

Отчёт по лабораторной работе №3

Дисциплина: Сетевые технологии

Мишина Анастасия Алексеевна

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
2.1 MAC-адресация	6
2.2 Анализ кадров канального уровня в Wireshark	8
2.3 Анализ протоколов транспортного уровня в Wireshark . . .	14
2.4 Анализ handshake протокола TCP в Wireshark	17
3 Выводы	21

Список иллюстраций

2.1 Команда ipconfig	7
2.2 Команда ipconfig /all	8
2.3 Запуск захвата трафика	9
2.4 Пинг шлюза по умолчанию	9
2.5 Кадр ICMP - эхо-запрос: информация о длине кадра, типе Ethernet и MAC-адресах	10
2.6 Кадр ICMP - эхо-ответ: информация о длине кадра, типе Ethernet, MAC-адресах	11
2.7 Кадр ARP: информация о длине кадра, типе Ethernet, MAC-адресах	12
2.8 Пинг сайта www.yandex.ru	12
2.9 Запрос протокола ICMP	13
2.10 Ответ протокола ICMP	13
2.11 Кадр ARP - эхо-ответ	14
2.12 Кадр http - запрос	15
2.13 Кадр http - ответ	15
2.14 Кадр dns - запрос	16
2.15 Кадр dns - ответ	16
2.16 Кадр quic - запрос	17
2.17 Первая ступень handshake TCP	18
2.18 Вторая ступень handshake TCP	18
2.19 Третья ступень handshake TCP	19
2.20 График потока	20

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

2.1 МАС-адресация

С помощью команды ipconfig для ОС типа Windows выводим информацию о текущем сетевом соединении. Просматриваем информацию о сетевых адаптерах и конкретно о беспроводном соединении. Отсюда можно узнать IPv6-адрес, IPv4-адрес (уникальный IPv4-адрес узла), маску подсети (используется для определения сетевой и узловой частей IPv4-адреса) и шлюз (рис. 2.1).

```
C:\Users\nasmi>ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet 2:

DNS-суффикс подключения . . . . . : 
IPv4-адрес. . . . . : 192.168.56.1
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . :

Неизвестный адаптер OpenVPN Data Channel Offload:

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* 2:

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

Адаптер Ethernet Ethernet 3:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . : yandex-team.ru

Адаптер беспроводной локальной сети Беспроводная сеть* 3:

DNS-суффикс подключения . . . . . : wifi.rudn.su
IPv4-адрес. . . . . : 10.200.41.156
Маска подсети . . . . . : 255.255.0.0
Основной шлюз. . . . . : 10.200.0.254

C:\Users\nasmi>
```

Рис. 2.1: Команда ipconfig

Вводим ipconfig /all для вывода более подробной информации. Просматриваем данные о беспроводном соединении. Видим описание устройства (производитель Intel, MAC-адрес - DC-45-46-63-D4-E5). MAC-адрес состоит из 6 октетов: первые 3 октета идентифицируют производителя, последние 3 октета идентифицируют сетевой интерфейс (рис. 2.2).

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 : DC-45-46-63-D4-E6
DHCP включен : Да
Автонастройка включена : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 2:

Состояние среды : Среда передачи недоступна.
DNS-суффикс подключения :
Описание : Microsoft Wi-Fi Direct Virtual Adapter #2
Физический адрес : DE-45-46-63-D4-E5
DHCP включен : Да
Автонастройка включена : Да

Адаптер Ethernet Ethernet 3:

Состояние среды : Среда передачи недоступна.
DNS-суффикс подключения : yandex-team.ru
Описание : TAP-Windows Adapter V9
Физический адрес : 00-FF-80-8F-B7-D6
DHCP включен : Да
Автонастройка включена : Да

Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения : wifi.rudn.su
Описание : Intel(R) Wi-Fi 6E AX211 160MHz
Физический адрес : DC-45-46-63-D4-E5
DHCP включен : Да
Автонастройка включена : Да
IPv4-адрес : 10.200.41.156(Основной)
Маска подсети : 255.255.0.0
Аренда получена : 11 октября 2024 г. 15:23:03
Срок аренды истекает : 12 октября 2024 г. 16:05:23
Основной шлюз : 10.200.0.254
DHCP-сервер : 1.1.1.1
DNS-серверы : 10.128.0.240
 80.250.174.240
NetBIOS через TCP/IP : Включен

Рис. 2.2: Команда ipconfig /all

Проверив на специальном сайте производителя устройства по первым 3 октетам выясняем, что устройство выпущено компанией Intel Corporate. Взяв первый байт (DC) и переведя в двоичную систему счисления, получаем 11011100. Так как последний бит = 0, адрес является индивидуальным. Предпоследний бит = 0, следовательно, адрес глобально администрируемый.

2.2 Анализ кадров канального уровня в Wireshark

Запускаем Wireshark и выбираем беспроводное соединение. Запускаем захват трафика (рис. 2.3).

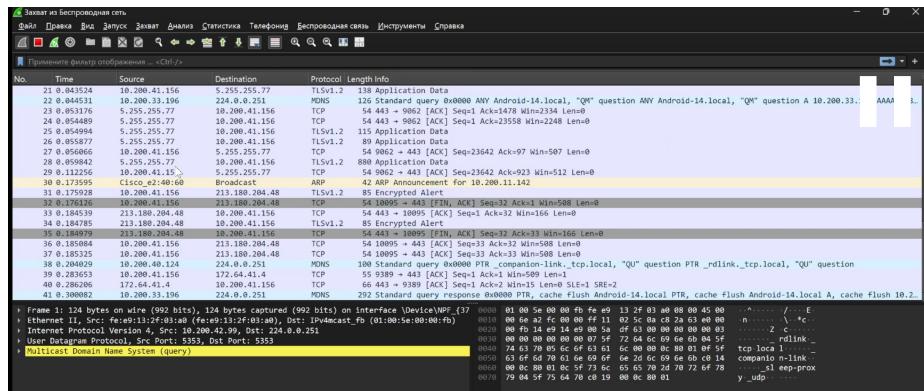


Рис. 2.3: Запуск захвата трафика

Шлюз по умолчанию для моего устройства - 100.200.0.254 (было определено в предыдущем задании). С помощью команды ping 100.200.0.254 пингуем шлюз по умолчанию (рис. 2.4).

```

Основной шлюз . . . . . : 10.200.0.254
DHCP-сервер . . . . . : 1.1.1.1
DNS-серверы . . . . . : 10.128.0.240
                                         80.250.174.240
NetBios через TCP/IP . . . . . : Включен

C:\Users\nasmii>ping 10.200.0.254

Обмен пакетами с 10.200.0.254 по с 32 байтами данных:
Ответ от 10.200.0.254: число байт=32 время=1мс TTL=254
Ответ от 10.200.0.254: число байт=32 время=3мс TTL=254
Ответ от 10.200.0.254: число байт=32 время=2мс TTL=254
Ответ от 10.200.0.254: число байт=32 время=1мс TTL=254

Статистика Ping для 10.200.0.254:
Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 3 мсек, Среднее = 1 мсек

C:\Users\nasmii>

```

Рис. 2.4: Пинг шлюза по умолчанию

Останавливаем захват трафика. В строке фильтра указываем icmp. Убедимся, что в списке пакетов отобразятся только пакеты ICMP, в частности пакеты, которые были сгенерированы с помощью команды ping, отправленной с моего устройства на шлюз по умолчанию. Видим 4 пакета-запроса и 4 пакета-ответа. Выбираем запрос и просматриваем в нижней части экрана информацию о нем. На вкладке физического уровня можно

найти длину кадра (74 бита). Чтобы узнать MAC-адрес источника и шлюза перейдем на канальный уровень. Адрес источника (Source, откуда запрос отправлен) – это адрес моего устройства (DC-45-46-63-D4-E5). Адрес шлюза (destination, то куда отправлен запрос) - B8-E3-B1-7D-D5-B6. Тип адреса тут указан (показаны нулевые и первые биты MAC-адресов). Что адрес источника, что адрес шлюза индивидуальные и глобально администрируемые (рис. 2.5)

```

[+] icmp
No. Time Source Destination Protocol Length Info
--> 5607 92.963522 10.200.41.156 10.200.0.254 ICMP 74 Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 5608)
--< 5608 92.965219 10.200.41.156 10.200.0.254 ICMP 74 Echo (ping) reply id=0x0001, seq=45/11520, ttl=254 (request in 5607)
5708 93.976866 10.200.41.156 10.200.0.254 ICMP 74 Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 5709)
5709 93.980367 10.200.0.254 10.200.41.156 ICMP 74 Echo (ping) reply id=0x0001, seq=46/11776, ttl=254 (request in 5708)
5753 94.991985 10.200.41.156 10.200.0.254 ICMP 74 Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (reply in 5754)
5754 94.994239 10.200.0.254 10.200.41.156 ICMP 74 Echo (ping) reply id=0x0001, seq=47/12032, ttl=254 (request in 5753)
5852 96.007988 10.200.41.156 10.200.0.254 ICMP 74 Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (reply in 5853)
5853 96.009507 10.200.0.254 10.200.41.156 ICMP 74 Echo (ping) reply id=0x0001, seq=48/12288, ttl=254 (request in 5852)

Frame 5607: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface '\Device\NPF_{37F84577-90A2-4D97-8135-C0E8F824A437}'
Section begin: [10.200.41.156 (0x0000000000000000) > 10.200.0.254 (0x0000000000000000)] [ether Intel(R) Dual Band Wireless-AC 7265]
Encapsulation type: Ethernet (1)
Arrival Time: Oct 11, 2024 16:22:34.082690000 RTT Z (это)
UTC Arrival Time: Oct 11, 2024 13:22:34.082690000 UTC
Epoch Arrival Time: 1728652954.082690000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.040503000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 92.063522000 seconds]
Frame Number: 5607
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule String: ICMPv6]
[Ethernet II, Src: Intel(R) Dual Band Wireless-AC 7265 (00:0c:29:9e:00:00), Dst: HuaweiTechno_7d:d5:b6 (b8:e3:b1:7d:d5:b6)]
Destination: HuaweiTechno_7d:d5:b6 (b8:e3:b1:7d:d5:b6)
Source: Intel(R) Dual Band Wireless-AC 7265 (00:0c:29:9e:00:00)
Type: IPv4 (0x0800)
[Stream index: 1]
Internet Protocol Version 4, Src: 10.200.41.156, Dst: 10.200.0.254
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4d2e [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 45 (0x002d)
Sequence Number (LE): 11520 (0xd200)

Frame 5608: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface '\Device\NPF_{37F84577-90A2-4D97-8135-C0E8F824A437}'
Section begin: [10.200.0.254 (0x0000000000000000) > 10.200.41.156 (0x0000000000000000)] [ether Intel(R) Dual Band Wireless-AC 7265]
Encapsulation type: Ethernet (1)
Arrival Time: Oct 11, 2024 16:22:34.082690000 RTT Z (это)
UTC Arrival Time: Oct 11, 2024 13:22:34.082690000 UTC
Epoch Arrival Time: 1728652954.082690000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.040503000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 92.063522000 seconds]
Frame Number: 5608
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule String: ICMPv6]
[Ethernet II, Src: Intel(R) Dual Band Wireless-AC 7265 (00:0c:29:9e:00:00), Dst: HuaweiTechno_7d:d5:b6 (b8:e3:b1:7d:d5:b6)]
Destination: HuaweiTechno_7d:d5:b6 (b8:e3:b1:7d:d5:b6)
Source: Intel(R) Dual Band Wireless-AC 7265 (00:0c:29:9e:00:00)
Type: IPv4 (0x0800)
[Stream index: 1]
Internet Protocol Version 4, Src: 10.200.0.254, Dst: 10.200.41.156
Internet Control Message Protocol
Type: 8 (Echo (ping) reply)
Code: 0
Checksum: 0x4d2e [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 45 (0x002d)
Sequence Number (LE): 11520 (0xd200)

```

Рис. 2.5: Кадр ICMP - эхо-запрос: информация о длине кадра, типе Ethernet и MAC-адресах

Далее посмотрим на полученный ответ. Тут все почти то же самое, что и в запросе (длина кадра 74 бита). Только теперь MAC-адрес источника – MAC-адрес шлюза (B8-E3-B1-7D-D5-B6), а адрес назначения – адрес моего устройства (DC-45-46-63-D4-E5) (рис. 2.6).

No.	Time	Source	Destination	Protocol	Length Info
→ 5687 92.963522	10.200.41.156	10.200.0.254	10.200.41.156	ICMP	74 Echo (ping) request id=0x0001, seq=45/11520, ttl=128 (reply in 5688)
← 5688 92.965219	10.200.0.254	10.200.41.156	10.200.41.156	ICMP	74 Echo (ping) reply id=0x0001, seq=45/11520, ttl=254 (request in 5687)
5708 93.976866	10.200.41.156	10.200.0.254	10.200.41.156	ICMP	74 Echo (ping) request id=0x0001, seq=46/11776, ttl=128 (reply in 5709)
5709 93.988367	10.200.0.254	10.200.41.156	10.200.41.156	ICMP	74 Echo (ping) reply id=0x0001, seq=46/11776, ttl=254 (request in 5708)
5753 94.991985	10.200.41.156	10.200.0.254	10.200.41.156	ICMP	74 Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (reply in 5754)
5754 94.994239	10.200.0.254	10.200.41.156	10.200.41.156	ICMP	74 Echo (ping) reply id=0x0001, seq=47/12032, ttl=254 (request in 5753)
5852 96.007988	10.200.41.156	10.200.0.254	10.200.41.156	ICMP	74 Echo (ping) request id=0x0001, seq=48/12288, ttl=128 (reply in 5853)
5853 96.009507	10.200.0.254	10.200.41.156	10.200.41.156	ICMP	74 Echo (ping) reply id=0x0001, seq=48/12288, ttl=254 (request in 5852)

Frame 5688: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface '\Device\NPF_{37FB4577-90A2-4D97-8135-C0E8F824A437}'
Section number: 1
Interface id: 0 (\Device\NPF_{37FB4577-90A2-4D97-8135-C0E8F824A437})
Encapsulation type: Ethernet (1)
Arrival Time: Oct 11, 2024 16:21:34.004387000 UTC 2 (эмана)
UTC Arrival Time: Oct 11, 2024 16:21:34.004387000 UTC
Epsilon Arrival Time: Oct 11, 2024 16:21:34.004387000 UTC
[Link layer shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.001697000 seconds]
[Time delta from previous displayed frame: 0.001697000 seconds]
[Time since reference or first frame: 92.965219000 seconds]
Frame Number: 5688
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:etherype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: HuaweiTechno_7d:d5:b6 (b8:e3:b1:7d:d5:b6), Dst: Intel_63:d4:e5 (dc:45:46:63:d4:
> Destination Intel_63:d4:e5 (dc:45:46:63:d4:e5) ↴
> Source HuaweiTechno_7d:d5:b6 (b8:e3:b1:7d:d5:b6)
Type: IPv4 (0x0800)
[Stream index: 1]
Internet Protocol Version 4, Src: 10.200.0.254, Dst: 10.200.41.156
Internet Control Message Protocol

Рис. 2.6: Кадр ICMP - эхо-ответ: информация о длине кадра, типе Ethernet, MAC-адресах

Изучим кадры данных протокола ARP: длина кадра равняется 42 байта. Hardware type – это адрес канального уровня (Ethernet (1)), Protocol type – сетевой уровень (протокол IPv4), далее указаны размеры MAC-адреса (6 байт) и размер IPv4-адреса (4 байта). Код запроса – 1. Изучим данные в полях заголовка Ethernet II. Здесь указаны MAC-адреса источника и получателя. Получатель в нашем случае – широковещательный адрес (групповой и локально администрируемый). Источник – адрес нашего шлюза (индивидуальный и глобально администрируемый) (рис. 2.7).

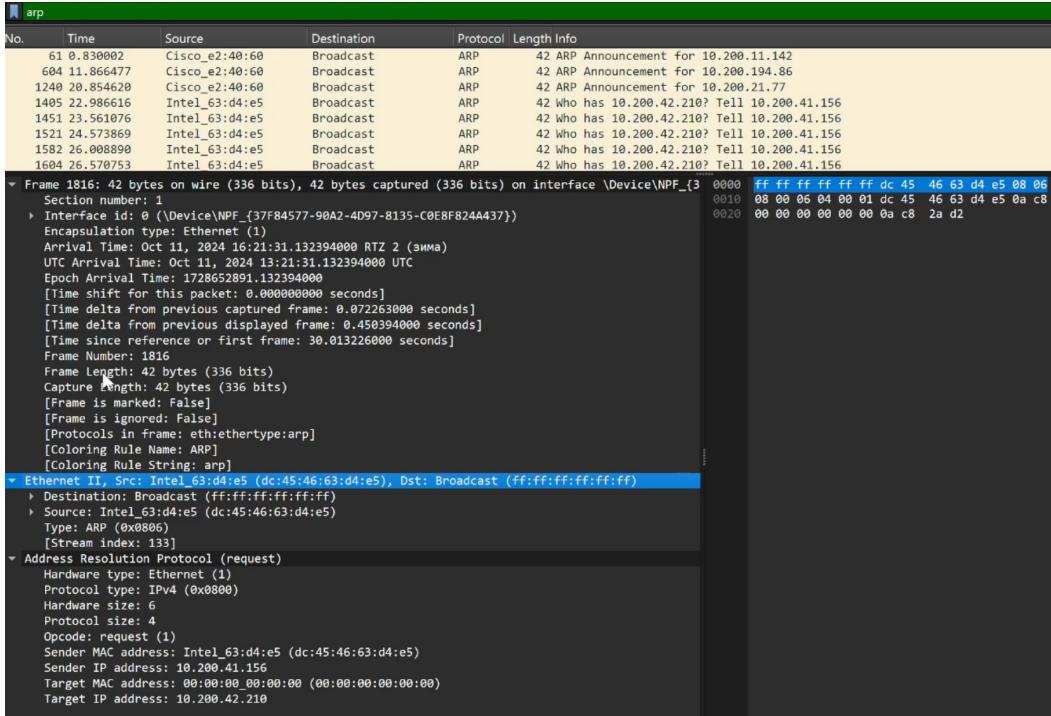


Рис. 2.7: Кадр ARP: информация о длине кадра, типе Ethernet, MAC-адресах

Начнем новый процесс захвата трафика в Wireshark. Пропингуем сайт яндекса - www.yandex.ru. На wi-fi sci-pfu ни один из сайтов не пинговался, поэтому переключаемся на раздачу интернета с телефона и продолжаем выполнение работы, сайт пингуется успешно (рис. 2.8).

```
C:\Users\nasmi>
C:\Users\nasmi>ping www.yandex.ru

Обмен пакетами с www.YANDEX.ru [5.255.255.77] с 32 байтами данных:
Ответ от 5.255.255.77: число байт=32 время=79мс TTL=51
Ответ от 5.255.255.77: число байт=32 время=32мс TTL=51
Ответ от 5.255.255.77: число байт=32 время=38мс TTL=51
Ответ от 5.255.255.77: число байт=32 время=51мс TTL=51

Статистика Ping для 5.255.255.77:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
        (0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 32мсек, Максимальное = 79 мсек, Среднее = 50 мсек

C:\Users\nasmi>
```

Рис. 2.8: Пинг сайта www.yandex.ru

Изучим запрос протокола ICMP. Адрес источника (Source, откуда запрос отправлен) – это адрес моего устройства (DC-45-46-63-D4-E5). Адрес полу-

чателя (destination, то куда отправлен запрос) - 02-4B-77-4D-6F-6A. Адрес источника индивидуальный и глобально администрируемые, адрес шлюза - индивидуальный и локально администрируемый (рис. 2.9).

No.	Time	Source	Destination	Protocol	Length Info
→ 106 2.769001	192.168.90.131	5.255.255.77		ICMP	74 Echo (ping) request id=0x0001, seq=65/16640, ttl=128 (reply in 108)
← 108 2.853351	5.255.255.77	192.168.90.131		ICMP	74 Echo (ping) reply id=0x0001, seq=65/16640, ttl=51 (request in 106)
118 3.775840	192.168.90.131	5.255.255.77		ICMP	74 Echo (ping) request id=0x0001, seq=66/16896, ttl=128 (reply in 119)
119 3.830786	5.255.255.77	192.168.90.131		ICMP	74 Echo (ping) reply id=0x0001, seq=66/16896, ttl=51 (request in 118)
122 4.791658	192.168.90.131	5.255.255.77		ICMP	74 Echo (ping) request id=0x0001, seq=67/17152, ttl=128 (reply in 125)
125 4.912462	5.255.255.77	192.168.90.131		ICMP	74 Echo (ping) reply id=0x0001, seq=67/17152, ttl=51 (request in 122)
135 5.805744	192.168.90.131	5.255.255.77		ICMP	74 Echo (ping) request id=0x0001, seq=68/17408, ttl=128 (reply in 137)
137 5.896679	5.255.255.77	192.168.90.131		ICMP	74 Echo (ping) reply id=0x0001, seq=68/17408, ttl=51 (request in 135)

```

Frame 106: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{37F84577-90A2-4097-8135-C0E8F824A437}
Section number: 1
Interface id: 0 (\Device\NPF_{37F84577-90A2-4097-8135-C0E8F824A437})
Encapsulation type: Ethernet (3)
Arrival Time: Oct 11, 2024 16:34:02.362148000 RTZ 2 (имма)
UTC Arrival Time: Oct 11, 2024 13:34:02.362148000 UTC
Epoch Arrival Time: 1728653642.362148000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.001189000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 2.769001000 seconds]
Frame Number: 106
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Intel_63:d4:e5 (dc:45:46:63:d4:e5), Dst: 02:4b:77:4d:6f:6a (02:4b:77:4d:6f:6a)
  Destination: Intel_63:d4:e5 (dc:45:46:63:d4:e5)
  Source: Intel_63:d4:e5 (dc:45:46:63:d4:e5)
  Type: IPv4 (0x0800)
  [Stream index: 0]
Internet Protocol Version 4, Src: 192.168.90.131, Dst: 5.255.255.77
  Internet Control Message Protocol

```

Рис. 2.9: Запрос протокола ICMP

Также изучим ответ протокола ICMP. Тут почти то же самое, однако адрес источника и получателя меняются местами (рис. 2.10).

No.	Time	Source	Destination	Protocol	Length Info
→ 106 2.769001	192.168.90.131	5.255.255.77		ICMP	74 Echo (ping) request id=0x0001, seq=65/16640, ttl=128 (reply in 108)
← 108 2.853351	5.255.255.77	192.168.90.131		ICMP	74 Echo (ping) reply id=0x0001, seq=65/16640, ttl=51 (request in 106)
118 3.775840	192.168.90.131	5.255.255.77		ICMP	74 Echo (ping) request id=0x0001, seq=66/16896, ttl=128 (reply in 119)
119 3.830786	5.255.255.77	192.168.90.131		ICMP	74 Echo (ping) reply id=0x0001, seq=66/16896, ttl=51 (request in 118)
122 4.791658	192.168.90.131	5.255.255.77		ICMP	74 Echo (ping) request id=0x0001, seq=67/17152, ttl=128 (reply in 125)
125 4.912462	5.255.255.77	192.168.90.131		ICMP	74 Echo (ping) reply id=0x0001, seq=67/17152, ttl=51 (request in 122)
135 5.805744	192.168.90.131	5.255.255.77		ICMP	74 Echo (ping) request id=0x0001, seq=68/17408, ttl=128 (reply in 137)
137 5.896679	5.255.255.77	192.168.90.131		ICMP	74 Echo (ping) reply id=0x0001, seq=68/17408, ttl=51 (request in 135)

```

Frame 108: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{37F84577-90A2-4097-8135-C0E8F824A437}
Section number: 1
Interface id: 0 (\Device\NPF_{37F84577-90A2-4097-8135-C0E8F824A437})
Encapsulation type: Ethernet (3)
Arrival Time: Oct 11, 2024 16:34:02.446498000 RTZ 2 (имма)
UTC Arrival Time: Oct 11, 2024 13:34:02.446498000 UTC
Epoch Arrival Time: 1728653642.446498000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.077327000 seconds]
[Time delta from previous displayed frame: 0.084358000 seconds]
[Time since reference or first frame: 2.853351000 seconds]
Frame Number: 108
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Intel_63:d4:e5 (dc:45:46:63:d4:e5), Dst: Intel_63:d4:e5 (dc:45:46:63:d4:e5)
  Destination: Intel_63:d4:e5 (dc:45:46:63:d4:e5)
  Source: Intel_63:d4:e5 (dc:45:46:63:d4:e5)
  Type: IPv4 (0x0800)
  [Stream index: 0]
Internet Protocol Version 4, Src: 5.255.255.77, Dst: 192.168.90.131
  Internet Control Message Protocol

```

Рис. 2.10: Ответ протокола ICMP

Изучим запросы и ответы ARP. MAC-адрес точки назначения – это первые 6 байт заголовка Ethernet, а MAC-адрес источника – следующие 6 байт заголовка Ethernet, оба MAC-адреса являются индивидуальными и глобально администрируемыми (рис. 2.11).

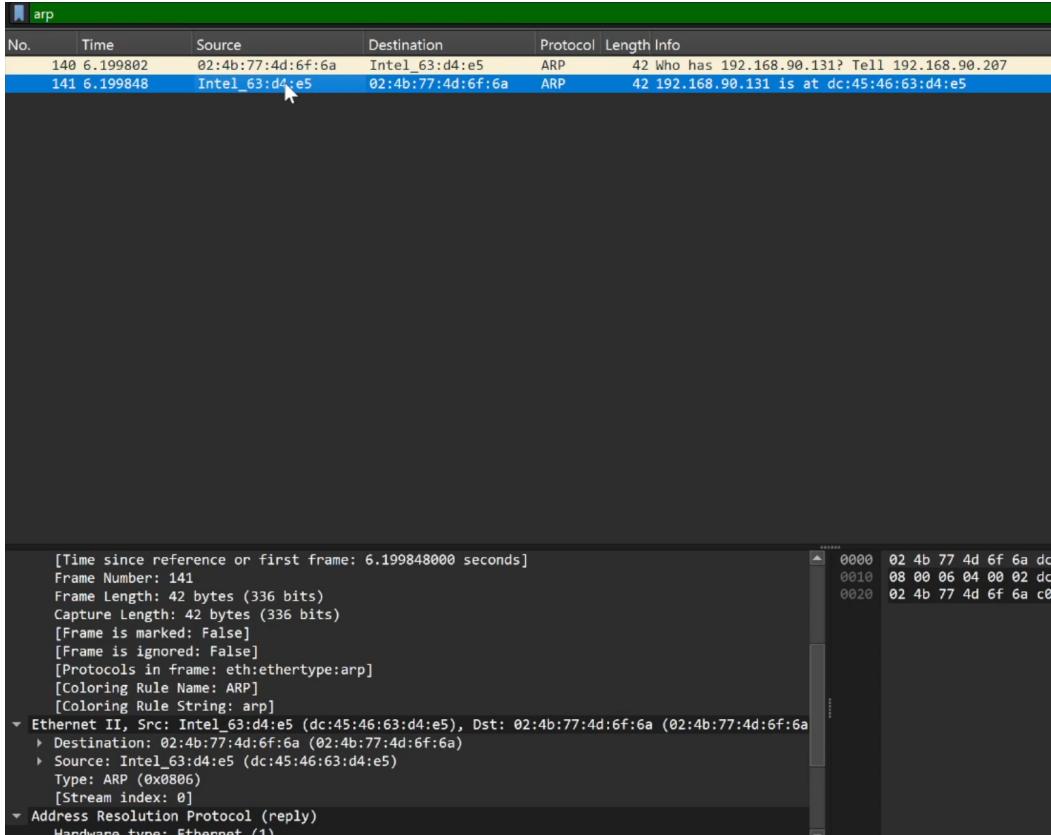


Рис. 2.11: Кадр ARP - эхо-ответ

2.3 Анализ протоколов транспортного уровня в Wireshark

Запустив Wireshark, начинаем захват трафика. Открываем в браузере сайт, работающий по протоколу HTTP (<http://info.cern.ch/>). Перемещаемся по страницам. В строке фильтра указываем http и просматриваем информацию по протоколу TCP о запросе. Порт источника задан случайно и равен 11298, порт назначения равен 80 - это стандартный порт HTTP. Также тут есть поле Порядковый номер (Sequence Number) и поле Номер подтверждения (Acknowledgment Number) (рис. 2.12)

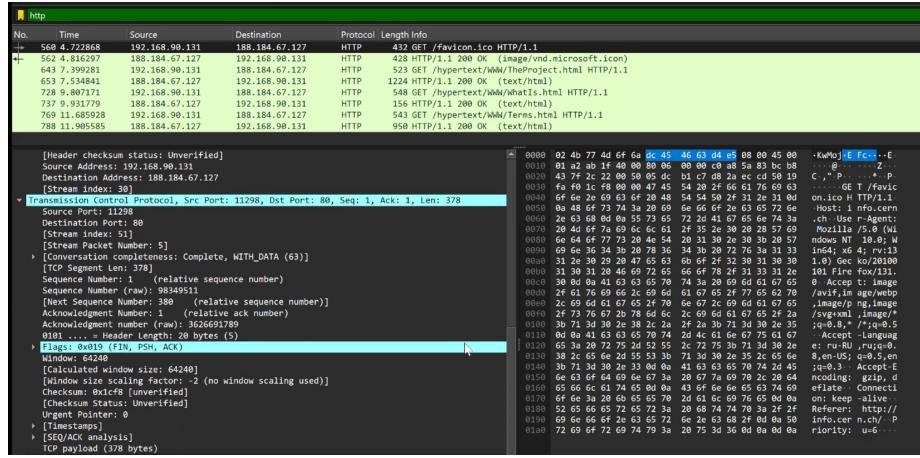


Рис. 2.12: Кадр http - запрос

В случае ответа порты заданы наоборот, то есть источник - 80 порт, назначение - 11298 (рис. 2.13)

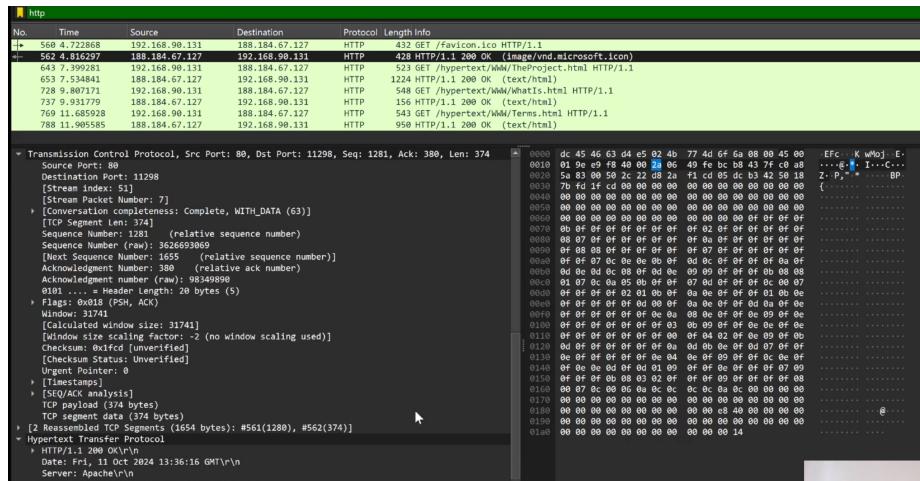


Рис. 2.13: Кадр http - ответ

В Wireshark в строке фильтра укажем dns и проанализируем информацию по протоколу UDP в случае запросов и ответов. Порт источника задан случайно и равен 52759, порт назначения равен 53 (порт DNS по умолчанию) (рис. 2.14). В случае ответа порты заданы наоборот рис. (2.15).

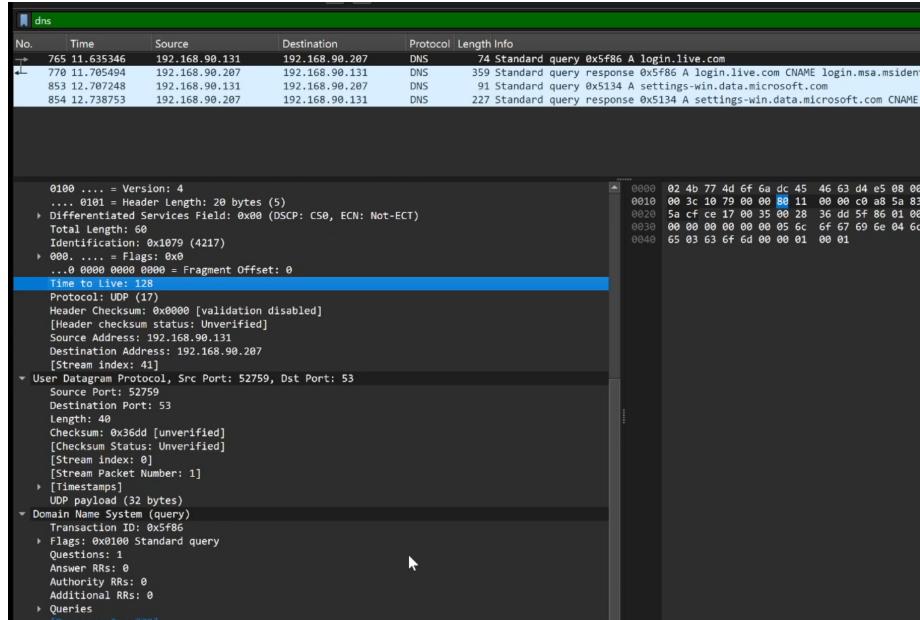


Рис. 2.14: Кадр dns - запрос

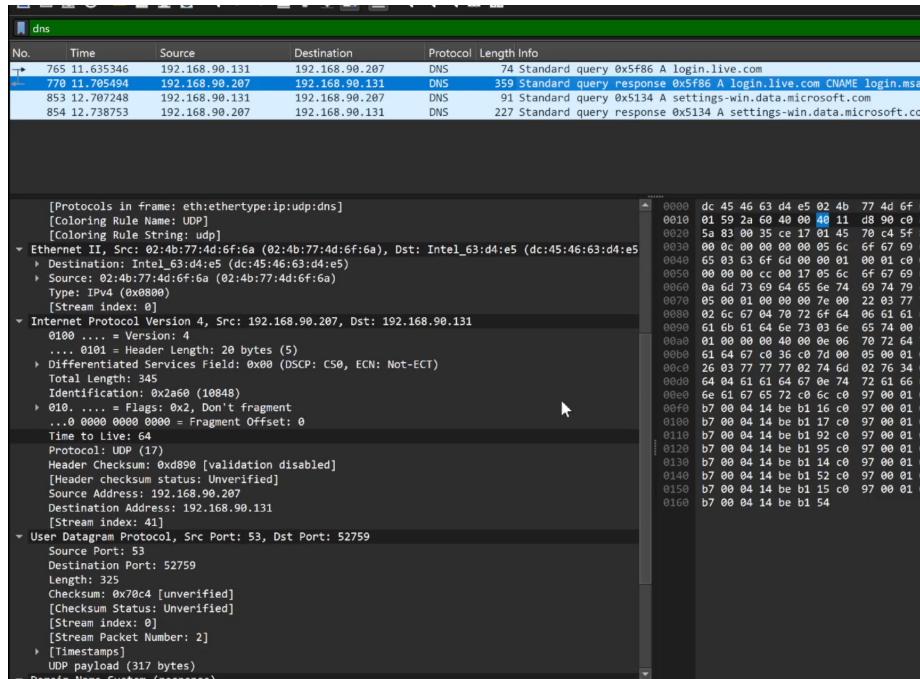


Рис. 2.15: Кадр dns - ответ

В строке фильтра указываем quic. Изначально ни одного запроса не находилось, пришлось сменить браузер с firefox на chrome. После этого запросы появились. Проанализируем информацию по протоколу quic. Как и в случае dns можем посмотреть информацию транспортного уровня по протоколу UDP. Порт источника задан случайно, выбором из непривелиги-

рованных и незанятых портов, и равен 52268, порт назначения равен 443 – это стандартный порт HTTPS, следовательно, quic сразу шифруется. Для создания альтернативы TCP поверх UDP строятся протоколы прикладного уровня QUIC IETF, которые управляют трафиком, управляют качеством обслуживания (рис. 2.16). В случае ответа порты заданы наоборот.

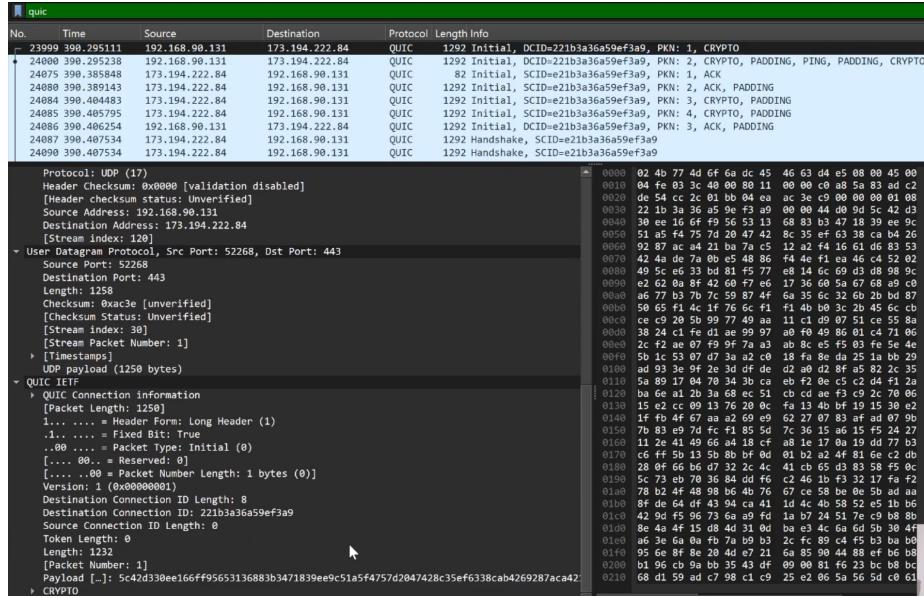


Рис. 2.16: Кадр quic - запрос

2.4 Анализ handshake протокола TCP в Wireshark

Начав захват трафика, запускаем в браузере сайт, работающий по протоколу HTTP (<http://info.cern.ch/>), однако анализировать будем тот handshake, который нашли для примера. Установление связи клиент-сервер в TCP осуществляется в три этапа (трёхступенчатый handshake).

1. Режим активного доступа (Active Open). Клиент посыпает сообщение SYN, ISSa, т.е. в передаваемом сообщении установлен бит SYN (Synchronize Sequence Number), а в поле Порядковый номер (Sequence Number) – начальное 32-битное значение ISSa (Initial Sequence Number)

Находим кадр с флагом SYN. Sequence Number = 0 (рис. 2.17).

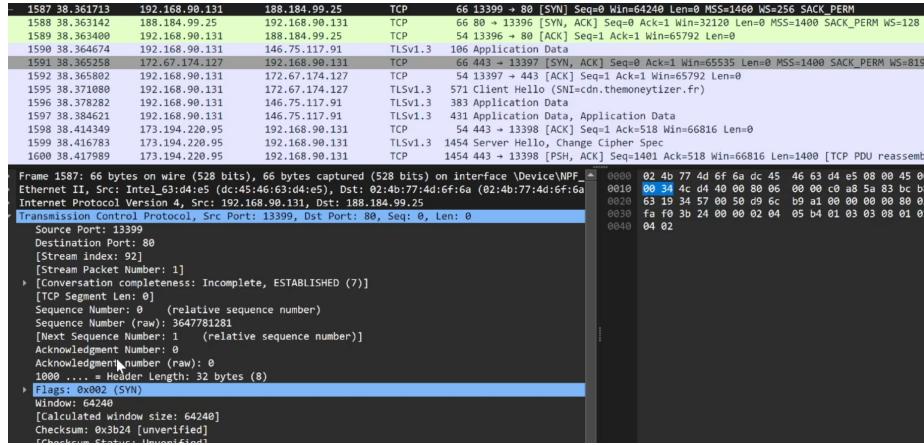


Рис. 2.17: Первая ступень handshake TCP

2. Режим пассивного доступа (Passive Open). Сервер откликается, посылая сообщение SYN, ACK, ISSb, ACK(ISSa+1), т.е. установлены биты SYN и ACK; в поле Порядковый номер (Sequence Number) хостом В устанавливается начальное значение счётчика — ISSb; поле Номер подтверждения (Acknowledgment Number) содержит значение ISSa, полученное в первом пакете от хоста А и увеличенное на единицу.

Кадр с флагами SYN и ACK, где ACK равен Sequence Number из предыдущего шага, увеличенный на 1 ($0 + 1 = 1$) (рис. 2.18).

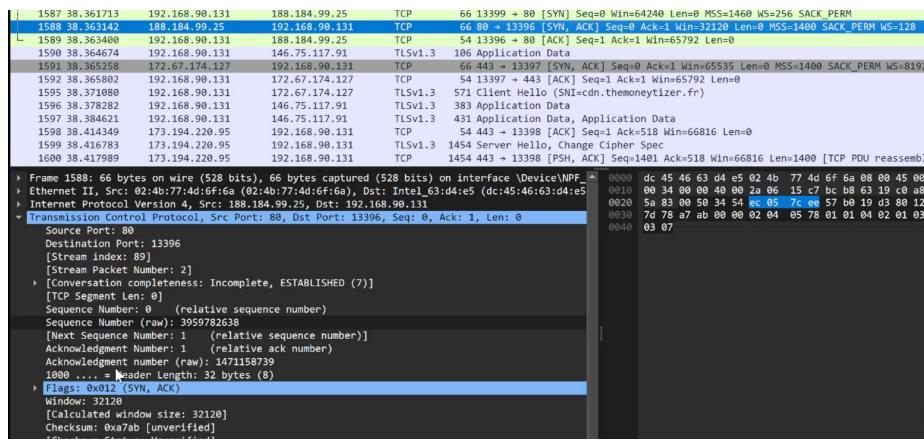


Рис. 2.18: Вторая ступень handshake TCP

3. Завершение рукопожатия. Клиент отправляет подтверждение получения SYNсегмента от сервера с идентификатором, равным ISN (сер-

вера)+1: ACK, ISSa+1, ACK(ISSb+1). В этом пакете установлен бит ACK, поле Порядковый номер (Sequence Number) содержит значение ISSa+1, поле Номер подтверждения (Acknowledgment Number) содержит значение ISSb+1. Посылкой этого пакета заканчивается трёхступенчатый handshake, и TCP-соединение считается установленным.

Теперь клиент может посыпать пакеты с данными на сервер по только что созданному виртуальному TCP-каналу: ACK, ISSa+1, ACK(ISSb+1); DATA.

Кадр с флагом ACK, где Sequence Number равен 1, Acknowledgment Number равен 1 (рис. 2.19).

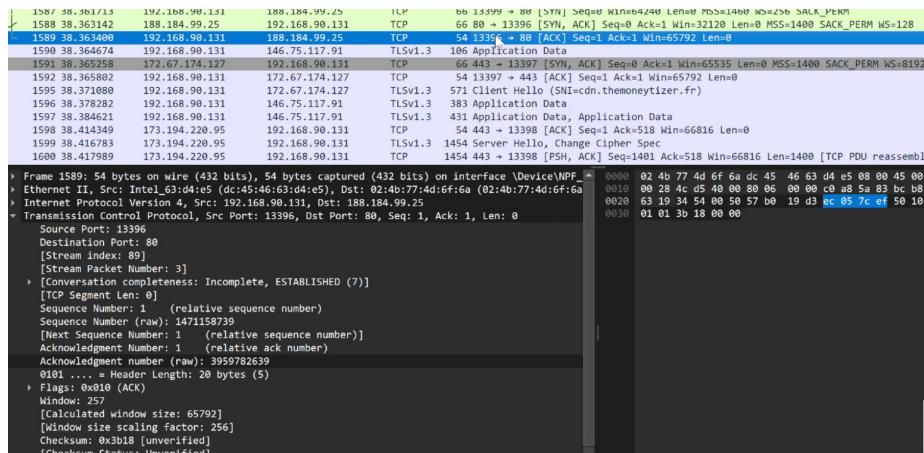


Рис. 2.19: Третья ступень handshake TCP

В Wireshark в меню «Статистика» выбираем «График Потока». На графике видно, что сначала клиент послал сообщение на сервер, значение Seq = 0. Затем сервер откликнулся, значение Seq = 0, а значение Ack = 1. И в третьем пакете клиент оправил подтверждение получение SYN-сегмента, оба значения Syn и Ack равны 1 (рис. 2.20).

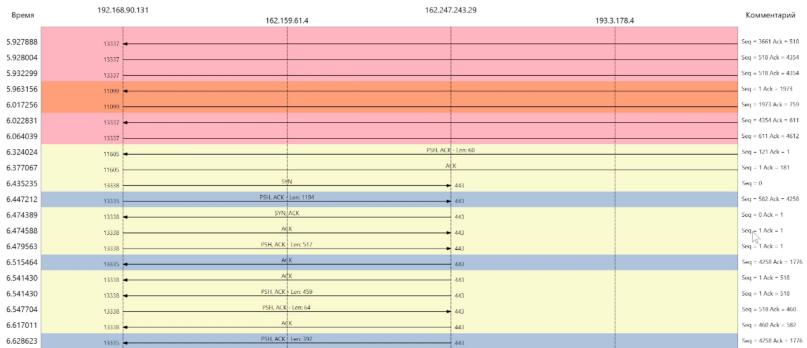


Рис. 2.20: График потока

В Wireshark останавливаем захват трафика.

3 Выводы

В результате выполнения работы были изучены посредством Wireshark кадры Ethernet, произведен анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP.