Минобрнауки России

Федеральное государственное бюджетное образовательное

учреждение высшего образования

**НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**ИМ. Р.Е. АЛЕКСЕЕВА**

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

|  |  |  |
| --- | --- | --- |
|  |  |  |

Курс “Сети и телекоммуникации”

**Отчет по лабораторной работе №3**

Выполнил: студент группы 18 В-2

Кожакин Р.А.

Проверил: Гай В.Е.

Нижний Новгород

2020

**Задание:**

Для экспериментов использовать схему из первой лабораторной работы. Все ip-адреса (или маски) необходимо поменять так, чтобы адрес сети у всех компьютеров был один. Все действия должны быть выполнены в симуляторе сетей CORE.

**Часть 1. Формирование запроса и получение ответа**

1. Начать захват пакетов при помощи WireShark.

2. Сформировать кадр ARP-запроса с помощью утилиты PackETH и отправить его в сеть (компьютеры выбрать самостоятельно).

3. Убедиться, что был получен кадр ARP-ответа, соответствующий посланному запросу. Захваченные пакеты сохранить для отчета. Вывести arp таблицу (команда «arp»).

4. Прекратить захват пакетов.

**Часть 2. ARP-спуфинг**

1. Выделить на схеме и обозначить три компьютера: A, B, Сервер.

2. Подготовить кадр ARP-ответа, направляемый Сервером хосту А с помощью программы PackETH. Кадр должен быть составлен так, чтобы MAC-адресу Сервера соответствовал IP-адрес хоста В. Вывести arp таблицу на хосте А. Отправить сформированный пакет от Сервера хосту А.

Для запуска packEth в консоли выполните команду «xhost +», в консоли узла «DISPLAY=:0 packeth» или «DISPLAY=:0 packeth --sync».

netcat (англ. net сеть + cat) — утилита Unix, позволяющая устанавливать соединения TCP и UDP, принимать оттуда данные и передавать их.

Организация чата между узлами с помощью netcat:

1. На первом узле (192.168.1.100):

$ nc -lp 9000

2. На втором узле:

$ nc 192.168.1.100 9000

3. Начать захват пакетов при помощи WireShark на Сервере.

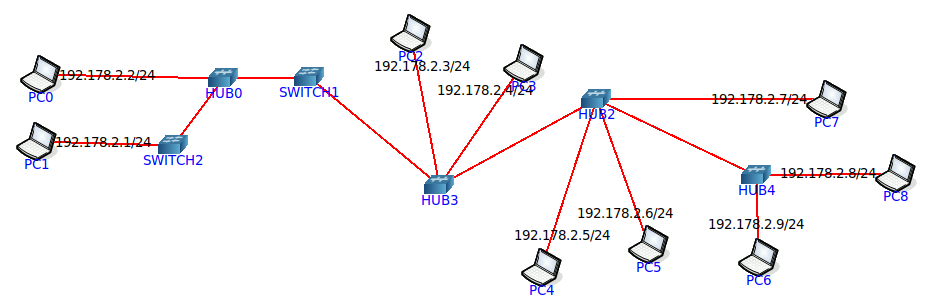
4. Попытаться установить соединение между хостом А и хостом В с помощью программы netcat (А отправляет сообщения В). Убедиться, что запросы от хоста A, направленные хосту В поступают на Сервер.

5. Прекратить захват пакетов.

6. Сохранить для отчета отправленный кадр ARP-ответа и несколько перехваченных пакетов, переданных на Сервер, arp таблицу хоста А.

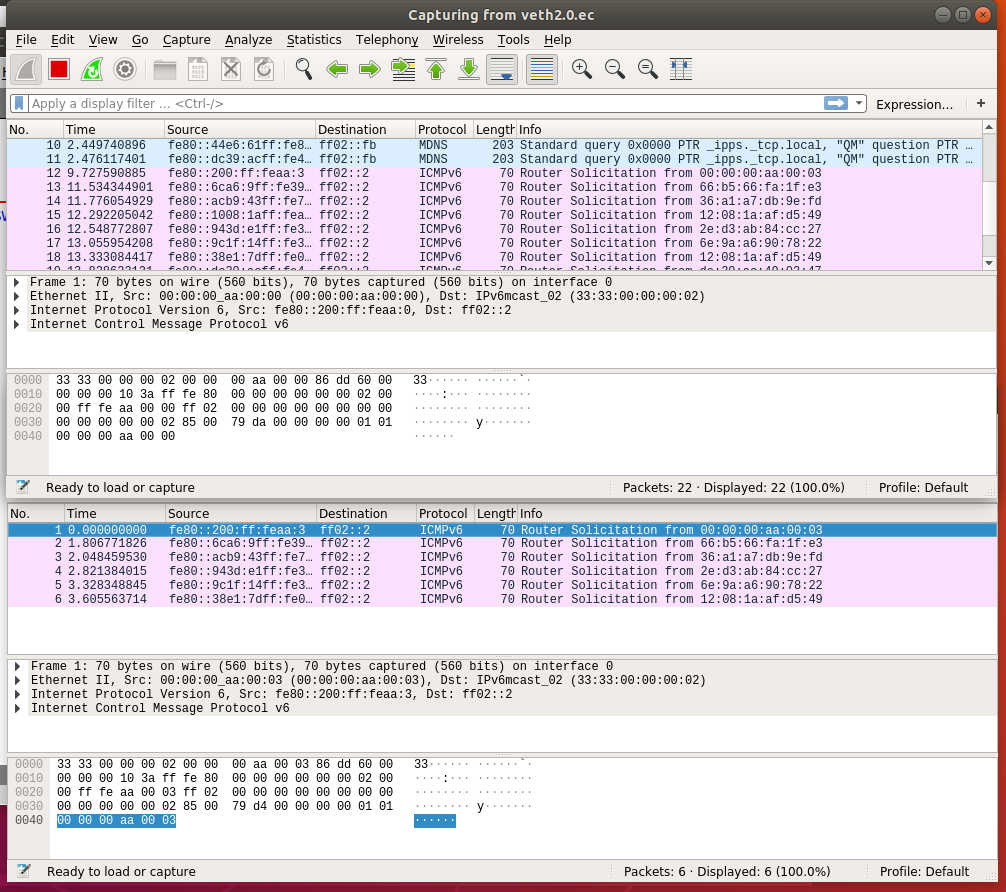
**Ход работы.**

Для экспериментов используем схему из первой лабораторной работы. Все ip-адреса необходимо поменять так, чтобы адрес сети у всех компьютеров был один.



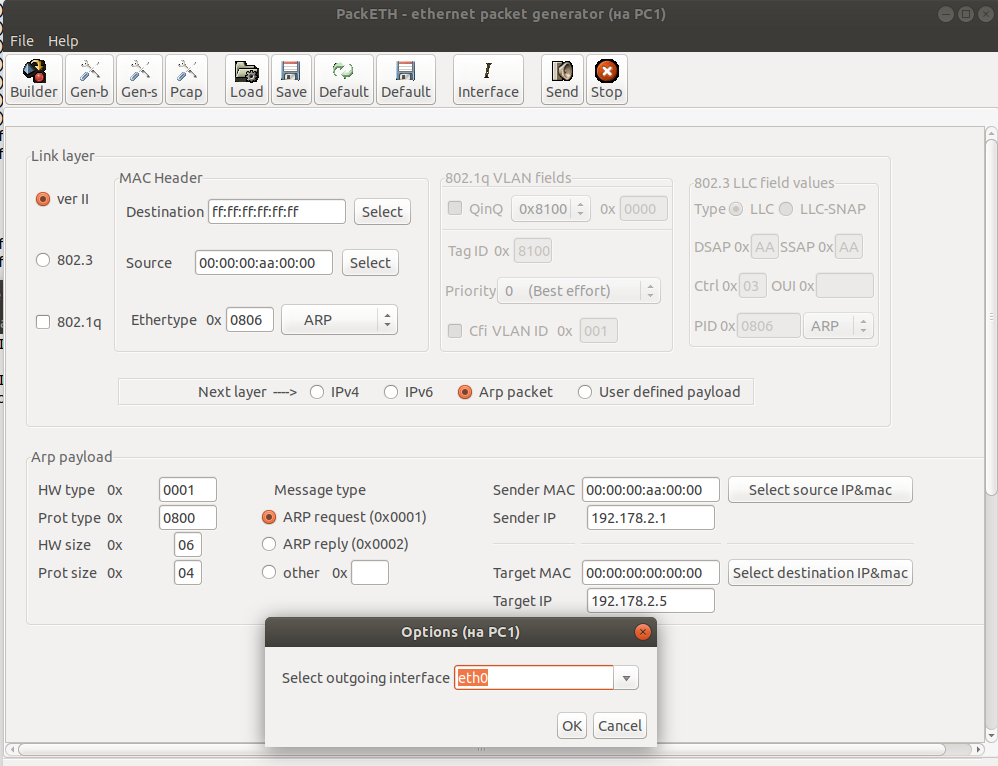
**Часть 1. Формирование запроса и получение ответ**

1. Для начала запустим WireShark на двух компьютерах. Я выбрал PC1 и PC4

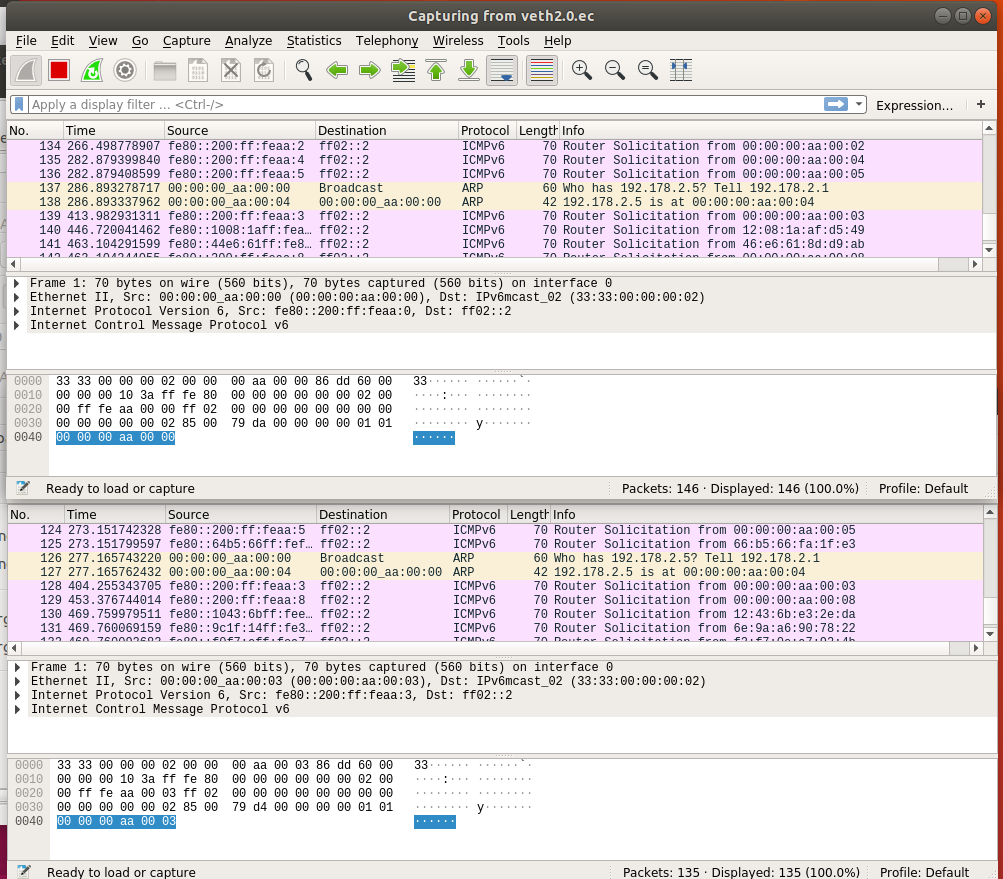


Всё работает.

1. Сформируем кадр ARP-запроса с помощью утилиты PackETH (на PC1) и отправим его в сеть.



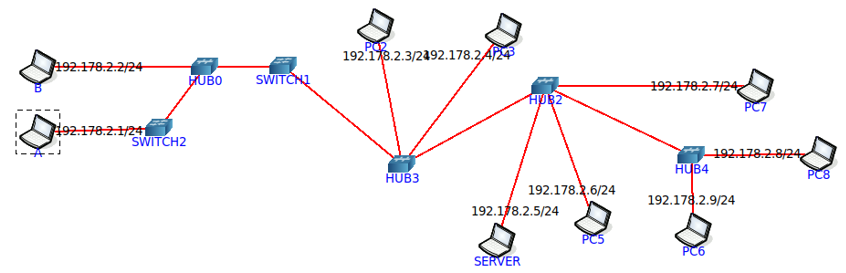
1. Убедимся, что кадр ARP-ответа был получен после посланного запроса.



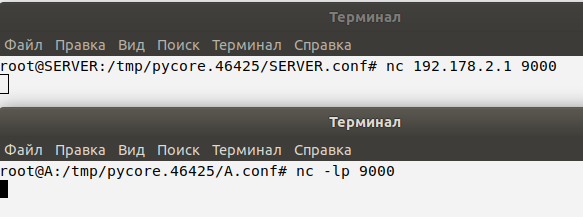
Прекратим захват пакетов.

**Часть 2. ARP-спуфинг**

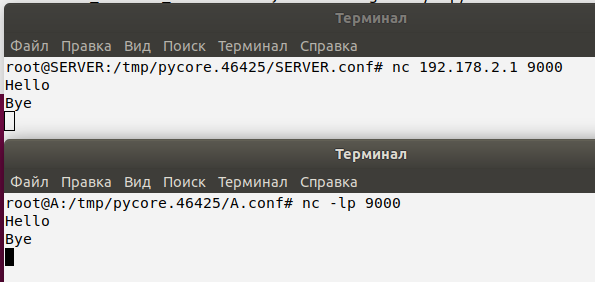
1) Выделить на схеме и обозначить три компьютера: A, B, Сервер.

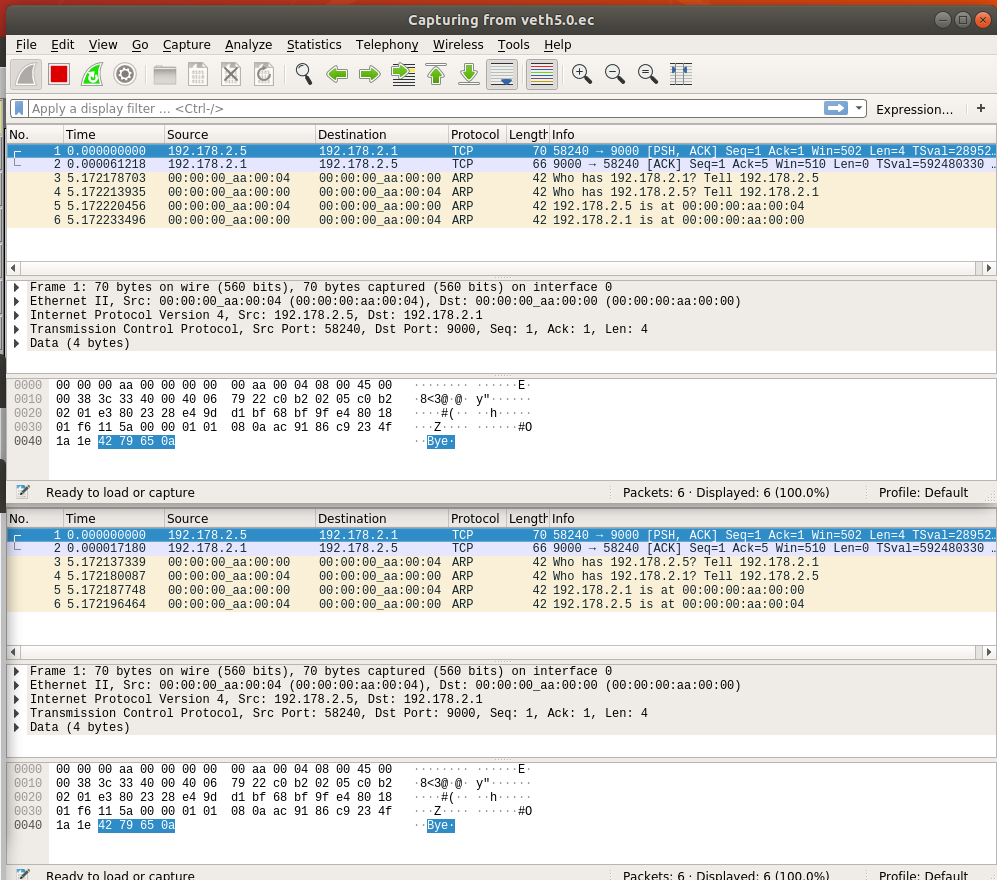


2) Установим связь между А и Server при помощи утилиты netcat, которая позволяет устанавливать соединения TCP и UDP.

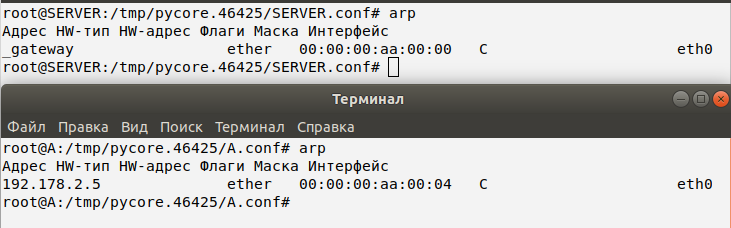


Напишем сообщение:



Если открыть wireshark A и Server и найти TCP–пакет, который закрывает соединение, то в нём можно обнаружить текст сообщений, которые мы отсылали:  


Также, если вывести ARP-таблицу на хосте А и Server увидим:



На других компьютерах такого нет.

1. Следующим действием нам нужно произвести атаку на это соединение и перехватить пакеты. Для этого мы вновь используем программу PackETH, которая запускается на хосте B.

Destination – mac-адрес отправителя (Server)

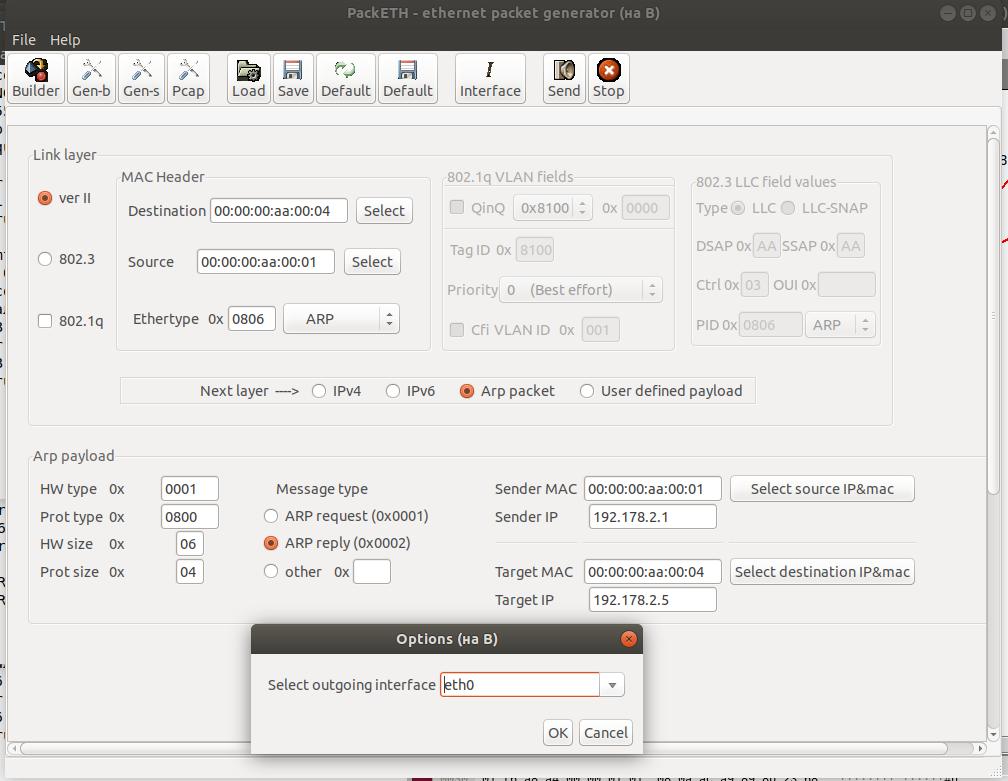
Source – mac-адрес перехватчика (B)

Sender MAC – mac-адрес перехватчика (B)

Sender IP – ip-адрес получателя (А)

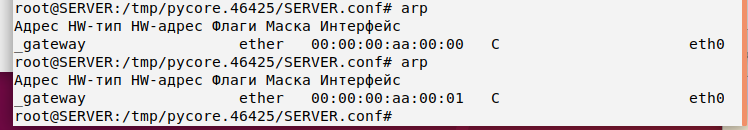
Targer MAC – mac-адрес отправителя (Server)

Target IP – ip-адрес отправителя (Server)

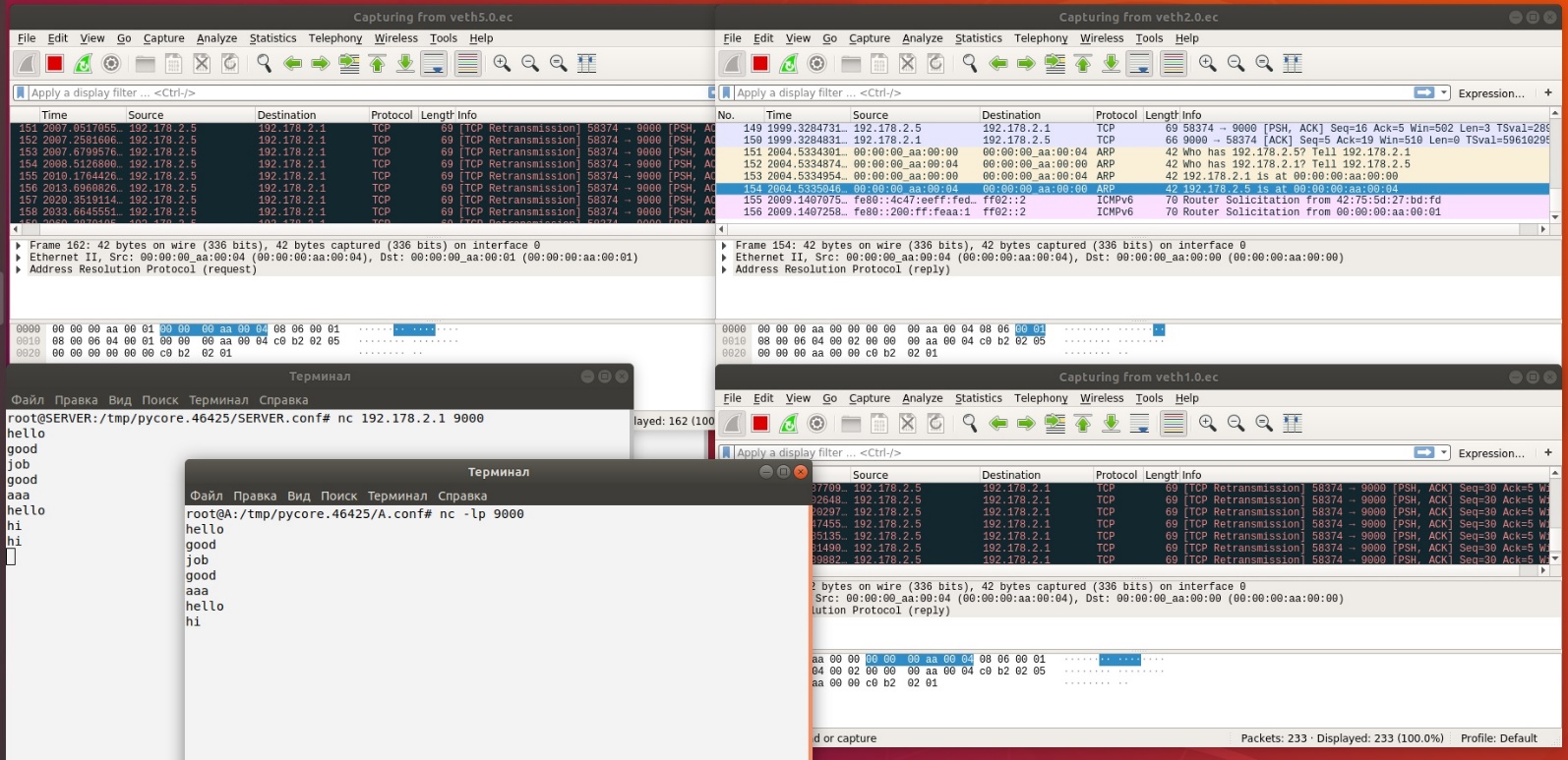


Нажимаем «send»:

Мак-адрес изменился.



Отправим сообщение.



В wireshark мы увидим TCP запросы черного цвета, поскольку TCP пытается доставить пакет, но этого не удаётся сделать. Это будет видно на компьютере Server и B, а на получателе A -ничего.

Чуть позже с задержкой перехваченные пакеты всё-таки дойдут до истинного адресата, потому что происходит перезапрос MAC-адреса хоста A.