Лабораторная работа № 3.

Анализ трафика в Wireshark

Диана Алексеевна Садова

Содержание

# 1 Цель работы

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

# 2 MAC-адресация

## 2.1 Постановка задачи

1. Изучение возможностей команды ipconfig для ОС типа Windows (ifconfig для систем типа Linux).
2. Определение MAC-адреса устройства и его типа.

## 2.2 Порядок выполнения работы

1. С помощью команды ipconfig для ОС типа Windows или ifconfig для систем типа Linux выведите информацию о текущем сетевом соединении. Используйте разные опции команды. В отчёте поясните детально полученную в каждом случае при выводе информацию. Подтвердите свой ответ скриншотами.(рис. 1),(рис. 2),(рис. 3),(рис. 4)

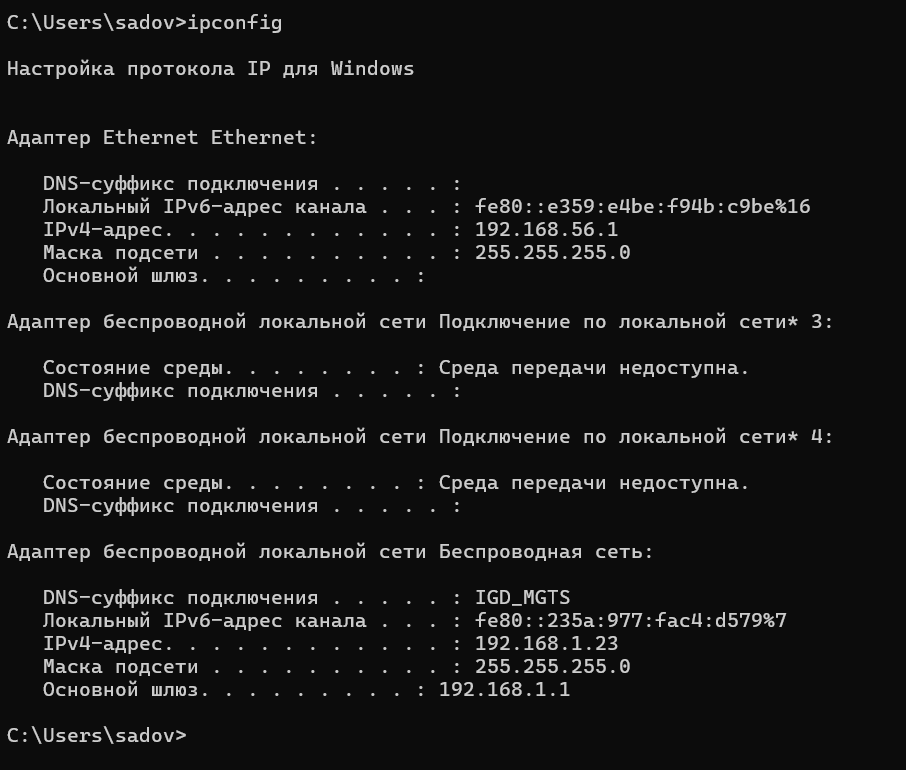


Рис. 1: Обычная команда ipconfig

Обычная команда ipconfig - выдает базовую информацию о текущем сетевом соединении

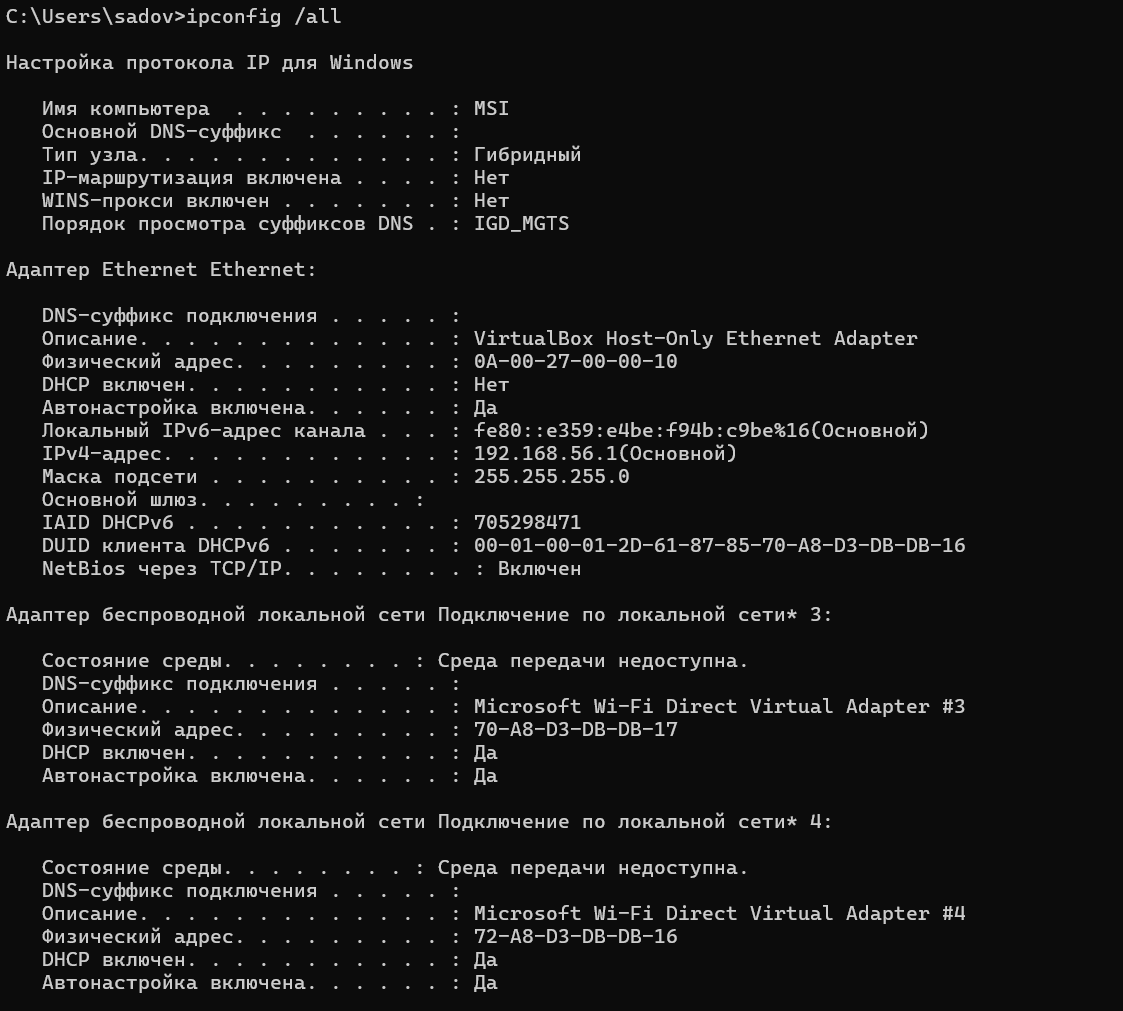


Рис. 2: Команда ipconfig /all

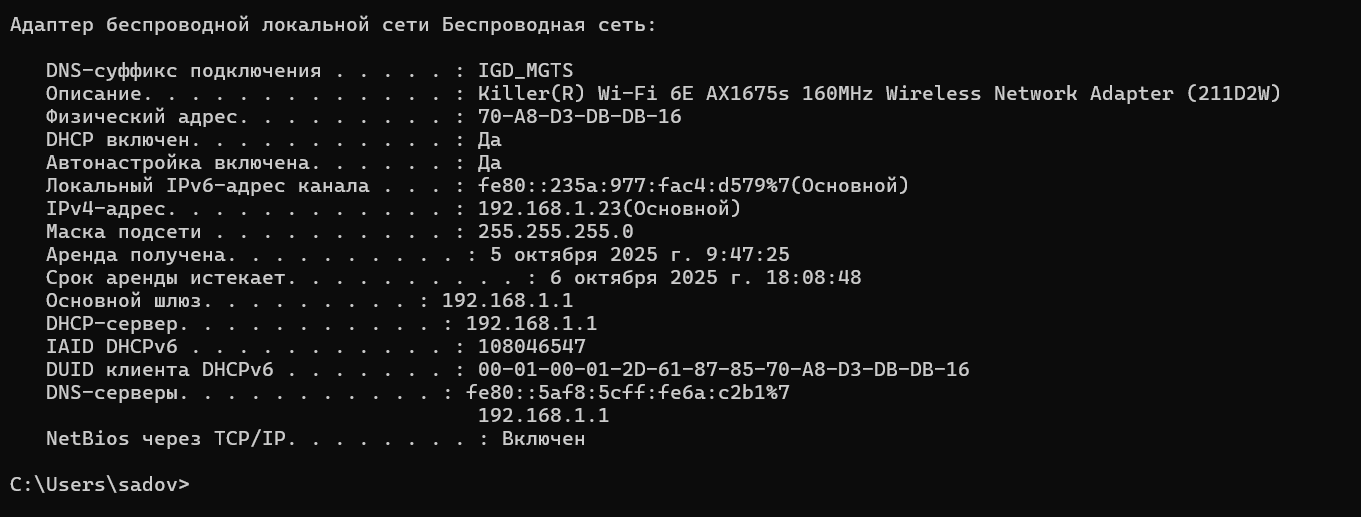


Рис. 3: Команда ipconfig /all

Команда ipconfig /all - выдает более полную (расширеную) информацию о текущем сетевом соединении

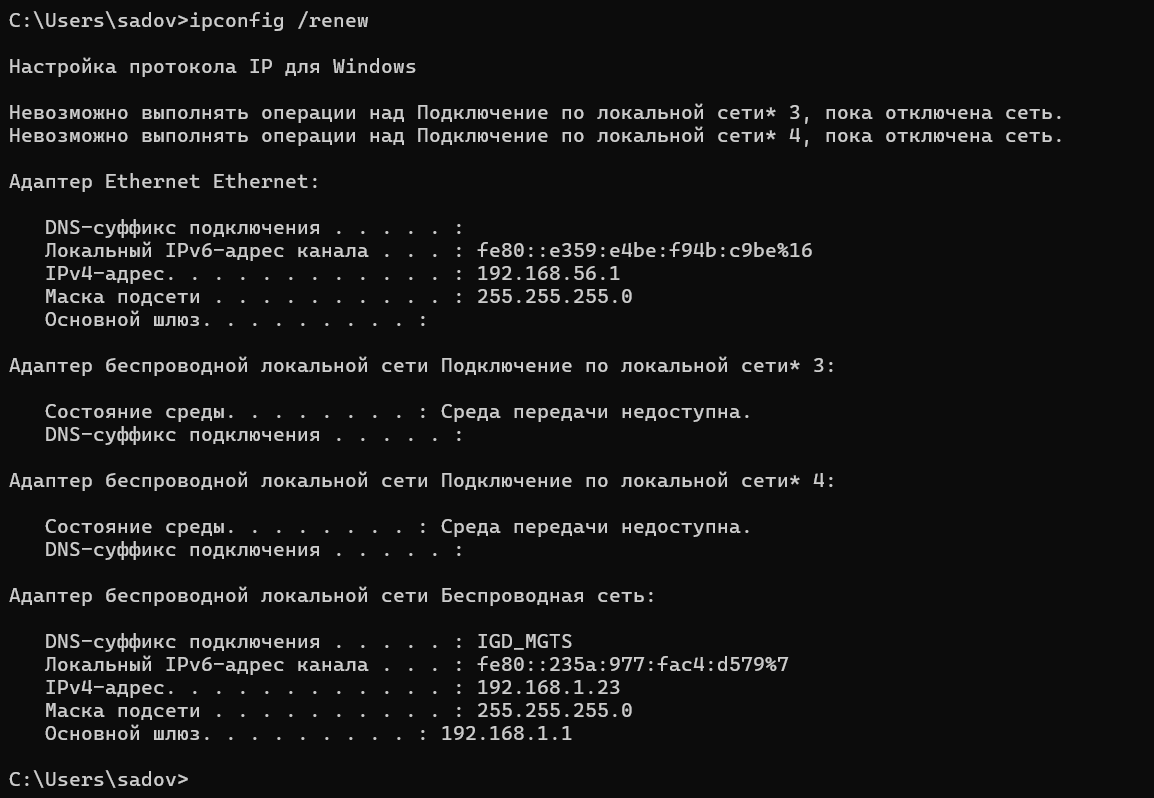


Рис. 4: Команда ipconfig /renew

Команда ipconfig /renew - обновляет IP текущего сетевого соединении

1. Определите MAC-адреса сетевых интерфейсов на вашем компьютере. Подтвердите свой ответ скриншотом.(рис. 5),(рис. 6)

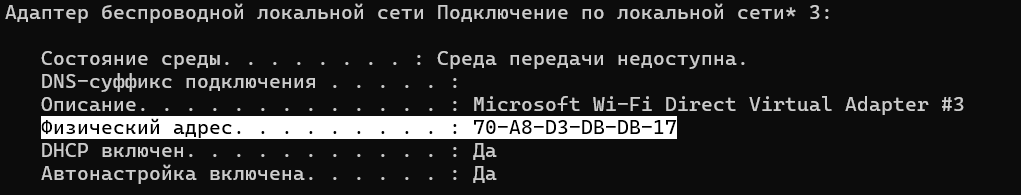


Рис. 5: MAC-адрес локальной сети \*3

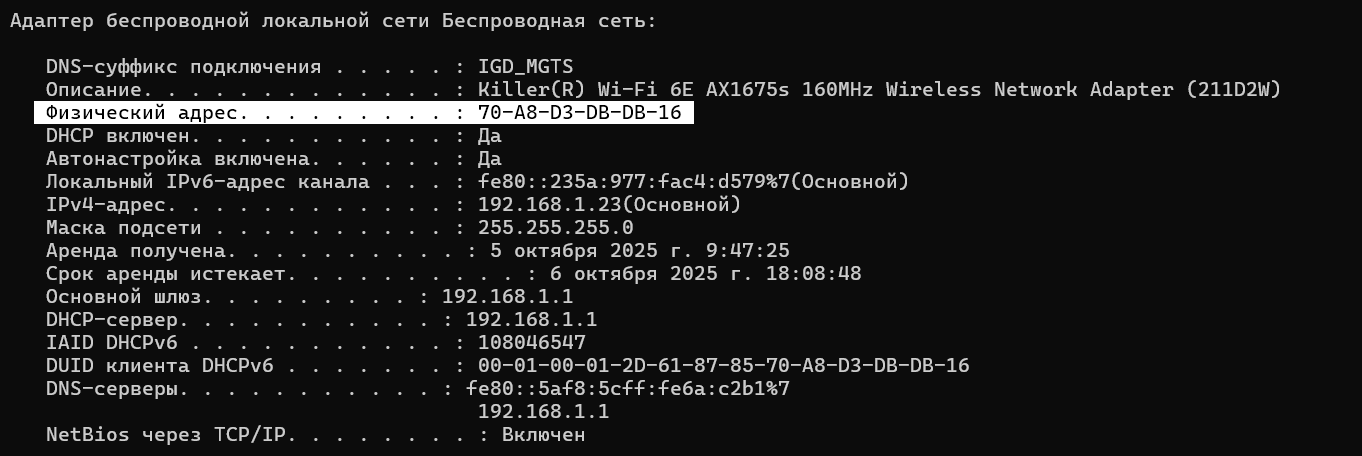


Рис. 6: MAC-адрес беспроводной сети

1. Опишите структуру MAC-адресов вашего устройства. Какая часть адреса идентифицирует производителя? Какая часть адреса идентифицирует сетевой интерфейс? Определите, каким является адрес — индивидуальным или групповым, глобально администрируемым или локально администрируемым. Поясните свой ответ. Используйте шестнадцатеричную запись MAC-адреса для пояснения.

Адрес 70:A8:D3:DB:DB:17 является индивидуальным (Unicast) и глобально администрируемым (UAA)

# 3 Анализ кадров канального уровня в Wireshark

## 3.1 Постановка задачи

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

## 3.2 Порядок выполнения работы

1. Установите на вашем устройстве Wireshark.
2. Запустите Wireshark. Выберите активный на вашем устройстве сетевой интерфейс. Убедитесь, что начался процесс захвата трафика.(рис. 7)

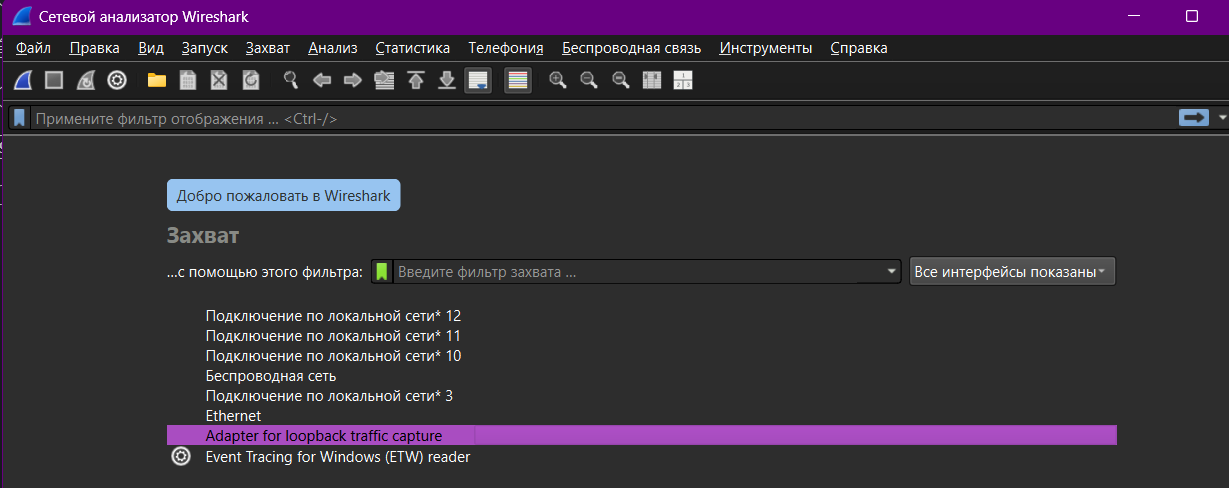


Рис. 7: Wireshark

1. На вашем устройстве в консоли определите с помощью команды ipconfig для ОС типа Windows или ifconfig для систем типа Linux IP-адрес вашего устройства и шлюз по умолчанию (default gateway).(рис. 8)

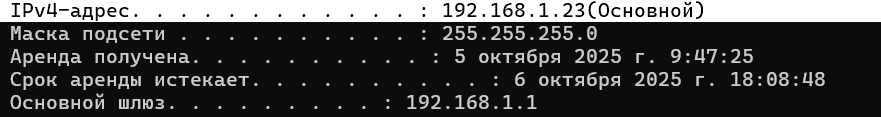


Рис. 8: IP-адрес и шлюз

1. На вашем устройстве в консоли с помощью команды ping адрес\_шлюза пропингуйте шлюз по умолчанию. Для остановки процесса используйте комбинацию клавиш Ctrl + c или изначально при помощи параметров команды ping задайте число сообщений эхо-запроса.(рис. 9)

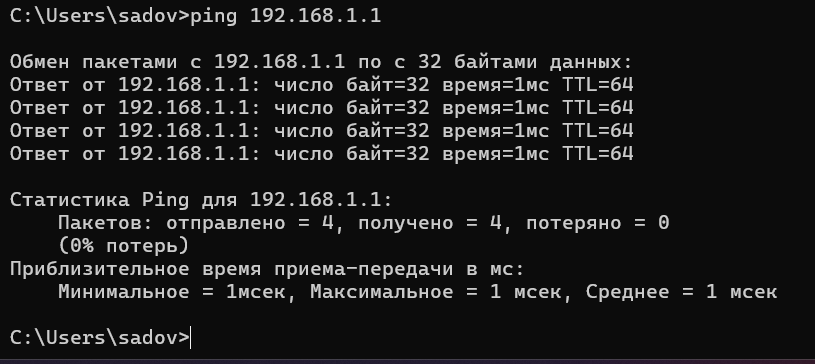


Рис. 9: пропингуем шлюз

1. В Wireshark остановите захват трафика. В строке фильтра пропишите фильтр arp or icmp. Убедитесь, что в списке пакетов отобразятся только пакеты ARP или ICMP, в частности пакеты, которые были сгенерированы с помощью команды ping, отправленной с вашего устройства на шлюз по умолчанию.(рис. 10),(рис. 11)

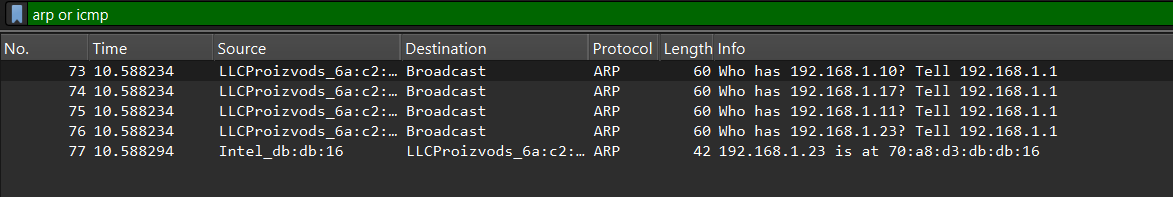


Рис. 10: Фильтр arp or icmp

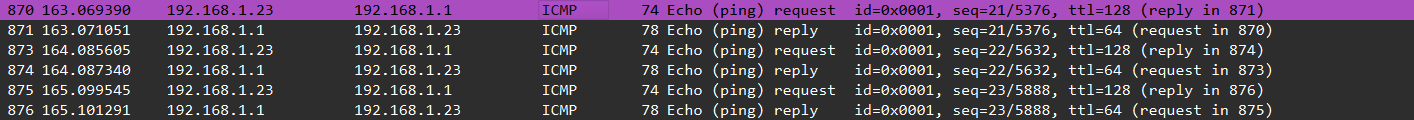


Рис. 11: пакеты что сгенерированы с помощью команды ping

1. Изучите эхо-запрос и эхо-ответ ICMP в программе Wireshark:

* На панели списка пакетов (верхний раздел) выберите первый указанный кадр ICMP — эхо-запрос. Изучите информацию на панели сведений о пакете в средней части экрана. В отчёте укажите длину кадра, к какому типу Ethernet относится кадр, определите MAC-адреса источника и шлюза, определите тип MAC-адресов.(рис. 12)

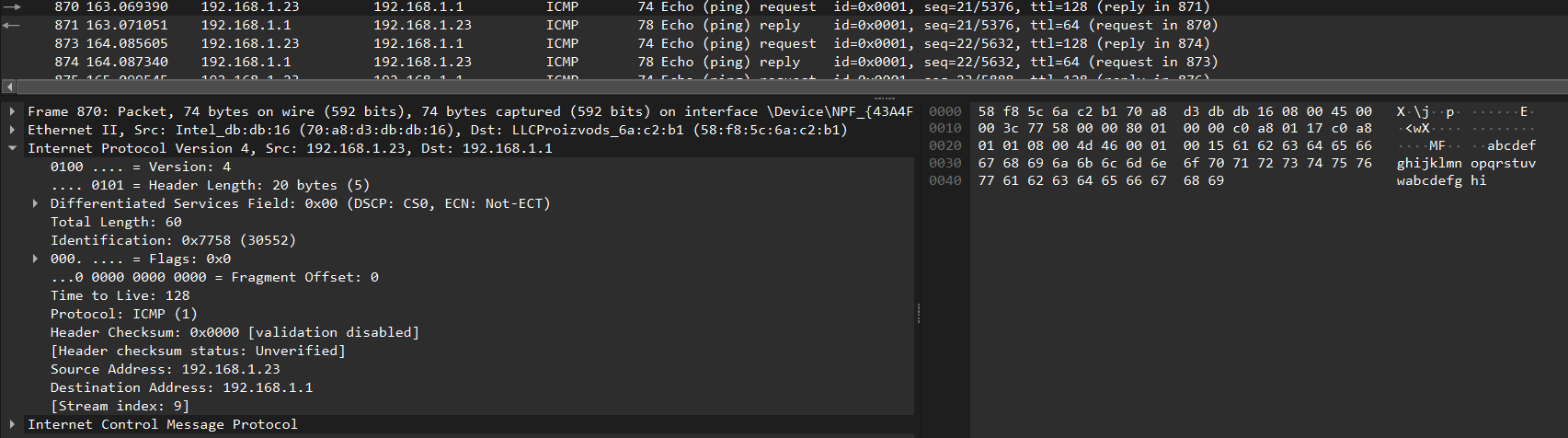


Рис. 12: ICMP — эхо-запрос

Длина кадра (Frame Length) - 74 байта

Типу Ethernet - Ethernet II

MAC-адреса источника - 70:a8:d3:db:db:16

Шлюз (Destination): MAC-адрес маршрутизатора (шлюза) с IP 192.168.1.1. Фактический MAC-адрес шлюза нужно посмотреть в захвате трафика Wireshark в поле “Destination” раздела “Ethernet II”. Например, это может быть адрес вида a4:b3:c2:d1:e0:f9.

Тип MAC-адресов:

* MAC-адрес источника (70:a8:d3:db:db:16): Индивидуальный (Unicast): Младший бит первого байта (70 = 01110000) равен 0. Глобально администрируемый (UAA): Второй младший бит первого байта равен 0.
* MAC-адрес назначения (шлюза a4:b3:c2:d1:e0:f9): Индивидуальный (Unicast): Младший бит первого байта (a4 = 10100100) равен 0. Глобально администрируемый (UAA): Второй младший бит первого байта равен 0.
* На панели списка пакетов (верхний раздел) выберите второй указанный кадр ICMP — эхо-ответ. Изучите информацию на панели сведений о пакете в средней части экрана. В отчёте укажите длину кадра, к какому типу Ethernet относится кадр, определите MAC-адреса источника и шлюза, определите тип MAC-адресов.(рис. 13)

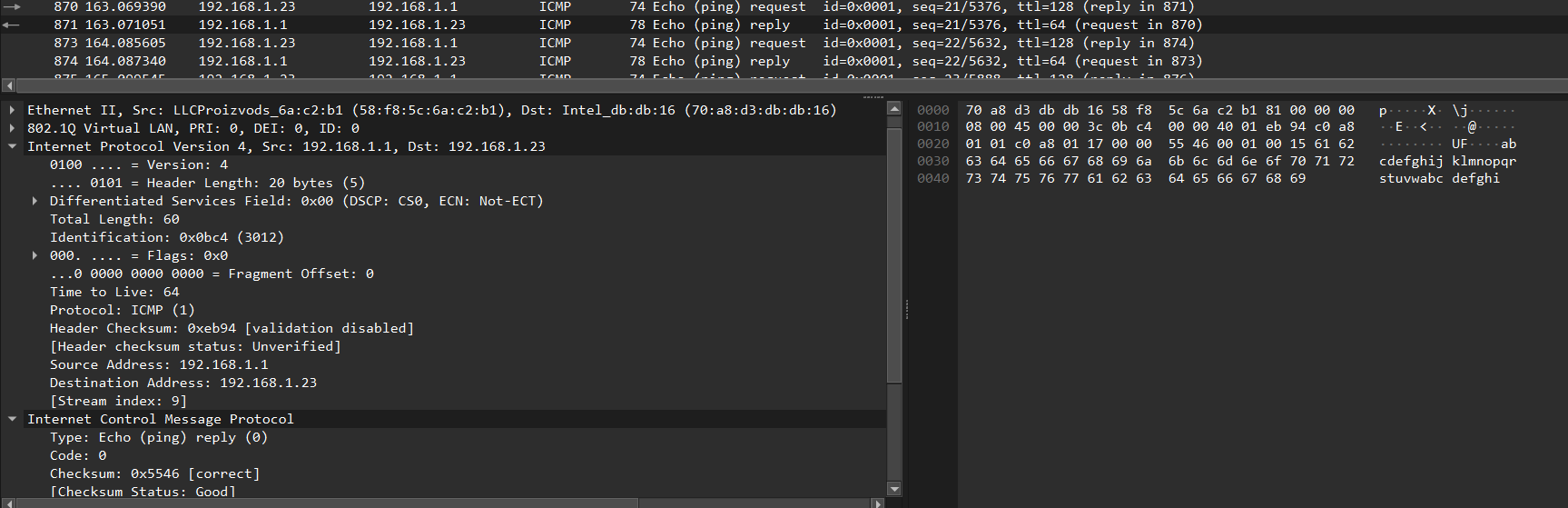


Рис. 13: ICMP — эхо-ответ

Длина кадра - 78 байт

Тип Ethernet - Ethernet II

MAC источника - 58:48:5c:6a:c2:b1

MAC назначения - 70:a8:d3:db:db:16

Тип адресов - Оба индивидуальные (Unicast) и глобальные (UAA)

1. Изучите кадры данных протокола ARP. Изучите данные в полях заголовка Ethernet II.(рис. 14)

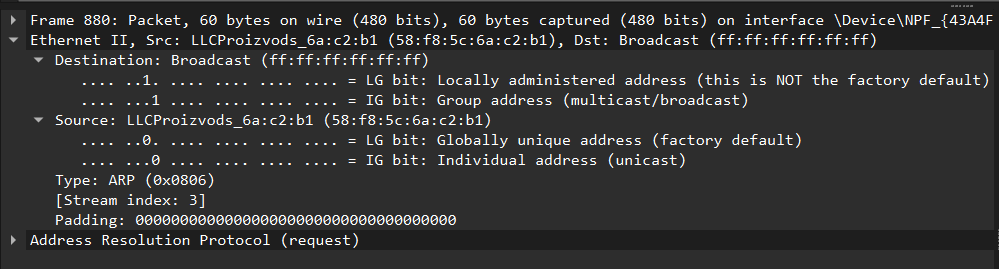


Рис. 14: Ethernet II

Длина кадра (Frame Length) - 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Типу Ethernet - Ethernet II

Broadcast ff:ff:ff:ff:ff:ff - Широковещательный адрес - кадр предназначен ВСЕМ устройствам в локальной сети

Source: LICProizvods\_6a:c2:b1 (58:f8:5c:6a:c2:b1)

MAC-адрес источника: 58:f8:5c:6a:c2:b1

Производитель: OUI 58:f8:5c соответствует производителю LICProizvods

Type: ARP (0x0806)

Stream index: 3 - Индекс потока для отслеживания связанных пакетов

1. Начните новый процесс захвата трафика в Wireshark. На вашем устройстве в консоли пропингуйте по имени какой-нибудь известный вам адрес, например ping rudn.ru.(рис. 15)

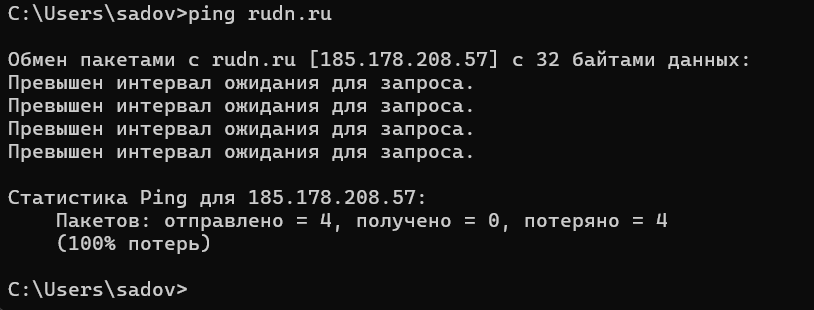


Рис. 15: Пропингуем rudn.ru

1. В Wireshark остановите захват трафика. Изучите запросы и ответы протоколов ARP и ICMP. Определите MAC-адреса источника и получателя, определите тип MAC-адресов.(рис. 16),(рис. 17),(рис. 18)

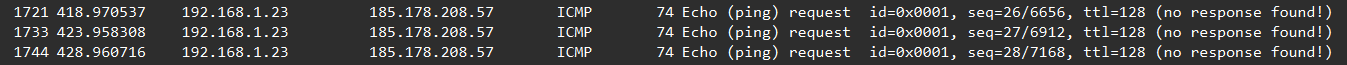


Рис. 16: Запросы и ответы

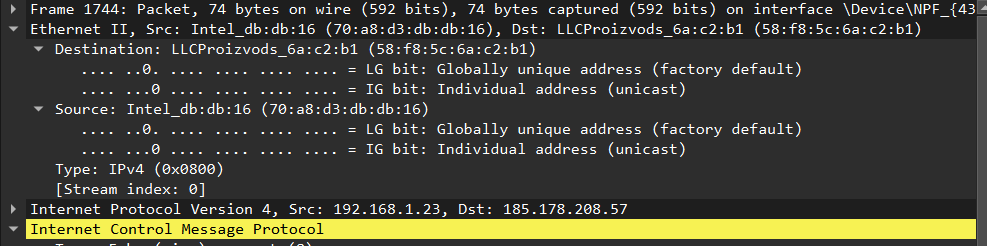


Рис. 17: эхо-запрос

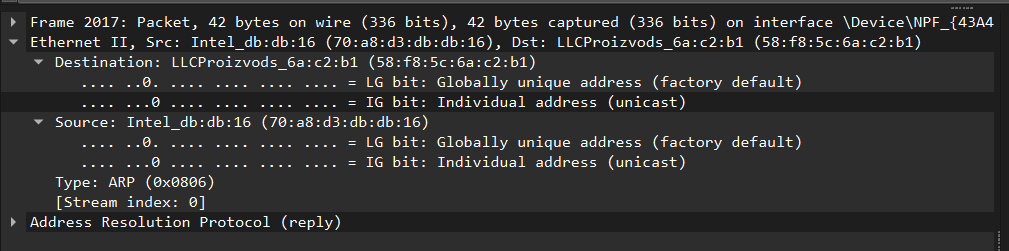


Рис. 18: эхо-ответ

ARP Request (запрос)

MAC-адреса:

Источник (Source): 58:f8:5c:6a:c2:b1

* Тип: Индивидуальный (Unicast)
* Администрирование: Глобальное (UAA)

Получатель (Destination): ff:ff:ff:ff:ff:ff

* Тип: Групповой (Broadcast)
* Администрирование: Широковещательный адрес

ARP Reply (ответ)

MAC-адреса:

Источник (Source): 70:a8:d3:db:db:16

* Тип: Индивидуальный (Unicast)
* Администрирование: Глобальное (UAA)

Получатель (Destination): 58:f8:5c:6a:c2:b1

* Тип: Индивидуальный (Unicast)
* Администрирование: Глобальное (UAA)

# 4 Анализ протоколов транспортного уровня в Wireshark

## 4.1 Постановка задачи

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

## 4.2 Порядок выполнения работы

1. Запустите Wireshark. Выберите активный на вашем устройстве сетевой интерфейс. Убедитесь, что начался процесс захвата трафика.
2. На вашем устройстве в браузере перейдите на сайт, работающий по протоколу HTTP (например, на сайт CERN http://info.cern.ch/). При необходимости получения большей информации для Wireshark поперемещайтесь по ссылкам или разделам сайта в браузере.(рис. 19)

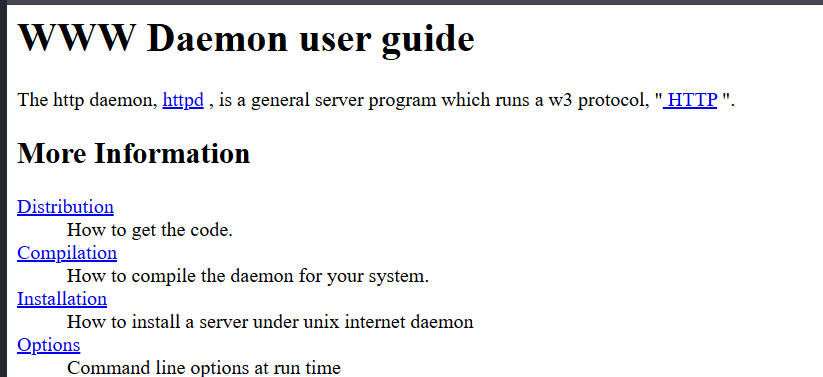


Рис. 19: Сайт http://info.cern.ch/

1. В Wireshark в строке фильтра укажите http и проанализируйте информацию по протоколу TCP в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.(рис. 20),(рис. 21),

Наш фильтор

Рис. 20: Наш фильтор

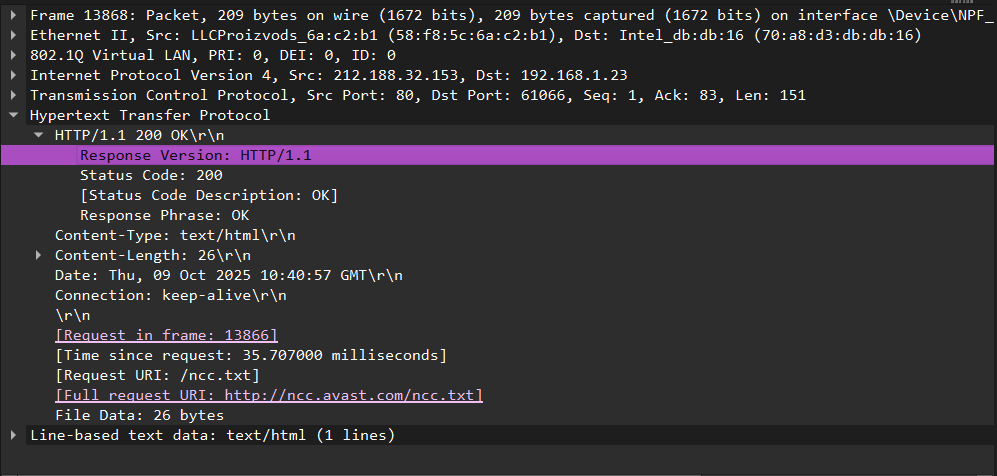


Рис. 21: Информация

Анализ уровня приложений (HTTP):

Статус: 200 OK - успешное выполнение запроса

Версия протокола: HTTP/1.1

Тип содержимого: text/html

Размер содержимого: 26 bytes

Cоединение: keep-alive (повторное использование TCP-соединения)

Контекст запроса:

Запрос был в кадре: 13866

Время обработки: 35.707 ms - быстрый ответ сервера

Запрашиваемый ресурс: /ncc.txt

Полный URL: http://ncc.avast.com/ncc.txt

Сервер: Сервер компании Avast (антивирусное ПО)

1. Wireshark в строке фильтра укажите dns и проанализируйте информацию по протоколу UDP в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.(рис. 22),(рис. 23)

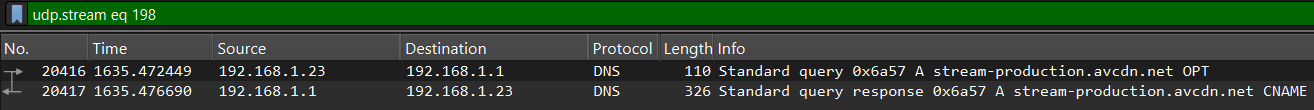


Рис. 22: эхо-запрос и эхо-ответ

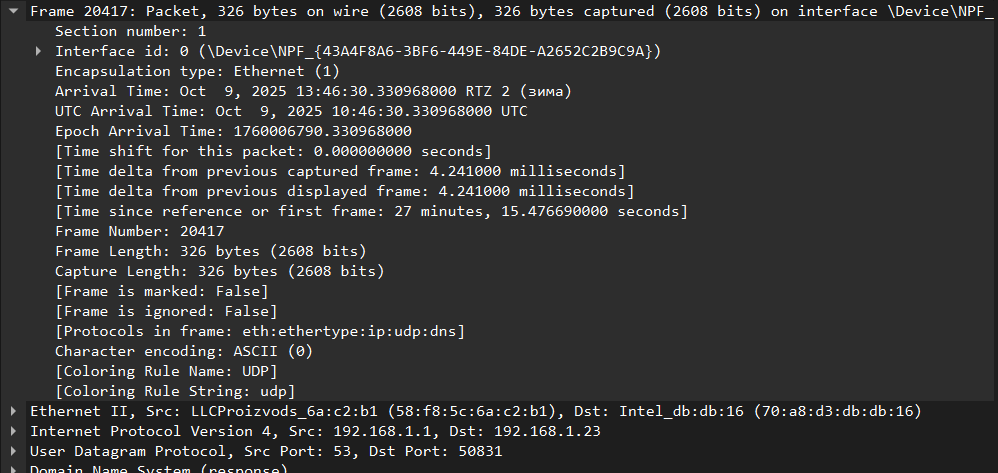


Рис. 23: Информация

Анализ пакета

Номер кадра: 20417

Длина кадра: 326 байт

Протоколы в кадре: eth:ethertype:ip:udp:dns

Источник: 192.168.1.1 (вероятно, локальный DNS-сервер или маршрутизатор)

Назначение: 192.168.1.23 (клиентское устройство)

Порты:

* Src Port: 53 (стандартный порт DNS-сервера)
* Dst Port: 50831 (порт клиента, с которого был отправлен запрос)

1. Wireshark в строке фильтра укажите quic и проанализируйте информацию по протоколу quic в случае запросов и ответов. В отчёте приведите пояснение по информации, захваченной в Wireshark.(рис. 24),(рис. 25)

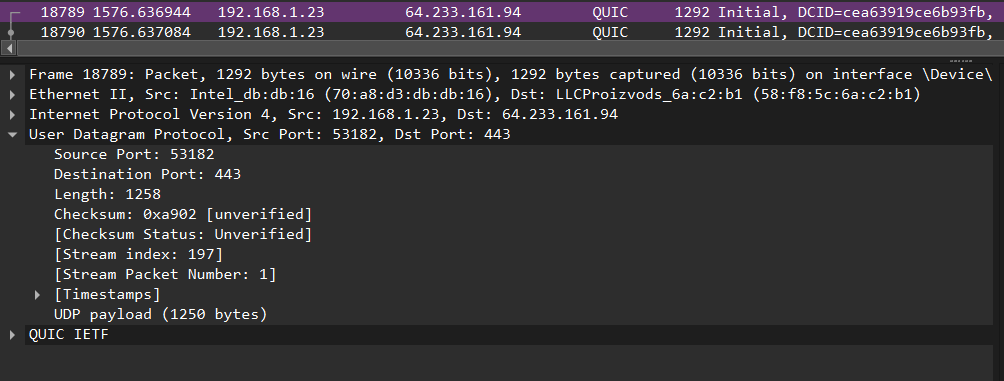


Рис. 24: эхо-запрос

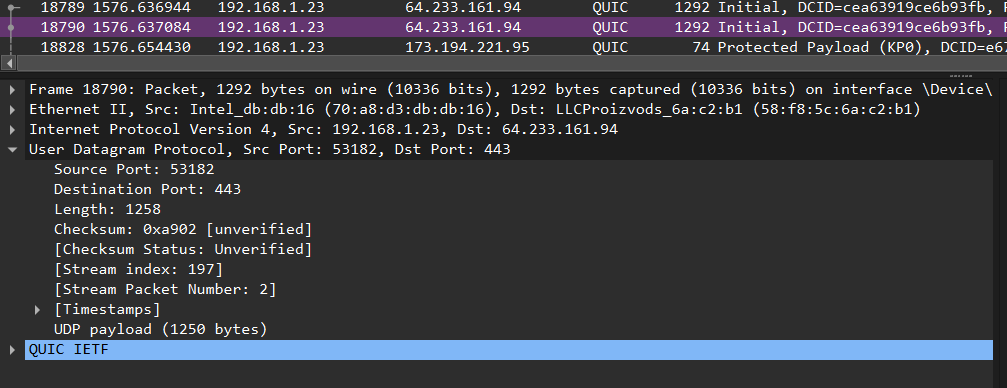


Рис. 25: эхо-ответ

Анализ пакета

Номер кадра: 18790

Время: 1576.637084 секунд от начала захвата

Источник: 192.168.1.23 (клиент)

Назначение: 64.233.161.94 (сервер, принадлежит Google)

Порты:

* Src Port: 53182 (клиентский)
* Dst Port: 443 (HTTPS/QUIC)

Длина UDP-датаграммы: 1258 байт

Протоколы в кадре: eth:ip:udp:quic

1. Остановите захват трафика в Wireshark.

# 5 Анализ handshake протокола TCP в Wireshark

## 5.1 Постановка задачи

С помощью Wireshark проанализировать handshake протокола TCP.

## 5.2 Порядок выполнения работы

1. Запустите Wireshark. Выберите активный на вашем устройстве сетевой интерфейс. Убедитесь, что начался процесс захвата трафика.
2. На вашем устройстве или используйте подсоединение по telnet или ssh к вашему маршрутизатору (например с помощью PUTTY или соответствующих команд в консоли), или соединение по HTTP с каким-то сайтом для захвата в Wireshark пакетов TCP.

Для работы с telnet нужно в консоле ее отдельно подключить. На версиях Windows 10/11 эта команда отключена. Ее можно обратно влючить зайдя в настройки устройсктва в раздел с подключением дополнительных параметров. После подключения, мне не потребовалось обновлять коомпьютер и я продолжила работу в терменале.

1. В Wireshark проанализируйте handshake протокола TCP, в отчёте приведите пример с пояснениями изменения значений соответствующих сообщений при установлении соединения по TCP.(рис. 26)

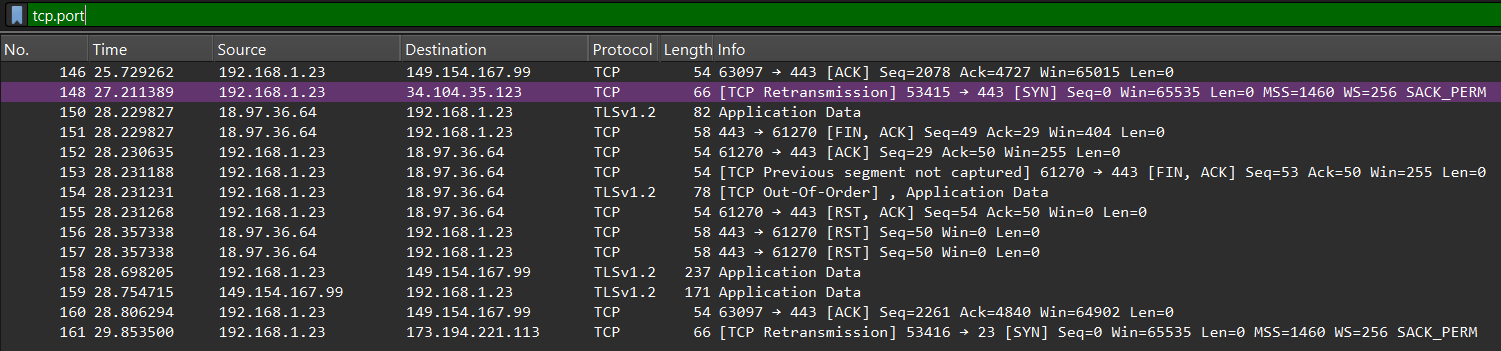


Рис. 26: Запускаем фильтор с протоколом TCP

1. В Wireshark в меню «Статистика» выберете «График Потока». В отчёте приведите пояснения по изменениям значений соответствующих сообщений при установлении соединения по TCP.(рис. 27)

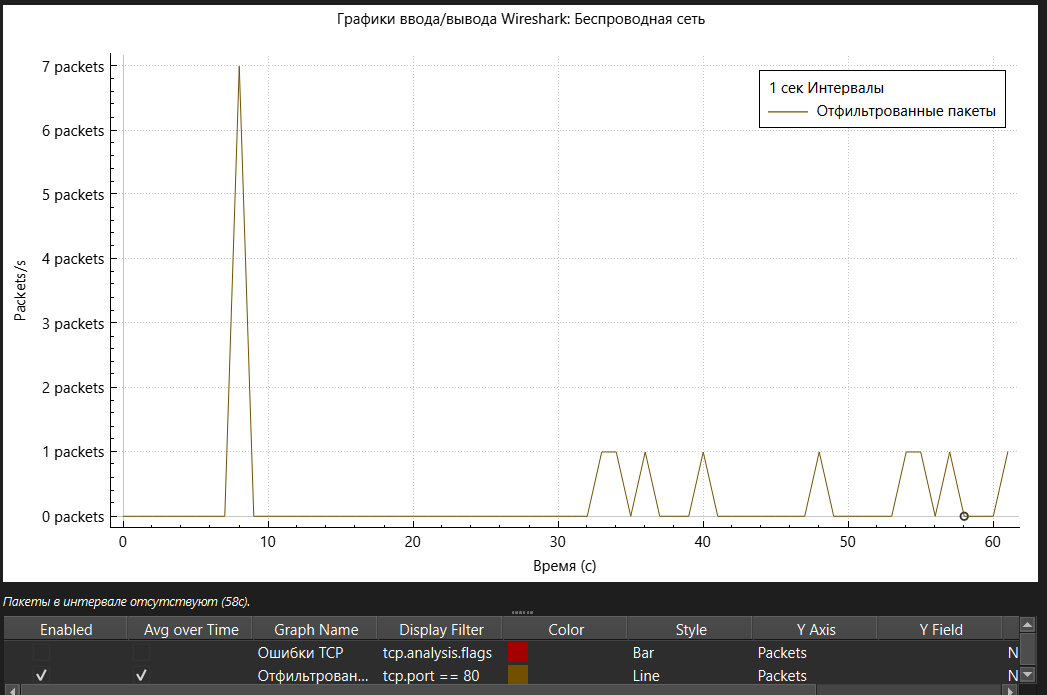


Рис. 27: График порта 80

На участке “Пакеты в интервале отсутствуют (58с)” оба графика падают до нуля, что означает полное отсутствие TCP-трафика (включая ошибки) на порту 80 в течение 58 секунд.

После третьего пакета соединение установлено.

Анализируя Graph Flow, вы можете четко видеть всю жизненную цепочку TCP-сессии: от установления соединения (рукопожатие), через передачу данных с постоянно растущими номерами подтверждений (Ack), до корректного завершения соединения (обмен пакетами FIN/ACK).

1. Остановите захват трафика в Wireshark.

# 6 Выводы

Изучили с помощью Wireshark кадры Ethernet, анализ PDU протоколов транспортного и прикладного уровней стека TCP/IP. Поработали с простейшими командами и фильтрами. Разобрались в выводимой информации Wireshark.

# Список литературы