# 15 CMD Commands Every Windows User Should Know

By Matt Smith

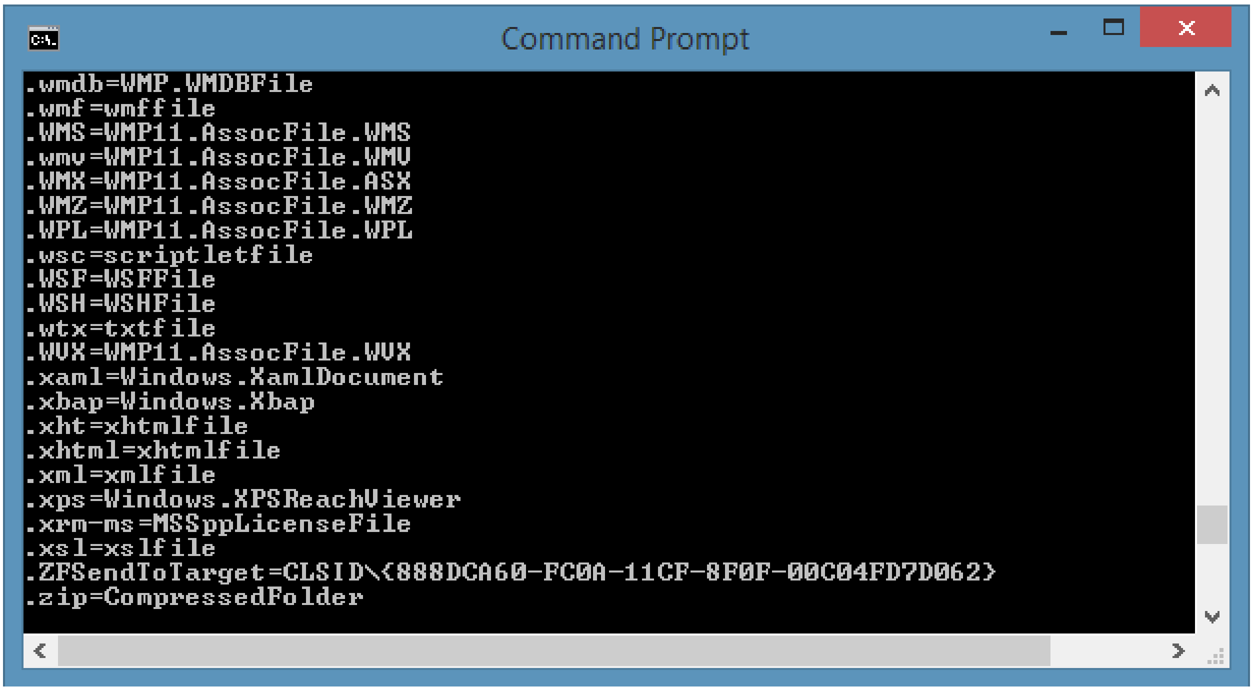
July 25, 2014

Microsoft has slowly but surely pushed the command line aside in the Windows interface. This is not without reason, as it's an antiquated and mostly unnecessary tool from an era of text-based input that has long passed.

But there still are some commands that remain useful, and Windows 8 even added new features. Here are the commands every Windows user needs to know.

In case you're not sure how to access the command prompt, forgot basic commands, or would like to know how to see a list of  switches for each command, you can refer to our beginners guide to the Windows command line for instructions.

## ASSOC

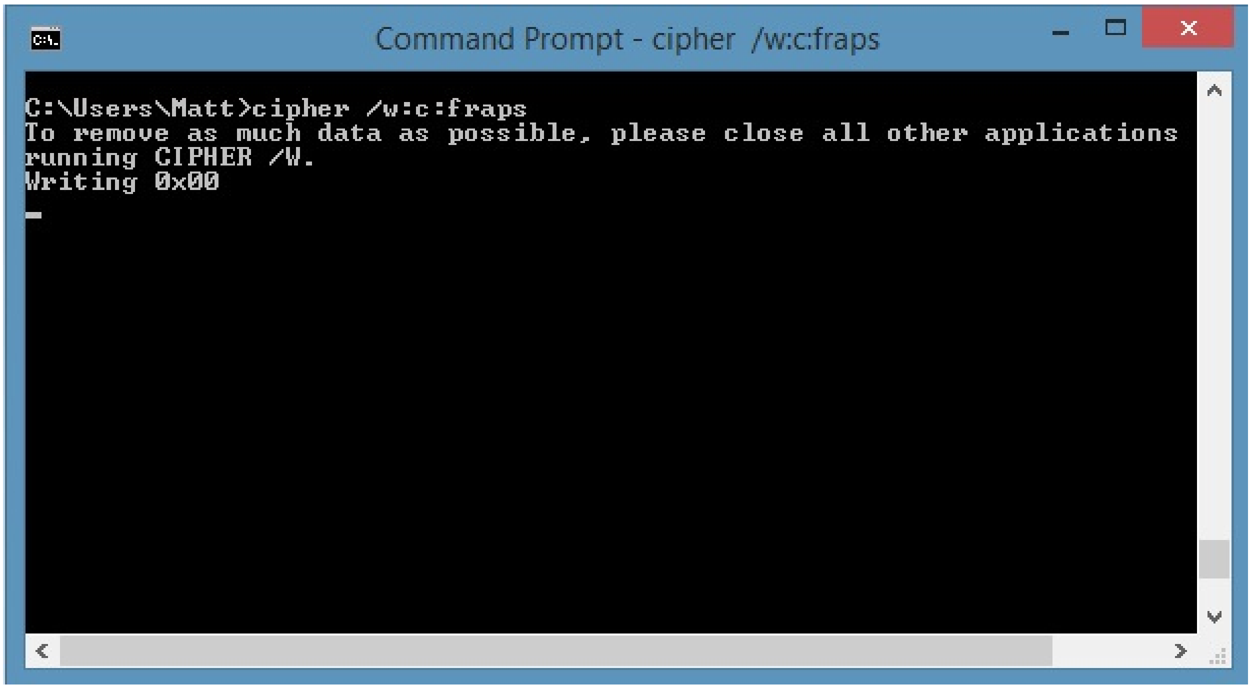


```
.wmdb=WMP.WMDBFile
.wmf=wmffile
.WMS=WMP11.AssocFile.WMS
.wmv=WMP11.AssocFile.WMV
.WMX=WMP11.AssocFile.ASX
.WMZ=WMP11.AssocFile.WMZ
.WPL=WMP11.AssocFile.WPL
.wsc=scriptletfile
.WSF=WSFFile
.WSH=WSHFile
.wtx=txtfile
.WVX=WMP11.AssocFile.WVX
.xaml=Windows.XamlDocument
.xbap=Windows.Xbap
.xht=xhtmlfile
.xhtml=xhtmlfile
.xml=xmlfile
.xps=Windows.XPSReachViewer
.xrm-ms=MSSppLicenseFile
.xsl=xslfile
.ZFSendToTarget=CLSID\{888DCA60-FC0A-11CF-8F0F-00C04FD7D062}
.zip=CompressedFolder
```

Most files in Windows are associated with a specific program that is assigned to open the file by default. At times, remembering these associations can become confusing. You can remind yourself by entering the command "assoc" to display a full list of file extensions and the programs they're connected with.

You can also extend the command to change file associations. For example, "assoc .txt=" will change the file association for text files to whatever program you enter after the equal sign. The ASSOC command itself will reveal both the extension names and program names, which will help you properly use this command. You can probably do this more easily in the GUI, but the command line interface is a perfectly functional alternative.

## Cipher



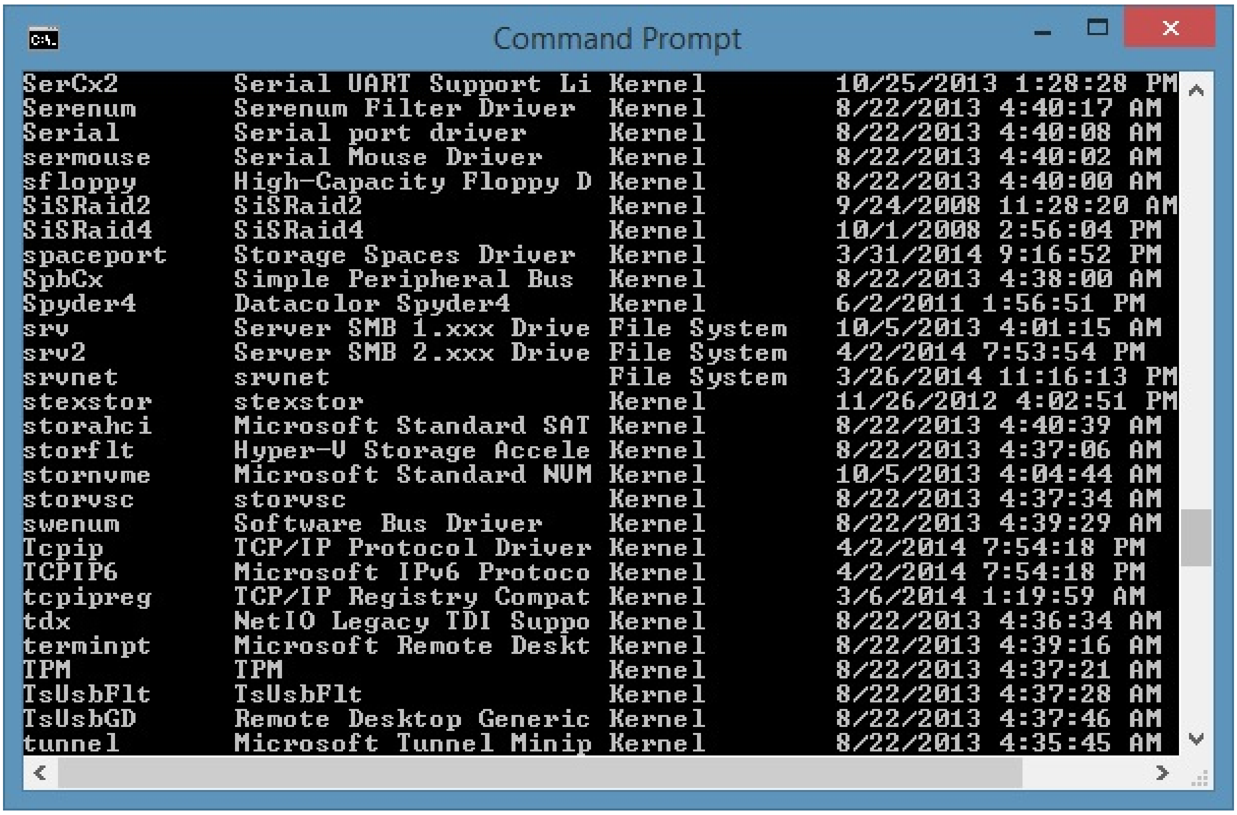
```
C:\Users\Matt>cipher /w:c:fraps
To remove as much data as possible, please close all other applications
running CIPHER /W.
Writing 0x00
_
```

Deleting files on a mechanical hard drive doesn't really delete them at all. Instead, it marks the files as no longer accessible and the space they took up as free. The files remain recoverable until they're overwritten with new data, which can take some time.

The cipher command, however, can be used to wipe a directory by writing random data to it. To wipe your C drive, for example, you'd use the command "cipher /w:c", which will wipe free space on the drive. The command does not overwrite undeleted data, so you will not wipe out files you need by running this command.

There's also a host of other cipher commands, however, they are generally redundant with Bitlocker enabled versions of Windows.

## Driverquery

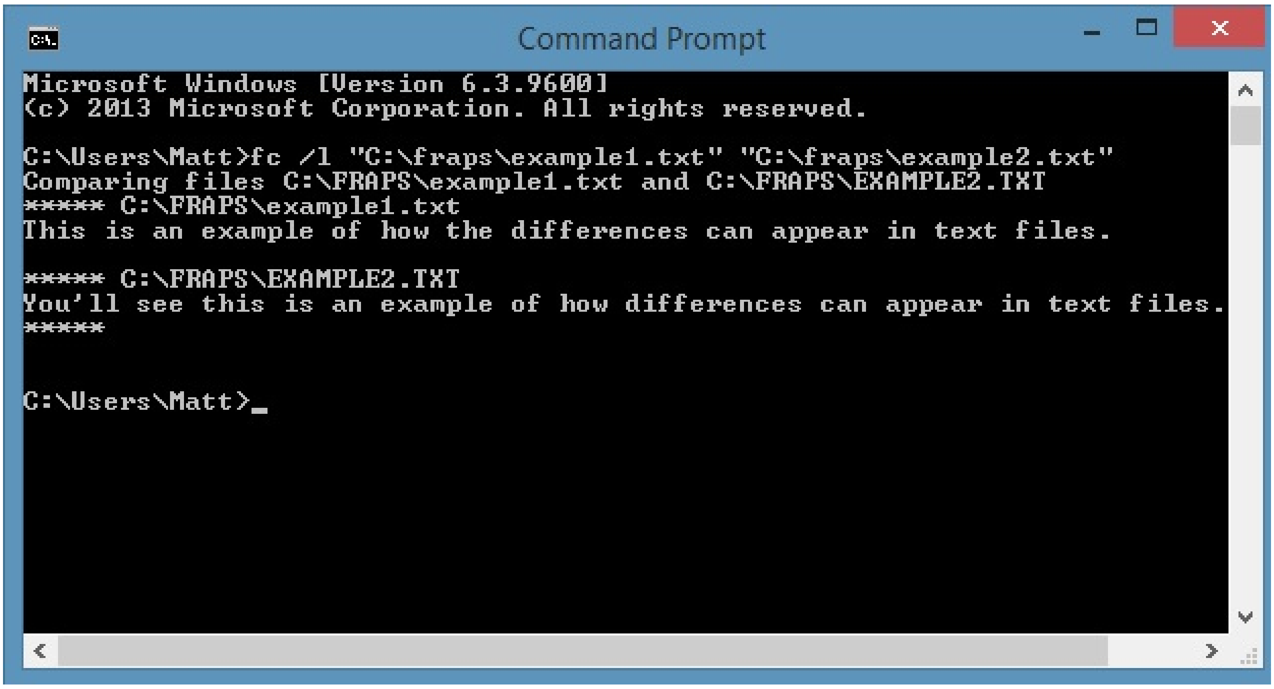


```
SerCx2       Serial UART Support Li Kernel        10/25/2013 1:28:28 PM
Serenum      Serenum Filter Driver  Kernel        8/22/2013 4:40:17 AM
Serial       Serial port driver     Kernel        8/22/2013 4:40:08 AM
sermouse     Serial Mouse Driver    Kernel        8/22/2013 4:40:02 AM
sfloppy      High-Capacity Floppy D Kernel        8/22/2013 4:40:00 AM
SiSRaid2     SiSRaid2               Kernel        9/24/2008 11:28:20 AM
SiSRaid4     SiSRaid4               Kernel        10/1/2008 2:56:04 PM
spaceport    Storage Spaces Driver  Kernel        3/31/2014 9:16:52 PM
SpbCx        Simple Peripheral Bus  Kernel        8/22/2013 4:38:00 AM
Spyder4      Datacolor Spyder4      Kernel        6/2/2011 1:56:51 PM
srv          Server SMB 1.xxx Drive File System   10/5/2013 4:01:15 AM
srv2         Server SMB 2.xxx Drive File System   4/2/2014 7:53:54 PM
srvnet       srvnet                 File System   3/26/2014 11:16:13 PM
stexstor     stexstor               Kernel        11/26/2012 4:02:51 PM
storahci     Microsoft Standard SAT Kernel        8/22/2013 4:40:39 AM
storflt      Hyper-V Storage Accele Kernel        8/22/2013 4:37:06 AM
stornvme     Microsoft Standard NVM Kernel        10/5/2013 4:04:44 AM
storvsc      storvsc                Kernel        8/22/2013 4:37:34 AM
swenum       Software Bus Driver    Kernel        8/22/2013 4:39:29 AM
Tcpip        TCP/IP Protocol Driver Kernel        4/2/2014 7:54:18 PM
TCPIP6       Microsoft IPv6 Protoco Kernel        4/2/2014 7:54:18 PM
tcpipreg     TCP/IP Registry Compat Kernel        3/6/2014 1:19:59 AM
tdx          NetIO Legacy TDI Suppo Kernel        8/22/2013 4:36:34 AM
terminpt     Microsoft Remote Deskt Kernel        8/22/2013 4:39:16 AM
TPM          TPM                    Kernel        8/22/2013 4:37:21 AM
TsUsbFlt     TsUsbFlt               Kernel        8/22/2013 4:37:28 AM
TsUsbGD      Remote Desktop Generic Kernel        8/22/2013 4:37:46 AM
tunnel       Microsoft Tunnel Minip Kernel        8/22/2013 4:35:45 AM
```

Drivers remain among the most important software installed on a PC. Improperly configured or missing drivers can cause all sorts of trouble, so its good to have access to a list of what's on your PC. That's exactly what the "driverquery" command does. You can extend it to "driverquery -v" to obtain more information including the directory in which the driver is installed.

## File Compare

This command can be used to identify differences in text between two files, and is particularly useful for writers and programmers trying to find small changes between two versions of a file. Simply type "fc" and then the directory path and file name of the two files you want to compare.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Matt>fc /l "C:\fraps\example1.txt" "C:\fraps\example2.txt"
Comparing files C:\FRAPS\example1.txt and C:\FRAPS\EXAMPLE2.TXT
***** C:\FRAPS\example1.txt
This is an example of how the differences can appear in text files.

***** C:\FRAPS\EXAMPLE2.TXT
You'll see this is an example of how differences can appear in text files.
*****


C:\Users\Matt>_
```

You can also extend the command in several ways. Typing "/b" compares only binary output, "/c" disregards the case of text in the comparison, and "/l" only compares ASCII text.

So, for example, you could use the following:

```
fc /l "C:\Program Files (x86)\example1.doc" "C:\Program Files (x86)\example2.doc"
```

to compare ASCII text in two word documents.

## Ipconfig

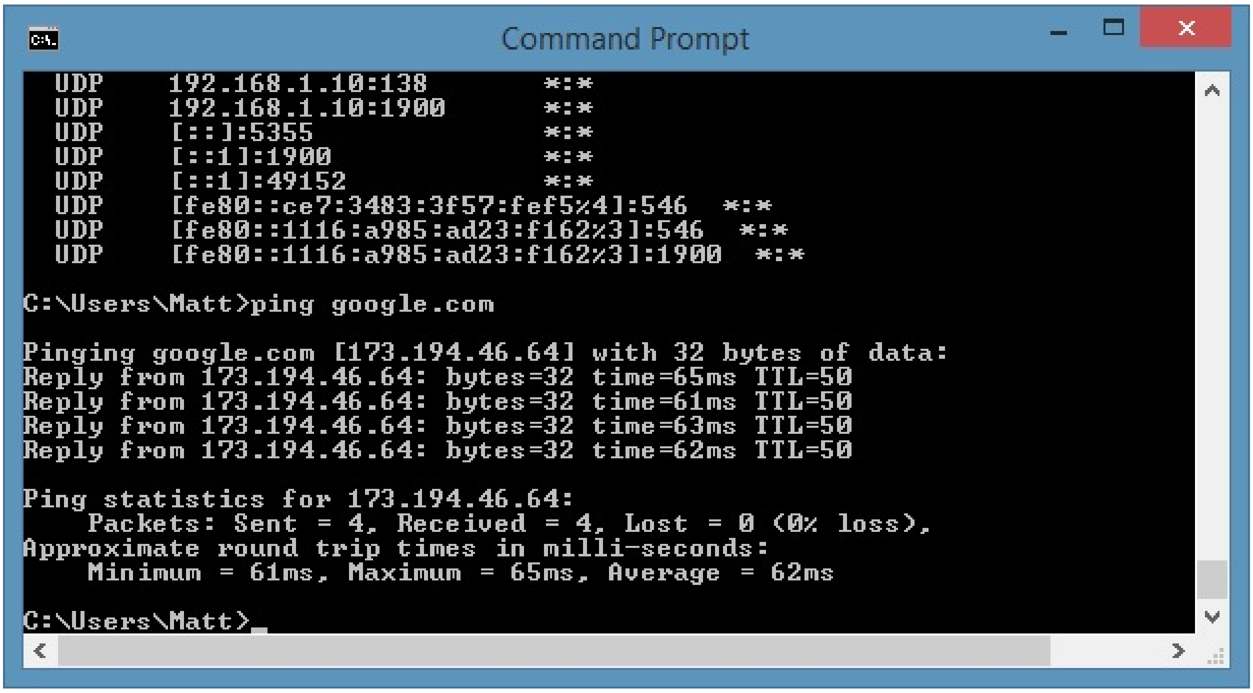
This command relays the IP address that your computer is currently using. However, if you're behind a router (like most computers today), you'll instead receive the local network address of the router.

Still, ipconfig is useful because of its extensions. "ipconfig /release" followed by "ipconfig /renew" can force your Windows PC into asking for a new IP address, which is useful if your computer claims one isn't available. You can also use "ipconfig /flushdns" to refresh your DNS address. These commands are great if the Windows network troubleshooter chokes, which does happen on occasion.

## Netstat

Entering the command "netstat -an" will provide you with a list of currently open ports and related IP addresses. You'll also be told what state the port is in – listening, established or closed. This is a great command if you're trying to troubleshoot the devices your PC is connected to or you're afraid you're infected with a Trojan and are trying to locate a malicious connection.

## Ping



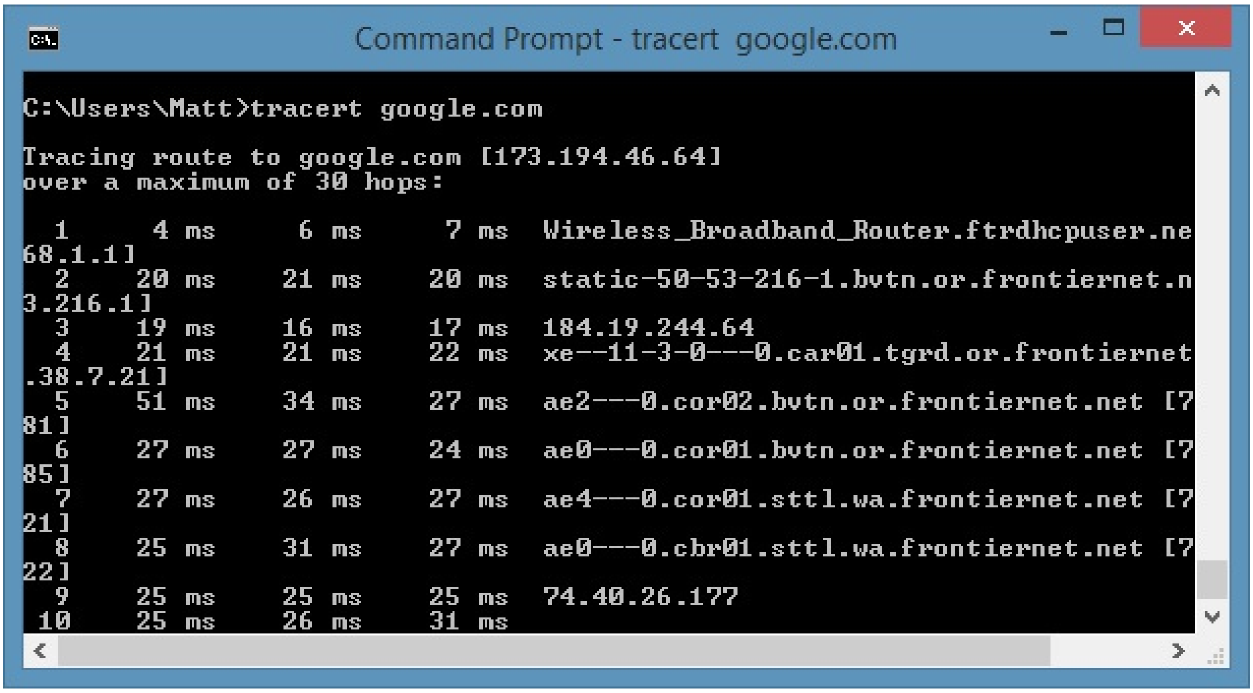
```
  UDP    192.168.1.10:138       *:*
  UDP    192.168.1.10:1900      *:*
  UDP    [::]:5355              *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:49152            *:*
  UDP    [fe80::ce7:3483:3f57:fef5%4]:546   *:*
  UDP    [fe80::1116:a985:ad23:f162%3]:546   *:*
  UDP    [fe80::1116:a985:ad23:f162%3]:1900   *:*

C:\Users\Matt>ping google.com

Pinging google.com [173.194.46.64] with 32 bytes of data:
Reply from 173.194.46.64: bytes=32 time=65ms TTL=50
Reply from 173.194.46.64: bytes=32 time=61ms TTL=50
Reply from 173.194.46.64: bytes=32 time=63ms TTL=50
Reply from 173.194.46.64: bytes=32 time=62ms TTL=50

Ping statistics for 173.194.46.64:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 61ms, Maximum = 65ms, Average = 62ms

C:\Users\Matt>_
```

Sometimes, you need to know whether or not packets are making it to a specific networked device. That's where ping comes in handy. Typing "ping" followed by an IP address or web domain will send a series of test packets to the specified address. If they arrive and are returned, you know the device is capable of communicating with your PC; if it fails, you know that there's something blocking communication between the device and your computer. This can help you decide if an issue is caused by improper configuration or a failure of network hardware.

## Pathping

This is a more advanced version of ping that's useful if there are multiple routers between your PC and the device you're testing. Like ping, you use this command by typing "pathping" followed by the IP address, but unlike ping, pathping also relays some information about the route the test packets take.

## Tracert



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

Tracing route to google.com [173.194.46.64]
over a maximum of 30 hops:

  1     4 ms     6 ms     7 ms  Wireless_Broadband_Router.ftrdhcpuser.ne
68.1.1]
  2    20 ms    21 ms    20 ms  static-50-53-216-1.bvtn.or.frontiernet.n
3.216.1]
  3    19 ms    16 ms    17 ms  184.19.244.64
  4    21 ms    21 ms    22 ms  xe--11-3-0---0.car01.tgrd.or.frontiernet
.38.7.21]
  5    51 ms    34 ms    27 ms  ae2---0.cor02.bvtn.or.frontiernet.net [7
81]
  6    27 ms    27 ms    24 ms  ae0---0.cor01.bvtn.or.frontiernet.net [7
85]
  7    27 ms    26 ms    27 ms  ae4---0.cor01.sttl.wa.frontiernet.net [7
21]
  8    25 ms    31 ms    27 ms  ae0---0.cbr01.sttl.wa.frontiernet.net [7
22]
  9    25 ms    25 ms    25 ms  74.40.26.177
 10    25 ms    26 ms    31 ms
```

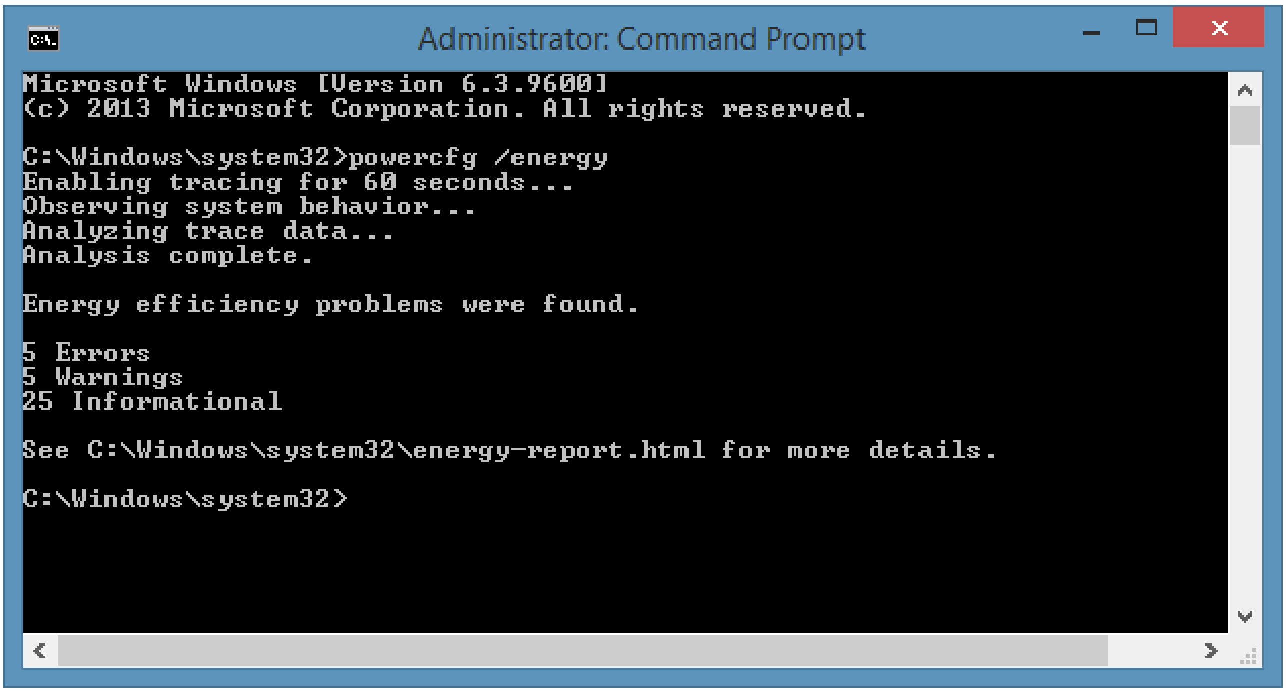
The “tracert” command is similar to pathping. Once again, type “tracert” followed by the IP address or domain you’d like to trace. You’ll receive information about each step in the route between your PC and the target. Unlike pathping, however, tracert also tracks how much time (in milliseconds) each hop between servers or devices takes.

## Powercfg

Powercfg is a very powerful command for managing and tracking how your computer uses energy. You can use the command “powercfg /hibernate on” and “powercfg /hibernate off” to manage hibernation, and you can also use the command “powercfg /a” to view the power-saving states currently available on your PC.

Another useful command is “powercfg /devicequery s1_supported” which displays a list of devices on your computer that support connected standby. When enabled, these devices can be used to bring your computer out o standby – even remotely. You can enable this by selecting the device in Device Manager, opening its properties, going to the Power Management tab and then checking the “Allow this device to wake the computer” box.

“Powercfg /lastwake” will show you what device last woke your PC from a sleep state. You can use this command to troubleshoot your PC if it seems to wake from sleep at random.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

Energy efficiency problems were found.

5 Errors
5 Warnings
25 Informational

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

C:\Windows\system32>
```

The “powercfg /energy” command can be used to build a detailed power consumption report for your PC, which is output to a directory indicated after the command finishes. This report will let you know of any system faults that might increase power consumption, like devices that are blocking certain sleep modes, or which aren’t properly configured to respond to your power management settings.

Windows 8 added “powercfg /batteryreport”, which provides a detailed analysis of battery use, if applicable. Normally output to your Windows user directory, the report provides details about the time and length of charge and discharge cycles, lifetime average battery life, and estimated battery capacity.

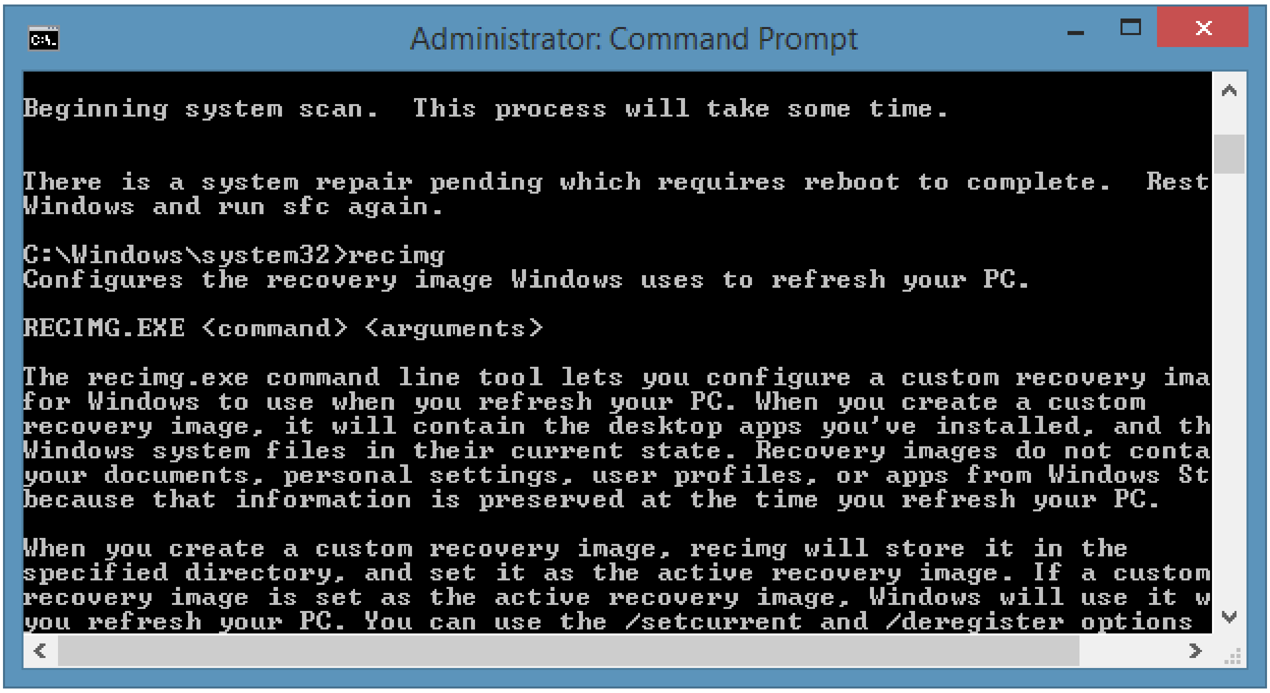
## Shutdown

As of Windows 8/8.1 there is now a shutdown command that – you guessed it! – shuts down your computer. This is of course redundant with the already easily accessed shutdown button, but what’s not redundant is the “shutdown /r /o” command, which restarts your PC and launches the Advanced Start Options menu, which is where you can access Safe Mode and Windows recovery utilities. This is useful if you want to restart your computer for troubleshooting purposes.

## System File Checker

System File Checker is an automatic scan and repair tool that focuses on Windows system files. You will need to run the command prompt with administrator privileges and enter the command “sfc /scannow”. If any corrupt or missing files are found, they’ll be automatically replaced using cached copies kept by Windows for just that purpose. The command can require a half-hour to run on older notebooks.

## Recovery Image

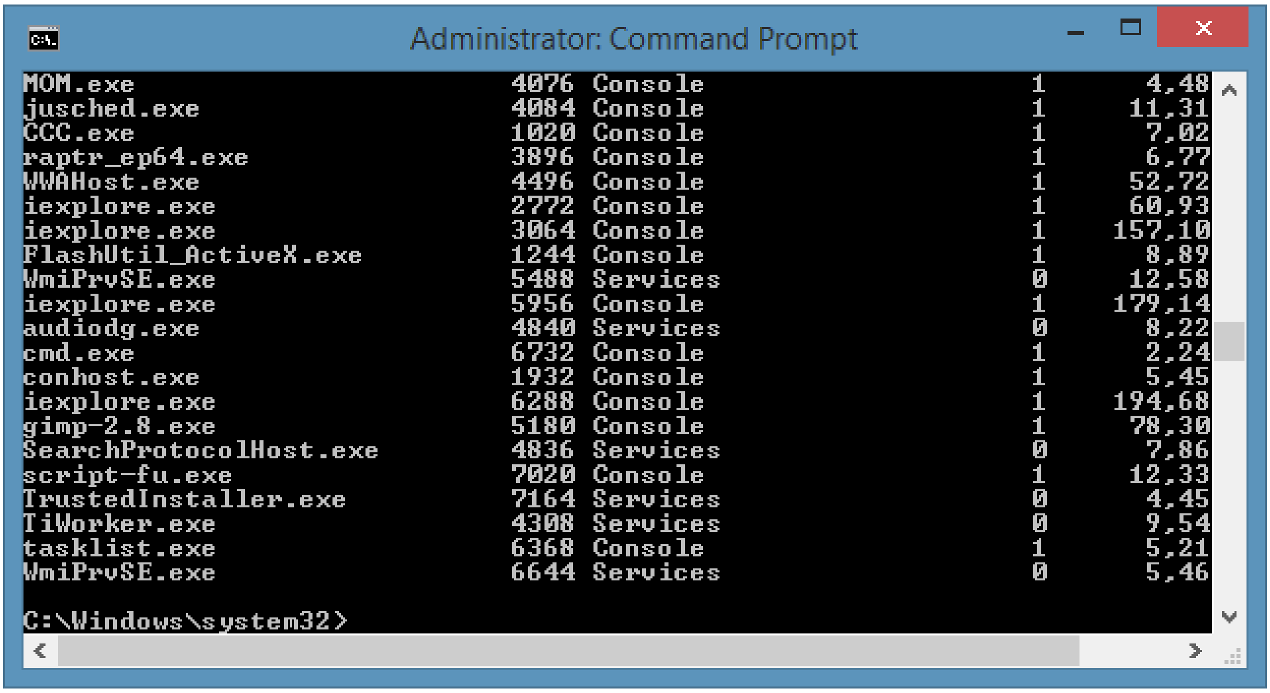


```
Beginning system scan.  This process will take some time.


There is a system repair pending which requires reboot to complete.  Rest
Windows and run sfc again.

C:\Windows\system32>recimg
Configures the recovery image Windows uses to refresh your PC.

RECIMG.EXE <command> <arguments>

The recimg.exe command line tool lets you configure a custom recovery ima
for Windows to use when you refresh your PC. When you create a custom
recovery image, it will contain the desktop apps you've installed, and th
Windows system files in their current state. Recovery images do not conta
your documents, personal settings, user profiles, or apps from Windows St
because that information is preserved at the time you refresh your PC.

When you create a custom recovery image, recimg will store it in the
specified directory, and set it as the active recovery image. If a custom
recovery image is set as the active recovery image, Windows will use it w
you refresh your PC. You can use the /setcurrent and /deregister options
```

Virtually all Windows 8/8.1 computers ship from the factory with a recovery image, but the image may include bloatware you'd rather not have re-installed. Once you've un-installed the software you can create a new image using the "recimg" command. Entering this command presents a very detailed explanation of how to use it. You must have administrator privileges to use the recimg command, and you can only access the custom recovery image you create via the Windows 8 "refresh" feature.

## Tasklist

The "tasklist" command can be used to provide a current list of all tasks running on your PC. Though somewhat redundant with Task Manager, the command may sometimes find tasks hidden from view in that utility.



```
MOM.exe                       4076 Console                    1      4,48
jusched.exe                   4084 Console                    1     11,31
CCC.exe                       1020 Console                    1      7,02
raptr_ep64.exe                3896 Console                    1      6,77
WWAHost.exe                   4496 Console                    1     52,72
iexplore.exe                  2772 Console                    1     60,93
iexplore.exe                  3064 Console                    1    157,10
FlashUtil_ActiveX.exe         1244 Console                    1      8,89
WmiPrvSE.exe                  5488 Services                   0     12,58
iexplore.exe                  5956 Console                    1    179,14
audiodg.exe                   4840 Services                   0      8,22
cmd.exe                       6732 Console                    1      2,24
conhost.exe                   1932 Console                    1      5,45
iexplore.exe                  6288 Console                    1    194,68
gimp-2.8.exe                  5180 Console                    1     78,30
SearchProtocolHost.exe        4836 Services                   0      7,86
script-fu.exe                 7020 Console                    1     12,33
TrustedInstaller.exe          7164 Services                   0      4,45
TiWorker.exe                  4308 Services                   0      9,54
tasklist.exe                  6368 Console                    1      5,21
WmiPrvSE.exe                  6644 Services                   0      5,46

C:\Windows\system32>
```

There's also a wide range of modifiers. "Tasklist -svc" shows services related to each task, "tasklist -v" can be used to obtain more detail on each task, and "tasklist -m" can be used to locate .dll files associated with active tasks. These commands are useful for advanced troubleshooting.

## Taskkill

Tasks that appear in the “tasklist” command will have an executable and process ID (a four-digit number) associated with them. You can force stop a program using “taskkill -im” followed by the executable’s name, or “taskkill -pid” followed by the process ID. Again, this is a bit redundant with Task Manager, but may be used to kill otherwise unresponsive or hidden programs.

## Conclusion

This article doesn’t cover every Windows command available. There are literally hundreds of them when all variables are included. Most, however, are no longer useful because they’ve been replaced by more convenient menus in the Windows GUI or simply aren’t commonly used (telnet, for example).

You can check out our Windows command cheat sheet for an expanded list or download Microsoft’s command line reference guide for advanced support and troubleshooting.

Which commands do you find yourself using frequently?