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

по дисциплине «Сети и Телекоммуникации»

Вариант 4

«Работа с утилитами ping, traceroute.

Работа с анализаторами протоколов tcpdump и wireshark»

ПРОВЕРИЛ:

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

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Зайкин А.М.

17-В-1

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

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

Нижний Новгород

2020

**Часть 1.**

**Цель работы**: получение базовых навыков по работе с утилитами ping, traceroute.

**Вариант 4:**

Исследуемые узлы: Число отправляемых пакетов:

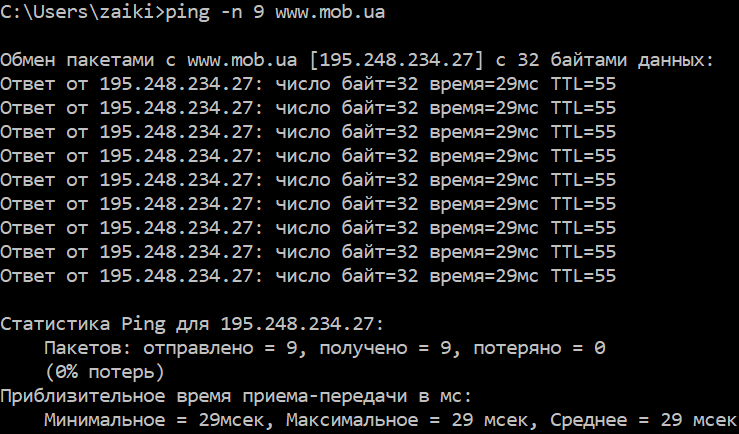
mob.ua 9

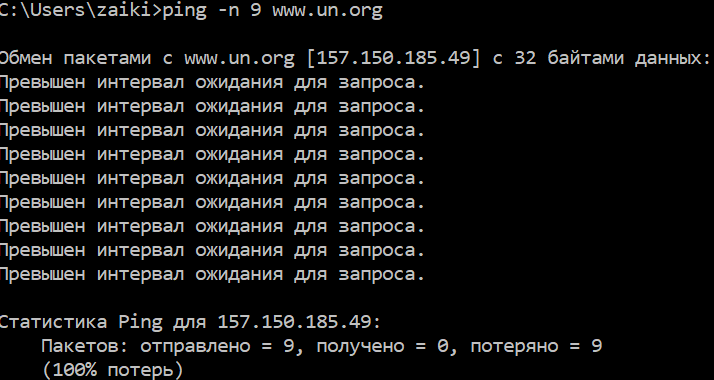
www.un.org

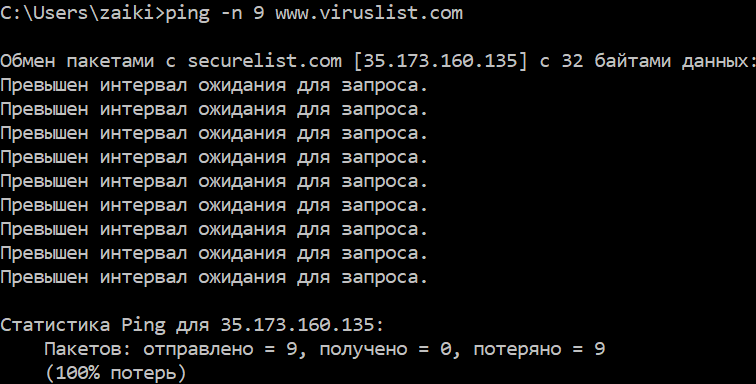
www.viruslist.com

**Порядок выполнения лабораторной работы:**

1) С помощью утилиты ping проверить состояние связи с узлами, заданными в варианте.







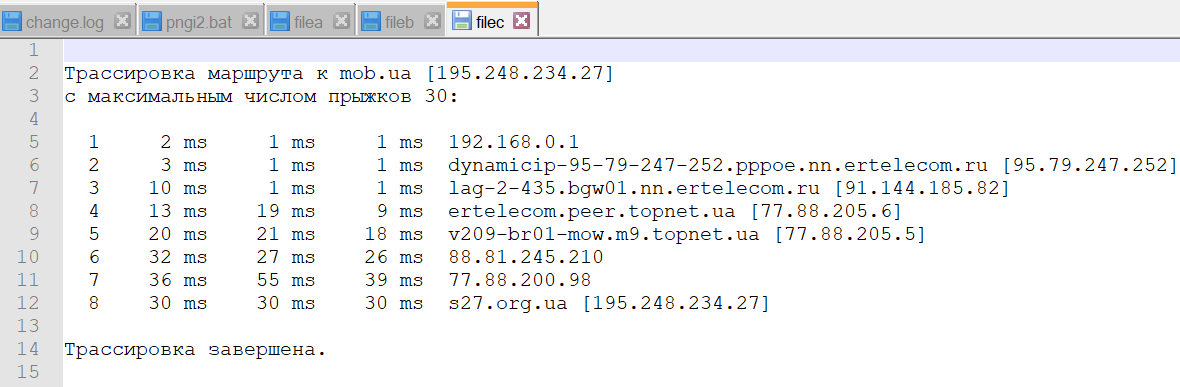
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Доменное имя | IP-адрес | Страна | Число потерянных запросов | Среднее время прохождения запроса, мс | TTL |
| mob.ua | 195.248.234.27 | Украина | 0 | 29 | 55 |
| www.un.org | 157.150.185.49 | США | 9 | - | - |
| www.viruslist.com | 35.173.160.135 | США | 9 | - | - |

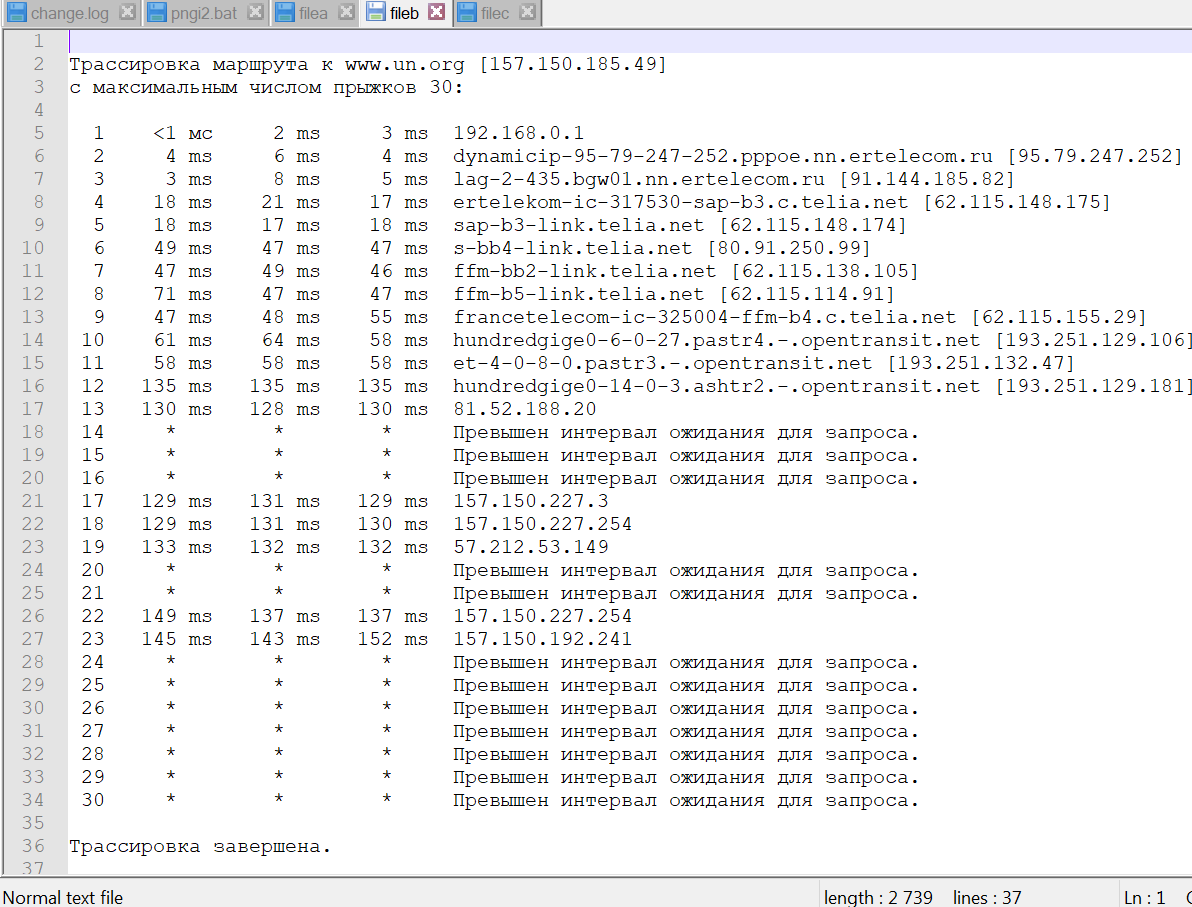
2) При помощи утилиты traceroute произвести трассировку узлов, заданных в варианте

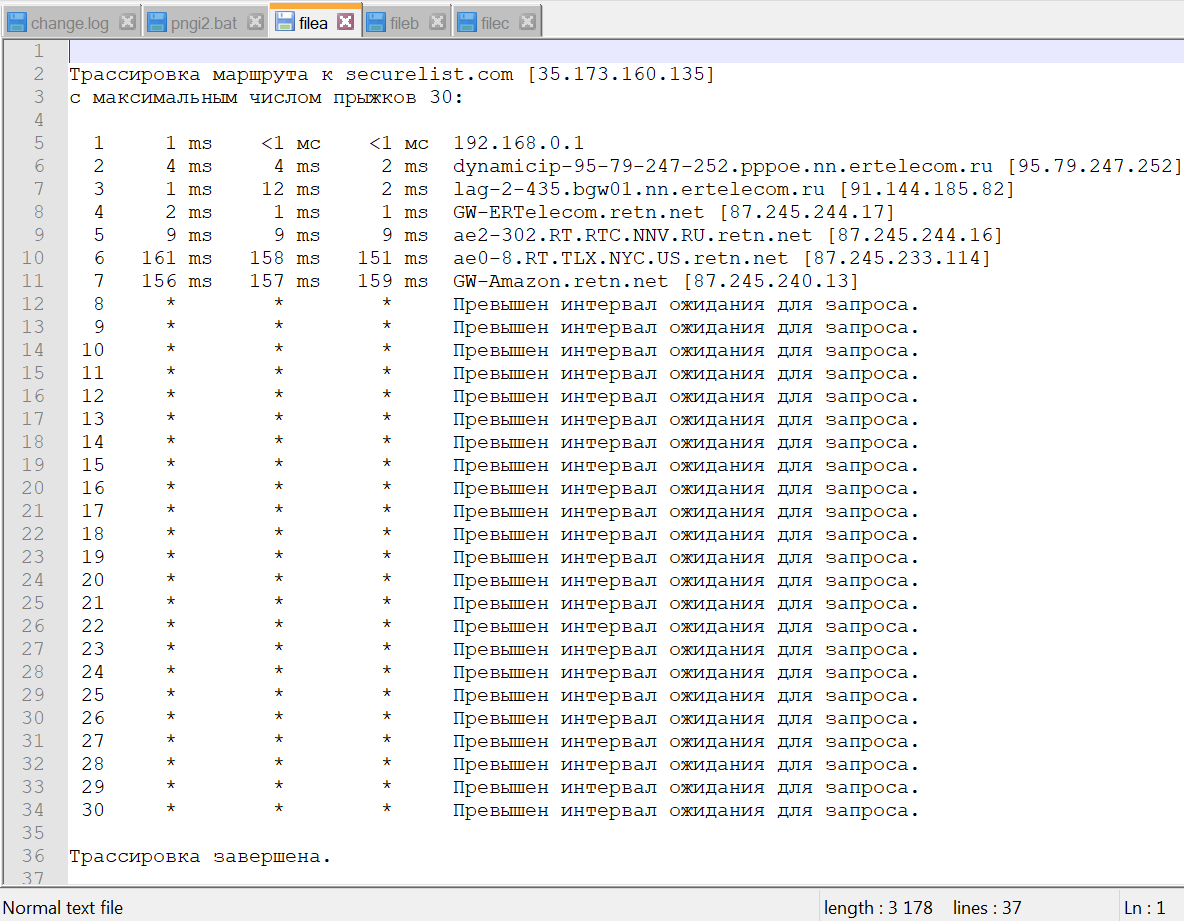
Результаты протоколировать в файл.

По результатам составить графики времени прохождения шлюзов для каждого узла

(для 3-х пакетов)

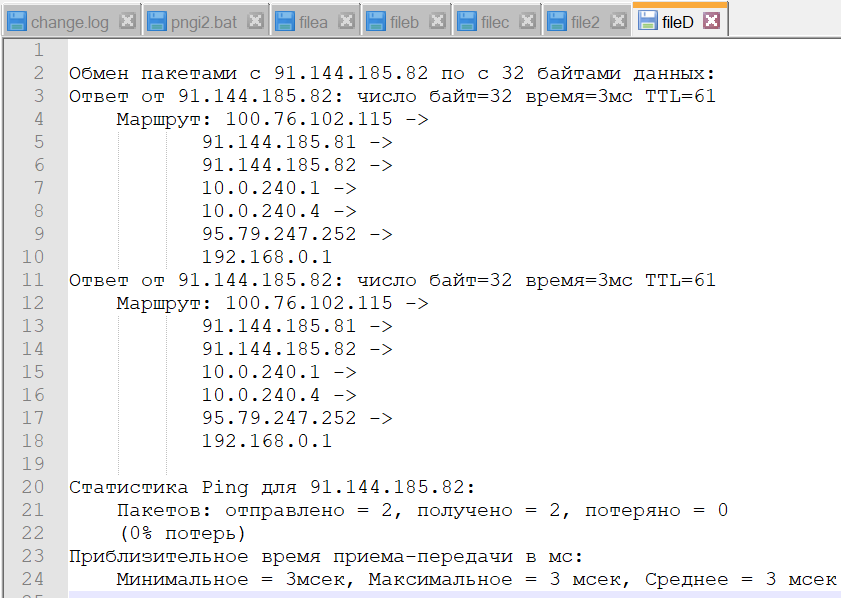






3) Получить маршрут прохождения пакетов до одного из заданных в варианте узлов при помощи утилиты ping. Результаты протоколировать в файл

D:\1 Учеба\семестр 6\Сети лабы\121.png



**Часть 2:**

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

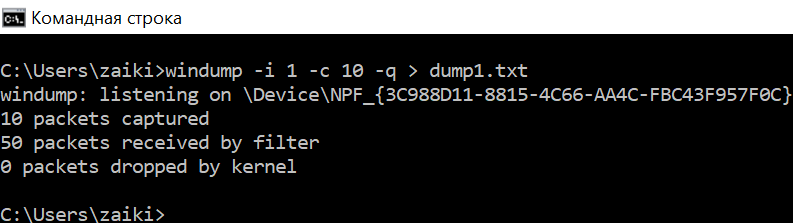
**Порядок выполнения лабораторной работы**

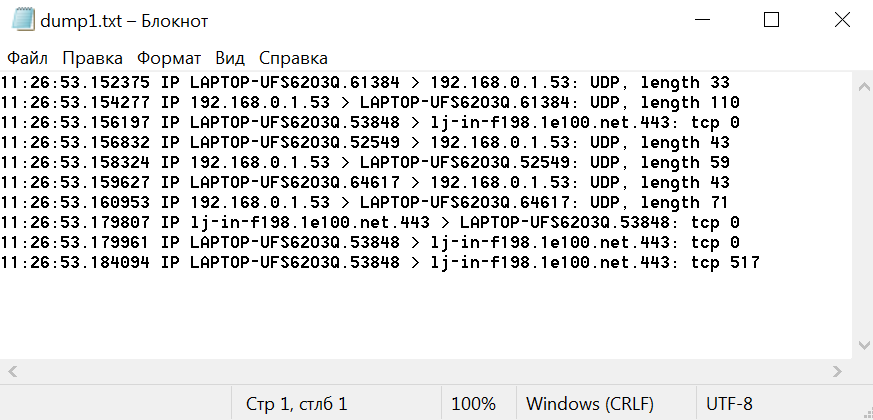
**Работа с анализатором протоколов tcpdump**

1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество

захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

windump -i 1 -c 10 -q > dump1.txt





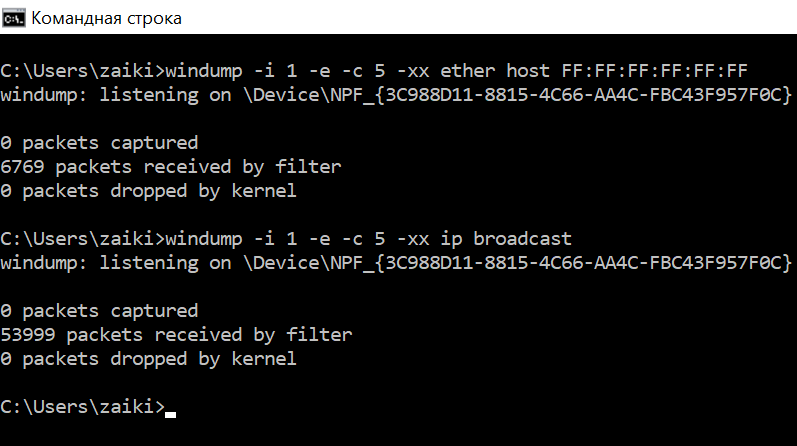
2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку па- кета в шестнадцатеричной системе (включая заголовок канального уровня).

Были выполнены запросы:

windump –i 1 –e –c 5 –xx ip broadcast

windump –i 1 –e –c 5 –xx ether host FF:FF:FF:FF:FF:FF

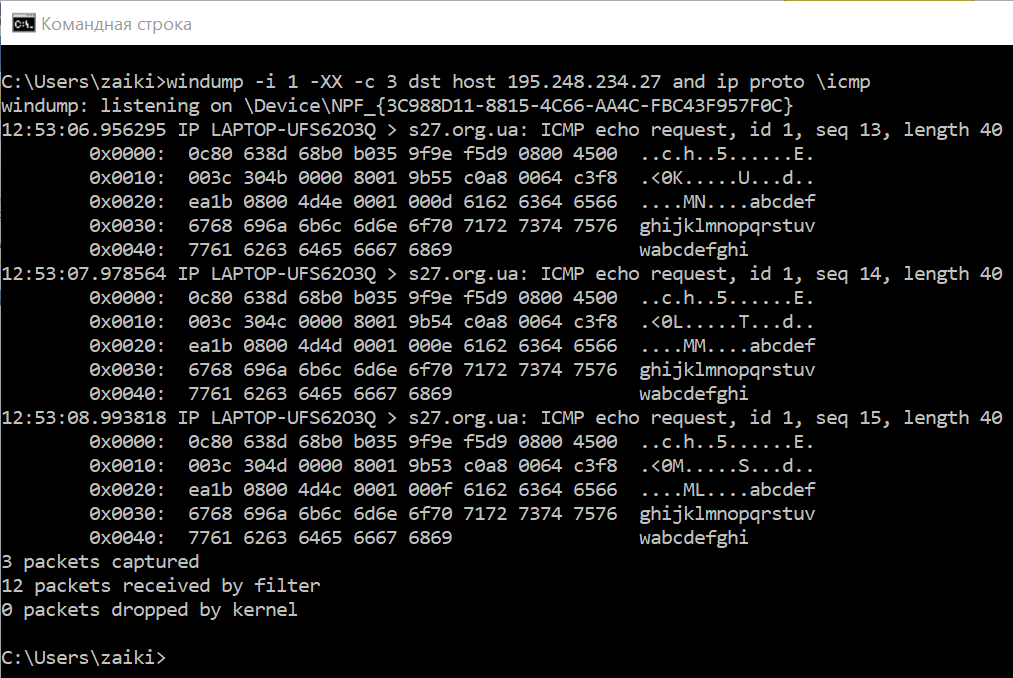
В результате после 5-ти минутного ожидания вывода не было.



Предположительно, от широковещательных пакетов экранирует роутер

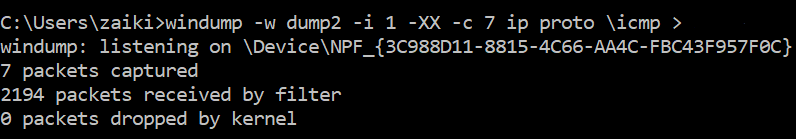
3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, от- правленные на определенный IP-адрес (возможные адреса можно посмотреть на схеме ЛВС лаб. 521). При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов возпользоваться утилитой ping.

windump –i 1 –XX –c 3 dst host 195.248.234.27 and ip proto \icmp



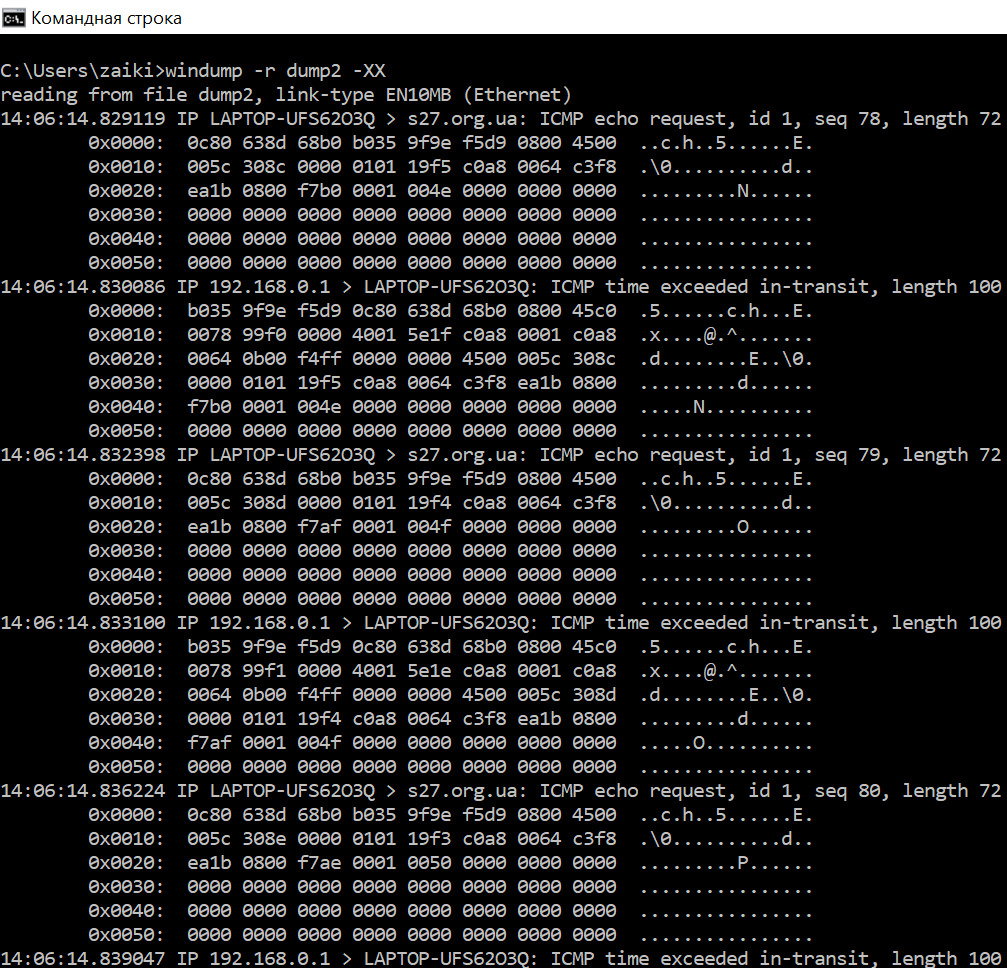
4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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

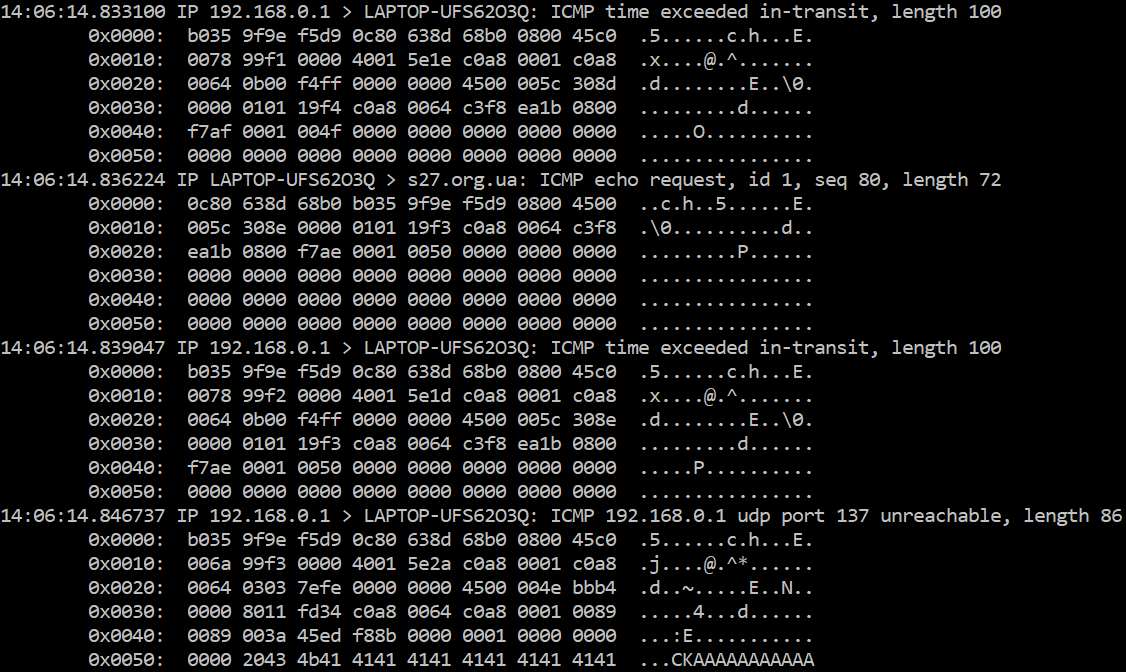
windump -w dump2 -i 1 -XX -c 7 ip proto \icmp



5. Прочесть программой tcpdump созданный в предыдущем пункте файл.

windump -r dump2 -XX



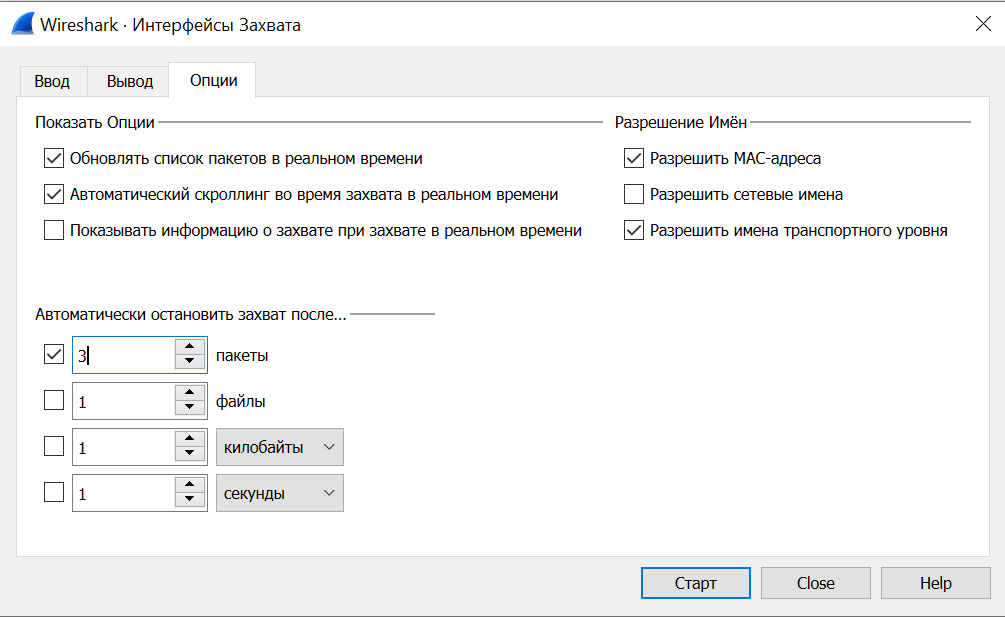


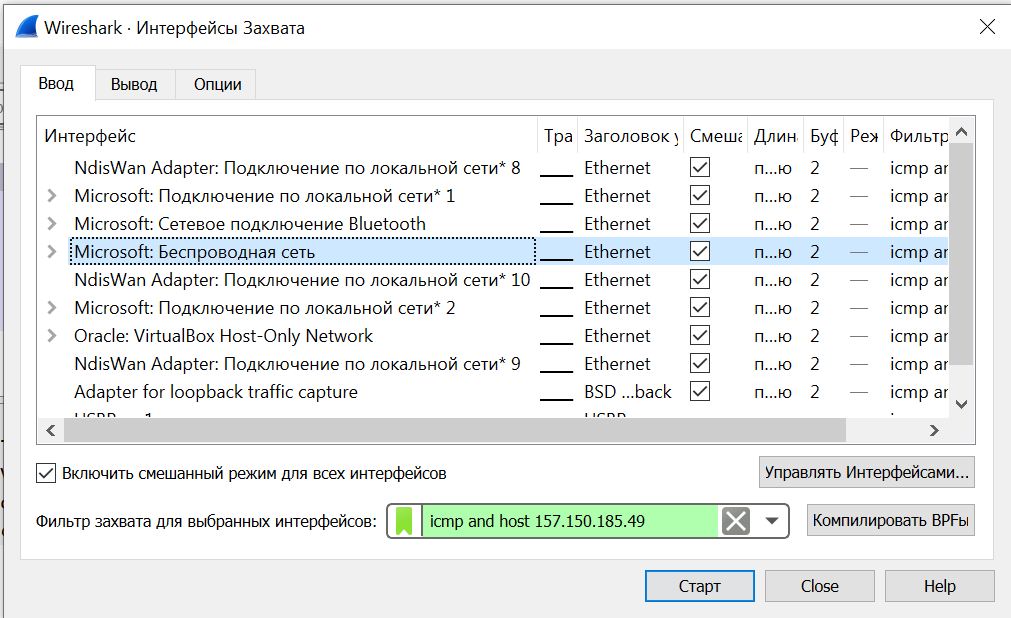
**Работа с анализатором протоколов wireshark**

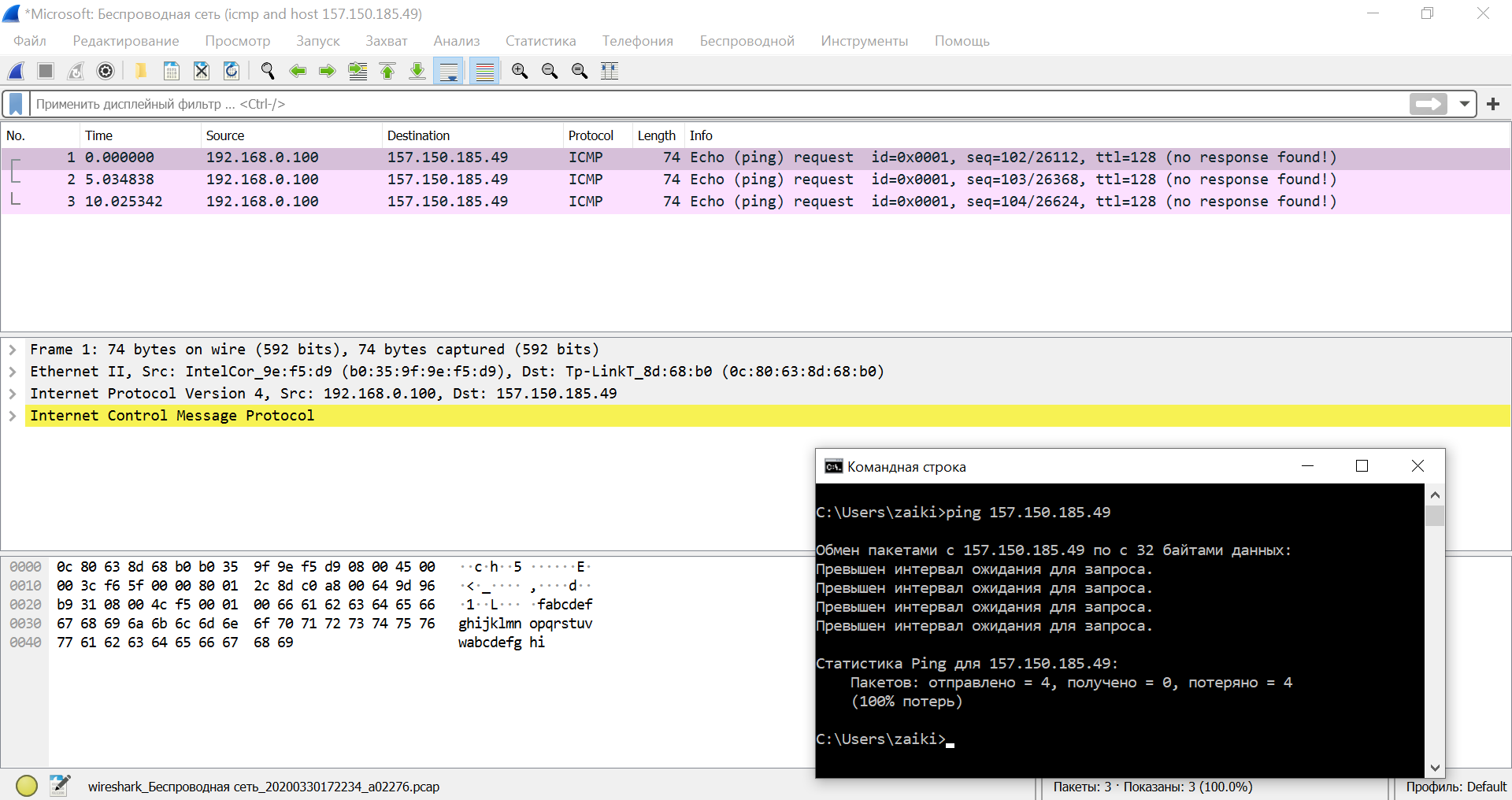
1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

Как и при использовании windump, за несколько минут работы широковещательных пакетов не было перехвачено. Предположительно, от широковещательных пакетов экранирует роутер

2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов возпользоваться утилитой ping. Результат сохранить в текстовый файл. Фильтр icmp and host 157.150.185.49



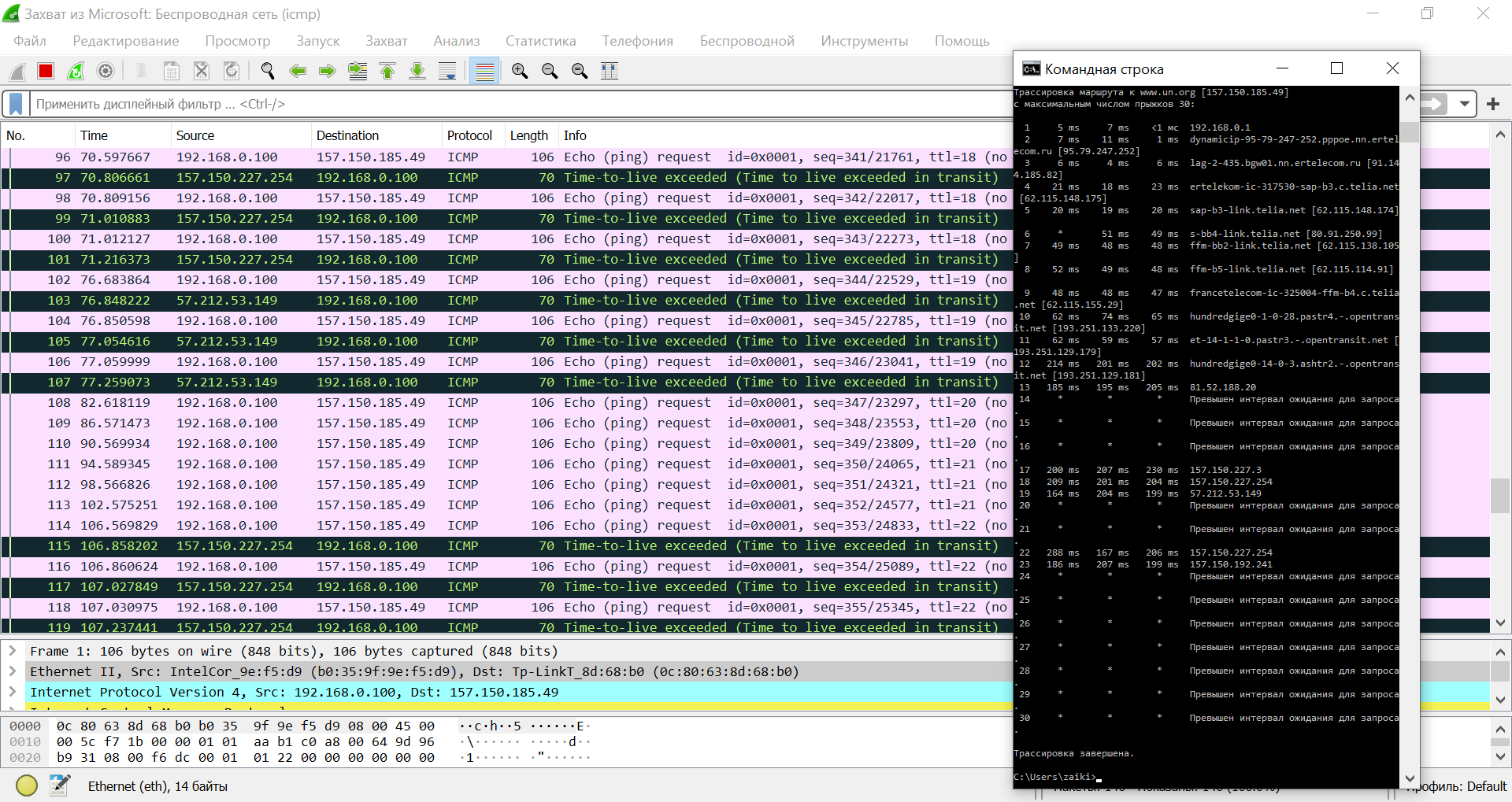


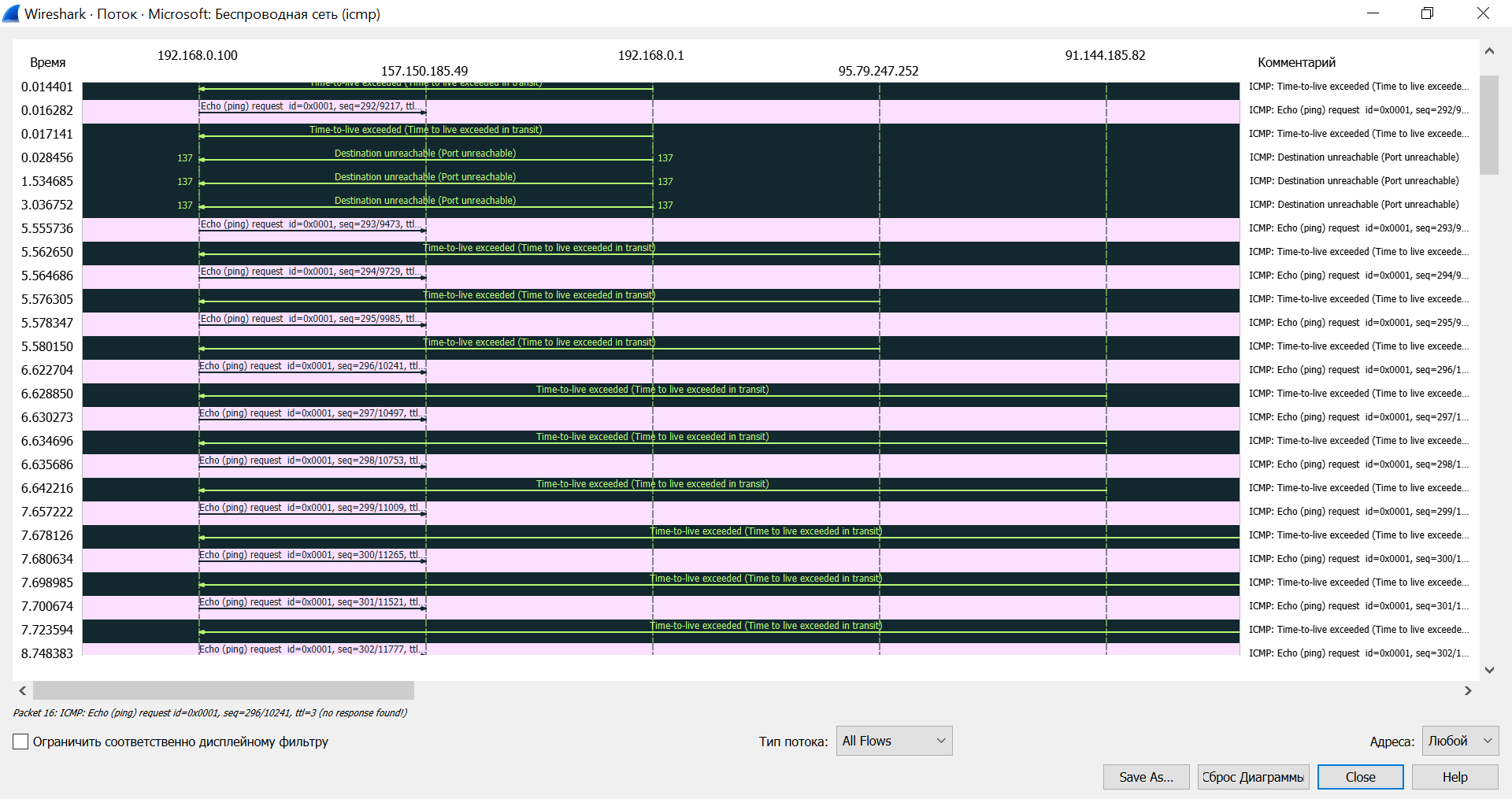


3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к за-

данному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму

сохранить либо в виде текстового файла либо в виде изображения.





**Вывод:**

В данной лабораторной работе произошло ознакомление с такими утилитами, как: ping, traceroute, предназначенными для проверки соединений в сетях, построенных на стеке протоколов TCP/IP. Также были проанализированы результаты данных утилит и сделаны соответствующие выводы об узких местах в сети. Во второй части были освоены приемы работы с анализаторами протоколов tcpdump и wireshark.