

# Лабораторная №3

Сетевые технологии - Жибицкая Е.Д.

---

Российский университет дружбы народов, Москва, Россия

Цель

---

- Знакомство с Wireshark, изучение с его помощью кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP

## Ход работы

---

# Информация об устройстве

```
edzhbitskaya x Windows PowerShell x + - □ x
PS C:\Users\janes> ipconfig

Настройка протокола IP для Windows

Адаптер беспроводной локальной сети Беспроводная сеть 2:

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

Адаптер беспроводной локальной сети Беспроводная сеть 3:

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

Адаптер беспроводной локальной сети Беспроводная сеть 4:

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

Адаптер Ethernet outline-tap0:

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

Адаптер беспроводной локальной сети Беспроводная сеть:

    DNS-суффикс подключения . . . . . : IGD_MGTS
    IPv6-адрес. . . . . : 2a00:1370:8178:119b:379:dab3:a
    800:6f21
    Временный IPv6-адрес. . . . . : 2a00:1370:8178:119b:d06f:dc5e:
    1308:566d
    Локальный IPv6-адрес канала . . . . : fe80::b9ce:7dcd:1e71:b97a%13
    IPv4-адрес. . . . . : 192.168.1.35
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : fe80::5af8:5cff:fe6b:355f%13
    192.168.1.1
```

Рис. 1: ipconfig

```
edzhbitskaya x Windows PowerShell x + - □ x
всех секциях
PS C:\Users\janes> ipconfig /all

Настройка протокола IP для Windows

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

Адаптер беспроводной локальной сети Беспроводная сеть 2:

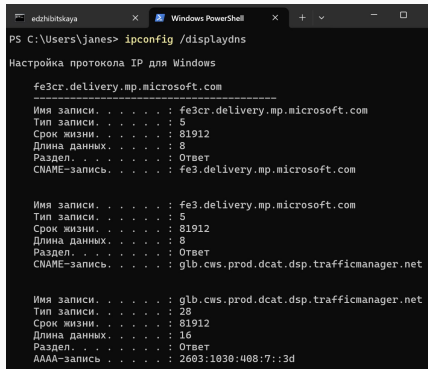
    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :
    Описание. . . . . : Qualcomm WCN685x Wi-Fi 6E Dual
    Band Simultaneous (DBS) Wi-Fi Network Adapter #2
    Физический адрес. . . . . : 3A-D5-7A-F6-60-DD
    DHCP включен. . . . . : Да
    Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Беспроводная сеть 3:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :
    Описание. . . . . : Qualcomm WCN685x Wi-Fi 6E Dual
    Band Simultaneous (DBS) Wi-Fi Network Adapter #3
    Физический адрес. . . . . : 5A-D5-7A-F6-60-DD
    DHCP включен. . . . . : Да
    Автонастройка включена. . . . . : Да
```

Рис. 2: ipconfig /all

# Информация об устройстве



```
PS C:\Users\janes> ipconfig /displaydns

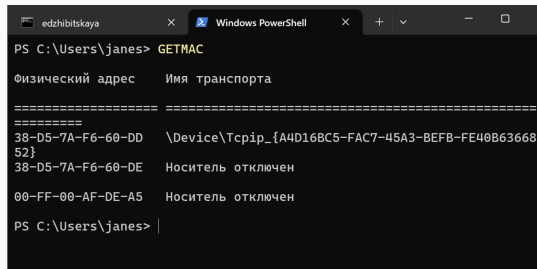
Настройка протокола IP для Windows

fe3cr.delivery.mp.microsoft.com
-----
Имя записи. . . . . : fe3cr.delivery.mp.microsoft.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 81912
Длина данных. . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . : fe3.delivery.mp.microsoft.com

Имя записи. . . . . : fe3.delivery.mp.microsoft.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 81912
Длина данных. . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . : glb.cws.prod.dcat.dsp.trafficmanager.net

Имя записи. . . . . : glb.cws.prod.dcat.dsp.trafficmanager.net
Тип записи. . . . . : 28
Срок жизни. . . . . : 81912
Длина данных. . . . : 16
Раздел. . . . . : Ответ
AAAA-запись. . . . . : 2603:1030:408:7::3d
```

Рис. 3: Содержимое кэша сопоставителя DNS



```
PS C:\Users\janes> GETMAC

Физический адрес      Имя транспорта
=====
38-D5-7A-F6-60-DD     \Device\Tcpip_{A4D16BC5-FAC7-45A3-BEFB-FE40B63668
52}
38-D5-7A-F6-60-DE     Носитель отключен
00-FF-00-AF-DE-A5     Носитель отключен

PS C:\Users\janes> |
```

Рис. 4: MAC-адрес

MAC-адрес 38-D5-7A-F6-60-DD

OUI (идентификатор производителя): 38-D5-7A

Идентификатор сетевого

интерфейса(уникальная часть: F6-60-DD

Тип адреса:

Индивидуальный (Unicast): Младший бит

первого байта (38 -> 00111000) равен 0.

Глобально администрируемый (UAA): Второй

младший бит первого байта равен 0.

```
PS C:\Users\janes> choco install wireshark
Chocolatey v2.5.1
Installing the following packages:
wireshark
By installing, you accept licenses for the packages.
Downloading package from source 'https://community.chocolatey.org/api/v2/'

chocolatey-windowsupdate.extension v1.0.5 [Approved]
chocolatey-windowsupdate.extension package files install completed. Performing other installation steps.
Installed/updated chocolatey-windowsupdate-extension
```

Рис. 5: Установка wireshark

```
PS C:\Users\janes> choco install winpcap
Chocolatey v2.5.1
Installing the following packages:
winpcap
By installing, you accept licenses for the packages.
Downloading package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading WinPcap 4.1.3.20161116... 100%

WinPcap v4.1.3.20161116 [Approved] - Likely broken for FOSS users (due to download location change)
```

Рис. 6: Установка winpcap



Далее запускаем Wireshark, выбираем активный на устройстве интерфейс и смотрим, что начался захват трафика

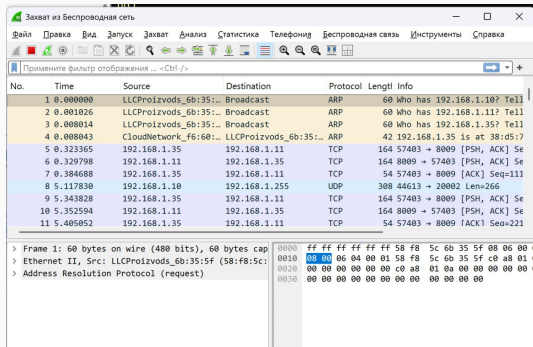


Рис. 7: Запуск программы

```
Адаптер беспроводной локальной сети Беспроводная сеть:  
  
DNS-суффикс подключения . . . . . : IGD_MGTS  
IPv6-адрес. . . . . : 2a00:1370:8178:119b:379:dab3:a  
300:6f21  
Временный IPv6-адрес. . . . . : 2a00:1370:8178:119b:d06f:dc5e:  
1308:566d  
Локальный IPv6-адрес канала . . . : fe80::b9ce:7dcd:1e71:b97a%13  
IPv4-адрес. . . . . : 192.168.1.35  
Маска подсети . . . . . : 255.255.255.0  
Основной шлюз. . . . . : fe80::5af8:5cff:fe6b:355f%13  
192.168.1.1
```

Далее командой `ipconfig` определим IP-адрес устройства и шлюз по умолчанию

Рис. 8: `ipconfig`

```

Администратор: Windo x Администратор: edzhibi x + v -
Основной шлюз. . . . . :
PS C:\Users\janes>
PS C:\Users\janes> ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по 32 байтами данных:
Ответ от 192.168.1.1: число байт=32 время=5мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=21мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=53мс TTL=64
Ответ от 192.168.1.1: число байт=32 время=4мс 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 = 4мсек, Максимальное = 53 мсек, Среднее = 20 мсек
PS C:\Users\janes>
    
```

Рис. 9: Команда ping

Беспроводная сеть

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

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
1709	26.608327	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request
1710	265.608327	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply
1718	266.617624	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request
1719	266.638901	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply
1727	267.625287	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request
1728	267.678283	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply
1731	268.634378	192.168.1.35	192.168.1.1	ICMP	74	Echo (ping) request
1732	268.638987	192.168.1.1	192.168.1.35	ICMP	74	Echo (ping) reply
1733	270.610214	LLCProizvods_6b:35:...	CloudNetwork_f6:60:...	ARP	42	who has 192.168.1.35?
1734	270.610252	CloudNetwork_f6:60:...	LLCProizvods_6b:35:...	ARP	42	192.168.1.35 is at 38
1777	283.034970	LLCProizvods_6b:35:...	Broadcast	ARP	60	Who has 192.168.1.10?

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured on interface 0, 60 bytes from 192.168.1.35 to 192.168.1.1 on interface 0

> Ethernet II, Src: LLCProizvods\_6b:35:5f (58:f8:5c:00:06:04), Dst: 08:00:06:04:00:01, ID: 0x00000000

> Address Resolution Protocol (request)

0000 ff ff ff ff ff ff 58 f8 5c 6b 35 5f 08 06 00 00  
 0010 08 00 06 04 00 01 58 f8 5c 6b 35 5f c0 a8 00 00  
 0020 00 00 00 00 00 00 c0 a8 01 0a 00 00 00 00 00 00  
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Рис. 10: Пакеты arp or icmp

# Эхо-запрос и эхо-ответ ICMP

The screenshot shows the Wireshark interface with the filter 'arp or icmp'. The packet list shows several ICMP Echo (ping) requests and replies. The selected packet (No. 1709) is an ICMP Echo (ping) request from 192.168.1.35 to 192.168.1.1. The packet details pane shows the following structure:

- Frame 1709: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface vti
- Ethernet II, Src: CloudNetwork\_f6:60:dd (38:d5:7a:f6:60:dd), Dst: Destination: LLCProizvods\_6b:35:5f (58:f8:5c:6b:35:5f)
- Source: CloudNetwork\_f6:60:dd (38:d5:7a:f6:60:dd) Type: IPv4 (0x0800) [Stream index: 1]
- Internet Protocol Version 4, Src: 192.168.1.35, Dst: 192.168.1.1
- Internet Control Message Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 58 f8 5c 6b 35 5f 38 d5 7a f6 60 dd 08 00 45 00
0010 00 3c 81 30 00 00 00 01 00 00 c0 a8 01 23 c0 a8
0020 01 01 08 00 4d 57 00 01 00 04 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
```

Рис. 11: Эхо-запрос

The screenshot shows the Wireshark interface with the filter 'arp or icmp'. The packet list shows several ICMP Echo (ping) requests and replies. The selected packet (No. 1710) is an ICMP Echo (ping) reply from 192.168.1.1 to 192.168.1.35. The packet details pane shows the following structure:

- Frame 1710: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface vti
- Ethernet II, Src: LLCProizvods\_6b:35:5f (58:f8:5c:6b:35:5f), Dst: CloudNetwork\_f6:60:dd (38:d5:7a:f6:60:dd)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.35
- Internet Control Message Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 38 d5 7a f6 60 dd 58 f8 5c 6b 35 5f 08 00 45 00
0010 00 3c 81 30 00 00 00 01 00 00 c0 a8 01 23 c0 a8
0020 01 01 08 00 4d 57 00 01 00 04 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
```

Рис. 12: Эхо-ответ

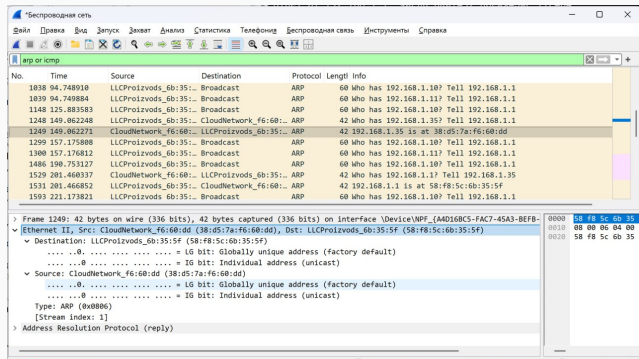


Рис. 13: Кадры протокола ARP

Начнем новый процесс захвата и пропингуем любой другой адрес, например, VK

При обмене пакетами с внешними сетями MAC-адреса источника и назначения в кадре Ethernet всегда принадлежат устройствам локальной сети (отправителю и шлюзу).

## Просмотр данных

No.	Time	Source	Destination	Protocol	Length	Info
80	33.268611	192.168.1.35	185.178.208.57	ICMP	74	Echo (ping) request id=0x0001, seq=10/256
81	33.273238	LLCProizvodis_6b:35::	CloudNetwork_f6:60::	ARP	42	192.168.1.1 is at 58:f8:5c:6b:35:5f
86	38.272655	192.168.1.35	185.178.208.57	ICMP	74	Echo (ping) request id=0x0001, seq=11/281
141	50.664331	192.168.1.35	87.240.129.133	ICMP	74	Echo (ping) request id=0x0001, seq=12/307
142	50.706836	87.240.129.133	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=12/307
143	51.675481	192.168.1.35	87.240.129.133	ICMP	74	Echo (ping) request id=0x0001, seq=13/332
144	51.699993	87.240.129.133	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=13/332
149	52.690834	192.168.1.35	87.240.129.133	ICMP	74	Echo (ping) request id=0x0001, seq=14/358
150	52.710597	87.240.129.133	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=14/358
151	53.701248	192.168.1.35	87.240.129.133	ICMP	74	Echo (ping) request id=0x0001, seq=15/384
152	53.735195	87.240.129.133	192.168.1.35	ICMP	74	Echo (ping) reply id=0x0001, seq=15/384

```

> Frame 86: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{
Ethernet II, Src: CloudNetwork_f6:60:dd (38:d5:7a:f6:60:dd), Dst: LLCProizvodis_6b:35:5f (58:f8:
  Destination: LLCProizvodis_6b:35:5f (58:f8:5c:6b:35:5f)
    ....0. .... : LG bit: Globally unique address (factory default)
    ....0. .... : LG bit: Individual address (unicast)
  > Source: CloudNetwork_f6:60:dd (38:d5:7a:f6:60:dd)
    ....0. .... : LG bit: Globally unique address (factory default)
    ....0. .... : LG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 1]
> Internet Protocol Version 4, Src: 192.168.1.35, Dst: 185.178.208.57

```

Рис. 14: Запрос

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Capture, Analyze, Statistics, Telephone, Беспроводная связь, and Инструменты. The top toolbar contains icons for file operations, capture, analysis, and search. The main window is divided into three panes:

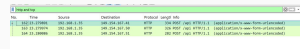
- Packet List:** Shows a list of captured packets. The selected packet is #142, an ARP request from 192.168.1.35 to 192.168.1.1.
- Packet Details:** Displays the hierarchical structure of the selected packet. It shows Ethernet II (Type I: IPv4 (0x0000)) and Internet Protocol Version 4 (Src: 192.246.129.135, Dst: 192.168.1.1).
- Packet Bytes:** Shows the raw data of the selected packet in hexadecimal and ASCII. The data represents an ARP request structure.

The selected packet details are as follows:

- Ethernet II:** Src: LLCProtocolzvs\_6b:35:5f (58:f8:5b:35:5f), Dst: CloudNetwork\_f6:60:dd (38:d5:7a:f6:60:dd)
- Internet Protocol Version 4:** Src: 192.246.129.135, Dst: 192.168.1.1
- ARP:** Request, Op: 1, Hardware type: 1, Protocol type: 2, Sender MAC: 58:f8:5b:35:5f, Target MAC: 38:d5:7a:f6:60:dd

Рис. 15: Ответ

Можно увидеть, что используются tcp протоколы, сетевые протоколы ipv4/6 В качестве DNS-сервера используется маршрутизатор (fe80::5af8:5cff:fe60:355f), который ретранслирует запросы на внешние DNS-серверы и возвращает ответы. Запросы отправляются на Microsoft-серверы. Для QUIC запросов используется UDP протокол, ipv6, видны типы пакетов - initial(с основными данными), handshake.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.10	192.168.1.10	HTTP	104	GET / HTTP/1.1 (application/javascript)
2	0.000000	192.168.1.10	192.168.1.10	HTTP	104	200 OK / HTTP/1.1 (application/javascript)
3	0.000000	192.168.1.10	192.168.1.10	HTTP	104	GET / HTTP/1.1 (application/javascript)

Рис. 16: HTTP



## Анализ протоколов транспортного уровня

[illegible]

Рис. 17: DNS

Вид Панель Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

Quic and qpack

No.	Time	Source	Destination	Protocol	Length	Info
12171	13.961852	2a00:1370:8178:110b...	2a00:1450:4010:0c91...	QUIC	1292	Initial, DCID=F996d81d97193ed, PKN: 2, CRYPTO, PING, CRYPTO, P...
12183	13.013169	2a00:1450:4010:0c91...	2a00:1370:8178:110b...	QUIC	102	Initial, SCID=F996d81d97193ed, PKN: 1, ACK
12186	13.034549	2a00:1450:4010:0c91...	2a00:1370:8178:110b...	QUIC	1292	Initial, SCID=F996d81d97193ed, PKN: 2, ACK, PADDING
12187	13.037749	2a00:1450:4010:0c91...	2a00:1370:8178:110b...	QUIC	1292	Initial, SCID=F996d81d97193ed, PKN: 3, CRYPTO, PADDING
12188	13.037749	2a00:1450:4010:0c91...	2a00:1370:8178:110b...	QUIC	1292	Initial, SCID=F996d81d97193ed, PKN: 4, CRYPTO, PADDING
12189	13.037749	2a00:1450:4010:0c91...	2a00:1370:8178:110b...	QUIC	1202	Handshake, SCID=F996d81d97193ed
12190	13.037749	2a00:1450:4010:0c91...	2a00:1370:8178:110b...	QUIC	1340	Protected Payload (KPB)
12191	13.038337	2a00:1370:8178:110b...	2a00:1450:4010:0c91...	QUIC	1292	Initial, DCID=F996d81d97193ed, PKN: 3, ACK, PADDING
12192	13.039064	2a00:1370:8178:110b...	2a00:1450:4010:0c91...	QUIC	102	Handshake, DCID=F996d81d97193ed
12193	13.039122	2a00:1370:8178:110b...	2a00:1450:4010:0c91...	QUIC	1240	Protected Payload (KPB), DCID=F996d81d97193ed
12194	13.129134	2a00:1450:4010:0c91...	2a00:1370:8178:110b...	QUIC	2017	Protected Payload (KPB)
12195	13.130688	2a00:1370:8178:110b...	2a00:1370:8178:110b...	QUIC	1835	Protected Payload (KPB)

Frame 12191: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on Interface 1  
 Ethernet II, Src: CloudNetwork, 6e:60:ad:38:05:7a (6e:60:ad:38:05:7a:60:ad), Dst: LLCProizvod, 6b:35:5f (58:f6:35:5f:58:f6:35:5f)  
 Destination: LLCProizvod, 6b:35:5f (58:f6:35:5f:58:f6:35:5f)  
 Source: CloudNetwork, 6e:60:ad:38:05:7a (6e:60:ad:38:05:7a:60:ad)  
 Type: IPv6 (0x06)  
 [Stream index: 0]

Internet Protocol Version 6, Src: 2a00:1370:8178:110b:08bf:d5c6:1308:5666, Dst: 2a00:1450:4010:0c91:0000:0000:0000:0000  
 Datagram Protocol, Src Port: 49208, Dst Port: 443

QUIC INFO

Frame (1292 bytes) Decrypted QUIC (1195 bytes)

Рис. 18: OUIС

# Handshake

No.	Time	Source	Destination	Protocol	Length	Info
1175	93.418777	2a00:1370:8178:119b...	2001:1458:d00:25::1	TLSv1.3	1865	Client Hello (SNI=line-node.cern.ch)
1176	93.418935	2001:1458:d00:25::1	2a00:1370:8178:119b...	TCP	320	[TCP Retransmission] 58238 → 443 [PSH, ACK] Seq=39...
1177	93.504161	2001:1458:d00:25::1	2a00:1370:8178:119b...	TCP	315	[TCP Spurious Retransmission] 443 → 58238 [PSH, ACK]
1178	93.504196	2a00:1370:8178:119b...	2001:1458:d00:25::1	TCP	86	[TCP Dup ACK 114541] 58238 → 443 [ACK] Seq=4779
1179	93.507052	2001:1458:d00:25::1	2a00:1370:8178:119b...	TLSv1.3	315	Application Data
1180	93.507052	2001:1458:d00:25::1	2a00:1370:8178:119b...	TCP	86	[TCP Dup ACK 115841] 443 → 58240 [ACK] Seq=246
1181	93.525641	2001:1458:d00:25::1	2a00:1370:8178:119b...	TCP	86	[TCP Dup ACK 114041] 443 → 58239 [ACK] Seq=246
1182	93.528818	2001:1458:d00:25::1	2a00:1370:8178:119b...	TCP	74	443 → 58239 [ACK] Seq=246 Ack=2159 Win=65664 Len=0
1183	93.548935	2001:1458:d00:25::1	2a00:1370:8178:119b...	TLSv1.3	345	Application Data
1184	93.548935	2001:1458:d00:25::1	2a00:1370:8178:119b...	TLSv1.3	315	Application Data
1185	93.549029	2a00:1370:8178:119b...	2001:1458:d00:25::1	TCP	74	58239 → 443 [ACK] Seq=3035 Ack=758 Win=64768 Len=0
1186	93.549226	2001:1458:d00:25::1	2a00:1370:8178:119b...	TLSv1.3	616	Application Data

> Frame 1176: 926 bytes on wire (7408 bits), 926 bytes captured (7408 bits) on interface 'Device'  
> Ethernet II, Src: CloudNetwork\_f6:60:dd (38:d5:7a:f6:60:dd), Dst: LLCProizvodsk\_6b:35:5f (58:f6:6b:35:5f)  
    > Destination: LLCProizvodsk\_6b:35:5f (58:f6:6b:35:5f)  
    > Source: CloudNetwork\_f6:60:dd (38:d5:7a:f6:60:dd)  
    Type: IPv6 (86:60:dd)  
        [Stream Index: 1]  
    > Internet Protocol Version 6, Src: 2a00:1370:8178:119b:d06fd5e:1308:566d, Dst: 2001:1458:d00:25::1  
    > Transmission Control Protocol, Src Port: 58238, Dst Port: 443, Seq: 3927, Ack: 7034, Len: 852

0000 58 f8 5c 6b 35 5f 38 d5 1  
0010 72 97 03 68 06 40 2a 00 1  
0020 dc 5e 13 00 56 6d 30 01 1  
0030 00 00 01 00 01 59 e3 7e 6  
0040 b5 e3 50 18 00 ff 2e ad 6  
0050 e1 3d 5c c2 bf f2 25 30 d  
0060 05 c9 8a ff e2 2e 2c 2d 6  
0070 6d 6f fd 83 75 b3 0a 01 c  
0080 38 f1 a8 1a d0 ba 18 22 c  
0090 22 63 a7 53 58 f6 ae cf 5  
00a0 6f 40 ce f6 63 f8 4c 82 4  
00b0 96 35 15 61 84 f0 ea 85 c

Рис. 19: Просмотр перехвата

TCP Handshake (3-way):

Клиент → Сервер: SYN (запрос на соединение)

Сервер → Клиент: SYN-ACK (подтверждение + свой запрос)

Клиент → Сервер: ACK (подтверждение).

Соединение установлено.

Далее просмотрим график потока в меню статистика и ознакомимся с информацией. Остановим захват.

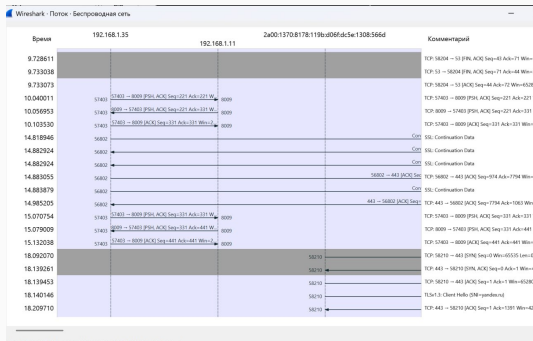


Рис. 20: График потока

## Вывод

---

- В ходе работы было произведено знакомство с Wireshark, были изучены с его помощью кадры Ethernet, произведен анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP