Лабораторная работа 11. Наблюдение за процессом трехстороннего квитирования протокола TCP с помощью программы Wireshark

1. Топология



1. Задачи

Часть 1. Подготовка программы Wireshark к захвату пакетов

Часть 2. Захват, поиск и изучение пакетов

1. Общие сведения/сценарий

В данной лабораторной работе вам предстоит воспользоваться программой Wireshark для захвата и изучения пакетов, которыми обмениваются браузер ПК, использующий HTTP-протокол, и веб-сервер, например [www.google.com](http://www.google.com). При первом запуске на хосте приложения, например HTTP или FTP, протокол TCP устанавливает между двумя узлами надежный TCP-сеанс с помощью трехстороннего квитирования. Например, при просмотре на ПК страниц Интернета через веб-обозреватель инициируется трехстороннее квитирование и устанавливается сеанс связи между хост-компьютером и веб-сервером. Одновременно на ПК могут иметь место сразу несколько активных TCP-сеансов с разными веб-сайтами.

1. Необходимые ресурсы

Один ПК (под управлением Windows 7, 8 или 10 с доступом к командной строке, доступом к Интернету и установленной программой Wireshark)

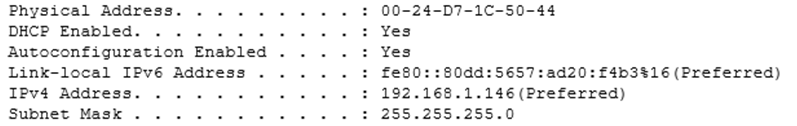
1. Подготовка программы Wireshark к захвату пакетов

В части 1 вам необходимо запустить программу Wireshark и выбрать подходящие интерфейсы для начала захвата пакетов.

* 1. Узнайте адреса интерфейсов ПК.

В данной лабораторной работе вам необходимо узнать IP-адрес компьютера и физический адрес сетевой интерфейсной платы, также называемый MAC-адресом.

* + 1. Откройте окно командной строки, введите команду **ipconfig /all** и нажмите клавишу Enter.

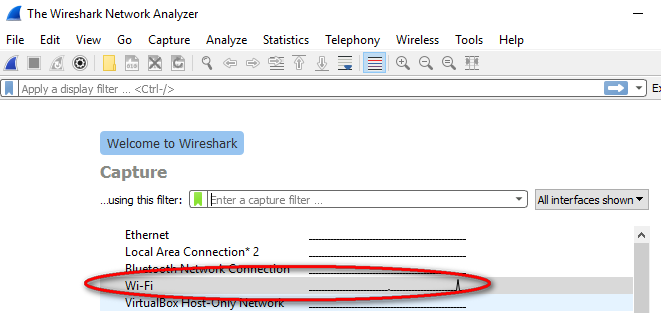


* + 1. Запишите полученные IP-адреса и MAC-адреса, связанные с выбранным адаптером Ethernet. Это адрес источника, который требуется найти при изучении захваченных пакетов.

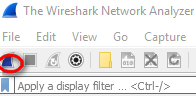
IP-адрес узла ПК: 192.168.8.2

MAC-адрес узла ПК: D8-5E-D3-43-06-C6

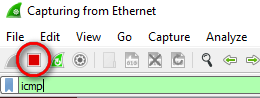
* 1. Запустите программу Wireshark и выберите подходящий интерфейс.
     1. Нажмите кнопку **Start** (Пуск) в системе Windows. Во всплывающем меню дважды щелкните **Wireshark**.
     2. После запуска программы Wireshark выберите активный интерфейс для захвата данных. В активном интерфейсе будут отображаться сведения о трафике.



1. Захват, поиск и изучение пакетов
   1. Выполните захват данных.
      1. Нажмите кнопку **Start** (Начать), чтобы начать захват данных.



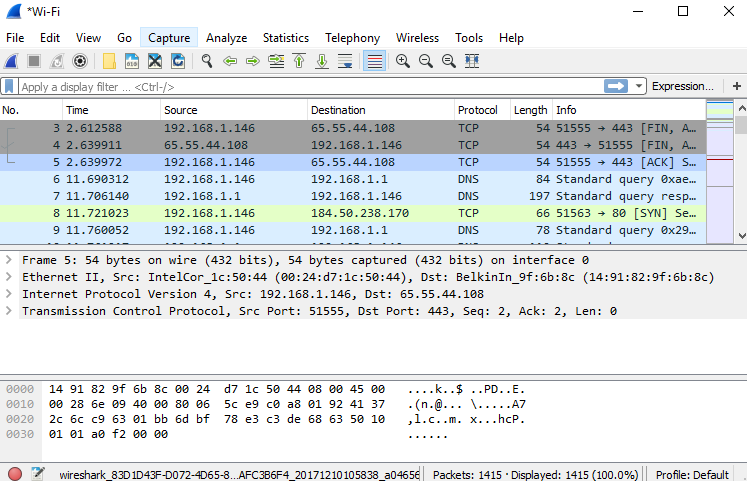
* + 1. Откройте веб-обозреватель и перейдите на страницу www.google.com.
    2. Сверните окно браузера и вернитесь в Wireshark. Остановите процесс захвата данных.



**Примечание**. Инструктор может предложить вам другой веб-сайт. В этом случае введите название или адрес сайта здесь:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Теперь окно захвата данных активно. Найдите столбцы **Source** (Источник), **Destination** (Назначение) и **Protocol** (Протокол).



* 1. Найдите соответствующие пакеты для веб-сеанса.

Если компьютер включен недавно и еще не использовался для доступа в Интернет, в захваченных данных вы сможете увидеть весь процесс, включая протокол разрешения адресов (ARP), систему доменных имен (DNS) и трехстороннее квитирование TCP. Если на ПК уже была запись ARP для шлюза по умолчанию, это значит, что был создан DNS-запрос для преобразования адреса www.google.com.

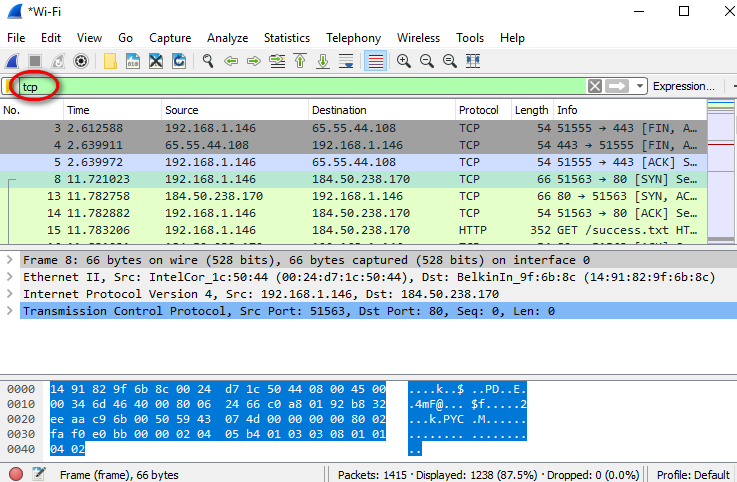
* + 1. В кадре 6 показан DNS-запрос от ПК к DNS-серверу, который пытается преобразовать доменное имя www.google.com в IP-адрес веб-сервера. Прежде чем отправить первый пакет на веб-сервер, ПК должен узнать IP-адрес.

Назовите IP-адрес DNS-сервера, запрошенного компьютером. 8.8.4.4

* + 1. Кадр 7 представляет собой ответ DNS-сервера. Он содержит IP-адрес сайта www.google.com.
    2. Найдите соответствующий пакет, чтобы запустить процедуру трехстороннего квитирования. В данном примере кадр 8 является началом трехстороннего квитирования TCP.

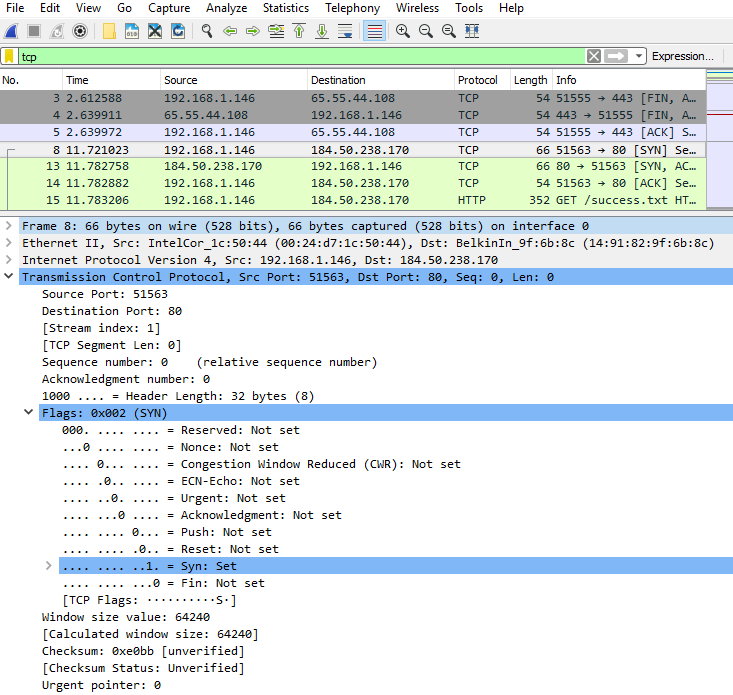
Назовите IP-адрес веб-сервера Google. 142.251.40.100

* + 1. Если вы получили много пакетов, не связанных с TCP-соединением, возможно, целесообразно воспользоваться средствами фильтрации программы Wireshark. В поле значения фильтра программы Wireshark введите **tcp** и нажмите **Enter** (Ввод).



* 1. Изучите содержащиеся в пакетах данные, включая IP-адреса, номера портов TCP и флаги управления TCP.
     1. В нашем примере кадр 8 представляет собой начало трехстороннего квитирования между ПК и веб-сервером Google. На панели списка пакетов (верхний раздел основного окна) выберите кадр. После этого будет выделена строка и отображена декодированная информация из этого пакета в двух нижних панелях. Изучите данные TCP в панели сведений о пакетах (средний раздел основного окна).
     2. На панели сведений о пакетах нажмите на значок **+** слева от строки Transmission Control Protocol (Протокол управления передачей данных), чтобы увидеть подробную информацию о TCP.
     3. Нажмите на значок **+** слева от строки Flags (Флаги). Обратите внимание на порты источника и места назначения, а также на установленные флаги.

**Примечание**. Чтобы отобразить все необходимые данные, может потребоваться скорректировать размеры верхнего и среднего окон программы Wireshark.



Назовите номер порта источника TCP. \_\_51850\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Как бы вы классифицировали порт источника? Динамически назначенный порт

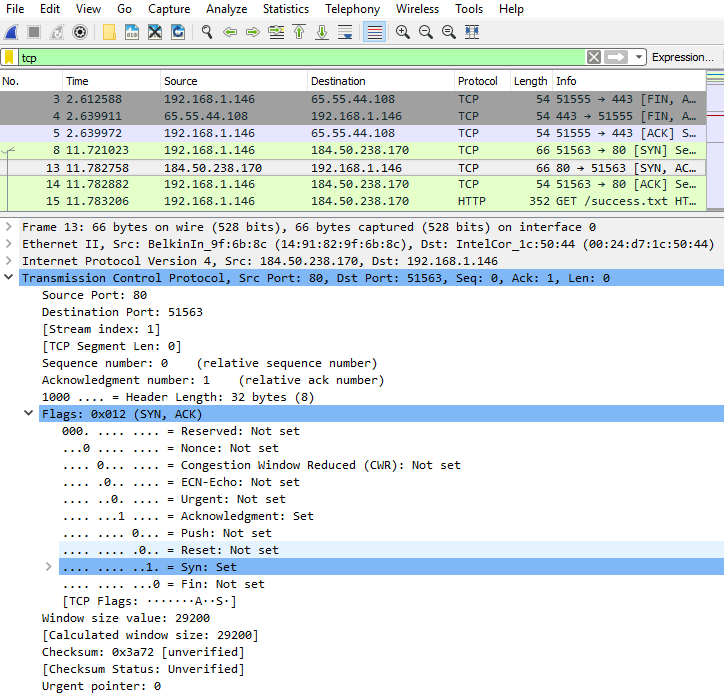
Назовите номер порта назначения TCP. \_\_443\_\_\_\_\_\_

Как бы вы классифицировали порт назначения? \_\_\_порт HTTPS протокола\_

Какие установлены флаги? \_\_ Acknowledgment\_

Какое значение задано для относительного порядкового номера? \_\_17050\_

* + 1. Для того чтобы выбрать следующий кадр в трехстороннем квитировании, в меню программы Wireshark выберите пункт **Go** (Перейти), а затем **Next Packet in Conversation** (Следующий пакет в диалоге). В данном примере это кадр 13. Это ответ веб-сервера Google на исходный запрос для начала сеанса.



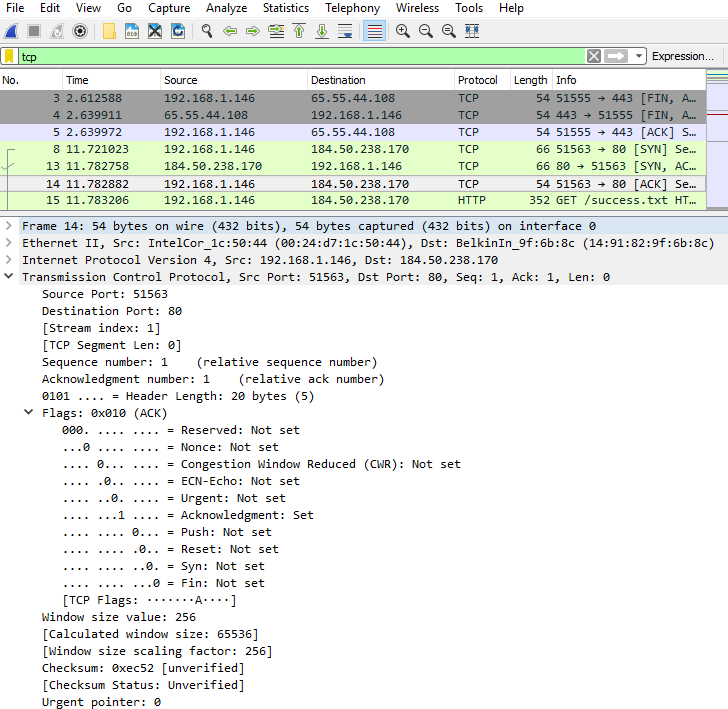
Назовите значения портов источника и назначения. \_443 >> 51850

Какие установлены флаги? \_\_ Acknowledgment

Какие значения заданы для относительного порядкового номера и относительного номера подтверждения?

\_90083, 10621\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. И наконец, изучите третий пакет трехстороннего квитирования в данном примере. Щелкнув по кадру 14 в верхнем окне, вы увидите следующую информацию в данном примере.



Изучите третий и последний пакет квитирования.

Какие установлены флаги? \_\_ Acknowledgment \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Для относительного порядкового номера и относительного номера подтверждения в качестве исходного значения выбрано значение 1. TCP-соединение установлено, и теперь может быть начата передача данных между ПК-источником и веб-сервером.

* + 1. Закройте программу Wireshark.

1. Вопросы для повторения
   1. В программе Wireshark предусмотрены сотни фильтров. В большой сети может существовать множество фильтров и различных типов трафика. Укажите три фильтра, которые могут быть полезны для сетевого администратора.

ip.addr == 192.168.1.1 — фильтрация по IP-адресу источника или назначения. Полезно для отслеживания трафика, связанного с конкретным устройством.

tcp.port == 80 — фильтрация по порту TCP. Может быть использован для отслеживания трафика HTTP.

http.request — фильтрация HTTP-запросов. Этот фильтр помогает отслеживать трафик веб-приложений.

* 1. Как еще можно использовать программу Wireshark в сети предприятия?

Мониторинг производительности сети: Wireshark может использоваться для анализа производительности сети, выявления узких мест и диагностики проблем с пропускной способностью.