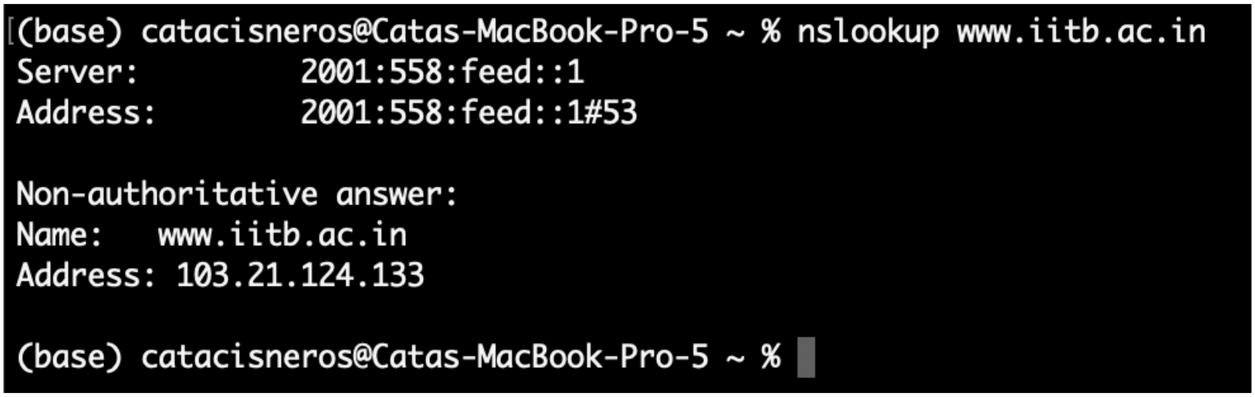
Catalina Cisneros

Lab: Wireshark DNS v9.0

1. nslookup

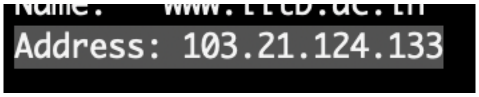


```
[(base) catacisneros@Catas-MacBook-Pro-5 ~ % nslookup www.iitb.ac.in
Server:         2001:558:feed::1
Address:        2001:558:feed::1#53

Non-authoritative answer:
Name:   www.iitb.ac.in
Address: 103.21.124.133

(base) catacisneros@Catas-MacBook-Pro-5 ~ %
```

Questions

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

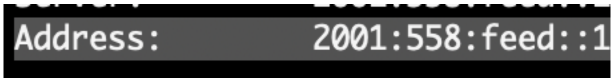
→ The IP Address is 103.21.124.133



```
Name:   www.iitb.ac.in
Address: 103.21.124.133
```

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

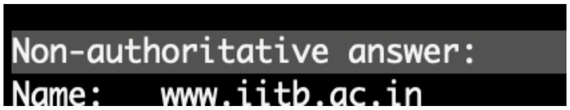
→ The IP Address from the DNS server is 2001:558:feed::1



```
Address:        2001:558:feed::1
```

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

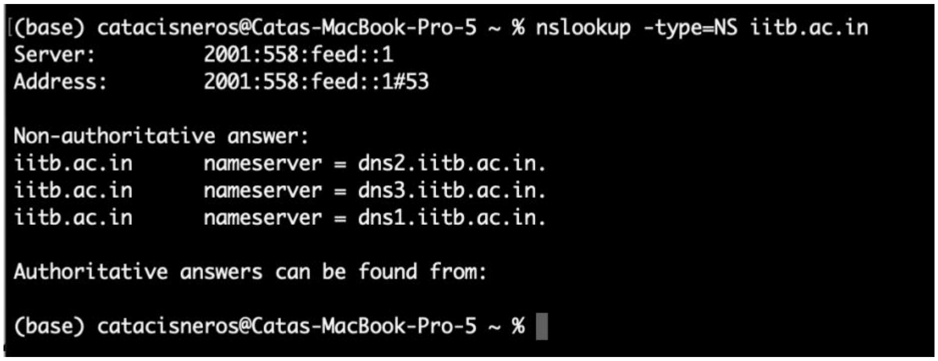
→ Non authoritative server



```
Non-authoritative answer:
Name:   www.iitb.ac.in
```

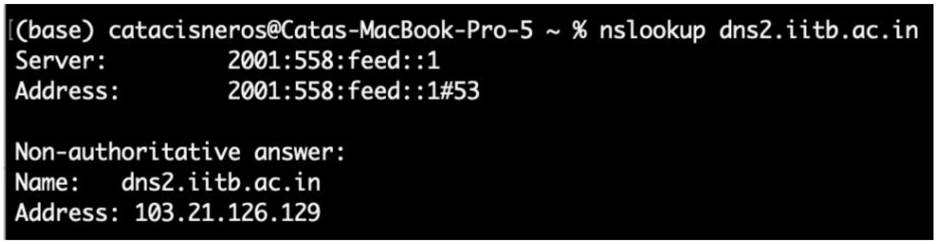
4. Use the nslookup command to determine the name of the authoritative name server for the iit.ac.in domain. What is that name? (If there are more than one authoritative servers, what is the name of the first authoritative server returned by nslookup)? If you had to find the IP address of that authoritative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

→ Authoritative name servers: dns2.iitb.ac.in, dns3.iitb.ac.in, dns1.iitb.ac.in
→ First one listed: dns2.iitb.ac.in



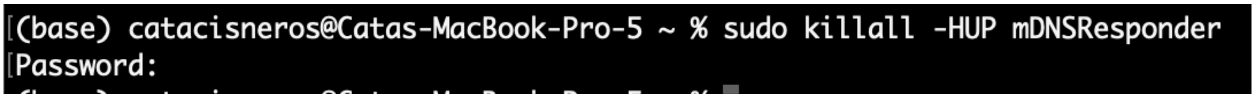
```
[(base) catacisneros@Catas-MacBook-Pro-5 ~ % nslookup -type=NS iitb.ac.in
Server:         2001:558:feed::1
Address:        2001:558:feed::1#53

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

Authoritative answers can be found from:

(base) catacisneros@Catas-MacBook-Pro-5 ~ %
```

→ To find its IP: nslookup dns2.iitb.ac.in



```
[(base) catacisneros@Catas-MacBook-Pro-5 ~ % nslookup dns2.iitb.ac.in
Server:         2001:558:feed::1
Address:        2001:558:feed::1#53

Non-authoritative answer:
Name:   dns2.iitb.ac.in
Address: 103.21.126.129
```

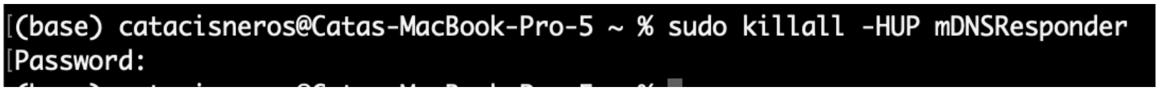
2. The DNS Cache on your computer



```
[(base) catacisneros@Catas-MacBook-Pro-5 ~ % sudo killall -HUP mDNSResponder
[Password:
```

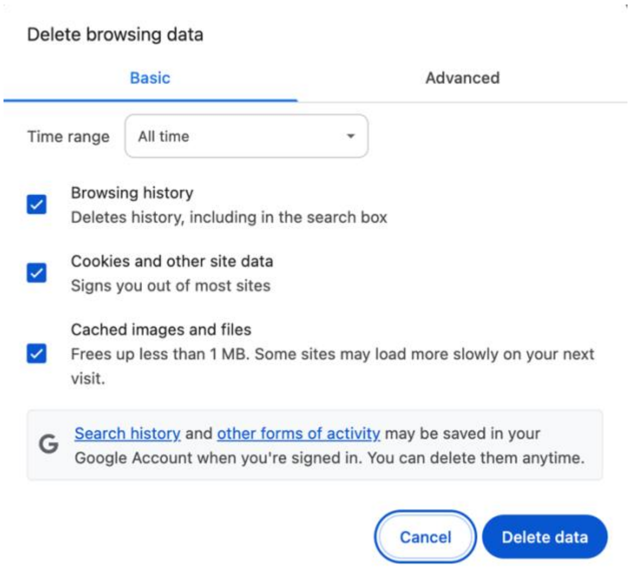
3. Tracing DNS with wireshark

- Clear the DNS cache in the host



```
[(base) catacisneros@Catas-MacBook-Pro-5 ~ % sudo killall -HUP mDNSResponder
[Password:
```

- Open browser and clear cache



Delete browsing data

Basic | Advanced

Time range: All time

☑ Browsing history
Deletes history, including in the search box

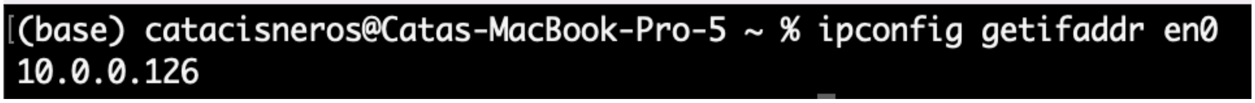
☑ Cookies and other site data
Signs you out of most sites

☑ Cached images and files
Frees up less than 1 MB. Some sites may load more slowly on your next visit.

Search history and other forms of activity may be saved in your Google Account when you're signed in. You can delete them anytime.

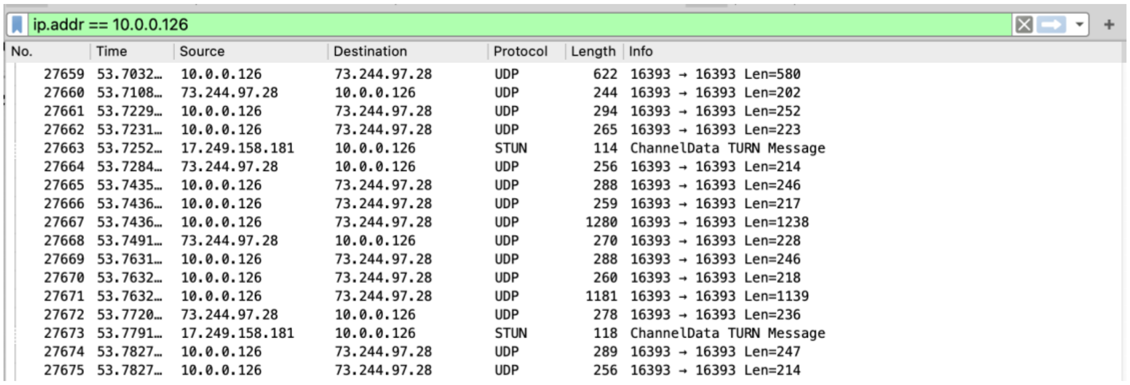
- Open wireshark and enter my IP address

→ My IP Address: 10.0.0.126



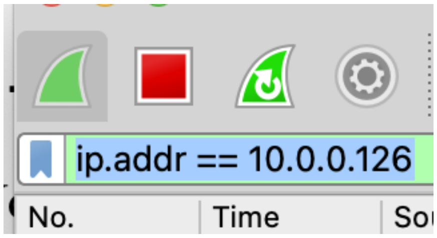
```
[(base) catacisneros@Catas-MacBook-Pro-5 ~ % ipconfig getifaddr en0
10.0.0.126
```

→ Enter it in Wireshark



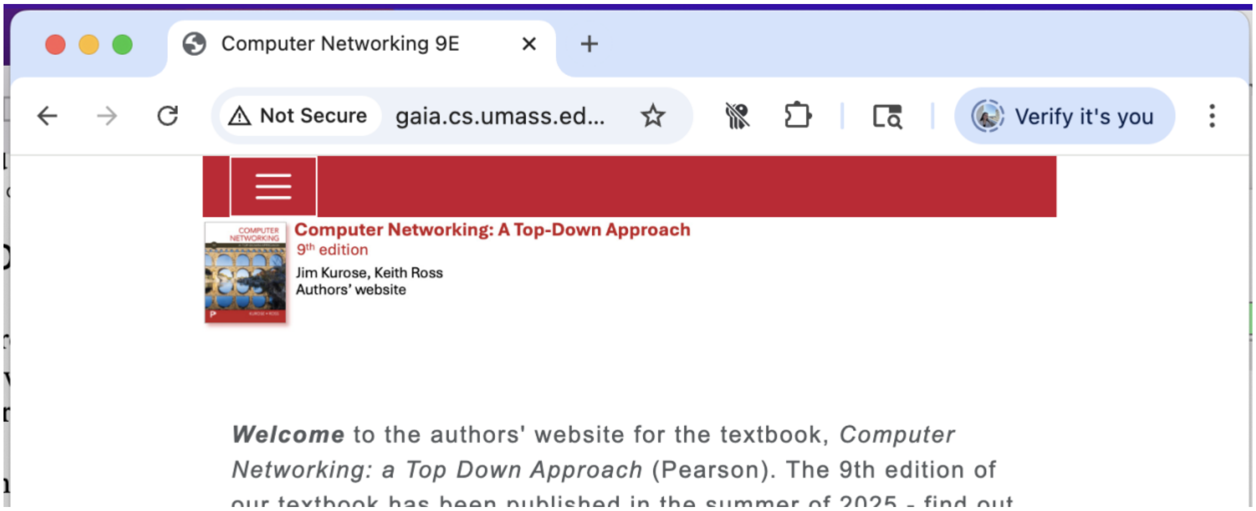
```
ip.addr == 10.0.0.126
No.    Time       Source          Destination    Protocol  Length Info
 27659 53.7032…   10.0.0.126      73.244.97.28   UDP        622  16393 → 16393 Len=580
 27660 53.7108…   73.244.97.28    10.0.0.126     UDP        244  16393 → 16393 Len=202
 27661 53.7229…   10.0.0.126      73.244.97.28   UDP        294  16393 → 16393 Len=252
 27662 53.7231…   10.0.0.126      73.244.97.28   UDP        265  16393 → 16393 Len=223
 27663 53.7252…   17.249.158.181  10.0.0.126     STUN       114  ChannelData TURN Message
 27664 53.7284…   73.244.97.28    10.0.0.126     UDP        256  16393 → 16393 Len=214
 27665 53.7435…   10.0.0.126      73.244.97.28   UDP        288  16393 → 16393 Len=246
 27666 53.7436…   10.0.0.126      73.244.97.28   UDP        259  16393 → 16393 Len=217
 27667 53.7436…   10.0.0.126      73.244.97.28   UDP       1280  16393 → 16393 Len=1238
 27668 53.7491…   73.244.97.28    10.0.0.126     UDP        270  16393 → 16393 Len=228
 27669 53.7631…   10.0.0.126      73.244.97.28   UDP        288  16393 → 16393 Len=246
 27670 53.7632…   10.0.0.126      73.244.97.28   UDP        260  16393 → 16393 Len=218
 27671 53.7632…   10.0.0.126      73.244.97.28   UDP       1181  16393 → 16393 Len=1139
 27672 53.7720…   73.244.97.28    10.0.0.126     UDP        278  16393 → 16393 Len=236
 27673 53.7791…   17.249.158.181  10.0.0.126     STUN       118  ChannelData TURN Message
 27674 53.7827…   10.0.0.126      73.244.97.28   UDP        289  16393 → 16393 Len=247
 27675 53.7827…   10.0.0.126      73.244.97.28   UDP        256  16393 → 16393 Len=214
```

- Start packet capture



ip.addr == 10.0.0.126

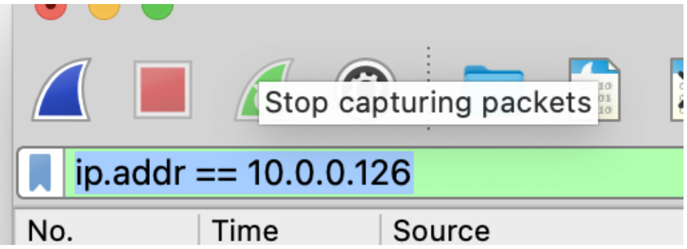
- Visit http://gaia.cs.umass.edu/kurose_ross/



Computer Networking: A Top-Down Approach
9th edition
Jim Kurose, Keith Ross
Authors' website

Welcome to the authors' website for the textbook, *Computer Networking: a Top Down Approach* (Pearson). The 9th edition of our textbook has been published in the summer of 2025 - find out

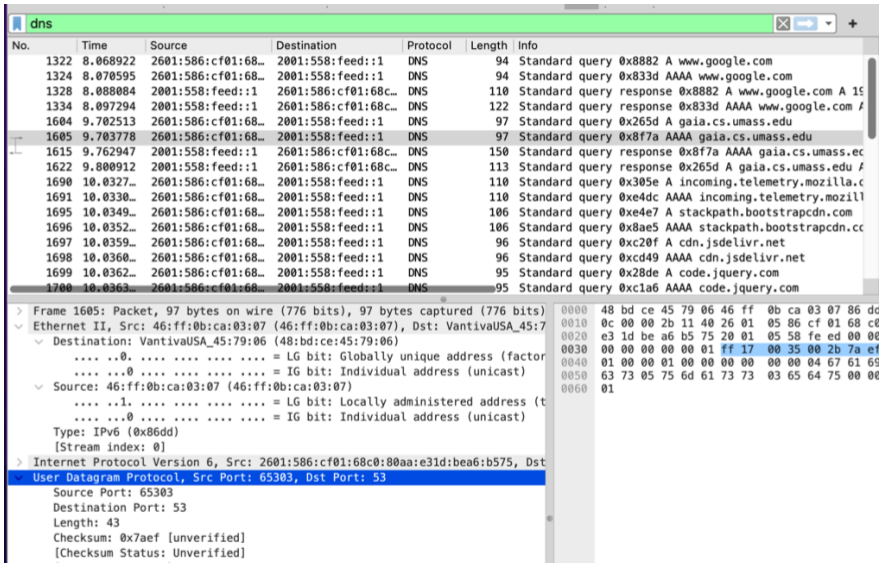
- Stop packet capture



Questions

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?

→ The first DNS query that resolved gaia.cs.umass.edu was packet 1605, using the UDP protocol.



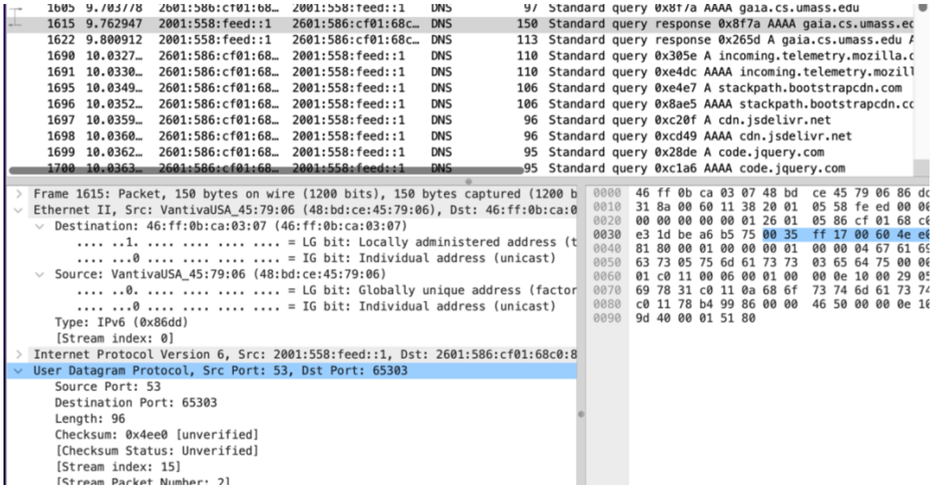
```
No.     Time      Source              Destination         Protocol  Length  Info
   1322 8.068922  2601:586:cf01:68…   2001:558:feed::1    DNS         94  Standard query 0x8882 A www.google.com
   1324 8.070595  2601:586:cf01:68…   2001:558:feed::1    DNS         94  Standard query 0x833d AAAA www.google.com
   1328 8.088084  2001:558:feed::1    2601:586:cf01:68c…  DNS        110  Standard query response 0x8882 A www.google.com A 1
   1334 8.097294  2001:558:feed::1    2601:586:cf01:68c…  DNS        122  Standard query response 0x833d AAAA www.google.com
   1604 9.702513  2601:586:cf01:68…   2001:558:feed::1    DNS         97  Standard query 0x265d A gaia.cs.umass.edu
   1605 9.703778  2601:586:cf01:68…   2001:558:feed::1    DNS         97  Standard query 0x8f7a AAAA gaia.cs.umass.edu
   1615 9.762947  2001:558:feed::1    2601:586:cf01:68c…  DNS        150  Standard query response 0x8f7a AAAA gaia.cs.umass.ec
   1622 9.800912  2001:558:feed::1    2601:586:cf01:68c…  DNS        113  Standard query response 0x265d A gaia.cs.umass.edu
   1690 10.0327…  2601:586:cf01:68…   2001:558:feed::1    DNS        110  Standard query 0x305e A incoming.telemetry.mozilla.c
   1691 10.0330…  2601:586:cf01:68…   2001:558:feed::1    DNS        110  Standard query 0xe4dc AAAA incoming.telemetry.mozill
   1695 10.0349…  2601:586:cf01:68…   2001:558:feed::1    DNS        106  Standard query 0xe4e7 A stackpath.bootstrapcdn.com
   1696 10.0352…  2601:586:cf01:68…   2001:558:feed::1    DNS        106  Standard query 0x8ae5 AAAA stackpath.bootstrapcdn.cc
   1697 10.0359…  2601:586:cf01:68…   2001:558:feed::1    DNS         96  Standard query 0xc20f A cdn.jsdelivr.net
   1698 10.0360…  2601:586:cf01:68…   2001:558:feed::1    DNS         96  Standard query 0xcd49 AAAA cdn.jsdelivr.net
   1699 10.0362…  2601:586:cf01:68…   2001:558:feed::1    DNS         95  Standard query 0x28de A code.jquery.com
   1700 10.0363…  2601:586:cf01:68…   2001:558:feed::1    DNS         95  Standard query 0xc1a6 AAAA code.jquery.com
```

```
> Frame 1605: Packet, 97 bytes on wire (776 bits), 97 bytes captured (776 bits)
v Ethernet II, Src: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07), Dst: VantivaUSA_45:7
  v Destination: VantivaUSA_45:79:06 (48:bd:ce:45:79:06)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factor
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07)
       .... ..1. .... .... .... .... = LG bit: Locally administered address (t
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
    [Stream index: 0]
> Internet Protocol Version 6, Src: 2601:586:cf01:68c0:80aa:e31d:bea6:b575, Dst
v User Datagram Protocol, Src Port: 65303, Dst Port: 53
    Source Port: 65303
    Destination Port: 53
    Length: 43
    Checksum: 0x7aef [unverified]
    [Checksum Status: Unverified]
```

```
0000  48 bd ce 45 79 06 46 ff  0b ca 03 07 86 dd
0010  0c 00 00 2b 11 40 26 01  05 86 cf 01 68 c0
0020  e3 1d be a6 b5 75 20 01  05 58 fe ed 00 00
0030  00 00 00 00 00 01 ff 17  00 35 00 2b 7a ef
0040  01 00 00 01 00 00 00 00  00 00 04 67 61 69
0050  63 73 05 75 6d 61 73 73  03 65 64 75 00 00
0060  01
```

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?

→ The matching DNS response appeared in packet 1615, using UDP



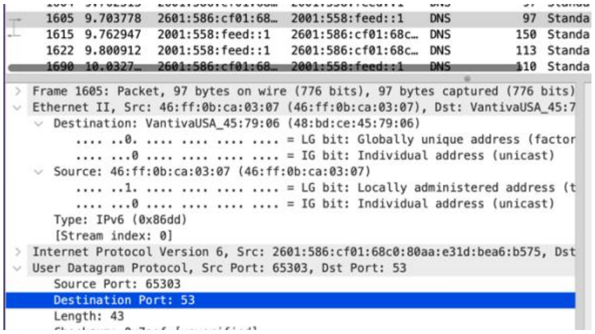
```
   1605 9.703778  2601:586:cf01:68…   2001:558:feed::1    DNS         97  Standard query 0x8f7a AAAA gaia.cs.umass.edu
   1615 9.762947  2001:558:feed::1    2601:586:cf01:68c…  DNS        150  Standard query response 0x8f7a AAAA gaia.cs.umass.ec
   1622 9.800912  2001:558:feed::1    2601:586:cf01:68c…  DNS        113  Standard query response 0x265d A gaia.cs.umass.edu
   1690 10.0327…  2601:586:cf01:68…   2001:558:feed::1    DNS        110  Standard query 0x305e A incoming.telemetry.mozilla.c
   1691 10.0330…  2601:586:cf01:68…   2001:558:feed::1    DNS        110  Standard query 0xe4dc AAAA incoming.telemetry.mozill
   1695 10.0349…  2601:586:cf01:68…   2001:558:feed::1    DNS        106  Standard query 0xe4e7 A stackpath.bootstrapcdn.com
   1696 10.0352…  2601:586:cf01:68…   2001:558:feed::1    DNS        106  Standard query 0x8ae5 AAAA stackpath.bootstrapcdn.cc
   1697 10.0359…  2601:586:cf01:68…   2001:558:feed::1    DNS         96  Standard query 0xc20f A cdn.jsdelivr.net
   1698 10.0360…  2601:586:cf01:68…   2001:558:feed::1    DNS         96  Standard query 0xcd49 AAAA cdn.jsdelivr.net
   1699 10.0362…  2601:586:cf01:68…   2001:558:feed::1    DNS         95  Standard query 0x28de A code.jquery.com
   1700 10.0363…  2601:586:cf01:68…   2001:558:feed::1    DNS         95  Standard query 0xc1a6 AAAA code.jquery.com
```

```
> Frame 1615: Packet, 150 bytes on wire (1200 bits), 150 bytes captured (1200 b
v Ethernet II, Src: VantivaUSA_45:79:06 (48:bd:ce:45:79:06), Dst: 46:ff:0b:ca:0
  v Destination: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07)
       .... ..1. .... .... .... .... = LG bit: Locally administered address (t
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: VantivaUSA_45:79:06 (48:bd:ce:45:79:06)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factor
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
    [Stream index: 0]
> Internet Protocol Version 6, Src: 2001:558:feed::1, Dst: 2601:586:cf01:68c0:8
v User Datagram Protocol, Src Port: 53, Dst Port: 65303
    Source Port: 53
    Destination Port: 65303
    Length: 96
    Checksum: 0x4ee0 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 15]
    [Stream Packet Number: 2]
```

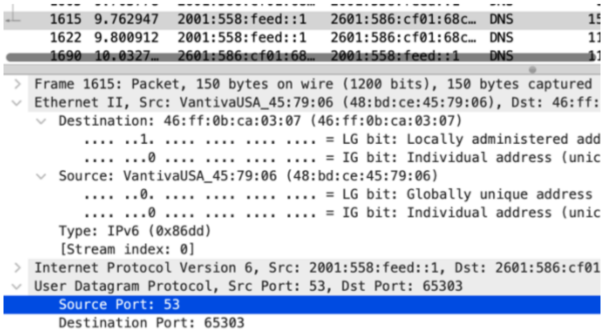
```
0000  46 ff 0b ca 03 07 48 bd  ce 45 79 06 86 dd
0010  31 8a 00 60 11 38 20 01  05 58 fe ed 00 00
0020  00 00 00 00 00 01 26 01  05 86 cf 01 68 c0
0030  e3 1d be a6 b5 75 00 35  ff 17 00 60 4e e0
0040  81 80 00 01 00 00 00 01  00 00 04 67 61 69
0050  63 73 05 75 6d 61 73 73  03 65 64 75 00 00
0060  01 c0 11 00 06 00 01 00  00 0e 10 00 29 05
0070  69 78 31 c0 11 0a 68 6f  73 74 6d 61 73 74
0080  c0 11 78 b4 99 86 00 00  46 50 00 00 0e 10
0090  9d 40 00 01 51 80
```

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

→ The DNS query was sent to destination port 53, and the response came from source port 53.



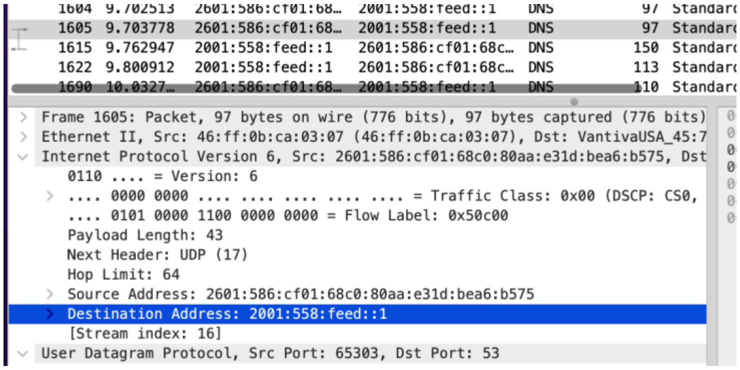
```
1605 9.703778  2601:586:cf01:68…  2001:558:feed::1   DNS    97 Standa
1615 9.762947  2001:558:feed::1   2601:586:cf01:68c… DNS   150 Standa
1622 9.800912  2001:558:feed::1   2601:586:cf01:68c… DNS   113 Standa
1690 10.0327…  2601:586:cf01:68…  2001:558:feed::1   DNS   110 Standa
> Frame 1605: Packet, 97 bytes on wire (776 bits), 97 bytes captured (776 bits)
v Ethernet II, Src: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07), Dst: VantivaUSA_45:7
  v Destination: VantivaUSA_45:79:06 (48:bd:ce:45:79:06)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factor
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (t
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv6 (0x86dd)
    [Stream index: 0]
> Internet Protocol Version 6, Src: 2601:586:cf01:68c0:80aa:e31d:bea6:b575, Dst
v User Datagram Protocol, Src Port: 65303, Dst Port: 53
    Source Port: 65303
    Destination Port: 53
    Length: 43
```



```
1615 9.762947  2001:558:feed::1   2601:586:cf01:68c… DNS   15
1622 9.800912  2001:558:feed::1   2601:586:cf01:68c… DNS   11
1690 10.0327…  2601:586:cf01:68…  2001:558:feed::1   DNS   11
> Frame 1615: Packet, 150 bytes on wire (1200 bits), 150 bytes captured
v Ethernet II, Src: VantivaUSA_45:79:06 (48:bd:ce:45:79:06), Dst: 46:ff:
  v Destination: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07)
      .... ..1. .... .... .... .... = LG bit: Locally administered add
      .... ...0 .... .... .... .... = IG bit: Individual address (unic
  v Source: VantivaUSA_45:79:06 (48:bd:ce:45:79:06)
      .... ..0. .... .... .... .... = LG bit: Globally unique address
      .... ...0 .... .... .... .... = IG bit: Individual address (unic
    Type: IPv6 (0x86dd)
    [Stream index: 0]
> Internet Protocol Version 6, Src: 2001:558:feed::1, Dst: 2601:586:cf01
v User Datagram Protocol, Src Port: 53, Dst Port: 65303
    Source Port: 53
    Destination Port: 65303
```

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

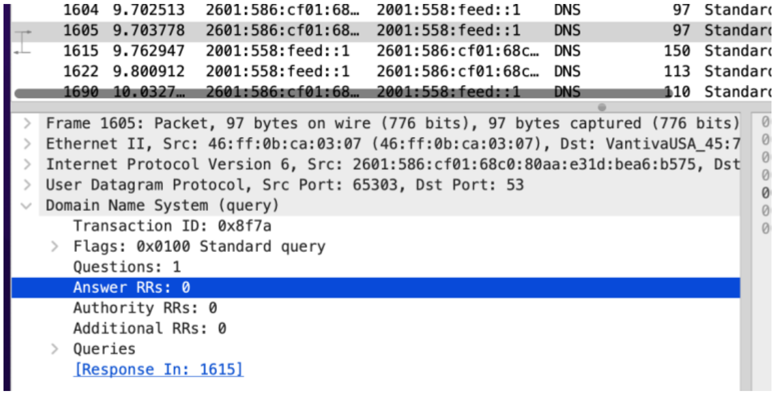
→ The destination IP address of the DNS query was 2001:558:feed::1, which is the DNS resolver.



```
1604 9.702513  2601:586:cf01:68…  2001:558:feed::1   DNS    97 Standar
1605 9.703778  2601:586:cf01:68…  2001:558:feed::1   DNS    97 Standar
1615 9.762947  2001:558:feed::1   2601:586:cf01:68c… DNS   150 Standar
1622 9.800912  2001:558:feed::1   2601:586:cf01:68c… DNS   113 Standar
1690 10.0327…  2601:586:cf01:68…  2001:558:feed::1   DNS   110 Standar
> Frame 1605: Packet, 97 bytes on wire (776 bits), 97 bytes captured (776 bits)
> Ethernet II, Src: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07), Dst: VantivaUSA_45:7
v Internet Protocol Version 6, Src: 2601:586:cf01:68c0:80aa:e31d:bea6:b575, Dst
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0,
    .... 0101 0000 1100 0000 0000 = Flow Label: 0x50c00
    Payload Length: 43
    Next Header: UDP (17)
    Hop Limit: 64
  > Source Address: 2601:586:cf01:68c0:80aa:e31d:bea6:b575
  > Destination Address: 2001:558:feed::1
    [Stream index: 16]
v User Datagram Protocol, Src Port: 65303, Dst Port: 53
```

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

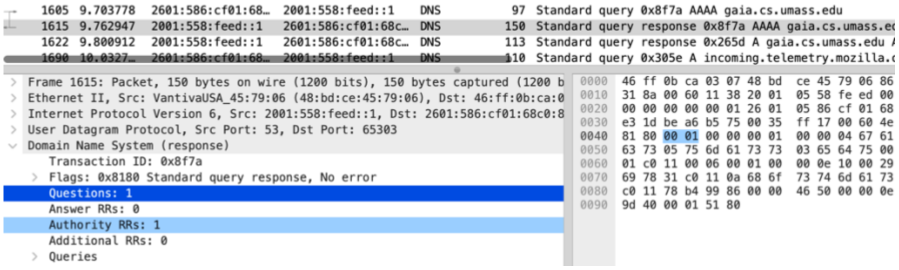
→ The DNS query contained 1 question and 0 answers.



```
1604 9.702513  2601:586:cf01:68…  2001:558:feed::1   DNS    97 Standar
1605 9.703778  2601:586:cf01:68…  2001:558:feed::1   DNS    97 Standar
1615 9.762947  2001:558:feed::1   2601:586:cf01:68c… DNS   150 Standar
1622 9.800912  2001:558:feed::1   2601:586:cf01:68c… DNS   113 Standar
1690 10.0327…  2601:586:cf01:68…  2001:558:feed::1   DNS   110 Standar
> Frame 1605: Packet, 97 bytes on wire (776 bits), 97 bytes captured (776 bits)
> Ethernet II, Src: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07), Dst: VantivaUSA_45:7
> Internet Protocol Version 6, Src: 2601:586:cf01:68c0:80aa:e31d:bea6:b575, Dst
> User Datagram Protocol, Src Port: 65303, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x8f7a
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 1615]
```

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?

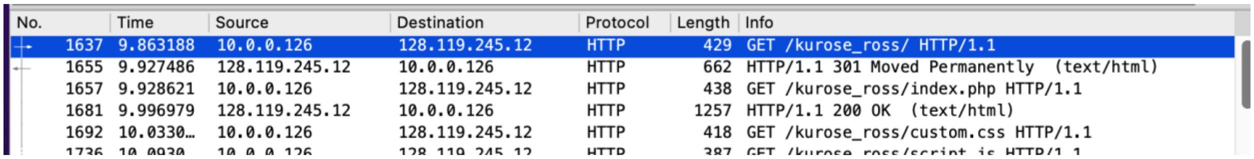
→ The DNS response contained 1 question and 0 answers, with 1 authority record indicating a referral instead of a direct IP.



```
1605  9.703778  2601:586:cf01:68…  2001:558:feed::1   DNS    97  Standard query 0x8f7a AAAA gaia.cs.umass.edu
1615  9.762947  2001:558:feed::1   2601:586:cf01:68c… DNS   150  Standard query response 0x8f7a AAAA gaia.cs.umass.ec
1622  9.800912  2001:558:feed::1   2601:586:cf01:68c… DNS   113  Standard query response 0x265d A gaia.cs.umass.edu /
1690  10.0327…  2601:586:cf01:68…  2001:558:feed::1   DNS   110  Standard query 0x305e A incoming.telemetry.mozilla.c

> Frame 1615: Packet, 150 bytes on wire (1200 bits), 150 bytes captured (1200 b
> Ethernet II, Src: VantivaUSA_45:79:06 (48:bd:ce:45:79:06), Dst: 46:ff:0b:ca:0
> Internet Protocol Version 6, Src: 2001:558:feed::1, Dst: 2601:586:cf01:68c0:8
> User Datagram Protocol, Src Port: 53, Dst Port: 65303
v Domain Name System (response)
    Transaction ID: 0x8f7a
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
  > Queries

0000  46 ff 0b ca 03 07 48 bd  ce 45 79 06 86
0010  31 8a 00 60 11 38 20 01  05 58 fe ed 00
0020  00 00 00 00 00 01 26 01  05 86 cf 01 68
0030  e3 1d be a6 b5 75 00 35  ff 17 00 60 4e
0040  81 80 00 01 00 00 00 01  00 00 04 67 61
0050  63 73 05 75 6d 61 73 73  03 65 64 75 00
0060  01 c0 11 00 06 00 01 00  00 0e 10 00 29
0070  69 78 31 c0 11 0a 68 6f  73 74 6d 61 73
0080  c0 11 78 b4 99 86 00 00  46 50 00 00 0e
0090  9d 40 00 01 51 80
```

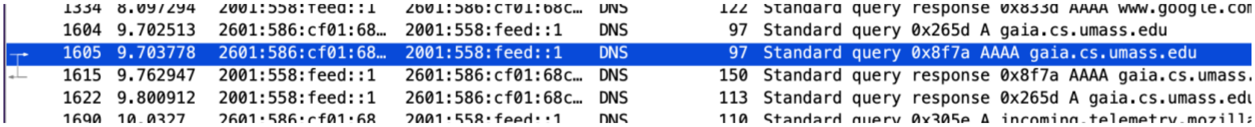
11. The web page for the base file http://gaia.cs.umass.edu/kurose_ross/ references the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg , which, like the base webpage, is on gaia.cs.umass.edu. What is the packet number in the trace for the initial HTTP GET request for the 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.

→ The initial HTTP GET request for the base file http://gaia.cs.umass.edu/kurose_ross/ occurred in packet 1637.



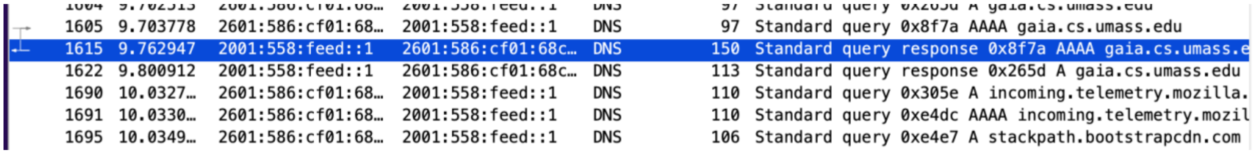
```
No.    Time       Source           Destination      Protocol  Length  Info
1637   9.863188   10.0.0.126       128.119.245.12   HTTP         429  GET /kurose_ross/ HTTP/1.1
1655   9.927486   128.119.245.12   10.0.0.126       HTTP         662  HTTP/1.1 301 Moved Permanently  (text/html)
1657   9.928621   10.0.0.126       128.119.245.12   HTTP         438  GET /kurose_ross/index.php HTTP/1.1
1681   9.996979   128.119.245.12   10.0.0.126       HTTP        1257  HTTP/1.1 200 OK  (text/html)
1692   10.0330…   10.0.0.126       128.119.245.12   HTTP         418  GET /kurose_ross/custom.css HTTP/1.1
1736   10.0930    10.0.0.126       128.119.245.12   HTTP         387  GET /kurose_ross/script.js HTTP/1.1
```

→The DNS query that resolved gaia.cs.umass.edu so the GET could be sent was packet 1605.



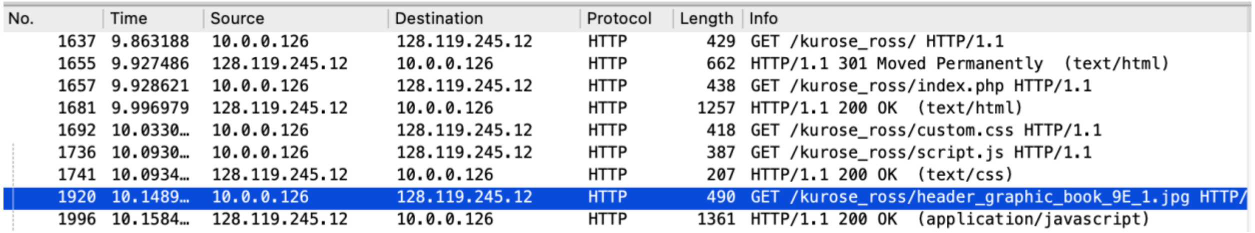
```
1334  8.097294  2001:558:feed::1   2601:586:cf01:68c…  DNS   122  Standard query response 0x833d AAAA www.google.com
1604  9.702513  2601:586:cf01:68…  2001:558:feed::1    DNS    97  Standard query 0x265d A gaia.cs.umass.edu
1605  9.703778  2601:586:cf01:68…  2001:558:feed::1    DNS    97  Standard query 0x8f7a AAAA gaia.cs.umass.edu
1615  9.762947  2001:558:feed::1   2601:586:cf01:68c…  DNS   150  Standard query response 0x8f7a AAAA gaia.cs.umass.
1622  9.800912  2001:558:feed::1   2601:586:cf01:68c…  DNS   113  Standard query response 0x265d A gaia.cs.umass.edu
1690  10.0327   2601:586:cf01:68   2001:558:feed::1    DNS   110  Standard query 0x305e A incoming.telemetry.mozill
```

→ The DNS response providing the server address was packet 1615.



```
1604 9.702513  2601:586:cf01:68…  2001:558:feed::1   DNS    97 Standard query 0x265d A gaia.cs.umass.edu
1605 9.703778  2601:586:cf01:68…  2001:558:feed::1   DNS    97 Standard query 0x8f7a AAAA gaia.cs.umass.edu
1615 9.762947  2001:558:feed::1   2601:586:cf01:68c… DNS   150 Standard query response 0x8f7a AAAA gaia.cs.umass.e
1622 9.800912  2001:558:feed::1   2601:586:cf01:68c… DNS   113 Standard query response 0x265d A gaia.cs.umass.edu
1690 10.0327…  2601:586:cf01:68…  2001:558:feed::1   DNS   110 Standard query 0x305e A incoming.telemetry.mozilla.
1691 10.0330…  2601:586:cf01:68…  2001:558:feed::1   DNS   110 Standard query 0xe4dc AAAA incoming.telemetry.mozil
1695 10.0349…  2601:586:cf01:68…  2001:558:feed::1   DNS   106 Standard query 0xe4e7 A stackpath.bootstrapcdn.com
```

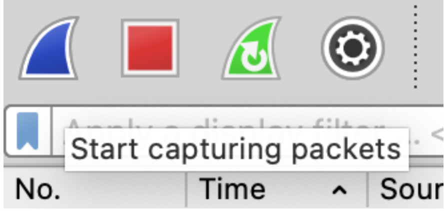
→ The HTTP GET request for the image header_graphic_book_9E_1.jpg was packet 1920.



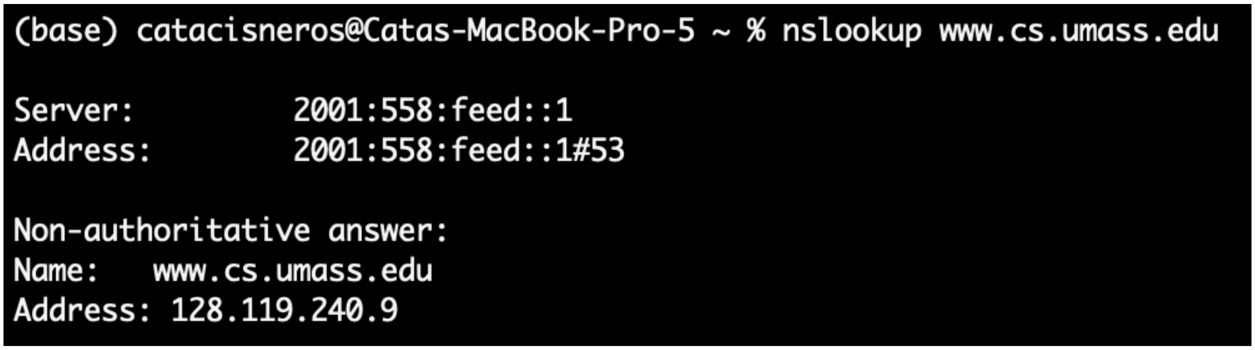
```
No.     Time       Source           Destination      Protocol  Length  Info
   1637 9.863188   10.0.0.126       128.119.245.12   HTTP       429    GET /kurose_ross/ HTTP/1.1
   1655 9.927486   128.119.245.12   10.0.0.126       HTTP       662    HTTP/1.1 301 Moved Permanently  (text/html)
   1657 9.928621   10.0.0.126       128.119.245.12   HTTP       438    GET /kurose_ross/index.php HTTP/1.1
   1681 9.996979   128.119.245.12   10.0.0.126       HTTP      1257    HTTP/1.1 200 OK  (text/html)
   1692 10.0330…   10.0.0.126       128.119.245.12   HTTP       418    GET /kurose_ross/custom.css HTTP/1.1
   1736 10.0930…   10.0.0.126       128.119.245.12   HTTP       387    GET /kurose_ross/script.js HTTP/1.1
   1741 10.0934…   128.119.245.12   10.0.0.126       HTTP       207    HTTP/1.1 200 OK  (text/css)
   1920 10.1489…   10.0.0.126       128.119.245.12   HTTP       490    GET /kurose_ross/header_graphic_book_9E_1.jpg HTTP/
   1996 10.1584…   128.119.245.12   10.0.0.126       HTTP      1361    HTTP/1.1 200 OK  (application/javascript)
```

→ No new DNS query was made before this second GET; the browser reused the cached DNS result from the earlier lookup since the hostname was already resolved and still valid.

- Start packet capture

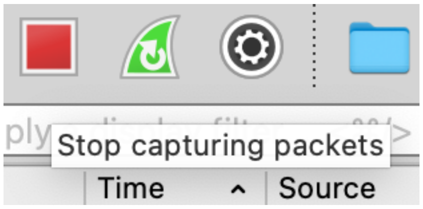


- Do an nslookup on www.cs.umass.edu

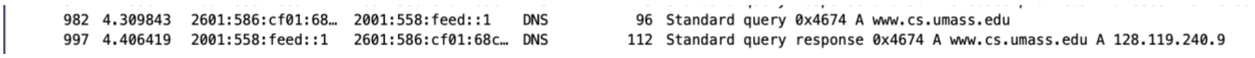


```
(base) catacisneros@Catas-MacBook-Pro-5 ~ % nslookup www.cs.umass.edu

Server:         2001:558:feed::1
Address:        2001:558:feed::1#53

Non-authoritative answer:
Name:    www.cs.umass.edu
Address: 128.119.240.9
```

- Stop capture



- Results

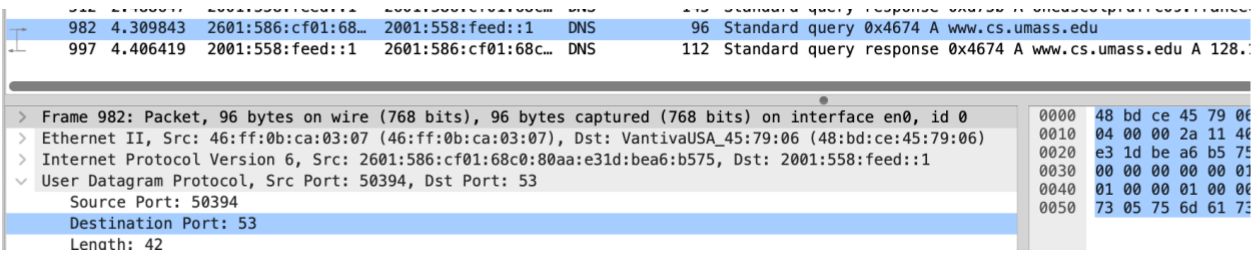


```
982  4.309843  2601:586:cf01:68…  2001:558:feed::1    DNS         96  Standard query 0x4674 A www.cs.umass.edu
997  4.406419  2001:558:feed::1   2601:586:cf01:68c…  DNS        112  Standard query response 0x4674 A www.cs.umass.edu A 128.119.240.9
```

Questions

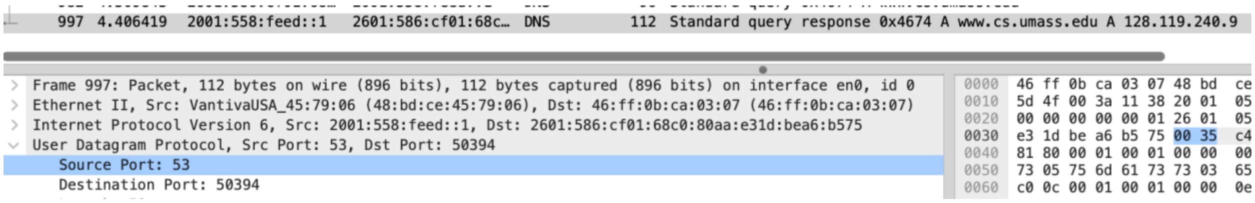
12. What is the destination port for the DNS query message? What is the source port of the DNS response message?

→ The DNS query used destination port 53 (standard DNS port)



```
982  4.309843  2601:586:cf01:68…  2001:558:feed::1    DNS         96  Standard query 0x4674 A www.cs.umass.edu
997  4.406419  2001:558:feed::1   2601:586:cf01:68c…  DNS        112  Standard query response 0x4674 A www.cs.umass.edu A 128.

> Frame 982: Packet, 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface en0, id 0      0000  48 bd ce 45 79 06
> Ethernet II, Src: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07), Dst: VantivaUSA_45:79:06 (48:bd:ce:45:79:06)     0010  04 00 00 2a 11 40
> Internet Protocol Version 6, Src: 2601:586:cf01:68c0:80aa:e31d:bea6:b575, Dst: 2001:558:feed::1           0020  e3 1d be a6 b5 75
v User Datagram Protocol, Src Port: 50394, Dst Port: 53                                                      0030  00 00 00 00 00 01
    Source Port: 50394                                                                                       0040  01 00 00 01 00 00
    Destination Port: 53                                                                                     0050  73 05 75 6d 61 73
    Length: 42
```

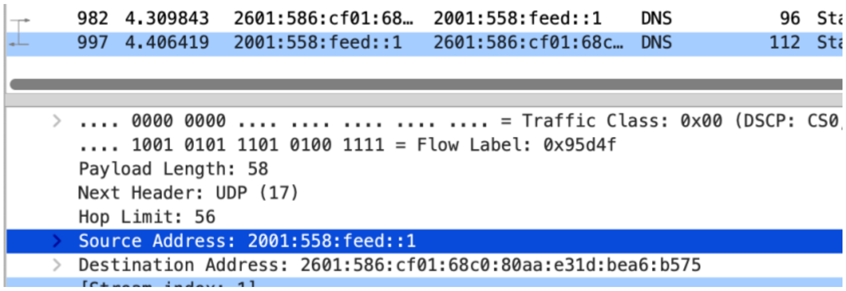
→ The DNS response came from source port 53.



```
997  4.406419  2001:558:feed::1   2601:586:cf01:68c…  DNS        112  Standard query response 0x4674 A www.cs.umass.edu A 128.119.240.9

> Frame 997: Packet, 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface en0, id 0     0000  46 ff 0b ca 03 07 48 bd  ce
> Ethernet II, Src: VantivaUSA_45:79:06 (48:bd:ce:45:79:06), Dst: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07)     0010  5d 4f 00 3a 11 38 20 01  05
> Internet Protocol Version 6, Src: 2001:558:feed::1, Dst: 2601:586:cf01:68c0:80aa:e31d:bea6:b575           0020  00 00 00 00 00 01 26 01  05
v User Datagram Protocol, Src Port: 53, Dst Port: 50394                                                      0030  e3 1d be a6 b5 75 00 35  c4
    Source Port: 53                                                                                          0040  81 80 00 01 00 01 00 00  00
    Destination Port: 50394                                                                                  0050  73 05 75 6d 61 73 73 03  65
                                                                                                             0060  c0 0c 00 01 00 01 00 00  0e
```

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

→ The DNS query was sent to 2001:558:feed::1, which is the same IP address of my default local DNS server

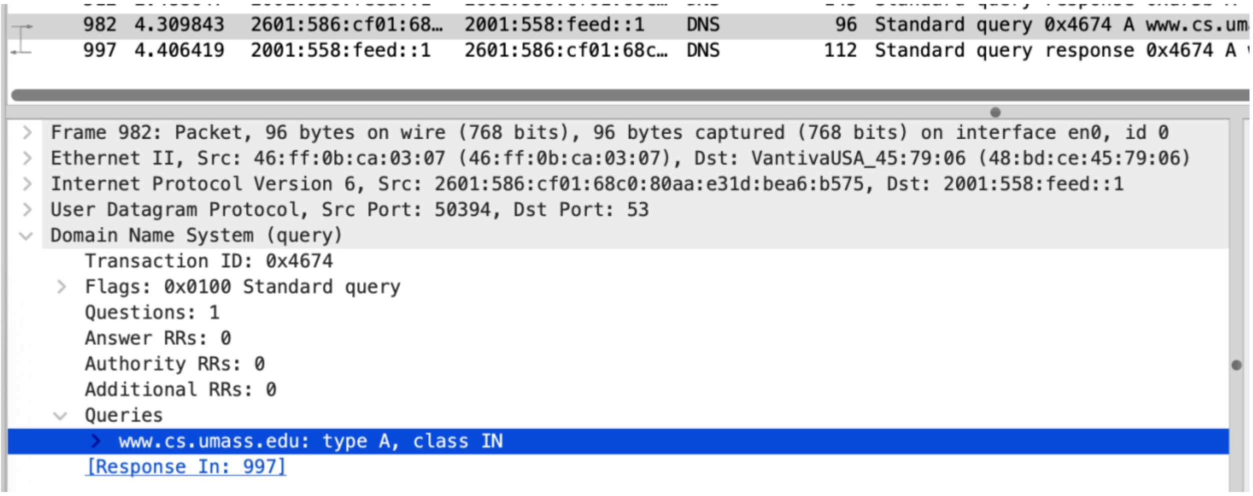


```
982  4.309843  2601:586:cf01:68…  2001:558:feed::1    DNS     96  Sta
997  4.406419  2001:558:feed::1   2601:586:cf01:68c…  DNS    112  Sta

  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0,
    .... 1001 0101 1101 0100 1111 = Flow Label: 0x95d4f
    Payload Length: 58
    Next Header: UDP (17)
    Hop Limit: 56
  > Source Address: 2001:558:feed::1
  > Destination Address: 2601:586:cf01:68c0:80aa:e31d:bea6:b575
    [Stream index: 1]
```

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

→ The DNS query type is A (host address) — requesting the IPv4 address of www.cs.umass.edu.

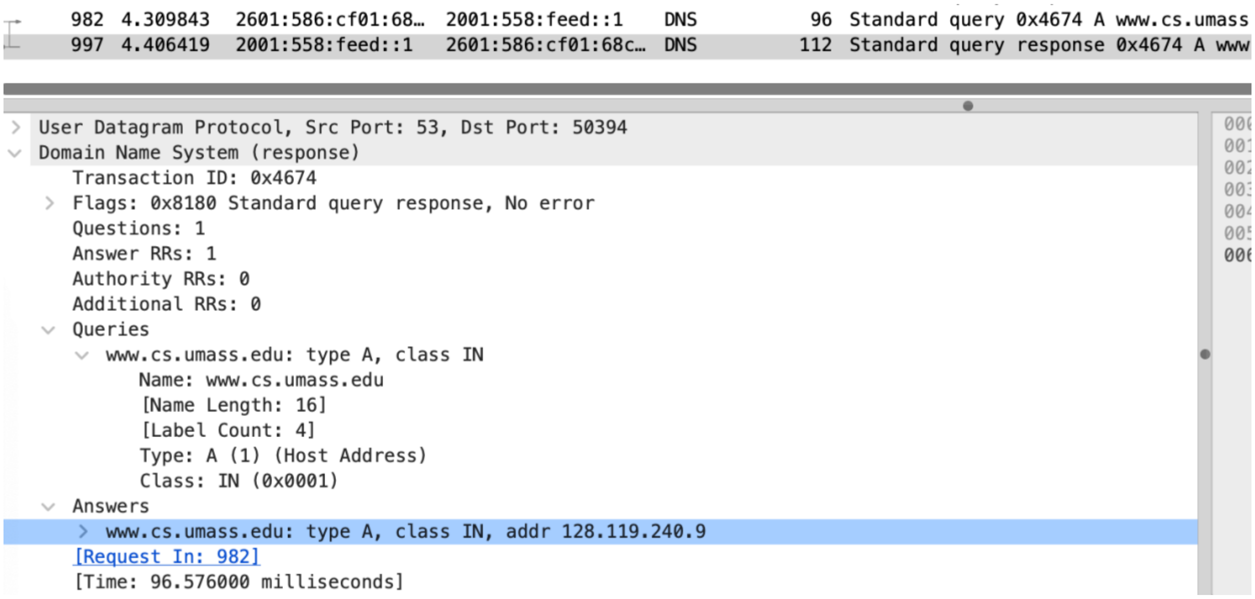
→ The query message contained 1 question and 0 answers.



```
982  4.309843  2601:586:cf01:68…  2001:558:feed::1   DNS      96  Standard query 0x4674 A www.cs.um
997  4.406419  2001:558:feed::1   2601:586:cf01:68c… DNS     112  Standard query response 0x4674 A

> Frame 982: Packet, 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface en0, id 0
> Ethernet II, Src: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07), Dst: VantivaUSA_45:79:06 (48:bd:ce:45:79:06)
> Internet Protocol Version 6, Src: 2601:586:cf01:68c0:80aa:e31d:bea6:b575, Dst: 2001:558:feed::1
> User Datagram Protocol, Src Port: 50394, Dst Port: 53
v Domain Name System (query)
     Transaction ID: 0x4674
   > 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: 997]
```

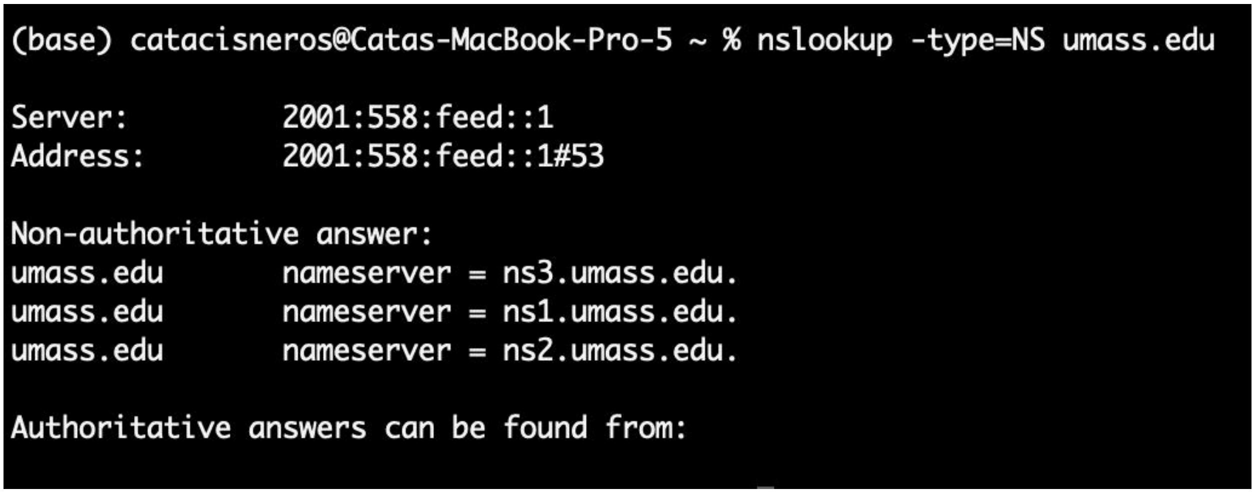
15. Examine the DNS response message to the query message. How many “questions” does this DNS response message contain? How many “answers”?

→ The DNS response message contained 1 question and 1 answer, returning the IP address 128.119.240.9 for www.cs.umass.edu.



```
982  4.309843  2601:586:cf01:68…  2001:558:feed::1   DNS      96  Standard query 0x4674 A www.cs.umass
997  4.406419  2001:558:feed::1   2601:586:cf01:68c… DNS     112  Standard query response 0x4674 A www

> User Datagram Protocol, Src Port: 53, Dst Port: 50394
v Domain Name System (response)
     Transaction ID: 0x4674
   > Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 1
     Authority RRs: 0
     Additional RRs: 0
   v Queries
      v www.cs.umass.edu: type A, class IN
           Name: www.cs.umass.edu
           [Name Length: 16]
           [Label Count: 4]
           Type: A (1) (Host Address)
           Class: IN (0x0001)
   v Answers
      > www.cs.umass.edu: type A, class IN, addr 128.119.240.9
     [Request In: 982]
     [Time: 96.576000 milliseconds]
```

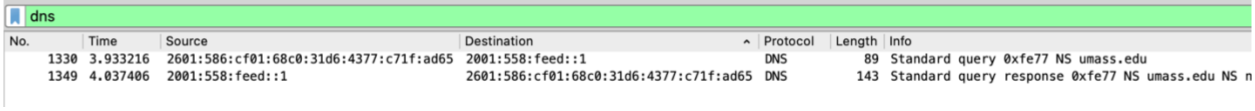
Last, let’s use nslookup to issue a command that will return a type NS DNS record, Enter the following command: nslookup –type=NS umass.edu and then answer the following questions:



```
(base) catacisneros@Catas-MacBook-Pro-5 ~ % nslookup -type=NS umass.edu

Server:         2001:558:feed::1
Address:        2001:558:feed::1#53

Non-authoritative answer:
umass.edu       nameserver = ns3.umass.edu.
umass.edu       nameserver = ns1.umass.edu.
umass.edu       nameserver = ns2.umass.edu.

Authoritative answers can be found from:
```

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

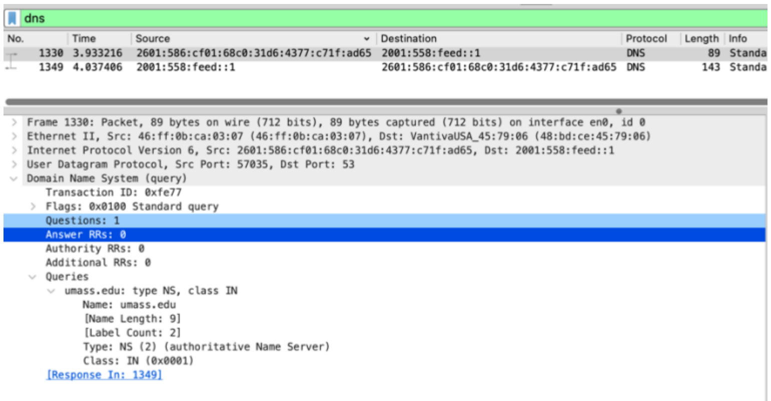
→The DNS query was sent to 2001:558:feed::1, which is the default local DNS server



```
dns
No.     Time      Source                                  Destination                             Protocol  Length  Info
   1330 3.933216  2601:586:cf01:68c0:31d6:4377:c71f:ad65  2001:558:feed::1                        DNS           89  Standard query 0xfe77 NS umass.edu
   1349 4.037406  2001:558:feed::1                        2601:586:cf01:68c0:31d6:4377:c71f:ad65  DNS          143  Standard query response 0xfe77 NS umass.edu NS n
```

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

→ The query message contains 1 question and 0 answers. It requests an NS (name server) record for umass.edu.



```
dns
No.     Time      Source                                  Destination                             Protocol  Length  Info
   1330 3.933216  2601:586:cf01:68c0:31d6:4377:c71f:ad65  2001:558:feed::1                        DNS           89  Standa
   1349 4.037406  2001:558:feed::1                        2601:586:cf01:68c0:31d6:4377:c71f:ad65  DNS          143  Standa

> Frame 1330: Packet, 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface en0, id 0
> Ethernet II, Src: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07), Dst: VantivaUSA_45:79:06 (48:bd:ce:45:79:06)
> Internet Protocol Version 6, Src: 2601:586:cf01:68c0:31d6:4377:c71f:ad65, Dst: 2001:558:feed::1
> User Datagram Protocol, Src Port: 57035, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xfe77
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v umass.edu: type NS, class IN
        Name: umass.edu
        [Name Length: 9]
        [Label Count: 2]
        Type: NS (2) (authoritative Name Server)
        Class: IN (0x0001)
    [Response In: 1349]
```

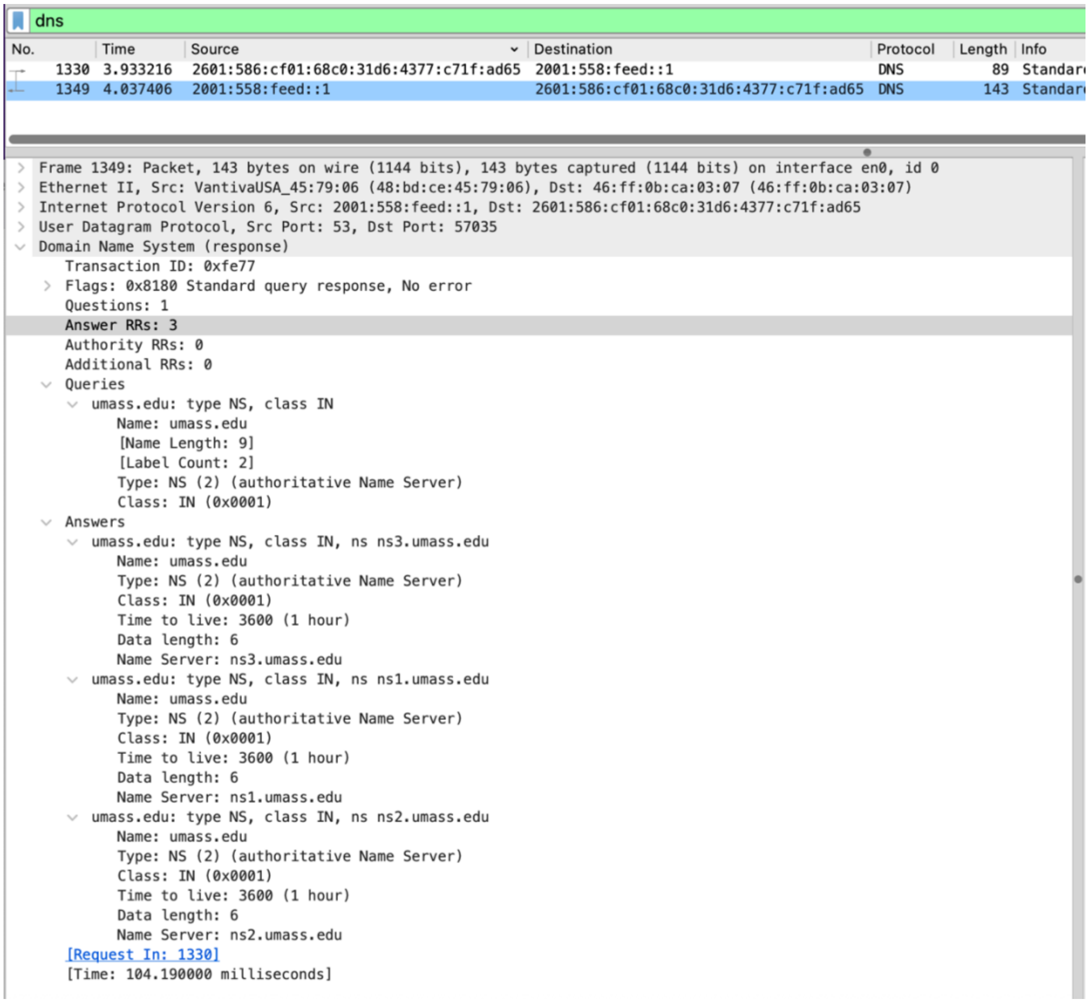
18. Examine the DNS response message (in particular the DNS response message that has type "NS"). How many answers does the response have? What information is contained in the answers? How many additional resource records are returned? What additional information is included in these additional resource records (if additional information is returned)?

→The DNS response contains 1 question and 3 answers.

→ The answers list the authoritative name servers for umass.edu:

- ns3.umass.edu
- ns1.umass.edu
- ns2.umass.edu.

→There are no additional resource records in this response.



dns

```
No.     Time      Source                                   Destination                              Protocol  Length  Info
 1330   3.933216  2601:586:cf01:68c0:31d6:4377:c71f:ad65  2001:558:feed::1                         DNS           89  Standar
 1349   4.037406  2001:558:feed::1                         2601:586:cf01:68c0:31d6:4377:c71f:ad65  DNS          143  Standar
```

```
> Frame 1349: Packet, 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface en0, id 0
> Ethernet II, Src: VantivaUSA_45:79:06 (48:bd:ce:45:79:06), Dst: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07)
> Internet Protocol Version 6, Src: 2001:558:feed::1, Dst: 2601:586:cf01:68c0:31d6:4377:c71f:ad65
> User Datagram Protocol, Src Port: 53, Dst Port: 57035
v Domain Name System (response)
    Transaction ID: 0xfe77
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v umass.edu: type NS, class IN
          Name: umass.edu
          [Name Length: 9]
          [Label Count: 2]
          Type: NS (2) (authoritative Name Server)
          Class: IN (0x0001)
  v Answers
    v umass.edu: type NS, class IN, ns ns3.umass.edu
          Name: umass.edu
          Type: NS (2) (authoritative Name Server)
          Class: IN (0x0001)
          Time to live: 3600 (1 hour)
          Data length: 6
          Name Server: ns3.umass.edu
    v umass.edu: type NS, class IN, ns ns1.umass.edu
          Name: umass.edu
          Type: NS (2) (authoritative Name Server)
          Class: IN (0x0001)
          Time to live: 3600 (1 hour)
          Data length: 6
          Name Server: ns1.umass.edu
    v umass.edu: type NS, class IN, ns ns2.umass.edu
          Name: umass.edu
          Type: NS (2) (authoritative Name Server)
          Class: IN (0x0001)
          Time to live: 3600 (1 hour)
          Data length: 6
          Name Server: ns2.umass.edu
    [Request In: 1330]
    [Time: 104.190000 milliseconds]
```