# Лабораторная работа №3

Тема «Анализ трафика в Wireshark»

по дисциплине «Сетевые технологии»

Выполнил: Щербак Маргарита Романовна

Студент группы: НПИбд-02-21

«22» сентября 2023г.

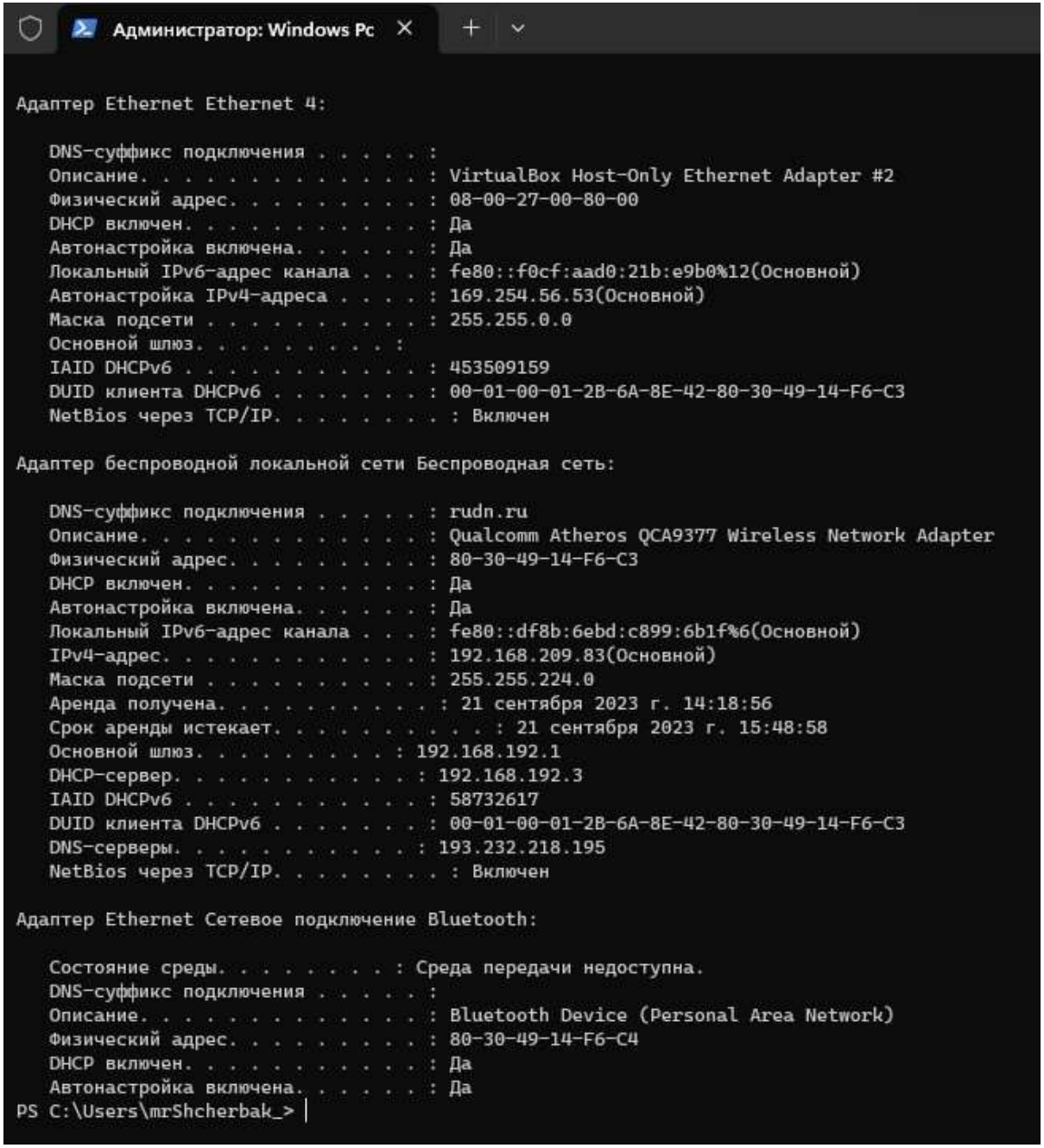
**Цели работы:**

Изучить посредством Wireshark кадры Ethernet, проанализировать PDU протоколы транспортного и прикладного уровней стека TCP/IP.

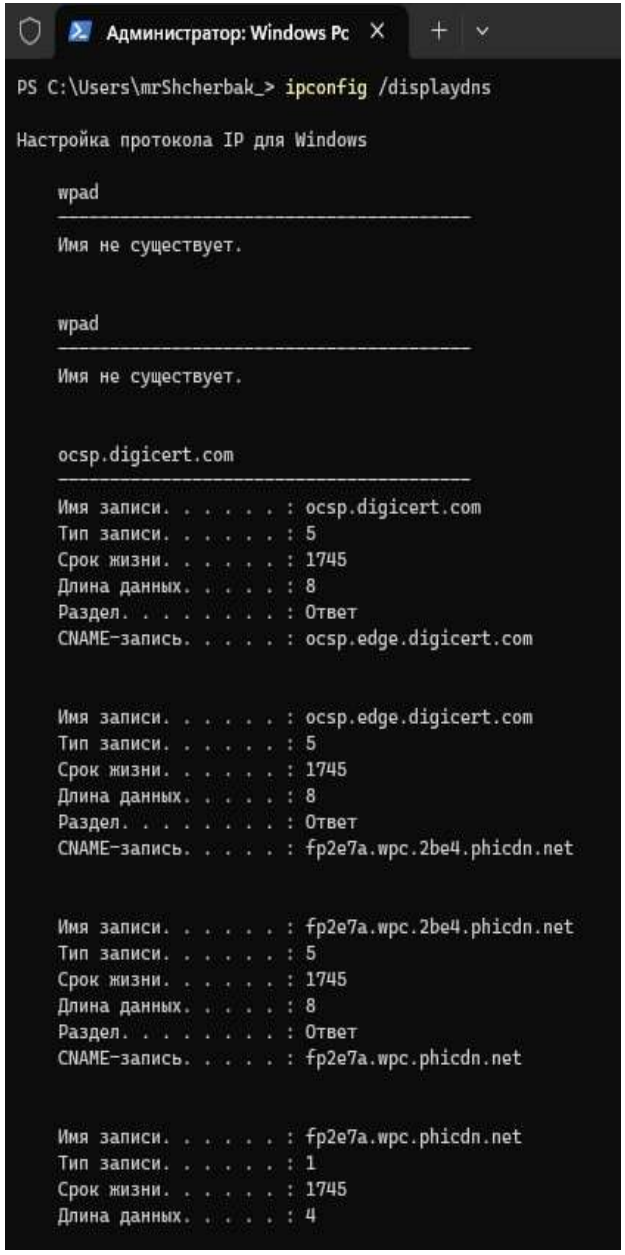
**Выполнение работы**

**MAC-адресация**

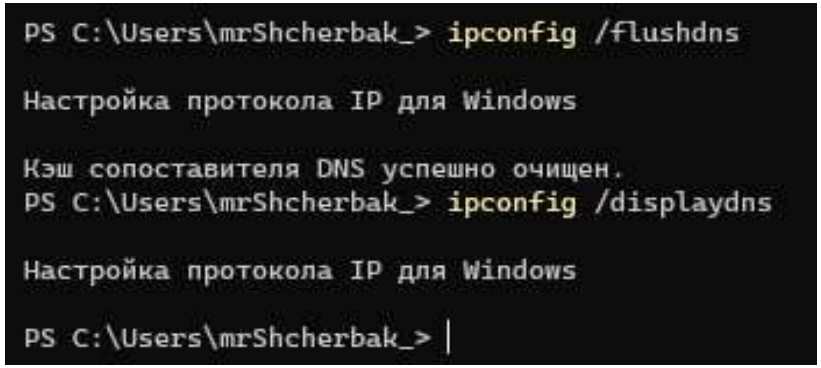
С помощью команды ipconfig я получила информацию о сетевых соединениях, включая Адаптеры Ethernet 3, Ethernet 4 и беспроводную сеть.



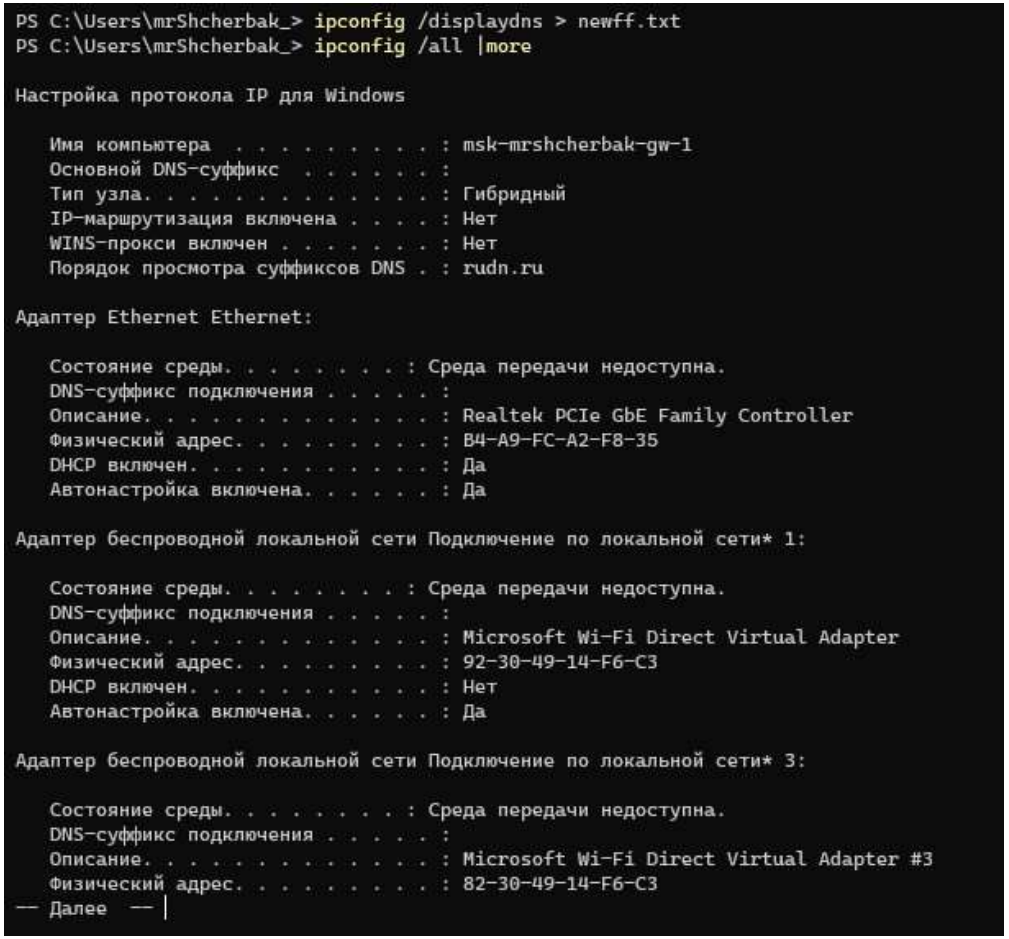

Вывод подробных сведений о конфигурации всех адаптеров

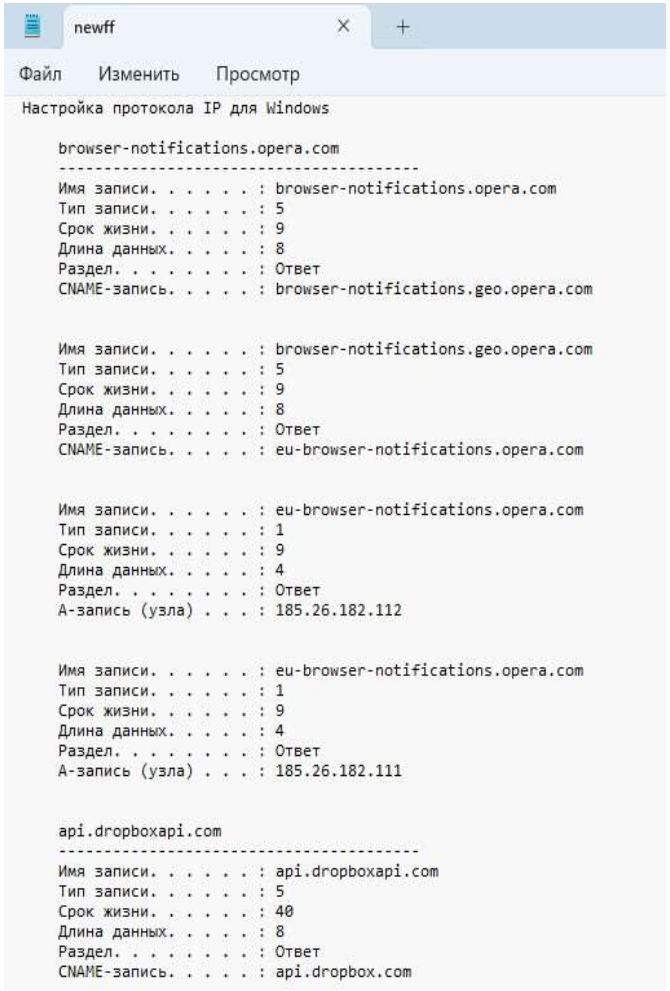



Выполнение команд ipconfig /displaydns и ipconfig /flushdns




Очистка кэша сопоставителя DNS с помощью команды ipconfig /flushdns и проверка наличия кэша командой ipconfig /displaydns



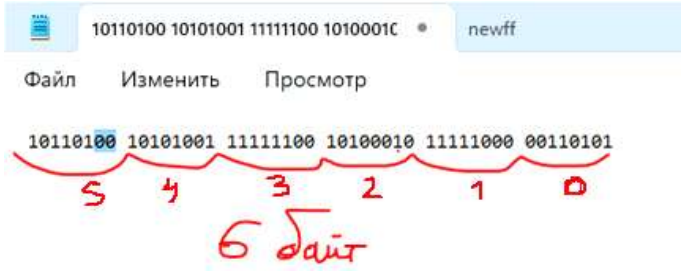




Командой ipconfig /displaydns > newff.txt создается файл newff.txt в папке C:\Users\mrShcherbak_, содержащий вывод команды ipconfig /displaydns.

Команда ipconfig /all | more разбивает подробные сведения о конфигурации всех адаптеров на страницы.

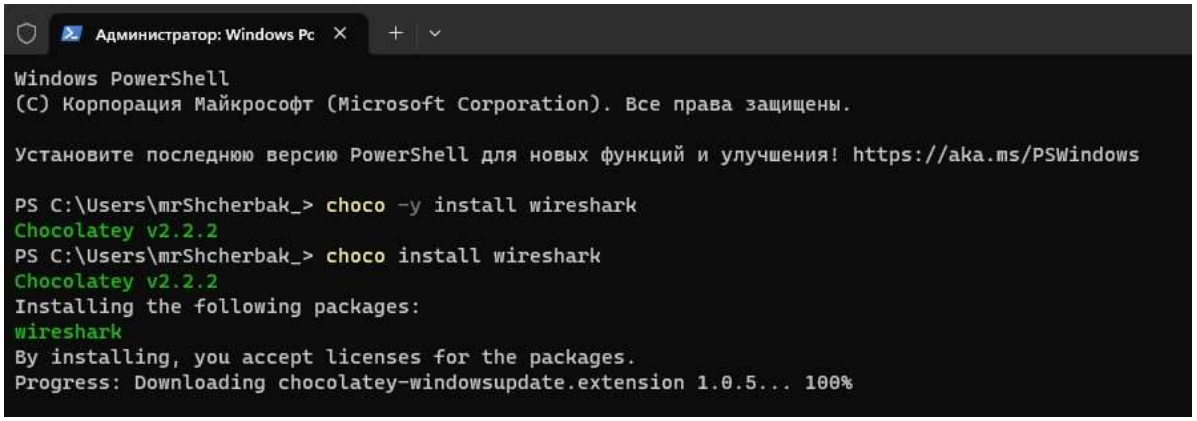
```
PS C:\Users\mrShcherbak_> ipconfig /all

Настройка протокола IP для Windows

   Имя компьютера  . . . . . . . . . . . : msk-mrshcherbak-gw-1
   Основной DNS-суффикс  . . . . . . . :
   Тип узла. . . . . . . . . . . . . . . : Гибридный
   IP-маршрутизация включена . . . . . : Нет
   WINS-прокси включен . . . . . . . . . : Нет
   Порядок просмотра суффиксов DNS . . : rudn.ru

Адаптер Ethernet Ethernet:

   Состояние среды. . . . . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . . :
   Описание. . . . . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Физический адрес. . . . . . . . . . . : B4-A9-FC-A2-F8-35
   DHCP включен. . . . . . . . . . . . . : Да
   Автонастройка включена. . . . . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

   Состояние среды. . . . . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . . :
   Описание. . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Физический адрес. . . . . . . . . . . : 92-30-49-14-F6-C3
   DHCP включен. . . . . . . . . . . . . : Нет
   Автонастройка включена. . . . . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 3:

   Состояние среды. . . . . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . . :
   Описание. . . . . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Физический адрес. . . . . . . . . . . : 82-30-49-14-F6-C3
   DHCP включен. . . . . . . . . . . . . : Да
   Автонастройка включена. . . . . . . . : Да

Адаптер Ethernet Ethernet 3:

   DNS-суффикс подключения . . . . . . :
   Описание. . . . . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter #3
   Физический адрес. . . . . . . . . . . : 08-00-27-00-88-D6
   DHCP включен. . . . . . . . . . . . . : Да
   Автонастройка включена. . . . . . . . : Да
   Локальный IPv6-адрес канала . . . . . : fe80::10d9:3b9e:6725:b3ab%11(Основной)
   Автонастройка IPv4-адреса . . . . . . : 169.254.181.151(Основной)
   Маска подсети . . . . . . . . . . . . : 255.255.0.0
   Основной шлюз. . . . . . . . . . . . :
   IAID DHCPv6 . . . . . . . . . . . . . : 1057488935
```

Определила MAC-адреса сетевых устройств, их тип и описала структуру MAC-адресов

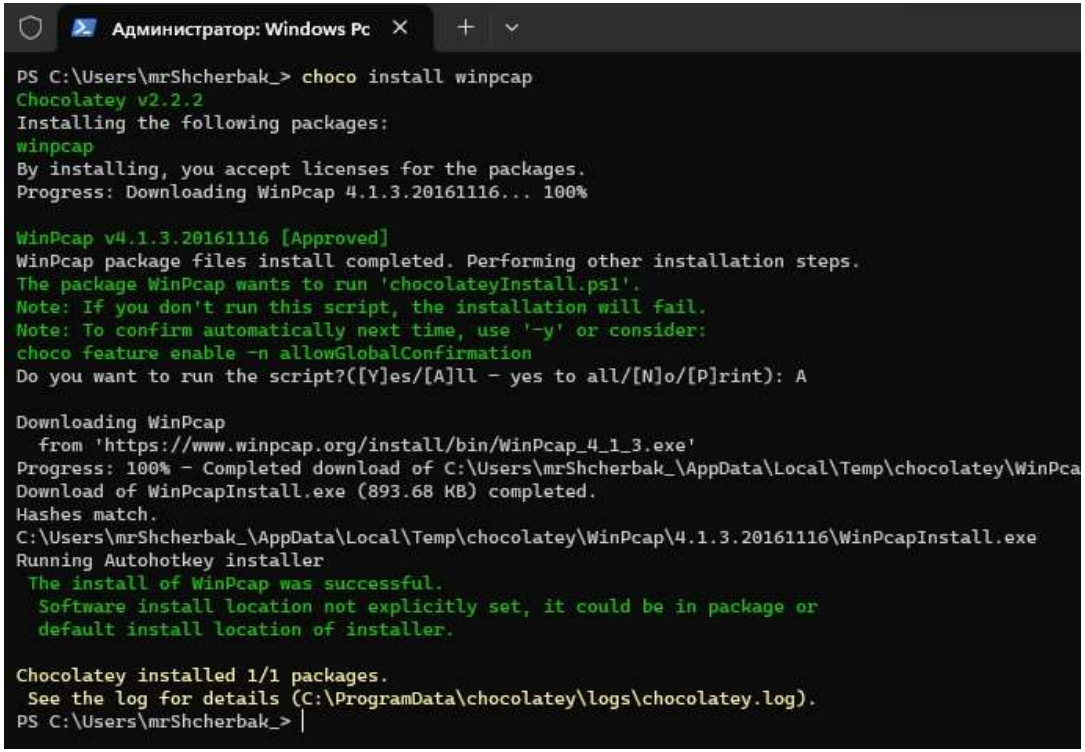


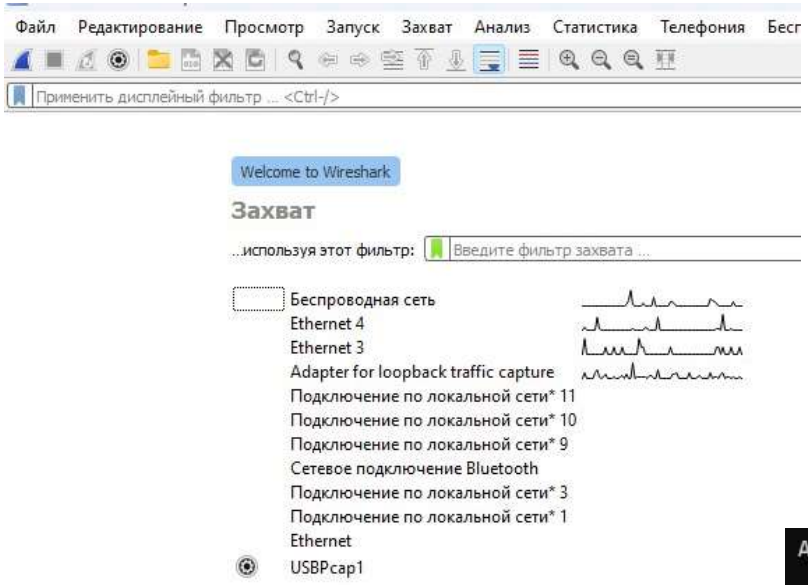

MAC-адрес сетевого устройства Ethernet в двоичной системе счисления

# Анализ кадров канального уровня в Wireshark




Установила на своем устройстве Wireshark

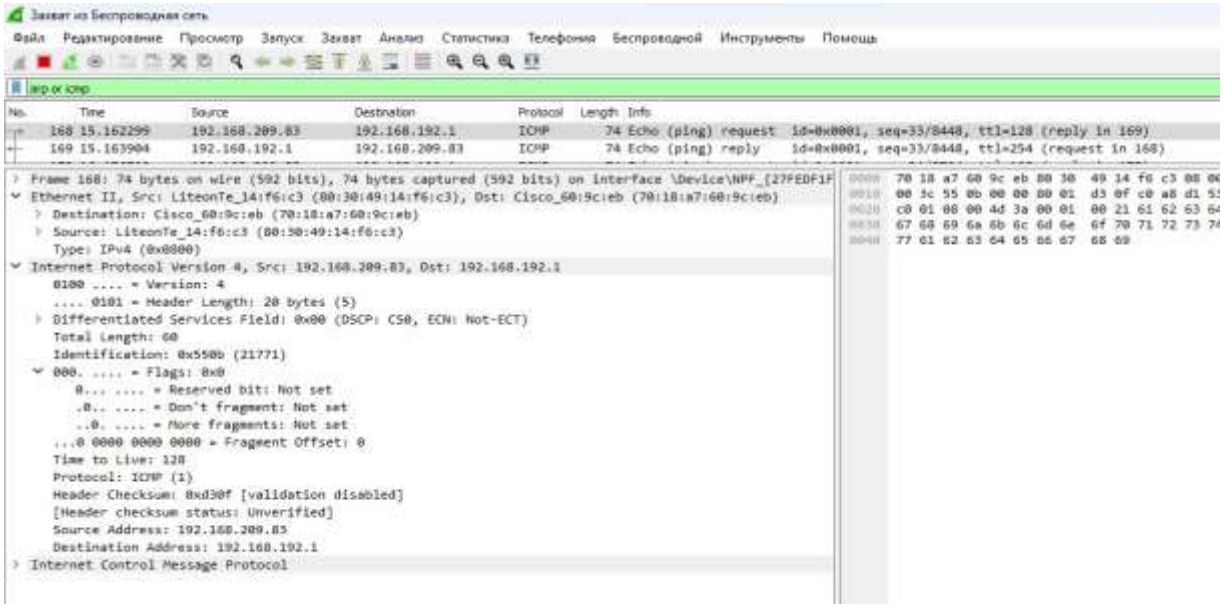


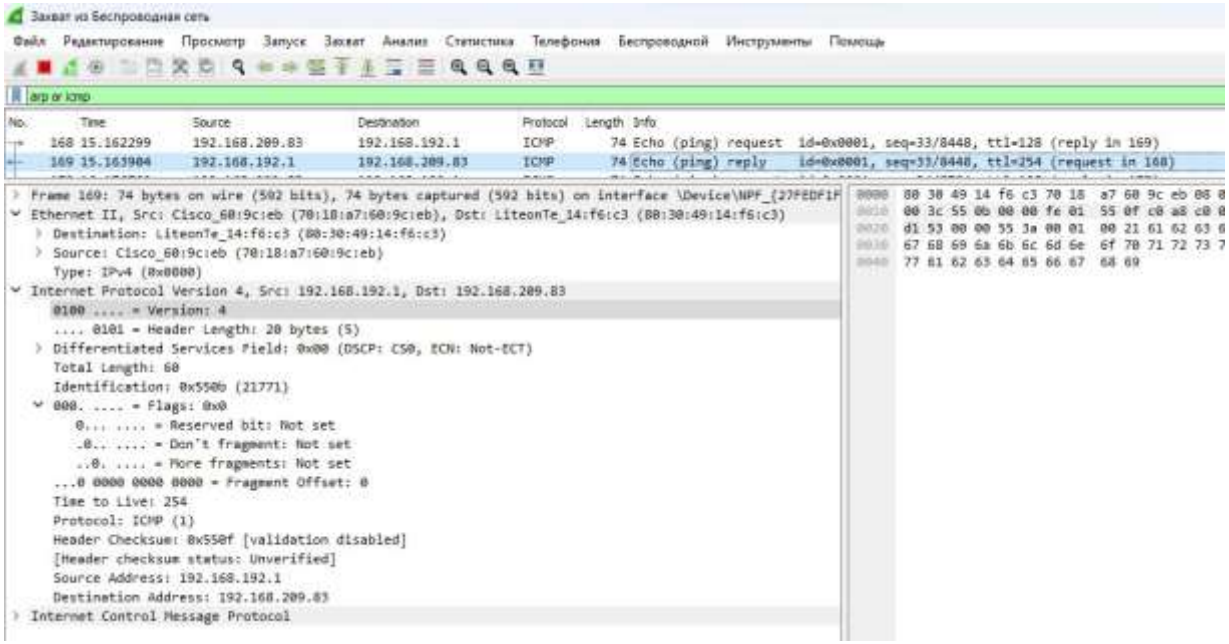



Список сетевых устройств на моем компьютере

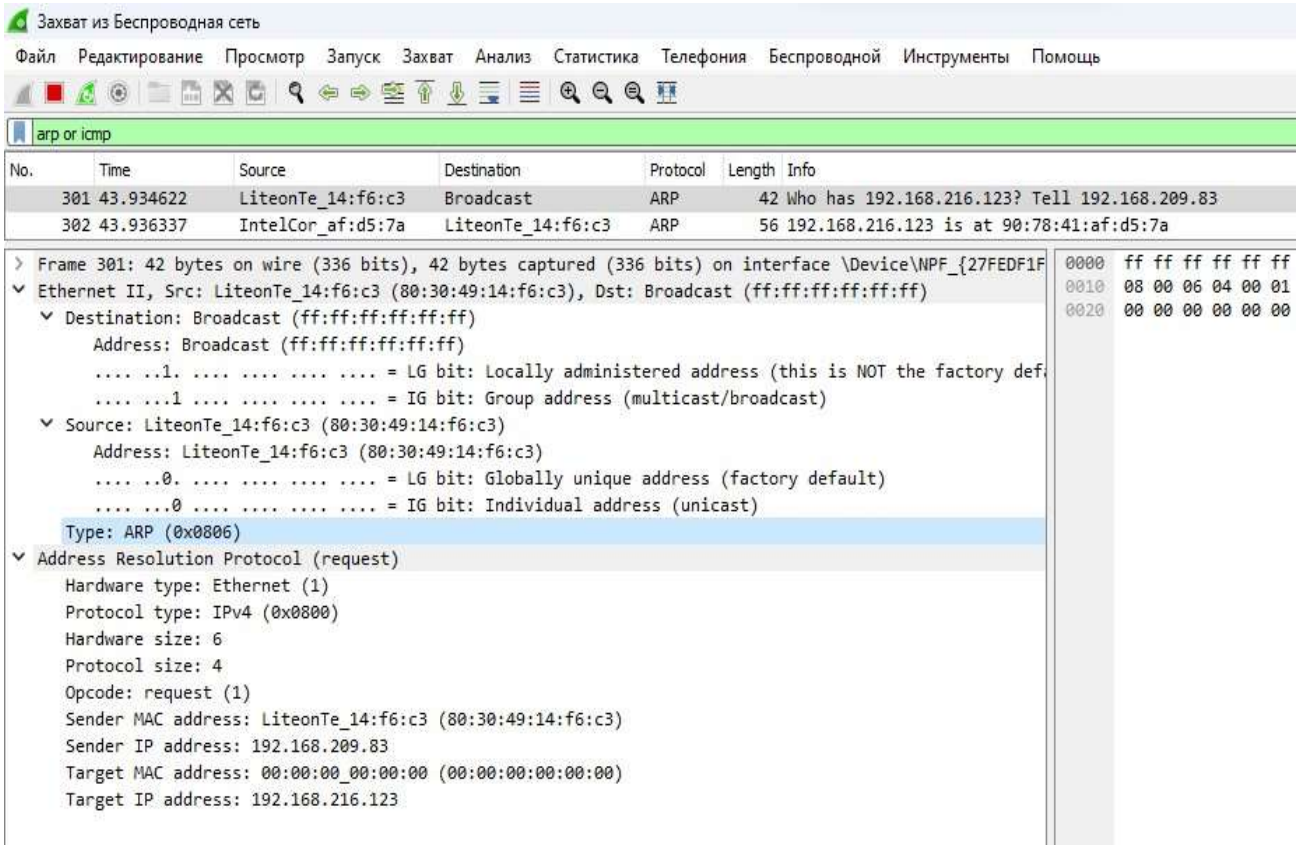
Пропинговала шлюз по умолчанию своего устройства

```
Адаптер беспроводной локальной сети Беспроводная сеть:

   DNS-суффикс подключения . . . . . : rudn.ru
   Локальный IPv6-адрес канала . . . : fe80::df8b:6ebd:c899:6b1f%6
   IPv4-адрес. . . . . . . . . . . . : 192.168.209.83
   Маска подсети . . . . . . . . . . : 255.255.224.0
   Основной шлюз. . . . . . . . . . : 192.168.192.1

Адаптер Ethernet Сетевое подключение Bluetooth:

   Состояние среды. . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
PS C:\Users\mrShcherbak_> ping -n 4 192.168.192.1

Обмен пакетами с 192.168.192.1 по с 32 байтами данных:
Ответ от 192.168.192.1: число байт=32 время=1мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=1мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=1мс TTL=254
Ответ от 192.168.192.1: число байт=32 время=1мс TTL=254

Статистика Ping для 192.168.192.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек
PS C:\Users\mrShcherbak_>
```



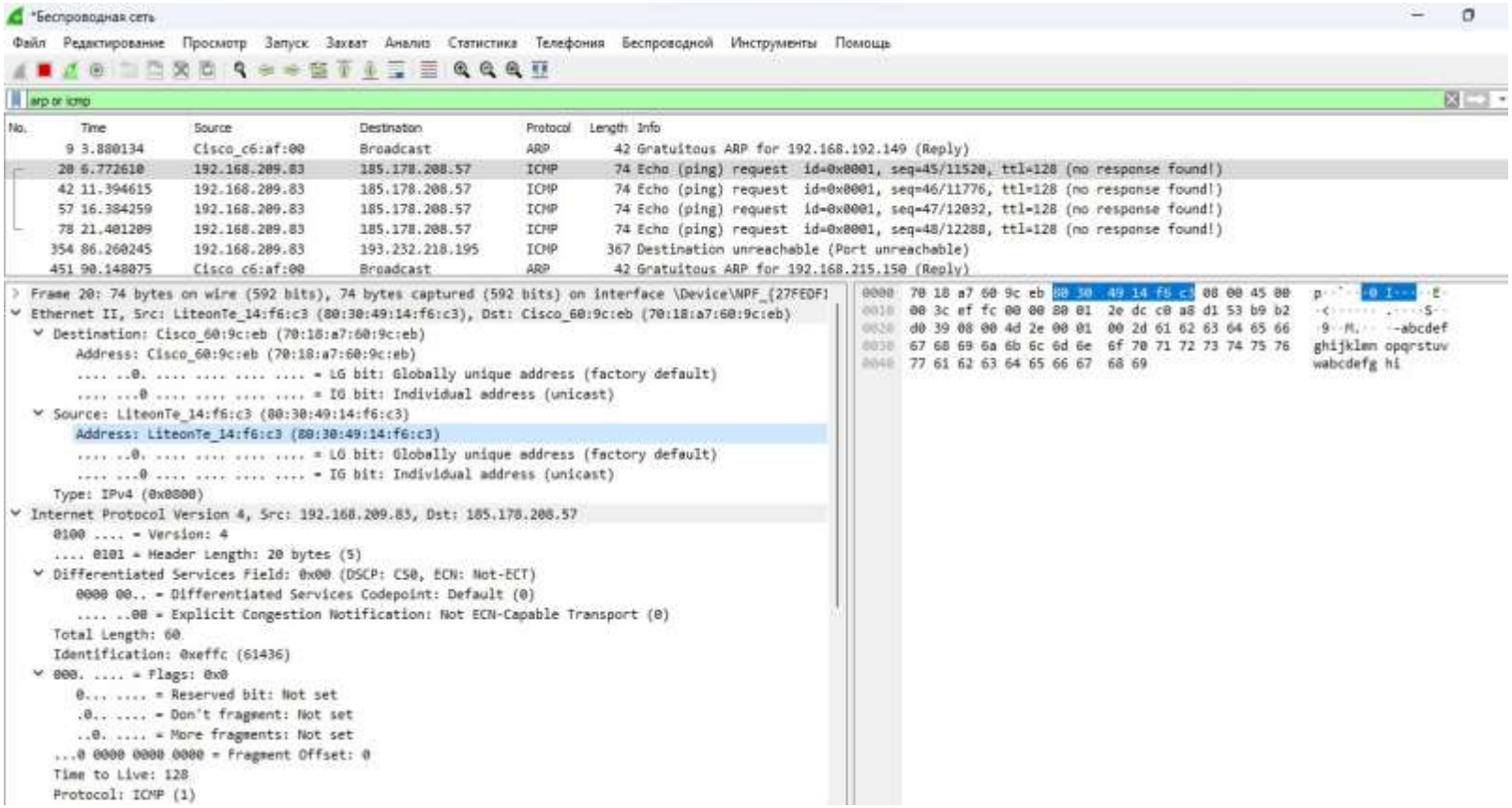

Изучила эхо-запрос и эхо-ответ ICMP в программе Wireshark




Изучила кадры данных протокола ARP

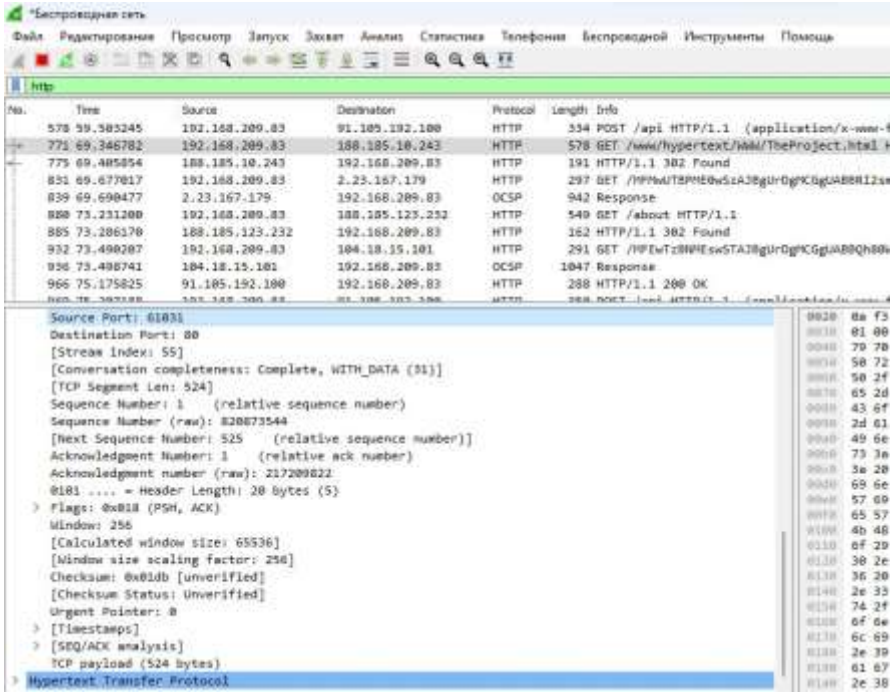
```
PS C:\Users\mrShcherbak_> ping rudn.ru

Обмен пакетами с rudn.ru [185.178.208.57] с 32 байтами данных:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 185.178.208.57:
    Пакетов: отправлено = 4, получено = 0, потеряно = 4
    (100% потерь)
PS C:\Users\mrShcherbak_>
```

Пропинговала по имени известный мне адрес — ping rudn.ru



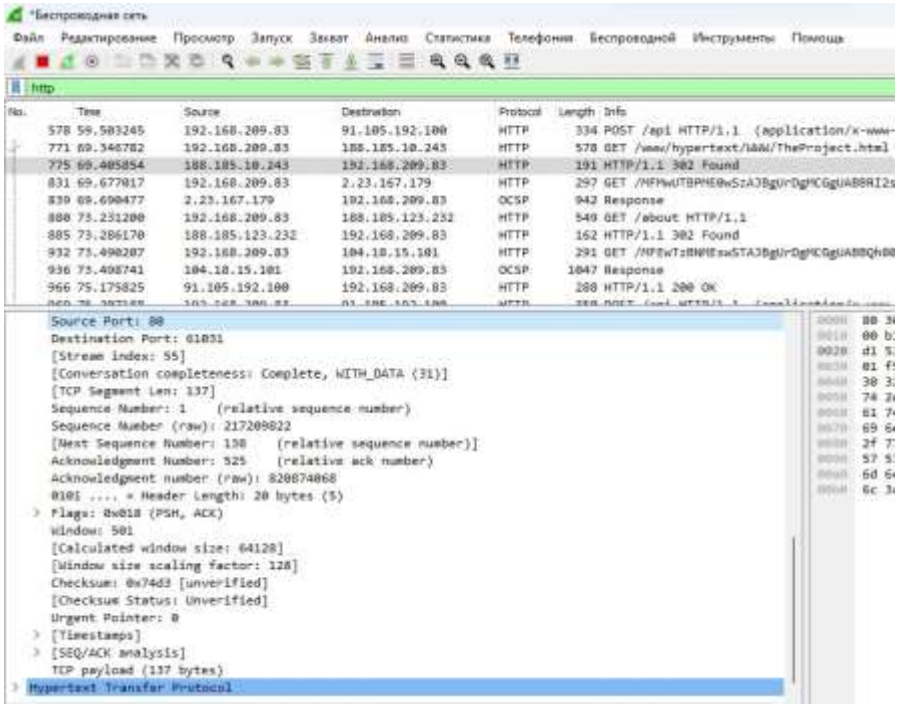

Сведения о запросах и ответах протоколов ARP и ICMP

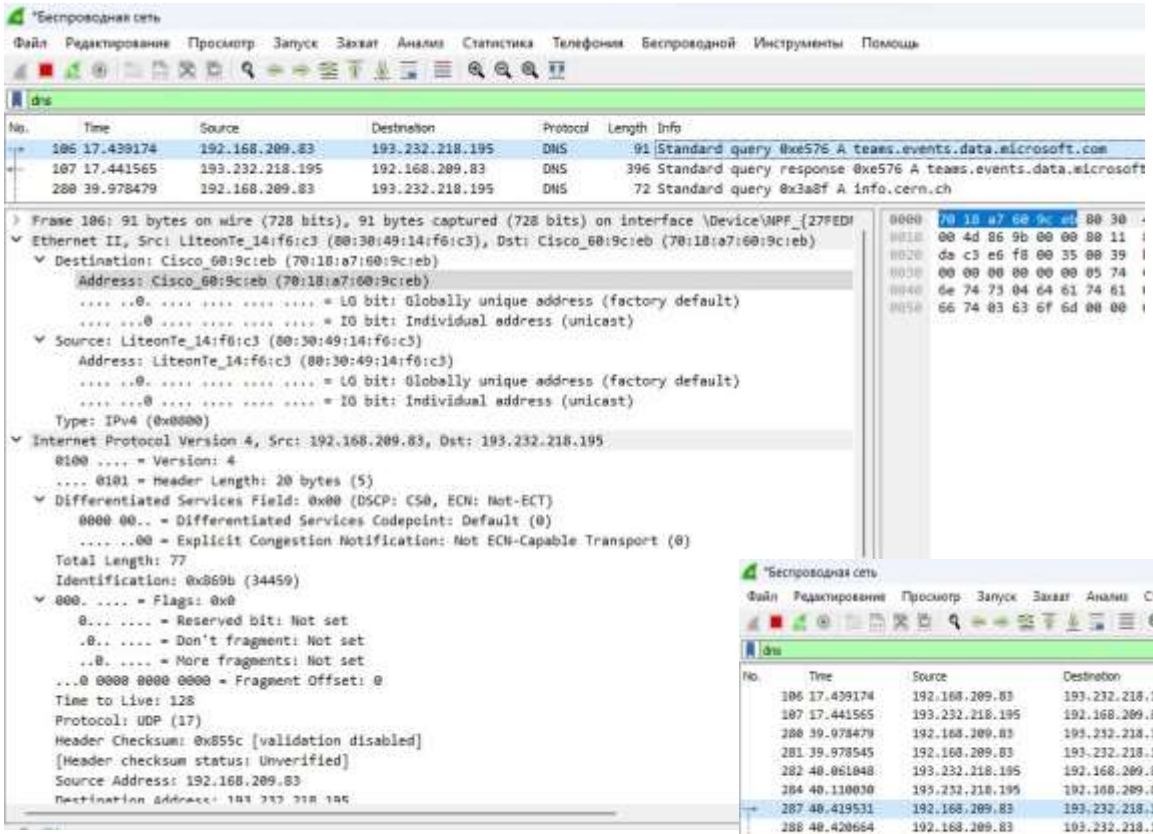
# Анализ протоколов транспортного уровня в Wireshark



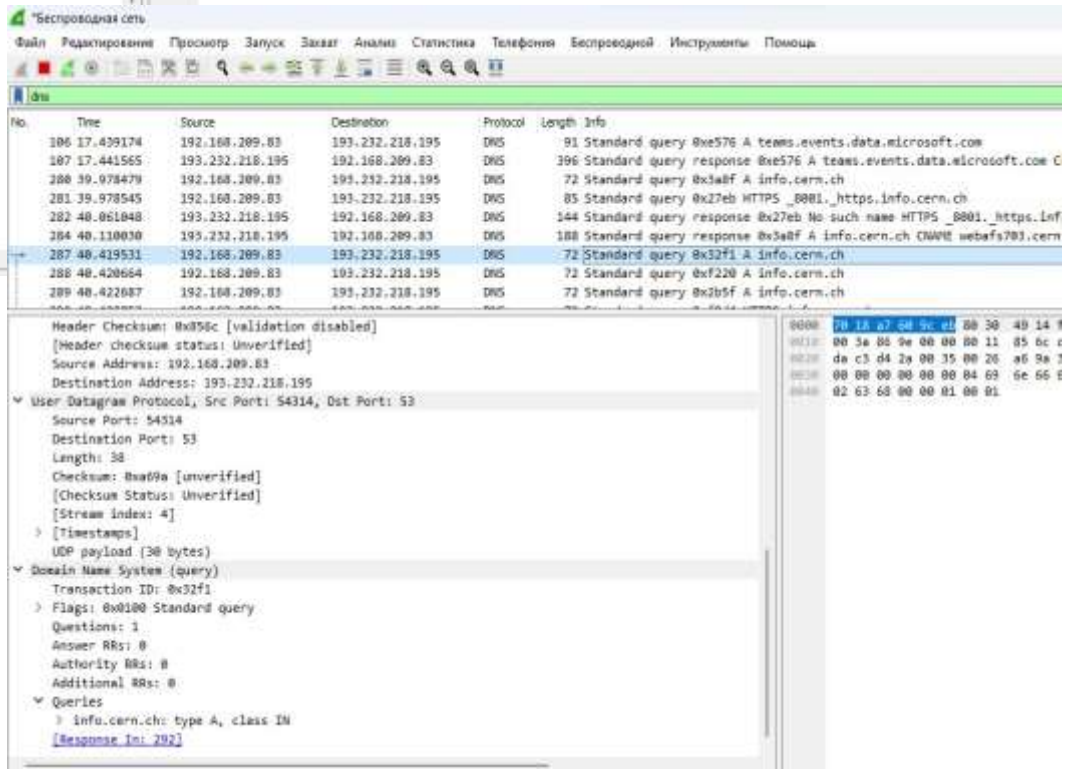

Сведения по протоколу TCP (GET)

Сведения по протоколу TCP



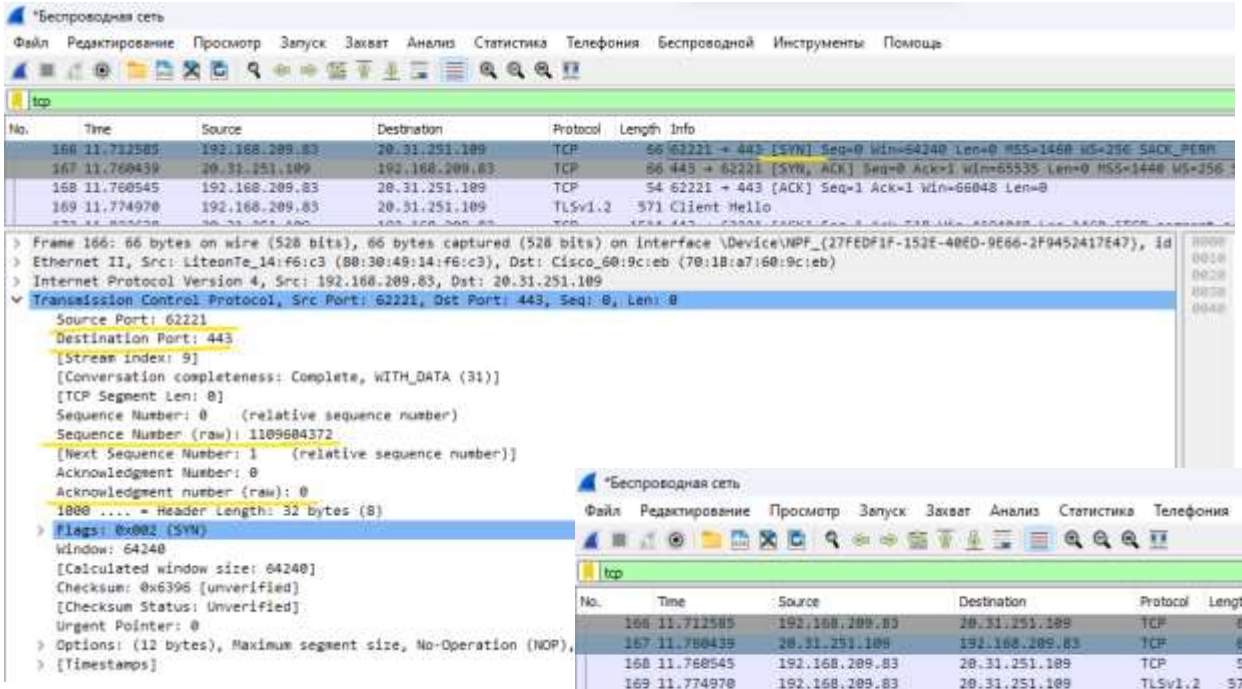



Поиск по фильтру dns

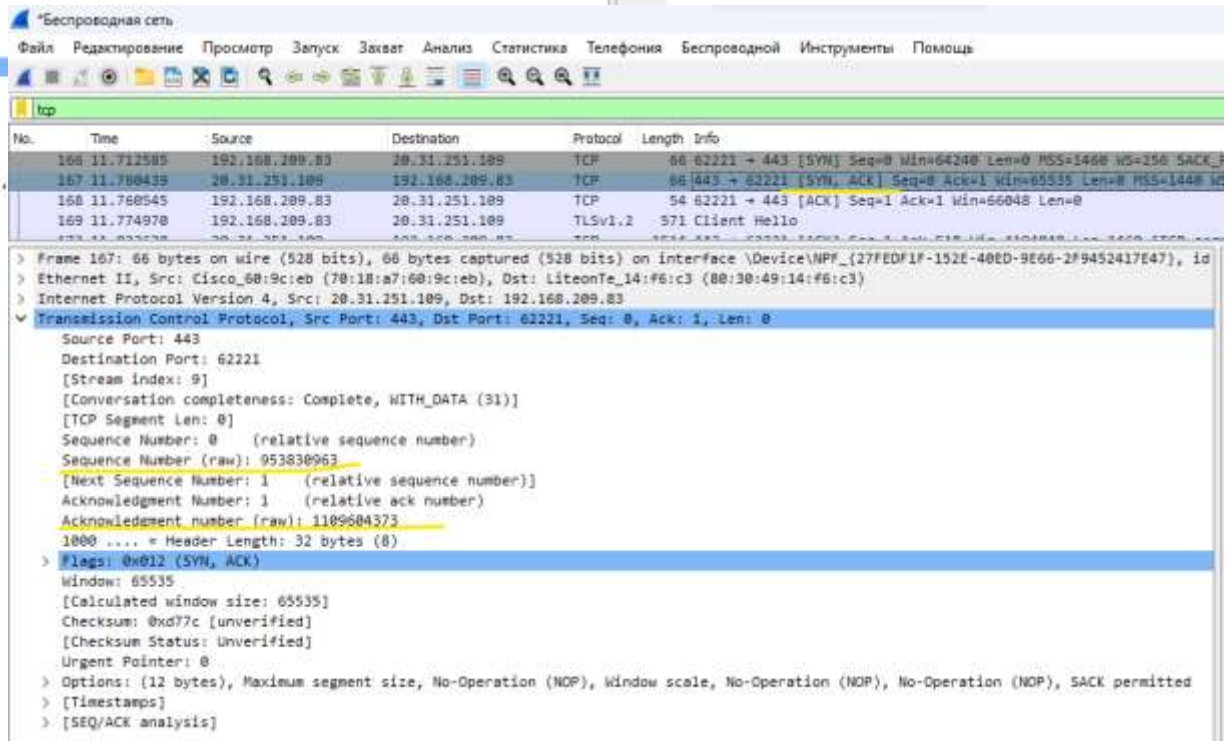



Сведения по протоколу UDP

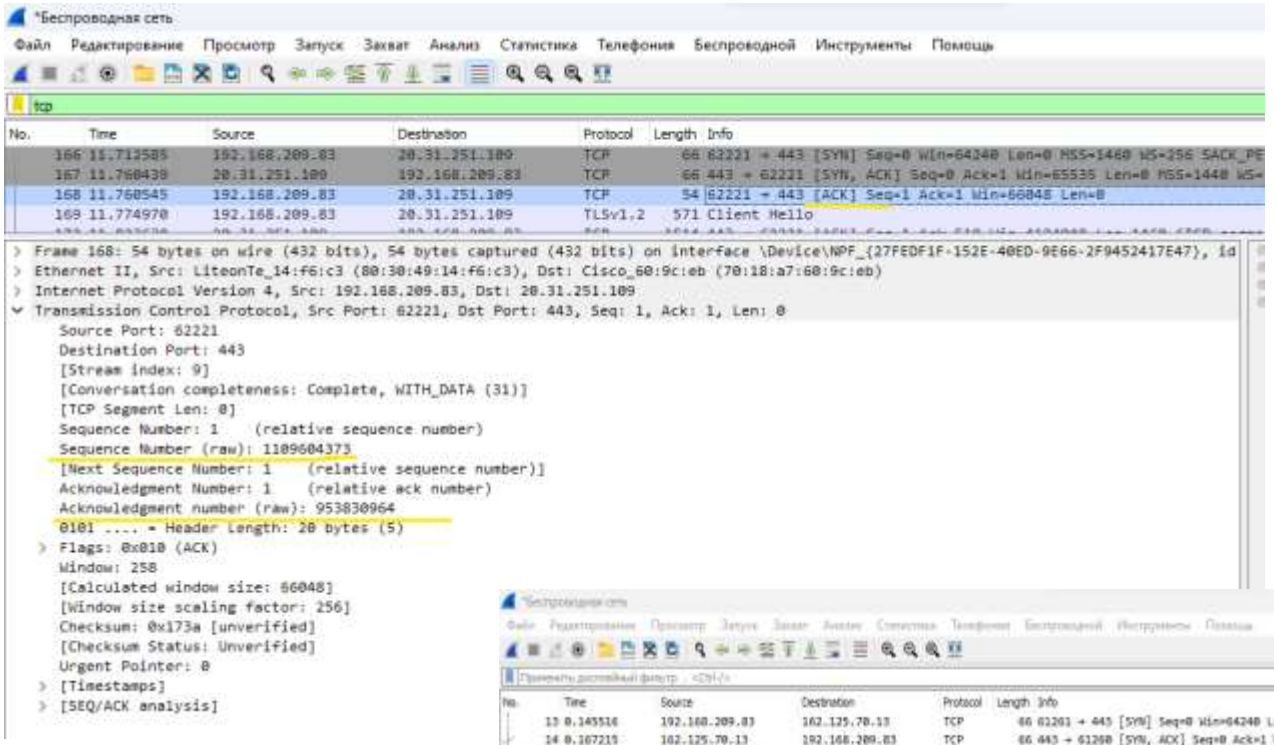
# Анализ handshake протокола TCP в Wireshark



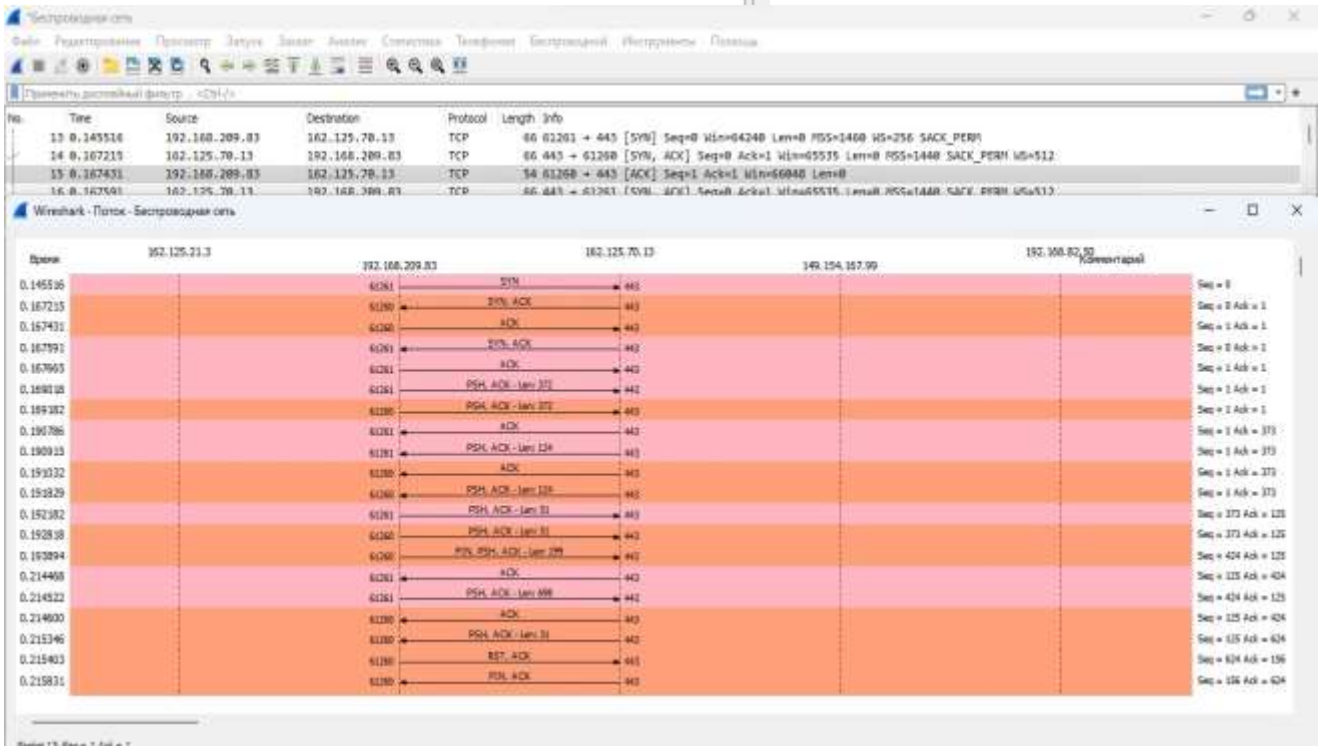

Первый этап «рукопожатия»



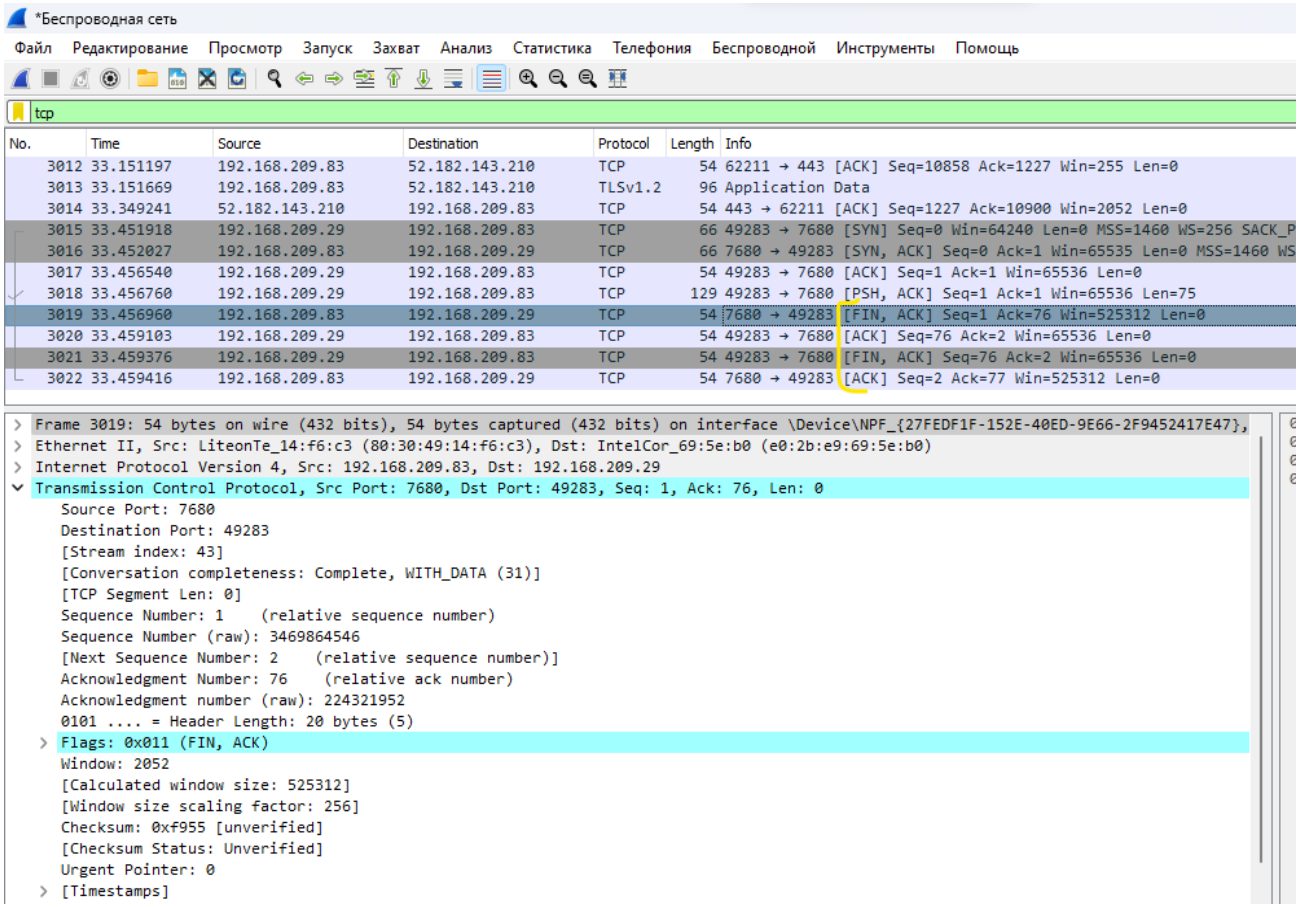

Второй этап «рукопожатия»




Третий этап «рукопожатия»




Просмотр графика потока




Закрытие TCP-соединения

**Вывод:** таким образом, в ходе выполнения л/р №3, я изучила посредством Wireshark кадры Ethernet, проанализировала PDU протоколы транспортного и прикладного уровней стека TCP/IP.