

Лабораторная работа №3

Дисциплина: Сетевые технологии

Жибицкая Евгения Дмитриевна

Содержание

| | | |
|----------|---------------------------------------|-----------|
| 1 | Цель работы | 5 |
| 2 | Выполнение лабораторной работы | 6 |
| 3 | Выводы | 17 |
| | Список литературы | 18 |

Список иллюстраций

| | | |
|------|---|----|
| 2.1 | ipconfig | 6 |
| 2.2 | ipconfig /all | 7 |
| 2.3 | Содержимое кэша сопоставителя DNS | 8 |
| 2.4 | MAC-адрес | 8 |
| 2.5 | Установка wireshark | 9 |
| 2.6 | Установка winpcap | 9 |
| 2.7 | Запуск программы | 10 |
| 2.8 | ipconfig | 10 |
| 2.9 | Команда ping | 11 |
| 2.10 | Пакеты arp or icmp | 11 |
| 2.11 | Эхо-запрос | 12 |
| 2.12 | Эхо-ответ | 12 |
| 2.13 | Кадры протокола ARP | 13 |
| 2.14 | Запрос | 13 |
| 2.15 | Ответ | 14 |
| 2.16 | HTTP | 14 |
| 2.17 | DNS | 15 |
| 2.18 | QUIC | 15 |
| 2.19 | Просмотр перехвата | 16 |
| 2.20 | График потока | 16 |

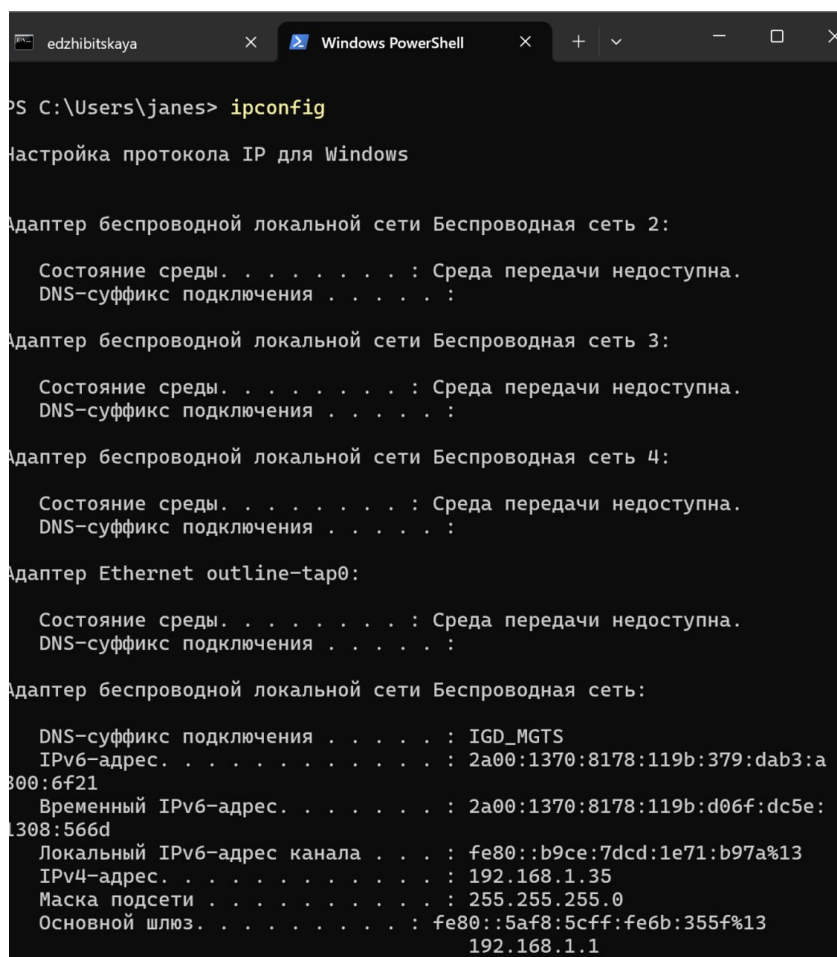
Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

Для начала введем `ipconfig`, получив информацию об устройстве, воспользуемся опциями для более подробного вывода (рис. 2.1 и (рис. 2.2) и (рис. 2.3)) узнаем MAC-адрес устройства (рис. 2.4).



```
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. 2.1: `ipconfig`

```
edzhibitskaya  Windows PowerShell  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) WiFiCx 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) WiFiCx Network Adapter #3
Физический адрес. . . . . : 5A-D5-7A-F6-60-DD
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
```

Рис. 2.2: ipconfig /all

```

edzhibitskaya  Windows PowerShell
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. 2.3: Содержимое кэша сопоставителя DNS

```

edzhibitskaya  Windows PowerShell
PS C:\Users\janes> GETMAC

Физический адрес      Имя транспорта
=====
38-D5-7A-F6-60-DD    \Device\NPF_{A4D16BC5-FAC7-45A3-BEFB-FE40B63668}
38-D5-7A-F6-60-DE    Носитель отключен
00-FF-00-AF-DE-A5    Носитель отключен
PS C:\Users\janes>

```

Рис. 2.4: MAC-адрес

Проанализируем MAC-адрес 38-D5-7A-F6-60-DD

Он состоит из нескольких частей и содержит следующую информацию:

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.

Для дальнейшего выполнения лабораторной работы нам необходимо установить Wireshark. Используем для этого Chocolatey(рис. 2.5). Также понадобится еще один пакет, который мы и установим(рис. 2.6)

```
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. 2.5: 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 changes)
```

Рис. 2.6: Установка winpcap

Далее запускаем Wireshark, выбираем активный на устройстве интерфейс и смотрим, что начался захват трафика(рис. 2.7)

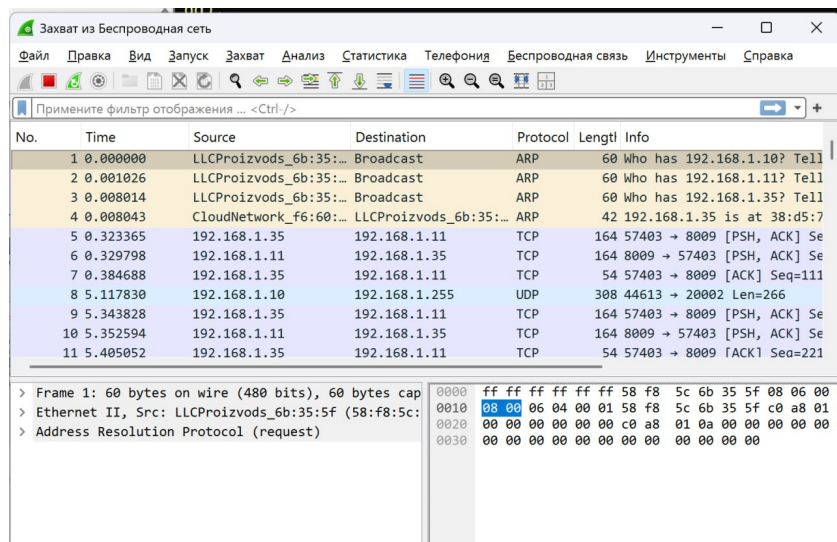


Рис. 2.7: Запуск программы

Далее командой `ipconfig` определим IP-адрес устройства и шлюз по умолчанию (рис. 2.8)

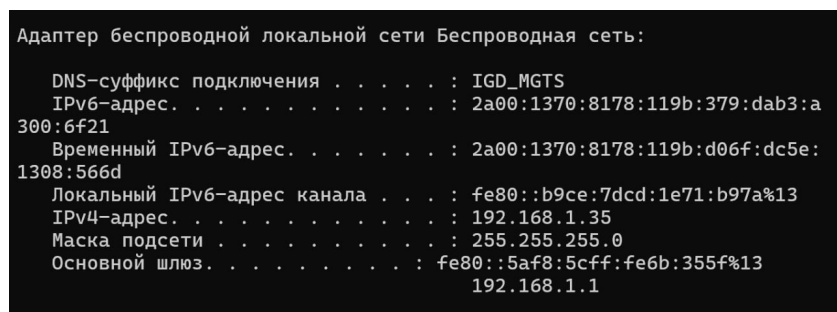


Рис. 2.8: `ipconfig`

Затем пропингуем шлюз по умолчанию, клавишами остановим процесс (рис. 2.7)

```

Администратор: Windo
Администратор: edzhibi
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. 2.9: Команда ping

После остановим захват трафика в Wireshark, пропишем фильтр arp or icmp и убедимся что в списке пакетов видны только пакеты ARP или ICMP(рис. 2.10)

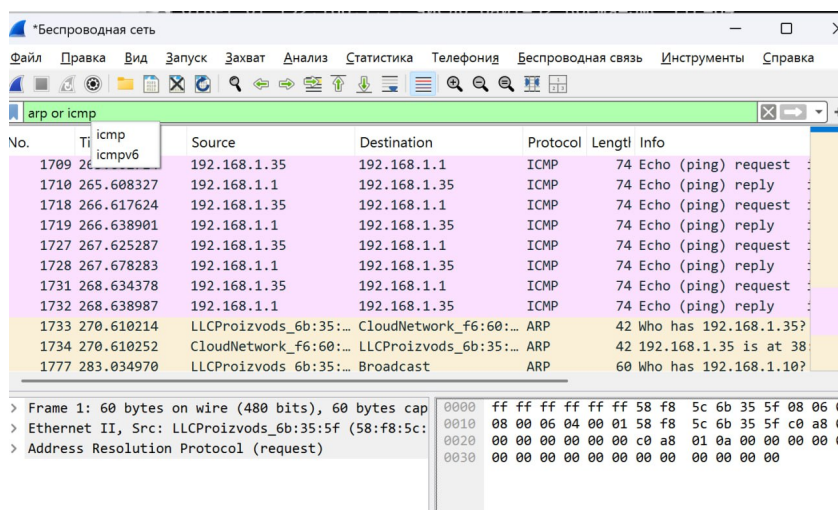


Рис. 2.10: Пакеты arp or icmp

Изучим эхо-запрос и эхо-ответ ICMP – На панели списка пакетов (верхний раздел) выберем первый указанный кадр ICMP – эхо-запрос(рис. 2.11)

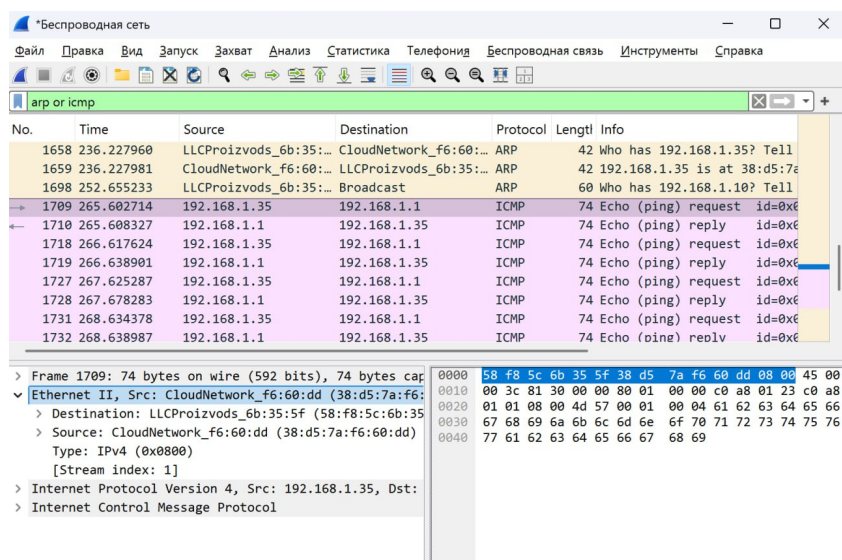


Рис. 2.11: Эхо-запрос

– На панели списка пакетов (верхний раздел) выберем второй указанный кадр ICMP — эхо-ответ. (рис. 2.12)

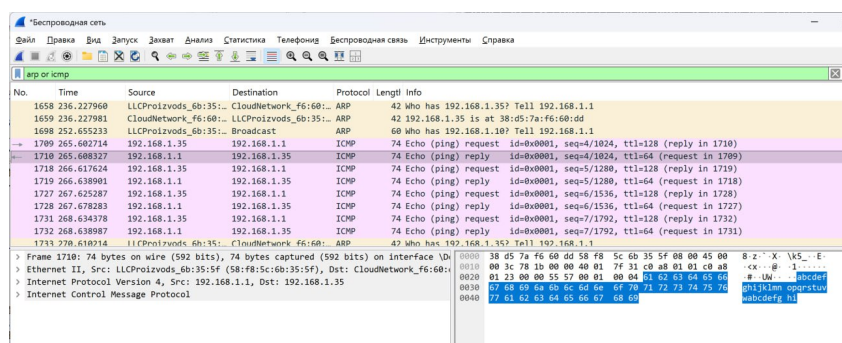


Рис. 2.12: Эхо-ответ

Длина кадров составляет 74 байта, тип - Ethernet 2, MAC-адреса - 38:d5:7a:f6:60:dd (UAA, Unicast) и 58:18:5c:6b:35:5f (UAA, Unicast), IP-адреса - 192.168.1.35 и 192.168.1.1

Также изучим кадры данных протокола ARP(рис. 2.13)

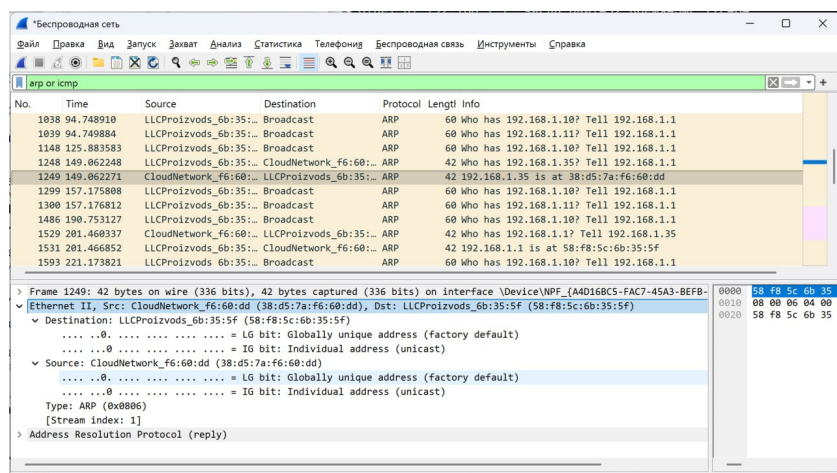


Рис. 2.13: Кадры протокола ARP

Начнем новый процесс захвата и пропингуем любой другой адрес, например, VK, изучим данные по нему.

MAC назначения 38:d5:7a:fc:60:dd Unicast, UAA. это устройство. MAC источника 58:48:5c:6b:35:5f Unicast, UAA. Маршрутизатор (шлюз, ip - 87.240.129.133) (рис. 2.14 и рис. 2.15). При обмене пакетами с внешними сетями (интернетом) MAC-адреса источника и назначения в кадре Ethernet всегда принадлежат устройствам локальной сети (отправителю и шлюзу). MAC-адреса устройств из глобального интернета тут не видны.

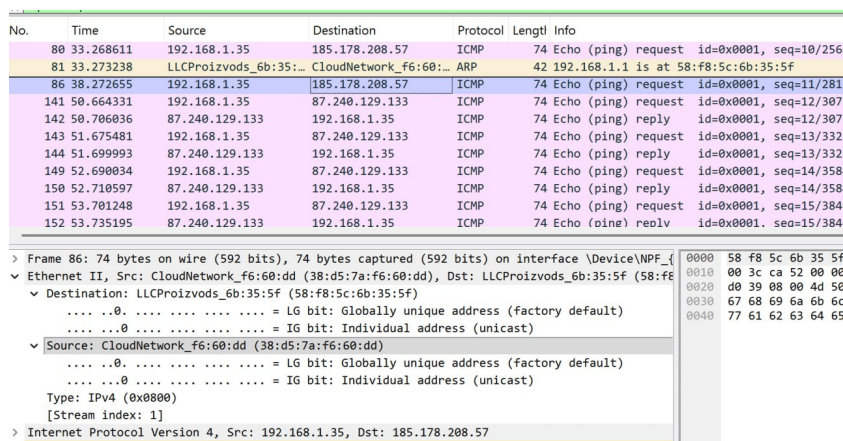


Рис. 2.14: Запрос

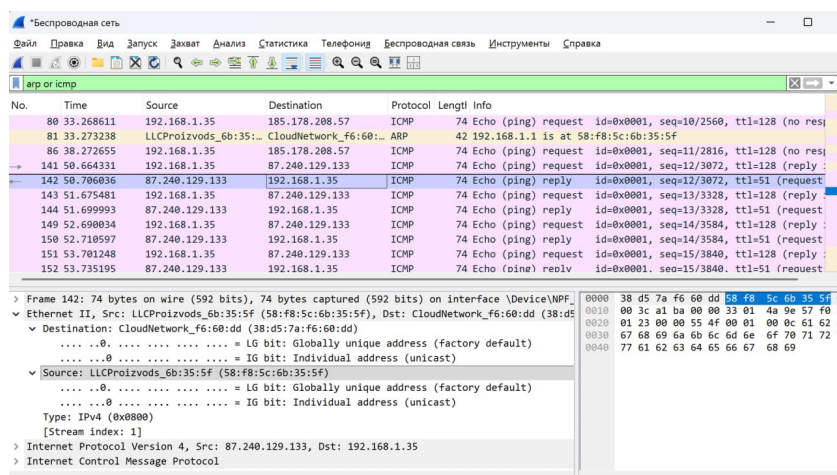


Рис. 2.15: Ответ

Проанализируем также протоколы транспортного уровня.

Начнем захват трафика, перейдем на сайт, работающий по протоколу HTTP.

В Wireshark в строке фильтра укажем http и проанализируем информацию по протоколу TCP в случае запросов и ответов, аналогично для DNS и QUIC(рис. 2.16, рис. 2.17 и рис. 2.18).

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 |
|-----|-----------|--------------|----------------|----------|--------|--|
| 162 | 23.279891 | 192.168.1.35 | 149.154.167.41 | HTTP | 334 | POST /api HTTP/1.1 (application/x-www-form-urlencoded) |
| 163 | 23.279974 | 192.168.1.35 | 149.154.167.50 | HTTP | 326 | POST /api HTTP/1.1 (application/x-www-form-urlencoded) |
| 164 | 23.280086 | 192.168.1.35 | 149.154.167.51 | HTTP | 282 | POST /api HTTP/1.1 (application/x-www-form-urlencoded) |

Рис. 2.16: HTTP

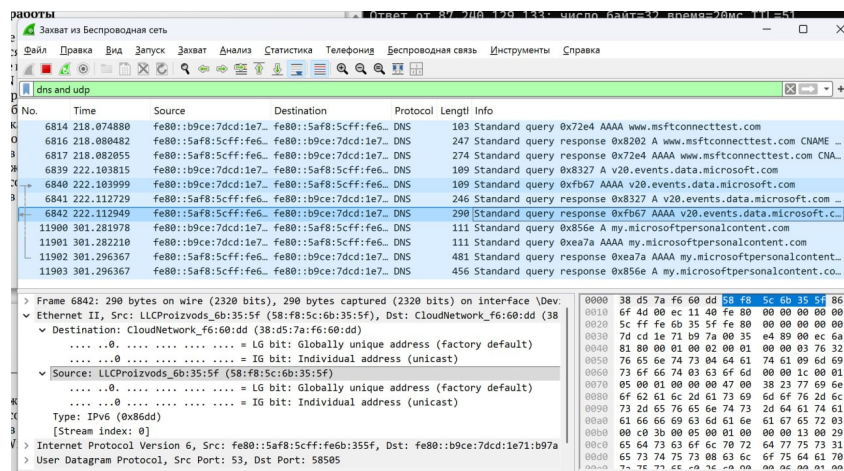


Рис. 2.17: DNS

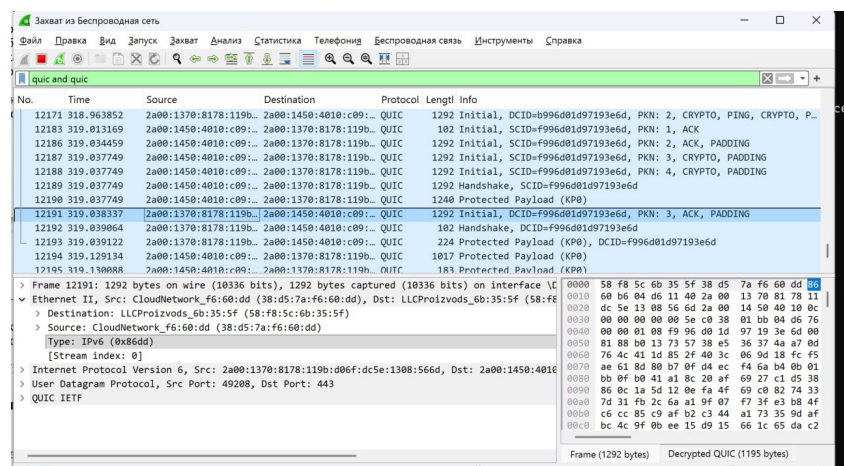


Рис. 2.18: QUIC

Проанализируем отдельно handshake protocol TCP.

Также захватим трафик, используем HTTP соединения и посмотрим на данные(рис. 2.19). TCP Handshake (3-way):

Клиент → Сервер: SYN (запрос на соединение)

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

Клиент → Сервер: ACK (подтверждение). Соединение установлено.

Пакет №1176 (после handshake):

Seq=3927 — клиент уже отправил 3926 байт данных.

Ask=7034 — клиент подтвердил получение 7033 байт от сервера.

TCP Retransmission — этот пакет был отправлен повторно, так как первый раз потерялся.

| 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-mode.cern.ch) |
| 1176 | 93.435975 | 2a00:1370:8178:119b... | 2001:1458:d00:25::1 | TCP | 926 | [TCP Retransmission] 58238 → 443 [PSH, ACK] Seq=3927 |
| 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 1145#1] 58238 → 443 [ACK] Seq=4779 Ack= |
| 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 1158#1] 443 → 58240 [ACK] Seq=246 Ack= |
| 1181 | 93.525641 | 2001:1458:d00:25::1 | 2a00:1370:8178:119b... | TCP | 86 | [TCP Dup ACK 1149#1] 443 → 58239 [ACK] Seq=246 Ack= |
| 1182 | 93.528810 | 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 | 93.549776 | 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\NPF{...}

> Ethernet II, Src: CloudNetwork_f6:60:dd (38:d5:7a:f6:60:dd), Dst: LLCProizvods_6b:35:5f (58:f8:5c:6b:35:5f)

> Destination: LLCProizvods_6b:35:5f (58:f8:5c:6b:35:5f)

> Source: CloudNetwork_f6:60:dd (38:d5:7a:f6:60:dd)

Type: IPv6 (0x86dd)

[Stream index: 1]

> Internet Protocol Version 6, Src: 2a00:1370:8178:119b:d06f:dc5e: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

0010 72 97 03 68 06 40 2a 00

0020 dc 5e 13 08 56 6d 20 01

0030 00 00 01 00 01 59 e3 7e

0040 b5 e3 50 18 00 ff 2e 0d

0050 e1 3d 5c c2 bf f2 25 30

0060 d9 c9 8a ff a2 2e 2c 2d

0070 6d 6f fd 83 75 b3 0a 01

0080 38 f1 a8 1a d0 ba 18 22

0090 22 63 a7 53 58 f6 ae cf

00a0 6f 49 ce f6 61 f8 4c 82

00b0 96 35 15 61 84 f0 ea 85

Рис. 2.19: Просмотр перехвата

Далее посмотрим график потока в меню статистика и ознакомимся с информацией(рис. 2.20). Остановим захват.

1. Установление соединения (Handshake) - Пакет 1 -3 - обмены в обе стороны
2. Передача данных
3. Разрыв соединения и прекращение обмена данными

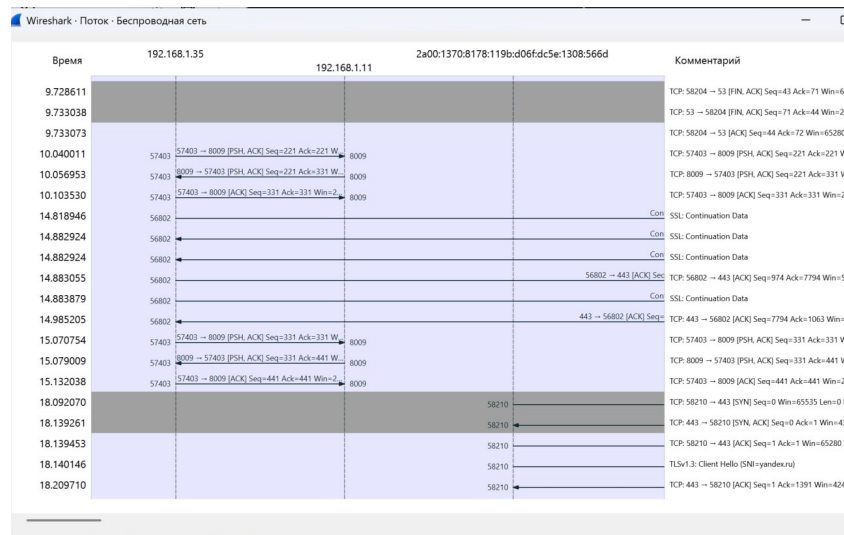


Рис. 2.20: График потока

3 Выводы

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

Список литературы

[ТУИС] (https://esystem.rudn.ru/pluginfile.php/2858360/mod_resource/content/3/003-lab_datalink-layer-WSh.pdf)