

Лабораторная работа 3

Генералов Даниил, НПИбд-01-21, 1032202280

2023

¹RUDN University, Moscow, Russian Federation

Задача

Задача

3.3.1.1. Изучение возможностей команды *ipconfig* для ОС типа Windows (*ifconfig* для систем типа Linux). 3.3.1.2. 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

```
[danya@archlinux ~]$ ip -c address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 4c:cc:6a:e2:4a:f6 brd ff:ff:ff:ff:ff:ff
        inet 10.0.0.128/24 brd 10.0.0.255 scope global dynamic noprefixroute enp3s0
            valid_lft 24531sec preferred_lft 24531sec
        inet6 fe80::4317:cdb3:c507:238d/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 9c:b6:d0:67:46:01 brd ff:ff:ff:ff:ff:ff
        inet 10.0.192.19/24 brd 10.0.192.255 scope global dynamic noprefixroute wlp2s0
            valid_lft 24540sec preferred_lft 24540sec
        inet6 fe80::5aed:c2bc:55d:f664/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
4: outline-tun0: <NO-CARRIER,POINTOPOINT,MULTICAST,NOARP,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 500
    link/none
        inet 10.0.85.1/32 scope global outline-tun0
            valid_lft forever preferred_lft forever
[danya@archlinux ~]$
```

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

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

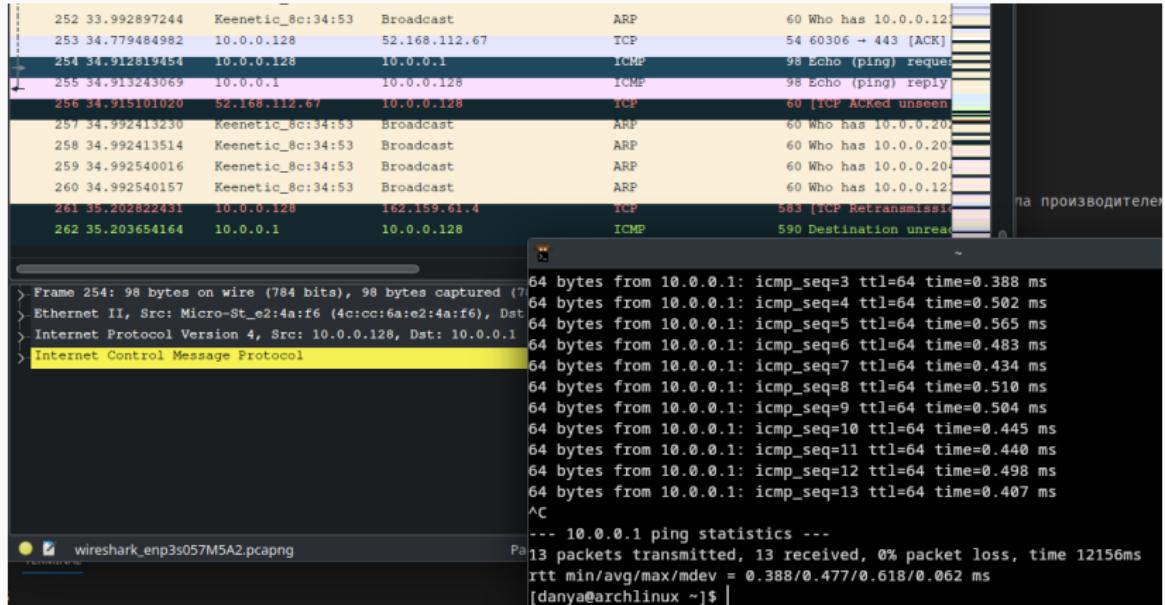


Рис. 5: wireshark

ICMP Echo

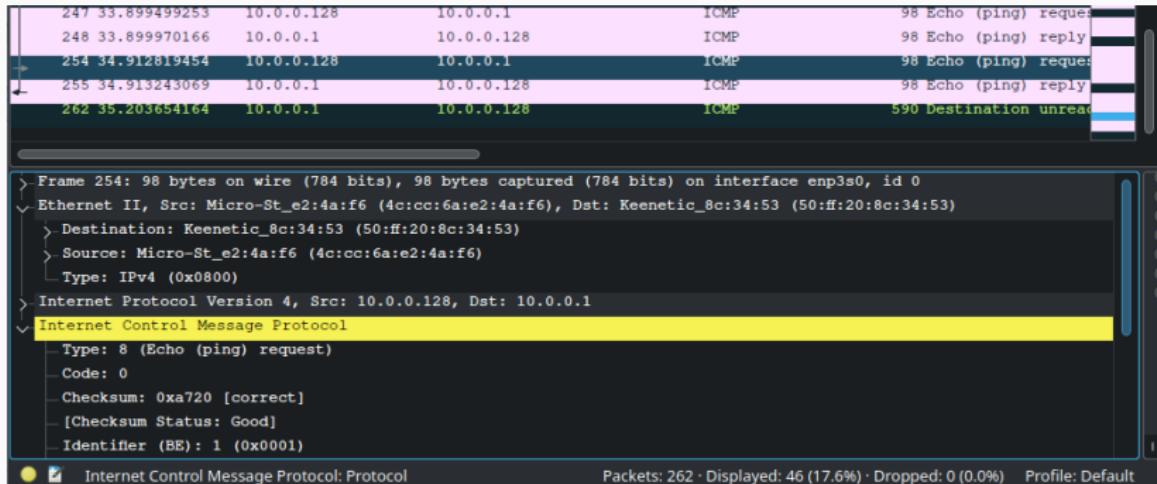


Рис. 6: icmp echo

ICMP Echo Reply

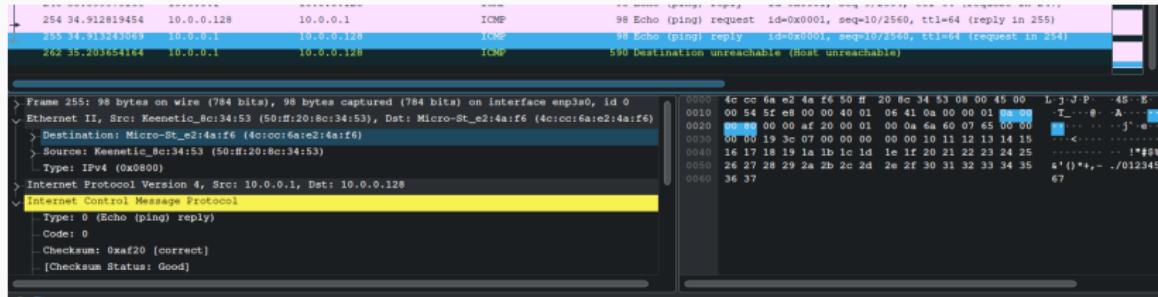


Рис. 7: icmp echo reply

ARP

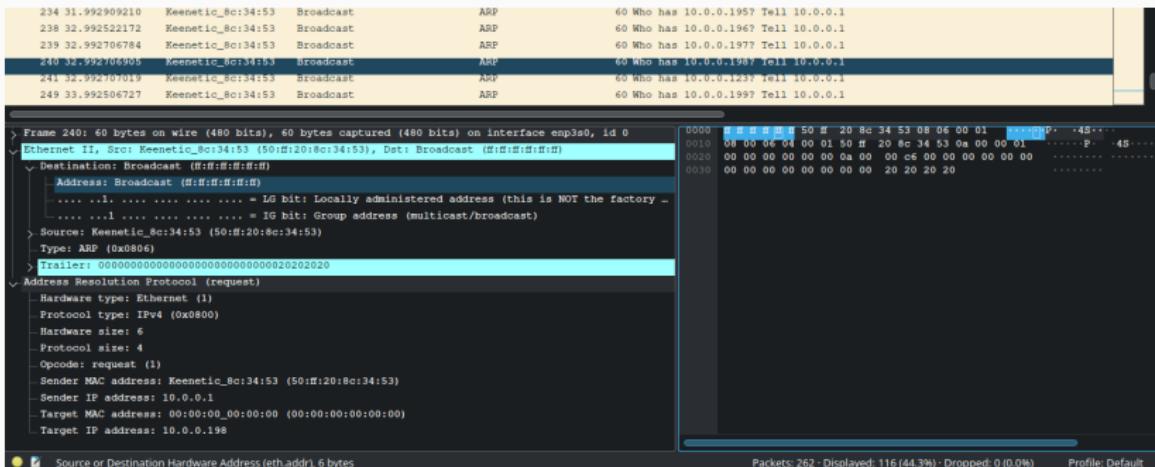


Рис. 8: arp

Ping rudn.ru

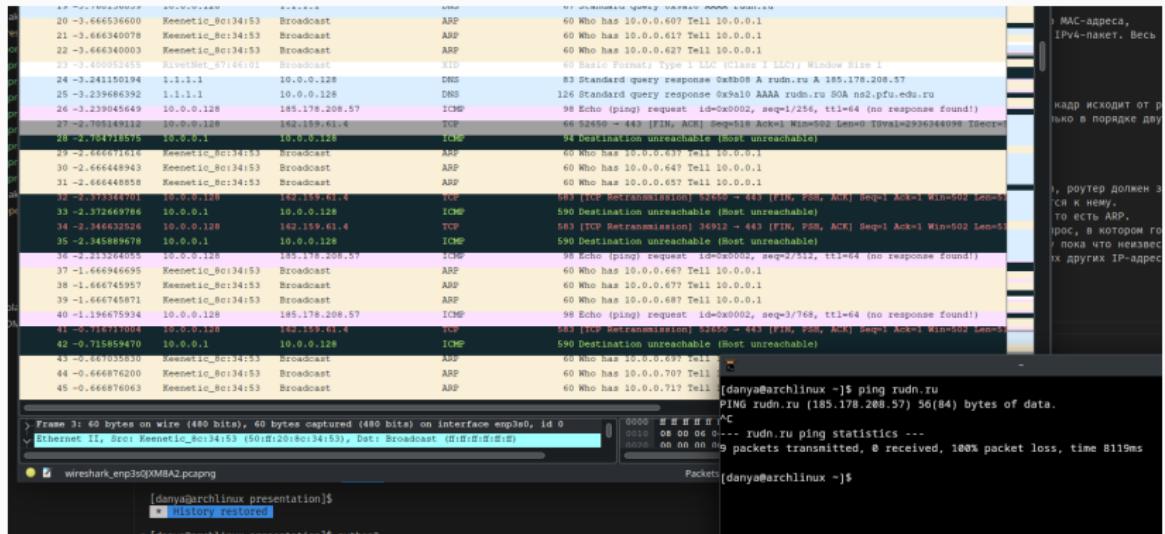


Рис. 9: rudn.ru

DNS-запрос

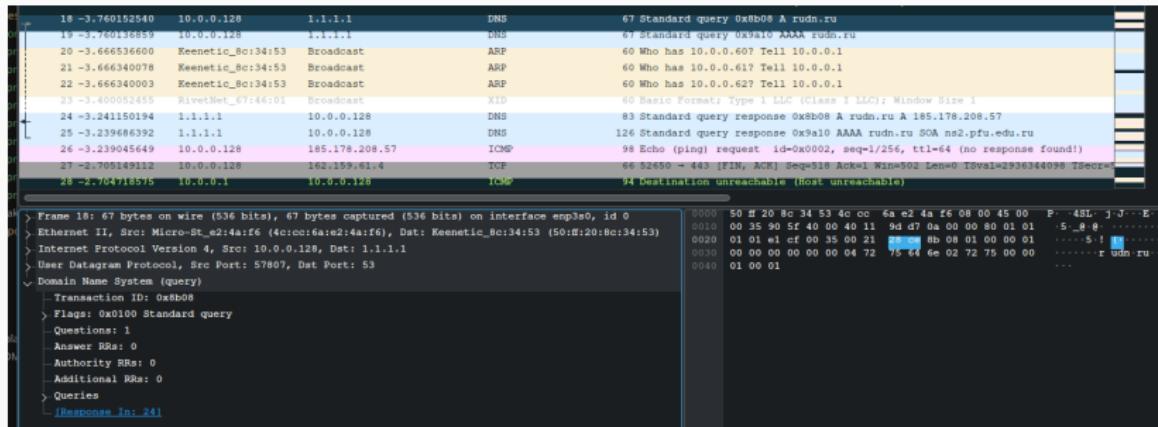


Рис. 10: dns query

DNS-ответ

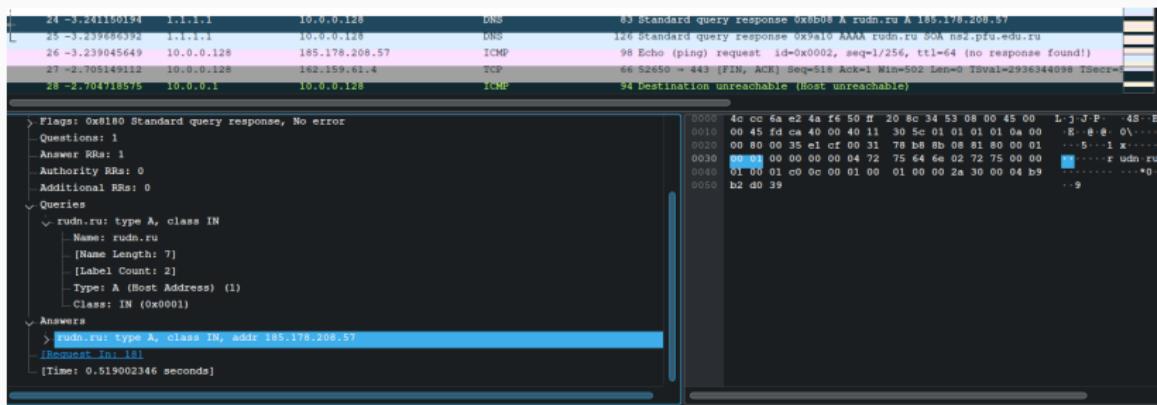


Рис. 11: dns response

Ping

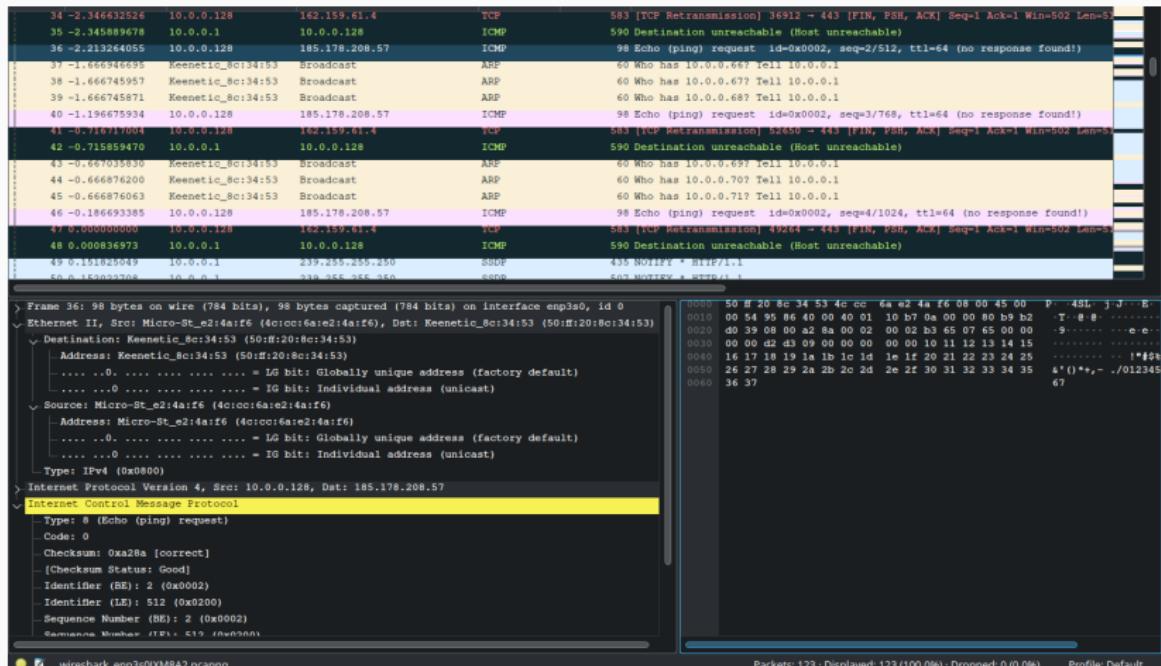


Рис. 12: ping

HTTP

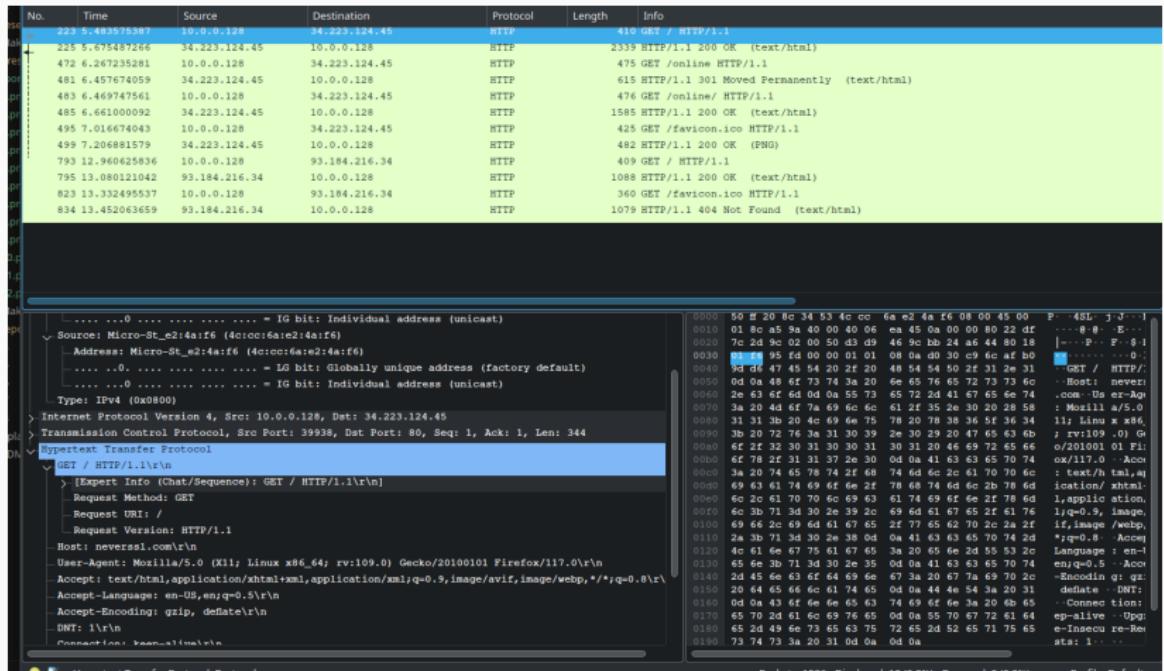


Рис. 13: http

TLS Client Hello

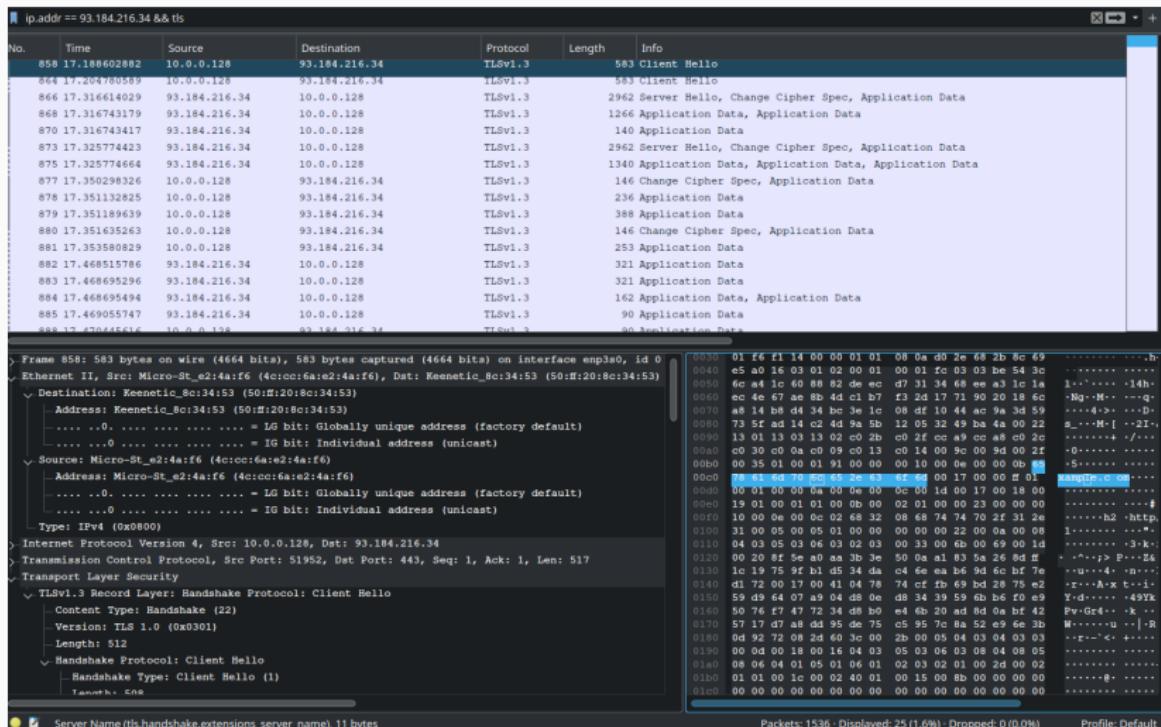


Рис. 14: tls client hello

TLS Server Hello

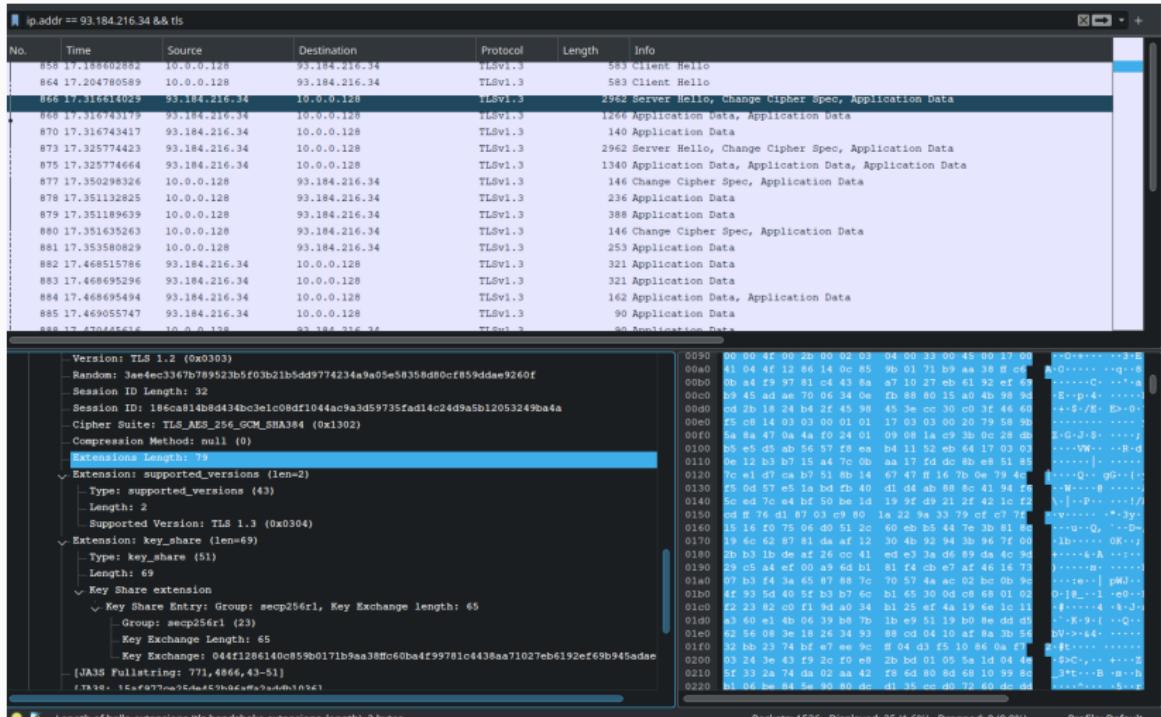


Рис. 15: tls server hello

QUIC

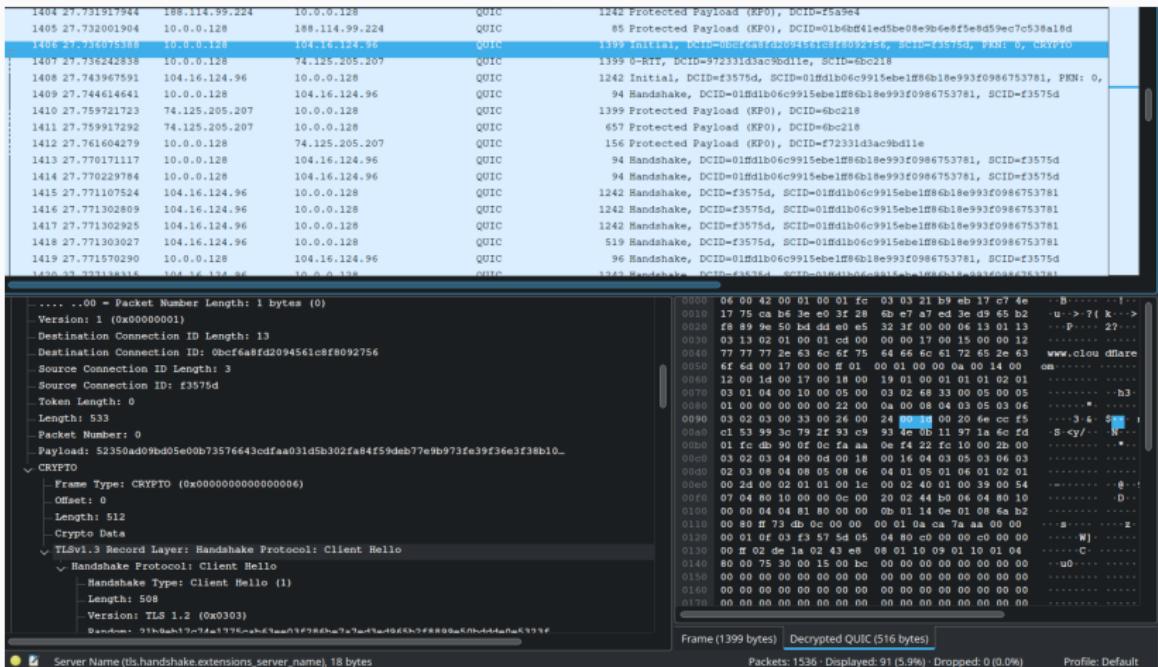


Рис. 16: quic

QUIC

Screenshot of Wireshark showing QUIC traffic. The packet list shows multiple QUIC frames, mostly protected payloads, with various connection IDs and lengths.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------|----------------|----------------|----------|---|---|
| 816 | 63.816557320 | 10.0.0.128 | 34.110.207.168 | QUIC | 1399 | Initial, DCID=6e253622f9c4f60a76, SCID=f2a78a, PKN: 0, CRYPTO |
| 818 | 63.839830312 | 34.110.207.168 | 10.0.0.128 | QUIC | 1399 Protected Payload (NFO), DCID=f2a78a | |
| 819 | 63.841980167 | 10.0.0.128 | 34.110.207.168 | QUIC | 196 Protected Payload (NFO), DCID=ee253622f9c4f60a | |
| 820 | 63.844443277 | 10.0.0.128 | 34.110.207.168 | QUIC | 1023 Protected Payload (NFO), DCID=ee253622f9c4f60a | |
| 827 | 63.862919189 | 34.110.207.168 | 10.0.0.128 | QUIC | 547 Protected Payload (NFO), DCID=f2a78a | |
| 828 | 63.862919406 | 34.110.207.168 | 10.0.0.128 | QUIC | 165 Protected Payload (NFO), DCID=f2a78a | |
| 829 | 63.8646620311 | 10.0.0.128 | 34.110.207.168 | QUIC | 74 Protected Payload (NFO), DCID=ee253622f9c4f60a | |
| 830 | 63.865831218 | 34.110.207.168 | 10.0.0.128 | QUIC | 72 Protected Payload (NFO), DCID=f2a78a | |
| 832 | 63.886610845 | 10.0.0.128 | 34.110.207.168 | QUIC | 74 Protected Payload (NFO), DCID=ee253622f9c4f60a | |
| 880 | 64.135435544 | 34.110.207.168 | 10.0.0.128 | QUIC | 397 Protected Payload (NFO), DCID=f2a78a | |
| 881 | 64.135846750 | 10.0.0.128 | 34.110.207.168 | QUIC | 73 Protected Payload (NFO), DCID=ee253622f9c4f60a | |
| 893 | 64.156334395 | 10.0.0.128 | 34.110.207.168 | QUIC | 74 Protected Payload (NFO), DCID=ee253622f9c4f60a | |
| 894 | 64.181930012 | 34.110.207.168 | 10.0.0.128 | QUIC | 69 Protected Payload (NFO), DCID=f2a78a | |

Selected packet details:

```

.... 00. = Reserved: 0
.... 00 - Packet Number Length: 1 bytes (0)
Version: 1 (0x0000000001)
Destination Connection ID Length: 9
Destination Connection ID: 6e253622f9c4f60a76
Source Connection ID Length: 3
Source Connection ID: f2a78a
Token Length: 70
Token: 00835e59a0e61ead67f6dcable5ld60e86a3abf7d3641abc46d0se282e68324be809ad132...
Length: 616
Packet Number: 0
Payload: 03d984676da#8c5eafe0fa98b19838737b98e13fc9f399bf7fea969f0dfd80006755cd...

```

Selected bytes view:

```

0000  50 ff 20 8c 34 b3 4c cc 6a e2 4a f6 08 00 45 00 P 45L j J ...
0010  05 69 00 00 40 00 40 11 38 ee 0a 00 00 80 22 6e 1 -@ 8 8
0020  c8 a8 9e 90 00 bb 05 55 75 38 c1 00 00 01 09 U u8
0030  6e 25 36 22 f9 c4 f6 0a 76 03 f2 7f 8a 40 46 00 nvc* v -i
0040  83 59 a9 00 e6 1e ad 67 f6 dc a1 e5 1d 60 e8 6a Y -g
0050  3a bf 7d 36 41 ab c4 6d 0a e2 82 e6 83 24 be 80 :1-6 m -i
0060  9d 32 22 60 f8 70 81 31 27 d7 27 d5 28 66 2** p 1
0070  3d 03 32 4e fb 6b 1b da 9c d5 94 13 90 10 34 f6 = 2N
0080  11 d9 b9 bf 42 68 b8 03 d9 84 86 76 da 88 c5 Bh v
0090  ea 1e 0f a9 19 83 87 37 b9 8e 13 fc 9f 39 9b ...
00a0  3f 7e a9 69 f0 df 00 06 75 f5 cd 30 13 9d 5d ?- i -u 0
00b0  e2 ee 6a b3 76 f7 df 11 2e 14 b7 2e 92 04 ba 29 -j v - .
00c0  c8 72 6f 0d c8 bd 1c 2c 37 40 d0 2f a7 ed 30 cc ro -/ 78 /
00d0  79 d5 c6 41 eb ed 49 95 52 a5 db 73 58 61 f4 c3 y -A -I R -x
00e0  3a dd a2 5a e9 cc e5 ed 5f 54 c5 a8 6d b3 4a 6c : - Z -T -
00f0  fc 7e a2 21 65 c6 69 70 a0 85 4c ba c7 d6 55 59 ~ -le ip L-
0100  09 2e 9b c9 40 5d 1a cb 09 08 2b 61 94 32 9e ba . - @ -i :a
0110  71 e9 3c aa 27 3e c9 e9 dd b7 57 0e ec 36 c3 24 q < > - M -i
0120  63 48 75 ea 02 cb fe ea 65 80 43 d3 23 03 04 cBu - - e C :
0130  ac ea ad 46 38 42 7c 96 79 3e fe 5c 01 0d bd cb FFB! y \ 
0140  20 83 53 36 38 33 d0 96 80 c6 6f 04 1a c1 7a e9 -86 3 - . 
0150  93 82 4f 64 60 58 60 e3 a0 ce 76 58 3b 15 54 0P X' -vXj
0160  58 53 49 4d 9d 98 4f 92 52 3d 57 9e 09 a9 XS C - O R/W
0170  hf 5f 3c 91 h1 d4 a3 hf hf 4a hf 34 hf 37 A4 >- d -J 4
```

Selected bytes view details:

```

Frame (1399 bytes) Decrypted QUIC (599 bytes)
Packets: 1191 - Displayed: 13 (1.1%)
Profile: Default

```

Рис. 17: quic

TCP

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------|------------|-------------|----------|--------|--|
| 51 | 8.1421724470 | 10.0.0.128 | 10.0.0.2 | TCP | 74 | 60358 → 12345 [SYN] Seq=0 Win=64256 Len=0 MSS=1460 SACK_PERM TSval=273789541 TSeср=62582 |
| 52 | 8.1421178657 | 10.0.0.2 | 10.0.0.128 | TCP | 74 | 12345 → 60358 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=62586 |
| 53 | 8.142176465 | 10.0.0.128 | 10.0.0.2 | TCP | 66 | 60358 → 12345 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=273789542 TSeср=625826415 |
| 88 | 13.819632604 | 10.0.0.128 | 10.0.0.2 | TCP | 85 | 60358 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=19 TSval=273795219 TSeср=625826 |
| 89 | 13.819860747 | 10.0.0.2 | 10.0.0.128 | TCP | 66 | 12345 → 60358 [ACK] Seq=1 Ack=20 Win=65152 Len=0 TSval=625832093 TSeср=273795219 |
| 247 | 20.661380638 | 10.0.0.2 | 10.0.0.128 | TCP | 85 | 12345 → 60358 [PSH, ACK] Seq=1 Ack=20 Win=65152 Len=19 TSval=625838933 TSeср=27379 |
| 248 | 20.661405167 | 10.0.0.128 | 10.0.0.2 | TCP | 66 | 60358 → 12345 [ACK] Seq=20 Ack=20 Win=64256 Len=0 TSval=273802061 TSeср=625838935 |
| 297 | 29.5730853175 | 10.0.0.128 | 10.0.0.2 | TCP | 84 | 60358 → 12345 [PSH, ACK] Seq=20 Ack=20 Win=64256 Len=18 TSval=273810972 TSeср=6258 |
| 298 | 29.573326876 | 10.0.0.2 | 10.0.0.128 | TCP | 66 | 12345 → 60358 [ACK] Seq=20 Ack=3 Win=65152 Len=0 TSval=625847844 TSeср=273810972 |
| 306 | 30.349792776 | 10.0.0.128 | 10.0.0.2 | TCP | 66 | 60358 → 12345 [FIN, ACK] Seq=38 Ack=20 Win=64256 Len=0 TSval=273811749 TSeср=62584 |
| 307 | 30.349817689 | 10.0.0.128 | 10.0.0.2 | TCP | 66 | 60358 → 12345 [RST, ACK] Seq=39 Ack=20 Win=64256 Len=0 TSval=273811749 TSeср=62584 |

Рис. 18: tcp

TCP SYN

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|------------|-------------|----------|--------|---|
| 51 | 8.141724470 | 10.0.0.128 | 10.0.0.2 | TCP | 74 | 60358 → 12345 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TStamp=273789541 TSecr=625626415 |
| 52 | 8.141117857 | 10.0.0.128 | 10.0.0.2 | TCP | 74 | 12345 → 60358 [SYN, Ack] Seq=1 Win=5360 Len=0 MSS=1460 SACK_PERM TStamp=273789542 TSecr=625626415 |
| 53 | 8.142176465 | 10.0.0.128 | 10.0.0.2 | TCP | 66 | 60358 → 12345 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TStamp=273789542 TSecr=625626415 |
| 88 | 13.619632604 | 10.0.0.128 | 10.0.0.2 | TCP | 85 | 60358 → 12345 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=19 TStamp=2737895219 TSecr=625626415 |
| 89 | 13.819860747 | 10.0.0.2 | 10.0.0.128 | TCP | 66 | 12345 → 60358 [ACK] Seq=1 Ack=20 Win=65152 Len=0 TStamp=625832093 TSecr=273795219 |
| 247 | 20.661380638 | 10.0.0.2 | 10.0.0.128 | TCP | 85 | 12345 → 60358 [PSH, ACK] Seq=1 Ack=20 Win=65152 Len=19 TStamp=625838935 TSecr=2737 |
| 248 | 20.661405167 | 10.0.0.128 | 10.0.0.2 | TCP | 66 | 60358 → 12345 [ACK] Seq=20 Ack=20 Win=64256 Len=0 TStamp=273802061 TSecr=625838935 |
| 297 | 29.573083175 | 10.0.0.128 | 10.0.0.2 | TCP | 84 | 60358 → 12345 [PSH, ACK] Seq=20 Ack=20 Win=64256 Len=18 TStamp=273810972 TSecr=625 |
| 298 | 29.573326876 | 10.0.0.2 | 10.0.0.128 | TCP | 66 | 12345 → 60358 [ACK] Seq=20 Ack=38 Win=65152 Len=0 TStamp=625847846 TSecr=273810972 |
| 306 | 30.349792776 | 10.0.0.128 | 10.0.0.2 | TCP | 66 | 60358 → 12345 [FIN, ACK] Seq=38 Ack=20 Win=64256 Len=0 TStamp=273811749 TSecr=6258 |
| 307 | 30.349817689 | 10.0.0.128 | 10.0.0.2 | TCP | 66 | 60358 → 12345 [RST, ACK] Seq=39 Ack=20 Win=64256 Len=0 TStamp=273811749 TSecr=6258 |

Transmission Control Protocol, Src Port: 60358, Dst Port: 12345, Seq: 0, Len: 0

```
Source Port: 60358
Destination Port: 12345
[Stream index: 4]
(Conversation completeness: Complete, WITH_DATA (63))
[TCP Segment Len: 0]
Sequence Number: 0      (relative sequence number)
Sequence Number (raw): 323417148
(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: 0x254 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
> Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window [Timestamp]
```

Value of sending machine's timestamp clock (tcp options timestamp) 4 bytes

Packets: 323 • Displayed: 11 (3.4%) • Dropped: 0 (0.0%) • Profile: Default

Рис. 19: tcp syn

TCP SYN ACK

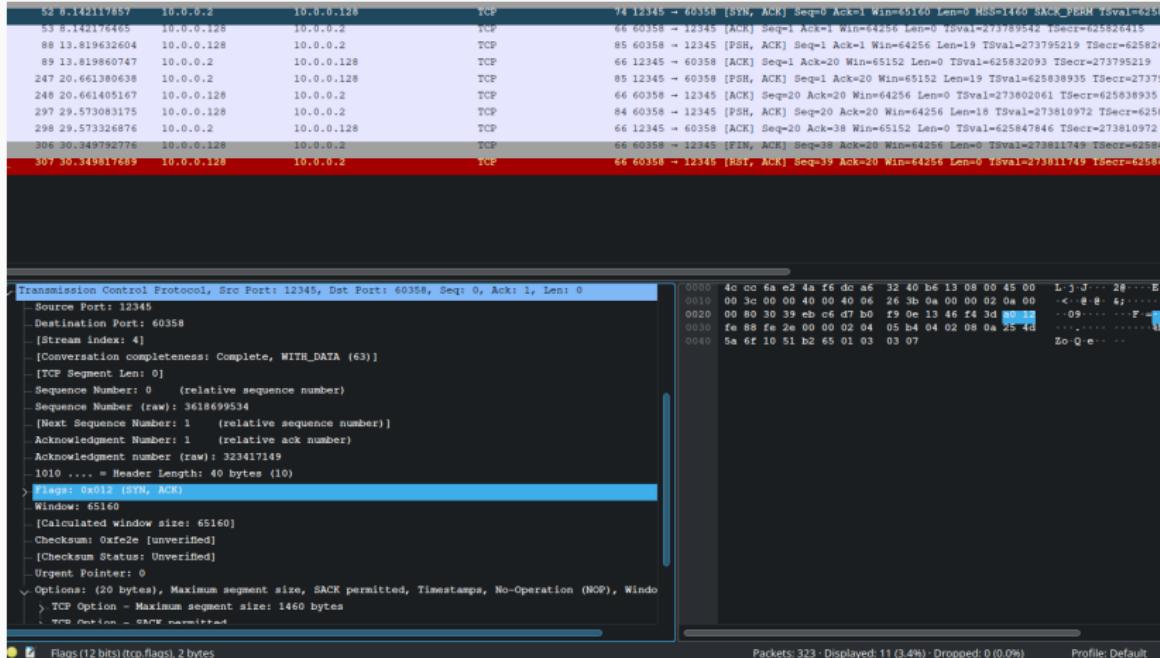


Рис. 20: tcp syn ack

TCP ACK

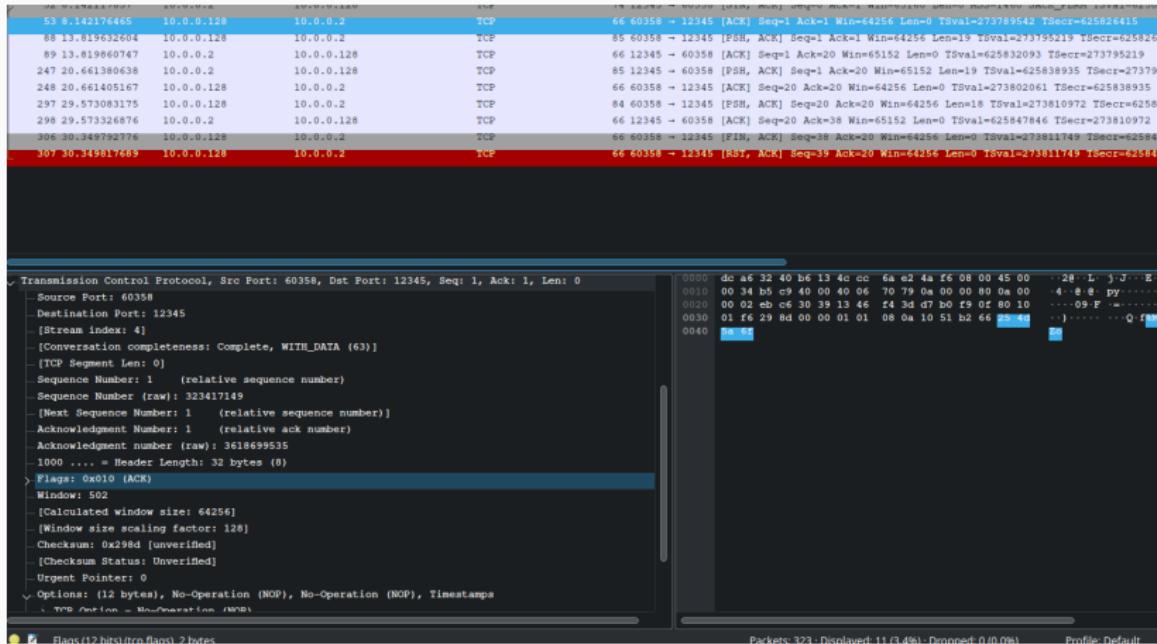


Рис. 21: tcp ack

TCP PSH ACK

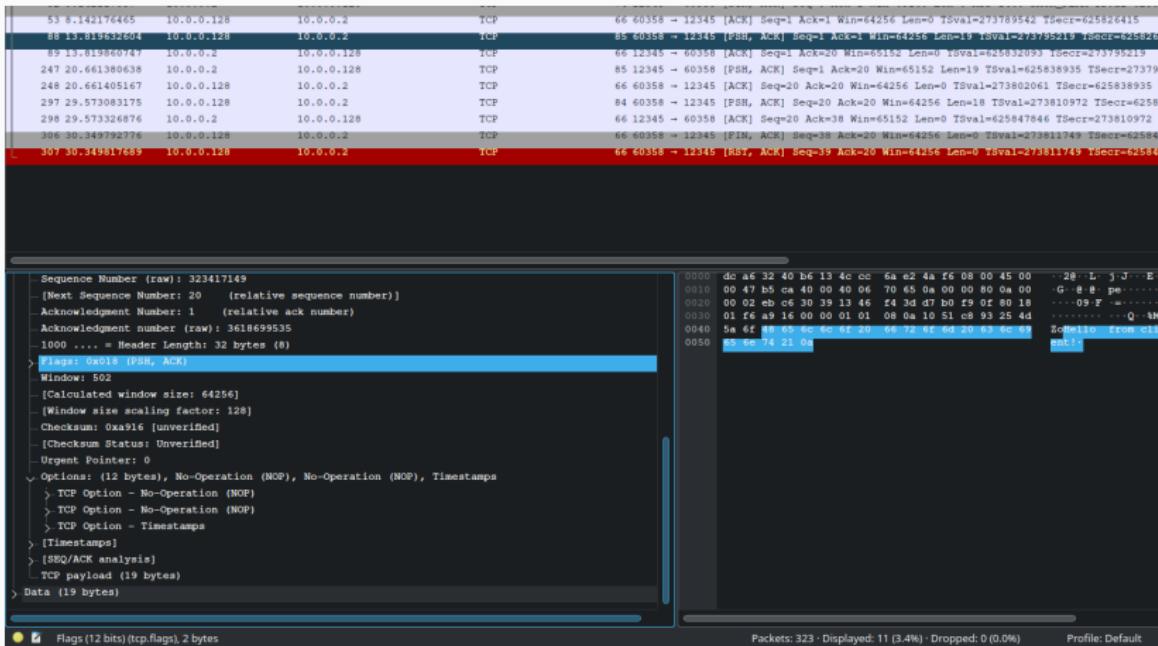


Рис. 22: tcp psh ack client

TCP PSH ACK

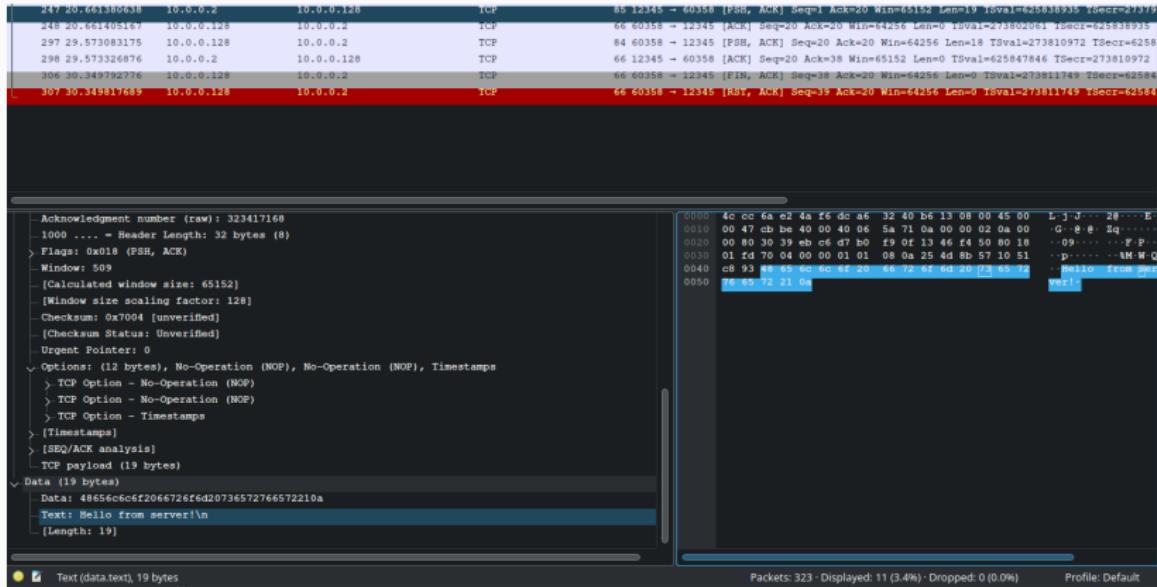


Рис. 23: tcp psh ack server

TCP FIN ACK

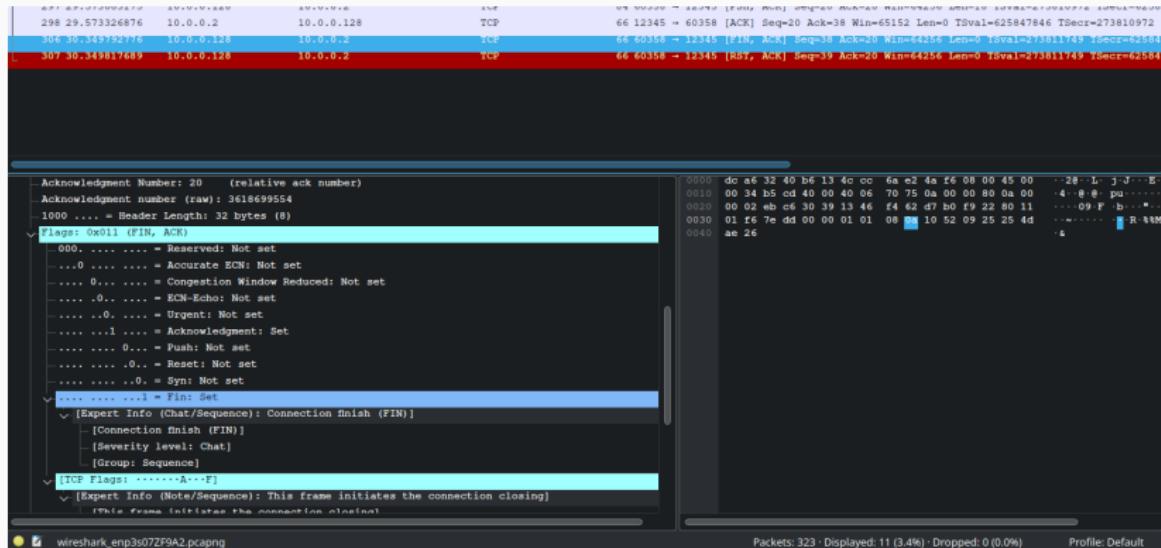


Рис. 24: tcp fin ack

Вывод

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