Лабораторная работа №3

Анализ трафика в Wireshark

Демидова Екатерина Алексеевна

Содержание

# 1 Цель работы

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

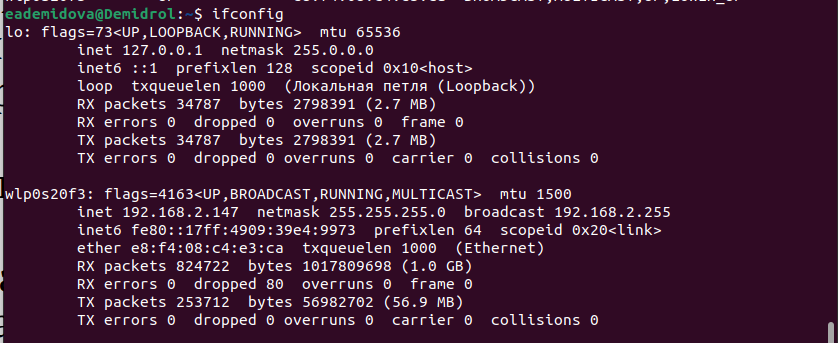
# 2 Задание

1. MAC-адресация
   1. Изучение возможностей команды ipconfig для ОС типа Windows (ifconfig для систем типа Linux).
   2. Определение MAC-адреса устройства и его типа.
2. Анализ кадров канального уровня в Wireshark
   1. Установить на домашнем устройстве Wireshark.
   2. С помощью Wireshark захватить и проанализировать пакеты ARP и ICMP в части кадров канального уровня
3. Анализ протоколов транспортного уровня в Wireshark. С помощью Wireshark захватить и проанализировать пакеты HTTP, DNS в части заголовков и информации протоколов TCP, UDP, QUIC.
4. Анализ handshake протокола TCP в Wireshark.С помощью Wireshark проанализировать handshake протокола TCP.

# 3 Выполнение лабораторной работы

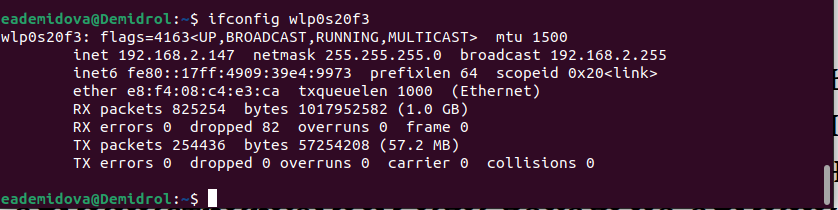
## 3.1 MAC-адресация

С помощью команды ifconfig выведем информацию о текущем сетевом соединении (рис. ??).



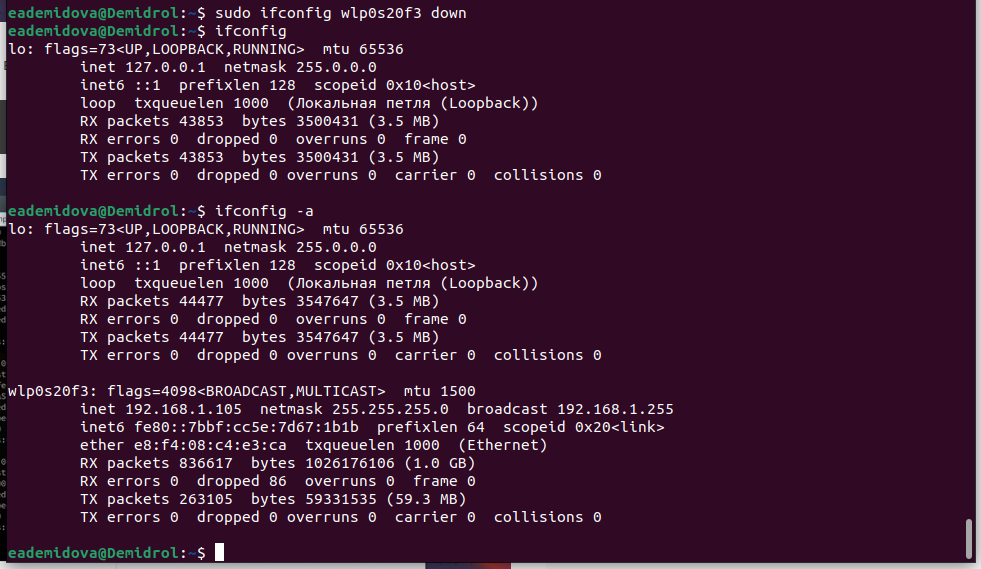
Вывод команды ifconfig

Так же добавив название сетевого интерфейса можно вывести информацию только о нём(рис. ??).



Вывод информации о конкретном сетевом интерфейсе`

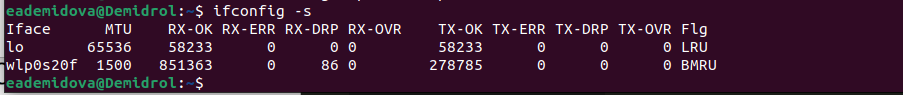
Теперь выключим сетевой интерфейс добавив команду down(с помощью командыup его можно включить). При использовании команды ifconfig его не видно, так как это сетевое соединение больше не активно, но можно использовать опцию -a, которая показывает все сетевые интерфейсы, даже не активные(рис. ??).



Выключение сетевого интерфейса и демонстрация опции -a

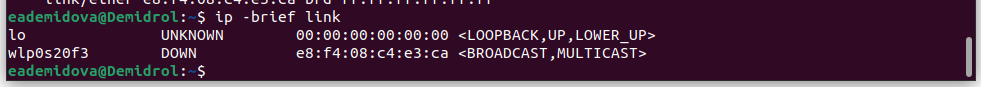
Также можно использовать опцию -s, с помощью которой выводится краткий список интерфейсов(рис. ??). При таком выводе можно увидеть информацию только о следующих параметрах:

* MTU – Максимальное число байтов в пакете
* RX-OK – Пакеты, принятые без ошибок
* RX-ERR – Пакеты, принятые с ошибками
* RX-DRR – Пропавшие пакеты
* RX-OVR – Ошибки из-за превышения скорости
* TX-OK – Пакеты, переданные без ошибок
* TX-ERR – Пакеты, переданные с ошибками
* TZ-DRR – Пакеты, потерянные при передаче
* TX-OVR – Пакеты, которые не смогли передать
* Flags – Характеристики интерфейса
  + A – принимает пакеты в случае многоадресной передачи
  + B – принимает широковещательные пакеты
  + D – отладка включена
  + L – закольцовывающий интерфейс
  + M – изменяется динамически (переадресация)
  + N – без обработки завершителей пакетов
  + O – протокол преобразования адресов выключен
  + P – интерфейс “точка-точка”
  + R – интерфейс работает
  + U – интерфейс активизирован



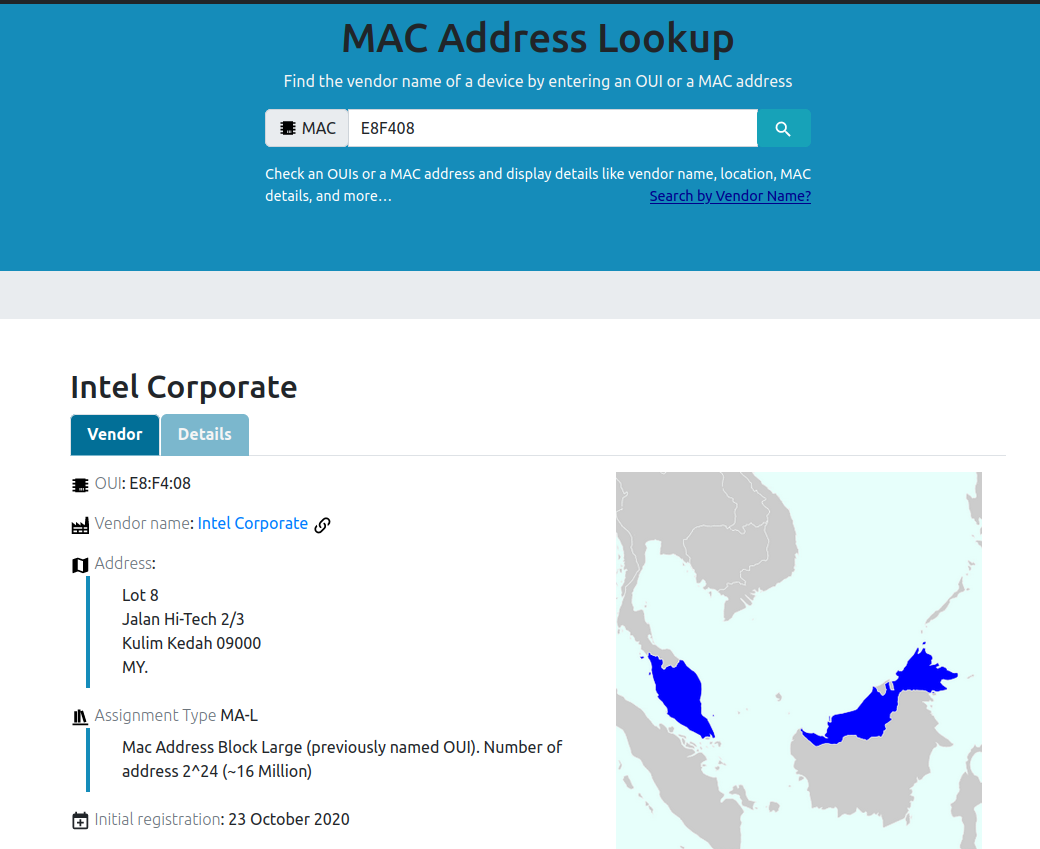
Использование опции -s

MAC-адрес сетевого интерфейса можно увидеть так же с помощью команды ifconfig, посмотрев на поле ether, но MAC-адрес виртуального интерфейса не показывается. Можно использовать команду ip -brief link, чтобы увидеть только MAC-адреса (рис. ??). Видно, что у виртуального интерфейса все биты в нуле, а у второго сетевого интерфейса MAC-адрес - e8:f4:08:c4:e3:ca.



Демонстрация MAC-адреса

Первые три байта e8:f4:08 в этом адресе соответствуют индентификатору производителя, в Интернете можно найти, какой компании соответствует этот индентификатор(рис. ??). Последние три байта c4:e3:ca индентифицируют сетевой интерфейс.

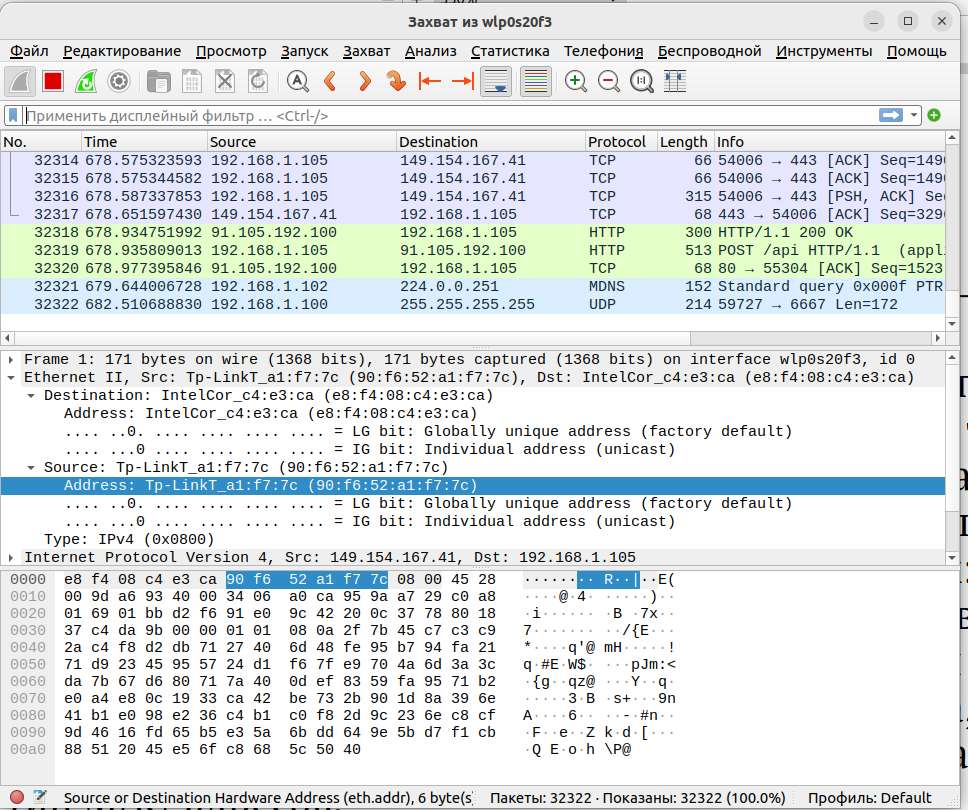


Демонстрация производителя сетевого оборудования

Возьмем первый байт e8 и переведём его в двоичную систему. Получим 11101000. Так как последний бит ноль, то адрес является индивидуальным. А так как предпоследний бит ноль, то адрес глобально администрируемый.

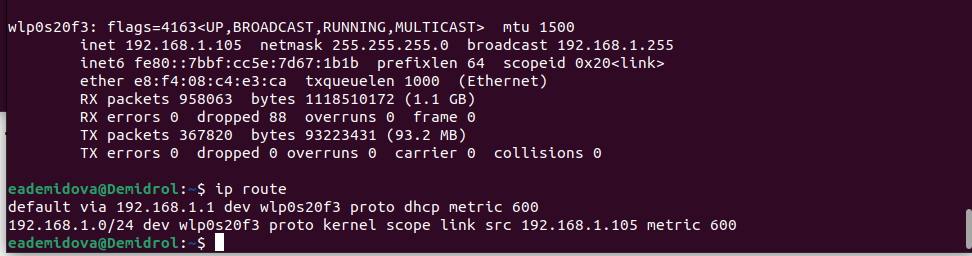
## 3.2 Анализ кадров канального уровня в Wireshark

Запустим wireshark и начнем захват трафика (рис. ??).



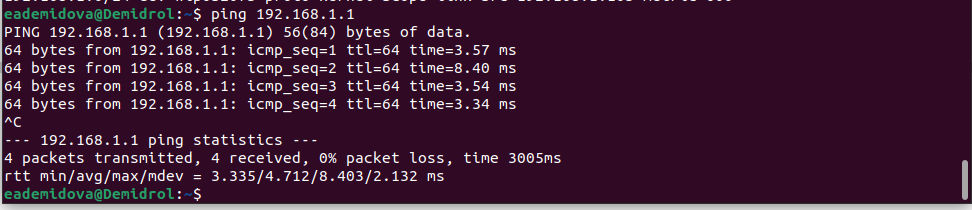
Захват трафика в wireshark

С помощью команды ifconfig определим IP-адрес устройства – 192.168.1.105. Шлюз по умолчанию на моём устройстве не отображается с помощью этой команды, поэтому я использовала также команду ip route, шлюз по умолчанию – 192.168.1.1(рис. ??).



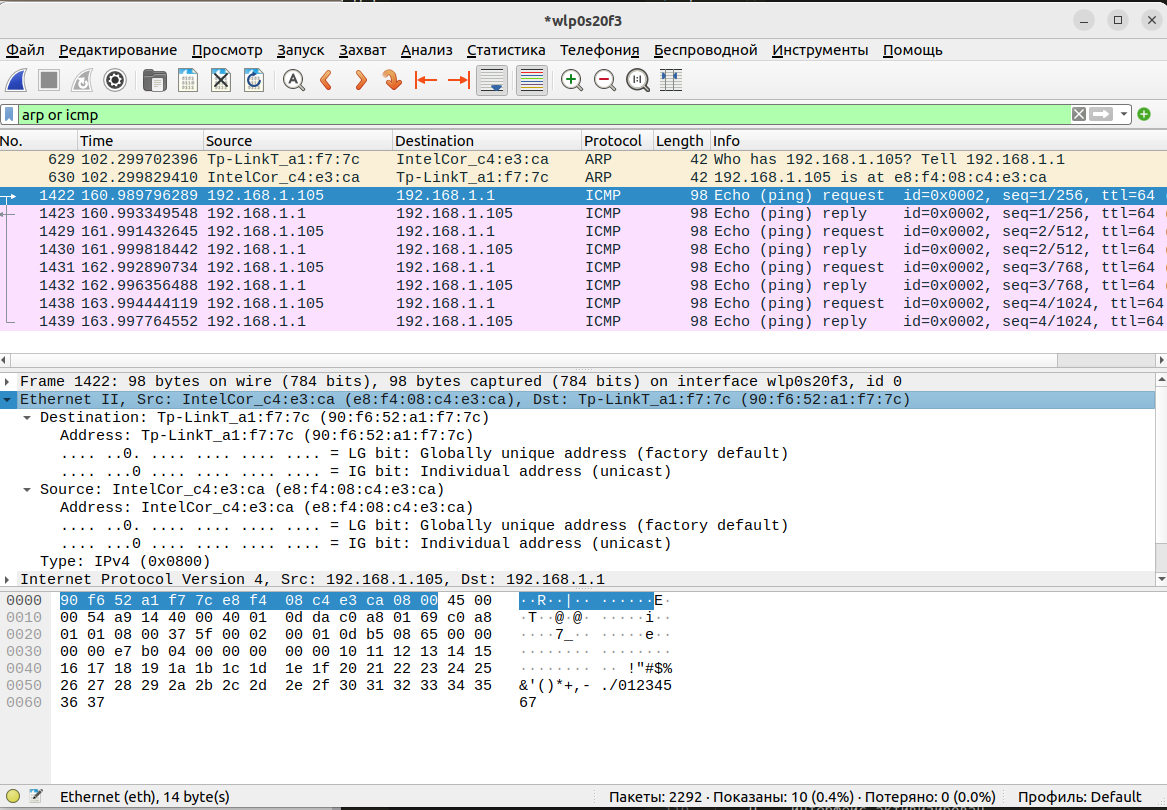
Определение IP-адреса устройства и шлюза по умолчанию

С помощью команды ping 192.168.1.1 пропингуем шлюз по умолчанию (рис. ??).



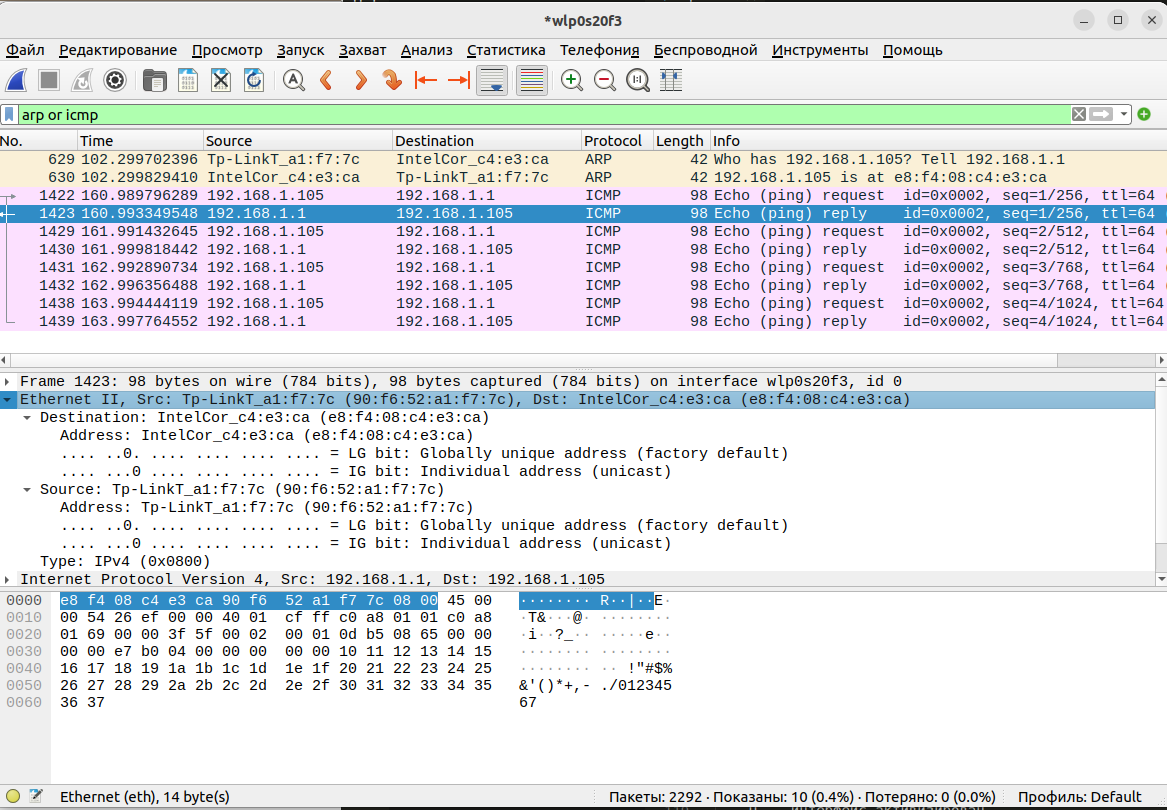
Пингование шлюза по умолчанию

Затем остановим захват трафика wireshark и пропишем фильтр arp or icmp. В списке пакетов отобразились только пакеты ARP и ICMP, в частности пакеты, которые были сгенерированы с помощью команды ping (рис. ??). Изучим эхо-запрос и эхо-ответ ICMP в программе Wireshark. На панели списка пакетов (верхний раздел) выберем первый указанный кадр ICMP — эхо-запрос (??). Изучим информацию на панели сведений о пакете в средней части экрана. Длинf кадра равняется 98 байт, заголовок Ethernet первые 14 байт кадра, кадр относится к типу Ethernet II. MAC-адрес шлюза – это первые 6 байт заголовка Ethernet, а MAC-адрес источника – следующие 6 байт заголовка Ethernet, оба MAC-адреса являются индивидуальными и глобально администрируемыми.



Кадр ICMP - эхо-запрос

На панели списка пакетов (верхний раздел) выберем второй указанный кадр ICMP — эхо-ответ (??). Изучим информацию на панели сведений о пакете в средней части экрана. Длинf кадра равняется 98 байт, заголовок Ethernet первые 14 байт кадра, кадр относится к типу Ethernet II. MAC-адрес пункта назначения – это первые 6 байт заголовка Ethernet, а MAC-адрес шлюза(источника) - следующие 6 байт заголовка Ethernet, оба MAC-адреса являются индивидуальными и глобально администрируемыми.



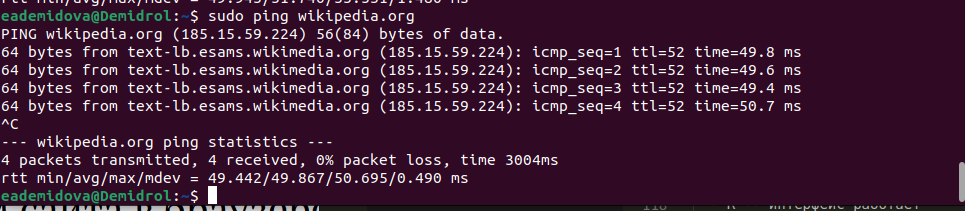
Кадр ICMP - эхо-ответ

На панели списка пакетов (верхний раздел) выберем второй указанный кадр ARP (??). Изучим информацию на панели сведений о пакете в средней части экрана. Длинf кадра равняется 42 байтf, заголовок Ethernet первые 14 байт кадра, кадр относится к типу Ethernet II. MAC-адрес пункта назначения – это первые 6 байт заголовка Ethernet, а MAC-адрес источника - следующие 6 байт заголовка Ethernet, оба MAC-адреса являются индивидуальными и глобально администрируемыми. Также в заголовке Ethernet последние два байта обозначают вложенным пакет типа ARP.



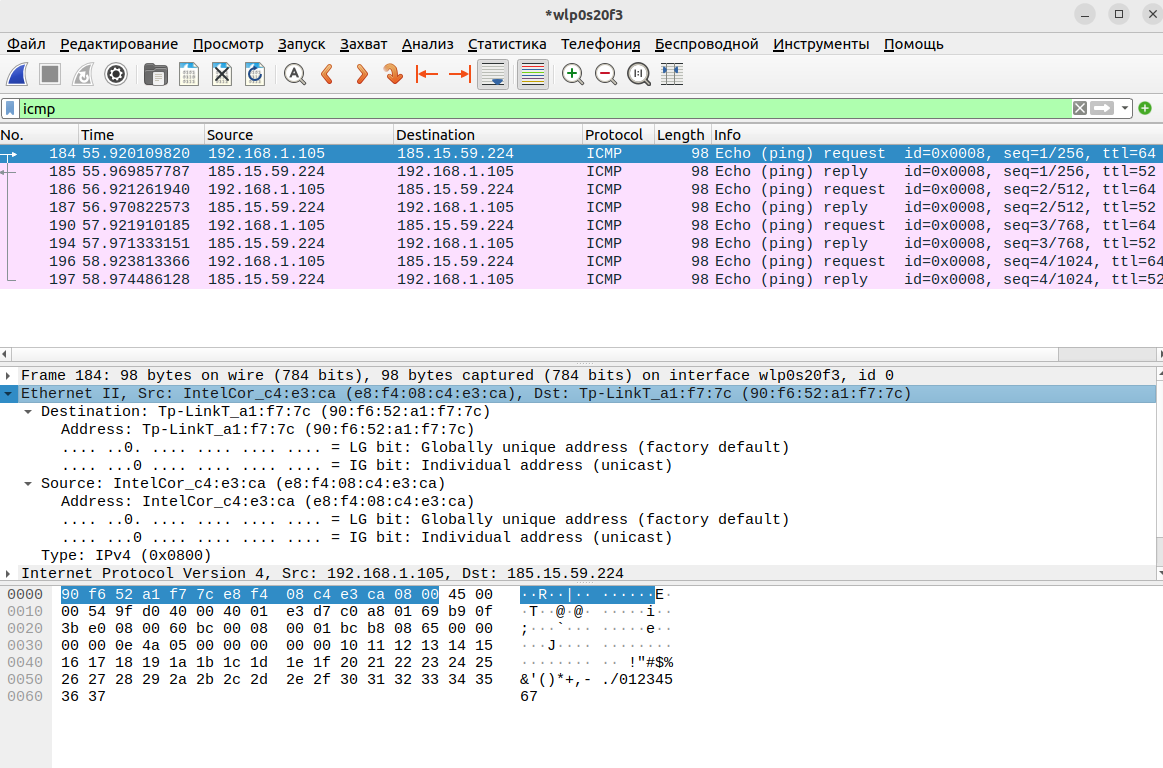
Кадр ARP

Теперь начнём новый процесс захвата трафика и пропингуем сайт wikipedia.org (??).

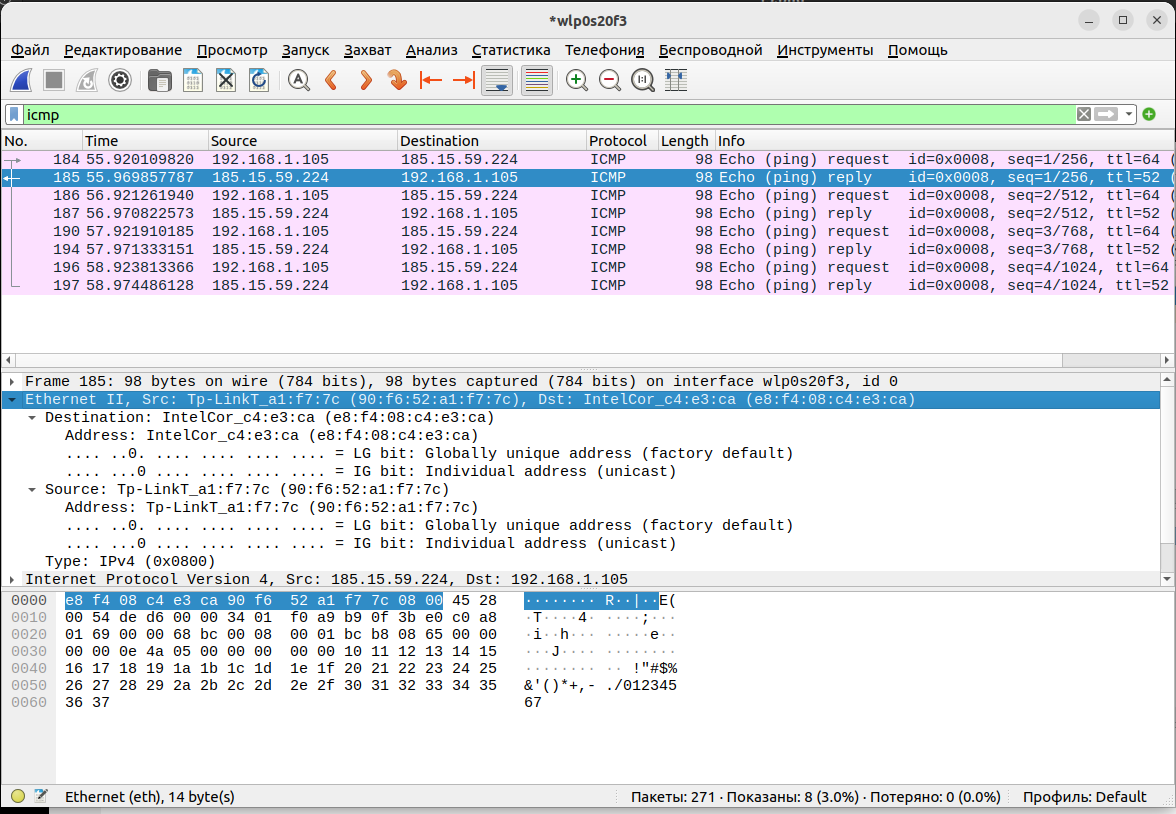


Пингование сайта wikipedia.org

Изучим эхо-запрос и эхо-ответ ICMP в программе Wireshark (??, ??). Изучим информацию на панели сведений о пакете в средней части экрана. В обоих случаях длина кадра равняется 98 байт, заголовок Ethernet первые 14 байт кадра и кадр относится к типу Ethernet II. В случае эхо-запроса точка назначения – сайт, а источник – сетевой интерфейс моего устройства, в случае же эхо-ответа – наоборот. 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.

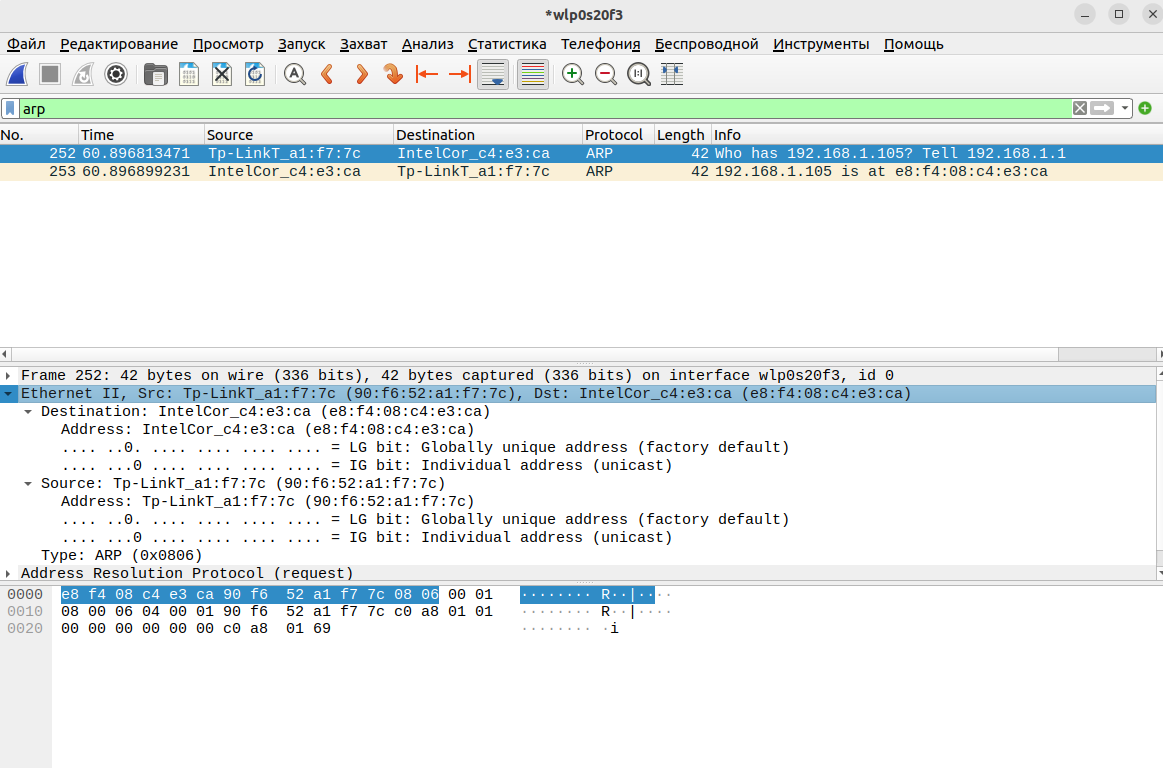


Пингование сайта wikipedia.org. Кадр ICMP - эхо-запрос

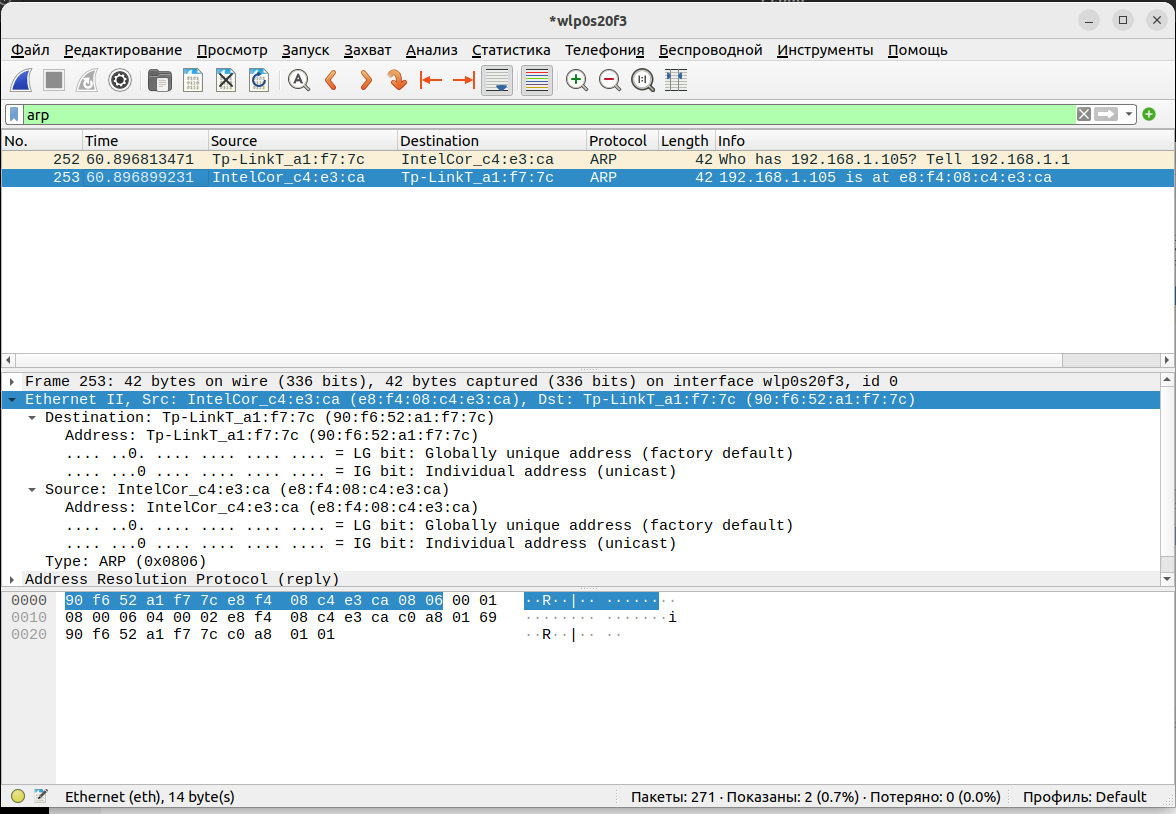


Пингование сайта wikipedia.org. Кадр ICMP - эхо-ответ

Изучим запрос и ответ ARP в программе Wireshark(??,??). Изучим информацию на панели сведений о пакете в средней части экрана. В обоих случаях длина кадра равняется 42 байтf, заголовок Ethernet первые 14 байт кадра и кадр относится к типу Ethernet II. В случае запроса точка назначения – сетевой интерфейс оборудования, а источник – шлюз по умолчанию, в случае же эхо-ответа – наоборот, эхо-ответ сообщает шлюзу по умолчанию MAC-адрес сетевого интерфейса. 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.



Пингование сайта wikipedia.org. Кадр ARP - запрос

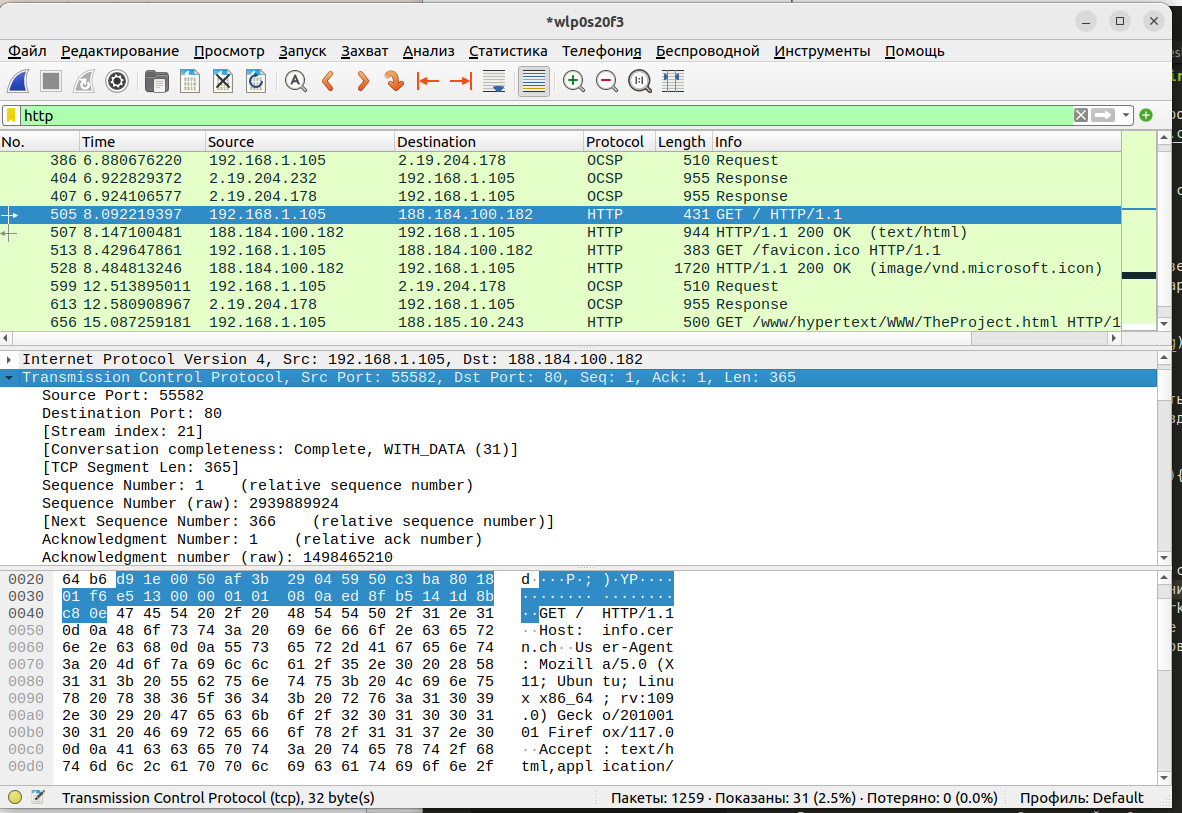


Пингование сайта wikipedia.org. Кадр ARP - ответ

## 3.3 Анализ протоколов транспортного уровня в Wireshark

В браузере перейдем на сайт, работающий по протоколу HTTP, а именно на сайт CERN http://info.cern.ch/. Поперемещаемся по ссылкам и разделам сайта. В Wireshark в строке фильтра укажим http и проанализируем информацию по протоколу TCP в случае запросов и ответов.

Порт источника задан случайно, выбором из непривелигированных и незанятых портов, и равен 555882, порт назначения равен 80 - это стандартный порт HTTP(??).

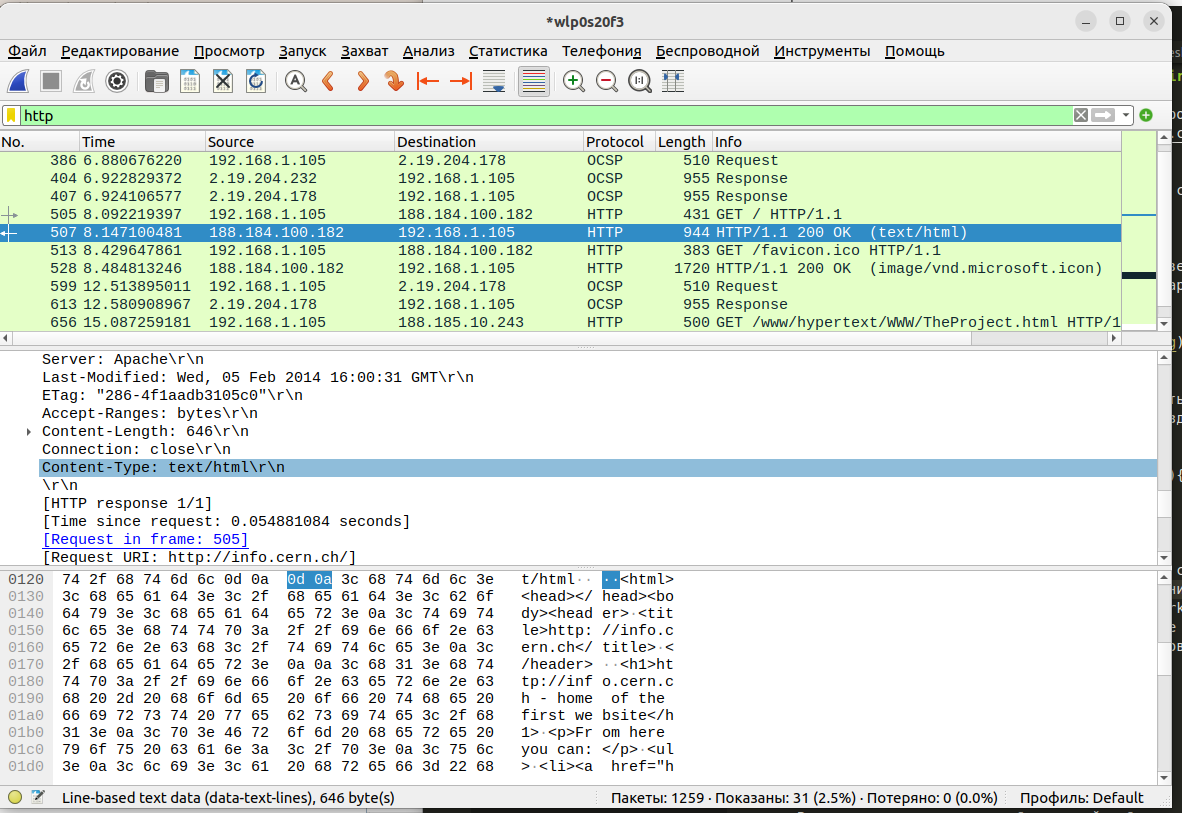


Запрос HTTP по протоколу TCP

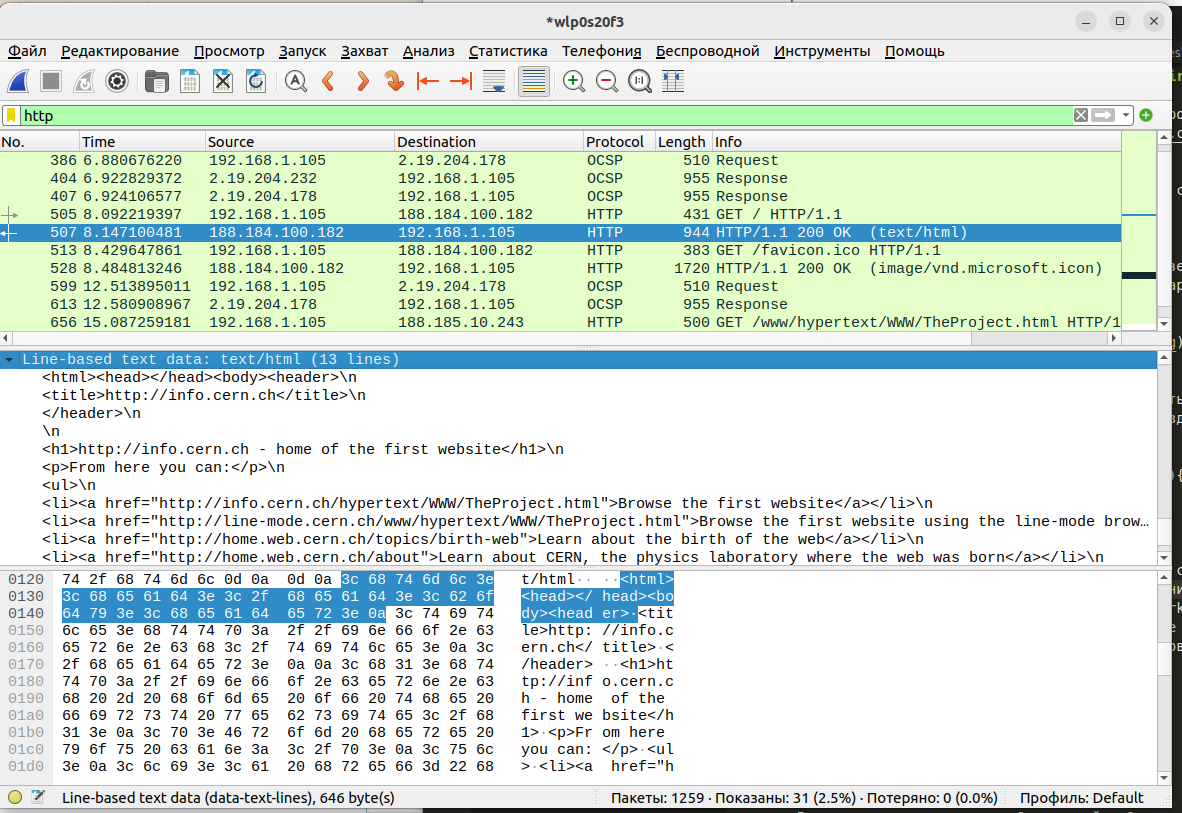
В случае ответа порты заданы наоборот, то есть источник - 80 порт, назначение - 55582 (??). В разделе HTP можно увидеть ссылку на html-страницу(??). А в разделе Line-based text data находится содержимое страницы, которую перехватил wireshark(??).



Ответ HTTP по протоколу TCP

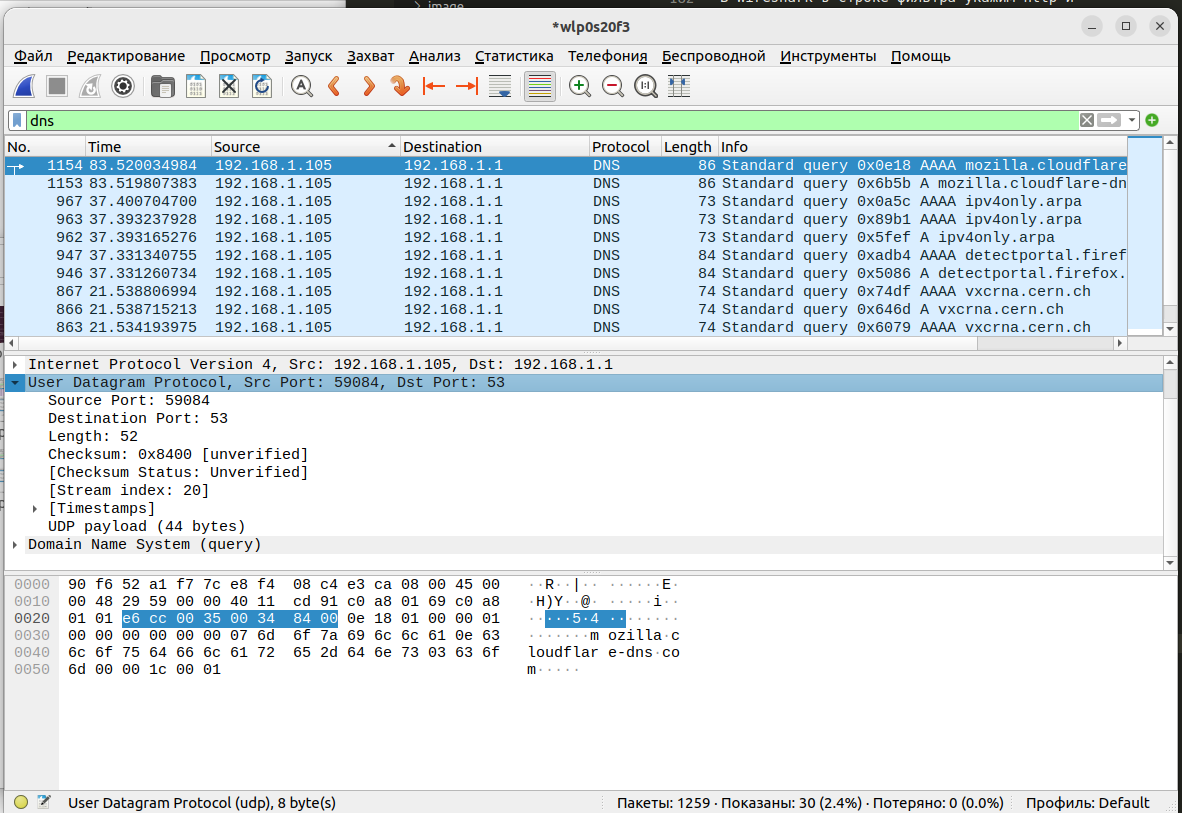


Раздел HTP



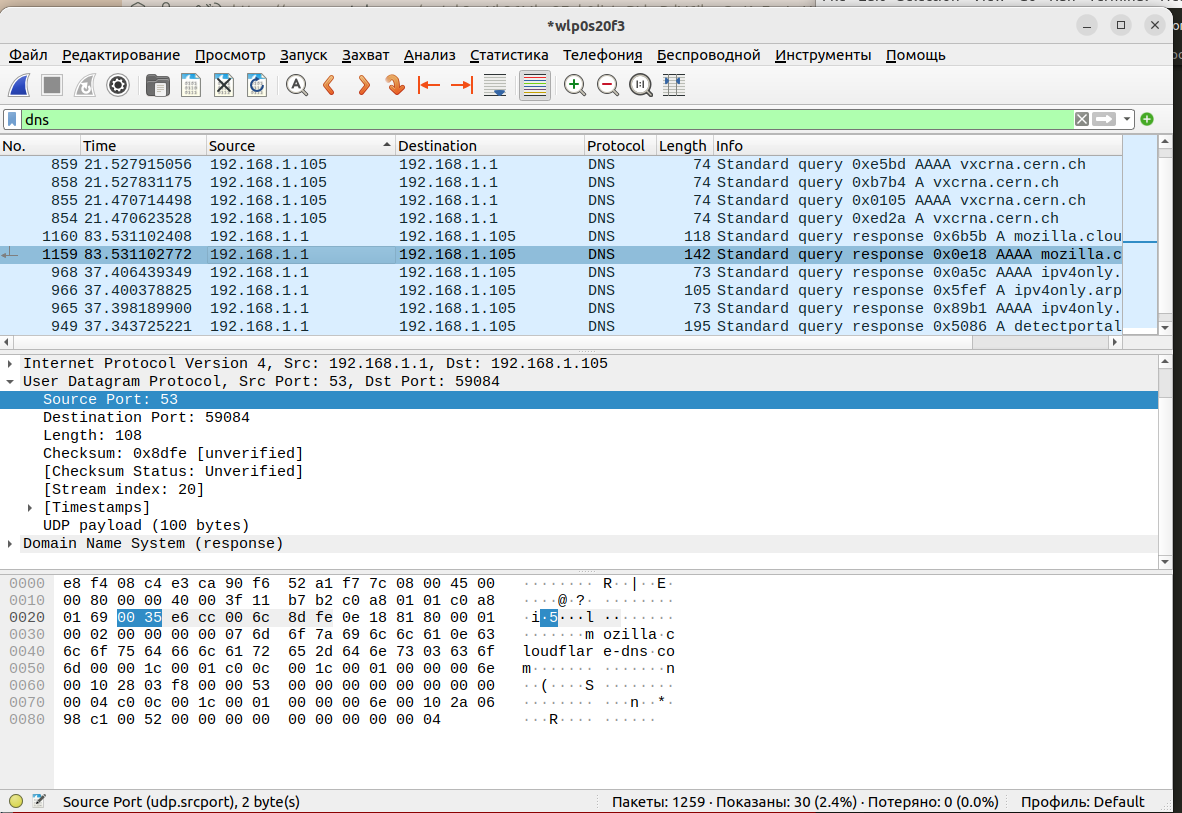
Раздел Line-based text data

Wireshark в строке фильтра укажем dns и проанализируем информацию по протоколу UDP в случае запросов и ответов. Протокол UDP добавляет номера портов, то есть вводит адрес транспортного уровня. Порт источника задан случайно, выбором из непривелигированных и незанятых портов, и равен 555882, порт назначения равен 53 - это стандартный порт DNS(??).



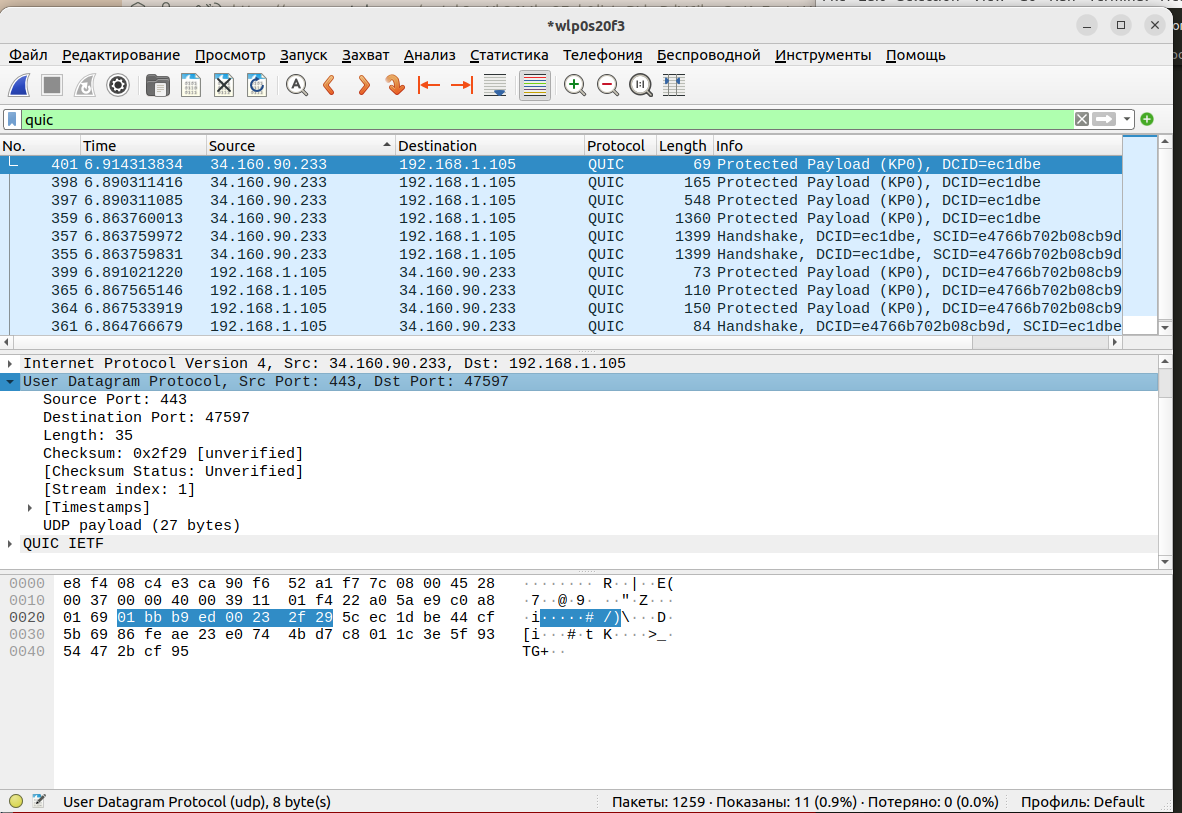
Запрос dns по протоколу UDP

В случае ответа порты заданы наоборот, то есть источник - 53 порт, назначение - 59084 (??).



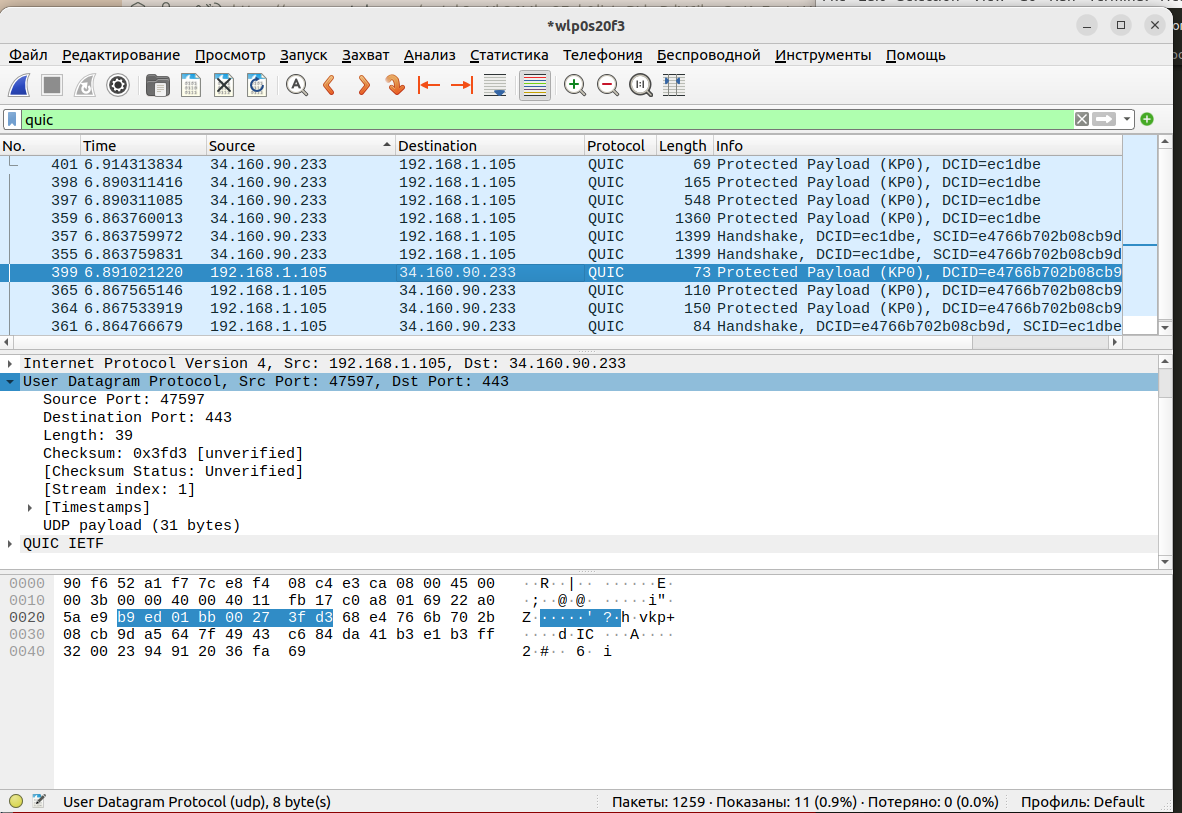
Ответ DNS по протоколу UDP

В Wireshark в строке фильтра укажем quic и проанализируем информацию по протоколу quic в случае запросов и ответов. Как и в случае dns можем посмотреть информацию транспортного уровня по протоколу UDP. Порт источника задан случайно, выбором из непривелигированных и незанятых портов, и равен 47597, порт назначения равен 443 - это стандартный порт HTTPS, то есть quic сразу криптуется(??).



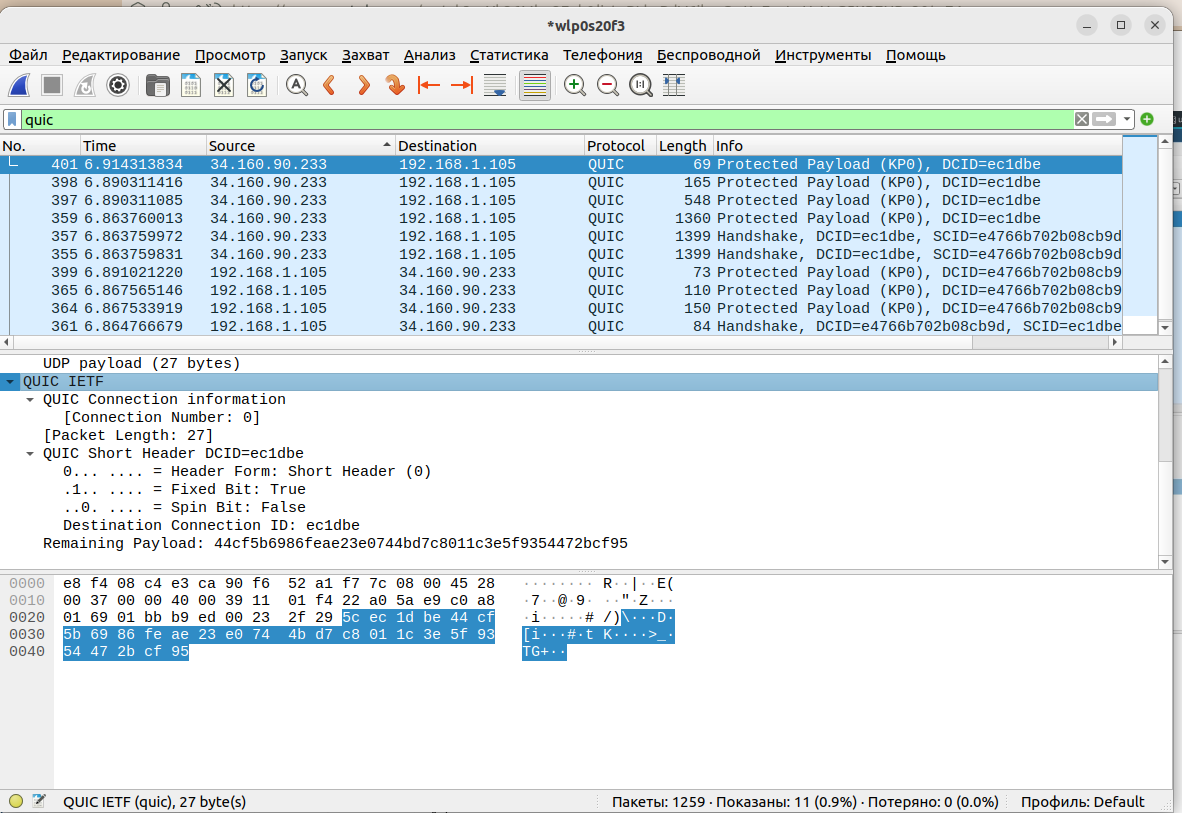
Запрос QUIC по протоколу UDP

В случае ответа порты заданы наоборот, то есть источник - 443 порт, назначение - 47597 (??).

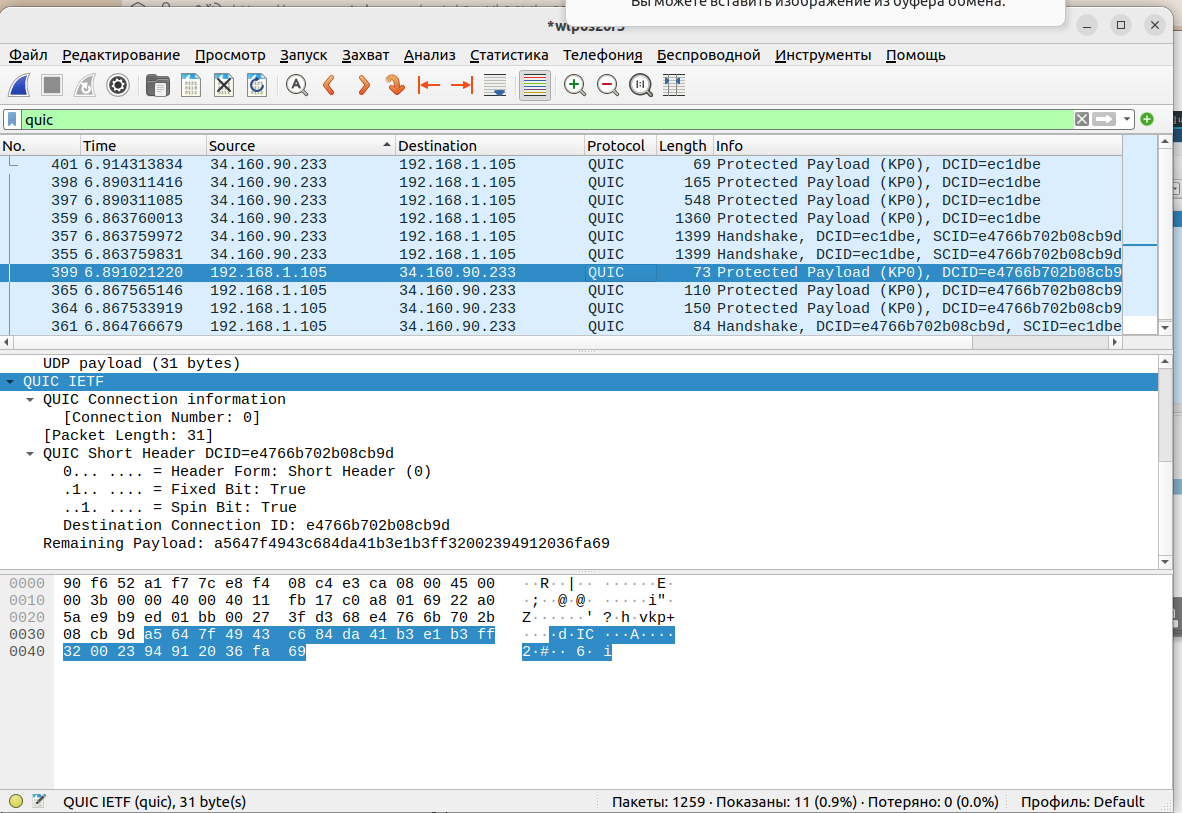


Ответ QUIC по протоколу UDP

Для создания альтернативы TCP поверх UDP строятся протоколы прикладного уровня QUIC IETF, которые управляют трафиком, управляют качеством обслуживания, устанавливают и разрывают соединение (??, ??).



Вкладка QUIK IETF в случае запроса quik



Вкладка QUIK IETF в случае ответа quik

## 3.4 Анализ handshake протокола TCP в Wireshark

Используем соединение по HTTP с сайтом http://info.cern.ch для захвата в Wireshark пакетов TCP.

Проанализируем handshake протокола TCP. Установление связи клиент-сервер в TCP осуществляется в три этапа (трёхступенчатый handshake). Опишем эти этапы на примере.

1. Режим активного доступа. Клиент посылает 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).

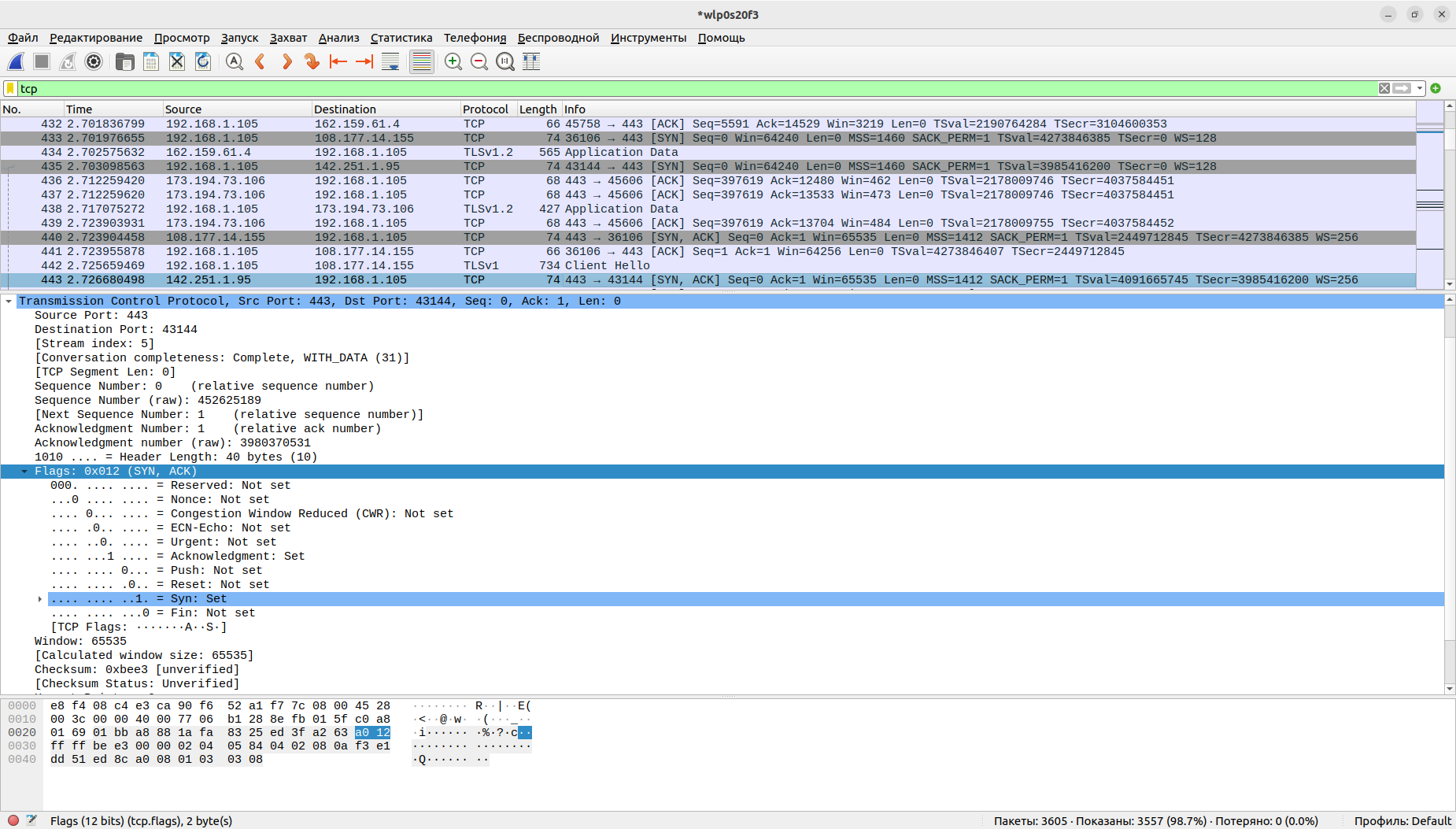
Во вкладке с флагами видно, что установлен бит SYN(Syn: set). Порядковый номер равен 3980370530(??).



Первая ступень handshake протокола TCP

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

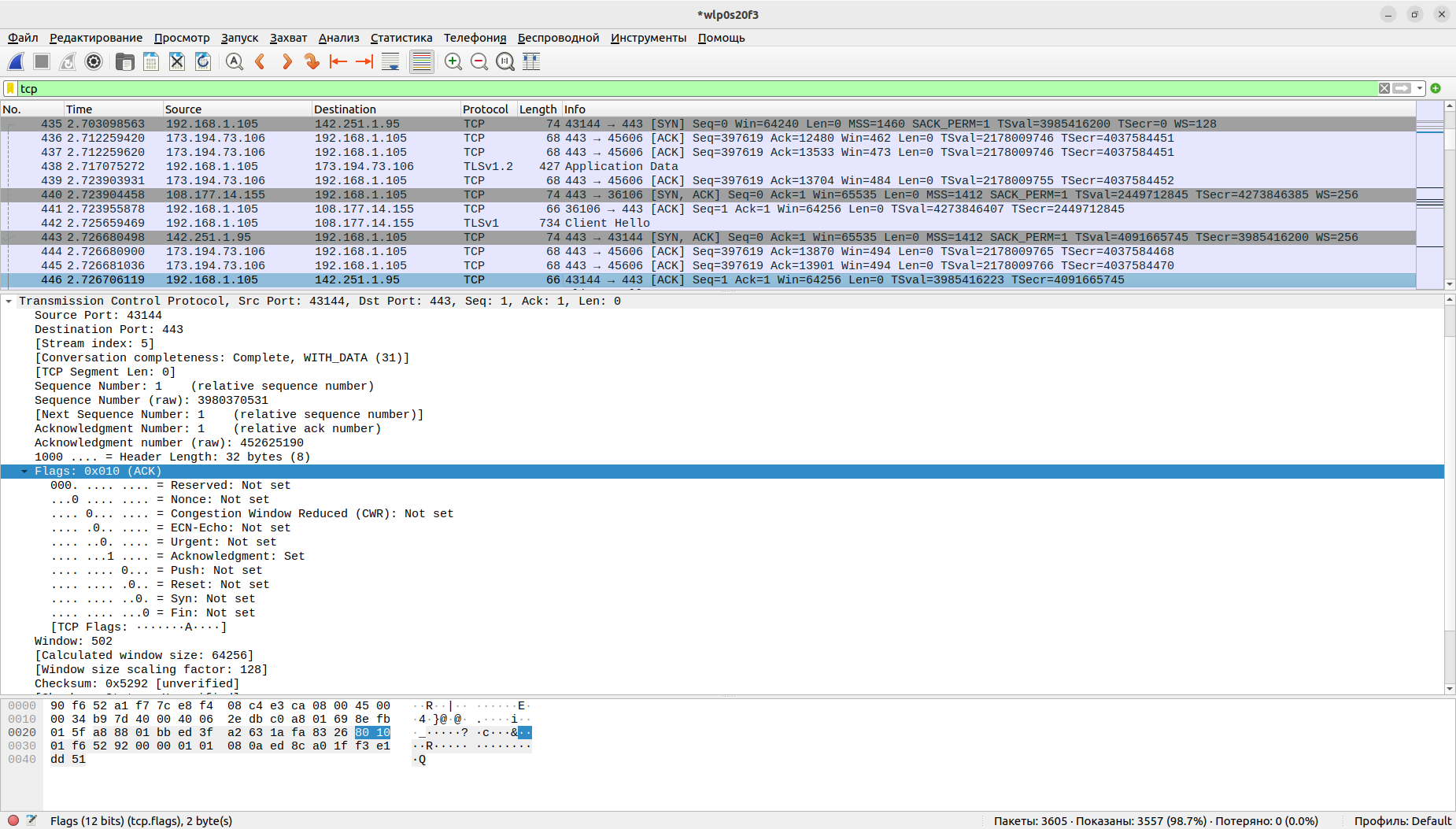
Во вкладке с флагами видно, что установлены биты SYN и ACK(Syn: set, Acknowldgment: set). Порядковый номер содержит значение ISSb и равен 452625189. Поле номер подтверждения равен значению ISSa, которое получил в предыдущем пакете, плюс 1, то есть 3980370531(??).



Вторая ступень handshake протокола TCP

1. Завершение рукопожатия. Клиент отправляет подтверждение получения SYN-сегмента от сервера с идентификатором, равным ISN (сервера)+1: ACK, ISSa+1, ACK(ISSb+1). В этом пакете установлен бит ACK, поле Порядковый номер (Sequence Number) содержит ISSa+1, поле Номер подтверждения (Acknowledgment Number) содержит значение ISSb+1. Посылкой этого пакета заканчивается трёхступен-чатый handshake, и TCP-соединение считается установленным.

Во вкладке с флагами видно, что установлен бит ACK(Acknowldgment: set). Порядковый номер равен ISSa+1 и равен 3980370531. Поле номер подтверждения равен значению ISSb, которое получил в предыдущем пакете, плюс 1, то есть 452625190.(??).



Третья ступень handshake протокола TCP

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

В Wireshark в меню «Статистика» выберем «График Потока». В отчёте приведите пояснения по изменениям значений соответствующих сообщений при установлении соединения по TCP.

На графике видно, что сначала клиент послал сообщение на сервер(стрелка вправо), а значение seq = 0. Затем сервер откликнулся(стрелка влево), значение seq = 0, а значение ack = 1. И в третьем пакете клиент оправил подтверждение получение SYN-сегмента(стрелка влево), оба значения syn и ack стали равны 1 (??).

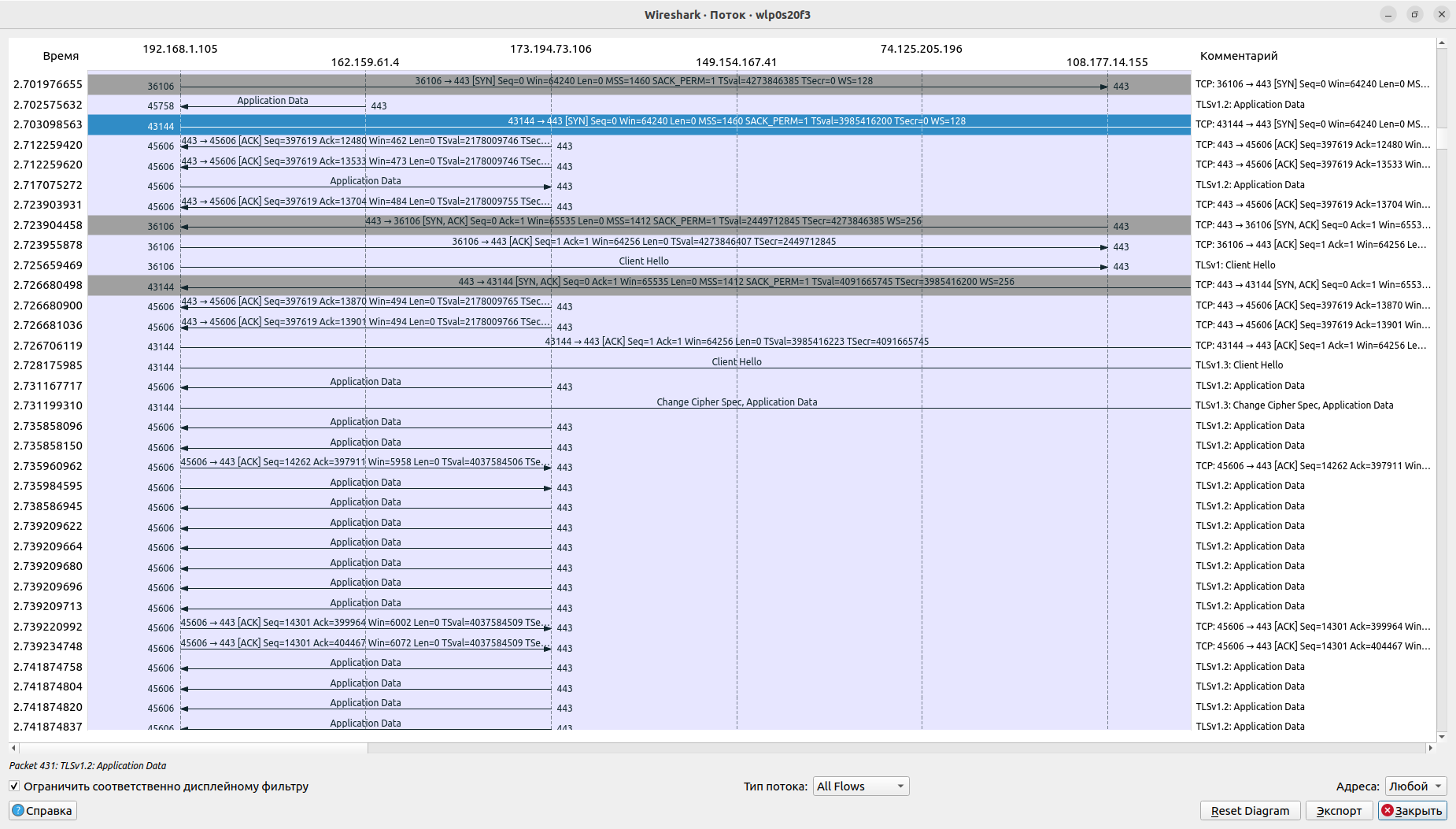


График потока

# 4 Выводы

В результате выполнения лабораторной работы посредством Wireshark были изучены кадры Ethernet, а также проанализированы PDU протоколы транспортного и прикладного уровней стека TCP/IP.