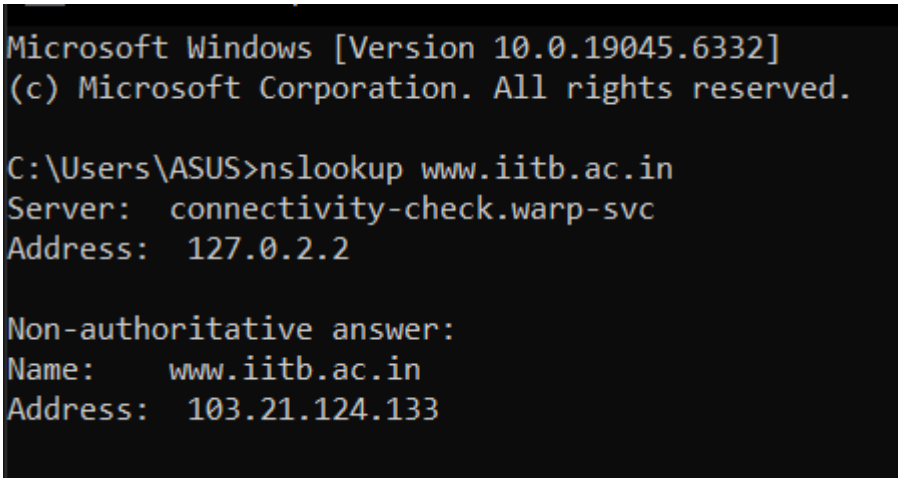
Lab5: Dns Wireshark

MD. Abu Bakar Siddique
Roll: 47

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
Ans: The IP address for **www.iitb.ac.in is 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?
Ans: **127.0.2.2**

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

Ans: The answer came from a **non-authoritative server**

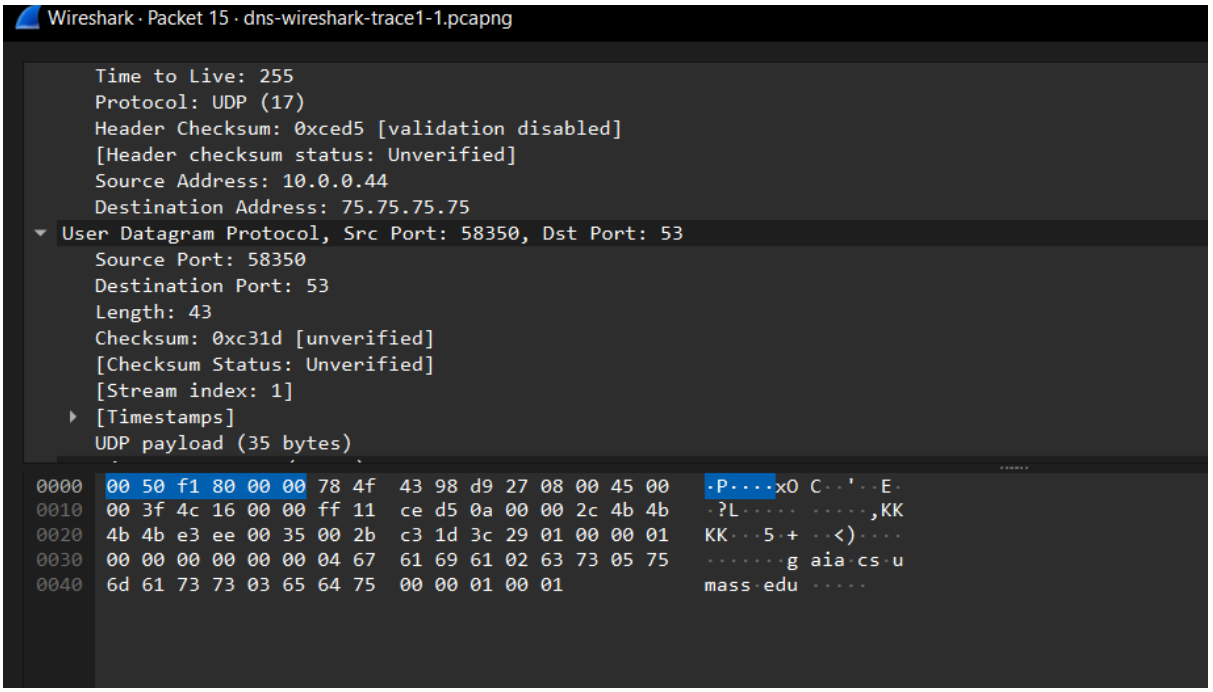
4. Use the nslookup command to determine the **name of the authoritative name server** for the iit.ac.in domain. What is that name? (If there are more than one authoritative servers, what is the name of the first authoritative server returned by nslookup)? If you had to find the IP address of that authoritative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

```
C:\Users\User>nslookup -type=NS iitb.ac.in
Server:  dns.google
Address:  8.8.8.8

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\User>nslookup dns3.iitb.ac.in
Server:  dns.google
Address:  8.8.8.8

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

Ans: dns3.iitb.ac.in
Name: dns3.iitb.ac.in
Address: 103.21.127.129

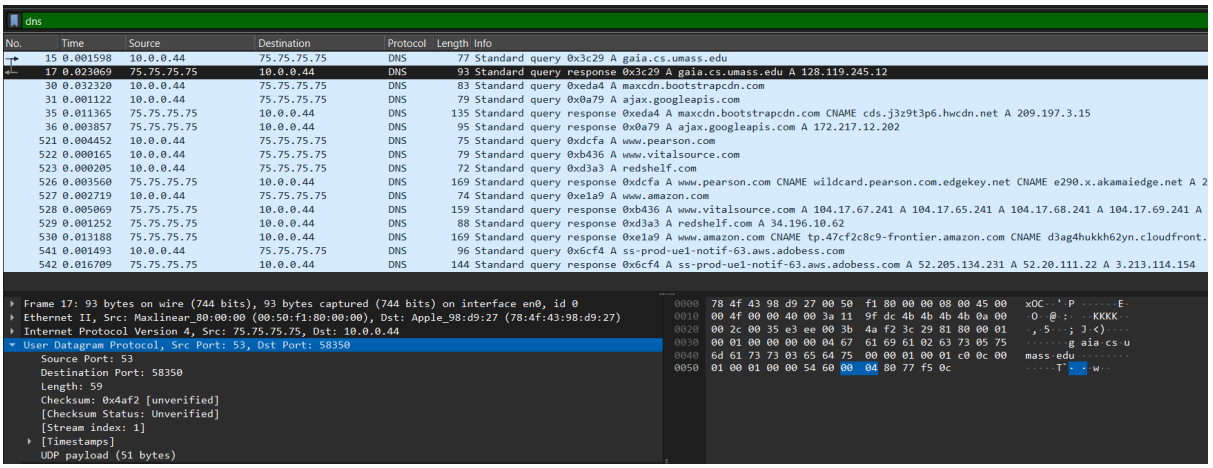
5. Locate the first DNS query message resolving the name gaia.cs.umass.edu. What is the packet number6 in the trace for the DNS query message? Is this query message sent over UDP or TCP?



Ans: packet number **15.** And it's **UDP.**

6. Now locate the corresponding DNS response to the initial DNS query. What is the

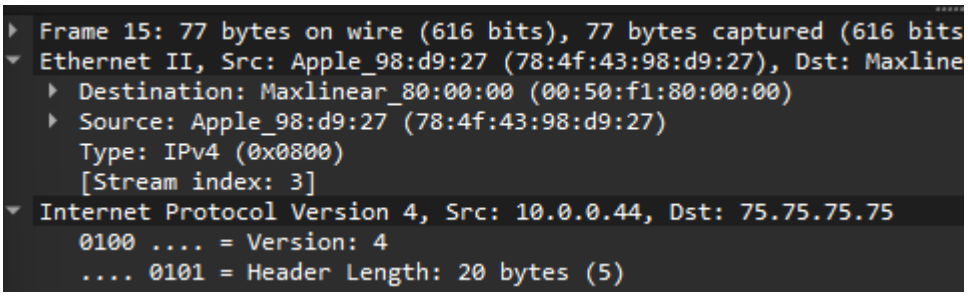
packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?



Ans: packet number **17**. And it's **UDP**

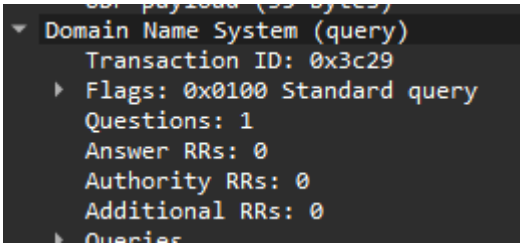
Q7.What is the destination port for the DNS query message? What is the source port of the DNS response message?
Ans: **Destination Port: 53**
Source Port: 53

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



Ans: **75.75.75.75**

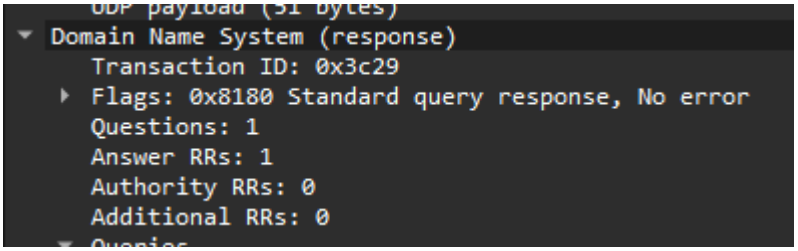
9. Examine the DNS query message. How many "questions" does this DNS message contain? How many "answers" answers does it contain?



Ans: **Questions 1, Answers 0**

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

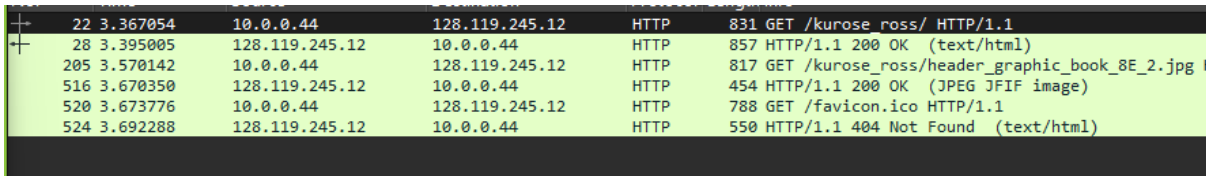
it contain?



Ans: Questions 1, Answers 1

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.

A) 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/?



Ans: **22**

B) 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?
Ans: **15**

C) What is the packet number in the trace of the received DNS response?
Ans: **17**

D) 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?
Ans: **205**

E) 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?
Ans: New Dns query not made

F) Discuss how DNS caching affects the answer to this last question

Ans: **Without caching:** Every HTTP request to a hostname may require a DNS query + response.
With caching (normal case): Only the first request requires DNS resolution; subsequent requests reuse the cached IP.

This is why, in most student traces, you will see **only one DNS query/response pair** for gaia.cs.umass.edu, even though two different HTTP objects are retrieved.

12. What is the destination port for the DNS query message? What is the source port of the DNS response message?
Ans: **53, 53**

13. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
Ans: **75.75.75.755, which is the IP address of the system's default local DNS server.**

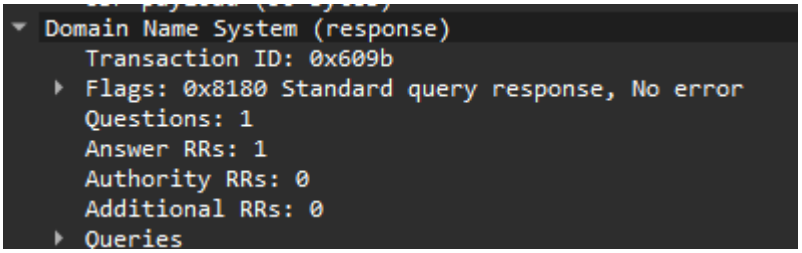
14. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

```
    [Time since previous frame: 0.000000000 seconds]
  UDP payload (34 bytes)
▾ Domain Name System (query)
  Transaction ID: 0x609b
  ▾ Flags: 0x0100 Standard query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... .0.. .... = Z: reserved (0)
    .... .... ...0 .... = Non-authenticated data: Unacceptable
  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 (1) (Host Address)
      Class: IN (0x0001)
  [Response In: 20]
```

Ans:**The type of DNS query is A (Address record) (IPv4) and query message does not contain any answers**

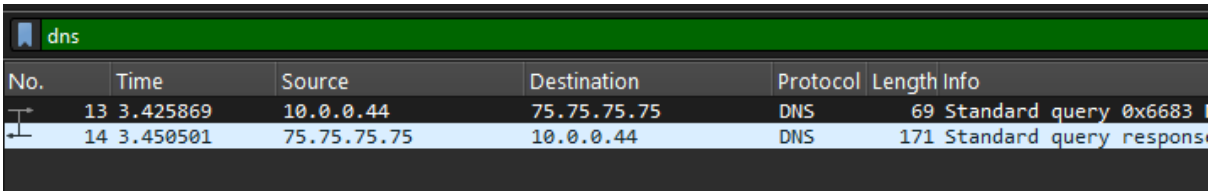
15. Examine the DNS response message to the query message. How many

“questions” does this DNS response message contain? How many “answers”?



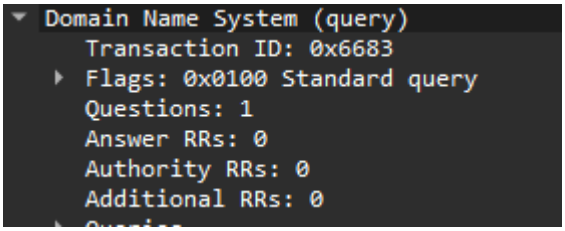
Ans: **1, 1**

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



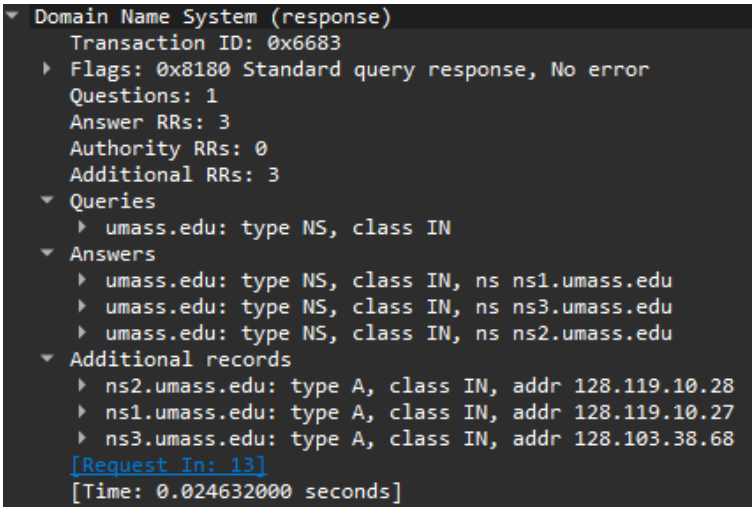
Ans: **75.75.75.75**, which is the IP address of the **default local DNS server**

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



Ans: **1, 0**

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?



Ans:
3,

The answers contain the names of the authoritative name servers for the umass.edu domain:
ns1.umass.edu
ns2.umass.edu
ns3.umass.edu

The response returns 3 additional resource records. These records provide the IP addresses for the name servers listed in the answers, specifically
ns2.umass.edu
ns1.umass.edu
ns3.umass.edu