МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Кафедра «Вычислительные системы и технологии»

ОТЧЕТ

по лабораторной работе №2

Дисциплина: **«Сети и телекоммуникации»**

Выполнили:

Студент группы 17-В-1

Дятлов Д.А.

Проверил:

Гай В.Е.

Нижний Новгород

2020 г.

**Цель работы:**

Получить практические навыки в составлении кадра для широковещательной передачи ARP-запроса хостом А и кадра ARP-ответа хостом В хосту А. Получение базовых навыков по работе с генератором пакетов PackETН.

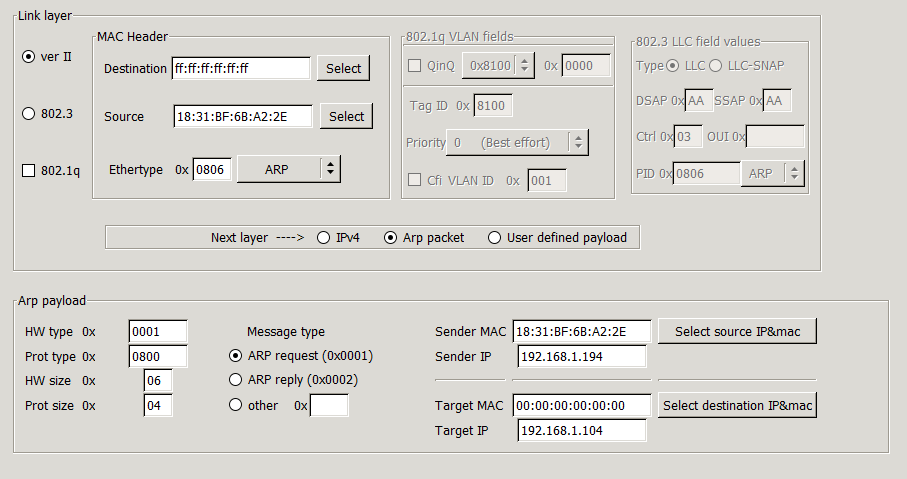
**Часть 1.**

Отправка ARP-запроса и получение ARP-ответа. Мы знаем IP-адрес отправителя (192.168.1.194) и МАС-адрес своего компьютера (18:31:BF:6B:A2:2E) и IP-адрес получателя (192.168.1.104).

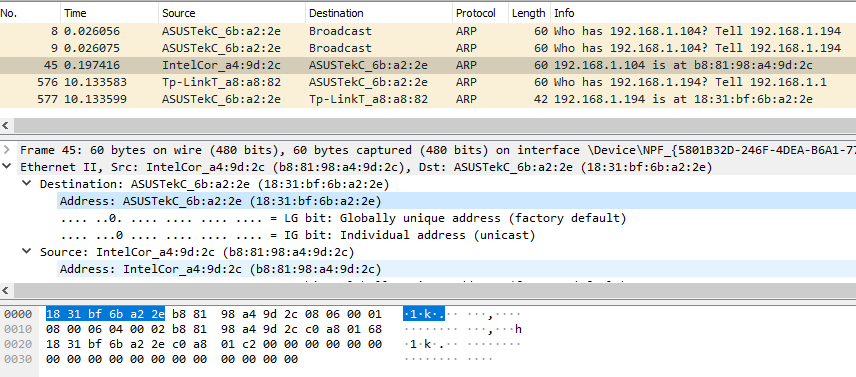
С помощью программ PackETH и Wireshark узнать МАС-адрес второго компьютера. Для этого загружаем программу PackETH и выставляем соответствующие параметры (рис. 1):

* Destination: ff:ff:ff:ff:ff:ff – для того, чтобы узнать МАС-адрес компьютера-получателя;
* Source – MAC-адрес компьютера-отправителя;
* Sender MAC - MAC-адрес компьютера-отправителя;
* Sender IP – IP компьютера-отправителя;
* Target MAC: 00:00:00:00:00:00 - для того, чтобы узнать МАС-адрес компьютера-получателя;
* Target IP - IP компьютера-получателя;

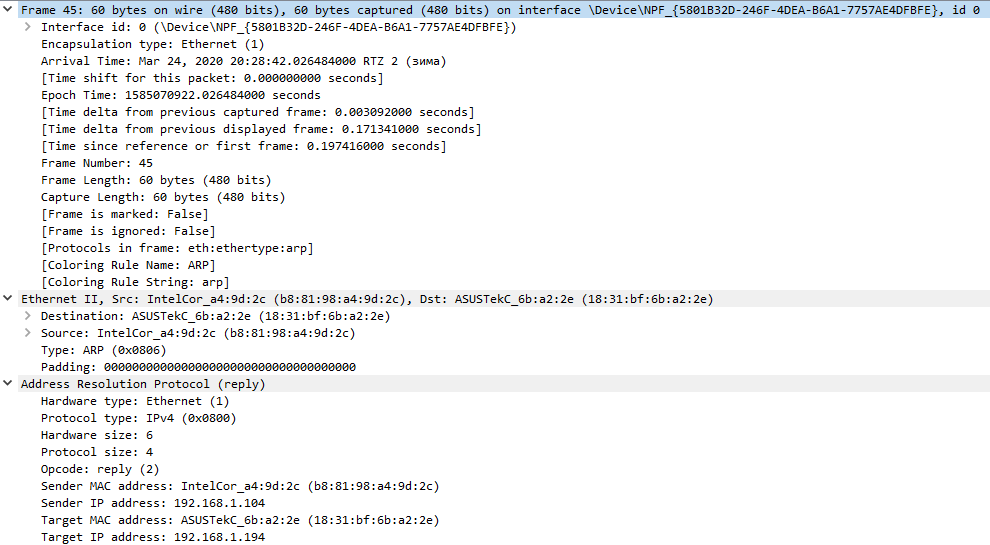
необходимо выбрать Interface, иначе – ошибка при отправке



Открываем wireshark, настраиваем параметры: фильтр arp, интерфейс – «подключение по локальной сети», нажимаем start. В PackETH нажимаем «send» и смотрим результат в wireshark



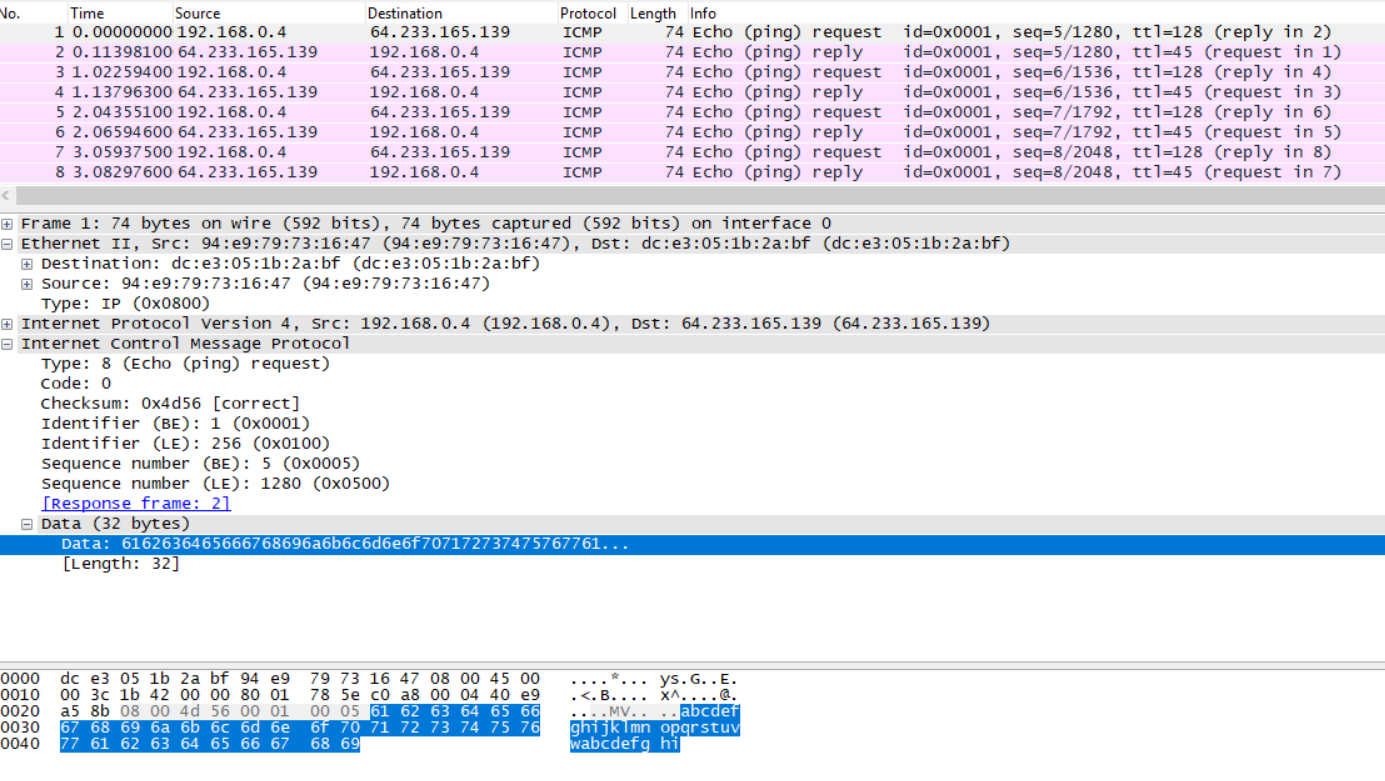
Видно, что пришел ответ с МАС-адресом компьютера-получателя. В данном случае этот МАС-адрес:18:31:bf:6b:a2:2e. Состав ответного пакета представлен ниже



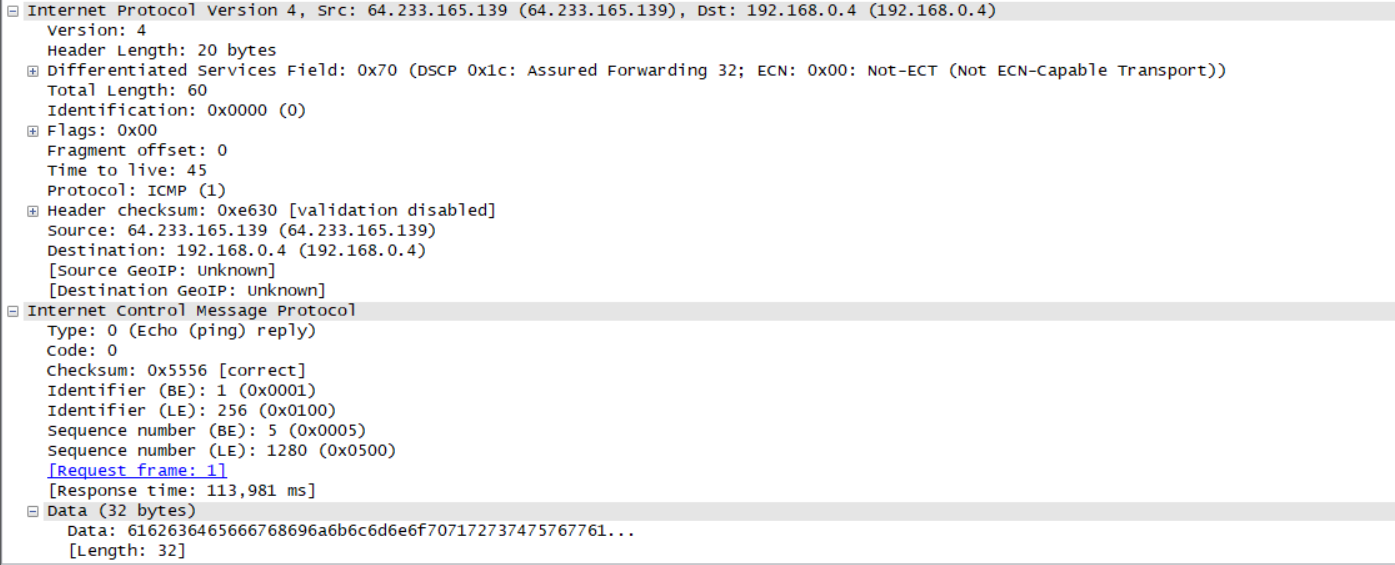
**Часть 2.**

Выполнение работы:

В программе WireShark выставляем фильтр icmp. Результат полученных и отправленных пакетов:



Далее идёт непосредственно заголовок пакета, и мы можем наблюдать:



4 – версия; IPv4

5 – IHL (Internet Header Length); длина IP-заголовка, 5 блоков длиной 4 байта каждый

003С – длина пакета (Total Length); 60 октетов, включая заголовок и данные

1b42 - идентификатор (Identification) пакета; значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке пакета

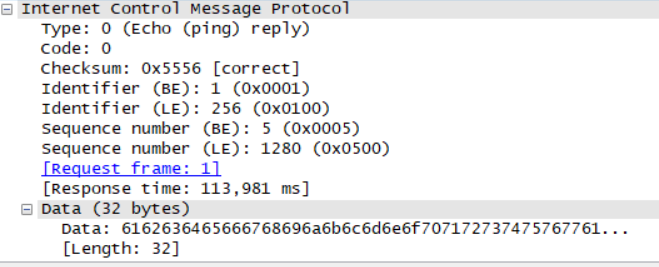
0000 – смещение фрагмента (Fragment offset); определяет позицию фрагмента в потоке данных, количество восьмибайтовых блоков

80 – время жизни (Time to live); число маршрутизаторов, которые может пройти этот пакет, 128

01 – протокол (Protocol); идентификатор, который указывает, данные какого протокола содержит пакет, 1- ICMP

785e - контрольная сумма заголовка (Header Checksum)

Для вычисления контрольной суммы необходимо просуммировать все двухбайтовые слова из заголовка без учёта значения контрольной суммы.



4500+003C+1B42+0000+8001+785E+C0A8+0004+40E9+A58B = 2FFFD

Переводим полученное число в двоичную систему счисления и побитово инвертируем его:

2FFFD16 = 001011111111111111012

0010. 1111. 1111. 1111. 1101. = 1101. 0000. 0000. 0000. 0010.

1101. 0000. 0000. 0000. 0010. = D0002

**Вывод:** В ходе выполнения лабораторной работы были получены практические навыки в составлении кадра для широковещательной передачи ARP-запроса хостом А и кадра ARP-ответа хостом В хосту А. Также были получены базовые навыки по работе с генератором пакетов PackETH. Так же были получены базовые представление об вычисление контрольной суммы в IP-пакетах.