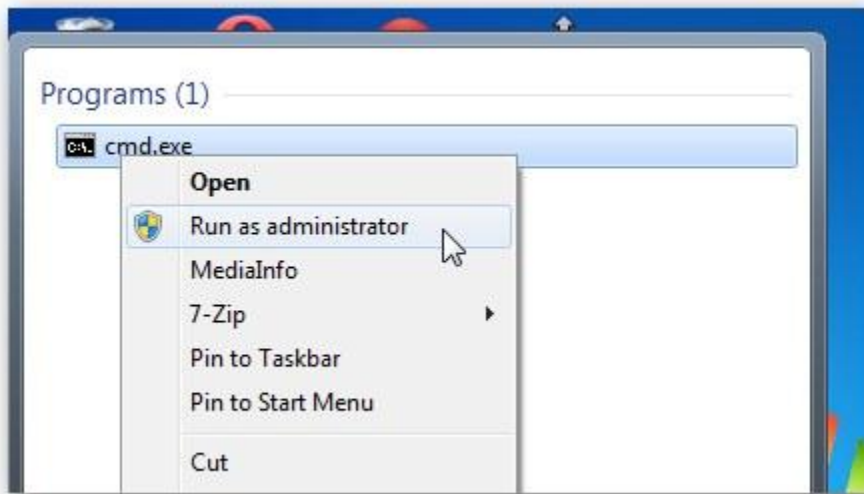


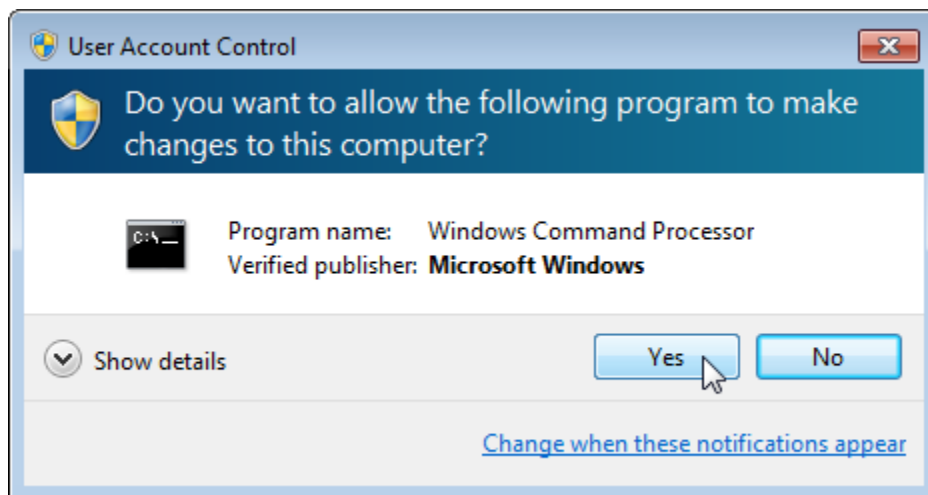
## How to Check What Your Computer is Connecting To

So, how do you find out what the problem is? There is an easy method using the netstat command from a command prompt window. This works with Windows 7, Vista, and XP. If you're still using XP, make sure you are running at least Service Pack 2.

We will use the netstat command to generate a list of everything that has made an internet connection in a specified amount of time. To use the netstat command, you must run the command prompt window as administrator. Open the Start menu and enter "cmd.exe" in the Search box. When the results display, right-click on cmd.exe and select Run as administrator from the popup menu.



If the User Account Control dialog box displays, click Yes to continue. Note: You may not see this dialog box, depending on your [User Account Control settings](#).

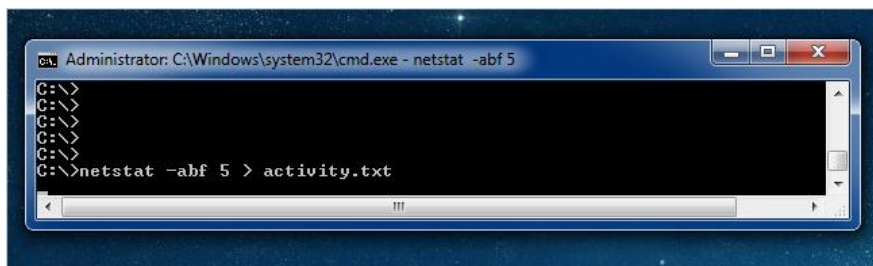


At the command prompt, type the following command and press Enter.

```
netstat -abf 5 > activity.txt
```

The `-a` option shows all connections and listening ports, the `-b` option shows you what application is making the connection, and the `-f` option displays the full DNS name for each connection option for easier understanding of where the connections are being made to. You can also use the `-n` option if you wish to only display the IP address. The 5 option will poll every 5 seconds for connections to make it more easy to track what is going on, and the results are then piped into the `activity.txt` file.

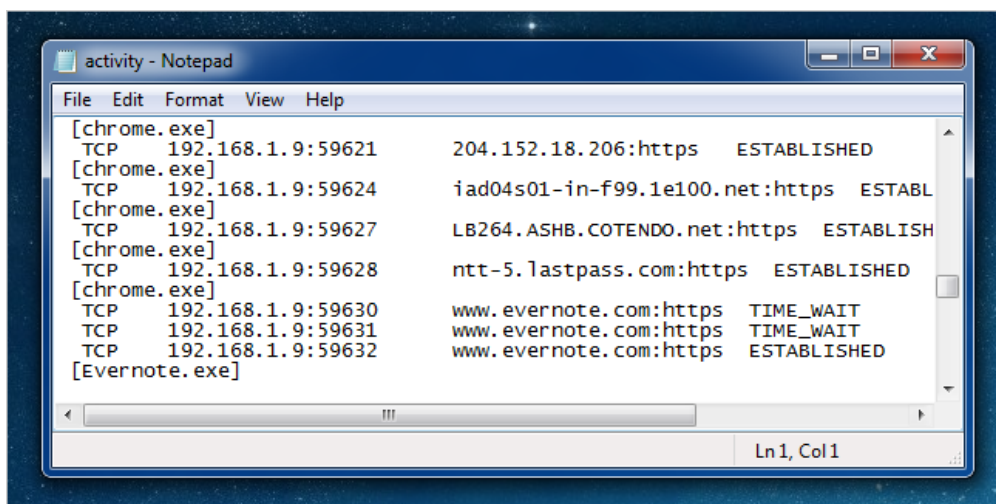
Wait about two minutes and then press `Ctrl + C` to stop the recording of data.



Once you've finished recording data, you can simply open the `activity.txt` file in your favorite editor to see the results, or you can type `activity.txt` at the command line to open it in Notepad.

The resulting file will list all processes on your computer (browsers, IM clients, email programs, etc.) that have made an internet connection in the last two minutes, or however long you waited before pressing `Ctrl + C`. It also lists which processes connected to which websites.

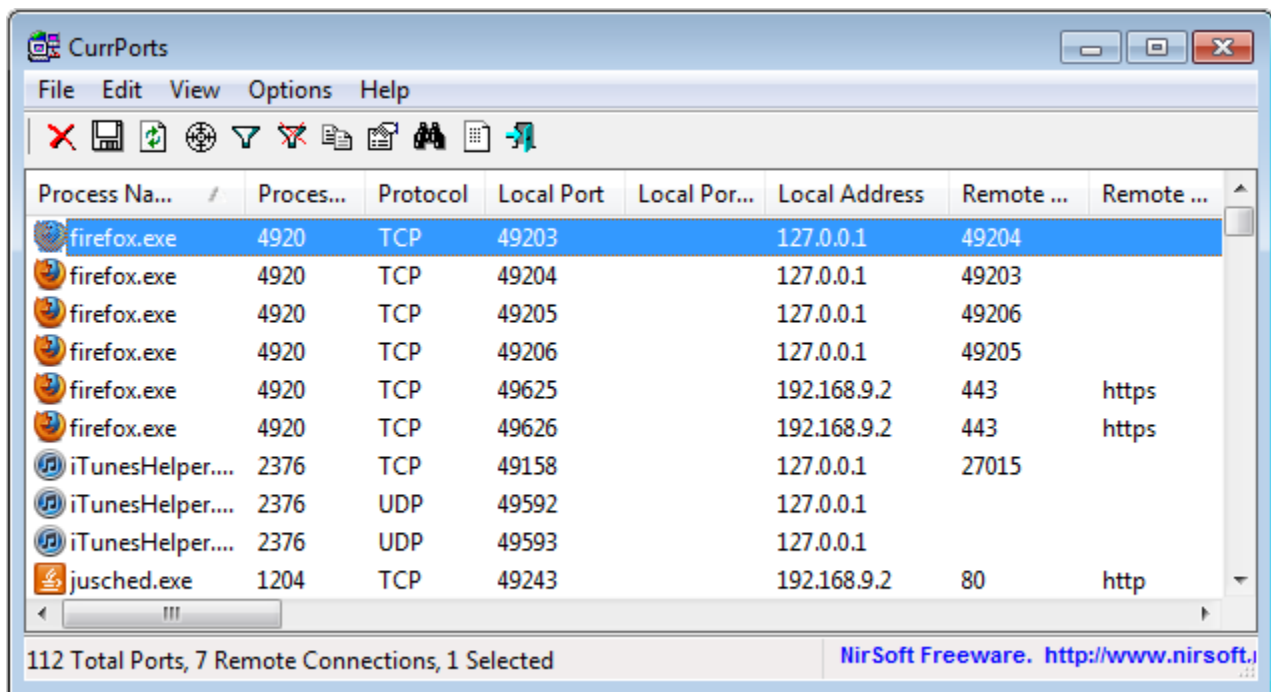
If you see process names or website addresses with which you are not familiar, you can search for "what is (name of unknown process)" in Google and see what it is. It may be a system function you don't know about or a function of one of your running programs. However, if it seems like a bad site, you can use Google again to find out how to get rid of it.



## Using CurrPorts to Check What Your PC is Connecting To

You can also use a free tool, called CurrPorts, to display a list of all currently opened TCP/IP and UDP ports on your local computer. It is a portable program and doesn't need to be installed. To use it, extract the .zip file you downloaded (see the link at the end of this article) and run cports.exe.

For each port that CurrPorts lists, information about the process that opened the port is displayed. You can select connections and close them, copy a port's information to the clipboard or save it to an HTML file, an XML file, or a tab-delimited text file. You can reorder the columns displayed on the CurrPorts main window and in the files you save. To sort the list by a specific column, simply click on the header of that column.



The screenshot shows the CurrPorts application window with a menu bar (File, Edit, View, Options, Help) and a toolbar. The main area contains a table of open ports and connections. The table has columns for Process Name, Process ID, Protocol, Local Port, Local Port (repeated), Local Address, Remote Port, and Remote Address. The status bar at the bottom indicates 112 total ports, 7 remote connections, and 1 selected.

| Process Na...    | Proces... | Protocol | Local Port | Local Por... | Local Address | Remote ... | Remote ... |
|------------------|-----------|----------|------------|--------------|---------------|------------|------------|
| firefox.exe      | 4920      | TCP      | 49203      |              | 127.0.0.1     | 49204      |            |
| firefox.exe      | 4920      | TCP      | 49204      |              | 127.0.0.1     | 49203      |            |
| firefox.exe      | 4920      | TCP      | 49205      |              | 127.0.0.1     | 49206      |            |
| firefox.exe      | 4920      | TCP      | 49206      |              | 127.0.0.1     | 49205      |            |
| firefox.exe      | 4920      | TCP      | 49625      |              | 192.168.9.2   | 443        | https      |
| firefox.exe      | 4920      | TCP      | 49626      |              | 192.168.9.2   | 443        | https      |
| iTunesHelper.... | 2376      | TCP      | 49158      |              | 127.0.0.1     | 27015      |            |
| iTunesHelper.... | 2376      | UDP      | 49592      |              | 127.0.0.1     |            |            |
| iTunesHelper.... | 2376      | UDP      | 49593      |              | 127.0.0.1     |            |            |
| jusched.exe      | 1204      | TCP      | 49243      |              | 192.168.9.2   | 80         | http       |

112 Total Ports, 7 Remote Connections, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

CurrPorts runs under Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista, and Windows 7. There is a separate download of CurrPorts for 64-bit versions of Windows. You can find more information about CurrPorts and how to use it on the website listed below.

Download CurrPorts from <http://www.nirsoft.net/utills/cports.html>.