Computer Network: Wireshark DNS

Assignment 1

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

Answer:

```
C:\Users\prashant>nslookup artasia.in
Server:  UnKnown
Address:  10.94.8.11

Non-authoritative answer:
Name:    artasia.in
Address:  107.180.40.26
```

IP Address-10.94.8.11

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

Answer:

```
C:\Users\prashant>nslookup -type=NS cam.ac.uk
Server:  UnKnown
Address:  10.94.8.11

Non-authoritative answer:
cam.ac.uk       nameserver = ns3.mythic-beasts.com
cam.ac.uk       nameserver = ns2.ic.ac.uk
cam.ac.uk       nameserver = ns1.mythic-beasts.com
cam.ac.uk       nameserver = auth0.dns.cam.ac.uk
cam.ac.uk       nameserver = dns0.cl.cam.ac.uk
cam.ac.uk       nameserver = dns0.eng.cam.ac.uk

ns2.ic.ac.uk    internet address = 155.198.142.82
dns0.cl.cam.ac.uk       internet address = 128.232.0.19
dns0.eng.cam.ac.uk      internet address = 129.169.8.8
auth0.dns.cam.ac.uk     internet address = 131.111.8.37
ns2.ic.ac.uk    AAAA IPv6 address = 2a0c:5bc0:4:1::82
auth0.dns.cam.ac.uk     AAAA IPv6 address = 2001:630:212:8::d:a0
```

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?

Answer:

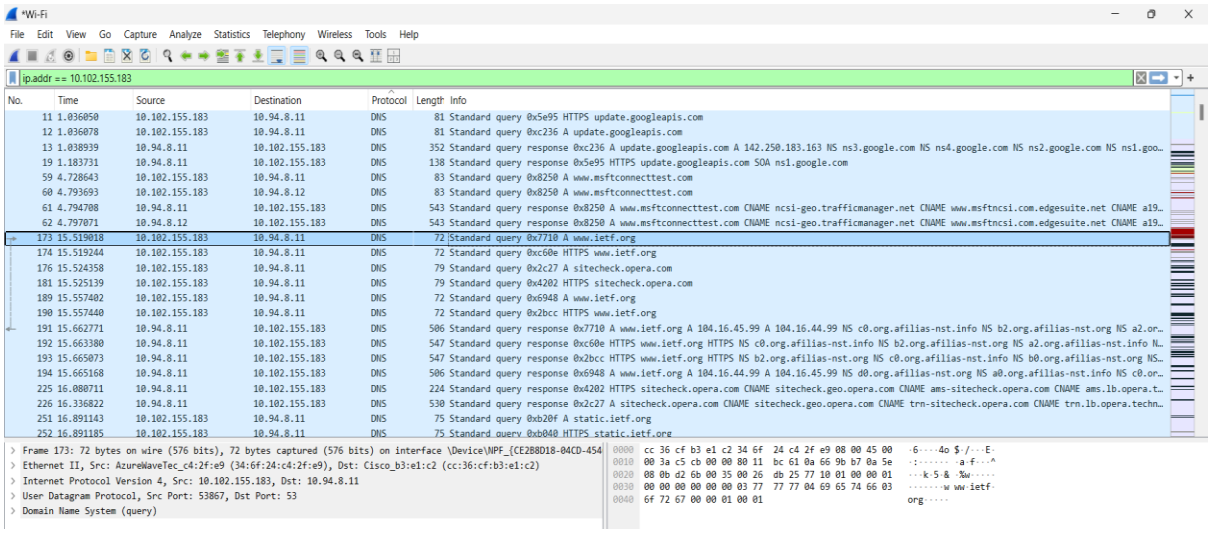
```
C:\Users\prashant>nslookup mail.yahoo.com cam.ac.uk
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  128.232.132.8

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

IP Address-128.232.132.8

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

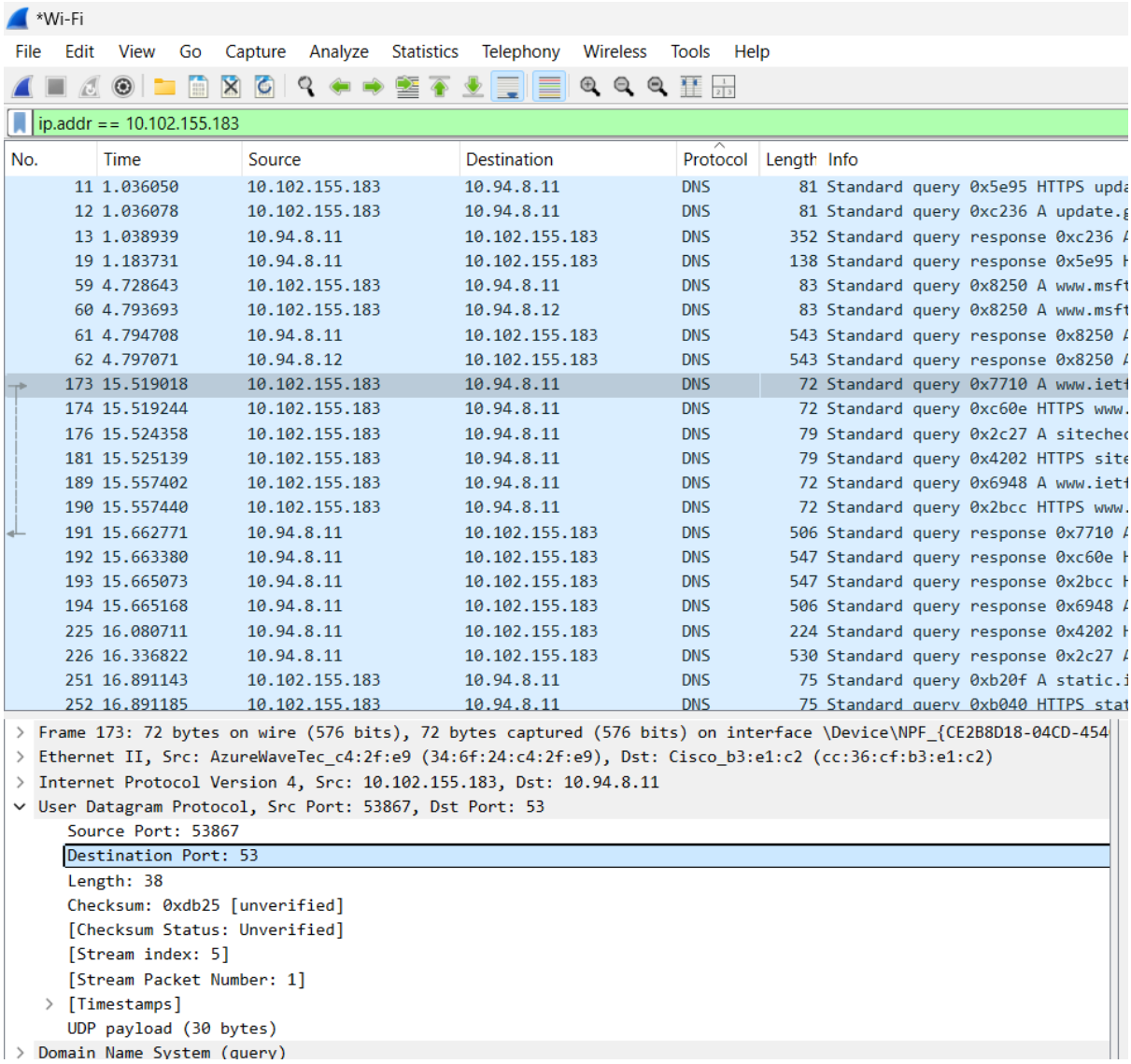
Answer:



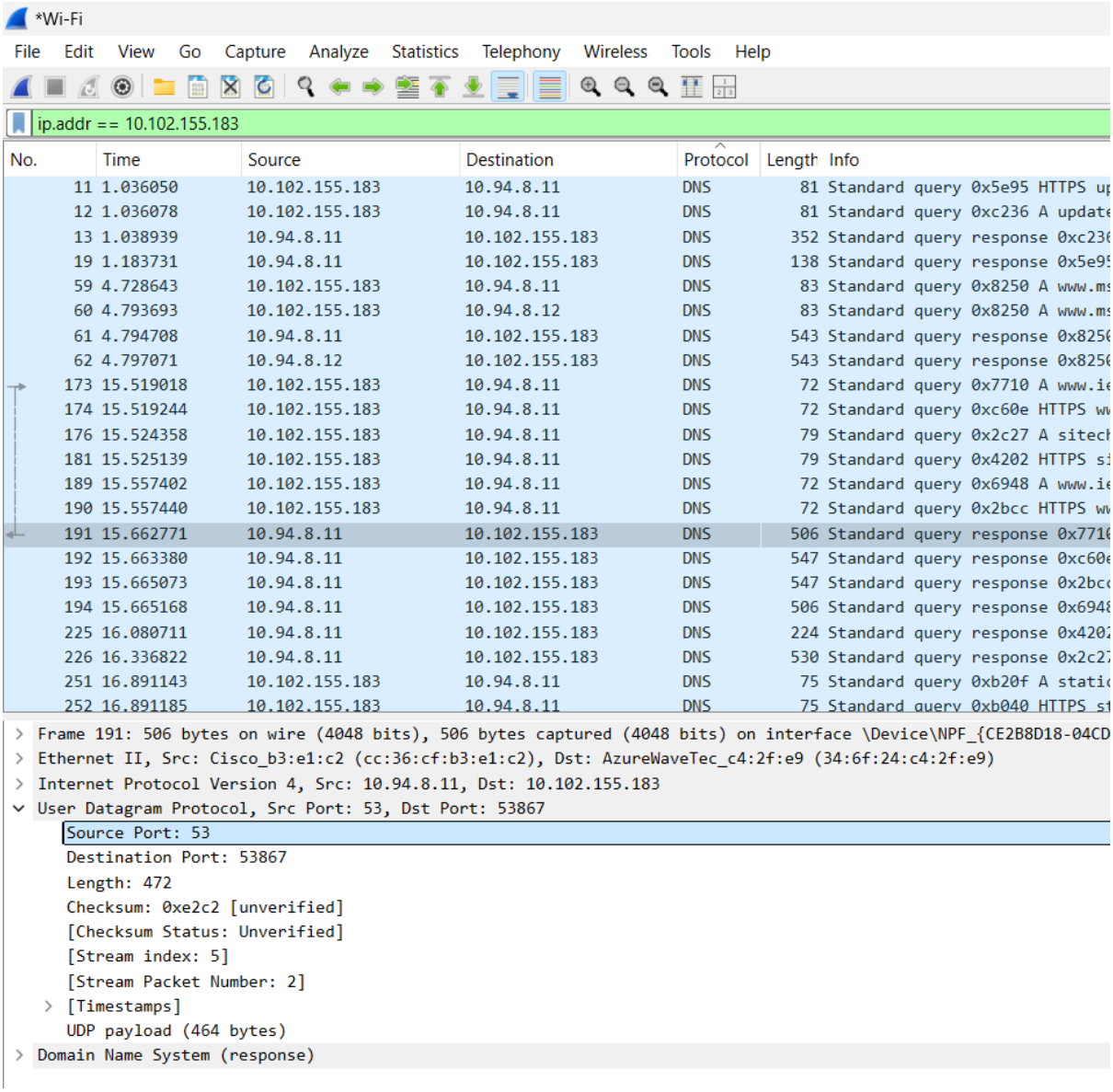
They are sent over UDP(User Datagram Protocol).

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

Answer:



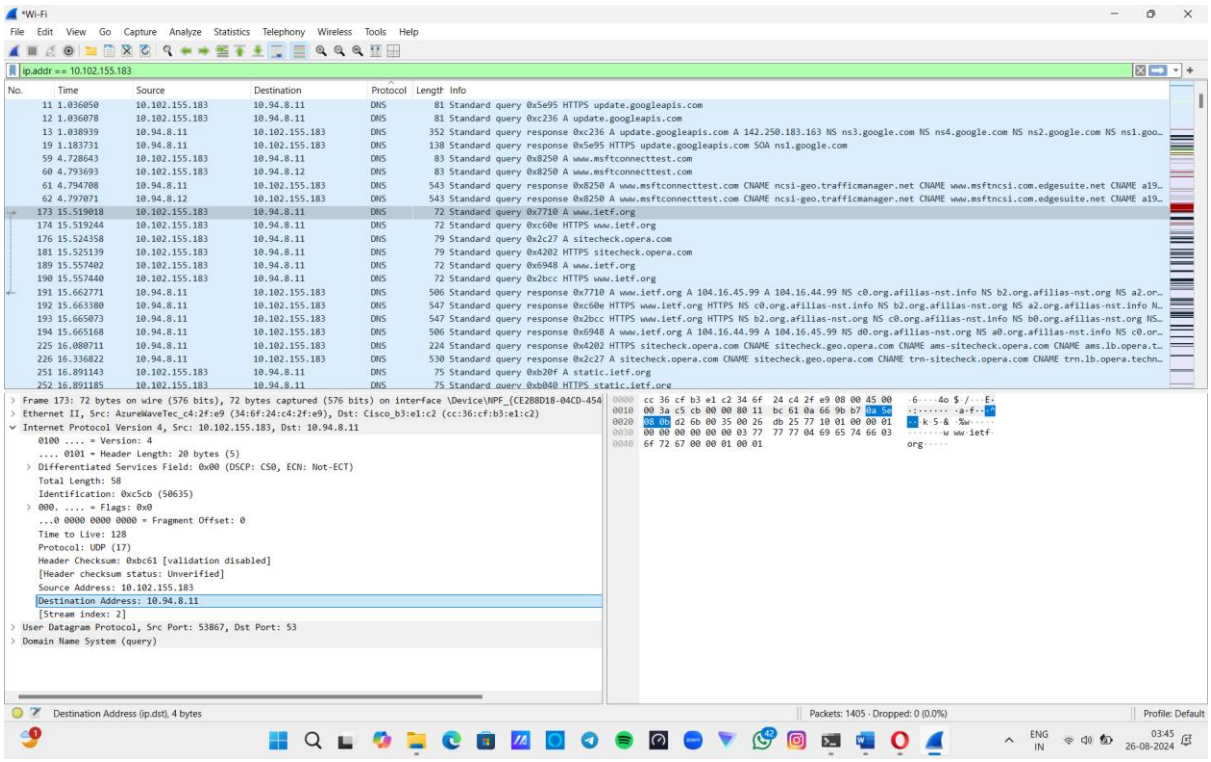
Destination Port of the query is – 53



Source Port of the response is – 53

6. 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 DNS query message is sent to IP Address 10.94.8.11

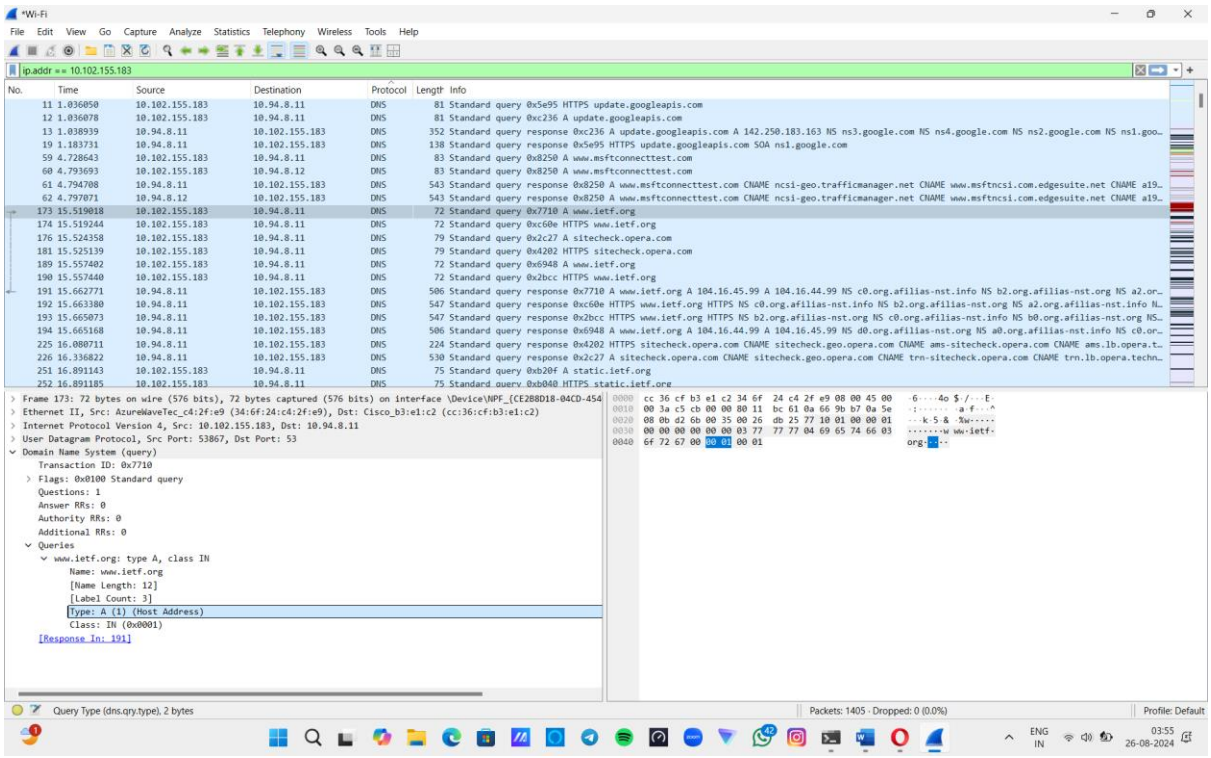
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
   Physical Address. . . . . . . . . : 34-6F-24-C4-2F-E9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.102.155.183(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Lease Obtained. . . . . . . . . . : 25 August 2024 17:56:35
   Lease Expires . . . . . . . . . . : 27 August 2024 02:19:12
   Default Gateway . . . . . . . . . : 10.102.152.1
   DHCP Server . . . . . . . . . . . : 10.102.152.1
   DNS Servers . . . . . . . . . . . : 10.94.8.11
                                       10.94.8.12
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Yes the IP address of destination is same as my device’s IP Address of DNS server address.

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

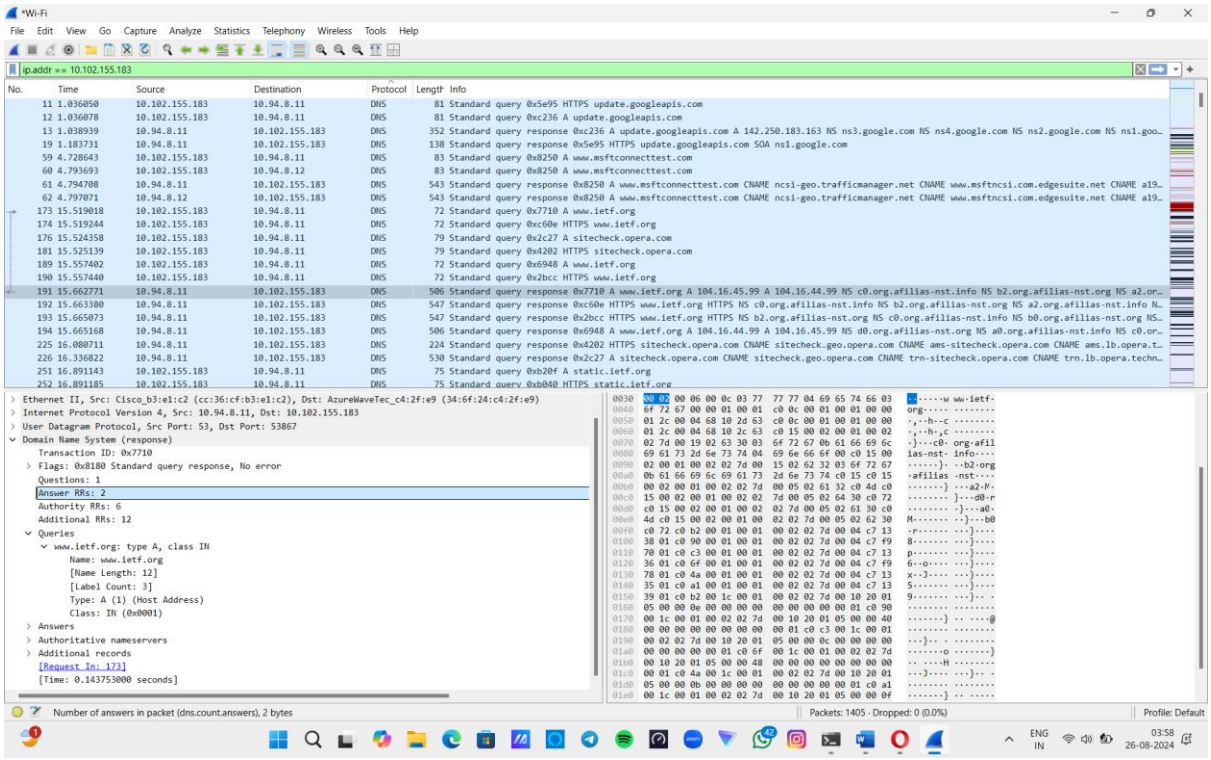
Answer:



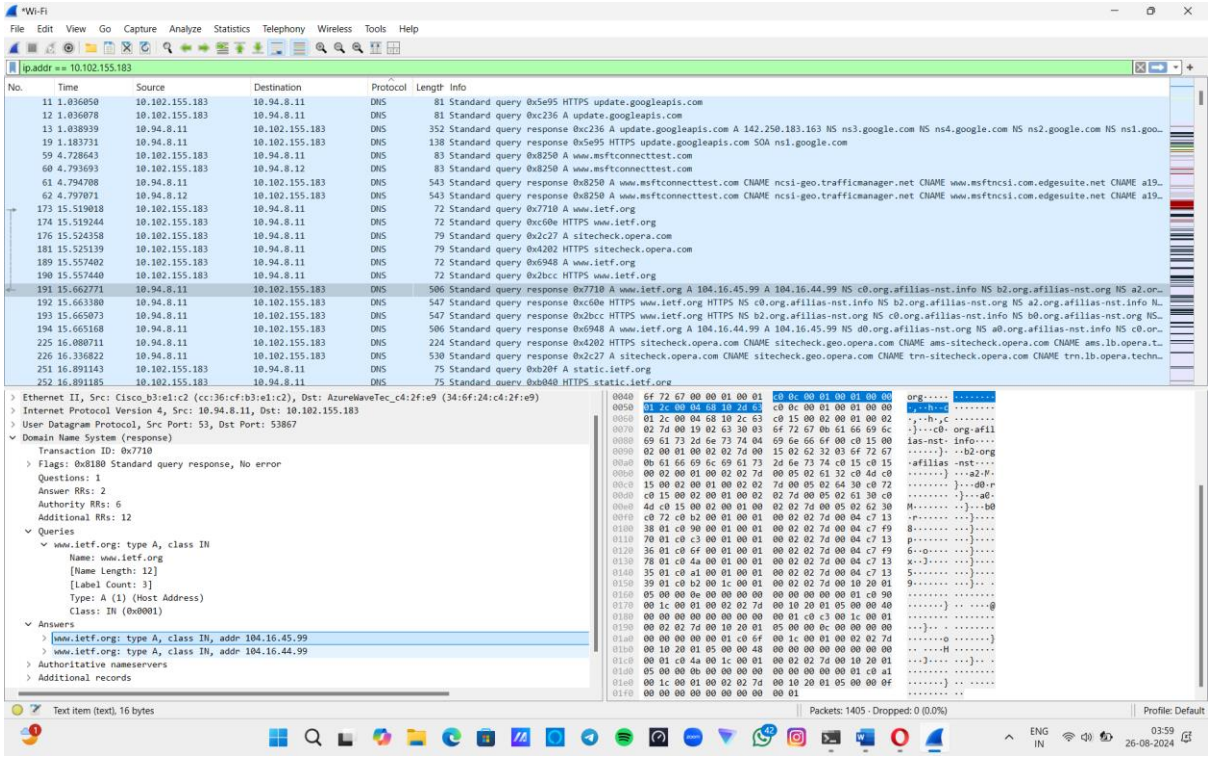
It is a Type A query. No is does not contain any answers.

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

Answers:

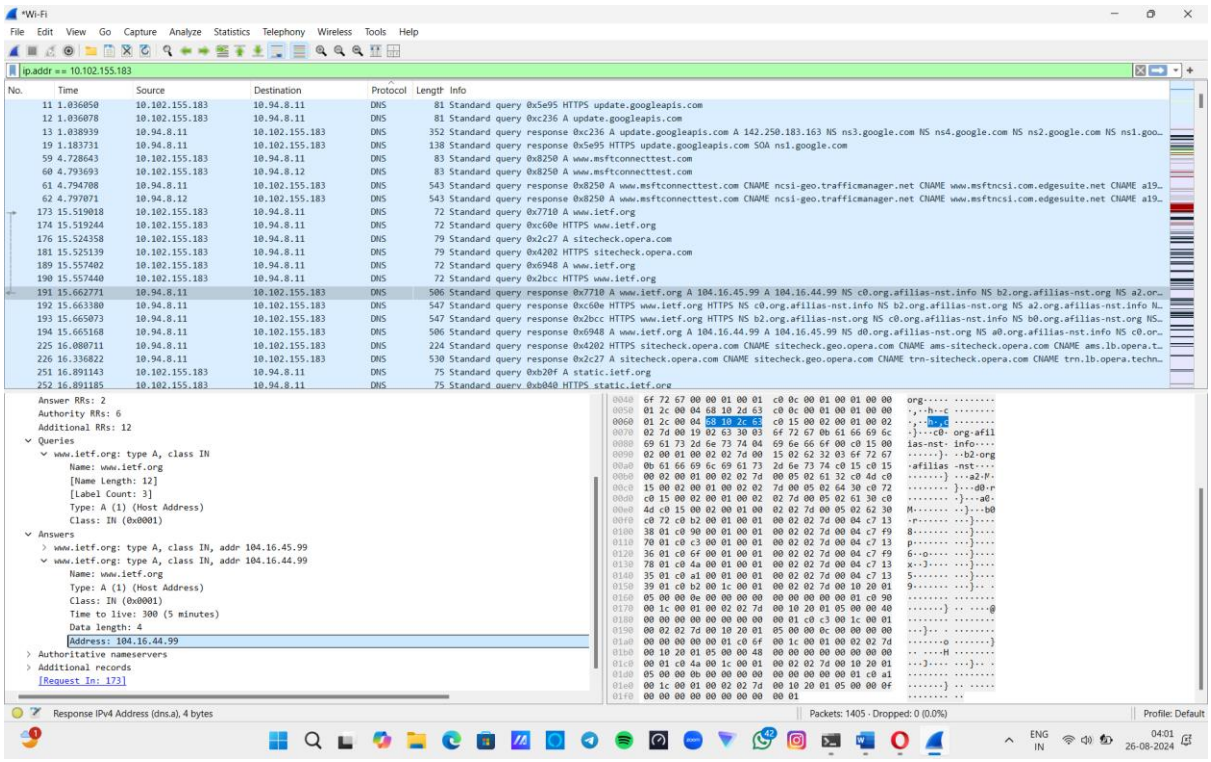


There are two answers.
They contain:



9. 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:



No the destination IP address of SYN packet does not correspond to any of the IP Addresses.

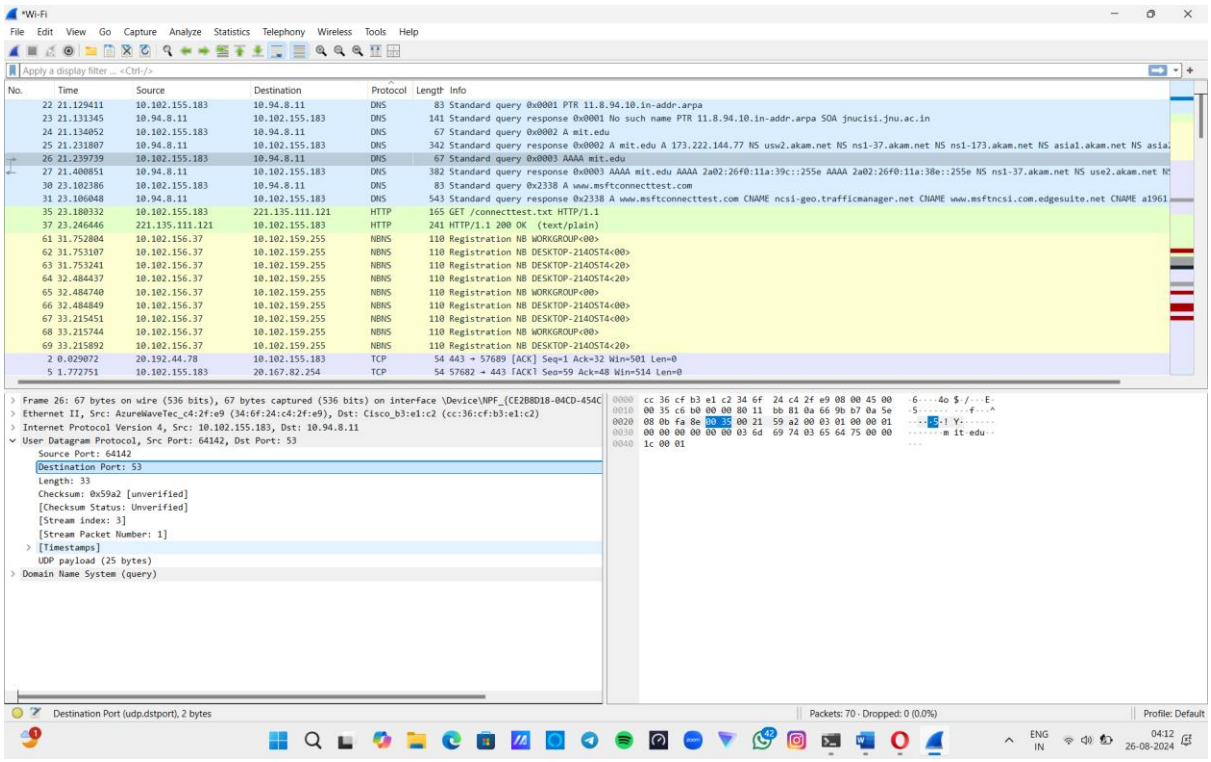
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Answers:

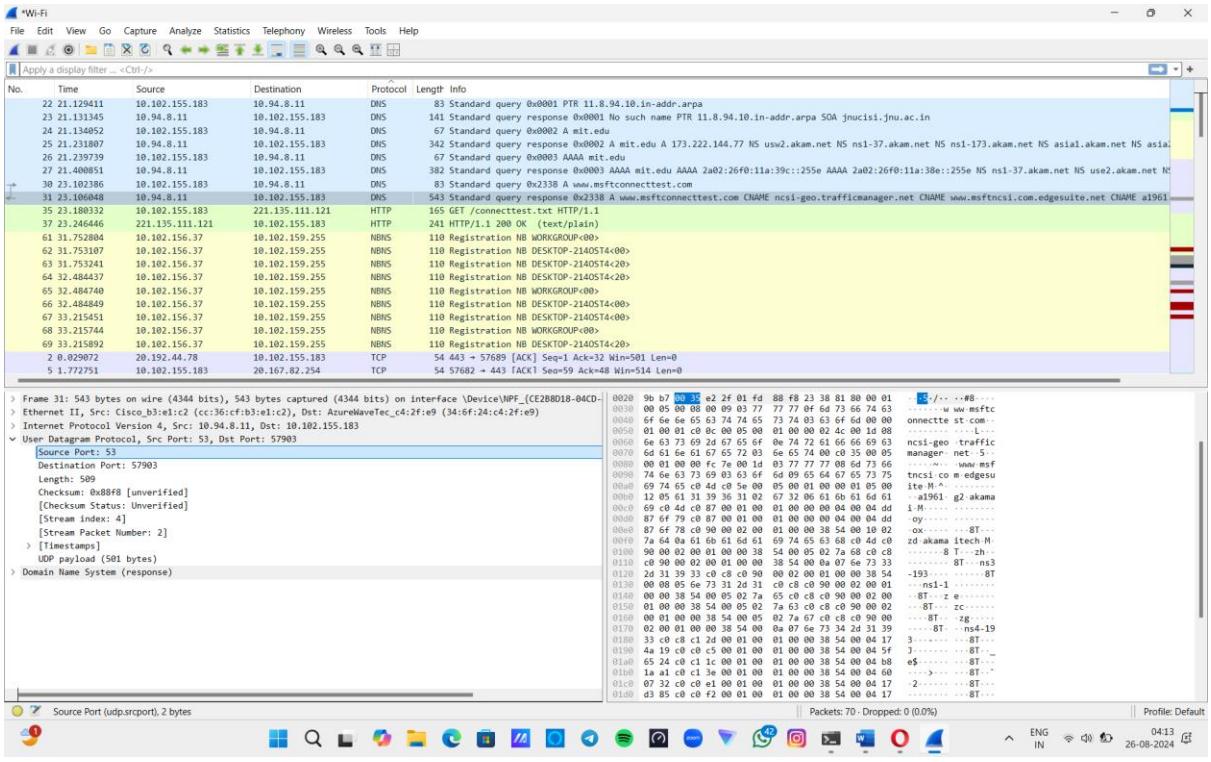
No the host issue new DNS queries.

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

Answer:



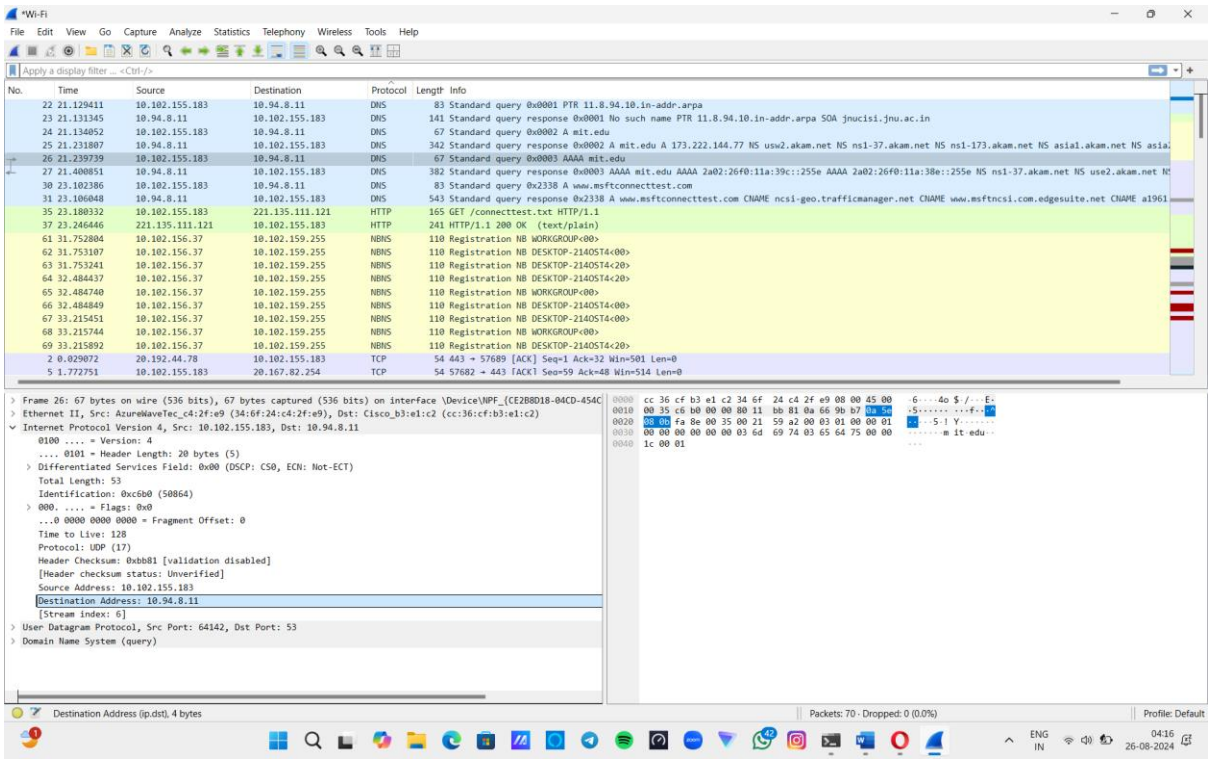
The destination port for the DNS query message is 53.



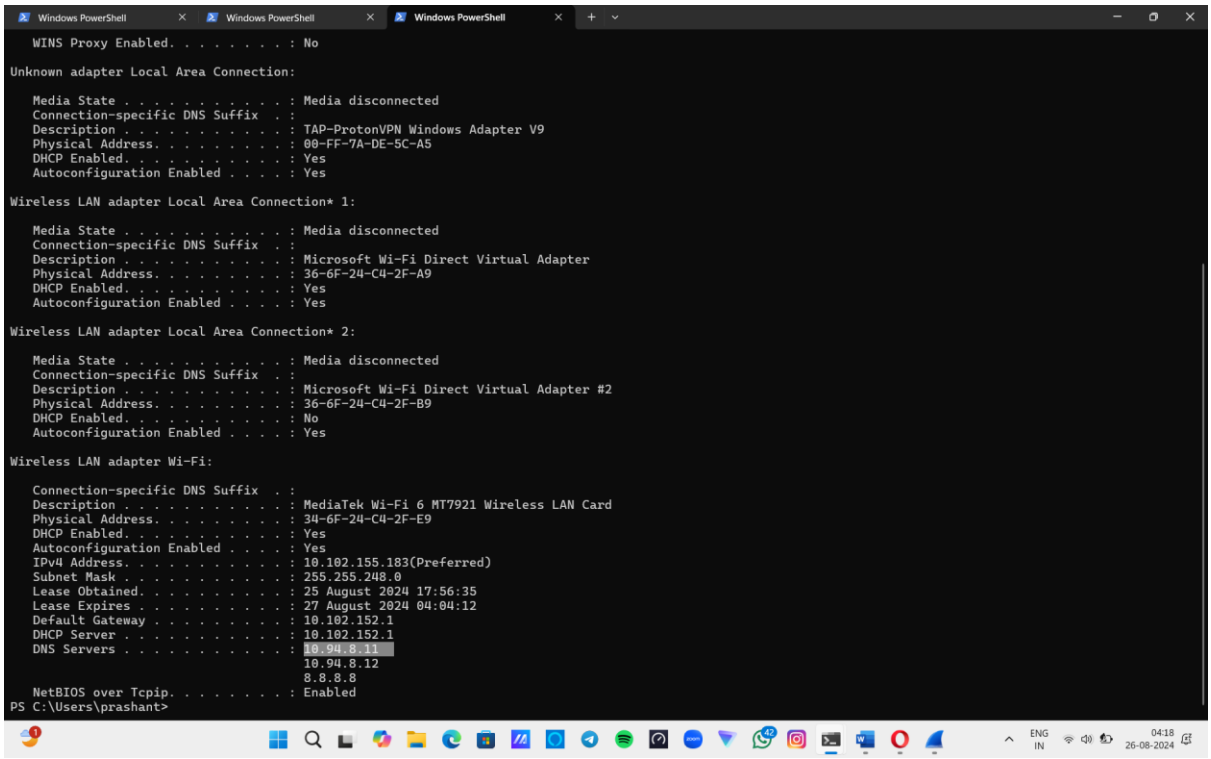
The source port of DNS response message is 53.

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

Answer:



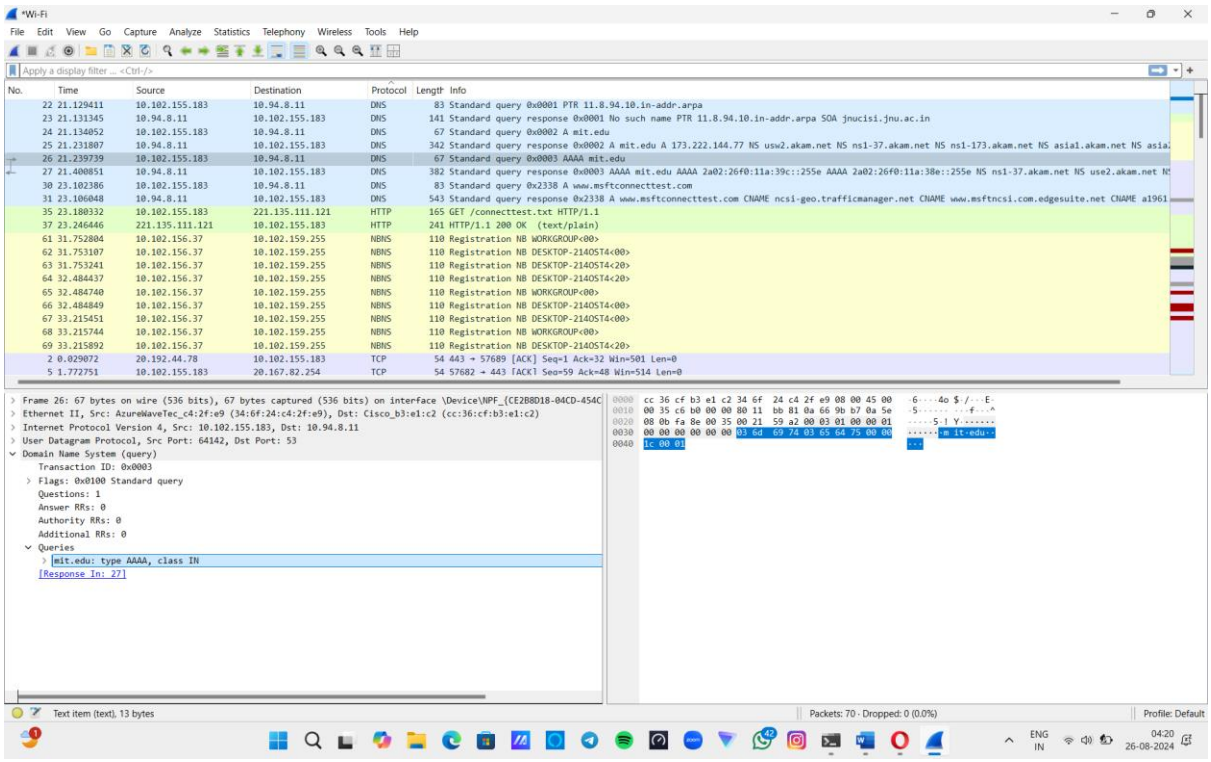
The DNS query message is sent to 10.94.8.11



Yes this is the IP address of default local DNS server.

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

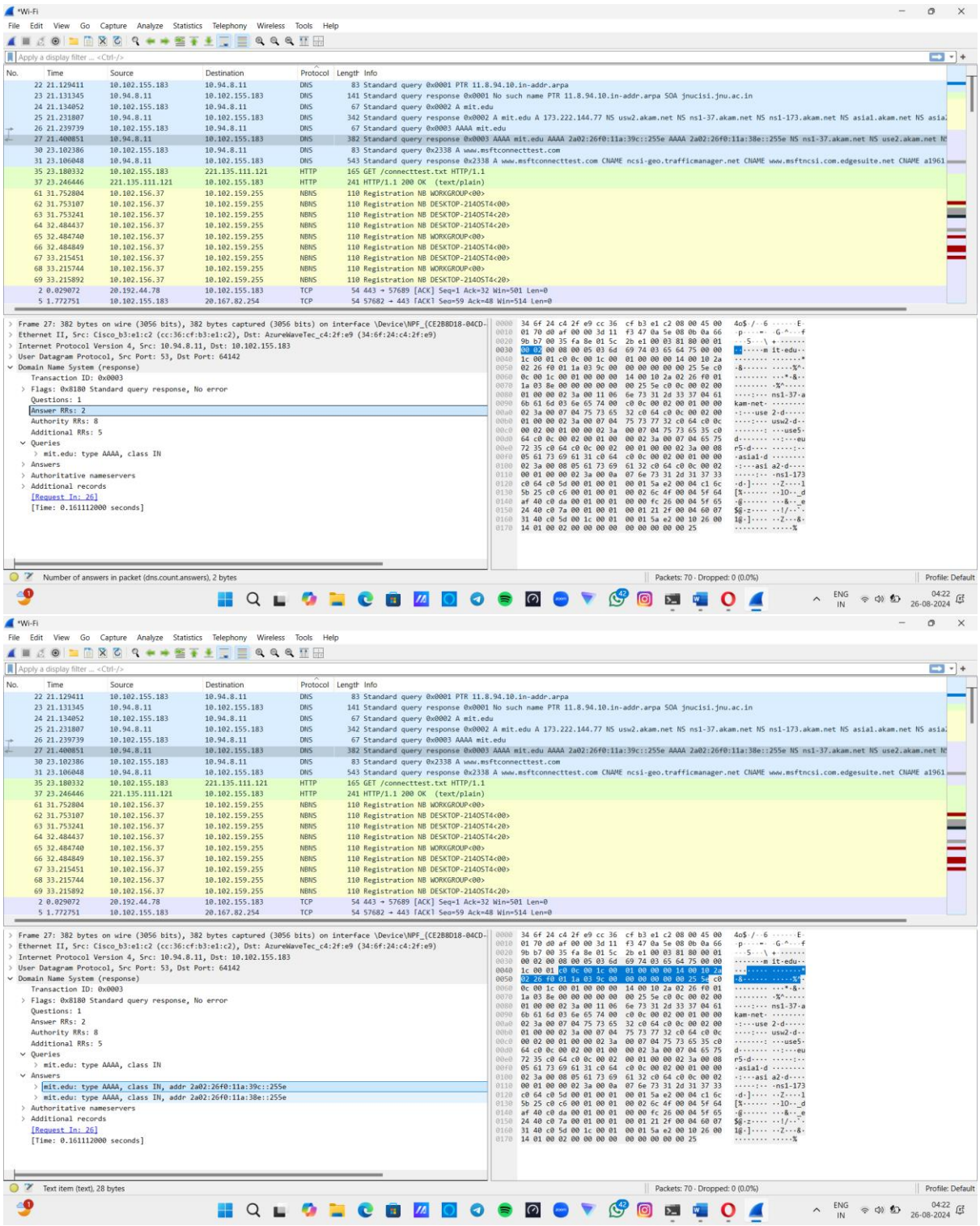
Answer:



The DNS query is of type AAAA.
No it does not ans answers.

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

Answer:

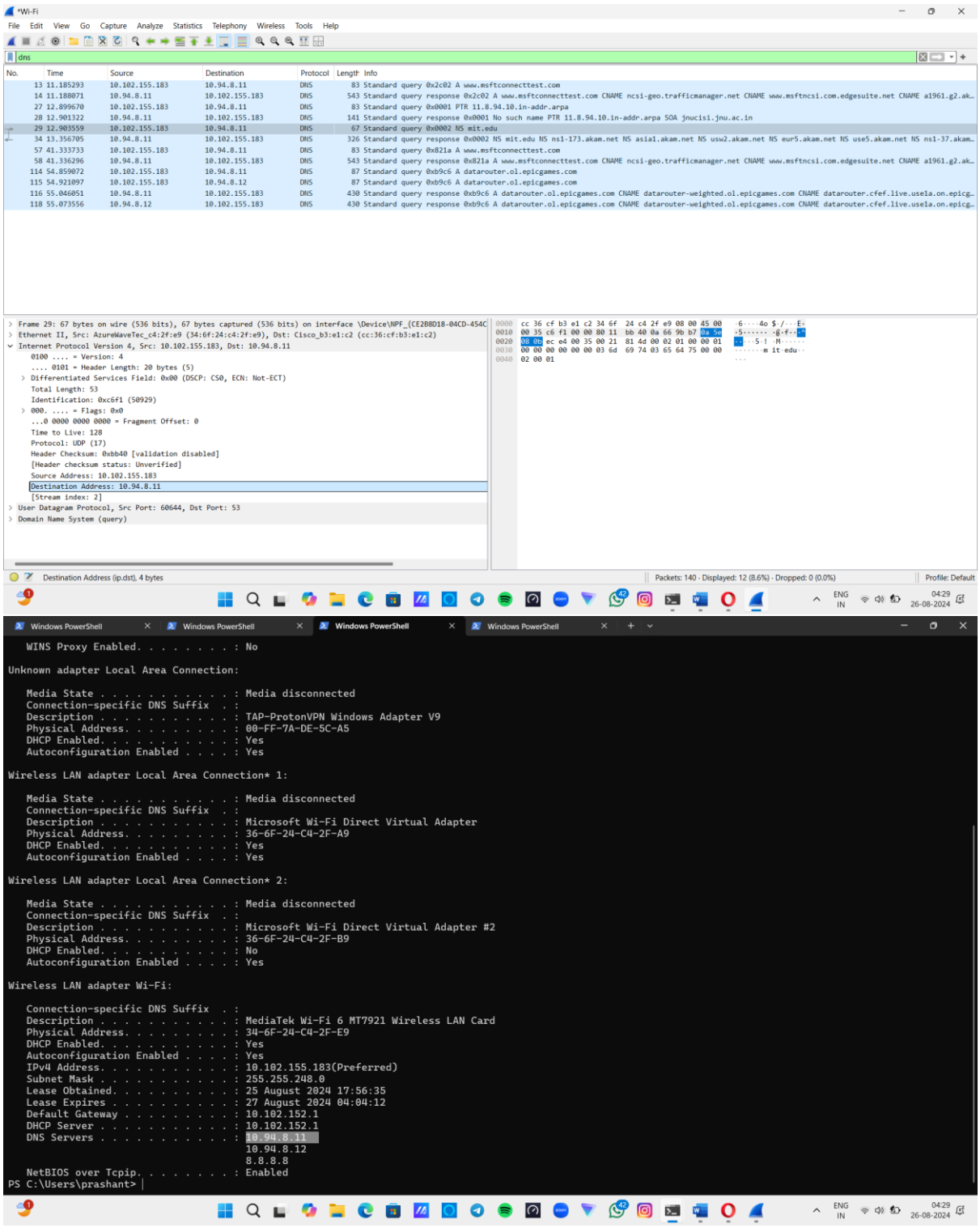


The response has 2 answers.

15. Provide a screenshot.

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

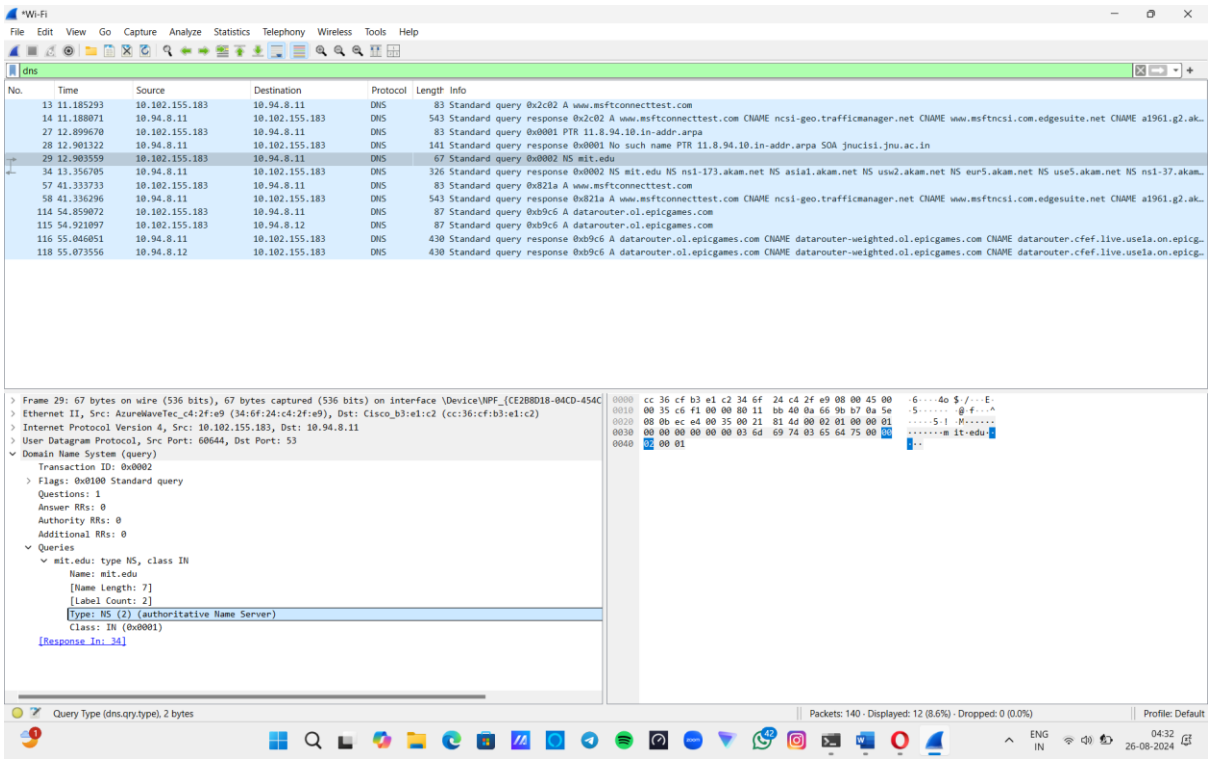
Answer:



Yes, this is my default DNS server.

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

Answer:

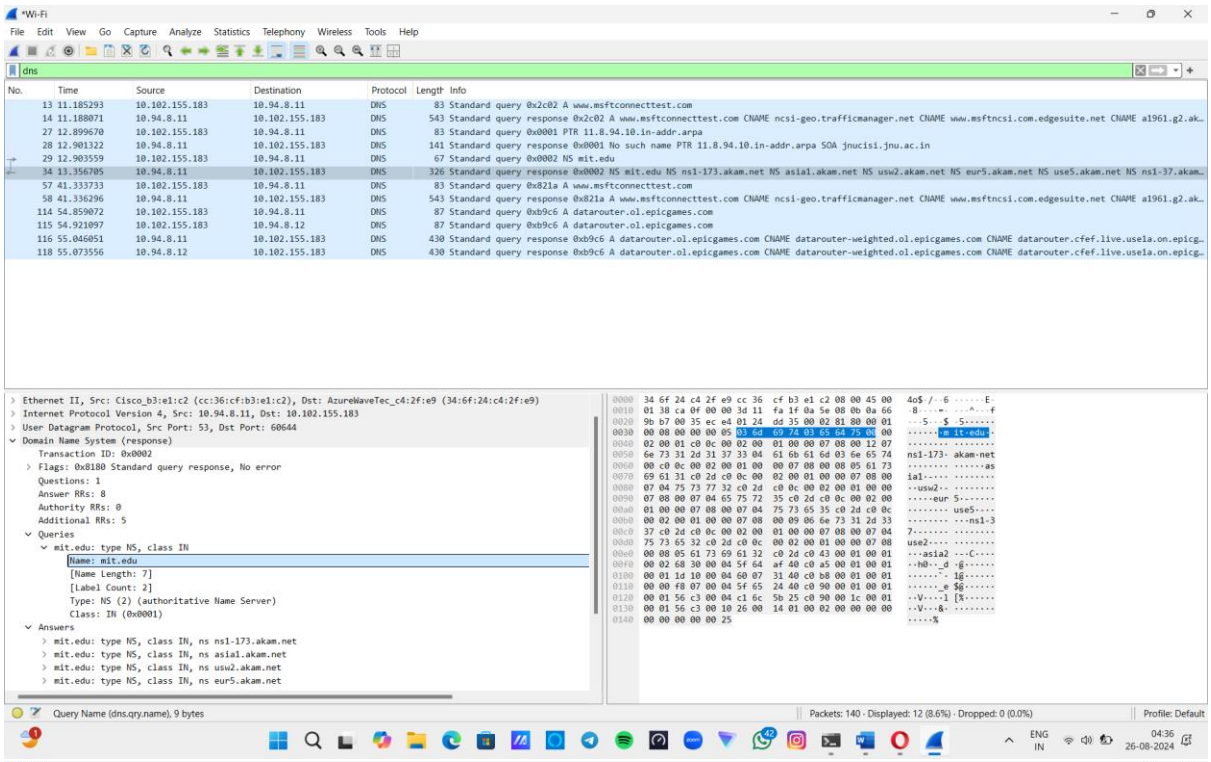


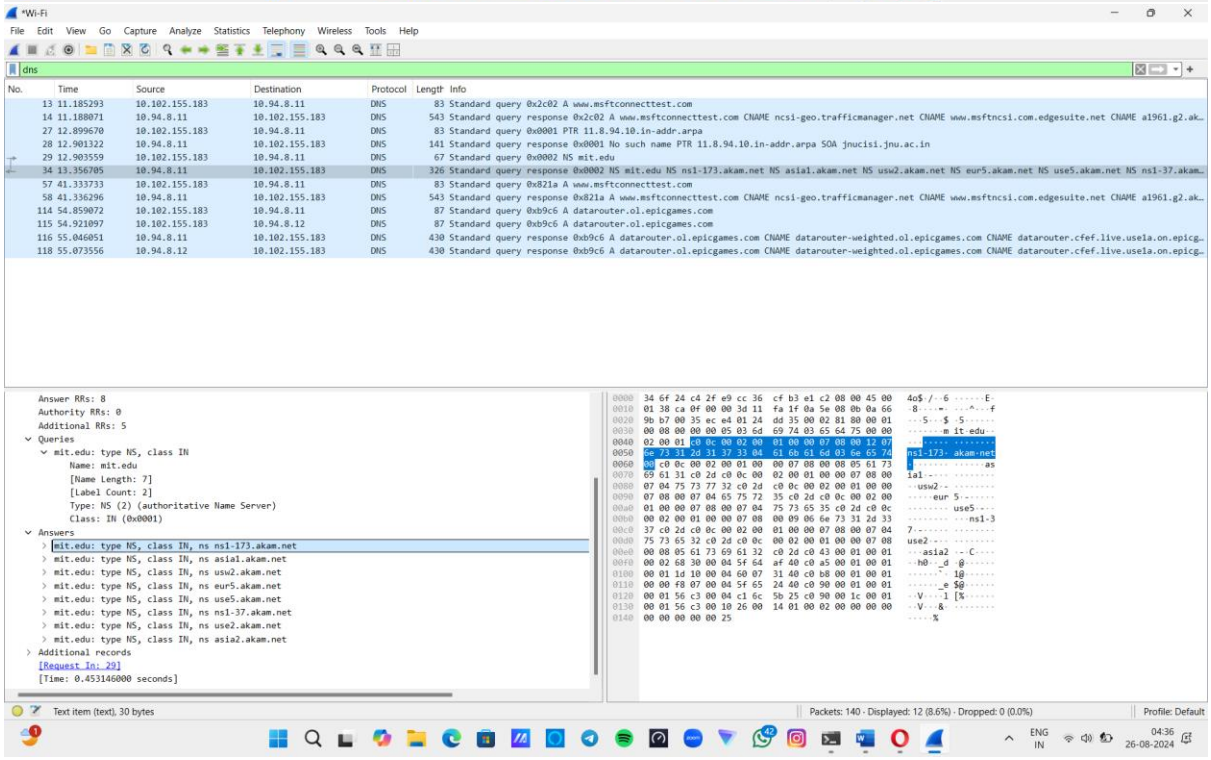
It is of type NS.

No, the query message does not contain any answers.

18. 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:



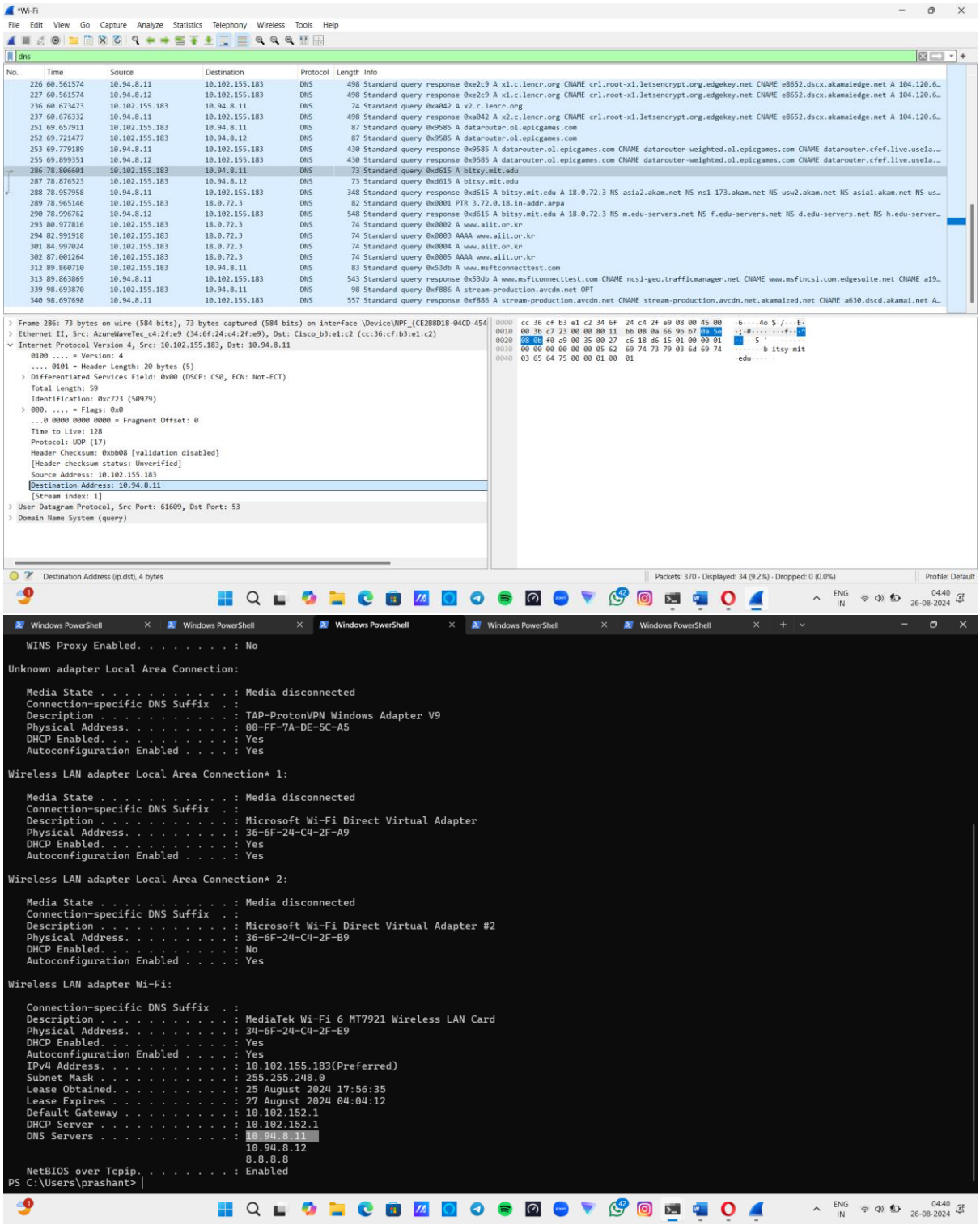


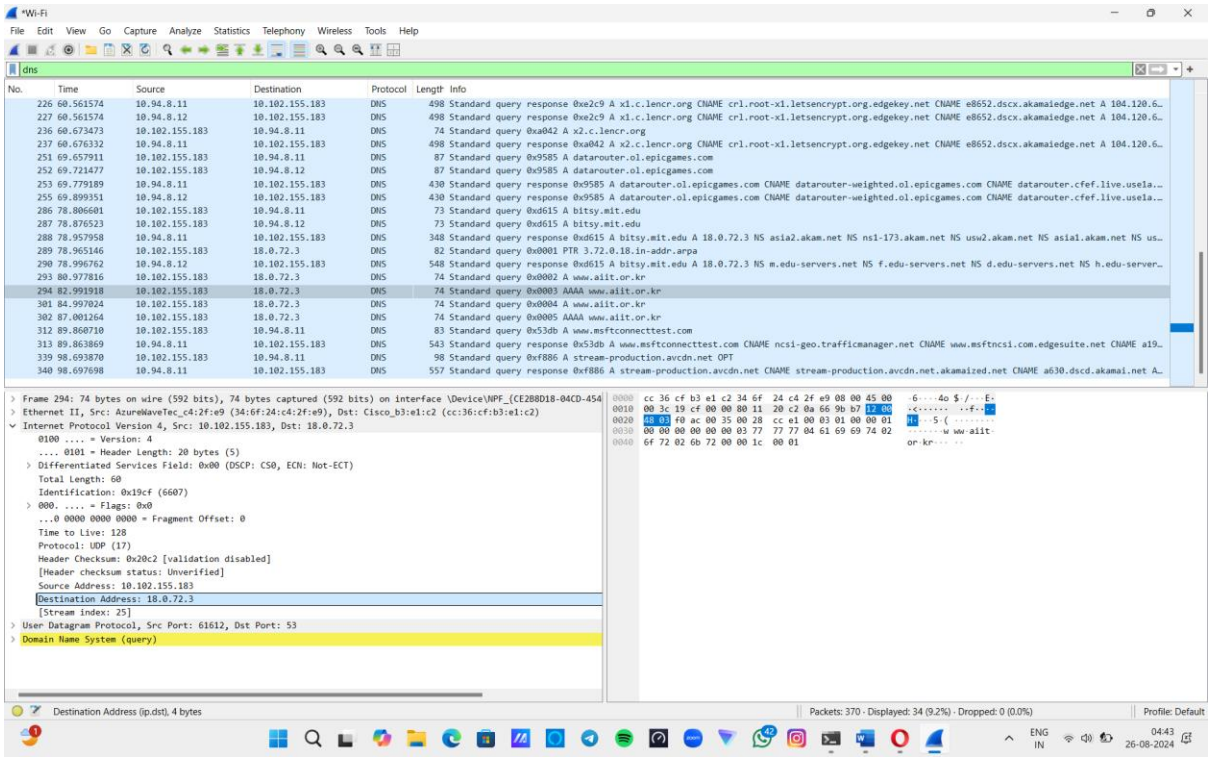
19. Provide a screenshot.

20. 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?

Answers:

Yes it corresponds to the local default DNS servers.

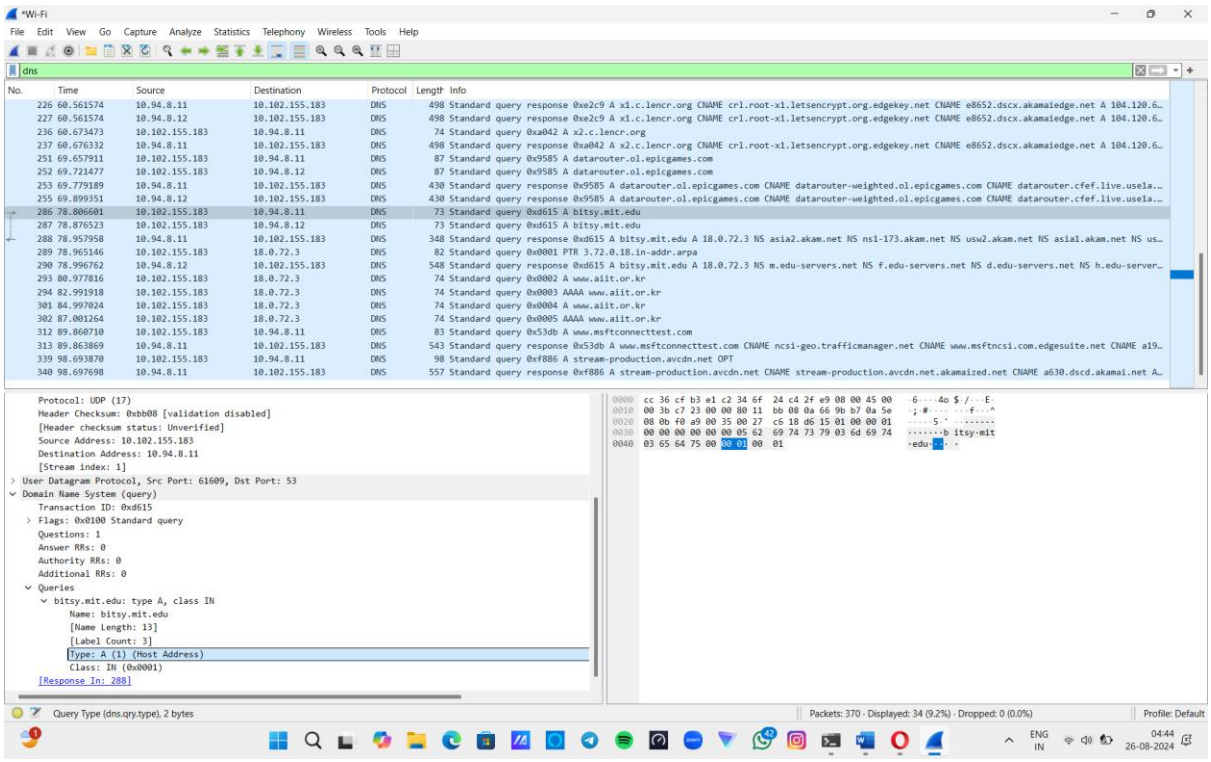




Here it is different

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

Answer:

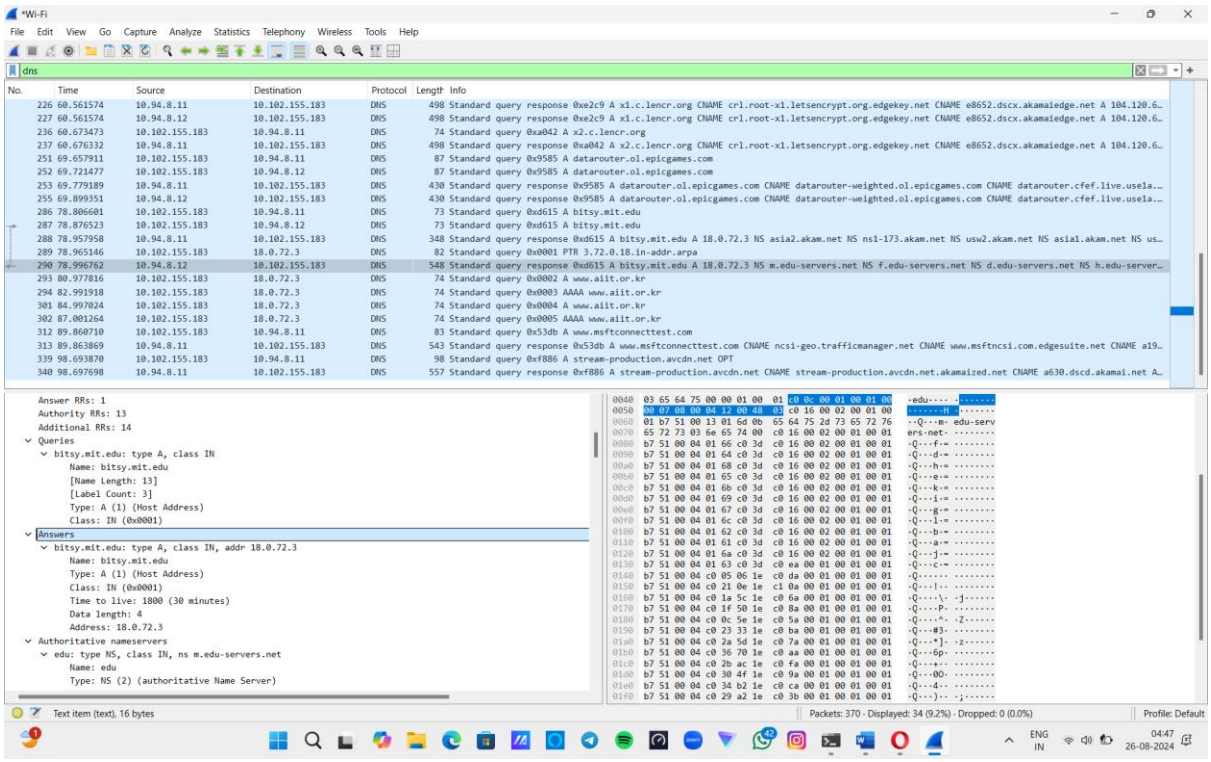


Type:A.

Answers: 0

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

Answer:



There is one answer.

23. Provide a screenshot.