Link: https://www.tecchannel.de/a/tcpview-tcp-und-udp-verbindungen-analysieren,2019023

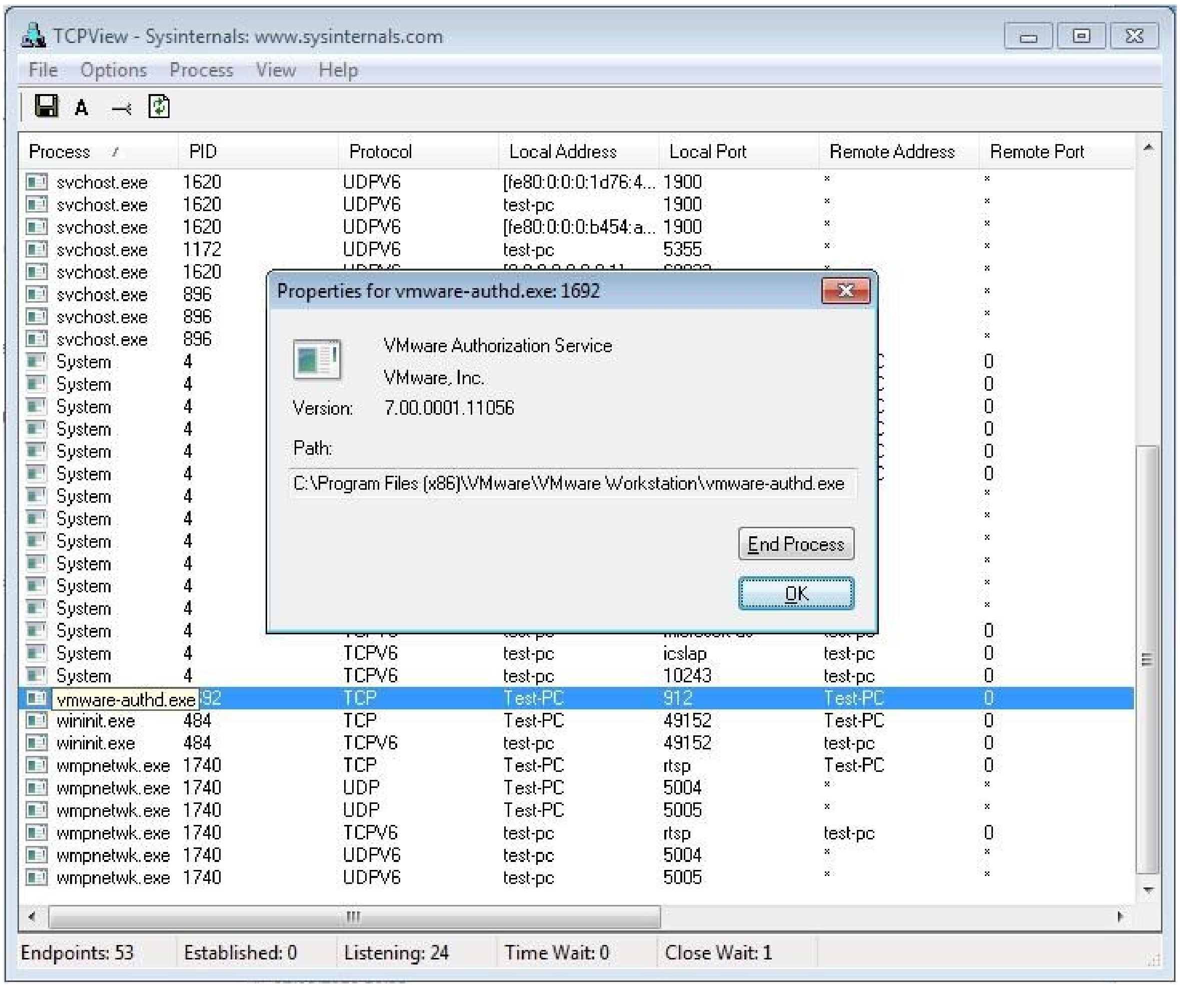
Kostenloses Netzwerk-Tool

TCPView - TCP- und UDP-Verbindungen analysieren

Datum: 30.08.2011
Autor(en): ALBERT LAUCHNER, Matthias Sternkopf

TCPView listet alle TCP- und UDP-Verbindungen eines Windows-Systems auf. Damit findet man schnell die Ursache für Verbindungsprobleme im Netzwerk. Auch geschwätzige Spyware lässt sich so enttarnen.

Funktionalität: Das Microsoft-Netzwerktool **TCPView**[1] listet alle Prozesse, die über das UDP- oder **TCP-Protokoll**[2] eine Datenverbindung im Netzwerk aufgebaut haben. Zu den angezeigten Informationen zählen die lokalen Adressen und Ports sowie die Remote-Adressen mit ihren Portnummern. Standardports setzt **TCPView** gleich in den passenden Klartextnamen wie etwa "https" um. Auch die Adressen kann TCPView optional in den Klartext-Domainnamen umwandeln.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
svchost.exe	1620	UDPV6	[fe80:0:0:0:1d76:4...	1900	*	*
svchost.exe	1620	UDPV6	test-pc	1900	*	*
svchost.exe	1620	UDPV6	[fe80:0:0:0:b454:a...	1900	*	*
svchost.exe	1172	UDPV6	test-pc	5355	*	*
svchost.exe	1620					*
svchost.exe	896					*
svchost.exe	896					*
svchost.exe	896					*
System	4					0
System	4					0
System	4					0
System	4					0
System	4					0
System	4					0
System	4					*
System	4					*
System	4					*
System	4					*
System	4					*
System	4					*
System	4					0
System	4	TCPV6	test-pc	icslap	test-pc	0
System	4	TCPV6	test-pc	10243	test-pc	0
vmware-authd.exe	92	TCP	Test-PC	912	Test-PC	0
wininit.exe	484	TCP	Test-PC	49152	Test-PC	0
wininit.exe	484	TCPV6	test-pc	49152	test-pc	0
wmpnetwk.exe	1740	TCP	Test-PC	rtsp	Test-PC	0
wmpnetwk.exe	1740	UDP	Test-PC	5004	*	*
wmpnetwk.exe	1740	UDP	Test-PC	5005	*	*
wmpnetwk.exe	1740	TCPV6	test-pc	rtsp	test-pc	0
wmpnetwk.exe	1740	UDPV6	test-pc	5004	*	*
wmpnetwk.exe	1740	UDPV6	test-pc	5005	*	*

Endpoints: 53 | Established: 0 | Listening: 24 | Time Wait: 0 | Close Wait: 1

Properties for vmware-authd.exe: 1692

VMware Authorization Service
VMware, Inc.
Version: 7.00.0001.11056
Path:
C:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe

Wer macht was: TCPView bietet eine Liste aller Prozesse mit einer TCP- oder UDP-Netzwerkverbindung.

Eine Statusinformation liefert zu jeder TCP-Verbindung den aktuellen Zustand wie etwa "Established" oder "Close_Wait". Zudem meldet TCPView den Namen und die Startparameter des Prozesses, der den Endpunkt besitzt.

Neue Endpunkte werden automatisch grün markiert, gelöschte dagegen rot. Die Endpunkte, die den Status von einem Update bis zum nächsten verändern, sind gelb markiert. TCPView wird in den Standardeinstellungen jede Sekunde aktualisiert. Dieses Intervall lässt sich jedoch über Optionen / Aktualisierungsrate auch manuell anpassen.

Installation: Nach dem **Download**[3] kann man ab **Windows XP**[4] das 284 KByte große TCPView ohne Installation direkt starten. Darüber hinaus liefert Microsoft mit TCPVcon auch eine Versionen für Kommandozeilennutzer.

[Hinweis auf Bildergalerie: **Bildergalerie: TCPView**] [gal1]

Fazit: Ein schnelles und schlankes Tool, das man bei Verbindungsproblemen zu Servern für den ersten Überblick immer einsetzen sollte. (ala/hal/mst)

TCPView für Windows

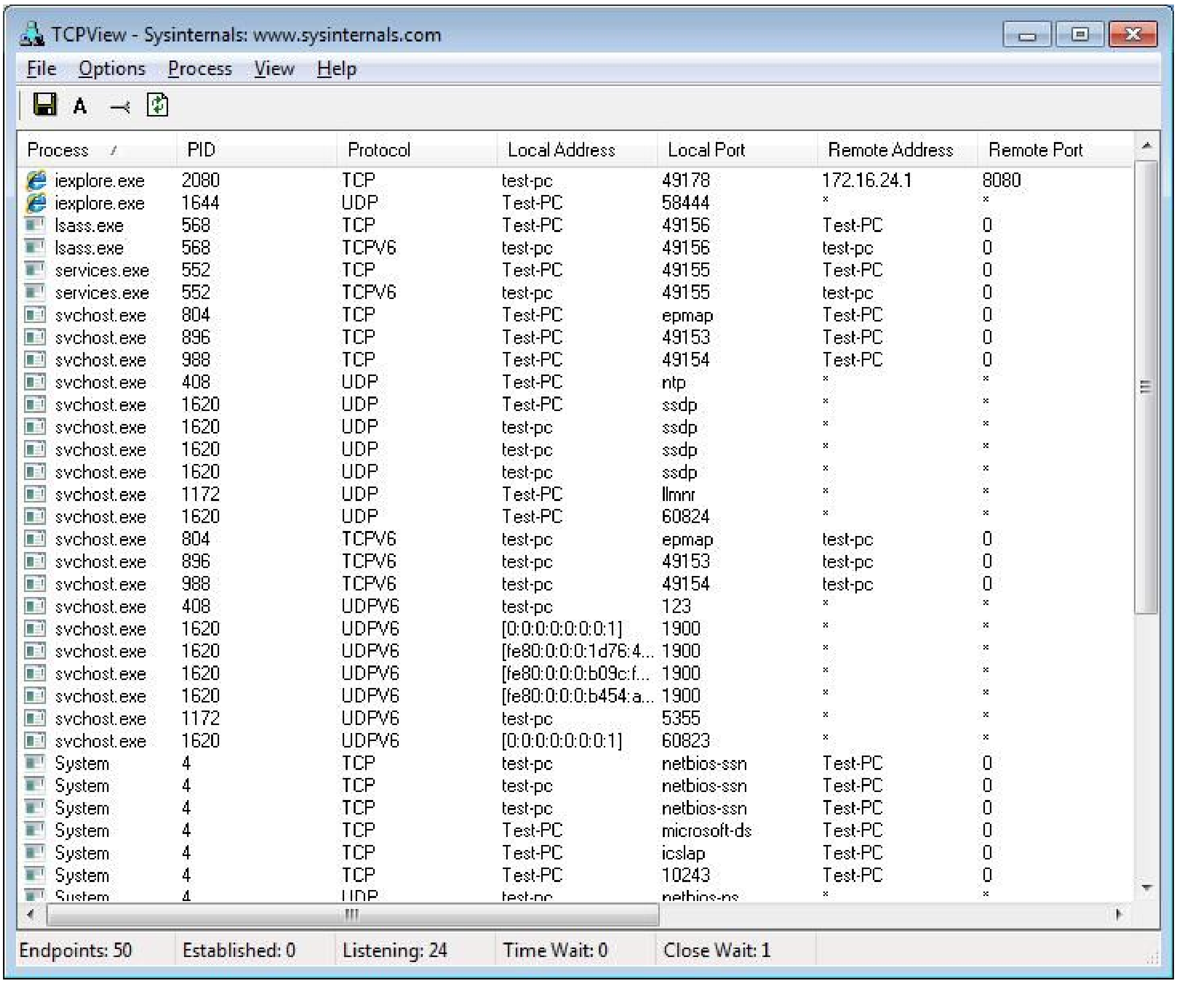
Version:	3.05
Hersteller:	**Microsoft / Mark Russinovich**[5]
Download Link:	**Herstellerseite**[6]
Sprache:	englisch
Preis:	kostenlos
System:	ab Windows XP
Alternative:	**Free Axence NetTools**[7]

Links im Artikel:

[1] **https://www.tecchannel.de/produkte/tools/netzwerk/tcpview/**
[2] **https://www.tecchannel.de/netzwerk/lan/401211/so_funktionieren_tcp_ip_und_ipv6/**
[3] **http://technet.microsoft.com/de-de/sysinternals/bb897437.aspx**
[4] **https://www.tecchannel.de/produkte/pc-mobil/betriebssystem/microsoft-windows-xp/**
[5] **http://technet.microsoft.com/de-de/sysinternals/bb897437.aspx**
[6] **http://technet.microsoft.com/de-de/sysinternals/bb897437.aspx**
[7] **http://www.axencesoftware.com/index.php?action=FreeNT**

Bildergalerien im Artikel:

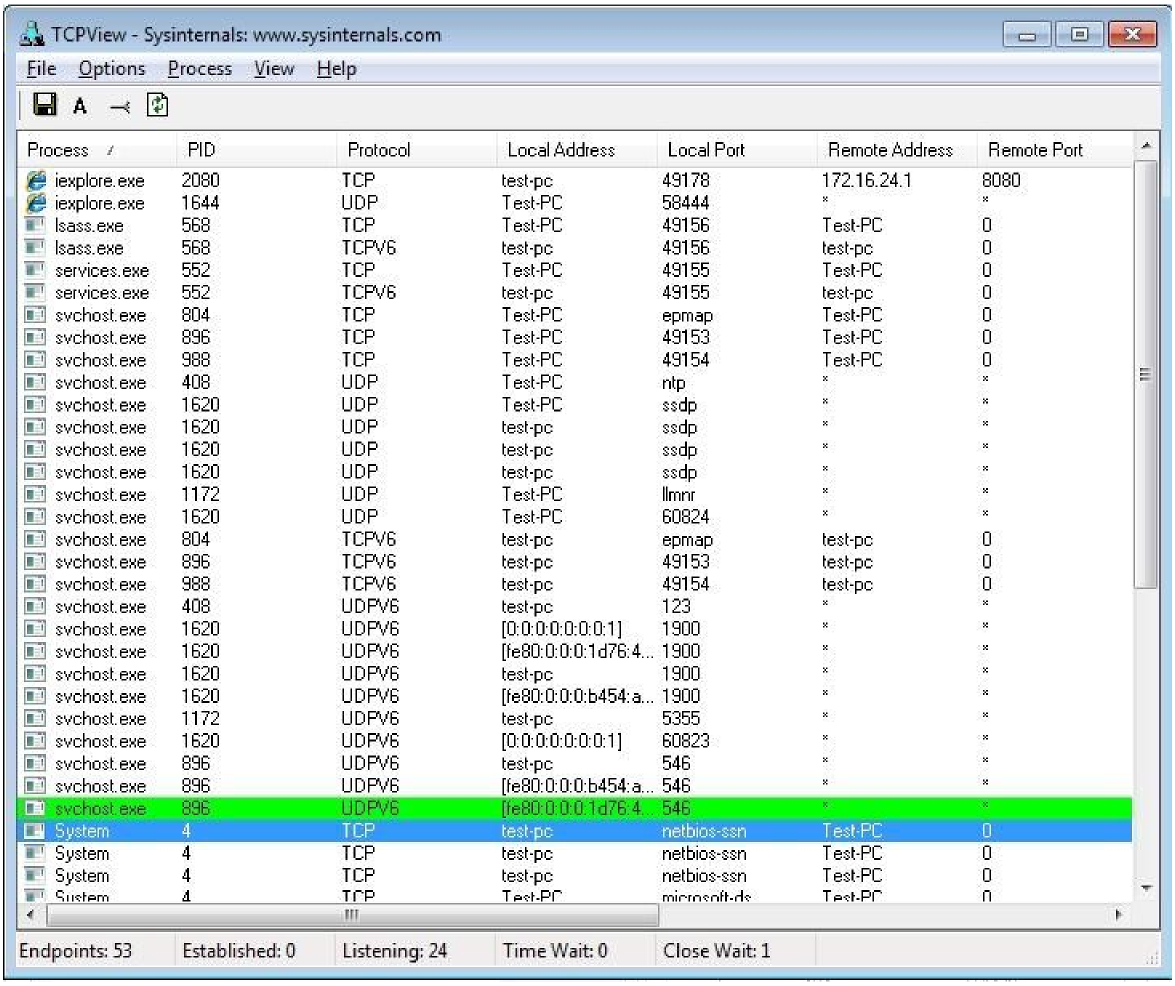
[gal1] **Bildergalerie: TCPView**



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
iexplore.exe	2080	TCP	test-pc	49178	172.16.24.1	8080
iexplore.exe	1644	UDP	Test-PC	58444	*	*
lsass.exe	568	TCP	Test-PC	49156	Test-PC	0
lsass.exe	568	TCPV6	test-pc	49156	test-pc	0
services.exe	552	TCP	Test-PC	49155	Test-PC	0
services.exe	552	TCPV6	test-pc	49155	test-pc	0
svchost.exe	804	TCP	Test-PC	epmap	Test-PC	0
svchost.exe	896	TCP	Test-PC	49153	Test-PC	0
svchost.exe	988	TCP	Test-PC	49154	Test-PC	0
svchost.exe	408	UDP	Test-PC	ntp	*	*
svchost.exe	1620	UDP	Test-PC	ssdp	*	*
svchost.exe	1620	UDP	test-pc	ssdp	*	*
svchost.exe	1620	UDP	test-pc	ssdp	*	*
svchost.exe	1620	UDP	test-pc	ssdp	*	*
svchost.exe	1172	UDP	Test-PC	llmnr	*	*
svchost.exe	1620	UDP	Test-PC	60824	*	*
svchost.exe	804	TCPV6	test-pc	epmap	test-pc	0
svchost.exe	896	TCPV6	test-pc	49153	test-pc	0
svchost.exe	988	TCPV6	test-pc	49154	test-pc	0
svchost.exe	408	UDPV6	test-pc	123	*	*
svchost.exe	1620	UDPV6	[0:0:0:0:0:0:0:1]	1900	*	*
svchost.exe	1620	UDPV6	[fe80:0:0:0:1d76:4...	1900	*	*
svchost.exe	1620	UDPV6	[fe80:0:0:0:b09c:f...	1900	*	*
svchost.exe	1620	UDPV6	[fe80:0:0:0:b454:a...	1900	*	*
svchost.exe	1172	UDPV6	test-pc	5355	*	*
svchost.exe	1620	UDPV6	[0:0:0:0:0:0:0:1]	60823	*	*
System	4	TCP	test-pc	netbios-ssn	Test-PC	0
System	4	TCP	test-pc	netbios-ssn	Test-PC	0
System	4	TCP	test-pc	netbios-ssn	Test-PC	0
System	4	TCP	Test-PC	microsoft-ds	Test-PC	0
System	4	TCP	Test-PC	icslap	Test-PC	0
System	4	TCP	Test-PC	10243	Test-PC	0
System	4	UDP	test-pc	netbios-ns	*	*

Endpoints: 50 | Established: 0 | Listening: 24 | Time Wait: 0 | Close Wait: 1

TCPView für Windows TCPView für Windows im Detail.

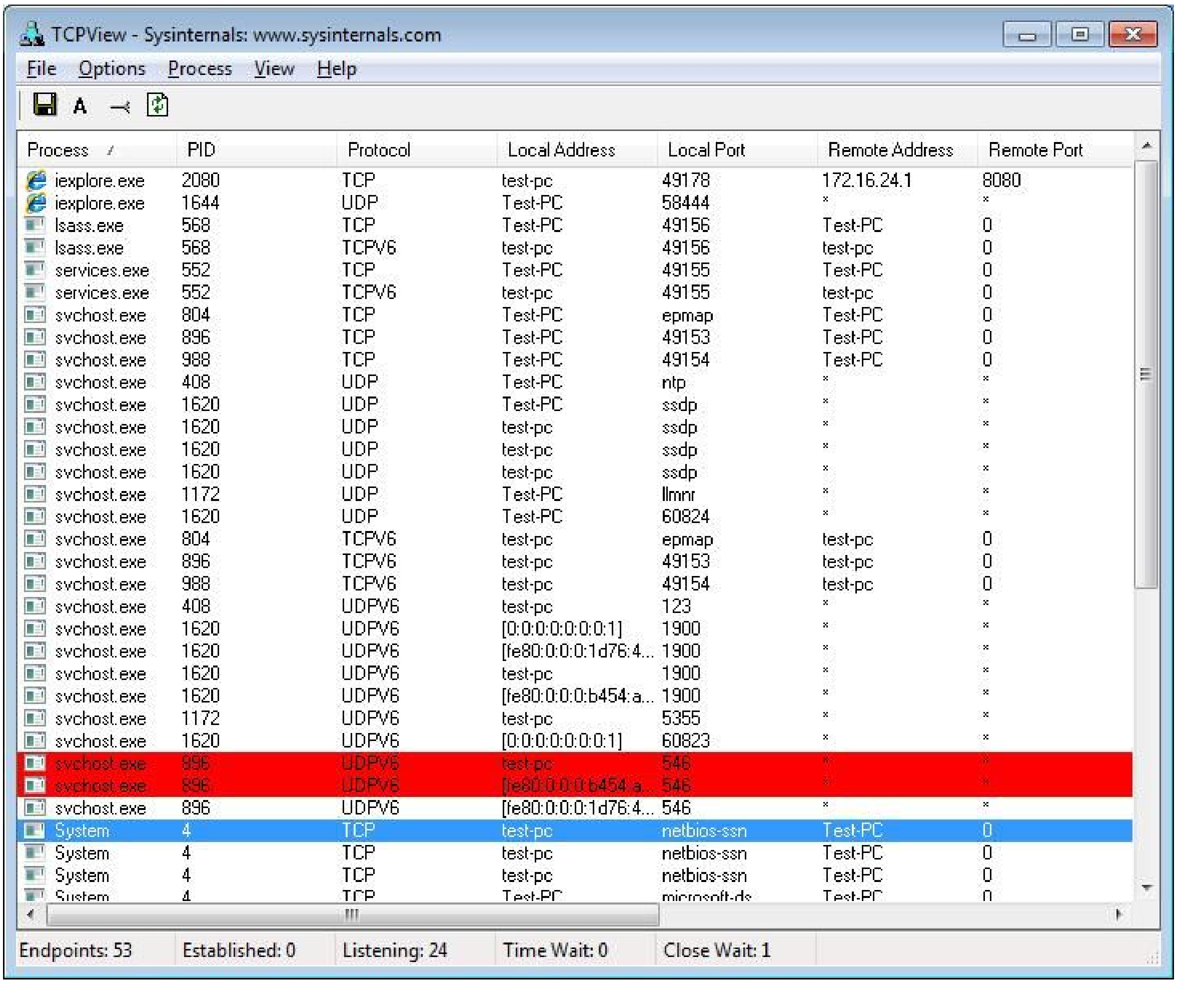


Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
iexplore.exe	2080	TCP	test-pc	49178	172.16.24.1	8080
iexplore.exe	1644	UDP	Test-PC	58444	*	*
lsass.exe	568	TCP	Test-PC	49156	Test-PC	0
lsass.exe	568	TCPV6	test-pc	49156	test-pc	0
services.exe	552	TCP	Test-PC	49155	Test-PC	0
services.exe	552	TCPV6	test-pc	49155	test-pc	0
svchost.exe	804	TCP	Test-PC	epmap	Test-PC	0
svchost.exe	896	TCP	Test-PC	49153	Test-PC	0
svchost.exe	988	TCP	Test-PC	49154	Test-PC	0
svchost.exe	408	UDP	Test-PC	ntp	*	*
svchost.exe	1620	UDP	Test-PC	ssdp	*	*
svchost.exe	1620	UDP	test-pc	ssdp	*	*
svchost.exe	1620	UDP	test-pc	ssdp	*	*
svchost.exe	1620	UDP	test-pc	ssdp	*	*
svchost.exe	1172	UDP	Test-PC	llmnr	*	*
svchost.exe	1620	UDP	Test-PC	60824	*	*
svchost.exe	804	TCPV6	test-pc	epmap	test-pc	0
svchost.exe	896	TCPV6	test-pc	49153	test-pc	0
svchost.exe	988	TCPV6	test-pc	49154	test-pc	0
svchost.exe	408	UDPV6	test-pc	123	*	*
svchost.exe	1620	UDPV6	[0:0:0:0:0:0:0:1]	1900	*	*
svchost.exe	1620	UDPV6	[fe80:0:0:0:1d76:4...	1900	*	*
svchost.exe	1620	UDPV6	test-pc	1900	*	*
svchost.exe	1620	UDPV6	[fe80:0:0:0:b454:a...	1900	*	*
svchost.exe	1172	UDPV6	test-pc	5355	*	*
svchost.exe	1620	UDPV6	[0:0:0:0:0:0:0:1]	60823	*	*
svchost.exe	896	UDPV6	test-pc	546	*	*
svchost.exe	896	UDPV6	[fe80:0:0:0:b454:a...	546	*	*
svchost.exe	896	UDPV6	[fe80:0:0:0:1d76:4...	546	*	*
System	4	TCP	test-pc	netbios-ssn	Test-PC	0
System	4	TCP	test-pc	netbios-ssn	Test-PC	0
System	4	TCP	test-pc	netbios-ssn	Test-PC	0
System	4	TCP	Test-PC	microsoft-ds	Test-PC	0

Endpoints: 53 | Established: 0 | Listening: 24 | Time Wait: 0 | Close Wait: 1

TCPView für Windows Neue Verbindungen werden in grün dargestellt.

TCPView für Windows

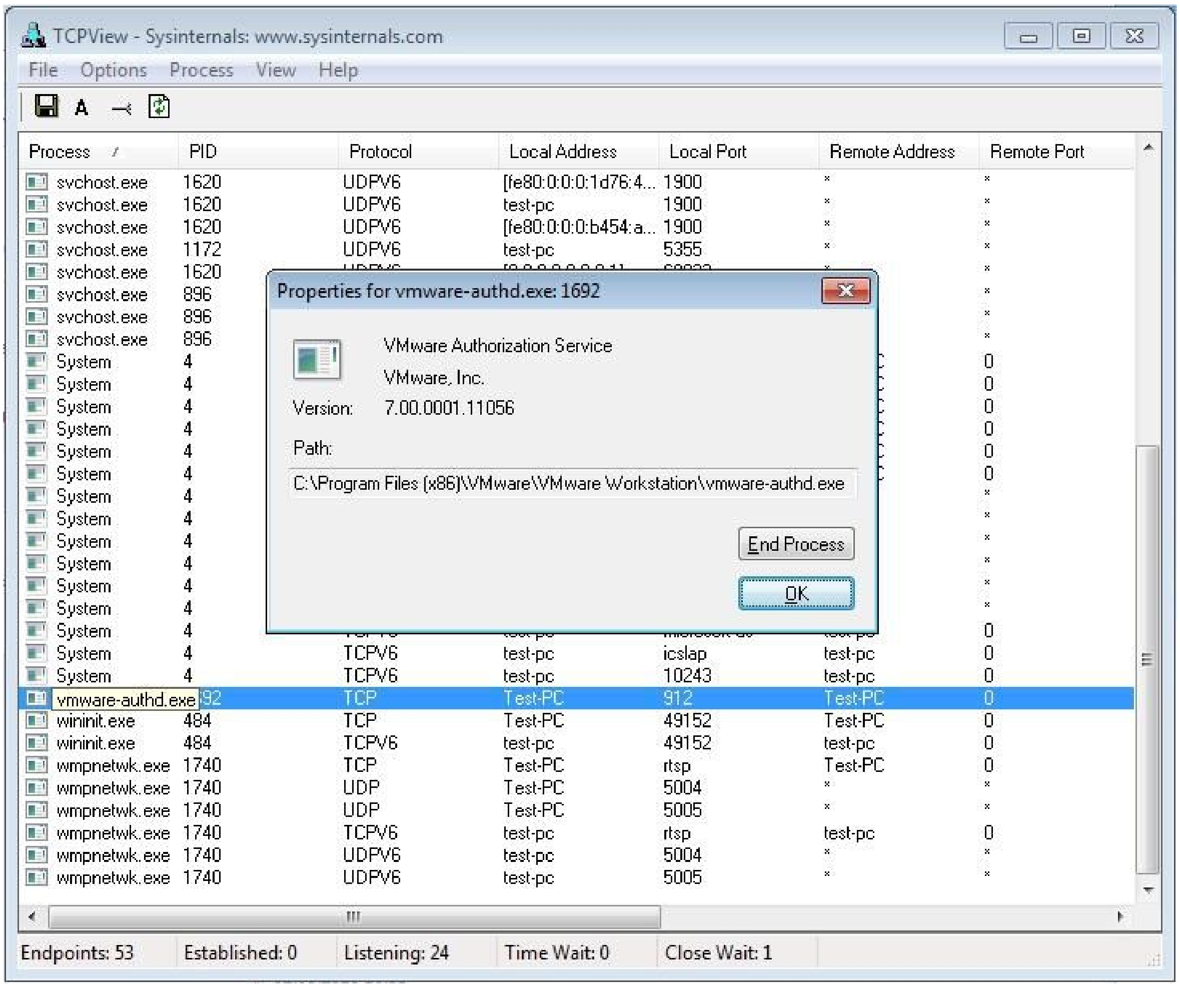

TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
iexplore.exe	2080	TCP	test-pc	49178	172.16.24.1	8080
iexplore.exe	1644	UDP	Test-PC	58444	*	*
lsass.exe	568	TCP	Test-PC	49156	Test-PC	0
lsass.exe	568	TCPV6	test-pc	49156	test-pc	0
services.exe	552	TCP	Test-PC	49155	Test-PC	0
services.exe	552	TCPV6	test-pc	49155	test-pc	0
svchost.exe	804	TCP	Test-PC	epmap	Test-PC	0
svchost.exe	896	TCP	Test-PC	49153	Test-PC	0
svchost.exe	988	TCP	Test-PC	49154	Test-PC	0
svchost.exe	408	UDP	Test-PC	ntp	*	*
svchost.exe	1620	UDP	Test-PC	ssdp	*	*
svchost.exe	1620	UDP	test-pc	ssdp	*	*
svchost.exe	1620	UDP	test-pc	ssdp	*	*
svchost.exe	1620	UDP	test-pc	ssdp	*	*
svchost.exe	1172	UDP	Test-PC	llmnr	*	*
svchost.exe	1620	UDP	Test-PC	60824	*	*
svchost.exe	804	TCPV6	test-pc	epmap	test-pc	0
svchost.exe	896	TCPV6	test-pc	49153	test-pc	0
svchost.exe	988	TCPV6	test-pc	49154	test-pc	0
svchost.exe	408	UDPV6	test-pc	123	*	*
svchost.exe	1620	UDPV6	[0:0:0:0:0:0:0:1]	1900	*	*
svchost.exe	1620	UDPV6	[fe80:0:0:0:1d76:4...	1900	*	*
svchost.exe	1620	UDPV6	test-pc	1900	*	*
svchost.exe	1620	UDPV6	[fe80:0:0:0:b454:a...	1900	*	*
svchost.exe	1172	UDPV6	test-pc	5355	*	*
svchost.exe	1620	UDPV6	[0:0:0:0:0:0:0:1]	60823	*	*
svchost.exe	896	UDPV6	test-pc	546	*	*
svchost.exe	896	UDPV6	[fe80:0:0:0:b454:a...	546	*	*
svchost.exe	896	UDPV6	[fe80:0:0:0:1d76:4...	546	*	*
System	4	TCP	test-pc	netbios-ssn	Test-PC	0
System	4	TCP	test-pc	netbios-ssn	Test-PC	0
System	4	TCP	test-pc	netbios-ssn	Test-PC	0
System	4	TCP	Test-PC	microsoft-ds	Test-PC	0

Endpoints: 53 | Established: 0 | Listening: 24 | Time Wait: 0 | Close Wait: 1

Terminierte Verbindungen werden in rot dargestellt.

TCPView für Windows


TCPView - Sysinternals: www.sysinternals.com
File Options Process View Help

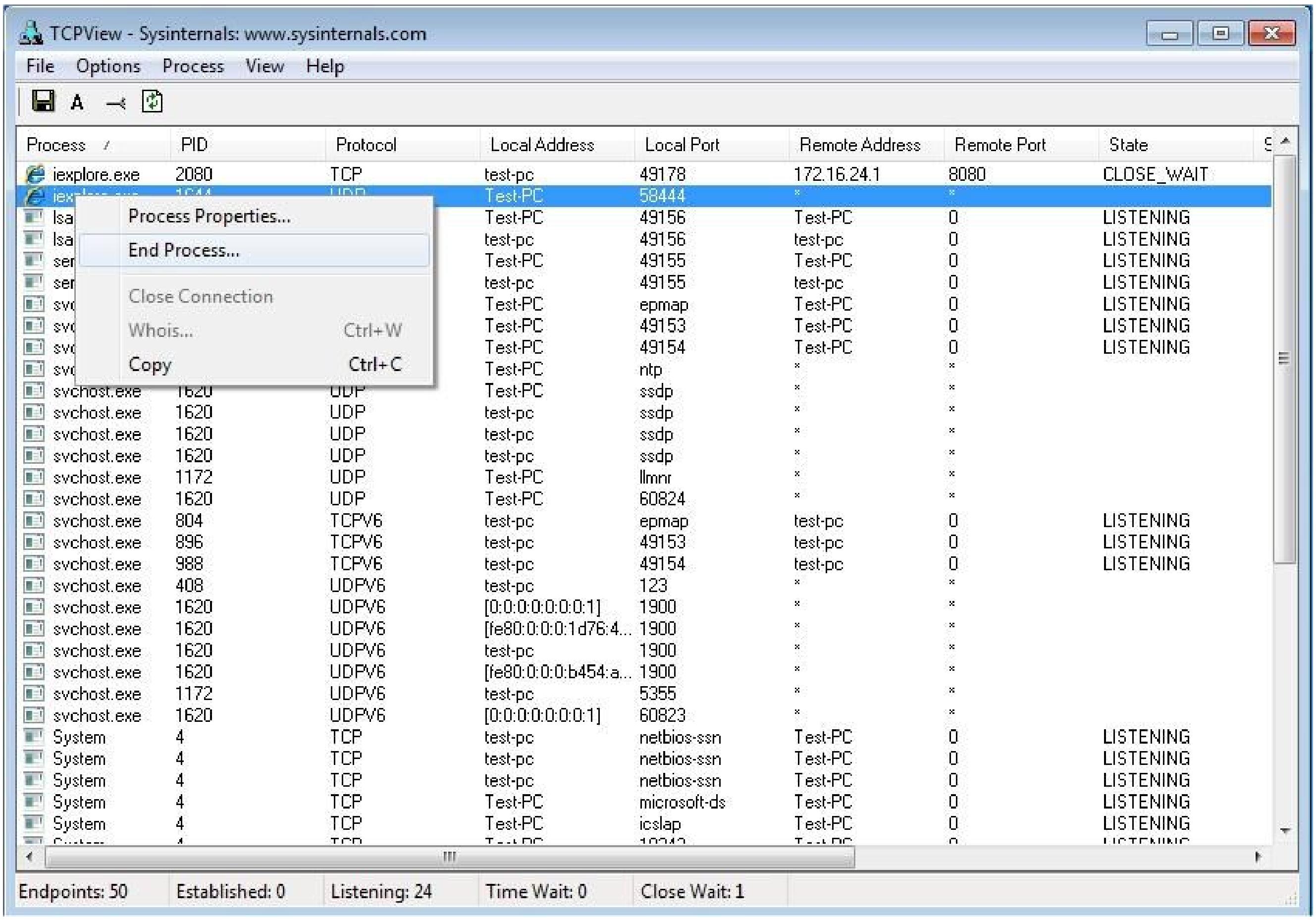
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
svchost.exe	1620	UDPV6	[fe80:0:0:0:1d76:4...	1900	*	*
svchost.exe	1620	UDPV6	test-pc	1900	*	*
svchost.exe	1620	UDPV6	[fe80:0:0:0:b454:a...	1900	*	*
svchost.exe	1172	UDPV6	test-pc	5355	*	*
svchost.exe	1620					*
svchost.exe	896					*
svchost.exe	896					*
svchost.exe	896					*
System	4					0
System	4					0
System	4					0
System	4					0
System	4					0
System	4					0
System	4					*
System	4					*
System	4					*
System	4					*
System	4					*
System	4					*
System	4					0
System	4	TCPV6	test-pc	icslap	test-pc	0
System	4	TCPV6	test-pc	10243	test-pc	0
vmware-authd.exe	92	TCP	Test-PC	912	Test-PC	0
wininit.exe	484	TCP	Test-PC	49152	Test-PC	0
wininit.exe	484	TCPV6	test-pc	49152	test-pc	0
wmpnetwk.exe	1740	TCP	Test-PC	rtsp	Test-PC	0
wmpnetwk.exe	1740	UDP	Test-PC	5004	*	*
wmpnetwk.exe	1740	UDP	Test-PC	5005	*	*
wmpnetwk.exe	1740	TCPV6	test-pc	rtsp	test-pc	0
wmpnetwk.exe	1740	UDPV6	test-pc	5004	*	*
wmpnetwk.exe	1740	UDPV6	test-pc	5005	*	*

Properties for vmware-authd.exe: 1692

VMware Authorization Service
VMware, Inc.
Version: 7.00.0001.11056
Path:
C:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe

Endpoints: 53 | Established: 0 | Listening: 24 | Time Wait: 0 | Close Wait: 1

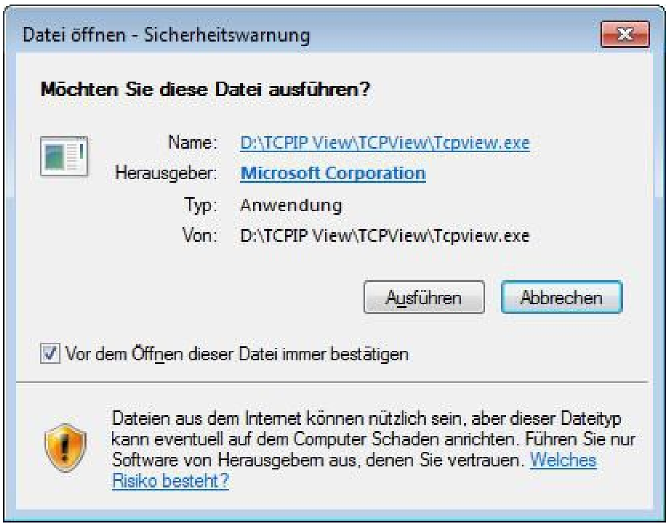
TCPVIew kann auch die Eigenschaften jedes Prozesess mit Netzwerkverbindung anzeigen.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
iexplore.exe	2080	TCP	test-pc	49178	172.16.24.1	8080	CLOSE_WAIT
iex			Test-PC	58444	*	*	
lsa			Test-PC	49156	Test-PC	0	LISTENING
lsa			test-pc	49156	test-pc	0	LISTENING
ser			Test-PC	49155	Test-PC	0	LISTENING
ser			test-pc	49155	test-pc	0	LISTENING
svc			Test-PC	epmap	Test-PC	0	LISTENING
svc			Test-PC	49153	Test-PC	0	LISTENING
svc			Test-PC	49154	Test-PC	0	LISTENING
svc			Test-PC	ntp	*	*	
svchost.exe	1620	UDP	Test-PC	ssdp	*	*	
svchost.exe	1620	UDP	test-pc	ssdp	*	*	
svchost.exe	1620	UDP	test-pc	ssdp	*	*	
svchost.exe	1620	UDP	test-pc	ssdp	*	*	
svchost.exe	1172	UDP	Test-PC	llmnr	*	*	
svchost.exe	1620	UDP	Test-PC	60824	*	*	
svchost.exe	804	TCPV6	test-pc	epmap	test-pc	0	LISTENING
svchost.exe	896	TCPV6	test-pc	49153	test-pc	0	LISTENING
svchost.exe	988	TCPV6	test-pc	49154	test-pc	0	LISTENING
svchost.exe	408	UDPV6	test-pc	123	*	*	
svchost.exe	1620	UDPV6	[0:0:0:0:0:0:0:1]	1900	*	*	
svchost.exe	1620	UDPV6	[fe80:0:0:0:1d76:4...	1900	*	*	
svchost.exe	1620	UDPV6	test-pc	1900	*	*	
svchost.exe	1620	UDPV6	[fe80:0:0:0:b454:a...	1900	*	*	
svchost.exe	1172	UDPV6	test-pc	5355	*	*	
svchost.exe	1620	UDPV6	[0:0:0:0:0:0:0:1]	60823	*	*	
System	4	TCP	test-pc	netbios-ssn	Test-PC	0	LISTENING
System	4	TCP	test-pc	netbios-ssn	Test-PC	0	LISTENING
System	4	TCP	test-pc	netbios-ssn	Test-PC	0	LISTENING
System	4	TCP	Test-PC	microsoft-ds	Test-PC	0	LISTENING
System	4	TCP	Test-PC	icslap	Test-PC	0	LISTENING

Endpoints: 50 Established: 0 Listening: 24 Time Wait: 0 Close Wait: 1

TCPView für Windows
Auf Wunsch kann man einen Prozess oder eine Verbindung abbrechen.



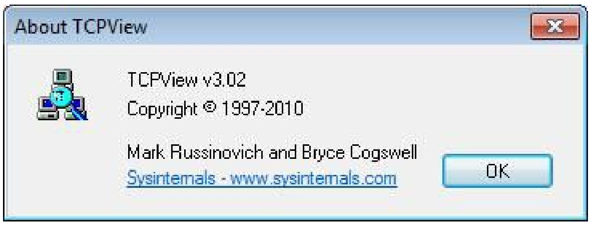
Möchten Sie diese Datei ausführen?

Name: D:\TCPIP View\TCPView\Tcpview.exe
Herausgeber: Microsoft Corporation
Typ: Anwendung
Von: D:\TCPIP View\TCPView\Tcpview.exe

☑ Vor dem Öffnen dieser Datei immer bestätigen

Dateien aus dem Internet können nützlich sein, aber dieser Dateityp kann eventuell auf dem Computer Schaden anrichten. Führen Sie nur Software von Herausgebern aus, denen Sie vertrauen. Welches Risiko besteht?

TCPView für Windows
Installation TCPView für Windows.



TCPView v3.02
Copyright © 1997-2010

Mark Russinovich and Bryce Cogswell
Sysinternals - www.sysinternals.com

TCPView für Windows
Versionsangabe TCPView für Windows.

IDG Tech Media GmbH
Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.