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»

7 вариант

«Работа с утилитами ping, traceroute.

Работа с анализаторами протоколов tcpdump и wireshark»

ПРОВЕРИЛ:

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

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Видюльцев Д.И.

17-АС

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

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

Нижний Новгород

2020

Часть№1

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

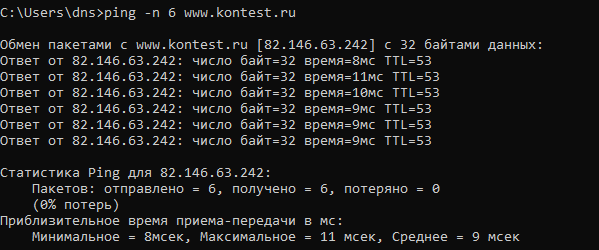
Вариант №2

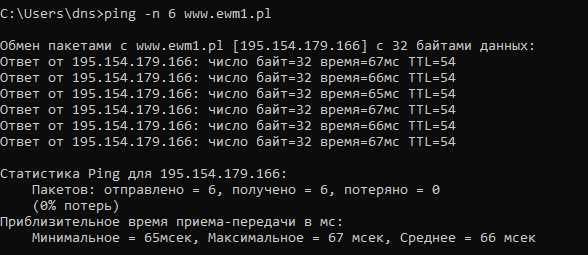
|  |  |  |
| --- | --- | --- |
| 7 | www.kontest.ru  [www.ewm1.pl](http://www.ewm1.pl)  pingmag.jp | |
| **Число отправляемых пакетов *N*** | | 6 |

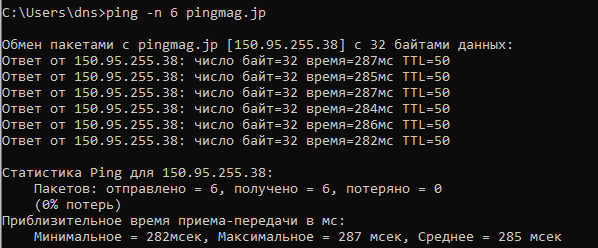
**Выполнение работы:**

1. С помощью утилиты ping проверить состояние связи с узлами. Число отправляемых запросов = 6.

ping –n 6 …

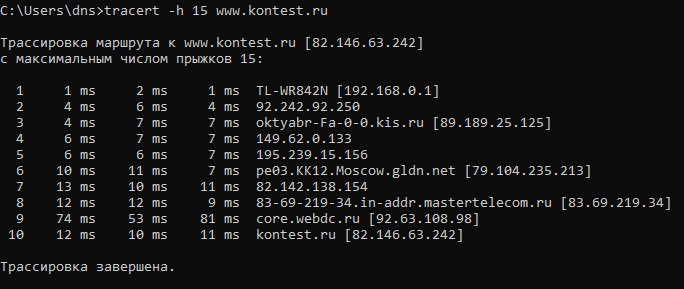


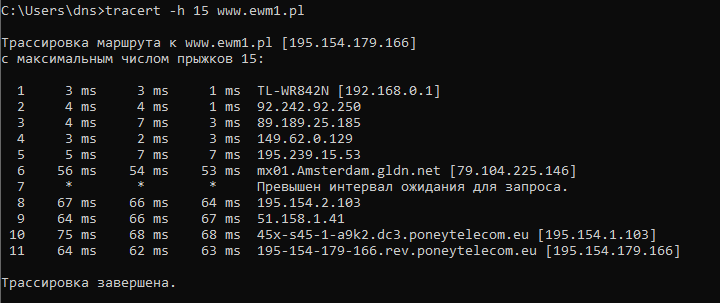


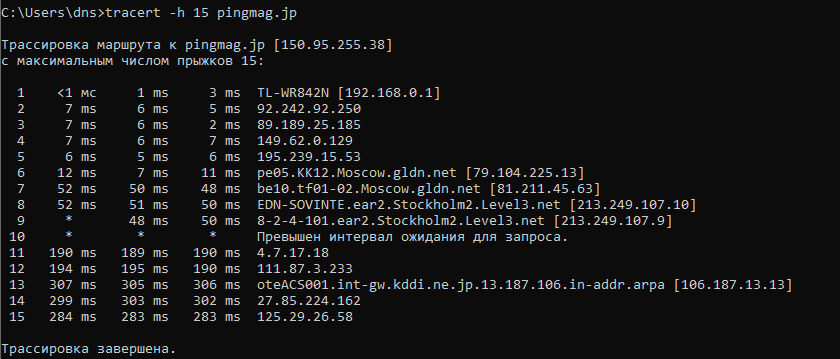


|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Доменное  имя | IP-адрес | Страна | Число потерянных  запросов | Среднее время  прохождения запроса, мс | TTL |
| www.kontest.ru | 82.146.63.242 | Россия | 0 | 9 | 53 |
| www.ewm1.pl | 195.154.179.166 | Польша | 0 | 66 | 54 |
| www.pingmag.jp | 150.95.255.38 | Япония | 0 | 285 | 50 |

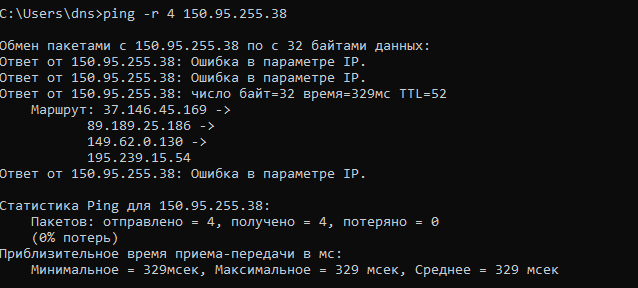
1. При помощи утилиты traceroute (tracert) произвести трассировку узлов.







1. Получить маршрут прохождения пакетов до одного из заданных в варианте узлов при помощи утилиты ping.



**Часть №2**

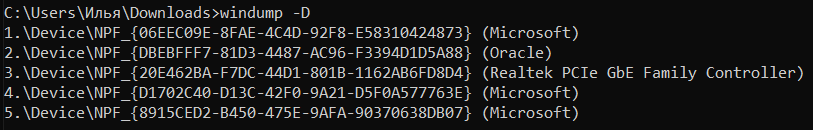
**Работа с анализаторами протоколов tcpdump и wireshark.**

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

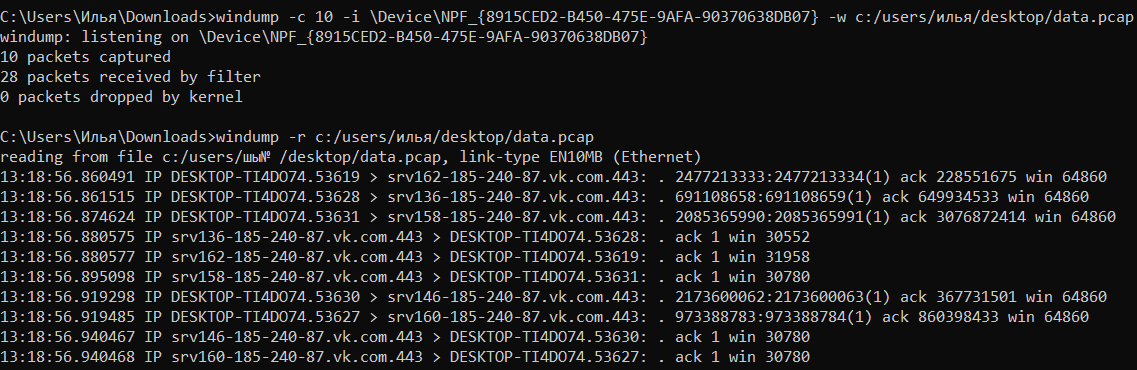
Работа с анализатором протоколов tcpdump.

Доступные сетевые интерфейсы:

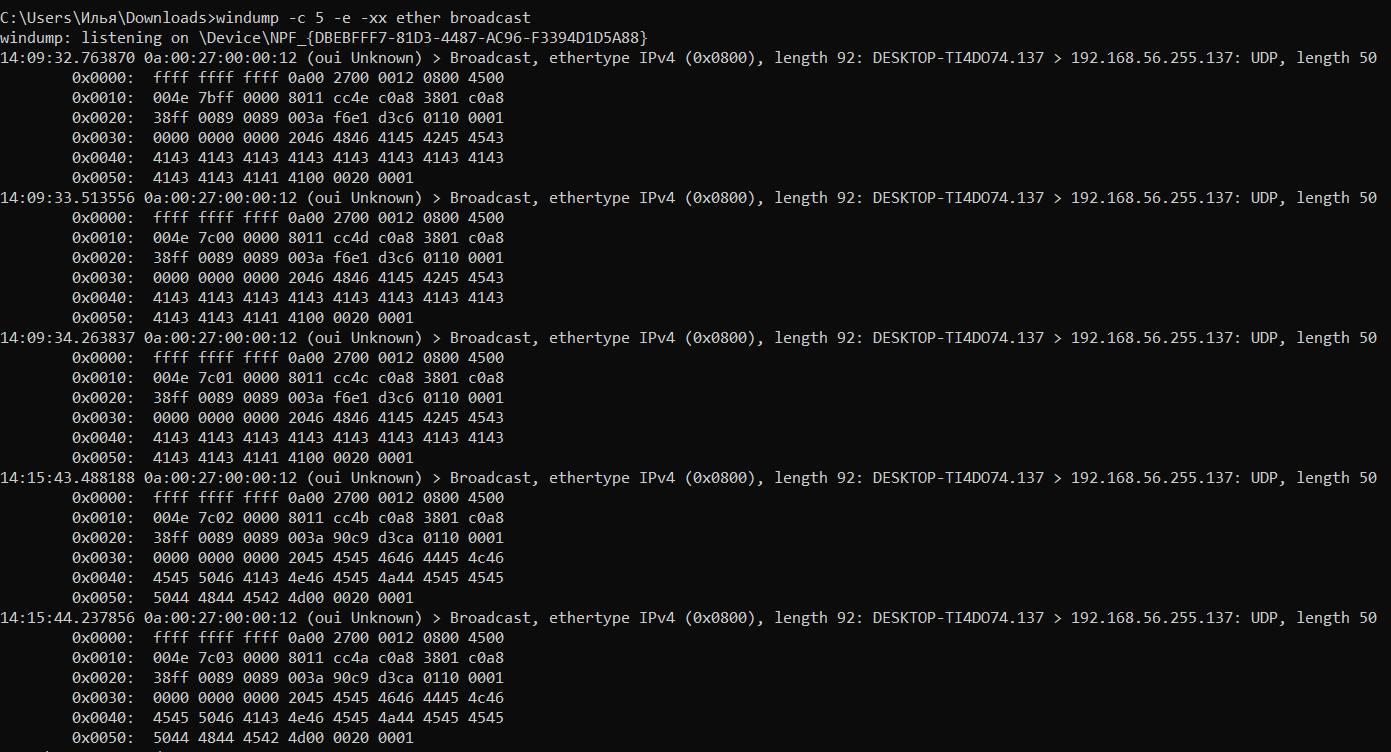
Windump -D

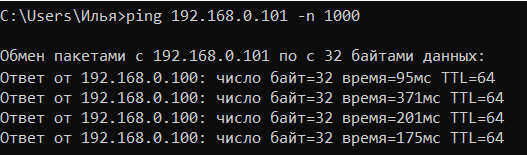


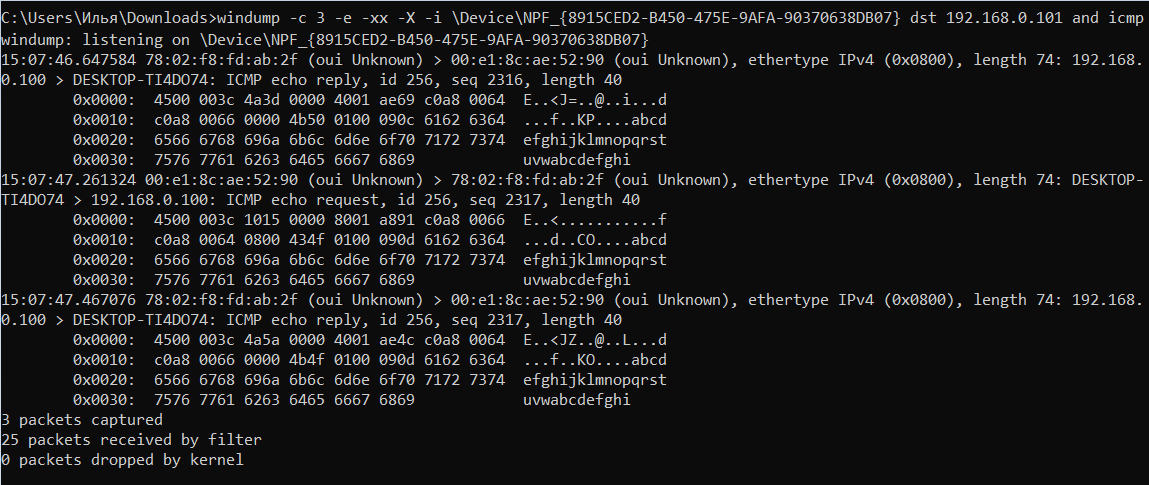
1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.



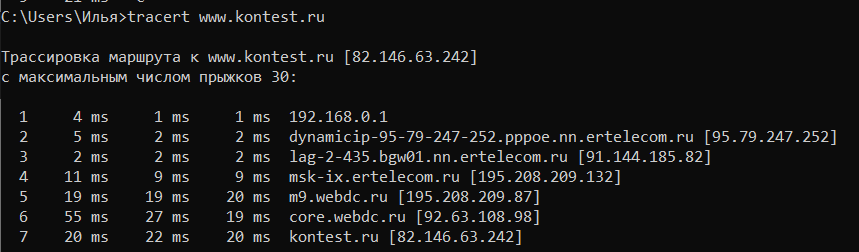
2. Запустить tcpdump в режиме перехвата широковещательного трафика. Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

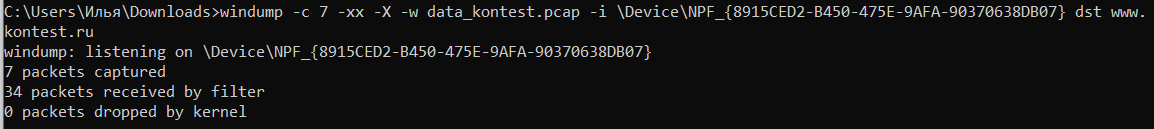


3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате(включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов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

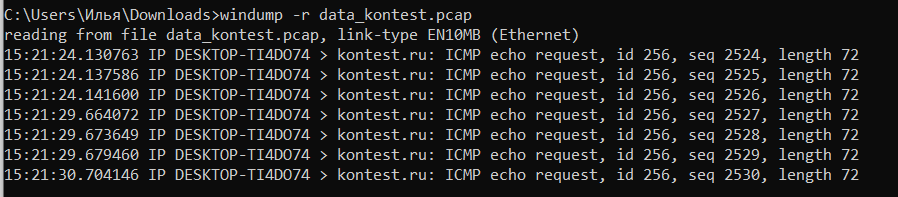


4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к узлу www.kontest.ru. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате(включая заголовок канального уровня). Количество захватываемых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



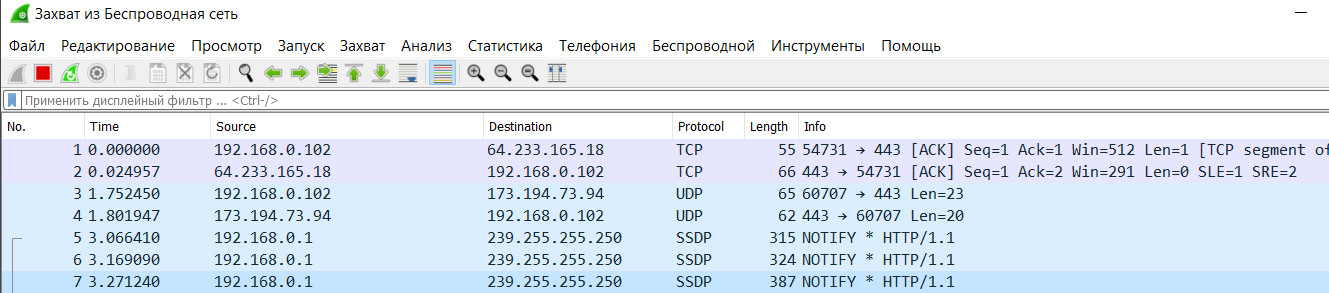


5. Прочесть программой tcpdump созданный в предыдущем пункте файл.

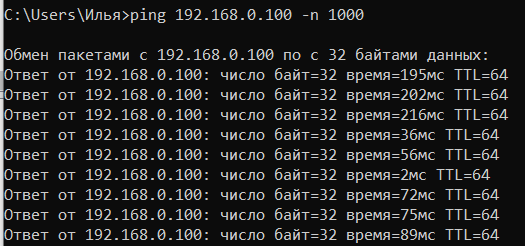


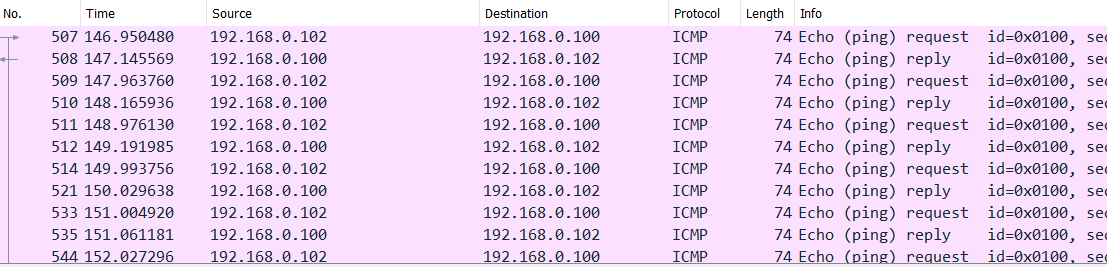
Работа с анализатором протоколов wireshark.

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

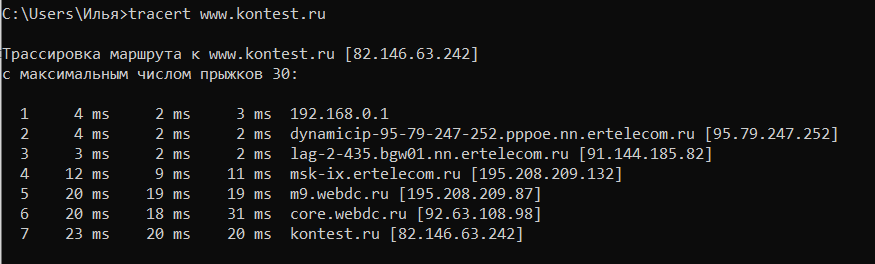


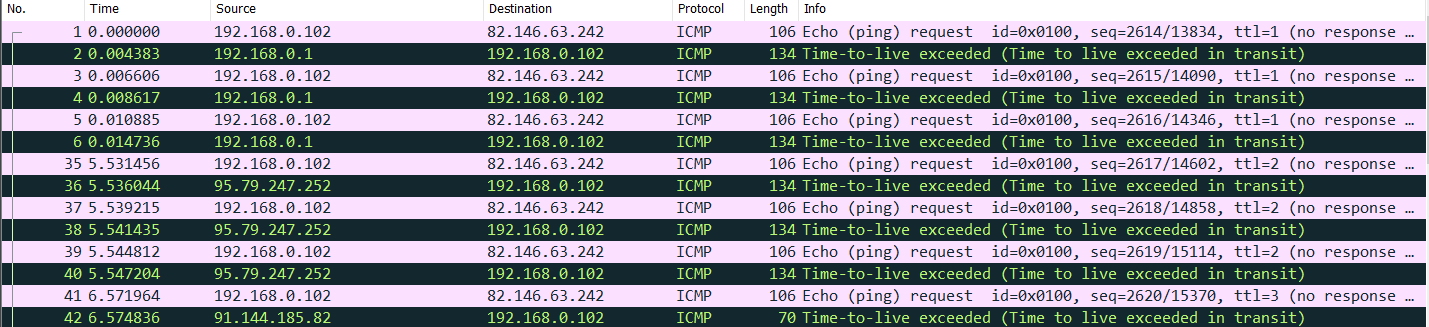
2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

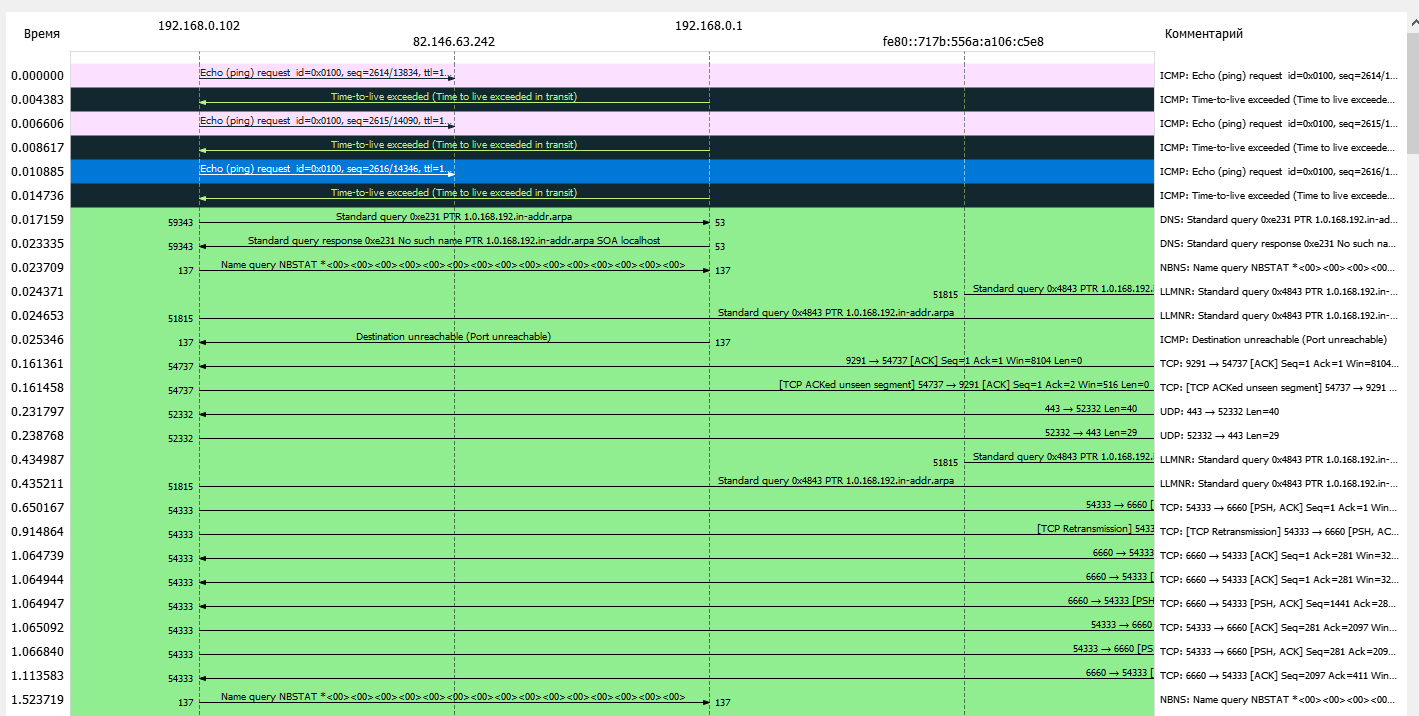


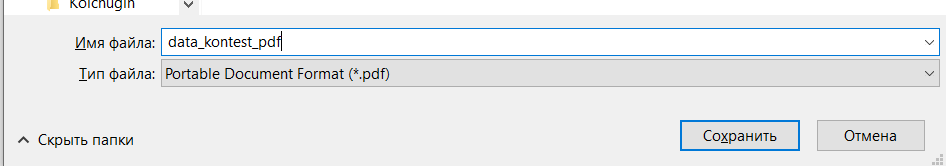


3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла, либо в виде изображения.









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

