Лабораторная работа: наблюдение за процессом трёхстороннего рукопожатия TCP с помощью программы Wireshark

Топология

Задачи

Часть 1. Подготовка программы Wireshark к захвату пакетов

- Выберите подходящий интерфейс сетевого адаптера для захвата пакетов.

Часть 2. Захват, поиск и изучение пакетов

- Захватите данные веб-сеанса на узле www.google.com.
- Найдите соответствующие пакеты для веб-сеанса.
- Изучите содержащиеся в пакетах данные, включая IP-адреса, номера портов TCP и флажки управления TCP.

Исходные данные/сценарий

В данной лабораторной работе вам предстоит воспользоваться программой Wireshark для захвата и изучения пакетов, сгенерированных между браузером ПК, где используется HTTP-протокол, и веб-сервером, например www.google.com. При первом запуске приложения на узле, например HTTP или FTP, TCP устанавливает связь между двумя узлами с помощью трёхстороннего рукопожатия. Например, при просмотре интернет-страниц через веб-браузер ПК трёхстороннее рукопожатие позволяет установить связь между узловым ПК и веб-сервером. Одновременно на ПК могут иметь место сразу несколько активных сеансов TCP с разными веб-сайтами.

Примечание. Эту лабораторную работу нельзя выполнять при помощи Netlab. Она предполагает наличие доступа к Интернету.

Необходимые ресурсы

1 ПК (Windows 7, Vista или XP с доступом к командной строке, доступу к Интернету и установленному анализатору пакетов Wireshark)

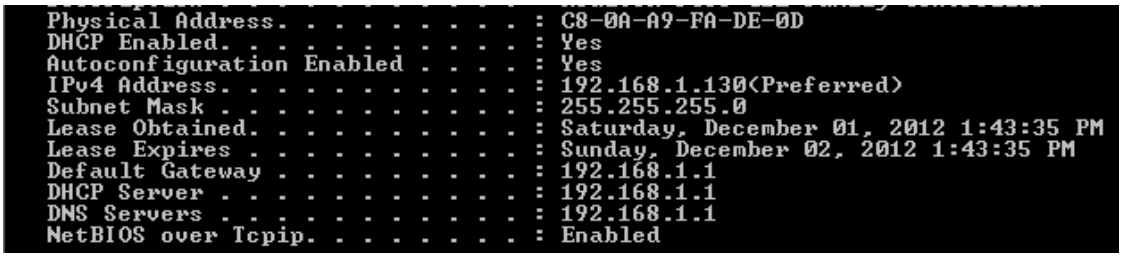
Часть 1: Подготовка программы Wireshark к захвату пакетов

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

Шаг 1: Узнайте адреса интерфейсов ПК.

Для выполнения лабораторной работы вам нужно узнать IP-адрес своего ПК и физический адрес сетевого адаптера, который также называется MAC-адресом.

a. Откройте окно командной строки, введите **ipconfig /all** и нажмите клавишу ВВОД.



b. Запишите IP- и MAC-адреса, связанные с выбранным адаптером Ethernet, поскольку это и есть тот адрес источника, который нужно искать при анализе захваченных пакетов.

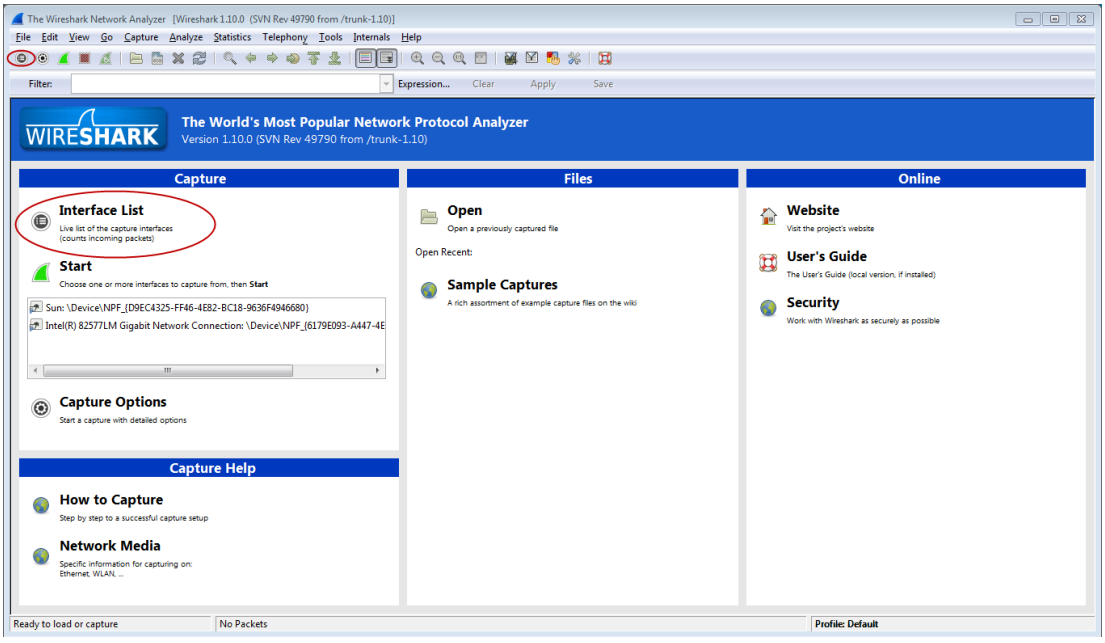
IP-адрес узла ПК: 192.168.0.110

MAC-адрес узла ПК: A0-A4-C5-CA-C7-E0

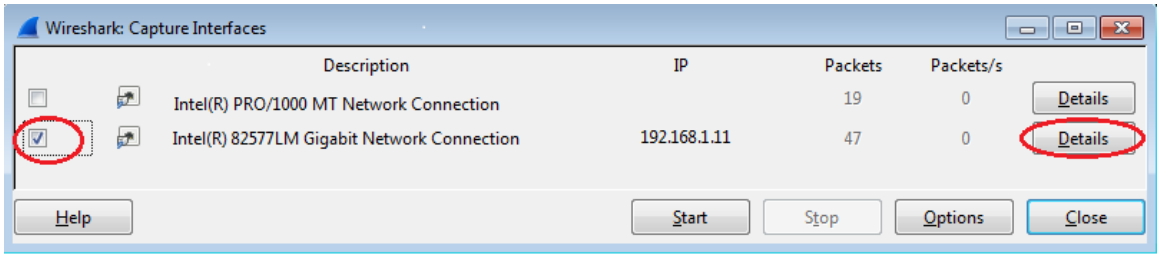
Шаг 2: Запустите программу Wireshark и выберите подходящий интерфейс.

a. Нажмите кнопку **Пуск** и дважды нажмите на **Wireshark**.

b. Запустив программу Wireshark, нажмите на параметр **Interface List** (Список интерфейсов).



c. В окне **Wireshark: Capture Interfaces** (Захват интерфейсов) установите флажок напротив интерфейса подключения к вашей локальной сети.



Примечание. Если указано несколько интерфейсов и вы не уверены в выборе, нажмите кнопку **Details** (Сведения). Откройте вкладку **802.3 (Ethernet)** и убедитесь в том, что MAC-адрес соответствует тому, что вы записали в шаге 1b. Проверив данные, закройте окно со сведениями об интерфейсе.

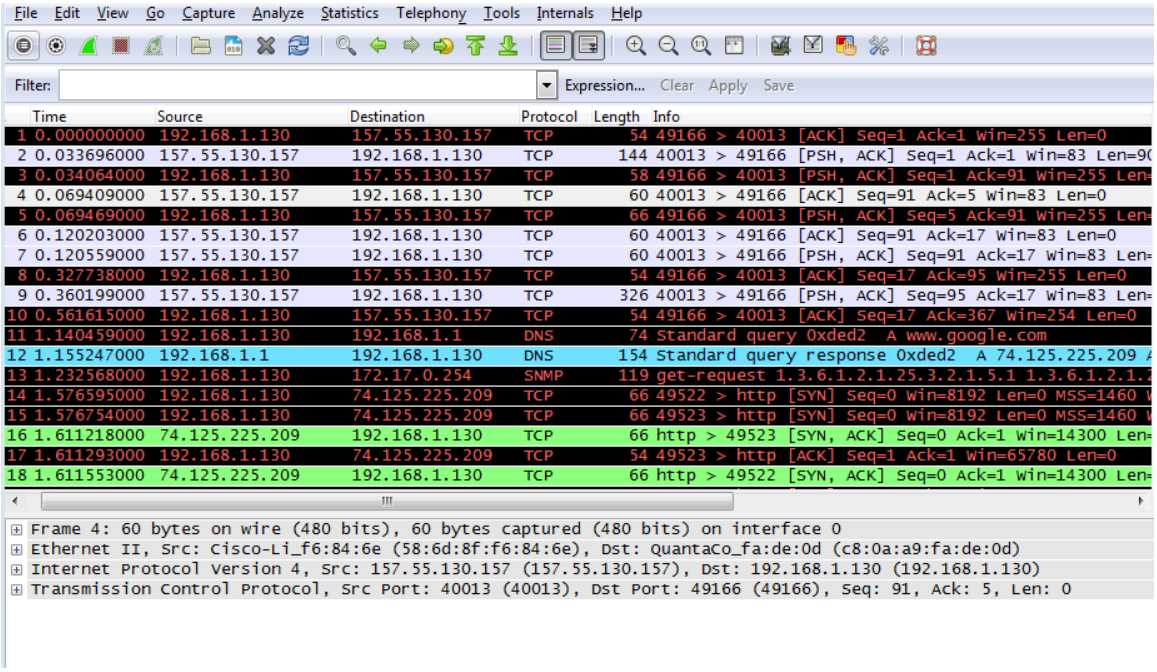
Часть 2: Захват, поиск и изучение пакетов

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

a. Откройте веб-сайт www.google.com. Сверните окно Google и вернитесь в программу Wireshark. Остановите процесс захвата данных. Вы увидите захваченный трафик, как показано на шаге b.

Примечание. Инструктор может предложить вам другой веб-сайт. В этом случае введите название или адрес сайта в соответствующее поле:

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



Шаг 2: Найдите соответствующие пакеты для веб-сеанса.

Если компьютер включён недавно и еще не использовался для доступа к Интернету, в захваченных данных вы сможете увидеть весь процесс, включая протокол разрешения адресов (ARP), службу доменных имен (DNS) и трёхстороннее рукопожатие TCP. На экране захвата в части 2, шаг 1 показаны

все пакеты, которые ПК должен отправить на адрес www.google.com. В данном случае ПК уже имел запись ARP для шлюза по умолчанию, поэтому первым делом он создал DNS-запрос для преобразования www.google.com.

a. В кадре 11 показан DNS-запрос от ПК к DNS-серверу, призванный преобразовать доменное имя www.google.com в IP-адрес веб-сервера. ПК должен знать IP-адрес до отправления первого пакета на веб-сервер.

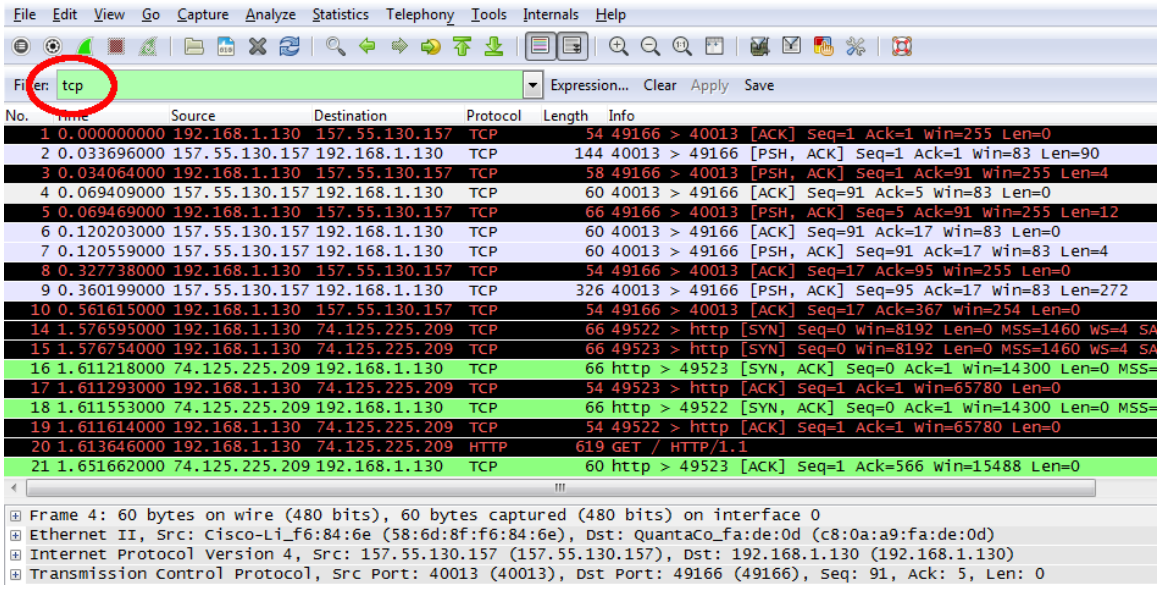
   Назовите IP-адрес DNS-сервера, запрошенного компьютером. 192.168.0.1

b. Кадр 12 показывает ответ DNS-сервера, содержащий IP-адрес www.google.com.

c. Найдите соответствующий пакет, чтобы запустить процедуру трёхстороннего рукопожатия. В данном примере кадр 15 показывает начало трёхстороннего рукопожатия TCP.

   Назовите IP-адрес веб-сервера Google. 172.217.20.4

d. Если вы получили много пакетов, связанных с TCP-соединением, воспользуйтесь фильтрами программы Wireshark. В поле фильтра программы Wireshark введите **tcp** и нажмите клавишу ВВОД.



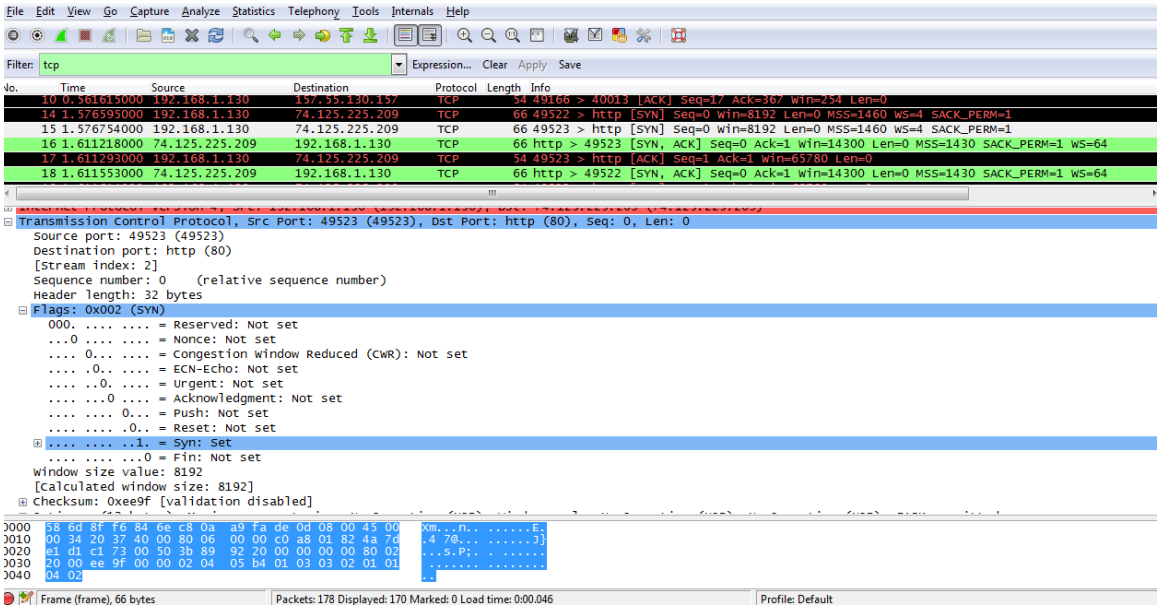
Шаг 3: Изучите содержащиеся в пакетах данные, включая IP-адреса, номера портов TCP и флажки управления TCP.

a. В нашем примере кадр 15 показывает начало трёхстороннего рукопожатия между ПК и веб-сервером Google. На панели списка пакетов (верхний раздел основного окна) выберите кадр. После этого будет выделена строка и отображена зашифрованная информация из пакета в двух нижних панелях. Проверьте данные TCP в панели сведений о пакетах (средний раздел основного окна).

b. На панели нажмите на значок **+** слева от строки Transmission Control Protocol (Протокол управления передачей данных), чтобы увидеть подробную информацию о TCP.

c. Слева от флажков нажмите на значок **+**. Обратите внимание на порты источника и назначения, а также на установленные флажки.

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



Назовите номер порта источника TCP. 63531

Как бы вы классифицировали порт источника? приватный, динамичный

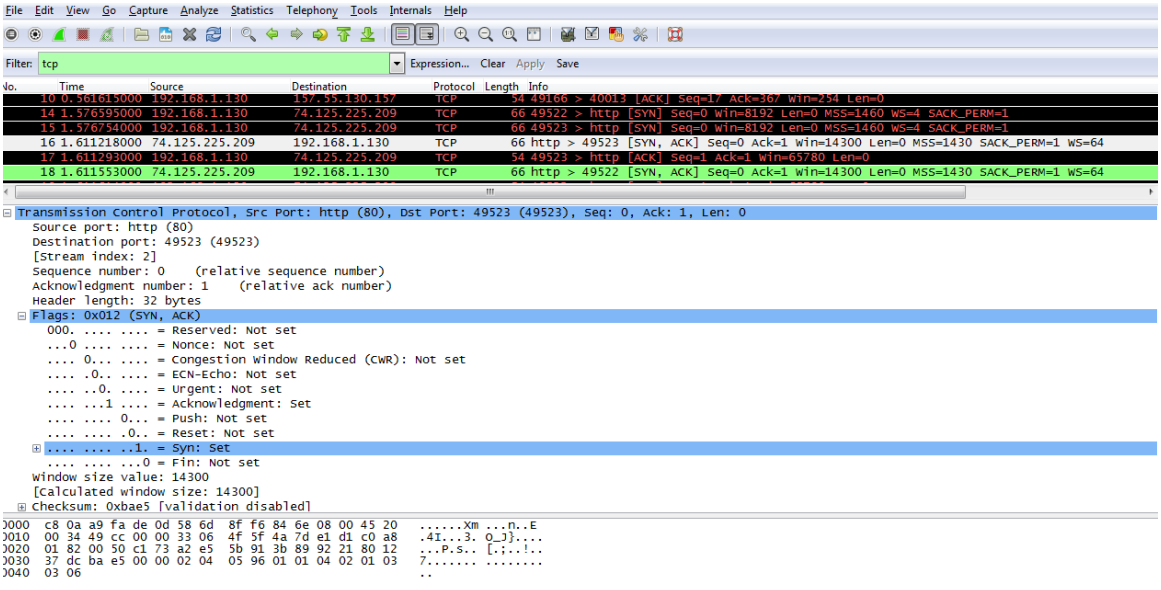
Назовите номер порта назначения TCP. 443

Как бы вы классифицировали порт назначения? публичный, общеизвестный

Какие установлены флажки? syn set

На какое значение настроен относительный последовательный номер? 0

d. Чтобы выбрать следующий кадр в трёхстороннем рукопожатии, в меню программы Wireshark выберите параметр **Go** (Перейти), а затем **Next Packet In Conversation** (Следующий пакет коммуникации). В данном примере это кадр 16. Это ответ веб-сервера Google на исходный запрос для начала сеанса.



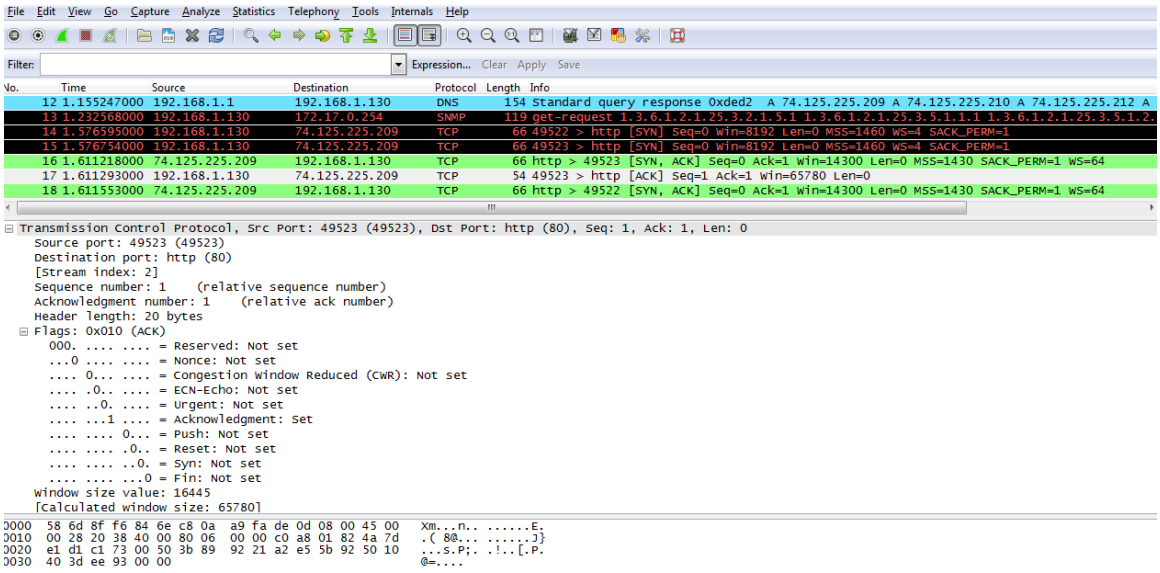
Назовите значения портов источника и назначения. 443 и 63531

Какие установлены флажки? syn acknowlejment

На какие значения настроены относительный последовательный номер и номер подтверждения?

0, 1

e. И, наконец, изучите третий пакет трёхстороннего рукопожатия в данном примере. Нажав на кадр 17 в верхнем окне, вы увидите следующую информацию в данном примере:



Изучите третий и последний пакет рукопожатия.

Какие установлены флажки? acknowlejment

Для относительного последовательного номера и номера подтверждения в качестве исходного значения выбрана единица. Соединение TCP настроено. Теперь можно начать передачу данных между ПК источника и веб-сервером.

f. Закройте программу Wireshark.

Вопросы на закрепление

1. В программе Wireshark доступны сотни фильтров. В большой сети может быть множество фильтров и различных типов трафика. Какие три фильтра в списке будут наиболее полезны для сетевого администратора?

   tcp, dns, ip.addr

2. Как ещё можно использовать программу Wireshark в производственной сети?

   удалить