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»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к лабораторной работе №1

по дисциплине

**Сети и телекоммуникации**

РУКОВОДИТЕЛЬ:

Гай Василий Евгеньевич \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

СТУДЕНТ:

Федоров Никита Алексеевич \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

19-В-2

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

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

Нижний Новгород 2022

**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 MAC-адресу). 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. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

**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 воспользоваться 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.

**Ход работы**

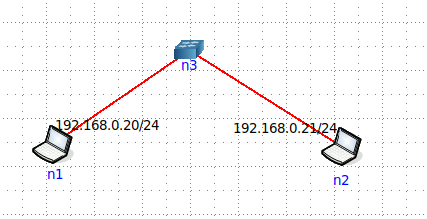


Рис.1 – Схема сети

**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.

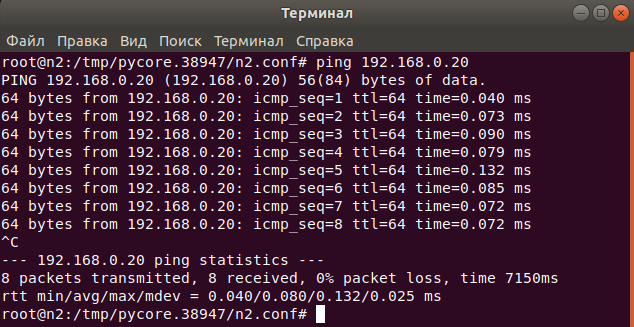


Рис.2 – Запущен ping c n2 на n1

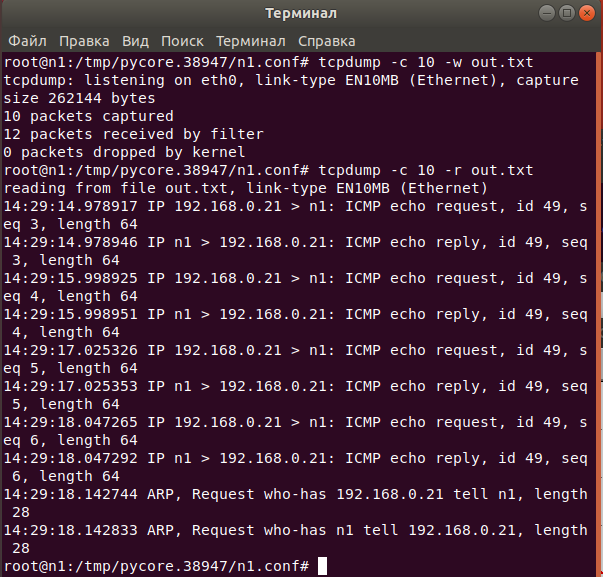


Рис.3 – Запущен захват с помощью tcpdump на n1

2. 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).

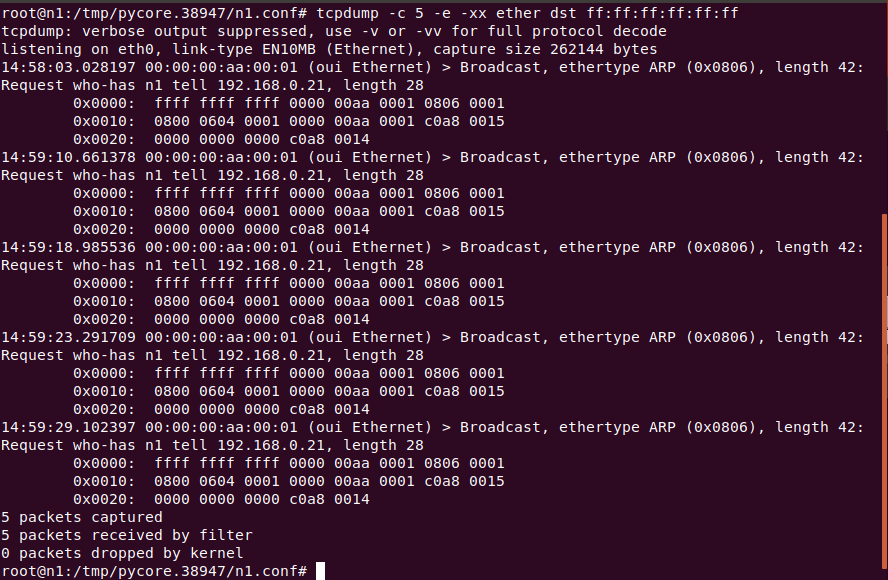


Рис.4 – Запущен захват arp-трафика с помощью tcpdump на n1

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.

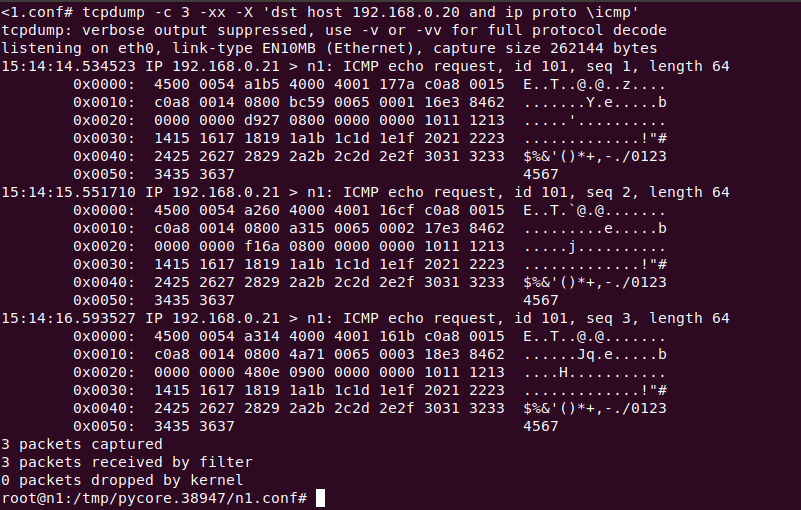


Рис.5 – Запущен захват пакетов ICMP на IP n1 с помощью tcpdump на n1

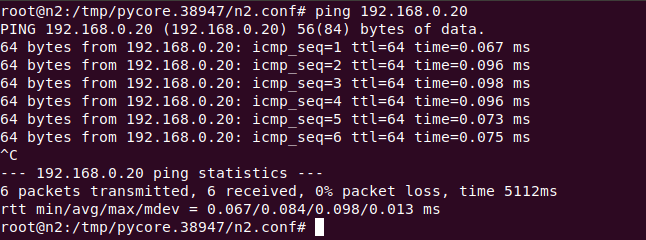


Рис.6 – Запущен ping на n2

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.

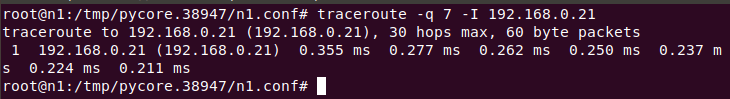


Рис.7 – Запущена трассировка с n1

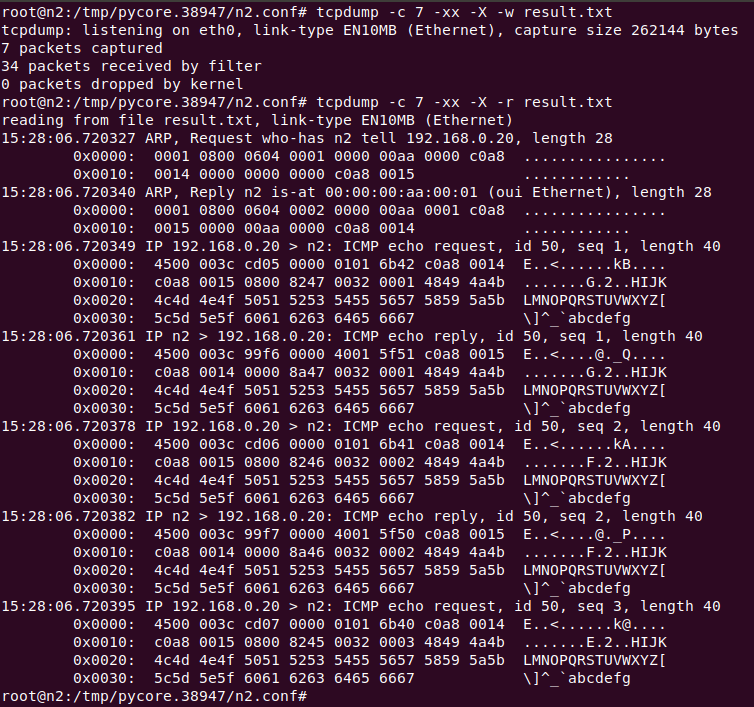


Рис.8 – Запущена трассировка с n1

5. Прочесть программой tcpdump созданный в предыдущем пункте файл.

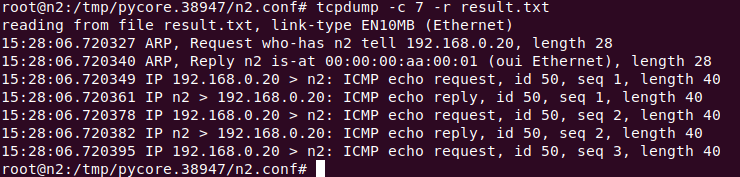


Рис.9 – Чтение результатов

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

1)Запустить tcpdump так, чтобы он перехватывал только пакеты протокола UDP, отправленные c определенного IP-адреса. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество захватываемых пакетов ограничить до 3.

Для генерирования пакетов воспользоваться утилитой traceroute.

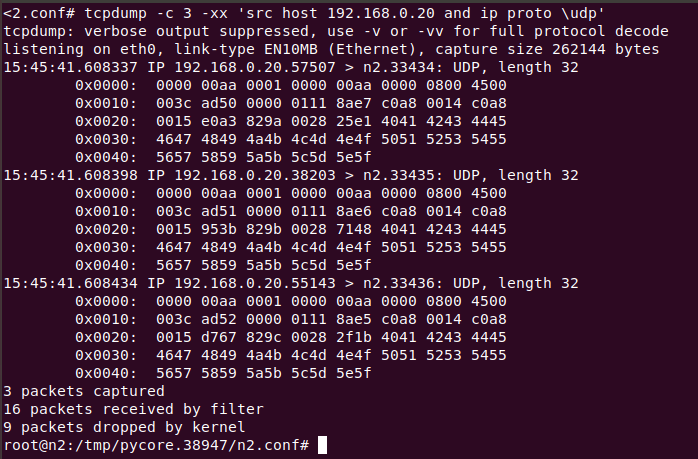


Рис.10 – Запущен захват 3 пакетов протокола UDP

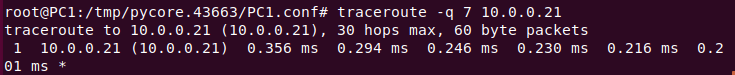


Рис.11 – Запущена трассировка до n2

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 ограничить 4. Для генерирования пакетов воспользоваться утилитой ping.

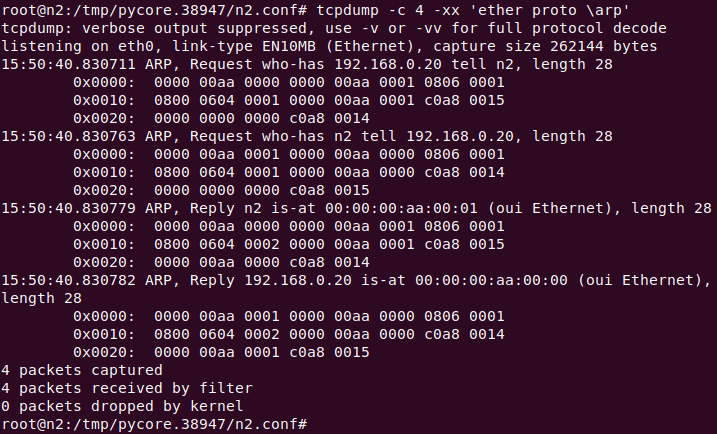


Рис.12 – Запущен захват на n1 4 пакетов ARP протокола

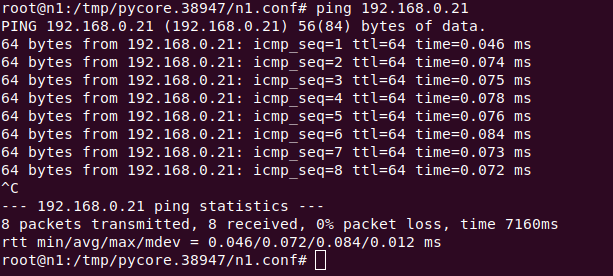


Рис.13 – Запущен пинг n2

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

Для генерирования пакетов воспользоваться утилитой traceroute.

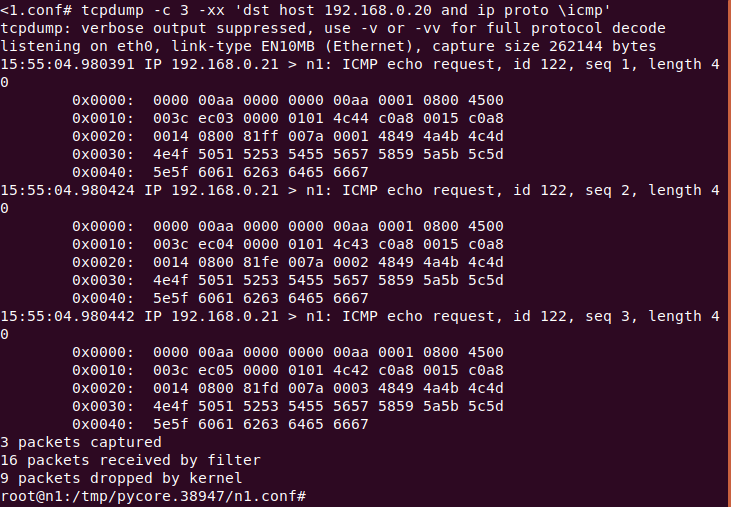


Рис.14 – Запущен захват пакетов на ip адрес n1 по протоколу ICMP

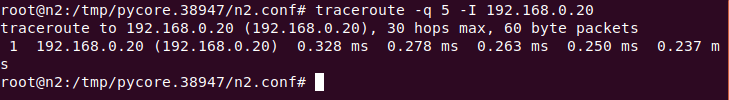


Рис.15 – Запущен пинг n1

**Работа с анализатором протоколов wireshark**

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

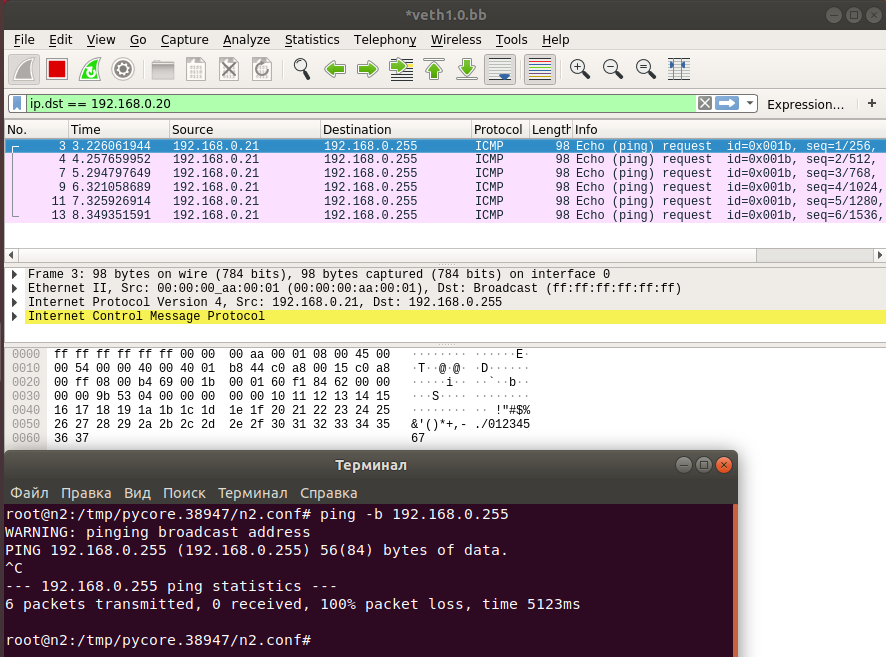


Рис.16 – Захват и фильтр по конечному ip, широковещательный ICMP трафик с n2

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

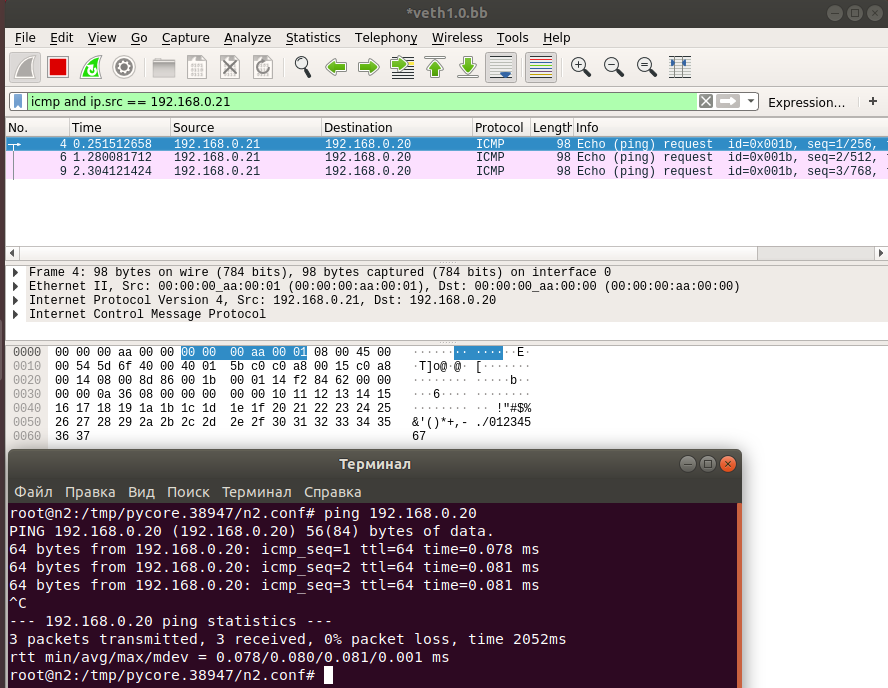


Рис.17 – Захват и фильтр по ip источника, пинг с n2 на n1

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.

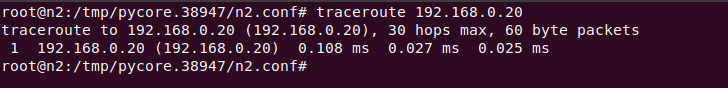


Рис.18 – Запуск трассировки с n2 на n1

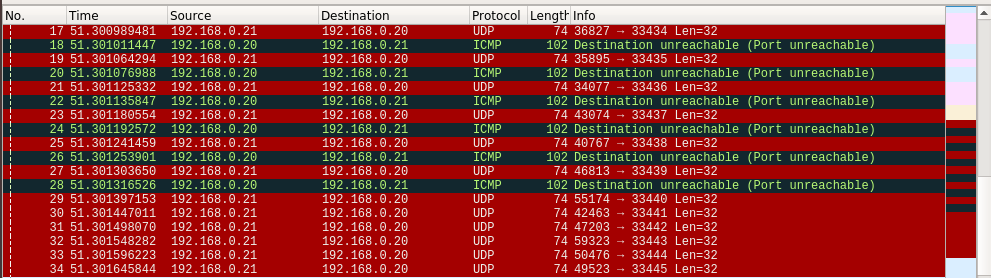


Рис.19 – Результат захвата пакетов в Wireshark

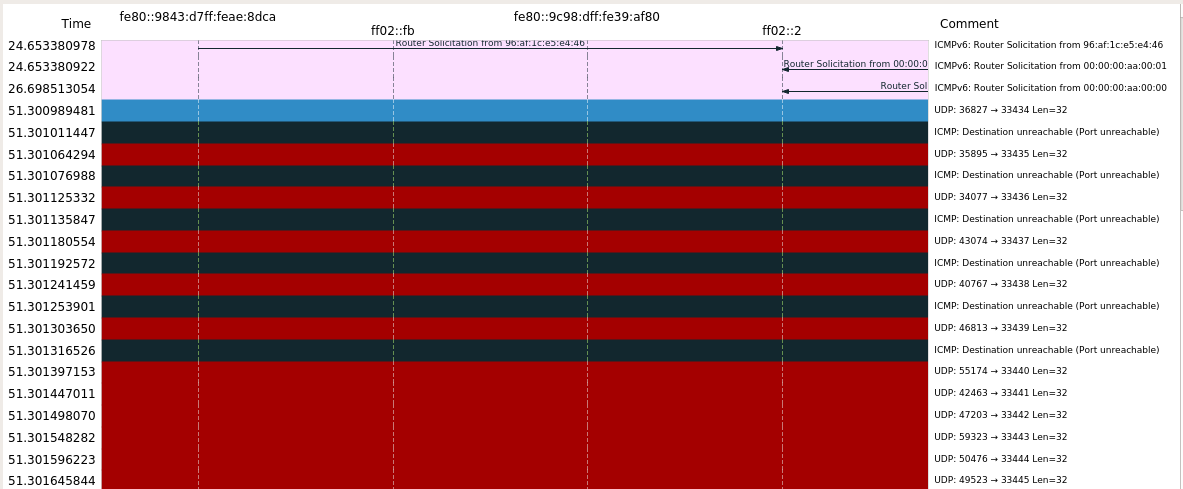


Рис.20 – Диаграмма Flow Graph

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

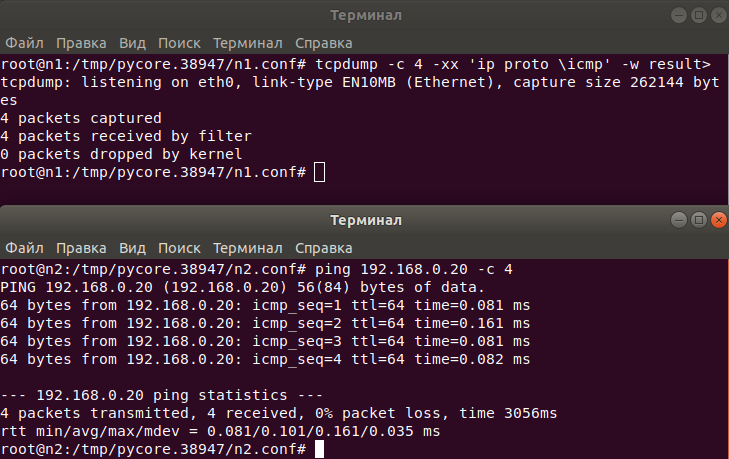


Рис.21 – На n1 запущен захват 4 пакетов ICMP с сохранением их в файл result.cap, на n2 – отправка 4 ICMP пакетов хосту n1

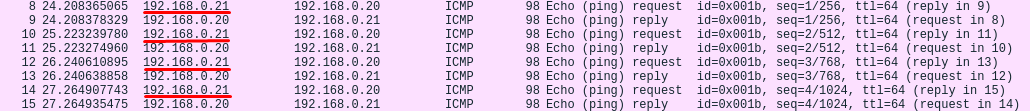


Рис.22 – Результат захвата в Wireshark

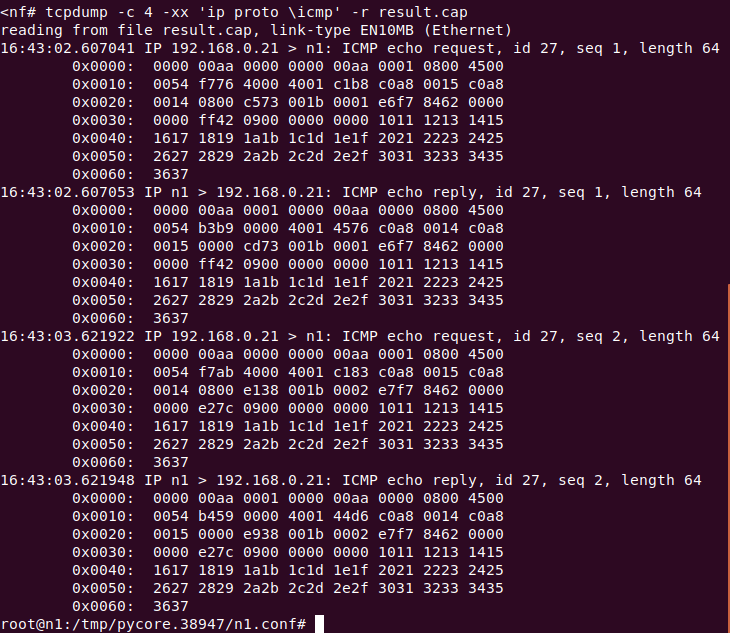


Рис.23 – Чтение результатов захвата с помощью tcpdump – захвачены первые 4 пакета в соответствии с фильтром