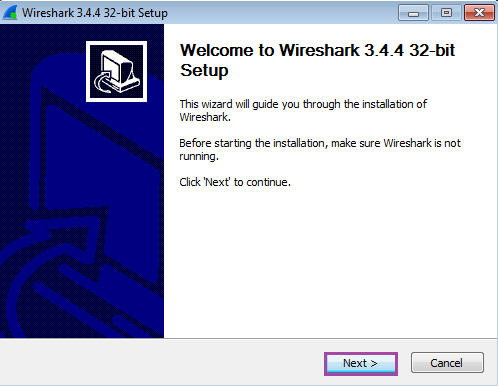
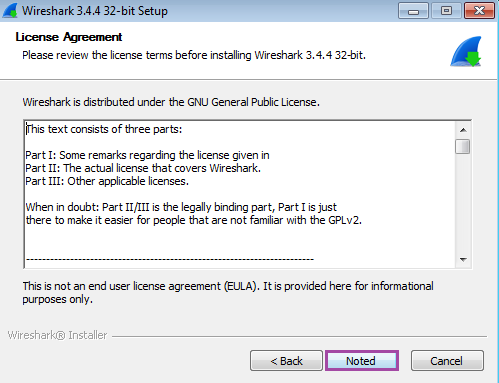
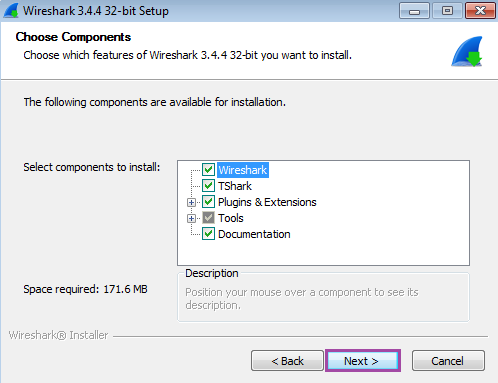
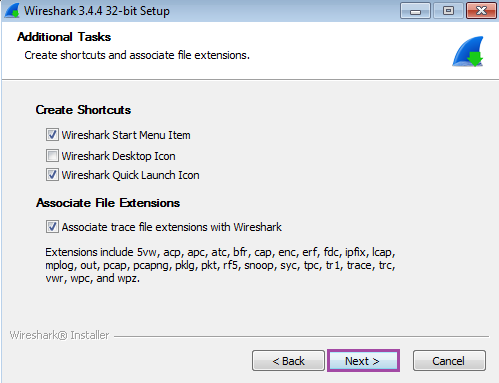
**Практическая работа 9. Использование Wireshark для просмотра сетевого трафика.**

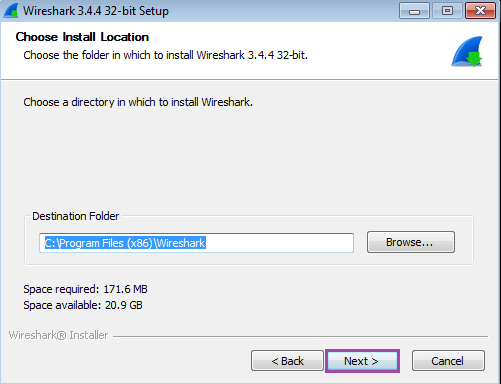
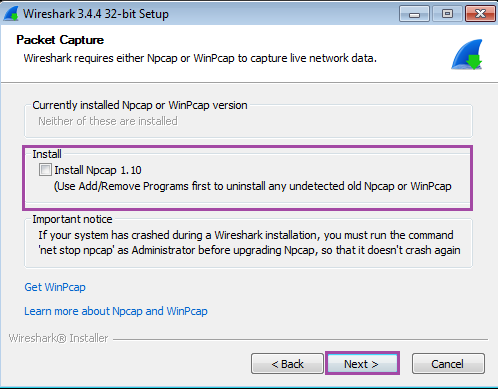
**Пункт 1. Установка Wireshark**

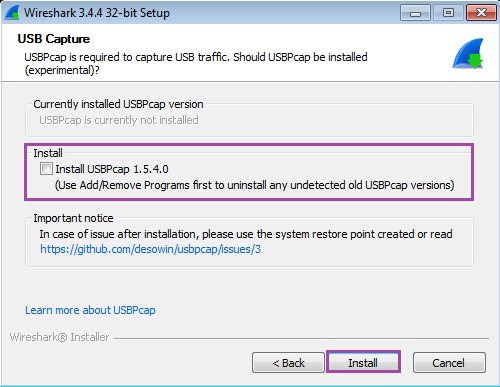
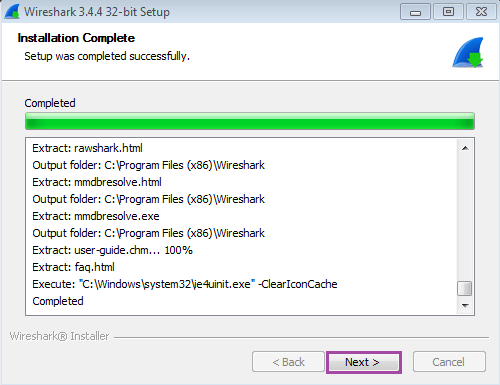
Установим Wireshark, для этого:

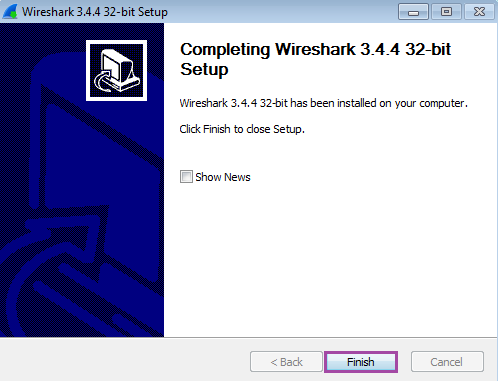
1. Запустим приложение и выполняем всё тоже самое, что показано на скринах

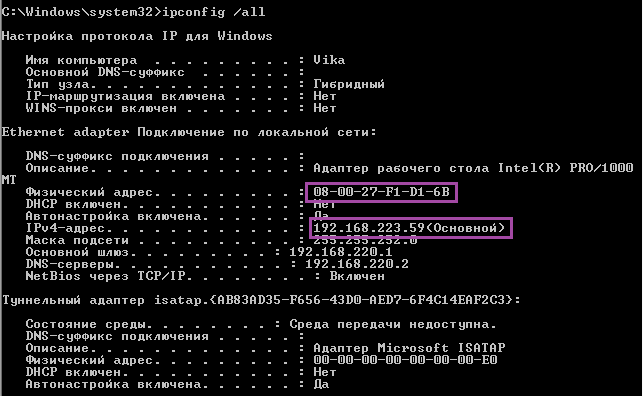


**Пункт 2. Работа в Wireshark**

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

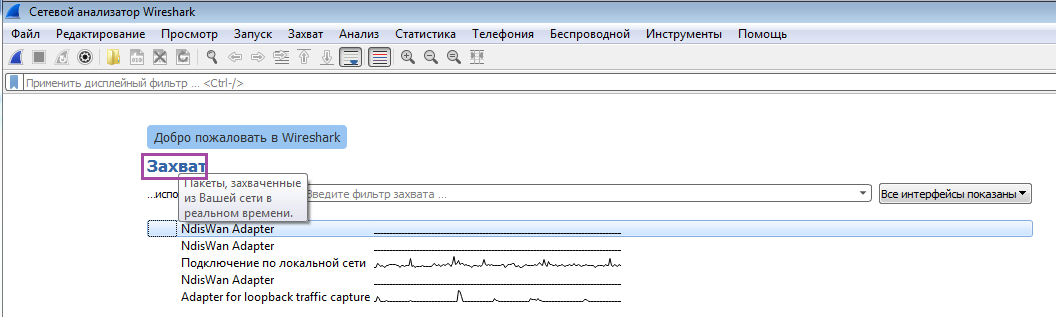
**Шаг 1. Определите адреса интерфейсов вашего ПК.**

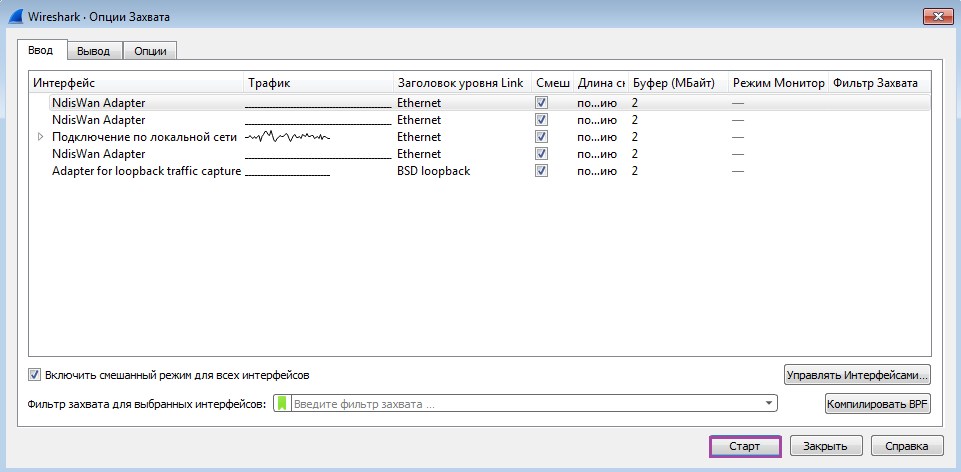
Откроем командную строку с помощью сочетания клавиш **Win + R 🡪 cmd**. Далее в открывшейся командной строке пишем ipconfig /all и смотрим наш iP-адрес и MAC-адрес (физический адрес)

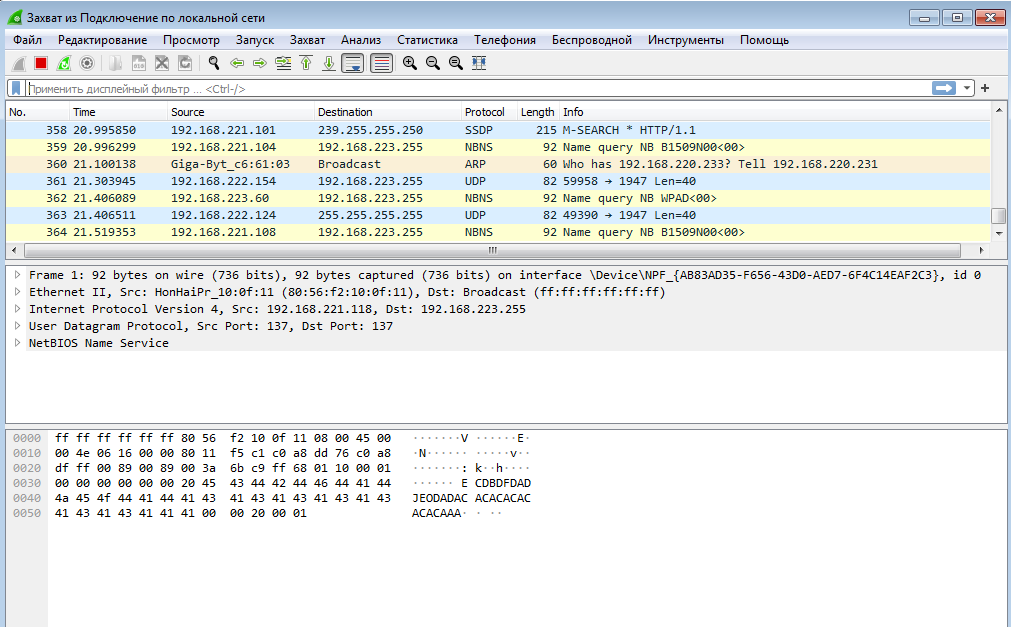


**Шаг 2. Запустить программу Wireshark и начните сбор данных.**

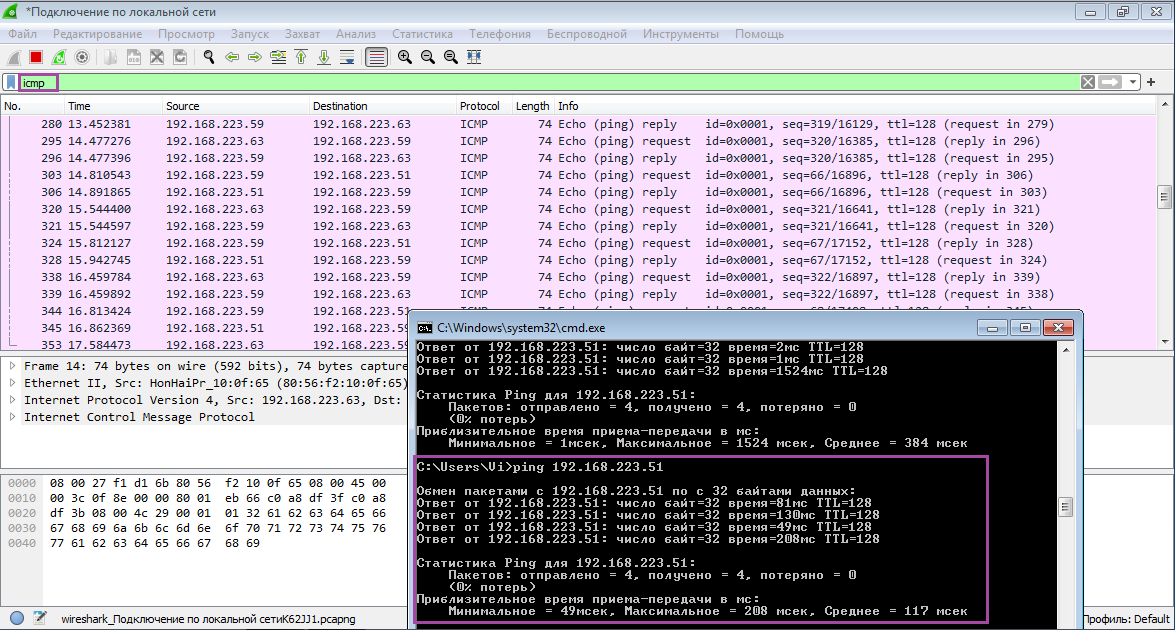
1. Начнём захват данных интерфейсов. Открываем список интерфейсов и начинаем кнопку «Старт»

****

****

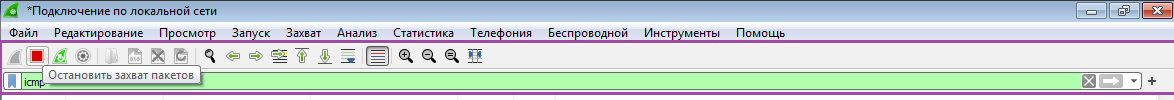
****

1. **Выведем на экран только единицы данных протокола ICMP и отправим эхо-запросы с помощью команды ping на iP-адрес друга**

****

**Шаг 3. Изучите полученные данные.**

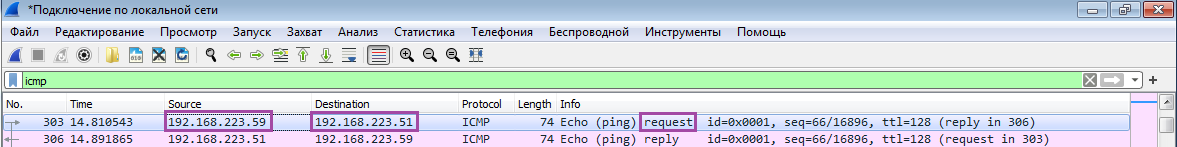
1. **Остановим захват данных**

****

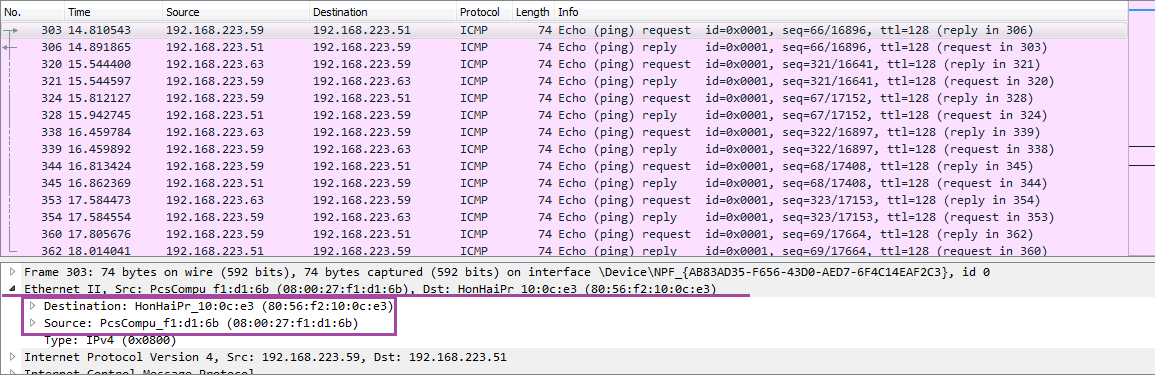
1. **Рассмотрим детально кадр PDU запроса ICMP.**

Source (Источник) – указывается iP-адрес нашего компьютера;

Destination (Назначение) – iP-адрес ПК другого участника, на который мы отправили эхо-запрос с помощью команды ping.

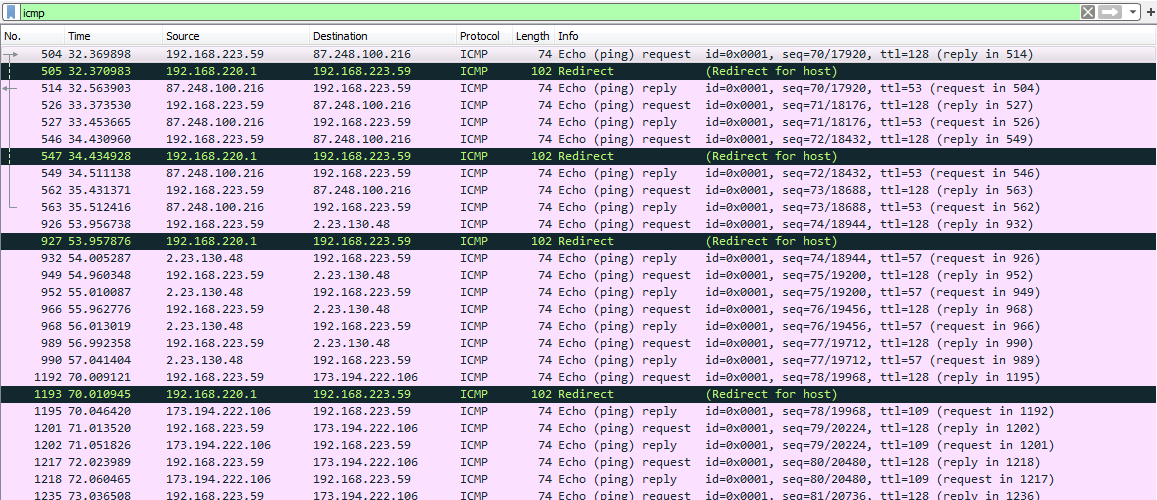


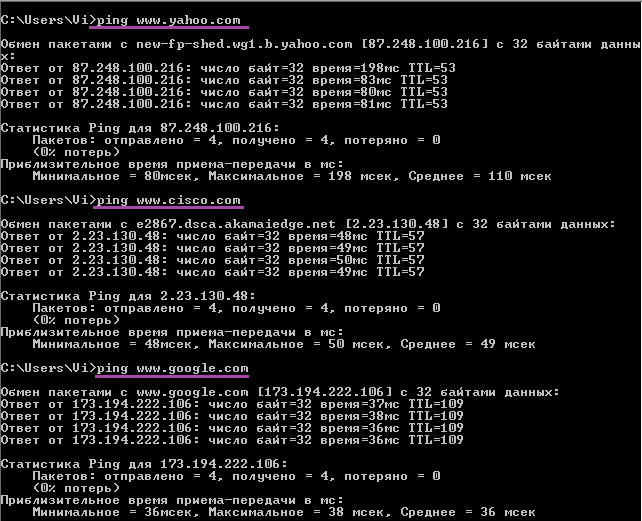
1. **Не меняя выбора кадра PDU переходим на средний раздел. Нажмём на символ + слева от строки «Ethernet 11», чтобы увидеть MAC-адреса источника назначения.**

****

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

1. **Запустим захват данных интерфейса и отправим 3 эхо-запроса с помощью команды ping на следующие три URL-адреса веб-сайтов**
2. [www.yahoo.com](http://www.yahoo.com)
3. [www.cisco.com](http://www.cisco.com)
4. [www.google.com](http://www.google.com)

****

****

**Шаг 2. Изучим и проанализируем данные, полученные от удалённых узлов.**

**1 адрес:**

**IP:** Yahoo = 87.248.100.215

**MAC:** 5c:d9:98:49:cb:0f

**2 адрес:**

**IP:** Google = 173.194.222.103

**MAC:** 5c:d9:98:49:cb:0f

**3 адрес:**

**IP:** Cisco = 2.23.130.48

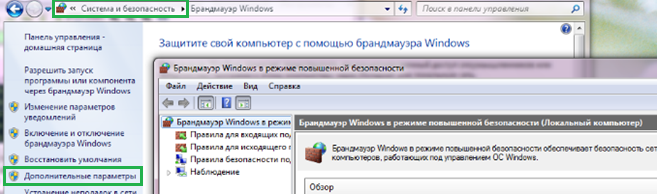
**MAC:** 5c:d9:98:49:cb:0f

Физический адрес у всех одинаковый. Это связано с тем, что мы отправляем пакеты на маршрутизатор, а в нашем случае физический адрес является шлюзом, через который идут пакеты.

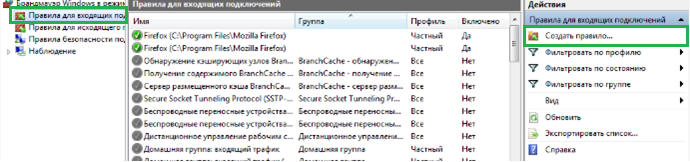
**Приложение А. Пропуск трафика ICMP через межсетевой экран.**

**Шаг 1. Создайте новое правило, разрешающее прохождение ICMP-трафика через межсетевой экран.**

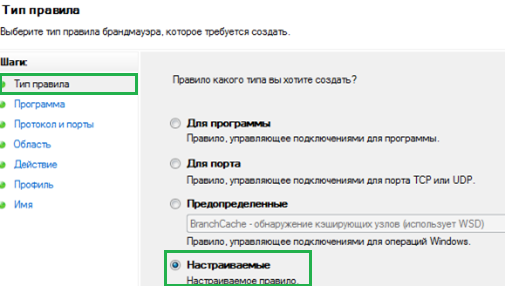
1. На панели управления выбираем пункт Система безопасность, а после заходим Брандмауэр Windows.
2. Выбираем дополнительные параметры.



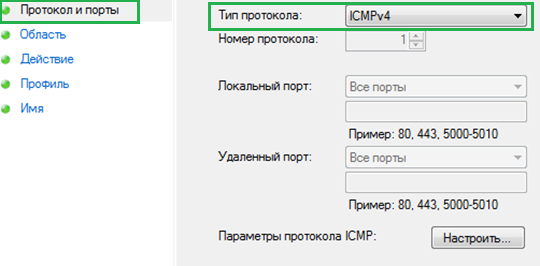
1. Заходим в правила для входящих подключений и выбираем создать правило.



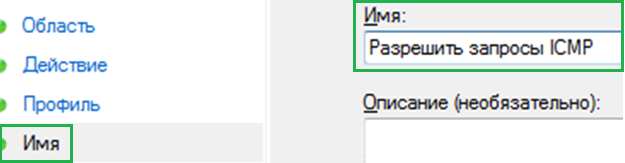
1. Создать правило и выбираем тип правил – настраиваемый.

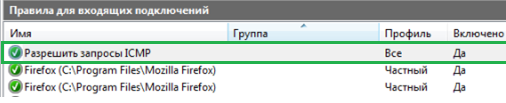


1. Переходим в раздел протокол и порты и выбираем в нем протокол ICMPv4.



1. Переходим в раздел «ИМЯ» и называем его и нажимаем готово.





1. Чтобы удалить просто кликаем по правило левой мышью и выбираем удалить.

