

# **Отчёт по лабораторной работе 3**

## **Анализ трафика в Wireshark**

Хамди Мохаммад

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Ход выполнения</b>	<b>6</b>
2.1 Анализ кадров канального уровня в Wireshark . . . . .	6
2.2 Анализ протоколов транспортного уровня в Wireshark . . . . .	12
2.3 Анализ handshake протокола TCP в Wireshark . . . . .	17
<b>3 Заключение</b>	<b>19</b>

# **Список иллюстраций**

2.1 Результат команды ipconfig . . . . .	7
2.2 Проверка доступности шлюза . . . . .	7
2.3 Проверка доступности внешнего ресурса . . . . .	11
2.4 Анализ ICMP-трафика при ping google.com . . . . .	12
2.5 Анализ TCP-сессии . . . . .	17
2.6 График потока TCP . . . . .	18

# **Список таблиц**

# **1 Цель работы**

Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

## **2 Ход выполнения**

### **2.1 Анализ кадров канального уровня в Wireshark**

1. На устройство была установлена программа **Wireshark** и запущен захват трафика на активном сетевом интерфейсе.
2. С помощью команды **ipconfig** были определены параметры сетевого подключения:
  - IP-адрес устройства – **192.168.1.35**
  - Маска подсети – **255.255.255.0**
  - Шлюз по умолчанию – **192.168.1.1**

```

PS C:\work\hamdimohammad\vagrant> ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet:

DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . . . : fe80::52ff:33b6:449a:870f%18
IPv4-адрес . . . . . : 192.168.1.35
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : 192.168.1.1

Адаптер Ethernet Ethernet 2:

DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . . . : fe80::d3f2:8384:1a21:d660%21
IPv4-адрес . . . . . : 192.168.56.1
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . :

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

```

Рис. 2.1: Результат команды ipconfig

3. Для проверки доступности шлюза по умолчанию выполнена команда **ping 192.168.1.1.**

Ответы получены успешно, потерь пакетов нет.

```

PS C:\work\hamdimohammad\vagrant>
PS C:\work\hamdimohammad\vagrant> ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по с 32 байтами данных:
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% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
PS C:\work\hamdimohammad\vagrant> |

```

Рис. 2.2: Проверка доступности шлюза

4. В **Wireshark** был применён фильтр **arp or icmp**, после чего зафиксированы ICMP-запросы и ответы между устройством и шлюзом.

Захват из Ethernet						
Файл	Правка	Вид	Запуск	Захват	Анализ	Статистика
arp or icmp						
No.	Time	Source	Destination	Protocol	Length	Info
43	25.470110	iCommSemicon_9a:80..	Broadcast	ARP	68	ARP Announcement for 192.168.1.32
45	26.353498	ASUSTekCOMPU_78:b6..	HuaweiTechno_66:db:..	ARP	68	Who has 192.168.1.35? Tell 192.168.1.1
46	26.353528	HuaweiTechno_66:db:..	ASUSTekCOMPU_78:b6:..	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28
67	38.559919	82:81:04:02:d3:54	Broadcast	ARP	68	Who has 192.168.1.1? Tell 192.168.1.145
→ 180	48.886492	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 181)
← 181	48.887000	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 180)
184	49.889283	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 185)
185	49.889874	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=64 (request in 184)
189	50.902327	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 190)
190	50.902821	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=64 (request in 189)
193	51.913548	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 194)
194	51.913999	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=64 (request in 193)
201	60.997244	iCommSemicon_9a:80..	Broadcast	ARP	68	ARP Announcement for 192.168.1.32
248	71.152221	ASUSTekCOMPU_78:b6:..	HuaweiTechno_66:db:..	ARP	68	Who has 192.168.1.35? Tell 192.168.1.1
249	71.152253	HuaweiTechno_66:db:..	ASUSTekCOMPU_78:b6:..	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28
298	98.414703	iCommSemicon_9a:80..	Broadcast	ARP	68	ARP Announcement for 192.168.1.32
307	98.596789	82:81:04:02:d3:54	Broadcast	ARP	68	Who has 192.168.1.1? Tell 192.168.1.145
361	119.790925	ASUSTekCOMPU_78:b6:..	HuaweiTechno_66:db:..	ARP	68	Who has 192.168.1.35? Tell 192.168.1.1
362	119.790945	HuaweiTechno_66:db:..	ASUSTekCOMPU_78:b6:..	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28

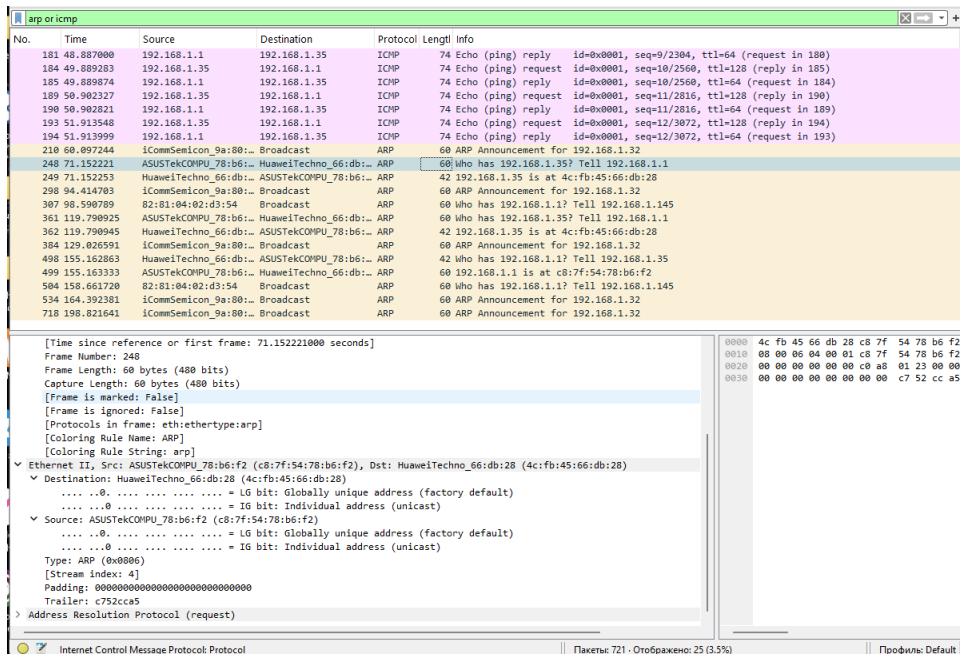
```
[Time delta from previous displayed frame: 10.326573000 seconds]
[Time since reference or first frame: 48.886492000 seconds]
Frame Number: 188
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:icmpv6]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
▼ Ethernet II, Src: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
    ... .0. .... .0. .... .0. .... = LG bit: Globally unique address (factory default)
    ... .0. .... .0. .... .0. .... = IG bit: Individual address (unicast)
    ▾ Source: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)
        ... .0. .... .0. .... .0. .... = LG bit: Globally unique address (factory default)
        ... .0. .... .0. .... .0. .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 4]
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 192.168.1.1
> Internet Control Message Protocol
```

Пакеты: 353 - Отображено: 17 (4.8%) | Профиль: Default

Захват из Ethernet						
Файл	Правка	Вид	Запуск	Захват	Анализ	Статистика
arp or icmp						
No.	Time	Source	Destination	Protocol	Length	Info
43	25.470110	iCommSemicon_9a:80..	Broadcast	ARP	68	ARP Announcement for 192.168.1.32
45	26.353498	ASUSTekCOMPU_78:b6:..	HuaweiTechno_66:db:..	ARP	68	Who has 192.168.1.35? Tell 192.168.1.1
46	26.353528	HuaweiTechno_66:db:..	ASUSTekCOMPU_78:b6:..	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28
67	38.559919	82:81:04:02:d3:54	Broadcast	ARP	68	Who has 192.168.1.1? Tell 192.168.1.145
→ 180	48.886492	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 181)
← 181	48.887000	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=64 (request in 180)
184	49.889283	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 185)
185	49.889874	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2560, ttl=64 (request in 184)
189	50.902327	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 190)
190	50.902821	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=64 (request in 189)
193	51.913548	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 194)
194	51.913999	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=64 (request in 193)
210	60.997244	iCommSemicon_9a:80..	Broadcast	ARP	68	ARP Announcement for 192.168.1.32
248	71.152221	ASUSTekCOMPU_78:b6:..	HuaweiTechno_66:db:..	ARP	68	Who has 192.168.1.35? Tell 192.168.1.1
249	71.152253	HuaweiTechno_66:db:..	ASUSTekCOMPU_78:b6:..	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28
298	98.414703	iCommSemicon_9a:80..	Broadcast	ARP	68	ARP Announcement for 192.168.1.32
307	98.596789	82:81:04:02:d3:54	Broadcast	ARP	68	Who has 192.168.1.1? Tell 192.168.1.145
361	119.790925	ASUSTekCOMPU_78:b6:..	HuaweiTechno_66:db:..	ARP	68	Who has 192.168.1.35? Tell 192.168.1.1
362	119.790945	HuaweiTechno_66:db:..	ASUSTekCOMPU_78:b6:..	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28

```
[Time delta from previous displayed frame: 0.000508000 seconds]
[Time since reference or first frame: 48.887000000 seconds]
Frame Number: 181
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:icmpv6]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
▼ Ethernet II, Src: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28), Dst: ASUSTekCOMPU_78:b6:f2 (c8:7f:54:78:b6:f2)
    ... .0. .... .0. .... .0. .... = LG bit: Globally unique address (factory default)
    ... .0. .... .0. .... .0. .... = IG bit: Individual address (unicast)
    ▾ Source: HuaweiTechno_66:db:28 (4c:fb:45:66:db:28)
        ... .0. .... .0. .... .0. .... = LG bit: Globally unique address (factory default)
        ... .0. .... .0. .... .0. .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 4]
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.35
> Internet Control Message Protocol
```

Пакеты: 372 - Отображено: 19 (5.1%) | Профиль: Default



### Анализ ICMP-запроса:

- Длина кадра: **74 байта**
- Тип кадра: **Ethernet II**
- MAC-адрес источника: **4c:fb:45:66:db:28** (устройство)
- MAC-адрес получателя (шлюз): **c8:7f:54:78:b6:f2**
- Тип MAC-адресов: **уникальные (unicast)**

### Анализ ICMP-ответа:

- Длина кадра: **74 байта**
- Тип кадра: **Ethernet II**
- MAC-адрес источника (шлюз): **c8:7f:54:78:b6:f2**

- MAC-адрес получателя (устройство): **4c:fb:45:66:db:28**

- Тип MAC-адресов: **уникальные (unicast)**

5. Далее изучены кадры протокола **ARP**, фиксирующие обмен информацией об IP- и MAC-адресах в сети.

```
PS C:\work\hamdimohammad\vagrant>
PS C:\work\hamdimohammad\vagrant> ping google.com

Обмен пакетами с google.com [209.85.233.138] с 32 байтами данных:
Ответ от 209.85.233.138: число байт=32 время=18мс TTL=105

Статистика Ping для 209.85.233.138:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потеря)
Приблизительное время приема-передачи в мс:
Минимальное = 18мсек, Максимальное = 18 мсек, Среднее = 18 мсек
PS C:\work\hamdimohammad\vagrant> |
```

No.	Time	Source	Destination	Protocol	Length	Info
42	7.023378	192.168.1.35	209.85.233.138	ICMP	74	[Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 43)]
43	7.042102	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=105 (request in 42)
44	8.035659	192.168.1.35	209.85.233.138	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 47)
47	8.054125	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=105 (request in 46)
49	9.051899	192.168.1.35	209.85.233.138	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 50)
50	9.070316	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=105 (request in 49)
51	10.065063	192.168.1.35	209.85.233.138	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 52)
52	10.083705	209.85.233.138	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=105 (request in 51)
68	13.317423	iComSemicon_9e:8b:..	Broadcast	ARP	68	ARP Announcement for 192.168.1.32
78	24.423832	ASUSTeKCOMPU_78:b6:..	HuaweiTechno_66:db:..	ARP	68	Who has 192.168.1.35 Tell 192.168.1.32
79	24.423844	HuaweiTechno_66:db:..	ASUSTeKCOMPU_78:b6:..	ARP	42	192.168.1.35 is at 4c:fb:45:66:db:28

### ARP-запрос:

- “Кто имеет IP **192.168.1.35**?”

- Источник: **c8:7f:54:78:b6:f2**

- Адрес назначения: **ff:ff:ff:ff:ff:ff** (широковещательный, broadcast)

### ARP-ответ:

- “IP **192.168.1.35** принадлежит MAC **4c:fb:45:66:db:28**”

- Источник: **4c:fb:45:66:db:28**

- Адрес назначения: **c8:7f:54:78:b6:f2**

6. Для анализа взаимодействия с внешними ресурсами был выполнен **ping google.com.**

Устройство получило ответы от IP-адреса **209.85.233.138**, время отклика составило в среднем **18 мс.**

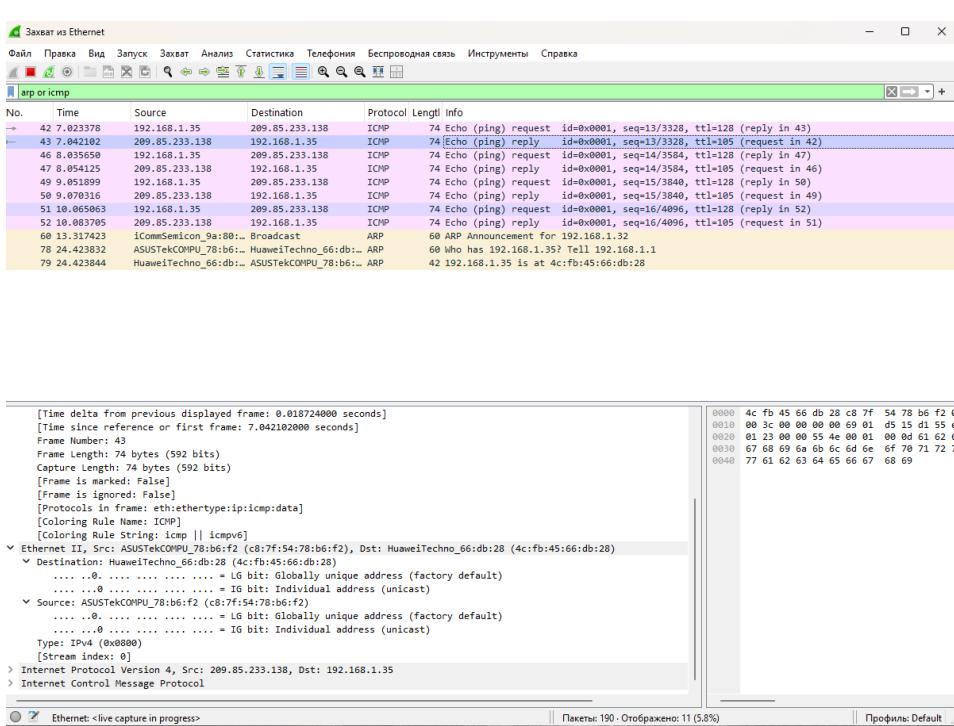


Рис. 2.3: Проверка доступности внешнего ресурса

В Wireshark были зафиксированы соответствующие ICMP-запросы и ответы, а также ARP-обмен для определения адреса шлюза.

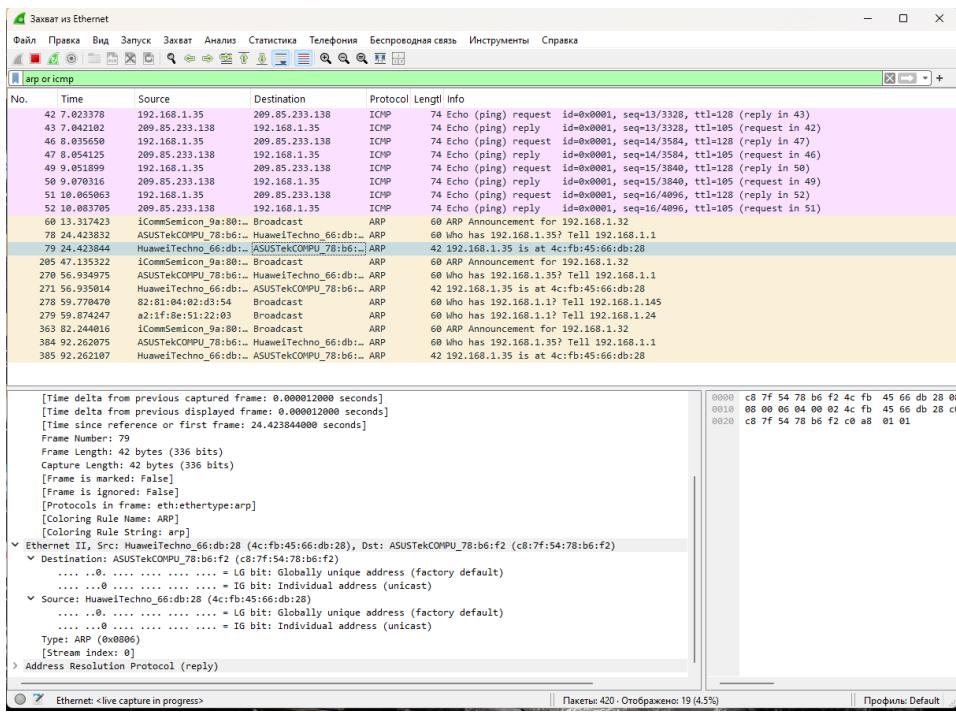


Рис. 2.4: Анализ ICMP-трафика при ping google.com

## 2.2 Анализ протоколов транспортного уровня в Wireshark

- В программе **Wireshark** был запущен захват трафика на активном сетевом интерфейсе.
- В браузере произведён переход на сайт <http://info.cern.ch/>, работающий по протоколу **HTTP**.
- В Wireshark применён фильтр **http**. Зафиксирован обмен HTTP-запросами и ответами поверх протокола **TCP**.

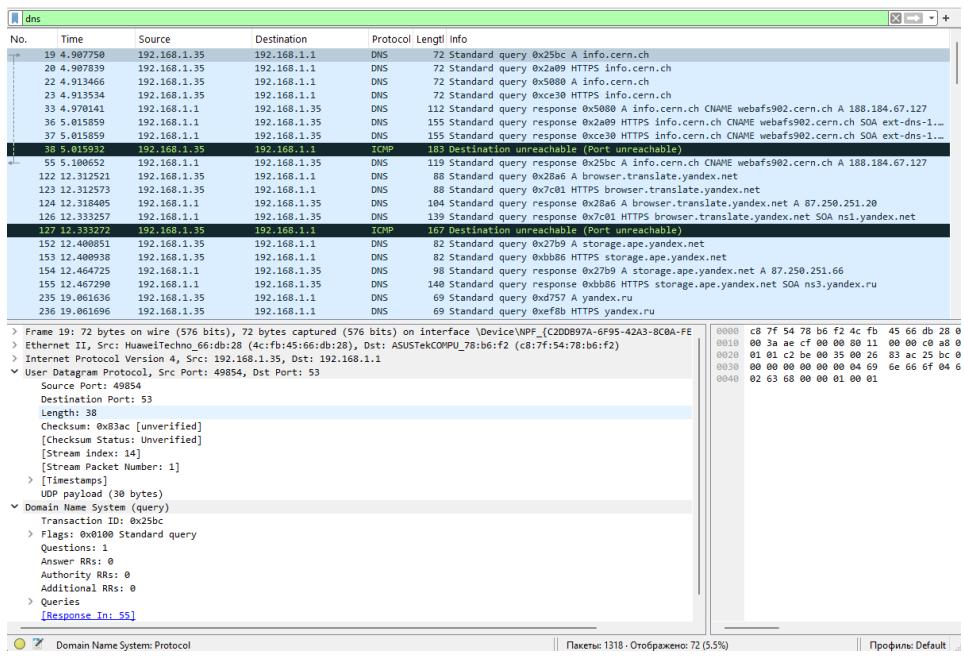
Захват из Ethernet						
Файл	Правка	Вид	Запуск	Захват	Анализ	Статистика
<b>http</b>						
No.	Time	Source	Destination	Protocol	Length	Info
347	23.756722	192.168.1.35	188.184.67.127	HTTP	497	497 GET / HTTP/1.1
349	23.810231	188.184.67.127	192.168.1.35	HTTP	932	932 HTTP/1.1 200 OK (text/html)
356	23.894813	192.168.1.35	188.184.67.127	HTTP	438	438 GET /favicon.ico HTTP/1.1
364	23.949575	188.184.67.127	192.168.1.35	HTTP	248	248 HTTP/1.1 200 OK (image/vnd.microsoft.icon)
503	41.501987	192.168.1.35	188.184.67.127	HTTP	557	557 GET /hypertext/WWW/TheProject.html HTTP/1.1
509	41.556199	188.184.67.127	192.168.1.35	HTTP	1044	1044 HTTP/1.1 200 OK (text/html)
<b>&gt; Frame 347: 497 bytes on wire (3976 bits), 497 bytes captured (3976 bits) on interface \Device\NPF_{C20DB97A-6F95-42A3-8C0A</b> <b>&gt; Ethernet II, Src: HuaweiTechno_66:db:28 (4:c:fb:45:66:db:28), Dst: ASUSTekCOMPU_78:b6:f2 (c:8:7f:54:78:b6:f2)</b> <b>&gt; Internet Protocol Version 4, Src: 192.168.1.35, Dst: 188.184.67.127</b> <b>&gt; Transmission Control Protocol, Src Port: 61111, Dst Port: 80, Seq: 1, Ack: 1, Len: 444</b> <b>Source Port: 61111</b> <b>Destination Port: 80</b> <b>[Stream index: 3]</b> <b>[Stream Packet Number: 4]</b> <b>&gt; [Conversation completeness: Complete, WITH_DATA (31)]</b> <b>[TCP Segment Len: 443]</b> <b>Sequence Number: 1 (relative sequence number)</b> <b>Sequence Number (raw): 3946666371</b> <b>[Next Sequence Number: 444 (relative sequence number)]</b> <b>Acknowledgment Number: 1 (relative ack number)</b> <b>Acknowledgment number (raw): 4115465422</b> <b>0101 .... = Header Length: 20 bytes (5)</b> <b>&gt; Flags: 0x018 (PSH, ACK)</b> <b>Window: 1026</b> <b>[Calculated window size: 262656]</b> <b>[Window size scaling factor: 256]</b> <b>Checksum: 0xc3d8 [unverified]</b> <b>[Checksum Status: Unverified]</b> <b>Urgent Pointer: 0</b> <b>&gt; [Timestamps]</b> <b>&gt; [SEQ/ACK analysis]</b> <b>TCP payload (443 bytes)</b> <b>&gt; Hypertext Transfer Protocol</b>						
0000	0b 7f 54 78 b5 f2 4c fb 45 66 db 28 9					
0010	c1 e3 7f fa 00 00 00 00 c0 a8 0					
0020	43 7f ee b7 00 50 eb 3d 59 83 f5 4d 0					
0030	04 02 c3 d8 00 00 47 45 54 20 2f 20 4					
0040	2f 31 2e 31 0d 00 48 6f 73 74 3a 20 6					
0050	2e 63 65 72 6e 2e 63 66 0d 00 43 6f 0					
0060	74 69 67 6e 3a 20 6b 65 65 78 24 61 6					
0070	20 6c 61 2f 3e 20 30 2e 30 20 57 69 6					
0080	72 65 2d 52 65 71 75 65 73 74 3a 24					
0090	55 73 65 72 2d 41 67 65 6e 74 3a 20 4					
00a0	6c 6e 61 2f 35 2e 30 28 57 69 6					
00b0	20 4e 54 20 31 30 2e 30 3b 20 57 69 6					
00c0	20 78 3d 34 29 20 41 79 70 6c 65 57 6					
00d0	20 6c 61 2f 35 2e 30 28 57 69 6					
00e0	20 6c 69 6b 65 66 65 63 6b 67 29 24					
00f0	6f 6d 5f 31 33 38 2e 30 2e 30 2e 34					
0100	42 72 6f 77 73 65 72 2f 32 35 2e 38 2					
0110	20 53 61 61 72 69 2f 35 33 37 2e 31					
0120	41 63 63 65 78 74 3a 26 74 65 78 74 2					
0130	6c 2d 61 72 69 78 74 3a 26 74 65 78 6					
0140	6c 2d 61 72 69 78 74 3a 26 74 65 78 6					
0150	69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 35					
0160	61 67 65 2f 61 76 69 66 2c 69 6d 61 6					
0170	65 62 79 2c 69 6d 61 67 65 2f 61 70 6					
0180	2f 2a 3b 73 3d 30 2e 38 2c 61 70 70 6					
0190	74 69 67 60 2f 73 69 67 6e 65 64 2d 6					
01a0	20 6c 61 2f 35 2e 30 28 57 69 6					
01b0	0a 41 63 63 65 70 74 2d 45 6e 63 6f 0					
01c0	3a 20 67 7a 69 70 2c 2d 64 65 66 6c 6					
01d0	0a 41 63 63 65 70 74 2d 4c 61 66 67 7					
01e0	3a 20 72 75 2c 65 6e 3b 71 3d 30 2e 35					
01f0	0a					
<b>Захват из Ethernet</b>						
Файл	Правка	Вид	Запуск	Захват	Статистика	Телефония
<b>http</b>						
No.	Time	Source	Destination	Protocol	Length	Info
347	23.756722	192.168.1.35	188.184.67.127	HTTP	497	497 GET / HTTP/1.1
349	23.810231	188.184.67.127	192.168.1.35	HTTP	932	932 HTTP/1.1 200 OK (text/html)
356	23.894813	192.168.1.35	188.184.67.127	HTTP	438	438 GET /favicon.ico HTTP/1.1
364	23.949575	188.184.67.127	192.168.1.35	HTTP	248	248 HTTP/1.1 200 OK (image/vnd.microsoft.icon)
503	41.501987	192.168.1.35	188.184.67.127	HTTP	557	557 GET /hypertext/WWW/TheProject.html HTTP/1.1
509	41.556199	188.184.67.127	192.168.1.35	HTTP	1044	1044 HTTP/1.1 200 OK (text/html)
<b>&gt; Frame 349: 932 bytes on wire (7456 bits), 932 bytes captured (7456 bits) on interface \Device\NPF_{C20DB97A-6F95-42A3-8C0A</b> <b>&gt; Ethernet II, Src: HuaweiTechno_66:db:28 (4:c:fb:45:66:db:28), Dst: ASUSTekCOMPU_78:b6:f2 (c:8:7f:54:78:b6:f2)</b> <b>&gt; Internet Protocol Version 4, Src: 192.168.1.35, Dst: 188.184.67.127</b> <b>&gt; Transmission Control Protocol, Src Port: 80, Dst Port: 61111, Seq: 1, Ack: 444, Len: 878</b> <b>Source Port: 80</b> <b>Destination Port: 61111</b> <b>[Stream index: 3]</b> <b>[Stream Packet Number: 6]</b> <b>&gt; [Conversation completeness: Complete, WITH_DATA (31)]</b> <b>[TCP Segment Len: 878]</b> <b>Sequence Number: 1 (relative sequence number)</b> <b>Sequence Number (raw): 4115465422</b> <b>[Next Sequence Number: 879 (relative sequence number)]</b> <b>Acknowledgment Number: 444 (relative ack number)</b> <b>Acknowledgment number (raw): 3946666314</b> <b>0101 .... = Header Length: 20 bytes (5)</b> <b>&gt; Flags: 0x018 (PSH, ACK)</b> <b>Window: 249</b> <b>[Calculated window size: 31872]</b> <b>[Window size scaling factor: 128]</b> <b>Checksum: 0xc3d8 [unverified]</b> <b>[Checksum Status: Unverified]</b> <b>Urgent Pointer: 0</b> <b>&gt; [Timestamps]</b> <b>&gt; [SEQ/ACK analysis]</b> <b>TCP payload (878 bytes)</b> <b>&gt; Hypertext Transfer Protocol</b> <b>&gt; Line-based text data: text/html (13 lines)</b>						
0000	4c fb 45 66 db 28 c8 7f 54 7b 6f f2					
0010	03 96 bf a1 40 00 2e 06 c7 bd b8					
0020	01 23 00 ff ee b7 f5 4d 04 ce eb 3d					
0030	00 f9 48 a3 00 00 48 54 50 50 2f 31					
0040	30 38 20 4f 6e 2d 69 66 08 74 20 65 3a					
0050	30 38 20 4f 6e 2d 69 66 08 74 20 65 3a					
0060	3a 33 34 3a 30 20 4f 74 20 4f 54 0d 0a					
0070	65 72 3a 20 61 63 68 65 0d 0a 4d 0d 0a					
0080	2d 4d 6f 6a 69 66 69 65 64 3a 20 57					
0090	30 35 20 4d 65 62 20 32 30 31 34 20					
00a0	30 3a 33 31 20 47 4d 54 0d 0a 45 54					
00b0	22 32 38 2d 66 31 66 31 61 65 62 64					
00c0	20 32 38 2d 66 31 66 31 61 65 62 64					
00d0	65 73 3a 20 62 79 74 65 73 0d 0a 43					
00e0	6e 74 2d 4c 65 66 74 68 3a 20 36					
00f0	43 6f 6e 65 63 74 69 6f 6e 3a 20					
0100	65 0d 0a 43 6f 6e 74 65 6e 74 2d 54					
0110	20 74 65 78 74 68 74 66 0d 0a 45 54					
0120	20 74 65 78 74 68 74 66 0d 0a 45 54					
0130	3e 3c 62 6f 64 79 3e 3c 68 65 61 64					
0140	3c 74 69 74 6c 65 3e 68 74 70 70 3a					
0150	66 6f 2e 63 65 72 6e 2e 63 68 3c 2f					
0160	65 3e 0a 3c 2f 68 65 61 64 65 72 3e					
0170	31 3e 68 74 70 3a 2f 2f 69 66 62					
0180	65 3e 0a 3c 2f 68 65 61 64 65 72 3e					
0190	74 68 65 20 66 69 73 74 20 65					
01a0	65 3c 2f 68 31 3e 0a 3c 70 3e 45 72					
01b0	65 72 65 20 79 6f 75 20 63 61 66 3a					
01c0	0a 3c 75 6c 3e 0a 3c 6c 69 3e 3c 6e 61					
01d0	66 3d 22 68 74 70 3a 2f 2f 69 66					
01e0	65 72 6e 2e 63 68 2f 68 79 70 65 72					
01f0	65 72 6e 2e 63 68 2f 68 79 70 65 72					
0200	68 74 6d 6c 22 3e 42 72 6f 77 73 65					
0210	20 66 69 72 73 74 20 77 65 72 69 69					
0220	61 3e 3c 2f 6c 69 3e 0a 3c 6c 69 3e					
0230	72 65 66 3d 22 68 74 70 70 3a 2f 2f					
0240	2d 6d 64 65 2e 63 65 72 6e 2e 63					
0250	77 2f 68 79 70 65 72 6e 2e 63					
<b>Hypertext Transfer Protocol: Protocol</b>						
Пакеты: 711 - Отображено: 6 (0.8%)						
Профиль: Default						

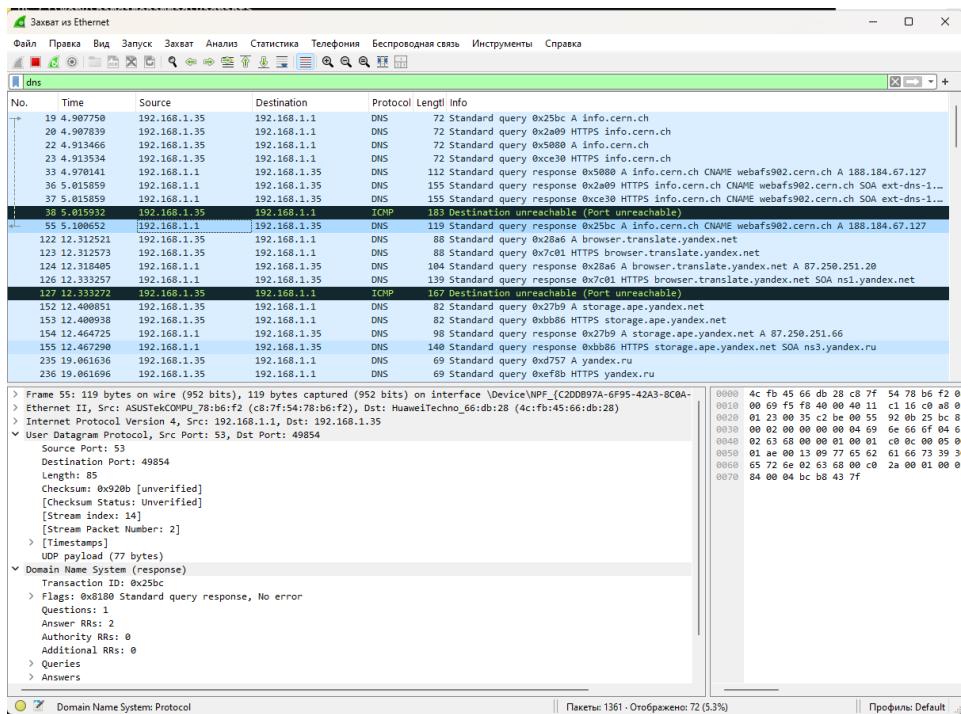
## Пояснение:

- Запрос отправляется с порта **61111** клиента (192.168.1.35) на порт **80** сервера (188.184.67.127).

- Используется протокол **Ethernet II → IPv4 → TCP → HTTP**.
- В TCP-сегменте указывается **Sequence Number** и **Acknowledgment Number**, обеспечивающие надёжную доставку данных.
- В кадре видно передачу **HTTP GET-запроса** и ответ **HTTP/1.1 200 OK** с HTML-страницей.

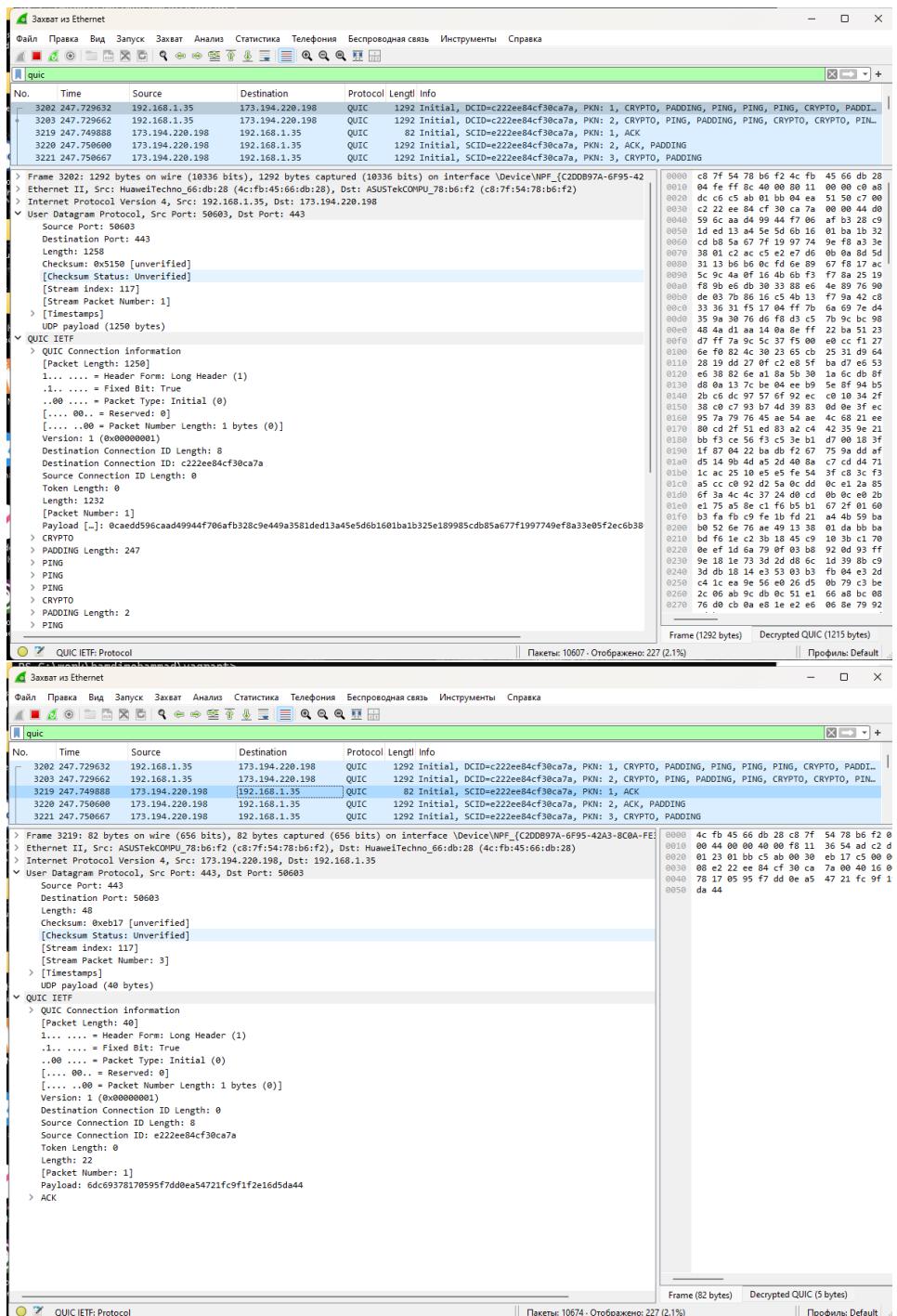
4. В Wireshark применён фильтр dns. Зафиксированы запросы и ответы по протоколу **DNS**, работающему поверх **UDP**.





### Пояснение:

- Запрос отправляется с порта **49854** клиента (192.168.1.35) на порт **53** сервера (192.168.1.1).
  - Пример: запрос имени **info.cern.ch** с типом записи **A**.
  - В ответ сервер возвращает IP-адрес **188.184.67.127**, что подтверждает успешное разрешение имени.
  - Используется структура: **Ethernet II → IPv4 → UDP → DNS**.
5. В Wireshark применён фильтр **quic**. Зафиксирован обмен трафиком по протоколу **QUIC**, работающему поверх **UDP**.



### Пояснение:

- Источник: клиент **192.168.1.35**, назначение: сервер **173.194.220.198**, порт **443**.

- Используется протокол: **Ethernet II → IPv4 → UDP → QUIC**.

## 2.3 Анализ handshake протокола TCP в Wireshark

- В программе **Wireshark** был запущен захват трафика на активном сетевом интерфейсе.
- Для генерации TCP-трафика было выполнено соединение с веб-сервером по протоколу **HTTP**.
- В Wireshark зафиксирован процесс установления TCP-сессии (трёхстороннее рукопожатие).

18 3.580515	192.168.1.35	192.168.1.1	DNS	72 Standard query 0xba41 HTTPS info.cern.ch
19 3.581124	192.168.1.35	188.184.67.127	HTTP	609 GET / HTTP/1.1
20 3.635289	188.184.67.127	192.168.1.35	TCP	60 80 → 61229 [ACK] Seq=1 Ack=556 Win=249 Len=0
21 3.636939	188.184.67.127	192.168.1.35	HTTP	258 HTTP/1.1 304 Not Modified
22 3.636973	188.184.67.127	192.168.1.35	TCP	60 80 → 61229 [FIN, ACK] Seq=197 Ack=556 Win=249 Len=0
23 3.636994	192.168.1.35	188.184.67.127	TCP	54 61229 → 80 [ACK] Seq=556 Ack=198 Win=1025 Len=0
24 3.637253	192.168.1.35	188.184.67.127	TCP	54 61229 → 80 [FIN, ACK] Seq=556 Ack=198 Win=1025 Len=0
25 3.647228	192.168.1.35	87.250.251.20	TLSv1.2	24 Application Data
26 3.647254	192.168.1.35	87.250.251.20	TLSv1.2	358 Application Data
27 3.655770	87.250.251.20	192.168.1.35	TCP	60 443 → 61182 [ACK] Seq=1 Ack=196 Win=166 Len=0
28 3.655770	87.250.251.20	192.168.1.35	TCP	60 443 → 61182 [ACK] Seq=1 Ack=500 Win=165 Len=0
29 3.656358	87.250.251.20	192.168.1.35	TLSv1.2	96 Application Data
30 3.658028	87.250.251.20	192.168.1.35	TLSv1.2	633 Application Data
31 3.658028	188.184.67.127	192.168.1.35	TCP	60 80 → 61229 [ACK] Seq=198 Ack=557 Win=249 Len=0
32 3.688107	192.168.1.35	87.250.251.20	TCP	54 61182 → 443 [ACK] Seq=500 Ack=622 Win=1019 Len=0
33 3.688797	192.168.1.35	87.250.251.20	TLSv1.2	96 Application Data
34 3.721314	192.168.1.1	192.168.1.35	DNS	155 Standard query response 0xba41 HTTPS info.cern.ch CNAME webafs902.cern.ch 50A ex
35 3.748820	87.250.251.20	109.168.1.46	TCP	60 443 → 61182 [ACK] Seq=557 Ack=557 Win=1025 Len=0

Рис. 2.5: Анализ TCP-сессии

### Этапы установления соединения:

- SYN:** клиент (192.168.1.35) отправляет на сервер (188.184.67.127) запрос на установление соединения с флагом SYN и начальным номером последовательности (**Seq = 1**).
- SYN + ACK:** сервер отвечает подтверждением с флагами SYN и ACK, устанавливая свой номер последовательности (**Seq = 1**) и подтверждая получение данных клиента (**Ack = 2**).
- ACK:** клиент подтверждает получение пакета от сервера, устанавливая **Ack = 2**.

После этого соединение считается установленным, и возможна передача данных (HTTP-запрос/ответ).

#### 4. Для анализа был построен **график потока** (Flow Graph) в Wireshark.

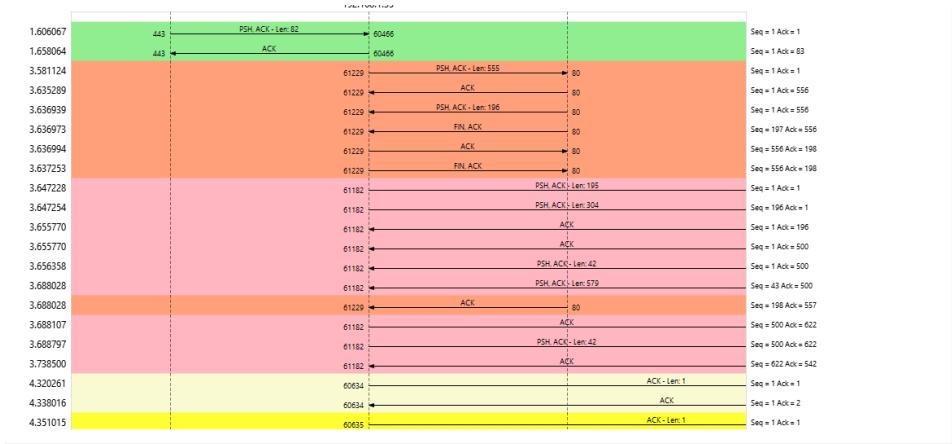


Рис. 2.6: График потока TCP

#### Пояснение к графику:

- На графике наглядно отображены все этапы TCP-взаимодействия.
- Видно трёхстороннее рукопожатие (SYN → SYN+ACK → ACK).
- После установления соединения фиксируется передача данных (HTTP GET, ответы сервера, обмен ACK).
- Завершение соединения происходит с помощью пакетов **FIN, ACK**, что также отражено на графике.

#### 5. После анализа захват трафика в Wireshark был остановлен.

## 3 Заключение

В ходе работы был проведён анализ установления соединения по протоколу **TCP** с использованием программы **Wireshark**.

Было зафиксировано трёхстороннее рукопожатие ( $\text{SYN} \rightarrow \text{SYN+ACK} \rightarrow \text{ACK}$ ), подтверждающее успешное начало TCP-сессии.

С помощью графика потока были проанализированы этапы установления и завершения соединения, а также последующая передача данных.