

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:

Состояние среды. : Среда передачи недоступна.

ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

```
PS C:\Users\Talebou 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 . . . . . : 255.255.248.0
    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)

```
DNS-суффикс подключения . . . . .
PS C:\Users\Taleubou tenkeu> ping 172.16.74.82

Обмен пакетами с 172.16.74.82 по 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% потерь)
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: 00000000000000000000000000000000

▼ 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

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: 00000000000000000000000000000000
- ▼ 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)
```

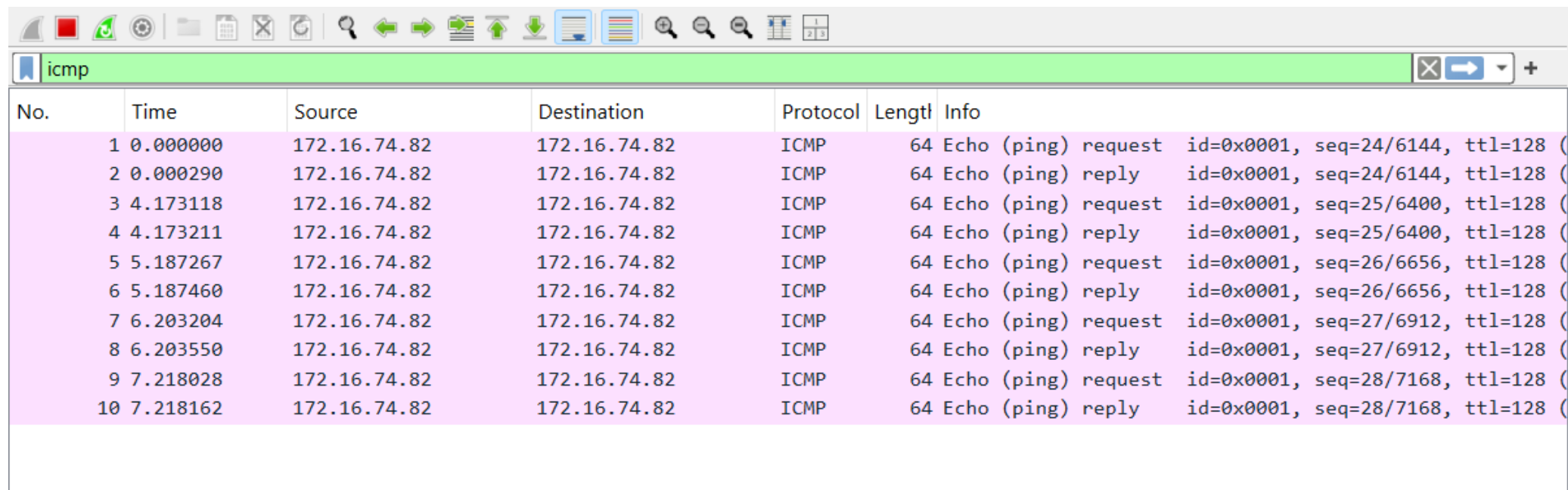
```
Приблизительное время приема-передачи в мс:
```

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

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

ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

Протокол ICMP



The image shows a Wireshark packet capture window for the ICMP protocol. The top toolbar contains various icons for file operations, navigation, and analysis. The packet list pane on the left shows 10 captured packets. The main packet details pane on the right shows the structure of the selected packet (No. 10), including the ICMP Echo (ping) request and reply fields.

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)

Захват с Беспроводная сеть

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

http

No.	Time	Source	Destination	Protocol	Length	Info
2844	124.661873	172.16.74.82	128.75.238.169	HTTP	201	GET /connecttest.txt HT
2846	124.681365	128.75.238.169	172.16.74.82	HTTP	241	HTTP/1.1 200 OK (text/
2855	124.750078	172.16.74.82	128.75.238.169	HTTP	201	GET /connecttest.txt HT
2857	124.774568	128.75.238.169	172.16.74.82	HTTP	241	HTTP/1.1 200 OK (text/
2869	124.926160	172.16.74.82	128.75.238.169	HTTP	201	GET /connecttest.txt HT
2873	124.946200	128.75.238.169	172.16.74.82	HTTP	241	HTTP/1.1 200 OK (text/
2894	125.041517	172.16.74.82	128.75.238.169	HTTP	201	GET /connecttest.txt HT
2897	125.044629	172.16.74.82	128.75.238.169	HTTP	201	GET /connecttest.txt HT
2899	125.069853	128.75.238.169	172.16.74.82	HTTP	241	HTTP/1.1 200 OK (text/
2902	125.069853	128.75.238.169	172.16.74.82	HTTP	241	HTTP/1.1 200 OK (text/

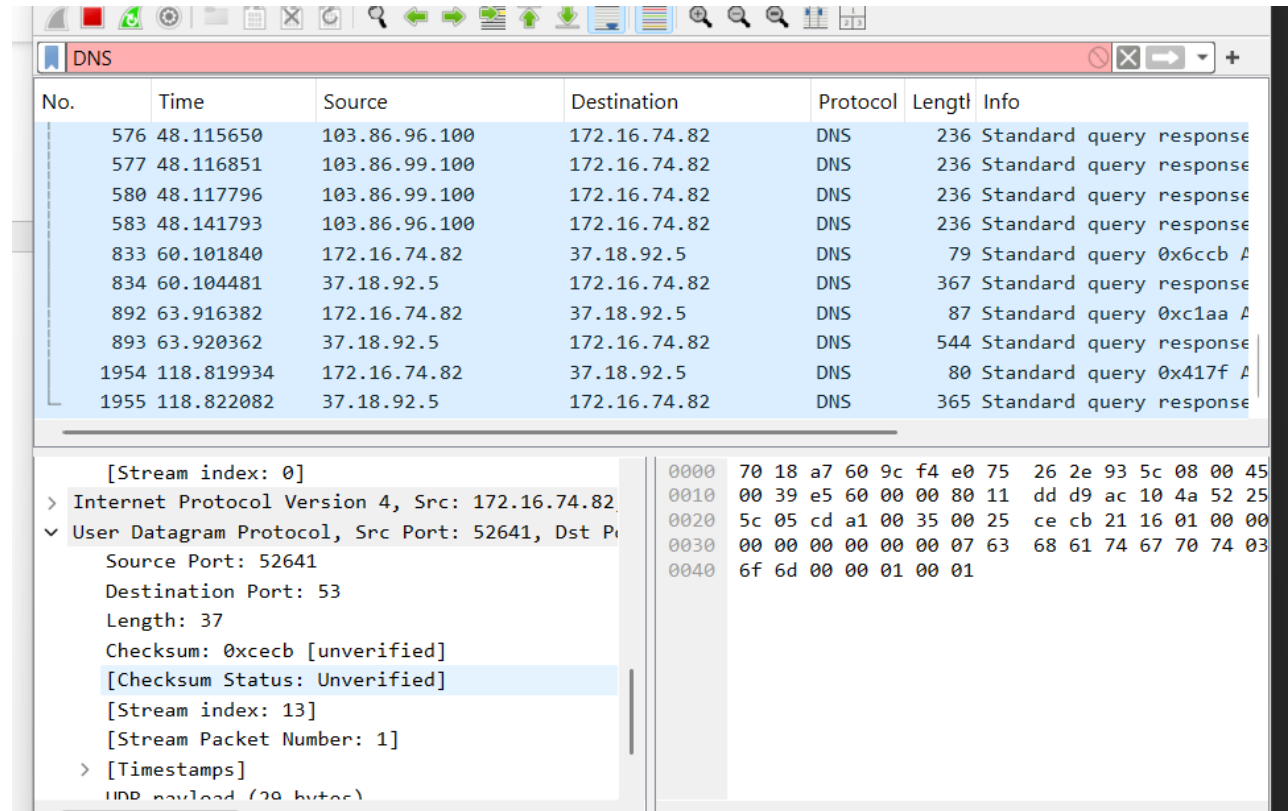
> Internet Protocol Version 4, Src: 172.16.74.82
✓ Transmission Control Protocol, Src Port: 52655
Source Port: 52655
Destination Port: 80
[Stream index: 10]
[Stream Packet Number: 5]
> [Conversation completeness: Complete, WITH_
[TCP Segment Len: 276]
Sequence Number: 228 (relative sequence r
Sequence Number (raw): 372759615
[Next Sequence Number: 505 (relative sequ
Acknowledgment Number: 1 (relative ack n

0000 70 18 a7 60 9c f4 e0 75 26 2e 93 5c 08 00
0010 01 3c aa f3 40 00 80 06 1b a2 ac 10 4a 52
0020 a7 29 cd af 00 50 16 37 dc 3f e4 8e c4 95
0030 00 ff 3a 3b 00 00 00 00 00 00 00 00 00 00
0040 e2 88 05 a6 ea 68 00 01 00 00 78 97 46 60
0050 98 4d 76 02 7b 0b 63 3e 1f 4d 9d 9c 8d 36
0060 bf 3e 47 18 cd 73 1f 92 5b 04 cf 23 a6 fe
0070 9f ee 14 32 7c b1 f7 93 ba bd 61 8d 13 53
0080 9a d5 72 58 e7 bf 9a 2f 46 70 e6 3e 8e 90
0090 aa e8 4c 5e f9 d6 f1 b3 9f 37 34 7d db 19
00a0 d6 78 7b d0 bb 3c f8 2d ff 39 d3 0c 99 d1
00b0 2a af 94 2d 99 75 0c d7 5b 69 31 8c 32 9e

Packet (330 bytes) Reassembled TCP (503 bytes)

ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

- Протокол UDP (случай запроса)



The image shows a Wireshark packet capture of DNS traffic. The top pane displays a list of packets, and the bottom pane shows the details of a selected packet.

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 0xc6cb 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: 0xc6cb [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

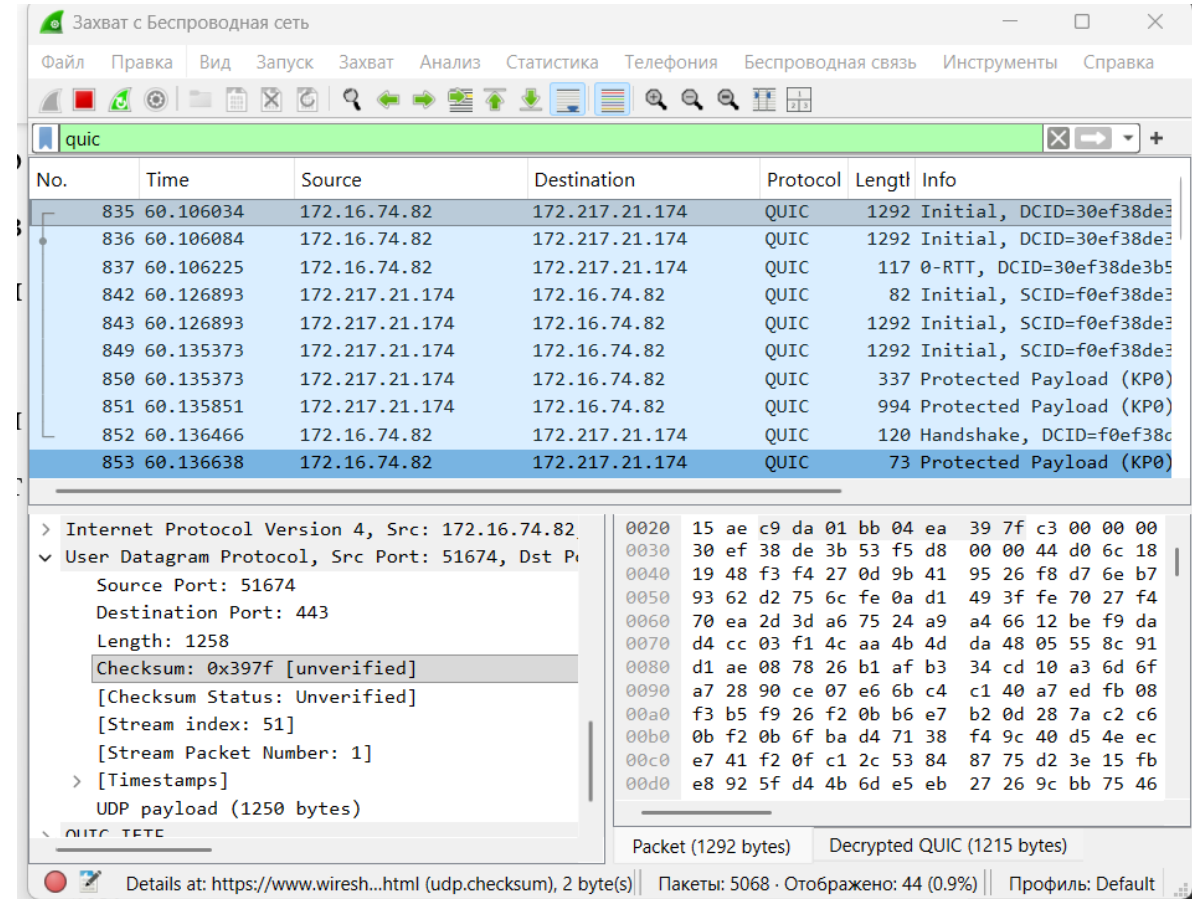
0020 5c 05 cd a1 00 35 00 25 ce cb 21 16 01 00 00

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



The image shows a Wireshark network traffic capture window titled "Захват с Беспроводная сеть". The filter bar shows "quic". The packet list displays several QUIC packets, with packet 853 selected. The packet details pane shows the structure of the selected packet: Internet Protocol Version 4, User Datagram Protocol (Source Port: 51674, Destination Port: 443, Length: 1258, Checksum: 0x397f [unverified]), and QUIC. The packet bytes pane shows the raw data of the packet, which is a QUIC Initial packet (DCID=30ef38de3b53f5d8).

No.	Time	Source	Destination	Protocol	Length	Info
835	60.106034	172.16.74.82	172.217.21.174	QUIC	1292	Initial, DCID=30ef38de3b53f5d8
836	60.106084	172.16.74.82	172.217.21.174	QUIC	1292	Initial, DCID=30ef38de3b53f5d8
837	60.106225	172.16.74.82	172.217.21.174	QUIC	117	0-RTT, DCID=30ef38de3b53f5d8
842	60.126893	172.217.21.174	172.16.74.82	QUIC	82	Initial, SCID=f0ef38de3b53f5d8
843	60.126893	172.217.21.174	172.16.74.82	QUIC	1292	Initial, SCID=f0ef38de3b53f5d8
849	60.135373	172.217.21.174	172.16.74.82	QUIC	1292	Initial, SCID=f0ef38de3b53f5d8
850	60.135373	172.217.21.174	172.16.74.82	QUIC	337	Protected Payload (KP0)
851	60.135851	172.217.21.174	172.16.74.82	QUIC	994	Protected Payload (KP0)
852	60.136466	172.16.74.82	172.217.21.174	QUIC	120	Handshake, DCID=f0ef38de3b53f5d8
853	60.136638	172.16.74.82	172.217.21.174	QUIC	73	Protected Payload (KP0)

Packet details for packet 853:

- Internet Protocol Version 4, Src: 172.16.74.82, Dst: 172.217.21.174
- User Datagram Protocol, Src Port: 51674, Dst Port: 443
 - Source Port: 51674
 - Destination Port: 443
 - Length: 1258
 - Checksum: 0x397f [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 51]
 - [Stream Packet Number: 1]
 - [Timestamps]
 - UDP payload (1250 bytes)
- QUIC

Packet bytes:

0020 15 ae c9 da 01 bb 04 ea 39 7f c3 00 00 00 00 00
0030 30 ef 38 de 3b 53 f5 d8 00 00 44 d0 6c 18 00 00
0040 19 48 f3 f4 27 0d 9b 41 95 26 f8 d7 6e b7 00 00
0050 93 62 d2 75 6c fe 0a d1 49 3f fe 70 27 f4 00 00
0060 70 ea 2d 3d a6 75 24 a9 a4 66 12 be f9 da 00 00
0070 d4 cc 03 f1 4c aa 4b 4d da 48 05 55 8c 91 00 00
0080 d1 ae 08 78 26 b1 af b3 34 cd 10 a3 6d 6f 00 00
0090 a7 28 90 ce 07 e6 6b c4 c1 40 a7 ed fb 08 00 00
00a0 f3 b5 f9 26 f2 0b b6 e7 b2 0d 28 7a c2 c6 00 00
00b0 0b f2 0b 6f ba d4 71 38 f4 9c 40 d5 4e ec 00 00
00c0 e7 41 f2 0f c1 2c 53 84 87 75 d2 3e 15 fb 00 00
00d0 e8 92 5f d4 4b 6d e5 eb 27 26 9c bb 75 46 00 00

Packet (1292 bytes) Decrypted QUIC (1215 bytes)

Details at: <https://www.wireshark.org/html/udp.checksum>, 2 byte(s) Пакеты: 5068 · Отображено: 44 (0.9%) Профиль: Default

ВЫПОЛНЕНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

- Запрос quic

The screenshot displays the Wireshark network protocol analyzer interface. The top pane, titled 'quic', shows a list of captured packets. Packet 854 is selected, showing a QUIC packet from 172.16.74.82 to 172.16.74.82, containing a Protected Payload (KP0).

The bottom-left pane shows the packet details for the selected QUIC packet:

- QUIC IETF
- 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: 30ef38de3b53f5d8
 - Source Connection ID Length: 0
 - Token Length: 0
 - Length: 1232
 - [Packet Number: 1]
 - Payload [...]: 188c561948f3f4270d9b419526f8d76el
- PING

The bottom-right pane shows the raw packet data in hexadecimal and ASCII. The packet is 1292 bytes long, and the decrypted QUIC payload is 1215 bytes.

Packet (1292 bytes) Decrypted QUIC (1215 bytes)

Specifies if this is an individual (unicast) address (eth.dst.ig), 1 bit(s) Пакеты: 10126 · Отображено: 44 (0.4%) Профиль: Default

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]

```

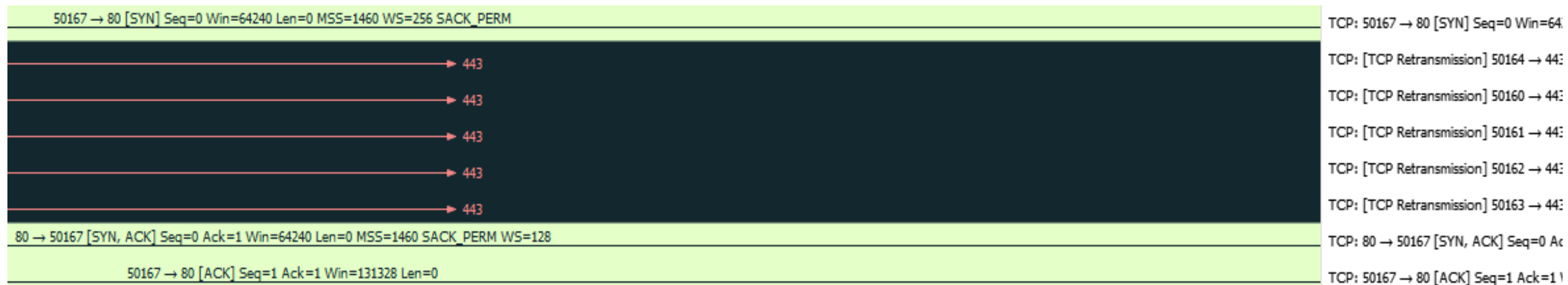
Протокол TCP для первой ступени handshake

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



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.