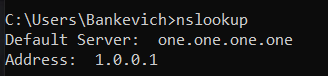
**АиПОС Лабораторная работа №4**

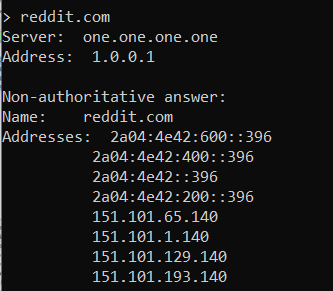
**Задание №6**

Перехватите 3 DNS запроса, используя свой DNS-сервер, и 3 DNS запроса, используя сторонний DNS-сервер (для этого необходимо использовать утилиту nslookup с правильной конфигурацией и Wireshark для перехвата пакетов).

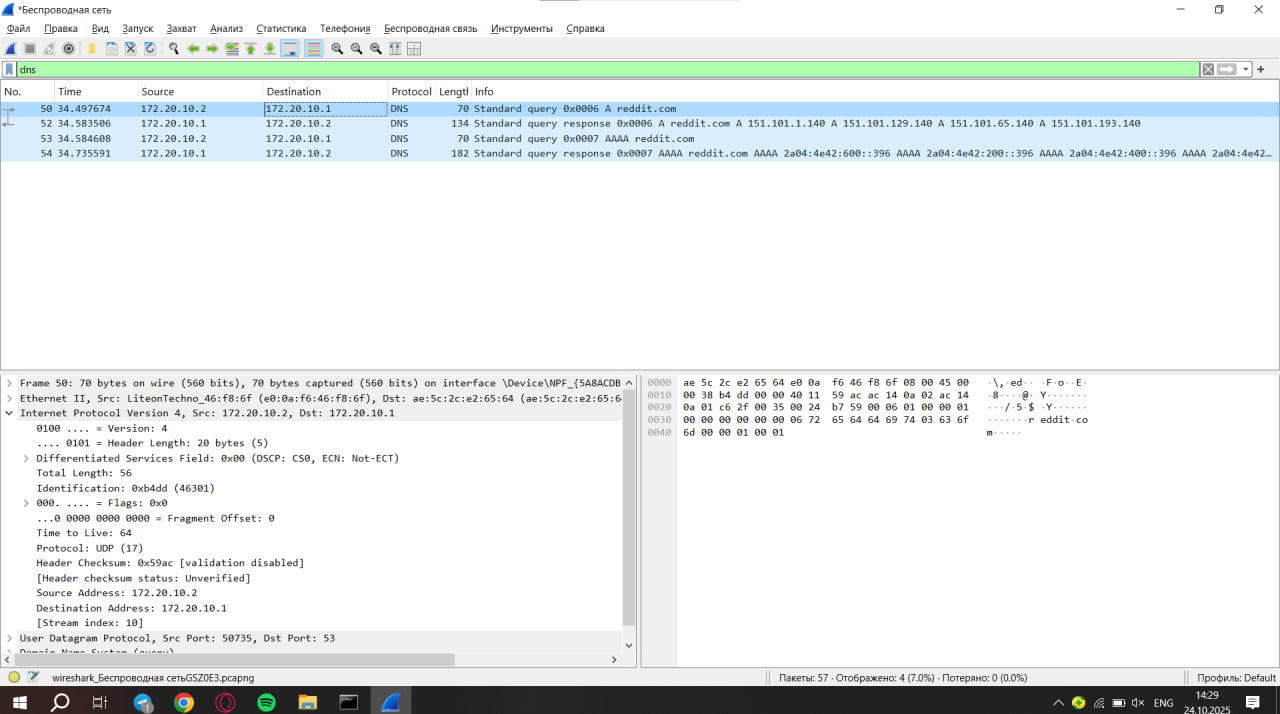
- Запускаем интерактивный режим для запросов к DNS серверу



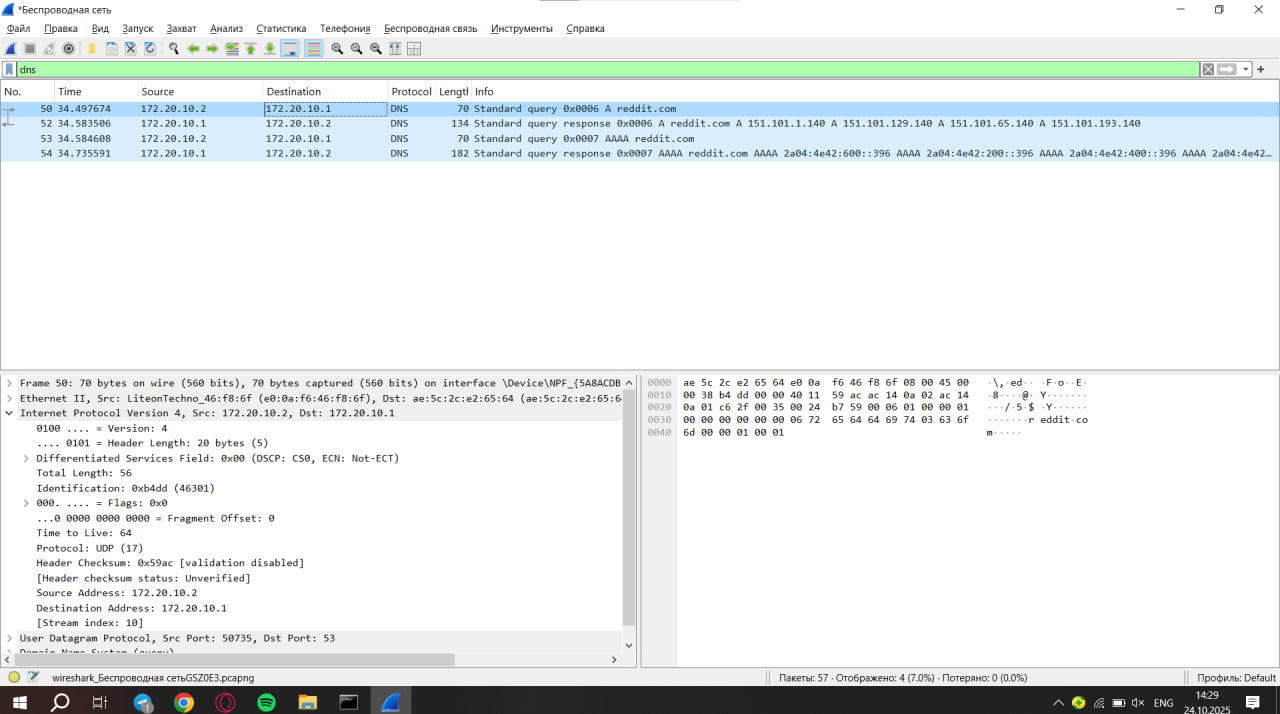
1. **DNS-запрос reddit.com**



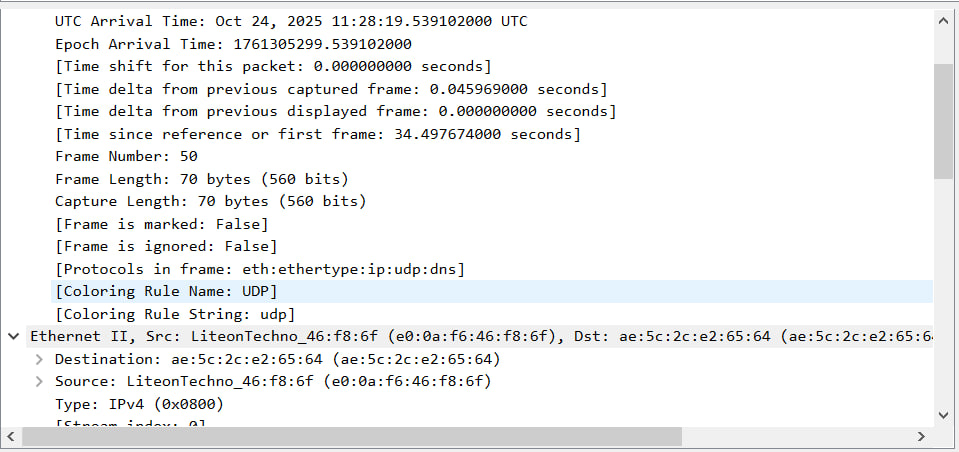
* *Найдите DNS-запрос и ответ на него. С использованием UDP или TCP они отправлены?*



* Было отправлено и получено по 2 запроса (запрос&ответ для А(Ipv4), запрос&ответ для АААА(Ipv6))



- Используется протокол UDP



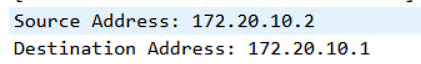
* *Какой порт назначения у запроса DNS? Каков исходящий порт у DNS-ответа?*

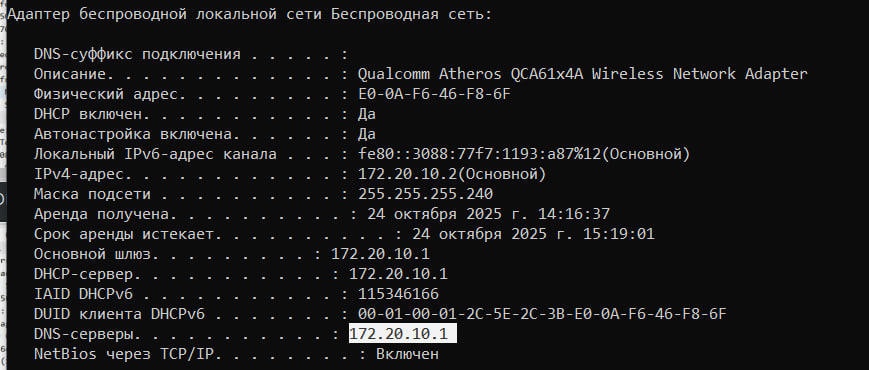
- DNS работает с 53 портом, отправляя и получая на него запросы



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

- Destination Address: DNS-запрос был отправлен на локальный DNS (IP-адрес роутера), т.к. мы используем свой => адреса одинаковы





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

- запрос для А(Ipv4), запрос для АААА(Ipv6)

- в DNS-**запросе** не содержатся ответы

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

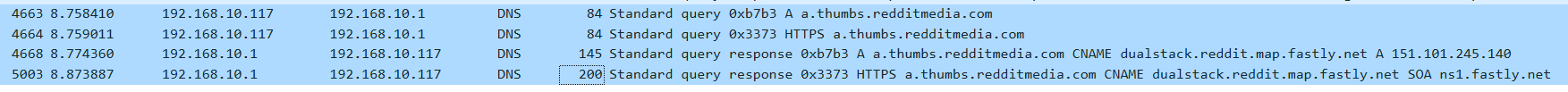
- На каждый запрос по одному ответу. В нашем случае было отправлено 2 запроса (А и АААА), следовательно было получено 2 ответа (А и АААА)

- В каждом ответном сообщении содержится один ответ (один IP-адрес)

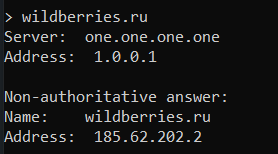
* *Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?*

- Если изображения на том же домене, хост использует кэш DNS. Если же изображение хранится на другом, то будут сделаны дополнительные DNS-запросы

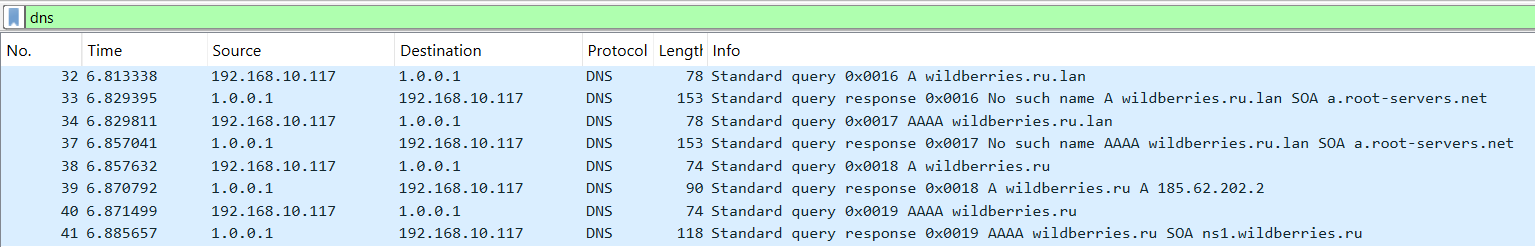
- В нашем случае были сделаны доп запросы для домена a.thumbs.redditmedia.com , который используется Reddit для хранения и доставки изображений.



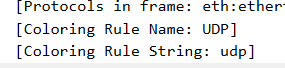
1. **DNS-запрос wildberries.com**



* *Найдите DNS-запрос и ответ на него. С использованием UDP или TCP они отправлены?*



* Было отправлено и получено по 4 запроса (запрос&ответ для А(Ipv4), причем первые 2 не дали ответ, т.к. на главном DNS-сервере не было информации об этом домене и пришлось перенаправить запрос на DNS-сервер 1-го уровня, который хранит информацию о .ru
* запрос&ответ для АААА(Ipv6)), используется протокол UDP



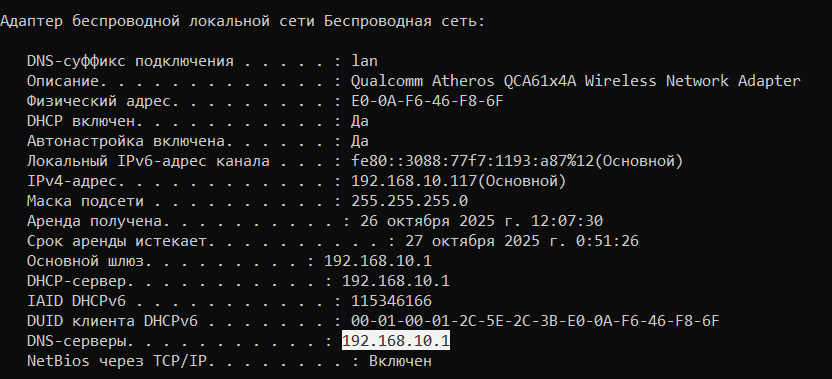
* *Какой порт назначения у запроса DNS? Каков исходящий порт у DNS-ответа?*



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

- Destination Address: DNS-запрос был отправлен на локальный DNS (IP-адрес роутера), т.к. мы используем свой => адреса одинаковы





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

- запрос для А(Ipv4), запрос для АААА(Ipv6)

- в DNS-**запросе** не содержатся ответы

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

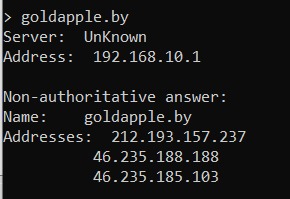
- На каждый запрос по одному ответу. В нашем случае было отправлено 2 запроса (А и АААА), следовательно было получено 2 ответа (А и АААА)

- В каждом ответном сообщении содержится один ответ (один IP-адрес или информация об отсутсвии на текущем сервере такого имени, как в первых двух запросах)

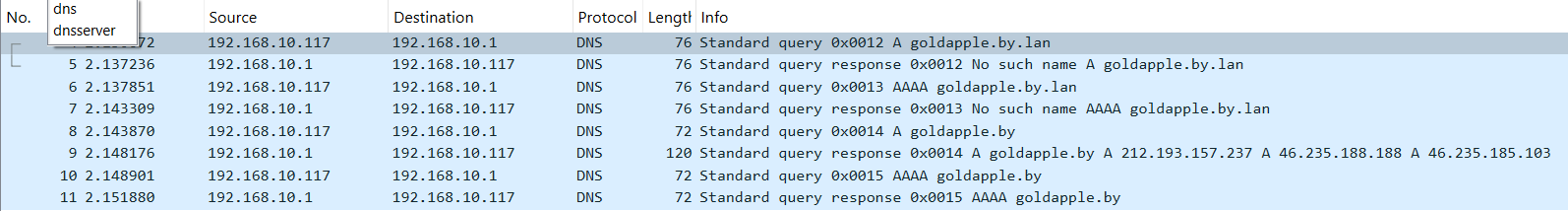
* *Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?*

**

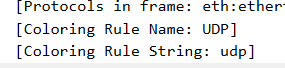
1. **DNS-запрос goldapple.by**



* *Найдите DNS-запрос и ответ на него. С использованием UDP или TCP они отправлены?*



* Было отправлено и получено по 4 запроса (запрос&ответ для А(Ipv4), причем первые 2 не дали ответ, т.к. на главном DNS-сервере не было информации об этом домене и пришлось перенаправить запрос на DNS-сервер 1-го уровня, который хранит информацию о .ru
* запрос&ответ для АААА(Ipv6)), используется протокол UDP



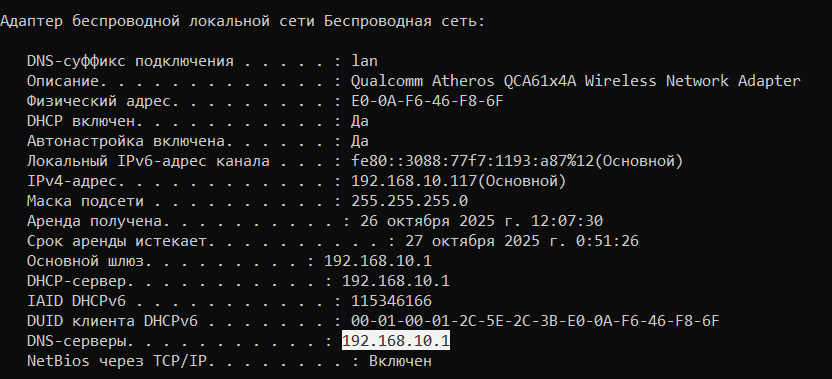
* *Какой порт назначения у запроса DNS? Каков исходящий порт у DNS-ответа?*



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

- Destination Address: DNS-запрос был отправлен на локальный DNS (IP-адрес роутера), т.к. мы используем свой => адреса одинаковы





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

- запрос для А(Ipv4), запрос для АААА(Ipv6)

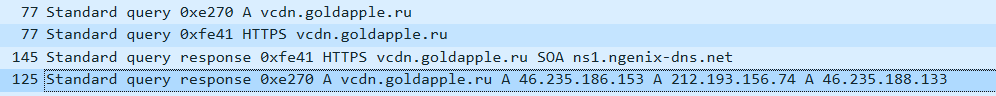
- в DNS-**запросе** не содержатся ответы

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

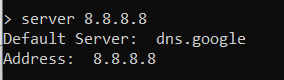
- На каждый запрос по одному ответу. В нашем случае было отправлено 2 запроса (А и АААА), следовательно было получено 2 ответа (А и АААА)

- В каждом ответном сообщении содержится один ответ (один IP-адрес или информация об отсутствии на текущем сервере такого имени, как в первых двух запросах)

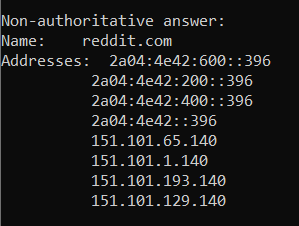
* *Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?*
* Запрос на vcdn

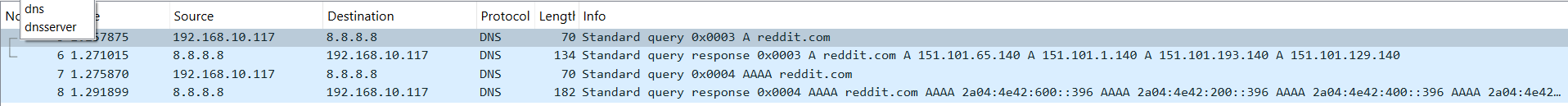


**Запросы через сервер google**

****

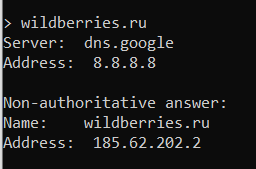
1. **Reddit.com**

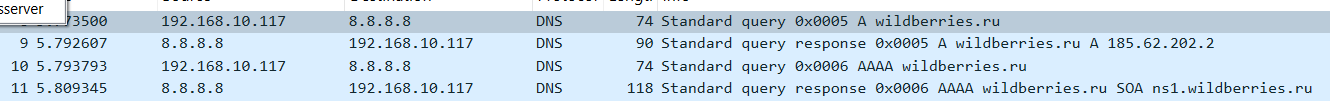
****

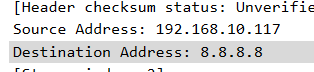




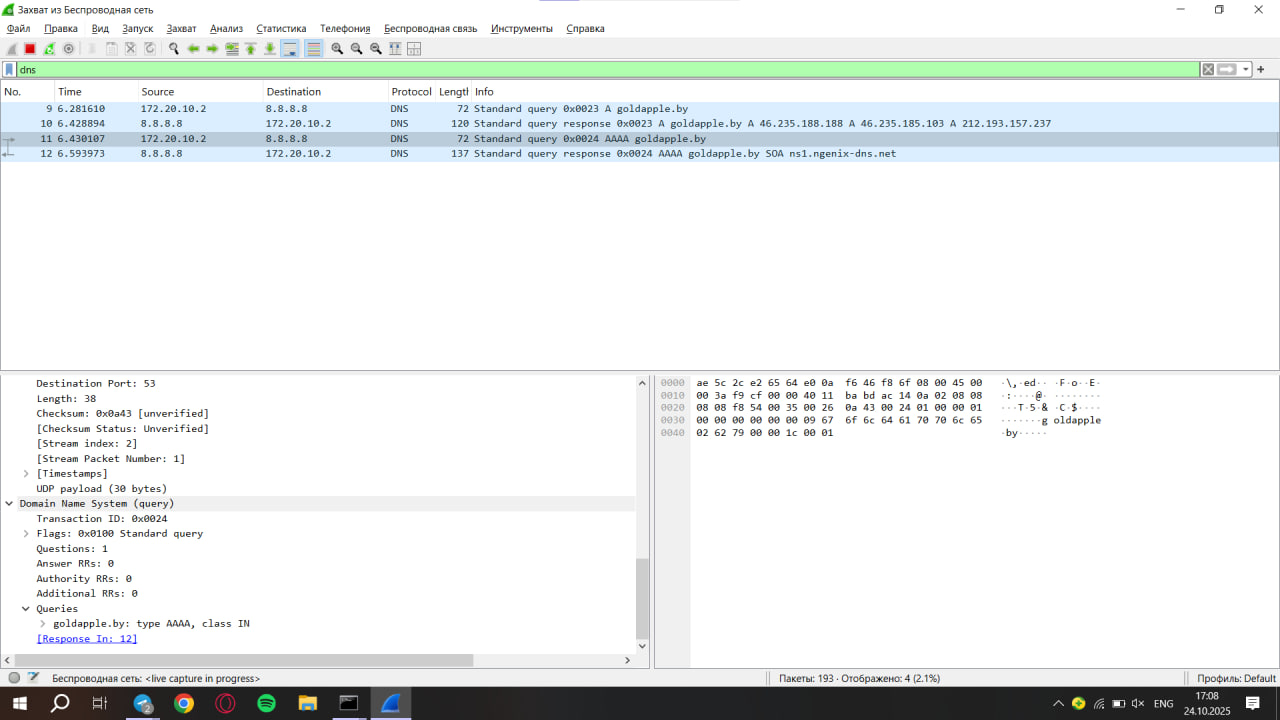
1. **Wildberries.ru**

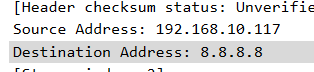


**

**

1. **Goldapple.by**



**