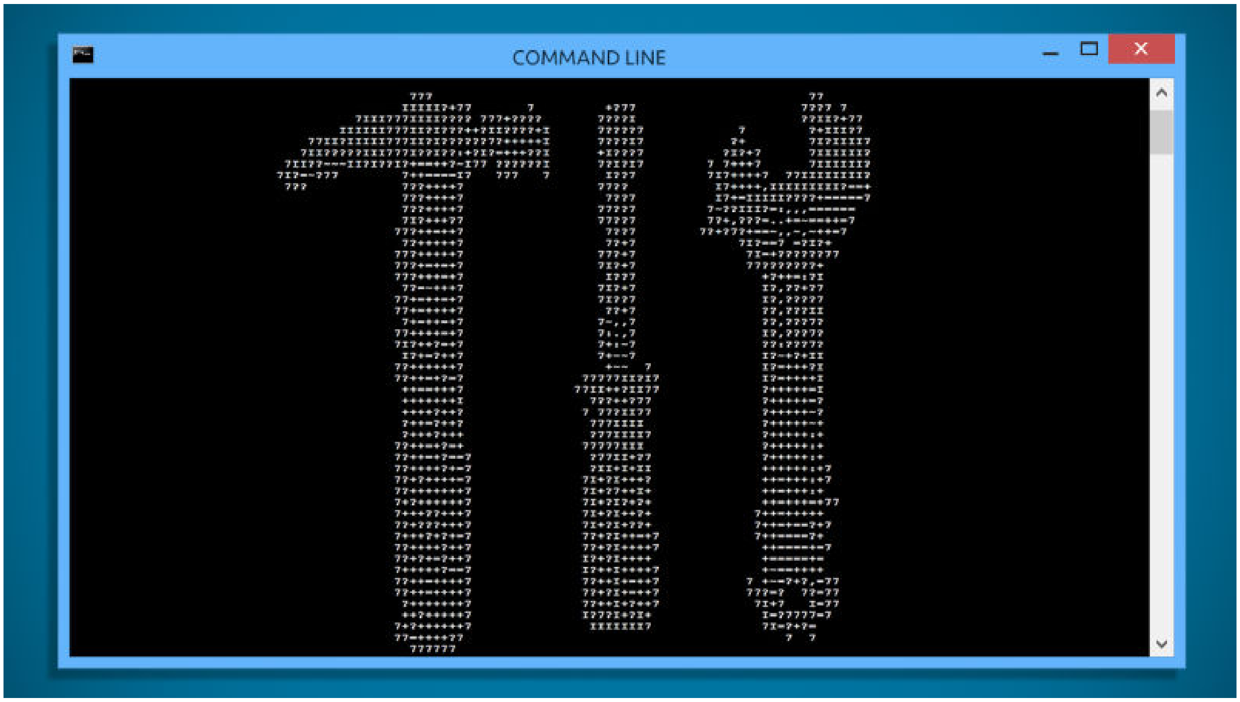
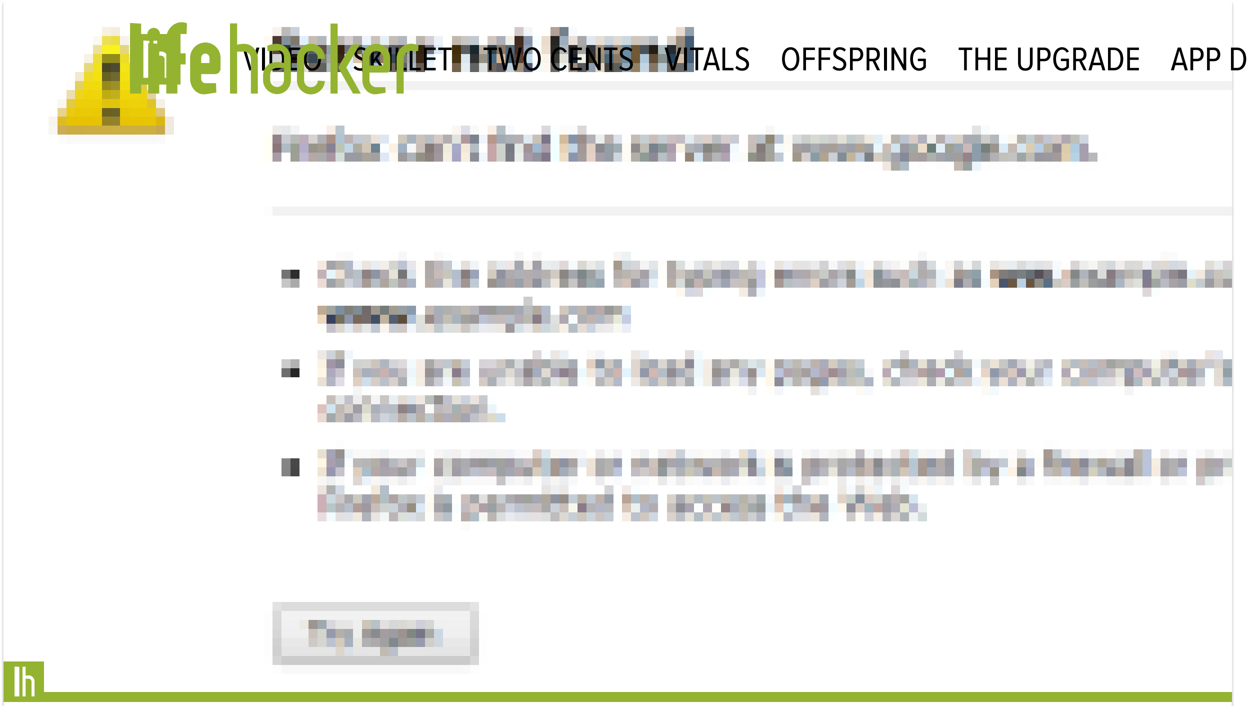
The Best Tools Hidden in Windows' Command Line

Walter Glenn
3/28/14 11:00am • Filed to: WINDOWS

292.3K 94 23



While it may not always be the best choice in Windows, there are certain things you can only do from the command line. We've talked about a few command line essentials before, like using tracert to troubleshoot a flaky Internet connection and using recimg to create a custom Windows recovery image. Here are a few more you should probably know about (if you don't already).



Server not found

Firefox can't find the server at www.google.com.

- Check the address for typing errors such as ww.example.co
  www.example.com
- If you are unable to load any pages, check your computer's
  connection.
- If your computer or network is protected by a firewall or pr
  Firefox is permitted to access the Web.

How to Troubleshoot a Flaky Internet Connection

You're zooming down the information superhighway getting things done when your usually-trusty...

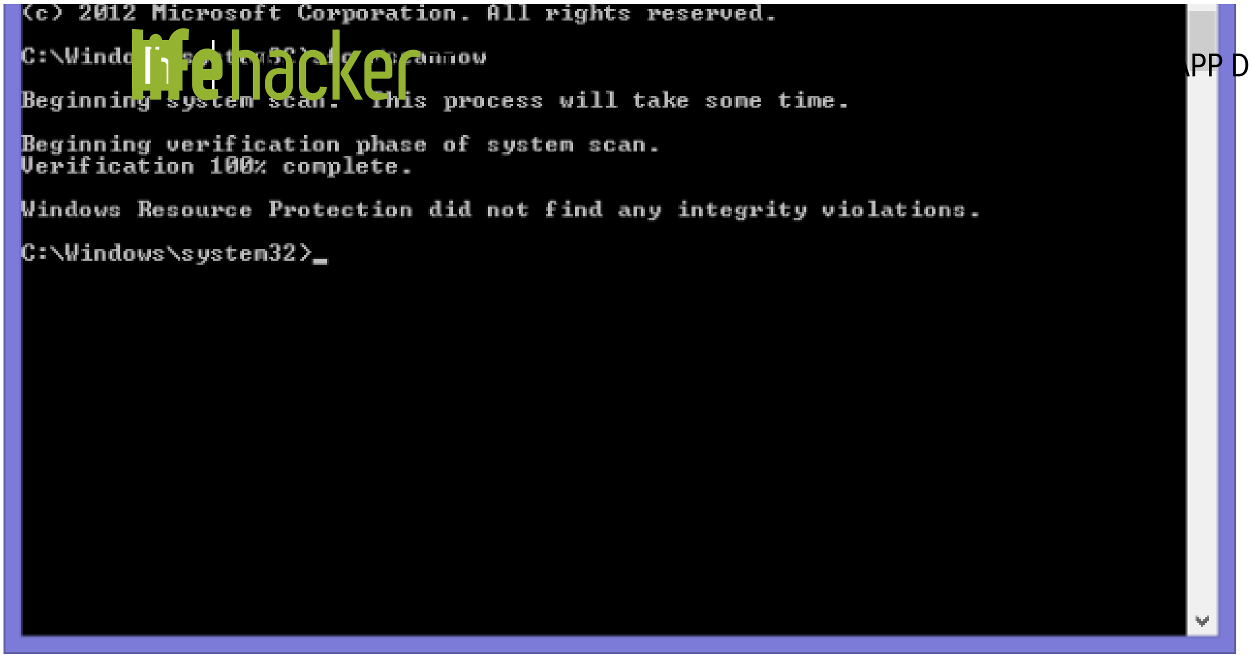
Read more

We're using Windows 8.1 for screenshots and details in this article, but most of these tools have been around a long time and are available in previous versions of Windows. If you have any doubt about whether they're available or if options are different, just open up the command prompt and type the command followed by `/?`. That will let you know if the command exists and what options you can use with it.

Also, many of these tools require that you run the Command Prompt with administrator privileges. To do that, right-click the Command Prompt icon and choose Run as administrator. Better yet, pin it to your Start menu or taskbar, right-click it and choose Properties, click the Advanced button, and choose Run as administrator. That way, it will run with elevated privileges every time.

System File Checker

```
Microsoft Windows [Version 6.2.9200]
```



```
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>sfc /scannow

Beginning system scan.  This process will take some time.

Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection did not find any integrity violations.

C:\Windows\system32>_
```

Windows can usually detect when a system file is missing and replace it for you without any intervention on your part. You typically won't even be notified when it happens. But even with this ability, system files can become corrupted or the wrong versions of system files can get installed by errant applications. Sometimes, these problems slip by Windows unnoticed.

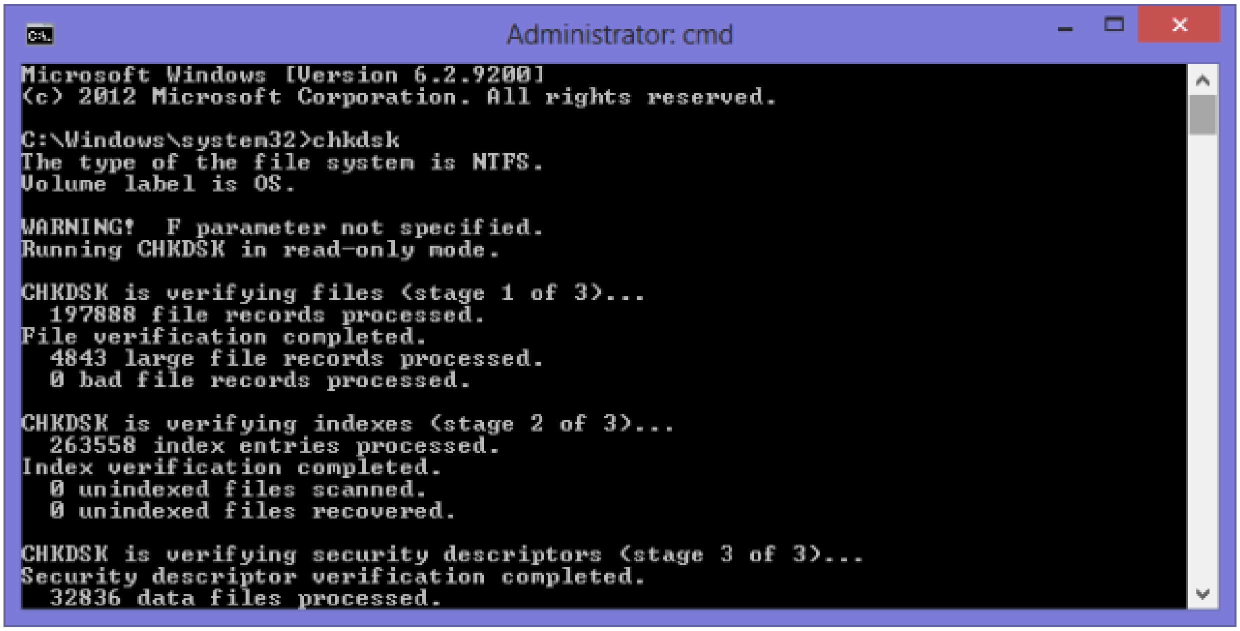
Windows includes the command line tool System File Checker, which scans several thousand basic Windows files, comparing them against the original versions that shipped with Windows or, depending on the files, that have been updated through Windows Updates. If System File Checker finds a mismatch, it replaces the original file. Depending on how you installed Windows, you may or may not need the installation media, but usually you won't.

To run the tool, just type `sfc` at the command prompt followed by a space and then any of the following common options:

- **/scannow**. This performs an immediate scan of your system and will replace files as necessary. You may need to restart Windows when it's done if it finds problems.
- **/scanonce**. This performs a scan the next time you restart your system.
- **/scanboot**. This schedules a scan to be performed every time you restart your system.

- **Revert**. This returns the System File Checker to its default settings. You can use it to turn off the /scanboot option, for example.

Check Disk



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>chkdsk
The type of the file system is NTFS.
Volume label is OS.

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

CHKDSK is verifying files (stage 1 of 3)...
  197888 file records processed.
File verification completed.
  4843 large file records processed.
  0 bad file records processed.

CHKDSK is verifying indexes (stage 2 of 3)...
  263558 index entries processed.
Index verification completed.
  0 unindexed files scanned.
  0 unindexed files recovered.

CHKDSK is verifying security descriptors (stage 3 of 3)...
Security descriptor verification completed.
  32836 data files processed.
```

Check Disk attempts to repair file system errors, locate bad sectors, and recover readable information from those bad sectors. If you ever start Windows and it tells you that it's scanning your hard disks before starting up, that's Check Disk at work. When Windows detects certain types of errors, it schedules a scan all by itself.

It takes a long time to run, especially if you let it scan the entire hard disk, including free space, so it's not really the kind of tool you want to run regularly. If you're concerned about general hard disk health, you should make use of one of the free S.M.A.R.T checkup utilities out there. I'm a fan of Passmark Disk Checkup, personally. It reads various self-monitoring data the hard disk itself collects and gives you a pretty good idea of how your hard disk is doing.

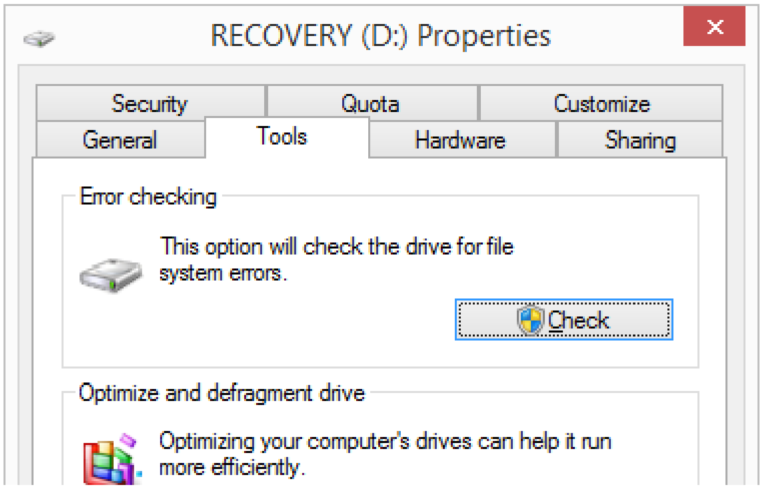
Still, sometimes hard disks are physically fine to keep using, but suffer from the occasional bad sector and corrupted files those bad sectors can cause. Windows tries its best to correct those problems for you, and it does a pretty good job. But if you ever notice that certain programs just refuse to start or you get an error when you try to access particular folders or files, bad sectors on the disk are a possible culprit. Check Disk can find those bad sectors, often recover data from them, and then map those sectors out so Windows doesn't use them anymore.

You can run Check Disk by typing `chkdsk` at the command prompt, followed by a space, and then any of these options:

- **Volume**. If you want to check a whole drive, just type the drive letter.
- **Filename**. You can also use chkdsk to check a single file or group of files.
- **/F**. Run it with this option to have chkdsk go ahead and fix those errors.
- **/R**. This option forces chkdsk to locate bad sectors and recover information from them. If chkdsk cannot lock the disk (which it usually can't since you're actually using Windows), it will prompt you run the command the next time you restart Windows. This is the option you'll use for the most thorough scan because running it also implies that you're running the /F option.

If you run chkdsk with no extra options, it will just perform a scan and give you a report without actually changing anything. So, you'll need to specify a volume or file name and one of the other options to make any fixes. Here's a common example. If you want chkdsk to scan your C: drive, locate bad sectors, recover information, and map over those bad sectors, type:

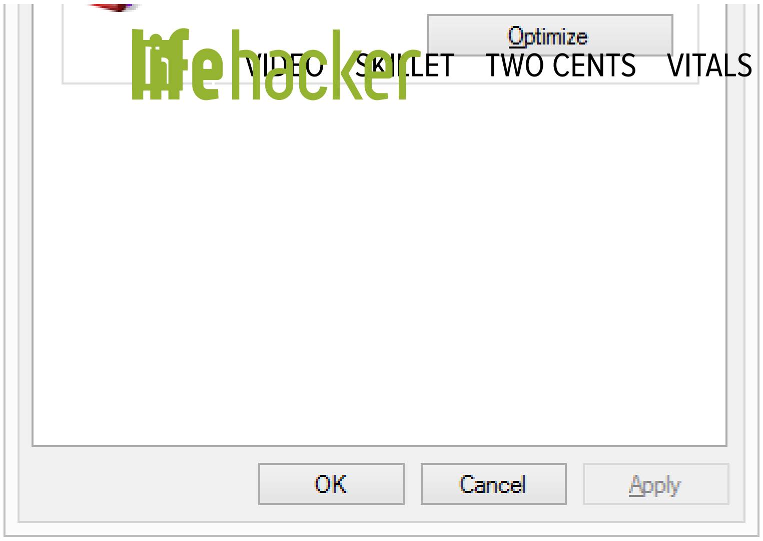
```
chkdsk C: /R
```



This option will check the drive for file system errors.

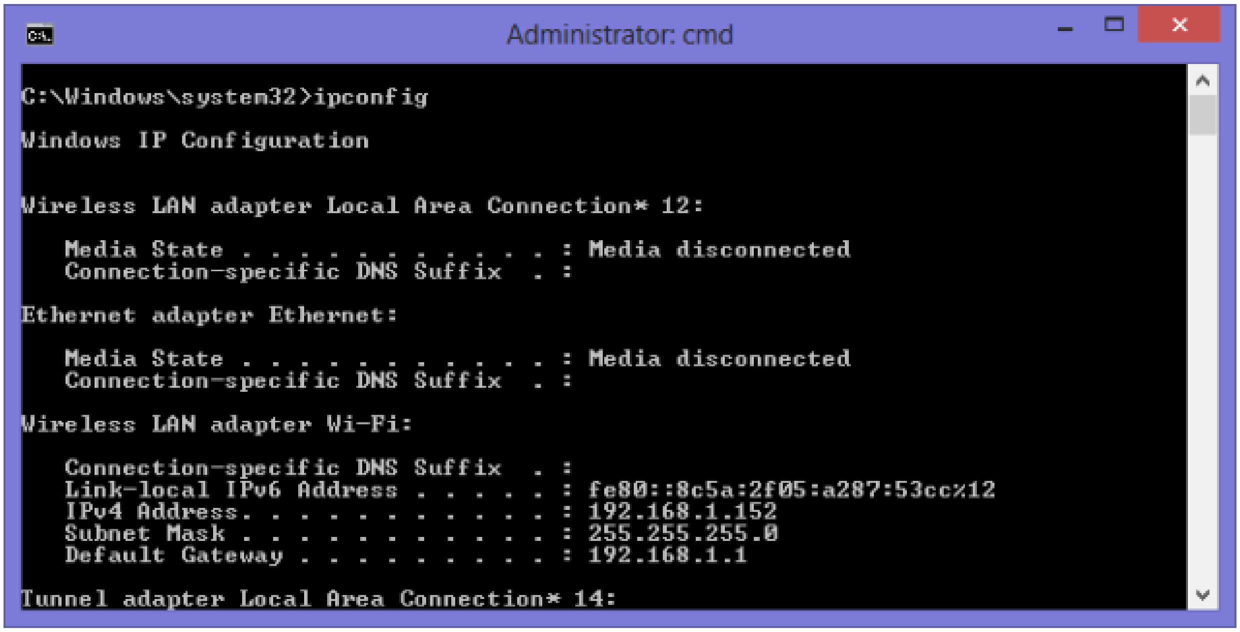
Optimizing your computer's drives can help it run more efficiently.

Note that there is a graphical interface of sorts for Check Disk. Open Windows Explorer, right-click a drive, and choose Properties. On the Tools tab, click the Check button. This opens up a prompt



that lets you schedule a scan on the next restart. You'll be prompted to fix any errors that are found. This interface doesn't provide any of the advanced options the command line version does and it also doesn't let you scan individual files.

Ipconfig



```
C:\Windows\system32>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 12:

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

Ethernet adapter Ethernet:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8c5a:2f05:a287:53cc%12
   IPv4 Address. . . . . . . . . . . : 192.168.1.152
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter Local Area Connection* 14:
```

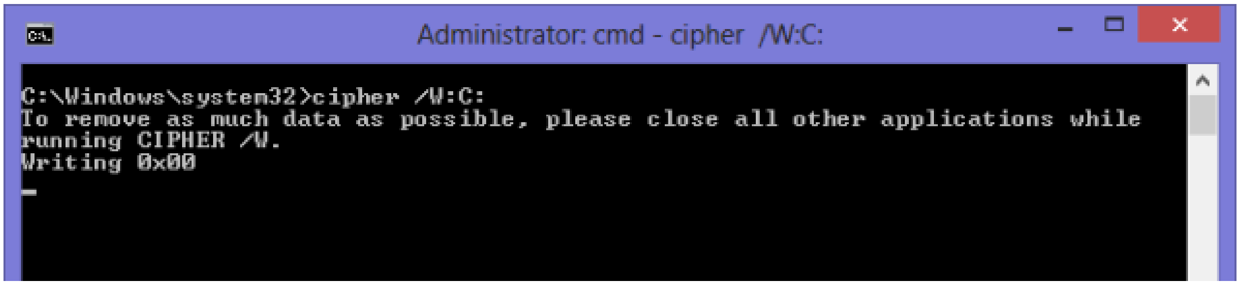
Ipconfig lets you view and work with TCP/IP information. You can use it to check your computer's IP address, have it release or renew that IP address if it's automatically assigned, and even purge the local DNS cache.

To use it, just type `ipconfig` at the command line. By itself, the command shows you IP addressing information about each of the network adapters on your computer. It may show several different adapters, so you'll have to do a little scouting to find the one you're looking for. You'll typically see a Wireless LAN adapter (for your wireless connection) and an Ethernet adapter (for your wired connection), and probably a few tunnel, virtual, or VPN adapters, depending on your setup. The information it shows you includes the IP address, physical (or MAC) address, default gateway, and subnet assigned to the adapter.

You can also add any of the following options to the ipconfig command by typing `ipconfig`, followed by a space, and then the option.

- **/all**. This option shows you all the same information as just running the ipconfig command by itself, plus a whole bunch more, such as whether the adapter is automatically assigned an IP address from a DHCP server, when that address was assigned, and when it expires.
- **/release**. Use this option to release all DHCP-assigned IP addresses. Note that your network will not work after this and typically you'll need use the /renew command afterward.
- **/renew**. Use this option to release and then immediately try to renew all DHCP-assigned information. This is probably the option you'll use most, as it forces your computer to reconnect to your router or to your ISP's servers (depending on your setup). It can be really helpful when troubleshooting connectivity problems.
- **/flushdns**. This option purges the local DNS cache. DNS is used to translate the more human-readable computer names and web addresses we use (like www.lifehacker.com) into IP addresses. The cache is DNS information stored locally on your computer so your computer doesn't have to look it up on a DNS server every time. Sometimes, flushing the DNS cache can resolve problems where you have network connectivity, but can't reach some computers or websites by name.

Cipher



```
C:\Windows\system32>cipher /W:C:
To remove as much data as possible, please close all other applications while
running CIPHER /W.
Writing 0x00
_
```

The cipher command is mostly for working with encrypted folders and files on NTFS volumes in Windows. Frankly, if you're using that type of encryption, you have a graphical interface available that does most of what you need, though the command is good for controlling encryption programmatically or through batch files and scripts.

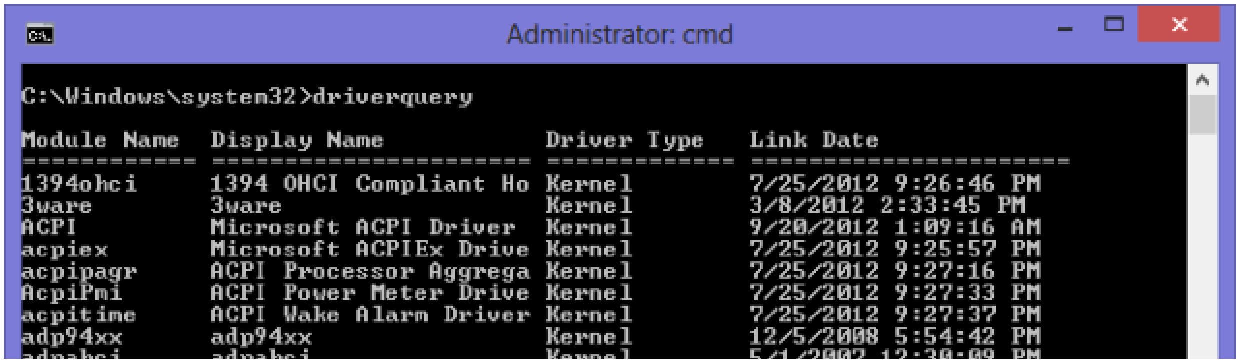
However, cipher does include one option at the command line that you might find useful:

```
cipher /W:pathname
```

The /W option removes data on unused portions of a volume, effectively erasing data that may be hanging around on your hard drive after deletion. You can point cipher at an entire volume (like C:) or a specific folder. As you probably already know, when you delete files from Windows, they are not actually erased from the hard drive. Instead, Windows marks that space as available to be written over with new files.

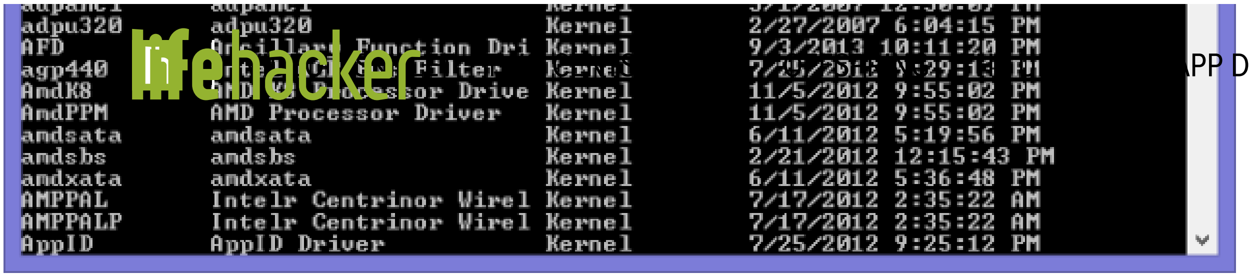
Note that this really applies to traditional hard drives and not SSDs. When you delete files from an SSD, those files are removed immediately.

Driverquery



```
C:\Windows\system32>driverquery

Module Name  Display Name           Driver Type   Link Date
============ ====================== ============= ======================
1394ohci     1394 OHCI Compliant Ho Kernel        7/25/2012 9:26:46 PM
3ware        3ware                  Kernel        3/8/2012 2:33:45 PM
ACPI         Microsoft ACPI Driver  Kernel        9/20/2012 1:09:16 AM
acpiex       Microsoft ACPIEx Drive Kernel        7/25/2012 9:25:57 PM
acpipagr     ACPI Processor Aggrega Kernel        7/25/2012 9:27:16 PM
AcpiPmi      ACPI Power Meter Drive Kernel        7/25/2012 9:27:33 PM
acpitime     ACPI Wake Alarm Driver Kernel        7/25/2012 9:27:37 PM
adp94xx      adp94xx                Kernel        12/5/2008 5:54:42 PM
```



```
adpu320      adpu320               Kernel      2/27/2007 6:04:15 PM
AFD          Ancillary Function Dri Kernel     9/3/2013 10:11:20 PM
agp440       Intel AGP Bus Filter  Kernel      7/25/2012 9:29:13 PM
AmdK8        AMD K8 Processor Drive Kernel     11/5/2012 9:55:02 PM
AmdPPM       AMD Processor Driver  Kernel      11/5/2012 9:55:02 PM
amdsata      amdsata               Kernel      6/11/2012 5:19:56 PM
amdsbs       amdsbs                Kernel      2/21/2012 12:15:43 PM
amdxata      amdxata               Kernel      6/11/2012 5:36:48 PM
AMPPAL       Intelr Centrinor Wirel Kernel     7/17/2012 2:35:22 AM
AMPPALP      Intelr Centrinor Wirel Kernel     7/17/2012 2:35:22 AM
AppID        AppID Driver          Kernel      7/25/2012 9:25:12 PM
```

The driverquery command generates a list of all hardware drivers installed in Windows. It's good for giving you a report about installed drivers that you can save for later reference or for investigating the version number of a currently installed driver so that you can make a better decision should you be thinking of updating.

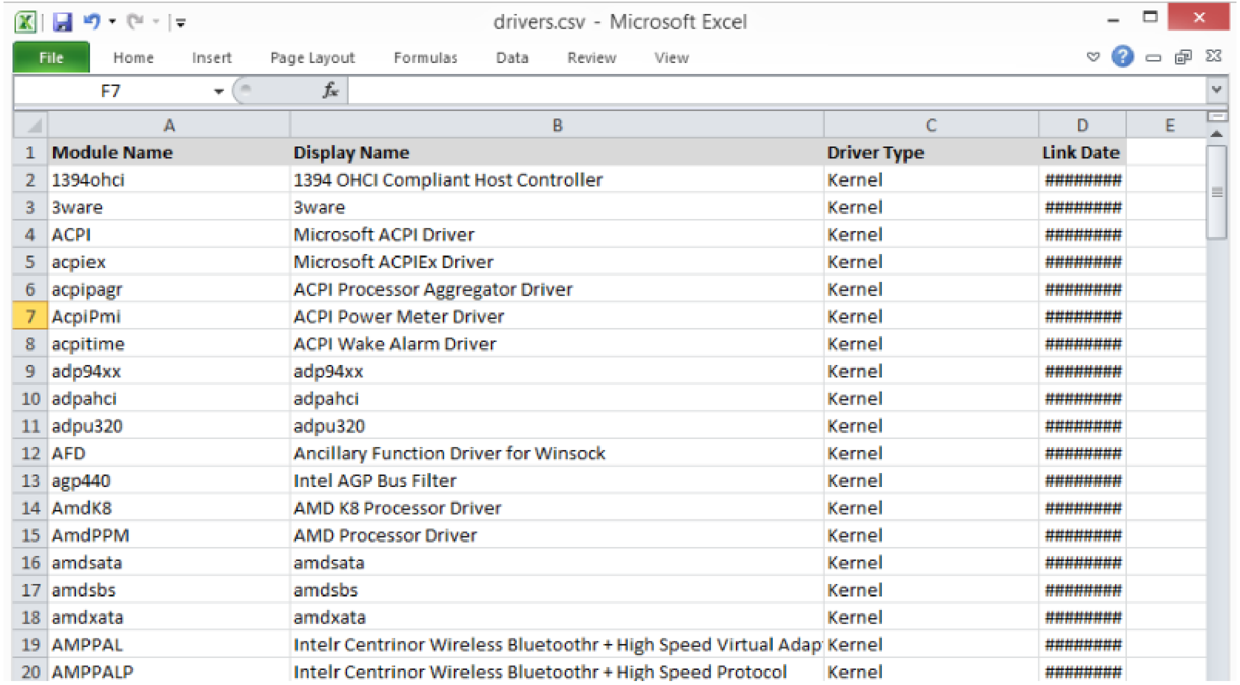
Typed by itself, `driverquery` just generates a list of drivers that you can scroll through. As usual, the power comes from the options you can add:

- **/s**. This option lets you specify the name or IP address of a remote computer so that you investigate the drivers it has installed.
- **/si**. This option shows you the digital signature information for drivers.
- **/fo**. This is really the key option you'll use with driverquery. It lets you specify the format in which information is displayed so that you can more effectively save it as a report. After typing /fo add one of the following options: TABLE (the default view), LIST (which lists each driver with all its information one after the other), and CSV (which shows data as comma separated values).

To save a report, you just need to pipe the information to a file instead of displaying it onscreen. To do that add `filename.extension` to the end of the command. Here's an example of perhaps the most useful way to use the command:

```
driverquery /fo CSV > drivers.csv
```

That queries all drivers, formats the result as comma separated values, and then saves them to a file named drivers.csv. You can then import that CSV file into Excel or another spreadsheet program to see a nicely-formatted report of all your installed drivers.



	A	B	C	D
1	**Module Name**	**Display Name**	**Driver Type**	**Link Date**
2	1394ohci	1394 OHCI Compliant Host Controller	Kernel	########
3	3ware	3ware	Kernel	########
4	ACPI	Microsoft ACPI Driver	Kernel	########
5	acpiex	Microsoft ACPIEx Driver	Kernel	########
6	acpipagr	ACPI Processor Aggregator Driver	Kernel	########
7	AcpiPmi	ACPI Power Meter Driver	Kernel	########
8	acpitime	ACPI Wake Alarm Driver	Kernel	########
9	adp94xx	adp94xx	Kernel	########
10	adpahci	adpahci	Kernel	########
11	adpu320	adpu320	Kernel	########
12	AFD	Ancillary Function Driver for Winsock	Kernel	########
13	agp440	Intel AGP Bus Filter	Kernel	########
14	AmdK8	AMD K8 Processor Driver	Kernel	########
15	AmdPPM	AMD Processor Driver	Kernel	########
16	amdsata	amdsata	Kernel	########
17	amdsbs	amdsbs	Kernel	########
18	amdxata	amdxata	Kernel	########
19	AMPPAL	Intelr Centrinor Wireless Bluetoothr + High Speed Virtual Adap	Kernel	########
20	AMPPALP	Intelr Centrinor Wireless Bluetoothr + High Speed Protocol	Kernel	########

Obviously, there are a lot more commands available to you at the Command Prompt. We didn't even cover every last option available with the commands in this article, just the stuff that we thought you might find useful. If you want to explore more of what's available at the Windows command line, you can't do better than starting right at the source. Microsoft TechNet has a full Command-Line Reference A-Z just waiting for you.

Photo by Dim Dimich (Shutterstock).