Computer Networking
(CSE 311)
DNS Lab using Wireshark

Submitted By:

Shifat Jahan Shifa

Roll: 1301

BSSE 13th batch

Session: 2020-2021

Submitted To:

Dr. Md. Shariful Islam

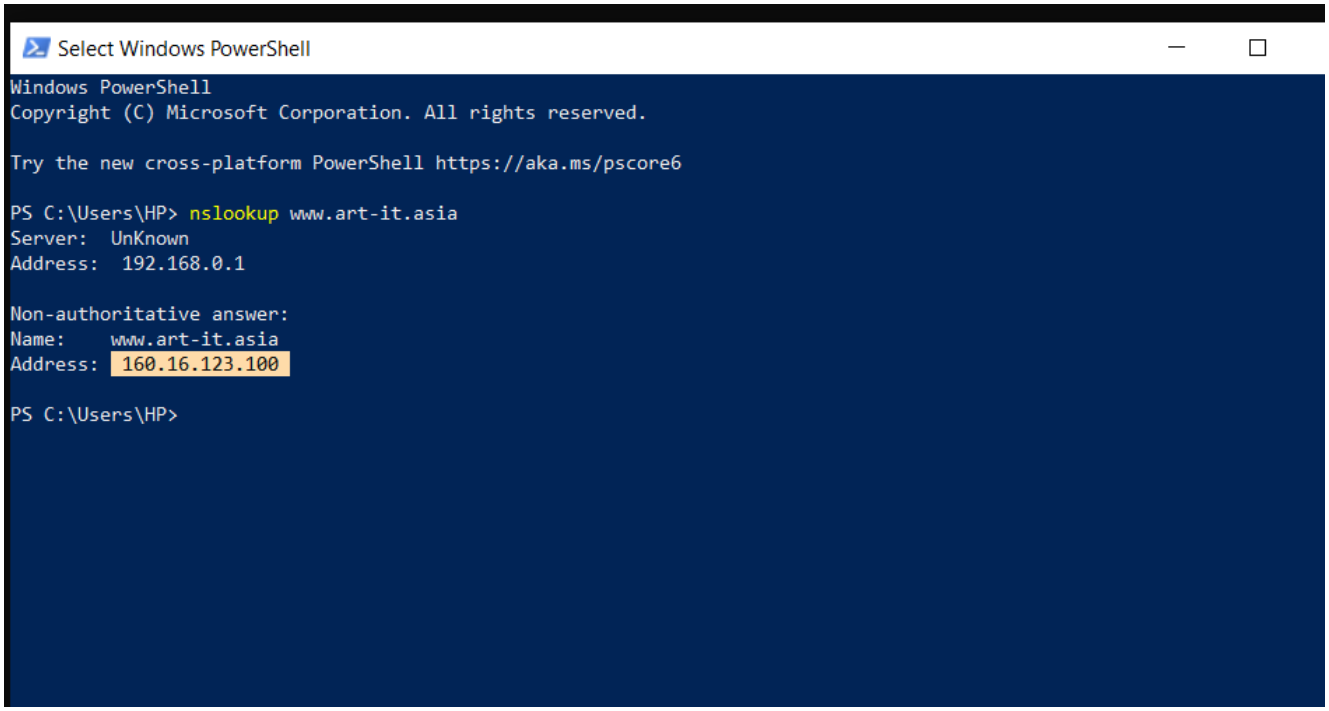
Professor

Institute of Information Technology

University of Dhaka

Date: 13/02/2023

Answer 1:

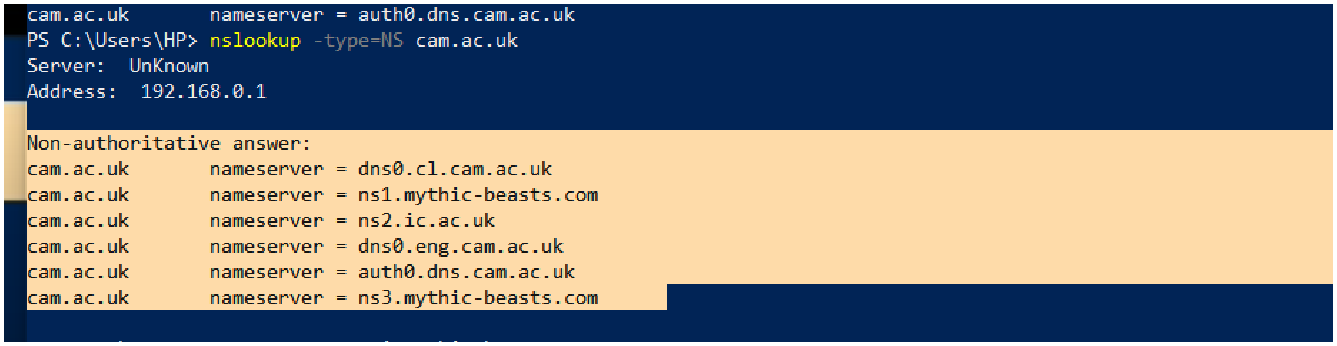


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\HP> nslookup www.art-it.asia
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    www.art-it.asia
Address:  160.16.123.100

PS C:\Users\HP>
```

Server name: www.art-it.asia

Ip address: 160.16.123.100

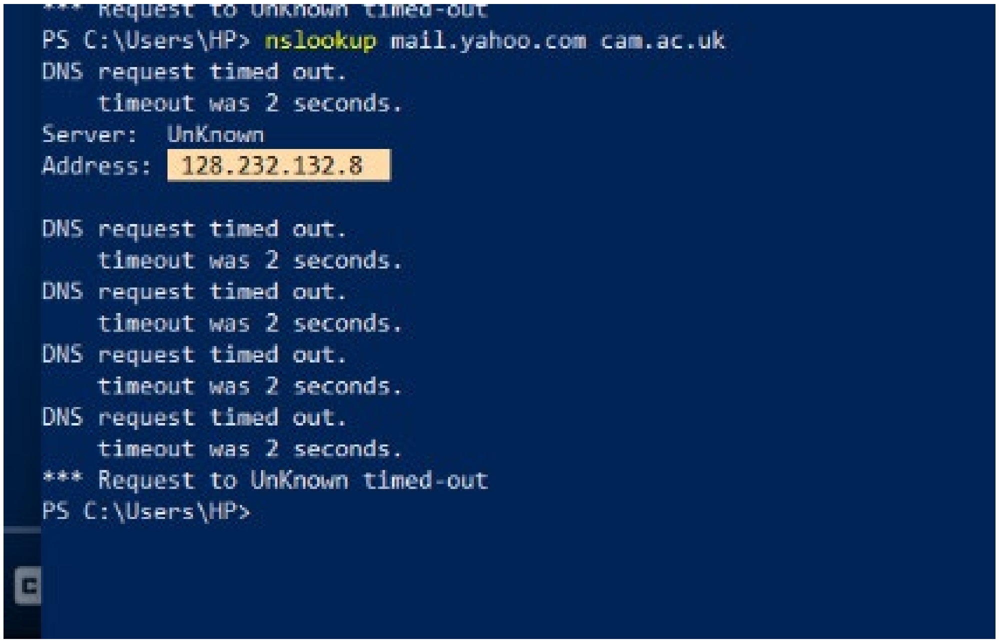
Answer 2:



```
cam.ac.uk       nameserver = auth0.dns.cam.ac.uk
PS C:\Users\HP> nslookup -type=NS cam.ac.uk
Server:  UnKnown
Address:  192.168.0.1

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

University: Cambridge university, UK.

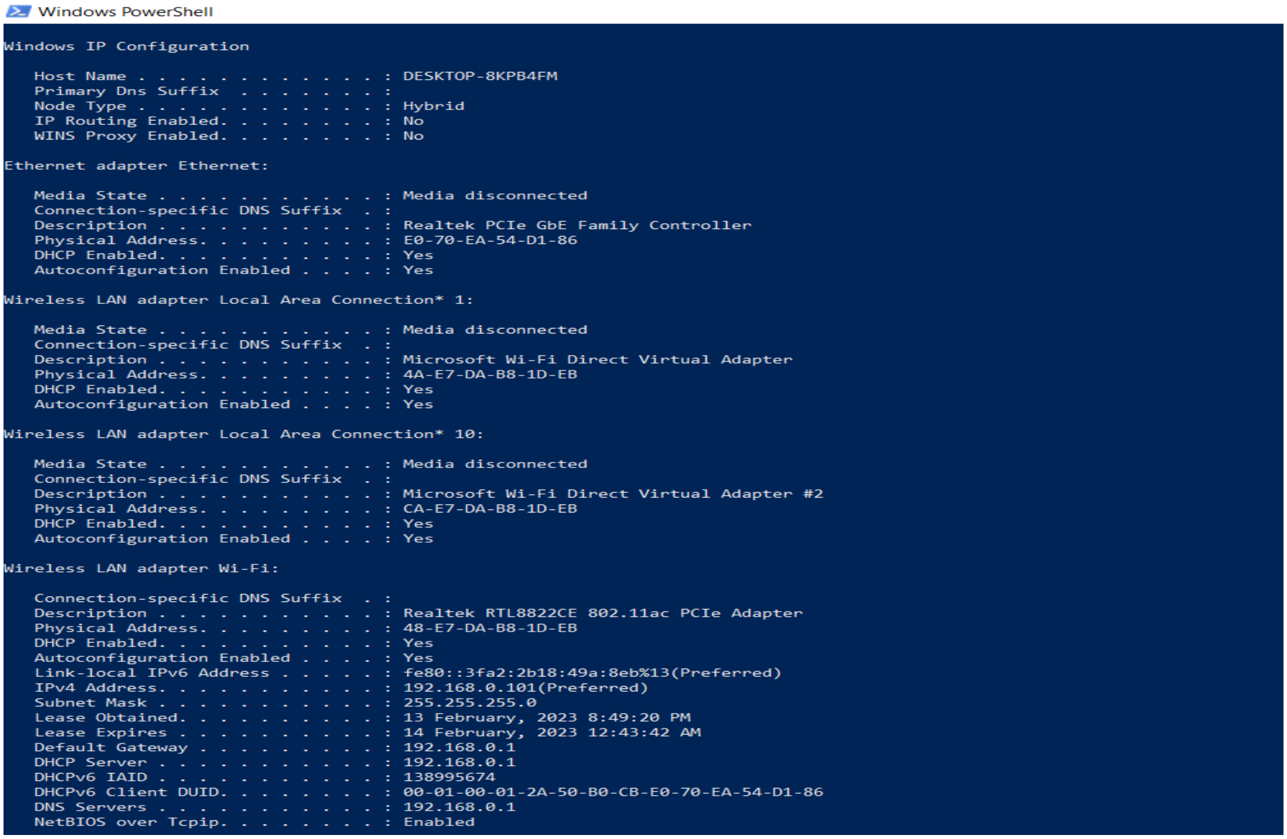
Answer 3:



```
*** Request to UnKnown timed-out
PS C:\Users\HP> 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
PS C:\Users\HP>
```

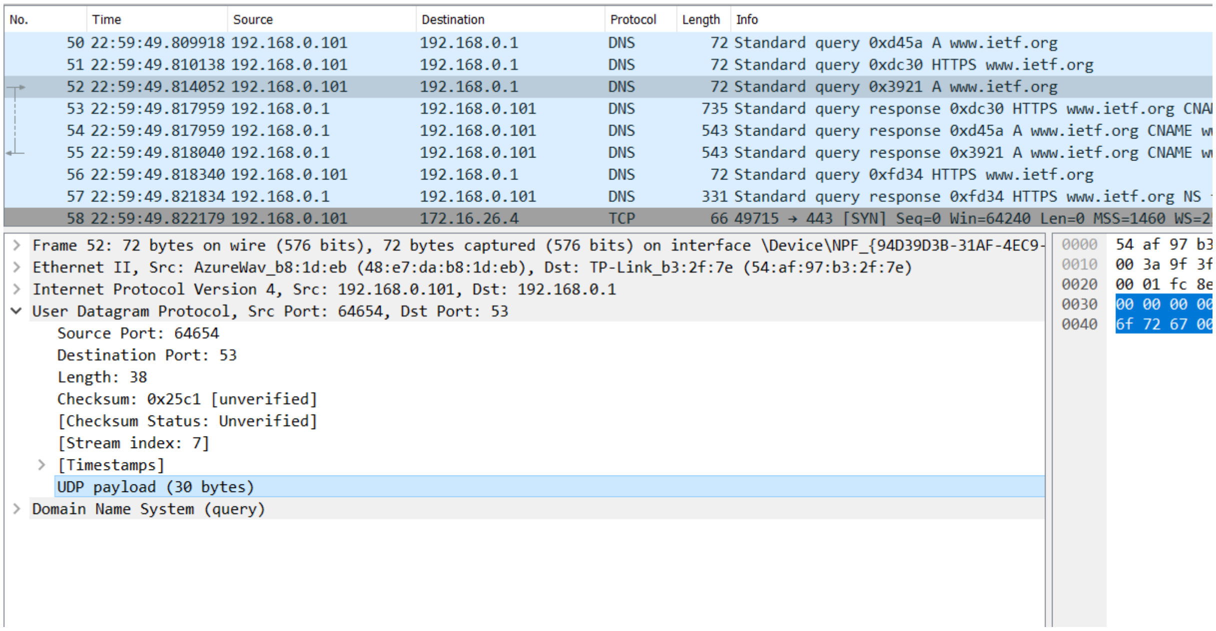
Ip address: **128.232.132.8**

Ipconfig command:



```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-8KPB4FM
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : E0-70-EA-54-D1-86
   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. . . . . . . . . : 4A-E7-DA-B8-1D-EB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : CA-E7-DA-B8-1D-EB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek RTL8822CE 802.11ac PCIe Adapter
   Physical Address. . . . . . . . . : 48-E7-DA-B8-1D-EB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::3fa2:2b18:49a:8eb%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.101(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 13 February, 2023 8:49:20 PM
   Lease Expires . . . . . . . . . . : 14 February, 2023 12:43:42 AM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 138995674
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-50-B0-CB-E0-70-EA-54-D1-86
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Answer 4:

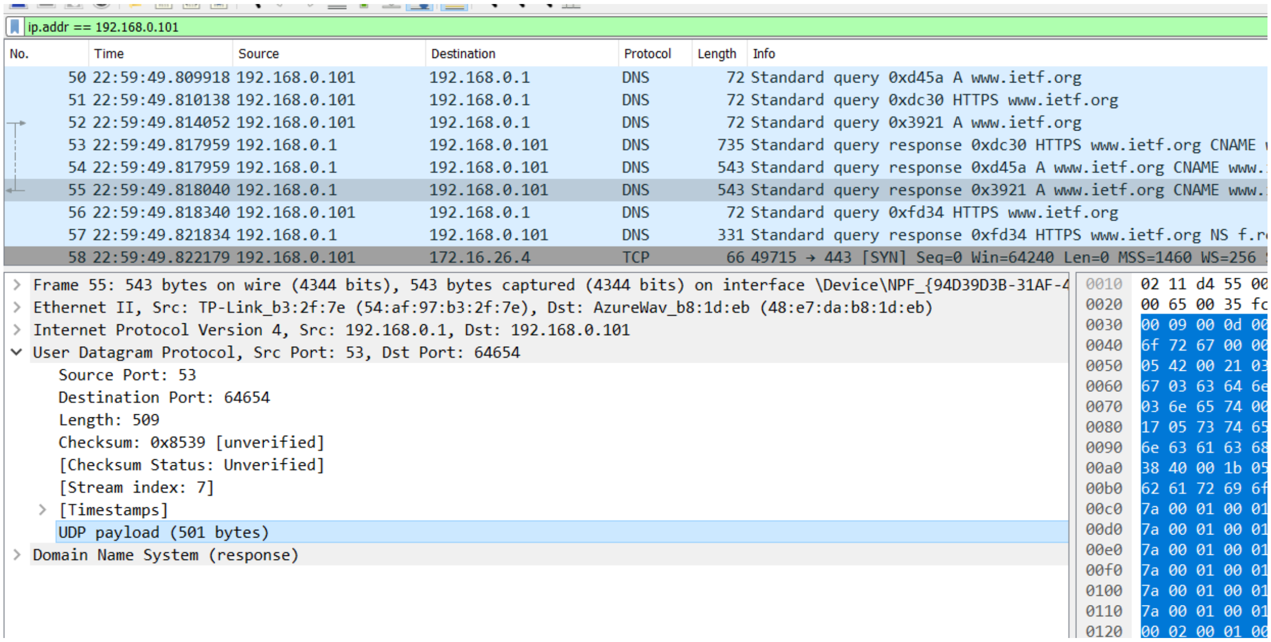


```
No.   Time               Source          Destination     Protocol  Length  Info
   50 22:59:49.809918 192.168.0.101   192.168.0.1     DNS        72 Standard query 0xd45a A www.ietf.org
   51 22:59:49.810138 192.168.0.101   192.168.0.1     DNS        72 Standard query 0xdc30 HTTPS www.ietf.org
   52 22:59:49.814052 192.168.0.101   192.168.0.1     DNS        72 Standard query 0x3921 A www.ietf.org
   53 22:59:49.817959 192.168.0.1     192.168.0.101   DNS       735 Standard query response 0xdc30 HTTPS www.ietf.org CNA
   54 22:59:49.817959 192.168.0.1     192.168.0.101   DNS       543 Standard query response 0xd45a A www.ietf.org CNAME w
   55 22:59:49.818040 192.168.0.1     192.168.0.101   DNS       543 Standard query response 0x3921 A www.ietf.org CNAME w
   56 22:59:49.818340 192.168.0.101   192.168.0.1     DNS        72 Standard query 0xfd34 HTTPS www.ietf.org
   57 22:59:49.821834 192.168.0.1     192.168.0.101   DNS       331 Standard query response 0xfd34 HTTPS www.ietf.org NS
   58 22:59:49.822179 192.168.0.101   172.16.26.4     TCP        66 49715 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
```

```
> Frame 52: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{94D39D3B-31AF-4EC9-
> Ethernet II, Src: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb), Dst: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
v User Datagram Protocol, Src Port: 64654, Dst Port: 53
    Source Port: 64654
    Destination Port: 53
    Length: 38
    Checksum: 0x25c1 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
  > [Timestamps]
    UDP payload (30 bytes)
> Domain Name System (query)
```

```
0000  54 af 97 b3
0010  00 3a 9f 3f
0020  00 01 fc 8e
0030  00 00 00 00
0040  6f 72 67 00
```

Screenshot for query message



```
ip.addr == 192.168.0.101
```

```
No.   Time               Source          Destination     Protocol  Length  Info
   50 22:59:49.809918 192.168.0.101   192.168.0.1     DNS        72 Standard query 0xd45a A www.ietf.org
   51 22:59:49.810138 192.168.0.101   192.168.0.1     DNS        72 Standard query 0xdc30 HTTPS www.ietf.org
   52 22:59:49.814052 192.168.0.101   192.168.0.1     DNS        72 Standard query 0x3921 A www.ietf.org
   53 22:59:49.817959 192.168.0.1     192.168.0.101   DNS       735 Standard query response 0xdc30 HTTPS www.ietf.org CNAME
   54 22:59:49.817959 192.168.0.1     192.168.0.101   DNS       543 Standard query response 0xd45a A www.ietf.org CNAME www.
   55 22:59:49.818040 192.168.0.1     192.168.0.101   DNS       543 Standard query response 0x3921 A www.ietf.org CNAME www.
   56 22:59:49.818340 192.168.0.101   192.168.0.1     DNS        72 Standard query 0xfd34 HTTPS www.ietf.org
   57 22:59:49.821834 192.168.0.1     192.168.0.101   DNS       331 Standard query response 0xfd34 HTTPS www.ietf.org NS f.r
   58 22:59:49.822179 192.168.0.101   172.16.26.4     TCP        66 49715 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
```

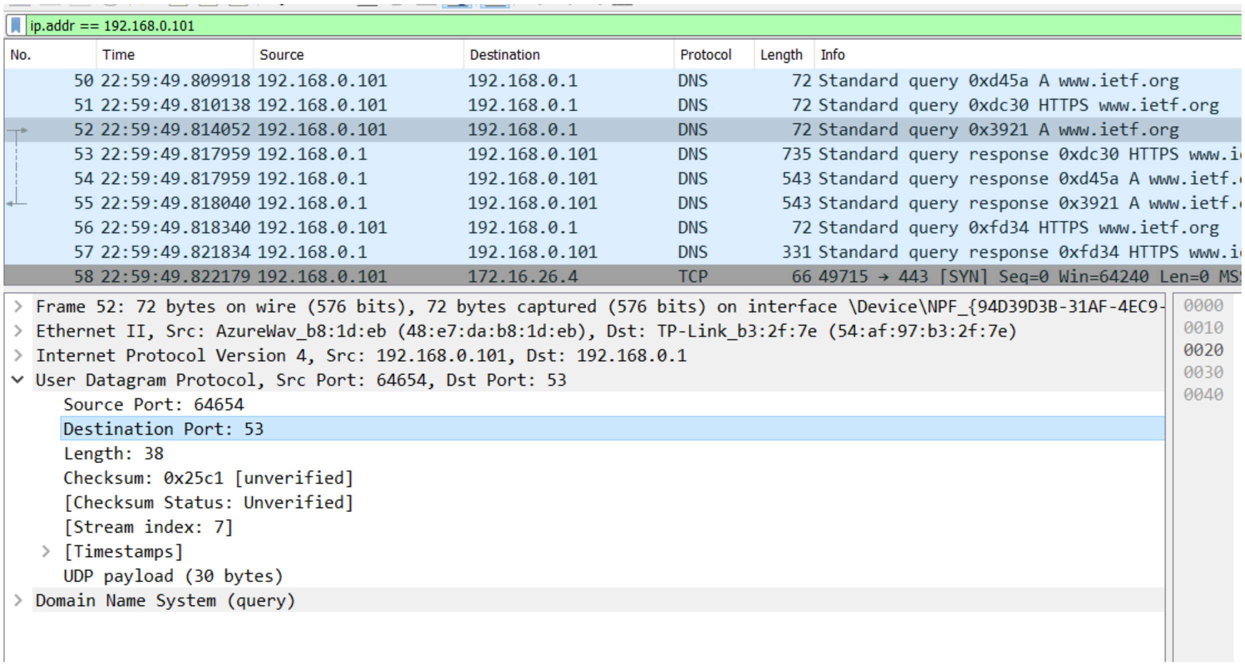
```
> Frame 55: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface \Device\NPF_{94D39D3B-31AF-4
> Ethernet II, Src: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e), Dst: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
v User Datagram Protocol, Src Port: 53, Dst Port: 64654
    Source Port: 53
    Destination Port: 64654
    Length: 509
    Checksum: 0x8539 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
  > [Timestamps]
    UDP payload (501 bytes)
> Domain Name System (response)
```

```
0010  02 11 d4 55 00
0020  00 65 00 35 fc
0030  00 09 00 0d 00
0040  6f 72 67 00 00
0050  05 42 00 21 03
0060  67 03 63 64 6e
0070  03 6e 65 74 00
0080  17 05 73 74 65
0090  6e 63 61 63 68
00a0  38 40 00 1b 05
00b0  62 61 72 69 6f
00c0  7a 00 01 00 01
00d0  7a 00 01 00 01
00e0  7a 00 01 00 01
00f0  7a 00 01 00 01
0100  7a 00 01 00 01
0110  7a 00 01 00 01
0120  00 02 00 01 00
```

Screenshot for response message.

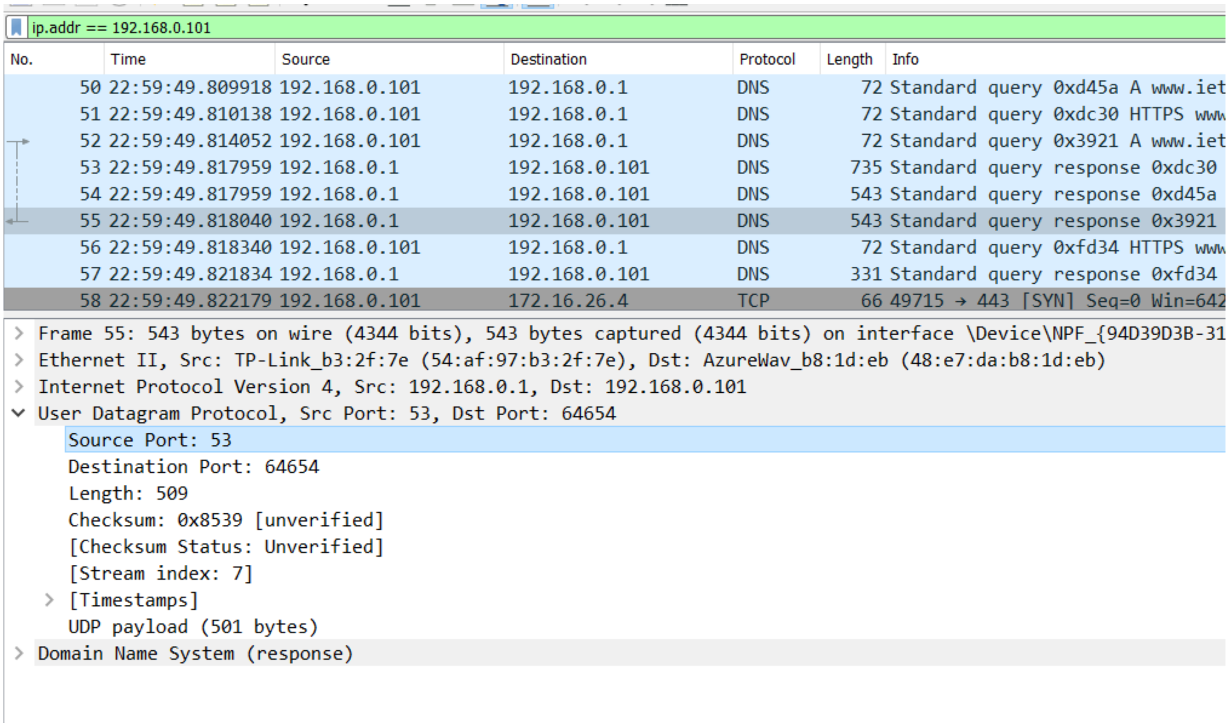
Both of them were sent over UDP.

Answer 5:



```
ip.addr == 192.168.0.101

No.   Time            Source          Destination     Protocol  Length  Info
   50 22:59:49.809918 192.168.0.101   192.168.0.1     DNS         72 Standard query 0xd45a A www.ietf.org
   51 22:59:49.810138 192.168.0.101   192.168.0.1     DNS         72 Standard query 0xdc30 HTTPS www.ietf.org
   52 22:59:49.814052 192.168.0.101   192.168.0.1     DNS         72 Standard query 0x3921 A www.ietf.org
   53 22:59:49.817959 192.168.0.1     192.168.0.101   DNS        735 Standard query response 0xdc30 HTTPS www.i
   54 22:59:49.817959 192.168.0.1     192.168.0.101   DNS        543 Standard query response 0xd45a A www.ietf.
   55 22:59:49.818040 192.168.0.1     192.168.0.101   DNS        543 Standard query response 0x3921 A www.ietf.
   56 22:59:49.818340 192.168.0.101   192.168.0.1     DNS         72 Standard query 0xfd34 HTTPS www.ietf.org
   57 22:59:49.821834 192.168.0.1     192.168.0.101   DNS        331 Standard query response 0xfd34 HTTPS www.i
   58 22:59:49.822179 192.168.0.101   172.16.26.4     TCP         66 49715 → 443 [SYN] Seq=0 Win=64240 Len=0 MS

> Frame 52: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{94D39D3B-31AF-4EC9-
> Ethernet II, Src: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb), Dst: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
v User Datagram Protocol, Src Port: 64654, Dst Port: 53
    Source Port: 64654
    Destination Port: 53
    Length: 38
    Checksum: 0x25c1 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
  > [Timestamps]
    UDP payload (30 bytes)
> Domain Name System (query)

0000
0010
0020
0030
0040
```

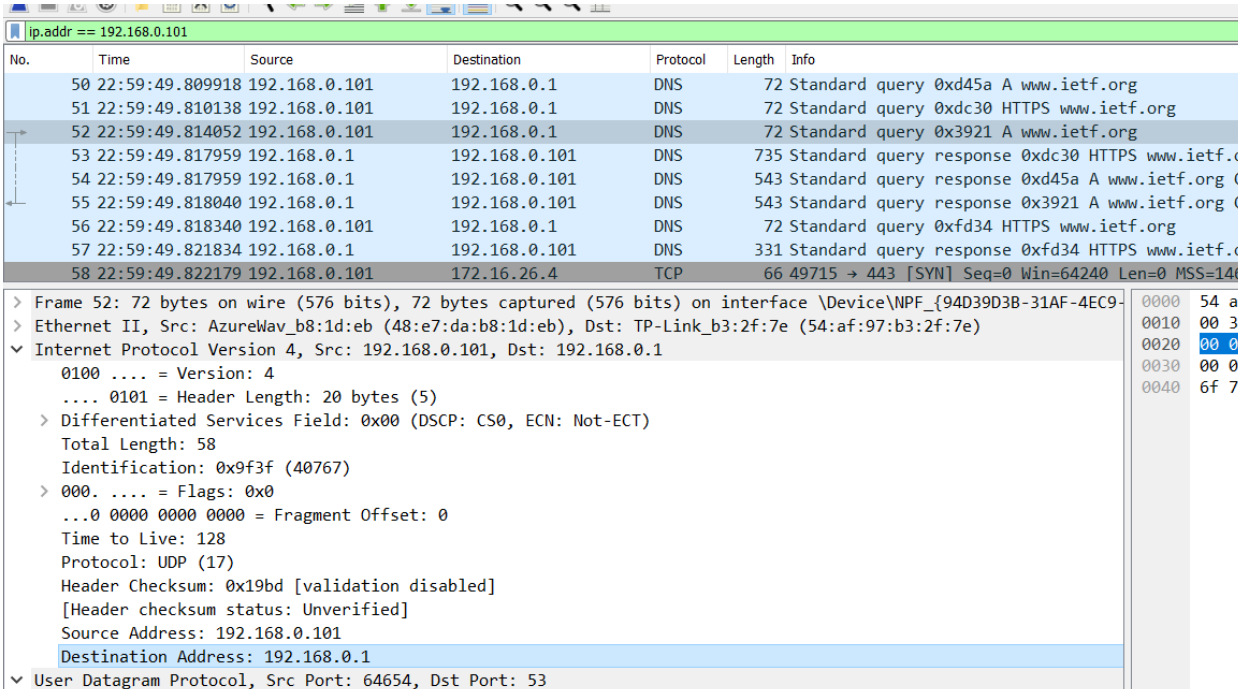
The destination port of the query message: 53



```
ip.addr == 192.168.0.101

No.   Time            Source          Destination     Protocol  Length  Info
   50 22:59:49.809918 192.168.0.101   192.168.0.1     DNS         72 Standard query 0xd45a A www.iet
   51 22:59:49.810138 192.168.0.101   192.168.0.1     DNS         72 Standard query 0xdc30 HTTPS www
   52 22:59:49.814052 192.168.0.101   192.168.0.1     DNS         72 Standard query 0x3921 A www.iet
   53 22:59:49.817959 192.168.0.1     192.168.0.101   DNS        735 Standard query response 0xdc30
   54 22:59:49.817959 192.168.0.1     192.168.0.101   DNS        543 Standard query response 0xd45a
   55 22:59:49.818040 192.168.0.1     192.168.0.101   DNS        543 Standard query response 0x3921
   56 22:59:49.818340 192.168.0.101   192.168.0.1     DNS         72 Standard query 0xfd34 HTTPS www
   57 22:59:49.821834 192.168.0.1     192.168.0.101   DNS        331 Standard query response 0xfd34
   58 22:59:49.822179 192.168.0.101   172.16.26.4     TCP         66 49715 → 443 [SYN] Seq=0 Win=642

> Frame 55: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface \Device\NPF_{94D39D3B-31
> Ethernet II, Src: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e), Dst: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
v User Datagram Protocol, Src Port: 53, Dst Port: 64654
    Source Port: 53
    Destination Port: 64654
    Length: 509
    Checksum: 0x8539 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
  > [Timestamps]
    UDP payload (501 bytes)
> Domain Name System (response)
```

The source port of the response message: 53

Answer 6:



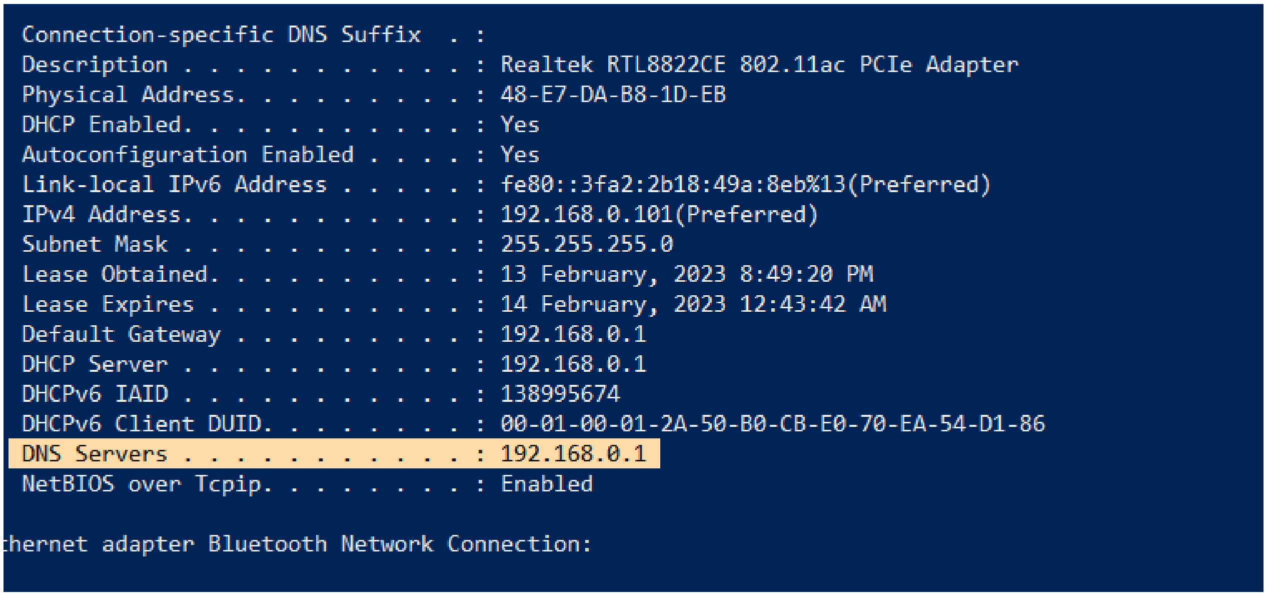
ip.addr == 192.168.0.101

```
No.    Time             Source         Destination    Protocol Length Info
    50 22:59:49.809918 192.168.0.101 192.168.0.1    DNS        72 Standard query 0xd45a A www.ietf.org
    51 22:59:49.810138 192.168.0.101 192.168.0.1    DNS        72 Standard query 0xdc30 HTTPS www.ietf.org
    52 22:59:49.814052 192.168.0.101 192.168.0.1    DNS        72 Standard query 0x3921 A www.ietf.org
    53 22:59:49.817959 192.168.0.1   192.168.0.101  DNS       735 Standard query response 0xdc30 HTTPS www.ietf.c
    54 22:59:49.817959 192.168.0.1   192.168.0.101  DNS       543 Standard query response 0xd45a A www.ietf.org (
    55 22:59:49.818040 192.168.0.1   192.168.0.101  DNS       543 Standard query response 0x3921 A www.ietf.org (
    56 22:59:49.818340 192.168.0.101 192.168.0.1    DNS        72 Standard query 0xfd34 HTTPS www.ietf.org
    57 22:59:49.821834 192.168.0.1   192.168.0.101  DNS       331 Standard query response 0xfd34 HTTPS www.ietf.c
    58 22:59:49.822179 192.168.0.101 172.16.26.4    TCP        66 49715 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=146
```

```
> Frame 52: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{94D39D3B-31AF-4EC9-
> Ethernet II, Src: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb), Dst: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e)
v Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0x9f3f (40767)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x19bd [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.101
    Destination Address: 192.168.0.1
v User Datagram Protocol, Src Port: 64654, Dst Port: 53
```

```
0000  54 a
0010  00 3
0020  00 0
0030  00 0
0040  6f 7
```

DNS query message was sent to IP address: **192.168.0.1**

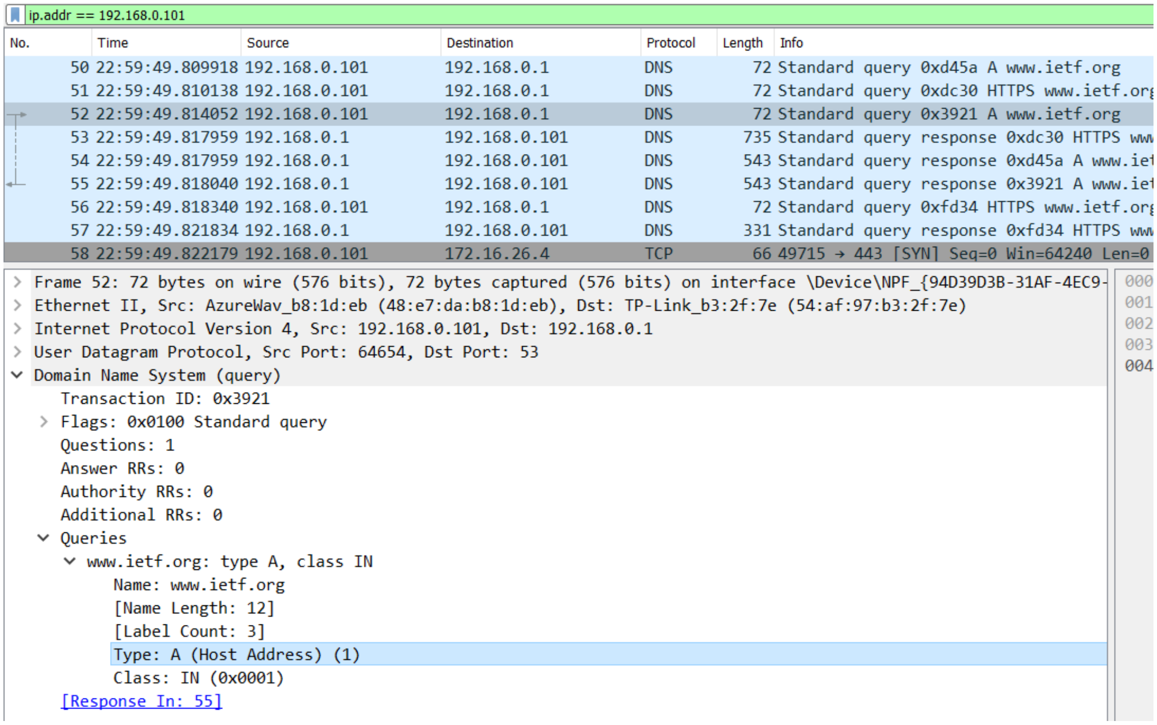


```
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek RTL8822CE 802.11ac PCIe Adapter
   Physical Address. . . . . . . . . : 48-E7-DA-B8-1D-EB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::3fa2:2b18:49a:8eb%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.101(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 13 February, 2023 8:49:20 PM
   Lease Expires . . . . . . . . . . : 14 February, 2023 12:43:42 AM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 138995674
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-50-B0-CB-E0-70-EA-54-D1-86
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

hernet adapter Bluetooth Network Connection:
```

Ip address of local DNS server: **192.168.0.**1

Both ip addresses are same.

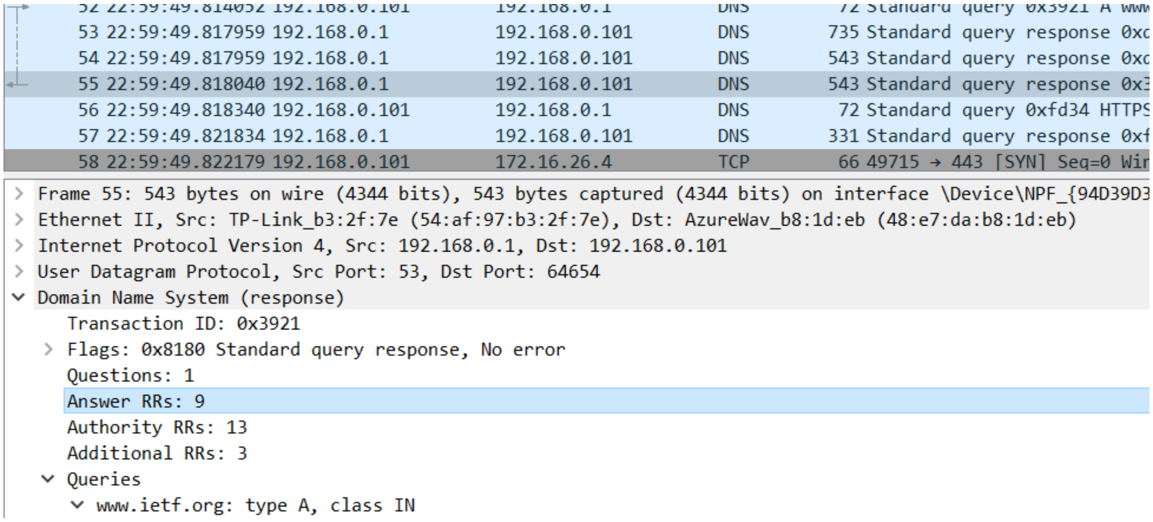
Answer 7:



```
ip.addr == 192.168.0.101
No.   Time               Source          Destination     Protocol  Length  Info
   50 22:59:49.809918 192.168.0.101   192.168.0.1     DNS         72 Standard query 0xd45a A www.ietf.org
   51 22:59:49.810138 192.168.0.101   192.168.0.1     DNS         72 Standard query 0xdc30 HTTPS www.ietf.org
   52 22:59:49.814052 192.168.0.101   192.168.0.1     DNS         72 Standard query 0x3921 A www.ietf.org
   53 22:59:49.817959 192.168.0.1     192.168.0.101   DNS        735 Standard query response 0xdc30 HTTPS www
   54 22:59:49.817959 192.168.0.1     192.168.0.101   DNS        543 Standard query response 0xd45a A www.iet
   55 22:59:49.818040 192.168.0.1     192.168.0.101   DNS        543 Standard query response 0x3921 A www.iet
   56 22:59:49.818340 192.168.0.101   192.168.0.1     DNS         72 Standard query 0xfd34 HTTPS www.ietf.org
   57 22:59:49.821834 192.168.0.1     192.168.0.101   DNS        331 Standard query response 0xfd34 HTTPS www
   58 22:59:49.822179 192.168.0.101   172.16.26.4     TCP         66 49715 → 443 [SYN] Seq=0 Win=64240 Len=0

> Frame 52: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{94D39D3B-31AF-4EC9-
> Ethernet II, Src: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb), Dst: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 64654, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x3921
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.ietf.org: type A, class IN
        Name: www.ietf.org
        [Name Length: 12]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 55]

000
001
002
003
004
```

Type: A. answer: 0.

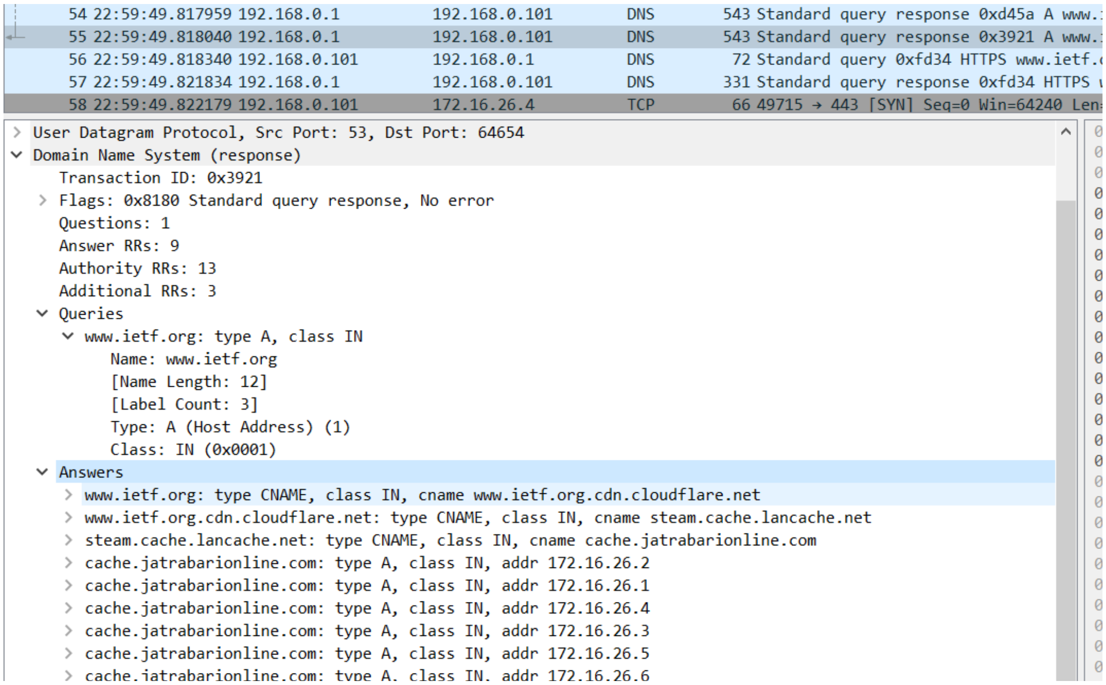
Answer 8:



```
   52 22:59:49.814052 192.168.0.101   192.168.0.1     DNS         72 Standard query 0x3921 A www
   53 22:59:49.817959 192.168.0.1     192.168.0.101   DNS        735 Standard query response 0xc
   54 22:59:49.817959 192.168.0.1     192.168.0.101   DNS        543 Standard query response 0xc
   55 22:59:49.818040 192.168.0.1     192.168.0.101   DNS        543 Standard query response 0x3
   56 22:59:49.818340 192.168.0.101   192.168.0.1     DNS         72 Standard query 0xfd34 HTTPS
   57 22:59:49.821834 192.168.0.1     192.168.0.101   DNS        331 Standard query response 0xf
   58 22:59:49.822179 192.168.0.101   172.16.26.4     TCP         66 49715 → 443 [SYN] Seq=0 Wir

> Frame 55: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface \Device\NPF_{94D39D3
> Ethernet II, Src: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e), Dst: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
> User Datagram Protocol, Src Port: 53, Dst Port: 64654
v Domain Name System (response)
    Transaction ID: 0x3921
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 9
    Authority RRs: 13
    Additional RRs: 3
  v Queries
    v www.ietf.org: type A, class IN
```

Total answer: 09

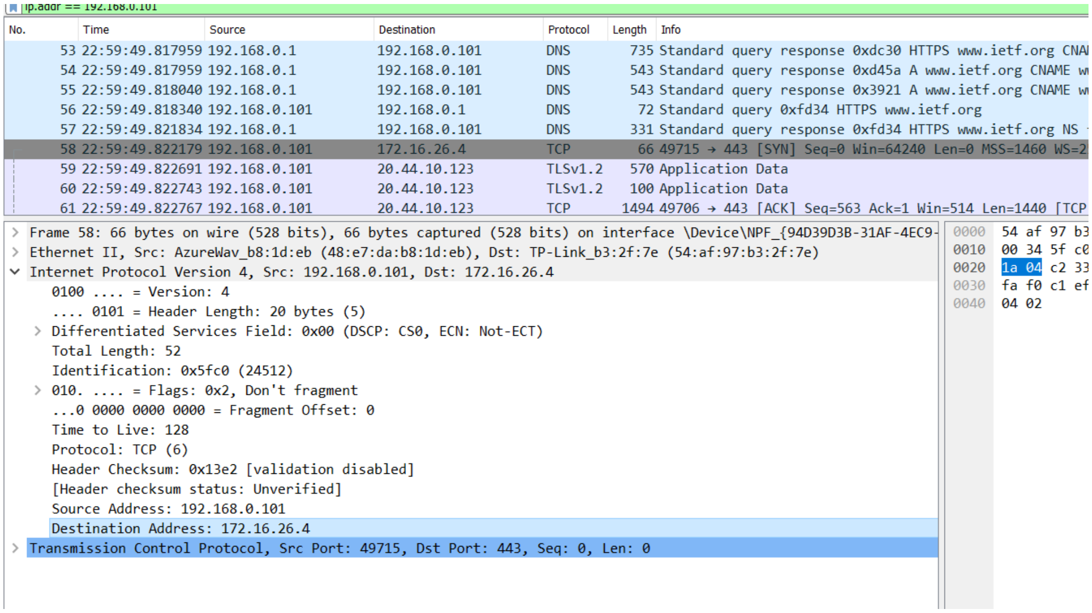
Each of the response contain> host name, type, class, ip address.



```
54 22:59:49.817959 192.168.0.1     192.168.0.101   DNS   543 Standard query response 0xd45a A www.:
55 22:59:49.818040 192.168.0.1     192.168.0.101   DNS   543 Standard query response 0x3921 A www.:
56 22:59:49.818340 192.168.0.101   192.168.0.1     DNS    72 Standard query 0xfd34 HTTPS www.ietf.
57 22:59:49.821834 192.168.0.1     192.168.0.101   DNS   331 Standard query response 0xfd34 HTTPS w
58 22:59:49.822179 192.168.0.101   172.16.26.4     TCP    66 49715 → 443 [SYN] Seq=0 Win=64240 Len
```

```
> User Datagram Protocol, Src Port: 53, Dst Port: 64654
v Domain Name System (response)
    Transaction ID: 0x3921
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 9
    Authority RRs: 13
    Additional RRs: 3
  v Queries
    v www.ietf.org: type A, class IN
          Name: www.ietf.org
          [Name Length: 12]
          [Label Count: 3]
          Type: A (Host Address) (1)
          Class: IN (0x0001)
  v Answers
    > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
    > www.ietf.org.cdn.cloudflare.net: type CNAME, class IN, cname steam.cache.lancache.net
    > steam.cache.lancache.net: type CNAME, class IN, cname cache.jatrabarionline.com
    > cache.jatrabarionline.com: type A, class IN, addr 172.16.26.2
    > cache.jatrabarionline.com: type A, class IN, addr 172.16.26.1
    > cache.jatrabarionline.com: type A, class IN, addr 172.16.26.4
    > cache.jatrabarionline.com: type A, class IN, addr 172.16.26.3
    > cache.jatrabarionline.com: type A, class IN, addr 172.16.26.5
    > cache.jatrabarionline.com: type A, class IN, addr 172.16.26.6
```

Answer 9:



```
ip.addr == 192.168.0.101
```

```
No.  Time               Source          Destination     Protocol  Length Info
  53 22:59:49.817959 192.168.0.1     192.168.0.101   DNS       735 Standard query response 0xdc30 HTTPS www.ietf.org CNAI
  54 22:59:49.817959 192.168.0.1     192.168.0.101   DNS       543 Standard query response 0xd45a A www.ietf.org CNAME w
  55 22:59:49.818040 192.168.0.1     192.168.0.101   DNS       543 Standard query response 0x3921 A www.ietf.org CNAME w
  56 22:59:49.818340 192.168.0.101   192.168.0.1     DNS        72 Standard query 0xfd34 HTTPS www.ietf.org
  57 22:59:49.821834 192.168.0.1     192.168.0.101   DNS       331 Standard query response 0xfd34 HTTPS www.ietf.org NS
  58 22:59:49.822179 192.168.0.101   172.16.26.4     TCP        66 49715 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
  59 22:59:49.822691 192.168.0.101   20.44.10.123    TLSv1.2   570 Application Data
  60 22:59:49.822743 192.168.0.101   20.44.10.123    TLSv1.2   100 Application Data
  61 22:59:49.822767 192.168.0.101   20.44.10.123    TCP      1494 49706 → 443 [ACK] Seq=563 Ack=1 Win=514 Len=1440 [TCP
```

```
> Frame 58: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{94D39D3B-31AF-4EC9-
> Ethernet II, Src: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb), Dst: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e)
v Internet Protocol Version 4, Src: 192.168.0.101, Dst: 172.16.26.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x5fc0 (24512)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x13e2 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.101
    Destination Address: 172.16.26.4
> Transmission Control Protocol, Src Port: 49715, Dst Port: 443, Seq: 0, Len: 0
```

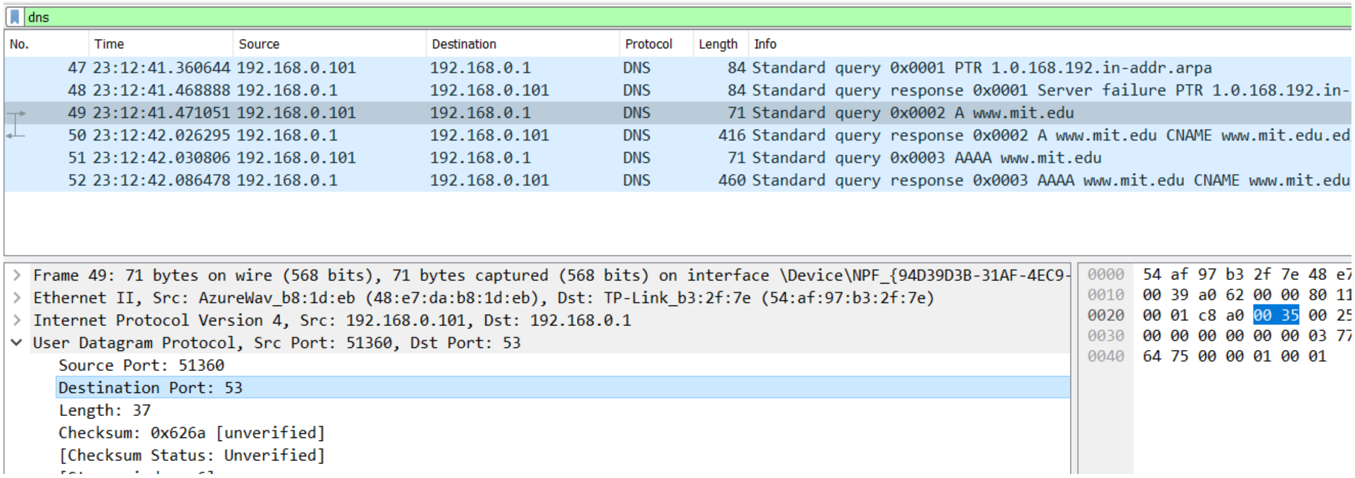
```
0000  54 af 97 b3
0010  00 34 5f c0
0020  1a 04 c2 33
0030  fa f0 c1 ef
0040  04 02
```

Yes. The destination ip address of the SYN packet correspond to ip address: **172.16.26.4** provided in the response message.

Answer 10:

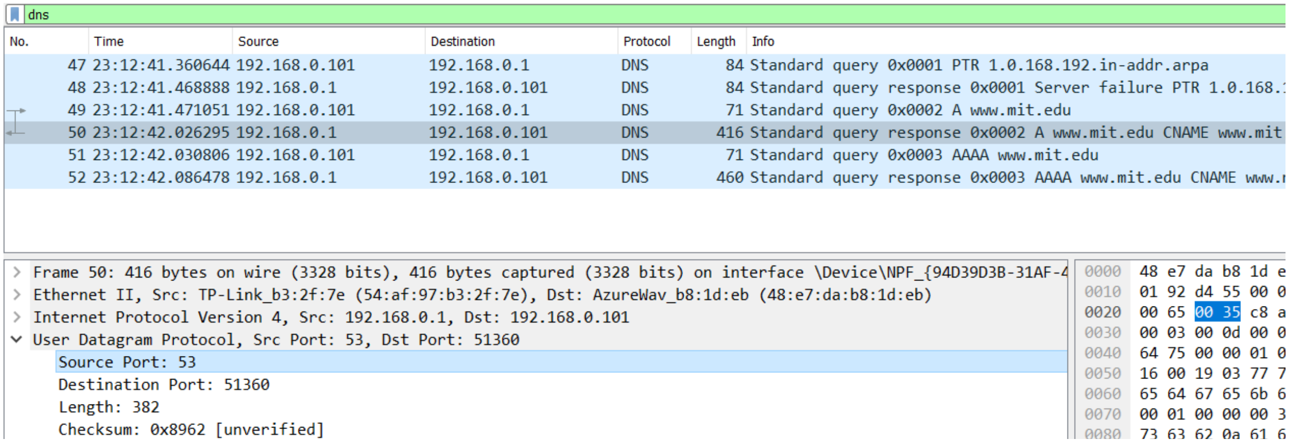
No. host doesn’t issue new DNS query before retrieving each image.

Answer 11:



```
dns
No.   Time             Source         Destination    Protocol  Length Info
   47 23:12:41.360644 192.168.0.101  192.168.0.1    DNS        84 Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
   48 23:12:41.468888 192.168.0.1    192.168.0.101  DNS        84 Standard query response 0x0001 Server failure PTR 1.0.168.192.in-
   49 23:12:41.471051 192.168.0.101  192.168.0.1    DNS        71 Standard query 0x0002 A www.mit.edu
   50 23:12:42.026295 192.168.0.1    192.168.0.101  DNS       416 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.ed
   51 23:12:42.030806 192.168.0.101  192.168.0.1    DNS        71 Standard query 0x0003 AAAA www.mit.edu
   52 23:12:42.086478 192.168.0.1    192.168.0.101  DNS       460 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu

> Frame 49: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{94D39D3B-31AF-4EC9-
> Ethernet II, Src: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb), Dst: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
v User Datagram Protocol, Src Port: 51360, Dst Port: 53
    Source Port: 51360
    Destination Port: 53
    Length: 37
    Checksum: 0x626a [unverified]
    [Checksum Status: Unverified]

0000  54 af 97 b3 2f 7e 48 e7
0010  00 39 a0 62 00 00 80 11
0020  00 01 c8 a0 00 35 00 25
0030  00 00 00 00 00 00 03 77
0040  64 75 00 00 01 00 01
```

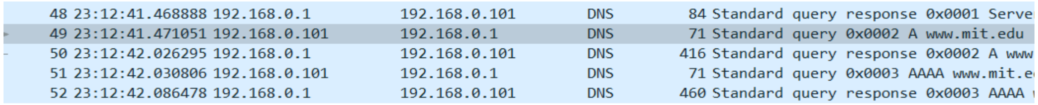
The destination port of the query message: 53



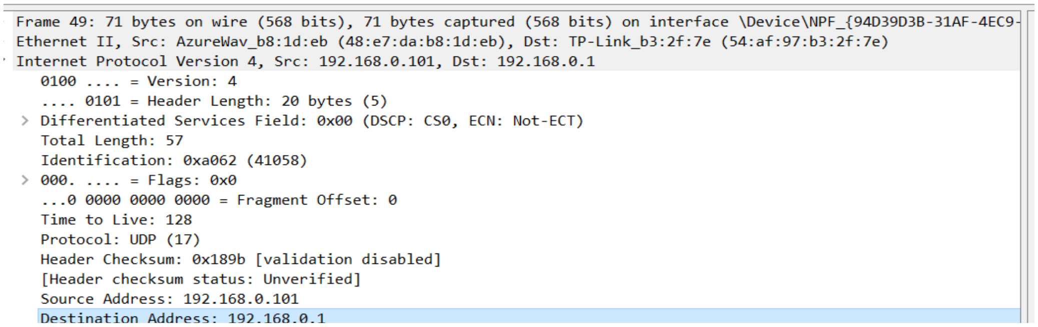
```
dns
No.   Time             Source         Destination    Protocol  Length Info
   47 23:12:41.360644 192.168.0.101  192.168.0.1    DNS        84 Standard query 0x0001 PTR 1.0.168.192.in-addr.arpa
   48 23:12:41.468888 192.168.0.1    192.168.0.101  DNS        84 Standard query response 0x0001 Server failure PTR 1.0.168.1
   49 23:12:41.471051 192.168.0.101  192.168.0.1    DNS        71 Standard query 0x0002 A www.mit.edu
   50 23:12:42.026295 192.168.0.1    192.168.0.101  DNS       416 Standard query response 0x0002 A www.mit.edu CNAME www.mit
   51 23:12:42.030806 192.168.0.101  192.168.0.1    DNS        71 Standard query 0x0003 AAAA www.mit.edu
   52 23:12:42.086478 192.168.0.1    192.168.0.101  DNS       460 Standard query response 0x0003 AAAA www.mit.edu CNAME www.

> Frame 50: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits) on interface \Device\NPF_{94D39D3B-31AF-4
> Ethernet II, Src: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e), Dst: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
v User Datagram Protocol, Src Port: 53, Dst Port: 51360
    Source Port: 53
    Destination Port: 51360
    Length: 382
    Checksum: 0x8962 [unverified]

0000  48 e7 da b8 1d e
0010  01 92 d4 55 00 0
0020  00 65 00 35 c8 a
0030  00 03 00 0d 00 0
0040  64 75 00 00 01 0
0050  16 00 19 03 77 7
0060  65 64 67 65 6b 6
0070  00 01 00 00 00 3
0080  73 63 62 0a 61 6
```

The source port of the response message: 53

Answer 12:

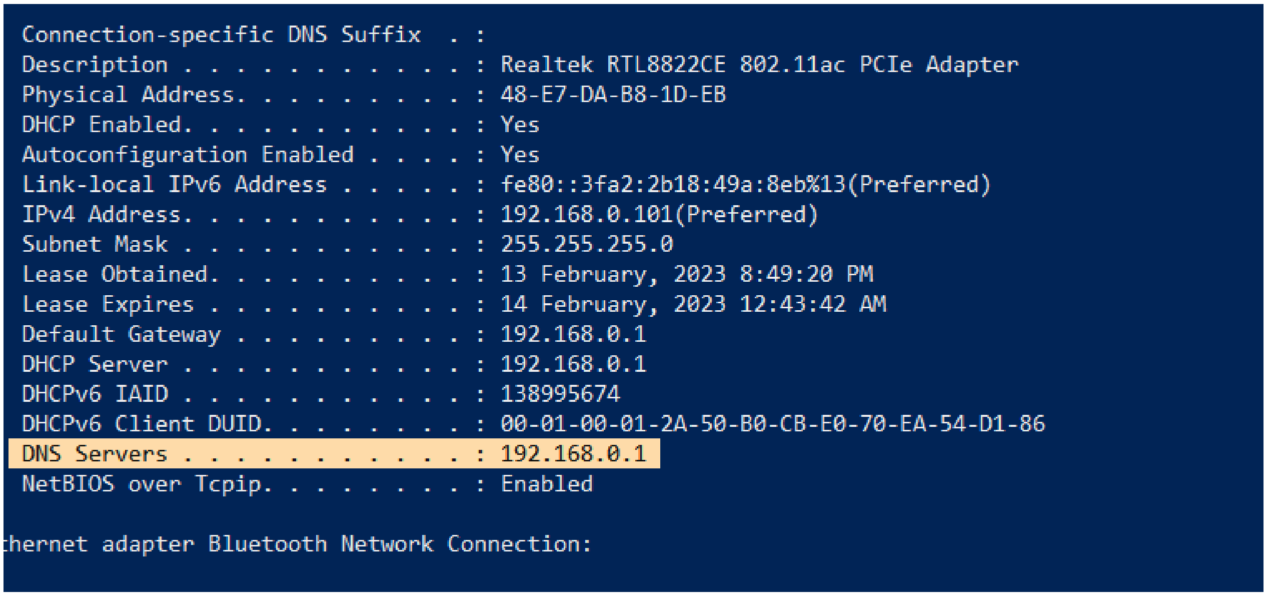


```
 48 23:12:41.468888 192.168.0.1      192.168.0.101    DNS     84 Standard query response 0x0001 Serve
 49 23:12:41.471051 192.168.0.101    192.168.0.1      DNS     71 Standard query 0x0002 A www.mit.edu
 50 23:12:42.026295 192.168.0.1      192.168.0.101    DNS    416 Standard query response 0x0002 A www
 51 23:12:42.030806 192.168.0.101    192.168.0.1      DNS     71 Standard query 0x0003 AAAA www.mit.e
 52 23:12:42.086478 192.168.0.1      192.168.0.101    DNS    460 Standard query response 0x0003 AAAA
```



```
Frame 49: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{94D39D3B-31AF-4EC9-
Ethernet II, Src: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb), Dst: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e)
Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 57
    Identification: 0xa062 (41058)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x189b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.101
    Destination Address: 192.168.0.1
```

DNS query message was sent to IP address: **192.168.0.1**

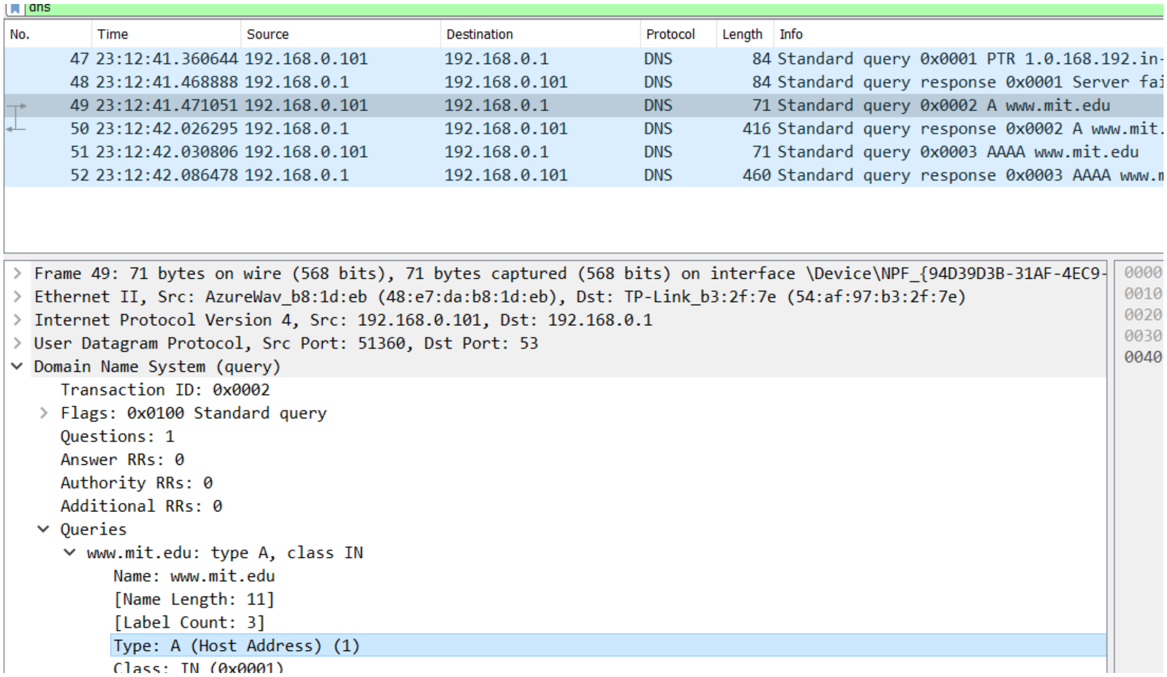


```
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : Realtek RTL8822CE 802.11ac PCIe Adapter
Physical Address. . . . . . . . . : 48-E7-DA-B8-1D-EB
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::3fa2:2b18:49a:8eb%13(Preferred)
IPv4 Address. . . . . . . . . . . : 192.168.0.101(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : 13 February, 2023 8:49:20 PM
Lease Expires . . . . . . . . . . : 14 February, 2023 12:43:42 AM
Default Gateway . . . . . . . . . : 192.168.0.1
DHCP Server . . . . . . . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . . . . . . . : 138995674
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-50-B0-CB-E0-70-EA-54-D1-86
DNS Servers . . . . . . . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . . . . : Enabled

hernet adapter Bluetooth Network Connection:
```

Ip address of local DNS server: **192.168.0.**1

Both ip addresses are same.

Answer 13:

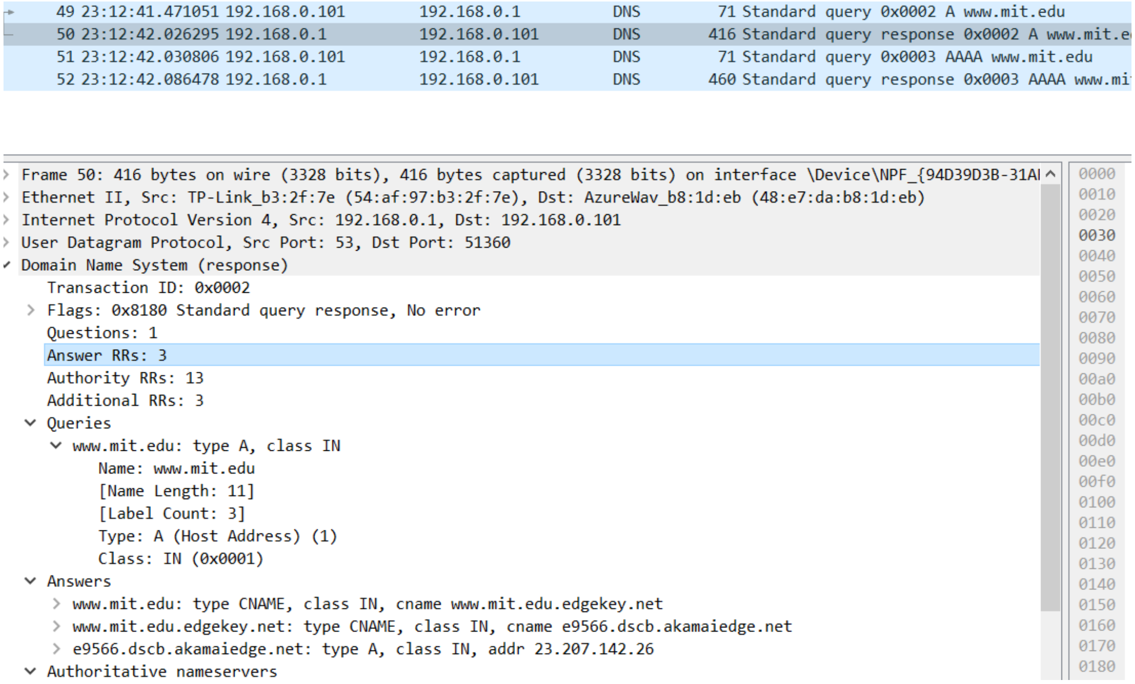


```
No.   Time              Source          Destination     Protocol  Length  Info
   47 23:12:41.360644 192.168.0.101   192.168.0.1     DNS        84 Standard query 0x0001 PTR 1.0.168.192.in-
   48 23:12:41.468888 192.168.0.1     192.168.0.101   DNS        84 Standard query response 0x0001 Server fai
   49 23:12:41.471051 192.168.0.101   192.168.0.1     DNS        71 Standard query 0x0002 A www.mit.edu
   50 23:12:42.026295 192.168.0.1     192.168.0.101   DNS       416 Standard query response 0x0002 A www.mit.
   51 23:12:42.030806 192.168.0.101   192.168.0.1     DNS        71 Standard query 0x0003 AAAA www.mit.edu
   52 23:12:42.086478 192.168.0.1     192.168.0.101   DNS       460 Standard query response 0x0003 AAAA www.m
```

```
> Frame 49: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{94D39D3B-31AF-4EC9-
> Ethernet II, Src: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb), Dst: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 51360, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

DNS query message type: A. No. query message doesn’t contain any answer.

Answer 14:



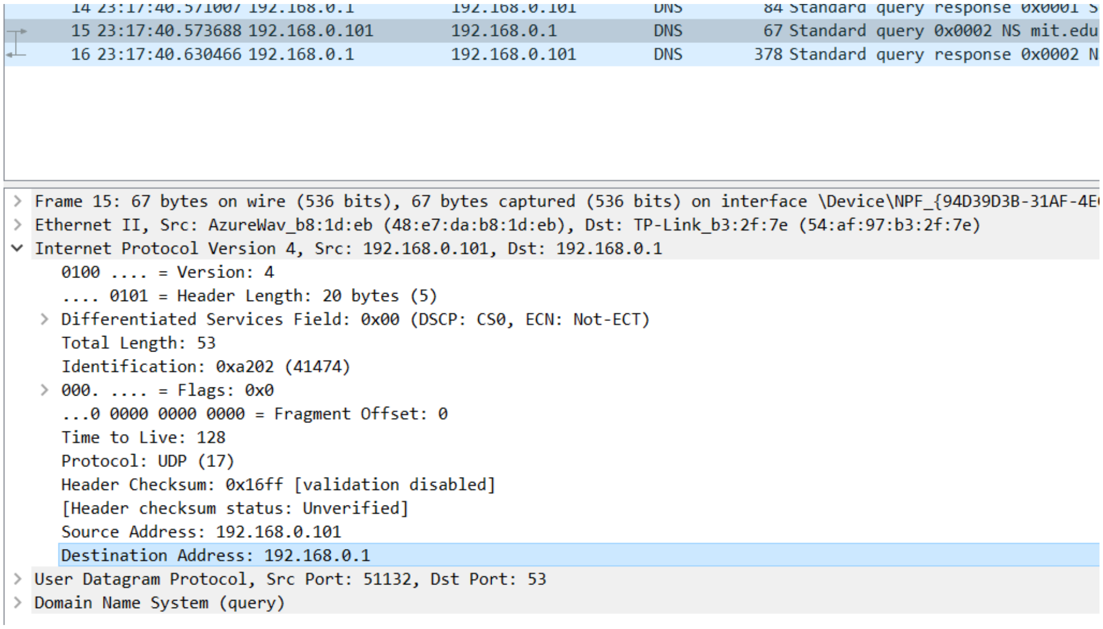
```
   49 23:12:41.471051 192.168.0.101   192.168.0.1     DNS        71 Standard query 0x0002 A www.mit.edu
   50 23:12:42.026295 192.168.0.1     192.168.0.101   DNS       416 Standard query response 0x0002 A www.mit.e
   51 23:12:42.030806 192.168.0.101   192.168.0.1     DNS        71 Standard query 0x0003 AAAA www.mit.edu
   52 23:12:42.086478 192.168.0.1     192.168.0.101   DNS       460 Standard query response 0x0003 AAAA www.mi
```

```
> Frame 50: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits) on interface \Device\NPF_{94D39D3B-31A
> Ethernet II, Src: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e), Dst: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
> User Datagram Protocol, Src Port: 53, Dst Port: 51360
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 13
    Additional RRs: 3
  v Queries
    v www.mit.edu: type A, class IN
        Name: www.mit.edu
        [Name Length: 11]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  v Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    > e9566.dscb.akamaiedge.net: type A, class IN, addr 23.207.142.26
  v Authoritative nameservers
```

Response message contain 3 answers.

Each of these answers contains: host name, type, class, ip address, CNAME.

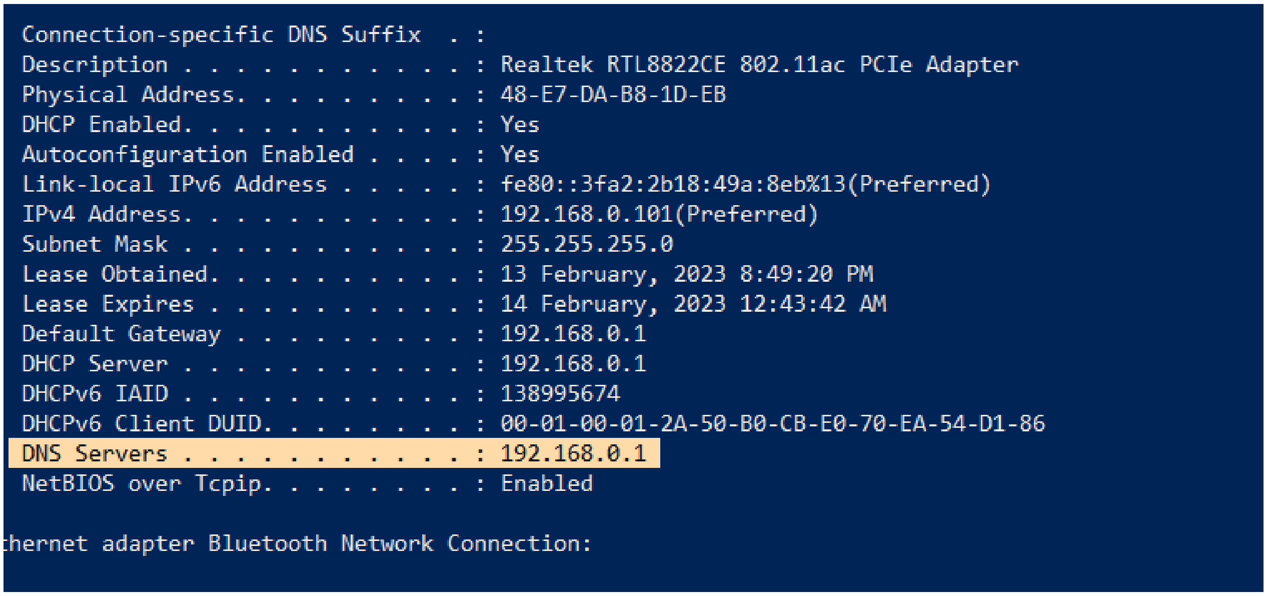
Answer 16:



```
   14 23:17:40.571007 192.168.0.1       192.168.0.101      DNS        84 Standard query response 0x0001 S
   15 23:17:40.573688 192.168.0.101     192.168.0.1        DNS        67 Standard query 0x0002 NS mit.edu
   16 23:17:40.630466 192.168.0.1       192.168.0.101      DNS       378 Standard query response 0x0002 N
```

```
> Frame 15: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{94D39D3B-31AF-4E
> Ethernet II, Src: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb), Dst: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e)
v Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 53
    Identification: 0xa202 (41474)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x16ff [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.101
    Destination Address: 192.168.0.1
> User Datagram Protocol, Src Port: 51132, Dst Port: 53
> Domain Name System (query)
```

DNS query message was sent to IP address: **192.168.0.1**

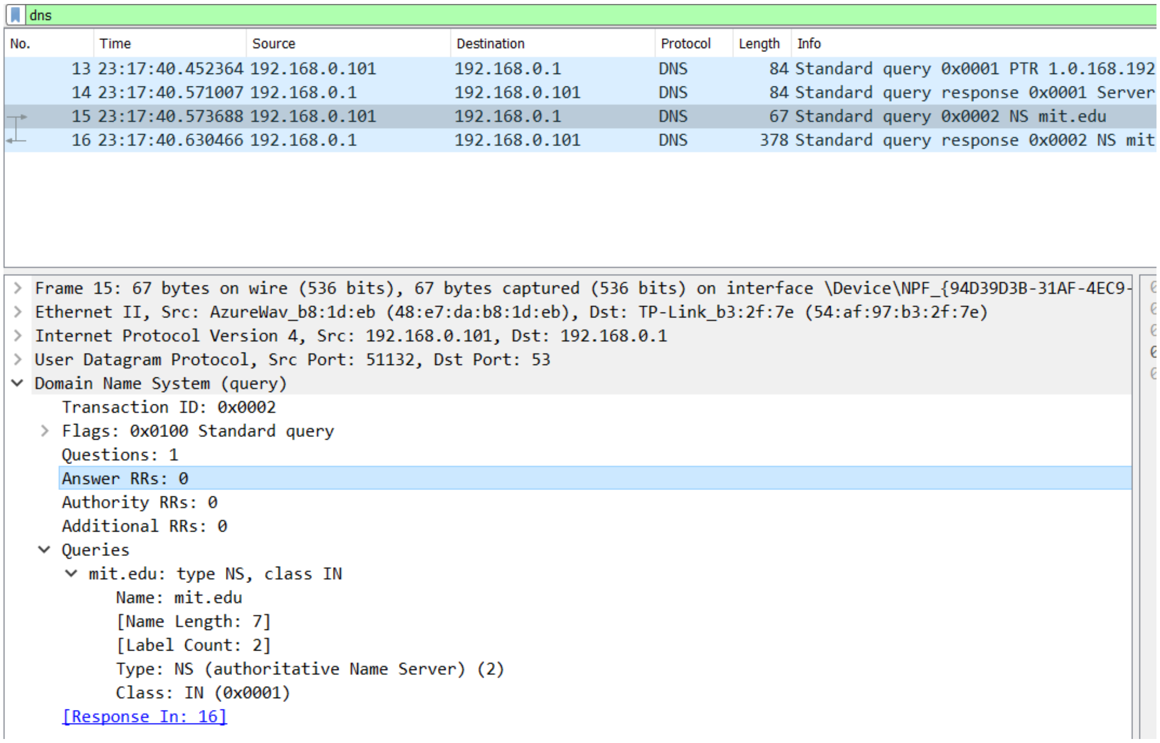


```
  Connection-specific DNS Suffix  . :
  Description . . . . . . . . . . . : Realtek RTL8822CE 802.11ac PCIe Adapter
  Physical Address. . . . . . . . . : 48-E7-DA-B8-1D-EB
  DHCP Enabled. . . . . . . . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::3fa2:2b18:49a:8eb%13(Preferred)
  IPv4 Address. . . . . . . . . . . : 192.168.0.101(Preferred)
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Lease Obtained. . . . . . . . . . : 13 February, 2023 8:49:20 PM
  Lease Expires . . . . . . . . . . : 14 February, 2023 12:43:42 AM
  Default Gateway . . . . . . . . . : 192.168.0.1
  DHCP Server . . . . . . . . . . . : 192.168.0.1
  DHCPv6 IAID . . . . . . . . . . . : 138995674
  DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-50-B0-CB-E0-70-EA-54-D1-86
  DNS Servers . . . . . . . . . . . : 192.168.0.1
  NetBIOS over Tcpip. . . . . . . . : Enabled

hernet adapter Bluetooth Network Connection:
```

Ip address of local DNS server: **192.168.0.**1

Both ip addresses are same.

Answer 17:

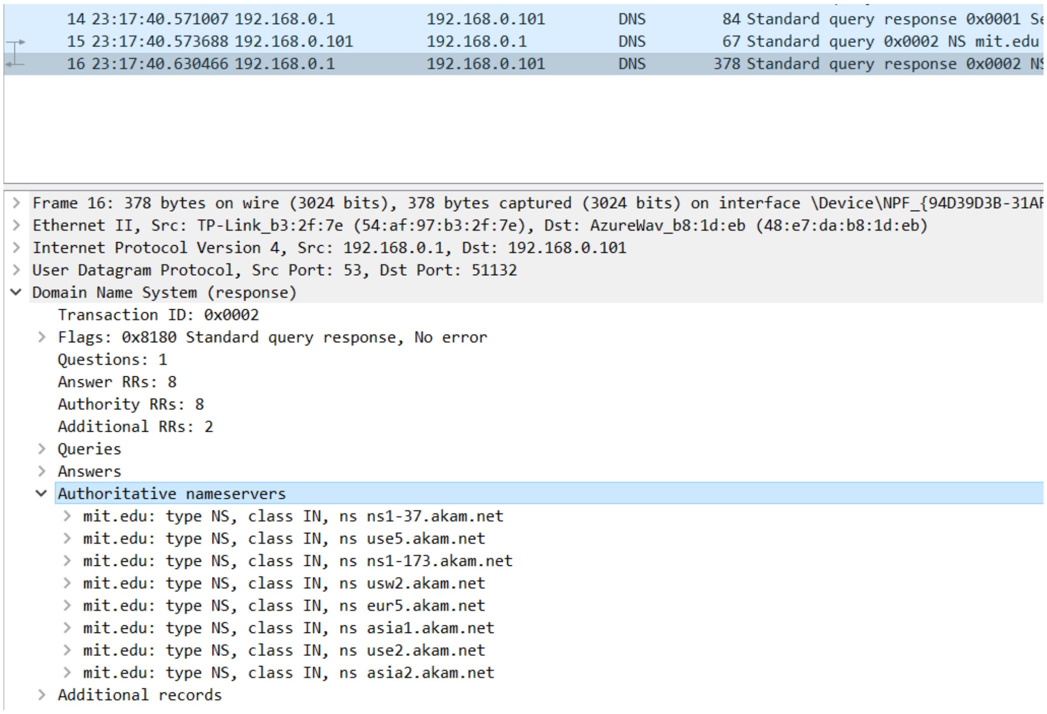


```
No.  Time             Source         Destination    Protocol Length Info
  13 23:17:40.452364 192.168.0.101  192.168.0.1    DNS      84 Standard query 0x0001 PTR 1.0.168.192
  14 23:17:40.571007 192.168.0.1    192.168.0.101  DNS      84 Standard query response 0x0001 Server
  15 23:17:40.573688 192.168.0.101  192.168.0.1    DNS      67 Standard query 0x0002 NS mit.edu
  16 23:17:40.630466 192.168.0.1    192.168.0.101  DNS     378 Standard query response 0x0002 NS mit
```

```
> Frame 15: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{94D39D3B-31AF-4EC9-
> Ethernet II, Src: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb), Dst: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 51132, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v mit.edu: type NS, class IN
        Name: mit.edu
        [Name Length: 7]
        [Label Count: 2]
        Type: NS (authoritative Name Server) (2)
        Class: IN (0x0001)
    [Response In: 16]
```

Type: NS. No, it doesn’t contain any answer.

Answer 18:

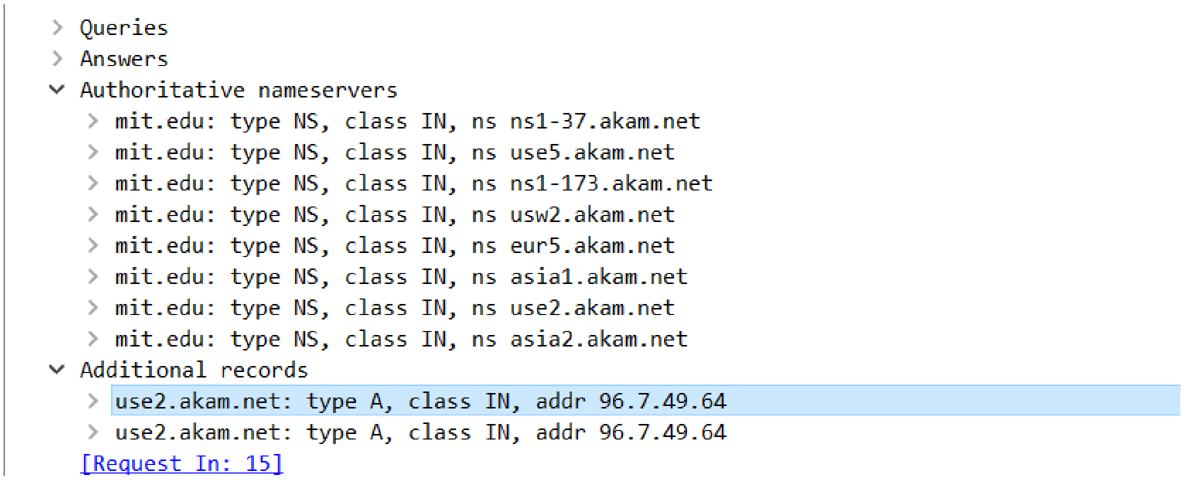


```
  14 23:17:40.571007 192.168.0.1    192.168.0.101  DNS      84 Standard query response 0x0001 Se
  15 23:17:40.573688 192.168.0.101  192.168.0.1    DNS      67 Standard query 0x0002 NS mit.edu
  16 23:17:40.630466 192.168.0.1    192.168.0.101  DNS     378 Standard query response 0x0002 NS
```

```
> Frame 16: 378 bytes on wire (3024 bits), 378 bytes captured (3024 bits) on interface \Device\NPF_{94D39D3B-31AF
> Ethernet II, Src: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e), Dst: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
> User Datagram Protocol, Src Port: 53, Dst Port: 51132
v Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 8
    Additional RRs: 2
  > Queries
  > Answers
  v Authoritative nameservers
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
  > Additional records
```

Total answer: 08

Each of the response contain> host name, type, class, server name.

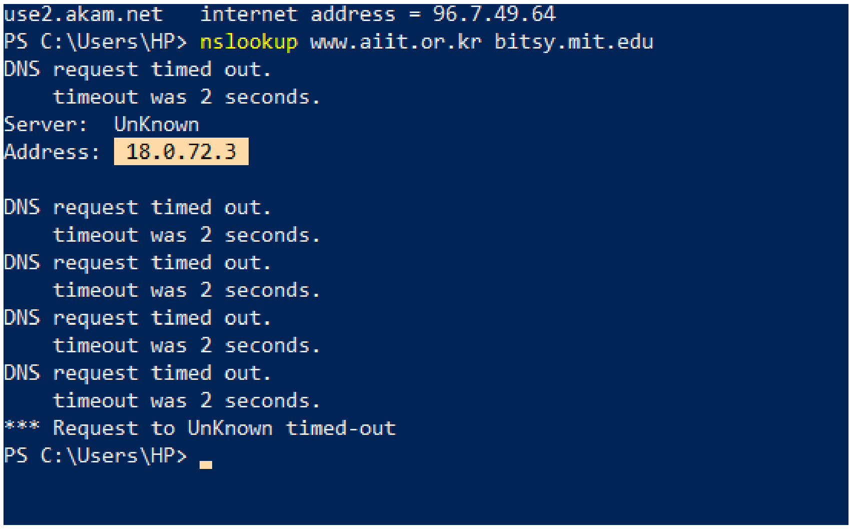


```
> Queries
> Answers
v Authoritative nameservers
    > mit.edu: type NS, class IN, ns ns1-37.akam.net
    > mit.edu: type NS, class IN, ns use5.akam.net
    > mit.edu: type NS, class IN, ns ns1-173.akam.net
    > mit.edu: type NS, class IN, ns usw2.akam.net
    > mit.edu: type NS, class IN, ns eur5.akam.net
    > mit.edu: type NS, class IN, ns asia1.akam.net
    > mit.edu: type NS, class IN, ns use2.akam.net
    > mit.edu: type NS, class IN, ns asia2.akam.net
v Additional records
    > use2.akam.net: type A, class IN, addr 96.7.49.64
    > use2.akam.net: type A, class IN, addr 96.7.49.64
  [Request In: 15]
```

In the additional records, the ip addresses are provided.

Answer 20:

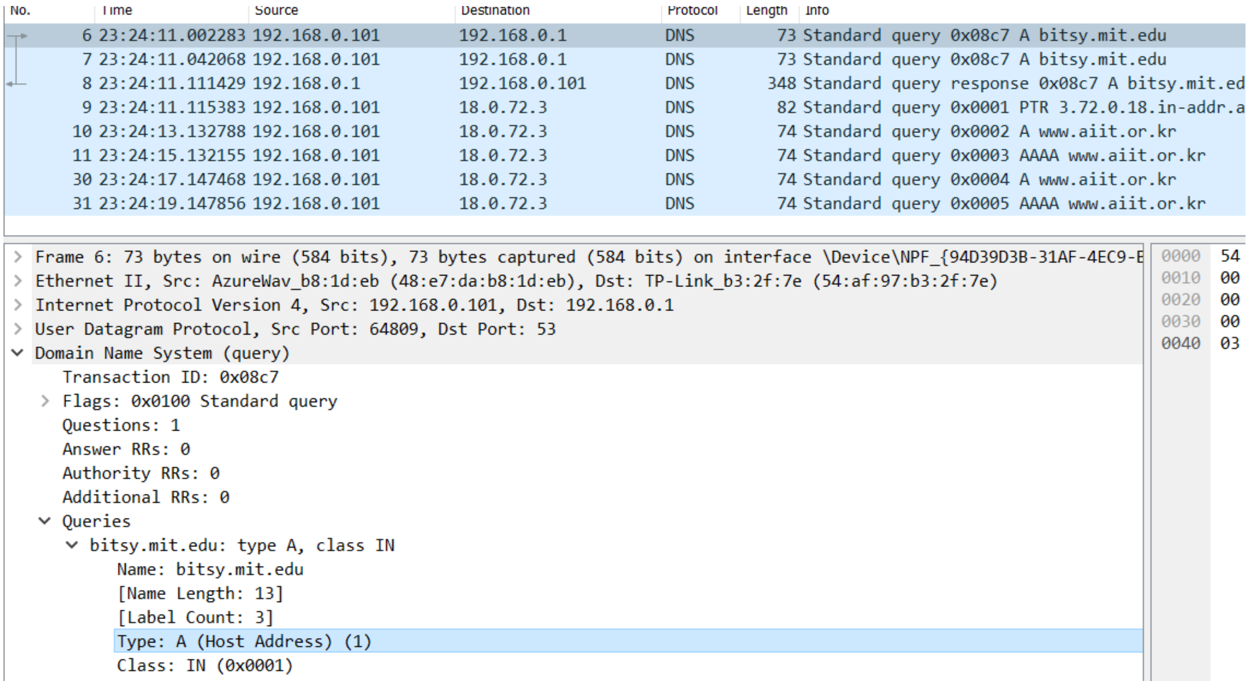
no, it is not the ip address of default local DNS server.



```
use2.akam.net   internet address = 96.7.49.64
PS C:\Users\HP> nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  18.0.72.3

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
PS C:\Users\HP>
```

Ip address: **18.0.72.3**

Answer 21:



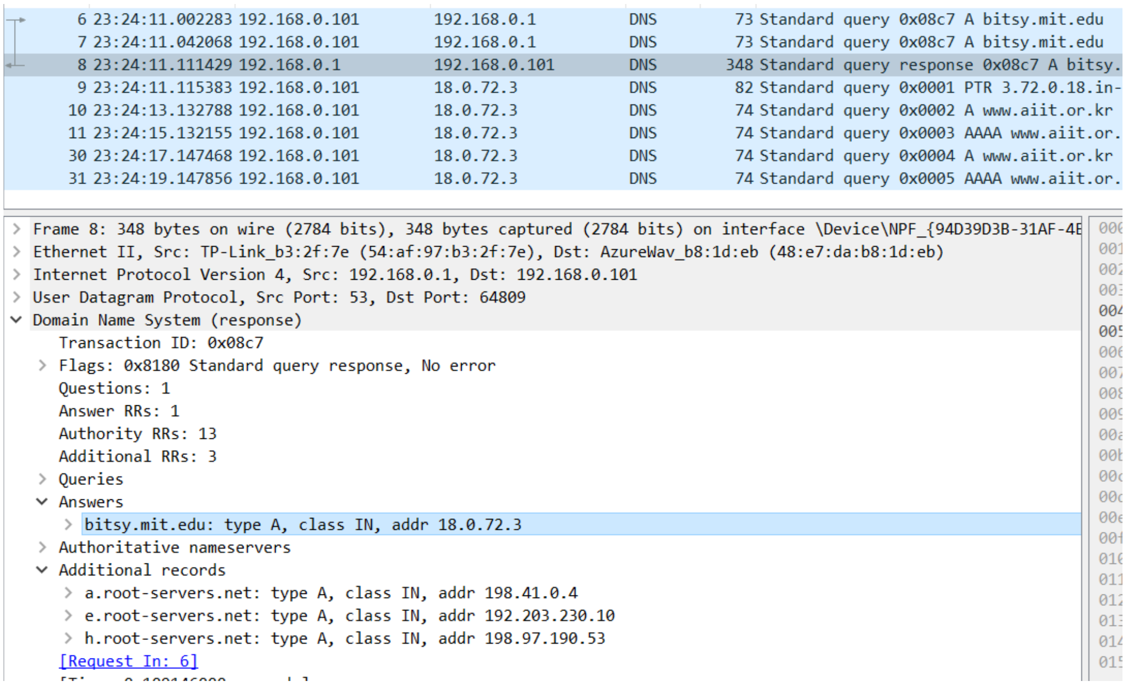
```
No.   Time            Source          Destination     Protocol Length Info
    6 23:24:11.002283 192.168.0.101   192.168.0.1     DNS       73 Standard query 0x08c7 A bitsy.mit.edu
    7 23:24:11.042068 192.168.0.101   192.168.0.1     DNS       73 Standard query 0x08c7 A bitsy.mit.edu
    8 23:24:11.111429 192.168.0.1     192.168.0.101   DNS      348 Standard query response 0x08c7 A bitsy.mit.ed
    9 23:24:11.115383 192.168.0.101   18.0.72.3       DNS       82 Standard query 0x0001 PTR 3.72.0.18.in-addr.a
   10 23:24:13.132788 192.168.0.101   18.0.72.3       DNS       74 Standard query 0x0002 A www.aiit.or.kr
   11 23:24:15.132155 192.168.0.101   18.0.72.3       DNS       74 Standard query 0x0003 AAAA www.aiit.or.kr
   30 23:24:17.147468 192.168.0.101   18.0.72.3       DNS       74 Standard query 0x0004 A www.aiit.or.kr
   31 23:24:19.147856 192.168.0.101   18.0.72.3       DNS       74 Standard query 0x0005 AAAA www.aiit.or.kr
```

```
> Frame 6: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{94D39D3B-31AF-4EC9-E
> Ethernet II, Src: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb), Dst: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e)
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.1
> User Datagram Protocol, Src Port: 64809, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x08c7
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v bitsy.mit.edu: type A, class IN
        Name: bitsy.mit.edu
        [Name Length: 13]
        [Label Count: 3]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

```
0000  54
0010  00
0020  00
0030  00
0040  03
```

type: A. no, it doesn’t contain any answer.

Answer 22:



```
    6 23:24:11.002283 192.168.0.101   192.168.0.1     DNS       73 Standard query 0x08c7 A bitsy.mit.edu
    7 23:24:11.042068 192.168.0.101   192.168.0.1     DNS       73 Standard query 0x08c7 A bitsy.mit.edu
    8 23:24:11.111429 192.168.0.1     192.168.0.101   DNS      348 Standard query response 0x08c7 A bitsy.
    9 23:24:11.115383 192.168.0.101   18.0.72.3       DNS       82 Standard query 0x0001 PTR 3.72.0.18.in-
   10 23:24:13.132788 192.168.0.101   18.0.72.3       DNS       74 Standard query 0x0002 A www.aiit.or.kr
   11 23:24:15.132155 192.168.0.101   18.0.72.3       DNS       74 Standard query 0x0003 AAAA www.aiit.or.
   30 23:24:17.147468 192.168.0.101   18.0.72.3       DNS       74 Standard query 0x0004 A www.aiit.or.kr
   31 23:24:19.147856 192.168.0.101   18.0.72.3       DNS       74 Standard query 0x0005 AAAA www.aiit.or.
```

```
> Frame 8: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface \Device\NPF_{94D39D3B-31AF-4E
> Ethernet II, Src: TP-Link_b3:2f:7e (54:af:97:b3:2f:7e), Dst: AzureWav_b8:1d:eb (48:e7:da:b8:1d:eb)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.101
> User Datagram Protocol, Src Port: 53, Dst Port: 64809
v Domain Name System (response)
    Transaction ID: 0x08c7
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 13
    Additional RRs: 3
  > Queries
  v Answers
    > bitsy.mit.edu: type A, class IN, addr 18.0.72.3
  > Authoritative nameservers
  v Additional records
    > a.root-servers.net: type A, class IN, addr 198.41.0.4
    > e.root-servers.net: type A, class IN, addr 192.203.230.10
    > h.root-servers.net: type A, class IN, addr 198.97.190.53
    [Request In: 6]
```

Answer: 1. Answer contains: host name, type, class, ip address.