Wireshark. Работа с DNS

Задание А

-

```
margo@laptop:~$ nslookup www.beijing2022.cn
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.beijing2022.cn      canonical name = www.beijing2022.cn.edgesuite.net.
www.beijing2022.cn.edgesuite.net        canonical name = a1807.dscr.akamai.net.
Name:   a1807.dscr.akamai.net
Address: 188.234.145.152
Name:   a1807.dscr.akamai.net
Address: 188.234.145.147
Name:   a1807.dscr.akamai.net
Address: 2a02:26f0:4600::213:cd12
Name:   a1807.dscr.akamai.net
Address: 2a02:26f0:4600::213:cce0
```

- DNS серверы Кембриджского университета

```
margo@laptop:~$ nslookup -type=NS cambridge.org
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
cambridge.org   nameserver = lex.ns.cloudflare.com.
cambridge.org   nameserver = nucum.ns.cloudflare.com.


margo@laptop:~$ nslookup cambridge.org  lex.ns.cloudflare.com
Server:         lex.ns.cloudflare.com
Address:        173.245.59.196#53

Name:   cambridge.org
Address: 104.16.56.52
Name:   cambridge.org
Address: 104.16.55.52

margo@laptop:~$ nslookup cambridge.org  nucum.ns.cloudflare.com
Server:         nucum.ns.cloudflare.com
Address:        172.64.34.145#53

Name:   cambridge.org
Address: 104.16.56.52
Name:   cambridge.org
Address: 104.16.55.52
```

- У Яндекса пять IP-адресов, а у СПбГУ один

```
margo@laptop:~$ nslookup yandex.ru
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   yandex.ru
Address: 5.255.255.77
Name:   yandex.ru
Address: 77.88.55.88
Name:   yandex.ru
Address: 5.255.255.70
Name:   yandex.ru
Address: 77.88.55.60
Name:   yandex.ru
Address: 2a02:6b8:a::a
```

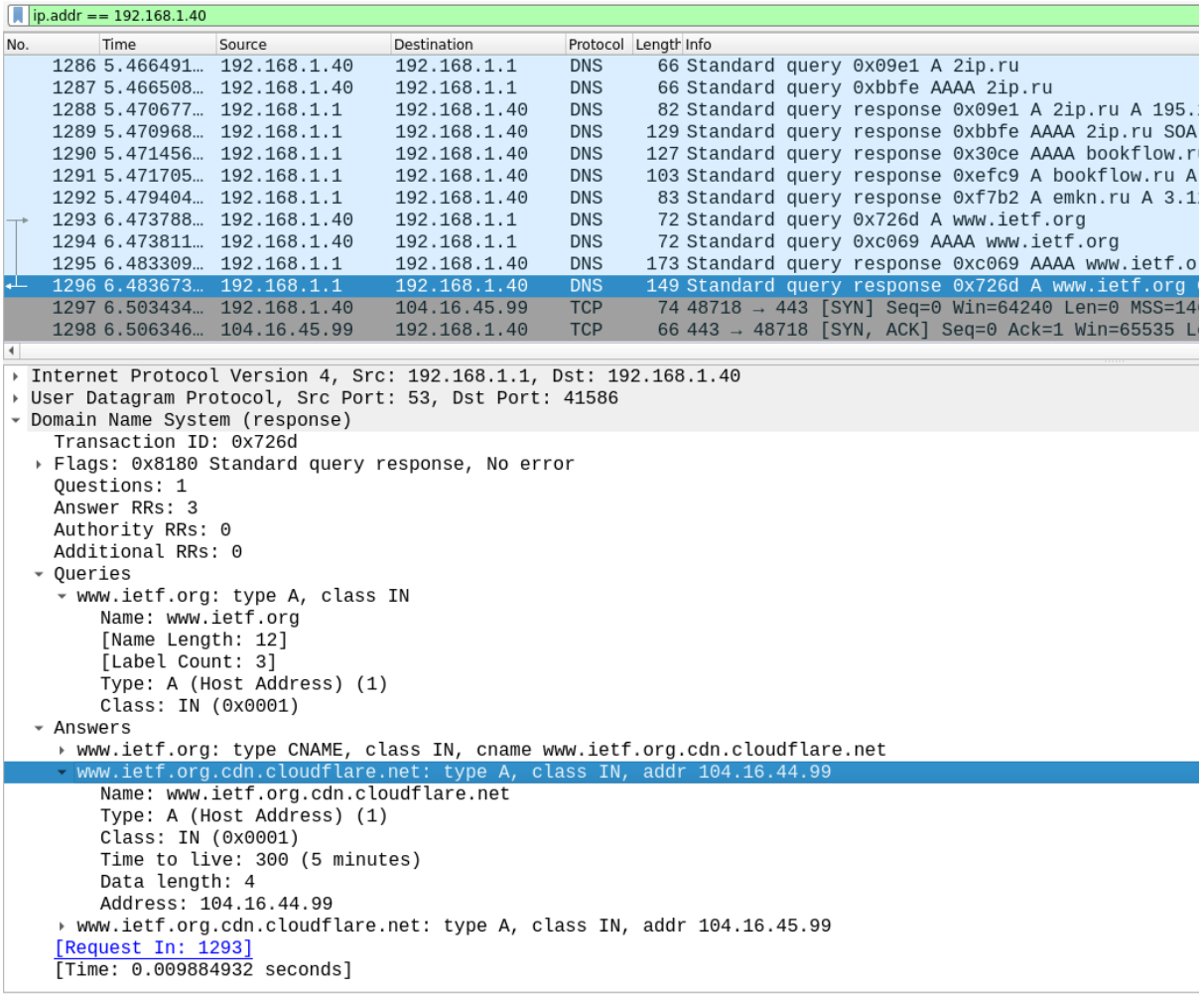
```
margo@laptop:~$ nslookup spbu.ru
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   spbu.ru
Address: 82.202.190.112
```

Задание Б

- Протокол UDP
- Port 53
- 192.168.1.1, и да, это в точности адрес локального DNS сервера:

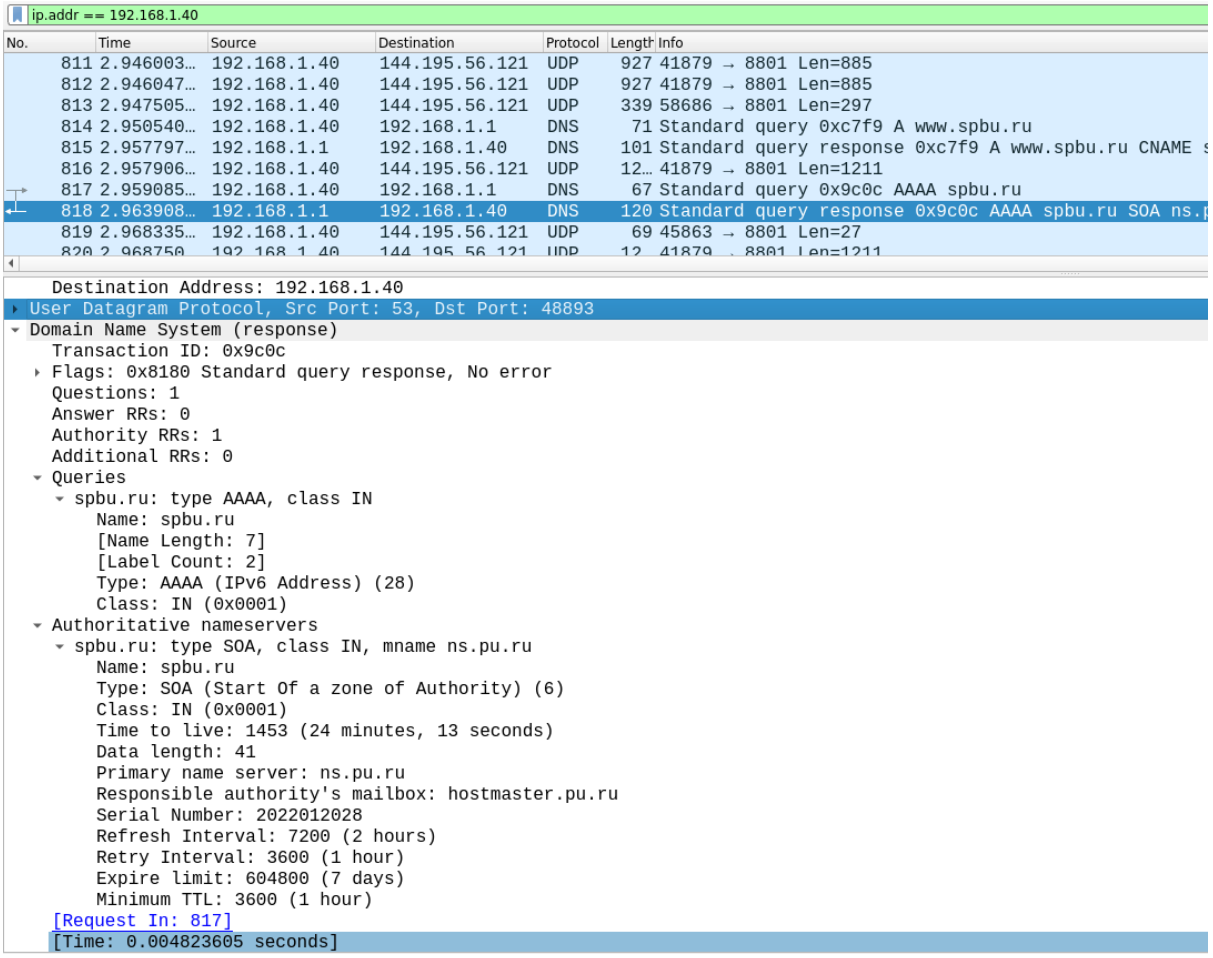
```
margo@laptop:~$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.1.1
```

- Type: A (Host Address)
- 3 ответа, в каждом имя, тип, класс, время жизни, длина данных, IP-адрес. В первом ответе вместо IP-адреса CNAME: www.ietf.org.cdn.cloudflare.net
- Да, соответствует IP-адресу 104.16.45.99 (3й ответ на запрос DNS)
- Еще два запроса DNS:
  1511 7.163624684 192.168.1.40 192.168.1.1 DNS 78 Standard query 0x7dba A analytics.ietf.org
  1512 7.163641099 192.168.1.40 192.168.1.1 DNS 78 Standard query 0xdfb6 AAAA analytics.ietf.org



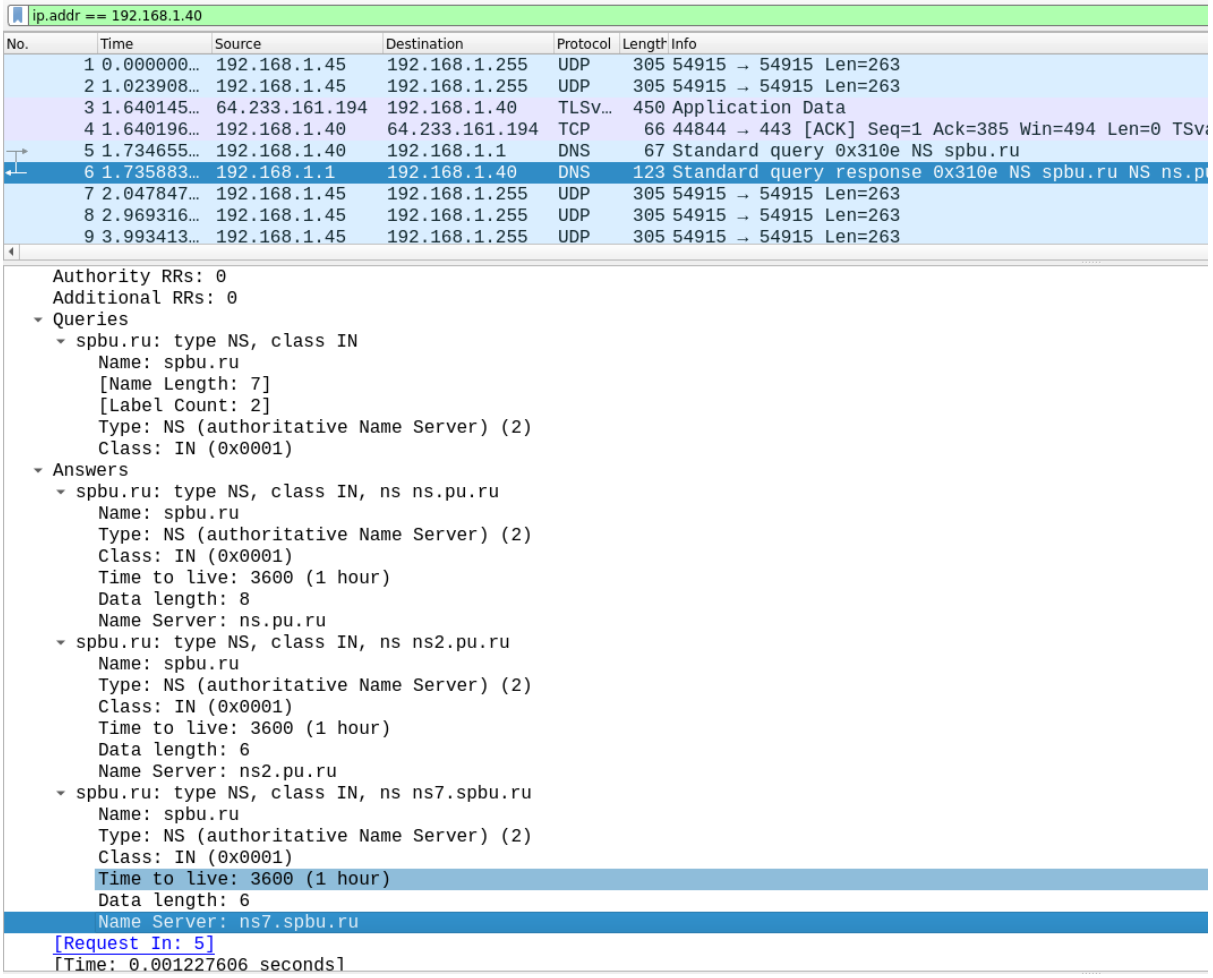
Задание В

- И тот, и тот порт 53
- 192.168.1.1, то есть на адрес локального DNS сервера
- Запрашивается запись типа AAAA (IPv6 Address). Кроме того в запросе указаны имя spbu.ru и некий класс IN
- Вижу один ответ: spbu.ru: type SOA (Start Of a zone of Authority), class IN, mname ns.pu.ru
  Поля ответа (имя, тип, класс, сериальный номер, различные временные интервалы и др) на скриншоте:



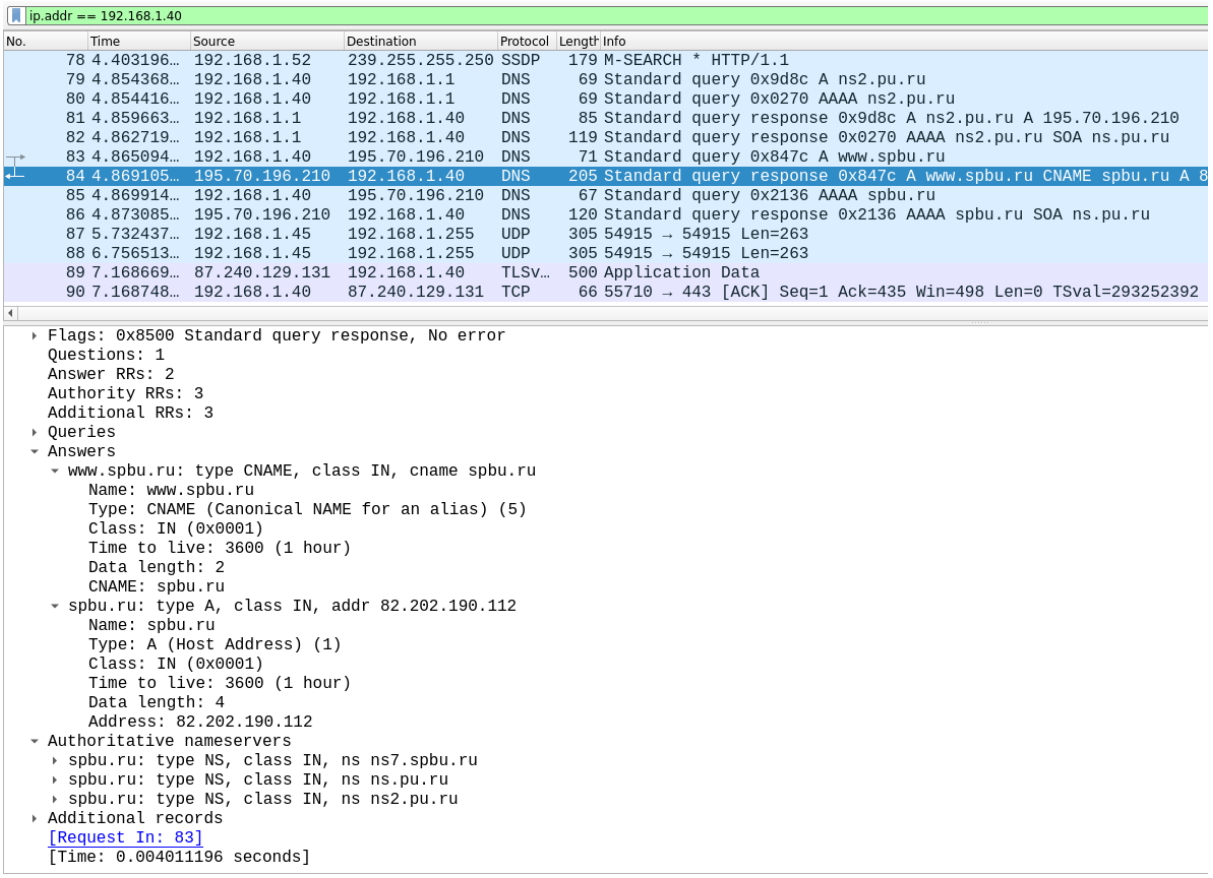
Задание Г

- 192.168.1.1, то есть на адрес локального DNS сервера
- запрашивается запись типа NS (authoritative Name Server), класса IN
- пришло 3 ответа про сервера: ns.pu.ru, ns2.pu.ru и ns7.spbu.ru. Их адреса не упоминаются.

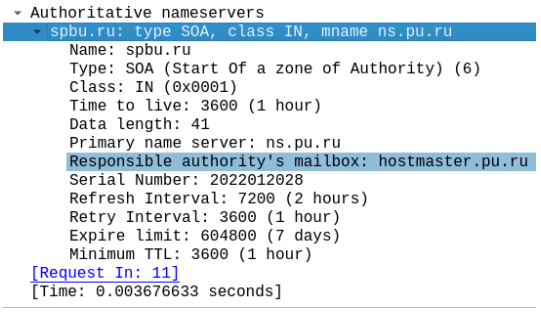


Задание Д

- Были отправлены 4 DNS запроса: 2 на стандартный локальный DNS сервер 192.168.1.1, и еще два на 195.70.196.210, это IP-адрес ns2.pu.ru.
- Два запроса типа A и два запроса типа AAA, все с классами IN.
- Наиболее интересные ответы те, которые пришли с 195.70.196.210. Как видно на скрине ниже, в ответе типа A кроме двух ответов про www.spbu.ru и spbu.ru есть также информация о 3 авторитетных DNS серверах и дополнительные записи про них (в которых содержатся их IP-адреса, например)



В ответе типа AAA в разделе Authoritative nameservers есть только одно поле spbu.ru: type SOA, class IN, mname ns.pu.ru, содержащее такую информацию про тот DNS сервер как имя домена, тип, класс, длина данных, имя сервера, почтовый адрес владельца, сериальный номер и различные временные интервалы.



Задание E

- Базы whois содержат данные о владельцах доменных имен, IP-адресов и автономных систем.
- У cambridge.org один из DNS серверов LEX.NS.CLOUDFLARE.COM (https://www.nic.ru/whois/), у yandex.ru — ns1.yandex.ru (https://whois.ru/)

```
Domain Name: CAMBRIDGE.ORG
Registry Domain ID: D1128807-LROR
Registrar WHOIS Server: whois.cscglobal.com
Registrar URL: www.cscglobal.com/global/web/csc/digital-brand
Updated Date: 2022-02-12T00:32:28Z
Creation Date: 1998-04-18T04:00:00Z
Registry Expiry Date: 2022-12-30T16:00:04Z
Registrar Registration Expiration Date:
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization: Cambridge University Press
Registrant State/Province:
Registrant Country: GB
Name Server: LEX.NS.CLOUDFLARE.COM
Name Server: NUCUM.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2022-03-19T08:57:59Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

Информация по данным whois.nic.ru

domain:	YANDEX.RU
nserver:	ns1.yandex.ru. 213.180.193.1, 2a02:6b8::1
nserver:	ns2.yandex.ru. 93.158.134.1, 2a02:6b8:0:1::1
nserver:	ns9.z5h64q92x9.net
state:	REGISTERED, DELEGATED
admin-contact:	https://www.nic.ru/whois/send-message/?domain=yandex.ru
org:	YANDEX, LLC.
registrar:	RU-CENTER-RU
created:	1997.09.23
paid-till:	2022.10.01
source:	RU-CENTER

>>> Last update of WHOIS database: 2022.03.19T12:10:40Z <<<

Запросы к локальному серверу DNS и тем двум:

```
margo@laptop:~$ nslookup spbu.ru
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   spbu.ru
Address: 82.202.190.112
```

```
margo@laptop:~$ nslookup cambridge.org LEX.NS.CLOUDFLARE.COM
Server:         LEX.NS.CLOUDFLARE.COM
Address:        173.245.59.196#53

Name:   cambridge.org
Address: 104.16.56.52
Name:   cambridge.org
Address: 104.16.55.52
```

```
margo@laptop:~$ nslookup yandex.ru ns1.yandex.ru
Server:         ns1.yandex.ru
Address:        213.180.193.1#53

Name:   yandex.ru
Address: 77.88.55.88
Name:   yandex.ru
Address: 5.255.255.70
Name:   yandex.ru
Address: 5.255.255.77
Name:   yandex.ru
Address: 77.88.55.60
Name:   yandex.ru
Address: 2a02:6b8:a::a
```