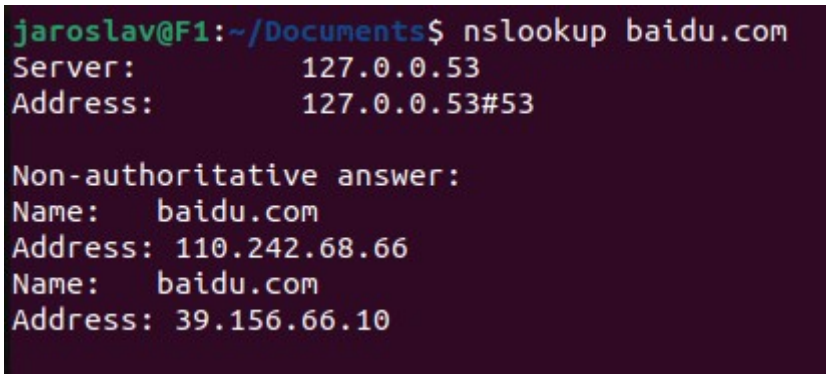
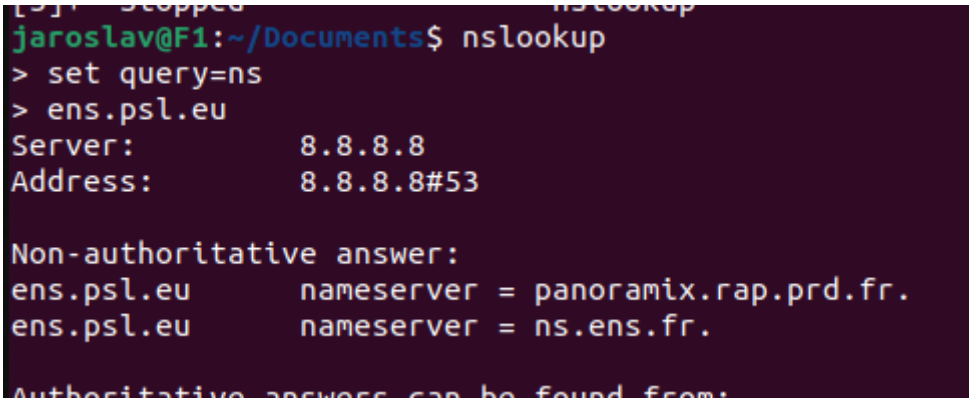
Курбатов Ярослав, 5 курс РПО МКН

Задание 2.A

1)

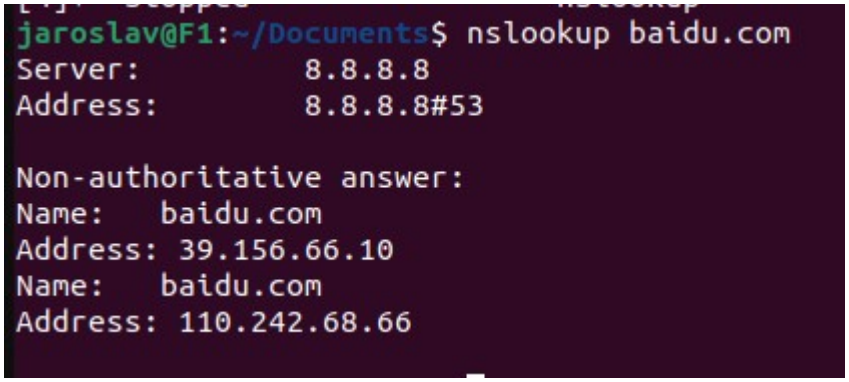


2)



nameserver – ns.ens.fr, panoramix.rap.prd.fr

3)

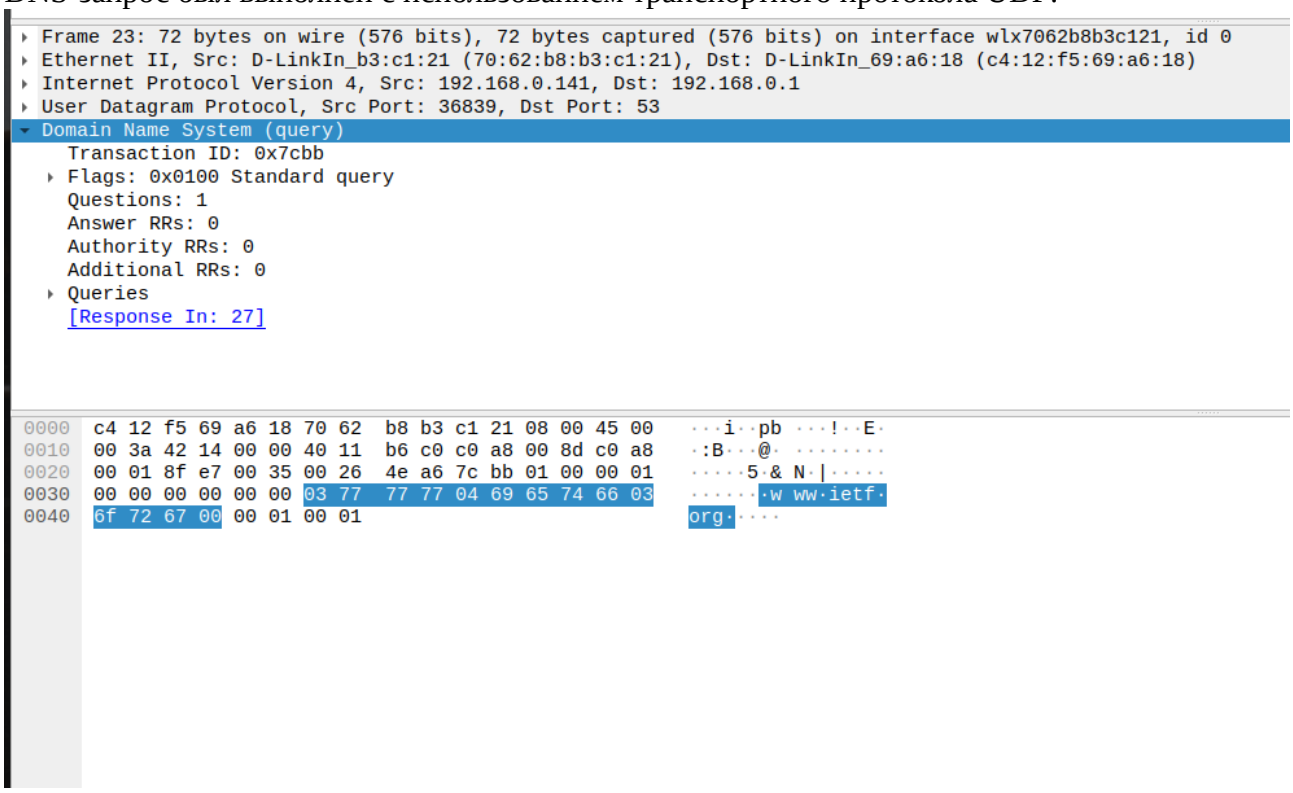


```
Address: 2a00:1450:400f:80b::200e

jaroslav@F1:~/Documents$ nslookup spbu.ru
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   spbu.ru
Address: 81.89.183.222
```

1 IP адрес

2.Б

DNS-запрос был выполнен с использованием транспортного протокола UDP:

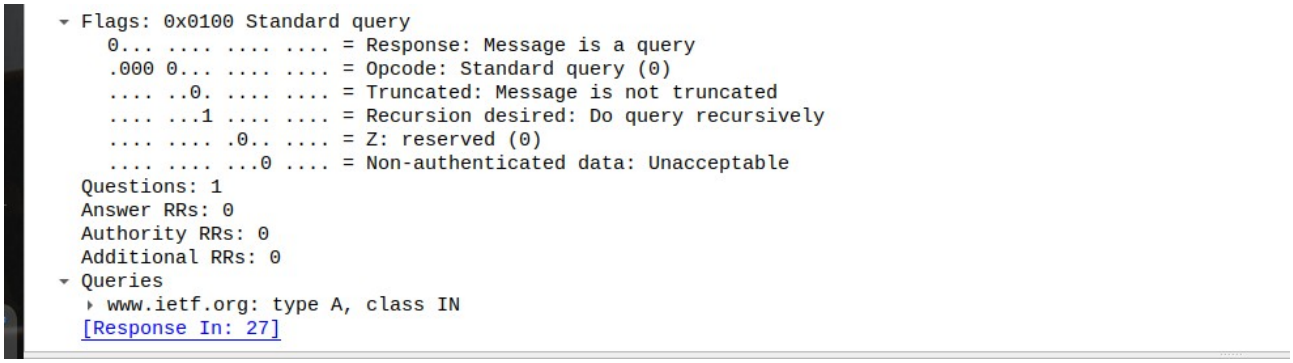


Порт назначения (dst port) – 53.

IP-адреса совпадают:

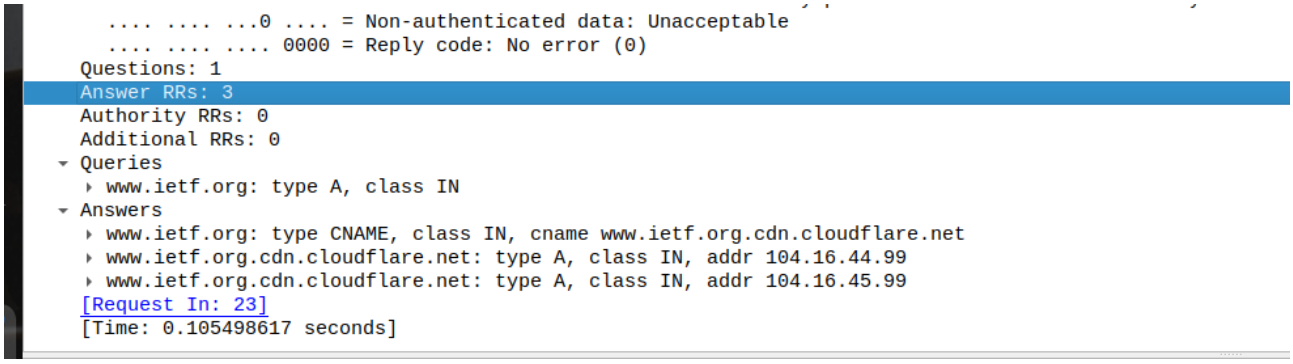
```
jaroslav@F1:~/Documents$ resolvectl
Global
       Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
resolv.conf mode: foreign

Link 2 (enp1s0)
Current Scopes: none
     Protocols: -DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

Link 3 (wlx7062b8b3c121)
    Current Scopes: DNS
         Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
Current DNS Server: 192.168.0.1
       DNS Servers: 192.168.0.1
```

Запрос на A-запись класса IN (Internet):

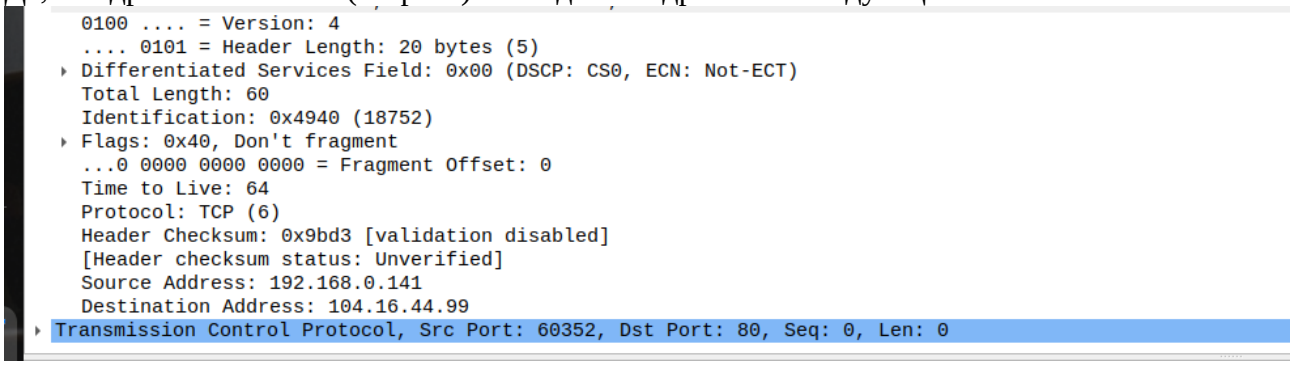


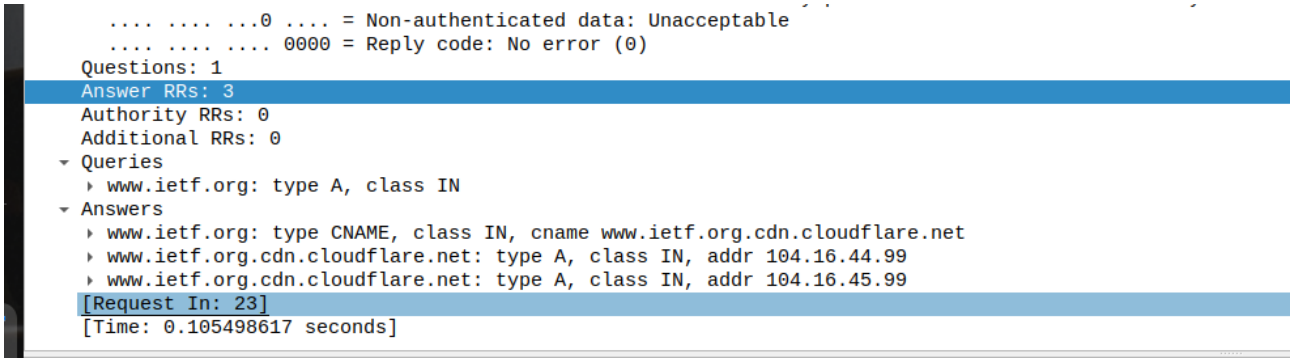
Answer Prs –0 (т.к. это запрос)

Ответ содержит 3 “ответа”. Первый из них – CNAME, слеующие 2 – A-записи для домена из первой CNAME-записи.



Да, IP-адрес DNS ответа (второго) совпадает и адресом последующего TCP-пакета:

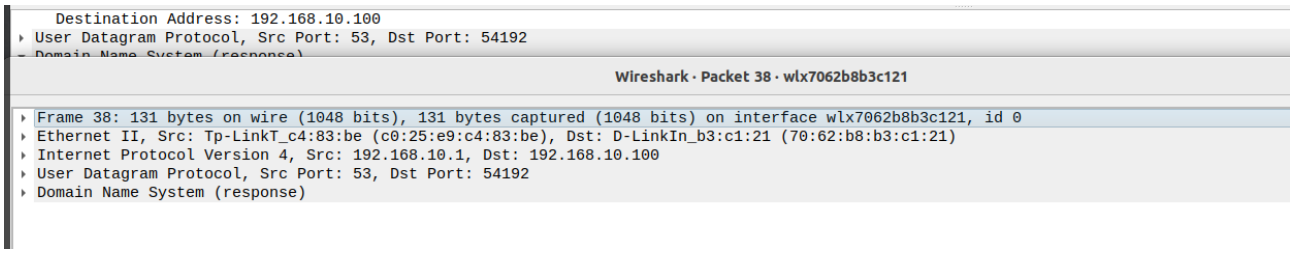




(104.16.44.99)

Для картинок, насколько я вижу, отдельных DNS-запросов не отпровляеются, потому что ссылки на них относятся к этому же домену. Дополнительный запрос отправляется на analytics.ietf.org, видимо, в HTML загружается соотвествующий скрипт с аналитикой.

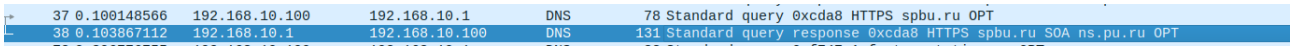
2.В



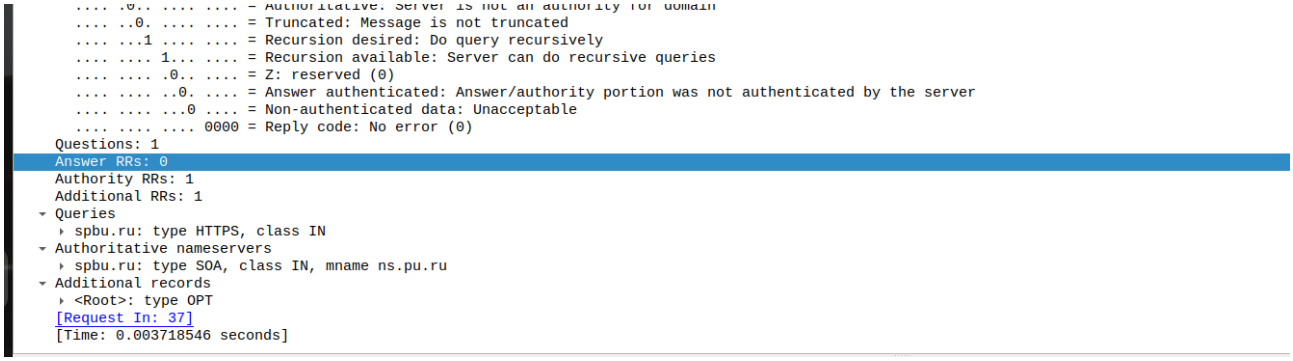
И порт назначения запроса, и порт отправления ответа одинаковые – UDP/53.

IP-адрес – мой локальный, запрос идет через мой локальный DNS-резолвер.

Запрос на запись класса HTTPS типа IN:

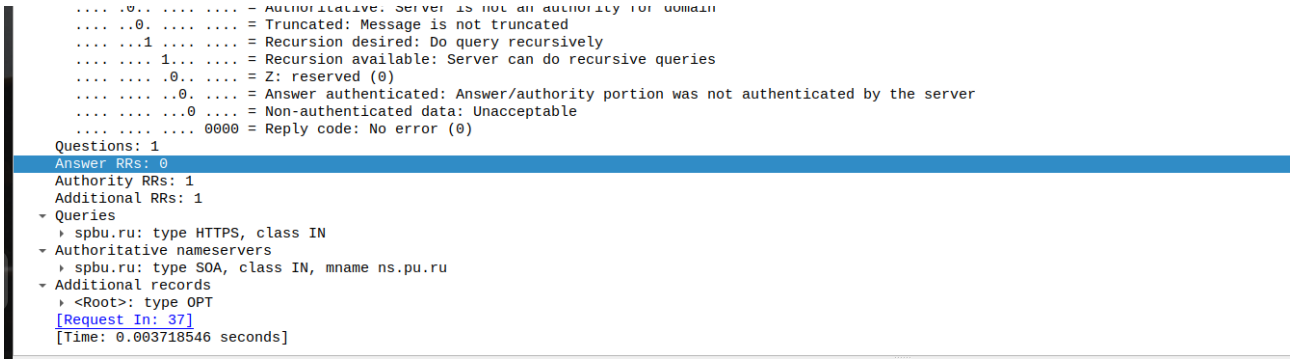


Ответов в запросе нет (Answers PR), потому что это DNS-запрос



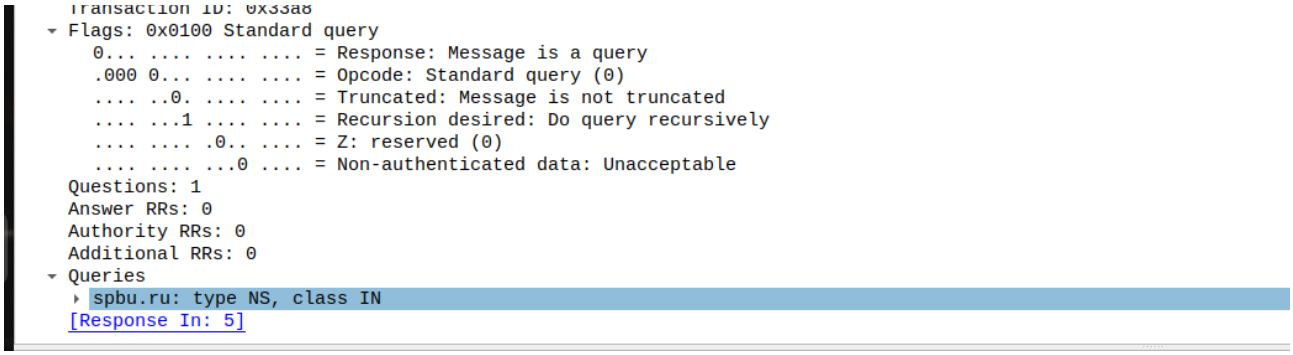
В ответе мы видим start-of-authority запись (nameserver) и дополнительные (OPT, options) данные

2.Г

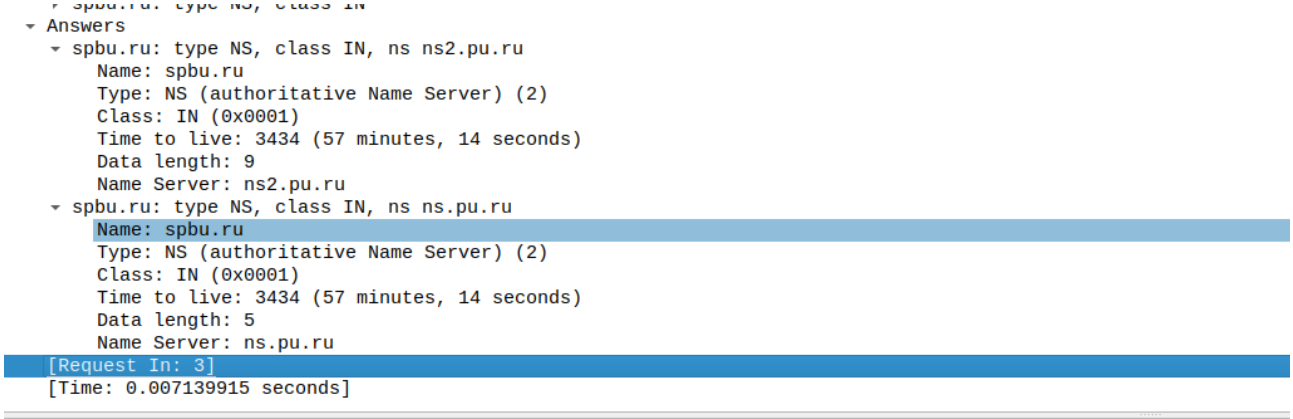


DNS-запрос отправлен за 8.8.4.4, потому что он указал приоритетным в *“/etc/resolv.conf”*

Тип запроса: NS:

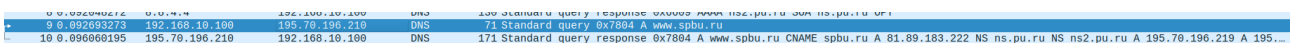


ответов в запросе нет.



Два доменных имени: ns.pu.ru, ns2.pu.ru. Их адресов в ответе ожидаемо нет.

2.Д



Запрос выполненен по IP-адресу того nameserver-а, который мы указали (ns2.pu.ru). Адрес этого nameserver тоже получен через DNS-запрос.

Запрос A-записи, ответов в нем нет:

```
Domain Name System (query)
    Transaction ID: 0x7804
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ www.spbu.ru: type A, class IN
    [Response In: 10]
```

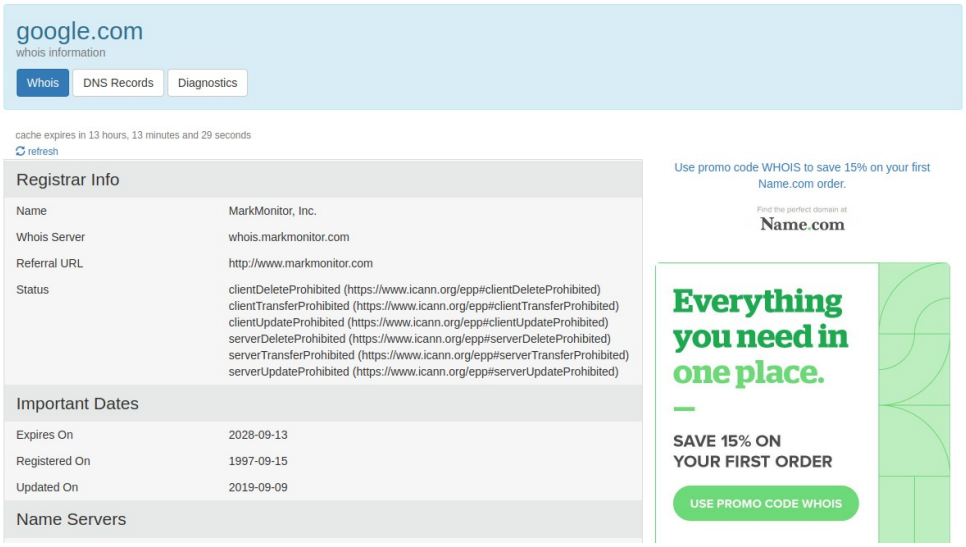
Ответ содержит CNAME и A запись для www.spbu.ru:

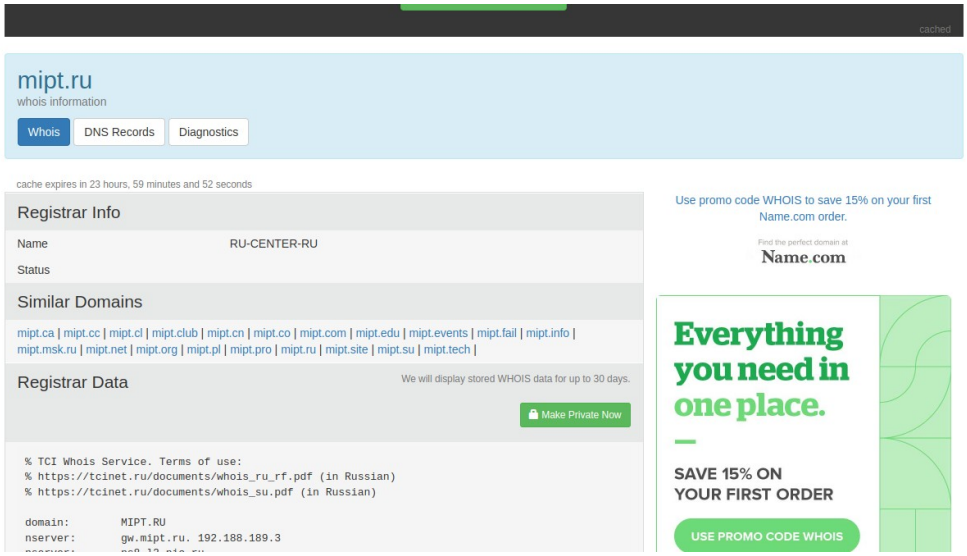
```
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 2
    Authority RRs: 2
    Additional RRs: 2
  ▾ Queries
    ▸ www.spbu.ru: type A, class IN
  ▾ Answers
    ▸ www.spbu.ru: type CNAME, class IN, cname spbu.ru
    ▸ spbu.ru: type A, class IN, addr 81.89.183.222
  ▸ Authoritative nameservers
  ▸ Additional records
    [Request In: 9]
    [Time: 0.003366922 seconds]
```

2.E

Whois – это база данных для хранения и распространения данных о доменных именах, их владельцах, занятости домена и прочей подобной информации

Используем сервис https://who.is





Отправим запросы 3 серверам:

```
jaroslav@F1:~/Documents$ nslookup google.com 127.0.0.53
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 64.233.164.100
Name:   google.com
Address: 64.233.164.101
Name:   google.com
Address: 64.233.164.113
Name:   google.com
Address: 64.233.164.138
Name:   google.com
Address: 64.233.164.102
Name:   google.com
Address: 64.233.164.139
Name:   google.com
Address: 2a00:1450:4010:c07::64
Name:   google.com
Address: 2a00:1450:4010:c07::8a
Name:   google.com
Address: 2a00:1450:4010:c07::66
Name:   google.com
Address: 2a00:1450:4010:c07::71

jaroslav@F1:~/Documents$ nslookup google.com ns2.pu.ru
Server:         ns2.pu.ru
Address:        195.70.196.210#53

** server can't find google.com: REFUSED

jaroslav@F1:~/Documents$ nslookup google.com ns.pu.ru
Server:         ns.pu.ru
Address:        195.70.196.219#53

** server can't find google.com: REFUSED

jaroslav@F1:~/Documents$
```

ns2.pu.ru и ns.pu.ru не ответили – они не обслуживают домен google.com