

## Задачи по 4-й лабораторной

### А. Утилита nslookup

IP-адрес сайта [www.aabi.info](http://www.aabi.info)

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.aabi.info
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.aabi.info
Address: 101.231.81.172

(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```

С поиском авторитетного DNS-сервера на линуксе у меня возникла какая-то проблема, ничего не выводится :(

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup -type=NS www.harvard.edu
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.harvard.edu canonical name = pantheon-systems.map.fastly.net.

Authoritative answers can be found from:

(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```

Я попросила человека с Windows ввести команду у себя. Получилось, что авторитетный DNS-сервер для гарвардского университета - это ns1.fastly.net, но как на линукс это сделать, не смогла найти

```
C:\Users\Lenovo>nslookup -type=NS www.harvard.edu
ѠхѠѠѠ: UnKnown
Address: 192.168.0.1

Не заслуживающий доверия ответ:
www.harvard.edu canonical name = pantheon-systems.map.fastly.net

fastly.net
    primary name server = ns1.fastly.net
    responsible mail addr = hostmaster.fastly.com
    serial = 2017052201
    refresh = 3600 (1 hour)
    retry = 600 (10 mins)
    expire = 604800 (7 days)
    default TTL = 30 (30 secs)
```

Несколько IP-адресов имеет, например [www.google.com](http://www.google.com)

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 173.194.222.105
Name:   www.google.com
Address: 173.194.222.99
Name:   www.google.com
Address: 173.194.222.147
Name:   www.google.com
Address: 173.194.222.106
Name:   www.google.com
Address: 173.194.222.103
Name:   www.google.com
Address: 173.194.222.104
Name:   www.google.com
Address: 2a00:1450:4010:c0b::69
Name:   www.google.com
Address: 2a00:1450:4010:c0b::63
Name:   www.google.com
Address: 2a00:1450:4010:c0b::6a
Name:   www.google.com
Address: 2a00:1450:4010:c0b::93

(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```

Веб-сервер [www.spbu.ru](http://www.spbu.ru) имеет один IP-адрес

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.spbu.ru
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
www.spbu.ru  canonical name = spbu.ru.
Name:   spbu.ru
Address: 195.239.37.91

(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```

## Б. DNS-трассировка [www.ietf.org](http://www.ietf.org)

Используется транспортный протокол UDP (User Datagram Protocol)

166	4.993594694	192.168.0.104	192.168.0.1	DNS	102 Standard query 0xf4d8 A www.ietf.org.cdn.cloudflare.net OPT
167	4.999090835	192.168.0.1	192.168.0.104	DNS	134 Standard query response 0xf4d8 A www.ietf.org.cdn.cloudflare...

```
> Frame 166: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface wlo1, id 0
> Ethernet II, Src: IntelCor_af:c4:4f (b4:69:21:af:c4:4f), Dst: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 55007, Dst Port: 53
  - Source Port: 55007
  - Destination Port: 53
  - Length: 68
  - Checksum: 0x3aee [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 3]
  > [Timestamps]
> Domain Name System (query)
```

Порт назначения у запроса DNS - 53.

```
> Frame 166: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface wlo1, id 0
> Ethernet II, Src: IntelCor_af:c4:4f (b4:69:21:af:c4:4f), Dst: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 55007, Dst Port: 53
  - Source Port: 55007
  - Destination Port: 53
  - Length: 68
  - Checksum: 0x3aee [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 3]
  > [Timestamps]
> Domain Name System (query)
```

Запрос был отправлен на IP-адрес 192.168.0.1, DNS-адрес у меня такой же.

Запрашивается запись типа A (type A), ответов в запросе нет.

Пришло 2 ответа - 2 IP-адреса сервера:

```
> Domain Name System (response)
  - Transaction ID: 0xf4d8
  > Flags: 0x8180 Standard query response, No error
  - Questions: 1
  - Answer RRs: 2
  - Authority RRs: 0
  - Additional RRs: 1
  > Queries
    > www.ietf.org.cdn.cloudflare.net: type A, class IN
  > Answers
    > 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
  > Additional records
    [Request In: 166]
    [Time: 0.005406141 seconds]
```

IP-адрес назначения TCP-пакета с флагом SYN совпадает с одним из IP-адресов, полученным в ответном сообщении (104.16.44.99)

166	4.903594694	192.168.0.104	192.168.0.1	DNS	102 Standard query 0xf4d8 A www.ietf.org.cdn.cloudflare.net OPT
167	4.9090080835	192.168.0.1	192.168.0.104	DNS	134 Standard query response 0xf4d8 A www.ietf.org.cdn.cloudflare...
168	4.909393605	192.168.0.104	104.16.44.99	TCP	74 48360 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 ...
169	4.909554333	192.168.0.104	104.16.44.99	TCP	74 48362 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 ...
170	4.912546778	104.16.44.99	192.168.0.104	TCP	66 443 → 48360 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 S...
171	4.912582588	192.168.0.104	104.16.44.99	TCP	54 48360 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
172	4.912765761	104.16.44.99	192.168.0.104	TCP	66 443 → 48362 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 S...
173	4.912777032	192.168.0.104	104.16.44.99	TCP	54 48362 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0
174	4.912805858	192.168.0.104	104.16.44.99	TLsv1.3	603 Client Hello
175	4.912978826	192.168.0.104	104.16.44.99	TLsv1.3	603 Client Hello
176	4.915445362	104.16.44.99	192.168.0.104	TCP	54 443 → 48360 [ACK] Seq=1 Ack=550 Win=68608 Len=0
177	4.915677464	104.16.44.99	192.168.0.104	TCP	54 443 → 48362 [ACK] Seq=1 Ack=550 Win=67584 Len=0
178	4.918909733	104.16.44.99	192.168.0.104	TLsv1.3	266 Server Hello, Change Cipher Spec, Application Data

```
> Frame 168: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface wlo1, id 0
> Ethernet II, Src: IntelCor_af:c4:4f (b4:69:21:af:c4:4f), Dst: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 104.16.44.99
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 60
  - Identification: 0x9434 (37940)
  > Flags: 0x4000, Don't fragment
  - Fragment offset: 0
  - Time to live: 64
  - Protocol: TCP (6)
  - Header checksum: 0x5104 [validation disabled]
  - [Header checksum status: Unverified]
  - Source: 192.168.0.104
  - Destination: 104.16.44.99
> Transmission Control Protocol, Src Port: 48360, Dst Port: 443, Seq: 0, Len: 0
```

Да, потом отправляется еще 2 DNS-запроса.

## В. DNS-трассировка [www.spbu.ru](http://www.spbu.ru)

Порт назначения и источника - 53.

```
> Frame 3: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface wlo1, id 0
> Ethernet II, Src: IntelCor_af:c4:4f (b4:69:21:af:c4:4f), Dst: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 43631, Dst Port: 53
  - Source Port: 43631
  - Destination Port: 53
  - Length: 44
  - Checksum: 0x302a [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 1]
  > [Timestamps]
> Domain Name System (query)
```

```
> Frame 4: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface wlo1, id 0
> Ethernet II, Src: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70), Dst: IntelCor_af:c4:4f (b4:69:21:af:c4:4f)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.104
> User Datagram Protocol, Src Port: 53, Dst Port: 43631
  - Source Port: 53
  - Destination Port: 43631
  - Length: 97
  - Checksum: 0x8e31 [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 1]
  > [Timestamps]
> Domain Name System (response)
```

Запрос был отправлен на IP-адрес 192.168.0.1, что совпадает с адресом локального DNS-сервера.

```
> Frame 3: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface wlo1, id 0
> Ethernet II, Src: IntelCor_af:c4:4f (b4:69:21:af:c4:4f), Dst: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 43631, Dst Port: 53
  - Source Port: 43631
  - Destination Port: 53
  - Length: 44
  - Checksum: 0x302a [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 1]
  > [Timestamps]
> Domain Name System (query)
```

Запрашивается запись типа AAAA, ответов не содержится

```
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 43631, Dst Port: 53
  > Domain Name System (query)
    - Transaction ID: 0x2695
    > Flags: 0x0100 Standard query
    - Questions: 1
    - Answer RRs: 0
    - Authority RRs: 0
    - Additional RRs: 1
    > Queries
      > spbu.ru: type AAAA, class IN
        - Name: spbu.ru
        - [Name Length: 7]
        - [Label Count: 2]
        - Type: AAAA (IPv6 Address) (28)
        - Class: IN (0x0001)
    > Additional records
      > <Root>: type OPT
      [Response In: 4]
```

Приходит один ответ, каноническое имя CNAME

## Г. DNS-трассировка nslookup -type=NS

Запрос был отправлен на IP-адрес 192.168.0.1, что все так же совпадает с адресом локального DNS-сервера.

В этот раз запрашиваются данные типа NS, ответов нет.

В ответе содержатся имена трех серверов: ns2.ru.ru, ns.ru.ru, ns7.ru.ru, а адресов там нет.

No.	Time	Source	Destination	Protocol	Length	Info
26	3.413359654	192.168.0.104	192.168.0.1	DNS	82	Standard query 0x5185 NS www.spbu.ru OPT
27	3.420360405	192.168.0.1	192.168.0.104	DNS	168	Standard query response 0x5185 NS www.spbu.ru CNAME spbu.ru N...

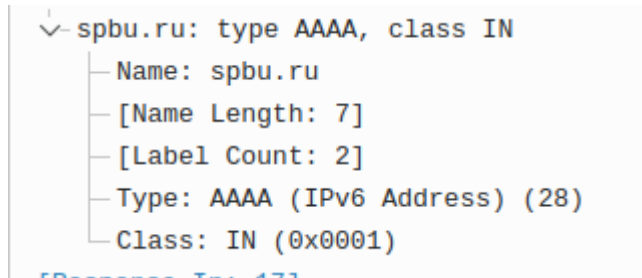
```
> Queries
> Answers
  > www.spbu.ru: type CNAME, class IN, cname spbu.ru
  > spbu.ru: type NS, class IN, ns ns.ru.ru
  > spbu.ru: type NS, class IN, ns ns2.ru.ru
  > spbu.ru: type NS, class IN, ns ns7.ru.ru
> Additional records
[Request In: 26]
```

## Д. DNS-трассировка nslookup www.spbu.ru ns2.ru.ru

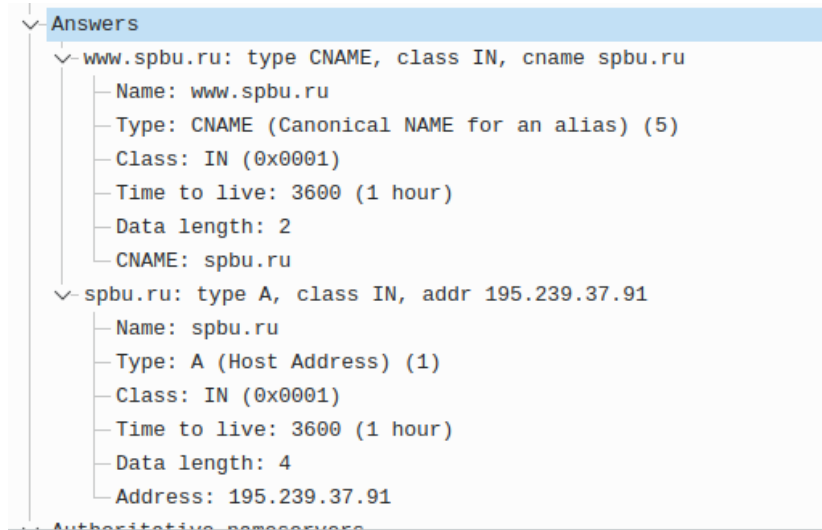
Последний запрос был отправлен на 195.70.196.210. Он принадлежит spbu.ru

```
> Frame 16: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface wlo1, id 0
> Ethernet II, Src: IntelCor_af:c4:4f (b4:69:21:af:c4:4f), Dst: Tp-LinkT_65:8a:70 (64:70:02:65:8a:70)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 195.70.196.210
> User Datagram Protocol, Src Port: 46824, Dst Port: 53
  > Domain Name System (query)
    - Transaction ID: 0x1d5f
    > Flags: 0x0100 Standard query
    - Questions: 1
    - Answer RRs: 0
    - Authority RRs: 0
    - Additional RRs: 0
    > Queries
    [Response In: 17]
```

Запрашивается тип AAAA, ответов нет.



В последнем ответов не было, а в предпоследнем нашлись два:



## Е. Сервисы whois

(ссылка на источник <https://support.google.com/domains/answer/3288171?hl=ru> )

WHOIS – это база данных, в которой хранятся сведения о доменах. В ней можно найти следующую информацию:

- контактные данные регистранта, администратора и технических специалистов;
- сведения о спонсирующем регистраторе;
- дату создания и обновления домена, а также срок его регистрации;
- DNS-серверы и статус домена.

Будем использовать сервис <https://www.reg.ru/whois/>

## Информация реестра

Домен	WILDBERRIES.RU
Сервер DNS	<a href="https://ns1.wildberries.ru">ns1.wildberries.ru</a> <a href="https://194.1.214.8">194.1.214.8</a>
Сервер DNS	<a href="https://ns2.wildberries.ru">ns2.wildberries.ru</a> <a href="https://91.230.107.70">91.230.107.70</a>
Сервер DNS	<a href="https://ns3.wildberries.ru">ns3.wildberries.ru</a> <a href="https://62.109.12.21">62.109.12.21</a>
Состояние	зарегистрирован, делегирован, проверен
Администратор домена	Частное лицо « <a href="#">Private Person</a> »
Регистратор	RU-CENTER-RU
Связь с администратором	— <a href="#">Форма обратной связи с администратором</a> — <a href="#">Обратиться через службу «Доменный брокер»</a>
Дата регистрации	2004-03-30T20:00:00Z
Дата окончания регистрации	2023-03-30T21:00:00Z
Преимущественное продление до	2023-05-01
Источник	TCI

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.wildberries.ru 192.168.0.1
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
Name:   www.wildberries.ru
Address: 185.138.253.1
Name:   www.wildberries.ru
Address: 185.138.254.1
Name:   www.wildberries.ru
Address: 185.138.252.1
```

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.wildberries.ru 194.1.214.8
Server:      194.1.214.8
Address:     194.1.214.8#53

Name:   www.wildberries.ru
Address: 185.138.254.1
Name:   www.wildberries.ru
Address: 185.138.253.1
Name:   www.wildberries.ru
Address: 185.138.252.1
```

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$ nslookup www.wildberries.ru 91.230.107.70
Server:      91.230.107.70
Address:     91.230.107.70#53

Name:   www.wildberries.ru
Address: 185.138.252.1
Name:   www.wildberries.ru
Address: 185.138.254.1
Name:   www.wildberries.ru
Address: 185.138.253.1
```

```
(base) margarita@margarita-HP-Pavilion-Laptop-15-cs0xxx:~$
```