Минобрнауки России

Федеральное государственное бюджетное образовательное

учреждение высшего образования

**НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**ИМ. Р.Е. АЛЕКСЕЕВА**

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Курс “Сети и телекоммуникации”

**Отчет по лабораторной работе №5**

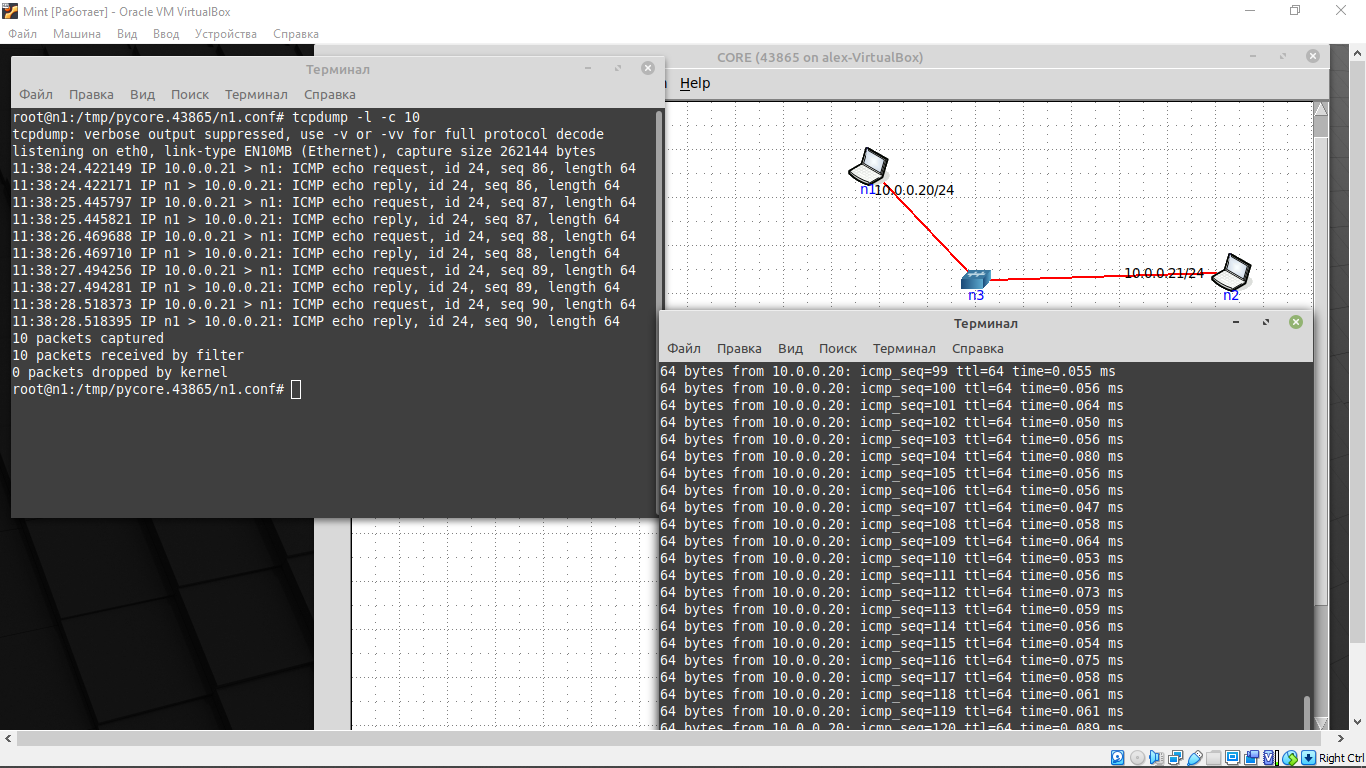
Выполнил: студент группы 19АС Груздев А.Д.

Проверил: Гай В.Е.

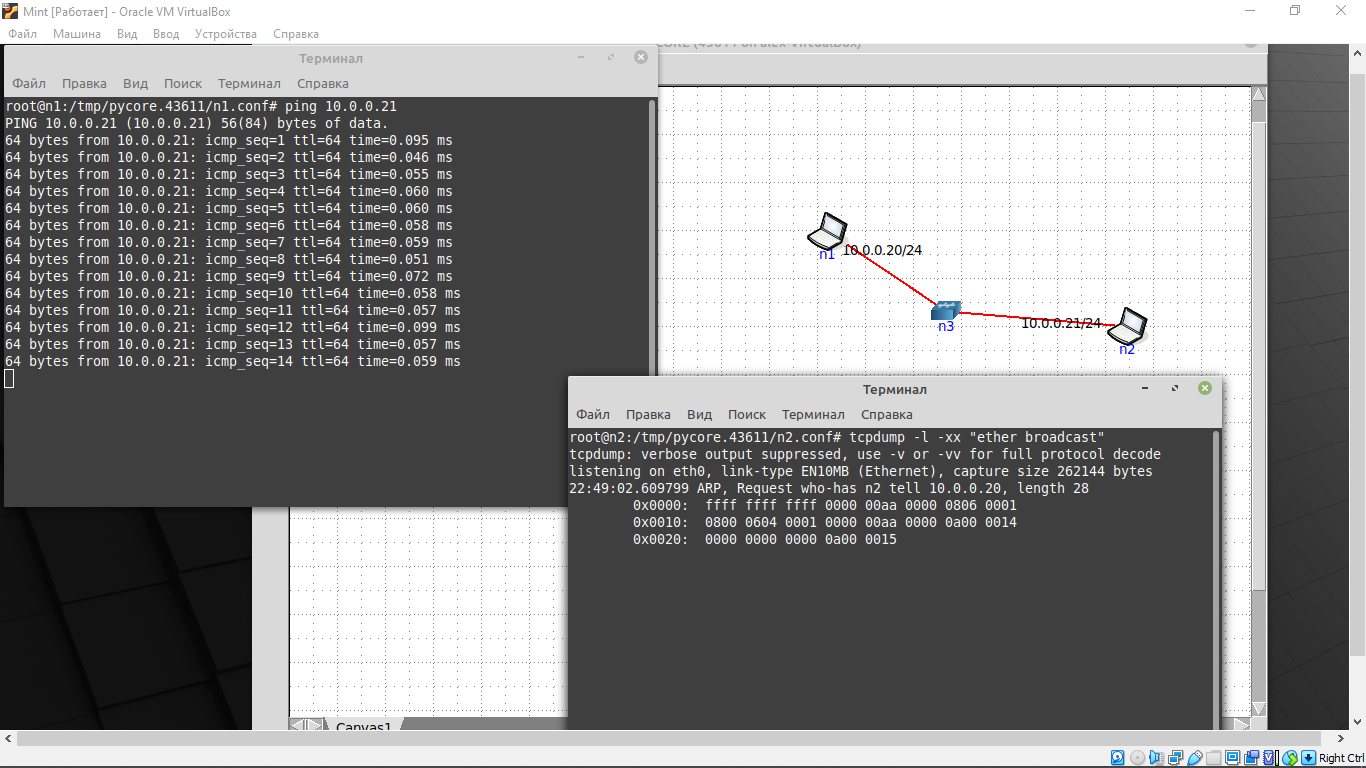
Нижний Новгород 2022

**Работа с анализатором протоколов tcpdump**

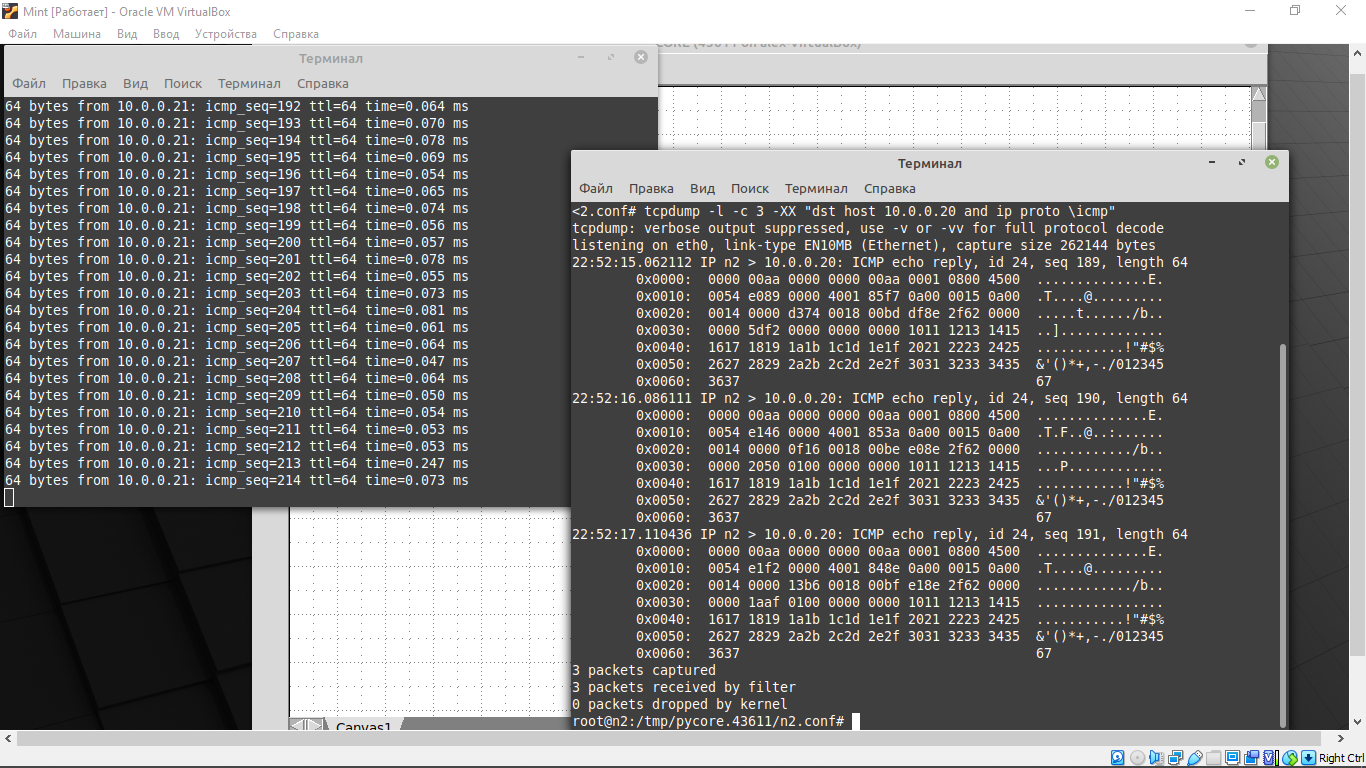
1) Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.



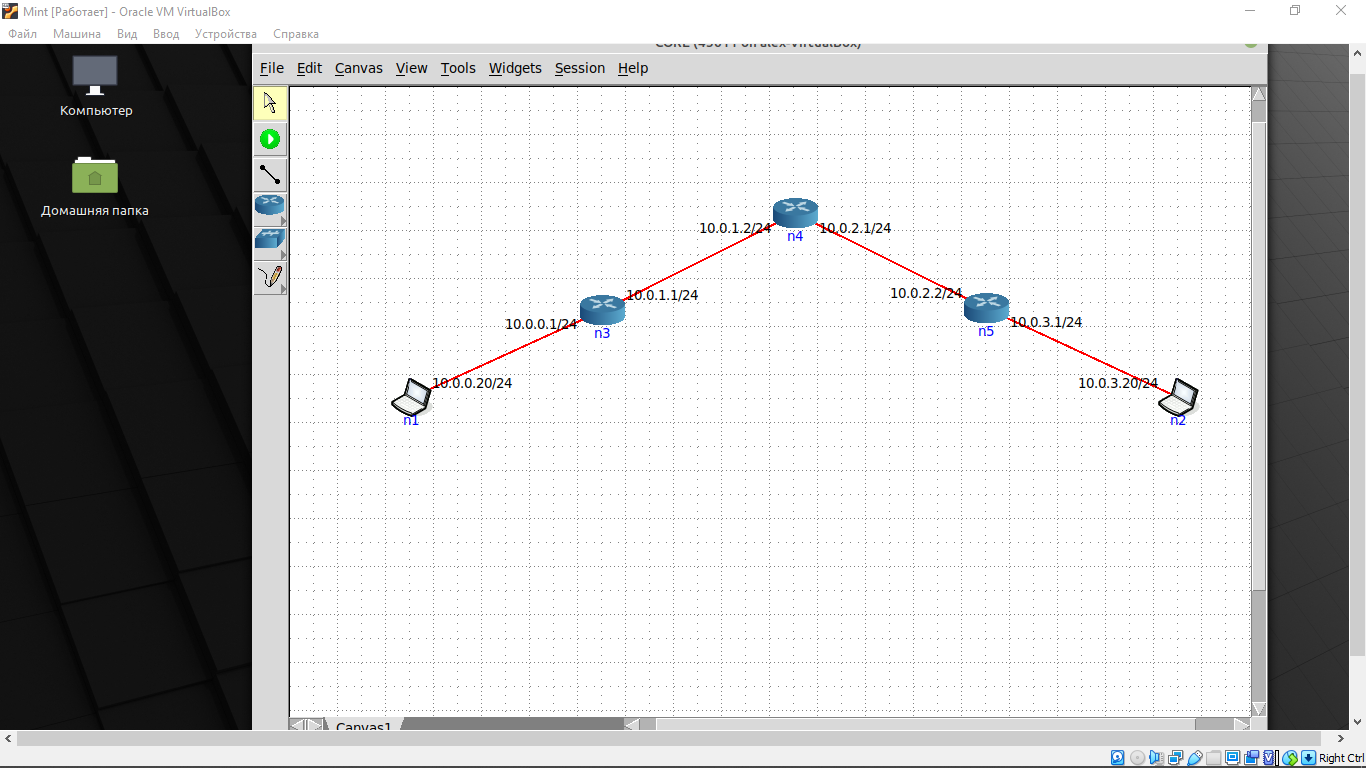
2) Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

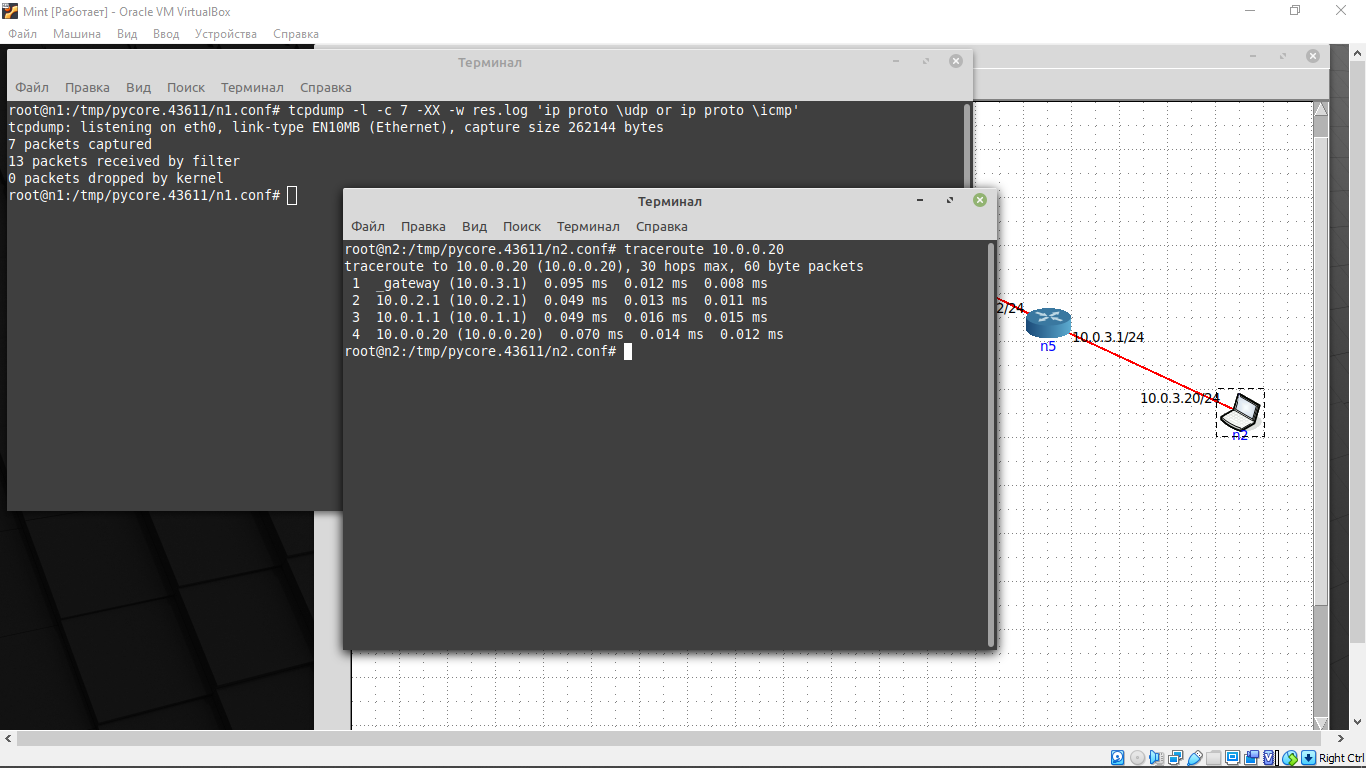


3) Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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

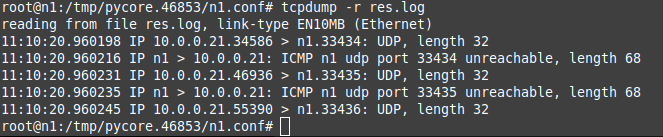


4) Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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



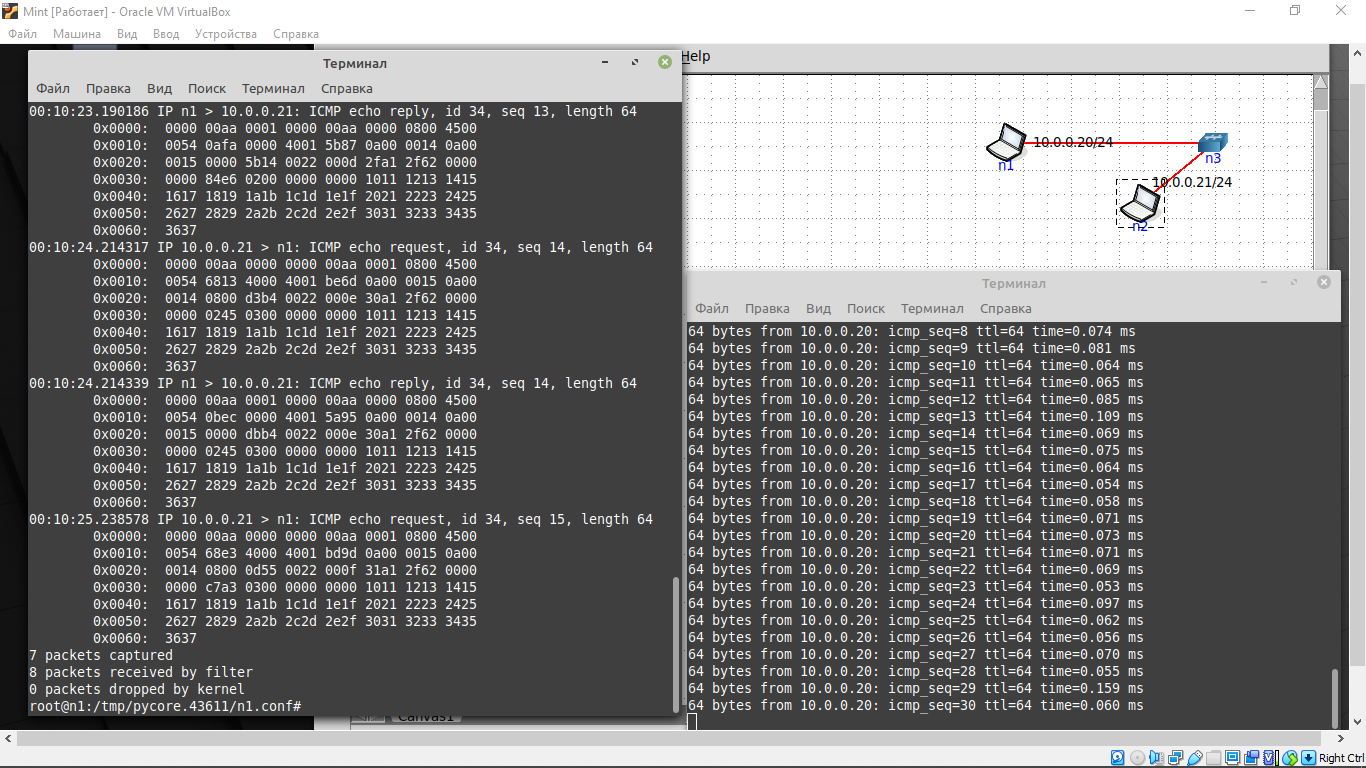


5) Прочесть программой tcpdump созданный в предыдущем пункте файл.

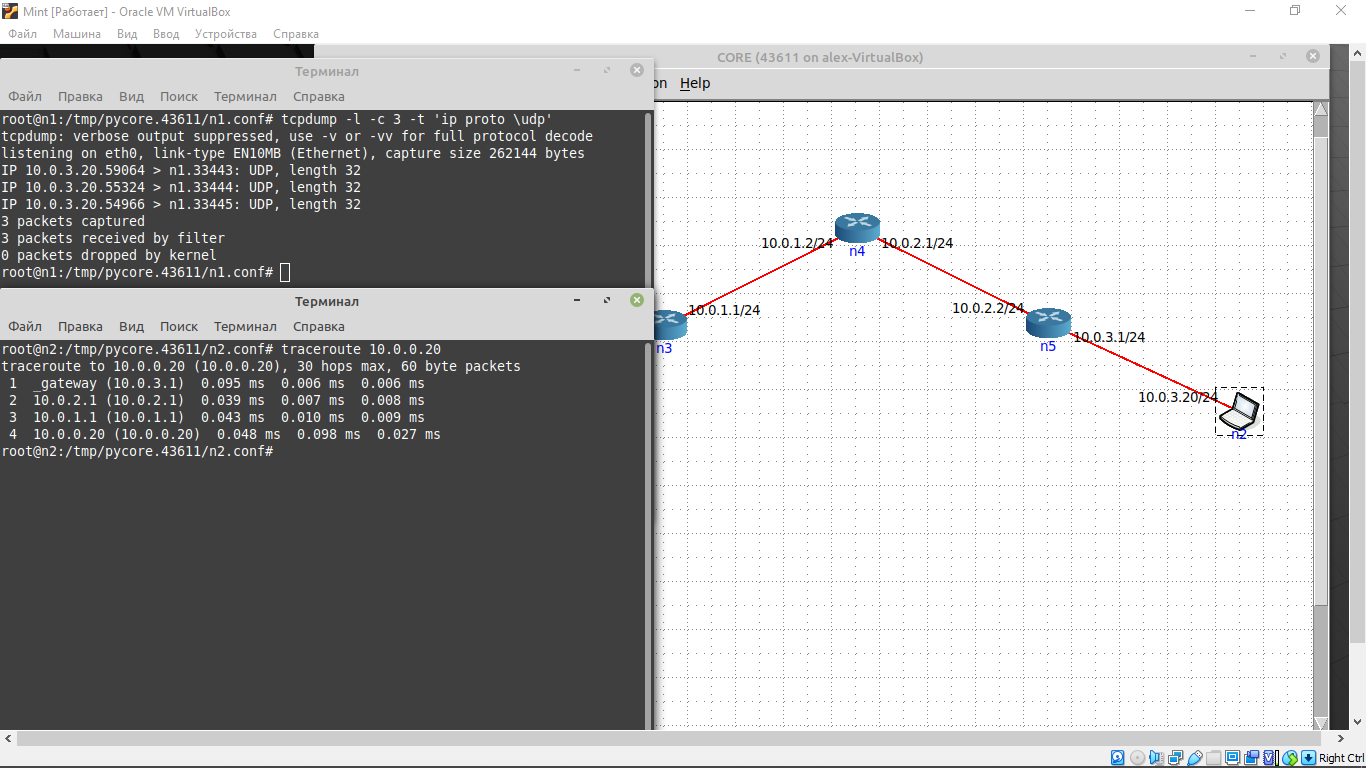


6) Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

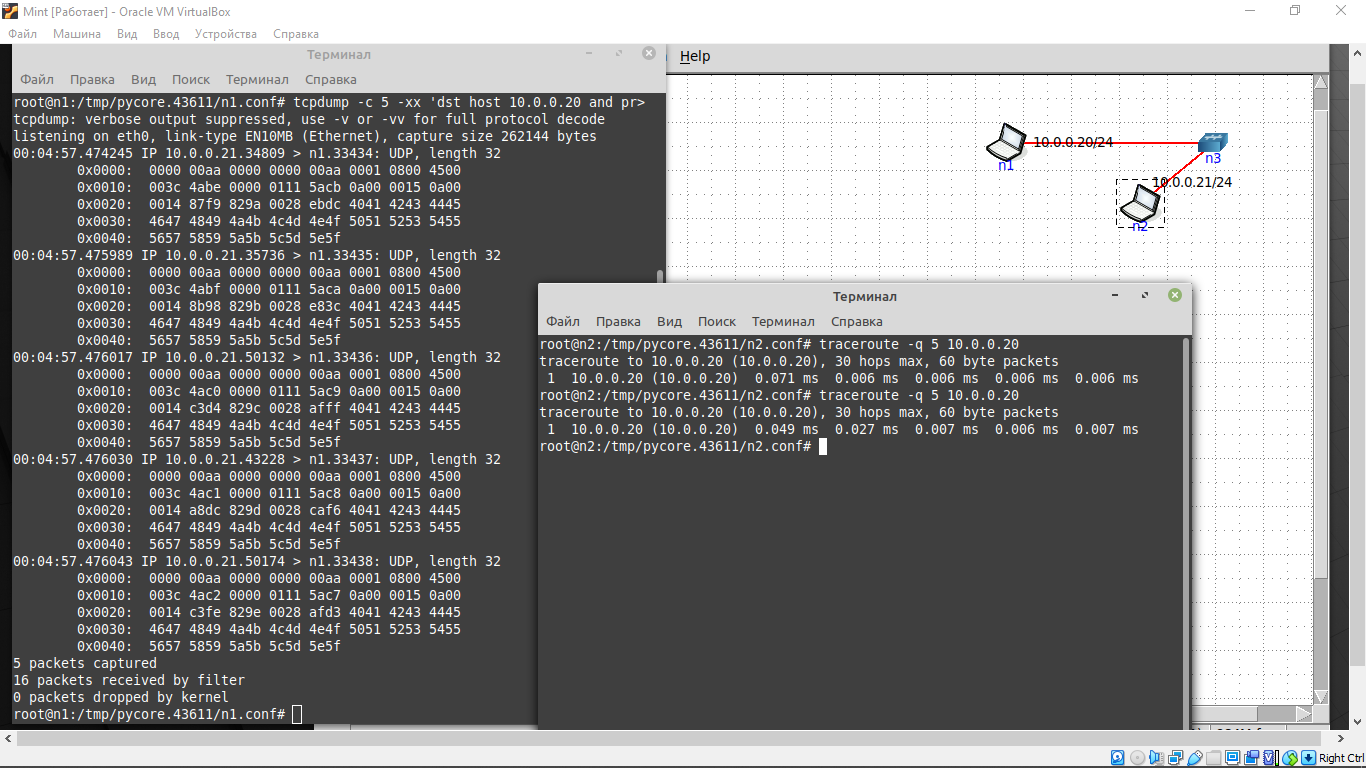
1) Запустить tcpdump для перехвата данных протокола ICMP. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7.



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

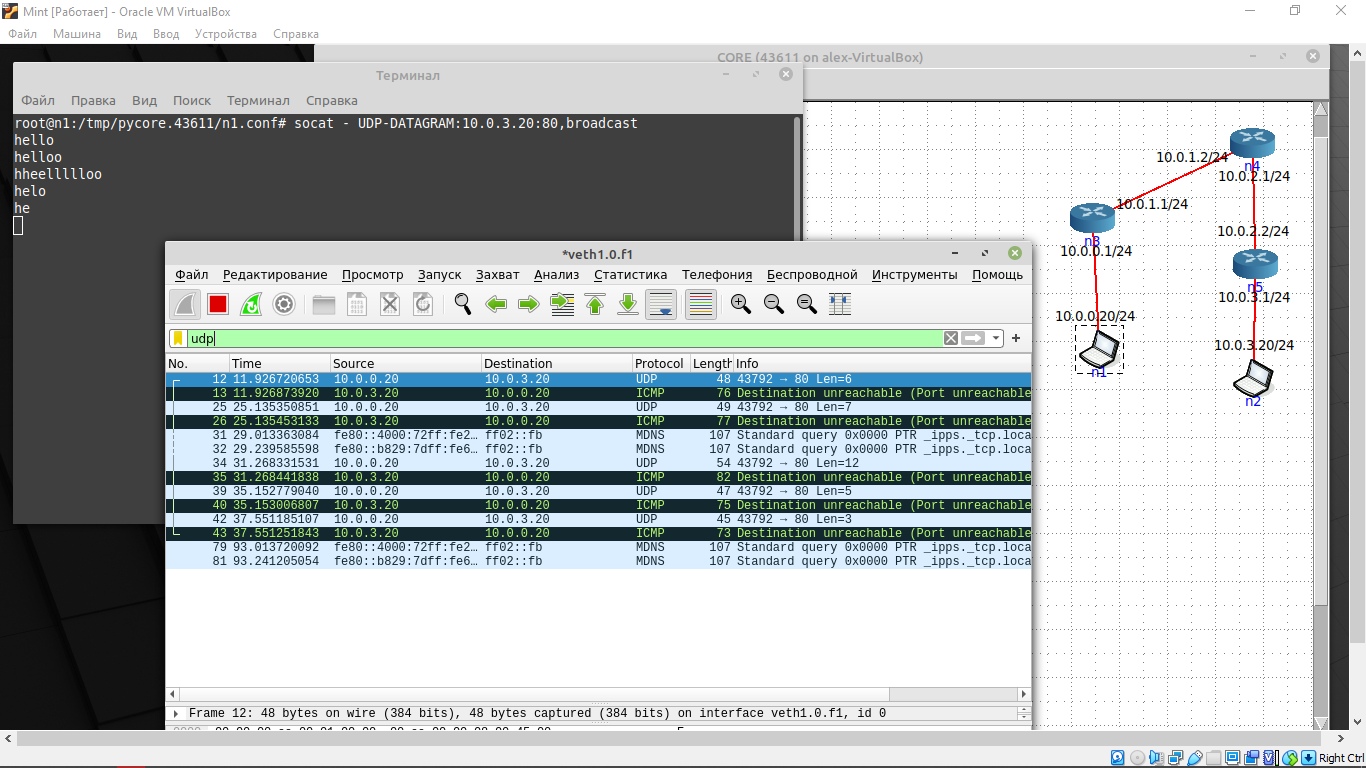


3) Запустить tcpdump так, чтобы он перехватывал только пакеты протокола UDP, созданные утилитой traceroute. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 5.

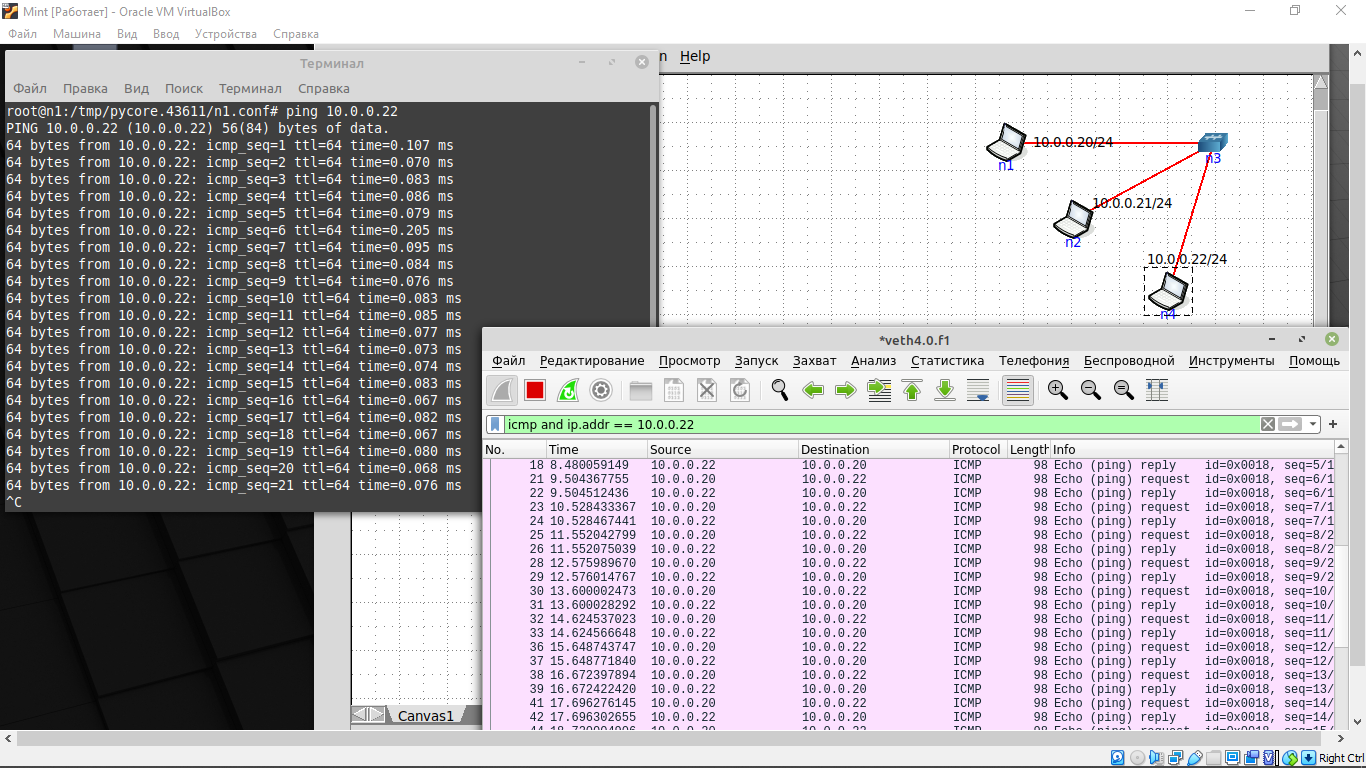


**Работа с анализатором протоколов wireshark**

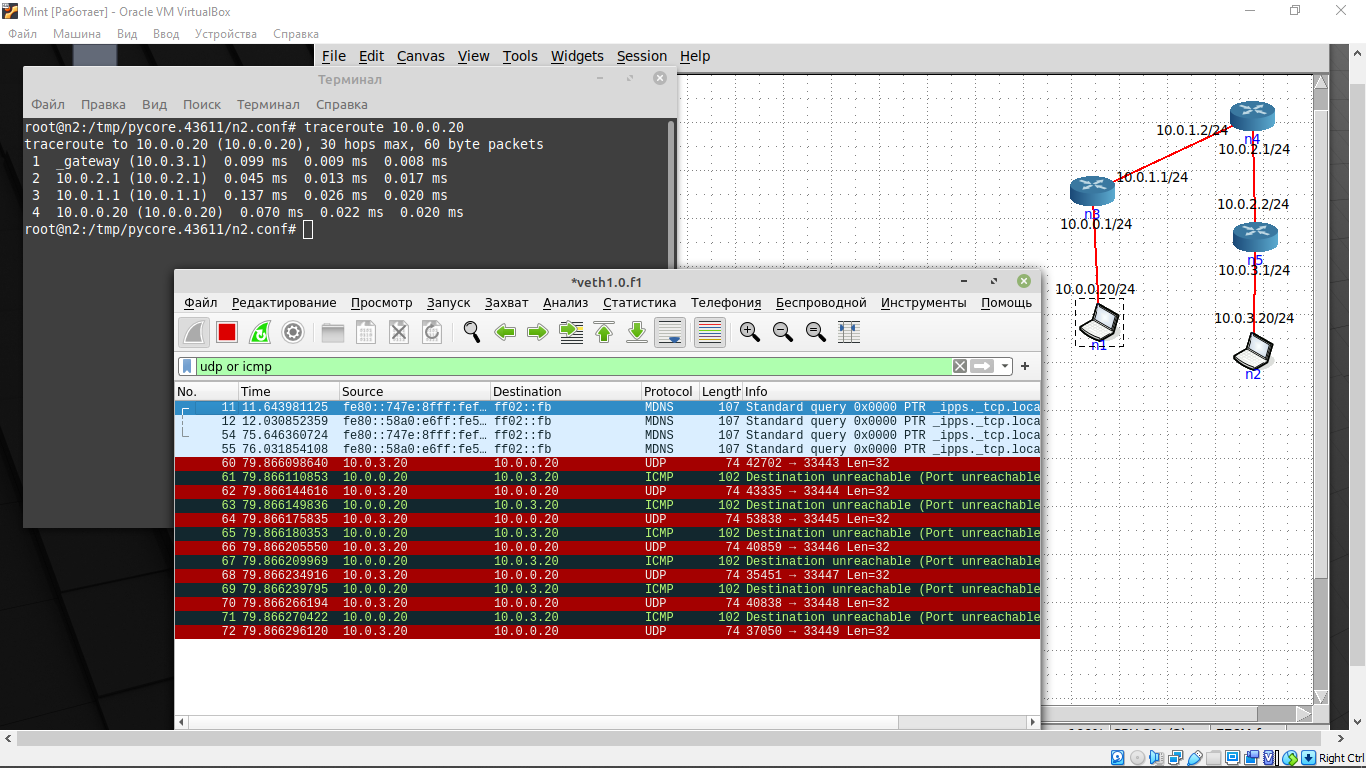
1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

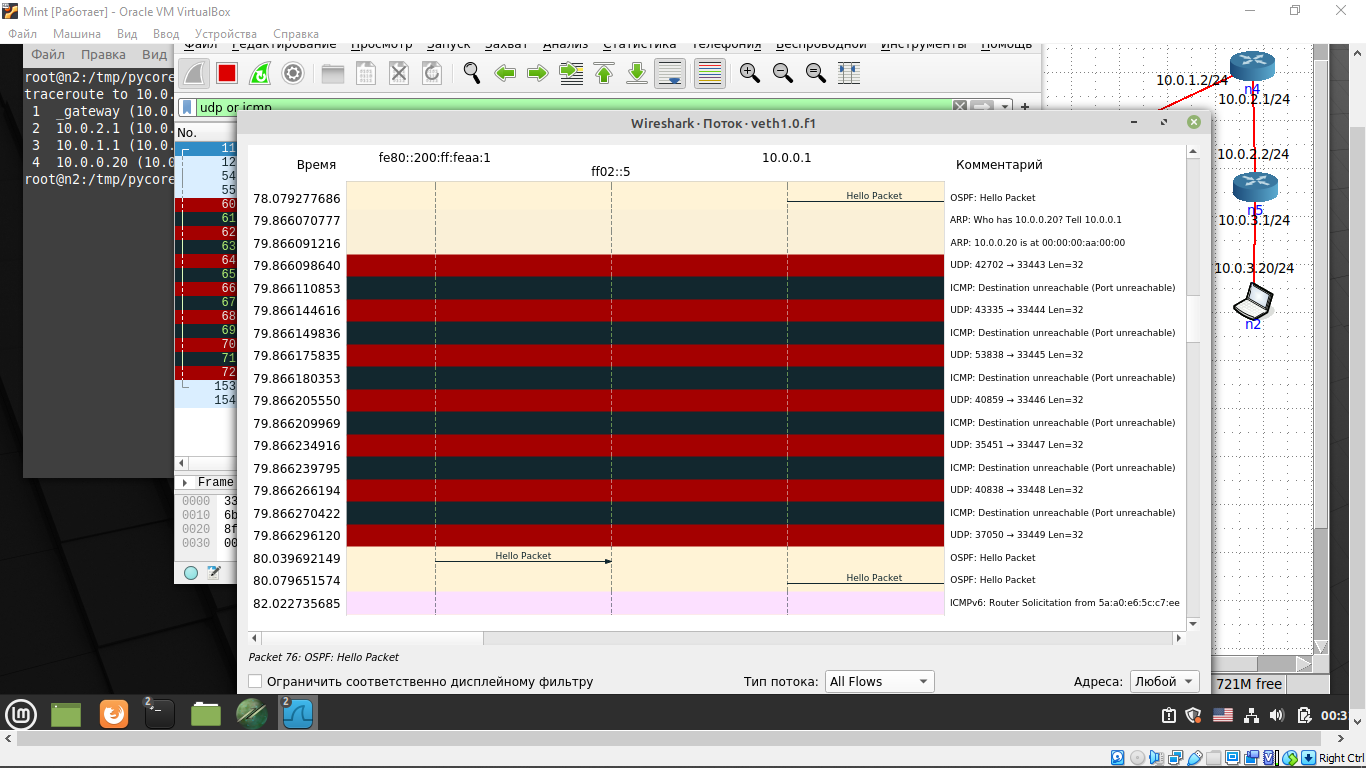


2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.



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.

