МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

ОТЧЕТ

по лабораторной работе №1

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

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

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Демин Д.И.

(подпись) (фамилия, и.,о.)

18-В-1

(шифр группы)

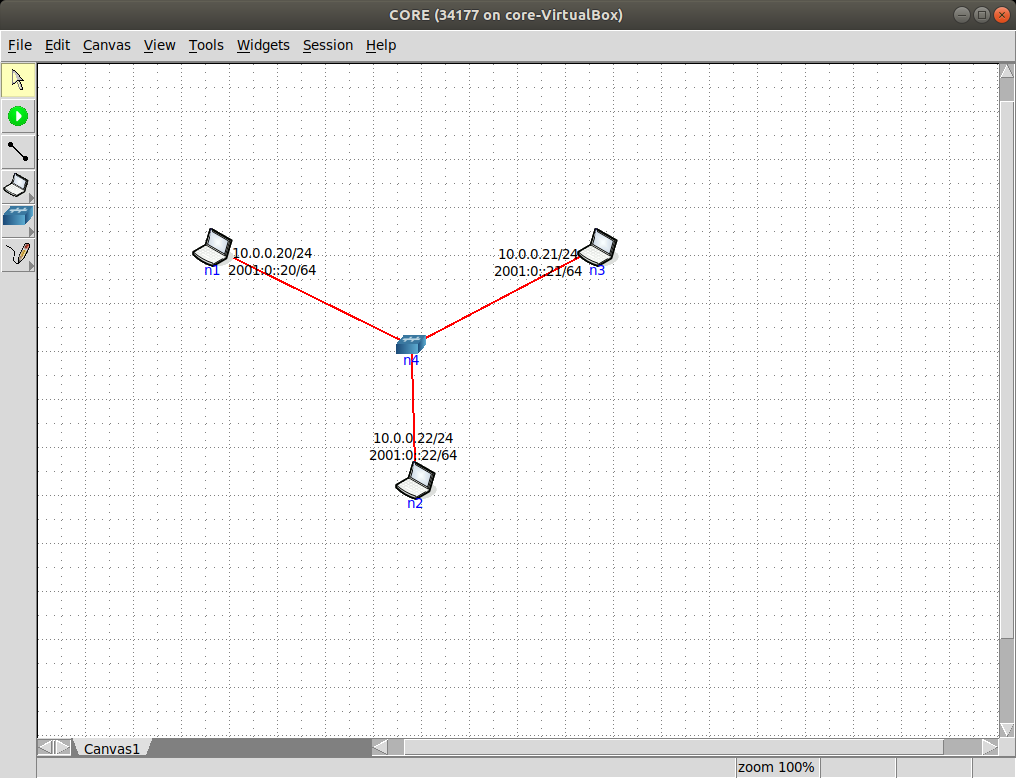
Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

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

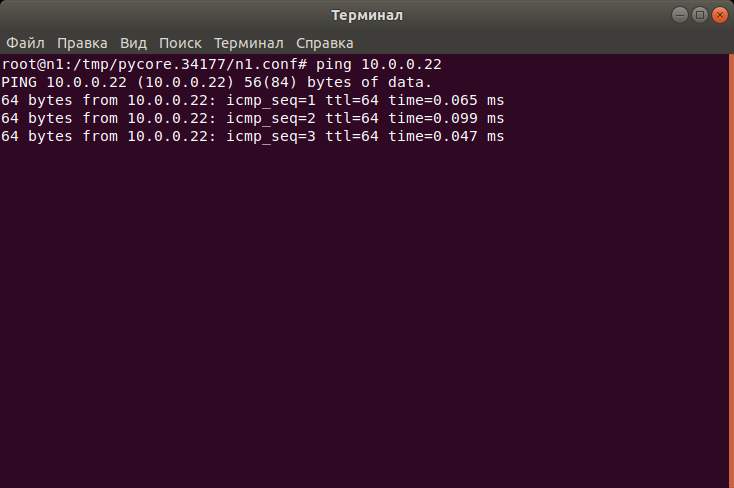
Нижний Новгород 2020

**Работа с анализатором протоколов tcpdump**

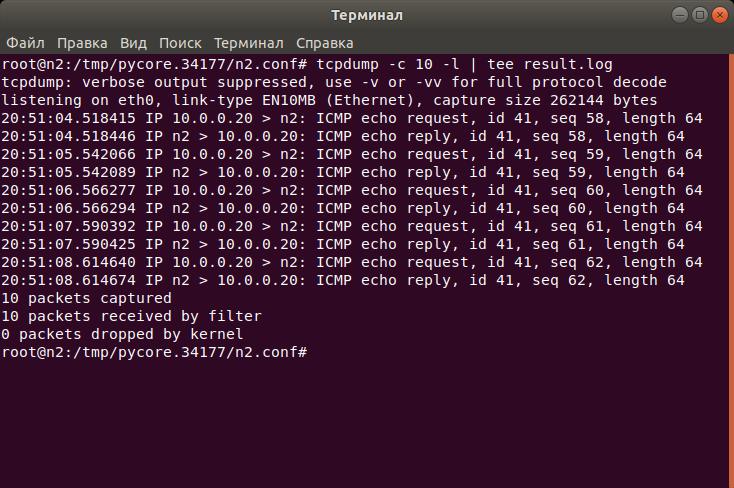
1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

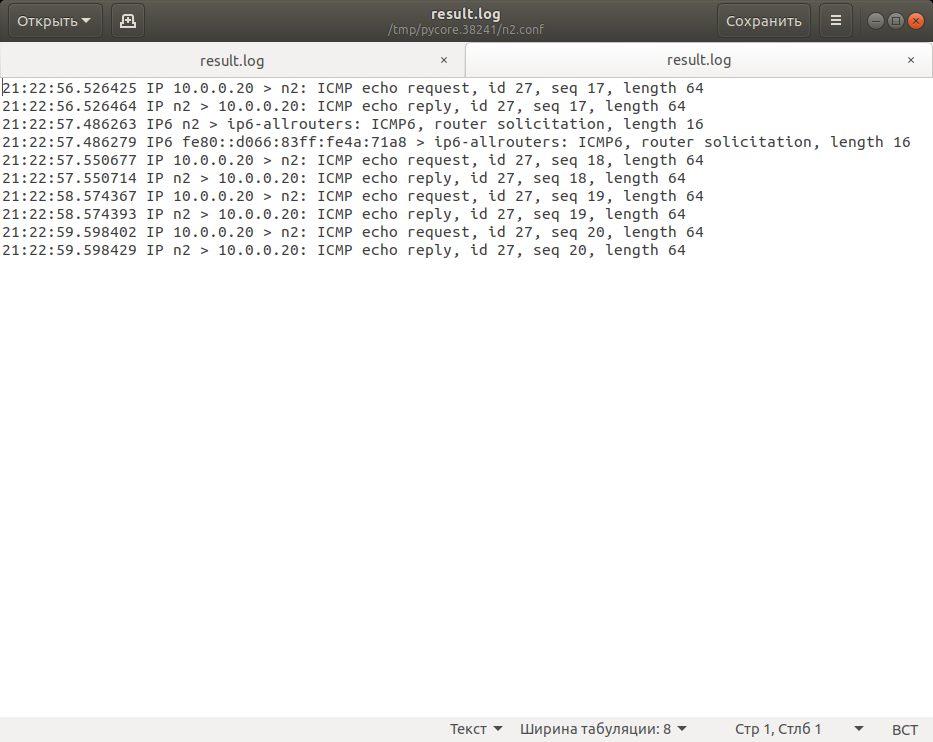


Передаем пакеты с хоста 1 на хост 2.



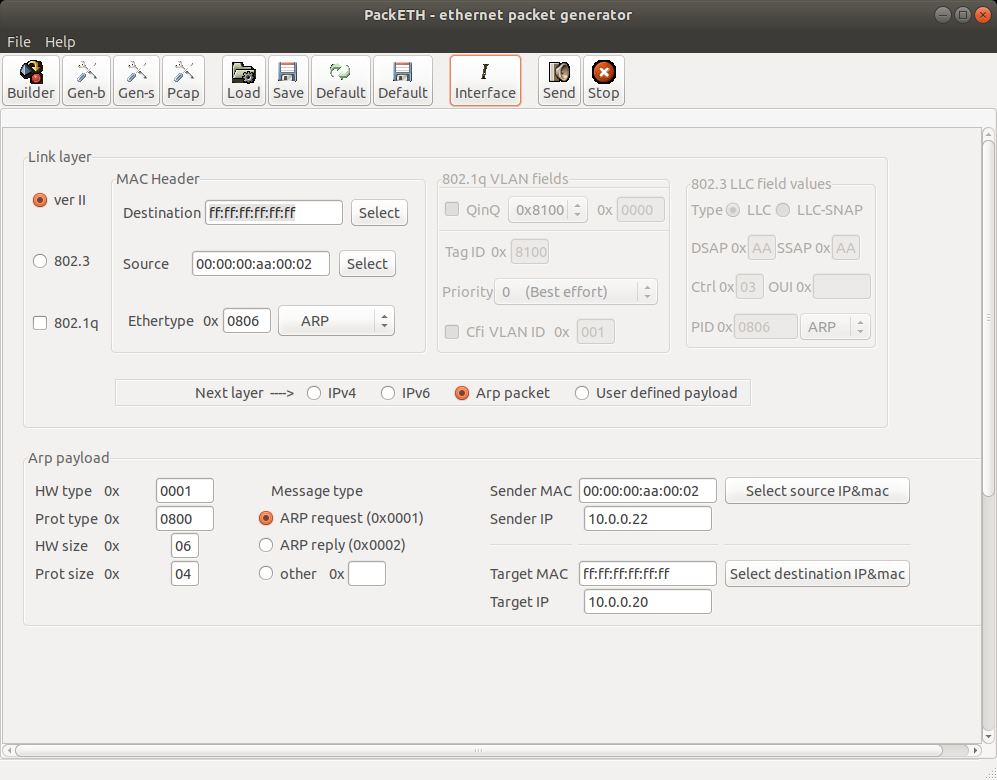
На хосте 2 запускаем tcpdump с нужными нам параметрами.



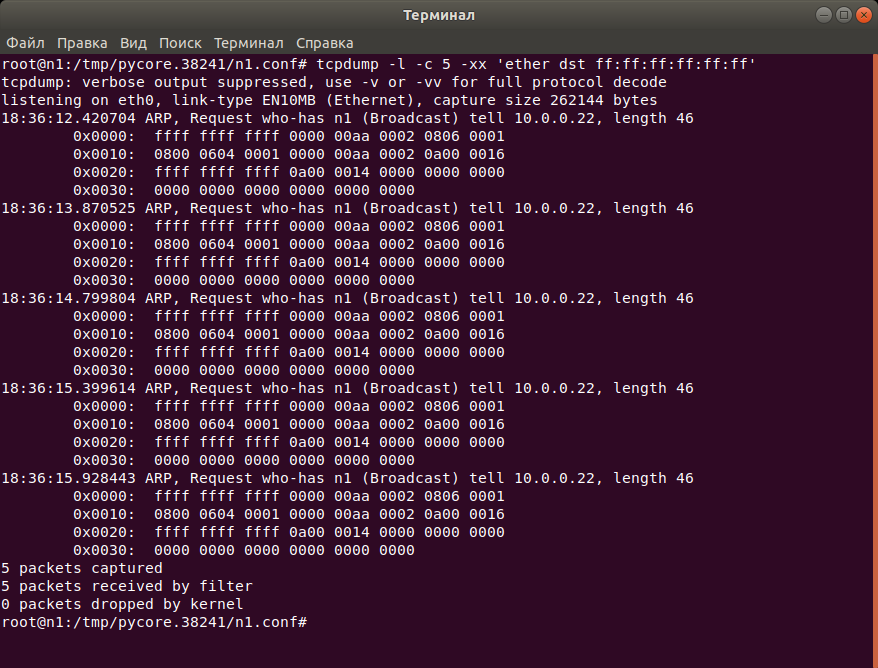


2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

С помощью PackEth формируем широковещательный MAC-пакет и отправляем его с n2 на n1.

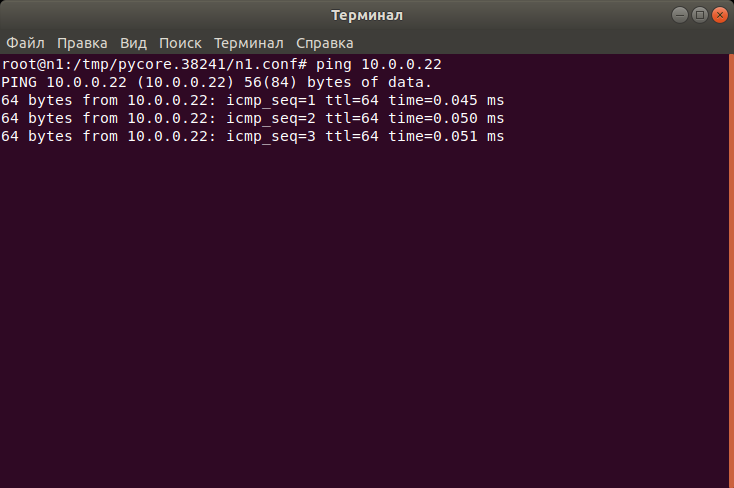


На хосте n1 запускаем tcpdump с фильтром и отправляем данные с n3.

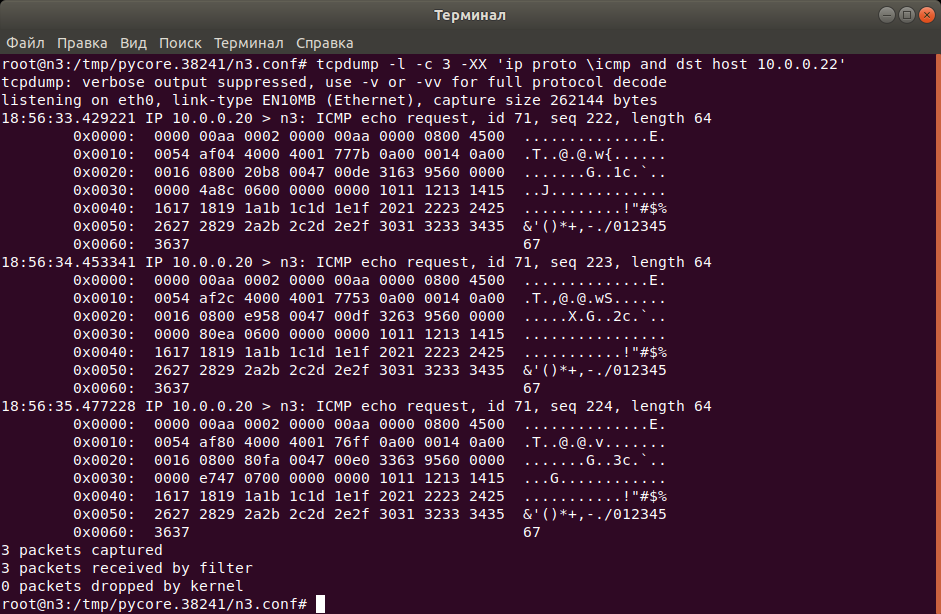


3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов воспользоваться утилитой ping.

Отправляем данные на хост n3.

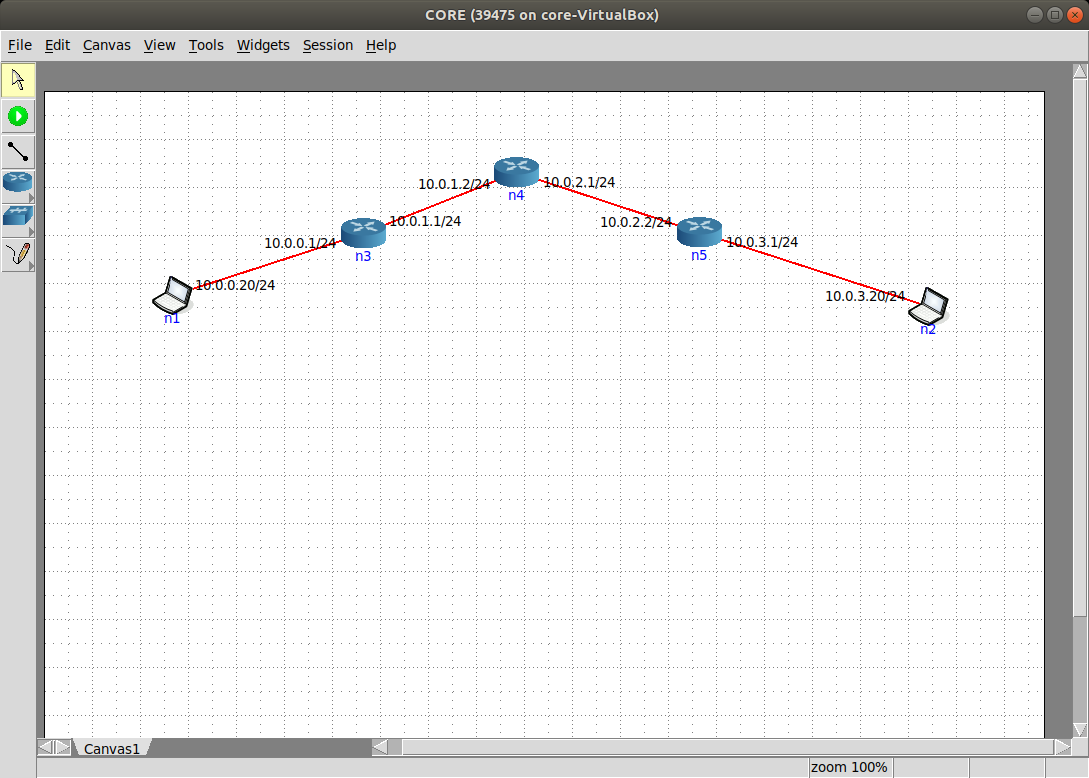


На хосте n3 запускаем tcpdump.

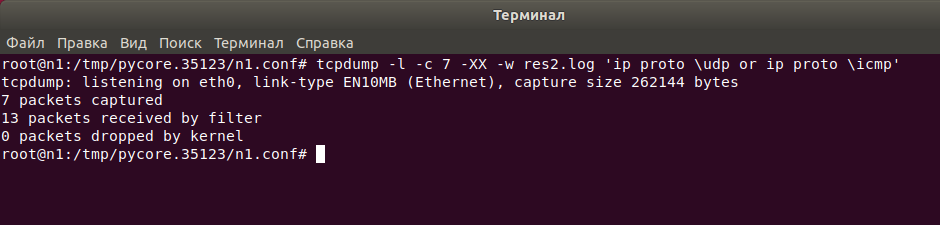


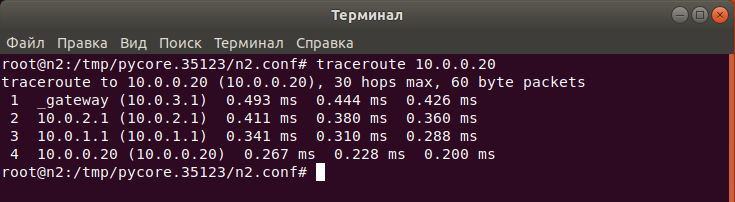
4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.

Схема:

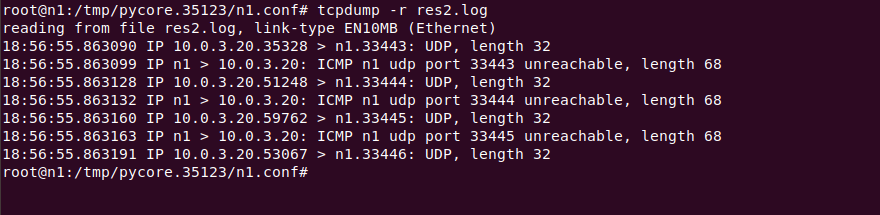


С хоста n2 с помощью утилиты traceroute передадим пакеты на n1. А на n1 запустим tcpdump с нужными параметрами.





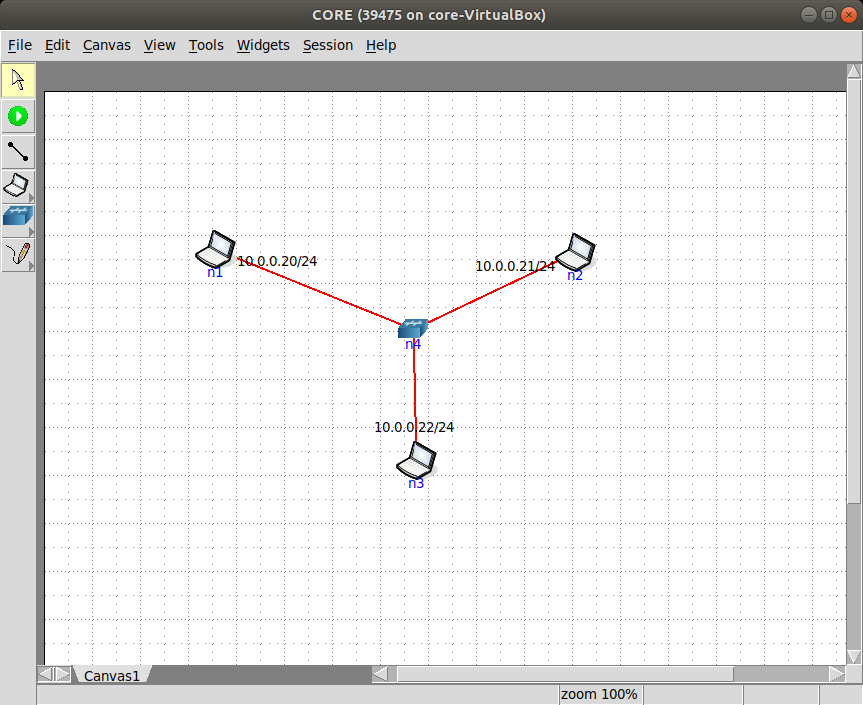
5. Прочесть программой tcpdump созданный в предыдущем пункте файл.

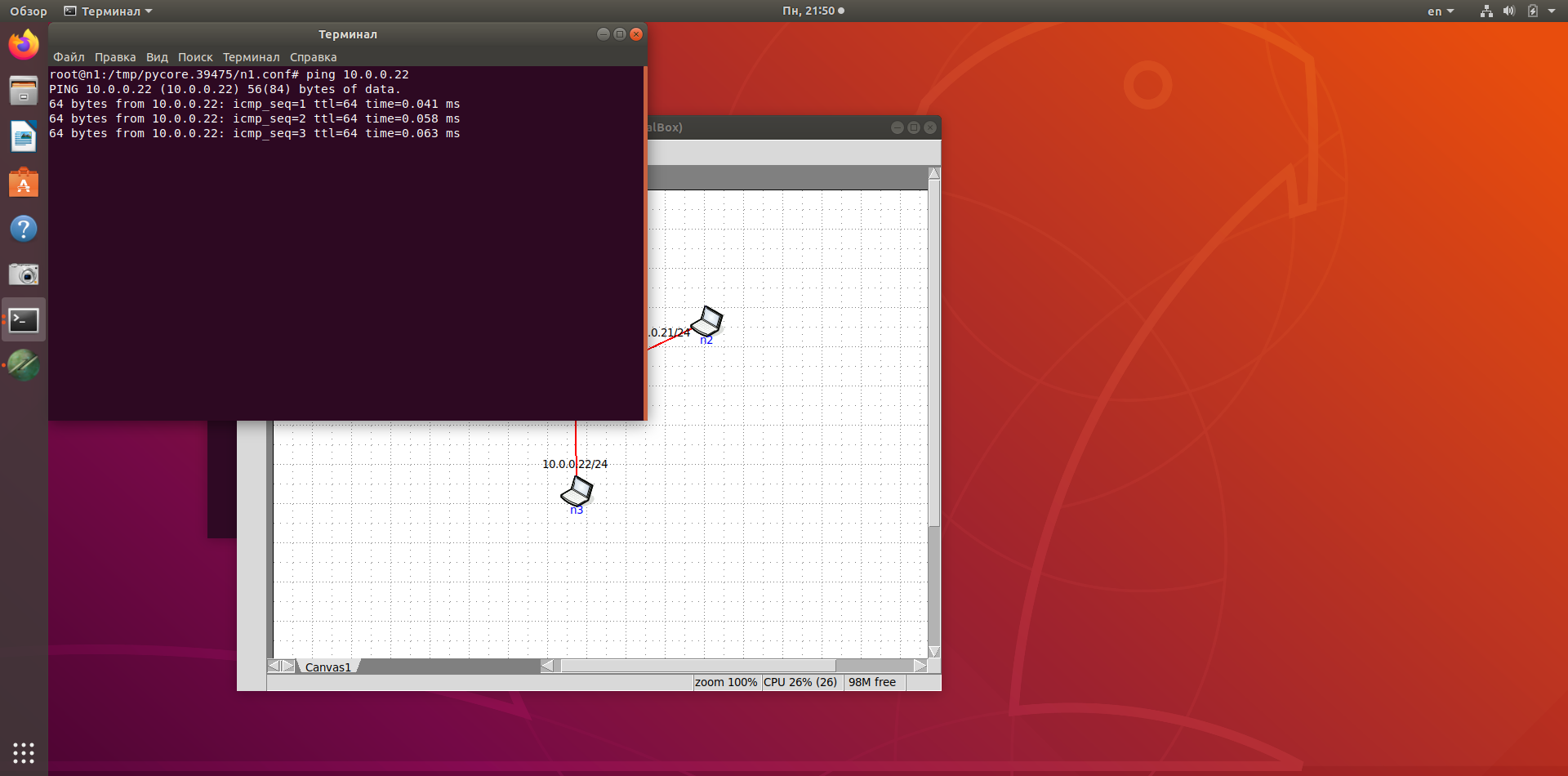


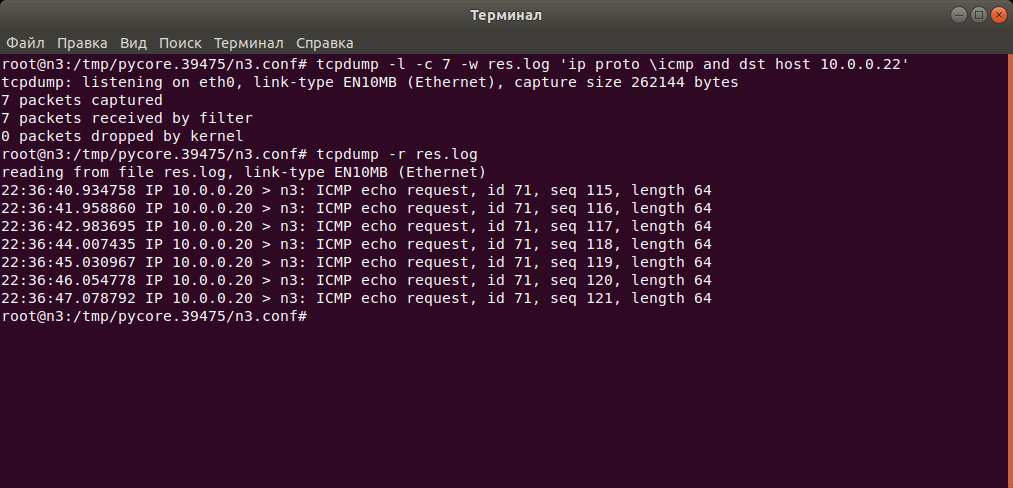
6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

1) Запустить tcpdump, перехватывающий пакеты протокола ICMP и адресом получателя 10.0.0.22. Сохранить данные в двоичном формате и ограничить количество пакетов до 7.

Схема:

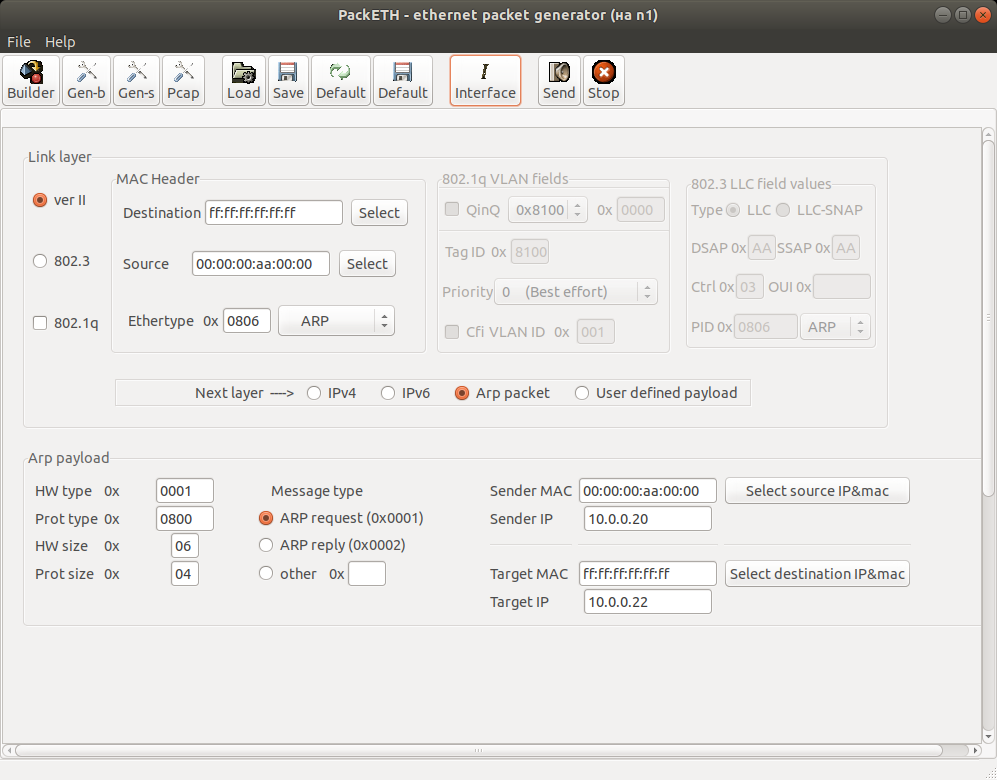


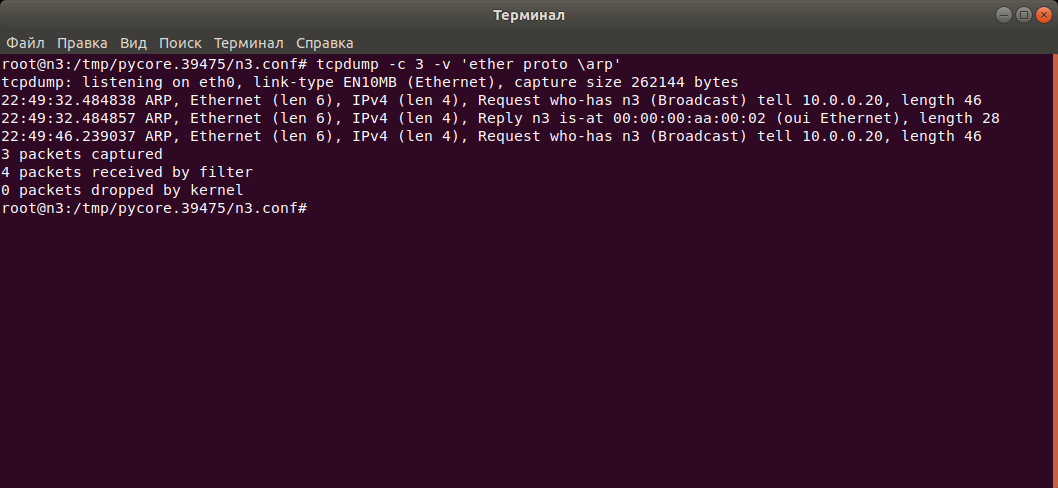




2) Запустить tcpdump для перехвата данных протокола ARP с выводом подробной информации. Количество пакетов ограничить до 3.

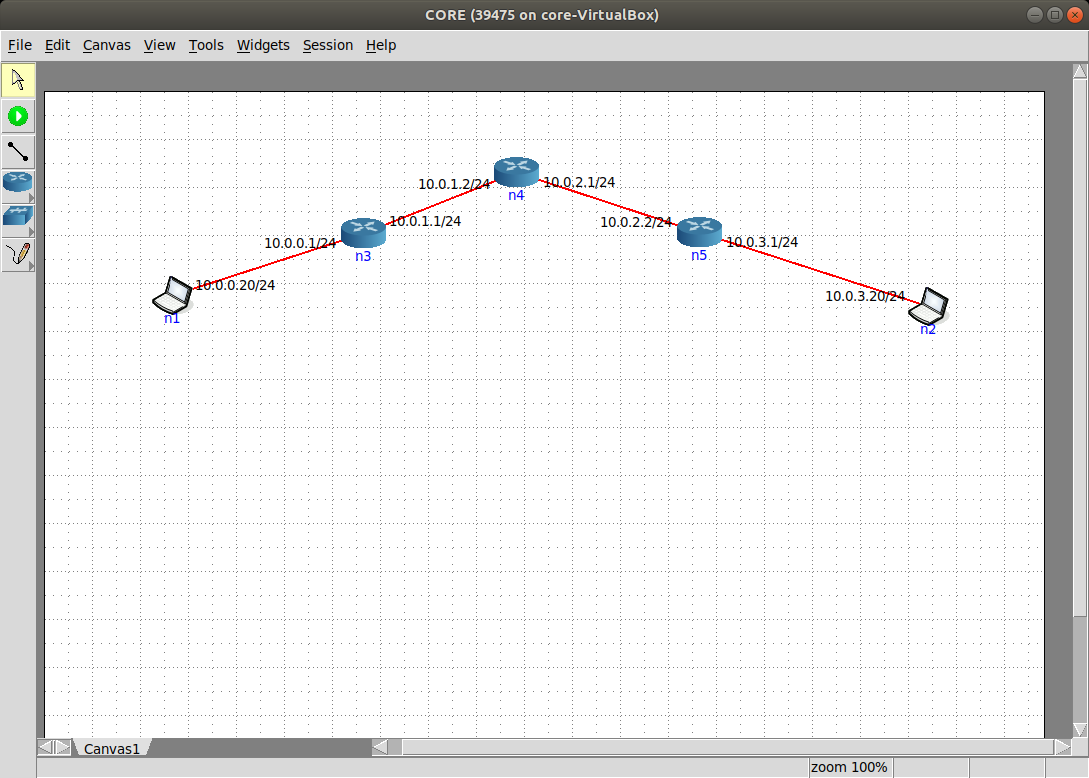
Формируем широковещательный ARP запрос на хосте n1.

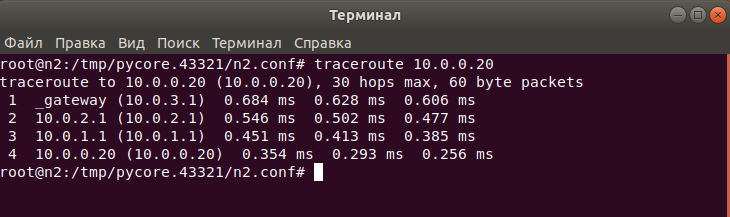


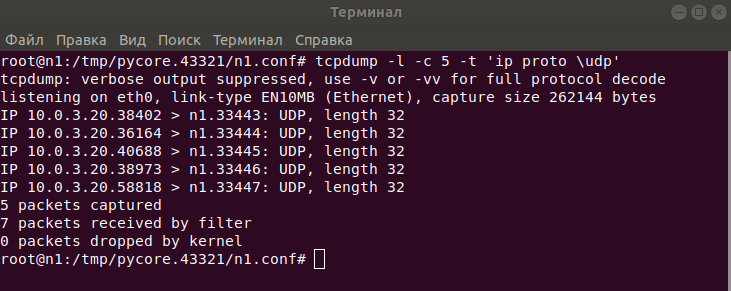


3) Запустить tcpdump, перехватывающий пакеты протокола UDP. Не отображать метку времени в каждой строке. Количество захватываемых пакетов ограничить до 5.

Схема:



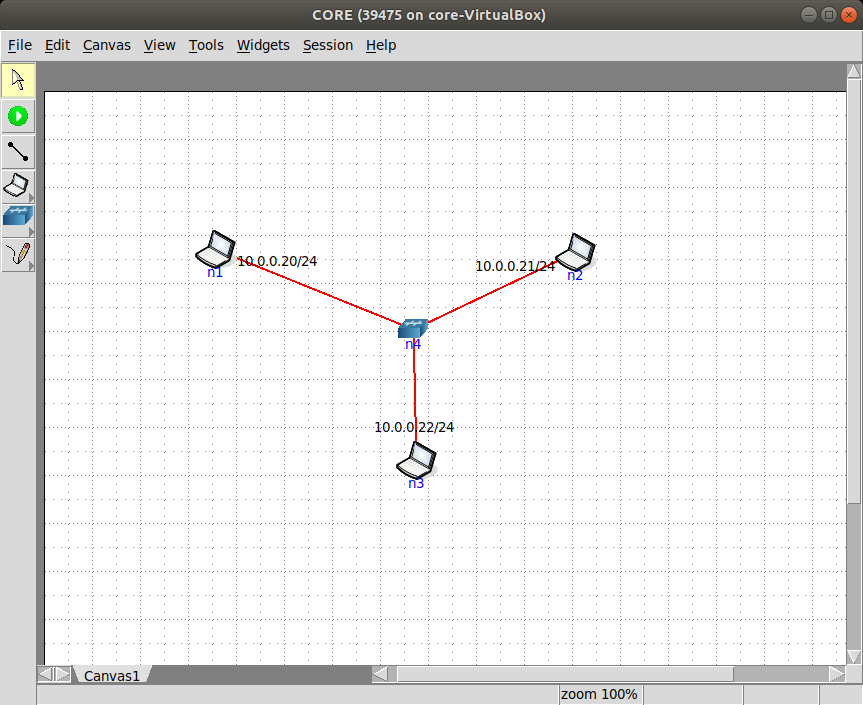


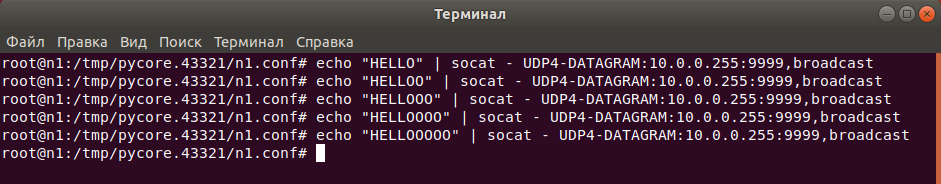


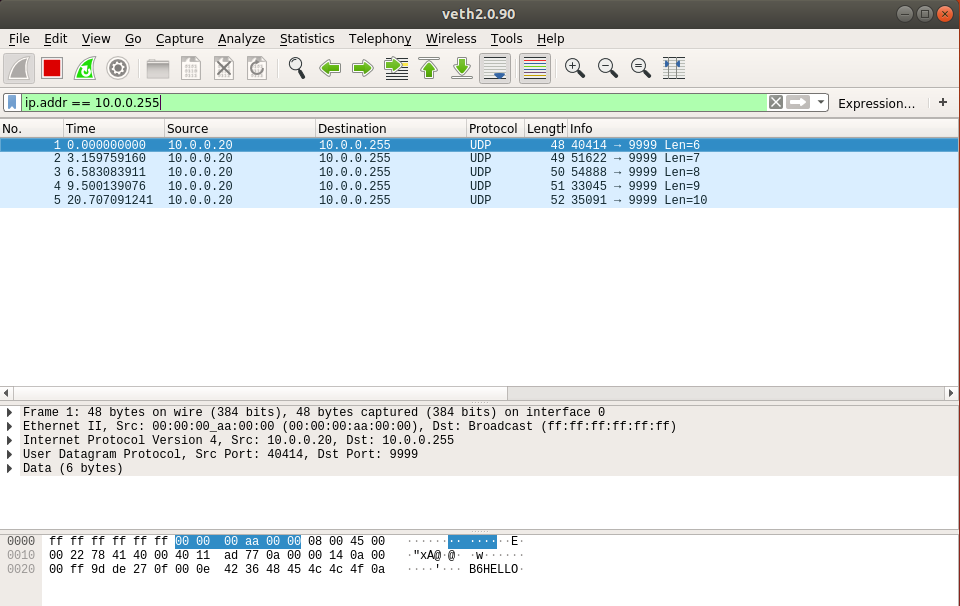
**Работа с анализатором протоколов wireshark**

1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

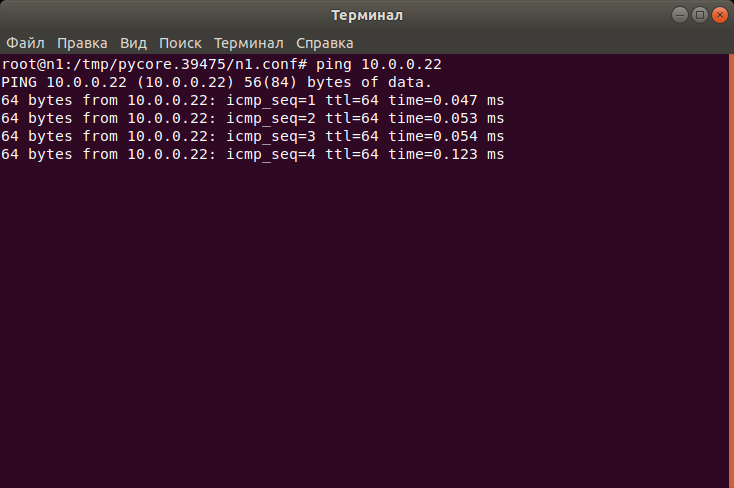
Схема:

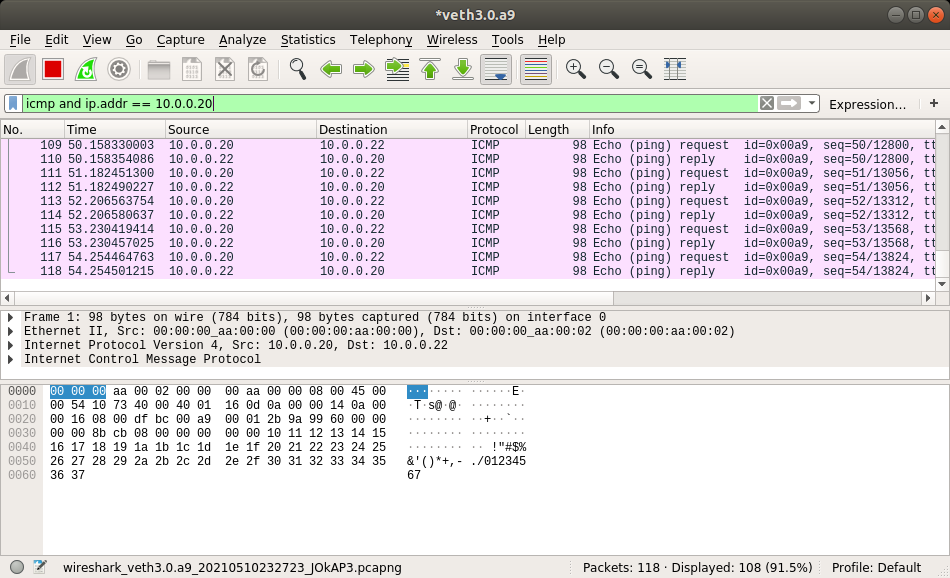




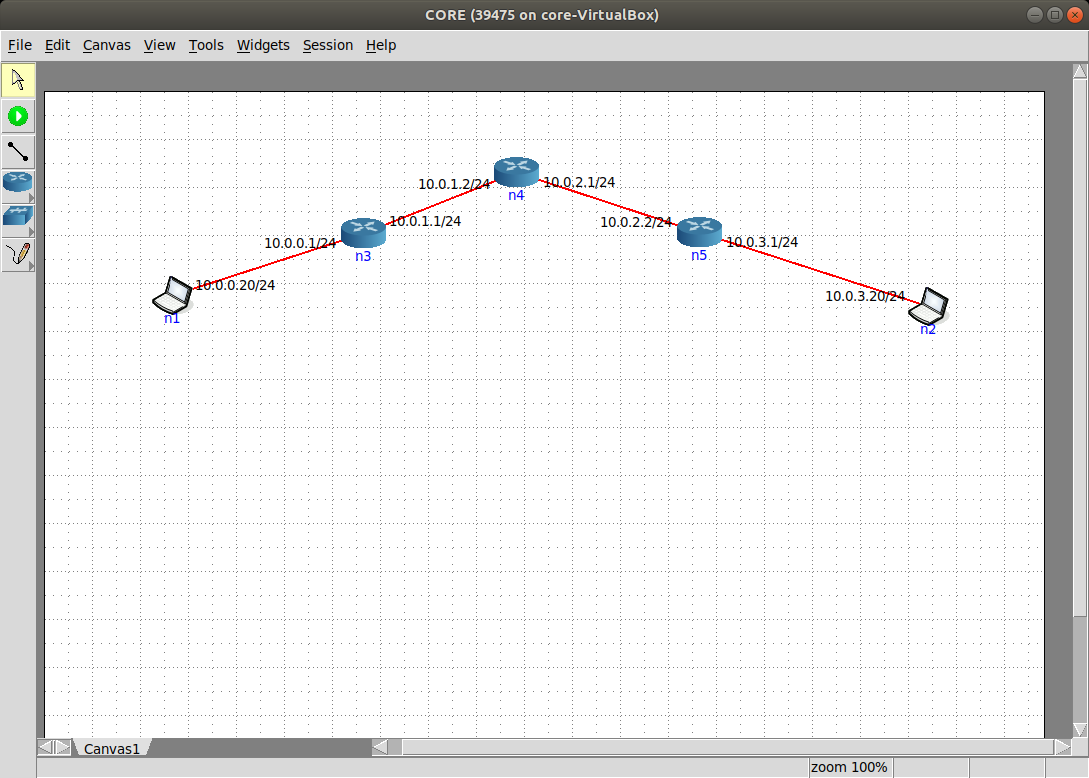


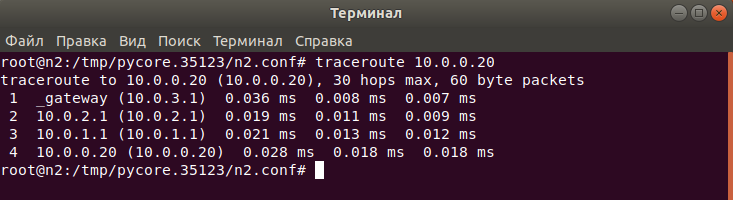
2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

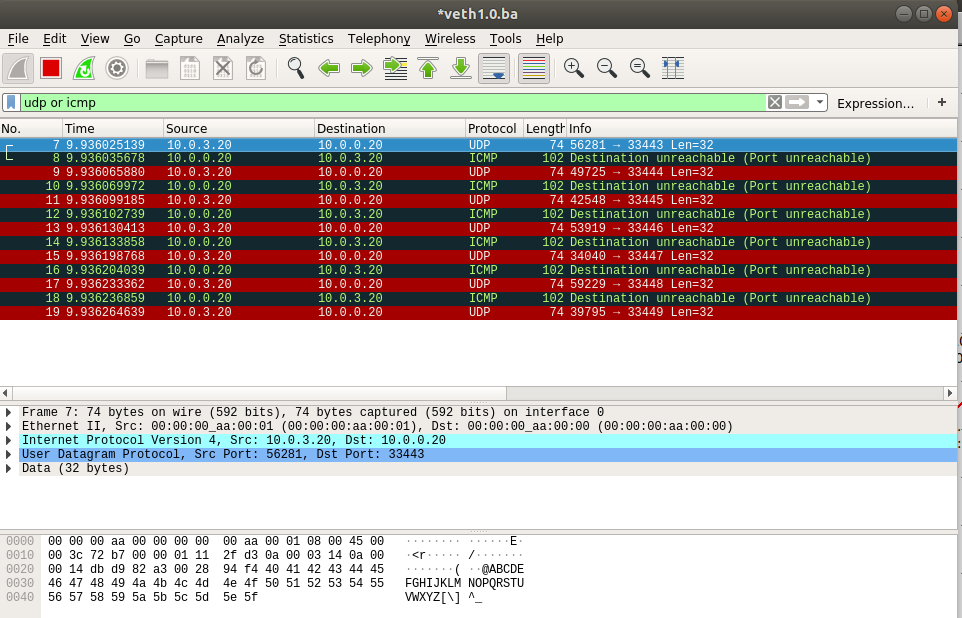


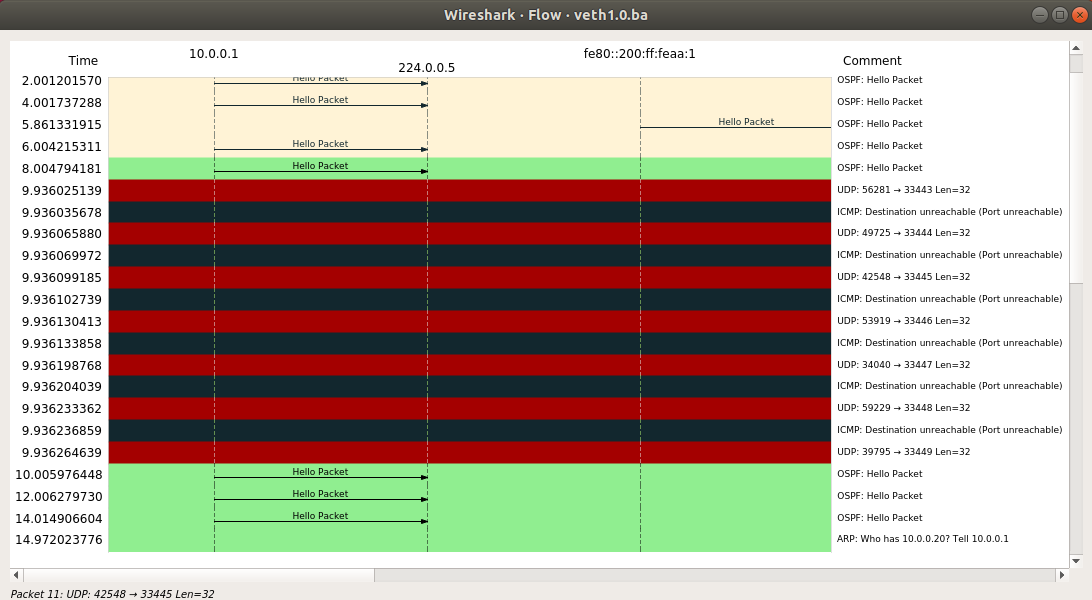


3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла, либо в виде изображения.









4. Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.

