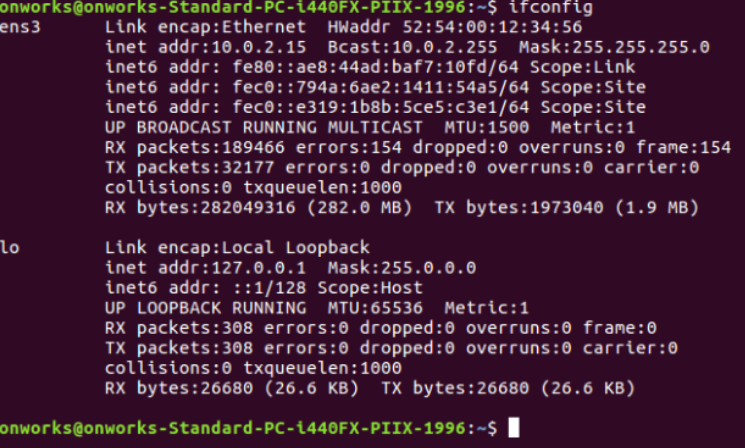
**Тестовое задание Галишина Павла Михайловича**

**Задание 1.**

Для того чтобы получить подробную запись трафика http, а также сохранить ее нужно использовать утилиту tcpdump, которая внедряется между драйвером сетевой карты и ядром операционной системы используя библиотеку pcap. Pcap – служит для создания программ анализа сетевых данных, поступающих на сетевую карту компьютера.  
 Для того чтобы получить какую-то запись, нужно узнать какой интерфейс доступен для вывода. Для этого используем команду: ifconfig. После чего получим список доступных интерфейсов.

  
Рисунок 1 – Список доступных интерфейсов

Для того чтобы получить информацию о проходящем трафике, используем команду:

sudo tcpdump -I [интерфейс]

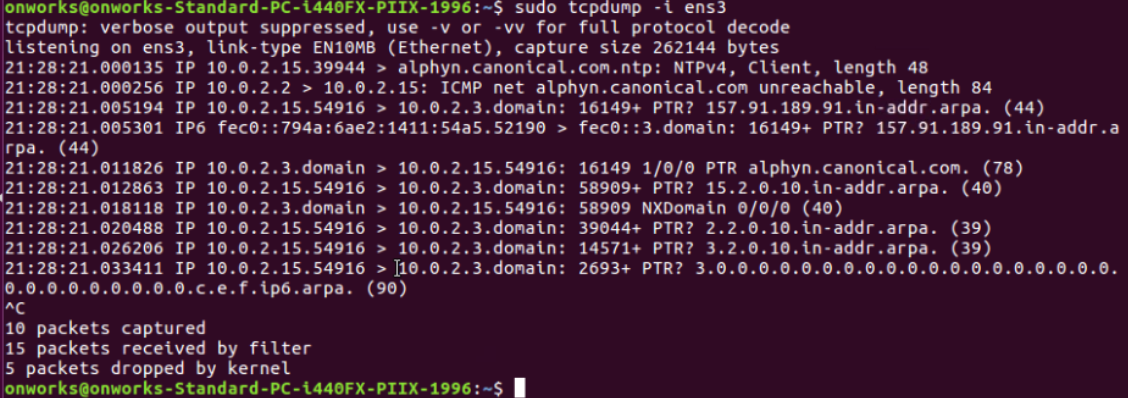


Рисунок 2 – Самый просто метод вывода информации о трафике

Усложним нашу задачу и выведем подробную запись трафика и запишем ее в файл. Для этого используем команду:

sudo tcpdump -i [интерфейс] -c [количество строк] -w [название файла].pcap

Где: параметр «-w» - запись трафика в файл.

Также используем параметр «-с» для того, чтобы ограничить количество выведенных записей о трафике.

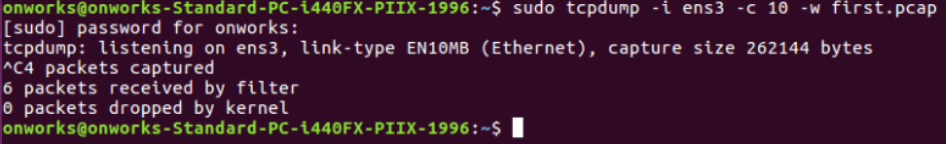


Рисунок 3 – Запись трафика в файл

После чего конечно же мы захотим его прочитать, для этого можно использовать как программу Wireshark, для того чтобы получить красивую систематичную картинку или же снова можем использовать команду из tcpdump:

sudo tcpdump -i [интерфейс] -r [название файла].pcap

Где: параметр «-r» - прочтение трафика из файла.

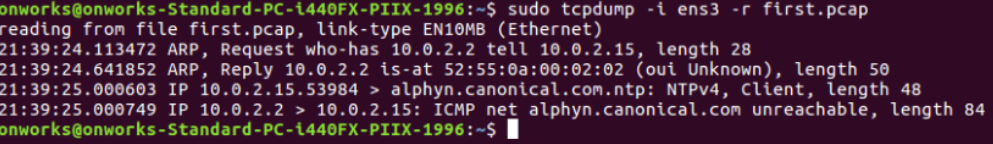
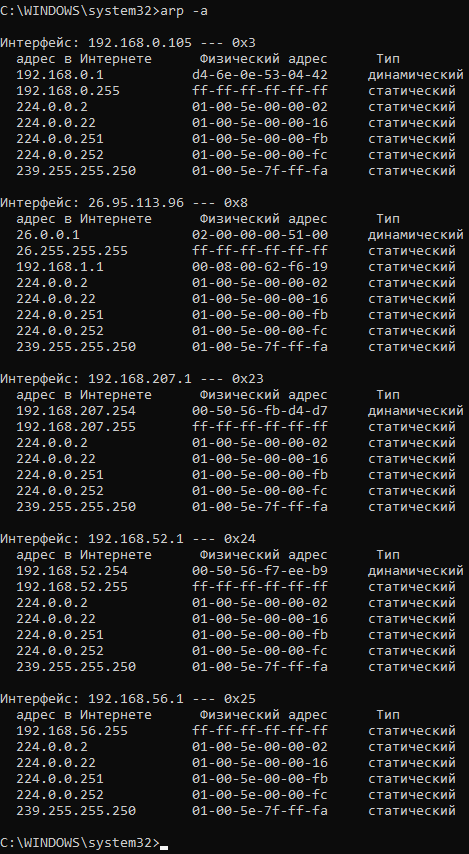


Рисунок 4 – Прочтение трафика из файла.

Где: первая строка – время, вторая строка – протокол, третья строка – тип сообщения.

**Задание 2.**

Для того чтобы получить информацию о таблице сетей, нужно ввести команду arp -a. После этого мы получим полный список внутренних ip-адрессов.  
  
  
Рисунок 5 – Список внутренних адресов

Для того чтобы изменить таблицу сети, используем команду:

arp -s [ip-aдрес] [физический адрес]

Где: параметр «-s» - добавляет значение в таблицу.



Рисунок 6 – Добавление значения в таблицу

Мы не получили никакого сообщения о добавление нового значения, но для того чтобы увидеть добавленное значение, снова нужно ввести команду arp -a.

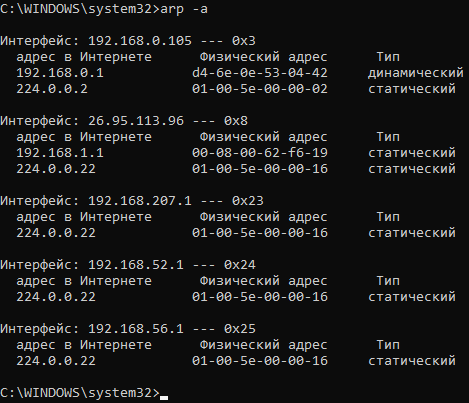


Рисунок 7 – Просмотр добавленного значения в таблицу

Также мы можем удалить значение из таблицы используя команду arp -d, но при использовании этой команды удалиться вся информация о таблице сети. Для того чтобы удалять определенный адрес используем команду:

arp -d [ip-aдрес] [физический адрес]

Добавим еще немного значений и получим следующий список.

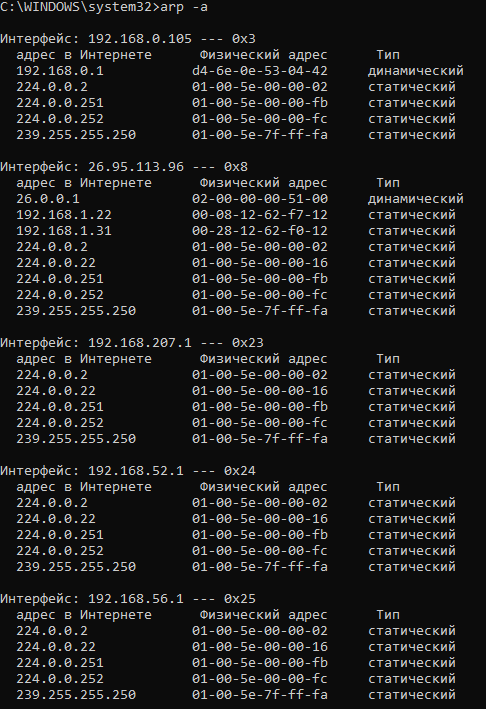


Рисунок 8 – Список значение после добавления их в таблицу

После чего используем команду для удаления и получаем следующие значения.

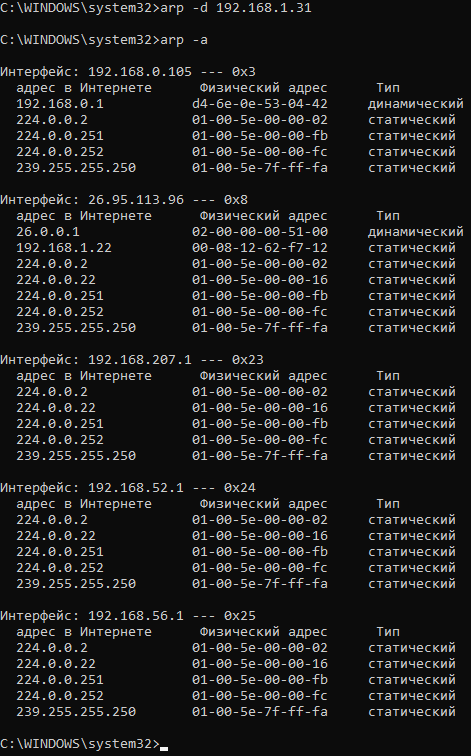


Рисунок 9 – Список значений после удаления одного из них