

# Анализ трафика в Wireshark

Лабораторная работа №3

---

Гафоров Нурмухаммад

9 октября 2025

Российский университет дружбы народов, Москва, Россия

## Цели и задачи работы

---

Изучить принципы работы сетевых протоколов ARP, ICMP, TCP, UDP и QUIC посредством анализа трафика в программе **Wireshark**.

## Ход выполнения

---

На локальном компьютере с помощью команды `ipconfig` были определены IP-адрес, маска подсети и шлюз по умолчанию.

```
Адаптер Ethernet Ethernet:
```

```
DNS-суффикс подключения . . . . . :  
Локальный IPv6-адрес канала . . . : fe80::c564:8f78:cb9:e047%18  
IPv4-адрес. . . . . : 192.168.1.180  
Маска подсети . . . . . : 255.255.255.0  
Основной шлюз. . . . . : 192.168.1.1
```

Рис. 1: Определение IP-адреса и шлюза по умолчанию

## Проверка доступности шлюза

Был выполнен тест связи командой `ping 192.168.1.1`. Пакеты получены без потерь, что подтвердило корректную работу сети.

```
PS C:\Users\gaforov\Documents> ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64
Ответ от 192.168.1.1: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
PS C:\Users\gaforov\Documents> |
```

Рис. 2: Проверка доступности шлюза

# Анализ ICMP-трафика

В Wireshark применён фильтр `arp or icmp`. Зафиксированы пакеты ICMP Echo Request и Echo Reply между устройством и шлюзом.

The screenshot shows the Wireshark interface with the filter `arp or icmp` applied. The packet list displays various ARP and ICMP packets. The selected packet is an ICMP Echo Request (ping) with ID 0x0001, sequence 4/1024, and TTL 128. The packet details pane shows the following information:

- Frame 328: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{C2D0B97A-6F95-42A3-8CBA-FE3689DA50K}
- Ethernet II, Src: HuaweiTechno\_8f:73:82 (e4:c:d1:8f:73:82), Dst: ASUSTekCOMPU\_78:b6:f2 (c8:7f:54:78:b6:f2)
- Destination: ASUSTekCOMPU\_78:b6:f2 (c8:7f:54:78:b6:f2)
- Source: HuaweiTechno\_8f:73:82 (e4:c:d1:8f:73:82)
- Type: IPv4 (0x0000)
- [Stream index: 3]
- Internet Protocol Version 4, Src: 192.168.1.180, Dst: 192.168.1.1
- .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 60
- Identification: 0xae19 (44569)
- 000. .... = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128

The packet bytes pane shows the raw data in hexadecimal and ASCII format.

# Анализ ICMP-трафика

В Wireshark применён фильтр `arp or icmp`. Зафиксированы пакеты ICMP Echo Request и Echo Reply между устройством и шлюзом.

The screenshot shows the Wireshark interface with the filter `arp or icmp` applied. The packet list displays several ICMP Echo (ping) requests and replies. The selected packet is an ICMP Echo (ping) reply from 192.168.1.100 to 192.168.1.1.

No.	Time	Source	Destination	Protocol	Length	Info
326	19.007406	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
327	20.054141	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
328	20.192605	192.168.1.100	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 329)
329	20.193070	192.168.1.1	192.168.1.100	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 328)
332	21.055424	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
333	21.197967	192.168.1.100	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 334)
334	21.198498	192.168.1.1	192.168.1.100	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 333)
348	22.079404	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
349	22.210801	192.168.1.100	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 350)
350	22.211334	192.168.1.1	192.168.1.100	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 349)
352	23.126086	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
353	23.226388	192.168.1.100	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 354)
354	23.226883	192.168.1.1	192.168.1.100	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 353)
356	24.127338	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
367	25.151301	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
372	26.197918	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
373	27.199311	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
375	27.357887	iCommSeemicon_9a:80:80::	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
381	28.223192	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
386	29.270108	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
391	30.271113	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
400	31.209099	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
404	32.341875	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
405	33.343051	ASUSTekCOMPU_78:b6:f2::	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1

Packet 329 details:

- Frame 329: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{C2D0097A-6F95-42A3-BC0A-FE36B9DA5B1} over Ethernet II, Src: ASUSTekCOMPU\_78:b6:f2:: (c8:7f:54:78:b6:f2), Dst: HuaweiTechno\_8f:73:82 (e4:c2:d1:8f:73:82)
- Destination: HuaweiTechno\_8f:73:82 (e4:c2:d1:8f:73:82)
- Source: ASUSTekCOMPU\_78:b6:f2 (c8:7f:54:78:b6:f2)
- Type: IPv4 (0x0000)
- [Stream index: 3]
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.100
- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 60
- Identification: 0x40a3 (16547)
- 000. .... = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 64

Packet bytes (hex): 0000 e4 c2 d1 8f 73 00 00 3c 40 a3 00 00 00 01 b4 00 00 51 00 30 67 68 69 6a 61 00 40 77 61 62 63 64



Перед ICMP-обменом выполняется разрешение MAC-адреса шлюза через ARP-запрос и ответ.

The screenshot displays the Wireshark interface with a packet capture on the 'Ethernet' interface. The packet list shows a series of ARP requests (broadcast) and one ICMP Echo (ping) reply. The selected packet (No. 474) is an ARP request from ASUSTekCOMPU\_78:b6:f2 to the gateway 192.168.1.180. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and ARP sections. The ARP section indicates a request for the MAC address of 192.168.1.180.

No.	Time	Source	Destination	Protocol	Length	Info
354	23.226883	192.168.1.1	192.168.1.180	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 353)
356	24.127330	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
367	25.151301	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
372	26.107918	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
373	27.109311	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
375	27.357887	iComsSemicon_9a:08:00	Broadcast	ARP	60	ARP Announcement for 192.168.1.32
381	28.223192	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
386	29.270160	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
391	30.271113	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
400	31.295099	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
404	32.341875	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
405	33.343051	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
408	34.366972	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
412	35.413548	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
417	36.414984	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
422	37.438965	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
441	38.485555	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
461	39.486859	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
466	40.510813	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
469	41.557402	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
473	42.558777	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1
474	43.550758	ASUSTekCOMPU_78:b6:f2	HuaweiTechno_8f:73:82	ARP	60	Who has 192.168.1.180? Tell 192.168.1.1
475	43.550789	HuaweiTechno_8f:73:82	ASUSTekCOMPU_78:b6:f2	ARP	42	192.168.1.180 is at e4:c2:d1:8f:73:82
476	43.582761	ASUSTekCOMPU_78:b6:f2	Broadcast	ARP	60	Who has 192.168.1.160? Tell 192.168.1.1

Frame 474: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF{C2D0B97A-6F95-42A3-BC0A-FE36B9DA5B} Ethernet II, Src: ASUSTekCOMPU\_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: HuaweiTechno\_8f:73:82 (e4:c2:d1:8f:73:82)

Destination: HuaweiTechno\_8f:73:82 (e4:c2:d1:8f:73:82)

Source: ASUSTekCOMPU\_78:b6:f2 (c8:7f:54:78:b6:f2)

Type: ARP (0x0806)

[Stream index: 3]

Padding: 00000000000000000000000000000000

Trailer: 11c450af

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: ASUSTekCOMPU\_78:b6:f2 (c8:7f:54:78:b6:f2)

Sender IP address: 192.168.1.1

Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.1.180

## Проверка связи с внешним ресурсом

Командой `ping yandex.ru` выполнен тест соединения с удалённым узлом. Среднее время отклика составило 8 мс.

```
PS C:\Users\gaforov\Documents>
PS C:\Users\gaforov\Documents> ping yandex.ru

Обмен пакетами с yandex.ru [77.88.55.88] с 32 байтами данных:
Ответ от 77.88.55.88: число байт=32 время=8мс TTL=247
Ответ от 77.88.55.88: число байт=32 время=8мс TTL=247
Ответ от 77.88.55.88: число байт=32 время=8мс TTL=247
Ответ от 77.88.55.88: число байт=32 время=8мс TTL=247

Статистика Ping для 77.88.55.88:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 8мсек, Максимальное = 8 мсек, Среднее = 8 мсек
PS C:\Users\gaforov\Documents> |
```

Рис. 6: Проверка доступности внешнего ресурса

# Анализ ICMP при обращении к внешнему серверу

Фильтр `arp or icmp` показал обмен ICMP-запросами с адресом 77.88.55.88 (yandex.ru).

27	8.287285	192.168.1.180	77.88.55.88	ICMP	74 Echo (ping) request	id=0x0001, seq=5/1280, ttl=128 (reply in 28)
28	8.295782	77.88.55.88	192.168.1.180	ICMP	74 Echo (ping) reply	id=0x0001, seq=5/1280, ttl=247 (request in 27)
34	9.291634	192.168.1.180	77.88.55.88	ICMP	74 Echo (ping) request	id=0x0001, seq=6/1536, ttl=128 (reply in 35)
35	9.300256	77.88.55.88	192.168.1.180	ICMP	74 Echo (ping) reply	id=0x0001, seq=6/1536, ttl=247 (request in 34)
36	10.307004	192.168.1.180	77.88.55.88	ICMP	74 Echo (ping) request	id=0x0001, seq=7/1792, ttl=128 (reply in 37)
37	10.315621	77.88.55.88	192.168.1.180	ICMP	74 Echo (ping) reply	id=0x0001, seq=7/1792, ttl=247 (request in 36)
40	11.320312	192.168.1.180	77.88.55.88	ICMP	74 Echo (ping) request	id=0x0001, seq=8/2048, ttl=128 (reply in 41)
41	11.328981	77.88.55.88	192.168.1.180	ICMP	74 Echo (ping) reply	id=0x0001, seq=8/2048, ttl=247 (request in 40)
49	14.397935	ASUSTekCOMPU_78:b6:f2::...	HuaweiTechno_8f:73:82::...	ARP	60 Who has 192.168.1.180? Tell 192.168.1.1	
50	14.397966	HuaweiTechno_8f:73:82::...	ASUSTekCOMPU_78:b6:f2::...	ARP	42 192.168.1.180 is at e4:c2:d1:8f:73:82	

> Frame 27: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{C2DD897A-6F95-42A3-8C0A-FE36B9DA58C}	0000 c8 7f 54 78 b6
> Ethernet II, Src: HuaweiTechno_8f:73:82 (e4:c2:d1:8f:73:82), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)	0010 00 3c 26 49 00
> Destination: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)	0020 37 58 00 00 4c
> Source: HuaweiTechno_8f:73:82 (e4:c2:d1:8f:73:82)	0030 67 68 69 6a 6b
Type: IPv4 (0x0800)	0040 77 61 62 63 64
[Stream index: 0]	
> Internet Protocol Version 4, Src: 192.168.1.180, Dst: 77.88.55.88	
0100 .... = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 60	
Identification: 0x2649 (9801)	
> 000. .... = Flags: 0x0	
...0 0000 0000 0000 = Fragment Offset: 0	
Time to Live: 128	
Protocol: ICMP (1)	
Header Checksum: 0x0000 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 192.168.1.180	
Destination Address: 77.88.55.88	

При фильтрации по **http** зафиксированы запросы **GET** и ответы **HTTP/1.1 304 Not Modified**.  
Данные передаются через TCP с портом 80.

The screenshot shows the Wireshark interface with a packet list and packet details pane. The packet list shows several HTTP GET requests and responses. The packet details pane shows the structure of a TCP segment and an HTTP response.

No.	Time	Source	Destination	Protocol	Length	Info
24	3.204475	192.168.1.180	188.184.67.127	HTTP	609	GET / HTTP/1.1
28	3.258332	188.184.67.127	192.168.1.180	HTTP	250	HTTP/1.1 304 Not Modified
53	4.638328	192.168.1.180	188.184.67.127	HTTP	609	GET / HTTP/1.1
57	4.692395	188.184.67.127	192.168.1.180	HTTP	250	HTTP/1.1 304 Not Modified
80	6.012460	192.168.1.180	188.184.67.127	HTTP	609	GET / HTTP/1.1
84	6.063829	188.184.67.127	192.168.1.180	HTTP	250	HTTP/1.1 304 Not Modified

Frame 28: 250 bytes on wire (2000 bits), 250 bytes captured (2000 bits) on interface \Device\NPF\_{C20DB97A-6F95-42A3-8C0A-FE368...}

Ethernet II, Src: ASUSTekCOMPU\_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: HuaweiTechno\_8f:73:02 (e4:c2:d1:8f:73:02)

Internet Protocol Version 4, Src: 188.184.67.127, Dst: 192.168.1.180

Transmission Control Protocol, Src Port: 80, Dst Port: 50781, Seq: 1, Ack: 556, Len: 196

Source Port: 80  
Destination Port: 50781  
[Stream index: 2]  
[Stream Packet Number: 6]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 196]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 545287938  
[Next Sequence Number: 197 (relative sequence number)]  
Acknowledgment Number: 556 (relative ack number)  
Acknowledgment number (raw): 3284002225  
R101 ... Header Length: 20 bytes (5)

0000 e4 c2 d1 8f 73  
0010 00 ec 22 a1 46  
0020 01 b4 00 50 c1  
0030 00 f9 40 45 06  
0040 30 34 20 4e 61  
0050 0a 44 61 74 65  
0060 63 74 20 32 36  
0070 20 47 4d 54 0c  
0080 61 63 66 65 06  
0090 69 65 64 3a 24  
00a0 20 32 30 31 34  
00b0 4d 54 0d 0a 45  
00c0 66 31 61 61 64  
00d0 63 63 65 70 74  
00e0 74 65 73 0d 06  
00f0 20 63 6c 6f 73

С помощью фильтра **dns** зафиксированы DNS-запросы и ответы, использующие порты 53 (сервер) и 50854 (клиент).

The screenshot shows the Wireshark interface with the 'dns' filter applied. The packet list pane displays several DNS queries and responses, along with an ICMP 'Destination unreachable' message. The packet details pane for packet 12 (1.797408) shows a User Datagram Protocol (UDP) segment with source port 53 and destination port 50854. The UDP payload is a Domain Name System (DNS) response.

No.	Time	Source	Destination	Protocol	Length	Info
5	1.254266	192.168.1.180	192.168.1.1	DNS	77	Standard query 0x1bf3 A line-mode.cern.ch
6	1.254358	192.168.1.180	192.168.1.1	DNS	77	Standard query 0x42b6 HTTPS line-mode.cern.ch
7	1.265861	192.168.1.180	192.168.1.1	DNS	76	Standard query 0x9cc4 A home.web.cern.ch
8	1.265915	192.168.1.180	192.168.1.1	DNS	76	Standard query 0x6c4f HTTPS home.web.cern.ch
12	1.797408	192.168.1.1	192.168.1.180	DNS	157	Standard query response 0x1bf3 A line-mode.cern.ch CNAME paas-apps-shard-
13	1.715791	192.168.1.1	192.168.1.180	DNS	158	Standard query response 0x9cc4 A home.web.cern.ch CNAME drupal-apps-shard-
14	1.790132	192.168.1.1	192.168.1.180	DNS	169	Standard query response 0x6c4f HTTPS home.web.cern.ch CNAME drupal-apps-s-
15	1.790156	192.168.1.180	192.168.1.1	ICMP	197	Destination unreachable (Port unreachable)
16	1.864207	192.168.1.1	192.168.1.180	DNS	168	Standard query response 0x42b6 HTTPS line-mode.cern.ch CNAME paas-apps-sh-

Frame 12: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF\_{C200B97A-6F95-42A3-8C0A-FE36B90D} Ethernet II, Src: ASUSTekCOMPU\_78:b6:f2 (c8:7f:54:78:b6:f2), Dst: HuaweiTechno\_8f:73:82 (e4:c2:d1:8f:73:82) Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.180 User Datagram Protocol, Src Port: 53, Dst Port: 50854 Source Port: 53 Destination Port: 50854 Length: 123 Checksum: 0x5f2e [unverified] [Checksum Status: Unverified] [Stream Index: 2] [Stream Packet Number: 2] [Timestamps] UDP payload (115 bytes) Domain Name System (response) Transaction ID: 0x1bf3 Flags: 0x1100 Standard query response. No error

# Анализ протокола QUIC

Фильтр `quic` выявил пакеты Initial, Handshake, PING и CRYPTO, передаваемые по UDP.  
Протокол обеспечивает быструю и защищённую передачу данных.

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Packets, Capture, Analysis, Statistics, Telephony, Wireless, Instruments, and Help. The packet list pane on the left shows a list of captured packets, with the filter 'quic' applied. The main packet details pane shows the selected packet (No. 1159) and its details. The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
1154	16.186939	192.168.1.100	142.250.74.138	QUIC	1292	Initial, DCID=ea4d5163ef9a29bf, PKN: 1, PING, PING, PADDING, PING...
1155	16.186960	192.168.1.100	142.250.74.138	QUIC	1292	Initial, DCID=ea4d5163ef9a29bf, PKN: 2, CRYPTO, PING, CRYPTO, CRY...
1156	16.187064	192.168.1.100	142.250.74.138	QUIC	124	0-RTT, DCID=ea4d5163ef9a29bf
1157	16.187675	192.168.1.100	142.250.74.131	QUIC	1292	Initial, DCID=1bea2bb6c8fe92f1, PKN: 1, PADDING, PING, CRYPTO, CR...
1158	16.187698	192.168.1.100	142.250.74.131	QUIC	1292	Initial, DCID=1bea2bb6c8fe92f1, PKN: 2, CRYPTO
1159	16.187711	192.168.1.100	142.250.74.131	QUIC	1292	Initial, DCID=1bea2bb6c8fe92f1, PKN: 3, PING, PADDING, PING, PING...
1160	16.187795	192.168.1.100	142.250.74.131	QUIC	124	0-RTT, DCID=1bea2bb6c8fe92f1
1162	16.211784	142.250.74.138	192.168.1.100	QUIC	82	Initial, SCID=ea4d5163ef9a29bf, PKN: 1, ACK
1163	16.212212	142.250.74.138	192.168.1.100	QUIC	1292	Initial, SCID=ea4d5163ef9a29bf, PKN: 2, ACK, PADDING
1164	16.214596	142.250.74.131	192.168.1.100	QUIC	82	Initial, SCID=fbae2bb6c8fe92f1, PKN: 1, ACK
1165	16.214596	142.250.74.131	192.168.1.100	QUIC	82	Initial, SCID=fbae2bb6c8fe92f1, PKN: 2, ACK
1166	16.214626	142.250.74.131	192.168.1.100	QUIC	1292	Initial, SCID=fbae2bb6c8fe92f1, PKN: 3, ACK, PADDING
1167	16.215095	142.250.74.131	192.168.1.100	QUIC	1292	Initial, SCID=fbae2bb6c8fe92f1, PKN: 4, ACK, PADDING
1168	16.221386	142.250.74.138	192.168.1.100	QUIC	1292	Initial, SCID=ea4d5163ef9a29bf, PKN: 3, CRYPTO, PADDING
1169	16.221386	142.250.74.138	192.168.1.100	QUIC	349	Protected Payload (K0)
1170	16.221386	142.250.74.138	192.168.1.100	QUIC	985	Protected Payload (K0)
1171	16.221648	142.250.74.138	192.168.1.100	QUIC	76	Protected Payload (K0)
1172	16.221694	192.168.1.100	142.250.74.138	QUIC	120	Handshake, DCID=ea4d5163ef9a29bf
1173	16.221732	192.168.1.100	142.250.74.138	QUIC	73	Protected Payload (K0), DCID=ea4d5163ef9a29bf
1174	16.222132	142.250.74.131	192.168.1.100	QUIC	1292	Initial, SCID=fbae2bb6c8fe92f1, PKN: 5, CRYPTO, PADDING
1175	16.222132	142.250.74.131	192.168.1.100	QUIC	342	Protected Payload (K0)
1176	16.223433	192.168.1.100	142.250.74.131	QUIC	120	Handshake, DCID=fbae2bb6c8fe92f1
1177	16.225541	142.250.74.131	192.168.1.100	QUIC	990	Protected Payload (K0)
1178	16.222705	192.168.1.100	142.250.74.131	QUIC	73	Protected Payload (K0), DCID=fbae2bb6c8fe92f1

The packet details pane shows the selected packet (No. 1159) and its details. The packet is a QUIC Initial packet, DCID=1bea2bb6c8fe92f1, PKN: 3, PING, PADDING, PING, PING... The packet length is 1292 bytes. The packet is a UDP payload (1250 bytes).

The packet details pane shows the following details:

- QUIC IETF
- QUIC Connection Information
- [Packet Length: 1250]
- 1... .. = Header Form: Long Header (1)
- 1... .. = Fixed Bit: True
- ..00 .. = Packet Type: Initial (0)
- [... 00.. = Reserved: 0]
- [... ..00 = Packet Number Length: 1 bytes (0)]
- Version: 1 (0x00000001)
- Destination Connection ID Length: 8
- Destination Connection ID: 1bea2bb6c8fe92f1
- Source Connection ID Length: 0
- Token Length: 70
- Token: 00f076291a471d426f0cc752a942d43ac3e711dd7ed81956b4f256ba7e62e6083c9082f0da73eda8ed8c3b790570d08460e43fbd4aa49e5f097010e0b1c310770

Исследован процесс установления TCP-соединения (Three-Way Handshake):

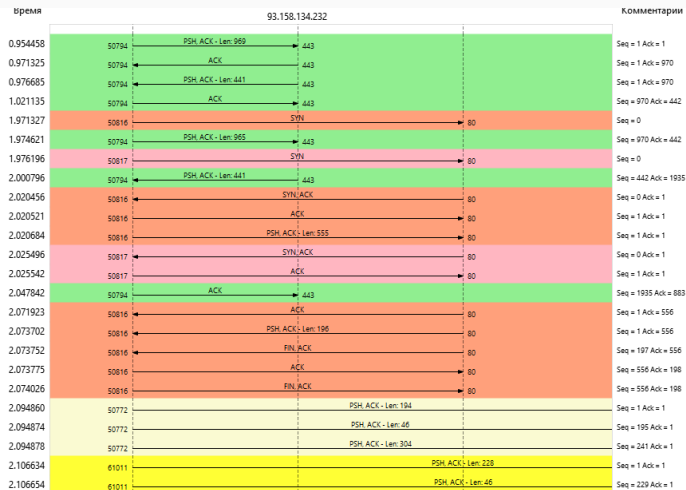
1. SYN — инициация соединения клиентом.
2. SYN/ACK — подтверждение сервером.
3. ACK — завершение установления.

No.	Time	Source	Destination	Protocol	Length	Info
7	1.084533	192.168.1.123	255.255.255.255	UDP	246	59728 → 6667 Len=204
8	1.971327	192.168.1.180	188.184.67.127	TCP	66	50816 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9	1.974621	192.168.1.180	93.158.134.232	TLSv1.2	1019	Application Data
10	1.976196	192.168.1.180	188.184.67.127	TCP	66	50817 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
11	1.983841	ASUSTekCOMPU_78:b6:...	Spanning-tree (for...	STP	60	Conf. Root = 32768/0/c8:7f:54:78:b6:f2 Cost = 0 Port = 0x8001
12	2.000796	93.158.134.232	192.168.1.180	TLSv1.2	495	Application Data
13	2.020456	188.184.67.127	192.168.1.180	TCP	66	80 → 50816 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_P...
14	2.020521	192.168.1.180	188.184.67.127	TCP	54	50816 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
15	2.020684	192.168.1.180	188.184.67.127	HTTP	609	GET / HTTP/1.1
16	2.025496	188.184.67.127	192.168.1.180	TCP	66	80 → 50817 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1460 SACK_P...
17	2.025542	192.168.1.180	188.184.67.127	TCP	54	50817 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
18	2.047842	192.168.1.180	93.158.134.232	TCP	54	50794 → 443 [ACK] Seq=1935 Ack=883 Win=1021 Len=0
19	2.071923	188.184.67.127	192.168.1.180	TCP	60	80 → 50816 [ACK] Seq=1 Ack=556 Win=31872 Len=0
20	2.073702	188.184.67.127	192.168.1.180	HTTP	250	HTTP/1.1 304 Not Modified
21	2.073752	188.184.67.127	192.168.1.180	TCP	60	80 → 50816 [FIN, ACK] Seq=197 Ack=556 Win=31872 Len=0
22	2.073775	192.168.1.180	188.184.67.127	TCP	54	50816 → 80 [ACK] Seq=556 Ack=198 Win=262400 Len=0
23	2.074026	192.168.1.180	188.184.67.127	TCP	54	50816 → 80 [FIN, ACK] Seq=556 Ack=198 Win=262400 Len=0
24	2.094659	192.168.1.180	192.168.1.1	DNS	88	Standard query 0x6fd7 A browser.translate.yandex.net
25	2.094721	192.168.1.180	192.168.1.1	DNS	88	Standard query 0x0336 HTTPS browser.translate.yandex.net
26	2.094860	192.168.1.180	87.250.251.20	TLSv1.2	248	Application Data
27	2.094874	192.168.1.180	87.250.251.20	TLSv1.2	100	Application Data
28	2.094878	192.168.1.180	87.250.251.20	TLSv1.2	358	Application Data
29	2.105578	192.168.1.1	192.168.1.180	DNS	104	Standard query response 0x6fd7 A browser.translate.yandex.net A 8...
30	2.106634	192.168.1.180	213.180.193.234	TLSv1.2	282	Application Data

Рис. 11: Захват TCP handshake в Wireshark

# График потока TCP

На графике потока отображается последовательность обмена сегментами SYN → SYN/ACK → ACK, подтверждающая корректное установление соединения.





## Выводы

---

В результате работы были исследованы протоколы **ARP**, **ICMP**, **TCP**, **UDP** и **QUIC** с помощью анализатора **Wireshark**.

Получены практические навыки по анализу сетевого трафика и пониманию принципов работы транспортного уровня стека TCP/IP.

Процесс трёхэтапного установления соединения (**TCP Handshake**) был подробно изучен, что подтвердило надёжность и согласованность протокола TCP.