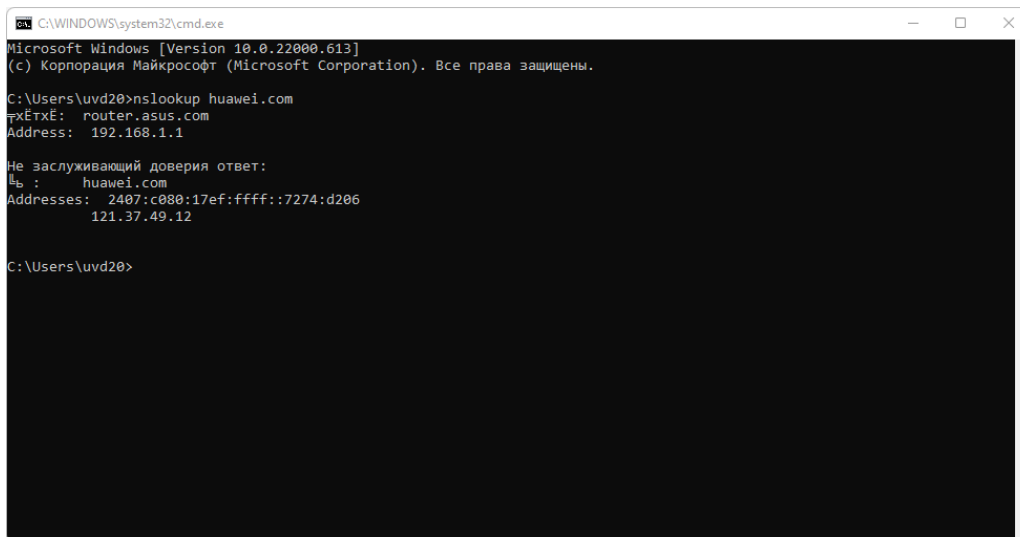


Домашняя работа 4

Задание 1:

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



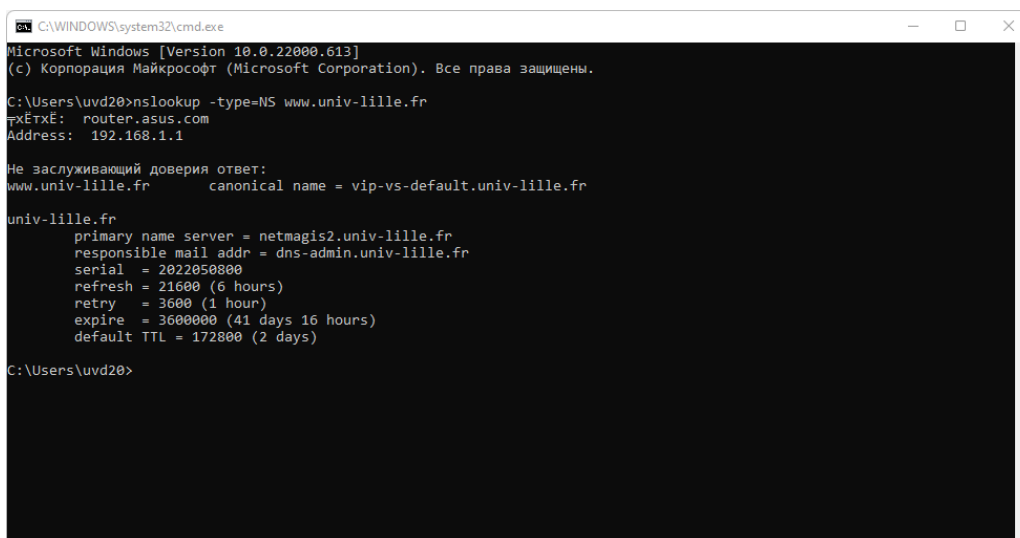
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.613]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\uvd20>nslookup huawei.com
Server: router.asus.com
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Вопрос : huawei.com
Addresses: 2407:c080:17ef:ffff::7274:d206
          121.37.49.12

C:\Users\uvd20>
```

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



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.613]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\uvd20>nslookup -type=NS www.univ-lille.fr
Server: router.asus.com
Address: 192.168.1.1

Не заслуживающий доверия ответ:
www.univ-lille.fr canonical name = vip-vs-default.univ-lille.fr

univ-lille.fr
primary name server = netmagis2.univ-lille.fr
responsible mail addr = dns-admin.univ-lille.fr
serial = 2022050800
refresh = 21600 (6 hours)
retry = 3600 (1 hour)
expire = 3600000 (41 days 16 hours)
default TTL = 172800 (2 days)

C:\Users\uvd20>
```

3. Используя nslookup, найдите веб-сервер, имеющий несколько IP-адресов.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.613]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\uvd20>nslookup yandex.ru
Server: router.asus.com
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Name: yandex.ru
Addresses: 2a02:6b8:a::a
          77.88.55.88
          5.255.255.70
          77.88.55.60
          5.255.255.77

C:\Users\uvd20>
```

Сколько IP-адресов имеет веб-сервер вашего учебного заведения?

Веб-сервер моего учебного заведения имеет один IP-адрес.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.613]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\uvd20>nslookup spbu.ru
Server: router.asus.com
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Name: spbu.ru
Address: 195.70.219.101

C:\Users\uvd20>
```

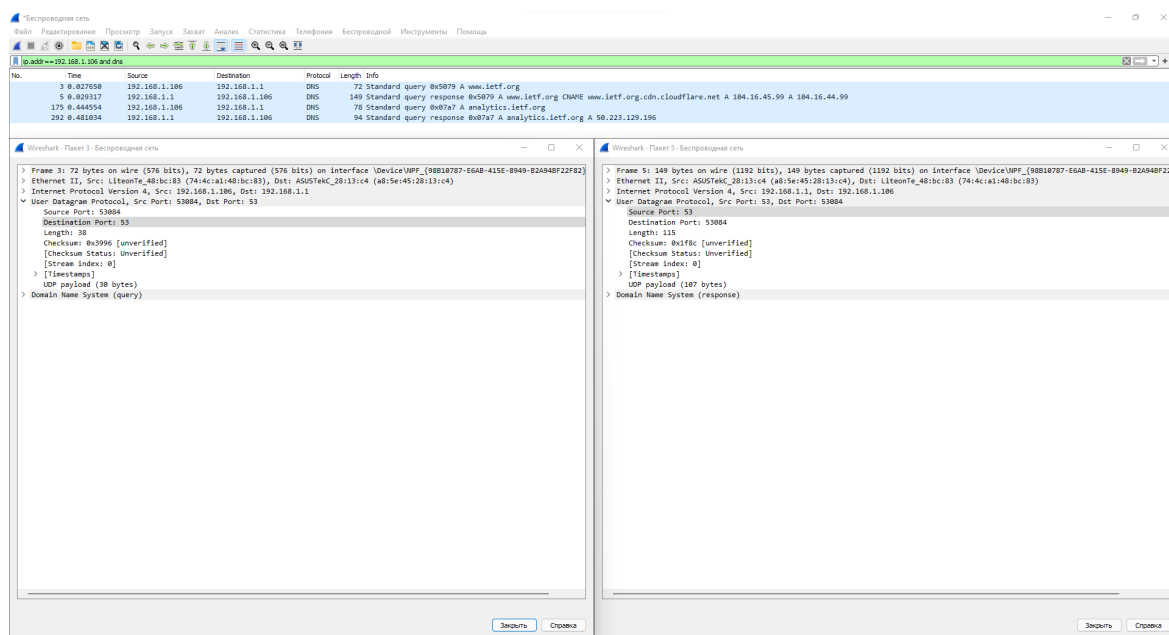
Задание 2:

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

Они отправлены с использованием транспортного протокола **UDP**.

2. Какой порт назначения у запроса DNS?

Порт 53.



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

DNS-запрос отправлен на IP-адрес 192.168.1.1.

Этот адрес совпадает с IP-адресом моего локального DNS-сервера.

```
C:\WINDOWS\system32\cmd.exe

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Физический адрес. . . . . : 76-4C-A1-48-BC-B3
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Беспроводная сеть:

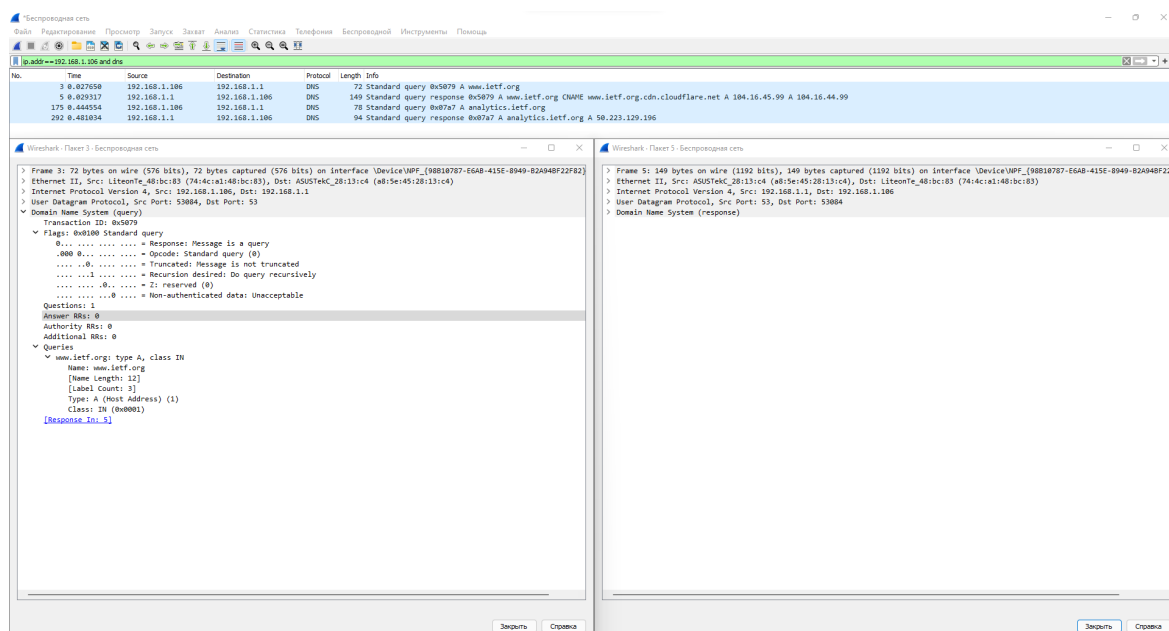
DNS-суффикс подключения . . . . . :
Описание. . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
Физический адрес. . . . . : 74-4C-A1-48-BC-83
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . . . : fe80::29f9:3d9a:bebb:3c64%13(Основной)
IPv4-адрес. . . . . : 192.168.1.106(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 8 мая 2022 г. 15:08:04
Срок аренды истекает. . . . . : 9 мая 2022 г. 15:08:04
Основной шлюз. . . . . : 192.168.1.1
DHCP-сервер. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 108285089
DUID клиента DHCPv6 . . . . . : 00-01-00-01-28-66-12-20-08-8F-C3-04-7A-B1
DNS-серверы. . . . . : 192.168.1.1
NetBios через TCP/IP. . . . . : Включен

Адаптер Ethernet Сетевое подключение Bluetooth:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
```

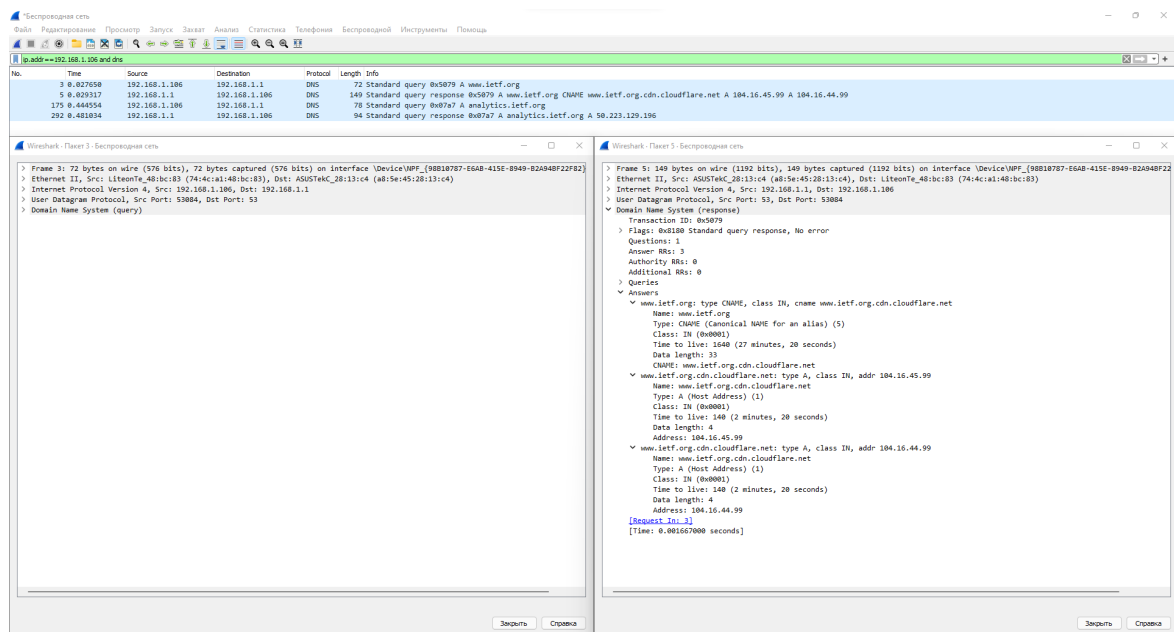
4. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

Запрашивается запись типа A (IPv4 Address). В запросе присутствует поле «Answer RRs». 0 в этом поле означает, что ответов нет.



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

В ответном сообщении DNS есть три ответа. Первый ответ имеет тип CNAME, он связывает имя, которое мы запросили, с другим. Два остальных ответа имеют тип A, они содержат два адреса хоста с именем www.ietf.org.cdn.cloudflare.net.



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?

Да, соответствует.

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Фильтр: [ip.addr==192.168.1.106 and (http or tcp.flags.syn==1)]

No.	Time	Source	Destination	Protocol	Length	Info
3	0.827558	192.168.1.106	192.168.1.1	DNS	72	Standard query 0x5879 A www.ietf.org
5	0.829517	192.168.1.1	192.168.1.106	DNS	149	Standard query response 0x5879 A www.ietf.org CNAME www.ietf.org.cdn.cloudflare.net A 104.16.45.99 A 104.16.44.99
6	0.831196	192.168.1.106	104.16.45.99	TCP	66	6340 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
11	0.852921	104.16.45.99	192.168.1.106	TCP	66	80 → 6240 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 US=1024
175	0.444554	192.168.1.106	192.168.1.1	DNS	78	Standard query 0x07a7 A analytics.ietf.org
292	0.481034	192.168.1.1	192.168.1.106	DNS	84	Standard query response 0x07a7 A analytics.ietf.org A 50.223.129.196
334	0.481786	192.168.1.106	50.223.129.196	TCP	66	6241 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
669	0.687623	50.223.129.196	192.168.1.106	TCP	66	443 → 6241 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 US=128

> Frame 6: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{08B10787-65A8-415E-8949-82A040F22F62}, id 0
> Ethernet II, Src: LiteonTe_481bc183 (74:4c:a1:48:1b:c183), Dst: ASUSTek_28113:c4 (a8:5e:45:28:11:3c4)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 104.16.45.99
 > 6108 ... = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 52
 Identification: 0x0558 (34384)
 > Flags: 0x00, Don't Fragment
 ... 0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 128
 Protocol: TCP (6)
 Header Checksum: 0x1cee [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.1.106
 Destination Address: 104.16.45.99
 > Transmission Control Protocol, Src Port: 6240, Dst Port: 80, Seq: 0, Len: 0

Destination Address [ip.dst], 4 bytes

Пакеты: 775 - Показаны: 8 (1.0%) - Потеряно: 0 (0.0%)

Профили: Default

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

Задание 3:

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

Порт назначения в запросе DNS – 53. Порт источника в DNS-ответе такой же.

Беспроводная сеть

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Фильтр: [ip.addr==192.168.1.106 and dns]

No.	Time	Source	Destination	Protocol	Length	Info
30	5.799286	192.168.1.106	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.1.168.192.in-addr.arpa
32	5.817787	192.168.1.1	192.168.1.106	DNS	113	Standard query response 0x0001 PTR 1.1.1.168.192.in-addr.arpa PTR router.asus.com
33	5.820054	192.168.1.106	192.168.1.1	DNS	71	Standard query 0x0002 A www.spbu.ru
34	5.822779	192.168.1.1	192.168.1.106	DNS	171	Standard query response 0x0002 A www.spbu.ru CNAME spbu.ru A 195.70.219.101 NS ns2.spb.ru NS ns.spb.ru A 195.70.196.219 A 195.70.196.218
35	5.823083	192.168.1.106	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.spbu.ru
36	5.824083	192.168.1.1	192.168.1.106	DNS	138	Standard query response 0x0003 AAAA www.spbu.ru CNAME spbu.ru SOA ns.spb.ru

Wireshark - Пакет 35: Беспроводная сеть

> Frame 35: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{08B10787-65A8-415E-8949-82A040F22F62}
> Ethernet II, Src: LiteonTe_481bc183 (74:4c:a1:48:1b:c183), Dst: ASUSTek_28113:c4 (a8:5e:45:28:11:3c4)
> Internet Protocol Version 4, Src: 192.168.1.106, Dst: 192.168.1.1
 > User Datagram Protocol, Src Port: 49675, Dst Port: 53
 Source Port: 49675
 Destination Port: 53
 Length: 37
 Checksum: 0xc467 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 3]
 > [Timestamps]
 > UDP payload (29 bytes)
 > Domain Name System (query)

Wireshark - Пакет 36: Беспроводная сеть

> Frame 36: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface \Device\NPF_{08B10787-65A8-415E-8949-82A040F22F62}
> Ethernet II, Src: ASUSTek_28113:c4 (a8:5e:45:28:11:3c4), Dst: LiteonTe_481bc183 (74:4c:a1:48:1b:c183)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.106
 > User Datagram Protocol, Src Port: 53, Dst Port: 49675
 Source Port: 53
 Destination Port: 49675
 Length: 104
 Checksum: 0xb798 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 3]
 > [Timestamps]
 > UDP payload (96 bytes)
 > Domain Name System (response)

Закрыть Справка

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

DNS-запрос отправлен на IP-адрес 192.168.1.1.

Этот адрес совпадает с адресом локального DNS-сервера, установленного по умолчанию.

```
C:\WINDOWS\system32\cmd.exe

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Физический адрес. . . . . : 76-4C-A1-48-BC-B3
DHCP включен. . . . . : Нет
Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Беспроводная сеть:

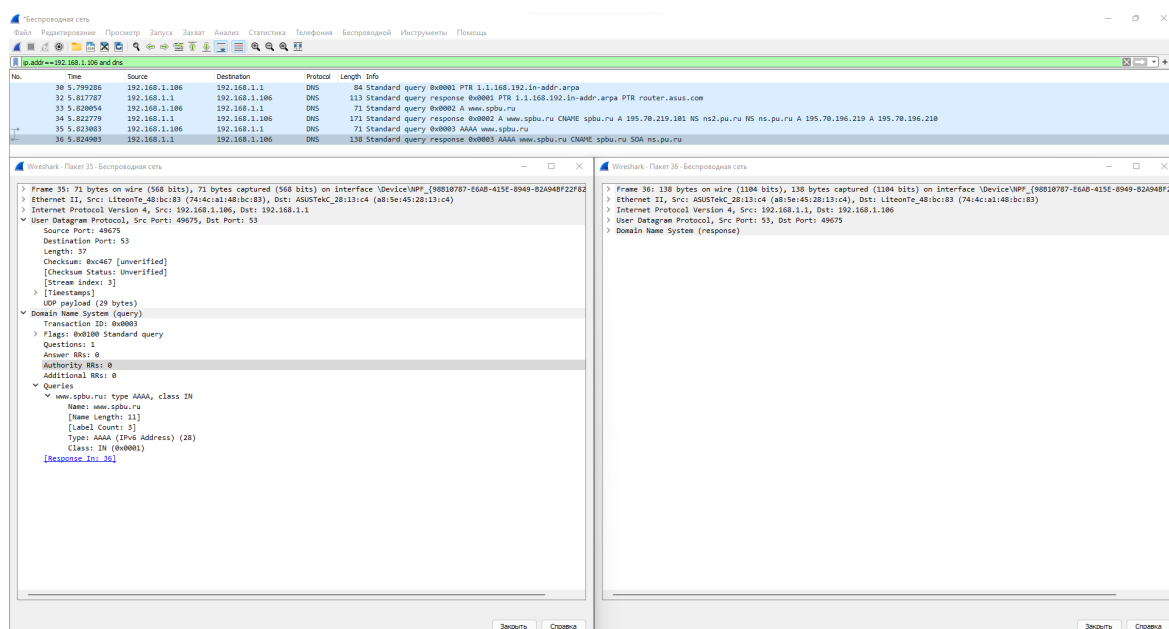
DNS-суффикс подключения . . . . . :
Описание. . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
Физический адрес. . . . . : 74-4C-A1-48-BC-83
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . . : fe80::29f9:3d9a:babb:3c64%13(Основной)
IPv4-адрес. . . . . : 192.168.1.106(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 8 мая 2022 г. 15:08:04
Срок аренды истекает. . . . . : 9 мая 2022 г. 15:08:04
Основной шлюз. . . . . : 192.168.1.1
DNS-сервер. . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 108285089
DUID клиента DHCPv6 . . . . . : 00-01-00-01-28-66-12-20-08-8F-C3-04-7A-B1
DNS-серверы. . . . . : 192.168.1.1
NetBios через TCP/IP. . . . . : Включен

Адаптер Ethernet Сетевое подключение Bluetooth:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
```

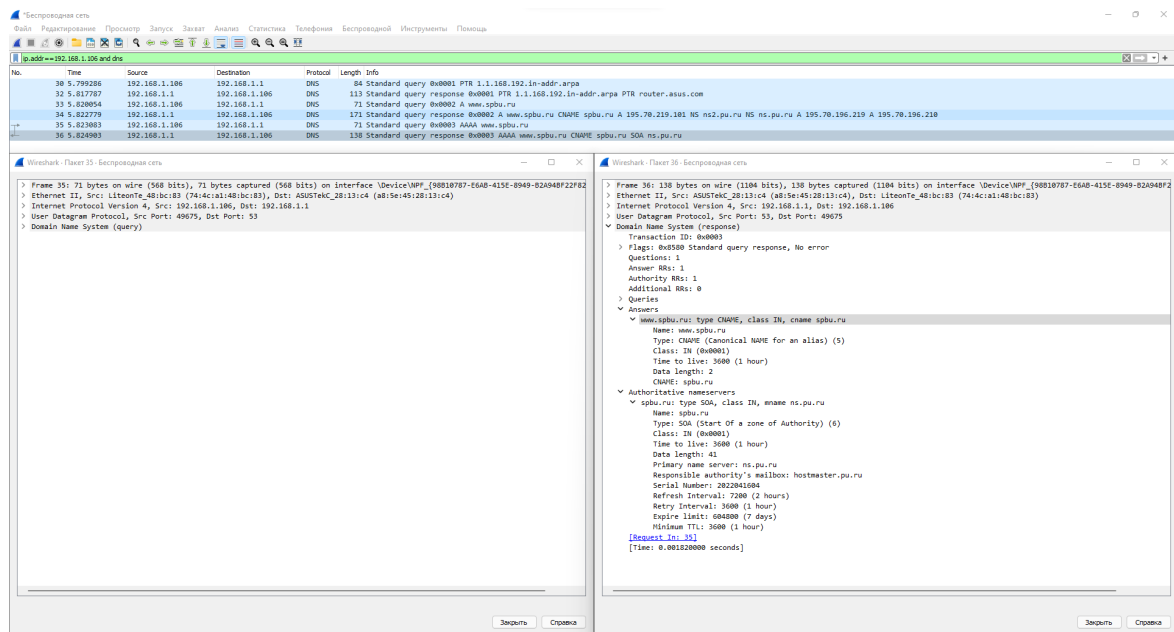
3. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

Запрашивается запись типа AAAA (IPv6 Address). В запросе присутствует поле «Answer RRs». 0 в этом поле означает, что ответов нет.



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

В ответном сообщении DNS есть один ответ. Он имеет тип CNAME и связывает имя, которое мы запросили, с другим (spbu.ru).

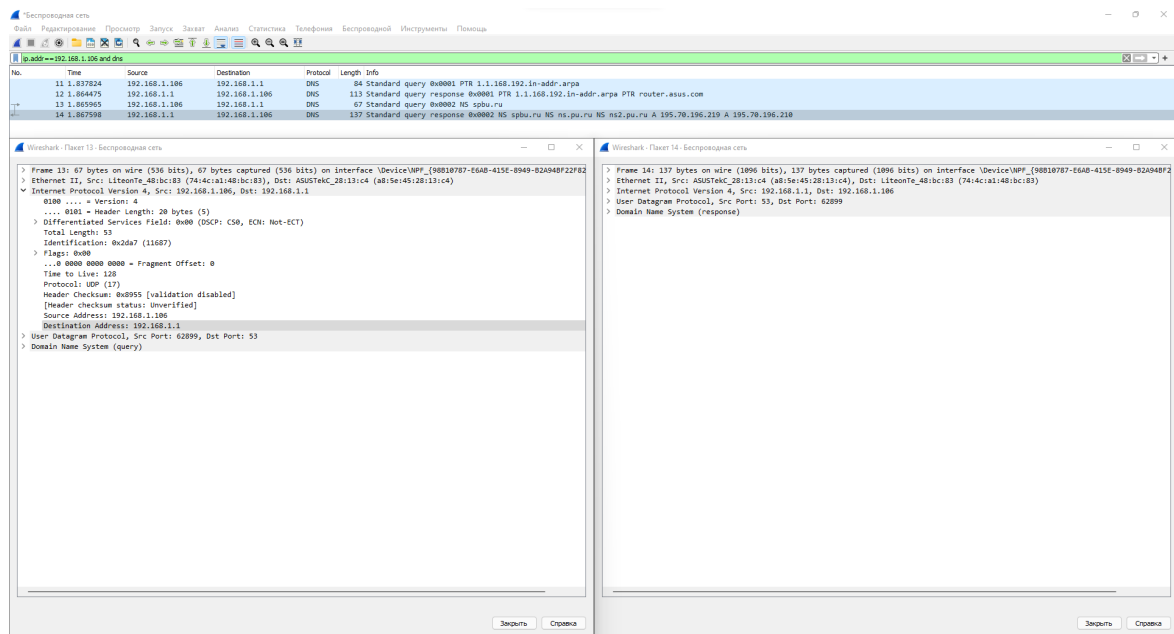


Задание 4:

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

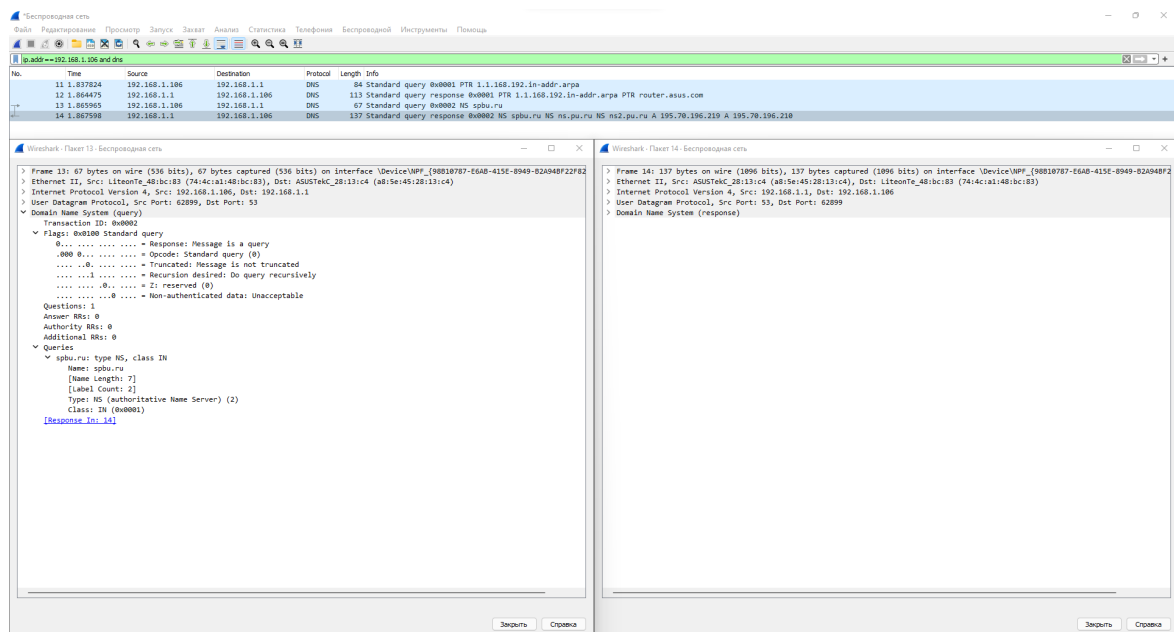
DNS-запрос отправлен на IP-адрес 192.168.1.1.

Да, все еще совпадает.



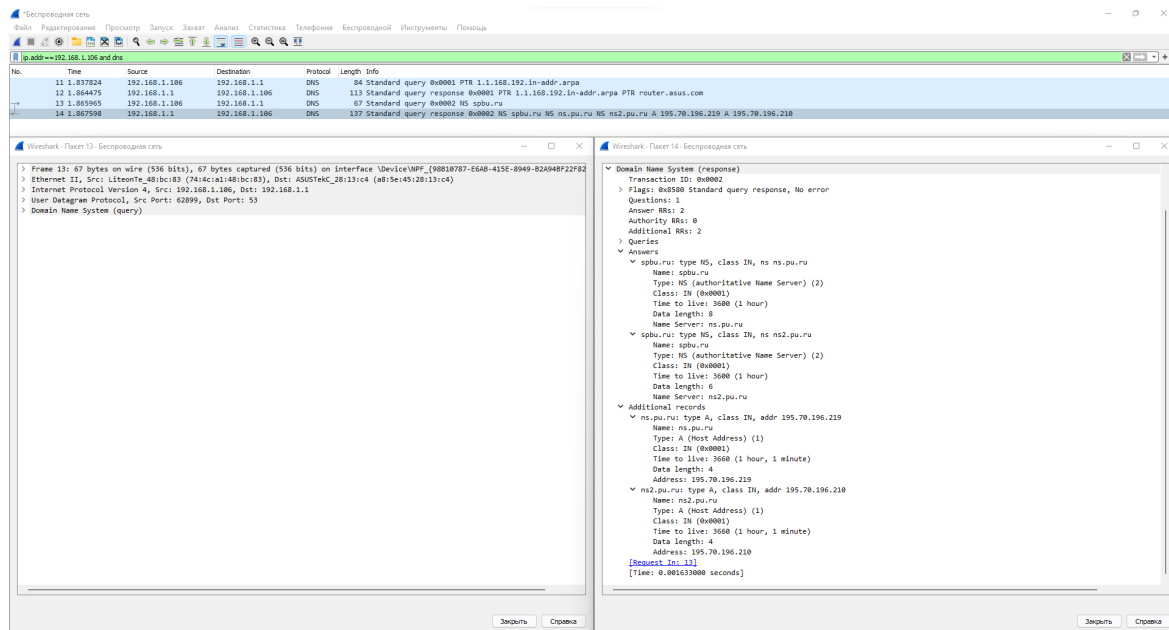
2. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

Запрашивается запись типа NS (authoritative Name Server). В запросе присутствует поле «Answer RRs». 0 в этом поле означает, что ответов нет.



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

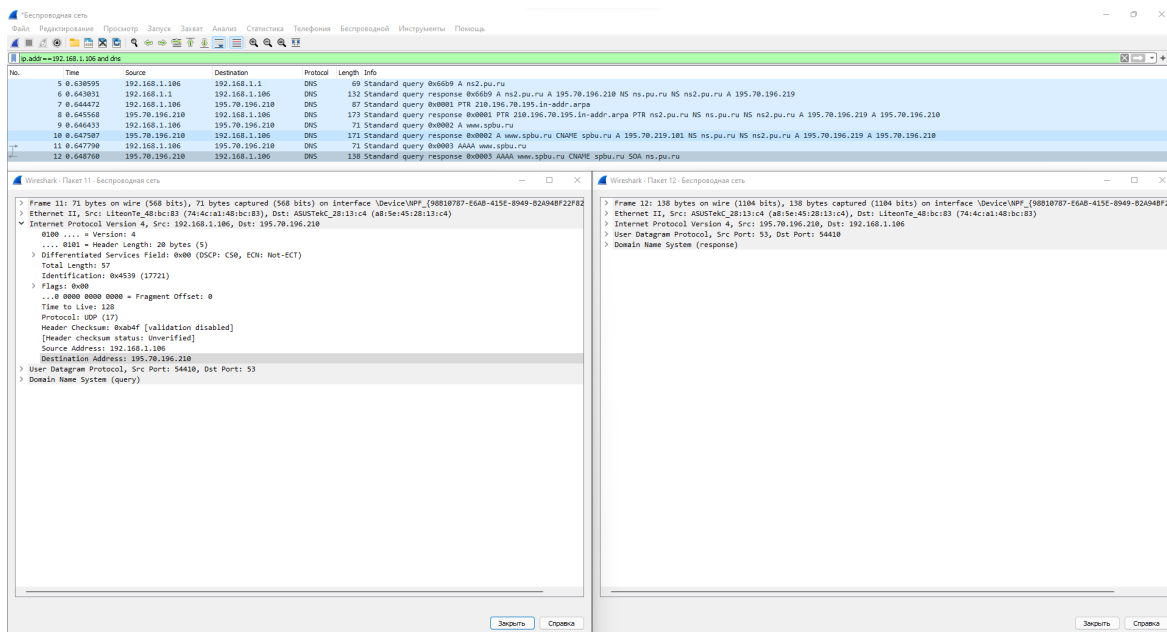
В ответном сообщении содержатся имена DNS-серверов университета ns.pu.ru и ns2.pu.ru. Их адреса содержатся в поле Additional records: 195.70.196.219 и 195.70.196.210.



Задание 5:

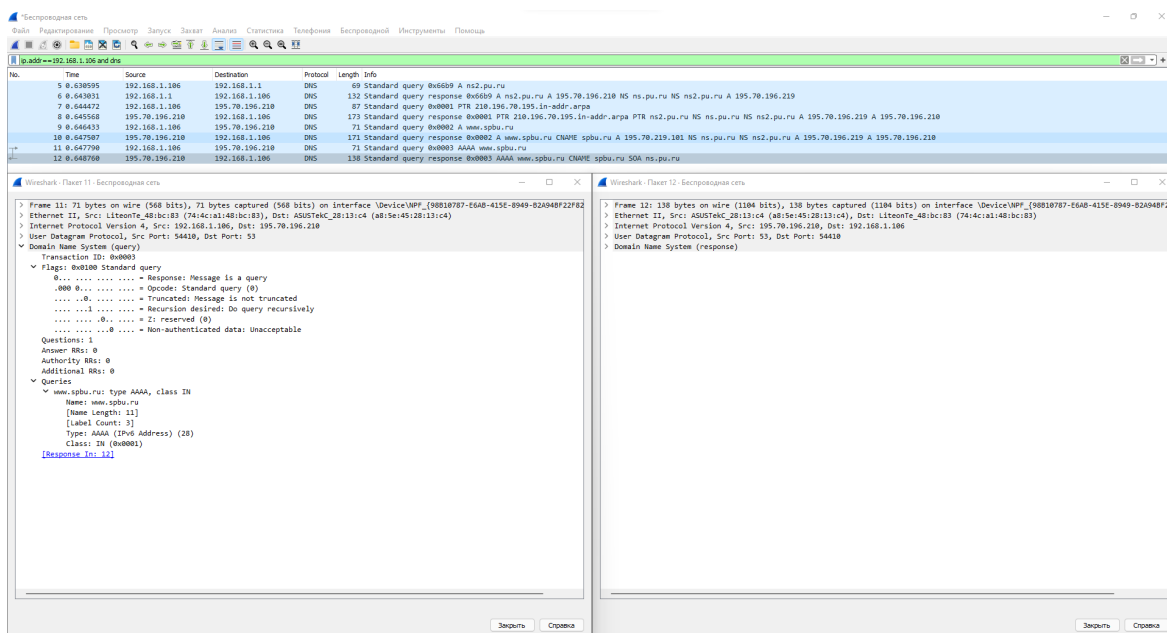
1. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию? Если нет, то какому хосту он принадлежит?

DNS-запрос отправлен на адрес 195.70.196.210. Он не совпадает с адресом локального DNS-сервера, установленного по умолчанию (192.168.1.1). Он принадлежит одному из DNS-серверов университета с доменным именем ns2.pu.ru.



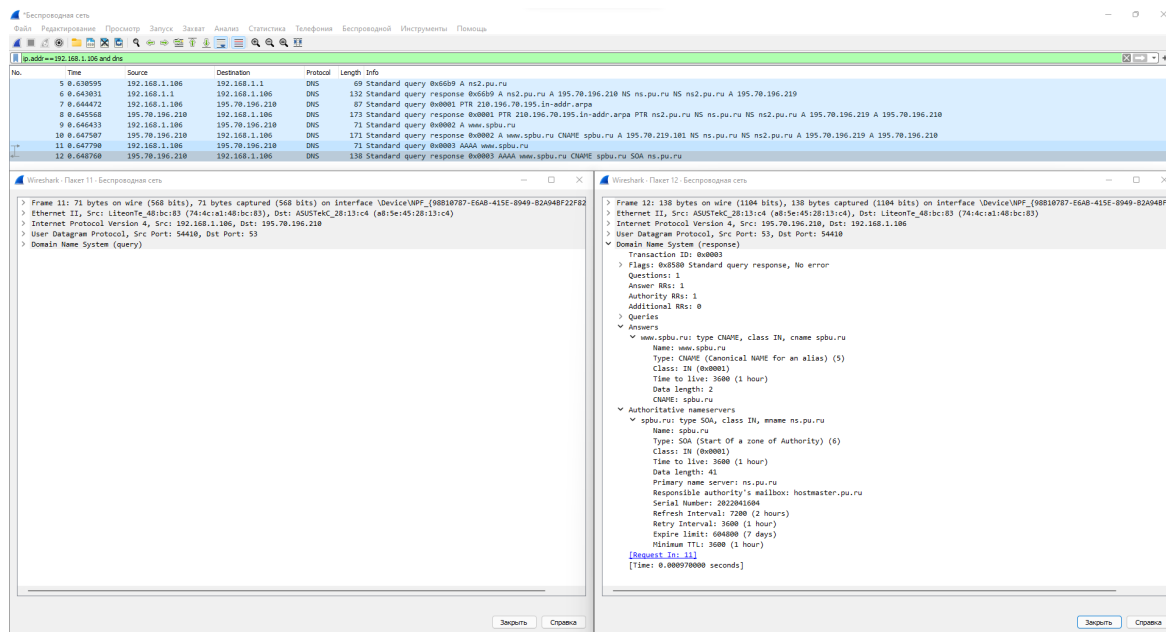
2. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

Запрашивается запись типа AAAA (IPv6 Address). В запросе присутствует поле «Answer RRs». 0 в этом поле означает, что ответов нет.



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

В ответном сообщении DNS есть один ответ. Он имеет тип CNAME и связывает имя, которое мы запросили, с другим (spbu.ru).



Задание 5:


1. Что такое база данных whois?

Whois (от англ. who is — «кто есть») — это общедоступная база данных, в которой хранится информация о доменах и их владельцах. Регулирует базу Международная корпорация по присвоению имен и номеров (ICANN), которая описывает службу WHOIS как бесплатный общедоступный каталог с контактной и технической информацией о зарегистрированном доменном имени.

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

Я воспользовался сервисом whois.ru и получил имена DNS-серверов ns1.google.com и ns2.google.com.

Главная | Регистрация доменов | Освобождающиеся домены | Парковка доменов | SIG

 **Официальный WHOIS сервис**
Информация о домене или IP

google.com Мой IP Путь-код-конвертация Q показать

Информация о домене: google.com Доступен через Бrowsers PDF (английский) PDF (русский)

<p>Domain Name: GOOGLE.COM Registry Domain ID: 2188554_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.markmonitor.com Registrar URL: http://www.markmonitor.com Updated Date: 2019-09-09T15:39:04Z Creation Date: 1997-09-15T04:00:00Z Registry Expiry Date: 2028-09-14T04:00:00Z Registrar: MarkMonitor Inc. Registrar Abuse Contact Email: abusecomplaints@markmonitor.com Registrar Abuse Contact Phone: +1.2086851750 Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited Name Server: NS1.GOOGLE.COM Name Server: NS2.GOOGLE.COM Name Server: NS3.GOOGLE.COM Name Server: NS4.GOOGLE.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/icc/f/ >>> Last update of whois database: 2022-05-09T10:28:08Z <<<</p>	<p>Домен: GOOGLE.COM Идентификатор домена в реестре: 2188554_DOMAIN_COM-VRSN Whois-сервис регистратора: whois.markmonitor.com URL сайта регистратора: http://www.markmonitor.com Дата изменения: 2019.09.09 15:39:04 MSK Дата регистрации: 1997.09.15 04:00:00 MSD Дата окончания: 2028.09.14 07:00:00 MSK Регистратор: MarkMonitor Inc. Идентификатор реестра в 24041: 202 E-mail: abusecomplaints@markmonitor.com Номер телефона: +1.2086851750 Состояние: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited Состояние: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Состояние: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited Состояние: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited Состояние: serverTransferProhibited https://icann.org/epp#serverTransferProhibited Состояние: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited Сервер: NS1.GOOGLE.COM Сервер: NS2.GOOGLE.COM Сервер: NS3.GOOGLE.COM Сервер: NS4.GOOGLE.COM DNSSEC: unsigned URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/icc/f/ >>> Last update of whois database: 2022-05-09T10:28:08Z <<<</p>
--	---

3. Используйте команду nslookup на локальном хосте чтобы послать запросы трем серверам DNS: вашему локальному серверу DNS и двум DNS-серверам, найденным в предыдущей части.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.22000.613]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\uvd20>nslookup google.com
Server: router.asus.com
Address: 192.168.1.1

Не заслуживающий доверия ответ:
Server: google.com
Addresses: 2a00:1450:4010:c08::64
          2a00:1450:4010:c08::8b
          2a00:1450:4010:c08::66
          2a00:1450:4010:c08::8a
          64.233.165.100
          64.233.165.139
          64.233.165.101
          64.233.165.138
          64.233.165.102
          64.233.165.113

C:\Users\uvd20>nslookup google.com ns1.google.com
Server: ns1.google.com
Address: 216.239.32.10

Server: google.com
Addresses: 2a00:1450:4010:c0d::65
          2a00:1450:4010:c0d::8a
          2a00:1450:4010:c0d::64
          2a00:1450:4010:c0d::71
          173.194.73.102
          173.194.73.100
          173.194.73.139
          173.194.73.101
          173.194.73.113
          173.194.73.138

C:\Users\uvd20>nslookup google.com ns2.google.com
Server: ns2.google.com
Address: 216.239.34.10

Server: google.com
Addresses: 2a00:1450:4010:c0d::71
          2a00:1450:4010:c0d::64
          2a00:1450:4010:c0d::8a
          2a00:1450:4010:c0d::8b
          173.194.73.138
          173.194.73.101
          173.194.73.100
          173.194.73.113
          173.194.73.139
          173.194.73.102

C:\Users\uvd20>
```