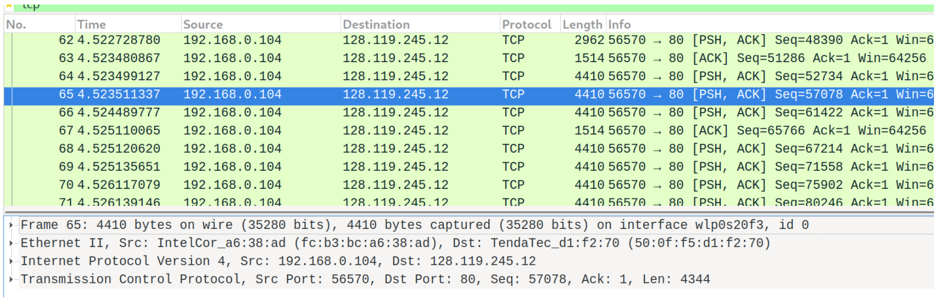
Wireshark: TCP (5 баллов).

1. Перехват TCP-передачи данных от вашего компьютера удаленному серверу

1.

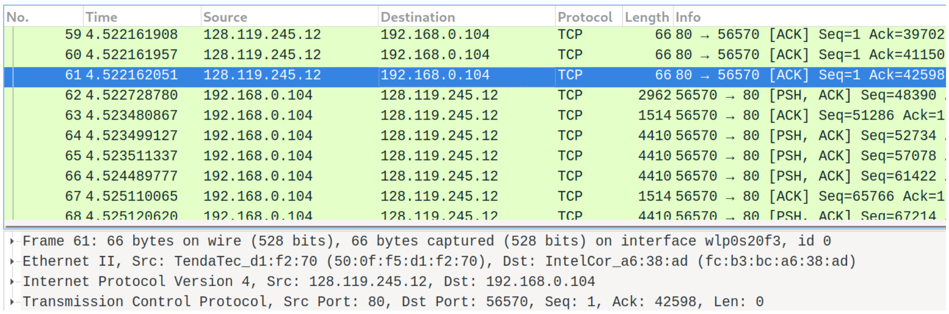


```
tcp
No.   Time         Source          Destination     Protocol Length Info
   62 4.522728780  192.168.0.104   128.119.245.12  TCP      2962 56570 → 80 [PSH, ACK] Seq=48390 Ack=1 Win=6
   63 4.523480867  192.168.0.104   128.119.245.12  TCP      1514 56570 → 80 [ACK] Seq=51286 Ack=1 Win=64256
   64 4.523499127  192.168.0.104   128.119.245.12  TCP      4410 56570 → 80 [PSH, ACK] Seq=52734 Ack=1 Win=6
   65 4.523511337  192.168.0.104   128.119.245.12  TCP      4410 56570 → 80 [PSH, ACK] Seq=57078 Ack=1 Win=6
   66 4.524489777  192.168.0.104   128.119.245.12  TCP      4410 56570 → 80 [PSH, ACK] Seq=61422 Ack=1 Win=6
   67 4.525110065  192.168.0.104   128.119.245.12  TCP      1514 56570 → 80 [ACK] Seq=65766 Ack=1 Win=64256
   68 4.525120620  192.168.0.104   128.119.245.12  TCP      4410 56570 → 80 [PSH, ACK] Seq=67214 Ack=1 Win=6
   69 4.525135651  192.168.0.104   128.119.245.12  TCP      4410 56570 → 80 [PSH, ACK] Seq=71558 Ack=1 Win=6
   70 4.526117079  192.168.0.104   128.119.245.12  TCP      4410 56570 → 80 [PSH, ACK] Seq=75902 Ack=1 Win=6
   71 4.526139146  192.168.0.104   128.119.245.12  TCP      4410 56570 → 80 [PSH, ACK] Seq=80246 Ack=1 Win=6

› Frame 65: 4410 bytes on wire (35280 bits), 4410 bytes captured (35280 bits) on interface wlp0s20f3, id 0
› Ethernet II, Src: IntelCor_a6:38:ad (fc:b3:bc:a6:38:ad), Dst: TendaTec_d1:f2:70 (50:0f:f5:d1:f2:70)
› Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 56570, Dst Port: 80, Seq: 57078, Ack: 1, Len: 4344
```

Адрес – 192.168.0.104, порт – 56570

2.

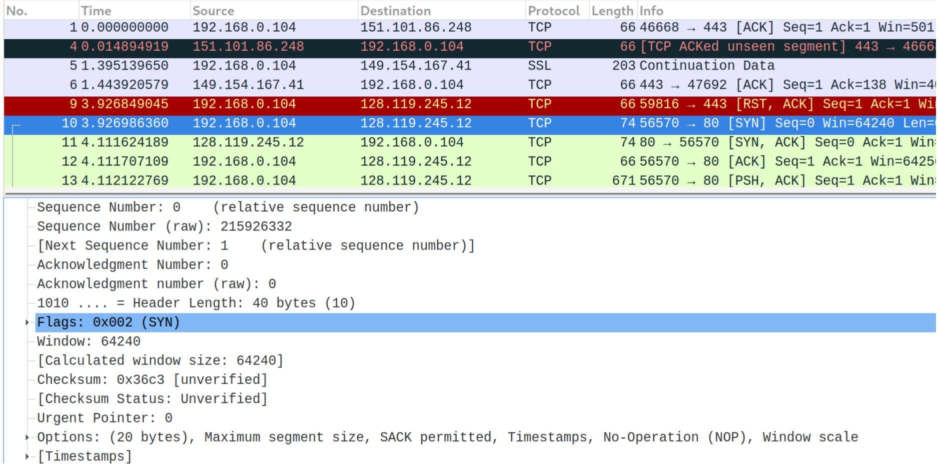


```
No.   Time         Source          Destination     Protocol Length Info
   59 4.522161908  128.119.245.12  192.168.0.104   TCP        66 80 → 56570 [ACK] Seq=1 Ack=39702
   60 4.522161957  128.119.245.12  192.168.0.104   TCP        66 80 → 56570 [ACK] Seq=1 Ack=41150
   61 4.522162051  128.119.245.12  192.168.0.104   TCP        66 80 → 56570 [ACK] Seq=1 Ack=42598
   62 4.522728780  192.168.0.104   128.119.245.12  TCP      2962 56570 → 80 [PSH, ACK] Seq=48390 .
   63 4.523480867  192.168.0.104   128.119.245.12  TCP      1514 56570 → 80 [ACK] Seq=51286 Ack=1
   64 4.523499127  192.168.0.104   128.119.245.12  TCP      4410 56570 → 80 [PSH, ACK] Seq=52734 .
   65 4.523511337  192.168.0.104   128.119.245.12  TCP      4410 56570 → 80 [PSH, ACK] Seq=57078 .
   66 4.524489777  192.168.0.104   128.119.245.12  TCP      4410 56570 → 80 [PSH, ACK] Seq=61422 .
   67 4.525110065  192.168.0.104   128.119.245.12  TCP      1514 56570 → 80 [ACK] Seq=65766 Ack=1
   68 4.525120620  192.168.0.104   128.119.245.12  TCP      4410 56570 → 80 [PSH, ACK] Seq=67214

› Frame 61: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp0s20f3, id 0
› Ethernet II, Src: TendaTec_d1:f2:70 (50:0f:f5:d1:f2:70), Dst: IntelCor_a6:38:ad (fc:b3:bc:a6:38:ad)
› Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.104
› Transmission Control Protocol, Src Port: 80, Dst Port: 56570, Seq: 1, Ack: 42598, Len: 0
```

Адрес сервера – 128.119.245.12, порт отправки и приема TCP-сегментов – 80

3.

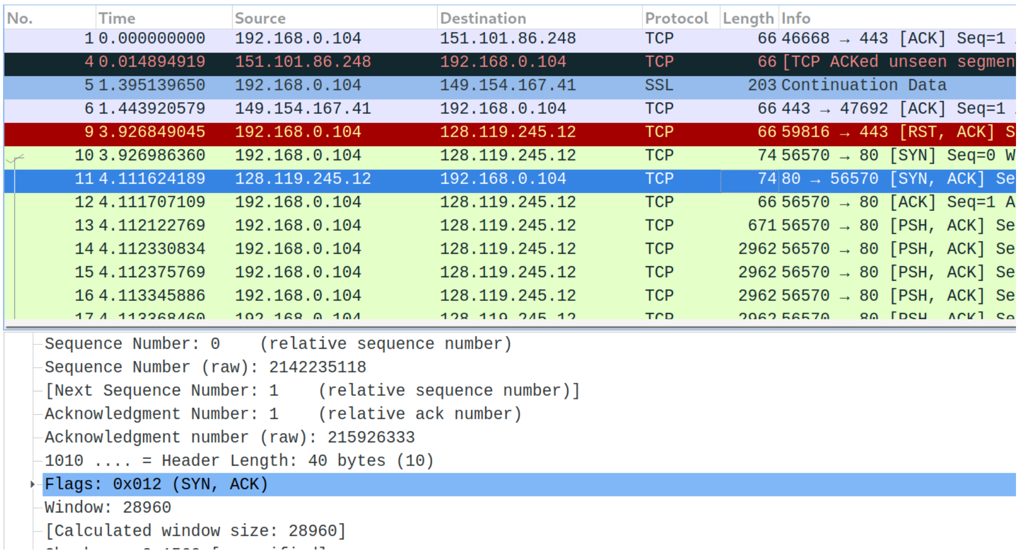


```
No.   Time         Source          Destination     Protocol Length Info
    1 0.000000000  192.168.0.104   151.101.86.248  TCP        66 46668 → 443 [ACK] Seq=1 Ack=1 Win=501
    4 0.014894919  151.101.86.248  192.168.0.104   TCP        66 [TCP ACKed unseen segment] 443 → 4666
    5 1.395139650  192.168.0.104   149.154.167.41  SSL       203 Continuation Data
    6 1.443920579  149.154.167.41  192.168.0.104   TCP        66 443 → 47692 [ACK] Seq=1 Ack=138 Win=4
    9 3.926849045  192.168.0.104   128.119.245.12  TCP        66 59816 → 443 [RST, ACK] Seq=1 Ack=1 Wi
   10 3.926986360  192.168.0.104   128.119.245.12  TCP        74 56570 → 80 [SYN] Seq=0 Win=64240 Len=
   11 4.111624189  128.119.245.12  192.168.0.104   TCP        74 80 → 56570 [SYN, ACK] Seq=0 Ack=1 Win
   12 4.111707109  192.168.0.104   128.119.245.12  TCP        66 56570 → 80 [ACK] Seq=1 Ack=1 Win=6425
   13 4.112122769  192.168.0.104   128.119.245.12  TCP       671 56570 → 80 [PSH, ACK] Seq=1 Ack=1 Win

   Sequence Number: 0    (relative sequence number)
   Sequence Number (raw): 215926332
   [Next Sequence Number: 1    (relative sequence number)]
   Acknowledgment Number: 0
   Acknowledgment number (raw): 0
   1010 .... = Header Length: 40 bytes (10)
 › Flags: 0x002 (SYN)
   Window: 64240
   [Calculated window size: 64240]
   Checksum: 0x36c3 [unverified]
   [Checksum Status: Unverified]
   Urgent Pointer: 0
 › Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
 › [Timestamps]
```

Порядковый номер SYN TCP-сегмента – 10 (в то же время Seq=0). Его можно определить по соответствующему флагу (SYN).

4.

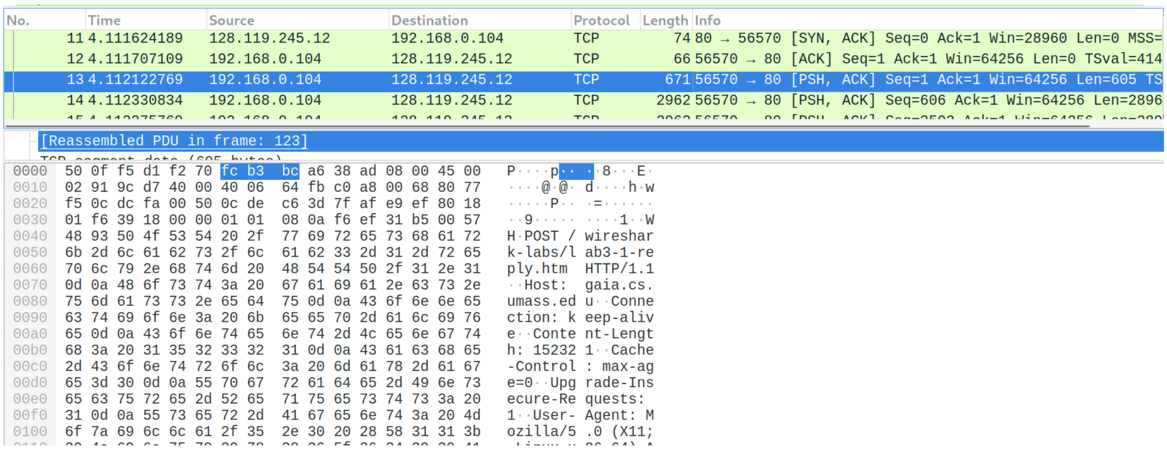


```
No.  Time         Source          Destination     Protocol Length Info
   1 0.000000000  192.168.0.104   151.101.86.248  TCP        66 46668 → 443 [ACK] Seq=1
   4 0.014894919  151.101.86.248  192.168.0.104   TCP        66 [TCP ACKed unseen segmen
   5 1.395139650  192.168.0.104   149.154.167.41  SSL       203 Continuation Data
   6 1.443920579  149.154.167.41  192.168.0.104   TCP        66 443 → 47692 [ACK] Seq=1
   9 3.926849045  192.168.0.104   128.119.245.12  TCP        66 59816 → 443 [RST, ACK] S
  10 3.926986360  192.168.0.104   128.119.245.12  TCP        74 56570 → 80 [SYN] Seq=0 W
  11 4.111624189  128.119.245.12  192.168.0.104   TCP        74 80 → 56570 [SYN, ACK] Se
  12 4.111707109  192.168.0.104   128.119.245.12  TCP        66 56570 → 80 [ACK] Seq=1 A
  13 4.112122769  192.168.0.104   128.119.245.12  TCP       671 56570 → 80 [PSH, ACK] Se
  14 4.112330834  192.168.0.104   128.119.245.12  TCP      2962 56570 → 80 [PSH, ACK] Se
  15 4.112375769  192.168.0.104   128.119.245.12  TCP      2962 56570 → 80 [PSH, ACK] Se
  16 4.113345886  192.168.0.104   128.119.245.12  TCP      2962 56570 → 80 [PSH, ACK] Se
```

```
Sequence Number: 0    (relative sequence number)
Sequence Number (raw): 2142235118
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 215926333
1010 .... = Header Length: 40 bytes (10)
Flags: 0x012 (SYN, ACK)
Window: 28960
[Calculated window size: 28960]
```

Порядковый номер SYNACK сегмента – 11 (в то же время Seq=0).
В поле подтверждения хранится значение 215926333. Это в точности Sequence Number SYN сегмента + 1. Понять, что данный сегмент SYNACK, можно посмотрев на поле Flags (там написано SYN, ACK).

5.



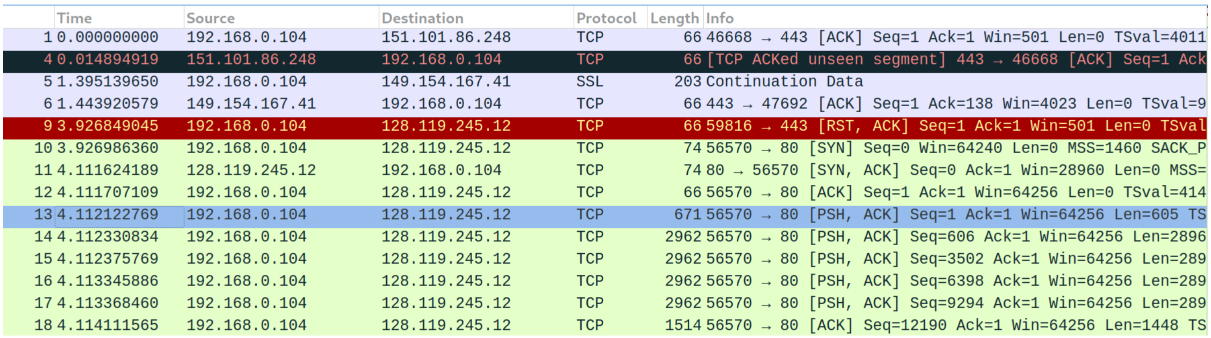
```
No.  Time         Source          Destination     Protocol Length Info
  11 4.111624189  128.119.245.12  192.168.0.104   TCP        74 80 → 56570 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=
  12 4.111707109  192.168.0.104   128.119.245.12  TCP        66 56570 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=414
  13 4.112122769  192.168.0.104   128.119.245.12  TCP       671 56570 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=605 TS
  14 4.112330834  192.168.0.104   128.119.245.12  TCP      2962 56570 → 80 [PSH, ACK] Seq=606 Ack=1 Win=64256 Len=2896
```

```
[Reassembled PDU in frame: 123]
```

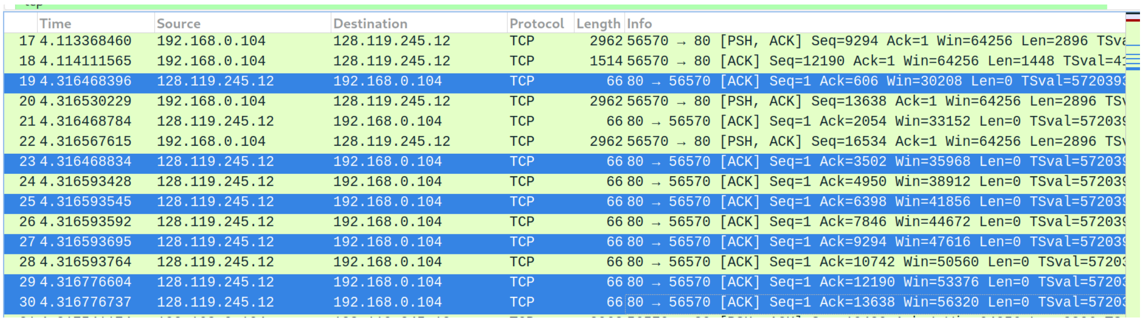
```
0000  50 0f f5 d1 f2 70 fc b3  bc a6 38 ad 08 00 45 00   P····p·· ·8···E·
0010  02 91 9c d7 40 00 40 06  64 fb c0 a8 00 68 80 77   ····@·@· d····h·w
0020  f5 0c dc fa 00 50 0c de  c6 3d 7f af e9 ef 80 18   ·····P·· ·=······
0030  01 f6 39 18 00 00 01 01  08 0a f6 ef 31 b5 00 57   ··9····· ····1··W
0040  48 93 50 4f 53 54 20 2f  77 69 72 65 73 68 61 72   H·POST / wireshar
0050  6b 2d 6c 61 62 73 2f 6c  61 62 33 2d 31 2d 72 65   k-labs/l ab3-1-re
0060  70 6c 79 2e 68 74 6d 20  48 54 54 50 2f 31 2e 31   ply.htm  HTTP/1.1
0070  0d 0a 48 6f 73 74 3a 20  67 61 69 61 2e 63 73 2e   ··Host:  gaia.cs.
0080  75 6d 61 73 73 2e 65 64  75 0d 0a 43 6f 6e 6e 65   umass.ed u··Conne
0090  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
00a0  65 0d 0a 43 6f 6e 74 65  6e 74 2d 4c 65 6e 67 74   e··Conte nt-Lengt
00b0  68 3a 20 31 35 32 33 32  31 0d 0a 43 61 63 68 65   h: 15232 1··Cache
00c0  2d 43 6f 6e 74 72 6f 6c  3a 20 6d 61 78 2d 61 67   -Control : max-ag
00d0  65 3d 30 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   e=0··Upg rade-Ins
00e0  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a 20   ecure-Re quests: 
00f0  31 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   1··User- Agent: M
0100  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
```

Порядковый номер – 13

6.



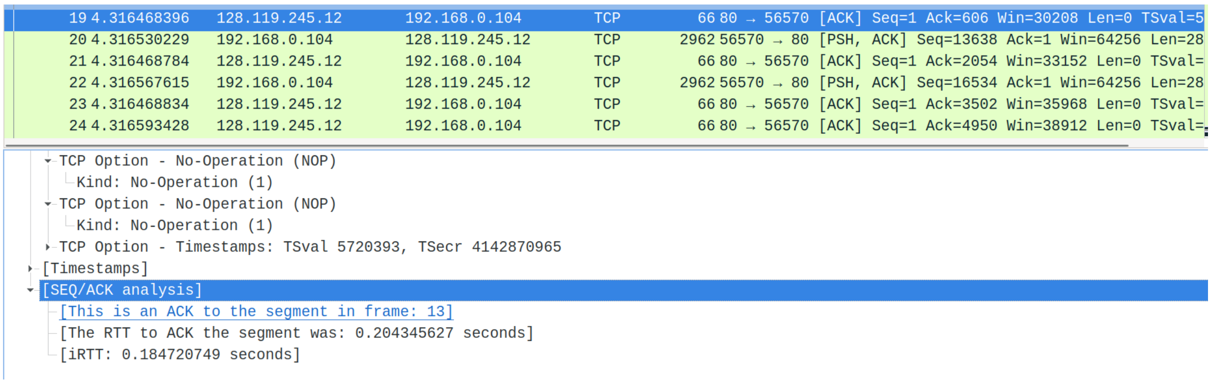
```
     Time         Source          Destination     Protocol Length Info
   1 0.000000000  192.168.0.104   151.101.86.248  TCP        66 46668 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=4011
   4 0.014894919  151.101.86.248  192.168.0.104   TCP        66 [TCP ACKed unseen segment] 443 → 46668 [ACK] Seq=1 Ack
   5 1.395139650  192.168.0.104   149.154.167.41  SSL       203 Continuation Data
   6 1.443920579  149.154.167.41  192.168.0.104   TCP        66 443 → 47692 [ACK] Seq=1 Ack=138 Win=4023 Len=0 TSval=9
   9 3.926849045  192.168.0.104   128.119.245.12  TCP        66 59816 → 443 [RST, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval
  10 3.926986360  192.168.0.104   128.119.245.12  TCP        74 56570 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_P
  11 4.111624189  128.119.245.12  192.168.0.104   TCP        74 80 → 56570 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=
  12 4.111707109  192.168.0.104   128.119.245.12  TCP        66 56570 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=414
  13 4.112122769  192.168.0.104   128.119.245.12  TCP       671 56570 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=605 TS
  14 4.112330834  192.168.0.104   128.119.245.12  TCP      2962 56570 → 80 [PSH, ACK] Seq=606 Ack=1 Win=64256 Len=2896
  15 4.112375769  192.168.0.104   128.119.245.12  TCP      2962 56570 → 80 [PSH, ACK] Seq=3502 Ack=1 Win=64256 Len=289
  16 4.113345886  192.168.0.104   128.119.245.12  TCP      2962 56570 → 80 [PSH, ACK] Seq=6398 Ack=1 Win=64256 Len=289
  17 4.113368460  192.168.0.104   128.119.245.12  TCP      2962 56570 → 80 [PSH, ACK] Seq=9294 Ack=1 Win=64256 Len=289
  18 4.114111565  192.168.0.104   128.119.245.12  TCP      1514 56570 → 80 [ACK] Seq=12190 Ack=1 Win=64256 Len=1448 TS
```



	Time	Source	Destination	Protocol	Length	Info
17	4.113368460	192.168.0.104	128.119.245.12	TCP	2962	56570 → 80 [PSH, ACK] Seq=9294 Ack=1 Win=64256 Len=2896 TSva
18	4.114111565	192.168.0.104	128.119.245.12	TCP	1514	56570 → 80 [ACK] Seq=12190 Ack=1 Win=64256 Len=1448 TSval=4
19	4.316468396	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=606 Win=30208 Len=0 TSval=572039
20	4.316530229	192.168.0.104	128.119.245.12	TCP	2962	56570 → 80 [PSH, ACK] Seq=13638 Ack=1 Win=64256 Len=2896 TS
21	4.316468784	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=2054 Win=33152 Len=0 TSval=57203
22	4.316567615	192.168.0.104	128.119.245.12	TCP	2962	56570 → 80 [PSH, ACK] Seq=16534 Ack=1 Win=64256 Len=2896 TS
23	4.316468834	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=3502 Win=35968 Len=0 TSval=57203
24	4.316593428	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=4950 Win=38912 Len=0 TSval=57203
25	4.316593545	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=6398 Win=41856 Len=0 TSval=57203
26	4.316593592	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=7846 Win=44672 Len=0 TSval=57203
27	4.316593695	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=9294 Win=47616 Len=0 TSval=57203
28	4.316593764	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=10742 Win=50560 Len=0 TSval=5720
29	4.316776604	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=12190 Win=53376 Len=0 TSval=5720
30	4.316776737	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=13638 Win=56320 Len=0 TSval=5720

Порядковые номера 13-18. Времена отправки указаны в поле Time на первом скрине, времена получения ACK-пакетов (выделенные синим) указаны в поле Time на втором скрине.

Разница (RTT) для пары сегментов 13, 19 показана на скрине (0.204345627s) (для остальных пар аналогично):

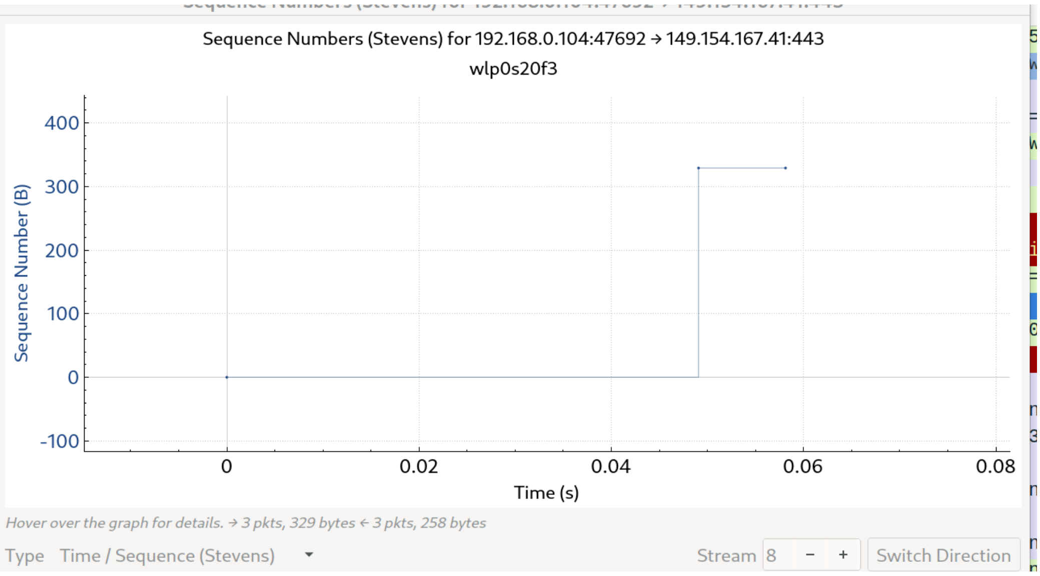


19	4.316468396	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=606 Win=30208 Len=0 TSval=5
20	4.316530229	192.168.0.104	128.119.245.12	TCP	2962	56570 → 80 [PSH, ACK] Seq=13638 Ack=1 Win=64256 Len=28
21	4.316468784	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=2054 Win=33152 Len=0 TSval=
22	4.316567615	192.168.0.104	128.119.245.12	TCP	2962	56570 → 80 [PSH, ACK] Seq=16534 Ack=1 Win=64256 Len=28
23	4.316468834	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=3502 Win=35968 Len=0 TSval=
24	4.316593428	128.119.245.12	192.168.0.104	TCP	66	80 → 56570 [ACK] Seq=1 Ack=4950 Win=38912 Len=0 TSval=

```
  ▾ TCP Option - No-Operation (NOP)
      Kind: No-Operation (1)
  ▾ TCP Option - No-Operation (NOP)
      Kind: No-Operation (1)
  ▸ TCP Option - Timestamps: TSval 5720393, TSecr 4142870965
▸ [Timestamps]
▾ [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 13]
    [The RTT to ACK the segment was: 0.204345627 seconds]
    [iRTT: 0.184720749 seconds]
```

7. Передано – 152,138 байт (размер файла alice.txt). Время отправки первого SYN-пакета – 3.926986360 секунд, время получения последнего ACK-пакета – 4.934425321 секунды. Скорость составляет – 152138 / (4.934425321 - 3.926986360) = 151014.608219 байт / с.

Wireshark: Работа с Time-Sequence-Graph (Stevens) (2 балла).



Hover over the graph for details. → 3 pkts, 329 bytes ← 3 pkts, 258 bytes