

Computer Network: Wireshark DNS

Assignment 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

- 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.
*** Request to Unknown timed-out
```

IP Address-128.232.132.8

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

Answer:

No.	Time	Source	Destination	Protocol	Length	Info
11	1.036050	10.102.155.183	10.94.8.11	DNS	81	Standard query 0x5e95 HTTPS update.googleapis.com
12	1.036078	10.102.155.183	10.94.8.11	DNS	81	Standard query 0xc236 A update.googleapis.com
13	1.038939	10.94.8.11	10.102.155.183	DNS	352	Standard query response 0xc236 A update.googleapis.com A 142.250.183.163 NS ns3.google.com NS ns4.google.com NS ns2.google.com NS ns1.google.com
19	1.183731	10.94.8.11	10.102.155.183	DNS	198	Standard query response 0x5e95 HTTPS update.googleapis.com SOA ns1.google.com
59	4.728643	10.102.155.183	10.94.8.11	DNS	83	Standard query 0x6250 A www.msftconnecttest.com
60	4.793693	10.102.155.183	10.94.8.11	DNS	83	Standard query 0x6250 A www.msftconnecttest.com
61	4.794796	10.94.8.11	10.102.155.183	DNS	543	Standard query response 0x6250 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a19...
62	4.797071	10.94.8.12	10.102.155.183	DNS	543	Standard query response 0x6250 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.net CNAME a19...
173	15.519018	10.102.155.183	10.94.8.11	DNS	72	Standard query 0x7710 A www.ietf.org
174	15.519244	10.102.155.183	10.94.8.11	DNS	72	Standard query 0xc606 HTTPS www.ietf.org
176	15.524358	10.102.155.183	10.94.8.11	DNS	79	Standard query 0x2c27 A sitecheck.opera.com
181	15.525139	10.102.155.183	10.94.8.11	DNS	79	Standard query 0x4202 HTTPS sitecheck.opera.com
189	15.557482	10.102.155.183	10.94.8.11	DNS	72	Standard query 0x6948 A www.ietf.org
190	15.557440	10.102.155.183	10.94.8.11	DNS	72	Standard query 0x2bcc HTTPS www.ietf.org
191	15.662771	10.94.8.11	10.102.155.183	DNS	506	Standard query response 0x7710 A www.ietf.org A 104.16.45.99 A 104.16.44.99 NS c0.org.afiliias-nst.info NS b2.org.afiliias-nst.org NS a2.or...
192	15.663380	10.94.8.11	10.102.155.183	DNS	547	Standard query response 0xc00e HTTPS www.ietf.org HTTPS NS c0.org.afiliias-nst.info NS b2.org.afiliias-nst.org NS a2.org.afiliias-nst.info NS...
193	15.665073	10.94.8.11	10.102.155.183	DNS	547	Standard query response 0x2bcc HTTPS www.ietf.org HTTPS NS b2.org.afiliias-nst.info NS c0.org.afiliias-nst.org NS b0.org.afiliias-nst.org NS...
194	15.665168	10.94.8.11	10.102.155.183	DNS	506	Standard query response 0x6948 A www.ietf.org A 104.16.44.99 A 104.16.45.99 NS d0.org.afiliias-nst.org NS a0.org.afiliias-nst.info NS c0.or...
225	16.080711	10.94.8.11	10.102.155.183	DNS	224	Standard query response 0x4202 HTTPS sitecheck.opera.com CNAME sitecheck.geo.opera.com CNAME ams-sitecheck.opera.com CNAME ams.lb.opera.t...
226	16.336822	10.94.8.11	10.102.155.183	DNS	530	Standard query response 0x2c27 A sitecheck.opera.com CNAME sitecheck.geo.opera.com CNAME sitecheck.opera.com CNAME trn.lb.opera.techn...
251	16.891143	10.102.155.183	10.94.8.11	DNS	75	Standard query 0xb20f A static.ietf.org
252	16.891185	10.102.155.183	10.94.8.11	DNS	75	Standard query 0xb040 HTTPS static.ietf.org

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:



*Wi-Fi

No.	Time	Source	Destination	Protocol	Length	Info
11	1.036050	10.102.155.183	10.94.8.11	DNS	81	Standard query 0x5e95 HTTPS update.g...
12	1.036078	10.102.155.183	10.94.8.11	DNS	81	Standard query 0xc236 A update.g...
13	1.038939	10.94.8.11	10.102.155.183	DNS	352	Standard query response 0xc236 A update.g...
19	1.183731	10.94.8.11	10.102.155.183	DNS	138	Standard query response 0x5e95 HTTPS update.g...
59	4.728643	10.102.155.183	10.94.8.11	DNS	83	Standard query 0x8250 A www.msft...
60	4.793693	10.102.155.183	10.94.8.12	DNS	83	Standard query 0x8250 A www.msft...
61	4.794708	10.94.8.11	10.102.155.183	DNS	543	Standard query response 0x8250 A www.msft...
62	4.797071	10.94.8.12	10.102.155.183	DNS	543	Standard query response 0x8250 A www.msft...
173	15.519018	10.102.155.183	10.94.8.11	DNS	72	Standard query 0x7710 A www.iet...
174	15.519244	10.102.155.183	10.94.8.11	DNS	72	Standard query 0xc60e HTTPS www.iet...
176	15.524358	10.102.155.183	10.94.8.11	DNS	79	Standard query 0x2c27 A sitecheck...
181	15.525139	10.102.155.183	10.94.8.11	DNS	79	Standard query 0x4202 HTTPS sitecheck...
189	15.557402	10.102.155.183	10.94.8.11	DNS	72	Standard query 0x6948 A www.iet...
190	15.557440	10.102.155.183	10.94.8.11	DNS	72	Standard query 0x2bcc HTTPS www.iet...
191	15.662771	10.94.8.11	10.102.155.183	DNS	506	Standard query response 0x7710 A www.iet...
192	15.663380	10.94.8.11	10.102.155.183	DNS	547	Standard query response 0xc60e HTTPS www.iet...
193	15.665073	10.94.8.11	10.102.155.183	DNS	547	Standard query response 0x2bcc A www.iet...
194	15.665168	10.94.8.11	10.102.155.183	DNS	506	Standard query response 0x6948 A www.iet...
225	16.080711	10.94.8.11	10.102.155.183	DNS	224	Standard query response 0x4202 HTTPS www.iet...
226	16.336822	10.94.8.11	10.102.155.183	DNS	530	Standard query response 0x2c27 A www.iet...
251	16.891143	10.102.155.183	10.94.8.11	DNS	75	Standard query 0xb20f A static.ip...
252	16.891185	10.102.155.183	10.94.8.11	DNS	75	Standard query 0xb040 HTTPS static.ip...

```

> Frame 173: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{CE2B8D18-04CD-454...
> Ethernet II, Src: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9), Dst: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2)
> Internet Protocol Version 4, Src: 10.102.155.183, Dst: 10.94.8.11
< User Datagram Protocol, Src Port: 53867, Dst Port: 53
  Source Port: 53867
  Destination Port: 53
  Length: 38
  Checksum: 0xdb25 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
    [Stream Packet Number: 1]
  > [Timestamps]
    UDP payload (30 bytes)
  > Domain Name System (query)

```

Destination Port of the query is – 53

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.102.155.183

No.	Time	Source	Destination	Protocol	Length	Info
11	1.036050	10.102.155.183	10.94.8.11	DNS	81	Standard query 0x5e95 HTTPS update
12	1.036078	10.102.155.183	10.94.8.11	DNS	81	Standard query 0xc236 A update
13	1.038939	10.94.8.11	10.102.155.183	DNS	352	Standard query response 0xc236
19	1.183731	10.94.8.11	10.102.155.183	DNS	138	Standard query response 0x5e95
59	4.728643	10.102.155.183	10.94.8.11	DNS	83	Standard query 0x8250 A www.ms
60	4.793693	10.102.155.183	10.94.8.12	DNS	83	Standard query 0x8250 A www.ms
61	4.794708	10.94.8.11	10.102.155.183	DNS	543	Standard query response 0x8256
62	4.797071	10.94.8.12	10.102.155.183	DNS	543	Standard query response 0x8256
173	15.519018	10.102.155.183	10.94.8.11	DNS	72	Standard query 0x7710 A www.ie
174	15.519244	10.102.155.183	10.94.8.11	DNS	72	Standard query 0xc60e HTTPS wv
176	15.524358	10.102.155.183	10.94.8.11	DNS	79	Standard query 0x2c27 A sitech
181	15.525139	10.102.155.183	10.94.8.11	DNS	79	Standard query 0x4202 HTTPS s
189	15.557402	10.102.155.183	10.94.8.11	DNS	72	Standard query 0x6948 A www.ie
190	15.557440	10.102.155.183	10.94.8.11	DNS	72	Standard query 0xbcc HTTPS wv
191	15.662771	10.94.8.11	10.102.155.183	DNS	506	Standard query response 0x7710
192	15.663380	10.94.8.11	10.102.155.183	DNS	547	Standard query response 0xc60e
193	15.665073	10.94.8.11	10.102.155.183	DNS	547	Standard query response 0x2bcc
194	15.665168	10.94.8.11	10.102.155.183	DNS	506	Standard query response 0x6948
225	16.080711	10.94.8.11	10.102.155.183	DNS	224	Standard query response 0x4202
226	16.336822	10.94.8.11	10.102.155.183	DNS	530	Standard query response 0x2c27
251	16.891143	10.102.155.183	10.94.8.11	DNS	75	Standard query 0xb20f A static
252	16.891185	10.102.155.183	10.94.8.11	DNS	75	Standard query 0xb040 HTTPS s

```

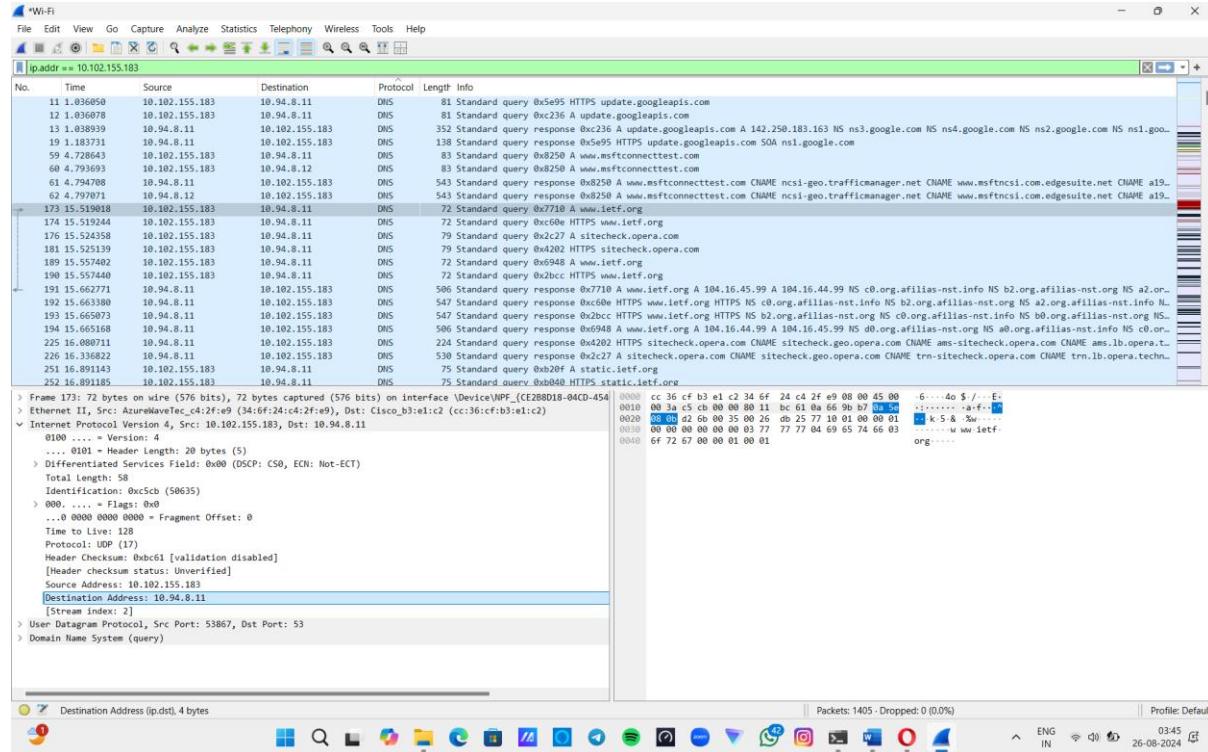
> Frame 191: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface \Device\NPF_{CE2B8D18-04CD-4A9E-AE0C-000000000000
> Ethernet II, Src: Cisco_b3:e1:c2 (cc:36:cf:b3:e1:c2), Dst: AzureWaveTec_c4:2f:e9 (34:6f:24:c4:2f:e9)
> Internet Protocol Version 4, Src: 10.94.8.11, Dst: 10.102.155.183
< User Datagram Protocol, Src Port: 53, Dst Port: 53867
    Source Port: 53
    Destination Port: 53867
    Length: 472
    Checksum: 0xe2c2 [unverified]
        [Checksum Status: Unverified]
        [Stream index: 5]
        [Stream Packet Number: 2]
    > [Timestamps]
        UDP payload (464 bytes)
    > Domain Name System (response)

```

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:



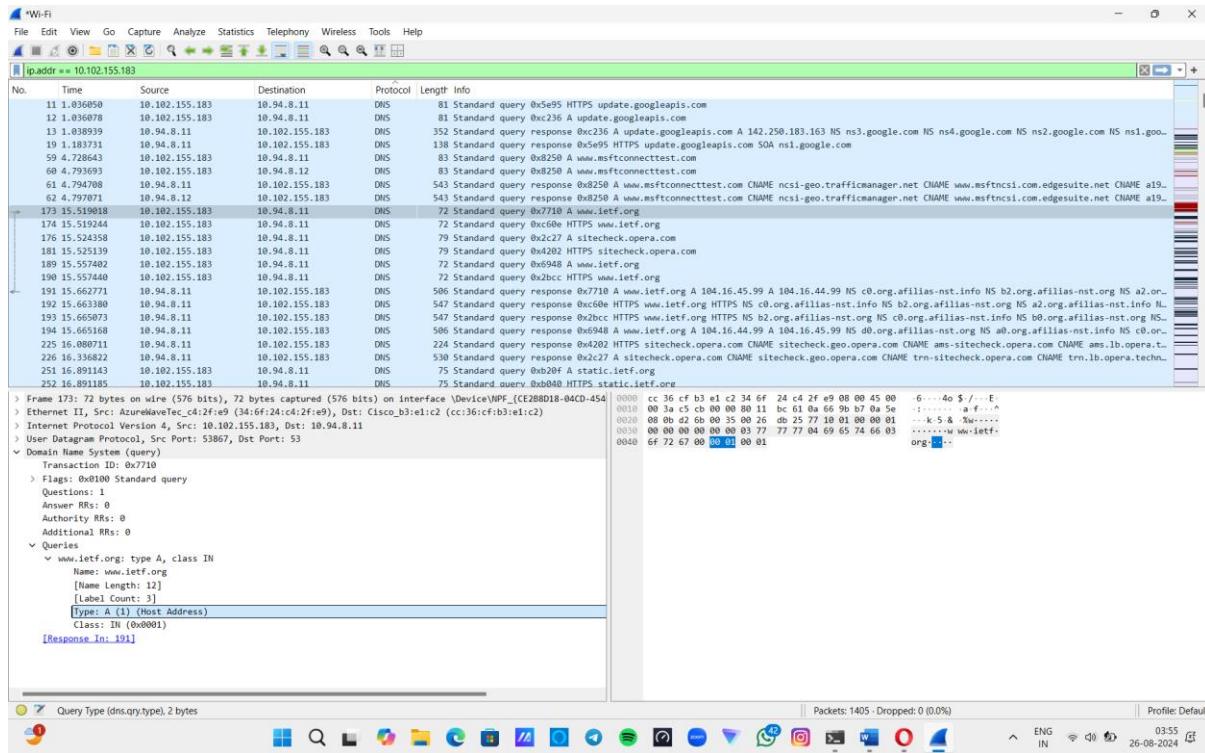
The DNS query message is sent to IP Address 10.94.8.11

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”?

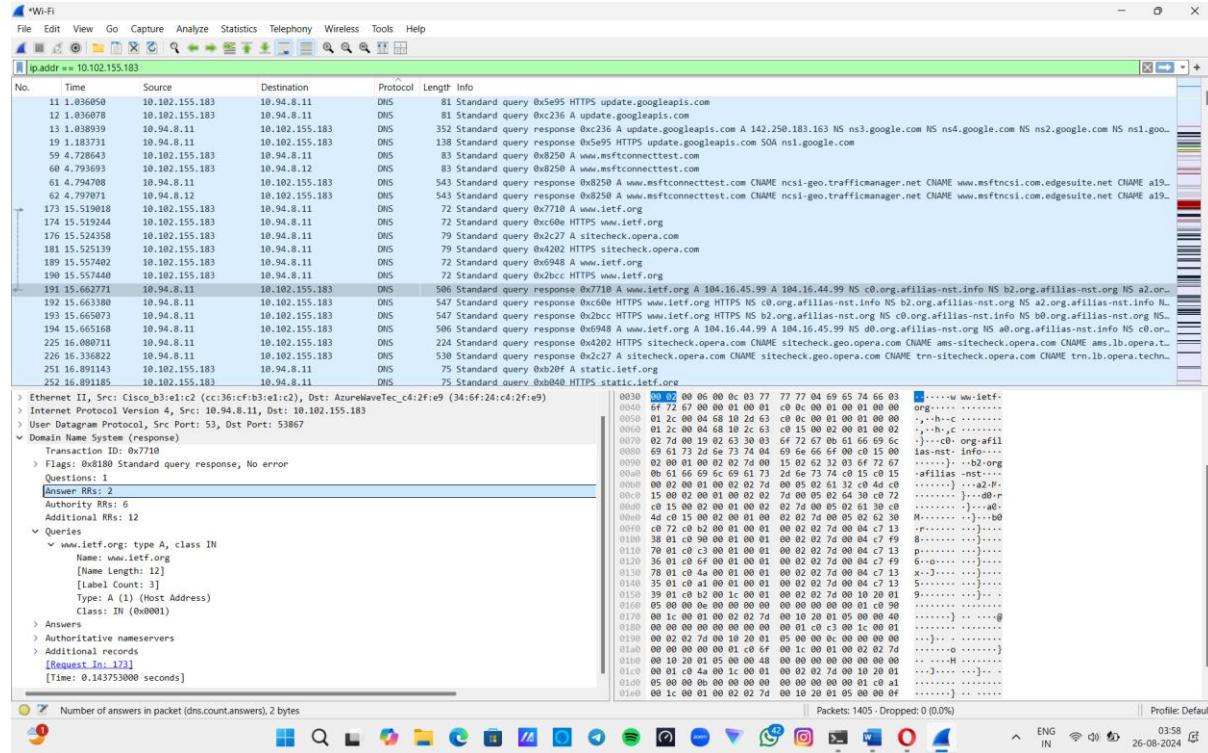
Answer:



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

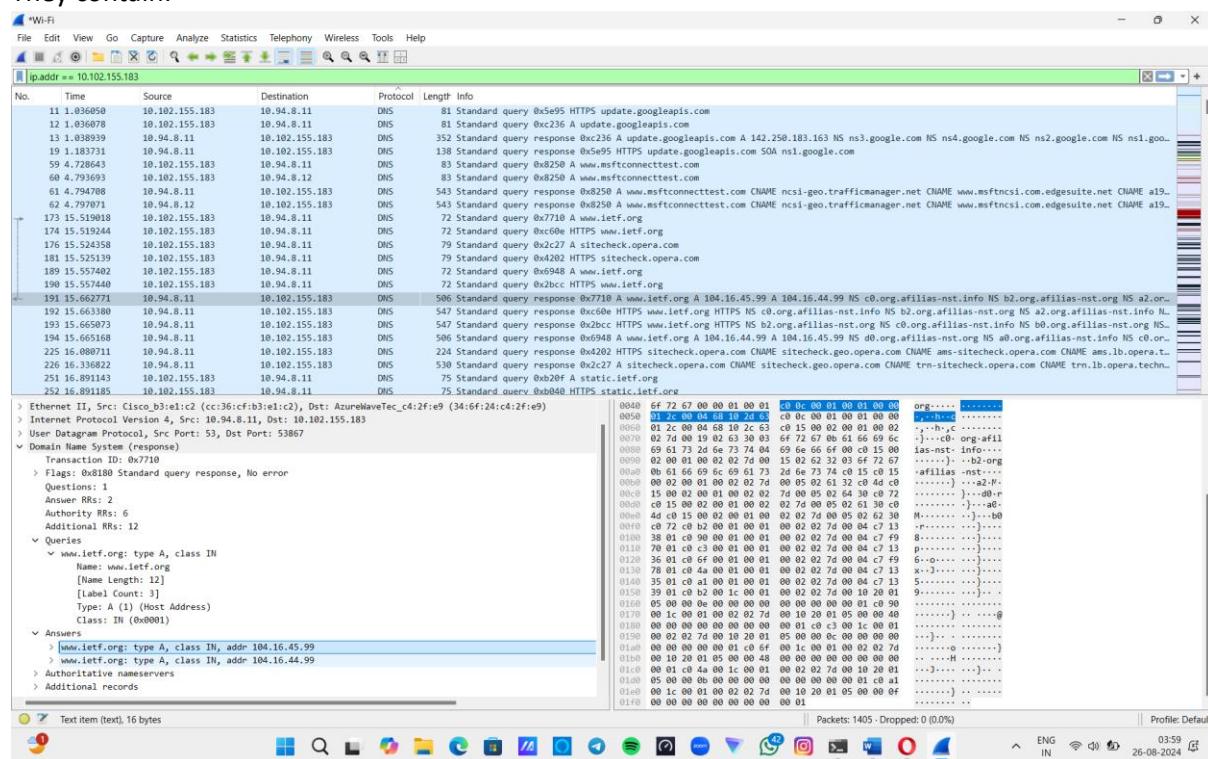
8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Answers:



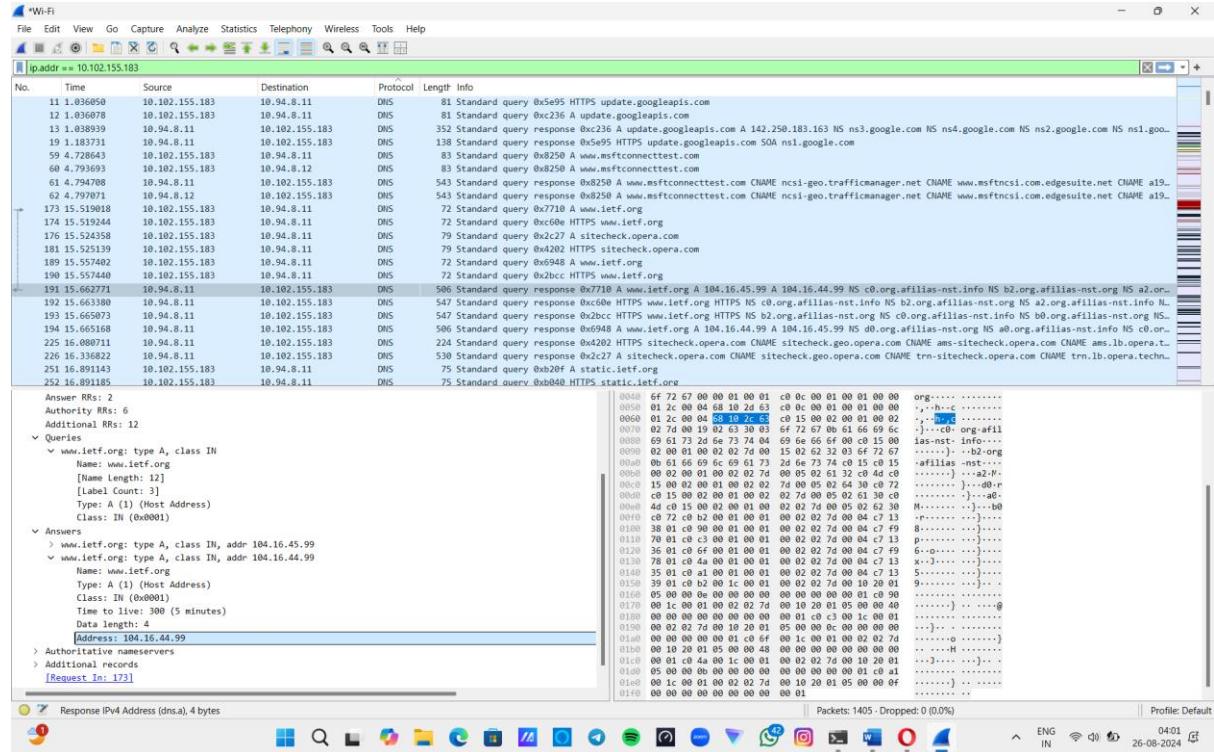
There are two answers.

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.

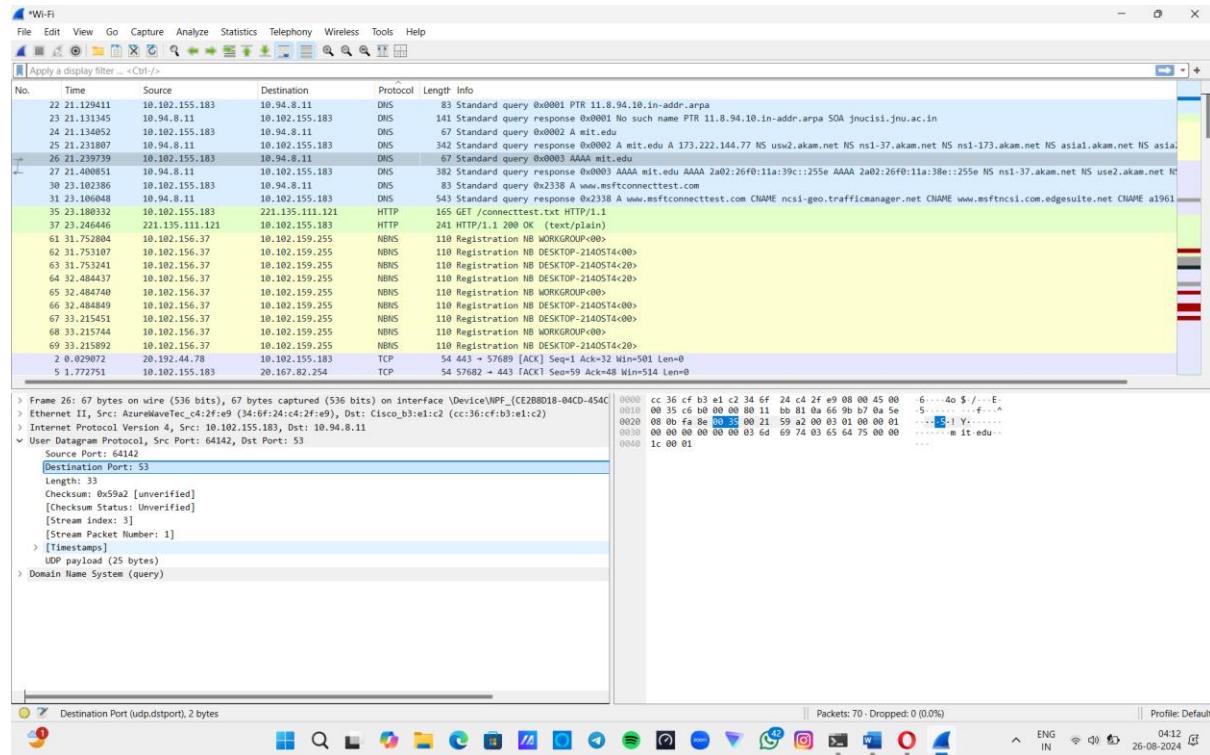
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Answers:

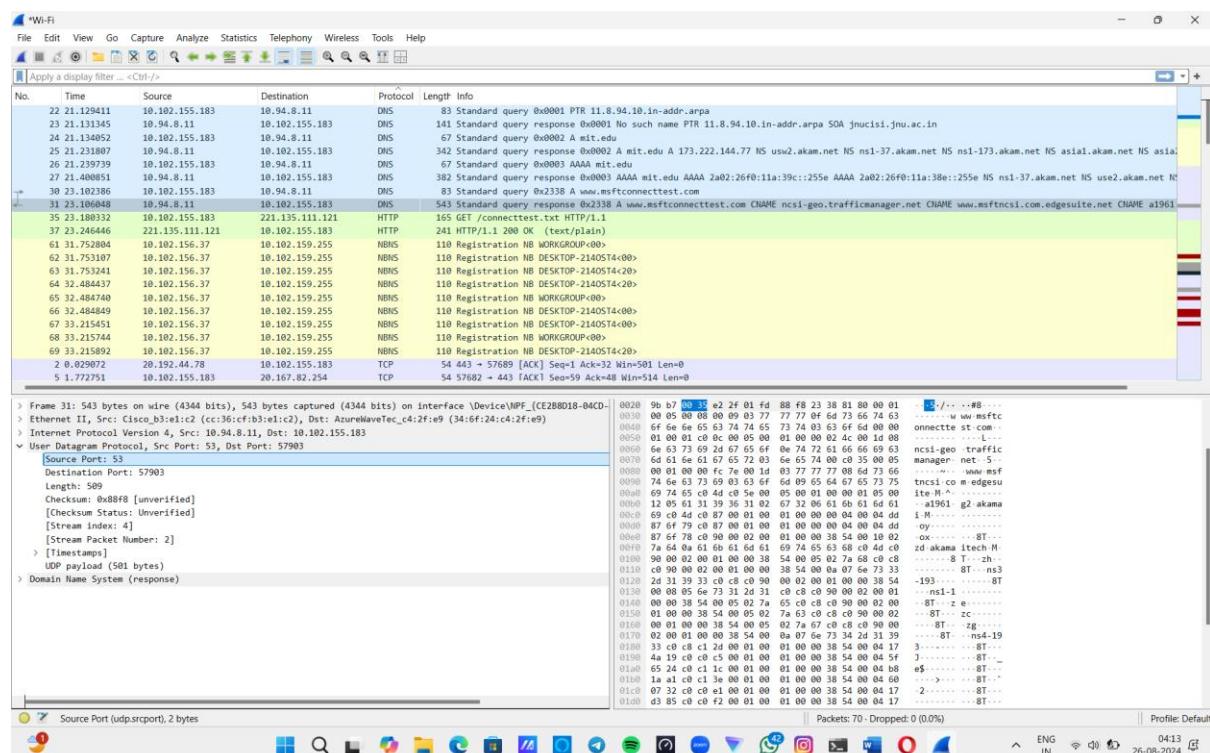
No the host issue new DNS queries.

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

Answer:



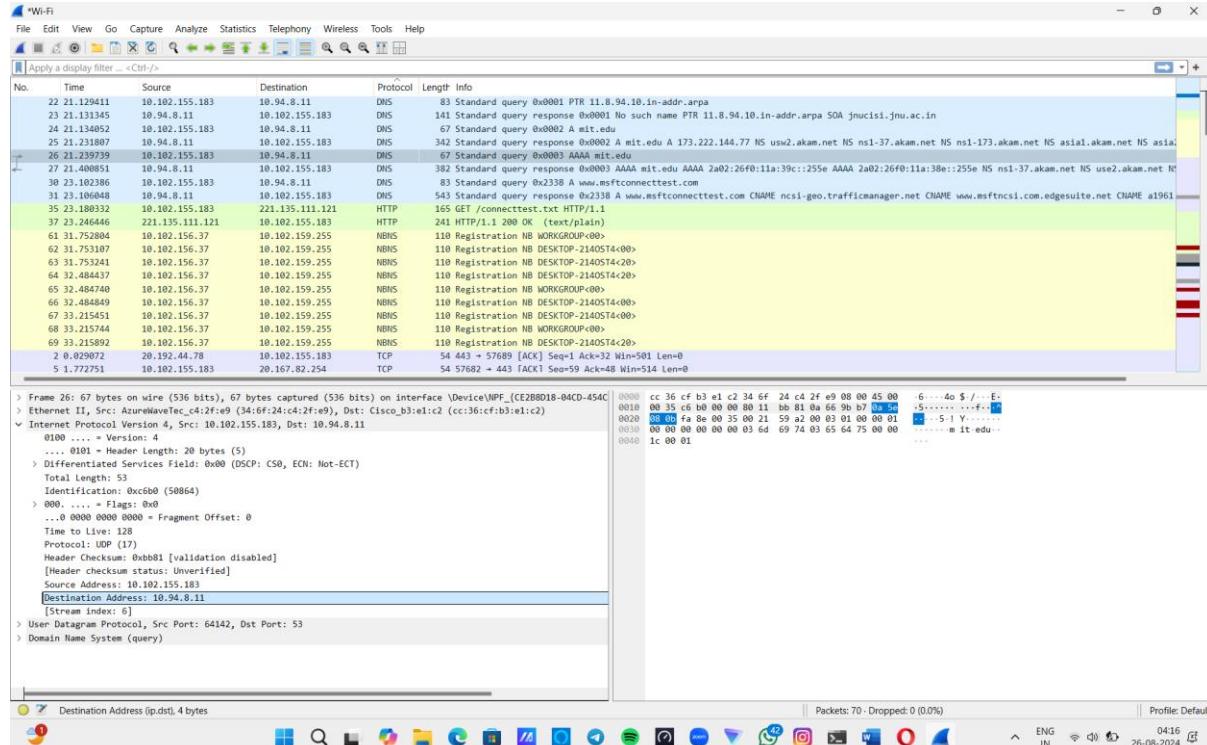
The destination port for the DNS query message is 53.



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:



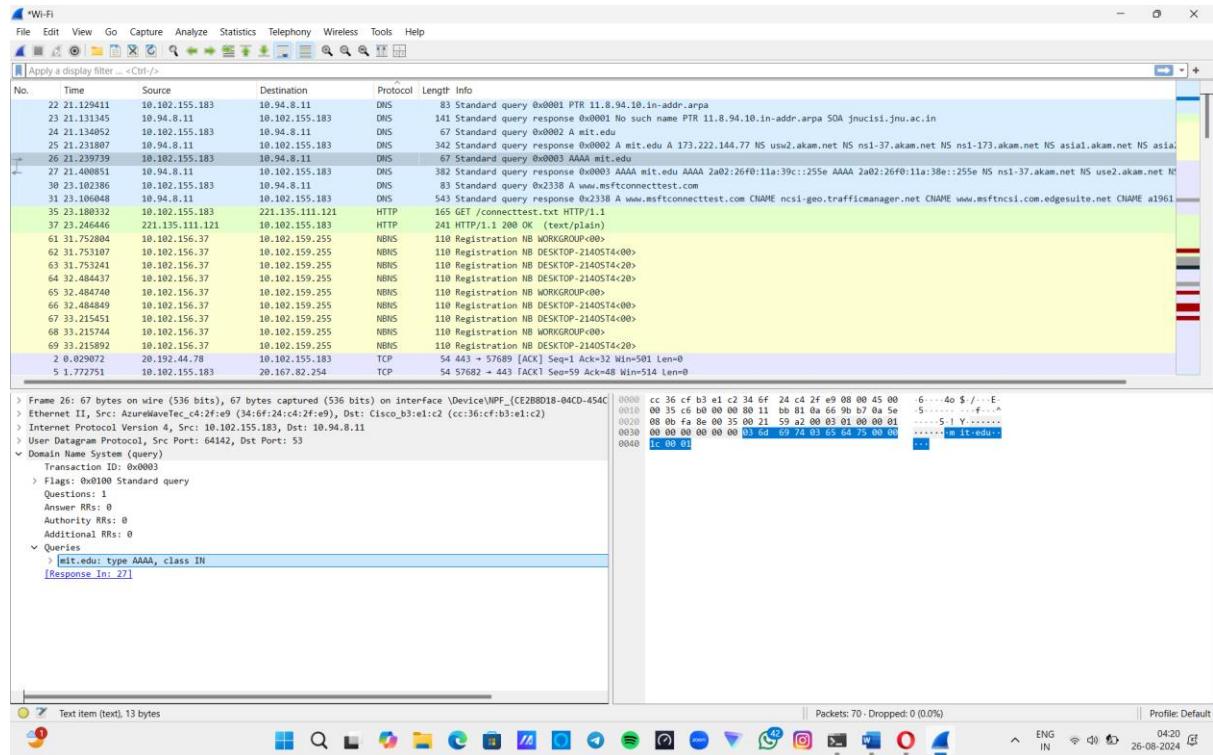
The DNS query message is sent to 10.94.8.11

```
Windows PowerShell * Windows PowerShell * Windows PowerShell * + 
WINS Proxy Enabled. . . . . : No
Unknown adapter Local Area Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .
Description . . . . . : TAP-ProtonVPN Windows Adapter V9
Physical Address. . . . . : 00-FF-7A-DE-5C-A5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 36-6F-24-C4-2F-A9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
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 04:04:12
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
PS C:\Users\prashant>
```

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 Wi-Fi Network Monitor interface displays network traffic. The top window shows a list of network packets, with the 27th packet selected. The bottom windows provide detailed analysis for this selected packet.

Detailed Analysis of Selected Packet (Frame 27):

- Protocol:** DNS
- Source:** 10.102.155.183
- Destination:** 10.94.8.11
- Length:** 382 bytes on wire (3056 bits), 382 bytes captured (3056 bits) on interface \Device\NPF_{CE2B8D18-04CD-4...
- Info:** 83 Standard query 0x0001 PTR 11.8.94.10.in-addr.arpa

Selected Response (Frame 27):

- Protocol:** DNS
- Source:** 10.94.8.11
- Destination:** 10.102.155.183
- Length:** 382 bytes on wire (3056 bits), 382 bytes captured (3056 bits) on interface \Device\NPF_{CE2B8D18-04CD-4...
- Info:** 342 Standard query response 0x0002 A mit.edu

Selected Response (Frame 27):

- Protocol:** DNS
- Source:** 10.94.8.11
- Destination:** 10.102.155.183
- Length:** 382 bytes on wire (3056 bits), 382 bytes captured (3056 bits) on interface \Device\NPF_{CE2B8D18-04CD-4...
- Info:** 342 Standard query response 0x0002 AAAA mit.edu

Selected Response (Frame 27):

- Protocol:** HTTP
- Source:** 10.102.155.183
- Destination:** 10.94.8.11
- Length:** 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{CE2B8D18-04CD-4...
- Info:** 165 GET /connecttest.txt HTTP/1.1

Selected Response (Frame 27):

- Protocol:** TCP
- Source:** 10.102.155.183
- Destination:** 10.94.8.11
- Length:** 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{CE2B8D18-04CD-4...
- Info:** 54 443 → 57689 [ACK] Seq=1 Ack=32 Win=501 Len=0

Selected Response (Frame 27):

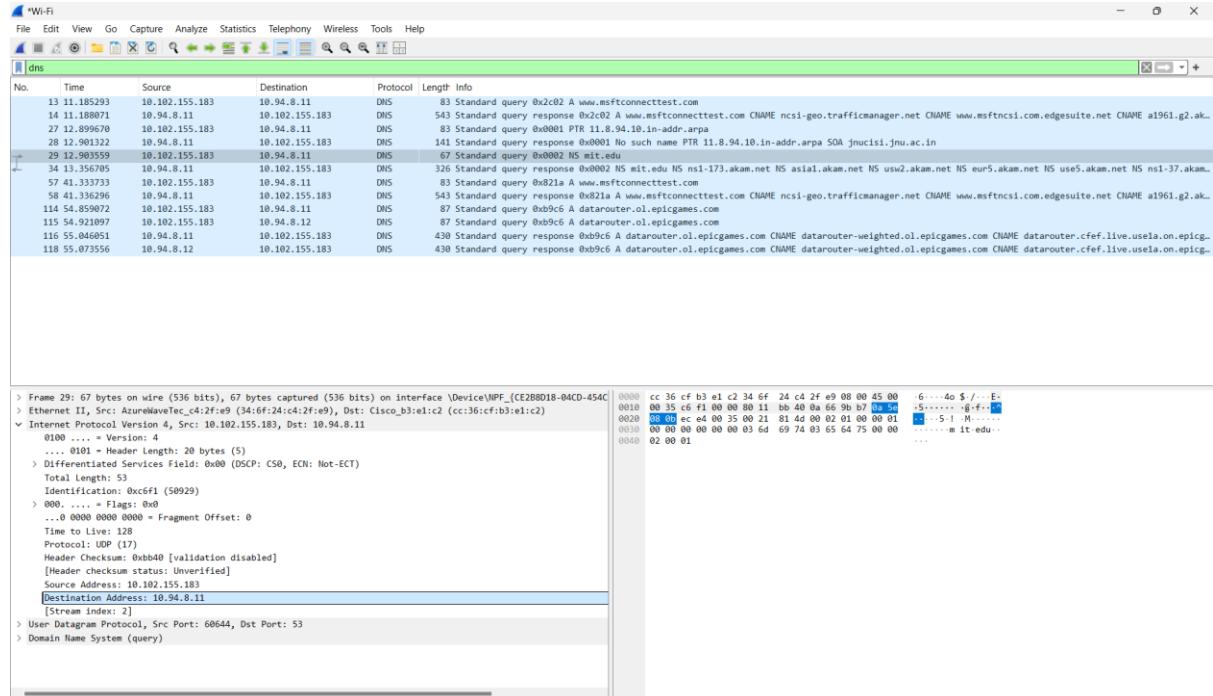
- Protocol:** TCP
- Source:** 10.102.155.183
- Destination:** 20.167.82.254
- Length:** 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{CE2B8D18-04CD-4...
- Info:** 54 57682 → 443 [ACK] Seq=59 Ack=48 Win=514 Len=0

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:



The Wireshark interface shows a list of captured DNS packets. The selected packet is number 29, which is a DNS query from 10.94.8.11 to 10.102.155.183. The 'Info' column shows the query for 'www.msftconnecttest.com'. The packet details pane shows the raw hex and ASCII data for the DNS request, including the source and destination ports (53), the query type (A), and the domain name.

Selected Packet Details:

```

> Frame 29: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface '\Device\NPF_{CE2B8D18-D4CD-454C
> Ethernet II, Src: AzurLaneTec_c4:2f:e9 (34:6f:24:c4:2f:e9), Dst: Cisco_b3:e1:c2 (cc:36:c9:b3:e1:c2)
> Internet Protocol Version 4, Src: 10.102.155.183, Dst: 10.94.8.11
 0100... = Version: 4
  ...0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSSCP: CS0, ECN: Not-ECT)
    Total Length: 53
    Identification: 0xc6f1 (50929)
    ...000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xbba0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.102.155.183
    Destination Address: 10.94.8.11
    [Stream index: 2]
  > User Datagram Protocol, Src Port: 60644, Dst Port: 53
  > Domain Name System (query)

```

Windows PowerShell Session:

```

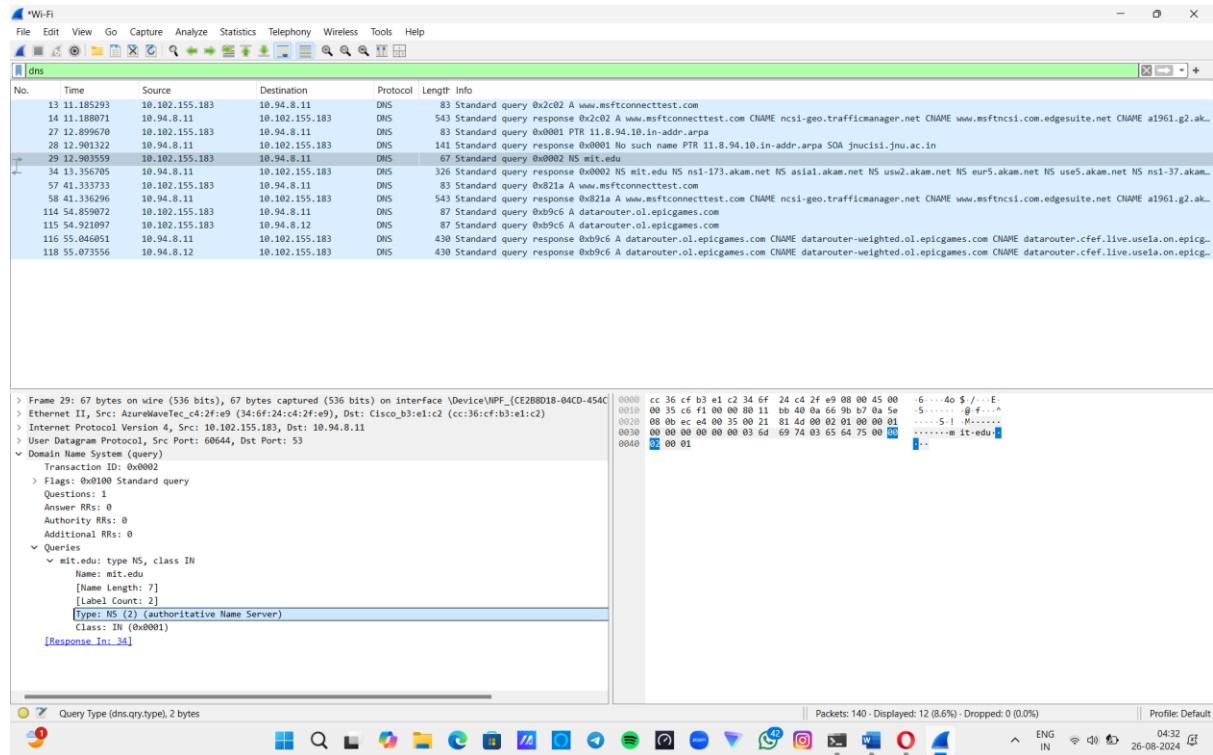
Destination Address (ip.dst), 4 bytes
Windows PowerShell
Windows PowerShell
Windows PowerShell
Windows PowerShell
Windows PowerShell
WINS Proxy Enabled. . . . . : No
Unknown adapter Local Area Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .
Description . . . . . : TAP-ProtonVPN Windows Adapter V9
Physical Address. . . . . : 00-FF-7A-DE-5C-A5
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Wireless LAN adapter Local Area Connection* 1:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 36-6F-24-C4-2F-A9
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Wireless LAN adapter Local Area Connection* 2:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 36-6F-24-C4-2F-B9
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
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 04:04:12
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
PS C:\Users\prashant>

```

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:

The Wireshark interface shows several DNS requests and responses. The main pane displays a list of captured packets, while the bottom pane provides detailed information for selected packets.

Selected DNS Response (Packet 14):

- Time:** 11.188071
- Source:** 10.94.8.11
- Destination:** 10.102.155.183
- Protocol:** DNS
- Length:** 45
- Info:** 83 Standard query 0x2c02 A www.msftconnecttest.com

Detailed Hex and ASCII Data:

```

0000  34 6f 24 c4 2f e9 cc 36 cf b3 e1 c2 00 00 45 00 4o$ / - 6 ..... E
0010  01 38 ca 0f 00 00 3d 11 fa 0f 0a 5e 08 00 0a 66 8 ... . ^ . f
0020  9b b7 00 35 ec e4 01 24 dd 35 00 02 81 80 00 01 ..-$. $ 5-----
0030  00 08 00 00 00 05 01 6d 69 74 03 65 64 75 00 00 ..... m it.edu
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... ns1-173.akam.net
0050  0e 73 31 2d 31 37 00 04 61 6b 61 64 03 6e 65 74 ns1-173.akam.net
0060  00 c0 0c 00 02 00 01 00 07 08 00 01 00 08 01 00 ..... as
0070  69 61 31 2d c0 0c 00 02 00 01 00 08 07 01 00 ..... iai.....
0080  07 04 75 00 77 32 c0 2d c0 0c 00 02 00 01 00 00 ..... usw2.....
0090  00 00 00 00 07 08 00 02 00 01 00 08 07 01 00 ..... eur 5....
00a0  01 00 00 07 08 00 07 04 75 73 65 35 c0 2d c0 0c ..... use5.....
00b0  00 02 00 01 00 00 07 08 00 09 06 6e 73 31 2d 33 ..... ns1-3
00c0  37 c0 2d c0 0c 00 02 00 01 00 08 07 08 00 07 04 7.....
00d0  75 73 65 35 c0 2d c0 0c 00 02 00 01 00 08 07 08 00 ..... use2.....
00e0  00 02 00 01 00 00 07 08 00 09 06 6e 73 31 2d 33 ..... ns1-173.akam.net
00f0  00 02 68 30 00 04 5f 64 af 40 c0 a5 00 01 00 01 ..... asia2.....
0100  00 01 1d 10 00 04 60 07 31 40 c0 b8 00 01 00 01 ..... hbo...d @.....
0110  00 00 f8 07 00 04 5f 65 24 40 c0 90 00 01 00 01 ..... e 56.....
0120  00 01 56 c3 00 04 21 63 5b 25 c0 90 00 01 00 01 ..... V...1 [%]...
0130  00 01 56 c3 00 00 1c 6c 5b 25 c0 90 00 01 00 01 ..... V...&.....
0140  00 00 00 00 00 25 ..... %

```

Selected DNS Response (Packet 14):

- Time:** 11.188071
- Source:** 10.94.8.11
- Destination:** 10.102.155.183
- Protocol:** DNS
- Length:** 45
- Info:** 83 Standard query 0x2c02 A www.msftconnecttest.com

Detailed Hex and ASCII Data:

```

0000  34 6f 24 c4 2f e9 cc 36 cf b3 e1 c2 00 00 45 00 4o$ / - 6 ..... E
0010  01 38 ca 0f 00 00 3d 11 fa 0f 0a 5e 08 00 0a 66 8 ... . ^ . f
0020  9b b7 00 35 ec e4 01 24 dd 35 00 02 81 80 00 01 ..-$. $ 5-----
0030  00 08 00 00 00 05 01 6d 69 74 03 65 64 75 00 00 ..... m it.edu
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... ns1-173.akam.net
0050  0e 73 31 2d 31 37 00 04 61 6b 61 64 03 6e 65 74 ns1-173.akam.net
0060  00 c0 0c 00 02 00 01 00 07 08 00 01 00 08 01 00 ..... as
0070  69 61 31 2d c0 0c 00 02 00 01 00 08 07 01 00 ..... iai.....
0080  07 04 75 00 77 32 c0 2d c0 0c 00 02 00 01 00 00 ..... usw2.....
0090  00 00 00 00 07 08 00 02 00 01 00 08 07 01 00 ..... eur 5....
00a0  01 00 00 07 08 00 07 04 75 73 65 35 c0 2d c0 0c ..... use5.....
00b0  00 02 00 01 00 00 07 08 00 09 06 6e 73 31 2d 33 ..... ns1-3
00c0  37 c0 2d c0 0c 00 02 00 01 00 08 07 08 00 07 04 7.....
00d0  75 73 65 35 c0 2d c0 0c 00 02 00 01 00 08 07 08 00 ..... use2.....
00e0  00 02 00 01 00 00 07 08 00 09 06 6e 73 31 2d 33 ..... ns1-173.akam.net
00f0  00 02 68 30 00 04 5f 64 af 40 c0 a5 00 01 00 01 ..... asia2.....
0100  00 01 1d 10 00 04 60 07 31 40 c0 b8 00 01 00 01 ..... hbo...d @.....
0110  00 00 f8 07 00 04 5f 65 24 40 c0 90 00 01 00 01 ..... e 56.....
0120  00 01 56 c3 00 04 21 63 5b 25 c0 90 00 01 00 01 ..... V...1 [%]...
0130  00 01 56 c3 00 00 1c 6c 5b 25 c0 90 00 01 00 01 ..... V...&.....
0140  00 00 00 00 00 25 ..... %

```

Selected DNS Response (Packet 14):

- Time:** 11.188071
- Source:** 10.94.8.11
- Destination:** 10.102.155.183
- Protocol:** DNS
- Length:** 45
- Info:** 83 Standard query 0x2c02 A www.msftconnecttest.com

Detailed Hex and ASCII Data:

```

0000  34 6f 24 c4 2f e9 cc 36 cf b3 e1 c2 00 00 45 00 4o$ / - 6 ..... E
0010  01 38 ca 0f 00 00 3d 11 fa 0f 0a 5e 08 00 0a 66 8 ... . ^ . f
0020  9b b7 00 35 ec e4 01 24 dd 35 00 02 81 80 00 01 ..-$. $ 5-----
0030  00 08 00 00 00 05 01 6d 69 74 03 65 64 75 00 00 ..... m it.edu
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... ns1-173.akam.net
0050  0e 73 31 2d 31 37 00 04 61 6b 61 64 03 6e 65 74 ns1-173.akam.net
0060  00 c0 0c 00 02 00 01 00 07 08 00 01 00 08 01 00 ..... as
0070  69 61 31 2d c0 0c 00 02 00 01 00 08 07 01 00 ..... iai.....
0080  07 04 75 00 77 32 c0 2d c0 0c 00 02 00 01 00 00 ..... usw2.....
0090  00 00 00 00 07 08 00 02 00 01 00 08 07 01 00 ..... eur 5....
00a0  01 00 00 07 08 00 07 04 75 73 65 35 c0 2d c0 0c ..... use5.....
00b0  00 02 00 01 00 00 07 08 00 09 06 6e 73 31 2d 33 ..... ns1-3
00c0  37 c0 2d c0 0c 00 02 00 01 00 08 07 08 00 07 04 7.....
00d0  75 73 65 35 c0 2d c0 0c 00 02 00 01 00 08 07 08 00 ..... use2.....
00e0  00 02 00 01 00 00 07 08 00 09 06 6e 73 31 2d 33 ..... ns1-173.akam.net
00f0  00 02 68 30 00 04 5f 64 af 40 c0 a5 00 01 00 01 ..... asia2.....
0100  00 01 1d 10 00 04 60 07 31 40 c0 b8 00 01 00 01 ..... hbo...d @.....
0110  00 00 f8 07 00 04 5f 65 24 40 c0 90 00 01 00 01 ..... e 56.....
0120  00 01 56 c3 00 04 21 63 5b 25 c0 90 00 01 00 01 ..... V...1 [%]...
0130  00 01 56 c3 00 00 1c 6c 5b 25 c0 90 00 01 00 01 ..... V...&.....
0140  00 00 00 00 00 25 ..... %

```

Selected DNS Response (Packet 14):

- Time:** 11.188071
- Source:** 10.94.8.11
- Destination:** 10.102.155.183
- Protocol:** DNS
- Length:** 45
- Info:** 83 Standard query 0x2c02 A www.msftconnecttest.com

Detailed Hex and ASCII Data:

```

0000  34 6f 24 c4 2f e9 cc 36 cf b3 e1 c2 00 00 45 00 4o$ / - 6 ..... E
0010  01 38 ca 0f 00 00 3d 11 fa 0f 0a 5e 08 00 0a 66 8 ... . ^ . f
0020  9b b7 00 35 ec e4 01 24 dd 35 00 02 81 80 00 01 ..-$. $ 5-----
0030  00 08 00 00 00 05 01 6d 69 74 03 65 64 75 00 00 ..... m it.edu
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... ns1-173.akam.net
0050  0e 73 31 2d 31 37 00 04 61 6b 61 64 03 6e 65 74 ns1-173.akam.net
0060  00 c0 0c 00 02 00 01 00 07 08 00 01 00 08 01 00 ..... as
0070  69 61 31 2d c0 0c 00 02 00 01 00 08 07 01 00 ..... iai.....
0080  07 04 75 00 77 32 c0 2d c0 0c 00 02 00 01 00 00 ..... usw2.....
0090  00 00 00 00 07 08 00 02 00 01 00 08 07 01 00 ..... eur 5....
00a0  01 00 00 07 08 00 07 04 75 73 65 35 c0 2d c0 0c ..... use5.....
00b0  00 02 00 01 00 00 07 08 00 09 06 6e 73 31 2d 33 ..... ns1-3
00c0  37 c0 2d c0 0c 00 02 00 01 00 08 07 08 00 07 04 7.....
00d0  75 73 65 35 c0 2d c0 0c 00 02 00 01 00 08 07 08 00 ..... use2.....
00e0  00 02 00 01 00 00 07 08 00 09 06 6e 73 31 2d 33 ..... ns1-173.akam.net
00f0  00 02 68 30 00 04 5f 64 af 40 c0 a5 00 01 00 01 ..... asia2.....
0100  00 01 1d 10 00 04 60 07 31 40 c0 b8 00 01 00 01 ..... hbo...d @.....
0110  00 00 f8 07 00 04 5f 65 24 40 c0 90 00 01 00 01 ..... e 56.....
0120  00 01 56 c3 00 04 21 63 5b 25 c0 90 00 01 00 01 ..... V...1 [%]...
0130  00 01 56 c3 00 00 1c 6c 5b 25 c0 90 00 01 00 01 ..... V...&.....
0140  00 00 00 00 00 25 ..... %

```

19. Provide a screenshot.

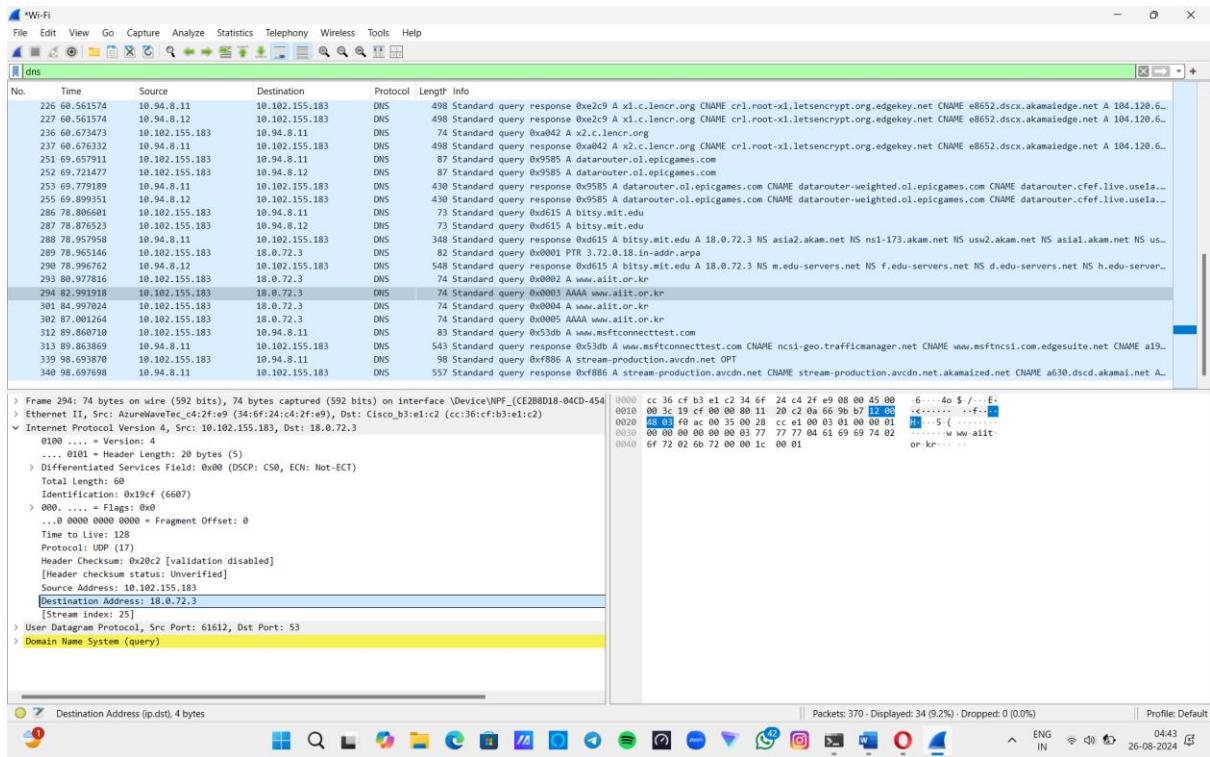
20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

Answers:

Yes it corresponds to the local default DNS servers.

The screenshot displays three windows illustrating network configuration and traffic analysis:

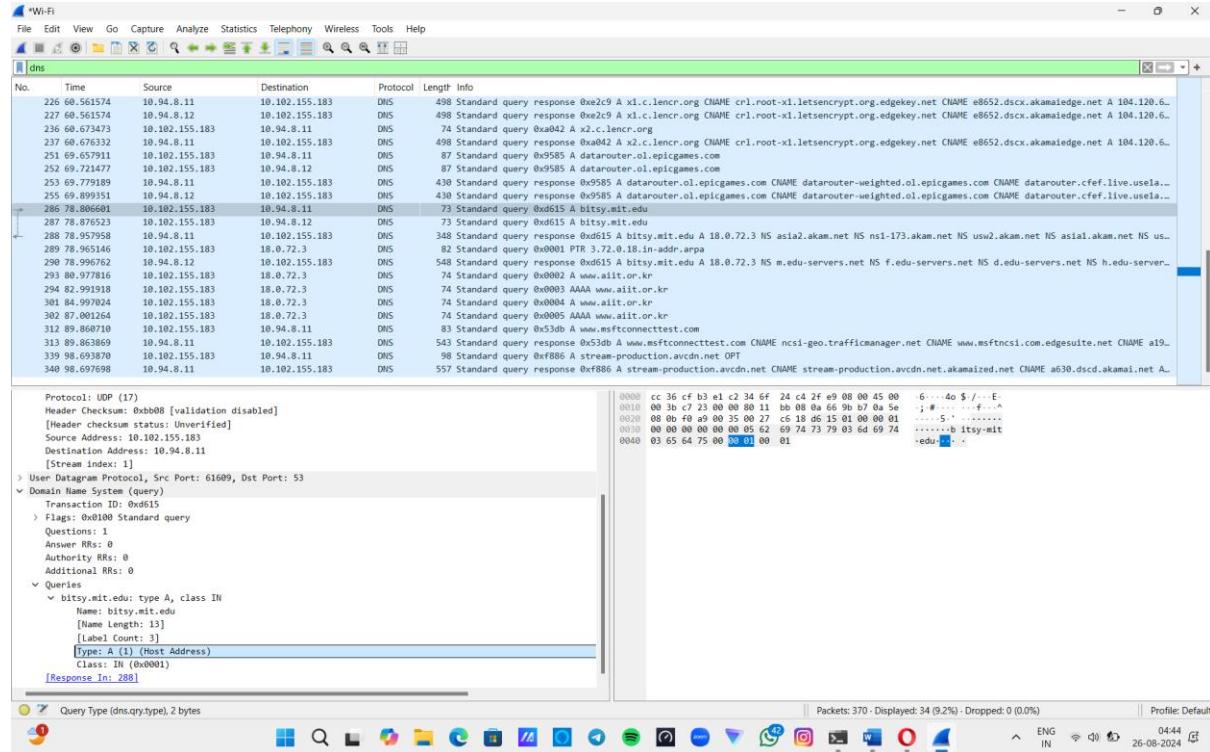
- Wireshark Window:** Shows captured network traffic on the "Wlan0" interface. A selected DNS query from the source IP 10.94.8.11 to the destination IP 10.102.155.183 is highlighted. The packet details pane shows the query for "www.epicgames.com". The bytes pane shows the raw hex and ASCII data of the packet.
- Browser Window:** A Microsoft Edge browser window titled "Destination Address (ip.dst), 4 bytes". It shows the network configuration for the "Local Area Connection" and "Wireless LAN adapter Local Area Connection* 1". Both show "Media State" as "Media disconnected".
- Terminal Window:** A Windows PowerShell window showing the output of the command "Get-NetAdapter -Name *". It lists several network adapters, including "TAP-ProtonVPN Windows Adapter V9", "Microsoft Wi-Fi Direct Virtual Adapter", and "MediaTek Wi-Fi 6 MT7921 Wireless LAN Card". The "Media State" for most is listed as "Media disconnected".



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:

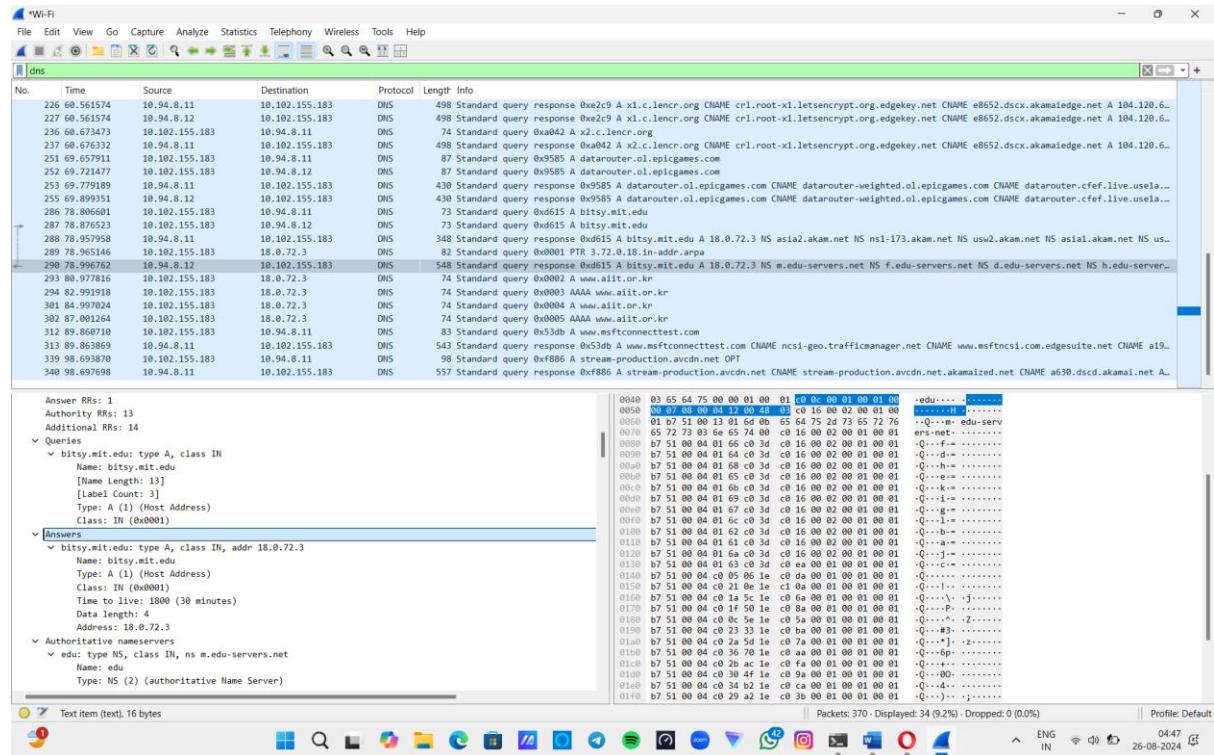


Type:A.

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.