МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра «Вычислительные Системы и Технологии»

ОТЧЕТ

По лабораторной работе №5

РУКОВОДИТЕЛЬ:

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

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Юрчук М.С.

(подпись) (фамилия, и.,о.)

19-В-1

(шифр группы)

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

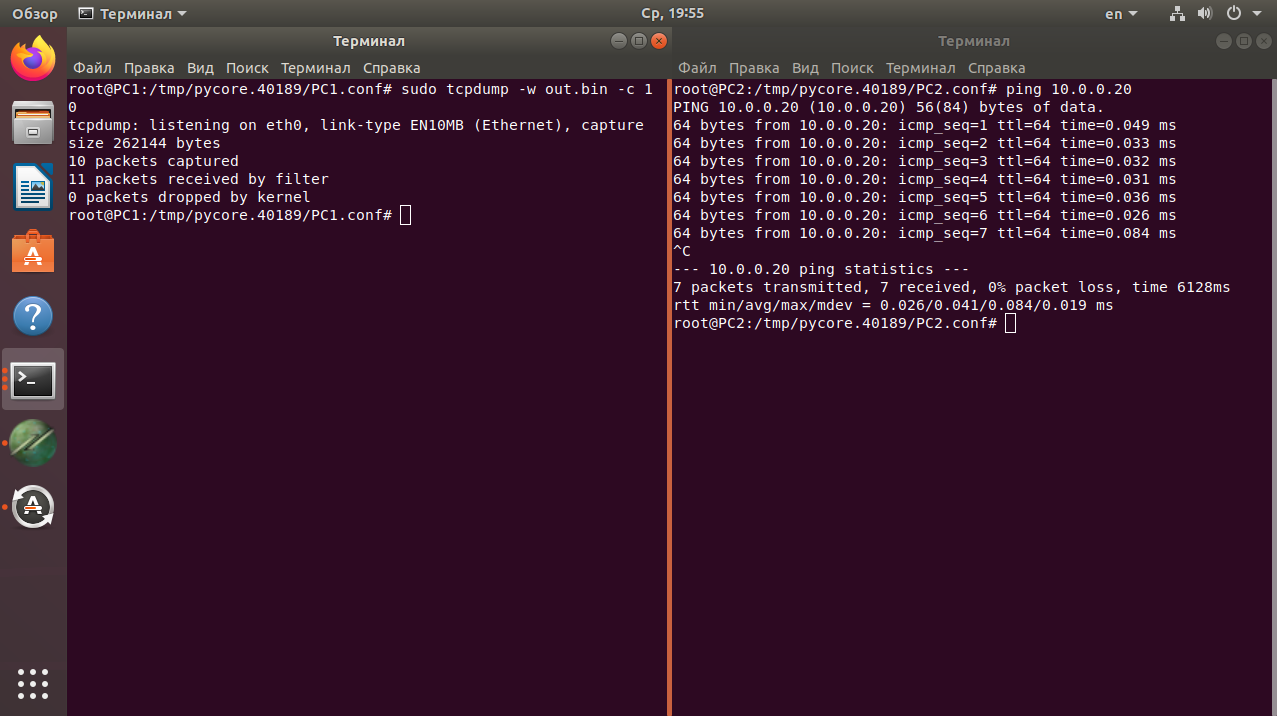
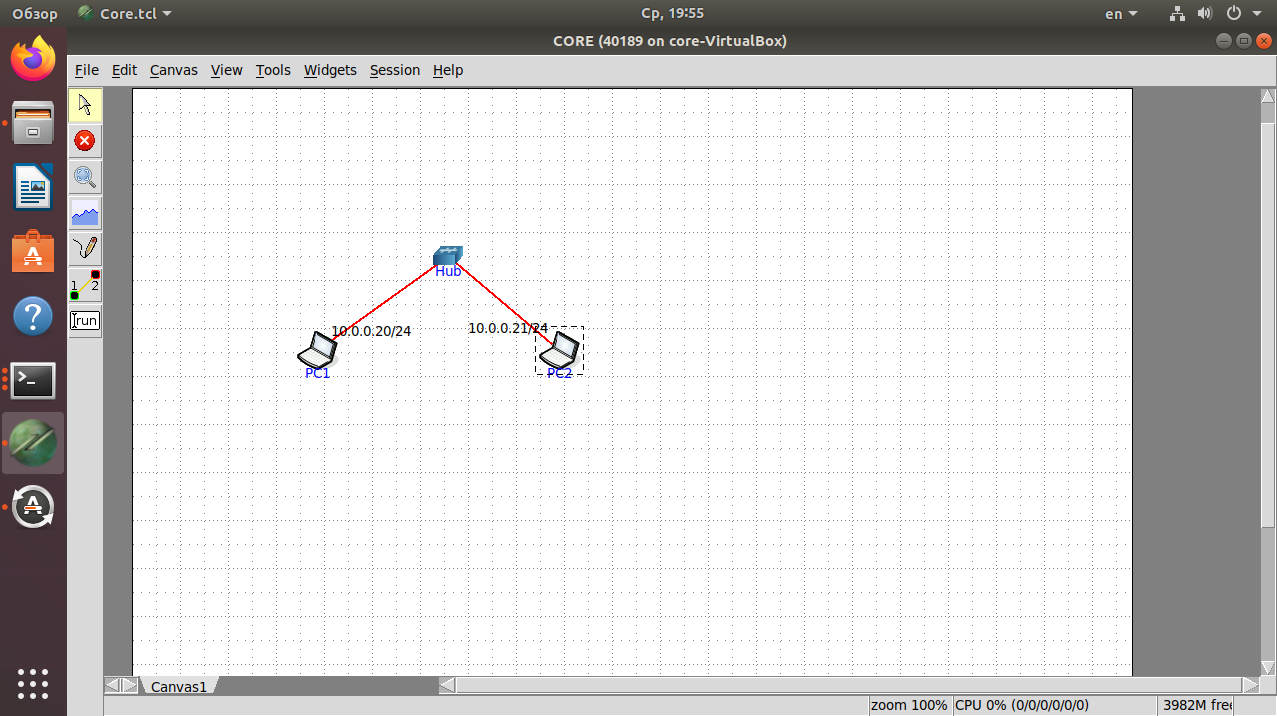
С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород 2021

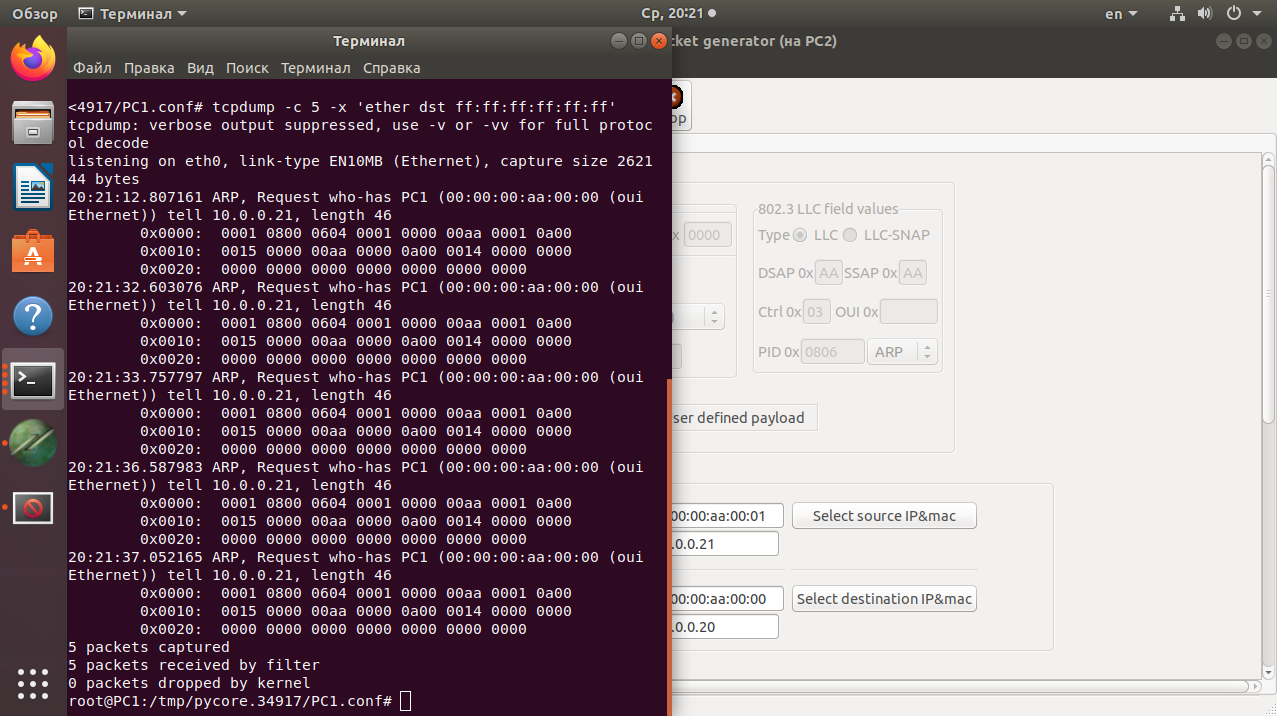
Задание:

**Работа с анализатором протоколов tcpdump**

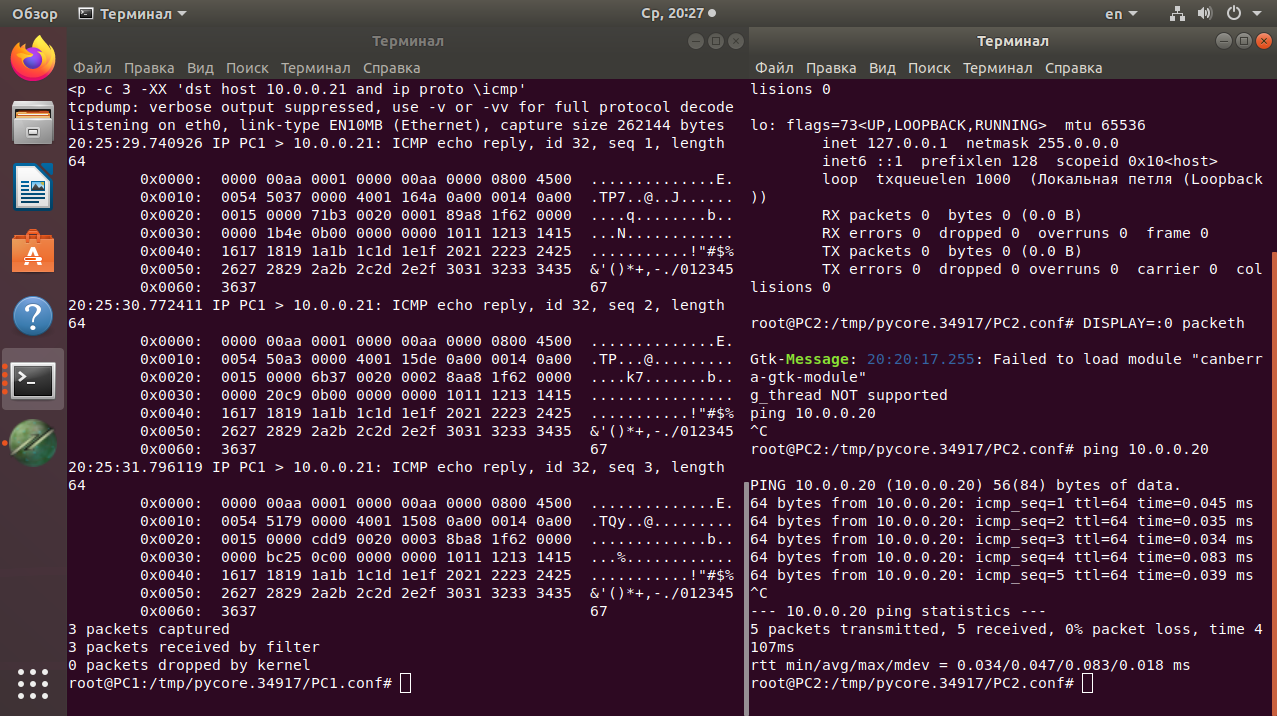
1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.



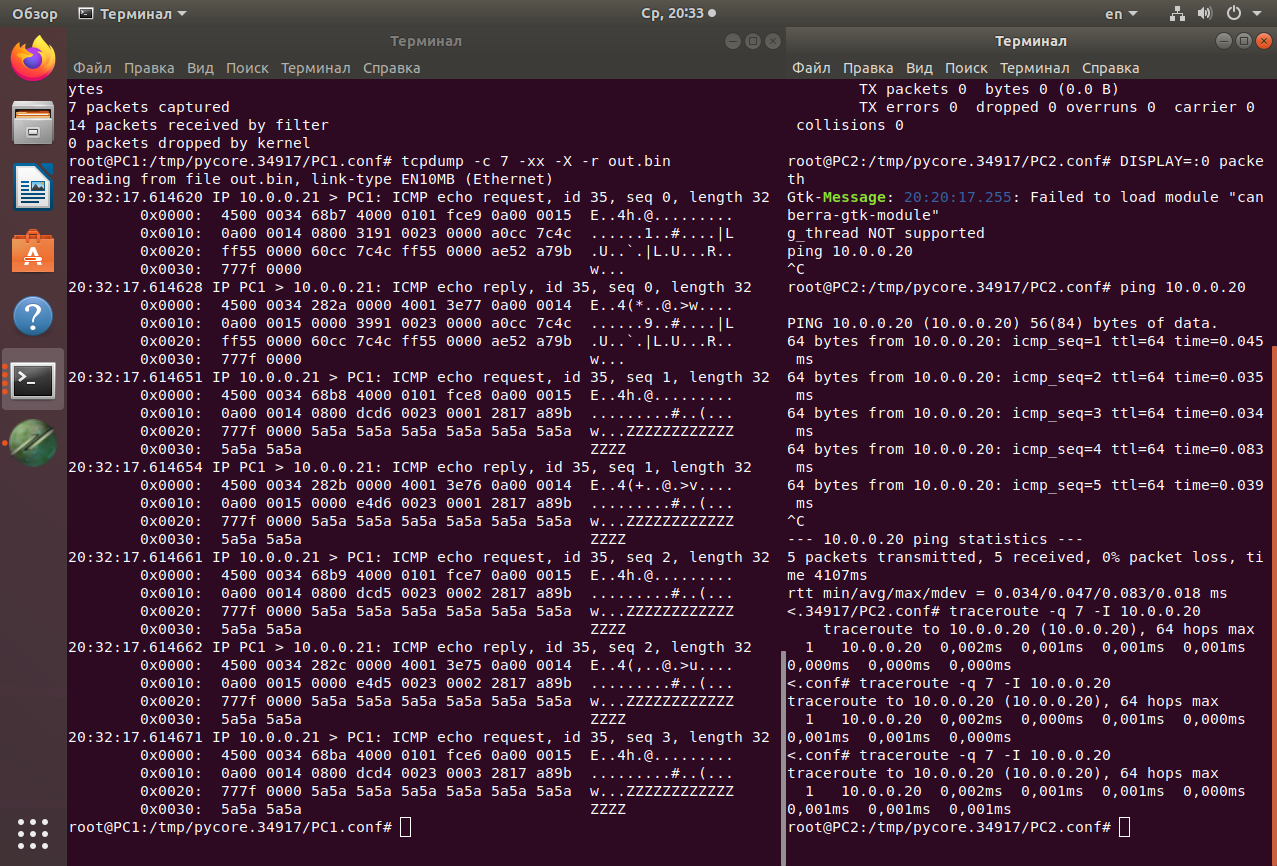
2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MACадресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).



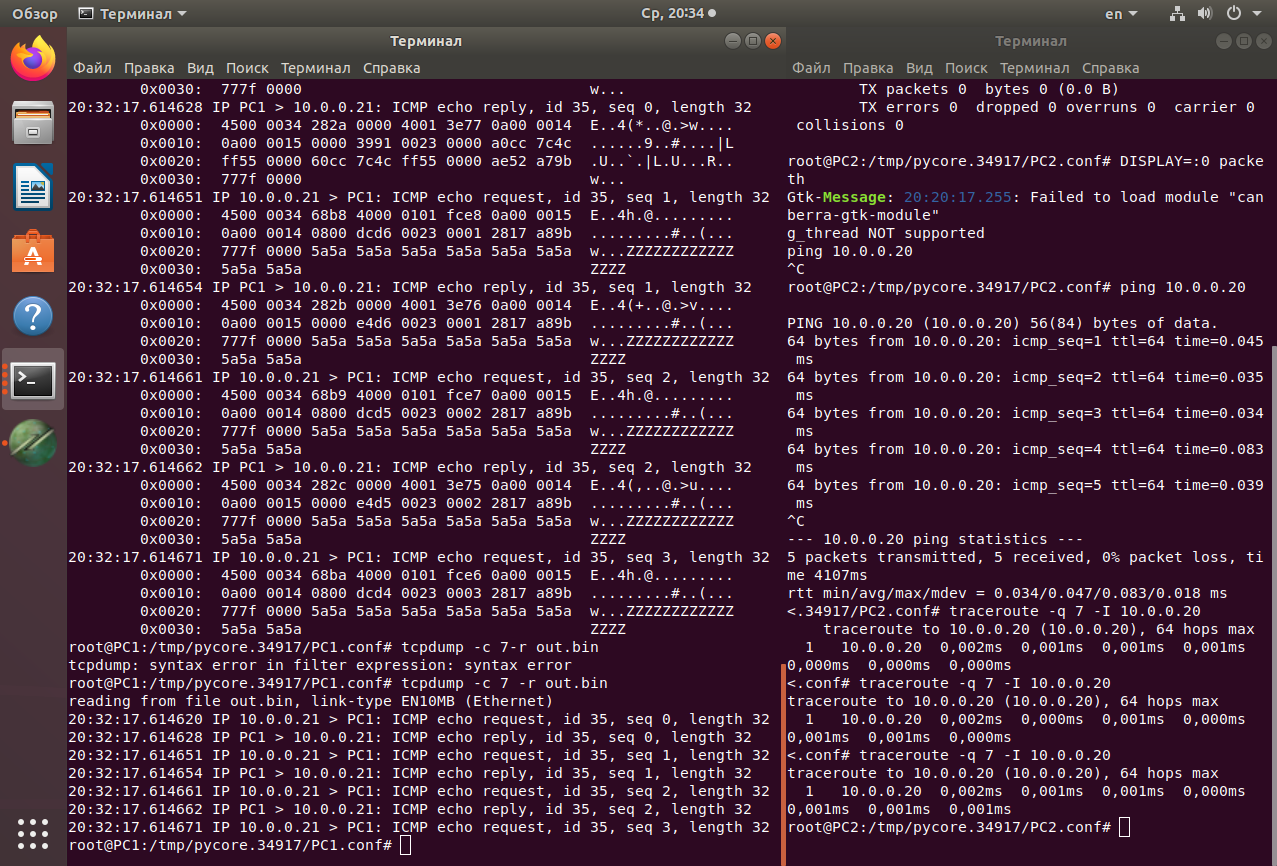
3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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



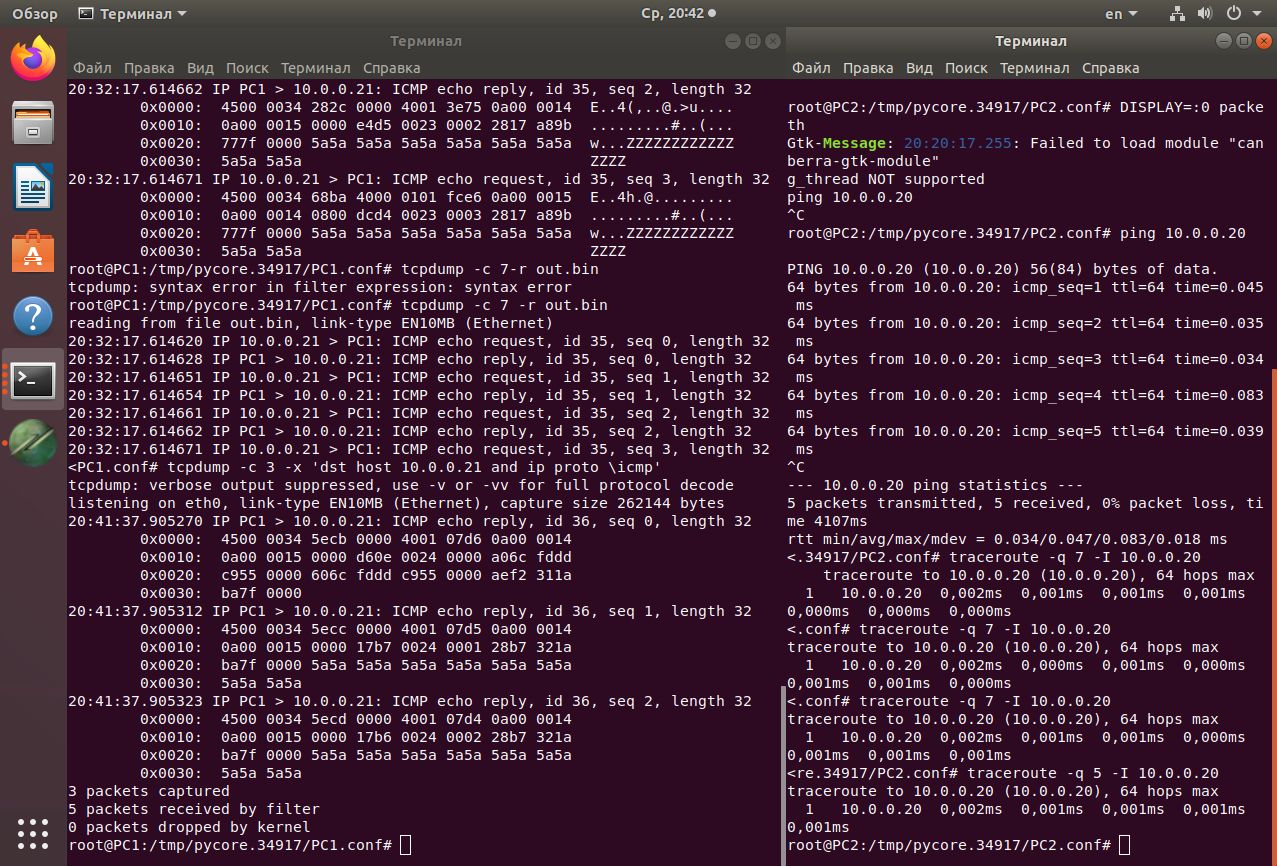
4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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



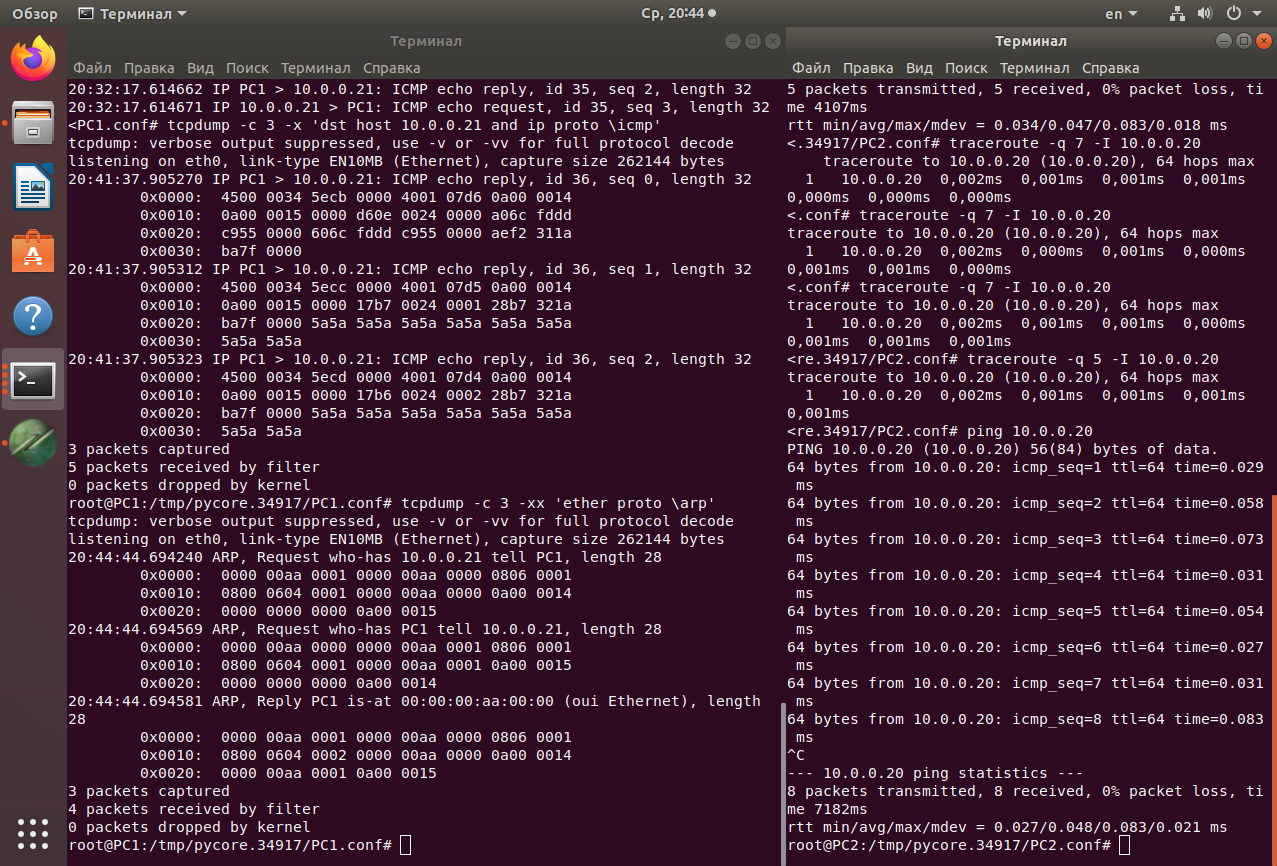
5. Прочесть программой tcpdump созданный в предыдущем пункте файл.



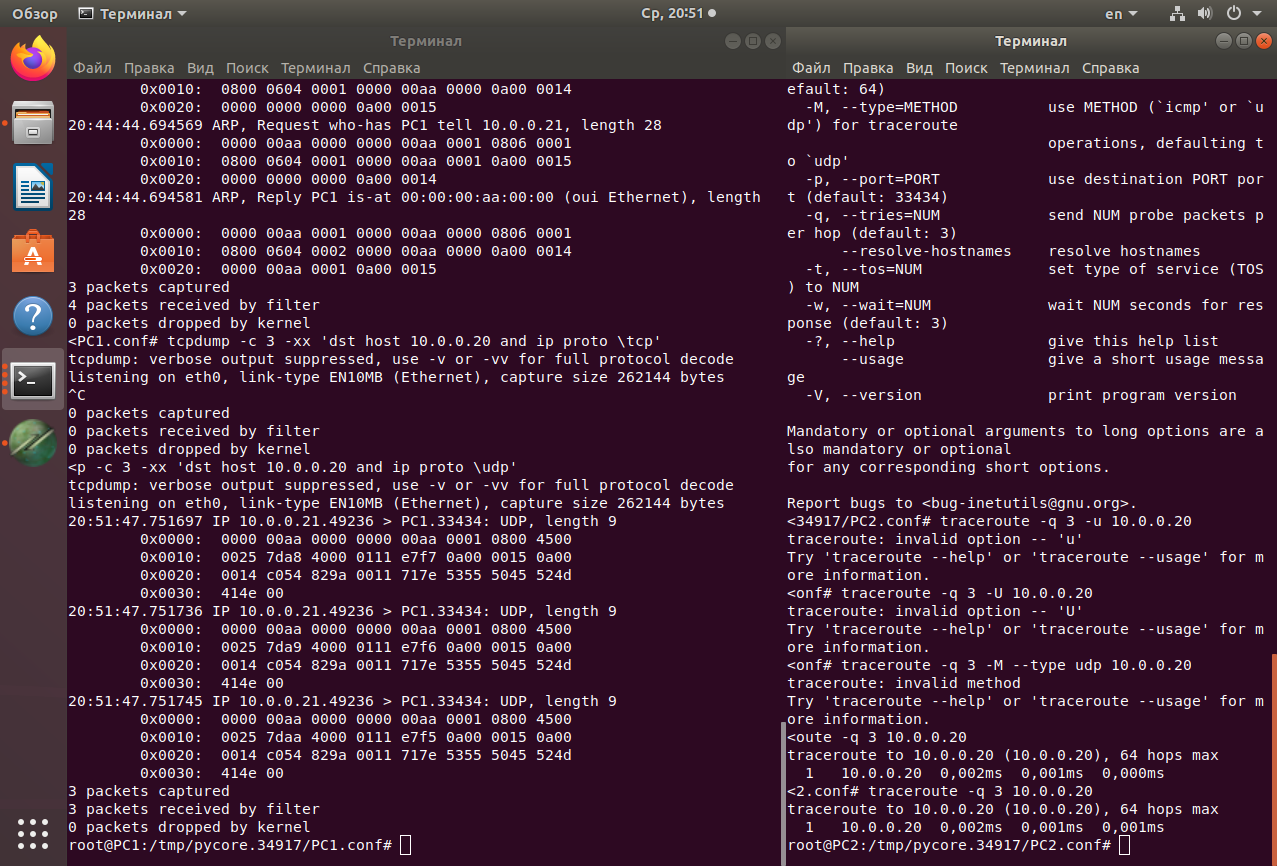
6.1. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. Включить распечатку пакета в шестнадцатеричной системе (не включая заголовок канального уровня). Количество захватываемых пакетов - 3. Пакеты создавать утилитой traceroute.



6.2. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ARP, отправленные на определенный IP-адрес. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество захватываемых пакетов – 3. Для генерирования пакетов воспользоваться утилитой ping.

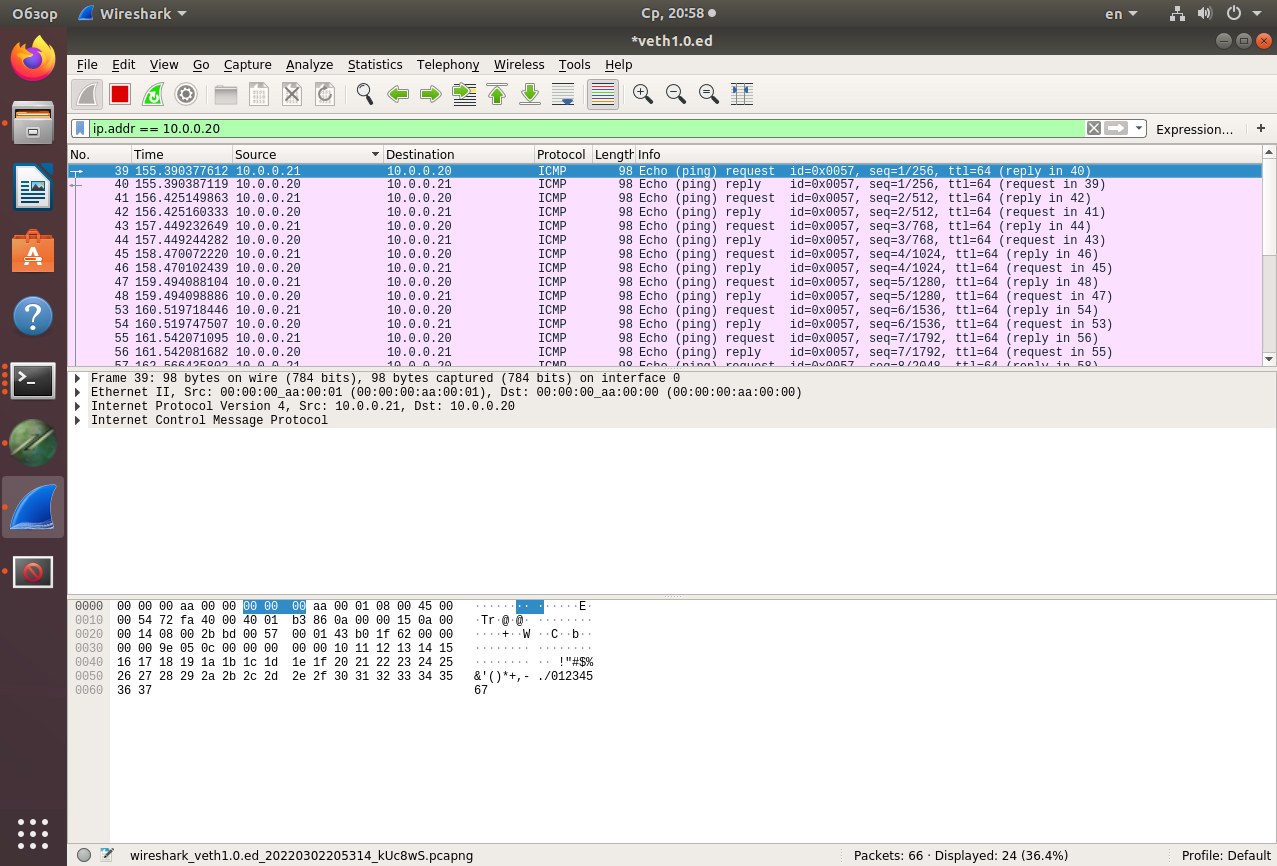


6.3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола UDP, отправленные на определенный IP-адрес. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество захватываемых пакетов – 3. Для генерирования пакетов воспользоваться утилитой traceroute.

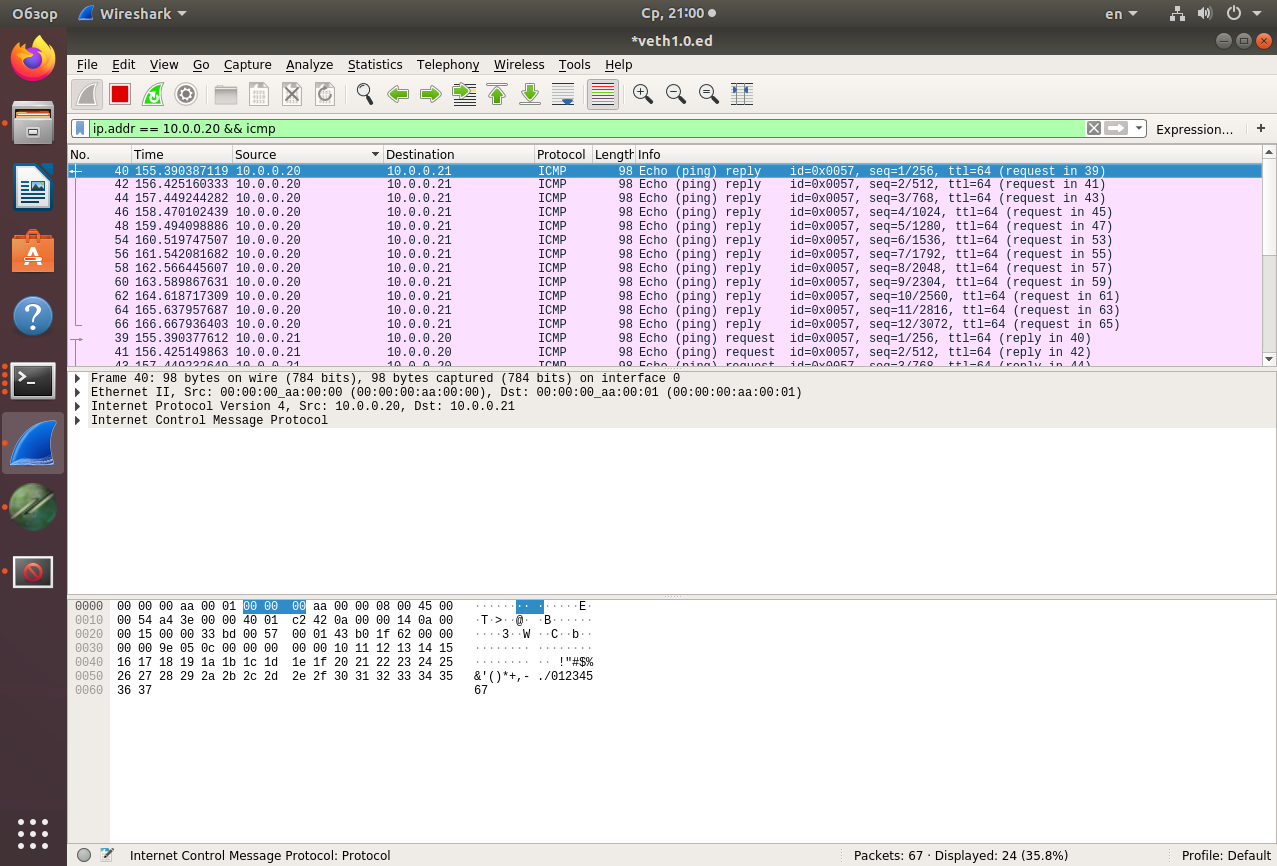


**Работа с анализатором протоколов wireshark**

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 возпользоваться 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.

