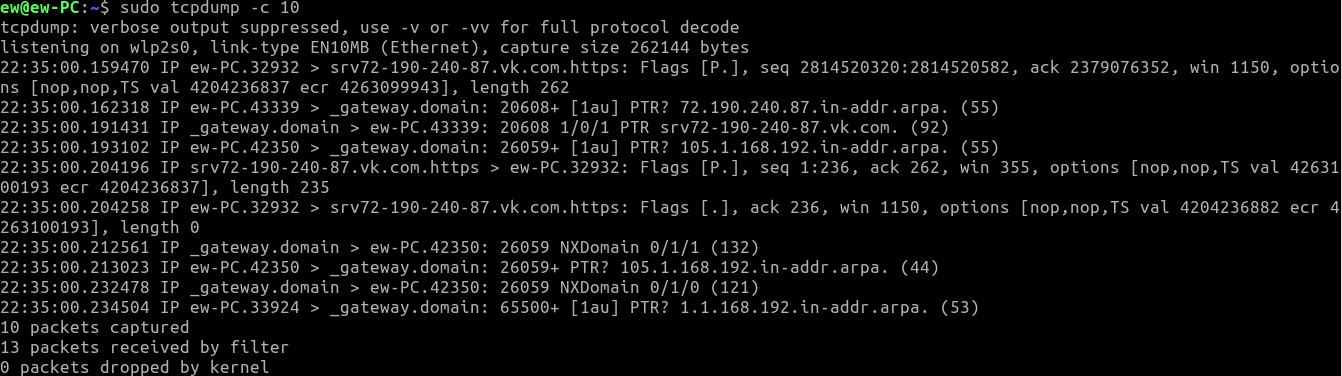
**Цель работы:** получение базовых навыков по работе с анализаторами протоколов windump и wireshark.

**Выполнение**

Вариант 7 – узел www.kontest.ru

**Анализатор протоколов windump**

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

****

**Задание 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).**

tcpdump –e –c 5 –xx ip broadcast ,где

–e – отобразить mac адреса,

-с 5 – ограничить количество пакетов 5 штуками,

-хх отобразить пакет в 16-ой системе с заголовком канального уровня

Ip broadcast – фильтрация широковещательных пакетов

**Задание 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.**

tcpdump -x -xx -c 3 icmp and dst host 192.168.0.1 , где

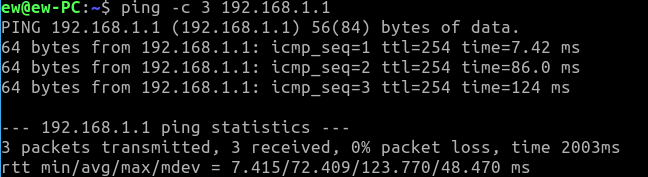
-x – распечатка пакета в 16-ом формате

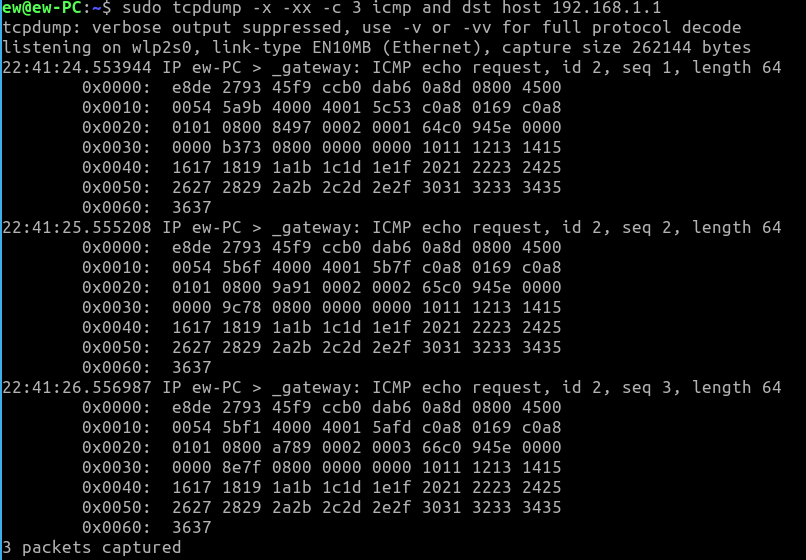
-ХХ – вывод пакета в ASCII формате с заголовком канального уровня

-с 3 – ограничение количества отфильтрованных пакетов – 3

Dst host 192.168.0.1 - фильтруются пакеты, у которых поле адреса получателя содержит ip-адрес 192.168.0.1

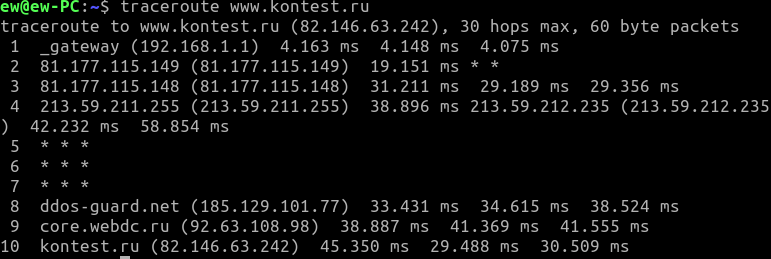
icmp – фильтрация icmp пакетов

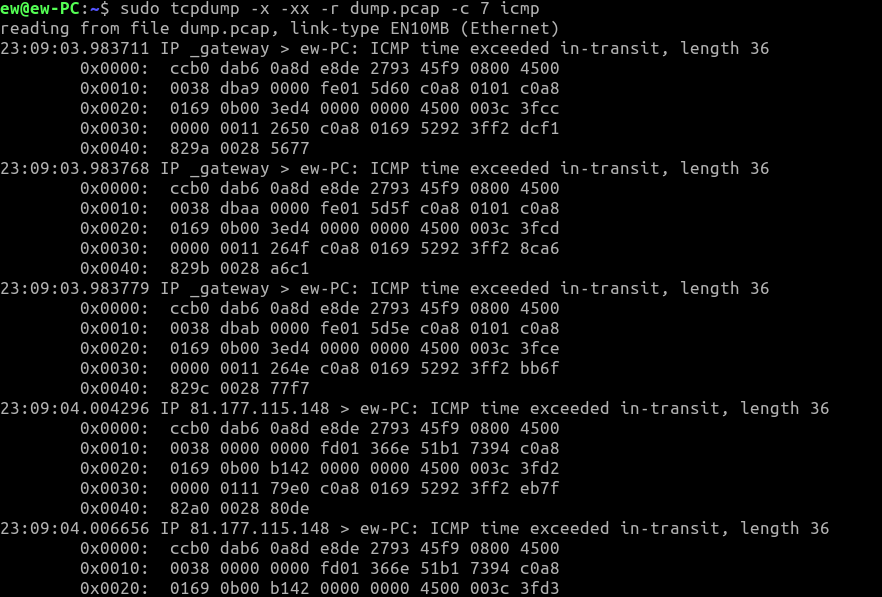
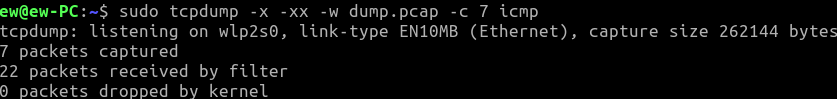




**Задание 4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня).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

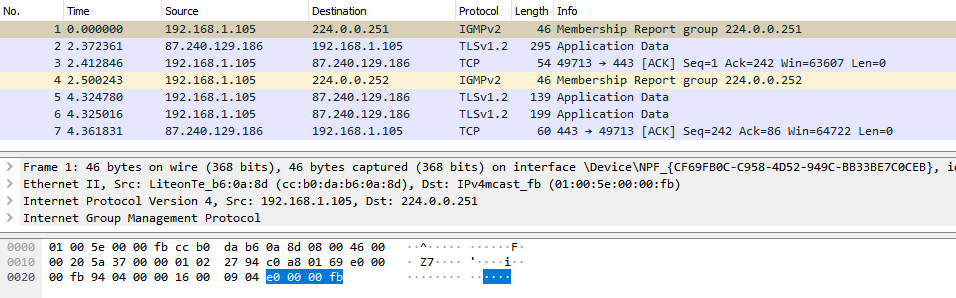
tcpdump -x -xx -w dump2.txt -c 7 icmp



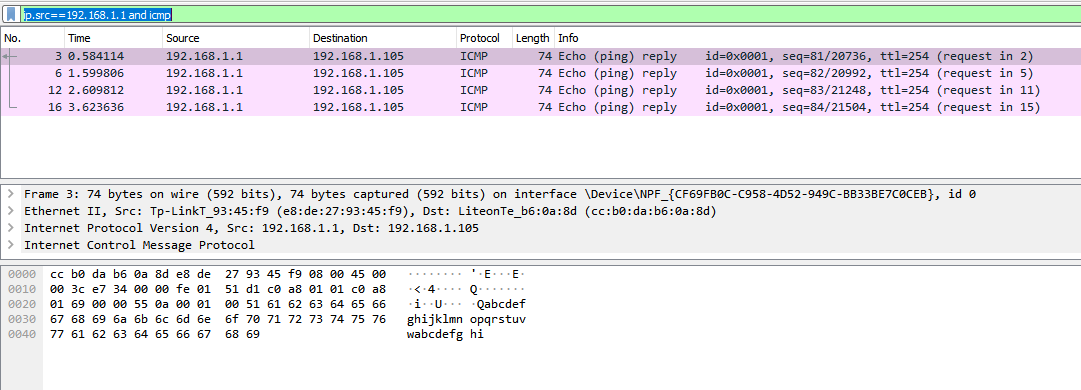


**Анализатор протоколов Wireshark**

**Задание 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.



3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу.

