

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
ИМЕНИ ПАТРИСА ЛУМУМБЫ

Факультет физико-математических и естественных наук
Кафедра теории вероятностей и кибербезопасности

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 3

Дисциплина «Сетевые технологии»

Тема «Анализ трафика в Wireshark»

Студент: Щербак Маргарита Романовна

Ст. билет: 1032216537

Группа: НПИбд-02-21

МОСКВА

2023 г.

Цель работы

Изучение посредством Wireshark кадров Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.

Выполнение работы

1. MAC-адресация

1.1. Постановка задачи

1. Изучение возможностей команды `ipconfig` для ОС типа Windows.
2. Определение MAC-адреса устройства и его типа.

1.2. Выполнение

1. С помощью команды `ipconfig` для ОС типа Windows я вывела информацию о текущем сетевом соединении (рис.1.1). Рассмотрим блоки настроек заголовков «Адаптер Ethernet Ethernet 3», «Адаптер Ethernet Ethernet 4», «Адаптер беспроводной локальной сети Беспроводная сеть». Название данных сетевых устройств Ethernet 3, Ethernet 4 и Беспроводная сеть соответственно. У Беспроводной сети мы можем увидеть DNS-суффикс подключения `rudn.ru` — DNS-суффикс из настроек сетевого подключения. У каждого из рассматриваемых сетевых устройств описан локальный IPv6-адрес канала — локальный IPv6 адрес (используется адресация IPv6), у Ethernet 3 и Ethernet 4 описана автонастройка IPv4-адреса — автоматически полученный локальный адрес, если используется APIPA. На практике, такое значение IP-адреса означает, что сервер DHCP недоступен, у Беспроводной сети указаны IPv4-адрес — используемый для данного адаптера IPv4-адрес и основной шлюз — IP-адрес маршрутизатора, используемого в качестве шлюза по умолчанию. У всех данных устройств указана маска подсети — номер, используемый для разграничения сетевой части и части хоста IP-адреса.

```
Администратор: Windows Pc X + v

PS C:\Users\mrShcherbak_> ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet:

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

Адаптер беспроводной локальной сети Подключение по локальной сети* 1:

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

Адаптер беспроводной локальной сети Подключение по локальной сети* 3:

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

Адаптер Ethernet Ethernet 3:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::10d9:3b9e:6725:b3ab%11
    Автонастройка IPv4-адреса . . . . : 169.254.181.151
    Маска подсети . . . . . : 255.255.0.0
    Основной шлюз. . . . . :

Адаптер Ethernet Ethernet 4:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::f0cf:aad0:21b:e9b0%12
    Автонастройка IPv4-адреса . . . . : 169.254.56.53
    Маска подсети . . . . . : 255.255.0.0
    Основной шлюз. . . . . :

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

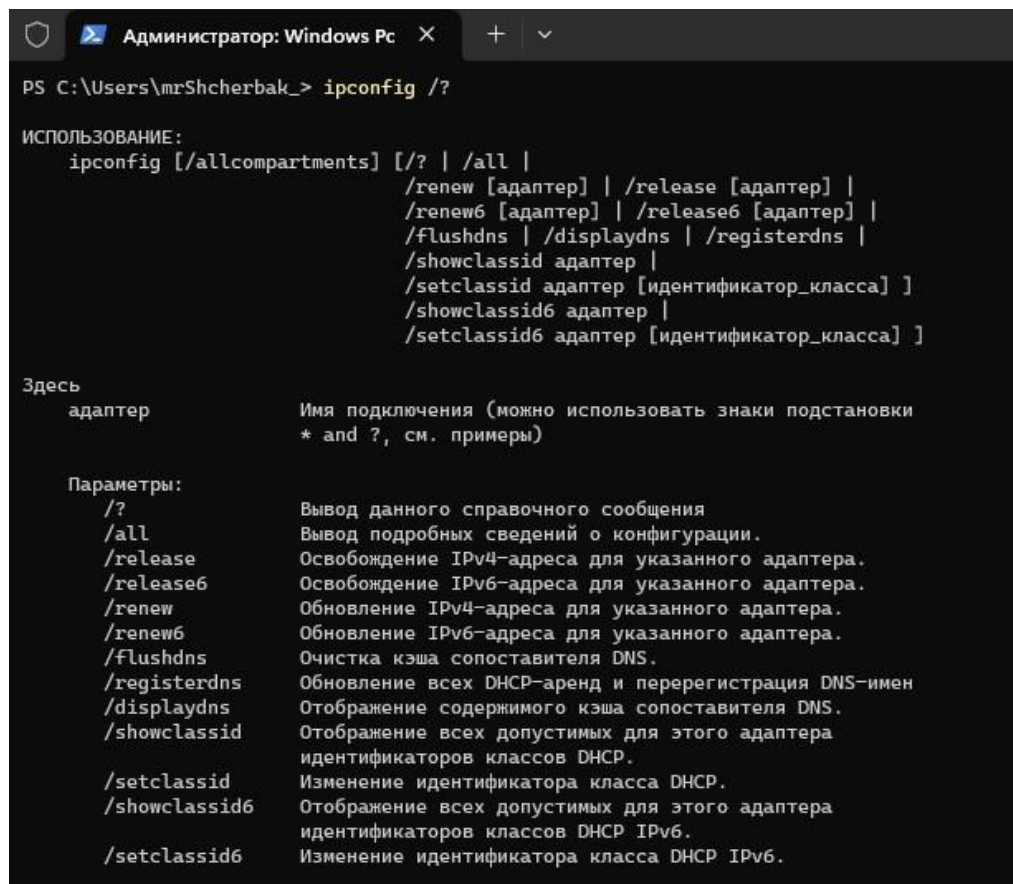
Адаптер Ethernet Сетевое подключение Bluetooth:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :
PS C:\Users\mrShcherbak_> |
```

Рис.1.1. Вывод базовых сетевых настроек для всех сетевых адаптеров, присутствующих в системе

Использовала разные опции команды (рис.1.2 – рис.1.7). У утилиты ipconfig достаточно много параметров, представленных на рис.1.2, также в подсказке (на скриншоте не влезло) приводятся примеры использования команды ipconfig, из

которых видно, что команду можно применять не сразу ко всем сетевым интерфейсам, а к конкретному интерфейсу или группе интерфейсов, используя их имена.



```
Администратор: Windows Pc
PS C:\Users\mrShcherbak> ipconfig /?

ИСПОЛЬЗОВАНИЕ:
ipconfig [/allcompartments] [/? | /all |
        /renew [адаптер] | /release [адаптер] |
        /renew6 [адаптер] | /release6 [адаптер] |
        /flushdns | /displaydns | /registerdns |
        /showclassid адаптер |
        /setclassid адаптер [идентификатор_класса] |
        /showclassid6 адаптер |
        /setclassid6 адаптер [идентификатор_класса] ]

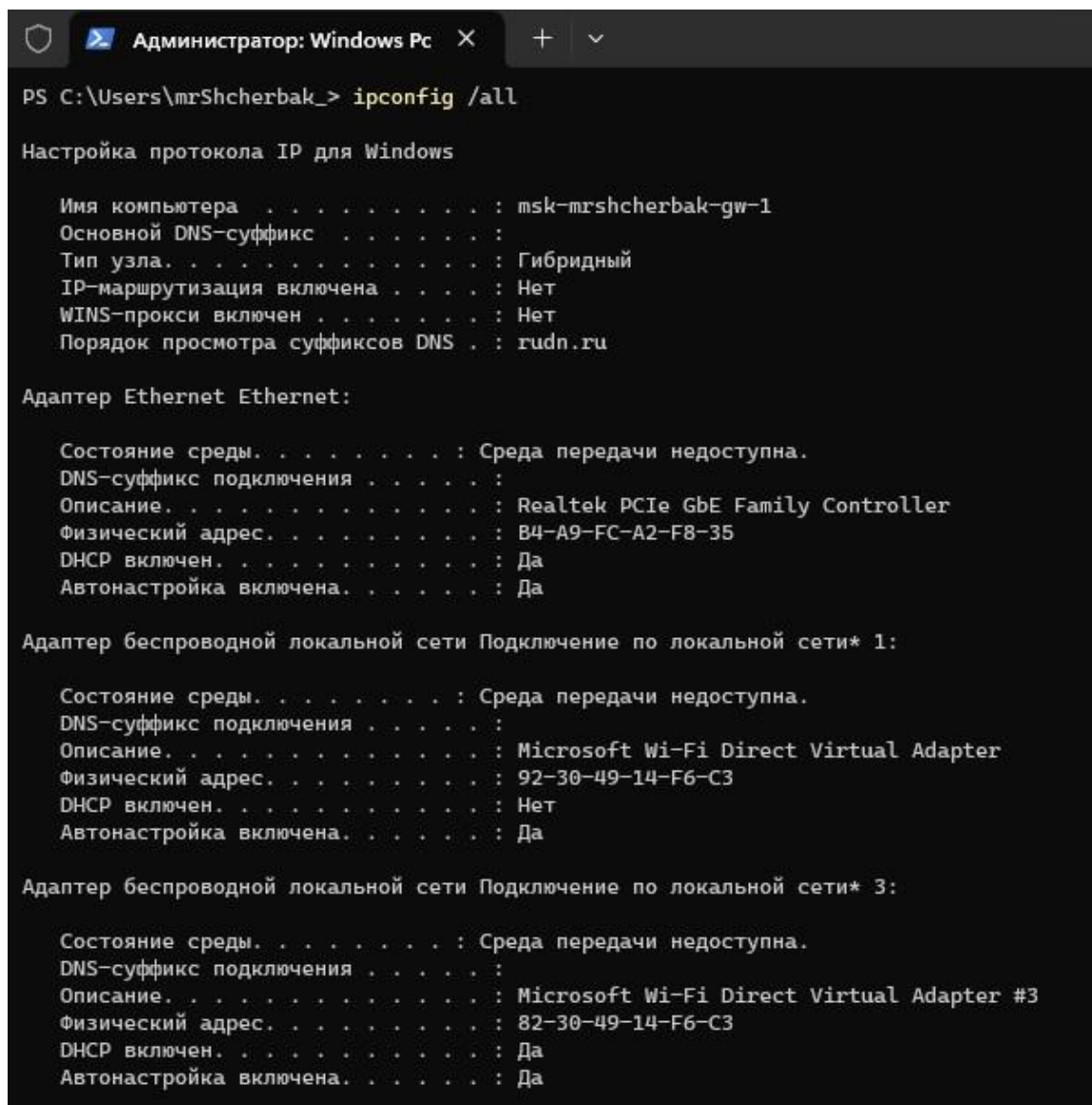
Здесь
адаптер          Имя подключения (можно использовать знаки подстановки
                  * and ?, см. примеры)

Параметры:
/?              Вывод данного справочного сообщения
/all           Вывод подробных сведений о конфигурации.
/release       Освобождение IPv4-адреса для указанного адаптера.
/release6      Освобождение IPv6-адреса для указанного адаптера.
/renew         Обновление IPv4-адреса для указанного адаптера.
/renew6        Обновление IPv6-адреса для указанного адаптера.
/flushdns      Очистка кэша сопоставителя DNS.
/registerdns   Обновление всех DHCP-аренд и перерегистрация DNS-имен
/displaydns    Отображение содержимого кэша сопоставителя DNS.
/showclassid   Отображение всех допустимых для этого адаптера
               идентификаторов классов DHCP.
/setclassid    Изменение идентификатора класса DHCP.
/showclassid6  Отображение всех допустимых для этого адаптера
               идентификаторов классов DHCP IPv6.
/setclassid6   Изменение идентификатора класса DHCP IPv6.
```

Рис.1.2. Вывод справки в командной строке

Наиболее часто используется команда `ipconfig /all`, позволяющая получить подробные сведения о сетевых настройках. Отображаются сведения о настройке протокола IP и о настройках сетевых адаптеров (рис.1.3 – рис.1.4). Из настроек протокола IP для Windows мы можем увидеть имя моего компьютера «msk-mrshcherbak-gw-1», тип узла — гибридный, также статус IP-маршрутизации и WINS-прокси. Также выводится конфигурация сетевых адаптеров: имя сетевого подключения — Ethernet (3/4), Беспроводная сеть, Подключение по локальной сети, Bluetooth, DNS-суффикс из настроек сетевого подключения (указан только у Беспроводной сети), описание — название сетевого адаптера, MAC-адрес данного адаптера, признак использования DHCP для конфигурирования сетевого адаптера, статус автонастройки, автоматически полученный локальный адрес (автонастройка IPv4-адреса), локальный IPv6-адрес, маска подсети, используемая для данного

адаптера IPv4 – адрес, дата и время получения сетевой конфигурации от сервера DHCP, срок истечения аренды сетевых настроек (определяется сервером DHCP), IP - адрес маршрутизатора, используемого в качестве шлюза по умолчанию, IP-адрес DHCP-сервера, от которого получена сетевая конфигурация, NetBios через TCP/IP — режим использования NetBios через протокол TCP/IP.



```
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
```

Рис.1.3. Вывод подробных сведений о конфигурации всех адаптеров

```
Администратор: Windows Pc X + v

Адаптер Ethernet Ethernet 4:

DNS-суффикс подключения . . . . . :
Описание. . . . . : VirtualBox Host-Only Ethernet Adapter #2
Физический адрес. . . . . : 08-00-27-00-80-00
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::f0cf:aad0:21b:e9b0%12(Основной)
Автонастройка IPv4-адреса . . . : 169.254.56.53(Основной)
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . :
IAID DHCPv6 . . . . . : 453509159
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2B-6A-8E-42-80-30-49-14-F6-C3
NetBios через TCP/IP. . . . . : Включен

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : rudn.ru
Описание. . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
Физический адрес. . . . . : 80-30-49-14-F6-C3
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::df8b:6ebd:c899:6b1f%6(Основной)
IPv4-адрес. . . . . : 192.168.209.83(Основной)
Маска подсети . . . . . : 255.255.224.0
Аренда получена. . . . . : 21 сентября 2023 г. 14:18:56
Срок аренды истекает. . . . . : 21 сентября 2023 г. 15:48:58
Основной шлюз. . . . . : 192.168.192.1
DHCP-сервер. . . . . : 192.168.192.3
IAID DHCPv6 . . . . . : 58732617
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2B-6A-8E-42-80-30-49-14-F6-C3
DNS-серверы. . . . . : 193.232.218.195
NetBios через TCP/IP. . . . . : Включен

Адаптер Ethernet Сетевое подключение Bluetooth:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Bluetooth Device (Personal Area Network)
Физический адрес. . . . . : 80-30-49-14-F6-C4
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
PS C:\Users\mrShcherbak_> |
```

Рис.1.4. Продолжение вывода команды ipconfig /all подробных сведений о конфигурации

Поля в выводе /displaydns соответствуют полям фактического ответа DNS (рис.1.5) . Имя записи — это домен, к которому производилось обращение, а тип записи — это соответствие имени и метаданных в системе доменных имен. Существует несколько типов DNS-записей, например, тип A (код 1) может содержать только IP-адрес четвертой версии, тип AAAA (код 28) содержит IP-адрес шестой версии, а тип записи CNAME (код 5) указывает на копирование другого домена. Срок жизни — это время в секундах, по истечении которого срок действия записи в кэше должен истечь. Длина данных — это длина в байтах (адрес IPv4 составляет четыре байта, IPv6 — шестнадцать байтов). Для CNAME или PTR

Windows отображает статический номер (4 или 8, в зависимости от системы) - это фактически размер адреса памяти, где хранится фактический текст. Каноническое имя (запись CNAME) – это тип записи DNS, которая привязывает псевдоним к действительному (каноническому) доменному имени.



```
Администратор: Windows Pc
PS C:\Users\mrShcherbak_> ipconfig /displaydns

Настройка протокола IP для Windows

wpad
-----
Имя не существует.

wpad
-----
Имя не существует.

ocsp.digicert.com
-----
Имя записи. . . . . : ocsp.digicert.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 1745
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : ocsp.edge.digicert.com

Имя записи. . . . . : ocsp.edge.digicert.com
Тип записи. . . . . : 5
Срок жизни. . . . . : 1745
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : fp2e7a.wpc.2be4.phicdn.net

Имя записи. . . . . : fp2e7a.wpc.2be4.phicdn.net
Тип записи. . . . . : 5
Срок жизни. . . . . : 1745
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
CNAME-запись. . . . . : fp2e7a.wpc.phicdn.net

Имя записи. . . . . : fp2e7a.wpc.phicdn.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 1745
Длина данных. . . . . : 4
```

Рис.1.5. Отображение содержимого кэша сопоставителя DNS

```

PS C:\Users\mrShcherbak_> ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.
PS C:\Users\mrShcherbak_> ipconfig /displaydns

Настройка протокола IP для Windows

PS C:\Users\mrShcherbak_> |

```

Рис.1.6. Очистка кэша сопоставителя DNS с помощью команды `ipconfig /flushdns` и проверка наличия кэша командой `ipconfig /displaydns`

С помощью команды `ipconfig /displaydns > newff.txt` будет создан файл `newff.txt` в папке `C:\Users\mrShcherbak_`, в котором будет записан вывод команды `ipconfig /displaydns` – отображение содержимого кэша сопоставителя DNS. Команда представлена на рис.1.7, а её вывод изображён на рис.1.8.

Команда `ipconfig /all | more` разобьет информацию о подробных сведениях конфигурации всех адаптеров на страницы, и чтобы читать данную информацию, нужно нажать Enter (рис.1.7).

```

PS C:\Users\mrShcherbak_> ipconfig /displaydns > newff.txt
PS C:\Users\mrShcherbak_> ipconfig /all | more

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
— Далее — |

```

Рис.1.7. Выполнение команд `ipconfig /displaydns > newff.txt` и `ipconfig /all | more`



Рис.1.8. Запись в файл содержимого кэша сопоставителя DNS

2. Определила MAC-адреса сетевых интерфейсов на своем компьютере. MAC-адреса подчеркнуты желтым цветом (рис.1.9).

```
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
```

Рис.1.9. Вывод подробных сведений о конфигурации всех адаптеров и определение MAC-адресов

3. Описала структуру MAC-адресов своего устройства. MAC-адрес — это 12-значное шестнадцатеричное число или 6-байтовое двоичное число. Первые 6 символов обычно идентифицируют производителя (идентификатор производителя). Оставшиеся 6 символов — идентификация производителем сетевого интерфейса. В пределах одного производителя эта часть должна быть уникальной для каждого сетевого устройства. На рис.1.10 MAC-адрес сетевого устройства Ethernet выглядит

как B4-A9-FC-A2-F8-35, где B4-A9-FC — идентификатор производителя, а A2-F8-35 — идентификатор сетевого устройства.

Индивидуальный адрес присваивается конкретному сетевому интерфейсу, а групповой адрес присваивается группе сетевых интерфейсов. Глобально администрируемый адрес присваивается производителем оборудования и уникален в масштабах всей сети, а локально администрируемый адрес может быть задан пользователем и не обязательно уникален в масштабах всей сети.

Для того, чтобы определить вид мак-адреса, нужно его перевести в двоичную систему счисления из 16-ичной. Если младший бит (нулевой) старшего байта (пятого по счёту справа, считая с 0) равен нулю, то это индивидуальный адрес, а если он равен единице, то адрес является групповым.

MAC-адрес может быть глобально администрируемым (GA) или локально администрируемым (LA). Если в том же старшем байте следующий бит после младшего (индекс 1) равен нулю, то это GA-адрес, что означает, что он был выдан производителем. Если этот бит равен единице, то это LA-адрес, и он может быть произвольно изменен администратором сети.

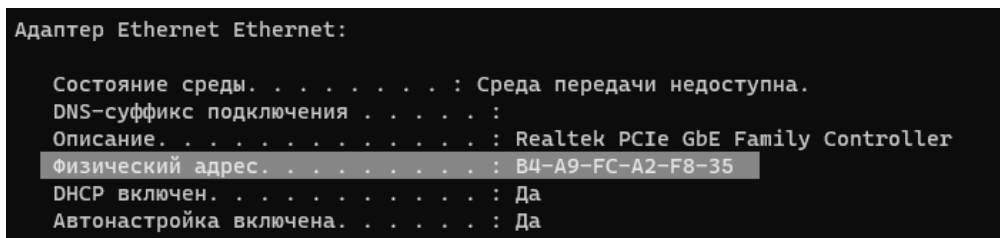


Рис.1.10. MAC-адрес сетевого устройства Ethernet

На рис.1.11 MAC-адрес сетевого устройства Ethernet B4-A9-FC-A2-F8-35 записан в двоичной системе счисления. 6 байт = 48 бит. Младшие два бита равны 0, следовательно, это индивидуальный, глобально администрируемый MAC-адрес.

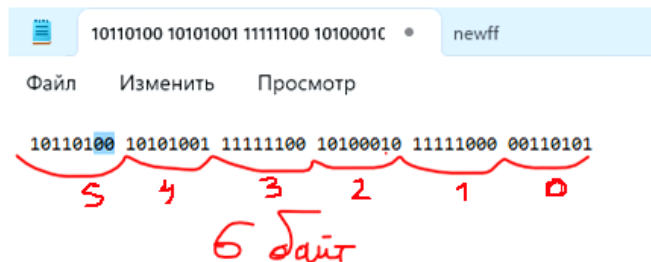


Рис.1.11. MAC-адрес сетевого устройства Ethernet в двоичной системе счисления.

По аналогии определим тип MAC-адреса Ethernet 4. На рис.1.12 MAC-адрес сетевого устройства Ethernet 4 выглядит как 08-00-27-00-80-00, где 08-00-27 — идентификатор производителя, а 00-80-00 — идентификатор сетевого устройства.

```
Адаптер Ethernet Ethernet 4:
DNS-суффикс подключения . . . . . :
Описание. . . . . : VirtualBox Host-Only Ethernet Adapter #2
Физический адрес. . . . . : 08-00-27-00-80-00
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::f0cf:aad0:21b:e9b0%12(Основной)
Автонастройка IPv4-адреса . . . : 169.254.56.53(Основной)
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . :
IAID DHCPv6 . . . . . : 453509159
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2B-6A-8E-42-80-30-49-14-F6-C3
NetBios через TCP/IP. . . . . : Включен
```

Рис.1.12. MAC-адрес сетевого устройства Ethernet 4

На рис.1.13 MAC-адрес сетевого устройства Ethernet 4 08-00-27-00-80-00 записан в двоичной системе счисления. 6 байт = 48 бит. Младшие два бита равны 0, следовательно, это индивидуальный, глобально администрируемый MAC-адрес.

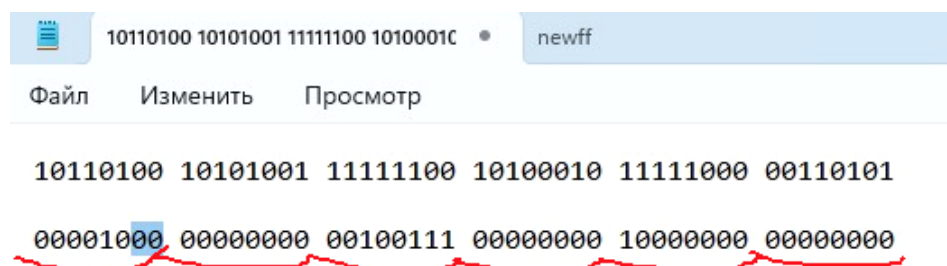


Рис.1.13. MAC-адрес сетевого устройства Ethernet 4 в двоичной системе счисления.

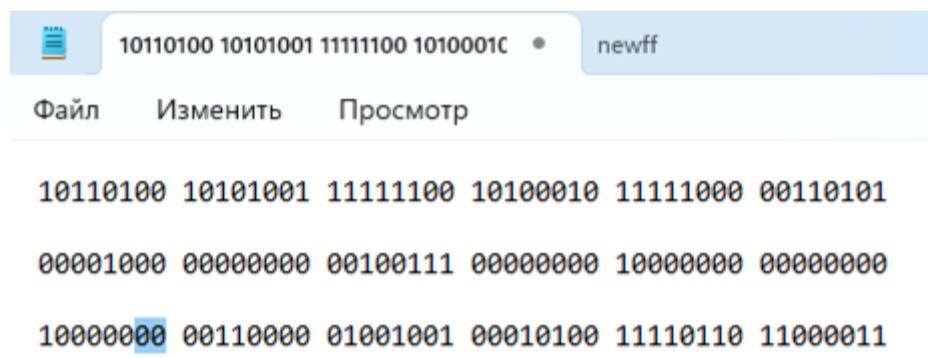
По аналогии определим тип MAC-адреса Беспроводной сети. На рис.1.14 MAC-адрес Беспроводной сети выглядит как 80-30-49-14-F6-C3, где 80-30-49 — идентификатор производителя, а 14-F6-C3 — идентификатор сетевого устройства.

```
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : rudn.ru
Описание. . . . . : Qualcomm Atheros QCA9377 Wireless Network Adapter
Физический адрес. . . . . : 80-30-49-14-F6-C3
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::df8b:6ebd:c899:6b1f%6(Основной)
IPv4-адрес. . . . . : 192.168.209.83(Основной)
Маска подсети . . . . . : 255.255.224.0
Аренда получена. . . . . : 21 сентября 2023 г. 21:25:19
Срок аренды истекает. . . . . : 21 сентября 2023 г. 23:21:22
Основной шлюз. . . . . : 192.168.192.1
DHCP-сервер. . . . . : 192.168.192.3
IAID DHCPv6 . . . . . : 58732617
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2B-6A-8E-42-80-30-49-14-F6-C3
DNS-серверы. . . . . : 193.232.218.195
NetBios через TCP/IP. . . . . : Включен
```

Рис.1.14. MAC-адрес Беспроводной сети

На рис.1.13 MAC-адрес Беспроводной сети 80-30-49-14-F6-C3 записан в двоичной системе счисления. Младшие два бита равны 0, следовательно, это индивидуальный, глобально администрируемый MAC-адрес.



```
10110100 10101001 11111100 10100010 11111000 00110101
00001000 00000000 00100111 00000000 10000000 00000000
10000000 00110000 01001001 00010100 11110110 11000011
```

Рис.1.15. MAC-адрес Беспроводной сети в двоичной системе счисления.

На рис.1.16 показана схема определения типа MAC-адреса

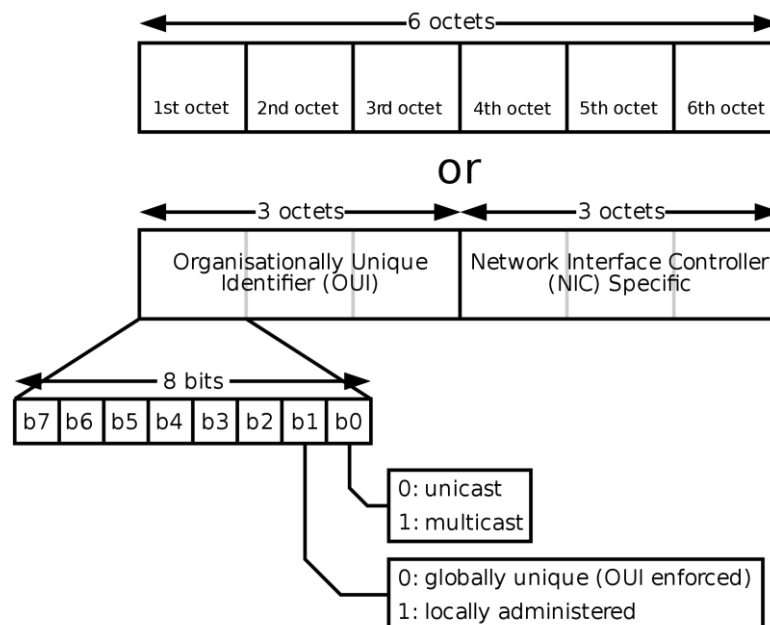


Рис.1.16. Определение типа MAC-адреса

2. Анализ кадров канального уровня в Wireshark

2.1. Постановка задачи

1. Установить на домашнем устройстве Wireshark.
2. С помощью Wireshark захватить и проанализировать пакеты ARP и ICMP в части кадров канального уровня.

2.2. Выполнение

1. Установила на своем устройстве Wireshark (рис.2.1 – рис.2.2).

```

Администратор: Windows Pc
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Установите последнюю версию PowerShell для новых функций и улучшения! https://aka.ms/PSWindows

PS C:\Users\mrShcherbak> choco -y install wireshark
Chocolatey v2.2.2
PS C:\Users\mrShcherbak> choco install wireshark
Chocolatey v2.2.2
Installing the following packages:
wireshark
By installing, you accept licenses for the packages.
Progress: Downloading chocolatey-windowsupdate.extension 1.0.5... 100%
  
```

Рис.2.1. Установка Wireshark


```
Администратор: Windows Pc
PS C:\Users\mrShcherbak_> choco install winpcap
Chocolatey v2.2.2
Installing the following packages:
winpcap
By installing, you accept licenses for the packages.
Progress: Downloading WinPcap 4.1.3.20161116... 100%

WinPcap v4.1.3.20161116 [Approved]
WinPcap package files install completed. Performing other installation steps.
The package WinPcap wants to run 'chocolateyInstall.ps1'.
Note: If you don't run this script, the installation will fail.
Note: To confirm automatically next time, use '-y' or consider:
choco feature enable -n allowGlobalConfirmation
Do you want to run the script?([Y]es/[A]ll - yes to all/[N]o/[P]rint): A

Downloading WinPcap
  from 'https://www.winpcap.org/install/bin/WinPcap_4_1_3.exe'
Progress: 100% - Completed download of C:\Users\mrShcherbak_\AppData\Local\Temp\chocolatey\WinPcap\WinPcapInstall.exe (893.68 KB) completed.
Hashes match.
C:\Users\mrShcherbak_\AppData\Local\Temp\chocolatey\WinPcap\4.1.3.20161116\WinPcapInstall.exe
Running Autohotkey installer
The install of WinPcap was successful.
Software install location not explicitly set, it could be in package or
default install location of installer.

Chocolatey installed 1/1 packages.
See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).
PS C:\Users\mrShcherbak_> |
```

Рис.2.2. Установка драйвера winpcap для Wireshark

2. Запустила Wireshark (рис.2.3). Выбрала активный на своем устройстве сетевой интерфейс – Беспроводная сеть. Убедилась, что начался процесс захвата трафика.

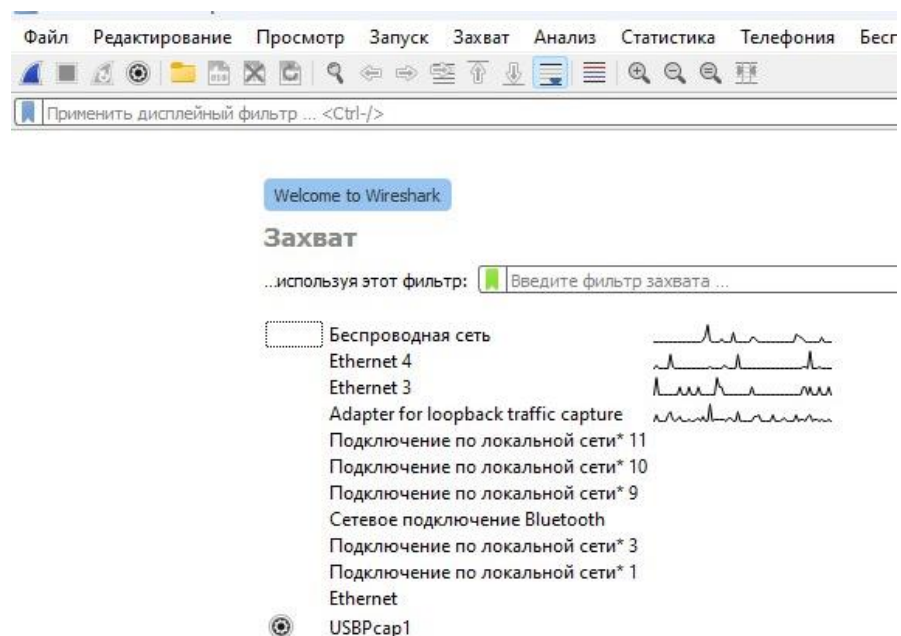


Рис.2.3. Список сетевых устройств на моем компьютере

3. Определила с помощью команды `ipconfig` IP-адрес своего устройства и шлюз по умолчанию (рис.2.4).

```
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
```

Рис.2.4. IP-адрес Беспроводной сети и шлюз

4. Пропинговала шлюз по умолчанию (рис.2.5).

```
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_> |
```

Рис.2.5. Выполнение команды `ping`

5. В строке фильтра в Wireshark прописала фильтр `arp or icmp`. Убедилась, что в списке пакетов отобразятся только пакеты ARP или ICMP (рис.2.6).

No.	Time	Source	Destination	Protocol	Length	Info
44	3.496446	Cisco_c6:af:00	Broadcast	ARP	42	Gratuitous ARP for 192.168.216.37 (Reply)
92	5.732203	Cisco_c6:af:00	Broadcast	ARP	42	Gratuitous ARP for 192.168.211.70 (Reply)
96	8.358861	Cisco_c6:af:00	Broadcast	ARP	42	Gratuitous ARP for 192.168.206.197 (Reply)
168	15.162299	192.168.209.83	192.168.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 169)
169	15.163904	192.168.192.1	192.168.209.83	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=254 (request in 168)
173	16.176729	192.168.209.83	192.168.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 175)
175	16.195789	192.168.192.1	192.168.209.83	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=254 (request in 173)
177	17.186981	192.168.209.83	192.168.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 179)
179	17.206277	192.168.192.1	192.168.209.83	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=254 (request in 177)
181	18.201830	192.168.209.83	192.168.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 182)
182	18.205988	192.168.192.1	192.168.209.83	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=254 (request in 181)
381	43.934622	LiteonTe_14:f6:c3	Broadcast	ARP	42	Who has 192.168.216.123? Tell 192.168.209.83
382	43.936337	IntelCor_af:d5:7a	LiteonTe_14:f6:c3	ARP	56	192.168.216.123 is at 90:78:41:af:d5:7a
389	53.709359	Cisco_c6:af:00	Broadcast	ARP	42	Gratuitous ARP for 192.168.197.210 (Reply)
443	71.378844	Cisco_c6:af:00	Broadcast	ARP	42	Gratuitous ARP for 192.168.201.172 (Reply)

Рис.2.6. Применение фильтра к поиску пакетов ARP иICMP

6. Изучила эхо-запрос и эхо-ответ ICMP в программе Wireshark:

– На панели списка пакетов выбрала первый указанный кадр ICMP — эхо-запрос (request) (рис.2.7). Изучила информацию на панели сведений о пакете. Длина кадра = 74 байта. Вторая строка в панели показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника Source (80:30:49:14:f6:c3) и назначения Destination (70:18:a7:60:9c:eb). MAC-адреса источника и назначения являются индивидуальными и глобально администрируемыми. На рис.2.8 переведены адреса в 2 сс и проанализированы соответственно. Показан заголовок протокола сетевого уровня IPv4. Средний раздел содержит информацию о поле данных кадра. Данные содержат IPv4-адреса источника (192.168.209.83) и назначения (192.168.192.1). В заголовке ICMP основные поля — это type и code. Type говорит о том, что произошло в сети (Echo (ping) request).

No.	Time	Source	Destination	Protocol	Length	Info
168	15.162299	192.168.209.83	192.168.192.1	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 169)
169	15.163904	192.168.192.1	192.168.209.83	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=254 (request in 168)

Frame 168: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{27FEDF1F-0000-0000-0000-000000000000}	
Ethernet II, Src: LiteonTe_14:f6:c3 (80:30:49:14:f6:c3), Dst: Cisco_60:9c:eb (70:18:a7:60:9c:eb)	0000 70 18 a7 60 9c eb 80 30 49 14 f6 c3 08 00 00 00
Source: LiteonTe_14:f6:c3 (80:30:49:14:f6:c3)	0010 00 3c 55 0b 00 00 00 01 d3 0f c0 a8 d1 5:00 21 61 62 63 64
Type: IPv4 (0x0800)	0020 c0 01 08 00 4d 3a 00 01 00 21 61 62 63 64 65 66 67 68 69
Internet Protocol Version 4, Src: 192.168.209.83, Dst: 192.168.192.1	
0100 = Version: 4	
.... 0101 = Header Length: 20 bytes (5)	
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 60	
Identification: 0x550b (21771)	
0000 = Flags: 0x00	
0... = Reserved bit: Not set	
.0... = Don't fragment: Not set	
..0... = More fragments: Not set	
...0 0000 0000 0000 = Fragment Offset: 0	
Time to Live: 128	
Protocol: ICMP (1)	
Header Checksum: 0xd30f [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 192.168.209.83	
Destination Address: 192.168.192.1	
Internet Control Message Protocol	

Рис.2.7. Сведения об эхо-запросе кадра ICMP

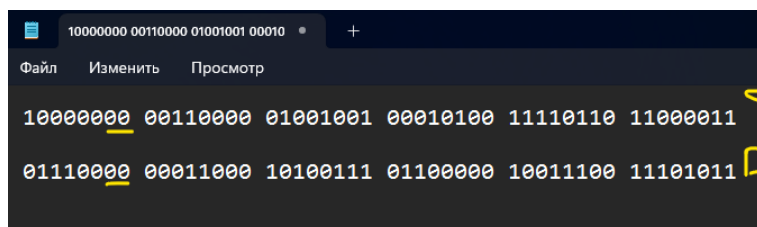


Рис.2.8. Определение типа MAC-адресов

– На панели списка пакетов выбрала второй указанный кадр ICMP — эхо-ответ (reply) (рис.2.9). Изучила информацию на панели сведений о пакете. Длина кадра = 74 байта. Вторая строка в панели показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника Source (70:18:a7:60:9c:eb) и назначения Destination (80:30:49:14:f6:c3). MAC-адреса источника и назначения являются индивидуальными и глобально администрируемыми. На рис.2.10 переведены адреса в 2 сс и проанализированы соответственно. Показан заголовок протокола сетевого уровня IPv4. Средний раздел содержит информацию о поле данных кадра. Данные содержат IPv4-адреса источника (192.168.192.1) и назначения (192.168.209.83). В заголовке ICMP основные поля — это type и code. Type говорит о том, что произошло в сети (Echo (ping) reply).

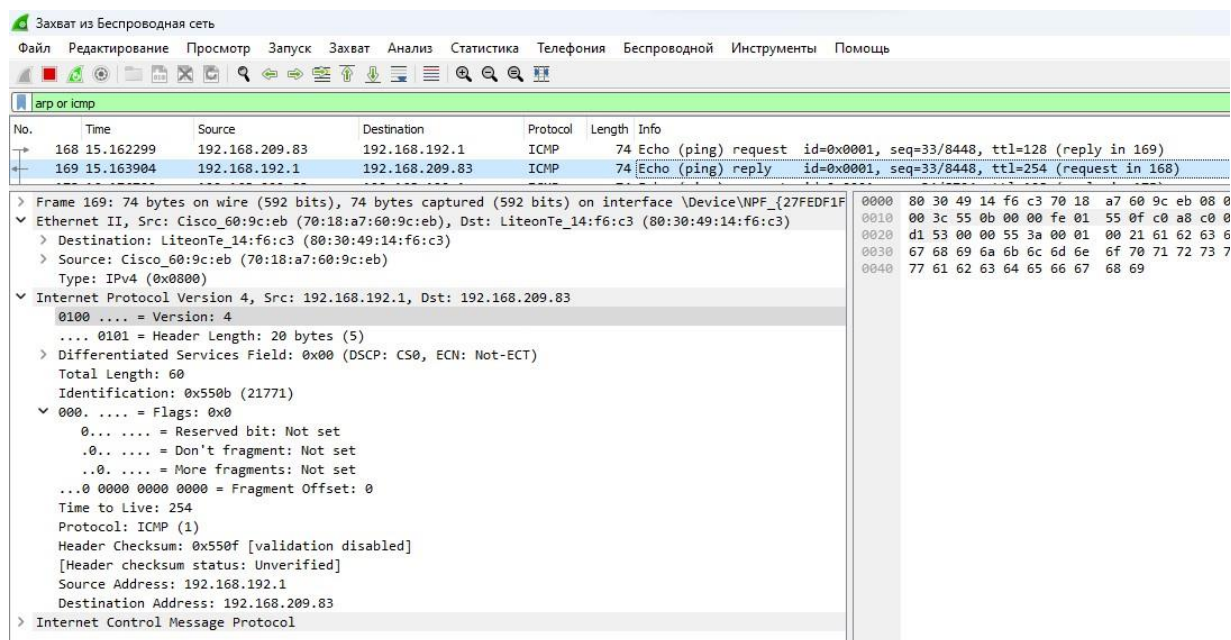


Рис.2.9. Сведения об эхо-ответе кадра ICMP

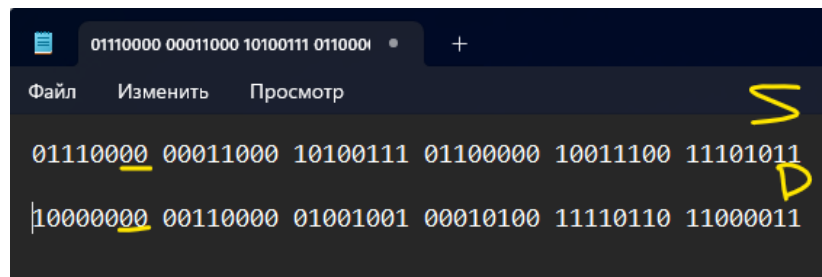


Рис.2.10. Определение типа MAC-адресов

7. Изучила кадры данных протокола ARP (рис.2.11). ARP протокол сетевого уровня состоит из запроса и ответа. Длина кадра = 42 байта. Вторая строка в панели показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника Source (80:30:49:14:f6:c3) и назначения Destination — широковещательный адрес. В заголовке ARP основные поля — это Hardware type Ethernet канальный уровень, Protocol type IPv4 сетевой уровень, Hardware size 6 байт = 48 бит, Protocol size 4 байта = 32 бита, Opcode код операции — запрос. Мы видим разницу в типе адресов: Source Address индивидуальный и глобально администрируемый, а Destination Address групповой и локально администрируемый.

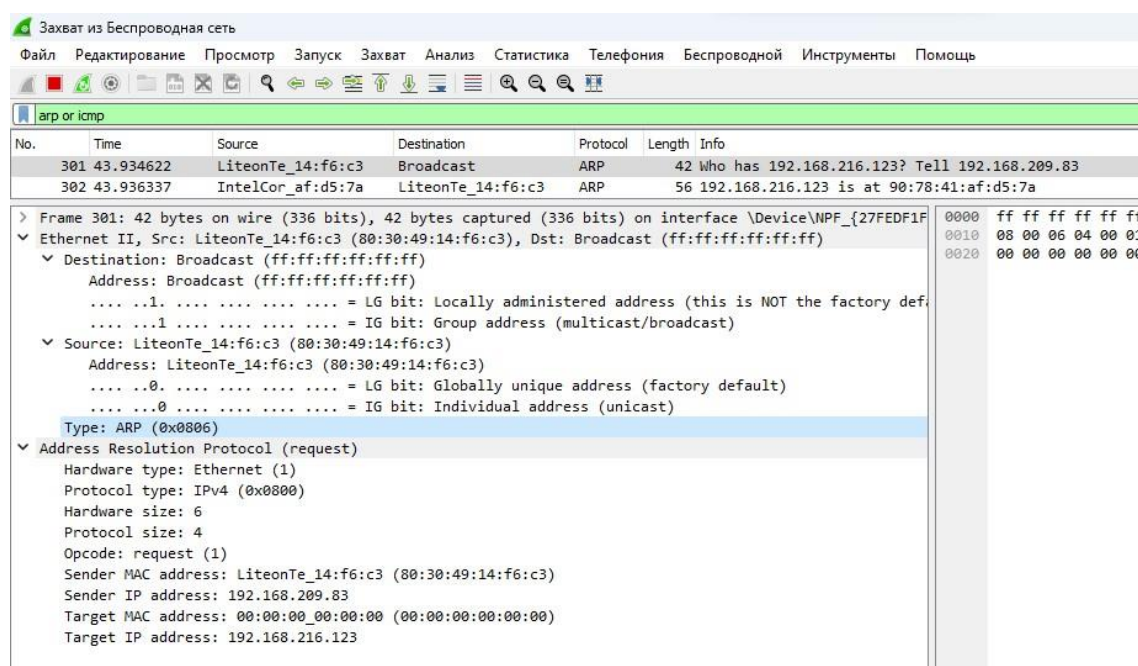


Рис.2.11. Сведения о кадрах данных протокола ARP

8. Начала новый процесс захвата трафика в Wireshark. Пропинговала по имени известный мне адрес — ping rudn.ru (рис.2.12).

```
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% потеря)
PS C:\Users\mrShcherbak_> |
```

Рис.2.12. Выполнение команды ping

9. Изучила запросы и ответы протоколов ARP и ICMP (рис.2.13). Определила MAC-адреса источника и получателя, определила тип MAC-адресов. Длина кадра = 74 байта. Вторая строка в панели показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника Source (80:30:49:14:f6:c3) и назначения Destination (70:18:a7:60:9c:eb). MAC-адреса источника и назначения являются индивидуальными и глобально администрируемыми. Мы получили [No response seen] (no response found!), отсутствие ответов.

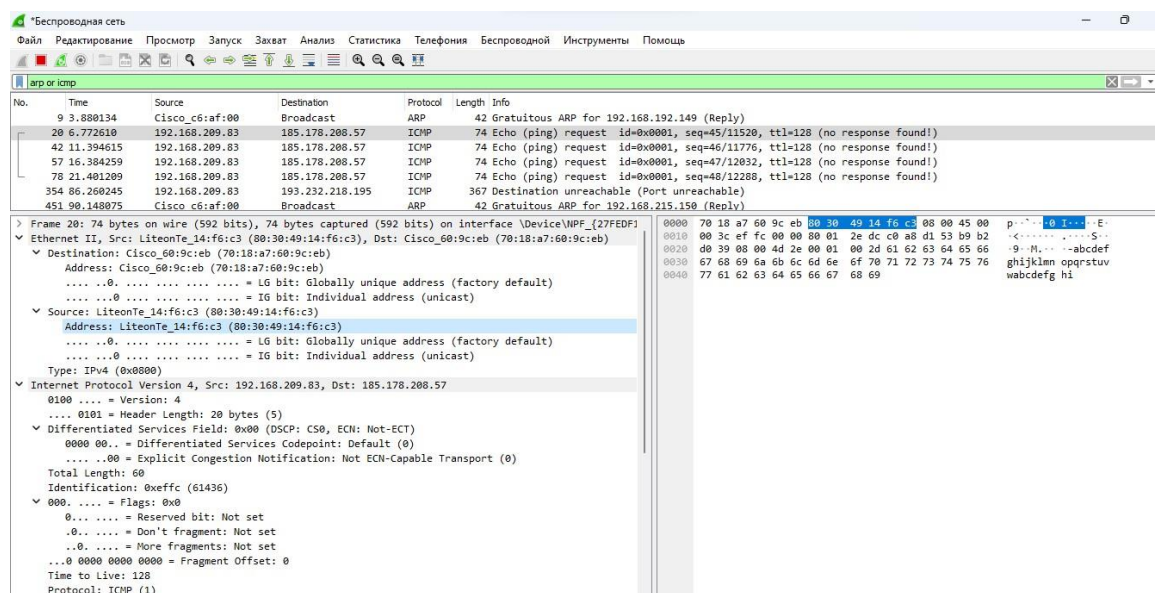


Рис.2.13. Сведения о запросах и ответах протоколов ARP и ICMP

3. Анализ протоколов транспортного уровня в Wireshark

3.1. Постановка задачи

С помощью Wireshark захватить и проанализировать пакеты HTTP, DNS в части заголовков и информации протоколов TCP, UDP, QUIC.

3.2. Выполнение

1. Запустила Wireshark. Выбрала активный сетевой интерфейс. Убедилась, что начался процесс захвата трафика (рис.3.1).

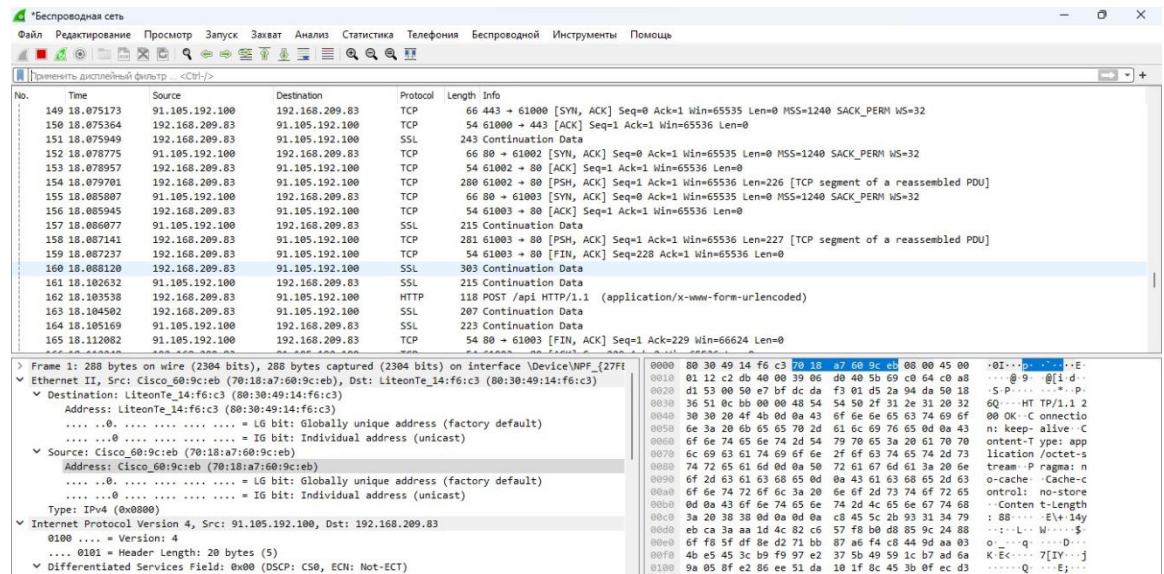


Рис.3.1. Показан процесс захвата трафика

2. В Wireshark в строке фильтра указала http и проанализировала информацию по протоколу TCP в случае запросов и ответов (рис.3.2 – рис.3.3). Get – запрос. Мы видим Source Port и Destination Port — источник и назначение. Порт на источнике задается случайным образом (порт клиента). Есть сведения про гипертекстовый протокол, где хранится информация. Адрес порта назначения — порт на локальной машине. Порт, который был источником на рис.3.2 является портом назначения на рис.3.3, то есть на этом порту клиент и прослушивает информацию и посылает.

*Беспроводная сеть						
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь						
http						
No.	Time	Source	Destination	Protocol	Length	Info
578	59.503245	192.168.209.83	91.105.192.100	HTTP	334	POST /api HTTP/1.1 (application/x-www-f
771	69.346782	192.168.209.83	188.185.10.243	HTTP	578	GET /www/hypertext/www/TheProject.html f
775	69.405854	188.185.10.243	192.168.209.83	HTTP	191	HTTP/1.1 302 Found
831	69.677017	192.168.209.83	2.23.167.179	HTTP	297	GET /MFwUTBPME0wSzAJBgUrDgMCGGUABBRISn
839	69.690477	2.23.167.179	192.168.209.83	OCSP	942	Response
880	73.231200	192.168.209.83	188.185.123.232	HTTP	549	GET /about HTTP/1.1
885	73.286170	188.185.123.232	192.168.209.83	HTTP	162	HTTP/1.1 302 Found
932	73.490207	192.168.209.83	104.18.15.101	HTTP	291	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBQh80h
936	73.498741	104.18.15.101	192.168.209.83	OCSP	1047	Response
966	75.175825	91.105.192.100	192.168.209.83	HTTP	288	HTTP/1.1 200 OK
969	75.207188	192.168.209.83	91.105.192.100	HTTP	350	POST /api HTTP/1.1 (application/x-www-f
<div> <div>Source Port: 61031</div> <div>Destination Port: 80</div> <div>[Stream index: 55]</div> <div>[Conversation completeness: Complete, WITH_DATA (31)]</div> <div>[TCP Segment Len: 524]</div> <div>Sequence Number: 1 (relative sequence number)</div> <div>Sequence Number (raw): 820873544</div> <div>[Next Sequence Number: 525 (relative sequence number)]</div> <div>Acknowledgment Number: 1 (relative ack number)</div> <div>Acknowledgment number (raw): 217209822</div> <div>0101 = Header Length: 20 bytes (5)</div> <div>> Flags: 0x018 (PSH, ACK)</div> <div>Window: 256</div> <div>[Calculated window size: 65536]</div> <div>[Window size scaling factor: 256]</div> <div>Checksum: 0x01db [unverified]</div> <div>[Checksum Status: Unverified]</div> <div>Urgent Pointer: 0</div> <div>> [Timestamps]</div> <div>> [SEQ/ACK analysis]</div> <div>TCP payload (524 bytes)</div> <div>Hypertext Transfer Protocol</div> </div> <div> <div>0020 0a f3</div> <div>0030 01 00</div> <div>0040 79 70</div> <div>0050 50 72</div> <div>0060 50 2f</div> <div>0070 65 2d</div> <div>0080 43 6f</div> <div>0090 2d 61</div> <div>00a0 49 6e</div> <div>00b0 73 3a</div> <div>00c0 3a 20</div> <div>00d0 69 6e</div> <div>00e0 57 69</div> <div>00f0 65 57</div> <div>0100 4b 48</div> <div>0110 6f 29</div> <div>0120 30 2e</div> <div>0130 36 20</div> <div>0140 2e 33</div> <div>0150 74 2f</div> <div>0160 6f 6e</div> <div>0170 6c 69</div> <div>0180 2e 39</div> <div>0190 61 67</div> <div>01a0 2e 38</div> </div>						

Рис.3.2. Сведения по протоколу TCP (GET)

*Беспроводная сеть						
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь						
http						
No.	Time	Source	Destination	Protocol	Length	Info
578	59.503245	192.168.209.83	91.105.192.100	HTTP	334	POST /api HTTP/1.1 (application/x-www-
771	69.346782	192.168.209.83	188.185.10.243	HTTP	578	GET /www/hypertext/www/TheProject.html
775	69.405854	188.185.10.243	192.168.209.83	HTTP	191	HTTP/1.1 302 Found
831	69.677017	192.168.209.83	2.23.167.179	HTTP	297	GET /MFwUTBPME0wSzAJBgUrDgMCGGUABBRISn
839	69.690477	2.23.167.179	192.168.209.83	OCSP	942	Response
880	73.231200	192.168.209.83	188.185.123.232	HTTP	549	GET /about HTTP/1.1
885	73.286170	188.185.123.232	192.168.209.83	HTTP	162	HTTP/1.1 302 Found
932	73.490207	192.168.209.83	104.18.15.101	HTTP	291	GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBQh80h
936	73.498741	104.18.15.101	192.168.209.83	OCSP	1047	Response
966	75.175825	91.105.192.100	192.168.209.83	HTTP	288	HTTP/1.1 200 OK
969	75.207188	192.168.209.83	91.105.192.100	HTTP	350	POST /api HTTP/1.1 (application/x-www-
<div> <div>Source Port: 80</div> <div>Destination Port: 61031</div> <div>[Stream index: 55]</div> <div>[Conversation completeness: Complete, WITH_DATA (31)]</div> <div>[TCP Segment Len: 137]</div> <div>Sequence Number: 1 (relative sequence number)</div> <div>Sequence Number (raw): 217209822</div> <div>[Next Sequence Number: 138 (relative sequence number)]</div> <div>Acknowledgment Number: 525 (relative ack number)</div> <div>Acknowledgment number (raw): 820874068</div> <div>0101 = Header Length: 20 bytes (5)</div> <div>> Flags: 0x018 (PSH, ACK)</div> <div>Window: 501</div> <div>[Calculated window size: 64128]</div> <div>[Window size scaling factor: 128]</div> <div>Checksum: 0x74d3 [unverified]</div> <div>[Checksum Status: Unverified]</div> <div>Urgent Pointer: 0</div> <div>> [Timestamps]</div> <div>> [SEQ/ACK analysis]</div> <div>TCP payload (137 bytes)</div> <div>Hypertext Transfer Protocol</div> </div> <div> <div>0000 80 3f</div> <div>0010 00 b0</div> <div>0020 d1 50</div> <div>0030 01 f0</div> <div>0040 30 30</div> <div>0050 74 2d</div> <div>0060 61 70</div> <div>0070 69 6e</div> <div>0080 2f 70</div> <div>0090 57 50</div> <div>00a0 6d 6e</div> <div>00b0 6c 30</div> </div>						

Рис.3.3. Сведения по протоколу TCP

3. В Wireshark в строке фильтра указала dns и проанализировала информацию по протоколу UDP в случае запросов и ответов (рис.3.4). Длина кадра = 91 байт. Вторая строка в панели показывает, что это кадр Ethernet II. Также отображаются MAC-адреса источника Source (80:30:49:14:f6:c3) и назначения Destination (70:18:a7:60:9c:eb). MAC-адреса источника и назначения являются индивидуальными и глобально администрируемыми. Показан заголовок протокола сетевого уровня IPv4. Средний раздел содержит информацию о поле данных кадра. Данные содержат IPv4-адреса источника (192.168.209.83) и назначения (193.232.218.195).

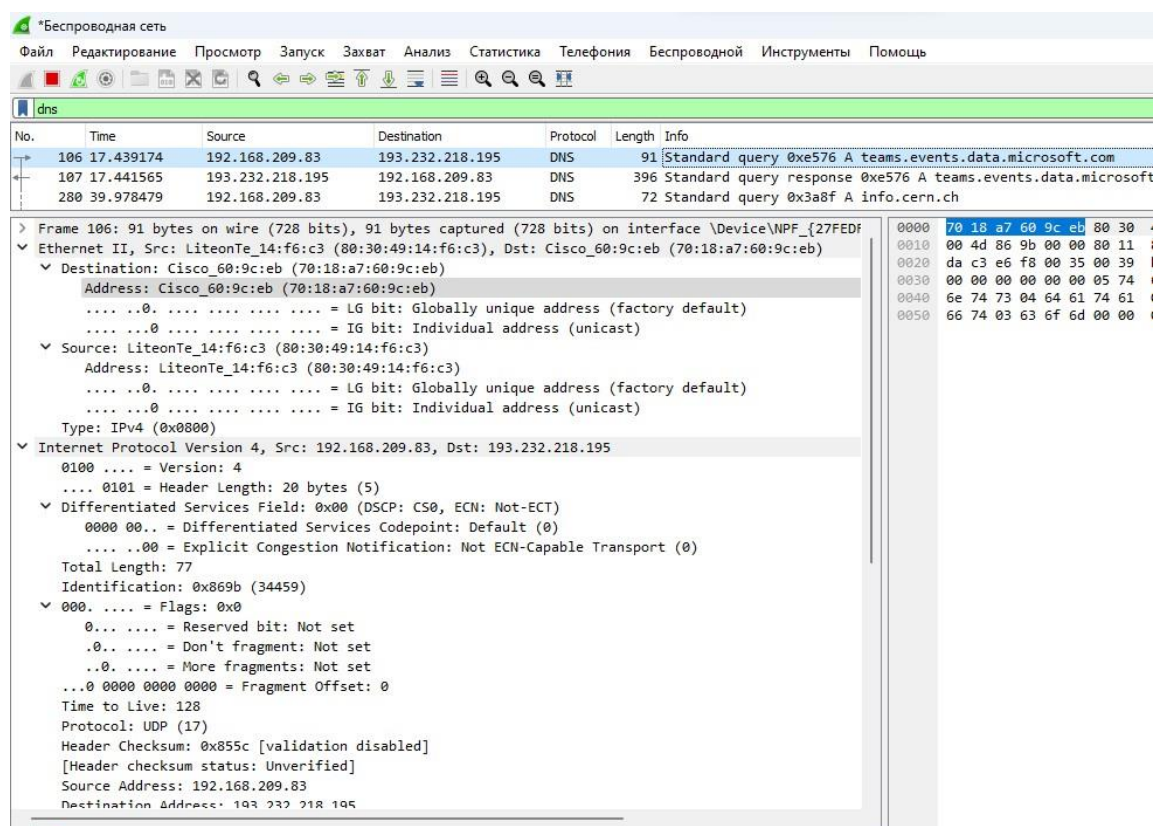


Рис.3.4. Поиск по фильтру dns

На рис.3.5 в заголовке UDP мы видим случайный непривилигированный Src port и Dst port 53 — порт назначения. Видим адрес источника 192.168.209.83 и назначения 193.232.218.195. В данном случае dns работает поверх udp. DNS (query).

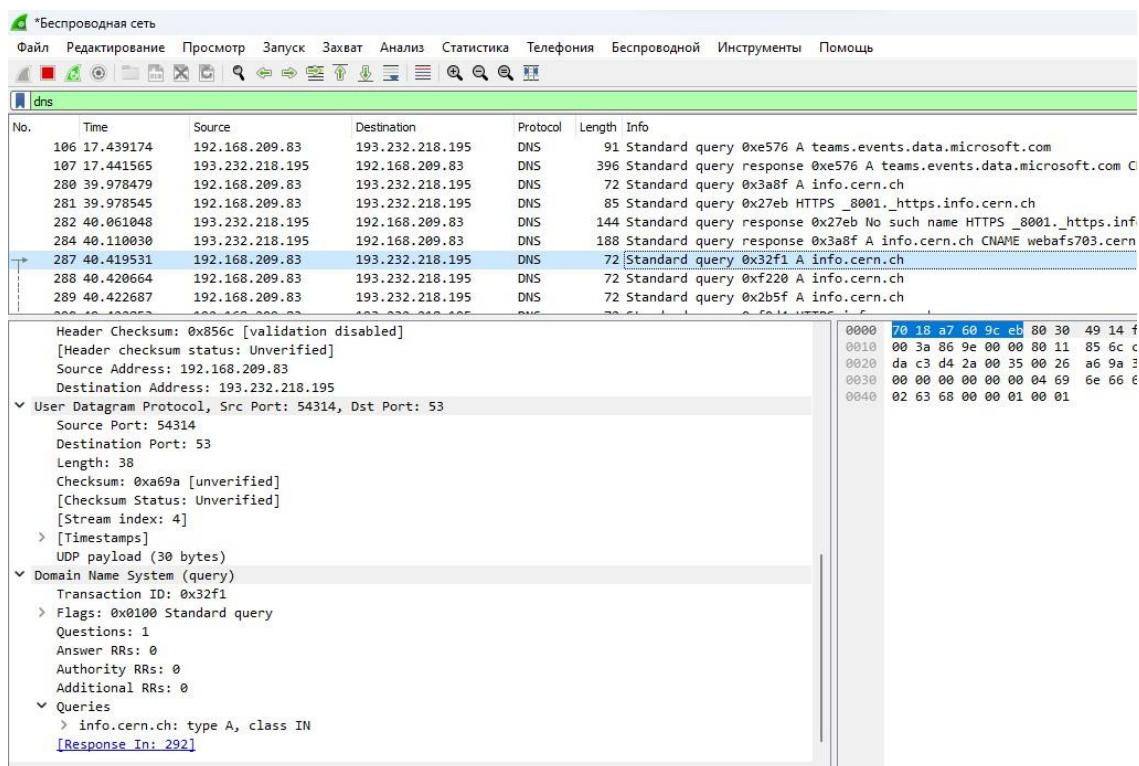


Рис.3.5. Сведения по протоколу UDP

4. В Wireshark в строке фильтра указала quic, однако на моем устройстве Wireshark не “зацепил” его.

Протокол QUIC может применяться в сети Интернет для обеспечения транспорта передаваемых по HTTP данных. Этот протокол позволяет мультиплексировать несколько потоков данных между двумя компьютерами, работая поверх протокола UDP, и содержит возможности шифрования, эквивалентные TLS и SSL.

QUIC является протоколом с установлением соединения, обеспечивающим взаимодействие между клиентом и сервером с сохранением состояния. Оконечные устройства взаимодействуют, обмениваясь пакетами QUIC. Большинство пакетов содержат кадры, которые несут управляющую информацию и данные приложения между оконечными устройствами. QUIC проверяет подлинность каждого пакета целиком и шифрует каждый пакет настолько, насколько это возможно. Пакеты QUIC передаются в дейтаграммах UDP, чтобы облегчить развёртывание в существующих системах и сетях.

QUIC обеспечивает необходимую обратную связь для реализации надёжной доставки и контроля перегрузки. Также соединения QUIC не привязаны строго к

одному сетевому пути. При переносе подключений используются идентификаторы подключения, чтобы позволить подключениям переходить на новый сетевой путь.

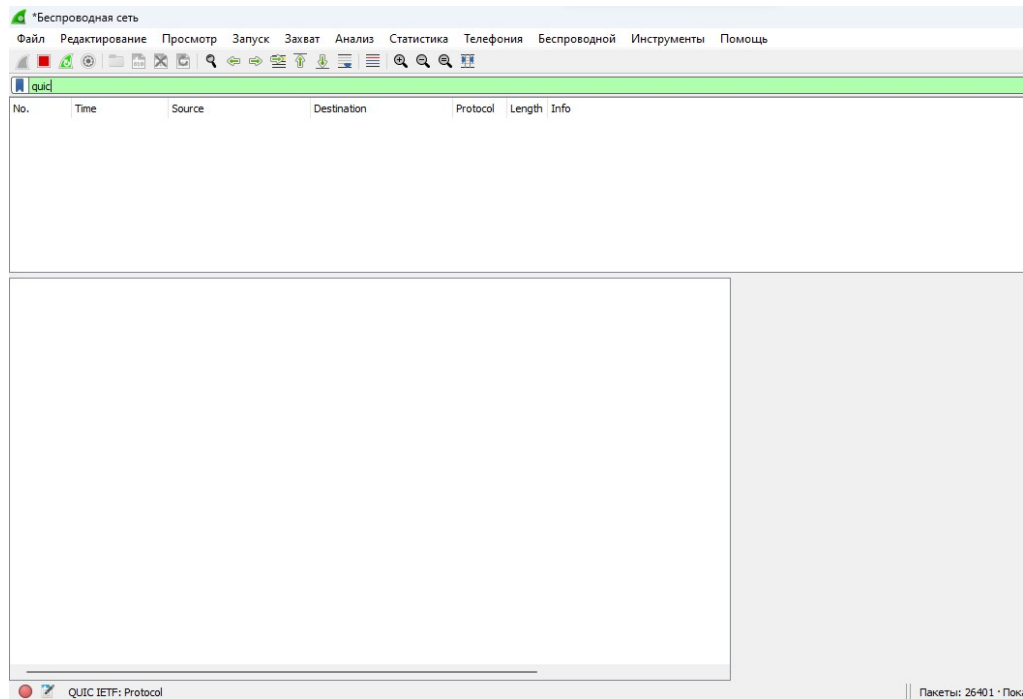


Рис.3.6. Сведения по протоколу UDP

5. Остановила захват трафика в Wireshark.

4. Анализ handshake протокола TCP в Wireshark

4.1. Постановка задачи

С помощью Wireshark проанализировать handshake протокола TCP.

4.2. Выполнение

1. Запустила Wireshark. Выбрала активный сетевой интерфейс. Убедилась, что начался процесс захвата трафика.

2. В Wireshark проанализировала handshake протокола TCP. Установление связи клиент-сервер в TCP осуществляется в три этапа (трёхступенчатый handshake). Сначала клиент отправляет SYN, т.е. в передаваемом сообщении установлен бит SYN (Synchronize Sequence Number — установить соединение), затем сервер отвечает ACK (подтверждение) + SYN, т.е. установлены биты SYN и ACK, и наконец, клиент отправляет ACK — подтверждение получения SYN сегмента от сервера. Это происходит после пассивного открытия сервера, где он начинает

прослушивать порт. Теперь клиент может посылать пакеты с данными на сервер по только что созданному виртуальному TCP-каналу. На рис.4.1. изображён первый этап рукопожатия — Sequence Number 1109604372, а Acknowledgment Number равен 0.

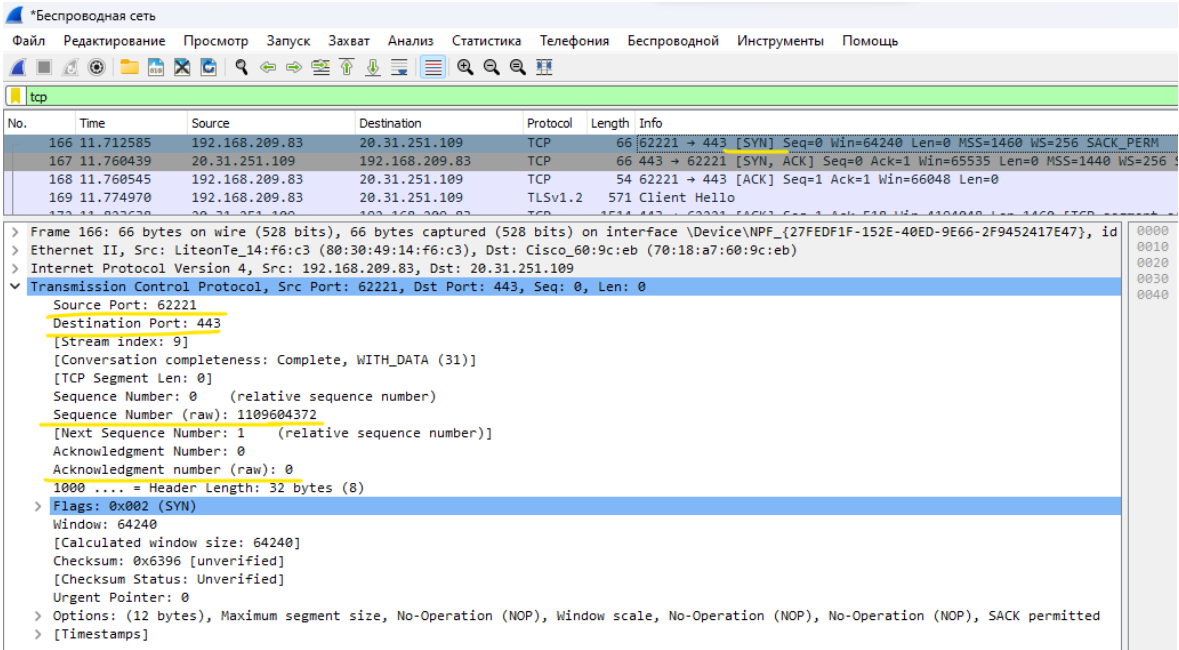


Рис.4.1. Первый этап рукопожатия протокола TCP

На рис.4.2 показан второй этап рукопожатия — Sequence Number стал равен 953830963 (хостом В установлено значение счётчика), а Acknowledgment Number стал равен Sequence Number первого этапа +1.

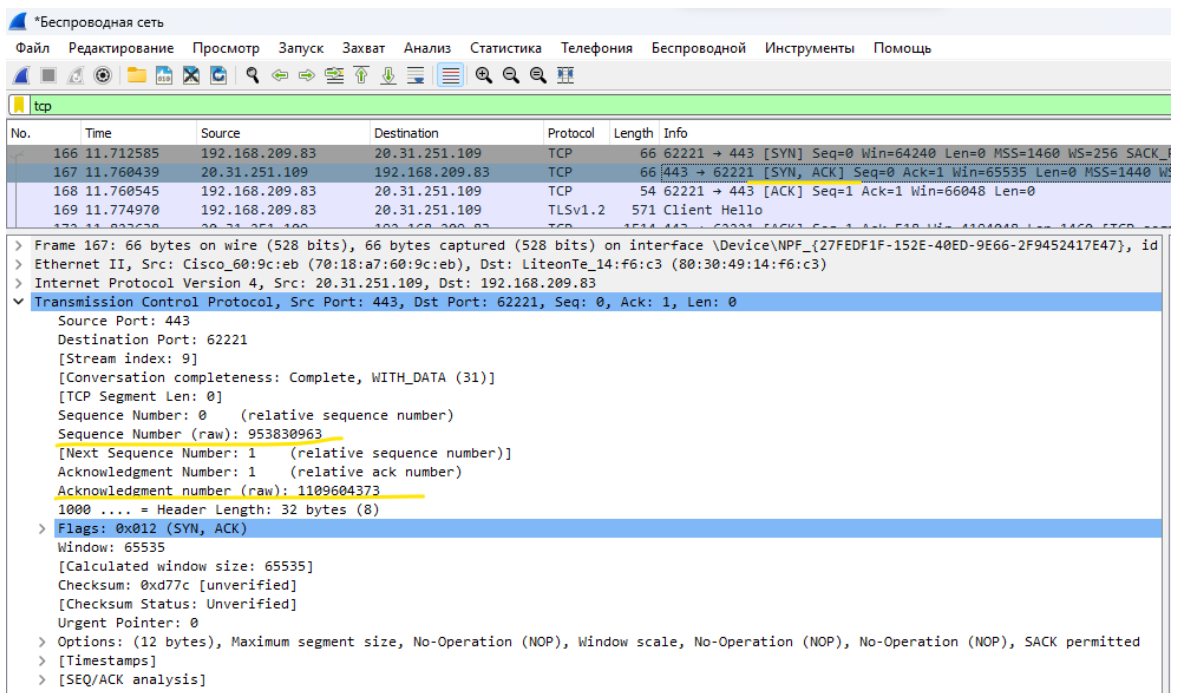


Рис.4.2. Второй этап рукопожатия протокола TCP

На рис.4.3 показан третий этап рукопожатия — Sequence Number стал равен Acknowledgment Number второго этапа, а Acknowledgment Number стал равен Sequence Number второго этапа +1.

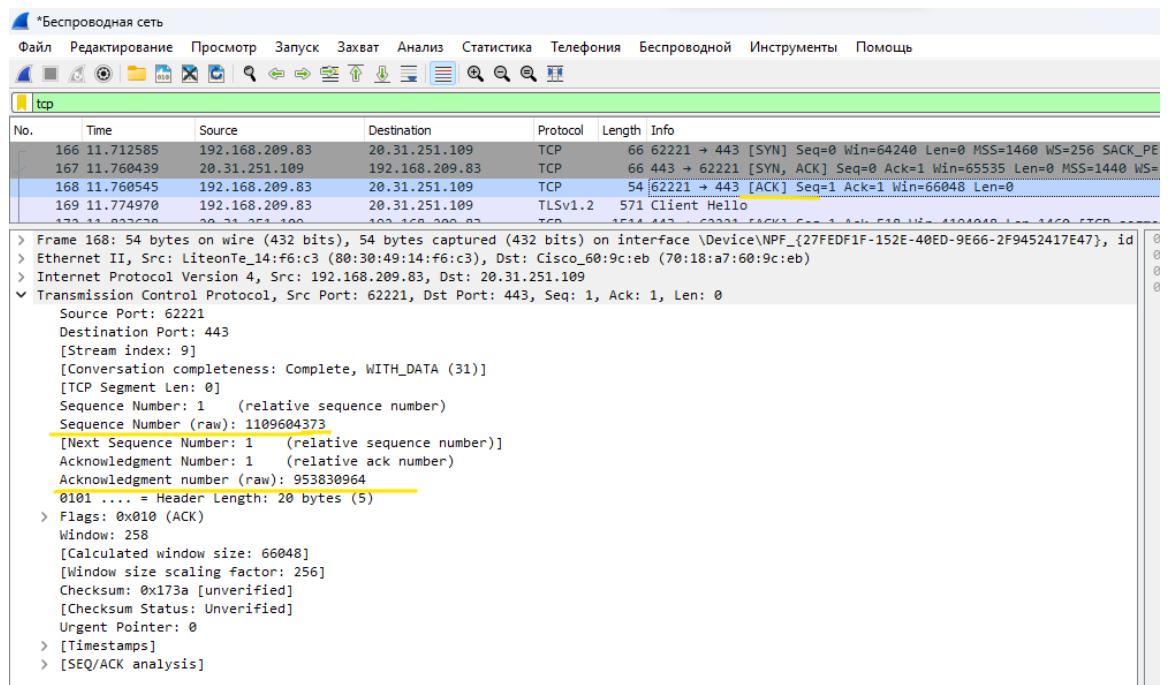


Рис.4.3. Третий этап рукопожатия протокола TCP

Из рассмотренной выше схемы создания TCP-соединения видно, что единственными идентификаторами TCP-абонентов и TCP-соединения являются два

параметра — Порядковый номер (Sequence Number) и Номер подтверждения (Acknowledgment Number).

3. В Wireshark в меню «Статистика» выбрала «График Потока» (рис.4.4). Мы можем увидеть трехэтапное рукопожатие. Цифра в начале стрелки — порт источника, а цифра на конце стрелки — порт назначения. Посылается флаг SYN (идёт установление сессии), затем посылаются два флага — SYN и ACK (в ответ сервер отвечает SYN-ACK. Номер подтверждения установлен на единицу больше принятого Порядкового номера (Sequence number). Поскольку сервер также будет отправлять данные, то для себя он тоже выбирает Порядковый номер (Sequence number) первого пакета с данными, который будет другим случайным числом. Затем отправляется флаг ACK (клиент отправляет ACK обратно на сервер. Порядковый номер устанавливается равным полученному значению подтверждения, а номер подтверждения устанавливается на единицу больше, чем принятый порядковый номер). Так работает handshake протокола TCP в Wireshark.

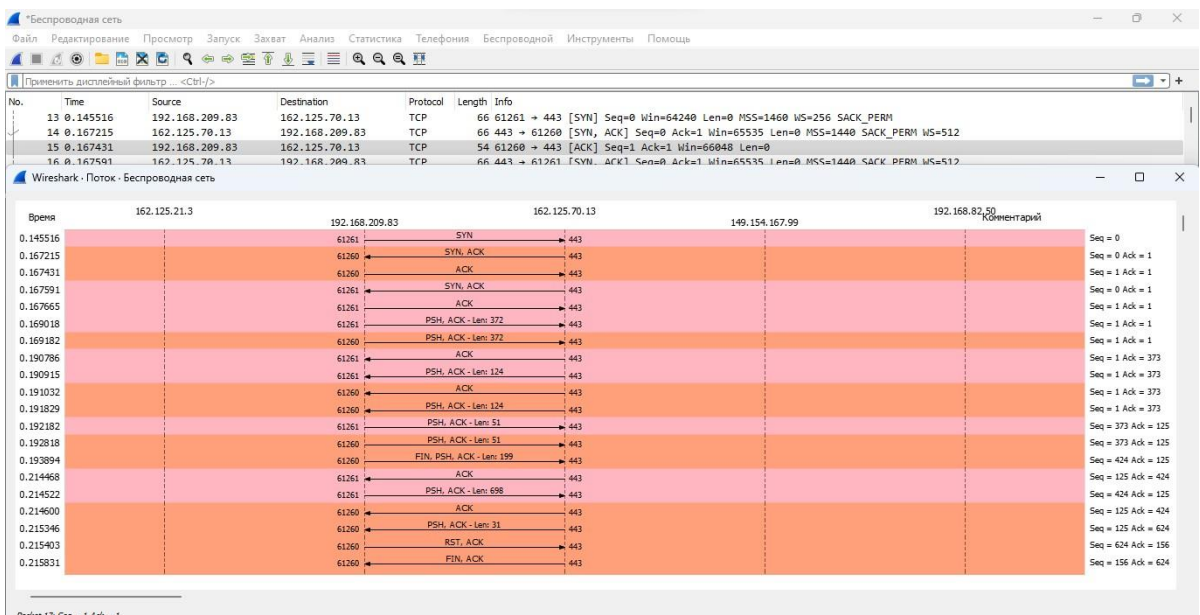


Рис.4.4. Просмотр графика потока

Закрытие соединения показано на рис.4.5. Чтобы закрыть TCP-соединение, закрывающая сторона должна отправить пакет FIN, который также содержит ACK для последних данных, полученных этой стороной, затем другая сторона должна ответить ACK о том, что она получила FIN, и уведомить приложение о том, что другая сторона закрывает соединение. Обычно приложение также закрывает соединение, что приводит к отправке другого FIN в сторону, инициирует закрытие

и ждет, пока АСК узнает, что соединение теперь полностью закрыто с обеих сторон.

Сторона, которая инициализировала закрытие соединения, не сможет снова использовать тот же IP-адрес и локальный порт для подключения к тому же IP-адресу и порту сервера в течение определенного периода времени, контролируемого операционной системой. Он должен дожидаться некоторого счетчика тайм-аута, установленного его ОС, чтобы истечь до истечения времени, прежде чем сможет это сделать.

Если во время закрытия соединения возникли какие-либо проблемы, соединение может быть прервано с помощью сброса вместо FIN.

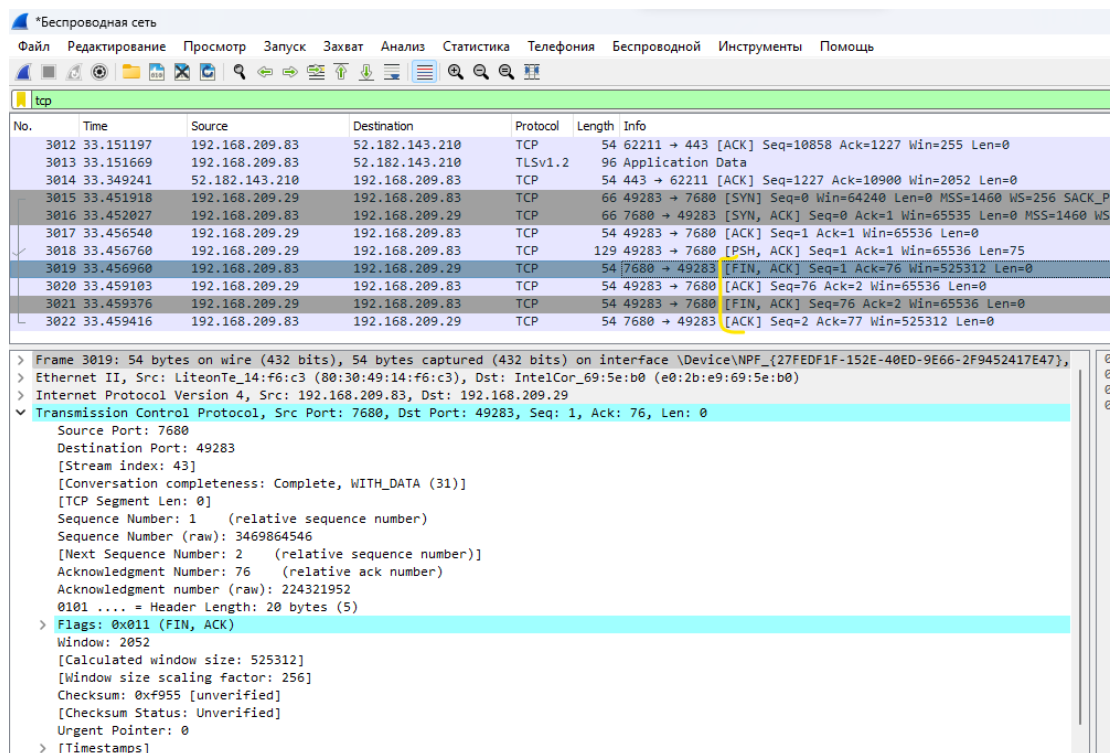


Рис.4.5. Закрытие TCP-соединения

4. Остановила захват трафика в Wireshark.

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.