

# Лабораторная работа №3

Анализ трафика в Wireshark

---

**Студент: БАНСИМБА КЛОДЕЛИ ДЬЕГРА**

**Группа: НПИбд 02–22**

**дисциплина: Сетевые технологии (Lab 03)**

# Цель работы

---

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



# MAC-адресация

```
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:ee4c%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.

# MAC-адресация

```
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. . . . . : 80-FF-E5-B7-8A-10  
DHCP включен. . . . . : Нет  
Автонастройка включена. . . . . : Да  
  
Адаптер Ethernet Ethernet:  
  
DNS-суффикс подключения . . . . . :  
Описание. . . . . : VirtualBox Host-Only Ethernet  
Адаптер  
Физический адрес. . . . . : 0A-00-27-00-00-05  
DHCP включен. . . . . : Нет  
Автонастройка включена. . . . . : Да  
Локальный IPv6-адрес канала . . . : fe80::6913:a1e4:1fca:fd04%5(0  
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.

# MAC-адресация

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

едgedl.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.



# MAC-адресация

```
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.
            /setclassid6 Изменяет ID класса DHCP IPv6.
```

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

# MAC-адресация

---

```
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.

# Анализ кадров канального уровня в Wireshark

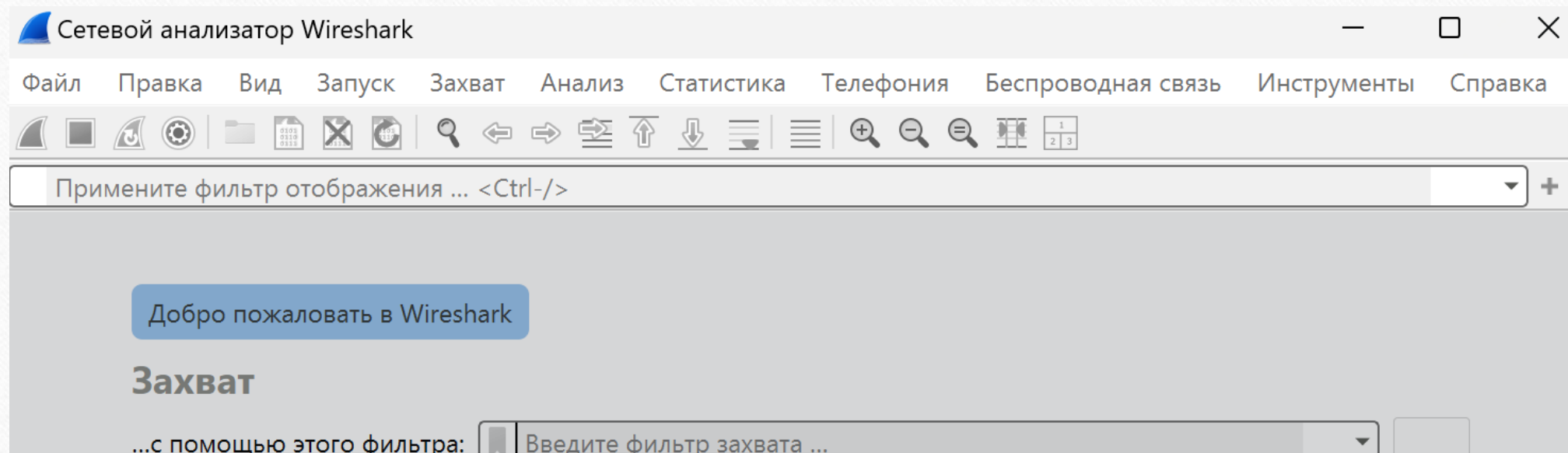
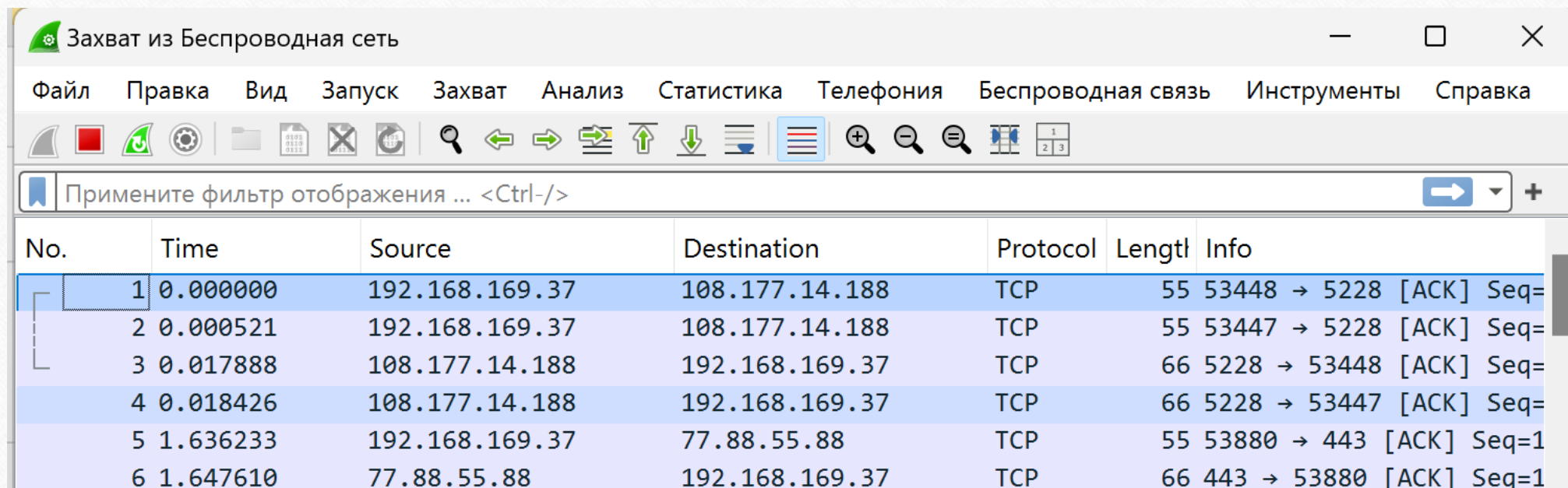


Рис. 2.1. Установка на нашем устройстве Wireshark.



# Анализ кадров канального уровня в Wireshark



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

# Анализ кадров канального уровня в Wireshark

---

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.

# Анализ кадров канального уровня в Wireshark

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

```
Обмен пакетами с 192.168.160.1 по 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:
```

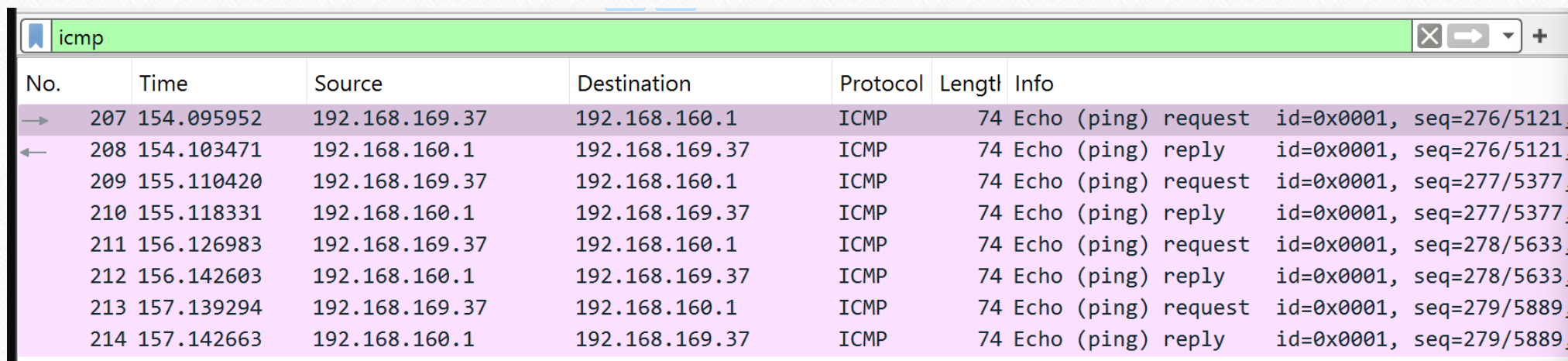
```
Минимальное = 3мсек, Максимальное = 15 мсек, Среднее = 8 мсек
```

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

Рис. 2.4. Пинг шлюза по умолчанию.



# Анализ кадров канального уровня в Wireshark



The image shows a Wireshark packet capture window with a filter bar at the top set to 'icmp'. Below the filter bar is a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are ICMP Echo (ping) requests and replies between 192.168.169.37 and 192.168.160.1. The packets are numbered 207 through 214. The 'Info' column shows details like 'Echo (ping) request' or 'Echo (ping) reply' and the ID and sequence number.

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 icmp.

# Анализ кадров канального уровня в Wireshark

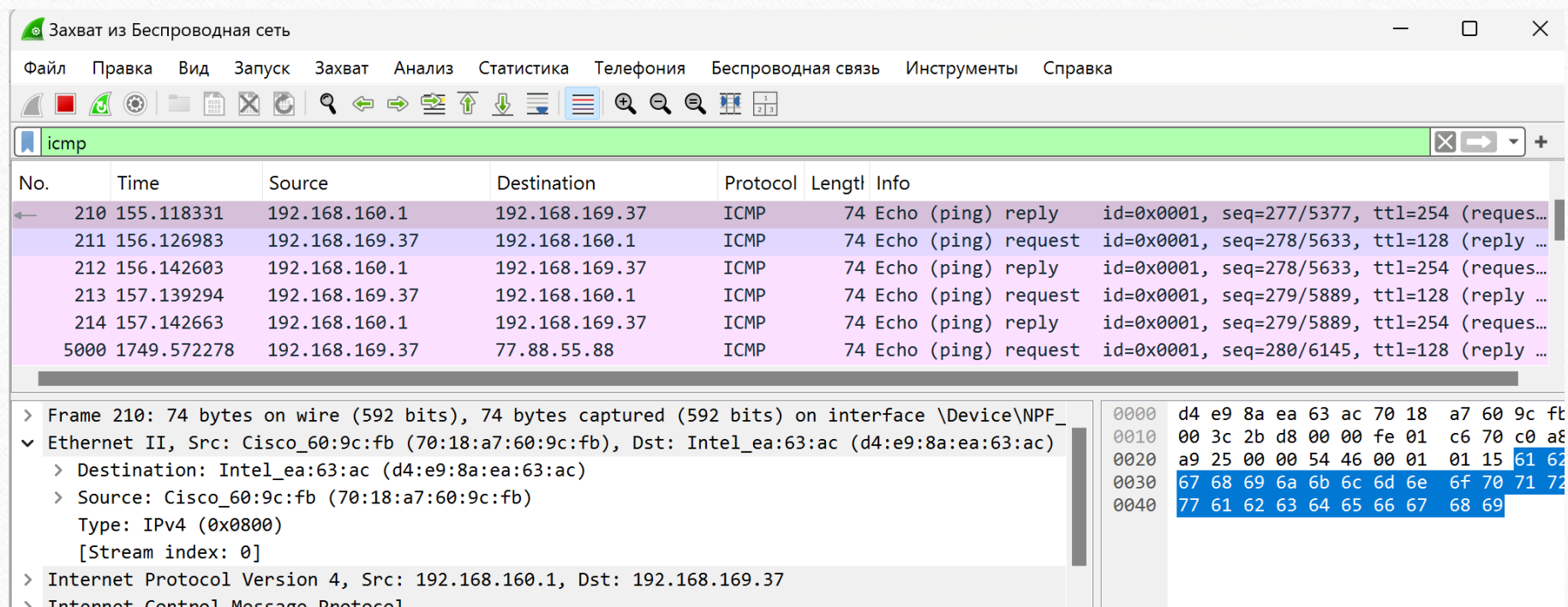
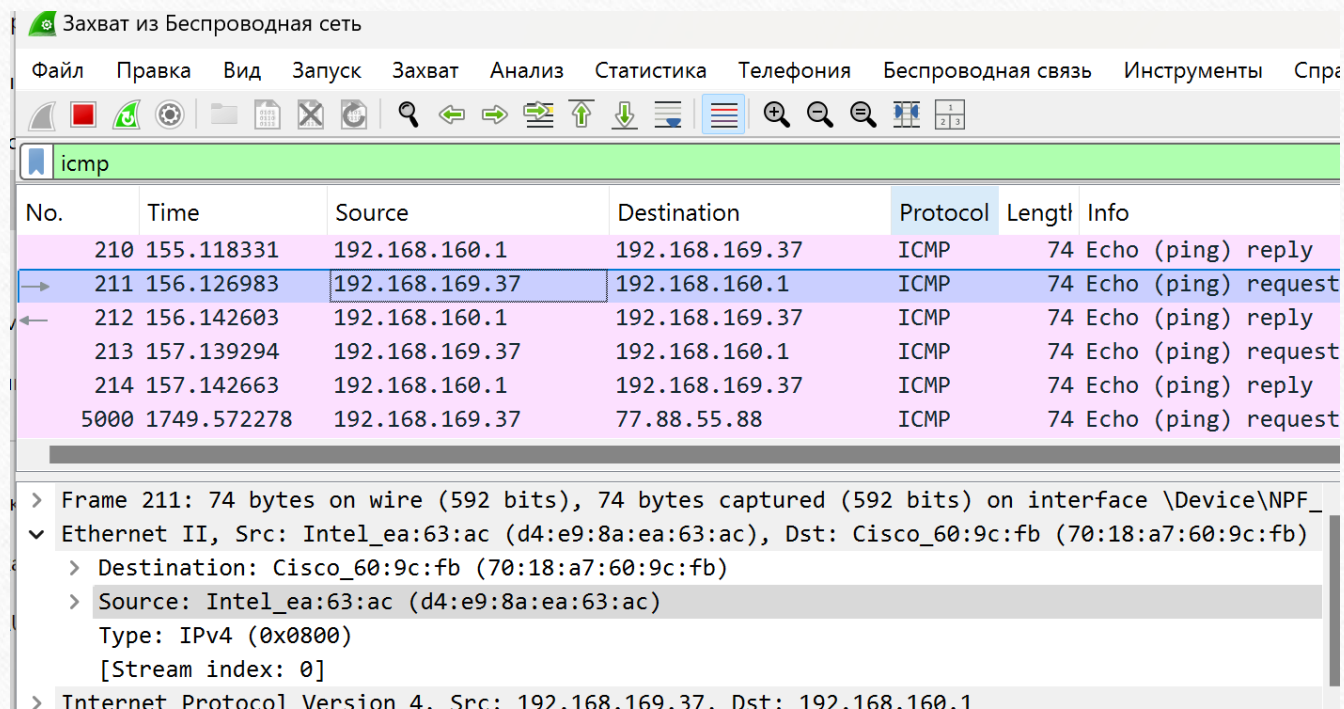


Рис. 2.6. Кадр ICMP — эхо-запрос.



# Анализ кадров канального уровня в Wireshark



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.



# Анализ кадров канального уровня в Wireshark

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes options like 'Захват из Беспроводная сеть', 'Файл', 'Правка', 'Вид', 'Запуск', 'Захват', 'Анализ', 'Статистика', 'Телефония', 'Беспроводная связь', 'Инструменты', and 'Справка'. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main display area is divided into three panes. The top pane shows a list of captured packets, with the 'arp' filter applied. The middle pane displays the details of the selected packet (Frame 139), showing the Ethernet II header and the ARP payload. The bottom pane shows the raw packet data in hexadecimal and ASCII.

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.

# Анализ кадров канального уровня в Wireshark

```
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 www.yandex.ru

# Анализ кадров канального уровня в Wireshark

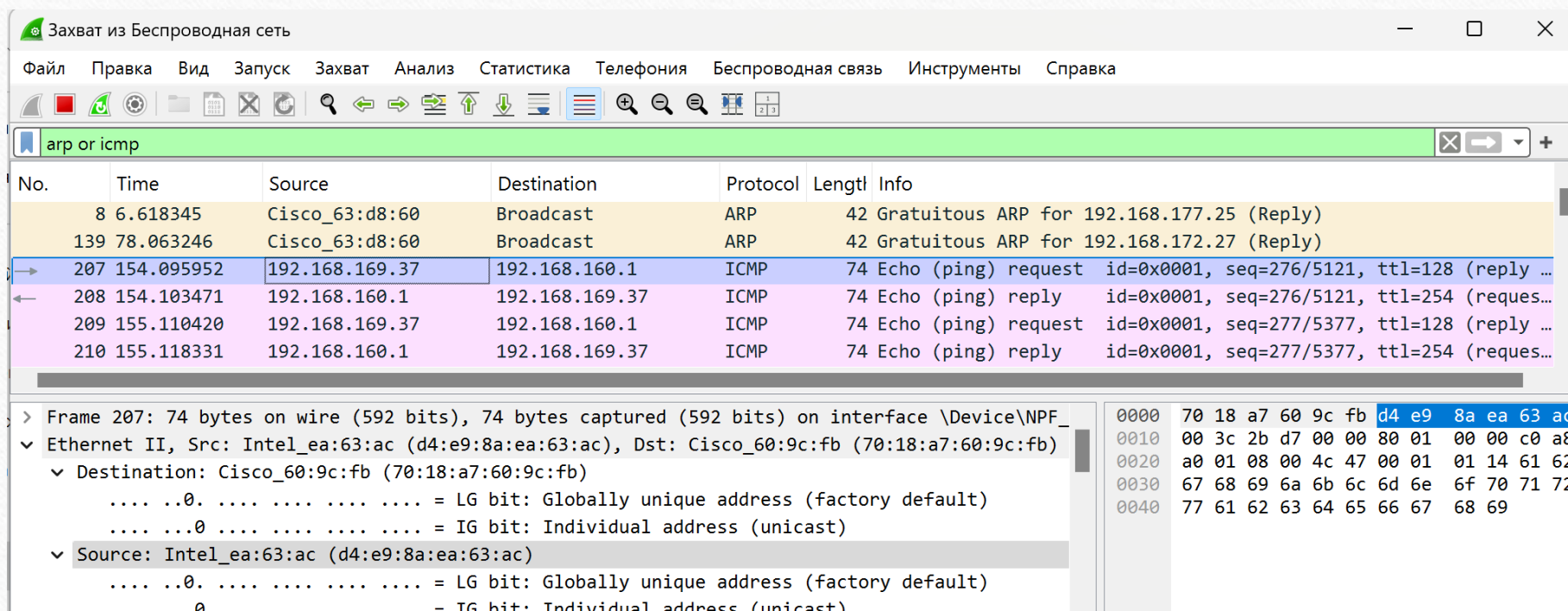


Рис. 2.10. MAC-адрес источника.



# Анализ кадров канального уровня в Wireshark

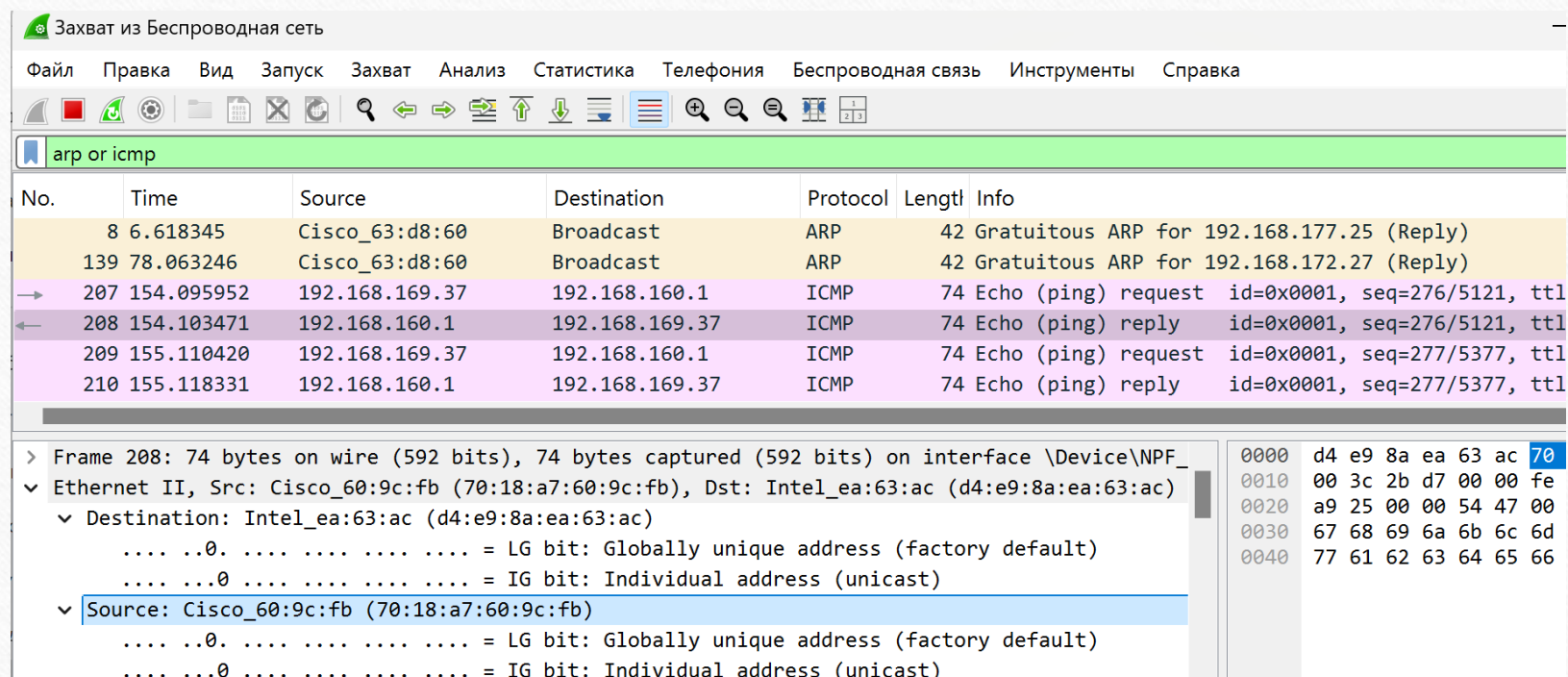


Рис. 2.11. MAC-адрес получателя.

# Анализ протоколов транспортного уровня в Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.169.37	87.250.251.15	TCP	55	53722 → 443 [ACK] Seq=1
2	0.005775	87.250.251.15	192.168.169.37	TCP	66	443 → 53722 [ACK] Seq=1
3	0.466298	192.168.169.37	5.255.255.77	TCP	55	53715 → 443 [ACK] Seq=1
4	0.471649	5.255.255.77	192.168.169.37	TCP	66	443 → 53715 [ACK] Seq=1
5	3.727257	192.168.169.37	152.199.19.161	TCP	54	54040 → 443 [RST, ACK]
6	3.727258	192.168.169.37	139.45.207.59	TCP	54	54028 → 443 [RST, ACK]
7	5.527143	192.168.169.37	192.168.80.63	DNS	83	Standard query 0x597f A
8	5.529054	192.168.80.63	192.168.169.37	DNS	227	Standard query response
9	5.530230	192.168.169.37	88.221.132.19	TCP	66	54289 → 80 [SYN] Seq=0
10	5.533390	88.221.132.19	192.168.169.37	TCP	66	80 → 54289 [SYN, ACK] S

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

# Анализ протоколов транспортного уровня в Wireshark

---

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

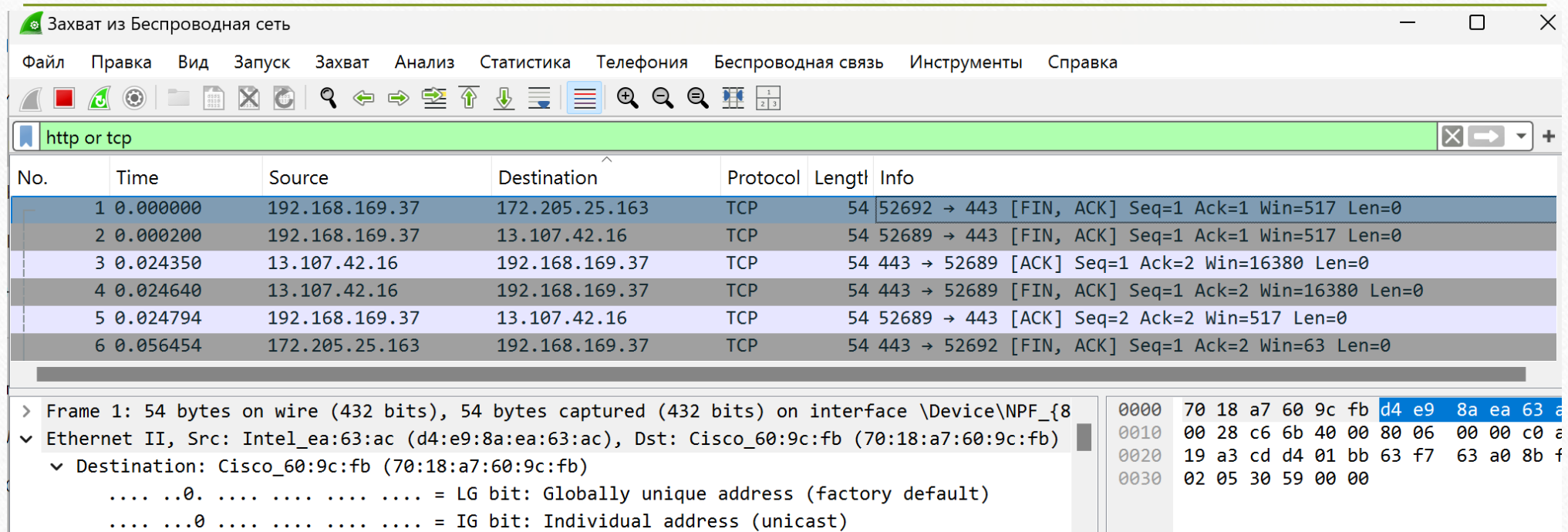
From here you can:

- [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.



# Анализ протоколов транспортного уровня в Wireshark



Захват из Беспроводная сеть

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

http or tcp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.169.37	172.205.25.163	TCP	54	52692 → 443 [FIN, ACK] Seq=1 Ack=1 Win=517 Len=0
2	0.000200	192.168.169.37	13.107.42.16	TCP	54	52689 → 443 [FIN, ACK] Seq=1 Ack=1 Win=517 Len=0
3	0.024350	13.107.42.16	192.168.169.37	TCP	54	443 → 52689 [ACK] Seq=1 Ack=2 Win=16380 Len=0
4	0.024640	13.107.42.16	192.168.169.37	TCP	54	443 → 52689 [FIN, ACK] Seq=1 Ack=2 Win=16380 Len=0
5	0.024794	192.168.169.37	13.107.42.16	TCP	54	52689 → 443 [ACK] Seq=2 Ack=2 Win=517 Len=0
6	0.056454	172.205.25.163	192.168.169.37	TCP	54	443 → 52692 [FIN, ACK] Seq=1 Ack=2 Win=63 Len=0

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{8...}

▼ 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)

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

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

0000 70 18 a7 60 9c fb d4 e9 8a ea 63 a

0010 00 28 c6 6b 40 00 80 06 00 00 c0 a

0020 19 a3 cd d4 01 bb 63 f7 63 a0 8b f

0030 02 05 30 59 00 00

Рис. 3.3. Анализ информации по протоколу TCP.

# Анализ протоколов транспортного уровня в Wireshark

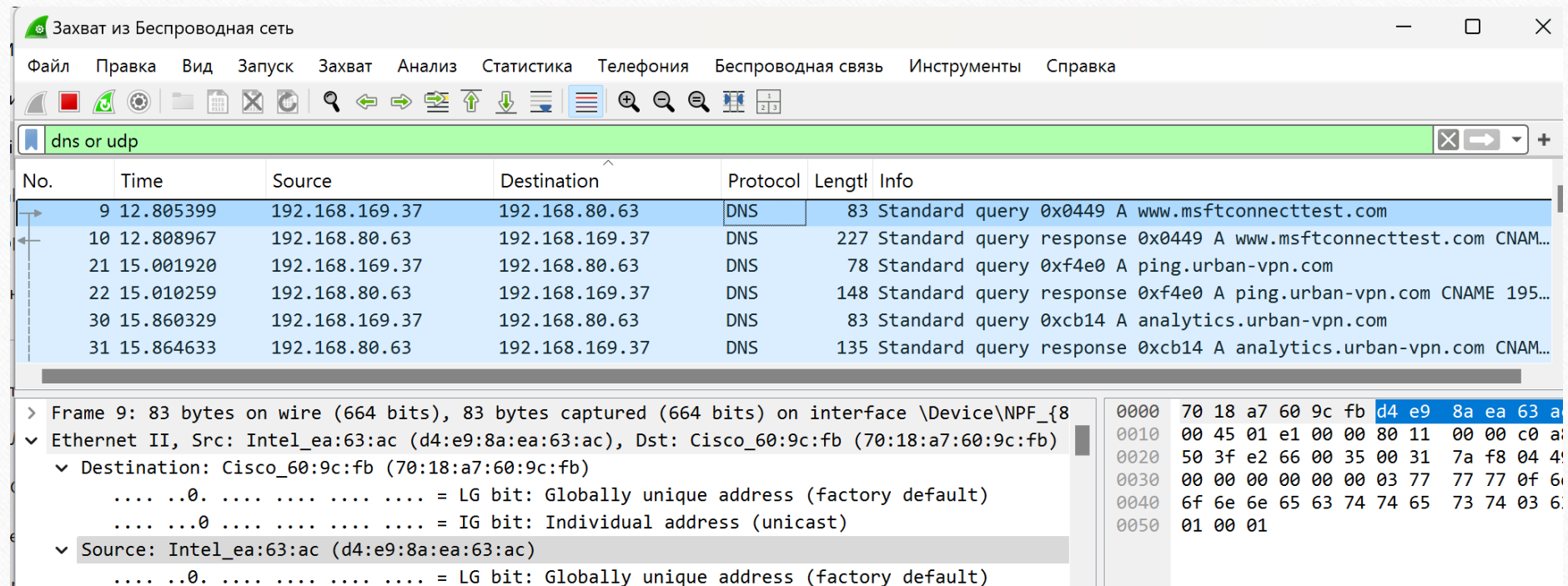
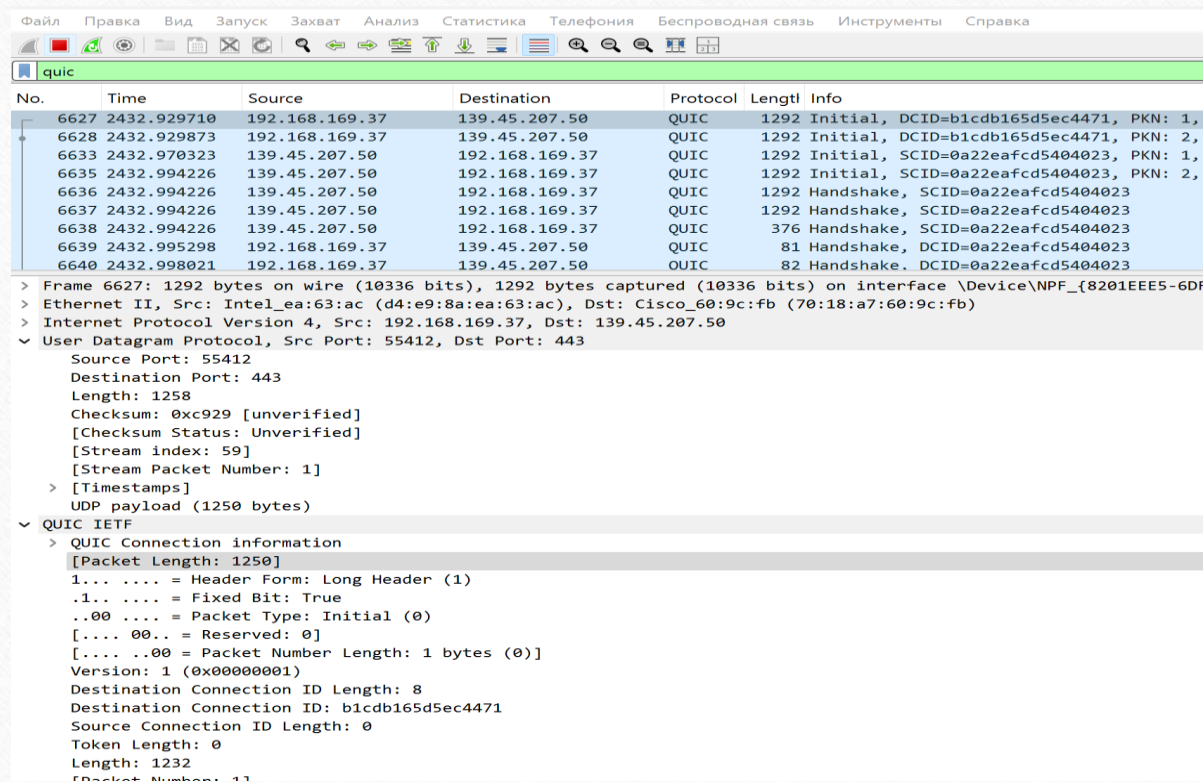


Рис. 3.4. Анализ информации по протоколу UDP.



# Анализ протоколов транспортного уровня в Wireshark



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\_{8201EEE5-6D...}

> 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)

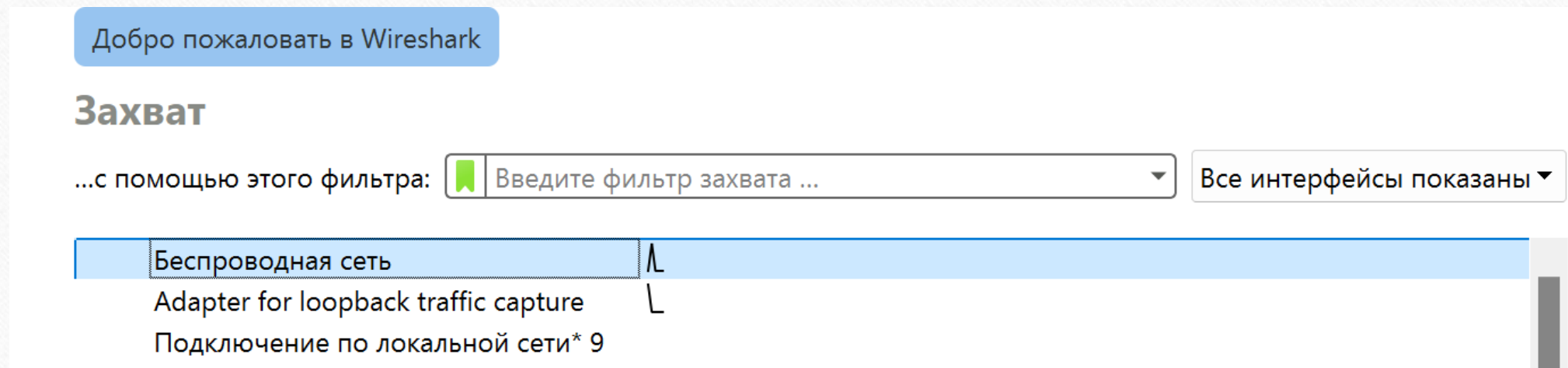
✓ QUIC IETF

- > 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.



# Анализ handshake протокола TCP в Wireshark



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

# Анализ handshake протокола TCP в Wireshark

---

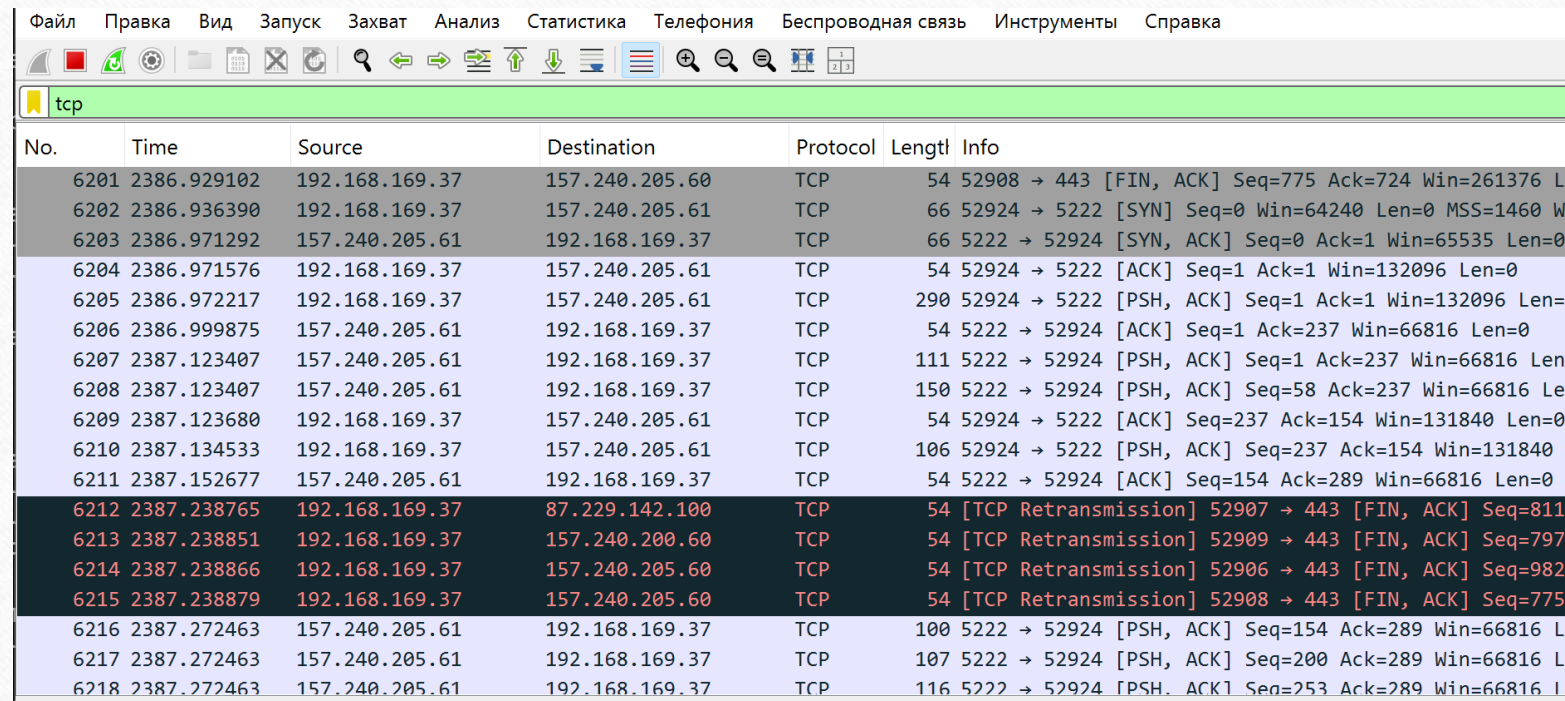
## **http://info.cern.ch - home of the first website**

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.

# Анализ handshake протокола TCP в Wireshark



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 Len=0
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.



# Анализ handshake протокола TCP в Wireshark

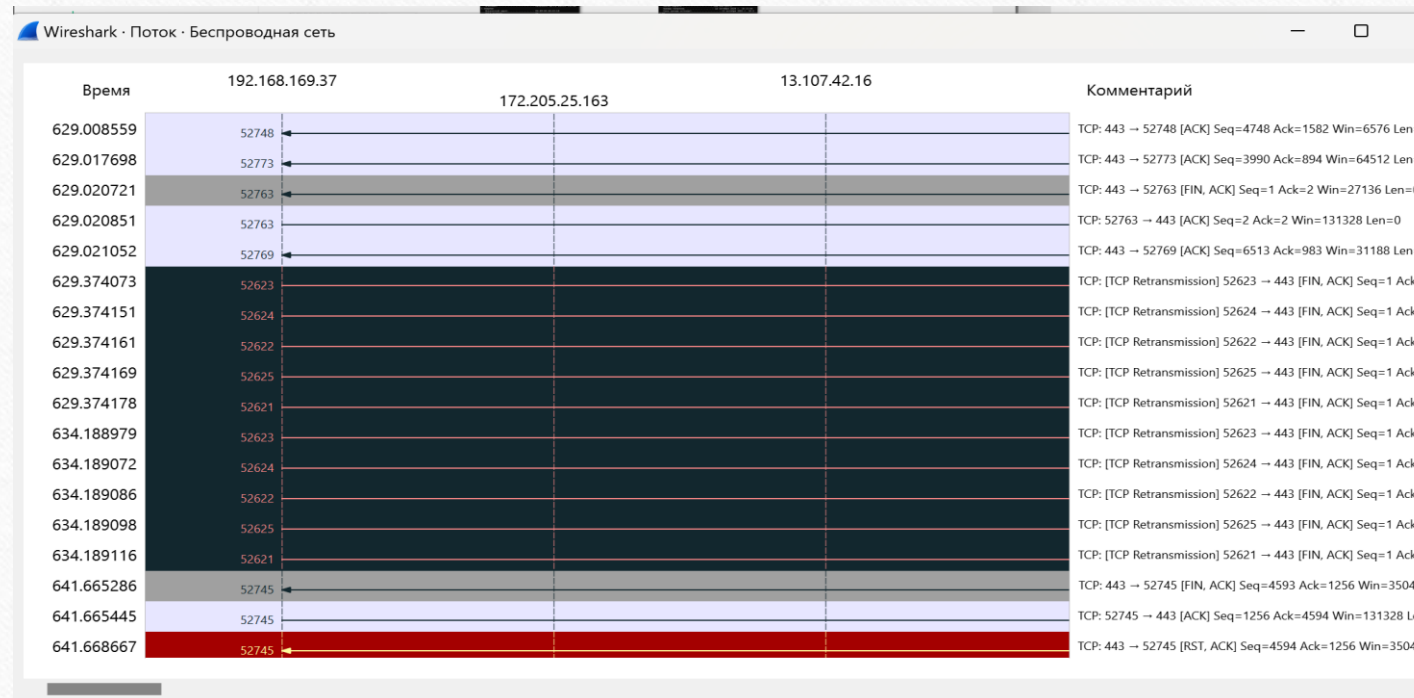


Рис. 4.4. График потока.

# ВЫВОД

---

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

---

*Спасибо за внимание!*