LAB 2_Jinbo Li / Taoran Liu
Statement: We have read and understood the course academic integrity policy.

Q1: 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?

A: The IP address of the web server for the IIT is 103.21.124.10

```
C:\WINDOWS\system32\cmd.

Microsoft Windows [Version 10.0.22621.2361]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ljb>nslookup www.iitb.ac.in
Server:  cdns01.comcast.net
Address:  75.75.75.75

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

Q2: What is the IP address of the DNS server that provided the answer to your nslookup command in question 1 above?

A: The IP address of the DNS server is 75.75.75.75 provided by Comcast.

```
C:\WINDOWS\system32\cmd.

Microsoft Windows [Version 10.0.22621.2361]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ljb>nslookup www.iitb.ac.in
Server:  cdns01.comcast.net
Address:  75.75.75.75

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

Q3: Did the answer to your nslookup command in question 1 above come from an authoritative or non-authoritative server?

A: It is from an non-anthoritative server.

```
C:\WINDOWS\system32\cmd.

Microsoft Windows [Version 10.0.22621.2361]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ljb>nslookup www.iitb.ac.in
Server:  cdns01.comcast.net
Address:  75.75.75.75

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

Q4: Use the nslookup command to determine the name of the authoritative name server for the iitb.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?

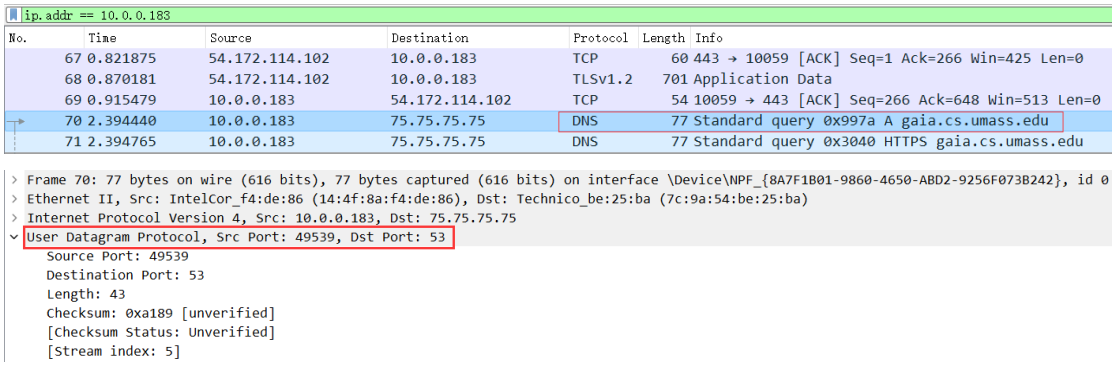
A: The name is “dns3.iitb.ac.in”. I can use command “nslookup dns3.iitb.ac.in” to find the IP address of the authoritative name server.

```
C:\Users\ljb>nslookup -type=NS iitb.ac.in
Server:  cdns01.comcast.net
Address:  75.75.75.75

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

```
C:\Users\ljb>nslookup dns3.iitb.ac.in
Server:  cdns01.comcast.net
Address:  75.75.75.75

Non-authoritative answer:
Name:    dns3.iitb.ac.in
Address:  103.21.127.129
```

Q5: Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number in the trace for the DNS query message? Is this query message sent over UDP or TCP?

A: The package number is 70. This query message sent over UDP.



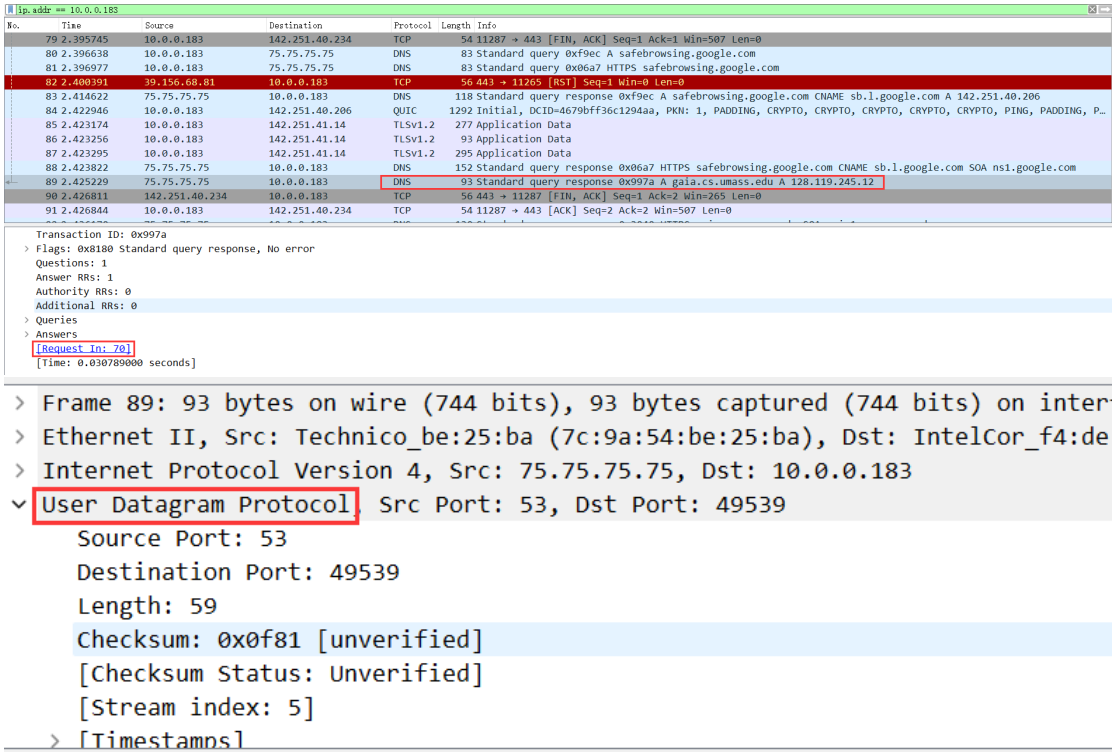
ip.addr == 10.0.0.183

No.	Time	Source	Destination	Protocol	Length	Info
67	0.821875	54.172.114.102	10.0.0.183	TCP	60	443 → 10059 [ACK] Seq=1 Ack=266 Win=425 Len=0
68	0.870181	54.172.114.102	10.0.0.183	TLSv1.2	701	Application Data
69	0.915479	10.0.0.183	54.172.114.102	TCP	54	10059 → 443 [ACK] Seq=266 Ack=648 Win=513 Len=0
70	2.394440	10.0.0.183	75.75.75.75	DNS	77	Standard query 0x997a A gaia.cs.umass.edu
71	2.394765	10.0.0.183	75.75.75.75	DNS	77	Standard query 0x3040 HTTPS gaia.cs.umass.edu

```
> Frame 70: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{8A7F1B01-9860-4650-ABD2-9256F073B242}, id 0
> Ethernet II, Src: IntelCor_f4:de:86 (14:4f:8a:f4:de:86), Dst: Technico_be:25:ba (7c:9a:54:be:25:ba)
> Internet Protocol Version 4, Src: 10.0.0.183, Dst: 75.75.75.75
v User Datagram Protocol, Src Port: 49539, Dst Port: 53
    Source Port: 49539
    Destination Port: 53
    Length: 43
    Checksum: 0xa189 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
```

Q6: 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?

A: The package number in the trace for the DNS response message is 89. This response message received via UDP.



ip.addr == 10.0.0.183

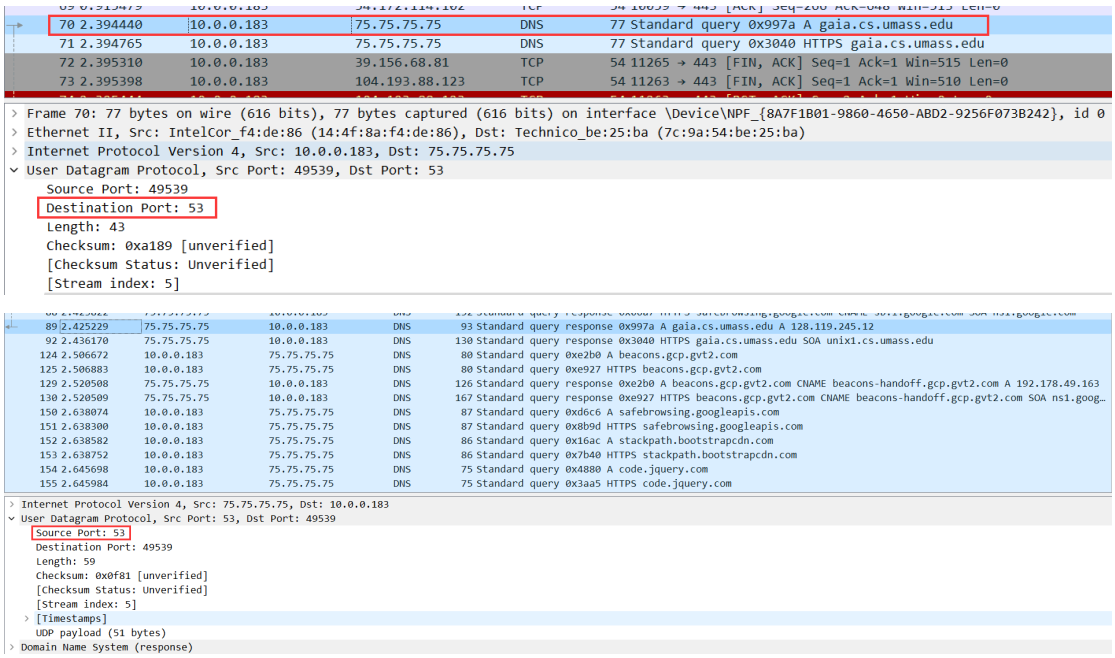
No.	Time	Source	Destination	Protocol	Length	Info
79	2.395745	10.0.0.183	142.251.40.234	TCP	54	11287 → 443 [FIN, ACK] Seq=1 Ack=1 Win=507 Len=0
80	2.396638	10.0.0.183	75.75.75.75	DNS	83	Standard query 0xf9ec A safebrowsing.google.com
81	2.396977	10.0.0.183	75.75.75.75	DNS	83	Standard query 0x06a7 HTTPS safebrowsing.google.com
82	2.400391	39.156.68.81	10.0.0.183	TCP	56	443 → 11265 [RST] Seq=1 Win=0 Len=0
83	2.414622	75.75.75.75	10.0.0.183	DNS	118	Standard query response 0xf9ec A safebrowsing.google.com CNAME sb.l.google.com A 142.251.40.206
84	2.422946	10.0.0.183	142.251.40.206	QUIC	1292	Initial, DCID=4679bff36c1294aa, PKN: 1, PADDING, CRYPTO, CRYPTO, CRYPTO, CRYPTO, CRYPTO, PING, PADDING, P…
85	2.423174	10.0.0.183	142.251.41.14	TLSv1.2	277	Application Data
86	2.423256	10.0.0.183	142.251.41.14	TLSv1.2	93	Application Data
87	2.423295	10.0.0.183	142.251.41.14	TLSv1.2	295	Application Data
88	2.423822	75.75.75.75	10.0.0.183	DNS	152	Standard query response 0x06a7 HTTPS safebrowsing.google.com CNAME sb.l.google.com SOA ns1.google.com
89	2.425229	75.75.75.75	10.0.0.183	DNS	93	Standard query response 0x997a A gaia.cs.umass.edu A 128.119.245.12
90	2.426811	142.251.40.234	10.0.0.183	TCP	56	443 → 11287 [FIN, ACK] Seq=1 Ack=2 Win=265 Len=0
91	2.426844	10.0.0.183	142.251.40.234	TCP	54	11287 → 443 [ACK] Seq=2 Ack=2 Win=507 Len=0

```
  Transaction ID: 0x997a
> Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
> Queries
> Answers
  [Request In: 70]
  [Time: 0.030789000 seconds]
```

```
> Frame 89: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on inter
> Ethernet II, Src: Technico_be:25:ba (7c:9a:54:be:25:ba), Dst: IntelCor_f4:de
> Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.183
v User Datagram Protocol, Src Port: 53, Dst Port: 49539
    Source Port: 53
    Destination Port: 49539
    Length: 59
    Checksum: 0x0f81 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
  > [Timestamps]
```

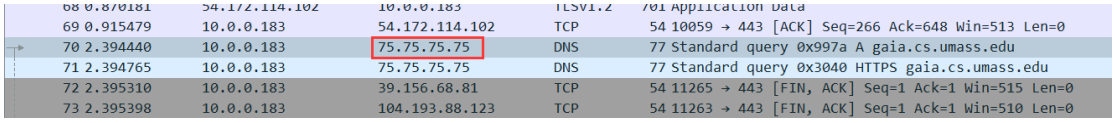
Q7: What is the destination port for the DNS query message? What is the source port of the DNS response message?

A: The destination port for the DNS query message is 53. The source port of the DNS response message is 53.



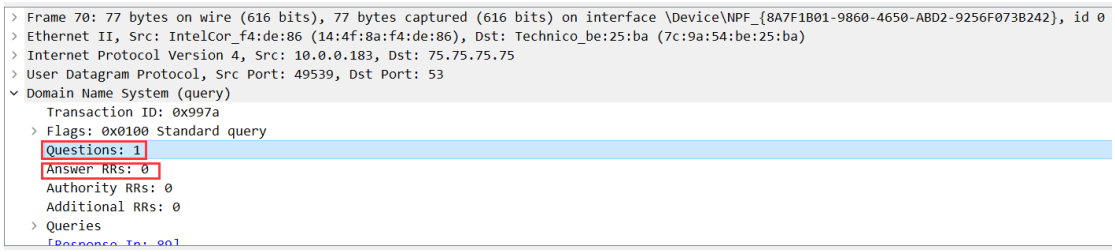
Q8: To what IP address is the DNS query message sent?

A: 75.75.75.75



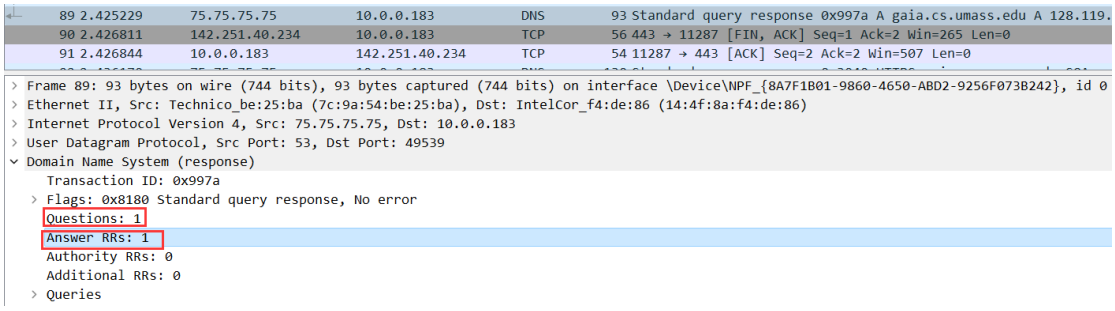
Q9: Examine the DNS query message. How many "questions" does this DNS message contain? How many "answers" answers does it contain?

A: This DNS message contains 1 question and it contains 0 answer.



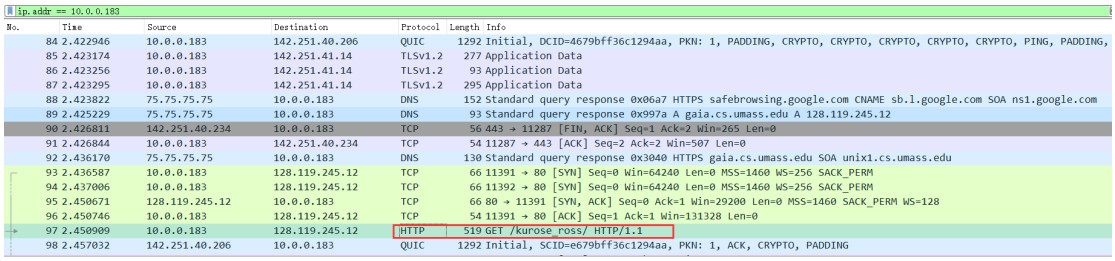
Q10: Examine the DNS response message to the initial query message. How many "questions" does this DNS message contain? How many "answers" answers does it contain?

A: This DNS message contains 1 question and contains 1 answer.



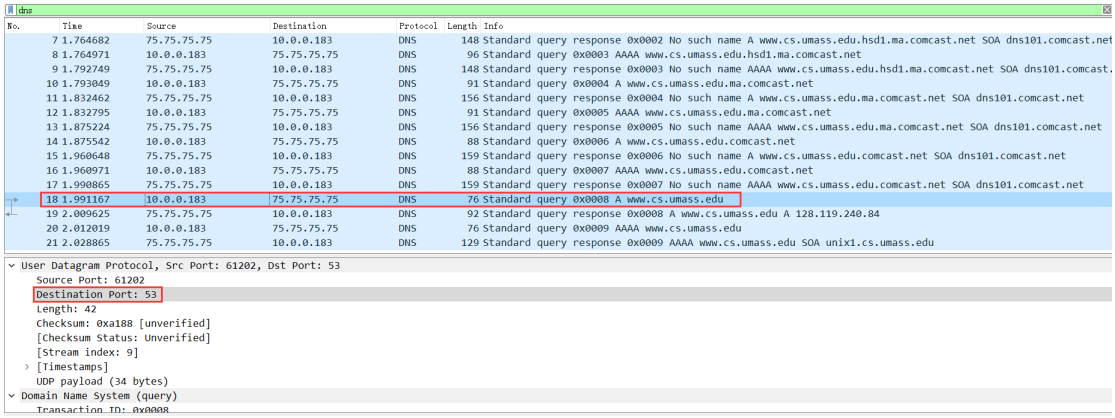
Q11: This web page contains images. Before retrieving each image, does your host issue new DNS queries?

A: No, my host did not issue new DNS queries according to WireShark (ignore HTTPS DNS query). When the web page was loaded at the first time, all the DNS records of images were cached in local. Thus, my host used cached DNS before retrieving each images.



Q12: What is the destination port for the DNS query message? What is the source port of the DNS response message?

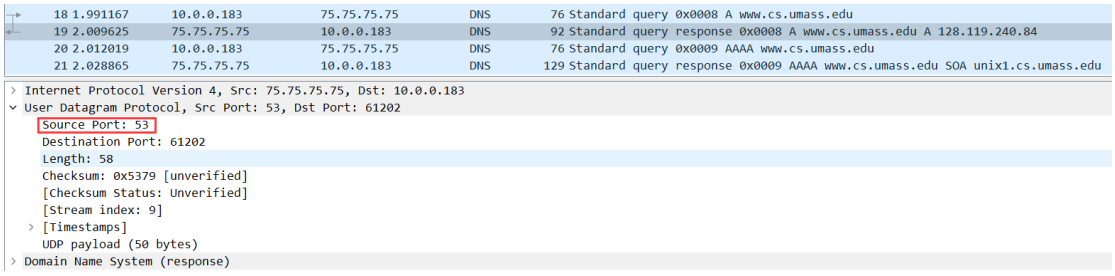
A: The destination port for the DNS query message is 53. The source port of the DNS response message is 53.



dns

No.	Time	Source	Destination	Protocol	Length	Info
7	1.764682	75.75.75.75	10.0.0.183	DNS	148	Standard query response 0x0002 No such name A www.cs.umass.edu.hsd1.ma.comcast.net SOA dns101.comcast.net
8	1.764971	10.0.0.183	75.75.75.75	DNS	96	Standard query 0x0003 AAAA www.cs.umass.edu.hsd1.ma.comcast.net
9	1.792749	75.75.75.75	10.0.0.183	DNS	148	Standard query response 0x0003 No such name AAAA www.cs.umass.edu.hsd1.ma.comcast.net SOA dns101.comcast.
10	1.793049	10.0.0.183	75.75.75.75	DNS	91	Standard query 0x0004 A www.cs.umass.edu.ma.comcast.net
11	1.832462	75.75.75.75	10.0.0.183	DNS	156	Standard query response 0x0004 No such name A www.cs.umass.edu.ma.comcast.net SOA dns101.comcast.net
12	1.832795	10.0.0.183	75.75.75.75	DNS	91	Standard query 0x0005 AAAA www.cs.umass.edu.ma.comcast.net
13	1.875224	75.75.75.75	10.0.0.183	DNS	156	Standard query response 0x0005 No such name AAAA www.cs.umass.edu.ma.comcast.net SOA dns101.comcast.net
14	1.875542	10.0.0.183	75.75.75.75	DNS	88	Standard query 0x0006 A www.cs.umass.edu.comcast.net
15	1.960648	75.75.75.75	10.0.0.183	DNS	159	Standard query response 0x0006 No such name A www.cs.umass.edu.comcast.net SOA dns101.comcast.net
16	1.960971	10.0.0.183	75.75.75.75	DNS	88	Standard query 0x0007 AAAA www.cs.umass.edu.comcast.net
17	1.990865	75.75.75.75	10.0.0.183	DNS	159	Standard query response 0x0007 No such name AAAA www.cs.umass.edu.comcast.net SOA dns101.comcast.net
18	1.991167	10.0.0.183	75.75.75.75	DNS	76	Standard query 0x0008 A www.cs.umass.edu
19	2.009625	75.75.75.75	10.0.0.183	DNS	92	Standard query response 0x0008 A www.cs.umass.edu A 128.119.240.84
20	2.012019	10.0.0.183	75.75.75.75	DNS	76	Standard query 0x0009 AAAA www.cs.umass.edu
21	2.028865	75.75.75.75	10.0.0.183	DNS	129	Standard query response 0x0009 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu

```
User Datagram Protocol, Src Port: 61202, Dst Port: 53
    Source Port: 61202
    Destination Port: 53
    Length: 42
    Checksum: 0xa188 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 9]
  > [Timestamps]
    UDP payload (34 bytes)
Domain Name System (query)
    Transaction ID: 0x0008
```

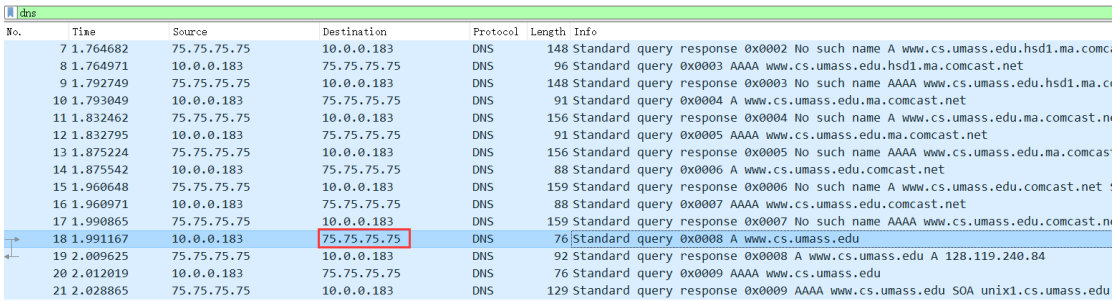


18	1.991167	10.0.0.183	75.75.75.75	DNS	76	Standard query 0x0008 A www.cs.umass.edu
19	2.009625	75.75.75.75	10.0.0.183	DNS	92	Standard query response 0x0008 A www.cs.umass.edu A 128.119.240.84
20	2.012019	10.0.0.183	75.75.75.75	DNS	76	Standard query 0x0009 AAAA www.cs.umass.edu
21	2.028865	75.75.75.75	10.0.0.183	DNS	129	Standard query response 0x0009 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu

```
> Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.183
  User Datagram Protocol, Src Port: 53, Dst Port: 61202
    Source Port: 53
    Destination Port: 61202
    Length: 58
    Checksum: 0x5379 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 9]
  > [Timestamps]
    UDP payload (50 bytes)
> Domain Name System (response)
```

Q13: To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

A: The DNS query message sent to 75.75.75.75. This IP address is my default local DNS server.

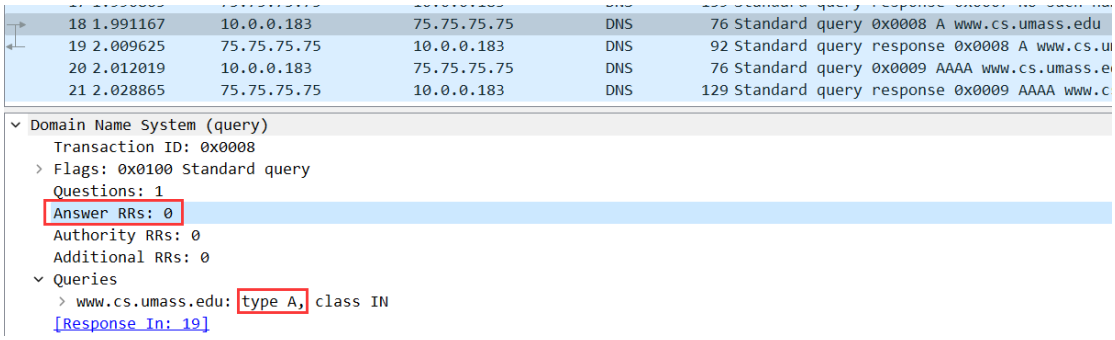


dns

No.	Time	Source	Destination	Protocol	Length	Info
7	1.764682	75.75.75.75	10.0.0.183	DNS	148	Standard query response 0x0002 No such name A www.cs.umass.edu.hsd1.ma.comc
8	1.764971	10.0.0.183	75.75.75.75	DNS	96	Standard query 0x0003 AAAA www.cs.umass.edu.hsd1.ma.comcast.net
9	1.792749	75.75.75.75	10.0.0.183	DNS	148	Standard query response 0x0003 No such name AAAA www.cs.umass.edu.hsd1.ma.c
10	1.793049	10.0.0.183	75.75.75.75	DNS	91	Standard query 0x0004 A www.cs.umass.edu.ma.comcast.net
11	1.832462	75.75.75.75	10.0.0.183	DNS	156	Standard query response 0x0004 No such name A www.cs.umass.edu.ma.comcast.n
12	1.832795	10.0.0.183	75.75.75.75	DNS	91	Standard query 0x0005 AAAA www.cs.umass.edu.ma.comcast.net
13	1.875224	75.75.75.75	10.0.0.183	DNS	156	Standard query response 0x0005 No such name AAAA www.cs.umass.edu.ma.comcas
14	1.875542	10.0.0.183	75.75.75.75	DNS	88	Standard query 0x0006 A www.cs.umass.edu.comcast.net
15	1.960648	75.75.75.75	10.0.0.183	DNS	159	Standard query response 0x0006 No such name A www.cs.umass.edu.comcast.net
16	1.960971	10.0.0.183	75.75.75.75	DNS	88	Standard query 0x0007 AAAA www.cs.umass.edu.comcast.net
17	1.990865	75.75.75.75	10.0.0.183	DNS	159	Standard query response 0x0007 No such name AAAA www.cs.umass.edu.comcast.n
18	1.991167	10.0.0.183	75.75.75.75	DNS	76	Standard query 0x0008 A www.cs.umass.edu
19	2.009625	75.75.75.75	10.0.0.183	DNS	92	Standard query response 0x0008 A www.cs.umass.edu A 128.119.240.84
20	2.012019	10.0.0.183	75.75.75.75	DNS	76	Standard query 0x0009 AAAA www.cs.umass.edu
21	2.028865	75.75.75.75	10.0.0.183	DNS	129	Standard query response 0x0009 AAAA www.cs.umass.edu SOA unix1.cs.umass.edu

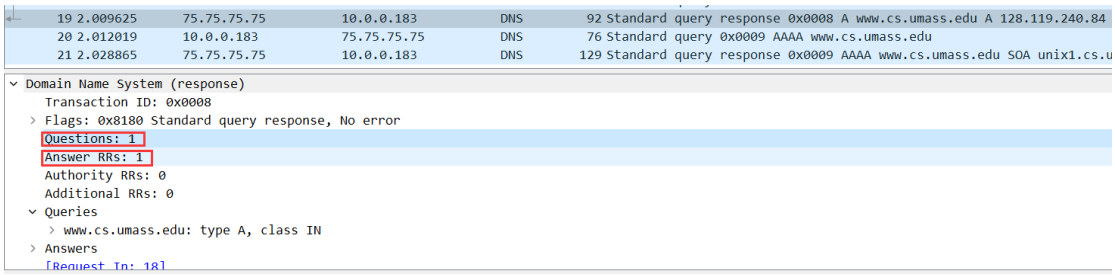
Q14: Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers" ?

A: The type is A. No, it does not contain any answer.



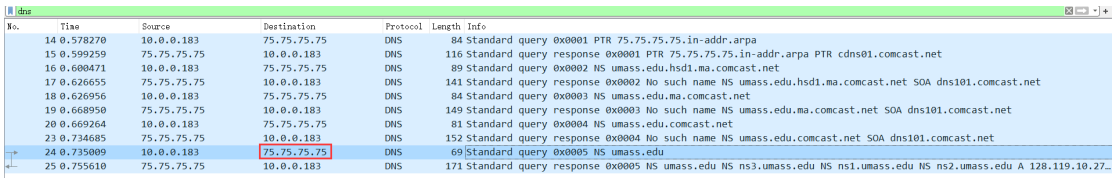
Q15: Examine the DNS response message to the query message. How many "questions" does this DNS response message contain? How many "answers"?

A: This DNS response message contains 1 question. It contains 1 answer.



Q16: To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

A: The IP address is 75.75.75.75. It is the IP address of my default local DNS server.



Q17: Examine the DNS query message. How many questions does the query have? Does the query message contain any "answers"?

A: The query has 1 question. The query message does not contain any answer.

```
> Frame 24: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{8A7F1B01-
> Ethernet II, Src: IntelCor_f4:de:86 (14:4f:8a:f4:de:86), Dst: Technico_be:25:ba (7c:9a:54:be:25:ba)
> Internet Protocol Version 4, Src: 10.0.0.183, Dst: 75.75.75.75
> User Datagram Protocol, Src Port: 53086, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0005
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

Q18: 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?

A: The response has 3 answers. The answers contain "umass.edu: type NS, class IN, ns ns3.umass.edu", "umass.edu: type NS, class IN, ns ns1.umass.edu" and "umass.edu: type NS, class IN, ns ns2.umass.edu".

3 additional resource records are returned. The additional information is "ns1.umass.edu: type A, class IN, addr 128.119.10.27"," ns2.umass.edu: type A, class IN, addr 128.119.10.28" and "ns3.umass.edu: type A, class IN, addr 69.16.40.18".

```
25 0.755610   75.75.75.75   10.0.0.183   DNS   171 Standard query response 0x0005 NS umass.edu NS ns3.umass.edu NS ns1.umass.edu NS ns2

> User Datagram Protocol, Src Port: 53, Dst Port: 53086
v Domain Name System (response)
    Transaction ID: 0x0005
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 3
  > Queries
  > Answers
  v Additional records
    v ns1.umass.edu: type A, class IN, addr 128.119.10.27
        Name: ns1.umass.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
        Time to live: 3130 (52 minutes, 10 seconds)
        Data length: 4
        Address: 128.119.10.27
```

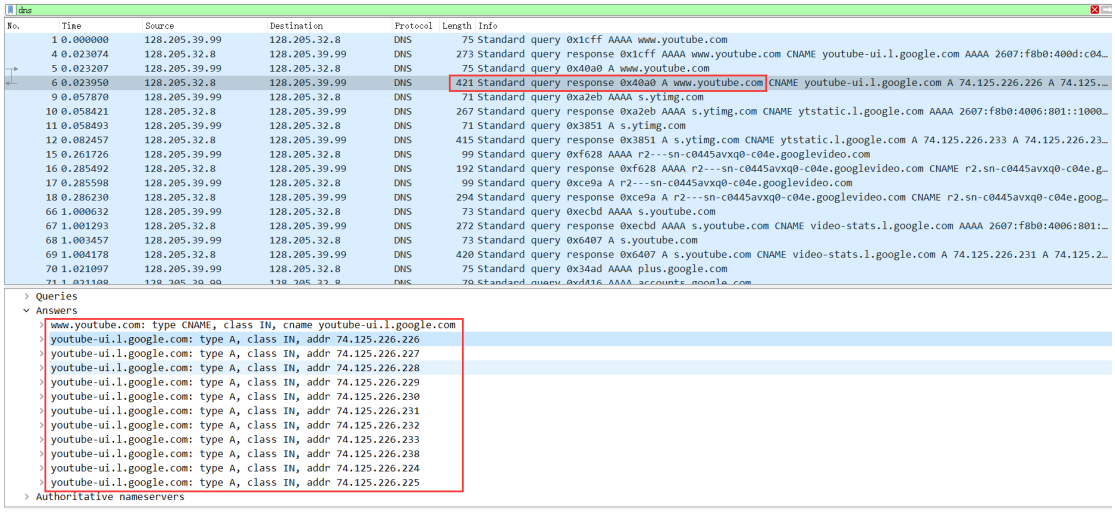
```
Answers
  umass.edu: type NS, class IN, ns ns3.umass.edu
    Name: umass.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 3600 (1 hour)
    Data length: 6
    Name Server: ns3.umass.edu
  umass.edu: type NS, class IN, ns ns1.umass.edu
    Name: umass.edu
    Type: NS (authoritative Name Server) (2)
    Class: IN (0x0001)
    Time to live: 3600 (1 hour)
    Data length: 6
    Name Server: ns1.umass.edu
  umass.edu: type NS, class IN, ns ns2.umass.edu
    Name: umass.edu
    Type: NS (authoritative Name Server) (2)
```

```
> Frame 25: 171 bytes on wire (1368 bits), 171 bytes captured (1368 bits) on interface \D
> Ethernet II, Src: Technico_be:25:ba (7c:9a:54:be:25:ba), Dst: IntelCor_f4:de:86 (14:4f:
> Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.183
> User Datagram Protocol, Src Port: 53, Dst Port: 53086
v Domain Name System (response)
    Transaction ID: 0x0005
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 3
  > Queries
  > Answers
  v Additional records
    v ns1.umass.edu: type A, class IN, addr 128.119.10.27
        Name: ns1.umass.edu
        Type: A (Host Address) (1)
        Class: IN (0x0001)
```

```
v Additional records
  v ns1.umass.edu: type A, class IN, addr 128.119.10.27
      Name: ns1.umass.edu
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 3130 (52 minutes, 10 seconds)
      Data length: 4
      Address: 128.119.10.27
  v ns2.umass.edu: type A, class IN, addr 128.119.10.28
      Name: ns2.umass.edu
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 2587 (43 minutes, 7 seconds)
      Data length: 4
      Address: 128.119.10.28
  v ns3.umass.edu: type A, class IN, addr 69.16.40.18
      Name: ns3.umass.edu
      Type: A (Host Address) (1)
```

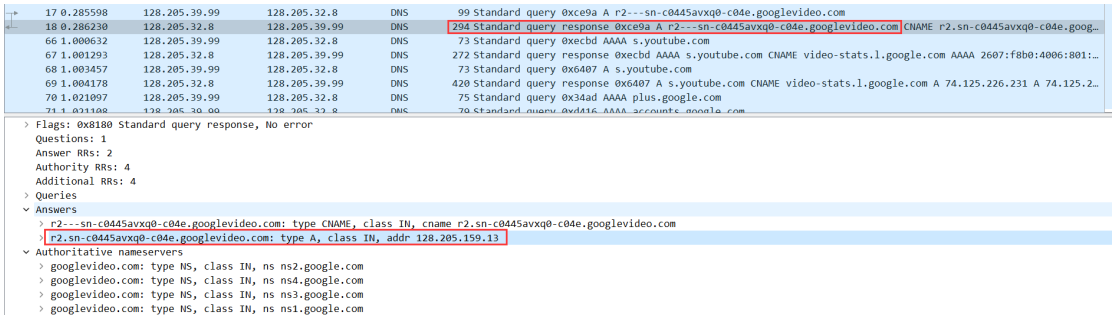
Q19: What are the IP addresses returned by DNS when the host requests a DNS lookup for www.youtube.com? If there is more than one DNS query, list all the unique IPs in the DNS responses.

A: The IP addresses returned by DNS are 74.125.226.224-74.125.226.233 and 74.125.226.238.



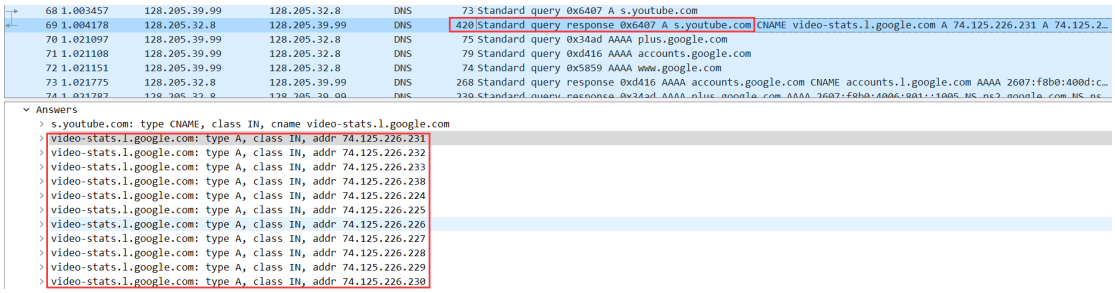
Q20: What are the IP addresses returned by DNS when the host requests a DNS lookup for any hostname containing googlevideo.com? If there is more than 1 DNS query, list all the unique IPs in the DNS responses.

A: The IP address returned by DNS is 128.205.159.13.



Q21: What are the IP addresses returned by DNS when the source requests a DNS lookup for s.youtube.com? If there is more than 1 DNS query, list all the unique IPs in the DNS responses.

A: The IP addresses returned by DNS are 74.125.226.224-74.125.226.233 and 74.125.226.238.



No.	Time	Source	Destination	Protocol	Length	Info
68	1.003457	128.205.39.99	128.205.32.8	DNS	73	Standard query 0x6407 A s.youtube.com
69	1.004178	128.205.32.8	128.205.39.99	DNS	420	Standard query response 0x6407 A s.youtube.com CNAME video-stats.l.google.com A 74.125.226.231 A 74.125.2…
70	1.021097	128.205.39.99	128.205.32.8	DNS	75	Standard query 0x34ad AAAA plus.google.com
71	1.021108	128.205.39.99	128.205.32.8	DNS	79	Standard query 0xd416 AAAA accounts.google.com
72	1.021151	128.205.39.99	128.205.32.8	DNS	74	Standard query 0x5859 AAAA www.google.com
73	1.021775	128.205.32.8	128.205.39.99	DNS	268	Standard query response 0xd416 AAAA accounts.google.com CNAME accounts.l.google.com AAAA 2607:f8b0:400d:c…

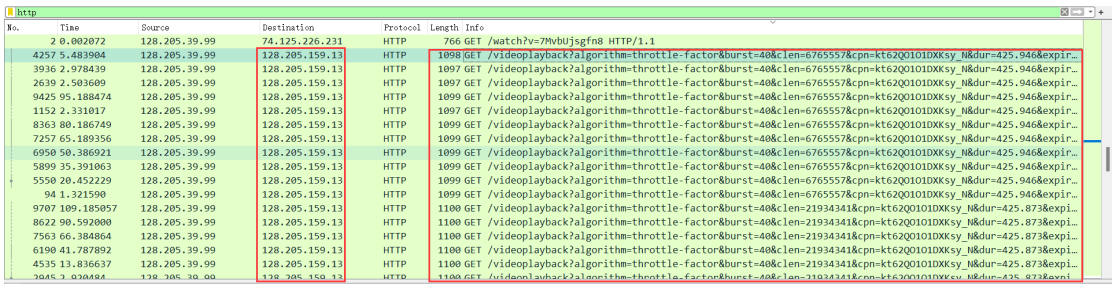
```
Answers
  s.youtube.com: type CNAME, class IN, cname video-stats.l.google.com
  video-stats.l.google.com: type A, class IN, addr 74.125.226.231
  video-stats.l.google.com: type A, class IN, addr 74.125.226.232
  video-stats.l.google.com: type A, class IN, addr 74.125.226.233
  video-stats.l.google.com: type A, class IN, addr 74.125.226.238
  video-stats.l.google.com: type A, class IN, addr 74.125.226.224
  video-stats.l.google.com: type A, class IN, addr 74.125.226.225
  video-stats.l.google.com: type A, class IN, addr 74.125.226.226
  video-stats.l.google.com: type A, class IN, addr 74.125.226.227
  video-stats.l.google.com: type A, class IN, addr 74.125.226.228
  video-stats.l.google.com: type A, class IN, addr 74.125.226.229
  video-stats.l.google.com: type A, class IN, addr 74.125.226.230
```

Q22: Are the IPs in questions (19), (20), and (21) the same or different? How do you explain this?

A: The DNS responses of www.youtube.com and s.youtube.com are the same. But the DNS response of IP addresses returned by DNS when the host requests a DNS lookup for any hostname containing googlevideo.com are different from them. This is because the contents on www.youtube.com and s.youtube.com are on the same servers. Thus, the DNS servers return the same IPs for both domains. However, the contents on googlevideo.com are on another server. Therefore, the DNS response from googlevideo.com is different from the other two.

Q23: Identify the GET request containing "videoplayback". To which IP is this request sent to?

A: This request sent to 128.205.159.13.



No.	Time	Source	Destination	Protocol	Length	Info
2	0.002072	128.205.39.99	74.125.226.231	HTTP	766	GET /watch?v=7MvbUjsgfn8 HTTP/1.1
4257	5.483904	128.205.39.99	128.205.159.13	HTTP	1098	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=6765557&cpn=kt62QO1O1DXKsy_N&dur=425.946&expir…
3936	2.978439	128.205.39.99	128.205.159.13	HTTP	1097	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=6765557&cpn=kt62QO1O1DXKsy_N&dur=425.946&expir…
2639	2.503609	128.205.39.99	128.205.159.13	HTTP	1097	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=6765557&cpn=kt62QO1O1DXKsy_N&dur=425.946&expir…
9425	95.188474	128.205.39.99	128.205.159.13	HTTP	1099	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=6765557&cpn=kt62QO1O1DXKsy_N&dur=425.946&expir…
1152	2.331017	128.205.39.99	128.205.159.13	HTTP	1097	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=6765557&cpn=kt62QO1O1DXKsy_N&dur=425.946&expir…
8363	80.186749	128.205.39.99	128.205.159.13	HTTP	1099	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=6765557&cpn=kt62QO1O1DXKsy_N&dur=425.946&expir…
7257	65.189356	128.205.39.99	128.205.159.13	HTTP	1099	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=6765557&cpn=kt62QO1O1DXKsy_N&dur=425.946&expir…
6950	50.386921	128.205.39.99	128.205.159.13	HTTP	1099	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=6765557&cpn=kt62QO1O1DXKsy_N&dur=425.946&expir…
5899	35.391063	128.205.39.99	128.205.159.13	HTTP	1099	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=6765557&cpn=kt62QO1O1DXKsy_N&dur=425.946&expir…
5550	20.452229	128.205.39.99	128.205.159.13	HTTP	1099	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=6765557&cpn=kt62QO1O1DXKsy_N&dur=425.946&expir…
94	1.321590	128.205.39.99	128.205.159.13	HTTP	1099	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=6765557&cpn=kt62QO1O1DXKsy_N&dur=425.946&expir…
9707	109.185057	128.205.39.99	128.205.159.13	HTTP	1100	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=21934341&cpn=kt62QO1O1DXKsy_N&dur=425.873&expi…
8622	90.592000	128.205.39.99	128.205.159.13	HTTP	1100	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=21934341&cpn=kt62QO1O1DXKsy_N&dur=425.873&expi…
7563	66.384864	128.205.39.99	128.205.159.13	HTTP	1100	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=21934341&cpn=kt62QO1O1DXKsy_N&dur=425.873&expi…
6190	41.787892	128.205.39.99	128.205.159.13	HTTP	1100	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=21934341&cpn=kt62QO1O1DXKsy_N&dur=425.873&expi…
4535	13.836637	128.205.39.99	128.205.159.13	HTTP	1100	GET /videoplayback?algorithm=throttle-factor&burst=40&clen=21934341&cpn=kt62QO1O1DXKsy_N&dur=425.873&expi…

Q24: Check the authoritative nameservers in all the DNS response packets corresponding to DNS queries for any hostname containing youtube.com or googlevideo.com. What do you observe about the order of the nameservers listed in each response? Is it the same or different? Justify your answer.

A: The authoritative nameservers are the same (ns1.google.com to ns4.google.com). However, the order of those authoritative nameservers listed in each response is different. To explain the order of those nameservers, it is because different domains need to use different authoritative nameservers so load balancing can be achieved. If all

domains correspond to the same order of authoritative nameservers, the load on the first nameserver will be too high, and the load on the second name server will be too low.

```
 5 0.023207   128.205.39.99   128.205.32.8    DNS   75 Standard query 0x40a0 A www.youtube.com
 6 0.023950   128.205.32.8    128.205.39.99   DNS  421 Standard query response 0x40a0 A www.youtube.com CNAME youtube-ui.l.google.com A 74.125.226.226 A 74.125.…
 9 0.057870   128.205.39.99   128.205.32.8    DNS   71 Standard query 0xa2eb AAAA s.ytimg.com
10 0.058421   128.205.32.8    128.205.39.99   DNS  267 Standard query response 0xa2eb AAAA s.ytimg.com CNAME ytstatic.l.google.com AAAA 2607:f8b0:4006:801::1000…
11 0.058493   128.205.39.99   128.205.32.8    DNS   71 Standard query 0x3851 A s.ytimg.com
12 0.082457   128.205.32.8    128.205.39.99   DNS  415 Standard query response 0x3851 A s.ytimg.com CNAME ytstatic.l.google.com A 74.125.226.233 A 74.125.226.23…
15 0.261726   128.205.39.99   128.205.32.8    DNS   99 Standard query 0xf628 AAAA r2---sn-c0445avxq0-c04e.googlevideo.com
16 0.285492   128.205.32.8    128.205.39.99   DNS  192 Standard query response 0xf628 AAAA r2---sn-c0445avxq0-c04e.googlevideo.com CNAME r2.sn-c0445avxq0-c04e.g…
17 0.285598   128.205.39.99   128.205.32.8    DNS   99 Standard query 0xce9a A r2---sn-c0445avxq0-c04e.googlevideo.com
18 0.286230   128.205.32.8    128.205.39.99   DNS  294 Standard query response 0xce9a A r2---sn-c0445avxq0-c04e.googlevideo.com CNAME r2.sn-c0445avxq0-c04e.goog…
66 1.000632   128.205.39.99   128.205.32.8    DNS   73 Standard query 0xecbd AAAA s.youtube.com
67 1.001293   128.205.32.8    128.205.39.99   DNS  272 Standard query response 0xecbd AAAA s.youtube.com CNAME video-stats.l.google.com AAAA 2607:f8b0:4006:801:…
68 1.003457   128.205.39.99   128.205.32.8    DNS   73 Standard query 0x6407 A s.youtube.com
69 1.004178   128.205.32.8    128.205.39.99   DNS  420 Standard query response 0x6407 A s.youtube.com CNAME video-stats.l.google.com A 74.125.226.231 A 74.125.2…
70 1.021097   128.205.39.99   128.205.32.8    DNS   75 Standard query 0x34ad AAAA plus.google.com
71 1.021108   128.205.39.99   128.205.32.8    DNS   79 Standard query 0xd416 AAAA accounts.google.com

Authority RRs: 4
Additional RRs: 4
> Queries
> Answers
v Authoritative nameservers
  > google.com: type NS, class IN, ns ns3.google.com
  > google.com: type NS, class IN, ns ns4.google.com
  > google.com: type NS, class IN, ns ns2.google.com
  > google.com: type NS, class IN, ns ns1.google.com
> Additional records
[Request In: 5]
[Time: 0.000743000 seconds]
```

www.youtube.com

```
68 1.003457   128.205.39.99   128.205.32.8    DNS   73 Standard query 0x6407 A s.youtube.com
69 1.004178   128.205.32.8    128.205.39.99   DNS  420 Standard query response 0x6407 A s.youtube.com CNAME video-stats.l.google.com A 74.125.226.231 A 74.125.2…
70 1.021097   128.205.39.99   128.205.32.8    DNS   75 Standard query 0x34ad AAAA plus.google.com
71 1.021108   128.205.39.99   128.205.32.8    DNS   79 Standard query 0xd416 AAAA accounts.google.com

Additional RRs: 4
> Queries
> Answers
v Authoritative nameservers
  > google.com: type NS, class IN, ns ns4.google.com
  > google.com: type NS, class IN, ns ns2.google.com
  > google.com: type NS, class IN, ns ns1.google.com
  > google.com: type NS, class IN, ns ns3.google.com
> Additional records
[Request In: 68]
[Time: 0.000721000 seconds]
```

s.youtube.com

```
17 0.285598   128.205.39.99   128.205.32.8    DNS   99 Standard query 0xce9a A r2---sn-c0445avxq0-c04e.googlevideo.com
18 0.286230   128.205.32.8    128.205.39.99   DNS  294 Standard query response 0xce9a A r2---sn-c0445avxq0-c04e.googlevideo.com CNAME r2.sn-c0445avxq0-c04e.goog…
66 1.000632   128.205.39.99   128.205.32.8    DNS   73 Standard query 0xecbd AAAA s.youtube.com
67 1.001293   128.205.32.8    128.205.39.99   DNS  272 Standard query response 0xecbd AAAA s.youtube.com CNAME video-stats.l.google.com AAAA 2607:f8b0:4006:801:…
68 1.003457   128.205.39.99   128.205.32.8    DNS   73 Standard query 0x6407 A s.youtube.com
69 1.004178   128.205.32.8    128.205.39.99   DNS  420 Standard query response 0x6407 A s.youtube.com CNAME video-stats.l.google.com A 74.125.226.231 A 74.125.2…
70 1.021097   128.205.39.99   128.205.32.8    DNS   75 Standard query 0x34ad AAAA plus.google.com
71 1.021108   128.205.39.99   128.205.32.8    DNS   79 Standard query 0xd416 AAAA accounts.google.com

Additional RRs: 4
> Queries
> Answers
v Authoritative nameservers
  > googlevideo.com: type NS, class IN, ns ns2.google.com
  > googlevideo.com: type NS, class IN, ns ns4.google.com
  > googlevideo.com: type NS, class IN, ns ns3.google.com
  > googlevideo.com: type NS, class IN, ns ns1.google.com
> Additional records
[Request In: 17]
[Time: 0.000632000 seconds]
```

.googlevideo.com