Home work 4

A.

-
```
intersection@i108588154:~$ nslookup z.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   z.com
Address: 163.44.130.37
```

-
```
intersection@i108588154:~$ nslookup -type=NS ethz.ch
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
ethz.ch nameserver = ns1.ethz.ch.
ethz.ch nameserver = ns2.ethz.ch.

Authoritative answers can be found from:
```

-
```
intersection@i108588154:~$ nslookup www.ox.ac.uk
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.ox.ac.uk
Address: 151.101.194.216
Name:   www.ox.ac.uk
Address: 151.101.66.216
Name:   www.ox.ac.uk
Address: 151.101.130.216
Name:   www.ox.ac.uk
Address: 151.101.2.216
```

Один:

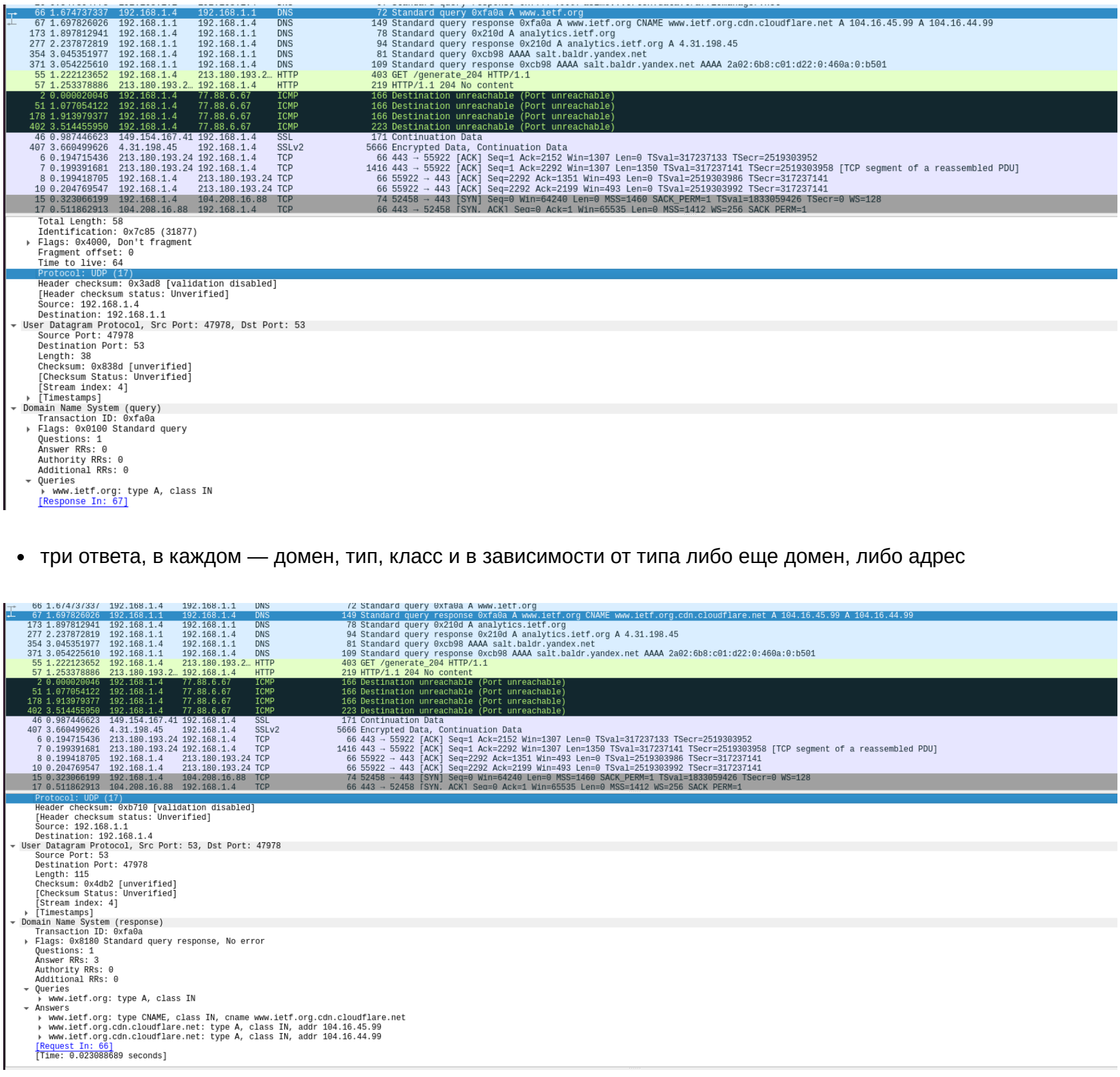
```
intersection@i108588154:~$ nslookup spbu.ru
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   spbu.ru
Address: 178.177.3.9
```

Б.

- Protocol: UDP (17)

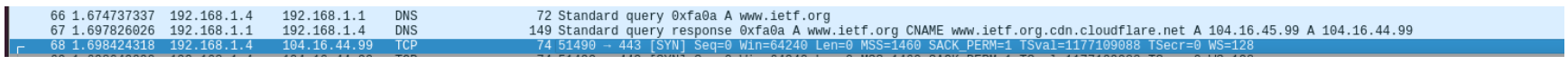
```
   66 1.674787337  192.168.1.4    192.168.1.1    DNS          72 Standard query 0xfa0a A www.ietf.org
   67 1.697826026  192.168.1.1    192.168.1.4    DNS         149 Standard query response 0xfa0a A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
  173 1.897812941  192.168.1.4    192.168.1.1    DNS          78 Standard query 0x210d A analytics.ietf.org
  277 2.237872819  192.168.1.1    192.168.1.4    DNS          94 Standard query response 0x210d A analytics.ietf.org A 4.31.198.45
  354 3.045351977  192.168.1.4    192.168.1.1    DNS          81 Standard query 0xcb98 AAAA salt.baldr.yandex.net
  371 3.054225610  192.168.1.1    192.168.1.4    DNS         109 Standard query response 0xcb98 AAAA salt.baldr.yandex.net AAAA 2a02:6b8:c01:d22:0:460a:0:b501
   55 1.222123652  192.168.1.4    213.180.193.2… HTTP        403 GET /generate_204 HTTP/1.1
   57 1.253378886  213.180.193.2… 192.168.1.4    HTTP        219 HTTP/1.1 204 No content
    2 0.000020046  192.168.1.4    77.88.6.67     ICMP        166 Destination unreachable (Port unreachable)
   51 1.077054122  192.168.1.4    77.88.6.67     ICMP        166 Destination unreachable (Port unreachable)
  178 1.913979377  192.168.1.4    77.88.6.67     ICMP        166 Destination unreachable (Port unreachable)
  402 3.514455950  192.168.1.4    77.88.6.67     ICMP        223 Destination unreachable (Port unreachable)
   46 0.987446623  149.154.167.41 192.168.1.4    SSL         171 Continuation Data
  407 3.660499626  4.31.198.45    192.168.1.4    SSLv2      5666 Encrypted Data, Continuation Data
    6 0.194715436  213.180.193.24 192.168.1.4    TCP          66 443 → 55922 [ACK] Seq=1 Ack=2152 Win=1307 Len=0 TSval=317237133 TSecr=2519303952
    7 0.199391681  213.180.193.24 192.168.1.4    TCP        1416 443 → 55922 [ACK] Seq=1 Ack=2292 Win=1307 Len=1350 TSval=317237141 TSecr=2519303958 [TCP segment of a reassembled PDU]
    8 0.199418705  192.168.1.4    213.180.193.24 TCP          66 55922 → 443 [ACK] Seq=2292 Ack=1351 Win=493 Len=0 TSval=2519303986 TSecr=317237141
   10 0.204769547  192.168.1.4    213.180.193.24 TCP          66 55922 → 443 [ACK] Seq=2292 Ack=2199 Win=493 Len=0 TSval=2519303992 TSecr=317237141
   15 0.323066199  192.168.1.4    104.208.16.88  TCP          74 52458 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1833059426 TSecr=0 WS=128
   17 0.511862913  104.208.16.88  192.168.1.4    TCP          66 443 → 52458 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 WS=256 SACK_PERM=1
▸ Frame 66: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface wlo1, id 0
▸ Ethernet II, Src: 64:6e:e0:a2:6f:89 (64:6e:e0:a2:6f:89), Dst: Netgear_0a:c2:48 (c4:04:15:0a:c2:48)
▾ Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0x7c85 (31877)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x3ad8 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.4
    Destination: 192.168.1.1
▾ User Datagram Protocol, Src Port: 47978, Dst Port: 53
    Source Port: 47978
    Destination Port: 53
    Length: 38
    Checksum: 0x838d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
  ▸ [Timestamps]
▸ Domain Name System (query)
```

- Destination Port: 53
- Destination: 192.168.1.1, совпадает
- www.ietf.org: type A, class IN, ответов не видно



- три ответа, в каждом — домен, тип, класс и в зависимости от типа либо еще домен, либо адрес

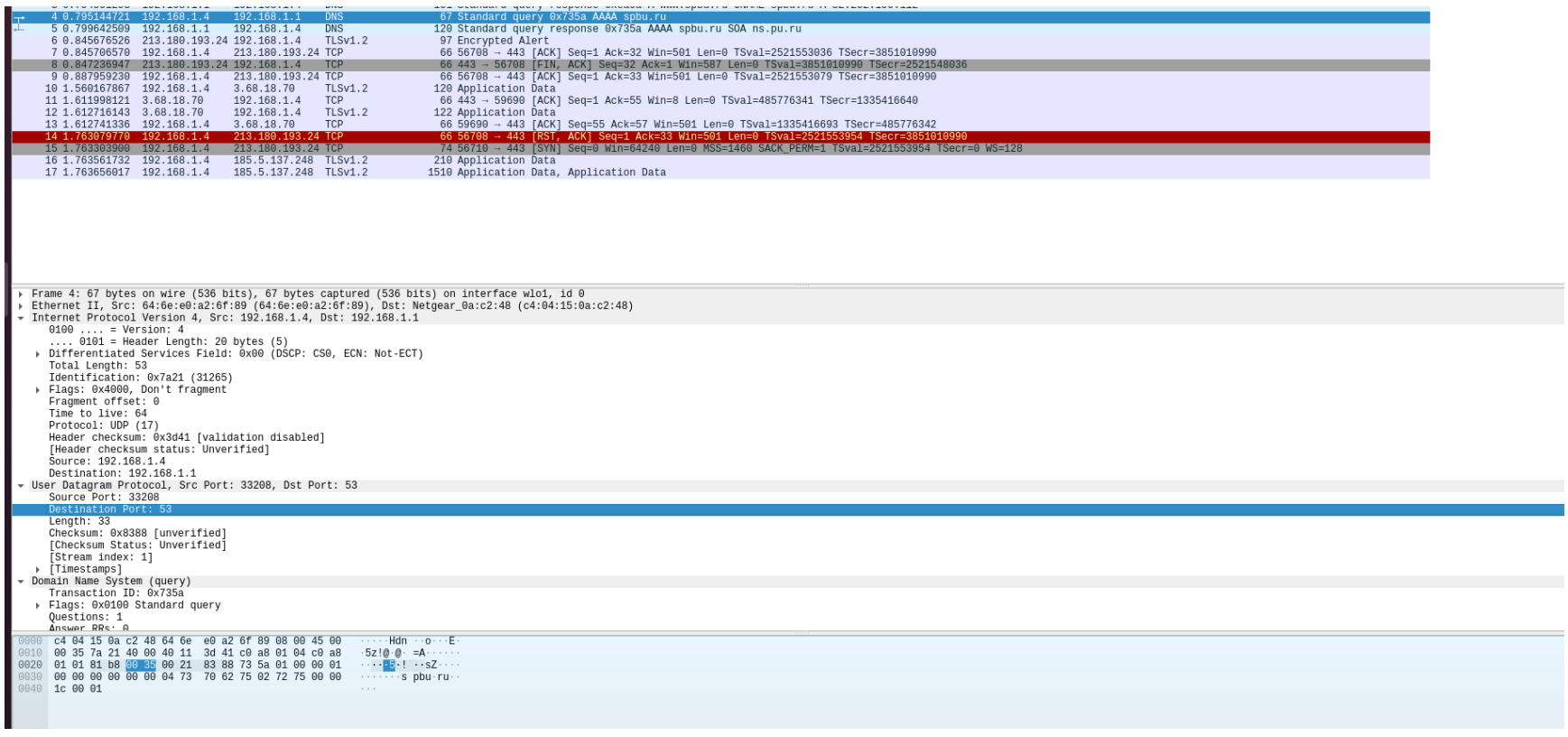
- Да, соответствует



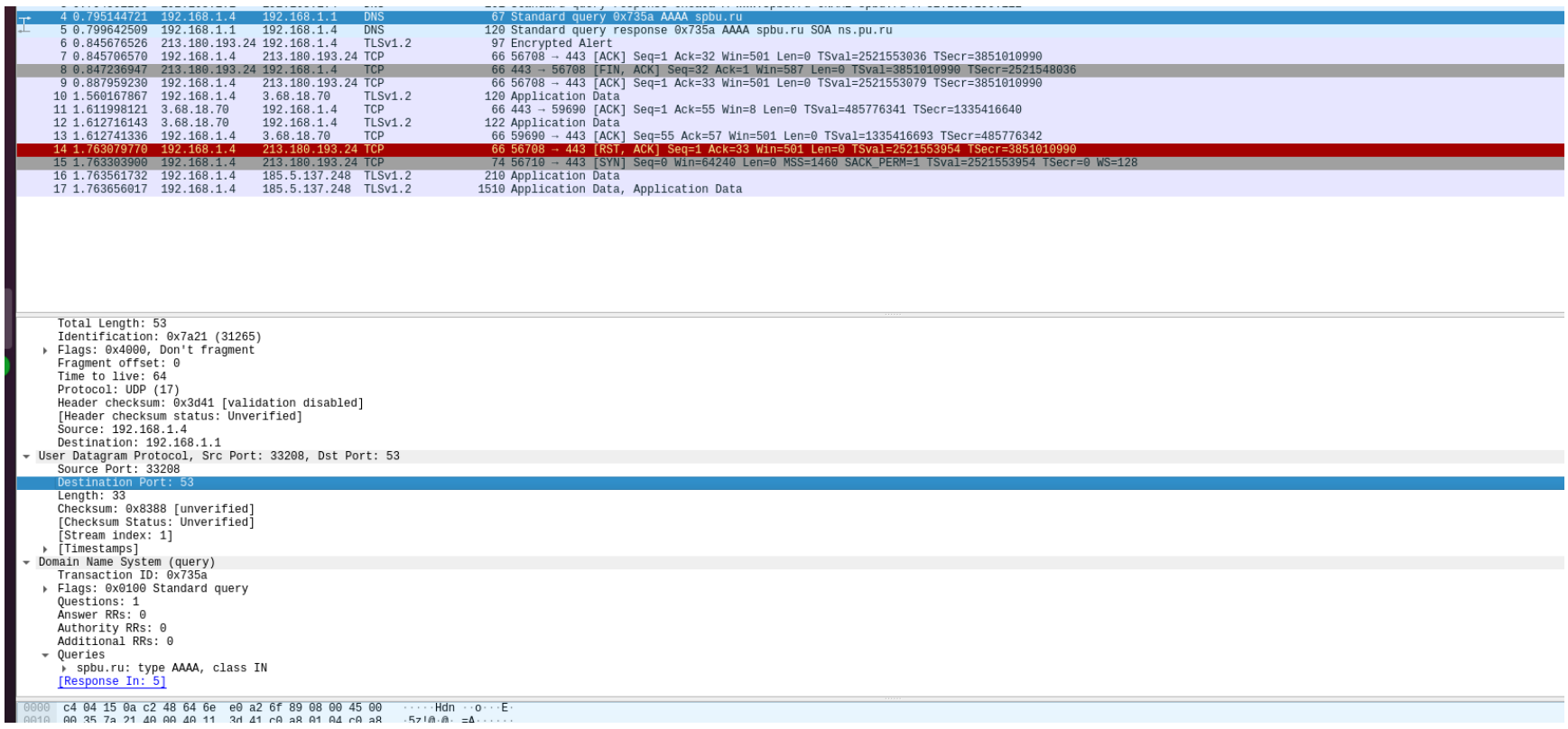
- Единственное, что видно — доп запрос в analytics.ietf.org, но я не нашел прямой связи этого с изображениями.

B.

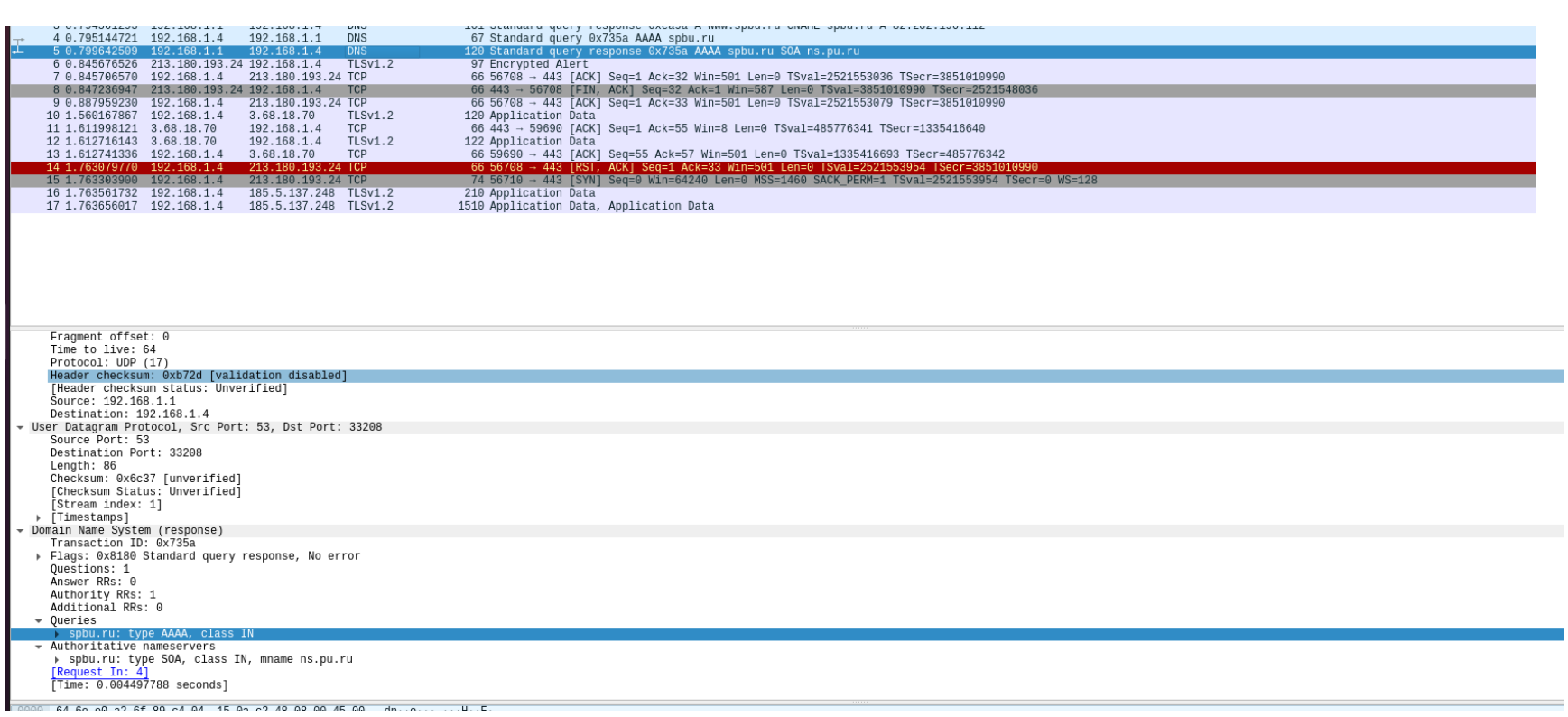
- Destination Port: 53



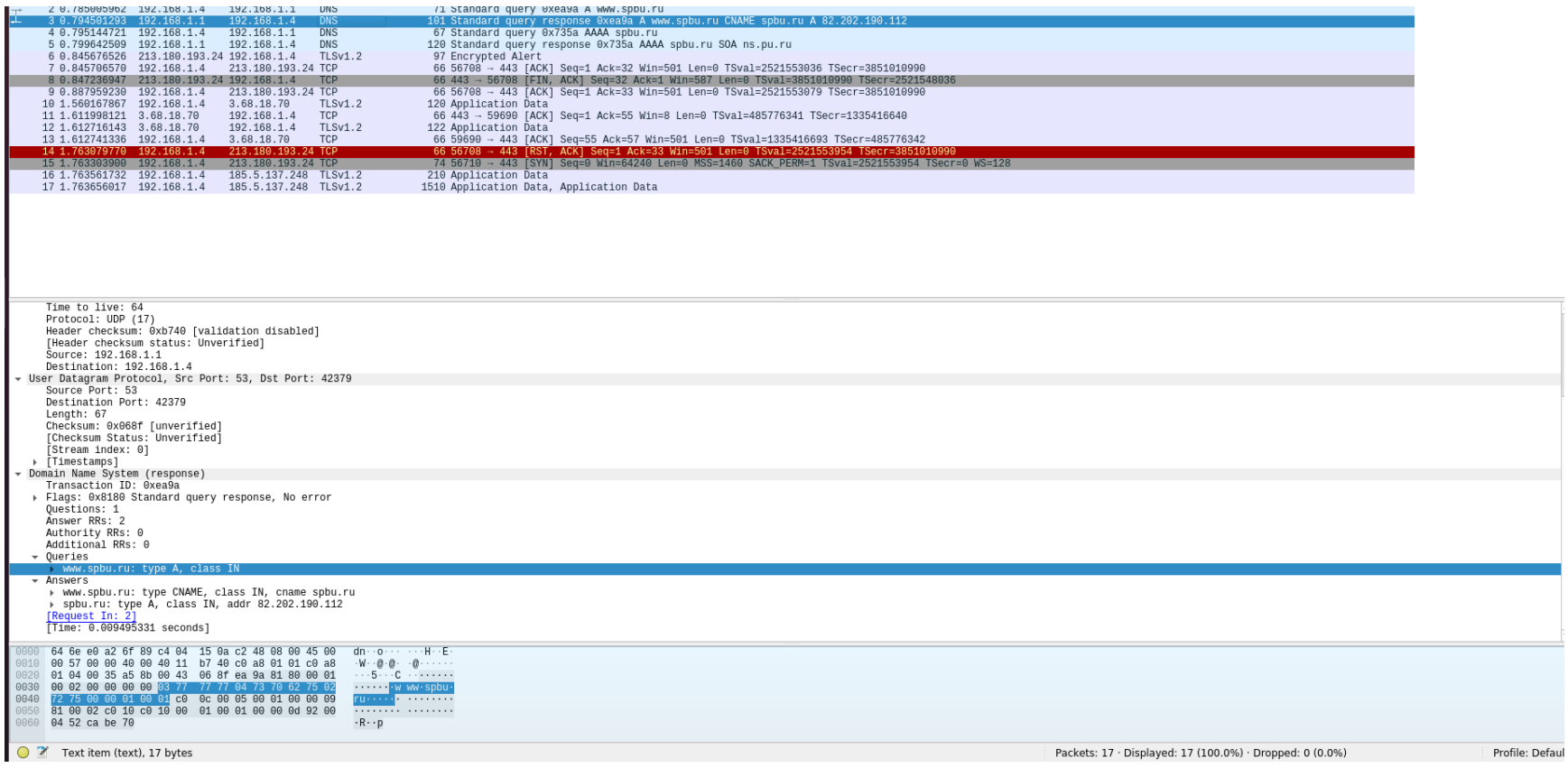
- Destination: 192.168.1.1, совпадает
- spbu.ru: type AAAA, class IN, ответов не видно



- в последней паре запросов DNS нет ответов:

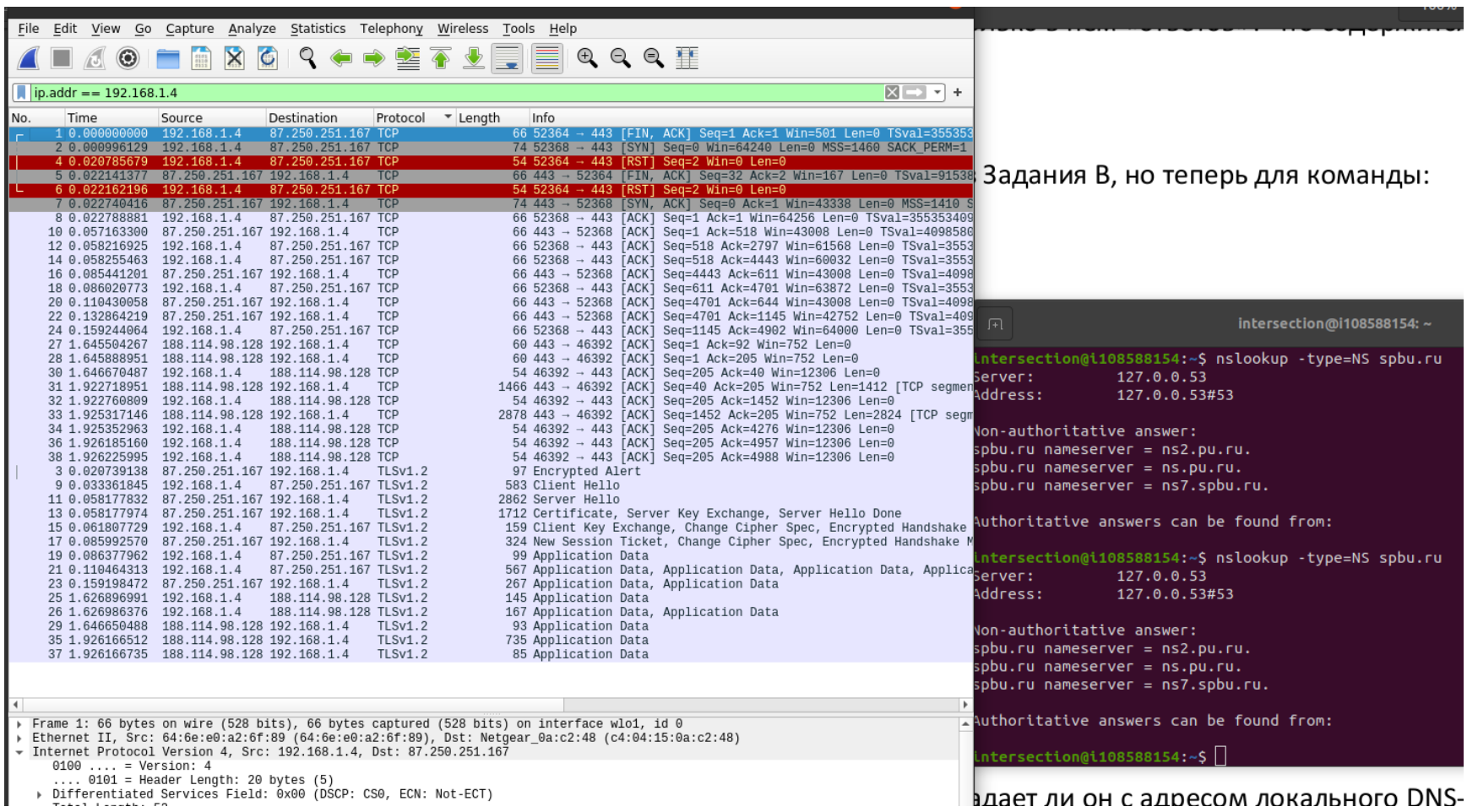


А вот в предпоследнем они были. Структура та же, что в предыдущем задании



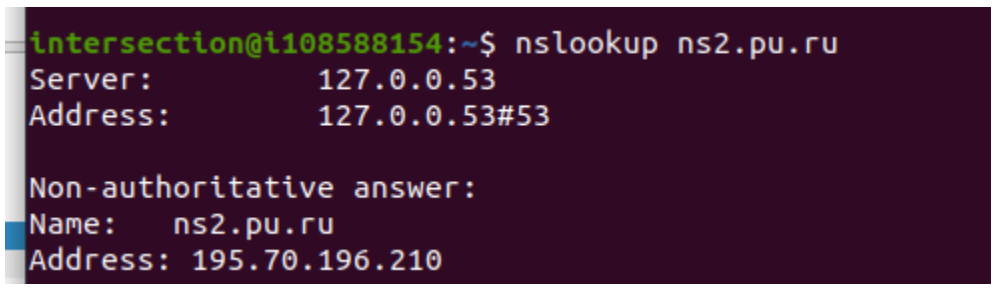
Г.

Нет DNS запросов

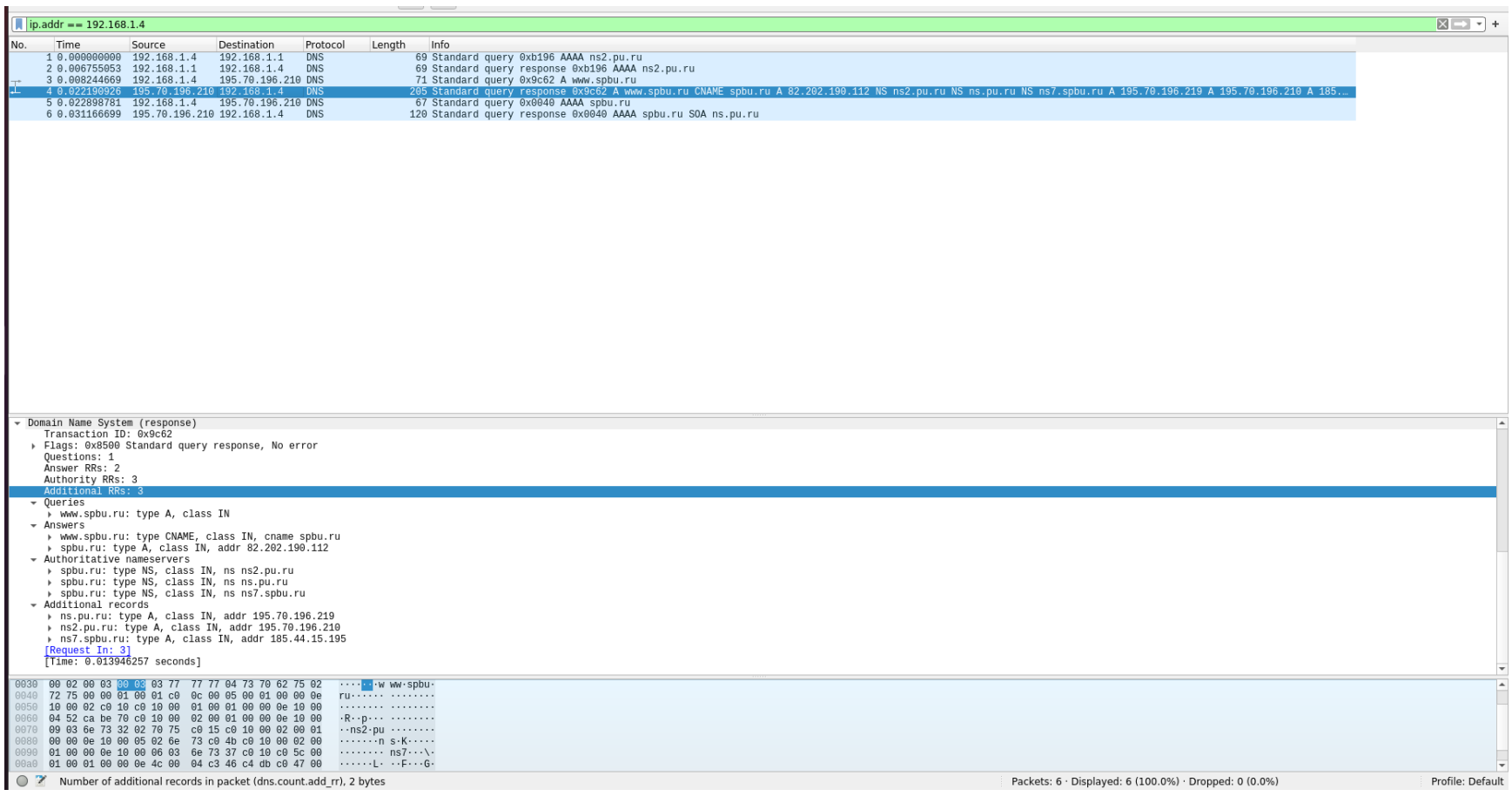


Д.

- Destination: 195.70.196.210, не совпадает, ns2.pu.ru



- Отвечаю сразу на два вопроса последующих: всё как в пункте В, в последней паре ничего интересного, а вот в предпоследней интереснее



E.

- WHOIS – это база данных, в которой хранятся сведения о доменах. В ней можно найти следующую информацию:
  - контактные данные регистранта, администратора и технических специалистов;
  - сведения о спонсирующем регистраторе;
  - дату создания и обновления домена, а также срок его регистрации;
  - DNS-серверы и статус домена.
- ns1.vkontakte.ru, ns2.vkontakte.ru; использовал 2domains.ru/whois

```
intersection@i108588154:~$ nslookup 192.168.1.1
1.1.168.192.in-addr.arpa        name = _gateway.

Authoritative answers can be found from:

intersection@i108588154:~$ nslookup ns1.vkontakte.ru
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns1.vkontakte.ru
Address: 87.240.131.131
Name:   ns1.vkontakte.ru
Address: 2a00:bdc0:ff:1::2

intersection@i108588154:~$ nslookup ns2.vkontakte.ru
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns2.vkontakte.ru
Address: 95.213.21.21
Name:   ns2.vkontakte.ru
Address: 2a00:bdc0:ff:2::2
```