

Einführung (Aufgabe3)

1. 5 Erkannte Protokolle nennen

- UDP
- SSDP
- TCP
- ARP
- TLSv1.2
- QUIC
- ICMP 3.2

3.2 117,6 ms

3.3 Internet-Adresse: 192.168.101.21

Source MAC: 00:0C:29:8D:AD:E7

Ziel MAC: 00:50:56:C0:00:01 -> MAC Adresse von Router

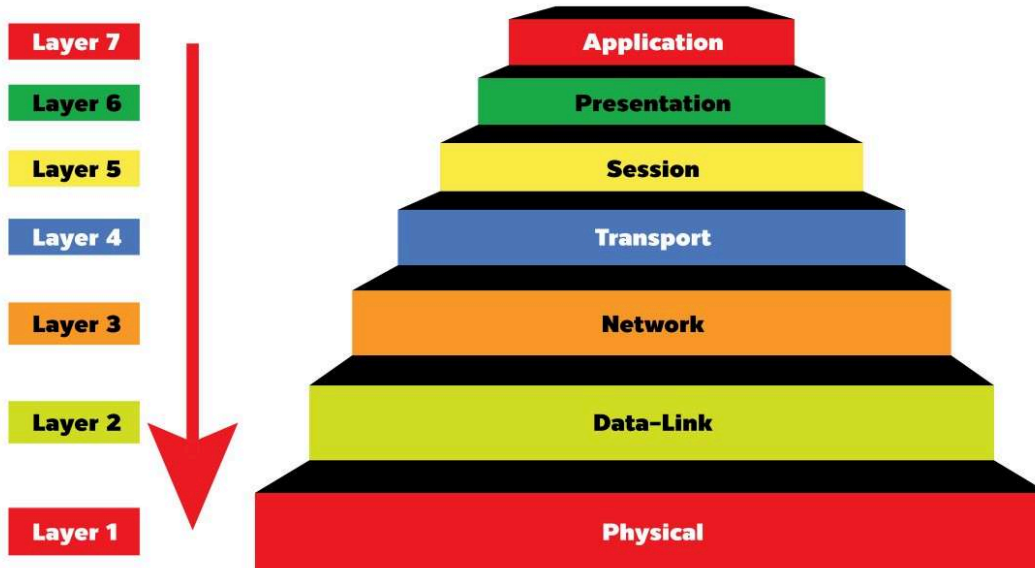
Schichtenmodell ISO/OSI(Aufgabe 3.4)

Ein HTTP-Paket nutzt folgende Protokolle:

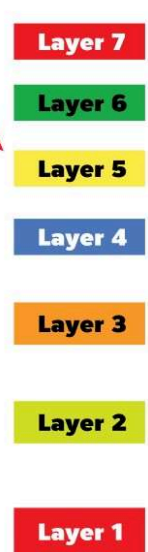
- **HTTP** → Application Layer (Schicht 7)
- **TCP** → Transport Layer (Schicht 4)
- **IP (IPv4 oder IPv6)** → Network Layer (Schicht 3)
- **Ethernet** → Link Layer (Schicht 2)

OSI MODEL

Client Side



Server Side



Analyse eines HTTP-Pakets: (Aufgabe 4)

Beispiel:

```

0000 38 22 d6 67 19 00 00 21 cc 63 82 2c 08 00 45 00 8".g...!.c,...E.
0010 02 9c 02 ed 40 00 80 06 40 66 8d 25 1d 5d 6b c6 ....@...@f.%.[.
0020 ae c0 e2 26 00 50 4f 4c 29 24 72 ce 3c d4 50 18 ...&.POL)$r.<.P.
0030 40 b0 62 e7 00 00 47 45 54 20 2f 77 69 6b 69 2f @.b...GET /wiki/
0040 53 69 6d 70 6c 65 5f 53 65 72 76 69 63 65 5f 44 Simple_Service_D
0050 69 73 63 6f 76 65 72 79 5f 50 72 6f 74 6f 63 6f iscovery_Protoco
0060 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 l HTTP/1.1..Host
0070 3a 20 64 65 2e 77 69 6b 69 70 65 64 69 61 2e 6f : de.wikipedia.o
0080 72 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 rg..User-Agent:
0090 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e Mozilla/5.0 (Win
00a0 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57 dows NT 6.1; WOW
00b0 36 34 3b 20 72 76 3a 33 32 2e 30 29 20 47 65 63 64; rv:32.0) Gec

```

Analysieren sie dieses Paket, indem Sie es mit einem anderen http Paket vergleichen, das in WireShark dargestellt ist. Wenn Sie in WireShark zu einem ausgewählten Paket, Header und Header-Felder im Fenster "details of selected packet headers" markieren, so werden die entsprechenden Bytes des Pakets ebenfalls markiert.

1. Markieren Sie im obigen Paket **Ethernet**, **IP** und **TCP** Header
2. Was sind die Quell- und Ziel-MAC-Adressen Adressen des dargestellten Pakets?
3. Was sind die Quell- und Ziel-IP-Adressen des dargestellten Pakets?
4. Was sind die verwendeten TCP-Ports des dargestellten Pakets?

hex

MAC Source: 00 21 cc 63 82 2c
MAC Dest: 38 22 d6 67 19 00

IP Source: 8d 25 1d 5d
IP Dest: 5b c6 ae c0

TCP Source: e2 26
TCP Dest: 00 50

umwandeln

MAC Source: 00:21:cc:63:82:2c
MAC Dest: 38:22:d6:67:19:00

IP Source: 8d 25 1d 5d = 141.37.29.93
IP Dest: 5b c6 ae c0 = 91.198.174.192

TCP Source: e2 26 = 57958
TCP Dest: 00 50 = 80

Filter in Wireshark (Aufgabe 5)

1. Wie lautet der Filter, mit dem Sie über den TCP-Port HTTPS-Verkehr filtern können?
 - `tcp.port == 443`
2. Vergleiche HTTP-Verkehr über Filter: `http` und über Filter: `tcp.port == 80`
 - **Filter `http` zeigt nur Pakete, bei denen der HTTP-Protokoll-Parser von Wireshark tatsächlich HTTP-Inhalte erkennt.**
→ Z. B. GET , POST , HTTP/1.1 200 OK usw.
 - **Filter `tcp.port == 80` zeigt alle TCP-Pakete, die auf Port 80 laufen, auch wenn sie keine erkennbaren HTTP-Inhalte haben (z. B. Verbindungsaufbau mit SYN , ACK , Keep-Alive, etc.).**
Der HTTP-Filter ist also **protokollbasiert**, während `tcp.port == 80` rein **portbasiert** ist.
3. Es gibt einen Filter `http` , aber keinen Filter `https` . Haben Sie eine Idee warum?
 - HTTPS ist verschlüsselter HTTP-Verkehr über TLS
 - Wird also verschlüsselt und somit nicht mehr lesbar und daher auch kein HTTPS-Filter
 - ABER es gibt `tcp.port == 443`
4. Welcher Filter bewirkt, dass nur Pakete angezeigt werden, die die eigene IP-Adresse als Zieladresse haben?
 - `ip.dst == EIGENE IP`

Upstream vs Downstream (Aufgabe 6)

Statistiken -> Endpunkte -> IPv4

Filter für Downstream (vom Server an dich):

```
ip.dst == 192.168.178.48
```

Filter für Upstream (von dir ins Internet):

```
ip.src == 192.168.178.48
```

Wireshark - Endpoints - Ethernet

Endpoint Settings: ☒ Namensauflösung, ☒ Auf Anzeigenfilter einschränken

Protokoll: ☒ Bluetooth, ☒ BPv7, ☒ DCCP, ☒ Ethernet, ☒ FC, ☒ FDDI, ☒ IEEE 802.11, ☒ IEEE 802.15.4, ☒ IPv4, ☒ IPv6, ☒ IPX, ☒ JXTA, ☒ LTP, ☒ MPTCP, ☒ NCP, ☒ openSAFETY, ☒ RSVP, ☒ SCTP, ☒ SLL, ☒ TCP, ☒ Token-Ring, ☒ UDP, ☒ USB, ☒ ZigBee

Adresse	Pakete	Bytes	Pakete gesamt	Prozent gefiltert	Tx Pakete	Tx Bytes	Rx Pakete	Rx Bytes
216.200.232.253	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
192.168.178.48	1.257	939 kB	1.557	80.73%	520	180 kB	737	759 kB
178.250.1.56	32	17 kB	32	100.00%	15	9 kB	17	9 kB
178.250.1.11	4	242 Bytes	4	100.00%	2	132 Bytes	2	110 Bytes
154.54.250.81	2	115 Bytes	2	100.00%	1	60 Bytes	1	55 Bytes
151.101.1.108	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
151.101.1.44	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
150.171.27.10	59	18 kB	59	100.00%	33	12 kB	26	6 kB
136.243.25.121	64	52 kB	64	100.00%	26	9 kB	38	43 kB
128.65.210.181	286	279 kB	286	100.00%	184	267 kB	102	11 kB
108.128.223.16	25	10 kB	25	100.00%	14	7 kB	11	3 kB
104.22.24.245	44	25 kB	44	100.00%	28	24 kB	16	1 kB
103.231.98.85	2	115 Bytes	2	100.00%	1	60 Bytes	1	55 Bytes
95.101.182.66	35	10 kB	35	100.00%	20	6 kB	15	5 kB
76.223.111.18	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
64.158.223.146	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
63.140.62.222	47	31 kB	47	100.00%	22	11 kB	25	20 kB
63.140.62.17	32	17 kB	32	100.00%	16	6 kB	16	11 kB
54.77.83.175	31	13 kB	31	100.00%	17	7 kB	14	5 kB
35.244.193.51	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
35.210.58.154	68	40 kB	68	100.00%	32	12 kB	36	27 kB
34.160.236.64	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
34.111.113.62	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
34.107.148.139	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
34.98.64.218	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
34.95.103.74	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
34.36.216.150	2	121 Bytes	2	100.00%	1	66 Bytes	1	55 Bytes
23.48.23.178	1	54 Bytes	1	100.00%	0	0 Bytes	1	54 Bytes
3.160.150.52	24	7 kB	24	100.00%	13	3 kB	11	4 kB
2.22.242.227	46	21 kB	46	100.00%	26	5 kB	20	16 kB
2.16.168.118	409	392 kB	409	100.00%	233	377 kB	146	15 kB
2.16.168.114	22	5 kB	22	100.00%	2	2 kB	10	3 kB

Aufruf <https://spiegel.de>

UPSTREAM = Tx Pakete = 520
DOWNSTREAM = Rx Pakete = 737 } 1257

TX_Bytes = 180 kB
RX_Bytes = 759 kB

Wie viele IP's haben Daten an mein Rechner gesendet beim Aufruf

Statistiken -> Endpunkte -> IPv4

Wir haben unseren Filter eingestellt und schauen jetzt welche IP-Adressen Tx(Upstream) Pakete an uns gesendet haben. (Alle IP Adressen mit Tx Pakete > 0) = 29 IP's

tcp.port == 443 && ip.dst == 192.168.178.48

No.	Time	Source	Destination	Protocol	Length	Info
11	2.729588	2.22.242.227	192.168.178.48	TCP	60	443 → 44077 [ACK] Seq=1 Ack=1385 Win=2450 Len=0

Wireshark · Endpoints · Ethernet

Endpoint Settings

- ☐ Namensauflösung
- ☒ Auf Anzeigenfilter einschränken
- Kopieren
- Karte
- Protokoll
 - ☐ Bluetooth
 - ☐ BPv7
 - ☐ DCCP
 - ☒ Ethernet
 - ☐ FC
 - ☐ FDDI
 - ☐ IEEE 802.11
 - ☐ IEEE 802.15.4
 - ☒ IPv4
 - ☒ IPv6
 - ☐ IPX
 - ☐ JXTA
 - ☐ LTP
 - ☐ MPTCP
 - ☐ NCP
 - ☐ openSAFETY
- Filtere Liste nach spezifischem Typ

Adresse	Pakete	Bytes	Pakete gesamt	Prozent gefiltert	Tx Pakete	Tx Bytes	Rx Pakete	Rx Bytes	Land
192.168.178.48	737	759 kB	1.557	47.33%	0	0 Bytes	737	759 kB	
154.54.250.81	1	60 Bytes	2	50.00%	1	60 Bytes	0	0 Bytes	
103.231.98.85	1	60 Bytes	2	50.00%	1	60 Bytes	0	0 Bytes	
151.101.1.44	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
34.107.148.139	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
151.101.1.108	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
76.223.111.18	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
64.158.223.146	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
34.95.103.74	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
34.98.64.218	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
34.36.216.150	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
34.111.113.62	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
35.244.193.51	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
216.200.232.253	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
34.160.236.64	1	66 Bytes	2	50.00%	1	66 Bytes	0	0 Bytes	
178.250.1.11	2	132 Bytes	4	50.00%	2	132 Bytes	0	0 Bytes	
2.16.168.114	12	2 kB	22	54.55%	12	2 kB	0	0 Bytes	
3.160.150.52	13	3 kB	24	54.17%	13	3 kB	0	0 Bytes	
108.128.223.16	14	7 kB	25	56.00%	14	7 kB	0	0 Bytes	
178.250.1.56	15	9 kB	32	46.88%	15	9 kB	0	0 Bytes	
63.140.62.17	16	6 kB	32	50.00%	16	6 kB	0	0 Bytes	
54.77.83.175	17	7 kB	31	54.84%	17	7 kB	0	0 Bytes	
95.101.182.66	20	6 kB	35	57.14%	20	6 kB	0	0 Bytes	
63.140.62.222	22	11 kB	47	46.81%	22	11 kB	0	0 Bytes	
2.22.242.227	26	5 kB	46	56.52%	26	5 kB	0	0 Bytes	
136.243.25.121	26	9 kB	64	40.63%	26	9 kB	0	0 Bytes	
104.22.24.245	28	24 kB	44	63.64%	28	24 kB	0	0 Bytes	
35.210.58.154	32	12 kB	68	47.06%	32	12 kB	0	0 Bytes	
150.171.27.10	33	12 kB	59	55.93%	33	12 kB	0	0 Bytes	
128.65.210.181	184	267 kB	286	64.34%	184	267 kB	0	0 Bytes	
2.16.168.118	263	377 kB	409	64.30%	263	377 kB	0	0 Bytes	

Über wie viele TCP Sockets hat dein Rechner die Daten empfangen?

✖ Ein **TCP-Socket** ist eindeutig identifiziert durch:

Quell-IP : Quell-Port → Ziel-IP : Ziel-Port

Das heißt: Kombination aus IP-Adressen und Ports in beide Richtungen.

FileBearbeitenAnsichtNavigationAufzeichnenAnalyseFiltersetzenToolsHilfe

tcp.port == 443

Wireshark - Conversations - Ethernet

Conversations Settings

Namesauflösung

Absolute Startzeit

W Auf Anzeigenfilter einschalten

Kopieren

Stream folgen...

Graph...

Protokoll

Bluetooth

BPV7

DCPP

Ethernet

F

FCB

IEEE 802.11

IEEE 802.15.4

IPv4

IPv6

JTA

LTP

MPTCP

TCP

openSAFETY

RSPV

SCPT

SLL

TCP

Token-Ring

Filtere Liste nach spezifischem Typ

Adresse A	Port A	Adresse B	Port B	Pakete	Bytes	Stream ID	Pakete gesamt	Prozent gefiltert	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel. Start	Dauer	Bits/s A → B	Bits/s B → A	Flows
192.168.178.48	44743	2.16.168.114	443	22	5 kb	11	22	100.00%	10	3 kb	12	2 kb	4.122079	0.1719	151 kbps	72 kbps	5
192.168.178.48	44745	2.16.168.118	443	409	392 kb	17	409	100.00%	146	15 kb	263	377 kb	5.182070	0.2631	460 kbps	111 kbps	6
192.168.178.48	44077	2.22.202.227	443	46	21 kb	0	46	100.00%	20	16 kb	26	5 kb	2.586375	4.3902	29 kbps	8903 bits/s	7
192.168.178.48	44087	3.160.150.52	443	11	4 kb	15	11	100.00%	5	2 kb	6	2 kb	4.295566	0.4134	31 kbps	40 kbps	4
192.168.178.48	44738	3.160.150.52	443	13	3 kb	2	13	100.00%	6	2 kb	7	883 Bytes	3.136512	0.0953	200 kbps	74 kbps	4
192.168.178.48	44699	2.48.23.178	443	1	54 Bytes	1	1	100.00%	1	54 Bytes	0	0 Bytes	3.082044	0.0000			0
192.168.178.48	44279	34.826.216.150	443	2	121 Bytes	22	2	100.00%	1	55 Bytes	1	66 Bytes	3.437024	0.0343	12 kbps	15 kbps	1
192.168.178.48	44481	34.95.103.74	443	2	121 Bytes	13	2	100.00%	1	55 Bytes	1	66 Bytes	4.164258	0.0301	14 kbps	17 kbps	1
192.168.178.48	44174	34.98.64.218	443	2	121 Bytes	20	2	100.00%	1	55 Bytes	1	66 Bytes	5.394778	0.0368	11 kbps	14 kbps	1
192.168.178.48	44477	34.107.148.139	443	2	121 Bytes	8	2	100.00%	1	55 Bytes	1	66 Bytes	3.852245	0.0294	14 kbps	17 kbps	1
192.168.178.48	44298	34.111.112.62	443	2	121 Bytes	24	2	100.00%	1	55 Bytes	1	66 Bytes	5.595740	0.0294	14 kbps	17 kbps	1
192.168.178.48	44265	34.160.236.64	443	2	121 Bytes	35	2	100.00%	1	55 Bytes	1	66 Bytes	6.984260	0.0391	11 kbps	13 kbps	1
192.168.178.48	44753	35.210.58.154	443	68	40 kb	33	68	100.00%	36	27 kb	32	12 kb	6.390904	0.2165	1000 kbps	459 kbps	8
192.168.178.48	44512	35.244.193.51	443	2	121 Bytes	28	2	100.00%	1	55 Bytes	1	66 Bytes	5.823608	0.0345	12 kbps	15 kbps	1
192.168.178.48	44747	54.7723.175	443	31	3 kb	19	31	100.00%	14	3 kb	17	7 kb	5.360311	0.0326	80 kbps	109 kbps	8
192.168.178.48	44749	63.140.62.17	443	32	17 kb	23	32	100.00%	16	11 kb	16	6 kb	5.474501	0.2268	377 kbps	207 kbps	6
192.168.178.48	44744	63.140.62.222	443	47	31 kb	16	47	100.00%	25	20 kb	22	11 kb	4.897743	0.4163	384 kbps	216 kbps	8
192.168.178.48	44479	64.158.223.148	443	2	121 Bytes	12	2	100.00%	1	55 Bytes	1	66 Bytes	4.148174	0.0378	11 kbps	13 kbps	1
192.168.178.48	44481	64.222.111.48	443	2	121 Bytes	10	2	100.00%	1	55 Bytes	1	66 Bytes	3.892628	0.0302	14 kbps	17 kbps	1
192.168.178.48	44705	65.101.182.66	443	35	10 kb	25	35	100.00%	15	5 kb	20	4 kb	5.695716	0.7820	49 kbps	56 kbps	8
192.168.178.48	44515	103.231.98.85	443	2	115 Bytes	29	2	100.00%	1	55 Bytes	1	60 Bytes	5.939614	0.0298	14 kbps	16 kbps	1
192.168.178.48	44084	104.22.24.245	443	34	22 kb	7	34	100.00%	12	851 Bytes	22	21 kb	3.732284	0.4821	14 kbps	344 kbps	4
192.168.178.48	44084	104.22.24.245	443	10	4 kb	14	10	100.00%	4	360 Bytes	6	3 kb	4.230937	0.1202	25 kbps	224 kbps	3
192.168.178.48	44751	108.182.22.14	443	25	10 kb	30	25	100.00%	11	3 kb	14	7 kb	6.026574	0.2814	92 kbps	197 kbps	6
192.168.178.48	44739	108.65.210.181	443	286	279 kb	3	286	100.00%	102	11 kb	184	267 kb	3.163329	0.2497	360 kbps	854 kbps	6
192.168.178.48	44746	136.243.25.121	443	64	52 kb	18	64	100.00%	38	43 kb	26	9 kb	5.241333	1.6019	212 kbps	46 kbps	6
192.168.178.48	44105	150.171.27.80	443	20	5 kb	26	20	100.00%	8	1 kb	12	4 kb	5.662560	0.0206	12 kbps	37 kbps	6
192.168.178.48	44241	150.171.27.80	443	18	5 kb	18	18	100.00%	11	5 kb	21	9 kb	3.489102	2.7496	12 kbps	24 kbps	12
192.168.178.48	44464	151.101.1.44	443	2	121 Bytes	4	2	100.00%	1	55 Bytes	1	66 Bytes	3.231430	0.0294	14 kbps	17 kbps	1
192.168.178.48	44177	151.101.1.108	443	2	121 Bytes	9	2	100.00%	1	55 Bytes	1	66 Bytes	3.884282	0.0294	14 kbps	17 kbps	1
192.168.178.48	44266	154.54.250.81	443	2	115 Bytes	21	2	100.00%	1	55 Bytes	1	60 Bytes	5.408931	0.0467	9427 bits/s	10 kbps	1
192.168.178.48	44178	178.201.1.11	443	2	121 Bytes	34	2	100.00%	1	55 Bytes	1	66 Bytes	6.820349	0.0362	12 kbps	14 kbps	1
192.168.178.48	44509	178.250.1.11	443	2	121 Bytes	27	2	100.00%	1	55 Bytes	1	66 Bytes	5.869337	0.0363	12 kbps	14 kbps	1
192.168.178.48	44732	178.250.1.56	443	32	17 kb	32	32	100.00%	17	9 kb	15	9 kb	6.384746	0.2086	326 kbps	341 kbps	6
192.168.178.48	44505	216.200.232.253	443	2	121 Bytes	31	2	100.00%	1	55 Bytes	1	66 Bytes	6.086640	0.1403	3135 bits/s	3762 bits/s	1

- Dadurch, dass wir überall als Quelle unsere eigene IP haben, sind wir der Client
- Nun können wir die Anzahl der Sockets mit unserer eigenen IP zählen
 - 34 Stück

Pakete bei Streams (Aufgabe 7)

`ip.addr == <deine IP> && tcp.port == <Port des Streams>`

Port des streams finden wir unter

- Menü: **"Statistiken"** → **"Gespräche" (Conversations)** → **TCP-Tab**
- Stream geht über Port B (Unserer lokaler Port in diesem Fall)

Conversations Settings		Filternet 1	IP v1 - 15	IP v6	TCP	UDP													
Namensauflösung		Adresse A	Port A	Adresse B	Port B	Pakete	Bytes	Stream ID	Pakete gesamt	Prozent gefiltert	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel. Start	Dauer	Bits/s A → B	Bits/s B → A	Flows
<input checked="" type="checkbox"/> Absolute Startzeit		80.208.234.208	443	192.168.178.48	46169	384	342 kb		384	100.00%	250	334 kb	134	7 kb	0.000000	18.6281	136 kbps	2949 bits/s	1
<input checked="" type="checkbox"/> Auf Anzeigefilter einschränken		192.168.178.48	443	192.168.178.48	46031	9	583 Bytes	6	9	100.00%	4	291 Bytes	5	284 Bytes	13.411536	0.0095	79 kbps	79 kbps	2
		2.232.227.208	443	192.168.178.48	46031	6	384 Bytes	8	6	100.00%	3	198 Bytes	3	186 Bytes	14.220187	0.0343	46 kbps	43 kbps	2
		91.215.100.77	443	192.168.178.48	46144	5	333 Bytes	2	5	100.00%	2	171 Bytes	3	162 Bytes	3.229556	0.0009			1
		91.215.100.77	443	192.168.178.48	46146	4	279 Bytes	34	4	100.00%	2	171 Bytes	2	108 Bytes	3.338563	0.0089			1
		18.65.147.16	443	192.168.178.48	45818	4	246 Bytes	7	4	100.00%	2	138 Bytes	2	108 Bytes	13.772623	0.0008			1
		192.168.178.48	45945	3.160.196.19	443	2	121 Bytes	1	2	100.00%	1	55 Bytes	1	66 Bytes	2.738403	0.0503	8744 bits/s	10 kbps	1
		192.168.178.48	46151	35.201.111.240	443	17	121 Bytes	2	17	100.00%	1	55 Bytes	1	66 Bytes	19.818102	0.0339	12 kbps	15 kbps	1
		192.168.178.48	46140	49.12.16.45	443	2	121 Bytes	13	2	100.00%	1	55 Bytes	1	66 Bytes	18.256831	0.0342	12 kbps	15 kbps	1
		192.168.178.48	46148	49.12.16.45	443	2	121 Bytes	14	2	100.00%	1	55 Bytes	1	66 Bytes	18.893339	0.0337	13 kbps	15 kbps	1
		192.168.178.48	46150	142.250.185.74	443	15	121 Bytes	2	15	100.00%	1	55 Bytes	1	66 Bytes	15.572135	0.0292	13 kbps	15 kbps	1
		192.168.178.48	46132	142.250.186.174	443	10	121 Bytes	2	10	100.00%	1	55 Bytes	1	66 Bytes	17.619375	0.0295	14 kbps	17 kbps	1
		192.168.178.48	46133	151.101.192.91	443	12	121 Bytes	2	12	100.00%	1	55 Bytes	1	66 Bytes	18.063190	0.0296	14 kbps	17 kbps	1
		192.168.178.48	46041	185.199.108.153	443	2	121 Bytes	16	2	100.00%	1	55 Bytes	1	66 Bytes	18.957134	0.0300	14 kbps	17 kbps	1
		192.168.178.48	46123	216.58.206.46	443	2	121 Bytes	5	2	100.00%	1	55 Bytes	1	66 Bytes	12.255464	0.0293	15 kbps	18 kbps	1
		190.171.27.11	443	192.168.178.48	46028	9	60 Bytes	1	9	100.00%	0	0 Bytes	0	0 Bytes	16.549564	0.0000			0
		190.171.27.11	443	192.168.178.48	46028	11	60 Bytes	1	11	100.00%	0	0 Bytes	0	0 Bytes	17.915099	0.0000			0
		192.168.178.48	46152	35.241.3.184	443	1	55 Bytes	18	1	100.00%	1	55 Bytes	0	0 Bytes	19.691584	0.0000			1

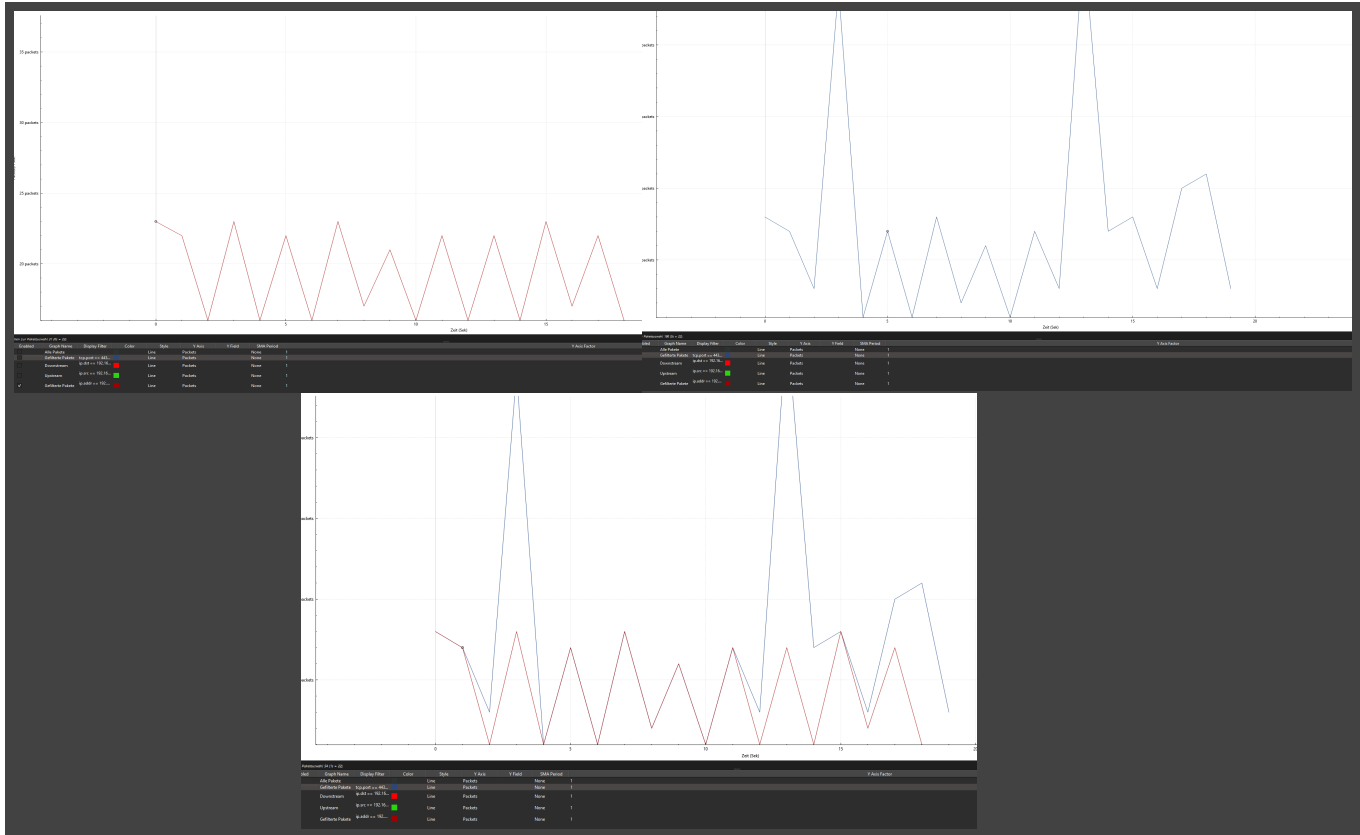
jetzt setzen wir:

`ip.addr == 192.168.178.48 && tcp.port == 46169 ROT`

`ip.addr == 192.168.178.48 && tcp.port == 443 BLAU`

und gehen in I/O Graph und bekommen:

Rot sollte der Stream-Traffic sein und Blau die allgemeine Up und Downstreams für SSL Pakete



Jetzt sehen wir deutlich wie eine Überlagerung der beiden Filter stattfindet und dass wir in regelmäßigen abständen große Pakete empfangen und senden.

Alle 2sek ein peek mit 22 - 25 Packets

Unter: - Menü: **"Statistiken"** → **"Gespräche" (Conversations)** → **TCP-Tab** können wir noch Bandbreite analysieren

Wireshark - Conversations - Ethernet														
Conversation Settings														
Ethernet - 1		IPv4 - 1		IPv6		TCP - 1		UDP						
Adresse A	Port A	Adresse B	Port B	Pakete	Bytes	Stream ID	Pakete gesamt	Prozent gefüllt	Pakete A → B	Bytes A → B	Pakete B → A	Bytes B → A	Rel. Start	Dauer
80.208.234.208	443	192.168.178.48	46169	384	342 kB	0	384	100.00%	250	334 kB	134	7 kB	0.000000	19.6283
														136 kbps
														2949 bits/s
														1

◆ Download (empfangen):

- 334 kB = $334 \times 1024 \times 8 = 2.731.008$ Bits
- Zeit: 19,6283 Sekunden

$$\frac{2.731.008 \text{ Bit}}{19,6283 \text{ Sek}} \approx 139.2 \text{ kbps}$$

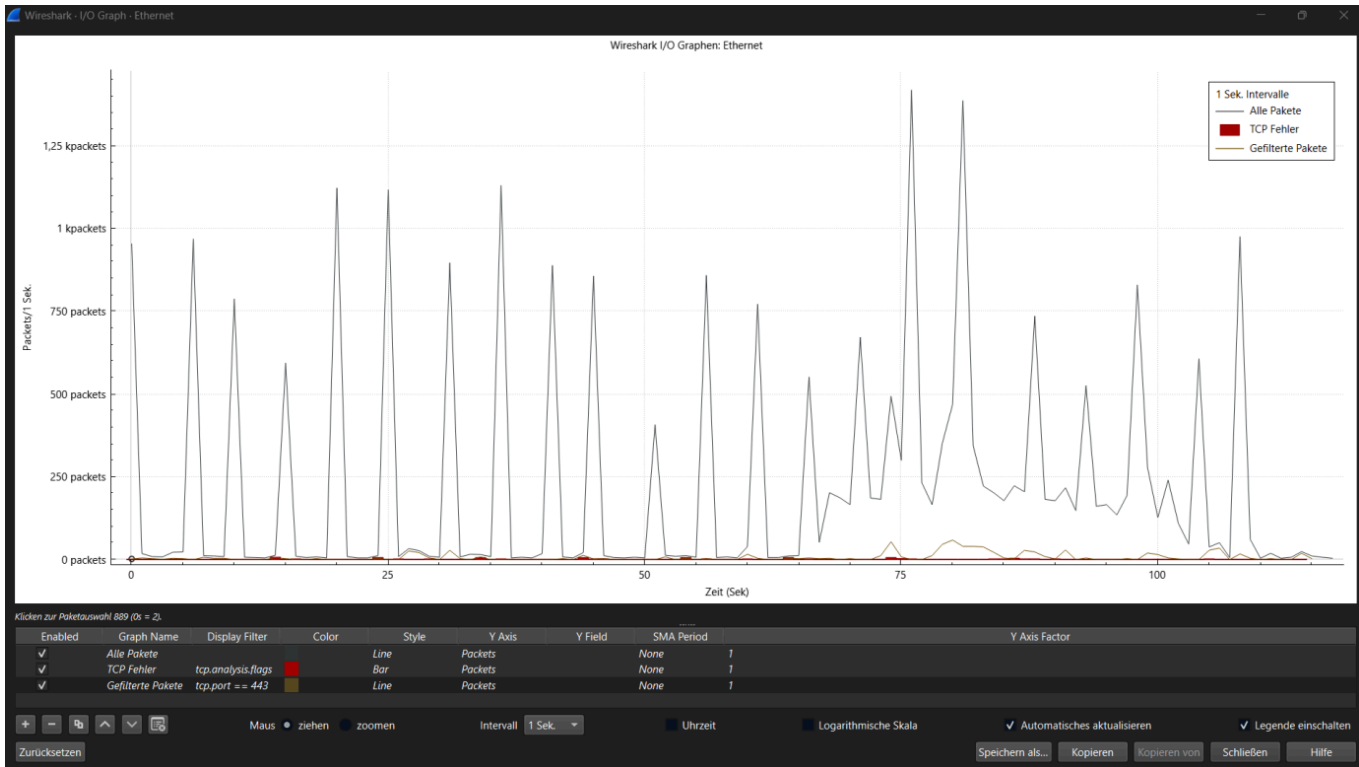
◆ Upload (gesendet):

- 7 kB = $7 \times 1024 \times 8 = 57.344$ Bits

- Zeit: 19,6283 Sekunden

$$\frac{57.344 \text{ Bit}}{19,6283 \text{ Sek}} \approx 2.9 \text{ kbps}$$

Wenn man den Stream noch etwas länger laufen lässt, sieht es in etwa so aus:



Beim Aufzeichnen eines HTTPS-basierten Streams zeigte der Netzwerkverkehr typische Pufferungs-Muster. Der Client fordert regelmäßig größere Datenmengen an, was sich in deutlich sichtbaren Paket-Bursts äußert (über 1.000 Pakete/Sekunde), gefolgt von Pausen. Der Datenverkehr lief vollständig über TCP-Port 443 (HTTPS). Es wurden keine UDP-Streams verwendet.

Die Übertragung war überwiegend stabil, mit nur wenigen TCP-Fehlern, die keine größere Störung darstellten.

Insgesamt lässt sich eine regelmäßige Paketübertragung in der ersten Hälfte feststellen, mit zunehmender Unregelmäßigkeit in der zweiten Hälfte, was auf unterschiedliche Pufferanforderungen oder parallele Hintergrundaktivität hindeuten könnte.