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 №1

Выполнил: Пестов А.А.

18-В-2

Проверил: Гай В.Е.

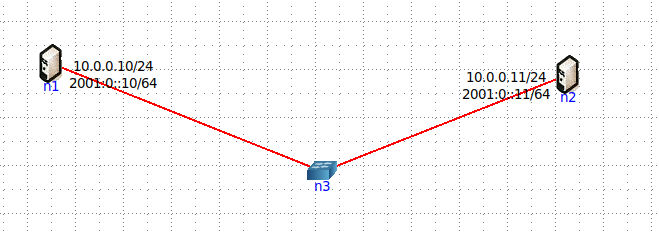
Нижний Новгород

2021

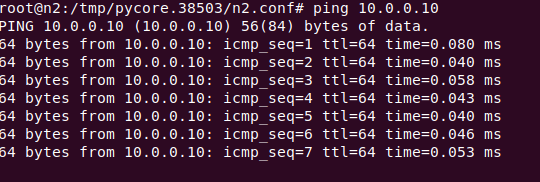
**Работа с анализатором протоколов tcpdump:**

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

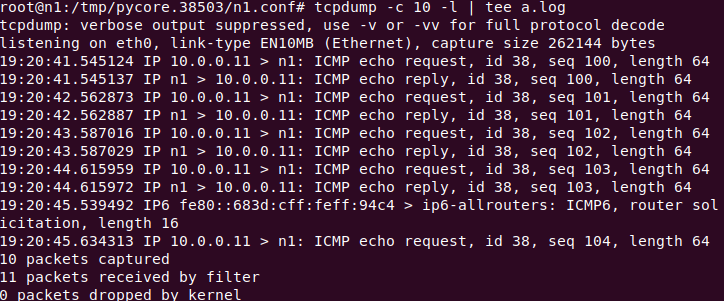
Создадим сеть:



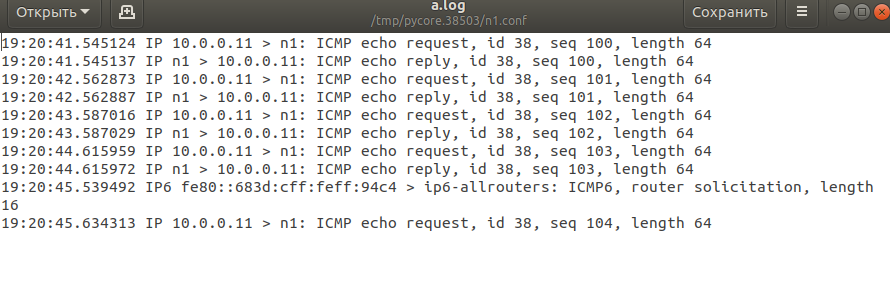
Передадим пакеты с хоста n2 на n1:



На n1 запустим tcpdump:

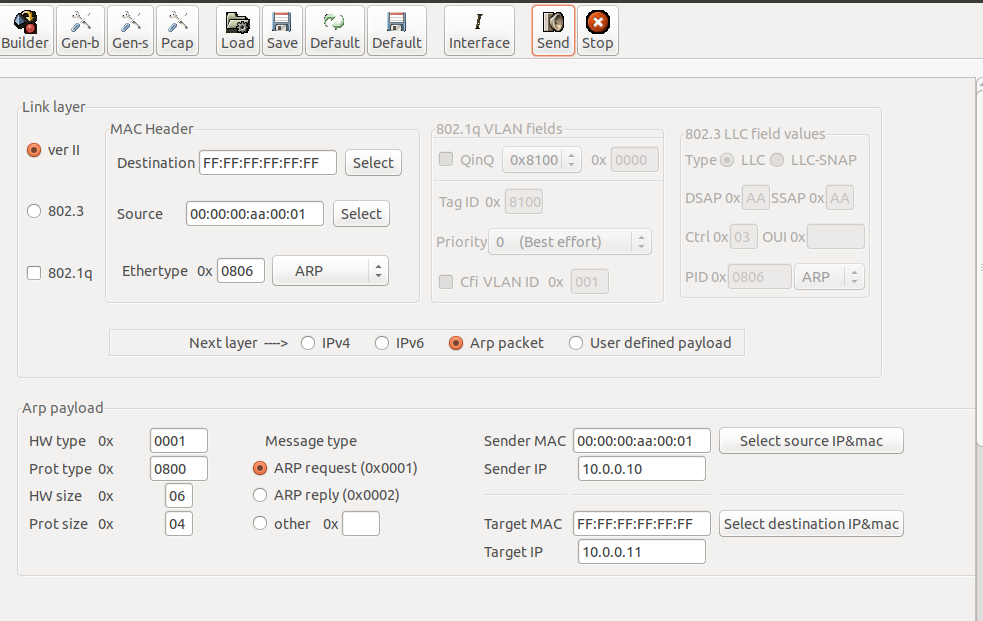


Откроем logfile a.log:

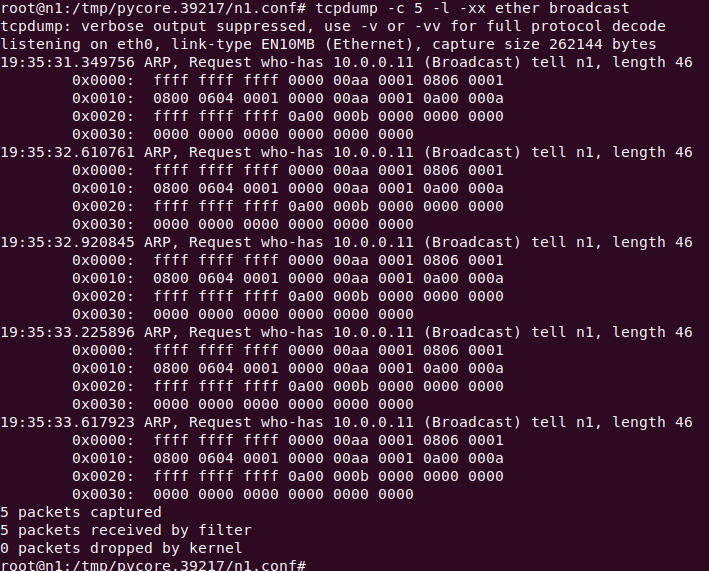


1. **Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).**

Составляем широковещательный MAC-пакет на хосте n2 с помощью PackETH:

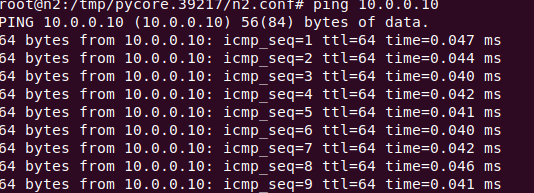


На хосте n1 запускаем tcpdump и совершаем широковещательную рассылку (send) в PackETH:

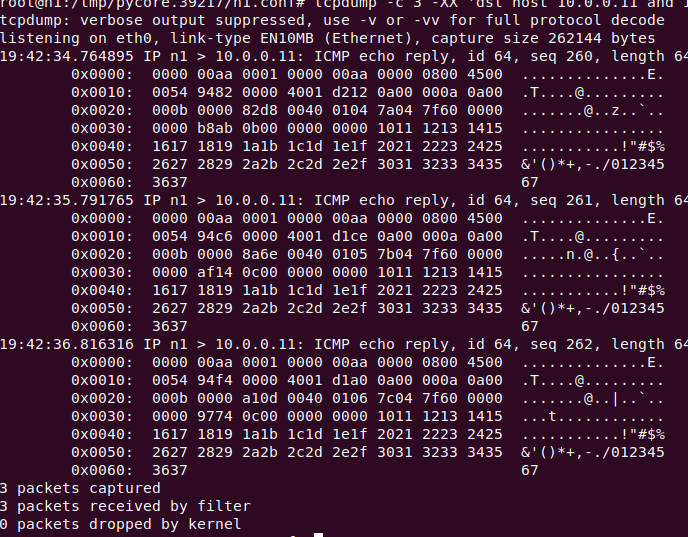


**3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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

Передаем пакеты с хоста n2 на n1:

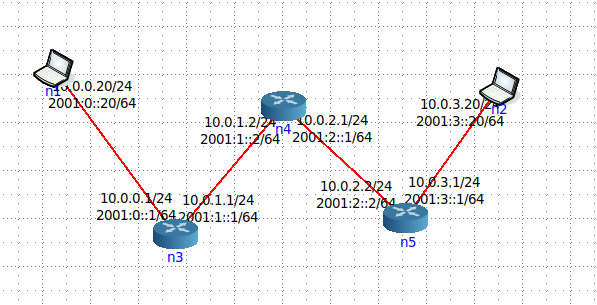


Запускаем tcpdump на хосте n1:



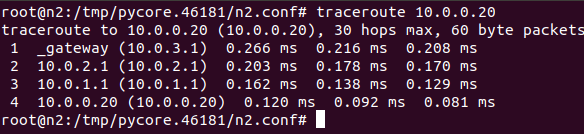
4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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

Увеличим структуру сети:

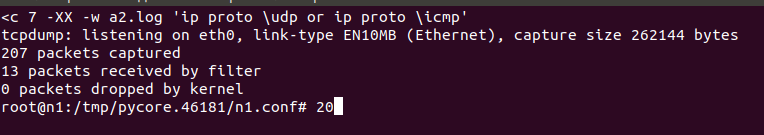


Запустим tcpdump на хосте n1 с нужными параметрами, фильтрами и одновременно передадим пакеты с хоста n2 с помощью утилиты traceroute:

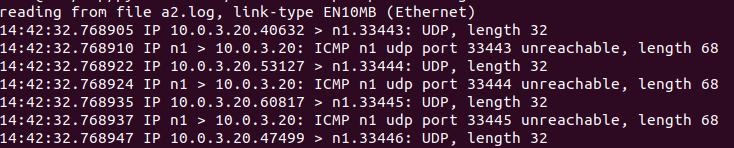
Запускаем traceroute:



Запускаем tcpdump:



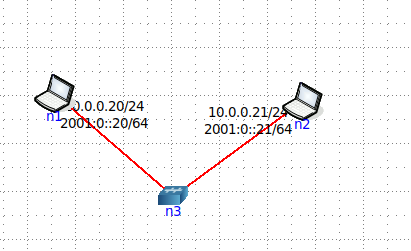
Открываем в консоли logfile a2.log:



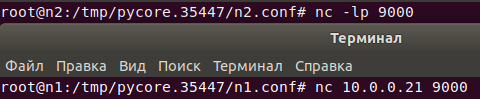
**6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP**

1. Захватить 4 пакета протокола TCP, отправленных с определенного MAC-адреса. Выводить все пакеты в формате ASCII.

Создадим сеть:



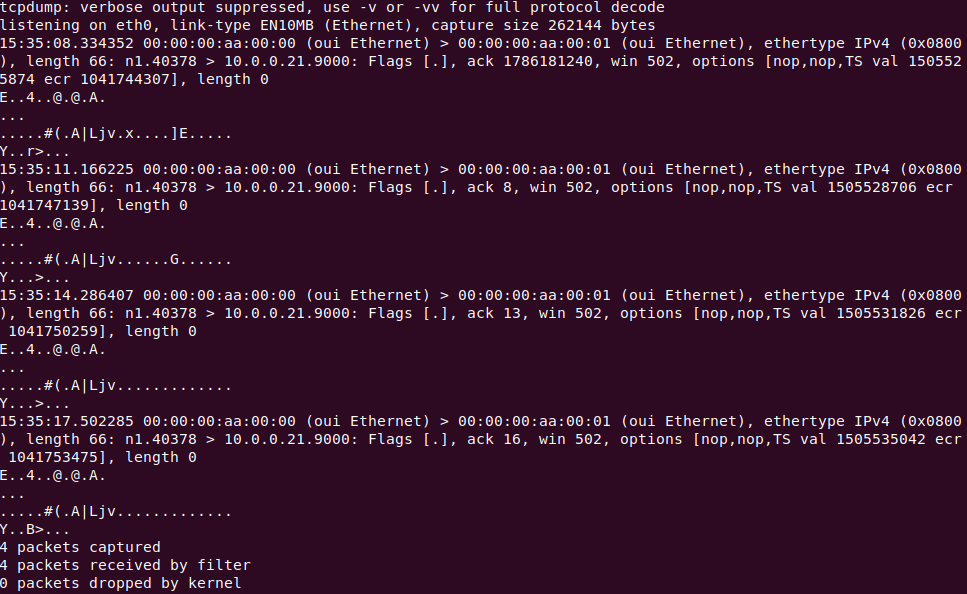
Создадим чат между двумя узлами:



Запустим tcpdump на 1 компьютере:

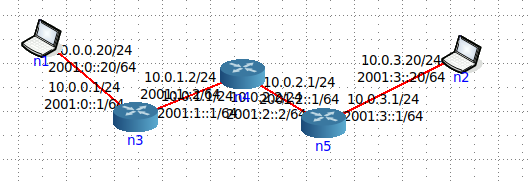


Результат:

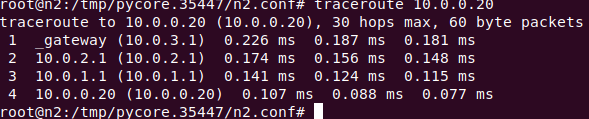


1. Захватить 5 пакетов протокола UDP, отправленных с определенного IP-адреса на определенный MAC-адрес. Результаты протоколировать в файл. Для генерирования пакетов воспользоваться утилитой traceroute.

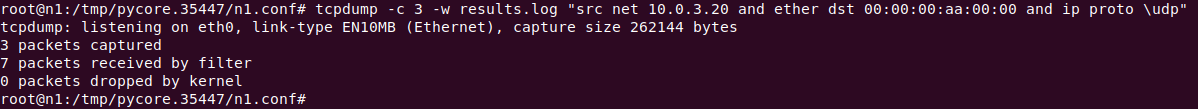
Сеть:



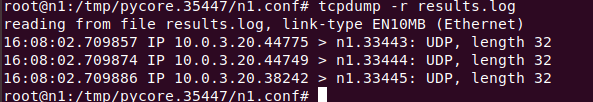
Traceroute:



Tcpdump:

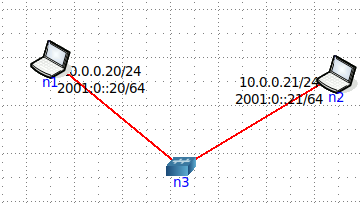


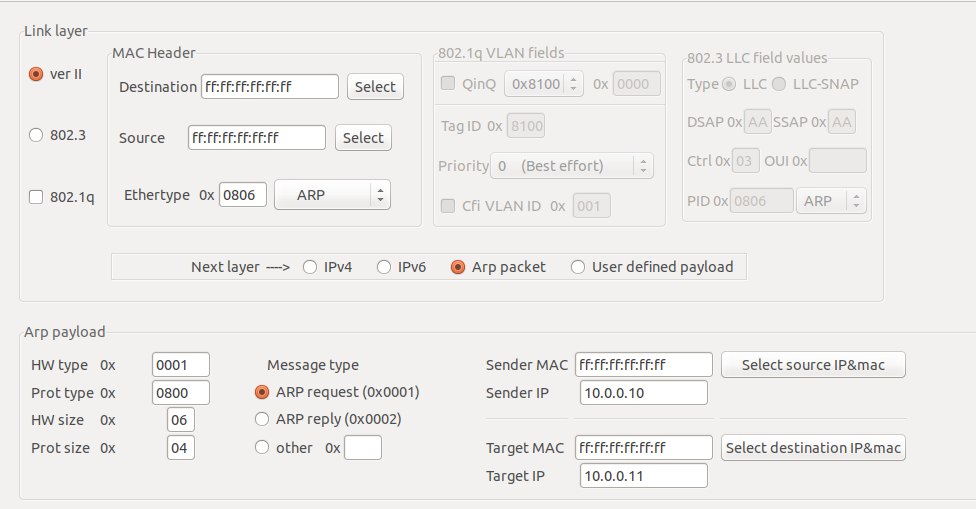
Logfile:



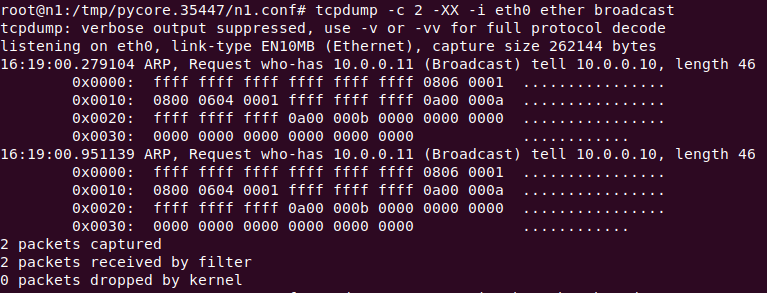
1. Запустить tcpdump в режиме перехвата широковещательного трафика через интерфейс eth0. Количество захватываемых пакетов ограничить 2. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня).

Создадим сеть:





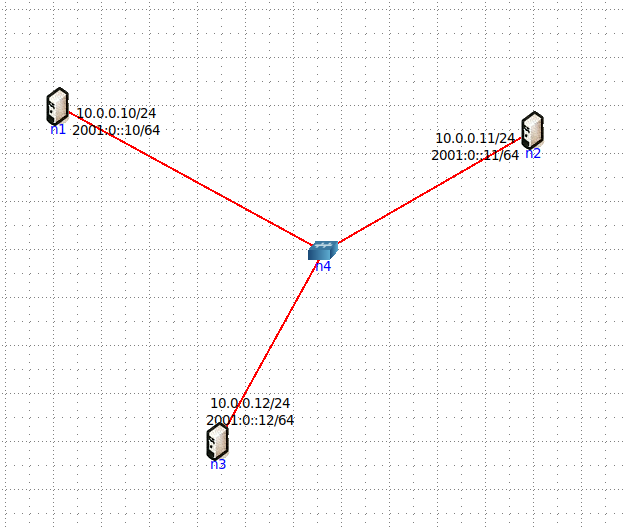
Tcpdump:



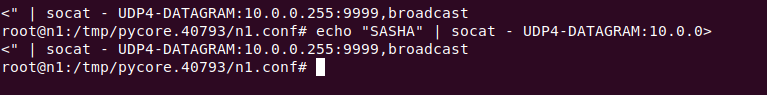
**Работа с анализатором протоколов wireshark**

1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл. Отобразить данные канального уровня и включить распечатку пакета в шестнадцатеричной системе.

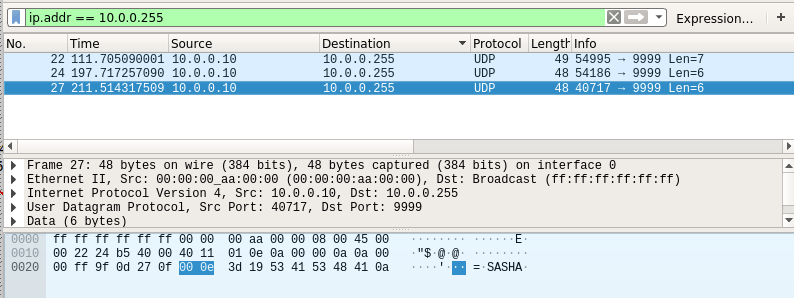
Создадим сеть:



Создаем широковещательный трафик на хосте n1:

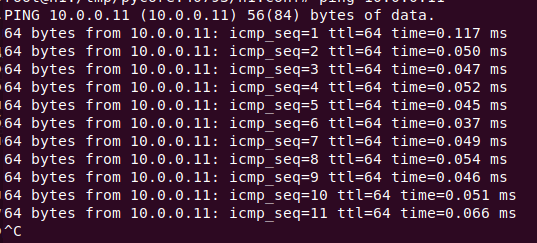


Захват пакетов с помощью Wireshark (фильтр по IP-адресу):

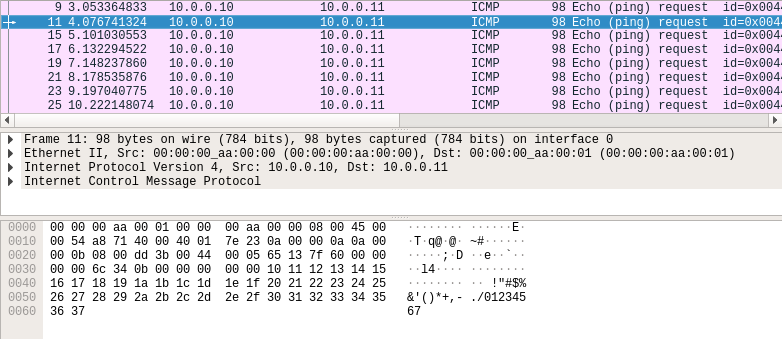


**2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.**

Передаем пакеты из хоста n1 в n2:

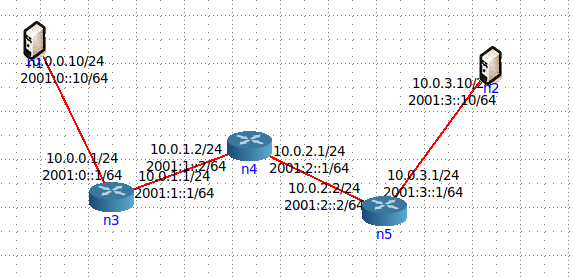


Захват пакетов с помощью Wireshark на хосте n2 (фильтр по протоколу ICMP и IP-адресу отправителя):

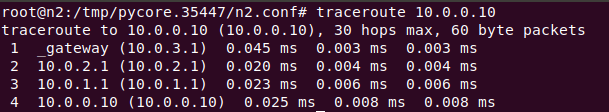


**3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла, либо в виде изображения.**

Создадим сеть:



Передадим пакеты при помощи утилиты traceroute с хоста n2:



Захват пакетов с помощью Wireshark на хосте n1:

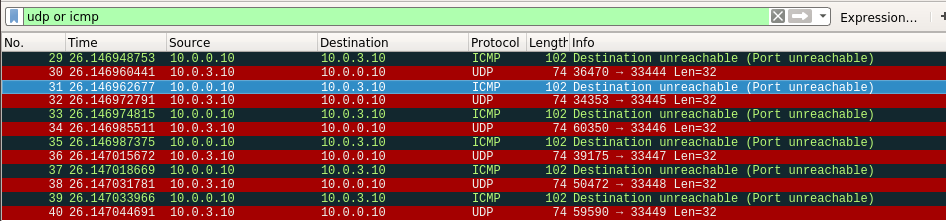
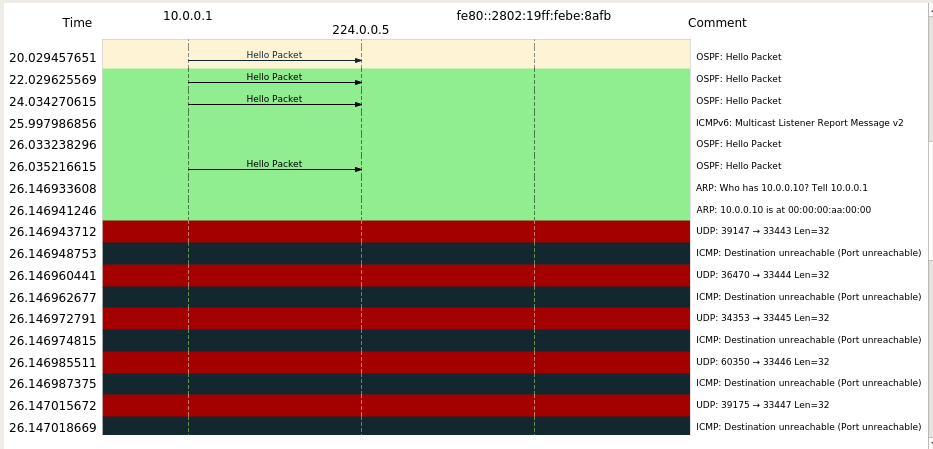
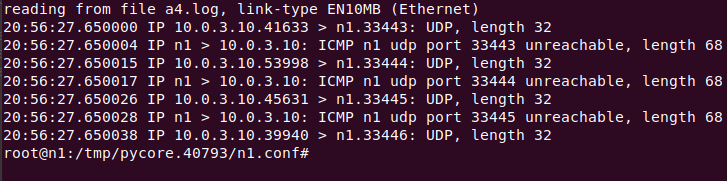


Диаграмма Flow Graph:

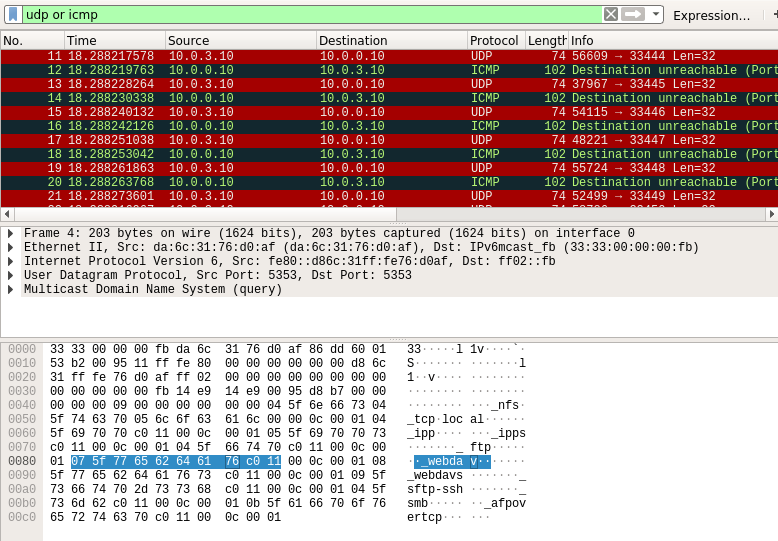


**4. Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.**

tcpdump:



Wireshark:



В wireshark мы можем более подробно изучить данные пересылаемых пакетов.