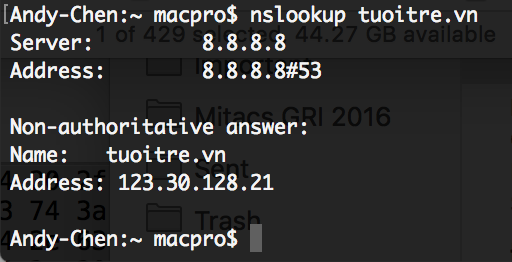
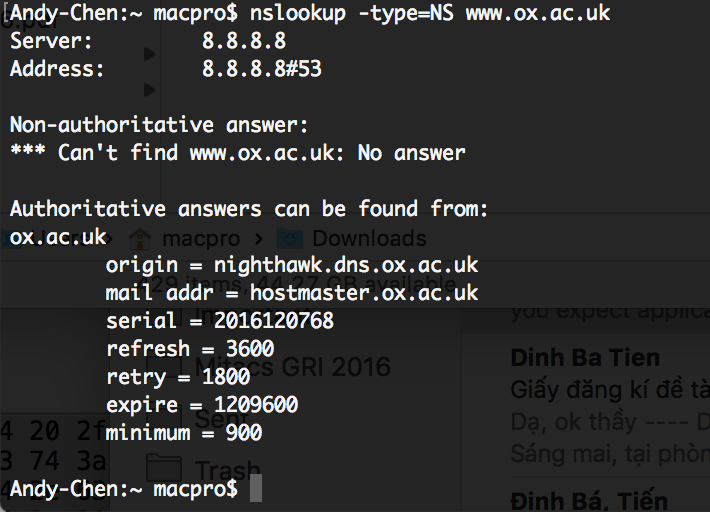
**Wireshark DNS**

1. **Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?**

Target web server is tuoitre.vn

The IP address is 123.30.128.21

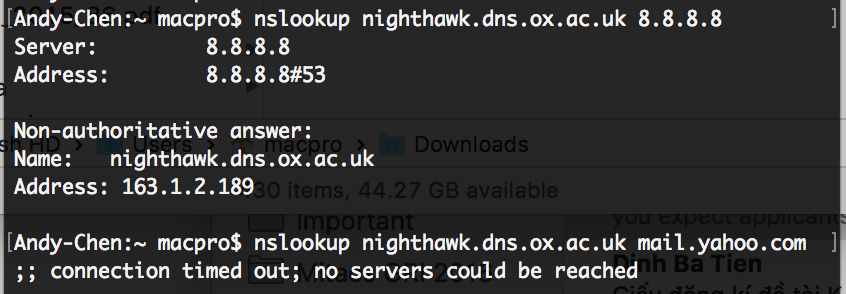
1. **Run nslookup to determine the authoritative DNS servers for a university in Europe.**

Target web server is www.ox.ac.uk

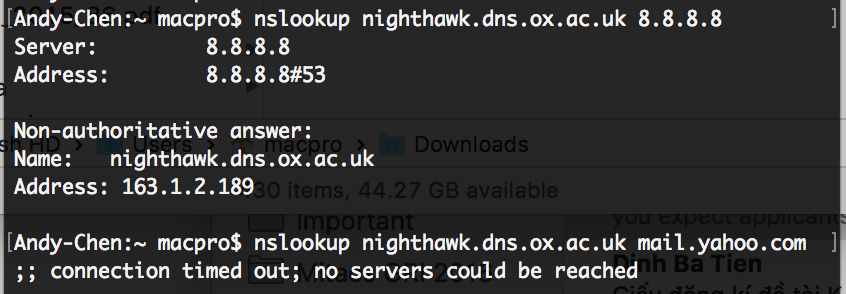
The authoritative DNS server is nighthawk.dns.ox.ac.uk

1. **Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?**

Selected DNS server of Oxford University: nighthawk.dns.ox.ac.uk

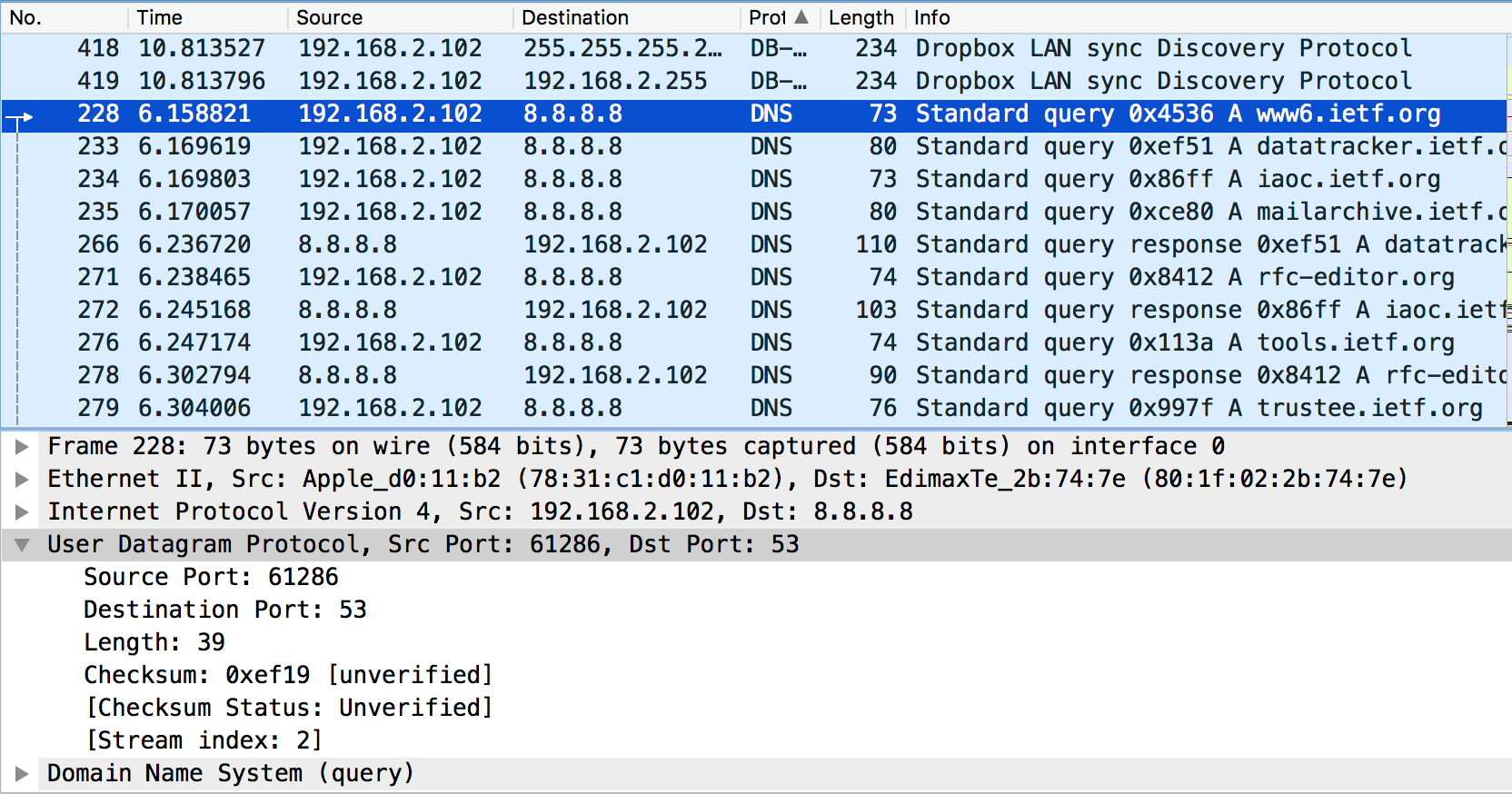


I did not get any result from **mail.yahoo.com**. Thus, I use **8.8.8.8** (Google DNS server) instead.



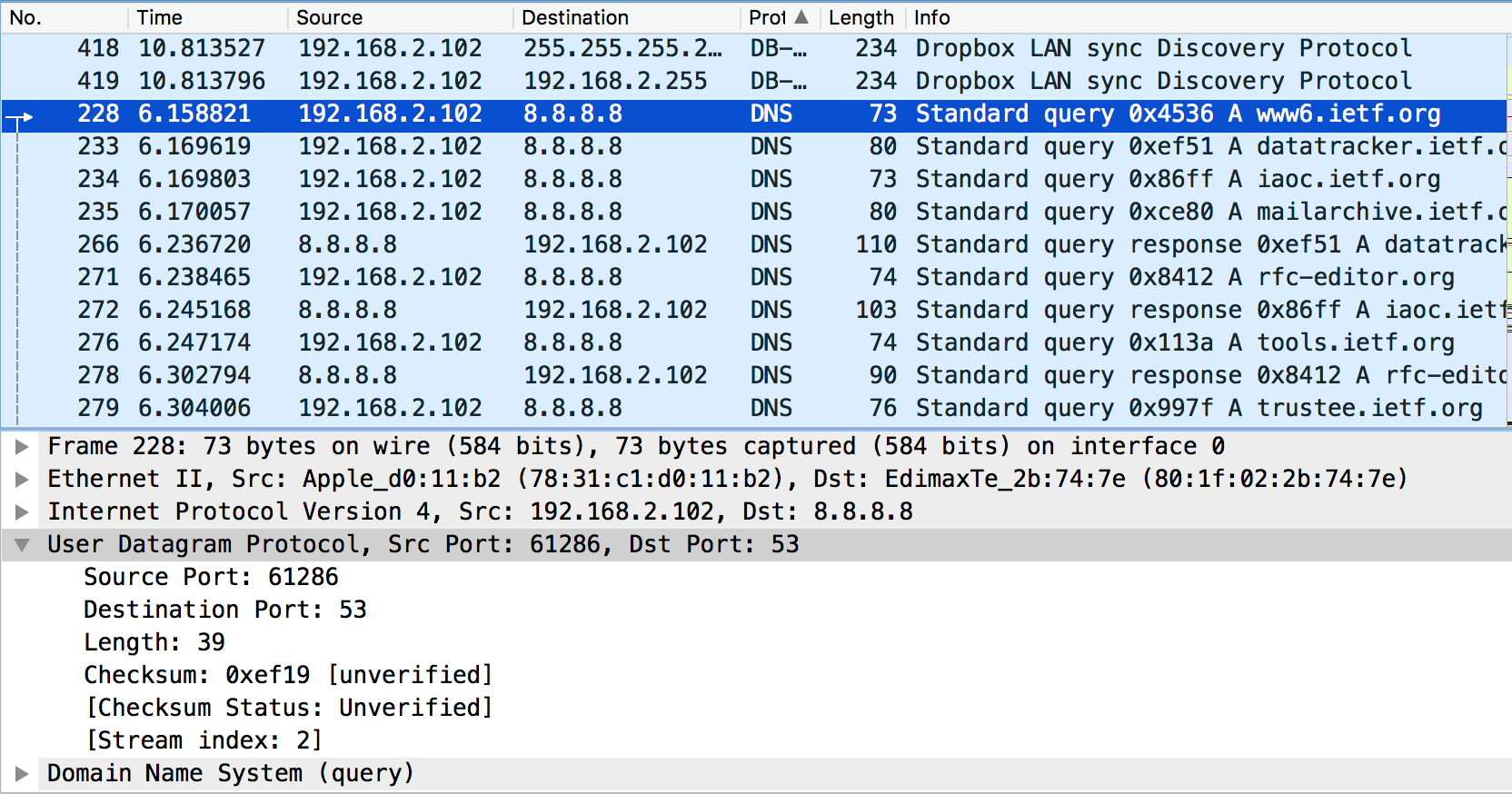
The IP address is **163.1.2.189**

1. **Locate the DNS query and response messages. Are then sent over UDP or TCP?**

****

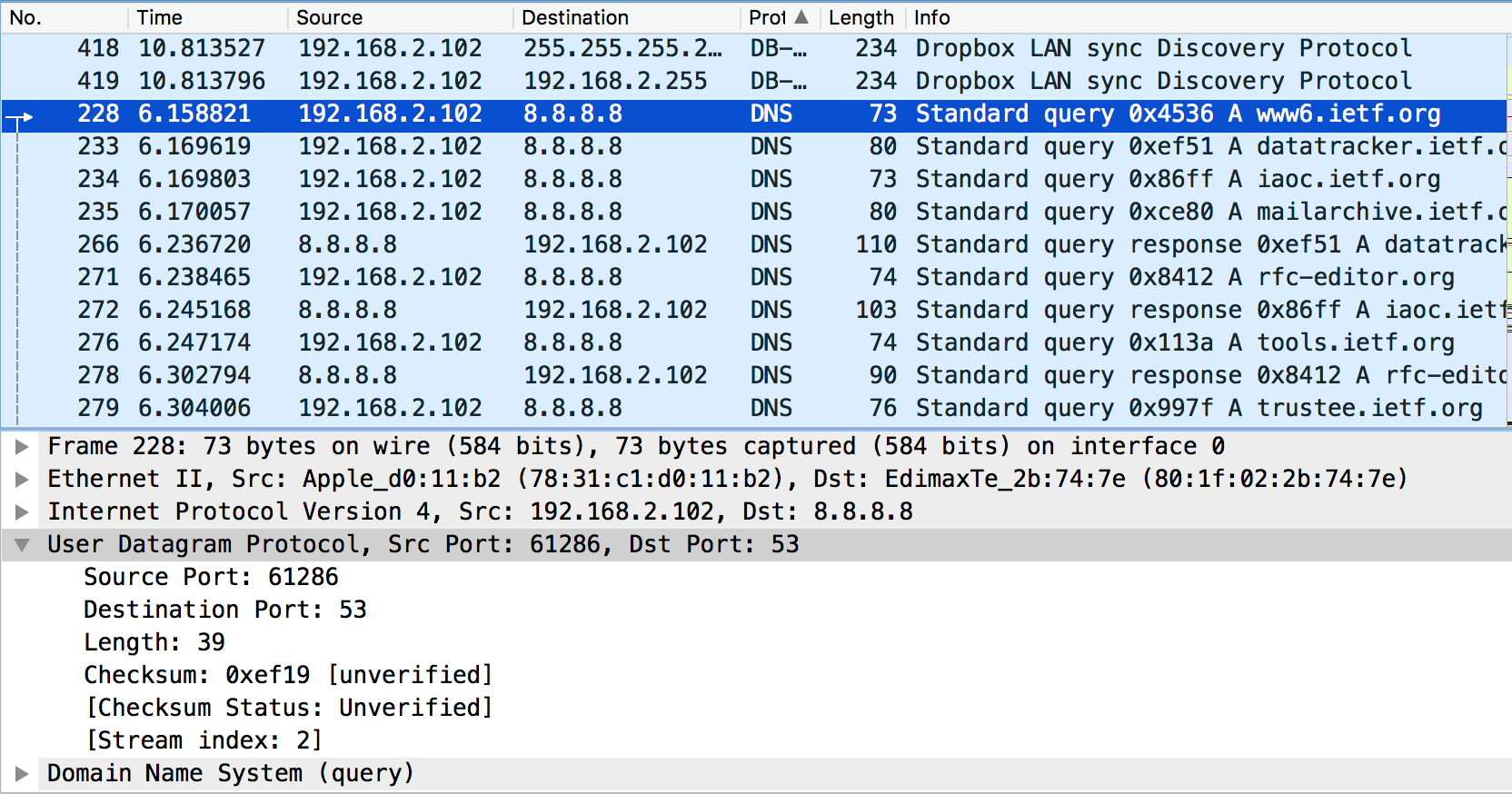
Sent over **UDP**

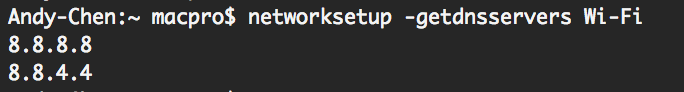
1. **What is the destination port for the DNS query message? What is the source port of DNS response message?**

****

Destination port: 53

Source port: 61286

1. **To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?**

**** The DNS query message was sent: 8.8.8.8

(There is no command like ipconfig /displaydns on macOS)

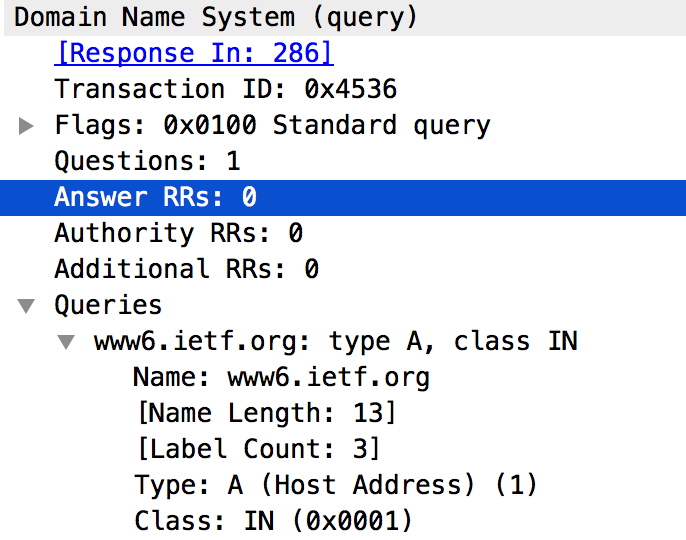
Local DNS server IP: 8.8.8.8 or 8.8.4.4

* The two IP addresses are the same

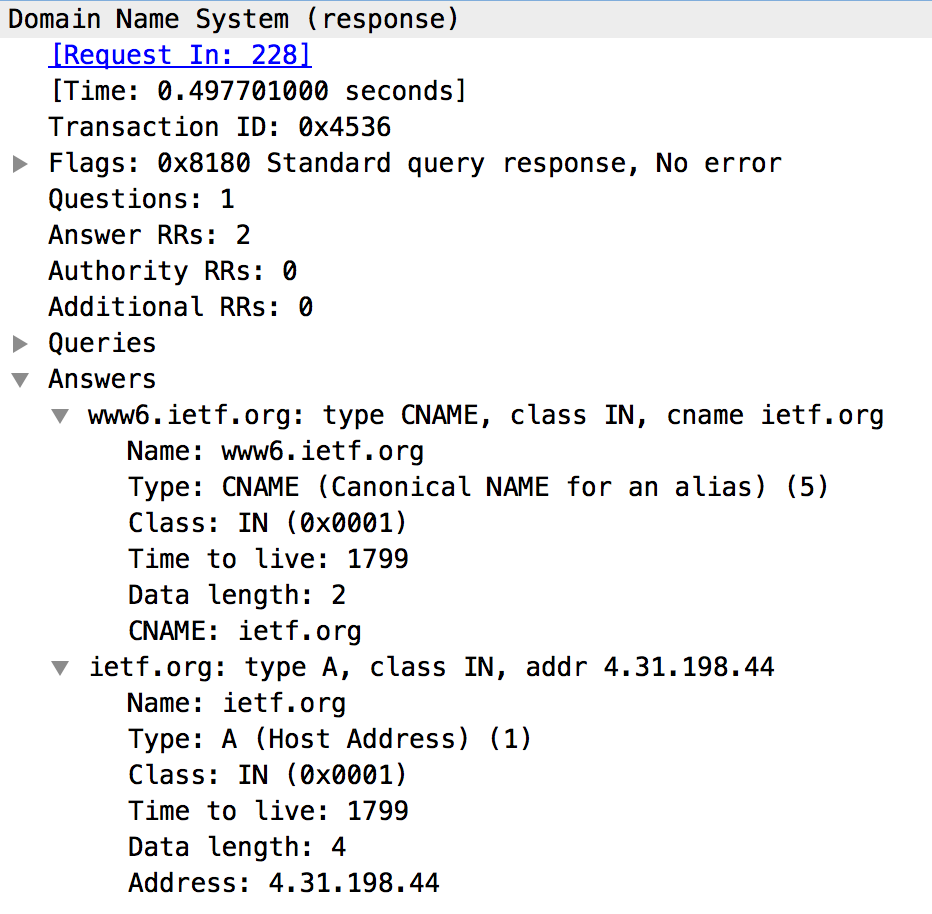
1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

Type of DNS query: A

It does not contain any “answers”.

****

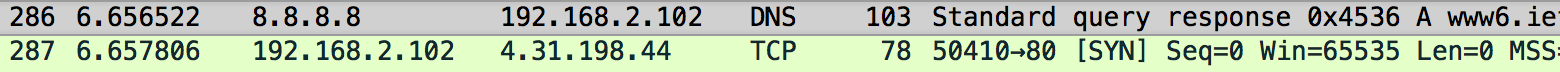
1. **Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?**

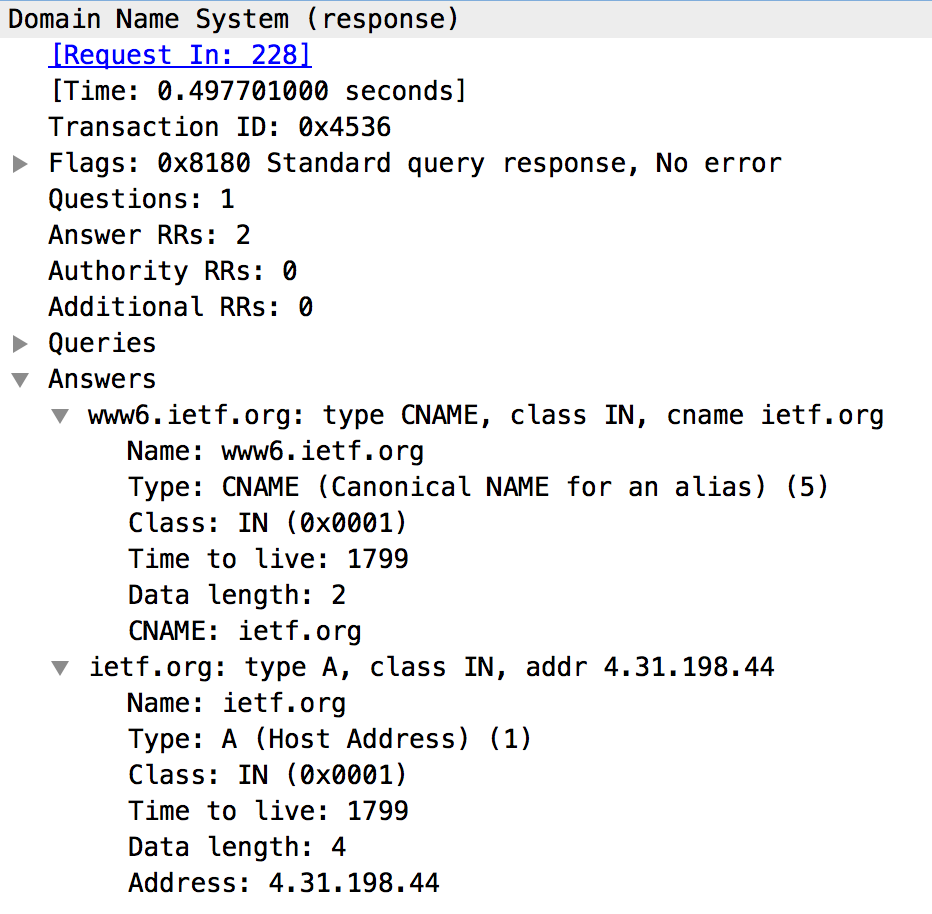
****

There are 2 answers:

* + The 1st one contains the Canonical name of the queried website, the Class, Type of Answer, TTL, Data length.
  + The 2nd one contains the Host Name and IP address of the queried website, the Class, Type of Answer, TTL, Data length.

1. **Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**

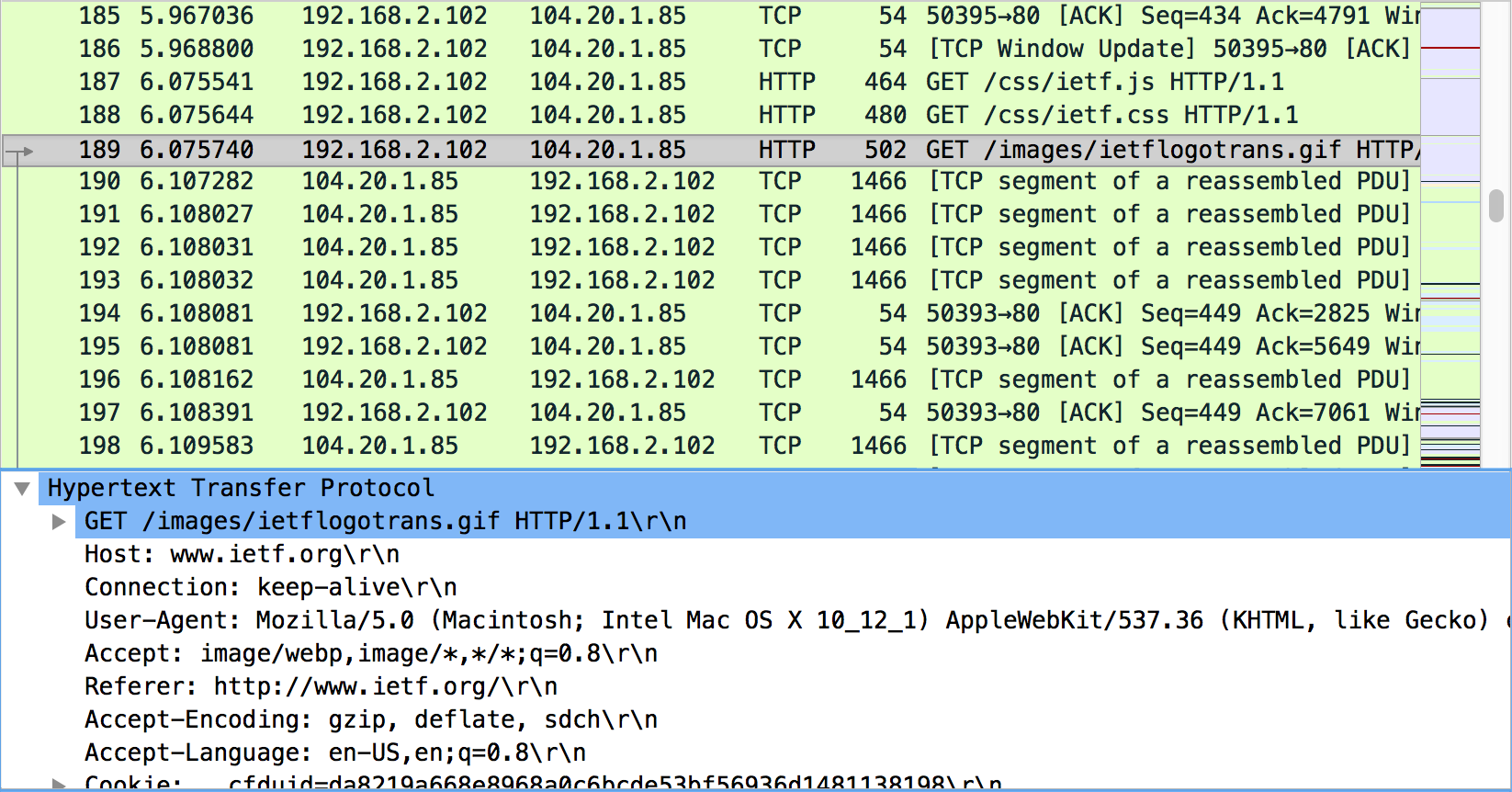
****

****The destination IP address of the subsequent TCP SYN (of the DNS response message): **4.31.198.44**

The IP address of the 2nd answer from DNS response message: **4.31.198.44**

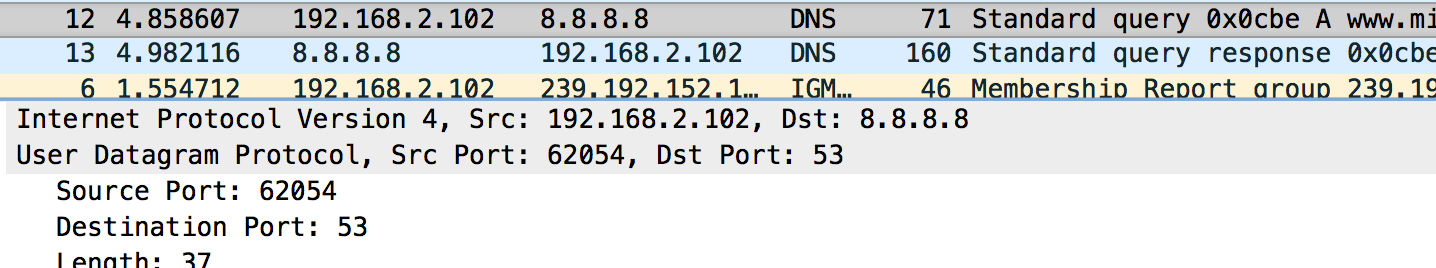
* The destination IP address of the SYN packet correspond to one of the IP addresses provided in the DNS response message

1. **This web page contains images. Before retrieving each image, does your host issue new DNS queries?**

****

* No, the images are all loaded from www.ietf.org, so no additional DNS queries are necessary (the host uses a cached address).

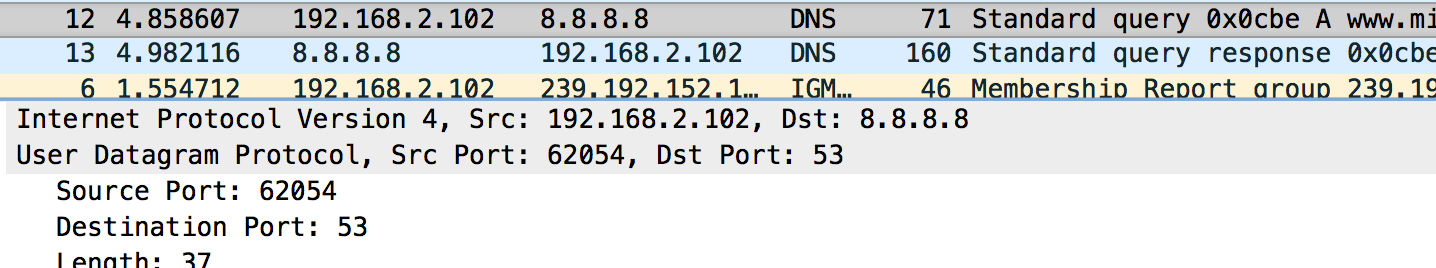
1. **What is the destination port for the DNS query message? What is the source port of DNS response message?**

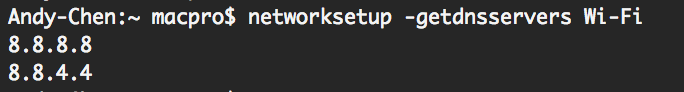
****

Source port: 62054

Destination port: 53

1. **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**

****

**** It sends to 8.8.8.8

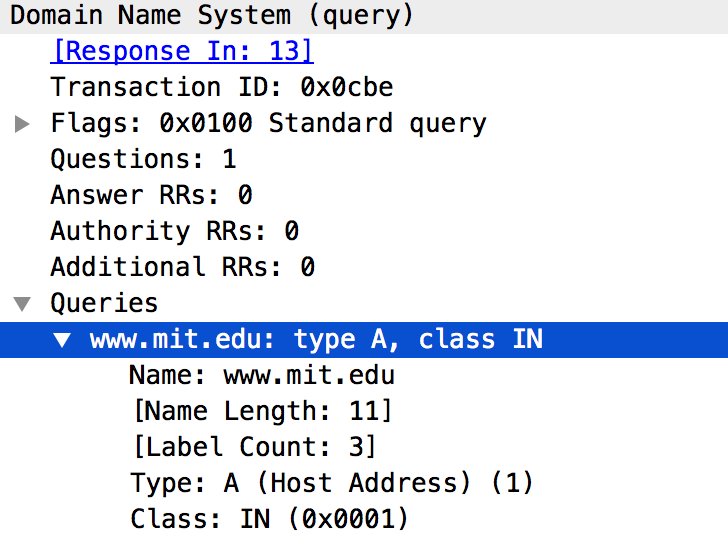
My local DNS server: 8.8.8.8

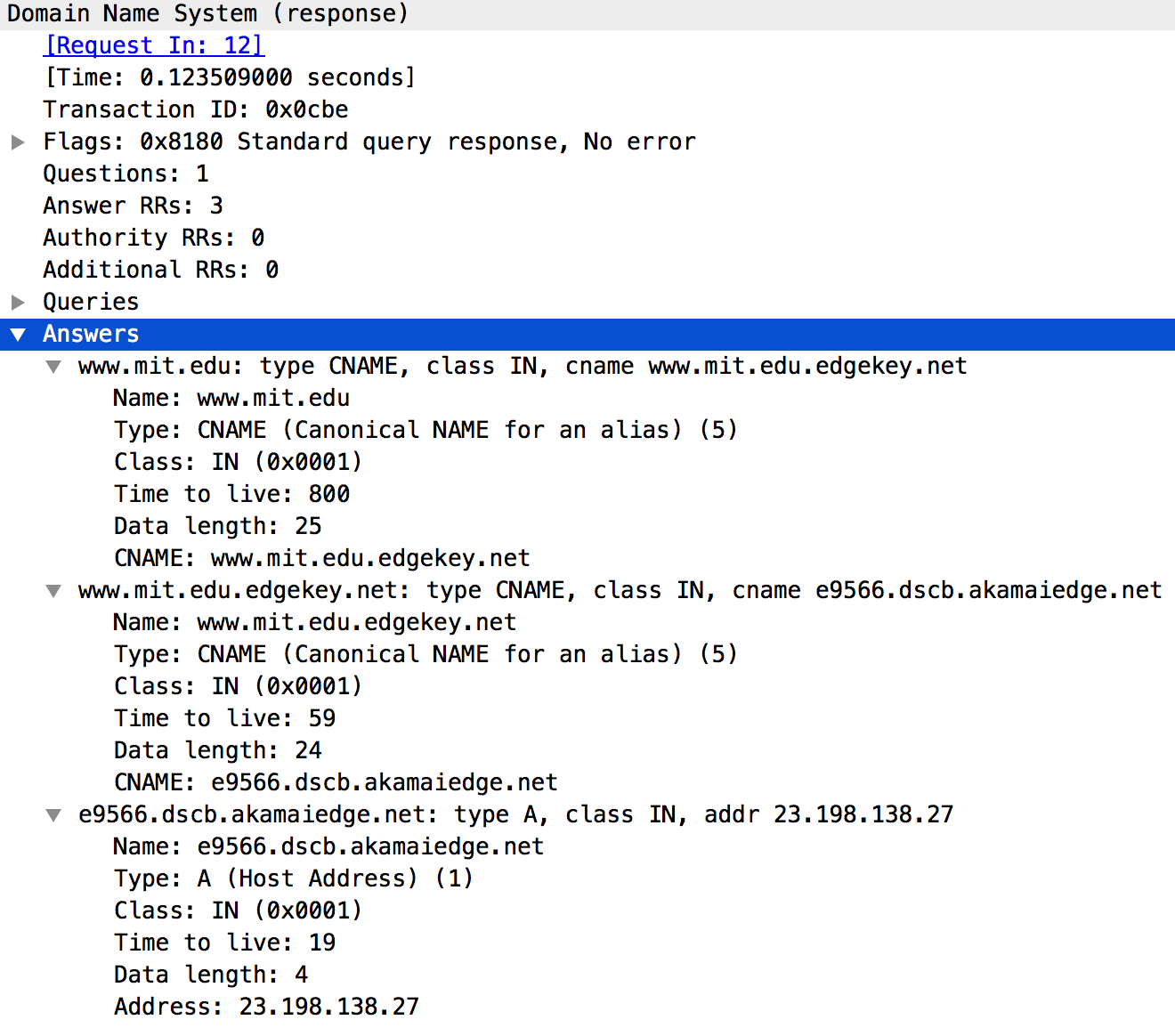
* The 2 IP addresses are the same

1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

Type of DNS query: A

It does not contain any “answers”.

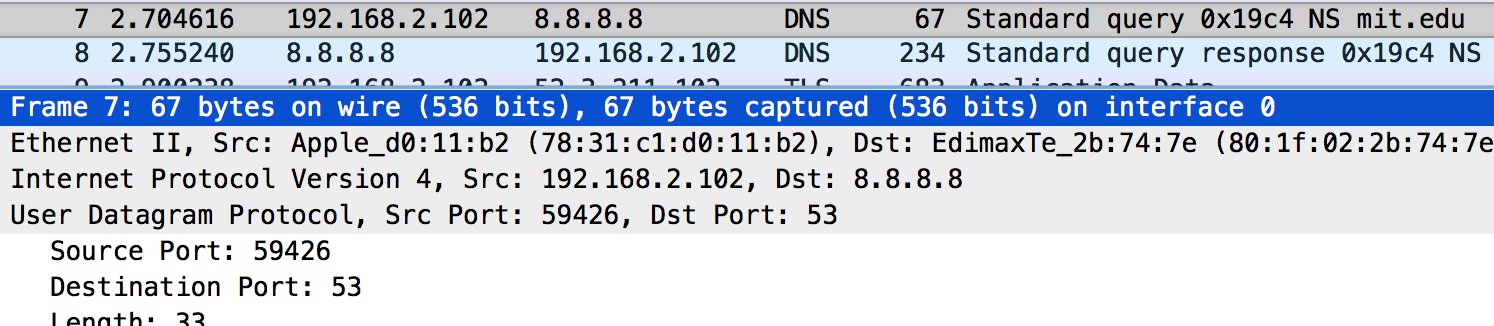


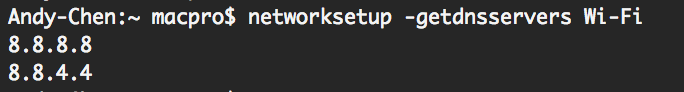
1. **Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?**

There are 3 answers:

* + The 1st and the 2nd ones contain the Canonical Name of the queried website, the Class, Type of Answer, TTL, Data length.
  + The 3rd one contains the Host Name and IP address of the queried website, the Class, Type of Answer, TTL, Data length.

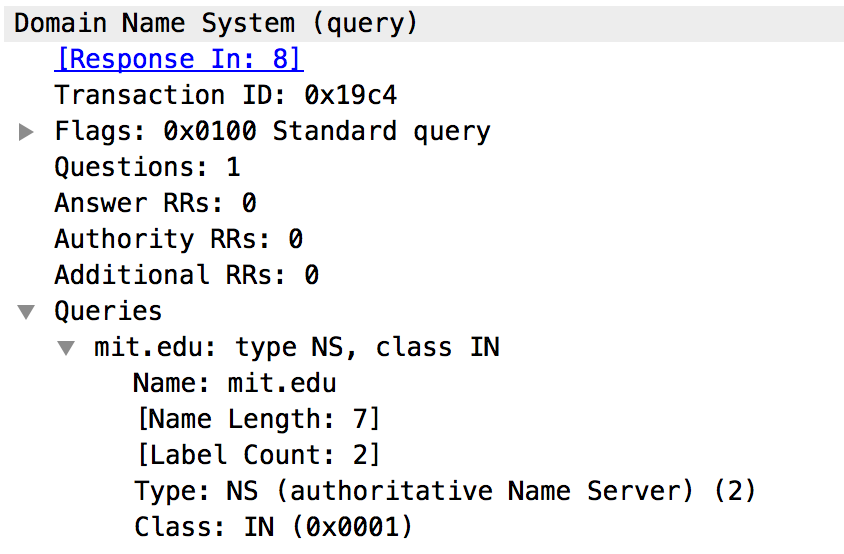
1. **Provide a screenshot.**
2. **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**

****

****It sends to 8.8.8.8

My local DNS server: 8.8.8.8

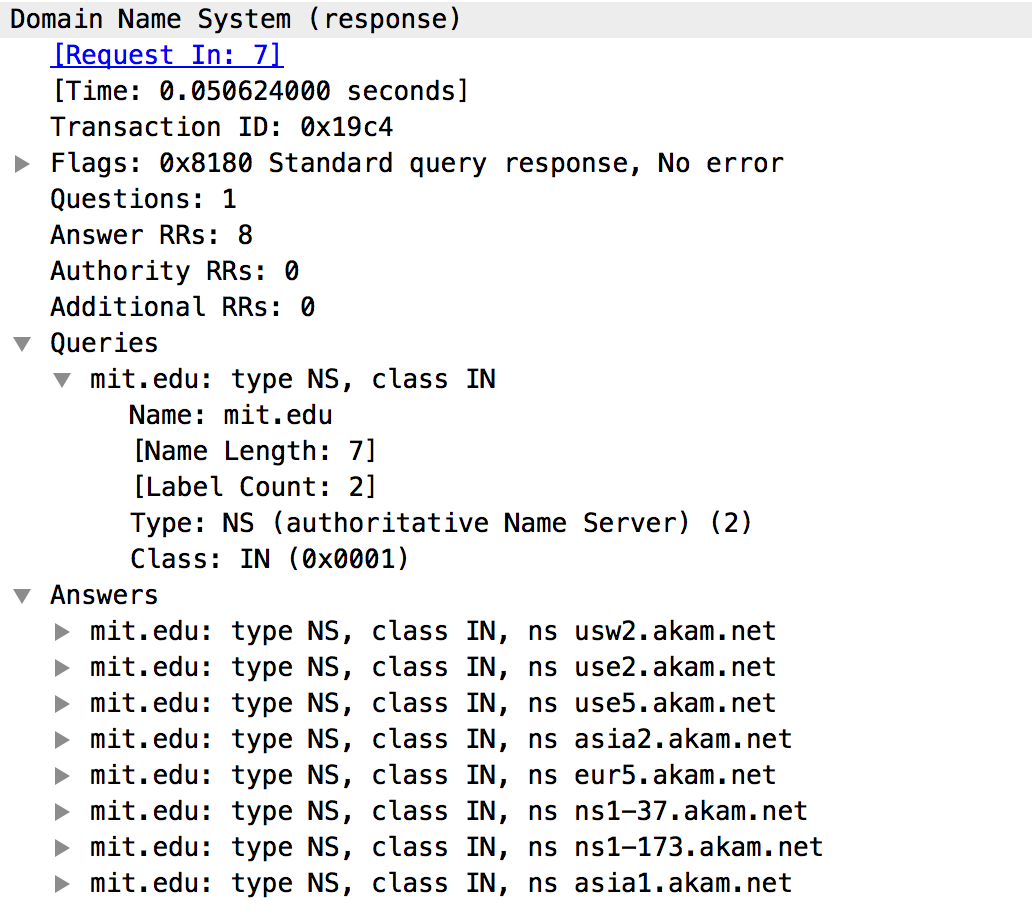
* The 2 IP addresses are the same

1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

Type of DNS query: NS

It does not contain any “answers”.

1. **Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?**

****

It provides 6 nameservers as shown in the **Answers**

It does not provide the IP address of the MIT nameservers.

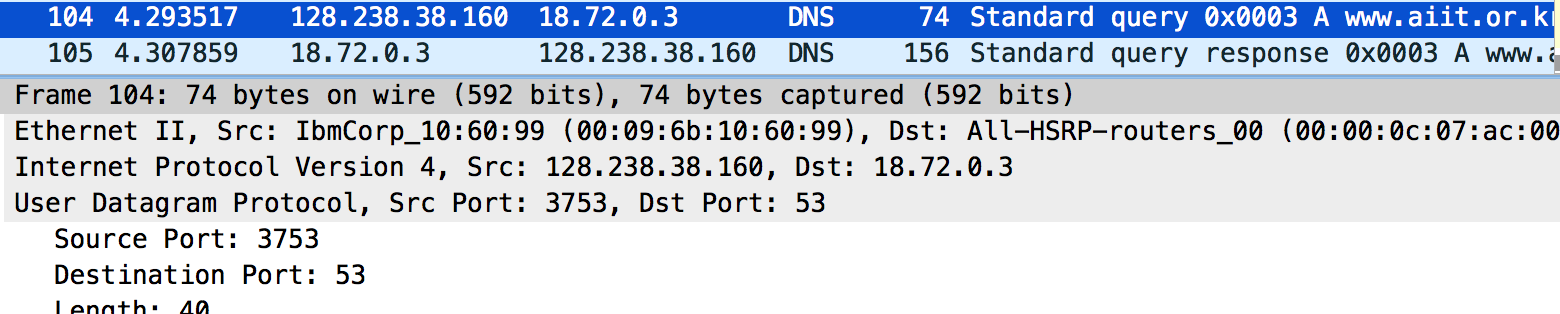
1. **Provide a screenshot.**

**I cannot perform:**

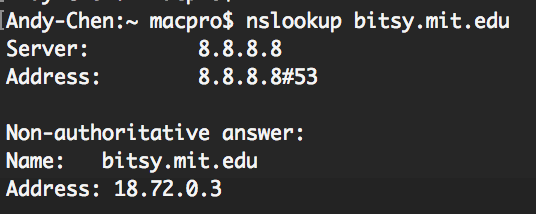
nslookup www.aiit.or.kr bitsy.mit.edu

**on my computer. Thus the following answers will be based on the trace file from another computer.**

1. **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?**

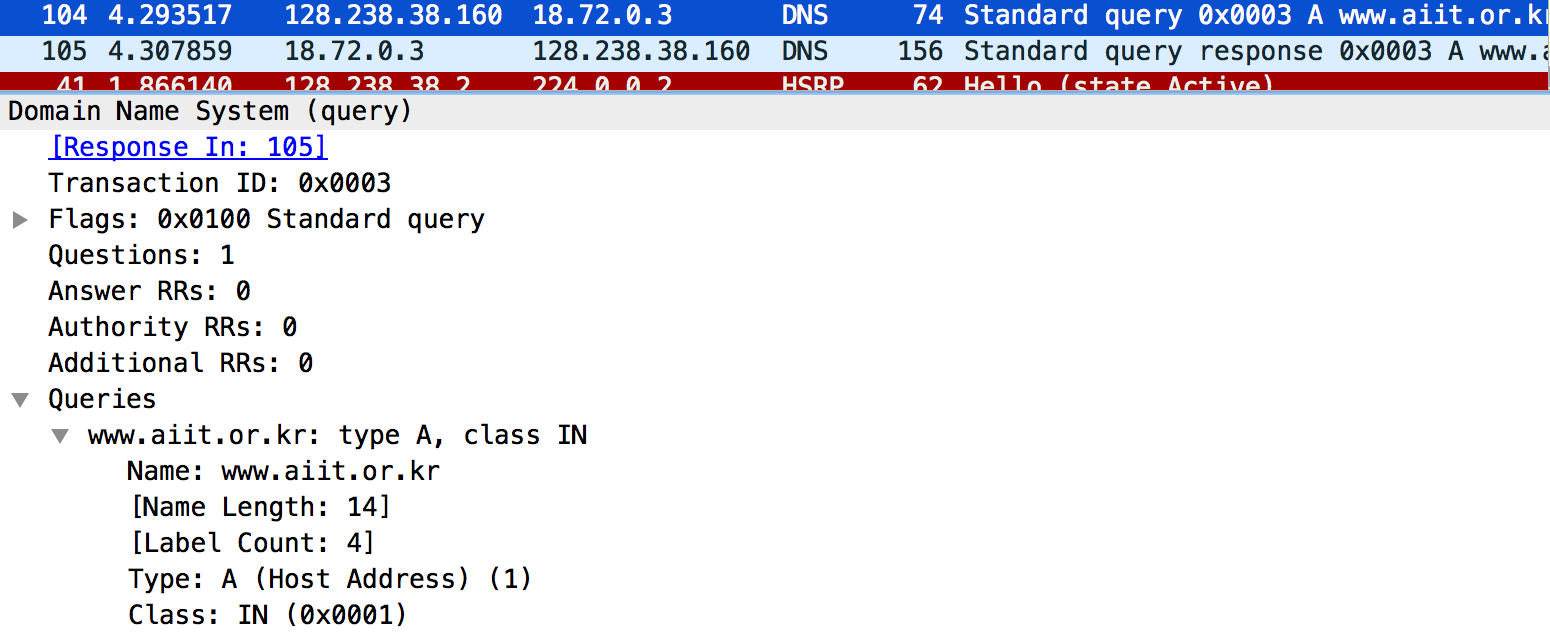
****

It sends to IP address: 18.72.0.3, which is not my default local DNS server (in the case of the trace file).



Instead, it corresponds to the IP address of bitsty.mit.edu

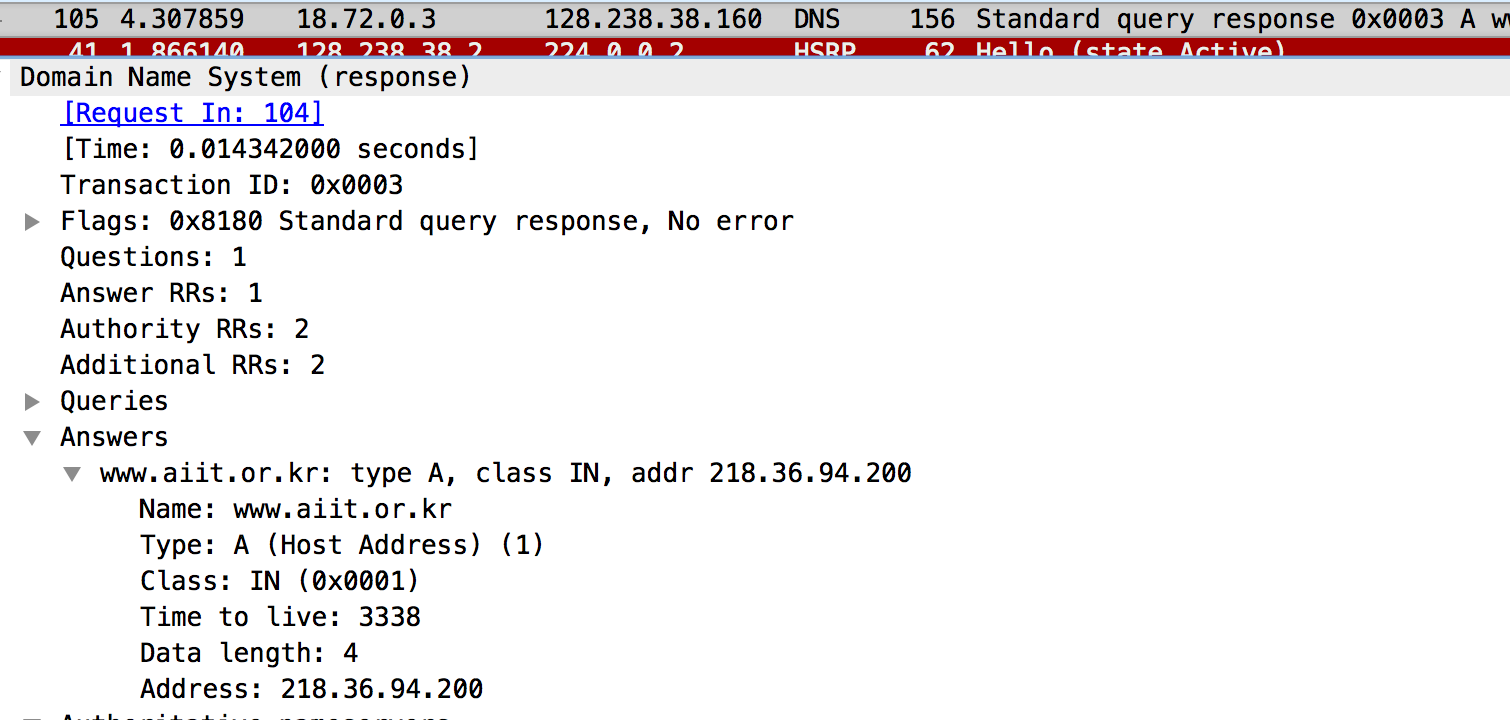
1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

****

Type: A

The message contains no answer.

1. **Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?**

****

It contains 1 answer. The answer contains the Host Name and the IP address, TTL, Data length, Class, Type.

1. **Provide a screenshot.**