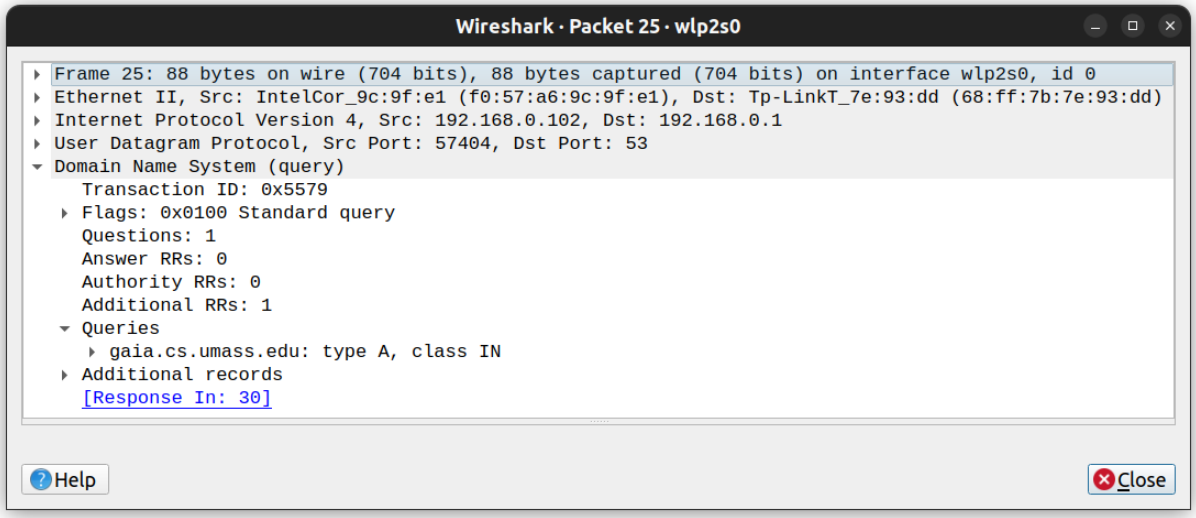
nslookup

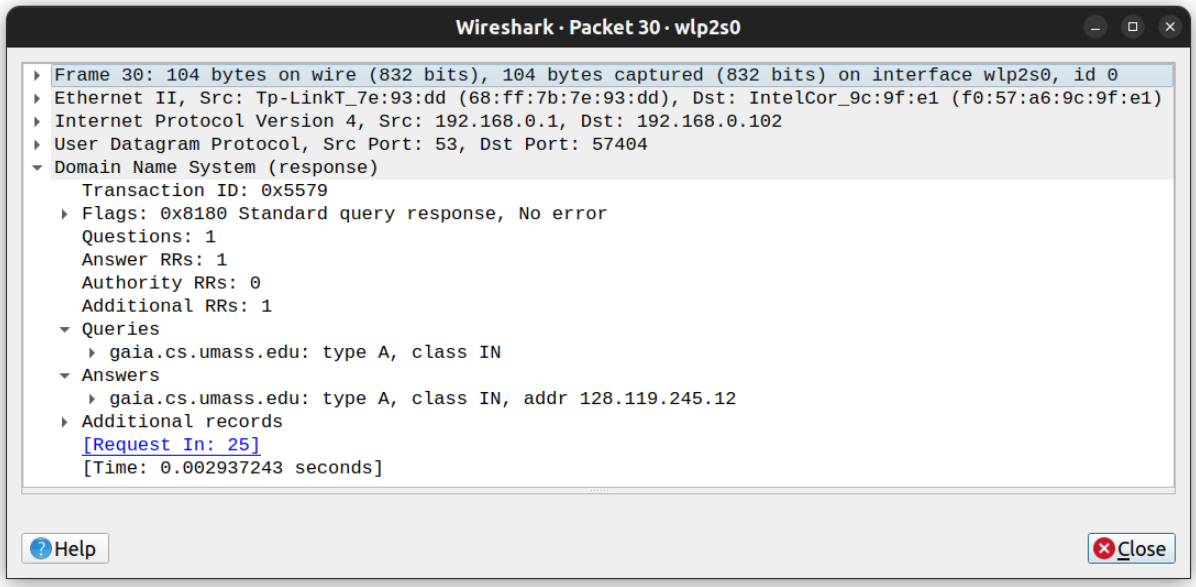
```
ptrvsrg@acer ~ » nslookup iitb.ac.in
Server:           127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
Name: iitb.ac.in
Address: 103.21.124.10

ptrvsrg@acer ~ » nslookup -type=NS iitb.ac.in
Server:           127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
iitb.ac.in  nameserver = dns3.iitb.ac.in.
iitb.ac.in  nameserver = dns2.iitb.ac.in.
iitb.ac.in  nameserver = dns1.iitb.ac.in.

Authoritative answers can be found from:

ptrvsrg@acer ~ »
```

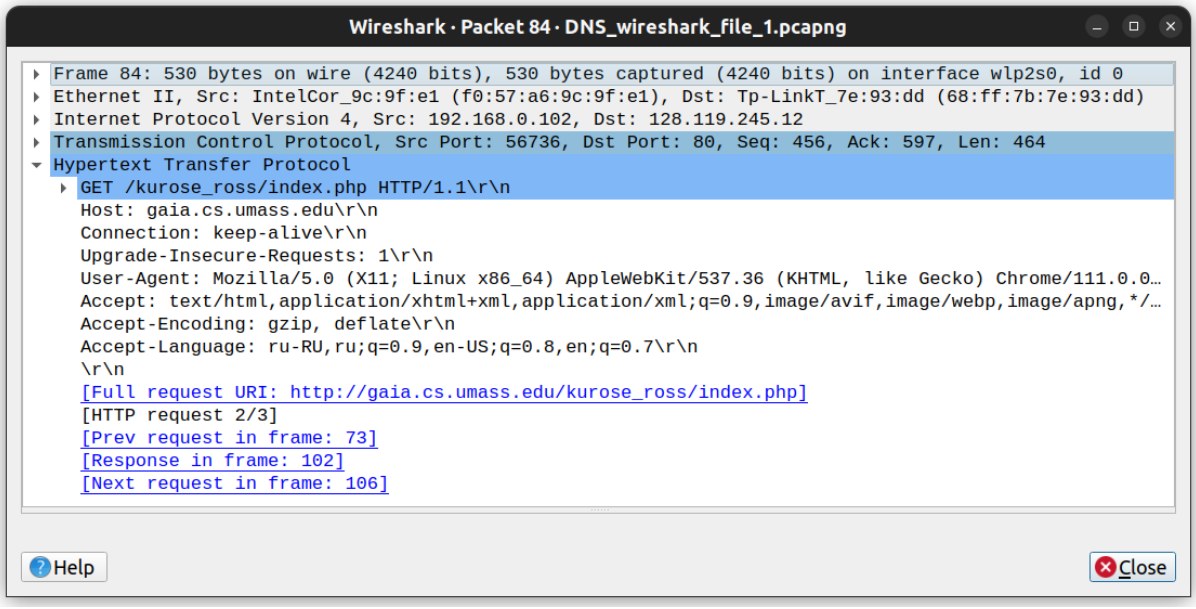
- Запустите nslookup, чтобы получить IP-адрес веб-сервера Индийского технологического института Бомбея: www.iitb.ac.in. Какой IP-адрес у www.iitb.ac.in?
    - 103.21.124.10
- Какой IP-адрес DNS-сервера?
    - 127.0.0.53
- Ответ исходит от авторитетного или не авторитетного DNS-сервера?
    - Не авторитетного
- Используйте nslookup для определения имени авторитетного сервера для домена iit.ac.in. Что это за имя? Если их несколько, какое имя первого авторитетных сервера возвращает nslookup? Если бы вам нужно было найти IP-адрес авторитетного сервера имен, как бы вы это сделали?
    - dns3.iitb.ac.in

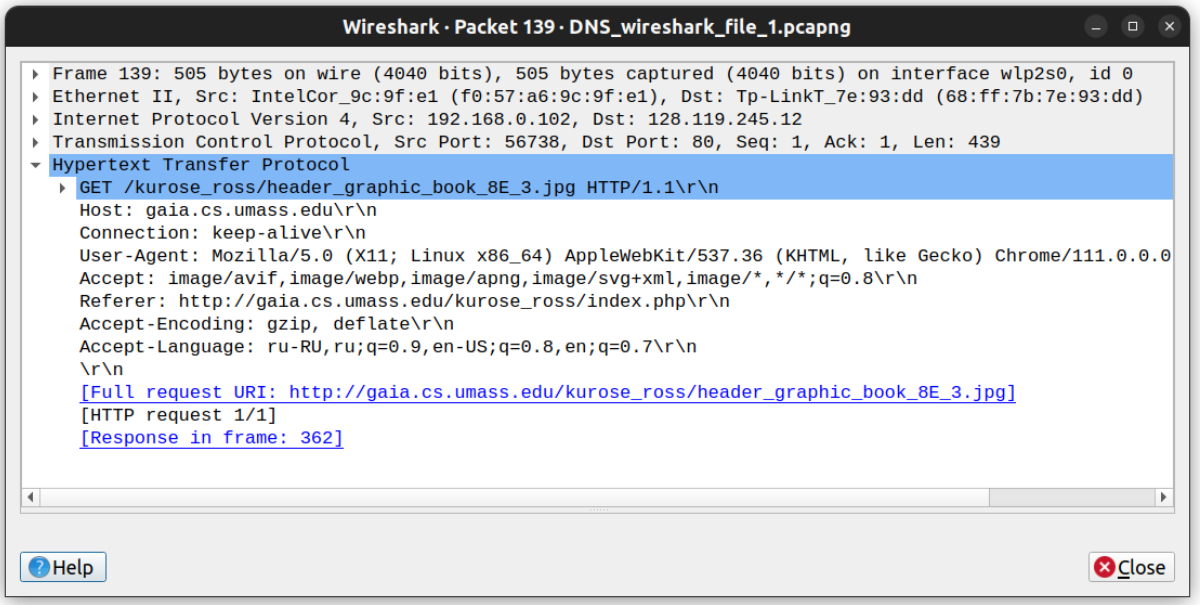
Отслеживание DNS с помощью Wireshark

```
ptrvsrg@acer ~ » sudo systemd-resolve --flush-caches
[sudo] password for ptrvsrg:
```



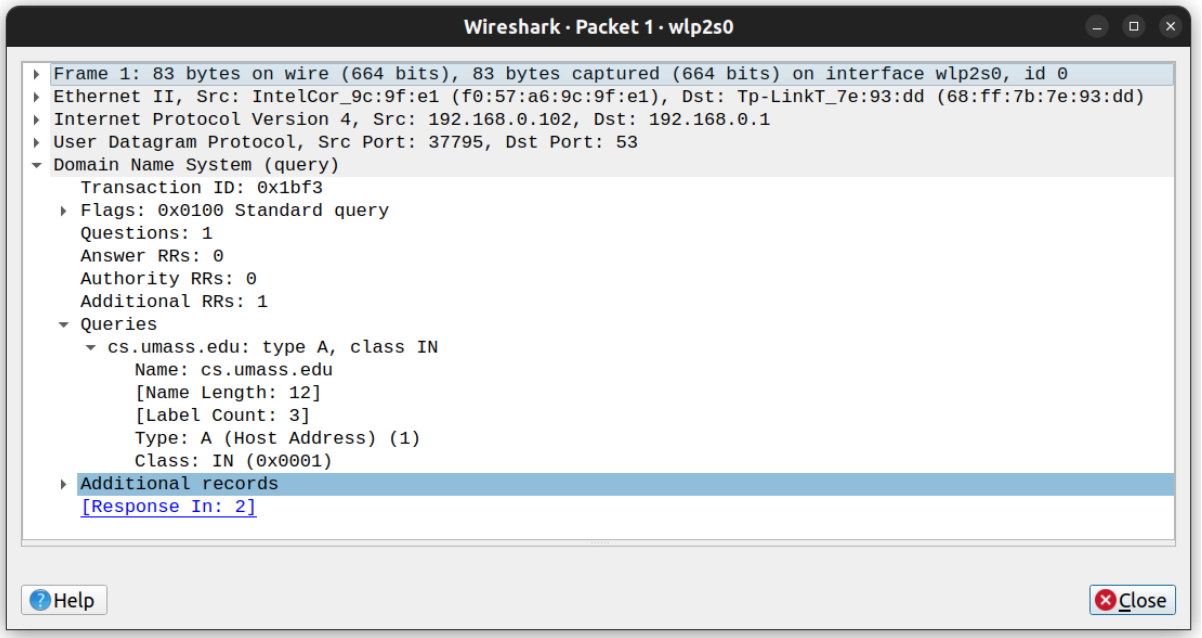


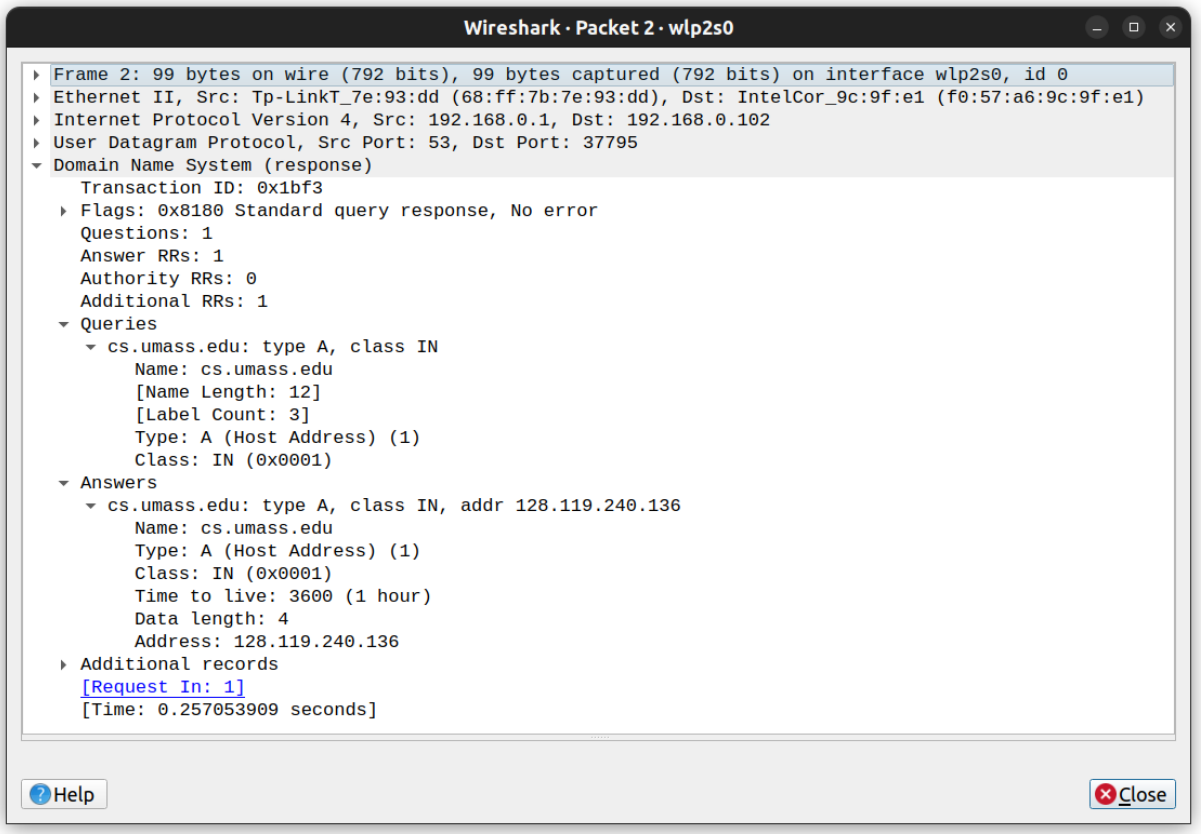




- Найдите первое сообщение запроса DNS, разрешающее имя gaia.cs.umass.edu. Какой номер пакета в трассировке сообщения DNS-запроса? Это сообщение запроса отправлено через UDP или TCP?
    - 25 пакет
    - Сообщение отправлено через UDP
- Теперь найдите соответствующий ответ DNS на исходный запрос DNS. Каков номер пакета в трассировке ответного сообщения DNS? Получено ли это ответное сообщение через UDP или TCP?
    - 30 пакет
    - Сообщение получено через UDP
- Каков порт назначения для сообщения DNS-запроса? Каков исходный порт ответного сообщения DNS?
    - Протокол DNS использует 53 порт протокола UDP
- На какой IP-адрес отправляется сообщение запроса DNS?
    - 192.168.0.1
- Изучите сообщение DNS-запроса. Сколько «вопросов» содержит это DNS-сообщение? Сколько «ответов»?
    - 1 “вопрос”, 0 “ответов”
- Изучите ответное DNS-сообщение. Сколько «вопросов» содержит это DNS-сообщение? Сколько ответов?
    - 1 “вопрос”, 1 “ответов”
- Веб-страница базового файла http://gaia.cs.umass.edu/kurose_ross/ ссылается на объект изображения http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg , который, как и основная веб-страница, находится на gaia.cs.umass.edu. Каков номер пакета в трассировке для исходного HTTP-запроса GET для базового файла? http://gaia.cs.umass.edu/kurose_ross/?
    - 84 пакет
- Какой номер пакета в трассировке DNS-запроса, сделанного для разрешения gaia.cs.umass.edu, чтобы этот первоначальный HTTP-запрос можно было отправить на IP-адрес gaia.cs.umass.edu?
    - 25 пакет
- Какой номер пакета в трассировке полученного ответа DNS?
    - 30 пакет
- Какой номер пакета в трассировке для HTTP-запроса GET для объекта изображения http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg?
    - 13 пакет

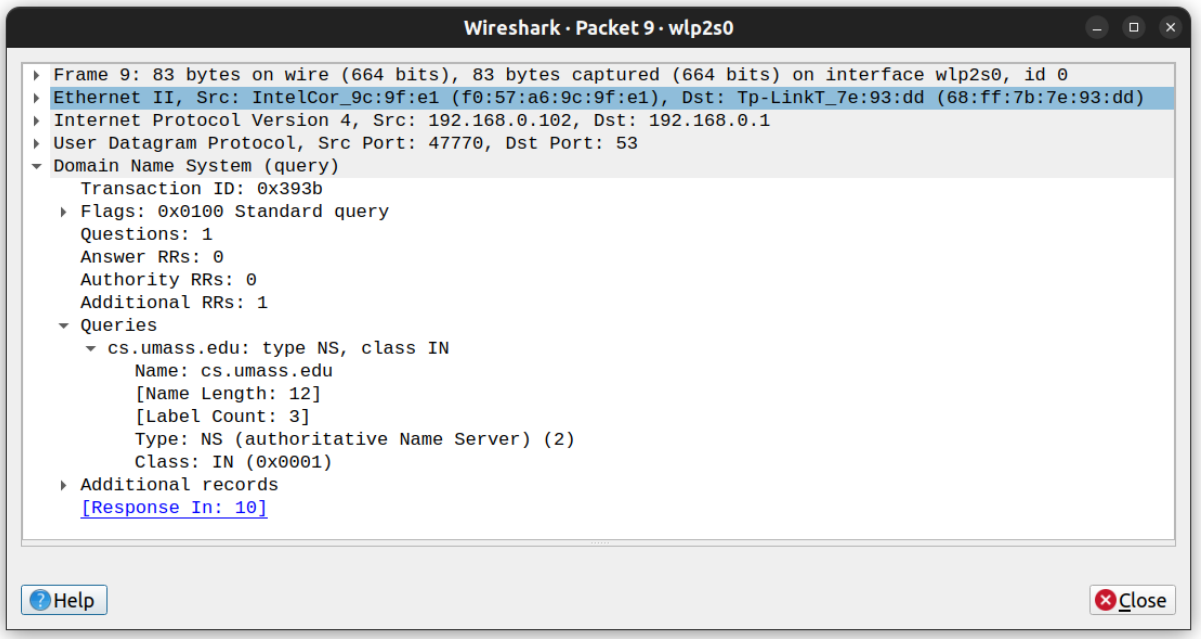
- Какой номер пакета в DNS-запросе используется для разрешения gaia.cs.umass.edu, чтобы этот второй HTTP-запрос можно было отправить на IP-адрес gaia.cs.umass.edu?
    - 25 пакет
- Обсудите, как кэширование DNS влияет на ответ на этот последний вопрос.
    - Благодаря кэшированию не делается DNS-запрос для разрешения IP-адреса gaia.cs.umass.edu, который уже был разрешен и сохранен на локальном DNS-сервере

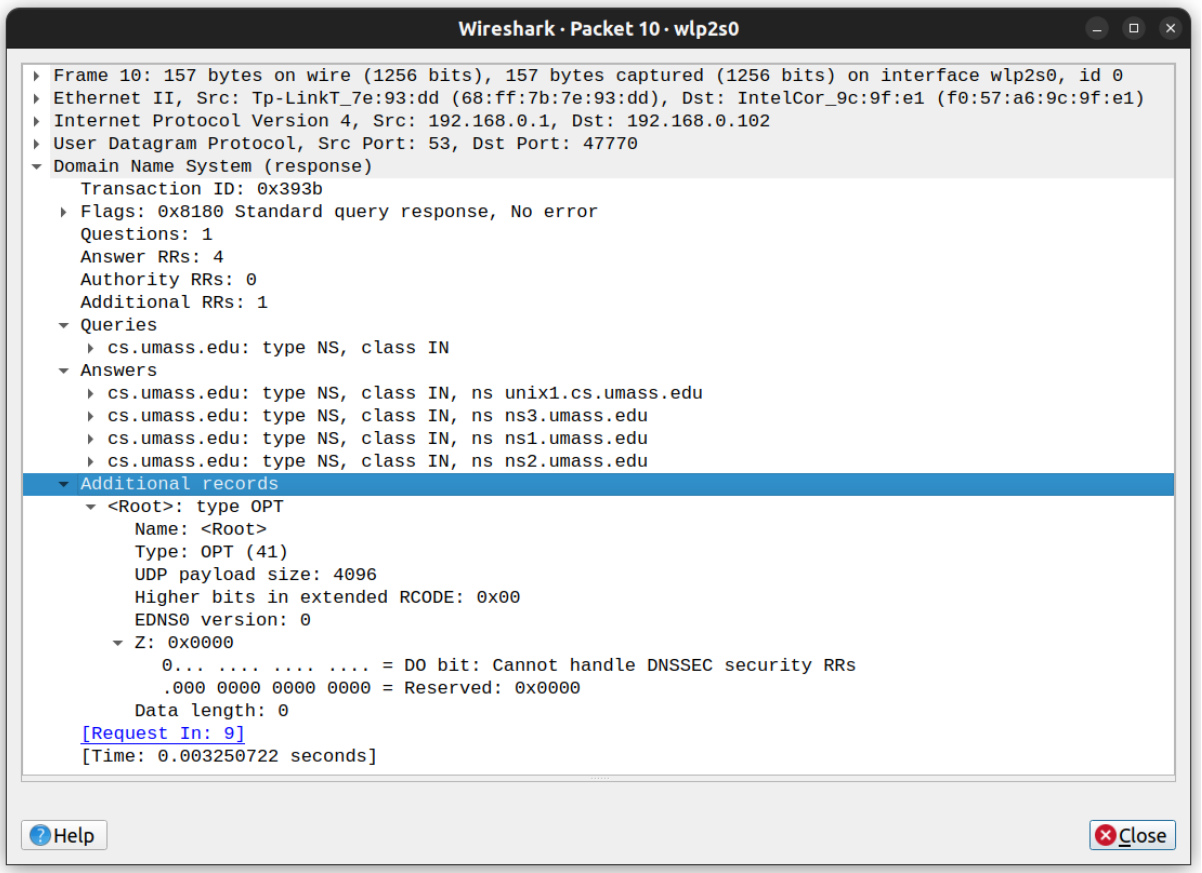




- Сделайте nslookup для сайта cs.umass.edu. Каков порт назначения для сообщения DNS-запроса? Каков исходный порт DNS-ответа?
    - 37795 порт источника
    - 53 порт назначения
- На какой IP-адрес отправляется сообщение запроса DNS? Это IP-адрес вашего локального DNS-сервера по умолчанию?

    - 193.168.0.1 - IP-адрес локального DNS-сервера
- Изучите сообщение запроса DNS. Какой «Тип» DNS-запроса? Содержит ли сообщение запроса какие-либо «ответы»?
    - Тип DNS-запроса - A
    - Не содержит “ответов”
- Изучите ответное сообщение DNS на сообщение запроса. Сколько «вопросов» содержит это ответное сообщение DNS? Сколько «ответов»?
    - 1 “вопрос”, 1 “ответ”





- Используйте nslookup, чтобы выполнить команду, которая вернет DNS-запись типа NS (nslookup -type=NS umass.edu). На какой IP-адрес отправляется сообщение запроса DNS? Это IP-адрес вашего локального DNS-сервера по умолчанию?
    - 192.168.0.1 - IP-адрес локального DNS-сервера

- Изучите сообщение запроса DNS. Сколько вопросов содержит запрос? Содержит ли сообщение запроса какие-либо «ответы»?
    - 1 “вопрос”, 0 “ответов”
- Изучите ответное сообщение DNS. Сколько ответов содержит ответ? Какая информация содержится в ответах? Сколько дополнительных ресурсных записей возвращается? Какая дополнительная информация содержится в этих дополнительных записях ресурсов?
    - 1 “вопрос”, 4 “ответ”
    - 1 дополнительная ресурсная запись