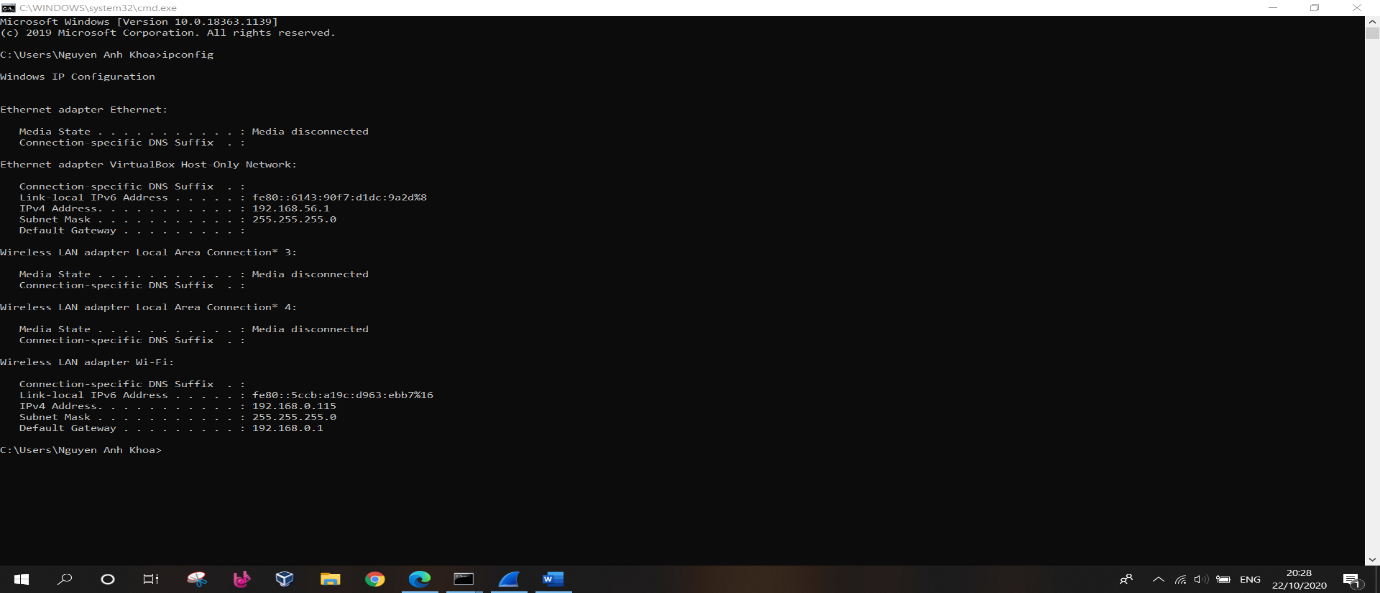
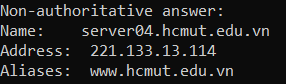
**Lab 2b**

My IP Address: 192.168.0.115

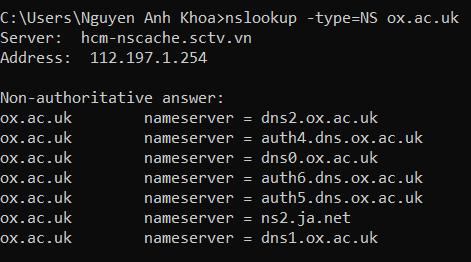


1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

Answer:

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

Answer: At Oxford University

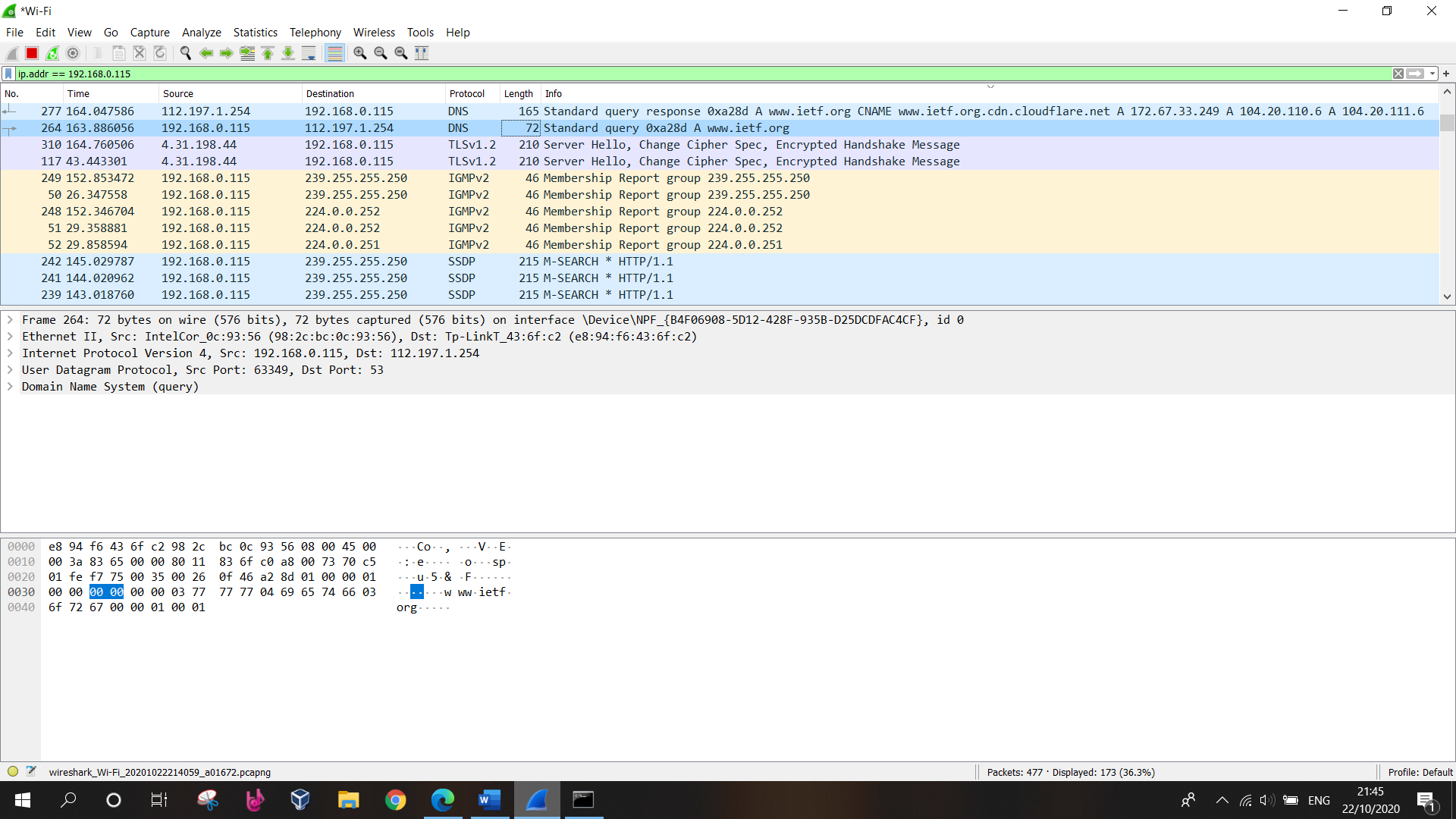


1. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

Answer: I was unable to get any of the DNS servers listed above to answer a query for a Yahoo mail server

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

Answer: UDP



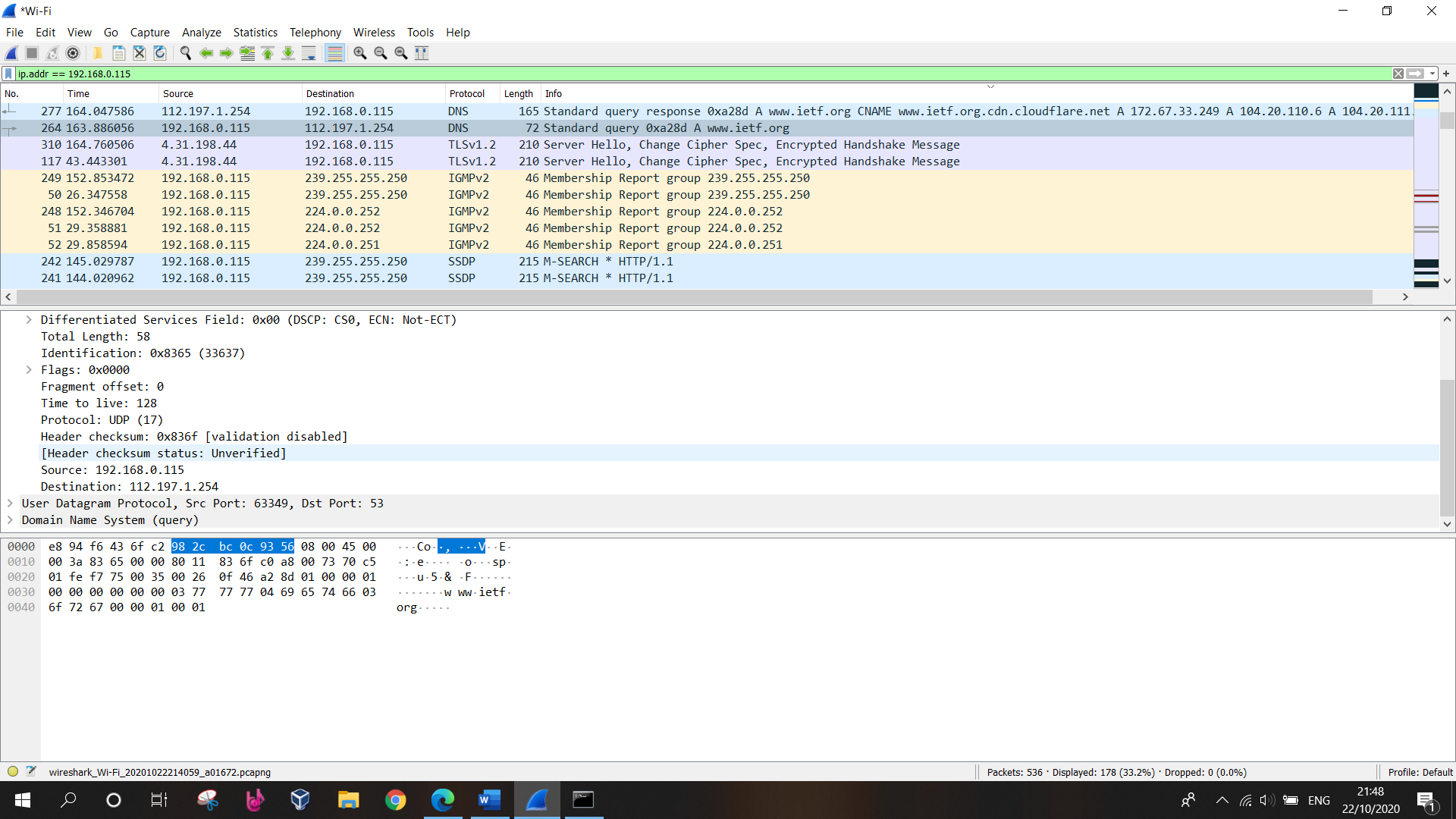
1. What is the destination port for the DNS query message? What is the source port of DNS response message?

Answer:

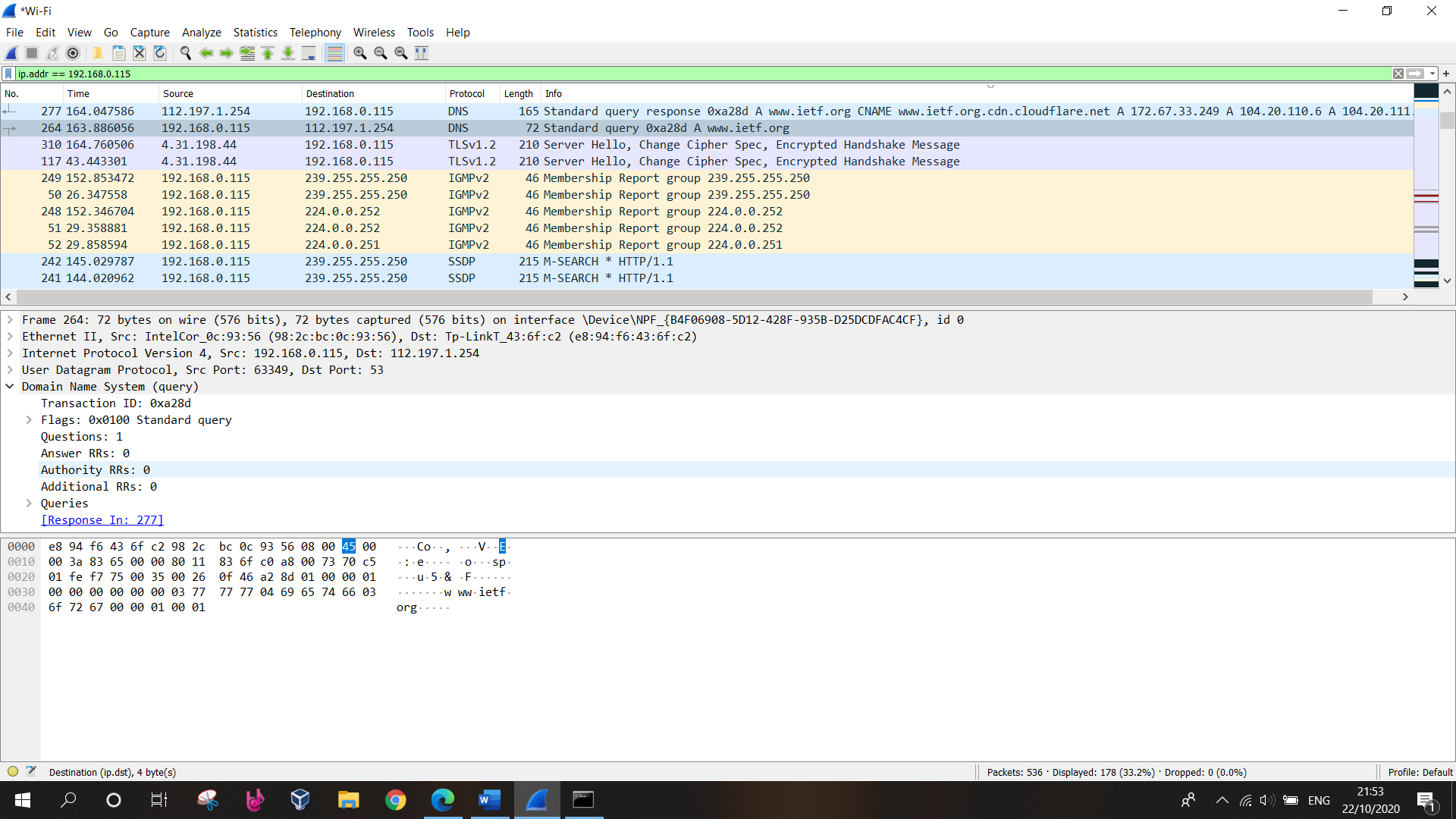
Destination port: 53

Source Port: 63349

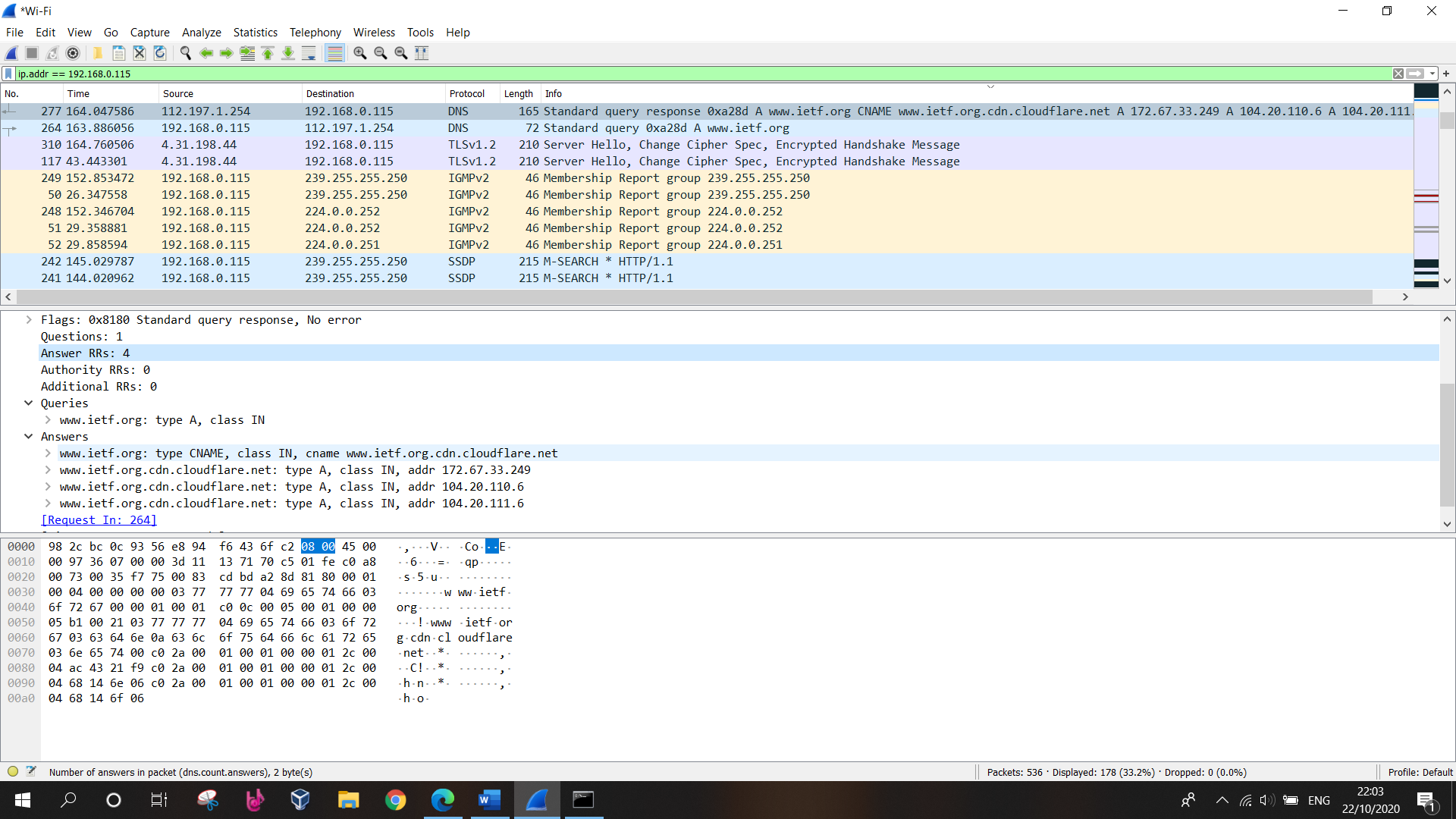
1. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

Answer: The screenshot shows that the DNS message was sent to 112.197.1.254

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

Answer: It is a “type A” query, which is for a standard host address resource record. No answers as shown in screenshot (one question)

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

Answer: 4 answer containing the IP address of www.ietf.org (see screenshot)

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?

Answer: Yes, as seen in the prior screenshot, the destination address is 172.67.33.249, 104.20.110.6, 104.20.111.6 which is the address provided by the DNS server for www.ietf.org.

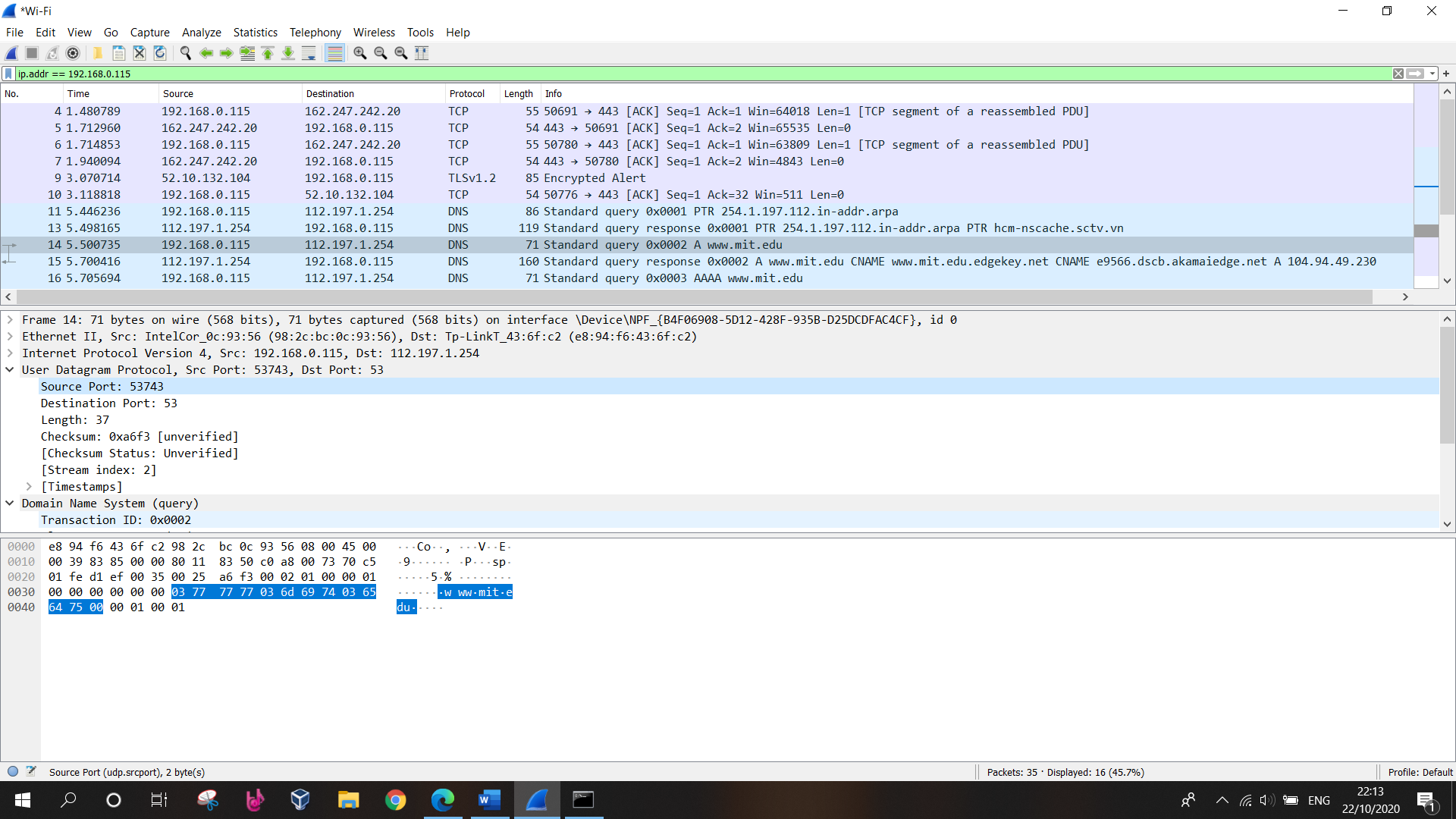
1. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Answer: 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?

Answer:

Source port: 53743

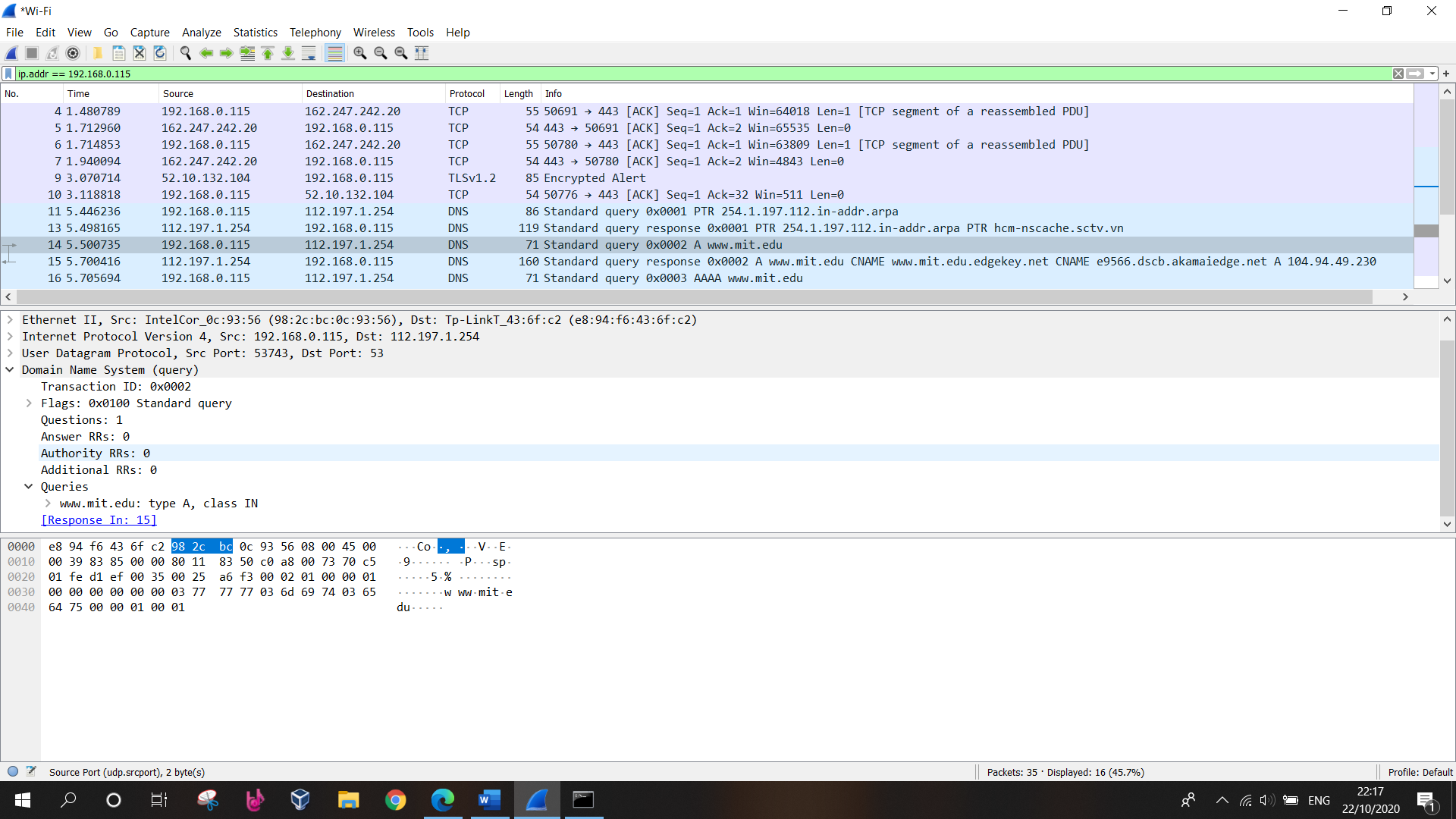
Destination port: 53

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

Answer: 192.168.0.115. Yes

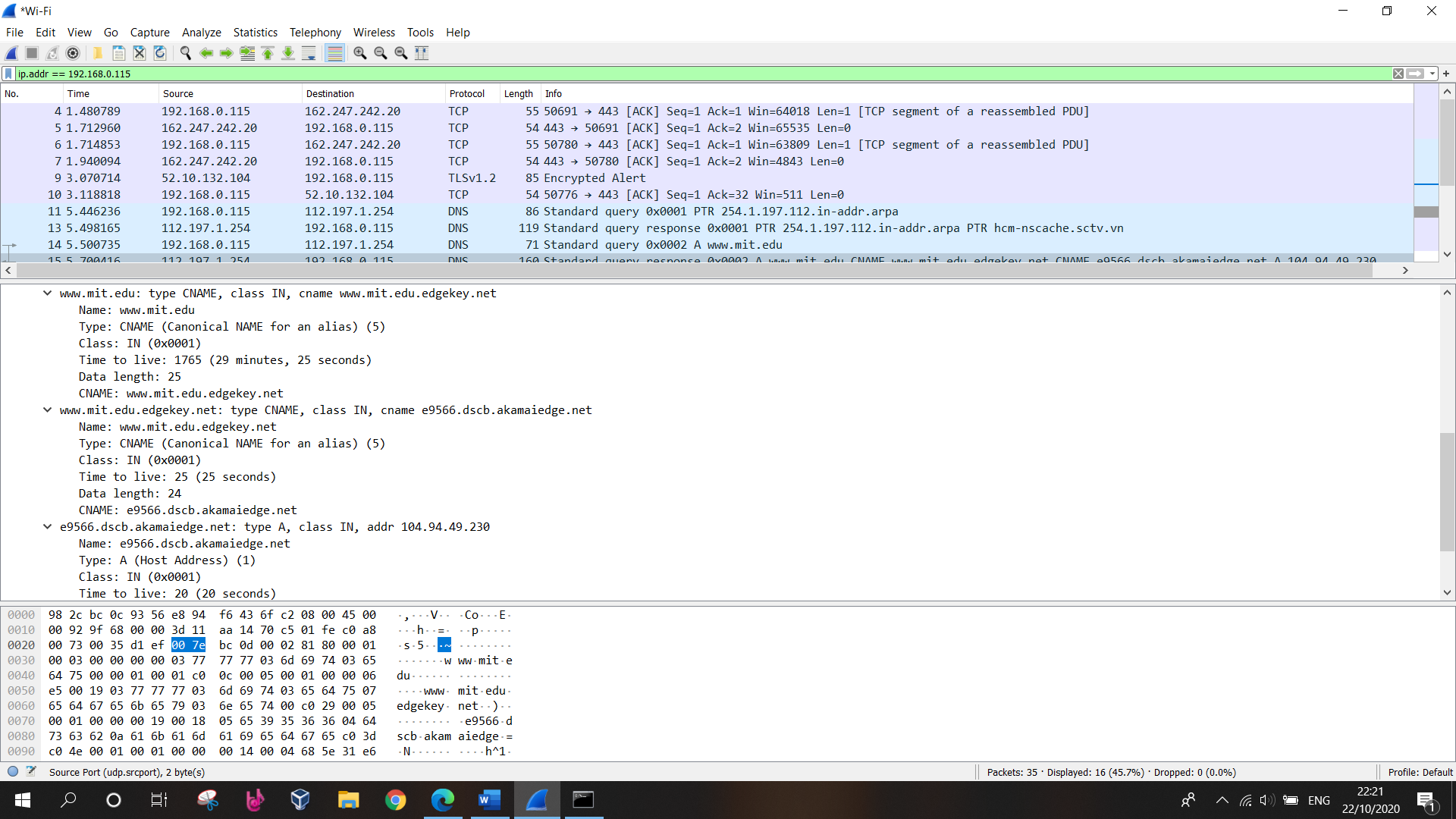
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: Standard type A (Host address) query (see screenshot). The message only contains a query (no answers).

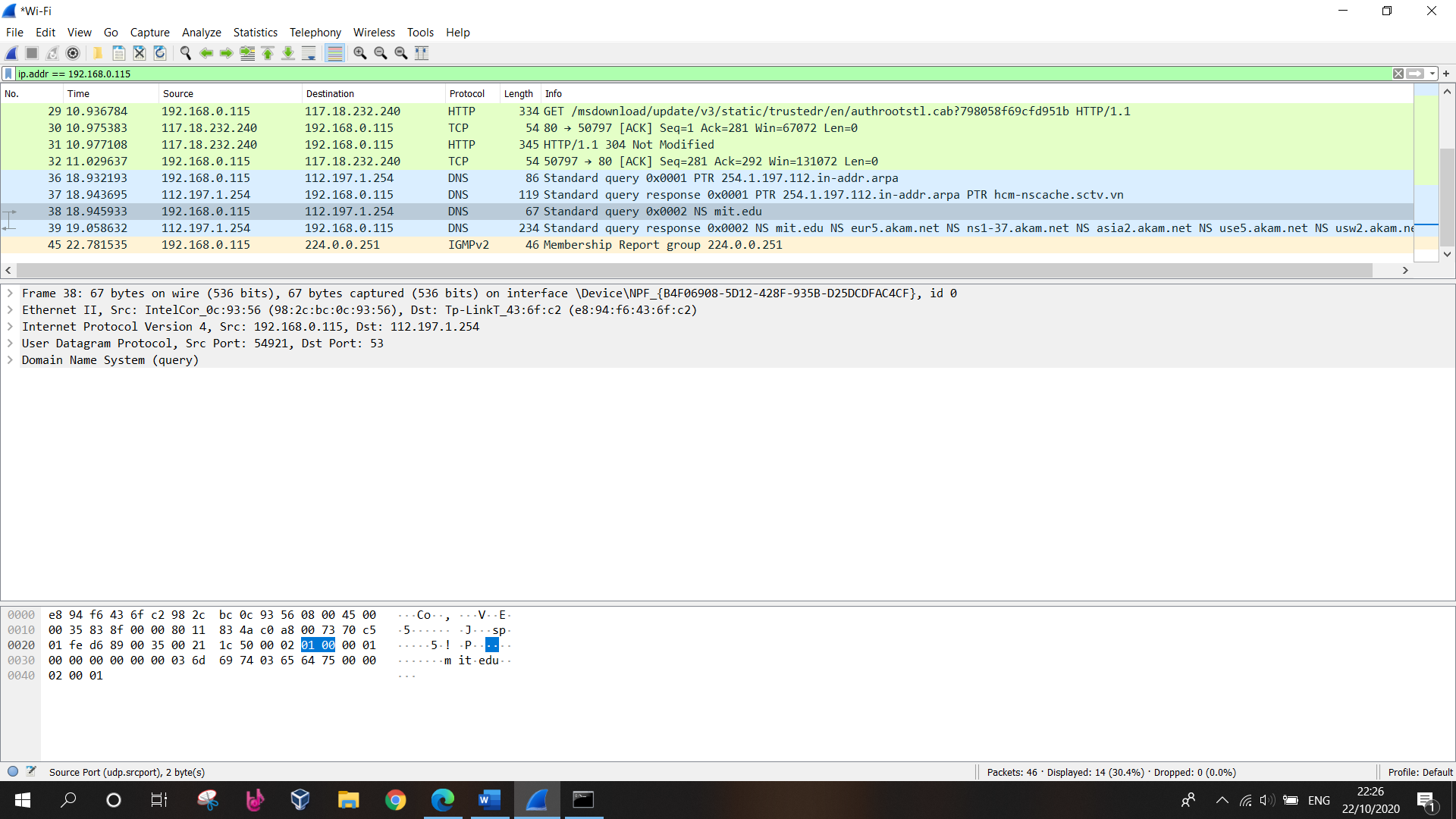


1. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

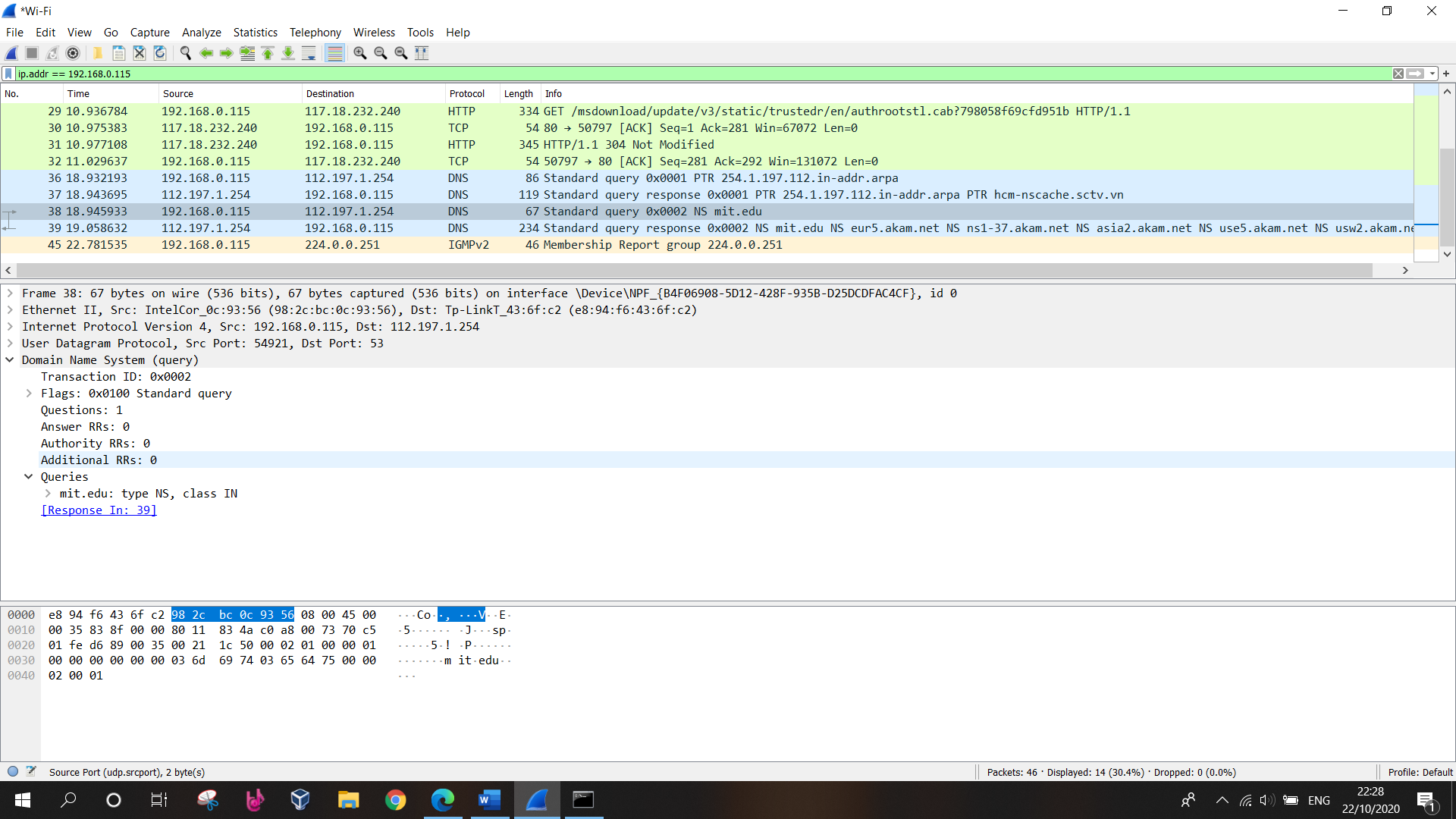
Answer: Three answers (resource records), two corresponding to CNAMEs and one host address.

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?

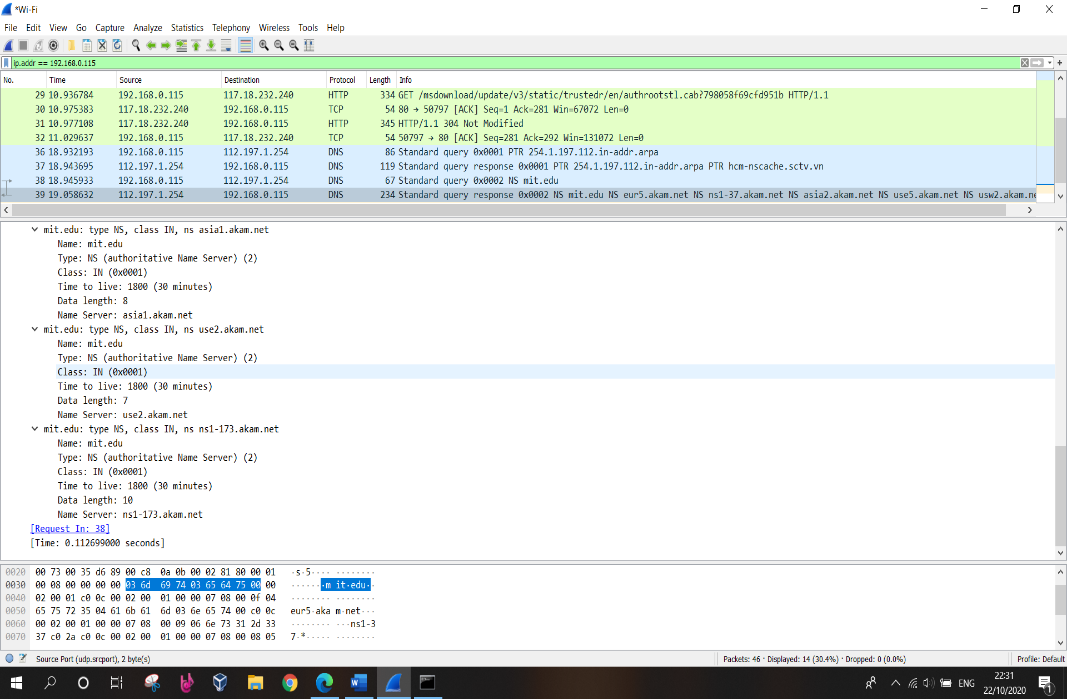
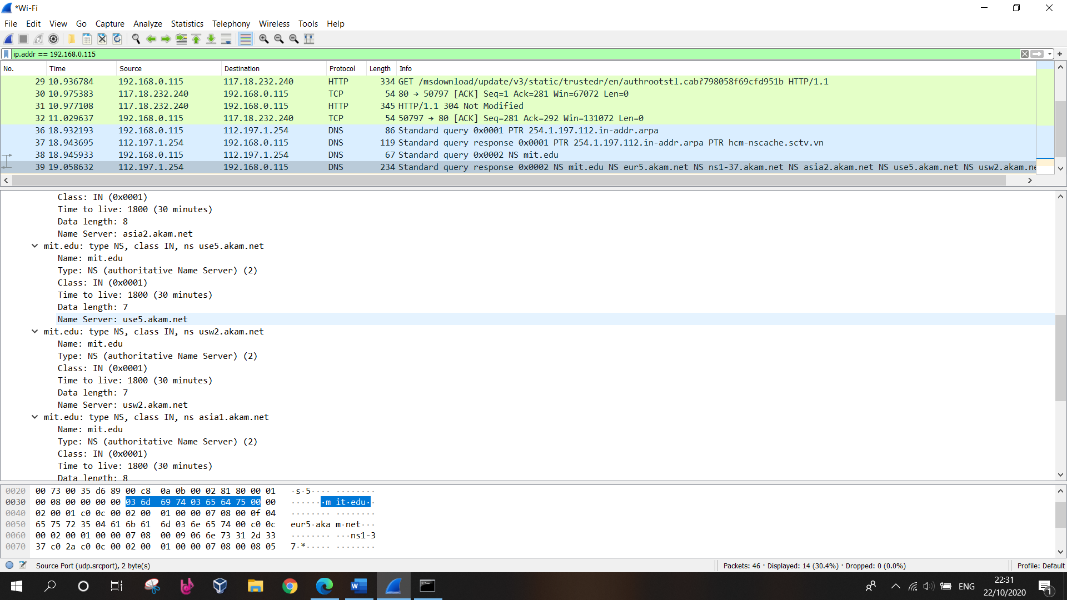
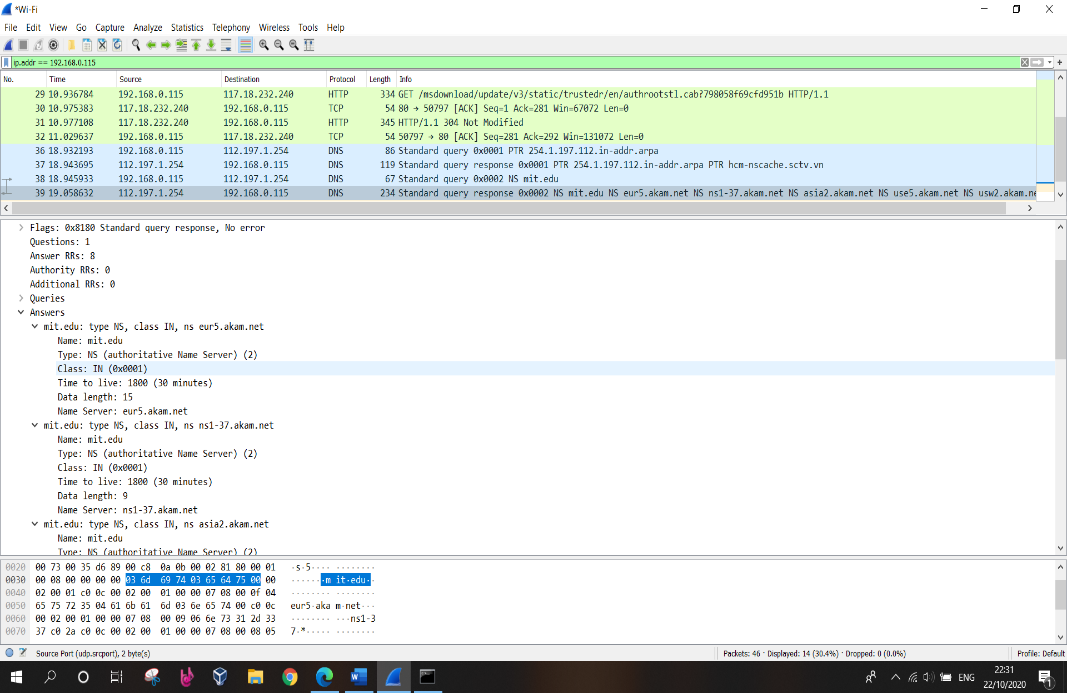
Answer: 192.168.0.115. Yes, this is my IP address



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

Answer: Type NS. Contain no answer

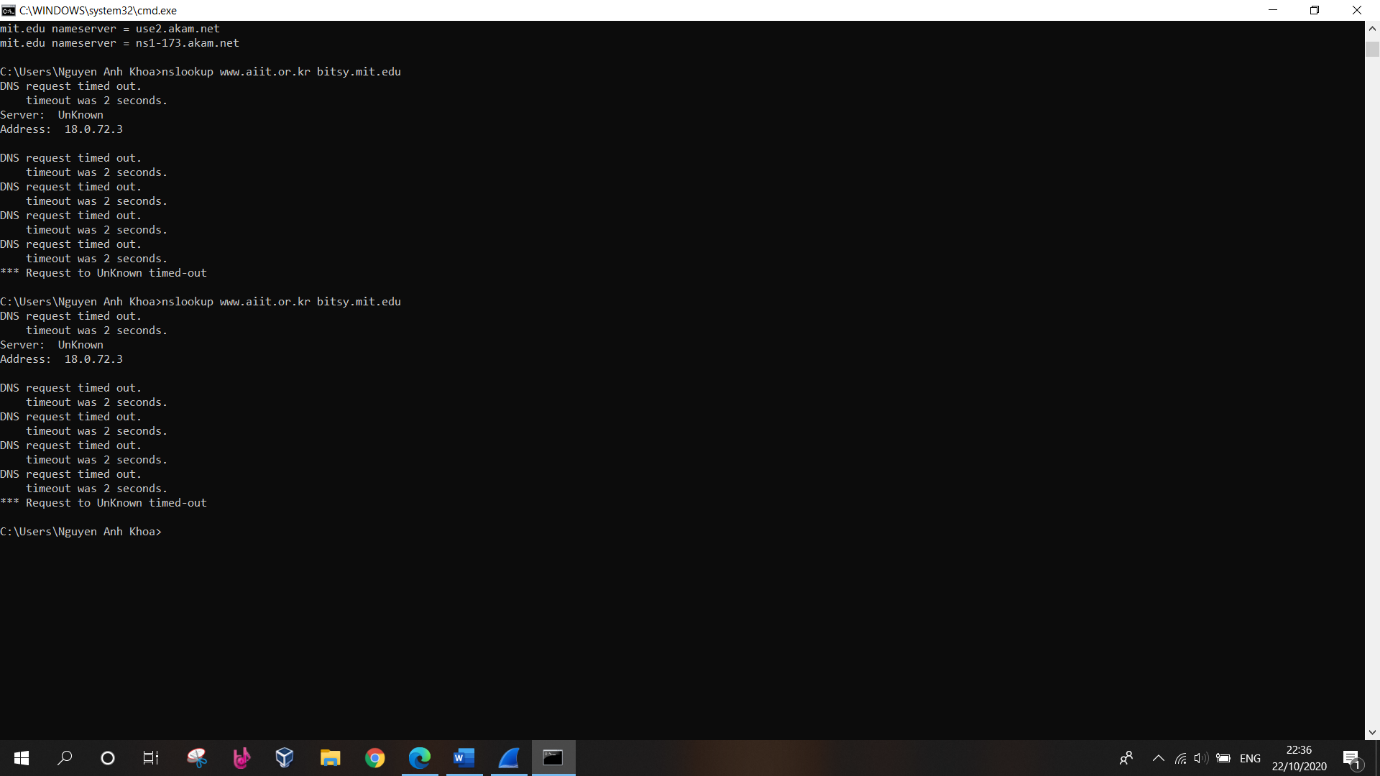
1. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

Answer: This reponse message do not contain any IP address of non-authoritative server

1. Provide a screenshot

Answer: above screenshot

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?

Answer: I was unable to get this to work with bitsy.mit.edu

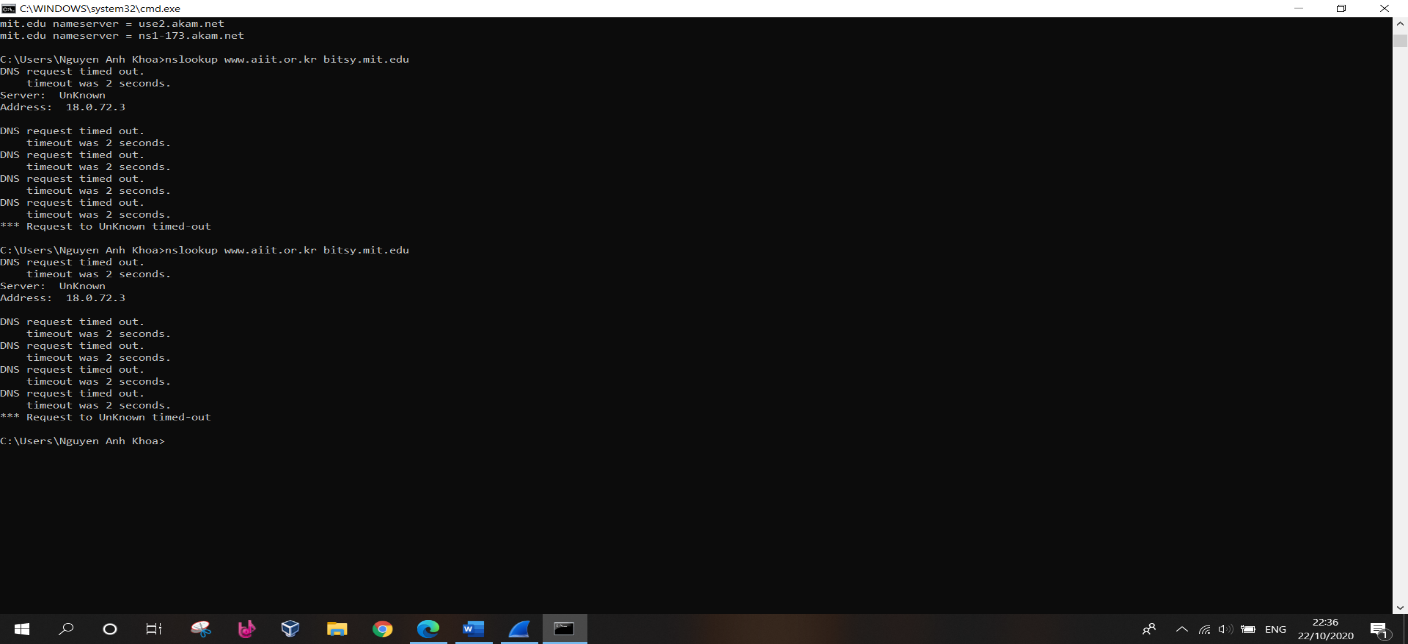
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Answer: I was unable to get this to work with bitsy.mit.edu

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

Answer: I was unable to get this to work with bitsy.mit.edu

1. Provide a screenshot.

Answer: