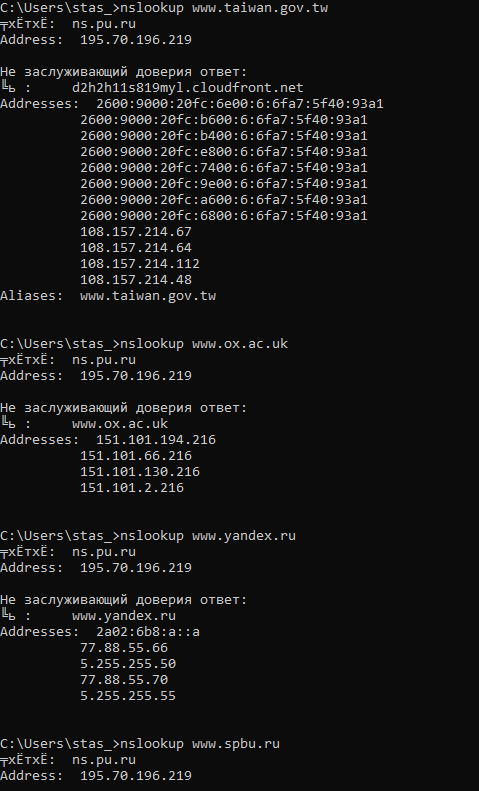
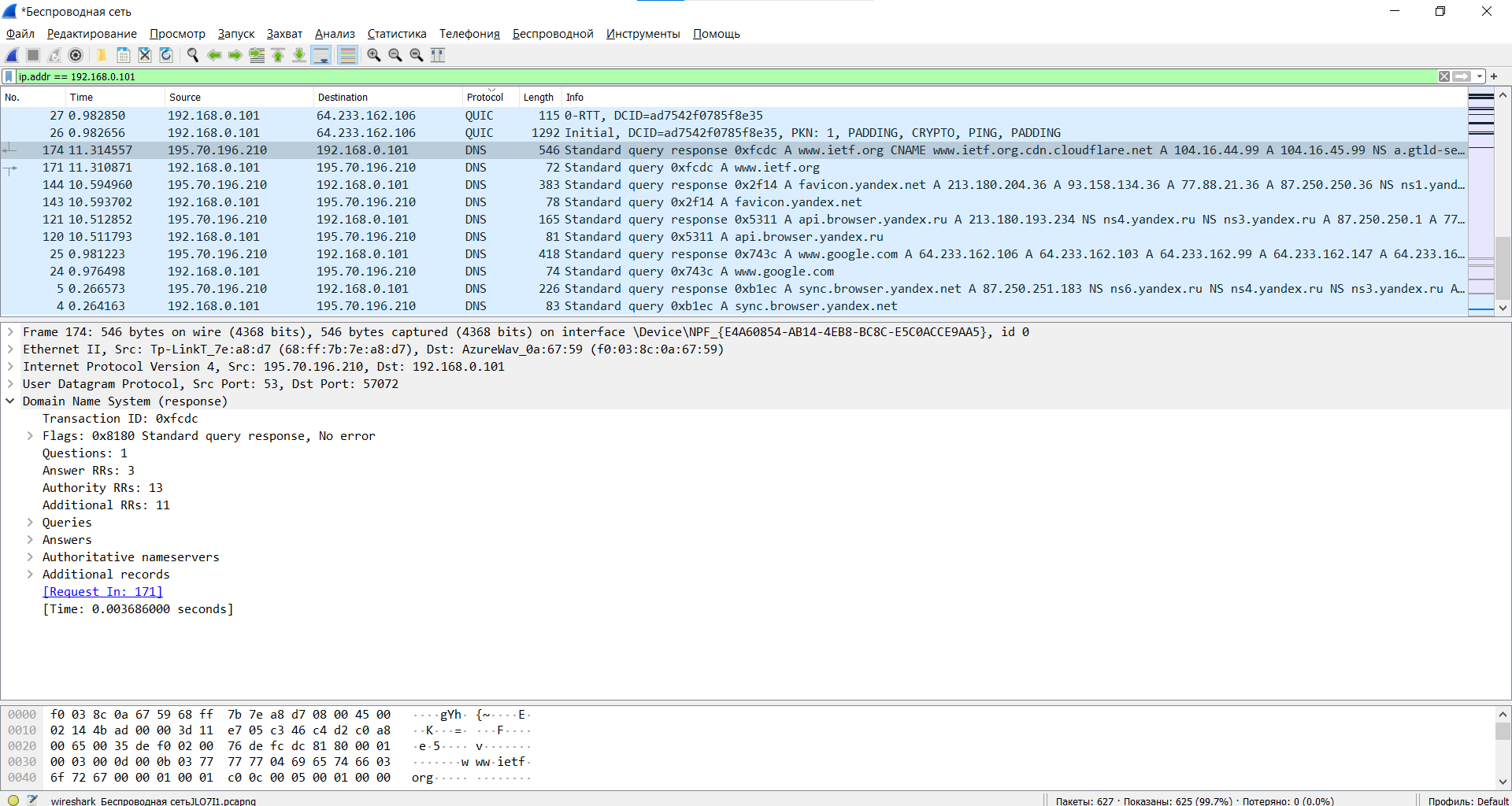
## WireShark. ДЗ4.

## А. Утилита nslookup

* Выполните nslookup, чтобы получить IP-адрес какого-либо веб-сервера в Азии
* Выполните nslookup, чтобы определить авторитетные DNS-серверы для какого-либо университета в Европе
* Используя nslookup, найдите веб-сервер, имеющий несколько IP-адресов. Сколько IPадресов имеет веб-сервер вашего учебного заведения?



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



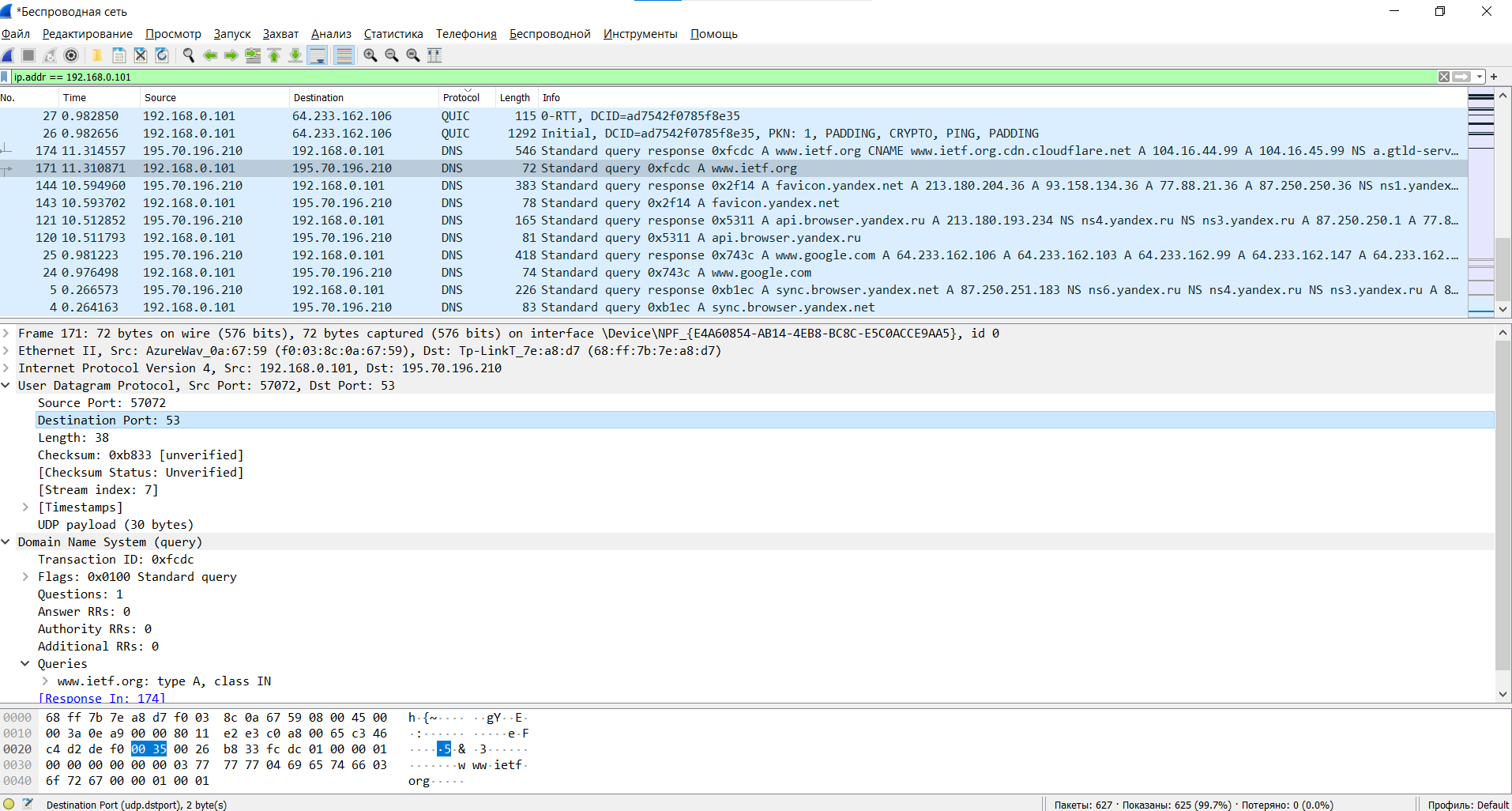
Вопросы:

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

DNS протокол.

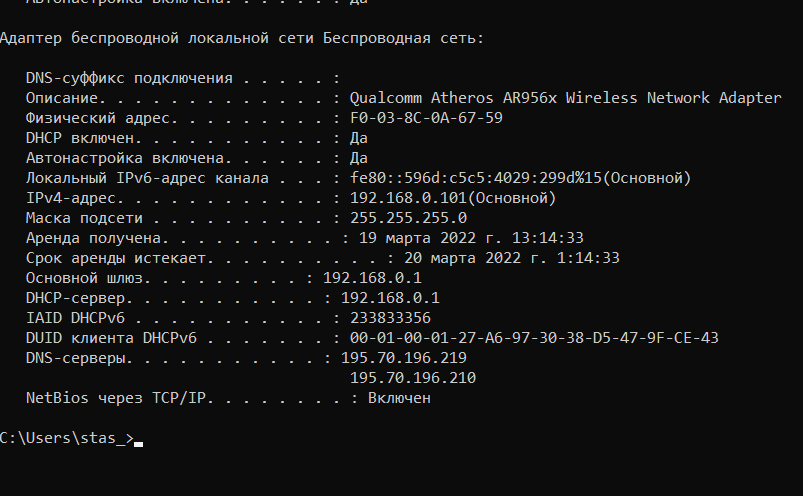
* Какой порт назначения у запроса DNS?

53



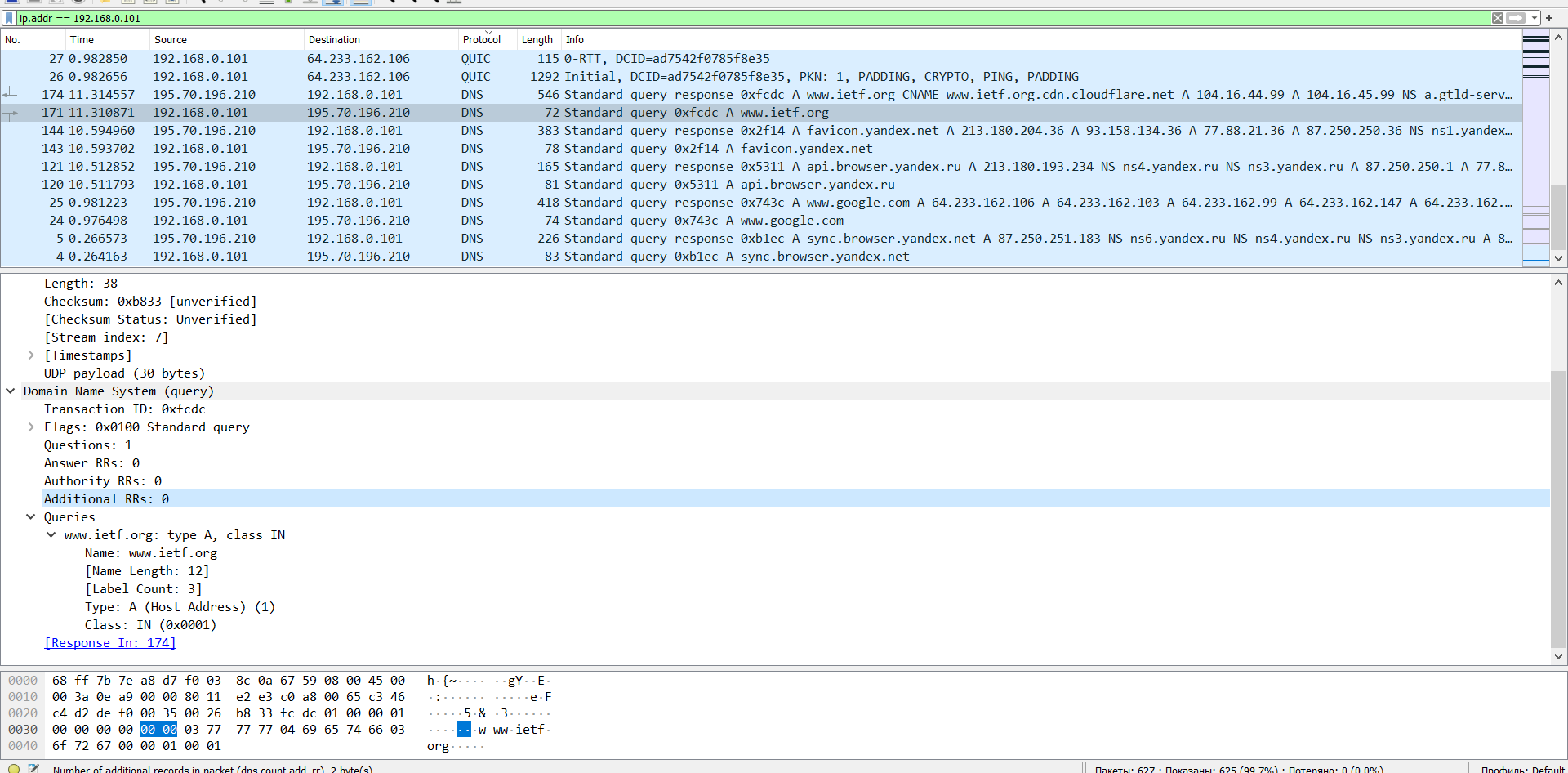
* На какой IP-адрес отправлен DNS-запрос? Используйте ipconfig для определения IP-адреса вашего локального DNS-сервера. Одинаковы ли эти два адреса?

195.70.196.210. Да, с помощью ipconfig /all видим, что совпадает.



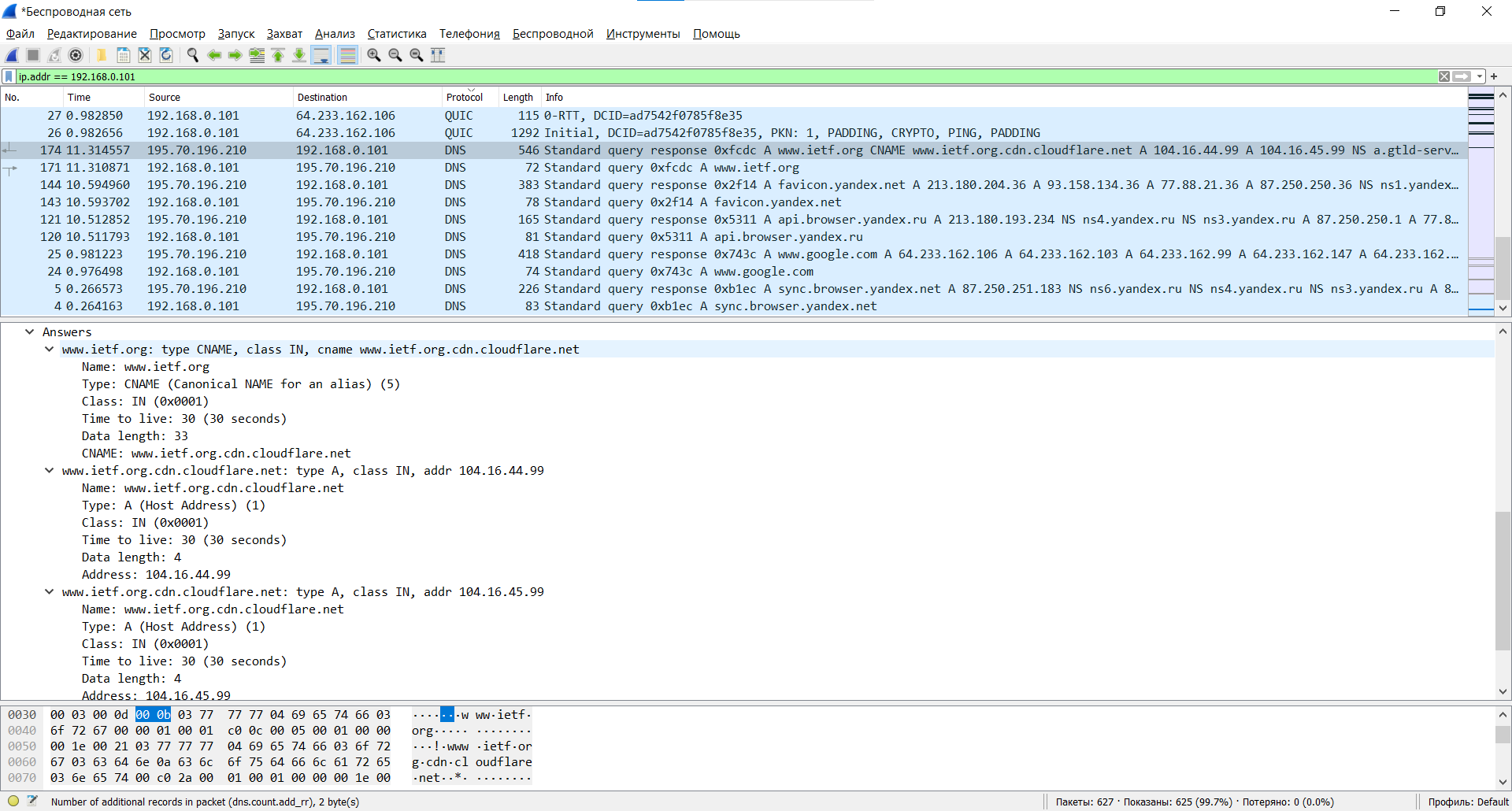
* Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?

Type A. Ответов нет.



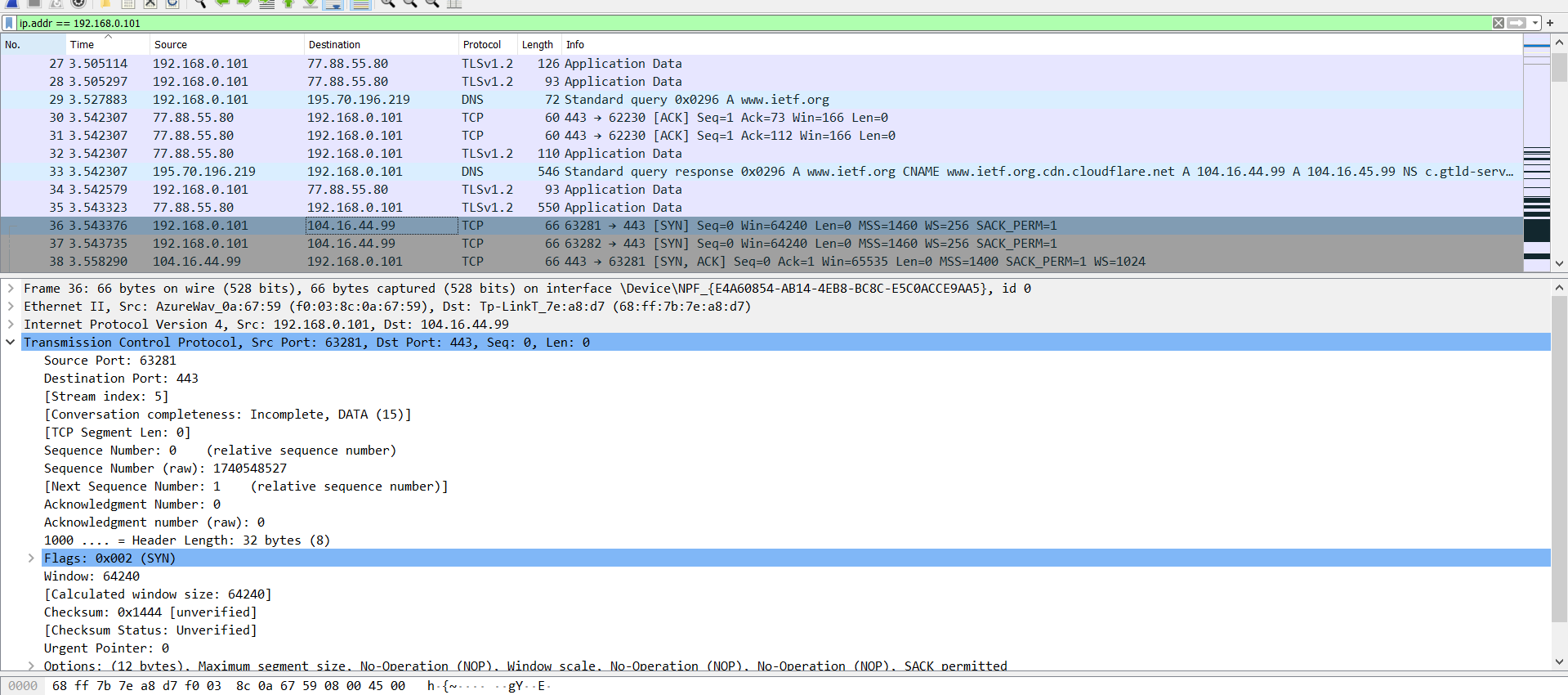
* Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

Получили 3 ответа: type CNAME, type A, type A. Содержание ответов на скрине.



* 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, совпадает (перезапускал захват, так как в первый раз сообщения TCP не было).

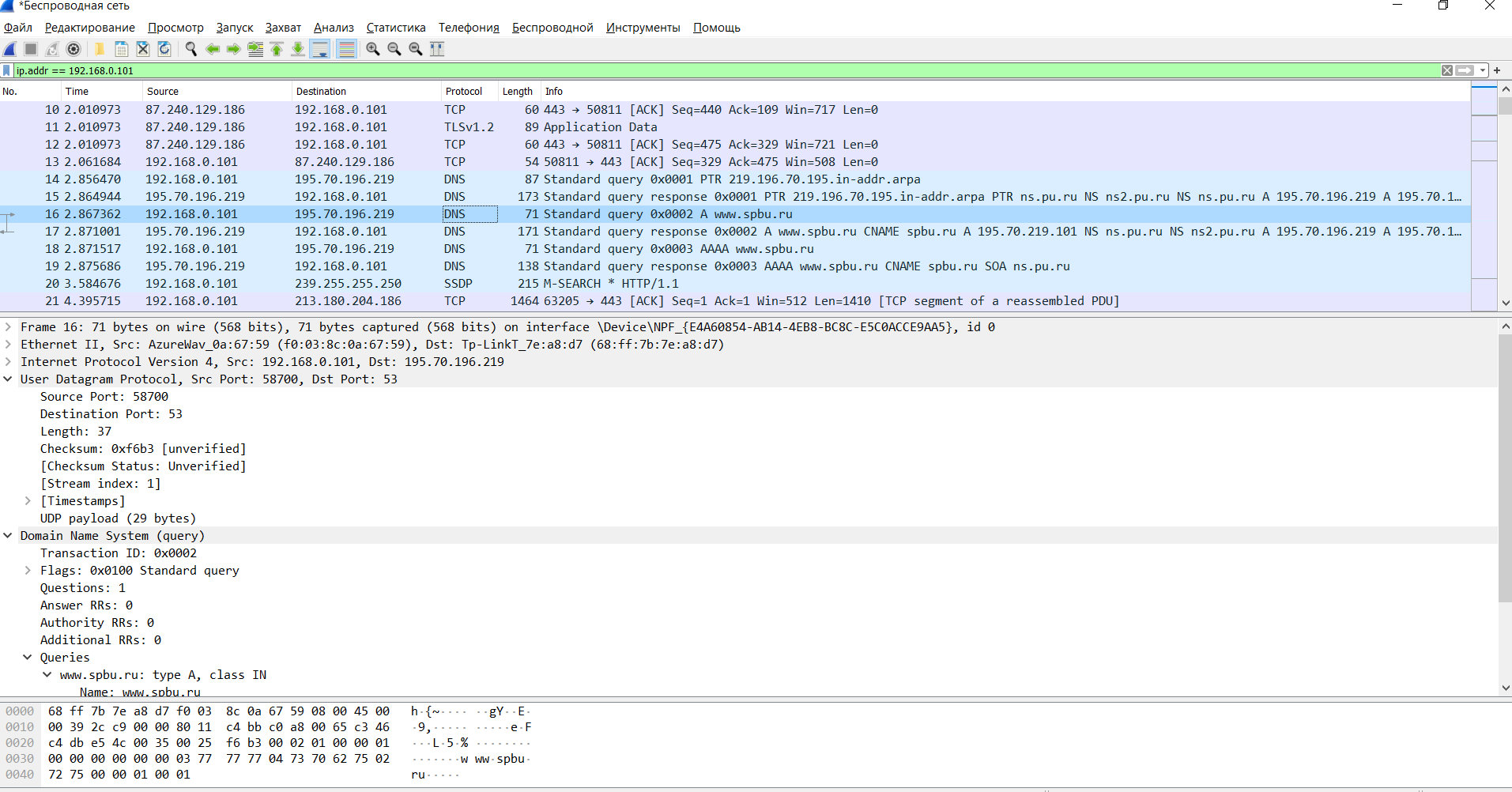


* Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?

Нет, не выполняет. После этого больше количество сообщений от ip-адреса из ответов, видимо вся информация была получена.

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

* Каков порт назначения в запросе DNS? Какой порт источника в DNS-ответе?

53

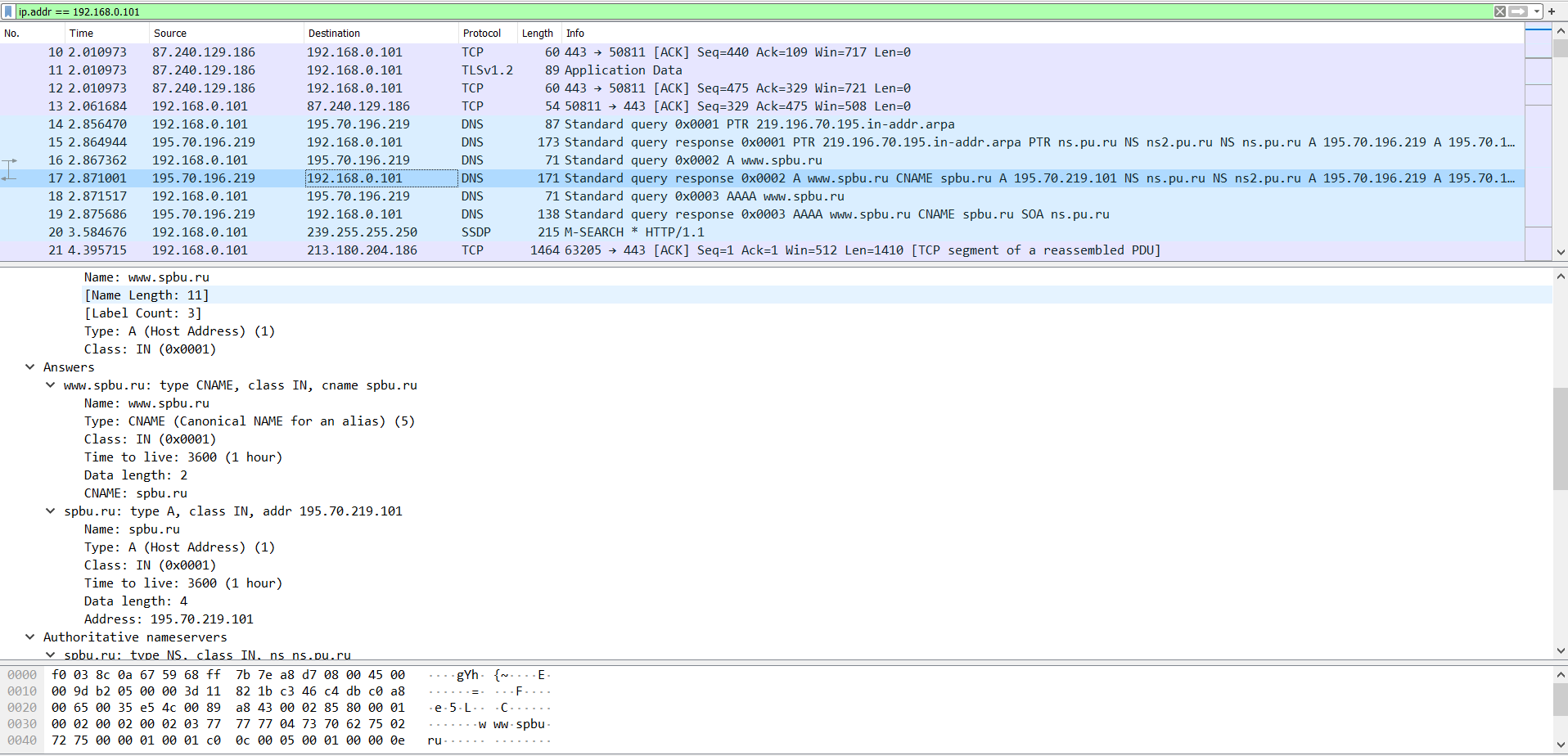
* На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNSсервера, установленного по умолчанию?

195.70.196.219  
Да, совпадает, был скрин выше.

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

Type A, ответов нет.

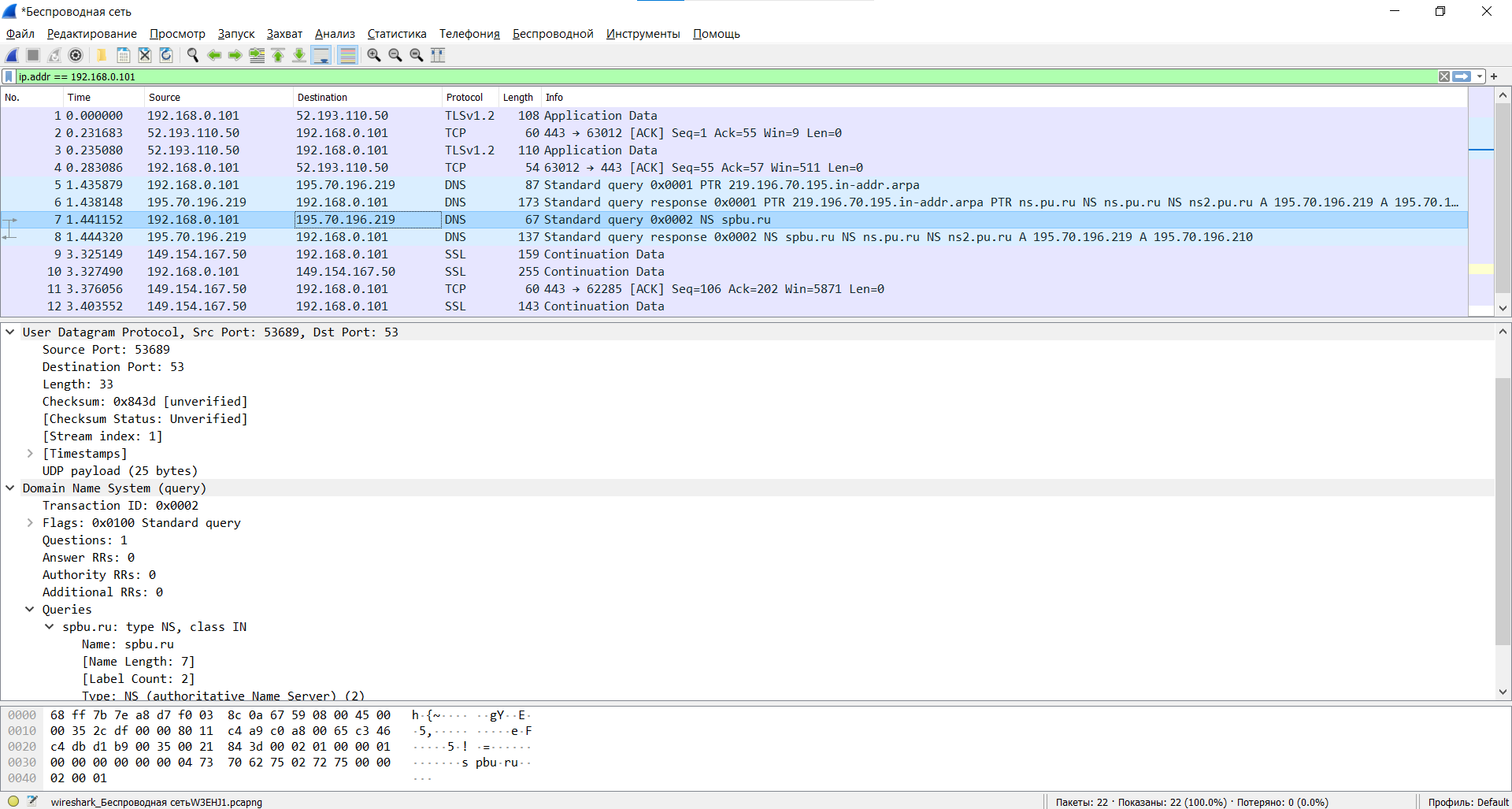
* Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?



Тут ответы есть, тоже Type A.

*В дополнение к заданию, я отметил, что также был DNS запрос(видно на скрине), в котором требовались ответы Type AAAA.*

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



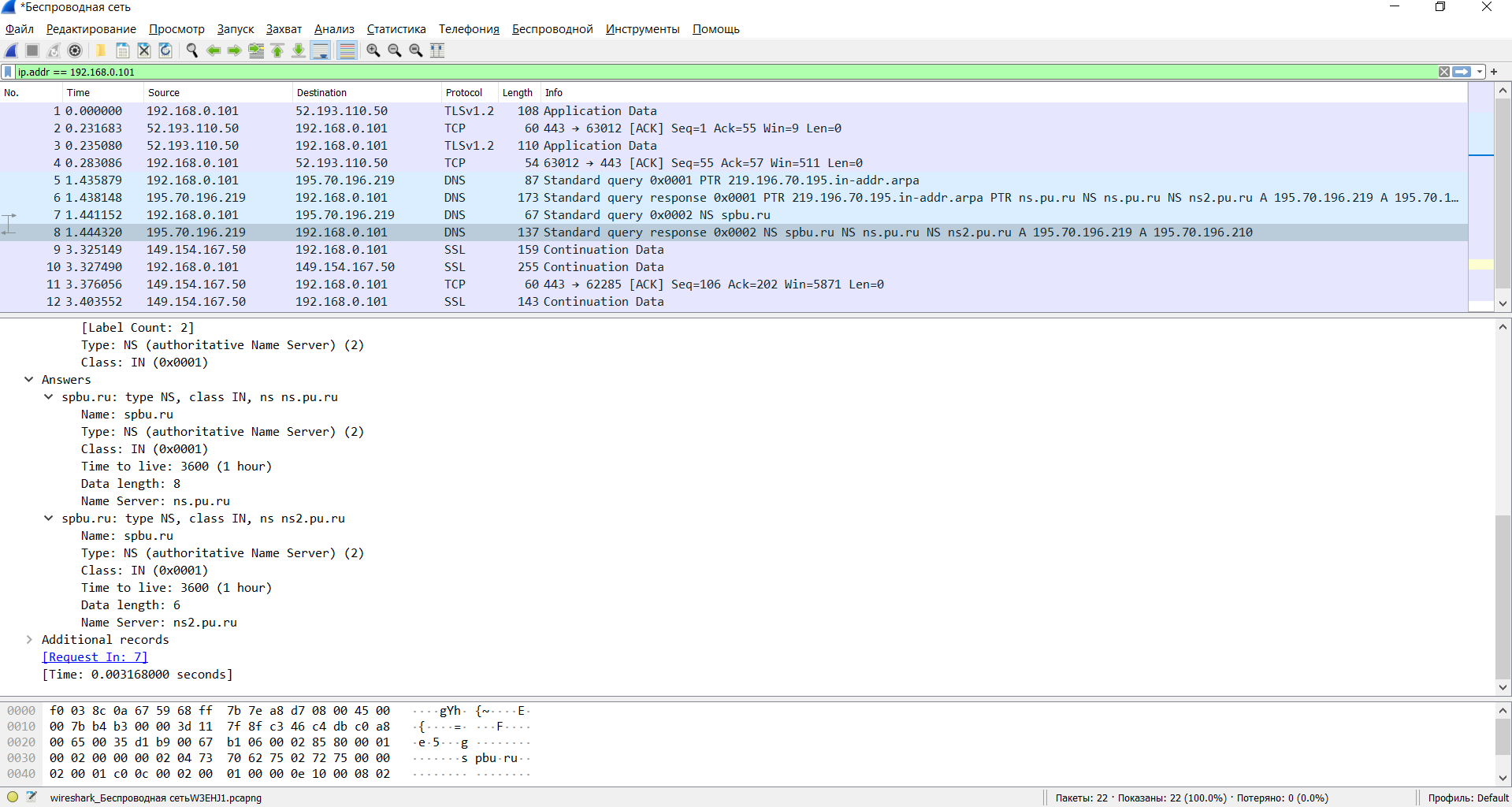
* На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNSсервера, установленного по умолчанию?

Да, совпадает с ip-адресом из скрина про локальные DNS сервера.

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

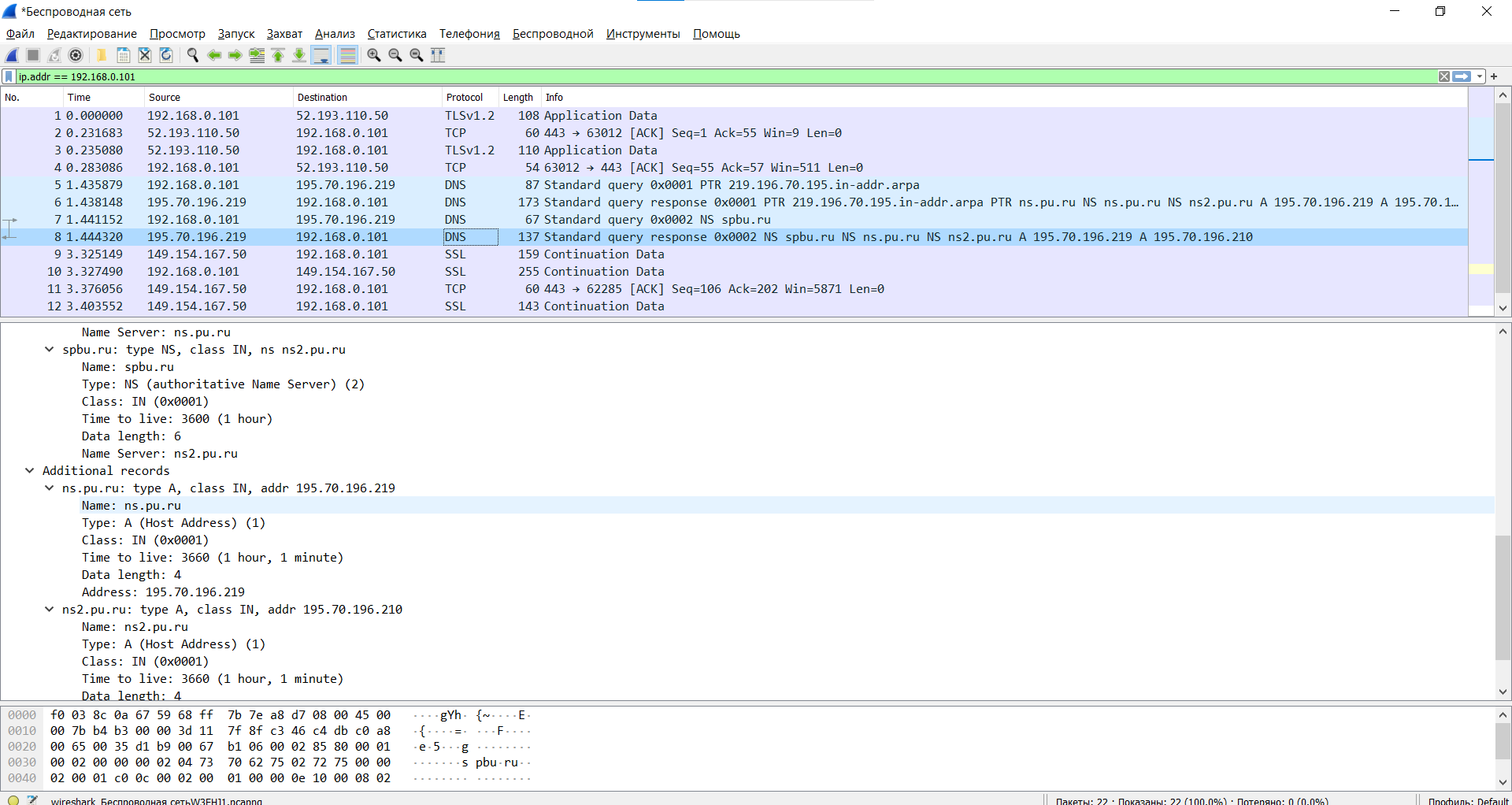
Type NS. Ответов нет.

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



Имена: ns.pu.ru, ns2.pu.ru

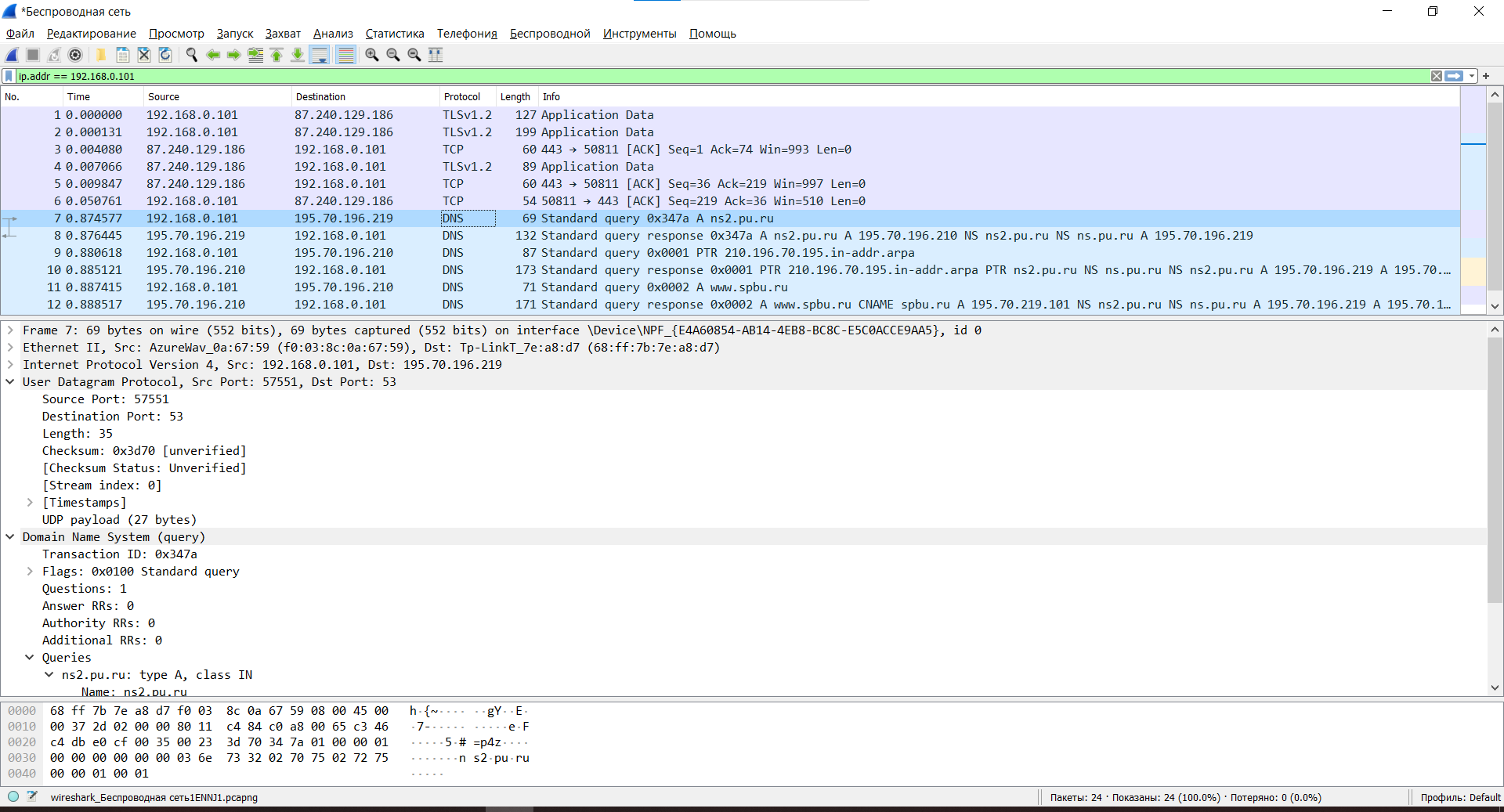
Да, адреса есть в Additional records:



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

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

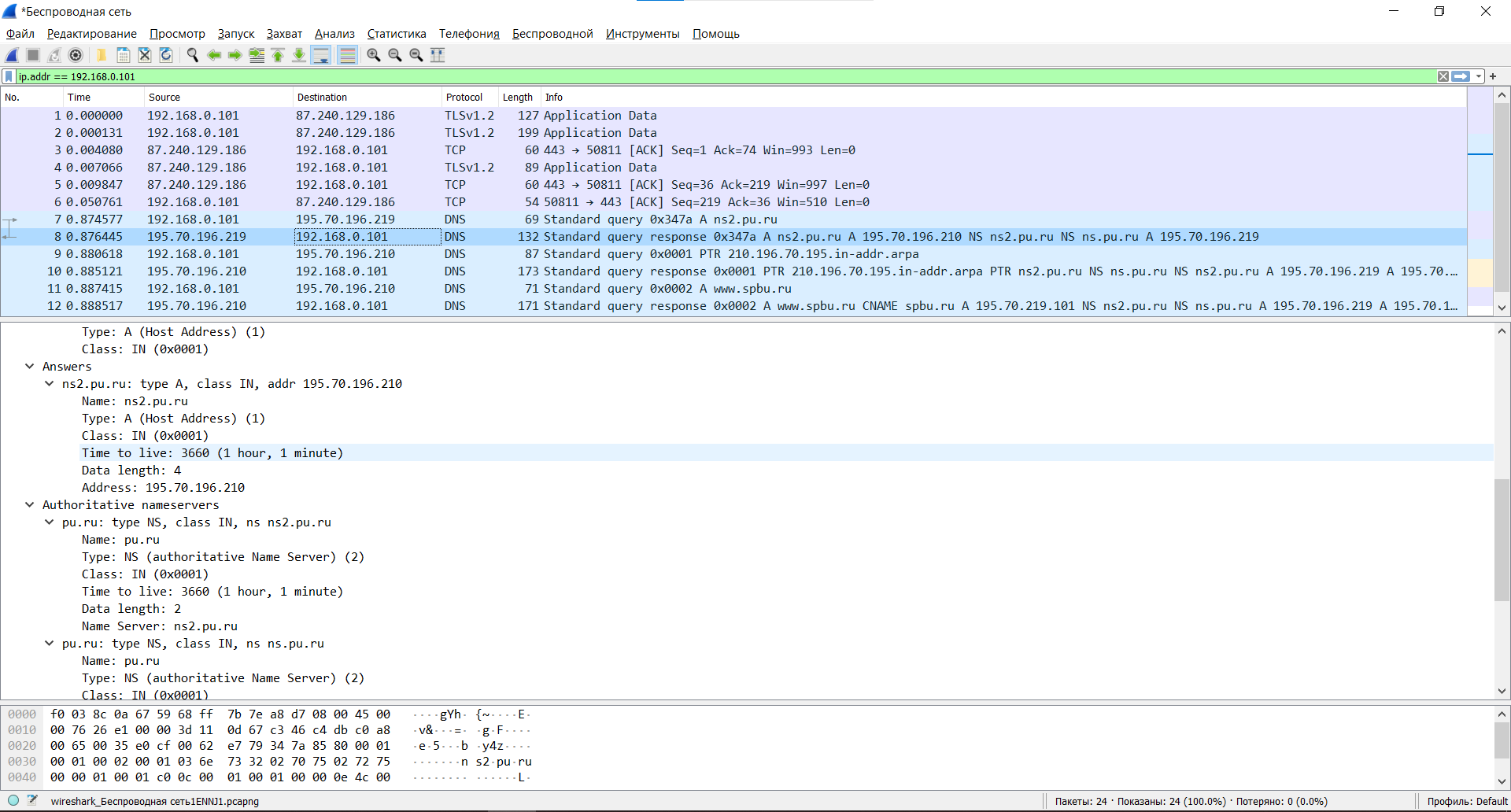
195.70.196.219. Совпадает с адресом локального DNS сервера.



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

Type A. Ответов нет.

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



1 ответ type A.

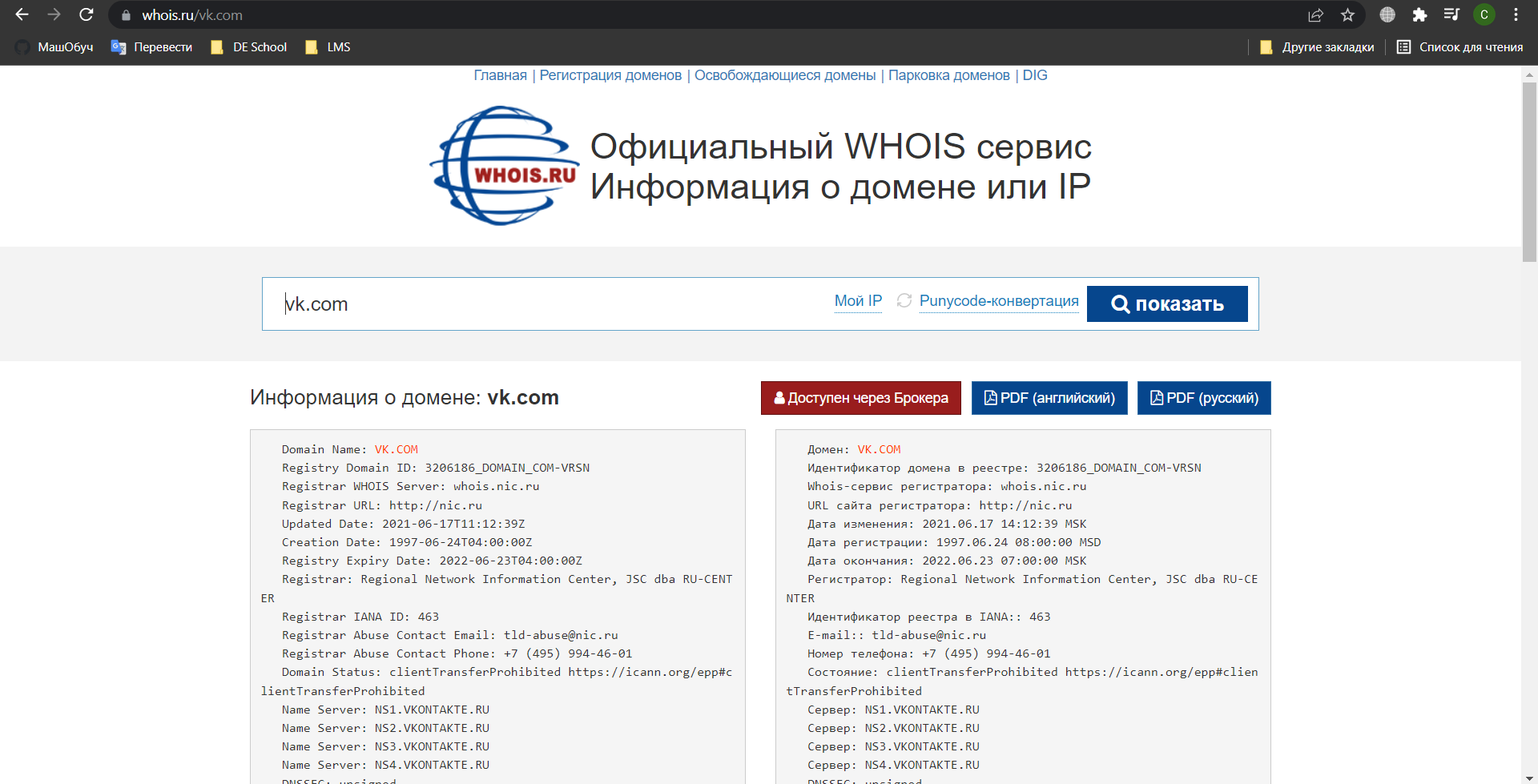
## Е. Сервисы whois

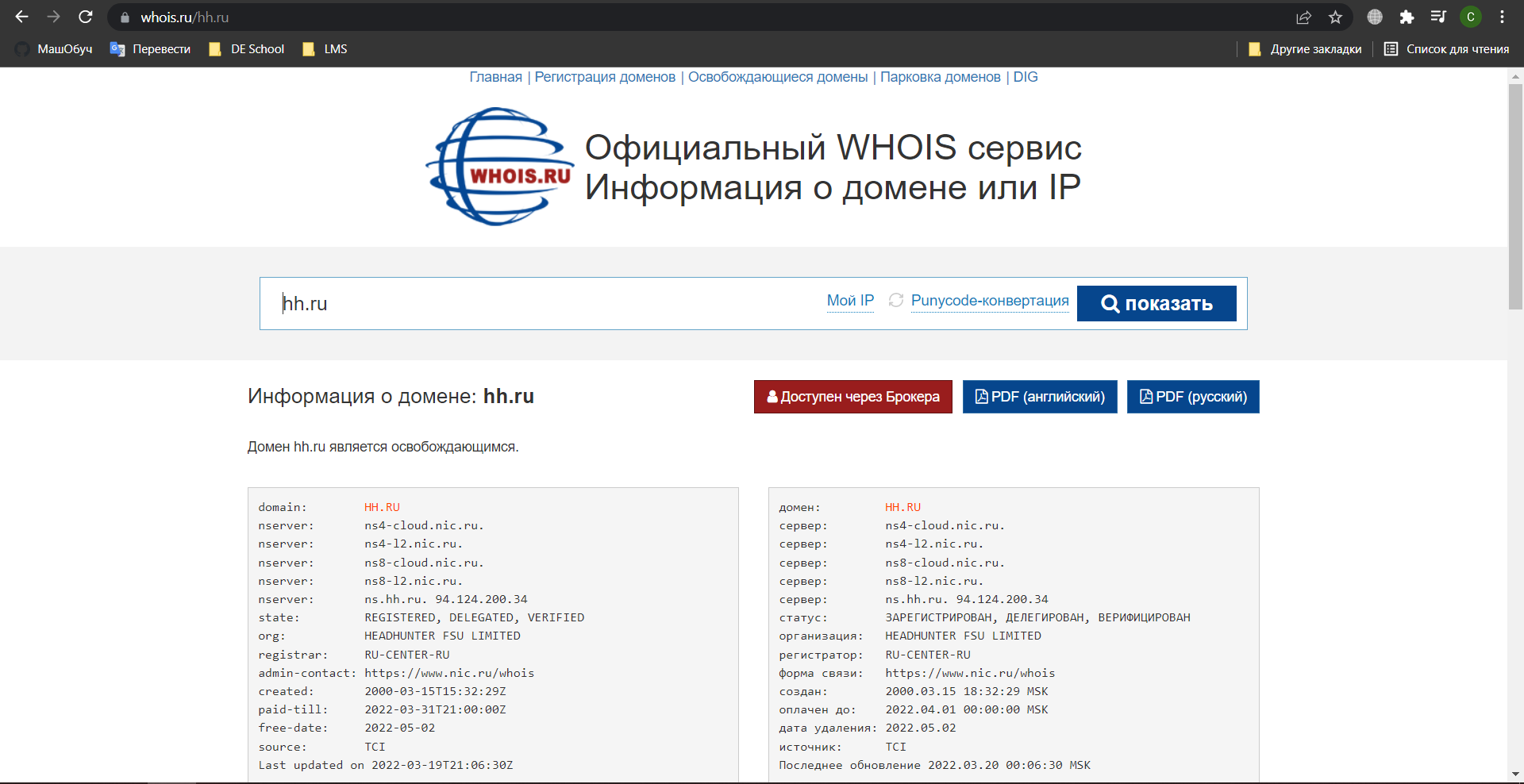
* Что такое база данных whois?

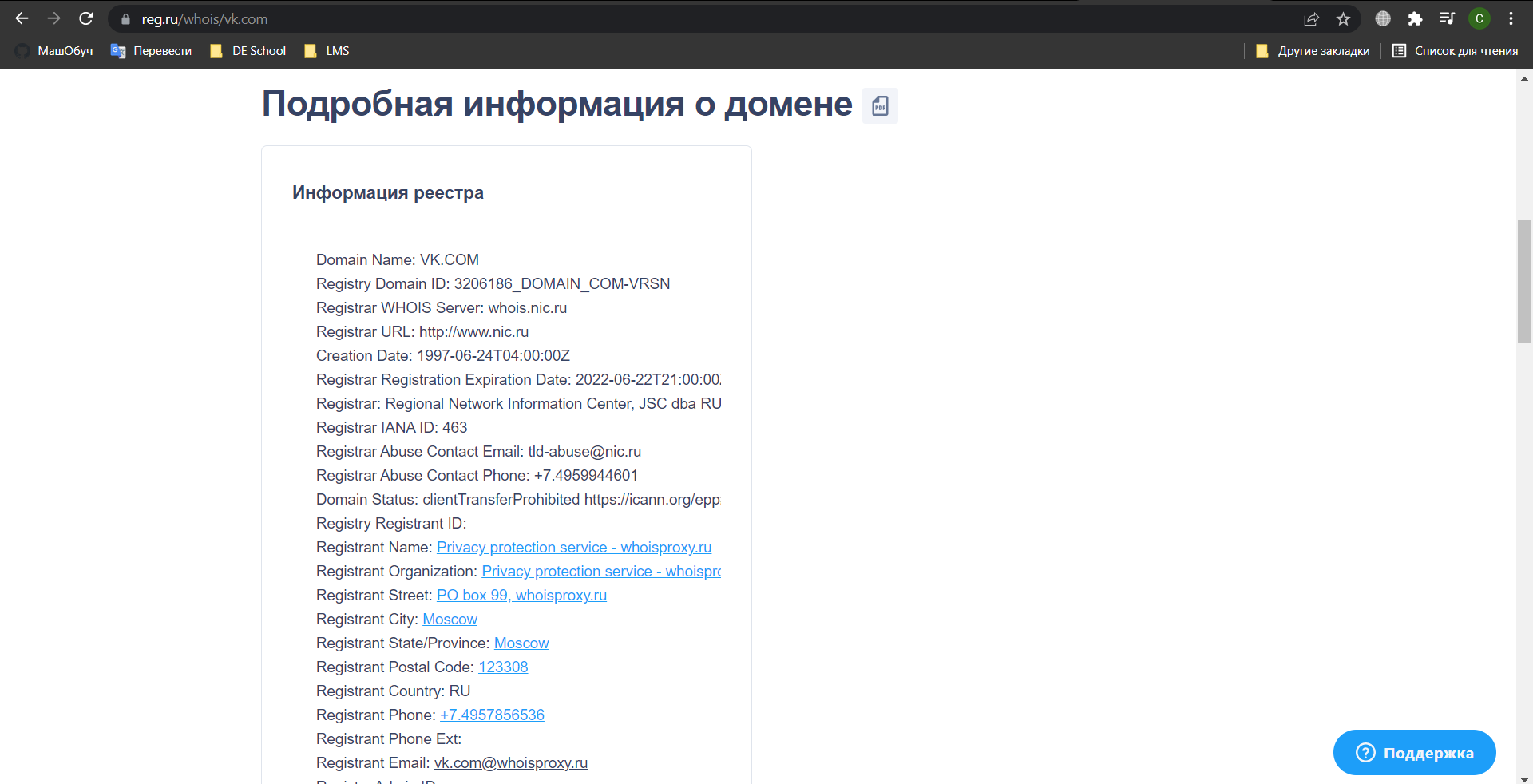
По данным русской википедии: WHOIS — сетевой протокол прикладного уровня, базирующийся на протоколе TCP (порт 43). Основное применение — получение регистрационных данных о владельцах доменных имён, IP-адресов и автономных систем.

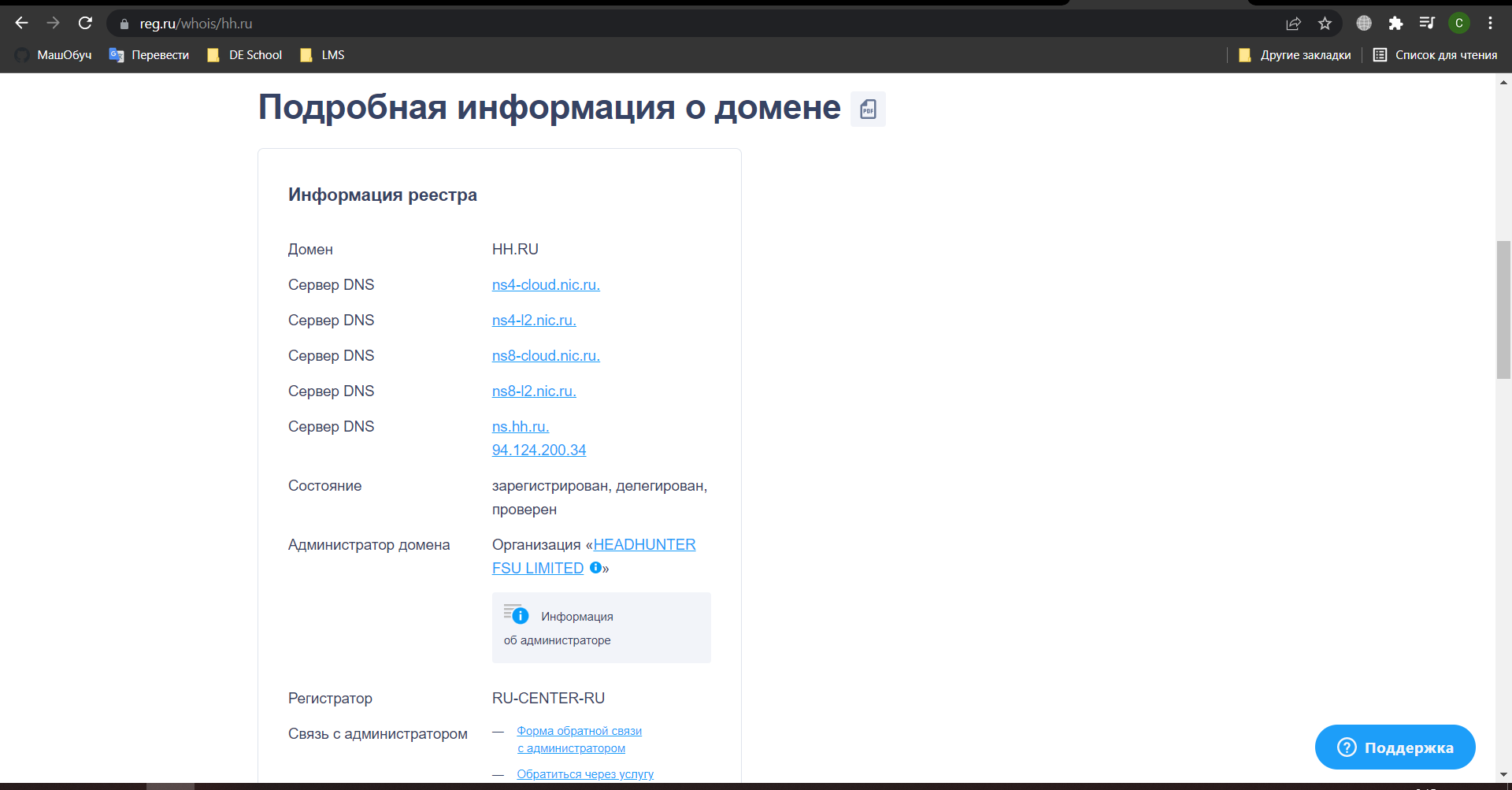
* Используя различные сервисы whois в Интернете, получите имена любых двух DNSсеверов. Какие сервисы вы при этом использовали?

Использовал сервисы: <https://whois.ru>, <https://www.reg.ru/whois/>









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

