

Wireshark spezifischen Port-Verkehr mitschneiden

Description

In diesem Artikel geht es kurz darum, wie wir mit Wireshark Datenverkehr mitschneiden können, welcher auf einen spezifischen Port gerichtet ist. Damit sind wir dann in der Lage uns z.B. nur den Verkehr anzuzeigen der auf Port 80 (HTTP) stattfindet.

Durchführung

Um den Wireshark-Verkehr jetzt mitszuschneiden, müssen wir im ersten Schritt Wireshark öffnen und stellen unsere Netzwerkschnittstelle ein. Im nächsten Schritt können wir dann den entsprechenden Filter setzen. In meinem Fall möchte ich jeglichen Datenverkehr, der auf Port 80 TCP und UDP ankommt oder ausgeht. Dazu verwende ich den folgenden Filter:

```
tcp.port == 80 or udp.port == 80
```

Info: Wir können beim Filter die Schlüsselwörter **and** und **or** verwenden, um Bedingungen miteinander zu verknüpfen.

Aufzeichnen von Ethernet 3

File Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe

tcp.port == 80 or udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
1036...	5854.362964	192.168.20.103	2.16.241.213	TCP	54	4201 → 80 [A
1036...	5854.363991	192.168.20.103	2.16.241.213	HTTP	411	GET / HTTP/1
1036...	5854.374010	2.16.241.213	192.168.20.103	TCP	66	[TCP Out-Of-
1036...	5854.374092	192.168.20.103	2.16.241.213	TCP	66	[TCP Dup ACK
1036...	5854.376102	2.16.241.213	192.168.20.103	TCP	60	80 → 4201 [A
1036...	5854.376102	2.16.241.213	192.168.20.103	HTTP	318	HTTP/1.1 304
1037...	5854.417111	192.168.20.103	2.16.241.213	TCP	54	4201 → 80 [A
1060...	5899.375839	192.168.20.103	2.16.241.213	TCP	55	[TCP Keep-Al
1060...	5899.387949	2.16.241.213	192.168.20.103	TCP	66	[TCP Keep-Al
1066...	5944.388731	192.168.20.103	2.16.241.213	TCP	55	[TCP Keep-Al
1066...	5944.400815	2.16.241.213	192.168.20.103	TCP	66	[TCP Keep-Al
1076...	5989.406343	192.168.20.103	2.16.241.213	TCP	55	[TCP Keep-Al
1076...	5989.418446	2.16.241.213	192.168.20.103	TCP	66	[TCP Keep-Al
1084...	6034.419935	192.168.20.103	2.16.241.213	TCP	55	[TCP Keep-Al
1084...	6034.431942	2.16.241.213	192.168.20.103	TCP	66	[TCP Keep-Al

Frame 4733: 55 bytes on wire (440 bits), 55 bytes
 Ethernet II, Src: Private_3c:bc:db (80:6d:97:3c:bc) 0010 00 29 29 fd 40 00 80 06 00 00
 Internet Protocol Version 4, Src: 192.168.20.103, 0020 fb 0c e8 88 00 50 88 29 09 a3
 Transmission Control Protocol, Src Port: 59528, Ds 0030 04 01 88 8e 00 00 00

Category

1. Software
2. Wireshark

Date Created

05.05.2025

Author

administrator