НИУ ИТМО
Факультет программной инженерии и компьютерных технологий

Отчет по лабораторной работе №4

по дисциплине Компьютерные сети

Студент группы № P33151 Шипулин Павел Андреевич

Преподаватель Тропченко Андрей Александрович

Санкт-Петербург

2024

ЭТАПЫ И ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

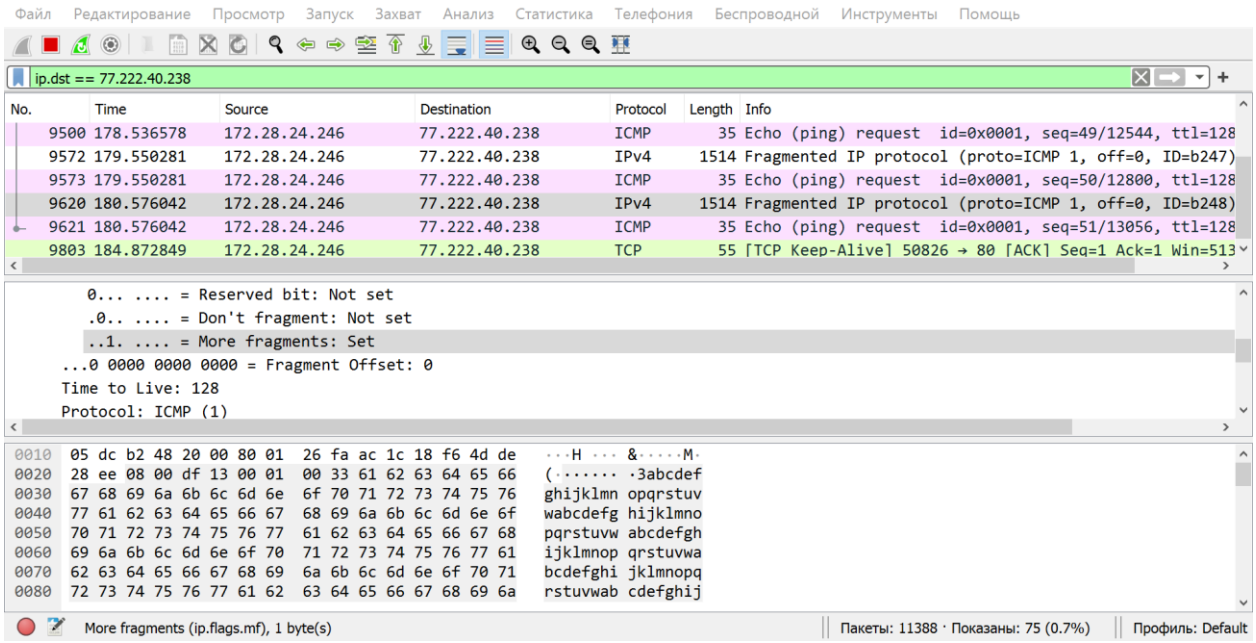
Этап 1. Анализ трафика утилиты ping

Необходимо отследить и проанализировать трафик, создаваемый утилитой ping, запустив её следующим образом из командной строки:

- «ping -l размер_пакета адрес_сайта_по_варианту».
- Например, «ping -l 2000 wireshark.org» (без кавычек).

В качестве «размера_пакета» необходимо поочерёдно использовать различные значения от 100 до 10000, самостоятельно выбрав шаг изменения. По результатам анализа собранной трассы, необходимо ответить на следующие вопросы и выполнить указанные задания.

```
C:\Users\User>ping -l 1472 shipulinpa.temp.swtest.ru

Обмен пакетами с shipulinpa.temp.swtest.ru [77.222.40.238] с 1472 байтами данных:
Ответ от 77.222.40.238: число байт=1472 время=4мс TTL=59
Ответ от 77.222.40.238: число байт=1472 время=4мс TTL=59
Ответ от 77.222.40.238: число байт=1472 время=3мс TTL=59
Ответ от 77.222.40.238: число байт=1472 время=241мс TTL=59

Статистика Ping для 77.222.40.238:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 241 мсек, Среднее = 63 мсек

C:\Users\User>ping -l 1473 shipulinpa.temp.swtest.ru

Обмен пакетами с shipulinpa.temp.swtest.ru [77.222.40.238] с 1473 байтами данных:
Ответ от 77.222.40.238: число байт=1473 время=3мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=3мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=5мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=5мс TTL=59

Статистика Ping для 77.222.40.238:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 5 мсек, Среднее = 4 мсек

C:\Users\User>
```



1. Имеет ли место фрагментация исходного пакета, какое поле на это указывает?

   Да. Поле More Fragments = 1.

2. Какая информация указывает, является ли фрагмент пакета последним или промежуточным?

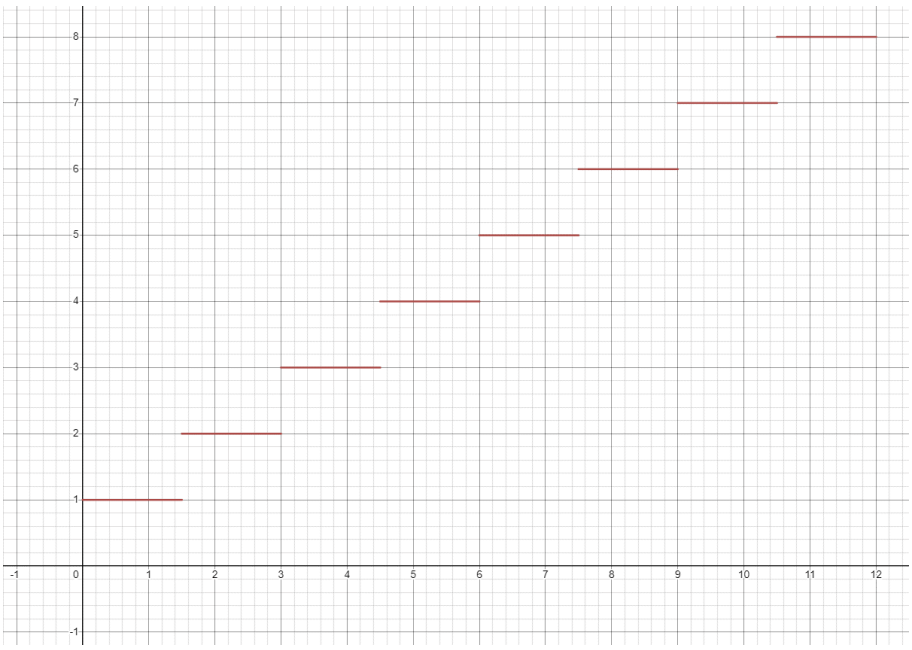
   Если поле More Fragments = 0, то пакет является последним.

3. Чему равно количество фрагментов при передаче ping-пакетов?

   Зависит от количества передаваемой информации, которая будет разбита на пакеты, у которых есть максимальный размер поля данных, равный 1472 байт (получено путём опыта).

$$\text{Количество пакетов} = \frac{\text{Весь объем данных}}{\text{максимальный объём данных пакета}}$$

4. Построить график, в котором на оси абсцисс находится размер пакета (килобайт), а по оси ординат – количество фрагментов, на которое был разделён каждый ping-пакет.



5. Как изменить поле TTL с помощью утилиты ping?

   ping -i <число>

```
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 241 мсек, Среднее = 63 мсек

C:\Users\User>ping -l 1473 shipulinpa.temp.swtest.ru

Обмен пакетами с shipulinpa.temp.swtest.ru [77.222.40.238] с 1473 байтами данных:
Ответ от 77.222.40.238: число байт=1473 время=3мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=3мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=5мс TTL=59
Ответ от 77.222.40.238: число байт=1473 время=5мс TTL=59

Статистика Ping для 77.222.40.238:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 3мсек, Максимальное = 5 мсек, Среднее = 4 мсек

C:\Users\User>ping -l 100 -i 1 shipulinpa.temp.swtest.ru

Обмен пакетами с shipulinpa.temp.swtest.ru [77.222.40.238] с 100 байтами данных:
Ответ от 172.28.16.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 172.28.16.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 172.28.16.1: Превышен срок жизни (TTL) при передаче пакета.
Ответ от 172.28.16.1: Превышен срок жизни (TTL) при передаче пакета.

Статистика Ping для 77.222.40.238:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)

C:\Users\User>
```

6. Что содержится в поле данных ping-пакета?

   Байты передаваемой информации. При использовании ping – это будут последовательные символы английского алфавита и прочие символы кодировки.

Этап 2. Анализ трафика утилиты tracert (traceroute)

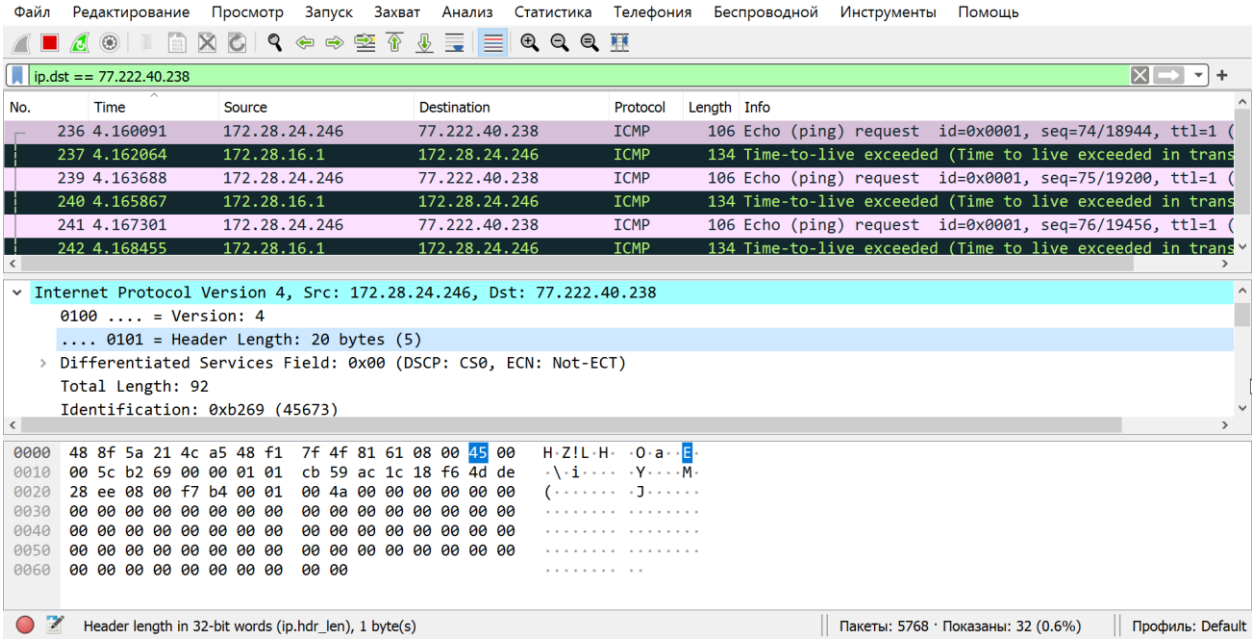
Необходимо отследить и проанализировать трафик, создаваемый утилитой tracert (или traceroute в Linux), запустив её следующим образом из командной строки:

- «tracert -d адрес_сайта_по_варианту»
- Например, tracert wireshark.org.

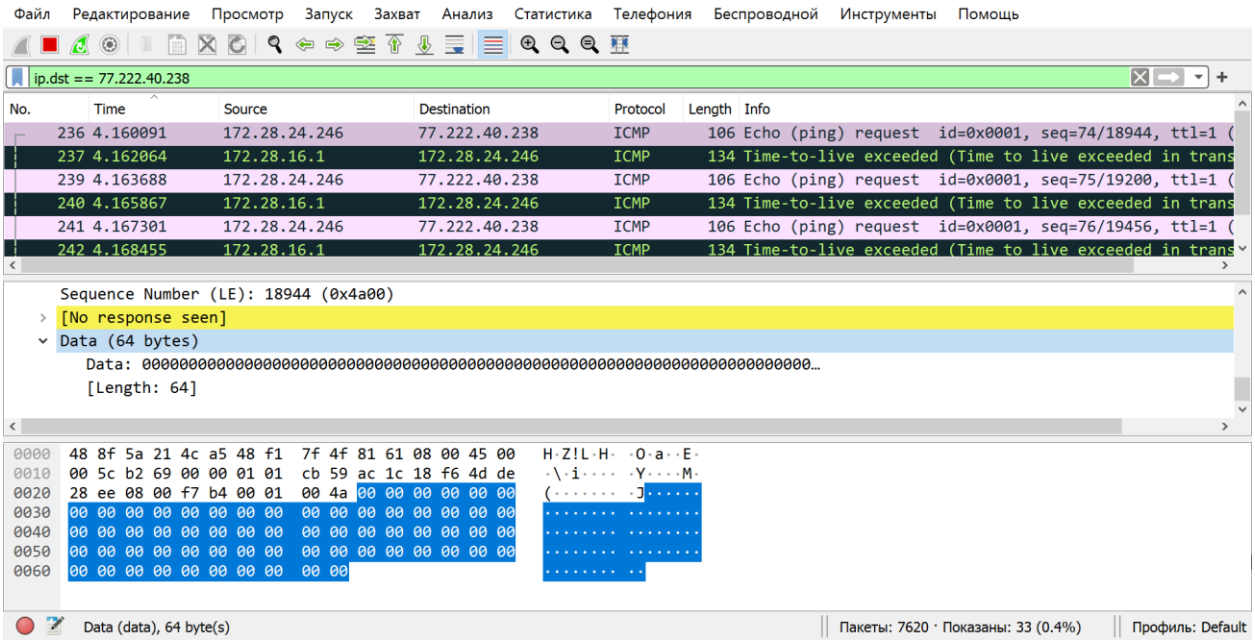
По результатам анализа собранной трассы, ответьте на следующие вопросы.

```
C:\Users\User>tracert -d shipulinpa.temp.swtest.ru

Трассировка маршрута к shipulinpa.temp.swtest.ru [77.222.40.238]
с максимальным числом прыжков 30:

  1     1 ms     1 ms     1 ms  172.28.16.1
  2     1 ms     2 ms     2 ms  77.234.199.66
  3     3 ms     3 ms     3 ms  87.248.228.102
  4     4 ms     3 ms     5 ms  185.1.152.93
  5     *        *        *     Превышен интервал ожидания для запроса.
  6     2 ms     2 ms     2 ms  77.222.40.238

Трассировка завершена.

C:\Users\User>tracert -d shipulinpa.temp.swtest.ru

Трассировка маршрута к shipulinpa.temp.swtest.ru [77.222.40.238]
с максимальным числом прыжков 30:

  1     2 ms     2 ms     1 ms  172.28.16.1
  2     2 ms     3 ms     2 ms  77.234.199.66
  3     3 ms     2 ms     2 ms  87.248.228.102
  4     8 ms     4 ms     6 ms  185.1.152.93
  5     *        4 ms     *     31.177.85.165
  6     3 ms     2 ms     4 ms  77.222.40.238

Трассировка завершена.

C:\Users\User>
```

1. Сколько байт содержится в заголовке IP? Сколько байт содержится в поле данных?



20 байт для заголовка.



64 байт для поля данных.

2. Как и почему изменяется поле TTL в следующих друг за другом ICMP пакетах tracert? Для ответа на этот вопрос нужно проследить изменение TTL при передаче по маршруту, состоящему из более чем двух хопов.

   Команда увеличивает TTL на 1 пока не будет получен ответ от следующего узла в маршруте.

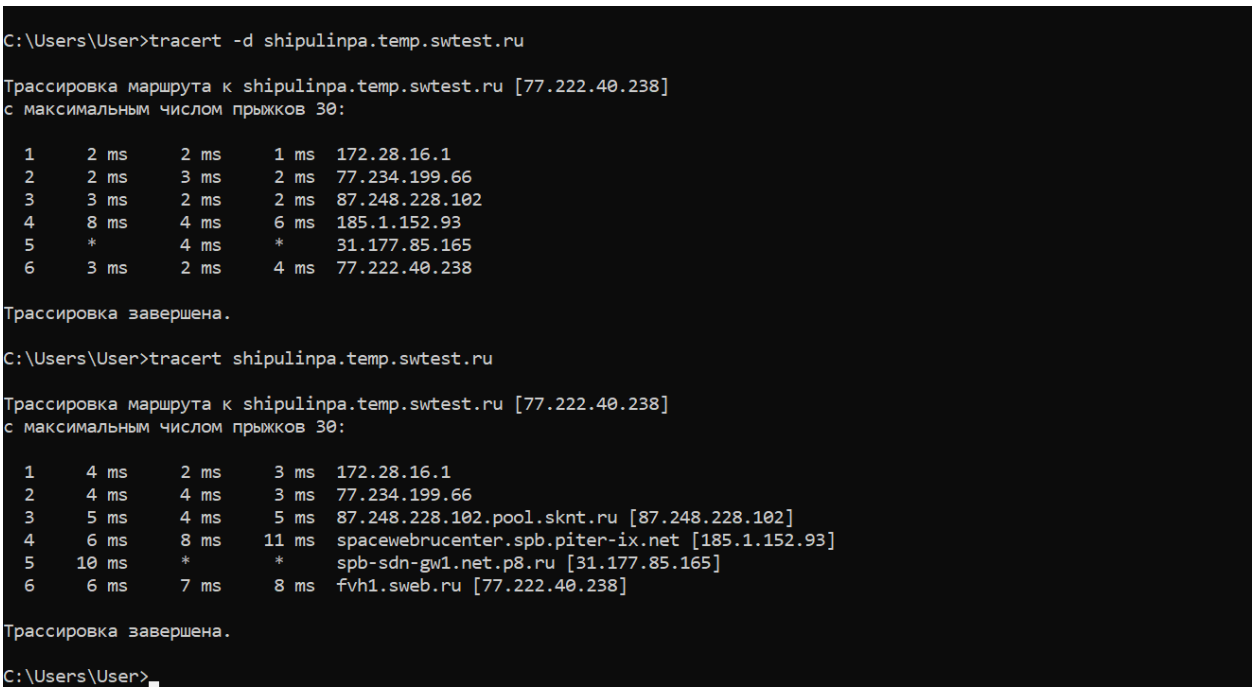
3. Чем отличаются ICMP-пакеты, генерируемые утилитой tracert, от ICMP пакетов, генерируемых утилитой ping (см. предыдущее задание).

Поле данных пакетов ICMP заполнено нулевыми байтами.

4. Чем отличаются полученные пакеты «ICMP reply» от «ICMP error» и зачем нужны оба этих типа ответов?

   Reply – ответ от узла. Error – произошла ошибка, например истекло время TTL.

5. Что изменится в работе tracert, если убрать ключ «-d»? Какой дополнительный трафик при этом будет генерироваться?



   Будут отображаться домены.

Этап 3. Анализ HTTP-трафика

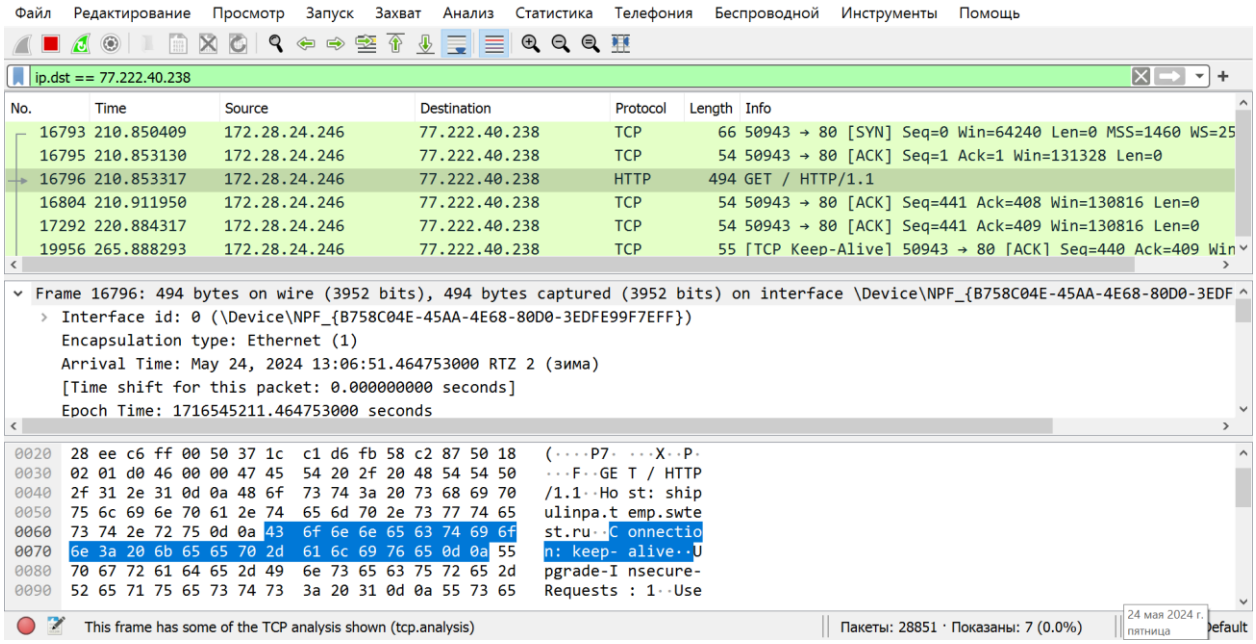
Необходимо отследить и проанализировать HTTP-трафик, создаваемый браузером при посещении Интернет-сайта, заданного по варианту. В списке захваченных пакетов необходимо проанализировать следующую пару HTTP сообщений (запрос-ответ):

- GET-сообщение от клиента (браузера);
- ответ сервера.

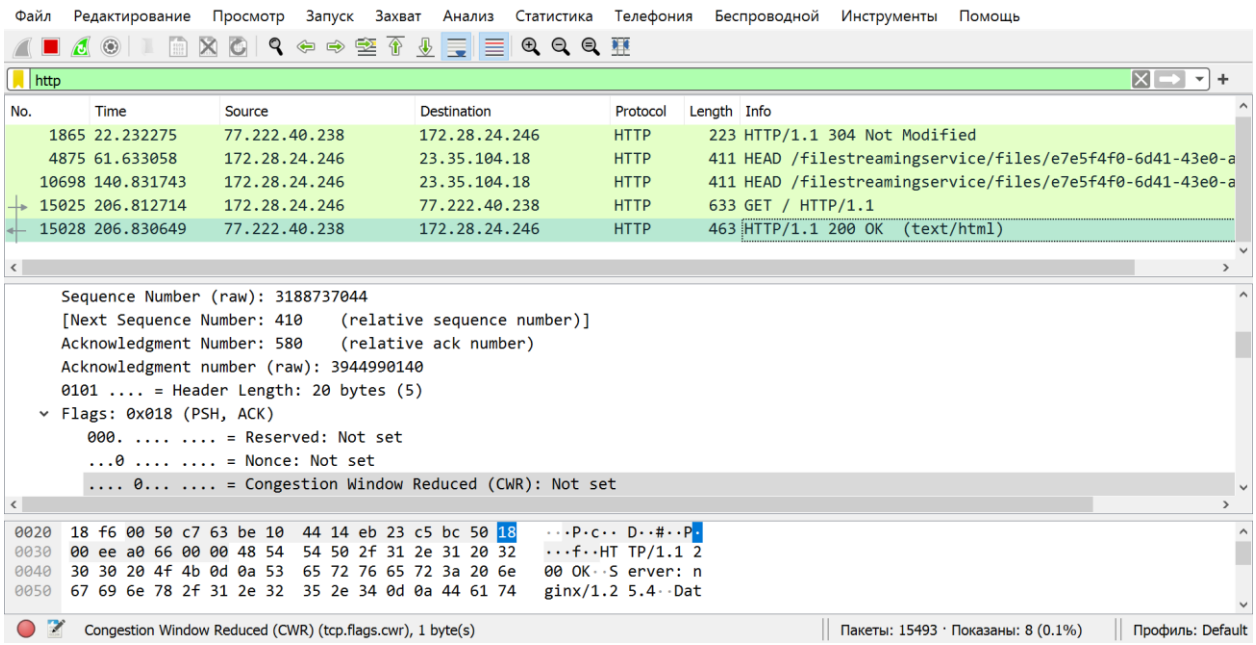
Для этого в поле с детальной информацией о пакете нужно развернуть строку «HTTP». Затем необходимо обновить страницу в браузере так, чтобы вместо «HTTP GET» был сгенерирован «HTTP CONDITIONAL GET» (так называемый «условный GET»). Условные запросы GET содержат поля

IfModified-Since, If-Match, If-Range и подобные, которые позволяют при повторном запросе не передавать редко изменяемые данные. В ответ на условный GET тело запрашиваемого ресурса передается только в том случае, если этот ресурс изменялся после даты «If-Modified-Since». Если ресурс не изменялся, сервер вернет код статуса «304 Not Modified».

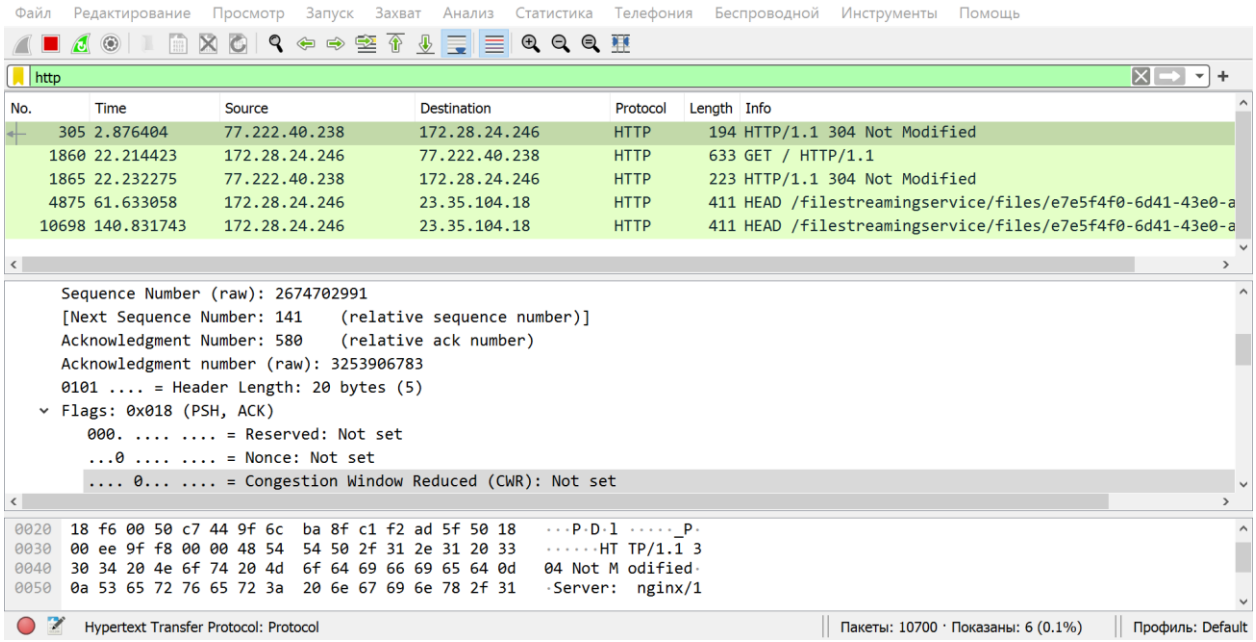
По результатам анализа собранной трассы покажите, каким образом протокол HTTP передавал содержимое страницы при первичном посещении страницы и при вторичном запросе-обновлении от браузера (т. е. при различных видах GET-запросов).



Сначала устанавливается TCP соединение, затем появляется ответ на GET запрос.



При обновлении содержимого страницы и её запросе – снова получаем HTTP OK с данными HTML.



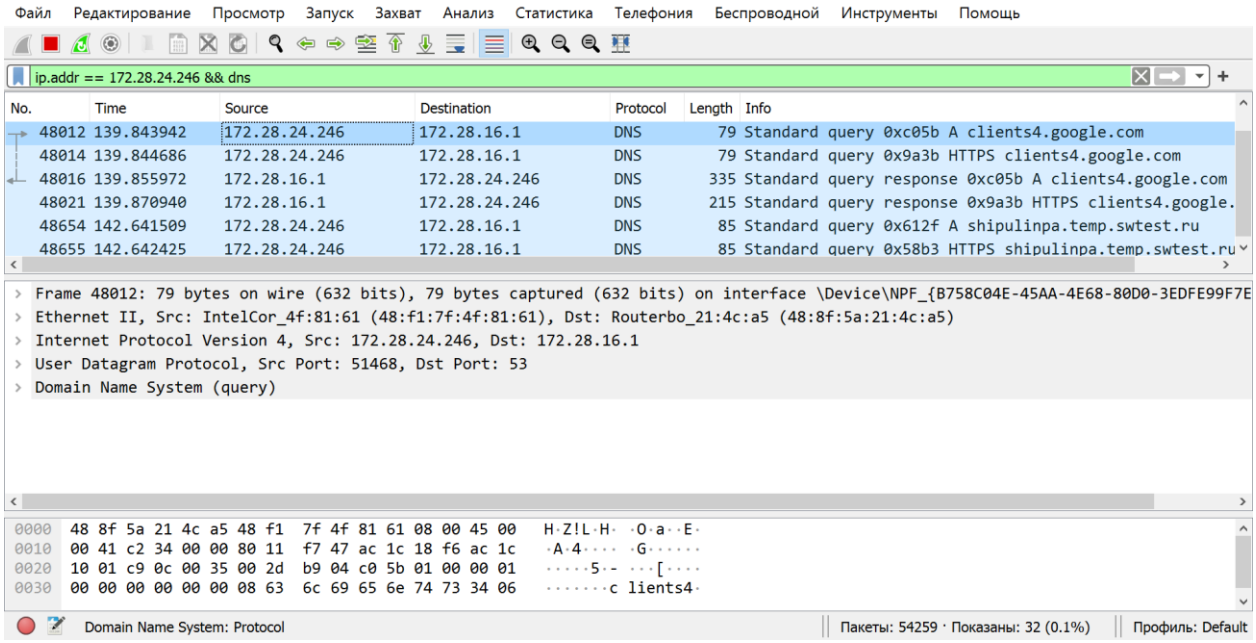
При повторном запросе страницы которая не обновлялась – компьютер получает “Not Modified”.

Этап 4. Анализ DNS-трафика

Необходимо отследить и проанализировать трафик протокола DNS, сгенерированный в результате выполнения следующих действий:

- настроить Wireshark-фильтр: «ip.addr == ваш_IP_адрес»;

- очистить кэш DNS с помощью команды ipconfig в командной строке: ipconfig /flushdns
- очистить кэш браузера;
- зайти на Интернет-сайт, заданный по варианту.



По результатам анализа собранной трассы, ответьте на следующие вопросы.

1. Почему адрес, на который отправлен DNS-запрос, не совпадает с адресом посещаемого сайта?

   Потому что компьютер не имеет достаточно информации про необходимый ресурс, и чтобы узнать о нём – обращается к маршрутизатору.

2. Какие бывают типы DNS-запросов?
   - Прямой – получить адрес по имени
   - Обратный – получить имя по адресу
   - Итеративный – ??
   - Рекурсивный – выполняется DNS сервером, чтобы найти домен.

3. В какой ситуации нужно выполнять независимые DNS-запросы для получения содержащихся на сайте изображений?

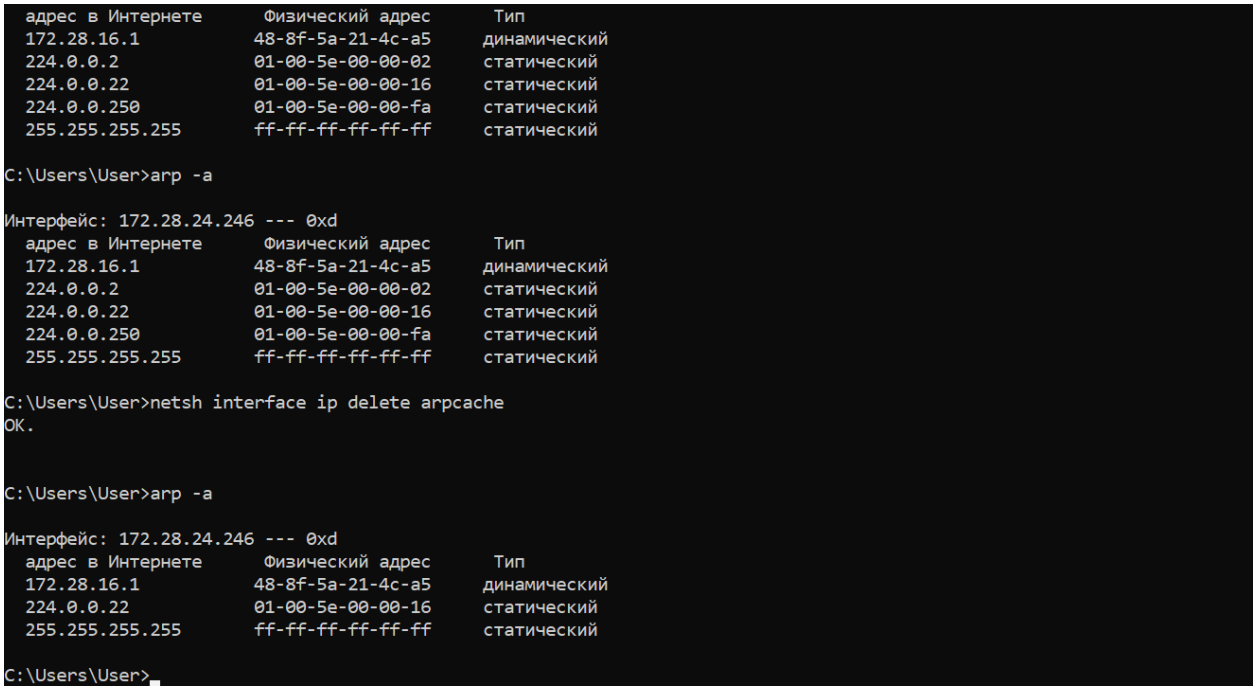
   Если эти изображения хранятся на другом ресурсе.

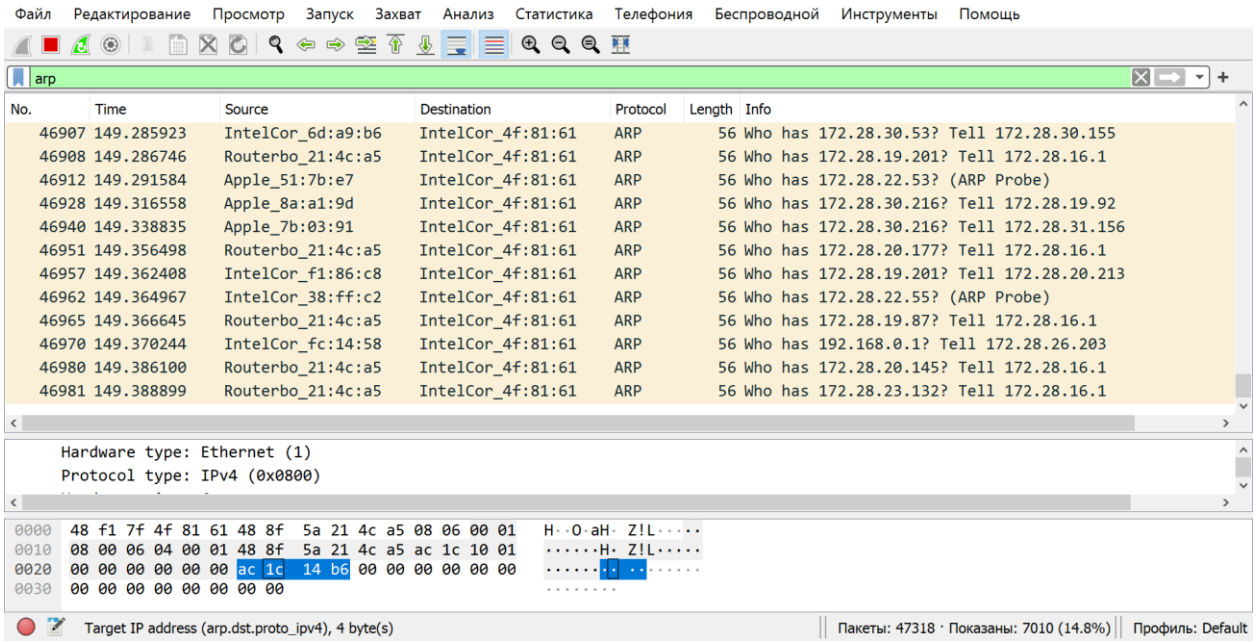
Этап 5. Анализ ARP-трафика

Необходимо отследить и проанализировать трафик протокола ARP, сгенерированный в результате выполнения следующих действий:

- очистить ARP-таблицу командой «netsh interface ip delete arpcache» (проверить очистилась ли таблица можно с помощью команды команды «arp -a», выводящей таблицу на экран);
- очистить кэш браузера;
- зайти на Интернет-сайт, заданный по варианту.

По результатам анализа собранной трассы, ответьте на следующие вопросы.





1. Какие MAC-адреса присутствуют в захваченных пакетах ARP протокола? Что означают эти адреса? Какие устройства они идентифицируют?

   Адрес отправителя (source) – маршрутизатор.
   Адрес получателя – компьютер, который делал запрос.

2. Какие MAC-адреса присутствуют в захваченных HTTP-пакетах и что означают эти адреса? Что означают эти адреса? Какие устройства они идентифицируют?

   Получатель ответа на GET запрос – мой компьютер.
   Отправитель – маршрутизатор.

3. Для чего ARP-запрос содержит IP-адрес источника?

   Чтобы те компьютеры, которые получат запрос могли сделать запись в ARP таблицу и не опрашивать снова.

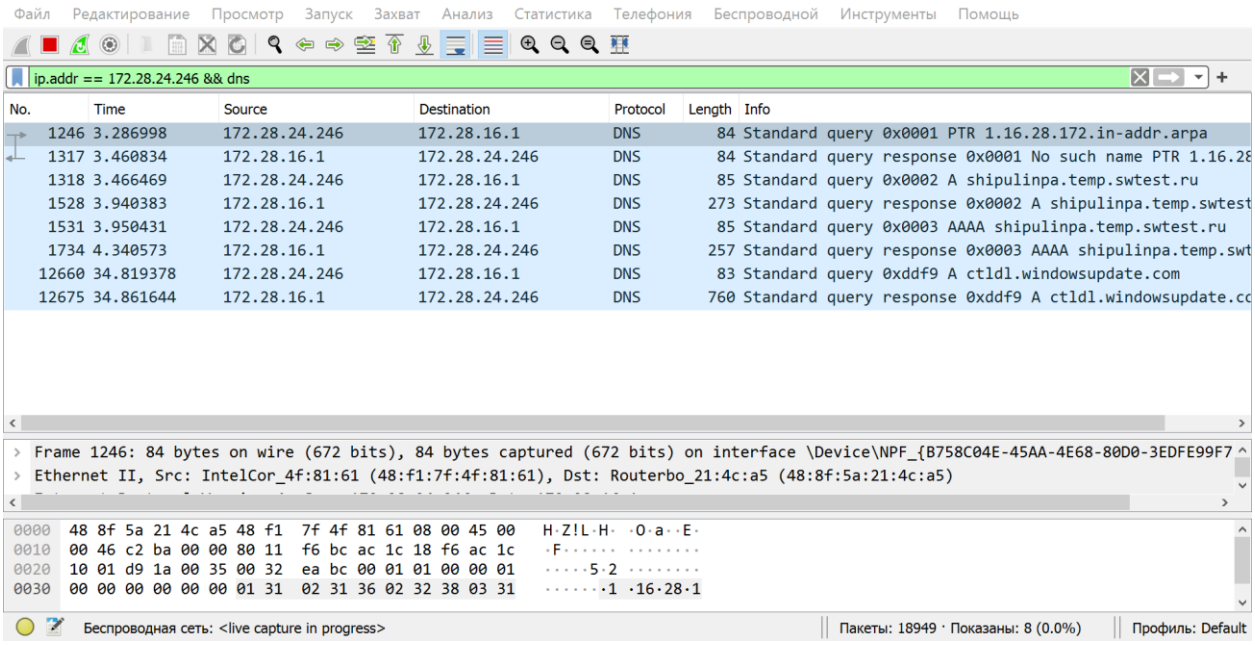
Этап 6. Анализ трафика утилиты nslookup

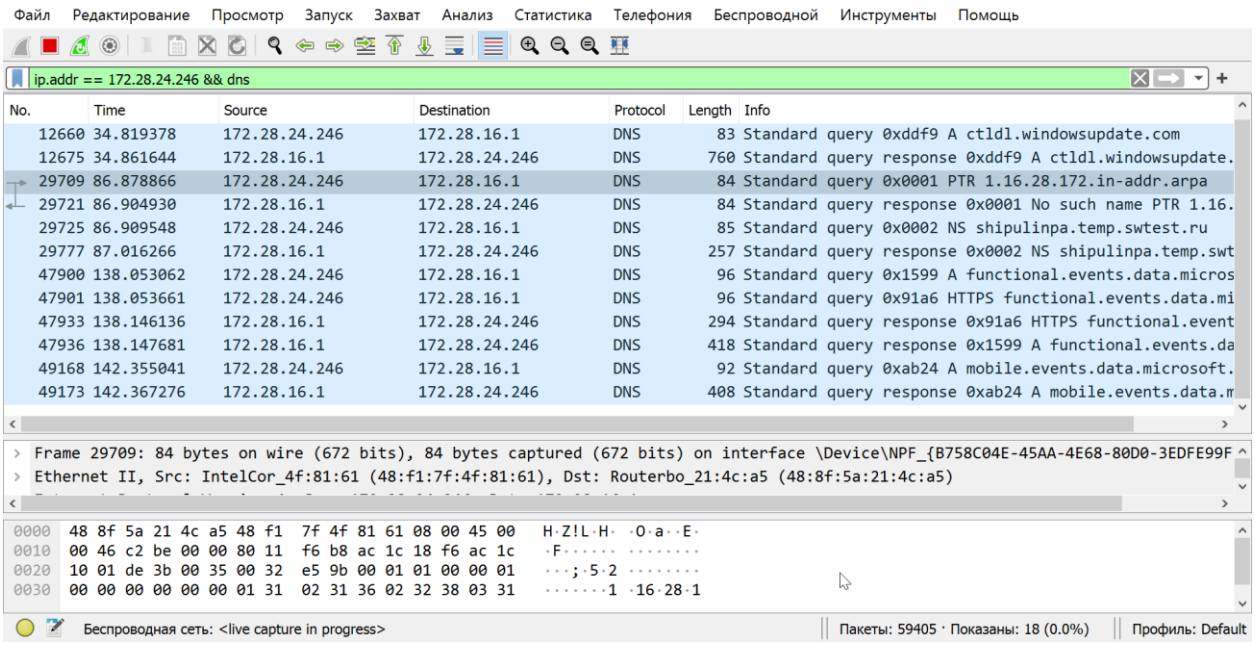
Это задание является необязательным, его необходимо выполнить только для желающих получить оценку «хорошо» или «отлично». Необходимо отследить и проанализировать трафик протокола DNS, сгенерированный в результате выполнения следующих действий:

1. Настроить Wireshark-фильтр: «ip.addr == ваш_IP_адрес».

2. Запустить в командной строке команду «nslookup адрес_сайта_по_варианту».
3. Дождаться отправки трёх DNS-запросов и трёх DNS-ответов (в работе нужно использовать только последние из них, т.к. первые два набора запросов/ответов специфичны для nslookup и не генерируются другими сетевыми приложениями).
4. Повторить предыдущие два шага, используя команду: «nslookup -type=NS имя_сайта_по_варианту».

По результатам анализа собранной трассы, ответьте на следующие вопросы.





```
Не заслуживающий доверия ответ:
╚ь :     shipulinpa.temp.swtest.ru
Address:  77.222.40.238


C:\Users\User>nslookup shipulinpa.temp.swtest.ru
╤xËтxË:  UnKnown
Address:  172.28.16.1

Не заслуживающий доверия ответ:
╚ь :     shipulinpa.temp.swtest.ru
Address:  77.222.40.238


C:\Users\User>nslookup -type=NS shipulinpa.temp.swtest.ru
╤xËтxË:  UnKnown
Address:  172.28.16.1

ru      nameserver = d.dns.ripn.net
ru      nameserver = b.dns.ripn.net
ru      nameserver = e.dns.ripn.net
ru      nameserver = f.dns.ripn.net
ru      nameserver = a.dns.ripn.net
d.dns.ripn.net  internet address = 194.190.124.17
b.dns.ripn.net  internet address = 194.85.252.62
e.dns.ripn.net  internet address = 193.232.142.17
f.dns.ripn.net  internet address = 193.232.156.17
a.dns.ripn.net  internet address = 193.232.128.6

C:\Users\User>
```

1. Чем различается трасса трафика в п.2 и п.4, указанных выше?

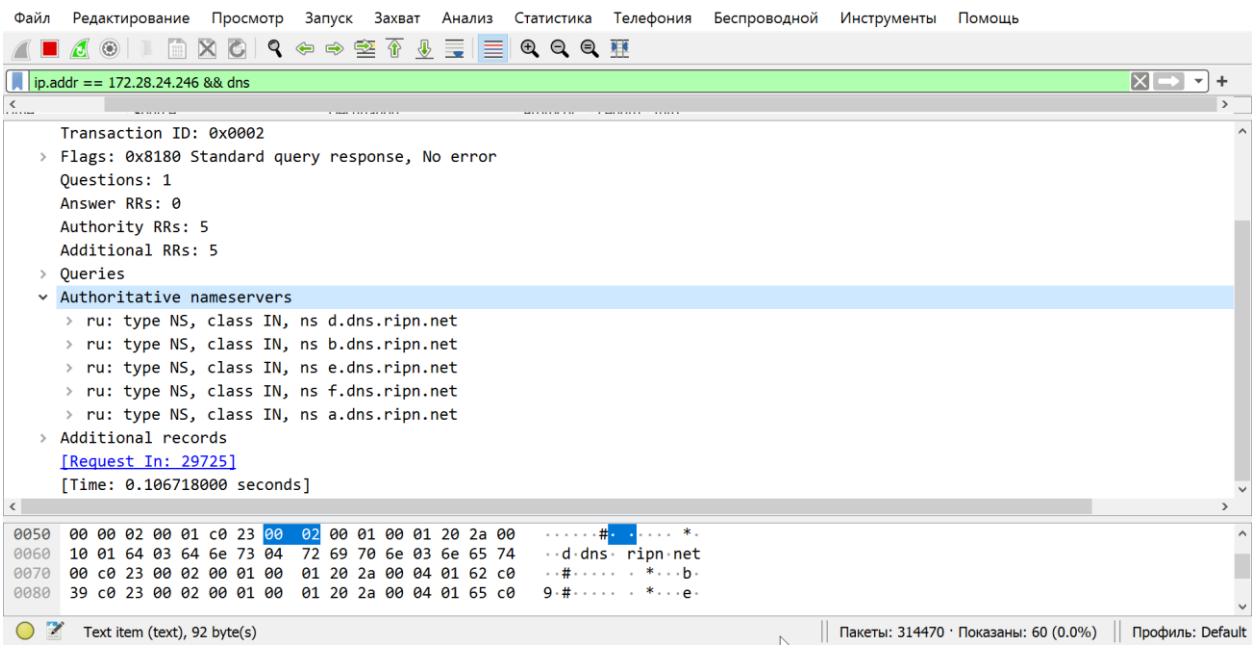
   Name Server – поле Answers будет пустым, но поле Authoritative nameservers будет содержать список серверов.

2. Что содержится в поле «Answers» DNS-ответа?

   ```
   ▾ Answers
     ▾ shipulinpa.temp.swtest.ru: type A, class IN, addr 77.222.40.238
         Name: shipulinpa.temp.swtest.ru
         Type: A (Host Address) (1)
         Class: IN (0x0001)
         Time to live: 548 (9 minutes, 8 seconds)
         Data length: 4
         Address: 77.222.40.238
   ```

   Для типа “A”: IPv4 адрес
   Для типа “AAAA”: IPv6 адрес
   Для типа “NS”: не содержит ничего в поле Answers

3. Каковы имена серверов, возвращающих авторитативный (authoritative) отклик?


Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
ip.addr == 172.28.24.246 && dns
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 0
Authority RRs: 5
Additional RRs: 5
Queries
Authoritative nameservers
ru: type NS, class IN, ns d.dns.ripn.net
ru: type NS, class IN, ns b.dns.ripn.net
ru: type NS, class IN, ns e.dns.ripn.net
ru: type NS, class IN, ns f.dns.ripn.net
ru: type NS, class IN, ns a.dns.ripn.net
Additional records
[Request In: 29725]
[Time: 0.106718000 seconds]
0050 00 00 02 00 01 c0 23 00 02 00 01 00 01 20 2a 00
0060 10 01 64 03 64 6e 73 04 72 69 70 6e 03 6e 65 74
0070 00 c0 23 00 02 00 01 00 01 20 2a 00 04 01 62 c0
0080 39 c0 23 00 02 00 01 00 01 20 2a 00 04 01 65 c0
Text item (text), 92 byte(s)
Пакеты: 314470 · Показаны: 60 (0.0%)
Профиль: Default