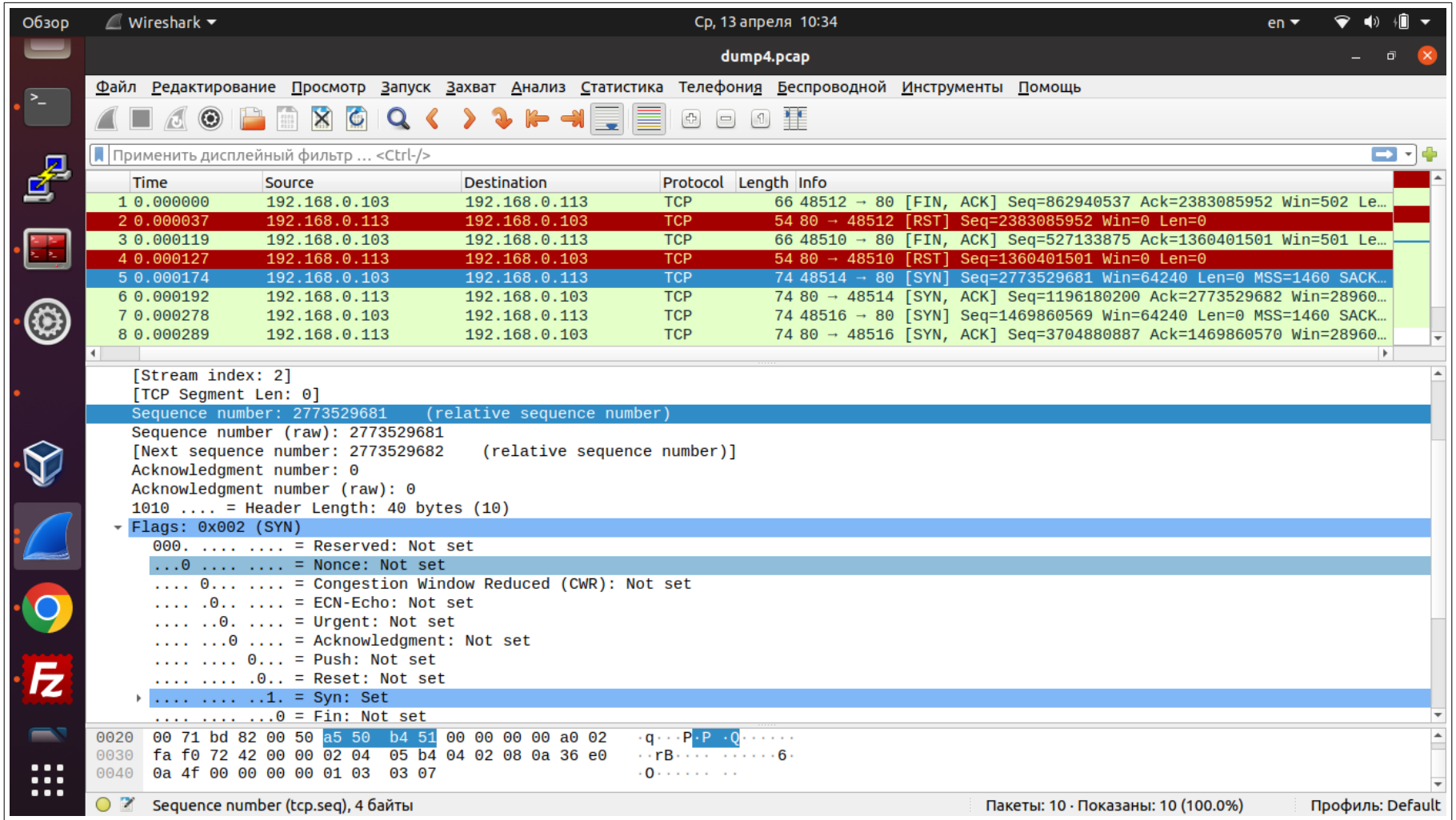
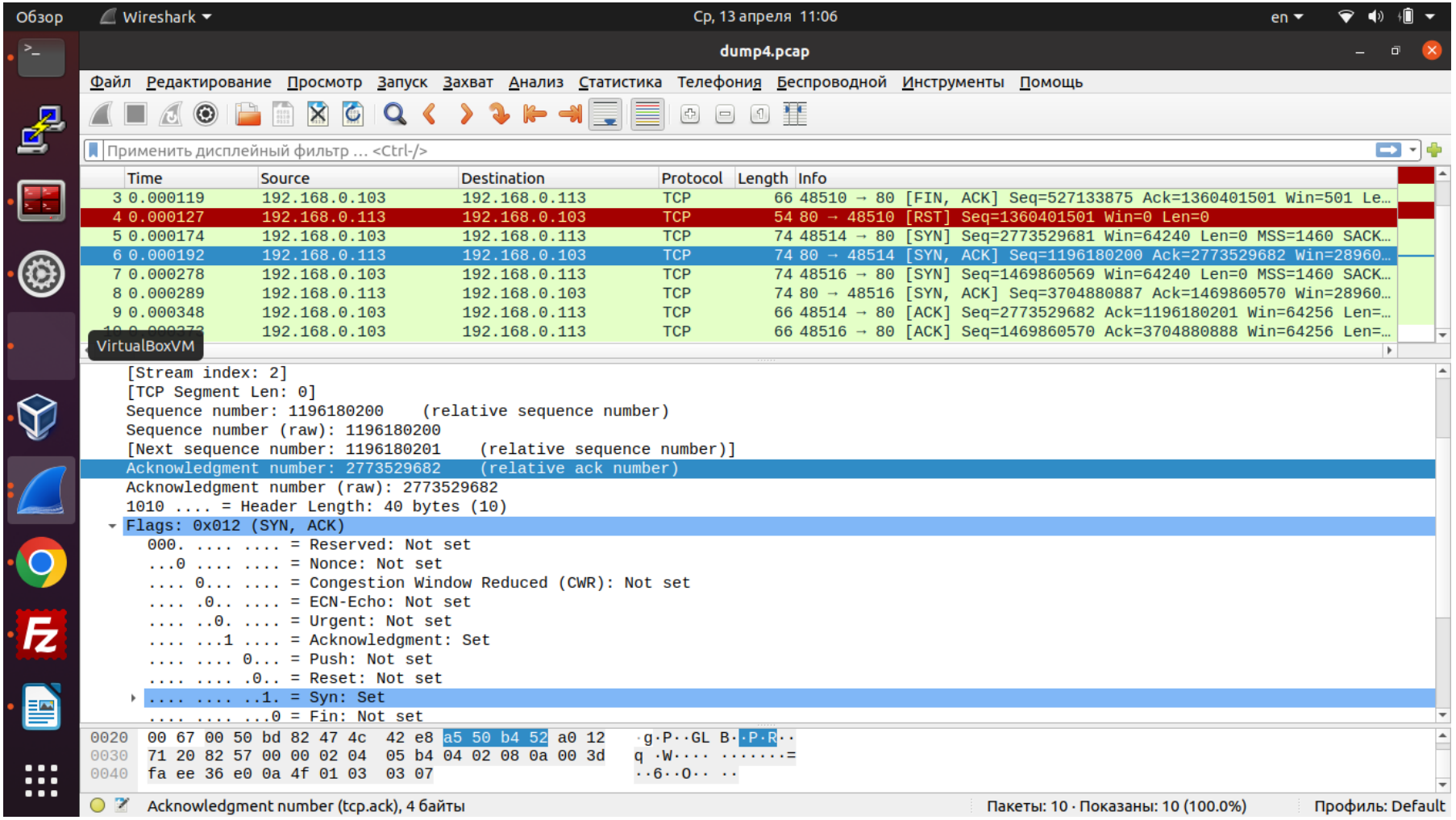
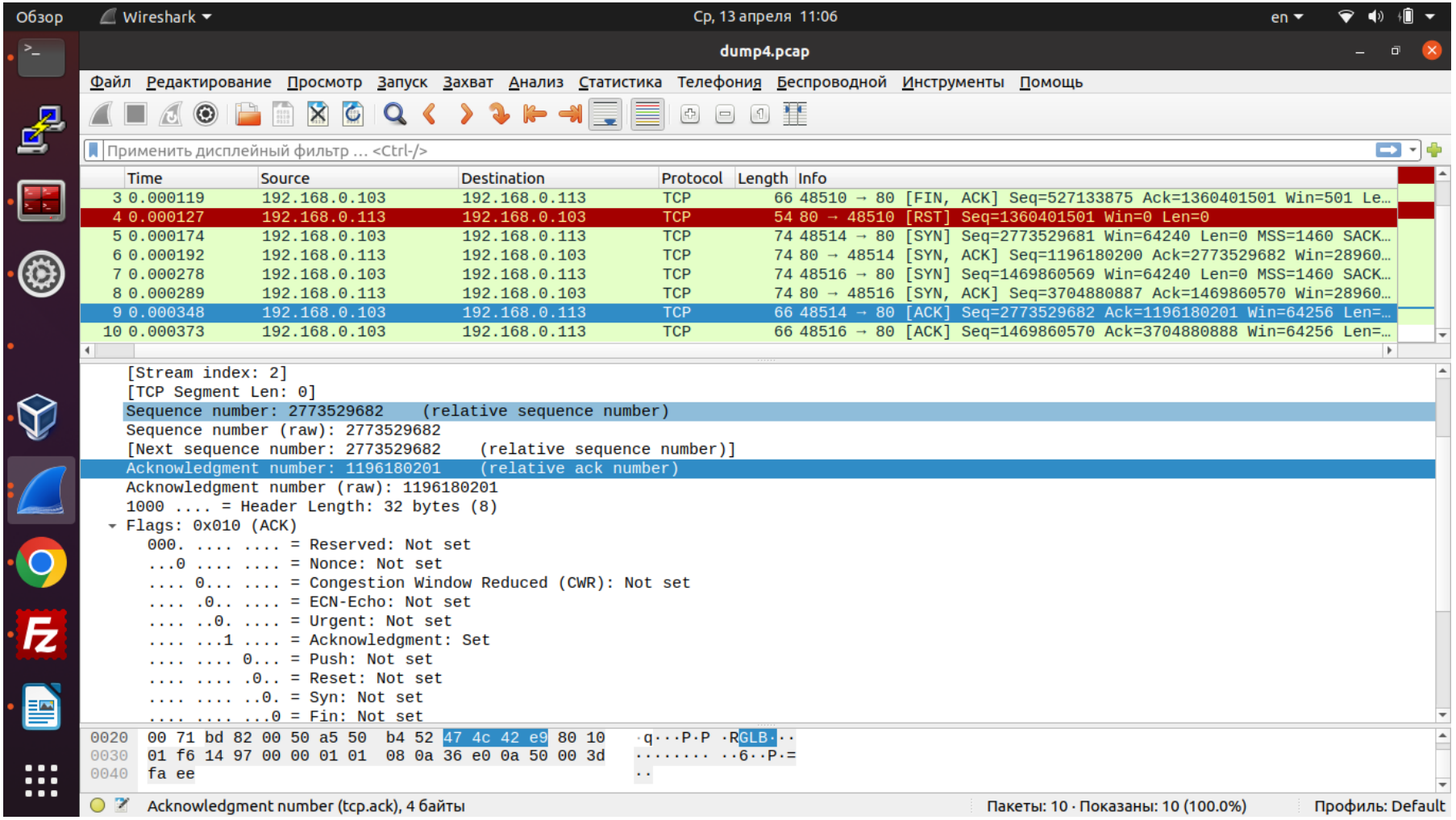
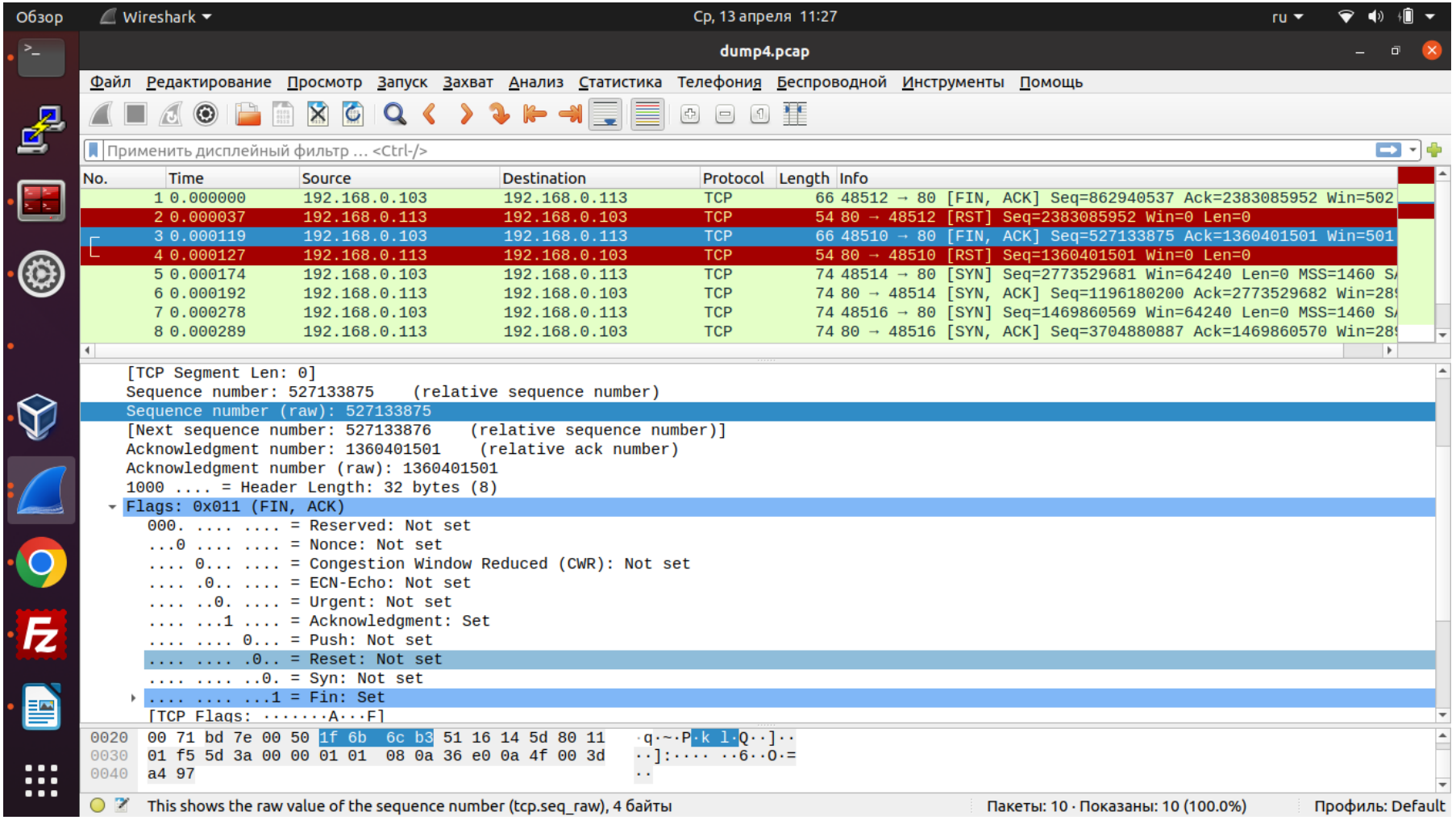
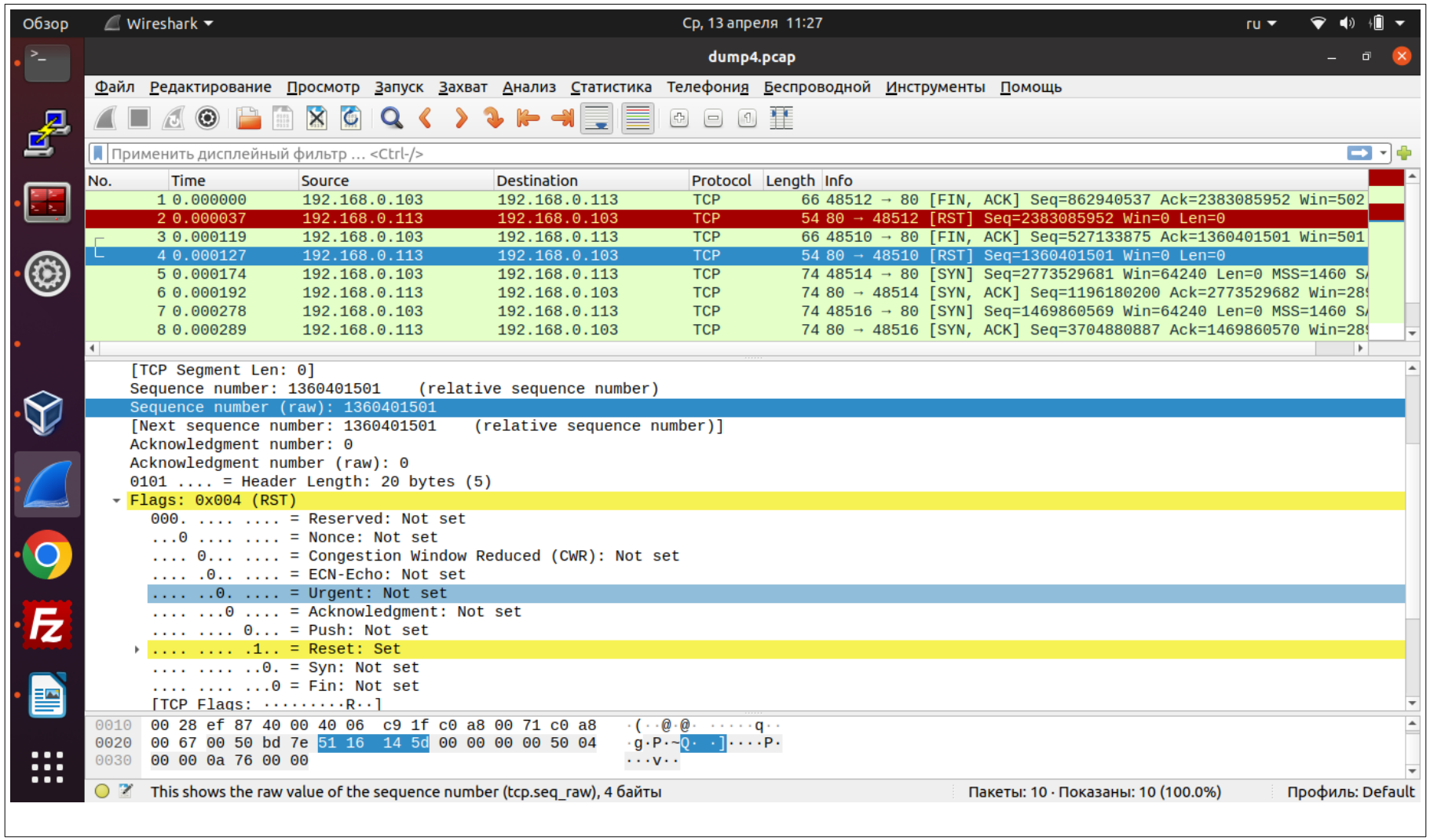

Обзор
Wireshark
Ср, 13 апреля 10:34
en
dump4.pcap
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
Применить дисплейный фильтр … <Ctrl-/>
Time Source Destination Protocol Length Info
1 0.000000 192.168.0.103 192.168.0.113 TCP 66 48512 → 80 [FIN, ACK] Seq=862940537 Ack=2383085952 Win=502 Le…
2 0.000037 192.168.0.113 192.168.0.103 TCP 54 80 → 48512 [RST] Seq=2383085952 Win=0 Len=0
3 0.000119 192.168.0.103 192.168.0.113 TCP 66 48510 → 80 [FIN, ACK] Seq=527133875 Ack=1360401501 Win=501 Le…
4 0.000127 192.168.0.113 192.168.0.103 TCP 54 80 → 48510 [RST] Seq=1360401501 Win=0 Len=0
5 0.000174 192.168.0.103 192.168.0.113 TCP 74 48514 → 80 [SYN] Seq=2773529681 Win=64240 Len=0 MSS=1460 SACK…
6 0.000192 192.168.0.113 192.168.0.103 TCP 74 80 → 48514 [SYN, ACK] Seq=1196180200 Ack=2773529682 Win=28960…
7 0.000278 192.168.0.103 192.168.0.113 TCP 74 48516 → 80 [SYN] Seq=1469860569 Win=64240 Len=0 MSS=1460 SACK…
8 0.000289 192.168.0.113 192.168.0.103 TCP 74 80 → 48516 [SYN, ACK] Seq=3704880887 Ack=1469860570 Win=28960…
[Stream index: 2]
[TCP Segment Len: 0]
Sequence number: 2773529681 (relative sequence number)
Sequence number (raw): 2773529681
[Next sequence number: 2773529682 (relative sequence number)]
Acknowledgment number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
....0 = Fin: Not set
0020 00 71 bd 82 00 50 a5 50 b4 51 00 00 00 00 a0 02
0030 fa f0 72 42 00 00 02 04 05 b4 04 02 08 0a 36 e0
0040 0a 4f 00 00 00 00 01 03 03 07
Sequence number (tcp.seq), 4 байты
Пакеты: 10 · Показаны: 10 (100.0%)
Профиль: Default


Обзор
Wireshark
Ср, 13 апреля 11:06
en
dump4.pcap
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
Применить дисплейный фильтр … <Ctrl-/>
Time Source Destination Protocol Length Info
3 0.000119 192.168.0.103 192.168.0.113 TCP 66 48510 → 80 [FIN, ACK] Seq=527133875 Ack=1360401501 Win=501 Le…
4 0.000127 192.168.0.113 192.168.0.103 TCP 54 80 → 48510 [RST] Seq=1360401501 Win=0 Len=0
5 0.000174 192.168.0.103 192.168.0.113 TCP 74 48514 → 80 [SYN] Seq=2773529681 Win=64240 Len=0 MSS=1460 SACK…
6 0.000192 192.168.0.113 192.168.0.103 TCP 74 80 → 48514 [SYN, ACK] Seq=1196180200 Ack=2773529682 Win=28960…
7 0.000278 192.168.0.103 192.168.0.113 TCP 74 48516 → 80 [SYN] Seq=1469860569 Win=64240 Len=0 MSS=1460 SACK…
8 0.000289 192.168.0.113 192.168.0.103 TCP 74 80 → 48516 [SYN, ACK] Seq=3704880887 Ack=1469860570 Win=28960…
9 0.000348 192.168.0.103 192.168.0.113 TCP 66 48514 → 80 [ACK] Seq=2773529682 Ack=1196180201 Win=64256 Len=…
66 48516 → 80 [ACK] Seq=1469860570 Ack=3704880888 Win=64256 Len=…
VirtualBoxVM
[Stream index: 2]
[TCP Segment Len: 0]
Sequence number: 1196180200 (relative sequence number)
Sequence number (raw): 1196180200
[Next sequence number: 1196180201 (relative sequence number)]
Acknowledgment number: 2773529682 (relative ack number)
Acknowledgment number (raw): 2773529682
1010 .... = Header Length: 40 bytes (10)
Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
....0 = Fin: Not set
0020 00 67 00 50 bd 82 47 4c 42 e8 a5 50 b4 52 a0 12 ·g·P··GL B··P·R··
0030 71 20 82 57 00 00 02 04 05 b4 04 02 08 0a 00 3d q ·W···· ·······=
0040 fa ee 36 e0 0a 4f 01 03 03 07 ··6··O·· ··
Acknowledgment number (tcp.ack), 4 байты
Пакеты: 10 · Показаны: 10 (100.0%)
Профиль: Default


Обзор
Wireshark
Ср, 13 апреля 11:06
en
dump4.pcap
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
Применить дисплейный фильтр … <Ctrl-/>
Time Source Destination Protocol Length Info
3 0.000119 192.168.0.103 192.168.0.113 TCP 66 48510 → 80 [FIN, ACK] Seq=527133875 Ack=1360401501 Win=501 Le…
4 0.000127 192.168.0.113 192.168.0.103 TCP 54 80 → 48510 [RST] Seq=1360401501 Win=0 Len=0
5 0.000174 192.168.0.103 192.168.0.113 TCP 74 48514 → 80 [SYN] Seq=2773529681 Win=64240 Len=0 MSS=1460 SACK…
6 0.000192 192.168.0.113 192.168.0.103 TCP 74 80 → 48514 [SYN, ACK] Seq=1196180200 Ack=2773529682 Win=28960…
7 0.000278 192.168.0.103 192.168.0.113 TCP 74 48516 → 80 [SYN] Seq=1469860569 Win=64240 Len=0 MSS=1460 SACK…
8 0.000289 192.168.0.113 192.168.0.103 TCP 74 80 → 48516 [SYN, ACK] Seq=3704880887 Ack=1469860570 Win=28960…
9 0.000348 192.168.0.103 192.168.0.113 TCP 66 48514 → 80 [ACK] Seq=2773529682 Ack=1196180201 Win=64256 Len=…
10 0.000373 192.168.0.103 192.168.0.113 TCP 66 48516 → 80 [ACK] Seq=1469860570 Ack=3704880888 Win=64256 Len=…
[Stream index: 2]
[TCP Segment Len: 0]
Sequence number: 2773529682 (relative sequence number)
Sequence number (raw): 2773529682
[Next sequence number: 2773529682 (relative sequence number)]
Acknowledgment number: 1196180201 (relative ack number)
Acknowledgment number (raw): 1196180201
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
0020 00 71 bd 82 00 50 a5 50 b4 52 47 4c 42 e9 80 10 ·q···P·P ·RGLB···
0030 01 f6 14 97 00 00 01 01 08 0a 36 e0 0a 50 00 3d ······ ··6··P·=
0040 fa ee ··
Acknowledgment number (tcp.ack), 4 байты
Пакеты: 10 · Показаны: 10 (100.0%)
Профиль: Default


Обзор
Wireshark
Ср, 13 апреля 11:27
ru
dump4.pcap
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
Применить дисплейный фильтр … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.103 192.168.0.113 TCP 66 48512 → 80 [FIN, ACK] Seq=862940537 Ack=2383085952 Win=502
2 0.000037 192.168.0.113 192.168.0.103 TCP 54 80 → 48512 [RST] Seq=2383085952 Win=0 Len=0
3 0.000119 192.168.0.103 192.168.0.113 TCP 66 48510 → 80 [FIN, ACK] Seq=527133875 Ack=1360401501 Win=501
4 0.000127 192.168.0.113 192.168.0.103 TCP 54 80 → 48510 [RST] Seq=1360401501 Win=0 Len=0
5 0.000174 192.168.0.103 192.168.0.113 TCP 74 48514 → 80 [SYN] Seq=2773529681 Win=64240 Len=0 MSS=1460 S
6 0.000192 192.168.0.113 192.168.0.103 TCP 74 80 → 48514 [SYN, ACK] Seq=1196180200 Ack=2773529682 Win=28
7 0.000278 192.168.0.103 192.168.0.113 TCP 74 48516 → 80 [SYN] Seq=1469860569 Win=64240 Len=0 MSS=1460 S
8 0.000289 192.168.0.113 192.168.0.103 TCP 74 80 → 48516 [SYN, ACK] Seq=3704880887 Ack=1469860570 Win=28
[TCP Segment Len: 0]
Sequence number: 527133875 (relative sequence number)
Sequence number (raw): 527133875
[Next sequence number: 527133876 (relative sequence number)]
Acknowledgment number: 1360401501 (relative ack number)
Acknowledgment number (raw): 1360401501
1000 .... = Header Length: 32 bytes (8)
Flags: 0x011 (FIN, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....1 = Fin: Set
[TCP Flags: ·····A···F]
0020 00 71 bd 7e 00 50 1f 6b 6c b3 51 16 14 5d 80 11 ·q·~·P·k l·Q··]··
0030 01 f5 5d 3a 00 00 01 01 08 0a 36 e0 0a 4f 00 3d ··]:···· ··6··O·=
0040 a4 97 ··
This shows the raw value of the sequence number (tcp.seq_raw), 4 байты
Пакеты: 10 · Показаны: 10 (100.0%)
Профиль: Default



Снят дамп VM с порта 80 при включенном nginx
По портам видно что происходит соединение между портом клиента 48514, 48516 и порт 80

№5
Порт 48514 это порт src
Порт 80 это порт dct
По src и dct видно что это запрос от клиента
установка соединения флаг стоит в строке
syn: set значит что был отправлен запрос на соединение syn
Номером байта
Sequence number: 2773529681
Acknowledgment numbe =0
Следующий номер байта в ответе должен быть
Next sequence number: 2773529682

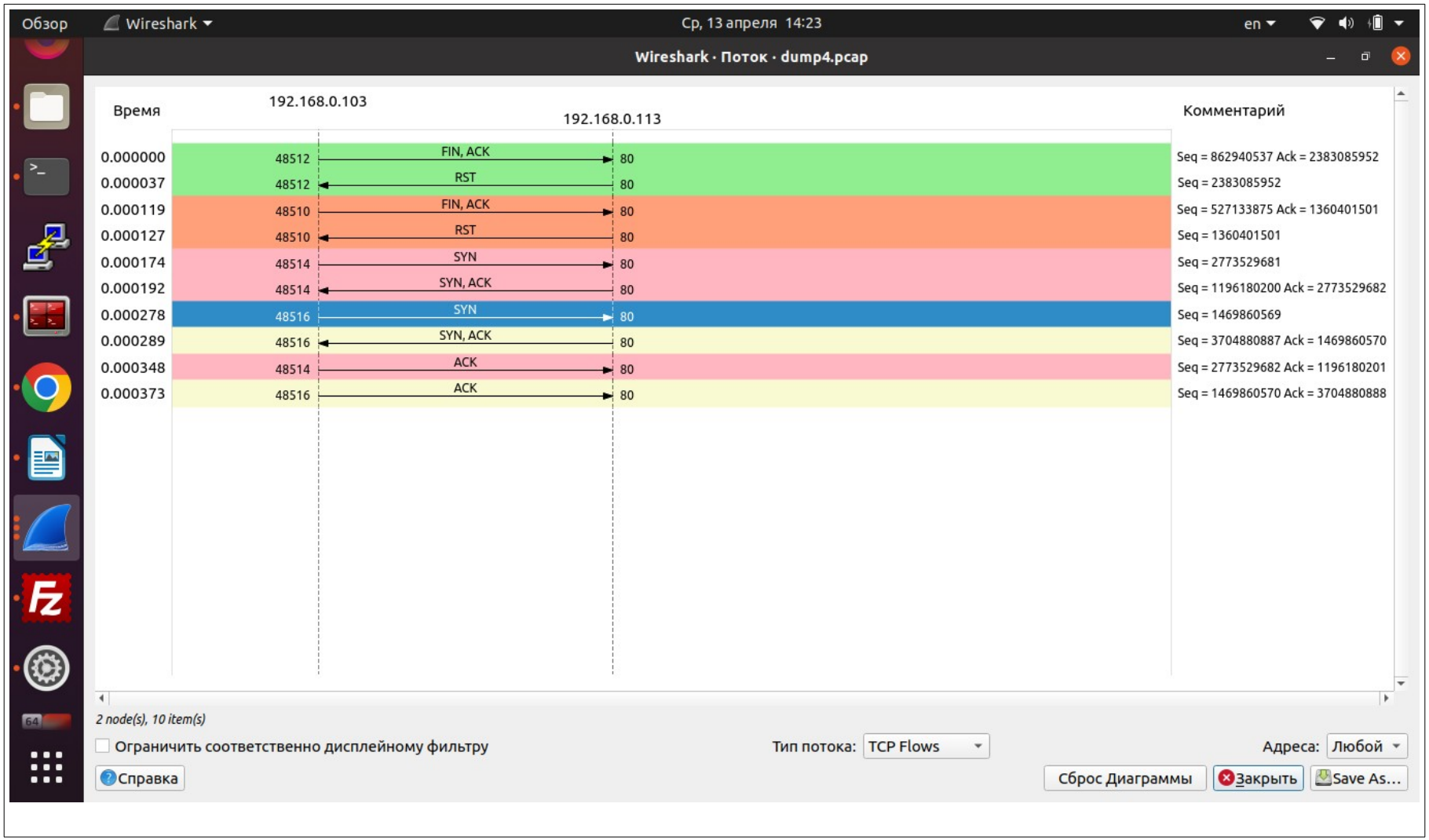
№6
Порт 80 это порт src
Порт 48514 это порт dct
По src и dct видно что это ответ от сервера
получаем ответ флаг стоит в строке
syn: set
acknowledgment; set значит мы получили ответ
Номером байта
Acknowledgment number: 2773529682 по номеру видно что номер соответствует Next sequence number: 2773529682 из строки №5 что значит что это ответ на наш запрос.
Sequence number: 1196180200
Следующий номер байта в ответе должен быть
Next sequence number: 1196180201

№9
Порт 48514 это порт src
Порт 80 это порт dct
По src и dct видно что это ответ от клиента
получаем ответ и разрешение на соединение флаг стоит в строке
acknowledgment; set
syn: set флага нет
Номером байта
Sequence number: 2773529682

Acknowledgment number: 1196180201 по номеру видно что номер соответствует Next sequence number: 1196180201 что означает что это ответ на запрос из строки №6

№3
Порт 48510 это порт src
Порт 80 это порт dct
По src и dct видно что это запрос от клиента
получаем запрос на разрыв соединения флаг стоит
acknowledgment; set
Fin: Set
Номер байта
Acknowledgment number: 1360401501

№4
Порт 80 это порт src
Порт 48510 это порт dct
По src и dct видно что это ответ от сервера о закрытие без пакета FIN чаще всего такое когда пользователь сам прервал соединение (например, закрыв браузер, не дожидаясь ответа); соединение не было нормально закрыто, но находится в неактивном состоянии некоторое время.
получаем ответ на разрыв соединения флаг стоит только в
Reset: Set
Номером полученного байта
Sequence number : 1360401501 что значит что это ответ от запроса с строки №3



Раздел статистика — график потока так же видно подключение портов 48514 и 80 (фиолетовый цвет)