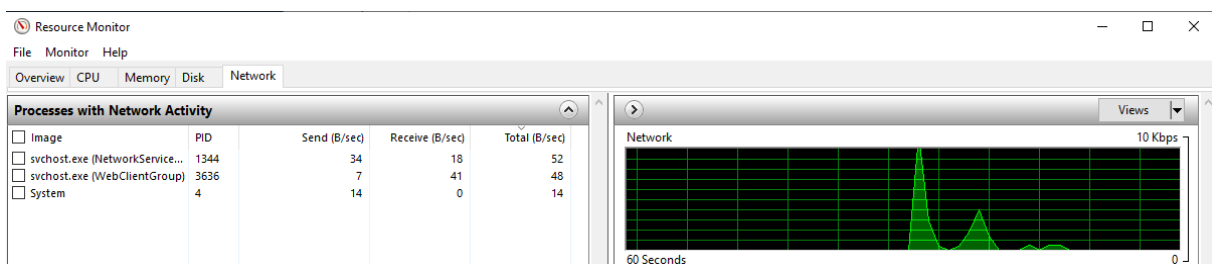


TCPView

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 TCPConnections to view the Remote Address for each Process with an outbound connection.

TCP Connections					
Image	PID	Local Address	Local Port	Remote Address	Remote Port
svchost.exe (netsh -p)	1220	192.168.10.142	50589	52.242.211.89	443
svchost.exe (WebClientGroup)	3636	192.168.10.142	50864	52.154.170.73	80

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.

Fewer details | [Open Resource Monitor](#)

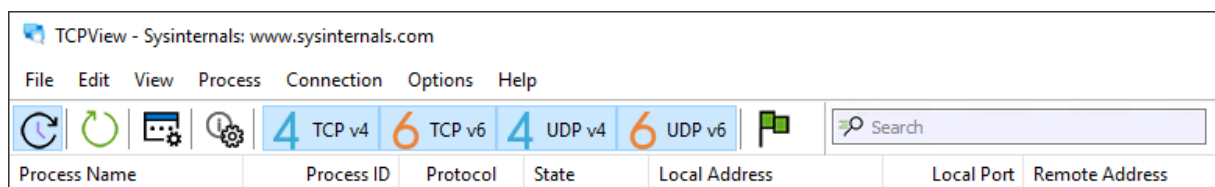
Now back to TCPView.

```
Y:\>tcpview -accepteula
Y:\>
```

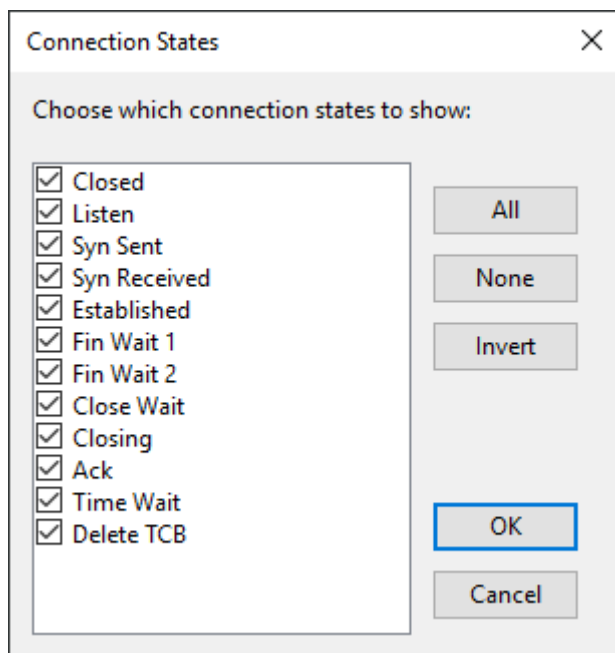
The below image shows the default view for TCPView.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets	Sent Bytes	Recv Bytes
svchost.exe	828	TCPv6	Listen	::	135	::	0	10/12/2022 4:18:48 AM	RpcSs				
System	4	TCPv6	Listen	::	445	::	0	10/12/2022 4:18:50 AM	System				
svchost.exe	1004	TCPv6	Listen	::	3389	::	0	10/12/2022 4:18:49 AM	TermService				
System	4	TCPv6	Listen	::	5985	::	0	10/12/2022 4:18:50 AM	System				
System	4	TCPv6	Listen	::	47001	::	0	10/12/2022 4:18:50 AM	System				
wininit.exe	456	TCPv6	Listen	::	49664	::	0	10/12/2022 4:18:48 AM	wininit.exe				
svchost.exe	320	TCPv6	Listen	::	49665	::	0	10/12/2022 4:18:49 AM	EventLog				
svchost.exe	1216	TCPv6	Listen	::	49666	::	0	10/12/2022 4:18:49 AM	Schedule				
spoolsv.exe	1964	TCPv6	Listen	::	49667	::	0	10/12/2022 4:18:50 AM	Spooler				
services.exe	596	TCPv6	Listen	::	49668	::	0	10/12/2022 4:18:51 AM	services.exe				
lsass.exe	608	TCPv6	Listen	::	49679	::	0	10/12/2022 4:18:58 AM	lsass.exe				
svchost.exe	1584	UDP		0.0.0.0	123	*		10/12/2022 4:18:50 AM	W32Time				
System	4	UDP		10.10.69.239	137	*		10/12/2022 4:18:49 AM	System				
System	4	UDP		10.10.69.239	138	*		10/12/2022 4:18:49 AM	System				
svchost.exe	1004	UDP		0.0.0.0	3389	*		10/12/2022 4:18:49 AM	TermService				
svchost.exe	1348	UDP		0.0.0.0	5353	*		10/12/2022 4:18:49 AM	Dnscache				
svchost.exe	1348	UDP		0.0.0.0	5355	*		10/12/2022 4:18:49 AM	Dnscache				
svchost.exe	1216	UDP		127.0.0.1	57141	*		10/12/2022 4:18:50 AM	iphlpvc				
svchost.exe	1584	UDPv6		::	123	*		10/12/2022 4:18:50 AM	W32Time				
svchost.exe	1004	UDPv6		::	3389	*		10/12/2022 4:18:49 AM	TermService				
svchost.exe	1348	UDPv6		::	5353	*		10/12/2022 4:18:49 AM	Dnscache				
svchost.exe	1348	UDPv6		::	5355	*		10/12/2022 4:18:49 AM	Dnscache				

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>