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»

«Сети и телекоммуникации»

**Отчет по лабораторной работе №1**

Выполнил студент группы 18 В-2

Модин Артем

«01» марта 2021 г.

Проверил преподаватель

Гай Василий Евгеньевич

«\_\_\_» \_\_\_\_\_\_\_ 20\_\_\_ г.

Нижний Новгород

2021 г.

**Цель работы:**

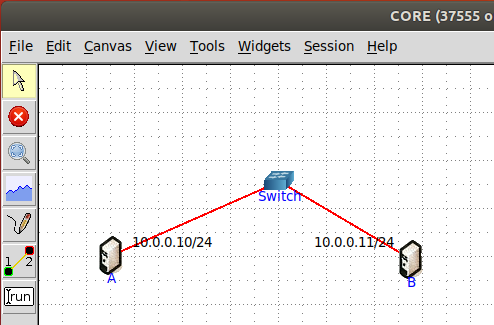
познакомиться с анализатором протоколов tcpdump и сравнить его работу с работой анализатора wireshark.

**Выполнение:**

**tcpdump**

1. Подготовительный этап.

* Создаем сеть. Два компьютера и Switch (коммутатор, работающий на канальном уровне. Соединяет компьютеры в сеть).

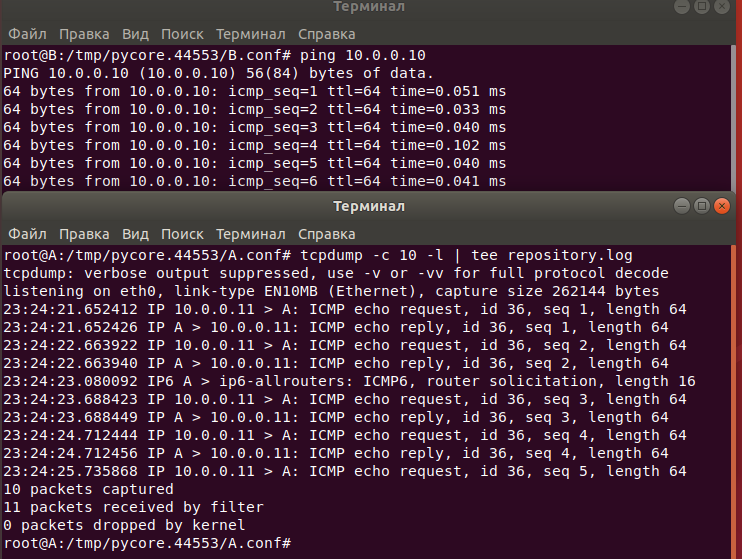


1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количества захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

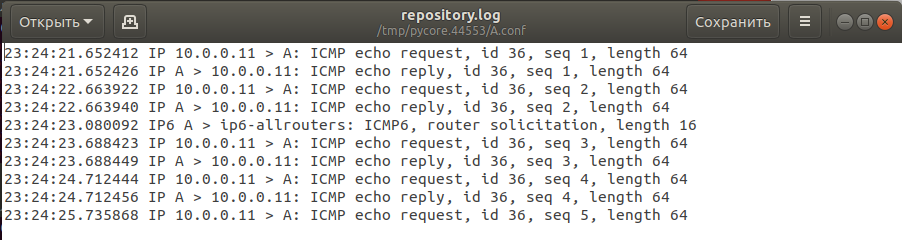
- Команды, используемые в выполнении задания:

ping 10.0.0.10 – команда пингования компьютера А с компьютера В.

tcpdump -c 10 -l | tee repository.log – команда захвата пакетов с компьютера А.



Откроем файл созданный при захвате пакетов и проверим содержимое.



1. Запустим 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).

- Команды, используемые в выполнении задания:

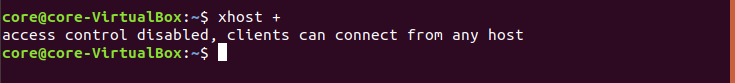
xhost + - подключение из эмулятора к графической подсистеме основной системы.

DISPLAY=:0 packeth – выбор дисплея.

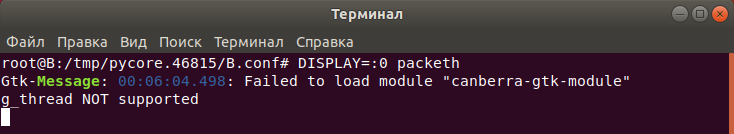
Ifconfig – информация о текущей конфигурации сети, настройки IP-адреса, сетевой маски или широковещательного адреса для сетевого интерфейса и тд.

tcpdump -c 5 -l -xx ether broadcast – завершит работу после 5 пакетов, распечатав пакет в шестнадцатеричной системе с заголовком канального уровня в широковещательном формате.

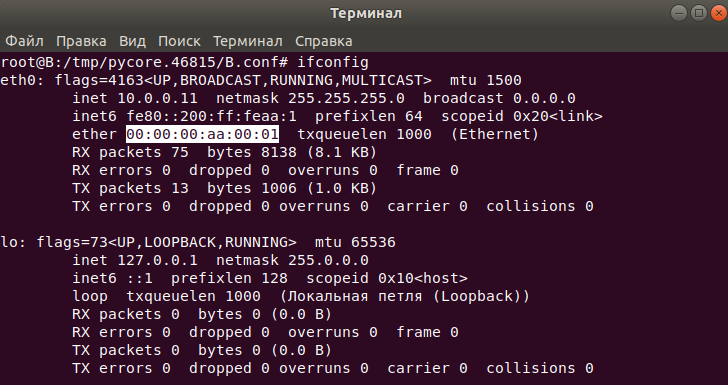
Подключаемся к графической подсистеме.



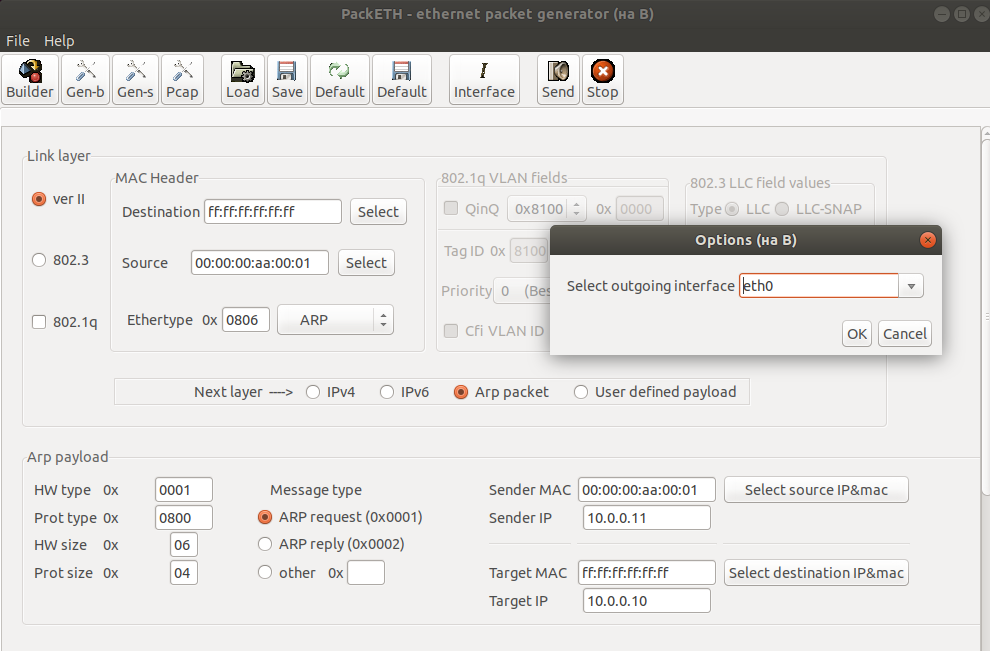
Выбираем дисплей.



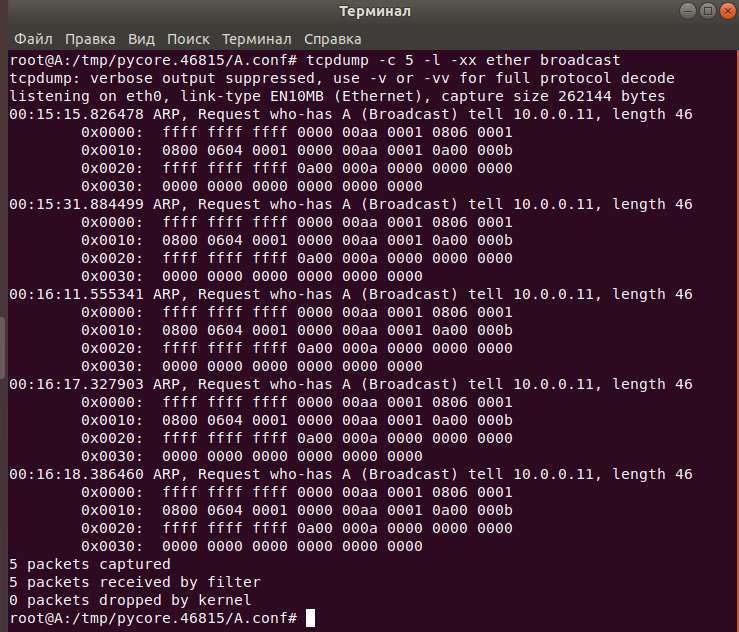
Узнаем MAC-адрес компьютера В.



Заполняем необходимые поля в packETHERNET. Составляем кадр запроса.



Перехватываем широковещательный трафик по MAC-адресу.

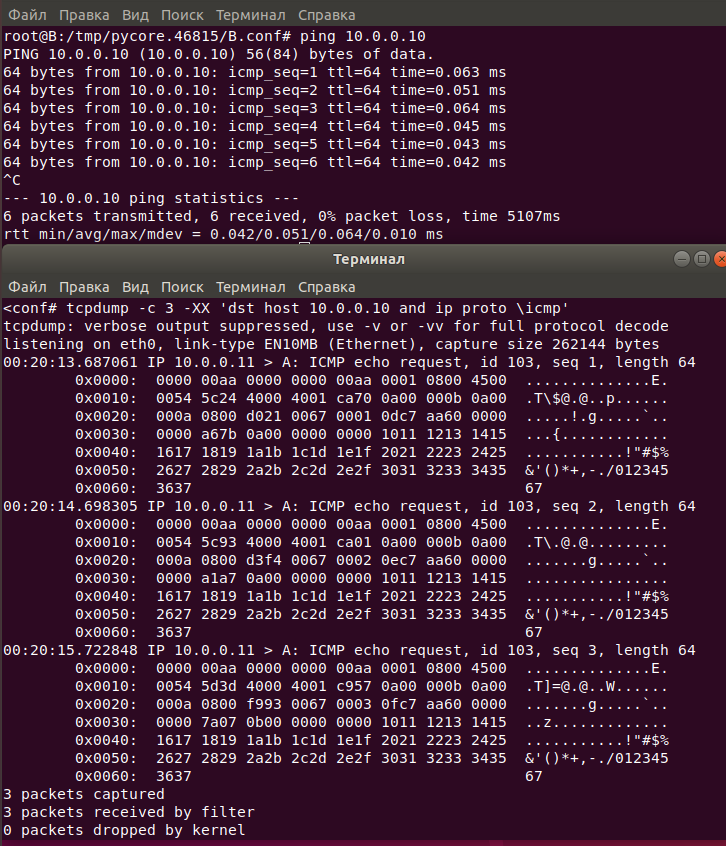


1. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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

- Команды, используемые в выполнении задания:

ping - 10.0.0.10 – команда пингования компьютера А с компьютера В.

tcpdump -c 3 -XX ‘dst host 10.0.0.10 and ip proto \icmp’ – завершит работу после получения 3 пакетов, выводя пакет в ASCII и hex-формате, включая заголовок канального уровня, отбирая пакеты, в которых поле адреса содержит адрес 10.0.0.10, отбирая все пакеты IP, содержащие ICMP.

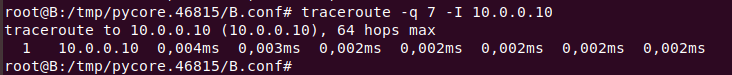


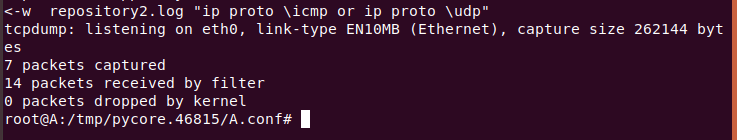
1. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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

- Команды, используемые в выполнении задания:

traceroute -q 7 -I 10.0.0.10 – определение маршрута следования данных с минимальным выводом информации.

tcpdump - -c 7 -XX -l -w repository2.log “ip proto \icmp pr ip proto \udp” -

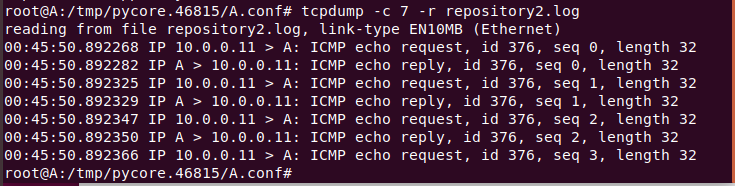




1. Прочесть программой tcpdump созданный в предыдущем пункте файл.

- Команды, используемые в выполнении задания:

tcpdump -c 7 -r repository2.log - чтение из файла( если он был сохранен с параметром -w). Выполнение команды прекратится после 7 пакета.



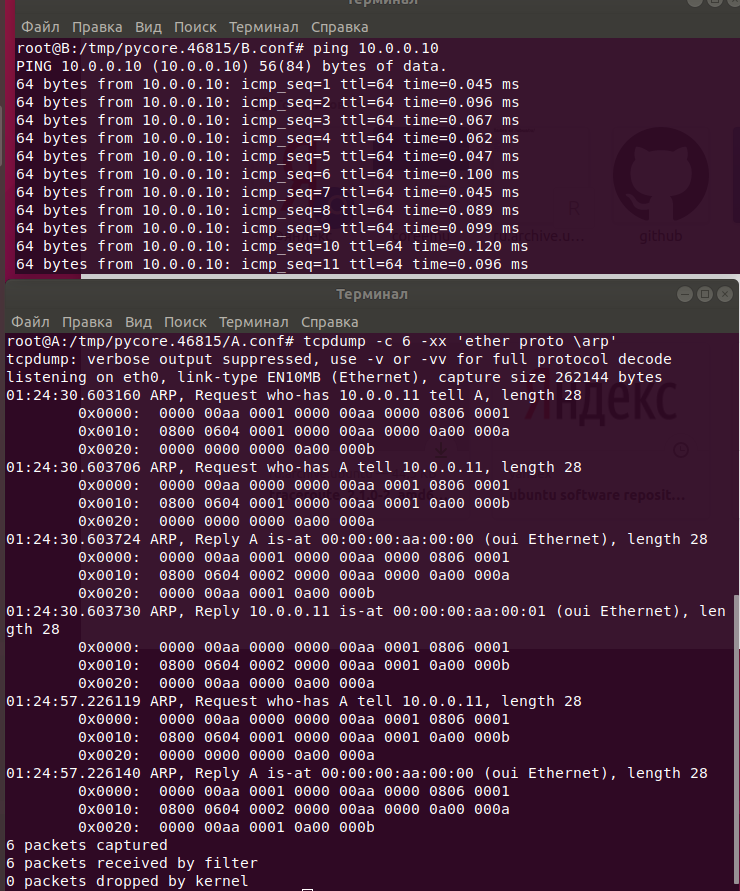
6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP.

6.1. Запустить tcpdump таким образом, чтобы перехватывались только ARP пакеты, которые отправлены на определенный IP-адрес, чтобы он перехватывал пакеты, созданные утилитой ping. Количество захватываемых пакетов ограничить 6. Включить распечатку пакета в шестнадцатеричной системе.

- Команды, используемые в выполнении задания:

ping 10.0.10 - команда пингования компьютера А с компьютера В.

tcpdump -c 6 -xx ‘ether proto \arp’ – прекратит работу после получения 6 пакетов, распечатав пакеты в шестнадцатеричном формате с заголовком канального уровня, отбирая кадры ARP протокола.



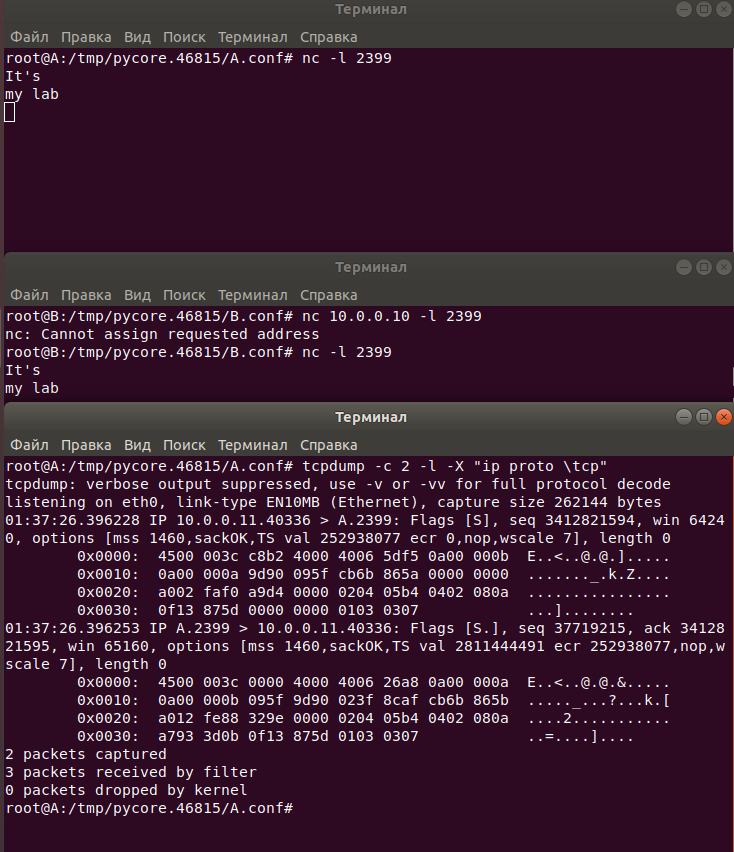
* 1. Запустить tcpdump в режиме захвата пакетов таким образом, чтобы tcpdump перехватывал только TCP пакеты. Пакеты создаем утилитой netcat (nc). Tcpdump должен отображать данные в 16-ричной системе и ASCII-формате. Количество пакетов ограничить двумя.

- Команды, используемые в выполнении задания:

nc -l 2399

nc 10.0.0.10 -l 2399

tcpdump -c 2 -l -X “ip proto \tcp” – прекратит работу после получения 2 пакетов, используя стандартный потоковый вывод пакета ASCII в hex-формате, отбирая все пакеты IP, содержащие TCP.

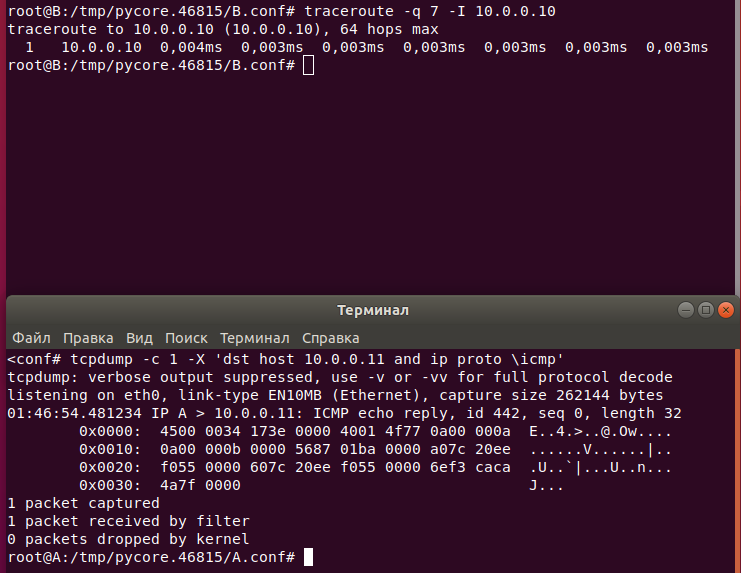


* 1. Запустить tcpdump так, чтобы он перехватывал только ICMP, которые отправлены на определенный IP-адрес, чтобы он перехватывал пакеты, созданные утилитой traceroute. Также, включить распечатку пакета в шестнадцатеричной системе и ASCII-формате. Заголовок канального уровня не включать. Количество захватываемых пакетов – 1. Количество созданных пакетов – 7.

- Команды, используемые в выполнении задания:

traceroute -q 7 -I 10.0.0.10

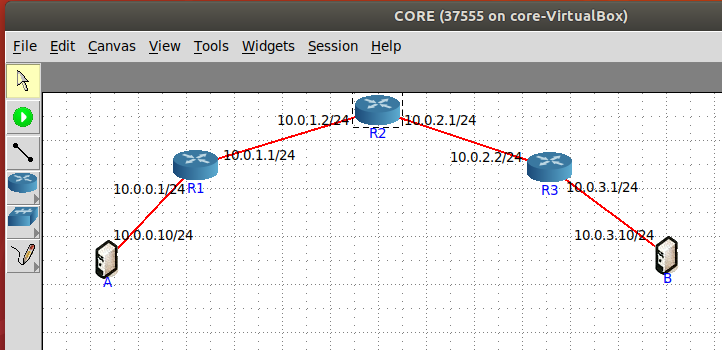
tcpdump -c 1 -X ‘dst host 10.0.0.11 and ip proto \icmp’



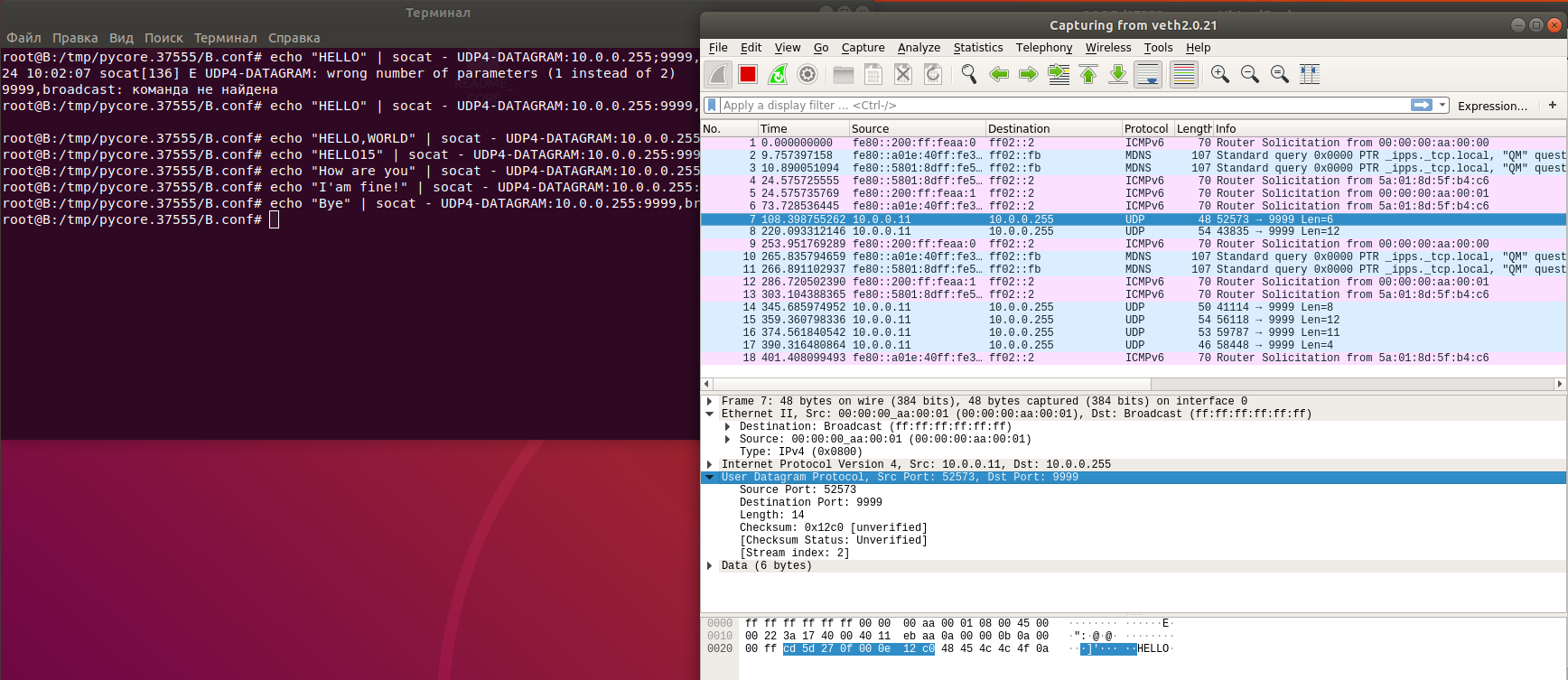
**wireshark**

1. Подготовительный этап.

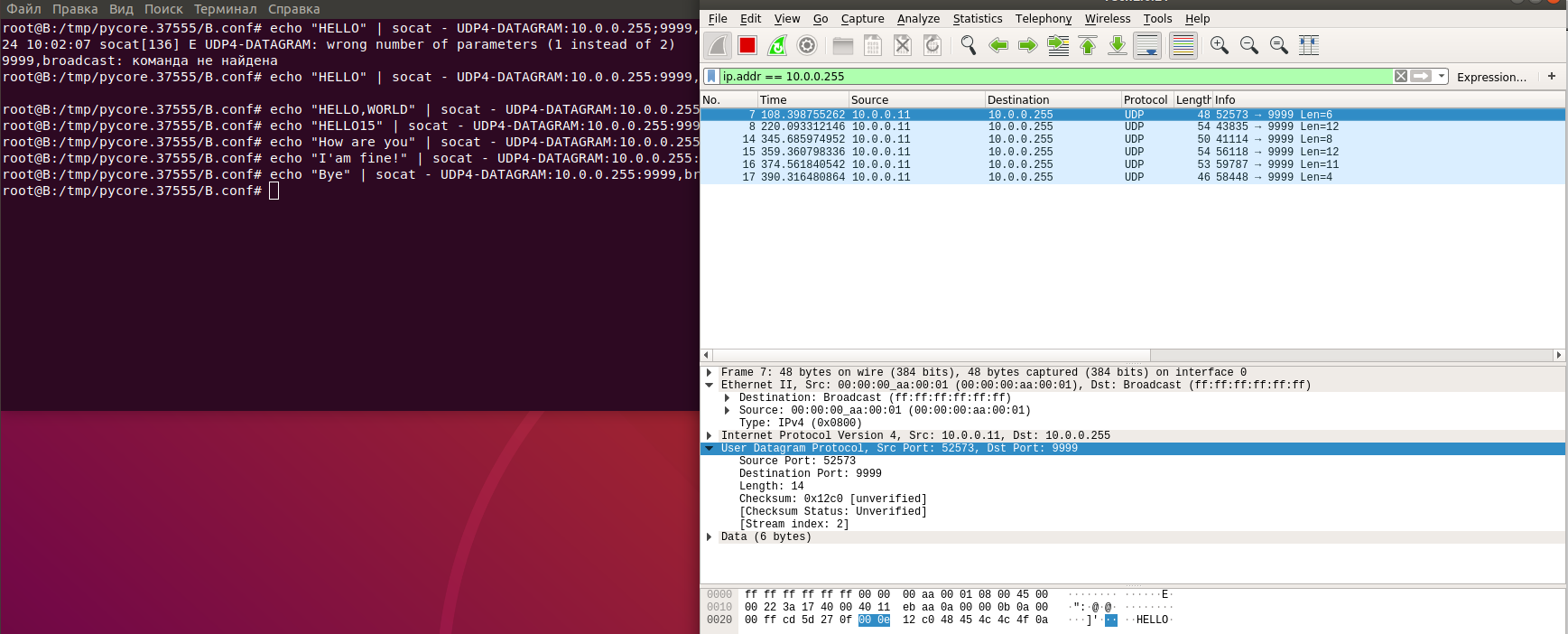
Схема для третьего задания.



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



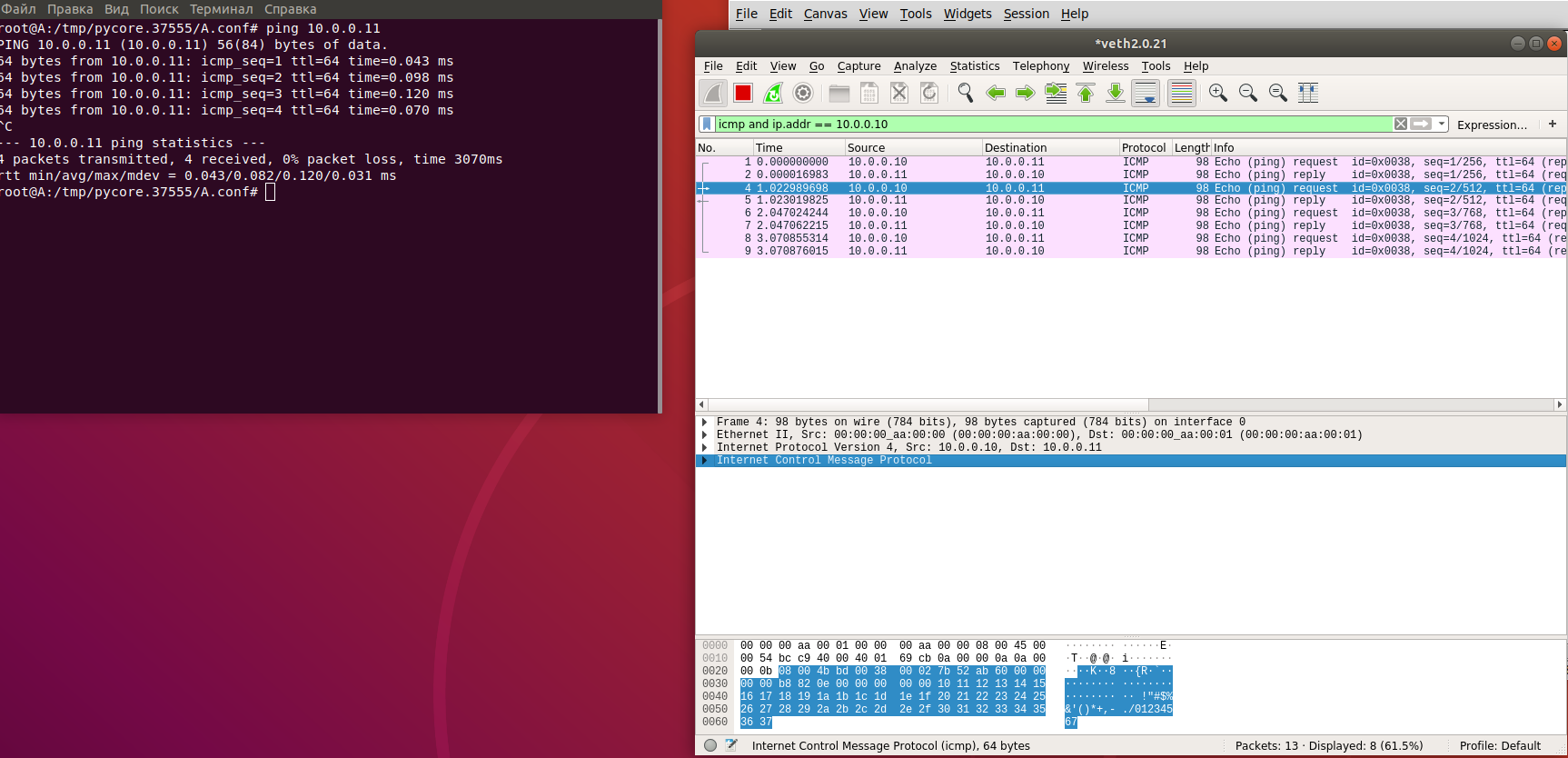
С фильтром по IP-адресу (ip.addr == 10.0.0.255).



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

С фильтром узла и протокола (icmp and ip.addr == 10.0.0.10).

Если вместо addr написать src, то в wireshark отобразятся только запросы.



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.

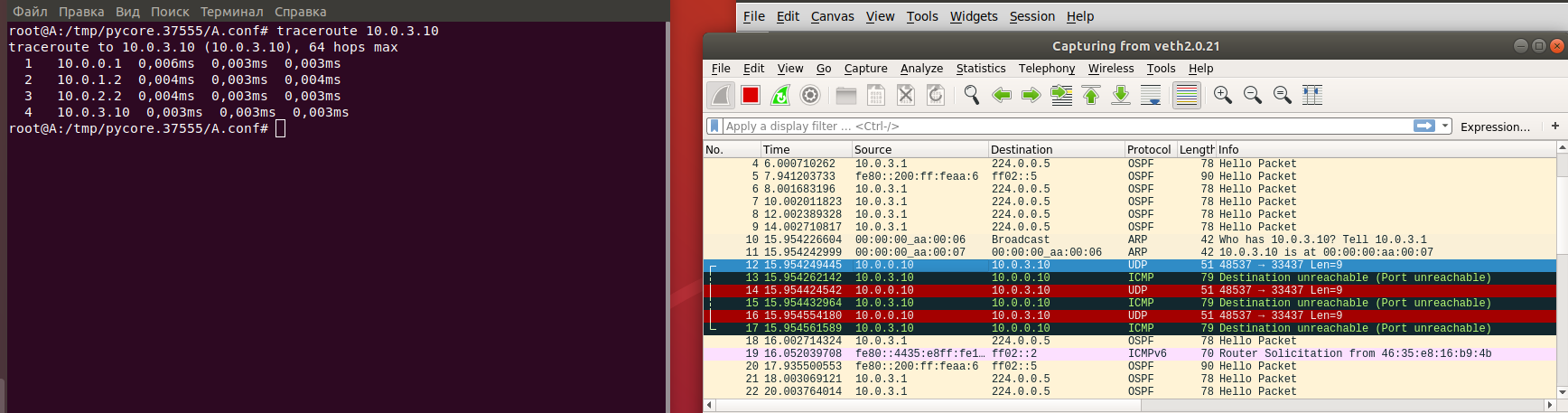
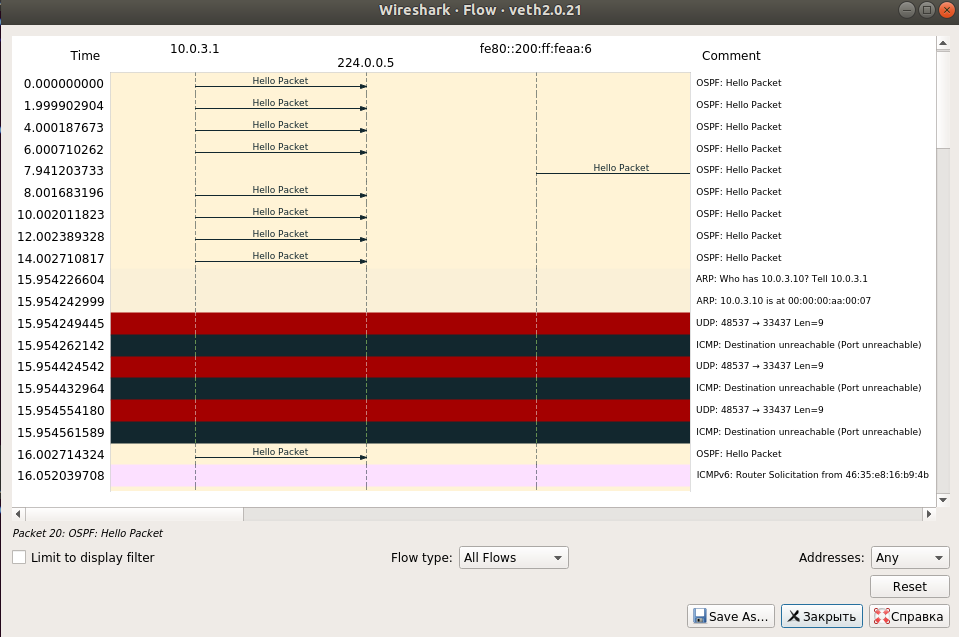
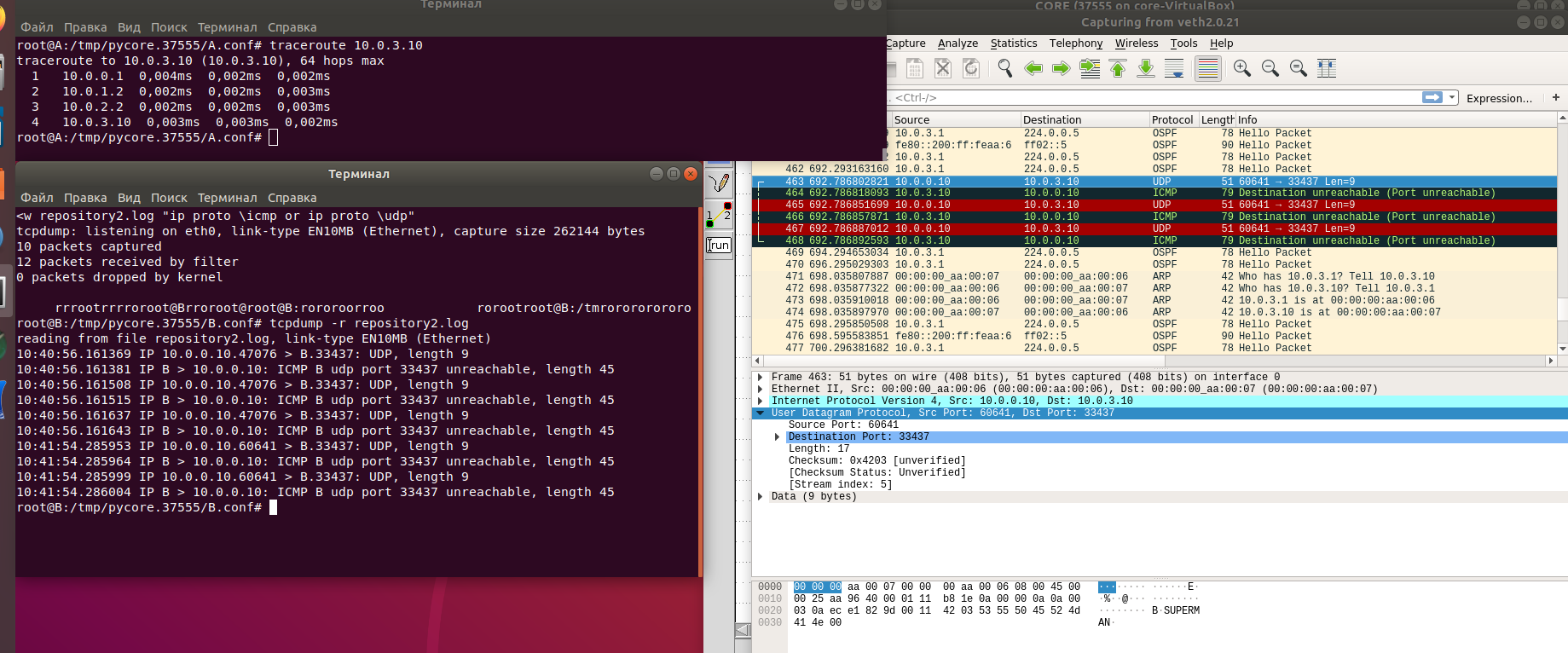


Диаграмма Flow Graph.



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



**Вывод:** в ходе данной лабораторной работы мы углубились в работу с tcpdump, traceroute, wireshark. Научились фильтровать выводимые строки wireshark и фильтровать выводимые данные tcpdump. В ходе сравнение мы выяснили, что wireshark более богат на информацию, нежели traceroute, так как при traceroute мы применяем фильтры.