

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра теории вероятностей и кибербезопасности

ОТЧЁТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №3

дисциплина: Сетевые технологии

Студент: Бансимба Клодели Дьегра

Студ. билет № 1032215651

Группа: НПИбд-02-22

МОСКВА

2024 г.

Цель работы:

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

Выполнение работы:

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

```
PS C:\Users\bansi> ipconfig

Настройка протокола IP для Windows

Неизвестный адаптер Подключение по локальной сети:

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

Адаптер Ethernet Ethernet:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::6913:a1e4:1fca:fd04%5
    IPv4-адрес. . . . . : 192.168.56.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . :

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* 1
0:

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

Адаптер беспроводной локальной сети Беспроводная сеть:

    DNS-суффикс подключения . . . . . : rudn.ru
    Локальный IPv6-адрес канала . . . : fe80::cde2:1581:c9f:ee8c%8
    IPv4-адрес. . . . . : 192.168.169.37
    Маска подсети . . . . . : 255.255.224.0
    Основной шлюз. . . . . : 192.168.160.1

Адаптер Ethernet Сетевое подключение Bluetooth:

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

Рис. 1.1. Вывод информации о текущем сетевом соединении.

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

```
Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
PS C:\Users\bansi>
PS C:\Users\bansi> ipconfig /all

Настройка протокола IP для Windows

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

Неизвестный адаптер Подключение по локальной сети:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : TAP-Windows Adapter V9
Физический адрес. . . . . : 00-FF-E5-B7-8A-10
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да

Адаптер Ethernet Ethernet:

DNS-суффикс подключения . . . . . :
Описание. . . . . : VirtualBox Host-Only Ethernet
Adapter
Физический адрес. . . . . : 0A-00-27-00-00-05
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::6913:a1e4:1fca:fd04%5(О
сновной)
IPv4-адрес. . . . . : 192.168.56.1(Основной)
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . :
IAID DHCPv6 . . . . . : 587857959
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2E-10-16-36-D4-E9
-8A-EA-63-AC
NetBios через TCP/IP. . . . . : Включен

Адаптер беспроводной локальной сети Подключение по локальной сети* 1
:

Состояние среды. . . . . : Среда передачи недоступна.
```

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

```
PS C:\Users\bansi> ipconfig /displaydns
Настройка протокола IP для Windows

edgedl.me.gvt1.com
-----
Имя записи. . . . . : edgedl.me.gvt1.com
Тип записи. . . . . : 1
Срок жизни. . . . . : 265
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 34.104.35.123

1.240.30.172.in-addr.arpa
-----
Имя записи. . . . . : 1.240.30.172.in-addr.arpa.
Тип записи. . . . . : 12
Срок жизни. . . . . : 518878
Длина данных. . . . . : 8
Раздел. . . . . : Ответ
PTR-запись. . . . . : DESKTOP-PATH1A1.mshome.net

desktop-path1a1.mshome.net
-----
Нет записей типа AAAA

desktop-path1a1.mshome.net
-----
Имя записи. . . . . : DESKTOP-PATH1A1.mshome.net
Тип записи. . . . . : 1
Срок жизни. . . . . : 518878
Длина данных. . . . . : 4
Раздел. . . . . : Ответ
А-запись (узла) . . . : 172.30.240.1
```

Рис. 1.3. Отображение содержимого кэша сопоставителя DNS-клиента, включающее как записи, предварительно загруженные из локального файла

Hosts, так и все недавно полученные записи ресурсов для запросов имен, разрешенных компьютером.

```
PS C:\Users\bansi>
PS C:\Users\bansi> ipconfig /registerdns
Запрошенная операция требует повышения.
PS C:\Users\bansi> |
```

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

```
PS C:\Users\bansi> ipconfig /setclassid

Ошибка: неопознанная или неполная командная строка.

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

где
    adapter          Имя подключения
                     (допускаются подстановочные знаки * и ?, см. примеры)

Параметры:
    /?              Вывод справки по использованию
    /all            Отображение полных сведений о конфигурации.
    /release        Освобождение IPv4-адреса для указанного адаптера.
    /release6       Освобождение IPv6-адреса для указанного адаптера.
    /renew          Освобождение IPv4-адреса для указанного адаптера.
    /renew6         Освобождение IPv6-адреса для указанного адаптера.
    /flushdns       Очищает кэш сопоставителя DNS.
    /registerdns    Обновляет все аренды DHCP и повторно регистрирует DNS-име
на
    /displaydns     Отображение содержимого кэша сопоставителя DNS.
    /showclassid    Отображает все ID класса DHCP, разрешенные для адаптеров.
    /setclassid     Изменяет ID класса DHCP.
    /showclassid6   Отображает все ID класса DHCP IPv6, разрешенные для адапт
еров.
```

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

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

```
PS C:\Users\bansi>
PS C:\Users\bansi> GETMAC

Физический адрес      Имя транспорта
=====
D4-E9-8A-EA-63-AC     \Device\Tcpip_{8201EEE5-6DFF-4AA9-BD93-71A71EC9D629}
D4-E9-8A-EA-63-B0     Носитель отключен
00-FF-E5-B7-8A-10     Носитель отключен
0A-00-27-00-00-05     \Device\Tcpip_{39319D58-5605-4BCB-A9C3-82EACB6CAE52}
PS C:\Users\bansi> |
```

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

Установим на нашем устройстве Wireshark (Рис. 2.1).

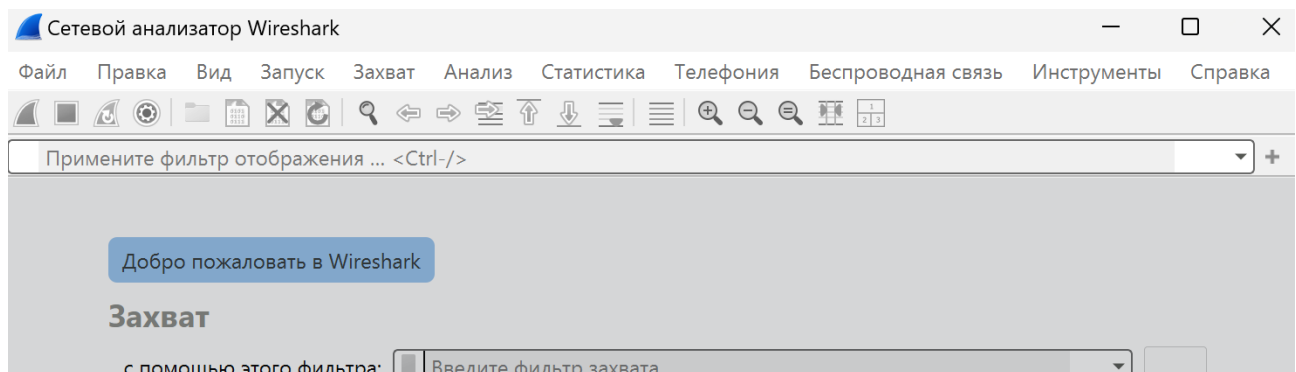


Рис. 2.1. Установка на нашем устройстве Wireshark.

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.169.37	108.177.14.188	TCP	55	53448 → 5228 [ACK] Seq=
2	0.000521	192.168.169.37	108.177.14.188	TCP	55	53447 → 5228 [ACK] Seq=
3	0.017888	108.177.14.188	192.168.169.37	TCP	66	5228 → 53448 [ACK] Seq=
4	0.018426	108.177.14.188	192.168.169.37	TCP	66	5228 → 53447 [ACK] Seq=
5	1.636233	192.168.169.37	77.88.55.88	TCP	55	53880 → 443 [ACK] Seq=1
6	1.647610	77.88.55.88	192.168.169.37	TCP	66	443 → 53880 [ACK] Seq=1

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

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

```
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . : rudn.ru
Локальный IPv6-адрес канала . . . : fe80::cde2:1581:c9f:eeefc%8
IPv4-адрес. . . . . : 192.168.169.37
Маска подсети . . . . . : 255.255.224.0
Основной шлюз. . . . . : 192.168.160.1
```

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

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

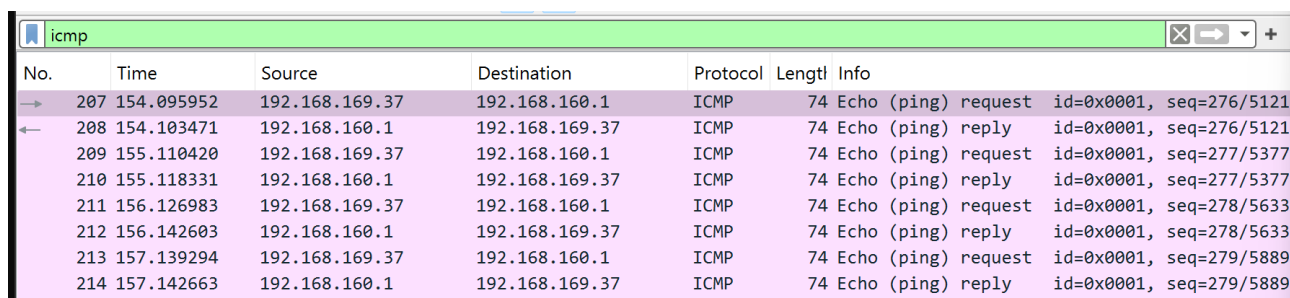
```
PS C:\Users\bansi> ping 192.168.160.1

Обмен пакетами с 192.168.160.1 по с 32 байтами данных:
Ответ от 192.168.160.1: число байт=32 время=7мс TTL=254
Ответ от 192.168.160.1: число байт=32 время=8мс TTL=254
Ответ от 192.168.160.1: число байт=32 время=15мс TTL=254
Ответ от 192.168.160.1: число байт=32 время=3мс TTL=254

Статистика Ping для 192.168.160.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 15 мсек, Среднее = 8 мсек
PS C:\Users\bansi>
```

Рис. 2.4. Пинг шлюза по умолчанию.

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



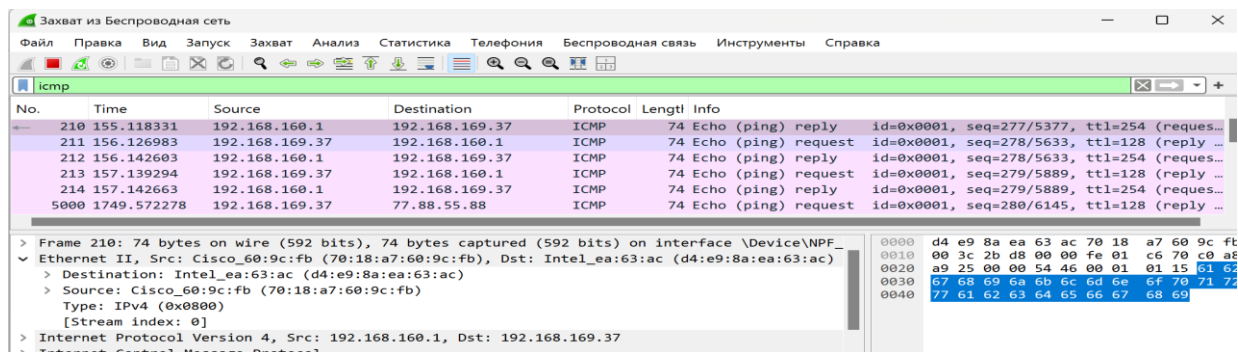
No.	Time	Source	Destination	Protocol	Length	Info
207	154.095952	192.168.169.37	192.168.160.1	ICMP	74	Echo (ping) request id=0x0001, seq=276/5121
208	154.103471	192.168.160.1	192.168.169.37	ICMP	74	Echo (ping) reply id=0x0001, seq=276/5121
209	155.110420	192.168.169.37	192.168.160.1	ICMP	74	Echo (ping) request id=0x0001, seq=277/5377
210	155.118331	192.168.160.1	192.168.169.37	ICMP	74	Echo (ping) reply id=0x0001, seq=277/5377
211	156.126983	192.168.169.37	192.168.160.1	ICMP	74	Echo (ping) request id=0x0001, seq=278/5633
212	156.142603	192.168.160.1	192.168.169.37	ICMP	74	Echo (ping) reply id=0x0001, seq=278/5633
213	157.139294	192.168.169.37	192.168.160.1	ICMP	74	Echo (ping) request id=0x0001, seq=279/5889
214	157.142663	192.168.160.1	192.168.169.37	ICMP	74	Echo (ping) reply id=0x0001, seq=279/5889

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

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

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

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



No.	Time	Source	Destination	Protocol	Length	Info
210	155.118331	192.168.160.1	192.168.169.37	ICMP	74	Echo (ping) reply id=0x0001, seq=277/5377, ttl=254 (request...)
211	156.126983	192.168.169.37	192.168.160.1	ICMP	74	Echo (ping) request id=0x0001, seq=278/5633, ttl=128 (reply ...)
212	156.142603	192.168.160.1	192.168.169.37	ICMP	74	Echo (ping) reply id=0x0001, seq=278/5633, ttl=254 (request...)
213	157.139294	192.168.169.37	192.168.160.1	ICMP	74	Echo (ping) request id=0x0001, seq=279/5889, ttl=128 (reply ...)
214	157.142663	192.168.160.1	192.168.169.37	ICMP	74	Echo (ping) reply id=0x0001, seq=279/5889, ttl=254 (request...)
5000	1749.572278	192.168.169.37	77.88.55.88	ICMP	74	Echo (ping) request id=0x0001, seq=280/6145, ttl=128 (reply ...)

Frame 210: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{...}	
Ethernet II, Src: Cisco_60:9c:fb (70:18:a7:60:9c:fb), Dst: Intel_ea:63:ac (d4:e9:8a:ea:63:ac)	0000 d4 e9 8a ea 63 ac 70 18 a7 60 9c fb
Destination: Intel_ea:63:ac (d4:e9:8a:ea:63:ac)	0010 00 3c 2b d8 00 00 fe 01 c6 70 c0 a8
Source: Cisco_60:9c:fb (70:18:a7:60:9c:fb)	0020 a9 25 00 00 54 46 00 01 01 15 61 62
Type: IPv4 (0x0800)	0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72
[Stream index: 0]	0040 77 61 62 63 64 65 66 67 68 69
Internet Protocol Version 4, Src: 192.168.160.1, Dst: 192.168.169.37	
Internet Control Message Protocol	

Рис. 2.6. Кадр ICMP — эхо-запрос.

Захват из Беспроводная сеть

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

icmp

No.	Time	Source	Destination	Protocol	Length	Info
210	155.118331	192.168.160.1	192.168.169.37	ICMP	74	Echo (ping) reply
211	156.126983	192.168.169.37	192.168.160.1	ICMP	74	Echo (ping) request
212	156.142603	192.168.160.1	192.168.169.37	ICMP	74	Echo (ping) reply
213	157.139294	192.168.169.37	192.168.160.1	ICMP	74	Echo (ping) request
214	157.142663	192.168.160.1	192.168.169.37	ICMP	74	Echo (ping) reply
5000	1749.572278	192.168.169.37	77.88.55.88	ICMP	74	Echo (ping) request

> Frame 211: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_...

▼ Ethernet II, Src: Intel_ea:63:ac (d4:e9:8a:ea:63:ac), Dst: Cisco_60:9c:fb (70:18:a7:60:9c:fb)

> Destination: Cisco_60:9c:fb (70:18:a7:60:9c:fb)

> Source: Intel_ea:63:ac (d4:e9:8a:ea:63:ac)

Type: IPv4 (0x0800)

[Stream index: 0]

> Internet Protocol Version 4. Src: 192.168.169.37. Dst: 192.168.160.1

Рис. 2.7. Кадр ICMP — эхо-ответ.

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

Захват из Беспроводная сеть

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

arp

No.	Time	Source	Destination	Protocol	Length	Info
8	6.618345	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.1
139	78.063246	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.1
446	284.555473	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.1
680	511.424894	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.1
721	579.413612	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.1
1947	619.836414	Cisco_63:d8:60	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.1

> Frame 139: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_...

▼ Ethernet II, Src: Cisco_63:d8:60 (7c:0e:ce:63:d8:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)

.... 1. = LG bit: Locally administered address (this is NOT the factory default)

.... 1. = IG bit: Group address (multicast/broadcast)

▼ Source: Cisco_63:d8:60 (7c:0e:ce:63:d8:60)

.... 0. = LG bit: Globally unique address (factory default)

.... 0. = IG bit: Individual address (unicast)

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

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

```
PS C:\Users\bansi> ping www.yandex.ru

Обмен пакетами с www.yandex.ru [77.88.55.88] с 32 байтами данных:
Ответ от 77.88.55.88: число байт=32 время=8мс TTL=54
Ответ от 77.88.55.88: число байт=32 время=10мс TTL=54
Ответ от 77.88.55.88: число байт=32 время=11мс TTL=54
Ответ от 77.88.55.88: число байт=32 время=29мс TTL=54

Статистика Ping для 77.88.55.88:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 8мсек, Максимальное = 29 мсек, Среднее = 14 мсек
PS C:\Users\bansi>
```

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

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

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

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

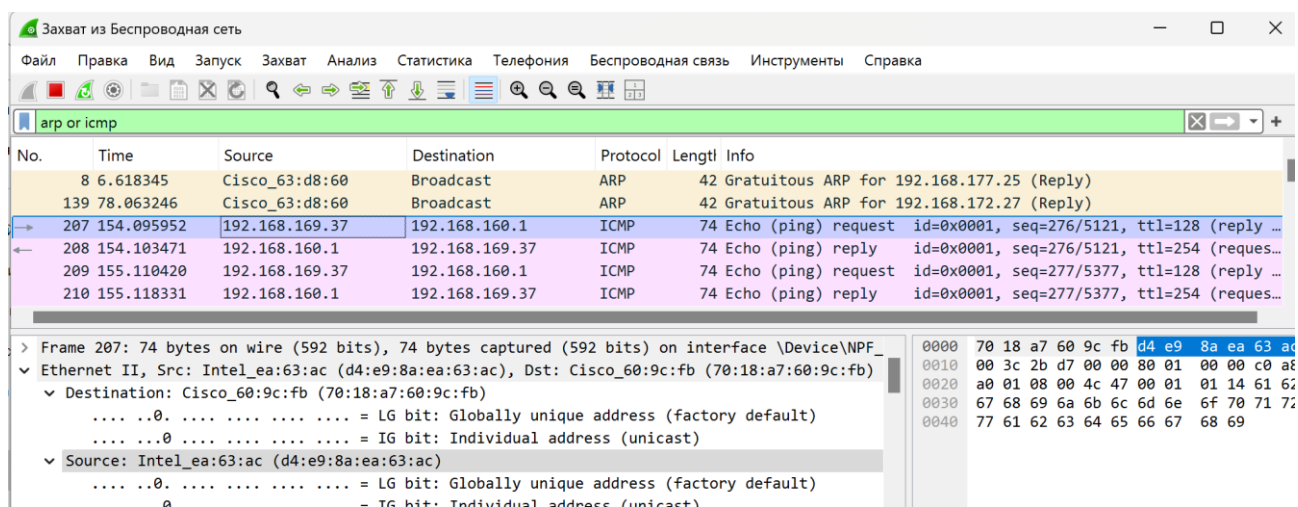


Рис. 2.10. MAC-адрес источника.

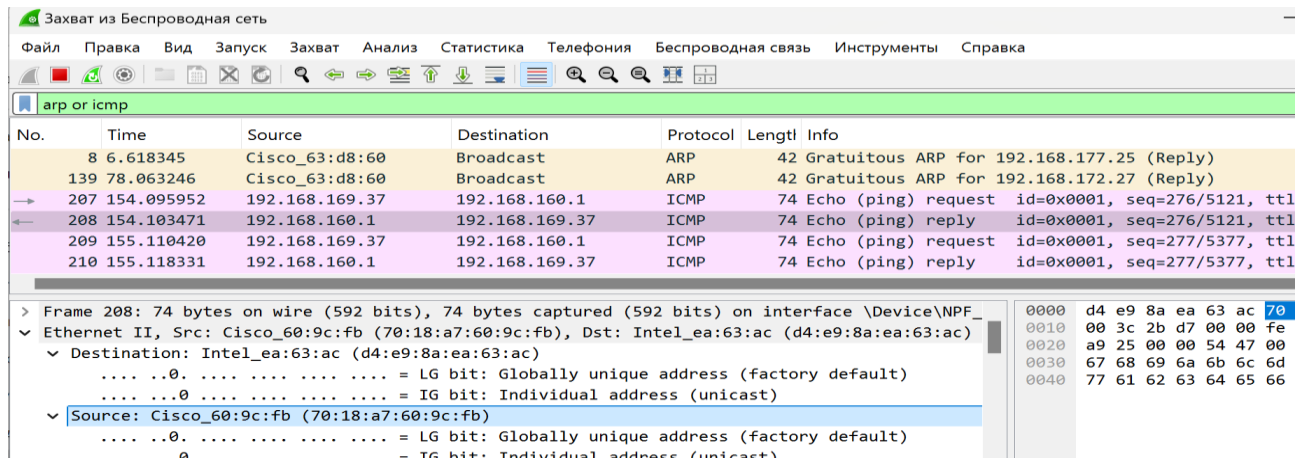


Рис. 2.11. MAC-адрес получателя.

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

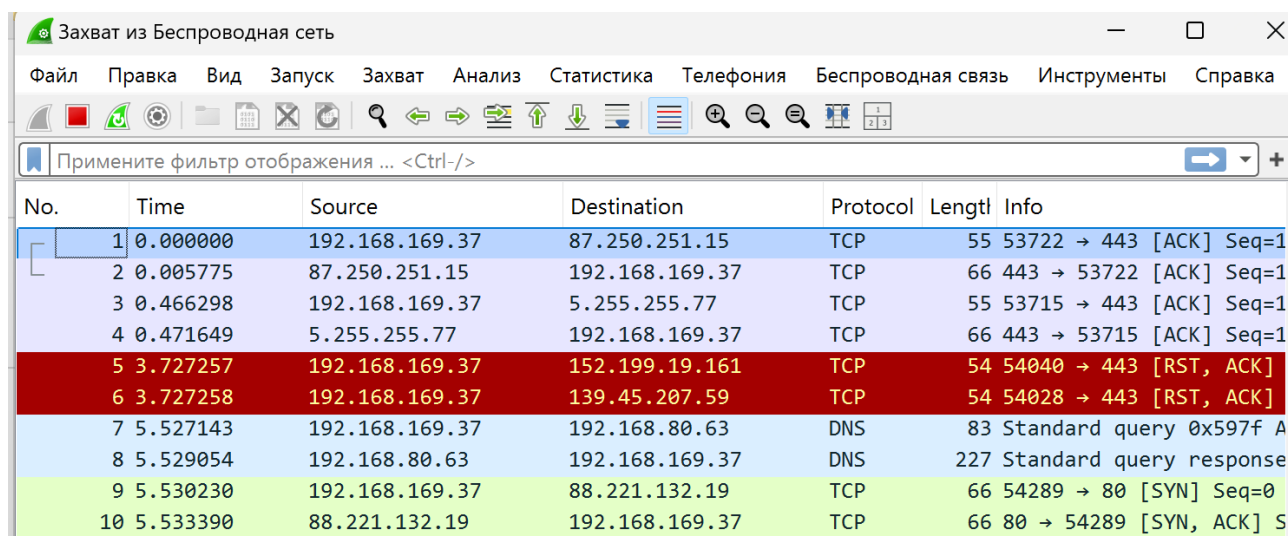


Рис. 3.1. Запуск Wireshark. Выбор активного сетевого интерфейса.

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

http://info.cern.ch - home of the first website

From here you can:

- [Browse the first website](#)
- [Browse the first website using the line-mode browser simulator](#)
- [Learn about the birth of the web](#)
- [Learn about CERN, the physics laboratory where the web was born](#)

Рис. 3.2. Открытие в браузере сайта CERN.

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

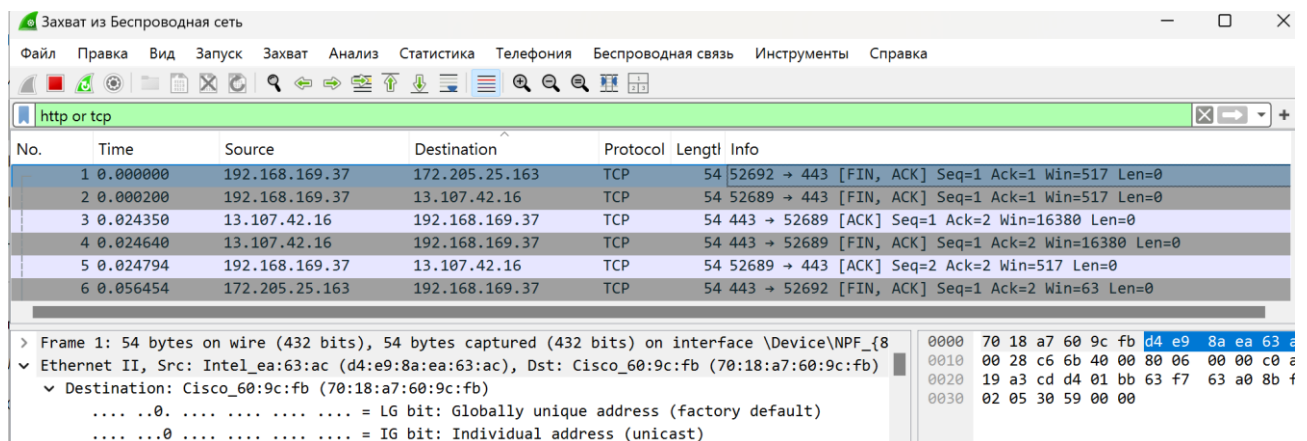


Рис. 3.3. Анализ информации по протоколу TCP.

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

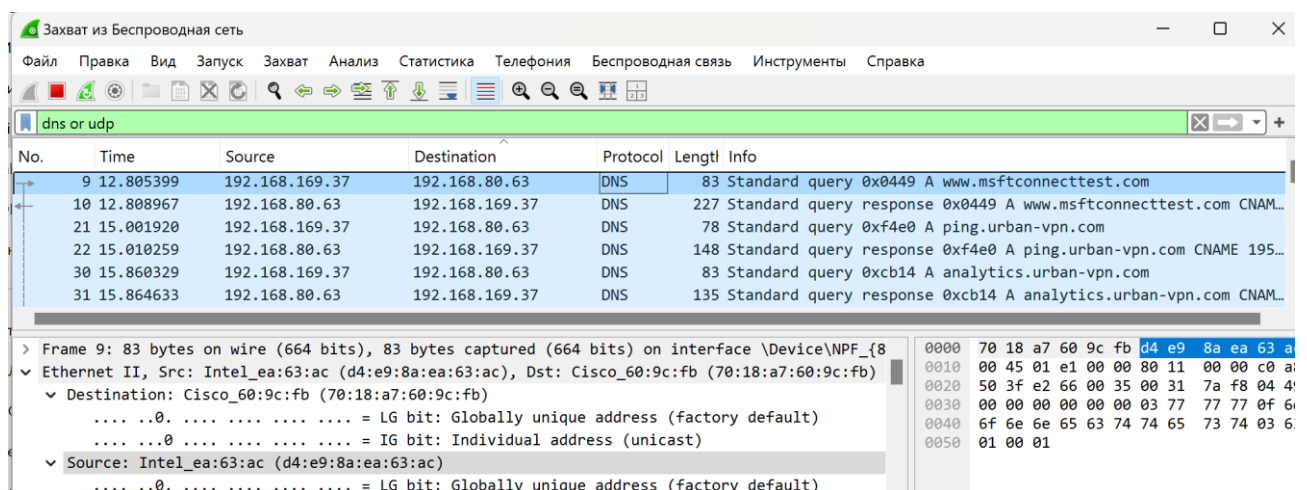


Рис. 3.4. Анализ информации по протоколу UDP.

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

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes options like 'Файл', 'Правка', 'Вид', 'Запуск', 'Захват', 'Анализ', 'Статистика', 'Телефония', 'Беспроводная связь', 'Инструменты', and 'Справка'. Below the menu is a toolbar with various icons. The filter bar at the top of the packet list contains the text 'quic'. The packet list table shows several packets, with packet 6627 selected. The packet details pane on the right shows the structure of packet 6627, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and QUIC IETF. The QUIC IETF section is expanded, showing connection information such as packet length, header form, fixed bit, packet type, reserved, packet number length, version, destination connection ID, source connection ID, token length, and packet number.

No.	Time	Source	Destination	Protocol	Length	Info
6627	2432.929710	192.168.169.37	139.45.207.50	QUIC	1292	Initial, DCID=b1cdb165d5ec4471, PKN: 1,
6628	2432.929873	192.168.169.37	139.45.207.50	QUIC	1292	Initial, DCID=b1cdb165d5ec4471, PKN: 2,
6633	2432.970323	139.45.207.50	192.168.169.37	QUIC	1292	Initial, SCID=0a22eafcd5404023, PKN: 1,
6635	2432.994226	139.45.207.50	192.168.169.37	QUIC	1292	Initial, SCID=0a22eafcd5404023, PKN: 2,
6636	2432.994226	139.45.207.50	192.168.169.37	QUIC	1292	Handshake, SCID=0a22eafcd5404023
6637	2432.994226	139.45.207.50	192.168.169.37	QUIC	1292	Handshake, SCID=0a22eafcd5404023
6638	2432.994226	139.45.207.50	192.168.169.37	QUIC	376	Handshake, SCID=0a22eafcd5404023
6639	2432.995298	192.168.169.37	139.45.207.50	QUIC	81	Handshake, DCID=0a22eafcd5404023
6640	2432.998021	192.168.169.37	139.45.207.50	QUIC	82	Handshake, DCID=0a22eafcd5404023

> Frame 6627: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{8201EEE5-6DF...}

> Ethernet II, Src: Intel_ea:63:ac (d4:e9:8a:ea:63:ac), Dst: Cisco_60:9c:fb (70:18:a7:60:9c:fb)

> Internet Protocol Version 4, Src: 192.168.169.37, Dst: 139.45.207.50

✓ User Datagram Protocol, Src Port: 55412, Dst Port: 443

- Source Port: 55412
- Destination Port: 443
- Length: 1258
- Checksum: 0xc929 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 59]
- [Stream Packet Number: 1]
- > [Timestamps]
- UDP payload (1250 bytes)

✓ QUIC IETF

- > QUIC Connection information
- [Packet Length: 1250]
- 1... = Header Form: Long Header (1)
- .1.. = Fixed Bit: True
- ..00 = Packet Type: Initial (0)
- [.... 00.. = Reserved: 0]
- [.... ..00 = Packet Number Length: 1 bytes (0)]
- Version: 1 (0x00000001)
- Destination Connection ID Length: 8
- Destination Connection ID: b1cdb165d5ec4471
- Source Connection ID Length: 0
- Token Length: 0
- Length: 1232
- [Packet Number: 1]

Рис. 3.5. Анализ информации по протоколу QUIC.

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

Добро пожаловать в Wireshark

Захват

...с помощью этого фильтра: Все интерфейсы показаны ▾

Беспроводная сеть	└
Adapter for loopback traffic capture	└
Подключение по локальной сети* 9	

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

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

http://info.cern.ch - home of the first website

From here you can:

- [Browse the first website](#)
- [Browse the first website using the line-mode browser simulator](#)
- [Learn about the birth of the web](#)
- [Learn about CERN, the physics laboratory where the web was born](#)

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

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

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка						
tcp						
No.	Time	Source	Destination	Protocol	Length	Info
6201	2386.929102	192.168.169.37	157.240.205.60	TCP	54	52908 → 443 [FIN, ACK] Seq=775 Ack=724 Win=261376 L
6202	2386.936390	192.168.169.37	157.240.205.61	TCP	66	52924 → 5222 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
6203	2386.971292	157.240.205.61	192.168.169.37	TCP	66	5222 → 52924 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
6204	2386.971576	192.168.169.37	157.240.205.61	TCP	54	52924 → 5222 [ACK] Seq=1 Ack=1 Win=132096 Len=0
6205	2386.972217	192.168.169.37	157.240.205.61	TCP	290	52924 → 5222 [PSH, ACK] Seq=1 Ack=1 Win=132096 Len=
6206	2386.999875	157.240.205.61	192.168.169.37	TCP	54	5222 → 52924 [ACK] Seq=1 Ack=237 Win=66816 Len=0
6207	2387.123407	157.240.205.61	192.168.169.37	TCP	111	5222 → 52924 [PSH, ACK] Seq=1 Ack=237 Win=66816 Len
6208	2387.123407	157.240.205.61	192.168.169.37	TCP	150	5222 → 52924 [PSH, ACK] Seq=58 Ack=237 Win=66816 Le
6209	2387.123680	192.168.169.37	157.240.205.61	TCP	54	52924 → 5222 [ACK] Seq=237 Ack=154 Win=131840 Len=0
6210	2387.134533	192.168.169.37	157.240.205.61	TCP	106	52924 → 5222 [PSH, ACK] Seq=237 Ack=154 Win=131840
6211	2387.152677	157.240.205.61	192.168.169.37	TCP	54	5222 → 52924 [ACK] Seq=154 Ack=289 Win=66816 Len=0
6212	2387.238765	192.168.169.37	87.229.142.100	TCP	54	[TCP Retransmission] 52907 → 443 [FIN, ACK] Seq=811
6213	2387.238851	192.168.169.37	157.240.200.60	TCP	54	[TCP Retransmission] 52909 → 443 [FIN, ACK] Seq=797
6214	2387.238866	192.168.169.37	157.240.205.60	TCP	54	[TCP Retransmission] 52906 → 443 [FIN, ACK] Seq=982
6215	2387.238879	192.168.169.37	157.240.205.60	TCP	54	[TCP Retransmission] 52908 → 443 [FIN, ACK] Seq=775
6216	2387.272463	157.240.205.61	192.168.169.37	TCP	100	5222 → 52924 [PSH, ACK] Seq=154 Ack=289 Win=66816 L
6217	2387.272463	157.240.205.61	192.168.169.37	TCP	107	5222 → 52924 [PSH, ACK] Seq=200 Ack=289 Win=66816 L
6218	2387.272463	157.240.205.61	192.168.169.37	TCP	116	5222 → 52924 [PSH, ACK] Seq=253 Ack=289 Win=66816 L

Рис. 4.3. Анализ handshake протокола TCP.

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

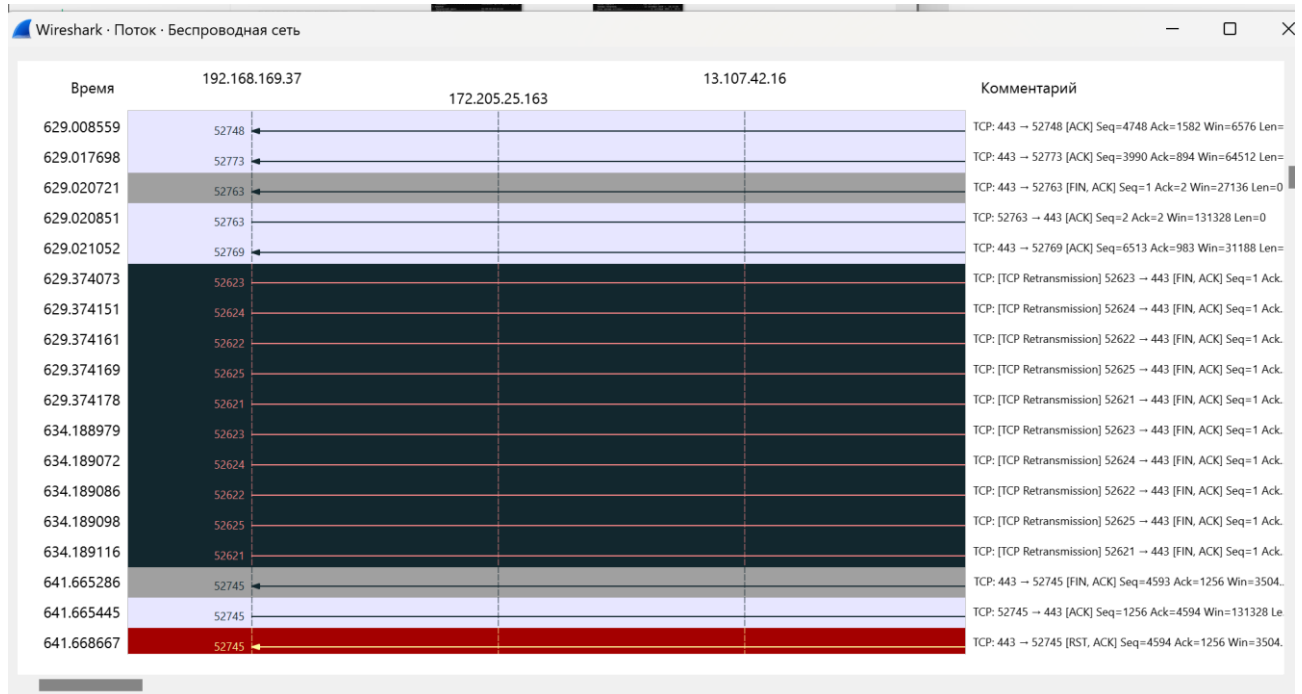


Рис. 4.4. График потока.

Вывод:

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