Lab Report

CSExxx, Course Name

Name: Mohamed Mohsen Mostafa ID: 22P0147
Kamel Mansour Zaima

Lab No: (3) Experiment Title:

Date: 30 / 10 /2025

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

103.21.124.133

```
C:\Users\moham>nslookup www.iitb.ac.in
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
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?

192.168.0.1

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

Non-authoritative answer

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?

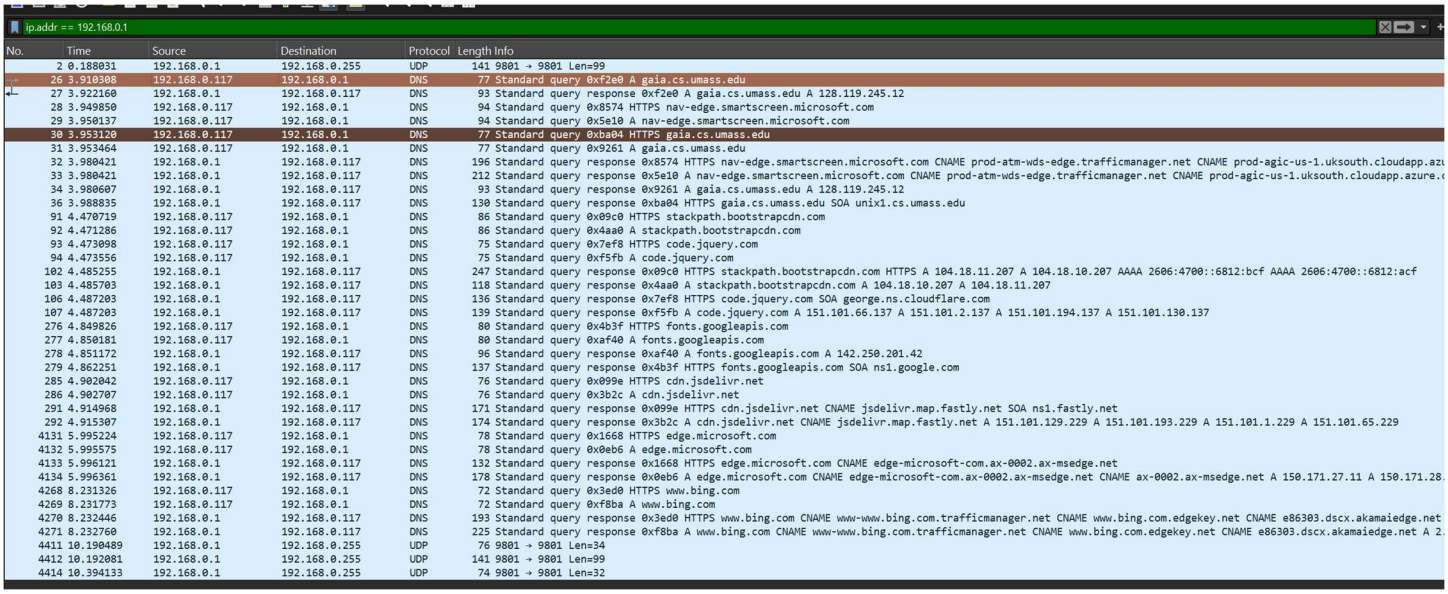
No authoritative answers

```
C:\Users\moham>nslookup -type=NS iitb.ac.in
Server:  UnKnown
Address:  192.168.0.1

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
```

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?

Packet no. 26, sent over UDP



ip.addr == 192.168.0.1

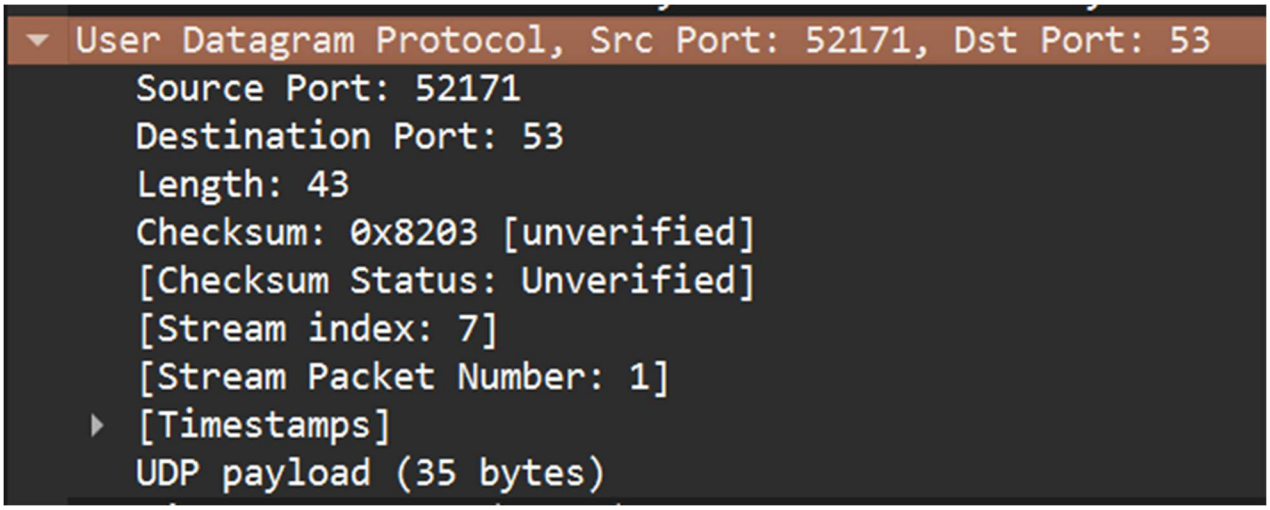
No.	Time	Source	Destination	Protocol	Length	Info
2	0.188031	192.168.0.1	192.168.0.255	UDP	141	9801 → 9801 Len=99
26	3.910308	192.168.0.117	192.168.0.1	DNS	77	Standard query 0xf2e0 A gaia.cs.umass.edu
27	3.922160	192.168.0.1	192.168.0.117	DNS	93	Standard query response 0xf2e0 A gaia.cs.umass.edu A 128.119.245.12
28	3.949850	192.168.0.117	192.168.0.1	DNS	94	Standard query 0x8574 HTTPS nav-edge.smartscreen.microsoft.com
29	3.950137	192.168.0.117	192.168.0.1	DNS	94	Standard query 0x5e10 A nav-edge.smartscreen.microsoft.com
30	3.953120	192.168.0.117	192.168.0.1	DNS	77	Standard query 0xba04 HTTPS gaia.cs.umass.edu
31	3.953464	192.168.0.117	192.168.0.1	DNS	77	Standard query 0x9261 A gaia.cs.umass.edu
32	3.980421	192.168.0.1	192.168.0.117	DNS	196	Standard query response 0x8574 HTTPS nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME prod-agic-us-1.uksouth.cloudapp.azu
33	3.980421	192.168.0.1	192.168.0.117	DNS	212	Standard query response 0x5e10 A nav-edge.smartscreen.microsoft.com CNAME prod-atm-wds-edge.trafficmanager.net CNAME prod-agic-us-1.uksouth.cloudapp.azure.c
34	3.980607	192.168.0.1	192.168.0.117	DNS	93	Standard query response 0x9261 A gaia.cs.umass.edu A 128.119.245.12
36	3.988835	192.168.0.1	192.168.0.117	DNS	130	Standard query response 0xba04 HTTPS gaia.cs.umass.edu SOA unix1.cs.umass.edu
91	4.470719	192.168.0.117	192.168.0.1	DNS	86	Standard query 0x09c0 HTTPS stackpath.bootstrapcdn.com
92	4.471286	192.168.0.117	192.168.0.1	DNS	86	Standard query 0x4aa0 A stackpath.bootstrapcdn.com
93	4.473098	192.168.0.117	192.168.0.1	DNS	75	Standard query 0x7ef8 HTTPS code.jquery.com
94	4.473556	192.168.0.117	192.168.0.1	DNS	75	Standard query 0xf5fb A code.jquery.com
102	4.485255	192.168.0.1	192.168.0.117	DNS	247	Standard query response 0x09c0 HTTPS stackpath.bootstrapcdn.com HTTPS A 104.18.11.207 A 104.18.10.207 AAAA 2606:4700::6812:bcf AAAA 2606:4700::6812:acf
103	4.485703	192.168.0.1	192.168.0.117	DNS	118	Standard query response 0x4aa0 A stackpath.bootstrapcdn.com A 104.18.10.207 A 104.18.11.207
106	4.487203	192.168.0.1	192.168.0.117	DNS	136	Standard query response 0x7ef8 HTTPS code.jquery.com SOA george.ns.cloudflare.com
107	4.487203	192.168.0.1	192.168.0.117	DNS	139	Standard query response 0xf5fb A code.jquery.com A 151.101.66.137 A 151.101.2.137 A 151.101.194.137 A 151.101.130.137
276	4.849826	192.168.0.117	192.168.0.1	DNS	80	Standard query 0x4b3f HTTPS fonts.googleapis.com
277	4.850181	192.168.0.117	192.168.0.1	DNS	80	Standard query 0xaf40 A fonts.googleapis.com
278	4.851172	192.168.0.1	192.168.0.117	DNS	96	Standard query response 0xaf40 A fonts.googleapis.com A 142.250.201.42
279	4.862251	192.168.0.1	192.168.0.117	DNS	137	Standard query response 0x4b3f HTTPS fonts.googleapis.com SOA ns1.google.com
285	4.902042	192.168.0.117	192.168.0.1	DNS	76	Standard query 0x099e HTTPS cdn.jsdelivr.net
286	4.902707	192.168.0.117	192.168.0.1	DNS	76	Standard query 0x3b2c A cdn.jsdelivr.net
291	4.914968	192.168.0.1	192.168.0.117	DNS	171	Standard query response 0x099e HTTPS cdn.jsdelivr.net CNAME jsdelivr.map.fastly.net SOA ns1.fastly.net
292	4.915307	192.168.0.1	192.168.0.117	DNS	174	Standard query response 0x3b2c A cdn.jsdelivr.net CNAME jsdelivr.map.fastly.net A 151.101.129.229 A 151.101.193.229 A 151.101.1.229 A 151.101.65.229
4131	5.995224	192.168.0.117	192.168.0.1	DNS	78	Standard query 0x1668 HTTPS edge.microsoft.com
4132	5.995575	192.168.0.117	192.168.0.1	DNS	78	Standard query 0x0eb6 A edge.microsoft.com
4133	5.996121	192.168.0.1	192.168.0.117	DNS	132	Standard query response 0x1668 HTTPS edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-msedge.net
4134	5.996361	192.168.0.1	192.168.0.117	DNS	178	Standard query response 0x0eb6 A edge.microsoft.com CNAME edge-microsoft-com.ax-0002.ax-msedge.net CNAME ax-0002.ax-msedge.net A 150.171.27.11 A 150.171.28.
4268	8.231326	192.168.0.117	192.168.0.1	DNS	72	Standard query 0x3ed0 HTTPS www.bing.com
4269	8.231773	192.168.0.117	192.168.0.1	DNS	72	Standard query 0xf8ba A www.bing.com
4270	8.232446	192.168.0.1	192.168.0.117	DNS	193	Standard query response 0x3ed0 HTTPS www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e86303.dscx.akamaiedge.net
4271	8.232760	192.168.0.1	192.168.0.117	DNS	225	Standard query response 0xf8ba A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e86303.dscx.akamaiedge.net A 2.
4411	10.190489	192.168.0.1	192.168.0.255	UDP	76	9801 → 9801 Len=34
4412	10.192081	192.168.0.1	192.168.0.255	UDP	141	9801 → 9801 Len=99
4414	10.394133	192.168.0.1	192.168.0.255	UDP	74	9801 → 9801 Len=32

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?

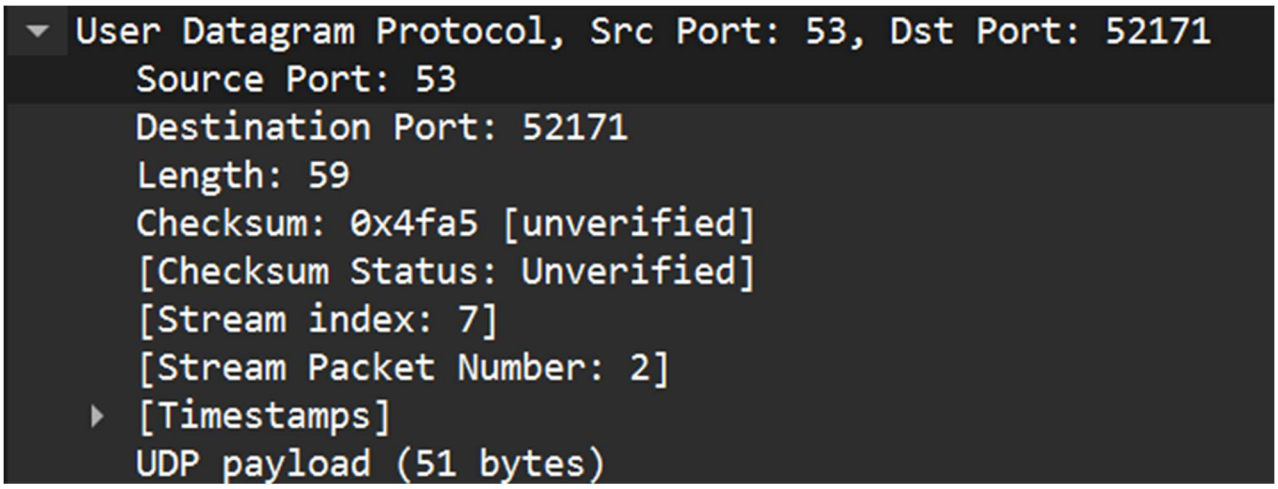
Packet no. 27, sent over UDP

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

Destination in the query message: 53



Source in the response message: 53

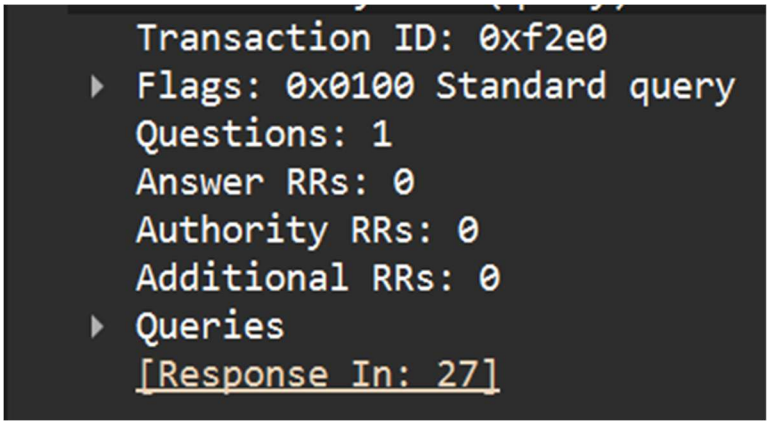


8. To what IP address is the DNS query message sent?

192.168.0.1

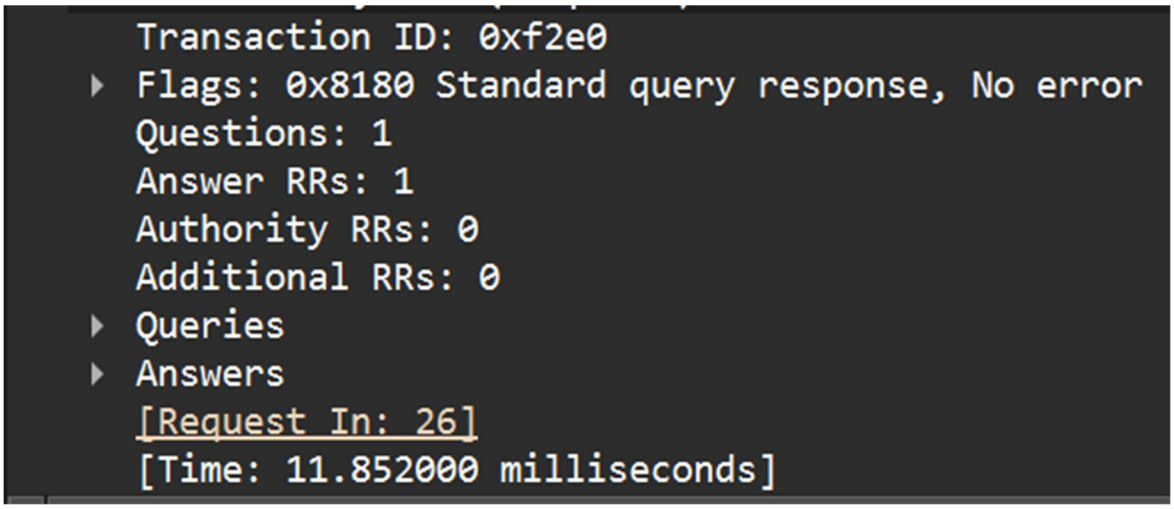
9. Examine the DNS query message. How many “questions” does this DNS message contain? How many “answers” answers does it contain?

1 Question and 0 Answers



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. 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/?

Packet no. 44

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?

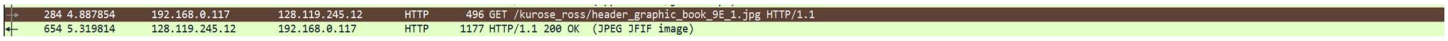
Packet no. 26

What is the packet number in the trace of the received DNS response?

Packet no. 27

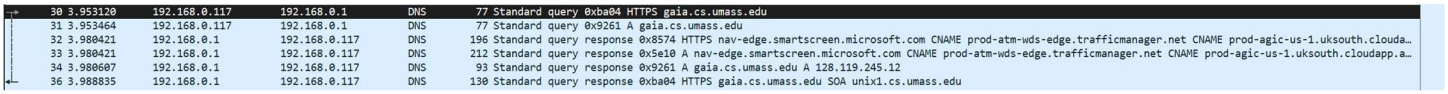
What is the packet number in the trace for the HTTP GET request for the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg?

Packet no. 284



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.

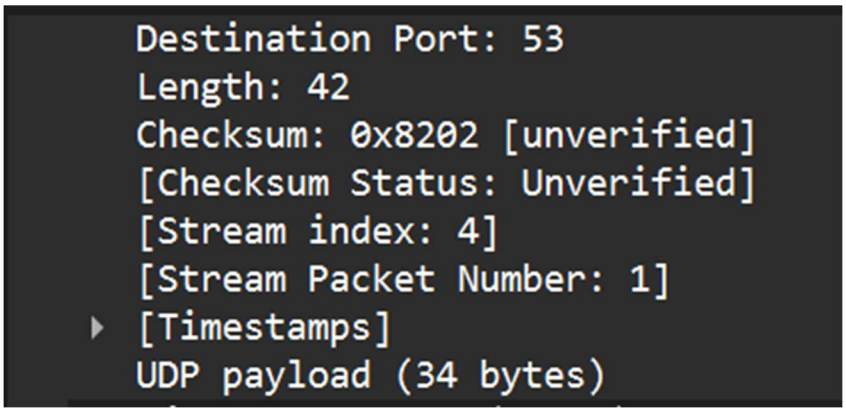
Packet no.30, it will not appear



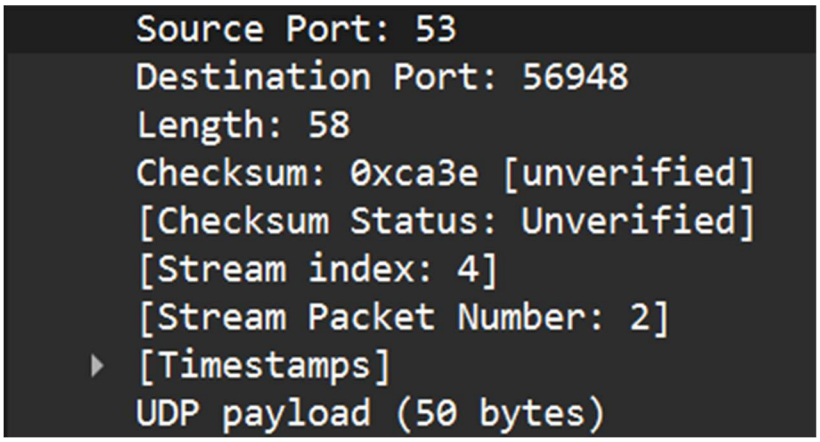
```
524 1.808233    192.168.0.117   192.168.0.1     DNS     76 Standard query 0x0002 A www.cs.umass.edu
525 1.810473    192.168.0.1     192.168.0.117   DNS     92 Standard query response 0x0002 A www.cs.umass.edu A 128.119.240.9
526 1.817423    192.168.0.117   192.168.0.1     DNS     76 Standard query 0x0003 AAAA www.cs.umass.edu
527 1.818467    192.168.0.1     192.168.0.117   DNS     76 Standard query response 0x0003 AAAA www.cs.umass.edu
```

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

Destination Port: 53



Source Port: 53

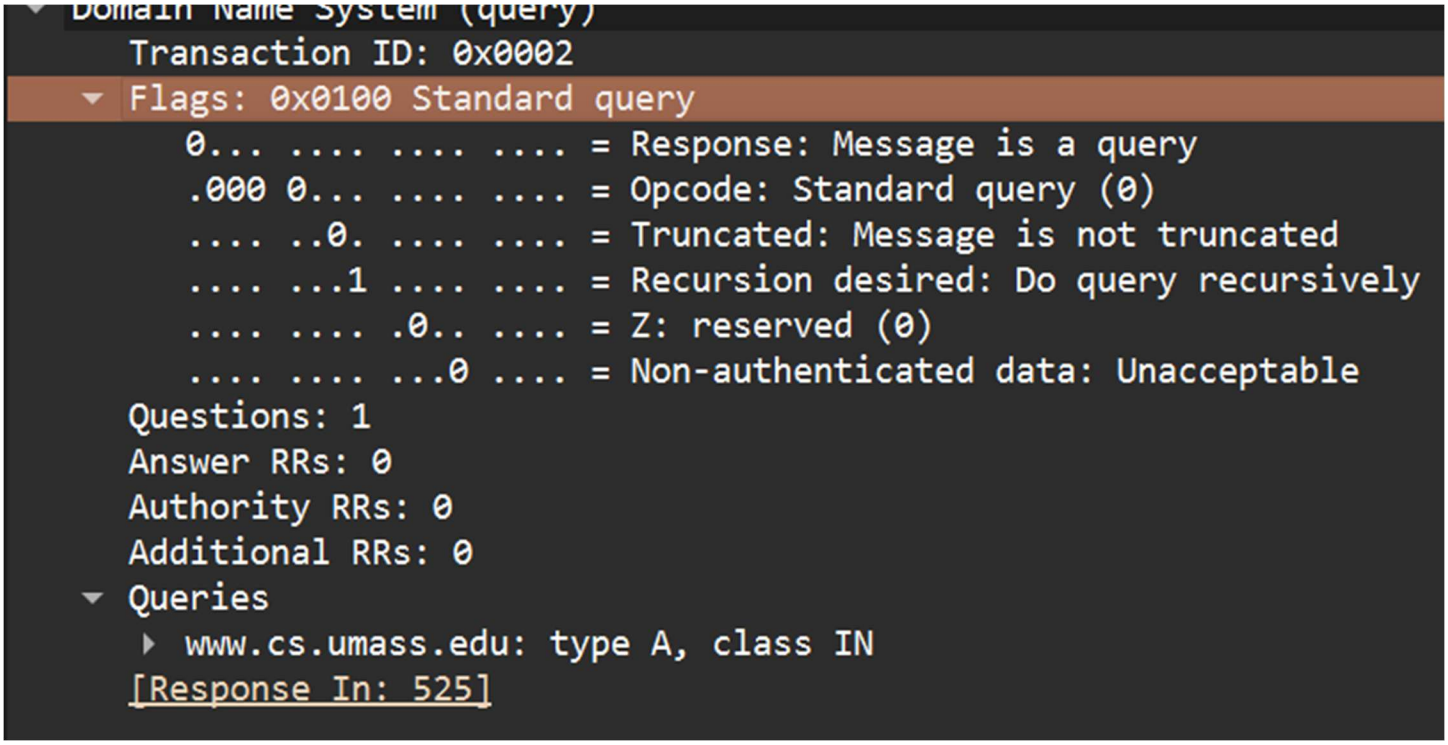


13. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

192.168.0.1, Yes

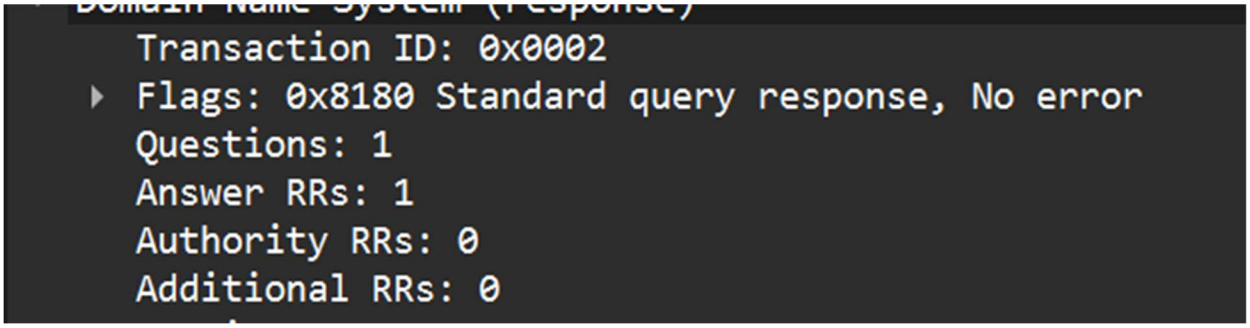
14. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

Type A, Zero answers



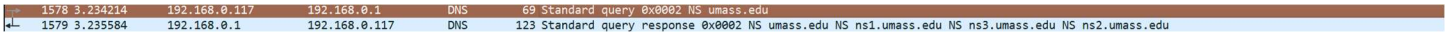
15. Examine the DNS response message to the query message. How many “questions” does this DNS response message contain? How many “answers”?

1 Question and 1 Answer



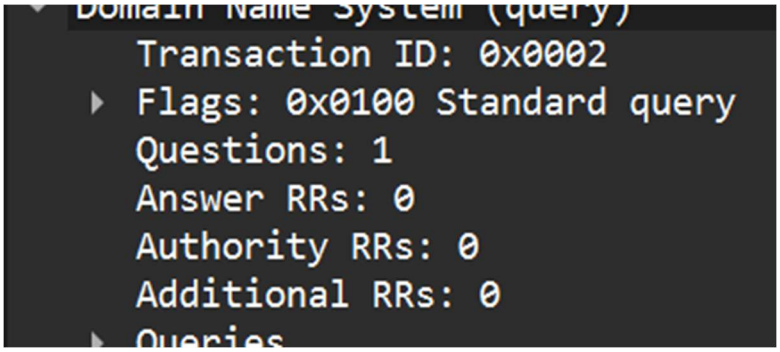
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

192.168.0.1, Yes



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

1 Question and 0 Answers



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?

3 Answers, 0 extra authority resource records needed