Федеральное государственное автономное образовательное учреждение высшего образования

Университет ИТМО

Дисциплина: Компьютерные сети

**Лабораторная работа №4**

## Выполнил:

Гуменник Петр Олегович

**Группа:** P3333

## Преподаватель:

Авксентьева Елена Юрьевна

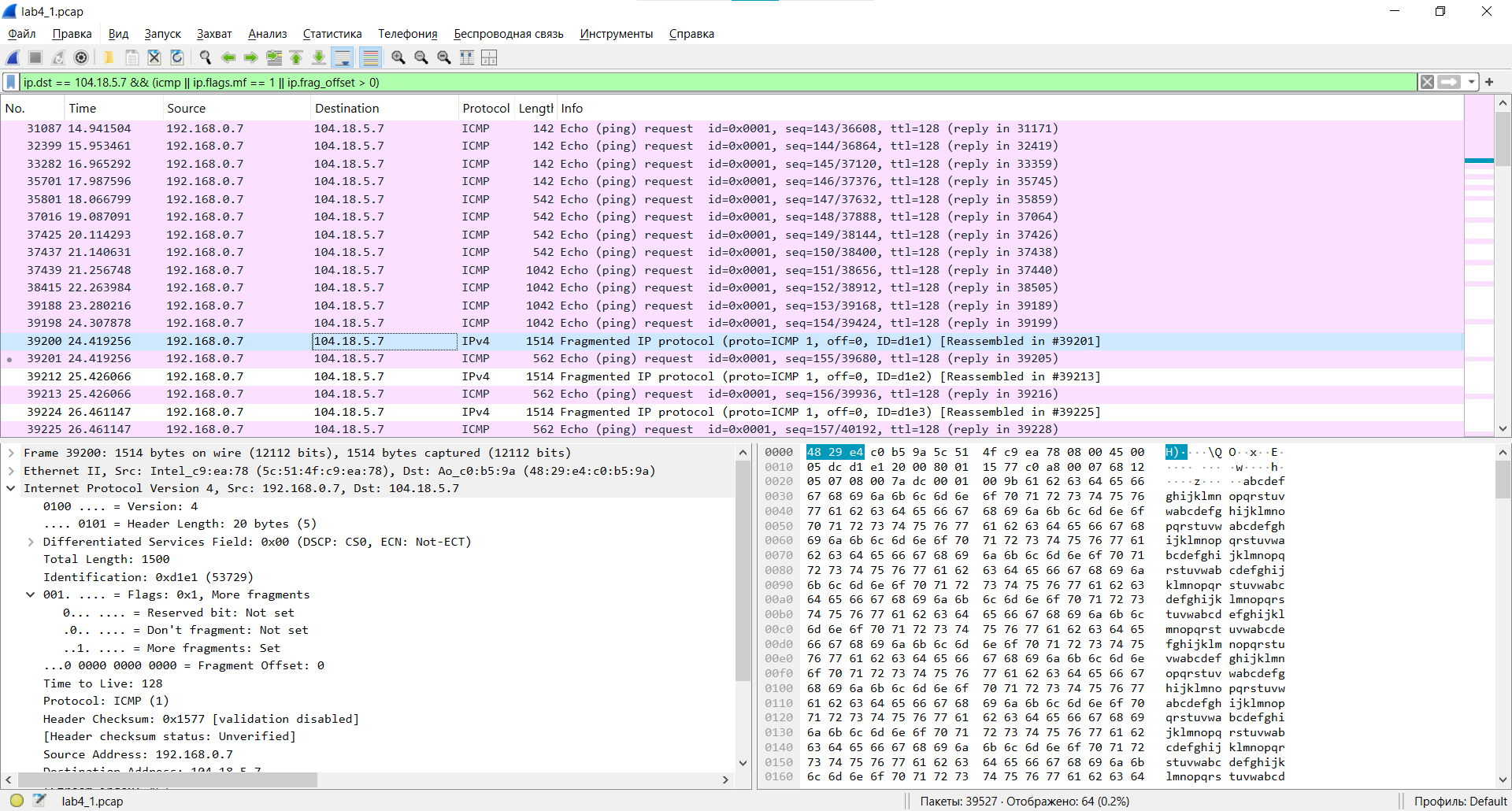
2025 г.

Санкт-Петербург

## Постановка задачи

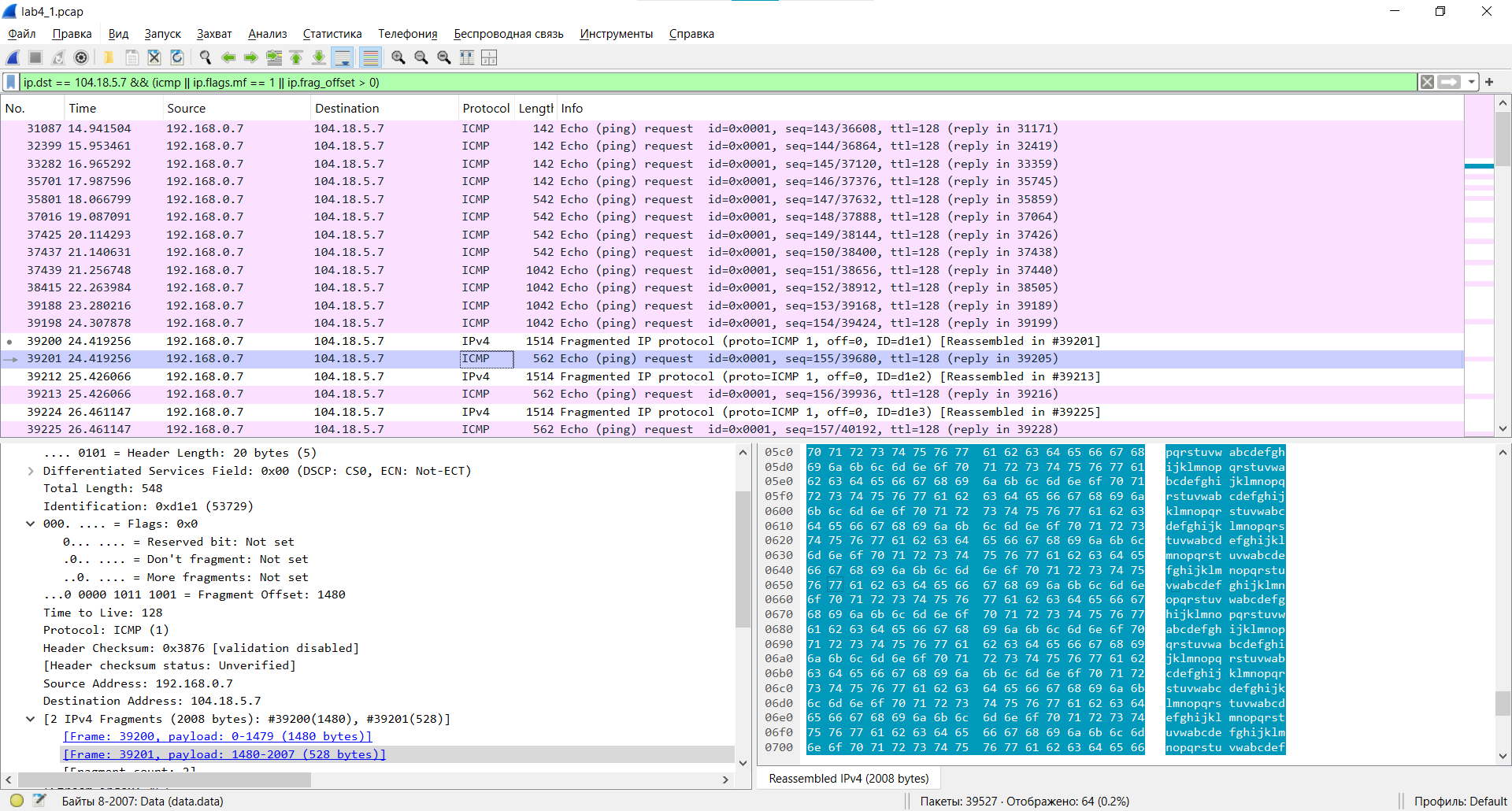
## Выполнение

1)

ip.dst == 104.18.5.7 && (icmp || ip.flags.mf == 1 || ip.frag\_offset > 0)  


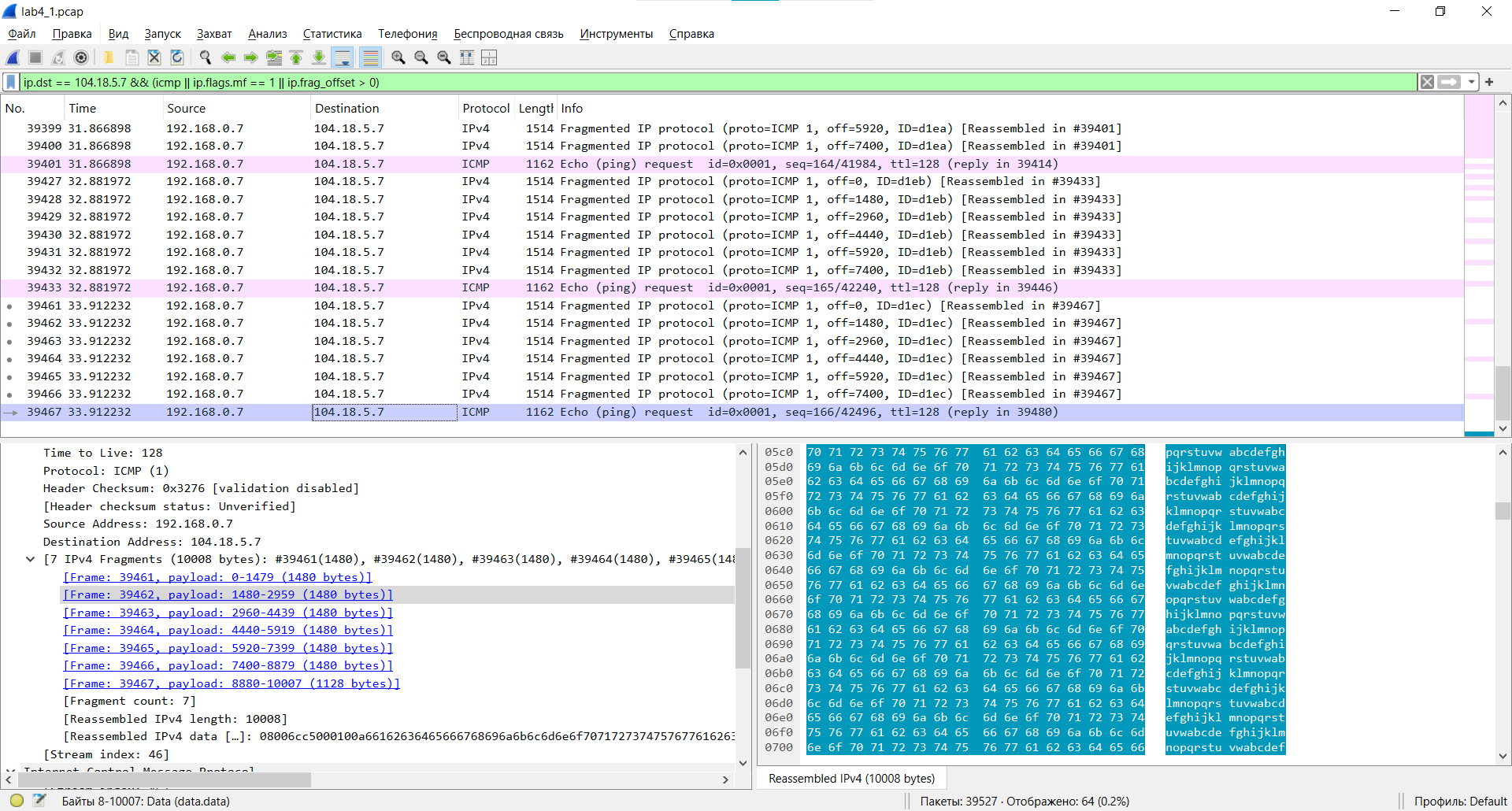
Фрагментация имеет место, если в IP-заголовке установлен флаг MF (More Fragments). На скриншоте видно, что значение MF = 1, что означает — данный пакет будет дополнен следующими фрагментами. Фактическое поле — **Flags** и **Fragment offset** в заголовке IPv4.

2)



Последний фрагмент всегда имеет MF = 0. Промежуточные — MF = 1. Это позволяет получателю понять, когда собраны все фрагменты. Поле Fragment offset показывает смещение в байтах и помогает восстановить порядок данных.

3)



На примере ping -l 10000 видно, что ICMP-запрос был разбит на 7 фрагментов. Это определяется по количеству IP-пакетов с одинаковым Identification. При MTU 1500 и полезной нагрузке ~1480 байт, 10000 байт разбивается на 7 частей.

4)

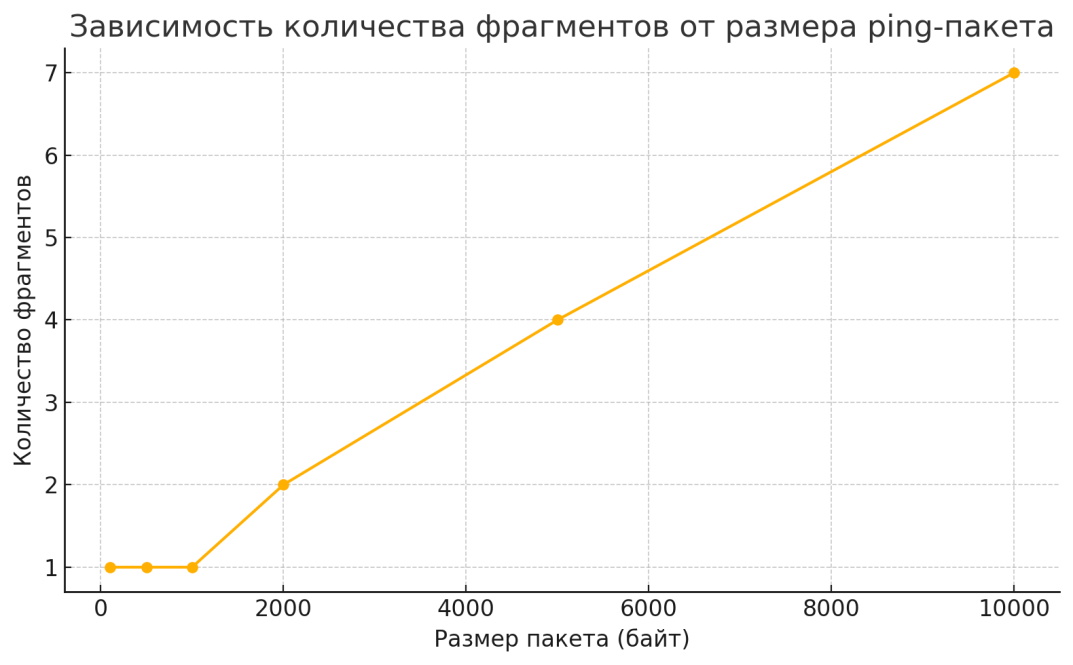


График демонстрирует линейную зависимость между размером ICMP-пакета и числом фрагментов, на которые он делится. Фрагментация начинается при превышении 1472 байт полезной нагрузки (MTU 1500 – заголовки IP/ICMP).

5)

ping -i 10 104.18.5.7

Поле TTL (Time to Live) можно изменить с помощью параметра -i. Это значение определяет максимальное количество хопов, которое может пройти пакет. Используется для контроля маршрута и диагностики сети.

6)

Поле данных содержит повторяющийся шаблон байтов в виде ASCII-букв: abcdefghijklmnopqrstuvwxyz.... Эти данные используются для проверки целостности передачи.

**Структура наблюдаемых пакетов (инкапсуляция):**

**Запрос Echo (ping):**

**Ethernet II:** содержит MAC-адреса источника и назначения

**IPv4:** задаёт IP-адреса, TTL, флаги фрагментации, идентификатор

**ICMP:** тип = 8 (Echo request), ID, sequence, данные

**Фрагментированный IP-пакет:**

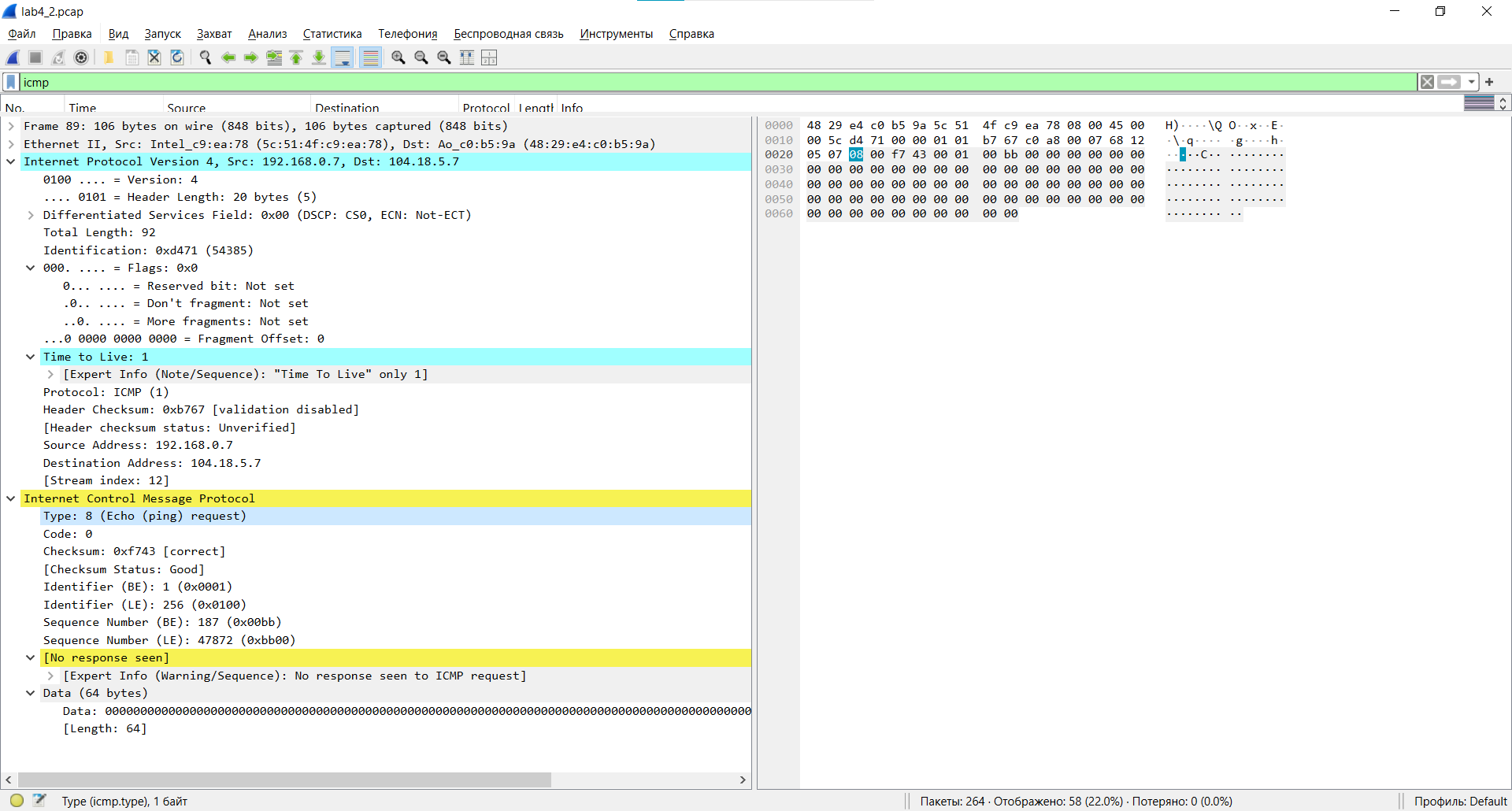
**Ethernet II**

**IPv4:** с флагами MF = 1, Fragment offset > 0, без ICMP-заголовка (кроме первого фрагмента)

Данные — только часть тела ICMP

## 4.2

1)



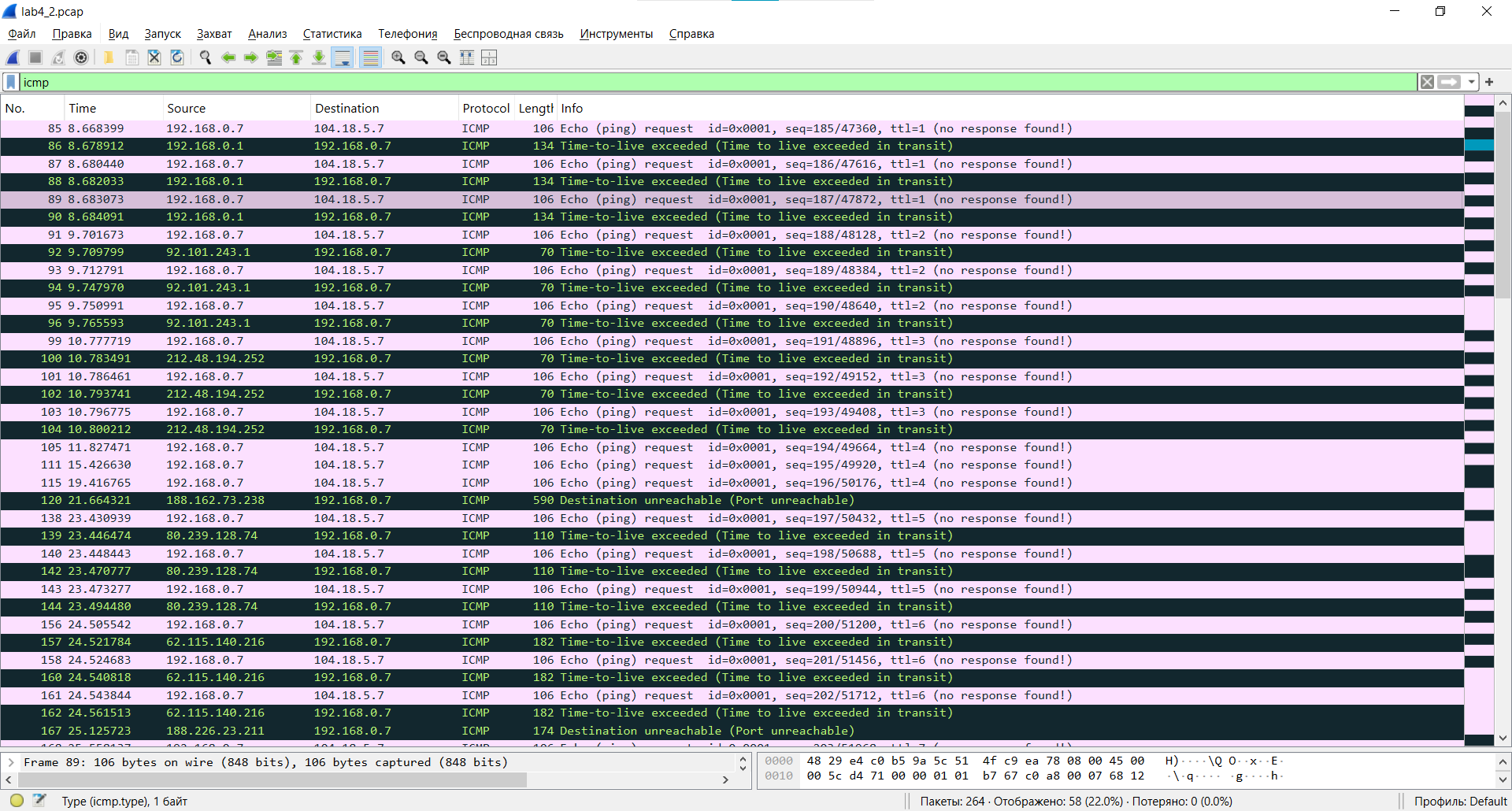
**IP-заголовок:**

* Размер: **20 байт**
* Это видно в поле Internet Protocol Version 4 → Header Length = 20 bytes  
  (значение 5 слов по 4 байта = 20)

**Поле данных:**

* ICMP-пакет содержит:
  + 8 байт заголовка ICMP (тип, код, чек-сумма, идентификатор, номер последовательности)
  + **64 байта данных** — как показано на скрине (все нули)
* Итого: **72 байта ICMP**

2)

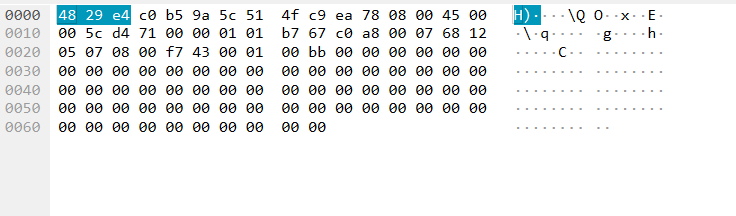


**Как**:  
TTL последовательно увеличивается: 1 → 2 → 3 → …  
Это видно в поле Time to Live в IP-заголовке каждого запроса.

**Почему**:  
Так работает tracert: он увеличивает TTL, чтобы на каждом шаге поймать ответ от очередного маршрутизатора. Когда TTL доходит до нуля — маршрутизатор сбрасывает пакет и отправляет Time Exceeded.

Пример:  
TTL=1 → ответ от первого хопа  
TTL=2 → ответ от второго хопа  
и т. д.

3)



**Общие черты:**

* И ping, и tracert используют ICMP Echo Request (тип 8)
* Разница — **в поведении и содержимом**

**Отличия:**

| **Характеристика** | **ping** | **tracert** |
| --- | --- | --- |
| TTL | Постоянный (обычно 128) | Последовательно: 1, 2, 3, … |
| Кол-во запросов | Обычно 4 | По 3 на каждый TTL |
| Ответы | Echo reply (тип 0) | Time Exceeded (тип 11) + Echo reply в конце |
| Данные ICMP | Повторяющийся шаблон/буквы | Все **нули** (как видно на скрине) |
| Результаты | Только «дошёл / не дошёл» | Показывает каждый хоп маршрута |

Также:

* tracert часто получает Time Exceeded или **No response** (если хоп молчит), чего нет в ping.

4)

**ICMP Echo Reply (тип 0):**

* Отправляется **конечным хостом**
* Говорит: "Запрос дошёл до меня"

**ICMP Time Exceeded (тип 11):**

* Отправляется **маршрутизатором**, если TTL = 0
* Говорит: "Пакет истёк по пути"

**Зачем нужны оба:**

* tracert строит маршрут по Time Exceeded — показывает каждый хоп
* Echo Reply — говорит, что маршрут завершён (достигли цели)

**Дополнительно:**

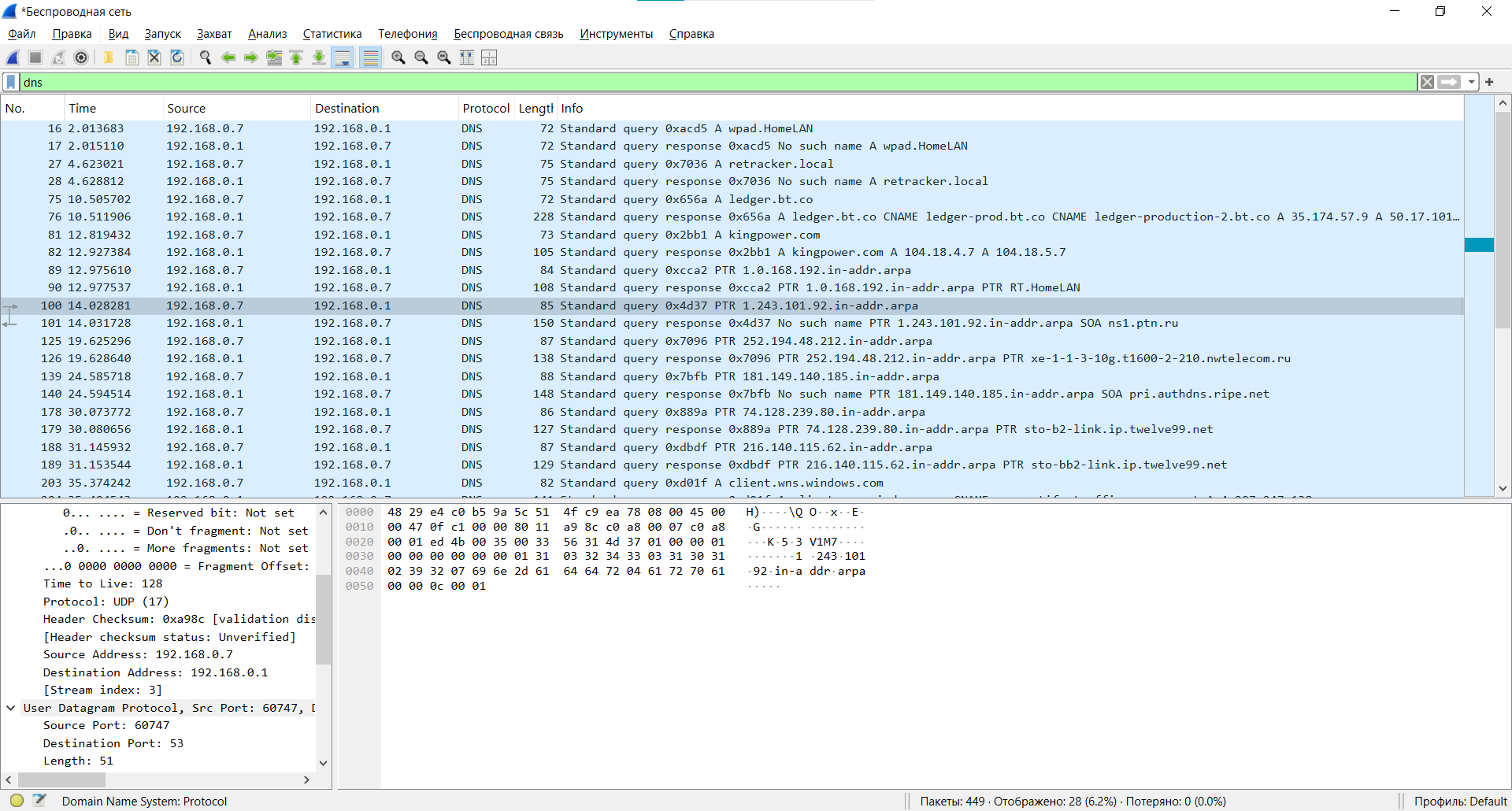
* Destination unreachable (port unreachable) — от целевого хоста, если порт недоступен (в Linux-реализациях, не в Windows)

5)

**Ключ -d** отключает DNS-резолвинг IP-адресов.

**Если убрать -d:**

* tracert будет пытаться разрешить IP-адреса хопов в доменные имена (обратное DNS)



**Дополнительный трафик:**

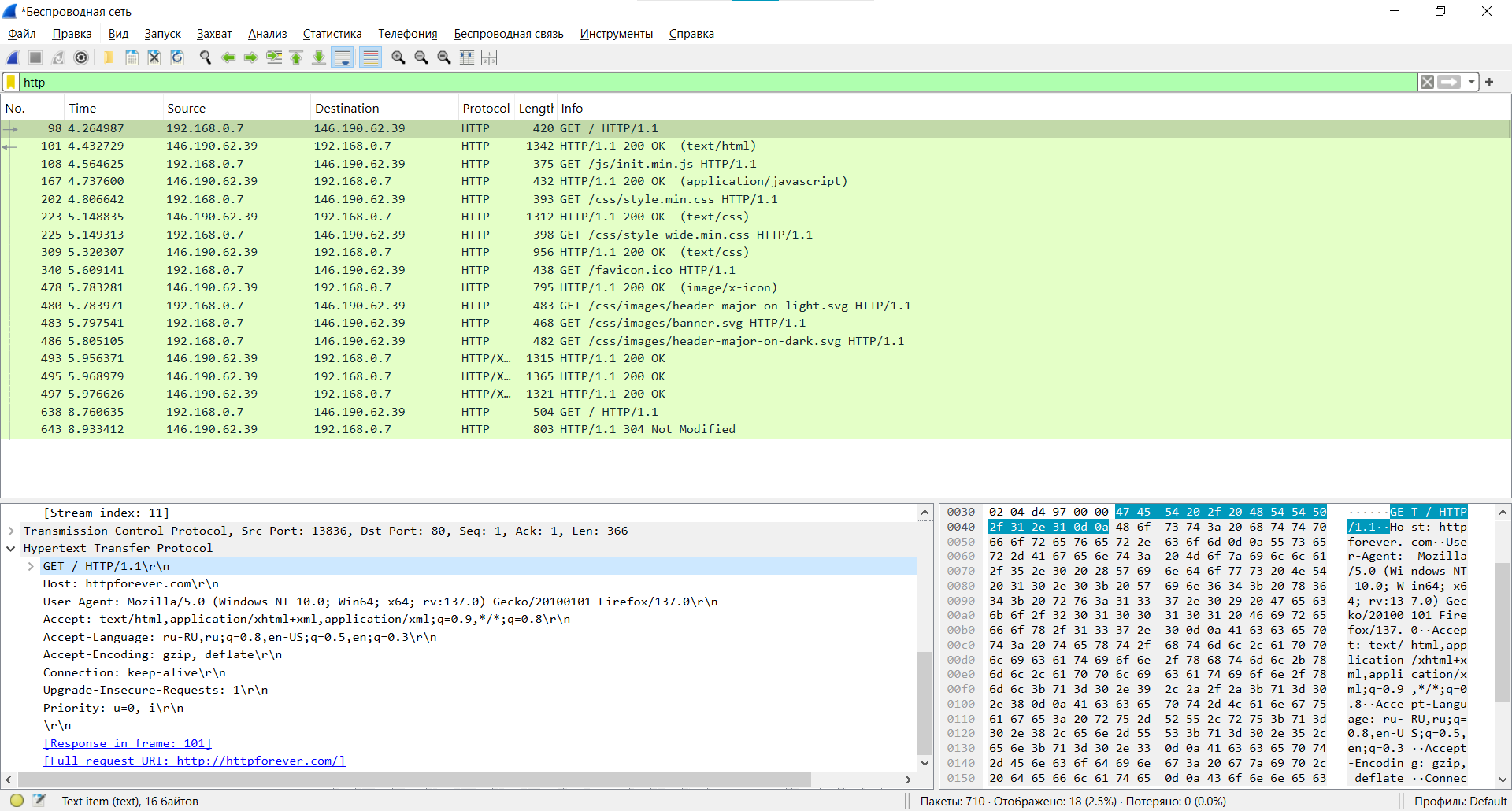
* Появятся **DNS-запросы по протоколу UDP порт 53**
* В Wireshark это видно по фильтру dns

**Зачем это нужно:**

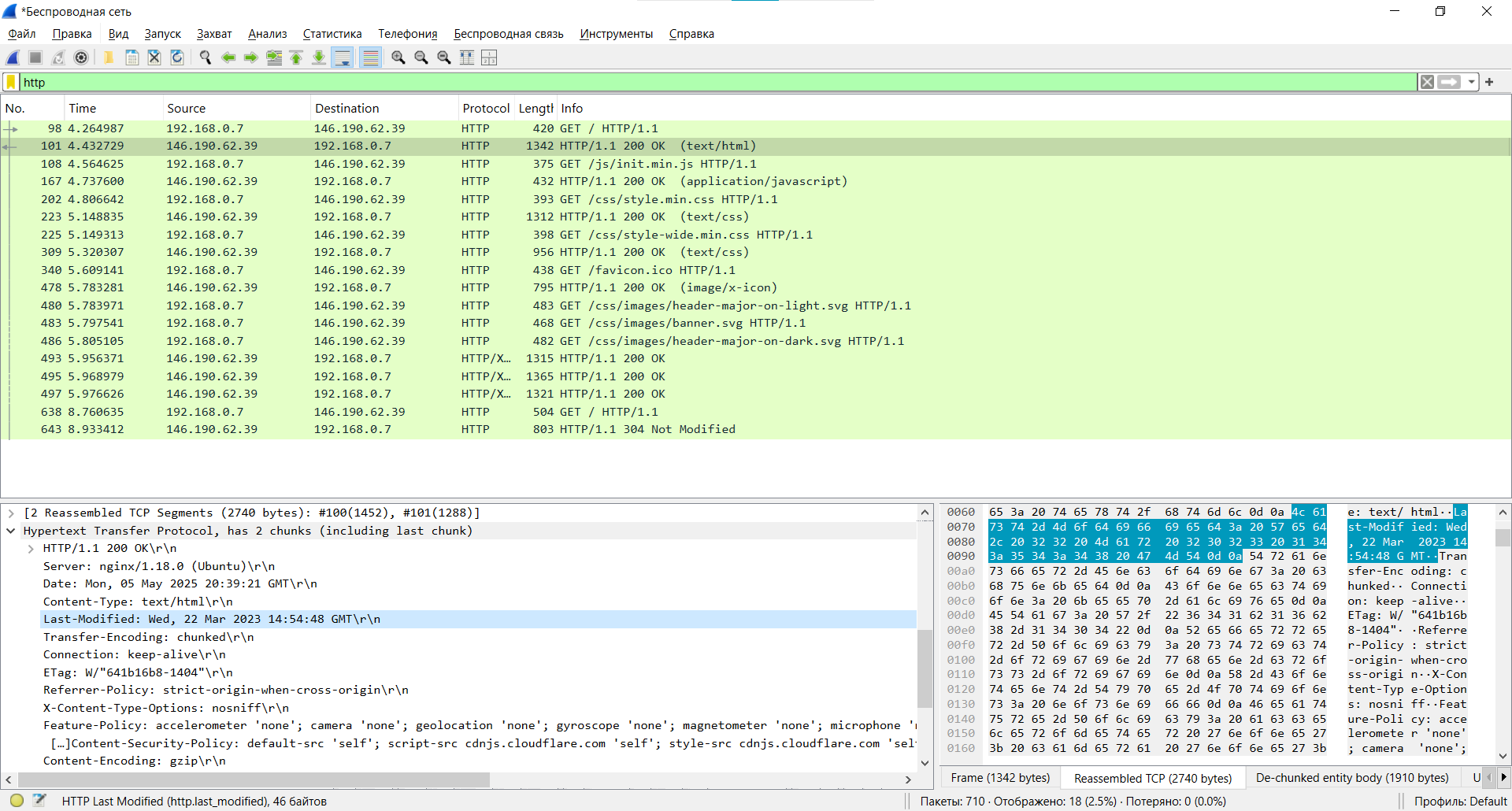
* Для удобства отображения — можно видеть домены, а не только IP
* Но при этом tracert может замедлиться

## 4.3

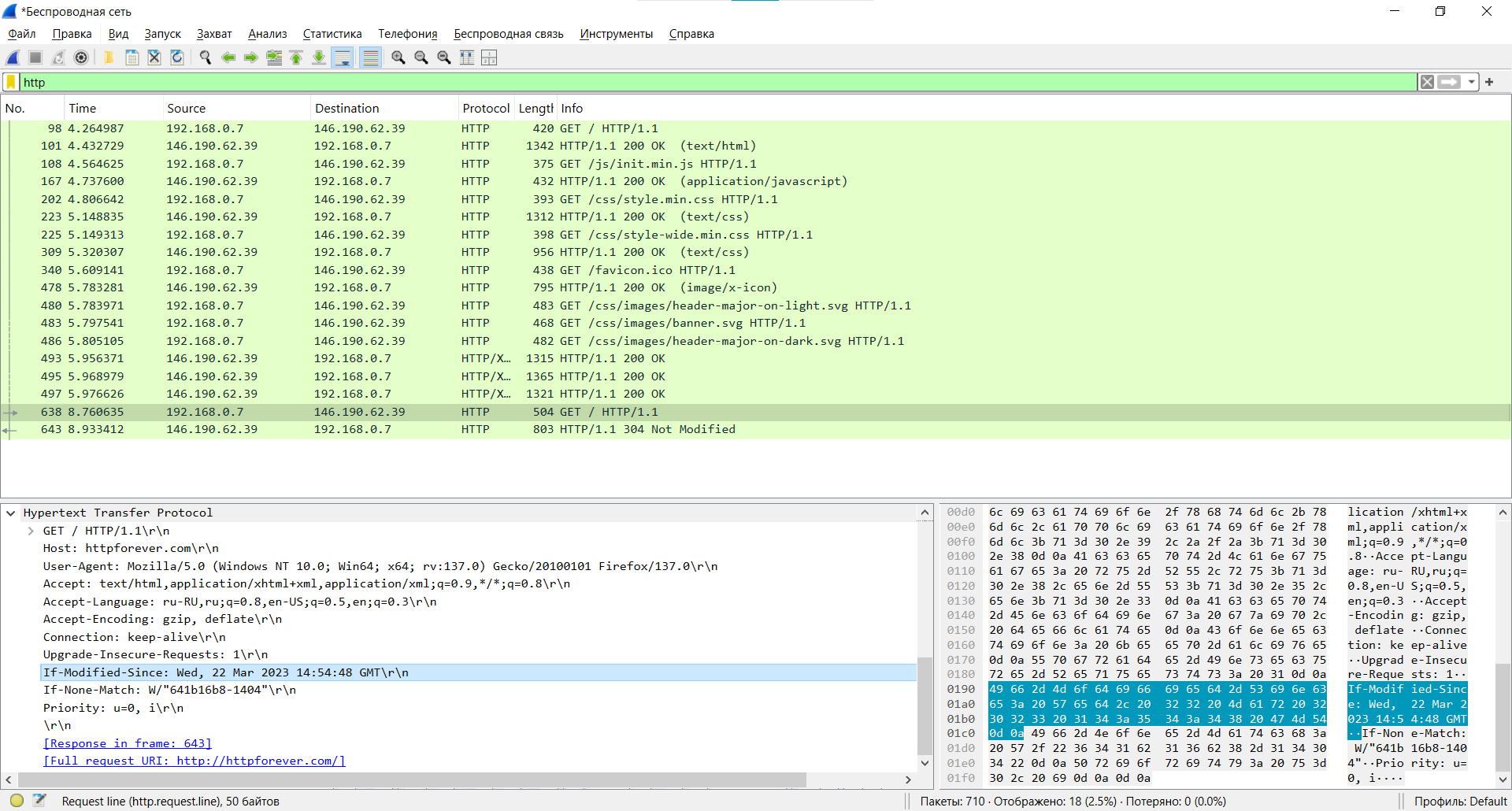
1) GET



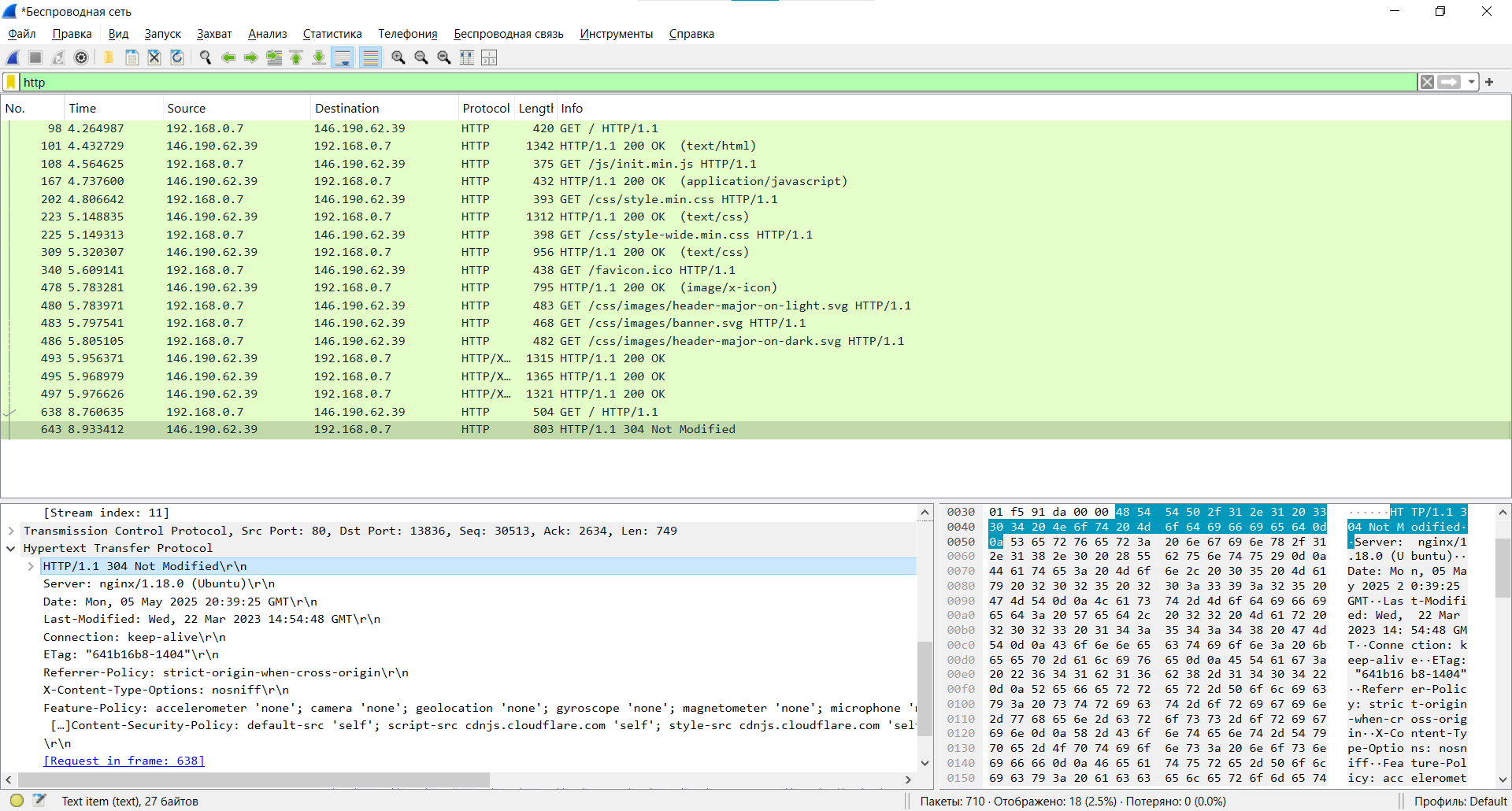
Браузер отправил обычный GET-запрос.  
Сервер ответил HTTP/1.1 200 OK и вернул содержимое HTML-страницы в теле ответа.



2) Conditional GET



Браузер отправил **Conditional GET** с заголовком If-Modified-Since.  
Сервер проверил дату последнего изменения ресурса и вернул:  
HTTP/1.1 304 Not Modified, **без тела**.



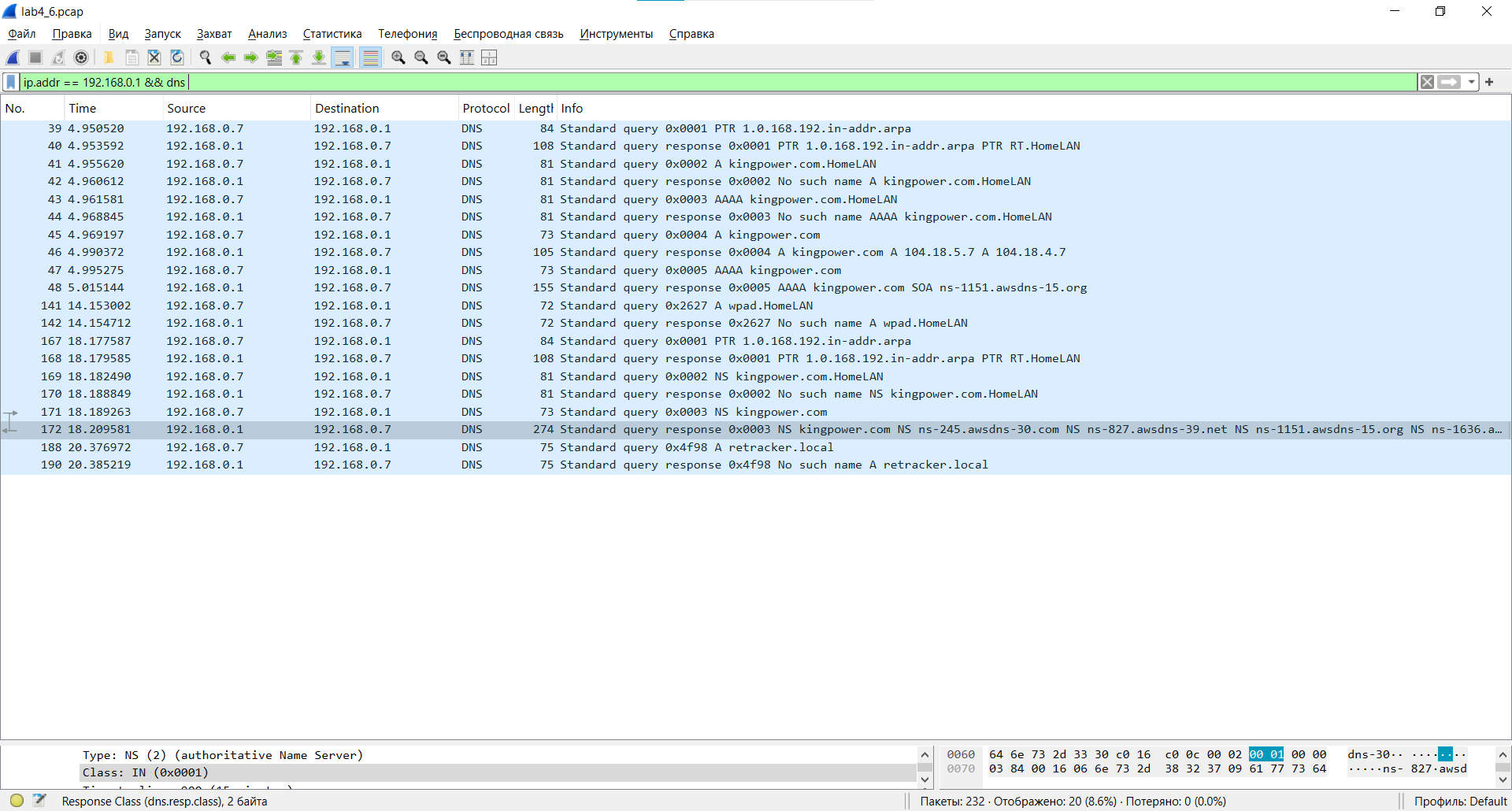
## 4.6

В данной части работы анализировался DNS-трафик, генерируемый утилитой nslookup при обращении к сайту kingpower.com.

**1. Подготовка и сбор данных**

В Wireshark был установлен фильтр:  
 ip.addr == 192.168.0.1 && dns  
Затем в командной строке были выполнены команды:  
 nslookup kingpower.com  
 nslookup -type=NS kingpower.com

**2. Наблюдаемый трафик**

  
В Wireshark были зафиксированы:  
- DNS-запрос типа A к домену kingpower.com, ответ: 104.18.4.7 и 104.18.5.7  
- DNS-запрос типа NS к домену kingpower.com, ответ: ns-827.awsdns-39.net, ns-1151.awsdns-15.org и др.

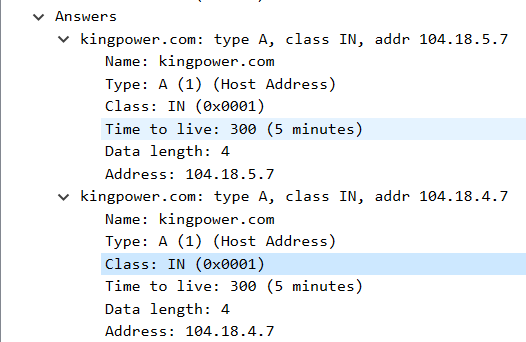
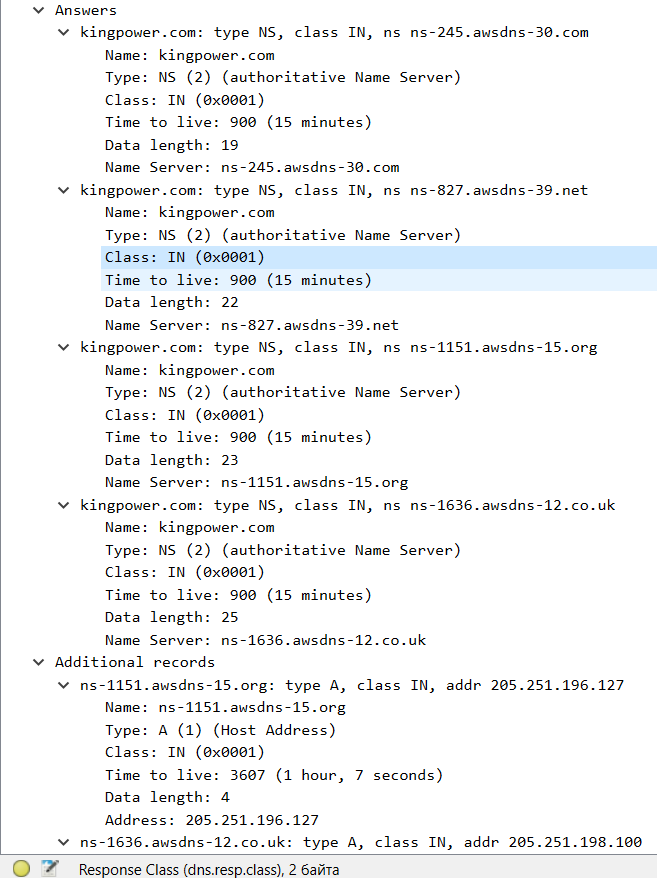
**Ответы на вопросы**

**1. Чем различается трасса трафика в п.2 и п.4?**

В п.2 (nslookup kingpower.com) происходит DNS-запрос типа A — клиент получает IP-адреса сайта.  
В п.4 (nslookup -type=NS kingpower.com) происходит DNS-запрос типа NS — клиент получает список NS-серверов зоны.

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

Ответ на запрос типа A:

  
Ответ на запрос типа NS:  


**3. Каковы имена серверов, возвращающих авторитативный отклик?**

Ответ содержит следующие имена NS-серверов:  
 ns-827.awsdns-39.net  
 ns-1151.awsdns-15.org  
 ns-245.awsdns-30.com  
 ns-1636.awsdns-12.co.uk

## Вывод:

В ходе лабораторной работы были проанализированы сетевые протоколы ICMP, HTTP и DNS. Утилита ping показала фрагментацию при передаче крупных пакетов, а tracert — механизм пошагового увеличения TTL для построения маршрута. При анализе HTTP-трафика зафиксированы обычный и условный GET-запросы, подтверждающие работу кеширования (ответ 304 Not Modified). Утилита nslookup позволила изучить запросы типов A и NS, а также определить авторитативные DNS-серверы сайта kingpower.com.