Лабораторная работа: просмотр сетевого трафика с помощью программы Wireshark

Топология

Задачи

Часть 1. Загрузка и установка программы Wireshark (необязательно)

Часть 2. Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark

- Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к локальным узлам.
- Найдите данные об IP- и MAC-адресах в полученных PDU.

Часть 3. Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark

- Начните и остановите сбор данных трафика эхо-запросов с помощью команды ping к удалённым узлам.
- Найдите данные об IP- и MAC-адресах в полученных PDU.
- Поясните, почему MAC-адреса удалённых узлов отличаются от MAC-адресов локальных узлов.

Исходные данные/сценарий

Wireshark — это программа для анализа протоколов (анализатор пакетов), которая используется для поиска и устранения неполадок в сети, анализа, разработки программного обеспечения и протоколов, а также обучения. По мере движения потоков данных по сети анализатор перехватывает каждый протокольный блок данных (PDU), после чего расшифровывает или анализирует его содержание согласно соответствующему документу RFC или другим спецификациям.

Wireshark — полезный инструмент для всех, кто работает с сетями. Его можно использовать для анализа данных, а также для поиска и устранения неполадок при выполнении большинства

лабораторных работ в рамках курсов CCNA. В данной лабораторной работе содержатся инструкции по загрузке и установке программы Wireshark. Воспользуйтесь ими, если программа не установлена. В ходе лабораторной работы вы научитесь пользоваться программой Wireshark для перехвата IP-адресов пакетов данных ICMP и MAC-адресов Ethernet-кадров.

Необходимые ресурсы

- 1 ПК (Windows 7, Vista или XP с выходом в Интернет)
- Дополнительные ПК в локальной сети будут использоваться для ответов на эхо-запросы.

Часть 1: Загрузка и установка программы Wireshark (необязательно)

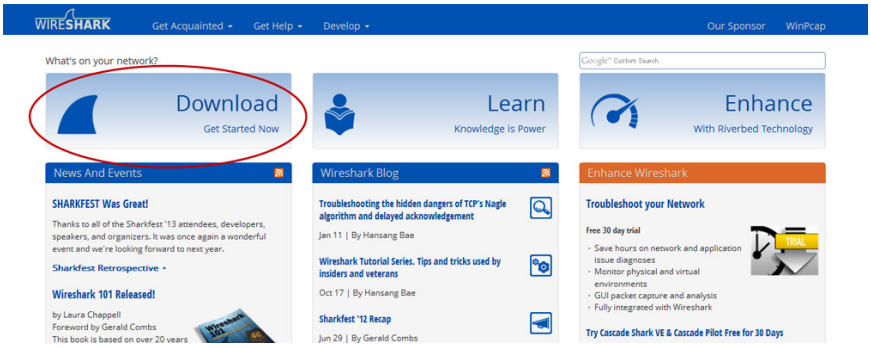
Программа Wireshark стала стандартным анализатором пакетов, используемым сетевыми инженерами. Версии этой программы с открытым исходным кодом доступны для различных операционных систем, включая Windows, Mac и Linux. В части 1 этой лабораторной работы вам нужно будет загрузить и установить программу Wireshark на ПК.

Примечание. Если программа Wireshark на вашем ПК уже установлена, вы можете пропустить часть 1 и перейти сразу к части 2. Если программа Wireshark на вашем ПК не установлена, узнайте у инструктора о правилах загрузки программного обеспечения в вашем учебном заведении.

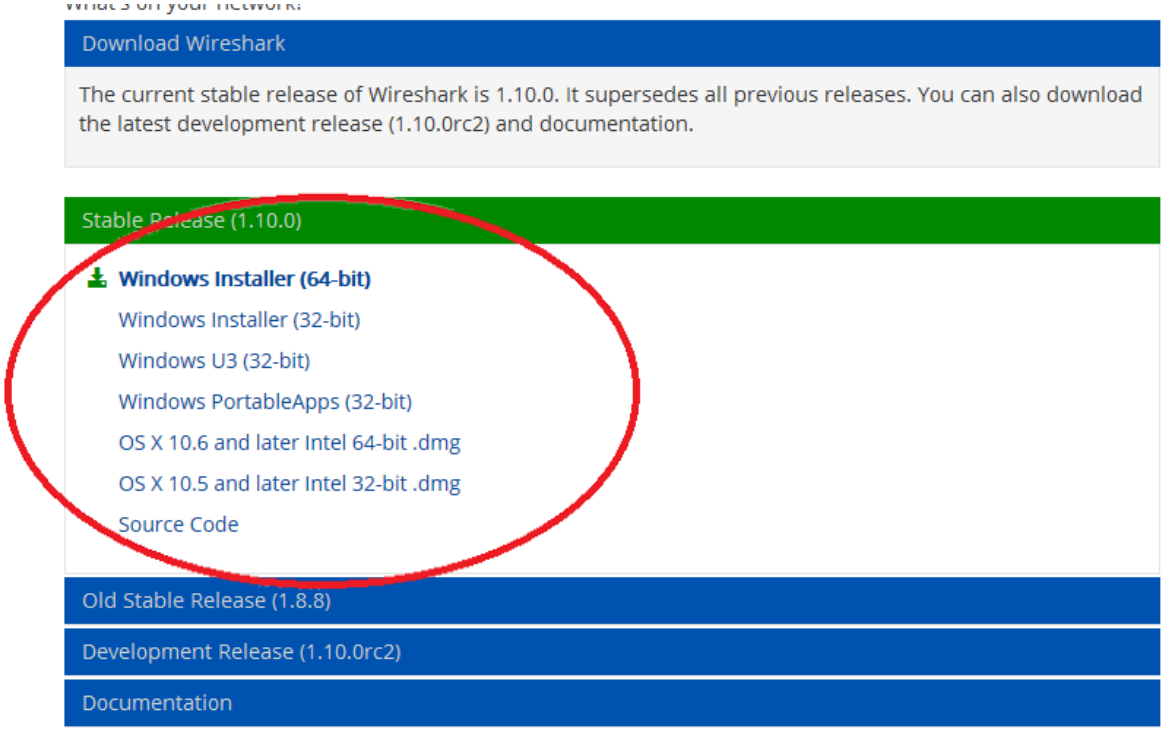
Шаг 1: Загрузите программу Wireshark.

a. Программу Wireshark можно загрузить по адресу www.wireshark.org.

b. Нажмите **Download Wireshark**.



c. Выберите версию программы в соответствии с архитектурой и операционной системой вашего ПК. Например, если ваш ПК работает под управлением 64-разрядной ОС Windows, выберите **Windows Installer (64-bit)**.

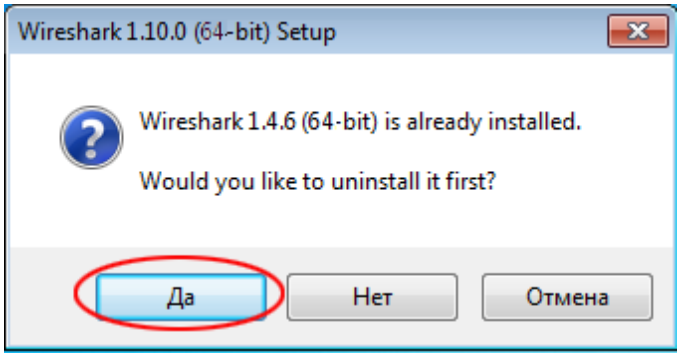


Сразу после этого начнётся загрузка. Местонахождение загруженного файла зависит от браузера и операционной системы, которыми вы пользуетесь. В ОС Windows загрузочные файлы по умолчанию находятся в папке **Загрузки.**

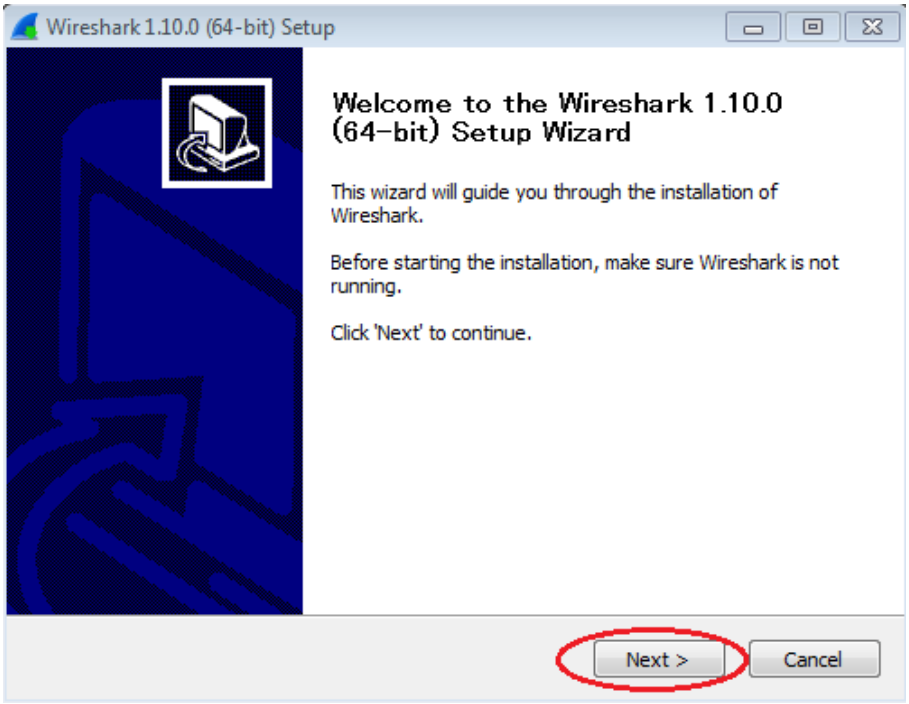
Шаг 2: Установите программу Wireshark.

a. Загруженный файл называется **Wireshark-win64-x.x.x.exe**, где «x» соответствует номеруверсии. Дважды нажмите на файл, чтобы начать установку.

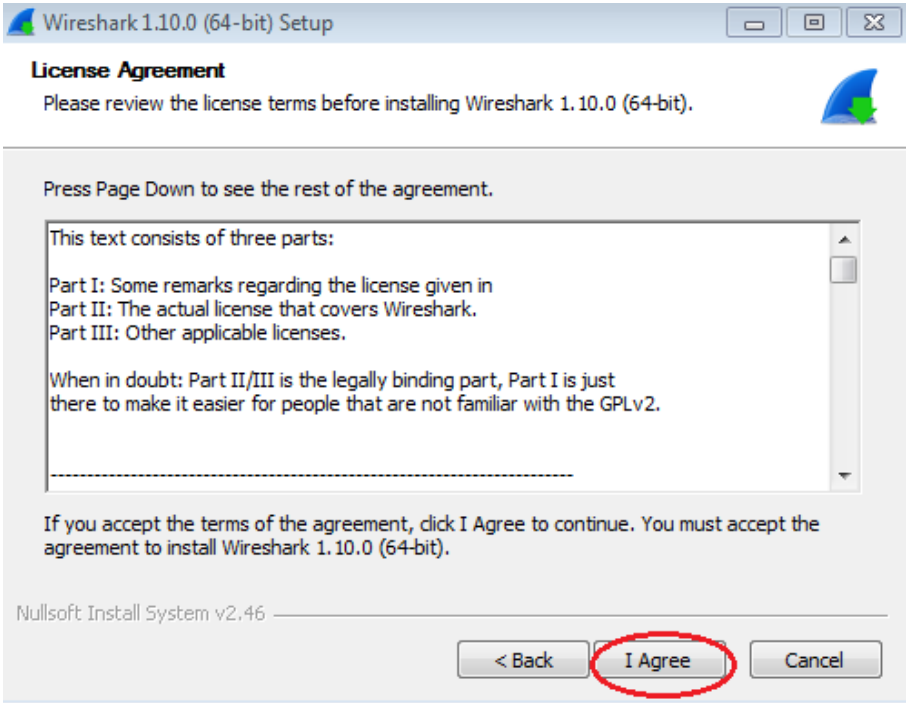
b. Ответьте на все сообщения безопасности, которые появятся на экране. Если на вашем ПК уже имеется копия Wireshark, перед установкой программы появится запрос на удаление прежней версии. Рекомендуется удалить старую версию программы перед установкой новой. Чтобы удалить предыдущую версию программы Wireshark, нажмите кнопку **Да**.



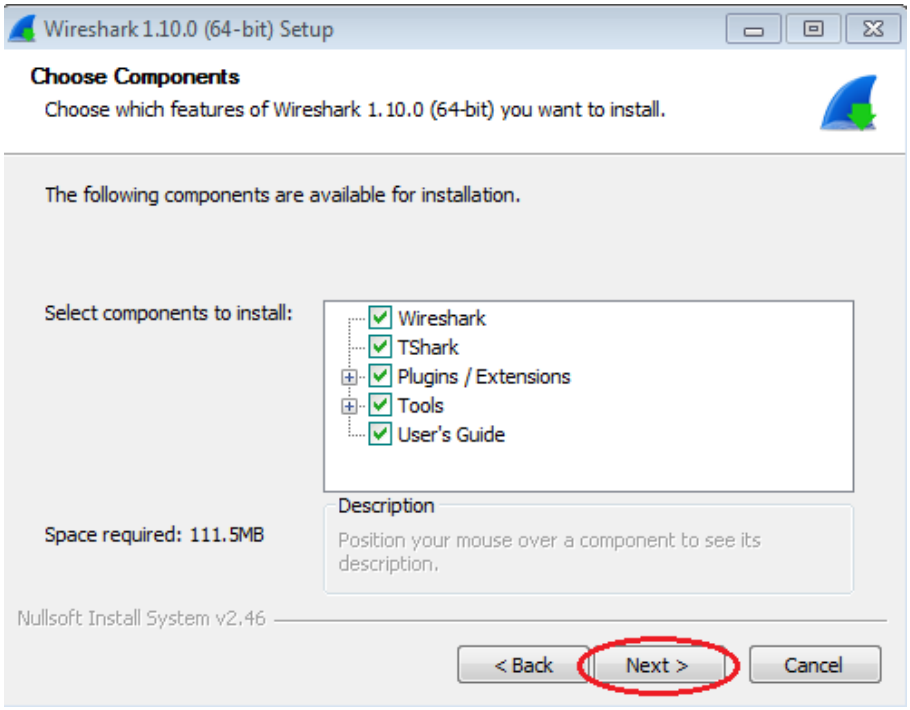
c. Если программа Wireshark устанавливается впервые или предыдущая версия была удалена, откроется мастер установки программы Wireshark. Нажмите кнопку **Next** (Далее).



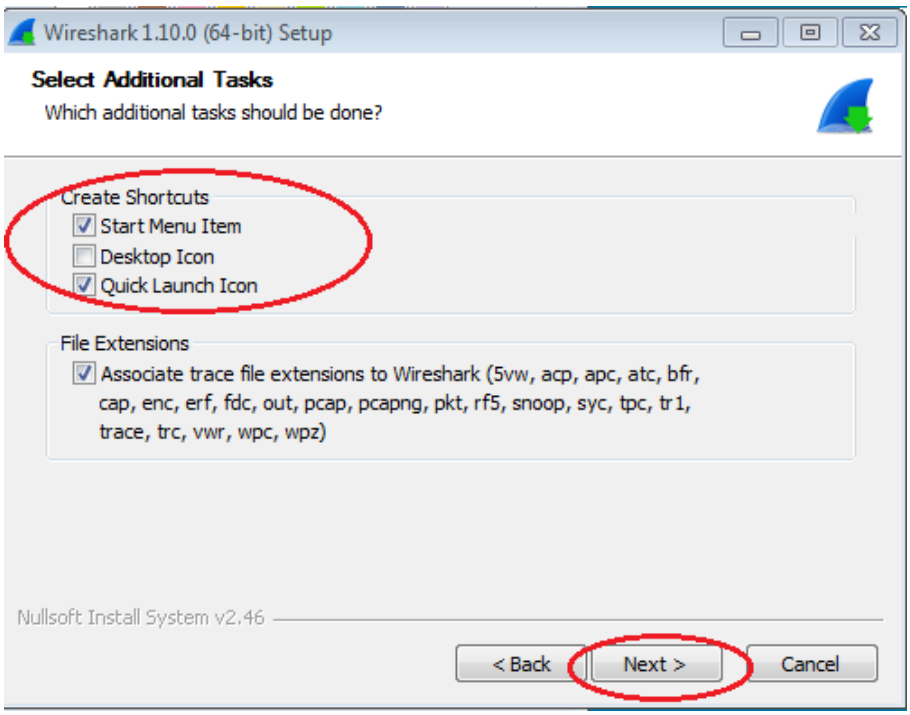
d. Выполните инструкции по установке. Когда откроется окно «License Agreement» (Лицензионное соглашение), нажмите кнопку **I accept** (Принять).



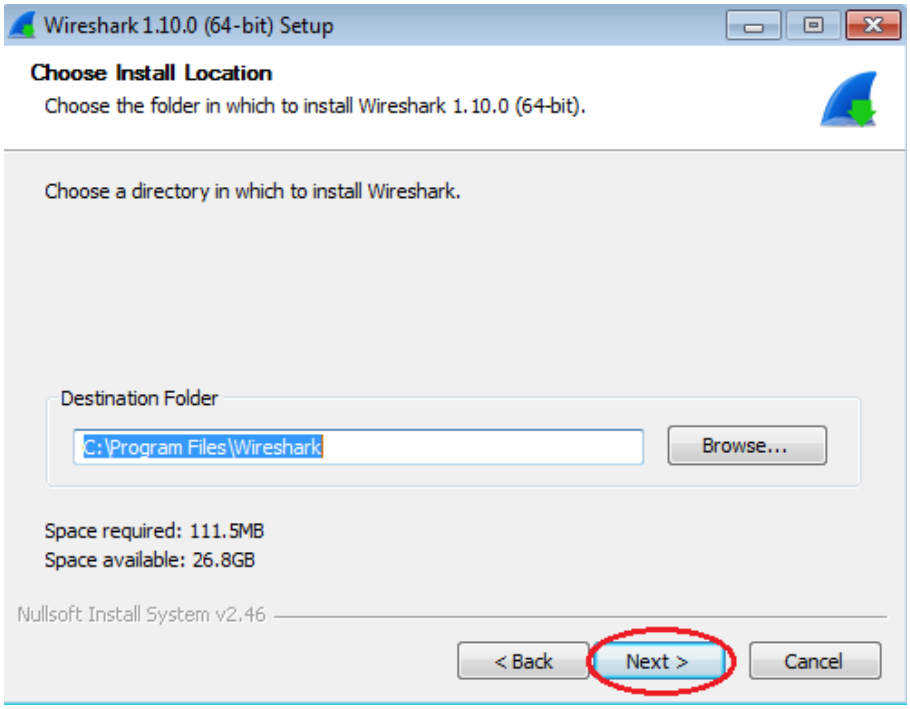
e. При выборе компонентов оставьте настройки по умолчанию и нажмите кнопку **Next** (Далее).



f. Выберите желаемые ярлыки и нажмите кнопку **Next** (Далее).

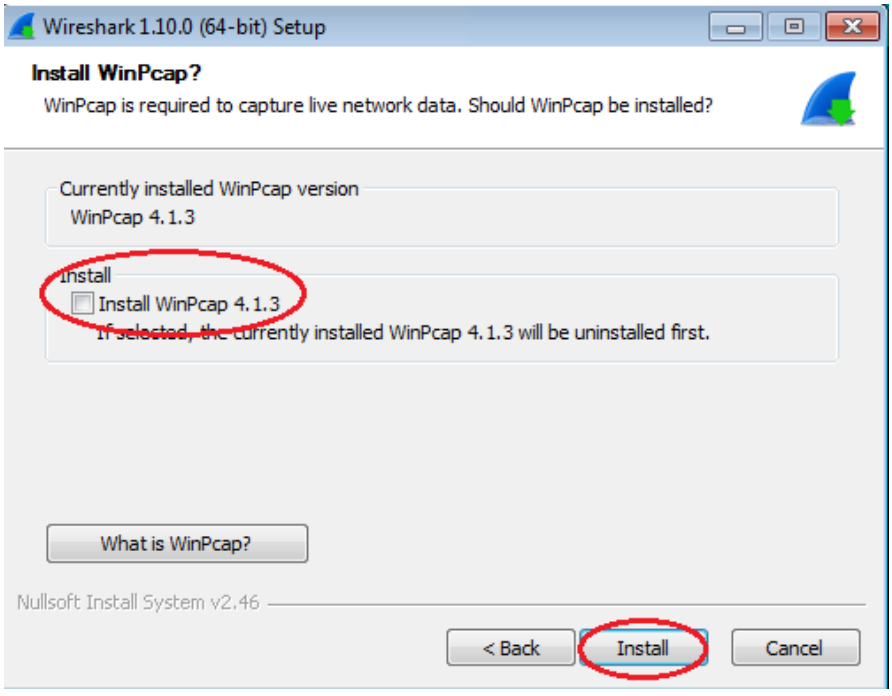


g. Если дисковое пространство ограничено, директорию установки можно изменить, в противном случае, оставьте адрес, указанный по умолчанию.

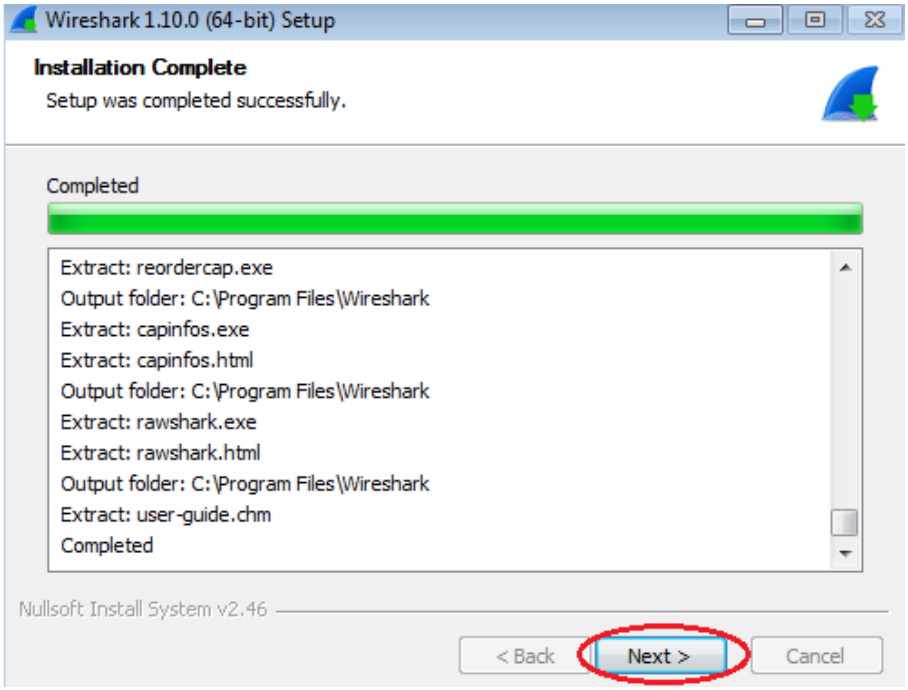


h. Для сбора сетевых данных на ваш ПК необходимо установить программу WinPcap. Если она уже установлена, флажок установки будет снят. Если установленная версия WinPcap старше версии, прилагаемой к программе Wireshark, рекомендуем установить более новую версию, нажав на флажок рядом с вариантом **Install WinPcap x.x.x** (Установить WinPcap x.x.x).

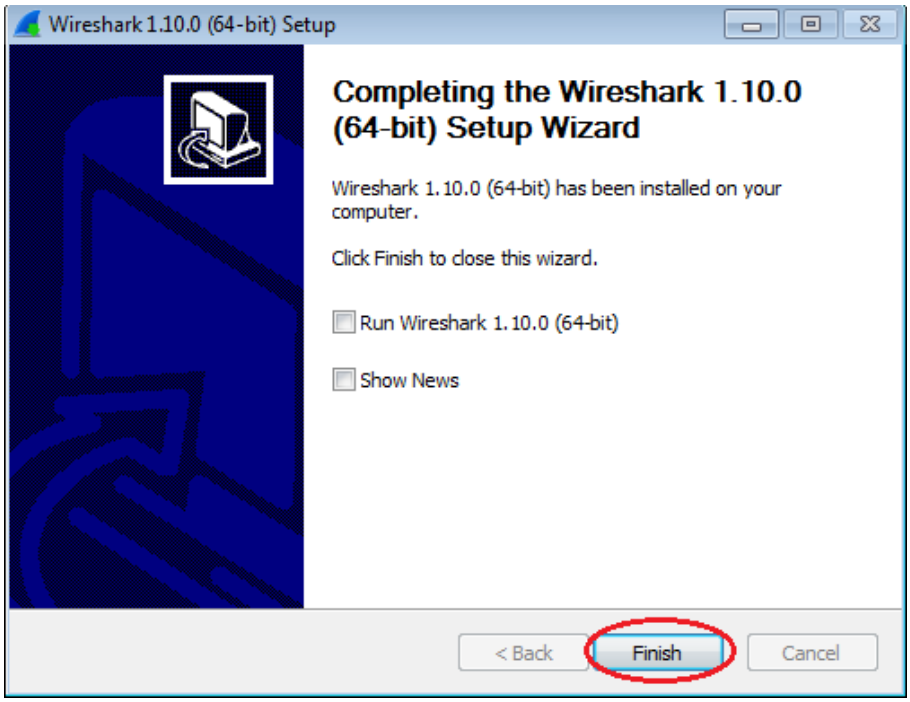
i. Если установка прошла успешно, закройте мастер установки WinPcap.



j. После этого начнётся установка программы Wireshark. Статус установки будет отображаться в отдельном окне. По завершении установки нажмите кнопку **Next** (Далее).



k. Для завершения процесса установки программы Wireshark нажмите **Finish** (Готово).



Часть 2: Сбор и анализ данных протокола ICMP по локальным узлам в программе Wireshark

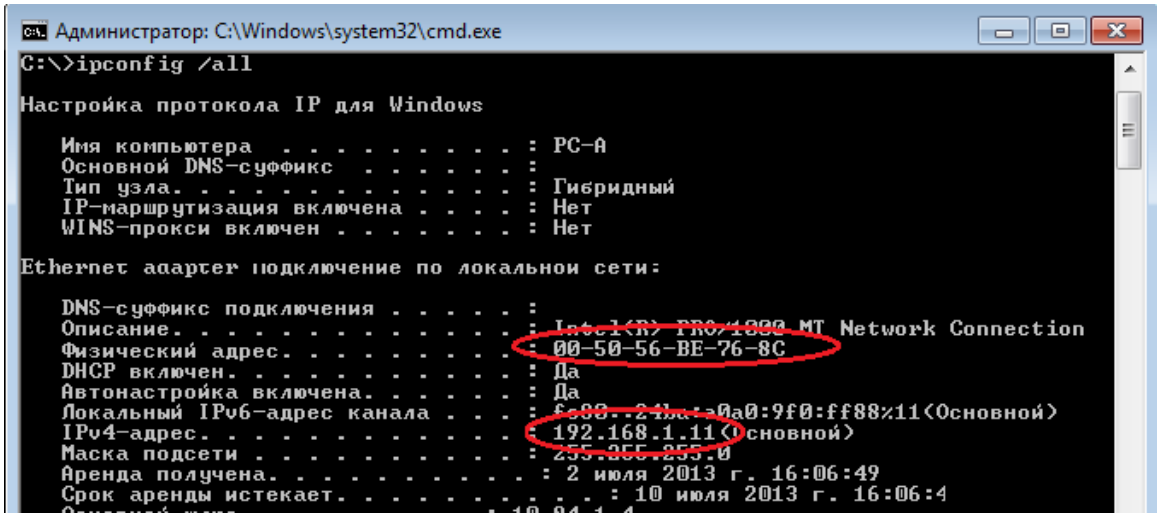
В части 2 этой лабораторной работы вы должны отправить эхо-запрос с помощью команды ping на другой ПК в локальной сети и перехватить ICMP-запросы и отклики в программе Wireshark. Кроме того, вам нужно найти необходимую информацию в собранных кадрах. Этот анализ поможет понять, как используются заголовки пакетов для передачи данных по месту назначения.

Шаг 1: Определите адреса интерфейсов вашего ПК.

В данной лабораторной работе вам необходимо узнать IP-адрес компьютера и физический адрес сетевого адаптера, который называется MAC-адресом.

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

b. Запишите IP-адрес интерфейса ПК и MAC-адрес (физический адрес).

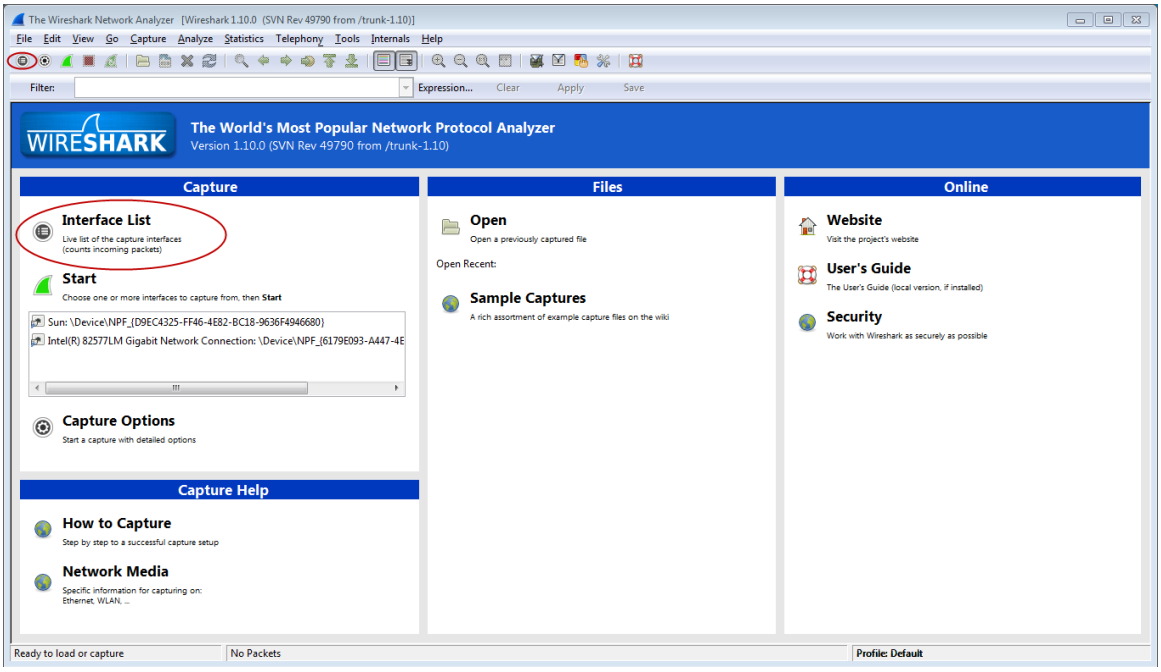


c. Обменяйтесь IP-адресами с другими учащимися, но пока что не сообщайте им свой MAC-адрес.

Шаг 2: Запустите программу Wireshark и начните перехват данных.

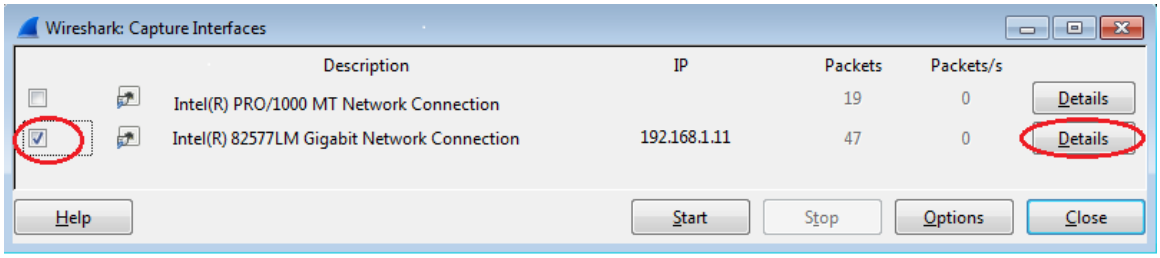
a. На своём ПК нажмите кнопку **Пуск** и найдите Wireshark в списке программ. Дважды нажмите на **Wireshark**.

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

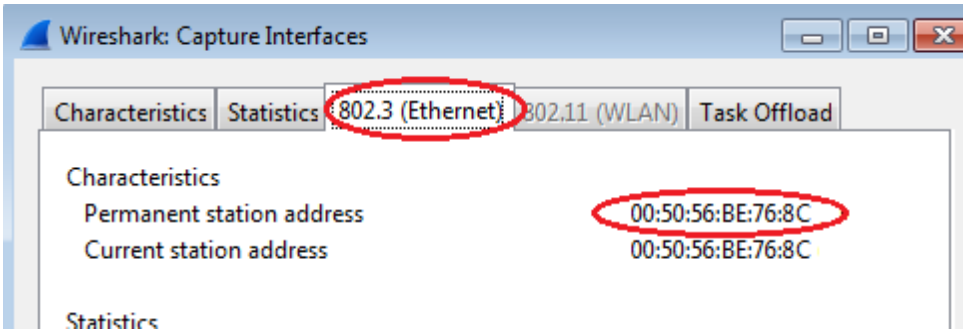


Примечание. Список интерфейсов можно также открыть, нажав на значок первого интерфейса в ряду значков.

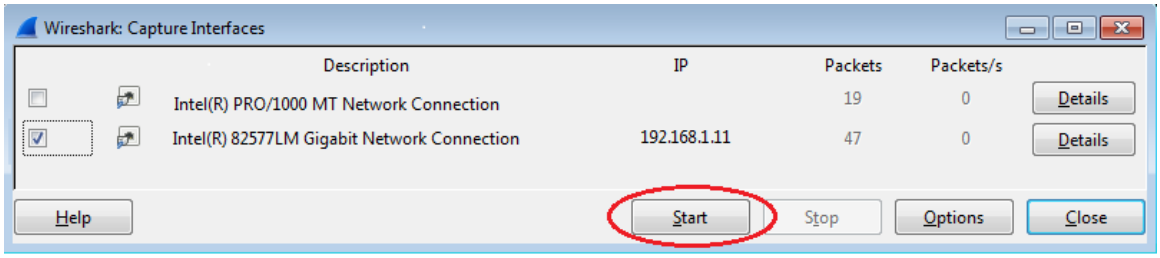
c. В окне «Capture Interfaces» (Перехват интерфейсов) программы Wireshark установите флажок рядом с интерфейсом, подключённым к вашей локальной сети.



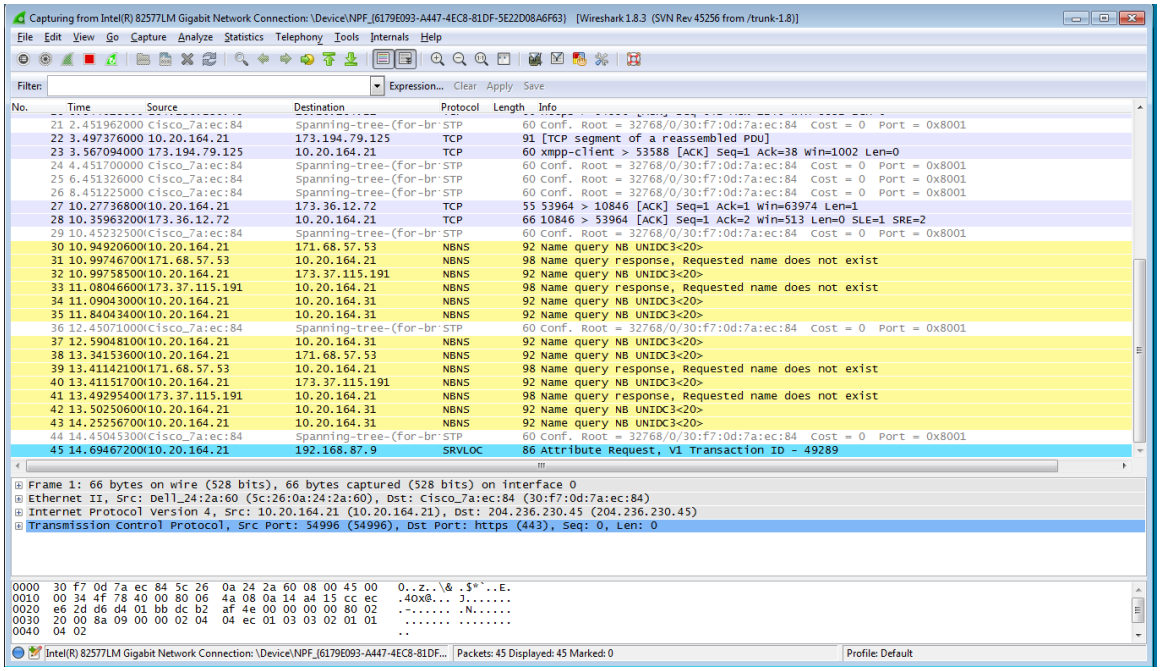
Примечание. Если перечислено несколько интерфейсов и вы не уверены в том, какой из них нужно выбрать, нажмите кнопку **Details** (Подробнее) и откройте вкладку **802.3 (Ethernet).** Убедитесь в том, что MAC-адрес соответствует результату, который вы получили в шаге 1b. Убедившись в правильности интерфейса, закройте окно информации.



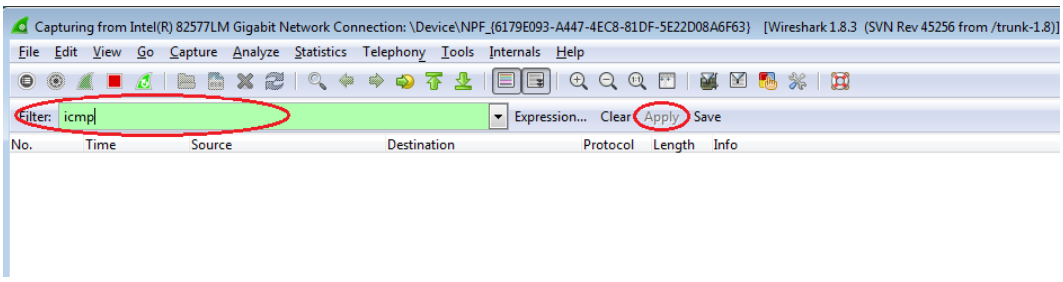
d. После этого нажмите кнопку **Start** (Начать), чтобы начать перехват данных.



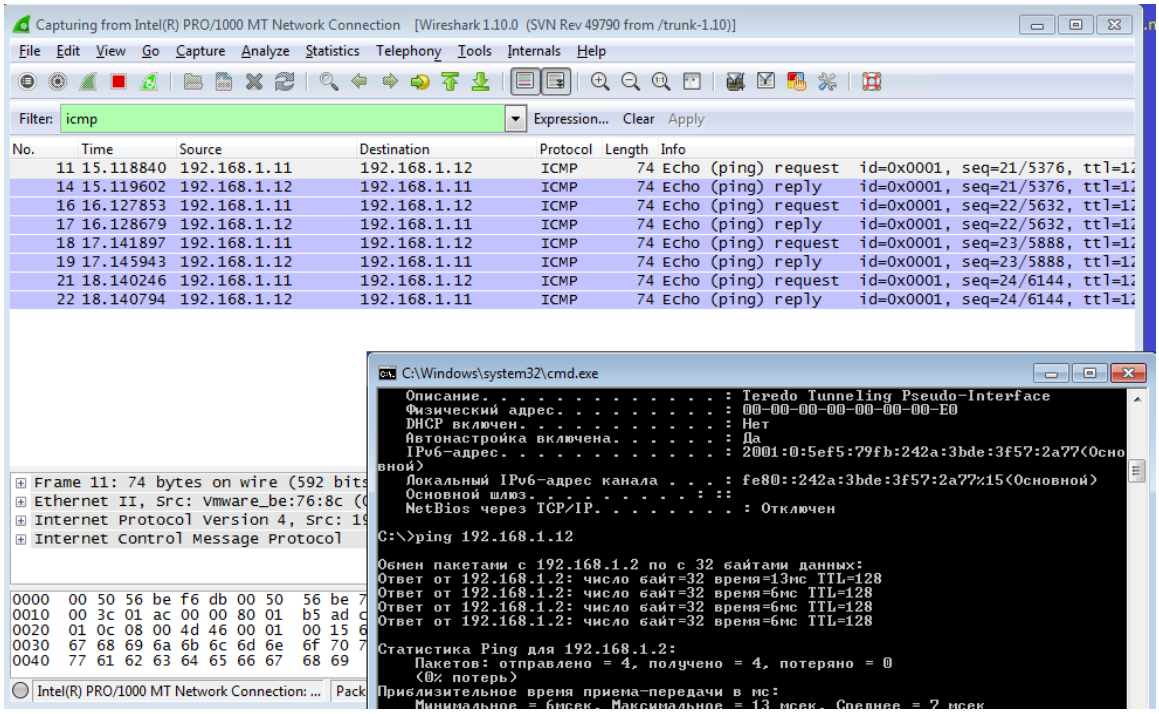
В верхней части окна программы Wireshark начнёт прокручиваться информация. Строки данных выделяются различными цветами в зависимости от протокола.



e. Информация может прокручиваться очень быстро в зависимости от типа связи между ПК и локальной сетью. Чтобы облегчить просмотр и работу с данными, собранными программой Wireshark, можно применить фильтр. В этой лабораторной работе нам нужны только протокольные блоки данных (PDU) ICMP (эхо-запрос с помощью команды ping). Чтобы вывести на экран только протокольные блоки данных ICMP (эхо-запрос с помощью команды ping), в поле фильтра в верхней части окна программы Wireshark введите **icmp** и нажмите клавишу ВВОД или кнопку **Apply** (Применить).

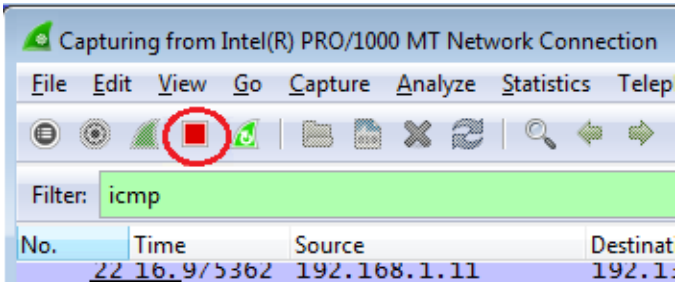


f. После этого все данные в верхнем окне исчезнут, однако перехват трафика в интерфейсе продолжится. Откройте окно командной строки, которое вы открывали ранее, и отправьте эхо-запрос с помощью команды ping на IP-адрес, полученный от другого учащегося. Обратите внимание на то, что в верхней части окна программы Wireshark снова появятся данные.



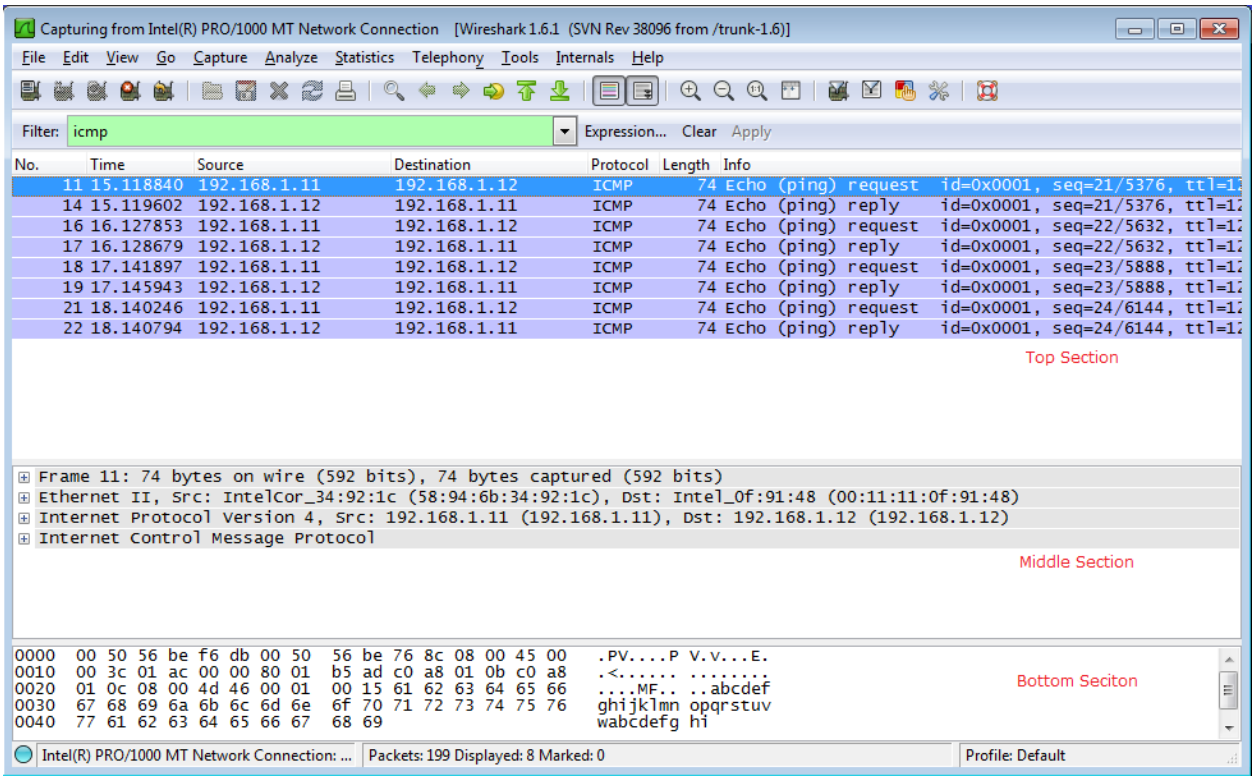
Примечание. Если компьютеры других учащихся не отвечают на ваши эхо-запросы, это может быть вызвано тем, что брандмауэры их компьютеров блокируют эти запросы. Информацию о том, как пропустить трафик ICMP через брандмауэр на ПК с ОС Windows 7, содержит Приложение A. Пропуск трафика ICMP через брандмауэр.

g. Остановите перехват данных, нажав на значок **Stop Capture** (Остановить перехват).

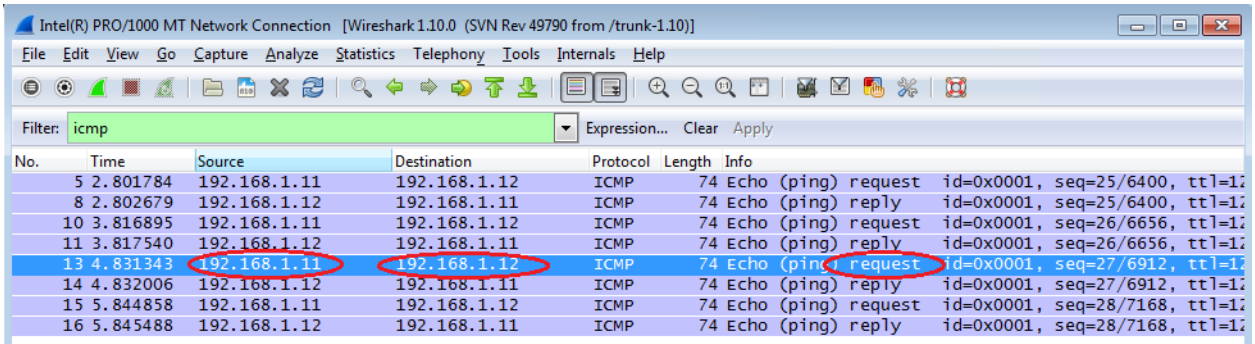


Шаг 3: Изучите полученные данные.

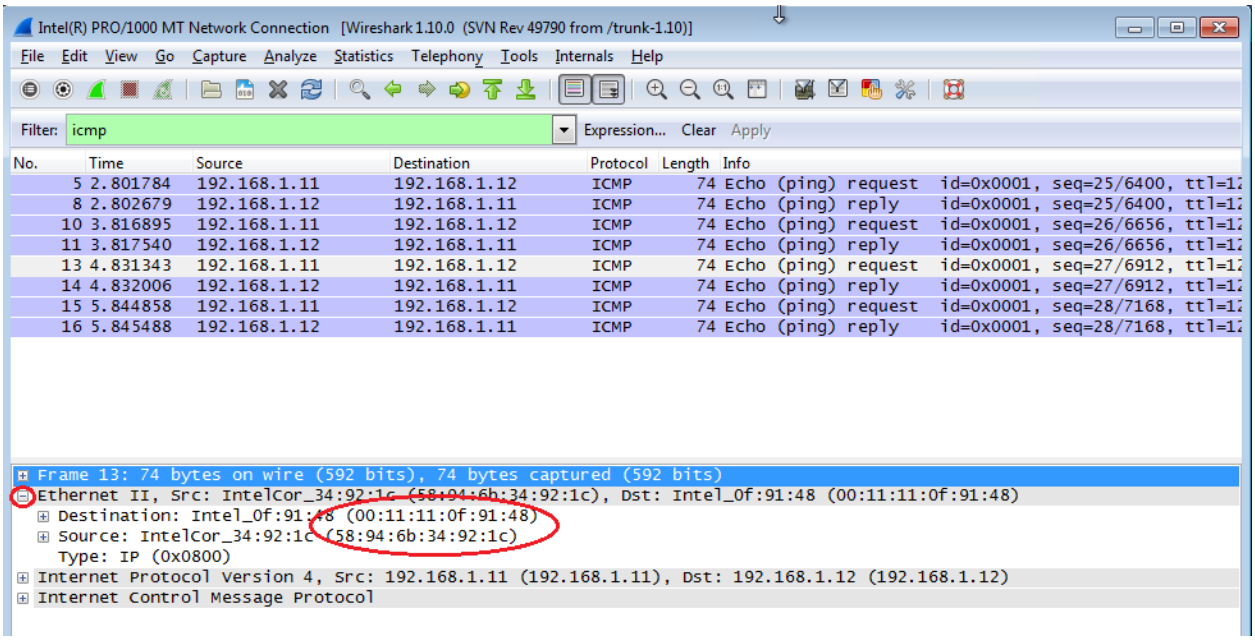
В шаге 3 необходимо проверить данные, сформированные эхо-запросами с помощью команды ping ПК других учащихся. Программа Wireshark отображает данные в трёх разделах: 1) в верхнем разделе отображается список полученных кадров PDU со сводной информацией об IP-пакетах; 2) в среднем разделе приводится информация о PDU для кадра, выбранного в верхнем разделе экрана, и деление кадра PDU на слои протоколов; 3) в нижнем разделе показываются необработанные данные каждого уровня. Необработанные данные отображаются как в шестнадцатеричном, так и десятичном форматах.



a. Выберите PDU-кадры первого запроса ICMP в верхнем разделе окна программы Wireshark. Обратите внимание на то, что в столбце Source (Источник) указывается IP-адрес вашего компьютера, а в столбце «Destination» (Назначение) — IP-адрес ПК, которому вы отправили эхо-запрос с помощью команды ping.



b. Не меняя выбор PDU-кадра в верхнем разделе программы, перейдите в средний раздел. Нажмите на символ + слева от строки «Ethernet II», чтобы увидеть MAC-адреса источника и назначения.



Совпадает ли MAC-адрес источника с интерфейсом вашего компьютера?

Совпадает ли MAC-адрес назначения в программе Wireshark с MAC-адресом другого учащегося?

Как ваш ПК вычислил MAC-адрес ПК, на который был отправлен эхо-запрос с помощью команды ping?

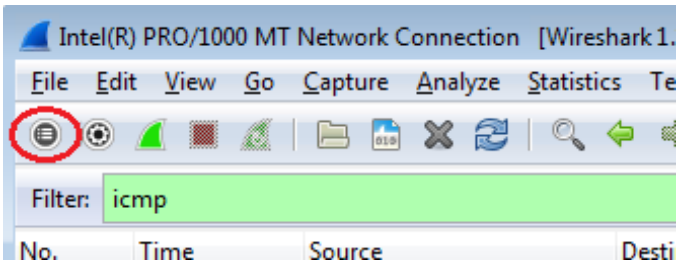
Примечание. В предыдущем примере перехваченного ICMP-запроса данные протокола ICMP инкапсулируются внутри PDU-пакета IPv4 (заголовка IPv4), который затем инкапсулируется в пакете кадра Ethernet II (заголовок Ethernet II) для передачи по локальной сети.

Часть 3: Сбор и анализ данных протокола ICMP по удалённым узлам в программе Wireshark

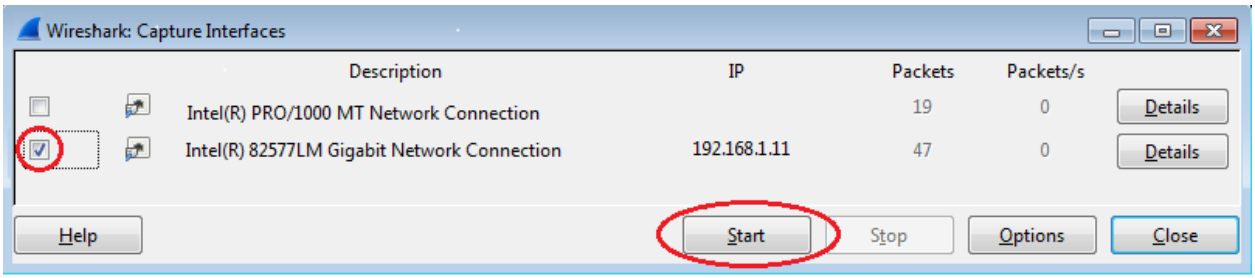
В части 3 вы должны будете отправить эхо-запросы с помощью команды ping на удалённые узлы (узлы за пределами локальной сети) и изучить данные, сформированные этими запросами. Затем вы определите различия между этими данными и данными, изученными в части 2.

Шаг 1: Запустите перехват данных в интерфейсе.

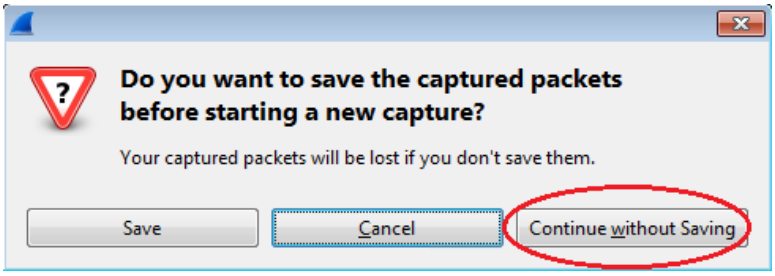
a. Нажмите на значок **Interface List** (Список интерфейсов), чтобы снова открыть список интерфейсов ПК.



b. Убедитесь в том, что напротив интерфейса локальной сети установлен флажок, и нажмите кнопку **Start** (Начать).

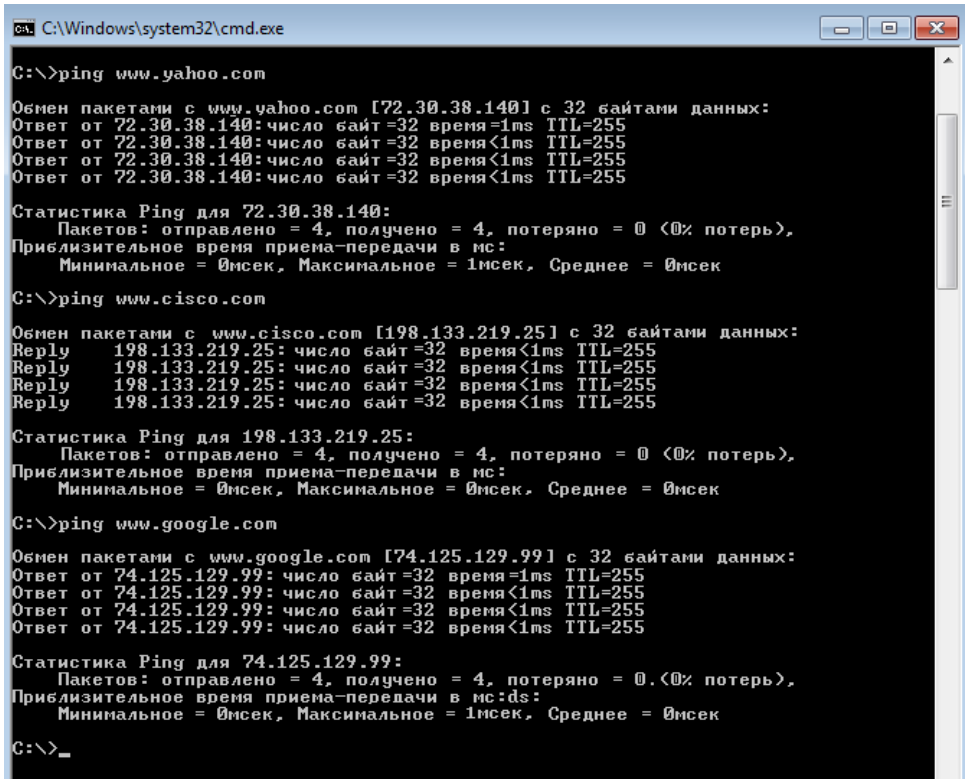


c. Появится окно с предложением сохранить полученные ранее данные перед началом нового перехвата. Сохранять эти данные необязательно. Нажмите кнопку **Continue withoutSaving** (Продолжить без сохранения).



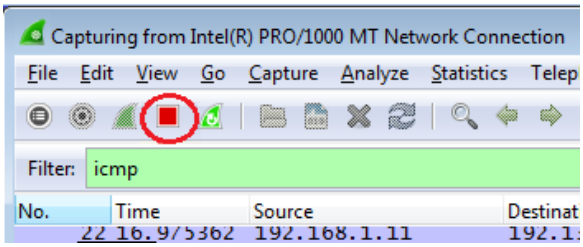
d. Активировав перехват данных, отправьте эхо-запрос с помощью команды ping на следующие три URL-адреса:

1) www.yahoo.com
2) www.cisco.com
3) www.google.com



Примечание. При отправке эхо-запросов с помощью команды ping на указанные URL-адреса обратите внимание на то, что служба доменных имен (DNS) преобразует URL в IP-адрес. Запишите IP-адреса, полученные для каждого URL-адреса.

e. Остановите перехват данных, нажав на значок **Stop Capture** (Остановить перехват).



Шаг 2: Изучите и проанализируйте данные, полученные от удалённых узлов.

a. Просмотрите собранные данные и изучите IP- и MAC-адреса трёх запрошенных веб-сайтов. Ниже укажите IP- и MAC-адреса назначения для всех трех веб-сайтов.

1адрес:IP: MAC:

2адрес:IP: MAC:

3адрес:IP: MAC:

b. Какова особенность этих данных?

c. Как эта информация отличается от данных, полученных в результате эхо-запросов локальных узлов в части 2?

Вопросы на закрепление

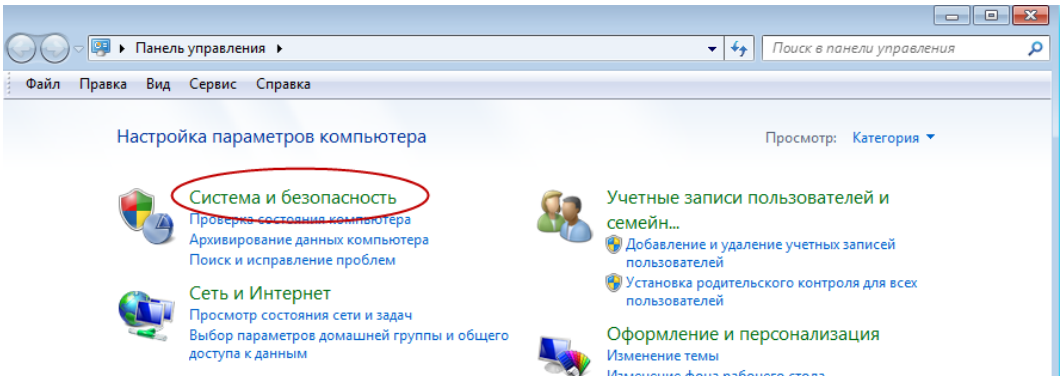
Почему программа Wireshark показывает фактический MAC-адрес локальных узлов, но не фактический MAC-адрес удалённых узлов?

Приложение A. Пропуск трафика ICMP через брандмауэр

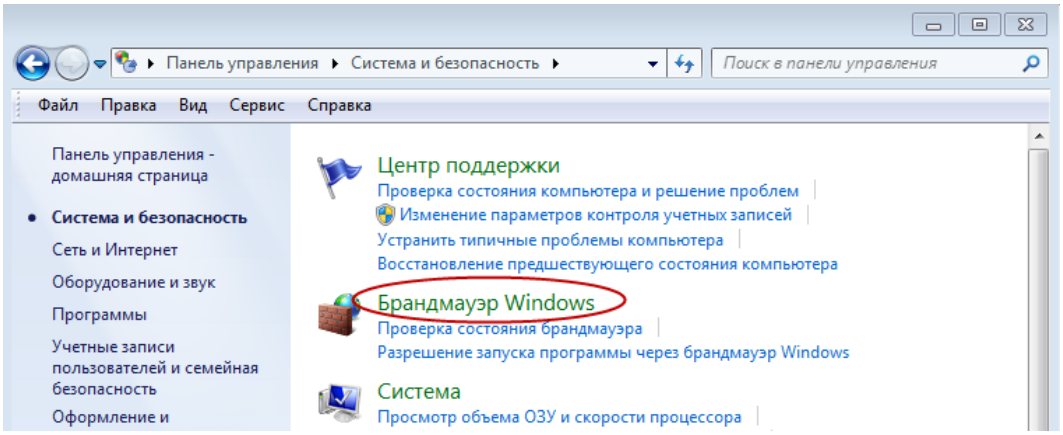
Если эхо-запросы с помощью команды ping с других компьютеров не проходят на ваш ПК, возможно, их блокирует брандмауэр. В этом приложении описывается, как пропустить эхо-запросы с помощью команды ping через брандмауэр и отменить новое правило брандмауэра по завершении лабораторной работы.

Шаг 1: Создайте новое правило, разрешающее прохождение ICMP-трафика через брандмауэр.

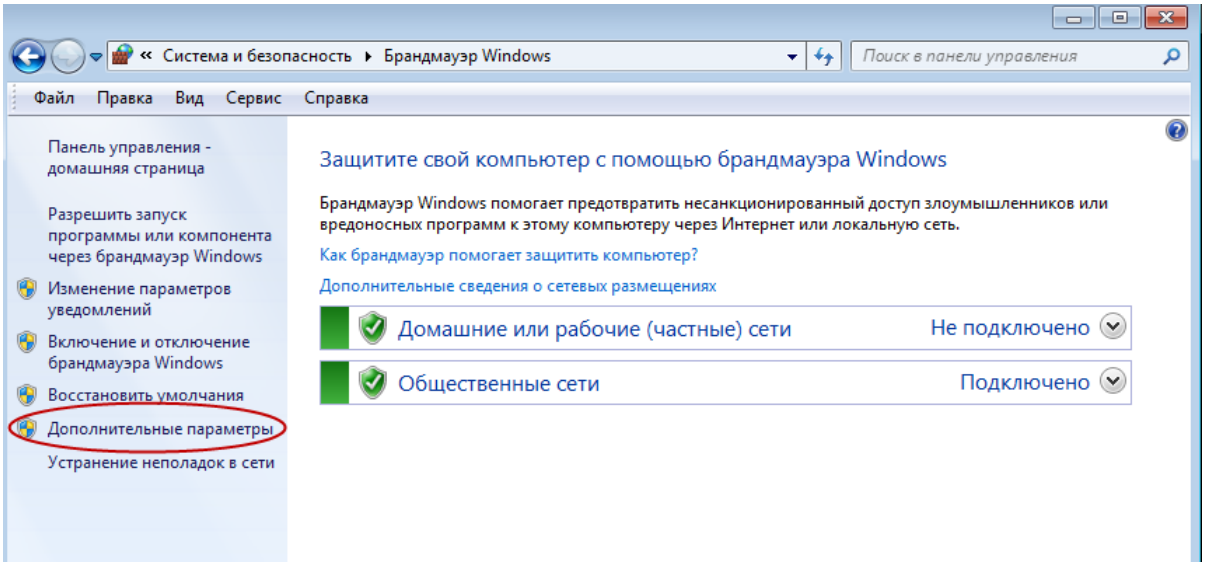
a. В панели управления выберите пункт **Система и безопасность**.



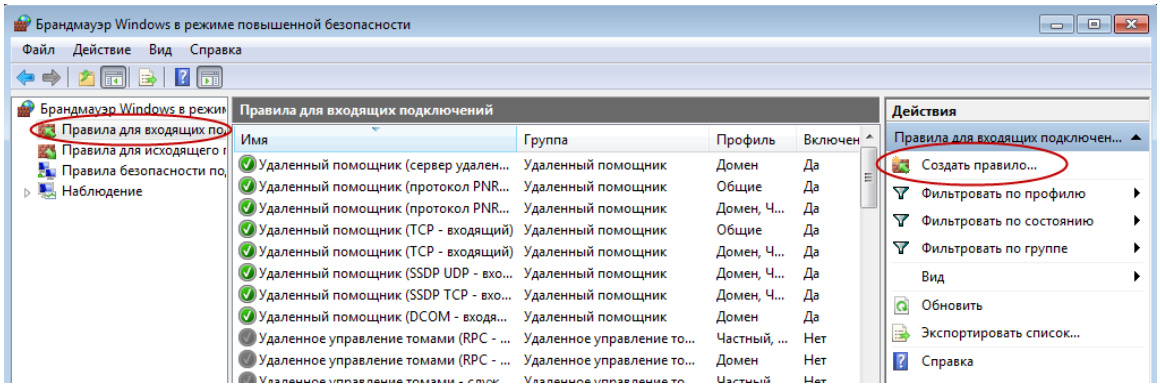
b. В окне «Система и безопасность» выберите **Брандмауэр Windows**.



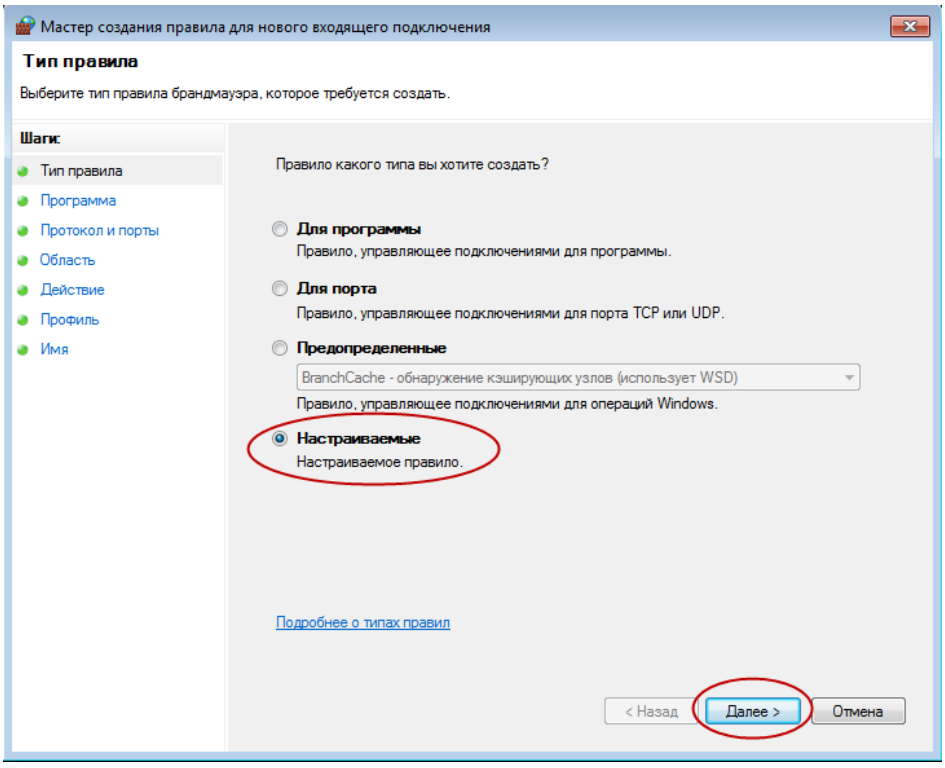
c. В левой части окна «Брандмауэр Windows» выберите **Дополнительные параметры**.



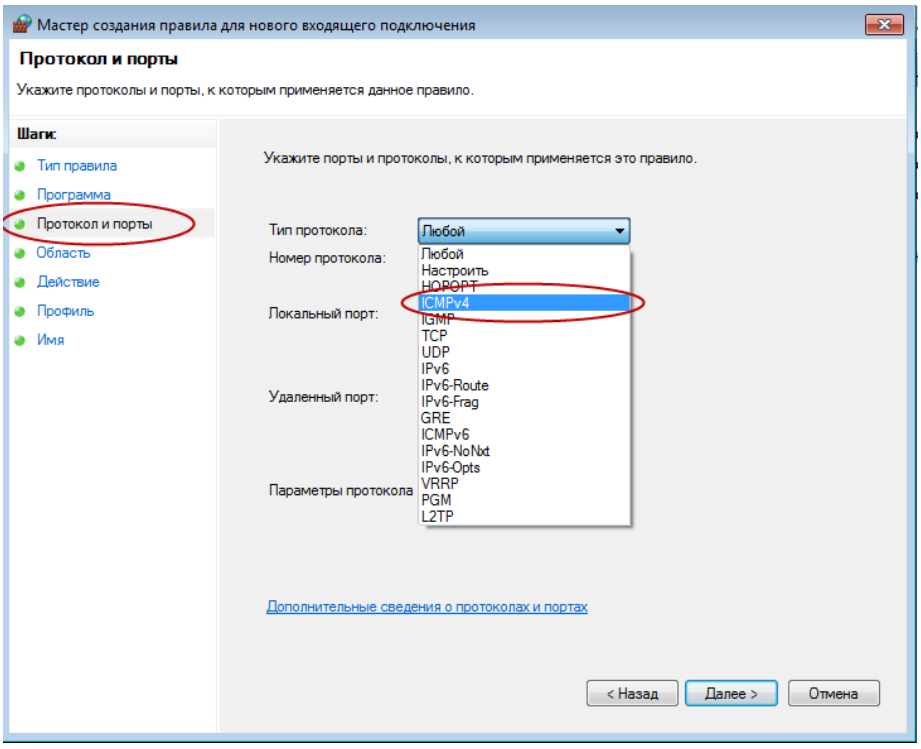
d. В окне «Дополнительные параметры» выберите в левой боковой панели **Правила для входящих подключений**, а затем **Создать правило...** в правой боковой панели.



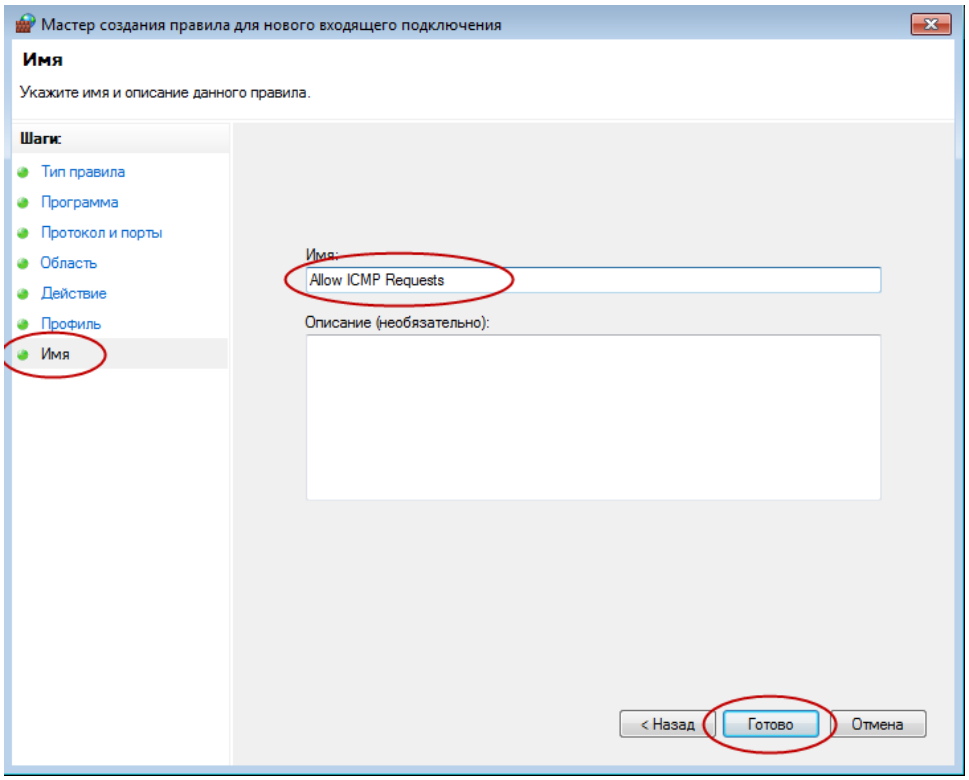
e. Откроется мастер создания новых правил для входящих подключений. В окне «Тип правила» установите переключатель **Настраиваемые**, и нажмите кнопку **Далее.**



f. В левой панели выберите **Протоколы и порты** и выберите пункт **ICMPv4** в раскрывающемся меню типов протокола. После этого нажмите кнопку **Далее**.



g. В левой панели выберите **Имя** и введите в соответствующее поле **Allow ICMP Requests.** Нажмите кнопку **Finish** (Готово).

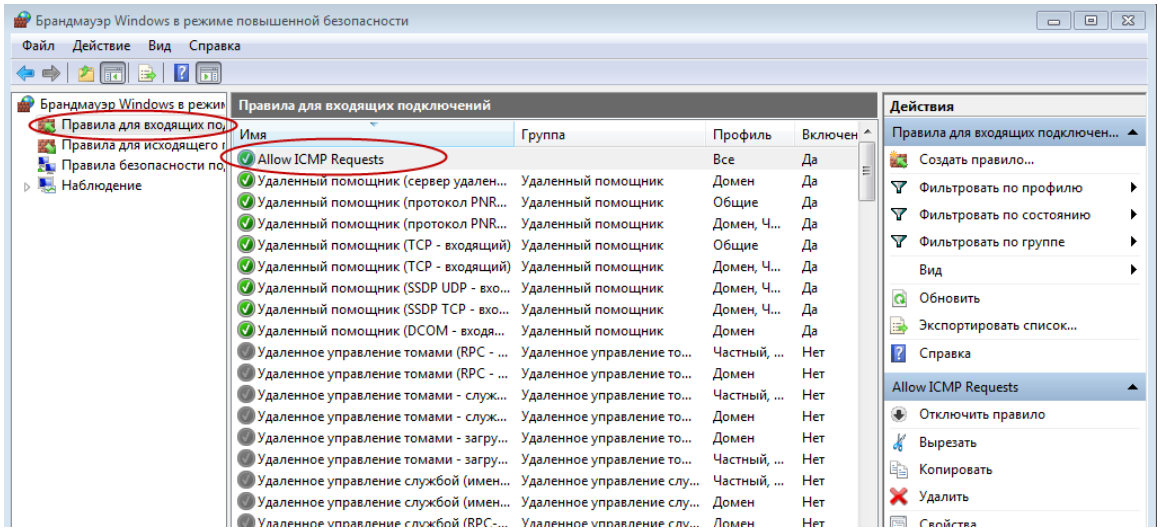


Созданное правило позволит другим учащимся получать эхо-отклики с вашего ПК.

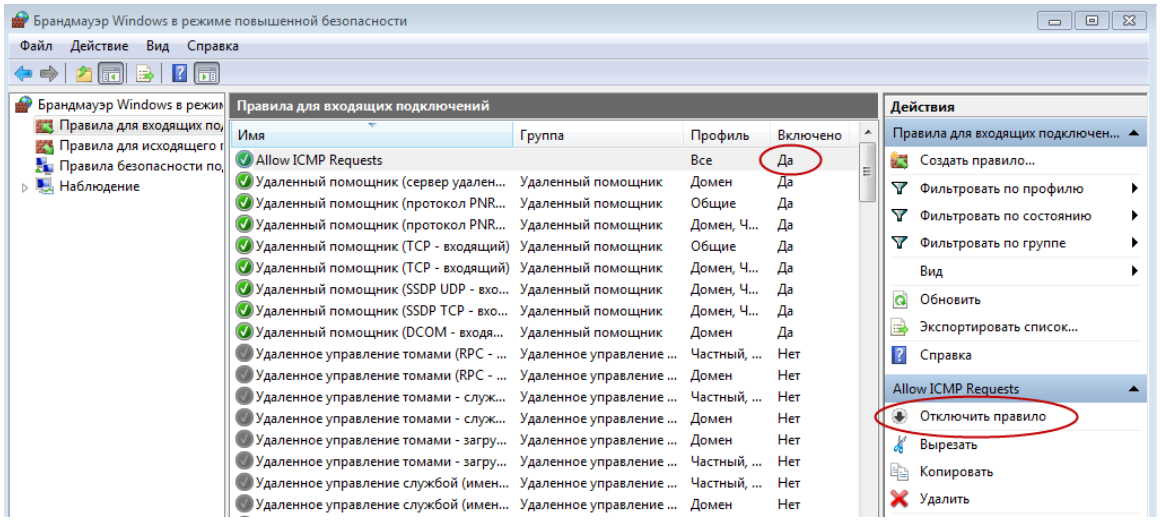
Шаг 2: Отключите и удалите новое правило ICMP.

По завершении лабораторной работы необходимо отключить или удалить новое правило, созданное в шаге 1. Вариант **Отключить правило** позволит снова включить его при необходимости. Полное удаление правила навсегда удалит его из списка правил для входящих подключений.

a. В левой части окна «Дополнительные настройки безопасности» выберите **Правила для входящих подключений** и найдите правило, созданное в шаге 1.



b. Чтобы отключить правило, выберите вариант **Отключить правило**. После этого она изменится на вариант **Включить правило**. Правило можно включать и отключать. Состояние правила отображается в столбце «Включено» списка правил для входящих подключений.



c. Чтобы удалить правило ICMP навсегда, выберите вариант **Удалить**. После этого для разрешения запросов ICMP это правило нужно будет создать заново.