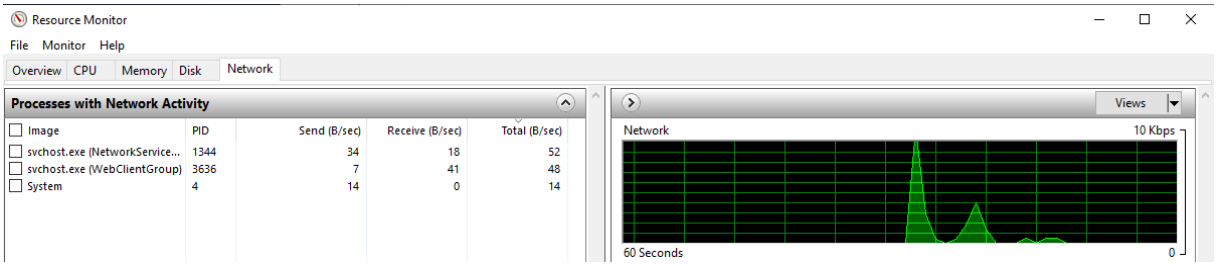
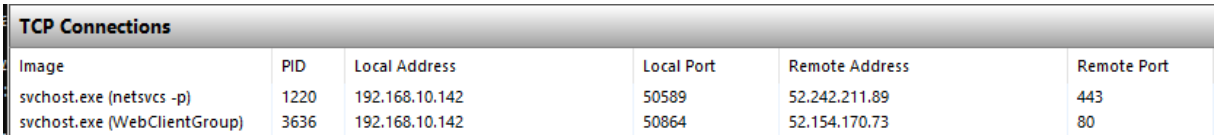
**TCPView**

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections. On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ships with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality." (official definition)

This is a good time to mention that Windows has a built-in utility that provides the same functionality. This tool is called Resource Monitor. There are many ways to open this tool. From the command line use **resmon.**

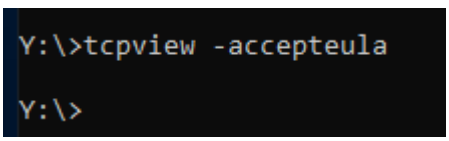



**Expand TCPConnectionsto view the Remote Address for each Process with an outbound connection.**

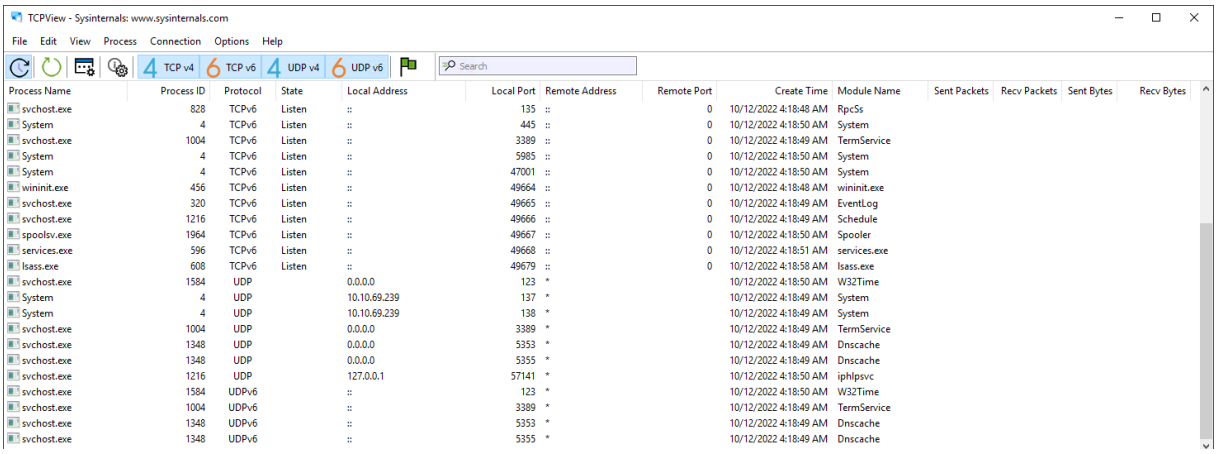



This tool can also be called from the Performance tab within Task Manager. Look at the bottom left for the link to open Resource Monitor.

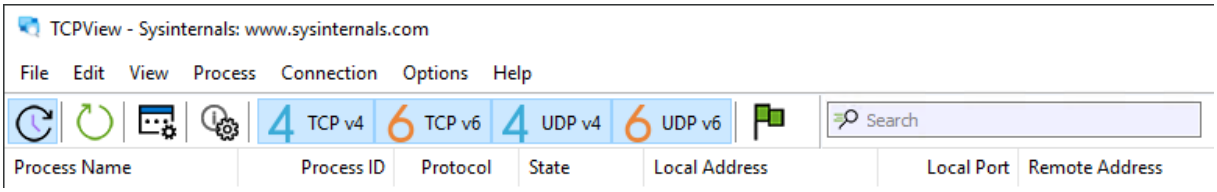

**Now back to TCPView.**



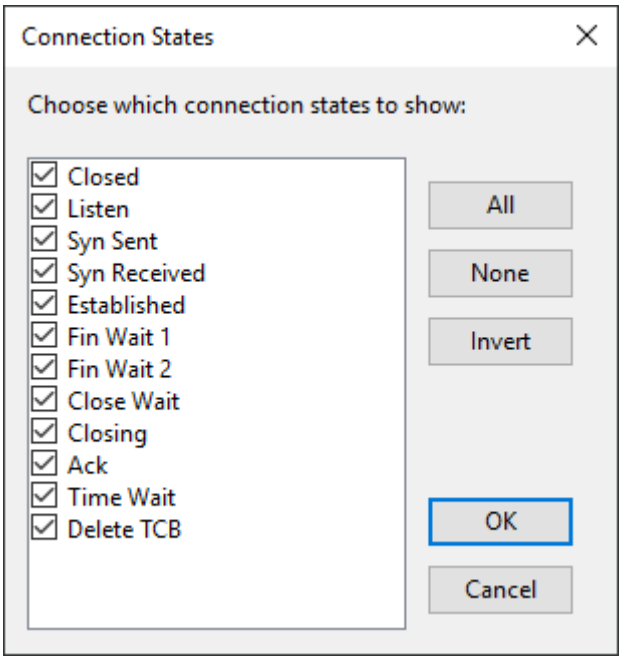

**The below image shows the default view for TCPView.**




**We can apply additional filtering by turning off TCP v4, TCP v6, UDPv4, and UDPv6 at the top toolbar, depending on which protocols we want to display. Moreover, we can click on the green flag to use the States Filter.**

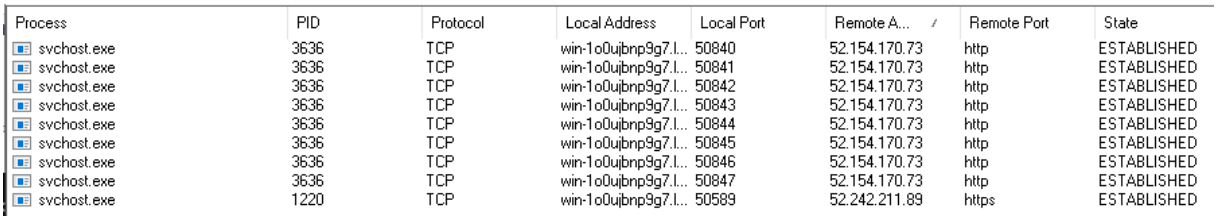



**Clicking the green flag opens the States Filter, which provides an extensive list of options to select which connection states we want to display. Most of the connection states available apply only to TCP connections. (UDP, being a connectionless protocol, cannot offer this flexibility in filtering.)**




**The list below shows all TCP v4 and TCP v6 connections in any state except in the "Listen" state. For instance, we notice that we have one TCP connection in an *Established* state and another connection in a *Close Wait* state.**

**In the below image, I unselected Listen in the Connection States from the States Filter and turned off UDPv4 and UDPv6 from the top toolbar.**



| Process | PID | Protocol | Local Address | Local Port | Remote A... | Remote Port | State |
|---|---|---|---|---|---|---|---|
| svchost.exe | 3636 | TCP | win-1o0ujbnp9g7.l... | 50840 | 52.154.170.73 | http | ESTABLISHED |
| svchost.exe | 3636 | TCP | win-1o0ujbnp9g7.l... | 50841 | 52.154.170.73 | http | ESTABLISHED |
| svchost.exe | 3636 | TCP | win-1o0ujbnp9g7.l... | 50842 | 52.154.170.73 | http | ESTABLISHED |
| svchost.exe | 3636 | TCP | win-1o0ujbnp9g7.l... | 50843 | 52.154.170.73 | http | ESTABLISHED |
| svchost.exe | 3636 | TCP | win-1o0ujbnp9g7.l... | 50844 | 52.154.170.73 | http | ESTABLISHED |
| svchost.exe | 3636 | TCP | win-1o0ujbnp9g7.l... | 50845 | 52.154.170.73 | http | ESTABLISHED |
| svchost.exe | 3636 | TCP | win-1o0ujbnp9g7.l... | 50846 | 52.154.170.73 | http | ESTABLISHED |
| svchost.exe | 3636 | TCP | win-1o0ujbnp9g7.l... | 50847 | 52.154.170.73 | http | ESTABLISHED |
| svchost.exe | 1220 | TCP | win-1o0ujbnp9g7.l... | 50589 | 52.242.211.89 | https | ESTABLISHED |

**Now the output only displays processes with an established outbound connection.**

**Other tools fall under the Networking Utilities category. I encourage you to explore these tools at your own leisure.**

**Link:**

**https://docs.microsoft.com/en-us/sysinternals/downloads/networking-utilities**