

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:

Адаптер Ethernet Ethernet:

Составные звезды : Среда, первозданные, недоступные

ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

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

Настройка протокола IP для Windows

Неизвестный адаптер NordLynx:

DNS-суффикс подключения . . . . . : fe80::7161:67dd:a012:e09e%88
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 среди. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

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

DNS-суффикс подключения . . . . . : fe80::9a25:8f65:b63f:2314%17
Локальный IPv6-адрес канала . . . . . : fe80::9a25:8f65:b63f:2314%17
IPv4-адрес . . . . . : 172.31.128.1
Маска подсети . . . . . : 255.255.248.0
Основной шлюз. . . . . :

Неизвестный адаптер Подключение по локальной сети 2:

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

Адаптер Ethernet Ethernet 6:

DNS-суффикс подключения . . . . . : fe80::dc85:3690:4793:5c0b%34
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 среди. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :

Адаптер Ethernet Ethernet 8:

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

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : ruds.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 среди. . . . . : 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)

```
PS C:\Users\Taleubou tenkeu> ping 172.16.74.82
```

```
Обмен пакетами с 172.16.74.82 по с 32 байтами данных:  
Ответ от 172.16.74.82: число байт=32 время<1мс TTL=128  
Ответ от 172.16.74.82: число байт=32 время<1мс TTL=128  
Ответ от 172.16.74.82: число байт=32 время<1мс TTL=128  
Ответ от 172.16.74.82: число байт=32 время<1мс TTL=128
```

```
Статистика Ping для 172.16.74.82:
```

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0  
(0% потеря)
```

```
Приблизительное время приема-передачи в мс:
```

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

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\NPF_{...}
▼ 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: 00
▼ 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% потеря)
```

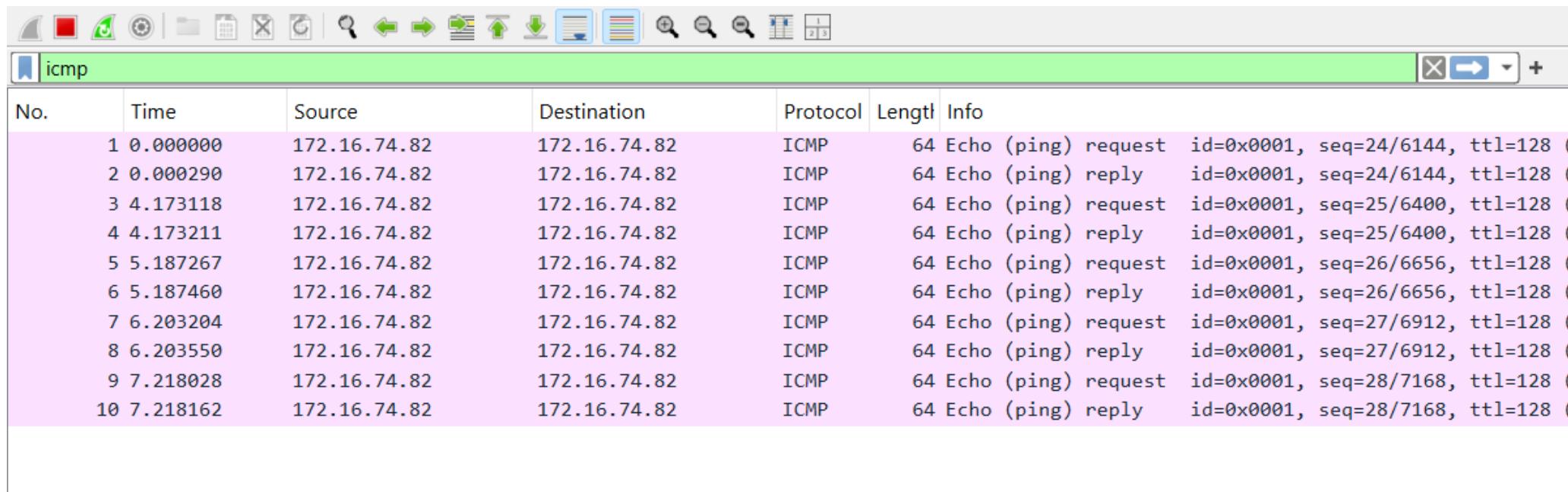
```
Приблизительное время приема-передачи в мс:
```

```
Минимальное = 9мсек, Максимальное = 9 мсек, Среднее = 9 мсек
```

```
C:\WINDOWS\system32>
```

ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

Протокол ICMP



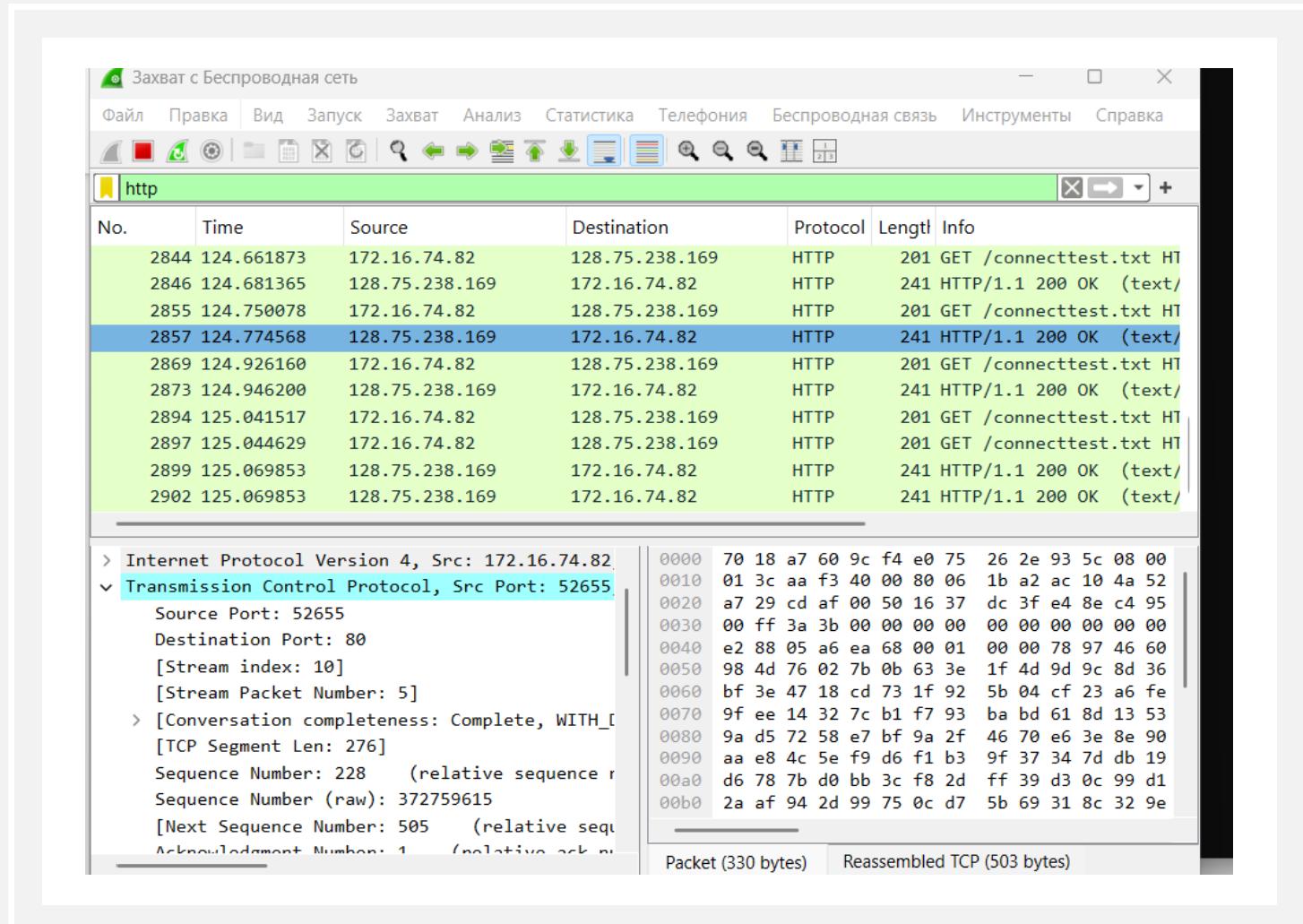
The screenshot shows a packet capture in Wireshark. The title bar says "icmp". The columns are: No., Time, Source, Destination, Protocol, Length, Info. The "Info" column provides detailed information about each ICMP request and reply. The sequence shows a series of Echo requests (ping) from source 172.16.74.82 to destination 172.16.74.82, with corresponding Echo replies. The "Info" column includes fields like id=0x0001, seq=24/6144, ttl=128.

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)

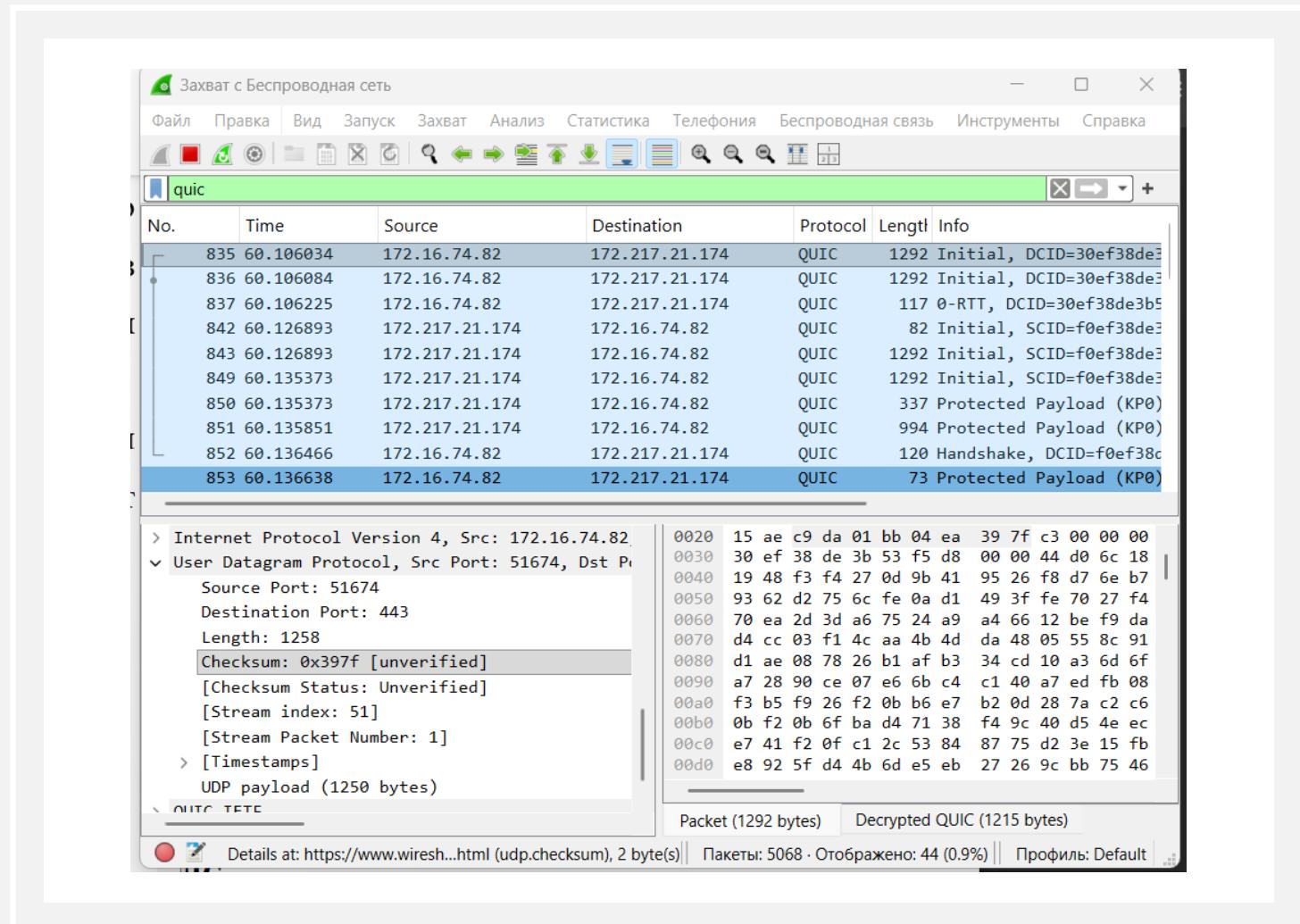
No.	Time	Source	Destination	Protocol	Length	Info
576	48.115650	103.86.96.100	172.16.74.82	DNS	236	Standard query response
577	48.116851	103.86.99.100	172.16.74.82	DNS	236	Standard query response
580	48.117796	103.86.99.100	172.16.74.82	DNS	236	Standard query response
583	48.141793	103.86.96.100	172.16.74.82	DNS	236	Standard query response
833	60.101840	172.16.74.82	37.18.92.5	DNS	79	Standard query 0x6ccb A
834	60.104481	37.18.92.5	172.16.74.82	DNS	367	Standard query response
892	63.916382	172.16.74.82	37.18.92.5	DNS	87	Standard query 0xc1aa A
893	63.920362	37.18.92.5	172.16.74.82	DNS	544	Standard query response
1954	118.819934	172.16.74.82	37.18.92.5	DNS	80	Standard query 0x417f A
1955	118.822082	37.18.92.5	172.16.74.82	DNS	365	Standard query response

[Stream index: 0]
> Internet Protocol Version 4, Src: 172.16.74.82.
 User Datagram Protocol, Src Port: 52641, Dst Port: 53
 Source Port: 52641
 Destination Port: 53
 Length: 37
 Checksum: 0xcecb [unverified]
 [Checksum Status: Unverified]
 [Stream index: 13]
 [Stream Packet Number: 1]
> [Timestamps]
 [UDP payload (29 bytes)]

0000 70 18 a7 60 9c f4 e0 75 26 2e 93 5c 08 00 45
0010 00 39 e5 60 00 00 80 11 dd d9 ac 10 4a 52 25
0020 5c 05 cd a1 00 35 00 25 ce cb 21 16 01 00 00
0030 00 00 00 00 00 00 07 63 68 61 74 67 70 74 03
0040 6f 6d 00 00 01 00 01

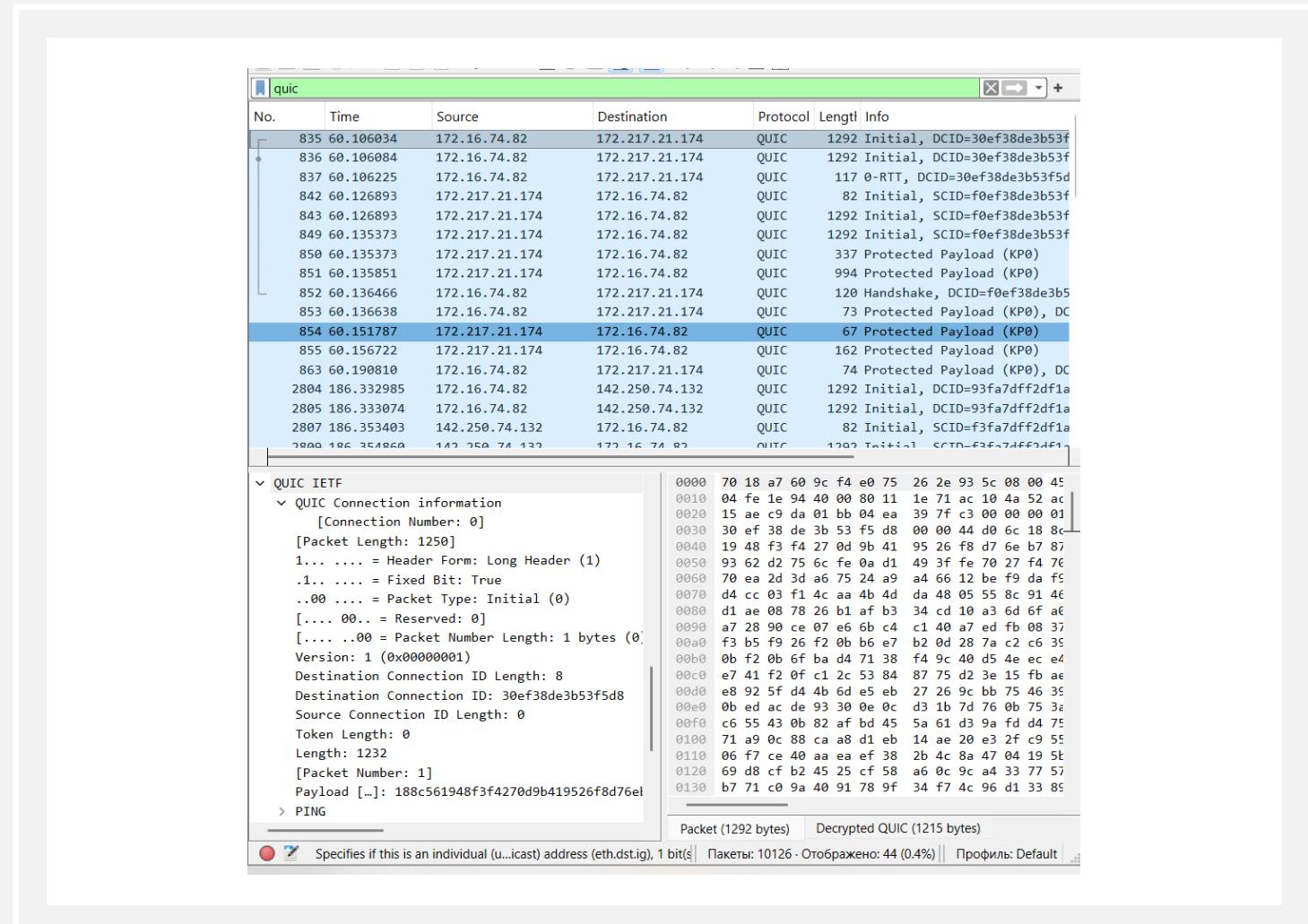
ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

- 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

```
✗ [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]
```

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

50167 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	TCP: 50167 → 80 [SYN] Seq=0 Win=64:
→ 443	TCP: [TCP Retransmission] 50164 → 44:
→ 443	TCP: [TCP Retransmission] 50160 → 44:
→ 443	TCP: [TCP Retransmission] 50161 → 44:
→ 443	TCP: [TCP Retransmission] 50162 → 44:
→ 443	TCP: [TCP Retransmission] 50163 → 44:
80 → 50167 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128	TCP: 80 → 50167 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
50167 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0	TCP: 50167 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0

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.