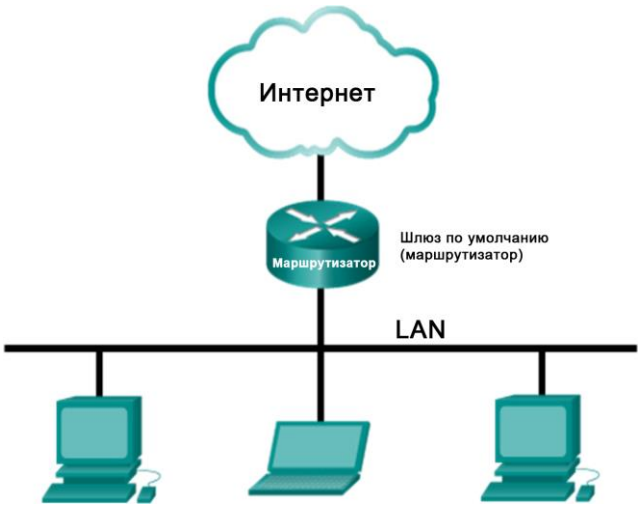
Использование программы Wireshark для просмотра сетевого трафика

Топология



Задачи

Часть 1. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в локальной сети

Часть 2. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в удаленную сеть

Общие сведения/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 «захватывает» каждую единицу данных протокола (PDU), после чего расшифровывает или анализирует ее 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 ходе лабораторной работы вы научитесь пользоваться программой Wireshark для захвата IP-адресов пакетов данных ICMP и MAC-адресов Ethernet-кадров.

Часть 1. Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в локальной сети

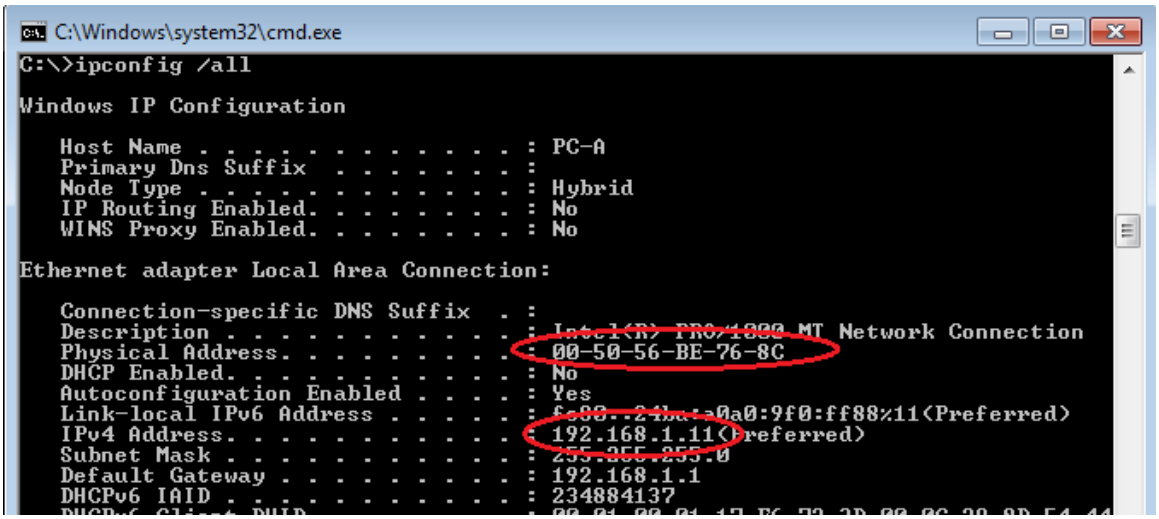
В части 1 необходимо отправить эхо-запрос с помощью команды ping на другой ПК в локальной сети и перехватить ICMP-запросы и отклики в программе Wireshark. Кроме того, вам нужно найти необходимую информацию в собранных кадрах. Этот анализ поможет понять, как заголовки пакетов позволяют доставлять данные адресатам.

Шаг 1: Определите адреса интерфейсов вашего ПК.

Вам необходимо узнать IP-адрес компьютера и физический адрес сетевой платы, который называется MAC-адресом.

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

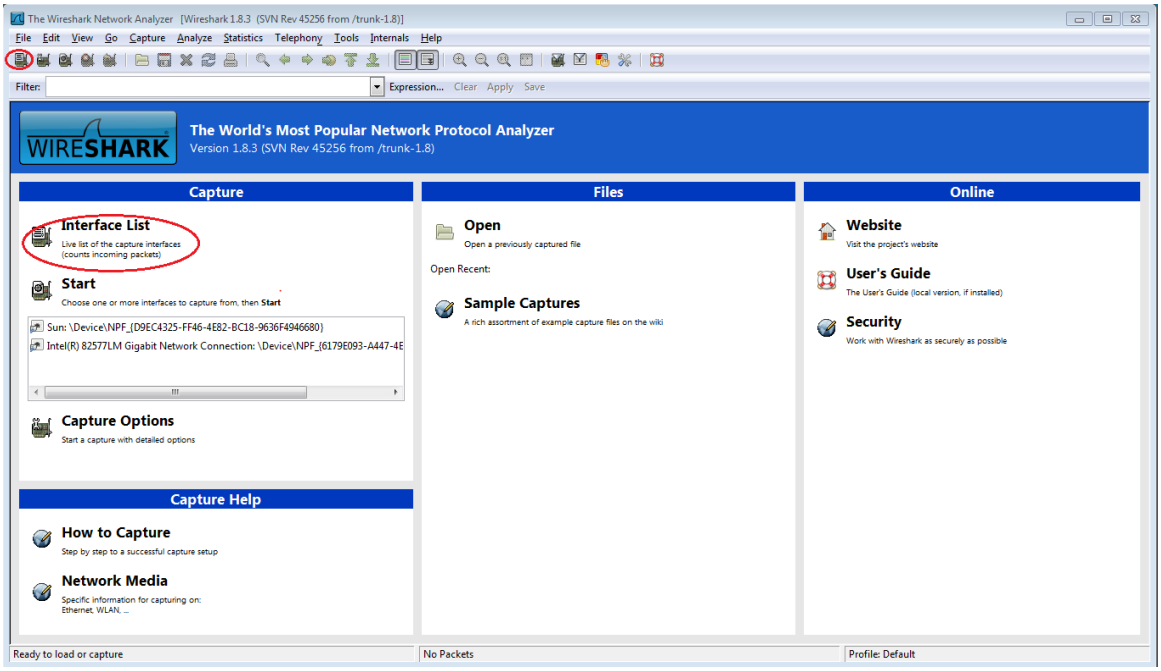
b. Запишите IP-адрес интерфейса ПК и MAC-адрес.



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

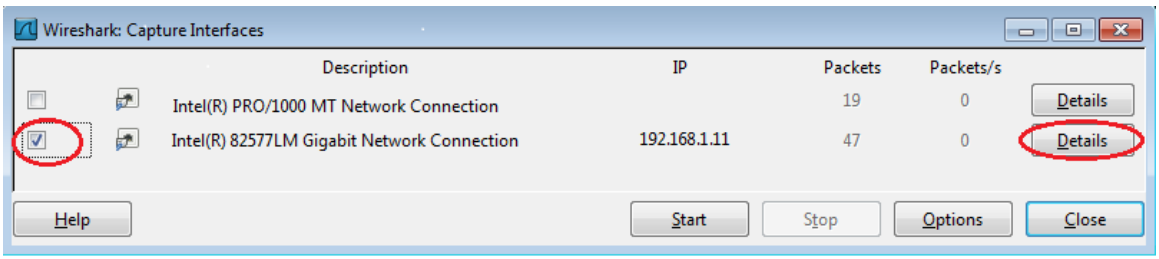
Шаг 2: Запустите программу Wireshark и начните сбор данных.

a. После запуска программы Wireshark нажмите на **Interface List** (Список интерфейсов).

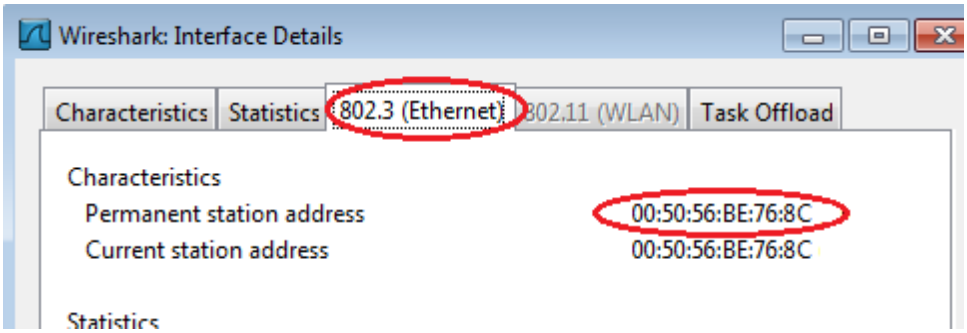


Примечание. Список интерфейсов можно также открыть, нажав на значок первого интерфейса в ряду значков.

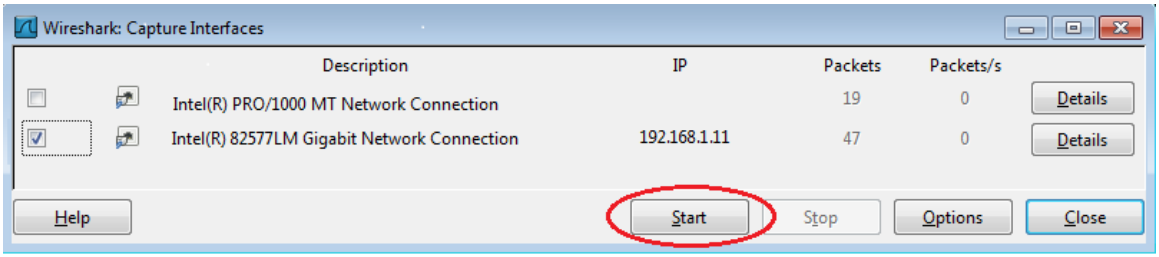
b. В окне Capture Interfaces (Захват интерфейсов) программы Wireshark установите флажок рядом с интерфейсом, подключенным к вашей локальной сети.



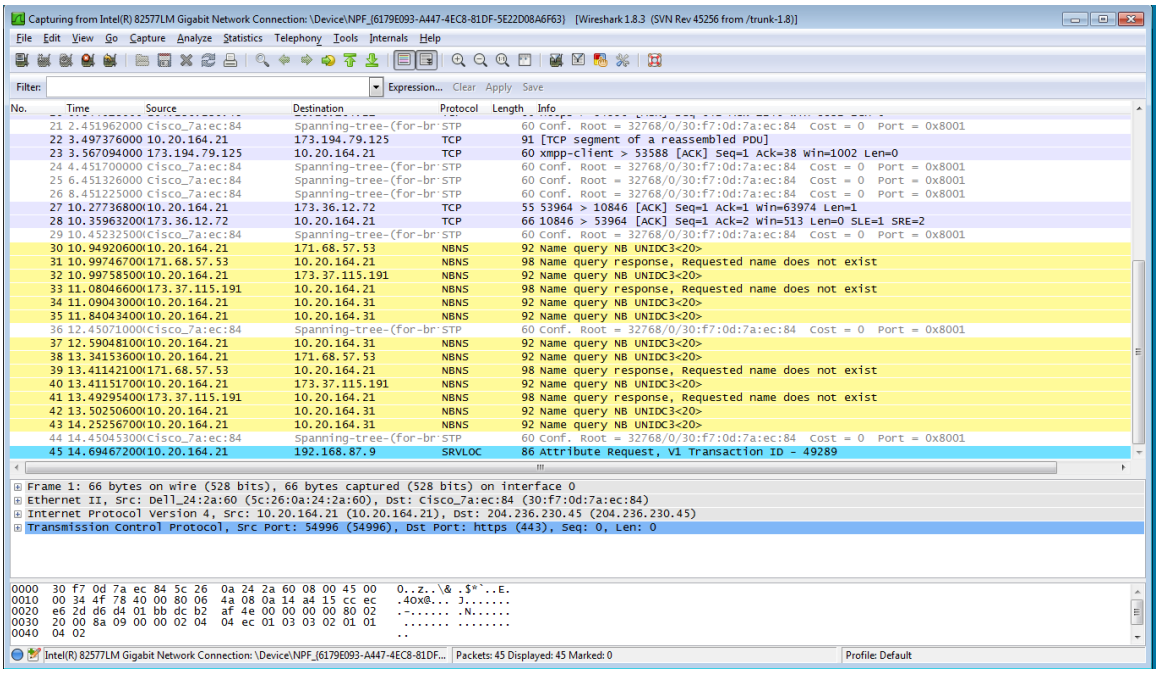
Примечание. Если перечислено несколько интерфейсов и вы не уверены в том, какой из них нужно выбрать, нажмите кнопку **Details** (Подробнее) и откройте вкладку **802.3 (Ethernet)**. Убедитесь в том, что MAC-адрес соответствует результату, который вы получили в шаге 1б. Убедившись в правильности интерфейса,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



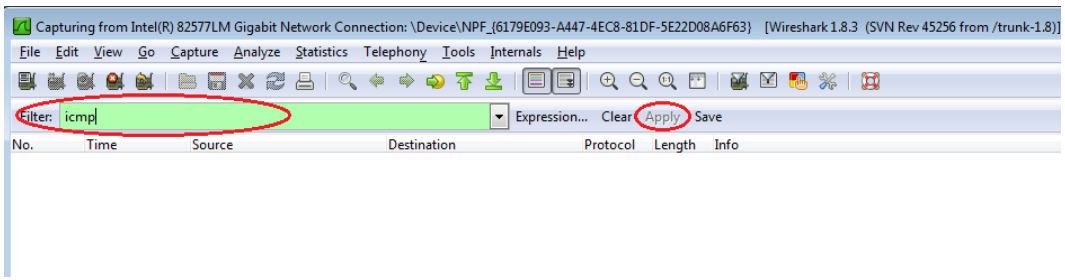
c. После этого нажмите кнопку **Start** (Начать), чтобы начать захват данных.



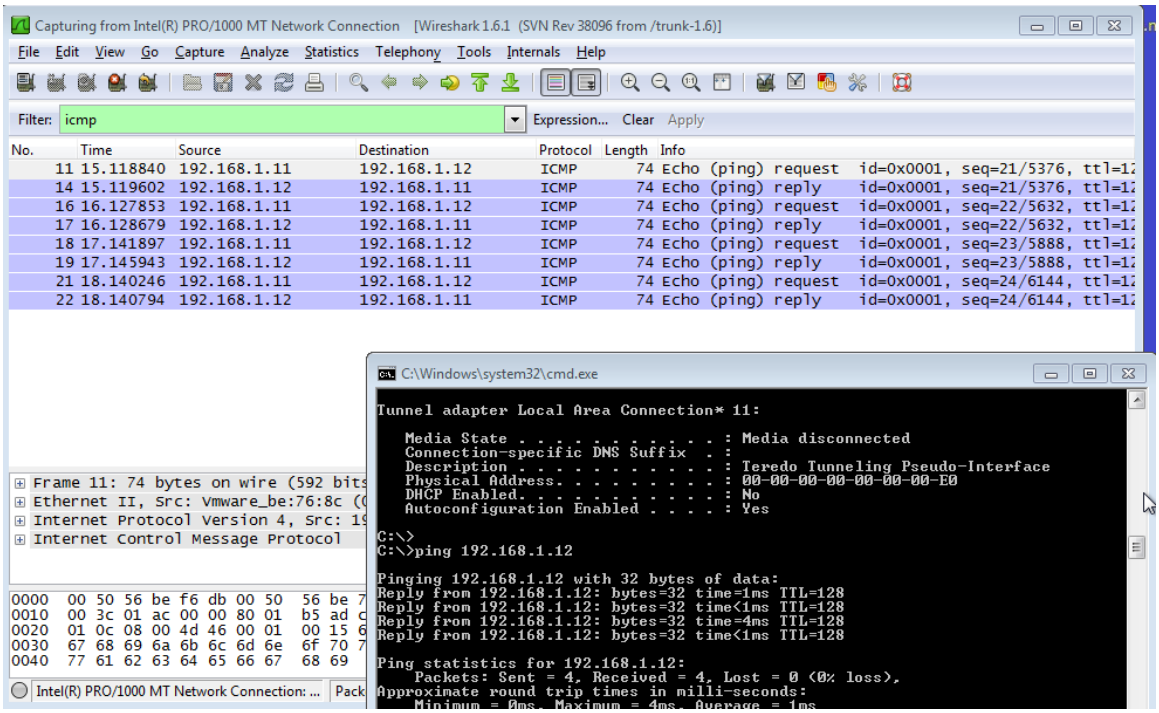
В верхней части окна программы Wireshark начнет прокручиваться информация. Строки данных выделяются различными цветами в зависимости от протокола.



d. Информация может прокручиваться очень быстро, это зависит от интенсивности взаимодействия ПК с локальной сетью. Чтобы облегчить просмотр и работу с данными, собранными программой Wireshark, можно применить фильтр. В этой лабораторной работе нас интересуют только единицы данных протокола (PDU) ICMP (эхо-запрос с помощью команды ping). Чтобы вывести на экран только единицы данных протокола ICMP (эхо-запрос с помощью команды ping), в поле фильтра в верхней части окна программы Wireshark введите **icmp** и нажмите клавишу ввода или кнопку **Apply** (Применить).

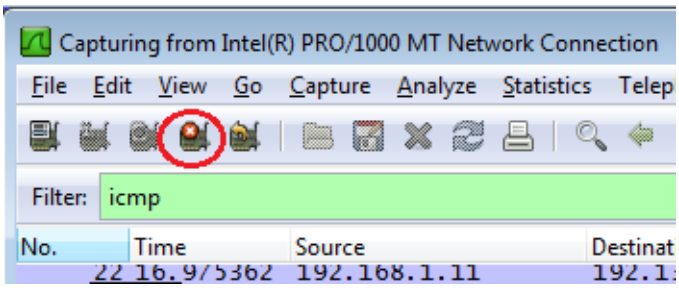


e. После этого все данные в верхнем окне исчезнут, однако захват трафика в интерфейсе продолжится. Откройте окно командной строки, которое вы открывали ранее, и отправьте эхо-запрос с помощью команды ping на IP-адрес, полученный от другого учащегося. Обратите внимание на то, что в верхней части окна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



Примечание. Если компьютеры других учащихся не отвечают на ваши эхо-запросы, это может быть вызвано тем, что межсетевые экраны их компьютеров блокируют эти запросы. Информацию о том, как обеспечить пропуск трафика ICMP через межсетевой экран на ПК с ОС Windows 7 см. в **Ошибка! Источник ссылки не найден.**.

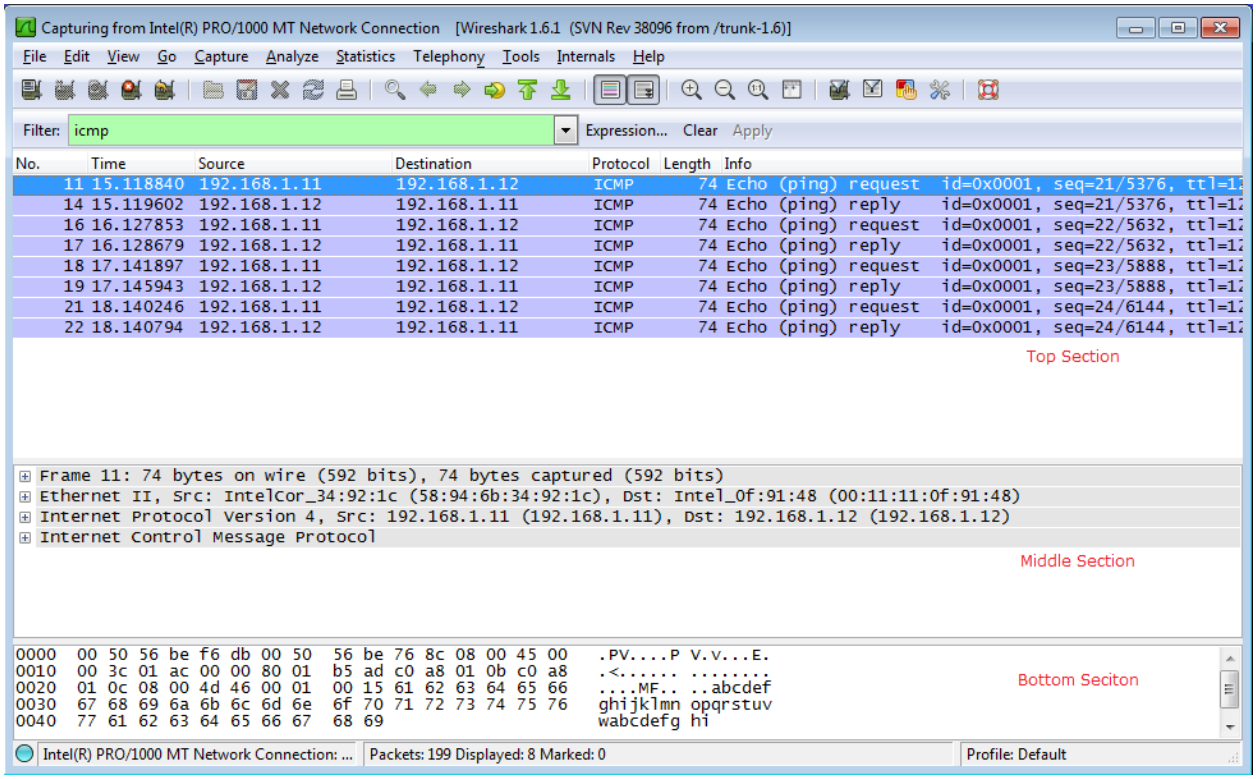
f. Остановите захват данных, нажав на значок **Stop Capture** (Остановить захват).



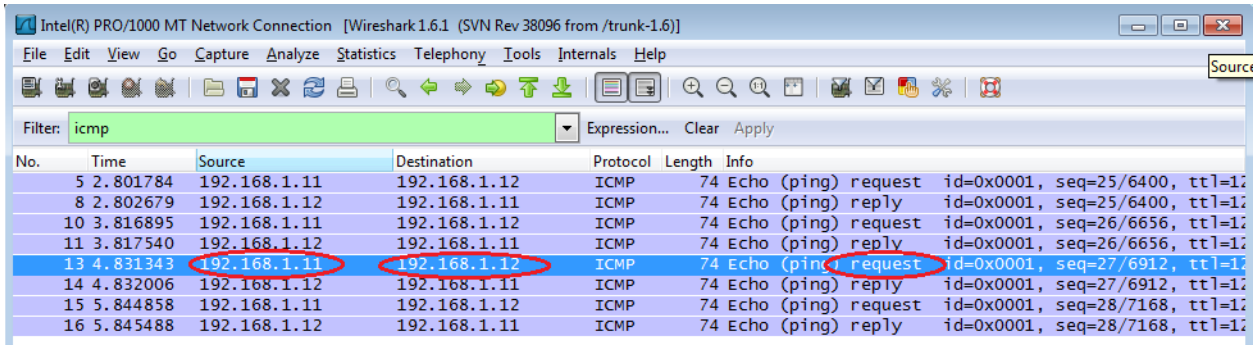
Шаг 3: Изучите полученные данные.

В шаге 3 необходимо проверить данные, сформированные эхо-запросами с помощью команды ping на ПК других учащихся. Программа Wireshark отображает данные в трех разделах: 1) в верхнем разделе отображается список полученных кадров PDU со сводной информацией об IP-пакетах; 2) в среднем разделе

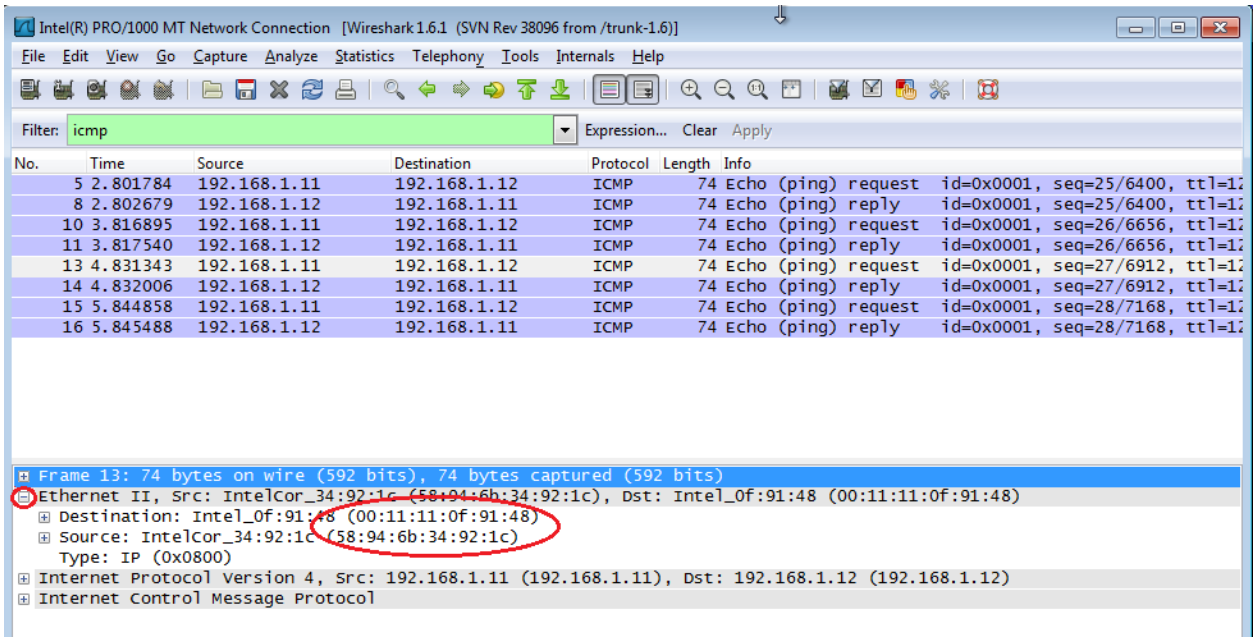
приводится информация о PDU для кадра, выбранного в верхней части экрана, а также разделение перехваченного кадра PDU по уровням протоколов; 3) в нижнем разделе показываются необработанные данные каждого уровня. Необработанные данные отображаются как в шестнадцатеричном, так и в десятичном форматах.



a. Выберите кадры PDU 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 другого участника, на который вы отправили эхо-запрос с помощью команды ping.



b. Не меняя выбор кадра PDU в верхнем разделе окна, 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 определил MAC-адрес другого ПК, на который был отправлен эхо-запрос с помощью команды ping?

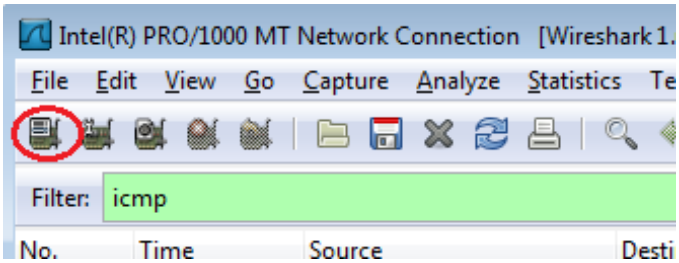
Примечание. В предыдущем примере захваченного ICMP-запроса данные протокола ICMP инкапсулируются внутри PDU пакета IPv4 (заголовка IPv4), который затем инкапсулируется в PDU кадра Ethernet II (заголовок Ethernet II) для передачи по локальной сети.

Часть 2: Сбор и анализ данных протокола ICMP в программе Wireshark при передаче данных в удаленную сеть

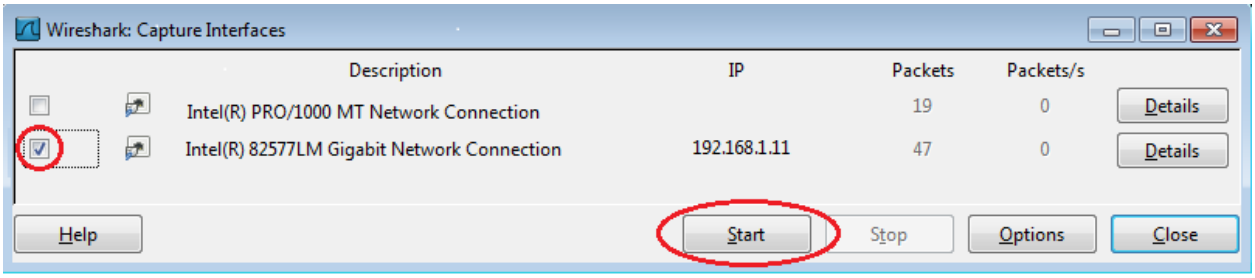
В части 2 вы должны будете отправить эхо-запросы с помощью команды ping на удаленные узлы (расположенные за пределами локальной сети) и изучить данные, сформированные этими запросами. Затем вам нужно будет определить различия между этими данными и данными, которые вы изучали в части 1.

Шаг 1: Запустите захват данных в интерфейсе.

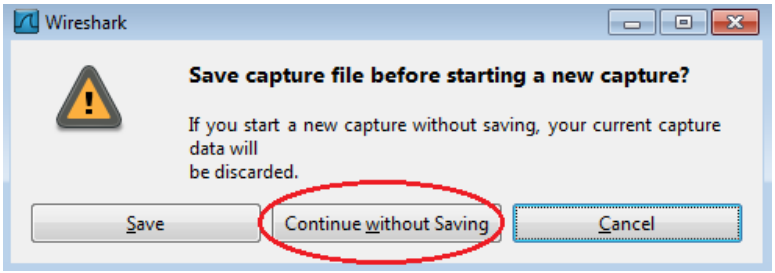
a. Нажмите на значок **Interface List** (Список интерфейсов), чтобы снова открыть список интерфейсов ПК.



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

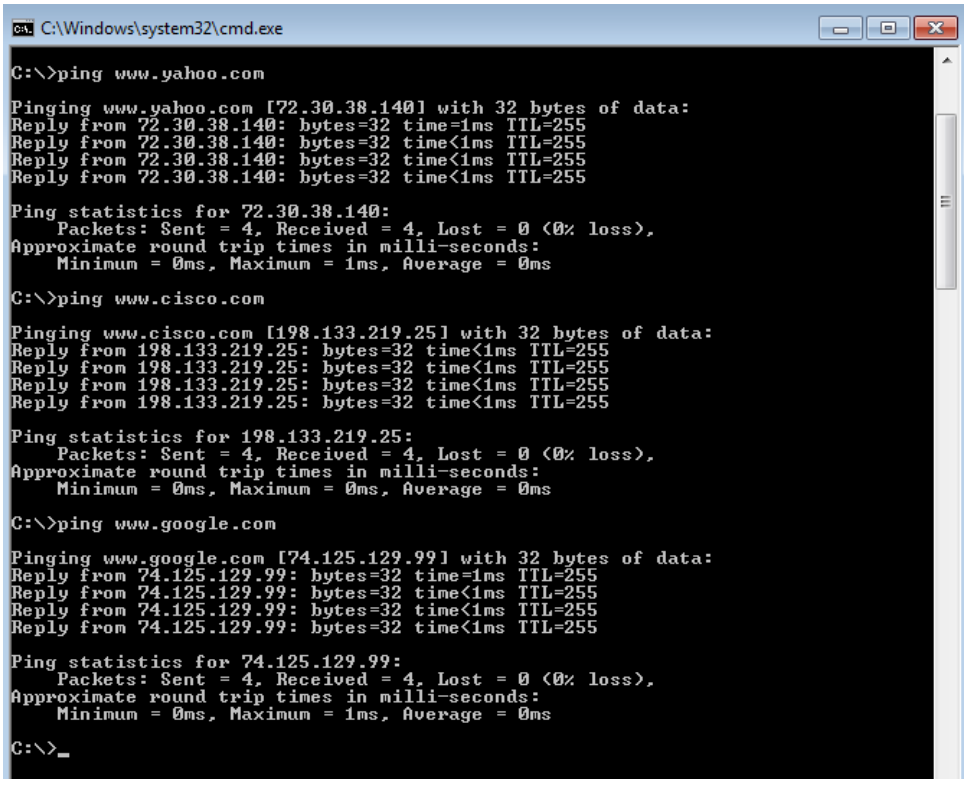


c. Появится окно с предложением сохранить полученные ранее данные перед началом нового захвата. Сохранять эти данные необязательно. Нажмите **Continue without Saving** (Продолжить без сохранения).



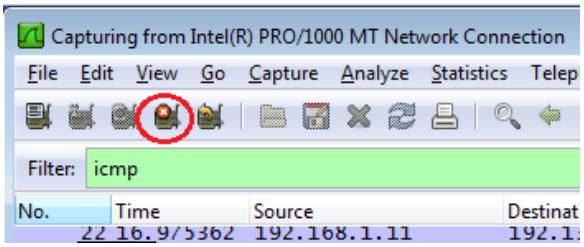
d. Активировав захват данных, отправьте эхо-запрос с помощью команды ping на следующие три URL-адреса веб-сайтов:

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 адрес URL в IP-адрес. Запишите IP-адреса, полученные для каждого URL-адреса.

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



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

a. Просмотрите собранные данные в программе Wireshark и изучите IP- и MAC-адреса трех веб-сайтов, на которые вы отправили эхо-запросы. Ниже в оставленном месте укажите IP- и MAC-адреса назначения для всех трех веб-сайтов.

1-й адрес: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

2-й адрес: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

3-й адрес: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

b. Какова существенная особенность этих данных?

c. Как эта информация отличается от данных, полученных в результате эхо-запросов локальных узлов в части 1?

Вопросы для повторения

Почему программа Wireshark показывает фактические MAC-адреса локальных узлов, но не показывает фактические MAC-адреса удаленных узлов?