, text files and or HTML files.

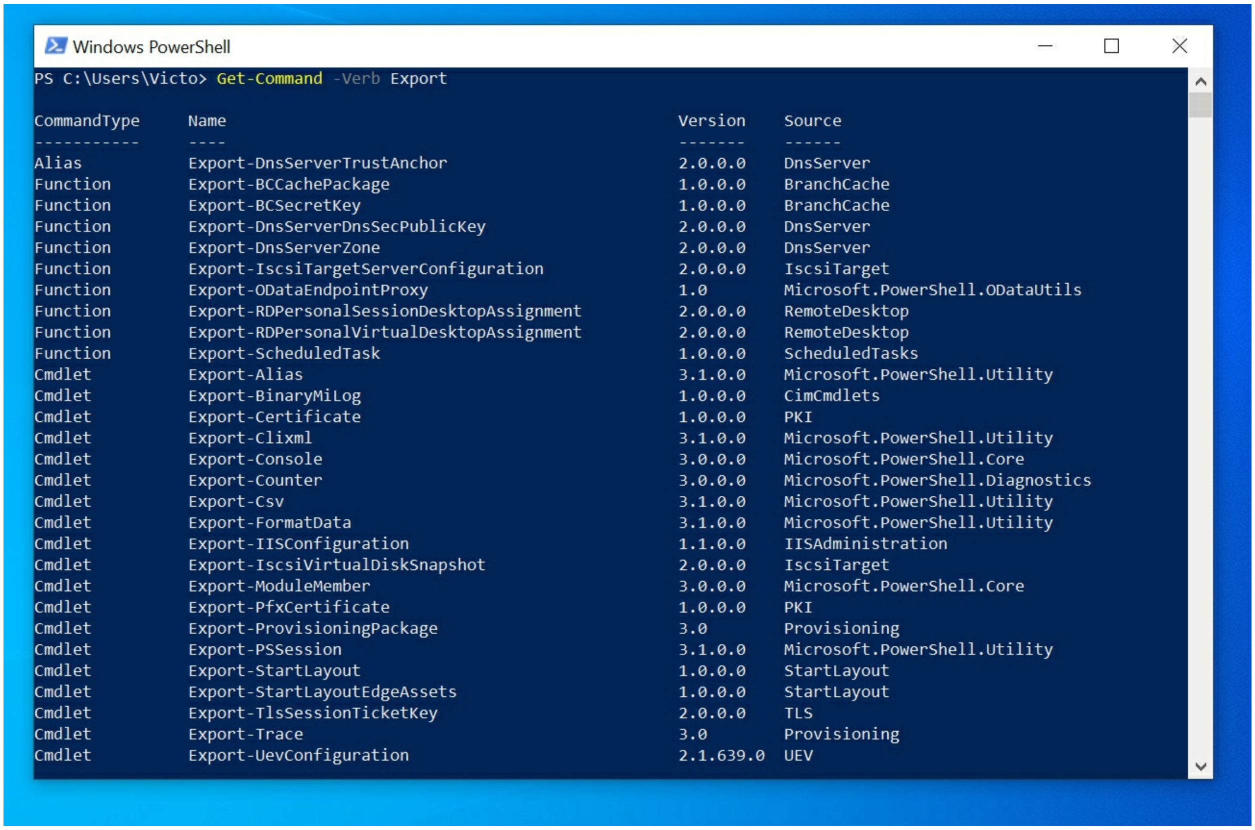
Export-Csv

Export-Csv converts a set of string into CSV and saves in a file. This Cmdlet is very important in reporting.

To demonstrate the use of Export-CSV, run the command below:

```
Get-Command -Verb Export
```

Here is the result of the command.



```
PS C:\Users\Victo> Get-Command -Verb Export

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Alias           Export-DnsServerTrustAnchor                        2.0.0.0    DnsServer
Function        Export-BCCachePackage                              1.0.0.0    BranchCache
Function        Export-BCSecretKey                                 1.0.0.0    BranchCache
Function        Export-DnsServerDnsSecPublicKey                    2.0.0.0    DnsServer
Function        Export-DnsServerZone                               2.0.0.0    DnsServer
Function        Export-IscsiTargetServerConfiguration              2.0.0.0    IscsiTarget
Function        Export-ODataEndpointProxy                          1.0        Microsoft.PowerShell.ODataUtils
Function        Export-RDPersonalSessionDesktopAssignment          2.0.0.0    RemoteDesktop
Function        Export-RDPersonalVirtualDesktopAssignment          2.0.0.0    RemoteDesktop
Function        Export-ScheduledTask                               1.0.0.0    ScheduledTasks
Cmdlet          Export-Alias                                       3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Export-BinaryMiLog                                 1.0.0.0    CimCmdlets
Cmdlet          Export-Certificate                                 1.0.0.0    PKI
Cmdlet          Export-Clixml                                      3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Export-Console                                     3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Export-Counter                                     3.0.0.0    Microsoft.PowerShell.Diagnostics
Cmdlet          Export-Csv                                         3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Export-FormatData                                  3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Export-IISConfiguration                            1.1.0.0    IISAdministration
Cmdlet          Export-IscsiVirtualDiskSnapshot                    2.0.0.0    IscsiTarget
Cmdlet          Export-ModuleMember                                3.0.0.0    Microsoft.PowerShell.Core
Cmdlet          Export-PfxCertificate                              1.0.0.0    PKI
Cmdlet          Export-ProvisioningPackage                         3.0        Provisioning
Cmdlet          Export-PSSession                                   3.1.0.0    Microsoft.PowerShell.Utility
Cmdlet          Export-StartLayout                                 1.0.0.0    StartLayout
Cmdlet          Export-StartLayoutEdgeAssets                       1.0.0.0    StartLayout
Cmdlet          Export-TlsSessionTicketKey                         2.0.0.0    TLS
Cmdlet          Export-Trace                                       3.0        Provisioning
Cmdlet          Export-UevConfiguration                            2.1.639.0  UEV
```

You can pipe the output of the previous command into Export-CSV to create a CVS report of the results shown in the previous image.

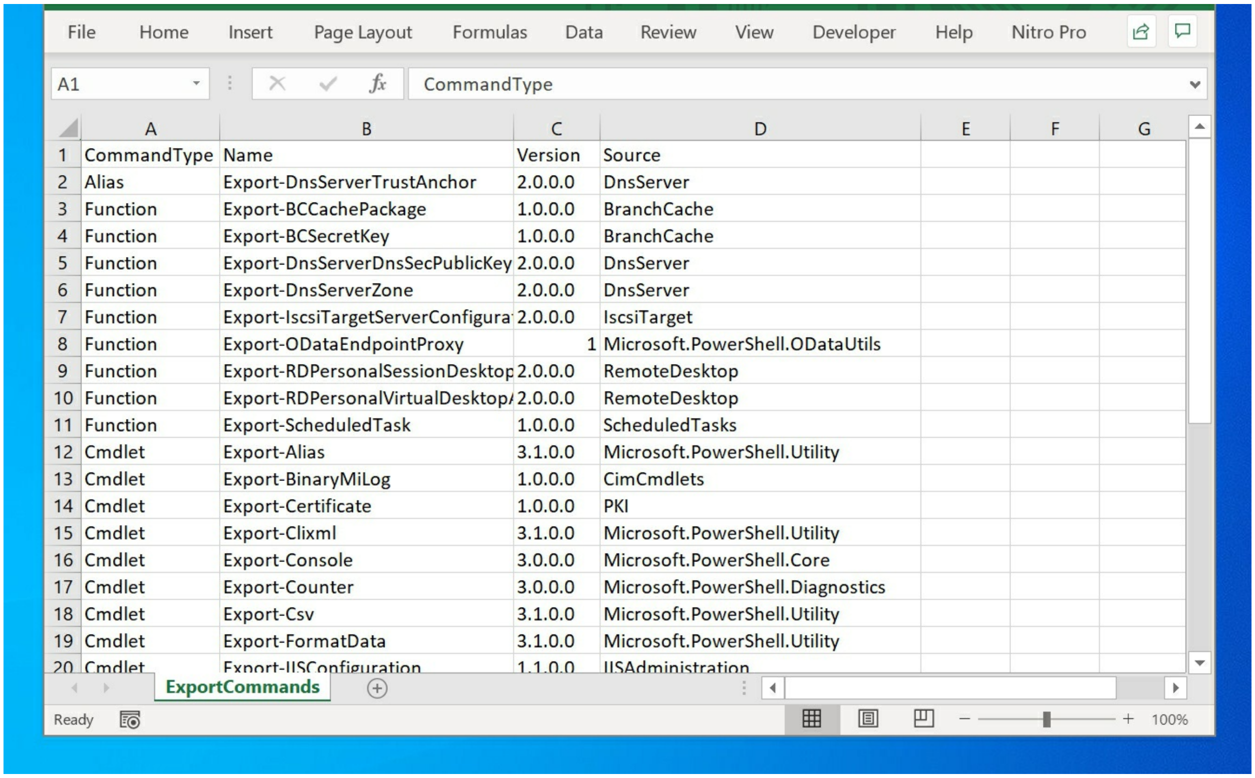
Here is the command to accomplish this task.

Get-Command -Verb Export | Select-Object CommandType, Name, Version, Source | Export-Csv -NoTypeInformation -Path C:\NewFolder\ExportCommands.CSV

Note that I had to include the CSV file name to the path. I also have another parameter -*NoTypeInformation* – To learn more about -NoTypeInformation, read this article PowerShell NoTypeInformation: Applications and Uses.

There is another Cmdlet in the previous command, Select-Object. This Cmdlet was used to specify the columns to return and export to CSV. If I excluded Select-Object the output of the CSV will contain a lot of unwanted data. Later in this tutorial, I will cover Select-Object.

For your reference, below is the output of the CSV file.



	A	B	C	D	E	F	G
1	CommandType	Name	Version	Source			
2	Alias	Export-DnsServerTrustAnchor	2.0.0.0	DnsServer			
3	Function	Export-BCCachePackage	1.0.0.0	BranchCache			
4	Function	Export-BCSecretKey	1.0.0.0	BranchCache			
5	Function	Export-DnsServerDnsSecPublicKey	2.0.0.0	DnsServer			
6	Function	Export-DnsServerZone	2.0.0.0	DnsServer			
7	Function	Export-IscsiTargetServerConfigura	2.0.0.0	IscsiTarget			
8	Function	Export-ODataEndpointProxy	1	Microsoft.PowerShell.ODataUtils			
9	Function	Export-RDPersonalSessionDesktop	2.0.0.0	RemoteDesktop			
10	Function	Export-RDPersonalVirtualDesktopA	2.0.0.0	RemoteDesktop			
11	Function	Export-ScheduledTask	1.0.0.0	ScheduledTasks			
12	Cmdlet	Export-Alias	3.1.0.0	Microsoft.PowerShell.Utility			
13	Cmdlet	Export-BinaryMiLog	1.0.0.0	CimCmdlets			
14	Cmdlet	Export-Certificate	1.0.0.0	PKI			
15	Cmdlet	Export-Clixml	3.1.0.0	Microsoft.PowerShell.Utility			
16	Cmdlet	Export-Console	3.0.0.0	Microsoft.PowerShell.Core			
17	Cmdlet	Export-Counter	3.0.0.0	Microsoft.PowerShell.Diagnostics			
18	Cmdlet	Export-Csv	3.1.0.0	Microsoft.PowerShell.Utility			
19	Cmdlet	Export-FormatData	3.1.0.0	Microsoft.PowerShell.Utility			
20	Cmdlet	Export-IISConfiguration	1.1.0.0	IISAdministration			

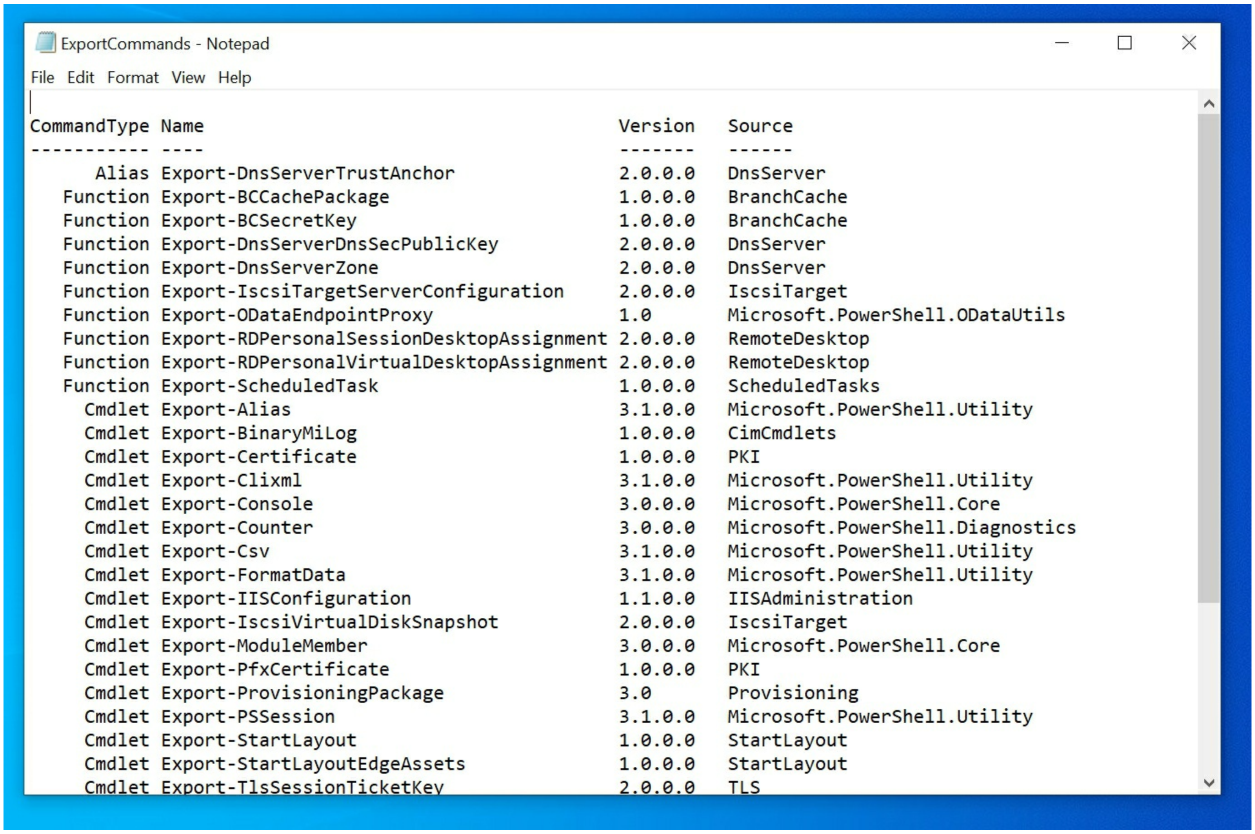
While this report is very similar to the output shown in the previous image, it is more useful as a report. You could send the CSV file to your boss!

Out-File

The Out-file Cmdlet sends output to a text file. The command below exports the out of the Get-Command PowerShell Cmdlet to a text file instead of a CSV:

```
Get-Command -Verb Export | Select-Object CommandType, Name, Version, Source | Out-File
C:\NewFolder\ExportCommands.txt
```

Here is the result in a text file: The same report, now in a text file! How good is that!



```
CommandType Name                                    Version    Source
----------- ----                                    -------    ------
      Alias Export-DnsServerTrustAnchor             2.0.0.0    DnsServer
   Function Export-BCCachePackage                   1.0.0.0    BranchCache
   Function Export-BCSecretKey                      1.0.0.0    BranchCache
   Function Export-DnsServerDnsSecPublicKey         2.0.0.0    DnsServer
   Function Export-DnsServerZone                    2.0.0.0    DnsServer
   Function Export-IscsiTargetServerConfiguration   2.0.0.0    IscsiTarget
   Function Export-ODataEndpointProxy               1.0        Microsoft.PowerShell.ODataUtils
   Function Export-RDPersonalSessionDesktopAssignment 2.0.0.0  RemoteDesktop
   Function Export-RDPersonalVirtualDesktopAssignment 2.0.0.0  RemoteDesktop
   Function Export-ScheduledTask                    1.0.0.0    ScheduledTasks
     Cmdlet Export-Alias                            3.1.0.0    Microsoft.PowerShell.Utility
     Cmdlet Export-BinaryMiLog                      1.0.0.0    CimCmdlets
     Cmdlet Export-Certificate                      1.0.0.0    PKI
     Cmdlet Export-Clixml                           3.1.0.0    Microsoft.PowerShell.Utility
     Cmdlet Export-Console                          3.0.0.0    Microsoft.PowerShell.Core
     Cmdlet Export-Counter                          3.0.0.0    Microsoft.PowerShell.Diagnostics
     Cmdlet Export-Csv                              3.1.0.0    Microsoft.PowerShell.Utility
     Cmdlet Export-FormatData                       3.1.0.0    Microsoft.PowerShell.Utility
     Cmdlet Export-IISConfiguration                 1.1.0.0    IISAdministration
     Cmdlet Export-IscsiVirtualDiskSnapshot         2.0.0.0    IscsiTarget
     Cmdlet Export-ModuleMember                     3.0.0.0    Microsoft.PowerShell.Core
     Cmdlet Export-PfxCertificate                   1.0.0.0    PKI
     Cmdlet Export-ProvisioningPackage              3.0        Provisioning
     Cmdlet Export-PSSession                        3.1.0.0    Microsoft.PowerShell.Utility
     Cmdlet Export-StartLayout                      1.0.0.0    StartLayout
     Cmdlet Export-StartLayoutEdgeAssets            1.0.0.0    StartLayout
     Cmdlet Export-TlsSessionTicketKey              2.0.0.0    TLS
```

The Out-File Cmdlet also allows you to append (add) contents to an existing text file. Here is an example.

Get-Command -Verb Export | Select-Object CommandType, Name, Version, Source | Out-File C:\NewFolder\ExportCommands.txt -Append

1.3 PowerShell Commands to Manage Processes

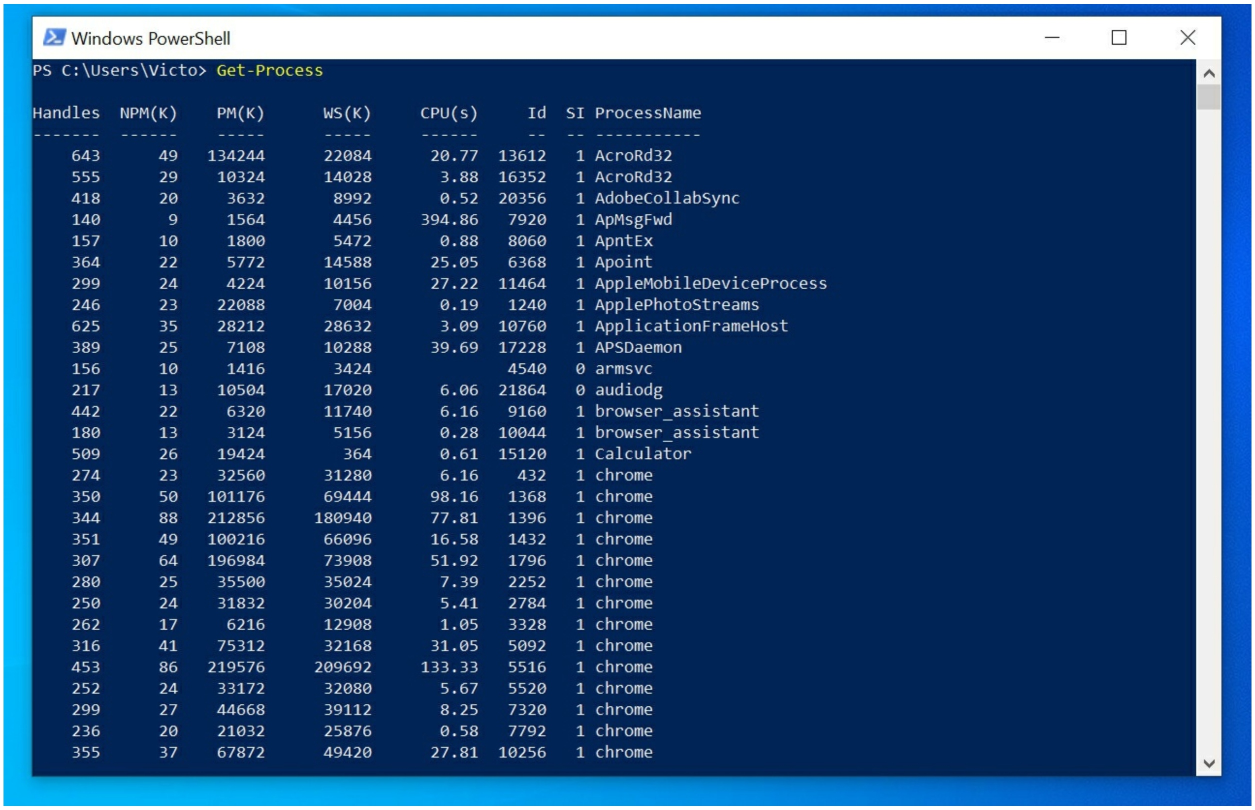
Another set of the most useful PowerShell commands for Windows administrators are Cmdlets to manage Windows processes.

Get-Process

This PowerShell Cmdlet lists all the processes running on a local computer. If you use the *ComputerName* parameter, you can display the processes on a remote computer.

However, when you run the Get-Process PowerShell Cmdlet without any parameter, it returns all processes running on the local computer. To try this, execute the command below. The result is shown in the image below.

Get-Process



```
PS C:\Users\Victo> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    643      49   134244      22084      20.77  13612   1 AcroRd32
    555      29    10324      14028       3.88  16352   1 AcroRd32
    418      20     3632       8992       0.52  20356   1 AdobeCollabSync
    140       9     1564       4456     394.86   7920   1 ApMsgFwd
    157      10     1800       5472       0.88   8060   1 ApntEx
    364      22     5772      14588      25.05   6368   1 Apoint
    299      24     4224      10156      27.22  11464   1 AppleMobileDeviceProcess
    246      23    22088       7004       0.19   1240   1 ApplePhotoStreams
    625      35    28212      28632       3.09  10760   1 ApplicationFrameHost
    389      25     7108      10288      39.69  17228   1 APSDaemon
    156      10     1416       3424              4540   0 armsvc
    217      13    10504      17020       6.06  21864   0 audiodg
    442      22     6320      11740       6.16   9160   1 browser_assistant
    180      13     3124       5156       0.28  10044   1 browser_assistant
    509      26    19424        364       0.61  15120   1 Calculator
    274      23    32560      31280       6.16    432   1 chrome
    350      50   101176      69444      98.16   1368   1 chrome
    344      88   212856     180940      77.81   1396   1 chrome
    351      49   100216      66096      16.58   1432   1 chrome
    307      64   196984      73908      51.92   1796   1 chrome
    280      25    35500      35024       7.39   2252   1 chrome
    250      24    31832      30204       5.41   2784   1 chrome
    262      17     6216      12908       1.05   3328   1 chrome
    316      41    75312      32168      31.05   5092   1 chrome
    453      86   219576     209692     133.33   5516   1 chrome
    252      24    33172      32080       5.67   5520   1 chrome
    299      27    44668      39112       8.25   7320   1 chrome
    236      20    21032      25876       0.58   7792   1 chrome
    355      37    67872      49420      27.81  10256   1 chrome
```

Start-Process and Stop-Process

While the Get-Process Cmdlet can list all processes on a computer, the Start-Process Cmdlet can start a stopped process while the Stop-Process Cmdlet can stop a running process.

To start a process, pipe the output of Get-Process command to the Start-Process command.

As an example, to stop a process with ID 10500, use the command below.

```
Get-Process -Id 10500 | Stop-Process
```

Warning!
Use the Stop-Process PowerShell Cmdlet with caution as stopping the wrong process could make your computer unstable.

1.4 PowerShell Commands to Manage Event logs

Event log management is one of the most important tasks for Windows Administrators. The next set of PowerShell commands will help you manage event logs.

Get-EventLog

The Get-EventLog PowerShell Cmdlet gets events in a specified event log. You can get events on a local or remote computer. To get events from a remote computer, use the -*ComputerName* parameter to specify the remote computer. However, note that you will require the right permissions to access the remote computer.

To get the last 5 events logged in the System event log, execute the command below…

```
Get-EventLog -LogName System -Newest 5
```

Tip
The last command could be used for troubleshooting purposes.

Clear-EventLog

As you would expect there are more event log Cmdlets, but we will cover this 2 for this tutorial.

The Clear-EventLog clears all events in the specified event log. The Cmdlet can clear event logs on both local and remote computers.

The command below clears all events with the name "Windows PowerShell" from the local computer

```
Clear-EventLog "Windows PowerShell"
```

To execute the command below, you need to open PowerShell as Administrator - right-click and select Run as Administrator.

1.5 PowerShell Commands to Get Computer Information

If you need to collect data about computers on your network - Computer Name, BIOS Version, RAM size, Disk Information, etc - Get-WmiObject PowerShell Cmdlet is your friend! let's explore this powerful Cmdlet, shall we?

Get-WmiObject

Get-WmiObject has a parameter called -*Class* this allows you to specify the

WMI object you wish to access. The command below will get a list of WMI classes,

```
Get-WmiObject -List -Class Win32*
```

Once you know the name of the WMI class, you can execute Get-WmiObject to return useful information from a local or remote computer. Below is a list of the most important WMI classes you may need:

- Win32_PhysicalMemory - information about available memory
- Win32_Processor - Processor information
- Win32_LogicalDisk - Logical disk drive information
- Win32_DiskDrive - Physical disk information
- Win32_OperatingSystem - Information about the operating system

To get information about the operating system, run the command below:

```
Get-WmiObject -Class Win32_OperatingSystem
```

1.6 PowerShell Commands to Connect to Remote PowerShell Sessions

You cannot discuss PowerShell commands without talking about PS remoting. As a Windows Systems Administrator, you will need to remotely connect to computers using PowerShell.

Here are the commands you will need.

Enter-PSSession and Exit-PSSession

The Enter-PSSession PowerShell command allows you to interactively start a remote PS session on a single computer. When you finish with the remote computer, you can end the session with the Exit-PSSession command.

To open a remote PS session to a computer called Computer1, run the command below:

```
Enter-PSSession Computer1
```

Invoke-Command

While the Enter-PSSession PowerShell Cmdlet allows you to execute commands on a single remote computer, the Invoke-Command Cmdlet allows you to execute commands on one or more remote computers.

If you wish to execute Get-Process command on Computer1, Computer2, Computer3, execute this command:

```
Invoke-Command -ComputerName Computer1, Computer2, Computer3, -ScriptBlock {Get-Process}
```

New-PSSession

The New-PSSession PowerShell Cmdlet allows you to open a persistent session with a remote computer. Because the session is persistent, it is recommended to add the remote session to a variable.

To open a persistent remote PS session on computers Computer1, Computer2, execute the command below:

```
$session = New-PSSession -ComputerName Computer1, Computer2
```

With the PS session established and stored in the $session variable, you can execute normal PowerShell commands on the remote session using the Invoke-Command PowerShell Cmdlet.

As a final example in remote PowerShell sessions, to execute the Get-Process on the remote computers, run the command:

```
Invoke-Command -Session $session {$Processes = Get-Process}
```

I stored the results of the Get-Process command in a variable called $Processes because there are multiple computers. Storing the result in a variable makes for easy data manipulation. For example, you could use a ForEach loop to extract and organize the data.

Chapter 2: 20 Most Useful Command Prompt Commands

Here is my ultimate list of Command Prompt commands for very serious Windows Systems Administrators. For each command, I explain its syntax and parameters. Then I give examples.

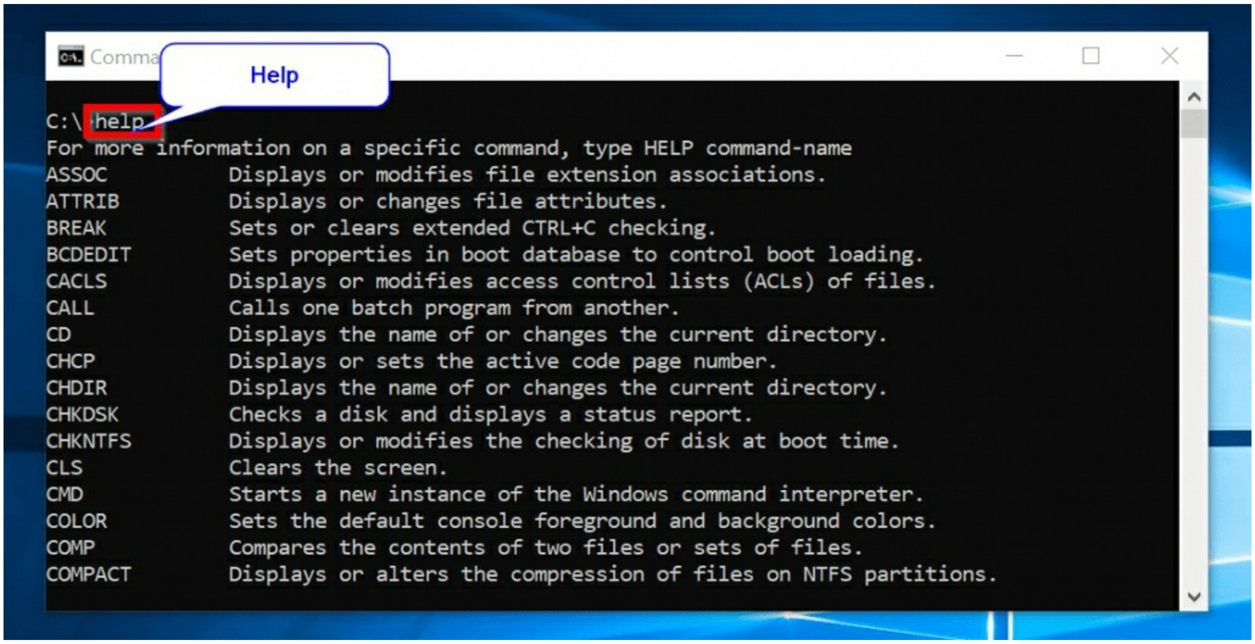
The commands are grouped into 5

1. **General** Command Prompt Commands
2. Commands to **Manage Disks & Partitions**
3. Commands to **Copy Files and Folders**
4. **System Administration and Reporting** commands and
5. Commands for **Managing Files and Folders**.

2.0 General Command Prompt Commands

HELP

The HELP command provides help information for Windows commands. When you type HELP in cmd without any parameters, it lists and briefly describes all available Windows commands.



```
C:\>help
For more information on a specific command, type HELP command-name
ASSOC          Displays or modifies file extension associations.
ATTRIB         Displays or changes file attributes.
BREAK          Sets or clears extended CTRL+C checking.
BCDEDIT        Sets properties in boot database to control boot loading.
CACLS          Displays or modifies access control lists (ACLs) of files.
CALL           Calls one batch program from another.
CD             Displays the name of or changes the current directory.
CHCP           Displays or sets the active code page number.
CHDIR          Displays the name of or changes the current directory.
CHKDSK         Checks a disk and displays a status report.
CHKNTFS        Displays or modifies the checking of disk at boot time.
CLS            Clears the screen.
CMD            Starts a new instance of the Windows command interpreter.
COLOR          Sets the default console foreground and background colors.
COMP           Compares the contents of two files or sets of files.
COMPACT        Displays or alters the compression of files on NTFS partitions.
```

This is very useful if you are trying to find a command but can't remember it.

HELP Syntax

The full syntax of the HELP command is

HELP [<command>]

Or

[<command>] /?

Tip

<command> is the Windows command you want to get information about.

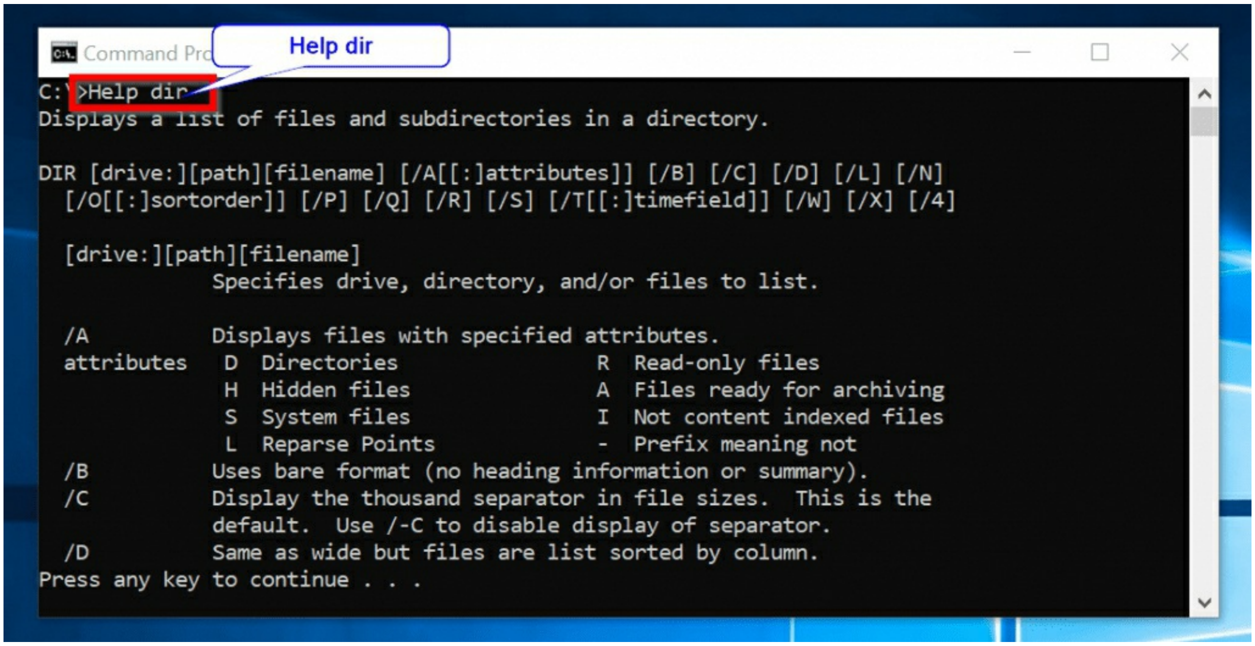
HELP Parameters

Parameter	Description
<command>	Specifies the name of the command prompt command you want information about

HELP Examples

As an example, to get information about the **DIR** command, type the following command and press enter.

HELP **DIR**



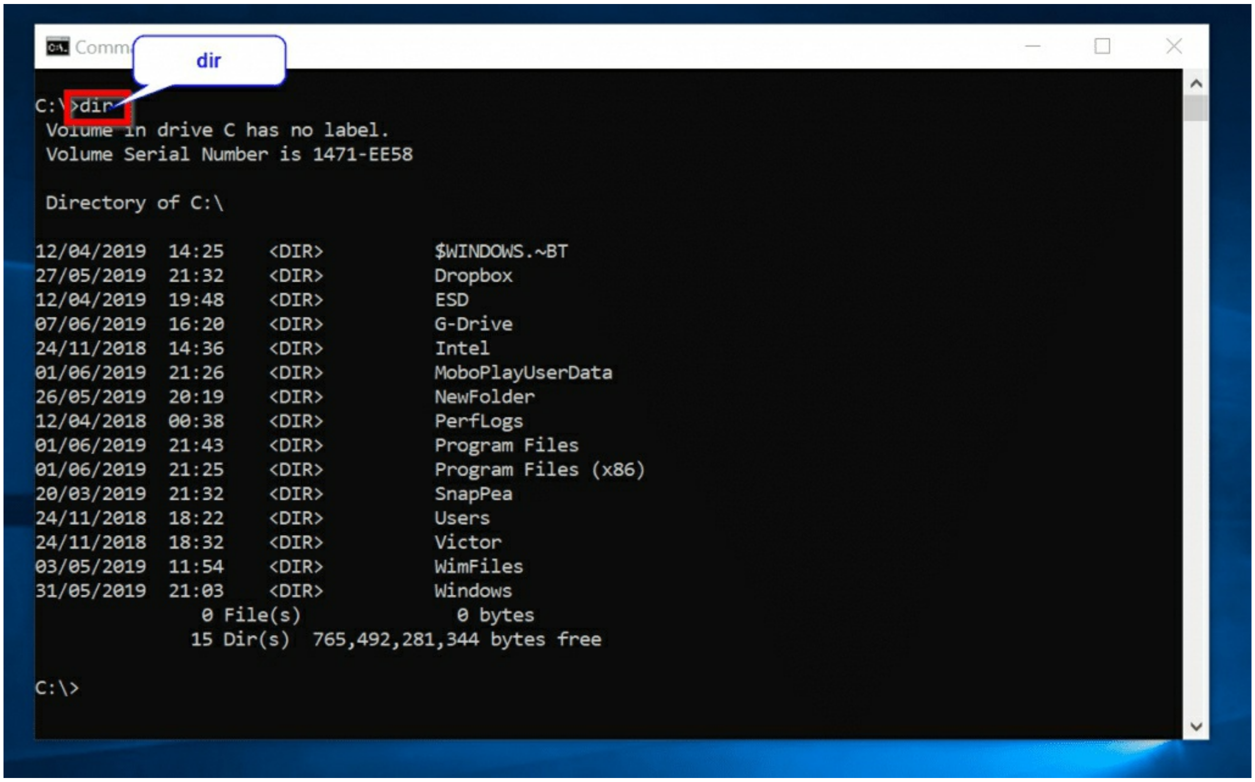
```
C:\>Help dir
Displays a list of files and subdirectories in a directory.

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             -  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.
Press any key to continue . . .
```

The command below will achieve the same result as **HELP DIR**:

DIR /?

DIR

The **DIR** command displays a list of files and sub-directories in a directory. If you use **DIR** without any parameter, it displays volume label, Volume Serial Number and a list of folders in the current path.



```
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 1471-EE58

 Directory of C:\

12/04/2019  14:25    <DIR>          $WINDOWS.~BT
27/05/2019  21:32    <DIR>          Dropbox
12/04/2019  19:48    <DIR>          ESD
07/06/2019  16:20    <DIR>          G-Drive
24/11/2018  14:36    <DIR>          Intel
01/06/2019  21:26    <DIR>          MoboPlayUserData
26/05/2019  20:19    <DIR>          NewFolder
12/04/2018  00:38    <DIR>          PerfLogs
01/06/2019  21:43    <DIR>          Program Files
01/06/2019  21:25    <DIR>          Program Files (x86)
20/03/2019  21:32    <DIR>          SnapPea
24/11/2018  18:22    <DIR>          Users
24/11/2018  18:32    <DIR>          Victor
03/05/2019  11:54    <DIR>          WimFiles
31/05/2019  21:03    <DIR>          Windows
               0 File(s)              0 bytes
              15 Dir(s)  765,492,281,344 bytes free

C:\>
```

DIR Syntax

The full syntax of the DIR command is:

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

For this guide, I will limit the syntax to include parameters that you need to use regularly. Below is the modified syntax for the DIR command.

DIR [drive:] [path] [filename] [/A[[:]attributes]] [/P] [/Q] [/W] [/D] [/L] /O[[:]<SortOrder>] [/S]

DIR Parameters

Parameter	**Description**
[drive:][path] [filename]	Specifies drive, directory, and/or files to list.
[/A[[:]*Attributes*]]	Displays files with specified attributes. Click *Attributes* for more information
	Pauses after each screenful of information. To see the next

/P	screen, press any key.
/Q	Display file ownership information.
/W	Displays the results in a wide list format.
/D	Same as /W but files are sorted by column.
/L	Displays directory and file names in lowercase (lists are not sorted).
/O[[:] <*SortOrder*>]	Files are listed as defined by <*SortOrder*>
/S	Displays all files in the specified directory and all sub-directories.

Tip

If ***/A*** *is used without specifying* Attributes*,* ***DIR*** *displays the names of all files, including hidden and system files. This is very useful if you wish to see hidden files in a directory.*

DIR Examples

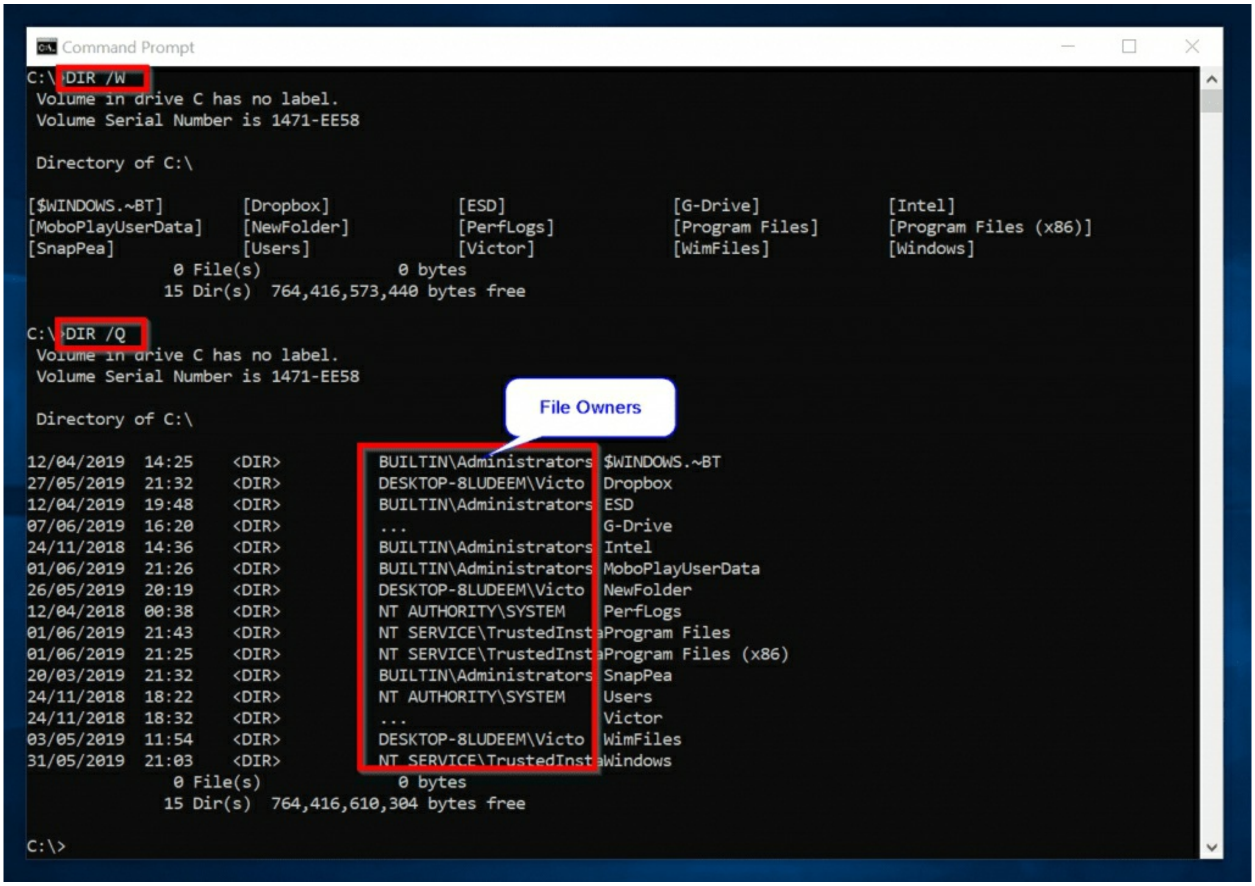
To display all top directories in drive C in a wide list, use this command below:

```
DIR /W
```

To display owners of the files, use the one below:

```
DIR /Q
```

Here are the results:



```
C:\>DIR /W
 Volume in drive C has no label.
 Volume Serial Number is 1471-EE58

 Directory of C:\

[$WINDOWS.~BT]       [Dropbox]            [ESD]                [G-Drive]            [Intel]
[MoboPlayUserData]   [NewFolder]          [PerfLogs]           [Program Files]      [Program Files (x86)]
[SnapPea]            [Users]              [Victor]             [WimFiles]           [Windows]
               0 File(s)              0 bytes
              15 Dir(s)  764,416,573,440 bytes free

C:\>DIR /Q
 Volume in drive C has no label.
 Volume Serial Number is 1471-EE58

 Directory of C:\

12/04/2019  14:25    <DIR>          BUILTIN\Administrators $WINDOWS.~BT
27/05/2019  21:32    <DIR>          DESKTOP-8LUDEEM\Victo  Dropbox
12/04/2019  19:48    <DIR>          BUILTIN\Administrators ESD
07/06/2019  16:20    <DIR>          ...                    G-Drive
24/11/2018  14:36    <DIR>          BUILTIN\Administrators Intel
01/06/2019  21:26    <DIR>          BUILTIN\Administrators MoboPlayUserData
26/05/2019  20:19    <DIR>          DESKTOP-8LUDEEM\Victo  NewFolder
12/04/2018  00:38    <DIR>          NT AUTHORITY\SYSTEM    PerfLogs
01/06/2019  21:43    <DIR>          NT SERVICE\TrustedInstaProgram Files
01/06/2019  21:25    <DIR>          NT SERVICE\TrustedInstaProgram Files (x86)
20/03/2019  21:32    <DIR>          BUILTIN\Administrators SnapPea
24/11/2018  18:22    <DIR>          NT AUTHORITY\SYSTEM    Users
24/11/2018  18:32    <DIR>          ...                    Victor
03/05/2019  11:54    <DIR>          DESKTOP-8LUDEEM\Victo  WimFiles
31/05/2019  21:03    <DIR>          NT SERVICE\TrustedInstaWindows
               0 File(s)              0 bytes
              15 Dir(s)  764,416,610,304 bytes free

C:\>
```

CHDIR (CD)

CD is the short version of **CHDIR**. **CHDIR** displays the name of or changes the current directory to another directory.

CHDIR Syntax

CHDIR [/D] [drive:] [path]

Or

CHDIR [..]

Tip

".." changes to the parent directory.

CD Parameters

Parameter	Description
/D	Changes the current drive as well as the current directory for a drive.
[drive:]	Specifies the drive to display or change to. (if different from the current drive).

[path]	Specifies the path to the directory that you want to display or change to.
[..]	Tells command prompt to change to the parent folder of the current directory.

CD Examples

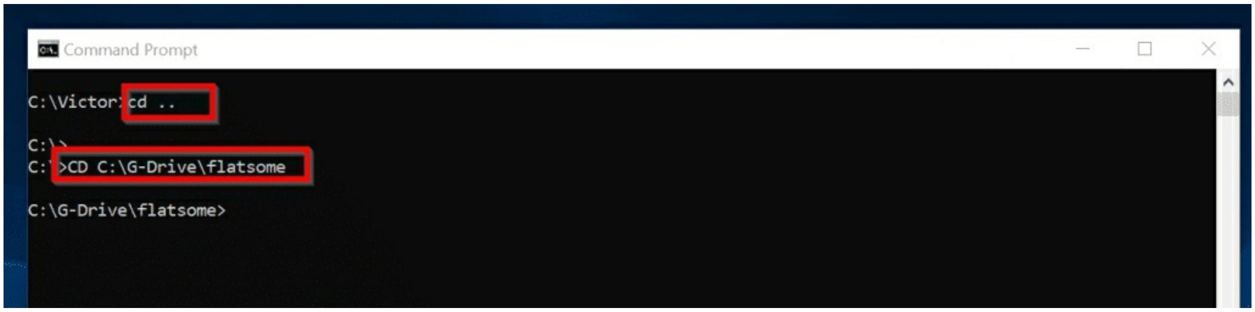
In the example below, I want to change from my current directory (\Victor) to the parent directory C:\

```
CD ..
```

To change to the directory, C:\G-Drive\flatsome, enter the command:

```
CD C:\G-Drive\flatsome
```

Results…



```
C:\Victor>cd ..

C:\>
C:\>CD C:\G-Drive\flatsome

C:\G-Drive\flatsome>
```

2.1 Command Prompt Commands to Manage Disks & Partitions

The next set of command prompt commands are used to check your disk for errors, fix problems with your disk or format disks.

CHKDSK

Checks the file system and file system metadata of a disk volume for logical and/or physical errors. It then displays a status report.

CHKDSK Syntax

The full syntax is:

```
CHKDSK [<volume>[[<path>]filename]]] [/F] [/V] [/R] [/X] [/I] [/C] [/L[:size]] [/B] [/scan] [/spotfix]
```

I will only discuss parameters that you will require to use often. Below is the modified syntax I will discuss in this guide:

```
CHKDSK [volume[[path]filename]]] [/F] [/R] [/X] [/B] [/SCAN]
```

Tip

If you use CHKDSK without specifying any parameters, it displays just the status of the volume without fixing any errors. Running CHKDSK requires admin permission.

CHKDSK Parameters

Parameters	**Description**
<volume>	Specifies the drive letter (followed by a colon), mount point, or volume name.
[<Path>] <filename>	Specifies the location and name of a file or set of files that you want **CHKDSK** to check for fragmentation.
/F	Fixes errors on the disk. The disk cannot be used by another process. If the disk is in use by another process, you will be prompted to fix errors at the next reboot.
/R	Locates bad sectors and recovers readable information. If the /scan option is not specified /R implies /F.
/X	Performs a less vigorous check of index entries. /X applies to NTFS only.
/B	Re-evaluates bad clusters on the volume. /B implies /R and only applies to NTFS volumes.
[/SCAN]	NTFS only - Runs an online scan on the volume.

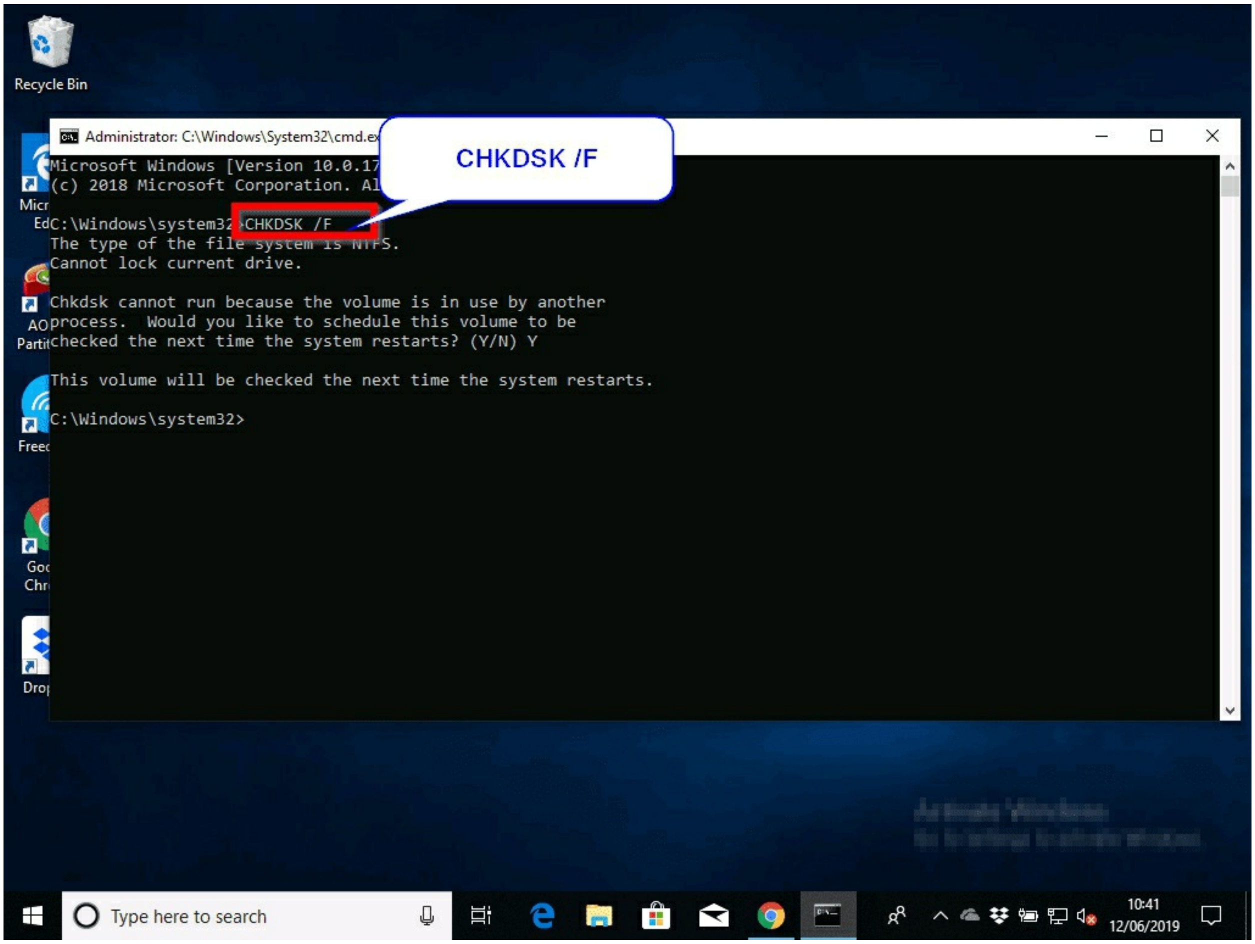
CHKDSK Examples

To find physical disk errors in the file system and attempt to recover data from any disk with bad sectors, run the command:

```
CHKDSK /F
```

Tip

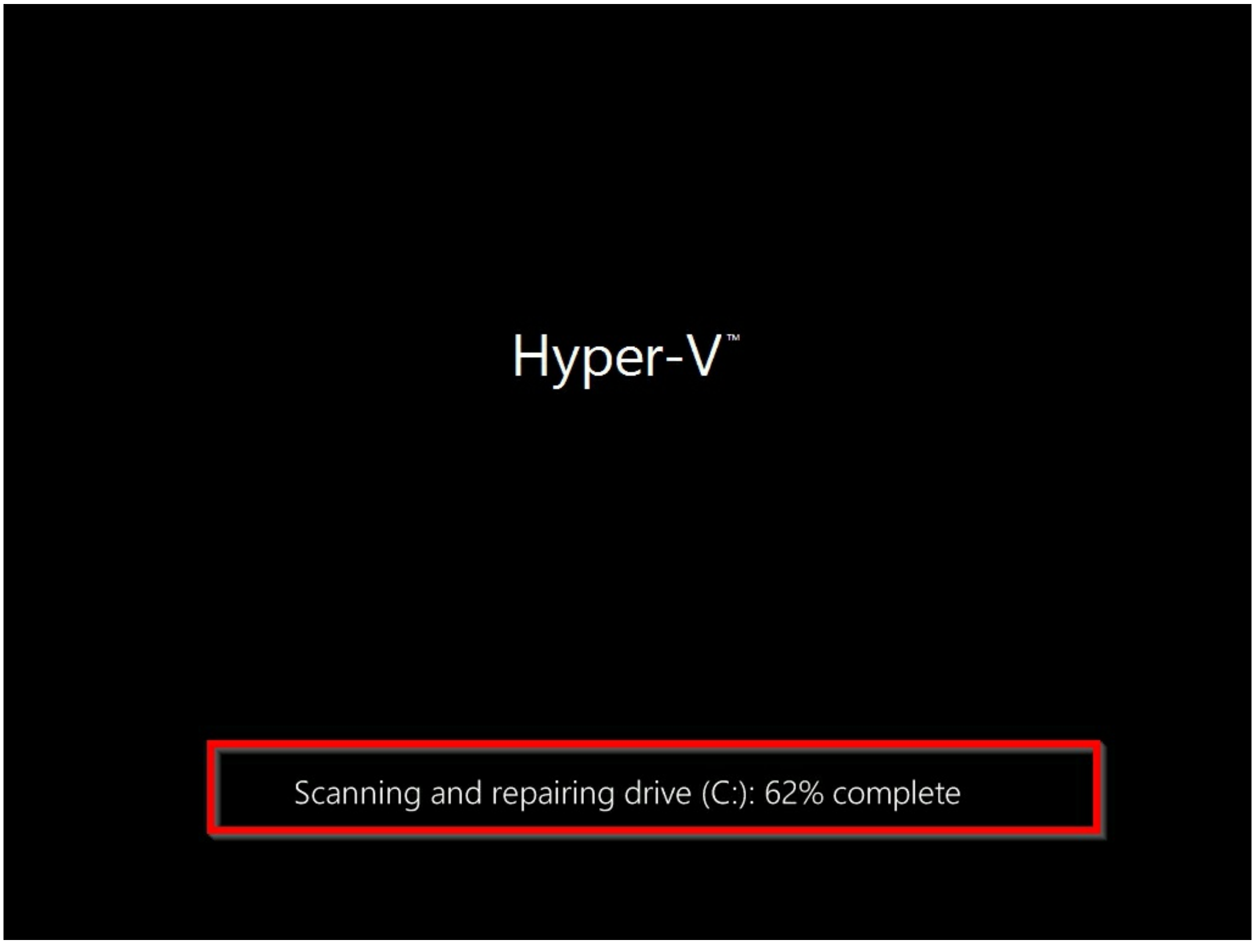
To run the previous command, you MUST open a command prompt as administrator. To open CMD as administrator: Search for cmd, right-click it and click Run as administrator.



```
Microsoft Windows [Version 10.0.17
(c) 2018 Microsoft Corporation. Al

C:\Windows\system32>CHKDSK /F
The type of the file system is NTFS.
Cannot lock current drive.

Chkdsk cannot run because the volume is in use by another
process.  Would you like to schedule this volume to be
checked the next time the system restarts? (Y/N) Y

This volume will be checked the next time the system restarts.

C:\Windows\system32>
```

From the last command, because I ran **CHKDSK** on a system volume (Drive C:), I received the message "chkdisk cannot run...". To run **CHKDSK** on the next reboot, enter **Y**. Then press Enter. Reboot your computer.

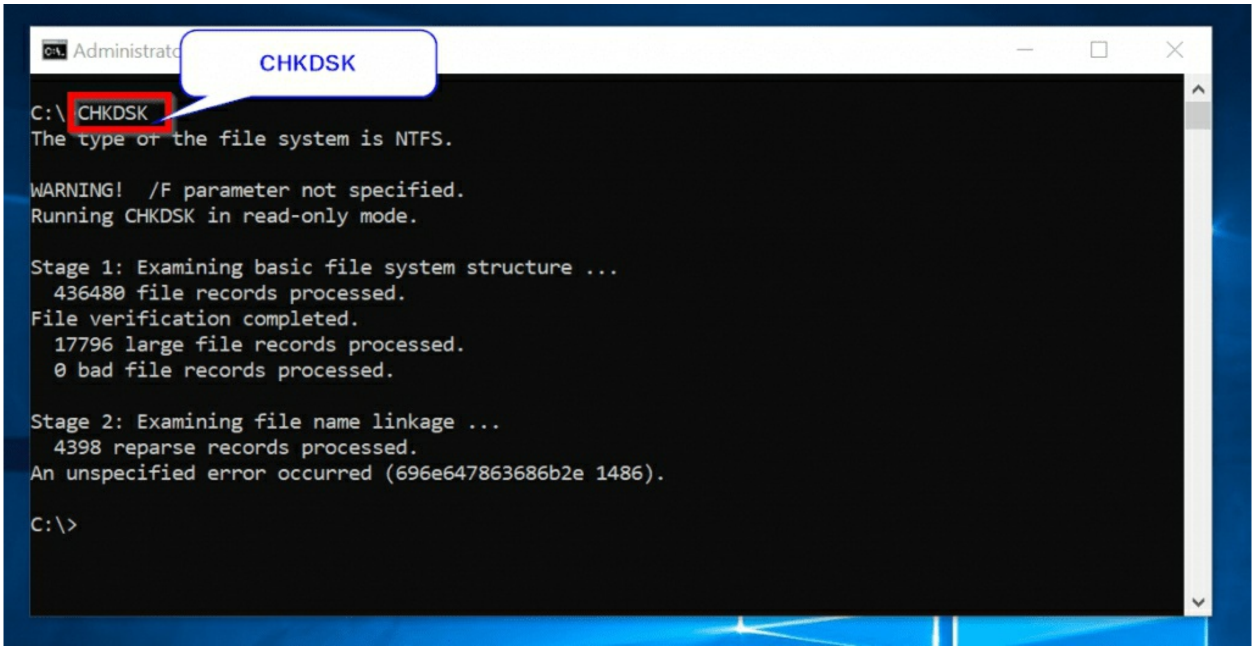
When I reboot my computer, **CHKDSK** is scanning and repairing my drive.



```
Scanning and repairing drive (C:): 62% complete
```

To check your disks for errors without attempting to fix errors, run **CHKDSK** without any parameter.

```
CHKDSK
```



```
C:\ CHKDSK
The type of the file system is NTFS.

WARNING!  /F parameter not specified.
Running CHKDSK in read-only mode.

Stage 1: Examining basic file system structure ...
  436480 file records processed.
File verification completed.
  17796 large file records processed.
  0 bad file records processed.

Stage 2: Examining file name linkage ...
  4398 reparse records processed.
An unspecified error occurred (696e647863686b2e 1486).

C:\>
```

CHKNTFS

This is one of the most ignored command prompt commands. **CHKNTFS** is as important as **CHKDSK**. The difference is that **CHKNTFS** displays or modifies the checking of disk at boot time while **CHKDSK** can run when the Operating System is running.

CHKNTFS Syntax

```
CHKNTFS volume […]
CHKNTFS /D
CHKNTFS /T[:time]
CHKNTFS /X volume […]
CHKNTFS /C volume […]
```

Tip
If CHKNTFS is used without specifying parameters, it will show if the specified drive is dirty or scheduled to be checked on the next reboot.

CHKNTFS Parameters

Parameters	Description
volume	Specifies the drive letter (then a colon), volume name or mount point.
/D	Restores the computer to the default behavior; all drives are checked the next time the computer reboots. **CHKNTFS** will then run on all drives that are marked as dirty.
/T:time	Changes the AUTOCHK initiation countdown time to the specified amount of time in seconds. If time is not specified, it displays the current setting.
/X	Used to define drives excluded from the default boot-time check.
/C	Schedules a drive to be checked at boot time; **CHKDSK** will then run if the drive is dirty.

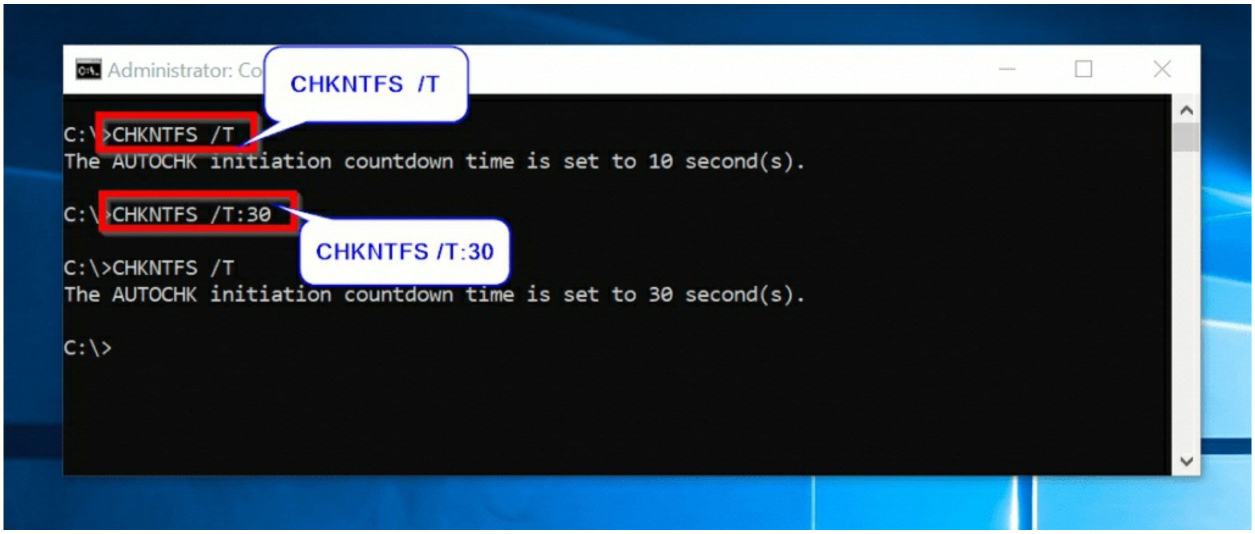
CHKNTFS Examples

To see the Autochk.exe initiation countdown time for a computer:

```
CHKNTFS /T
```

If you wish to modify the initiation countdown time for Autochk.exe to 30 secs:

CHKNTFS /T:30



```
C:\>CHKNTFS /T
The AUTOCHK initiation countdown time is set to 10 second(s).

C:\>CHKNTFS /T:30

C:\>CHKNTFS /T
The AUTOCHK initiation countdown time is set to 30 second(s).

C:\>
```

DISKPART

DISKPART command is used to manage disks, partitions, volumes, or virtual hard disks. **DISKPART** loads its interface within cmd. For this reason, it does not operate like other command prompt commands.

DISKPART commands

DISKPART has a long list of commands you can run. Below, I have listed the commands that you will need for most disk management tasks:

HELP: Displays all DISKPART commands.

LIST: Display a list of objects

SELECT: Shift the focus to an object - makes the object available for editing

RESCAN: Rescan your PC for new disks and volumes.

COMPACT: Attempts to reduce the physical size of a specified file.

ACTIVE: Mark the selected partition as active.

ASSIGN: Assigns a drive letter or mount point to the selected volume.

ATTACH: Attaches a virtual disk file.

DETACH: Detaches a virtual disk file.

CONVERT: Convert between different disk formats (FAT, FAT32, NTFS).

CREATE: Creates a volume, partition or virtual disk.

DELETE: Deletes an object.

EXIT: Exit DISKPART.

EXTEND: Extend a volume.

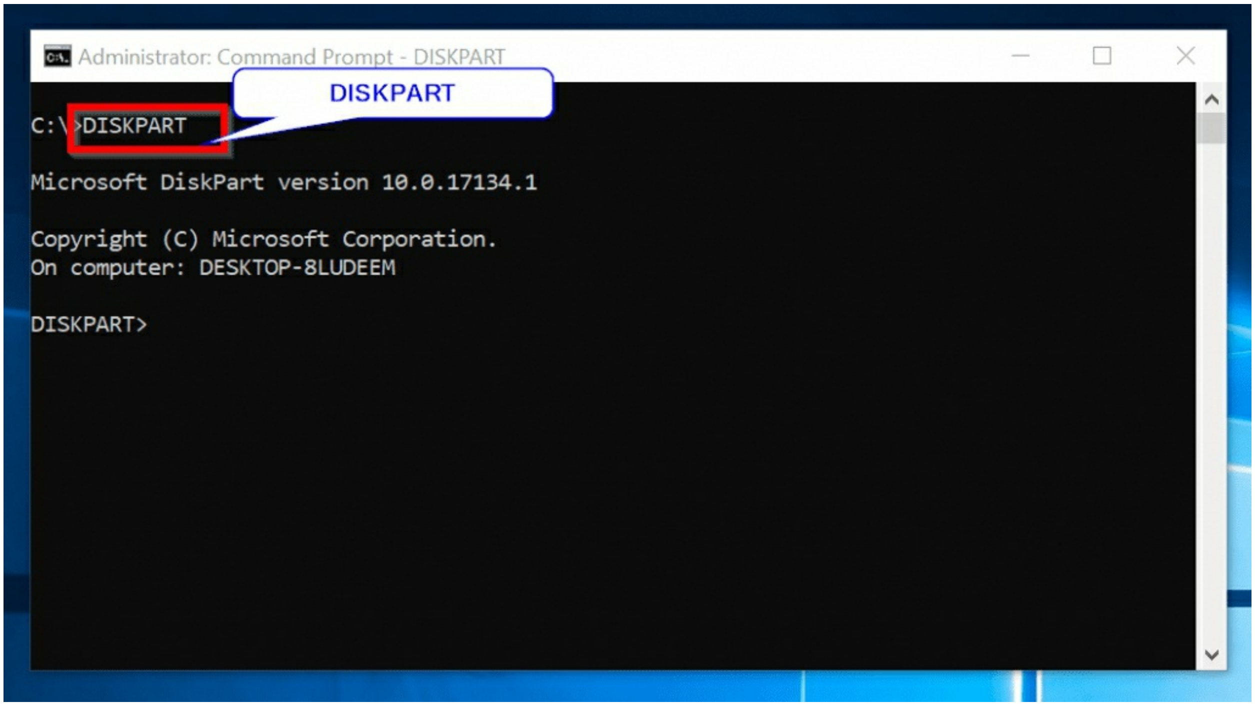
FORMAT: Formats the selected volume or partition.

For a full list of all DISKPART commands, execute HELP within the DISKPART interface. More on this later. You could also get the full list of DISKPART commands by clicking DiskPart commands.

To get into the DISKPART command interface, execute the command below:

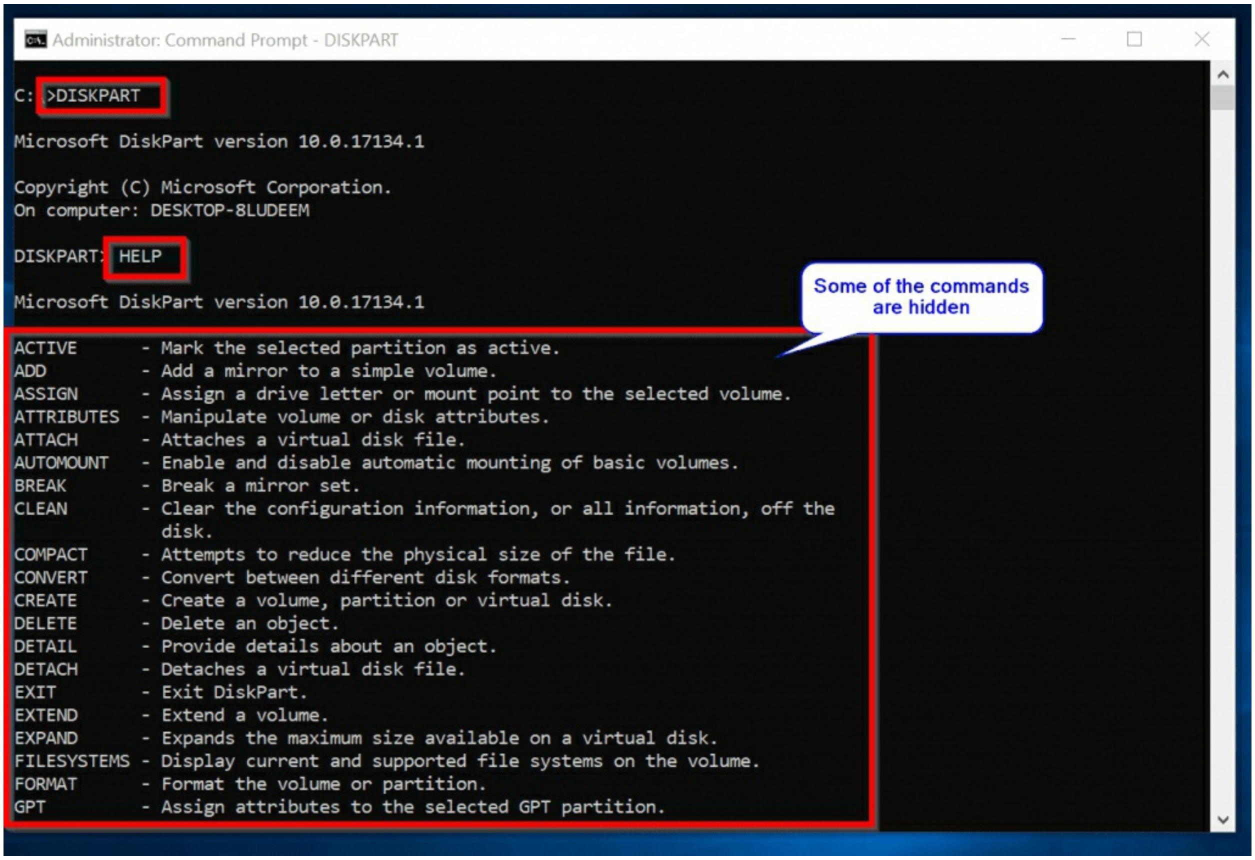
DISKPART

The DISKPART command prompt will load:



```
C:\>DISKPART

Microsoft DiskPart version 10.0.17134.1

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-8LUDEEM

DISKPART>
```

To list all available commands, run the HELP command:



```
C: >DISKPART

Microsoft DiskPart version 10.0.17134.1

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-8LUDEEM

DISKPART: HELP

Microsoft DiskPart version 10.0.17134.1

ACTIVE      - Mark the selected partition as active.
ADD         - Add a mirror to a simple volume.
ASSIGN      - Assign a drive letter or mount point to the selected volume.
ATTRIBUTES  - Manipulate volume or disk attributes.
ATTACH      - Attaches a virtual disk file.
AUTOMOUNT   - Enable and disable automatic mounting of basic volumes.
BREAK       - Break a mirror set.
CLEAN       - Clear the configuration information, or all information, off the
              disk.
COMPACT     - Attempts to reduce the physical size of the file.
CONVERT     - Convert between different disk formats.
CREATE      - Create a volume, partition or virtual disk.
DELETE      - Delete an object.
DETAIL      - Provide details about an object.
DETACH      - Detaches a virtual disk file.
EXIT        - Exit DiskPart.
EXTEND      - Extend a volume.
EXPAND      - Expands the maximum size available on a virtual disk.
FILESYSTEMS - Display current and supported file systems on the volume.
FORMAT      - Format the volume or partition.
GPT         - Assign attributes to the selected GPT partition.
```

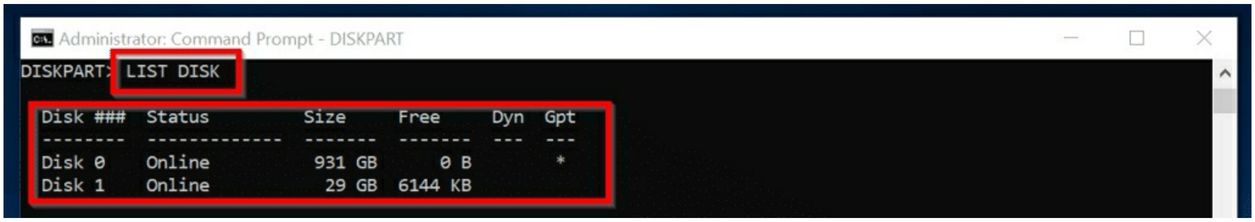
Some of the commands are hidden

DISKPART Examples

Once you get into DISKPART, run the **LIST DISK** command

LIST DISK

This will display all available disks on your computer

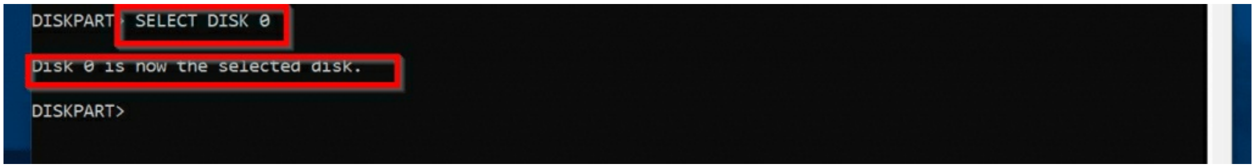


```
DISKPART: LIST DISK

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          931 GB      0 B        *
  Disk 1    Online           29 GB  6144 KB
```

Next, to work on disk 0, execute:

SELECT DISK 0

DISK 0 is now selected



```
DISKPART> SELECT DISK 0

Disk 0 is now the selected disk.

DISKPART>
```

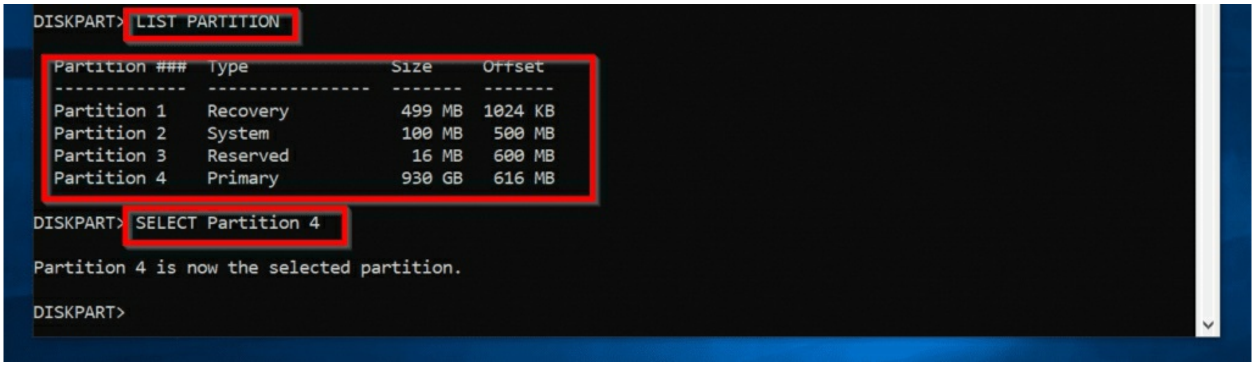
To view available partitions on disk 0, run this command:

LIST PARTITION

To work on Partition 4, for example, run:

SELECT Partition 4

Below are the result of both commands:



```
DISKPART> LIST PARTITION

  Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
  Partition 1    Recovery           499 MB  1024 KB
  Partition 2    System             100 MB   500 MB
  Partition 3    Reserved            16 MB   600 MB
  Partition 4    Primary            930 GB   616 MB

DISKPART> SELECT Partition 4

Partition 4 is now the selected partition.

DISKPART>
```

You can then DELETE the selected partition. I believe you get the gist now.

FORMAT

This command formats a disk for use with Windows. Most people normally format a disk using Disk Management. For administrators, using the FORMAT command may sometimes be necessary.

FORMAT Syntax

FORMAT has a long list of parameters. For this guide, I will stick to the commonly used parameters as shown in the syntax below:

FORMAT volume [/FS:file-system] [/V:label] [/Q]

FORMAT Parameters

Parameters	Description
volume	Specifies the drive letter. Must specify a colon after the drive letter. volume parameter may also specify mount point or volume name.
/FS:filesystem	Specifies the type of the file system for format the drive for. Available options are FAT, FAT32, exFAT, NTFS, UDF and ReFS.
/V:label	Specifies the volume label.
/Q	Performs a quick format.

FORMAT Examples

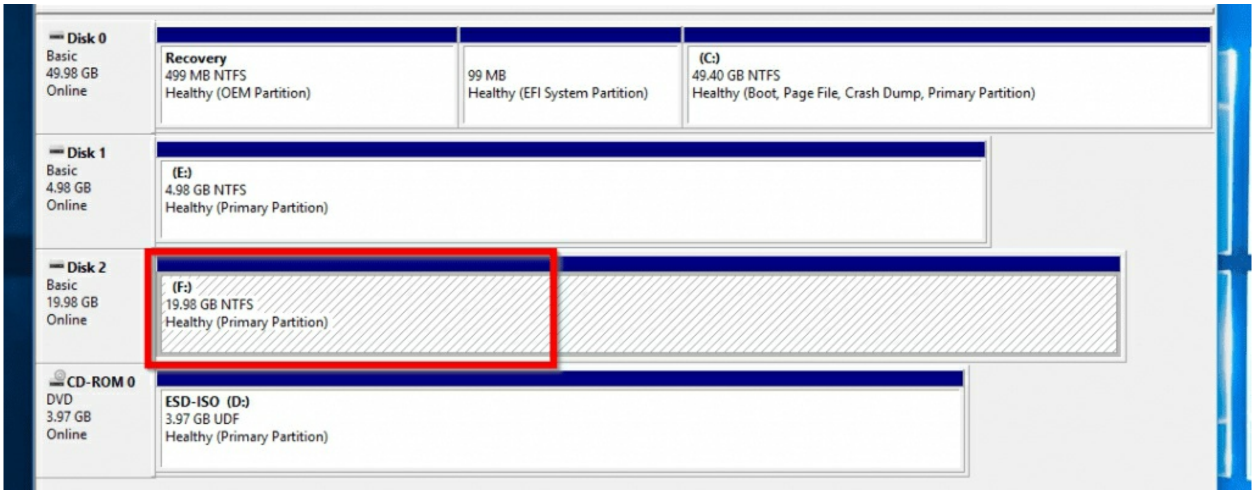
To format the volume highlighted in the image below with the NTFS file system, and a volume label "FORMAT-Test", then perform a quick format, use the command:

FORMAT F: /FS:NTFS /Q /V:FORMAT-Test

Tip

To use the FORMAT command, you MUST open a command prompt as Administrator.

From the previous command, the volume is now formatted.



Disk 0
Basic
49.98 GB
Online

Recovery
499 MB NTFS
Healthy (OEM Partition)

99 MB
Healthy (EFI System Partition)

(C:)
49.40 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
4.98 GB
Online

(E:)
4.98 GB NTFS
Healthy (Primary Partition)

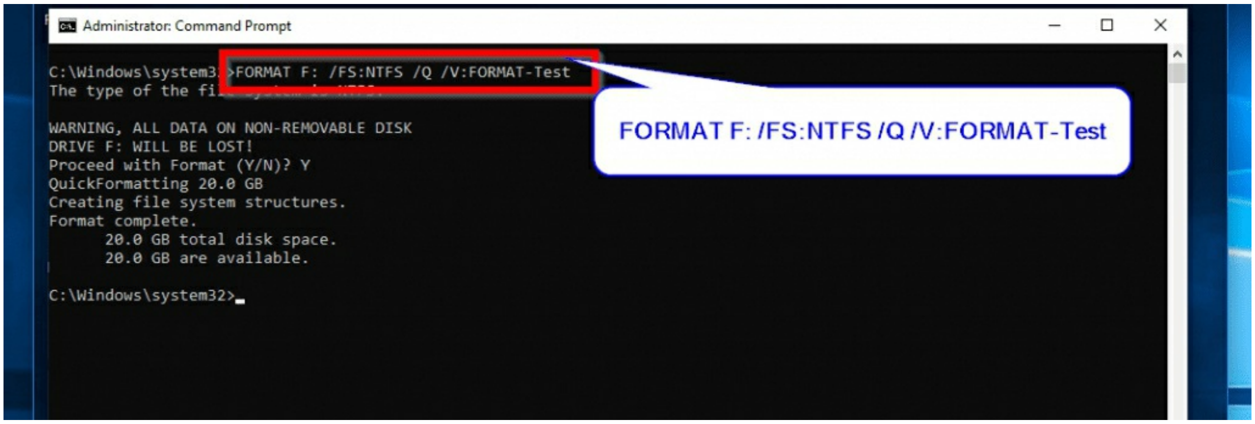
Disk 2
Basic
19.98 GB
Online

(F:)
19.98 GB NTFS
Healthy (Primary Partition)

CD-ROM 0
DVD
3.97 GB
Online

ESD-ISO (D:)
3.97 GB UDF
Healthy (Primary Partition)

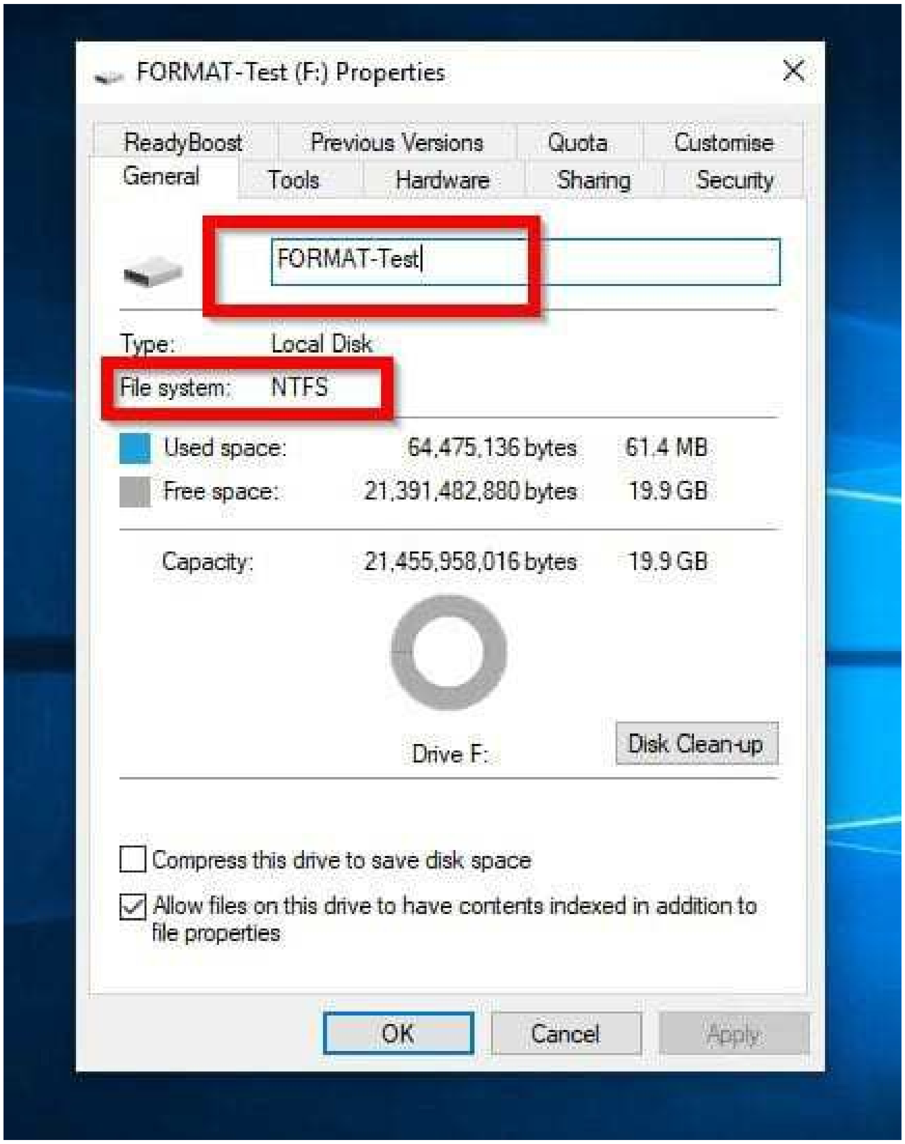
When you click Enter to run the last command you will be asked to confirm. Enter **Y**, then press the Enter key. See the result of the command below:



```
C:\Windows\system32>FORMAT F: /FS:NTFS /Q /V:FORMAT-Test
The type of the file system is NTFS.

WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE F: WILL BE LOST!
Proceed with Format (Y/N)? Y
QuickFormatting 20.0 GB
Creating file system structures.
Format complete.
      20.0 GB total disk space.
      20.0 GB are available.

C:\Windows\system32>_
```

FORMAT F: /FS:NTFS /Q /V:FORMAT-Test

The disk is formatted as NTFS with volume label "FORMAT-Test"



FORMAT-Test (F:) Properties

FORMAT-Test

Type: Local Disk

File system: NTFS

🟦 Used space: 64,475,136 bytes 61.4 MB

▨ Free space: 21,391,482,880 bytes 19.9 GB

Capacity: 21,455,958,016 bytes 19.9 GB

Drive F:

□ Compress this drive to save disk space

☑ Allow files on this drive to have contents indexed in addition to file properties

2.2 Command Prompt Commands to Copy Files and Folders

In this category, I will discuss three commands: COPY, XCOPY, and ROBOCOPY.

COPY

This command copies one or more files to another location.

COPY Syntax

```
COPY [/D] [/V] [/N] [/Y | /-Y] [/Z] [/L] [/A | /B ] source [/A | /B] [+ source [/A | /B] [+ …]]
[destination [/A | /B]]
```

Like some command prompt commands I discussed earlier in this guide, the COPY command has a lot of parameters. But I will only discuss the most relevant parameters. Below is a shortened syntax.

```
COPY <Source> <Destination> [/Y]
COPY <Source> <Destination> /-Y
```

COPY Parameters

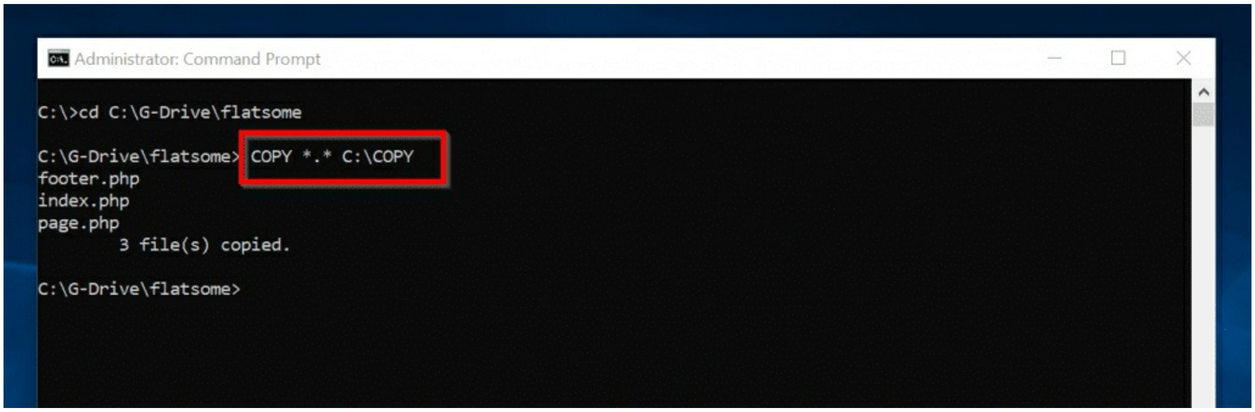
Parameters	Description
<Source>	Specifies the file or files to be copied.
<destination>	Specifies the directory and/or filename for the new file(s).
/Y	Suppresses prompting you to confirm whether you want to overwrite an existing destination file or not.
/-Y	Causes prompting to confirm you want to overwrite an existing destination file.

COPY Examples

To copy all files in the current directory to a new directory, use the command below:

```
COPY *.* C:\COPY
```

Note
In the last command, C:\COPY is the destination directory



```
C:\>cd C:\G-Drive\flatsome

C:\G-Drive\flatsome>COPY *.* C:\COPY
footer.php
index.php
page.php
        3 file(s) copied.

C:\G-Drive\flatsome>
```

XCOPY

Copies files and directories, including sub-directories. **XCOPY** has more advanced features than **COPY**.

XCOPY Syntax

Full syntax

```
XCOPY source [destination] [/A | /M] [/D[:date]] [/P] [/S [/E]] [/V] [/W] [/C] [/I] [/Q] [/F] [/L] [/G] [/H] [/R] [/T] [/U] [/K] [/N] [/O] [/X] [/Y] [/-Y] [/Z] [/B] [/J] [/EXCLUDE:file1[+file2][+file3]…]
```

Shortened version with mostly used parameters

```
XCOPY source [destination] [/A] [/M] [/D:m-d-y] [/EXCLUDE:file1[+file2][+file3]…] [/S] [/E] [/C] [/Y] [/-Y]
```

Tip
To see a full list of all XCOPY parameters and what they do, run the command *HELP XCOPY*.

XCOPY Parameters

Parameters	**Description**
source	Specifies the file(s) to copy.
destination	Specifies the location and/or name of new files.
/A	Copies only files with the archive attribute set, doesn't change the attribute.
/M	Copies only files with the archive attribute set, turns off the archive attribute.
/D:m-d-y	Copies files changed on or after the specified date. If no date is given, copies only those files whose source time is newer than the destination time.
/EXCLUDE:file1[+file2][+file3]…	Specifies a string defining files to be excluded from being copied.
/S	Copies directories and sub-directories except for empty ones.
/E	Copies directories and sub-directories, including empty ones.
/C	Ignores errors and continues copying.
	Stops XCOPY prompting you to confirm for the

/Y	destination file to be overwritten.
/-Y	/-Y parameter makes XCOPY prompt confirmation for an existing destination file to be overwritten.

XCOPY Examples

If you automatically update a report, you may want to copy report files that are have changed since a particular date. The command below will copy all files that have changed since May 20, 2019.

```
XCOPY  \BackReports \Current /D:05-20-2019
```

ROBOCOPY

This is an even more advanced copy command.

ROBOCOPY Syntax

```
ROBOCOPY <source> <destination> [file [file]…] [options]
```

ROBOCOPY Parameters

Parameters	**Description**
<Source>	Used to define the path to the source folder.
<Destination>	This is the path to the destination folder or directory.
[file [file]	Specifies the file or files to be copied. Wildcard characters (* or ?) are supported.
[options]	Specifies options to be used with the ROBOCOPY command.

For a full list of all parameters, open a command prompt and run the command below;

```
HELP ROBOCOPY
```

The command will return detailed information about ROBOCOPY. Alternatively, click the ROBOCOPY link to read about the command.

2.3 Command Prompt Commands for System Administration and Reporting

These set of command prompt commands are useful for advanced system administration. Here they are.

SCHTASKS

This command is used to **create**, **delete**, **query**, **change**, **run** or **end** scheduled tasks on a local or remote system. To run **SCHTASKS** you require administrator privilege.

SCHTASKS Syntax

```
SCHTASKS /parameter [arguments]
```

SCHTASKS Parameter Lists

Parameters	Description
/Create	Use this parameter to create a new scheduled task.
/Delete	Opposite of /Create, the /Delete parameter deletes an existing scheduled task(s).
/Query	Lists all available scheduled tasks.
/Run	This switch runs a specified scheduled task.
/Change	Changes the properties of a specified scheduled task
/End	Ends a currently running scheduled task
/ShowSid	Shows the security identifier corresponding to a scheduled task name.

To get help with how to use a parameter, enter SCHTASKS followed by the parameter. Then end with "/ ?". For example, to learn how to use the /Create parameter, run the command below:

```
SCHTASKS /Create /?
```

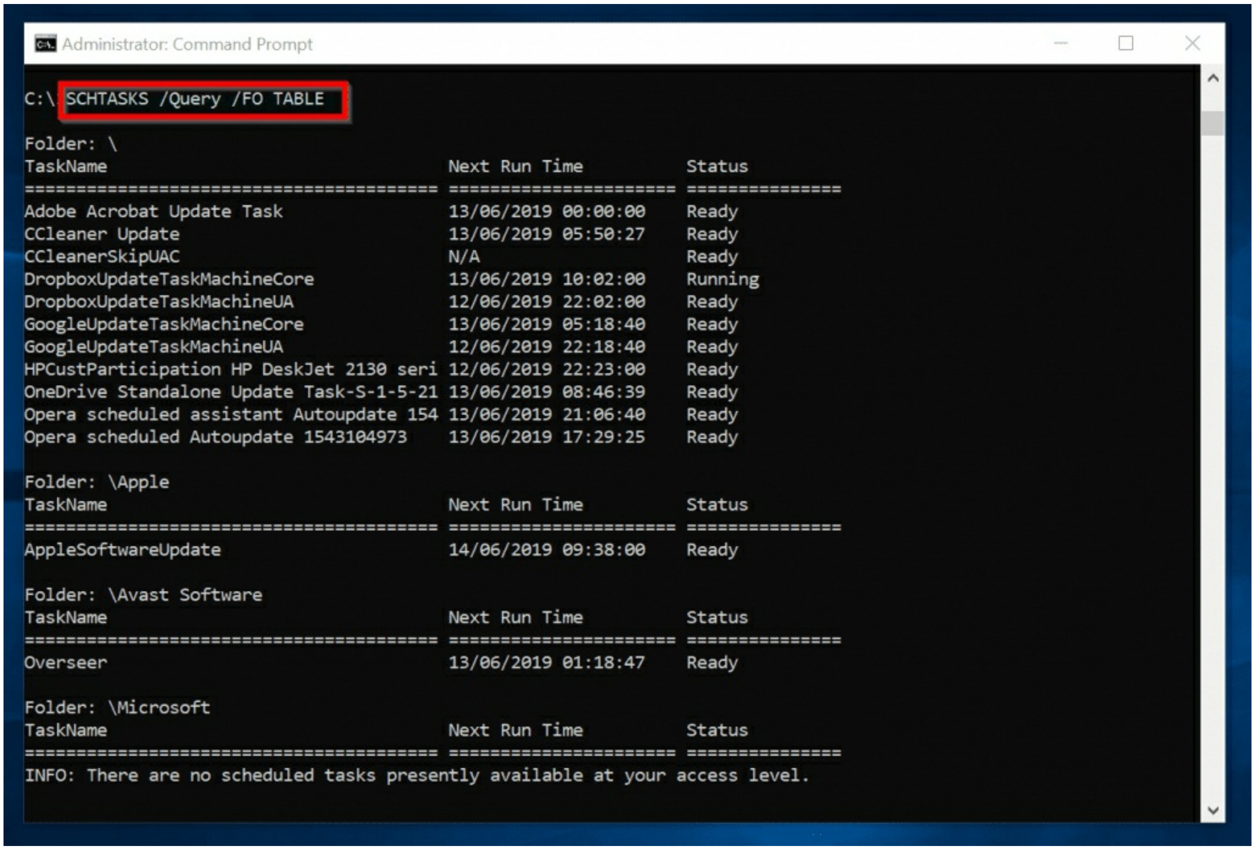
This will give you a full list of all the [arguments] for the /Create parameter and how to use them.

SCHTASKS Examples

To get a full list of all the scheduled tasks on your computer, use this command:

```
SCHTASKS /Query /FO TABLE
```

The result…s



```
C:\ SCHTASKS /Query /FO TABLE

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Adobe Acrobat Update Task                13/06/2019 00:00:00    Ready
CCleaner Update                          13/06/2019 05:50:27    Ready
CCleanerSkipUAC                          N/A                    Ready
DropboxUpdateTaskMachineCore             13/06/2019 10:02:00    Running
DropboxUpdateTaskMachineUA               12/06/2019 22:02:00    Ready
GoogleUpdateTaskMachineCore              13/06/2019 05:18:40    Ready
GoogleUpdateTaskMachineUA                12/06/2019 22:18:40    Ready
HPCustParticipation HP DeskJet 2130 seri 12/06/2019 22:23:00    Ready
OneDrive Standalone Update Task-S-1-5-21 13/06/2019 08:46:39    Ready
Opera scheduled assistant Autoupdate 154 13/06/2019 21:06:40    Ready
Opera scheduled Autoupdate 1543104973    13/06/2019 17:29:25    Ready

Folder: \Apple
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
AppleSoftwareUpdate                      14/06/2019 09:38:00    Ready

Folder: \Avast Software
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Overseer                                 13/06/2019 01:18:47    Ready

Folder: \Microsoft
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
INFO: There are no scheduled tasks presently available at your access level.
```

SYSTEMINFO

This is one of the command prompt commands that I use very often. SYSTEMINFO displays operating system configuration information for a local or remote computer. The information displayed includes service pack and patch levels.

SYSTEMINFO Syntax

```
SYSTEMINFO [/S system [/U username [/P [password]]]] [/FO format] [/NH]
```

SYSTEMINFO Parameters

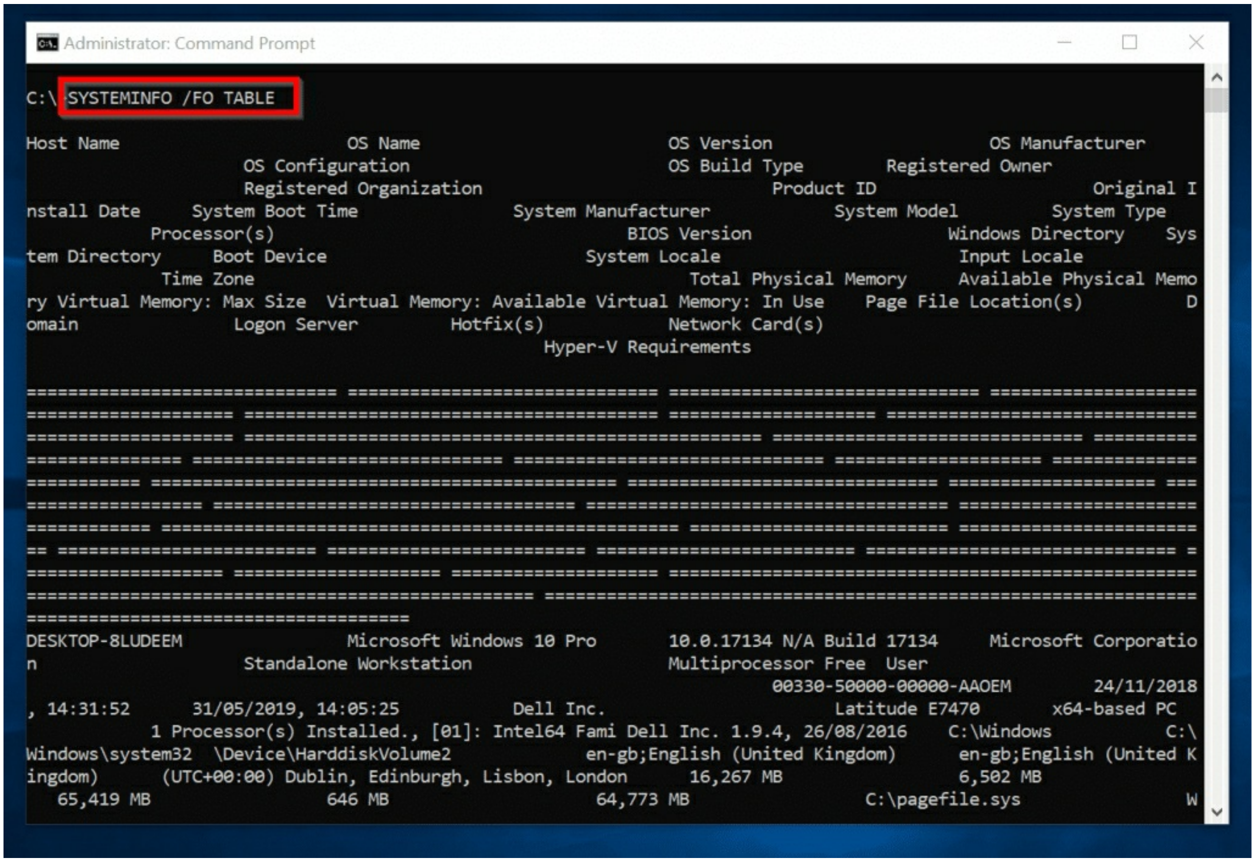
Parameters	**Description**
/S system	Used to specify a remote computer to connect to.
/U username	Specifies a user with admin privilege to connect to the remote computer and run commands.
/P [password]	The password for the username specified with the /U parameter
/FO format	Specifies the format in which the output is to be displayed. Acceptable values: TABLE, LIST or CSV.
/NH	If used, the output will not display the "Column Header" in the output. /NH is only valid if /FO is used and TABLE and CSV formats are specified.

SYSTEMINFO Examples

To display system information for your computer and display output in a table, use this SYSTEMINFO command:

```
SYSTEMINFO /FO TABLE
```

The output is not very readable!

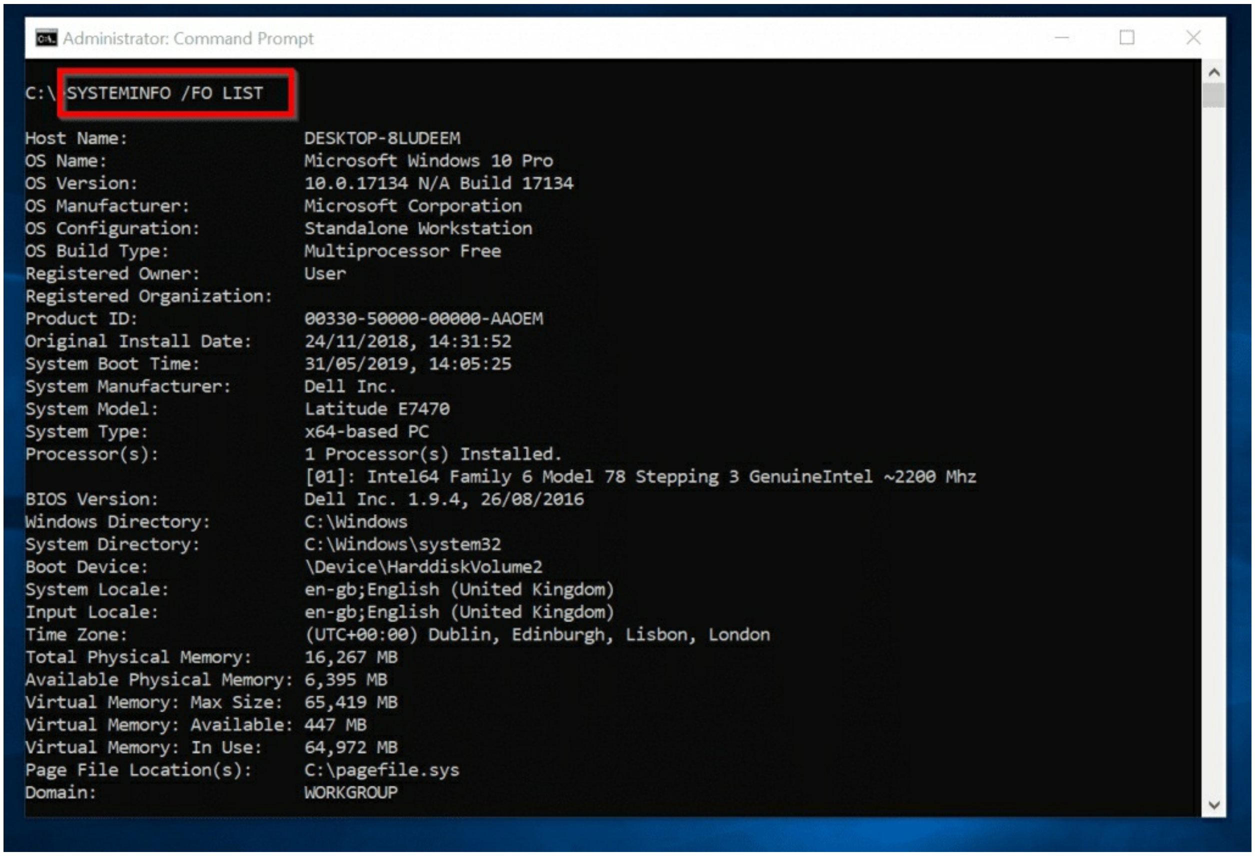


```
C:\ SYSTEMINFO /FO TABLE

Host Name                      OS Name                        OS Version                     OS Manufacturer
                     OS Configuration                         OS Build Type        Registered Owner
                     Registered Organization                            Product ID                     Original I
nstall Date     System Boot Time               System Manufacturer            System Model         System Type
            Processor(s)                                  BIOS Version                   Windows Directory    Sys
tem Directory     Boot Device                         System Locale                       Input Locale
             Time Zone                                          Total Physical Memory     Available Physical Memo
ry Virtual Memory: Max Size  Virtual Memory: Available Virtual Memory: In Use    Page File Location(s)          D
omain               Logon Server         Hotfix(s)            Network Card(s)
                                                  Hyper-V Requirements

============================== ============================== ============================== ====================
==================== ======================================== ==================== ==============================
======================================================================= =============================== =========
=============== ============================== ============================== ==================== ==============
=========== ============================================= ============================== ==================== ===
================= =================================== =================================== =======================
============ ================================================== ========================= =======================
== ========================= ========================= ========================= ============================== =
=================== ==================== ==================== ===================================================
================================================= ===============================================================
=====================================
DESKTOP-8LUDEEM                Microsoft Windows 10 Pro       10.0.17134 N/A Build 17134     Microsoft Corporatio
n                    Standalone Workstation                   Multiprocessor Free  User
                                                                        00330-50000-00000-AAOEM        24/11/2018
, 14:31:52      31/05/2019, 14:05:25           Dell Inc.                      Latitude E7470       x64-based PC
            1 Processor(s) Installed., [01]: Intel64 Fami Dell Inc. 1.9.4, 26/08/2016    C:\Windows           C:\
Windows\system32  \Device\HarddiskVolume2             en-gb;English (United Kingdom)      en-gb;English (United K
ingdom)      (UTC+00:00) Dublin, Edinburgh, Lisbon, London      16,267 MB                 6,502 MB
   65,419 MB                 646 MB                   64,773 MB                C:\pagefile.sys                W
```

I may also display the result in a LIST format:

SYSTEMINFO /FO LIST

Gives a better result



```
C:\ SYSTEMINFO /FO LIST

Host Name:                 DESKTOP-8LUDEEM
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.17134 N/A Build 17134
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          User
Registered Organization:
Product ID:                00330-50000-00000-AAOEM
Original Install Date:     24/11/2018, 14:31:52
System Boot Time:          31/05/2019, 14:05:25
System Manufacturer:       Dell Inc.
System Model:              Latitude E7470
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 78 Stepping 3 GenuineIntel ~2200 Mhz
BIOS Version:              Dell Inc. 1.9.4, 26/08/2016
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-gb;English (United Kingdom)
Input Locale:              en-gb;English (United Kingdom)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     16,267 MB
Available Physical Memory: 6,395 MB
Virtual Memory: Max Size:  65,419 MB
Virtual Memory: Available: 447 MB
Virtual Memory: In Use:    64,972 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
```

TASKLIST

Displays a list of all currently running processes on the local computer. It can also display processes on a remote computer.

TASKLIST Syntax

TASKLIST [/S system [/U username [/P [password]]]] [/M [module] | /SVC | /V] [/FI filter] [/FO format] [/NH]

TASKLIST Parameters

The description of the parameters: /S system, /U username, /P [password], /FO format and /NH are the same for the same parameters in the SYSTEMINFO command. Please read about this parameters in SYSTEMINFO (opens in a new window/tab).

The remaining parameters for TASKLIST are described in the table below:

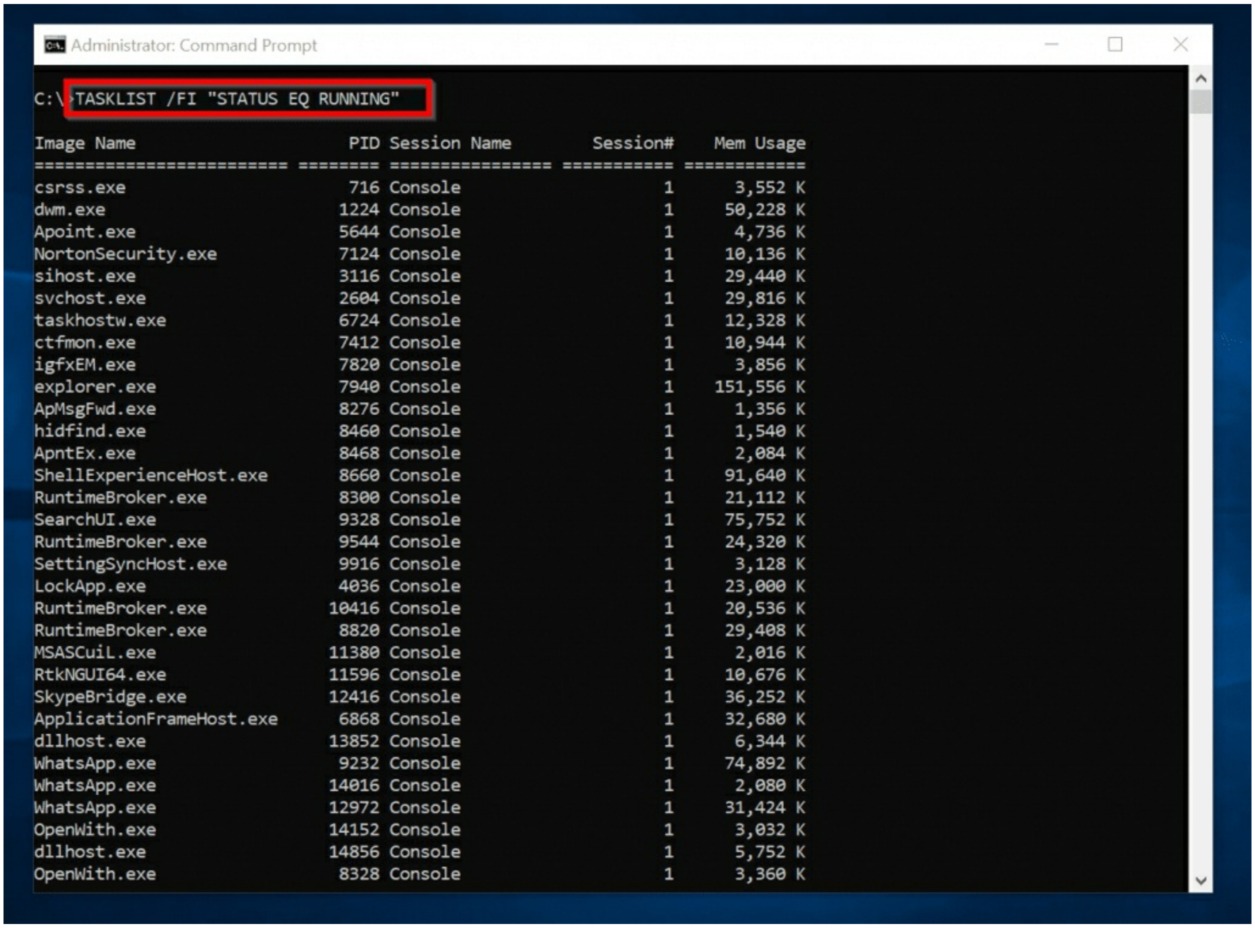
Parameters	Description
/M [module]	Lists all tasks currently running processes using the given exe/dll name. If the module name is not specified all loaded modules are displayed.

/SVC	Displays services hosted in each process.
/V	Displays verbose task information - shows the tasks as they are being displayed.
/FI filter	Displays a set of tasks that match the given criteria specified by the filter.

TASKLIST Examples

To display currently running processes on your computer, run the command below.

TASKLIST /FI "STATUS EQ RUNNING"

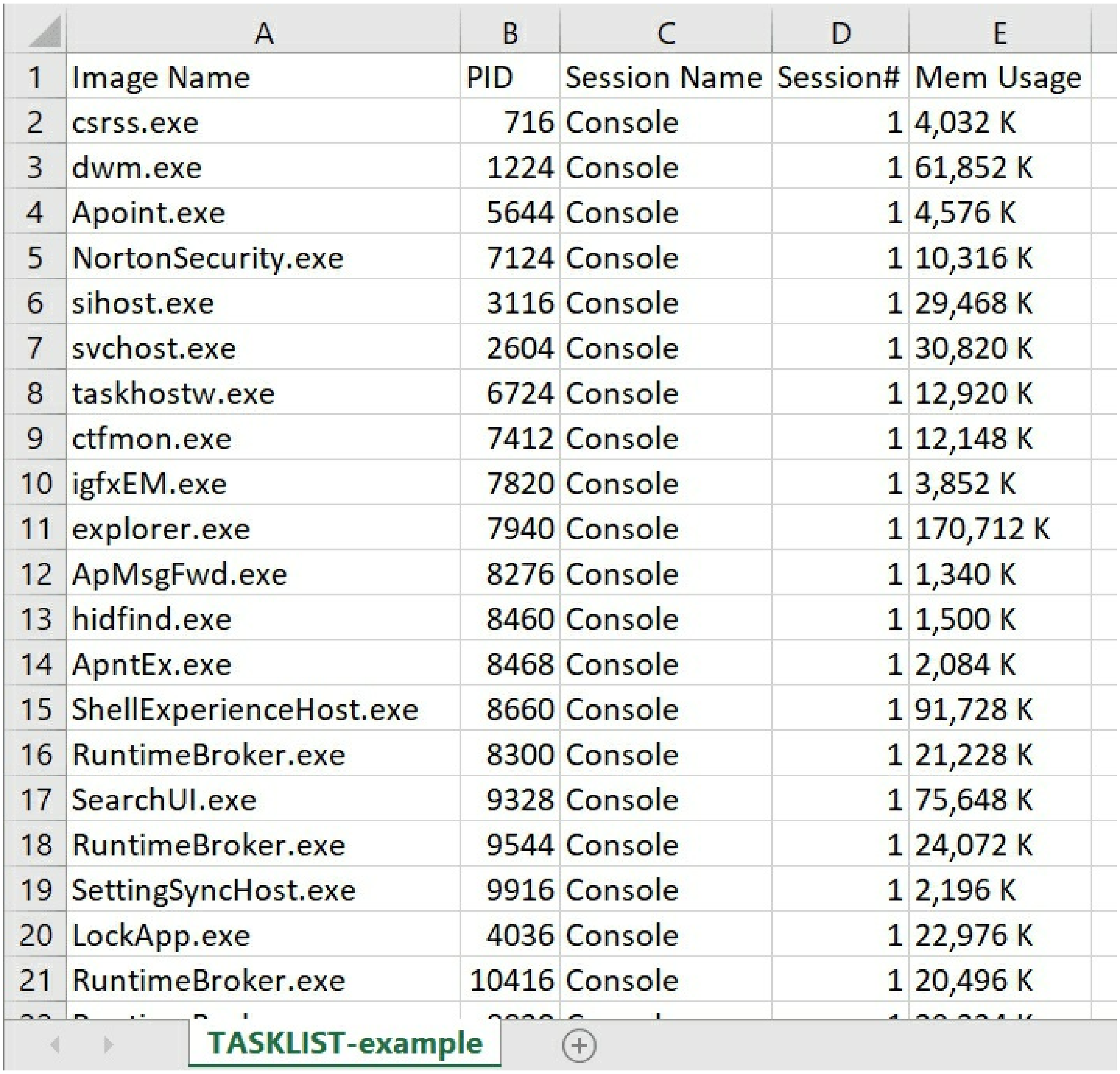


```
C:\>TASKLIST /FI "STATUS EQ RUNNING"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
csrss.exe                      716 Console                    1      3,552 K
dwm.exe                       1224 Console                    1     50,228 K
Apoint.exe                    5644 Console                    1      4,736 K
NortonSecurity.exe            7124 Console                    1     10,136 K
sihost.exe                    3116 Console                    1     29,440 K
svchost.exe                   2604 Console                    1     29,816 K
taskhostw.exe                 6724 Console                    1     12,328 K
ctfmon.exe                    7412 Console                    1     10,944 K
igfxEM.exe                    7820 Console                    1      3,856 K
explorer.exe                  7940 Console                    1    151,556 K
ApMsgFwd.exe                  8276 Console                    1      1,356 K
hidfind.exe                   8460 Console                    1      1,540 K
ApntEx.exe                    8468 Console                    1      2,084 K
ShellExperienceHost.exe       8660 Console                    1     91,640 K
RuntimeBroker.exe             8300 Console                    1     21,112 K
SearchUI.exe                  9328 Console                    1     75,752 K
RuntimeBroker.exe             9544 Console                    1     24,320 K
SettingSyncHost.exe           9916 Console                    1      3,128 K
LockApp.exe                   4036 Console                    1     23,000 K
RuntimeBroker.exe            10416 Console                    1     20,536 K
RuntimeBroker.exe             8820 Console                    1     29,408 K
MSASCuiL.exe                 11380 Console                    1      2,016 K
RtkNGUI64.exe                11596 Console                    1     10,676 K
SkypeBridge.exe              12416 Console                    1     36,252 K
ApplicationFrameHost.exe      6868 Console                    1     32,680 K
dllhost.exe                  13852 Console                    1      6,344 K
WhatsApp.exe                  9232 Console                    1     74,892 K
WhatsApp.exe                 14016 Console                    1      2,080 K
WhatsApp.exe                 12972 Console                    1     31,424 K
OpenWith.exe                 14152 Console                    1      3,032 K
dllhost.exe                  14856 Console                    1      5,752 K
OpenWith.exe                  8328 Console                    1      3,360 K
```

To export all running processes to CSV, use this command:

TASKLIST /FI "STATUS EQ RUNNING" /FO CSV > C:\G-Drive\flatsome\TASKLIST-csv

Here is what the CSV looks like



	A	B	C	D	E
1	Image Name	PID	Session Name	Session#	Mem Usage
2	csrss.exe	716	Console	1	4,032 K
3	dwm.exe	1224	Console	1	61,852 K
4	Apoint.exe	5644	Console	1	4,576 K
5	NortonSecurity.exe	7124	Console	1	10,316 K
6	sihost.exe	3116	Console	1	29,468 K
7	svchost.exe	2604	Console	1	30,820 K
8	taskhostw.exe	6724	Console	1	12,920 K
9	ctfmon.exe	7412	Console	1	12,148 K
10	igfxEM.exe	7820	Console	1	3,852 K
11	explorer.exe	7940	Console	1	170,712 K
12	ApMsgFwd.exe	8276	Console	1	1,340 K
13	hidfind.exe	8460	Console	1	1,500 K
14	ApntEx.exe	8468	Console	1	2,084 K
15	ShellExperienceHost.exe	8660	Console	1	91,728 K
16	RuntimeBroker.exe	8300	Console	1	21,228 K
17	SearchUI.exe	9328	Console	1	75,648 K
18	RuntimeBroker.exe	9544	Console	1	24,072 K
19	SettingSyncHost.exe	9916	Console	1	2,196 K
20	LockApp.exe	4036	Console	1	22,976 K
21	RuntimeBroker.exe	10416	Console	1	20,496 K

TASKKILL

Terminate tasks by process id (PID) or image name.

TASKKILL Syntax

TASKKILL [/S system [/U username [/P [password]]]] { [/FI filter] [/PID processid | /IM imagename] } [/T] [/F]

TASKKILL Parameters

Like TASKLIST, the description of the parameters: /S system, /U username and /P are the same for the same parameters in the SYSTEMINFO command. Please read about this parameter click SYSTEMINFO (opens in a new window/tab).

The parameter table below describes TASKKILL parameters that have not been described in this guide.

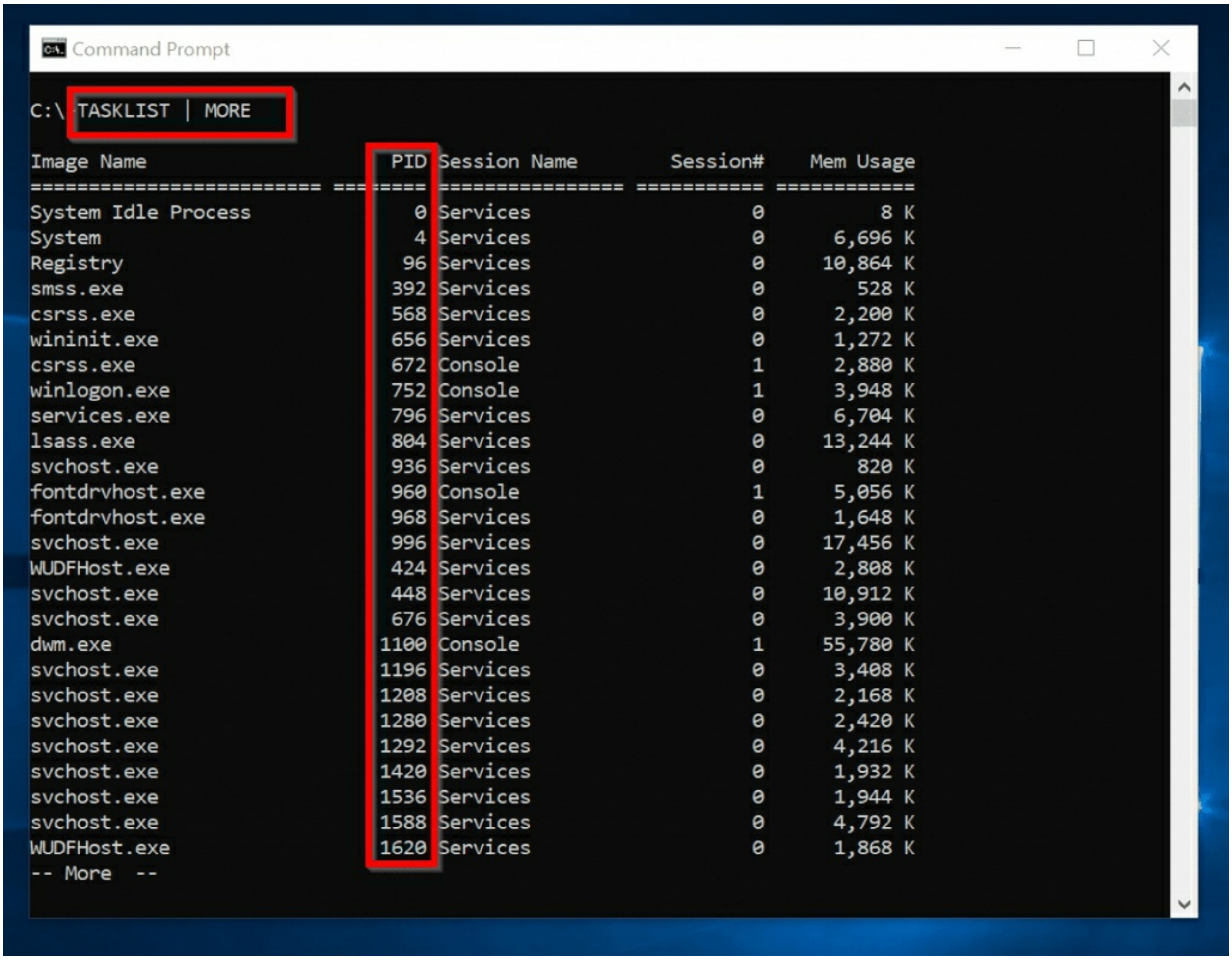
Parameters	Description
/FI filter	Used to apply a filter to select a set of tasks. Allowed filters: "*" _to be used. ex. imagename eq acme*_
/PID processid	Specifies the PID of the process to be terminated. You can use the TASKLIST command to get the PID of the process.
/IM imagename	Specifies the image name of the process to be terminated. You can use wildcard '*' to specify all tasks or image names.
/T	This parameter tells TASKKILL to terminate the specified process and any child processes started by the original process.
/F	If /F is used, it forcefully terminates the specified process.

Warning!
Use TASKKILL with caution as terminating certain processes could make your Operating System unstable. Specifically, be careful with using wildcard "*".

TASKKILL Examples

If you wish to terminate processes based on process ID, run the TASKLIST command and pipe it to the MORE command.

```
TASKLIST | MORE
```



```
C:\ TASKLIST | MORE

Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0      6,696 K
Registry                        96 Services                   0     10,864 K
smss.exe                       392 Services                   0        528 K
csrss.exe                      568 Services                   0      2,200 K
wininit.exe                    656 Services                   0      1,272 K
csrss.exe                      672 Console                    1      2,880 K
winlogon.exe                   752 Console                    1      3,948 K
services.exe                   796 Services                   0      6,704 K
lsass.exe                      804 Services                   0     13,244 K
svchost.exe                    936 Services                   0        820 K
fontdrvhost.exe                960 Console                    1      5,056 K
fontdrvhost.exe                968 Services                   0      1,648 K
svchost.exe                    996 Services                   0     17,456 K
WUDFHost.exe                   424 Services                   0      2,808 K
svchost.exe                    448 Services                   0     10,912 K
svchost.exe                    676 Services                   0      3,900 K
dwm.exe                       1100 Console                    1     55,780 K
svchost.exe                   1196 Services                   0      3,408 K
svchost.exe                   1208 Services                   0      2,168 K
svchost.exe                   1280 Services                   0      2,420 K
svchost.exe                   1292 Services                   0      4,216 K
svchost.exe                   1420 Services                   0      1,932 K
svchost.exe                   1536 Services                   0      1,944 K
svchost.exe                   1588 Services                   0      4,792 K
WUDFHost.exe                  1620 Services                   0      1,868 K
-- More  --
```

To terminate processes with IDs 960, 996 and 936, use the command below

TASKKILL /PID 960 /PID 996 /PID 936

SHUTDOWN

Used to shut down or restart a local or remote computer.

SHUTDOWN Syntax

SHUTDOWN [/I | /L | /S | /SG | /R | /G | /A | /P | /H | /E | /O] [/Hybrid] [/Soft] [/FW] [/F] [/M \\Computer] [/T xxx]

SHUTDOWN Parameters

Parameters	**Description**
/I	The /I switch displays Remote Shutdown GUI dialogue with options to specify remote computers to shutdown. The /I switch must be the first option in a SHUTDOWN command. See SHUTDOWN examples below.

/L	Logs the computer off. This cannot be used with /M or /D options.
/S	Shutdowns the computer.
/SG	Shutdown the computer. On the next boot, restart any registered applications.
/R	Shutdown and restart the computer.
/G	Full shutdown and restart the computer. After the system is rebooted, 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. It can be used with /D and /F parameters.
/H	Hibernate the local computer. It can be used with the /F switch.
/E	Document the reason for an unexpected shutdown of a computer.
/O	Go to the advanced boot options menu and restart the computer. Must be used with /R option.
/Hybrid	Performs a shutdown of the computer and prepares it for a fast startup. Must be used with /S switch.
/FW	Combine with a shutdown option (/S) to cause the next boot to go to the firmware user interface.
/F	Force running applications to close without forewarning users. The /F parameter is implied when a value greater than 0 is specified for the /T parameter.
/M \\Computer	Specify a target remote computer.
/T xxx	Set the time-out period before shutdown to xxx seconds. The default is 30s with a max value of 315360000s (10 years).

Important Information

I left out ***/D [P\|U:]xx:yy]*** *and* ***/C ["comment"]*** *parameters as you may not need them often.*

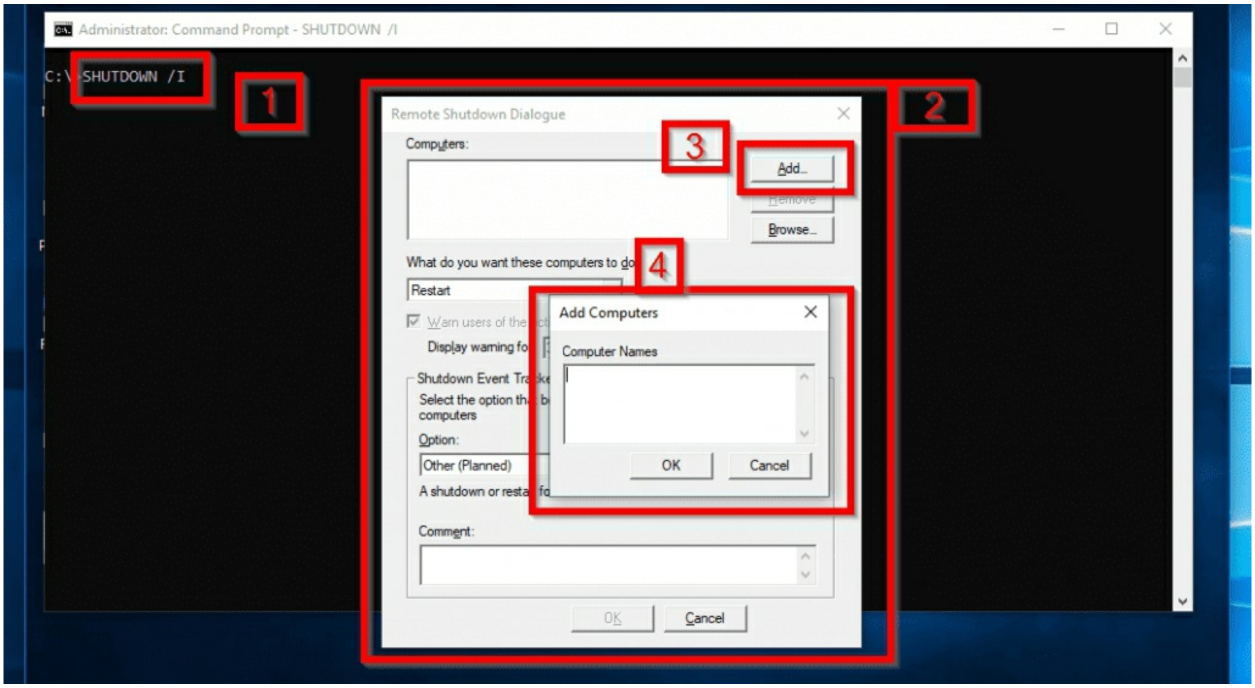
Tip

If you run SHUTDOWN without specifying any parameter, it will display *help. Running SHUTDOWN without specifying any parameter is like typing "SHUTDOWN /?".*

SHUTDOWN Examples

To display a dialogue box with options to shutdown specified computers, simply use SHUTDOWN with /I switch:

SHUTDOWN /I



```
C:\>SHUTDOWN /I
```

What do you want these computers to do: Restart

Option: Other (Planned)

When you execute SHUTDOWN /I [1], the Remote Shutdown Dialogue GUI opens [2]. To add computers, click **Add** [3], this opens the Computer Names box [4]. When you finish adding the computers, click Ok. Then Ok to shut them down.

DRIVERQUERY

This is another very important but often ignored command prompt commands. An administrator can use DRIVERQUERY to display a list of installed device drivers on a local or remote computer.

DRIVERQUERY Syntax

```
DRIVERQUERY [/S system [/U username [/P [password]]]] [/FO format] [/NH] [/SI] [/V]
```

DRIVERQUERY Parameters

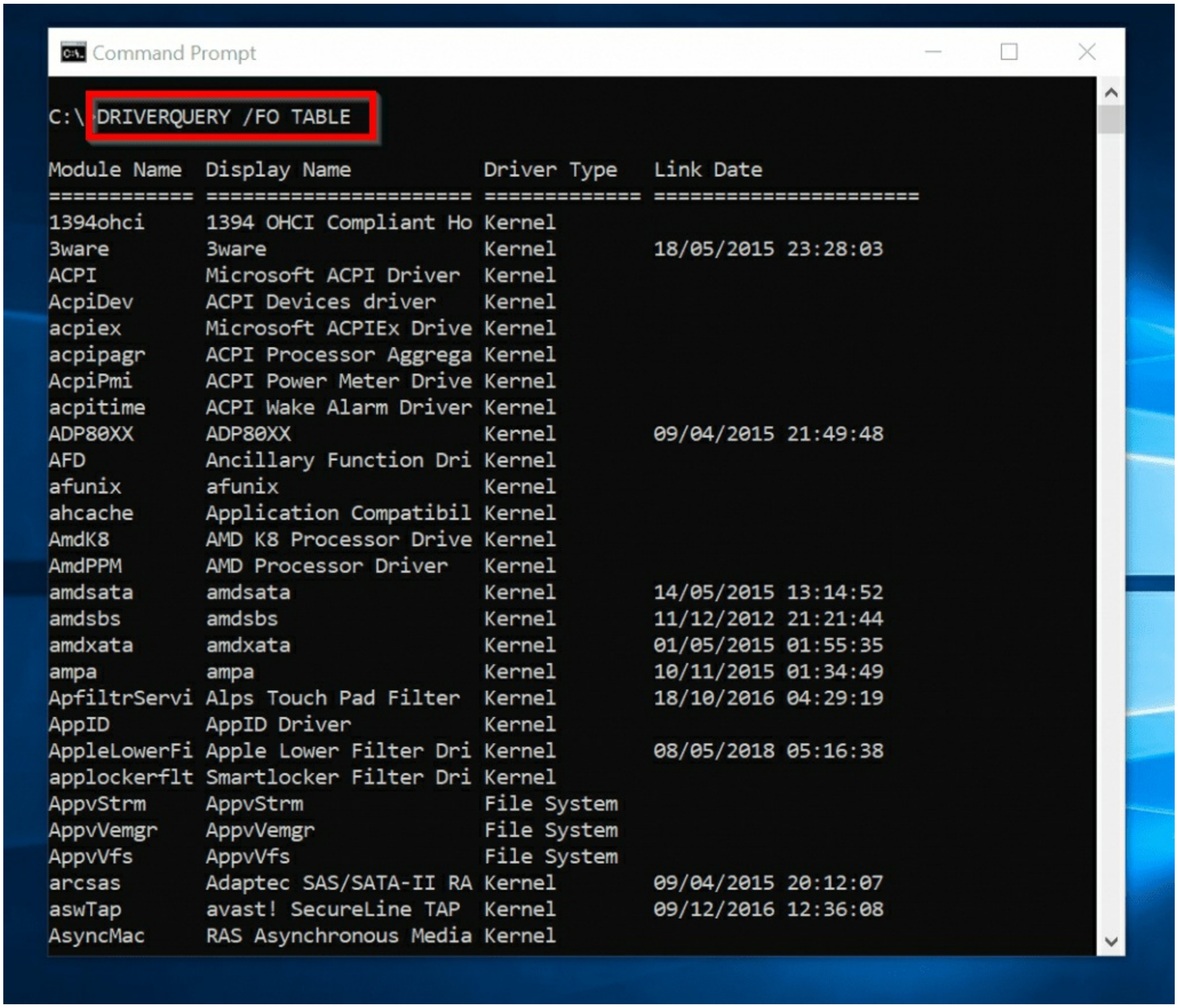
/S	Specifies a remote computer to connect to.
/U username	Used to specify a user name with permission to connect to the remote computer.
/P password	Specifies the password for the user above.
/FO format	Specifies the type of output to display. Acceptable formats: "TABLE", "LIST" or "CSV", without the quotes.
/NH	Removes the column headers from the output.
/SI	Provides information about signed drivers.
/V	Displays verbose output. Not valid for signed drivers.

DRIVERQUERY Examples

To list all drivers on your computer and display the result in a tabular format, use the command below:

```
DRIVERQUERY /FO TABLE
```

Here is the result…

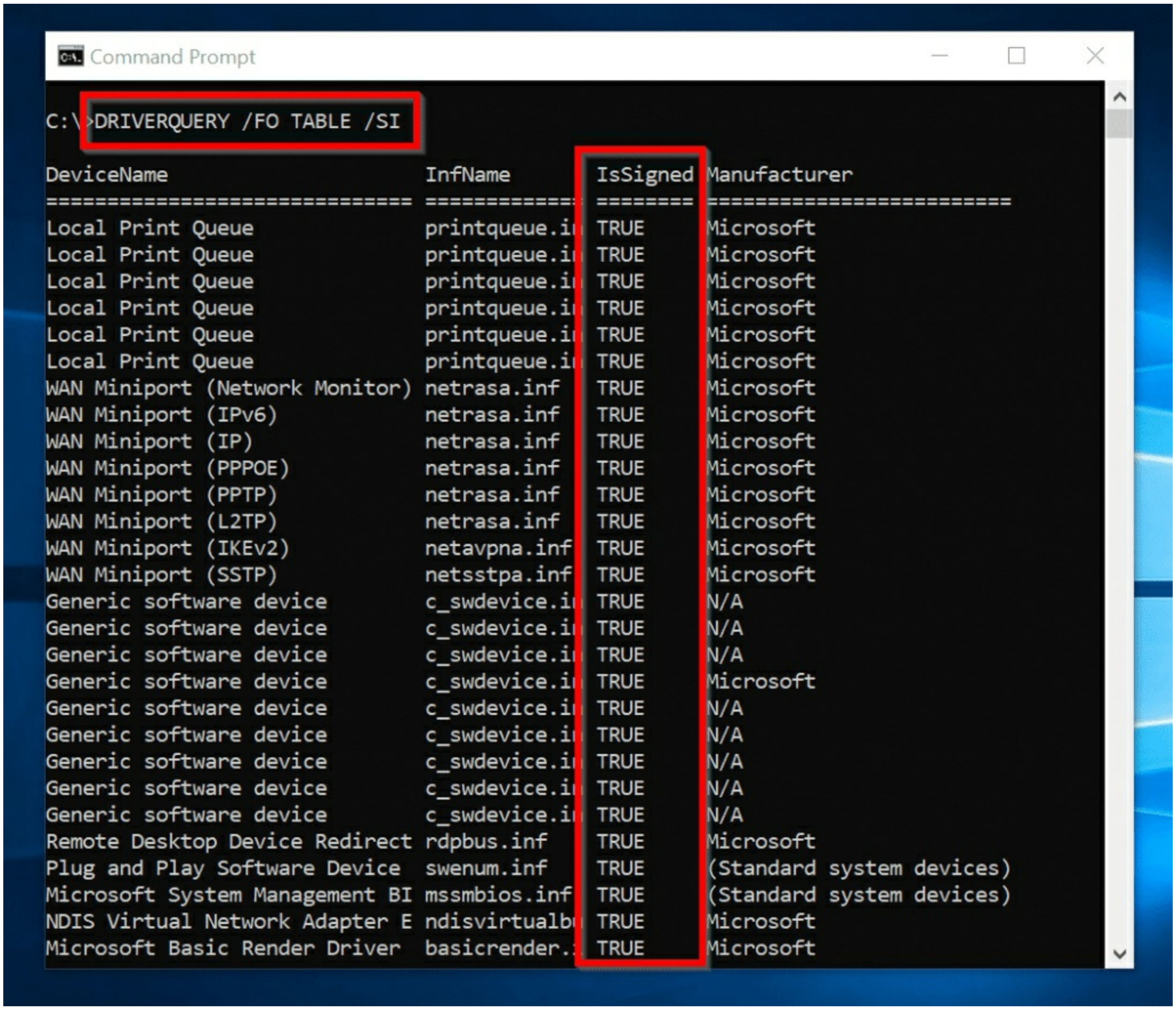


```
C:\ DRIVERQUERY /FO TABLE

Module Name  Display Name           Driver Type   Link Date
============ ====================== ============= ======================
1394ohci     1394 OHCI Compliant Ho Kernel
3ware        3ware                  Kernel        18/05/2015 23:28:03
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
ADP80XX      ADP80XX                Kernel        09/04/2015 21:49:48
AFD          Ancillary Function Dri Kernel
afunix       afunix                 Kernel
ahcache      Application Compatibil Kernel
AmdK8        AMD K8 Processor Drive Kernel
AmdPPM       AMD Processor Driver   Kernel
amdsata      amdsata                Kernel        14/05/2015 13:14:52
amdsbs       amdsbs                 Kernel        11/12/2012 21:21:44
amdxata      amdxata                Kernel        01/05/2015 01:55:35
ampa         ampa                   Kernel        10/11/2015 01:34:49
ApfiltrServi Alps Touch Pad Filter  Kernel        18/10/2016 04:29:19
AppID        AppID Driver           Kernel
AppleLowerFi Apple Lower Filter Dri Kernel        08/05/2018 05:16:38
applockerflt Smartlocker Filter Dri Kernel
AppvStrm     AppvStrm               File System
AppvVemgr    AppvVemgr              File System
AppvVfs      AppvVfs                File System
arcsas       Adaptec SAS/SATA-II RA Kernel        09/04/2015 20:12:07
aswTap       avast! SecureLine TAP  Kernel        09/12/2016 12:36:08
AsyncMac     RAS Asynchronous Media Kernel
```

To add the information whether a driver is signed or not, include /SI switch to the previous command:

DRIVERQUERY /FO TABLE /SI

A new column, "IsSigned" is now included.



```
C:\>DRIVERQUERY /FO TABLE /SI

DeviceName                     InfName       IsSigned Manufacturer
============================== ============= ======== =========================
Local Print Queue              printqueue.in TRUE     Microsoft
Local Print Queue              printqueue.in TRUE     Microsoft
Local Print Queue              printqueue.in TRUE     Microsoft
Local Print Queue              printqueue.in TRUE     Microsoft
Local Print Queue              printqueue.in TRUE     Microsoft
Local Print Queue              printqueue.in TRUE     Microsoft
WAN Miniport (Network Monitor) netrasa.inf   TRUE     Microsoft
WAN Miniport (IPv6)            netrasa.inf   TRUE     Microsoft
WAN Miniport (IP)              netrasa.inf   TRUE     Microsoft
WAN Miniport (PPPOE)           netrasa.inf   TRUE     Microsoft
WAN Miniport (PPTP)            netrasa.inf   TRUE     Microsoft
WAN Miniport (L2TP)            netrasa.inf   TRUE     Microsoft
WAN Miniport (IKEv2)           netavpna.inf  TRUE     Microsoft
WAN Miniport (SSTP)            netsstpa.inf  TRUE     Microsoft
Generic software device        c_swdevice.in TRUE     N/A
Generic software device        c_swdevice.in TRUE     N/A
Generic software device        c_swdevice.in TRUE     N/A
Generic software device        c_swdevice.in TRUE     Microsoft
Generic software device        c_swdevice.in TRUE     N/A
Generic software device        c_swdevice.in TRUE     N/A
Generic software device        c_swdevice.in TRUE     N/A
Generic software device        c_swdevice.in TRUE     N/A
Generic software device        c_swdevice.in TRUE     N/A
Remote Desktop Device Redirect rdpbus.inf    TRUE     Microsoft
Plug and Play Software Device  swenum.inf    TRUE     (Standard system devices)
Microsoft System Management BI mssmbios.inf  TRUE     (Standard system devices)
NDIS Virtual Network Adapter E ndisvirtualbu TRUE     Microsoft
Microsoft Basic Render Driver  basicrender.i TRUE     Microsoft
```

Tip

In the above result, if IsSigned is FALSE, it means the driver is NOT signed.

2.4 Command Prompt Commands for Managing Files and Folders

These sets of command prompt commands are used to rename, move or delete files and folders.

RENAME (REN)

Renames a file or files. The short version of the command is REN.

RENAME Syntax

RENAME [drive:][path] filename1 filename2.

REN [drive:][path] filename1 filename2.

Tip

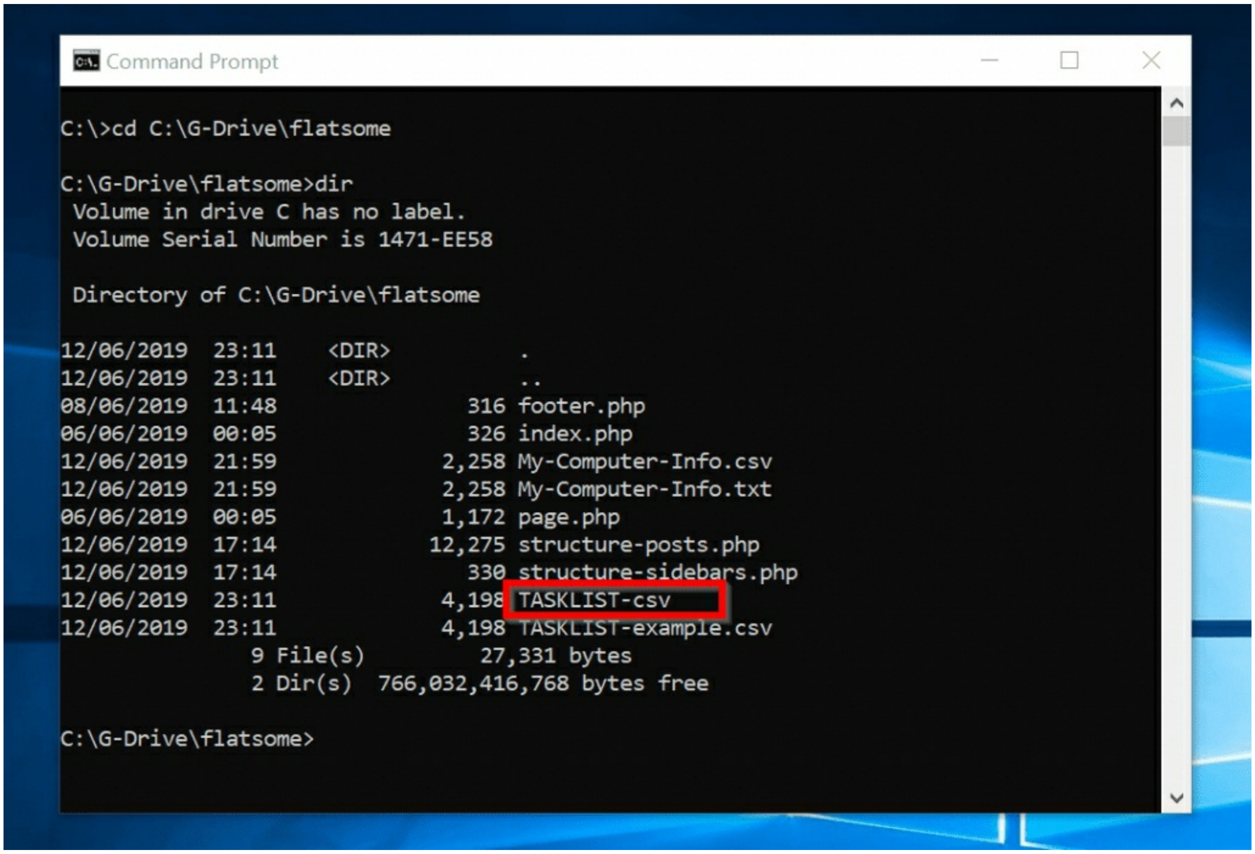
RENAME command does not allow you to specify a new drive or path for your destination file.

RENAME Parameters

Parameters	Description
[drive:] [path]filename1	Specifies the location and name of the file or set of files you want to rename. *FileName1* can include wildcard characters (* and ?).
filename2	The new name of the file

RENAME Examples

In the image below, I want to rename the file "TASKLIST-csv" to "New-CSV"

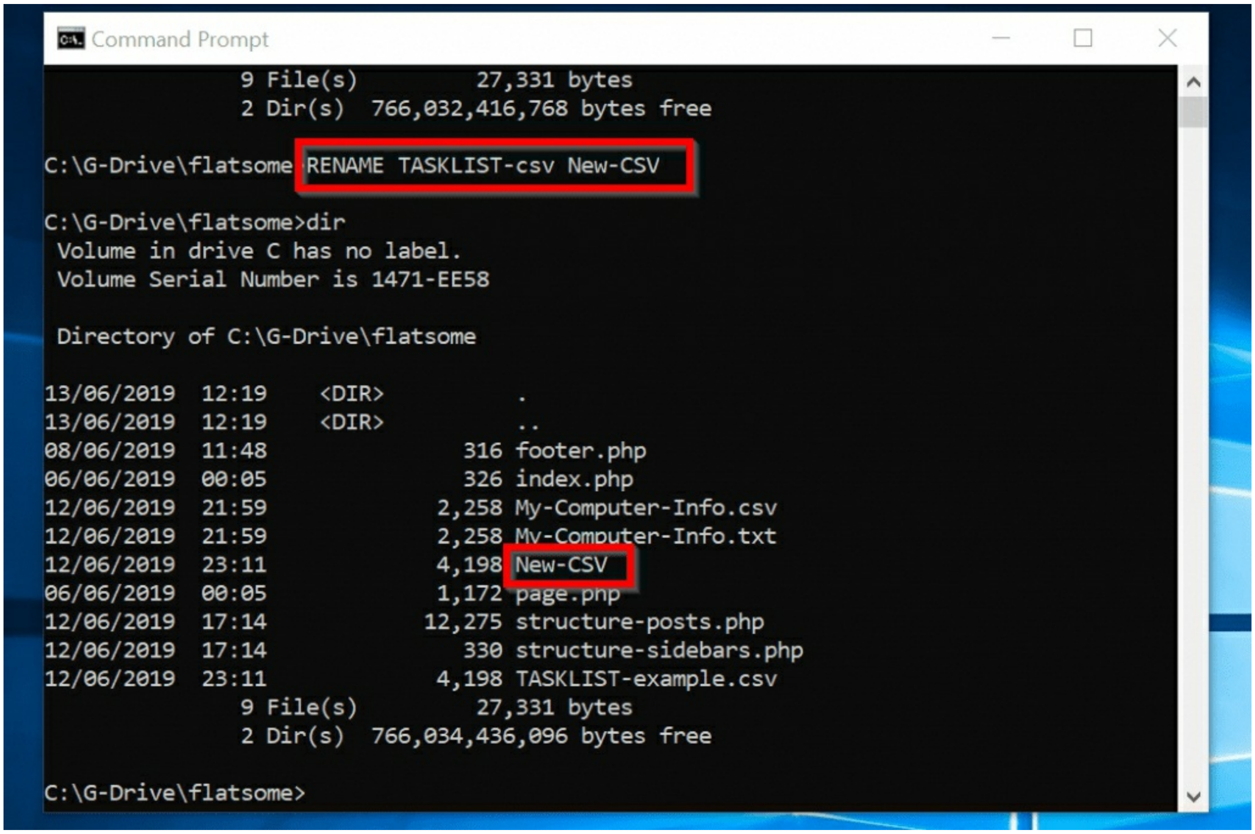


```
C:\>cd C:\G-Drive\flatsome

C:\G-Drive\flatsome>dir
 Volume in drive C has no label.
 Volume Serial Number is 1471-EE58

 Directory of C:\G-Drive\flatsome

12/06/2019  23:11    <DIR>          .
12/06/2019  23:11    <DIR>          ..
08/06/2019  11:48               316 footer.php
06/06/2019  00:05               326 index.php
12/06/2019  21:59             2,258 My-Computer-Info.csv
12/06/2019  21:59             2,258 My-Computer-Info.txt
06/06/2019  00:05             1,172 page.php
12/06/2019  17:14            12,275 structure-posts.php
12/06/2019  17:14               330 structure-sidebars.php
12/06/2019  23:11             4,198 TASKLIST-csv
12/06/2019  23:11             4,198 TASKLIST-example.csv
               9 File(s)         27,331 bytes
               2 Dir(s)  766,032,416,768 bytes free

C:\G-Drive\flatsome>
```

Here is the command I used:

```
RENAME TASKLIST-csv New-CSV
```

Here is the result:



```
               9 File(s)         27,331 bytes
               2 Dir(s)  766,032,416,768 bytes free

C:\G-Drive\flatsome>RENAME TASKLIST-csv New-CSV

C:\G-Drive\flatsome>dir
 Volume in drive C has no label.
 Volume Serial Number is 1471-EE58

 Directory of C:\G-Drive\flatsome

13/06/2019  12:19    <DIR>          .
13/06/2019  12:19    <DIR>          ..
08/06/2019  11:48               316 footer.php
06/06/2019  00:05               326 index.php
12/06/2019  21:59             2,258 My-Computer-Info.csv
12/06/2019  21:59             2,258 My-Computer-Info.txt
12/06/2019  23:11             4,198 New-CSV
06/06/2019  00:05             1,172 page.php
12/06/2019  17:14            12,275 structure-posts.php
12/06/2019  17:14               330 structure-sidebars.php
12/06/2019  23:11             4,198 TASKLIST-example.csv
               9 File(s)         27,331 bytes
               2 Dir(s)  766,034,436,096 bytes free

C:\G-Drive\flatsome>
```

MKDIR (MD)

Creates a directory or folder. The short version is MD.

MKDIR Syntax

MKDIR [drive:]path
MD [drive:]path

MKDIR Parameters

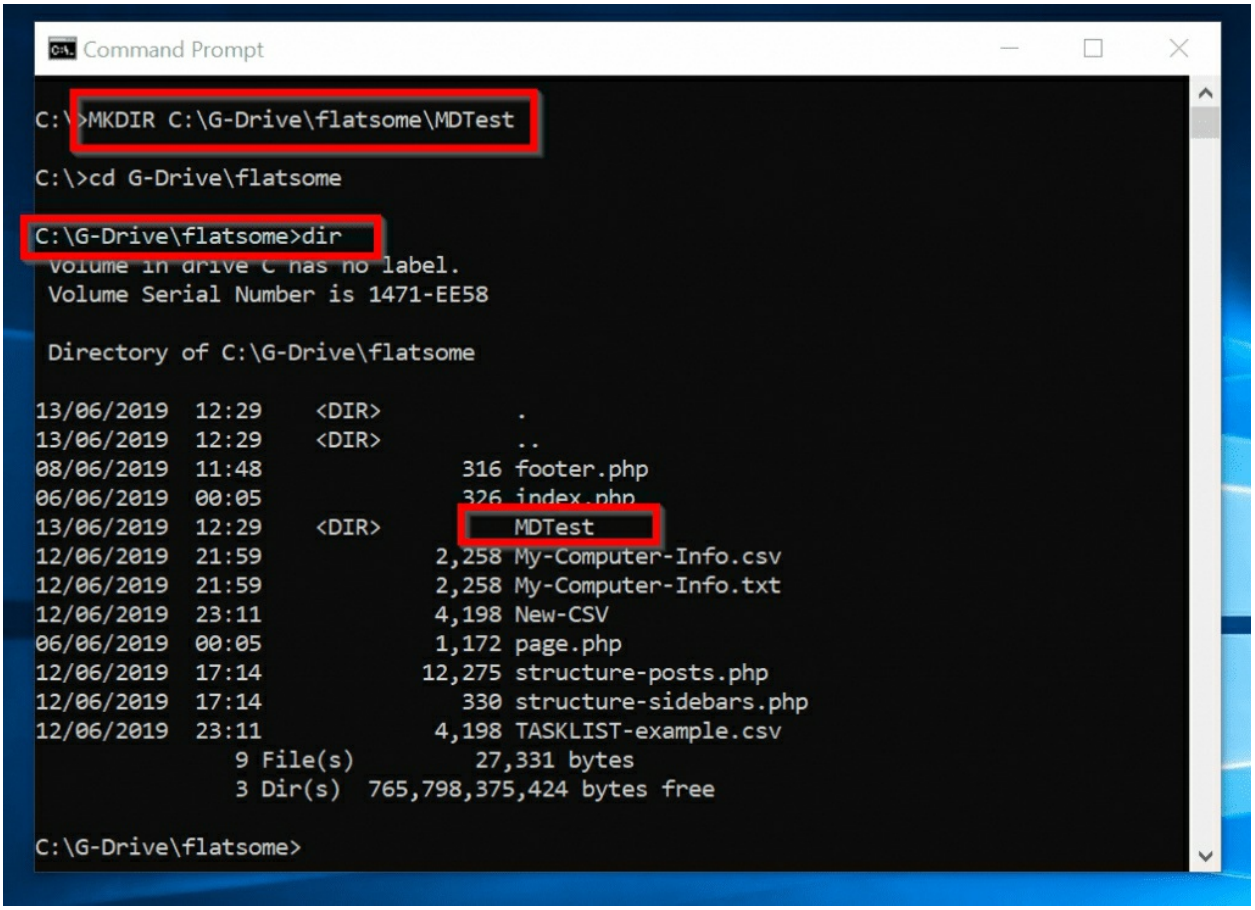
Parameters	Description
[drive:]	Specifies the drive on which you want to create the new directory.
path	This is a required parameter. It specifies the name and location of the new directory. The maximum length of any single path is determined by the file system (FAT, FAT32 or NTFS).

MKDIR Examples

To create a folder called MDTest in the path "C:\G-Drive\flatsome", run the command below:

MKDIR C:\G-Drive\flatsome\MDTest

The results:



```
C:\>MKDIR C:\G-Drive\flatsome\MDTest

C:\>cd G-Drive\flatsome

C:\G-Drive\flatsome>dir
 Volume in drive C has no label.
 Volume Serial Number is 1471-EE58

 Directory of C:\G-Drive\flatsome

13/06/2019  12:29    <DIR>          .
13/06/2019  12:29    <DIR>          ..
08/06/2019  11:48               316 footer.php
06/06/2019  00:05               326 index.php
13/06/2019  12:29    <DIR>          MDTest
12/06/2019  21:59             2,258 My-Computer-Info.csv
12/06/2019  21:59             2,258 My-Computer-Info.txt
12/06/2019  23:11             4,198 New-CSV
06/06/2019  00:05             1,172 page.php
12/06/2019  17:14            12,275 structure-posts.php
12/06/2019  17:14               330 structure-sidebars.php
12/06/2019  23:11             4,198 TASKLIST-example.csv
               9 File(s)         27,331 bytes
               3 Dir(s)  765,798,375,424 bytes free

C:\G-Drive\flatsome>
```

MOVE

The MOVE command moves files and folders (directories). It also renames files and folders.

MOVE Syntax

Syntax to rename a file

MOVE [/Y | /-Y] [drive:][path]filename1[,…] destination

Syntax to a directory (folder)

MOVE [/Y | /-Y] [drive:][path]dirname1 dirname2

MOVE Parameters

Parameters	**Description**
[drive:]	Specifies the location and name of the file or files you want

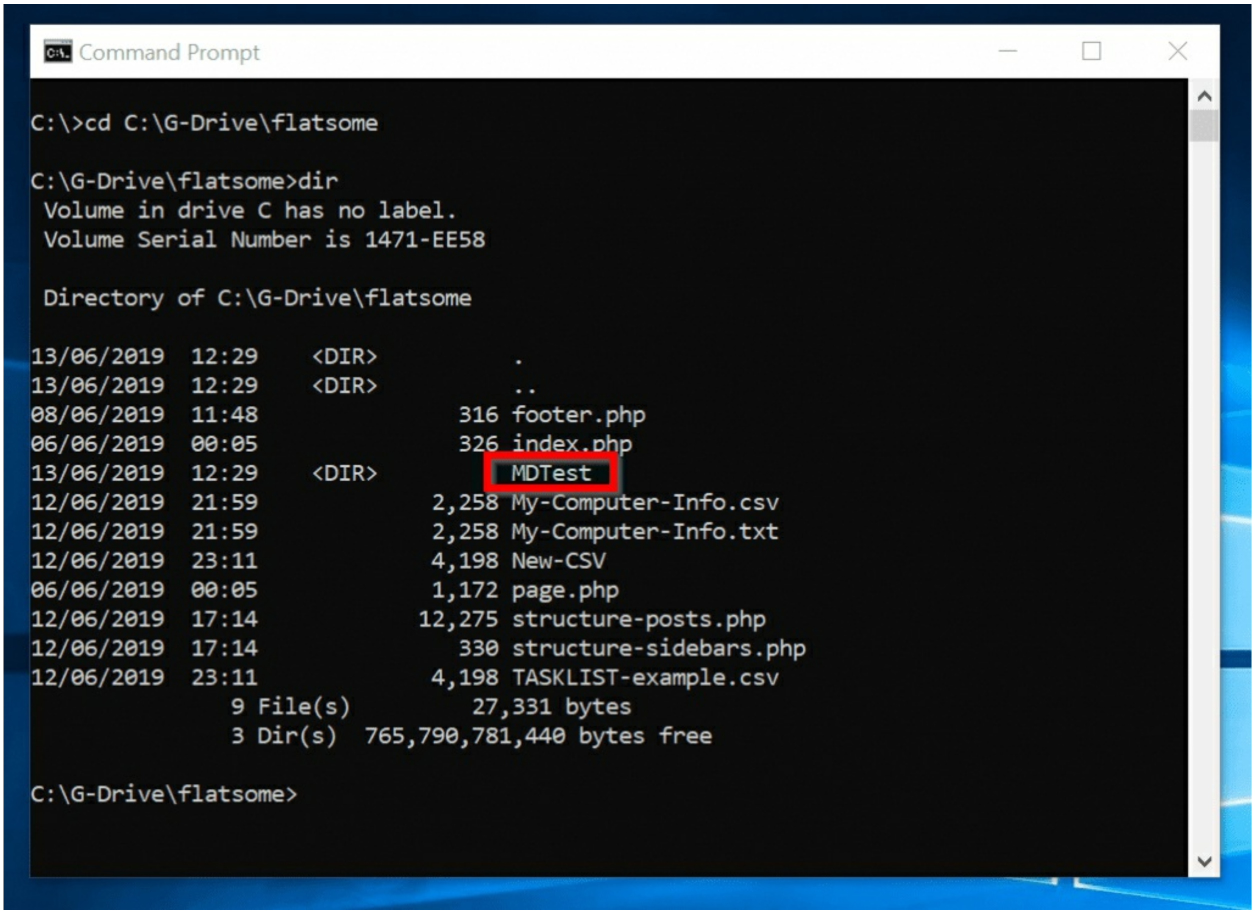
[path]filename1	to move.
destination	Specifies the new location of the file.
[drive:] [path]dirname1	Specifies the directory you want to rename.
dirname2	Specifies the new name for dirname1.
/Y	Suppresses prompting to confirm you want to overwrite an existing destination file.
/-Y	Causes prompting to confirm you want to overwrite an existing destination file.

Tip

For the file ***destination*** *parameter, "destination" can be a drive letter and colon, a directory name, or a combination of both. If you are moving only one file and want to rename the file when you move it, you can also include a filename.*

MOVE Examples

In this example, I want to rename MDTest (highlighted in the image below) to MDTest2

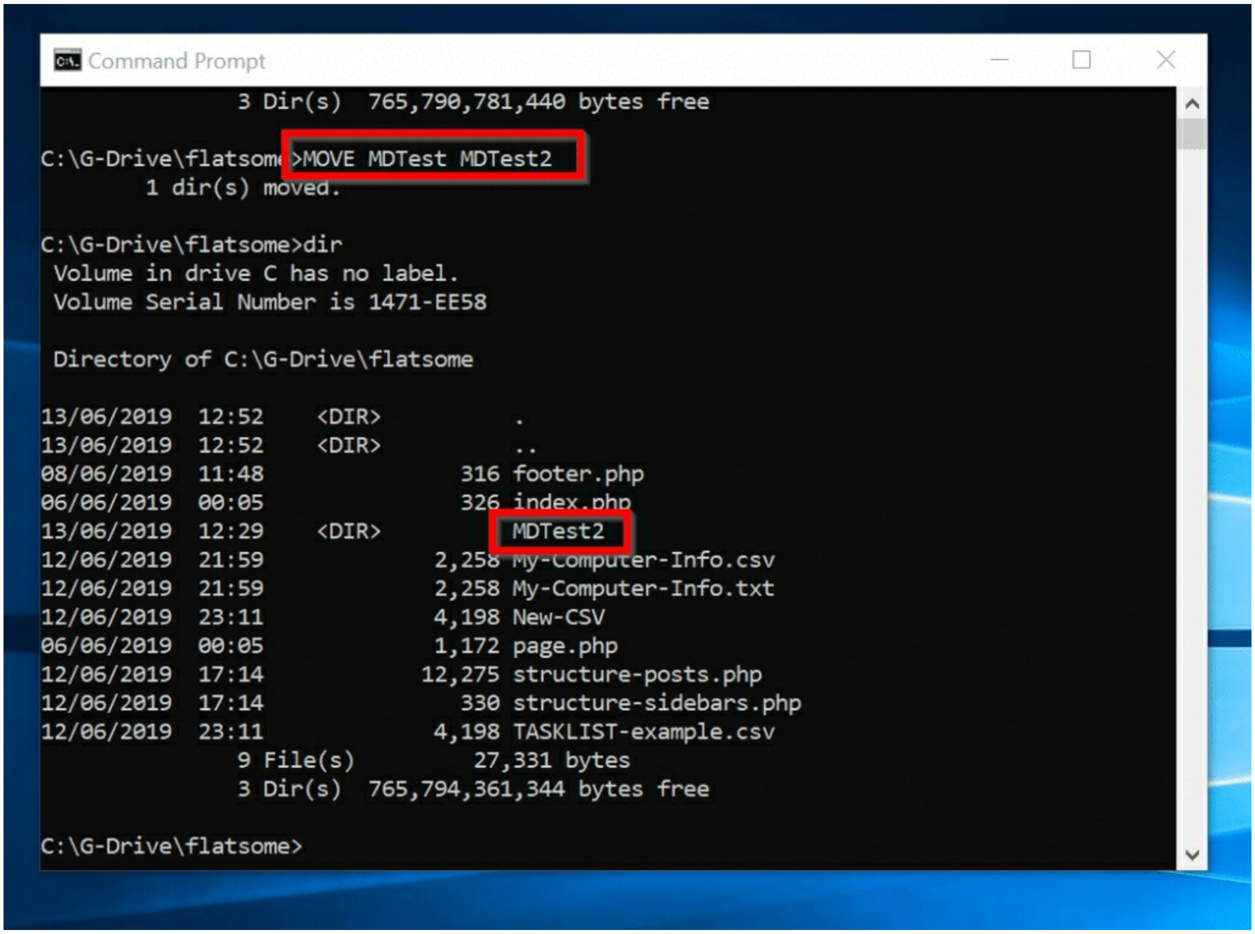


```
C:\>cd C:\G-Drive\flatsome

C:\G-Drive\flatsome>dir
 Volume in drive C has no label.
 Volume Serial Number is 1471-EE58

 Directory of C:\G-Drive\flatsome

13/06/2019  12:29    <DIR>          .
13/06/2019  12:29    <DIR>          ..
08/06/2019  11:48               316 footer.php
06/06/2019  00:05               326 index.php
13/06/2019  12:29    <DIR>          MDTest
12/06/2019  21:59             2,258 My-Computer-Info.csv
12/06/2019  21:59             2,258 My-Computer-Info.txt
12/06/2019  23:11             4,198 New-CSV
06/06/2019  00:05             1,172 page.php
12/06/2019  17:14            12,275 structure-posts.php
12/06/2019  17:14               330 structure-sidebars.php
12/06/2019  23:11             4,198 TASKLIST-example.csv
               9 File(s)         27,331 bytes
               3 Dir(s)  765,790,781,440 bytes free

C:\G-Drive\flatsome>
```

Here is the command:

MOVE MDTest MDTest2

Here is the result:



```
               3 Dir(s)  765,790,781,440 bytes free

C:\G-Drive\flatsome>MOVE MDTest MDTest2
        1 dir(s) moved.

C:\G-Drive\flatsome>dir
 Volume in drive C has no label.
 Volume Serial Number is 1471-EE58

 Directory of C:\G-Drive\flatsome

13/06/2019  12:52    <DIR>          .
13/06/2019  12:52    <DIR>          ..
08/06/2019  11:48               316 footer.php
06/06/2019  00:05               326 index.php
13/06/2019  12:29    <DIR>          MDTest2
12/06/2019  21:59             2,258 My-Computer-Info.csv
12/06/2019  21:59             2,258 My-Computer-Info.txt
12/06/2019  23:11             4,198 New-CSV
06/06/2019  00:05             1,172 page.php
12/06/2019  17:14            12,275 structure-posts.php
12/06/2019  17:14               330 structure-sidebars.php
12/06/2019  23:11             4,198 TASKLIST-example.csv
               9 File(s)         27,331 bytes
               3 Dir(s)  765,794,361,344 bytes free

C:\G-Drive\flatsome>
```

Tip
In the previous command, I did not need to specify the [drive:][path] because I wanted the command performed in the directory I was running the command from. The folder I was renaming was in the same directory.

ERASE (DEL)

This is the final in my ultimate list of command prompt commands. ERASE command deletes one or more files.

ERASE is the same as DEL command.

Warning!
*Use ERASE (DEL) with caution as the command may delete important Operating System files depending on how you use it. If you use **DEL** or **ERASE** to delete a file from your computer, you cannot retrieve the file.*

ERASE (DEL) Syntax

ERASE [/P] [/F] [/S] [/Q] [/A[[:]attributes]] names
DEL [/P] [/F] [/S] [/Q] [/A[[:]attributes]] names

ERASE (DEL) Parameters

Parameters	**Description**
/P	Asks for confirmation before deleting each file.
/F	Force deleting of files marked as read-only.
/S	Delete specified files from all sub-directories.
/Q	The quiet mode does not ask if ok to delete when a global wildcard is used. If you use /Q switch, all files will be deleted without prompting you for confirmation. [Use with caution!]
/A	Selects files to delete based on file attributes.
attributes	See below for acceptable attributes*.
names	Specifies a list of one or more files or directories. Wildcards may be used to delete multiple files. If a directory is specified, all files within the directory will be deleted.

*Acceptable attributes of the /A parameter:

R Read-only files

S System files

H Hidden files

A Files ready for archiving

I Not content indexed Files

L Reparse Points

- Prefix meaning not

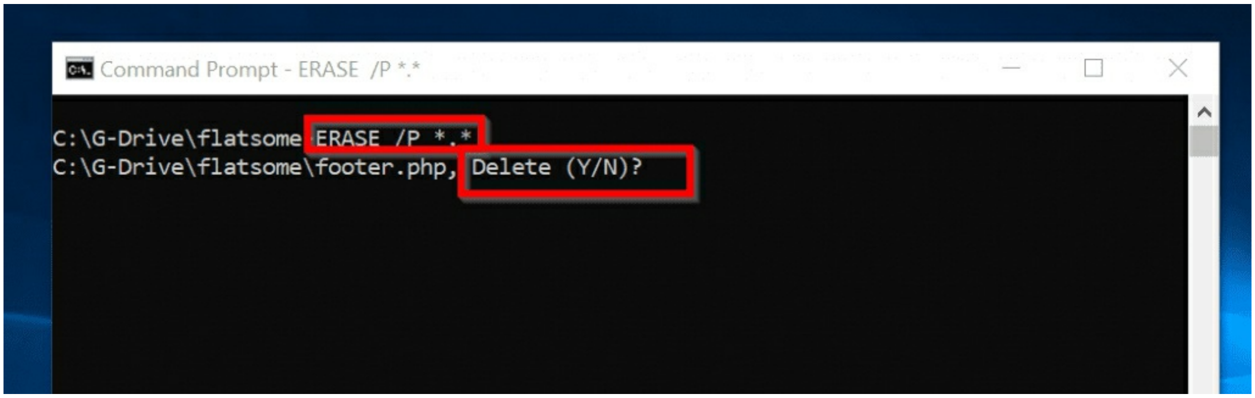
ERASE (DEL) Examples

TO delete all files in the current directory but prompt you for confirmation, use the command:

```
ERASE /P *.*
```

Tip
**.* is a wildcard meaning delete every file in the current directory*

When you press Enter key, for each file you will be asked to confirm with **Y** or **N**. Here is the result:



```
C:\G-Drive\flatsome ERASE /P *.*
C:\G-Drive\flatsome\footer.php, Delete (Y/N)?
```

Sign up to my PowerShell mailing list.
To receive PowerShell Freebies from Itechguides.com, click this link:

Itechguides.com/powershell-list-amazon/