

Задачи по 6-й лабораторной

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

1) Src: 192.168.0.104, Src Port: 58278

No.	Time	Source	Destination	Protocol	Length	Info
169	7.549111292	192.168.0.104	128.119.245.12	HTTP	321	POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1 (text/plain)
207	7.724164907	128.119.245.12	192.168.0.104	HTTP	843	HTTP/1.1 200 OK (text/html)

```

> Frame 169: 321 bytes on wire (2568 bits), 321 bytes captured (2568 bits) on interface wlo1, id 0
> Ethernet II, Src: IntelCor_af:c4:4f (b4:69:21:af:c4:4f), Dst: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58278, Dst Port: 80, Seq: 149145, Ack: 1, Len: 255
> [104 Reassembled TCP Segments (149399 bytes): #16(1448), #17(1448), #18(1448), #19(1448), #20(1448), #21(1448), #23(1448), #24(1448), #25(1448), #26(1448), #27(1448), #28(1448), #29(1448), #30(1448), #31(1448), #32(1448), #33(1448), #34(1448), #35(1448), #36(1448), #37(1448), #38(1448), #39(1448), #40(1448), #41(1448), #42(1448), #43(1448), #44(1448), #45(1448), #46(1448), #47(1448), #48(1448), #49(1448), #50(1448), #51(1448), #52(1448), #53(1448), #54(1448), #55(1448), #56(1448), #57(1448), #58(1448), #59(1448), #60(1448), #61(1448), #62(1448), #63(1448), #64(1448), #65(1448), #66(1448), #67(1448), #68(1448), #69(1448), #70(1448), #71(1448), #72(1448), #73(1448), #74(1448), #75(1448), #76(1448), #77(1448), #78(1448), #79(1448), #80(1448), #81(1448), #82(1448), #83(1448), #84(1448), #85(1448), #86(1448), #87(1448), #88(1448), #89(1448), #90(1448), #91(1448), #92(1448), #93(1448), #94(1448), #95(1448), #96(1448), #97(1448), #98(1448), #99(1448), #100(1448), #101(1448), #102(1448), #103(1448), #104(1448), #105(1448), #106(1448), #107(1448), #108(1448), #109(1448), #110(1448), #111(1448), #112(1448), #113(1448), #114(1448), #115(1448), #116(1448), #117(1448), #118(1448), #119(1448), #120(1448), #121(1448), #122(1448), #123(1448), #124(1448), #125(1448), #126(1448), #127(1448), #128(1448), #129(1448), #130(1448), #131(1448), #132(1448), #133(1448), #134(1448), #135(1448), #136(1448), #137(1448), #138(1448), #139(1448), #140(1448), #141(1448), #142(1448), #143(1448), #144(1448), #145(1448), #146(1448), #147(1448), #148(1448), #149(1448), #150(1448), #151(1448), #152(1448), #153(1448), #154(1448), #155(1448), #156(1448), #157(1448), #158(1448), #159(1448), #160(1448), #161(1448), #162(1448), #163(1448), #164(1448), #165(1448), #166(1448), #167(1448), #168(1448), #169(1448), #170(1448), #171(1448), #172(1448), #173(1448), #174(1448), #175(1448), #176(1448), #177(1448), #178(1448), #179(1448), #180(1448), #181(1448), #182(1448), #183(1448), #184(1448), #185(1448), #186(1448), #187(1448), #188(1448), #189(1448), #190(1448), #191(1448), #192(1448), #193(1448), #194(1448), #195(1448), #196(1448), #197(1448), #198(1448), #199(1448), #200(1448), #201(1448), #202(1448), #203(1448), #204(1448), #205(1448), #206(1448), #207(1448), #208(1448), #209(1448), #210(1448), #211(1448), #212(1448), #213(1448), #214(1448), #215(1448), #216(1448), #217(1448), #218(1448), #219(1448), #220(1448), #221(1448), #222(1448), #223(1448), #224(1448), #225(1448), #226(1448), #227(1448), #228(1448), #229(1448), #230(1448), #231(1448), #232(1448), #233(1448), #234(1448), #235(1448), #236(1448), #237(1448), #238(1448), #239(1448), #240(1448), #241(1448), #242(1448), #243(1448), #244(1448), #245(1448), #246(1448), #247(1448), #248(1448), #249(1448), #250(1448), #251(1448), #252(1448), #253(1448), #254(1448), #255(1448), #256(1448), #257(1448), #258(1448), #259(1448), #260(1448), #261(1448), #262(1448), #263(1448), #264(1448), #265(1448), #266(1448), #267(1448), #268(1448), #269(1448), #270(1448), #271(1448), #272(1448), #273(1448), #274(1448), #275(1448), #276(1448), #277(1448), #278(1448), #279(1448), #280(1448), #281(1448), #282(1448), #283(1448), #284(1448), #285(1448), #286(1448), #287(1448), #288(1448), #289(1448), #290(1448), #291(1448), #292(1448), #293(1448), #294(1448), #295(1448), #296(1448), #297(1448), #298(1448), #299(1448), #300(1448), #301(1448), #302(1448), #303(1448), #304(1448), #305(1448), #306(1448), #307(1448), #308(1448), #309(1448), #310(1448), #311(1448), #312(1448), #313(1448), #314(1448), #315(1448), #316(1448), #317(1448), #318(1448), #319(1448), #320(1448), #321(1448), #322(1448), #323(1448), #324(1448), #325(1448), #326(1448), #327(1448), #328(1448), #329(1448), #330(1448), #331(1448), #332(1448), #333(1448), #334(1448), #335(1448), #336(1448), #337(1448), #338(1448), #339(1448), #340(1448), #341(1448), #342(1448), #343(1448), #344(1448), #345(1448), #346(1448), #347(1448), #348(1448), #349(1448), #350(1448), #351(1448), #352(1448), #353(1448), #354(1448), #355(1448), #356(1448), #357(1448), #358(1448), #359(1448), #360(1448), #361(1448), #362(1448), #363(1448), #364(1448), #365(1448), #366(1448), #367(1448), #368(1448), #369(1448), #370(1448), #371(1448), #372(1448), #373(1448), #374(1448), #375(1448), #376(1448), #377(1448), #378(1448), #379(1448), #380(1448), #381(1448), #
```

2) Dst: 128.119.245.12, Dst port: 80

3) Sequence number (raw): 580654141, Sequence number: 0 (relative sequence number).

Определяется соответствующим флагом SYN.

```

> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 128.119.245.12
✓ Transmission Control Protocol, Src Port: 58278, Dst Port: 80, Seq: 0, Len: 0
  - Source Port: 58278
  - Destination Port: 80
  - [Stream index: 2]
  - [TCP Segment Len: 0]
  - Sequence number: 0 (relative sequence number)
  - Sequence number (raw): 580654141
  - [Next sequence number: 1 (relative sequence number)]
  - Acknowledgment number: 0
  - Acknowledgment number (raw): 0
  - 1010 .... = Header Length: 40 bytes (10)
  > Flags: 0x002 (SYN)
  - Window size value: 64240
  - [Calculated window size: 64240]

```

4) Sequence number (raw): 3509045917, Sequence number: 0 (relative sequence number).

В поле подтверждения: Acknowledgment number (raw): 580654142, это Sequence number (raw) у SYN-сегмента плюс 1. То, что это SYNACK-сегмент определяется двумя флагами (SYN, ACK).

11	6.992021080	192.168.0.104	128.119.245.12	TCP	74	58280 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
12	6.997318864	192.168.0.104	128.119.245.12	TCP	74	58280 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
13	6.947885310	192.168.0.104	128.119.245.12	TCP	74	80 → 58278 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA...
14	6.950783848	128.119.245.12	192.168.0.104	TCP	66	58278 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1818451713...
15	6.950884735	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=1448 TSval=1818451...
16	6.951594804	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] Seq=1449 Ack=1 Win=64256 Len=1448 TSval=181...
17	6.951627337	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [ACK] Seq=2897 Ack=1 Win=64256 Len=1448 TSval=1818...
18	6.951651552	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] Seq=4345 Ack=1 Win=64256 Len=1448 TSval=1818...
19	6.951657833	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [ACK] Seq=5793 Ack=1 Win=64256 Len=1448 TSval=1818...
20	6.965592653	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] Seq=7241 Ack=1 Win=64256 Len=1448 TSval=1818...
21	6.965623163	192.168.0.104	128.119.245.12	TCP	81	Standard query 0x0000 PTR _mywifiext._tcp.local, "QM" question
22	6.968607236	10.33.51.198	224.0.0.251	MDNS	1514	58278 → 80 [ACK] Seq=8689 Ack=1 Win=64256 Len=1448 TSval=1818...
23	6.995398325	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] Seq=10137 Ack=1 Win=64256 Len=1448 TSva...
24	6.995429333	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [ACK] Seq=11585 Ack=1 Win=64256 Len=1448 TSval=181...
25	7.021495232	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] Seq=13033 Ack=1 Win=64256 Len=1448 TSva...
26	7.021530228	192.168.0.104	128.119.245.12	TCP	74	80 → 58280 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA...
27	7.121937271	128.119.245.12	192.168.0.104	TCP	66	58280 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1818451805...

> Frame 14: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlo1, id 0

> Ethernet II, Src: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70), Dst: IntelCor_af:c4:4f (b4:69:21:af:c4:4f)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.104

✓ Transmission Control Protocol, Src Port: 80, Dst Port: 58278, Seq: 0, Ack: 1, Len: 0

Source Port: 80

Destination Port: 58278

[Stream index: 2]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Sequence number (raw): 3509045917

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 580654142

1010 = Header Length: 40 bytes (10)

> Flags: 0x012 (SYN, ACK)

Window size value: 28960

[Calculated window size: 28960]

5). TCP-сегмент, содержащий команду POST имеет:

Sequence number (raw): 580654142, Sequence number: 1 (relative sequence number)

No.	Time	Source	Destination	Protocol	Length	Info
13	6.947885310	192.168.0.104	128.119.245.12	TCP	74	58280 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
14	6.950783848	128.119.245.12	192.168.0.104	TCP	74	80 → 58278 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA...
15	6.950884735	192.168.0.104	128.119.245.12	TCP	66	58278 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1818451713...
16	6.951594804	128.119.245.12	192.168.0.104	TCP	1514	58278 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=1448 TSval=1818451...
17	6.951627337	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] Seq=1449 Ack=1 Win=64256 Len=1448 TSval=181...
18	6.951651552	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [ACK] Seq=2897 Ack=1 Win=64256 Len=1448 TSval=1818...
19	6.951657833	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] Seq=4345 Ack=1 Win=64256 Len=1448 TSval=181...
20	6.965592653	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [ACK] Seq=5793 Ack=1 Win=64256 Len=1448 TSval=1818...
21	6.965623163	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] Seq=7241 Ack=1 Win=64256 Len=1448 TSval=1818...
22	6.968607236	10.33.51.198	224.0.0.251	MDNS	81	Standard query 0x0000 PTR _mywifiext._tcp.local, "QM" question
23	6.995398325	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [ACK] Seq=8689 Ack=1 Win=64256 Len=1448 TSval=1818...
24	6.995429333	192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] Seq=10137 Ack=1 Win=64256 Len=1448 TSva...

[TCP Segment Len: 1448]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 580654142

[Next sequence number: 1449 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 3509045918

1000 = Header Length: 32 bytes (8)

> Flags: 0x010 (ACK)

Window size value: 502

[Calculated window size: 64256]

[Window size scaling factor: 128]

Checksum: 0x2657 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

> [SEQ/ACK analysis]

> [Timestamps]

TCP payload (1448 bytes)

[Reassembled PDU in frame: 169]

TCP segment data (1448 bytes)

```

0040 e5 9b 60 4f 53 54 20 2f 77 69 72 65 73 68 61 72 ..POST / wireshar
0050 00 20 6c 61 62 73 2f 6c 61 62 33 2d 31 2d 72 65 /libs/1 ab5-1-re
0060 70 6c 79 2e 68 74 6d 29 48 54 54 50 2f 31 2e 31 ply.htm HTTP/1.1
0070 04 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 55 73 65 72 2d umass.ed u-User:
0090 41 67 65 6e 74 3a 20 46 67 7a 69 6c 6c 61 2f 35 Agent: Mozilla/5
00a0 2a 30 20 28 5b 31 31 3b 20 5b 60 75 6e 74 75 3b /5 (X11; Ubuntu;
00b0 29 4c 69 6e 75 78 20 79 38 3e 5f 3e 3a 3b 20 72 Linux x 86_64; r
00c0 76 3a 39 39 2e 30 29 20 47 65 63 6b 6f 2f 32 38 v:99.0) Gecko/20
00d0 31 38 30 31 30 31 20 46 69 72 65 66 6f 78 2f 39 108101 Firefox/9
00e0 30 2e 30 04 0a 41 63 63 76 74 3a 20 74 65 78 0.0; Acc opt: tex
00f0 74 2f 68 74 6d 6c 2c 61 70 78 6e 69 63 61 74 68 /html/a publicat

```

6). TCP-сегмент, содержащий команду POST, мы рассмотрели в предыдущем номере.

Рассмотрим следующие 5.

2: Sequence number (raw): 580655590, Sequence number: 1449 (relative sequence number)

3: Sequence number (raw): 580657038, Sequence number: 2897 (relative sequence number)

4: Sequence number (raw): 580658486, Sequence number: 4345 (relative sequence number)

5: Sequence number (raw): 580659934, Sequence number: 5793 (relative sequence number)

6: Sequence number (raw): 580661382, Sequence number: 7241 (relative sequence number)

Времена отправки:

No.	Time	✓	Source	Destination	Protocol	Length	Info
16	2022-05-07 13:26:47,266910537		192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [ACK] Seq=1
17	2022-05-07 13:26:47,266943070		192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] S
18	2022-05-07 13:26:47,266967285		192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [ACK] Seq=28
19	2022-05-07 13:26:47,266973566		192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] S
20	2022-05-07 13:26:47,280908386		192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [ACK] Seq=57
21	2022-05-07 13:26:47,280938896		192.168.0.104	128.119.245.12	TCP	1514	58278 → 80 [PSH, ACK] S

Время получения АСК-пакетов для каждого сегмента:

27	2022-05-07	13:26:47,437253004	128.119.245.12	192.168.0.104	TCP	74 80 → 58280 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA...
28	2022-05-07	13:26:47,437370926	192.168.0.104	128.119.245.12	TCP	66 58280 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1818451885...
29	2022-05-07	13:26:47,454489299	128.119.245.12	192.168.0.104	TCP	66 80 → 58278 [ACK] Seq=1 Ack=1449 Win=31872 Len=0 TSval=3022448...
30	2022-05-07	13:26:47,454589100	192.168.0.104	128.119.245.12	TCP	1514 58278 → 80 [ACK] Seq=14481 Ack=1 Win=64256 Len=1448 TSval=181...
31	2022-05-07	13:26:47,454626092	192.168.0.104	128.119.245.12	TCP	1514 58278 → 80 [PSH, ACK] Seq=15929 Ack=1 Win=64256 Len=1448 TSva...
32	2022-05-07	13:26:47,470659910	128.119.245.12	192.168.0.104	TCP	66 80 → 58278 [ACK] Seq=1 Ack=2897 Win=34816 Len=0 TSval=3022448...
33	2022-05-07	13:26:47,470755293	192.168.0.104	128.119.245.12	TCP	1514 58278 → 80 [ACK] Seq=17377 Ack=1 Win=64256 Len=1448 TSval=181...
34	2022-05-07	13:26:47,470792263	192.168.0.104	128.119.245.12	TCP	1514 58278 → 80 [PSH, ACK] Seq=18825 Ack=1 Win=64256 Len=1448 TSva...
35	2022-05-07	13:26:47,489385244	128.119.245.12	192.168.0.104	TCP	66 80 → 58278 [ACK] Seq=1 Ack=4345 Win=37760 Len=0 TSval=3022448...
36	2022-05-07	13:26:47,489503811	192.168.0.104	128.119.245.12	TCP	1514 58278 → 80 [ACK] Seq=20273 Ack=1 Win=64256 Len=1448 TSval=181...
37	2022-05-07	13:26:47,489541747	192.168.0.104	128.119.245.12	TCP	1514 58278 → 80 [PSH, ACK] Seq=21721 Ack=1 Win=64256 Len=1448 TSva...
38	2022-05-07	13:26:47,504677229	128.119.245.12	192.168.0.104	TCP	66 80 → 58278 [ACK] Seq=1 Ack=5793 Win=40576 Len=0 TSval=3022448...
39	2022-05-07	13:26:47,504774907	192.168.0.104	128.119.245.12	TCP	1514 58278 → 80 [ACK] Seq=23169 Ack=1 Win=64256 Len=1448 TSval=181...
40	2022-05-07	13:26:47,504811081	192.168.0.104	128.119.245.12	TCP	1514 58278 → 80 [PSH, ACK] Seq=24617 Ack=1 Win=64256 Len=1448 TSva...
41	2022-05-07	13:26:47,511769008	128.119.245.12	192.168.0.104	TCP	66 80 → 58278 [ACK] Seq=1 Ack=7241 Win=43520 Len=0 TSval=3022448...
42	2022-05-07	13:26:47,511861337	192.168.0.104	128.119.245.12	TCP	1514 58278 → 80 [ACK] Seq=26065 Ack=1 Win=64256 Len=1448 TSval=181...
43	2022-05-07	13:26:47,511897936	192.168.0.104	128.119.245.12	TCP	1514 58278 → 80 [PSH, ACK] Seq=27513 Ack=1 Win=64256 Len=1448 TSva...
44	2022-05-07	13:26:47,522213713	128.119.245.12	192.168.0.104	TCP	66 80 → 58278 [ACK] Seq=1 Ack=8689 Win=46336 Len=0 TSval=3022448...

Пакеты действительно те, если в поле [SEQ/ACK analysis] нажать на [This is an ACK to the segment in frame: 16], то перенесемся как раз на рассмотренные выше пакеты.

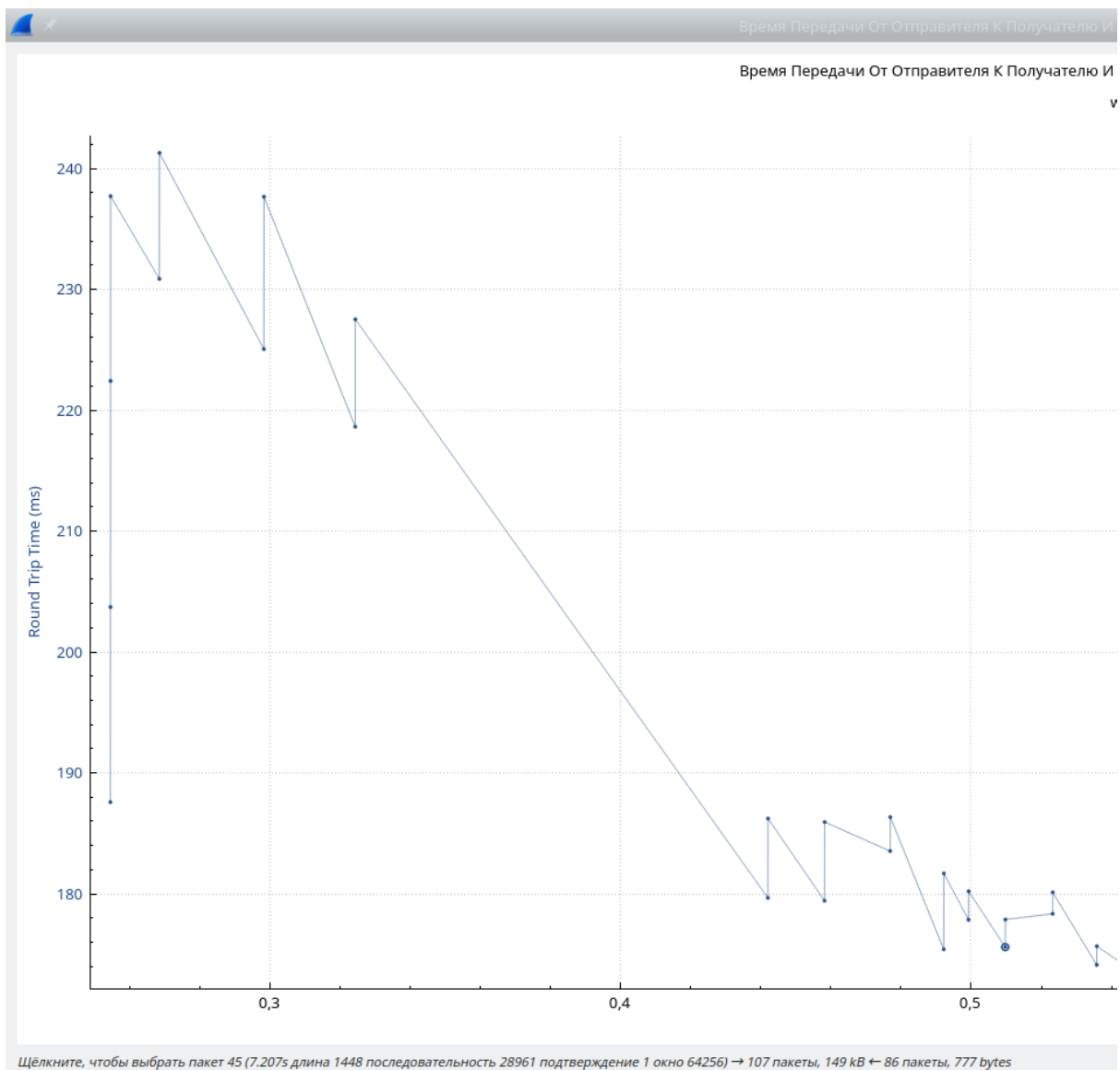
[SEQ/ACK analysis]

- [This is an ACK to the segment in frame: 16]
- [The RTT to ACK the segment was: 0.187578762 seconds]
- [iRTT: 0.253565871 seconds]

[Timestamps]

RTT посмотрим на графике (первые 6 точек слева)

1: 187,5 ms, 2: 203,5 ms, 3: 222,5 ms, 4: 238 ms, 5: 231 ms, 6: 241,5 ms



7). Время между получением последнего ACK сегмента и отправкой первого SYN равно 3215.79438453 мс = 3.21579438453 с. Размер нашего файла 158138 байт. Тогда пропускная способность равна $158138 / 3.21579438453 = 49175.4077191$ байт / с.

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

