Лабораторная работа №3

СТУДЕНТ: САХНО НИКИТА

ГРУППА: НФИБД-02-23

Цель работы

Изучить посредством Wireshark кадры Ethernet, проанализировать PDU протоколы транспортного и прикладного уровней стека TCP/IP.

Задание

Изучение возможностей команды ipconfig для ОС типа Windows.

Определение MAC-адреса устройства и его типа.

С помощью Wireshark захватить и проанализировать пакеты ARP и ICMP в части кадров канального уровня.

С помощью Wireshark захватить и проанализировать пакеты HTTP, DNS в части заголовков и информации протоколов TCP, UDP, QUIC.

Выполнение лабораторной работы

```
C:\WINDOWS\system32>ipconfig

Настройка протокола IP для Windows


Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

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

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

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

Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . : beeline
   Локальный IPv6-адрес канала . . . : fe80::4c08:7b9d:d7e4:beba%16
   IPv4-адрес. . . . . . . . . . . . : 192.168.1.72
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . . : 192.168.1.1
```

Выполнение лабораторной работы

```
Настройка протокола IP для Windows

   Имя компьютера  . . . . . . . . . . : DESKTOP-O358DT0
   Основной DNS-суффикс  . . . . . . . :
   Тип узла. . . . . . . . . . . . . . : Гибридный
   IP-маршрутизация включена . . . . . : Нет
   WINS-прокси включен . . . . . . . . : Нет
   Порядок просмотра суффиксов DNS . . : beeline

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

   Состояние среды. . . . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Физический адрес. . . . . . . . . . : 58-96-1D-DC-86-ED
   DHCP включен. . . . . . . . . . . . : Да
   Автонастройка включена. . . . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

   Состояние среды. . . . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Физический адрес. . . . . . . . . . : 5A-96-1D-DC-86-EC
   DHCP включен. . . . . . . . . . . . : Да
   Автонастройка включена. . . . . . . : Да

Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . : beeline
   Описание. . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Физический адрес. . . . . . . . . . : 58-96-1D-DC-86-EC
   DHCP включен. . . . . . . . . . . . : Да
   Автонастройка включена. . . . . . . : Да
```

Выполнение лабораторной работы

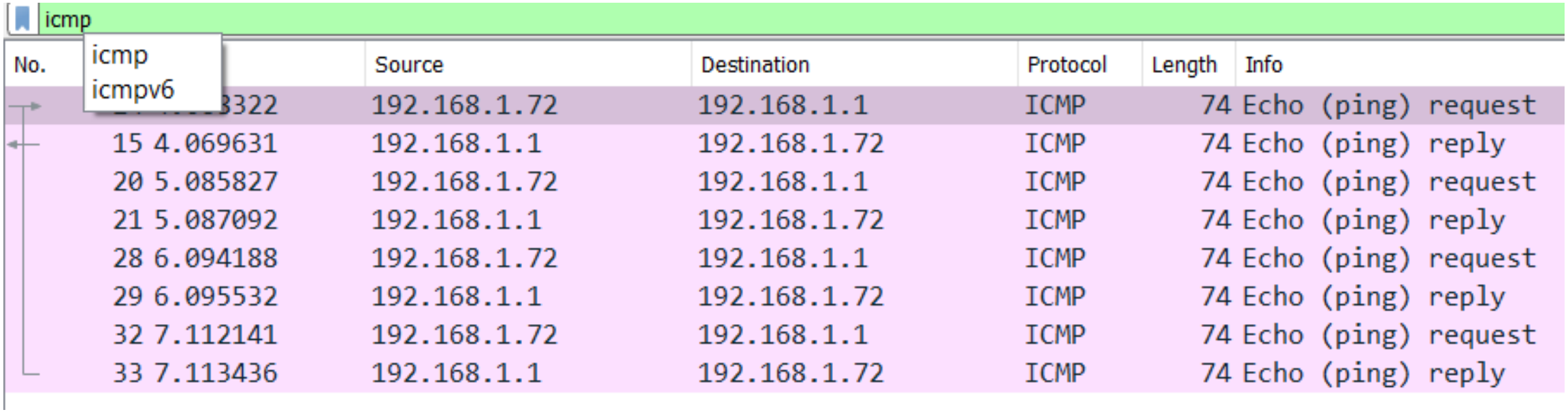
Переводим первый байт в двоичный код 58 = 01011000. Этот адрес является индивидуальным и глобально администрируемым.

```
Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . : beeline
   Описание. . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Физический адрес. . . . . . . . . : 58-96-1D-DC-86-EC
```

Выполнение лабораторной работы

- Берем адрес основного шлюза и пингуем его (предварительно включив захват трафика в Wireshark)

```
C:\WINDOWS\system32>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
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 = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек
```



Выполнение лабораторной работы

Выполнение лабораторной работы

Кадр физического уровня

```
Frame 14: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
    Section number: 1
  > Interface id: 0 (\Device\NPF_{D13C22B7-8811-4040-B55E-62D23A46C914})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 23, 2023 19:39:07.251288000 RTZ 2 (зима)
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1695487147.251288000 seconds
    [Time delta from previous captured frame: 0.565813000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 4.068322000 seconds]
    Frame Number: 14
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: IntelCor_dc:86:ec (58:96:1d:dc:86:ec), Dst: SernetSu_bf:13:f4
```

Кадр канального уровня

```
Ethernet II, Src: IntelCor_dc:86:ec (58:96:1d:dc:86:ec), Dst: SernetSu_bf:13:f4 (58:76:ac:bf:13:f4)
  Destination: SernetSu_bf:13:f4 (58:76:ac:bf:13:f4)
      Address: SernetSu_bf:13:f4 (58:76:ac:bf:13:f4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: IntelCor_dc:86:ec (58:96:1d:dc:86:ec)
      Address: IntelCor_dc:86:ec (58:96:1d:dc:86:ec)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

Выполнение лабораторной работы

arp

No.	Time	Source	Destination	Protocol	Length	Info
198	50.075300	SernetSu_bf:13:f4	Broadcast	ARP	60	Who has 192.16
199	50.075301	SernetSu_bf:13:f4	Broadcast	ARP	60	Who has 192.16
200	50.075301	SernetSu_bf:13:f4	Broadcast	ARP	60	Who has 192.16
201	50.075302	SernetSu_bf:13:f4	Broadcast	ARP	60	Who has 192.16
202	50.075302	SernetSu_bf:13:f4	Broadcast	ARP	60	Who has 192.16
203	50.075303	SernetSu_bf:13:f4	Broadcast	ARP	60	Who has 192.16
204	50.075303	SernetSu_bf:13:f4	Broadcast	ARP	60	Who has 192.16
205	50.075343	IntelCor_dc:86:ec	SernetSu_bf:13:f4	ARP	42	192.168.1.72 i

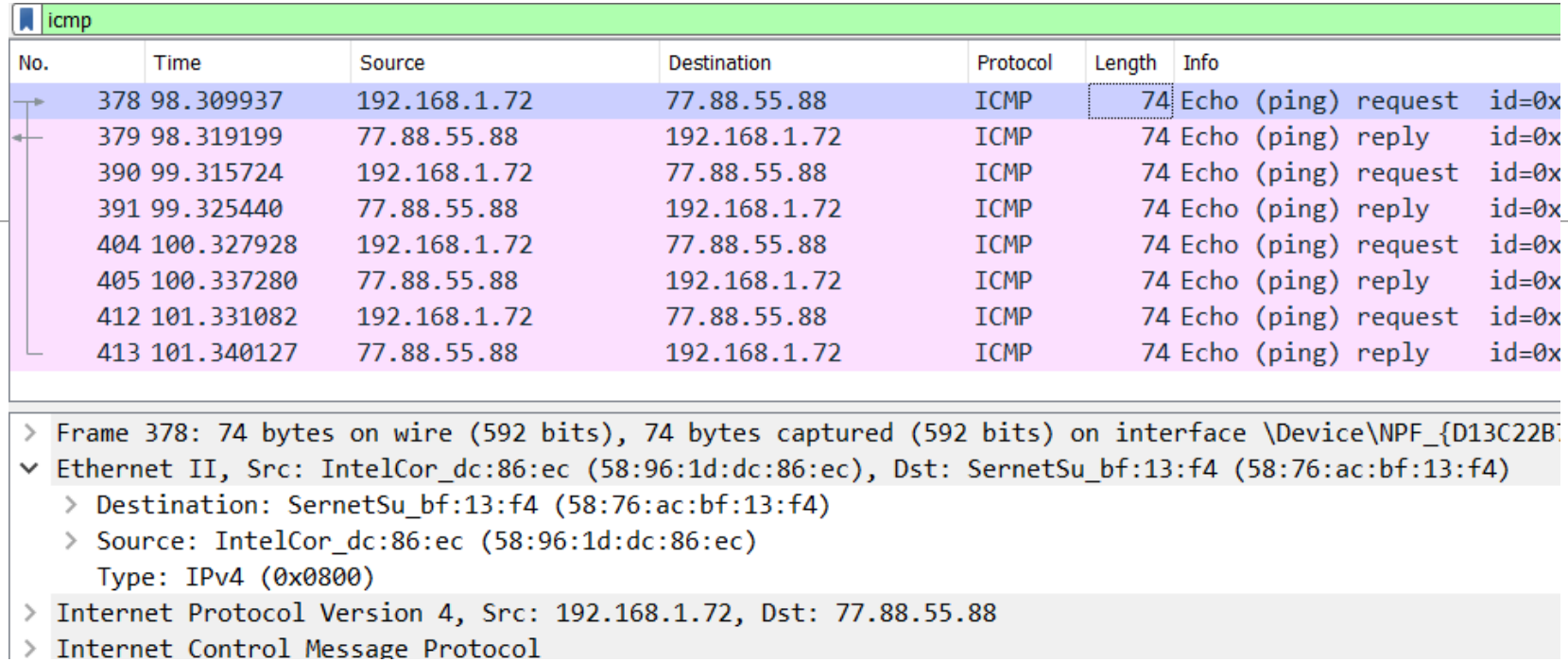
```
> Frame 204: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\
v Ethernet II, Src: SernetSu_bf:13:f4 (58:76:ac:bf:13:f4), Dst: Broadcast (ff:ff:ff:ff:ff:ff
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: SernetSu_bf:13:f4 (58:76:ac:bf:13:f4)
      Type: ARP (0x0806)
      Padding: 000000000000000000000000000000000000
v Address Resolution Protocol (request)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: request (1)
      Sender MAC address: SernetSu_bf:13:f4 (58:76:ac:bf:13:f4)
      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: 192.168.1.103
```

Пропингуем сайт yandex

```
C:\WINDOWS\system32>ping www.yandex.ru

Обмен пакетами с www.yandex.ru [77.88.55.88] с 32 байтами данных:
Ответ от 77.88.55.88: число байт=32 время=9мс TTL=55
Ответ от 77.88.55.88: число байт=32 время=9мс TTL=55
Ответ от 77.88.55.88: число байт=32 время=9мс TTL=55
Ответ от 77.88.55.88: число байт=32 время=9мс TTL=55

Статистика Ping для 77.88.55.88:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 9мсек, Максимальное = 9 мсек, Среднее = 9 мсек

C:\WINDOWS\system32>_
```

Выполнение лабораторной работы

Протокол ICMP



Выполнение лабораторной работы

Протокол TCP (случай запроса)

Выполнение лабораторной работы

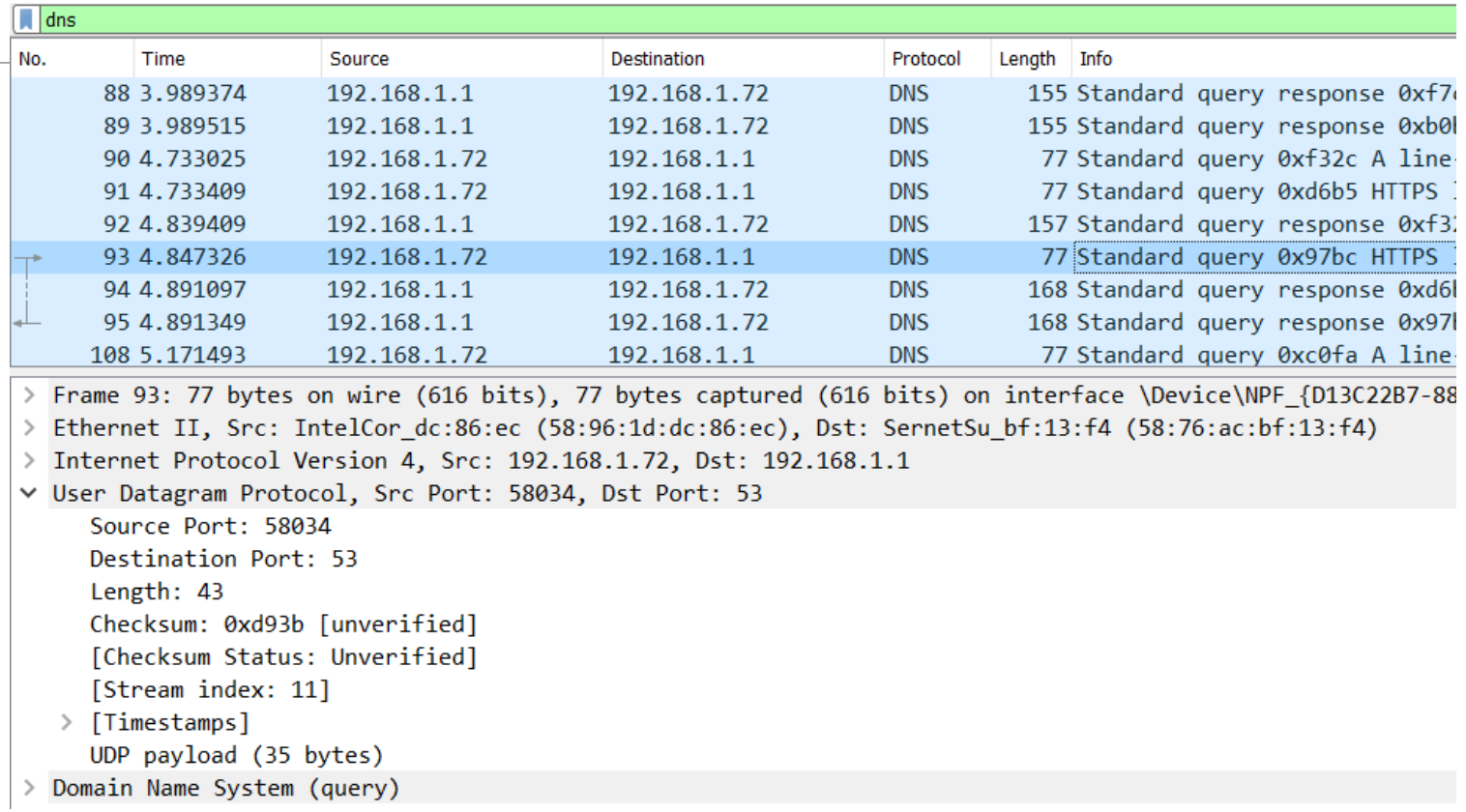
http

No.	Time	Source	Destination	Protocol	Length	Info
104	5.111717	192.168.1.72	188.185.22.9	HTTP	579	GET /www/hypertext/WWW/TheProje
107	5.167733	188.185.22.9	192.168.1.72	HTTP	191	HTTP/1.1 302 Found
172	8.147097	192.168.1.72	188.184.103.21	HTTP	550	GET /about HTTP/1.1
176	8.201340	188.184.103.21	192.168.1.72	HTTP	162	HTTP/1.1 302 Found

```
> Frame 104: 579 bytes on wire (4632 bits), 579 bytes captured (4632 bits) on interface \Device\NPF_{D13C22B7-
> Ethernet II, Src: IntelCor_dc:86:ec (58:96:1d:dc:86:ec), Dst: SernetSu_bf:13:f4 (58:76:ac:bf:13:f4)
> Internet Protocol Version 4, Src: 192.168.1.72, Dst: 188.185.22.9
v Transmission Control Protocol, Src Port: 50758, Dst Port: 80, Seq: 1, Ack: 1, Len: 525
    Source Port: 50758
    Destination Port: 80
    [Stream index: 4]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 525]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3878750177
    [Next Sequence Number: 526    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3157049948
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0xbc55 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (525 bytes)
```

Протокол UDP (случай запроса)

Выполнение лабораторной работы



Выполнение лабораторной работы

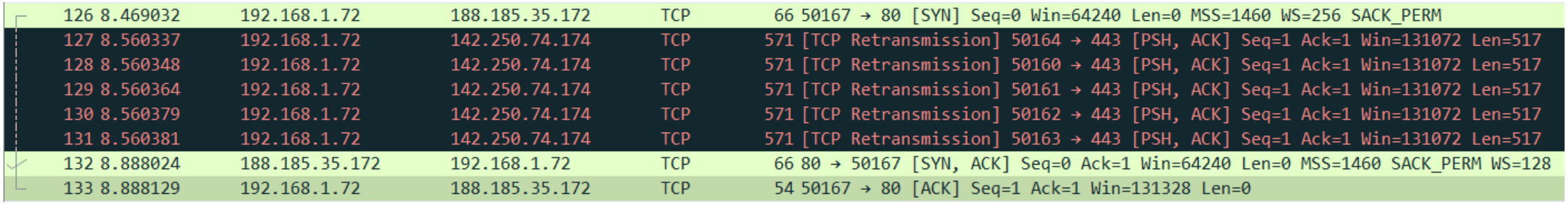
Запрос quic

quic

No.	Time	Source	Destination	Protocol	Length	Info
12	2.441944	192.168.1.72	142.250.74.131	QUIC	1292	Initial, DCID=2604f68
13	2.444788	192.168.1.72	142.250.74.131	QUIC	119	0-RTT, DCID=2604f6824
14	2.464871	142.250.74.131	192.168.1.72	QUIC	1292	Initial, SCID=e604f68
15	2.467843	192.168.1.72	142.250.74.131	QUIC	1292	Initial, DCID=e604f68
16	2.471307	142.250.74.131	192.168.1.72	QUIC	1292	Handshake, SCID=e604f
17	2.471310	142.250.74.131	192.168.1.72	QUIC	1292	Handshake, SCID=e604f
18	2.471311	142.250.74.131	192.168.1.72	QUIC	1292	Handshake, SCID=e604f
19	2.471312	142.250.74.131	192.168.1.72	QUIC	242	Protected Payload (KP
20	2.471545	192.168.1.72	142.250.74.131	QUIC	81	Handshake, DCID=e604f

```
> Frame 12: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\N
> Ethernet II, Src: IntelCor_dc:86:ec (58:96:1d:dc:86:ec), Dst: SernetSu_bf:13:f4 (58:76:ac:bf:13:f4
> Internet Protocol Version 4, Src: 192.168.1.72, Dst: 142.250.74.131
v User Datagram Protocol, Src Port: 64952, Dst Port: 443
    Source Port: 64952
    Destination Port: 443
    Length: 1258
    Checksum: 0xe3f0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 3]
  > [Timestamps]
    UDP payload (1250 bytes)
v QUIC IETF
  v QUIC Connection information
      [Connection Number: 0]
    [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: 2604f6824825e9cb
    Source Connection ID Length: 0
    Token Length: 70
    Token: 004630e0538a5bdbca09c1fec23d67ffb83eb6e46d704e12e134463c0b3a5aed1cff2023…
    Length: 1161
    Packet Number: 1
    Payload: df06381fab53acd6636b311f8881fc04761bc282b9fc6735746908f8dce3f7db2bc4619a…
```

Handshake TCP



126	8.469032	192.168.1.72	188.185.35.172	TCP	66 50167 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
127	8.560337	192.168.1.72	142.250.74.174	TCP	571 [TCP Retransmission] 50164 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131072 Len=517
128	8.560348	192.168.1.72	142.250.74.174	TCP	571 [TCP Retransmission] 50160 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131072 Len=517
129	8.560364	192.168.1.72	142.250.74.174	TCP	571 [TCP Retransmission] 50161 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131072 Len=517
130	8.560379	192.168.1.72	142.250.74.174	TCP	571 [TCP Retransmission] 50162 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131072 Len=517
131	8.560381	192.168.1.72	142.250.74.174	TCP	571 [TCP Retransmission] 50163 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131072 Len=517
132	8.888024	188.185.35.172	192.168.1.72	TCP	66 80 → 50167 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
133	8.888129	192.168.1.72	188.185.35.172	TCP	54 50167 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0

Выполнение лабораторной работы

Протокол TCP для первой ступени handshake

```
Sequence Number: 0    (relative sequence number)
Sequence Number (raw): 848625695
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 .... = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
```

Протокол TCP для второй ступени handshake

```
Sequence Number: 0    (relative sequence number)
Sequence Number (raw): 2149321476
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 848625696
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
```

Протокол TCP для третьей ступени handshake

```
Sequence Number: 1    (relative sequence number)
Sequence Number (raw): 848625696
[Next Sequence Number: 1    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 2149321477
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
```

График потока

Выполнение лабораторной работы

Выводы

В процессе выполнения данной лабораторной работы я изучил посредством Wireshark кадры Ethernet, проанализировал PDU протоколы транспортного и прикладного уровней стека TCP/IP.