Лабораторная работа 3

Генералов Даниил, НПИбд-01-21, 1032202280

2023

[1]RUDN University, Moscow, Russian Federation

Задача

Задача

3.3.1.1.1. Изучение возможностей команды ipconfig для ОС типа Windows (ifconfig для систем типа Linux). 3.3.1.1.2. Определение MAC-адреса устройства и его типа. 3.3.2.1.1. Установить на домашнем устройстве Wireshark. 3.3.2.1.2. С помощью Wireshark захватить и проанализировать пакеты ARP и ICMP в части кадров канального уровня. 3.3.3.1. С помощью Wireshark захватить и проанализировать пакеты HTTP, DNS в части заголовков и информации протоколов TCP, UDP, QUIC. 3.3.4.1. С помощью Wireshark проанализировать handshake протокола TCP.

Выполнение

ip addr

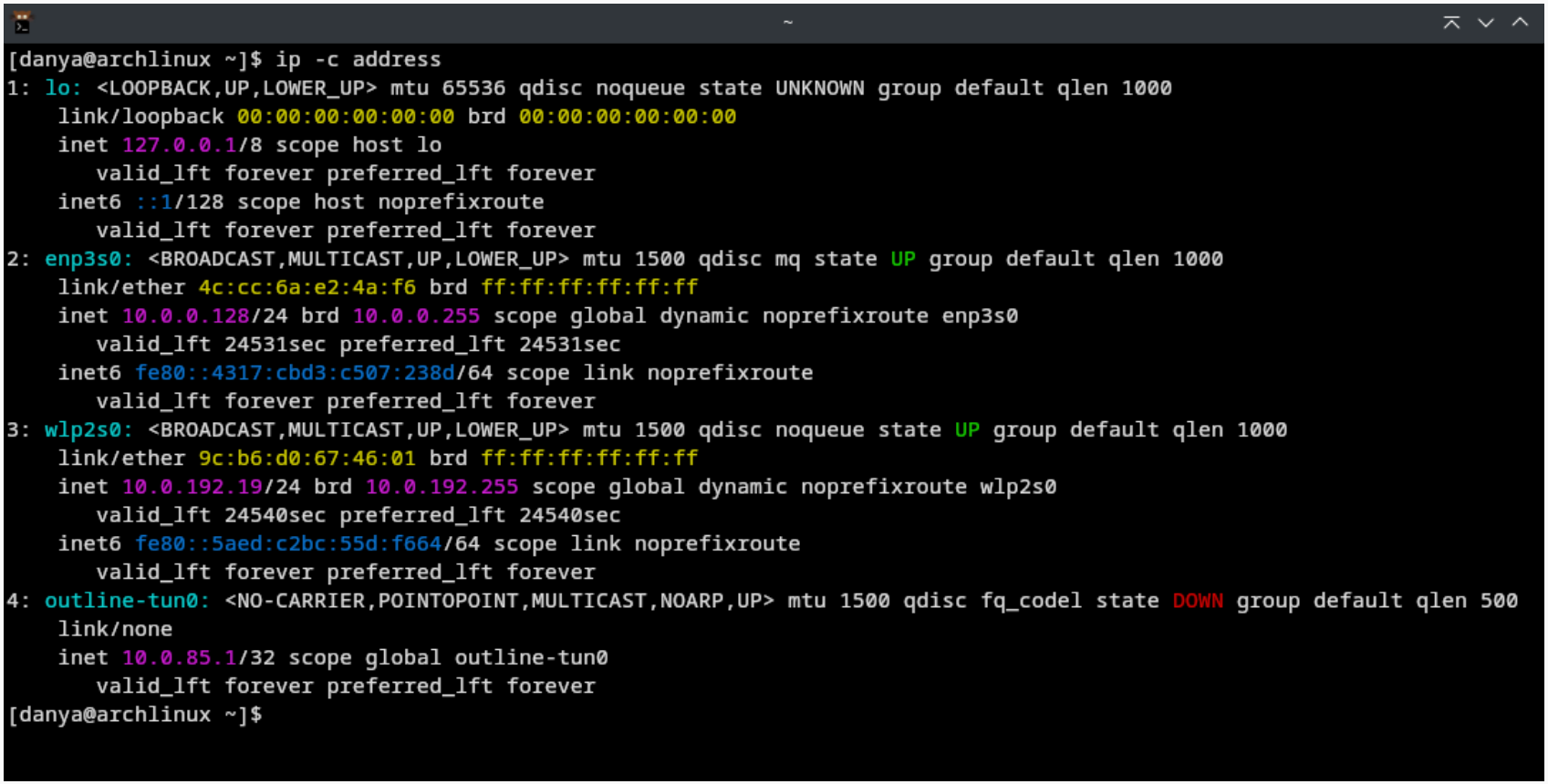

Рис. 1: ip addr

ip link, route, neighbor

```
[danya@archlinux ~]$ ip -c link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
    link/ether 4c:cc:6a:e2:4a:f6 brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode DORMANT group default qlen 1000
    link/ether 9c:b6:d0:67:46:01 brd ff:ff:ff:ff:ff:ff
4: outline-tun0: <NO-CARRIER,POINTOPOINT,MULTICAST,NOARP,UP> mtu 1500 qdisc fq_codel state DOWN mode DEFAULT group default
 qlen 500
    link/none
[danya@archlinux ~]$ ip -c neighbor
10.0.0.1 dev enp3s0 lladdr 50:ff:20:8c:34:53 REACHABLE
10.0.192.3 dev wlp2s0 lladdr 60:a4:b7:ea:21:e0 REACHABLE
10.0.192.1 dev wlp2s0 lladdr 52:ff:20:8c:34:51 STALE
fe80::52ff:20ff:fe8c:3453 dev enp3s0 lladdr 50:ff:20:8c:34:53 router STALE
[danya@archlinux ~]$ ip -c route
default via 10.0.0.1 dev enp3s0 proto dhcp src 10.0.0.128 metric 100
default via 10.0.192.1 dev wlp2s0 proto dhcp src 10.0.192.19 metric 600
10.0.0.0/24 dev enp3s0 proto kernel scope link src 10.0.0.128 metric 100
10.0.85.2 dev outline-tun0 scope link src 10.0.85.1 linkdown
10.0.192.0/24 dev wlp2s0 proto kernel scope link src 10.0.192.19 metric 600
[danya@archlinux ~]$
```

Рис. 2: ip link+route+neighbor

4c:cc:6a = MSI

Micro-Star INTL CO., LTD.

Vendor | **Details**

OUI: 4C:CC:6A

Vendor name: Micro-Star INTL CO., LTD.

Address:

No.69
Lide St.

New Taipei City Taiwan 235
TW.

Assignment Type MA-L

Mac Address Block Large (previously named OUI). Number of address 2^24 (~16 Million)

Initial registration: 03 December 2015

Rivet Networks

Vendor | Details

OUI: 9C:B6:D0

Vendor name: Rivet Networks

Address:

> 11940 Jollyville Rd
> Austin tx 78759
> US.

Assignment Type MA-L

> Mac Address Block Large (previously named OUI). Number of address 2^24 (~16 Million)

Wireshark

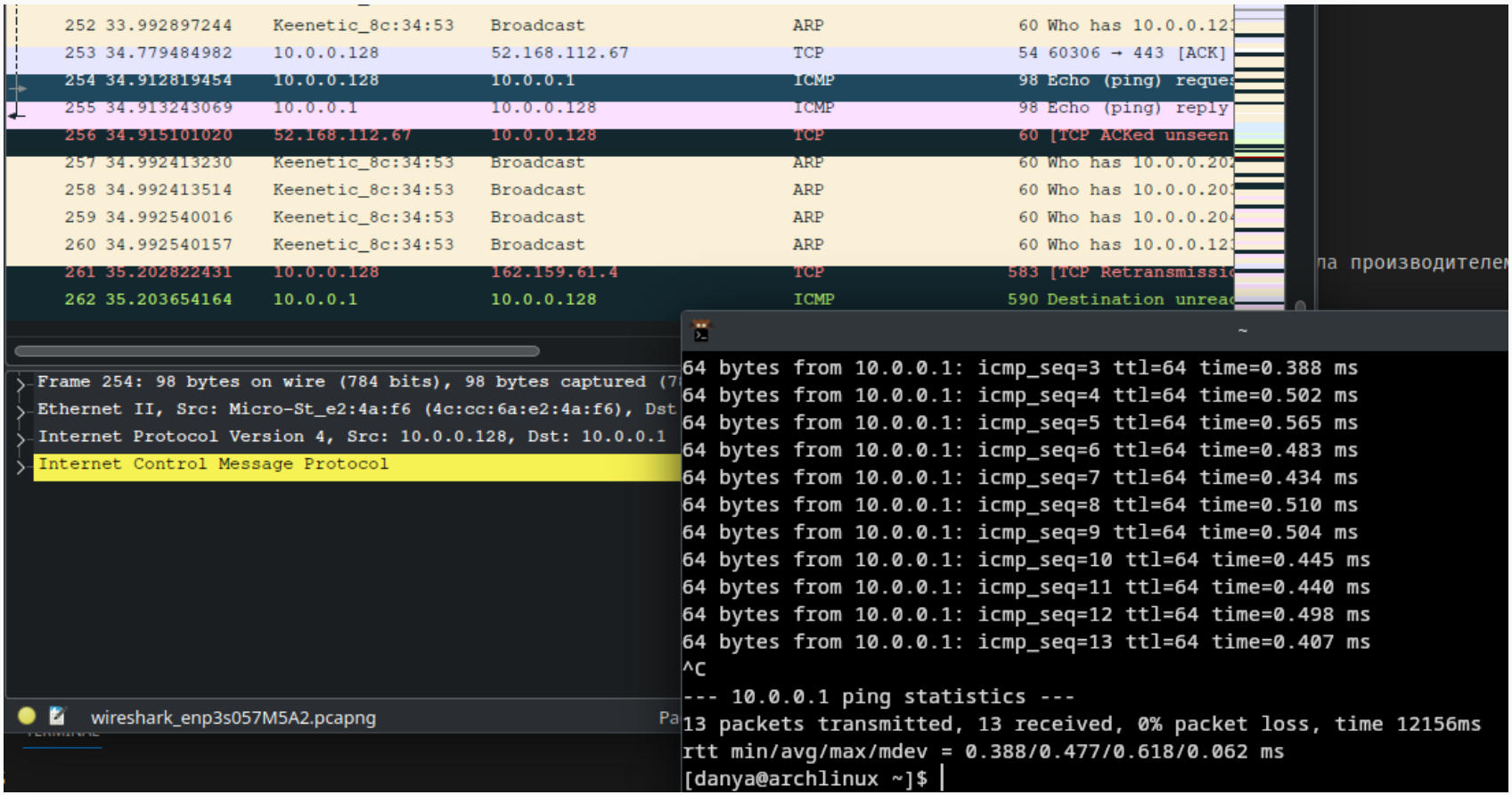

Рис. 5: wireshark

ICMP Echo

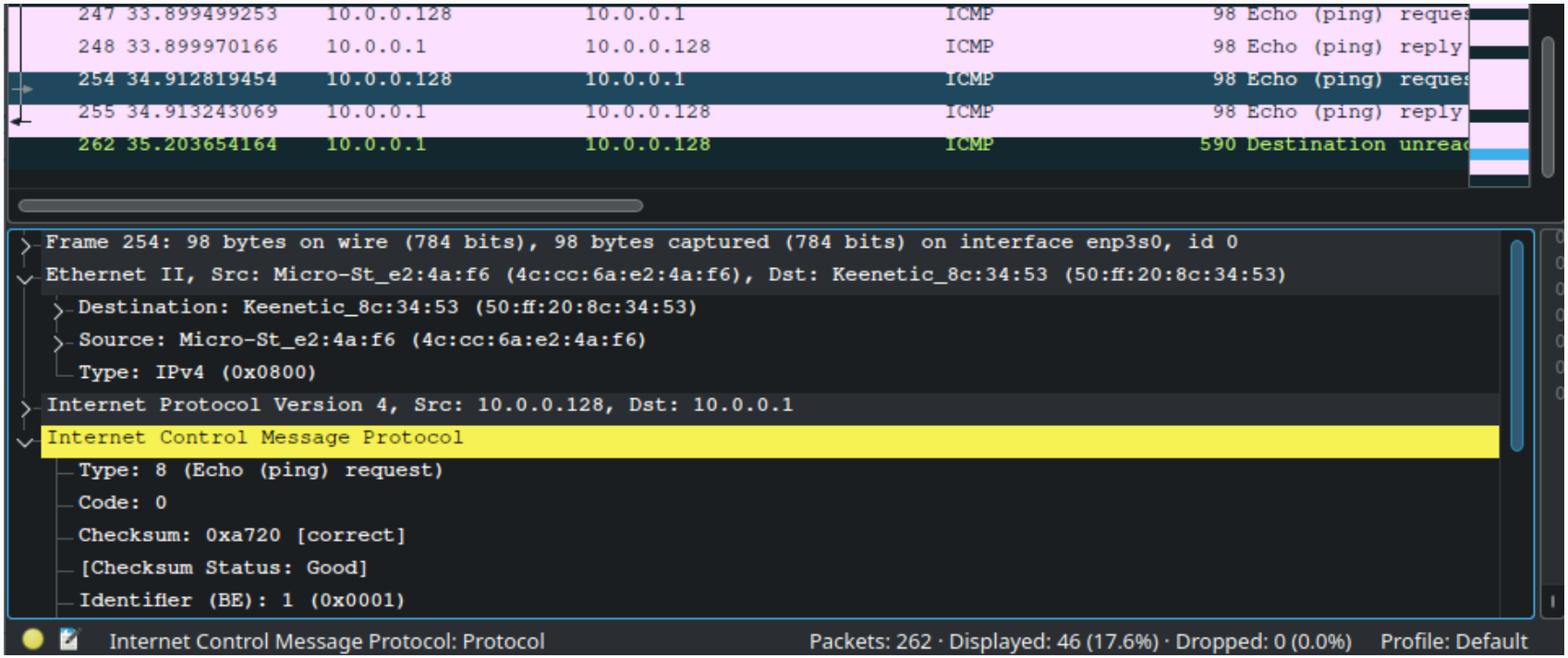

Рис. 6: icmp echo

ICMP Echo Reply

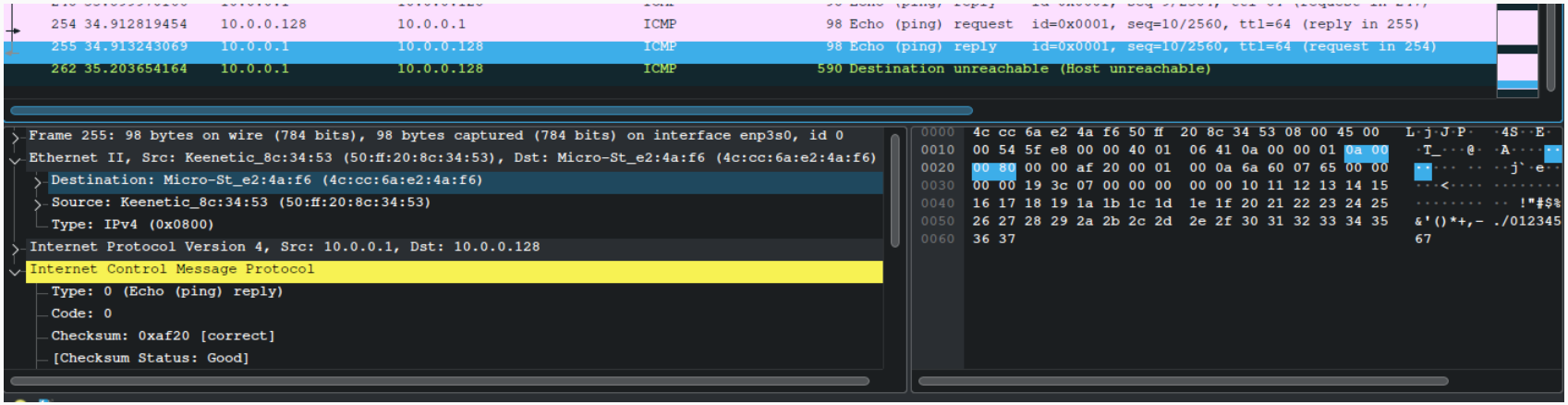

Рис. 7: icmp echo reply

ARP

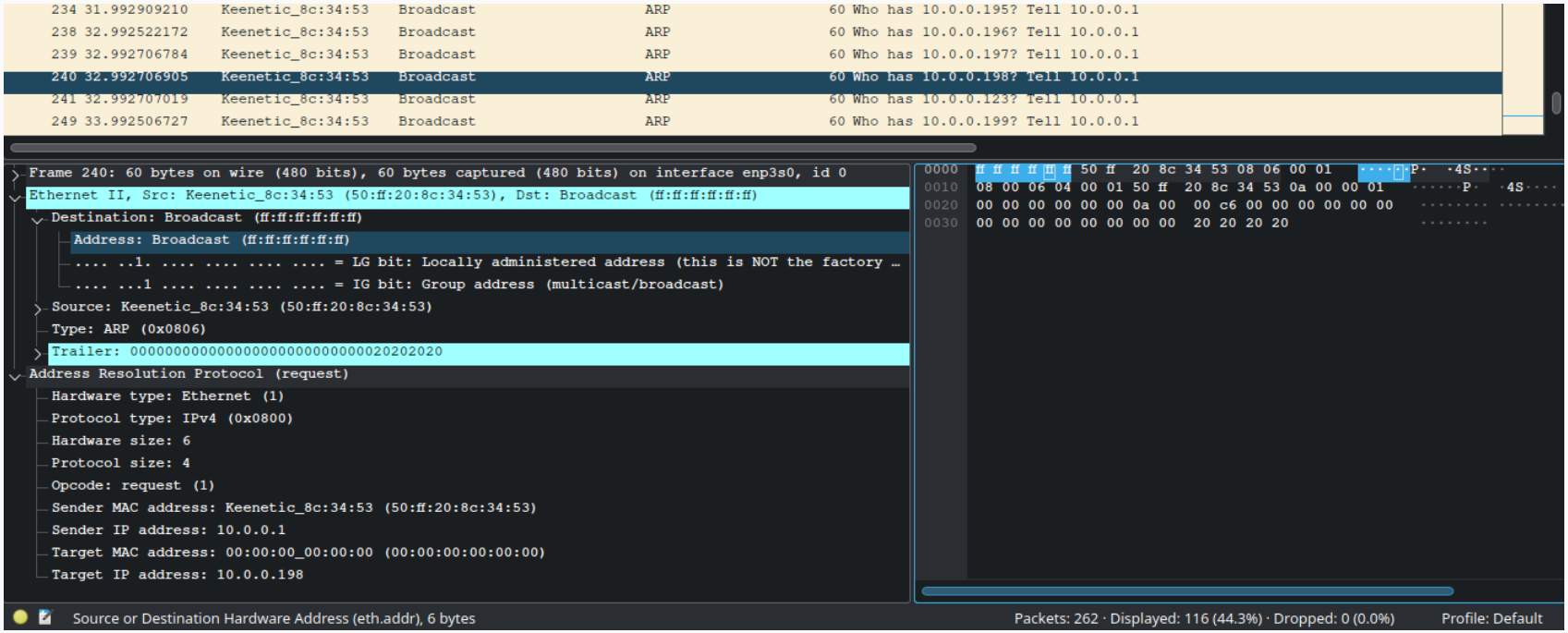
234 31.992909210 Keenetic_8c:34:53 Broadcast ARP 60 Who has 10.0.0.195? Tell 10.0.0.1
238 32.992522172 Keenetic_8c:34:53 Broadcast ARP 60 Who has 10.0.0.196? Tell 10.0.0.1
239 32.992706784 Keenetic_8c:34:53 Broadcast ARP 60 Who has 10.0.0.197? Tell 10.0.0.1
240 32.992706905 Keenetic_8c:34:53 Broadcast ARP 60 Who has 10.0.0.198? Tell 10.0.0.1
241 32.992707019 Keenetic_8c:34:53 Broadcast ARP 60 Who has 10.0.0.123? Tell 10.0.0.1
249 33.992506727 Keenetic_8c:34:53 Broadcast ARP 60 Who has 10.0.0.199? Tell 10.0.0.1
Frame 240: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp3s0, id 0
Ethernet II, Src: Keenetic_8c:34:53 (50:ff:20:8c:34:53), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Address: Broadcast (ff:ff:ff:ff:ff:ff)
.... ..1. .... = LG bit: Locally administered address (this is NOT the factory …
....1 .... = IG bit: Group address (multicast/broadcast)
Source: Keenetic_8c:34:53 (50:ff:20:8c:34:53)
Type: ARP (0x0806)
Trailer: 00000000000000000000000000020202020
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: Keenetic_8c:34:53 (50:ff:20:8c:34:53)
Sender IP address: 10.0.0.1
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 10.0.0.198
0000 ff ff ff ff ff ff 50 ff 20 8c 34 53 08 06 00 01
0010 08 00 06 04 00 01 50 ff 20 8c 34 53 0a 00 00 01
0020 00 00 00 00 00 00 0a 00 00 c6 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 20 20 20 20
Source or Destination Hardware Address (eth.addr), 6 bytes
Packets: 262 · Displayed: 116 (44.3%) · Dropped: 0 (0.0%)
Profile: Default

Рис. 8: arp

Ping rudn.ru

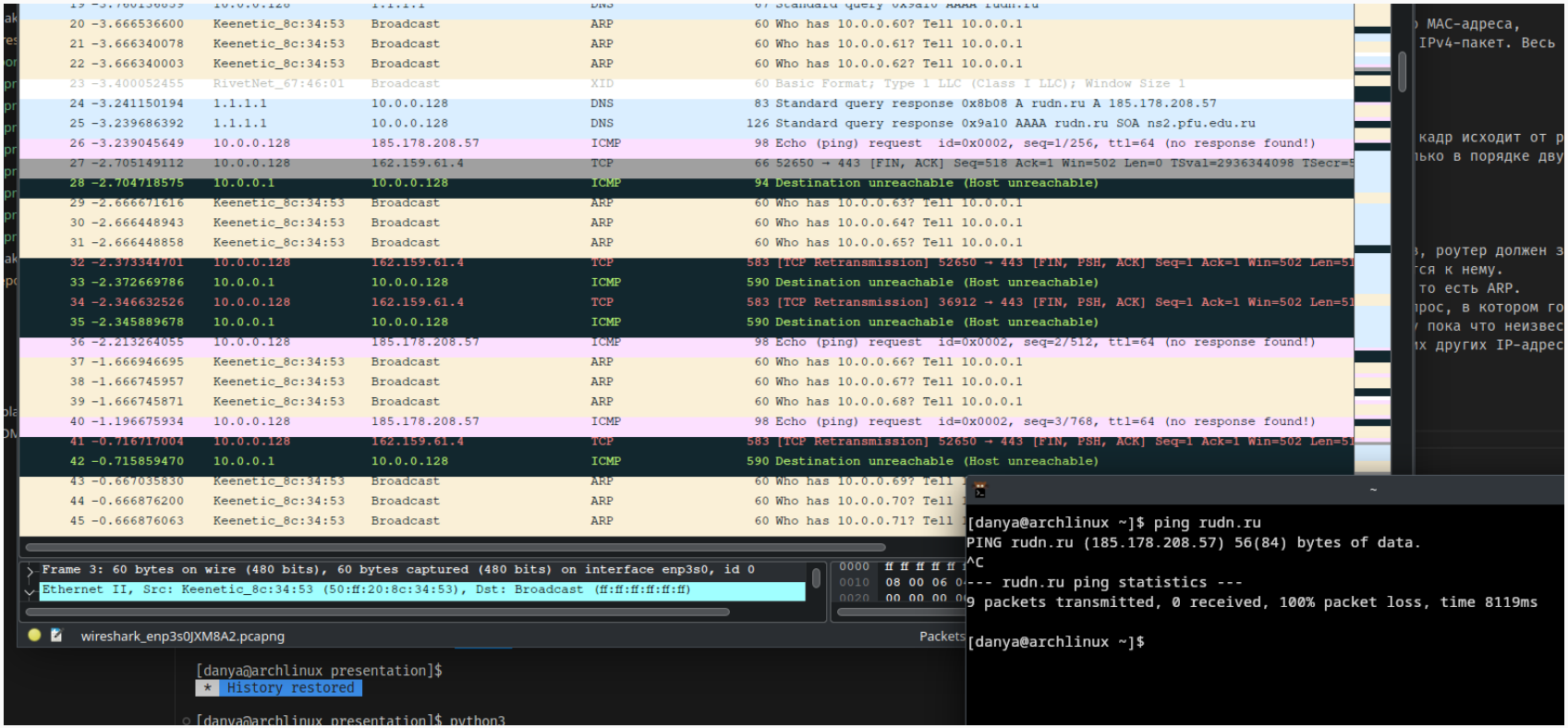

Рис. 9: rudn.ru

DNS-запрос

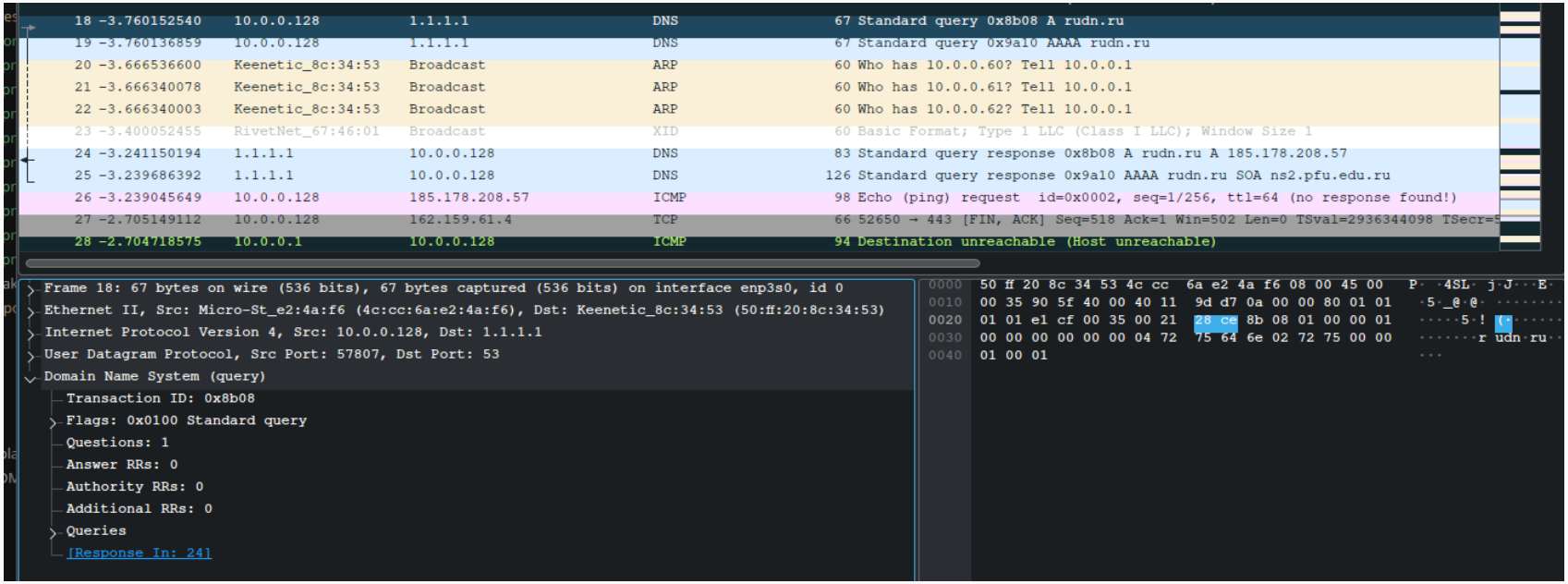

Рис. 10: dns query

DNS-ответ

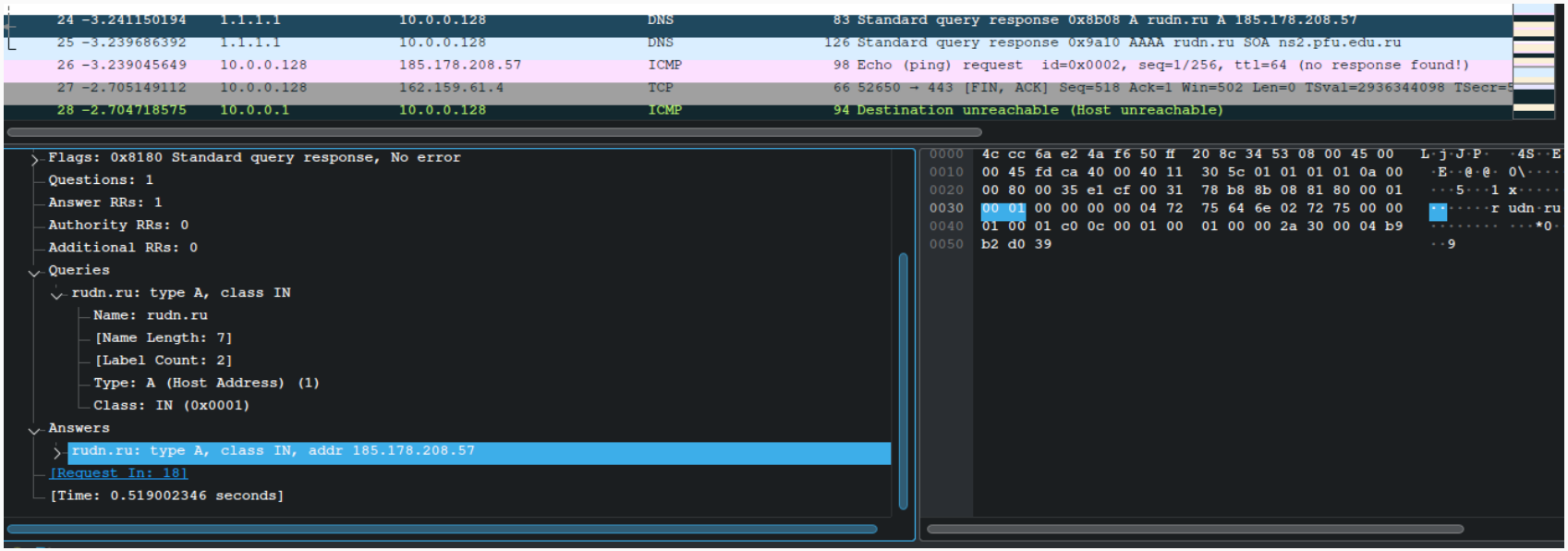

Рис. 11: dns response

Ping

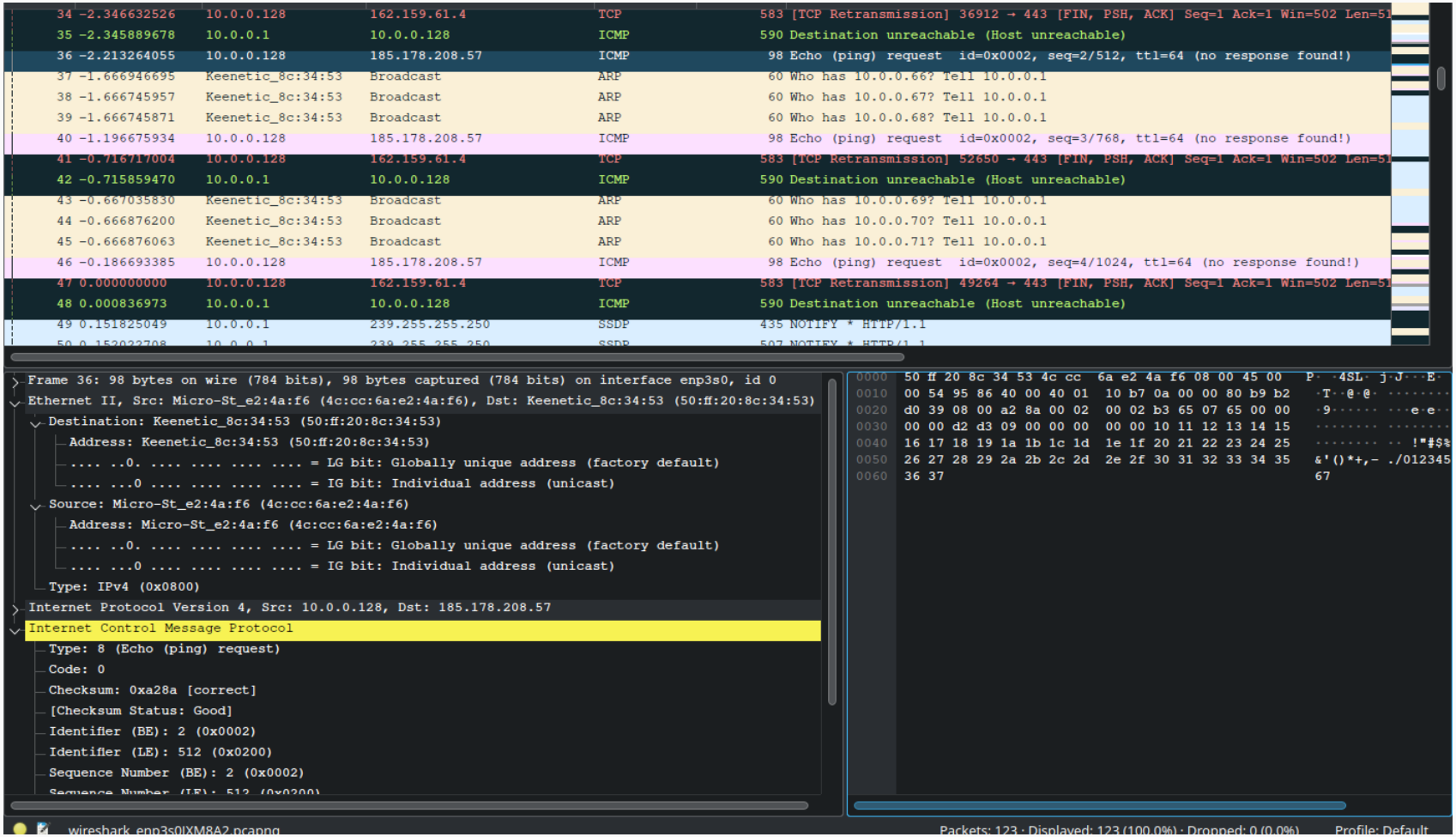

Рис. 12: ping

HTTP

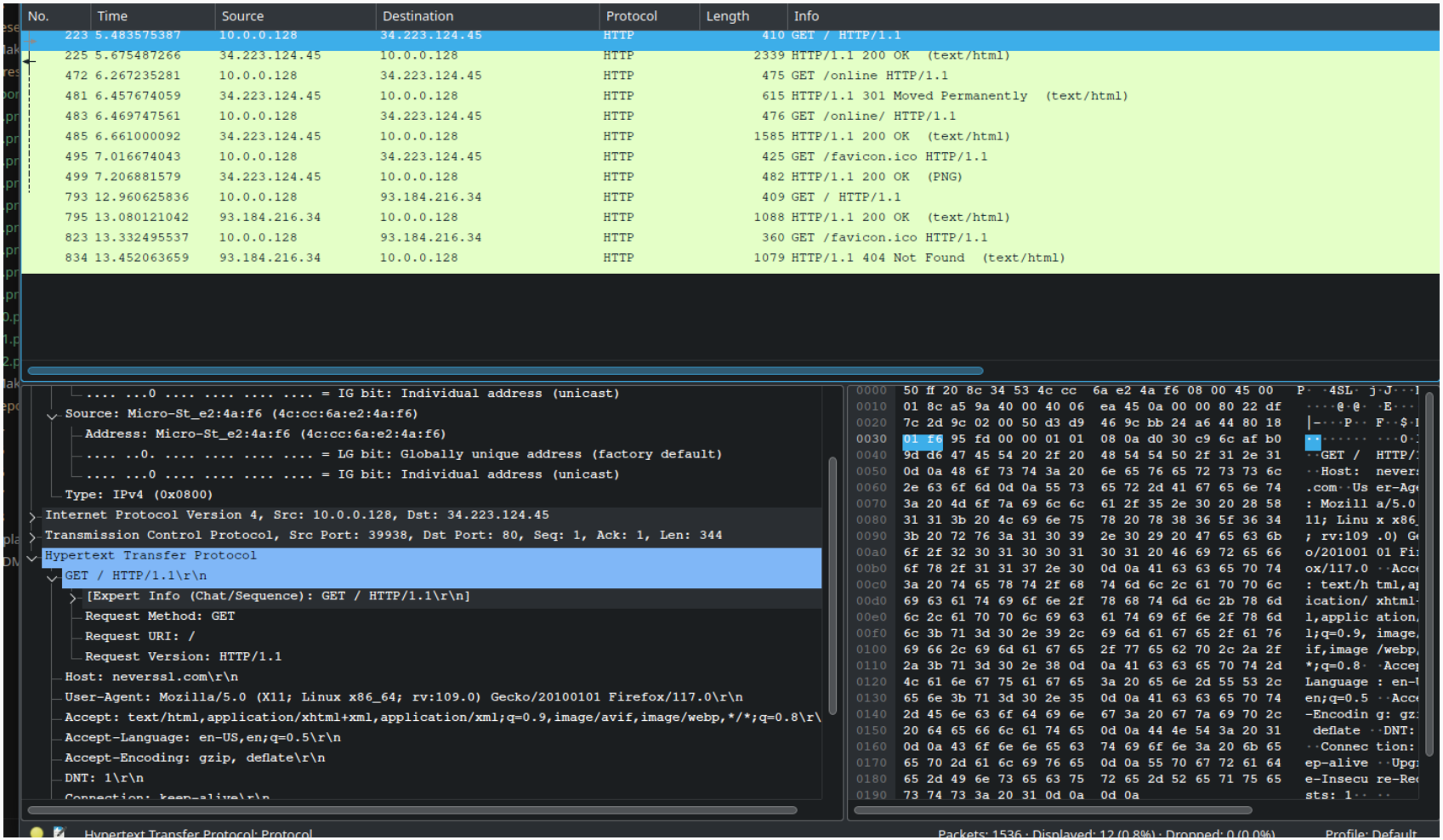

Рис. 13: http

TLS Client Hello

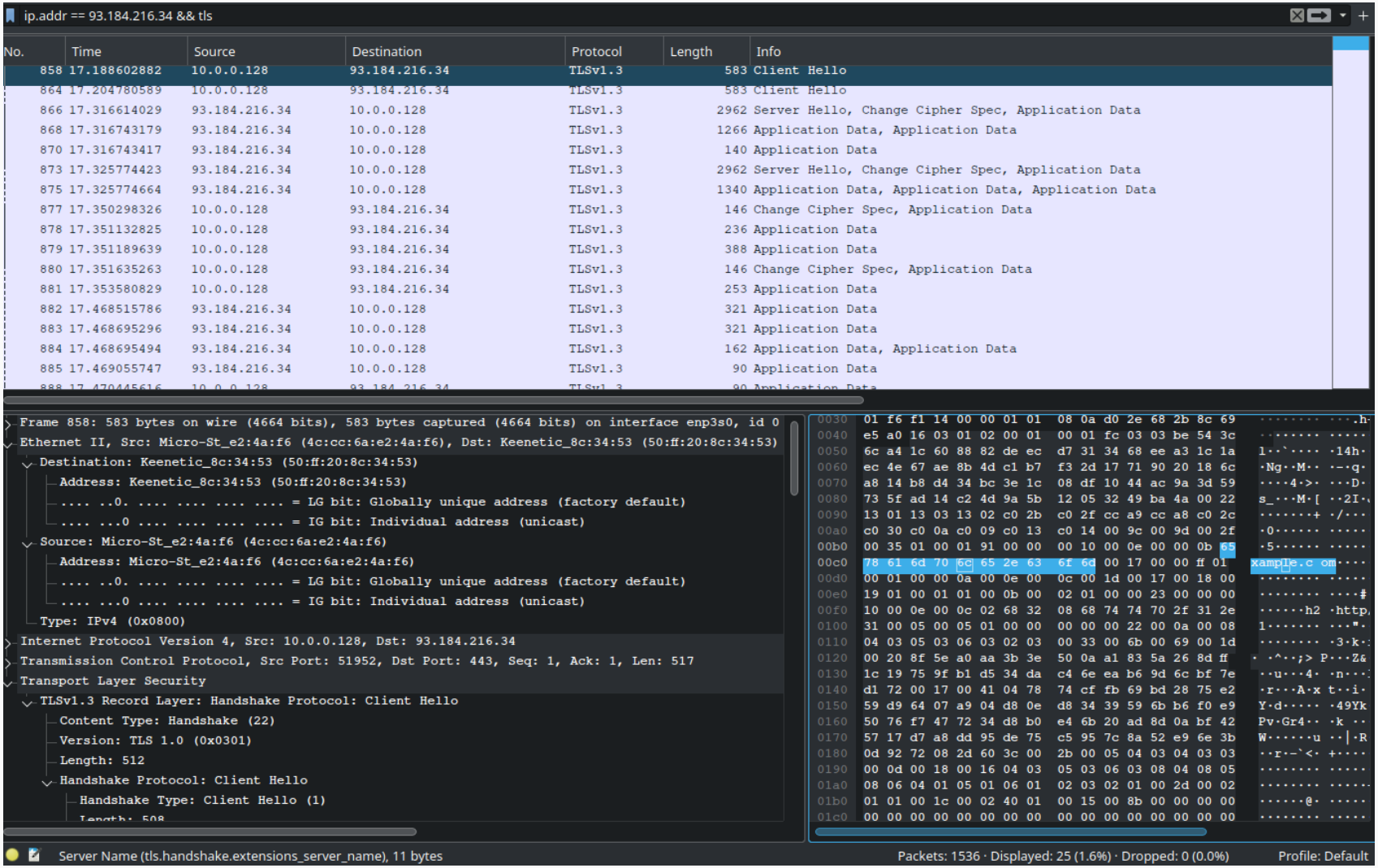

Рис. 14: tls client hello

TLS Server Hello

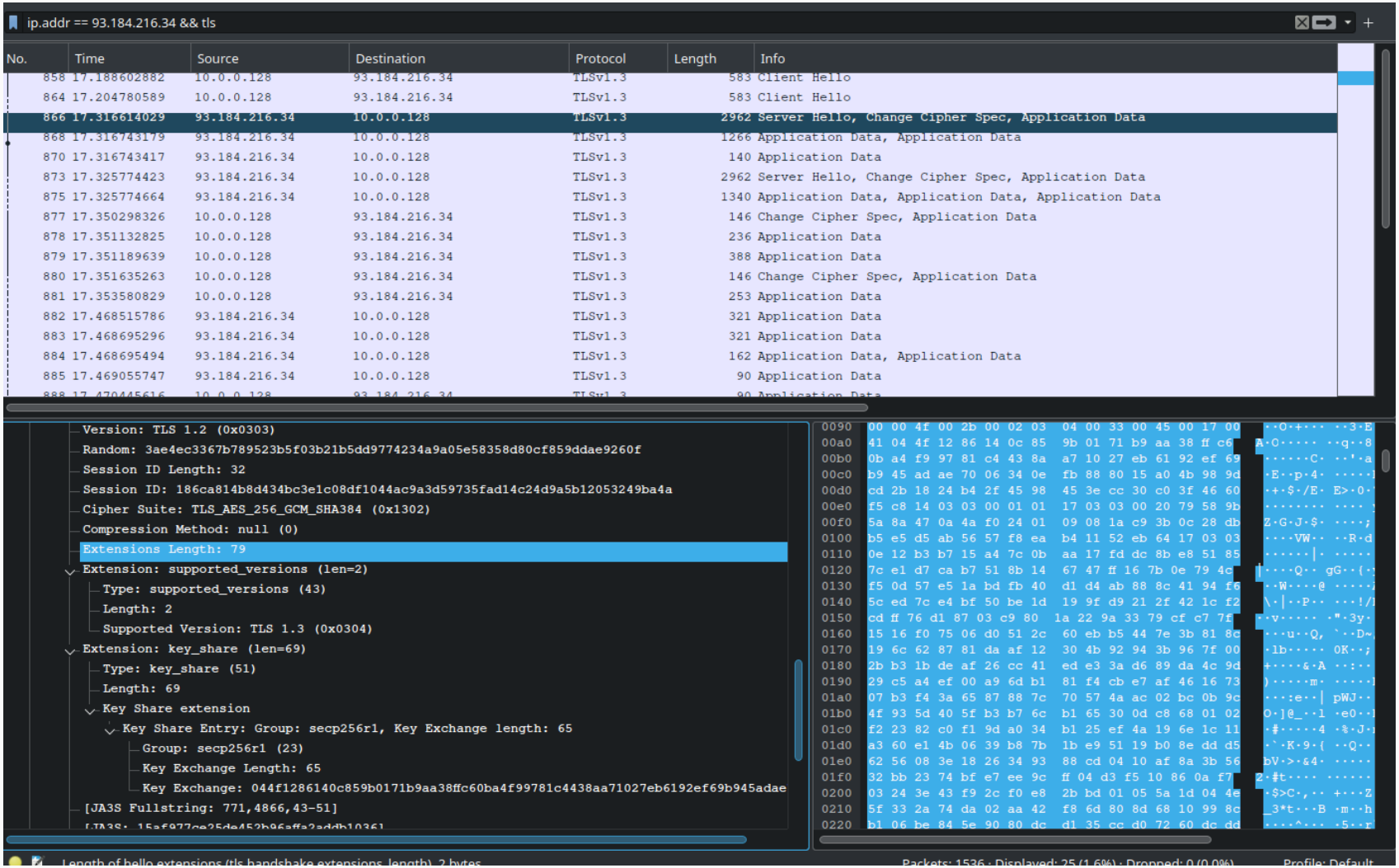

Рис. 15: tls server hello

QUIC

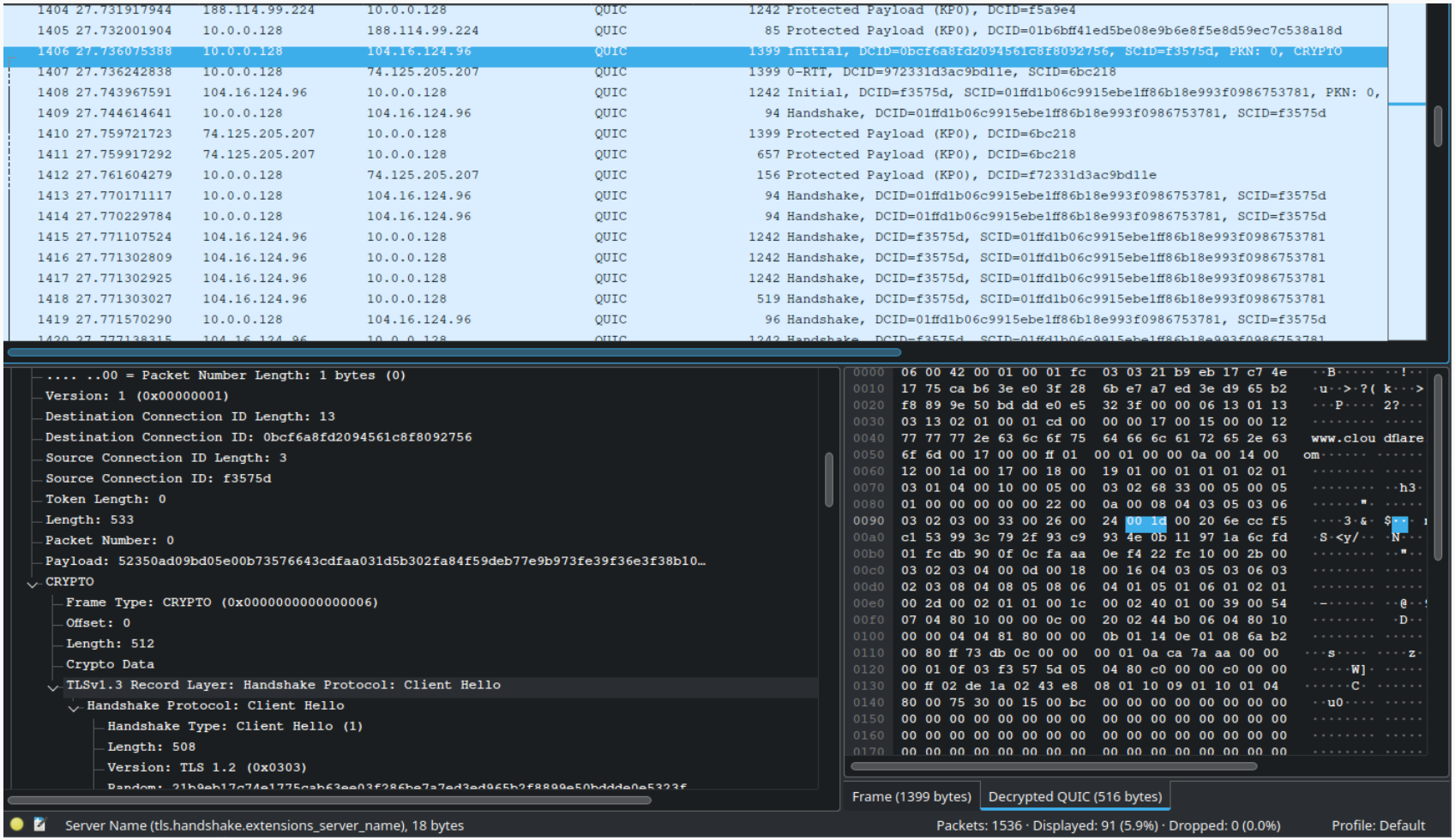

Рис. 16: quic

QUIC

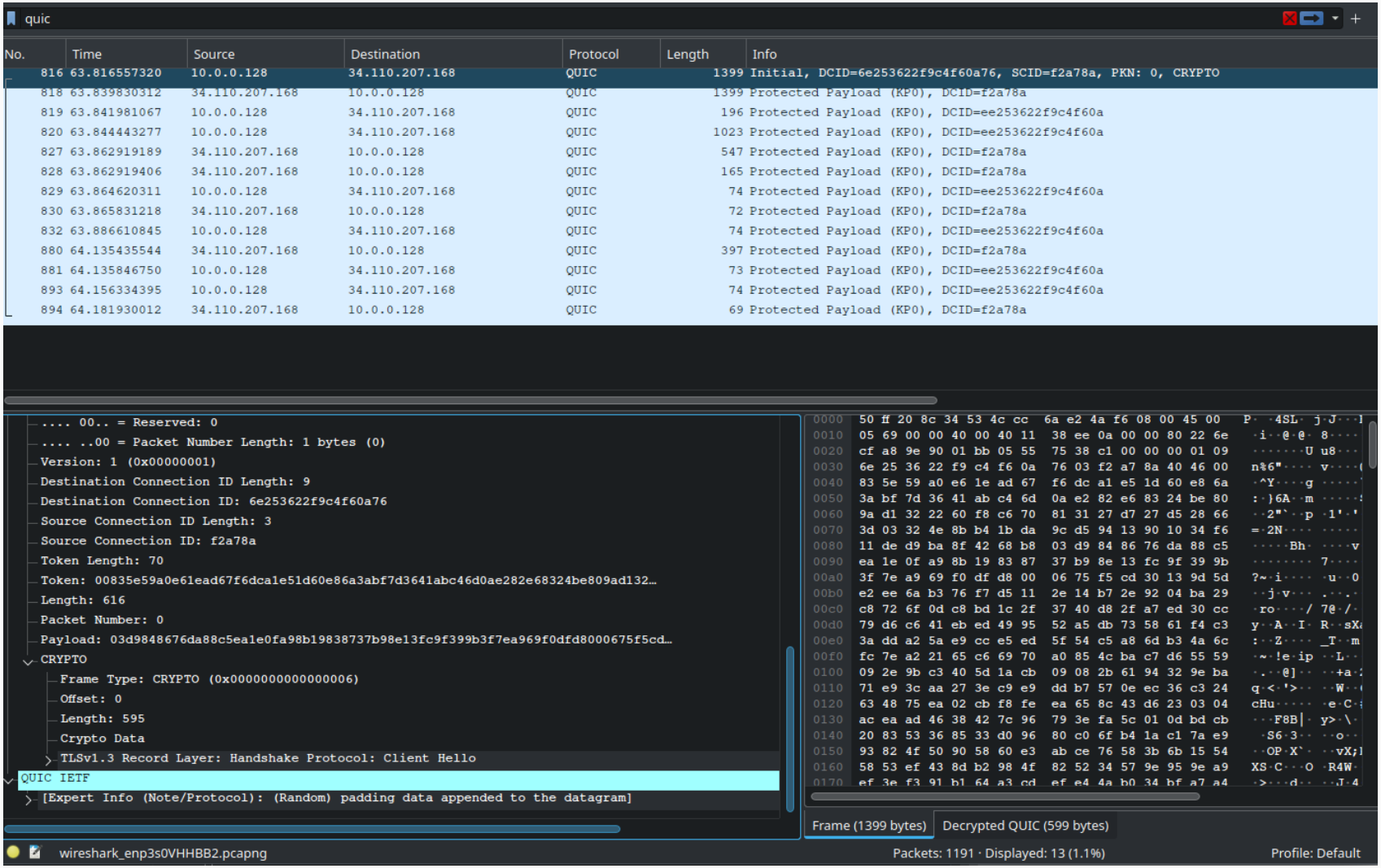

Рис. 17: quic

TCP

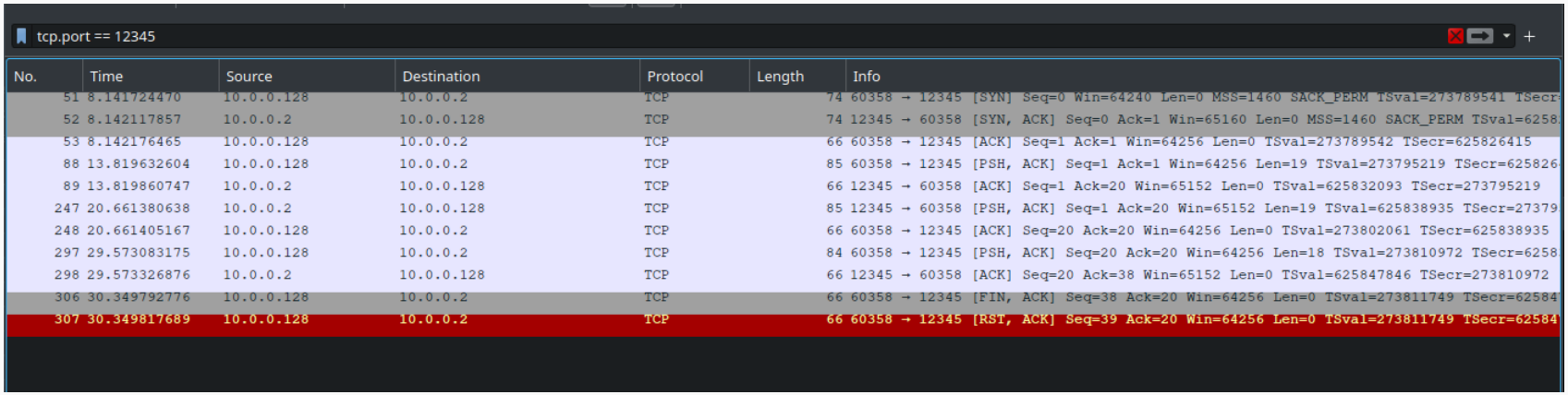

Рис. 18: tcp

TCP SYN

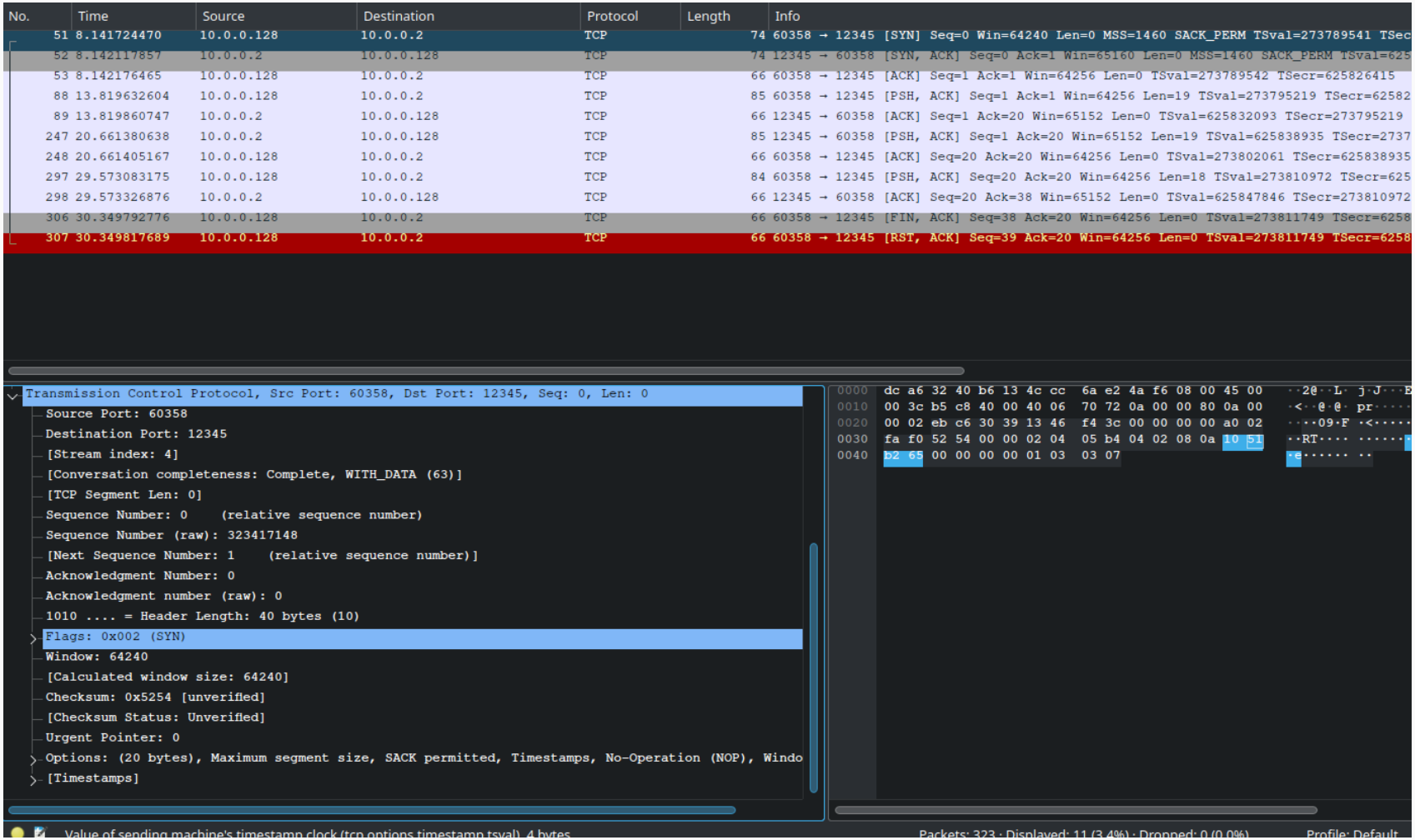

Рис. 19: tcp syn

TCP SYN ACK

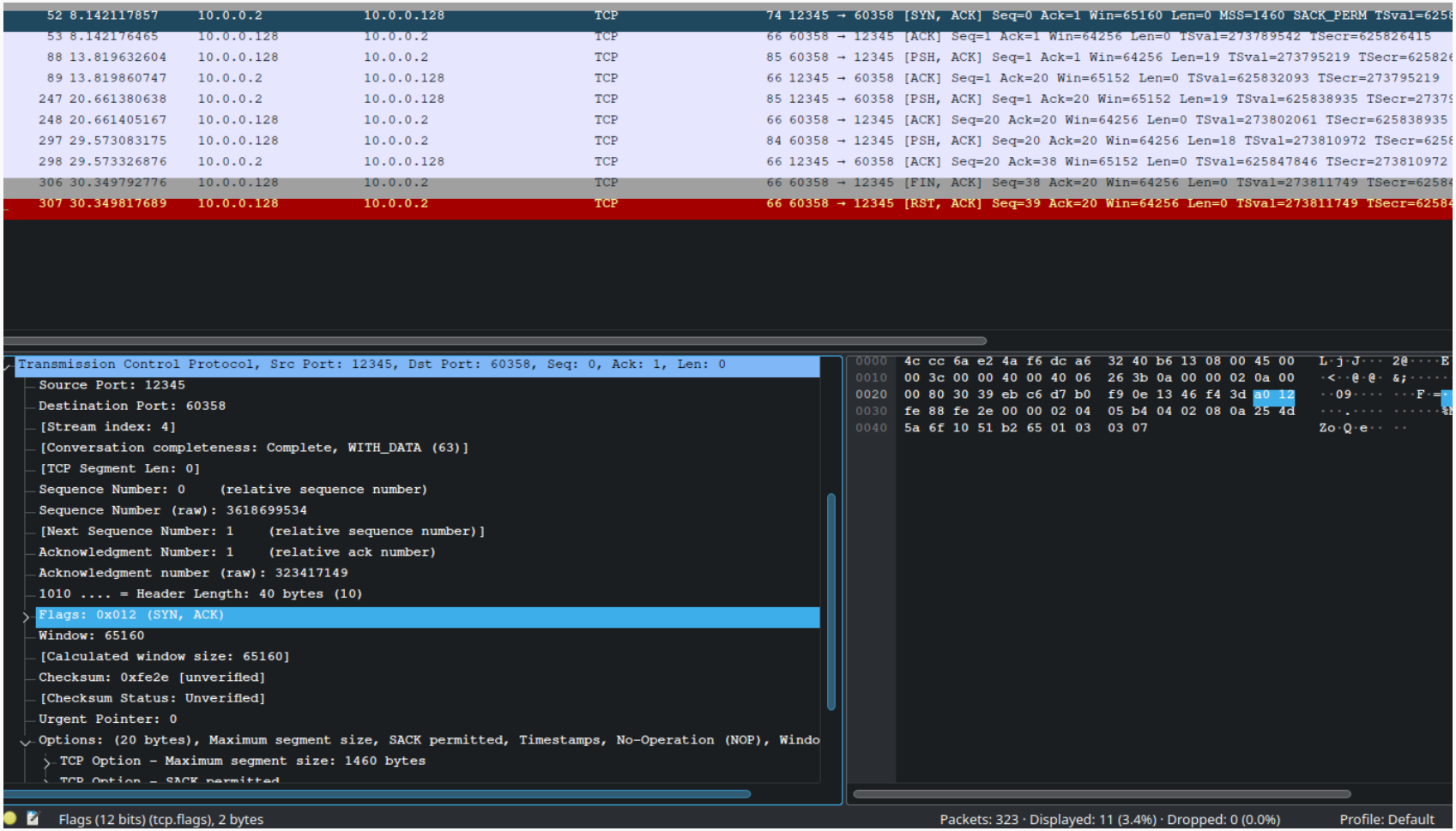

Рис. 20: tcp syn ack

TCP ACK

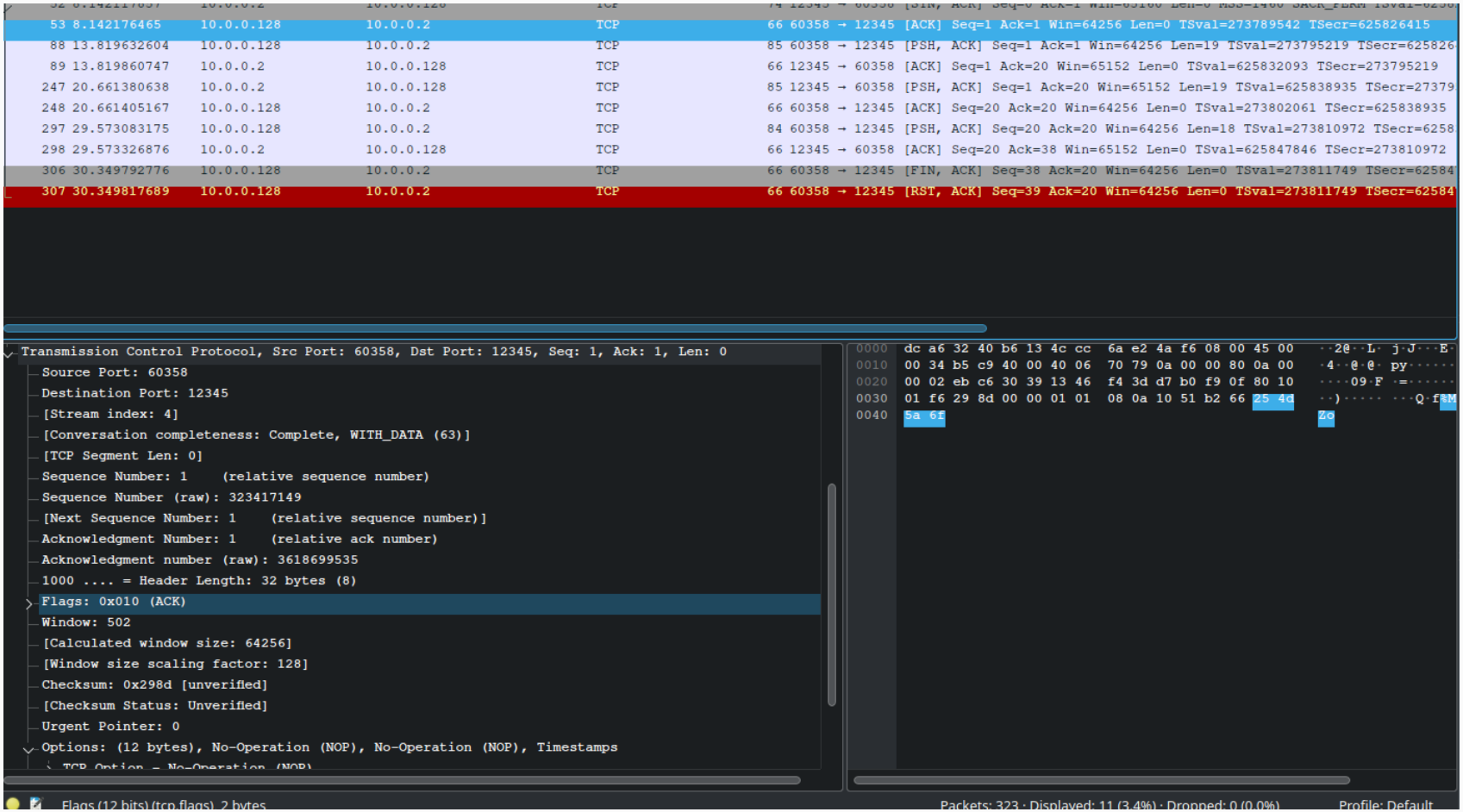

Рис. 21: tcp ack

TCP PSH ACK

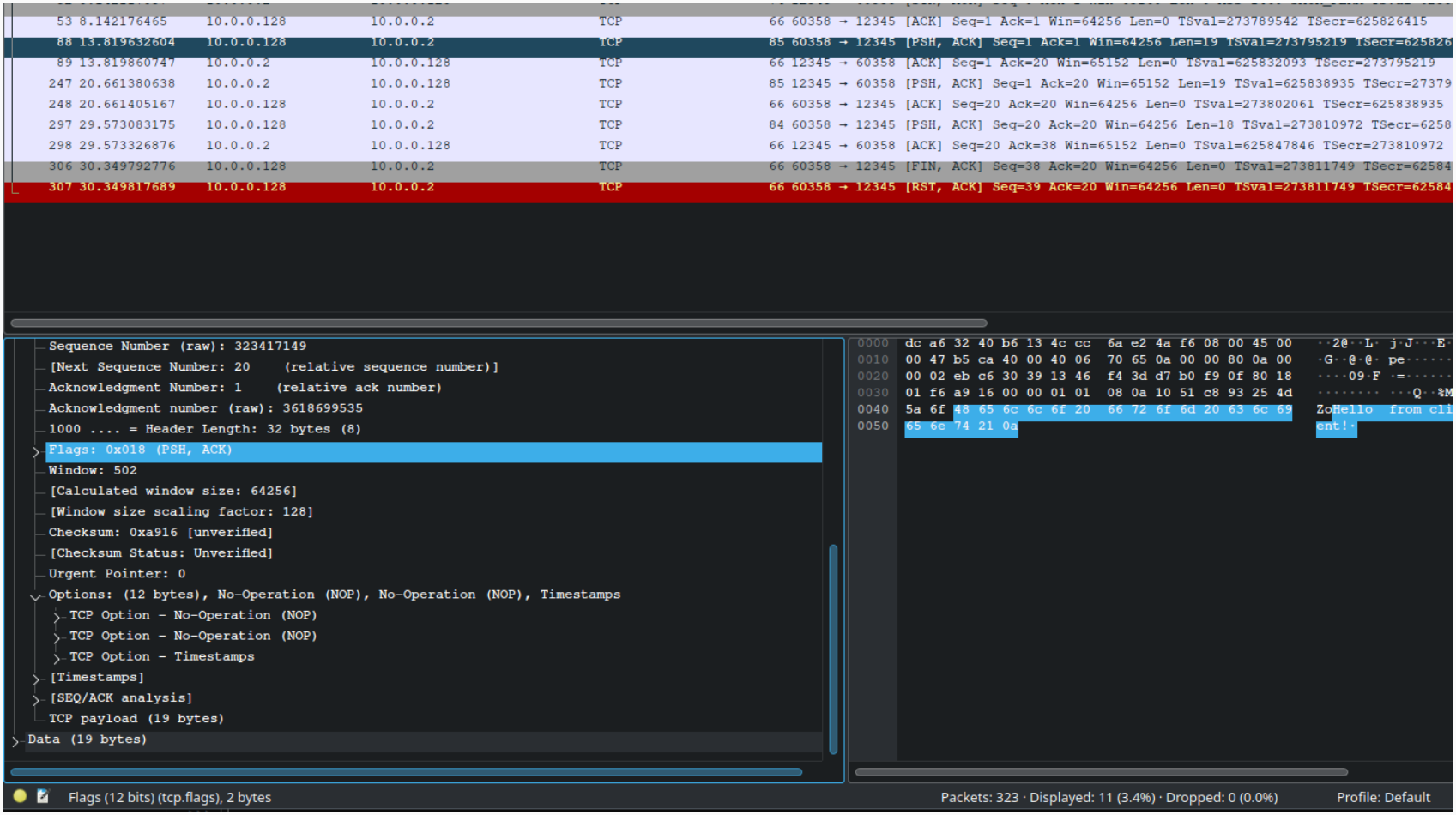

Рис. 22: tcp psh ack client

TCP PSH ACK

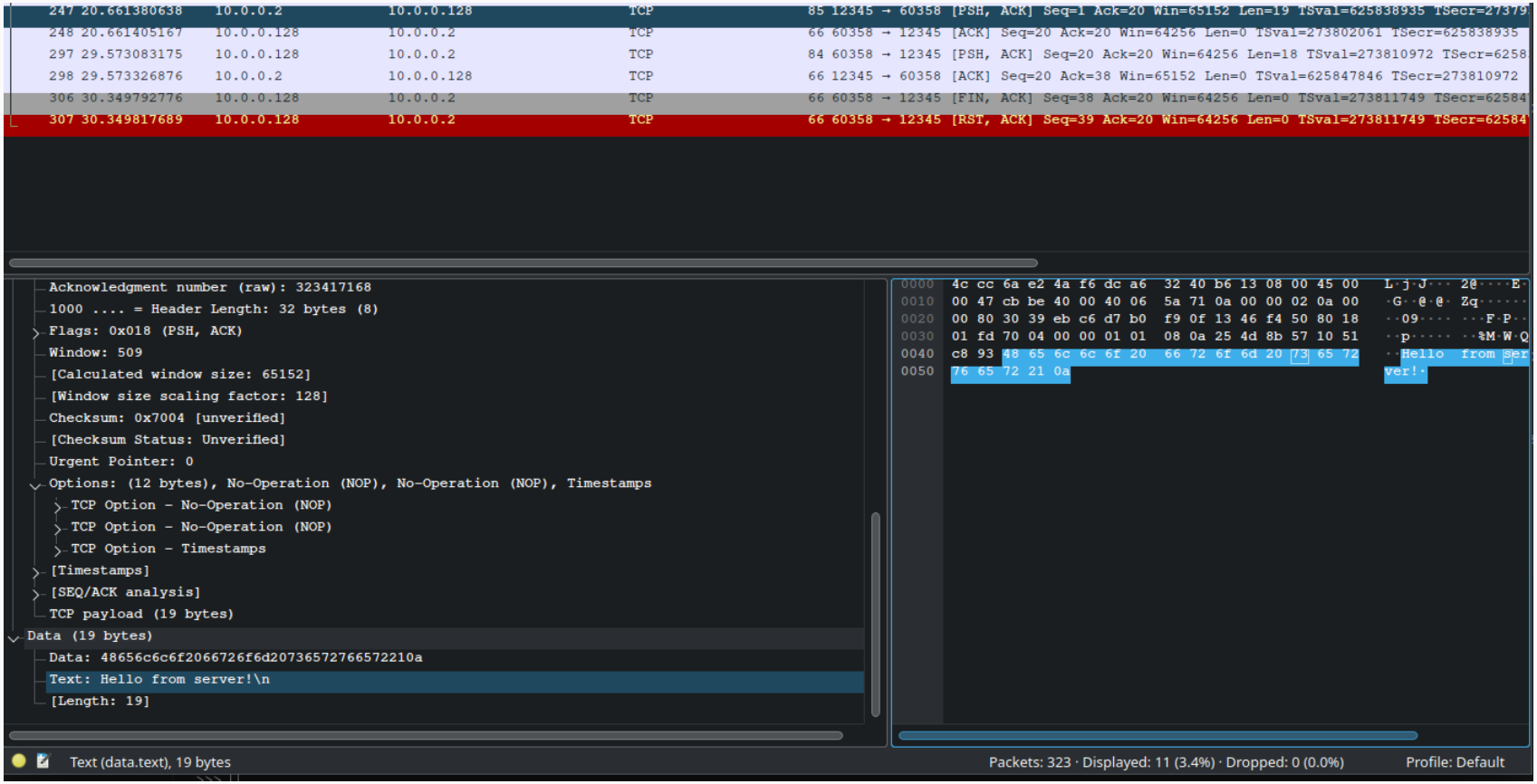

Рис. 23: tcp psh ack server

TCP FIN ACK

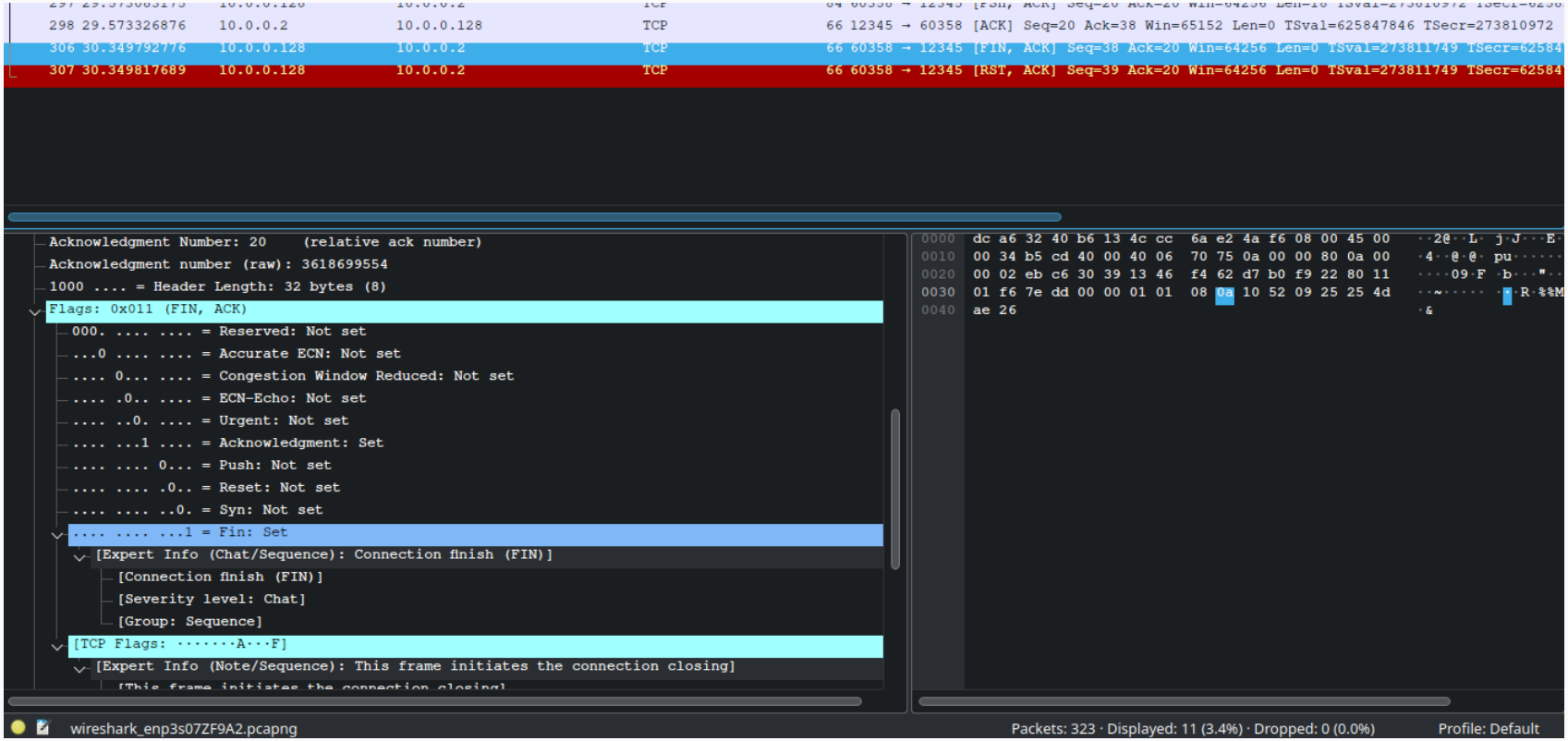

Рис. 24: tcp fin ack

Вывод

Я получил опыт работы с Wireshark для анализа пакетов в сети, а также с общими правилами работы различных сетевых протоколов.