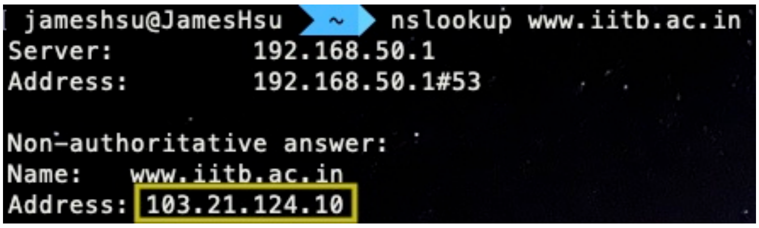
EE 450

Lab 2

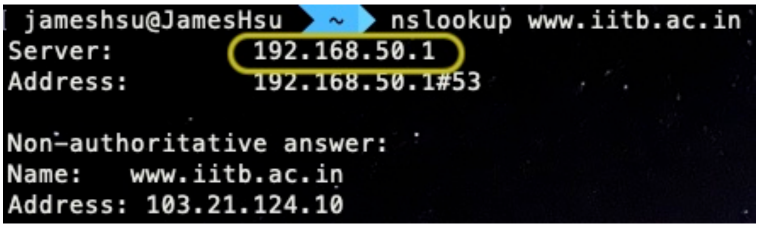
Name: Shih-Ju Hsu

1. The IP address of www.iitb.ac.in is **103.21.124.10**.



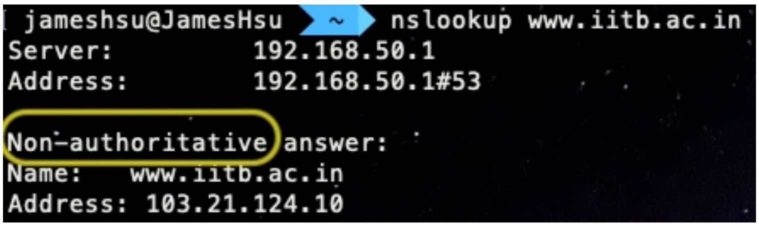
```
 jameshsu@JamesHsu  ~  nslookup www.iitb.ac.in
Server:         192.168.50.1
Address:        192.168.50.1#53

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

2. The IP address of the DNS server that provided the answer above is **192.168.50.1**.



```
 jameshsu@JamesHsu  ~  nslookup www.iitb.ac.in
Server:         192.168.50.1
Address:        192.168.50.1#53

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

3. The answer came from non-authoritative server.

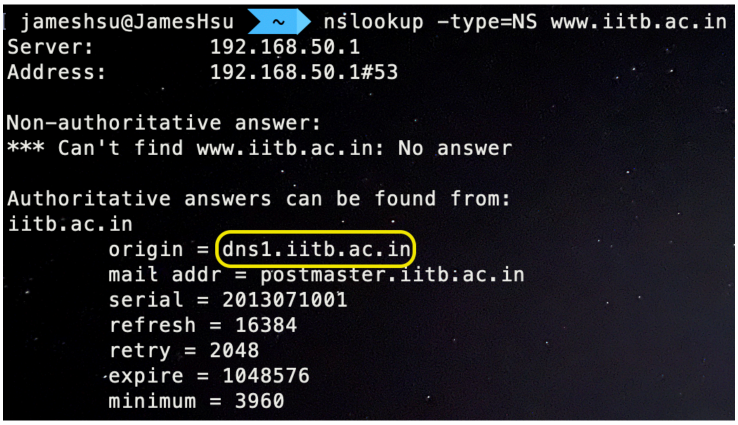


```
 jameshsu@JamesHsu  ~  nslookup www.iitb.ac.in
Server:         192.168.50.1
Address:        192.168.50.1#53

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

4.

(1) The name of the authoritative name server is **dns1.iitb.ac.in**.

(2) I would use another `nslookup` command to find the IP address of the authoritative name server.

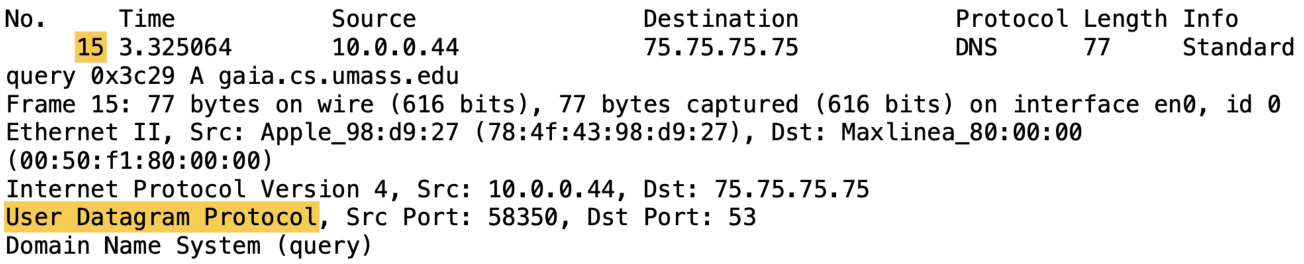


```
 jameshsu@JamesHsu  ~  nslookup -type=NS www.iitb.ac.in
Server:         192.168.50.1
Address:        192.168.50.1#53

Non-authoritative answer:
*** Can't find www.iitb.ac.in: No answer

Authoritative answers can be found from:
iitb.ac.in
        origin = dns1.iitb.ac.in
        mail addr = postmaster.iitb.ac.in
        serial = 2013071001
        refresh = 16384
        retry = 2048
        expire = 1048576
        minimum = 3960
```

5.

(1) The packet number is **15**.

(2) It is sent over **UDP**.

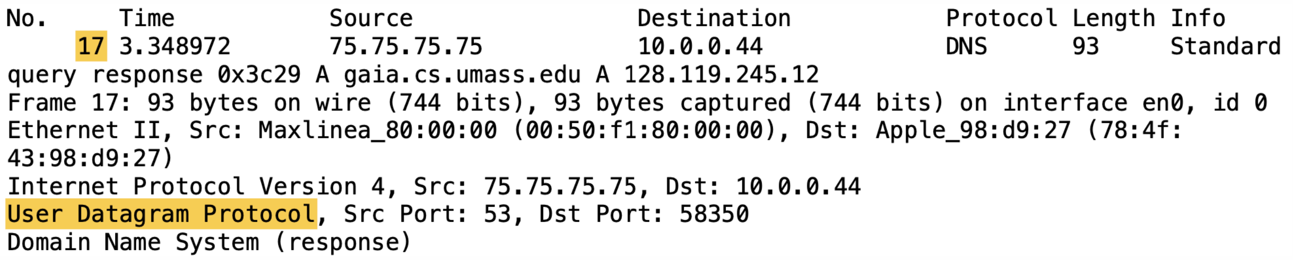


```
No.     Time           Source                Destination           Protocol Length Info
     15 3.325064       10.0.0.44             75.75.75.75           DNS      77     Standard
query 0x3c29 A gaia.cs.umass.edu
Frame 15: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface en0, id 0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinea_80:00:00
(00:50:f1:80:00:00)
Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 58350, Dst Port: 53
Domain Name System (query)
```

6.

(1) The packet number is **17**.

(2) It is sent over **UDP**.

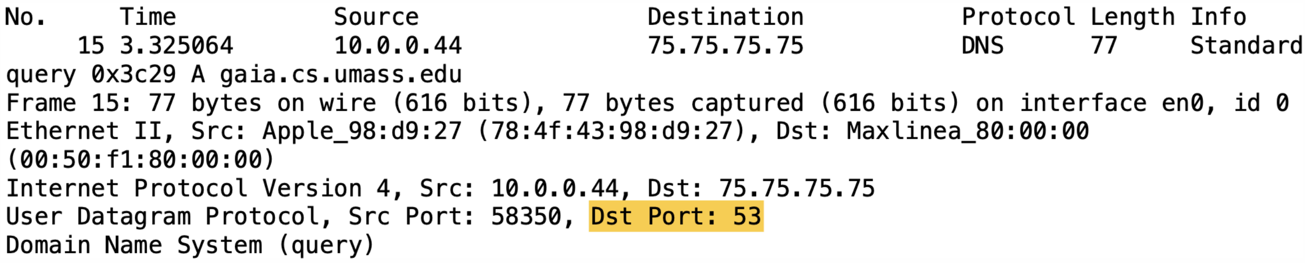


```
No.     Time           Source                Destination           Protocol Length Info
     17 3.348972       75.75.75.75           10.0.0.44             DNS      93     Standard
query response 0x3c29 A gaia.cs.umass.edu A 128.119.245.12
Frame 17: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface en0, id 0
Ethernet II, Src: Maxlinea_80:00:00 (00:50:f1:80:00:00), Dst: Apple_98:d9:27 (78:4f:
43:98:d9:27)
Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.44
User Datagram Protocol, Src Port: 53, Dst Port: 58350
Domain Name System (response)
```

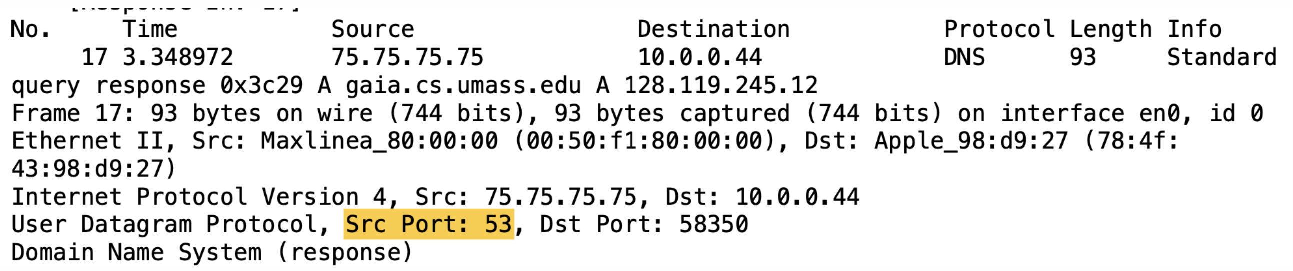
7.

The destination port for the DNS query message is **53**.

The source port of the DNS response message is also **53**.



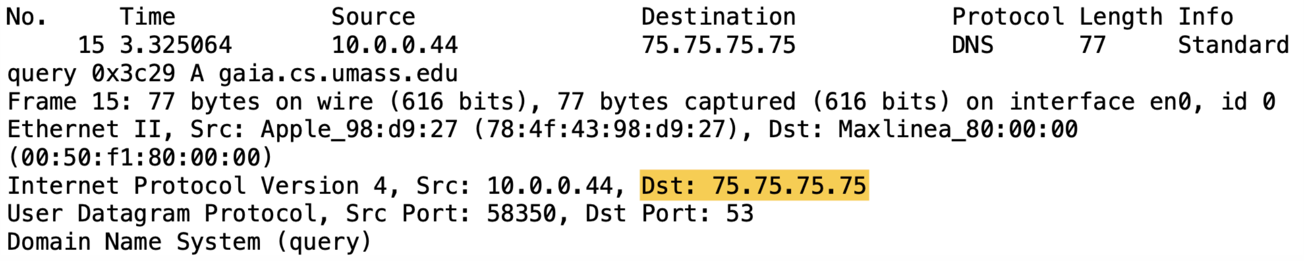
```
No.     Time           Source                Destination           Protocol Length Info
     15 3.325064       10.0.0.44             75.75.75.75           DNS      77     Standard
query 0x3c29 A gaia.cs.umass.edu
Frame 15: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface en0, id 0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinea_80:00:00
(00:50:f1:80:00:00)
Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 58350, Dst Port: 53
Domain Name System (query)
```



```
No.     Time           Source                Destination           Protocol Length Info
     17 3.348972       75.75.75.75           10.0.0.44             DNS      93     Standard
query response 0x3c29 A gaia.cs.umass.edu A 128.119.245.12
Frame 17: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface en0, id 0
Ethernet II, Src: Maxlinea_80:00:00 (00:50:f1:80:00:00), Dst: Apple_98:d9:27 (78:4f:
43:98:d9:27)
Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.44
User Datagram Protocol, Src Port: 53, Dst Port: 58350
Domain Name System (response)
```

8.

DNS query message is sent to **75.75.75.75**.

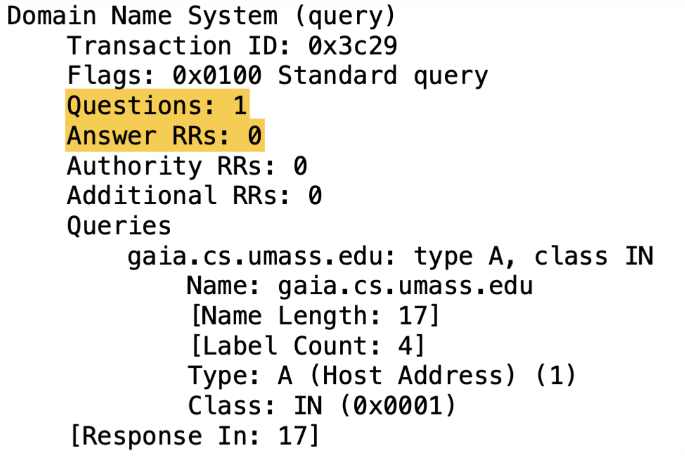


```
No.     Time           Source                Destination           Protocol Length Info
     15 3.325064       10.0.0.44             75.75.75.75           DNS      77     Standard
query 0x3c29 A gaia.cs.umass.edu
Frame 15: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface en0, id 0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinea_80:00:00
(00:50:f1:80:00:00)
Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 58350, Dst Port: 53
Domain Name System (query)
```

9. .

(1) There is **one** "questions" in the DNS query message.

(2) There are **no** "answers" in the DNS query message.

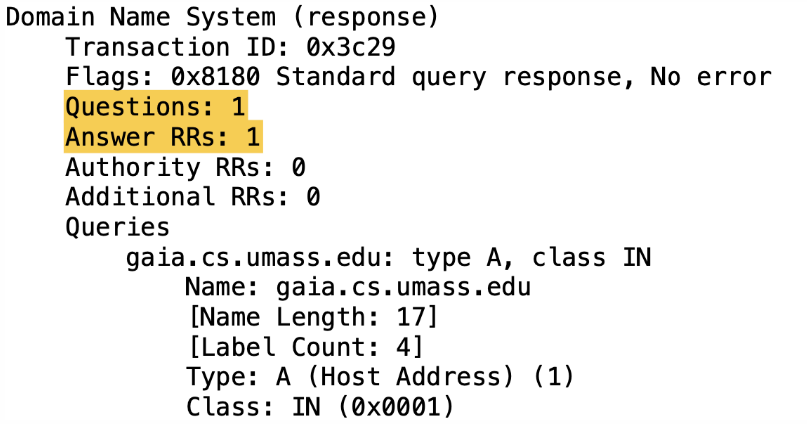


```
Domain Name System (query)
    Transaction ID: 0x3c29
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        gaia.cs.umass.edu: type A, class IN
            Name: gaia.cs.umass.edu
            [Name Length: 17]
            [Label Count: 4]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    [Response In: 17]
```

10. .

(1) There is **one** "questions" in the DNS response message.

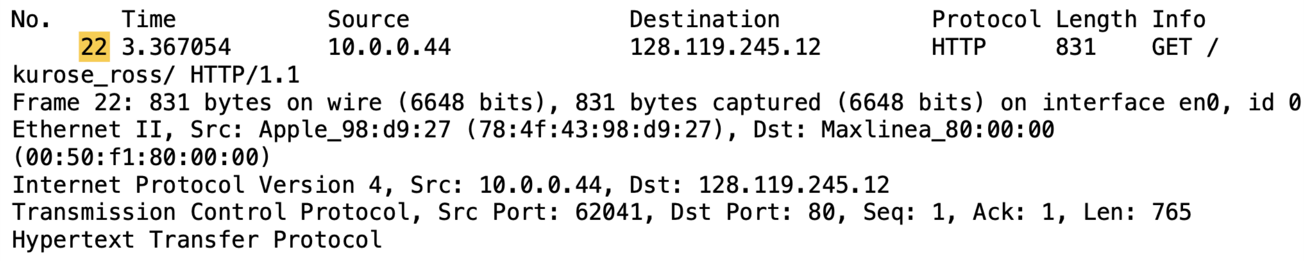
(2) There is **one** "answers" in the DNS response message.



```
Domain Name System (response)
    Transaction ID: 0x3c29
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        gaia.cs.umass.edu: type A, class IN
            Name: gaia.cs.umass.edu
            [Name Length: 17]
            [Label Count: 4]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
```

11. .

(1) The packet number of base file is **22**.



```
No.     Time           Source                Destination           Protocol Length Info
     22 3.367054       10.0.0.44             128.119.245.12        HTTP     831    GET /
kurose_ross/ HTTP/1.1
Frame 22: 831 bytes on wire (6648 bits), 831 bytes captured (6648 bits) on interface en0, id 0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinea_80:00:00
(00:50:f1:80:00:00)
Internet Protocol Version 4, Src: 10.0.0.44, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62041, Dst Port: 80, Seq: 1, Ack: 1, Len: 765
Hypertext Transfer Protocol
```

(2) The packet number of DNS query is **15**. (the screenshot is in Q5)

(3) The packet number of DNS response is **17**. (the screenshot is in Q6)

(4) The packet number is **205**.

```
No.     Time           Source                Destination           Protocol Length Info
    205 3.570142       10.0.0.44             128.119.245.12        HTTP     817    GET /
kurose_ross/header_graphic_book_8E_2.jpg HTTP/1.1
Frame 205: 817 bytes on wire (6536 bits), 817 bytes captured (6536 bits) on interface en0, id 0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinea_80:00:00
(00:50:f1:80:00:00)
Internet Protocol Version 4, Src: 10.0.0.44, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62042, Dst Port: 80, Seq: 1, Ack: 1, Len: 751
Hypertext Transfer Protocol
```

(5) The packet number of DNS query is **15**. (the screenshot is in Q5)

(6) DNS caching allows the default local DNS server to store the mappings of domain name and its IP address. In this question, the IP address of http://gaia.cs.umass.edu has been stored in the cache of after the initial query.

12.

(1) The destination port of the DNS query message is **53**.

(2) The source port of the DNS response message is also **53**.

```
No.     Time           Source                Destination           Protocol Length Info
     19 6.003804       10.0.0.44             75.75.75.75           DNS      76     Standard
query 0x609b A www.cs.umass.edu
Frame 19: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface en0, id 0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinea_80:00:00
(00:50:f1:80:00:00)
Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 57837, Dst Port: 53
Domain Name System (query)
```

```
No.     Time           Source                Destination           Protocol Length Info
     20 6.037987       75.75.75.75           10.0.0.44             DNS      92     Standard
query response 0x609b A www.cs.umass.edu A 128.119.240.84
Frame 20: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface en0, id 0
Ethernet II, Src: Maxlinea_80:00:00 (00:50:f1:80:00:00), Dst: Apple_98:d9:27 (78:4f:
43:98:d9:27)
Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.44
User Datagram Protocol, Src Port: 53, Dst Port: 57837
Domain Name System (response)
```

13. .

(1) DNS query message is sent to **75.75.75.75**.

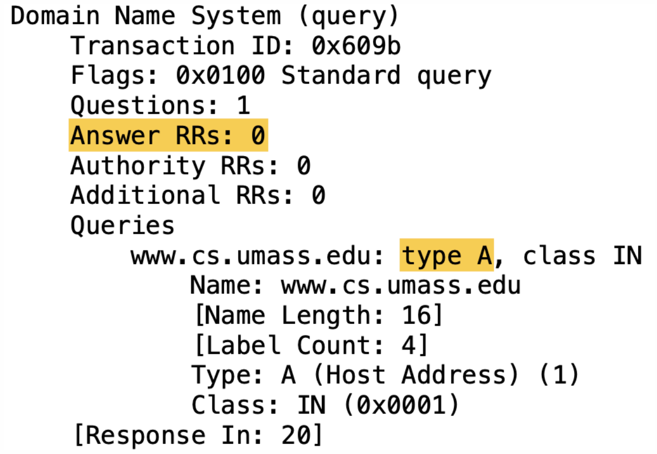
(2) Yes. It is the default local DNS sever.

```
No.     Time           Source                Destination           Protocol Length Info
     19 6.003804       10.0.0.44             75.75.75.75           DNS      76     Standard
query 0x609b A www.cs.umass.edu
Frame 19: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface en0, id 0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinea_80:00:00
(00:50:f1:80:00:00)
Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 57837, Dst Port: 53
Domain Name System (query)
```

14.

(1) It is **Type A**.

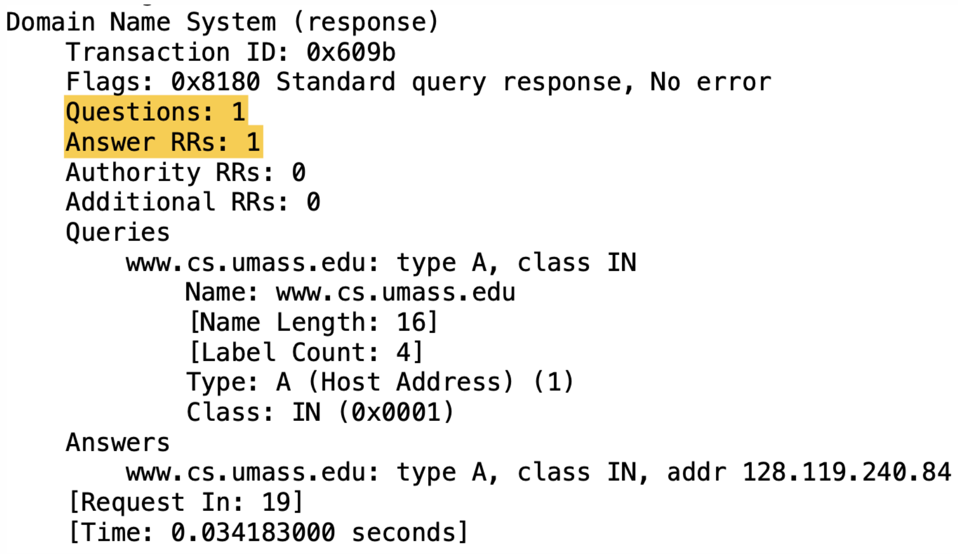
(2) No. It does not contain any "answers"



```
Domain Name System (query)
    Transaction ID: 0x609b
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.cs.umass.edu: type A, class IN
            Name: www.cs.umass.edu
            [Name Length: 16]
            [Label Count: 4]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    [Response In: 20]
```

15. .

DNS response message contain **1** "questions" and **1** "answers".

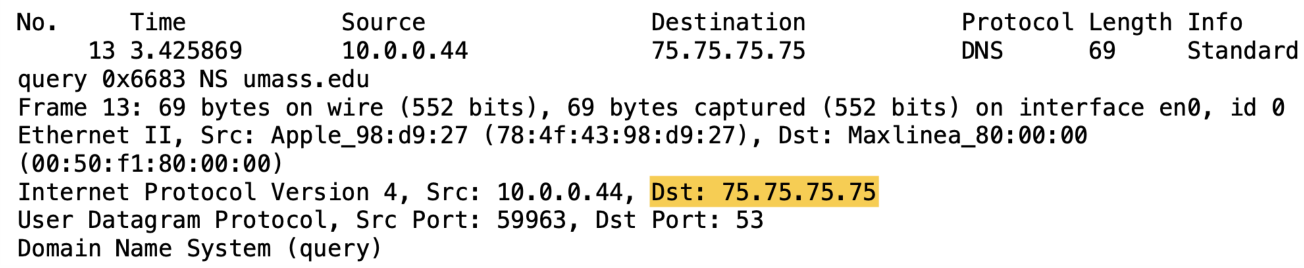


```
Domain Name System (response)
    Transaction ID: 0x609b
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.cs.umass.edu: type A, class IN
            Name: www.cs.umass.edu
            [Name Length: 16]
            [Label Count: 4]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    Answers
        www.cs.umass.edu: type A, class IN, addr 128.119.240.84
    [Request In: 19]
    [Time: 0.034183000 seconds]
```

16.

(1) The DNS query message is sent to **75.75.75.75**.

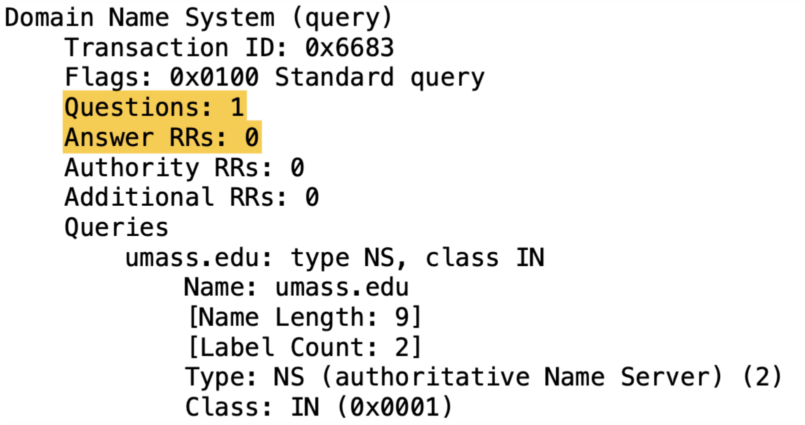
(2) Yes. This is the IP address of the default local DNS server.



```
No.     Time           Source                Destination           Protocol Length Info
     13 3.425869       10.0.0.44             75.75.75.75           DNS      69     Standard
query 0x6683 NS umass.edu
Frame 13: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface en0, id 0
Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: Maxlinea_80:00:00
(00:50:f1:80:00:00)
Internet Protocol Version 4, Src: 10.0.0.44, Dst: 75.75.75.75
User Datagram Protocol, Src Port: 59963, Dst Port: 53
Domain Name System (query)
```

17.

The query has **one** "questions" and **does not** contain any "answers".



```
Domain Name System (query)
    Transaction ID: 0x6683
    Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
        umass.edu: type NS, class IN
            Name: umass.edu
            [Name Length: 9]
            [Label Count: 2]
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
```

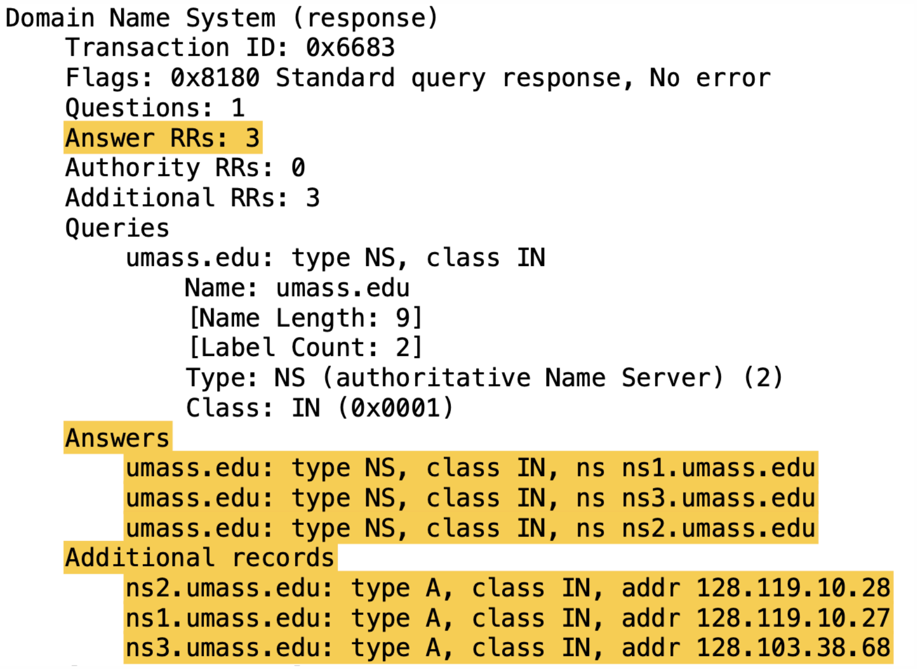
18. .

(1) There are **3** answers.

(2) The answers contain three authoritative name servers.

(3) **Three** additional records are returned.

(4) The additional records provide the **IP addresses** of the authoritative name servers.



```
Domain Name System (response)
    Transaction ID: 0x6683
    Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 3
    Queries
        umass.edu: type NS, class IN
            Name: umass.edu
            [Name Length: 9]
            [Label Count: 2]
            Type: NS (authoritative Name Server) (2)
            Class: IN (0x0001)
    Answers
        umass.edu: type NS, class IN, ns ns1.umass.edu
        umass.edu: type NS, class IN, ns ns3.umass.edu
        umass.edu: type NS, class IN, ns ns2.umass.edu
    Additional records
        ns2.umass.edu: type A, class IN, addr 128.119.10.28
        ns1.umass.edu: type A, class IN, addr 128.119.10.27
        ns3.umass.edu: type A, class IN, addr 128.103.38.68
```

Conclusion

This lab uses two tools including `nslookup` and `Wireshark`. `nslookup` is used to find out the IP address (Type A) or authoritative name server (Type NS) of one domain name. `Wireshark` functions as a packet tracer, capturing and analyzing DNS queries and responses. The outcomes of this experiment indicate that the DNS packets are sent over UDP. The host sends queries to and receives responses from the default local DNS server. The DNS server is sent and received messages on port 53. With DNS caching, the DNS servers can store the mappings of domain names and their corresponding IP addresses, which prevents it from querying the same domain names repeatedly.