

# 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

ip.addr == 192.168.1.40						
No.	Time	Source	Destination	Protocol	Length	Info
1286	5.466491...	192.168.1.40	192.168.1.1	DNS	66	Standard query 0x09e1 A 2ip.ru
1287	5.466508...	192.168.1.40	192.168.1.1	DNS	66	Standard query 0xbbfe AAAA 2ip.ru
1288	5.470677...	192.168.1.1	192.168.1.40	DNS	82	Standard query response 0x09e1 A 2ip.ru A 195.
1289	5.470968...	192.168.1.1	192.168.1.40	DNS	129	Standard query response 0xbbfe AAAA 2ip.ru SOA
1290	5.471456...	192.168.1.1	192.168.1.40	DNS	127	Standard query response 0x30ce AAAA bookflow.r
1291	5.471705...	192.168.1.1	192.168.1.40	DNS	103	Standard query response 0xefc9 A bookflow.ru A
1292	5.479404...	192.168.1.1	192.168.1.40	DNS	83	Standard query response 0xf7b2 A emkn.ru A 3.1
1293	6.473788...	192.168.1.40	192.168.1.1	DNS	72	Standard query 0x726d A www.ietf.org
1294	6.473811...	192.168.1.40	192.168.1.1	DNS	72	Standard query 0xc069 AAAA www.ietf.org
1295	6.483309...	192.168.1.1	192.168.1.40	DNS	173	Standard query response 0xc069 AAAA www.ietf.o
1296	6.483673...	192.168.1.1	192.168.1.40	DNS	149	Standard query response 0x726d A www.ietf.org
1297	6.503434...	192.168.1.40	104.16.45.99	TCP	74	48718 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=14
1298	6.506346...	104.16.45.99	192.168.1.40	TCP	66	443 → 48718 [SYN, ACK] Seq=0 Ack=1 Win=65535 L

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.40

User Datagram Protocol, Src Port: 53, Dst Port: 41586

Domain Name System (response)

Transaction ID: 0x726d

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 0

Additional RRs: 0

Queries

- www.ietf.org: type A, class IN
- Name: www.ietf.org
- [Name Length: 12]
- [Label Count: 3]
- Type: A (Host Address) (1)
- Class: IN (0x0001)

Answers

- www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
- www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
- Name: www.ietf.org.cdn.cloudflare.net
- Type: A (Host Address) (1)
- Class: IN (0x0001)
- Time to live: 300 (5 minutes)
- Data length: 4
- Address: 104.16.44.99
- www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99

[\[Request In: 1293\]](#)

[Time: 0.009884932 seconds]

## 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:

ip.addr == 192.168.1.40					
No.	Time	Source	Destination	Protocol	Length Info
811	2.946003...	192.168.1.40	144.195.56.121	UDP	927 41879 → 8801 Len=885
812	2.946047...	192.168.1.40	144.195.56.121	UDP	927 41879 → 8801 Len=885
813	2.947505...	192.168.1.40	144.195.56.121	UDP	339 58686 → 8801 Len=297
814	2.950540...	192.168.1.40	192.168.1.1	DNS	71 Standard query 0xc7f9 A www.spbu.ru
815	2.957797...	192.168.1.1	192.168.1.40	DNS	101 Standard query response 0xc7f9 A www.spbu.ru CNAME s
816	2.957906...	192.168.1.40	144.195.56.121	UDP	12... 41879 → 8801 Len=1211
817	2.959085...	192.168.1.40	192.168.1.1	DNS	67 Standard query 0x9c0c AAAA spbu.ru
818	2.963908...	192.168.1.1	192.168.1.40	DNS	120 Standard query response 0x9c0c AAAA spbu.ru SOA ns.p
819	2.968335...	192.168.1.40	144.195.56.121	UDP	69 45863 → 8801 Len=27
820	2.968750...	192.168.1.40	144.195.56.121	UDP	12 41879 → 8801 Len=1211

  

Destination Address: 192.168.1.40	
User Datagram Protocol, Src Port: 53, Dst Port: 48893	
Domain Name System (response)	
Transaction ID: 0x9c0c	
Flags: 0x8180 Standard query response, No error	
Questions: 1	
Answer RRs: 0	
Authority RRs: 1	
Additional RRs: 0	
Queries	
spbu.ru: type AAAA, class IN	
Name: spbu.ru	
[Name Length: 7]	
[Label Count: 2]	
Type: AAAA (IPv6 Address) (28)	
Class: IN (0x0001)	
Authoritative nameservers	
spbu.ru: type SOA, class IN, mname ns.pu.ru	
Name: spbu.ru	
Type: SOA (Start Of a zone of Authority) (6)	
Class: IN (0x0001)	
Time to live: 1453 (24 minutes, 13 seconds)	
Data length: 41	
Primary name server: ns.pu.ru	
Responsible authority's mailbox: hostmaster.pu.ru	
Serial Number: 2022012028	
Refresh Interval: 7200 (2 hours)	
Retry Interval: 3600 (1 hour)	
Expire limit: 604800 (7 days)	
Minimum TTL: 3600 (1 hour)	
[Request In: 817]	
[Time: 0.004823605 seconds]	

## 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.

ip.addr == 192.168.1.40						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000...	192.168.1.45	192.168.1.255	UDP	305	54915 → 54915 Len=263
2	1.023908...	192.168.1.45	192.168.1.255	UDP	305	54915 → 54915 Len=263
3	1.640145...	64.233.161.194	192.168.1.40	TLSv...	450	Application Data
4	1.640196...	192.168.1.40	64.233.161.194	TCP	66	44844 → 443 [ACK] Seq=1 Ack=385 Win=494 Len=0 TSv...
5	1.734655...	192.168.1.40	192.168.1.1	DNS	67	Standard query 0x310e NS spbu.ru
6	1.735883...	192.168.1.1	192.168.1.40	DNS	123	Standard query response 0x310e NS spbu.ru NS ns.p...
7	2.047847...	192.168.1.45	192.168.1.255	UDP	305	54915 → 54915 Len=263
8	2.969316...	192.168.1.45	192.168.1.255	UDP	305	54915 → 54915 Len=263
9	3.993413...	192.168.1.45	192.168.1.255	UDP	305	54915 → 54915 Len=263

  

Authority RRs: 0
Additional RRs: 0
Queries
spbu.ru: type NS, class IN
Name: spbu.ru
[Name Length: 7]
[Label Count: 2]
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Answers
spbu.ru: type NS, class IN, ns ns.pu.ru
Name: spbu.ru
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 3600 (1 hour)
Data length: 8
Name Server: ns.pu.ru
spbu.ru: type NS, class IN, ns ns2.pu.ru
Name: spbu.ru
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 3600 (1 hour)
Data length: 6
Name Server: ns2.pu.ru
spbu.ru: type NS, class IN, ns ns7.spbu.ru
Name: spbu.ru
Type: NS (authoritative Name Server) (2)
Class: IN (0x0001)
Time to live: 3600 (1 hour)
Data length: 6
Name Server: ns7.spbu.ru
[Request In: 5]
[Time: 0.001227606 seconds]

## 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](http://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)

ip.addr == 192.168.1.40						
No.	Time	Source	Destination	Protocol	Length	Info
78	4.403196...	192.168.1.52	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
79	4.854368...	192.168.1.40	192.168.1.1	DNS	69	Standard query 0x9d8c A ns2.pu.ru
80	4.854416...	192.168.1.40	192.168.1.1	DNS	69	Standard query 0x0270 AAAA ns2.pu.ru
81	4.859663...	192.168.1.1	192.168.1.40	DNS	85	Standard query response 0x9d8c A ns2.pu.ru A 195.70.196.210
82	4.862719...	192.168.1.1	192.168.1.40	DNS	119	Standard query response 0x0270 AAAA ns2.pu.ru SOA ns.pu.ru
83	4.865094...	192.168.1.40	195.70.196.210	DNS	71	Standard query 0x847c A www.spbu.ru
84	4.869105...	195.70.196.210	192.168.1.40	DNS	205	Standard query response 0x847c A www.spbu.ru CNAME spbu.ru A 8
85	4.869914...	192.168.1.40	195.70.196.210	DNS	67	Standard query 0x2136 AAAA spbu.ru
86	4.873085...	195.70.196.210	192.168.1.40	DNS	120	Standard query response 0x2136 AAAA spbu.ru SOA ns.pu.ru
87	5.732437...	192.168.1.45	192.168.1.255	UDP	305	54915 → 54915 Len=263
88	6.756513...	192.168.1.45	192.168.1.255	UDP	305	54915 → 54915 Len=263
89	7.168669...	87.240.129.131	192.168.1.40	TLSv...	500	Application Data
90	7.168748...	192.168.1.40	87.240.129.131	TCP	66	55710 → 443 [ACK] Seq=1 Ack=435 Win=498 Len=0 TSval=293252392

Flags: 0x8500 Standard query response, No error

Questions: 1

Answer RRs: 2

Authority RRs: 3

Additional RRs: 3

Queries

Answers

- www.spbu.ru: type CNAME, class IN, cname spbu.ru
  - Name: www.spbu.ru
  - Type: CNAME (Canonical NAME for an alias) (5)
  - Class: IN (0x0001)
  - Time to live: 3600 (1 hour)
  - Data length: 2
  - CNAME: spbu.ru
- spbu.ru: type A, class IN, addr 82.202.190.112
  - Name: spbu.ru
  - Type: A (Host Address) (1)
  - Class: IN (0x0001)
  - Time to live: 3600 (1 hour)
  - Data length: 4
  - Address: 82.202.190.112
- Authoritative nameservers
  - spbu.ru: type NS, class IN, ns ns7.spbu.ru
  - spbu.ru: type NS, class IN, ns ns.pu.ru
  - spbu.ru: type NS, class IN, ns ns2.pu.ru
- Additional records

[Request In: 83]

[Time: 0.004011196 seconds]

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, серийный номер и различные временные интервалы.

Authoritative nameservers	
spbu.ru: type SOA, class IN, mname ns.pu.ru	
Name: spbu.ru	
Type: SOA (Start Of a zone of Authority) (6)	
Class: IN (0x0001)	
Time to live: 3600 (1 hour)	
Data length: 41	
Primary name server: ns.pu.ru	
Responsible authority's mailbox: hostmaster.pu.ru	
Serial Number: 2022012028	
Refresh Interval: 7200 (2 hours)	
Retry Interval: 3600 (1 hour)	
Expire limit: 604800 (7 days)	
Minimum TTL: 3600 (1 hour)	
[Request In: 11]	
[Time: 0.003676633 seconds]	

## Задание Е

- 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-bran
d
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/ep
p#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://ww
w.icann.org/wicf/)
>>> Last update of WHOIS database: 2022-03-19T08:57:59Z <<<

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

```

#### Информация по данным whois.nic.ru

```

domain: YANDEX.RU
ns1: ns1.yandex.ru. 213.180.193.1, 2a02:6b8::1
ns2: ns2.yandex.ru. 93.158.134.1, 2a02:6b8:0:1::1
ns3: ns3.yandex.ru. 193.10.134.1, 2a02:6b8:0:1::1
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

```