**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЁТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №3**

*дисциплина: Сетевые технологии*

Студент: Бансимба Клодели Дьегра

Студ. билет № 1032215651

Группа: НПИбд-02-22

**МОСКВА**

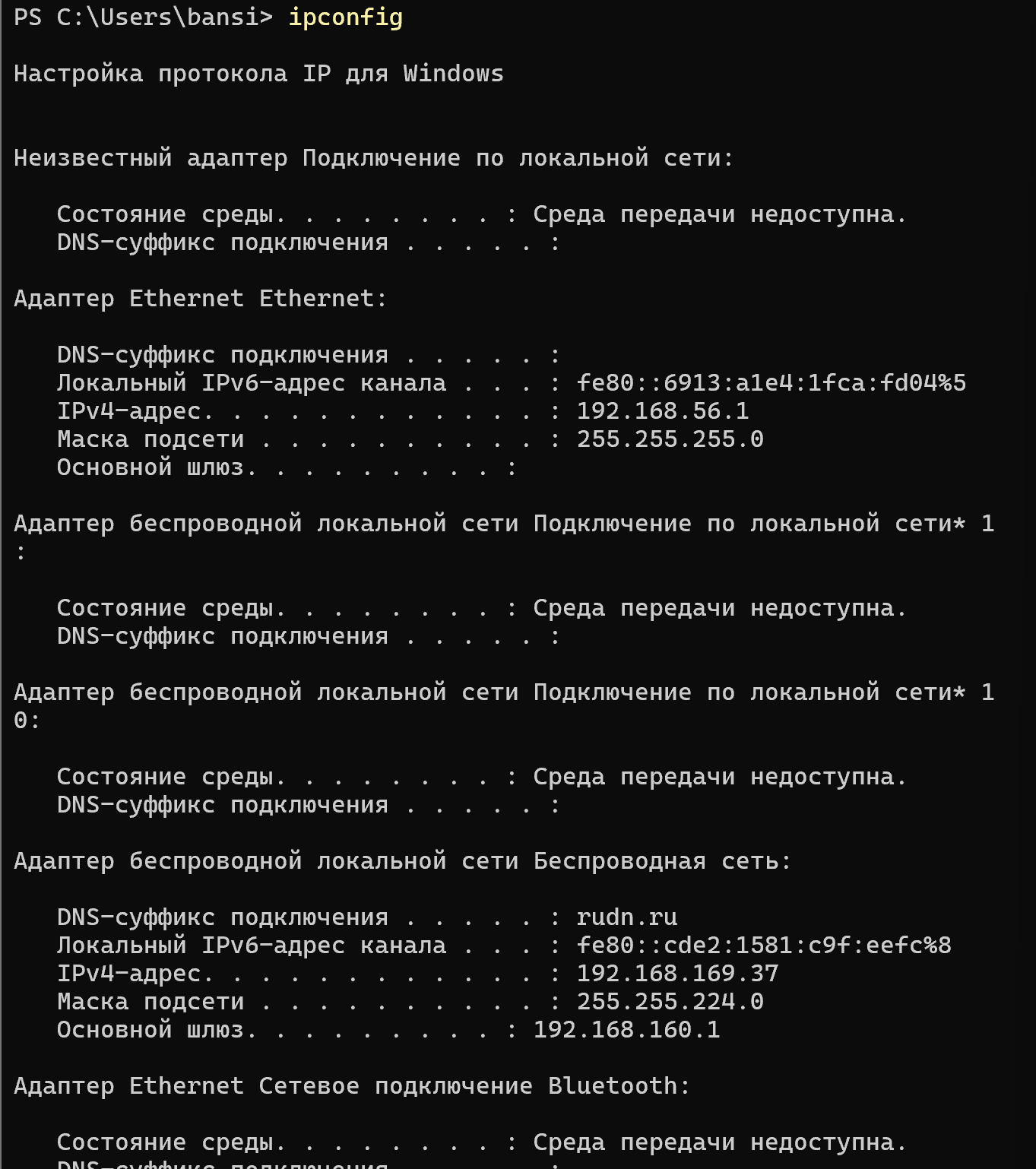
2024 г.

# Цель работы:

# Целью данной работы является изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

**Выполнение работы:**

С помощью команды ipconfig выведем информацию о текущем сетевом соединении (Рис. 1.1):

****

**Рис. 1.1.** Вывод информации о текущем сетевом соединении.

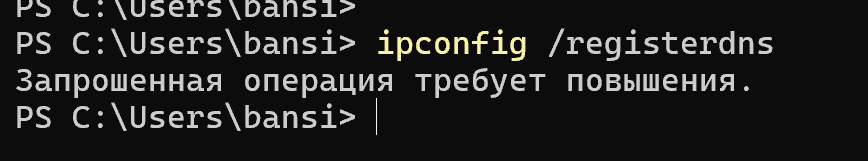
Теперь используем разные опции команды (Рис. 1.2-1.5):

****

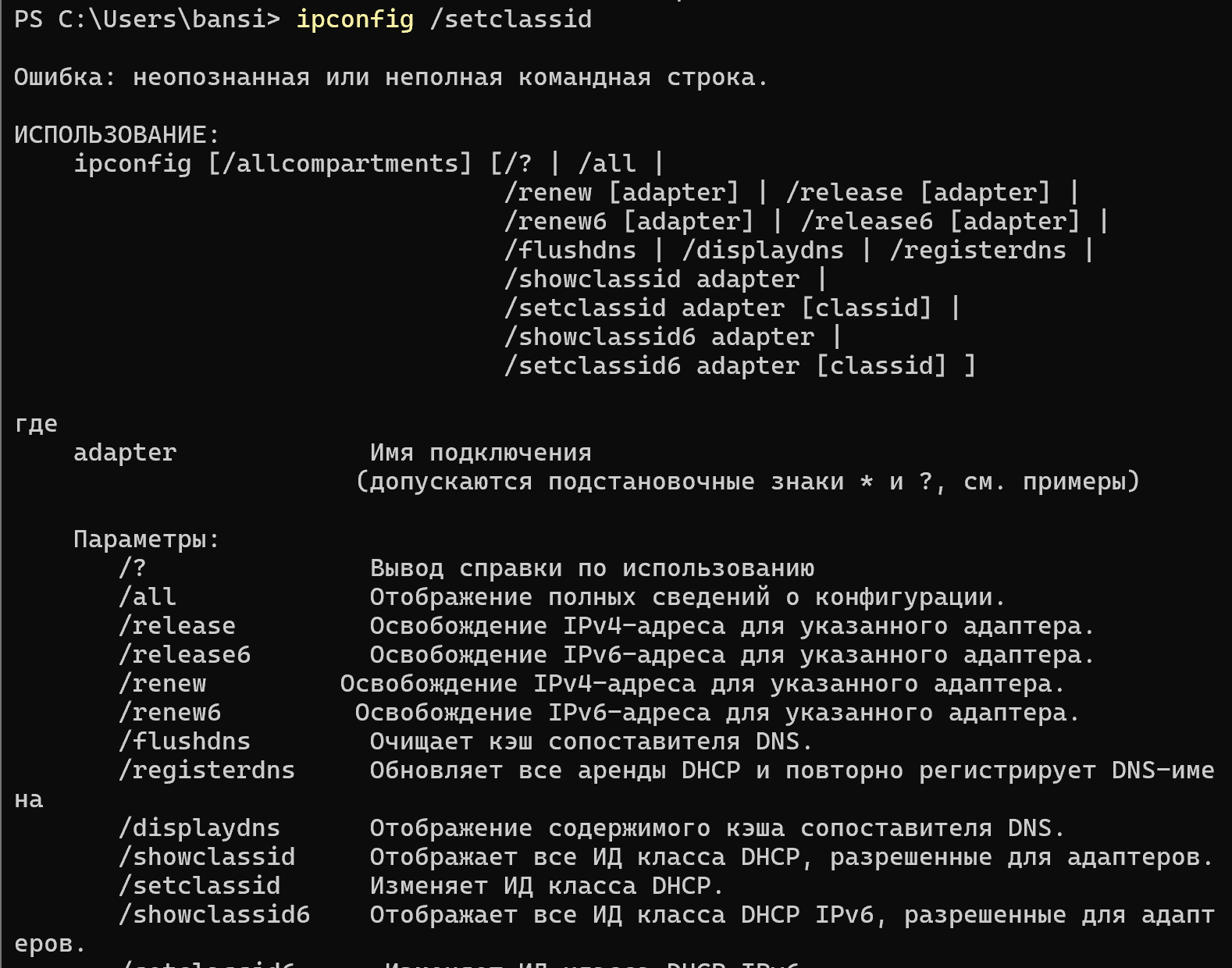
**Рис. 1.2.** Отображение полной конфигурации TCP/IP для всех адаптеров.

****

**Рис. 1.3.** Отображение содержимого кэша сопоставителя DNS-клиента, включающее как записи, предварительно загруженные из локального файла Hosts, так и все недавно полученные записи ресурсов для запросов имен, разрешенных компьютером.

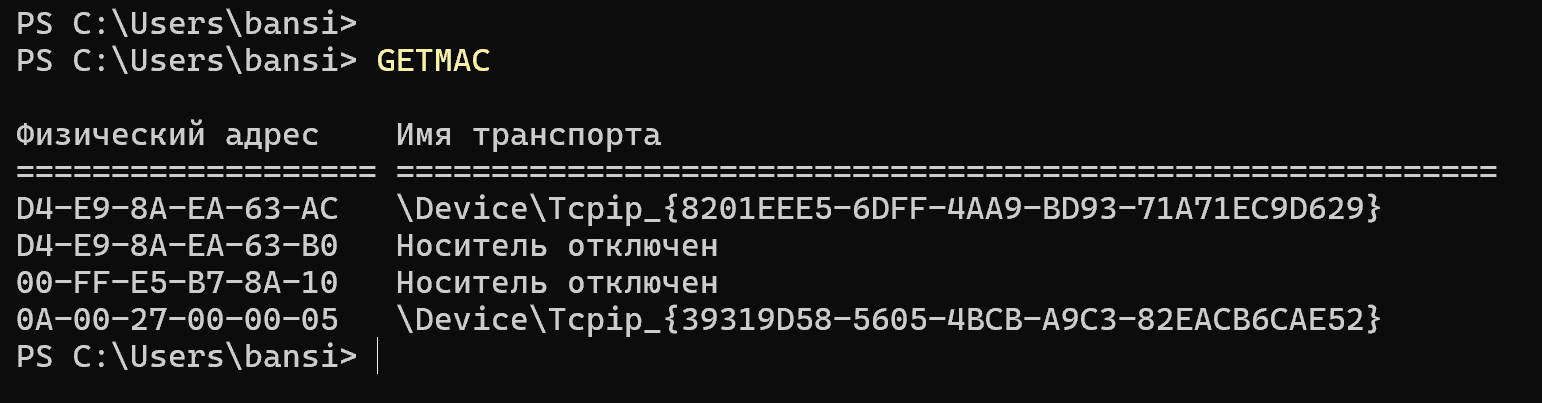
****

**Рис. 1.4.** Инициализация динамической регистрации вручную для DNS-имен и IP-адресов, настроенных на компьютере.



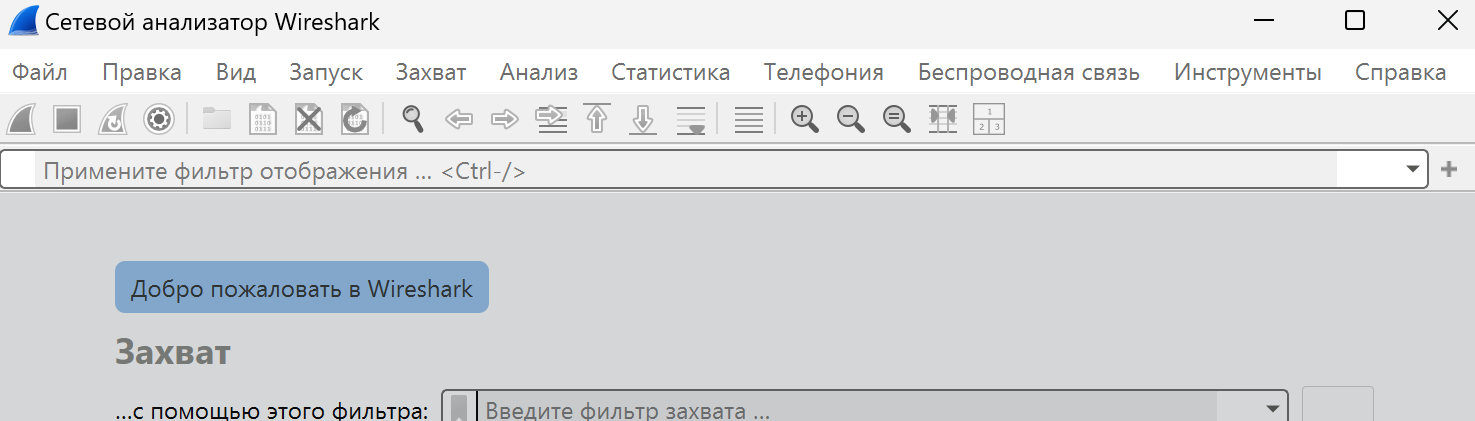
**Рис. 1.5.** Отображение идентификатора класса DHCP для указанного адаптера.

Определим MAC-адреса сетевых интерфейсов на нашем компьютере с помощью команды GETMAC. (Рис. 1.6).



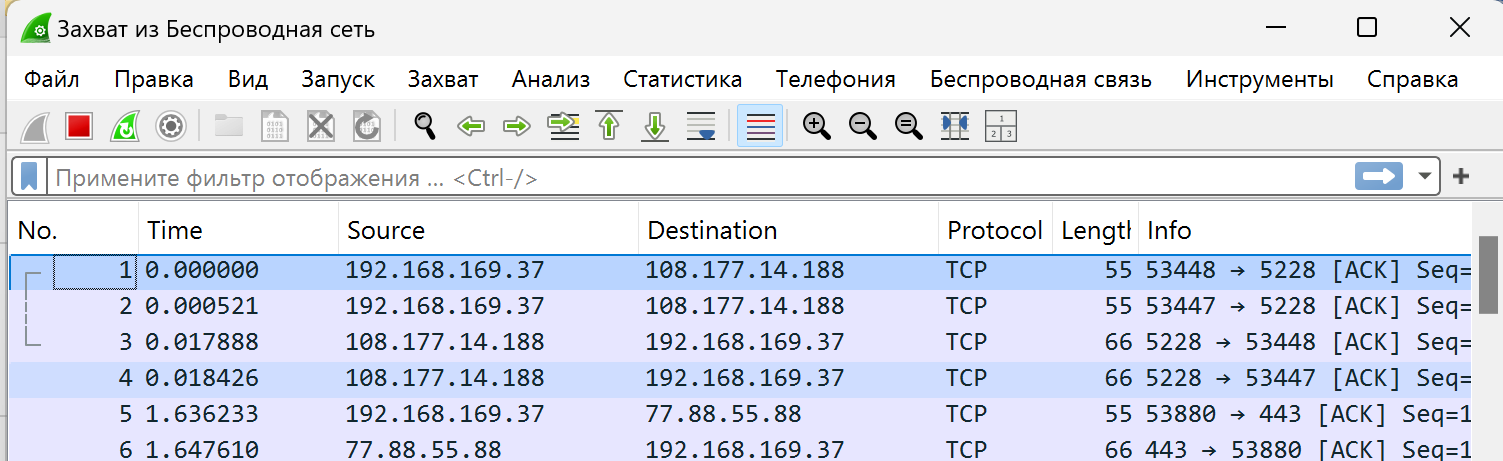
**Рис. 1.6.** Определение MAC-адреса сетевых интерфейсов на нашем компьютере.

Установим на нашем устройстве Wireshark (Рис. 2.1).



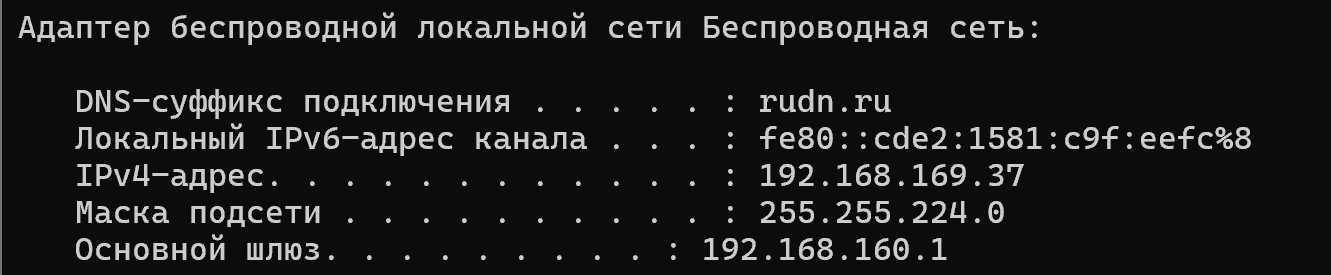
**Рис. 2.1.** Установка на нашем устройстве Wireshark.

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика (Рис. 2.2).

****

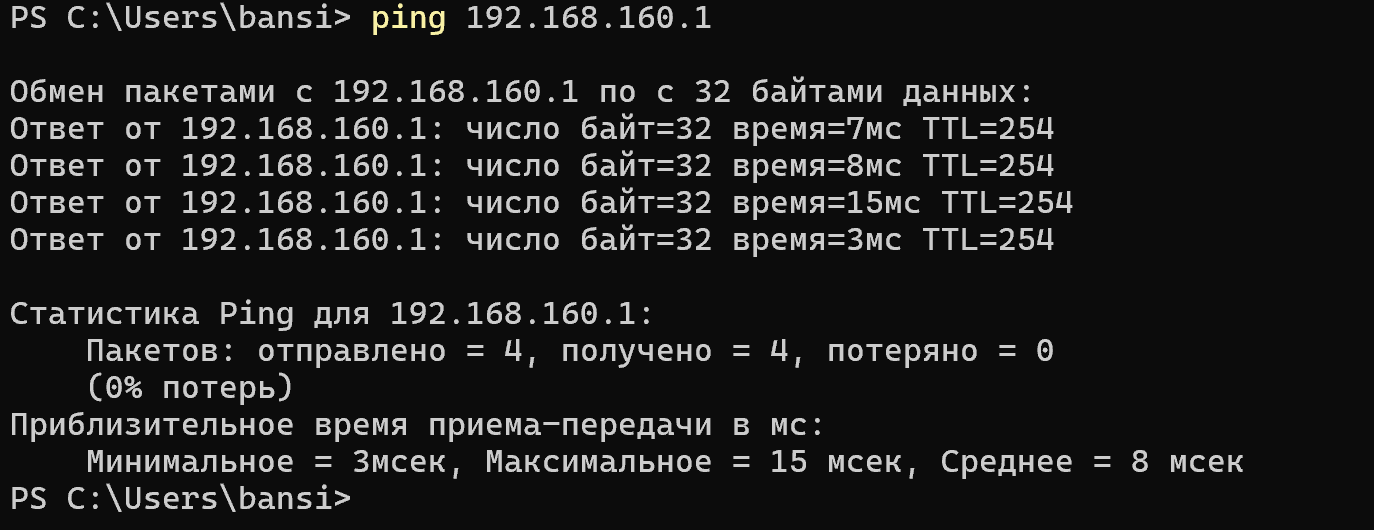
**Рис. 2.2.** Запуск Wireshark. Выбор активного сетевого интерфейса.

На нашем устройстве в консоли определим с помощью команды ipconfig IP-адрес устройства и шлюз по умолчанию (Рис. 2.3).



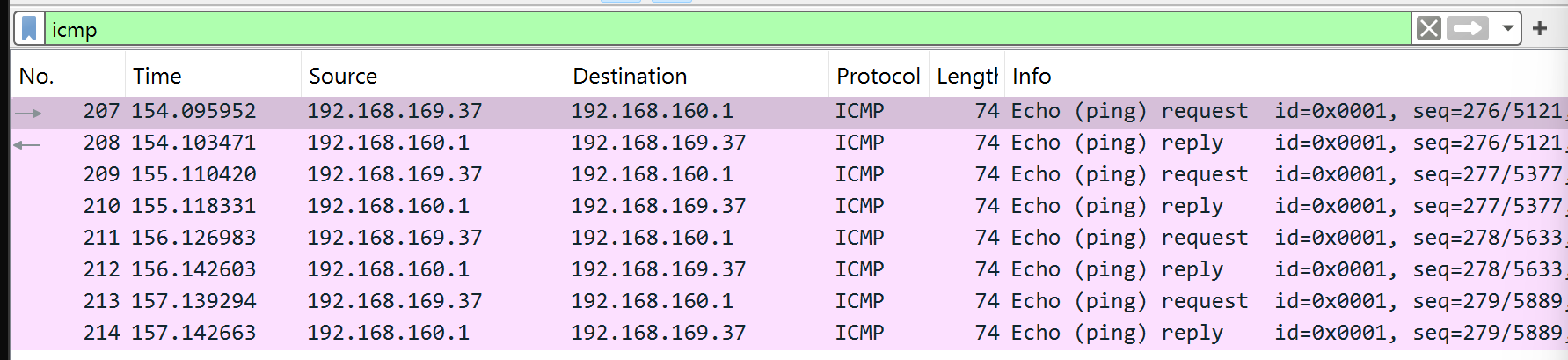
**Рис. 2.3.** Определение IP-адреса устройства и шлюза по умолчанию.

На нашем устройстве в консоли с помощью команды ping 192.168.160.1 пропингуем шлюз по умолчанию (Рис. 2.4).

****

**Рис. 2.4.** Пинг шлюза по умолчанию.

В Wireshark остановим захват трафика. В строке фильтра пропишем фильтр arp or icmp и убедимся, что в списке пакетов отобразились только пакеты ARP или ICMP, в частности пакеты, которые были сгенерированы с помощью команды ping, отправленной с нашего устройства на шлюз по умолчанию (Рис. 2.5).

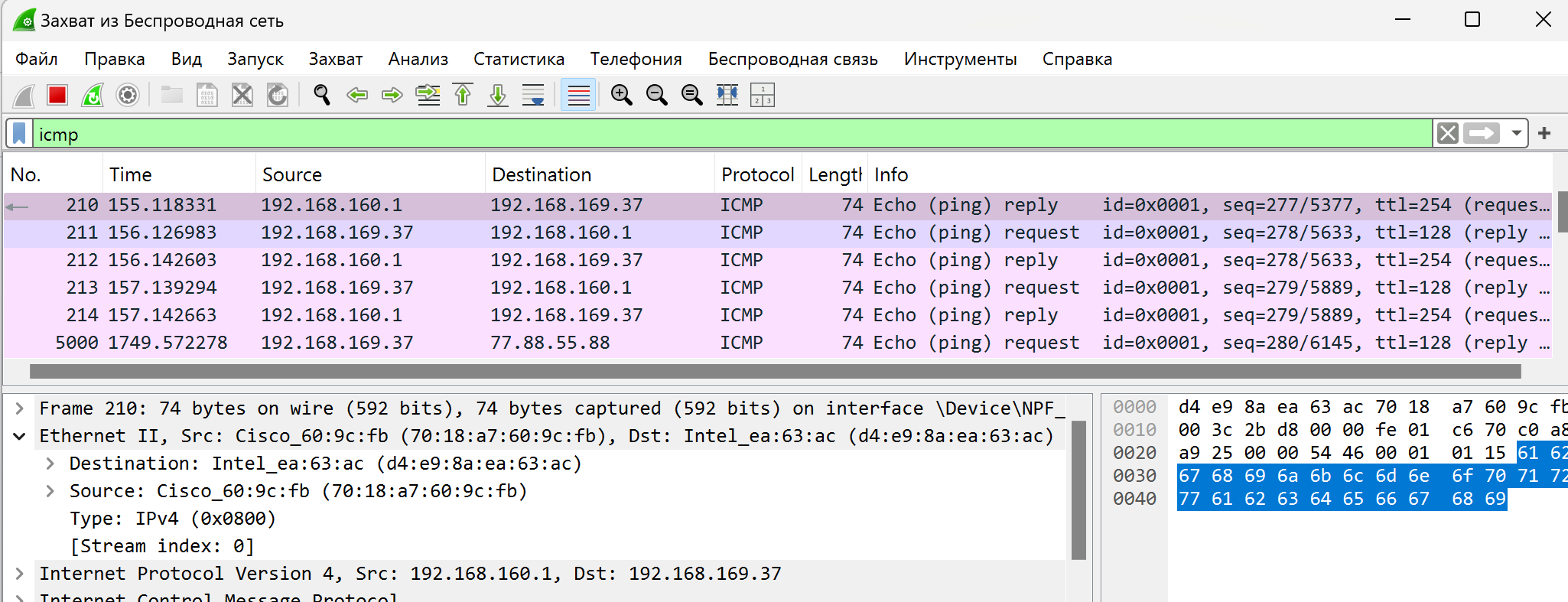
****

**Рис. 2.5.** Остановка захвата трафика. Фильтр arp or icmp.

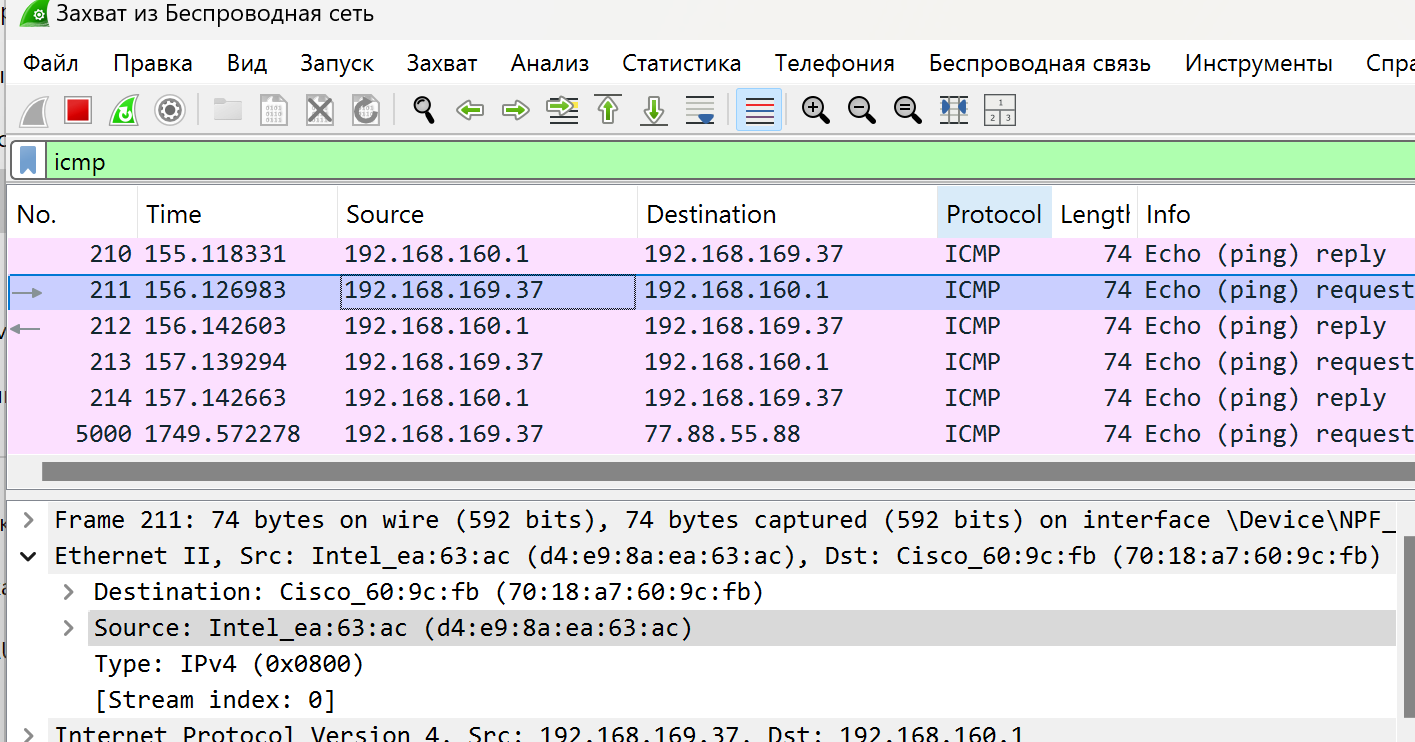
Изучим эхо-запрос и эхо-ответ ICMP в программе Wireshark:

– На панели списка пакетов выберем первый указанный кадр ICMP — эхо-запрос. 770:18:a7:60:9c:fb - MAC-адрес. Globally unique address, individual address (Рис. 2.6).

– На панели списка пакетов выберем второй указанный кадр ICMP — эхо-ответ. d4:e9:8a:ea:63:ac - MAC-адрес. Globally unique address, individual address (Рис. 2.7).

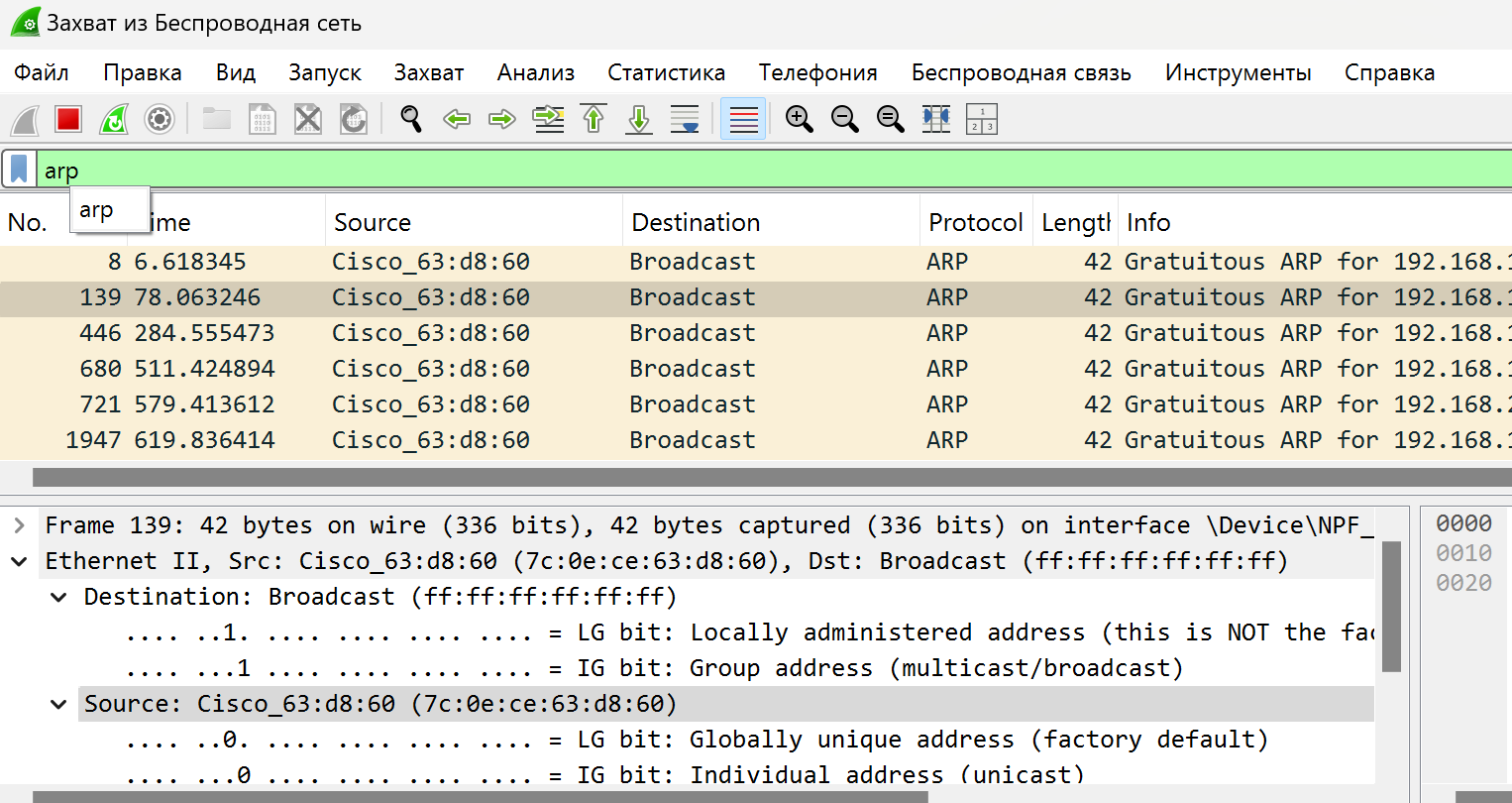


**Рис. 2.6.** Кадр ICMP — эхо-запрос.



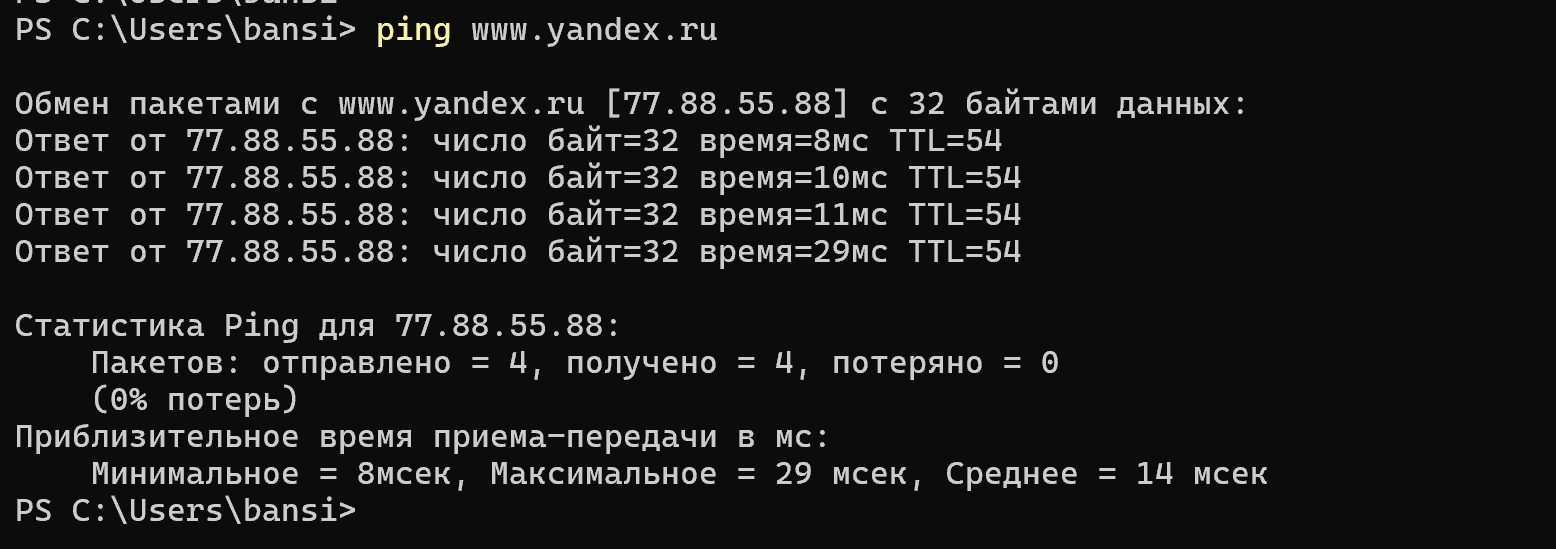
**Рис. 2.7.** Кадр ICMP — эхо-ответ.

Изучим кадры данных протокола ARP и данные в полях заголовка Ethernet II (Рис. 2.8).

****

**Рис. 2.8.** Изучение кадров данных протокола ARP и данных в полях заголовка Ethernet II.

Начнём новый процесс захвата трафика в Wireshark. На нашем устройстве в консоли пропингуем по имени адрес ping www.yandex.ru (Рис. 2.9).

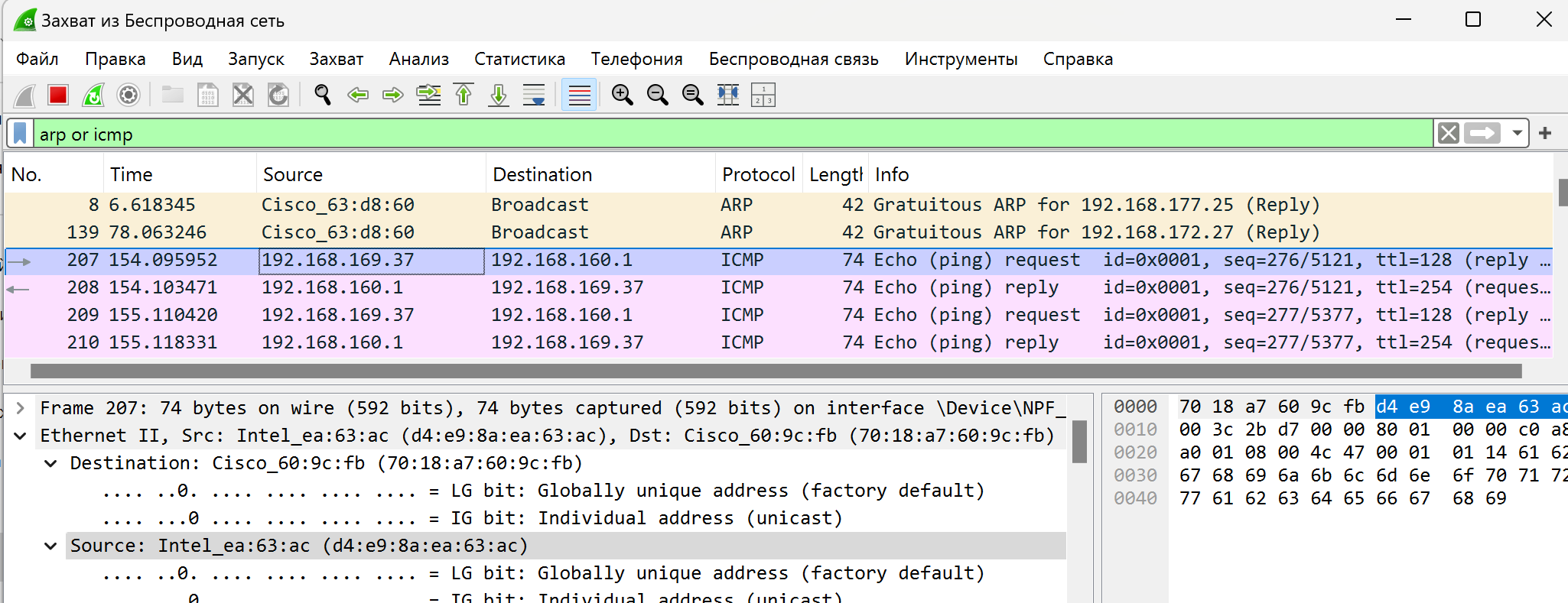


**Рис. 2.9.** Пингуем по имени адрес vk.com.

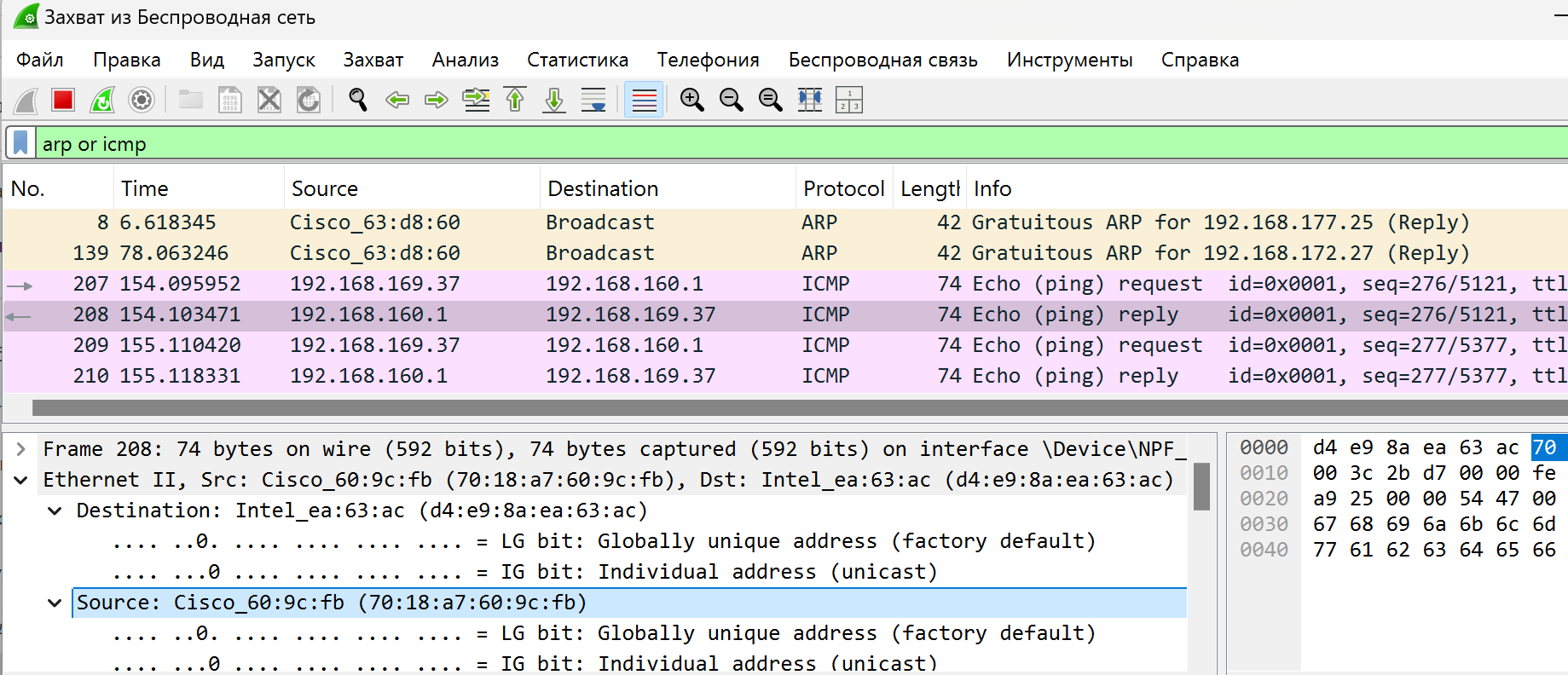
В Wireshark остановим захват трафика. Изучим запросы и ответы протоколов ARP и ICMP.

d4:e9:8a:ea:63:ac - MAC-адрес источника, Globally unique address, individual address (Рис. 2.10).

70:18:a7:60:9c:fb - MAC-адрес получателя, Globally unique address, individual address (Рис. 2.11).

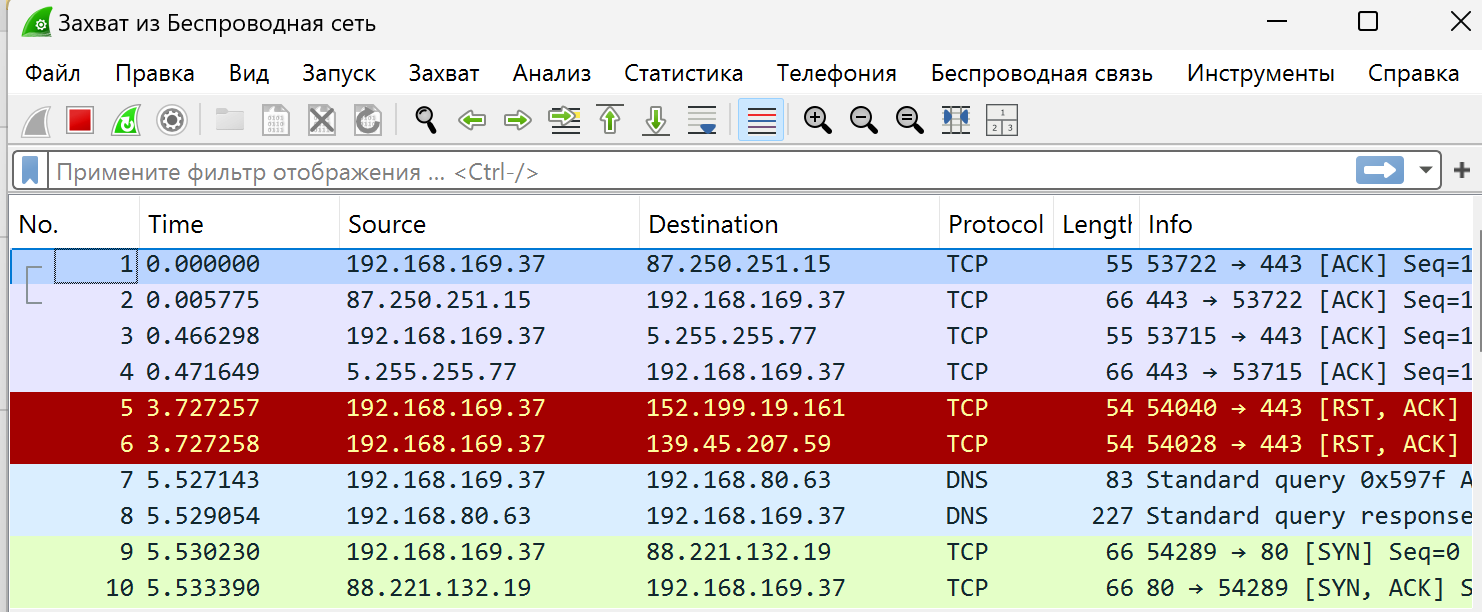


**Рис. 2.10.** MAC-адрес источника.



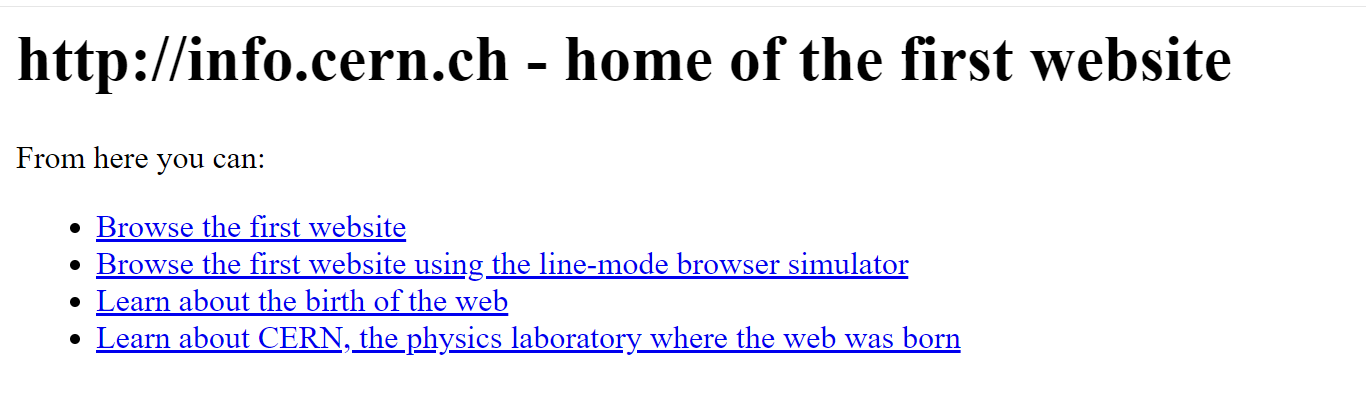
**Рис. 2.11.** MAC-адрес получателя.

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика (Рис. 3.1).

****

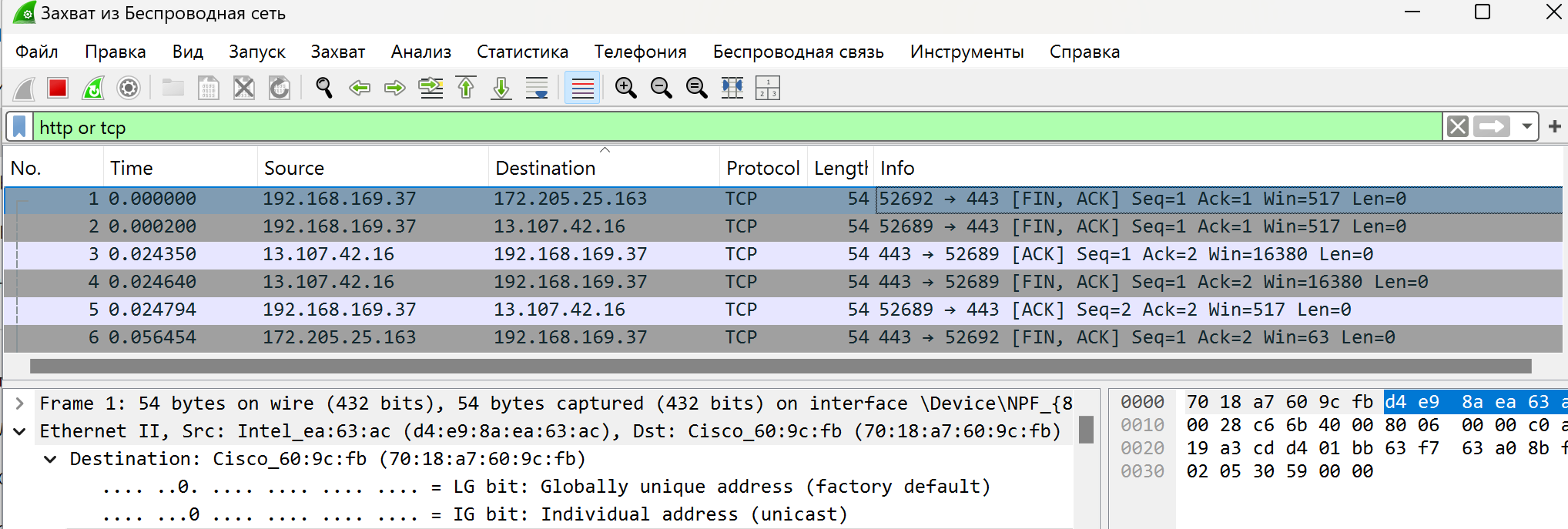
**Рис. 3.1.** Запуск Wireshark. Выбор активного сетевого интерфейса.

На устройстве в браузере перейдём на сайт, работающий по протоколу HTTP (<http://info.cern.ch/>) и поперемещаемся по ссылкам и разделам сайта в браузере (Рис. 3.2).



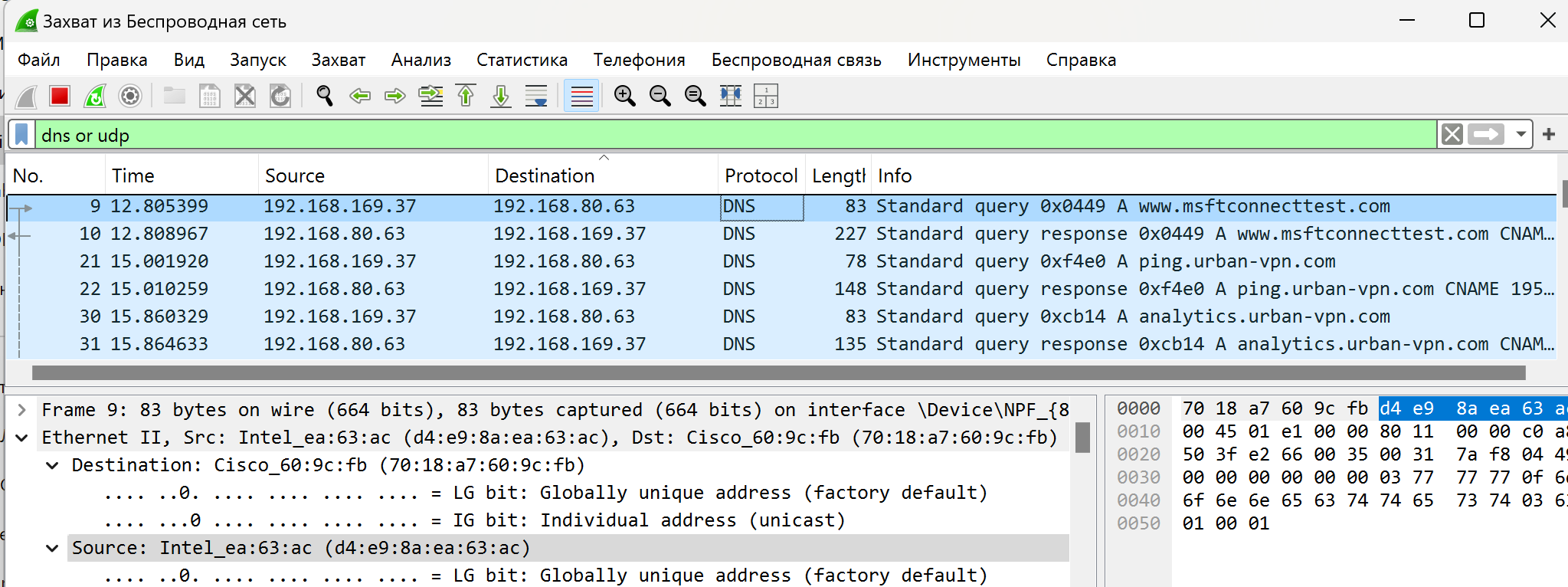
**Рис. 3.2.** Открытие в браузере сайта CERN.

В Wireshark в строке фильтра укажем http и проанализируем информацию по протоколу TCP в случае запросов и ответов (Рис. 3.3).



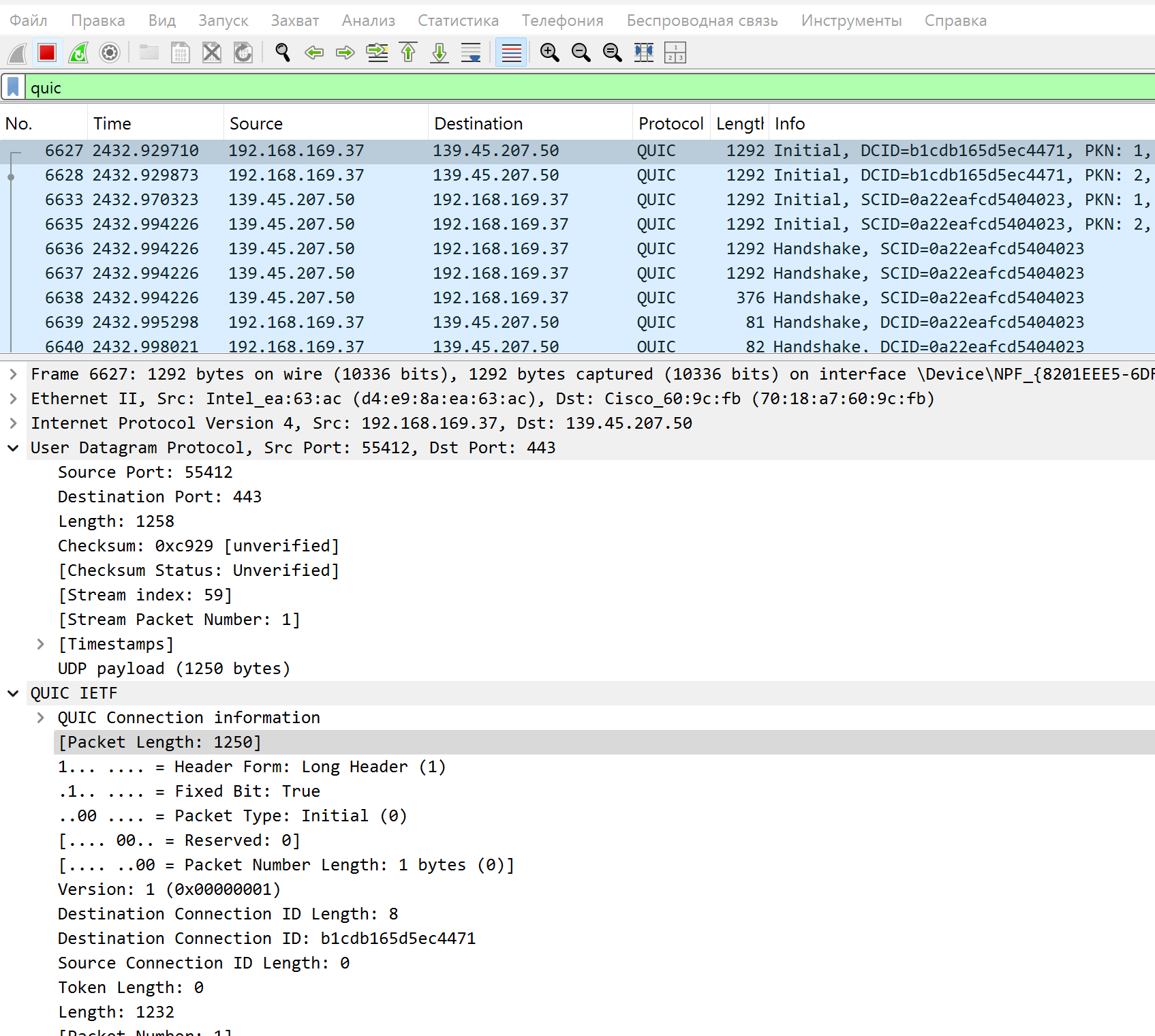
**Рис. 3.3.** Анализ информации по протоколу TCP.

В Wireshark в строке фильтра укажем dns и проанализируем информацию по протоколу UDP в случае запросов и ответов (Рис. 3.4).



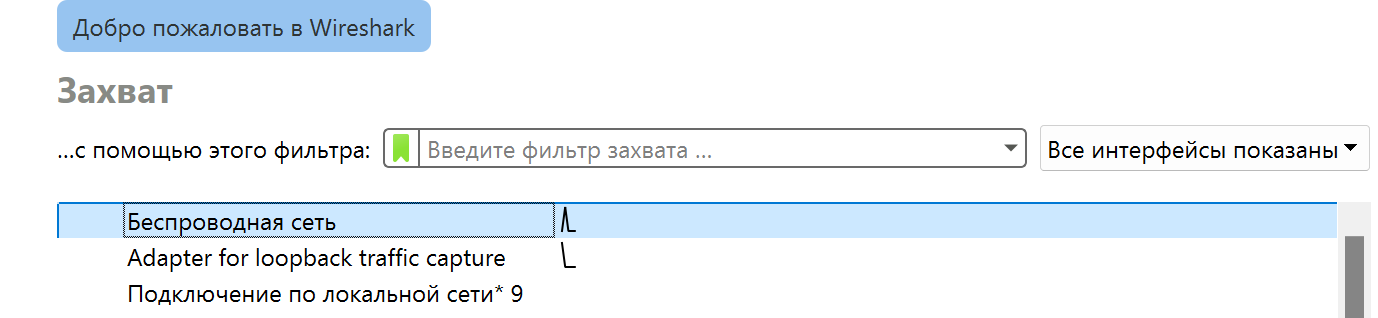
**Рис. 3.4.** Анализ информации по протоколу UDP.

В Wireshark в строке фильтра укажем quic и проанализируем информацию по протоколу quic в случае запросов и ответов (Рис. 3.5).

****

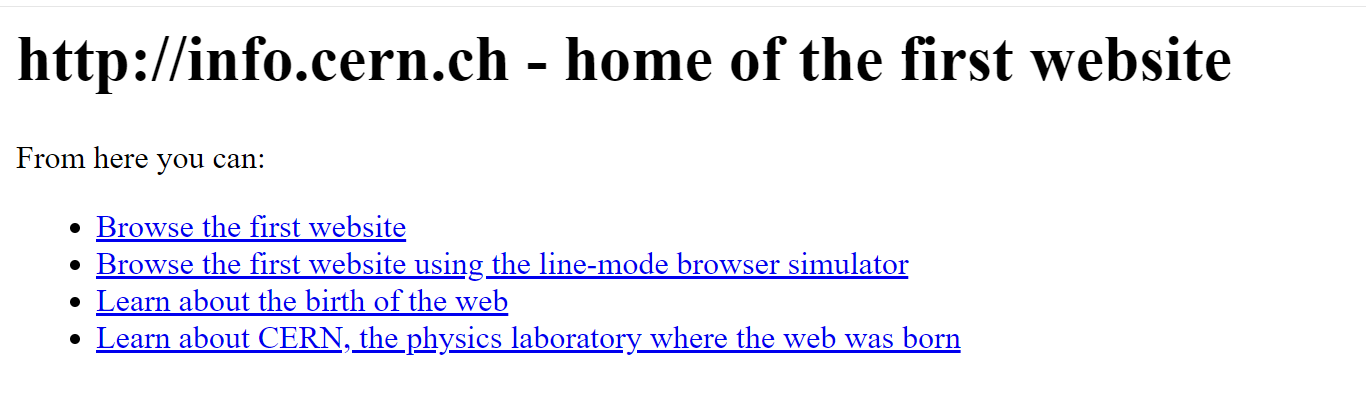
**Рис. 3.5.** Анализ информации по протоколу QUIC.

Запустим Wireshark. Выберем активный на нашем устройстве сетевой интерфейс и убедимся, что начался процесс захвата трафика (Рис. 4.1).



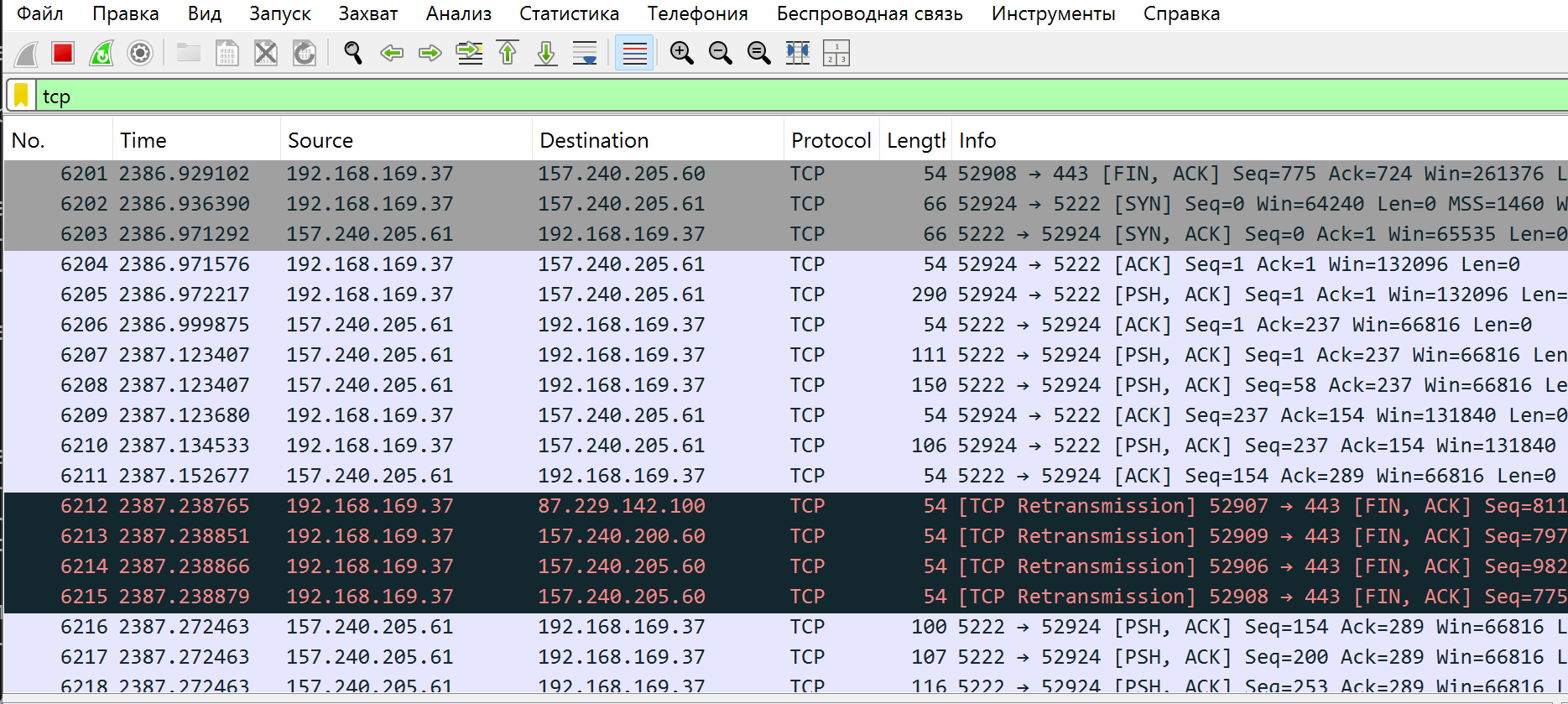
**Рис. 4.1.** Запуск Wireshark. Выбор активного сетевого интерфейса.

На устройстве используем соединение по HTTP с сайтом CERN для захвата в Wireshark пакетов TCP (Рис. 4.2).



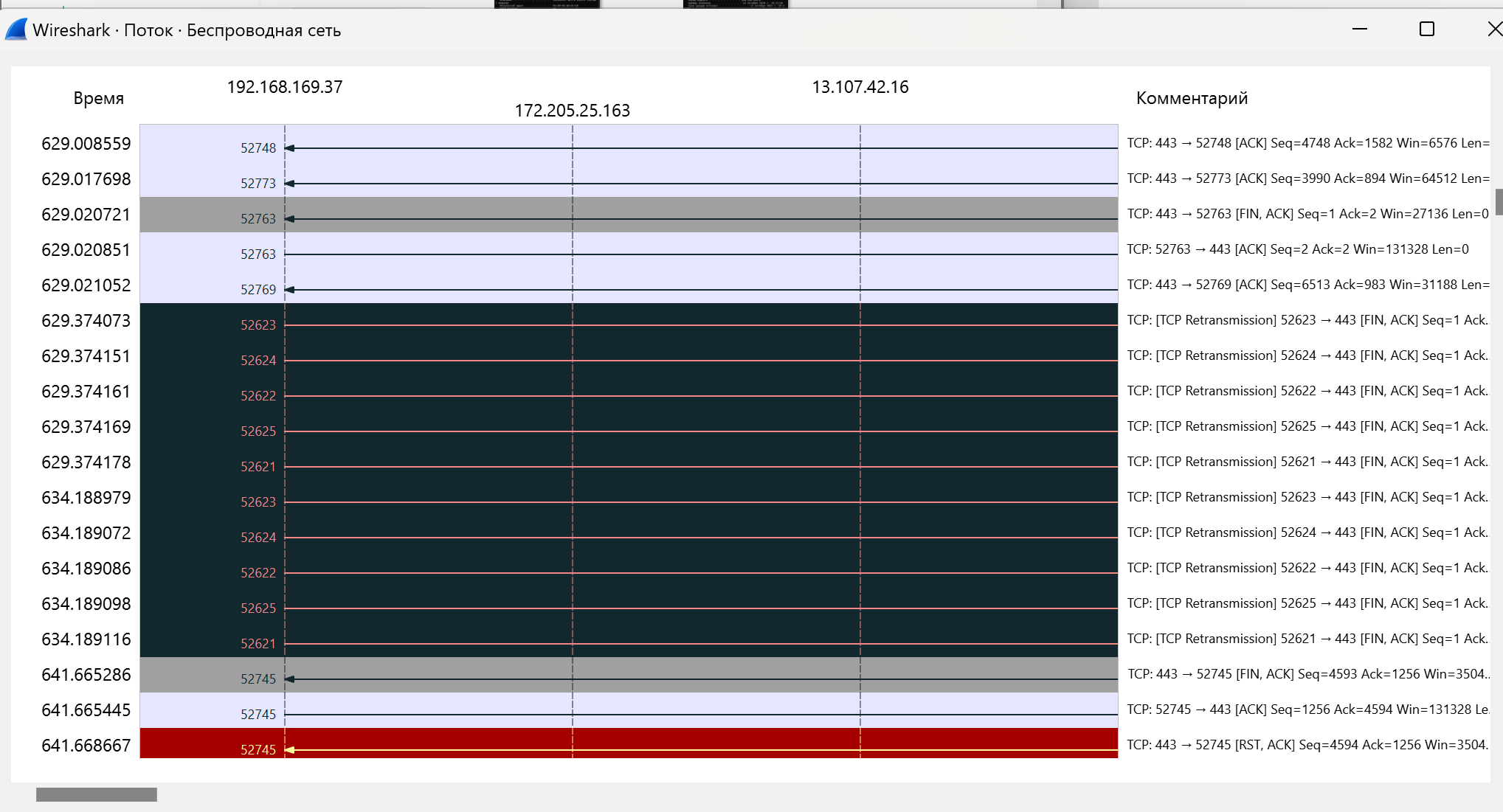
**Рис. 4.2.** Использование соединения по HTTP с сайтом CERN.

В Wireshark проанализируем handshake протокола TCP (Рис. 4.3).



**Рис. 4.3.** Анализ handshake протокола TCP.

В Wireshark в меню «Статистика» выберем «График Потока» (Рис. 4.4).



**Рис. 4.4.** График потока.

**Вывод:**

В ходе выполнения лабораторной работы мы изучили посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.