

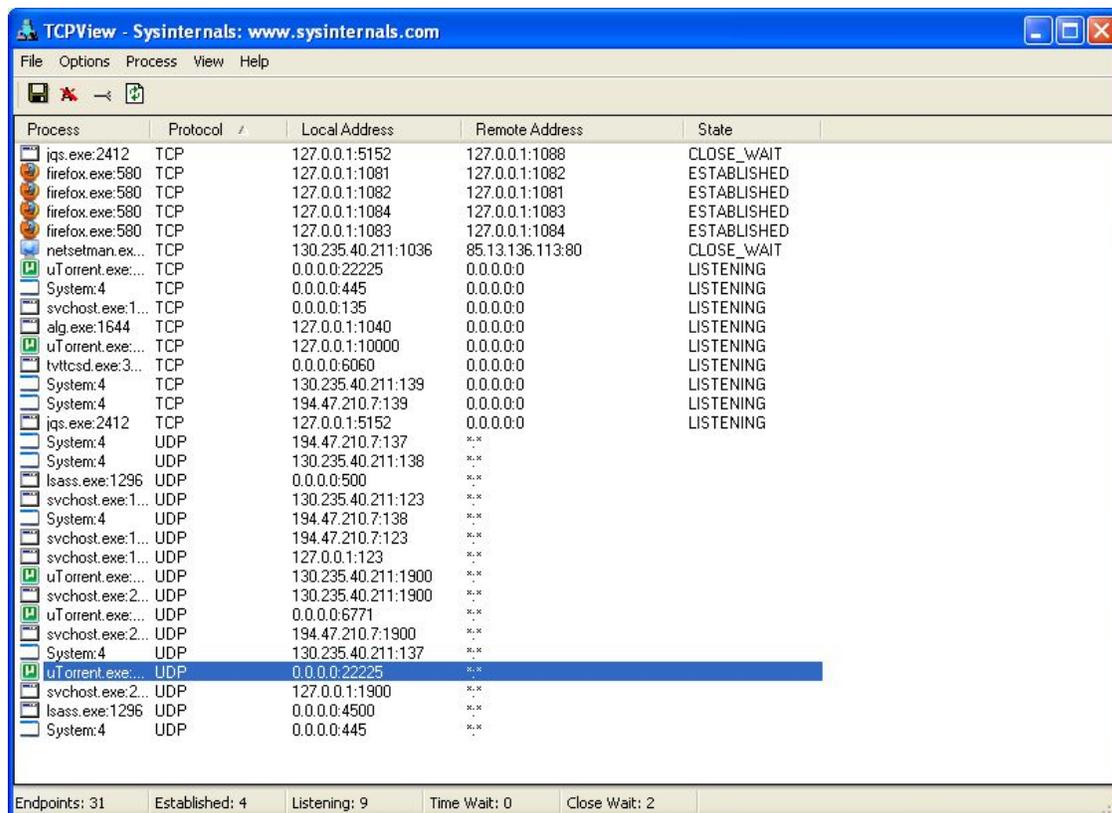
## My computer is blocked and I don't know why

If your computer gets blocked within 15 minutes from when you connect it to the network and you can't understand the reason why, it is almost always a Bittorrent client running on the computer. It can be included in other programs like "World of Warcraft" or "Steam" and startup automatically when the computer starts. This process can have a name that makes it hard to identify as a Bittorrent client.

If you think you have a program that use Bittorrent to update itself, you should check the setup and see if it is possible to change it to update by FTP or some other method.

You can use this method to identify a Bittorrent client on a PC running Windows:

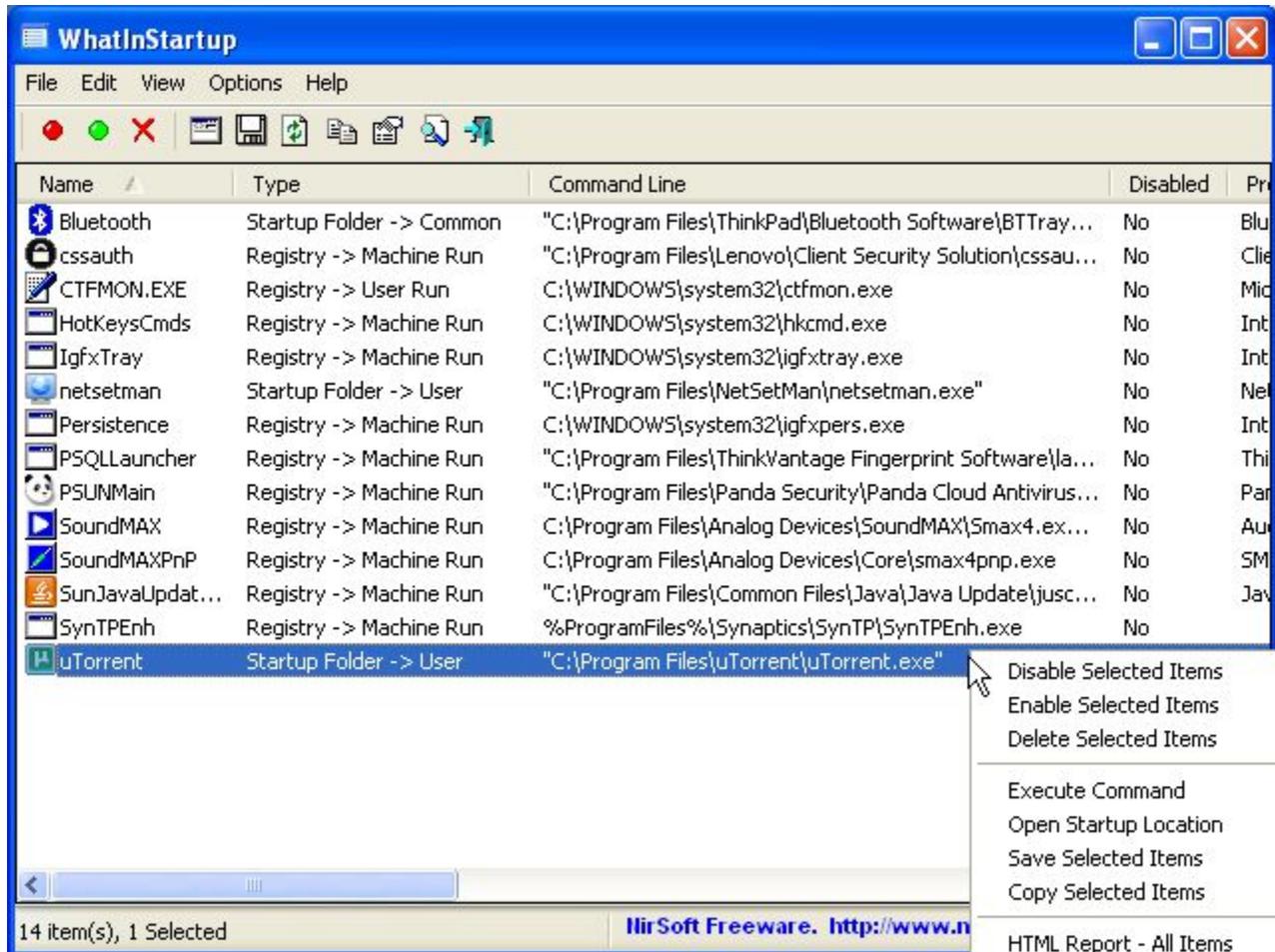
1. Turn off all programs you do not need to check like emailclients and webbrowsers
2. Fetch the program "[TCPview](http://technet.microsoft.com/sv-se/sysinternals/bb897437%28en-us%29.aspx)" (<http://technet.microsoft.com/sv-se/sysinternals/bb897437%28en-us%29.aspx>) from [Sysinternals](http://technet.microsoft.com/sv-se/sysinternals/default(en-us).aspx) ([http://technet.microsoft.com/sv-se/sysinternals/default\(en-us\).aspx](http://technet.microsoft.com/sv-se/sysinternals/default(en-us).aspx)) and run it. It is possible to run the program directly [over the network](#).
3. Click on the column "Protocol" to make it easy to see what programs that are running UDP traffic. There are normally fewer programs using UDP which makes it easier to find the Bittorrent client by this traffic.
4. Disregard Windows programs (like lsass.exe, svchost.exe, System) and identify the other programs by double clicking on the line. That will show you where the program is installed in your computer.



Process	Protocol	Local Address	Remote Address	State
iqs.exe:2412	TCP	127.0.0.1:5152	127.0.0.1:1088	CLOSE_WAIT
firefox.exe:580	TCP	127.0.0.1:1081	127.0.0.1:1082	ESTABLISHED
firefox.exe:580	TCP	127.0.0.1:1082	127.0.0.1:1081	ESTABLISHED
firefox.exe:580	TCP	127.0.0.1:1084	127.0.0.1:1083	ESTABLISHED
firefox.exe:580	TCP	127.0.0.1:1083	127.0.0.1:1084	ESTABLISHED
netsetman.exe...	TCP	130.235.40.211:1036	85.13.136.113:80	CLOSE_WAIT
uTorrent.exe:...	TCP	0.0.0.0:22225	0.0.0.0	LISTENING
System:4	TCP	0.0.0.0:445	0.0.0.0	LISTENING
svchost.exe:1...	TCP	0.0.0.0:135	0.0.0.0	LISTENING
alg.exe:1644	TCP	127.0.0.1:1040	0.0.0.0	LISTENING
uTorrent.exe:...	TCP	127.0.0.1:10000	0.0.0.0	LISTENING
tvttcsd.exe:3...	TCP	0.0.0.0:6060	0.0.0.0	LISTENING
System:4	TCP	130.235.40.211:139	0.0.0.0	LISTENING
System:4	TCP	194.47.210.7:139	0.0.0.0	LISTENING
iqs.exe:2412	TCP	127.0.0.1:5152	0.0.0.0	LISTENING
System:4	UDP	194.47.210.7:137	...	...
System:4	UDP	130.235.40.211:138	...	...
lsass.exe:1296	UDP	0.0.0.0:500	...	...
svchost.exe:1...	UDP	130.235.40.211:123	...	...
System:4	UDP	194.47.210.7:138	...	...
svchost.exe:1...	UDP	194.47.210.7:123	...	...
svchost.exe:1...	UDP	127.0.0.1:123	...	...
uTorrent.exe:...	UDP	130.235.40.211:1900	...	...
svchost.exe:2...	UDP	130.235.40.211:1900	...	...
uTorrent.exe:...	UDP	0.0.0.0:6771	...	...
svchost.exe:2...	UDP	194.47.210.7:1900	...	...
System:4	UDP	130.235.40.211:137	...	...
uTorrent.exe:...	UDP	0.0.0.0:22225	...	...
svchost.exe:2...	UDP	127.0.0.1:1900	...	...
lsass.exe:1296	UDP	0.0.0.0:4500	...	...
System:4	UDP	0.0.0.0:445	...	...

Endpoints: 31    Established: 4    Listening: 9    Time Wait: 0    Close Wait: 2

5. When you have identified the program you must try to find where it is started. You can use the program "[WhatInStartup](#)" from [Nirsoft](#) where you also can disable the automatic startup of the program. Another program that do the same thing is "[Autoruns](#)" from [Sysinternals](#) that also can be run [over the network](#). The program "WhatInStartup" is somewhat easier to work with.



ITsecurity, Lunds universitet (Security@lu.se)