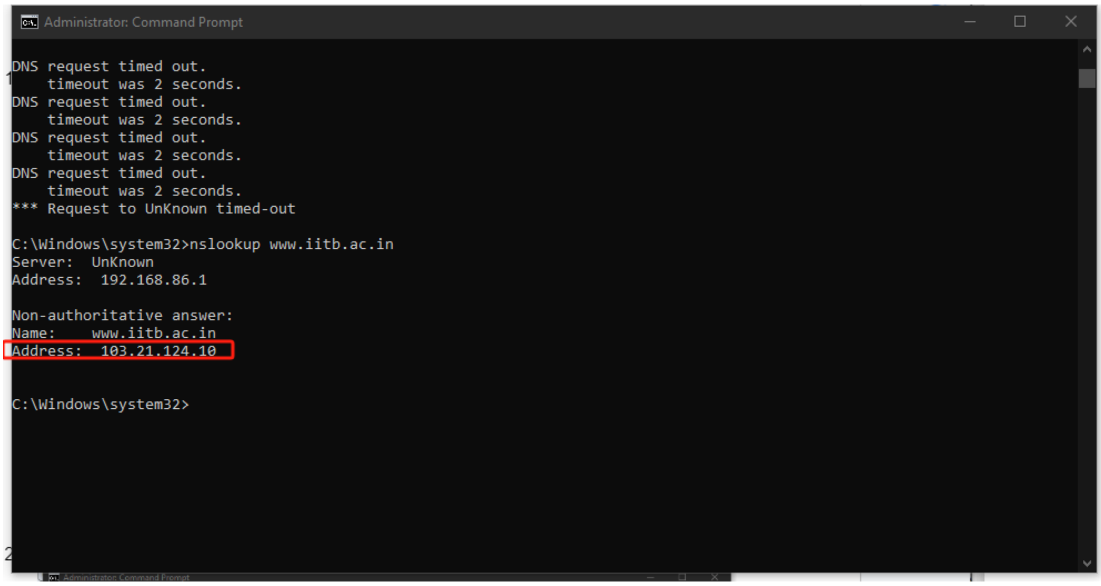
Sheng Wang

Wireshark-DHCP Lab 1

EE450

1. Run nslookup to obtain the IP address of the web server for the Indian Institute of Technology in Bombay, India: www.iitb.ac.in. What is the IP address of www.iitb.ac.in



```
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

C:\Windows\system32>nslookup www.iitb.ac.in
Server:  UnKnown
Address:  192.168.86.1

Non-authoritative answer:
Name:    www.iitb.ac.in
Address:  103.21.124.10


C:\Windows\system32>
```

The Ip address is: 103.21.124.10

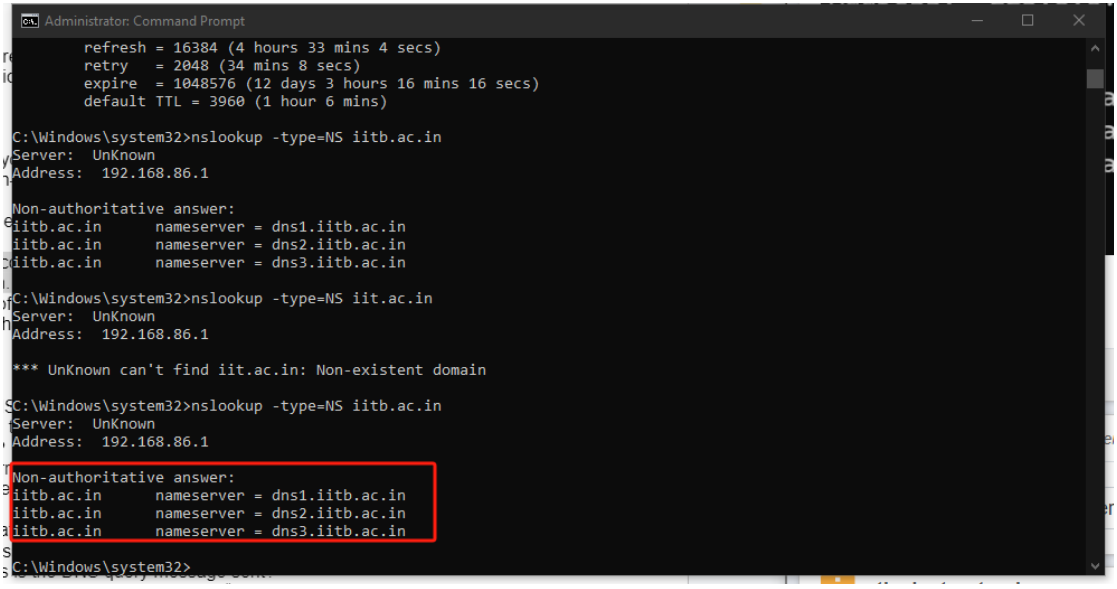
2. What is the IP address of the DNS server that provided the answer to your nslookup command in question 1 above?

   192.168.86.1

3. Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server?

   non-authoritative server

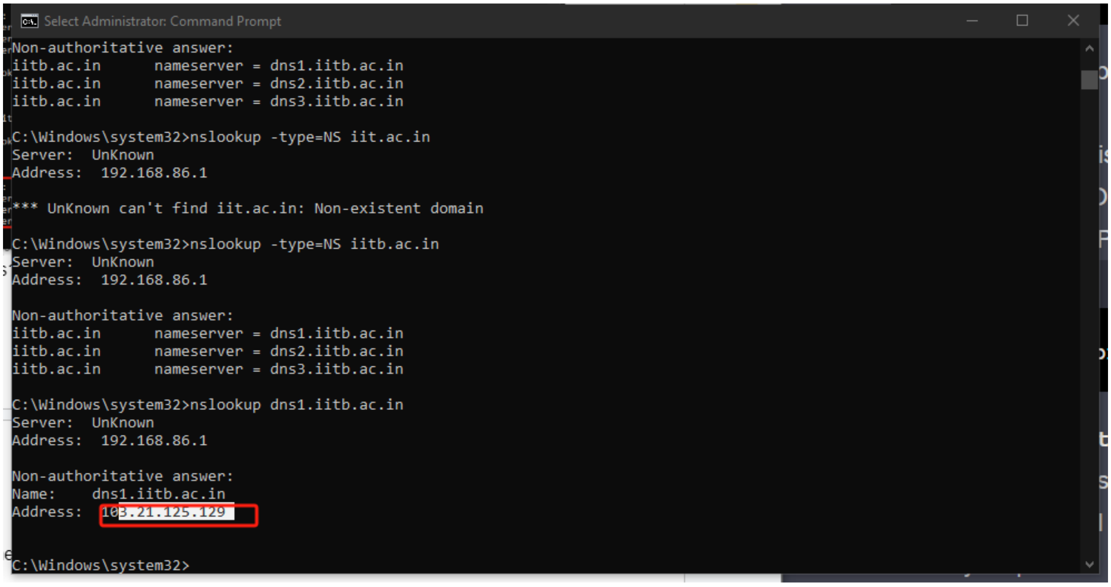
4. Use the nslookup command to determine the name of the authoritative name server for the iit.ac.in domain. What is that name? (If there are more than one authoritative servers, what is the name of the first authoritative server returned by nslookup)? If you had to find the IP address of that authoritative name server, how would you do so?



```
        refresh = 16384 (4 hours 33 mins 4 secs)
        retry   = 2048 (34 mins 8 secs)
        expire  = 1048576 (12 days 3 hours 16 mins 16 secs)
        default TTL = 3960 (1 hour 6 mins)

C:\Windows\system32>nslookup -type=NS iitb.ac.in
Server:  UnKnown
Address:  192.168.86.1

Non-authoritative answer:
iitb.ac.in      nameserver = dns1.iitb.ac.in
iitb.ac.in      nameserver = dns2.iitb.ac.in
iitb.ac.in      nameserver = dns3.iitb.ac.in

C:\Windows\system32>nslookup -type=NS iit.ac.in
Server:  UnKnown
Address:  192.168.86.1

*** UnKnown can't find iit.ac.in: Non-existent domain

C:\Windows\system32>nslookup -type=NS iitb.ac.in
Server:  UnKnown
Address:  192.168.86.1

Non-authoritative answer:
iitb.ac.in      nameserver = dns1.iitb.ac.in
iitb.ac.in      nameserver = dns2.iitb.ac.in
iitb.ac.in      nameserver = dns3.iitb.ac.in

C:\Windows\system32>
```

The first one is dns1.iitb.ac.in

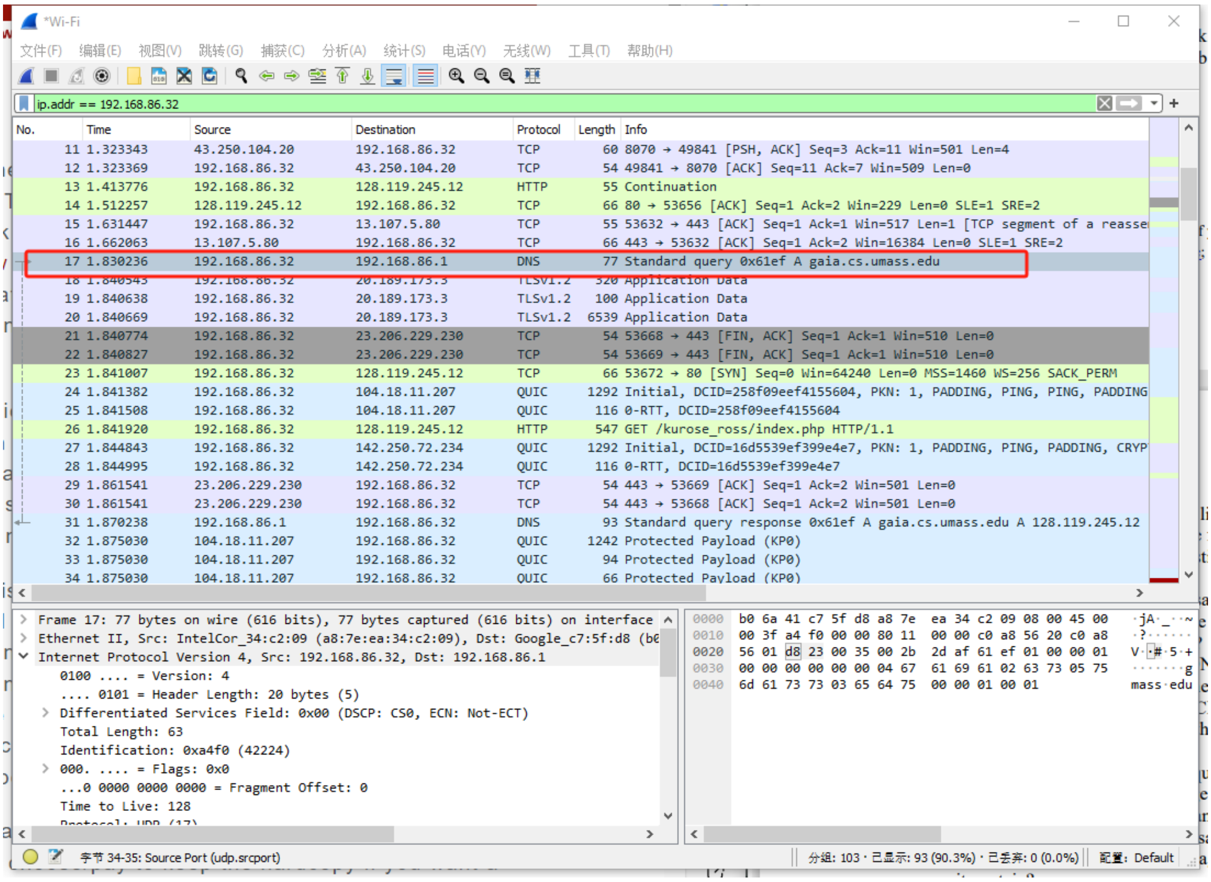
Use nslookup nameserver to get its ip address.



```
Non-authoritative answer:
iitb.ac.in      nameserver = dns1.iitb.ac.in
iitb.ac.in      nameserver = dns2.iitb.ac.in
iitb.ac.in      nameserver = dns3.iitb.ac.in

C:\Windows\system32>nslookup -type=NS iit.ac.in
Server:  UnKnown
Address:  192.168.86.1

*** UnKnown can't find iit.ac.in: Non-existent domain

C:\Windows\system32>nslookup -type=NS iitb.ac.in
Server:  UnKnown
Address:  192.168.86.1

Non-authoritative answer:
iitb.ac.in      nameserver = dns1.iitb.ac.in
iitb.ac.in      nameserver = dns2.iitb.ac.in
iitb.ac.in      nameserver = dns3.iitb.ac.in

C:\Windows\system32>nslookup dns1.iitb.ac.in
Server:  UnKnown
Address:  192.168.86.1

Non-authoritative answer:
Name:    dns1.iitb.ac.in
Address:  103.21.125.129

C:\Windows\system32>
```

The ip address of dns1.iitb.ac.in is 103.21.125.129

5. Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number6 in the trace for the DNS query message? Is this query message sent over UDP or TCP?


*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

ip.addr == 192.168.86.32

```
No.  Time       Source           Destination      Protocol Length Info
  11 1.323343   43.250.104.20    192.168.86.32    TCP        60 8070 → 49841 [PSH, ACK] Seq=3 Ack=11 Win=501 Len=4
  12 1.323369   192.168.86.32    43.250.104.20    TCP        54 49841 → 8070 [ACK] Seq=11 Ack=7 Win=509 Len=0
  13 1.413776   192.168.86.32    128.119.245.12   HTTP       55 Continuation
  14 1.512257   128.119.245.12   192.168.86.32    TCP        66 80 → 53656 [ACK] Seq=1 Ack=2 Win=229 Len=0 SLE=1 SRE=2
  15 1.631447   192.168.86.32    13.107.5.80      TCP        55 53632 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reasse
  16 1.662063   13.107.5.80      192.168.86.32    TCP        66 443 → 53632 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
  17 1.830236   192.168.86.32    192.168.86.1     DNS        77 Standard query 0x61ef A gaia.cs.umass.edu
  18 1.840543   192.168.86.32    20.189.173.3     TLSv1.2   320 Application Data
  19 1.840638   192.168.86.32    20.189.173.3     TLSv1.2   100 Application Data
  20 1.840669   192.168.86.32    20.189.173.3     TLSv1.2  6539 Application Data
  21 1.840774   192.168.86.32    23.206.229.230   TCP        54 53668 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  22 1.840827   192.168.86.32    23.206.229.230   TCP        54 53669 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  23 1.841007   192.168.86.32    128.119.245.12   TCP        66 53672 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  24 1.841382   192.168.86.32    104.18.11.207    QUIC     1292 Initial, DCID=258f09eef4155604, PKN: 1, PADDING, PING, PING, PADDING
  25 1.841508   192.168.86.32    104.18.11.207    QUIC      116 0-RTT, DCID=258f09eef4155604
  26 1.841920   192.168.86.32    128.119.245.12   HTTP      547 GET /kurose_ross/index.php HTTP/1.1
  27 1.844843   192.168.86.32    142.250.72.234   QUIC     1292 Initial, DCID=16d5539ef399e4e7, PKN: 1, PADDING, PING, PADDING, CRYP
  28 1.844995   192.168.86.32    142.250.72.234   QUIC      116 0-RTT, DCID=16d5539ef399e4e7
  29 1.861541   23.206.229.230   192.168.86.32    TCP        54 443 → 53669 [ACK] Seq=1 Ack=2 Win=501 Len=0
  30 1.861541   23.206.229.230   192.168.86.32    TCP        54 443 → 53668 [ACK] Seq=1 Ack=2 Win=501 Len=0
  31 1.870238   192.168.86.1     192.168.86.32    DNS        93 Standard query response 0x61ef A gaia.cs.umass.edu A 128.119.245.12
  32 1.875030   104.18.11.207    192.168.86.32    QUIC     1242 Protected Payload (KP0)
  33 1.875030   104.18.11.207    192.168.86.32    QUIC       94 Protected Payload (KP0)
  34 1.875030   104.18.11.207    192.168.86.32    QUIC       66 Protected Payload (KP0)
```

```
> Frame 17: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface
> Ethernet II, Src: IntelCor_34:c2:09 (a8:7e:ea:34:c2:09), Dst: Google_c7:5f:d8 (b0
v Internet Protocol Version 4, Src: 192.168.86.32, Dst: 192.168.86.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 63
    Identification: 0xa4f0 (42224)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
```

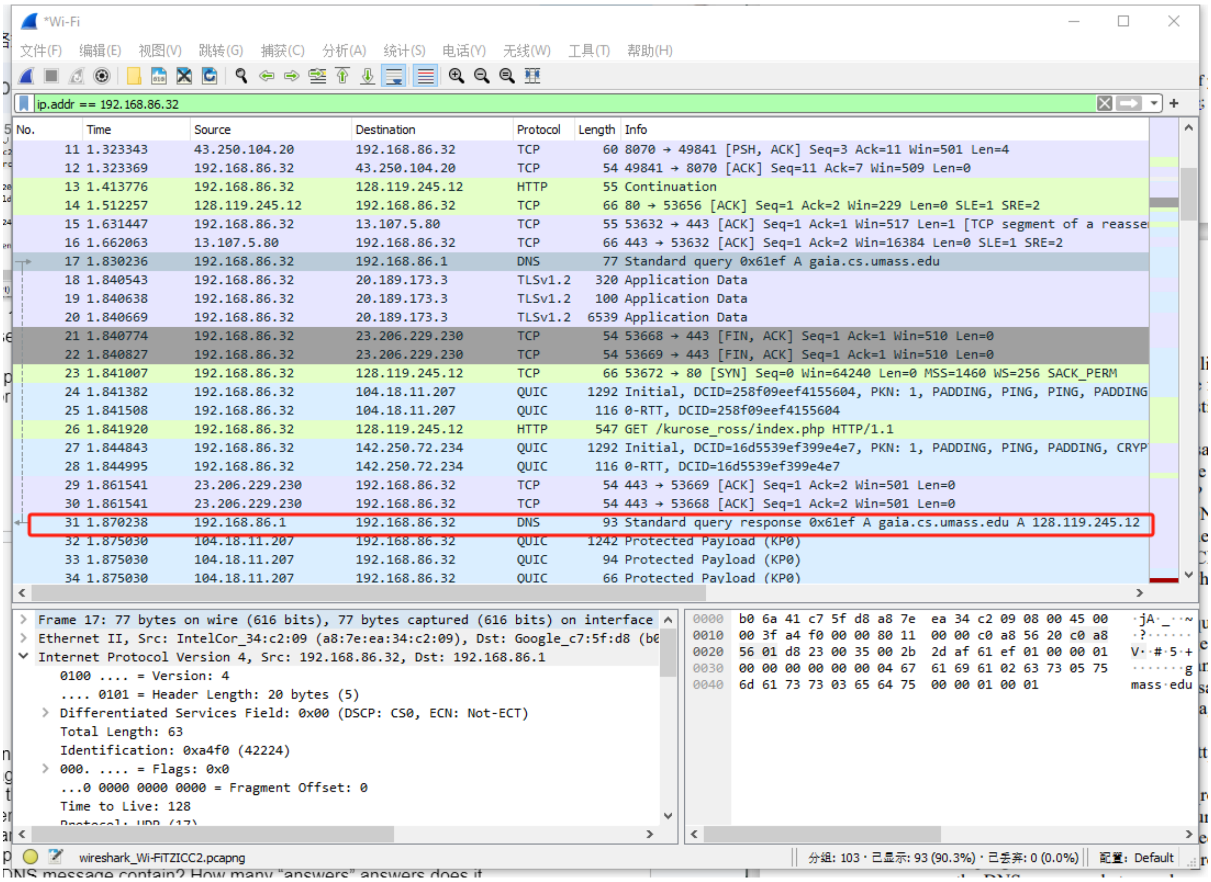
```
0000  b0 6a 41 c7 5f d8 a8 7e  ea 34 c2 09 08 00 45 00   ·jA·_··~
0010  00 3f a4 f0 00 00 80 11  00 00 c0 a8 56 20 c0 a8   ·?······
0020  56 01 d8 23 00 35 00 2b  2d af 61 ef 01 00 00 01   V··#·5·+
0030  00 00 00 00 00 00 04 67  61 69 61 02 63 73 05 75   ·······g
0040  6d 61 73 73 03 65 64 75  00 00 01 00 01            mass·edu
```

字节 34-35: Source Port (udp.srcport)   分组: 103 · 已显示: 93 (90.3%) · 已丢弃: 0 (0.0%)   配置: Default

The packet number is 17
This query message send through UDP

6. Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received

via UDP or TCP?


*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

ip.addr == 192.168.86.32

```
No.  Time       Source          Destination      Protocol  Length Info
  11 1.323343   43.250.104.20   192.168.86.32    TCP         60 8070 → 49841 [PSH, ACK] Seq=3 Ack=11 Win=501 Len=4
  12 1.323369   192.168.86.32   43.250.104.20    TCP         54 49841 → 8070 [ACK] Seq=11 Ack=7 Win=509 Len=0
  13 1.413776   192.168.86.32   128.119.245.12   HTTP        55 Continuation
  14 1.512257   128.119.245.12  192.168.86.32    TCP         66 80 → 53656 [ACK] Seq=1 Ack=2 Win=229 Len=0 SLE=1 SRE=2
  15 1.631447   192.168.86.32   13.107.5.80      TCP         55 53632 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reasse
  16 1.662063   13.107.5.80     192.168.86.32    TCP         66 443 → 53632 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
  17 1.830236   192.168.86.32   192.168.86.1     DNS         77 Standard query 0x61ef A gaia.cs.umass.edu
  18 1.840543   192.168.86.32   20.189.173.3     TLSv1.2    320 Application Data
  19 1.840638   192.168.86.32   20.189.173.3     TLSv1.2    100 Application Data
  20 1.840669   192.168.86.32   20.189.173.3     TLSv1.2   6539 Application Data
  21 1.840774   192.168.86.32   23.206.229.230   TCP         54 53668 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  22 1.840827   192.168.86.32   23.206.229.230   TCP         54 53669 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  23 1.841007   192.168.86.32   128.119.245.12   TCP         66 53672 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  24 1.841382   192.168.86.32   104.18.11.207    QUIC      1292 Initial, DCID=258f09eef4155604, PKN: 1, PADDING, PING, PING, PADDING
  25 1.841508   192.168.86.32   104.18.11.207    QUIC       116 0-RTT, DCID=258f09eef4155604
  26 1.841920   192.168.86.32   128.119.245.12   HTTP       547 GET /kurose_ross/index.php HTTP/1.1
  27 1.844843   192.168.86.32   142.250.72.234   QUIC      1292 Initial, DCID=16d5539ef399e4e7, PKN: 1, PADDING, PING, PADDING, CRYP
  28 1.844995   192.168.86.32   142.250.72.234   QUIC       116 0-RTT, DCID=16d5539ef399e4e7
  29 1.861541   23.206.229.230  192.168.86.32    TCP         54 443 → 53669 [ACK] Seq=1 Ack=2 Win=501 Len=0
  30 1.861541   23.206.229.230  192.168.86.32    TCP         54 443 → 53668 [ACK] Seq=1 Ack=2 Win=501 Len=0
  31 1.870238   192.168.86.1    192.168.86.32    DNS         93 Standard query response 0x61ef A gaia.cs.umass.edu A 128.119.245.12
  32 1.875030   104.18.11.207   192.168.86.32    QUIC      1242 Protected Payload (KP0)
  33 1.875030   104.18.11.207   192.168.86.32    QUIC        94 Protected Payload (KP0)
  34 1.875030   104.18.11.207   192.168.86.32    QUIC        66 Protected Payload (KP0)
```

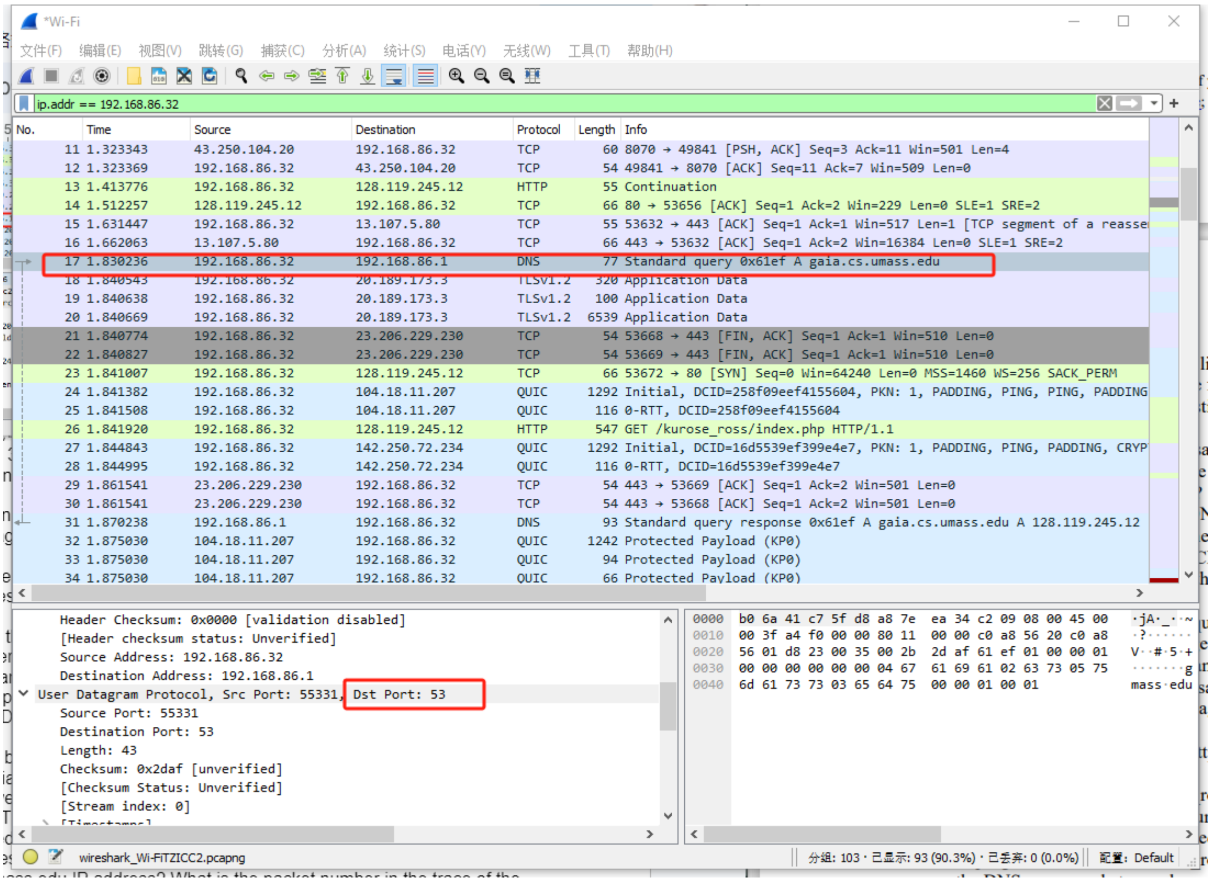
```
> Frame 17: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface
> Ethernet II, Src: IntelCor_34:c2:09 (a8:7e:ea:34:c2:09), Dst: Google_c7:5f:d8 (b0
v Internet Protocol Version 4, Src: 192.168.86.32, Dst: 192.168.86.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 63
    Identification: 0xa4f0 (42224)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
```

```
0000  b0 6a 41 c7 5f d8 a8 7e  ea 34 c2 09 08 00 45 00   ·jA·_··~
0010  00 3f a4 f0 00 00 80 11  00 00 c0 a8 56 20 c0 a8   ·?······
0020  56 01 d8 23 00 35 00 2b  2d af 61 ef 01 00 00 01   V··#·5·+
0030  00 00 00 00 00 00 04 67  61 69 61 02 63 73 05 75   ·······g
0040  6d 61 73 73 03 65 64 75  00 00 01 00 01            mass·edu
```

wireshark_Wi-FiTZICC2.pcapng　分组: 103 · 已显示: 93 (90.3%) · 已丢弃: 0 (0.0%)　配置: Default

The packet number is 31.
This message was sent through UDP.

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



*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

ip.addr == 192.168.86.32

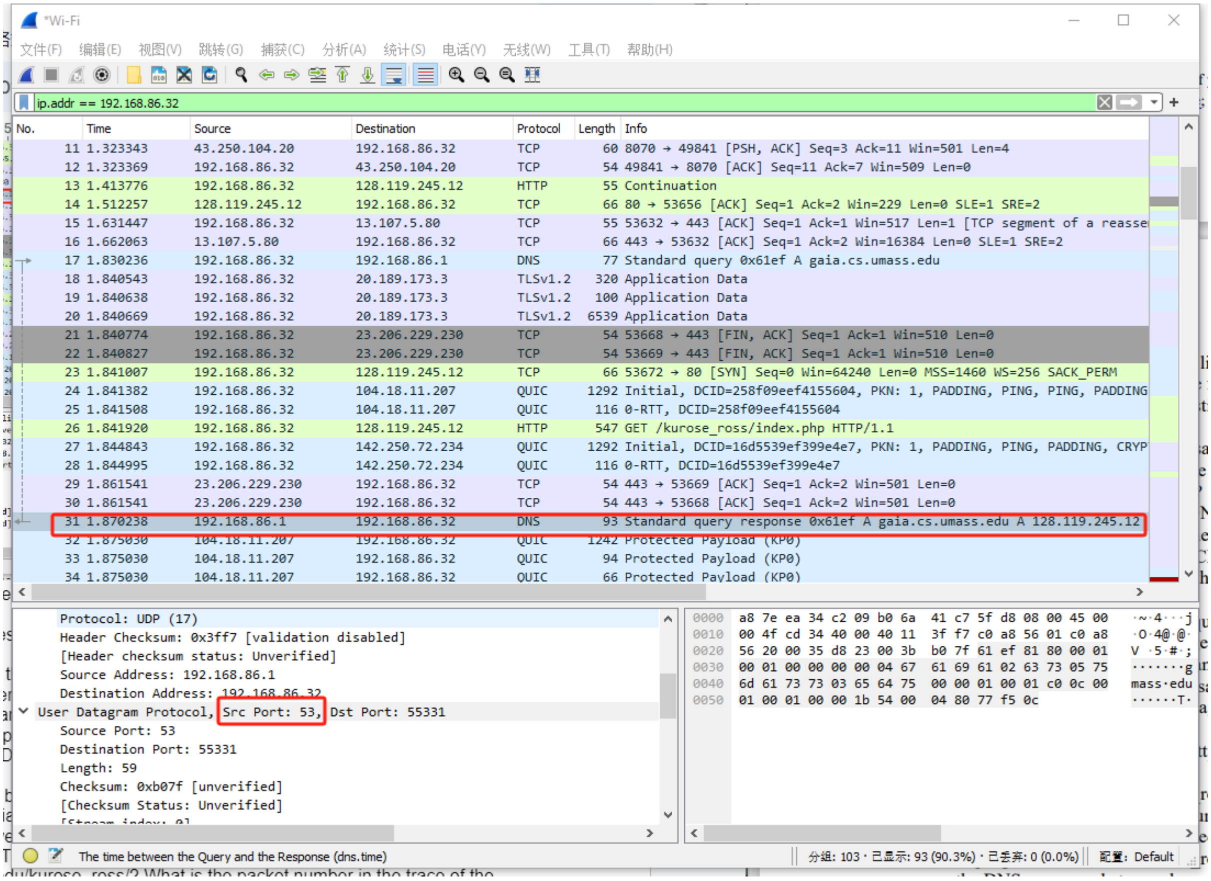
```
No.  Time      Source          Destination     Protocol Length Info
  11 1.323343  43.250.104.20   192.168.86.32   TCP        60 8070 → 49841 [PSH, ACK] Seq=3 Ack=11 Win=501 Len=4
  12 1.323369  192.168.86.32   43.250.104.20   TCP        54 49841 → 8070 [ACK] Seq=11 Ack=7 Win=509 Len=0
  13 1.413776  192.168.86.32   128.119.245.12  HTTP       55 Continuation
  14 1.512257  128.119.245.12  192.168.86.32   TCP        66 80 → 53656 [ACK] Seq=1 Ack=2 Win=229 Len=0 SLE=1 SRE=2
  15 1.631447  192.168.86.32   13.107.5.80     TCP        55 53632 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reasse
  16 1.662063  13.107.5.80     192.168.86.32   TCP        66 443 → 53632 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
  17 1.830236  192.168.86.32   192.168.86.1    DNS        77 Standard query 0x61ef A gaia.cs.umass.edu
  18 1.840543  192.168.86.32   20.189.173.3    TLSv1.2   320 Application Data
  19 1.840638  192.168.86.32   20.189.173.3    TLSv1.2   100 Application Data
  20 1.840669  192.168.86.32   20.189.173.3    TLSv1.2  6539 Application Data
  21 1.840774  192.168.86.32   23.206.229.230  TCP        54 53668 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  22 1.840827  192.168.86.32   23.206.229.230  TCP        54 53669 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  23 1.841007  192.168.86.32   128.119.245.12  TCP        66 53672 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  24 1.841382  192.168.86.32   104.18.11.207   QUIC     1292 Initial, DCID=258f09eef4155604, PKN: 1, PADDING, PING, PING, PADDING
  25 1.841508  192.168.86.32   104.18.11.207   QUIC      116 0-RTT, DCID=258f09eef4155604
  26 1.841920  192.168.86.32   128.119.245.12  HTTP      547 GET /kurose_ross/index.php HTTP/1.1
  27 1.844843  192.168.86.32   142.250.72.234  QUIC     1292 Initial, DCID=16d5539ef399e4e7, PKN: 1, PADDING, PING, PADDING, CRYP
  28 1.844995  192.168.86.32   142.250.72.234  QUIC      116 0-RTT, DCID=16d5539ef399e4e7
  29 1.861541  23.206.229.230  192.168.86.32   TCP        54 443 → 53669 [ACK] Seq=1 Ack=2 Win=501 Len=0
  30 1.861541  23.206.229.230  192.168.86.32   TCP        54 443 → 53668 [ACK] Seq=1 Ack=2 Win=501 Len=0
  31 1.870238  192.168.86.1    192.168.86.32   DNS        93 Standard query response 0x61ef A gaia.cs.umass.edu A 128.119.245.12
  32 1.875030  104.18.11.207   192.168.86.32   QUIC     1242 Protected Payload (KP0)
  33 1.875030  104.18.11.207   192.168.86.32   QUIC       94 Protected Payload (KP0)
  34 1.875030  104.18.11.207   192.168.86.32   QUIC       66 Protected Payload (KP0)
```

```
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.32
    Destination Address: 192.168.86.1
v User Datagram Protocol, Src Port: 55331, Dst Port: 53
    Source Port: 55331
    Destination Port: 53
    Length: 43
    Checksum: 0x2daf [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
```

```
0000  b0 6a 41 c7 5f d8 a8 7e  ea 34 c2 09 08 00 45 00   ·jA·_·~
0010  00 3f a4 f0 00 00 80 11  00 00 c0 a8 56 20 c0 a8   ·?······
0020  56 01 d8 23 00 35 00 2b  2d af 61 ef 01 00 00 01   V··#·5·+
0030  00 00 00 00 00 00 04 67  61 69 61 02 63 73 05 75   ·······g
0040  6d 61 73 73 03 65 64 75  00 00 01 00 01            mass·edu
```

wireshark_Wi-FiTZICC2.pcapng | 分组: 103 · 已显示: 93 (90.3%) · 已丢弃: 0 (0.0%) | 配置: Default

Destination port for the DNS query message is 53.



*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

ip.addr == 192.168.86.32

```
No.  Time      Source          Destination     Protocol Length Info
  11 1.323343  43.250.104.20   192.168.86.32   TCP        60 8070 → 49841 [PSH, ACK] Seq=3 Ack=11 Win=501 Len=4
  12 1.323369  192.168.86.32   43.250.104.20   TCP        54 49841 → 8070 [ACK] Seq=11 Ack=7 Win=509 Len=0
  13 1.413776  192.168.86.32   128.119.245.12  HTTP       55 Continuation
  14 1.512257  128.119.245.12  192.168.86.32   TCP        66 80 → 53656 [ACK] Seq=1 Ack=2 Win=229 Len=0 SLE=1 SRE=2
  15 1.631447  192.168.86.32   13.107.5.80     TCP        55 53632 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reasse
  16 1.662063  13.107.5.80     192.168.86.32   TCP        66 443 → 53632 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
  17 1.830236  192.168.86.32   192.168.86.1    DNS        77 Standard query 0x61ef A gaia.cs.umass.edu
  18 1.840543  192.168.86.32   20.189.173.3    TLSv1.2   320 Application Data
  19 1.840638  192.168.86.32   20.189.173.3    TLSv1.2   100 Application Data
  20 1.840669  192.168.86.32   20.189.173.3    TLSv1.2  6539 Application Data
  21 1.840774  192.168.86.32   23.206.229.230  TCP        54 53668 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  22 1.840827  192.168.86.32   23.206.229.230  TCP        54 53669 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  23 1.841007  192.168.86.32   128.119.245.12  TCP        66 53672 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  24 1.841382  192.168.86.32   104.18.11.207   QUIC     1292 Initial, DCID=258f09eef4155604, PKN: 1, PADDING, PING, PING, PADDING
  25 1.841508  192.168.86.32   104.18.11.207   QUIC      116 0-RTT, DCID=258f09eef4155604
  26 1.841920  192.168.86.32   128.119.245.12  HTTP      547 GET /kurose_ross/index.php HTTP/1.1
  27 1.844843  192.168.86.32   142.250.72.234  QUIC     1292 Initial, DCID=16d5539ef399e4e7, PKN: 1, PADDING, PING, PADDING, CRYP
  28 1.844995  192.168.86.32   142.250.72.234  QUIC      116 0-RTT, DCID=16d5539ef399e4e7
  29 1.861541  23.206.229.230  192.168.86.32   TCP        54 443 → 53669 [ACK] Seq=1 Ack=2 Win=501 Len=0
  30 1.861541  23.206.229.230  192.168.86.32   TCP        54 443 → 53668 [ACK] Seq=1 Ack=2 Win=501 Len=0
  31 1.870238  192.168.86.1    192.168.86.32   DNS        93 Standard query response 0x61ef A gaia.cs.umass.edu A 128.119.245.12
  32 1.875030  104.18.11.207   192.168.86.32   QUIC     1242 Protected Payload (KP0)
  33 1.875030  104.18.11.207   192.168.86.32   QUIC       94 Protected Payload (KP0)
  34 1.875030  104.18.11.207   192.168.86.32   QUIC       66 Protected Payload (KP0)
```

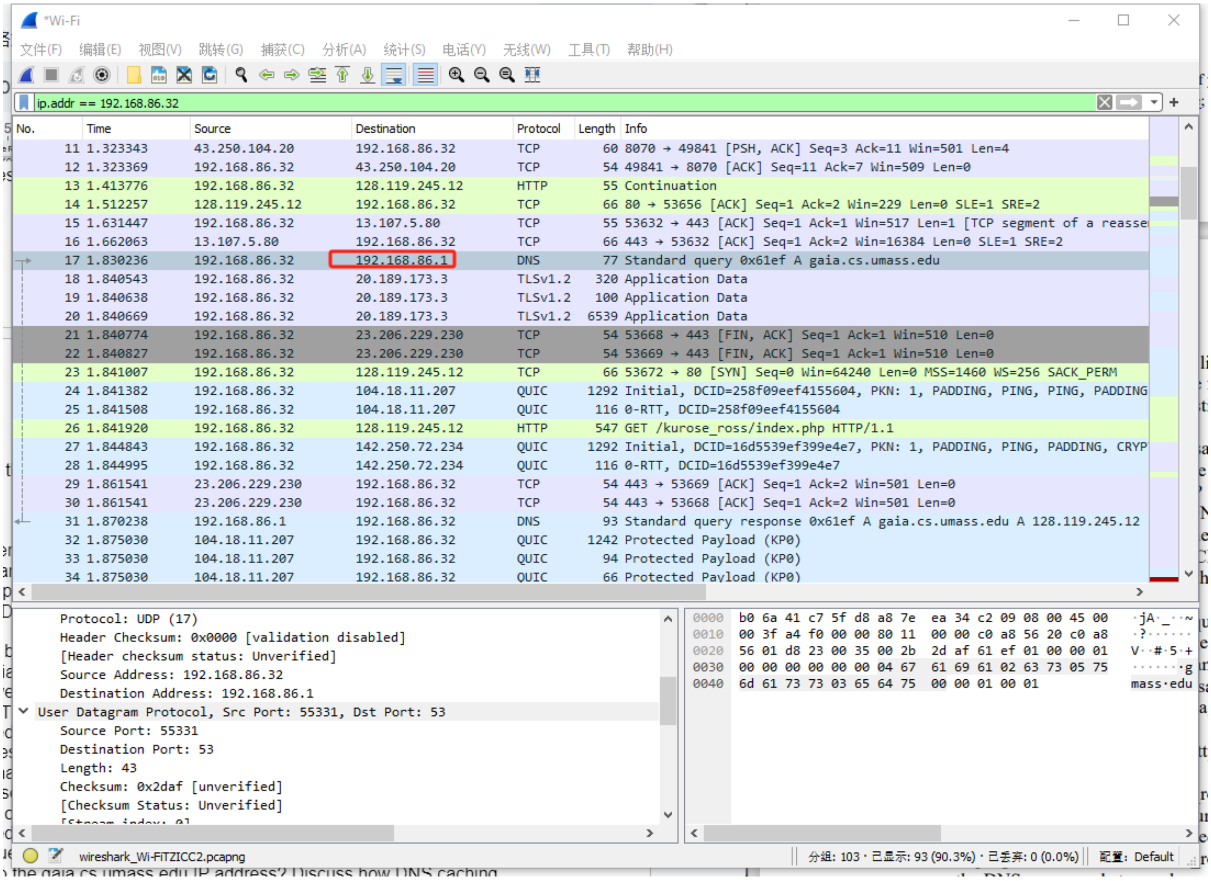
```
    Protocol: UDP (17)
    Header Checksum: 0x3ff7 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.1
    Destination Address: 192.168.86.32
v User Datagram Protocol, Src Port: 53, Dst Port: 55331
    Source Port: 53
    Destination Port: 55331
    Length: 59
    Checksum: 0xb07f [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
```

```
0000  a8 7e ea 34 c2 09 b0 6a  41 c7 5f d8 08 00 45 00   ·~·4···j
0010  00 4f cd 34 40 00 40 11  3f f7 c0 a8 56 01 c0 a8   ·O·4@·@·
0020  56 20 00 35 d8 23 00 3b  b0 7f 61 ef 81 80 00 01   V ·5·#·;
0030  00 01 00 00 00 00 04 67  61 69 61 02 63 73 05 75   ·······g
0040  6d 61 73 73 03 65 64 75  00 00 01 00 01 c0 0c 00   mass·edu
0050  01 00 01 00 00 1b 54 00  04 80 77 f5 0c            ······T·
```

The time between the Query and the Response (dns.time) | 分组: 103 · 已显示: 93 (90.3%) · 已丢弃: 0 (0.0%) | 配置: Default

Source port of DNS response message is 53

8. To what IP address is the DNS query message sent?


*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

ip.addr == 192.168.86.32

```
No.   Time      Source          Destination     Protocol Length Info
   11 1.323343  43.250.104.20   192.168.86.32   TCP        60 8070 → 49841 [PSH, ACK] Seq=3 Ack=11 Win=501 Len=4
   12 1.323369  192.168.86.32   43.250.104.20   TCP        54 49841 → 8070 [ACK] Seq=11 Ack=7 Win=509 Len=0
   13 1.413776  192.168.86.32   128.119.245.12  HTTP       55 Continuation
   14 1.512257  128.119.245.12  192.168.86.32   TCP        66 80 → 53656 [ACK] Seq=1 Ack=2 Win=229 Len=0 SLE=1 SRE=2
   15 1.631447  192.168.86.32   13.107.5.80     TCP        55 53632 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reasse
   16 1.662063  13.107.5.80     192.168.86.32   TCP        66 443 → 53632 [ACK] Seq=1 Ack=2 Win=16384 Len=0 SLE=1 SRE=2
   17 1.830236  192.168.86.32   192.168.86.1    DNS        77 Standard query 0x61ef A gaia.cs.umass.edu
   18 1.840543  192.168.86.32   20.189.173.3    TLSv1.2   320 Application Data
   19 1.840638  192.168.86.32   20.189.173.3    TLSv1.2   100 Application Data
   20 1.840669  192.168.86.32   20.189.173.3    TLSv1.2  6539 Application Data
   21 1.840774  192.168.86.32   23.206.229.230  TCP        54 53668 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
   22 1.840827  192.168.86.32   23.206.229.230  TCP        54 53669 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
   23 1.841007  192.168.86.32   128.119.245.12  TCP        66 53672 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   24 1.841382  192.168.86.32   104.18.11.207   QUIC     1292 Initial, DCID=258f09eef4155604, PKN: 1, PADDING, PING, PING, PADDING
   25 1.841508  192.168.86.32   104.18.11.207   QUIC      116 0-RTT, DCID=258f09eef4155604
   26 1.841920  192.168.86.32   128.119.245.12  HTTP      547 GET /kurose_ross/index.php HTTP/1.1
   27 1.844843  192.168.86.32   142.250.72.234  QUIC     1292 Initial, DCID=16d5539ef399e4e7, PKN: 1, PADDING, PING, PADDING, CRYP
   28 1.844995  192.168.86.32   142.250.72.234  QUIC      116 0-RTT, DCID=16d5539ef399e4e7
   29 1.861541  23.206.229.230  192.168.86.32   TCP        54 443 → 53669 [ACK] Seq=1 Ack=2 Win=501 Len=0
   30 1.861541  23.206.229.230  192.168.86.32   TCP        54 443 → 53668 [ACK] Seq=1 Ack=2 Win=501 Len=0
   31 1.870238  192.168.86.1    192.168.86.32   DNS        93 Standard query response 0x61ef A gaia.cs.umass.edu A 128.119.245.12
   32 1.875030  104.18.11.207   192.168.86.32   QUIC     1242 Protected Payload (KP0)
   33 1.875030  104.18.11.207   192.168.86.32   QUIC       94 Protected Payload (KP0)
   34 1.875030  104.18.11.207   192.168.86.32   QUIC       66 Protected Payload (KP0)
```

```
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.86.32
    Destination Address: 192.168.86.1
v User Datagram Protocol, Src Port: 55331, Dst Port: 53
    Source Port: 55331
    Destination Port: 53
    Length: 43
    Checksum: 0x2daf [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
```

```
0000  b0 6a 41 c7 5f d8 a8 7e  ea 34 c2 09 08 00 45 00   ·jA·_··~
0010  00 3f a4 f0 00 00 80 11  00 00 c0 a8 56 20 c0 a8   ·?······
0020  56 01 d8 23 00 35 00 2b  2d af 61 ef 01 00 00 01   V··#·5·+
0030  00 00 00 00 00 00 04 67  61 69 61 02 63 73 05 75   ·······g
0040  6d 61 73 73 03 65 64 75  00 00 01 00 01            mass·edu
```

wireshark_Wi-FiTZICC2.pcapng   分組: 103 · 已显示: 93 (90.3%) · 已丢弃: 0 (0.0%)   配置: Default

The ip address is 192.168.86.1

9. Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

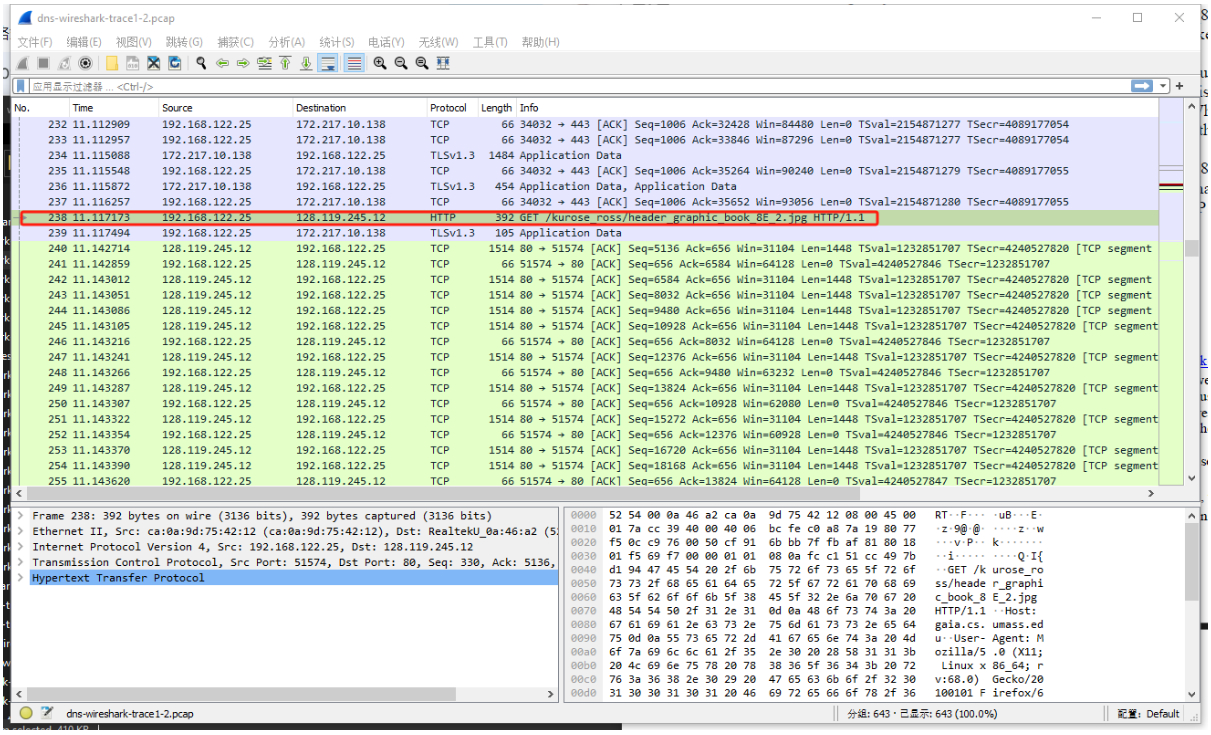
There is one question in the DNS query message.
There is no answer in this query message.

10. Examine the DNS response message to the initial query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

There is one question in this DNS response message.
There is one answer in this DNS response.

11. The web page for the base file http://gaia.cs.umass.edu/kurose_ross/ references the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg , which, like the base webpage, is on gaia.cs.umass.edu. What is the packet number in the trace for the initial HTTP GET request for the base file http://gaia.cs.umass.edu/kurose_ross/? What is the packet number in the trace of the DNS query made to resolve gaia.cs.umass.edu so that this initial HTTP request can be sent to the gaia.cs.umass.edu IP address? What is the packet number in the trace of the received DNS response? What is the packet number in the trace for the HTTP GET request for the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg? What is the packet number in the DNS query made to resolve gaia.cs.umass.edu so that this second HTTP request can be sent to the gaia.cs.umass.edu IP address? Discuss how DNS caching affects the answer to this last question.

1. The packet number is 26 for init visiting
2. number 17(Q5)
3. number 31(Q6)
4. I did not find the packet to get this picture. I use the trace file which was provided by the author. The packet number for getting this image is 238



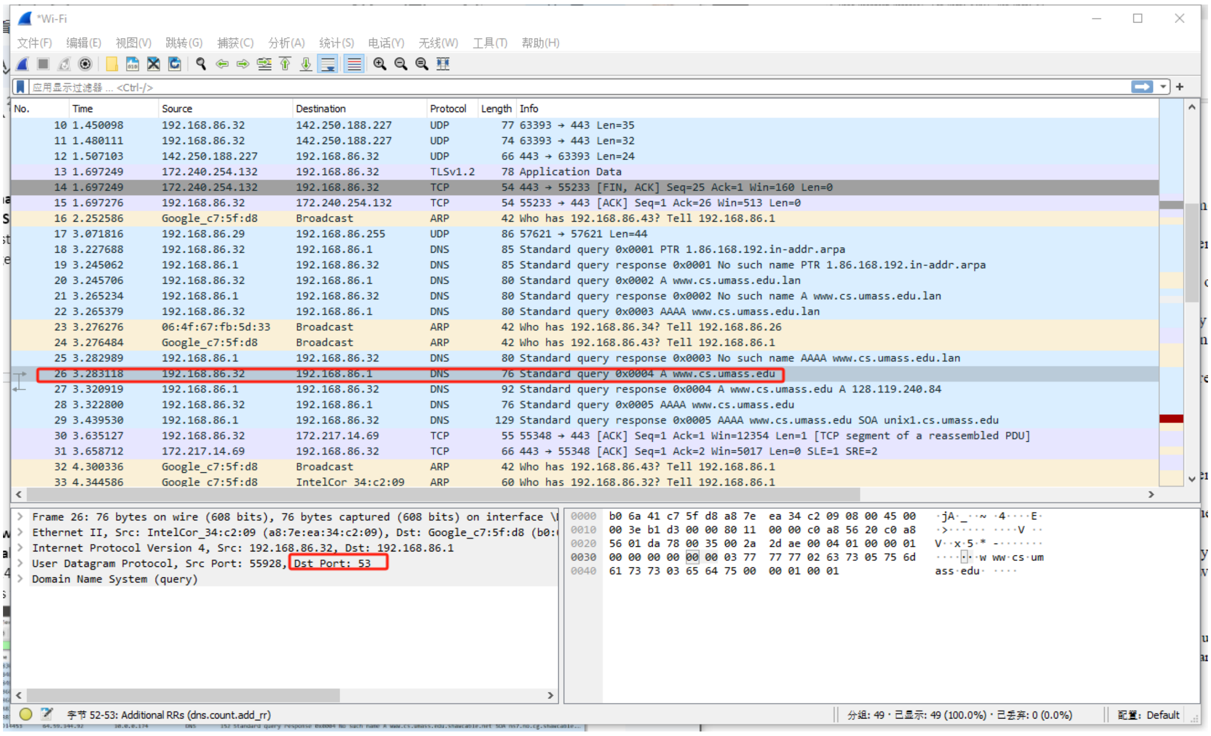
```
No.   Time       Source          Destination     Protocol Length Info
  232 11.112909  192.168.122.25  172.217.10.138  TCP        66 34032 → 443 [ACK] Seq=1006 Ack=32428 Win=84480 Len=0 TSval=2154871277 TSecr=4089177054
  233 11.112957  192.168.122.25  172.217.10.138  TCP        66 34032 → 443 [ACK] Seq=1006 Ack=33846 Win=87296 Len=0 TSval=2154871277 TSecr=4089177054
  234 11.115088  172.217.10.138  192.168.122.25  TLSv1.3  1484 Application Data
  235 11.115548  192.168.122.25  172.217.10.138  TCP        66 34032 → 443 [ACK] Seq=1006 Ack=35264 Win=90240 Len=0 TSval=2154871279 TSecr=4089177055
  236 11.115872  172.217.10.138  192.168.122.25  TLSv1.3   454 Application Data, Application Data
  237 11.116257  192.168.122.25  172.217.10.138  TCP        66 34032 → 443 [ACK] Seq=1006 Ack=35652 Win=93056 Len=0 TSval=2154871280 TSecr=4089177055
  238 11.117173  192.168.122.25  128.119.245.12  HTTP      392 GET /kurose_ross/header_graphic_book_8E_2.jpg HTTP/1.1
  239 11.117494  192.168.122.25  172.217.10.138  TLSv1.3   105 Application Data
  240 11.142714  128.119.245.12  192.168.122.25  TCP      1514 80 → 51574 [ACK] Seq=5136 Ack=656 Win=31104 Len=1448 TSval=1232851707 TSecr=4240527820 [TCP segment
  241 11.142859  192.168.122.25  128.119.245.12  TCP        66 51574 → 80 [ACK] Seq=656 Ack=6584 Win=64128 Len=0 TSval=4240527846 TSecr=1232851707
  242 11.143012  128.119.245.12  192.168.122.25  TCP      1514 80 → 51574 [ACK] Seq=6584 Ack=656 Win=31104 Len=1448 TSval=1232851707 TSecr=4240527820 [TCP segment
  243 11.143051  128.119.245.12  192.168.122.25  TCP      1514 80 → 51574 [ACK] Seq=8032 Ack=656 Win=31104 Len=1448 TSval=1232851707 TSecr=4240527820 [TCP segment
  244 11.143086  128.119.245.12  192.168.122.25  TCP      1514 80 → 51574 [ACK] Seq=9480 Ack=656 Win=31104 Len=1448 TSval=1232851707 TSecr=4240527820 [TCP segment
  245 11.143105  128.119.245.12  192.168.122.25  TCP      1514 80 → 51574 [ACK] Seq=10928 Ack=656 Win=31104 Len=1448 TSval=1232851707 TSecr=4240527820 [TCP segment
  246 11.143216  192.168.122.25  128.119.245.12  TCP        66 51574 → 80 [ACK] Seq=656 Ack=8032 Win=64128 Len=0 TSval=4240527846 TSecr=1232851707
  247 11.143241  128.119.245.12  192.168.122.25  TCP      1514 80 → 51574 [ACK] Seq=12376 Ack=656 Win=31104 Len=1448 TSval=1232851707 TSecr=4240527820 [TCP segment
  248 11.143266  192.168.122.25  128.119.245.12  TCP        66 51574 → 80 [ACK] Seq=656 Ack=9480 Win=63232 Len=0 TSval=4240527846 TSecr=1232851707
  249 11.143287  128.119.245.12  192.168.122.25  TCP      1514 80 → 51574 [ACK] Seq=13824 Ack=656 Win=31104 Len=1448 TSval=1232851707 TSecr=4240527820 [TCP segment
  250 11.143307  192.168.122.25  128.119.245.12  TCP        66 51574 → 80 [ACK] Seq=656 Ack=10928 Win=62080 Len=0 TSval=4240527846 TSecr=1232851707
  251 11.143322  128.119.245.12  192.168.122.25  TCP      1514 80 → 51574 [ACK] Seq=15272 Ack=656 Win=31104 Len=1448 TSval=1232851707 TSecr=4240527820 [TCP segment
  252 11.143354  192.168.122.25  128.119.245.12  TCP        66 51574 → 80 [ACK] Seq=656 Ack=12376 Win=60928 Len=0 TSval=4240527846 TSecr=1232851707
  253 11.143370  128.119.245.12  192.168.122.25  TCP      1514 80 → 51574 [ACK] Seq=16720 Ack=656 Win=31104 Len=1448 TSval=1232851707 TSecr=4240527820 [TCP segment
  254 11.143390  128.119.245.12  192.168.122.25  TCP      1514 80 → 51574 [ACK] Seq=18168 Ack=656 Win=31104 Len=1448 TSval=1232851707 TSecr=4240527820 [TCP segment
  255 11.143620  192.168.122.25  128.119.245.12  TCP        66 51574 → 80 [ACK] Seq=656 Ack=13824 Win=64128 Len=0 TSval=4240527847 TSecr=1232851707
```

```
> Frame 238: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits)
> Ethernet II, Src: ca:0a:9d:75:42:12 (ca:0a:9d:75:42:12), Dst: RealtekU_0a:46:a2 (5:
> Internet Protocol Version 4, Src: 192.168.122.25, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51574, Dst Port: 80, Seq: 330, Ack: 5136,
> Hypertext Transfer Protocol
```

```
0000  52 54 00 0a 46 a2 ca 0a  9d 75 42 12 08 00 45 00   RT··F··· ·uB···E·
0010  01 7a cc 39 40 00 40 06  bc fe c0 a8 7a 19 80 77   ·z·9@·@· ····z··w
0020  f5 0c c9 76 00 50 cf 91  6b bb 7f fb af 81 80 18   ···v·P·· k·······
0030  01 f5 69 f7 00 00 01 01  08 0a fc c1 51 cc 49 7b   ··i····· ····Q·I{
0040  d1 94 47 45 54 20 2f 6b  75 72 6f 73 65 5f 72 6f   ··GET /k urose_ro
0050  73 73 2f 68 65 61 64 65  72 5f 67 72 61 70 68 69   ss/heade r_graphi
0060  63 5f 62 6f 6f 6b 5f 38  45 5f 32 2e 6a 70 67 20   c_book_8 E_2.jpg
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host:
0080  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
0090  75 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   u··User- Agent: M
00a0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
00b0  20 4c 69 6e 75 78 20 78  38 36 5f 36 34 3b 20 72    Linux x 86_64; r
00c0  76 3a 36 38 2e 30 29 20  47 65 63 6b 6f 2f 32 30   v:68.0)  Gecko/20
00d0  31 30 30 31 30 31 20 46  69 72 65 66 6f 78 2f 36   100101 F irefox/6
```

5. No DNS query and response, DNS caching will cache the record of previous DNS response, after live time, the corresponding cache will disappear. Thus, in living time. the host does not need to ask the DNS server, just go to the DNS cache to find the answer.

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



*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 ... <Ctrl-/>

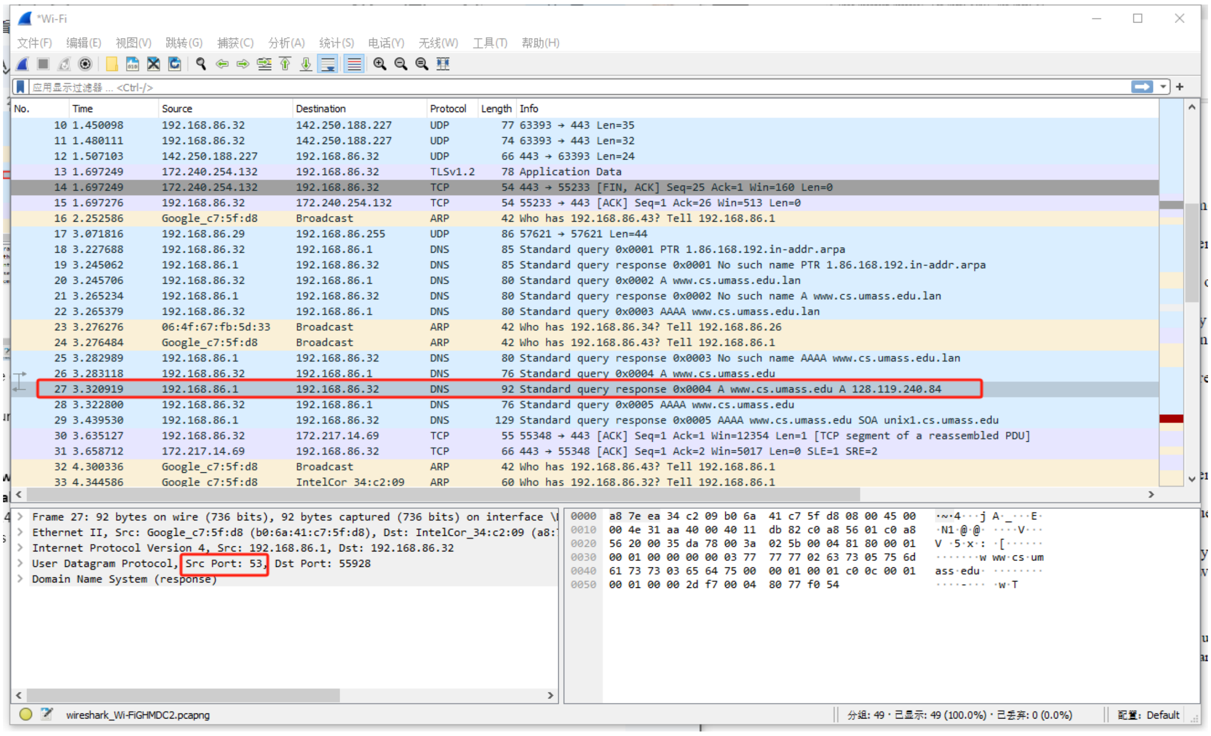
```
No.   Time      Source             Destination      Protocol Length Info
   10 1.450098  192.168.86.32      142.250.188.227  UDP        77 63393 → 443 Len=35
   11 1.480111  192.168.86.32      142.250.188.227  UDP        74 63393 → 443 Len=32
   12 1.507103  142.250.188.227    192.168.86.32    UDP        66 443 → 63393 Len=24
   13 1.697249  172.240.254.132    192.168.86.32    TLSv1.2    78 Application Data
   14 1.697249  172.240.254.132    192.168.86.32    TCP        54 443 → 55233 [FIN, ACK] Seq=25 Ack=1 Win=160 Len=0
   15 1.697276  192.168.86.32      172.240.254.132  TCP        54 55233 → 443 [ACK] Seq=1 Ack=26 Win=513 Len=0
   16 2.252586  Google_c7:5f:d8    Broadcast        ARP        42 Who has 192.168.86.43? Tell 192.168.86.1
   17 3.071816  192.168.86.29      192.168.86.255   UDP        86 57621 → 57621 Len=44
   18 3.227688  192.168.86.32      192.168.86.1     DNS        85 Standard query 0x0001 PTR 1.86.168.192.in-addr.arpa
   19 3.245062  192.168.86.1       192.168.86.32    DNS        85 Standard query response 0x0001 No such name PTR 1.86.168.192.in-addr.arpa
   20 3.245706  192.168.86.32      192.168.86.1     DNS        80 Standard query 0x0002 A www.cs.umass.edu.lan
   21 3.265234  192.168.86.1       192.168.86.32    DNS        80 Standard query response 0x0002 No such name A www.cs.umass.edu.lan
   22 3.265379  192.168.86.32      192.168.86.1     DNS        80 Standard query 0x0003 AAAA www.cs.umass.edu.lan
   23 3.276276  06:4f:67:fb:5d:33  Broadcast        ARP        42 Who has 192.168.86.34? Tell 192.168.86.26
   24 3.276484  Google_c7:5f:d8    Broadcast        ARP        42 Who has 192.168.86.43? Tell 192.168.86.1
   25 3.282989  192.168.86.1       192.168.86.32    DNS        80 Standard query response 0x0003 No such name AAAA www.cs.umass.edu.lan
   26 3.283118  192.168.86.32      192.168.86.1     DNS        76 Standard query 0x0004 A www.cs.umass.edu
   27 3.320919  192.168.86.1       192.168.86.32    DNS        92 Standard query response 0x0004 A www.cs.umass.edu A 128.119.240.84
   28 3.322800  192.168.86.32      192.168.86.1     DNS        76 Standard query 0x0005 AAAA www.cs.umass.edu
   29 3.439530  192.168.86.1       192.168.86.32    DNS       129 Standard query response 0x0005 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu
   30 3.635127  192.168.86.32      172.217.14.69    TCP        55 55348 → 443 [ACK] Seq=1 Ack=1 Win=12354 Len=1 [TCP segment of a reassembled PDU]
   31 3.658712  172.217.14.69      192.168.86.32    TCP        66 443 → 55348 [ACK] Seq=1 Ack=2 Win=5017 Len=0 SLE=1 SRE=2
   32 4.300336  Google_c7:5f:d8    Broadcast        ARP        42 Who has 192.168.86.43? Tell 192.168.86.1
   33 4.344586  Google_c7:5f:d8    IntelCor_34:c2:09 ARP       60 Who has 192.168.86.32? Tell 192.168.86.1
```

```
> Frame 26: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \
> Ethernet II, Src: IntelCor_34:c2:09 (a8:7e:ea:34:c2:09), Dst: Google_c7:5f:d8 (b0:
> Internet Protocol Version 4, Src: 192.168.86.32, Dst: 192.168.86.1
> User Datagram Protocol, Src Port: 55928, Dst Port: 53
> Domain Name System (query)
```

```
0000  b0 6a 41 c7 5f d8 a8 7e  ea 34 c2 09 08 00 45 00   ·jA·_··~ ·4····E·
0010  00 3e b1 d3 00 00 80 11  00 00 c0 a8 56 20 c0 a8   ·>······ ····V ··
0020  56 01 da 78 00 35 00 2a  2d ae 00 04 01 00 00 01   V··x·5·* -·······
0030  00 00 00 00 00 00 03 77  77 77 02 63 73 05 75 6d   ·······w ww·cs·um
0040  61 73 73 03 65 64 75 00  00 01 00 01               ass·edu· ····
```

字节 52-53: Additional RRs (dns.count.add_rr)
分组: 49 · 已显示: 49 (100.0%) · 已丢弃: 0 (0.0%)
配置: Default

The destination port for the DNS query message is 53



*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 ... <Ctrl-/>

```
No.   Time      Source             Destination      Protocol Length Info
   10 1.450098  192.168.86.32      142.250.188.227  UDP        77 63393 → 443 Len=35
   11 1.480111  192.168.86.32      142.250.188.227  UDP        74 63393 → 443 Len=32
   12 1.507103  142.250.188.227    192.168.86.32    UDP        66 443 → 63393 Len=24
   13 1.697249  172.240.254.132    192.168.86.32    TLSv1.2    78 Application Data
   14 1.697249  172.240.254.132    192.168.86.32    TCP        54 443 → 55233 [FIN, ACK] Seq=25 Ack=1 Win=160 Len=0
   15 1.697276  192.168.86.32      172.240.254.132  TCP        54 55233 → 443 [ACK] Seq=1 Ack=26 Win=513 Len=0
   16 2.252586  Google_c7:5f:d8    Broadcast        ARP        42 Who has 192.168.86.43? Tell 192.168.86.1
   17 3.071816  192.168.86.29      192.168.86.255   UDP        86 57621 → 57621 Len=44
   18 3.227688  192.168.86.32      192.168.86.1     DNS        85 Standard query 0x0001 PTR 1.86.168.192.in-addr.arpa
   19 3.245062  192.168.86.1       192.168.86.32    DNS        85 Standard query response 0x0001 No such name PTR 1.86.168.192.in-addr.arpa
   20 3.245706  192.168.86.32      192.168.86.1     DNS        80 Standard query 0x0002 A www.cs.umass.edu.lan
   21 3.265234  192.168.86.1       192.168.86.32    DNS        80 Standard query response 0x0002 No such name A www.cs.umass.edu.lan
   22 3.265379  192.168.86.32      192.168.86.1     DNS        80 Standard query 0x0003 AAAA www.cs.umass.edu.lan
   23 3.276276  06:4f:67:fb:5d:33  Broadcast        ARP        42 Who has 192.168.86.34? Tell 192.168.86.26
   24 3.276484  Google_c7:5f:d8    Broadcast        ARP        42 Who has 192.168.86.43? Tell 192.168.86.1
   25 3.282989  192.168.86.1       192.168.86.32    DNS        80 Standard query response 0x0003 No such name AAAA www.cs.umass.edu.lan
   26 3.283118  192.168.86.32      192.168.86.1     DNS        76 Standard query 0x0004 A www.cs.umass.edu
   27 3.320919  192.168.86.1       192.168.86.32    DNS        92 Standard query response 0x0004 A www.cs.umass.edu A 128.119.240.84
   28 3.322800  192.168.86.32      192.168.86.1     DNS        76 Standard query 0x0005 AAAA www.cs.umass.edu
   29 3.439530  192.168.86.1       192.168.86.32    DNS       129 Standard query response 0x0005 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu
   30 3.635127  192.168.86.32      172.217.14.69    TCP        55 55348 → 443 [ACK] Seq=1 Ack=1 Win=12354 Len=1 [TCP segment of a reassembled PDU]
   31 3.658712  172.217.14.69      192.168.86.32    TCP        66 443 → 55348 [ACK] Seq=1 Ack=2 Win=5017 Len=0 SLE=1 SRE=2
   32 4.300336  Google_c7:5f:d8    Broadcast        ARP        42 Who has 192.168.86.43? Tell 192.168.86.1
   33 4.344586  Google_c7:5f:d8    IntelCor_34:c2:09 ARP       60 Who has 192.168.86.32? Tell 192.168.86.1
```

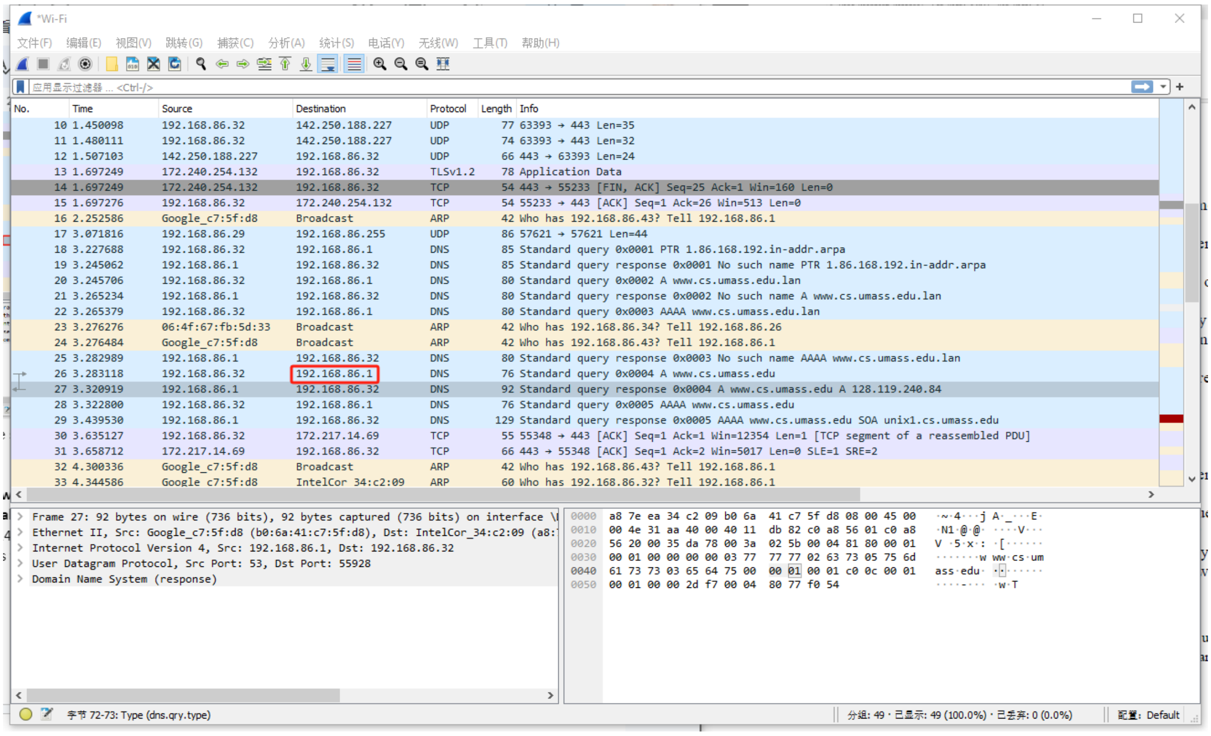
```
> Frame 27: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \
> Ethernet II, Src: Google_c7:5f:d8 (b0:6a:41:c7:5f:d8), Dst: IntelCor_34:c2:09 (a8:
> Internet Protocol Version 4, Src: 192.168.86.1, Dst: 192.168.86.32
> User Datagram Protocol, Src Port: 53, Dst Port: 55928
> Domain Name System (response)
```

```
0000  a8 7e ea 34 c2 09 b0 6a  41 c7 5f d8 08 00 45 00   ·~·4···j A·_···E·
0010  00 4e 31 aa 40 00 40 11  db 82 c0 a8 56 01 c0 a8   ·N1·@·@· ····V···
0020  56 20 00 35 da 78 00 3a  02 5b 00 04 81 80 00 01   V ·5·x·: ·[······
0030  00 01 00 00 00 00 03 77  77 77 02 63 73 05 75 6d   ·······w ww·cs·um
0040  61 73 73 03 65 64 75 00  00 01 00 01 c0 0c 00 01   ass·edu· ········
0050  00 01 00 00 2d f7 00 04  80 77 f0 54               ····-··· ·w·T
```

wireshark_Wi-FiGHMDC2.pcapng
分组: 49 · 已显示: 49 (100.0%) · 已丢弃: 0 (0.0%)
配置: Default

The source port of the DNS response message is 53

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


*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.   Time       Source              Destination         Protocol  Length Info
   10 1.450098   192.168.86.32       142.250.188.227     UDP          77 63393 → 443 Len=35
   11 1.480111   192.168.86.32       142.250.188.227     UDP          74 63393 → 443 Len=32
   12 1.507103   142.250.188.227     192.168.86.32       UDP          66 443 → 63393 Len=24
   13 1.697249   172.240.254.132     192.168.86.32       TLSv1.2      78 Application Data
   14 1.697249   172.240.254.132     192.168.86.32       TCP          54 443 → 55233 [FIN, ACK] Seq=25 Ack=1 Win=160 Len=0
   15 1.697276   192.168.86.32       172.240.254.132     TCP          54 55233 → 443 [ACK] Seq=1 Ack=26 Win=513 Len=0
   16 2.252586   Google_c7:5f:d8     Broadcast           ARP          42 Who has 192.168.86.43? Tell 192.168.86.1
   17 3.071816   192.168.86.29       192.168.86.255      UDP          86 57621 → 57621 Len=44
   18 3.227688   192.168.86.32       192.168.86.1        DNS          85 Standard query 0x0001 PTR 1.86.168.192.in-addr.arpa
   19 3.245062   192.168.86.1        192.168.86.32       DNS          85 Standard query response 0x0001 No such name PTR 1.86.168.192.in-addr.arpa
   20 3.245706   192.168.86.32       192.168.86.1        DNS          80 Standard query 0x0002 A www.cs.umass.edu.lan
   21 3.265234   192.168.86.1        192.168.86.32       DNS          80 Standard query response 0x0002 No such name A www.cs.umass.edu.lan
   22 3.265379   192.168.86.32       192.168.86.1        DNS          80 Standard query 0x0003 AAAA www.cs.umass.edu.lan
   23 3.276276   06:4f:67:fb:5d:33   Broadcast           ARP          42 Who has 192.168.86.34? Tell 192.168.86.26
   24 3.276484   Google_c7:5f:d8     Broadcast           ARP          42 Who has 192.168.86.43? Tell 192.168.86.1
   25 3.282989   192.168.86.1        192.168.86.32       DNS          80 Standard query response 0x0003 No such name AAAA www.cs.umass.edu.lan
   26 3.283118   192.168.86.32       192.168.86.1        DNS          76 Standard query 0x0004 A www.cs.umass.edu
   27 3.320919   192.168.86.1        192.168.86.32       DNS          92 Standard query response 0x0004 A www.cs.umass.edu A 128.119.240.84
   28 3.322800   192.168.86.32       192.168.86.1        DNS          76 Standard query 0x0005 AAAA www.cs.umass.edu
   29 3.439530   192.168.86.1        192.168.86.32       DNS         129 Standard query response 0x0005 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu
   30 3.635127   192.168.86.32       172.217.14.69       TCP          55 55348 → 443 [ACK] Seq=1 Ack=1 Win=12354 Len=1 [TCP segment of a reassembled PDU]
   31 3.658712   172.217.14.69       192.168.86.32       TCP          66 443 → 55348 [ACK] Seq=1 Ack=2 Win=5017 Len=0 SLE=1 SRE=2
   32 4.300336   Google_c7:5f:d8     Broadcast           ARP          42 Who has 192.168.86.43? Tell 192.168.86.1
   33 4.344586   Google_c7:5f:d8     IntelCor_34:c2:09   ARP          60 Who has 192.168.86.32? Tell 192.168.86.1
```

```
> Frame 27: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \[
> Ethernet II, Src: Google_c7:5f:d8 (b0:6a:41:c7:5f:d8), Dst: IntelCor_34:c2:09 (a8:]
> Internet Protocol Version 4, Src: 192.168.86.1, Dst: 192.168.86.32
> User Datagram Protocol, Src Port: 53, Dst Port: 55928
> Domain Name System (response)
```

```
0000  a8 7e ea 34 c2 09 b0 6a  41 c7 5f d8 08 00 45 00   ·~·4···j A·_···E·
0010  00 4e 31 aa 40 00 40 11  db 82 c0 a8 56 01 c0 a8   ·N1·@·@· ····V···
0020  56 20 00 35 da 78 00 3a  02 5b 00 04 81 80 00 01   V ·5·x·: ·[······
0030  00 01 00 00 00 00 03 77  77 77 02 63 73 05 75 6d   ·······w ww·cs·um
0040  61 73 73 03 65 64 75 00  00 01 00 01 c0 0c 00 01   ass·edu· ········
0050  00 01 00 00 2d f7 00 04  80 77 f0 54               ····-··· ·w·T
```

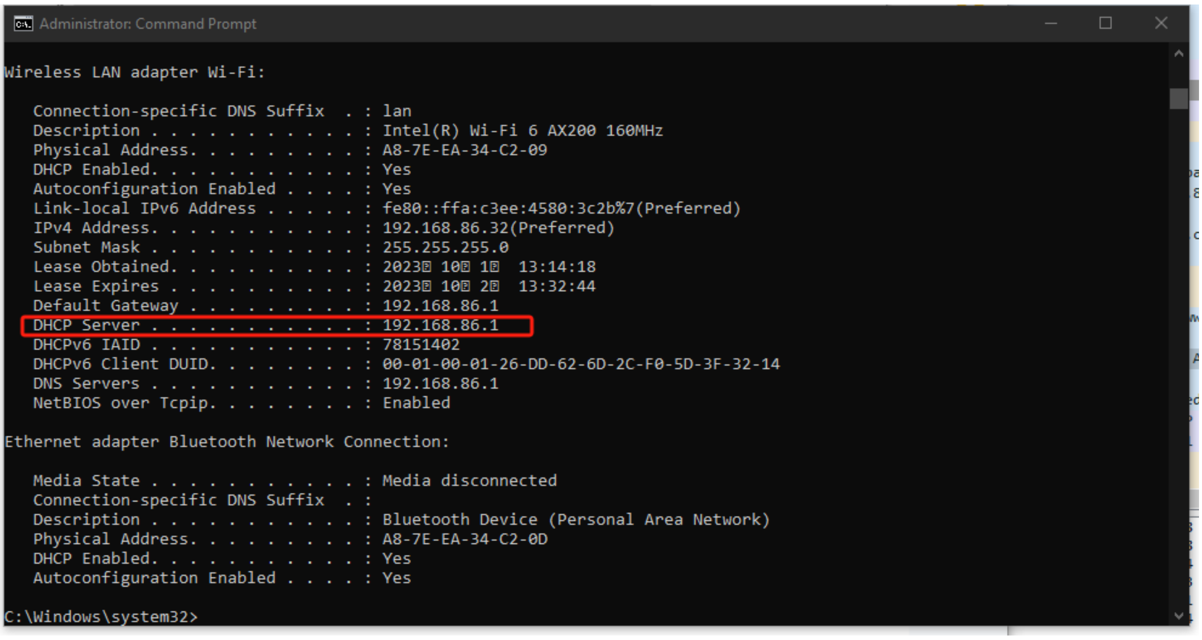
字节 72-73: Type (dns.qry.type)

分组: 49 · 已显示: 49 (100.0%) · 已丢弃: 0 (0.0%)

配置: Default

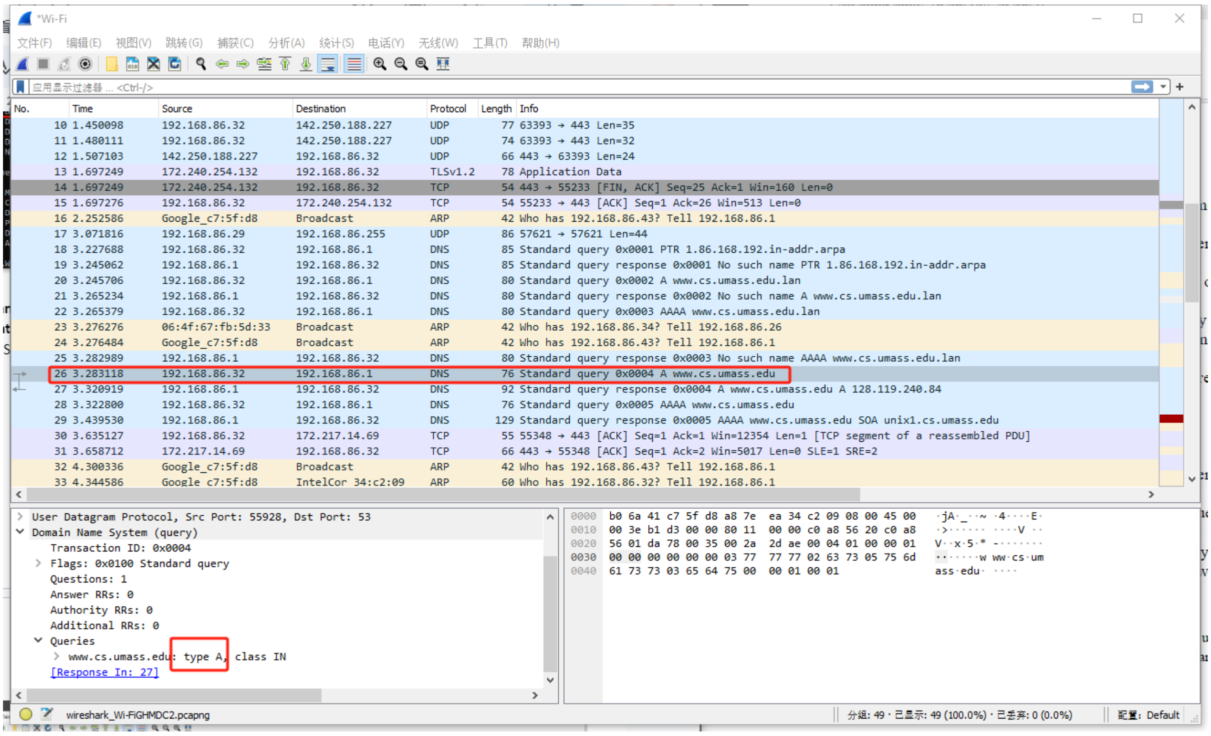
192.168.86.1

Yes, it is the same address as my default local DNS server.



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
   Physical Address. . . . . . . . . : A8-7E-EA-34-C2-09
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::ffa:c3ee:4580:3c2b%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.86.32(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 2023▯ 10▯ 1▯  13:14:18
   Lease Expires . . . . . . . . . . : 2023▯ 10▯ 2▯  13:32:44
   Default Gateway . . . . . . . . . : 192.168.86.1
   DHCP Server . . . . . . . . . . . : 192.168.86.1
   DHCPv6 IAID . . . . . . . . . . . : 78151402
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-DD-62-6D-2C-F0-5D-3F-32-14
   DNS Servers . . . . . . . . . . . : 192.168.86.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : A8-7E-EA-34-C2-0D
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Windows\system32>
```

14. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?


*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 ... <Ctrl-/>

```
No.    Time      Source             Destination        Protocol  Length  Info
    10 1.450098  192.168.86.32      142.250.188.227    UDP         77 63393 → 443 Len=35
    11 1.480111  192.168.86.32      142.250.188.227    UDP         74 63393 → 443 Len=32
    12 1.507103  142.250.188.227    192.168.86.32      UDP         66 443 → 63393 Len=24
    13 1.697249  172.240.254.132    192.168.86.32      TLSv1.2     78 Application Data
    14 1.697249  172.240.254.132    192.168.86.32      TCP         54 443 → 55233 [FIN, ACK] Seq=25 Ack=1 Win=160 Len=0
    15 1.697276  192.168.86.32      172.240.254.132    TCP         54 55233 → 443 [ACK] Seq=1 Ack=26 Win=513 Len=0
    16 2.252586  Google_c7:5f:d8    Broadcast          ARP         42 Who has 192.168.86.43? Tell 192.168.86.1
    17 3.071816  192.168.86.29      192.168.86.255     UDP         86 57621 → 57621 Len=44
    18 3.227688  192.168.86.32      192.168.86.1       DNS         85 Standard query 0x0001 PTR 1.86.168.192.in-addr.arpa
    19 3.245062  192.168.86.1       192.168.86.32      DNS         85 Standard query response 0x0001 No such name PTR 1.86.168.192.in-addr.arpa
    20 3.245706  192.168.86.32      192.168.86.1       DNS         80 Standard query 0x0002 A www.cs.umass.edu.lan
    21 3.265234  192.168.86.1       192.168.86.32      DNS         80 Standard query response 0x0002 No such name A www.cs.umass.edu.lan
    22 3.265379  192.168.86.32      192.168.86.1       DNS         80 Standard query 0x0003 AAAA www.cs.umass.edu.lan
    23 3.276276  06:4f:67:fb:5d:33  Broadcast          ARP         42 Who has 192.168.86.34? Tell 192.168.86.26
    24 3.276484  Google_c7:5f:d8    Broadcast          ARP         42 Who has 192.168.86.43? Tell 192.168.86.1
    25 3.282989  192.168.86.1       192.168.86.32      DNS         80 Standard query response 0x0003 No such name AAAA www.cs.umass.edu.lan
    26 3.283118  192.168.86.32      192.168.86.1       DNS         76 Standard query 0x0004 A www.cs.umass.edu
    27 3.320919  192.168.86.1       192.168.86.32      DNS         92 Standard query response 0x0004 A www.cs.umass.edu A 128.119.240.84
    28 3.322800  192.168.86.32      192.168.86.1       DNS         76 Standard query 0x0005 AAAA www.cs.umass.edu
    29 3.439530  192.168.86.1       192.168.86.32      DNS        129 Standard query response 0x0005 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu
    30 3.635127  192.168.86.32      172.217.14.69      TCP         55 55348 → 443 [ACK] Seq=1 Ack=1 Win=12354 Len=1 [TCP segment of a reassembled PDU]
    31 3.658712  172.217.14.69      192.168.86.32      TCP         66 443 → 55348 [ACK] Seq=1 Ack=2 Win=5017 Len=0 SLE=1 SRE=2
    32 4.300336  Google_c7:5f:d8    Broadcast          ARP         42 Who has 192.168.86.43? Tell 192.168.86.1
    33 4.344586  Google_c7:5f:d8    IntelCor_34:c2:09  ARP         60 Who has 192.168.86.32? Tell 192.168.86.1
```

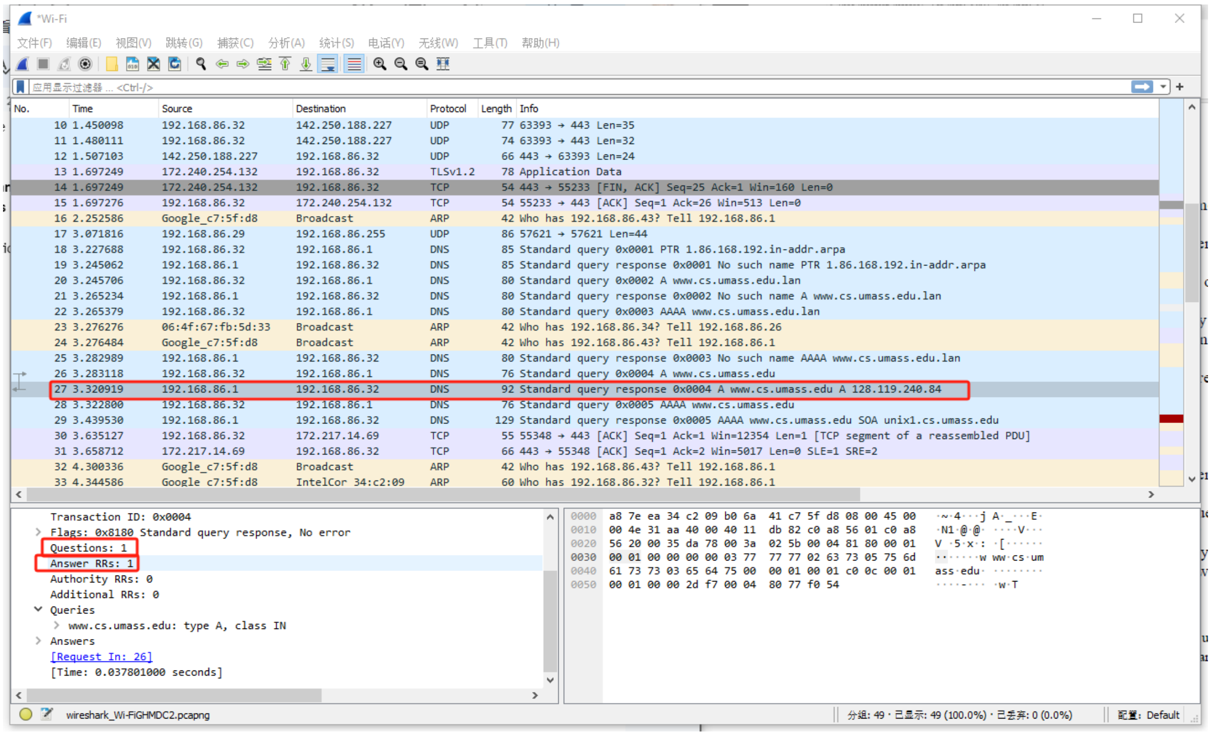
```
> User Datagram Protocol, Src Port: 55928, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.cs.umass.edu: type A, class IN
    [Response In: 27]
```

```
0000  b0 6a 41 c7 5f d8 a8 7e  ea 34 c2 09 08 00 45 00   ·jA·_··~ ·4····E·
0010  00 3e b1 d3 00 00 80 11  00 00 c0 a8 56 20 c0 a8   ·>······ ····V ··
0020  56 01 da 78 00 35 00 2a  2d ae 00 04 01 00 00 01   V··x·5·* -·······
0030  00 00 00 00 00 00 03 77  77 77 02 63 73 05 75 6d   ·······w ww·cs·um
0040  61 73 73 03 65 64 75 00  00 01 00 01               ass·edu· ····
```

wireshark_Wi-FiGHMDC2.pcapng
分组: 49 · 已显示: 49 (100.0%) · 已丢弃: 0 (0.0%)
配置: Default

The DNS query message type is A. It doesn't contain answer.

15. Examine the DNS response message to the query message. How many "questions" does this DNS response message contain? How many "answers"?


*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 ... <Ctrl-/>

```
No.    Time      Source             Destination        Protocol  Length  Info
    10 1.450098  192.168.86.32      142.250.188.227    UDP         77 63393 → 443 Len=35
    11 1.480111  192.168.86.32      142.250.188.227    UDP         74 63393 → 443 Len=32
    12 1.507103  142.250.188.227    192.168.86.32      UDP         66 443 → 63393 Len=24
    13 1.697249  172.240.254.132    192.168.86.32      TLSv1.2     78 Application Data
    14 1.697249  172.240.254.132    192.168.86.32      TCP         54 443 → 55233 [FIN, ACK] Seq=25 Ack=1 Win=160 Len=0
    15 1.697276  192.168.86.32      172.240.254.132    TCP         54 55233 → 443 [ACK] Seq=1 Ack=26 Win=513 Len=0
    16 2.252586  Google_c7:5f:d8    Broadcast          ARP         42 Who has 192.168.86.43? Tell 192.168.86.1
    17 3.071816  192.168.86.29      192.168.86.255     UDP         86 57621 → 57621 Len=44
    18 3.227688  192.168.86.32      192.168.86.1       DNS         85 Standard query 0x0001 PTR 1.86.168.192.in-addr.arpa
    19 3.245062  192.168.86.1       192.168.86.32      DNS         85 Standard query response 0x0001 No such name PTR 1.86.168.192.in-addr.arpa
    20 3.245706  192.168.86.32      192.168.86.1       DNS         80 Standard query 0x0002 A www.cs.umass.edu.lan
    21 3.265234  192.168.86.1       192.168.86.32      DNS         80 Standard query response 0x0002 No such name A www.cs.umass.edu.lan
    22 3.265379  192.168.86.32      192.168.86.1       DNS         80 Standard query 0x0003 AAAA www.cs.umass.edu.lan
    23 3.276276  06:4f:67:fb:5d:33  Broadcast          ARP         42 Who has 192.168.86.34? Tell 192.168.86.26
    24 3.276484  Google_c7:5f:d8    Broadcast          ARP         42 Who has 192.168.86.43? Tell 192.168.86.1
    25 3.282989  192.168.86.1       192.168.86.32      DNS         80 Standard query response 0x0003 No such name AAAA www.cs.umass.edu.lan
    26 3.283118  192.168.86.32      192.168.86.1       DNS         76 Standard query 0x0004 A www.cs.umass.edu
    27 3.320919  192.168.86.1       192.168.86.32      DNS         92 Standard query response 0x0004 A www.cs.umass.edu A 128.119.240.84
    28 3.322800  192.168.86.32      192.168.86.1       DNS         76 Standard query 0x0005 AAAA www.cs.umass.edu
    29 3.439530  192.168.86.1       192.168.86.32      DNS        129 Standard query response 0x0005 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu
    30 3.635127  192.168.86.32      172.217.14.69      TCP         55 55348 → 443 [ACK] Seq=1 Ack=1 Win=12354 Len=1 [TCP segment of a reassembled PDU]
    31 3.658712  172.217.14.69      192.168.86.32      TCP         66 443 → 55348 [ACK] Seq=1 Ack=2 Win=5017 Len=0 SLE=1 SRE=2
    32 4.300336  Google_c7:5f:d8    Broadcast          ARP         42 Who has 192.168.86.43? Tell 192.168.86.1
    33 4.344586  Google_c7:5f:d8    IntelCor_34:c2:09  ARP         60 Who has 192.168.86.32? Tell 192.168.86.1
```

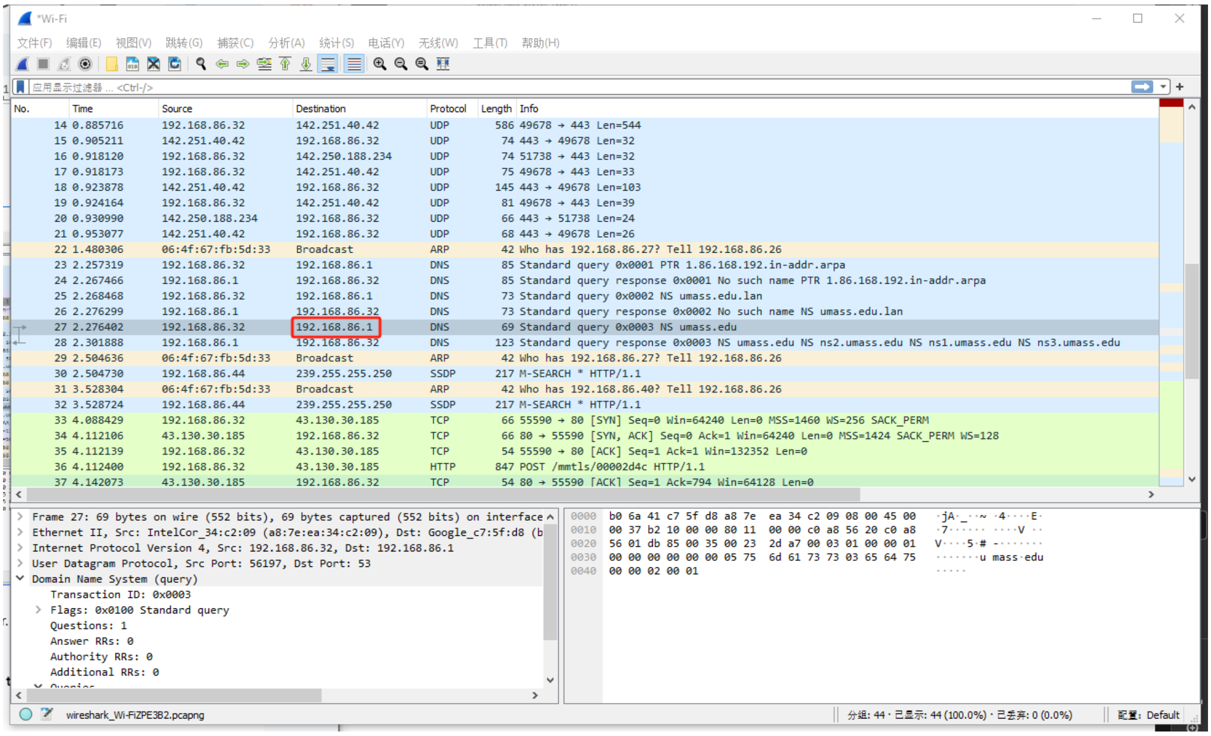
```
    Transaction ID: 0x0004
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.cs.umass.edu: type A, class IN
  > Answers
    [Request In: 26]
    [Time: 0.037801000 seconds]
```

```
0000  a8 7e ea 34 c2 09 b0 6a  41 c7 5f d8 08 00 45 00   ·~·4···j A·_···E·
0010  00 4e 31 aa 40 00 40 11  db 82 c0 a8 56 01 c0 a8   ·N1·@·@· ····V···
0020  56 20 00 35 da 78 00 3a  02 5b 00 04 81 80 00 01   V ·5·x·: ·[······
0030  00 01 00 00 00 00 03 77  77 77 02 63 73 05 75 6d   ·······w ww·cs·um
0040  61 73 73 03 65 64 75 00  00 01 00 01 c0 0c 00 01   ass·edu· ········
0050  00 01 00 00 2d f7 00 04  80 77 f0 54               ····-··· ·w·T
```

wireshark_Wi-FiGHMDC2.pcapng
分组: 49 · 已显示: 49 (100.0%) · 已丢弃: 0 (0.0%)
配置: Default

1 question and 1 answer

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


*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 ... <Ctrl-/>

```
No.    Time       Source               Destination        Protocol  Length  Info
    14 0.885716   192.168.86.32        142.251.40.42      UDP       586 49678 → 443 Len=544
    15 0.905211   142.251.40.42        192.168.86.32      UDP        74 443 → 49678 Len=32
    16 0.918120   192.168.86.32        142.250.188.234    UDP        74 51738 → 443 Len=32
    17 0.918173   192.168.86.32        142.251.40.42      UDP        75 49678 → 443 Len=33
    18 0.923878   142.251.40.42        192.168.86.32      UDP       145 443 → 49678 Len=103
    19 0.924164   192.168.86.32        142.251.40.42      UDP        81 49678 → 443 Len=39
    20 0.930990   142.250.188.234      192.168.86.32      UDP        66 443 → 51738 Len=24
    21 0.953077   142.251.40.42        192.168.86.32      UDP        68 443 → 49678 Len=26
    22 1.480306   06:4f:67:fb:5d:33    Broadcast          ARP        42 Who has 192.168.86.27? Tell 192.168.86.26
    23 2.257319   192.168.86.32        192.168.86.1       DNS        85 Standard query 0x0001 PTR 1.86.168.192.in-addr.arpa
    24 2.267466   192.168.86.1         192.168.86.32      DNS        85 Standard query response 0x0001 No such name PTR 1.86.168.192.in-addr.arpa
    25 2.268468   192.168.86.32        192.168.86.1       DNS        73 Standard query 0x0002 NS umass.edu.lan
    26 2.276299   192.168.86.1         192.168.86.32      DNS        73 Standard query response 0x0002 No such name NS umass.edu.lan
    27 2.276402   192.168.86.32        192.168.86.1       DNS        69 Standard query 0x0003 NS umass.edu
    28 2.301888   192.168.86.1         192.168.86.32      DNS       123 Standard query response 0x0003 NS umass.edu NS ns2.umass.edu NS ns1.umass.edu NS ns3.umass.edu
    29 2.504636   06:4f:67:fb:5d:33    Broadcast          ARP        42 Who has 192.168.86.27? Tell 192.168.86.26
    30 2.504730   192.168.86.44        239.255.255.250    SSDP      217 M-SEARCH * HTTP/1.1
    31 3.528304   06:4f:67:fb:5d:33    Broadcast          ARP        42 Who has 192.168.86.40? Tell 192.168.86.26
    32 3.528724   192.168.86.44        239.255.255.250    SSDP      217 M-SEARCH * HTTP/1.1
    33 4.088429   192.168.86.32        43.130.30.185      TCP        66 55590 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    34 4.112106   43.130.30.185        192.168.86.32      TCP        66 80 → 55590 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1424 SACK_PERM WS=128
    35 4.112139   192.168.86.32        43.130.30.185      TCP        54 55590 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
    36 4.112400   192.168.86.32        43.130.30.185      HTTP      847 POST /mmtls/00002d4c HTTP/1.1
    37 4.142073   43.130.30.185        192.168.86.32      TCP        54 80 → 55590 [ACK] Seq=1 Ack=794 Win=64128 Len=0
```

```
> Frame 27: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface
> Ethernet II, Src: IntelCor_34:c2:09 (a8:7e:ea:34:c2:09), Dst: Google_c7:5f:d8 (b
> Internet Protocol Version 4, Src: 192.168.86.32, Dst: 192.168.86.1
> User Datagram Protocol, Src Port: 56197, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
```

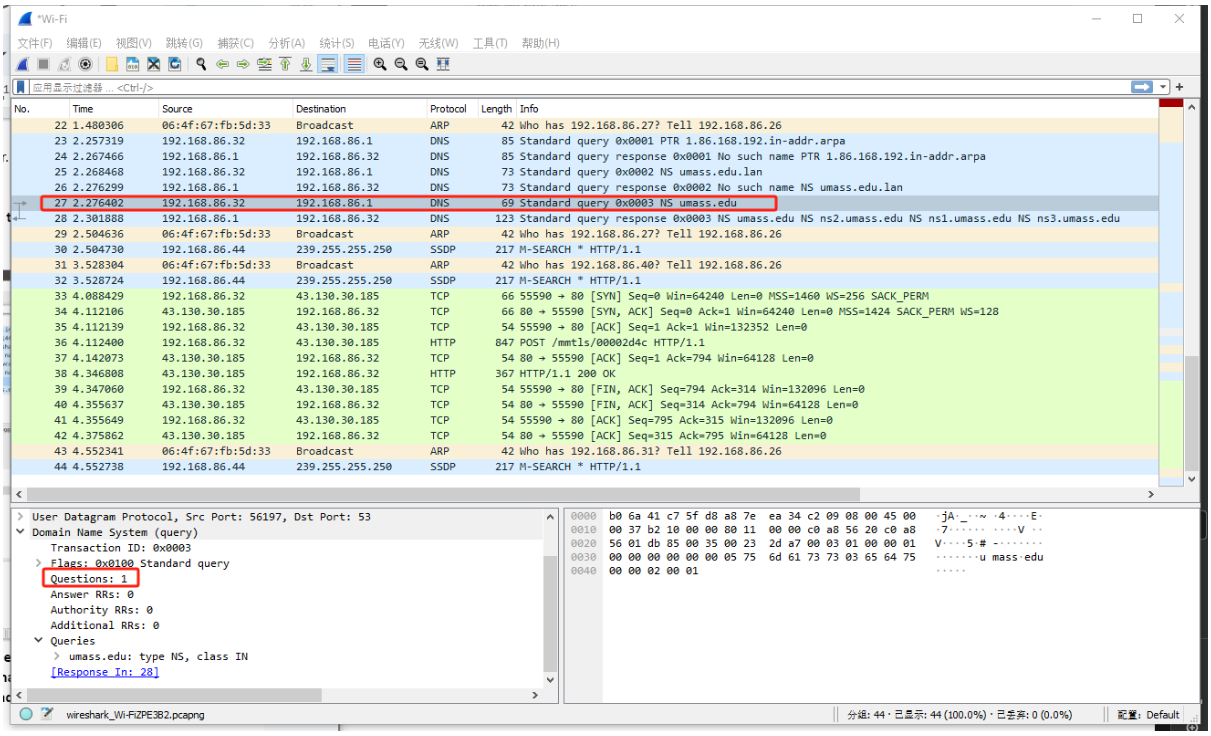
```
0000  b0 6a 41 c7 5f d8 a8 7e  ea 34 c2 09 08 00 45 00   ·jA·_··~ ·4····E·
0010  00 37 b2 10 00 00 80 11  00 00 c0 a8 56 20 c0 a8   ·7······ ····V ··
0020  56 01 db 85 00 35 00 23  2d a7 00 03 01 00 00 01   V····5·# -·······
0030  00 00 00 00 00 00 05 75  6d 61 73 73 03 65 64 75   ·······u mass·edu
0040  00 00 02 00 01                                     ·····
```

wireshark_Wi-FiZPE3B2.pcapng   分组: 44 · 已显示: 44 (100.0%) · 已丢弃: 0 (0.0%)   配置: Default

192.168.86.1

It is the same IP address as that of my default local DNS server.

17. Examine the DNS query message. How many questions does the query have? Does the query message contain any "answers"?


*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 ... <Ctrl-/>

```
No.    Time       Source               Destination        Protocol  Length  Info
    22 1.480306   06:4f:67:fb:5d:33    Broadcast          ARP        42 Who has 192.168.86.27? Tell 192.168.86.26
    23 2.257319   192.168.86.32        192.168.86.1       DNS        85 Standard query 0x0001 PTR 1.86.168.192.in-addr.arpa
    24 2.267466   192.168.86.1         192.168.86.32      DNS        85 Standard query response 0x0001 No such name PTR 1.86.168.192.in-addr.arpa
    25 2.268468   192.168.86.32        192.168.86.1       DNS        73 Standard query 0x0002 NS umass.edu.lan
    26 2.276299   192.168.86.1         192.168.86.32      DNS        73 Standard query response 0x0002 No such name NS umass.edu.lan
    27 2.276402   192.168.86.32        192.168.86.1       DNS        69 Standard query 0x0003 NS umass.edu
    28 2.301888   192.168.86.1         192.168.86.32      DNS       123 Standard query response 0x0003 NS umass.edu NS ns2.umass.edu NS ns1.umass.edu NS ns3.umass.edu
    29 2.504636   06:4f:67:fb:5d:33    Broadcast          ARP        42 Who has 192.168.86.27? Tell 192.168.86.26
    30 2.504730   192.168.86.44        239.255.255.250    SSDP      217 M-SEARCH * HTTP/1.1
    31 3.528304   06:4f:67:fb:5d:33    Broadcast          ARP        42 Who has 192.168.86.40? Tell 192.168.86.26
    32 3.528724   192.168.86.44        239.255.255.250    SSDP      217 M-SEARCH * HTTP/1.1
    33 4.088429   192.168.86.32        43.130.30.185      TCP        66 55590 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
    34 4.112106   43.130.30.185        192.168.86.32      TCP        66 80 → 55590 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1424 SACK_PERM WS=128
    35 4.112139   192.168.86.32        43.130.30.185      TCP        54 55590 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
    36 4.112400   192.168.86.32        43.130.30.185      HTTP      847 POST /mmtls/00002d4c HTTP/1.1
    37 4.142073   43.130.30.185        192.168.86.32      TCP        54 80 → 55590 [ACK] Seq=1 Ack=794 Win=64128 Len=0
    38 4.346808   43.130.30.185        192.168.86.32      HTTP      367 HTTP/1.1 200 OK
    39 4.347060   192.168.86.32        43.130.30.185      TCP        54 55590 → 80 [FIN, ACK] Seq=794 Ack=314 Win=132096 Len=0
    40 4.355637   43.130.30.185        192.168.86.32      TCP        54 80 → 55590 [FIN, ACK] Seq=314 Ack=794 Win=64128 Len=0
    41 4.355649   192.168.86.32        43.130.30.185      TCP        54 55590 → 80 [ACK] Seq=795 Ack=315 Win=132096 Len=0
    42 4.375862   43.130.30.185        192.168.86.32      TCP        54 80 → 55590 [ACK] Seq=315 Ack=795 Win=64128 Len=0
    43 4.552341   06:4f:67:fb:5d:33    Broadcast          ARP        42 Who has 192.168.86.31? Tell 192.168.86.26
    44 4.552738   192.168.86.44        239.255.255.250    SSDP      217 M-SEARCH * HTTP/1.1
```

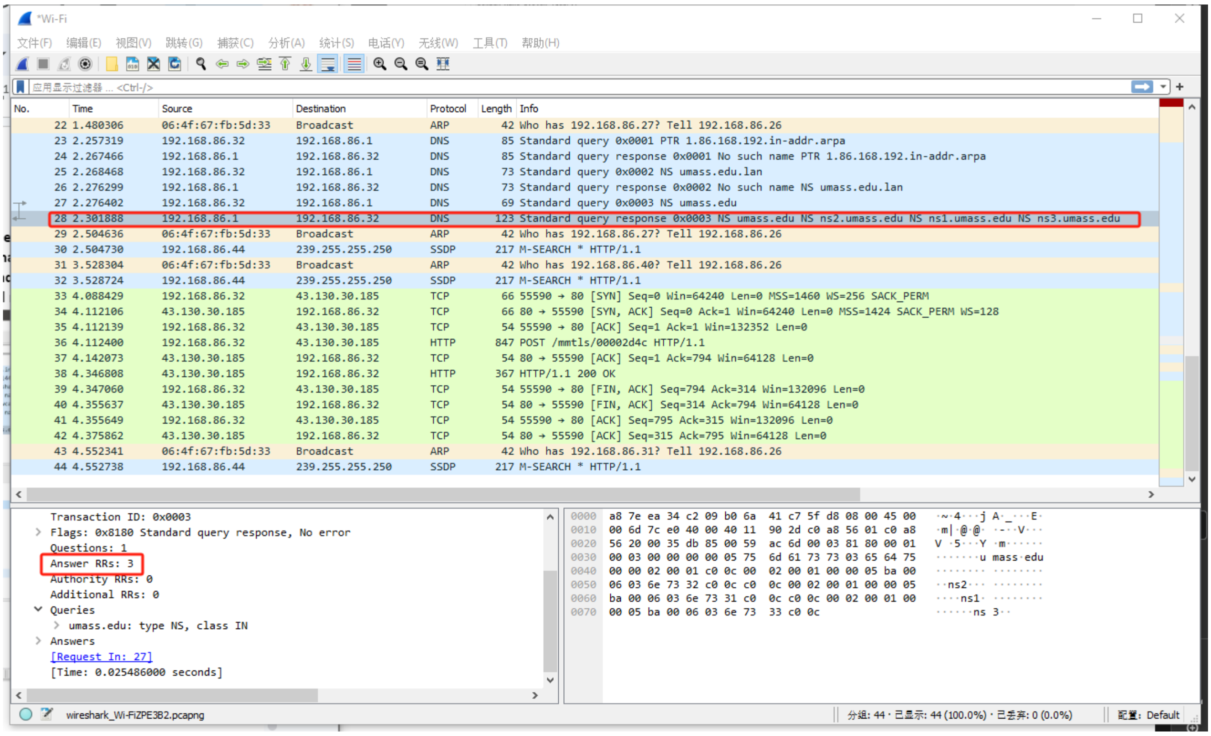
```
> User Datagram Protocol, Src Port: 56197, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > umass.edu: type NS, class IN
    [Response In: 28]
```

```
0000  b0 6a 41 c7 5f d8 a8 7e  ea 34 c2 09 08 00 45 00   ·jA·_··~ ·4····E·
0010  00 37 b2 10 00 00 80 11  00 00 c0 a8 56 20 c0 a8   ·7······ ····V ··
0020  56 01 db 85 00 35 00 23  2d a7 00 03 01 00 00 01   V····5·# -·······
0030  00 00 00 00 00 00 05 75  6d 61 73 73 03 65 64 75   ·······u mass·edu
0040  00 00 02 00 01                                     ·····
```

wireshark_Wi-FiZPE3B2.pcapng   分组: 44 · 已显示: 44 (100.0%) · 已丢弃: 0 (0.0%)   配置: Default

1 question and 0 answer

18. **Examine the DNS response message. How many answers does the response have? What information is contained in the answers? How many additional resource records are returned? What additional information is included in these additional resource records?**


*Wi-Fi
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 ... <Ctrl-/>

```
No.     Time        Source              Destination        Protocol  Length  Info
     22 1.480306    06:4f:67:fb:5d:33   Broadcast          ARP         42 Who has 192.168.86.27? Tell 192.168.86.26
     23 2.257319    192.168.86.32       192.168.86.1       DNS         85 Standard query 0x0001 PTR 1.86.168.192.in-addr.arpa
     24 2.267466    192.168.86.1        192.168.86.32      DNS         85 Standard query response 0x0001 No such name PTR 1.86.168.192.in-addr.arpa
     25 2.268468    192.168.86.32       192.168.86.1       DNS         73 Standard query 0x0002 NS umass.edu.lan
     26 2.276299    192.168.86.1        192.168.86.32      DNS         73 Standard query response 0x0002 No such name NS umass.edu.lan
     27 2.276402    192.168.86.32       192.168.86.1       DNS         69 Standard query 0x0003 NS umass.edu
     28 2.301888    192.168.86.1        192.168.86.32      DNS        123 Standard query response 0x0003 NS umass.edu NS ns2.umass.edu NS ns1.umass.edu NS ns3.umass.edu
     29 2.504636    06:4f:67:fb:5d:33   Broadcast          ARP         42 Who has 192.168.86.27? Tell 192.168.86.26
     30 2.504730    192.168.86.44       239.255.255.250    SSDP       217 M-SEARCH * HTTP/1.1
     31 3.528304    06:4f:67:fb:5d:33   Broadcast          ARP         42 Who has 192.168.86.40? Tell 192.168.86.26
     32 3.528724    192.168.86.44       239.255.255.250    SSDP       217 M-SEARCH * HTTP/1.1
     33 4.088429    192.168.86.32       43.130.30.185      TCP         66 55590 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
     34 4.112106    43.130.30.185       192.168.86.32      TCP         66 80 → 55590 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1424 SACK_PERM WS=128
     35 4.112139    192.168.86.32       43.130.30.185      TCP         54 55590 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
     36 4.112400    192.168.86.32       43.130.30.185      HTTP       847 POST /mmtls/00002d4c HTTP/1.1
     37 4.142073    43.130.30.185       192.168.86.32      TCP         54 80 → 55590 [ACK] Seq=1 Ack=794 Win=64128 Len=0
     38 4.346808    43.130.30.185       192.168.86.32      HTTP       367 HTTP/1.1 200 OK
     39 4.347060    192.168.86.32       43.130.30.185      TCP         54 55590 → 80 [FIN, ACK] Seq=794 Ack=314 Win=132096 Len=0
     40 4.355637    43.130.30.185       192.168.86.32      TCP         54 80 → 55590 [FIN, ACK] Seq=314 Ack=794 Win=64128 Len=0
     41 4.355649    192.168.86.32       43.130.30.185      TCP         54 55590 → 80 [ACK] Seq=795 Ack=315 Win=132096 Len=0
     42 4.375862    43.130.30.185       192.168.86.32      TCP         54 80 → 55590 [ACK] Seq=315 Ack=795 Win=64128 Len=0
     43 4.552341    06:4f:67:fb:5d:33   Broadcast          ARP         42 Who has 192.168.86.31? Tell 192.168.86.26
     44 4.552738    192.168.86.44       239.255.255.250    SSDP       217 M-SEARCH * HTTP/1.1
```

```
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
      > umass.edu: type NS, class IN
  > Answers
    [Request In: 27]
    [Time: 0.025486000 seconds]
```

```
0000  a8 7e ea 34 c2 09 b0 6a  41 c7 5f d8 08 00 45 00   ·~·4···j A·_···E·
0010  00 6d 7c e0 40 00 40 11  90 2d c0 a8 56 01 c0 a8   ·m|·@·@· ·-··V···
0020  56 20 00 35 db 85 00 59  ac 6d 00 03 81 80 00 01   V ·5···Y ·m······
0030  00 03 00 00 00 00 05 75  6d 61 73 73 03 65 64 75   ·······u mass·edu
0040  00 00 02 00 01 c0 0c 00  02 00 01 00 00 05 ba 00   ········ ········
0050  06 03 6e 73 32 c0 0c c0  0c 00 02 00 01 00 00 05   ··ns2··· ········
0060  ba 00 06 03 6e 73 31 c0  0c c0 0c 00 02 00 01 00   ····ns1· ········
0070  00 05 ba 00 06 03 6e 73  33 c0 0c                  ······ns 3··
```

wireshark_Wi-FiZPE3B2.pcapng | 分组: 44 · 已显示: 44 (100.0%) · 已丢弃: 0 (0.0%) | 配置: Default

1. 3 answers
2. It contains the type, class, time to live and nameserver.
3. There are 0 additional resource records returned in my case. However, there are 3 additional resource records in the author's trace.
4. The additional resource is Ip address of authoritative DNS servers.