

Задание 1.

Сервер в Азии

```
dumtrii@dumtrii-peka:~  
-> Could not find all required packages:  
    nslookup (Target)  
^C  
[dumtrii@dumtrii-peka ~]$ yay -S nslookup  
-> Could not find all required packages:  
    nslookup (Target)  
[dumtrii@dumtrii-peka ~]$ nslookup www.huawei.com  
Server:          192.168.1.1  
Address:         192.168.1.1#53  
  
Non-authoritative answer:  
www.huawei.com canonical name = www.huawei.com.akadns.net.  
www.huawei.com.akadns.net canonical name = ion-ssl6.huawei.com.edgekey.net.  
ion-ssl6.huawei.com.edgekey.net canonical name = e11285.dsca.akamaiedge.net.  
Name:   e11285.dsca.akamaiedge.net  
Address: 95.100.189.124  
Name:   e11285.dsca.akamaiedge.net  
Address: 2a02:2d8:0:7986::2c15  
Name:   e11285.dsca.akamaiedge.net  
Address: 2a02:2d8:0:798e::2c15  
  
[dumtrii@dumtrii-peka ~]$
```

Универ в Европе

```
dumtrii@dumtrii-peka:~  
Name:   e11285.dsca.akamaiedge.net  
Address: 2a02:2d8:0:798e::2c15  
  
[dumtrii@dumtrii-peka ~]$ nslookup ethz.ch  
Server:          192.168.1.1  
Address:         192.168.1.1#53  
  
Non-authoritative answer:  
Name:   ethz.ch  
Address: 129.132.19.216  
Name:   ethz.ch  
Address: 2001:67c:10ec:254::216  
  
[dumtrii@dumtrii-peka ~]$ nslookup www.ethz.ch  
Server:          192.168.1.1  
Address:         192.168.1.1#53  
  
Non-authoritative answer:  
Name:   www.ethz.ch  
Address: 129.132.19.216  
Name:   www.ethz.ch  
Address: 2001:67c:10ec:254::216  
  
[dumtrii@dumtrii-peka ~]$
```

Много IP адресов:

```
dumtrii@dumtrii-peka:~  
[dumtrii@dumtrii-peka ~]$ nslookup yandex.ru/  
Server:      192.168.1.1  
Address:     192.168.1.1#53  
  
** server can't find yandex.ru/: NXDOMAIN  
  
[dumtrii@dumtrii-peka ~]$ nslookup yandex.ru  
Server:      192.168.1.1  
Address:     192.168.1.1#53  
  
Non-authoritative answer:  
Name:   yandex.ru  
Address: 5.255.255.60  
Name:   yandex.ru  
Address: 77.88.55.80  
Name:   yandex.ru  
Address: 5.255.255.5  
Name:   yandex.ru  
Address: 77.88.55.77  
Name:   yandex.ru  
Address: 2a02:6b8:a::a  
  
[dumtrii@dumtrii-peka ~]$
```

Один IP у СПбГУ:

```
dumtrii@dumtrii-peka:~  
Server:      192.168.1.1  
Address:     192.168.1.1#53  
  
Non-authoritative answer:  
Name:   yandex.ru  
Address: 5.255.255.60  
Name:   yandex.ru  
Address: 77.88.55.80  
Name:   yandex.ru  
Address: 5.255.255.5  
Name:   yandex.ru  
Address: 77.88.55.77  
Name:   yandex.ru  
Address: 2a02:6b8:a::a  
  
[dumtrii@dumtrii-peka ~]$ 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  
  
[dumtrii@dumtrii-peka ~]$
```

Задание 2.

1. UDP
2. 53
3. 192.168.1.1, cat /etc/resolv.conf дает то же
4. Сначала AAAA (IPv6 Address) (28), потом A (Host Address) (1). Ответов нет
5. 3 ответа, в каждом содержится ipv4 адрес
6. Да, соответствует
7. Судя по количеству DNS-запросов — да.

Wireshark capture of DNS traffic on interface enp4s0. The filter is `ip.addr == 192.168.1.48 && dns`.

No.	Time	Source	Destination	Protocol	Length	Info
196	6.330995841	192.168.1.48	192.168.1.1	DNS	91	Standard query 0x4ddb A www.ietf.org.cdn.cloudflare.net
197	6.332364233	192.168.1.1	192.168.1.48	DNS	123	Standard query response 0x4ddb A www.ietf.org.cdn.cloudflare.net A 194.16.45.99 A 194.16.44.99
198	6.332454232	192.168.1.48	192.168.1.1	DNS	91	Standard query 0xba06 A www.ietf.org.cdn.cloudflare.net
200	6.334174515	192.168.1.1	192.168.1.48	DNS	123	Standard query response 0xba06 A www.ietf.org.cdn.cloudflare.net A 194.16.45.99 A 194.16.44.99
676	6.466790947	192.168.1.48	192.168.1.1	DNS	78	Standard query 0xf2b2 A analytics.ietf.org
677	6.466819961	192.168.1.48	192.168.1.1	DNS	78	Standard query 0x9de1 AAAA analytics.ietf.org
678	6.466844998	192.168.1.48	192.168.1.1	DNS	78	Standard query 0x7ac6 A analytics.ietf.org
679	6.466866649	192.168.1.48	192.168.1.1	DNS	78	Standard query 0xe85a AAAA analytics.ietf.org
844	6.504249938	192.168.1.1	192.168.1.48	DNS	106	Standard query response 0x9de1 AAAA analytics.ietf.org AAAA 2001:1900:3001:11::2d

Class: IN (0x0001)

Answers

- www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 194.16.45.99
 - 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: 194.16.45.99
- www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 194.16.44.99
 - 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: 194.16.44.99

[Request In: 196]

[Time: 0.001368392 seconds]

0030 00 02 00 00 00 00 03 77 77 77 04 69 65 74 66 03W www.ietf
0040 6f 72 67 93 63 64 6e 0a 63 6e 6f 75 64 66 6c 61rg-cdn- cloudfla
0050 72 65 03 6e 65 74 00 00 01 00 01 c0 0c 00 01 00re.net-
0060 01 00 00 01 2c 00 04 68 10 2d 63 c0 0c 00 01 00-c
0070 01 00 00 01 2c 00 04 68 10 2c 63-h -,c

Query Type (dns.qry.type), 2 bytes

Packets: 1116 · Displayed: 28 (2.5%) · Dropped: 0 (0.0%)

Profile: Default

Задание 3.

1. Назначения: 53, источник: 59066
2. 192.168.1.1, совпадает
3. AAAA (IPv6 Address) (28). Ответов нет
4. Повторение запроса, ответов нет.

Есть поле Authoritative nameservers. В нем primary name server: ns.pu.ru. (ns.pu.ru — новосибирский университет). Почта ответственного авторитета и другие поля.

The image shows a Wireshark packet capture analysis of a DNS query and response. The filter is set to `ip.addr == 192.168.1.48`. The packet list shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
45	2.834299401	192.168.1.48	192.168.1.1	DNS	67	Standard query 0xeb2 A spbu.ru
46	2.835771967	192.168.1.1	192.168.1.48	DNS	83	Standard query response 0xeb2 A spbu.ru A 82.202.190.112
47	2.835879570	192.168.1.48	192.168.1.1	DNS	67	Standard query 0x7dcb AAAA spbu.ru
48	2.844195238	192.168.1.1	192.168.1.48	DNS	122	Standard query response 0x7dcb AAAA spbu.ru SOA ns.pu.ru

The packet details pane shows the structure of the selected packet (No. 47):

- [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: 30 (30 seconds)
 - Data length: 43
 - 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)

The packet bytes pane shows the raw data of the packet, with a text item (text) of 55 bytes highlighted.

Packets: 110 · Displayed: 4 (3.6%) · Dropped: 0 (0.0%) · Profile: Default

Задание 4.

1. 192.168.1.1, совпадает.
2. AAAA (IPv6 Address) (28), ответов нет
3. ns.pu.ru. Адреса нет

Wireshark capture showing DNS traffic. The filter is `ip.addr == 192.168.1.48`. The packet list shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
7	0.687830108	192.168.1.48	192.168.1.1	DNS	67	Standard query 0xec24 AAAA spbu.ru
8	0.687870594	192.168.1.48	192.168.1.1	DNS	67	Standard query 0x5f93 AAAA spbu.ru
9	0.728060810	192.168.1.1	192.168.1.48	DNS	122	Standard query response 0xec24 AAAA spbu.ru SOA ns.pu.ru
10	0.728825611	192.168.1.1	192.168.1.48	DNS	122	Standard query response 0x5f93 AAAA spbu.ru SOA ns.pu.ru

The detailed view of packet 10 shows the following structure:

- [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: 30 (30 seconds)
 - Data length: 43
 - 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: 8]
[Time: 0.040955107 seconds]

Packet 10 (0.728825611) details:

```
0000 70 85 c2 ff 50 bf 50 ff 20 68 3d 28 08 00 45 00  b...P...P...h=(...E-
0010 00 6c 50 b2 40 00 40 11 66 4d c0 a8 01 01 c0 a8  1P...@...fM...
0020 01 30 00 35 9f 9e 00 58 8a 3d 5f 93 81 80 00 01  0-5...X...=...
0030 00 00 00 01 00 00 04 73 70 62 75 02 72 75 00 00  .....s pbu.ru...
0040 1c 00 01 c0 0c 00 00 00 01 00 00 00 1e 00 2b 02  .....+...
```

Destination Hardware Address (eth.dst), 6 bytes

Packets: 49 - Displayed: 4 (8.2%) - Dropped: 0 (0.0%)

Profile: Default

Задание 5.

1. 192.70.196.210, нет, ns2.pu.ru
2. AAAA (IPv6 Address) (28), ответов нет
3. Ответов нет. Повторение запроса + тот же самый authority nameserver

Wireshark packet capture showing DNS traffic. The packet list shows a query for ns2.pu.ru and a response. The packet details show the authoritative nameserver information for spbu.ru.

No.	Time	Source	Destination	Protocol	Length	Info
42	2.722394436	192.168.1.1	192.168.1.48	DNS	85	Standard query response 0xb2ea A ns2.pu.ru A 195.70.196.210
43	2.723232389	192.168.1.1	192.168.1.48	DNS	85	Standard query response 0x7455 A ns2.pu.ru A 195.70.196.210
44	2.724086877	192.168.1.1	192.168.1.48	DNS	119	Standard query response 0x740b AAAA ns2.pu.ru SOA ns.pu.ru
45	2.724597751	192.168.1.48	195.70.196.210	DNS	71	Standard query 0xc558 A www.spbu.ru
46	2.725009299	192.168.1.1	192.168.1.48	DNS	119	Standard query response 0xc583 AAAA ns2.pu.ru SOA ns.pu.ru
47	2.726728779	195.70.196.210	192.168.1.48	DNS	205	Standard query response 0xc558 A www.spbu.ru CNAME spbu.ru A 82.202.190.112 NS ns7.spbu.ru NS ns8.spbu.ru
48	2.726950928	192.168.1.48	195.70.196.210	DNS	67	Standard query 0x402f AAAA spbu.ru
49	2.728618783	195.70.196.210	192.168.1.48	DNS	120	Standard query response 0x402f AAAA spbu.ru SOA ns.pu.ru

Packet 49 details:

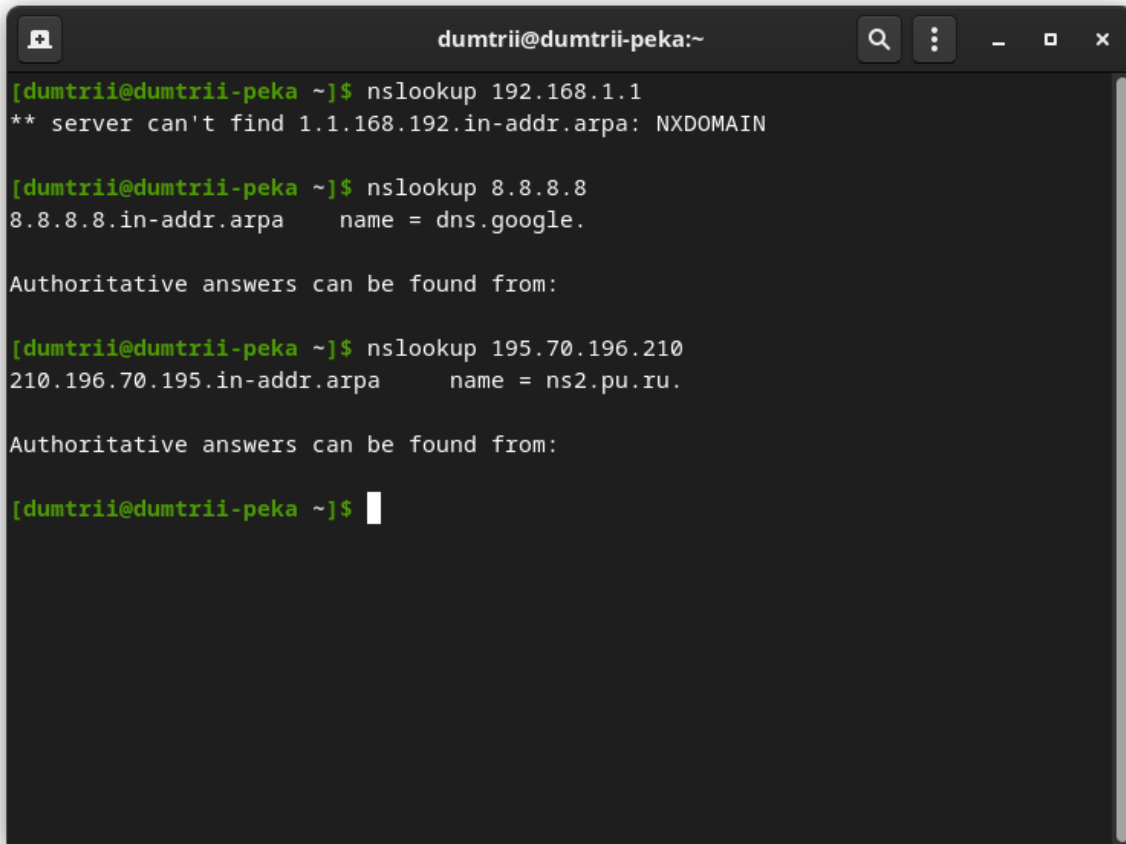
- [Label Count: 2]
- Type: AAAA (IPv6 Address) (28)
- Class: IN (0x0001)
- Authoritative nameservers
 - spbu.ru: type SOA, class IN, mname ns.pu.ru
 - Name: spbu.ru
 - Type: SOA (Start Of a zone of Authority) (6)
 - Class: IN (0x0001)
 - Time to live: 3600 (1 hour)
 - Data length: 41
 - Primary name 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: 48]
- [Time: 0.001667855 seconds]

Packet 49 raw data:

```
0030 00 00 00 01 00 00 04 73 70 62 75 02 72 75 00 00 .....s pbu.ru..
0040 1c 00 01 c9 0c 00 06 00 01 00 00 0e 10 09 29 02 ...
0050 6e 73 02 70 75 c9 11 0a 68 6f 73 74 6d 61 73 74 ns-pu... hostmast
0060 65 72 c0 20 78 85 74 7c 00 00 1c 20 00 00 0e 10 er-(x;t| .....
0070 00 09 3a 80 00 00 0e 1c .....
```

Задание 6.

1. whois — сервис для получения регистрационной информации домена.
2. whois 8.8.8.8 — Google, whois 195.70.196.210 — Spbu. Arin и RIPE

A terminal window titled 'dumtrii@dumtrii-peka:~' with standard window controls. It shows three 'nslookup' commands and their outputs. The first command for 192.168.1.1 results in an NXDOMAIN error. The second for 8.8.8.8 identifies it as dns.google. The third for 195.70.196.210 identifies it as ns2.pu.ru. The window has a dark background with green text for prompts and white for output.

```
[dumtrii@dumtrii-peka ~]$ nslookup 192.168.1.1
** server can't find 1.1.168.192.in-addr.arpa: NXDOMAIN

[dumtrii@dumtrii-peka ~]$ nslookup 8.8.8.8
8.8.8.8.in-addr.arpa      name = dns.google.

Authoritative answers can be found from:

[dumtrii@dumtrii-peka ~]$ nslookup 195.70.196.210
210.196.70.195.in-addr.arpa      name = ns2.pu.ru.

Authoritative answers can be found from:

[dumtrii@dumtrii-peka ~]$
```