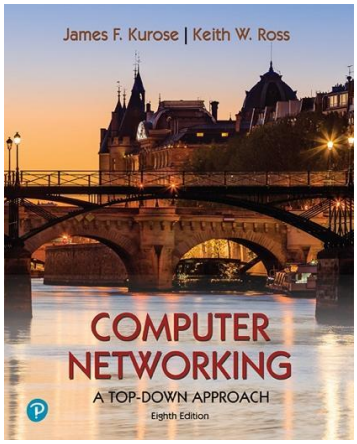
**** Team member: Qiulin Luo, Jiayuan Huang**

Wireshark Lab: DNS v8.1

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.*, J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb



---

0. Academic integrity

We have read and understood the course academic integrity policy.

1. nslookup

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

   103.21.124.10

```
C:\>nslookup www.iitb.ac.in
服务器:  rdns01.anycast.twdx.net
Address:  216.93.240.240

非权威应答:
名称:    www.iitb.ac.in
Address:  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?

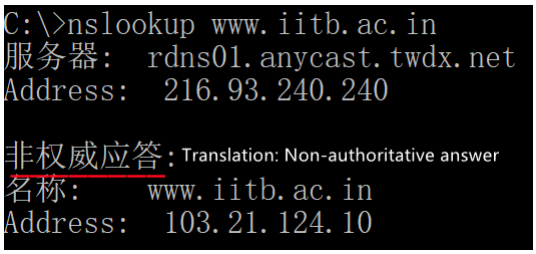
   216.93.240.240

```
C:\>nslookup www.iitb.ac.in
服务器:  rdns01.anycast.twdx.net
Address:  216.93.240.240

非权威应答:
名称:    www.iitb.ac.in
Address:  103.21.124.10
```

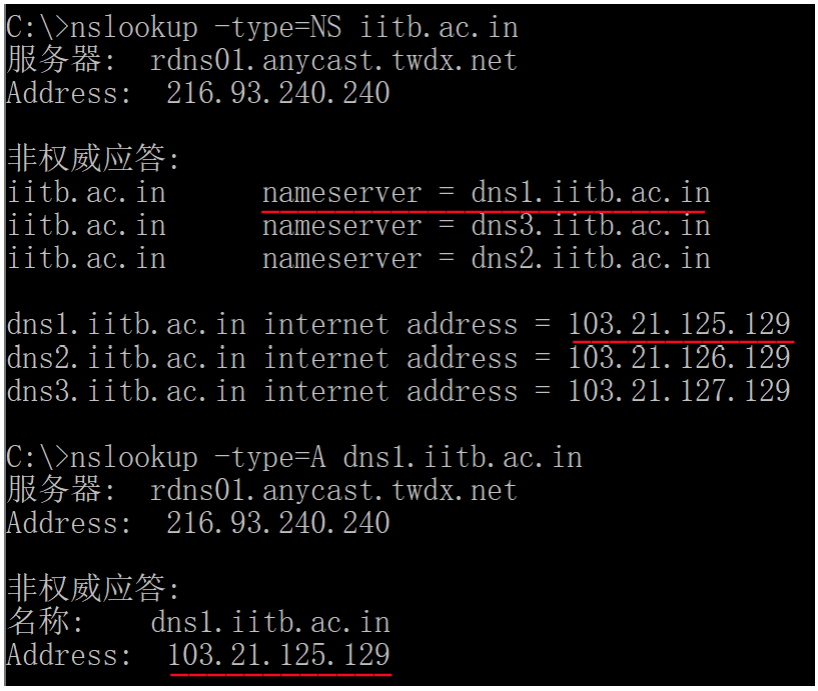
3) Did the answer to your `nslookup` command in question 1 above come from an authoritative or non-authoritative server?

The answer comes from an 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?

dns1.iitb.ac.in



103.21.125.129

2. The DNS cache on your computer

From the description of iterative and recursive DNS query resolution (Figures 2.19 and 2.20) in our textbook, you might think that the local DNS server must be contacted *every* time an application needs to translate from a hostname to an IP address. That's not always true in practice!

Most hosts (e.g., your personal computer) keep a *cache* of recently retrieved DNS records (sometimes called a DNS *resolver cache*), just like many Web browsers keep a cache of objects recently retrieved by HTTP. When DNS services need to be invoked by a host, that host will first check if the DNS record needed is resident in this host's DNS cache; if the record is found, the host will not even bother to contact the local DNS server and will instead use this cached DNS record. A DNS record in a resolver cache will eventually timeout and be removed from the resolver cache, just as records cached in a local DNS server (see Figures 2.19, 2.20) will timeout.

You can also explicitly clear the records in your DNS cache. There's no harm in doing so – it will just mean that your computer will need to invoke the distributed DNS service next time it needs to use the DNS name resolution service, since it will find no records in the cache. On a Mac computer, you can enter the following command into a terminal window to clear your DNS resolver cache:

```
sudo killall -HUP mDNSResponder
```

On Windows computer you can enter the following command at the command prompt:

```
ipconfig /flushdns
```

and on a Linux computer, enter:

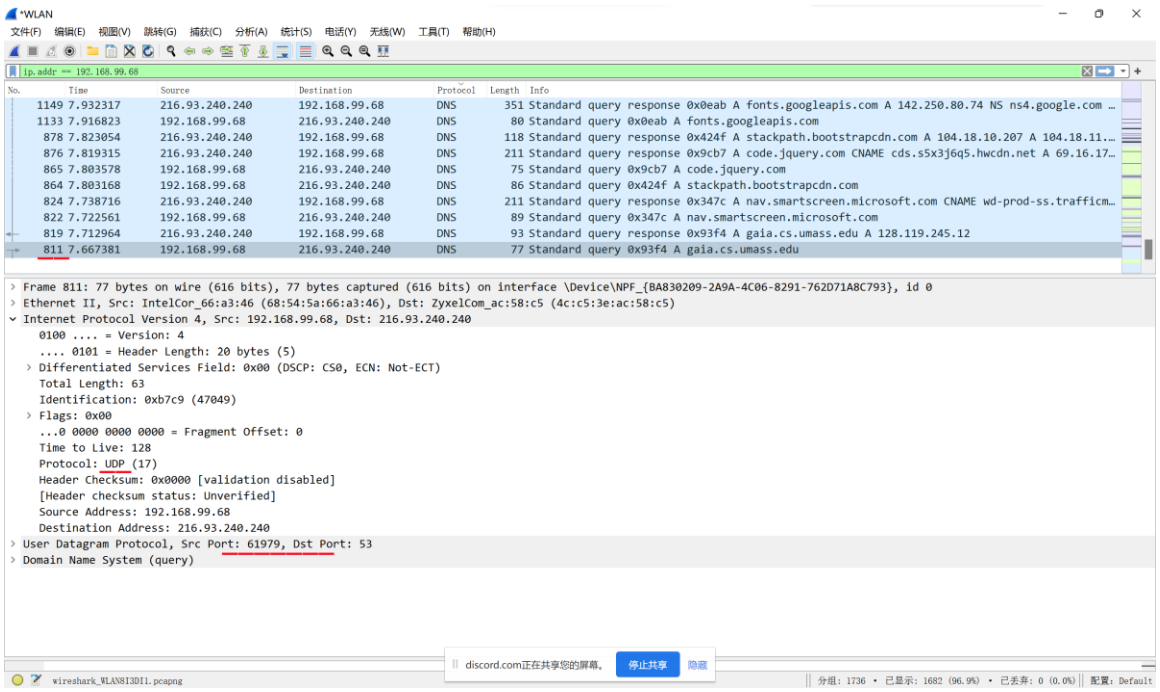
```
sudo systemd-resolve --flush-caches
```

3. Tracing DNS with Wireshark

5) Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number[1] in the trace for the DNS query message? Is this query message sent over UDP or TCP?

   The packet number is 811.

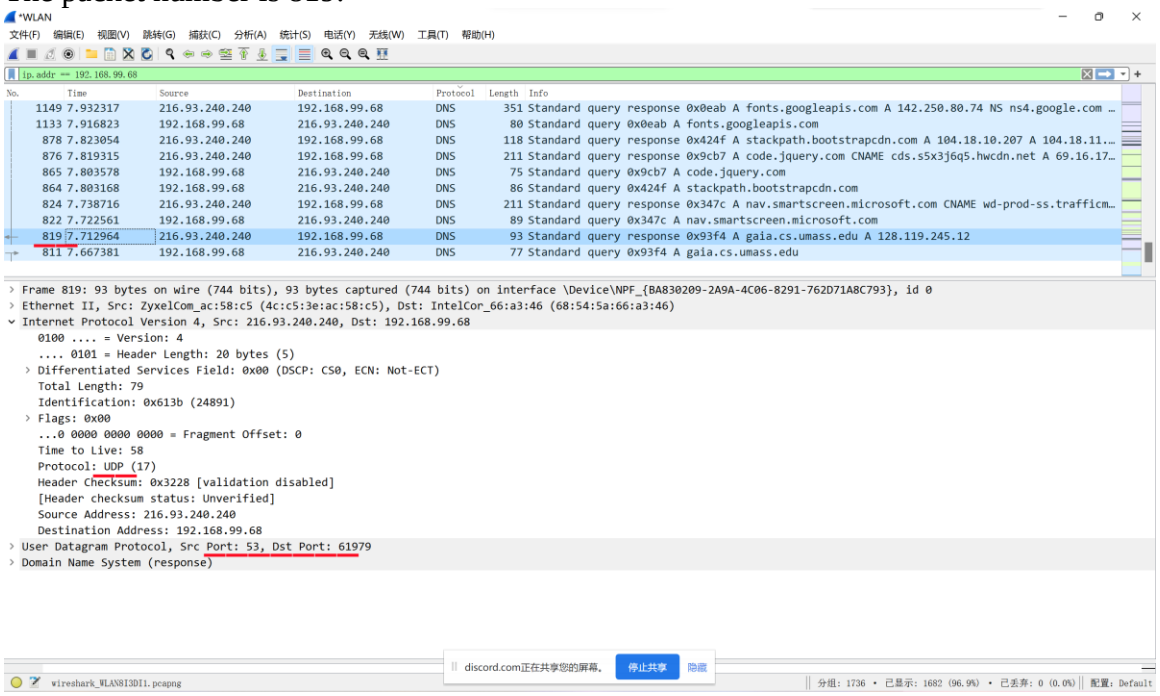
[1] Remember that this "packet number" is assigned by Wireshark for listing purposes only; it is NOT a packet number contained in any real packet header.



This query message was sent over 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?

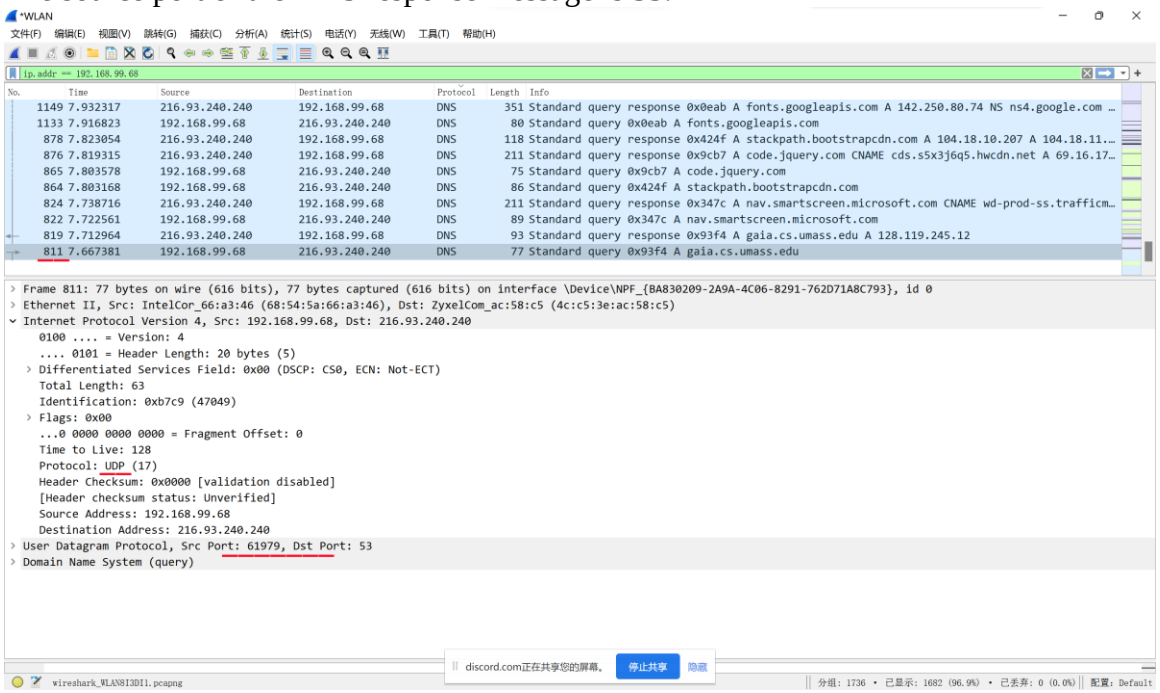
The packet number is 819.

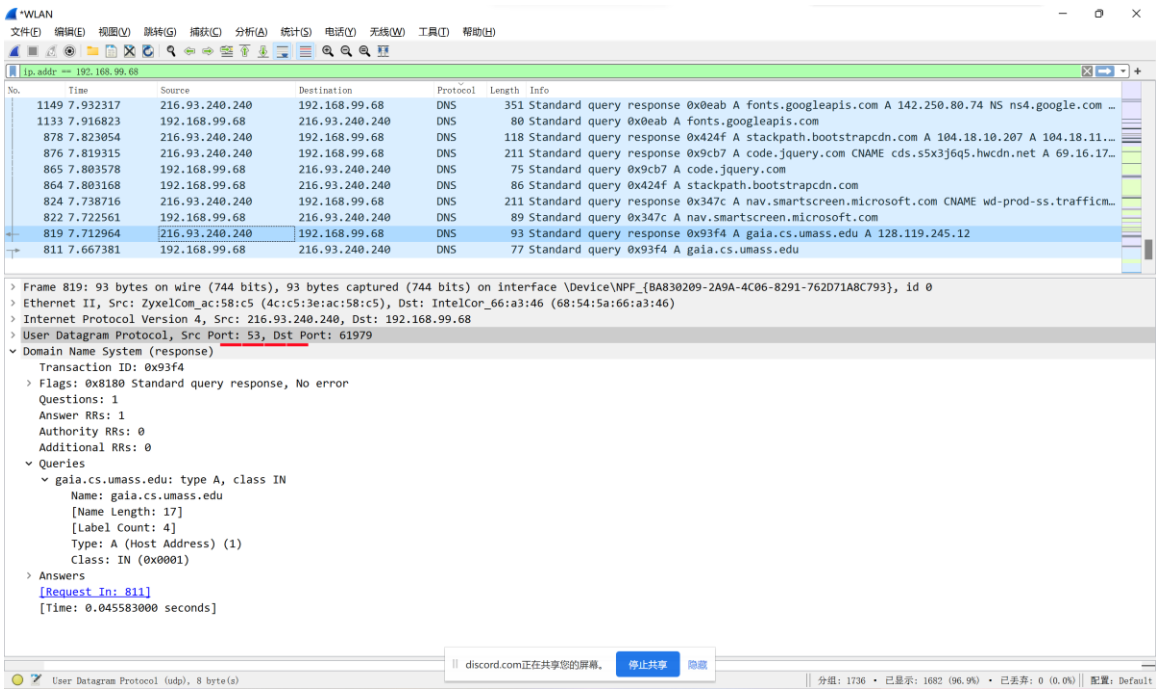


This response message was received via UDP.

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

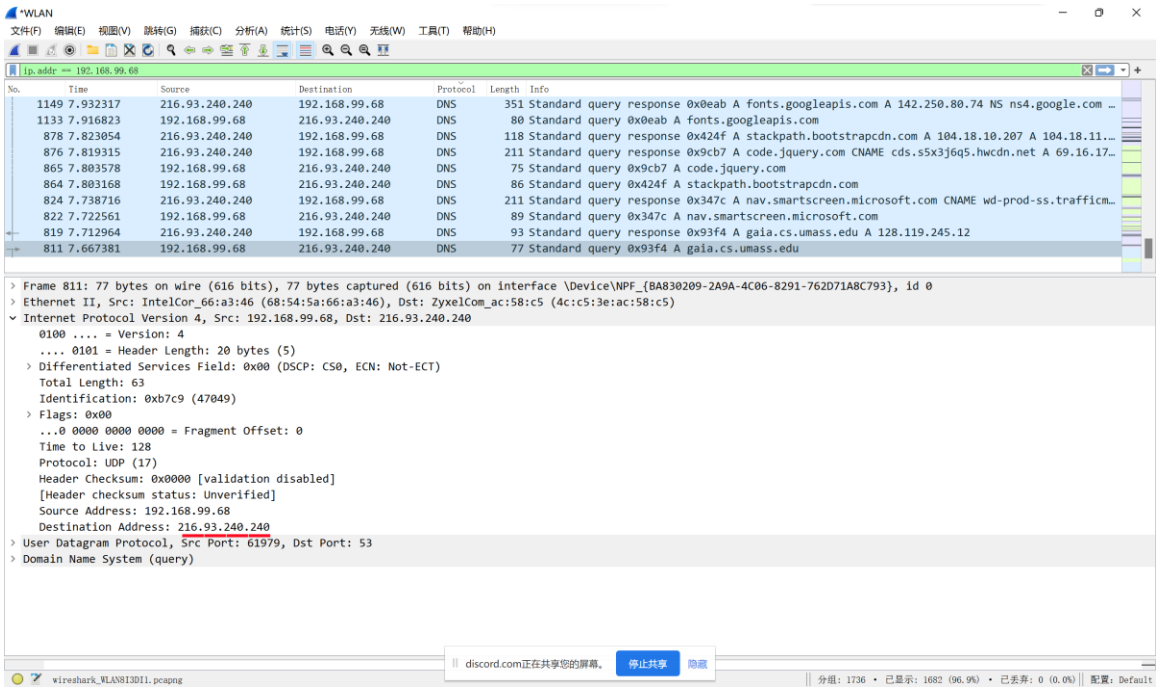
The destination port for the DNS query message is 53.
The source port of the DNS response message is 53.





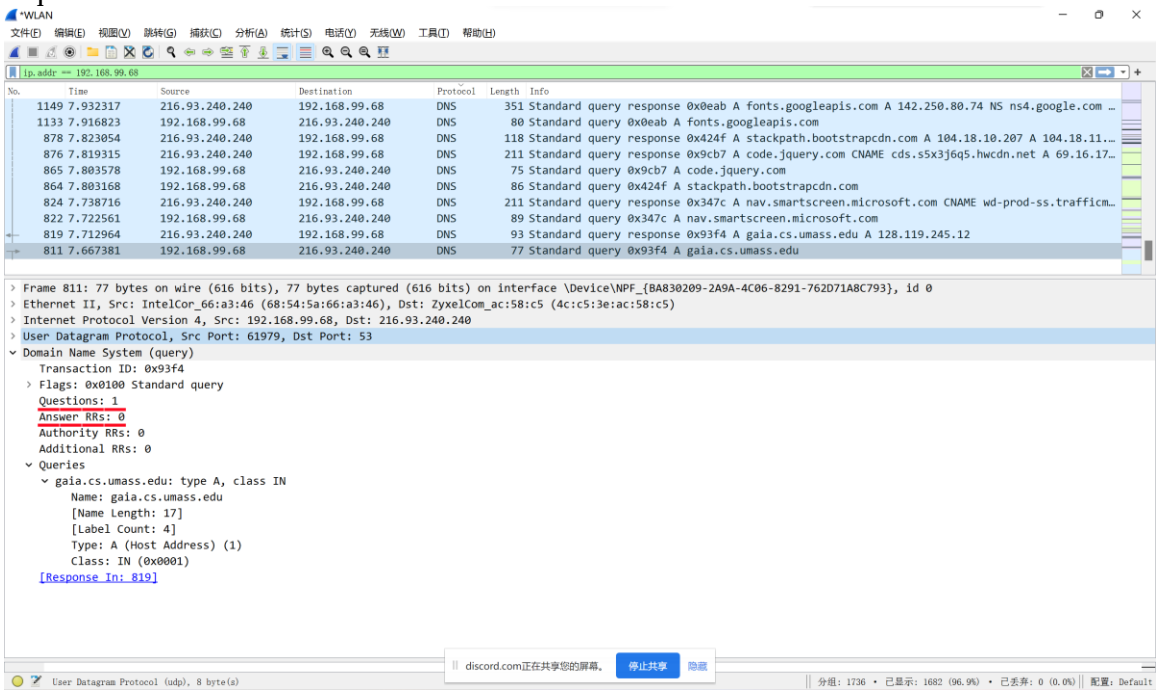
8) To what IP address is the DNS query message sent?

216.93.240.240



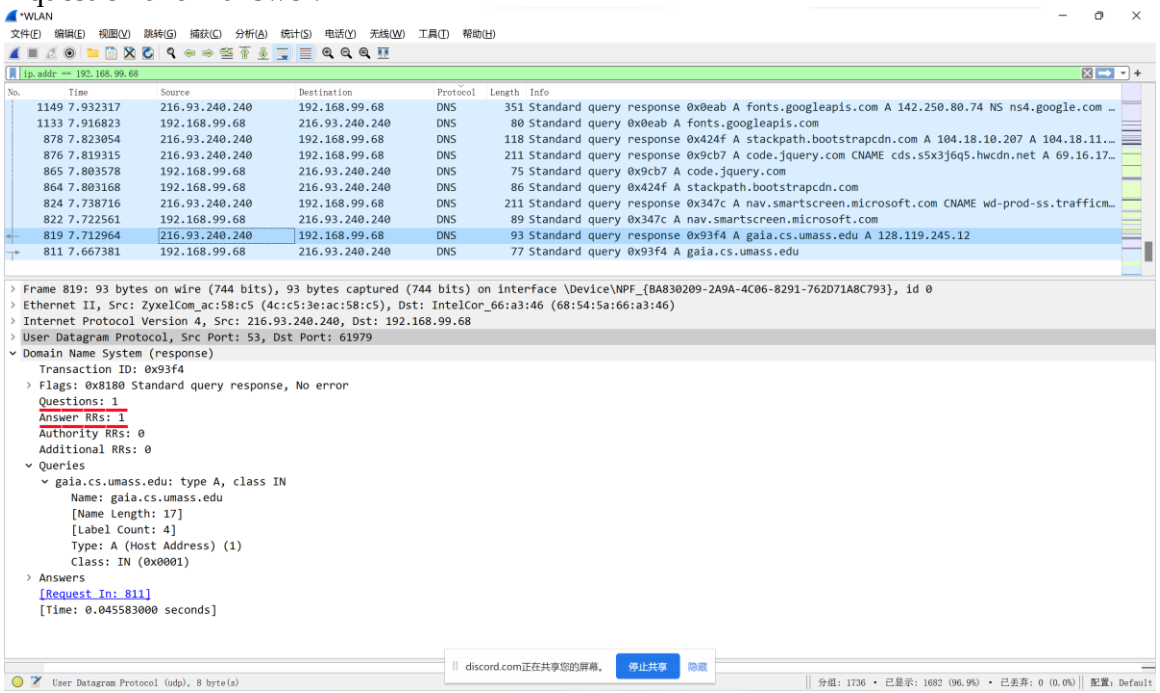
9) Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

1 question and 0 answer.



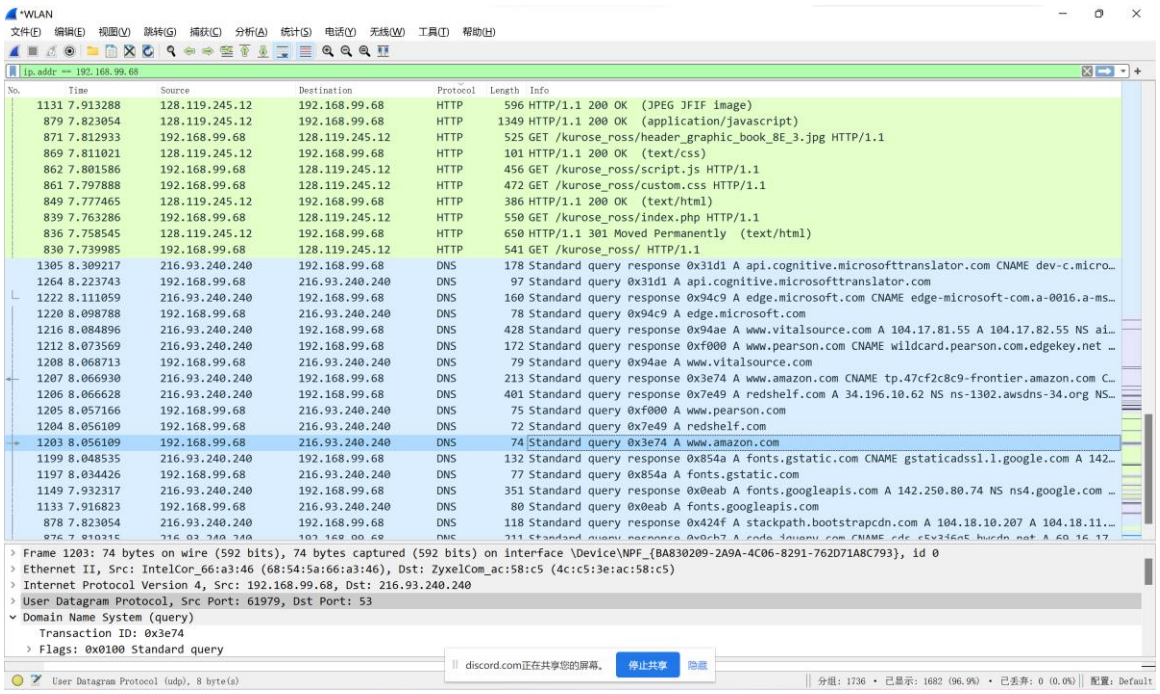
10) Examine the DNS response message to the initial query message. How many "questions" does this DNS message contain? How many "answers" answers does it contain?

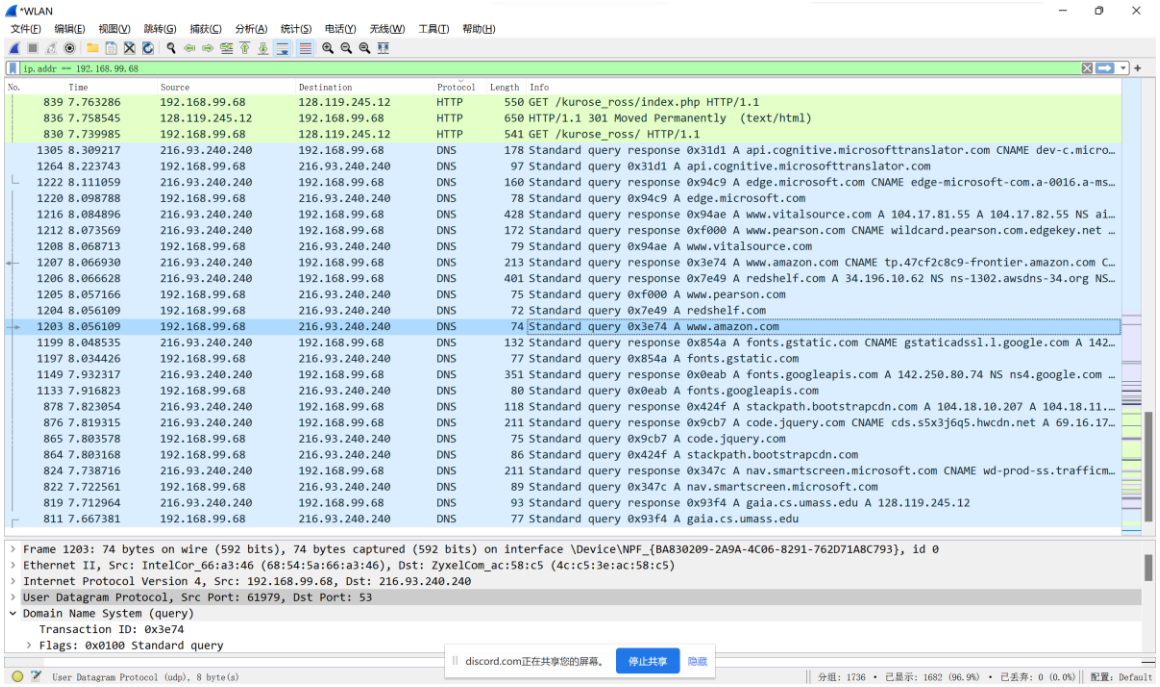
1 question and 1 answer.



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

No, we didn't see any new DNS queries.

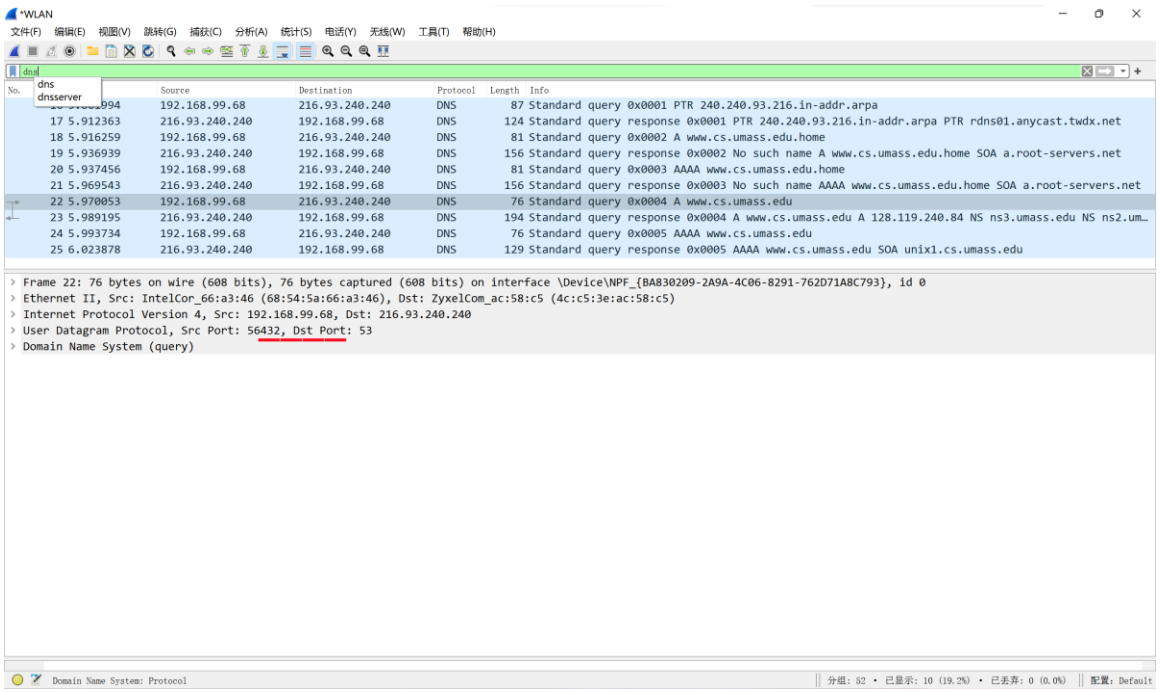


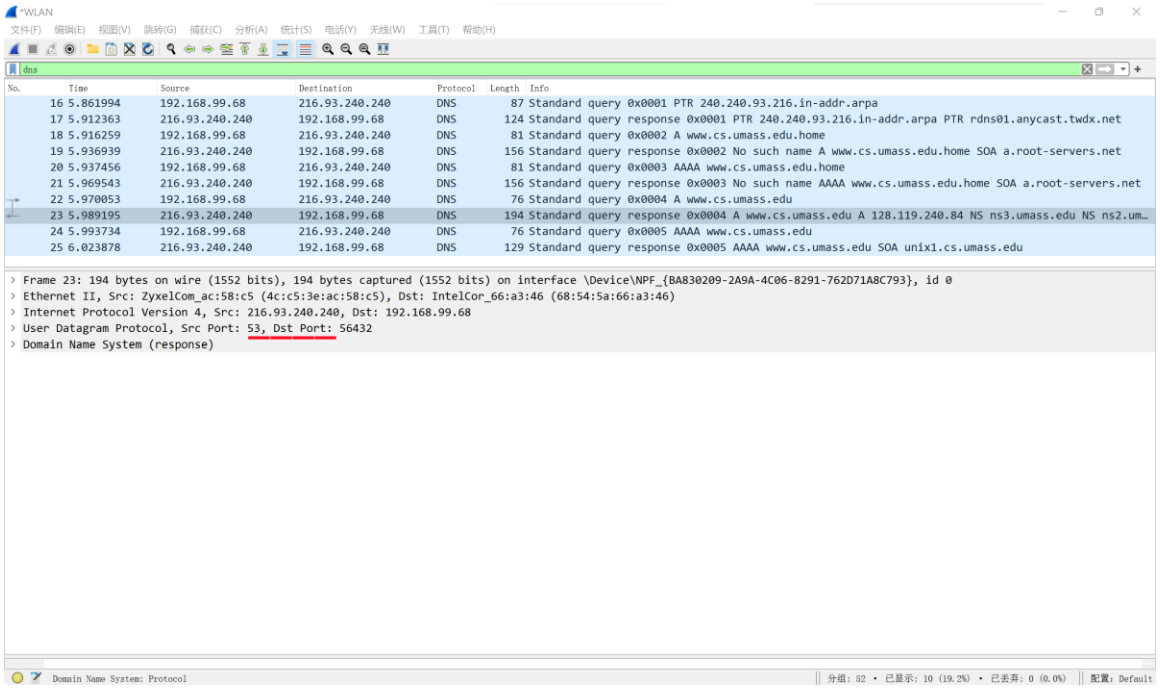


12) What is the destination port for the DNS query message? What is the source port of the DNS response message?

The destination port for the DNS query message is 53.

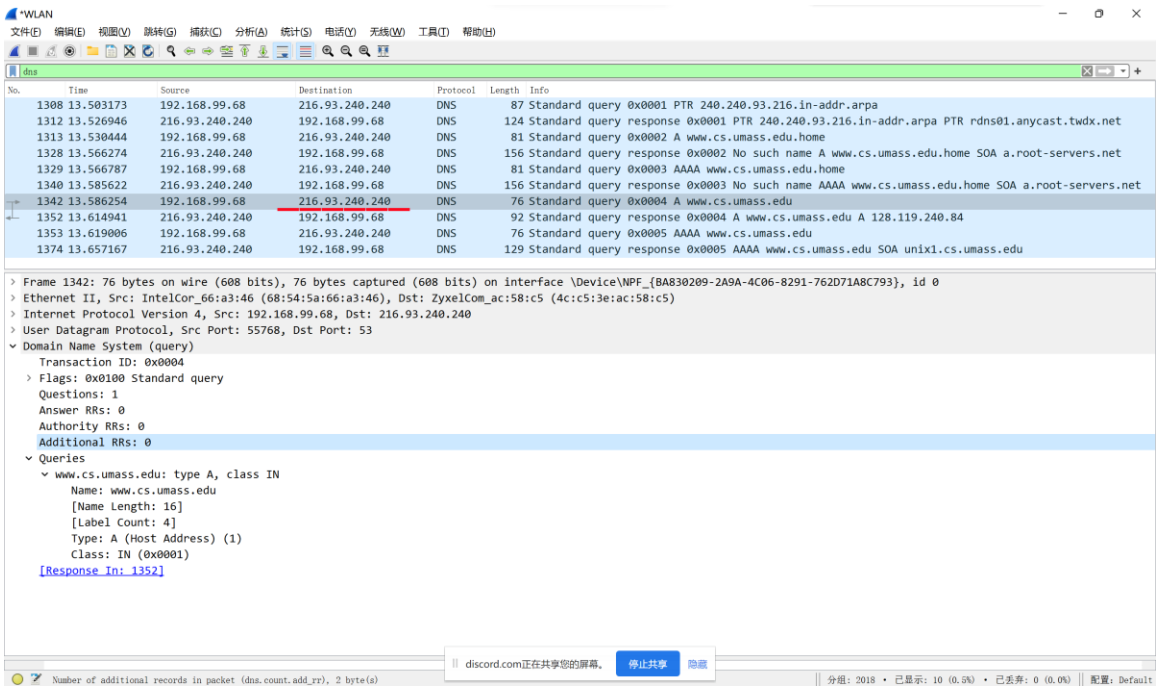
The source port of the DNS response message is 53.





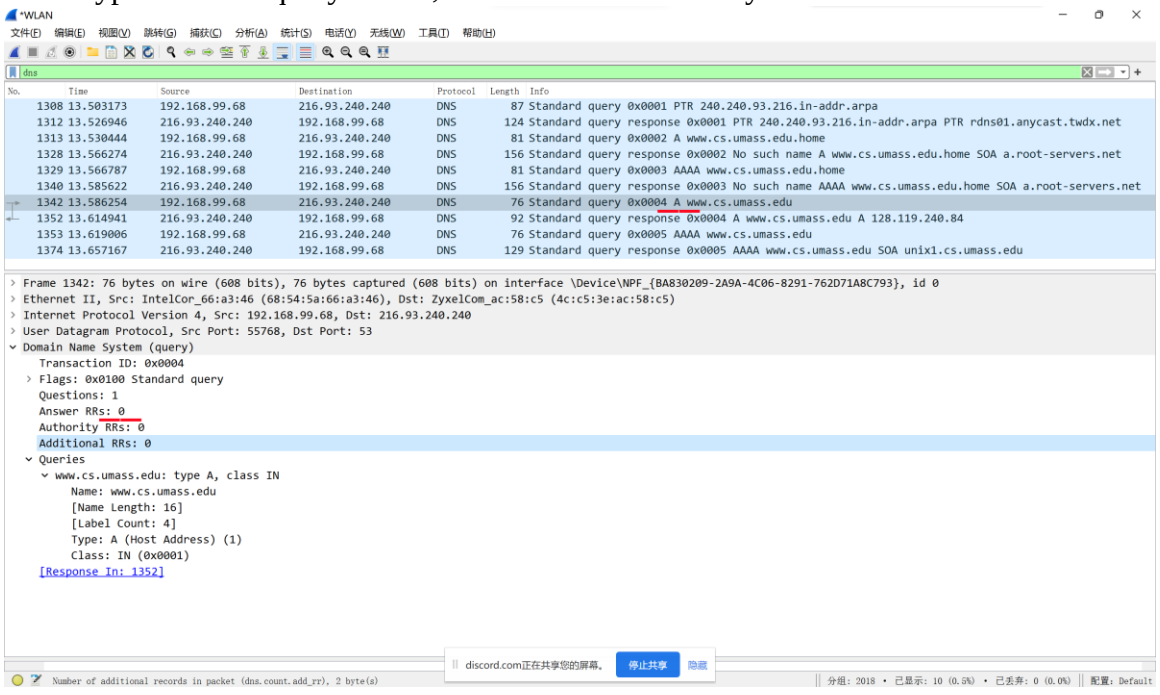
13) To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

216.93.240.240, and this IP address is the same as the default local DNS server.



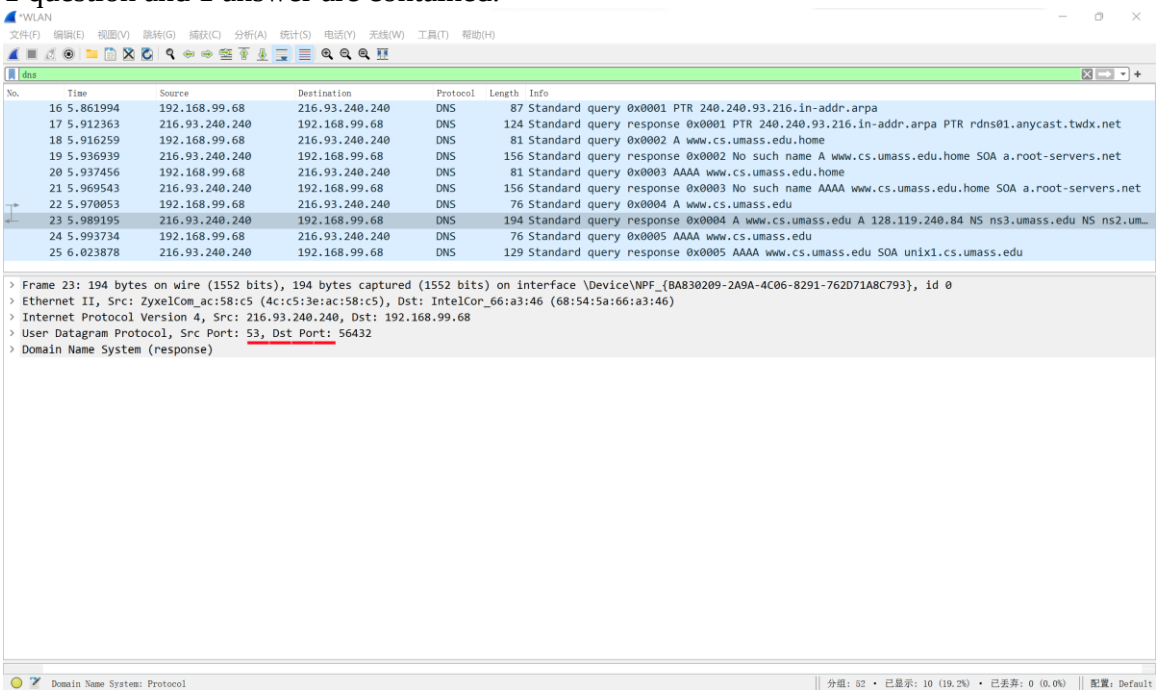
14) Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The “Type” of DNS query is “A”, and it didn’t contain any “answers”.



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

1 question and 1 answer are contained.



Last, let's use `nslookup` to issue a command that will return a type NS DNS record, Enter the following command:

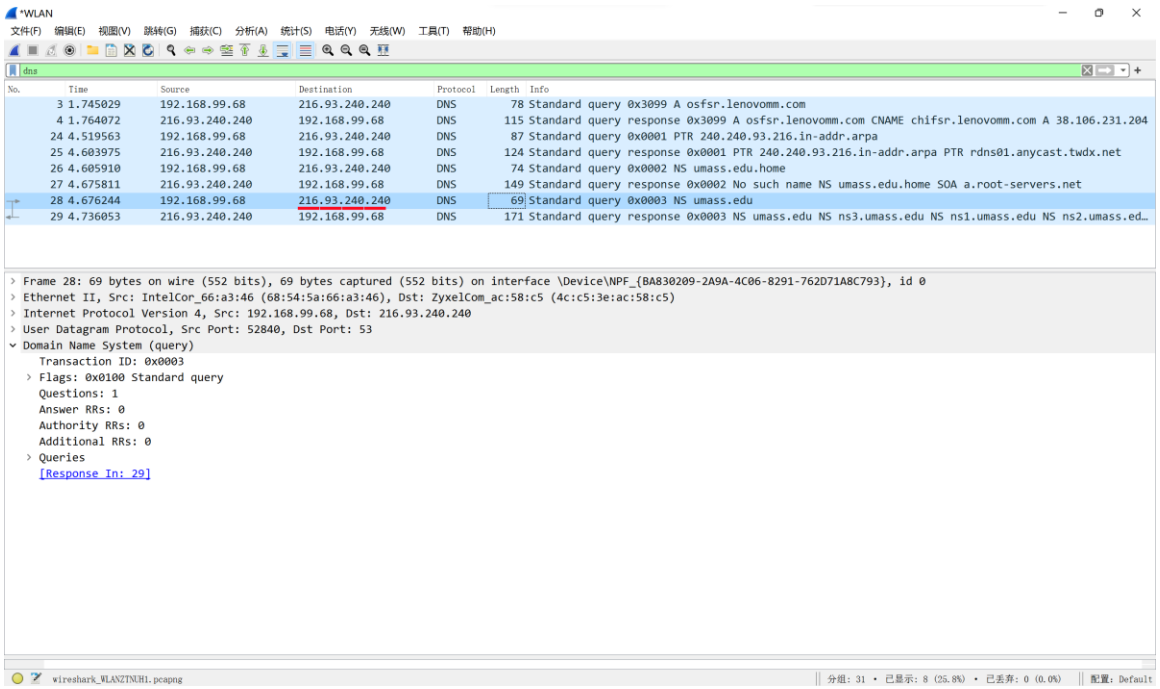
`nslookup -type=NS umass.edu`

and then answer the following questions[2] :

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

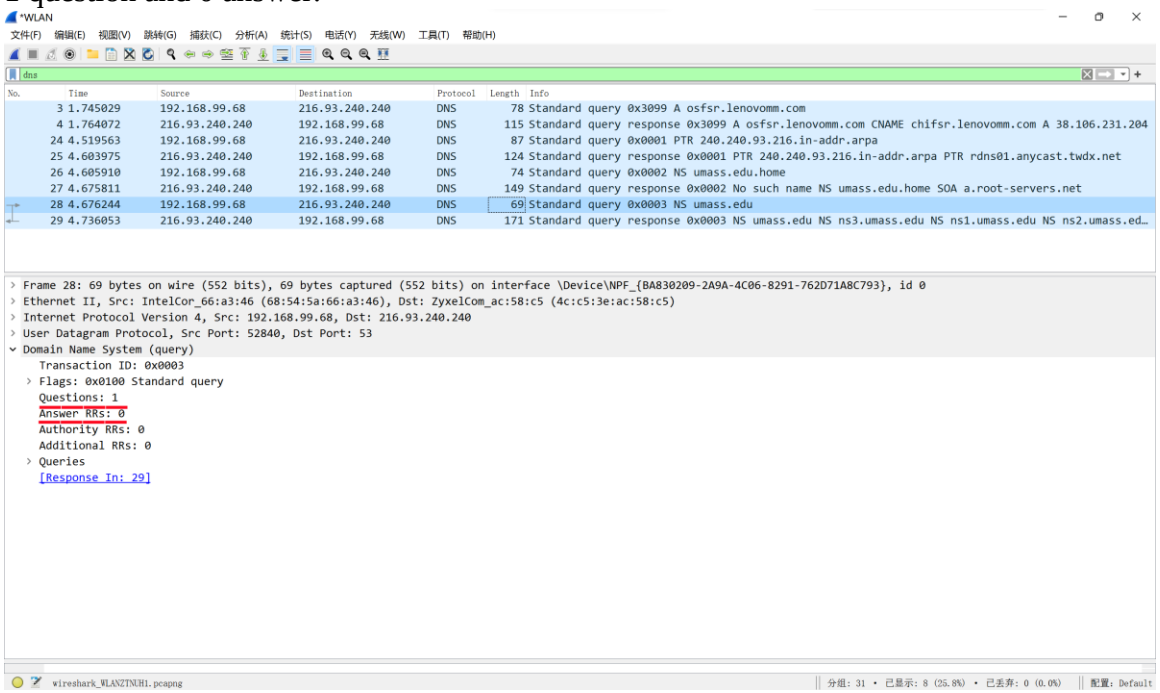
    216.93.240.240, and this IP address is the same as the default local DNS server.

[2] If you are unable to run Wireshark and capture a trace file, or are using an LMS, use the trace file *dns-wireshark-trace-3* in the zip file of traces in the footnote above to answer questions 17-19 below.



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

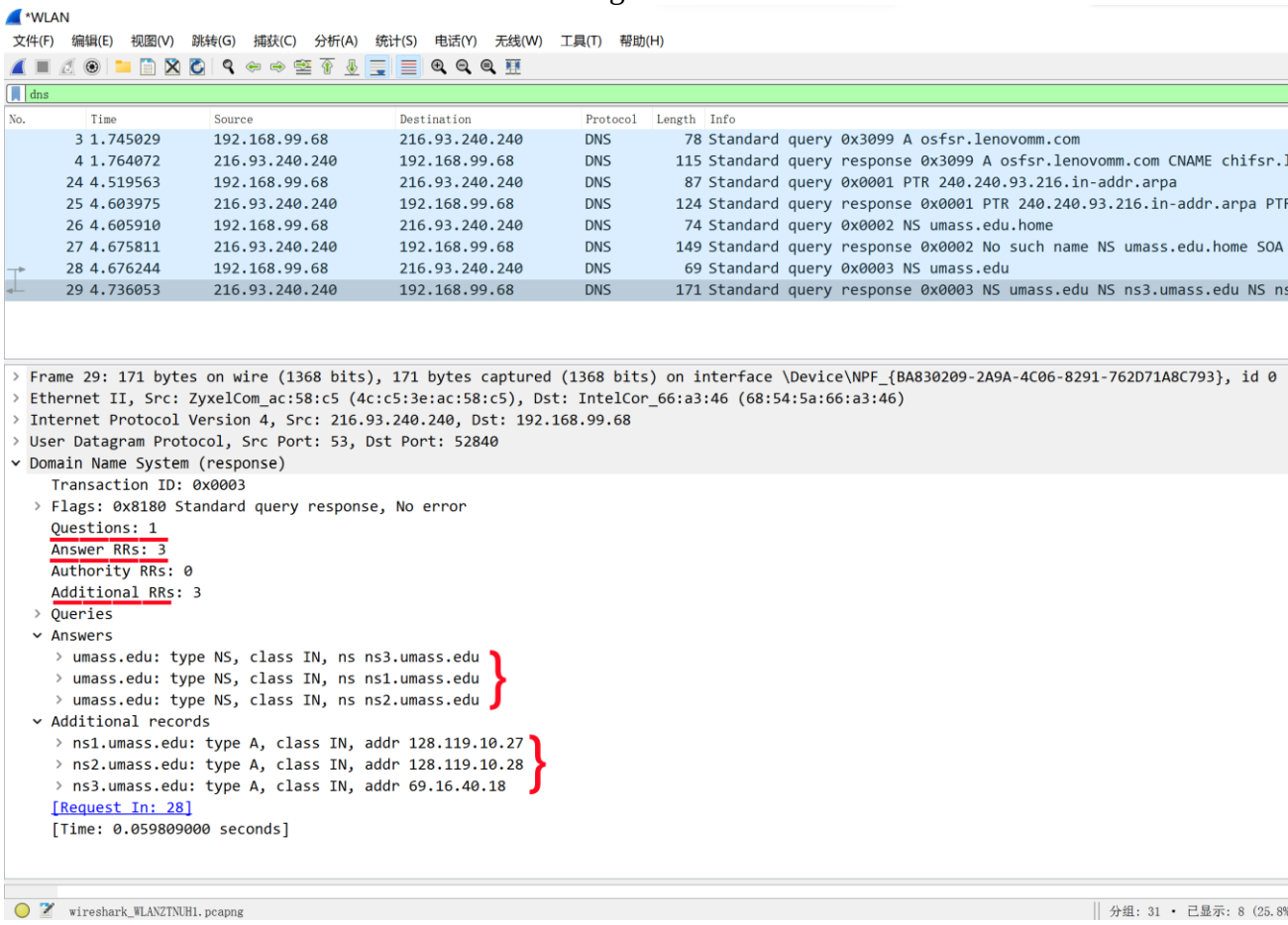
1 question and 0 answer.



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?

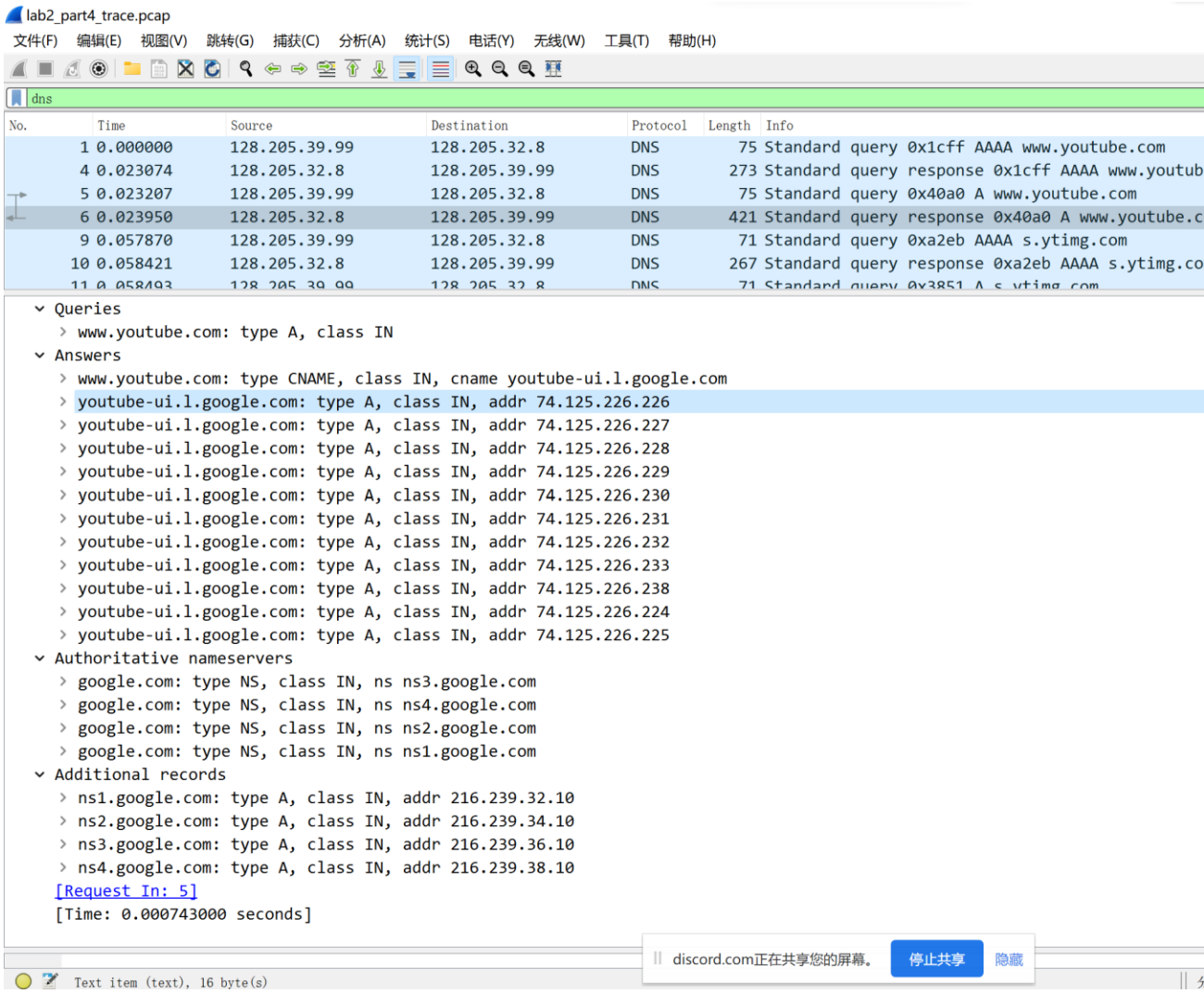
3 answers and 3 additional resource records.
The information is shown in brackets on the diagram below.



4. Content Distribution Networks, Caching, and DNS

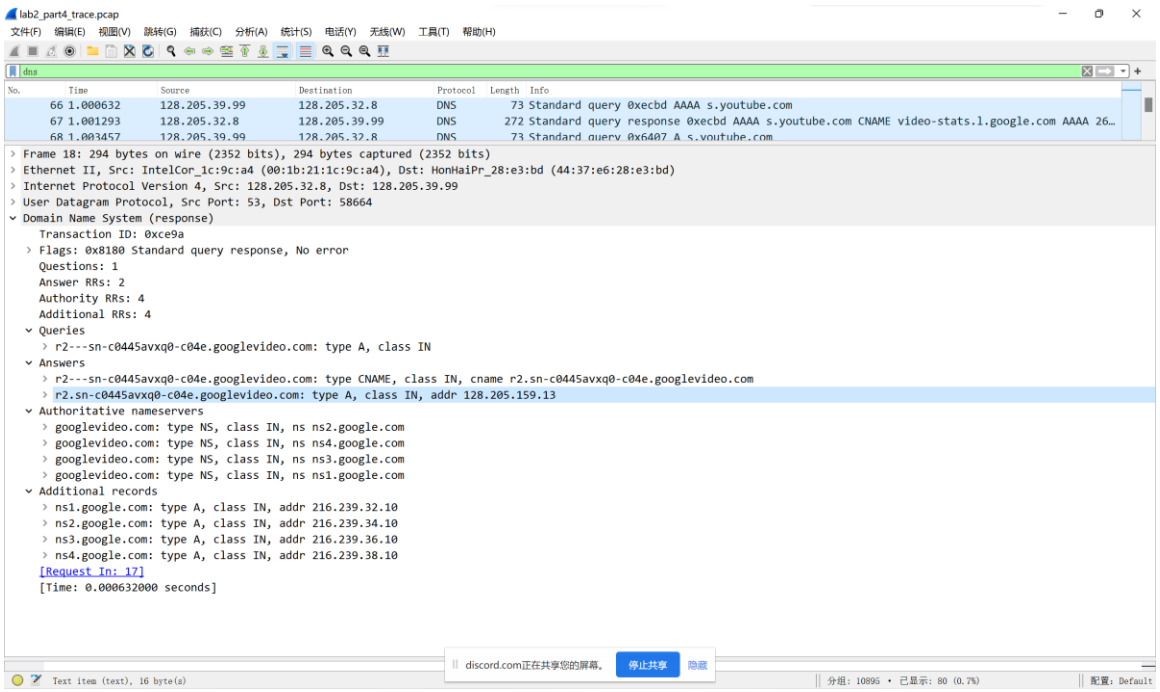
19) What are the IP addresses returned by DNS when the host requests a DNS lookup for www.youtube.com? If there is more than one DNS query, list all the unique IPs in the DNS responses.

As follows in graph: 74.125.226.2xx



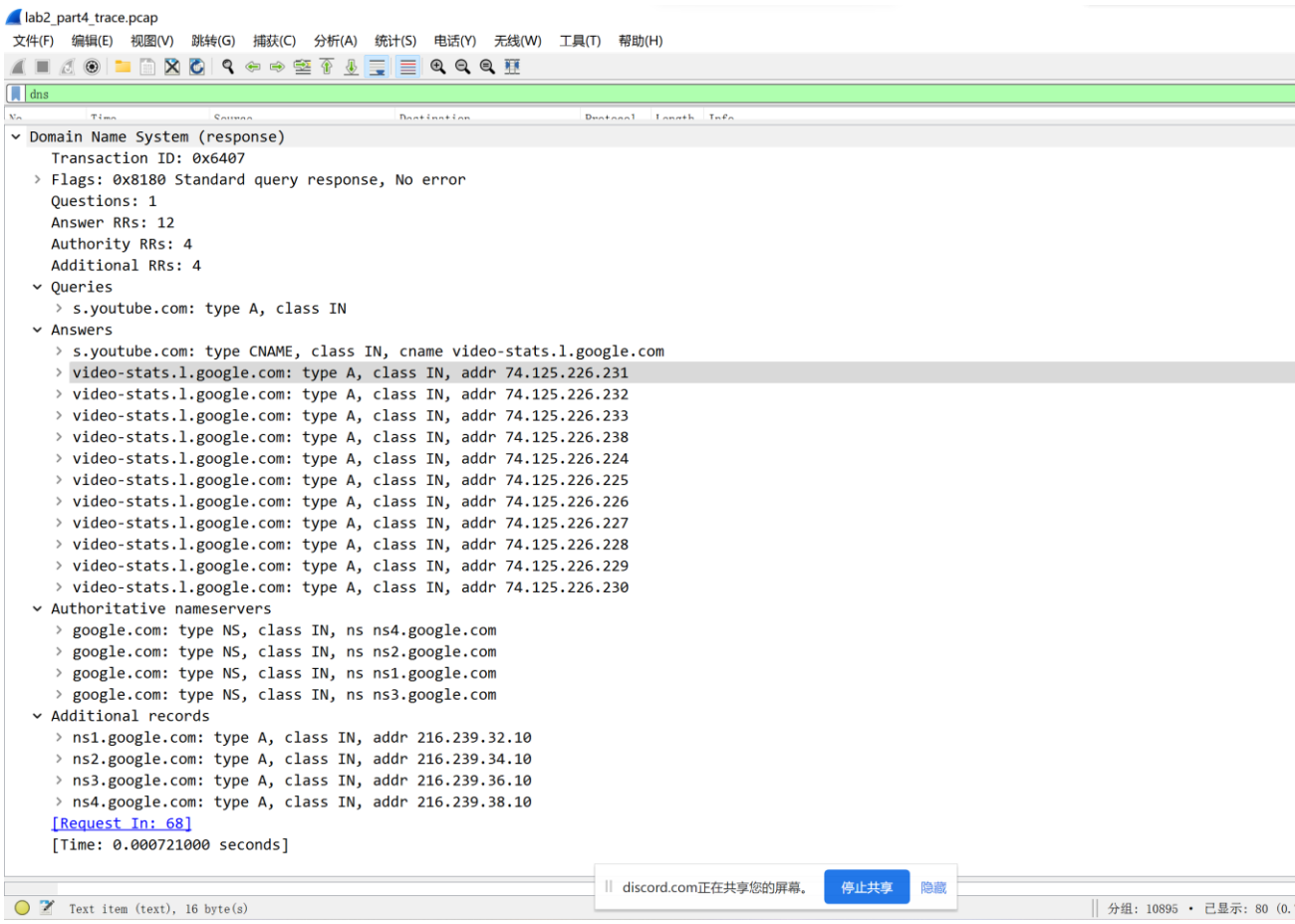
20) What are the IP addresses returned by DNS when the host requests a DNS lookup for any hostname containing googlevideo.com? If there is more than 1 DNS query, list all the unique IPs in the DNS responses.

As follows in graph: 128.205.259.13



21) 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.

As follows in graph: 74.125.226.2xx



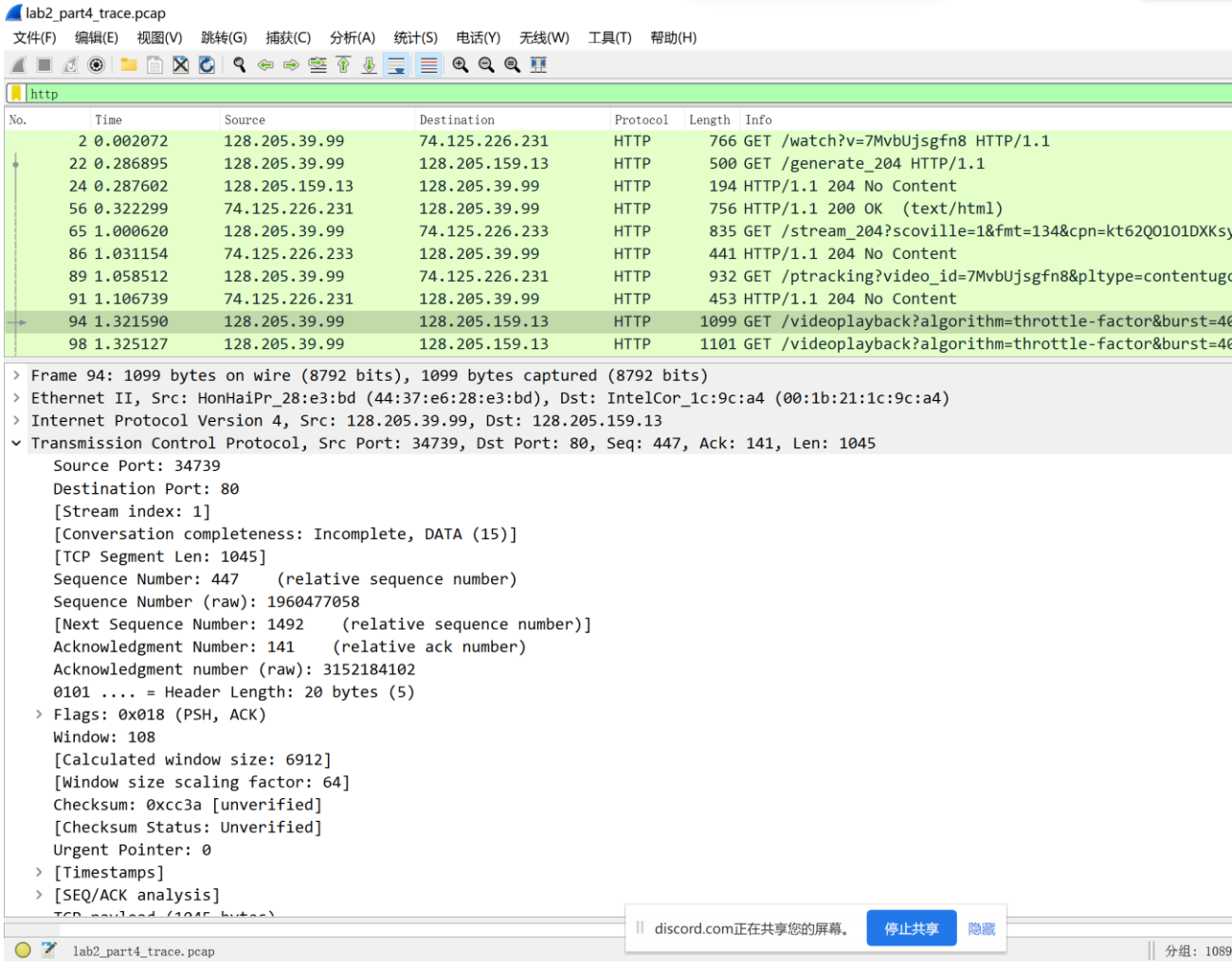
22) Are the IPs in questions (19), (20), and (21) the same or different? How do you explain this?

19 and 21 is the same but 20 is different, since 19 and 21 all access youtube.com domain name, and 20 access googlevideo.com.
For 19 and 21, they are all have type CNAME alias for the domain name xxx.l.google.com and thus they should have the same IP address.

```
273 Standard query response 0x1cff AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA 260
 75 Standard query 0x40a0 A www.youtube.com
421 Standard query response 0x40a0 A www.youtube.com CNAME youtube-ui.l.google.com A 74.125.22
 71 Standard query 0xa2eb AAAA s.ytimg.com
267 Standard query response 0xa2eb AAAA s.ytimg.com CNAME ytstatic.l.google.com AAAA 2607:f8b0
 71 Standard query 0x3851 A s.ytimg.com
415 Standard query response 0x3851 A s.ytimg.com CNAME ytstatic.l.google.com A 74.125.226.233
 99 Standard query 0xf628 AAAA r2---sn-c0445avxq0-c04e.googlevideo.com
192 Standard query response 0xf628 AAAA r2---sn-c0445avxq0-c04e.googlevideo.com CNAME r2.sn-c0
 99 Standard query 0xce9a A r2---sn-c0445avxq0-c04e.googlevideo.com
294 Standard query response 0xce9a A r2---sn-c0445avxq0-c04e.googlevideo.com CNAME r2.sn-c0445
 73 Standard query 0xecbd AAAA s.youtube.com
272 Standard query response 0xecbd AAAA s.youtube.com CNAME video-stats.l.google.com AAAA 2607
 73 Standard query 0x6407 A s.youtube.com
420 Standard query response 0x6407 A s.youtube.com CNAME video-stats.l.google.com A 74.125.226
 75 Standard query 0x34ad AAAA plus.google.com
```

23) Identify the GET request containing “videoplayback”. To which IP is this request sent to?

128.205.159.13



24) 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.

It is very randomized in order with the same content, Our guess is that either it is randomized or listed in the order of loadedness to best use the four server without overloading one of them.