**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Российский экономический университет имени Г.В. Плеханова»**

**Московский приборостроительный техникум**

**Практическая работа №1**

по учебной практике

УП.01.02 Средства мониторинга и анализа в локальных сетях

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*индекс по УП и наименование практики*

Профессионального модуля ПМ.01«Выполнение работ по проектированию

сетевой инфраструктуры»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*индекс по УП и наименование профессионального модуля*

Специальность 09.02.06 Сетевое и системное администрирование

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*код и наименование специальности*

Студент Нилов Егор Сергеевич

*(фамилия, имя, отчество)*

Группа СА50-1-22

Руководитель по практической подготовке от техникума

Кульчинская Нелли Андреевна

*(фамилия, имя, отчество)*

«\_\_\_\_» \_\_\_\_\_\_\_\_\_ 2024 года

1. Смотрим какие интерфейсы доступны для прослушки

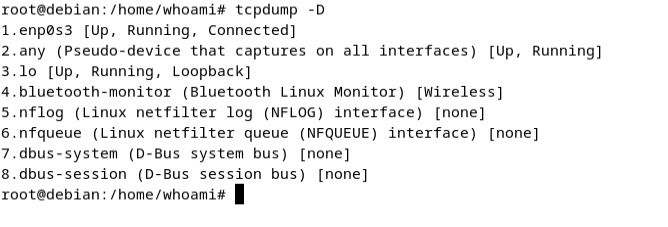
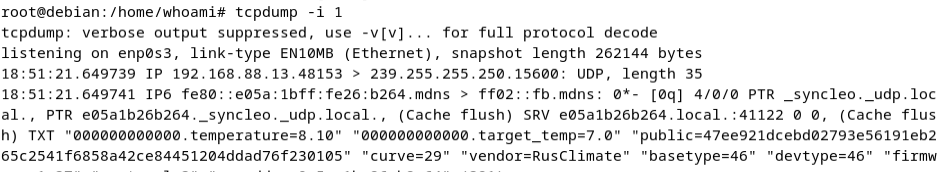


Рис. 1 - все интерфейсы

1. Слушаем определенный интерфейс, например 1 (enp0s3)



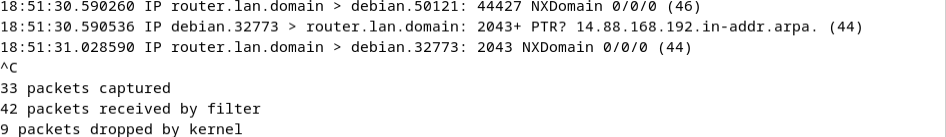


Рис. 2 – интерфейс enp0s3

1. Смотрим интерфейсы, которые есть на виртуальной машине Debian (lo, enp0s3)

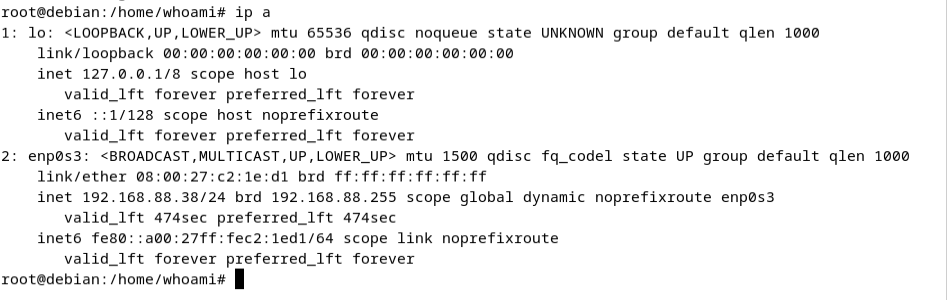


Рис. 3 - интерфейсы

1. Запускаем прослушку на интерфейсе enp0s3 и отрываем какой-нибудь сайт.

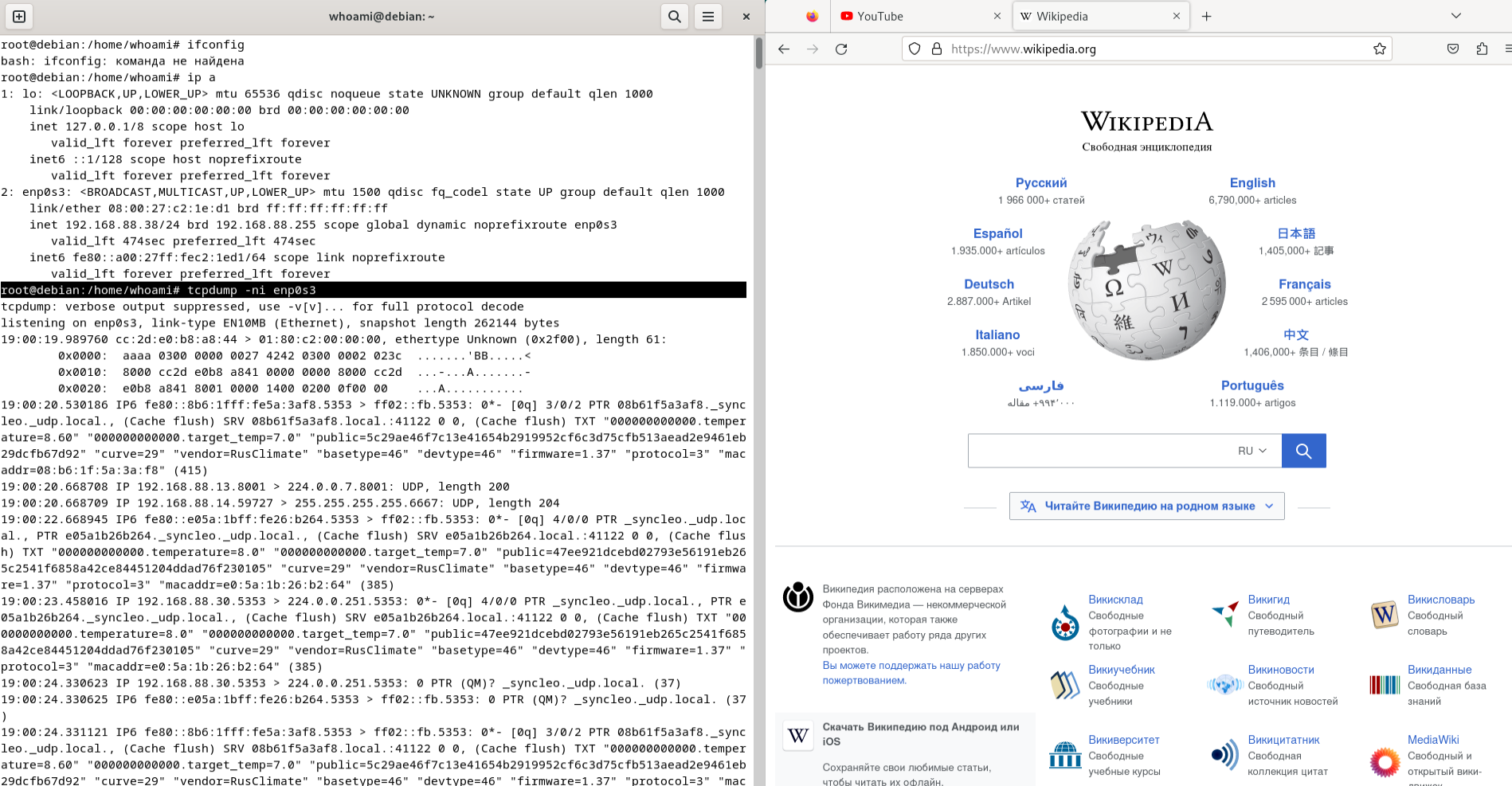


Рис. 4 – запускаем прослушку

1. Если мы хотим отразить содержимое наших пакетов, то надо добавить ключ -X и ключ -vv для большей информации

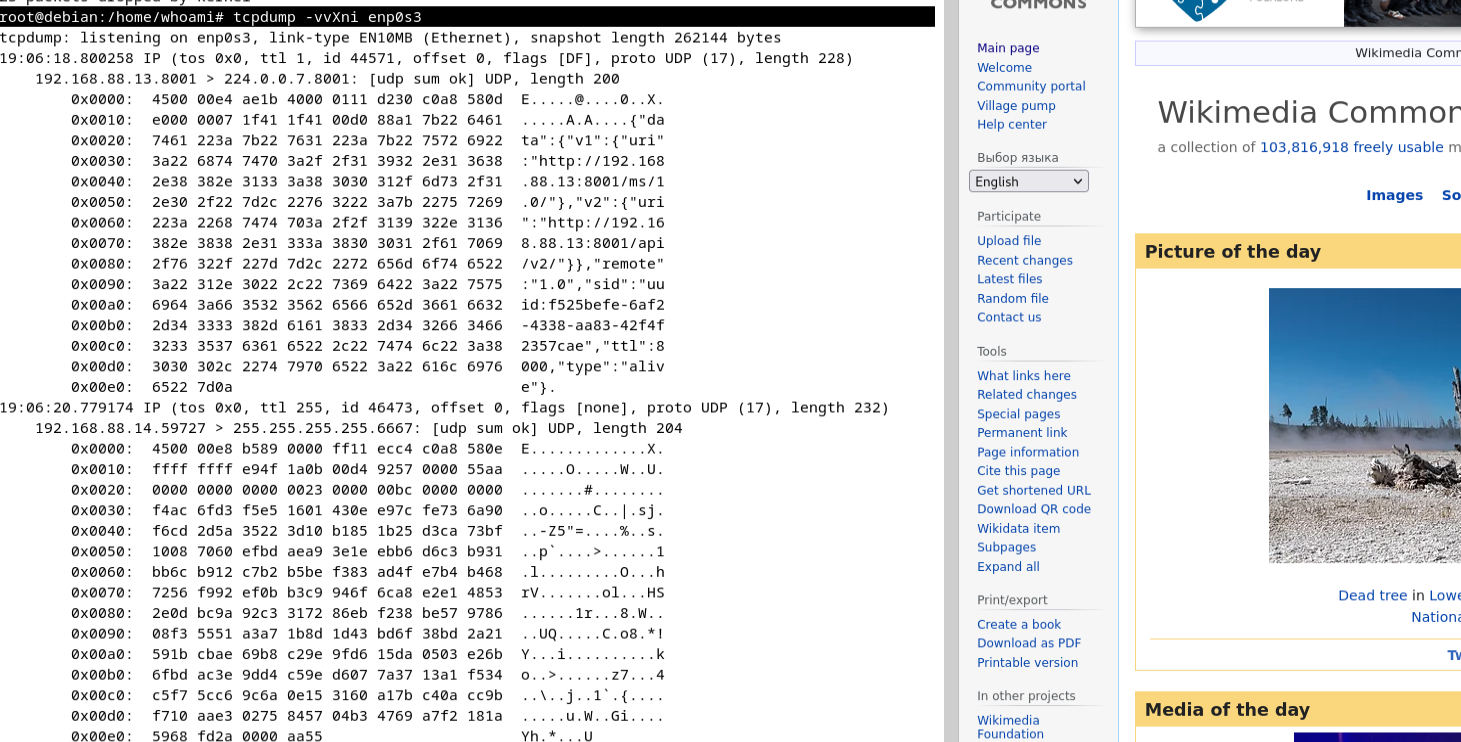
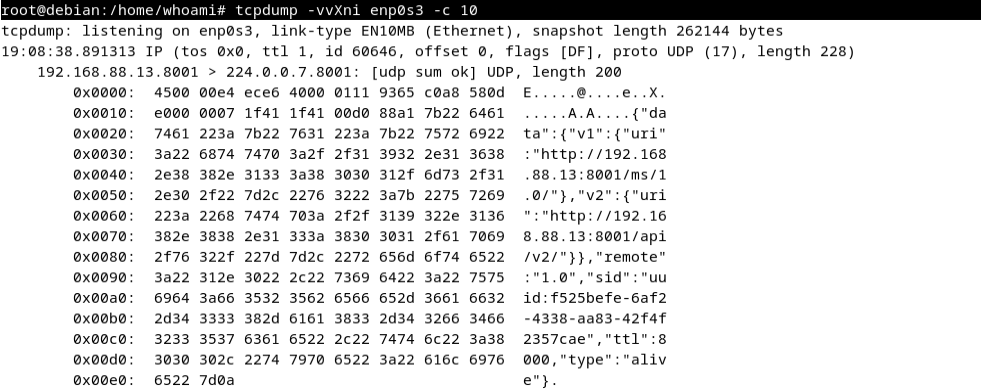


Рис. 5 – использование разных ключей

1. Чтобы не нагружать систему можно ограничить кол-во прослушанных пакетов с помощью ключа -c, например до 10 пакетов



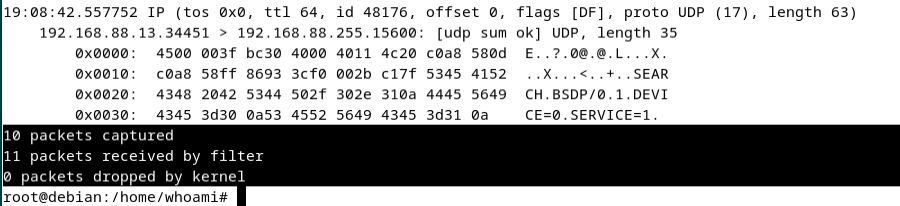


Рис. 6 – ограничение по пакетам

1. Отображение mac адресов хостов, которые участвуют во взаимодействии это можно сделать с помощью ключа -e

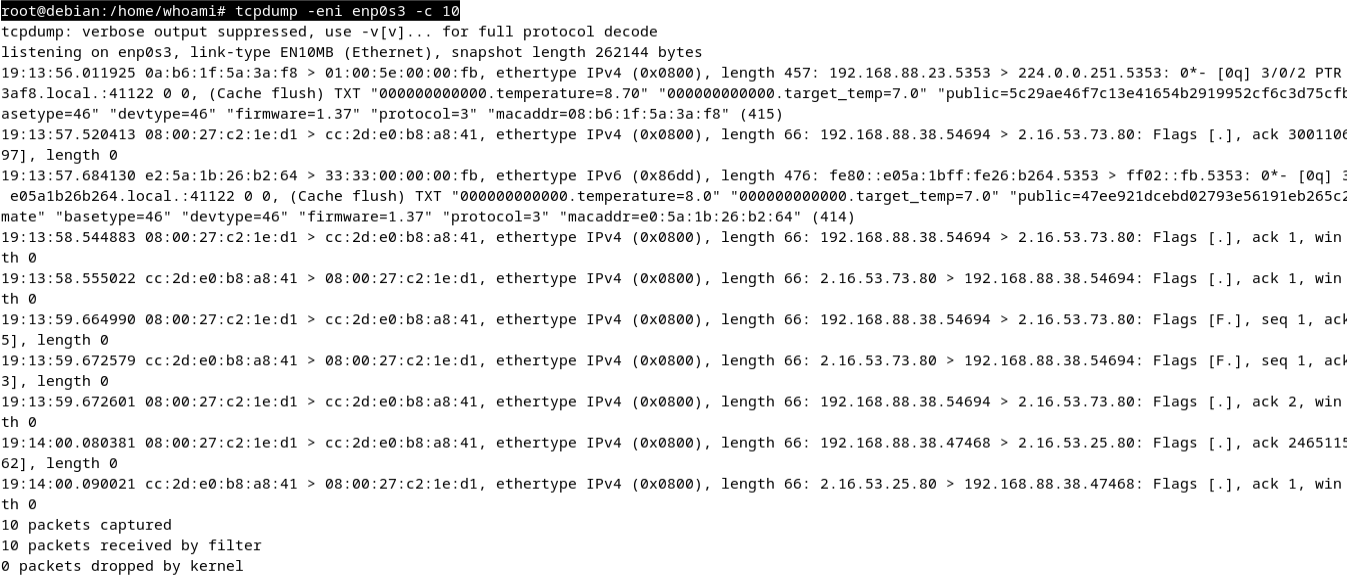


Рис. 7 – mac адреса хостов

1. Можно посмотреть, что за устройство по его mac-address через специальный сайт: macaddress.io

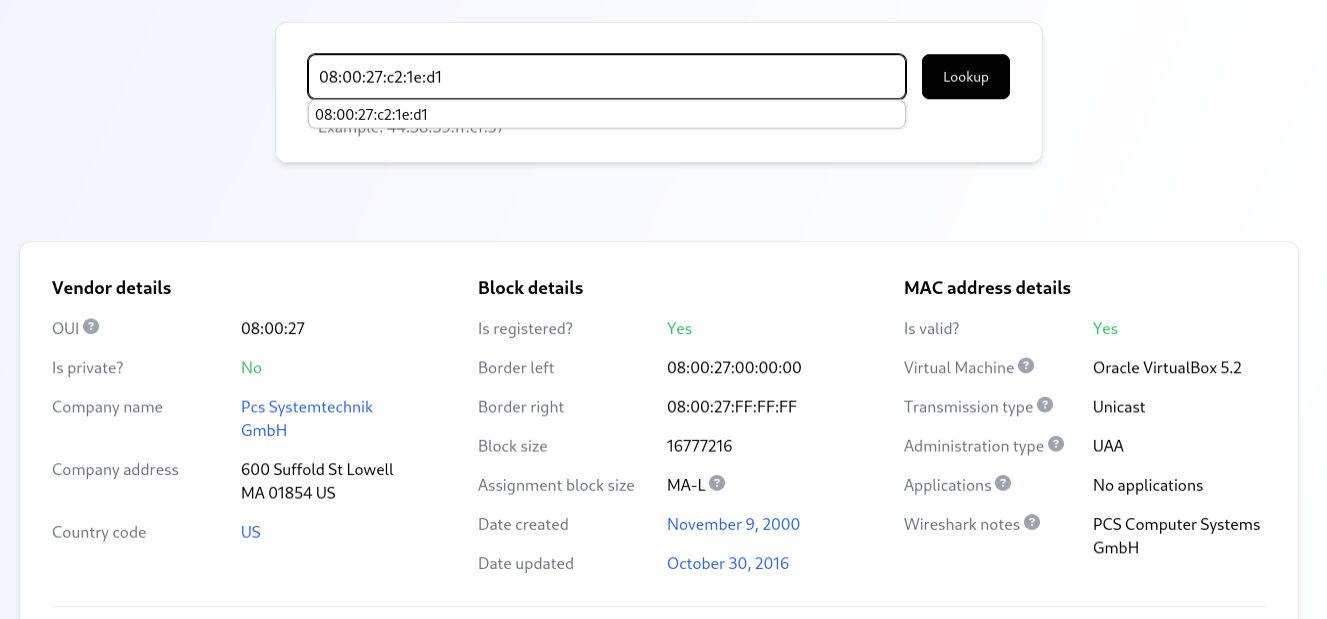
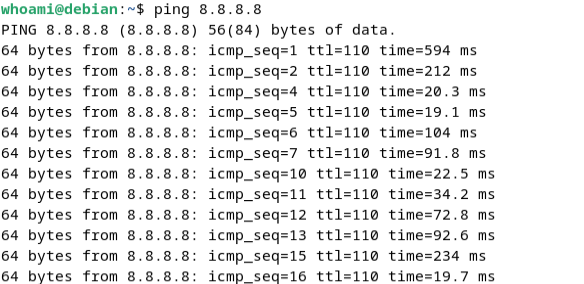


Рис. 8 – устройство и его mac

1. Отфильтровываем трафик по отдельному хосту. Параллельно запускаем команду ping на google и пишем host 8.8.8.8 (ip google.com).



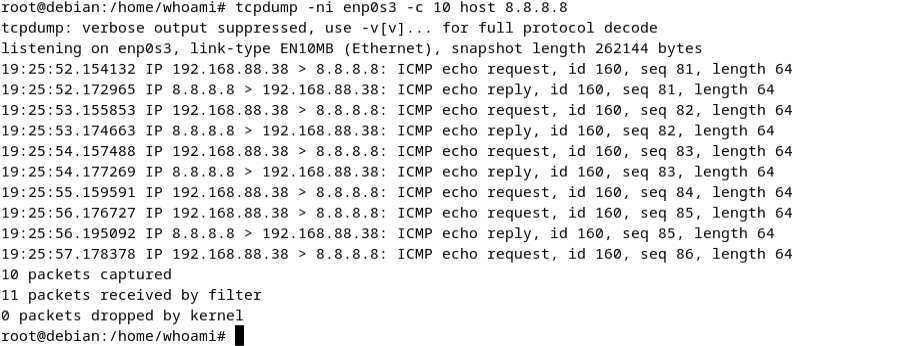


Рис. 9 – фильтр по отдельному хосту

1. Чтобы не собирать пакеты в обе стороны надо добавить dst (distention)

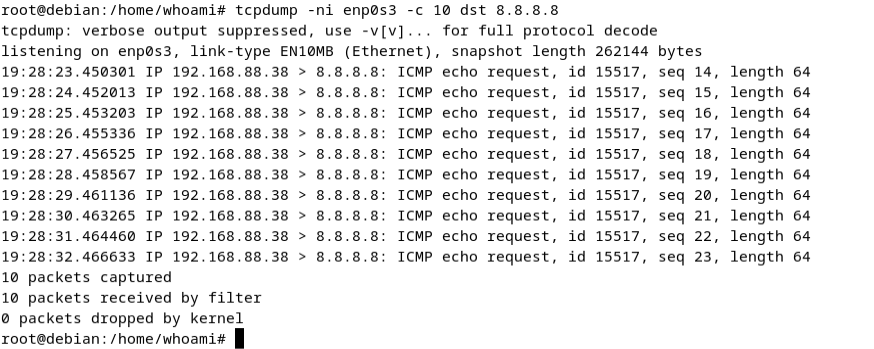
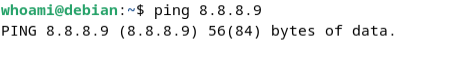


Рис. 10 – собирать пакеты в одну сторону

1. Можно прослушивать не только по хосту, но и по целой сетке, для этого есть команда net.



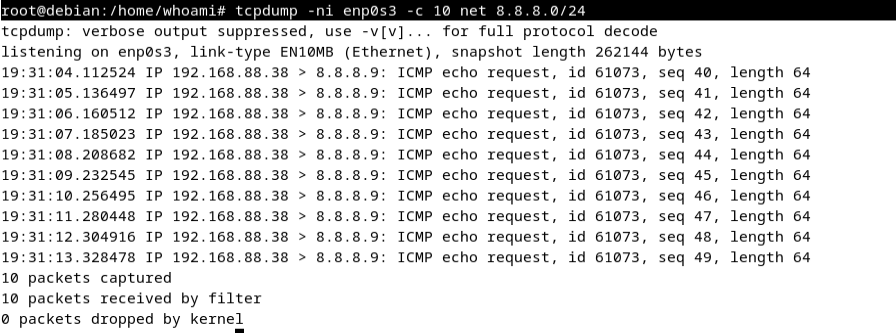


Рис. 11 – прослушка по целой сетке

1. Теперь можно прослушать по порту, например 80 (port 80), расширим информацию по пакетам (-vv) и выведем содержимое пакета (-X) и открываем любой сайт, например blog.netskils.ru

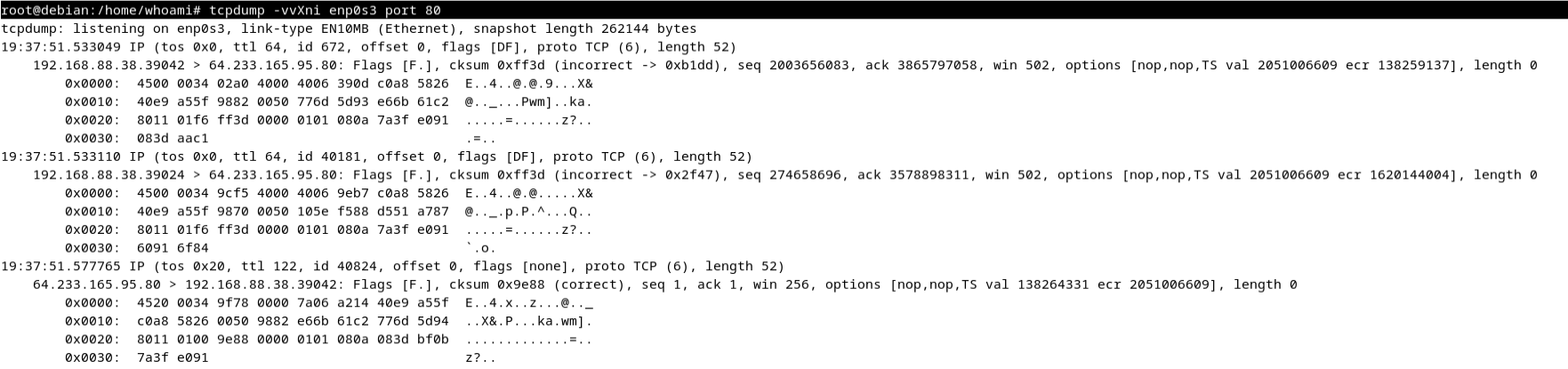


Рис. 12 – прослушка по порту

1. Можно положить дополнительный фильтр с помощью grep который, например будет искать в содержимых пакетах слово “tcpdump”, в это время на сайте сделать запрос tcpdump.

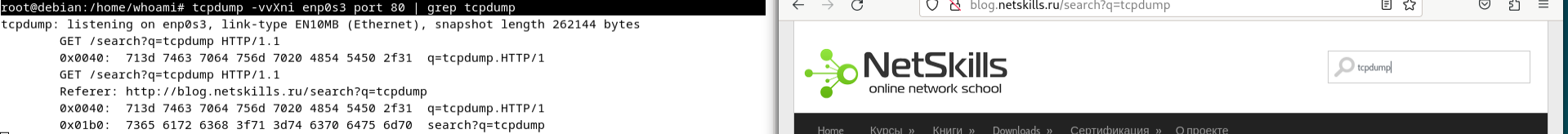
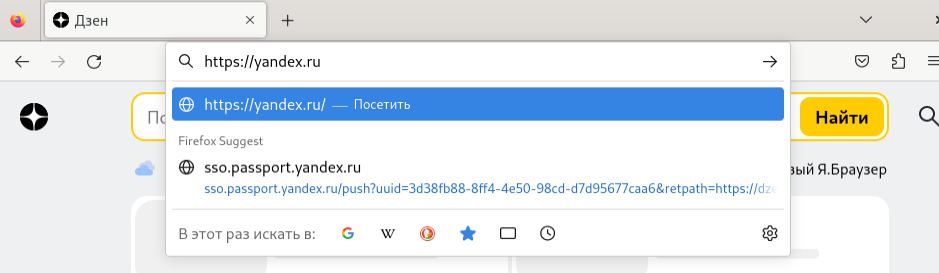
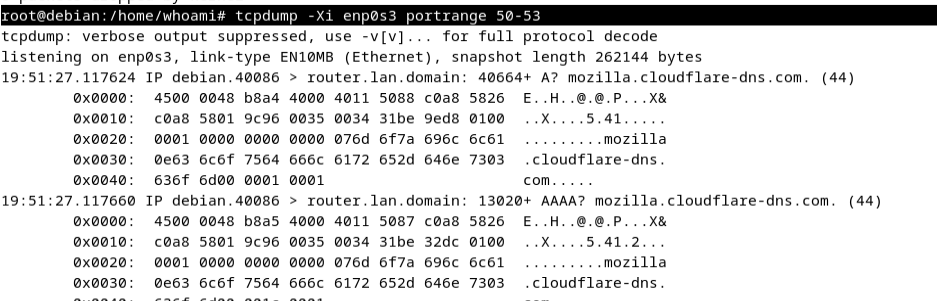


Рис. 13 – ищем слово в пакетах

1. Можно прослушать сразу по нескольким портам portrange, 53 порт – dns





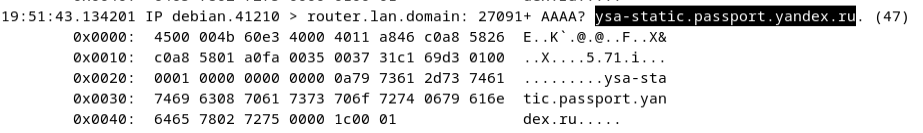
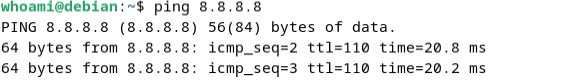


Рис. 14 – прослушка по нескольким портам

1. Также можно мониторить по конкретному протоколу например: icmp



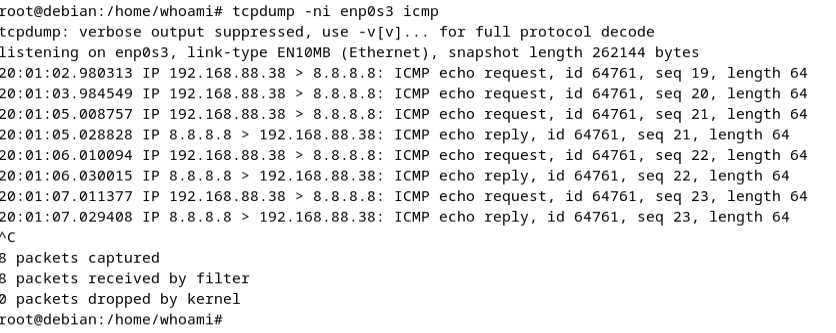


Рис. 15 – мониторинг по протоколам

1. Теперь можно рассмотреть реальный пример. Просматривать будем трафик моего маршрутизатора

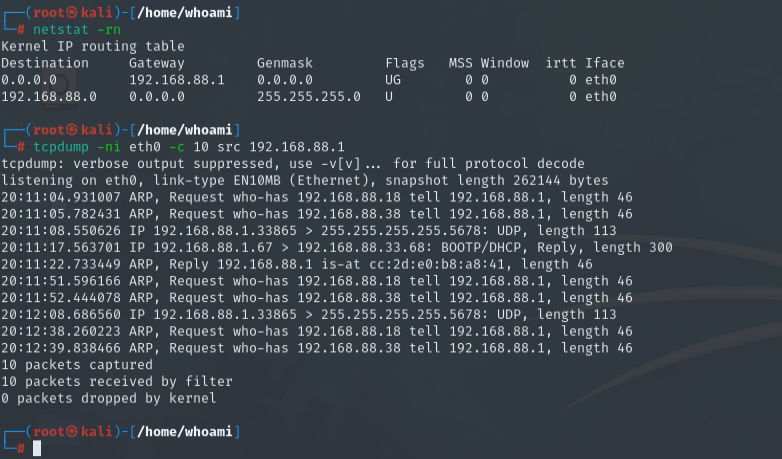
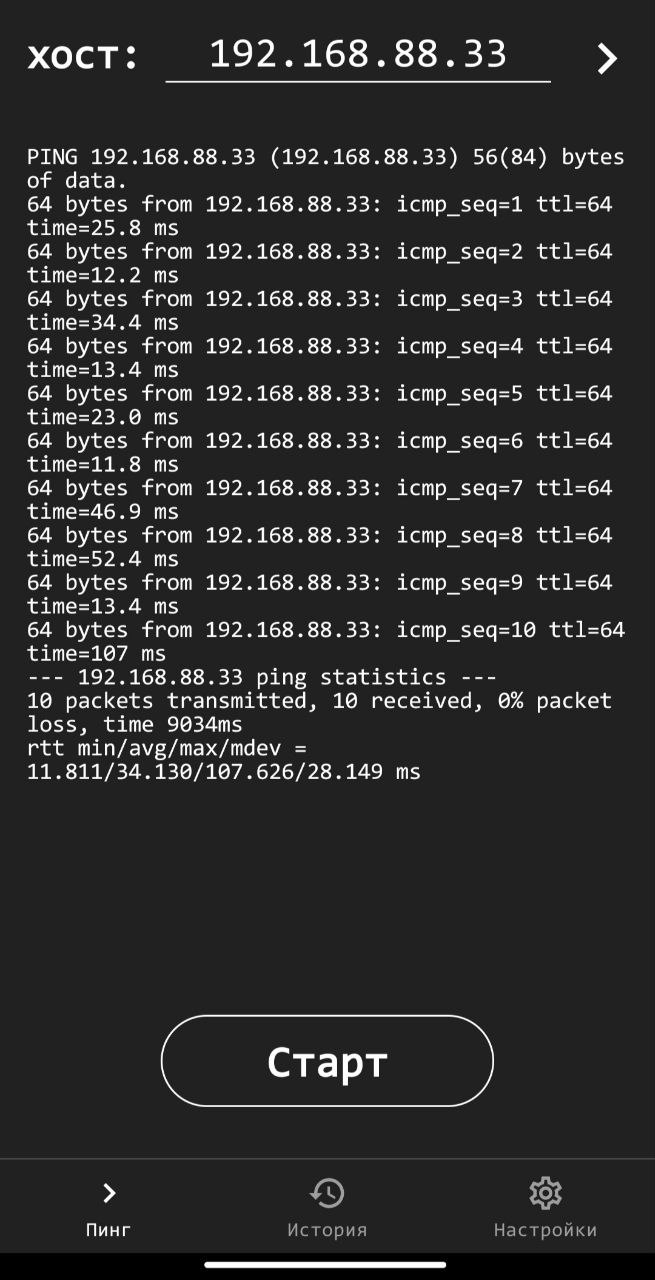


Рис. 16 – трафик моего маршрутизатора

1. Теперь попробуем дождаться пингов от телефона



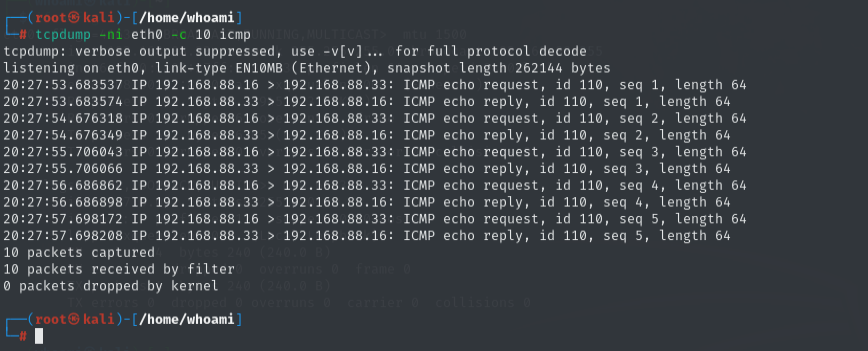
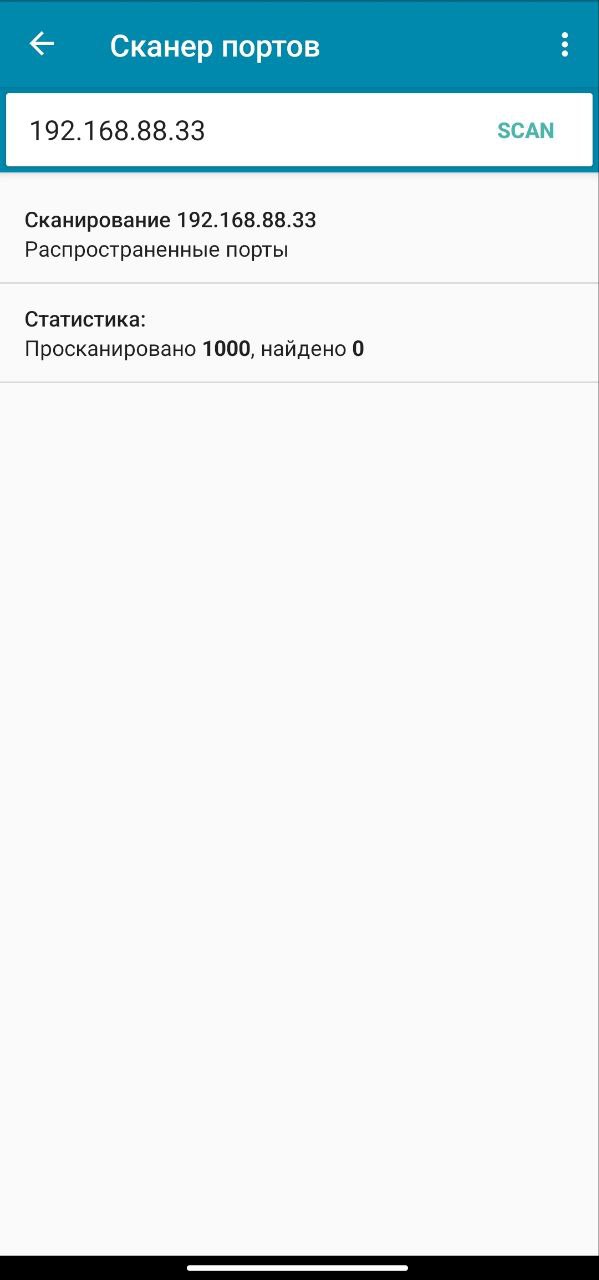


Рис. 17 – пинги от телефона

1. Теперь просканируем порты с помощью телефона



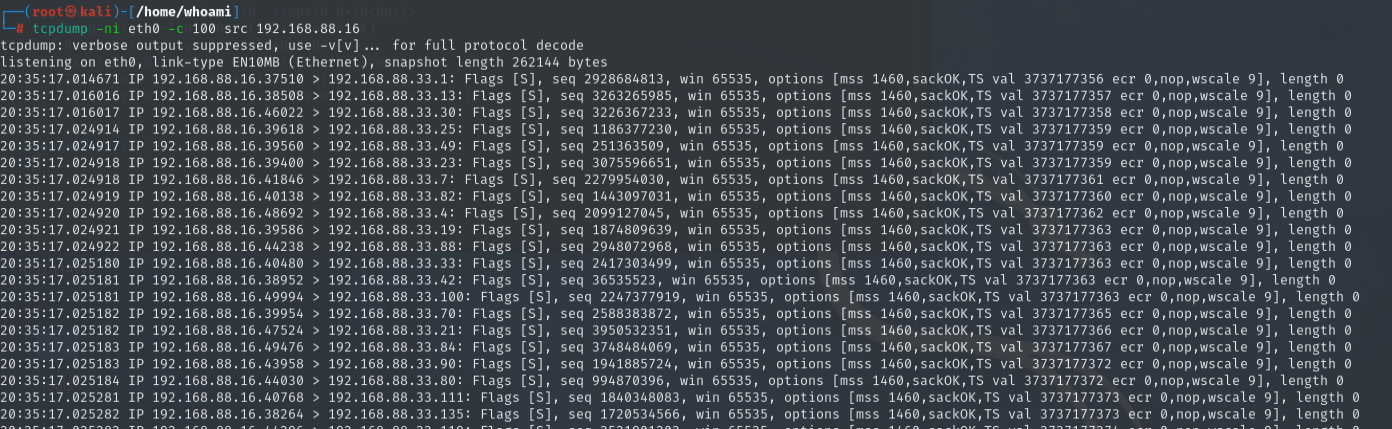
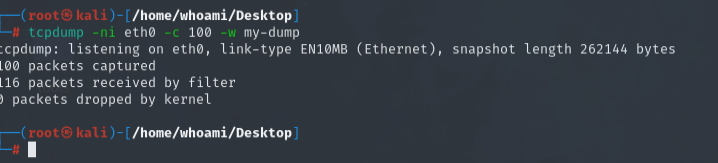


Рис. 18 – скан портов через телефон

1. Теперь запишем весь трафик на интерфейсе eth0 в отдельный файл



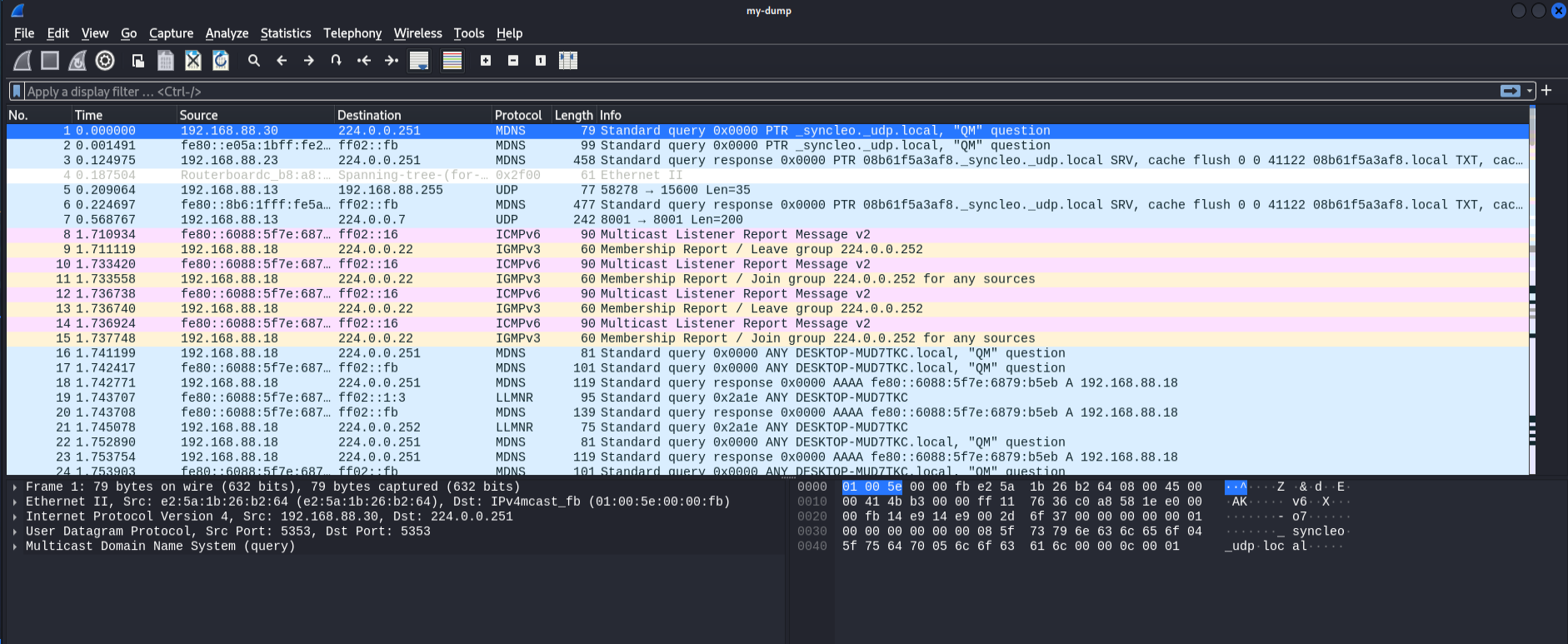


Рис. 19 – запись прослушки в файл