МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

ОТЧЕТ

по лабораторной работе №1

«Работа с анализатором протоколов tcpdump и wireshark»

по дисциплине

«Сети и телекоммуникации»

РУКОВОДИТЕЛЬ:

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

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_ Кабальцев Н.Д

(подпись) (фамилия, и.,о.)

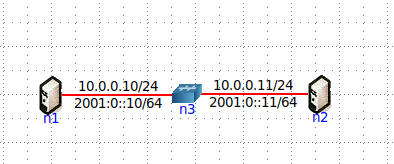
\_\_\_\_\_\_19-В-2\_\_\_\_\_\_\_\_

(шифр группы)

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

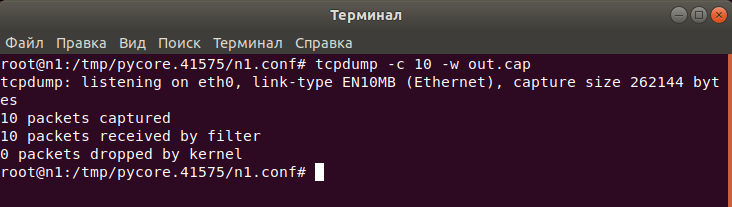
С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

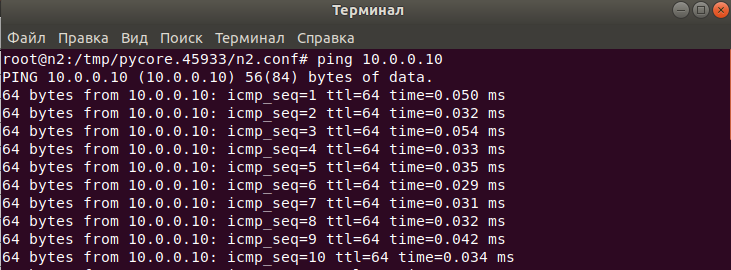
Нижний Новгород 2022



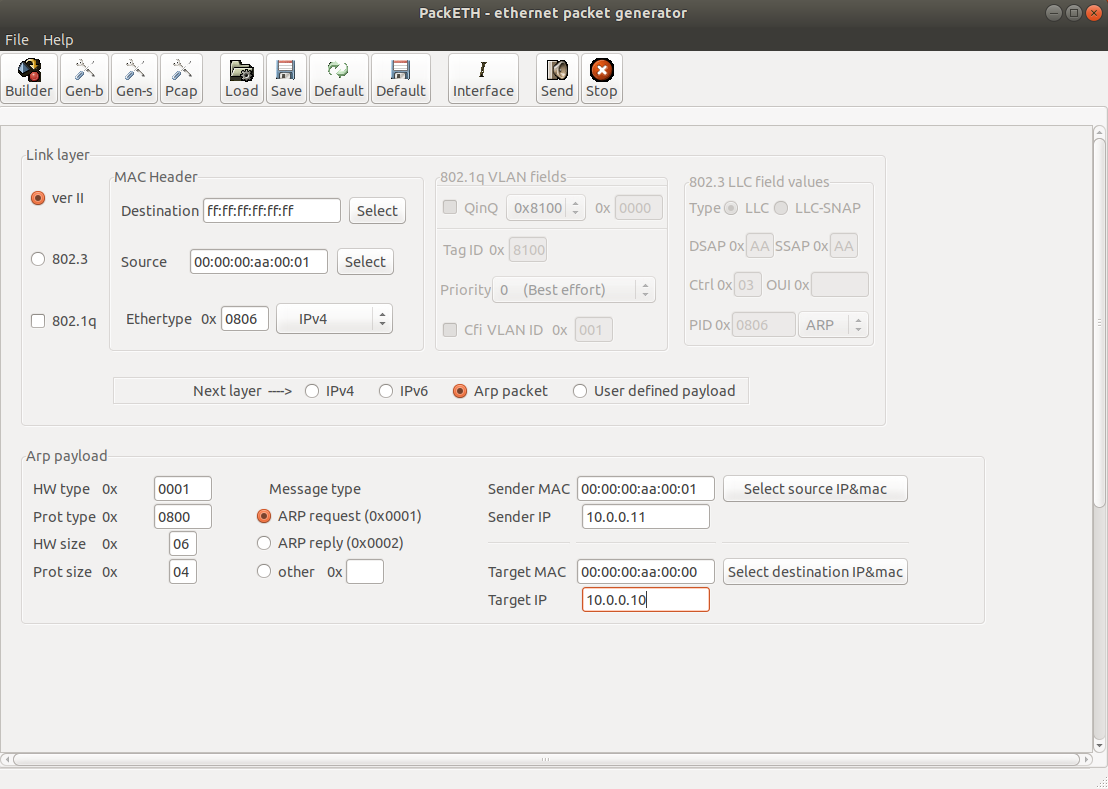
**Работа с анализатором протоколов tcpdump**

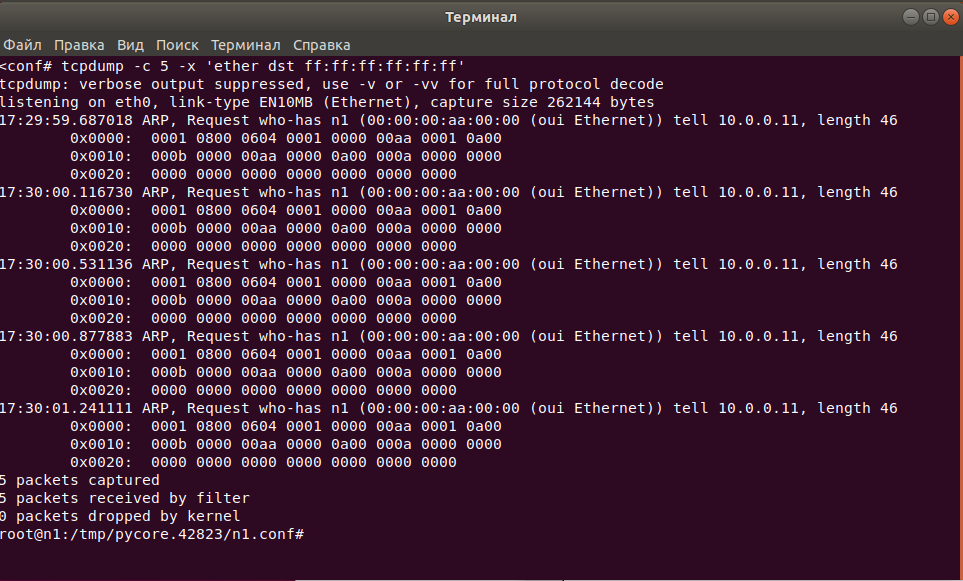
1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.



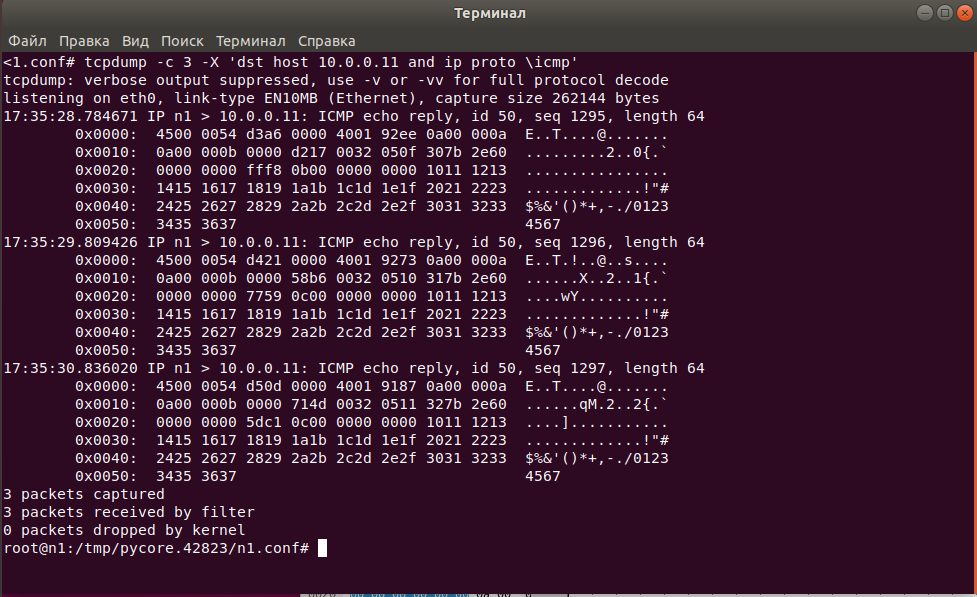


2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе.

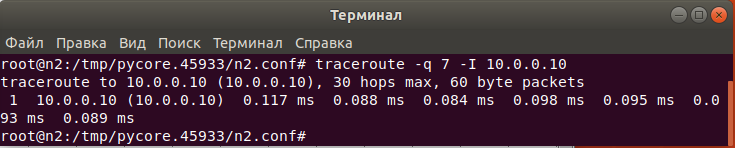


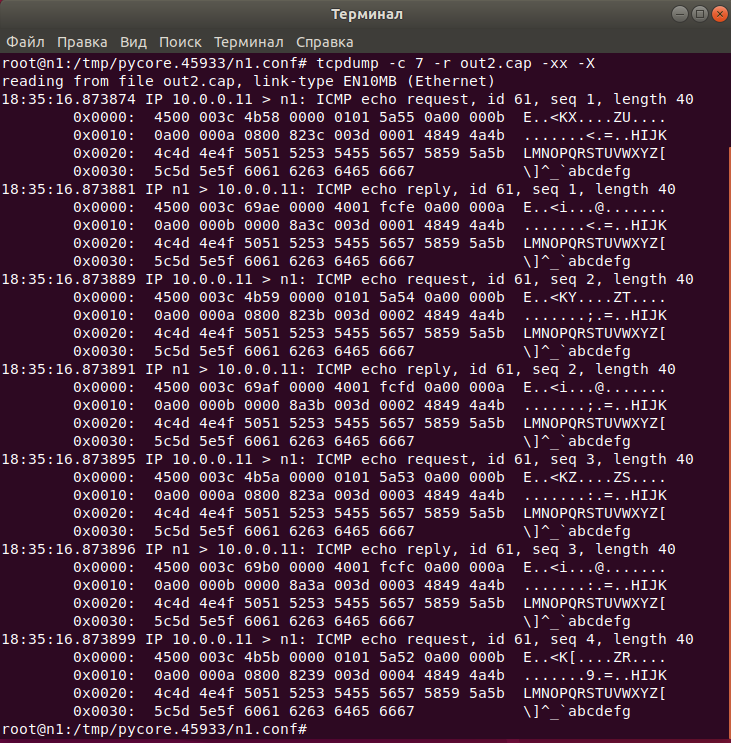


3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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

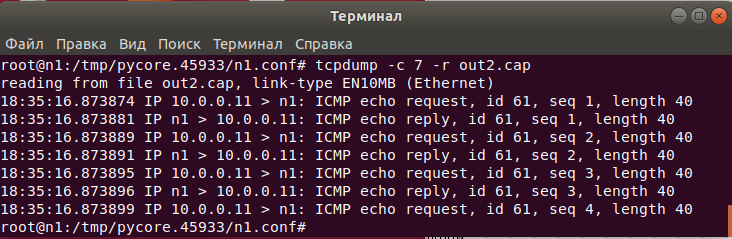


4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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



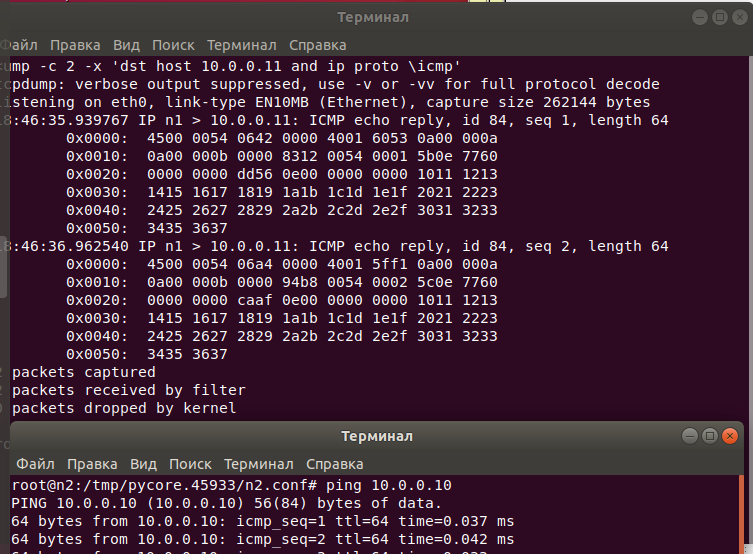


5. Прочесть программой tcpdump созданный в предыдущем пункте файл.



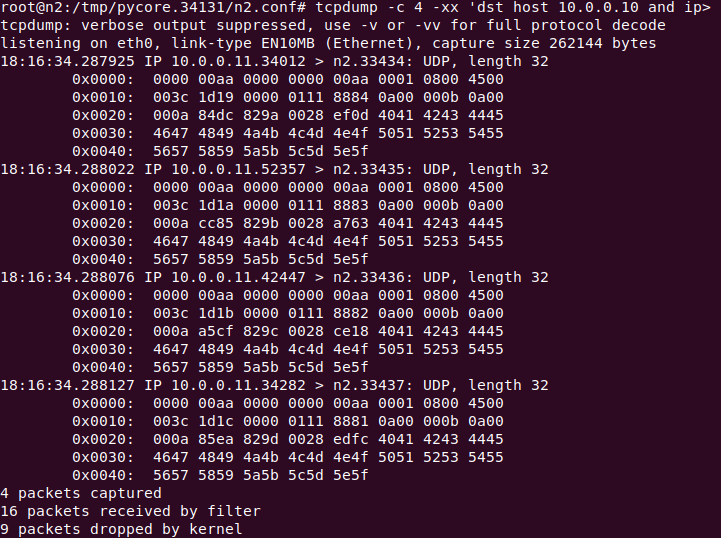
6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

1)Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес, чтобы он перехватывал пакеты, созданные утилитой ping. Включить распечатку пакета в шестнадцатеричной системе. Количество захватываемых пакетов ограничить 2.

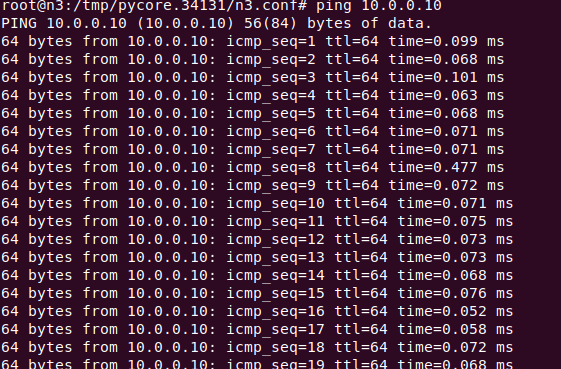


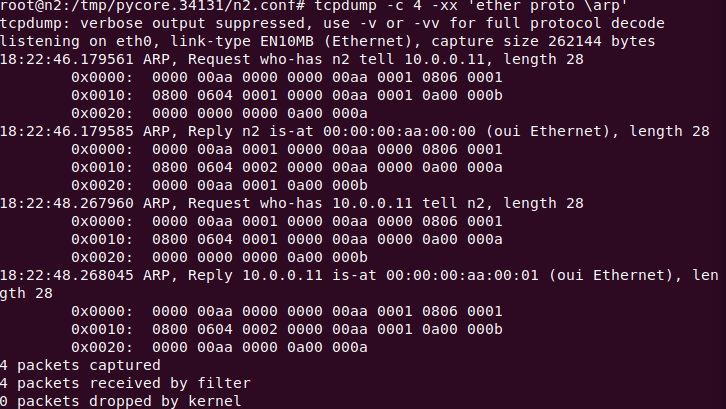
2) Запустить tcpdump так, чтобы он перехватывал только пакеты протокола UDP, отправленные наопределенный IP-адрес, чтобы он перехватывал пакеты, созданные утилитой traceroute. Включить распечатку пакета в шестнадцатеричной системе( включая заголовок канального уровня). Количество захватываемых пакетов ограничить 4.





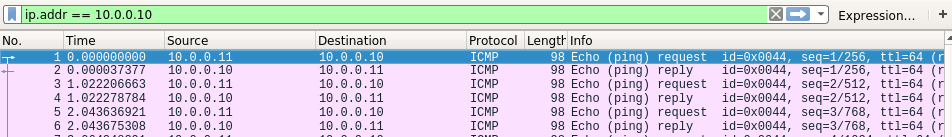
3) Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ARP, отправленные наопределенный IP-адрес, чтобы он перехватывал пакеты, созданные утилитой ping. Включить распечатку пакета в шестнадцатеричной системе( включая заголовок канального уровня). Количество захватываемых пакетов ограничить 4.



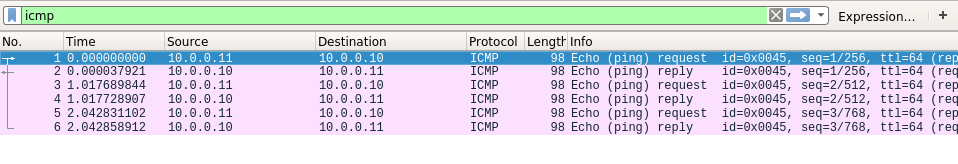


**Работа с анализатором протоколов wireshark**

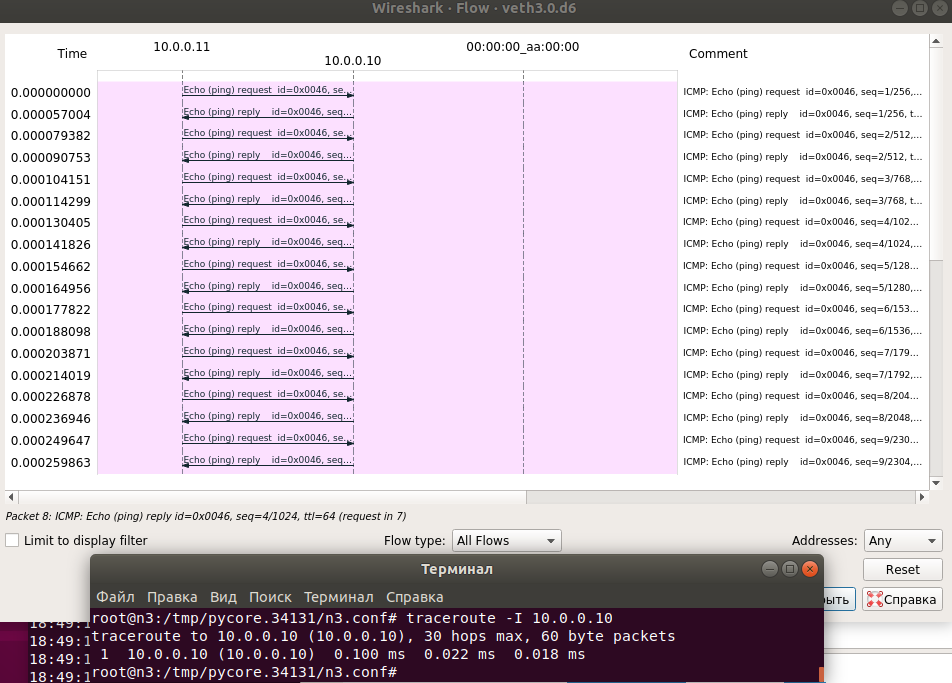
1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.



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 FlowGraph. 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.

