**COMPUTER NETWORKS**

**NAME: M.ISTAFA MALIK**

**ROLL: P190033**

**SECTION: BSCS-5A**

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

**Solution:**

Here we use nslookup on [http://www.gundam.jp.](http://www.gundam.jp/)

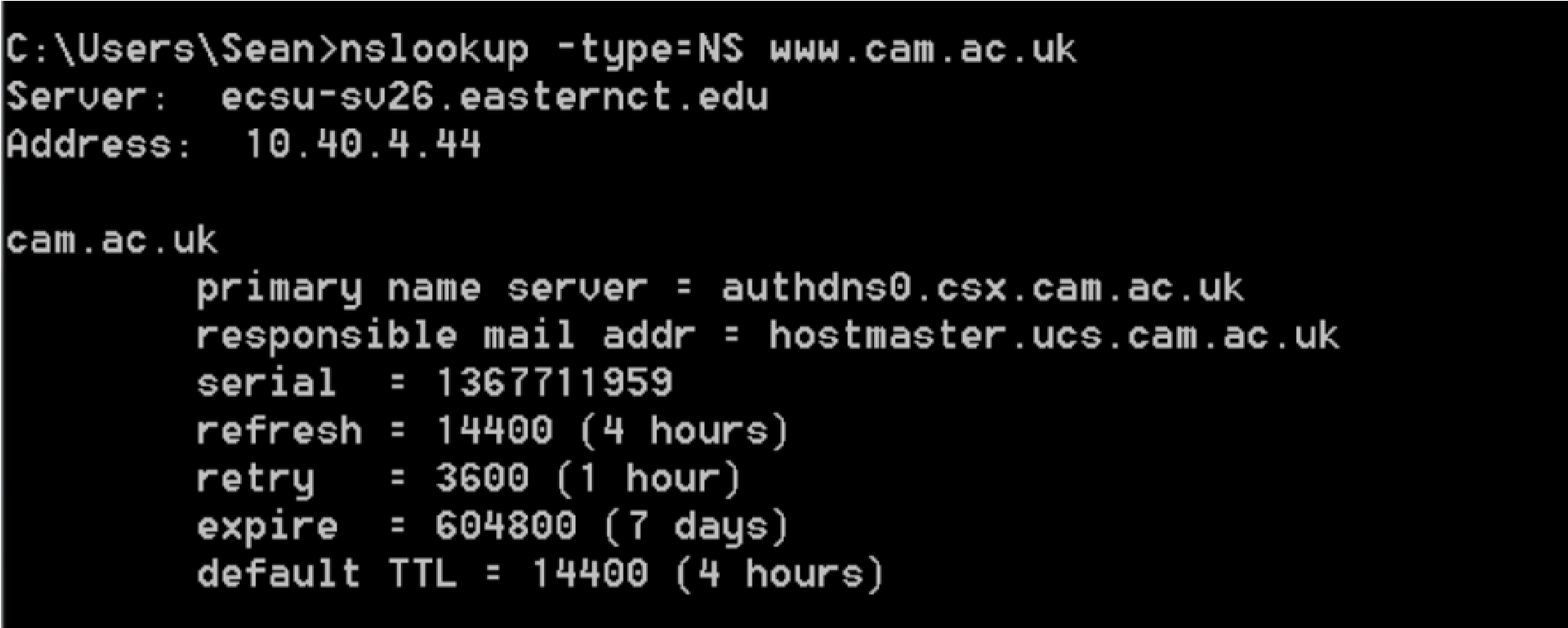


The IP address of the server is 60.32.7.37.

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

**Solution:**

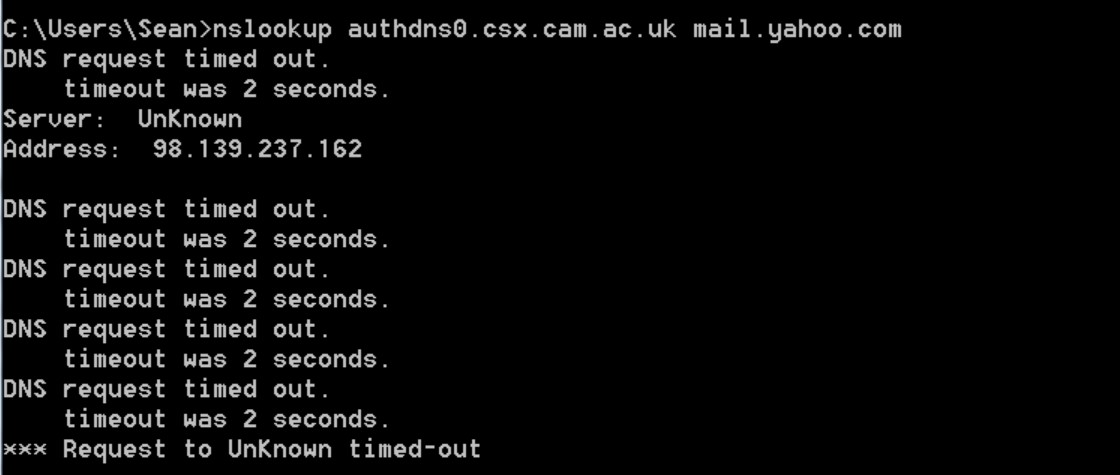
University of Cambridge was the target of this nslookup at [http://www.cam.ac.uk.](http://www.cam.ac.uk/)



The authoritative DNS server for Cambridge is authdns0.csx.cam.ac.uk.

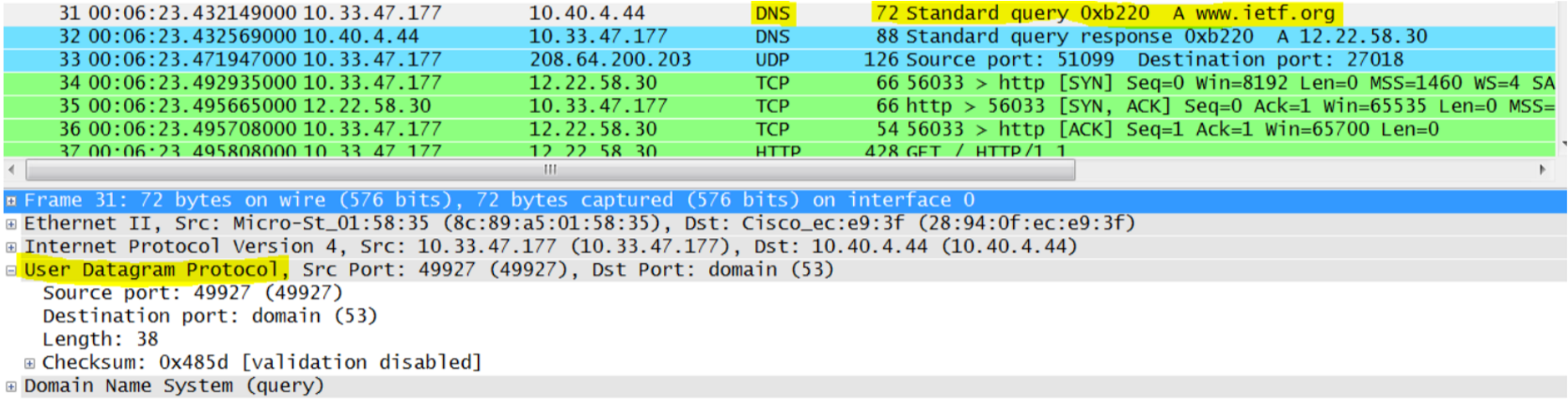
**3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?**

**Solution:**



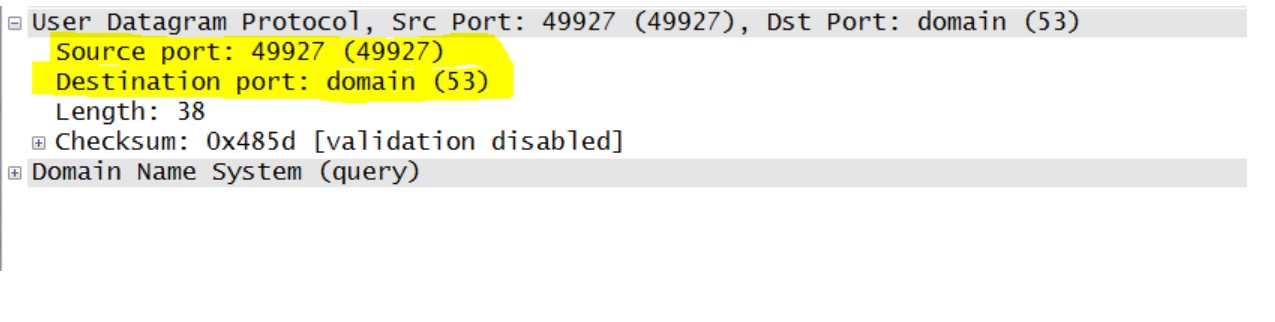
The IP address is 98.139.237.162.

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



The query and response messages are sent via UDP.

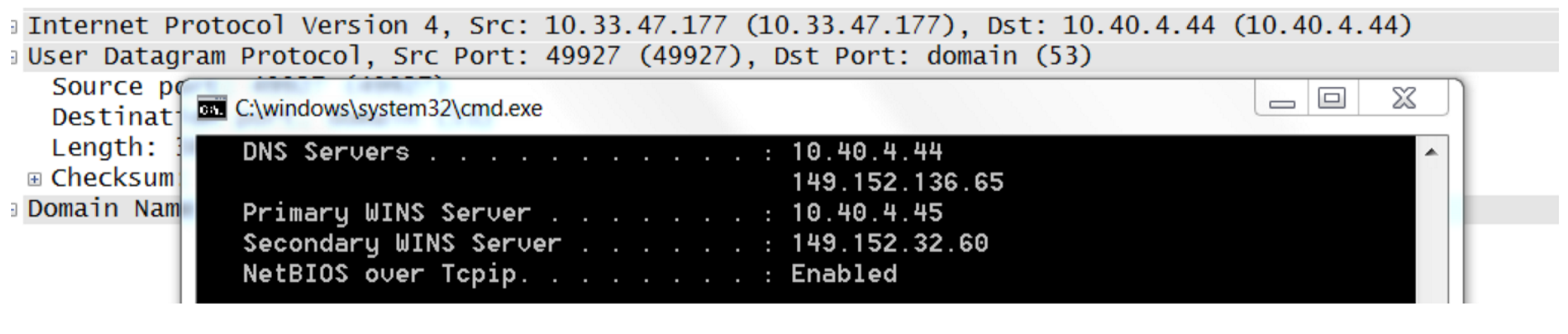
**What is the destination port for the DNS query message? What is the source port of DNS response message?**



The destination port is port 53, and the source port is port 49927.

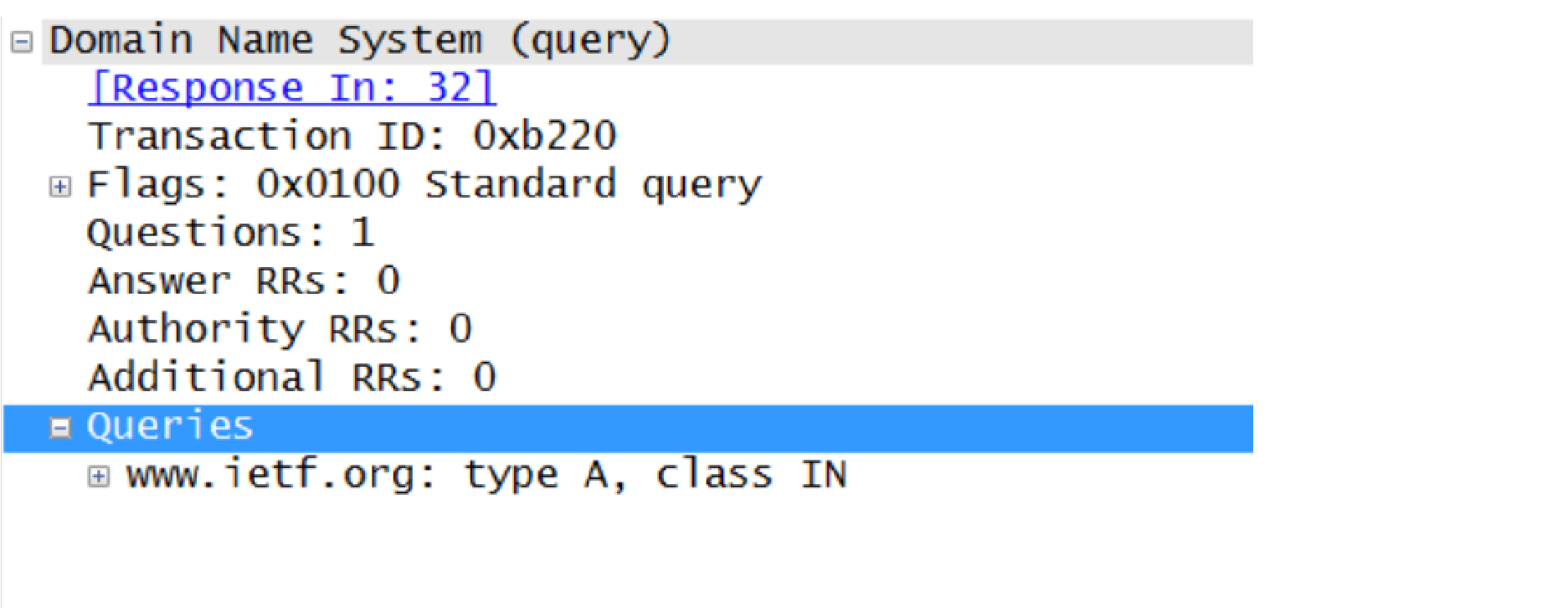
**To what IP address is the DNS query message sent? Use ipconfig to determine the IP**

**address of your local DNS server. Are these two IP addresses the same?**



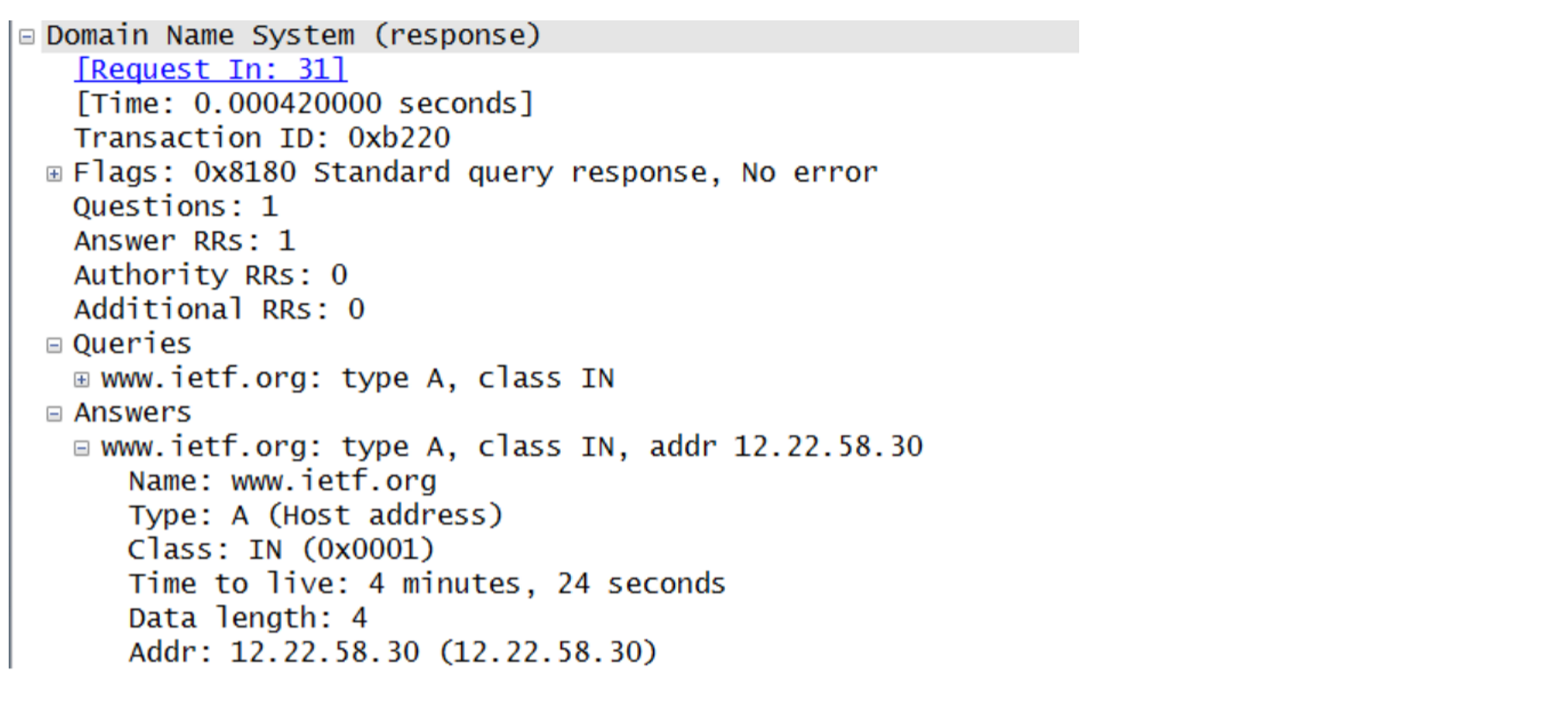
The DNS query message was sent to 10.40.4.44. This is the same IP address as the local DNS server.

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



This query was a type A query. It did not contain any “answers”.

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



This DNS response message provided only one answer. The answer contains the address of the website that it was queried for.

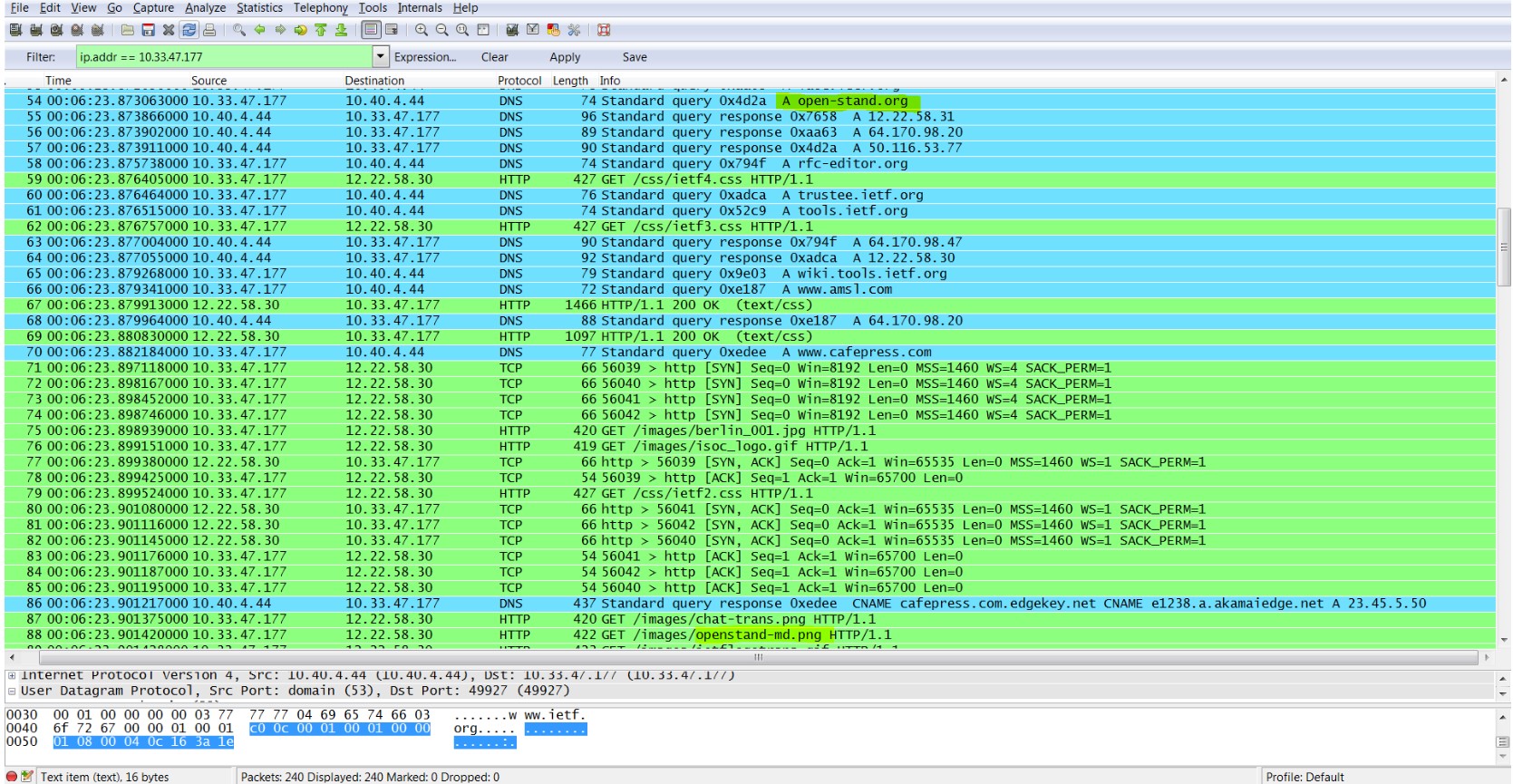
**Consider the subsequent TCP SYN packet sent by**

**your host. Does the destination IP**

**address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**

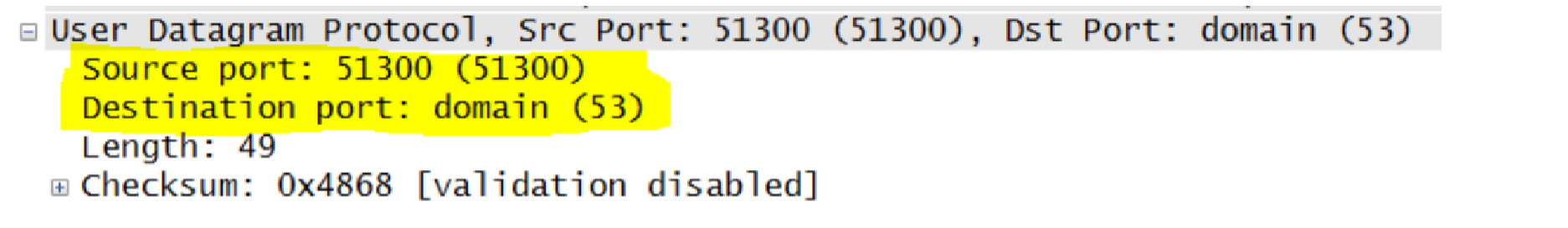
The destination IP address of the SYN packet corresponds to the address provided by the DNS response, 12.22.58.30.

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



Yes, the host issues new DNS queries for each image.

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

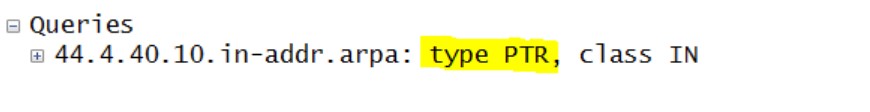


The destination port for the DNS query message is port 53. The source port of the DNS response message is also port 53.

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

The DNS query message is sent to IP 10.40.4.44. This is the same IP address of my local DNS server.

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



This message is of type PTR. This query contains no answers.

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

The first DNS response message contains one answer. This answer contains the next DNS server to query en route to [http://www.mit.edu.](http://www.mit.edu/)

**Provide a screenshot.**

