Pandit Deendayal Energy University
School of Technology
Department of ICT
Academic Year: 2022-23
Computer Communication and Networking Lab
20IC306P

Name: Janakar Patel

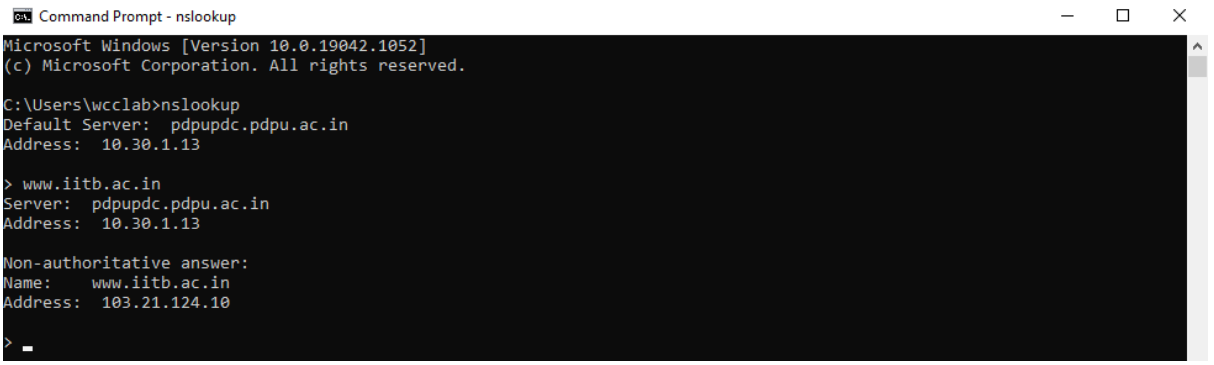
Roll No: 20BIT061

Experiment 4:

Aim: To understand the working of DNS by using wire shark and packet tracer.
Software Tools required: - Wire-shark and Cisco packet tracer

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
   Ans:

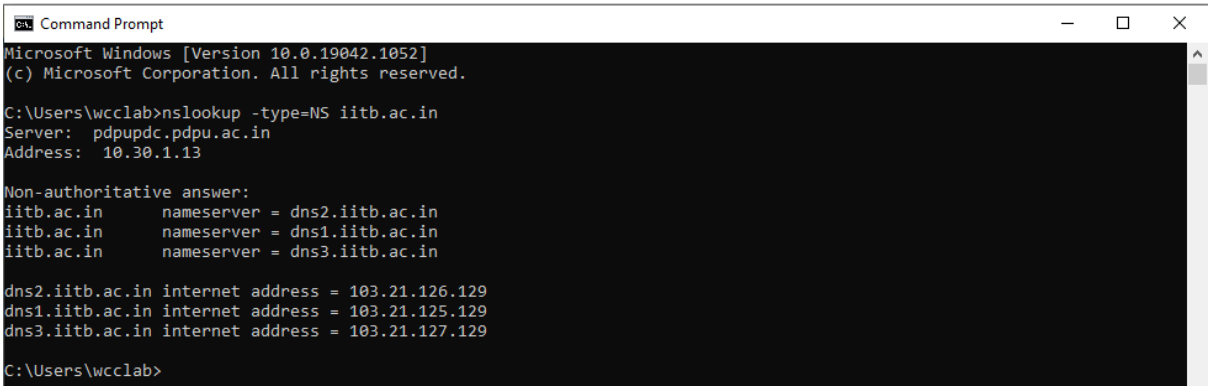


   IP Address: 103.21.124.18

2. What is the IP address of the DNS server that provided the answer to your `nslookup` command in question 1 above?
   Ans: IP Address: 103.21.124.18

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

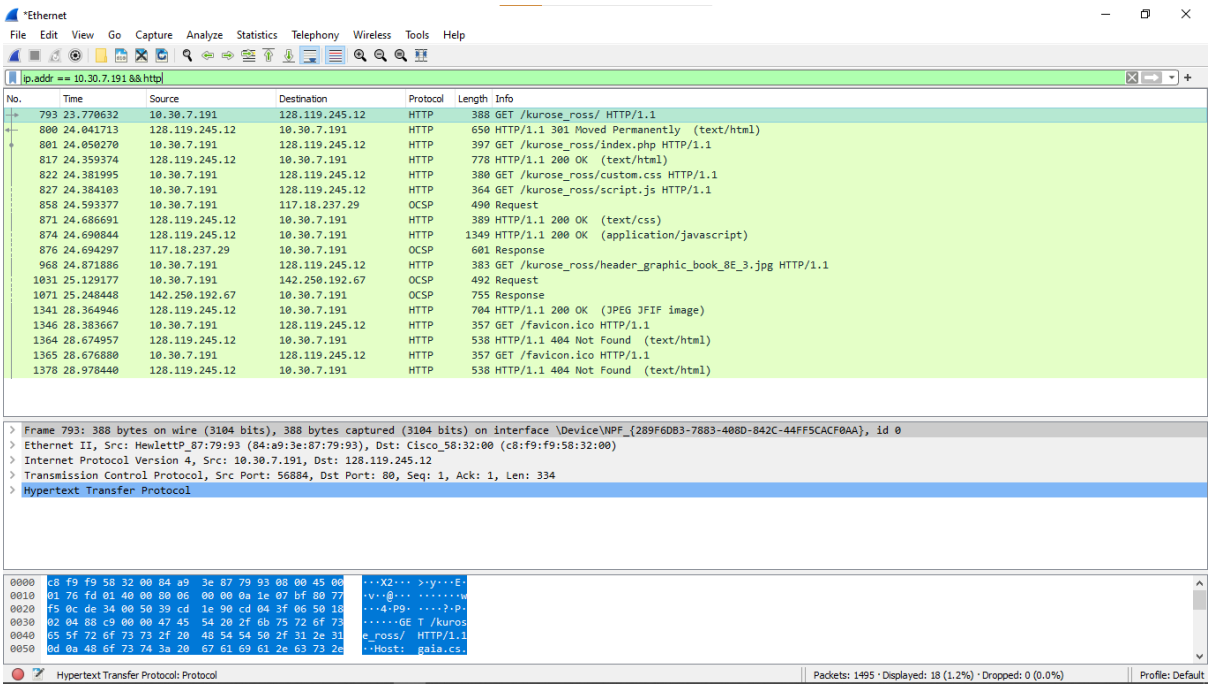
4. Use the `nslookup` command to determine the name of the authoritative name server for the iitb.ac.in domain. What is that name? (If there are more than one authoritative servers, what is the name of the first authoritative server returned by `nslookup`)? If you had to find the IP address of that authoritative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



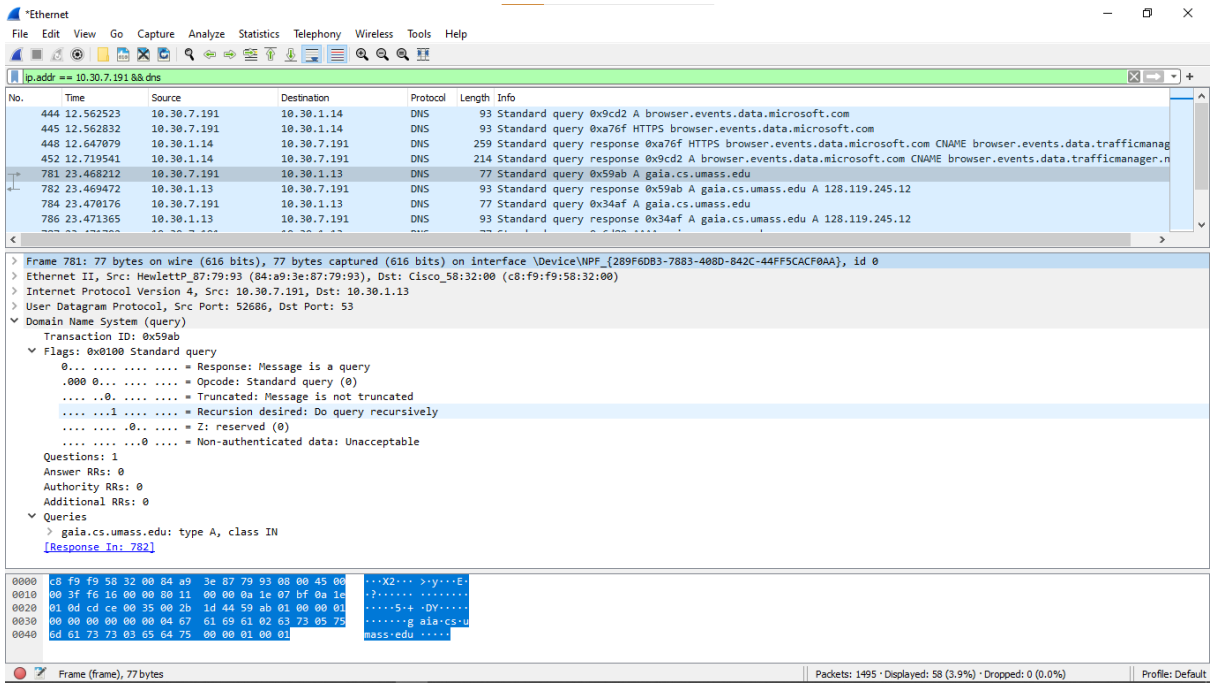
Three authoritative servers. The first server name is dns2.iitb.ac.in and internet address 103.21.126.129

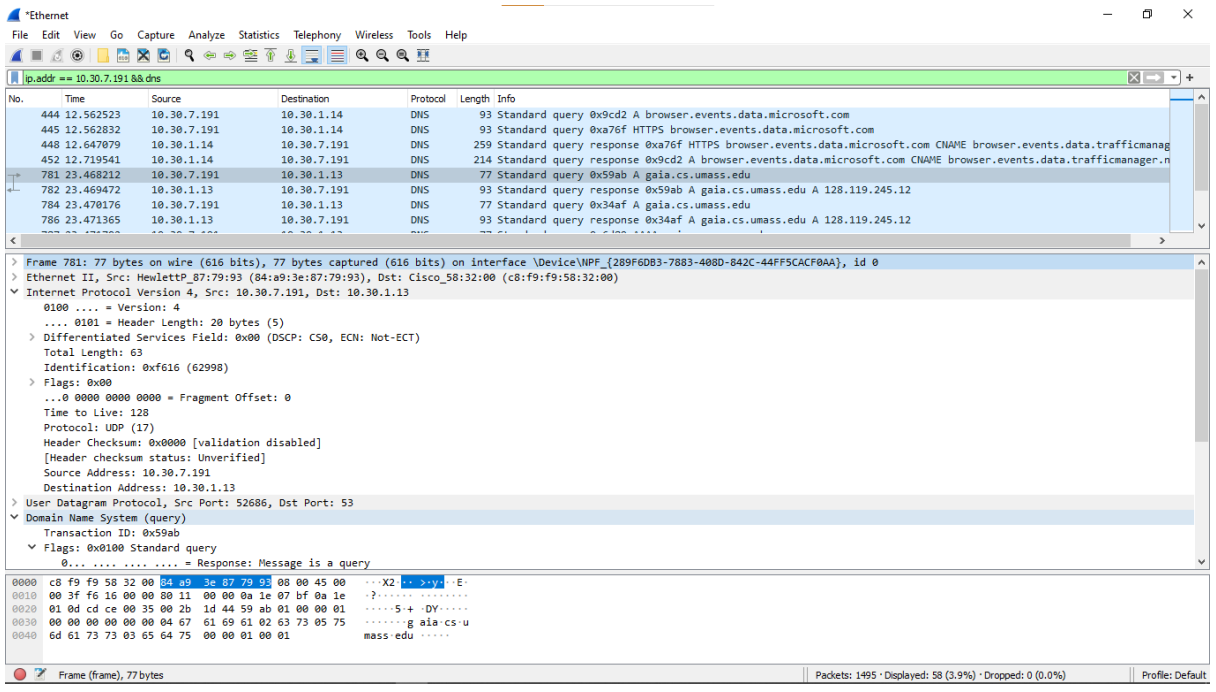
2. The DNS cache on your computer

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?

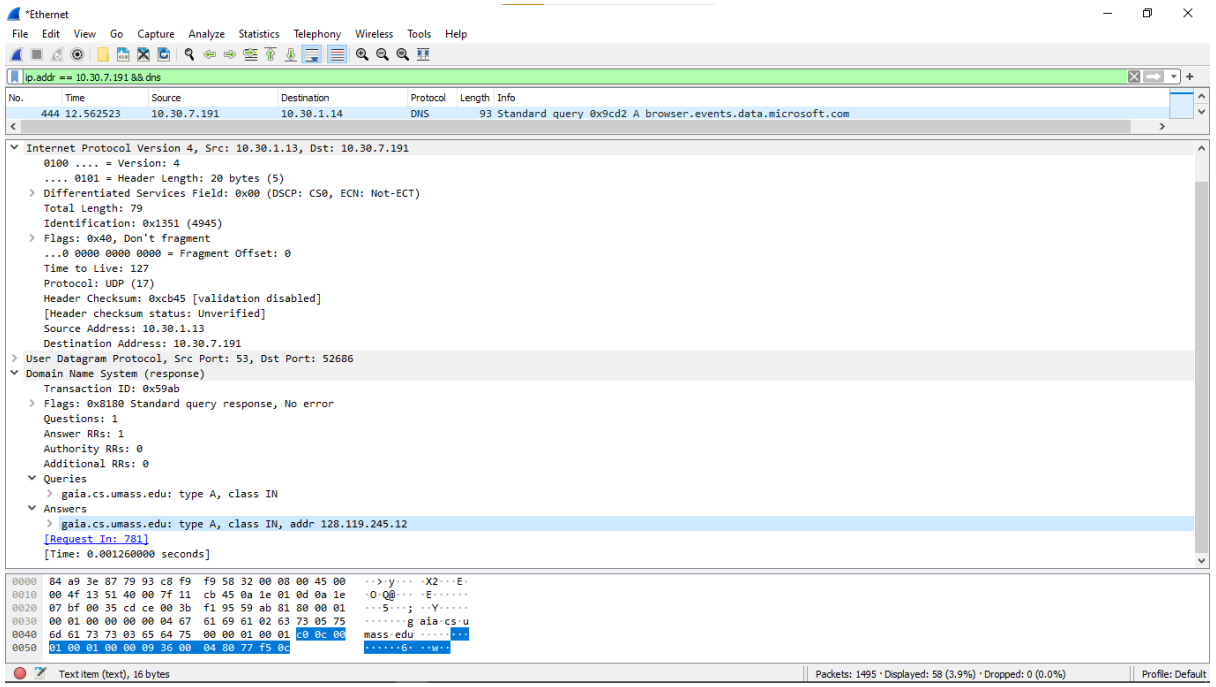




Ans: The query is sent over a UDP Protocol. The packet number is 781.

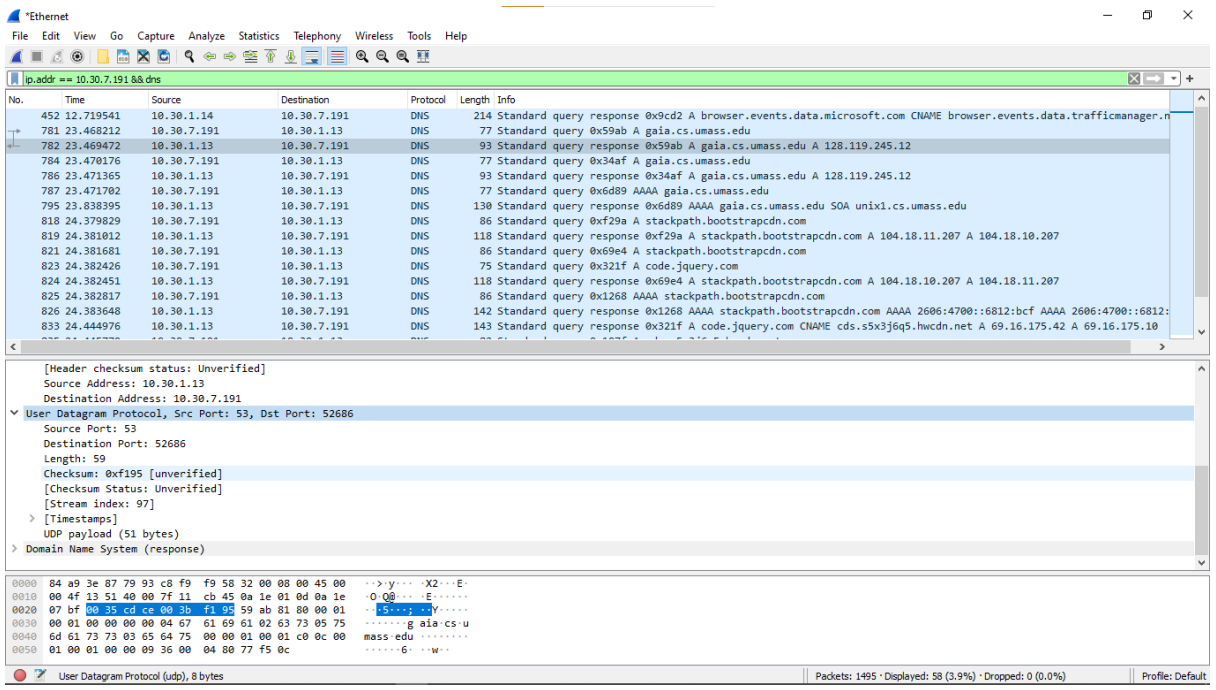
6. Now locate the corresponding DNS response to the initial DNS query. What is the packet number in the trace for the DNS response message? Is this response message received via UDP or TCP?

[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.



Ans: The message is received via UDP and packet number is 782.

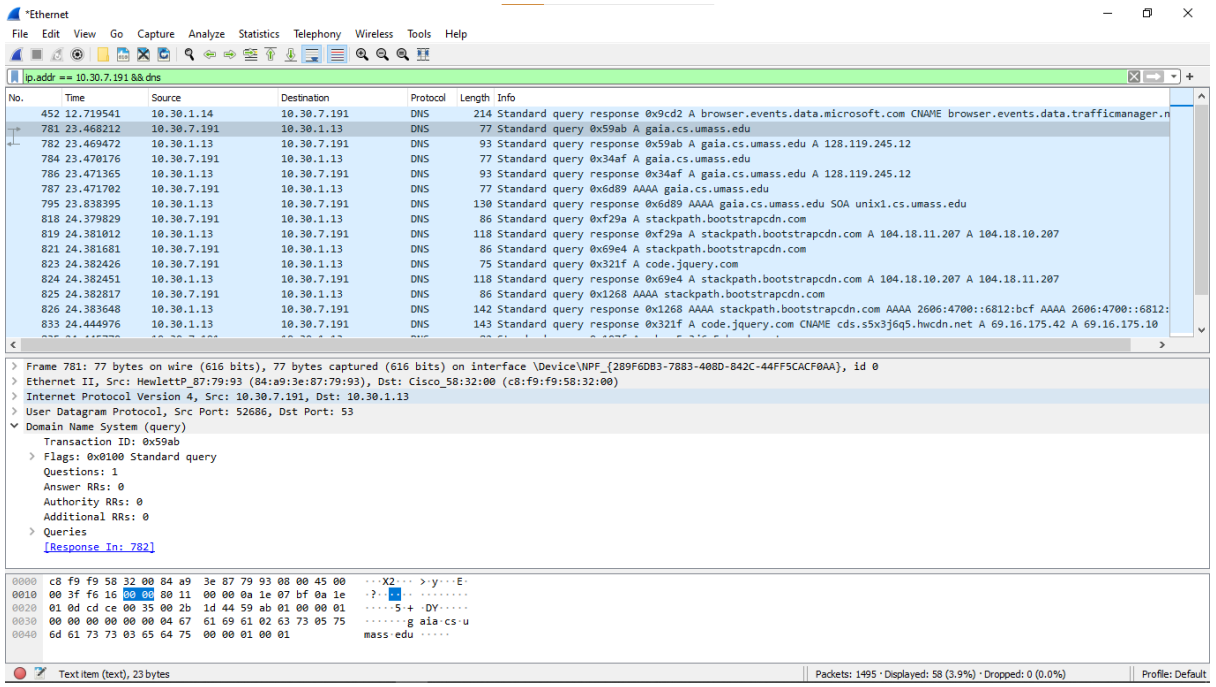
7. What is the destination port for the DNS query message? What is the source port of the DNS response message?



Ans: The port number of destination port for query and source source port of response is 53.

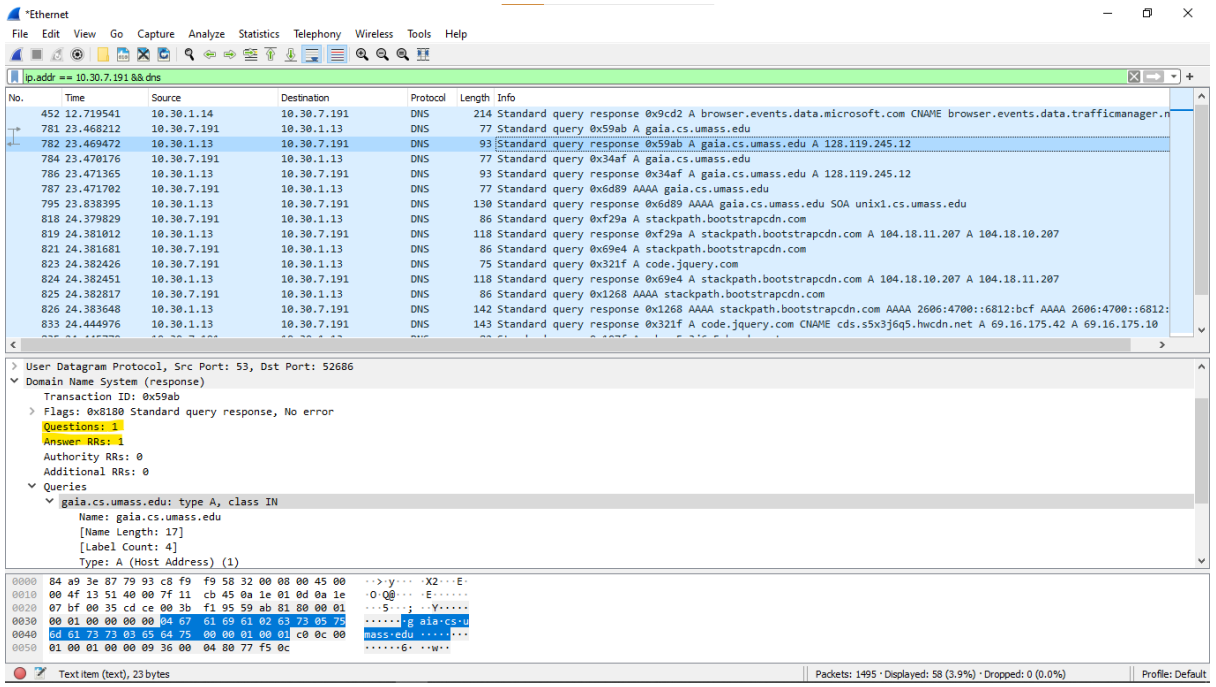
8. To what IP address is the DNS query message sent?
   Ans: IP Address: 10.30.1.13

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



Question is 1 and the answer is 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:

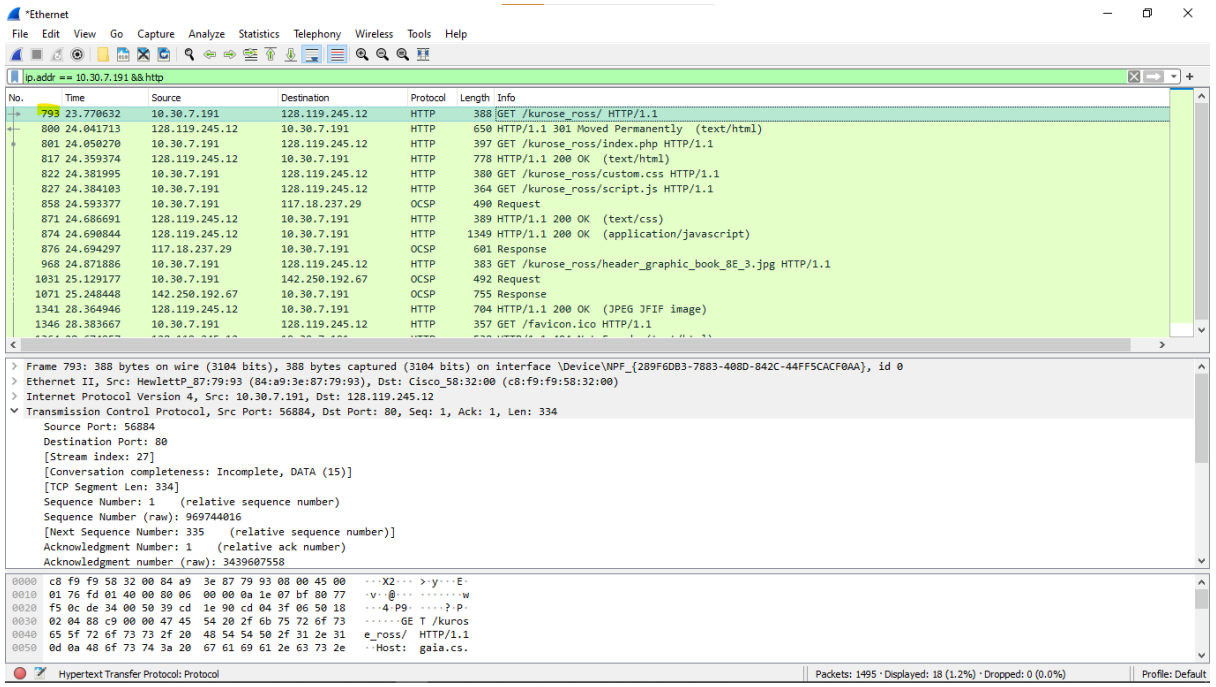


Question is 1 and Answer is 1.

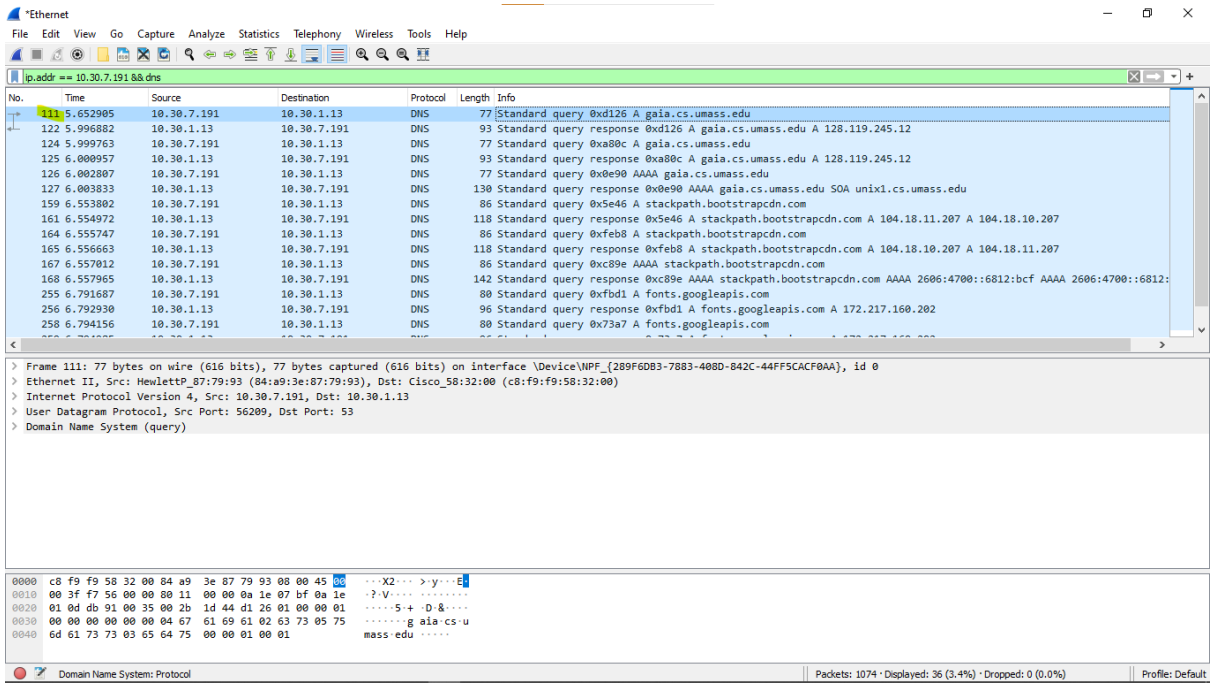
11. The web page for the base file http://gaia.cs.umass.edu/kurose_ross/ references the image object http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg , which, like the base webpage, is on gaia.cs.umass.edu. What is the packet number in the trace for the initial HTTP GET request for the base file http://gaia.cs.umass.edu/kurose_ross/? 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? What is the packet number in the trace of the received DNS response? 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? 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.

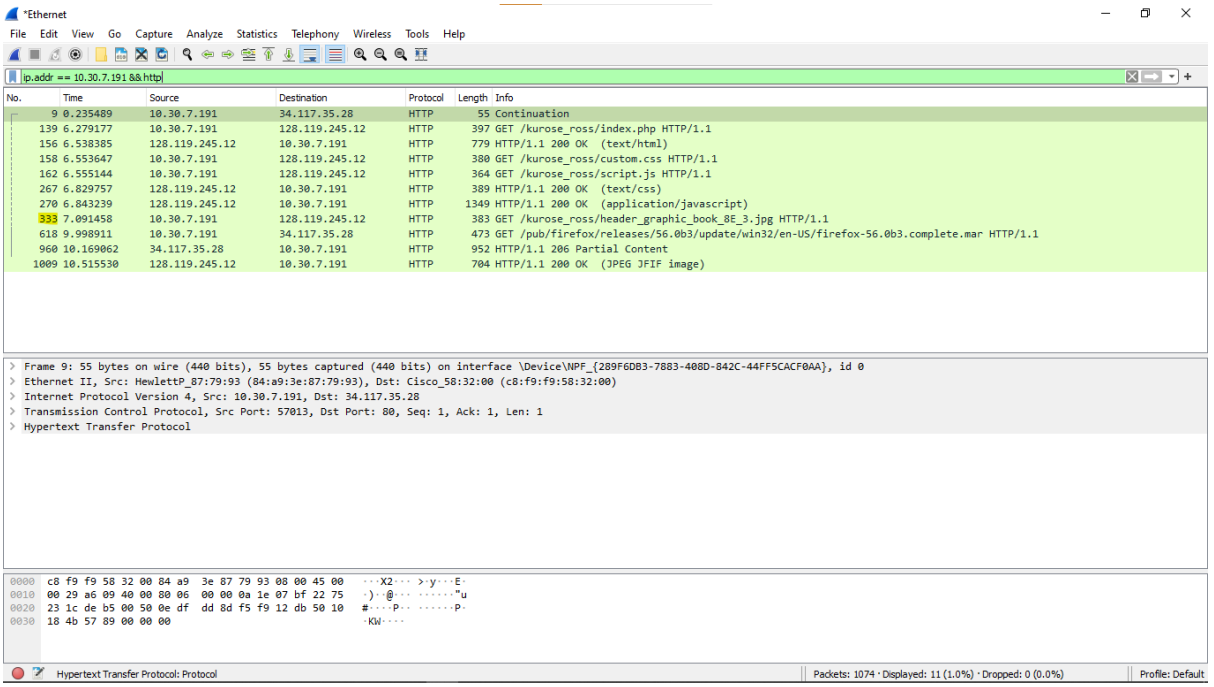
Ans:



Packet Number for initial HTTP is 793.



Packet number is 111, In response to query the packet number is 112

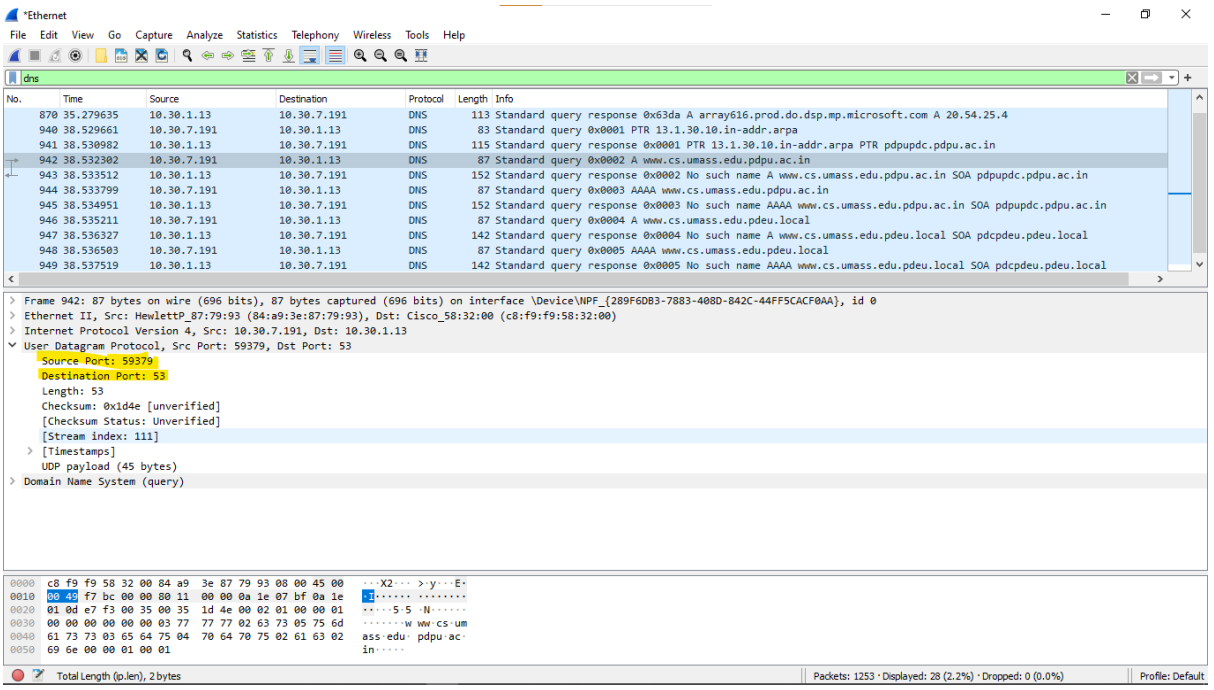


Packet number is 333.

No DNS query is sent for the second HTTP GET request. Because the IP address is already store in local DNS cache memory.

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

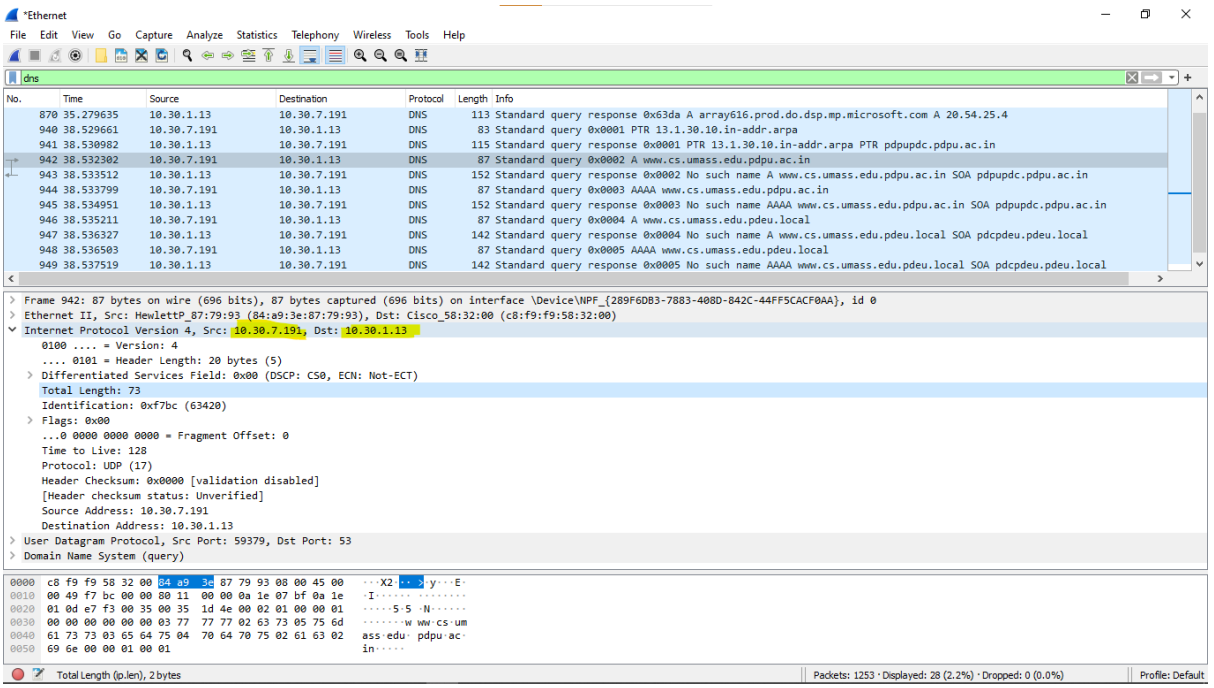
Ans:



The port number of destination for query and source for response is 53.

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

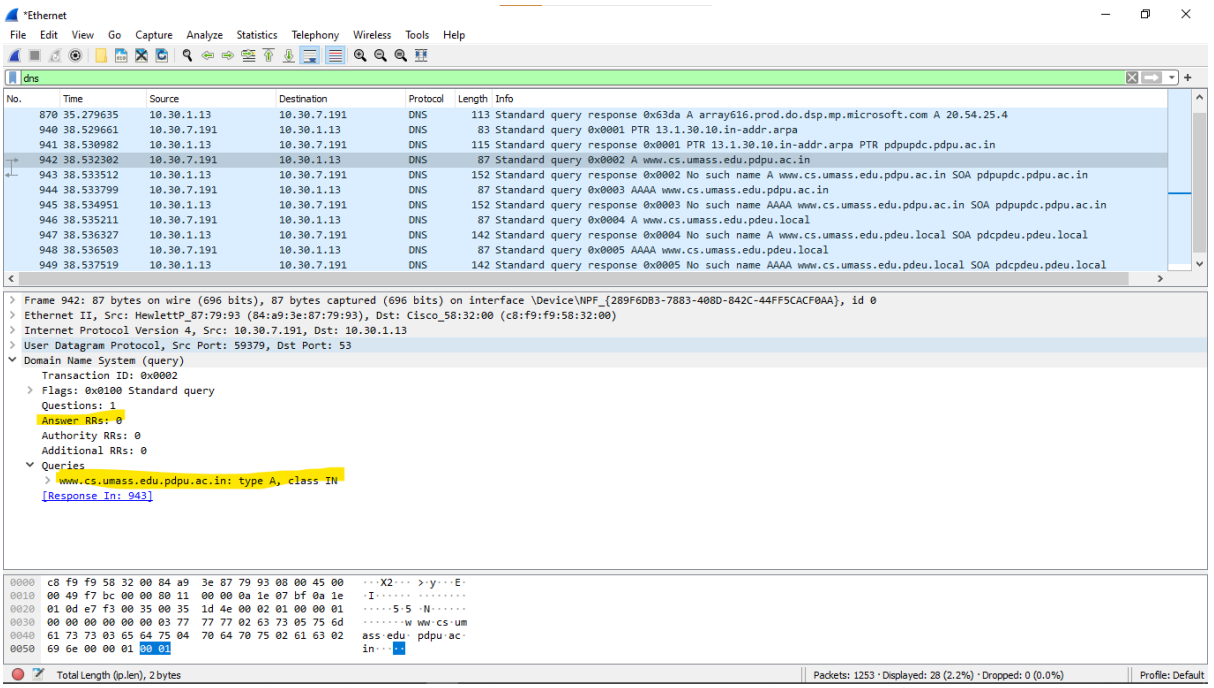
Ans:



It is a local dns server.

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

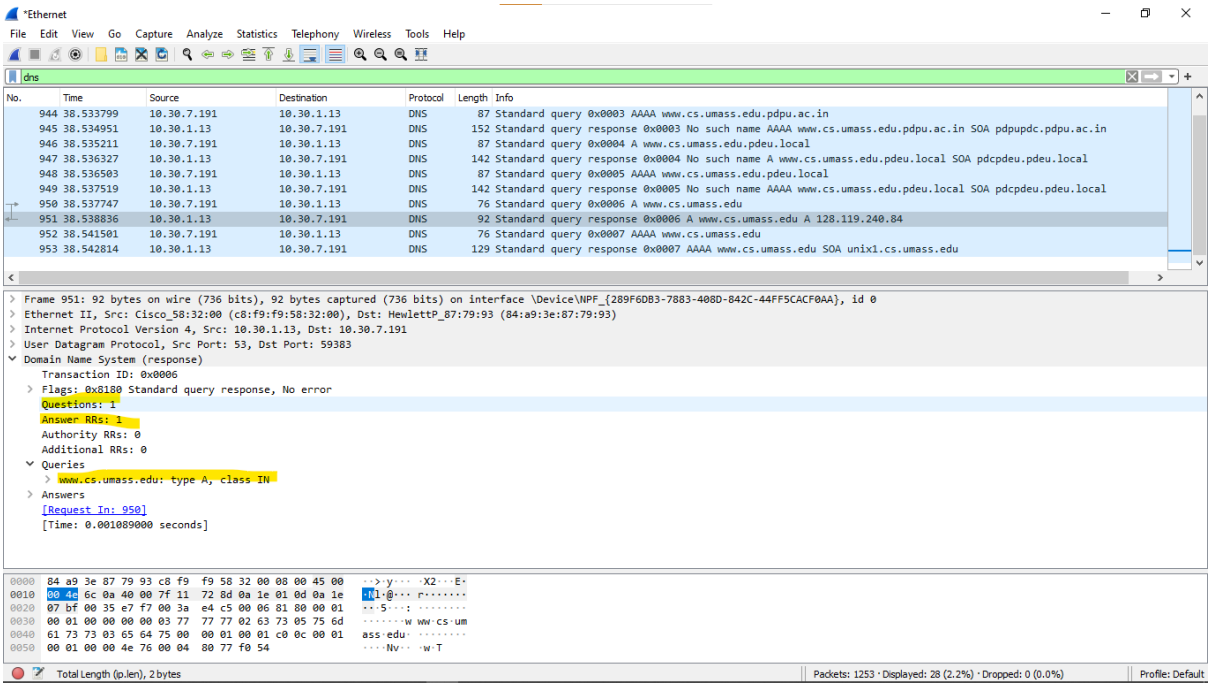
Ans:



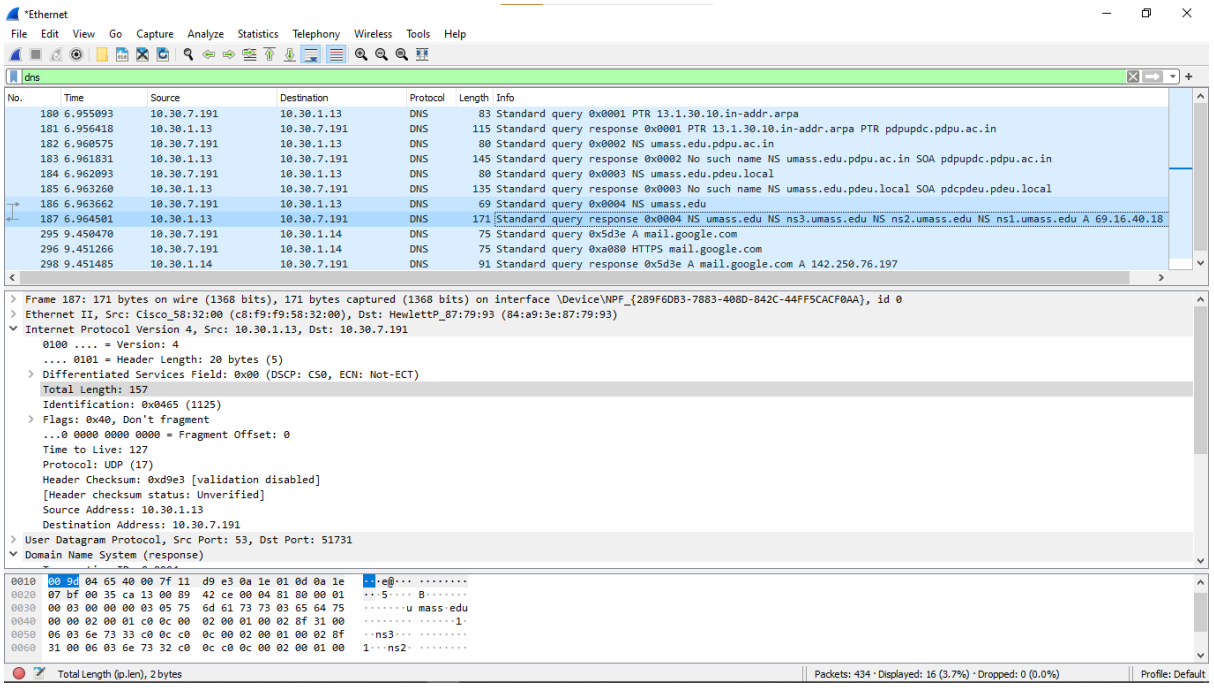
Type is A, It contains 0 answers.

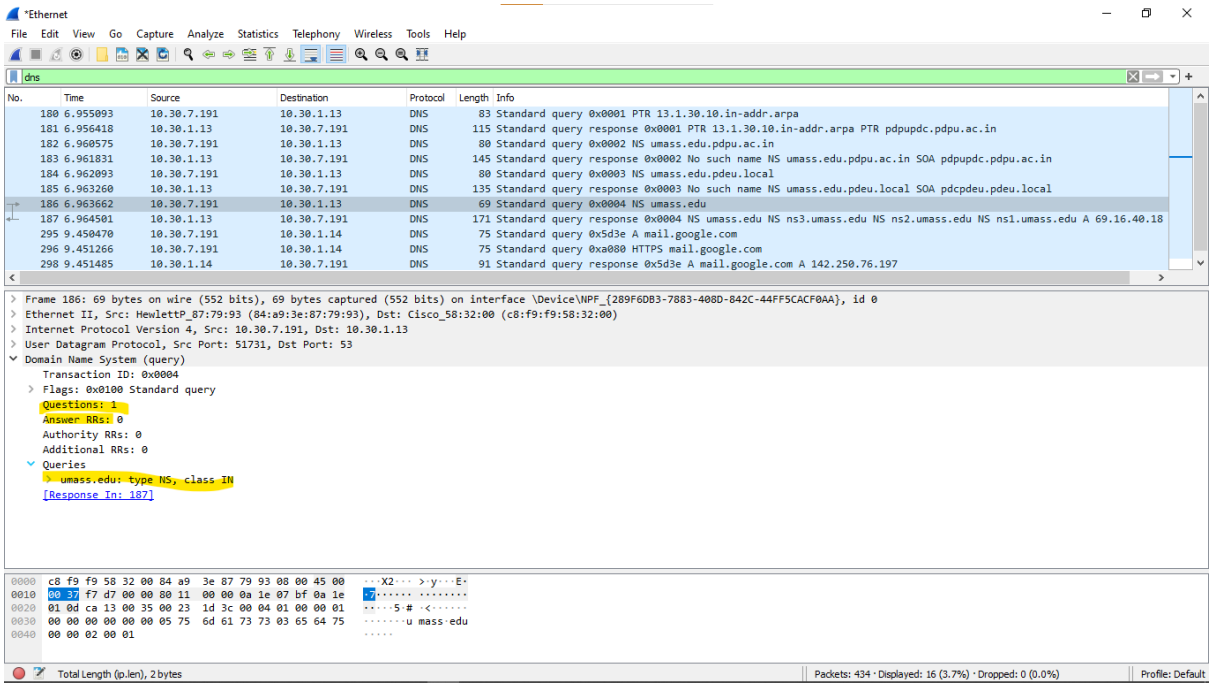
15. Examine the DNS response message to the query message. How many “questions” does this DNS response message contain? How many “answers”?

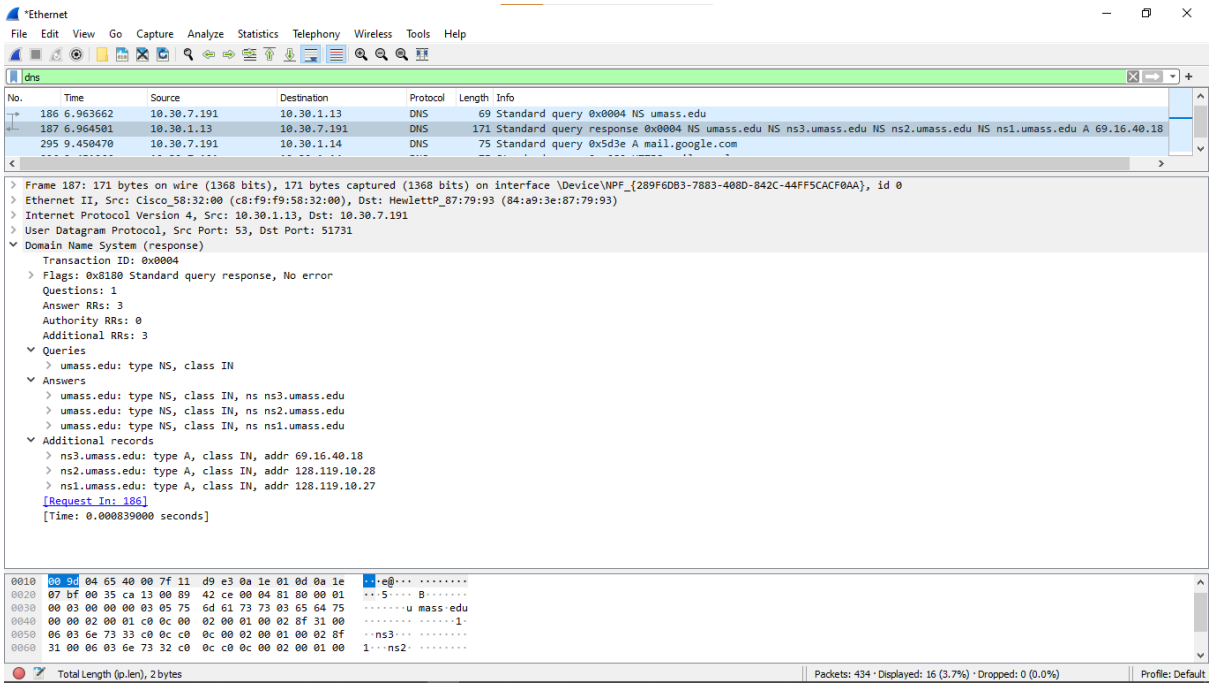
Ans:



It is type A and it contains 1 question and 1 answer.

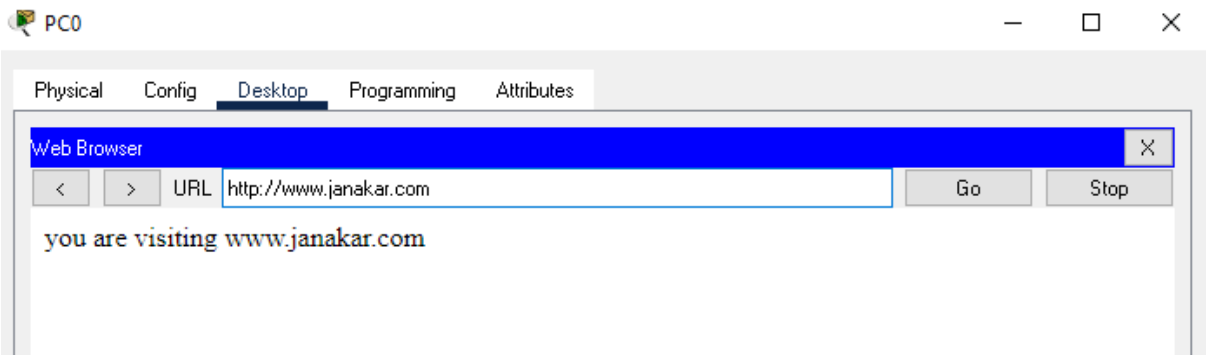


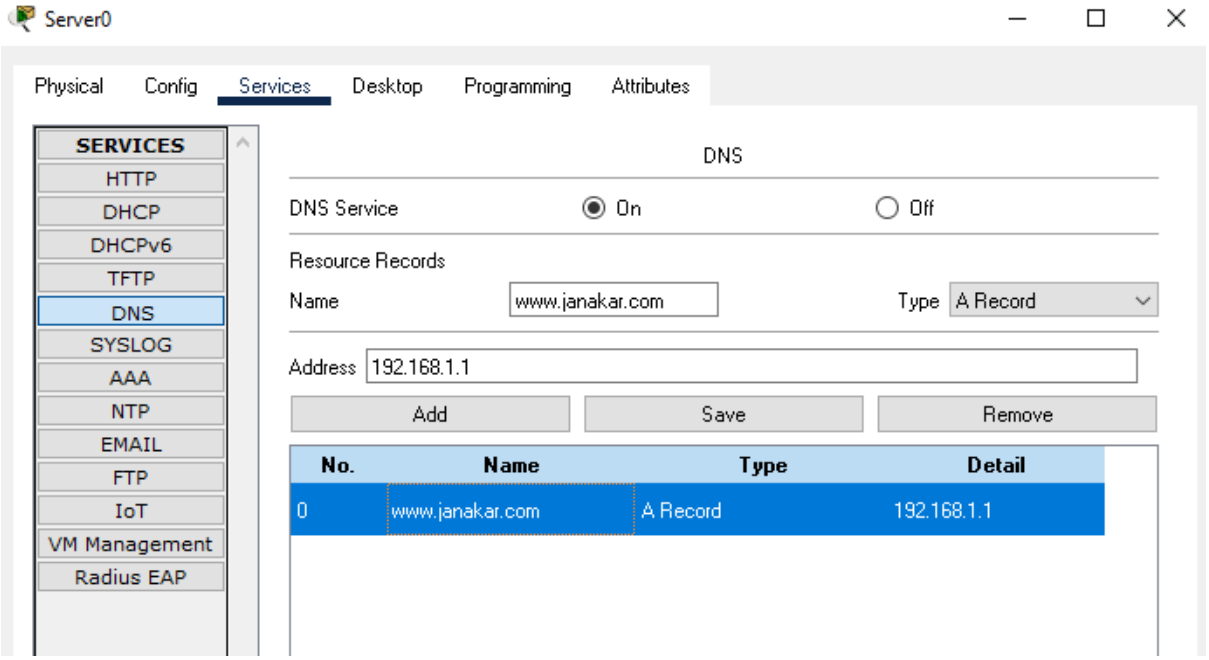


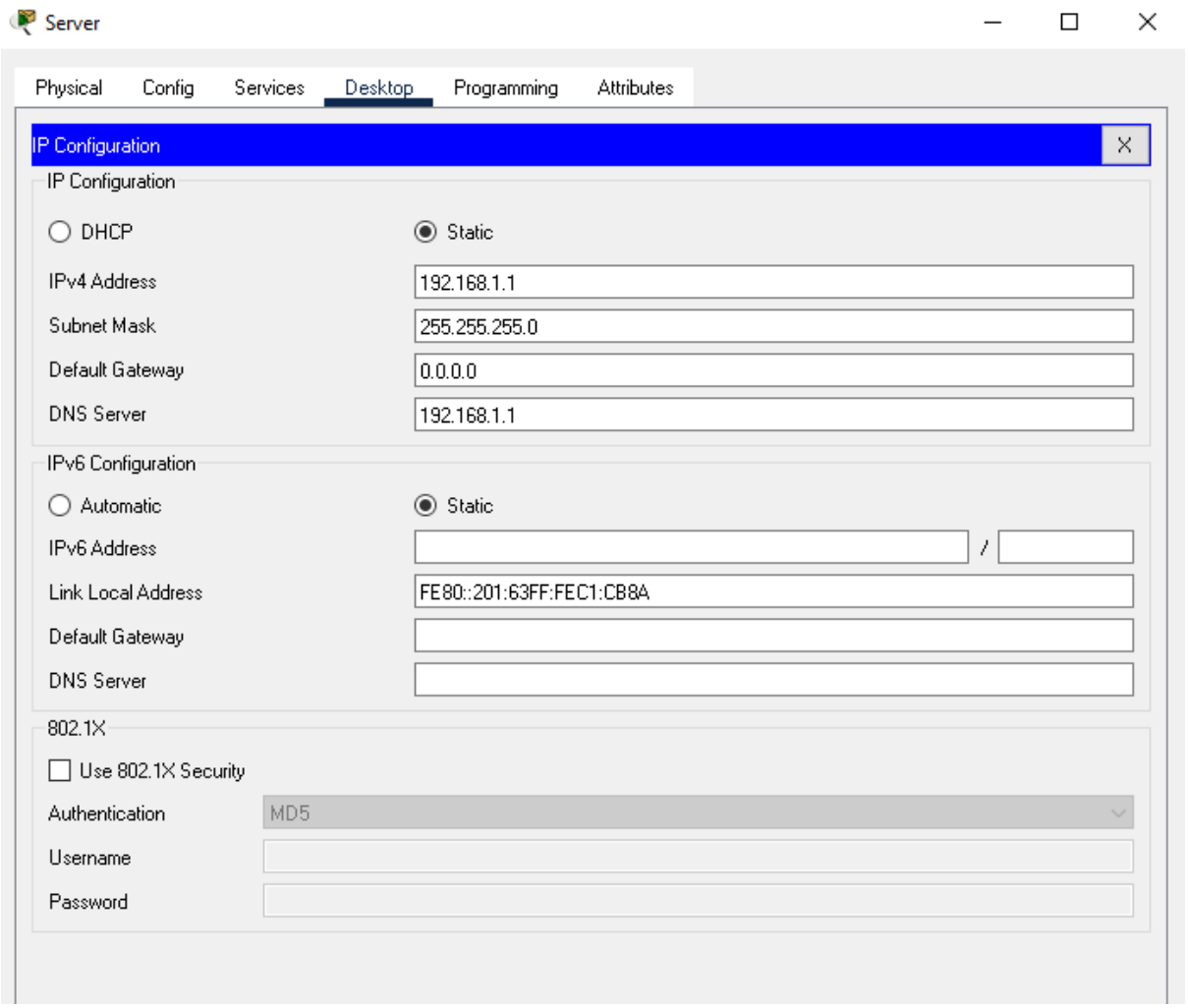


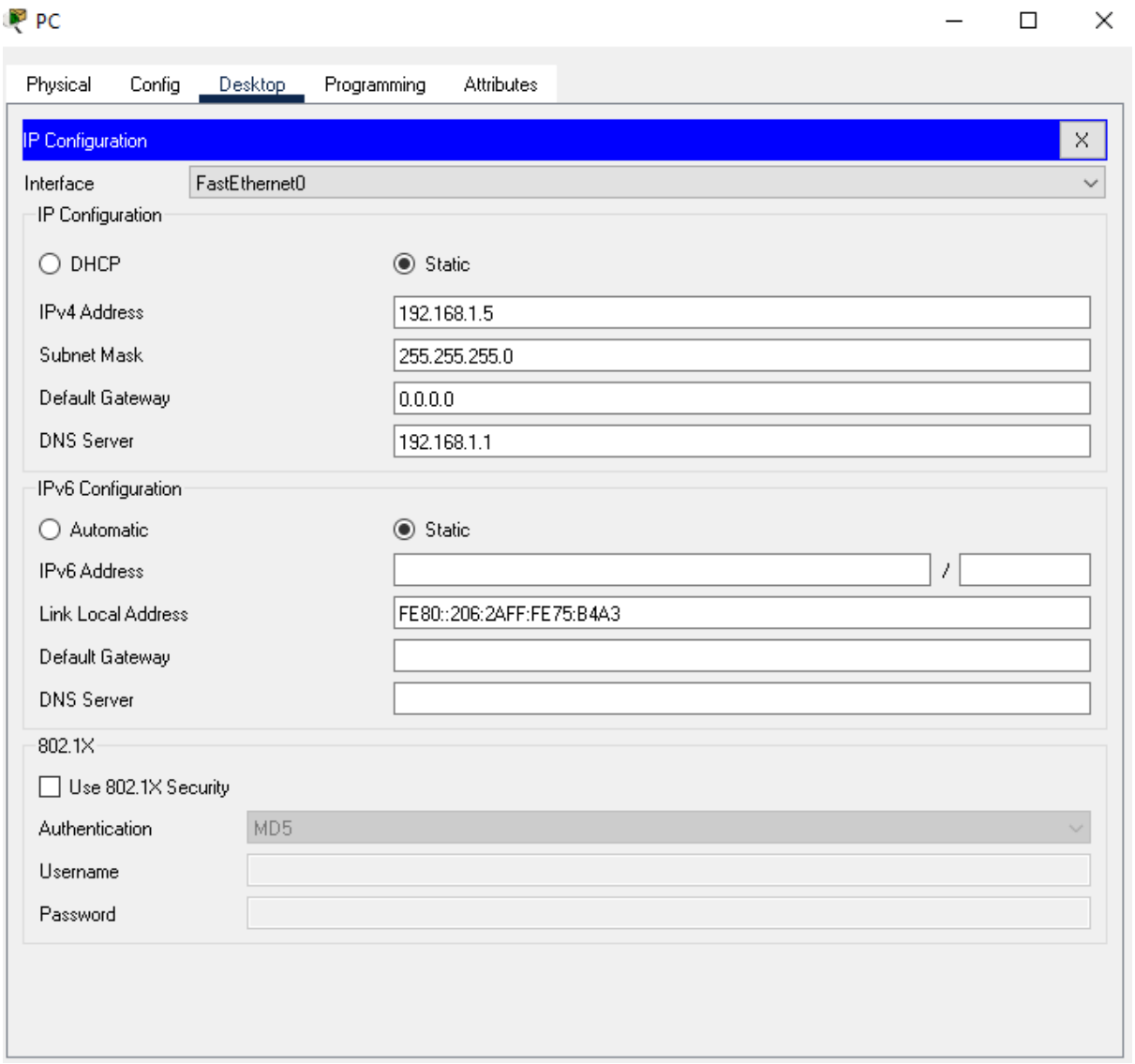
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    Ans: IP Address : 10.30.1.13 It is a local DNS Server.
17. Examine the DNS query message. How many questions does the query have? Does the query message contain any “answers”?
    It contains 1 question and 0 answers.
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?
    It contains 3 answers. It contained the name,type,class and browser name address. It also contains additional information about authoritative server information and their IP Address.

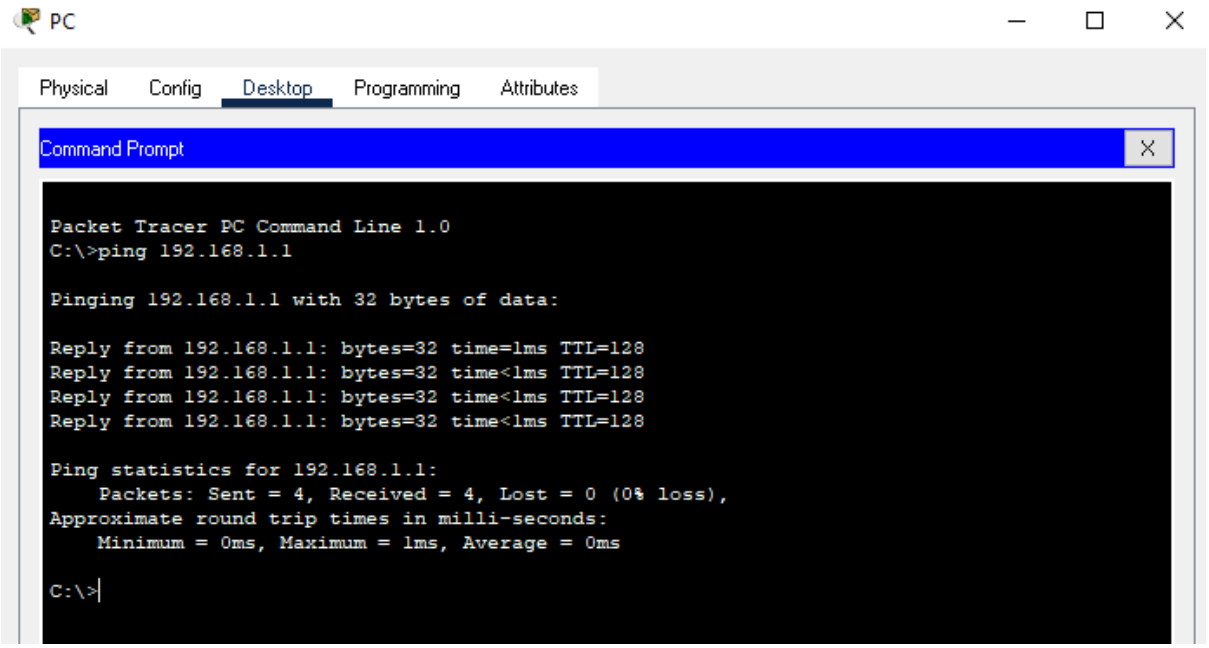
3. Implement a DNS server in packet tracer and understand how it works.






Server
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.1
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
192.168.1.1
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::201:63FF:FEC1:CB8A
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password


PC
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.5
Subnet Mask
255.255.255.0
Default Gateway
0.0.0.0
DNS Server
192.168.1.1
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::206:2AFF:FE75:B4A3
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password


PC
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>


Server0
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
File Name: index.html
<html>
you are visiting www.janakar.com
</html>