

Российский Университет Дружбы Народов

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

Отчёт

о выполнении лабораторной работы № 3

Анализ трафика в Wireshark

по дисциплине: Сетевые технологии

Студент: Танрибергенов Эльдар

Группа: НПИбд-02-20

Студ. билет № 1032208074

Москва, 2022 г.

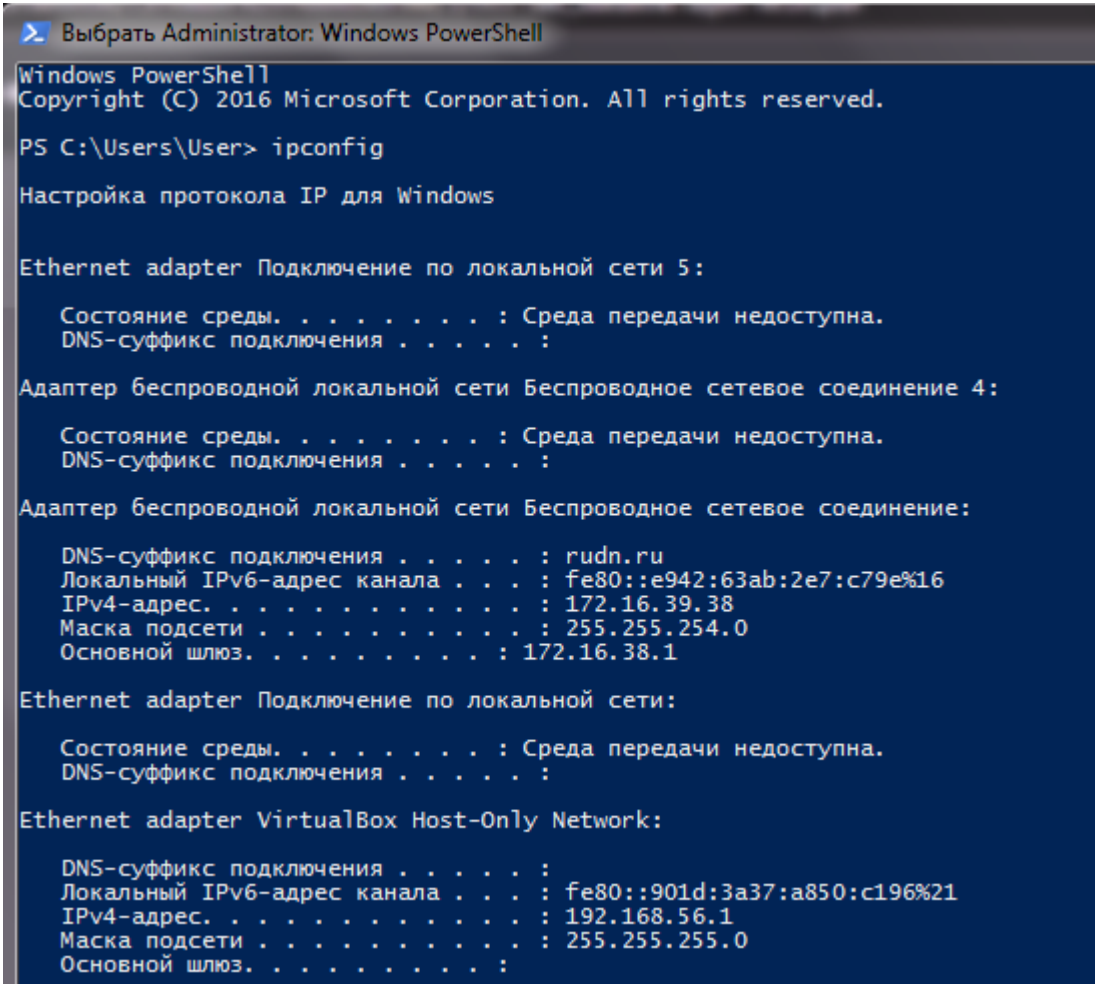
Цели работы:

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

Ход работы:

1. MAC-адресация

- 1.1. С помощью команды `ipconfig` вывел информацию о текущем сетевом соединении.



```
Выбрать Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\User> ipconfig

Настройка протокола IP для Windows

Ethernet adapter Подключение по локальной сети 5:

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

Адаптер беспроводной локальной сети Беспроводное сетевое соединение 4:

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

Адаптер беспроводной локальной сети Беспроводное сетевое соединение:

    DNS-суффикс подключения . . . . . : rudn.ru
    Локальный IPv6-адрес канала . . . : fe80::e942:63ab:2e7:c79e%16
    IPv4-адрес. . . . . : 172.16.39.38
    Маска подсети . . . . . : 255.255.254.0
    Основной шлюз. . . . . : 172.16.38.1

Ethernet adapter Подключение по локальной сети:

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

Ethernet adapter VirtualBox Host-Only Network:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::901d:3a37:a850:c196%21
    IPv4-адрес. . . . . : 192.168.56.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . :
```

Рис. 1.1.1. Текущее сетевое соединение.

Использовал разные опции команды.

Список опций.

Параметры:	
/?	Вывод данного справочного сообщения
/all	Вывод подробных сведений о конфигурации.
/release	Освобождение адреса IPv4 для указанного адаптера.
/release6	Освобождение адреса IPv6 для указанного адаптера.
/renew	Обновление адреса IPv4 для указанного адаптера.
/renew6	Обновление адреса IPv6 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. 1.1.2. Список опций команды `ipconfig`.

Параметр `/all` – вывод детальной информации по сетевым соединениям.

Адаптер беспроводной локальной сети Беспроводное сетевое соединение:	
DNS-суффикс подключения	: rudn.ru
Описание.	: Qualcomm Atheros AR956x Wireless Network Adapter
Физический адрес.	: 40-F0-2F-D4-48-14
DHCP включен.	: Да
Автонастройка включена.	: Да
Локальный IPv6-адрес канала	: fe80::e942:63ab:2e7:c79e%16(Основной)
IPv4-адрес.	: 172.16.39.38(Основной)
Маска подсети	: 255.255.254.0
Аренда получена.	: 19 октября 2022 г. 21:01:29
Срок аренды истекает.	: 19 октября 2022 г. 22:01:28
Основной шлюз.	: 172.16.38.1
Код класса DHCPv4.	:
DHCP-сервер.	: 192.168.80.59
IAID DHCPv6	: 205582383
DUID клиента DHCPv6	: 00-01-00-01-1A-BD-BE-FF-20-1A-06-B8-A5-F7
DNS-серверы.	: 37.18.92.5 193.232.218.194
NetBios через TCP/IP.	: Включен

Рис. 1.1.3. Параметр `/all`.

Параметр ***/release*** – сброс IPv4-адреса сетевого интерфейса. После сброса адреса активируется механизм Windows APIPA (Automatic Private IP Addressing). Этот механизм работает, когда компьютеры настроены на автоматическое получение IP-адресов, но в сети нет DHCP-сервера или компьютер не может до него достучаться. В этих случаях APIPA сам назначает себе адрес. IPv4-адрес моего адаптера изменился:

```
Адаптер беспроводной локальной сети Беспроводное сетевое соединение:
DNS-суффикс подключения . . . . . :
Описание. . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
Физический адрес. . . . . : 40-F0-2F-D4-48-14
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::e942:63ab:2e7:c79e%16(Основной)
Автонастройка IPv4-адреса . . . . : 169.254.199.158(Основной)
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . :
Код класса DHCPv4. . . . . :
IAID DHCPv6 . . . . . : 205582383
DUID клиента DHCPv6 . . . . . : 00-01-00-01-1A-BD-BE-FF-20-1A-06-B8-A5-F7
DNS-серверы. . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBios через TCP/IP. . . . . : Включен
```

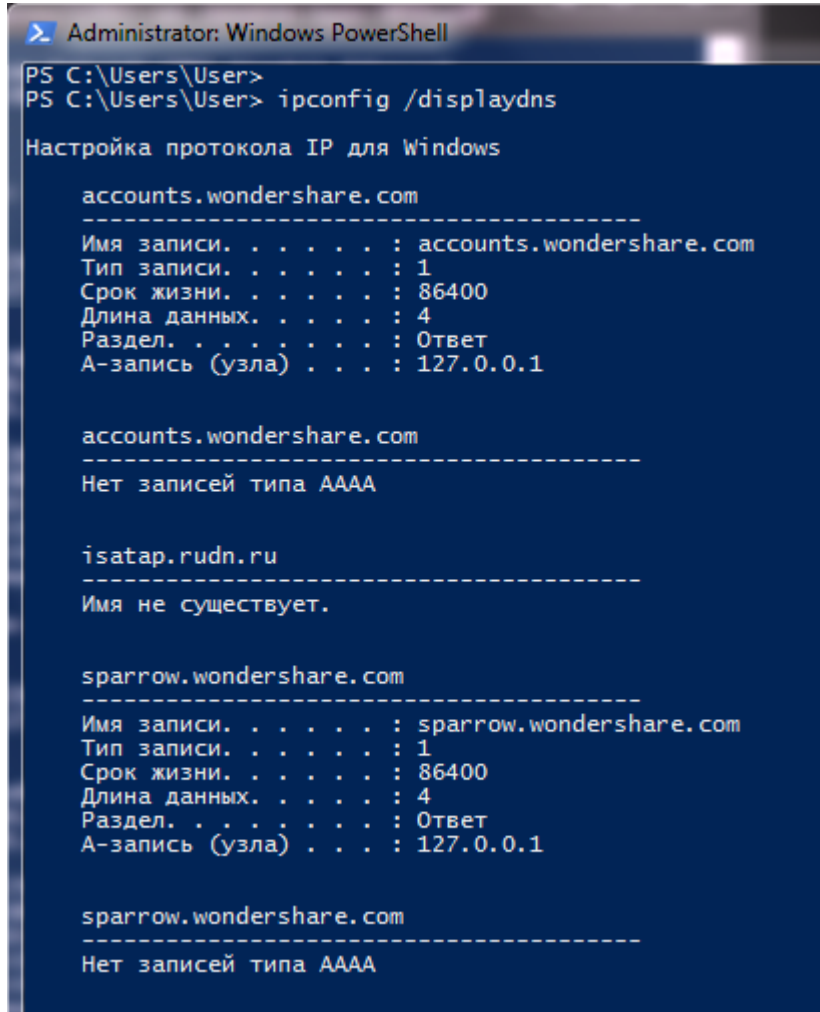
Рис. 1.1.4. Параметр */release*

Параметр ***/renew*** – обновление IPv4-адреса. В принудительном порядке заставит компьютер повторно получить IPv4-адрес от сервера. Значения вернулись к начальным:

```
Адаптер беспроводной локальной сети Беспроводное сетевое соединение:
DNS-суффикс подключения . . . . . : rudn.ru
Описание. . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
Физический адрес. . . . . : 40-F0-2F-D4-48-14
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::e942:63ab:2e7:c79e%16(Основной)
IPv4-адрес. . . . . : 172.16.39.38(Основной)
Маска подсети . . . . . : 255.255.254.0
Аренда получена. . . . . : 19 октября 2022 г. 21:28:58
Срок аренды истекает. . . . . : 19 октября 2022 г. 22:28:58
Основной шлюз. . . . . : 172.16.38.1
Код класса DHCPv4. . . . . :
DHCP-сервер. . . . . : 192.168.80.59
IAID DHCPv6 . . . . . : 205582383
DUID клиента DHCPv6 . . . . . : 00-01-00-01-1A-BD-BE-FF-20-1A-06-B8-A5-F7
DNS-серверы. . . . . : 37.18.92.5
                        193.232.218.194
NetBios через TCP/IP. . . . . : Включен
```

Рис. 1.1.5. Параметр */renew*.

Параметр */displaydns* – отображение кэша.



```
Administrator: Windows PowerShell
PS C:\Users\User>
PS C:\Users\User> ipconfig /displaydns

Настройка протокола IP для Windows

accounts.wondershare.com
-----
Имя записи. . . . . : accounts.wondershare.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 86400
Длина данных. . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 127.0.0.1

accounts.wondershare.com
-----
Нет записей типа AAAA

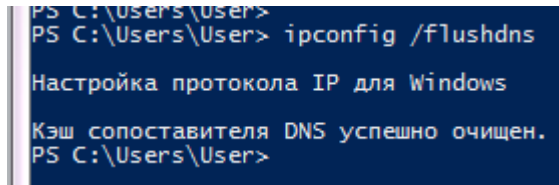
isatap.rudn.ru
-----
Имя не существует.

sparrow.wondershare.com
-----
Имя записи. . . . . : sparrow.wondershare.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 86400
Длина данных. . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 127.0.0.1

sparrow.wondershare.com
-----
Нет записей типа AAAA
```

Рис. 1.1.6. Параметр */displaydns* .

Параметр */flushdns* – удаление кэша. Однако у меня не получилось удалить кэш: при проверке кэша все значения сохранились.



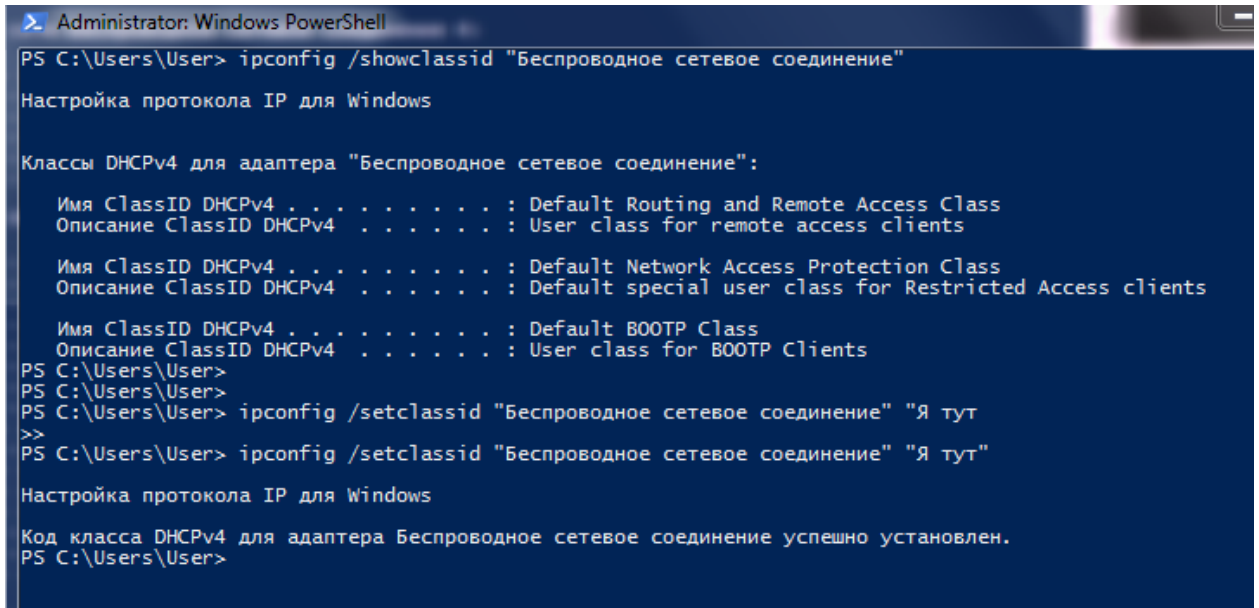
```
PS C:\Users\User>
PS C:\Users\User> ipconfig /flushdns

Настройка протокола IP для Windows

Кэш сопоставителя DNS успешно очищен.
PS C:\Users\User>
```

Рис. 1.1.7. Параметр */flushdns* .

Параметр */showclassid* – отображение всех допустимых идентификаторов класса DHCP для указанного адаптера.



```
Administrator: Windows PowerShell
PS C:\Users\User> ipconfig /showclassid "Беспроводное сетевое соединение"
Настройка протокола IP для Windows

Классы DHCPv4 для адаптера "Беспроводное сетевое соединение":

    Имя ClassID DHCPv4 . . . . . : Default Routing and Remote Access Class
    Описание ClassID DHCPv4 . . . . . : User class for remote access clients

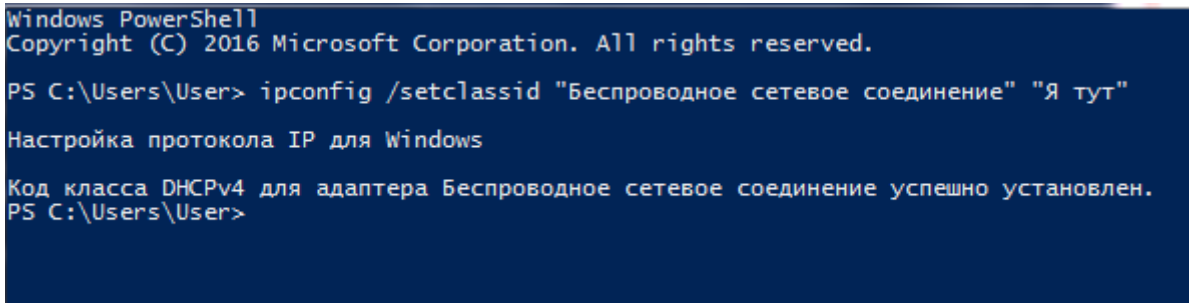
    Имя ClassID DHCPv4 . . . . . : Default Network Access Protection Class
    Описание ClassID DHCPv4 . . . . . : Default special user class for Restricted Access clients

    Имя ClassID DHCPv4 . . . . . : Default BOOTP Class
    Описание ClassID DHCPv4 . . . . . : User class for BOOTP Clients
PS C:\Users\User>
PS C:\Users\User>
PS C:\Users\User> ipconfig /setclassid "Беспроводное сетевое соединение" "Я тут"
>>
PS C:\Users\User> ipconfig /setclassid "Беспроводное сетевое соединение" "Я тут"
Настройка протокола IP для Windows

Код класса DHCPv4 для адаптера Беспроводное сетевое соединение успешно установлен.
PS C:\Users\User>
```

Рис. 1.1.8. Параметр */showclassid*.

Параметр */setclassid* – установка значения идентификатора класса DHCP указанному адаптеру. Я задал своему рабочему адаптеру значение ID – «Я тут».



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\User> ipconfig /setclassid "Беспроводное сетевое соединение" "Я тут"
Настройка протокола IP для Windows

Код класса DHCPv4 для адаптера Беспроводное сетевое соединение успешно установлен.
PS C:\Users\User>
```

Рис. 1.1.9. Параметр */setclassid*.

```

Адаптер беспроводной локальной сети Беспроводное сетевое соединение:

DNS-суффикс подключения . . . . . : rudn.ru
Описание. . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
Физический адрес. . . . . : 40-F0-2F-D4-48-14
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::e942:63ab:2e7:c79e%16(Основной)
IPv4-адрес. . . . . : 172.16.39.38(Основной)
Маска подсети . . . . . : 255.255.254.0
Аренда получена. . . . . : 19 октября 2022 г. 21:28:58
Срок аренды истекает. . . . . : 19 октября 2022 г. 23:46:41
Основной шлюз. . . . . : 172.16.38.1
Код класса DHCPv4. . . . . : Я тут
DHCP-сервер. . . . . : 192.168.80.59
IAID DHCPv6 . . . . . : 205582383
DUID клиента DHCPv6 . . . . . : 00-01-00-01-1A-BD-BE-FF-20-1A-06-B8-A5-F7
DNS-серверы. . . . . : 37.18.92.5
                        193.232.218.194
NetBios через TCP/IP. . . . . : Включен

```

Рис. 1.1.10. Параметр /setclassid. Проверка результата.

Для того чтобы сбросить данное значение, нужно просто оставить пустым ID при вводе команды.

```

PS C:\Users\User> ipconfig /setclassid "Беспроводное сетевое соединение"

Настройка протокола IP для Windows

Код класса DHCPv4 для адаптера Беспроводное сетевое соединение успешно установлен.
PS C:\Users\User>

```

Рис. 1.1.11. Сброс значения id класса .

```

Адаптер беспроводной локальной сети Беспроводное сетевое соединение:

DNS-суффикс подключения . . . . . : rudn.ru
Описание. . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
Физический адрес. . . . . : 40-F0-2F-D4-48-14
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::e942:63ab:2e7:c79e%16(Основной)
IPv4-адрес. . . . . : 172.16.39.38(Основной)
Маска подсети . . . . . : 255.255.254.0
Аренда получена. . . . . : 19 октября 2022 г. 21:28:58
Срок аренды истекает. . . . . : 19 октября 2022 г. 23:48:23
Основной шлюз. . . . . : 172.16.38.1
Код класса DHCPv4. . . . . :
DHCP-сервер. . . . . : 192.168.80.59
IAID DHCPv6 . . . . . : 205582383
DUID клиента DHCPv6 . . . . . : 00-01-00-01-1A-BD-BE-FF-20-1A-06-B8-A5-F7
DNS-серверы. . . . . : 37.18.92.5
                        193.232.218.194
NetBios через TCP/IP. . . . . : Включен

```

Рис. 1.1.12. Проверка сброса.

1.2. Определить MAC-адреса сетевых интерфейсов на компьютере.

Вот MAC-адреса моих сетевых интерфейсов (отмечены жёлтым).

```
DNS-суффикс подключения . . . . . : rudn.ru
Описание. . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
Физический адрес. . . . . : 40-F0-2E-D4-48-14
DHCP-включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::e942:63ab:2e7:c79e%16(Основной)
IPv4-адрес. . . . . : 172.16.39.38(Основной)
Маска подсети . . . . . : 255.255.254.0
Аренда получена. . . . . : 19 октября 2022 г. 21:28:58
Срок аренды истекает. . . . . : 19 октября 2022 г. 23:48:23
Основной шлюз. . . . . : 172.16.38.1
Код класса DHCPv4. . . . . :
DHCP-сервер. . . . . : 192.168.80.59
IAID DHCPv6 . . . . . : 205582383
DUID клиента DHCPv6 . . . . . : 00-01-00-01-1A-BD-BE-FF-20-1A-06-B8-A5-F7
DNS-серверы. . . . . : 37.18.92.5
                        193.232.218.194
NetBios через TCP/IP. . . . . : Включен

Ethernet adapter Подключение по локальной сети:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Broadcom NetLink (TM) Gigabit Ethernet
Физический адрес. . . . . : 20-1A-06-DF-C7-D8
DHCP-включен. . . . . : Да
Автонастройка включена. . . . . : Да

Ethernet adapter VirtualBox Host-Only Network:

DNS-суффикс подключения . . . . . :
Описание. . . . . : VirtualBox Host-Only Ethernet Adapter
Физический адрес. . . . . : 0A-00-27-00-00-15
DHCP-включен. . . . . : Нет
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::901d:3a37:a850:c196%21(Основной)
IPv4-адрес. . . . . : 192.168.56.1(Основной)
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . :
IAID DHCPv6 . . . . . : 386531367
DUID клиента DHCPv6 . . . . . : 00-01-00-01-1A-BD-BE-FF-20-1A-06-B8-A5-F7
DNS-серверы. . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBios через TCP/IP. . . . . : Включен

Ethernet adapter Беспроводное подключение по локальной сети:
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
Физический адрес. . . . . : 40-F0-2E-D4-48-14
DHCP-включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::e942:63ab:2e7:c79e%16(Основной)
IPv4-адрес. . . . . : 172.16.39.38(Основной)
Маска подсети . . . . . : 255.255.254.0
Основной шлюз. . . . . : 172.16.38.1
Код класса DHCPv4. . . . . :
DHCP-сервер. . . . . : 192.168.80.59
IAID DHCPv6 . . . . . : 205582383
DUID клиента DHCPv6 . . . . . : 00-01-00-01-1A-BD-BE-FF-20-1A-06-B8-A5-F7
DNS-серверы. . . . . : 37.18.92.5
                        193.232.218.194
NetBios через TCP/IP. . . . . : Включен
```

Рис. 1.2.1. MAC-адреса сетевых интерфейсов.

1.3. Описание структуры MAC-адресов моего устройства.

Первые 6 цифр идентифицируют производителя, оставшиеся 6 – сетевой интерфейс.

- a) MAC-адрес адаптера «Беспроводное сетевое соединение» «Qualcomm Atheros ...»:
Значение: 40-F0-2F-D4-48-14.

Старший байт: 40

Двоичное представление старшего байта: 01000000

Первый бит старшего байта = 0 – адрес индивидуальный

Второй бит старшего байта = 0 – адрес глобально администрированный.

- b) MAC-адрес адаптера «Подключение по локальной сети» «Broadcom NetLink ...»:
Значение: 20-1A-06-DF-C7-D8

Старший байт: 20

Двоичное представление старшего байта: 00100000

Первый бит старшего байта = 0 – адрес индивидуальный

Второй бит старшего байта = 0 – адрес глобально администрированный.

- c) MAC-адрес адаптера «Беспроводное сетевое соединение» «VirtualBox Host-Only ...»:
Значение: 0A-00-27-00-00-15

Старший байт: 0A

Двоичное представление старшего байта: 00001010

Первый бит старшего байта = 0 – адрес индивидуальный

Второй бит старшего байта = 1 – адрес локально администрированный.

2. Анализ кадров канального уровня в Wireshark.

2.1. Установил Wireshark. Запустил. (рис. 2.1).

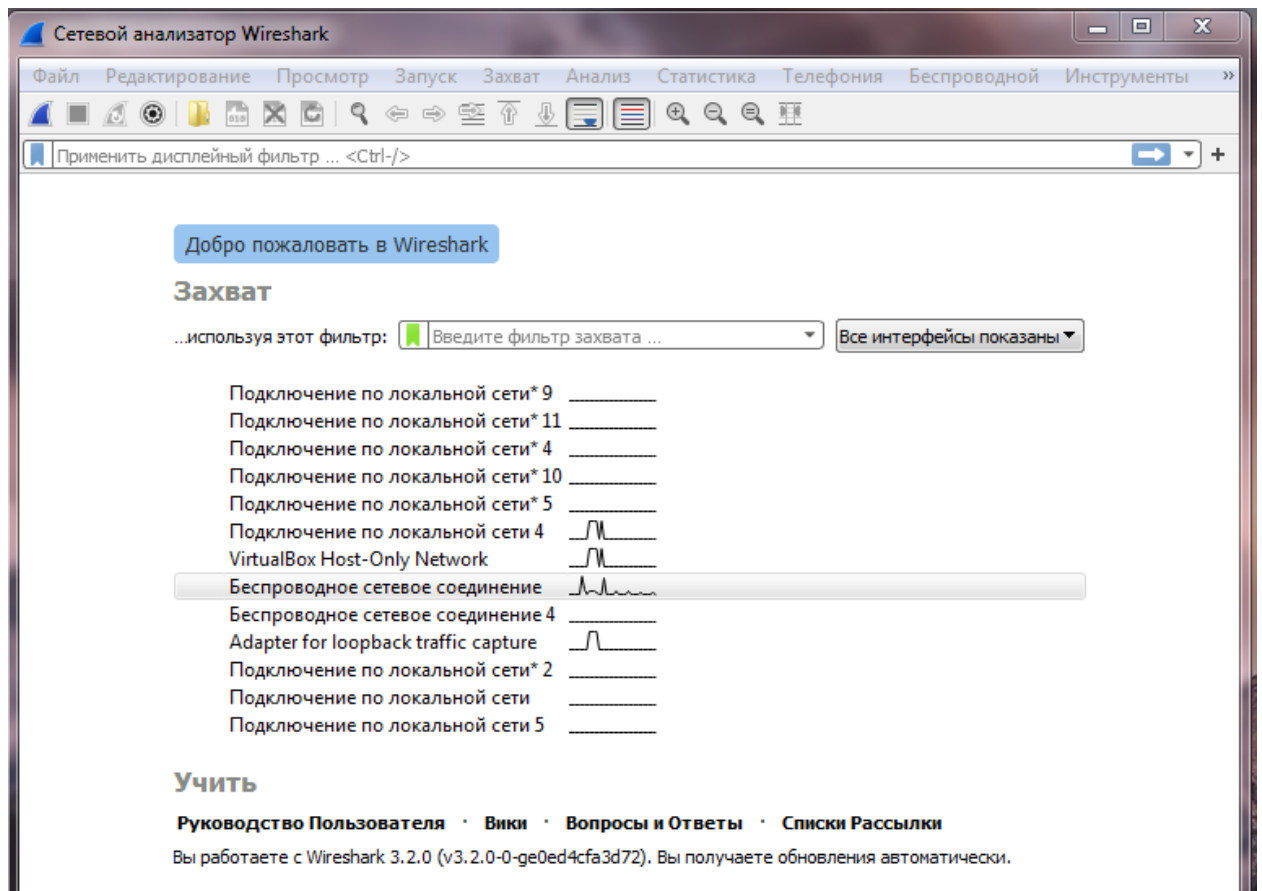


Рис. 2.1. Запуск Wireshark.

2.2. Выбрал активный на устройстве сетевой интерфейс. Убедился, что начался процесс захвата трафика (рис. 2.2).

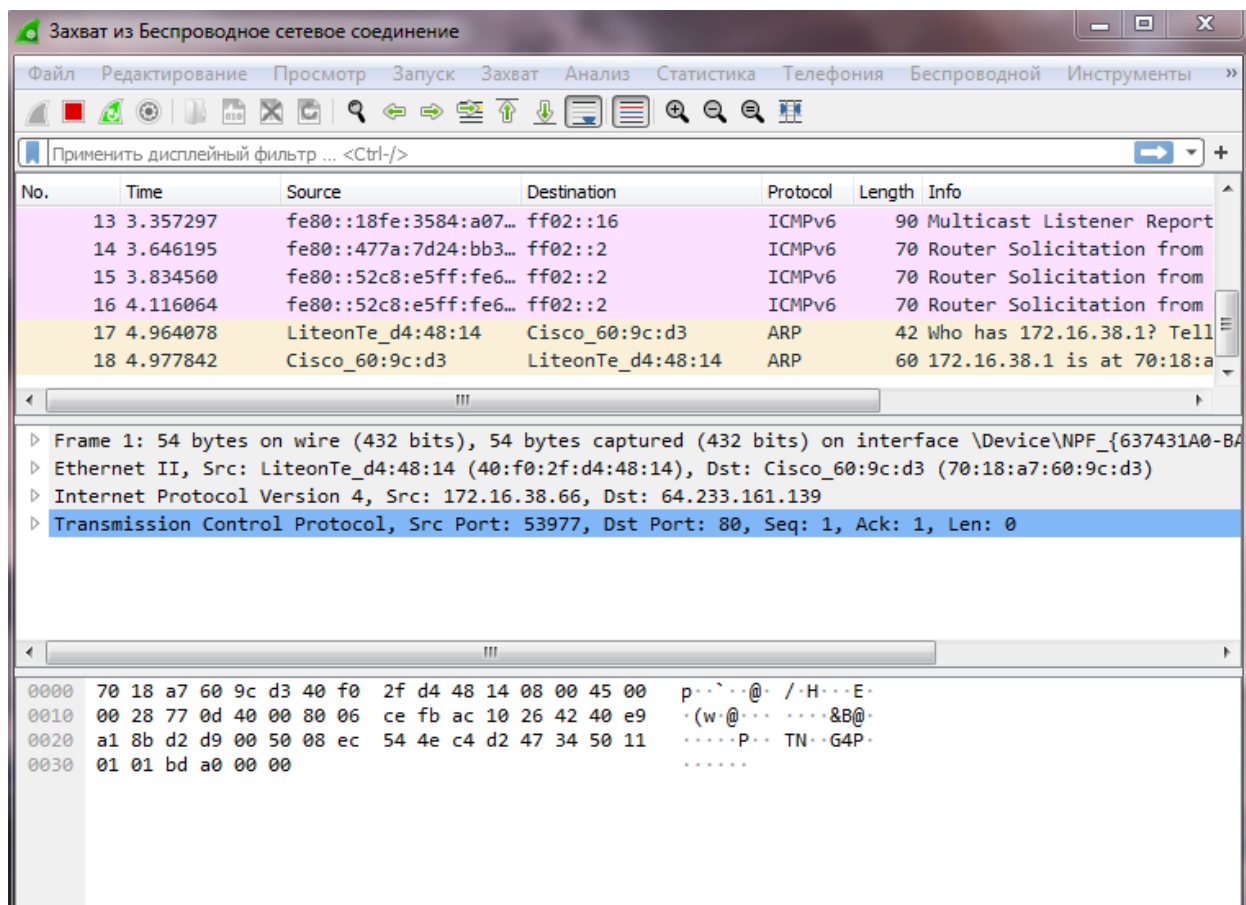


Рис. 2.2. Захват пакетов.

2.3. В консоли определил с помощью команды `ipconfig` IP-адрес и шлюз по умолчанию (default gateway) (рис. 2.3).

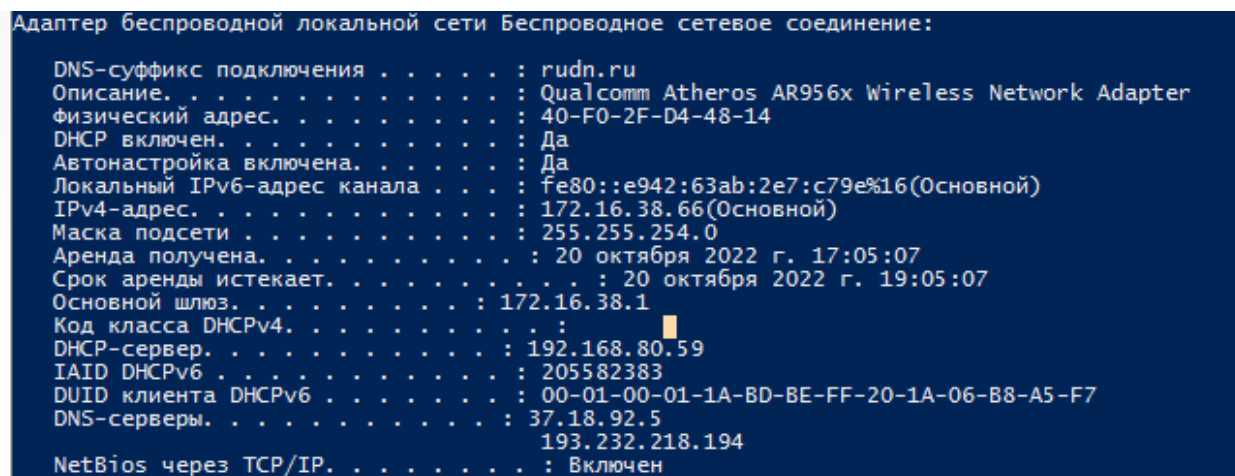


Рис. 2.3. IP-адрес и шлюз.

2.4. С помощью команды `ping` пропинговал шлюз по умолчанию. Изначально при помощи параметра `-n` команды `ping` задал число сообщений эхо-запроса – 5 (рис. 2.4).

```

PS C:\Users\User> ping 172.16.38.1 -n 5

Обмен пакетами с 172.16.38.1 по 32 байтами данных:
Ответ от 172.16.38.1: число байт=32 время=11мс TTL=254
Ответ от 172.16.38.1: число байт=32 время=9мс TTL=254
Ответ от 172.16.38.1: число байт=32 время=16мс TTL=254
Ответ от 172.16.38.1: число байт=32 время=19мс TTL=254
Ответ от 172.16.38.1: число байт=32 время=17мс TTL=254

Статистика Ping для 172.16.38.1:
    Пакетов: отправлено = 5, получено = 5, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 9мсек, Максимальное = 19 мсек, Среднее = 14 мсек
PS C:\Users\User>

```

Рис. 2.4. Пингование шлюза.

2.5. В Wireshark остановил захват трафика (рис. 2.5.1). В строке фильтра прописал фильтр `arp or icmp`. Убедился, что в списке пакетов отобразились только пакеты ARP или ICMP, в частности пакеты, которые были сгенерированы с помощью команды `ping`, отправленной с устройства на шлюз по умолчанию (рис. 2.5.2).

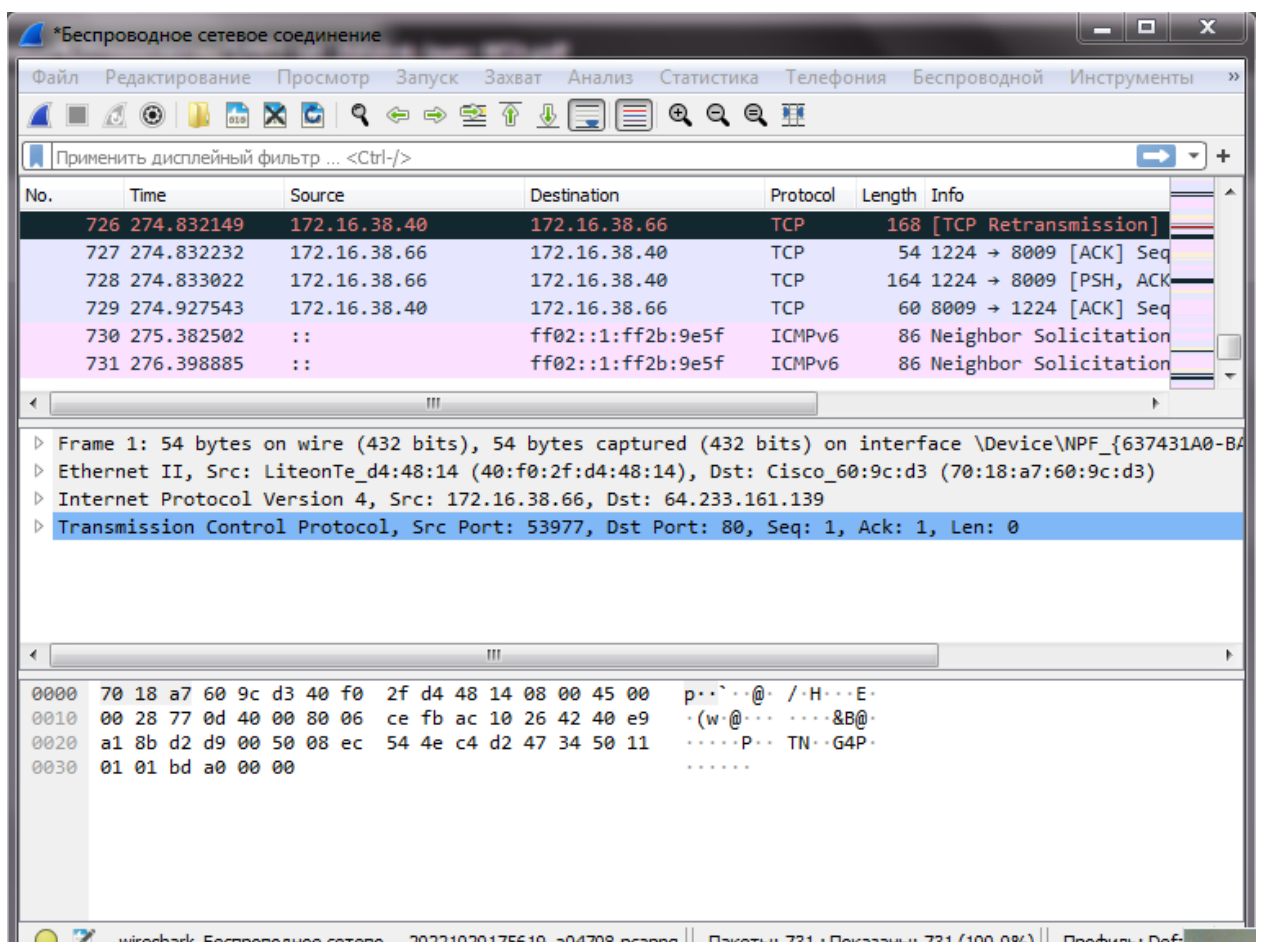


Рис. 2.5.1. Остановка захвата трафика.

*Беспроводное сетевое соединение

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты

arp or icmp

No.	Time	Source	Destination	Protocol	Length	Info
506	171.115642	HuiZhouG_fc:7b:9f	Broadcast	ARP	60	Who has 172.16.39.79?
507	171.120587	HuiZhouG_fc:7b:9f	Broadcast	ARP	60	Who has 172.16.39.88?
533	181.185852	HuiZhouG_fc:7b:9f	LiteonTe_d4:48:14	ARP	60	Who has 172.16.38.66?
534	181.185873	LiteonTe_d4:48:14	HuiZhouG_fc:7b:9f	ARP	42	172.16.38.66 is at 40
558	191.888067	LiteonTe_d4:48:14	Broadcast	ARP	42	Who has 172.16.38.1?
559	191.901483	Cisco_60:9c:d3	LiteonTe_d4:48:14	ARP	60	172.16.38.1 is at 70:
582	201.460746	LiteonTe_d4:48:14	HuiZhouG_fc:7b:9f	ARP	42	Who has 172.16.38.40?
585	201.486882	HuiZhouG_fc:7b:9f	LiteonTe_d4:48:14	ARP	60	172.16.38.40 is at 44
587	201.636143	172.16.38.66	172.16.38.1	ICMP	74	Echo (ping) request
590	206.461012	172.16.38.66	172.16.38.1	ICMP	74	Echo (ping) request
592	206.483343	172.16.38.1	172.16.38.66	ICMP	74	Echo (ping) reply
593	206.483343	172.16.38.1	172.16.38.66	ICMP	74	Echo (ping) reply
597	207.462026	172.16.38.66	172.16.38.1	ICMP	74	Echo (ping) request
598	207.481735	172.16.38.1	172.16.38.66	ICMP	74	Echo (ping) reply
600	208.463630	172.16.38.66	172.16.38.1	ICMP	74	Echo (ping) request
601	208.475650	172.16.38.1	172.16.38.66	ICMP	74	Echo (ping) reply
626	222.960597	LiteonTe_d4:48:14	HuiZhouG_fc:7b:9f	ARP	42	Who has 172.16.38.40?
627	223.959652	LiteonTe_d4:48:14	HuiZhouG_fc:7b:9f	ARP	42	Who has 172.16.38.40?
628	224.053898	HuiZhouG_fc:7b:9f	LiteonTe_d4:48:14	ARP	60	172.16.38.40 is at 44
629	226.117224	172.16.38.66	172.16.38.1	ICMP	74	Echo (ping) request
630	226.128763	172.16.38.1	172.16.38.66	ICMP	74	Echo (ping) reply
635	227.118788	172.16.38.66	172.16.38.1	ICMP	74	Echo (ping) request
636	227.128555	172.16.38.1	172.16.38.66	ICMP	74	Echo (ping) reply

Internet Control Message Protocol: Protocol || Пакеты: 731 · Показаны: 73 (10.0%) · Потеряно: 0 (0.0%) || Профиль: Defa

Рис. 2.5.2. Просмотр пакетов ARP и ICMP .

2.6. Изучил эхо-запрос и эхо-ответ ICMP в программе Wireshark (рис. 2.6.1 – 2.6.2).

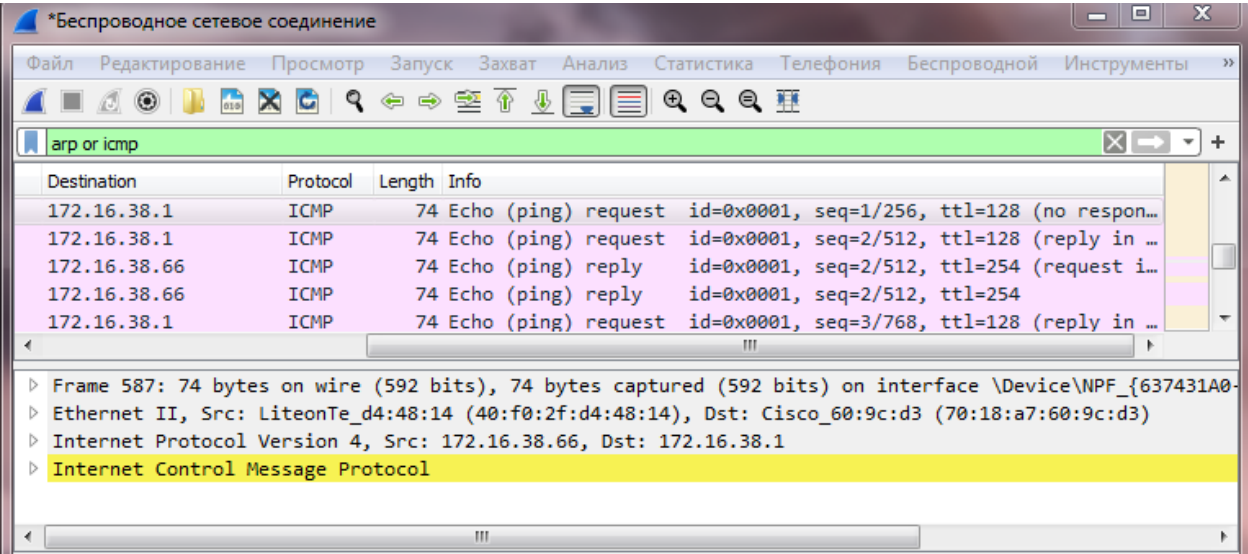


Рис. 2.6.1. Эхо-запрос ICMP

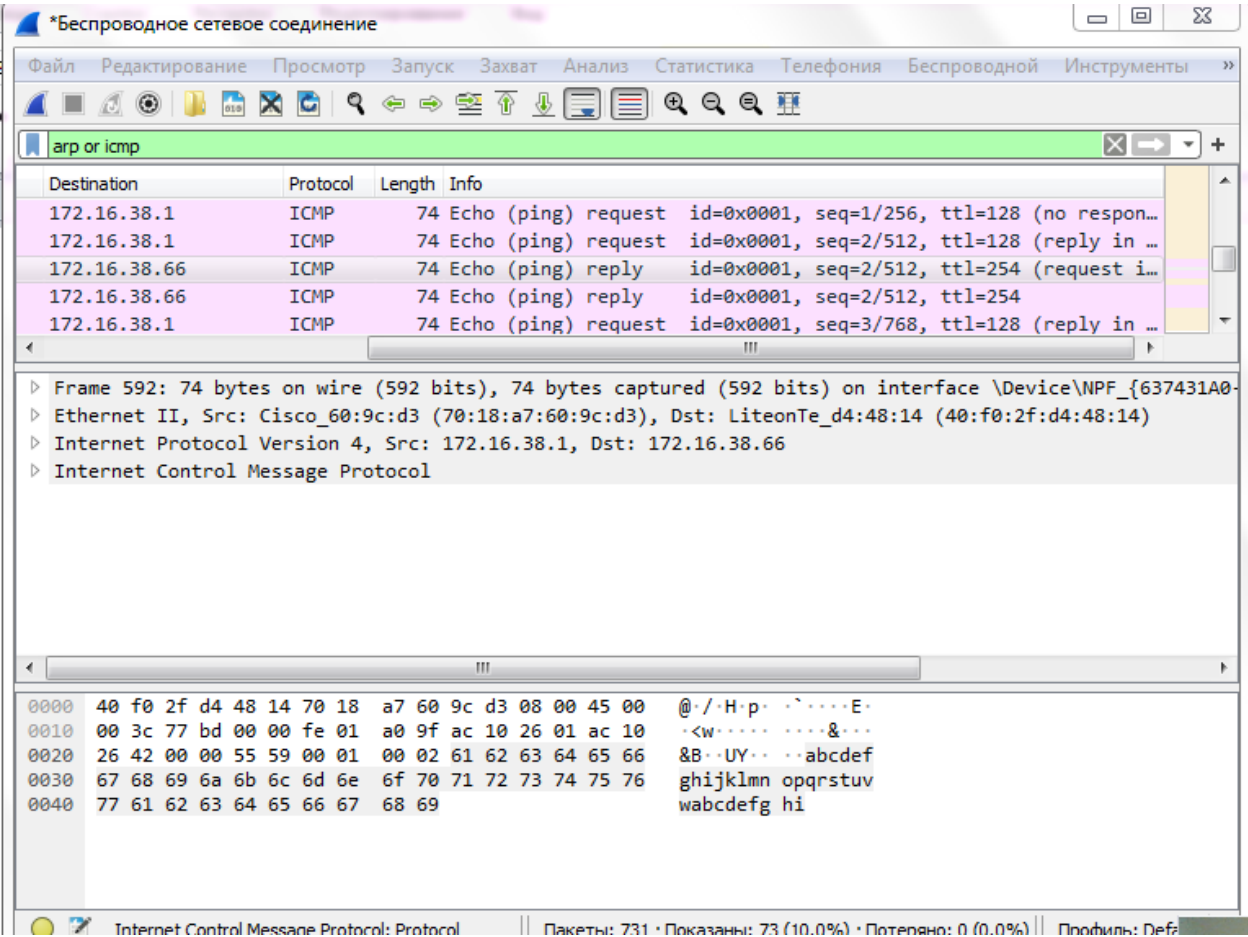


Рис. 2.6.2. Эхо-ответ ICMP

Таблица 1. Характеристики эхо-запроса и ответа ICMP

Характеристика	Значение
Длина кадра	74 байта (592 бита)
Тип Ethernet	Ethernet II
MAC-адрес источника	40:f0:2f:d4:48:14
MAC-адрес шлюза	70:18:a7:60:9c:d3
Тип MAC-адреса источника	Индивидуальный (Unicast), глобальный
Тип MAC-адреса шлюза	Индивидуальный (Unicast), глобальный

2.7. Изучил кадры данных протокола ARP. Изучил данные в полях заголовка Ethernet II.

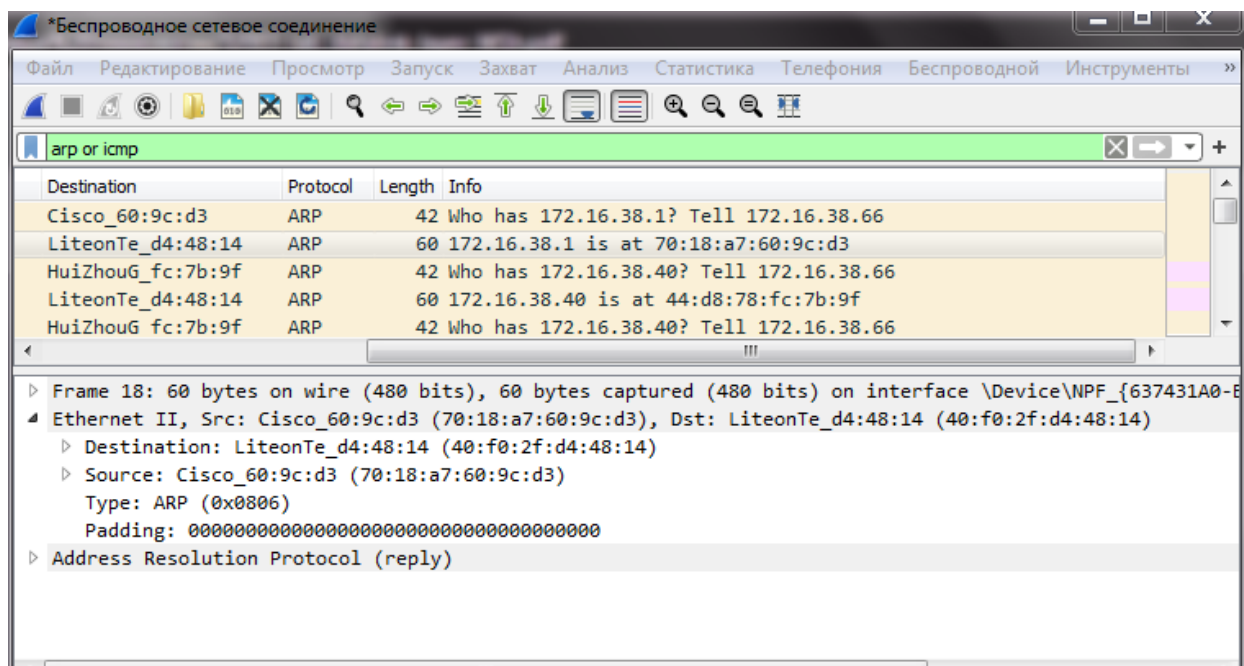


Рис. 2.7. Кадр данных протокола ARP

2.7. Начал новый процесс захвата трафика в Wireshark. В консоли пропинговал по имени адрес yandex.ru.

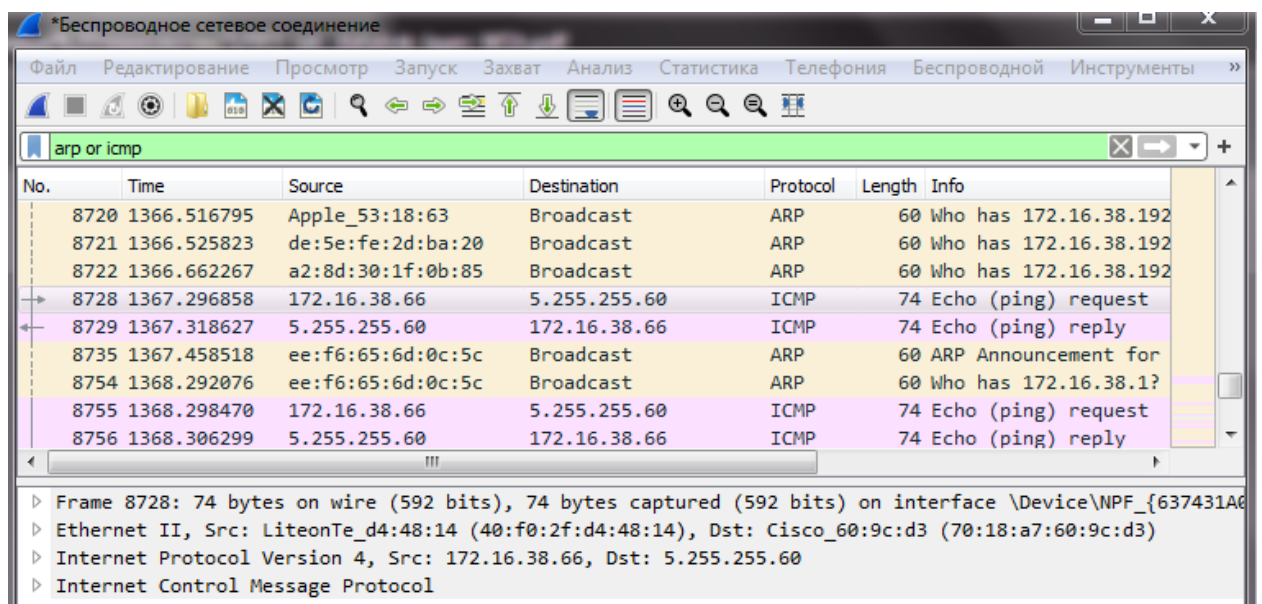
```
PS C:\Users\User> ping yandex.ru -n 5

Обмен пакетами с yandex.ru [5.255.255.60] с 32 байтами данных:
Ответ от 5.255.255.60: число байт=32 время=19мс TTL=248
Ответ от 5.255.255.60: число байт=32 время=21мс TTL=248
Ответ от 5.255.255.60: число байт=32 время=7мс TTL=248
Ответ от 5.255.255.60: число байт=32 время=6мс TTL=248
Ответ от 5.255.255.60: число байт=32 время=7мс TTL=248

Статистика Ping для 5.255.255.60:
    Пакетов: отправлено = 5, получено = 5, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 6мсек, Максимальное = 21 мсек, Среднее = 12 мсек
PS C:\Users\User>
```

Рис. 2.8. Пингование адреса yandex.ru по имени

2.9. В Wireshark остановил захват трафика. Изучил запросы и ответы протоколов ARP и ICMP.



No.	Time	Source	Destination	Protocol	Length	Info
8720	1366.516795	Apple_53:18:63	Broadcast	ARP	60	Who has 172.16.38.192
8721	1366.525823	de:5e:fe:2d:ba:20	Broadcast	ARP	60	Who has 172.16.38.192
8722	1366.662267	a2:8d:30:1f:0b:85	Broadcast	ARP	60	Who has 172.16.38.192
8728	1367.296858	172.16.38.66	5.255.255.60	ICMP	74	Echo (ping) request
8729	1367.318627	5.255.255.60	172.16.38.66	ICMP	74	Echo (ping) reply
8735	1367.458518	ee:f6:65:6d:0c:5c	Broadcast	ARP	60	ARP Announcement for
8754	1368.292076	ee:f6:65:6d:0c:5c	Broadcast	ARP	60	Who has 172.16.38.1?
8755	1368.298470	172.16.38.66	5.255.255.60	ICMP	74	Echo (ping) request
8756	1368.306299	5.255.255.60	172.16.38.66	ICMP	74	Echo (ping) reply

Frame 8728: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{637431A6...}

Ethernet II, Src: LiteonTe_d4:48:14 (40:f0:2f:d4:48:14), Dst: Cisco_60:9c:d3 (70:18:a7:60:9c:d3)

Internet Protocol Version 4, Src: 172.16.38.66, Dst: 5.255.255.60

Internet Control Message Protocol

Рис. 2.9.1. Эхо-запрос протокола ICMP

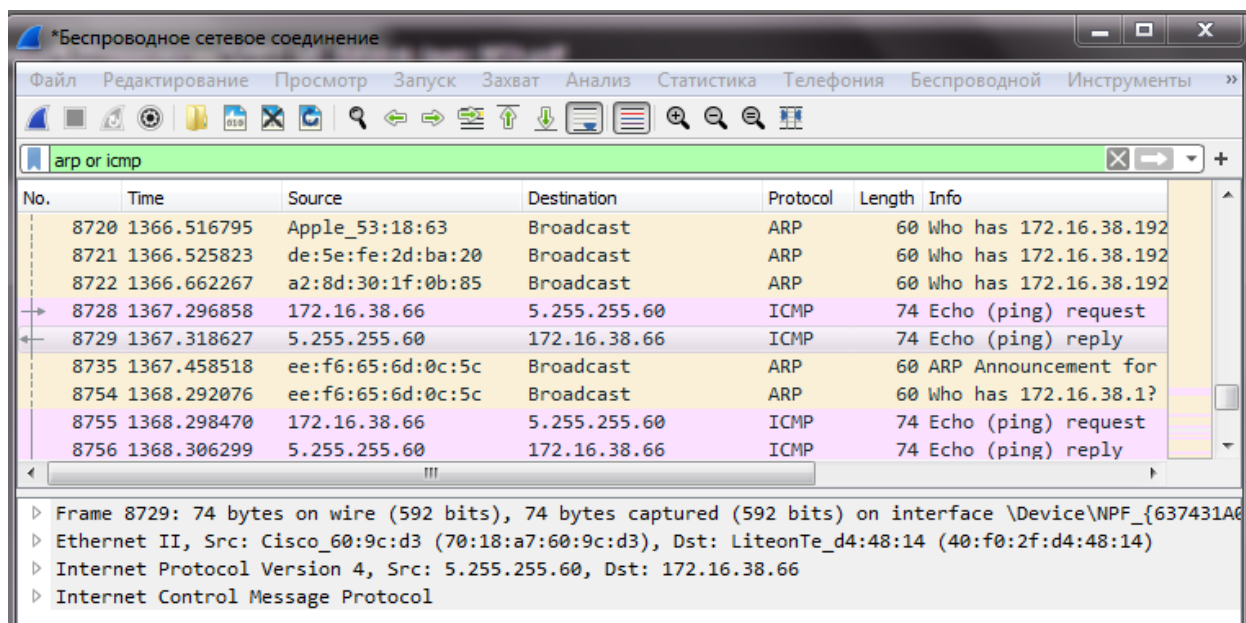


Рис. 2.9.2. Эхо-ответ протокола ICMP

Таблица 2. Характеристики эхо-запроса и ответа ICMP (yandex.ru).

Характеристика	Значение
Длина кадра	74 байта (592 бита)
Тип Ethernet	Ethernet II
MAC-адрес источника	40:f0:2f:d4:48:14
MAC-адрес шлюза	70:18:a7:60:9c:d3
Тип MAC-адреса источника	Индивидуальный (Unicast), глобальный
Тип MAC-адреса шлюза	Индивидуальный (Unicast), глобальный

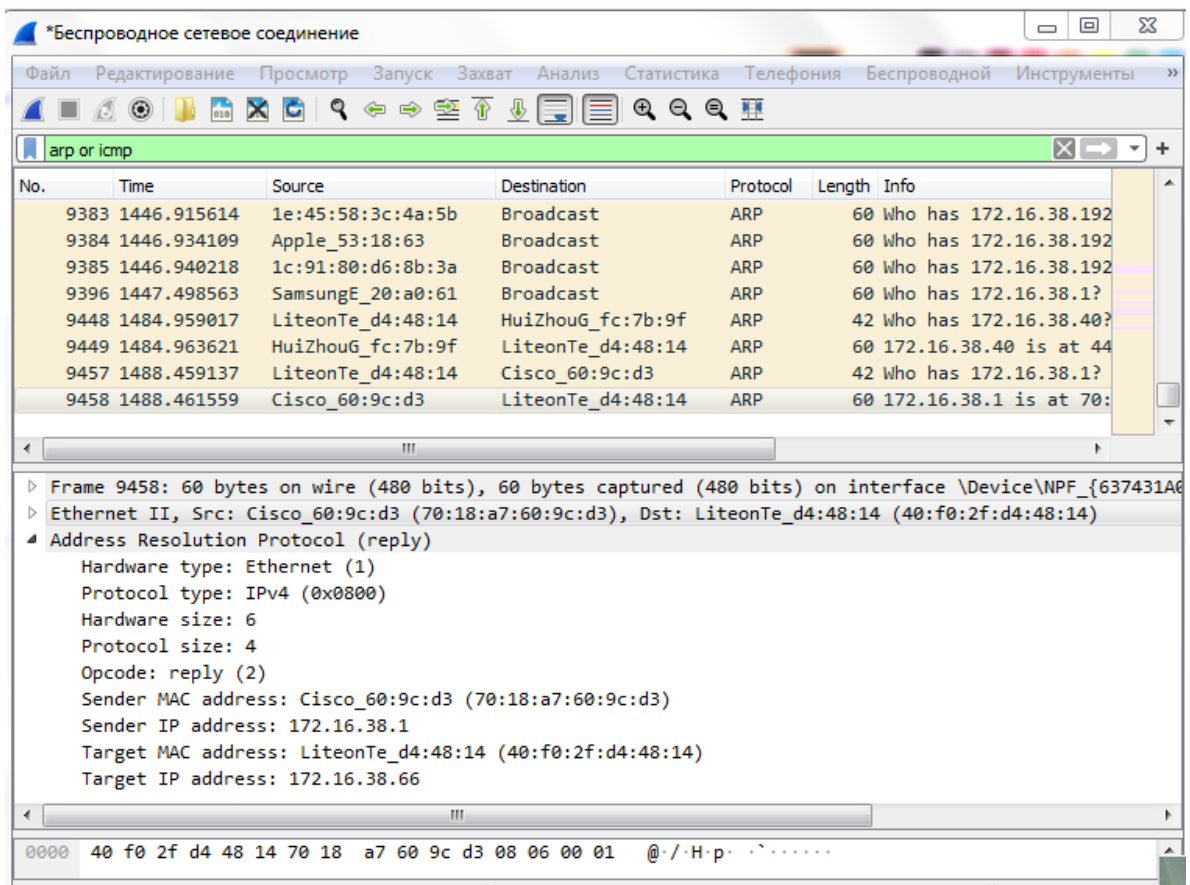


Рис. 2.9.3. Эхо-ответ протокола ARP

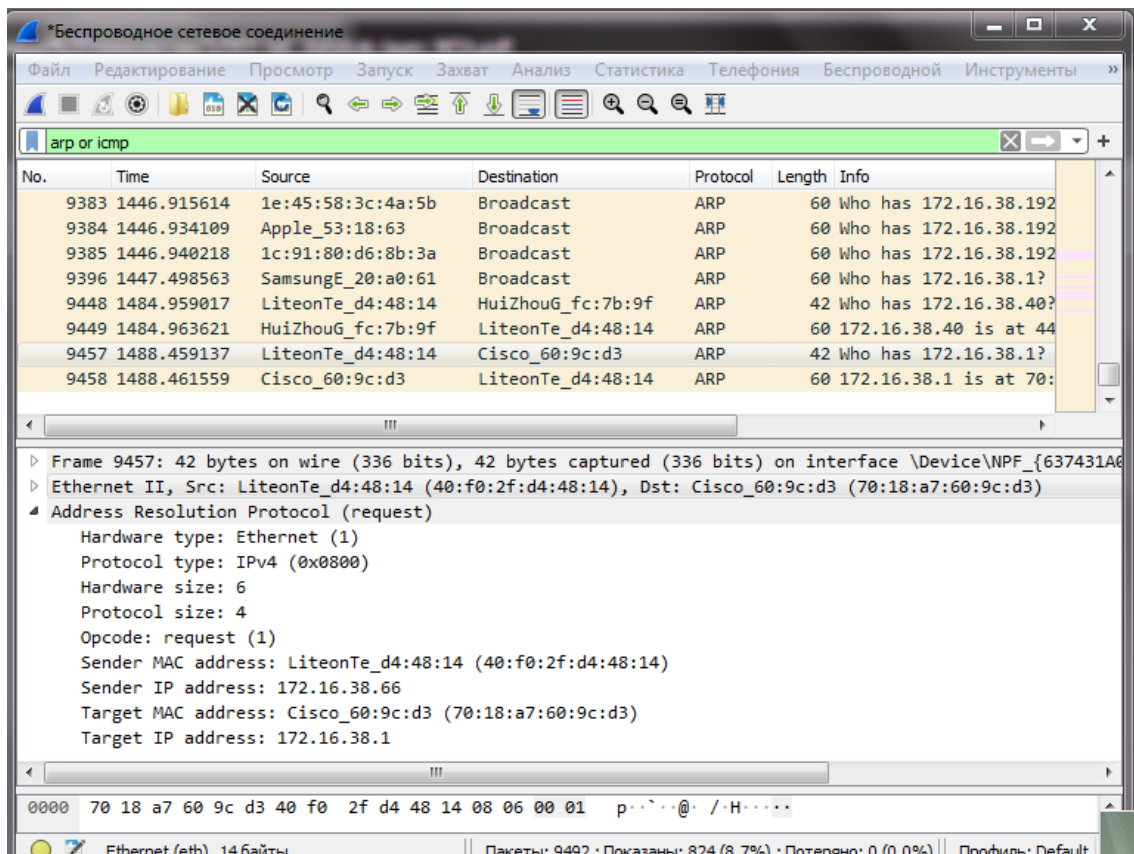


Рис. 2.9.4. Эхо-ответ протокола ARP

3. Анализ протоколов транспортного уровня в Wireshark

3.1. Запустил Wireshark. Выбрал активный сетевой интерфейс. Убедился, что начался процесс захвата трафика.

3.2. В браузере перешёл на сайт, работающий по протоколу HTTP (на сайт CERN <http://info.cern.ch/>).

3.3. В Wireshark в строке фильтра указал http и проанализировал информацию по протоколу TCP в случае запросов и ответов.

http						
No.	Time	Source	Destination	Protocol	Length	Info
167	48.904288	172.16.38.66	188.184.21.108	HTTP	501	GET / HTTP/1.1
171	48.963211	188.184.21.108	172.16.38.66	HTTP	932	HTTP/1.1 200 OK (text/html)
176	49.079490	172.16.38.66	188.184.21.108	HTTP	442	GET /favicon.ico HTTP/1.1
181	49.134858	188.184.21.108	172.16.38.66	HTTP	248	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

Рис. 3.1. Захваченные HTTP-пакеты

167	48.904288	172.16.38.66	188.184.21.108	HTTP	501	GET / HTTP/1.1
171	48.963211	188.184.21.108	172.16.38.66	HTTP	932	HTTP/1.1 200 OK (text/html)
176	49.079490	172.16.38.66	188.184.21.108	HTTP	442	GET /favicon.ico HTTP/1.1
181	49.134858	188.184.21.108	172.16.38.66	HTTP	248	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

▶ Frame 167: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface \Device\NPF_{637431A0-BA5B-492D-9D54-09C08D3B4286}, id 0

▶ Ethernet II, Src: LiteonTe_d4:48:14 (40:f0:2f:d4:48:14), Dst: Cisco_60:9c:d3 (70:18:a7:60:9c:d3)

▶ Internet Protocol Version 4, Src: 172.16.38.66, Dst: 188.184.21.108

▶ Transmission Control Protocol, Src Port: 54000, Dst Port: 80, Seq: 1, Ack: 1, Len: 447

Source Port: 54000

Destination Port: 80

[Stream index: 2]

[TCP Segment Len: 447]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 2580200004

[Next sequence number: 448 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 4082052324

0101 = Header Length: 20 bytes (5)

▶ Flags: 0x018 (PSH, ACK)

Window size value: 256

[Calculated window size: 65536]

[Window size scaling factor: 256]

Checksum: 0xdaf7 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

▶ [SEQ/ACK analysis]

▶ [Timestamps]

TCP payload (447 bytes)

▶ Hypertext Transfer Protocol

Рис. 3.2. Запрос по протоколу TCP

167	48.904288	172.16.38.66	188.184.21.108	HTTP	501 GET / HTTP/1.1
171	48.963211	188.184.21.108	172.16.38.66	HTTP	932 HTTP/1.1 200 OK (text/html)
176	49.079490	172.16.38.66	188.184.21.108	HTTP	442 GET /favicon.ico HTTP/1.1
181	49.134858	188.184.21.108	172.16.38.66	HTTP	248 HTTP/1.1 200 OK (image/vnd.microsoft.icon)

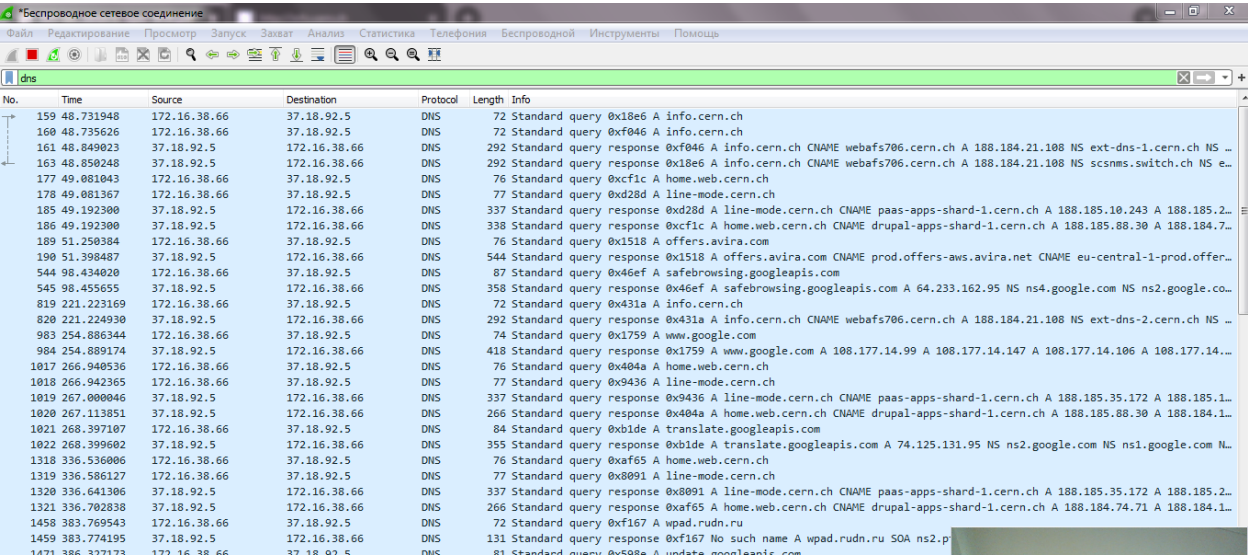
▶ Frame 171: 932 bytes on wire (7456 bits), 932 bytes captured (7456 bits) on interface \Device\NPF_{637431A0-BA5B-492D-9D54-09C08D3B4286}, id 0
 ▶ Ethernet II, Src: Cisco_60:9c:d3 (70:18:a7:60:9c:d3), Dst: LiteonTe_d4:48:14 (40:f0:2f:d4:48:14)
 ▶ Internet Protocol Version 4, Src: 188.184.21.108, Dst: 172.16.38.66
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 54000, Seq: 1, Ack: 448, Len: 878
 Source Port: 80
 Destination Port: 54000
 [Stream index: 2]
 [TCP Segment Len: 878]
 Sequence number: 1 (relative sequence number)
 Sequence number (raw): 4082052324
 [Next sequence number: 879 (relative sequence number)]
 Acknowledgment number: 448 (relative ack number)
 Acknowledgment number (raw): 2580200451
 0101 = Header Length: 20 bytes (5)
 ▶ Flags: 0x018 (PSH, ACK)
 Window size value: 237
 [Calculated window size: 30336]
 [Window size scaling factor: 128]
 Checksum: 0x4b9e [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0
 ▶ [SEQ/ACK analysis]
 ▶ [Timestamps]
 TCP payload (878 bytes)
 ▶ Hypertext Transfer Protocol
 ▶ Line-based text data: text/html (13 lines)

Рис. 3.3. Ответ по протоколу TCP

Таблица 3. Характеристики эхо-запроса и ответа TCP

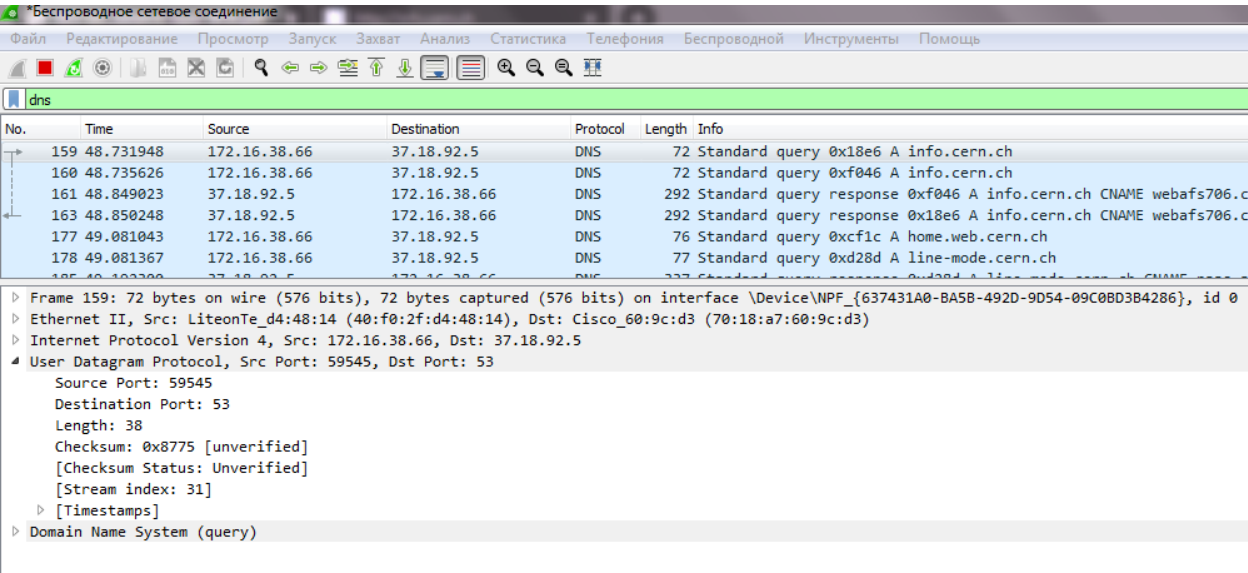
Характеристика	Значение
Длина сегмента TCP	447 байт (запрос), 878 байт (ответ)
Тип Ethernet	Ethernet II
Порт источника	54000
Порт получателя	80
Тип MAC-адреса источника	Индивидуальный (Unicast), глобальный
Тип MAC-адреса получателя	Индивидуальный (Unicast), глобальный

3.4. Wireshark в строке фильтра указал dns и проанализировал информацию по протоколу UDP в случае запросов и ответов.



No.	Time	Source	Destination	Protocol	Length	Info
159	48.731948	172.16.38.66	37.18.92.5	DNS	72	Standard query 0x18e6 A info.cern.ch
160	48.735626	172.16.38.66	37.18.92.5	DNS	72	Standard query 0xf046 A info.cern.ch
161	48.849023	37.18.92.5	172.16.38.66	DNS	292	Standard query response 0xf046 A info.cern.ch CNAME webafs706.cern.ch A 188.184.21.108 NS ext-dns-1.cern.ch NS ...
163	48.850248	37.18.92.5	172.16.38.66	DNS	292	Standard query response 0x18e6 A info.cern.ch CNAME webafs706.cern.ch A 188.184.21.108 NS scsmms.switch.ch NS e...
177	49.081043	172.16.38.66	37.18.92.5	DNS	76	Standard query 0xcfc1c A home.web.cern.ch
178	49.081367	172.16.38.66	37.18.92.5	DNS	77	Standard query 0xd28d A line-mode.cern.ch
185	49.192300	37.18.92.5	172.16.38.66	DNS	337	Standard query response 0xd28d A line-mode.cern.ch CNAME paas-apps-shard-1.cern.ch A 188.185.10.243 A 188.185.2...
186	49.192300	37.18.92.5	172.16.38.66	DNS	338	Standard query response 0xcfc1c A home.web.cern.ch CNAME drupal-apps-shard-1.cern.ch A 188.185.88.30 A 188.184.7...
189	51.250384	172.16.38.66	37.18.92.5	DNS	76	Standard query 0x1518 A offers.avira.com
190	51.398487	37.18.92.5	172.16.38.66	DNS	544	Standard query response 0x1518 A offers.avira.com CNAME prod.offers-aws.avira.net CNAME eu-central-1-prod.offer...
544	98.434020	172.16.38.66	37.18.92.5	DNS	87	Standard query 0x46ef A safebrowsing.googleapis.com
545	98.455655	37.18.92.5	172.16.38.66	DNS	358	Standard query response 0x46ef A safebrowsing.googleapis.com A 64.233.162.95 NS ns4.google.com NS ns2.google.co...
819	221.223169	172.16.38.66	37.18.92.5	DNS	72	Standard query 0x431a A info.cern.ch
820	221.224930	37.18.92.5	172.16.38.66	DNS	292	Standard query response 0x431a A info.cern.ch CNAME webafs706.cern.ch A 188.184.21.108 NS ext-dns-2.cern.ch NS ...
983	254.886344	172.16.38.66	37.18.92.5	DNS	74	Standard query 0x1759 A www.google.com
984	254.889174	37.18.92.5	172.16.38.66	DNS	418	Standard query response 0x1759 A www.google.com A 108.177.14.99 A 108.177.14.147 A 108.177.14.106 A 108.177.14...
1017	266.940536	172.16.38.66	37.18.92.5	DNS	76	Standard query 0xa46a A home.web.cern.ch
1018	266.942365	172.16.38.66	37.18.92.5	DNS	77	Standard query 0x9436 A line-mode.cern.ch
1019	267.000046	37.18.92.5	172.16.38.66	DNS	337	Standard query response 0x9436 A line-mode.cern.ch CNAME paas-apps-shard-1.cern.ch A 188.185.35.172 A 188.185.1...
1020	267.113851	37.18.92.5	172.16.38.66	DNS	266	Standard query response 0xa46a A home.web.cern.ch CNAME drupal-apps-shard-1.cern.ch A 188.185.88.30 A 188.184.1...
1021	268.397107	172.16.38.66	37.18.92.5	DNS	84	Standard query 0xb1de A translate.googleapis.com
1022	268.399602	37.18.92.5	172.16.38.66	DNS	355	Standard query response 0xb1de A translate.googleapis.com A 74.125.131.95 NS ns2.google.com NS ns1.google.com N...
1318	336.536006	172.16.38.66	37.18.92.5	DNS	76	Standard query 0xaf65 A home.web.cern.ch
1319	336.586127	172.16.38.66	37.18.92.5	DNS	77	Standard query 0x8091 A line-mode.cern.ch
1320	336.641306	37.18.92.5	172.16.38.66	DNS	337	Standard query response 0x8091 A line-mode.cern.ch CNAME paas-apps-shard-1.cern.ch A 188.185.35.172 A 188.185.2...
1321	336.702838	37.18.92.5	172.16.38.66	DNS	266	Standard query response 0xaf65 A home.web.cern.ch CNAME drupal-apps-shard-1.cern.ch A 188.184.74.71 A 188.184.1...
1458	383.769543	172.16.38.66	37.18.92.5	DNS	72	Standard query 0xf167 A wpad.rudn.ru
1459	383.774195	37.18.92.5	172.16.38.66	DNS	131	Standard query response 0xf167 No such name A wpad.rudn.ru SOA ns2.p...
1471	386.377173	172.16.38.66	37.18.92.5	DNS	81	Standard query 0x508a A update.googleapis.com

Рис. 3.4. Захваченные пакеты протокола dns



No.	Time	Source	Destination	Protocol	Length	Info
159	48.731948	172.16.38.66	37.18.92.5	DNS	72	Standard query 0x18e6 A info.cern.ch
160	48.735626	172.16.38.66	37.18.92.5	DNS	72	Standard query 0xf046 A info.cern.ch
161	48.849023	37.18.92.5	172.16.38.66	DNS	292	Standard query response 0xf046 A info.cern.ch CNAME webafs706.c
163	48.850248	37.18.92.5	172.16.38.66	DNS	292	Standard query response 0x18e6 A info.cern.ch CNAME webafs706.c
177	49.081043	172.16.38.66	37.18.92.5	DNS	76	Standard query 0xcfc1c A home.web.cern.ch
178	49.081367	172.16.38.66	37.18.92.5	DNS	77	Standard query 0xd28d A line-mode.cern.ch
185	49.192300	37.18.92.5	172.16.38.66	DNS	337	Standard query response 0xd28d A line-mode.cern.ch CNAME paas...

Frame 159: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{637431A0-BA5B-492D-9D54-09C08D3B4286}, id 0

Ethernet II, Src: LiteonTe_d4:48:14 (40:f0:2f:d4:48:14), Dst: Cisco_60:9c:d3 (70:18:a7:60:9c:d3)

Internet Protocol Version 4, Src: 172.16.38.66, Dst: 37.18.92.5

User Datagram Protocol, Src Port: 59545, Dst Port: 53

Source Port: 59545
Destination Port: 53
Length: 38
Checksum: 0x8775 [unverified]
[Checksum Status: Unverified]
[Stream index: 31]
[Timestamps]

Domain Name System (query)

Рис. 3.5. Информация по протоколу UDP (запрос)

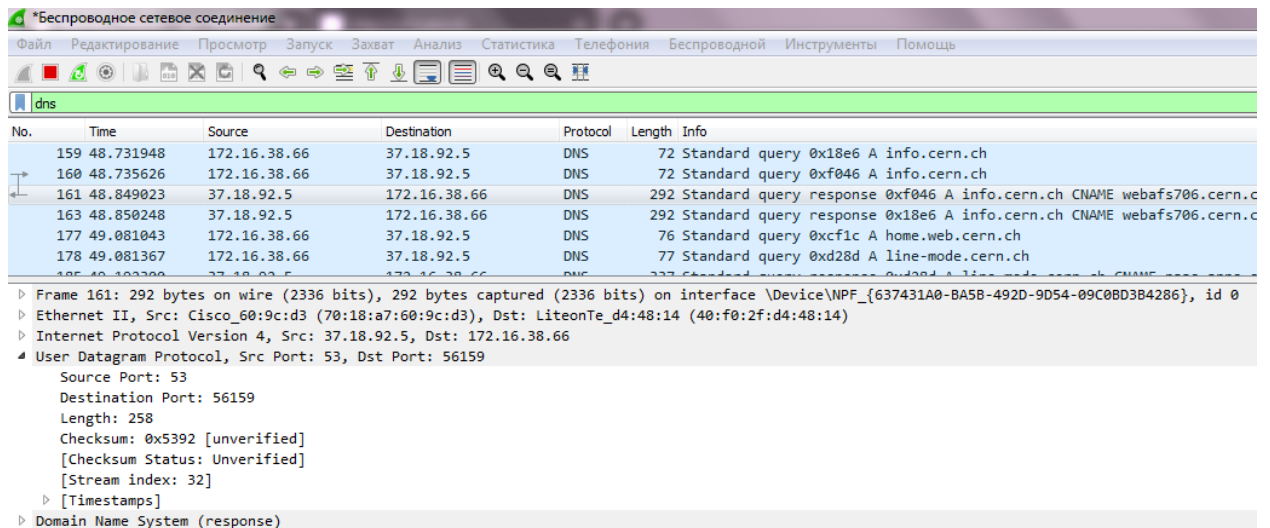


Рис. 3.6. Информация по протоколу UDP (ответ)

Таблица 4. Характеристики эхо-запроса и ответа по протоколу UDP

Характеристика	Значение
Длина сегмента UDP	38 байт (запрос), 258 байт (ответ)
Тип Ethernet	Ethernet II
Порт источника	56159
Порт получателя	53
Тип MAC-адреса источника	Индивидуальный (Unicast), глобальный
Тип MAC-адреса получателя	Индивидуальный (Unicast), глобальный

3.5. Wireshark в строке фильтра указал quic и проанализировал информацию по протоколу quic в случае запросов и ответов. Не обнаружилось никаких пакетов по протоколу quic.

3.6. Остановил захват трафика в Wireshark.

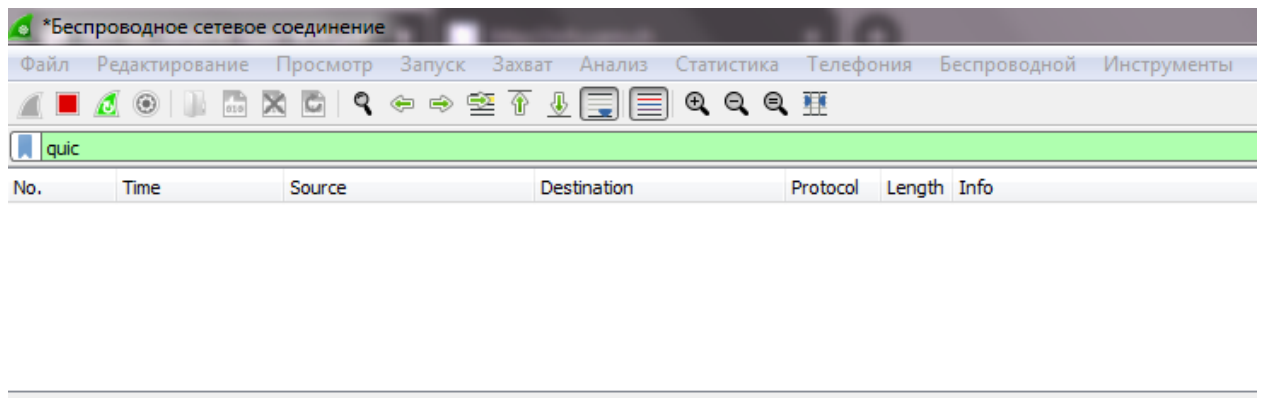


Рис. 3.7. Захваченные пакеты протокола quic

4. Анализ handshake протокола TCP в Wireshark

4.1. С помощью Wireshark проанализировал handshake протокола TCP.

4.2. Запустил Wireshark. Выбрал активный сетевой интерфейс. Убедился, что начался процесс захвата трафика.

4.3. Использовал соединение по HTTP с сайтом info.cern.ch для захвата в Wireshark пакетов TCP.

4.4. В Wireshark проанализировал handshake протокола TCP: трёхступенчатая система handshake –

- клиент посылает сообщение [SYN, ISSa],
- сервер откликается, посылая сообщение [SYN, ACK, ISSb, ACK(ISSa+1)],
- клиент отправляет подтверждение получения SYN-сегмента от сервера, сообщение [ACK]

No.	Time	Source	Destination	Protocol	Length	Info
29516	1423.158424	172.16.38.66	188.184.21.108	TCP	66	54257 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
29517	1423.158579	172.16.38.66	188.184.21.108	TCP	66	54258 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
29518	1423.213375	188.184.21.108	172.16.38.66	TCP	66	80 → 54257 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
29519	1423.213375	188.184.21.108	172.16.38.66	TCP	66	80 → 54258 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
29520	1423.213429	172.16.38.66	188.184.21.108	TCP	54	54257 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
29521	1423.213471	172.16.38.66	188.184.21.108	TCP	54	54258 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0

Рис. 3.8. Handshake

```

Transmission Control Protocol, Src Port: 54257, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 54257
  Destination Port: 80
  [Stream index: 246]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Sequence number (raw): 335202583
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x002 (SYN)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....0... = Congestion Window Reduced (CWR): Not set
    ....0... = ECN-Echo: Not set
    ....0... = Urgent: Not set
    ....0... = Acknowledgment: Not set
    ....0... = Push: Not set
    ....0... = Reset: Not set
    > ....0...1. = Syn: Set
    ....0...0 = Fin: Not set
  [TCP Flags: .....S.]
  Window size value: 8192
  [Calculated window size: 8192]
  Checksum: 0xf945 [unverified]
  [Checksum Status: Unverified]

```

Рис. 3.9. [SYN] от клиента


```

Transmission Control Protocol, Src Port: 80, Dst Port: 54257, Seq: 0, Ack: 1, Len: 0
Source Port: 80
Destination Port: 54257
[Stream index: 246]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Sequence number (raw): 2519529415
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 335202584
1000 .... = Header Length: 32 bytes (8)
Flags: 0x012 (SYN, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... 0... = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
... ..1. = Syn: Set
.... .... ...0 = Fin: Not set
[TCP Flags: .....A..S.]
Window size value: 29200
[Calculated window size: 29200]
Checksum: 0x1931 [unverified]
[Checksum Status: Unverified]

```

Рис. 4.1. [SYN, ACK] от сервера

```

Transmission Control Protocol, Src Port: 54257, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
Source Port: 54257
Destination Port: 80
[Stream index: 246]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 335202584
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 2519529416
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... 0... = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
.... .... 0... = Push: Not set
.... .... .0.. = Reset: Not set
.... .... ..0. = Syn: Not set
.... .... ...0 = Fin: Not set
[TCP Flags: .....A....]
Window size value: 256
[Calculated window size: 65536]
[Window size scaling factor: 256]
Checksum: 0xcb13 [unverified]

```

Рис. 4.2. [ACK] от клиента

4.6. Остановил захват трафика в Wireshark.



В результате выполнения лабораторной работы я изучил посредством Wireshark кадры Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.