

Задание А

1. Азиатский сайт www.rediff.com имеет 2 IP-адреса: 2.19.183.47 и 2.19.183.5

```
C:\Users\Анастасия>nslookup www.rediff.com
Server:      dns.google
Address:     8.8.8.8

Не заслуживающий доверия ответ:
_._. :       e81366.a.akamaiedge.net
Addresses:  2.19.183.47
            2.19.183.5
Aliases:     www.rediff.com
            rediff.com.edgekey.net
```

2. Авторитетный DNS-сервер для оксфордского университета - raptor.dns.ox.ac.uk

```
C:\Users\Анастасия>nslookup -type=NS www.ox.ac.uk
Server:      dns.google
Address:     8.8.8.8

ox.ac.uk
    primary name server = raptor.dns.ox.ac.uk
    responsible mail addr = hostmaster.ox.ac.uk
    serial = 2022031948
    refresh = 3600 (1 hour)
    retry = 1800 (30 mins)
    expire = 1209600 (14 days)
    default TTL = 900 (15 mins)
```

3. Сервер www.google.com имеет 10 IP-адресов:

```
C:\Users\Анастасия>nslookup www.google.com
ТхЁтхЁ: dns.google
Address: 8.8.8.8

Не заслуживающий доверия ответ:
Ль : www.google.com
Addresses: 2a00:1450:4010:c0b::69
2a00:1450:4010:c0b::6a
2a00:1450:4010:c0b::68
2a00:1450:4010:c0b::63
209.85.233.106
209.85.233.103
209.85.233.147
209.85.233.104
209.85.233.99
209.85.233.105
```

Веб-сервер www.spbu.ru имеет один IP-адрес: 82.202.190.112

```
C:\Users\Анастасия>nslookup www.spbu.ru
ТхЁтхЁ: dns.google
Address: 8.8.8.8

Не заслуживающий доверия ответ:
Ль : spbu.ru
Address: 82.202.190.112
Aliases: www.spbu.ru
```

Задание Б

1. Запрос и ответ на него были отправлены с помощью протокола UDP

3324	42.916960	10.0.0.100	8.8.8.8	DNS	72 Standard query 0xb369 A www.ietf.org
3325	42.994285	10.0.0.100	8.8.4.4	DNS	72 Standard query 0xb369 A www.ietf.org
3326	43.039067	13.83.65.43	10.0.0.100	TCP	66 443 → 55376 [ACK] Seq=1 Ack=2 Win=2050 Len=0 SLE=1 SRE=2
3327	43.046331	8.8.4.4	10.0.0.100	TCP	66 [TCP Window Update] 443 → 53737 [ACK] Seq=7916 Ack=2640 Win=380 Len=0 SLE=2868 SRE=2903
3328	43.056082	8.8.4.4	10.0.0.100	DNS	149 Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
3329	43.058123	8.8.8.8	10.0.0.100	DNS	149 Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
3330	43.060272	10.0.0.100	104.16.45.99	TCP	66 53792 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3331	43.061035	10.0.0.100	104.16.45.99	TCP	66 53793 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3332	43.062484	10.0.0.100	8.8.4.4	TLSv1.2	243 Application Data
3333	43.297245	104.16.45.99	10.0.0.100	TCP	66 443 → 53792 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3334	43.297368	10.0.0.100	104.16.45.99	TCP	54 53792 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
3335	43.297513	104.16.45.99	10.0.0.100	TCP	66 80 → 53793 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3336	43.297585	10.0.0.100	104.16.45.99	TCP	54 53793 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
3339	43.298576	10.0.0.100	104.16.45.99	TLSv1.3	603 Client Hello
3340	43.298965	10.0.0.100	104.16.45.99	HTTP	505 GET / HTTP/1.1
3341	43.307005	8.8.4.4	10.0.0.100	TCP	66 [TCP Window Update] 443 → 53737 [ACK] Seq=7916 Ack=2640 Win=380 Len=0 SLE=2868 SRE=3002

> Frame 3324: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{72634749-96BF-4B16-ACBE-E152688589CC}, id 0

> Ethernet II, Src: ac:7d:eb:a7:7d:3e (ac:7d:eb:a7:7d:3e), Dst: 00:d1:e6:e6:e6 (00:d1:e6:e6:e6)

> Internet Protocol Version 4, Src: 10.0.0.100, Dst: 8.8.8.8

> User Datagram Protocol, Src Port: 56488, Dst Port: 53

Source Port: 56488

Destination Port: 53

Length: 38

Checksum: 0x32a2 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

345	3.949632	10.0.0.100	8.8.8.8	DNS	80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
346	3.969767	142.251.1.132	10.0.0.100	TCP	66 443 → 52441 [ACK] Seq=1 Ack=2 Win=266 Len=0 SLE=1 SRE=2
347	3.982061	8.8.8.8	10.0.0.100	DNS	104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
348	3.983564	10.0.0.100	8.8.8.8	DNS	72 Standard query 0x0002 A www.ietf.org
349	4.022097	8.8.8.8	10.0.0.100	DNS	149 Standard query response 0x0002 A www.ietf.org CNAME www.ietf.org.cdn.c
350	4.025074	10.0.0.100	8.8.8.8	DNS	72 Standard query 0x0003 AAAA www.ietf.org
351	4.049682	10.0.0.100	68.232.34.200	TCP	55 62083 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reassemb
352	4.063155	8.8.8.8	10.0.0.100	DNS	173 Standard query response 0x0003 AAAA www.ietf.org CNAME www.ietf.org.cdn.c
353	4.117302	68.232.34.200	10.0.0.100	TCP	66 443 → 62083 [ACK] Seq=1 Ack=2 Win=136 Len=0 SLE=1 SRE=2
354	4.195462	10.0.0.100	87.240.129.131	TLSv1.2	128 Application Data
355	4.195537	10.0.0.100	87.240.129.131	TLSv1.2	274 Application Data

> Frame 349: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface \Device\NPF_{72634749-96BF-4B16-ACBE-E152688589CC}, id 0

> Ethernet II, Src: 00:d1:e6:e6:e6:e6 (00:d1:e6:e6:e6:e6), Dst: ac:7d:eb:a7:7d:3e (ac:7d:eb:a7:7d:3e)

> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.0.0.100

> User Datagram Protocol, Src Port: 53, Dst Port: 58193

> Domain Name System (response)

2. Порт назначения запроса – 53

3324	42.916960	10.0.0.100	8.8.8.8	DNS	72 Standard query 0xb369 A www.ietf.org
3325	42.994285	10.0.0.100	8.8.4.4	DNS	72 Standard query 0xb369 A www.ietf.org
3326	43.039067	13.83.65.43	10.0.0.100	TCP	66 443 → 55376 [ACK] Seq=1 Ack=2 Win=2050 Len=0 SLE=1 SRE=2
3327	43.046331	8.8.4.4	10.0.0.100	TCP	66 [TCP Window Update] 443 → 53737 [ACK] Seq=7916 Ack=2640 Win=380 Len=0 SLE=2868 SRE=2903
3328	43.056082	8.8.4.4	10.0.0.100	DNS	149 Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
3329	43.058123	8.8.8.8	10.0.0.100	DNS	149 Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
3330	43.060272	10.0.0.100	104.16.45.99	TCP	66 53792 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3331	43.061035	10.0.0.100	104.16.45.99	TCP	66 53793 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3332	43.062484	10.0.0.100	8.8.4.4	TLSv1.2	243 Application Data
3333	43.297245	104.16.45.99	10.0.0.100	TCP	66 443 → 53792 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3334	43.297368	10.0.0.100	104.16.45.99	TCP	54 53792 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
3335	43.297513	104.16.45.99	10.0.0.100	TCP	66 80 → 53793 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3336	43.297585	10.0.0.100	104.16.45.99	TCP	54 53793 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
3339	43.298576	10.0.0.100	104.16.45.99	TLSv1.3	603 Client Hello
3340	43.298965	10.0.0.100	104.16.45.99	HTTP	505 GET / HTTP/1.1
3341	43.307805	8.8.4.4	10.0.0.100	TCP	66 [TCP Window Update] 443 → 53737 [ACK] Seq=7916 Ack=2640 Win=380 Len=0 SLE=2868 SRE=2903

> Frame 3324: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{72634749-96BF-4B16-ACBE-E152688589CC}, id 0

> Ethernet II, Src: ac:7d:eb:a7:7d:3e (ac:7d:eb:a7:7d:3e), Dst: 00:d1:e6:e6:e6:e6 (00:d1:e6:e6:e6:e6)

> Internet Protocol Version 4, Src: 10.0.0.100, Dst: 8.8.8.8

> User Datagram Protocol, Src Port: 56488, Dst Port: 53

Source Port: 56488

Destination Port: 53

Length: 38

Checksum: 0x32a2 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

3. Запрос был отправлен на IP-адрес 8.8.8.8

3324	42.916960	10.0.0.100	8.8.8.8	DNS	72 Standard query 0xb369 A www.ietf.org
3325	42.994285	10.0.0.100	8.8.4.4	DNS	72 Standard query 0xb369 A www.ietf.org
3326	43.039067	13.83.65.43	10.0.0.100	TCP	66 443 → 55376 [ACK] Seq=1 Ack=2 Win=2050 Len=0 SLE=1 SRE=2
3327	43.046331	8.8.4.4	10.0.0.100	TCP	66 [TCP Window Update] 443 → 53737 [ACK] Seq=7916 Ack=2640 Win=380 Len=0 SLE=2868 SRE=2903
3328	43.056082	8.8.4.4	10.0.0.100	DNS	149 Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
3329	43.058123	8.8.8.8	10.0.0.100	DNS	149 Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
3330	43.060272	10.0.0.100	104.16.45.99	TCP	66 53792 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3331	43.061035	10.0.0.100	104.16.45.99	TCP	66 53793 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3332	43.062484	10.0.0.100	8.8.4.4	TLSv1.2	243 Application Data
3333	43.297245	104.16.45.99	10.0.0.100	TCP	66 443 → 53792 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3334	43.297368	10.0.0.100	104.16.45.99	TCP	54 53792 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
3335	43.297513	104.16.45.99	10.0.0.100	TCP	66 80 → 53793 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3336	43.297585	10.0.0.100	104.16.45.99	TCP	54 53793 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
3339	43.298576	10.0.0.100	104.16.45.99	TLSv1.3	603 Client Hello
3340	43.298965	10.0.0.100	104.16.45.99	HTTP	505 GET / HTTP/1.1
3341	43.307805	8.8.4.4	10.0.0.100	TCP	66 [TCP Window Update] 443 → 53737 [ACK] Seq=7916 Ack=2640 Win=380 Len=0 SLE=2868 SRE=2903

> Frame 3324: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{72634749-96BF-4B16-ACBE-E152688589CC}, id 0

> Ethernet II, Src: ac:7d:eb:a7:7d:3e (ac:7d:eb:a7:7d:3e), Dst: 00:d1:e6:e6:e6:e6 (00:d1:e6:e6:e6:e6)

> Internet Protocol Version 4, Src: 10.0.0.100, Dst: 8.8.8.8

> User Datagram Protocol, Src Port: 56488, Dst Port: 53

Source Port: 56488

Destination Port: 53

Length: 38

Checksum: 0x32a2 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

Если мы запустим ipconfig /all, то увидим, что он совпадает с адресом локального DNS-сервера:

```

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Физический адрес. . . . . : 52-9F-38-E2-60-6D
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да

```

адаптер Ethernet Ethernet 3:

```

DNS-суффикс подключения . . . . . :
Описание. . . . . : Remote NDIS Compatible Device
Физический адрес. . . . . : AC-7D-EB-A7-7D-3E
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::18b5:347:7066:8e42%12(Основной)
IPv4-адрес. . . . . : 10.0.0.100(Основной)
Маска подсети . . . . . : 255.0.0.0
Аренда получена. . . . . : 19 марта 2022 г. 14:09:20
Срок аренды истекает. . . . . : 20 марта 2022 г. 14:09:20
Основной шлюз. . . . . : 10.0.0.1
DHCP-сервер. . . . . : 10.0.0.1
IAID DHCPv6 . . . . . : 749501931
DUID клиента DHCPv6 . . . . . : 00-01-00-01-23-61-F3-32-2C-FD-A1-83-BA-9A
DNS-серверы. . . . . : 8.8.8.8
                        8.8.4.4
NetBios через TCP/IP. . . . . : Включен

```

4. Запрашивается запись типа A (адрес хоста):

3324	42.916960	10.0.0.100	8.8.8.8	DNS	72 Standard query 0xb369 A www.ietf.org
3325	42.994285	10.0.0.100	8.8.4.4	DNS	72 Standard query 0xb369 A www.ietf.org
3326	43.039067	13.83.65.43	10.0.0.100	TCP	66 443 → 5376 [ACK] Seq=1 Ack=2 Win=2050 Len=0 SLE=1 SRE=2
3327	43.046331	8.8.4.4	10.0.0.100	TCP	66 [TCP Window Update] 443 → 53737 [ACK] Seq=7916 Ack=2640 Win=380 Len=0 SLE=2868 SRE=2903
3328	43.056082	8.8.4.4	10.0.0.100	DNS	149 Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
3329	43.058123	8.8.8.8	10.0.0.100	DNS	149 Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
3330	43.066272	10.0.0.100	104.16.45.99	TCP	66 53792 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3331	43.061035	10.0.0.100	104.16.45.99	TCP	66 53793 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3332	43.062484	10.0.0.100	8.8.4.4	TLSv1.2	243 Application Data
3333	43.297245	104.16.45.99	10.0.0.100	TCP	66 443 → 53792 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3334	43.297368	10.0.0.100	104.16.45.99	TCP	64 53792 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0

Questions: 1
Answer RRs: 0
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)

[Response In: 3329]

Ответов в запросе не содержится:

No.	Time	Source	Destination	Protocol	Length	Info
3315	41.324236	173.194.222.136	10.0.0.100	TCP	54	443 → 53788 [ACK] Seq=1518 Ack=2050 Win=70656 Len=0
3316	42.255197	44.195.64.169	10.0.0.100	TCP	54	[TCP Dup ACK 1902#1] 443 → 58023 [ACK] Seq=1 Ack=1 Win=13 Len=0
3317	42.255282	10.0.0.100	44.195.64.169	TCP	54	[TCP Dup ACK 1903#1] [TCP ACKed unseen segment] 58023 → 443 [ACK] Seq=1 Ack=2 Win=514 Len=0
3318	42.807482	10.0.0.100	5.255.255.55	TCP	55	55845 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
3319	42.838243	10.0.0.100	13.83.65.43	TCP	55	55376 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
3320	42.851685	149.154.167.50	10.0.0.100	SSL	159	Continuation Data
3321	42.871070	5.255.255.55	10.0.0.100	TCP	66	443 → 55845 [ACK] Seq=1 Ack=2 Win=166 Len=0 SLE=1 SRE=2
3322	42.900437	10.0.0.100	149.154.167.50	TCP	54	64409 → 443 [ACK] Seq=1271 Ack=1340 Win=515 Len=0
3323	42.915983	10.0.0.100	8.8.4.4	TLSv1.2	89	Application Data
3324	42.916960	10.0.0.100	8.8.8.8	DNS	72	Standard query 0xb369 A www.ietf.org
3325	42.994285	10.0.0.100	8.8.4.4	DNS	72	Standard query 0xb369 A www.ietf.org
3326	43.039067	13.83.65.43	10.0.0.100	TCP	66	443 → 55376 [ACK] Seq=1 Ack=2 Win=2050 Len=0 SLE=1 SRE=2
3327	43.046331	8.8.4.4	10.0.0.100	TCP	66	[TCP Window Update] 443 → 53737 [ACK] Seq=7916 Ack=2640 Win=380 Len=0 SLE=2868 SRE=2903
3328	43.056082	8.8.4.4	10.0.0.100	DNS	149	Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
3329	43.058123	8.8.8.8	10.0.0.100	DNS	149	Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
3330	43.060272	10.0.0.100	104.16.45.99	TCP	66	53792 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3331	43.061035	10.0.0.100	104.16.45.99	TCP	66	53793 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3332	43.062484	10.0.0.100	8.8.4.4	TLSv1.2	243	Application Data
3333	43.297245	104.16.45.99	10.0.0.100	TCP	66	443 → 53792 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3334	43.297245	10.0.0.100	104.16.45.99	TCP	54	53792 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0

Domain Name System (query)
Transaction ID: 0xb369
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.ietf.org: type A, class IN
Name: www.ietf.org
[Name Length: 12]
[Label Count: 3]

5. Пришло 3 ответа:

3324	42.916960	10.0.0.100	8.8.8.8	DNS	72	Standard query 0xb369 A www.ietf.org
3325	42.994285	10.0.0.100	8.8.4.4	DNS	72	Standard query 0xb369 A www.ietf.org
3326	43.039067	13.83.65.43	10.0.0.100	TCP	66	443 → 55376 [ACK] Seq=1 Ack=2 Win=2050 Len=0 SLE=1 SRE=2
3327	43.046331	8.8.4.4	10.0.0.100	TCP	66	[TCP Window Update] 443 → 53737 [ACK] Seq=7916 Ack=2640 Win=380 Len=0 SLE=2868 SRE=2903
3328	43.056082	8.8.4.4	10.0.0.100	DNS	149	Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
3329	43.058123	8.8.8.8	10.0.0.100	DNS	149	Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
3330	43.060272	10.0.0.100	104.16.45.99	TCP	66	53792 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3331	43.061035	10.0.0.100	104.16.45.99	TCP	66	53793 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3332	43.062484	10.0.0.100	8.8.4.4	TLSv1.2	243	Application Data
3333	43.297245	104.16.45.99	10.0.0.100	TCP	66	443 → 53792 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3334	43.297368	10.0.0.100	104.16.45.99	TCP	54	53792 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
3335	43.297513	104.16.45.99	10.0.0.100	TCP	66	80 → 53793 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3336	43.297585	10.0.0.100	104.16.45.99	TCP	54	53793 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
3330.43.208576	10.0.0.100	104.16.45.99	TLSv1.3	603	Client Hello	

Domain Name System (response)

Transaction ID: 0xb369

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

Они представляют собой каноническое имя (CNAME), которое привязывает псевдоним к действительному (каноническому) доменному имени, а также 2 IP-адреса веб-сервера:

```

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
> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
[Request In: 3324]
[Time: 0.141163000 seconds]

```

6. Последующий TCP-пакет с флагом SYN отправляется на IP-адрес 104.16.45.99, что соответствует адресу, полученным в ответном сообщении ранее:

No.	Time	Source	Destination	Protocol	Length	Info
3318	42.807482	10.0.0.100	5.255.255.55	TCP	55	55845 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
3319	42.838243	10.0.0.100	13.83.65.43	TCP	55	55376 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
3320	42.851685	149.154.167.50	10.0.0.100	SSL	159	Continuation Data
3321	42.871070	5.255.255.55	10.0.0.100	TCP	66	443 → 55845 [ACK] Seq=1 Ack=2 Win=166 Len=0 SLE=1 SRE=2
3322	42.900437	10.0.0.100	149.154.167.50	TCP	54	64499 → 443 [ACK] Seq=1271 Ack=1140 Win=515 Len=0
3323	42.915983	10.0.0.100	8.8.4.4	TLSv1.2	89	Application Data
3324	42.916960	10.0.0.100	8.8.8.8	DNS	72	Standard query 0xb369 A www.ietf.org
3325	42.994285	10.0.0.100	8.8.4.4	DNS	72	Standard query 0xb369 A www.ietf.org
3326	43.039067	13.83.65.43	10.0.0.100	TCP	66	443 → 55376 [ACK] Seq=1 Ack=2 Win=2050 Len=0 SLE=1 SRE=2
3327	43.046331	8.8.4.4	10.0.0.100	TCP	66	[TCP Window Update] 443 → 53737 [ACK] Seq=7916 Ack=2640 Win=380 Len=0 SLE=2868 SRE=2903
3328	43.056082	8.8.4.4	10.0.0.100	DNS	149	Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
3329	43.058123	8.8.8.8	10.0.0.100	DNS	149	Standard query response 0xb369 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.44.99 A 104.16.45.99
3330	43.060272	10.0.0.100	104.16.45.99	TCP	66	53792 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3331	43.061035	10.0.0.100	104.16.45.99	TCP	66	53793 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3332	43.062484	10.0.0.100	8.8.4.4	TLSv1.2	243	Application Data
3333	43.297245	104.16.45.99	10.0.0.100	TCP	66	443 → 53792 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3334	43.297368	10.0.0.100	104.16.45.99	TCP	54	53792 → 443 [ACK] Seq=1 Ack=1 Win=131840 Len=0
3335	43.297513	104.16.45.99	10.0.0.100	TCP	66	80 → 53793 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 WS=1024
3336	43.297585	10.0.0.100	104.16.45.99	TCP	54	53793 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
3330.42.208576	10.0.0.100	104.16.45.99	TLSv1.2	603	Client Hello	

> Frame 3330: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{72634749-96BF-4B16-ACBE-E152688589CC}, id 0
 > Ethernet II, Src: ac:7d:eb:a7:7d:3e (ac:7d:eb:a7:7d:3e), Dst: 00:d1:e6:e6:e6:e6 (00:d1:e6:e6:e6:e6)
 > Internet Protocol Version 4, Src: 10.0.0.100, Dst: 104.16.45.99
 > Transmission Control Protocol, Src Port: 53792, Dst Port: 443, Seq: 0, Len: 0

7. Да, потом отправляет еще 2 DNS-запроса

Задание В

1. Порт назначения в запросе – 53

No.	Time	Source	Destination	Protocol	Length	Info
226	20.622880	10.0.0.100	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
227	20.650121	8.8.8.8	10.0.0.100	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
228	20.653542	10.0.0.100	8.8.8.8	DNS	71	Standard query 0x0002 A www.spbu.ru
229	20.686756	8.8.8.8	10.0.0.100	DNS	101	Standard query response 0x0002 A www.spbu.ru CNAME spbu.ru A 82.202.190.112
230	20.690122	10.0.0.100	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.spbu.ru
232	20.744892	8.8.8.8	10.0.0.100	DNS	138	Standard query response 0x0003 AAAA www.spbu.ru CNAME spbu.ru SOA ns.pu.ru
234	21.253735	10.0.0.100	8.8.8.8	DNS	80	Standard query 0x6e81 A cc-api-data.adobe.io
235	21.292956	8.8.8.8	10.0.0.100	DNS	128	Standard query response 0x6e81 A cc-api-data.adobe.io A 3.248.26.100 A 54.74.179.44 A 54.77.72.255

> Frame 230: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{72634749-96BF-4B16-ACBE-E152688589CC}, id 0
 > Ethernet II, Src: ac:7d:eb:a7:7d:3e (ac:7d:eb:a7:7d:3e), Dst: 00:d1:e6:e6:e6:e6 (00:d1:e6:e6:e6:e6)
 > Internet Protocol Version 4, Src: 10.0.0.100, Dst: 8.8.8.8
 > User Datagram Protocol, Src Port: 55258, Dst Port: 53
 > Domain Name System (query)

Порт источника в ответе – также 53

No.	Time	Source	Destination	Protocol	Length	Info
226	20.622880	10.0.0.100	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
227	20.650121	8.8.8.8	10.0.0.100	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
228	20.653542	10.0.0.100	8.8.8.8	DNS	71	Standard query 0x0002 A www.spbu.ru
229	20.686756	8.8.8.8	10.0.0.100	DNS	101	Standard query response 0x0002 A www.spbu.ru CNAME spbu.ru A 82.202.190.112
230	20.690122	10.0.0.100	8.8.8.8	DNS	71	Standard query 0x0003 AAAA www.spbu.ru
232	20.744892	8.8.8.8	10.0.0.100	DNS	138	Standard query response 0x0003 AAAA www.spbu.ru CNAME spbu.ru SOA ns.pu.ru
234	21.253735	10.0.0.100	8.8.8.8	DNS	80	Standard query 0x6e81 A cc-api-data.adobe.io
235	21.292956	8.8.8.8	10.0.0.100	DNS	128	Standard query response 0x6e81 A cc-api-data.adobe.io A 3.248.26.100 A 54.74.179.44 A 54.77.72.255

> Frame 232: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface \Device\NPF_{72634749-96BF-4B16-ACBE-E152688589CC}, id 0
 > Ethernet II, Src: 00:d1:e6:e6:e6:e6 (00:d1:e6:e6:e6:e6), Dst: ac:7d:eb:a7:7d:3e (ac:7d:eb:a7:7d:3e)
 > Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.0.0.100
 > User Datagram Protocol, Src Port: 53, Dst Port: 55258
 > Domain Name System (response)

2. DNS-запрос был направлен на адрес 8.8.8.8, что, как мы выяснили ранее, совпадает с адресом локального DNS-сервера:

</

3. Запрашивается тип AAAA (IPv6-адрес), ответов не содержится:

Ethernet 3

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

4. Ответ один, это каноническое имя CNAME:

Ethernet 3					
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь					
dns					
No.	Time	Source	Destination	Protocol	Length Info
226	20.622880	10.0.0.100	8.8.8.8	DNS	80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
227	20.650121	8.8.8.8	10.0.0.100	DNS	104 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
228	20.653542	10.0.0.100	8.8.8.8	DNS	71 Standard query 0x0002 A www.spbu.ru
229	20.686756	8.8.8.8	10.0.0.100	DNS	101 Standard query response 0x0002 A www.spbu.ru CNAME spbu.ru A 82.202.190.112
230	20.690122	10.0.0.100	8.8.8.8	DNS	71 Standard query 0x0003 AAAA www.spbu.ru
232	20.744892	8.8.8.8	10.0.0.100	DNS	138 Standard query response 0x0003 AAAA www.spbu.ru CNAME spbu.ru SOA ns.pu.ru
234	21.253735	10.0.0.100	8.8.8.8	DNS	80 Standard query 0x6e81 A cc-api-data.adobe.io
235	21.292956	8.8.8.8	10.0.0.100	DNS	128 Standard query response 0x6e81 A cc-api-data.adobe.io A 3.248.26.100 A 54.74.179.44 A 54.77.72.255

Domain Name System (response)

Transaction ID: 0x0003

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 1

Additional RRs: 0

Queries

Answers

www.spbu.ru: type CNAME, class IN, cname spbu.ru

Authoritative nameservers

[Request In: 230]

Задание Г

1. Запрос отправлен на IP-адрес 8.8.8.8, что совпадает с адресом локального сервера по умолчанию:

200	21.970355	10.0.0.100	8.8.8.8	DNS	67 Standard query 0x0002 NS spbu.ru
201	22.012731	8.8.8.8	10.0.0.100	DNS	123 Standard query response 0x0002

2. Запрашиваются данные типа NS (authoritative Name Server), ответов нет:

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
<div> <div>spbu.ru: type NS, class IN</div> <div> <div>Name: spbu.ru</div> <div>[Name Length: 7]</div> <div>[Label Count: 2]</div> <div>Type: NS (authoritative Name Server) (2)</div> <div>Class: IN (0x0001)</div> </div> </div>
[Response In: 201]

3. В ответном сообщении содержатся имена трех серверов: ns2.pu.ru, ns7.spbu.ru, ns.pu.ru. IP – адресов в ответе нет:

▼ Answers

- > spbu.ru: type NS, class IN, ns ns2.pu.ru
- > spbu.ru: type NS, class IN, ns ns7.spbu.ru
- > spbu.ru: type NS, class IN, ns ns.pu.ru

[Request In: 200]

▼ Answers

- ▼ 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: 9
 - Name Server: ns2.pu.ru
- > spbu.ru: type NS, class IN, ns ns7.spbu.ru
- > spbu.ru: type NS, class IN, ns ns.pu.ru

[Request In: 200]

[Time: 0.042376000 seconds]

Задание Д

1. Последний запрос был направлен на IP-адрес 195.70.196.210, принадлежащий spbu.ru:

No.	Time	Source	Destination	Protocol	Length	Info
52	12.114738	10.0.0.100	8.8.8.8	DNS	80	Standard query 0x1b02 A activity.windows.com
53	12.146739	10.0.0.100	8.8.4.4	DNS	80	Standard query 0x1b02 A activity.windows.com
54	12.158602	8.8.8.8	10.0.0.100	DNS	141	Standard query response 0x1b02 A activity.windows.com CNAME activity-geo.trafficmanager.net A 20.54.232.160
56	12.183976	8.8.4.4	10.0.0.100	DNS	141	Standard query response 0x1b02 A activity.windows.com CNAME activity-geo.trafficmanager.net A 20.54.232.160
106	17.178212	10.0.0.100	8.8.8.8	DNS	73	Standard query 0x47fa A p13n.adobe.io
107	17.209899	8.8.8.8	10.0.0.100	DNS	137	Standard query response 0x47fa A p13n.adobe.io A 107.22.247.231 A 34.193.227.236 A 54.144.73.197 A 18.207.85.246
140	18.414183	10.0.0.100	8.8.8.8	DNS	69	Standard query 0xd466 A ns2.pu.ru
143	18.452374	10.0.0.100	8.8.4.4	DNS	69	Standard query 0xd466 A ns2.pu.ru
144	18.454309	8.8.8.8	10.0.0.100	DNS	85	Standard query response 0xd466 A ns2.pu.ru A 195.70.196.210
145	18.456758	10.0.0.100	195.70.196.210	DNS	87	Standard query 0x0001 PTR 210.196.70.195.in-addr.arpa PTR ns2.pu.ru NS ns2.pu.ru A 195.70.196.210 A 195.70.196.210
146	18.480032	195.70.196.210	10.0.0.100	DNS	173	Standard query response 0x0001 PTR 210.196.70.195.in-addr.arpa PTR ns2.pu.ru NS ns2.pu.ru A 195.70.196.210 A 195.70.196.210
147	18.484217	10.0.0.100	195.70.196.210	DNS	71	Standard query 0x0002 A www.spbu.ru
148	18.488516	8.8.4.4	10.0.0.100	DNS	85	Standard query response 0xd466 A ns2.pu.ru A 195.70.196.210
149	18.520068	195.70.196.210	10.0.0.100	DNS	205	Standard query response 0x0002 A www.spbu.ru CNAME spbu.ru A 82.202.190.112 NS ns2.pu.ru NS ns7.spbu.ru NS ns.pu.ru A 195.70.196.210
150	18.521195	10.0.0.100	195.70.196.210	DNS	71	Standard query 0x0003 AAAA www.spbu.ru
151	18.559884	195.70.196.210	10.0.0.100	DNS	138	Standard query response 0x0003 AAAA www.spbu.ru CNAME spbu.ru SOA ns.pu.ru

> Frame 150: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{72634749-968F-4B16-ACBE-E152688589CC}, id 0
> Ethernet II, Src: ac:7d:eb:a7:7d:3e (ac:7d:eb:a7:7d:3e), Dst: 00:d1:e6:e6:e6:e6 (00:d1:e6:e6:e6:e6)
> Internet Protocol Version 4, Src: 10.0.0.100, Dst: 195.70.196.210
> User Datagram Protocol, Src Port: 58600, Dst Port: 53
▼ Domain Name System (query)
Transaction ID: 0x0003
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
▼ Queries

2. Запрашивается тип AAAA (IPv6-адрес), ответов не содержится:

150	18.521195	10.0.0.100	195.70.196.210	DNS	71 Standard query 0x0003 AAAA www.spbu.ru
151	18.559884	195.70.196.210	10.0.0.100	DNS	138 Standard query response 0x0003 AAAA www.spbu.ru CNAME spbu.ru SOA ns.pu.ru

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.spbu.ru: type AAAA, class IN
Name: www.spbu.ru
[Name Length: 11]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
[Response In: 151]

0000	00 d1 e6 e6 e6 ac 7d eb a7 7d 3e 08 00 45 00} ..}>..E
0010	00 39 ed 2f 00 00 80 11 bb 07 0a 00 00 64 c3 46	.9 /... ..d.F
0020	c4 d2 e4 e8 00 35 00 25 92 c9 00 03 01 00 00 01	...5 %
0030	00 00 00 00 00 00 03 77 77 77 04 73 70 62 75 02-w ww.spbu-
0040	72 75 00 00 1c 00 01	ru.....

Активация Wi
Чтобы активировать
"Параметры".

3. Ответ один, это каноническое имя CNAME:

150	18.521195	10.0.0.100	195.70.196.210	DNS	71 Standard query 0x0003 AAAA www.spbu.ru
151	18.559884	195.70.196.210	10.0.0.100	DNS	138 Standard query response 0x0003 AAAA www.spbu.ru CNAME spbu.ru SOA ns.pu.ru


Answer RRs: 1
Authority RRs: 1
Additional RRs: 0
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

Задание Е

- Whois – база данных, содержащая сведения о доменах. В ней можно найти сведения о спонсирующем регистраторе, DNS-серверы и статус домена, контакты администратора и других технических специалистов, информацию о дате создания и сроке регистрации, проверить занятость домена, определить с ее помощью связи компании, организации или отдельного лица с доменным именем, а также определить сторону, управляющей сайтом или другим общественным сервисом при помощи доменного имени, в коммерческих или других целях и т. п.
- С помощью сервиса <https://www.reg.ru/whois/> была получена информация о DNS-серверах интернет-магазина «OZON»:

Информация реестра

Домен	OZON.RU
Сервер DNS	ns4-cloud.nic.ru.
Сервер DNS	ns4-l2.nic.ru.
Сервер DNS	ns8-cloud.nic.ru.
Сервер DNS	ns8-l2.nic.ru.
Сервер DNS	nsz1s1.ozon.ru. 185.73.193.15
Сервер DNS	nsz20s1.ozon.ru. 185.73.195.247
Сервер DNS	nsz23s1.ozon.ru. 91.223.93.10
Состояние	зарегистрирован, делегирован, проверен
Администратор домена	Организация « LLC "Internet Solutions" ⓘ »

 Информация
об администраторе

3.

```
C:\Users\Анастасия>nslookup www.ozon.ru 8.8.8.8
Получены данные: dns.google
Address: 8.8.8.8

Не заслуживающий доверия ответ:
Получены данные: www.ozon.ru
Address: 178.248.238.156
```

```
C:\Users\Анастасия>nslookup www.ozon.ru 185.73.193.15
ТхЁтхЁ: nsz1s1.ozon.ru
Address: 185.73.193.15
```

```
Лб : www.ozon.ru
Address: 178.248.238.156
```

```
C:\Users\Анастасия>nslookup www.ozon.ru 91.223.93.10
ТхЁтхЁ: nsz23s1.ozon.ru
Address: 91.223.93.10
```

```
Лб : www.ozon.ru
Address: 178.248.238.156
```