ЛАБОРАТОРНАЯ РАБОТА №3

Студент: Талебу Тенке Франк Устон

Группа: НФИбд-02-23

ЦЕЛЬ РАБОТЫ

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

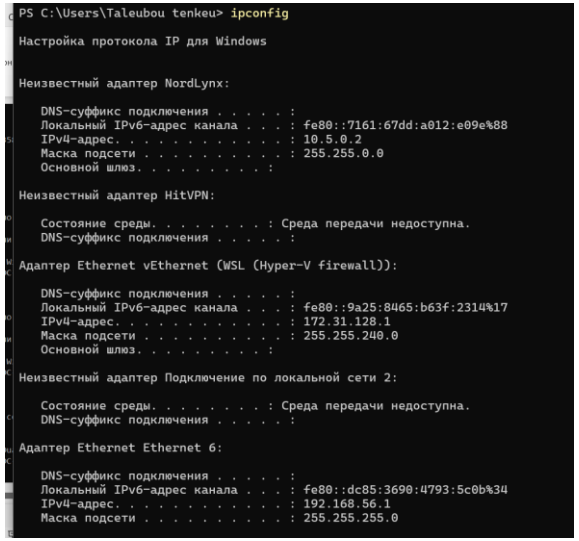
ЗАДАНИЕ

- 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

```
Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

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

Адаптер Ethernet Ethernet 8:

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

Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . : rudn.ru
   Локальный IPv6-адрес канала . . . : fe80::f505:9056:79e9:894%20
   IPv4-адрес. . . . . . . . . . . . : 192.168.205.147
   Маска подсети . . . . . . . . . . : 255.255.224.0
   Основной шлюз. . . . . . . . . . : 192.168.192.1

Адаптер Ethernet Ethernet:
```

ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ



```
PS C:\Users\Taleubou tenkeu> ipconfig

Настройка протокола IP для Windows


Неизвестный адаптер NordLynx:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::7161:67dd:a012:e09e%88
   IPv4-адрес. . . . . . . . . . . . : 10.5.0.2
   Маска подсети . . . . . . . . . . : 255.255.0.0
   Основной шлюз. . . . . . . . . :

Неизвестный адаптер HitVPN:

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

Адаптер Ethernet vEthernet (WSL (Hyper-V firewall)):

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::9a25:8465:b63f:2314%17
   IPv4-адрес. . . . . . . . . . . . : 172.31.128.1
   Маска подсети . . . . . . . . . . : 255.255.240.0
   Основной шлюз. . . . . . . . . :

Неизвестный адаптер Подключение по локальной сети 2:

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

Адаптер Ethernet Ethernet 6:

   DNS-суффикс подключения . . . . . :
   Локальный IPv6-адрес канала . . . : fe80::dc85:3690:4793:5c0b%34
   IPv4-адрес. . . . . . . . . . . . : 192.168.56.1
   Маска подсети . . . . . . . . . . : 255.255.255.0
```

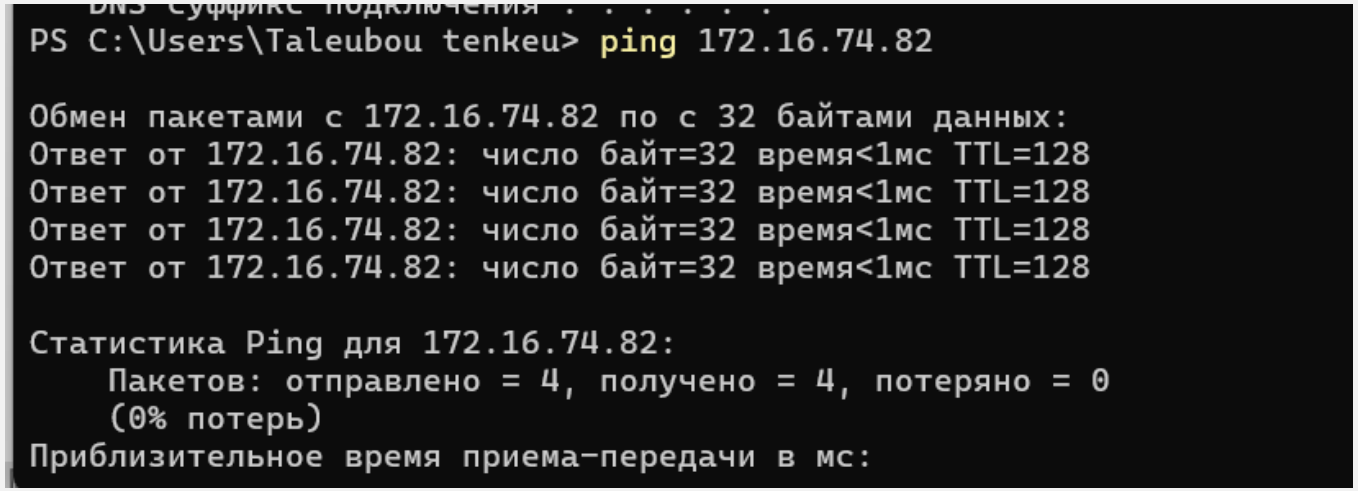
```
Адаптер беспроводной локальной сети Подключение по локальной сети* 2

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

Адаптер Ethernet Ethernet 8:

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

Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . : rudn.ru
   Локальный IPv6-адрес канала . . . : fe80::f505:9056:79e9:894%20
   IPv4-адрес. . . . . . . . . . . . : 192.168.205.147
   Маска подсети . . . . . . . . . . : 255.255.224.0
   Основной шлюз. . . . . . . . . : 192.168.192.1

Адаптер Ethernet Ethernet:

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

ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

```
Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . : rudn.ru
   Локальный IPv6-адрес канала . . . : fe80::f505:9056:79e9:894%20
   IPv4-адрес. . . . . . . . . . . . : 192.168.205.147
   Маска подсети . . . . . . . . . . : 255.255.224.0
   Основной шлюз. . . . . . . . . . : 192.168.192.1
```

ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

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



ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

Кадр физического уровня

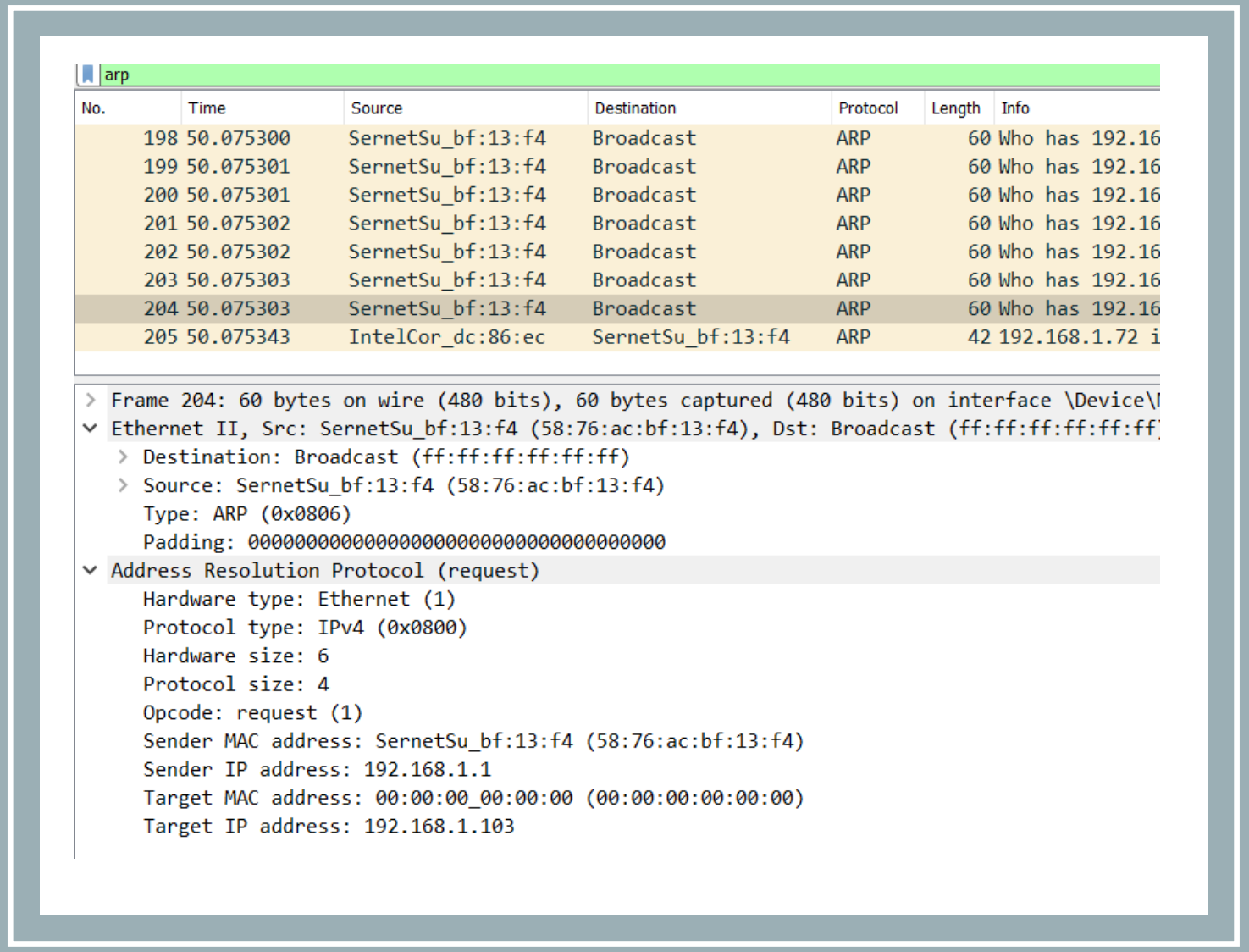
```
Frame 14: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
    Section number: 1
  > Interface id: 0 (\Device\NPF_{D13C22B7-8811-4040-B55E-62D23A46C914})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 23, 2023 19:39:07.251288000 RTZ 2 (зима)
    [Time shift for this 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

Протокол ARP

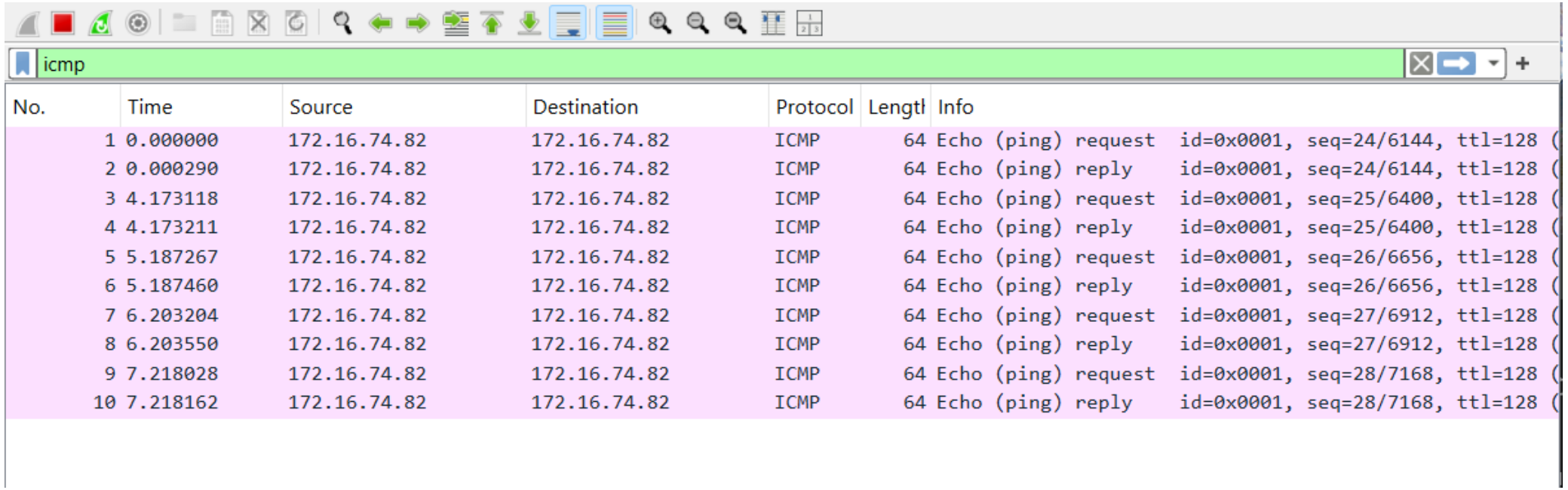


Пропингуем сайт yandex

```
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



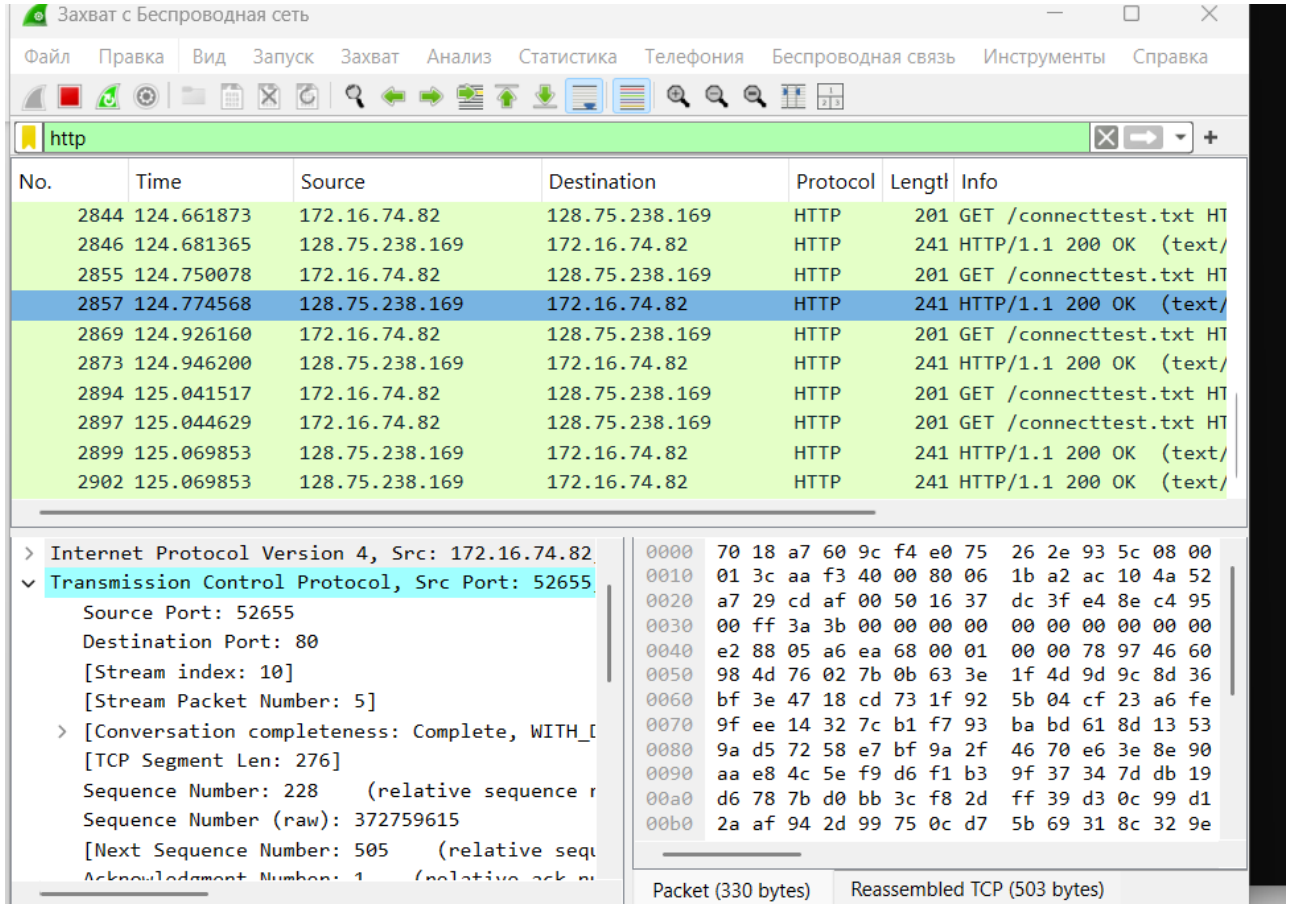
icmp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.74.82	172.16.74.82	ICMP	64	Echo (ping) request id=0x0001, seq=24/6144, ttl=128 (
2	0.000290	172.16.74.82	172.16.74.82	ICMP	64	Echo (ping) reply id=0x0001, seq=24/6144, ttl=128 (
3	4.173118	172.16.74.82	172.16.74.82	ICMP	64	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (
4	4.173211	172.16.74.82	172.16.74.82	ICMP	64	Echo (ping) reply id=0x0001, seq=25/6400, ttl=128 (
5	5.187267	172.16.74.82	172.16.74.82	ICMP	64	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (
6	5.187460	172.16.74.82	172.16.74.82	ICMP	64	Echo (ping) reply id=0x0001, seq=26/6656, ttl=128 (
7	6.203204	172.16.74.82	172.16.74.82	ICMP	64	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (
8	6.203550	172.16.74.82	172.16.74.82	ICMP	64	Echo (ping) reply id=0x0001, seq=27/6912, ttl=128 (
9	7.218028	172.16.74.82	172.16.74.82	ICMP	64	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (
10	7.218162	172.16.74.82	172.16.74.82	ICMP	64	Echo (ping) reply id=0x0001, seq=28/7168, ttl=128 (

ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

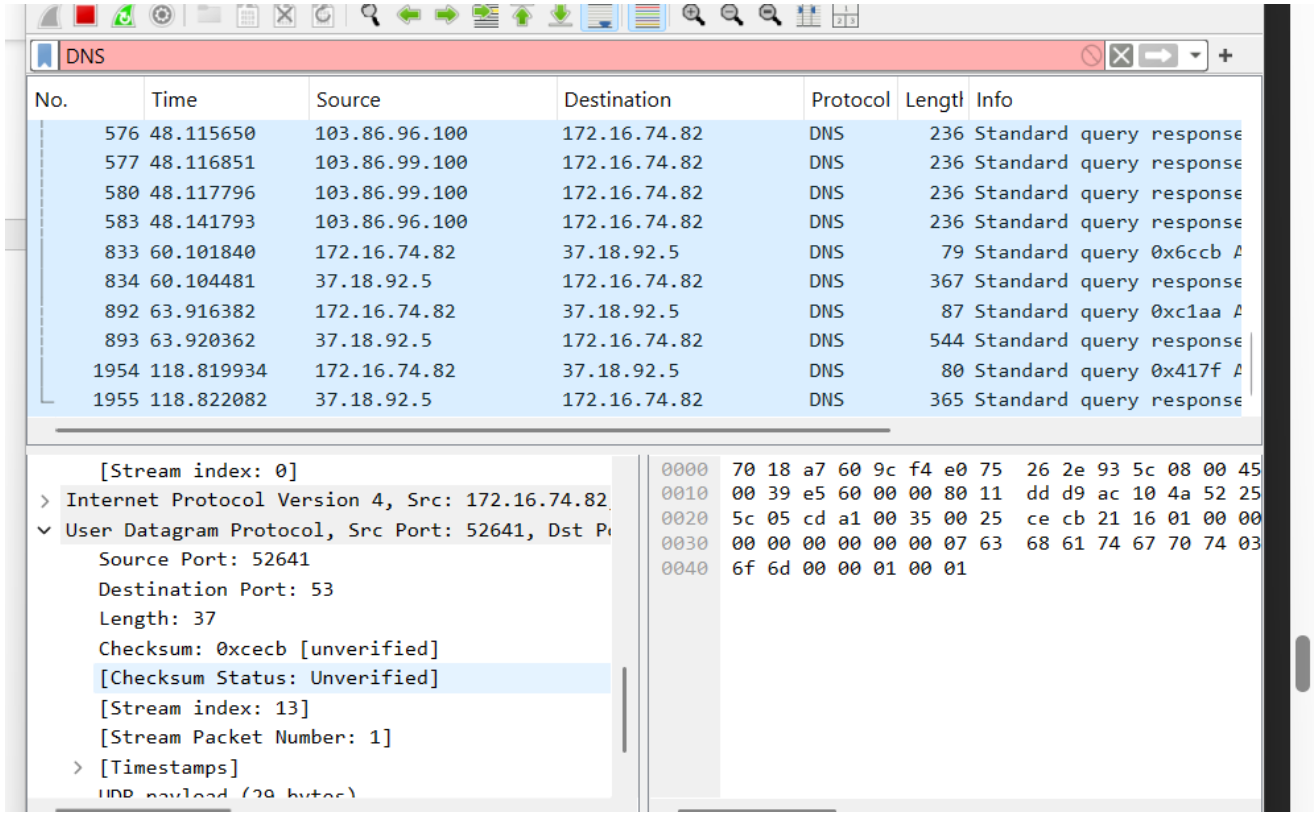
ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

- Протокол TCP (случай запроса)



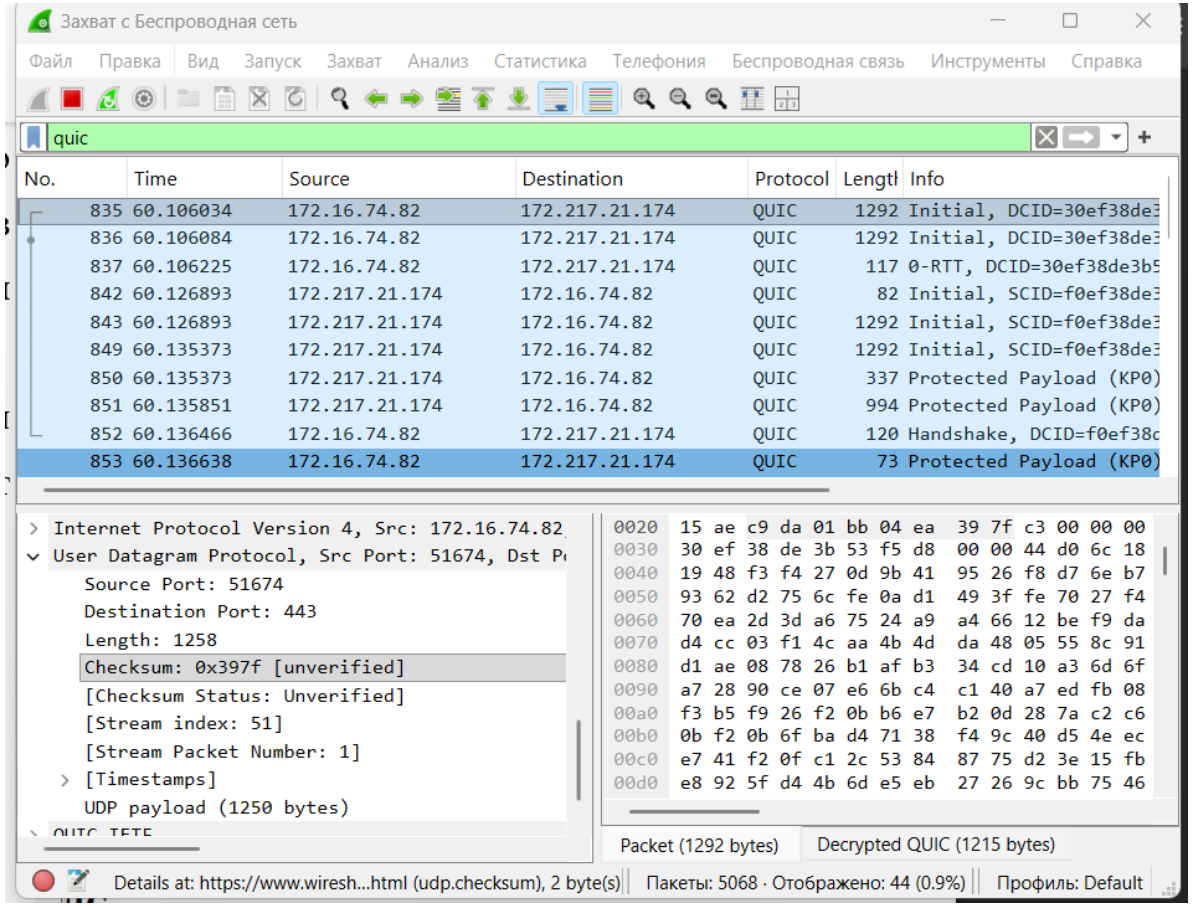
ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

- Протокол UDP (случай запроса)



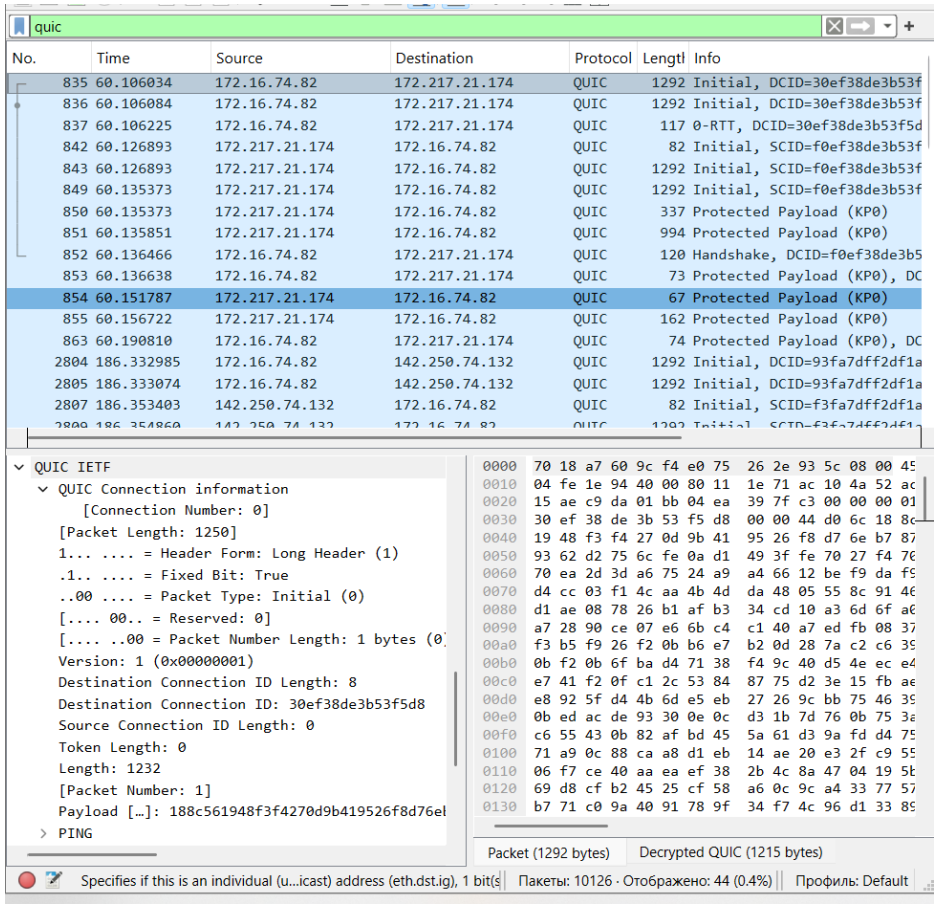
ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

- Запрос quic



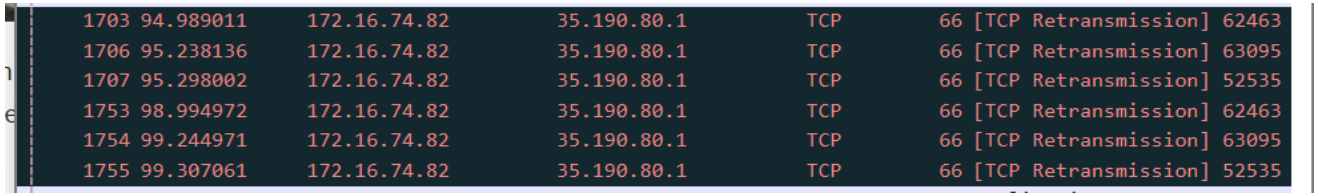
ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

- Запрос quic



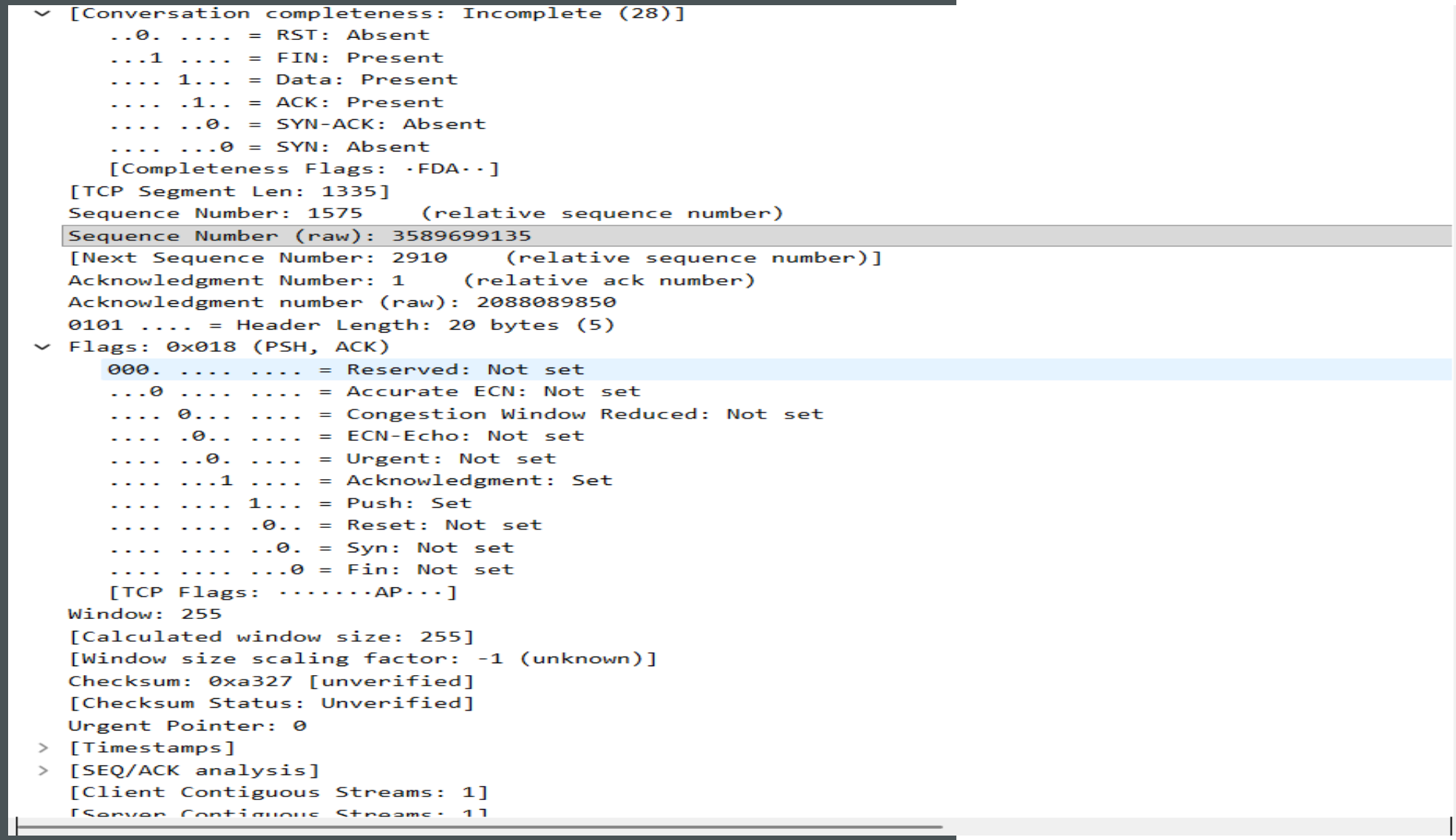
ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

- Handshake TCP



1703	94.989011	172.16.74.82	35.190.80.1	TCP	66 [TCP Retransmission] 62463
1706	95.238136	172.16.74.82	35.190.80.1	TCP	66 [TCP Retransmission] 63095
1707	95.298002	172.16.74.82	35.190.80.1	TCP	66 [TCP Retransmission] 52535
1753	98.994972	172.16.74.82	35.190.80.1	TCP	66 [TCP Retransmission] 62463
1754	99.244971	172.16.74.82	35.190.80.1	TCP	66 [TCP Retransmission] 63095
1755	99.307061	172.16.74.82	35.190.80.1	TCP	66 [TCP Retransmission] 52535

Протокол TCP для первой ступени handshake
Протокол TCP для второй ступени handshake
Протокол TCP для третьей ступени handshake



Протокол TCP для первой ступени handshake

Протокол TCP для второй ступени handshake

Протокол TCP для третьей ступени handshake

```
[Conversation completeness: Incomplete (28)]
    ..0. .... = RST: Absent
    ...1 .... = FIN: Present
    .... 1... = Data: Present
    .... .1.. = ACK: Present
    .... ..0. = SYN-ACK: Absent
    .... ...0 = SYN: Absent
    [Completeness Flags: ·FDA··]
[TCP Segment Len: 1335]
Sequence Number: 1575    (relative sequence number)
Sequence Number (raw): 3589699135
[Next Sequence Number: 2910    (relative sequence number)]
Acknowledgment Number: 1    (relative ack number)
Acknowledgment number (raw): 2088089850
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·····AP···]
Window: 255
[Calculated window size: 255]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xa327 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
[Client Contiguous Streams: 1]
[Server Contiguous Streams: 1]
```

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.