Лабораторная работа №3

Дисциплина: Сетевые технологии

Жибицкая Евгения Дмитриевна

Содержание

# 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. 1 и (рис. 2) и (рис. 3)) узнаем MAC-адрес устройства(рис. 4).

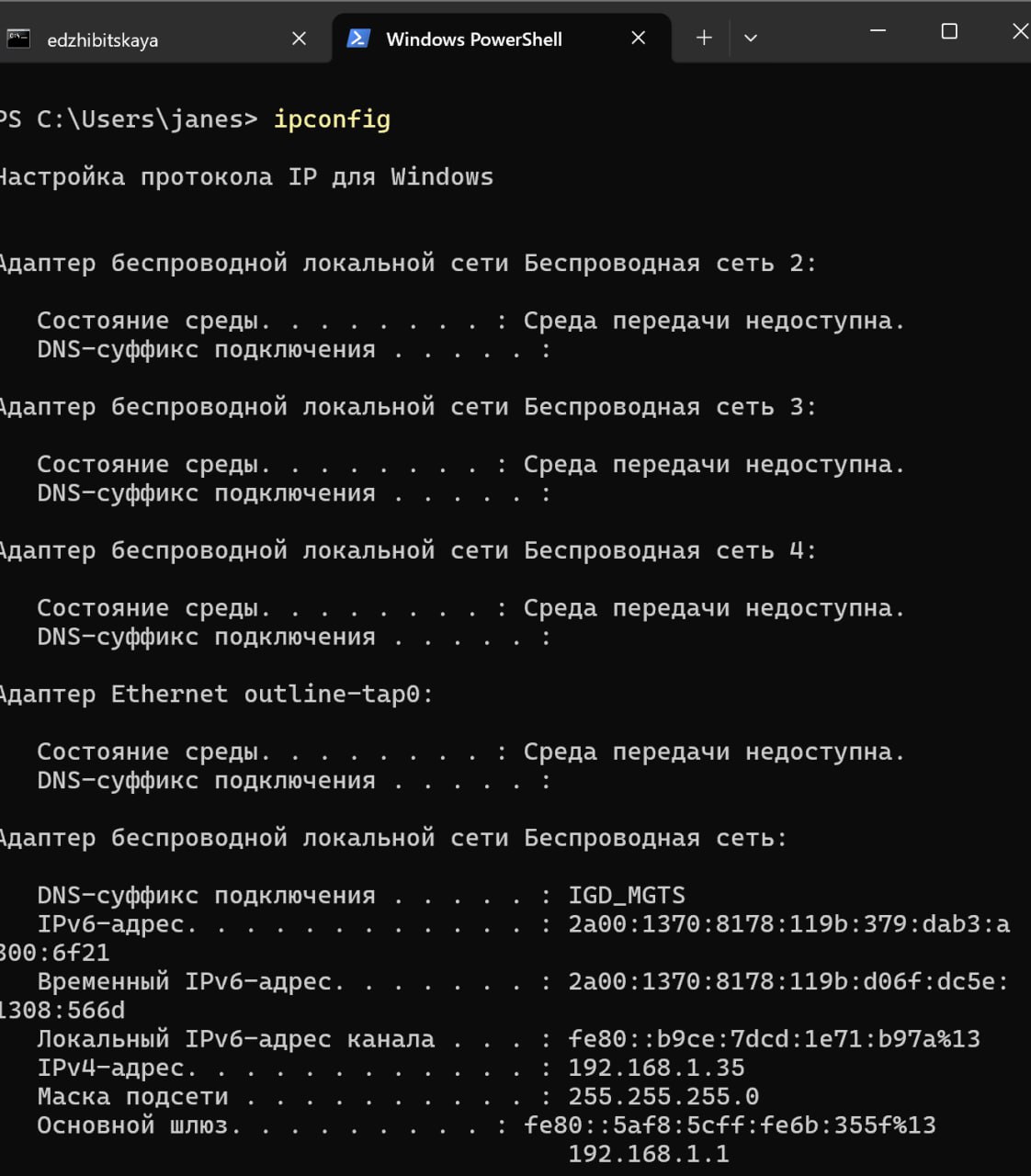


Рис. 1: ipconfig

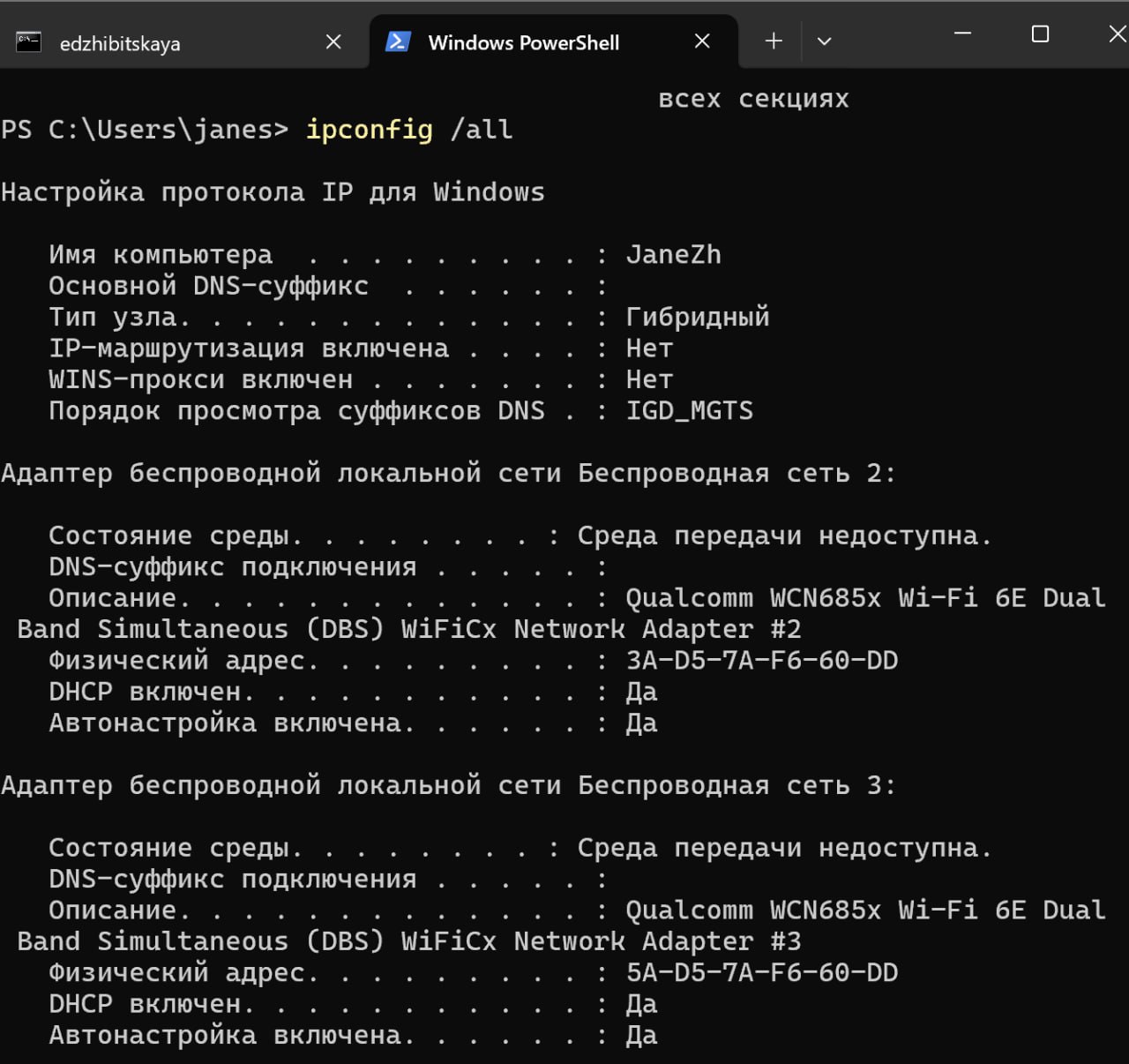


Рис. 2: ipconfig /all

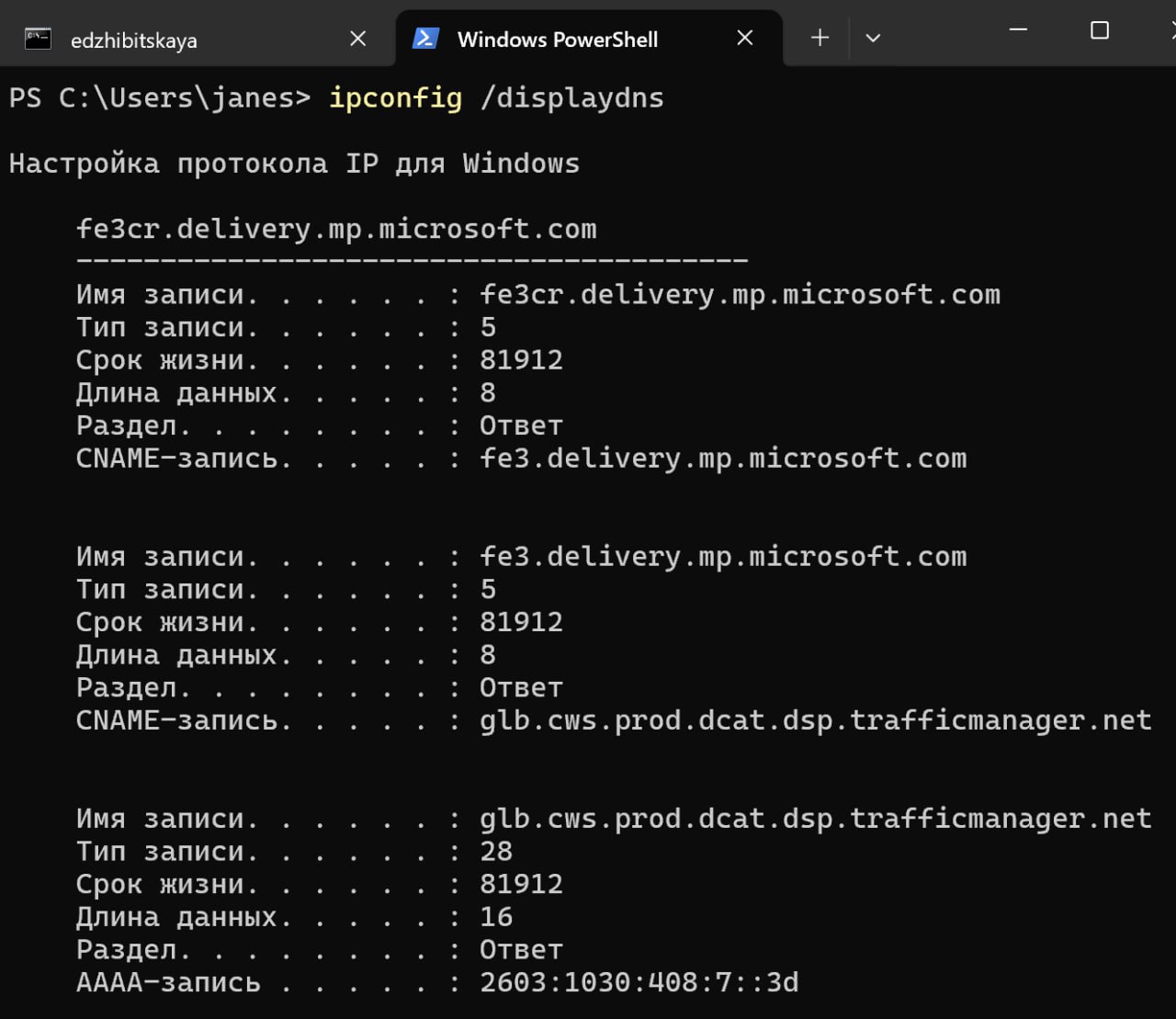


Рис. 3: Содержимое кэша сопоставителя DNS

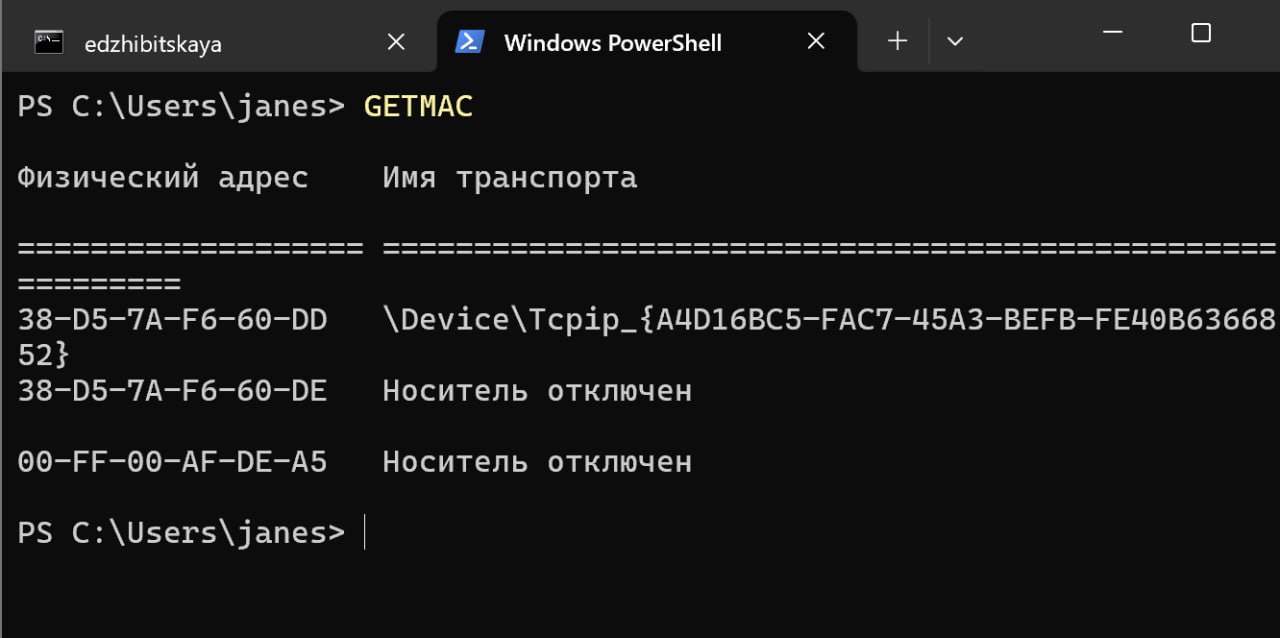


Рис. 4: MAC-адрес

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 утановить Wireshark. Используем для этого Chocolatey(рис. 5). Также понадобится еще один пакет, который мы и установим(рис. 6)

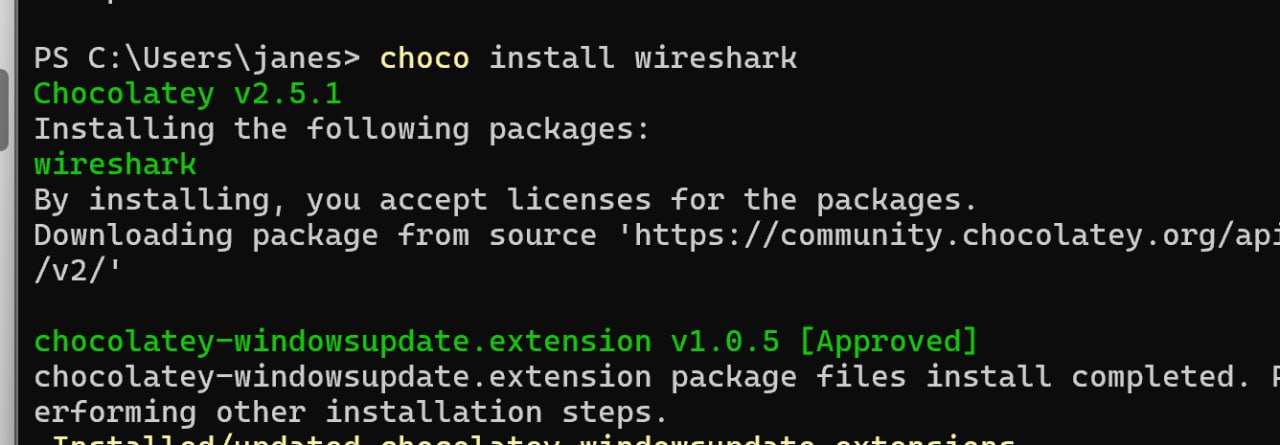


Рис. 5: Установка wireshark

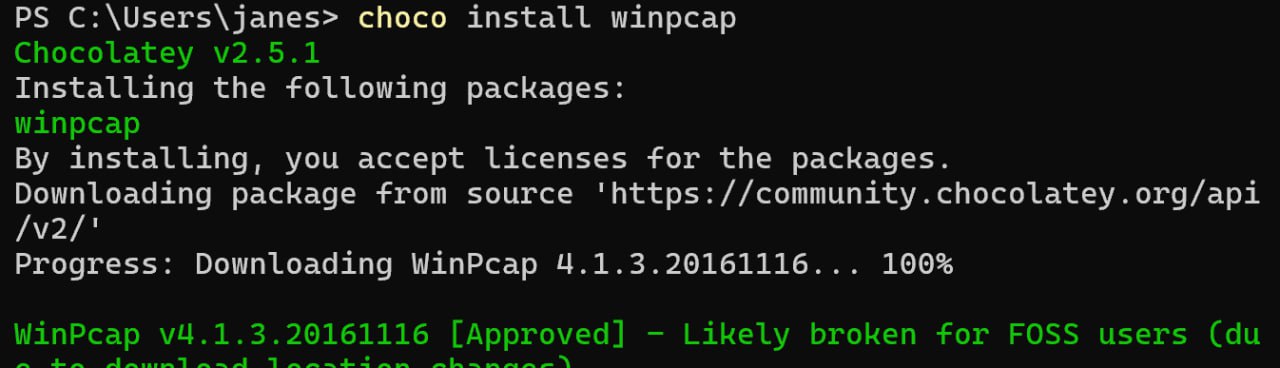


Рис. 6: Установка winpcap

Далее запускаем Wireshark, выбираем активный на устройстве интерфейс и смотрим, что начался захват трафика(рис. 7)

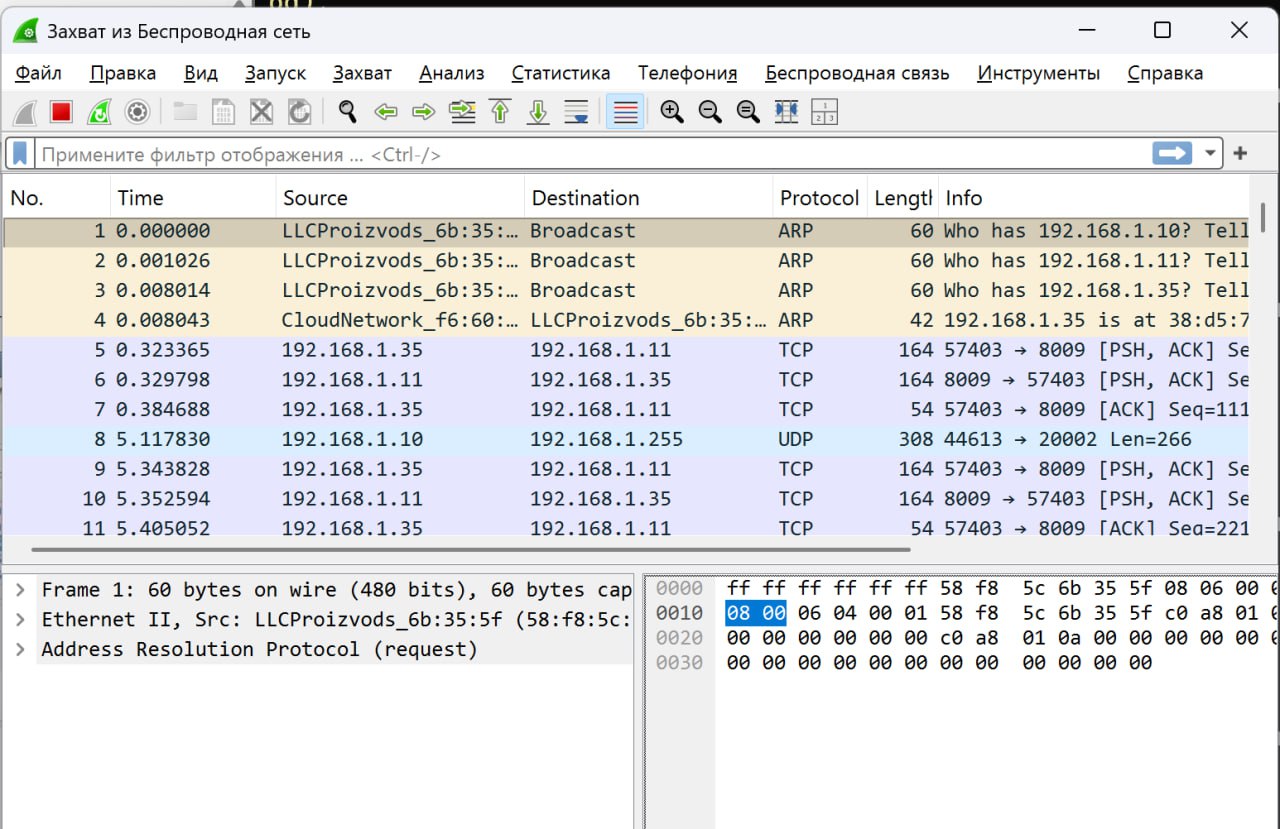


Рис. 7: Запуск программы

Далее командой ipconfig определим IP-адрес устройства и шлюз по умолчанию(рис. 8)

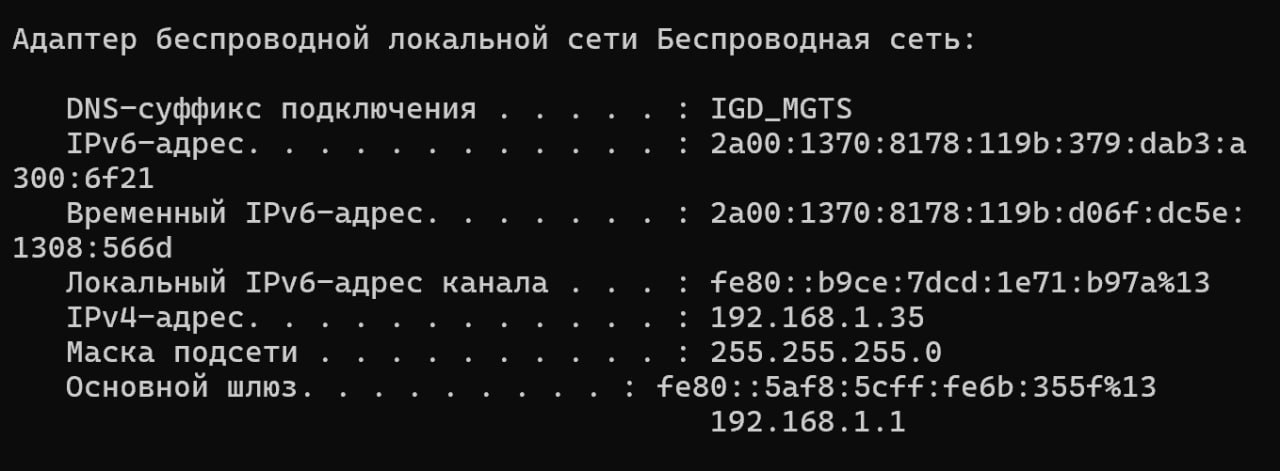


Рис. 8: ipconfig

Затем пропингуем шлюз по умолчанию, клавишами остановим процесс(рис. 7)

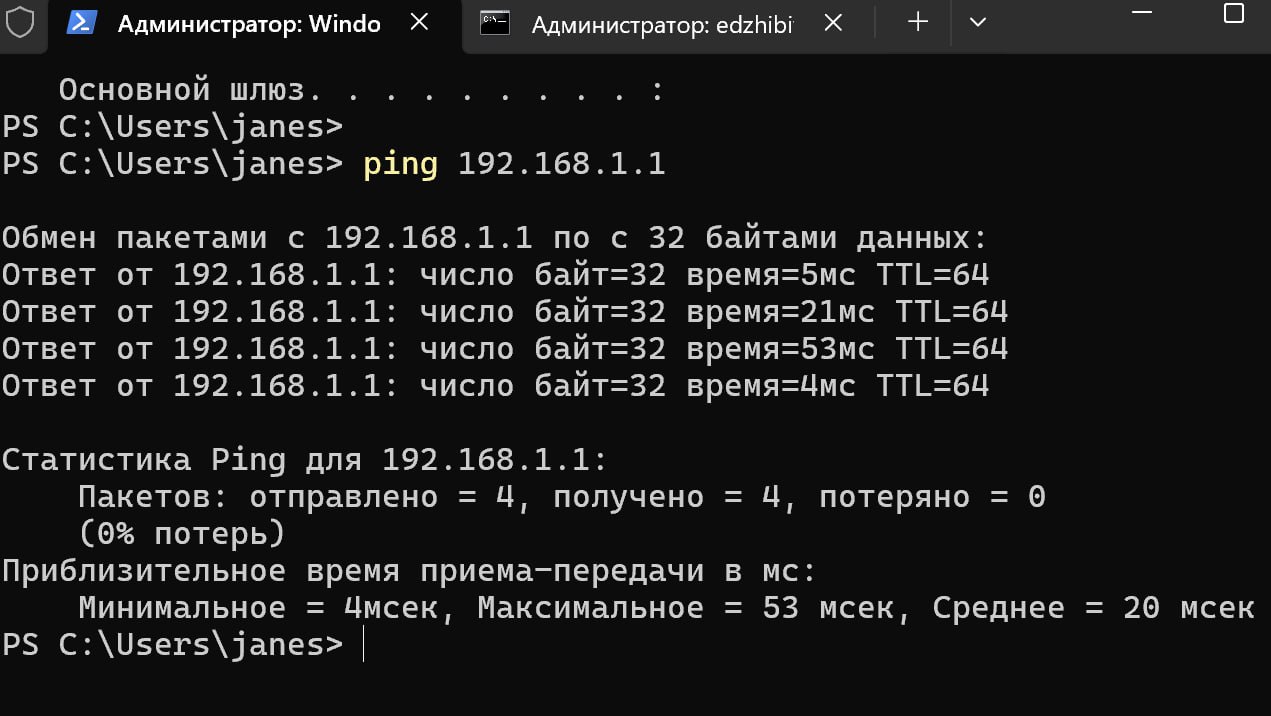


Рис. 9: Команда ping

После остановим захват трафика в Wireshark, пропишем фильтр arp or icm и убедимся что в списке пакетов видны только пакеты ARP или ICMP(рис. 10)

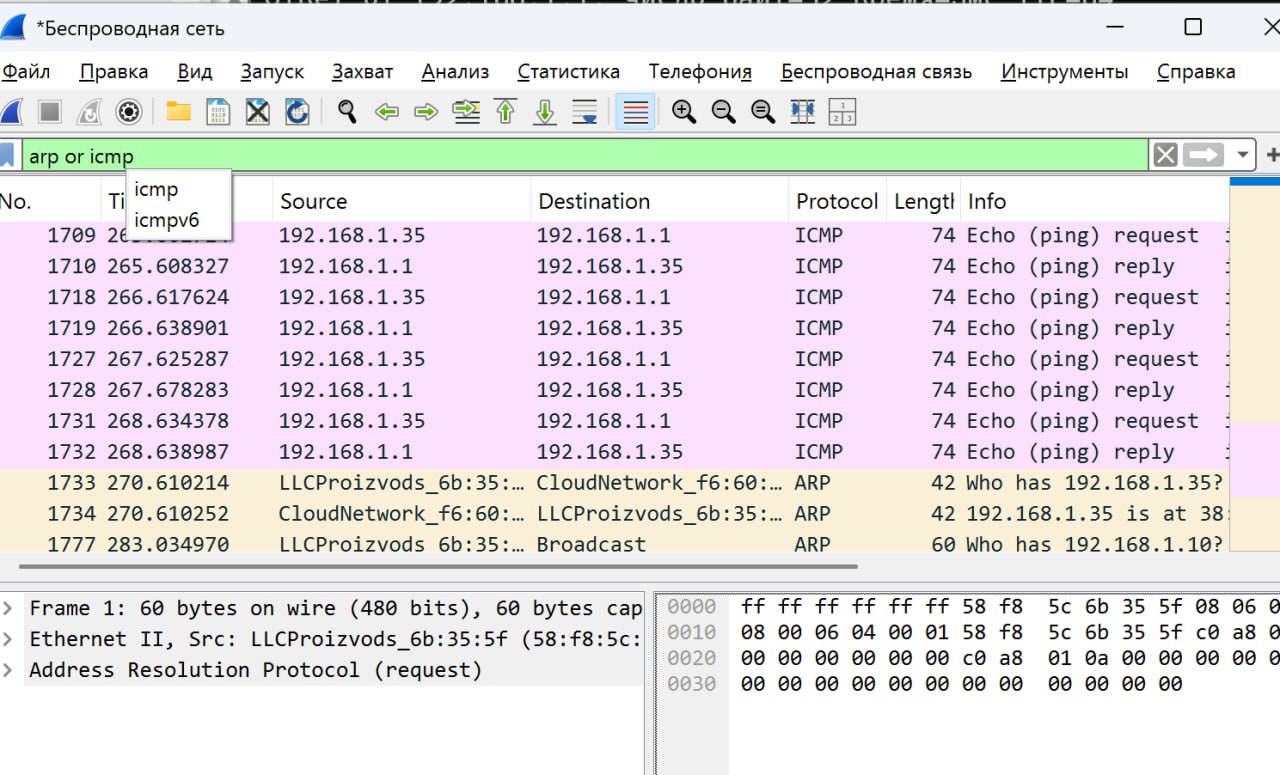


Рис. 10: Пакеты arp or icm

Изучим эхо-запрос и эхо-ответ ICMP – На панели списка пакетов (верхний раздел) выберим первый указанный кадр ICMP — эхо-запрос(рис. 11)

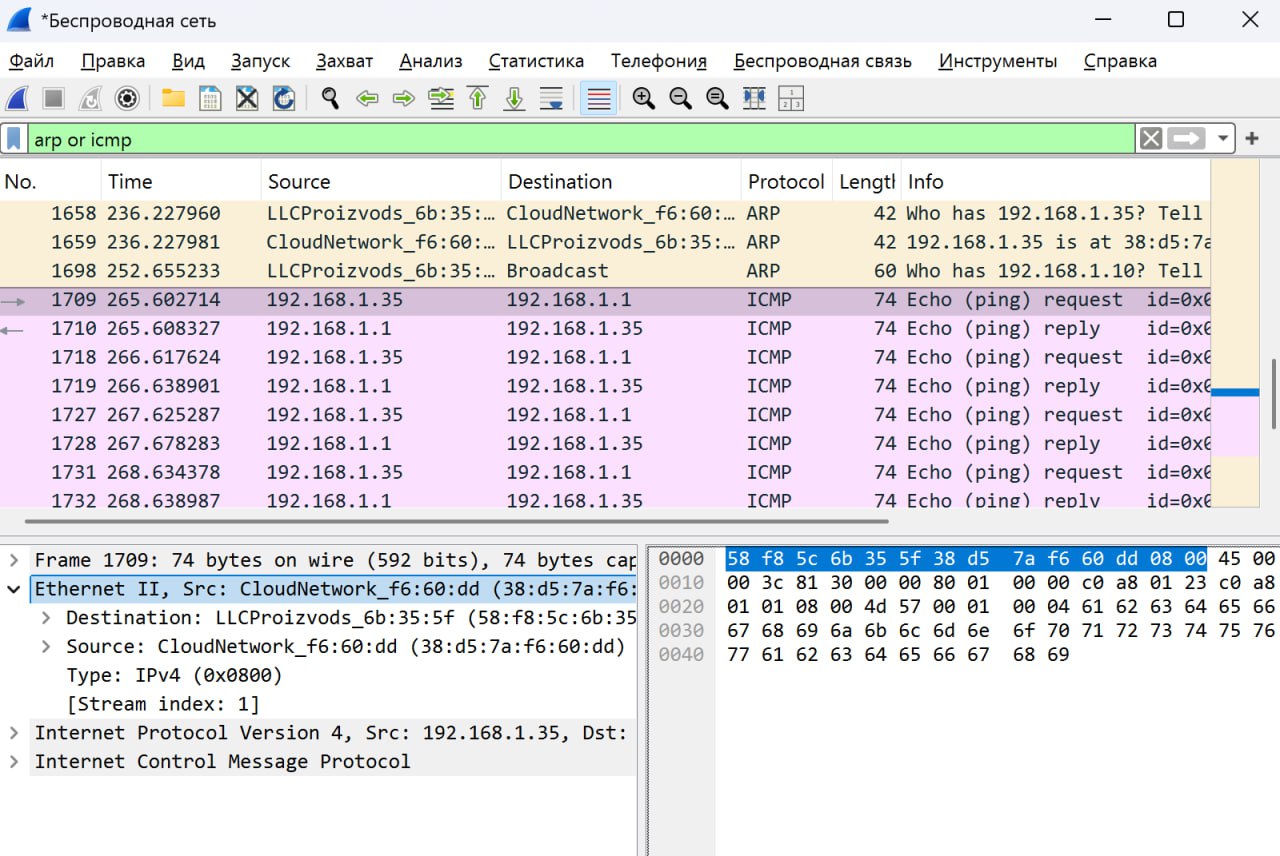


Рис. 11: Эхо-запрос

– На панели списка пакетов (верхний раздел) выберем второй указанный кадр ICMP — эхо-ответ. (рис. 12)

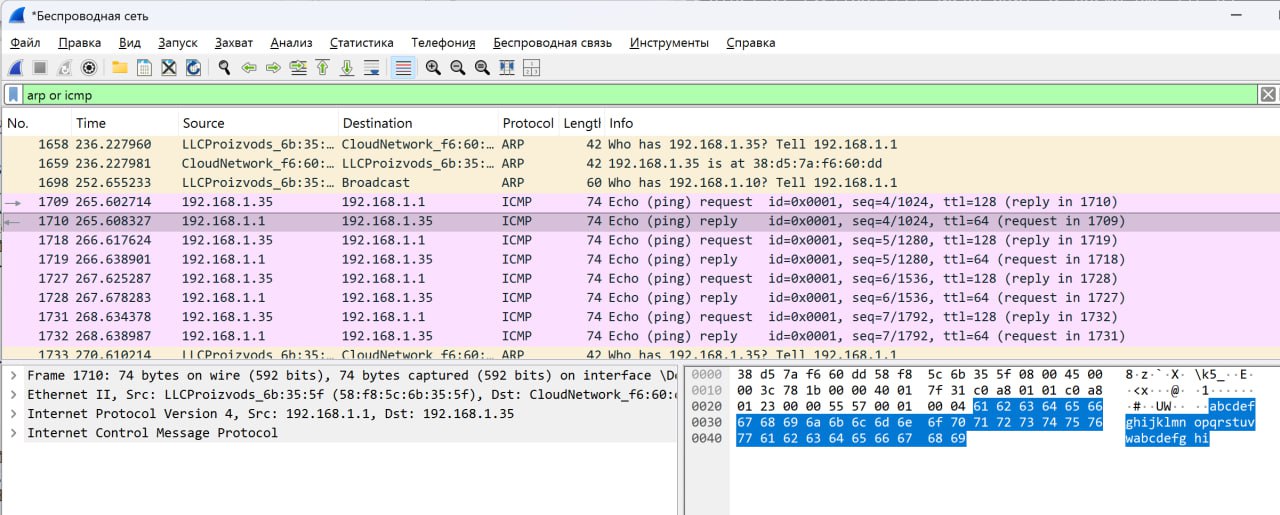


Рис. 12: Эхо-ответ

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. 13)

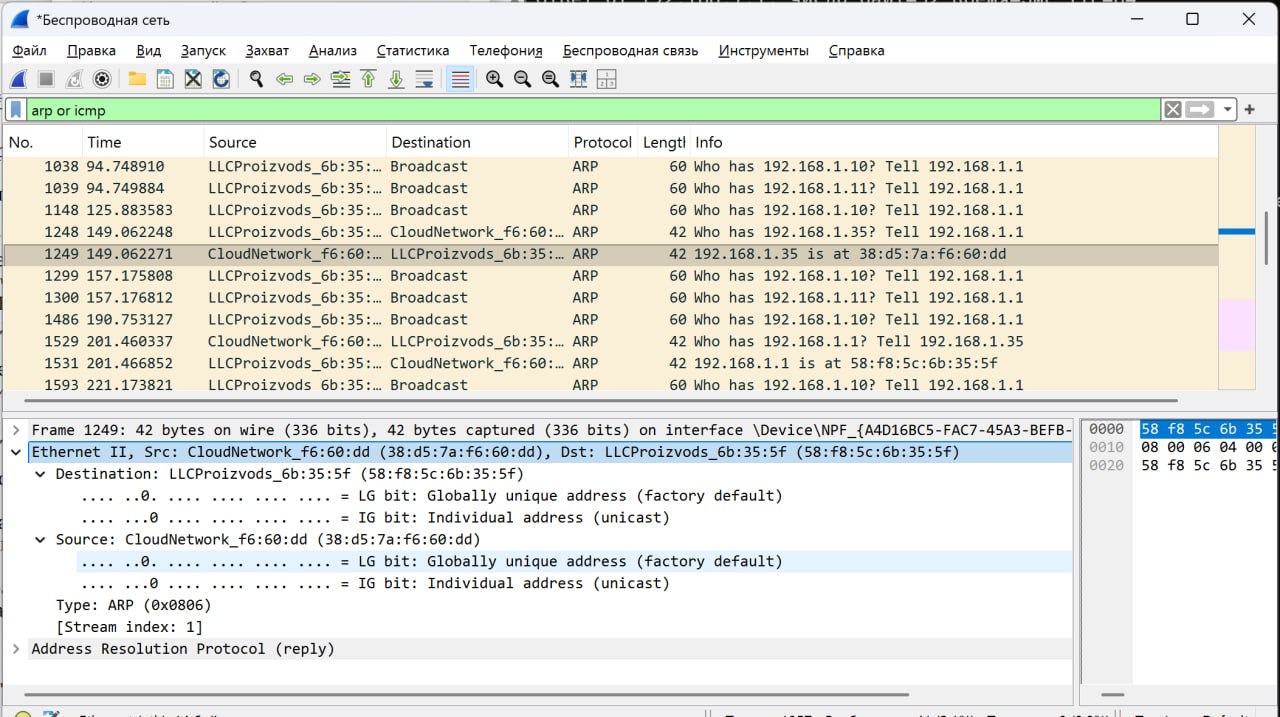


Рис. 13: Кадры протокола ARP

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. 14 и рис. 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.

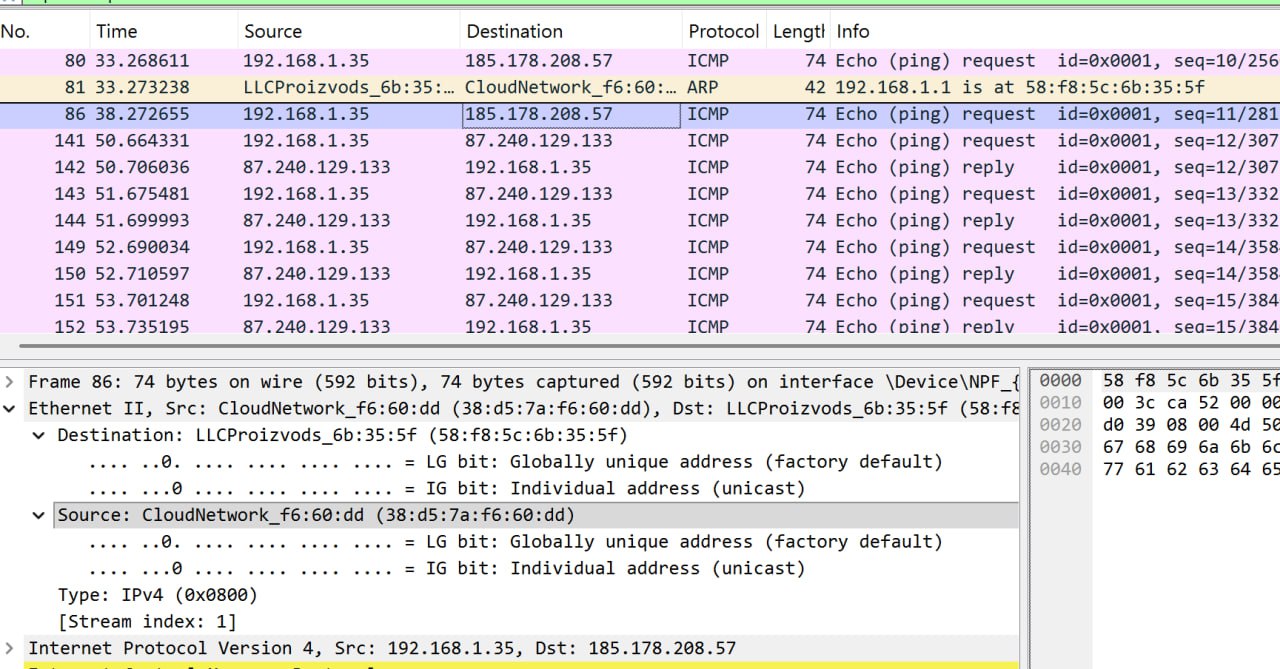


Рис. 14: Запрос

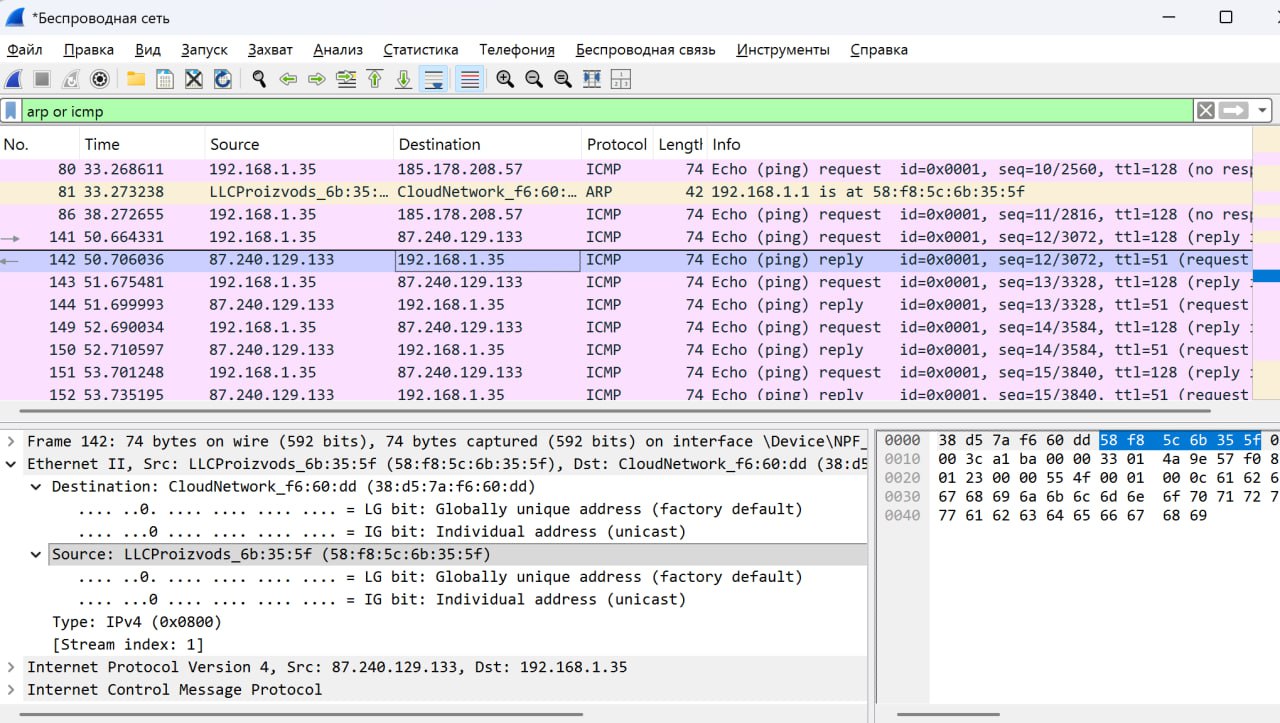


Рис. 15: Ответ

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. 16, рис. 17 и рис. 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 пактов - initial(c основными данными), handshake.

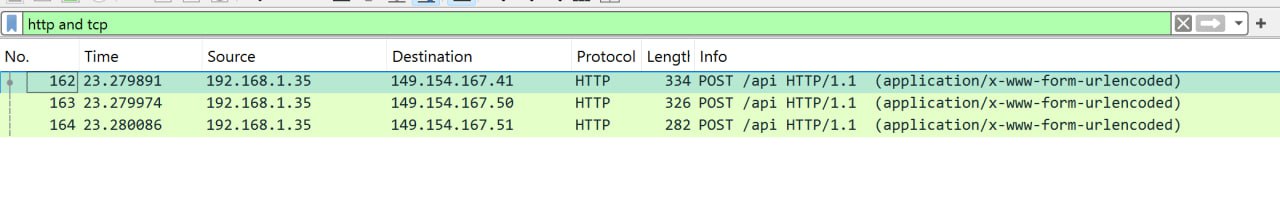


Рис. 16: HTTP

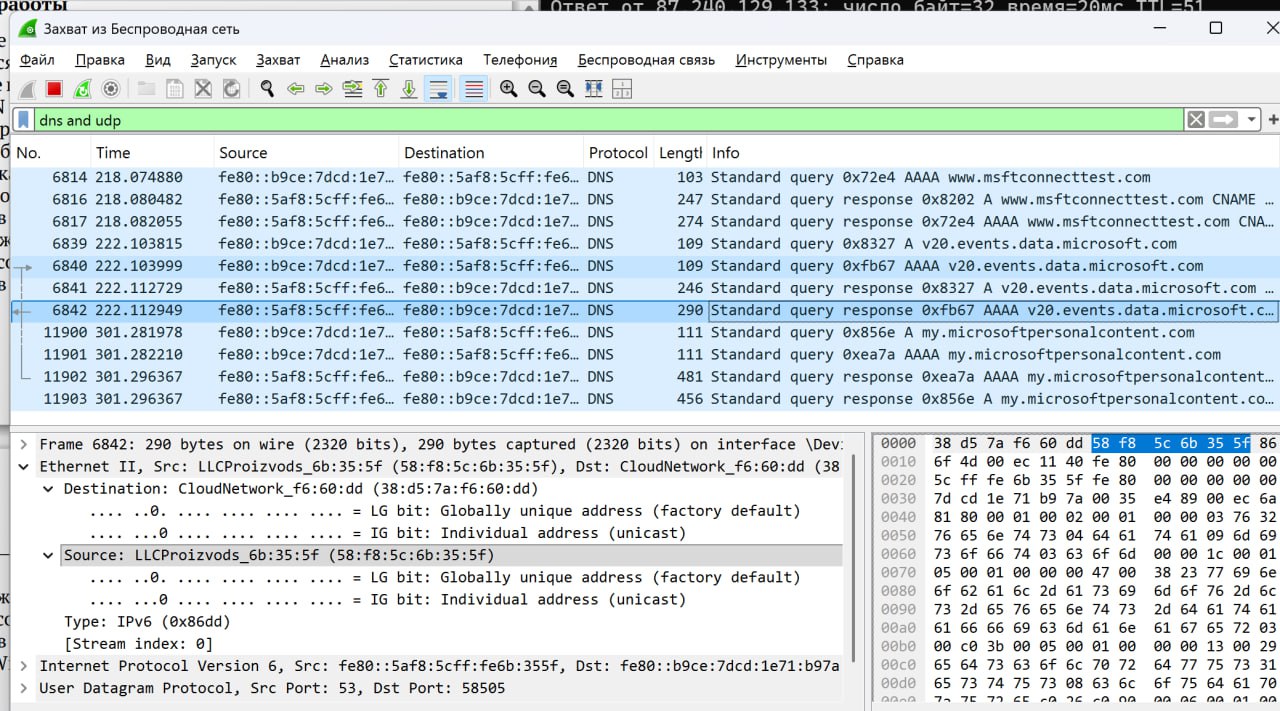


Рис. 17: DNS

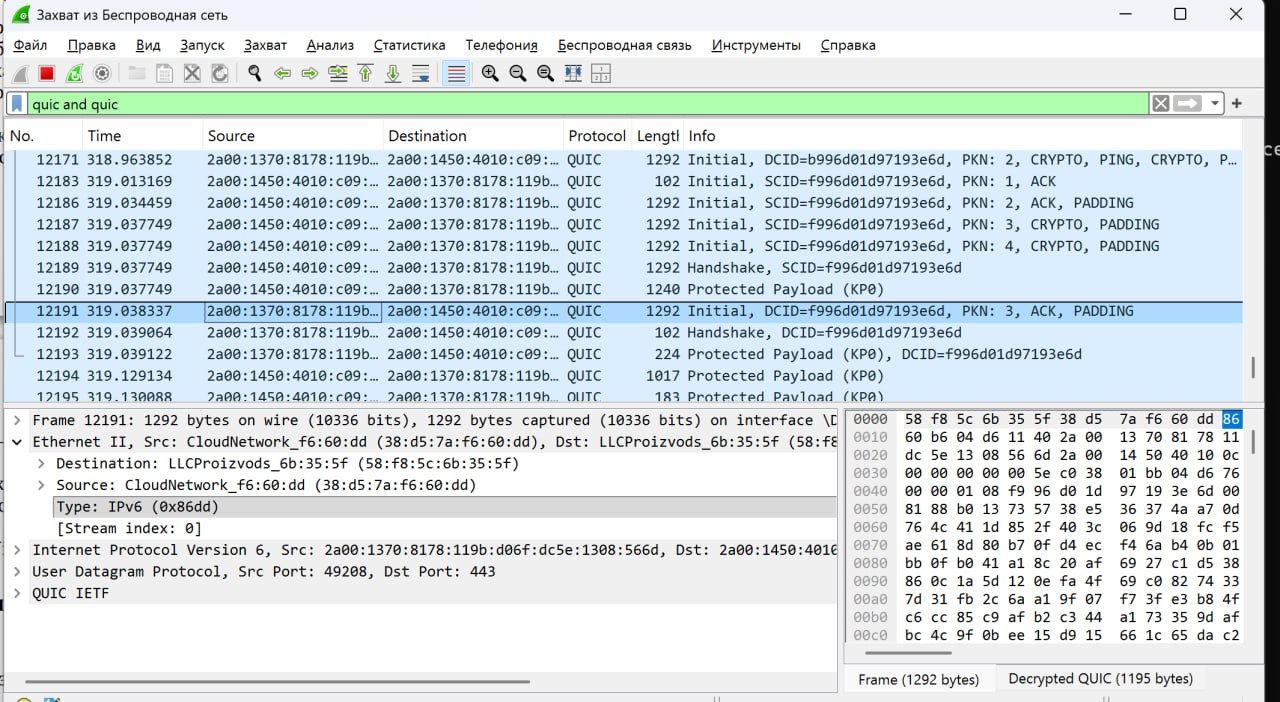


Рис. 18: QUIC

Проанализируем отдельно handshake protocol TCP.

Также захватим трафик, используем HTTP соединения и посмотрим на данные(рис. 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.

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

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

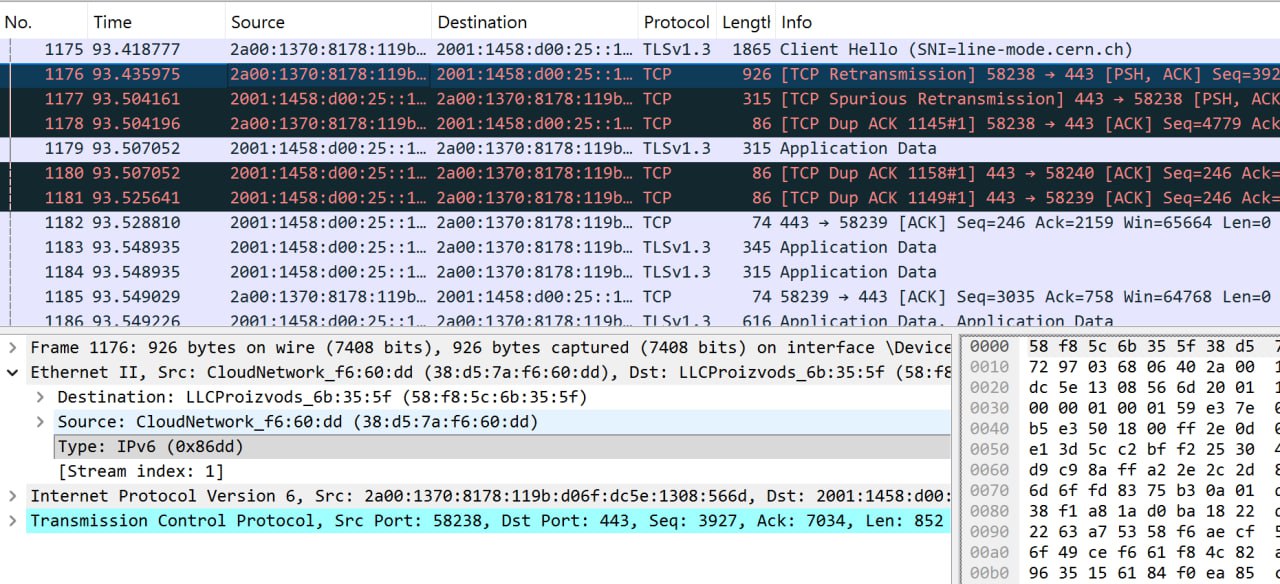


Рис. 19: Просмотр перехвата

Далее просмотрим график потока в меню статистика и ознакомимся с информацией(рис. 20). Остановим захват.

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

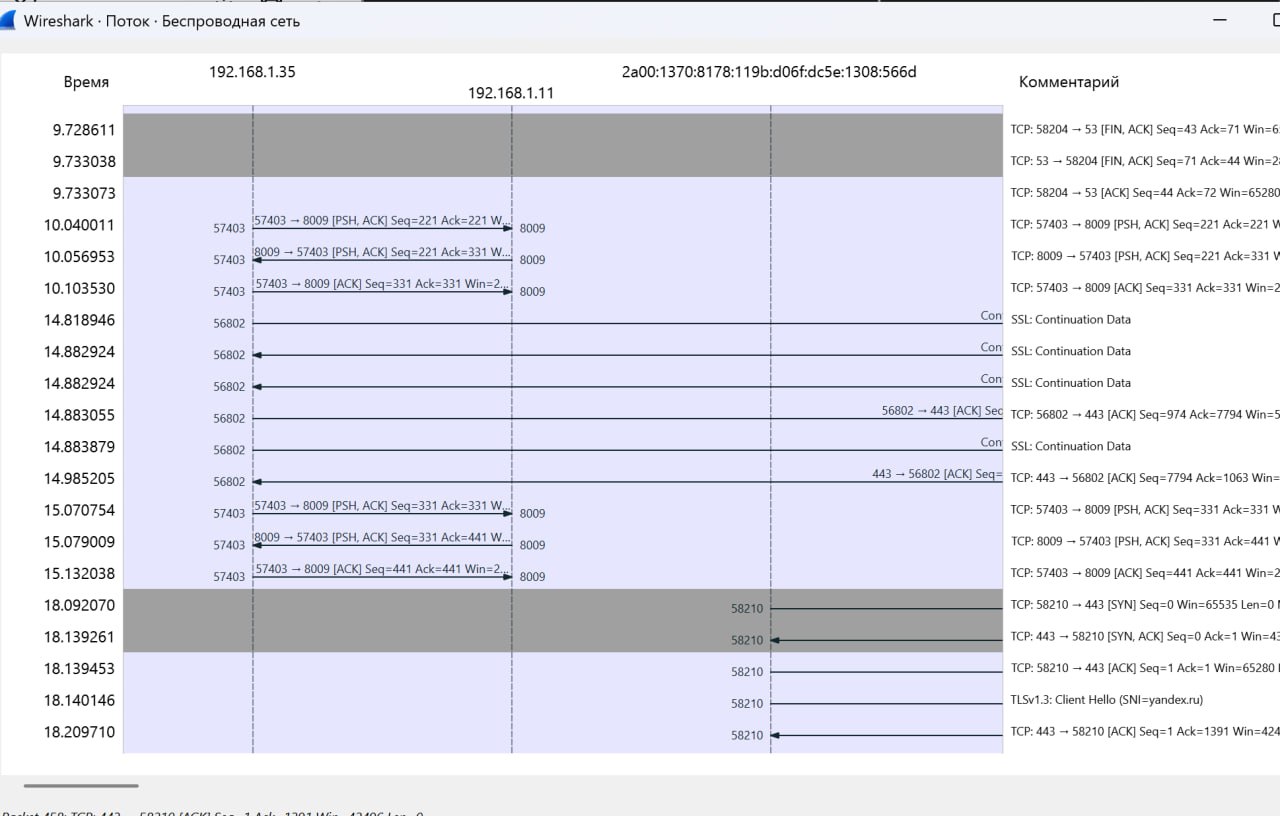


Рис. 20: График потока

# 3 Выводы

В ходе работы было произведено знакомство с Wireshark, были изучены с его помощью кадры Ethernet, произведенр 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)