

## Задание 2.А

1)

```
jaroslav@F1:~/Documents$ nslookup baidu.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   baidu.com
Address: 110.242.68.66
Name:   baidu.com
Address: 39.156.66.10
```

2)

```
[5] - stopped nslookup
jaroslav@F1:~/Documents$ nslookup
> set query=ns
> ens.psl.eu
Server:          8.8.8.8
Address:         8.8.8.8#53

Non-authoritative answer:
ens.psl.eu      nameserver = panoramix.rap.prd.fr.
ens.psl.eu      nameserver = ns.ens.fr.

Authoritative answers can be found from:
```

nameserver – ns.ens.fr, panoramix.rap.prd.fr

3)

```
[5] - stopped nslookup
jaroslav@F1:~/Documents$ nslookup baidu.com
Server:          8.8.8.8
Address:         8.8.8.8#53

Non-authoritative answer:
Name:   baidu.com
Address: 39.156.66.10
Name:   baidu.com
Address: 110.242.68.66
```

```

Address: 2a00:1450:400f:80b::200e

jaroslav@F1:~/Documents$ nslookup spbu.ru
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   spbu.ru
Address: 81.89.183.222

```

1 IP адрес

2.Б

DNS-запрос был выполнен с использованием транспортного протокола UDP:

```

> Frame 23: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface wlx7062b8b3c121, id 0
> Ethernet II, Src: D-LinkIn_b3:c1:21 (70:62:b8:b3:c1:21), Dst: D-LinkIn_69:a6:18 (c4:12:f5:69:a6:18)
> Internet Protocol Version 4, Src: 192.168.0.141, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 36839, Dst Port: 53
< Domain Name System (query)
  Transaction ID: 0x7cbb
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    [Response In: 27]

```

0000	c4 12 f5 69 a6 18 70 62 b8 b3 c1 21 08 00 45 00	...i..pb ...!..E.
0010	00 3a 42 14 00 00 40 11 b6 c0 c0 a8 00 8d c0 a8	.:B...@. ....
0020	00 01 8f e7 00 35 00 26 4e a6 7c bb 01 00 00 01	.....5.& N. ....
0030	00 00 00 00 00 00 03 77 77 77 04 69 65 74 66 03	.....w ww.ietf.
0040	6f 72 67 00 00 01 00 01	org.....

Порт назначения (dst port) – 53.

IP-адреса совпадают:

```

jaroslav@F1:~/Documents$ resolvectl
Global
  Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: foreign

Link 2 (enp1s0)
  Current Scopes: none
  Protocols: -DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

Link 3 (wlx7062b8b3c121)
  Current Scopes: DNS
  Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  Current DNS Server: 192.168.0.1
  DNS Servers: 192.168.0.1

```

Запрос на А-запись класса IN (Internet):

```
Flags: 0x0100 Standard query
 0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
... ..0. .... = Truncated: Message is not truncated
... ..1 .... = Recursion desired: Do query recursively
... ..0... .. = Z: reserved (0)
... ..0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  www.ietf.org: type A, class IN
[Response In: 27]
```

Answer Rrs –0 (т.к. это запрос)

Ответ содержит 3 “ответа”. Первый из них – CNAME, следующие 2 – А-записи для домена из первой CNAME-записи.

```
... ..0 .... = Non-authenticated data: Unacceptable
... ..0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
  www.ietf.org: type A, class IN
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: 23]
[Time: 0.105498617 seconds]
```

Да, IP-адрес DNS ответа (второго) совпадает и адресом последующего TCP-пакета:

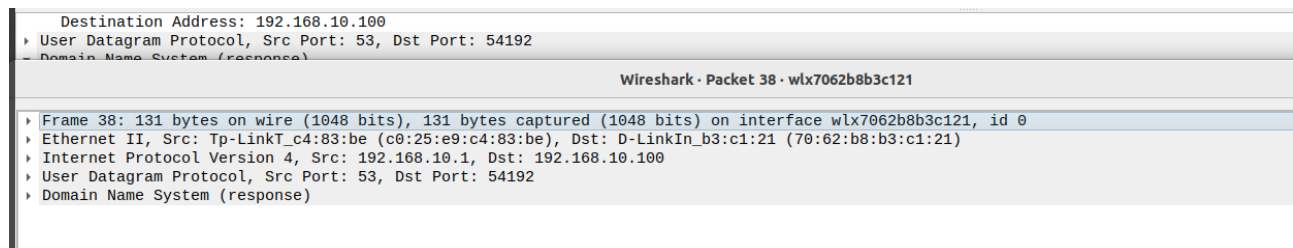
```
0100 .... = Version: 4
... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x4940 (18752)
  Flags: 0x40, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0x9bd3 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.0.141
  Destination Address: 104.16.44.99
  Transmission Control Protocol, Src Port: 60352, Dst Port: 80, Seq: 0, Len: 0
```

```
... ..0 .... = Non-authenticated data: Unacceptable
... ..0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
  www.ietf.org: type A, class IN
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: 23]
[Time: 0.105498617 seconds]
```

(104.16.44.99)

Для картинок, насколько я вижу, отдельных DNS-запросов не отправляются, потому что ссылки на них относятся к этому же домену. Дополнительный запрос отправляется на analytics.ietf.org, видимо, в HTML загружается соответствующий скрипт с аналитикой.

## 2.В



И порт назначения запроса, и порт отправления ответа одинаковые – UDP/53.

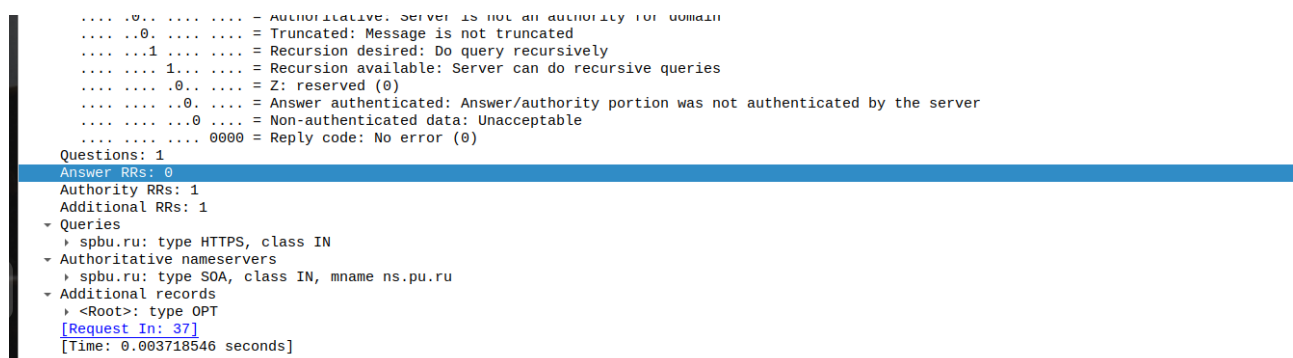
IP-адрес – мой локальный, запрос идет через мой локальный DNS-резолвер.

37	0.100148566	192.168.10.100	192.168.10.1	DNS	78 Standard query 0xcda8 HTTPS spbu.ru OPT
38	0.103867112	192.168.10.1	192.168.10.100	DNS	131 Standard query response 0xcda8 HTTPS spbu.ru SOA ns.pu.ru OPT

Запрос на запись класса HTTPS типа IN:

37	0.100148566	192.168.10.100	192.168.10.1	DNS	78 Standard query 0xcda8 HTTPS spbu.ru OPT
38	0.103867112	192.168.10.1	192.168.10.100	DNS	131 Standard query response 0xcda8 HTTPS spbu.ru SOA ns.pu.ru OPT

Ответов в запросе нет (Answers PR), потому что это DNS-запрос



В ответе мы видим start-of-authority запись (nameserver) и дополнительные (OPT, options) данные

## 2.Г

```

... ..0.. ..0.. ..0.. = Authoritative: Server is not an authority for domain
... ..0.. ..0.. ..0.. = Truncated: Message is not truncated
... ..1.. ..0.. ..0.. = Recursion desired: Do query recursively
... ..1.. ..0.. ..0.. = Recursion available: Server can do recursive queries
... ..0.. ..0.. ..0.. = Z: reserved (0)
... ..0.. ..0.. ..0.. = Answer authenticated: Answer/authority portion was not authenticated by the server
... ..0.. ..0.. ..0.. = Non-authenticated data: Unacceptable
... ..0.. ..0.. ..0.. = Reply code: No error (0)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 1
- Queries
  > spbu.ru: type HTTPS, class IN
- Authoritative nameservers
  > spbu.ru: type SOA, class IN, mname ns.pu.ru
- Additional records
  > <Root>: type OPT
[Request In: 37]
[Time: 0.003718546 seconds]

```

DNS-запрос отправлен за 8.8.4.4, потому что он указал приоритетным в “/etc/resolv.conf”

Тип запроса: NS:

```

transaction ID: 0x33a8
- Flags: 0x0100 Standard query
  0... ..0.. ..0.. ..0.. = Response: Message is a query
  .000 0... ..0.. ..0.. = Opcode: Standard query (0)
  .... ..0.. ..0.. ..0.. = Truncated: Message is not truncated
  .... ..1.. ..0.. ..0.. = Recursion desired: Do query recursively
  .... ..0.. ..0.. ..0.. = Z: reserved (0)
  .... ..0.. ..0.. ..0.. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
- Queries
  > spbu.ru: type NS, class IN
[Response In: 5]

```

ответов в запросе нет.

```

- spbu.ru: type NS, class IN
- 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: 3434 (57 minutes, 14 seconds)
    Data length: 9
    Name Server: ns2.pu.ru
  > 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: 3434 (57 minutes, 14 seconds)
    Data length: 5
    Name Server: ns.pu.ru
[Request In: 3]
[Time: 0.007139915 seconds]

```

Два доменных имени: ns.pu.ru, ns2.pu.ru. Их адресов в ответе ожидаемо нет.

2.Д

IP	Port	Protocol	Length	Info
192.168.10.100	53	DNS	71	Standard query 0x7604 A www.spbu.ru
195.70.196.210	53	DNS	171	Standard query response 0x7604 A www.spbu.ru CNAME spbu.ru A 81.89.183.222 NS ns.pu.ru NS ns2.pu.ru A 195.70.196.219 A 195...

Запрос выполнен по IP-адресу того nameserver-а, который мы указали (ns2.pu.ru). Адрес этого nameserver тоже получен через DNS-запрос.

Запрос А-записи, ответов в нем нет:

```

- Domain Name System (query)
  Transaction ID: 0x7804
  Flags: 0x0100 Standard query
    0... .. = Response: Message is a query
    .000 0... .. = Opcode: Standard query (0)
    ....0... .. = Truncated: Message is not truncated
    ....1... .. = Recursion desired: Do query recursively
    ....0... .. = Z: reserved (0)
    ....0... .. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
- Queries
  > www.spbu.ru: type A, class IN
  [Response In: 10]

```

Ответ содержит CNAME и A запись для [www.spbu.ru](http://www.spbu.ru):

```

.... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
.... ..0... .. = Non-authenticated data: Unacceptable
.... ..0000 .. = Reply code: No error (0)
Questions: 1
Answer RRs: 2
Authority RRs: 2
Additional RRs: 2
- Queries
  > www.spbu.ru: type A, class IN
- Answers
  > www.spbu.ru: type CNAME, class IN, cname spbu.ru
  > spbu.ru: type A, class IN, addr 81.89.183.222
- Authoritative nameservers
- Additional records
  [Request In: 9]
  [Time: 0.003366922 seconds]

```

## 2.E

Whois – это база данных для хранения и распространения данных о доменных именах, их владельцах, занятости домена и прочей подобной информации

Используем сервис <https://who.is>

google.com  
whois information

Whois
DNS Records
Diagnostics

cache expires in 13 hours, 13 minutes and 29 seconds  
refresh

Registrar Info	
Name	MarkMonitor, Inc.
Whois Server	whois.markmonitor.com
Referral URL	http://www.markmonitor.com
Status	clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited) clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited) clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited) serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited) serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited) serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Important Dates	
Expires On	2028-09-13
Registered On	1997-09-15
Updated On	2019-09-09
Name Servers	

Use promo code WHOIS to save 15% on your first Name.com order.  
Find the perfect domain at  
**Name.com**

Everything  
you need in  
one place.

SAVE 15% ON  
YOUR FIRST ORDER

USE PROMO CODE WHOIS



cached

# mipt.ru

whois information

Whois DNS Records Diagnostics

cache expires in 23 hours, 59 minutes and 52 seconds

## Registrar Info

Name RU-CENTER-RU

Status

## Similar Domains

mipt.ca | mipt.cc | mipt.cl | mipt.club | mipt.cn | mipt.co | mipt.com | mipt.edu | mipt.events | mipt.fail | mipt.info | mipt.msk.ru | mipt.net | mipt.org | mipt.pl | mipt.pro | mipt.ru | mipt.site | mipt.su | mipt.tech |

## Registrar Data

We will display stored WHOIS data for up to 30 days.

[Make Private Now](#)

% TCI Whois Service. Terms of use:  
% https://tcinet.ru/documents/whois\_ru\_rf.pdf (in Russian)  
% https://tcinet.ru/documents/whois\_su.pdf (in Russian)

domain: MIPT.RU  
nserver: gw.mipt.ru. 192.188.189.3

Use promo code WHOIS to save 15% on your first Name.com order.

Find the perfect domain at **Name.com**

**Everything you need in one place.**

**SAVE 15% ON YOUR FIRST ORDER**

[USE PROMO CODE WHOIS](#)

Отправим запросы 3 серверам:

```
jaroslav@F1:~/Documents$ nslookup google.com 127.0.0.53
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 64.233.164.100
Name:   google.com
Address: 64.233.164.101
Name:   google.com
Address: 64.233.164.113
Name:   google.com
Address: 64.233.164.138
Name:   google.com
Address: 64.233.164.102
Name:   google.com
Address: 64.233.164.139
Name:   google.com
Address: 2a00:1450:4010:c07::64
Name:   google.com
Address: 2a00:1450:4010:c07::8a
Name:   google.com
Address: 2a00:1450:4010:c07::66
Name:   google.com
Address: 2a00:1450:4010:c07::71

jaroslav@F1:~/Documents$ nslookup google.com ns2.pu.ru
Server:      ns2.pu.ru
Address:     195.70.196.210#53

** server can't find google.com: REFUSED

jaroslav@F1:~/Documents$ nslookup google.com ns.pu.ru
Server:      ns.pu.ru
Address:     195.70.196.219#53

** server can't find google.com: REFUSED

jaroslav@F1:~/Documents$
```

ns2.pu.ru и ns.pu.ru не ответили – они не обслуживают домен google.com

