МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра информатики и систем управления

**Отчет**

по лабораторной работе № 2

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гай В.Е. (подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Кольчугин И.А.

(подпись) (фамилия, и.,о.)

17-АС

(шифр группы)

Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород 2020

**Цель работы:**

1. 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 генераторами пакетов PackETH.

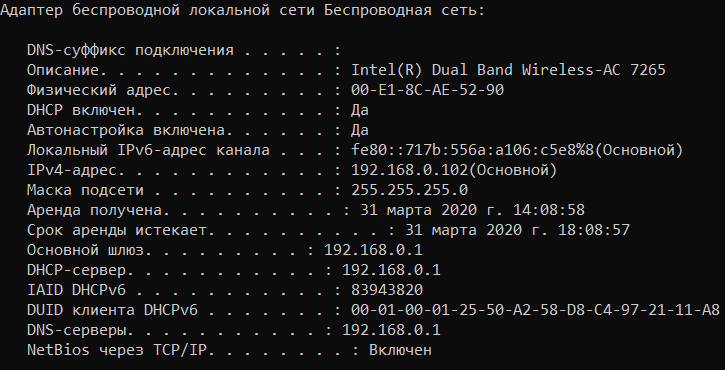
2. Изучить структуру IP-пакета, TCP-сегмента и UDP-датаграммы. Получить практические навыки в вычислении контрольной суммы заголовка IP-пакета.

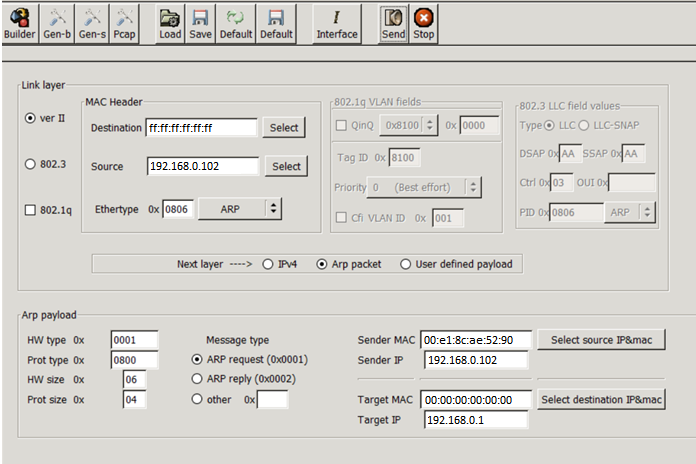
**3.3.1 Отправка ARP-запроса и получение ARP-ответа.**

IP-адрес отправителя: 192.168.0.102

MAC-адрес отправителя: 00:e1:8c:ae:52:90

IP-адрес получателя: 192.168.0.1





Параметры в программе PackETH:

Destination: ff:ff:ff:ff:ff:ff – чтобы узнать MAC-адрес получателя;

Source: 192:168:0:102 – IP-адрес отправителя;

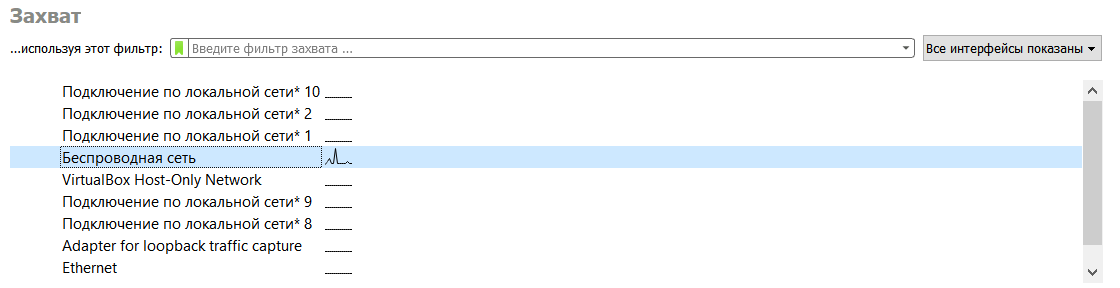
Sender MAC: 00:e1:8c:ae:52:90 – MAC-адрес отправителя;

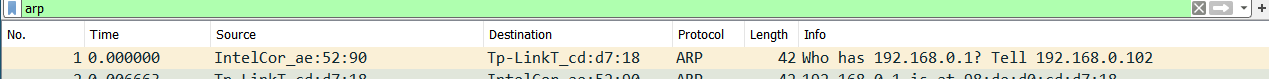
Sender IP: IP-адрес отправителя;

Target MAC: 00:00:00:00:00:00 – чтобы узнать MAC-адрес получателя;

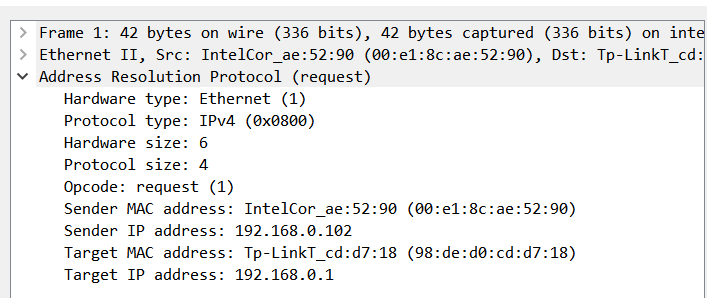
Target IP: 192.168.0.1 – IP-адрес получателя.

В программе Wireshark: выбираем “Беспроводная сеть”, фильтр по “arp”, в PackETH нажимаем “send”.





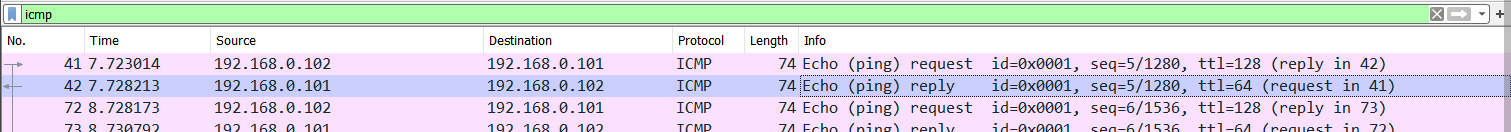
Пришел ответ с MAC-адресом получателя: 98:de:d0:cd:d7:18

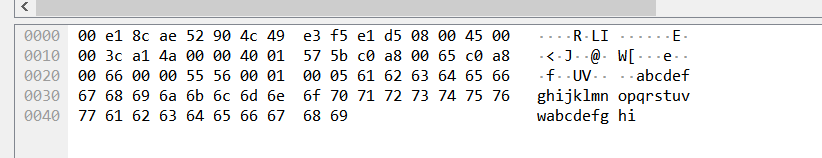


**Вывод:**В ходе выполнения лабораторной работы были получены практические навыки в составлении кадра для широковещательной передачи ARP-запроса хостом А и кадра ARP-ответа хостом В хосту А. Также были получены базовые навыки по работе с генератором пакетов PackETH.

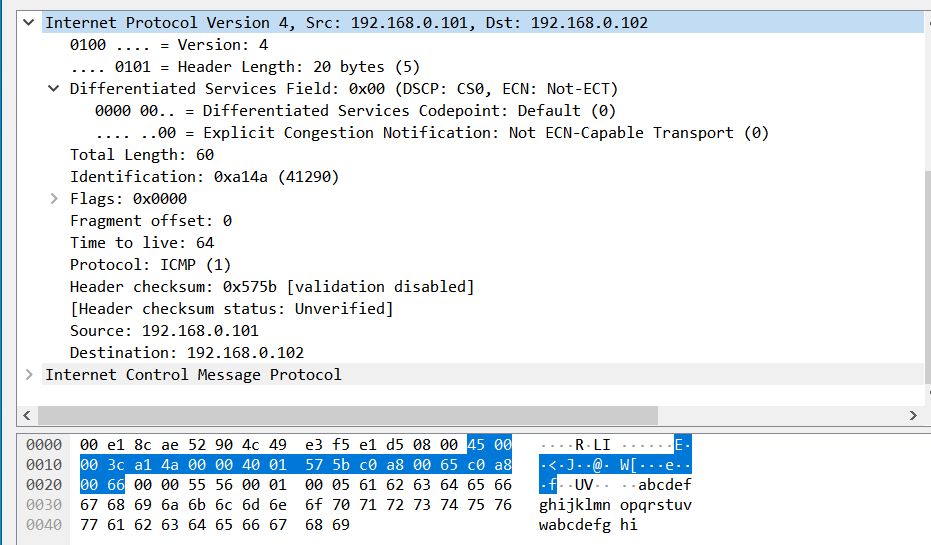
**6. Вычисление контрольной суммы в IP-пакетах**

В программе Wireshark:





Заголовок пакета:



версия - IPv4: **4**

Header Length (длина IP-заголовка, 5 блоков длиной 4 байта каждый): **5**

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

Identification - идентификатор пакета; значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке пакета: **A14A**

Fragment offset - смещение фрагмента; определяет позицию фрагмента в потоке данных, количество восьмибайтовых блоков: **0000**

Time to live - время жизни; число маршрутизаторов, которые может пройти этот пакет: **40**

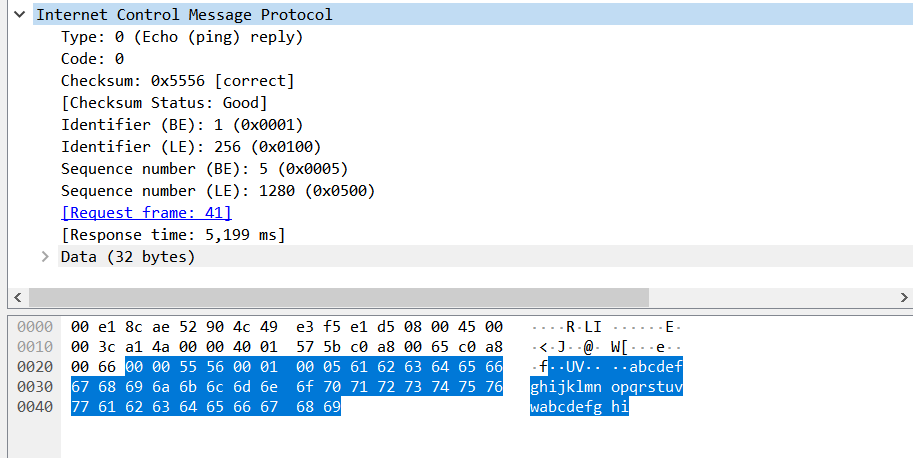
Protocol - протокол; идентификатор, который указывает, данные какого протокола содержит пакет, 1- ICMP: **01**

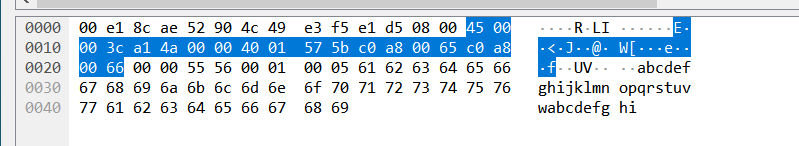
Header Checksum - контрольная сумма заголовка: **575B**

Source - адрес отправителя; 192.168.0.101: **C0A80065**

Destination - адрес получателя; 192.168.0.102: **C0A80066**

Последующие байты – это поле данных.



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

4500 + 003C+A14A+0000 + 4001+575B+C0A8+0065+C0A8+0066 = 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