

A)

1. Выполните nslookup, чтобы получить IP-адрес какого-либо веб-сервера в Азии

```
[ → ~ nslookup samsung.kr
Server:          192.168.0.1
Address:         192.168.0.1#53

Non-authoritative answer:
Name:    samsung.kr
Address: 112.106.21.70
```

2. Выполните nslookup, чтобы определить авторитетные DNS-серверы для какого-либо университета в Европе

o

```
[ → ~ nslookup -type=NS www.rug.nl
Server:          192.168.0.1
Address:         192.168.0.1#53

Non-authoritative answer:
www.rug.nl      canonical name = production.uems.rug.nl.

Authoritative answers can be found from:
rug.nl
origin = ns.rug.nl
mail addr = hostmaster.nic.rug.nl
serial = 2025030501
refresh = 14400
retry = 3600
expire = 1209600
minimum = 600
```

o

3. Используя nslookup, найдите веб-сервер, имеющий несколько IP-адресов.  
Сколько IP-адресов имеет веб-сервер вашего учебного заведения?

1

```
[ → ~ nslookup www.vk.com
Server:          192.168.0.1
Address:         192.168.0.1#53

Non-authoritative answer:
Name:    www.vk.com
Address: 93.186.225.194
Name:    www.vk.com
Address: 87.240.137.164
Name:    www.vk.com
Address: 87.240.132.67
Name:    www.vk.com
Address: 87.240.132.72
Name:    www.vk.com
Address: 87.240.129.133
Name:    www.vk.com
Address: 87.240.132.78
```

```
[ → ~ nslookup spbu.ru
Server:          192.168.0.1
Address:         192.168.0.1#53

Non-authoritative answer:
Name:    spbu.ru
Address: 85.193.83.151
```

4)

1. Найдите DNS-запрос и ответ на него. С использованием какого транспортного протокола они отправлены?

No.	Time	Source	Destination	Protocol	Length	Info
267	9.3556450	192.168.0.130	172.217.10.10	TLSv1...	151	Application Data
268	9.358507	192.168.0.130	172.217.18.10	TLSv1...	162	Application Data
269	9.359541	192.168.0.130	192.168.0.1	DNS	72	Standard query 0x10fb A www.ietf.org
270	9.359728	192.168.0.130	192.168.0.1	DNS	72	Standard query 0x7a96 HTTPS www.ietf.org
271	9.360056	192.168.0.130	142.250.184.202	UDP	405	57641 → 443 Len=363
272	9.360937	192.168.0.1	192.168.0.130	DNS	104	Standard query response 0xbc7e A www.ietf.org A 104.16.44.99 ...

UDP

2. Какой порт назначения у запроса DNS?

No.	Time	Source	Destination	Protocol	Length	Info
268	9.358507	192.168.0.130	172.217.18.10	TLSv1...	162	Application Data
269	9.359541	192.168.0.130	192.168.0.1	DNS	72	Standard query 0x10fb A www.ietf.org
270	9.359728	192.168.0.130	192.168.0.1	DNS	72	Standard query 0x7a96 HTTPS www.ietf.org
271	9.360056	192.168.0.130	142.250.184.202	UDP	405	57641 → 443 Len=363
272	9.360937	192.168.0.1	192.168.0.130	DNS	104	Standard query response 0xbc7e A www.ietf.org A 104.16.44.99 ...

53

3. На какой IP-адрес отправлен DNS-запрос? Используйте ipconfig для определения IP-адреса вашего локального DNS-сервера. Одинаковы ли эти два адреса?

192.168.0.1, ga

```
[ ~ ] ipconfig getoption en0 domain_name_server
192.168.0.1
[ ~ ]
```

4. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

UDP payload (30 bytes)	
Domain Name System (query)	
Transaction ID:	0x10fb
> 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]	
Type: A (1) (Host Address)	
Class: IN (0x0001)	
[Response In: 274]	

type A ,  
ответов нет

- 5. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

```
Questions: 1
Answer RRs: 2
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 (1) (Host Address)
        Class: IN (0x0001)
└─ Answers
    └─ www.ietf.org: type A, class IN, addr 104.16.44.99
        Name: www.ietf.org
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 78 (1 minute, 18 seconds)
        Data length: 4
        Address: 104.16.44.99
    └─ www.ietf.org: type A, class IN, addr 104.16.45.99
        Name: www.ietf.org
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 78 (1 minute, 18 seconds)
        Data length: 4
        Address: 104.16.45.99
```

2 ответа

IP-Адреса

- 6. Посмотрите на последующий TCP-пакет с флагом SYN, отправленный вашим компьютером. Соответствует ли IP-адрес назначения пакета с SYN одному из адресов, приведенных в ответном сообщении DNS?

823	9.961495	104.16.44.99	192.168.0.130	QUIC	1242 Protected Payload (KP0)
824	9.961496	104.16.44.99	192.168.0.130	QUIC	1242 Protected Payload (KP0)
825	9.961496	104.16.44.99	192.168.0.130	QUIC	1242 Protected Payload (KP0)
826	9.961657	192.168.0.130	104.16.44.99	QUIC	87 Protected Payload (KP0), DCID=0191566d94ab3cc4bd91056df8ab399...
827	9.961703	192.168.0.130	104.16.44.99	QUIC	87 Protected Payload (KP0), DCID=0191566d94ab3cc4bd91056df8ab399...
828	9.961988	192.168.0.130	104.16.45.99	TCP	78 51046 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=...
829	9.962970	104.16.44.99	192.168.0.130	QUIC	1242 Protected Payload (KP0)

Da

- 7. Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?

Da

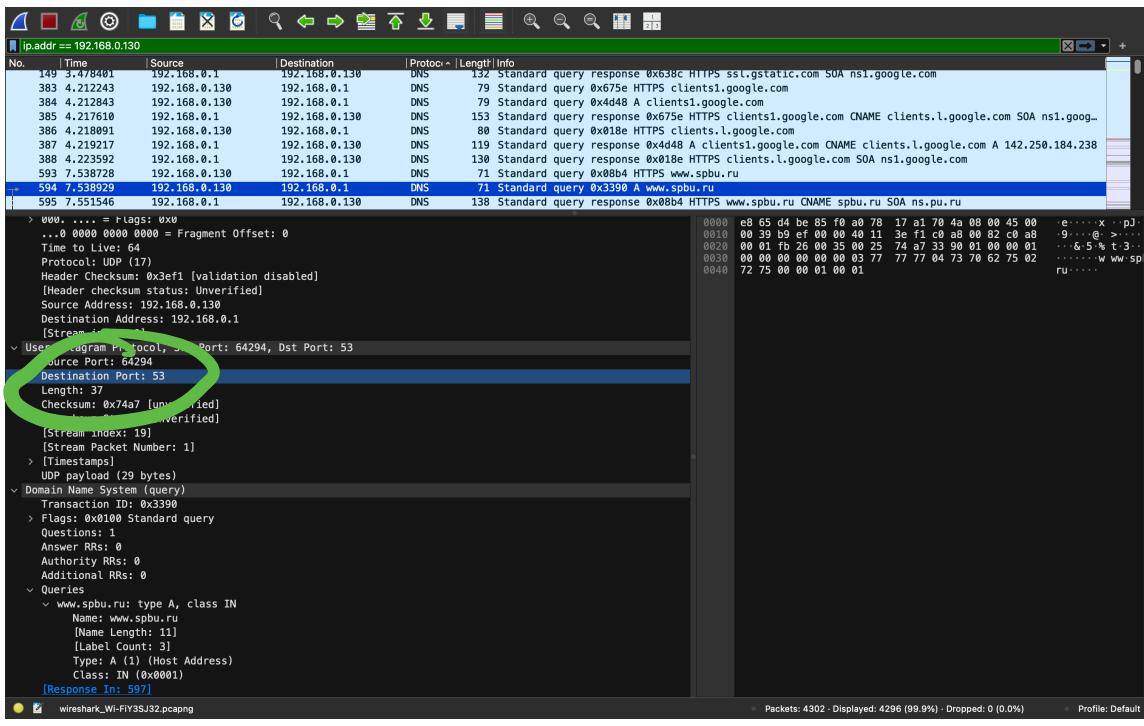
### Вопросы



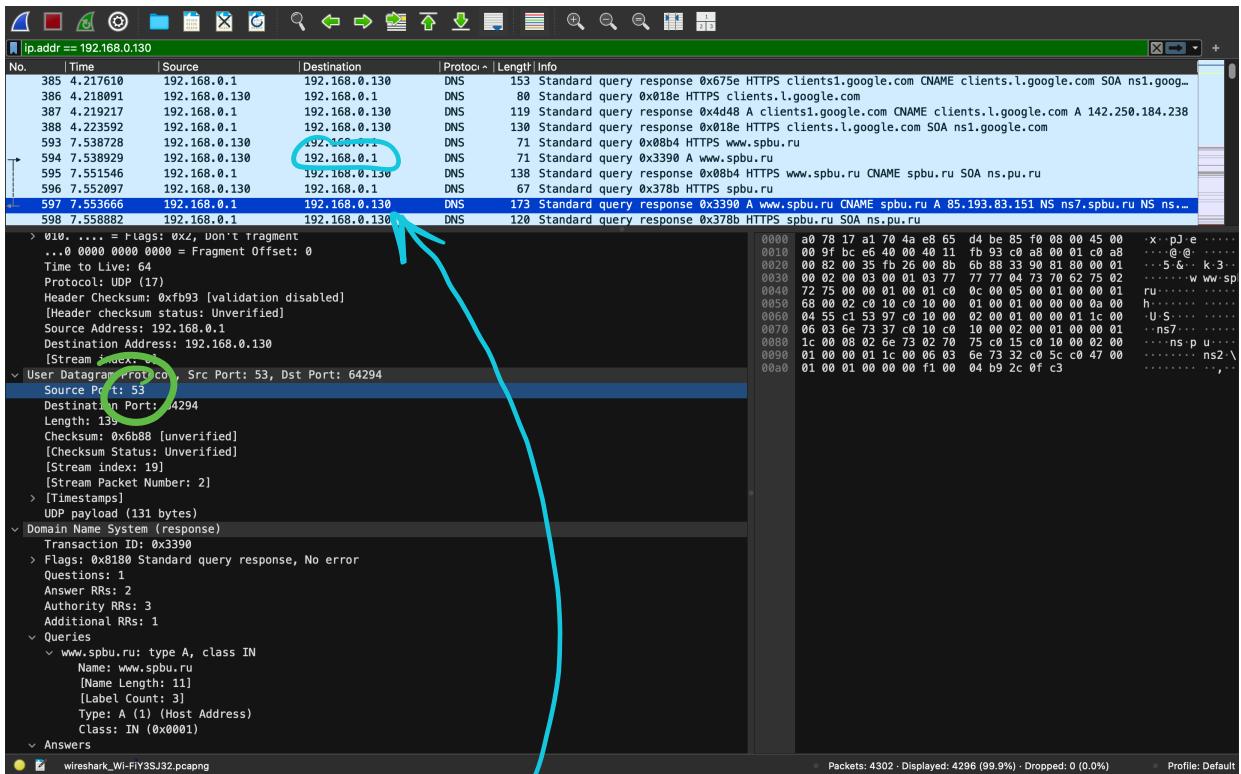
1. Каков порт назначения в запросе DNS? Какой порт источника в DNS-

ответе?

-



53, 53



2. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?

192.168.0.1, да

3. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

о

```
Transaction ID: 0x3390
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
< Queries
  < www.spbu.ru: type A, class IN
    Name: www.spbu.ru
    [Name Length: 11]
    [Label Count: 3]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
  [Response In: 597]
```

wireshark\_Wi-FiY3SJ32.pcapng

type A, нет

4. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

о

```
Name: www.spbu.ru
[Name Length: 11]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)
< Answers
  < www.spbu.ru: type CNAME, class IN, cname spbu.ru
    Name: www.spbu.ru
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 360 (6 minutes)
    Data length: 2
    CNAME: spbu.ru
  < spbu.ru: type A, class IN, addr 85.193.83.151
    Name: spbu.ru
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 10 (10 seconds)
    Data length: 4
    Address: 85.193.83.151
< Authoritative nameservers
  < spbu.ru: type NS, class IN, ns ns7.spbu.ru
    Name: spbu.ru
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 284 (4 minutes, 44 seconds)
    Data length: 6
    Name Server: ns7.spbu.ru
  < spbu.ru: type NS, class IN, ns ns.pu.ru
    Name: spbu.ru
    Type: NS (2) (authoritative Name Server)
    Class: IN (0x0001)
    Time to live: 284 (4 minutes, 44 seconds)
    Data length: 8
```

wireshark\_Wi-FiY3SJ32.pcapng

2 ответа,  
IP-адреса

## Вопросы

1. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?

о

50	26.480969	17.248.214.69	192.168.0.130	TCP	66	443 → 62992 [ACK] Seq=65 Ack=64 Win=63
51	26.480970	17.248.214.69	192.168.0.130	TCP	66	443 → 62992 [ACK] Seq=65 Ack=65 Win=63
52	26.827209	192.168.0.130	192.168.0.1	DNS	67	Standard query 0x49ae NS spbu.ru
53	26.849709	192.168.0.130	224.0.0.251	MDNS	466	Standard query response 0x0000 TXT, ca
55	26.888713	192.168.0.1	192.168.0.130	DNS	139	Standard query response 0x49ae NS spbu.ru
58	28.099706	192.168.0.130	224.0.0.251	MDNS	503	Standard query response 0x0000 TXT, ca
61	29.106372	192.168.0.130	224.0.0.251	MDNS	546	Standard query 0x0000 PTR lb._dns-sd._

198.168.0.1, га

2. Проанализируйте сообщение-запрос DNS. Запись какого типа  
запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

- 
- 

```

51 26.480970 17.248.214.69 192.168.0.130 TCP
52 26.827209 192.168.0.130 192.168.0.1 DNS
53 26.849709 192.168.0.130 224.0.0.251 MDNS
55 26.888713 192.168.0.1 192.168.0.130 DNS
58 28.099706 192.168.0.130 224.0.0.251 MDNS
61 29.106372 192.168.0.130 224.0.0.251 MDNS
66 29.850026 192.168.0.130 224.0.0.251 MDNS

Checksum: 0xda0e [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
[Stream Packet Number: 1]
> [Timestamps]
  UDP payload (25 bytes)
  Domain Name System (query)
    Transaction ID: 0x49ae
    > Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
    > Queries
      > spbu.ru: type NS, class IN
        Name: spbu.ru
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
        [Response In: 55]

```

Wireshark Wi-FIND4M32.pcapng

type NS,  
кнг

- 

3. Проанализируйте ответное сообщение DNS. Имена каких DNS-серверов  
университета в нем содержатся? А есть ли их адреса в этом ответе?

- 

```

  Class: IN (0x0001)
  > Answers
    > spbu.ru: type NS, class IN, ns ns.pu.ru
      Name: spbu.ru
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
      Time to live: 360 (6 minutes)
      Data length: 8
      Name Server: ns.pu.ru
    > spbu.ru: type NS, class IN, ns ns7.spbu.ru
      Name: spbu.ru
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
      Time to live: 360 (6 minutes)
      Data length: 6
      Name Server: ns7.spbu.ru
    > spbu.ru: type NS, class IN, ns ns2.pu.ru
      Name: spbu.ru
      Type: NS (2) (authoritative Name Server)
      Class: IN (0x0001)
      Time to live: 360 (6 minutes)
      Data length: 6
      Name Server: ns2.pu.ru

```

ns.pu.ru  
ns7.spbu.ru  
ns2.pu.ru

кнг, адреса отсутствуют

Д)

- На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию? Если нет, то какому хосту он принадлежит?

о

No.	Time	Source	Destination	Protocol	Length	Info
12	20.095281	192.168.0.130	192.168.0.1	DNS	69	Standard query 0xfe93 A ns2.pu.ru
13	20.145396	192.168.0.1	192.168.0.130	DNS	155	Standard query response 0xfe93 A ns2.pu.ru A 195.70.196.210 NS ns2.pu.ru NS ns.pu.ru NS ns7.spbu.ru A ...
14	20.151534	192.168.0.130	195.70.196.210	DNS	71	Standard query 0xd814 A www.spbu.ru
15	20.193341	195.70.196.210	192.168.0.130	DNS	101	Standard query response 0xd814 A www.spbu.ru CNAME spbu.ru A 85.193.83.151

195.70.196.210

тес

ns2.pu.ru

о

- Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержится ли в запросе какие-нибудь «ответы»?

о

> Ethernet II, Src: Apple_a1:70:4a (00:78:17:a1:70:4a), Dst: TendaTechnol_be:85:f0 (e8:65:d4:be:85:f0)
> Internet Protocol Version 4, Src: 192.168.0.130, Dst: 195.70.196.210
> User Datagram Protocol, Src Port: 58386, Dst Port: 53
` Domain Name System (query)
Transaction ID: 0xd814
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
` Queries
` www.spbu.ru: type A, class IN
Name: www.spbu.ru
[Name Length: 11]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)
[Response In: 15]

• type A

• тес

о

- Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

о

о

• 2, CNAME запись и IP-адрес

```

Class: IN (0x0001)
  ▼ Answers
    ▼ www.spbu.ru: type CNAME, class IN, cname spbu.ru
      Name: www.spbu.ru
      Type: CNAME (5) (Canonical NAME for an alias)
      Class: IN (0x0001)
      Time to live: 360 (6 minutes)
      Data length: 2
      CNAME: spbu.ru
    ▼ spbu.ru: type A, class IN, addr 85.193.83.151
      Name: spbu.ru
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 10 (10 seconds)
      Data length: 4
      Address: 85.193.83.151
    [Request In: 14]
    [Time: 0.041807000 seconds]
  ●  User Datagram Protocol (udp), 8 bytes

```

E)

- Что такое база данных whois?

◦

• База данных с информацией о доменах и IP-адресах (DNS-адреса, на кого зарегистрирован домен, адреса гана реигстрации и тд)

◦

- Используя различные сервисы whois в Интернете, получите имена любых двух DNS-серверов. Какие сервисы вы при этом использовали?

◦

• Whois.domain-tools

DomainTools PROFILE CONNECT MONITOR SUPPORT

Updated on 2024-05-29

Name Servers NS1.VK.COM (has 12 domains)  
NS2.VK.COM (has 12 domains)  
NS3.VK.COM (has 12 domains)  
NS4.VK.COM (has 12 domains)

IP Address 87.240.129.133 - 15 other sites hosted on this server

IP Location 🇷🇺 - Sankt-peterburg - Sankt-peterburg - Vkontakte Services

ASN AS47541 VKONTAKTE-SPB-AS VKontakte Ltd, RU (registered)

IP History 133 changes on 133 unique IP addresses over 21 years

Hosting History 2 changes on 3 unique name servers over 16 years

Whois Record (last updated on 2023-03-11)

Domain Name: VK.COM  
Registry Domain ID: 2286186\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.nic.ru  
Registrar URL: https://nic.ru  
Updated Date: 2024-05-29T08:40:12Z  
Creation Date: 1997-06-24T04:00:00Z  
Registrar: Regional Networks Information Center, JSC dba RU-C  
Registrar IANA ID: 48  
Registrar Abuse Contact Email: n Abuse@nic.ru  
Registrar Abuse Contact Phone: +74958091333  
Domain Status: clientTransferProhibited https://icann.org/ep  
Name Servers: NS1.VK.COM  
Name Servers: NS2.VK.COM  
Name Servers: NS3.VK.COM  
Name Servers: NS4.VK.COM  
DNSSEC Configuration: None  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www

## Whois Record for Muji.com

### Domain Profile

Registrar 1API GmbH  
IANA ID: 1387  
URL: http://www.1api.net  
Whois Server: whois.1api.net  
abuse@1api.net  
(p) +49.6894939650

Registrar Status clientTransferProhibited

Dates 10,133 days old  
Created on 1997-06-13  
Expires on 2025-06-12  
Updated on 2024-09-20

Name Servers NS-1405.AWSDNS-47.ORG (has 53,256 domains)  
NS-1591.AWSDNS-06.CO.UK (has 309 domains)  
NS-395.AWSDNS-49.COM (has 2,666 domains)  
NS-709.AWSDNS-24.NET (has 21 domains)

IP Address 23.38.191.154 - 331 other sites hosted on this server

IP Location 🇺🇸 - Washington - Seattle - Akamai Technologies Inc.

ASN AS20940 AKAMAI-ASN1 Akamai International B.V., NL (registered Jul 10, 2001)

Domain Status Registered And No Website

IP History 712 changes on 712 unique IP addresses over 19 years

Hosting History 7 changes on 6 unique name servers over 22 years

Whois Record (last updated on 2025-03-11)

Domain Name: MUJI.COM  
Registry Domain ID: 296039\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.1api.net

DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup

strar Status 15 6,588 days old  
Created on 2007-02-28  
Expires on 2026-02-28  
Updated on 2021-06-12

ie Servers DNS-AS-SAMSUNG.COM (has 1,449 domains)  
DNS-AS-SAMSUNG.COM (has 1,449 domains)  
DNS-AS-SAMSUNG.COM (has 1,449 domains)  
DNS-AS-SAMSUNG.COM (has 1,449 domains)  
DNS-AS-SAMSUNG.COM (has 1,449 domains)

ddress 112.20.6.21.70 - 6 other sites hosted on this server

ocation 🇰🇷 - Seoul Teukbyeoil - Seoul - Samsungs Inc.

is Record (last updated on 2025-03-13)

try : samsung.kr  
OREAN(UTF8)

인 이름 : samsung.kr  
인 주소 : 삼성전자주식회사  
인 수반번호 : 118-81-20000  
자 전자우편 : seoul@samsung.com  
자 전화번호 : +82-777-7770  
설명 번역 : 2007. 02. 28.  
설명 번역 : 2026. 02. 28.  
설명 번역 : Y  
설명 번역 : (주)삼성전자주식회사  
설명 번역 : clientTransferProhibited  
설명 번역 : clientUpdateProhibited

네임서버 정보 : dnssm.samsung.com

3. Используйте команду nslookup на локальном хосте, чтобы послать запросы трем конкретным серверам DNS (по аналогии с Заданием Д): вашему локальному серверу DNS и двум DNS-серверам, найденным в предыдущей части.

o

```
[ ~ ~ nslookup muji.com
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
Name: muji.com
Address: 3.5.158.14
Name: muji.com
Address: 52.219.162.195
Name: muji.com
Address: 3.5.158.234
Name: muji.com
Address: 52.219.150.203
Name: muji.com
Address: 3.5.158.66
Name: muji.com
Address: 3.5.156.83
Name: muji.com
Address: 3.5.158.136
Name: muji.com
Address: 52.219.162.115

[ ~ ~ nslookup muji.com NS-1405.AWSDNS-47.ORG
Server:      NS-1405.AWSDNS-47.ORG
Address:     205.251.197.125#53

Name: muji.com
Address: 3.5.156.253
Name: muji.com
Address: 52.219.150.171
Name: muji.com
Address: 3.5.156.117
Name: muji.com
Address: 52.219.1.60
Name: muji.com
Address: 52.219.150.155
Name: muji.com
Address: 3.5.154.71
Name: muji.com
Address: 52.219.150.59
Name: muji.com
Address: 3.5.158.136

[ ~ ~ nslookup muji.com NS-1591.AWSDNS-06.CO.UK
Server:      NS-1591.AWSDNS-06.CO.UK
Address:     205.251.198.55#53

Name: muji.com
Address: 52.219.150.143
Name: muji.com
Address: 52.219.199.23
Name: muji.com
Address: 52.219.8.24
Name: muji.com
Address: 52.219.150.155
Name: muji.com
Address: 52.219.136.32
Name: muji.com
Address: 3.5.156.228
Name: muji.com
Address: 52.219.198.27
```