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

**Отчёт**  
**по лабораторной работе № 1**

**Получение базовых навыков работы с анализаторами протоколов tcpdump и wireshark.**

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

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

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Мосташов В.С.

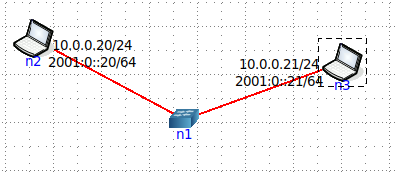
19-В-2

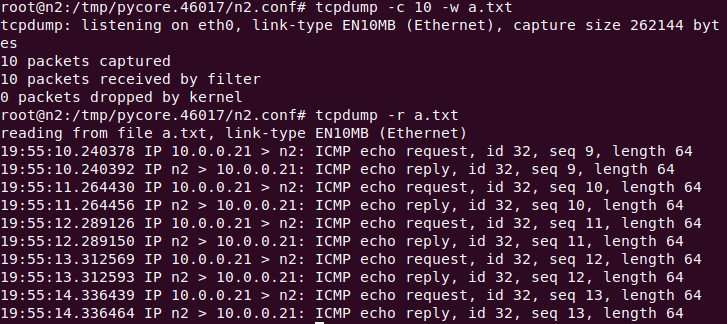
Нижний Новгород 2022

**Работа с анализатором протоколов tcpdump**

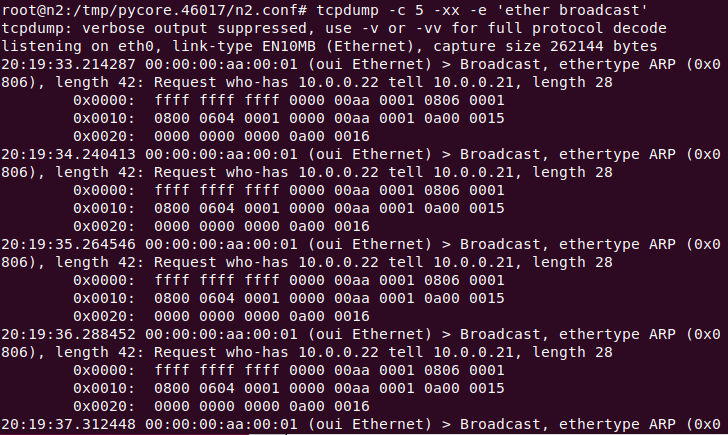
1) Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

Составленная схема:

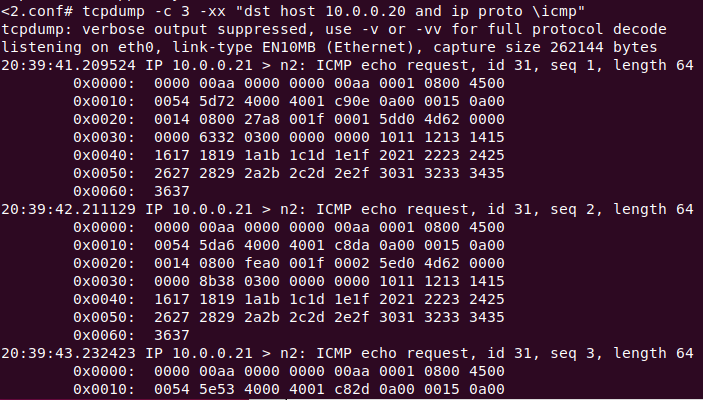
****

****

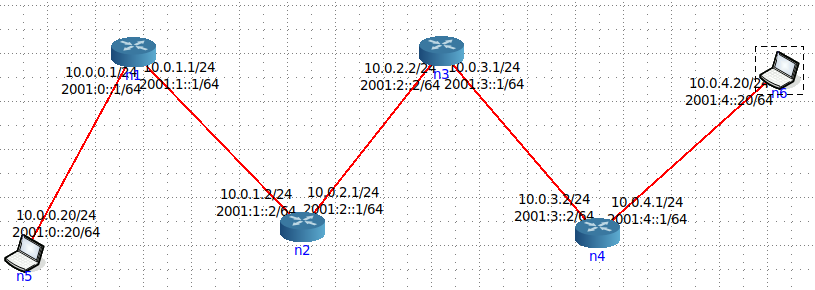
2) Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

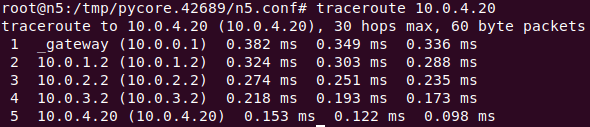
****

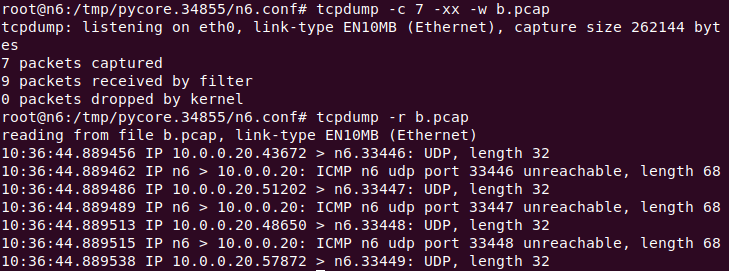
3) Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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

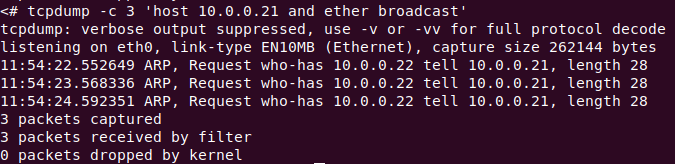




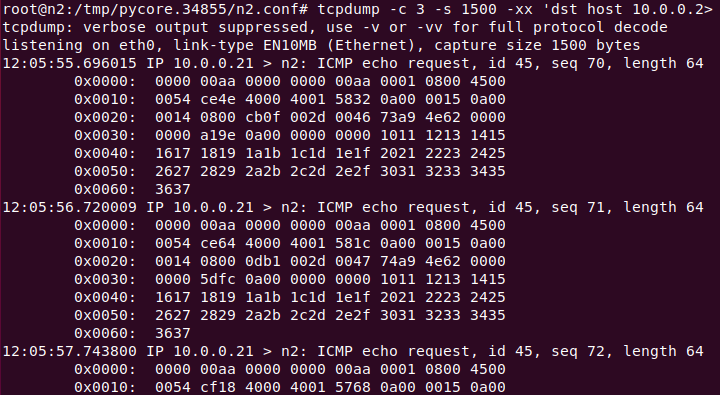


5) Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

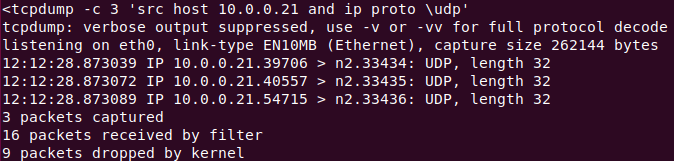
Захват 3 широковещательных пакетов, отправленных с 10.0.0.21:



Захват 3 пакетов ICMP. Отображение пакетов в шестнадцатеричном виде с заголовком канального уровня. Размер пакета 1500 байт.

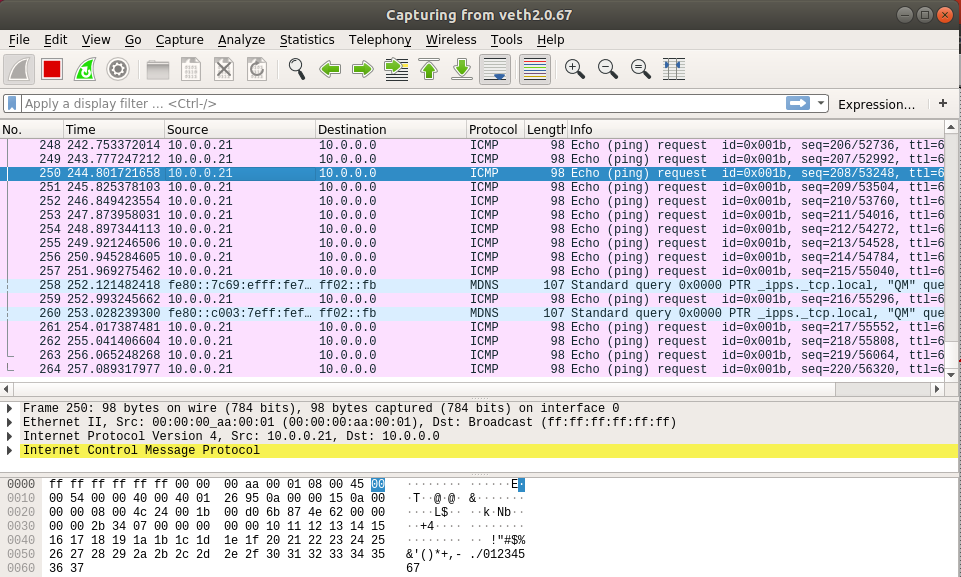


Захват 3 пакетов UDP, отправленных с адреса 10.0.0.21:

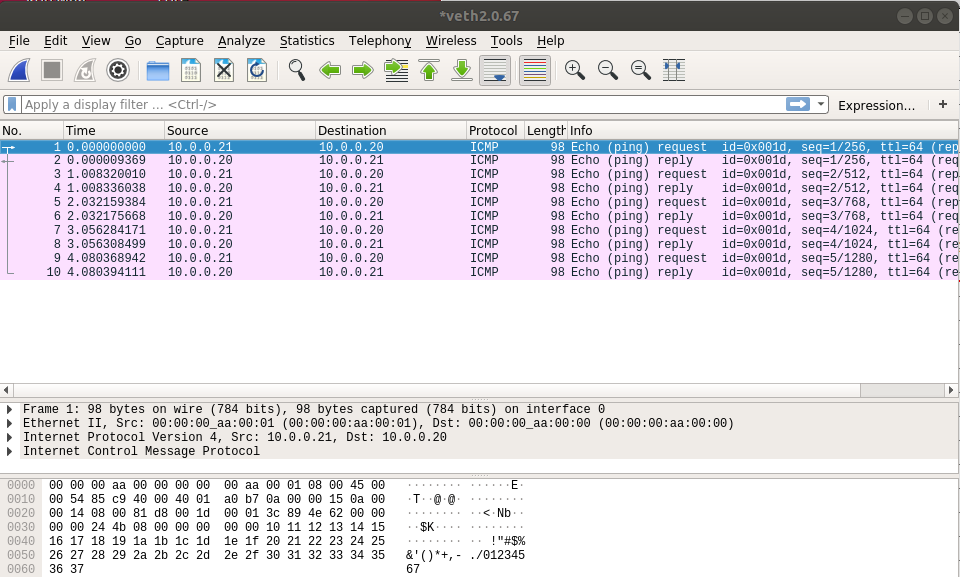


**Работа с анализатором протоколов wireshark**

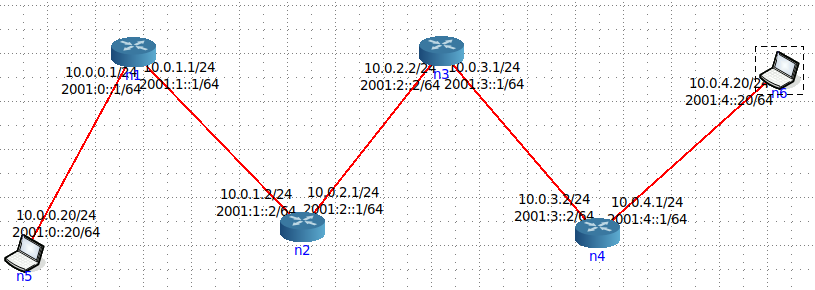
1) Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

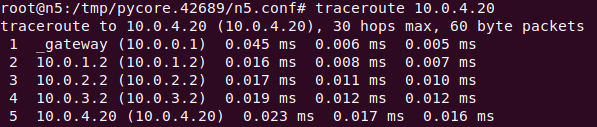


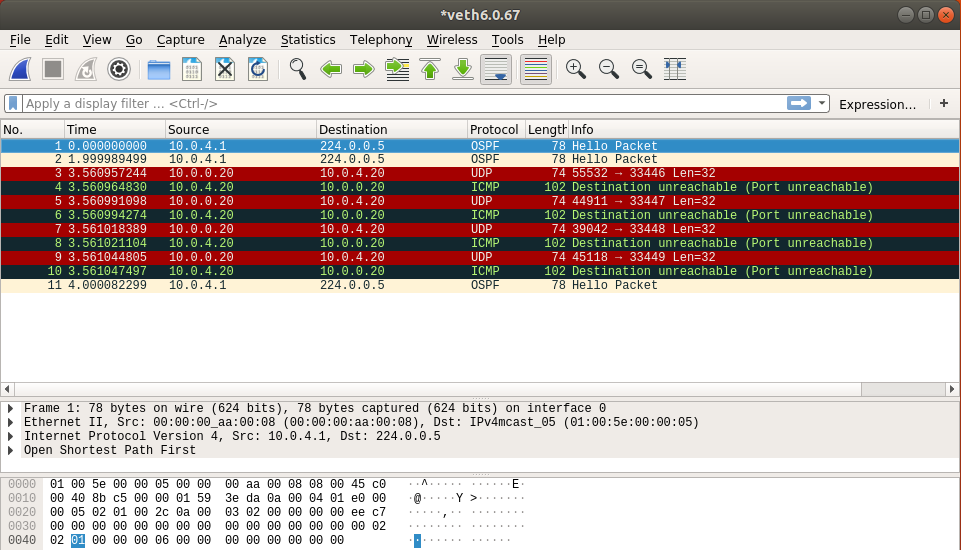
2) Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

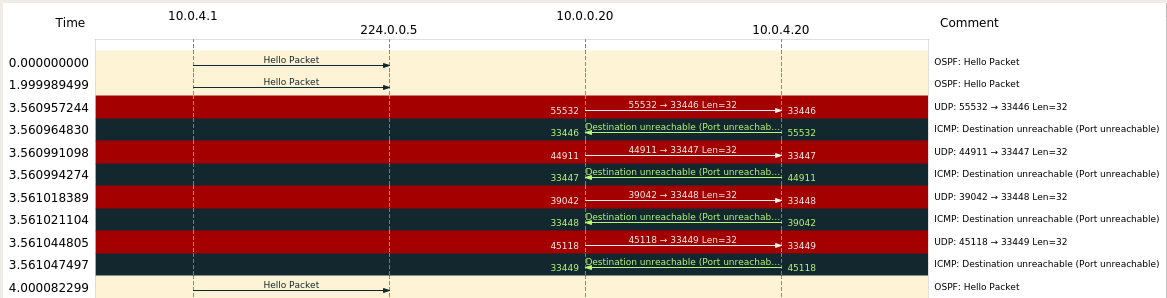


3) Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.



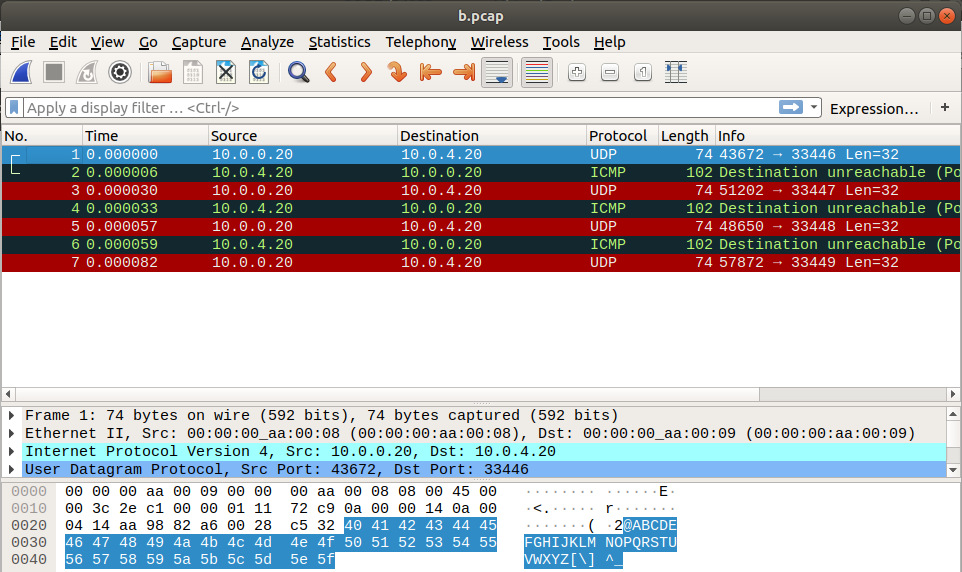




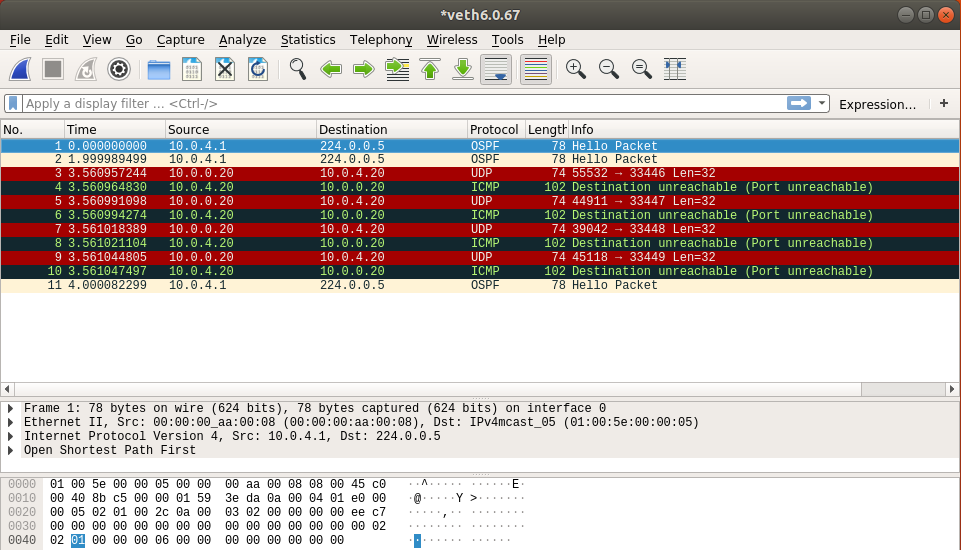


4) Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.

Данные полученные tcpdump:



Данные полученные wireshark:



Данные полученные с помощью tcpdump и wireshark совпадают.

**Вывод:**

В результате данной лабораторной работы были получены базовые навыки работы с анализаторами протоколов tcpdump и wireshark.