МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. Р.Е. АЛЕКСЕЕВА» (НГТУ)

Институт ИРИТ

Кафедра «Информатика и системы управления»

ОТЧЕТ

по лабораторной работе №6

Выполнил:

Студент

группы 18-АС

Корнилов А.И

Проверил:

Гай В.Е.

Отчет защищен с оценкой: _____

Дата защиты «___» _____20__ г.

Нижний Новгород

2021 год

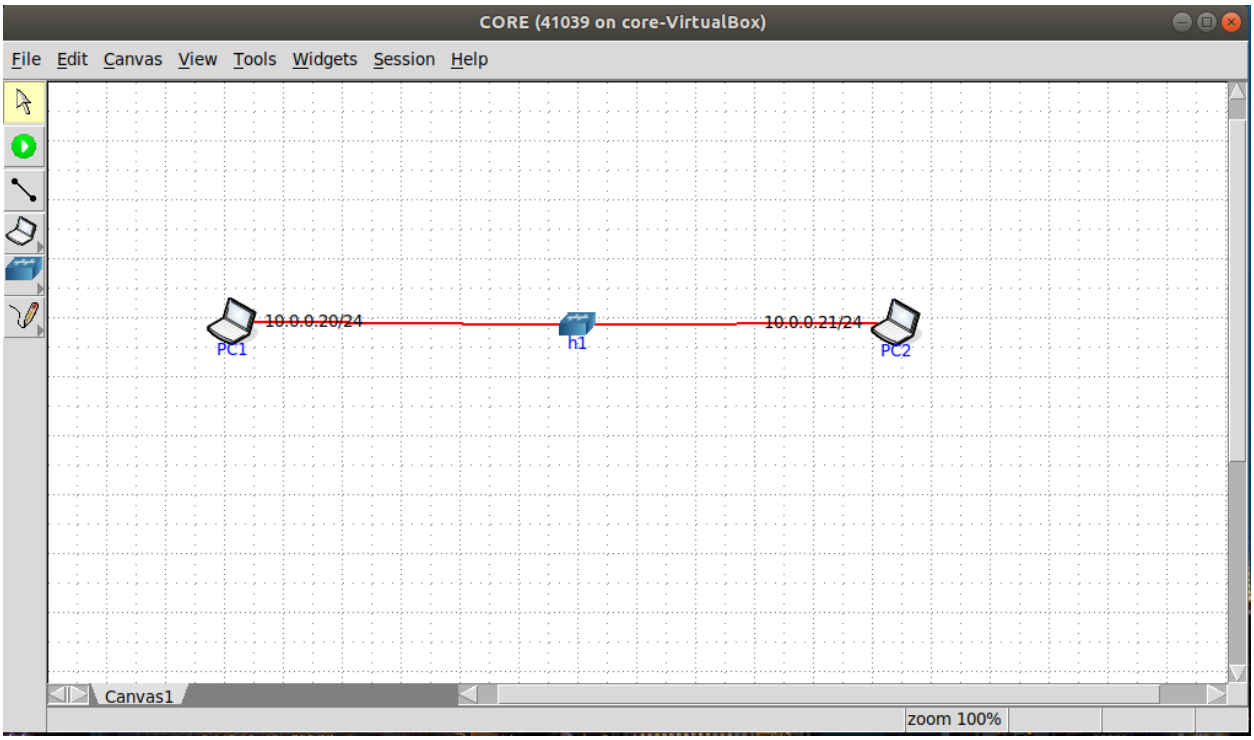
Задание на лабораторную работу:

1. Перехватить udp (icmp, tcp) пакет

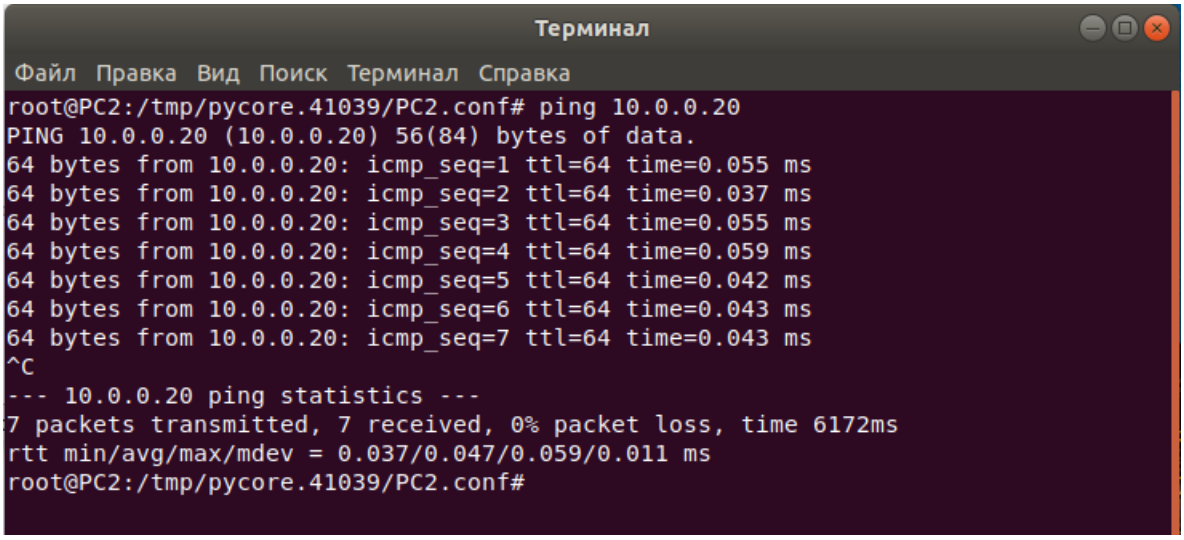
2. Рассчиать контрольную сумму заголовка вручную

3. Процесс расчёта привести в отчёте

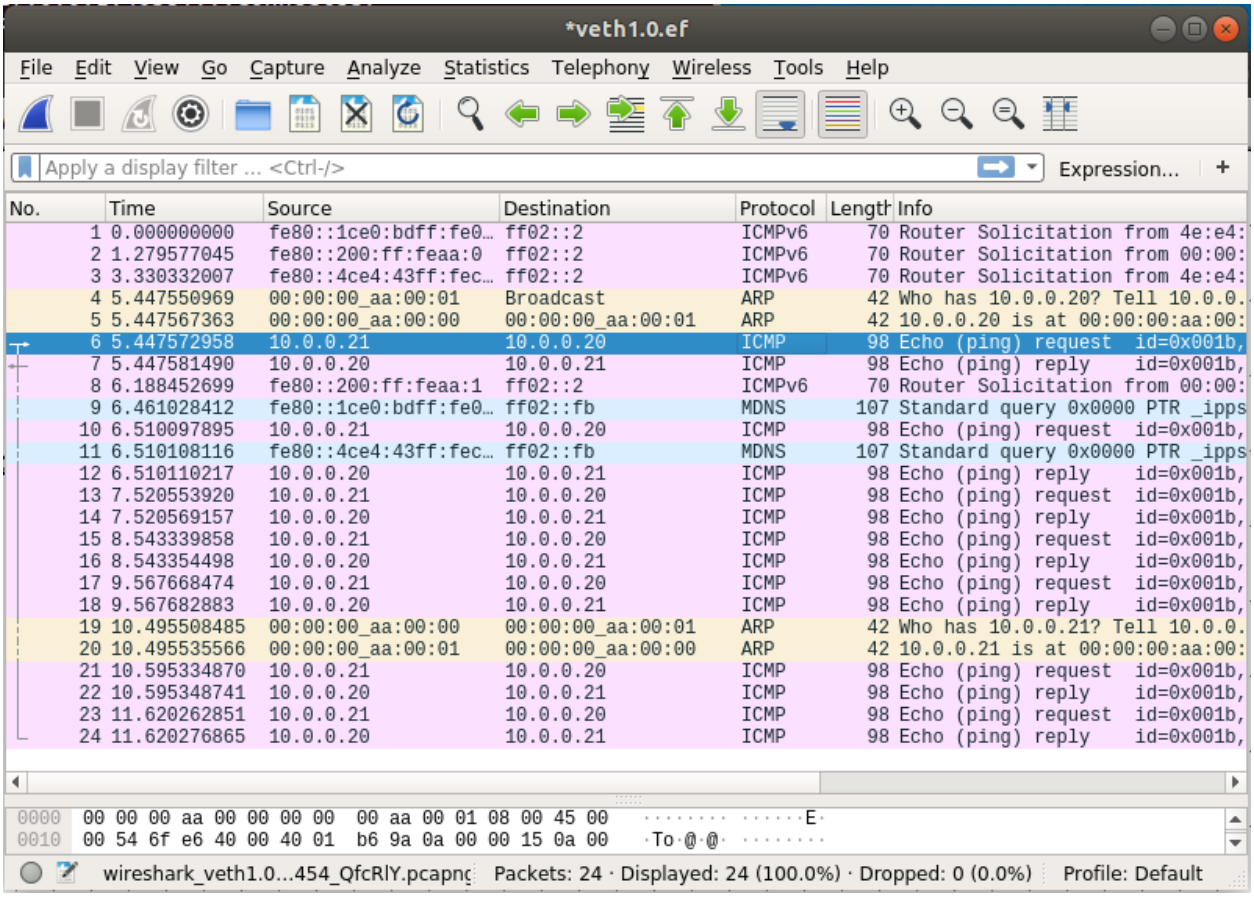
Ход работы:



Запустим ping с PC2 на PC1



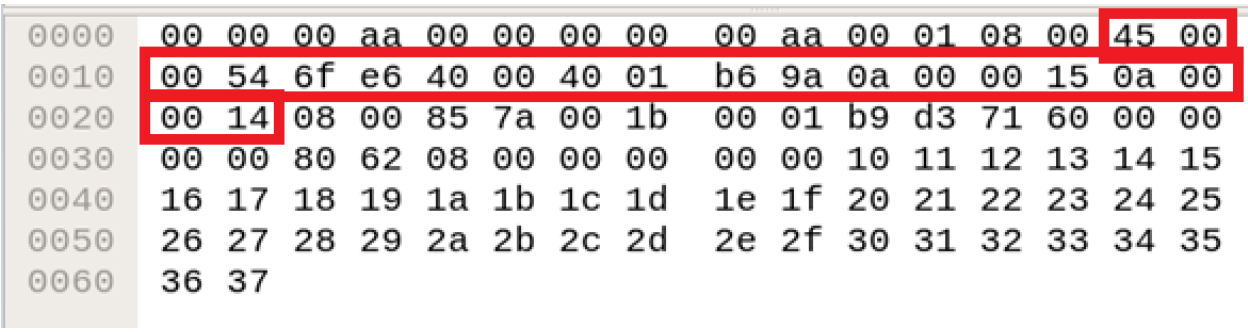
В wireshark выберем пакет.



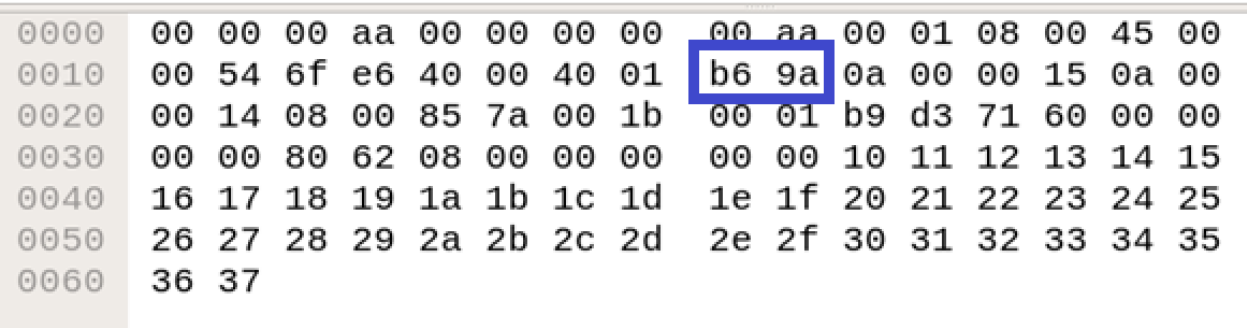
Рассмотрим кадр Ethernet:

```
0000  00 00 00 aa 00 00 00 00  00 aa 00 01 08 00 45 00
0010  00 54 6f e6 40 00 40 01  b6 9a 0a 00 00 15 0a 00
0020  00 14 08 00 85 7a 00 1b  00 01 b9 d3 71 60 00 00
0030  00 00 80 62 08 00 00 00  00 00 10 11 12 13 14 15
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35
0060  36 37
```

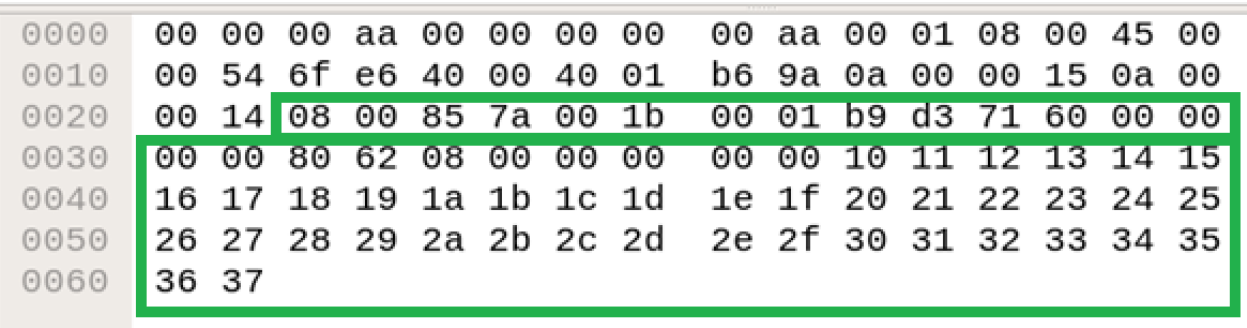
Заголовок IP-пакета:



Контрольная сумма:



Параметры ICMP протокола:



00 00 00 aa 00 00 – MAC-адрес получателя;

00 00 00 aa 00 01 – MAC-адрес отправителя;

08 00 – код протокола (IP);

Заголовок IP-пакета:

4 – номер версии протокола IP (IPv4);
5 – длина заголовка (пять 32-битных слов);
00 – тип сервиса: приоритет пакета (первые три бита) - 0, критерии выбора маршрута (задержка, пропускная способность и надежность) – так же 0;
00 54 – общая длина IP-пакета;
6f e6 – идентификатор пакета;

40 00– флаги и смещение фрагмента: первые три бита (флаги) – 0 1 0, где 2-й бит – флаг DF, который запрещает маршрутизатору фрагментировать пакет; так как пакет не фрагментируется, поле смещения – 0;
40 – время жизни пакета (в секундах – 64 с);
01 – протокол верхнего уровня (ICMP);
b6 9a– контрольная сумма заголовка;
0a 00 00 15 – IP-адрес источника
0a 00 00 14 – IP-адрес назначения

4500	0054
6FE6	4000
4001	0000
0A00	0015
0A00	0014

1) Разбиваем заголовок на слова по 16 бит и суммируем полученные 16-битные слова между собой:

$(4500)_{16} + (0054)_{16} + (6FE6)_{16} + (4000)_{16} + (4001)_{16} + (0000)_{16} + (0A00)_{16} + (0015)_{16} + (0A00)_{16} + (0014)_{16} = (14964)_{16}$

2) Поскольку результат сложения в двоичном представлении превышает 16 разрядов (или 4 шестнадцатеричных цифры), разбиваем его на два слова по 16 бит каждое и снова их суммируем:

$(0001)_{16} + (4964)_{16} = (4965)_{16}$

3) Находим контрольную сумму, как двоичное поразрядное дополнение результата сложения:

$CS_{IP} = (FFFF)_{16} - (4965)_{16} = (B69A)_{16}$

Контрольные суммы совпадают.