ФГБОУ ВО НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. Р.Е. АЛЕКСЕЕВА

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Вычислительные системы и технологии»

ОТЧЕТ

*по лабораторной работе №1*

*«*Работа с анализаторами протоколов tcpdump и wireshark*»*

Дисциплина: «Сети и телекоммуникации»

Выполнили:

Студенты гр. 17-В-2

Брызгалов М.М.  
Шипунов Г.Д.

Проверил:

Гай В.Е.

Нижний Новгород

2020

**Цель работы:**

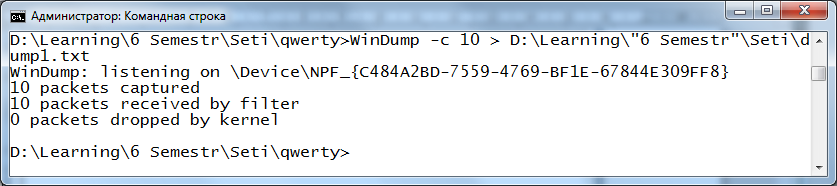
Получение базовых навыков по работе с анализаторами протоколов windump (аналог tcpdump для windows) и wireshark.

Вариант:

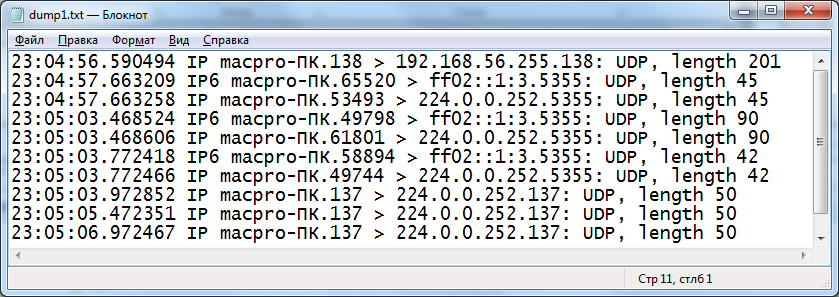


1. Работа с анализатором протоколов **tcpdump**

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



Файл:



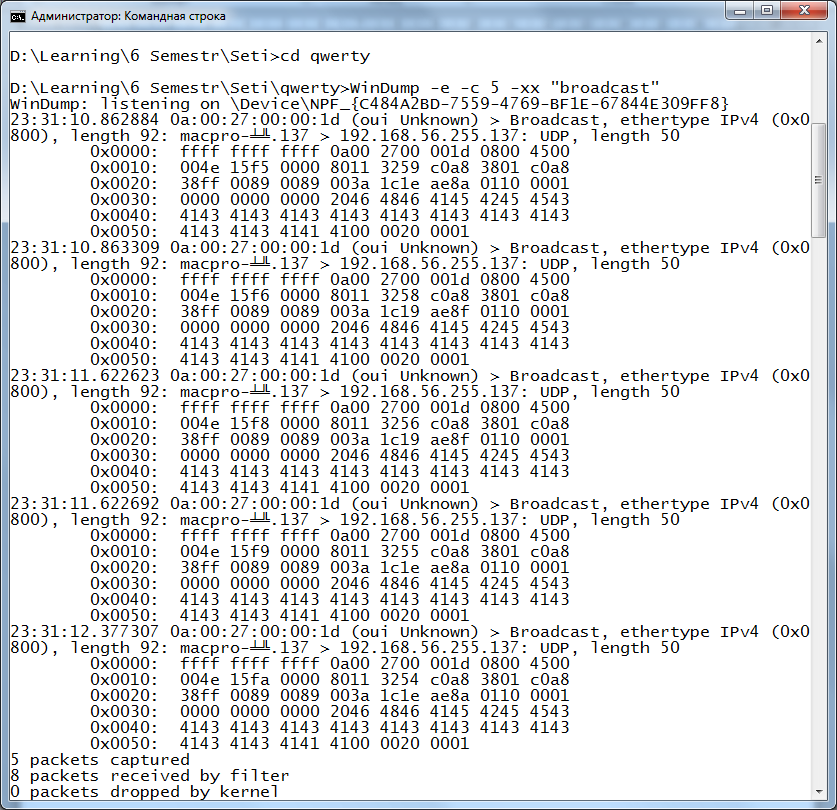
2) Запустить windump в режиме перехвата широковещательного трафика (фильтр по MAC - адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня)

*-e – Отображение mac адресов*

*-с 5 – Ограничение пакетов <=5*

*-xx – Отображение в 16 СС, включая заголовок канального уровня*

*Broadcast – широковещательный трафик*



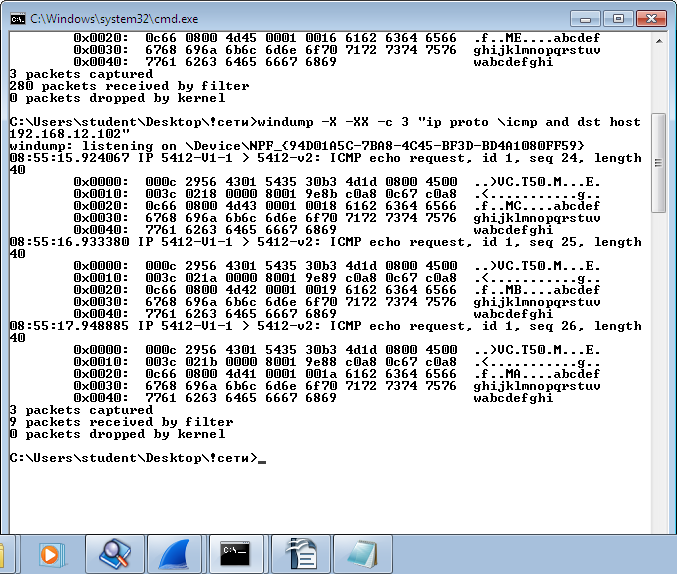
3) Запустить windump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определённый IPадрес. При этом включить распечатку пакета в шестнадцатеричной системе ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов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

*-x – Вывод в 16 СС*

*-xx – Вывод в ASCII формате с заголовком канального уровня*

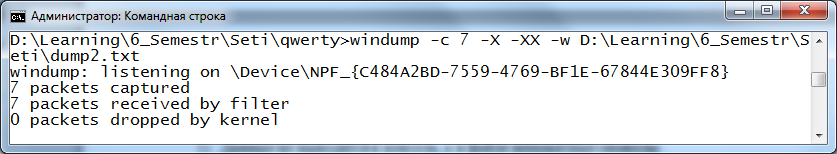
*-c 3 – Ограничение пакетов <= 3*

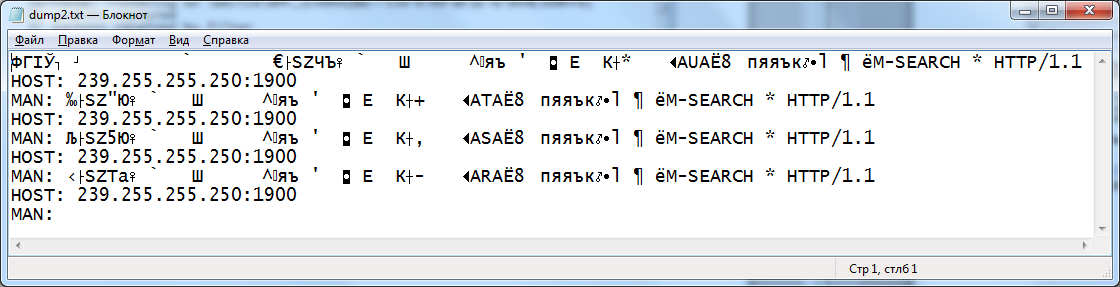
*ip proto\ icmp and dst host – Фильтрация icmp пакетов, у которых ip = ipdst*



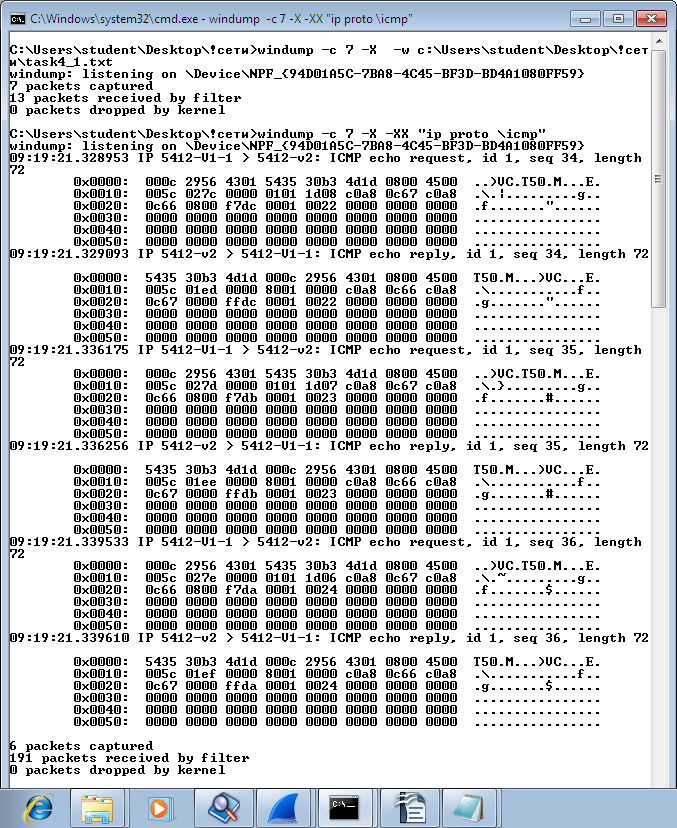
4) Запустить tcpdump в режиме сохранении данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой tracerouteдля определения маршрута к заданному в варианте узлу. Включить распечатку ракета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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

Данные не выводятся в консоль, а в файле непонятные символы





Фильтрация по протоколу icmp, просмотр информации прямо в консоли в 16 формате и ASCII

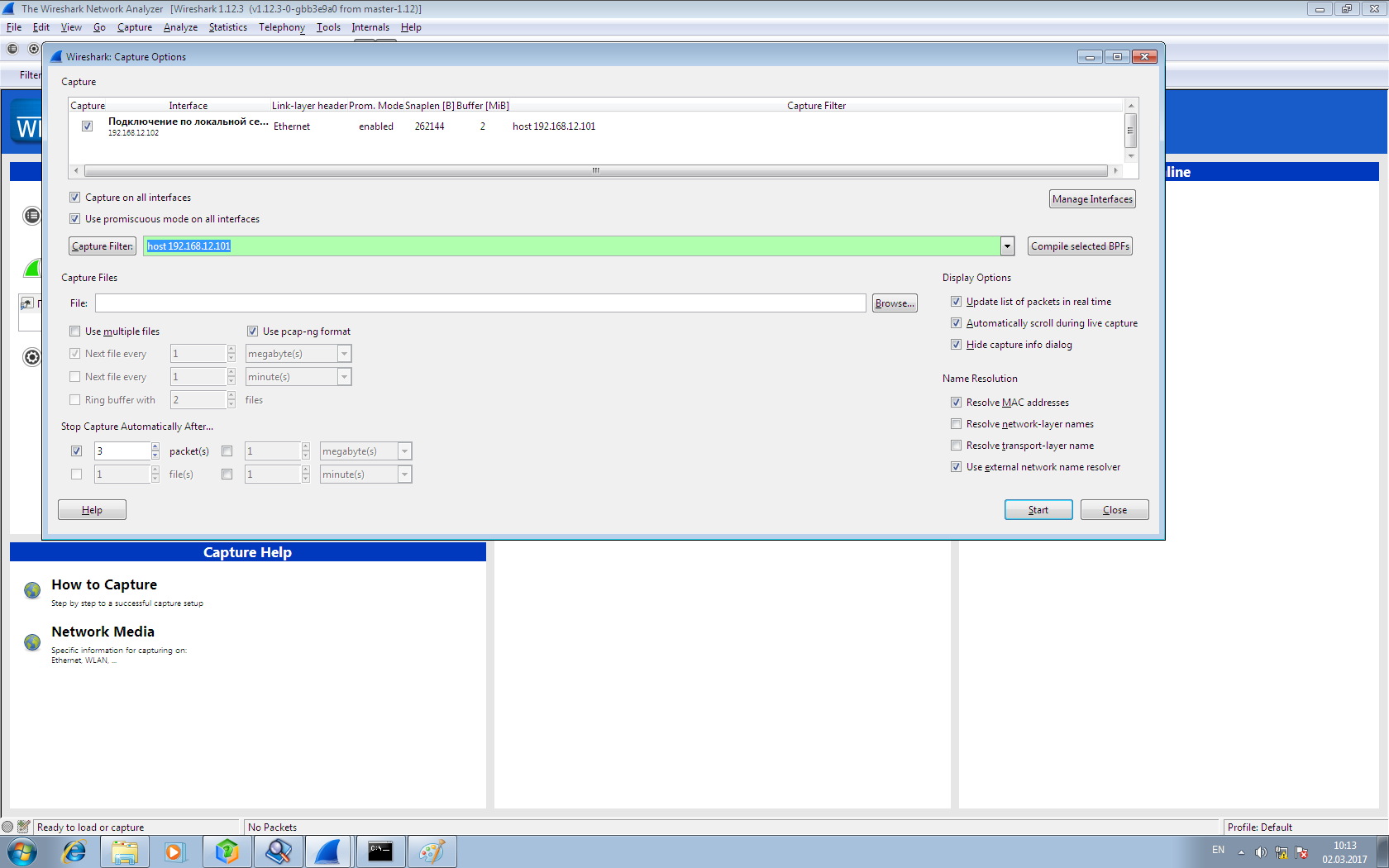


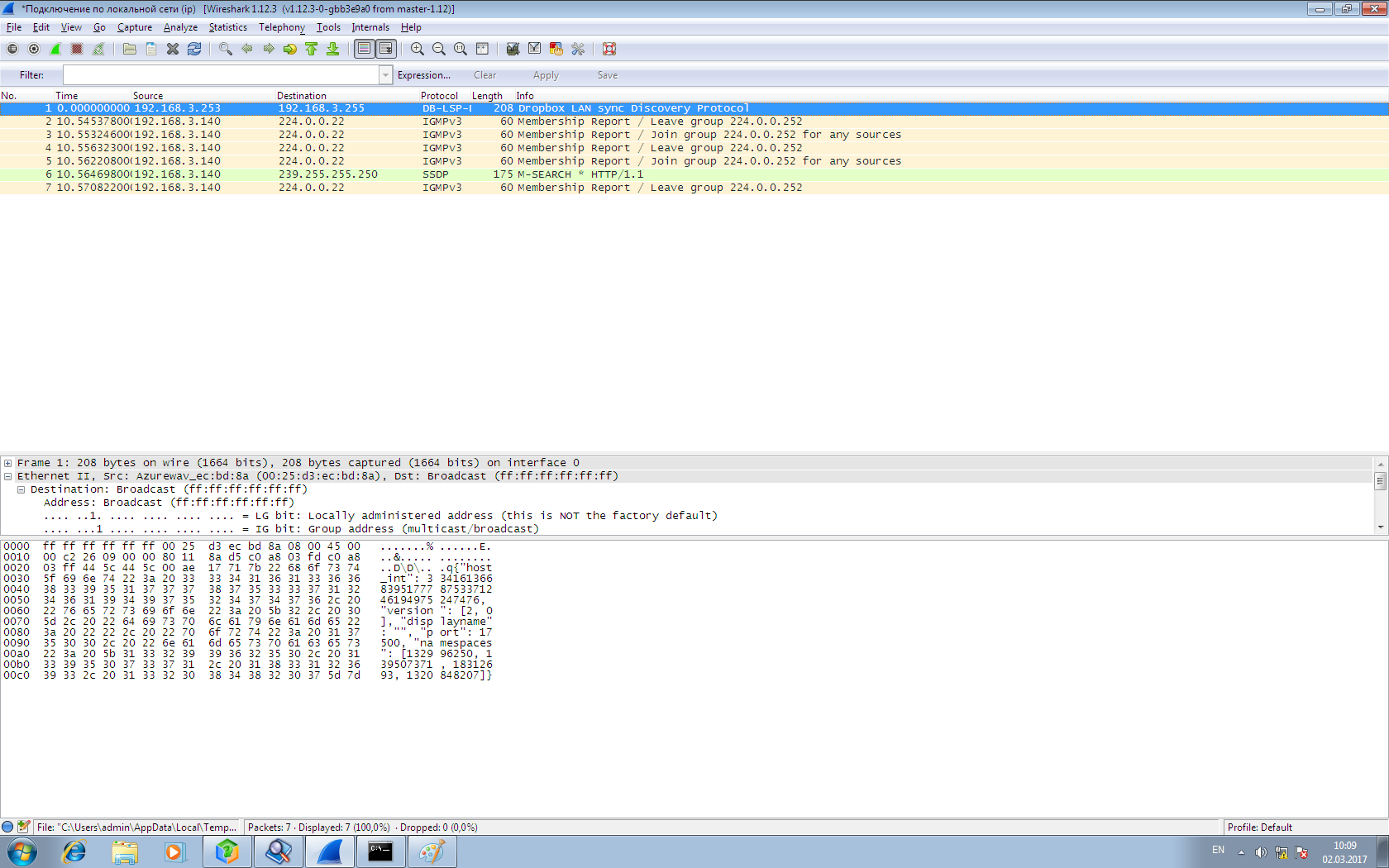
5) Прочесть файл, созданный программой windump.

2. Работа с анализатором протоколов wireshark

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

Для выполнения этого задания необходимо открыть Wireshark, затем открыть окно «Capture-Options», задать в поле «Capture filter» - ether broadcast (фильтровать широковещательный трафик по MAC адресу), а также в поле «Stop Capture Automatically After…» задать количество пакетов = 7.

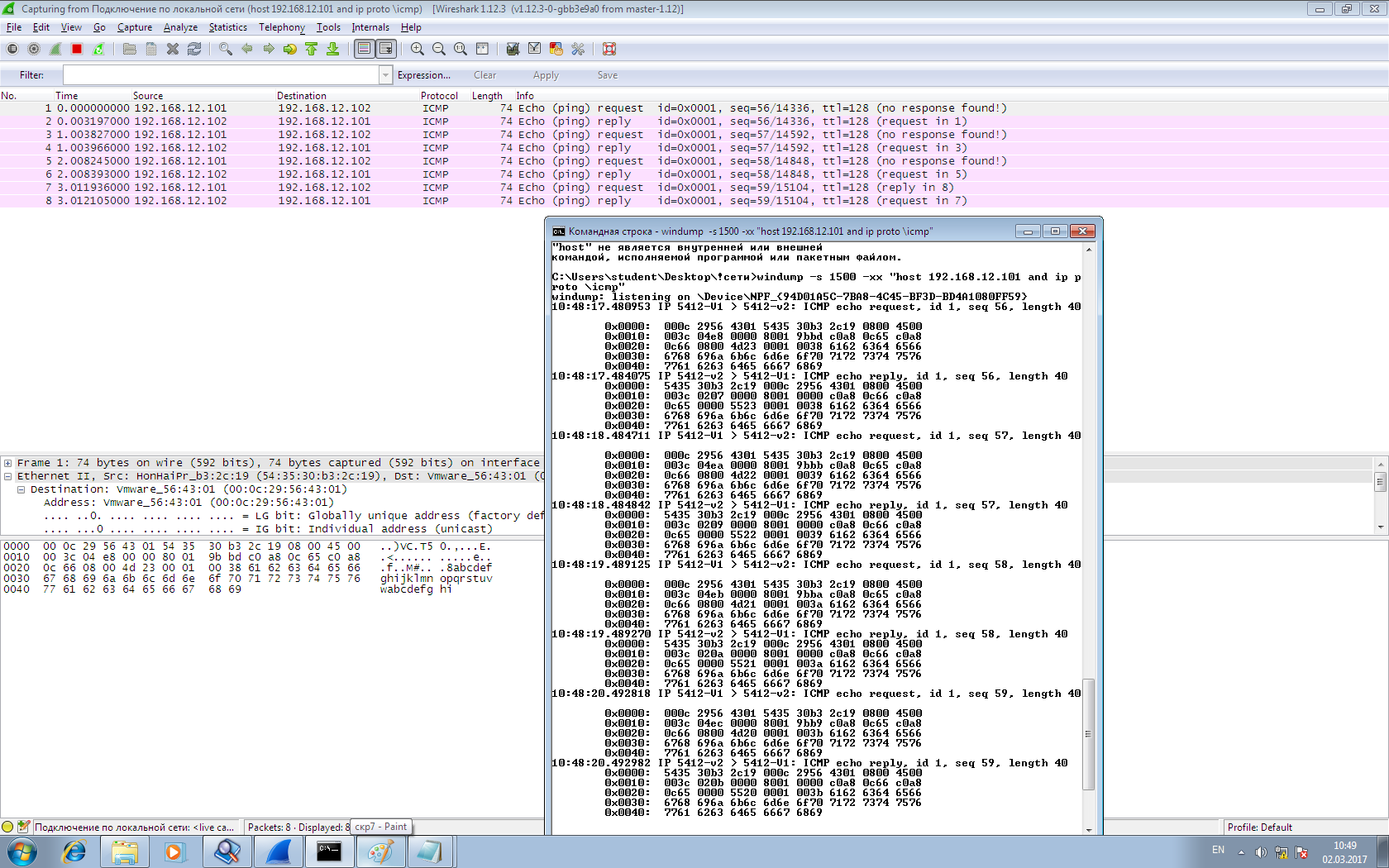




1. Захватить 3-4 пакета ICMP , полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

«Capture filter» - icmp and src 192.168.12.101 and 192.168.12.102,

«Stop Capture Automatically After…» - 8.



1. 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.

Capture filter» - icmp,

«Stop Capture Automatically After…» снять галочку.

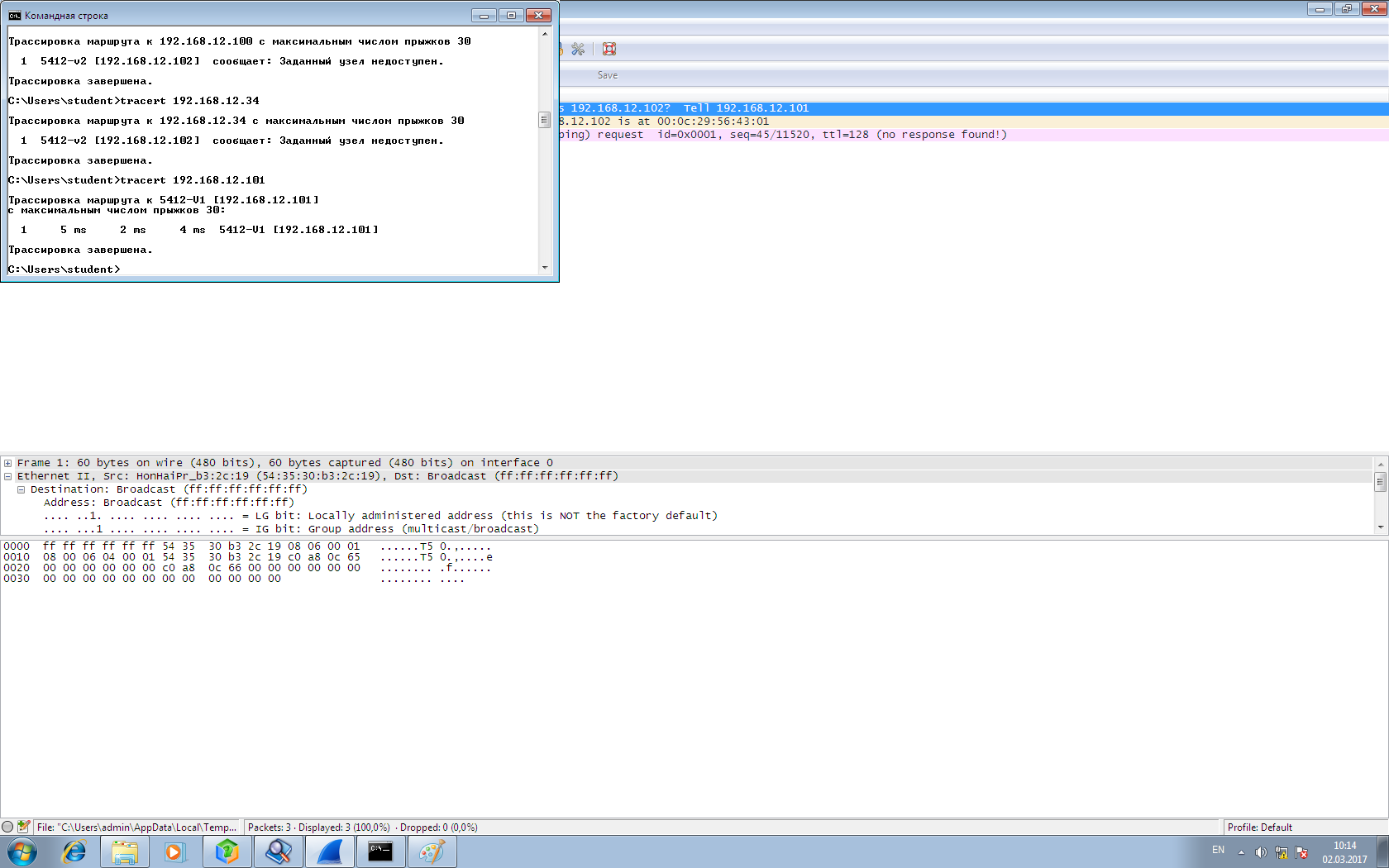
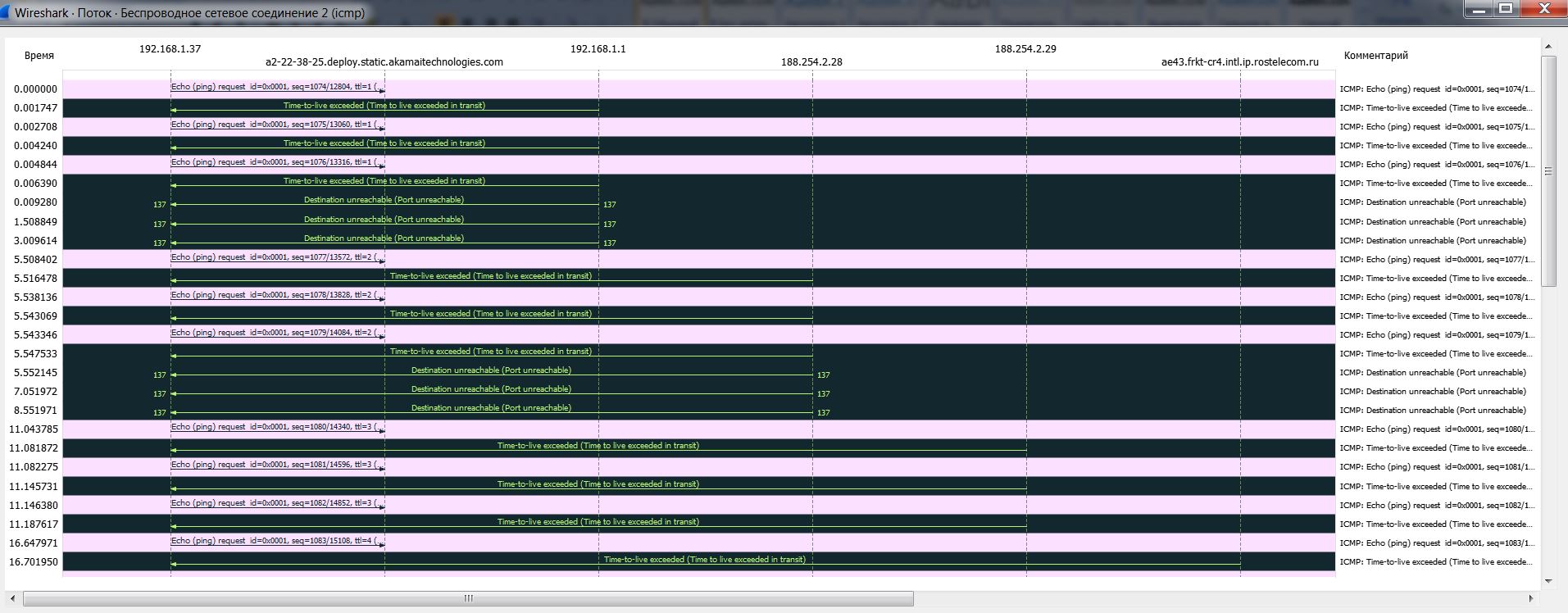
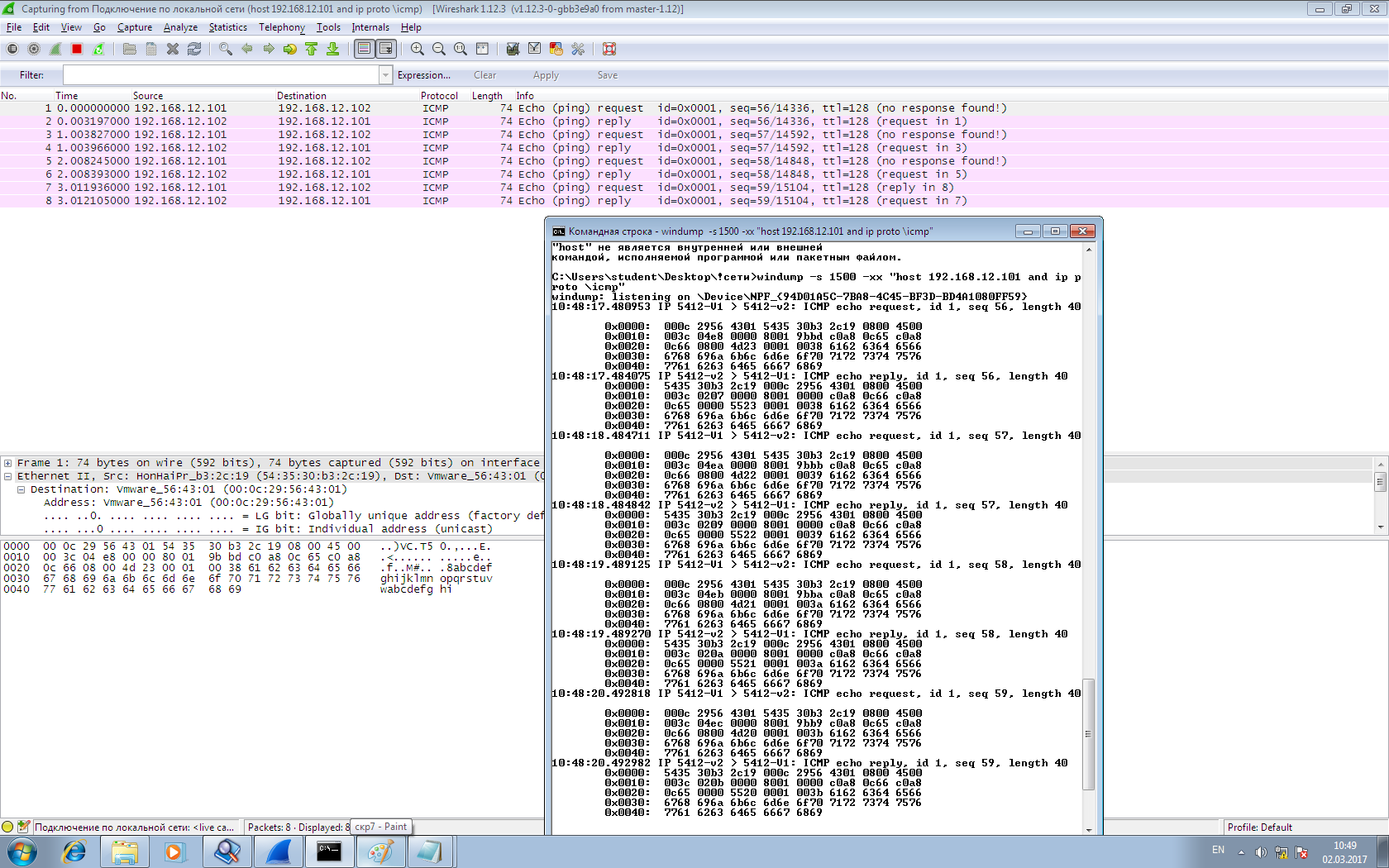


Диаграмма FlowGraph.



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

На рис. представлен открытый программой Wireshark файл trace\_in\_2, где отфильтрованы первые 8 пакетов, созданные утилитой windump.



**Вывод:** в ходе выполнения лабораторной работы были получены базовые навыки по работе с анализаторами трафика – WinDump и WireShark.