

# Отчет по лабораторной работе № 3

Анализ трафика в Wireshark

---

Бызова Мария Олеговна

2025-09-05



# 1 Цель работы

---

Целью данной работы является изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

## 2 MAC-адресация

С помощью команды `ipconfig` выведем информацию о текущем сетевом соединении (рис. 1)

```
C:\Windows\system32> ipconfig

Настройка протокола IP для Windows

Неизвестный адаптер Подключение по локальной сети:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер Ethernet Ethernet:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер Ethernet Ethernet 2:
```

**Рисунок 1:** Вывод информации о текущем сетевом соединении.

Теперь используем разные опции команды (рис. 2 - 5)

## 4 MAC-адресация

```
C:\Windows\system32> ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : DESKTOP-UR4UATB
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . : rudn.ru

Неизвестный адаптер Подключение по локальной сети:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : TAP-Windows Adapter V9 for OpenVPN Connect
Физический адрес. . . . . : 00-FF-AD-94-98-8E
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да

Адаптер Ethernet Ethernet:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Intel(R) Ethernet Connection (16) I219-LM
Физический адрес. . . . . : A0-36-BC-6B-61-DE
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да

Адаптер Ethernet Ethernet 2:
```

Рисунок 2: Отображение полной конфигурации TCP/IP для всех адаптеров.

```
C:\Windows\system32> ipconfig /displaydns

Настройка протокола IP для Windows

array622.prod.do.dsp.mp.microsoft.com
-----
Имя записи. . . . . : array622.prod.do.dsp.mp.microsoft.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 647
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 72.145.35.117
```

**Рисунок 3:** Отображение содержимого кэша сопоставителя DNS-клиента, включающее как записи, предварительно загруженные из локального файла Hosts, так и все недавно полученные записи ресурсов для запросов имен, разрешенных компьютером.

```
C:\Windows\system32> ipconfig /registerdns  
Настройка протокола IP для Windows  
Начата регистрация записей ресурсов DNS для всех адаптеров этого компьютера. Отчет об ошибках будет выведен в окне "Просмотр событий" через 15 минут.  
C:\Windows\system32>
```

**Рисунок 4:** Инициализация динамической регистрации вручную для DNS-имен и IP-адресов, настроенных на компьютере



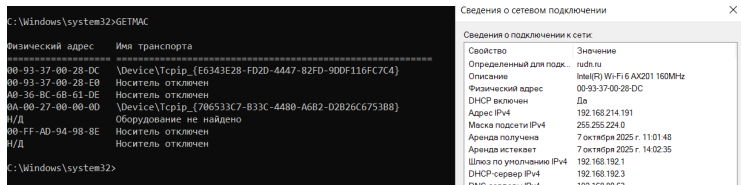
## 7 MAC-адресация

```
C:\Windows\system32> ipconfig /showclassid *  
  
Настройка протокола IP для Windows  
  
Не удастся изменить код класса DHCPv4 для адаптера Подключение по локальной сети: Не удастся найти указанный файл.  
  
Не удастся изменить код класса DHCPv4 для адаптера Ethernet: Не удастся найти указанный файл.  
  
Нет классов DHCPv4, определенных для Ethernet 2.  
Не удастся изменить код класса DHCPv4 для адаптера OpenVPN Connect DCO Adapter: Не удастся найти указанный файл.  
  
Не удастся изменить код класса DHCPv4 для адаптера Подключение по локальной сети* 9: Не удастся найти указанный файл.  
Не удастся изменить код класса DHCPv4 для адаптера Подключение по локальной сети* 10: Не удастся найти указанный файл.  
  
Нет классов DHCPv4, определенных для Беспроводная сеть.  
Не удастся изменить код класса DHCPv4 для адаптера Сетевое подключение Bluetooth: Не удастся найти указанный файл.  
  
Не удастся изменить код класса DHCPv4 для адаптера Loopback Pseudo-Interface 1: Не удастся найти указанный файл.  
  
C:\Windows\system32>
```

**Рисунок 5:** Отображение идентификатора класса DHCP для указанного адаптера.

## 8 MAC-адресация

Определим MAC-адреса сетевых интерфейсов на нашем компьютере с помощью команды GETMAC (рис. 6)

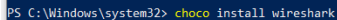


**Рисунок 6:** Определение MAC-адреса сетевых интерфейсов на нашем компьютере.

## 9 Анализ кадров канального уровня в Wireshark

---

Установим на нашем устройстве Wireshark (рис. 7)

A screenshot of a Windows command prompt window with a dark blue background. The text is white. It shows the command 'choco install wireshark' being entered at the prompt 'PS C:\Windows\system32>'.

```
PS C:\Windows\system32> choco install wireshark
```

**Рисунок 7:** Установка на нашем устройстве Wireshark.

# 10 Анализ кадров канального уровня в Wireshark

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика (рис. 8)

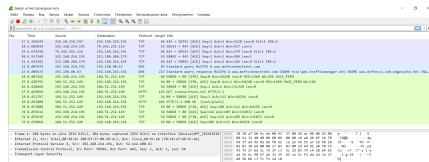


Рисунок 8: Запуск Wireshark. Выбор активного сетевого интерфейса.

## 11 Анализ кадров канального уровня в Wireshark

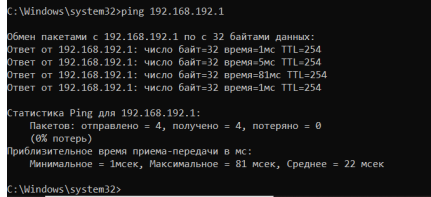
На нашем устройстве в консоли определим с помощью команды `ipconfig` IP-адрес устройства и шлюз по умолчанию (рис. 9)

```
Адаптер беспроводной локальной сети Беспроводная сеть:  
  
DNS-суффикс подключения . . . . . : rudn.ru  
Локальный IPv6-адрес канала . . . : fe80::c19f:aa15:e013:b32e%23  
IPv4-адрес. . . . . : 192.168.214.191  
Маска подсети . . . . . : 255.255.224.0  
Основной шлюз. . . . . : 192.168.192.1  
  
Адаптер Ethernet Сетевое подключение Bluetooth:
```

**Рисунок 9:** Определение IP-адреса устройства и шлюза по умолчанию.

## 12 Анализ кадров канального уровня в Wireshark

На нашем устройстве в консоли с помощью команды ping пропингуем шлюз по умолчанию (рис. 10)



```
C:\Windows\system32>ping 192.168.192.1

Обмен пакетами с 192.168.192.1 по 32 байтами данных:
Ответ от 192.168.192.1: число байт=32 время=1мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=5мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=81мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=1мс TTL=254

Статистика Ping для 192.168.192.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
            (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 81 мсек, Среднее = 22 мсек

C:\Windows\system32>
```

**Рисунок 10:** Пинг шлюза по умолчанию.

## 13 Анализ кадров канального уровня в Wireshark

---

В Wireshark остановим захват трафика. В строке фильтра пропишем фильтр `arp or icmp` и убедимся, что в списке пакетов отобразились только пакеты ARP или ICMP, в частности пакеты, которые были сгенерированы с помощью команды `ping`, отправленной с нашего устройства на шлюз по умолчанию (рис. 11)

# 14 Анализ кадров канального уровня в Wireshark

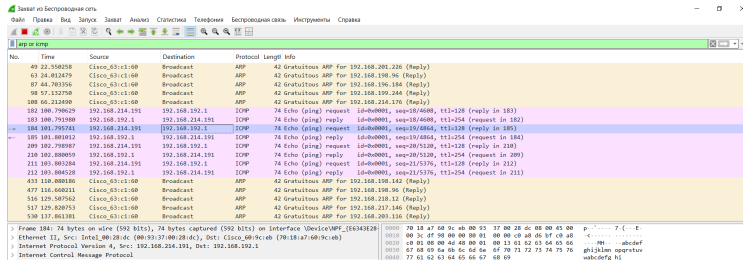


Рисунок 11: Остановка захвата трафика. Фильтр arp or icmp.



## 15 Анализ кадров канального уровня в Wireshark

---

Изучим эхо-запрос и эхо-ответ ICMP в программе Wireshark (рис. 12 - 13)

# 16 Анализ кадров канального уровня в Wireshark

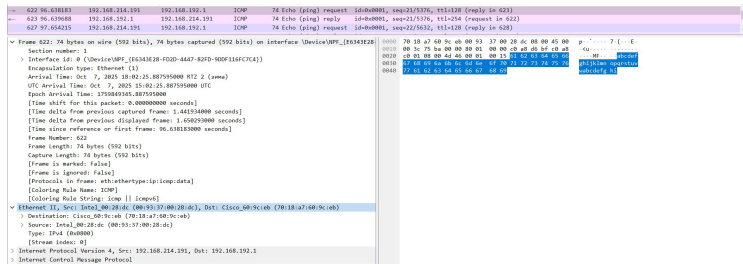


Рисунок 12: Кадр ICMP — эхо-запрос.

# 17 Анализ кадров канального уровня в Wireshark

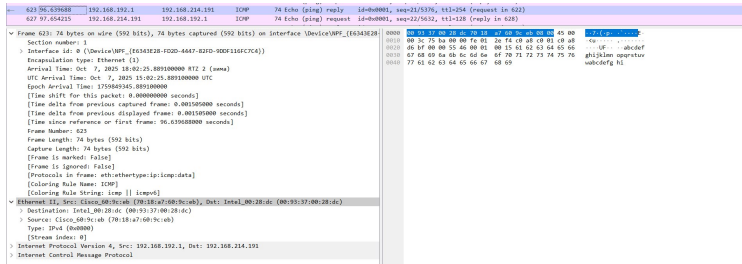
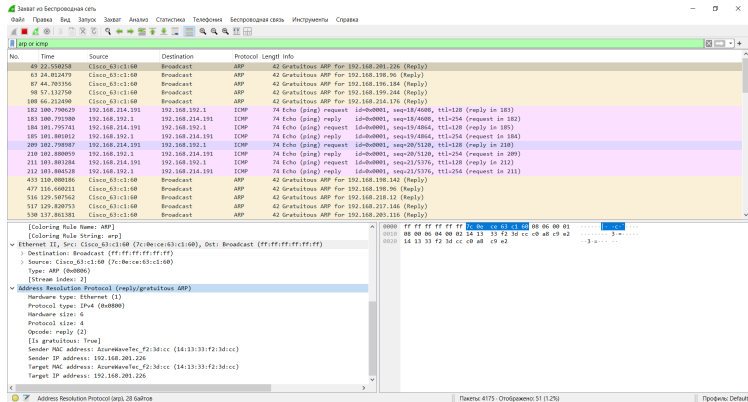


Рисунок 13: Кадр ICMP — эхо-ответ.

Изучим кадры данных протокола ARP и данные в полях заголовка Ethernet II (рис. 14)

# 19 Анализ кадров канального уровня в Wireshark



**Рисунок 14:** Изучение кадров данных протокола ARP и данных в полях заголовка Ethernet II.

## 20 Анализ кадров канального уровня в Wireshark

Начнём новый процесс захвата трафика в Wireshark. На нашем устройстве в консоли пропингуем по имени адрес ping vk.com (рис. 15)

```
C:\Users\Vladimir>ping vk.com

Обмен пакетами с vk.com [87.240.132.78] с 32 байтами данных:
Ответ от 87.240.132.78: число байт=32 время=11мс TTL=53
Ответ от 87.240.132.78: число байт=32 время=11мс TTL=53
Ответ от 87.240.132.78: число байт=32 время=78мс TTL=53
Ответ от 87.240.132.78: число байт=32 время=13мс TTL=53

Статистика Ping для 87.240.132.78:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 11мсек, Максимальное = 78 мсек, Среднее = 35 мсек

C:\Users\Vladimir>
```

**Рисунок 15:** Пингуем по имени адрес vk.com.

## 21 Анализ кадров канального уровня в Wireshark

---

В Wireshark остановим захват трафика. Изучим запросы и ответы протоколов ARP и ICMP (рис. 16 - 17)

# 22 Анализ кадров канального уровня в Wireshark

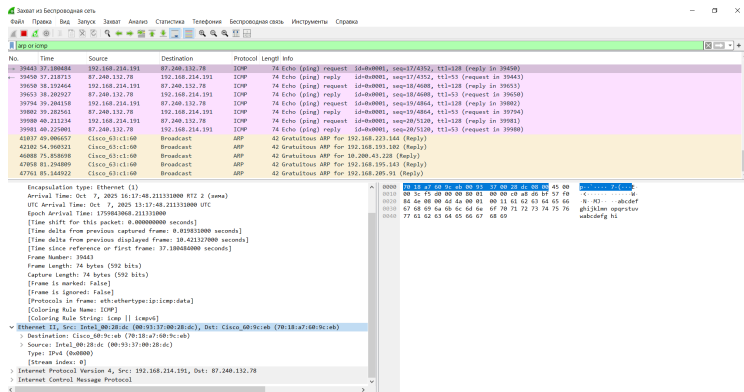


Рисунок 16: Кадр ICMP — эхо-запрос.



# 23 Анализ кадров канального уровня в Wireshark

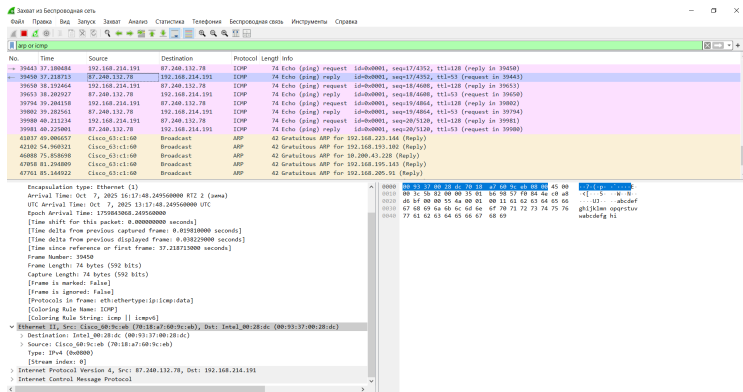


Рисунок 17: Кадр ICMP — эхо-ответ.

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика (рис. 18)

# 25 Анализ протоколов транспортного уровня в Wireshark

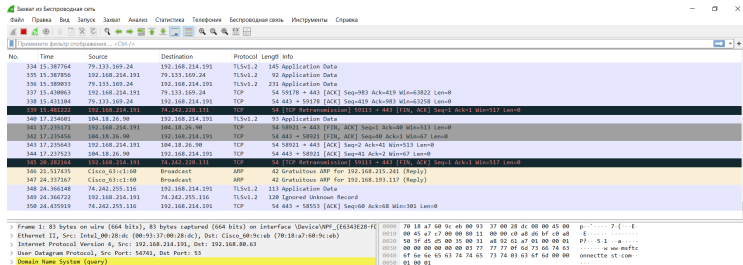
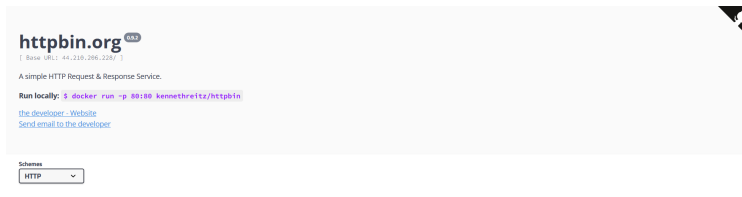


Рисунок 18: Запуск Wireshark. Выбор активного сетевого интерфейса.

## 26 Анализ протоколов транспортного уровня в Wireshark

На устройстве в браузере перейдём на сайт, работающий по протоколу HTTP (<http://httpbin.org/>) и поперемещаемся по ссылкам и разделам сайта в браузере (рис. 19)



**Рисунок 19:** Открытие в браузере сайта

В Wireshark в строке фильтра укажем http и проанализируем информацию по протоколу TCP в случае запросов и ответов (рис. 20 - 21)

# 28 Анализ протоколов транспортного уровня в Wireshark

42622.645.840375	10.193.235.206	44.210.206.228	HTTP	504 GET / HTTP/1.1
42713.646.287639	10.193.235.206	44.210.206.228	HTTP	420 GET /?flagger-static/swagger-ui.css HTTP/1.1
▼ Frame 42622: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on Interface 0 (Device\NPF_{E6...})				
Section number: 1				
Interface id: 0 (Device\NPF_{E6343E28-F02D-4647-82FD-90DF116FC7C4})				
Encapsulation type: Ethernet (1)				
Arrival Time: Oct 7, 2025 14:45:12.986063000 RTT 2 (www)				
UTC Arrival Time: Oct 7, 2025 11:45:11.986063000 UTC				
Epoch Arrival Time: 1759837512.986063000				
[Time shift for this packet: 0.000000000 seconds]				
[Time delta from previous captured frame: 0.001085000 seconds]				
[Time delta from previous displayed frame: 0.003932400 seconds]				
[Time since reference or first frame: 645.840375000 seconds]				
Frame Number: 42622				
Frame Length: 504 bytes (4032 bits)				
Capture Length: 504 bytes (4032 bits)				
[Frame is marked: False]				
[Frame is Ignored: False]				
[Protocols in frame: eth:ethertype:ip:tcp:http]				
[Coloring Rule Name: HTTP]				
[Coloring Rule String: http    tcp.port == 80    http2]				
▼ Ethernet II, Src: Intel_00:28:dc: (00:93:37:00:28:dc), Dst: 76:81:8d:19:a6:eb (76:81:8d:19:a6:eb)				
Destination: 76:81:8d:19:a6:eb (76:81:8d:19:a6:eb)				
Source: Intel_00:28:dc: (00:93:37:00:28:dc)				
Type: IPv4 (0x0800)				
[Stream index: 0]				
▼ Internet Protocol Version 4, Src: 10.193.235.206, Dst: 44.210.206.228				
Transmission Control Protocol, Src Port: 50906, Dst Port: 80, Seq: 1, Ack: 1, Len: 450				
▼ Hypertext Transfer Protocol				

Рисунок 20: Анализ информации по протоколу TCP

# 29 Анализ протоколов транспортного уровня в Wireshark

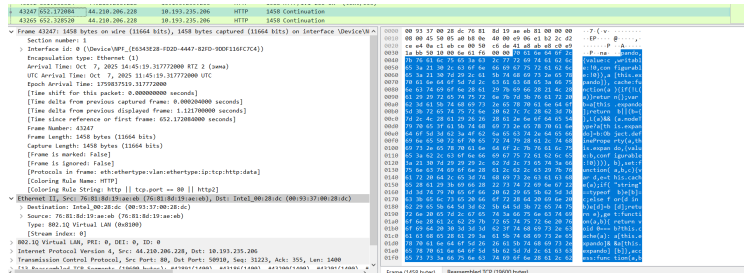


Рисунок 21: Анализ информации по протоколу TCP

В Wireshark в строке фильтра укажем dns и проанализируем информацию по протоколу UDP в случае запросов и ответов (рис. 22 - 23)



# 31 Анализ протоколов транспортного уровня в Wireshark

1573 48.451452	192.168.214.191	192.168.80.63	DNS	71 Standard query 0x0004 A httpbin.org
1575 48.459616	192.168.80.63	192.168.214.191	DNS	167 Standard query response 0x0004 A httpbin.org A 3.221.229.78 A 34.236.61.135 A 54.234.120.160 A 35.170.234.92 A 44.210.206.228 A 100...
▼ Frame 1573: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on Interface \Device\NPF_{E6343E28-10D2-4447-82F0-900F116FC7C4}				
Section number: 1				
> Interface id: 0 (\Device\NPF_{E6343E28-10D2-4447-82F0-900F116FC7C4})				
Encapsulation type: Ethernet (1)				
Arrival Time: Oct 7, 2025 15:03:17.694898000 RTZ 2 (sma)				
UTC Arrival Time: Oct 7, 2025 12:05:17.694898000 UTC				
Tpcsh Arrival Time: 1759538557.694898000				
[Time shift for this packet: 0.000000000 seconds]				
[Time delta from previous captured frame: 0.000306000 seconds]				
[Time delta from previous displayed frame: 0.000106000 seconds]				
[Time since reference or first frame: 48.431452000 seconds]				
Frame Number: 1573				
Frame Length: 71 bytes (568 bits)				
Capture Length: 71 bytes (568 bits)				
[Frame is marked: False]				
[Frame is ignored: False]				
[Protocols in frame: eth:ethertype:ip:udp:dns]				
[Coloring Rule Name: UDP]				
[Coloring Rule String: udp]				
▼ Ethernet II, Src: Intel_00:28:dc (00:93:37:00:28:dc), Dst: Cisco_60:9c:eb (70:18:a7:60:9c:eb)				
> Destination: Cisco_60:9c:eb (70:18:a7:60:9c:eb)				
> Source: Intel_00:28:dc (00:93:37:00:28:dc)				
Type: IPv4 (0x0800)				
[Stream index: 0]				
> Internet Protocol Version 4, Src: 192.168.214.191, Dst: 192.168.80.63				
> User Datagram Protocol, Src Port: 65251, Dst Port: 53				
> Domain Name System (query)				
0000	70 18 a7 60 9c eb 00 93	37 00 28 dc 08 00 45 00	p.....7.(-E-	
0010	00 39 85 cc 00 00 80 11	00 00 c0 a8 d6 bf c0 a8	-9.....	
0020	50 3f fe a5 00 35 00 25	a8 86 00 04 01 00 00 01	PZ...5%.....	
0030	00 00 00 00 00 07 06	74 74 70 62 69 6e 03 6f	.....h httpbin-o	
0040	72 67 00 00 01 00 01		rg.....	

Рисунок 22: Анализ информации по протоколу UDP.

# 32 Анализ протоколов транспортного уровня в Wireshark

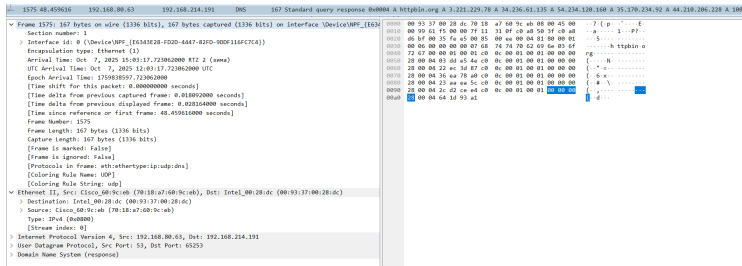


Рисунок 23: Анализ информации по протоколу UDP.

В Wireshark в строке фильтра укажем `quic` и проанализируем информацию по протоколу `quic` в случае запросов и ответов (рис. 24 - 25)

# 34 Анализ протоколов транспортного уровня в Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
58208	984.228996	192.168.214.191	173.194.178.225	QUIC	1292	Initial, DCID=9a57b61af41526c, PN: 1, PADDING, PING, PADDING, CRYPTO, PADDING, PING, PING, PADDING, CRYPTO, CRYPTO
58209	984.228998	192.168.214.191	173.194.178.225	QUIC	1292	Initial, DCID=9a57b61af41526c, PN: 2, CRYPTO, CRYPTO, PADDING, PING, PING, PADDING, PING, PADDING, PING, CRYPTO, CRYPTO, CRYPTO
▼ Frame 58208: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface Device\NPF...						
Section number: 1						
Interface 0: {Device\NPF_{E6343E28-F0D2-4447-82FD-90DF116FC7C4}}						
Encapsulation type: Ethernet (1)						
Arrival Time: Oct 7, 2025 15:26:46.467106000 RTT 2 (sma)						
UTC Arrival Time: Oct 7, 2025 12:26:46.067106000 UTC						
Epoch Arrival Time: 1759840006.467106000						
[Time shift for this packet: 0.000000000 seconds]						
[Time delta from previous captured frame: 0.005750000 seconds]						
[Time delta from previous displayed frame: 0.000000000 seconds]						
[Time since reference or first frame: 984.228996000 seconds]						
Frame Number: 58208						
Frame Length: 1292 bytes (10336 bits)						
Capture Length: 1292 bytes (10336 bits)						
[Frame is marked: False]						
[Frame is ignored: False]						
[Protocols in frame: ethertypesipudpquictls]						
[Coloring Rule Name: UDP]						
[Coloring Rule String: udp]						
▼ Ethernet II, Src: Intel_80:28:dc:00:93:37:00:28:dc, Dst: Cisco_60:9c:eb:78:18:a7:60:9c:eb						
Destination: Cisco_60:9c:eb:78:18:a7:60:9c:eb						
Source: Intel_80:28:dc:00:93:37:00:28:dc						
Type: IPv4 (0x0800)						
(Stream index: 0)						
▼ Internet Protocol Version 4, Src: 192.168.214.191, Dst: 173.194.178.225						
User Datagram Protocol, Src Port: 57781, Dst Port: 443						
▼ QUIC IETF						

Рисунок 24: Анализ информации по протоколу QUIC.

## 35 Анализ протоколов транспортного уровня в Wireshark

```

No.      Time      Source                Destination           Protocol Length Info
-----
58280 984.228896   192.168.214.191      173.194.178.225      QUIC      1292 Initial, DCID=e9a57b61af41526c, PKN: 1, PADDING, PING, PADDING, CRYPTO, PADDING, PING, CRYPTO, PING, PING, PADDING, CRYPTO, CRYPTO
58280 984.228928   192.168.214.191      173.194.178.225      QUIC      1292 Initial, DCID=e9a57b61af41526c, PKN: 2, CRYPTO, CRYPTO, PADDING, PING, PING, PADDING, PING, PADDING, PING, CRYPTO, CRYPTO, CRYPTO, ...
58212 984.230744    173.194.178.225      192.168.214.191      QUIC      82 Initial, SCID=e9a57b61af41526c, PKN: 1, ACK

▼ Frame 58212: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface Device\NPF_{E6143E28-F02D-4447-82F0-90D6116FC7C4}
  Section Number: 1
  > Interface: 0 {\Device\NPF_{E6143E28-F02D-4447-82F0-90D6116FC7C4}}
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct 7, 2025 15:26:46.468954000 RTT 2 {same}
  UTC Arrival Time: Oct 7, 2025 12:26:46.468954000 UTC
  Epoch Arrival Time: 1759840806.468954000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.001764000 seconds]
  [Time delta from previous displayed frame: 0.001816000 seconds]
  [Time since reference or first frame: 504.230744000 seconds]
  Frame Number: 58212
  Frame Length: 82 bytes (656 bits)
  Capture Length: 82 bytes (656 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: ethertype:ip:udp:quic]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]

▼ Ethernet II, Src: Cisco_60:9c:eb (70:1b:a7:60:9c:eb), Dst: Intel_00:28:dc (00:93:37:00:28:dc)
  > Destination: Intel_00:28:dc (00:93:37:00:28:dc)
  > Source: Cisco_60:9c:eb (70:1b:a7:60:9c:eb)
  Type: IPv4 (0x0800)
  [Stream Index: 0]

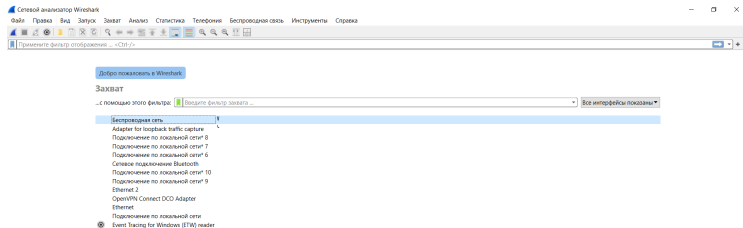
▼ Internet Protocol Version 4, Src: 173.194.178.225, Dst: 192.168.214.191
  > User Datagram Protocol, Src Port: 443, Dst Port: 57781
  > QUIC IETF

```

**Рисунок 25:** Анализ информации по протоколу QUIC.

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика (рис. 26)

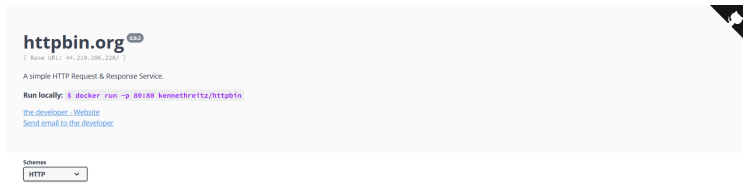
# 37 Анализ handshake протокола TCP в Wireshark



**Рисунок 26:** Запуск Wireshark. Выбор активного сетевого интерфейса.

## 38 Анализ handshake протокола TCP в Wireshark

На устройстве используем соединение по HTTP с сайтом для захвата в Wireshark пакетов TCP (рис. 27)



**Рисунок 27:** Использование соединения по HTTP с сайтом



## 39 Анализ handshake протокола TCP в Wireshark

---

В Wireshark проанализируем handshake протокола TCP (рис. 28 - 30)

# 40 Анализ handshake протокола TCP в Wireshark

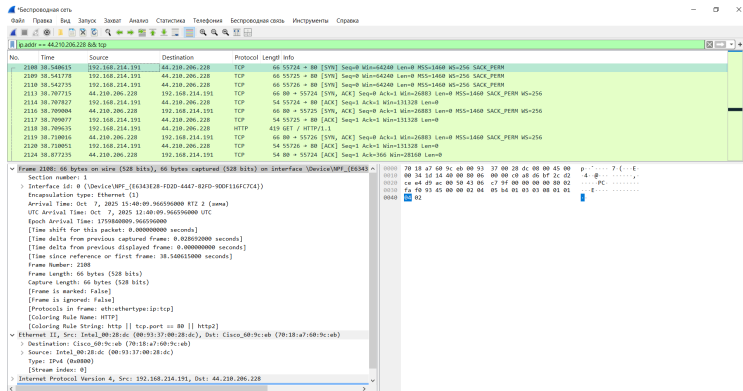


Рисунок 28: Анализ handshake протокола TCP.

# 41 Анализ handshake протокола TCP в Wireshark

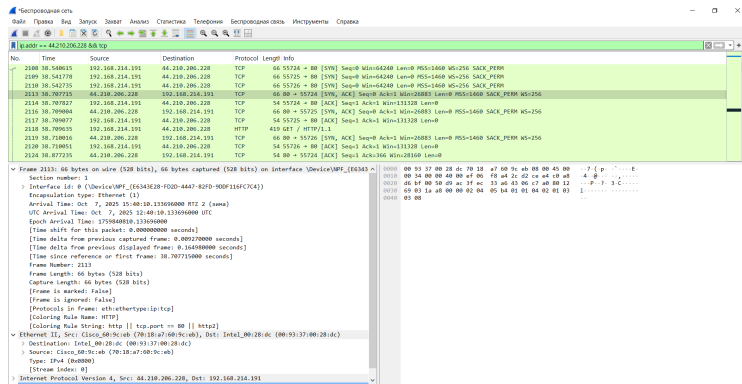


Рисунок 29: Анализ handshake протокола TCP.

# 42 Анализ handshake протокола TCP в Wireshark

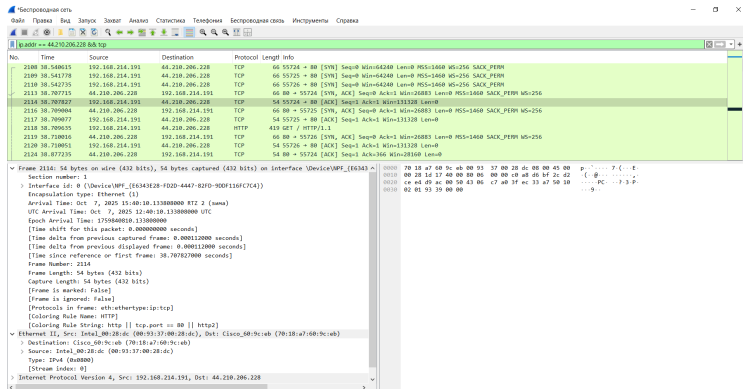


Рисунок 30: Анализ handshake протокола TCP.

В Wireshark в меню «Статистика» выберем «График Потока» (рис. 31)

# 44 Анализ handshake протокола TCP в Wireshark

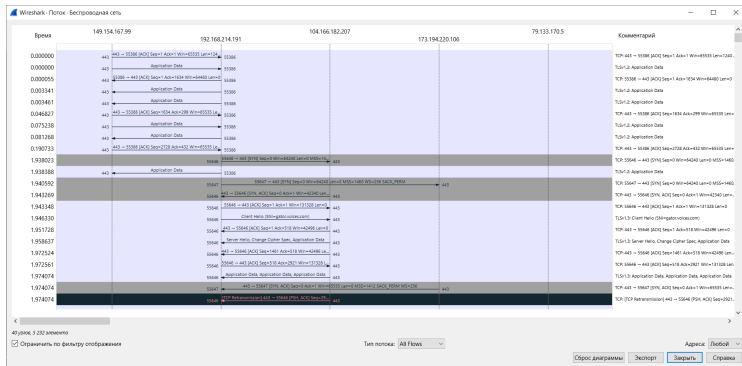


Рисунок 31: График потока.

В ходе выполнения лабораторной работы мы изучили посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.