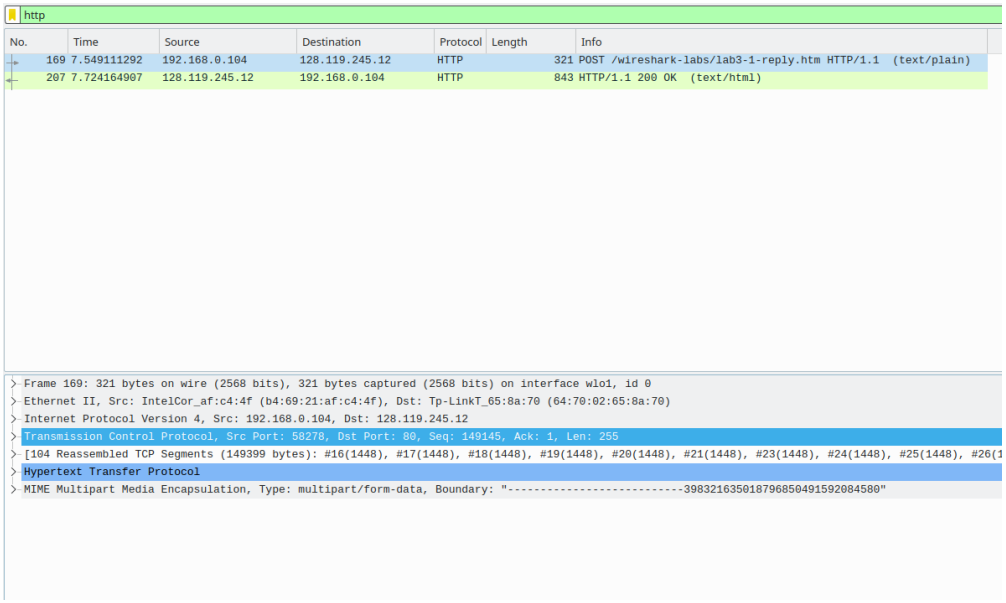
Задачи по 6-й лабораторной

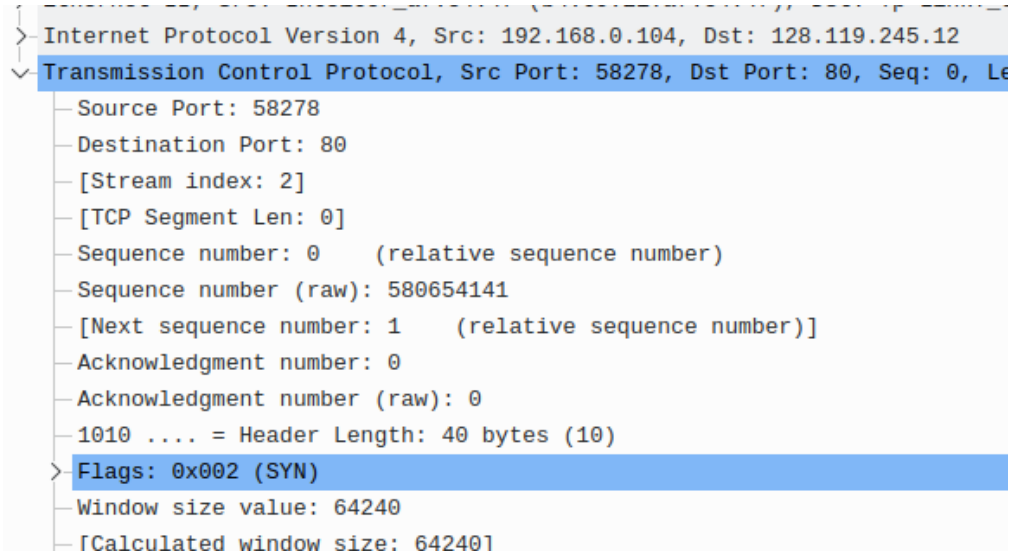
1. Перехват TCP-передачи данных от вашего компьютера удаленному серверу

1) Src: 192.168.0.104, Src Port: 58278

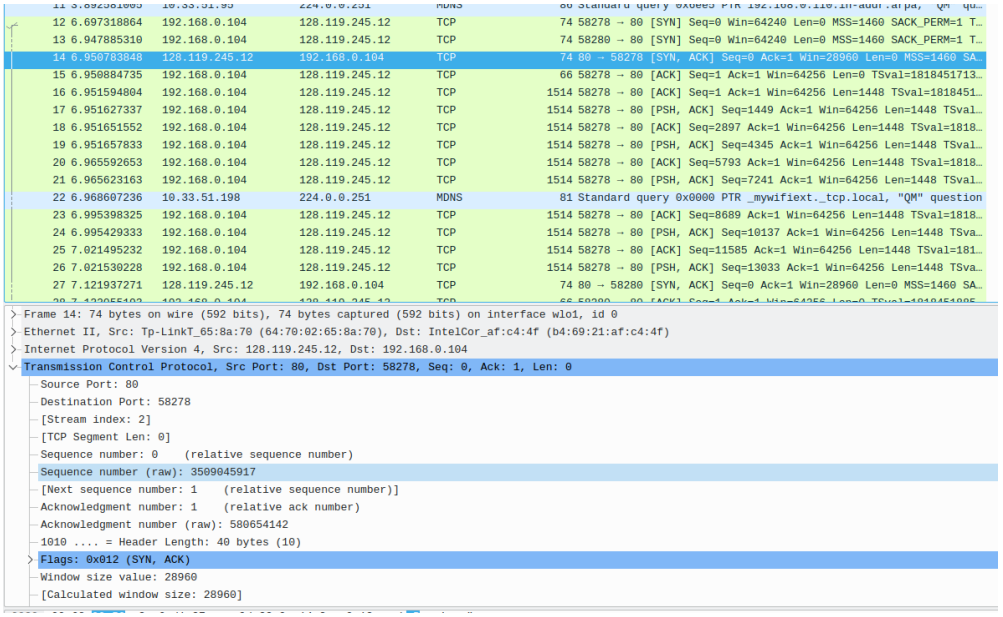


2) Dst: 128.119.245.12, Dst port: 80

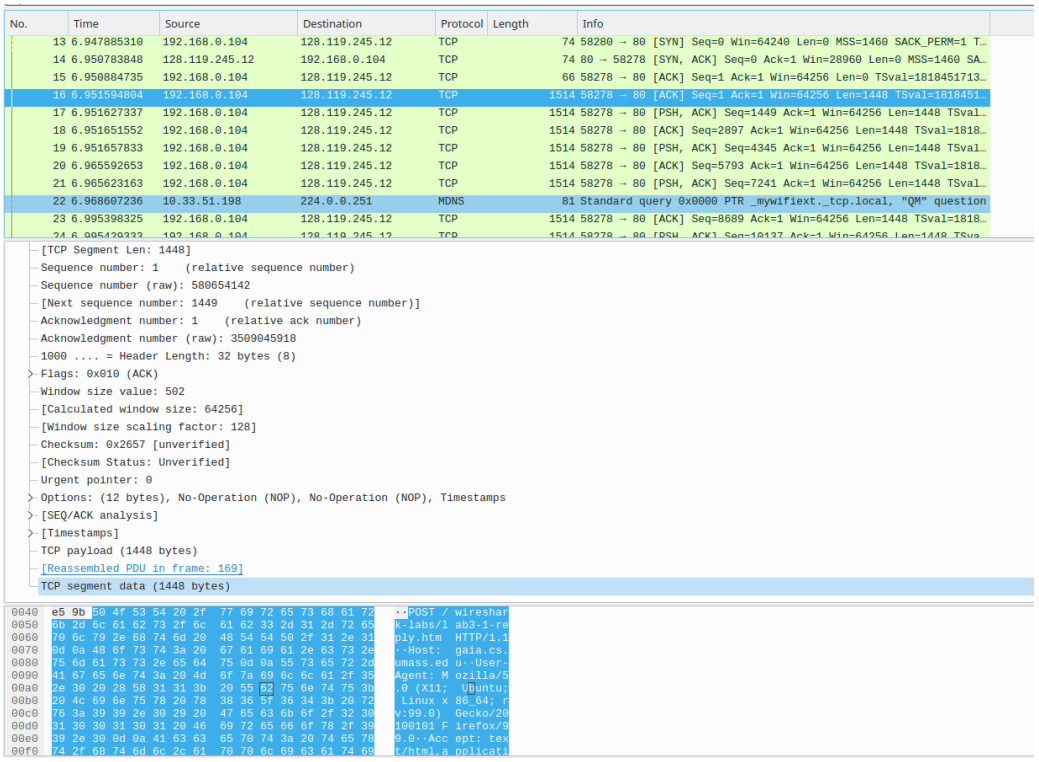
3) Sequence number (raw): 580654141, Sequence number: 0 (relative sequence number). Определяется соответствующим флагом SYN.



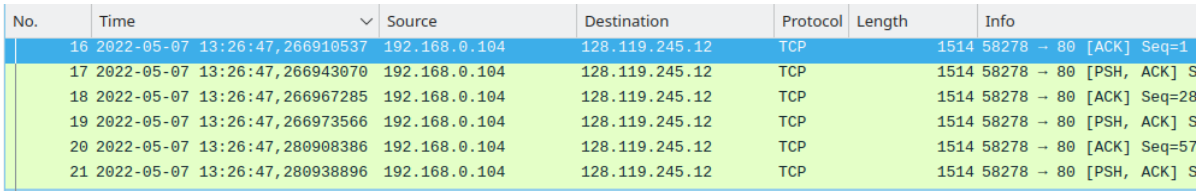
4) Sequence number (raw): 3509045917, Sequence number: 0 (relative sequence number). В поле подтверждения: Acknowledgment number (raw): 580654142, это Sequence number (raw) у SYN-сегмента плюс 1. То, что это SYNACK-сегмент определяется двумя флагами (SYN, ACK).



5). TCP-сегмент, содержащий команду POST имеет:
Sequence number (raw): 580654142, Sequence number: 1 (relative sequence number)



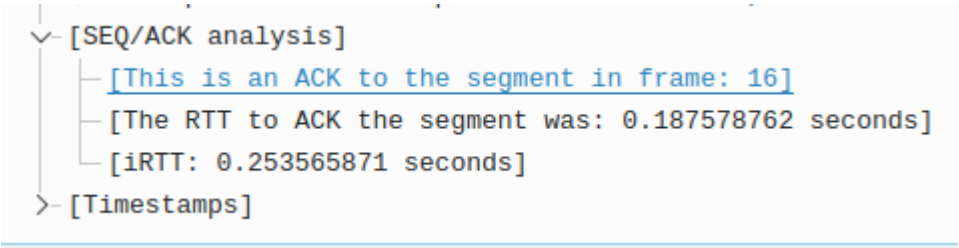
6). TCP-сегмент, содержащий команду POST, мы рассмотрели в предыдущем номере.
Рассмотрим следующие 5.
2: Sequence number (raw): 580655590, Sequence number: 1449 (relative sequence number)
3: Sequence number (raw): 580657038, Sequence number: 2897 (relative sequence number)
4: Sequence number (raw): 580658486, 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:



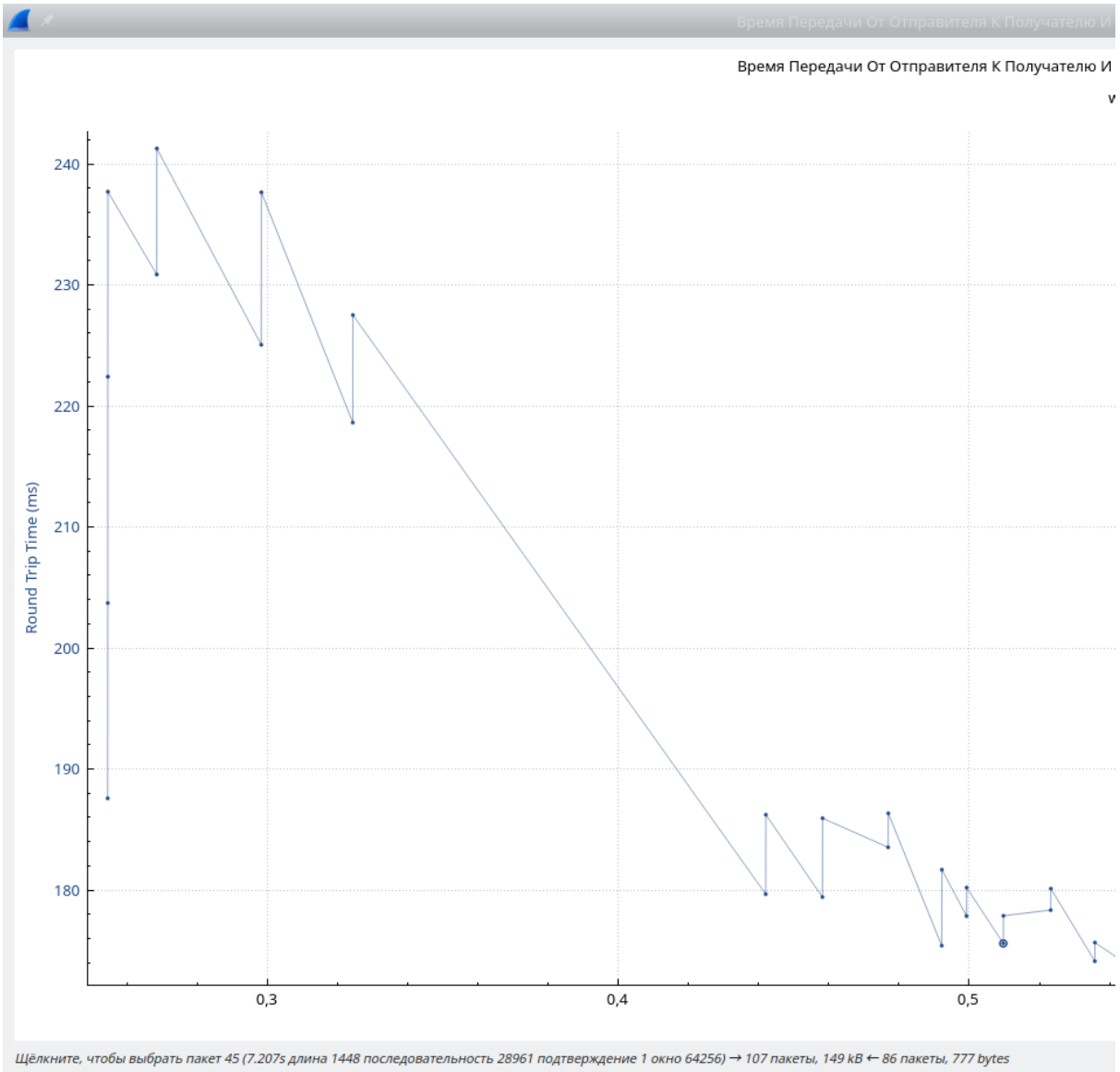
Время получения ACK-пакетов для каждого сегмента:

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.



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)