МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального 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

«Изучение протокола ARP. Получение навыков работы с генераторами пакетов. Вычисление контрольной суммы в IP-пакетах»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гай В.Е

(подпись)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Демидова А.С

(подпись)

Группа: 17-АС

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

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

Нижний Новгород, 2020

**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 генераторами пакетов PackETH и packit.

**Порядок выполнения работы:**

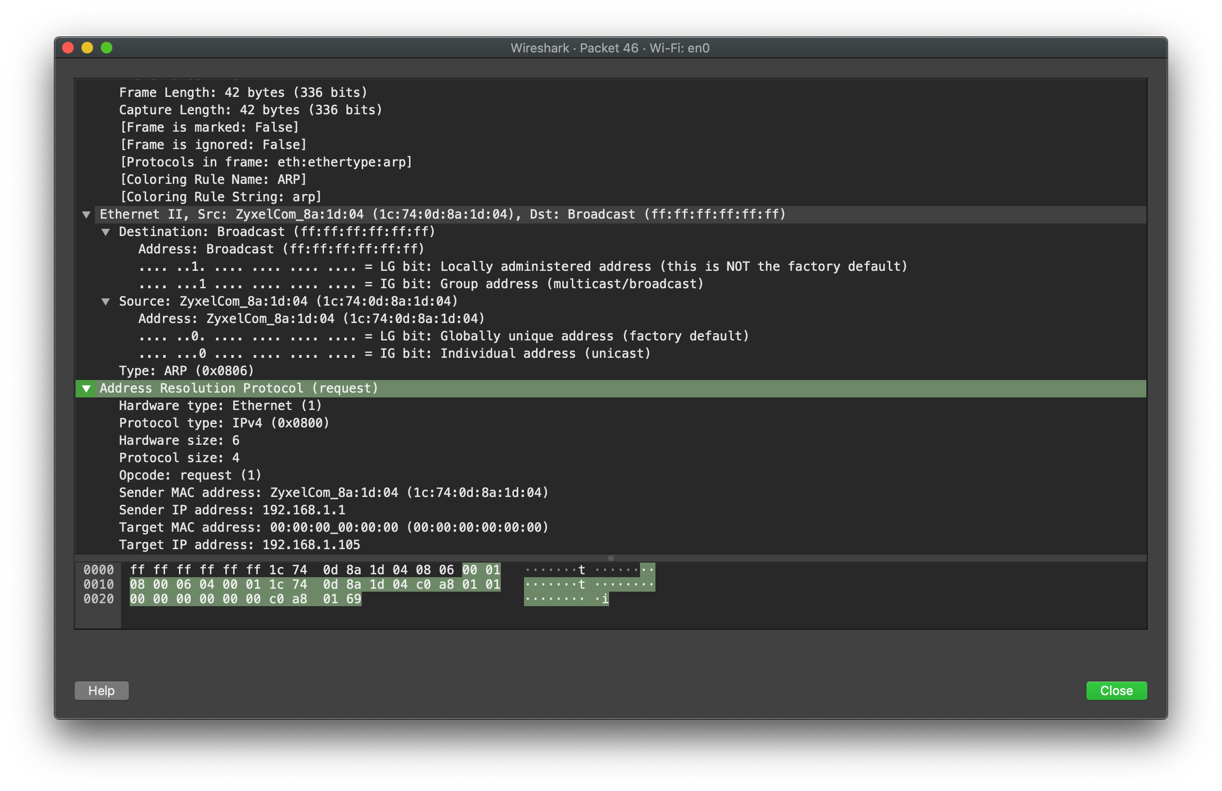
**Часть 1:**

1. Получить у преподавателя бланк с формами для заполнения.
2. Подготовить и записать в 16-теричном виде пример кадра для широковещательной передачи ARP-запроса хостом А и кадра ARP-ответа хостом В хосту А. В кадре ARP- ответа поля для МАС-адреса хоста В не заполнять. (Хост А - это ПК, за которым работает бригада студентов. IP-адрес хоста В выбирается студентом по схеме ЛВС лаб. 521). IP-адрес хоста A можно узнать с помощью команд ifconfig и ip addr show.
3. Начать захват пакетов при помощи любого из изученных анализаторов протоколов. Захват проводить по фильтру (IP-адреса источника и получателя, протокол ARP; для tcpdump дополнительно указать размер пакета 1500 байт, а также флаг отображения пакета (включая заголовок кадра Ethernet) в 16-теричном и ASCII виде).
4. Сформировать кадр ARP-запроса с помощью утилиты packit и отправить его в сеть. Команду сохранить для отчета.
5. Убедиться что был получен кадр ARP-ответа, соответствующий посланному запросу. Захваченные пакеты сохранить для отчета.
6. Сравнить полученный ARP-ответ с подготовленным в первом пункте примером.
7. Сформировать кадр ARP-запроса с помощью утилиты PackETH и отправить его в сеть.
8. Убедиться что был получен кадр ARP-ответа, соответствующий посланному запросу. Захваченные пакеты сохранить для отчета.
9. Сравнить полученный ARP-ответ с подготовленным в первом пункте примером.
10. Прекратить захват пакетов.

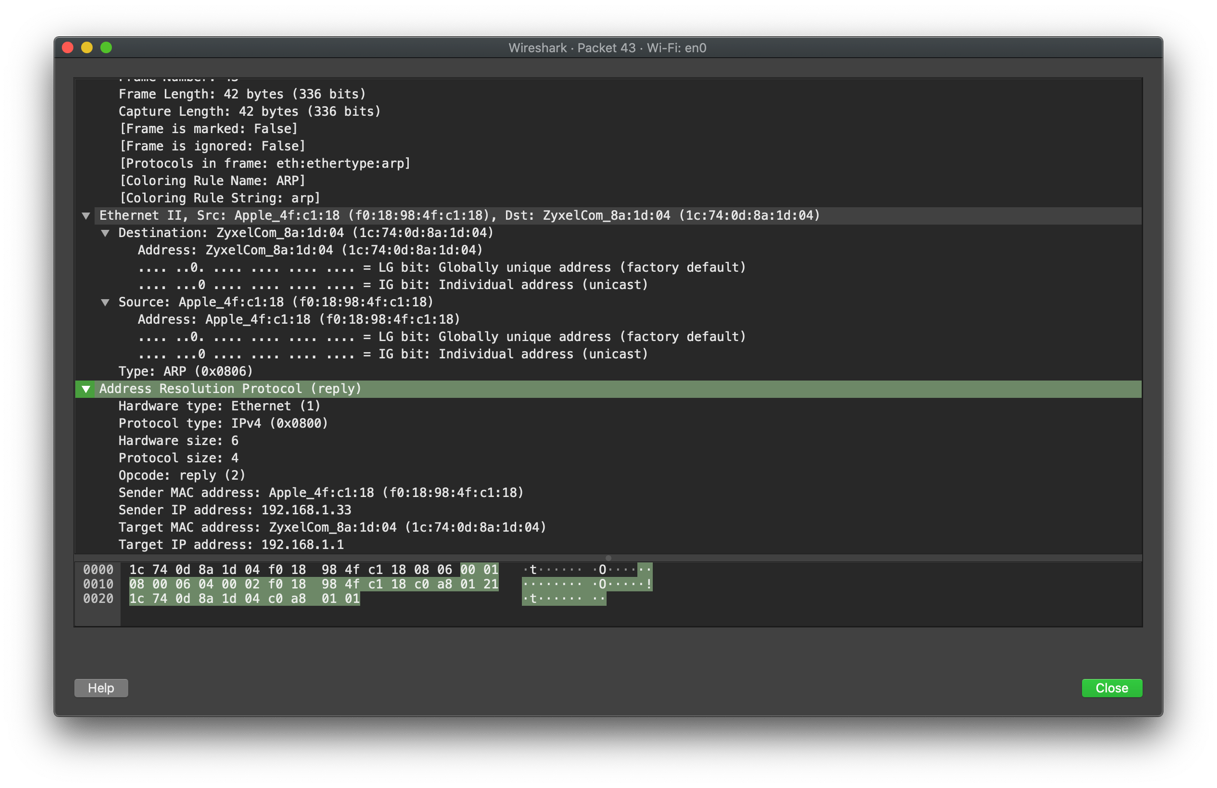
Часть 2:

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

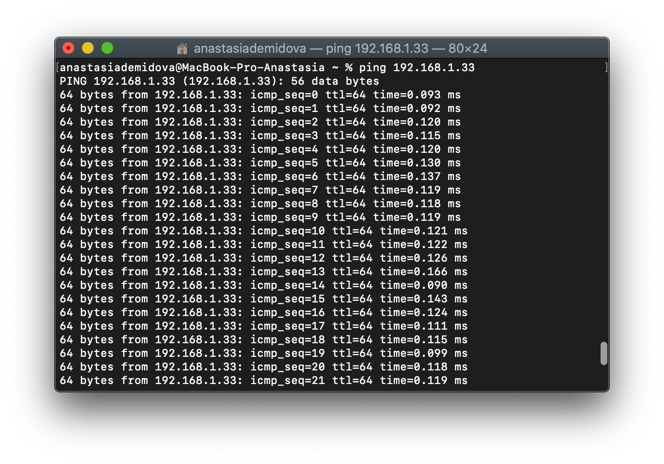
**Кадр широковещательной передачи ARP-ответа хостом А хосту В**

****

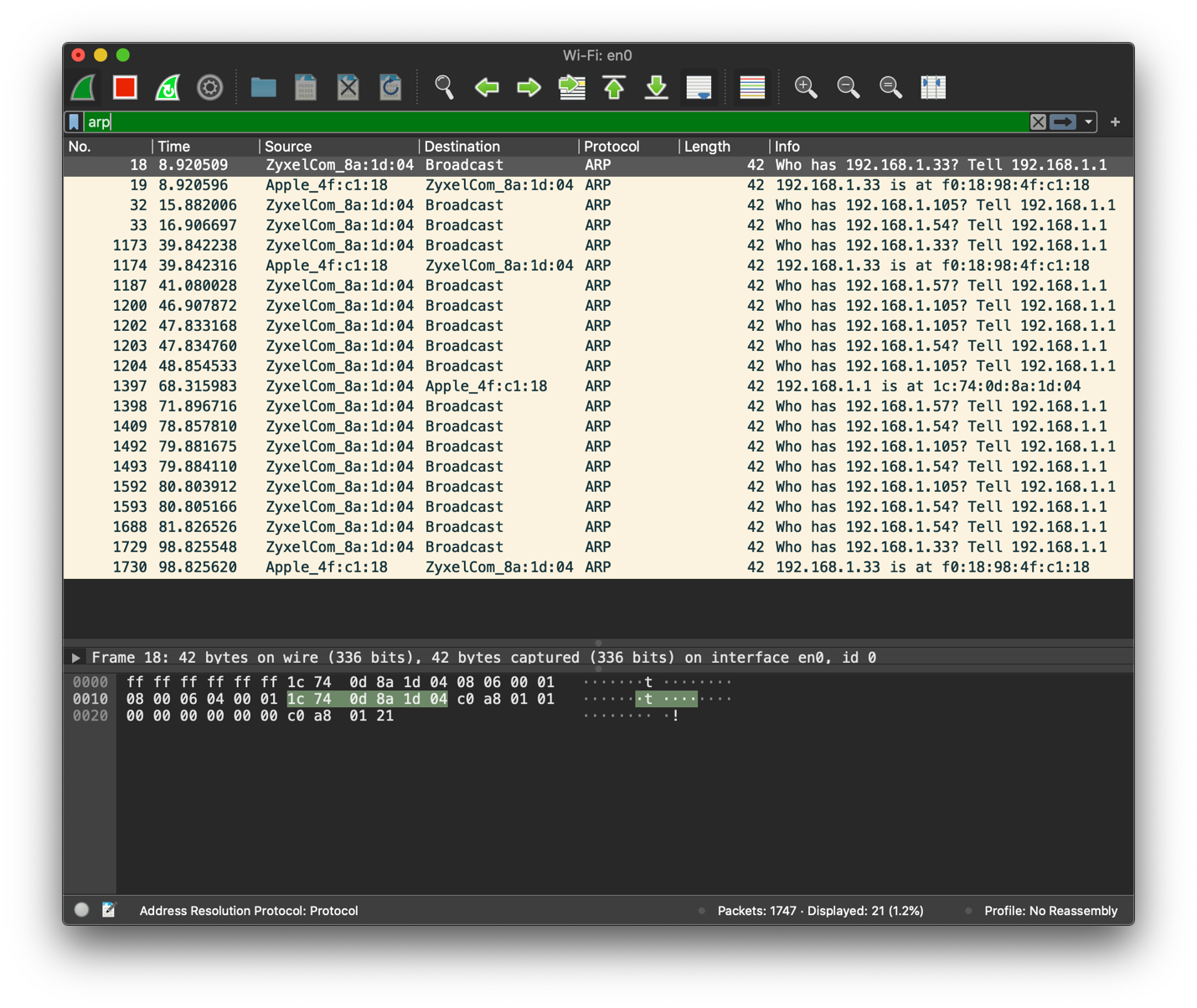
**Кадр широковещательной передачи ARP-ответа хостом В хосту А**



Захват пакетов:



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

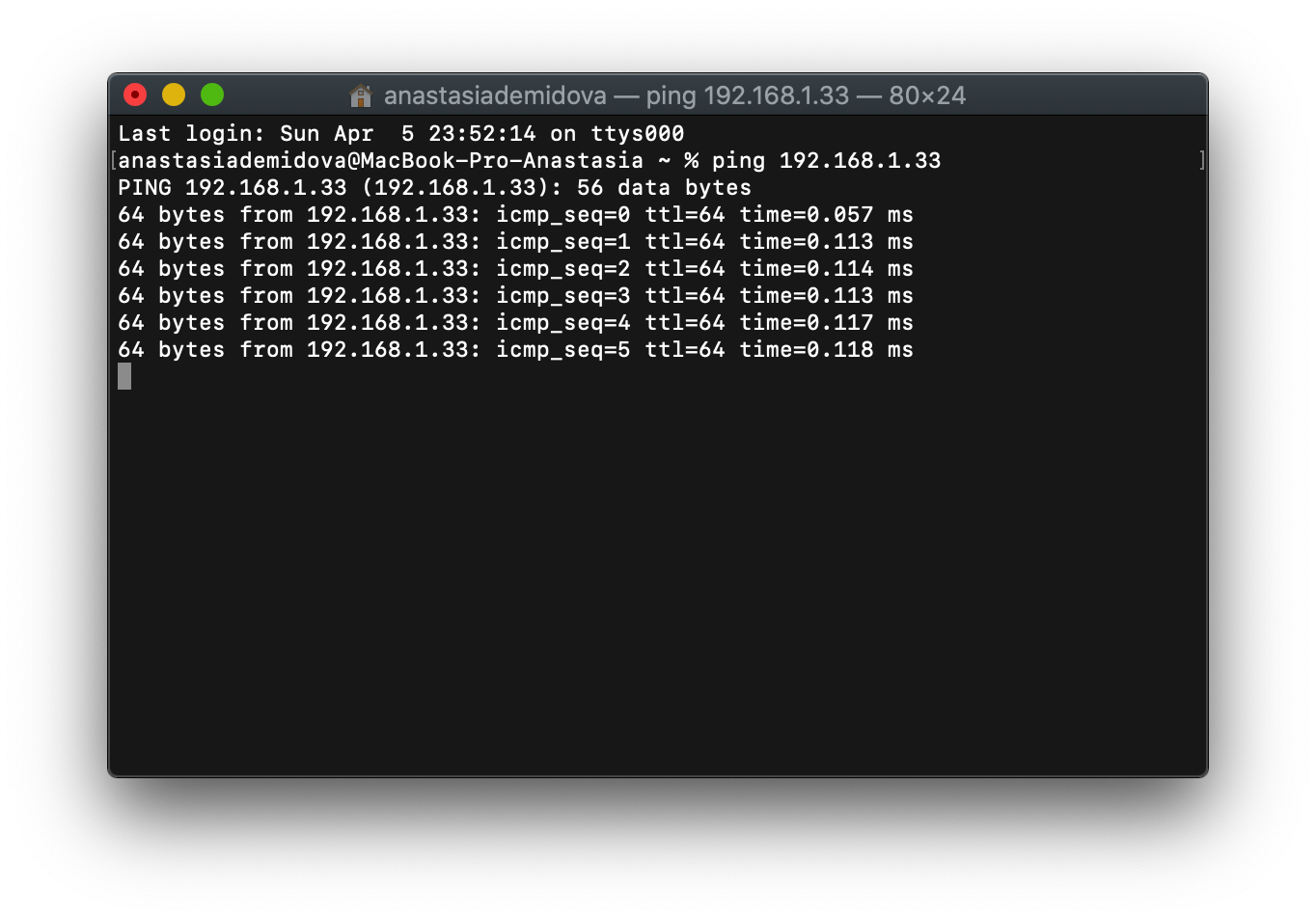


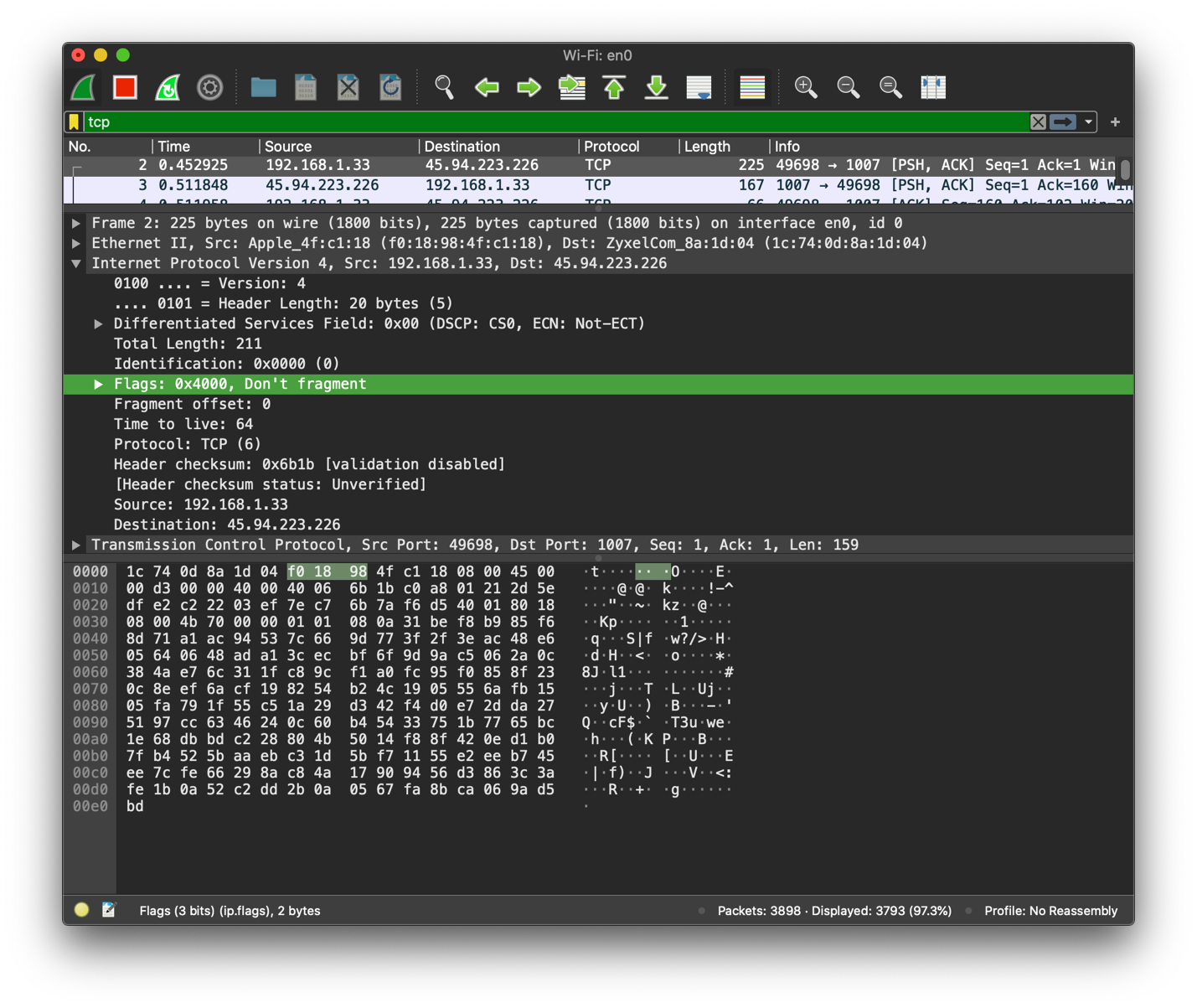
**Вывод:**

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.

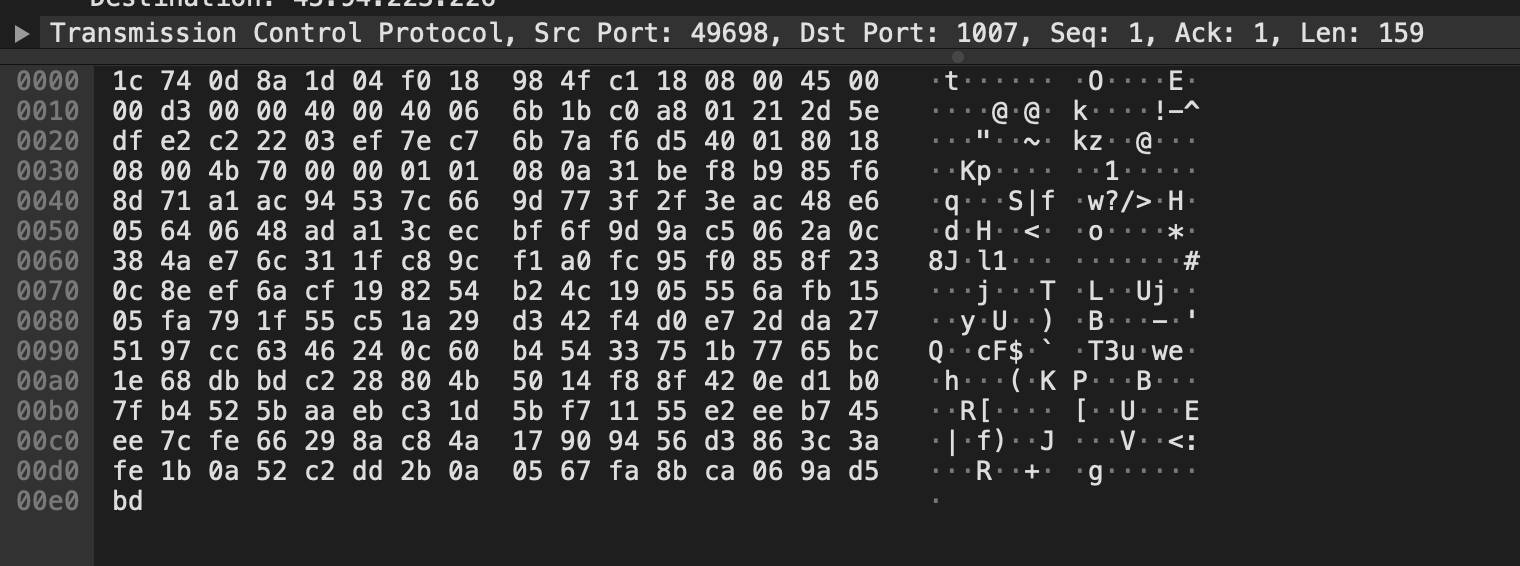
Часть 2:

Произведем отправку пакетов:





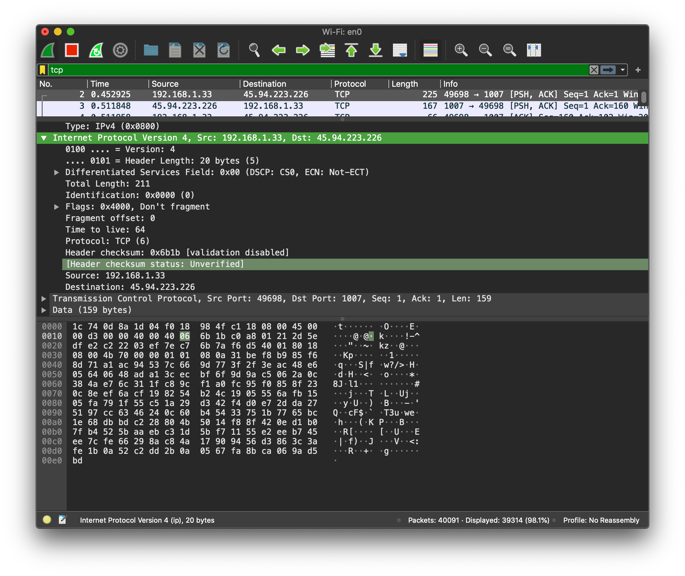
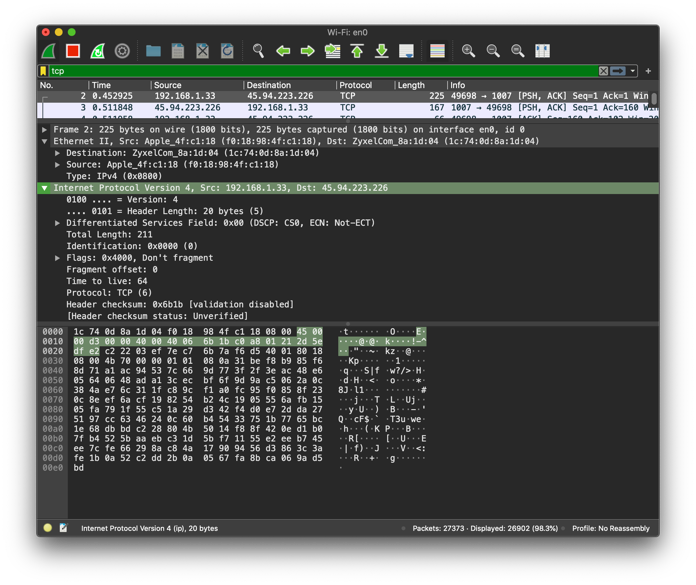
Анализируем второй пакет:



Первые 14 байтов отведены под следующие значения:



Далее идёт непосредственно заголовок пакета, и мы можем наблюдать:



4 – версия; IPv4

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

00d3 – длина пакета (Total Length); 60 октетов, включая заголовок и данные

0000 - идентификатор (Identification) пакета; значение, назначаемое отправителем пакета и предназначенное для определения корректной последовательности фрагментов при сборке пакета

4000 – смещение фрагмента (Fragmentoffset); определяет позицию фрагмента в потоке данных, количество восьмибайтовых блоков

40 – время жизни (Timetolive); число маршрутизаторов, которые может пройти этот пакет, 64

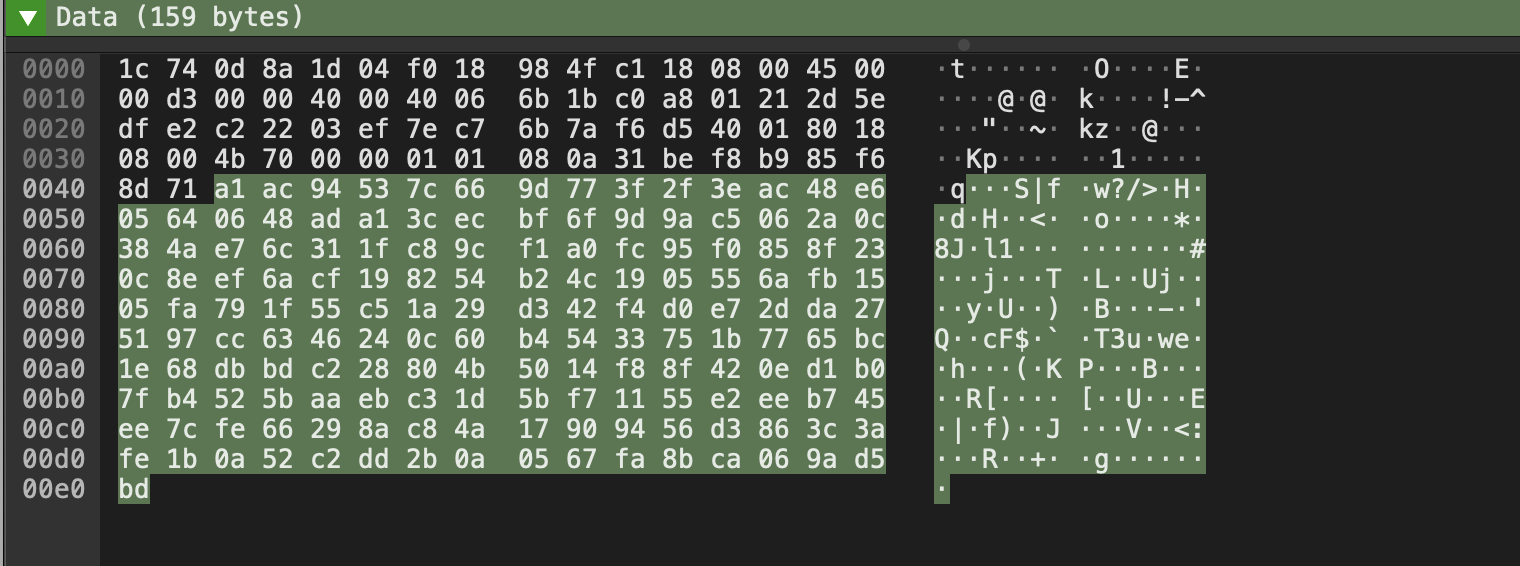
06 – протокол (Protocol); идентификатор, который указывает, данные какого протокола содержит пакет, 6- TCP

6b 1b - контрольная сумма заголовка (Header Checksum)

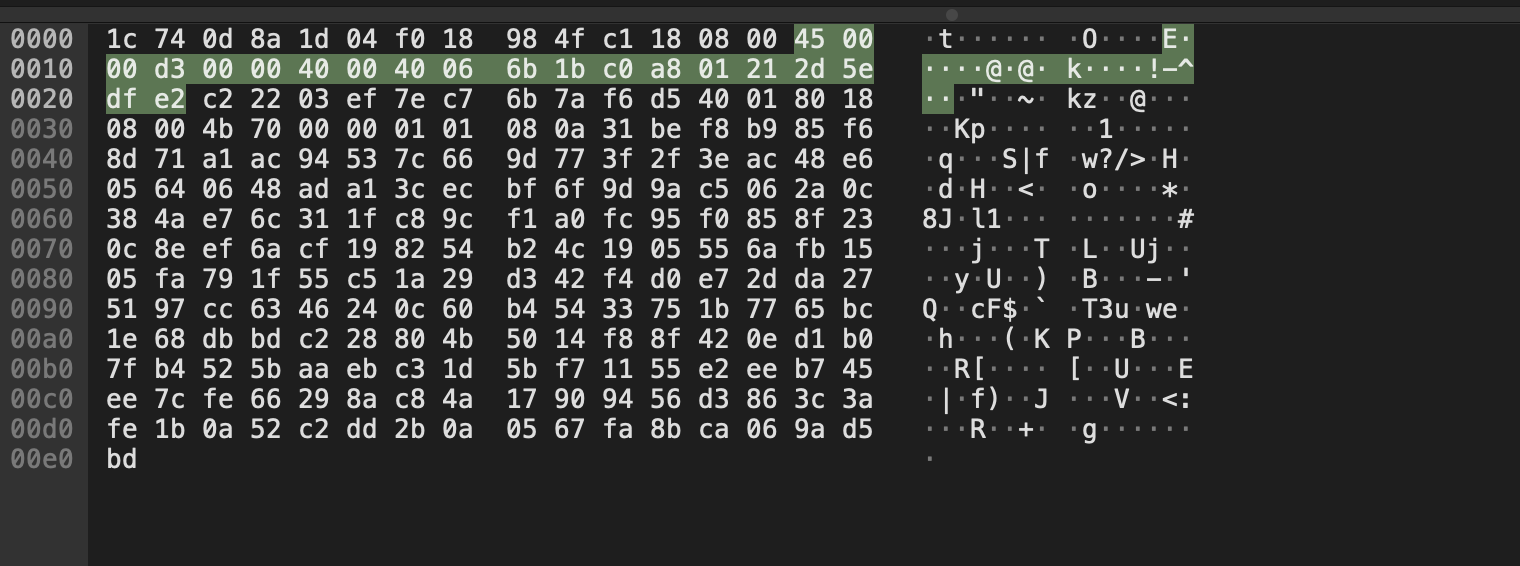
c0a80121 – адрес отправителя (Source); 192.168.1.33

2d5edfe2 – адрес получателя (Destination); 45.94.223.226

Последующие байты – это поле данных.



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



4500 + 00d3 + 0000 + 4000 + 4006 + 6b1b + c0a8 + 0121 + 2d5e + dfe2 =

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 работы изучили структуру IP-пакета, TCP-сегмента и UDP-датаграммы. Получили практические навыки в вычислении контрольной суммы заголовка IP-пакета.