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 №1**

Выполнил:

Студент

группы 18-АС

Кремлев Антон

Проверил:

Гай В.Е.

Отчет защищен с оценкой: \_\_\_\_\_\_\_\_\_\_\_\_

Дата защиты «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_ г.

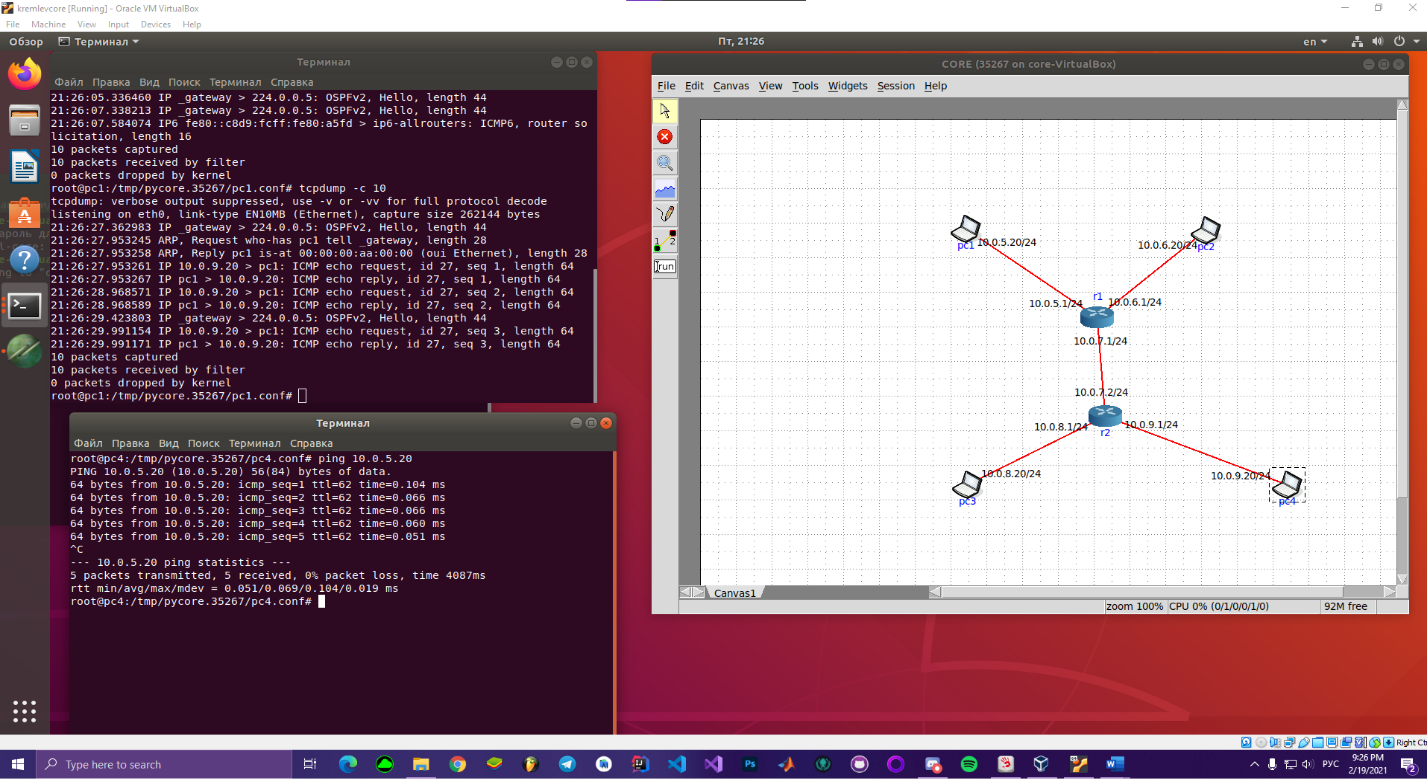
Нижний Новгород

2020 год

**Задания:**

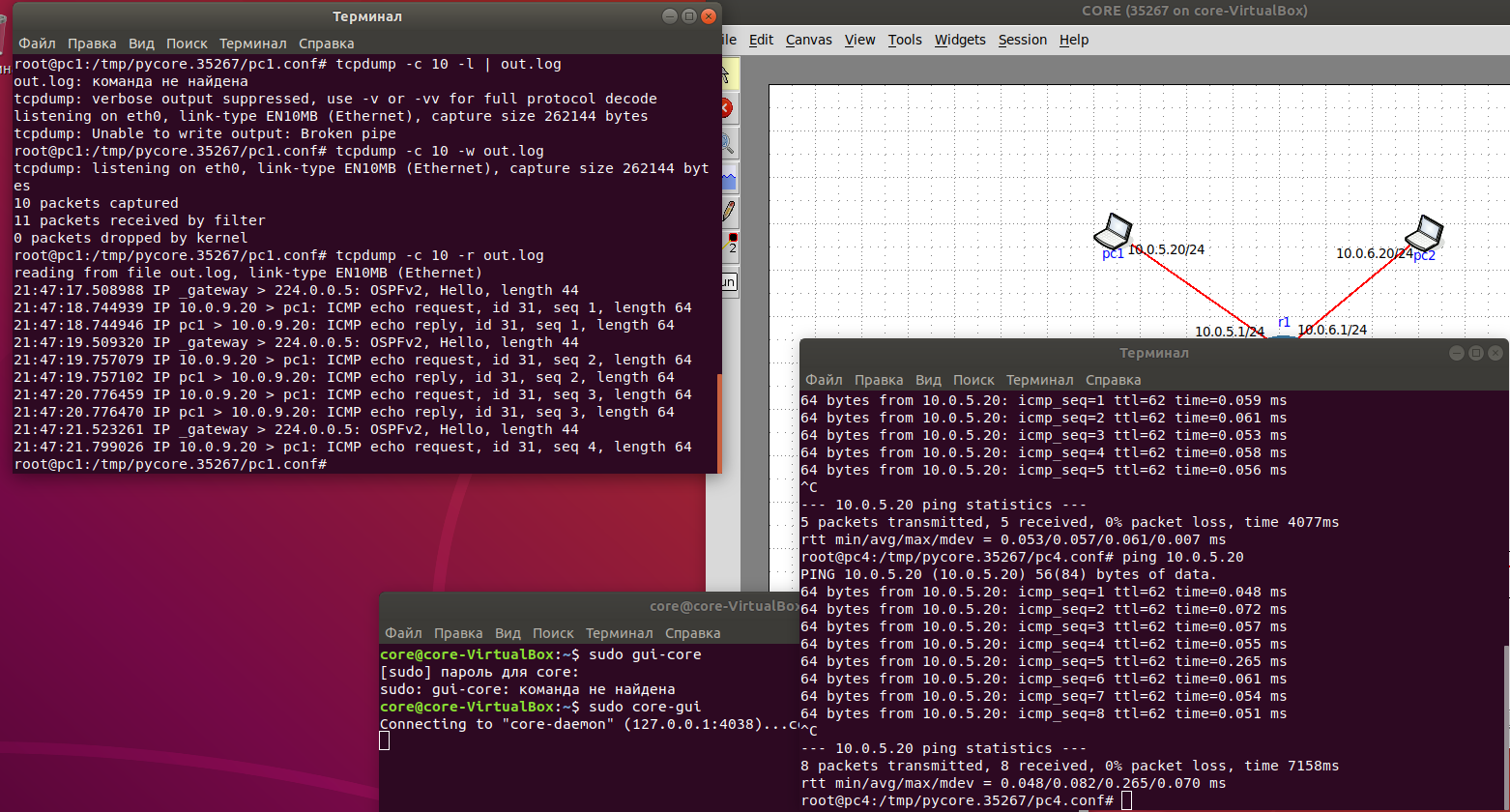
**Работа с анализатором протоколов tcpdump**

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

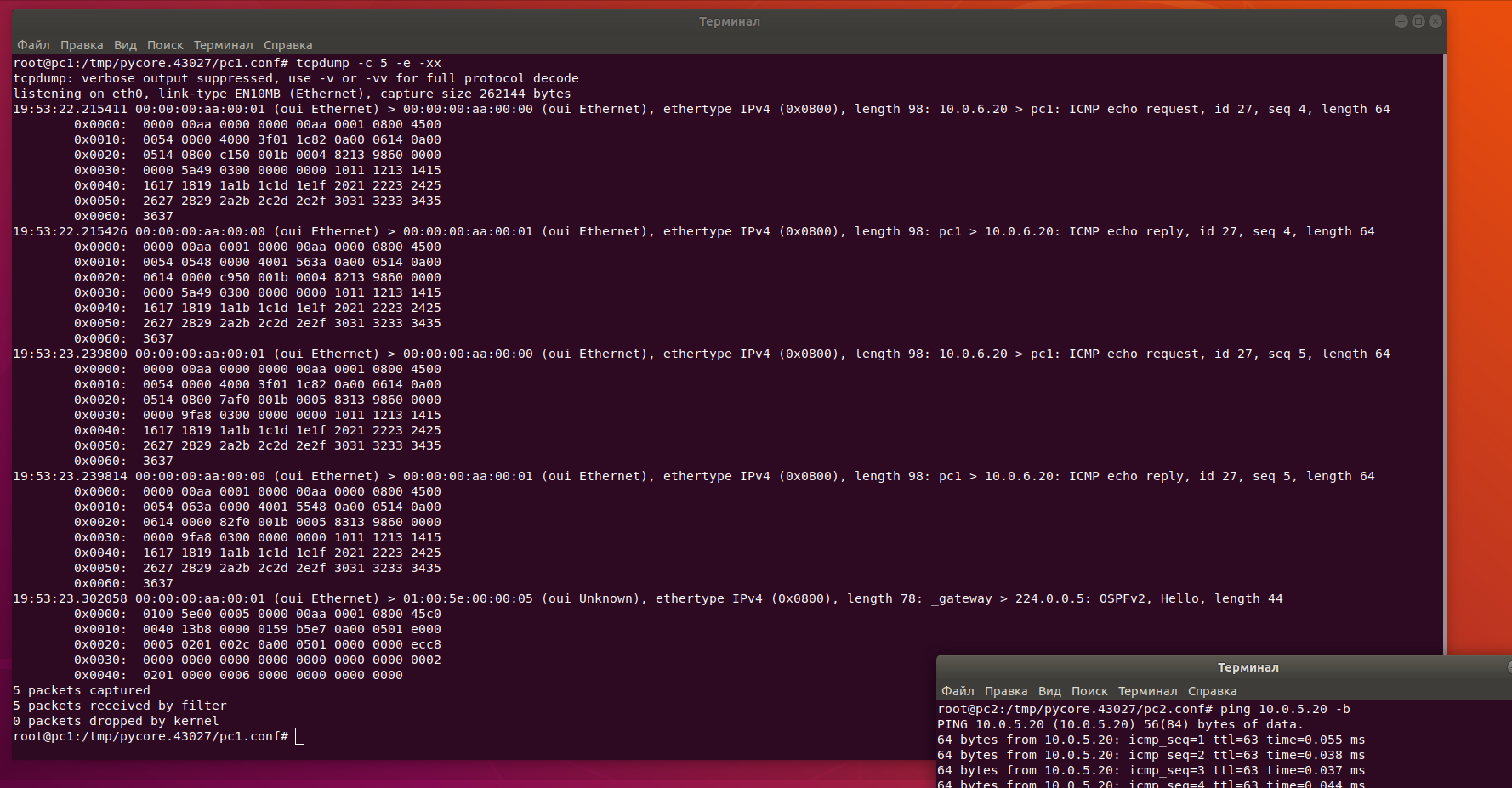


Логируем через ключ -w name

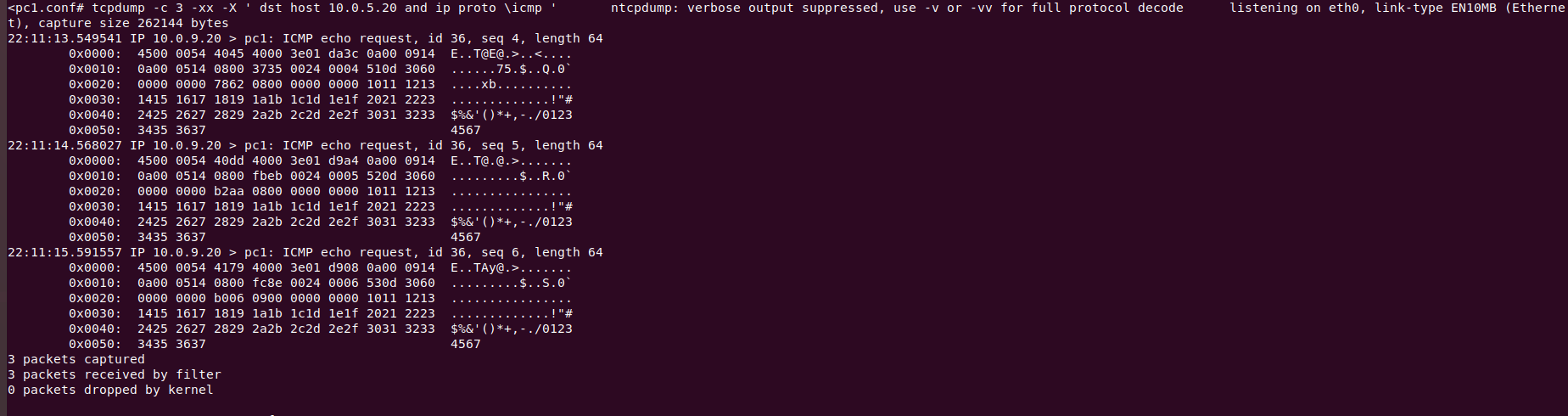
Производим чтение через -r name



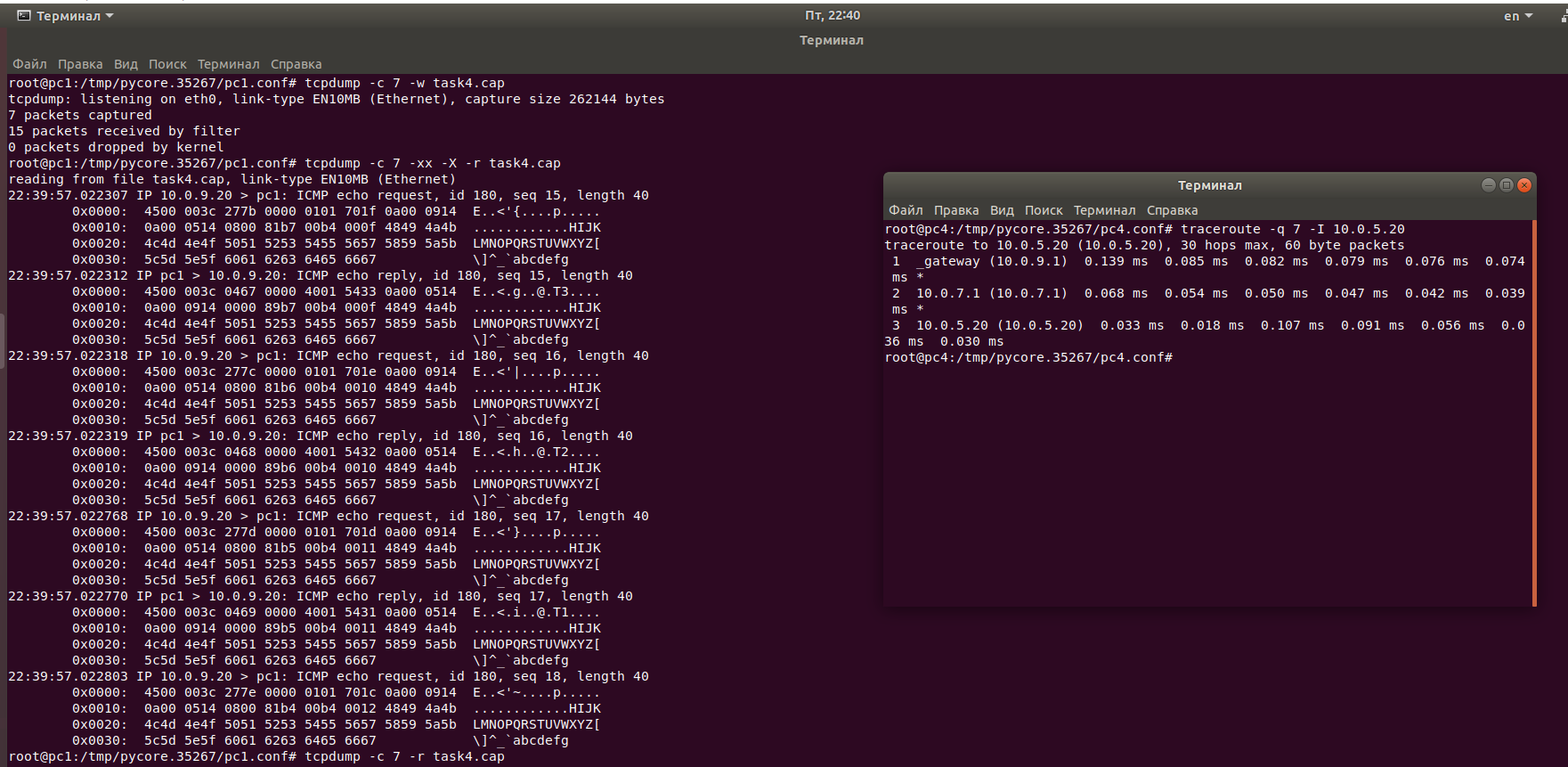
1. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).



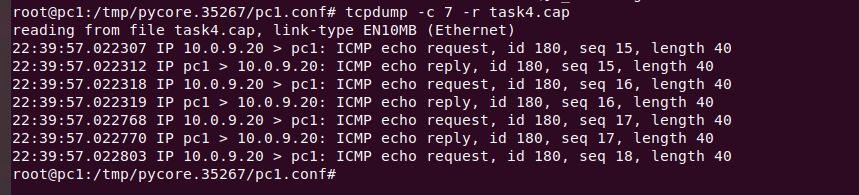
1. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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



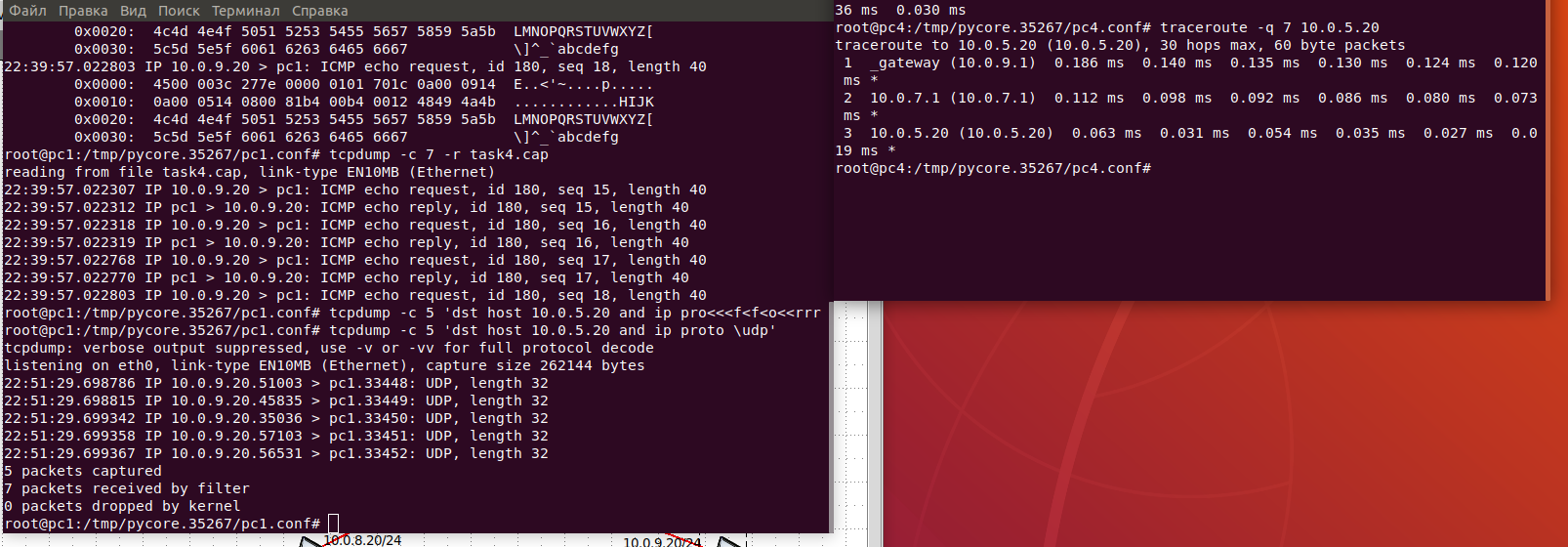
1. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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



1. Прочесть программой tcpdump созданный в предыдущем пункте файл.

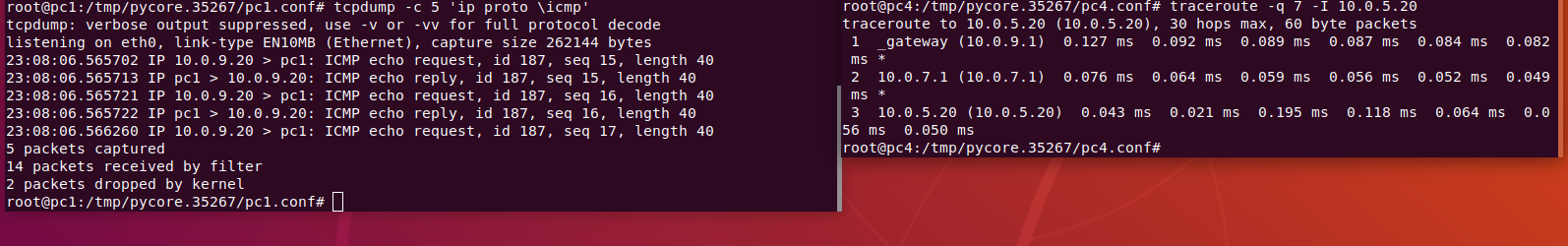


1. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP



Отправляем пакеты через ТСП, и ставим фильтр на прием UDP – ничего не поймал, все правильно

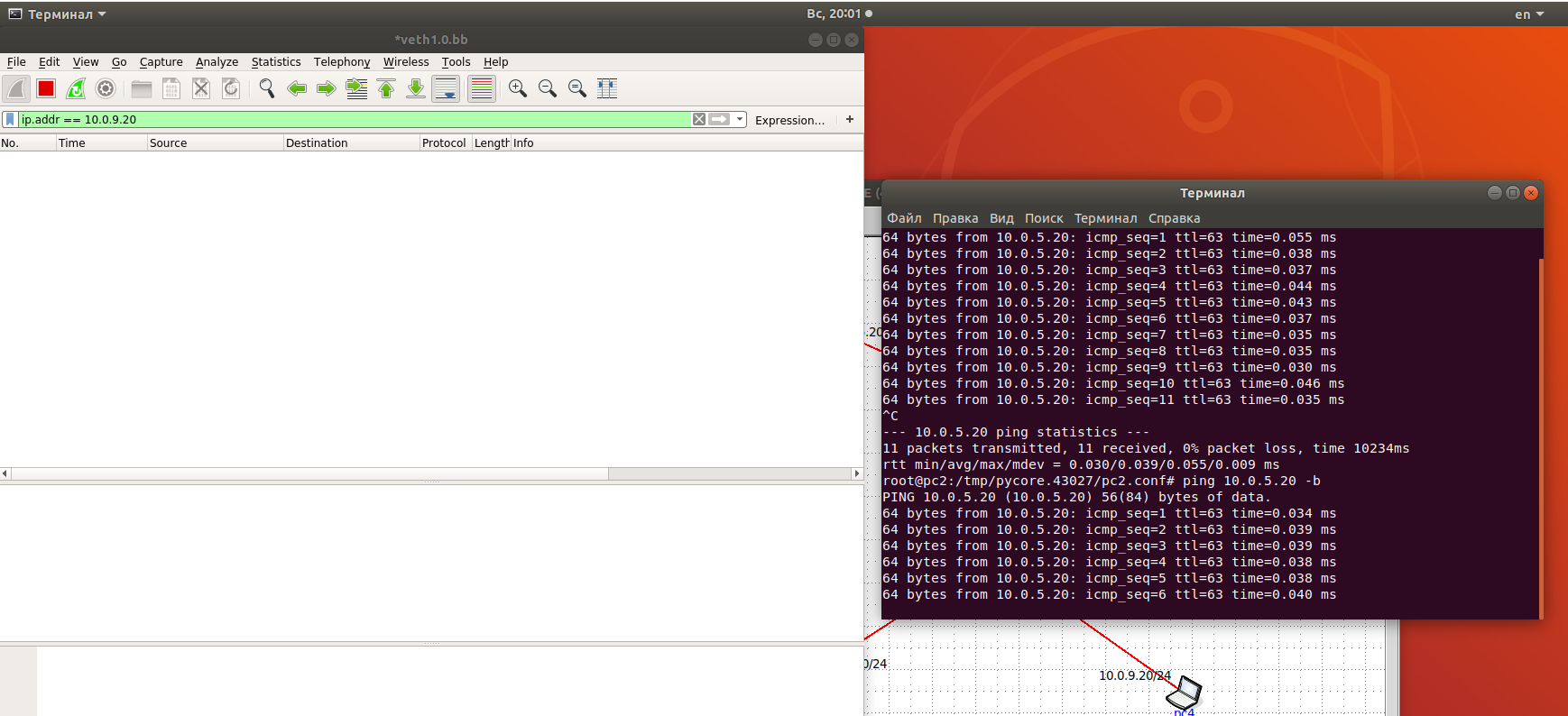




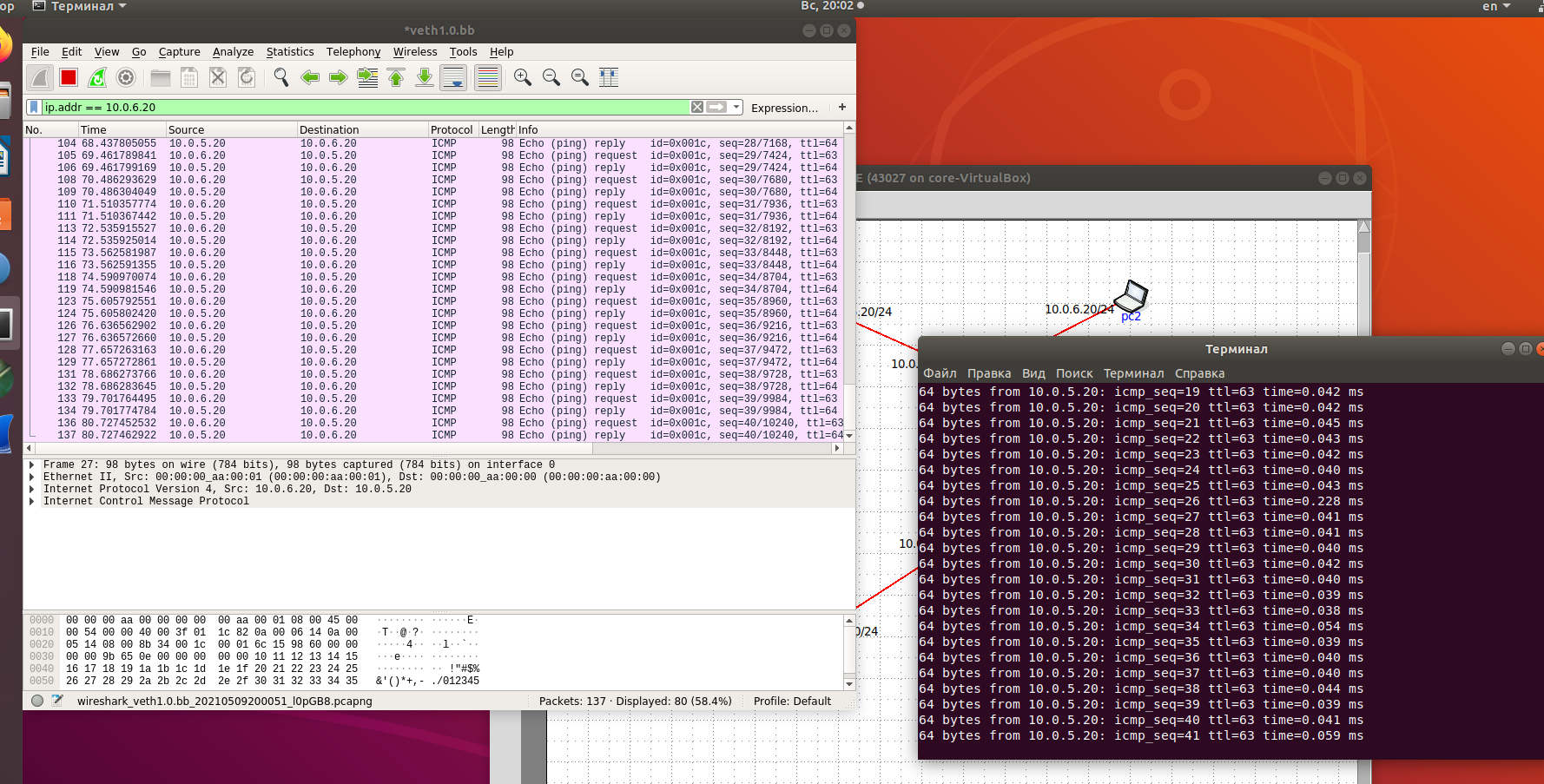
**Работа с анализатором протоколов wireshark**

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

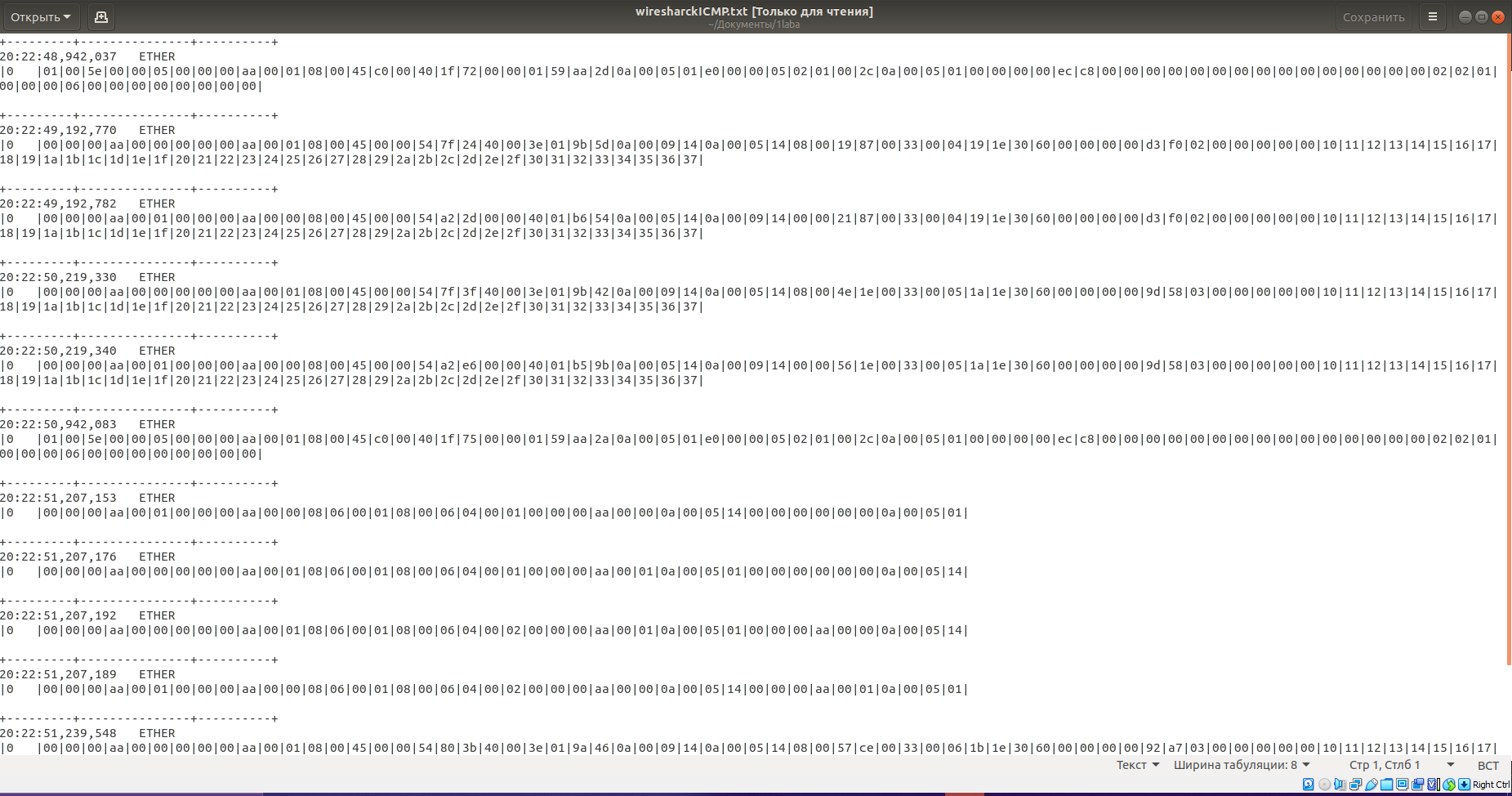
Пробуем пинговать второй пк ( wireshark на первом и фильтр на первый ) -> пакеты не отображаются -> верно



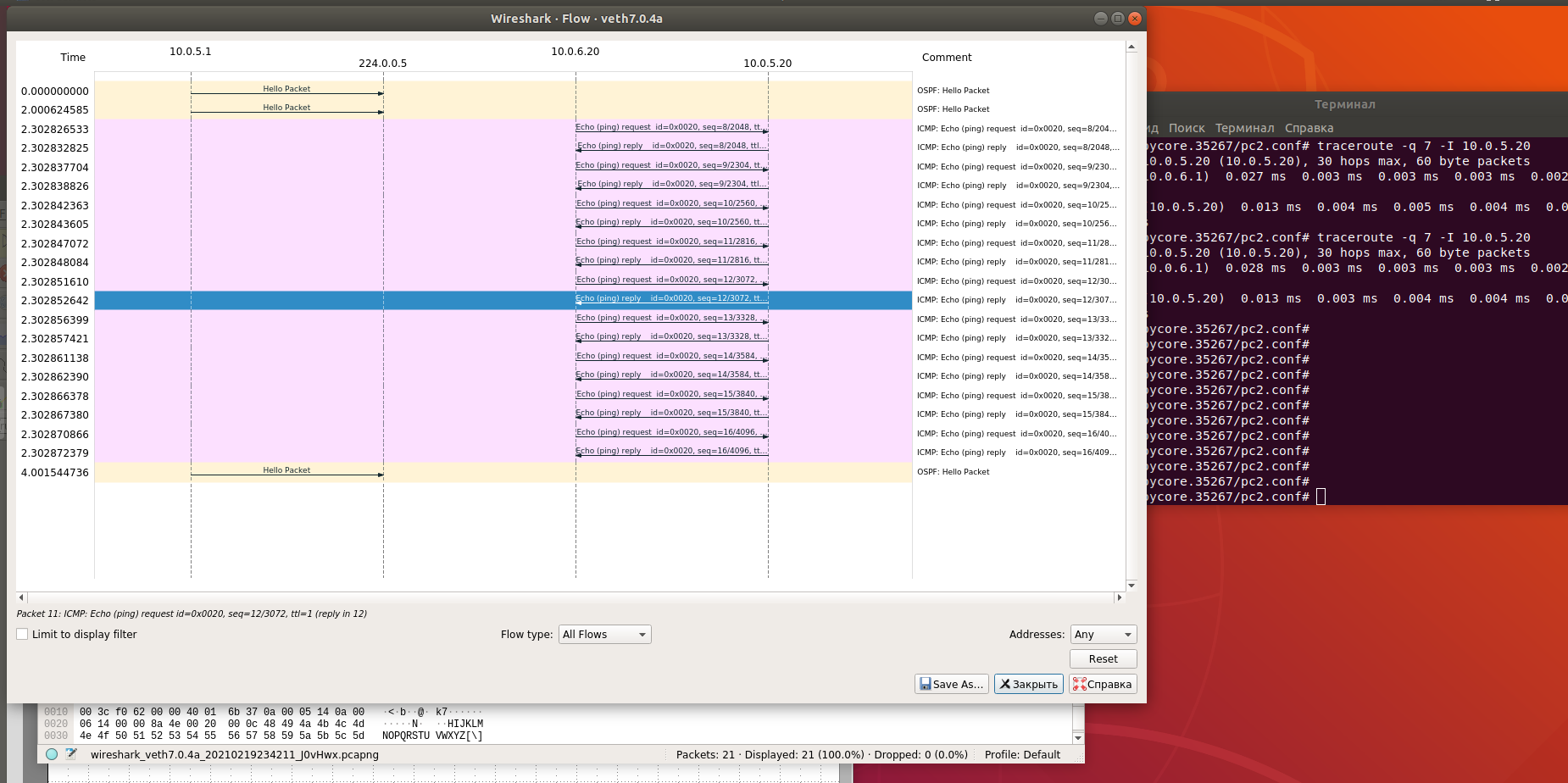
Пробуем пинговать первый пк ( wireshark на первом и фильтр на первый ) -> пакеты отображаются -> верно



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



1. 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 wiresharkек 