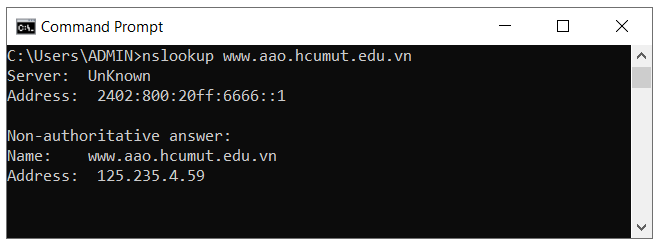
**LAB 2B**

**Wireshark DNS v8.0**

**Name: Hồ Đức Trí**

**Student No: 1912288**

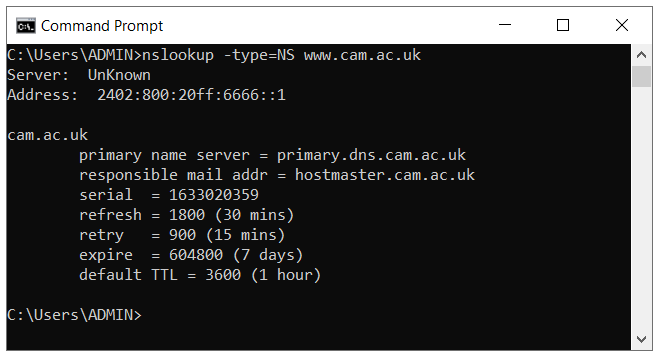
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?



Web server: [www.aao.hcmut.edu.vn](http://www.aao.hcmut.edu.vn)

IP address: 125.235.4.59

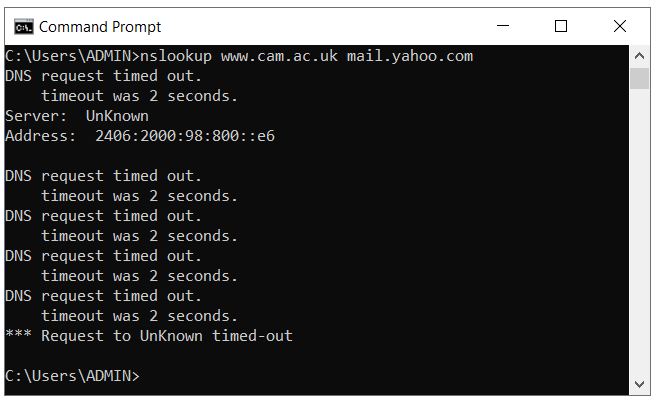
1. Run nslookup to determine the authoritative DNS servers for a university in Europe.



Web server: [www.cam.ac.uk](http://www.cam.ac.uk) (University of Cambridge)

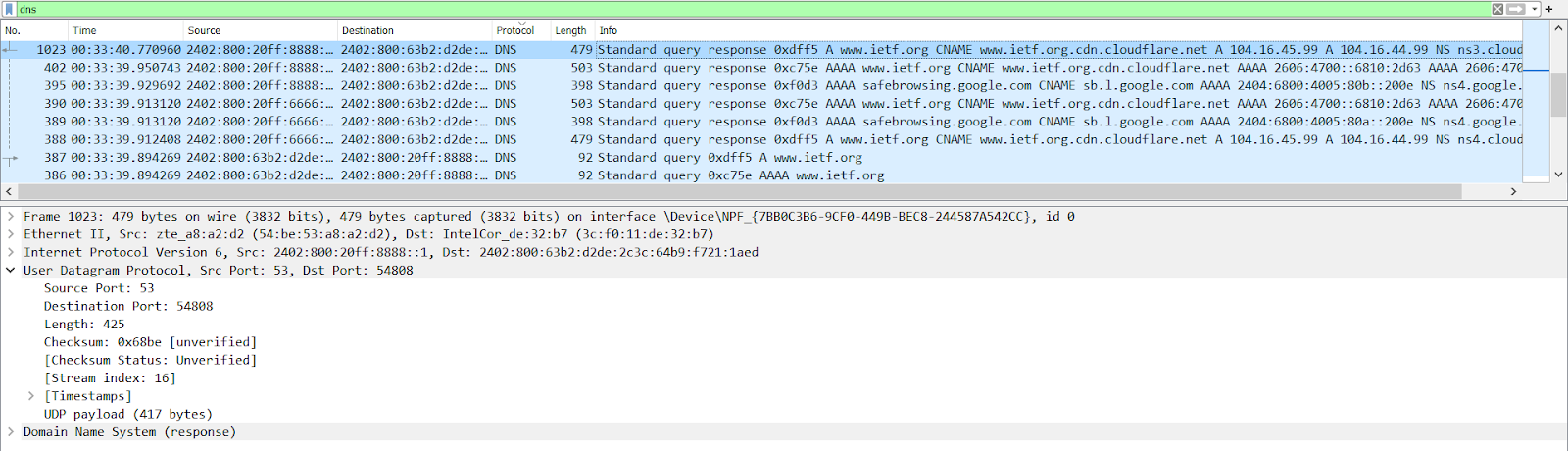
The authoritative DNS server: primary.dns.cam.ac.uk

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?



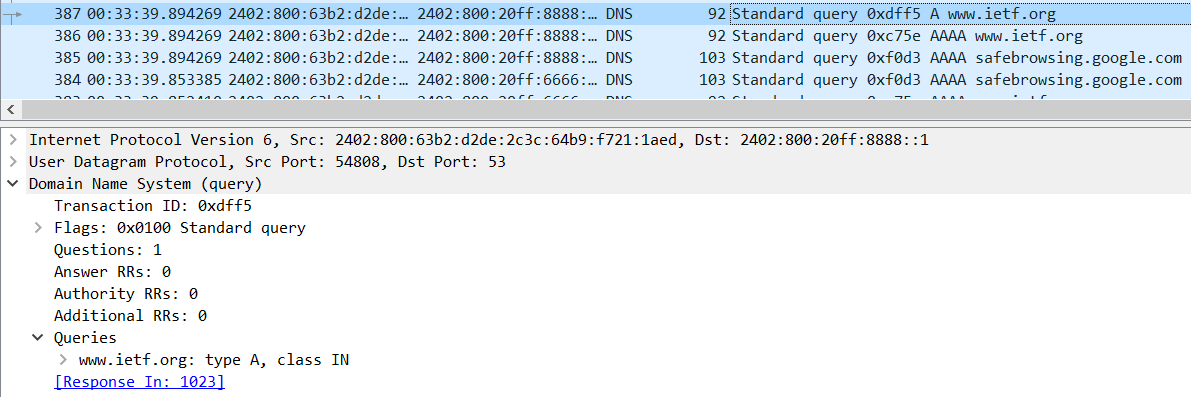
Its IP address: 2406:2000:98:800::e6

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



The DNS query and response message are sent over UDP

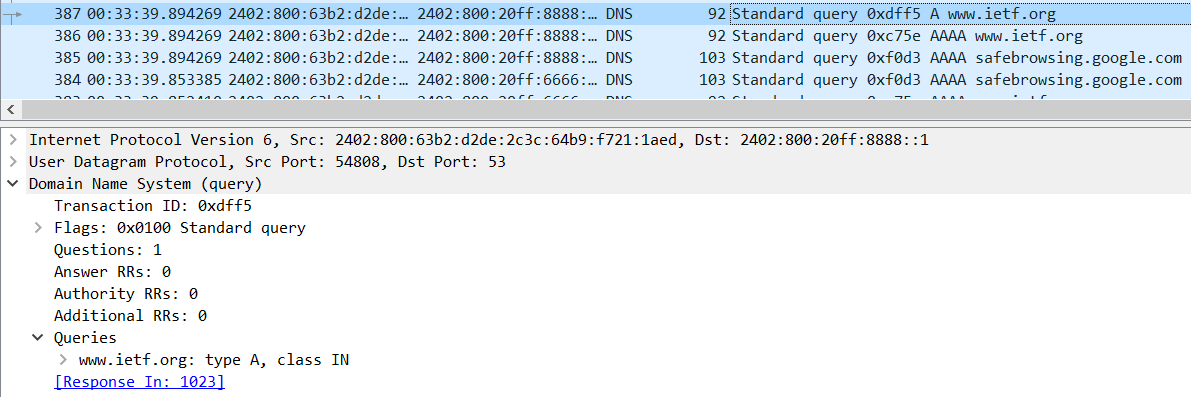
1. What is the destination port for the DNS query message? What is the source port of DNS response message?



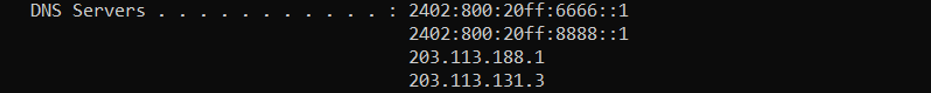
Destination port: 53

Source port: 54808

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?

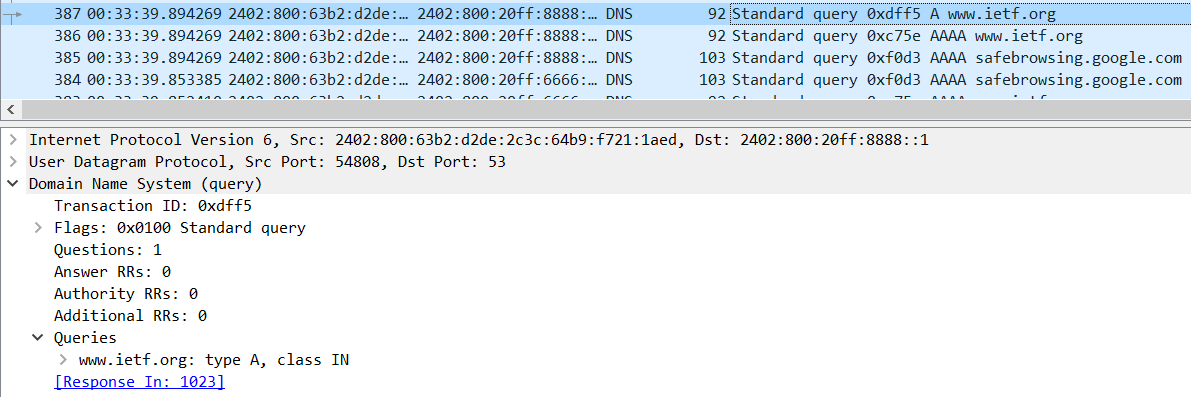


IP address the DNS query message sent to: 2402:800:20ff:8888::1



IP address of my local DNS server is: 2402:800:20ff:8888::1. So yes, they are the same.

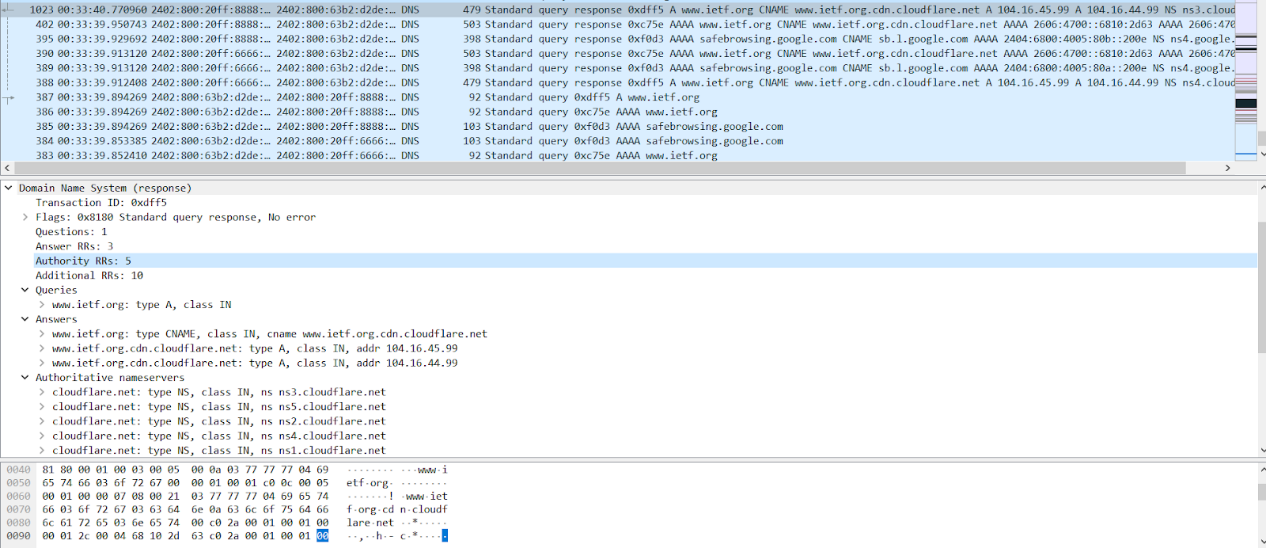
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



Type of DNS query: A

No, the query message does not contain any answer

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



3 answers are provided

They contain answers to the query: nameservers, address

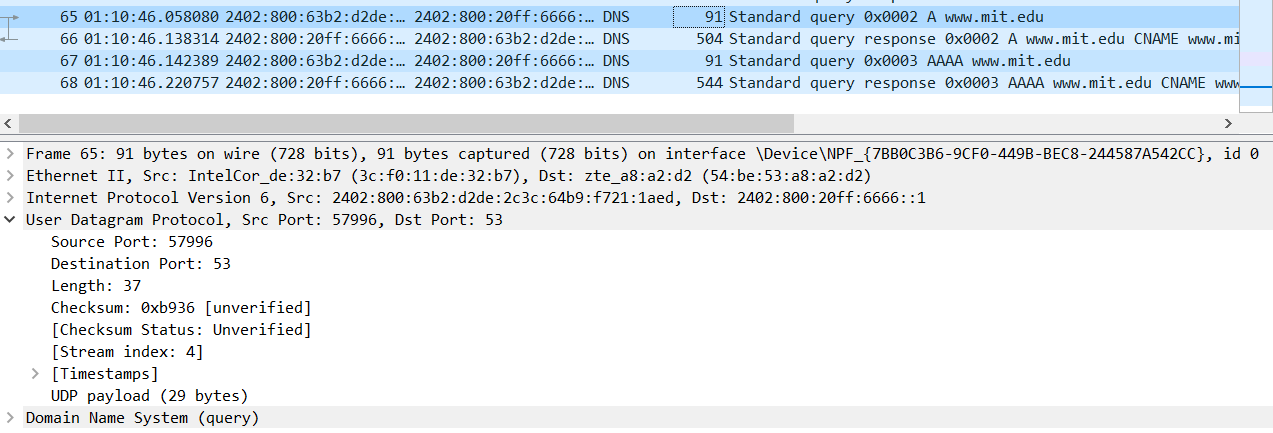
1. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

No, it does not

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

No, it does not

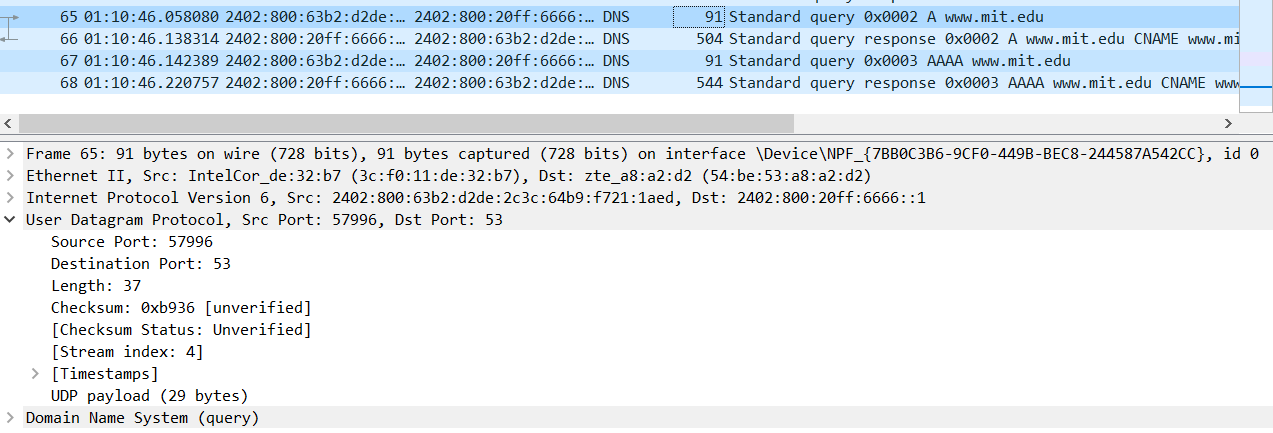
1. What is the destination port for the DNS query message? What is the source port of DNS response message?



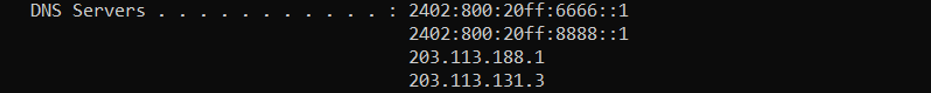
Destination port: 53

Source port: 57996

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

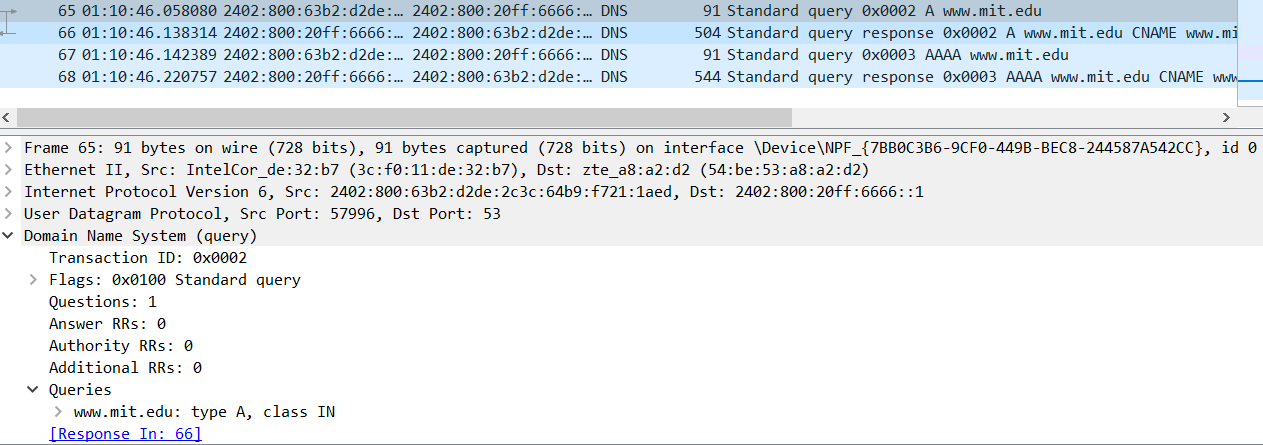


IP address the DNS query message sent to: 2402:800:20ff:6666::1



Yes, it is the IP address of my default local DNS server

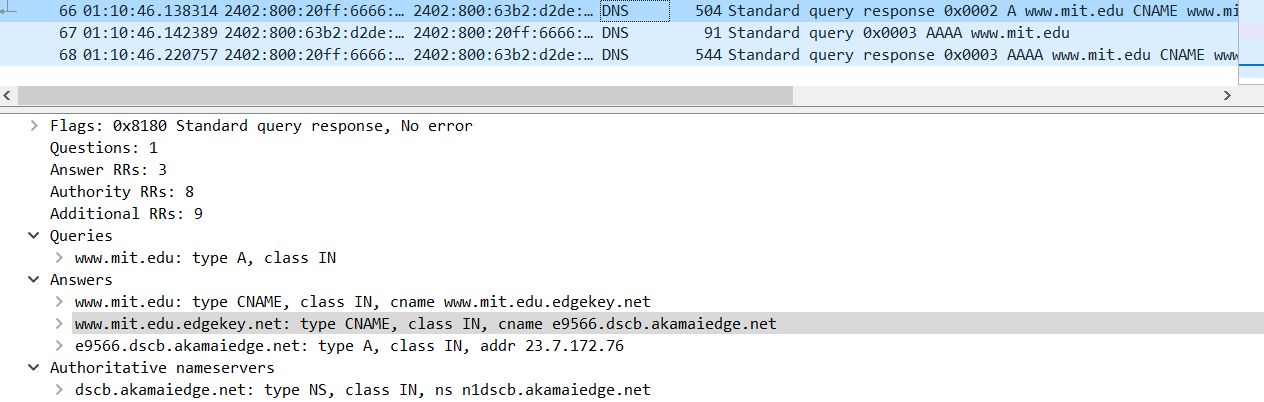
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



Type of DNS query: A

No, the query message does not contain any answer

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



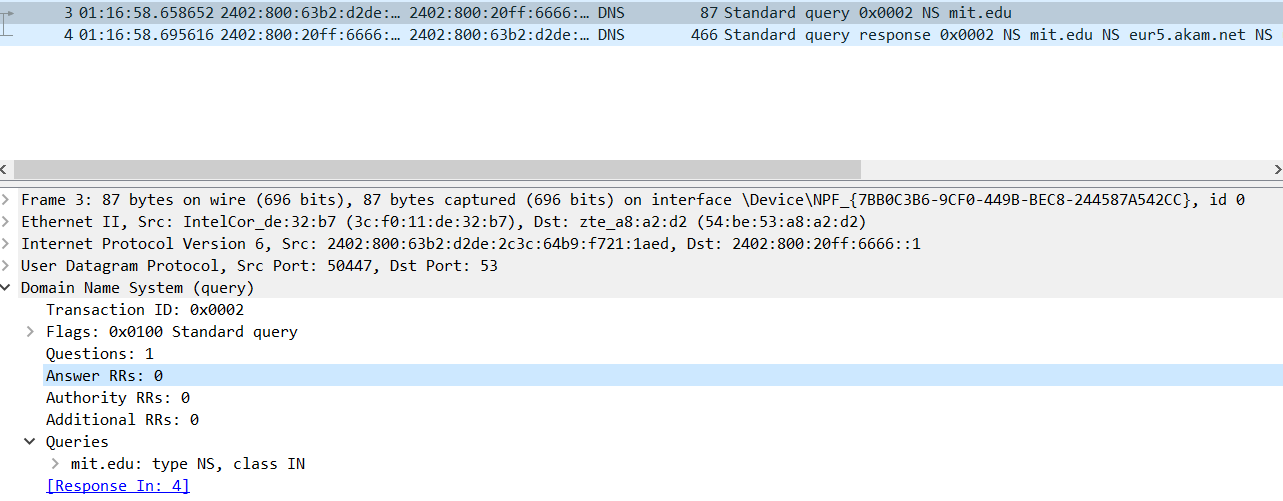
3 answers are provided

They contain the answers for the query: nameservers, address

1. Provide a screenshot.

They are provided in each question

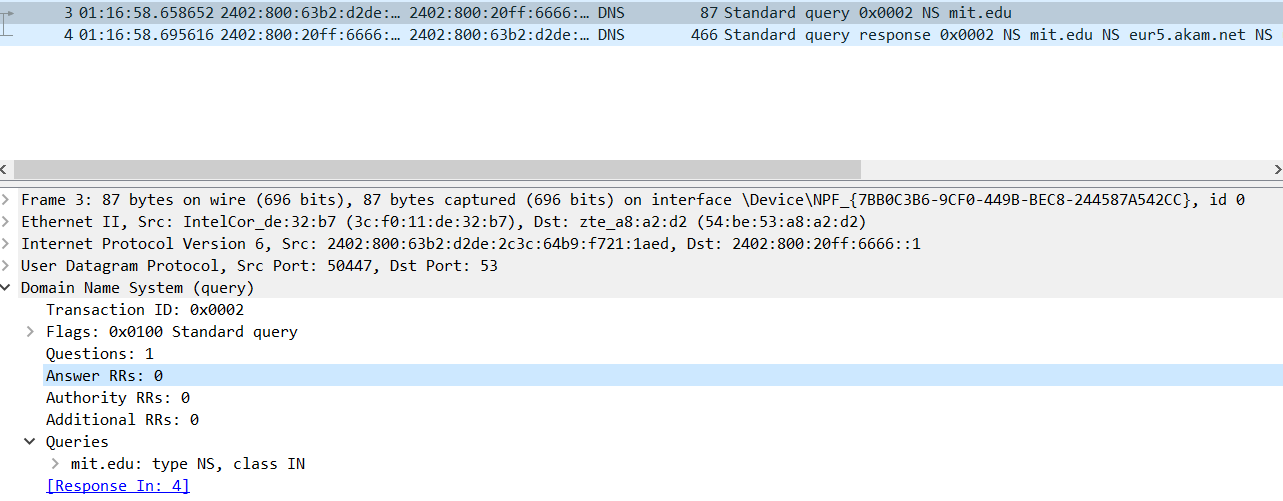
1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?



IP address the DNS query sent to: 2402:800:20ff:6666::1

Yes, it is the IP address of my default local DNS server

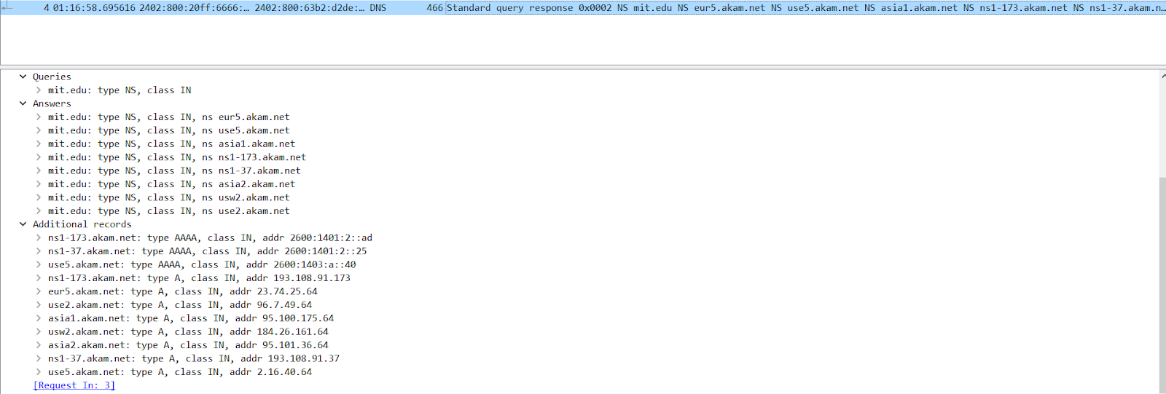
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



Type of DNS query: NS

No, the query message does not contain any answer

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 nameservers?



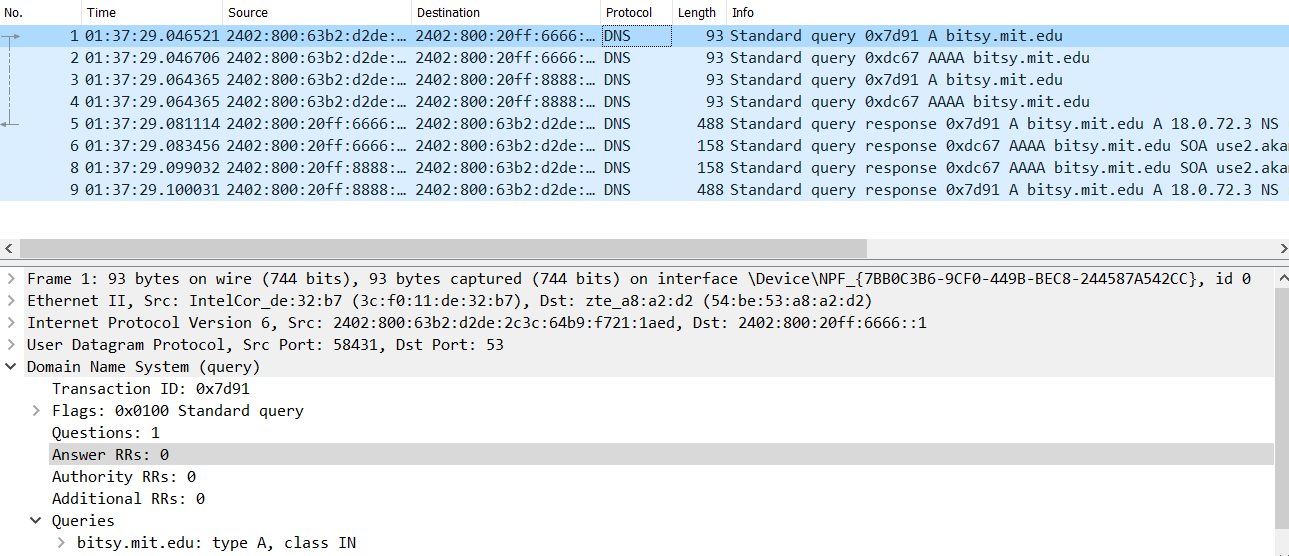
MIT nameservers the response message provides: eur5.akam.net, use5.akam.net, asia1.akam.net, ns1-173.akam.net, ns1-37.akam.net, asia2.akam.net, usw2.akam.net, use2.akam.net

Yes,  this response message also provide the IP addresses of the MIT nameservers

1. Provide a screenshot.

They are provided in each question

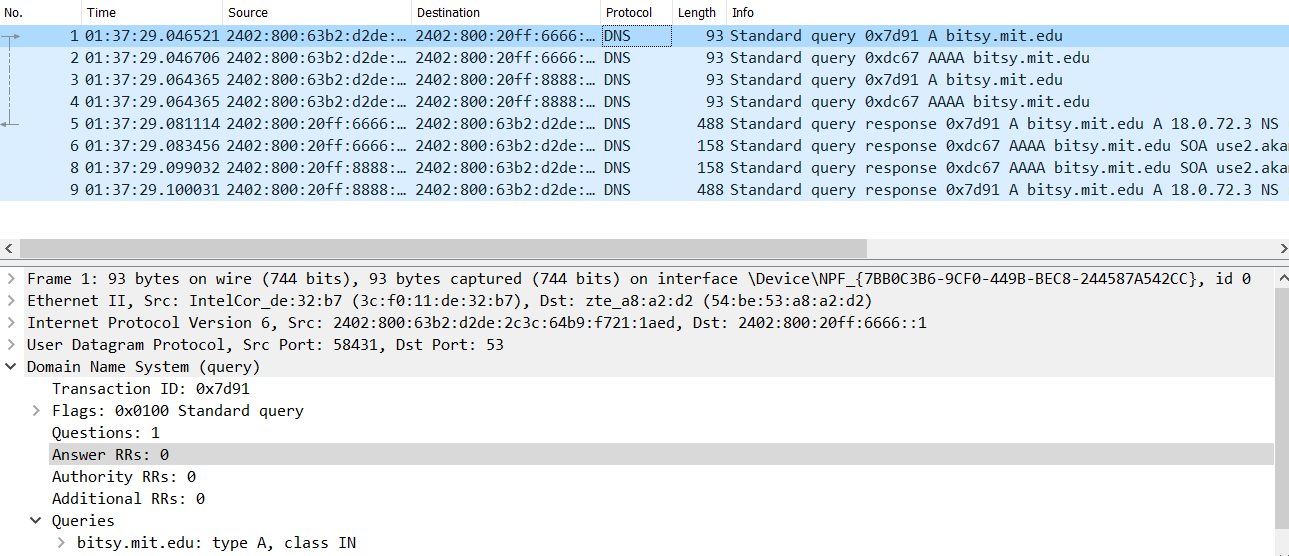
1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?



IP address the DNS query message sent to: 2402:800:20ff:6666::1

Yes, it is the IP address of my default local DNS server

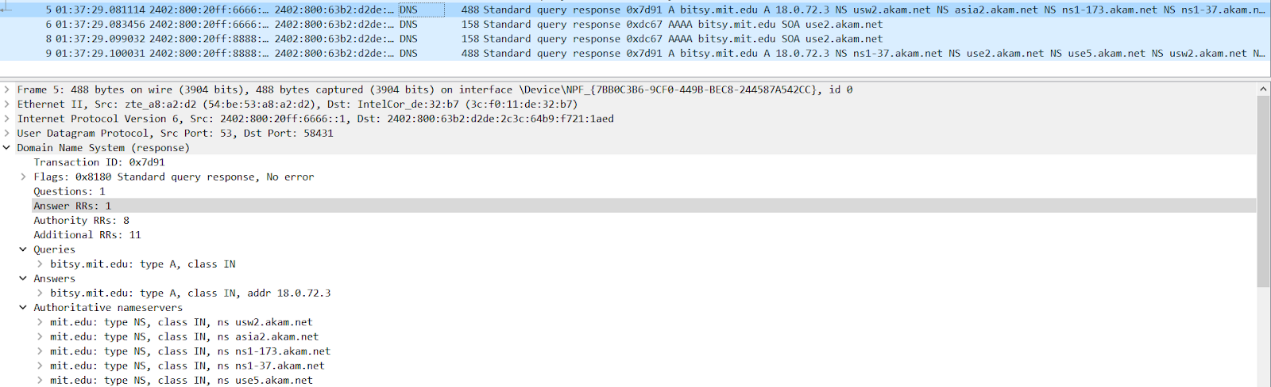
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



Type of DNS query: A

No, the query message does not contain any answer

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



1 answer is provided

It contains the answer for the query: address

1. Provide a screenshot.

They are provided in each question