

Лабораторная работа

Наблюдение за процессом трёхстороннего рукопожатия протокола TCP с помощью программы Wireshark

Топология



Задачи

Часть 1. Подготовка программы [Wireshark](#) к захвату кадров

- Выберите необходимый интерфейс сетевого адаптера для захвата кадров.

Часть 2. Захват, поиск и анализ кадров

- Захват данных веб-сеанса с узлом <https://mospolytech.ru/>.
- Поиск соответствующих кадров для веб-сеанса.
- Анализ данных, содержащихся в кадрах, включая IP-адреса, номера портов и флаги управления TCP.

Общие сведения

В данной лабораторной работе необходимо использовать программу [Wireshark](#) для захвата и изучения кадров, генерируемых браузером компьютера, использующим HTTP-протокол, и веб-сервером, например <https://mospolytech.ru/>. При запуске приложения (например HTTP или FTP) на узле, протокол TCP устанавливает соединение между взаимодействующими узлами с помощью трёхстороннего рукопожатия. Например, при работе в Интернете через веб-браузер компьютера трёхстороннее рукопожатие устанавливает соединение между компьютером и веб-сервером. У компьютера может быть одновременно несколько активных сеансов TCP с разными узлами.

Примечание. В этой лабораторной работе предполагается, что компьютер имеет доступ к Интернету.

Необходимые ресурсы

1 компьютер с ОС [Windows](#) с доступом в Интернет и установленной программой [Wireshark](#).

Часть 1. Подготовка программы Wireshark к захвату кадров

В части 1 требуется запустить программу [Wireshark](#) и выбрать необходимый интерфейс для начала захвата кадров.

Шаг 1. Определение адресов интерфейсов ПК.

Для выполнения лабораторной работы необходимо определить IP-адрес своего компьютера и физический адрес сетевого адаптера (MAC-адрес).

a. Откройте окно командной строки на компьютере и введите команду `ipconfig /all`

и нажмите на клавиатуре **ВВОД**.

```
Физический адрес. . . . . : 84-34-97-7B-F1-39
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::a037:4716:80af:f844%19(Основной)
IPv4-адрес. . . . . : 192.168.1.33(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 3 августа 2022 г. 8:42:16
Срок аренды истекает. . . . . : 7 августа 2022 г. 0:13:19
Основной шлюз. . . . . : 192.168.1.1
DHCP-сервер. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 327431319
DUID клиента DHCPv6 . . . . . : 00-01-00-01-2A-01-21-AF-C0-25-E9-16-EA-26
DNS-серверы. . . . . : 192.168.1.1
```

b. IP- и физический адреса, связанные с выбранным адаптером **Ethernet**, будут являться тем адресом источника, который нужно искать при анализе захваченных кадров.

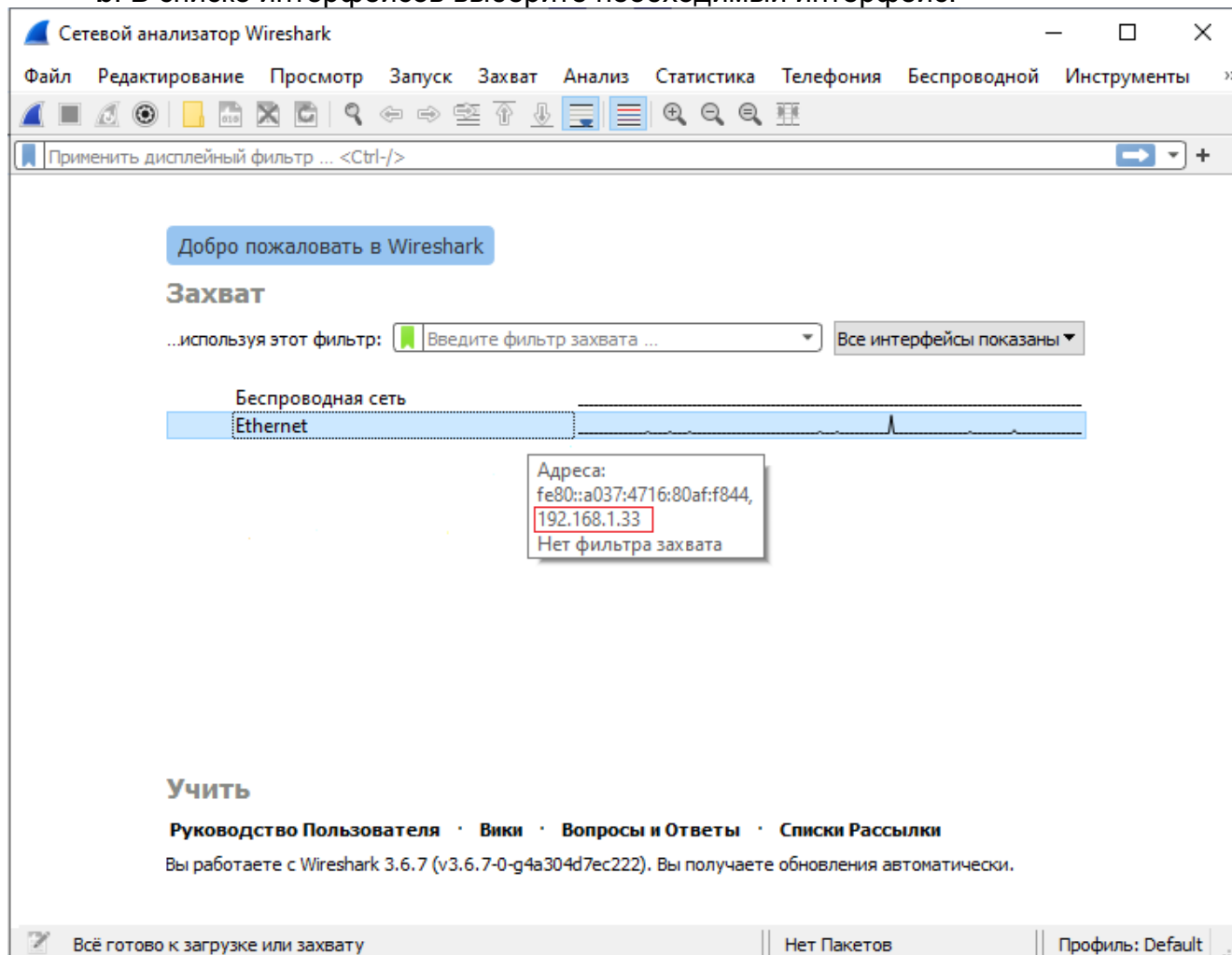
Запишите IP-адрес компьютера: 192.168.1.33

Запишите физический адрес сетевой интерфейсной платы компьютера: 84-34-97-7B-F1-39

Шаг 2. Запустите программу Wireshark и выберите необходимый интерфейс.

a. Запустите программу **Wireshark**.

b. В списке интерфейсов выберите необходимый интерфейс.



Примечание. Если указано несколько интерфейсов, убедитесь в том, что IP-адрес выбранного интерфейса **соответствует** тому, что вы записали в шаге 1b.

Часть 2: Захват, поиск и анализ кадров

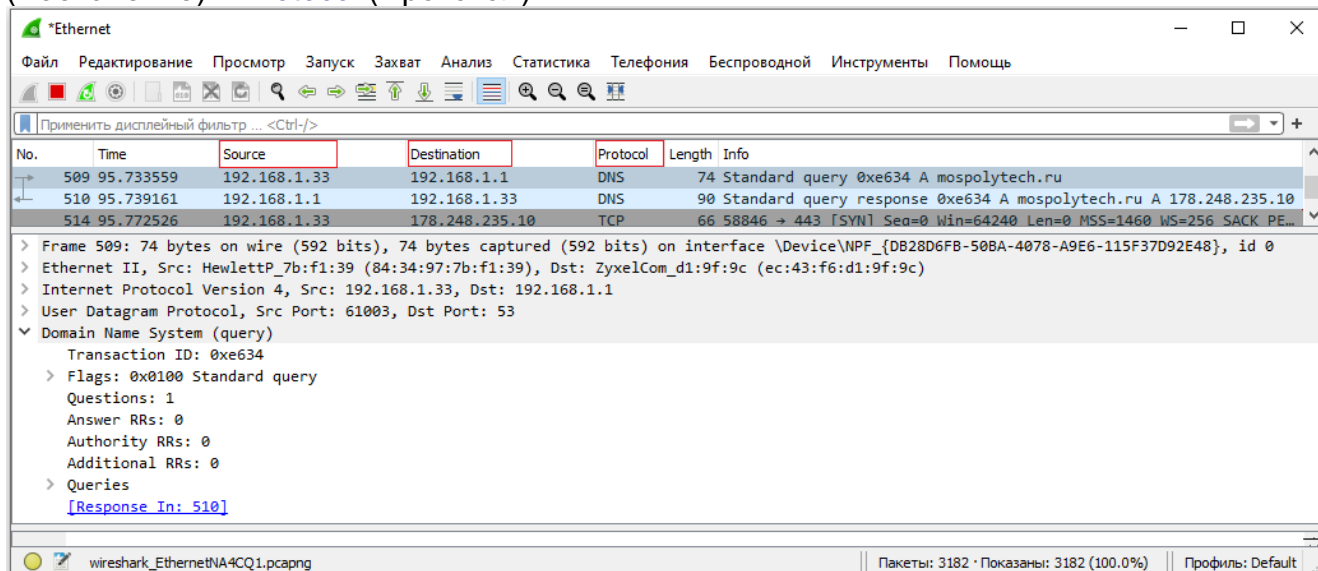
Шаг 1: Нажмите кнопку Старт, чтобы начать захват данных.

а. Откройте в браузере веб-сайт <https://mospolytech.ru/>.

б. Сверните окно браузера и вернитесь в программу Wireshark. Остановите процесс захвата данных. Вы увидите захваченный трафик, как показано ниже.

Примечание. Преподаватель может предложить для исследования другой веб-сайт.

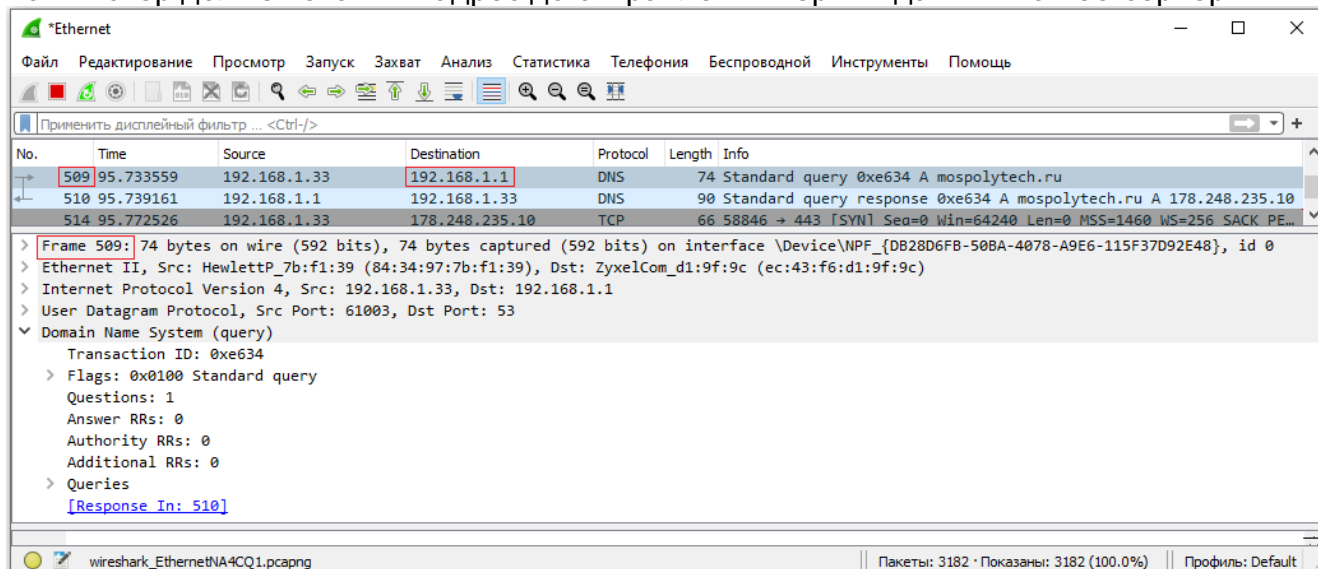
с. Окно захвата кадров активно. Найдите столбцы **Source** (Источник), **Destination** (Назначение) и **Protocol** (Протокол).



Шаг 2: Найдите соответствующие кадры веб-сеанса.

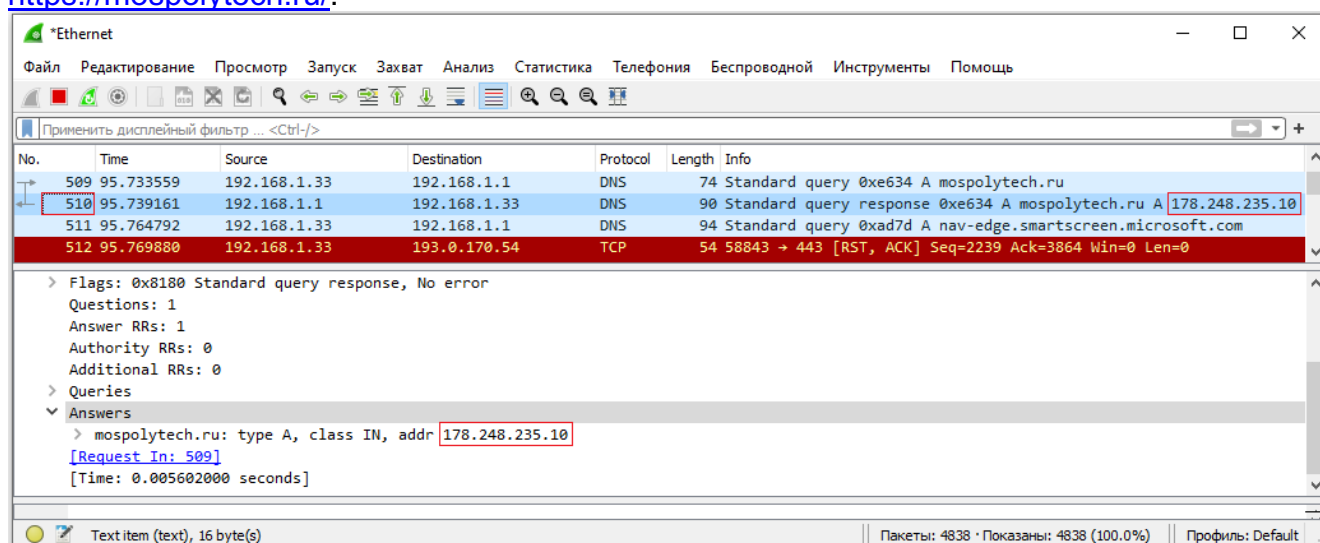
Если компьютер только что включён и еще не использовался для доступа к Интернету, в захваченных данных можно проследить весь процесс взаимодействия, включая работу протокола разрешения адресов (ARP), службы доменных имен (DNS) и процесс трёхстороннего рукопожатия TCP. В примере захвата в части 2, шаг 1 показаны все пакеты, которые компьютер должен отправить на адрес <https://mospolytech.ru/>. В рассматриваемом примере на компьютере уже была запись ARP для основного шлюза, поэтому он сначала создал DNS-запрос для сопоставления <https://mospolytech.ru/>.

а. В кадре 509 примера показан DNS-запрос от компьютера к DNS-серверу, на сопоставление доменного имени <https://mospolytech.ru/> и IP-адреса веб-сервера. Компьютер должен знать IP-адрес до отправления первых данных на веб-сервер.



Выделите соответствующий кадр в **Вашем** окне **Wireshark** и определите IP-адрес DNS-сервера, запрошенного компьютером.

b. Кадр **510** является ответом DNS-сервера, содержащим IP-адрес <https://mospolytech.ru/>.

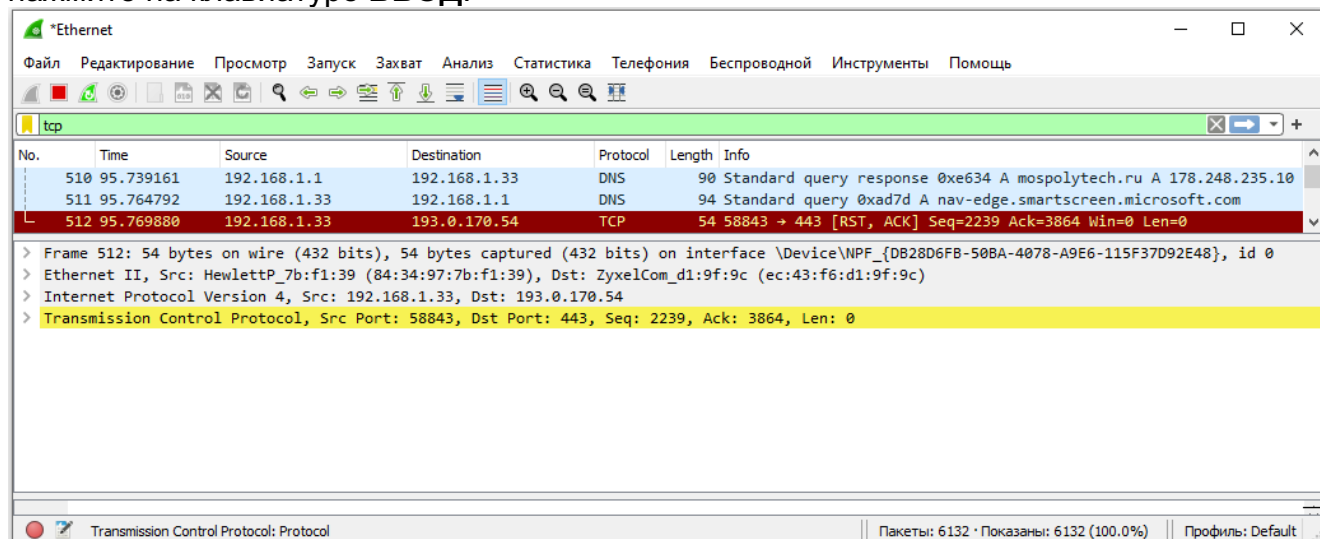


Примечание. Чтобы отобразить все необходимые данные, измените размеры окон программы **Wireshark**.

Выделите соответствующий кадр в Вашем окне **Wireshark** и назовите IP-адрес <https://mospolytech.ru/>, содержащийся в ответе DNS-сервера.

c. Найдите соответствующий кадр (в показанном примере это кадр **512**), начинающий процедуру трёхстороннего рукопожатия **TCP**.

d. Если получено много пакетов, связанных с **TCP**-соединением, воспользуйтесь фильтром программы **Wireshark**. В поле фильтра программы **Wireshark** введите **tcp** и нажмите на клавиатуре **ВВОД**.




Шаг 3: Изучите данные, содержащиеся в кадрах, включая IP-адреса, номера портов TCP и флаги управления TCP.

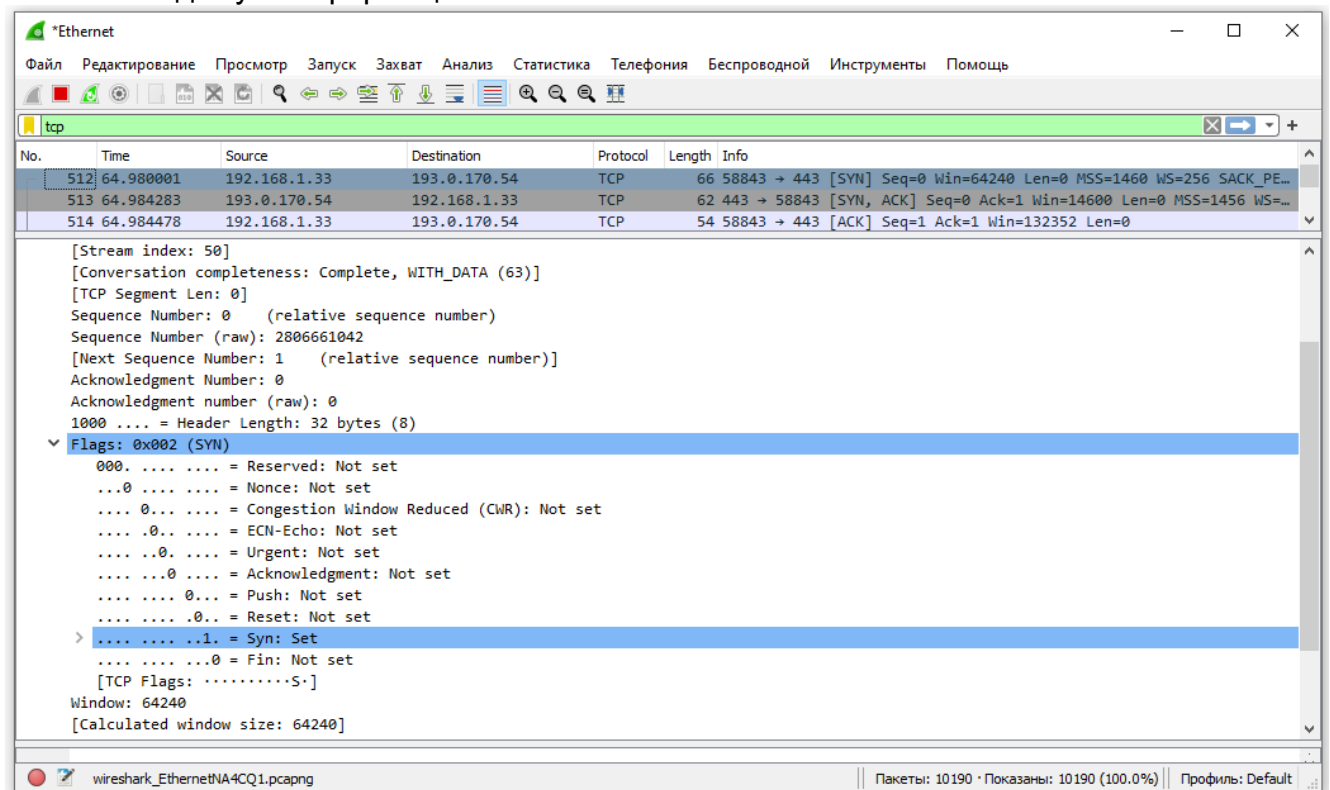
a. В показанном примере кадр **512** показывает начало (содержит первый сегмент) трёхстороннего рукопожатия между компьютером и веб-сервером <https://mospolytech.ru/>. В окне Вашего **Wireshark** на панели списка кадров (верхняя часть основного окна) выделите соответствующий кадр. После этого в двух нижних панелях будет выделена строка и отображена декодированная информация из кадра. Изучите данные о инкапсулированном **TCP** сегменте в средней части основного окна **Wireshark**.

b. На панели сведений о кадрах нажмите на значок > слева от строки **Transmission Control Protocol** (Протокол управления передачей данных), чтобы

просмотреть подробную информацию о TCP сегменте.

с. Слева от **Flags** (Флаги) нажмите на значок . Обратите внимание на порты источника и назначения, а также на установленные флаги.

Примечание. Измените размеры окон программы **Wireshark**, чтобы отобразить всю необходимую информацию.



Назовите номер порта источника TCP.

Как можно охарактеризовать порт источника?

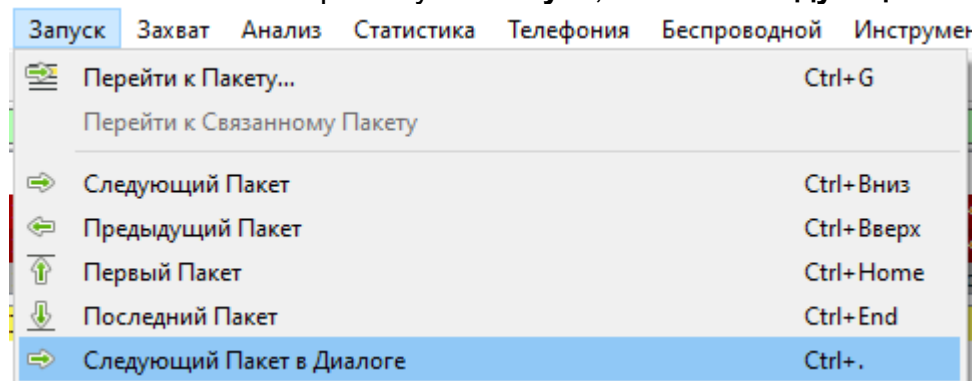
Назовите номер порта назначения TCP.

Как можно охарактеризовать порт назначения?

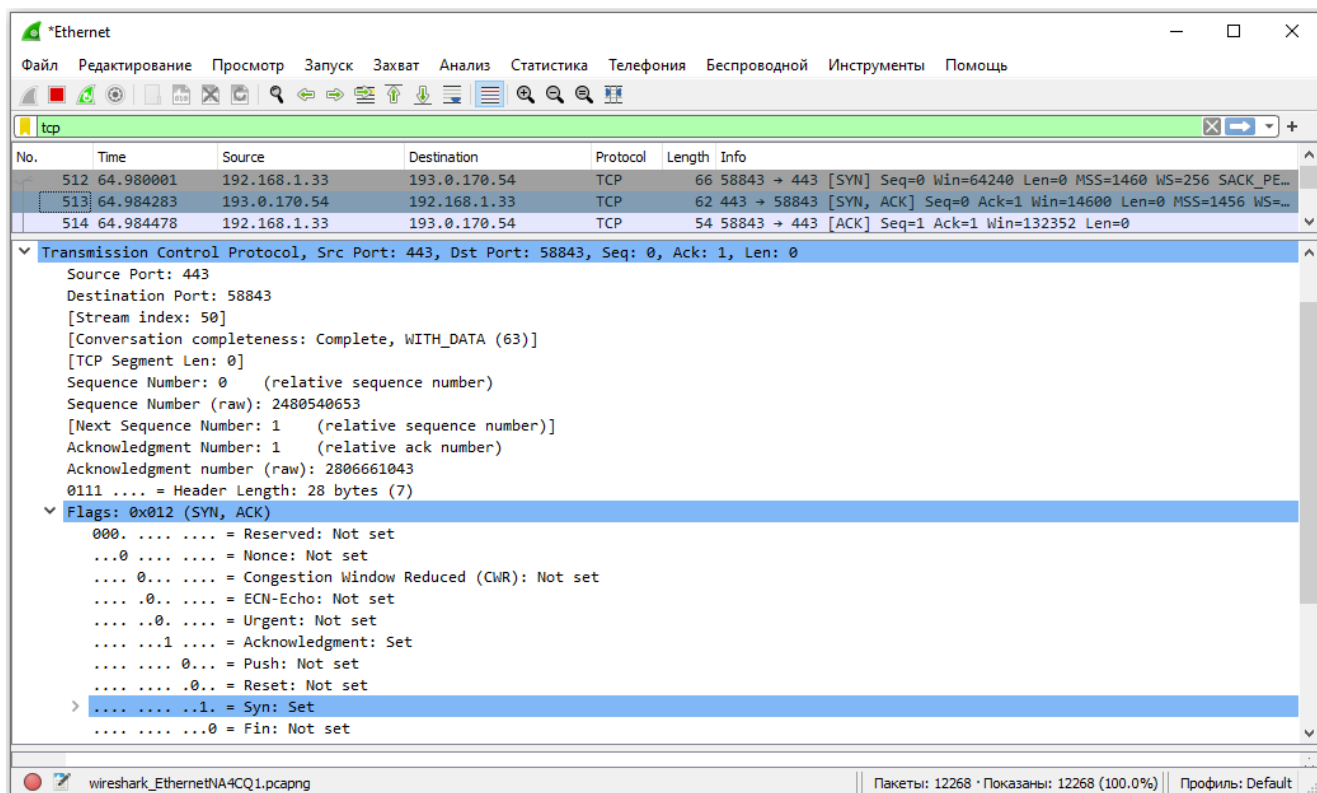
Какие установлены флаги?

Какие значения имеют относительный последовательный номер и номер подтверждения?

d. Чтобы выбрать следующий сегмент в трёхстороннем рукопожатии, в меню программы **Wireshark** выберите пункт **Запуск**, а затем **Следующий Пакет в Диалоге**.



В примере кадр **513** содержит следующий сегмент в трёхстороннем рукопожатии. Это ответ веб-сервера <https://mospolytech.ru/> на исходный запрос для начала сеанса.

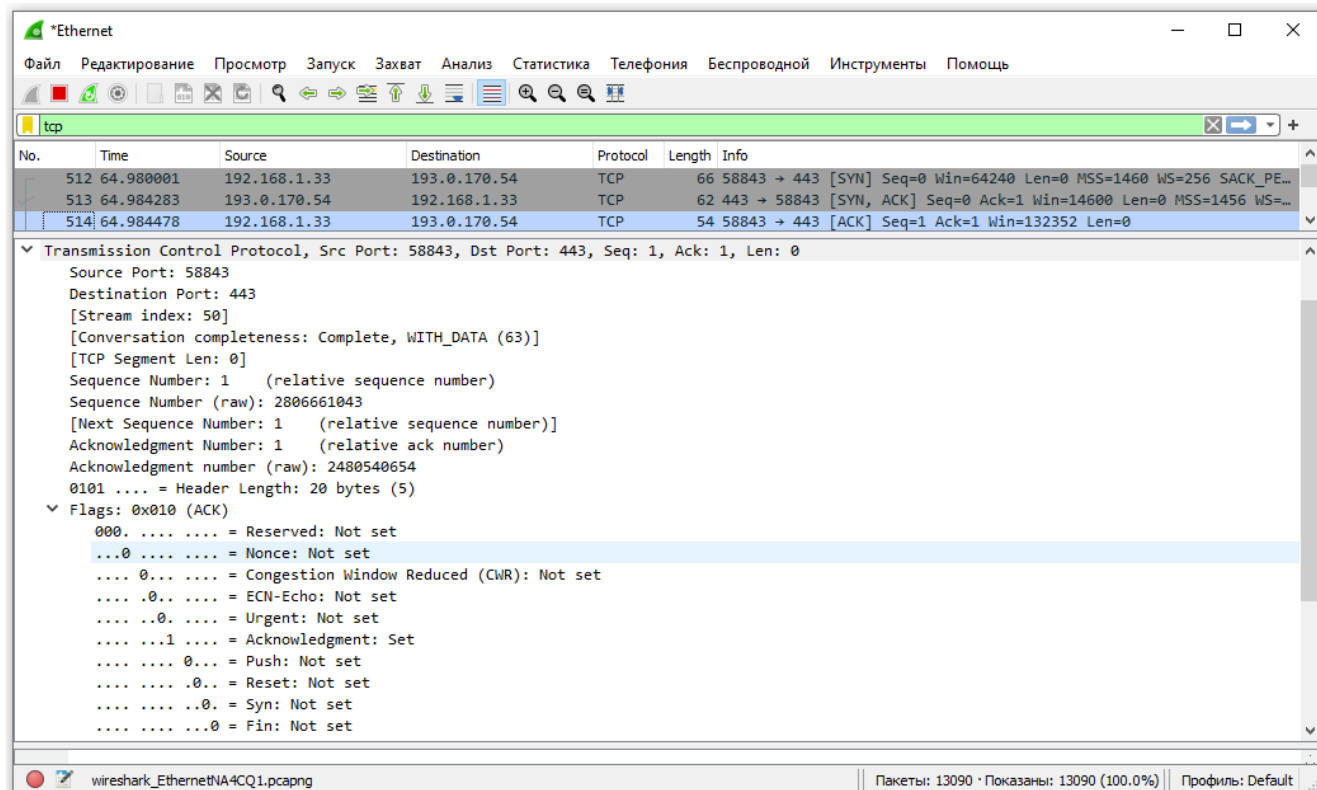


Назовите номера портов источника и назначения.

Какие установлены флаги?

Какие значения имеют относительный последовательный номер и номер подтверждения?

е. Изучите третий (последний) сегмент трёхстороннего рукопожатия (в данном примере его содержит кадр **514**), нажав на соответствующий кадр в верхней части окна Вашего **Wireshark**:



Какие установлены флаги?

Для относительного последовательного номера и номера подтверждения

исходным значением является единица. Соединение [TCP](#) установлено. Можно начать передачу данных между компьютером-источником и веб-сервером.

f. Закройте программу [Wireshark](#).

Вопросы на повторение

1. В программе [Wireshark](#) доступны сотни фильтров. В большой сети может быть множество различных типов трафика. Какие три фильтра [Wireshark](#) будут наиболее полезны сетевому администратору?

2. Как ещё можно использовать программу [Wireshark](#) в производственной сети?