Paket Monitor Tool - pktmon

Das Tool Paket Monitor „pktmon.exe" macht im Grunde nichts anderes wie „netsh trace" oder andere kostenlose Tools.

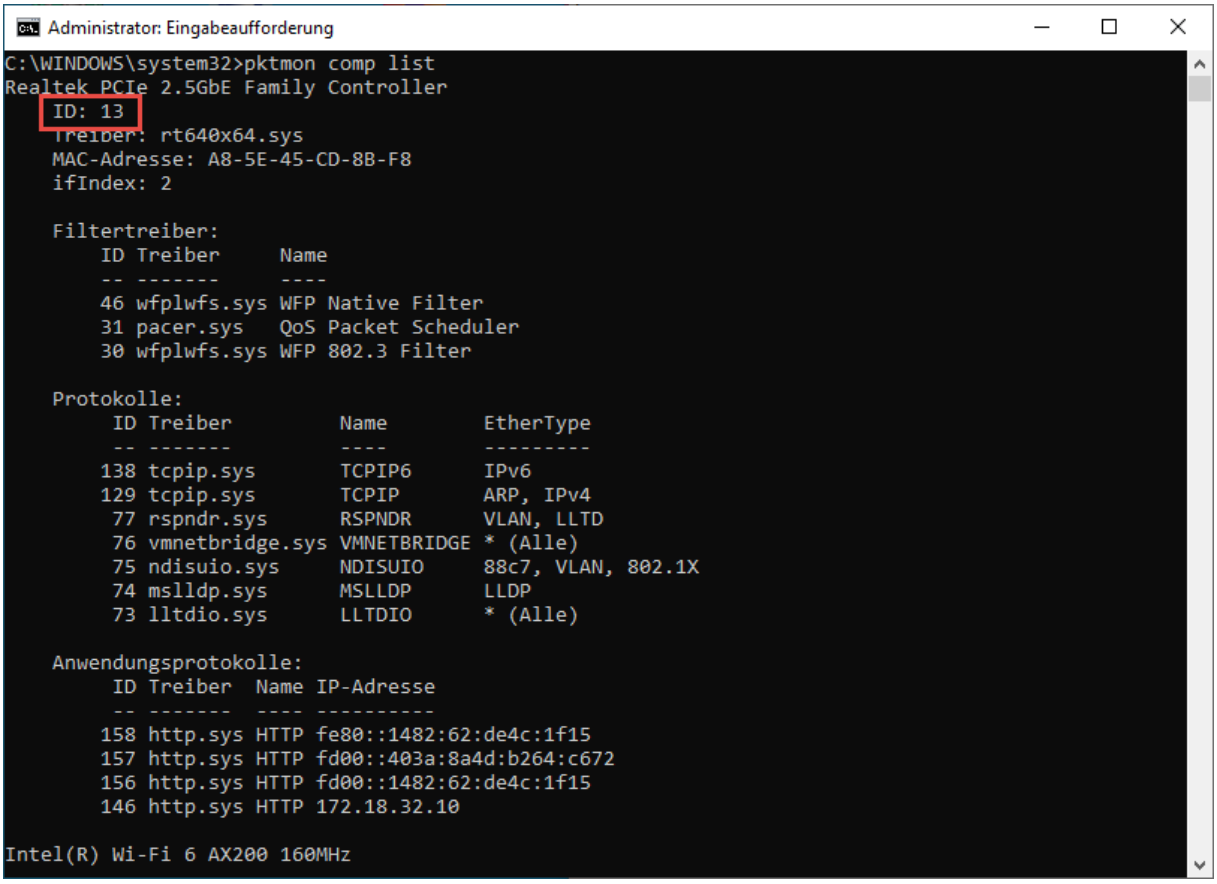
Zur Ausführung von pktmon gehen wir wie folgt vor:

Starten die CMD mit administrativen Rechten und lesen zuerst unsere vorhandene Netzwerkadapter aus.

Das machwir desewegen, um den Mitschnitt auf nur eine Schnittstelle zu begrenzen.

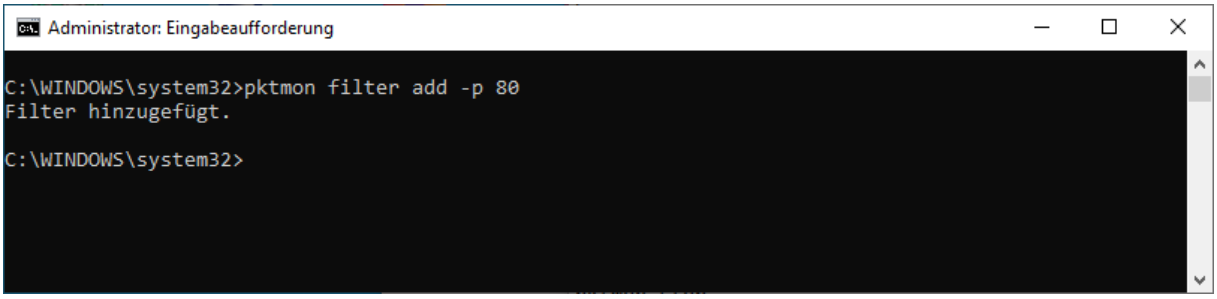
Meine Netzwerkkarte mit der ID 13 ist die aktive mit der ich auch ins Internet gehe.

pktmon comp list



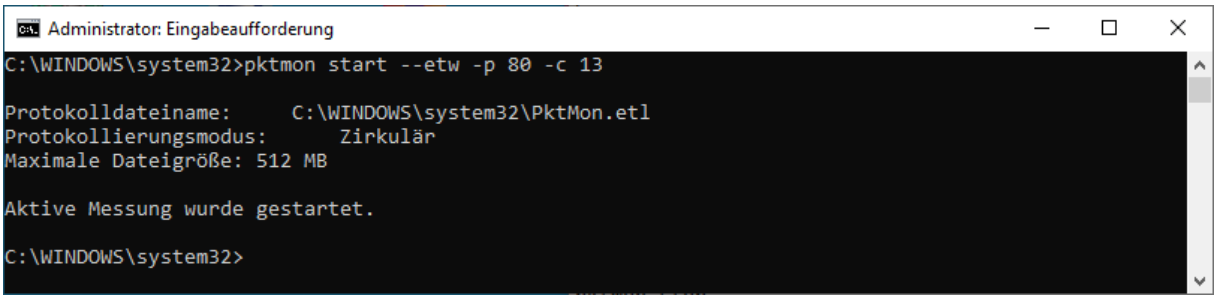
Danach setzen wir einen Filter auf Port 80 den wir überwachen wollen.

pktmon filter add -p 80



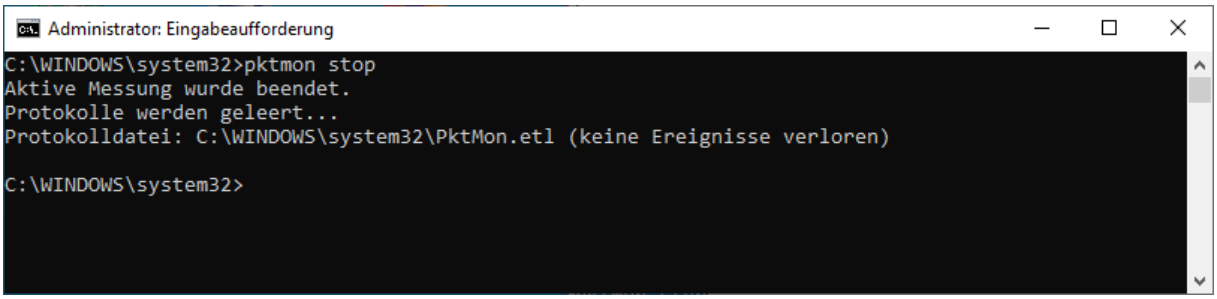
Danach starten wir die Paketaufzeichnung.

pktmon start --etw -p 80 -c 13



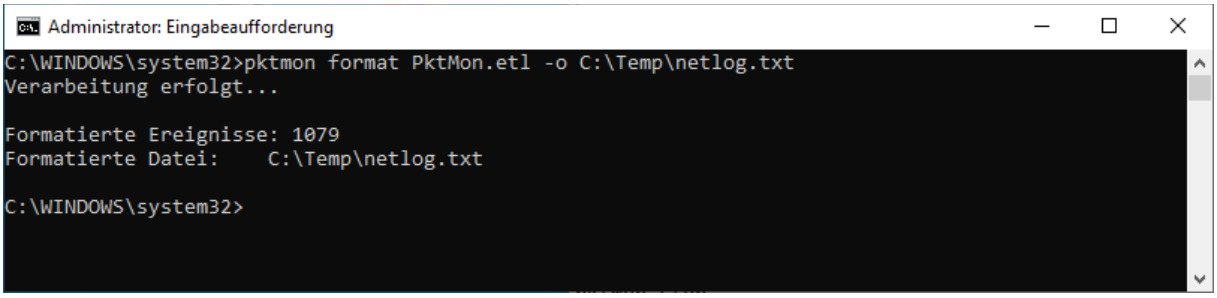
Beenden die Aufzeichnung.

pktmon stop



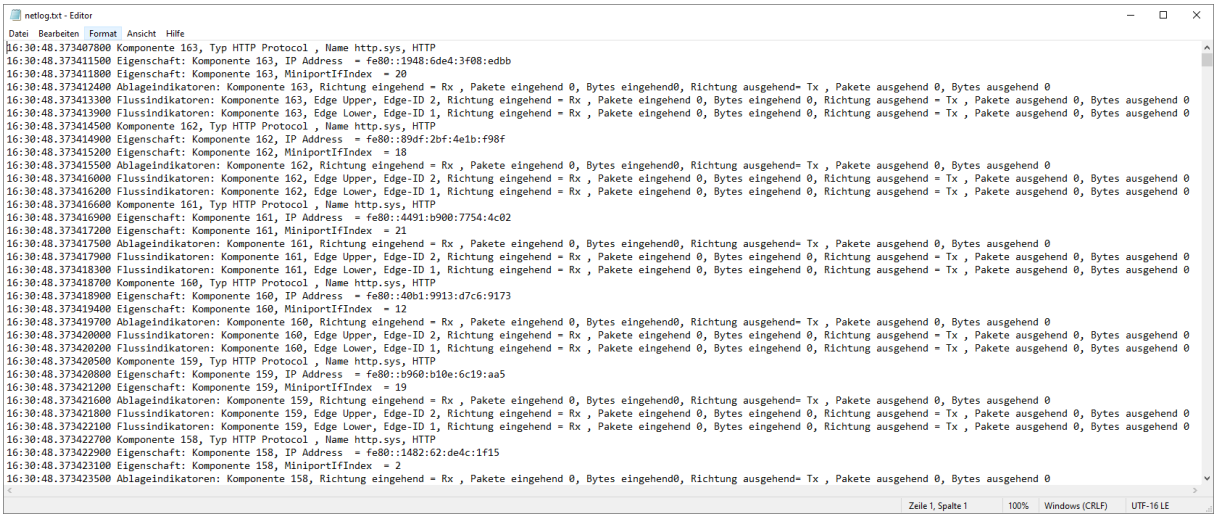
Sofern wir kein Tool zum Auslesen einer .etl Datei installiert haben, können wir diese auch in ein lesbares Format konvertieren.

pktmon format PktMon.etl -o C:\Temp\netlog443.txt

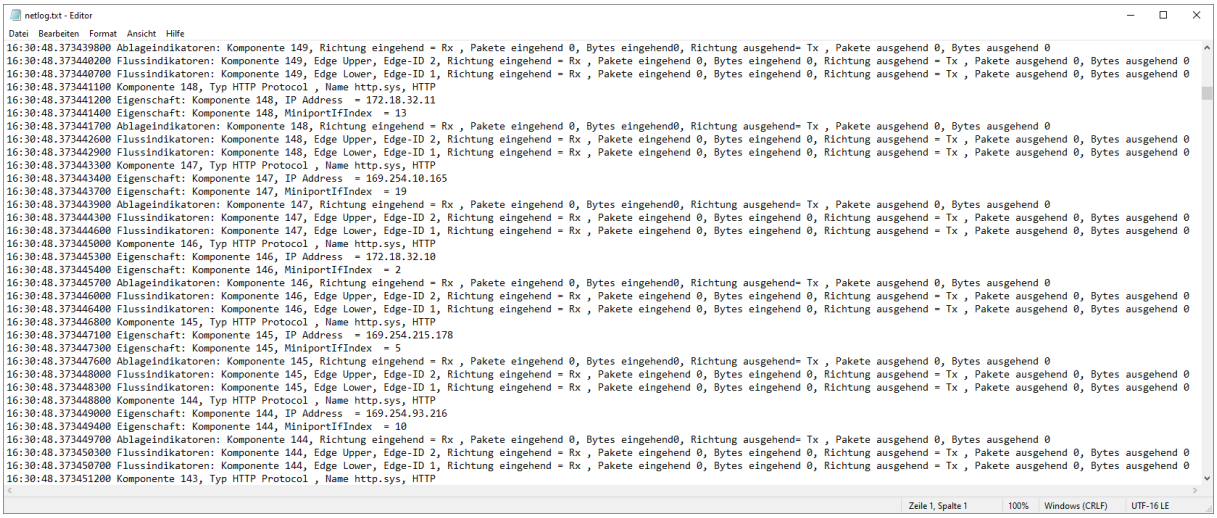


Paket Monitor Tool - pktmon

Umgewandelt sieht das Log wie folgt aus:

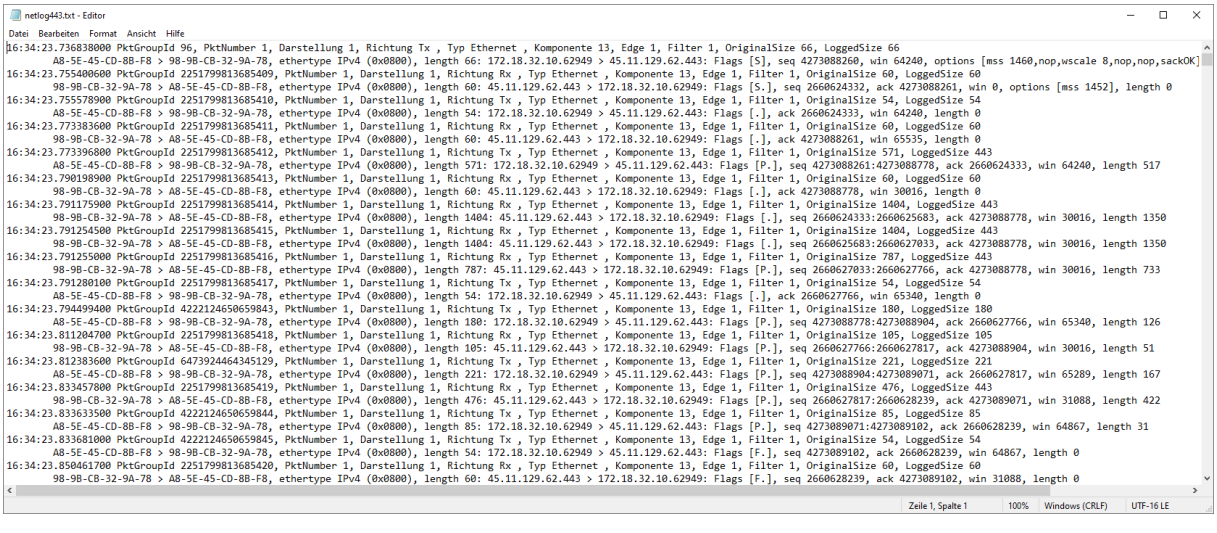


```
netlog.txt - Editor
Datei Bearbeiten Format Ansicht Hilfe
16:30:48.373407800 Komponente 163, Typ HTTP Protocol , Name http.sys, HTTP
16:30:48.373411500 Eigenschaft: Komponente 163, IP Address  = fe80::1948:6de4:3f08:edbb
16:30:48.373411800 Eigenschaft: Komponente 163, MiniportIfIndex  = 20
16:30:48.373412400 Ablageindikatoren: Komponente 163, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373413300 Flussindikatoren: Komponente 163, Edge Upper, Edge-ID 2, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373413900 Flussindikatoren: Komponente 163, Edge Lower, Edge-ID 1, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373414500 Komponente 162, Typ HTTP Protocol , Name http.sys, HTTP
16:30:48.373414900 Eigenschaft: Komponente 162, IP Address  = fe80::89df:2bf:4e1b:f98f
16:30:48.373415200 Eigenschaft: Komponente 162, MiniportIfIndex  = 18
16:30:48.373415500 Ablageindikatoren: Komponente 162, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373416000 Flussindikatoren: Komponente 162, Edge Upper, Edge-ID 2, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373416200 Flussindikatoren: Komponente 162, Edge Lower, Edge-ID 1, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373416600 Komponente 161, Typ HTTP Protocol , Name http.sys, HTTP
16:30:48.373416900 Eigenschaft: Komponente 161, IP Address  = fe80::4491:b900:7754:4c02
16:30:48.373417200 Eigenschaft: Komponente 161, MiniportIfIndex  = 21
16:30:48.373417500 Ablageindikatoren: Komponente 161, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373417900 Flussindikatoren: Komponente 161, Edge Upper, Edge-ID 2, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373418300 Flussindikatoren: Komponente 161, Edge Lower, Edge-ID 1, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373418700 Komponente 160, Typ HTTP Protocol , Name http.sys, HTTP
16:30:48.373418900 Eigenschaft: Komponente 160, IP Address  = fe80::40b1:9913:d7c6:9173
16:30:48.373419400 Eigenschaft: Komponente 160, MiniportIfIndex  = 12
16:30:48.373419700 Ablageindikatoren: Komponente 160, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373420000 Flussindikatoren: Komponente 160, Edge Upper, Edge-ID 2, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373420200 Flussindikatoren: Komponente 160, Edge Lower, Edge-ID 1, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373420500 Komponente 159, Typ HTTP Protocol , Name http.sys, HTTP
16:30:48.373420800 Eigenschaft: Komponente 159, IP Address  = fe80::b960:b10e:6c19:aa5
16:30:48.373421200 Eigenschaft: Komponente 159, MiniportIfIndex  = 19
16:30:48.373421600 Ablageindikatoren: Komponente 159, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373421800 Flussindikatoren: Komponente 159, Edge Upper, Edge-ID 2, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373422100 Flussindikatoren: Komponente 159, Edge Lower, Edge-ID 1, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373422700 Komponente 158, Typ HTTP Protocol , Name http.sys, HTTP
16:30:48.373422900 Eigenschaft: Komponente 158, IP Address  = fe80::1482:62:de4c:1f15
16:30:48.373423100 Eigenschaft: Komponente 158, MiniportIfIndex  = 2
16:30:48.373423500 Ablageindikatoren: Komponente 158, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
Zeile 1, Spalte 1  100%  Windows (CRLF)  UTF-16 LE
```



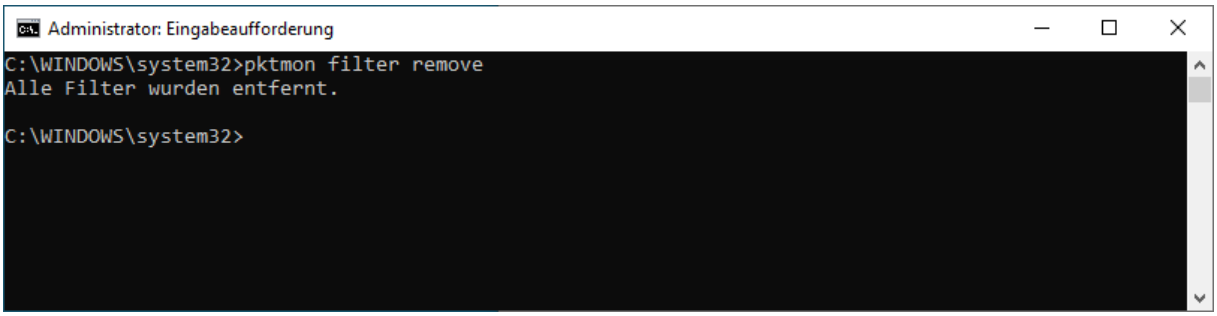
```
netlog.txt - Editor
Datei Bearbeiten Format Ansicht Hilfe
16:30:48.373439800 Ablageindikatoren: Komponente 149, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373440200 Flussindikatoren: Komponente 149, Edge Upper, Edge-ID 2, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373440700 Flussindikatoren: Komponente 149, Edge Lower, Edge-ID 1, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373441100 Komponente 148, Typ HTTP Protocol , Name http.sys, HTTP
16:30:48.373441200 Eigenschaft: Komponente 148, IP Address  = 172.18.32.11
16:30:48.373441400 Eigenschaft: Komponente 148, MiniportIfIndex  = 13
16:30:48.373441700 Ablageindikatoren: Komponente 148, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373442600 Flussindikatoren: Komponente 148, Edge Upper, Edge-ID 2, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373442900 Flussindikatoren: Komponente 148, Edge Lower, Edge-ID 1, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373443300 Komponente 147, Typ HTTP Protocol , Name http.sys, HTTP
16:30:48.373443400 Eigenschaft: Komponente 147, IP Address  = 169.254.10.165
16:30:48.373443700 Eigenschaft: Komponente 147, MiniportIfIndex  = 19
16:30:48.373443900 Ablageindikatoren: Komponente 147, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373444300 Flussindikatoren: Komponente 147, Edge Upper, Edge-ID 2, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373444600 Flussindikatoren: Komponente 147, Edge Lower, Edge-ID 1, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373445000 Komponente 146, Typ HTTP Protocol , Name http.sys, HTTP
16:30:48.373445300 Eigenschaft: Komponente 146, IP Address  = 172.18.32.10
16:30:48.373445400 Eigenschaft: Komponente 146, MiniportIfIndex  = 2
16:30:48.373445700 Ablageindikatoren: Komponente 146, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373446000 Flussindikatoren: Komponente 146, Edge Upper, Edge-ID 2, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373446400 Flussindikatoren: Komponente 146, Edge Lower, Edge-ID 1, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373446800 Komponente 145, Typ HTTP Protocol , Name http.sys, HTTP
16:30:48.373447100 Eigenschaft: Komponente 145, IP Address  = 169.254.215.178
16:30:48.373447300 Eigenschaft: Komponente 145, MiniportIfIndex  = 5
16:30:48.373447600 Ablageindikatoren: Komponente 145, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373448000 Flussindikatoren: Komponente 145, Edge Upper, Edge-ID 2, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373448300 Flussindikatoren: Komponente 145, Edge Lower, Edge-ID 1, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373448800 Komponente 144, Typ HTTP Protocol , Name http.sys, HTTP
16:30:48.373449000 Eigenschaft: Komponente 144, IP Address  = 169.254.93.216
16:30:48.373449400 Eigenschaft: Komponente 144, MiniportIfIndex  = 10
16:30:48.373449700 Ablageindikatoren: Komponente 144, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend0, Richtung ausgehend= Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373450300 Flussindikatoren: Komponente 144, Edge Upper, Edge-ID 2, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373450700 Flussindikatoren: Komponente 144, Edge Lower, Edge-ID 1, Richtung eingehend = Rx , Pakete eingehend 0, Bytes eingehend 0, Richtung ausgehend = Tx , Pakete ausgehend 0, Bytes ausgehend 0
16:30:48.373451200 Komponente 143, Typ HTTP Protocol , Name http.sys, HTTP
Zeile 1, Spalte 1  100%  Windows (CRLF)  UTF-16 LE
```

Den Filter auf den Port 443 begrenzt:



```
netlog443.txt - Editor
Datei Bearbeiten Format Ansicht Hilfe
16:34:23.736838000 PktGroupId 96, PktNumber 1, Darstellung 1, Richtung Tx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 66, LoggedSize 66
        A8-5E-45-CD-8B-F8 > 98-9B-CB-32-9A-78, ethertype IPv4 (0x0800), length 66: 172.18.32.10.62949 > 45.11.129.62.443: Flags [S], seq 4273088260, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK]
16:34:23.755400600 PktGroupId 2251799813685409, PktNumber 1, Darstellung 1, Richtung Rx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 60, LoggedSize 60
        98-9B-CB-32-9A-78 > A8-5E-45-CD-8B-F8, ethertype IPv4 (0x0800), length 60: 45.11.129.62.443 > 172.18.32.10.62949: Flags [S.], seq 2660624332, ack 4273088261, win 0, options [mss 1452], length 0
16:34:23.755578900 PktGroupId 2251799813685410, PktNumber 1, Darstellung 1, Richtung Tx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 54, LoggedSize 54
        A8-5E-45-CD-8B-F8 > 98-9B-CB-32-9A-78, ethertype IPv4 (0x0800), length 54: 172.18.32.10.62949 > 45.11.129.62.443: Flags [.], ack 2660624333, win 64240, length 0
16:34:23.773383600 PktGroupId 2251799813685411, PktNumber 1, Darstellung 1, Richtung Rx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 60, LoggedSize 60
        98-9B-CB-32-9A-78 > A8-5E-45-CD-8B-F8, ethertype IPv4 (0x0800), length 60: 45.11.129.62.443 > 172.18.32.10.62949: Flags [.], ack 4273088261, win 65535, length 0
16:34:23.773396800 PktGroupId 2251799813685412, PktNumber 1, Darstellung 1, Richtung Tx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 571, LoggedSize 443
        A8-5E-45-CD-8B-F8 > 98-9B-CB-32-9A-78, ethertype IPv4 (0x0800), length 571: 172.18.32.10.62949 > 45.11.129.62.443: Flags [P.], seq 4273088261:4273088778, ack 2660624333, win 64240, length 517
16:34:23.790198900 PktGroupId 2251799813685413, PktNumber 1, Darstellung 1, Richtung Rx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 60, LoggedSize 60
        98-9B-CB-32-9A-78 > A8-5E-45-CD-8B-F8, ethertype IPv4 (0x0800), length 60: 45.11.129.62.443 > 172.18.32.10.62949: Flags [.], ack 4273088778, win 30016, length 0
16:34:23.791175900 PktGroupId 2251799813685414, PktNumber 1, Darstellung 1, Richtung Rx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 1404, LoggedSize 443
        98-9B-CB-32-9A-78 > A8-5E-45-CD-8B-F8, ethertype IPv4 (0x0800), length 1404: 45.11.129.62.443 > 172.18.32.10.62949: Flags [.], seq 2660624333:2660625683, ack 4273088778, win 30016, length 1350
16:34:23.791254500 PktGroupId 2251799813685415, PktNumber 1, Darstellung 1, Richtung Rx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 1404, LoggedSize 443
        98-9B-CB-32-9A-78 > A8-5E-45-CD-8B-F8, ethertype IPv4 (0x0800), length 1404: 45.11.129.62.443 > 172.18.32.10.62949: Flags [.], seq 2660625683:2660627033, ack 4273088778, win 30016, length 1350
16:34:23.791255000 PktGroupId 2251799813685416, PktNumber 1, Darstellung 1, Richtung Rx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 787, LoggedSize 443
        98-9B-CB-32-9A-78 > A8-5E-45-CD-8B-F8, ethertype IPv4 (0x0800), length 787: 45.11.129.62.443 > 172.18.32.10.62949: Flags [P.], seq 2660627033:2660627766, ack 4273088778, win 30016, length 733
16:34:23.791280100 PktGroupId 2251799813685417, PktNumber 1, Darstellung 1, Richtung Tx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 54, LoggedSize 54
        A8-5E-45-CD-8B-F8 > 98-9B-CB-32-9A-78, ethertype IPv4 (0x0800), length 54: 172.18.32.10.62949 > 45.11.129.62.443: Flags [.], ack 2660627766, win 65340, length 0
16:34:23.794499400 PktGroupId 4222124650659843, PktNumber 1, Darstellung 1, Richtung Tx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 180, LoggedSize 180
        A8-5E-45-CD-8B-F8 > 98-9B-CB-32-9A-78, ethertype IPv4 (0x0800), length 180: 172.18.32.10.62949 > 45.11.129.62.443: Flags [P.], seq 4273088778:4273088904, ack 2660627766, win 65340, length 126
16:34:23.811204700 PktGroupId 2251799813685418, PktNumber 1, Darstellung 1, Richtung Rx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 105, LoggedSize 105
        98-9B-CB-32-9A-78 > A8-5E-45-CD-8B-F8, ethertype IPv4 (0x0800), length 105: 45.11.129.62.443 > 172.18.32.10.62949: Flags [P.], seq 2660627766:2660627817, ack 4273088904, win 30016, length 51
16:34:23.812383600 PktGroupId 6473924464345129, PktNumber 1, Darstellung 1, Richtung Tx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 221, LoggedSize 221
        A8-5E-45-CD-8B-F8 > 98-9B-CB-32-9A-78, ethertype IPv4 (0x0800), length 221: 172.18.32.10.62949 > 45.11.129.62.443: Flags [P.], seq 4273088904:4273089071, ack 2660627817, win 65289, length 167
16:34:23.833457800 PktGroupId 2251799813685419, PktNumber 1, Darstellung 1, Richtung Rx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 476, LoggedSize 443
        98-9B-CB-32-9A-78 > A8-5E-45-CD-8B-F8, ethertype IPv4 (0x0800), length 476: 45.11.129.62.443 > 172.18.32.10.62949: Flags [P.], seq 2660627817:2660628239, ack 4273089071, win 31088, length 422
16:34:23.833633500 PktGroupId 4222124650659844, PktNumber 1, Darstellung 1, Richtung Tx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 85, LoggedSize 85
        A8-5E-45-CD-8B-F8 > 98-9B-CB-32-9A-78, ethertype IPv4 (0x0800), length 85: 172.18.32.10.62949 > 45.11.129.62.443: Flags [P.], seq 4273089071:4273089102, ack 2660628239, win 64867, length 31
16:34:23.833681000 PktGroupId 4222124650659845, PktNumber 1, Darstellung 1, Richtung Tx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 54, LoggedSize 54
        A8-5E-45-CD-8B-F8 > 98-9B-CB-32-9A-78, ethertype IPv4 (0x0800), length 54: 172.18.32.10.62949 > 45.11.129.62.443: Flags [F.], seq 4273089102, ack 2660628239, win 64867, length 0
16:34:23.850461700 PktGroupId 2251799813685420, PktNumber 1, Darstellung 1, Richtung Rx , Typ Ethernet , Komponente 13, Edge 1, Filter 1, OriginalSize 60, LoggedSize 60
        98-9B-CB-32-9A-78 > A8-5E-45-CD-8B-F8, ethertype IPv4 (0x0800), length 60: 45.11.129.62.443 > 172.18.32.10.62949: Flags [F.], seq 2660628239, ack 4273089102, win 31088, length 0
Zeile 1, Spalte 1  100%  Windows (CRLF)  UTF-16 LE
```

Nach Abschluß bereinigen wir die gesetzten Filter wieder.

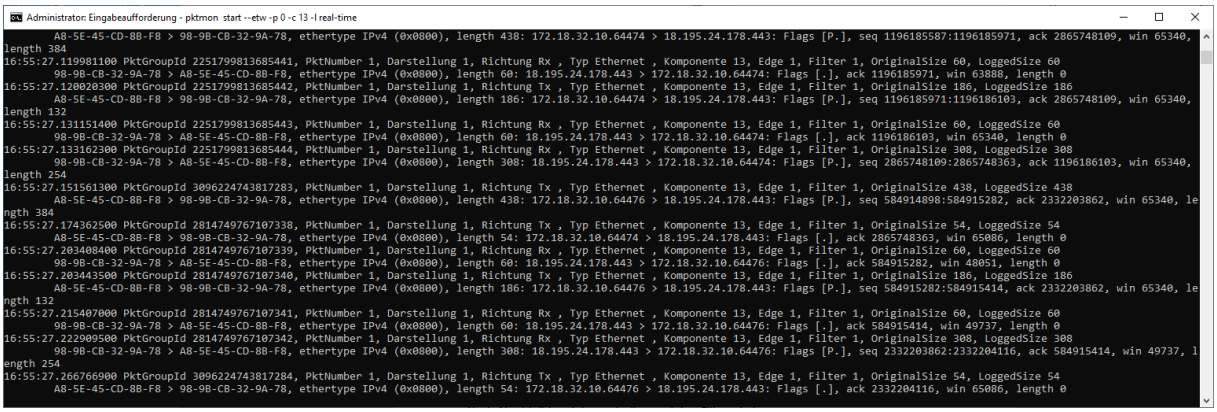


Möchte man alle Ports überwachen, dann setzt man diesen Befehl ab:

pktmon start --etw -p 0 -c 13

Eine Echtzeit-Monitoring ist auch möglich:

pktmon start --etw -p 0 -c 13 -l real-time



OPTIONAL:

NETSH TRACE

netsh trace start scenario=NetConnection level=5 capture=yes report=yes overwrite=yes persistent=yes tracefile="C:\Temp\NetshMon.etl"

netsh trace stop

netsh trace start capture=yes tracefile=C:\Temp\NetshMon.etl maxsize=512 filemode=circular overwrite=yes report=no correlation=no IPv4.SourceAddress=(172.18.32.10,172.18.32.11) IPv4.DestinationAddress=(172.18.32.10,172.18.32.11) Ethernet.Type=IPv4

netsh trace stop

Level	Setting	Description
1	Critical	Only critical events will be shown.
2	Errors	Critical events and errors will be shown.
3	Warnings	Critical events, errors, and warnings will be shown.
4	Informational	Critical events, errors, warnings, and informational events will be shown.
5	Verbose	All events will be shown.