# Лабораторная работа 9.1.3 Использование программы Wireshark для наблюдения процесса трехэтапного согласования TCP

## Задачи

- Использование программы Wireshark для отслеживания и записи процессов передачи пакетов на интерфейсе Ethernet
- Создание TCP-соединения с помощью веб-обозревателя
- Наблюдение процесса трехэтапного согласования TCP/IP

## Основная информация/сведения для подготовки

В этой лабораторной работе для просмотра пакетов TCP/I, созданных в процессе трехэтапного согласования TCP, будет использован анализатор сетевых пакетов Wireshark (именуемый также перехватчиком пакетов). При первом запуске на узле приложения, использующего TCP, для установки надежного TCP-соединения между двумя узлами протокол осуществляет трехэтапное согласование. При выполнении этого задания вы будете наблюдать за передачей трех исходных пакетов потока TCP: пакет SYN, затем пакет SYN ACK и, наконец, пакет ACK.

**Внимание.** Установка или применение приложения перехватчика пакетов может считаться нарушением политики безопасности организации, которое может повлечь серьезные юридические и финансовые последствия. Рекомендуется перед загрузкой, установкой или запуском подобного приложения получить соответствующее разрешение.

**Примечание.** В данной лабораторной работе будет использоваться термин «пакет». Фактически программа Wireshark перехватывает кадры Ethernet, которые содержат IP-пакеты. При анализе перехватов в приложении Wireshark используется термин «кадр». Эти два термина часто подменяют друг друга, однако следует помнить, что кадр представляет собой элемент инкапсуляции канального уровня 2, а пакет относится к инкапсуляции на сетевом уровне 3.

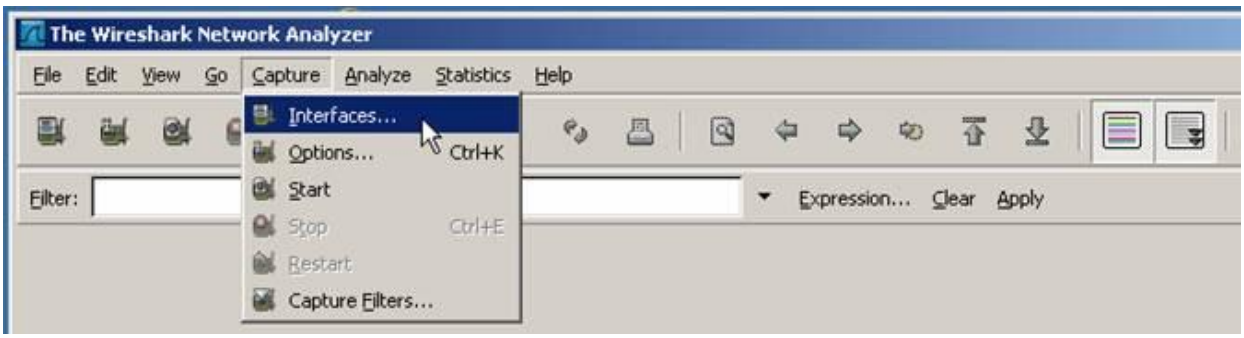
## Задача 1. Подготовка Wireshark к перехвату пакетов

### Шаг 1. Запуск программы Wireshark.

Дважды щелкните мышью значок Wireshark на рабочем столе.

### Шаг 2. Выбор интерфейса для сбора пакетов.

a. В меню Capture (Сбор) выберите пункт **Interfaces** (Интерфейсы).

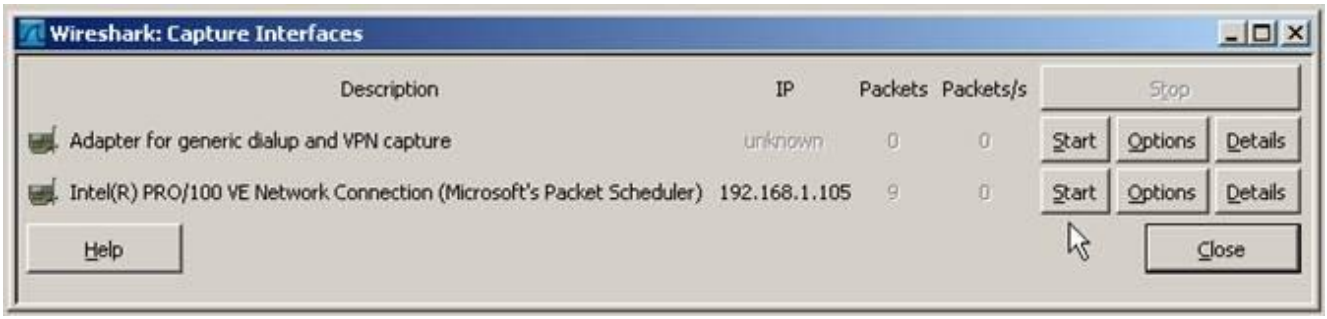


### Шаг 3. Запуск перехвата сетевых данных.

а. Выберите адаптер интерфейса Ethernet локальной сети для перехвата сетевого трафика. Нажмите кнопку **Start** (Начать) на выбранном интерфейсе.

б. Запишите IP-адрес, связанный с выбранным адаптером Ethernet, поскольку он служит исходным IP-адресом для поиска при проверке перехваченных пакетов.

IP-адрес узла: _____




## Задача 2. Создание и анализ перехваченных пакетов.

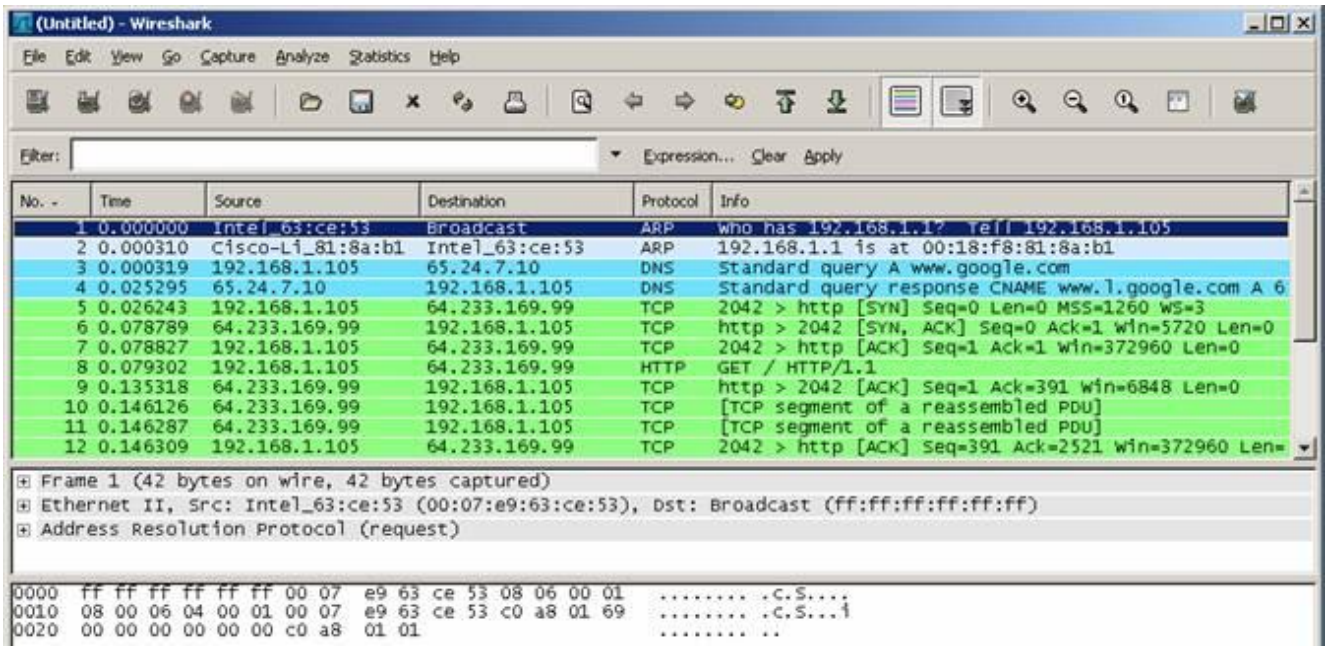
### Шаг 1. Переход на веб-сайт с помощью обозревателя.

а. Перейдите по ссылке www.google.com. Сверните окно Google и вернитесь в Wireshark. Должен быть отображен трафик, схожий с тем, что представлен ниже.

**Примечание.** Преподаватель может указать другой веб-сайт. В этом случае введите ниже название или адрес веб-сайта:

_____

б. Окна перехвата станут активными. Найдите столбцы Source, Destination и Protocol («Источник», «Адрес назначения» и «Протокол») на экране Wireshark. Для надежности в данных HTTP, которые содержат текст и графику веб-страницы, используется протокол TCP.



### Шаг 2. Остановка перехвата

В меню Capture (Сбор) программы Wireshark выберите пункт **Stop** (Остановить).


### Шаг 3. Анализ захваченных выходных данных.

Если компьютер был включен недавно и подключение к Интернету не выполнялось, в перехваченных выходных данных можно видеть весь процесс, включая ARP, DNS и трехэтапное согласование TCP.

На экране перехвата в задаче 2 на шаге 1 отображаются все пакеты, которые компьютер должен передать на веб-сайт, начиная с исходного ARP для MAC-адреса интерфейса маршрутизатора шлюза. (Экраны перехвата в каждом конкретном случае могут отличаться.)

а. На экране перехвата процесс начинается с кадра 1, который представляет собой широковещательную рассылку ARP с исходного компьютера для определения MAC-адреса шлюза маршрутизатора по умолчанию. Роль шлюза выполняет локальный интерфейс Fast Ethernet LAN на маршрутизаторе. Компьютеру необходимо преобразовать IP-адрес шлюза по умолчанию в MAC-адрес интерфейса перед отправкой первого кадра или пакета на маршрутизатор.

Какой IP-адрес у шлюза по умолчанию на маршрутизаторе? _____

б. Второй кадр представляет собой ответ маршрутизатора с сообщением MAC-адреса его интерфейса Fast Ethernet.

Укажите MAC-адрес. _____

в. Третий кадр представляет собой запрос DNS с компьютера к настроенному серверу DNS, который пытается преобразовать имя домена www.google.com в IP-адрес веб-сервера. Для отправки первого кадра на веб-сервер компьютеру требуется его IP-адрес.

Какой IP-адрес у запрашиваемого компьютером сервера DNS? _____

г. Четвертый кадр — это ответ с сервера DNS с IP-адресом www.google.com. Чтобы увидеть IP-адрес сервера Google в ответе DNS, необходимо прокрутить окно вправо, но его можно увидеть в следующем кадре.

д. Пятый кадр служит началом трехэтапного согласования TCP [SYN].

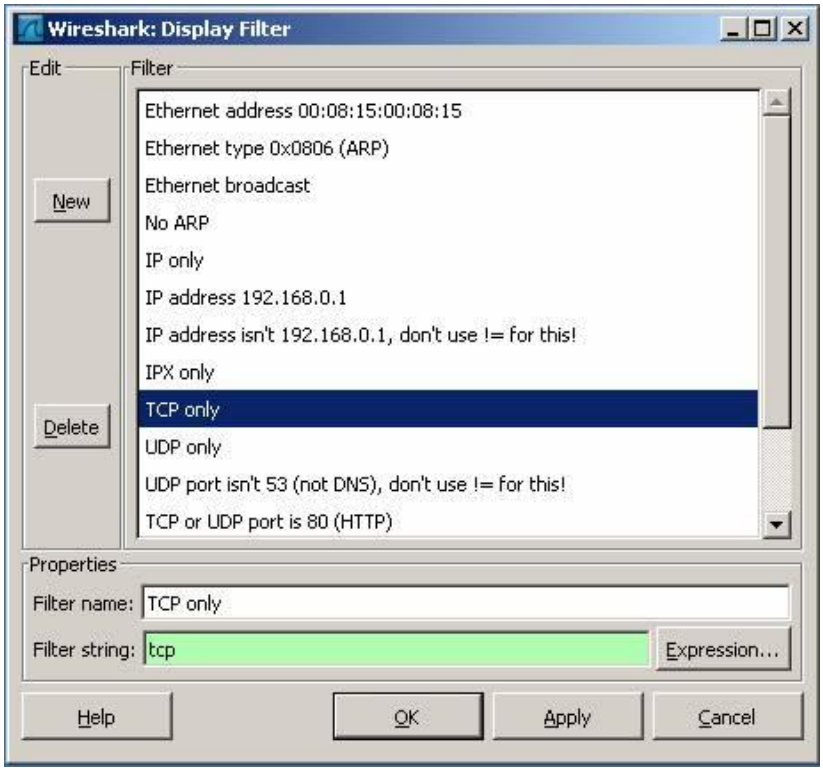
Какой IP-адрес у веб-сервера Google? _____

### Шаг 4. Фильтрация перехваченных данных для отображения только пакетов TCP.

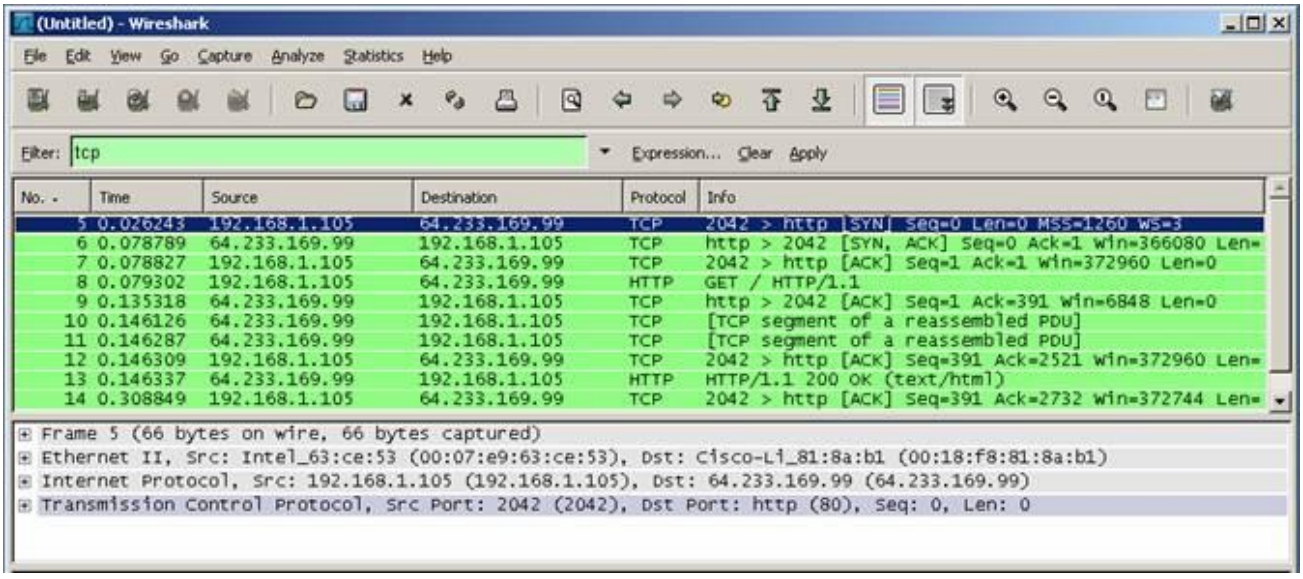
При наличии большого количества пакетов, не связанных с TCP-соединением, возможно, потребуется воспользоваться средством фильтрации Wireshark.

а. Чтобы использовать предварительно настроенный фильтр, выберите пункт меню **Analyze** (Анализ), а затем щелкните **Display Filters** (Показать фильтры).

б. В окне **Display Filter** (Фильтры) выберите параметр **TCP only** (Только TCP) и нажмите кнопку **OK**.




в. В окне Wireshark воспользуйтесь прокруткой, чтобы найти первый перехваченный пакет TCP. Это должен быть первый пакет потока.



г. В столбце Info (Сведения) найдите три пакета, похожих на первые три пакета, показанные в данном окне. Первый пакет TCP — это пакет [SYN] с компьютера-отправителя. Второй — это ответ [SYN, ACK] с веб-сервера. Третий пакет, [ACK], с исходного компьютера, завершает трехэтапное согласование.

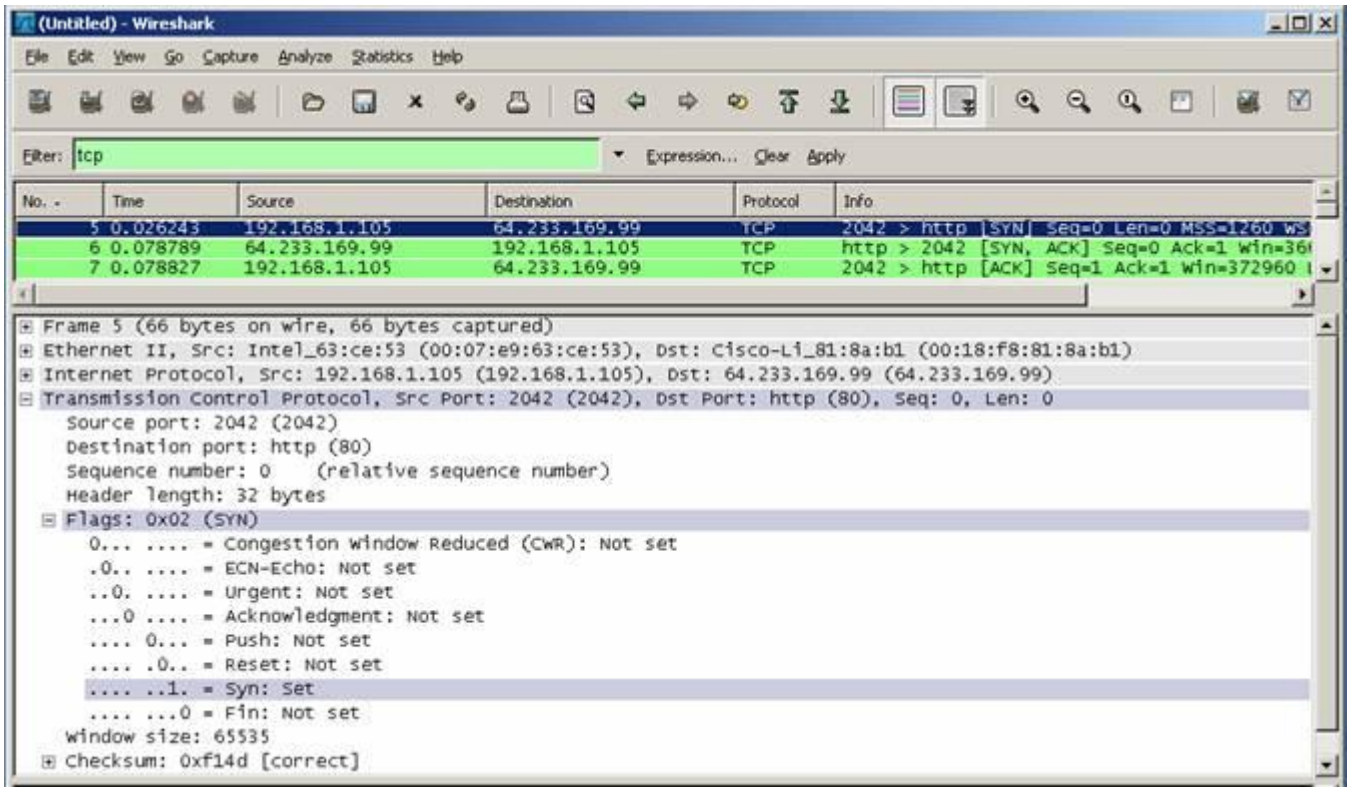
### Шаг 5. Проверка последовательности инициализации TCP

а. В верхней части окна Wireshark щелкните строку, содержащую первый пакет, обнаруженный на шаге 4. Строка будет выделена, и в двух нижних окнах будет отображена расшифрованная информация из этого пакета.

**Примечание.** Показанное ниже окно программы Wireshark было скорректировано для компактного отображения необходимой информации. В среднем окне содержится подробная расшифровка пакета.

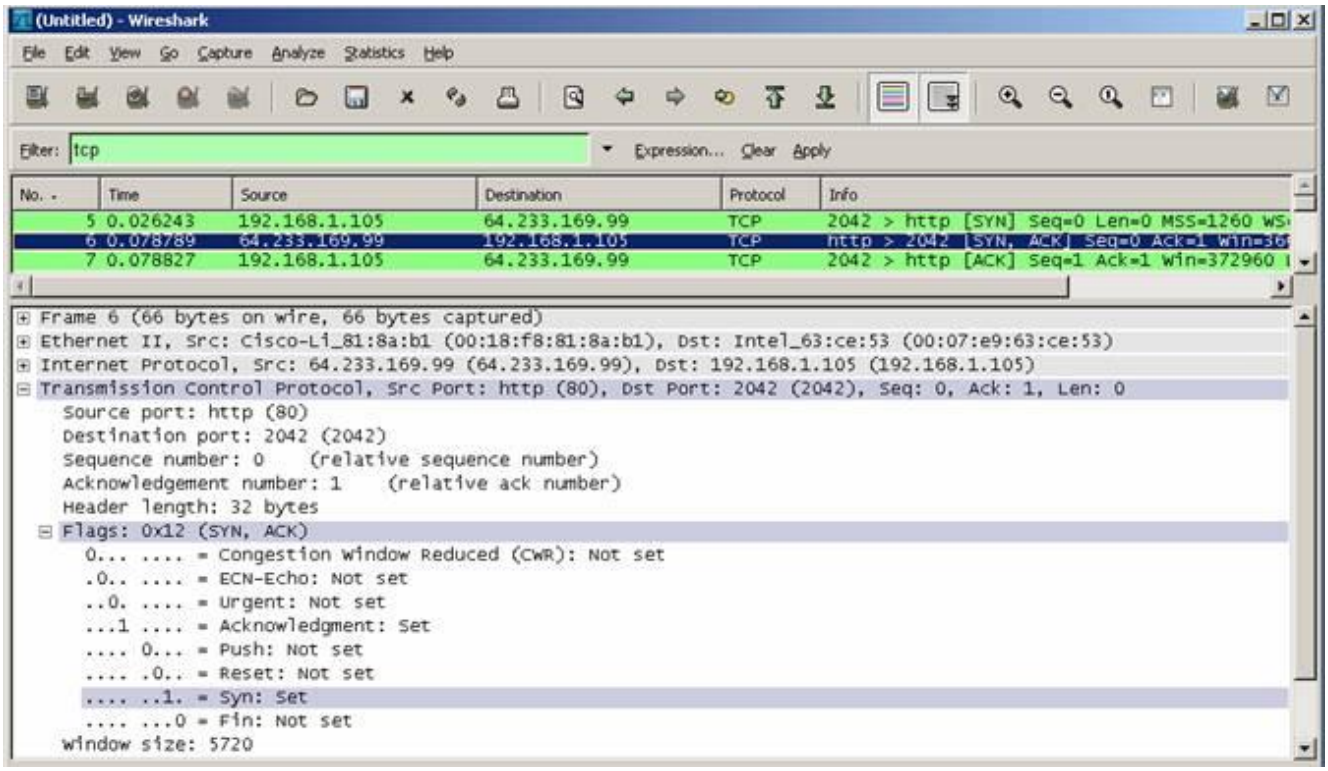
б. Щелкните значок **+**, чтобы развернуть представление сведений TCP. Чтобы уменьшить представление, щелкните значок (—).

в. Обратите внимание, что в первом пакете TCP относительный порядковый номер в поле Flags (Флаги) имеет значение 0, а бит SYN — 1.

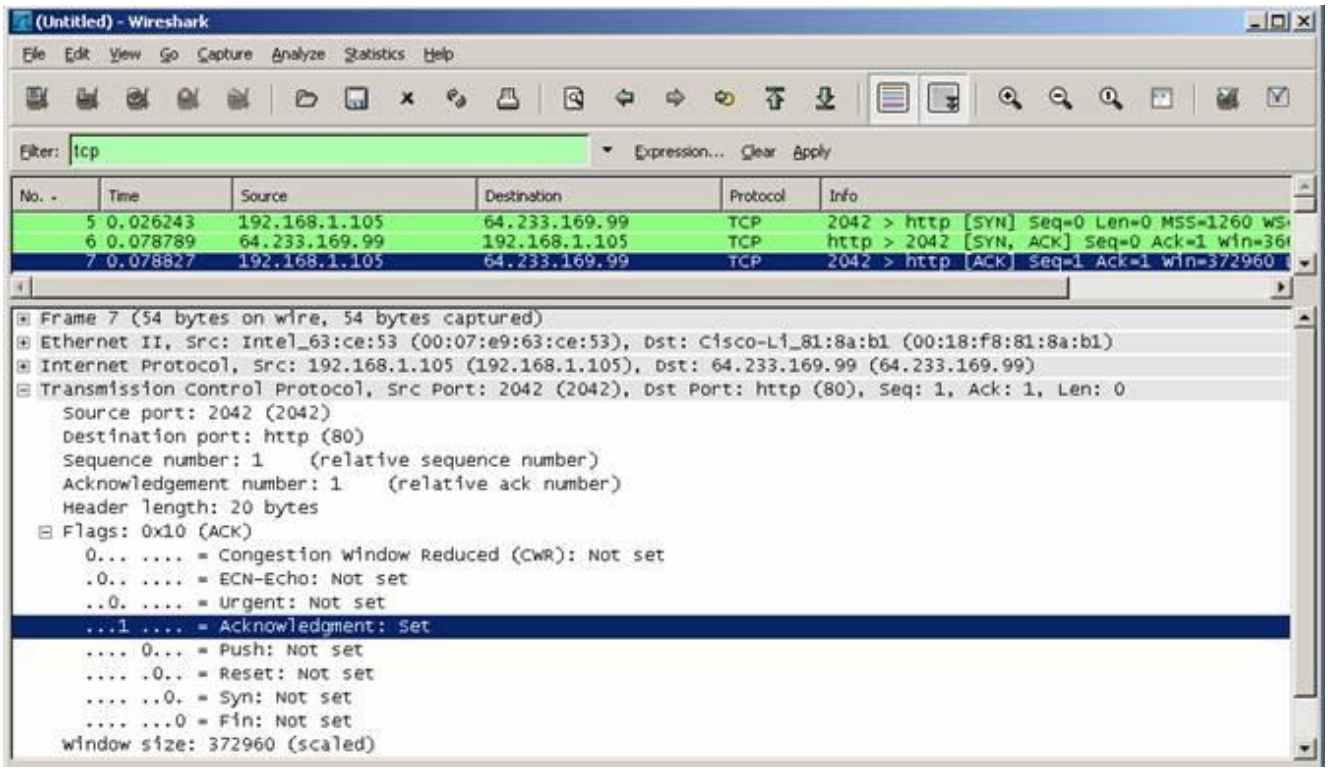



г. Обратите внимание, что во втором пакете TCP согласования относительный порядковый номер в поле Flags (Флаги) имеет значение 0, а бит SYN и бит ACK — 1.




д. В третьем и последнем кадре согласования задано только значение бита ACK, а в качестве порядкового номера установлено значение начальной точки 1. Подтверждение тоже имеет номер 1, как начальная точка. Теперь TCP-соединение установлено, и можно начать обмен данными между исходным компьютером и веб-сервером.




е. Закройте программу Wireshark.

## Задача 3. Вопросы для обсуждения

а. В программе Wireshark существуют сотни фильтров. В крупной сети могут существовать множество фильтров и различные типы трафика. Какие три фильтра из списка могут быть наиболее полезными для сетевого администратора?

_____

б. Программа Wireshark — это средство для внеполосного или внутриполосного мониторинга сетей? _____

Поясните свой ответ.

_____

_____