**Московский государственный технический**

**университет им. Н.Э. Баумана**

Факультет «Информатика и системы управления»

Кафедра ИУ5 «Системы обработки информации и управления»

Курс «Сети и телекоммуникации»

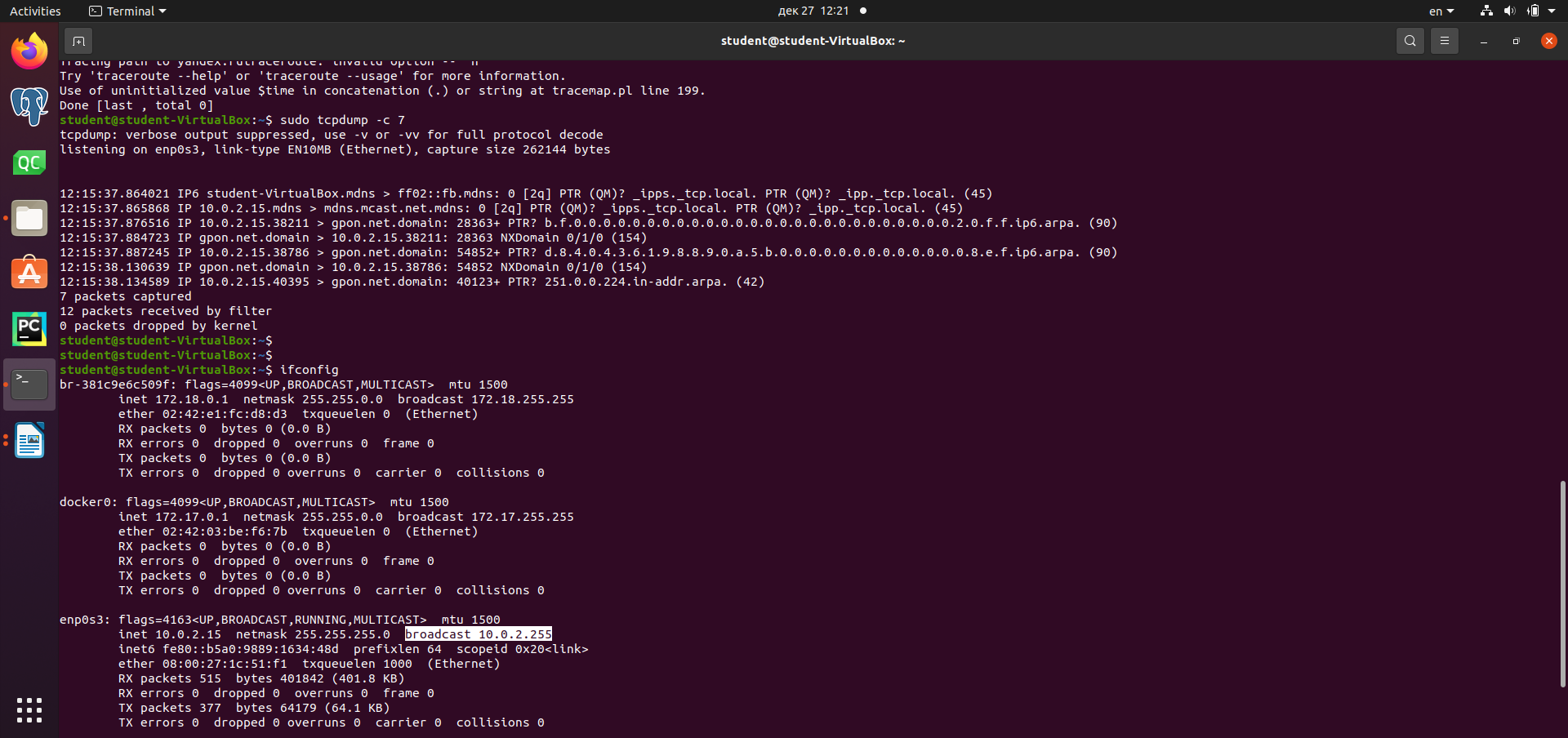
Отчет по лабораторной работе №7 «Работа с программным анализатором протоколов tcpdump»

|  |  |  |
| --- | --- | --- |
| Выполнил: |  | Проверил: |
| студент группы ИУ5-53Б |  | преподаватель каф. ИУ5 |
| Терентьева Софья  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |  | Антонов Артем Ильич  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |

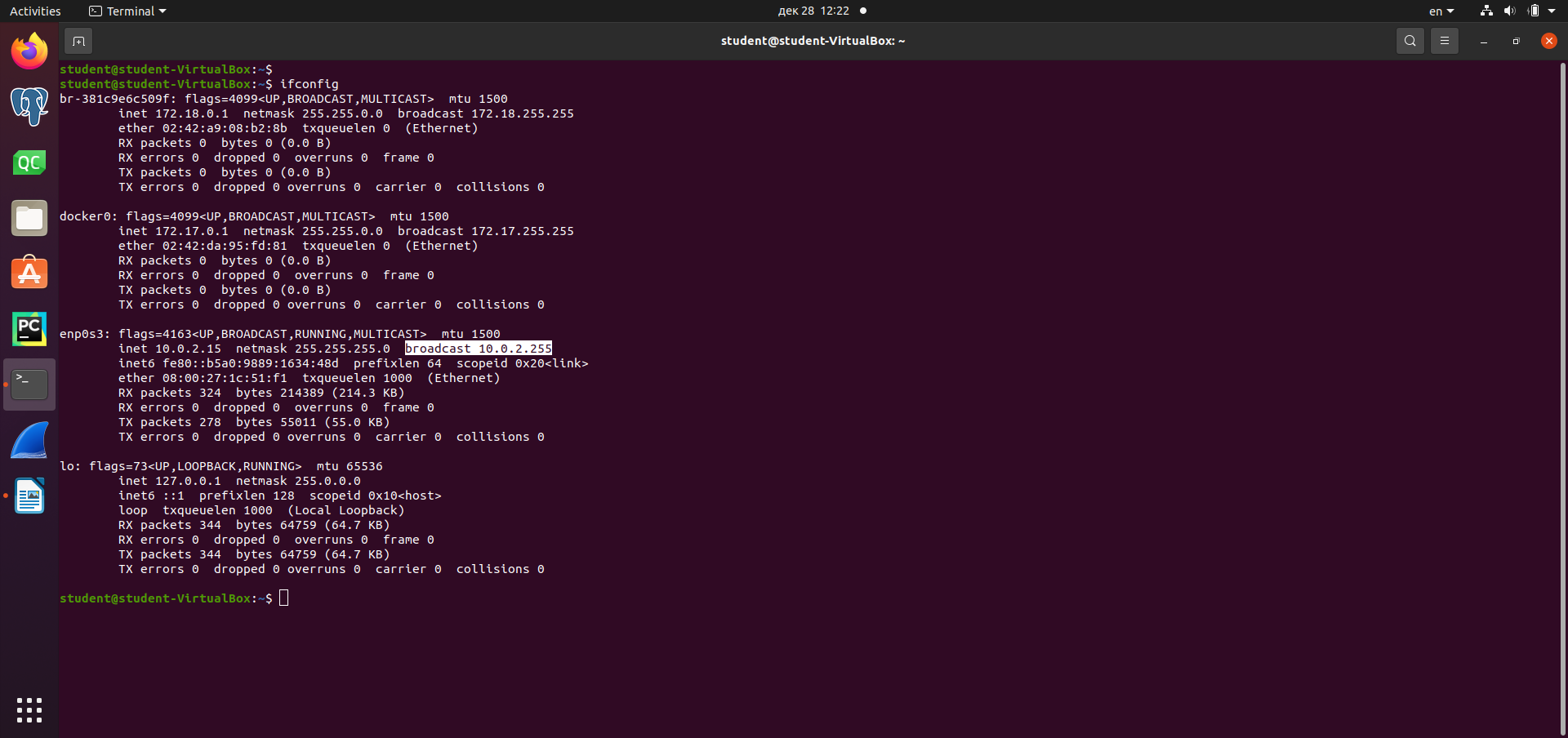
Москва, 2023 г.

Ход работы:

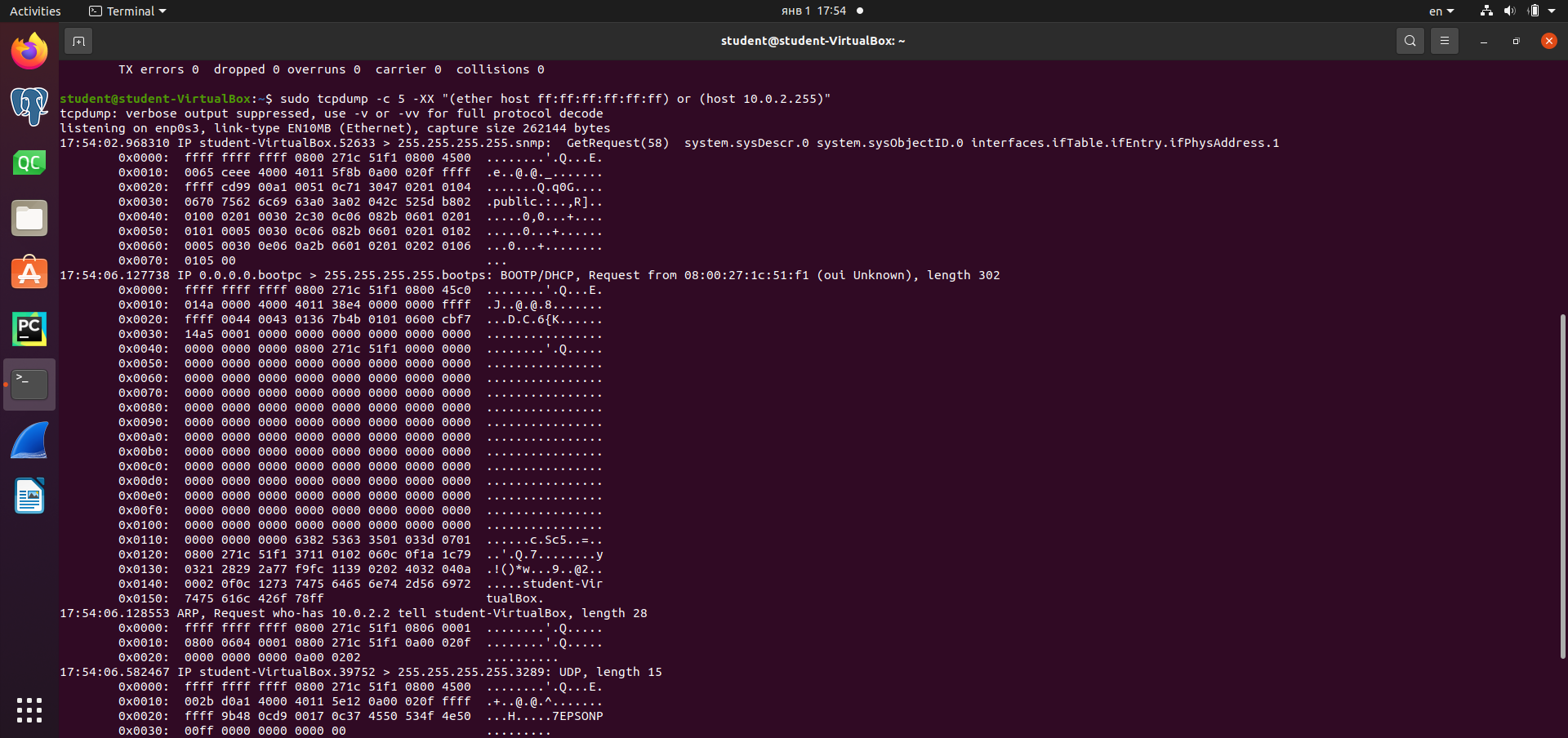
1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети (без фильтра). Количество захватываемых пакетов ограничить семью.

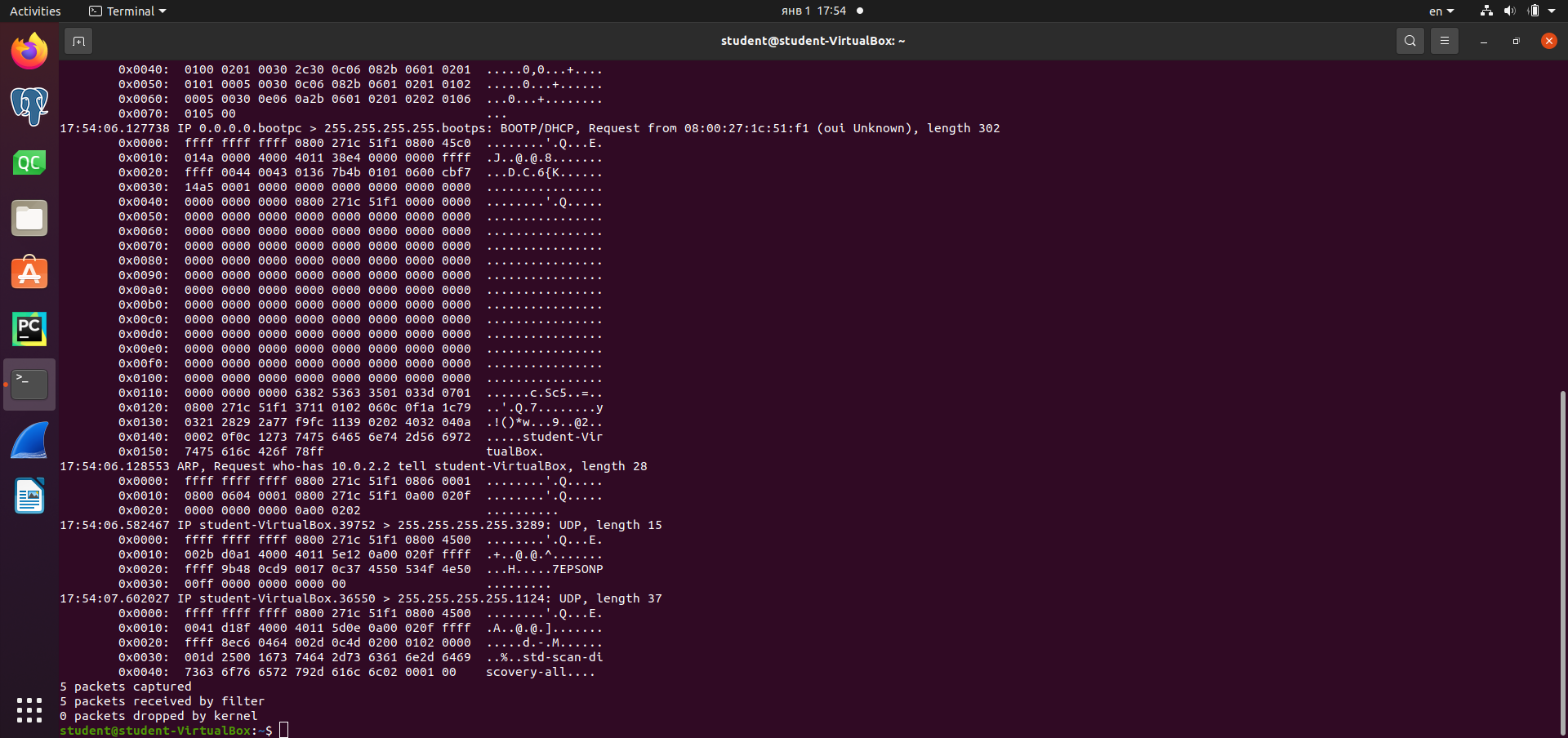


1. Запустить tcpdump в режиме перехвата широковещательного трафика. Фильтровать трафик и по широковещательному аппаратному MAC-адресу (FF:FF:FF:FF:FF:FF), и по широковещательному IP-адресу (можно посмотреть с помощью утилиты ifconfig). Фильтры должны быть связаны логическим объединением. Количество захватываемых пакетов ограничить пятью. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

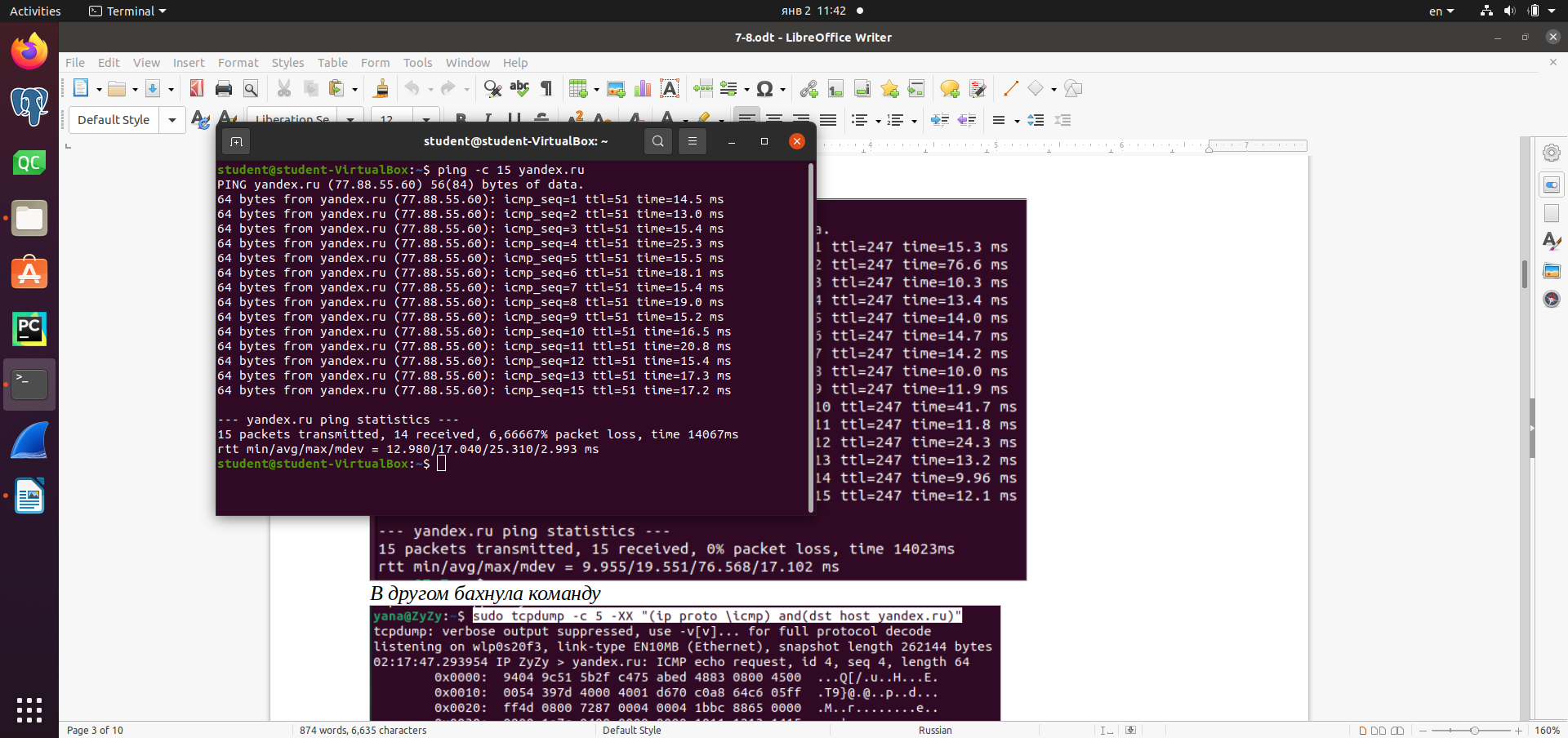


Вводим команду и ожидаем результат.

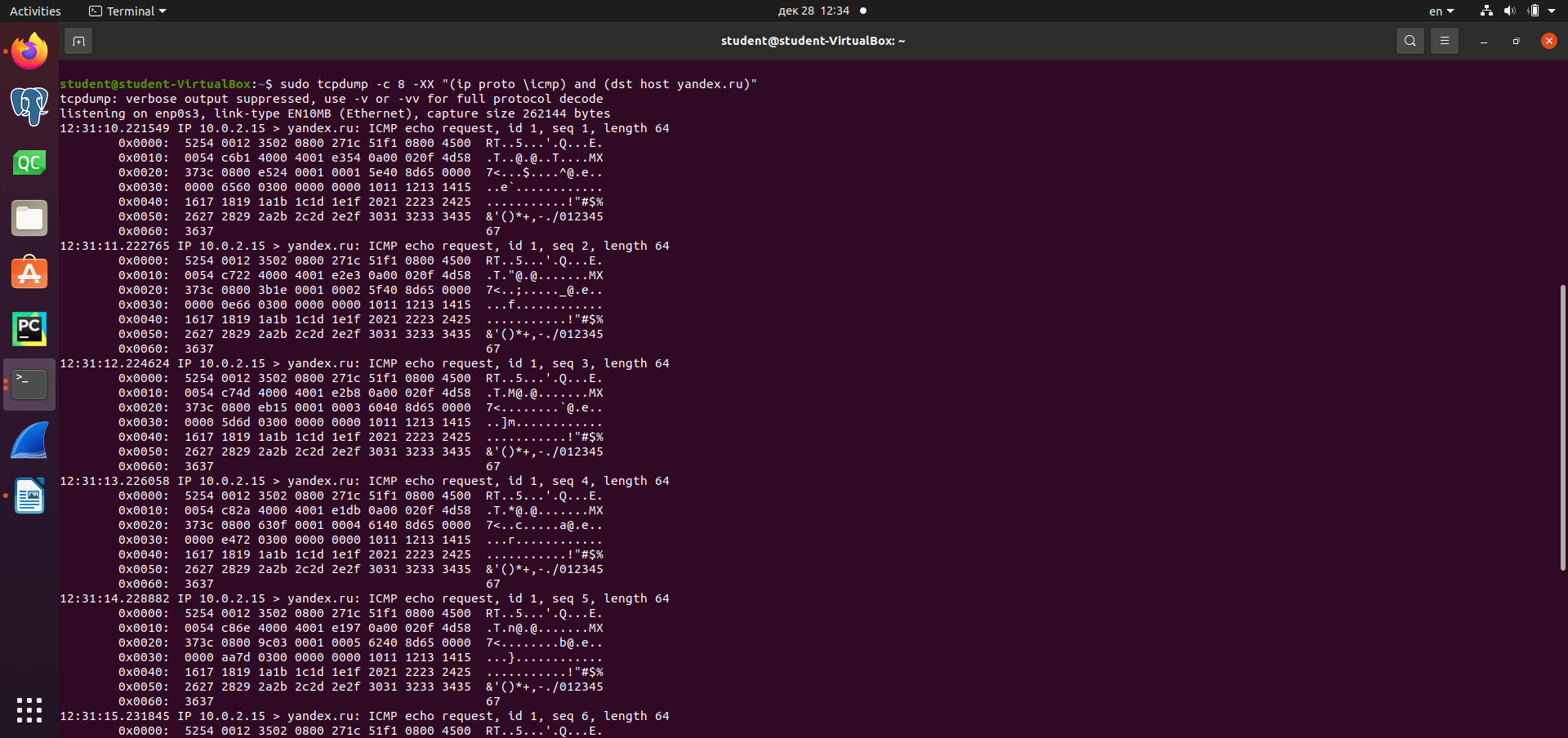


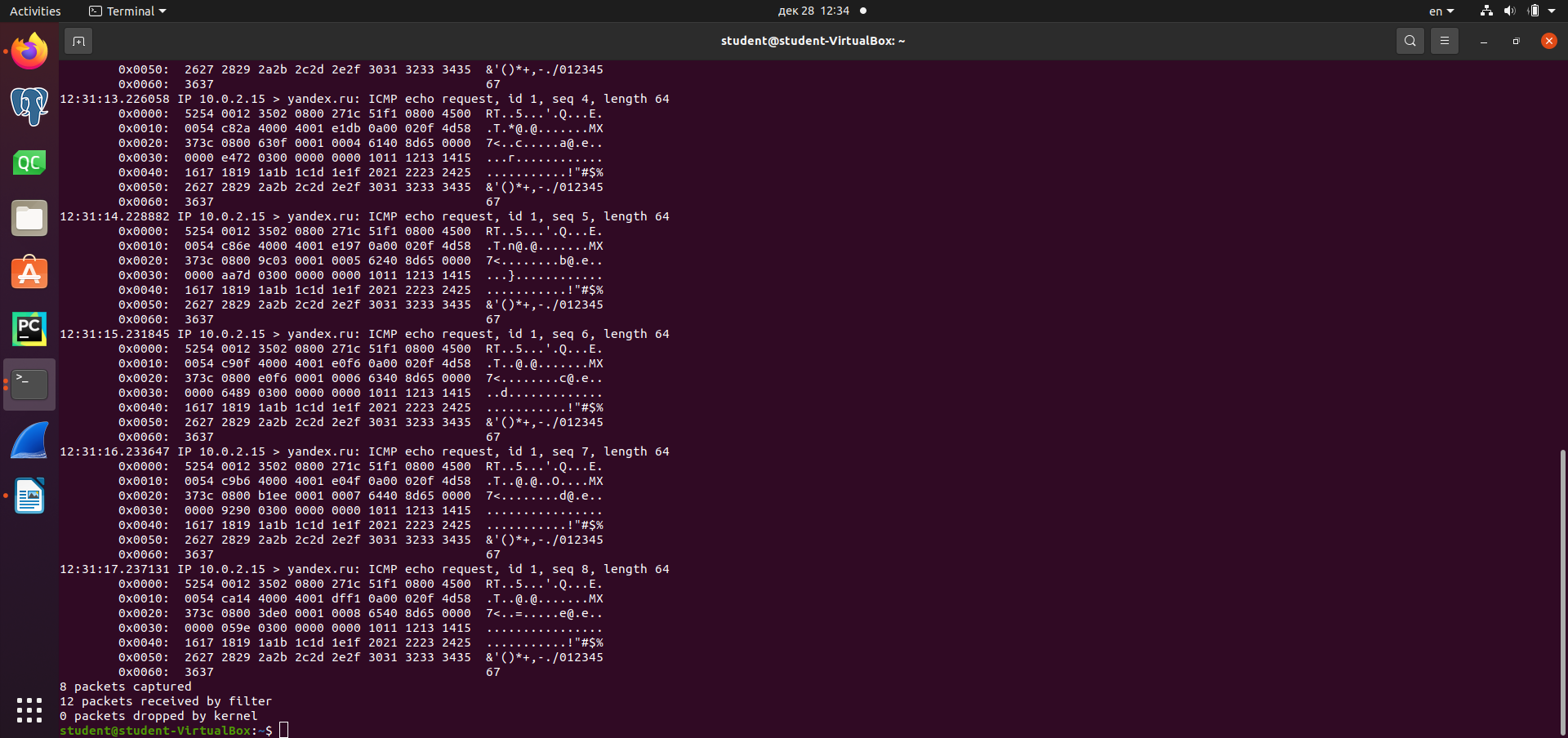


1. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на IP-адрес одного из лабораторных компьютеров. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить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

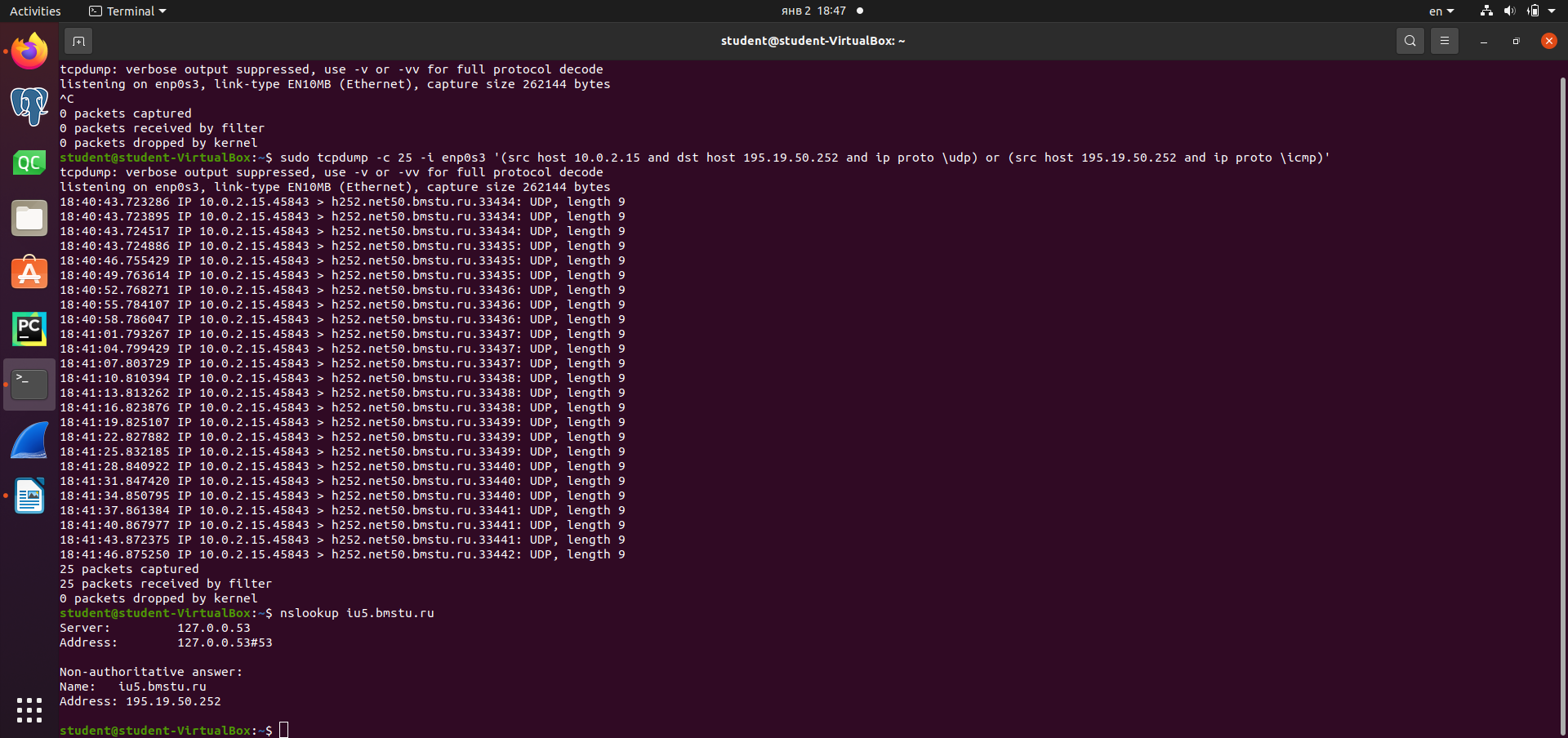


Открываем второй терминал, пингуем с него сайт yandex.ru. На основном терминале совершаем такие действия:



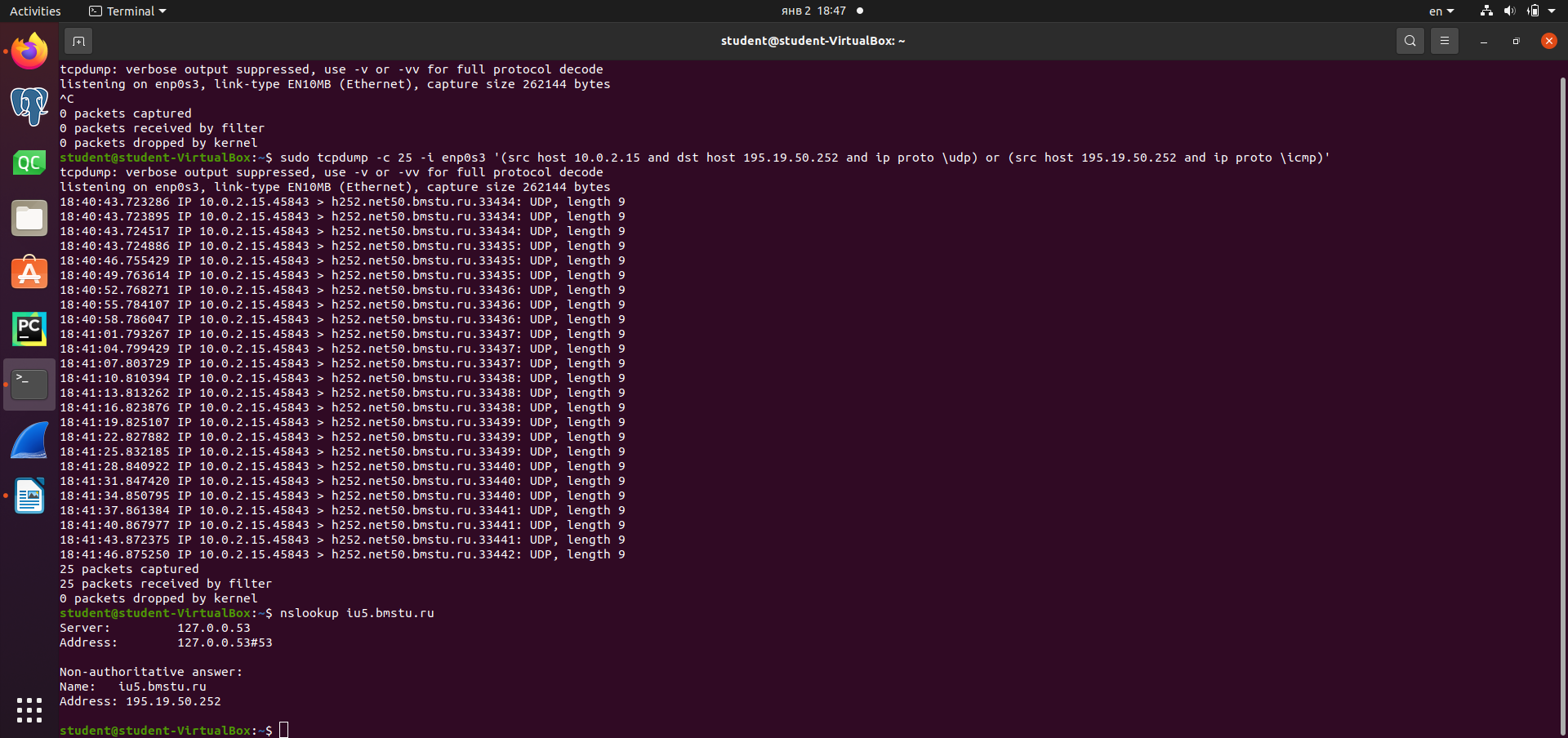


1. По образцу рассмотренного в теории примера перехватить трафик утилиты traceroute при определении маршрута до какого-либо узла в сети Интернет.

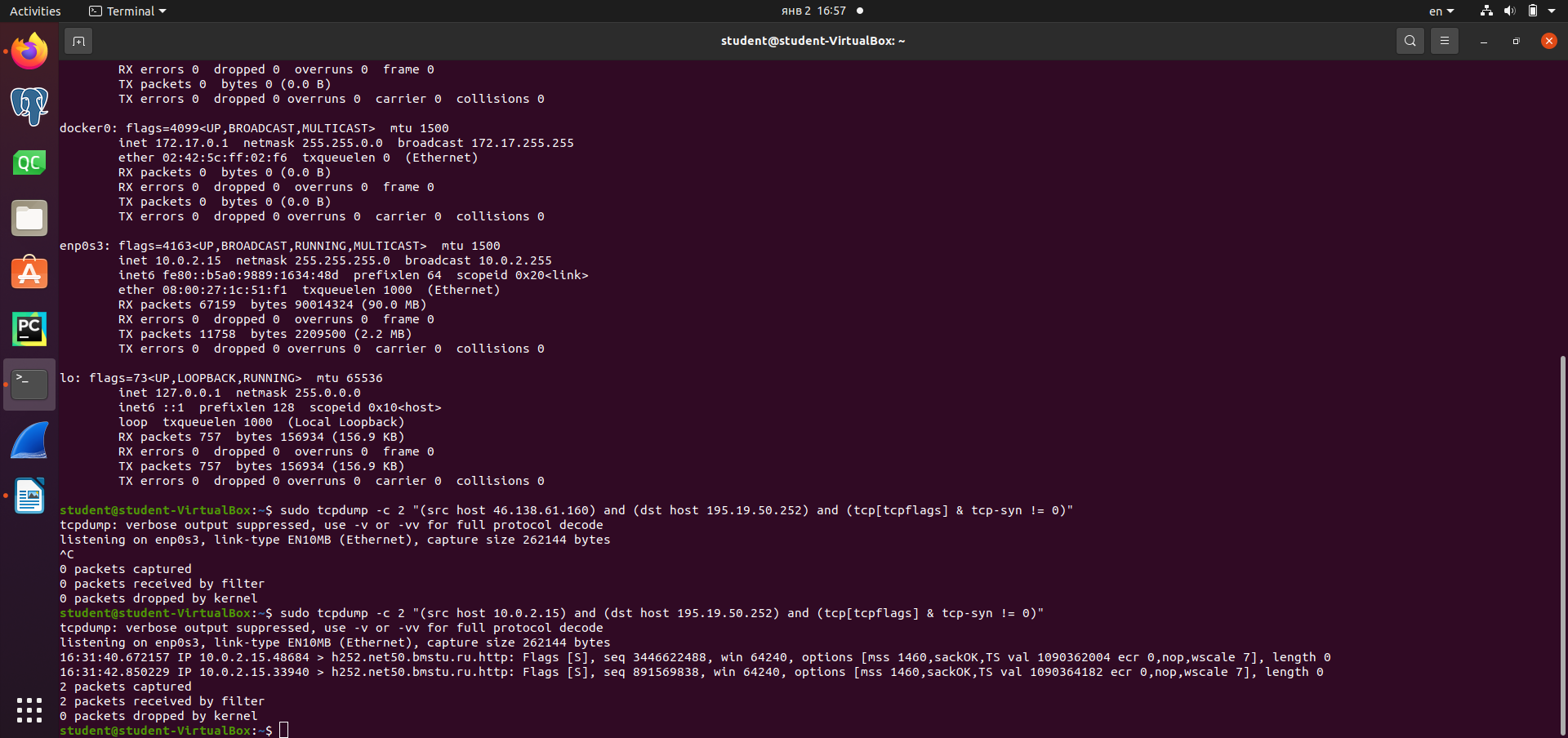


Так выяснили, что IP-адрес узла (сайта нашей кафедры) 195.19.50.252.

Чтобы начался трафик, в соседнем терминале следует запустить команду ***traceroute*** ***195.19.50.252***.

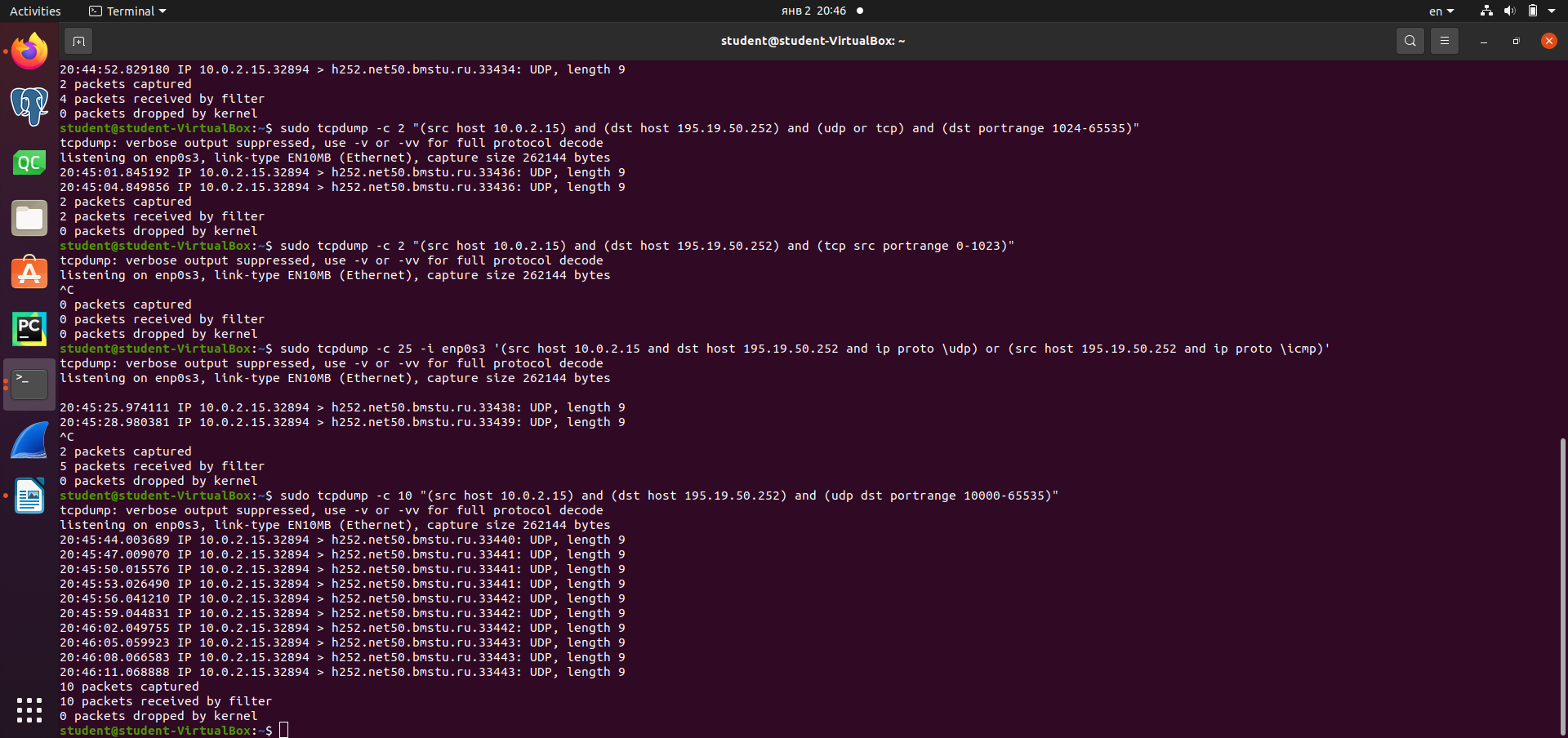


1. Используя утилиту tcpdump, отобрать дейтаграммы, принадлежащие соединению TCP между локальным лабораторным ПК и кафедральным сервером, и содержащие флаг SYN в заголовке транспортного уровня. Количество дейтаграмм ограничить двумя.

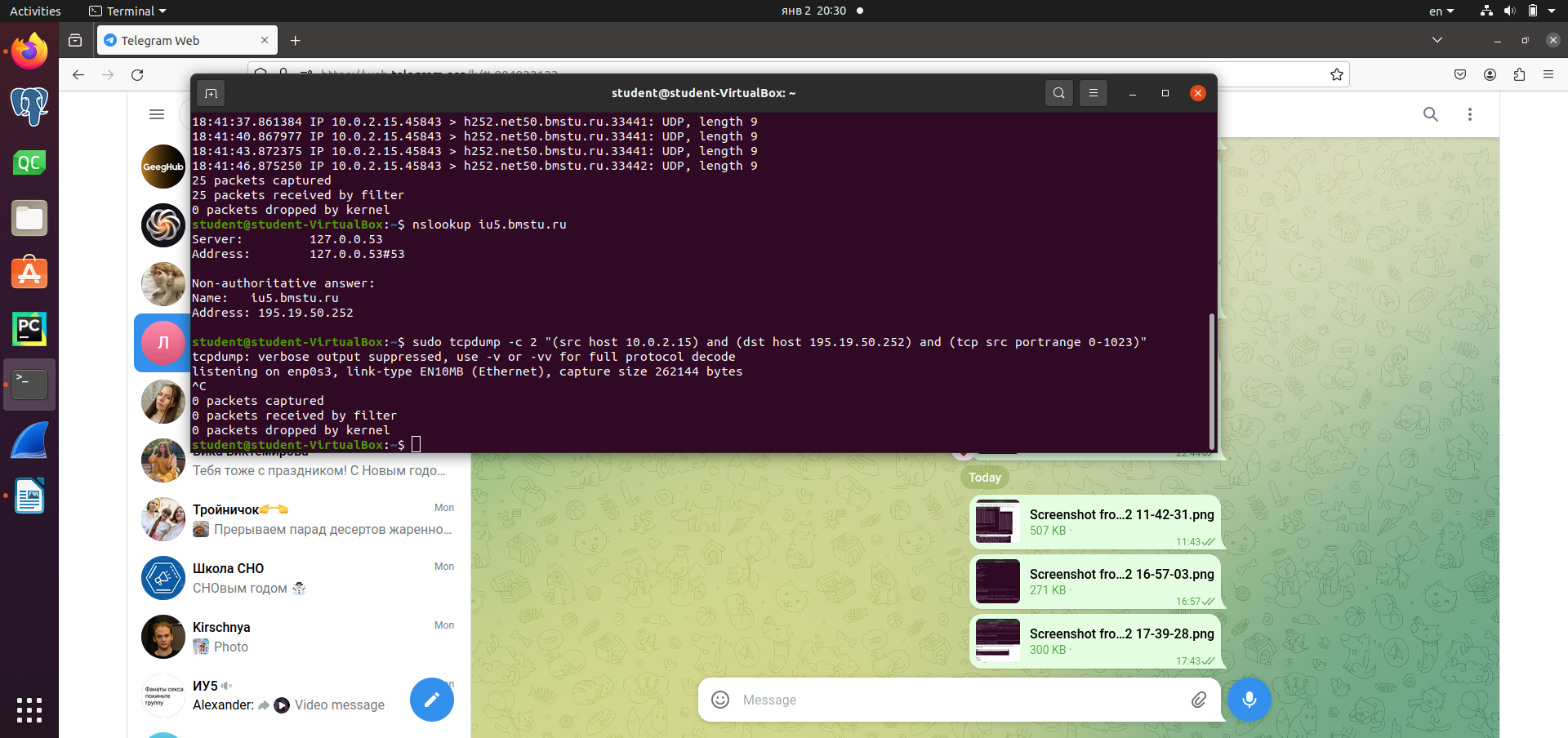


Трафик не будет происходить, пока мы не попытаемся зайти на сайт по указанному адресу и что-то там сделать.

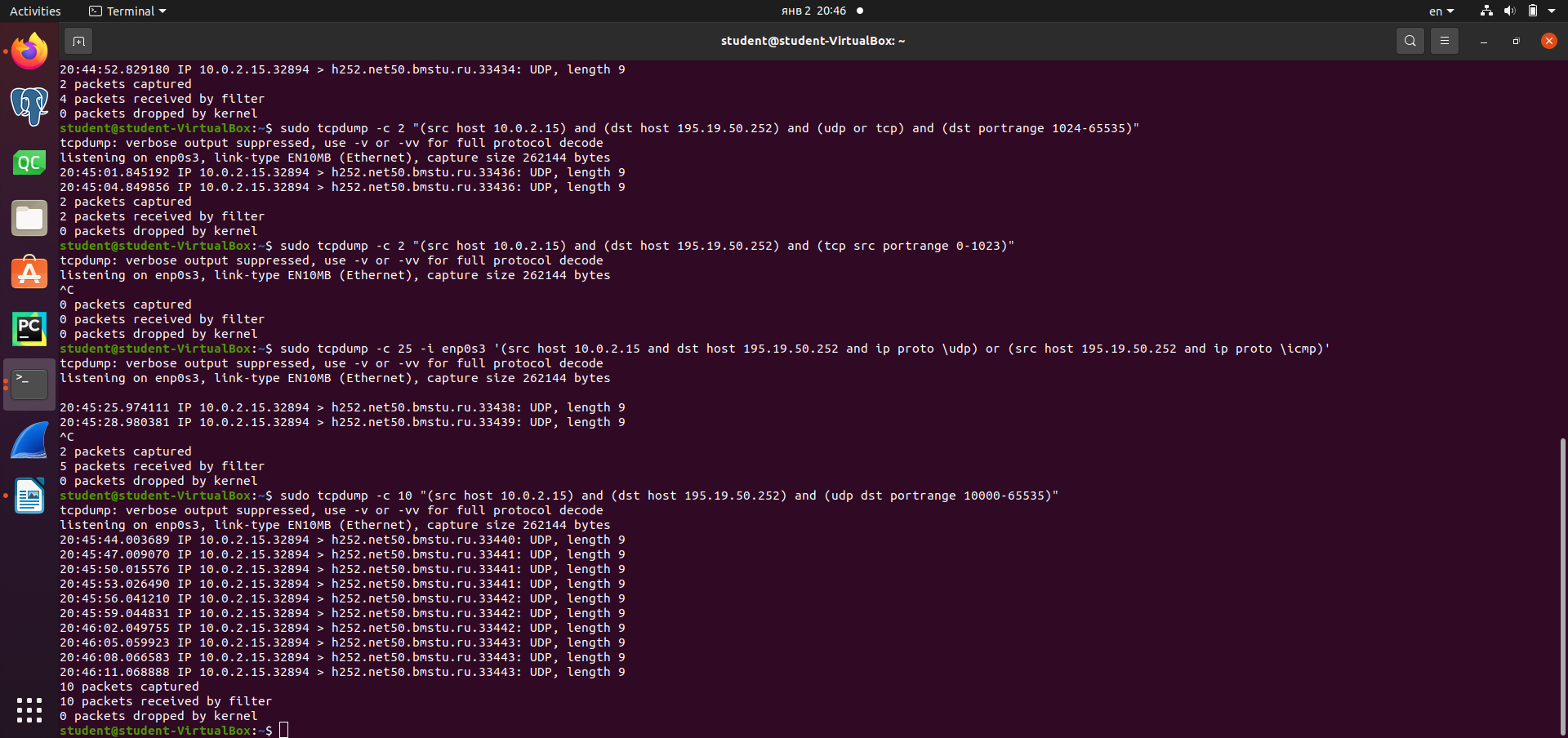
1. Отобрать дейтаграммы UDP, пересылаемые между локальным лабораторным ПК и сервером, отправленные с номера порта UDP службы DSN, на диапазон портов назначения 10000–65535. Количество дейтаграмм ограничить десятью.



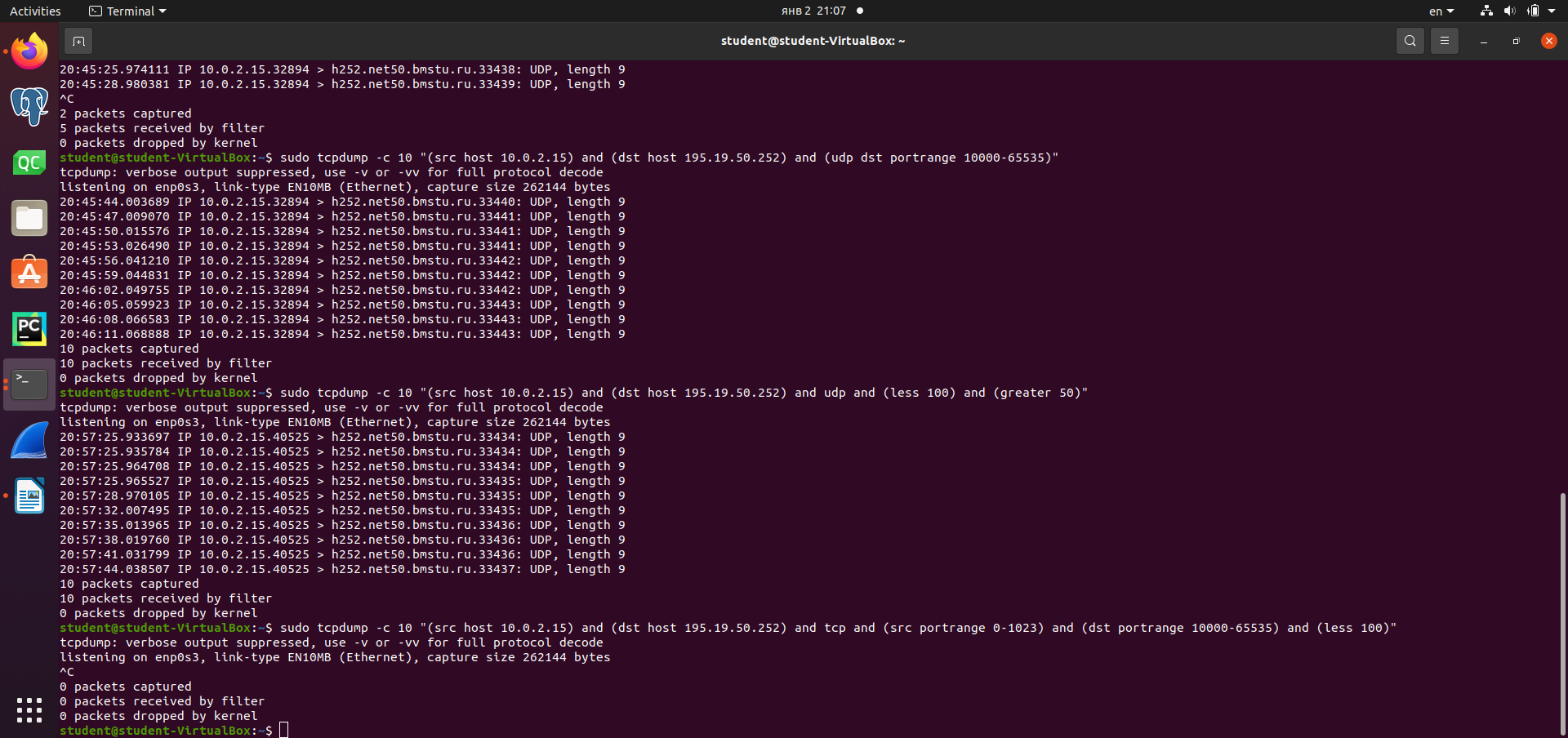
1. Отобрать дейтаграммы, принадлежащие соединениям TCP между локальным лабораторным ПК и сервером, установленные между номерами исходящих портов TCP со значением меньше 1024. Количество дейтаграмм ограничить двумя.



1. Отобрать дейтаграммы, пересылаемые между локальным лабораторным ПК и сервером, и использующие номера портов назначения (UDP или TCP) со значениями большими 1024. Количество дейтаграмм ограничить двумя.



1. Отобрать дейтаграммы, UDP пересылаемые между локальным лабораторным ПК и сервером, размер которых больше 50 байт, но не превышает 100 байт. Количество дейтаграмм ограничить десятью. Следует напомнить, что для отбора дейтаграмм в соответствии с размером необходимо использовать выражение less X или greater X, отображающее дейтаграммы размером (в байтах) меньше или больше X, соответственно.



1. Отобрать дейтаграммы IP, пересылаемые между локальным лабораторным ПК и сервером, принадлежащие соединению TCP, отправленные с порта источника менее 1024 на порт назначения более 10000, размер которых не превышает 100 байт.

