

ICMP & DNS

OMIS 660



COURSE NAME: BUSINESS COMPUTING ENVIRONMENT AND

NETWORKS (OMIS 660)

DEPARTMENT: OPERATIONS MANAGEMENT AND

INFORMATIONS SYSTEM

DONE BY : P.CHAITANYA SWAROOP (Z1853880)

HEMANTH TUMMALA (Z1850110)

DATE OF SUBBMISSION: 12I-04-2018

**LAB SUMMARY:**

In this lab with the use of Wireshark we get to know in depth how the ICMP and DNS servers work. We get an idea on how the ICMP messages are generated by the Ping program and the Traceroute program. With this lab we will be familiar with “nslookup” and ipconfig, we capture the DNS packets that are created by web serving activity.

**LAB OBJECTIVES:**

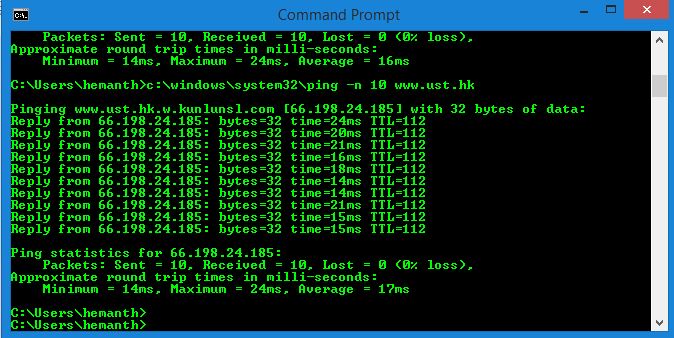
* To capture packets created with ping program with the help of Wireshark.
* To capture packets created with traceroute program with the help of Wireshark.
* To get closer look at client side of the DNS server.

ICMP

Step 1:

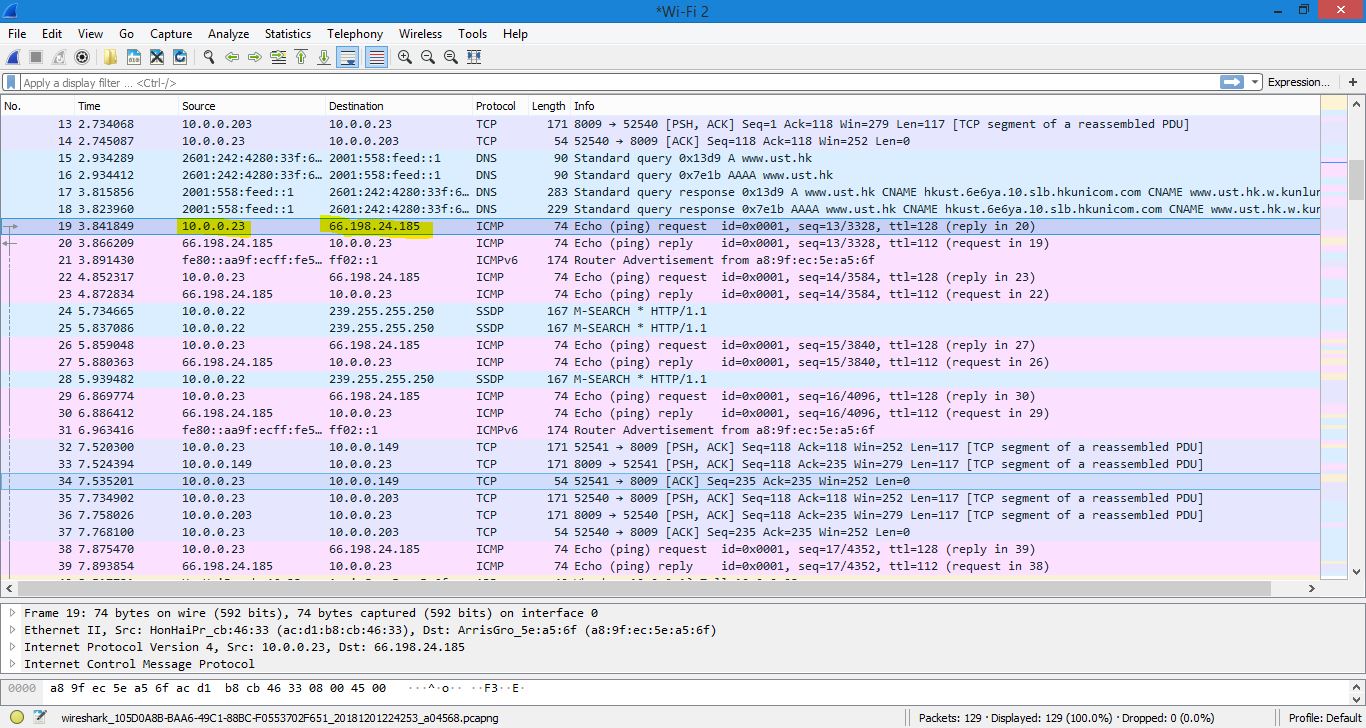
Open windows command prompt and type “c:\windows\system32\ping –n 10 [www.ust.hk](http://www.ust.hk)”

and click enter.



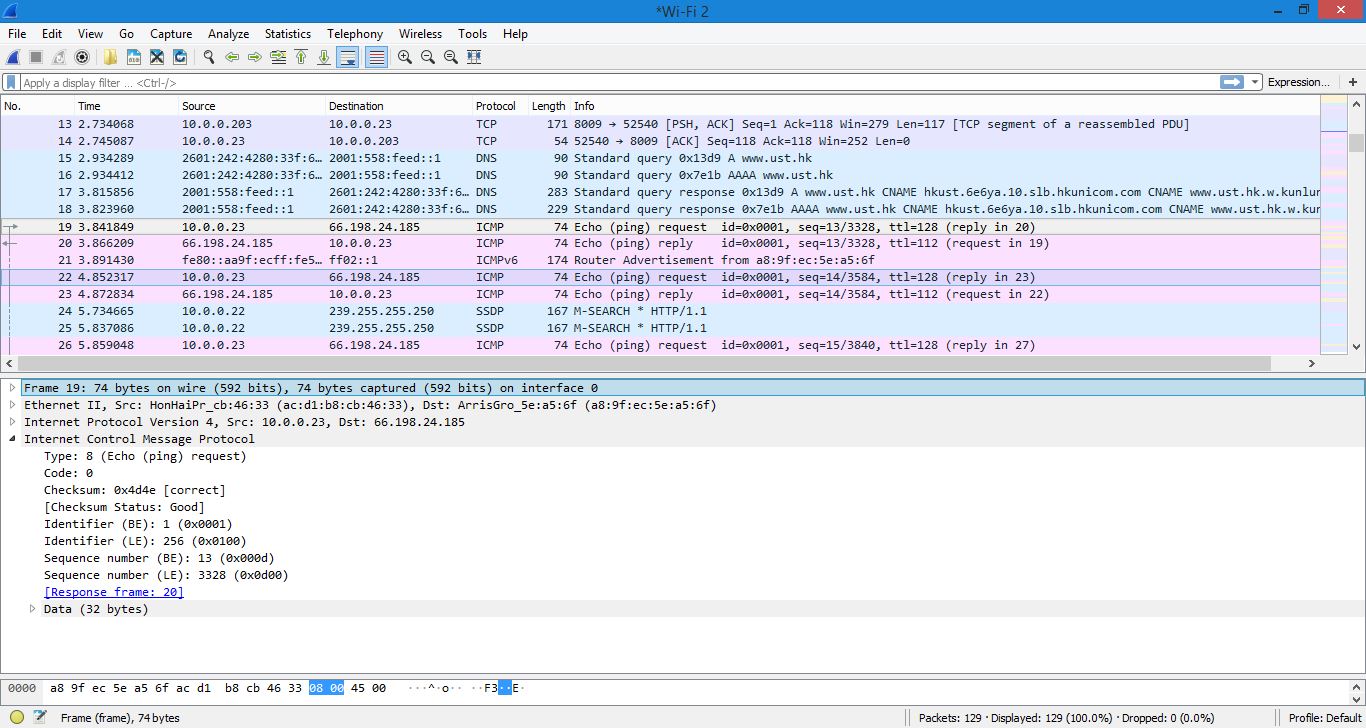
Step 2:

After clicking on enter run the wireshark and when the command prompt terminates we have to stop the wireshark.



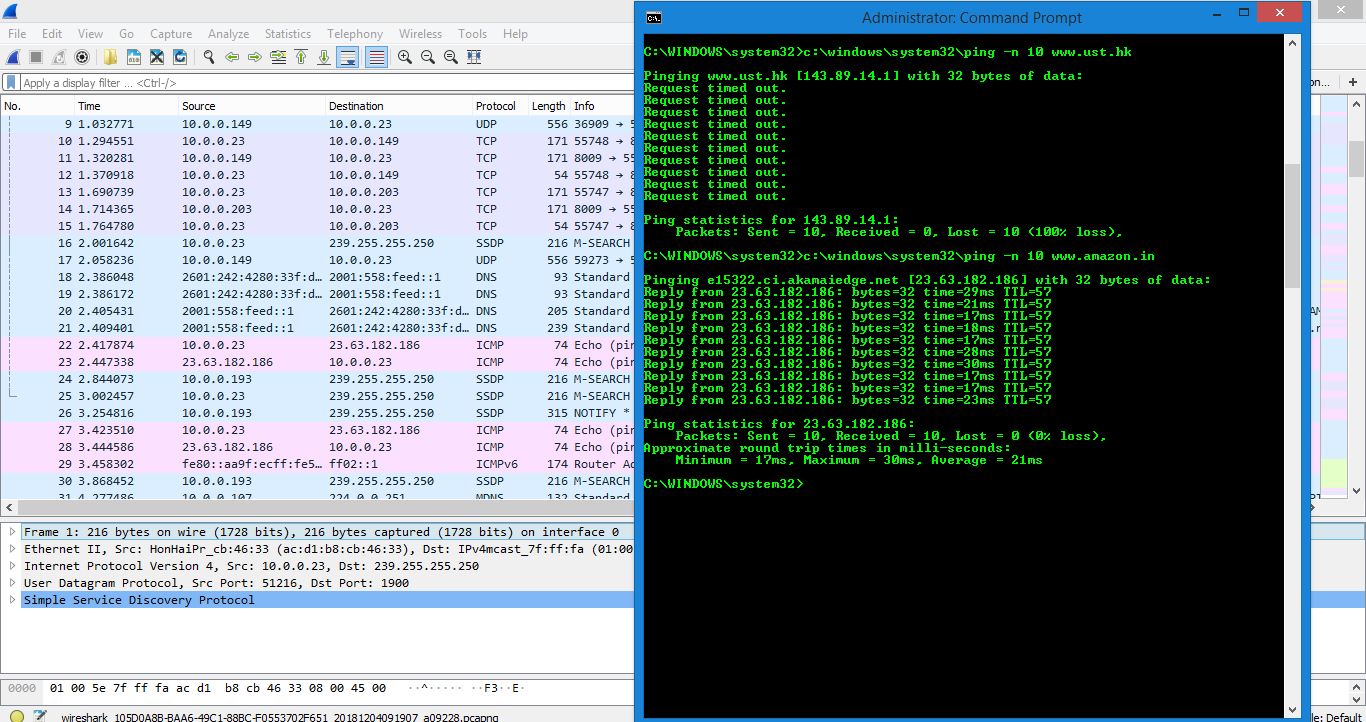
Step 3:

Now capture the first ping packet with ICMP packet expanded.



\*\*\*We have done the screenshots at first then we realized that we need to attach the trace work so, while doing the trace we are getting error for the website [www.ust.hk](http://www.ust.hk)

So we have use [www.amazon.in](http://www.amazon.in).



Here is the trace:



1. What is the IP address of your host? What is the IP address of the destination host?

Ans: Source IP : 10.0.0.23

Destination IP : 66.198.24.185

2. Why is it that an ICMP packet does not have source and destination port numbers?

Ans: The ICMP parcel does not have source and destination port numbers because they communicate in network layer rather it has TYPE and Code .

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Ans: Type : 8

Code : 0

The other fields are Checksum, identifier , sequence number and data fields

CheckSum : 2 bytes

Sequence number : 2 bytes

Identifier : 2 bytes

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

Ans : Type : 0

Code : 0

The other fields are Checksum, sequence number , identifier and data fields

Checksum: 2 bytes

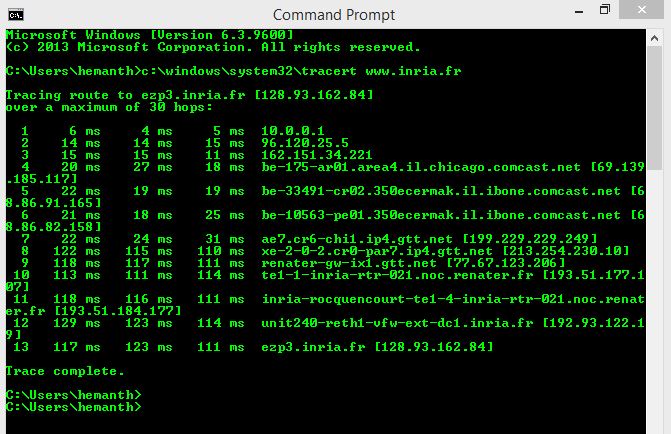
Sequence number : 2 bytes

Identifier : 2 bytes

Step 4:

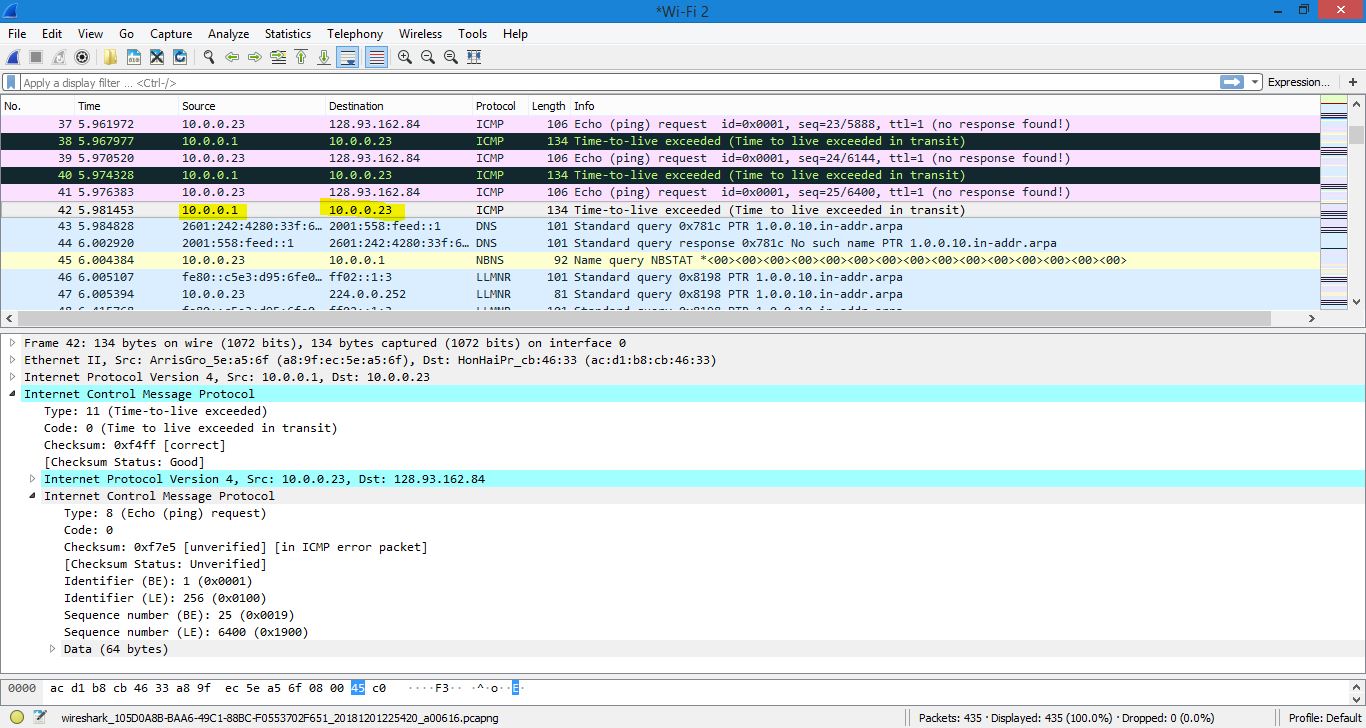
Open the windows command prompt and type”c:\windows\system32\tracert [www.inria.fr](http://www.inria.fr)”

and click enter.



Step 5:

After clicking on enter run the wireshark.



Here is the trace:



5. What is the IP address of your host? What is the IP address of the target destination host?

Ans: Source IP: 10.0.0.1

Destination IP: 10.0.0.23

6. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

Ans: The ICMP packet has the same fields as the PING packet

7. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

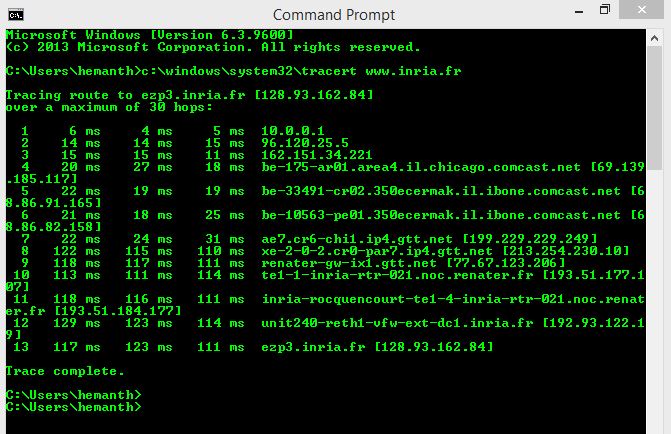
Ans: The ICMP packet is not same as PING packet , it contains the IP header and first 8 bytes of original ICMP packet that the error if for.



8. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

Ans: The last 3 ICMP packets are message type 0 but the previous packets have type 11 and they are different because the datagram have made it all the way to the destination host before the TTL expired.

9. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to your own trace (CMD), is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

Ans: 

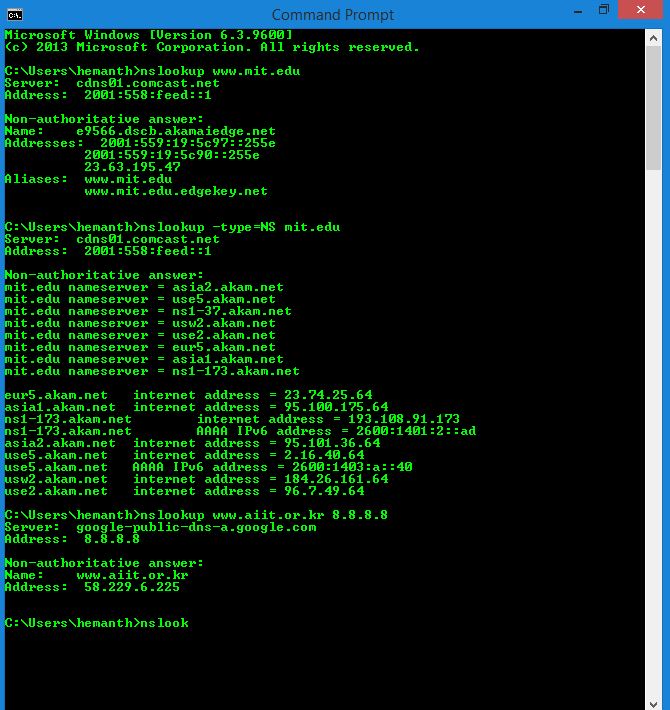
DNS

Step 1:

Open command prompt and type “nslookup [www.mit.edu](http://www.mit.edu)”

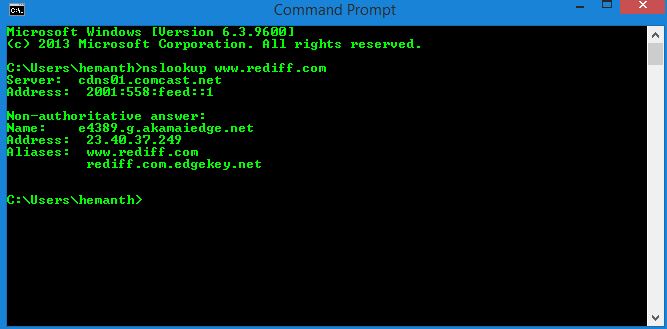
“nslookup –type=NS mit.edu”

“nslookup [www.aiit.or.kr](http://www.aiit.or.kr) bitsy.mit.edu”



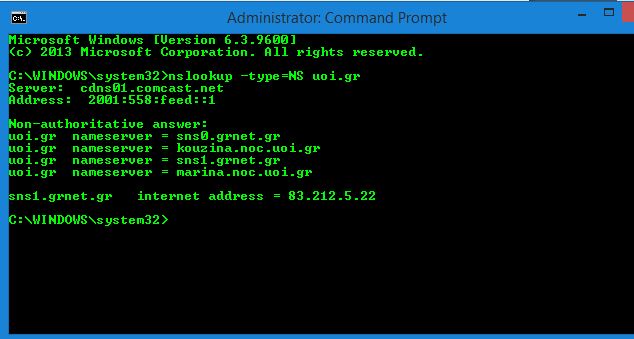
1. Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server? (for example: [www.rediff.com](http://www.rediff.com))

Ans :



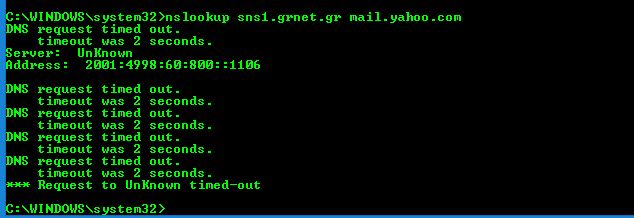
2. Run nslookup to determine the authoritative DNS servers for a university in Europe. (for example: uoi.gr)

Ans :



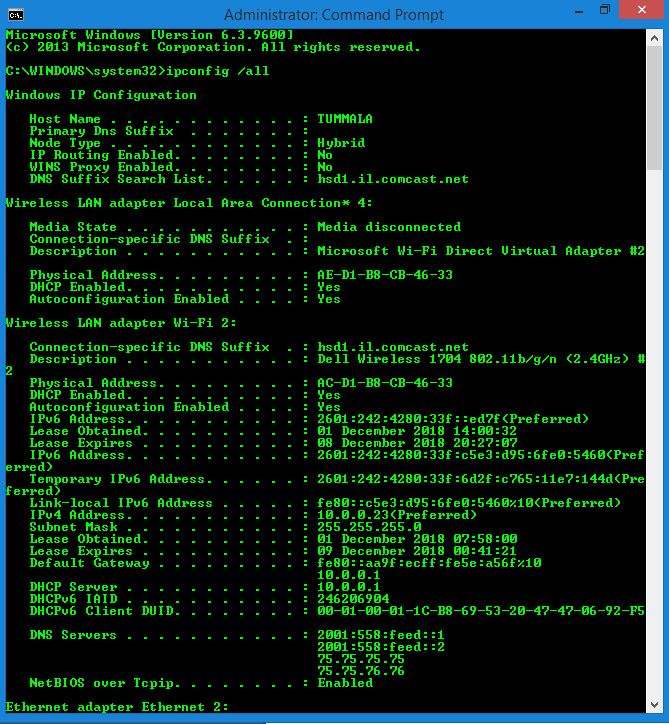
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! Mail (mail.yahoo.com). What is its IP address?

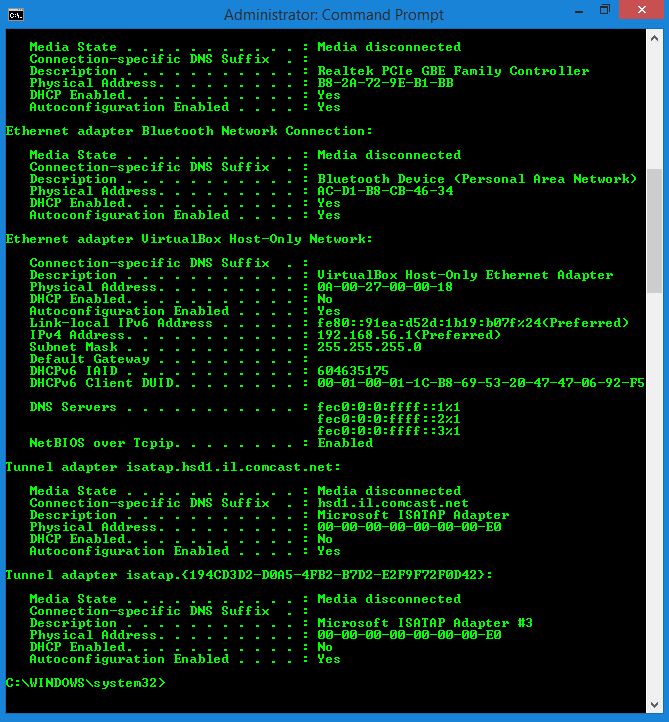
Ans:



Step 2:

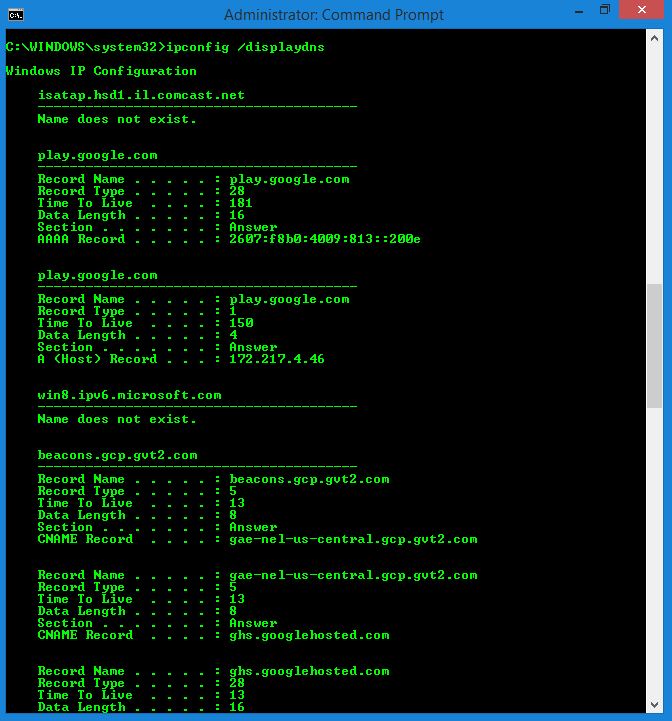
Open command prompt and type “ipconfig /all”

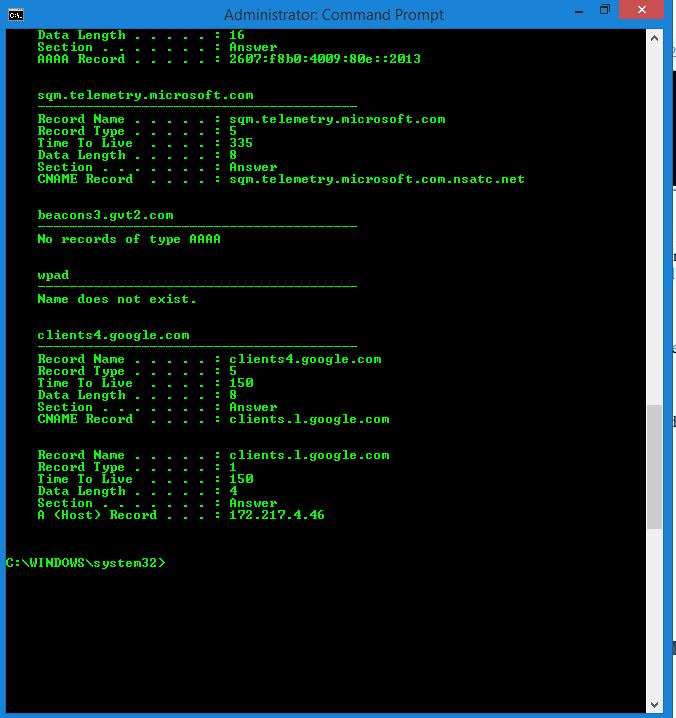




Step 3:

Open Command prompt and type “ipconfig /displaydns”





Step 4:

Open command prompt and type “ipconfig /flushdns”



Step 5:

Now To track DNS with wireshark.

Open command and use ipconfig /flushdns to clear the cache.

Open the browser and delete the cache manually.

Now open the wireshark and type “ip.addr = = 192.168.56.1(system ip address)” in the filter.

And start the wireshark and capture the packets.

Now open the browser with the web page : <http://www.ietf.org>.

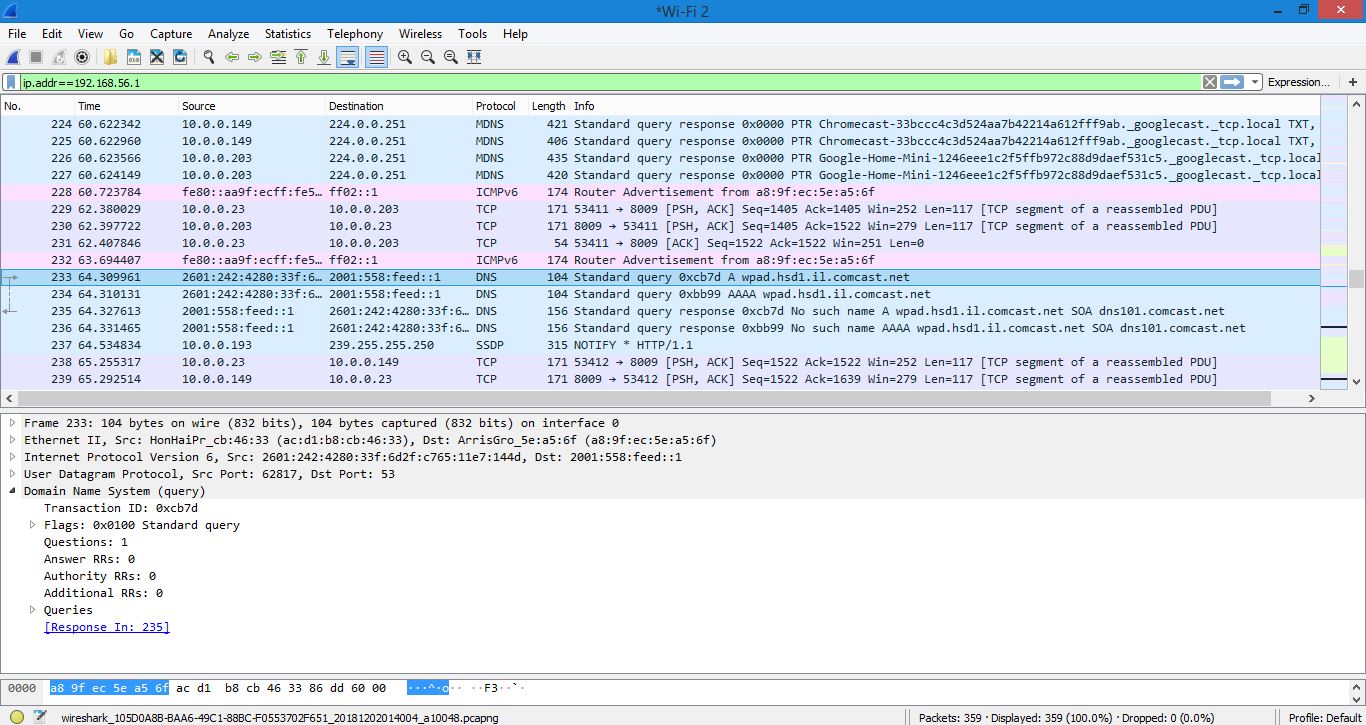
Now stop capturing packets.

Here is the trace:



4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

Ans : sent over UDP.





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

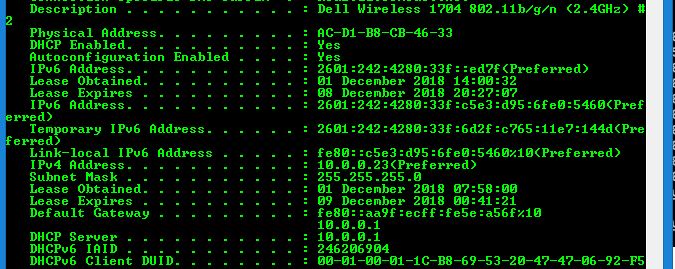
Ans:

Source port : 52623

Destination port : 53

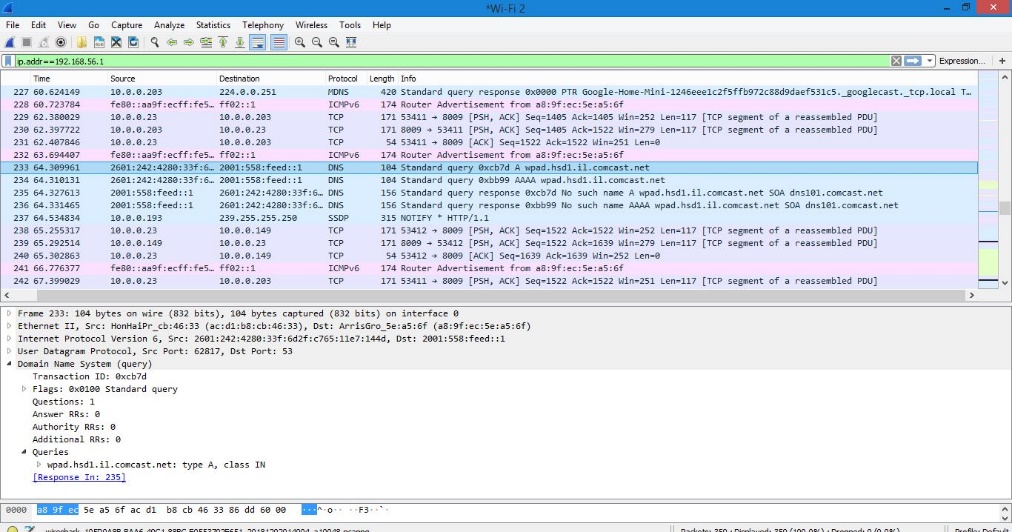
6. To what IP address is the DNS query message sent? Use ipconfig/all to determine the IP address of your local DNS server. Are these two IP addresses the same?

Ans : The IPv6 address is : 2601:242:4280:33f:c5e3:d95:6fe0:5460



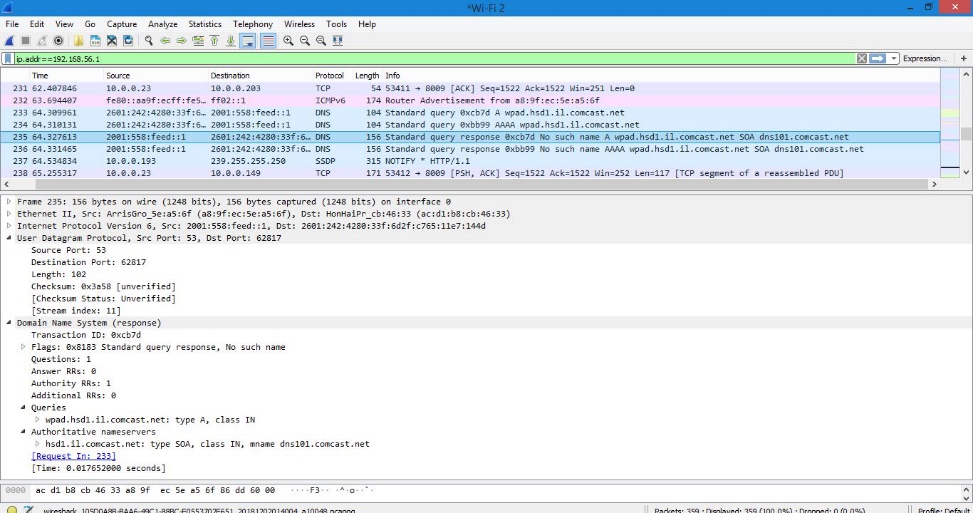
7. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

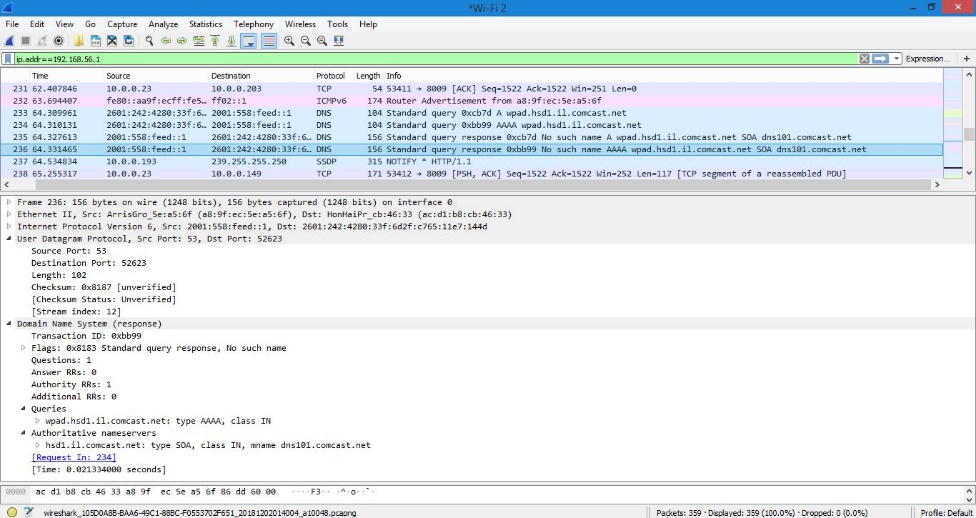
Ans: The Type is : A and it doesn’t contain any answers.



8. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

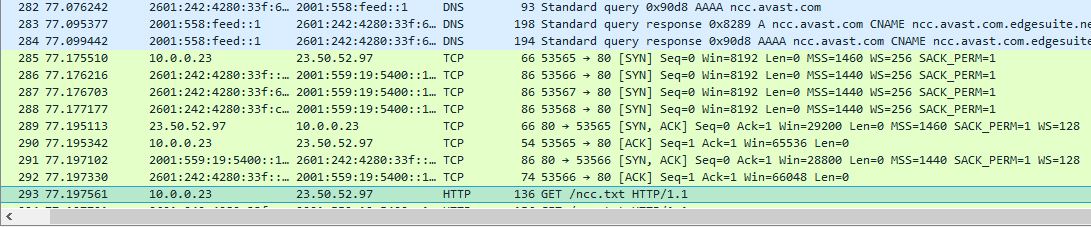
Ans: There were 2 answers containing information about the name of the host, the type of address, class, the TTL, the data length and the IP address, they are:





9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

Ans: The first SYN packet was sent to 23.50.52.97 which corresponds to the first IP address provided in the DNS response message.



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

Ans: NO.

Step 6:

Open wireshark and start capturing packets.

Open command prompt and type “nslookup [www.mit.edu](http://www.mit.edu)” and click enter

Now stop capturing packets in the wireshark

And now type “ip.addr = = 192.168.56.1” in the filter .

Here is the trace:

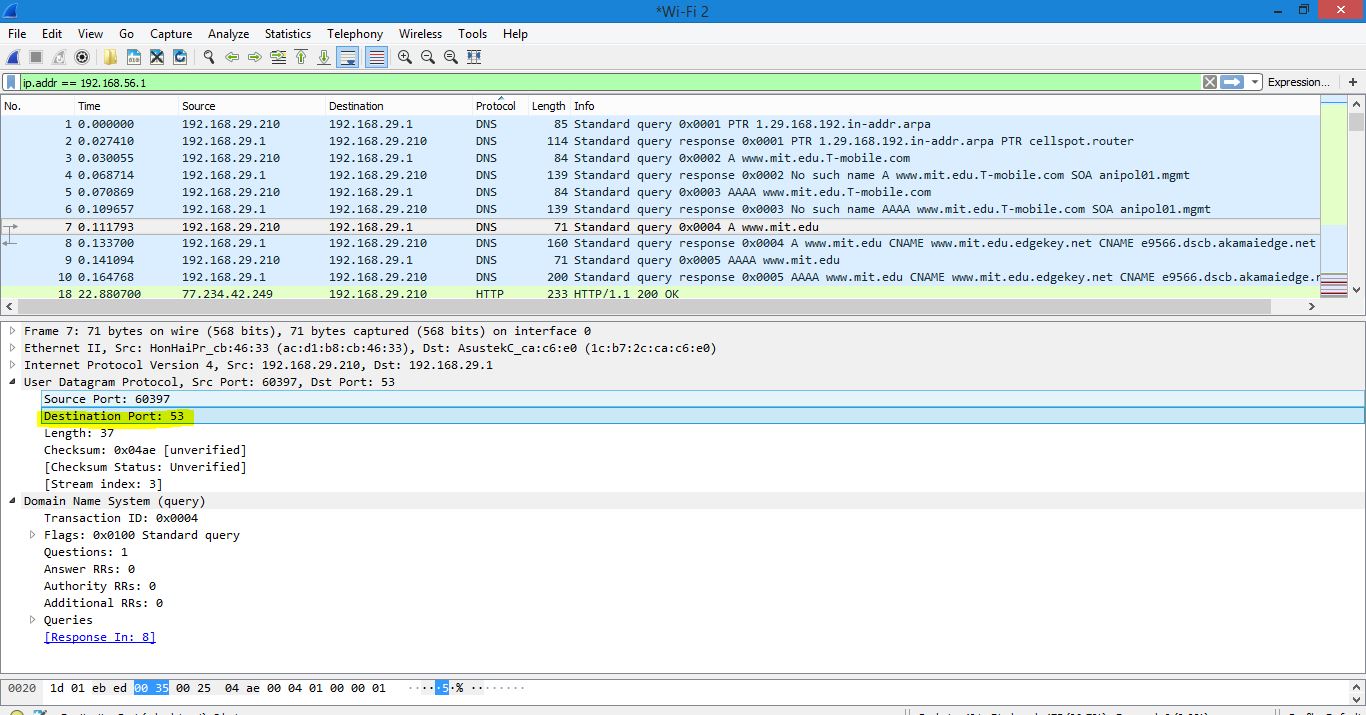


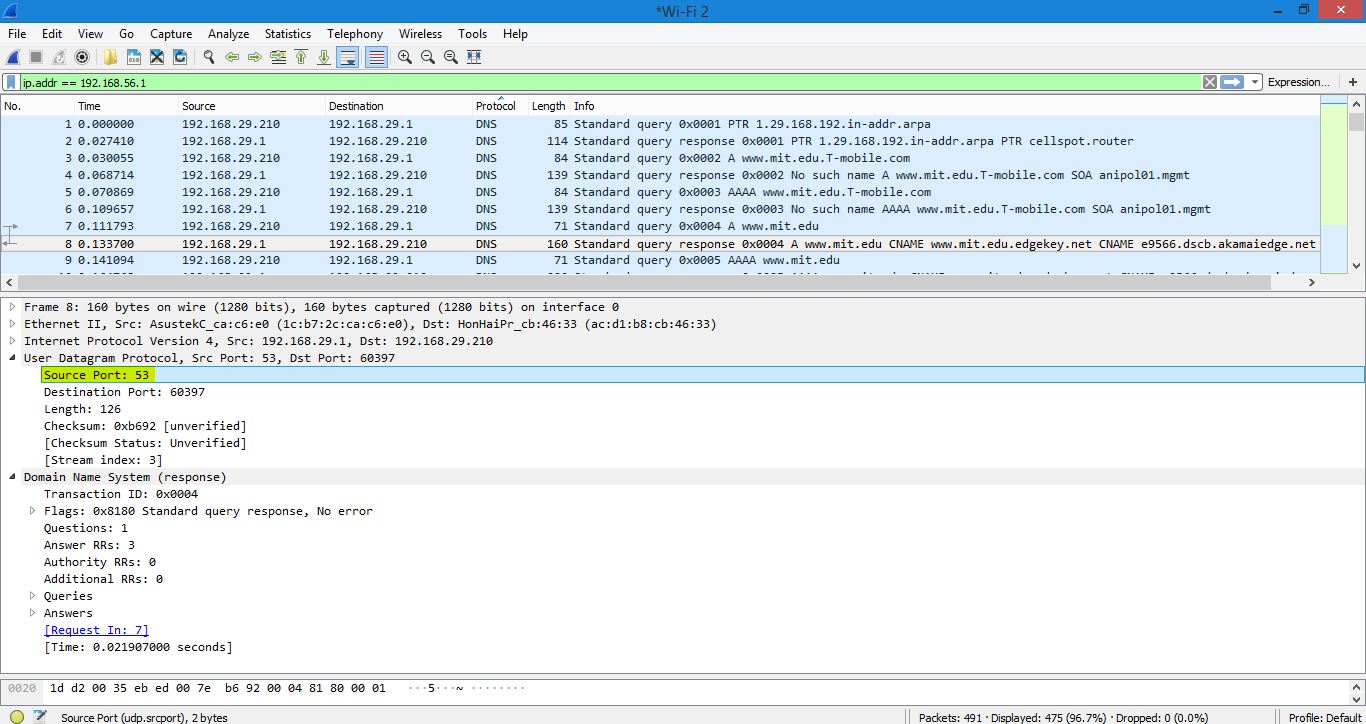
11. What is the destination port for the DNS query message? What is the source port of DNS response message?

Ans:

Destination port : 53

Source port : 53



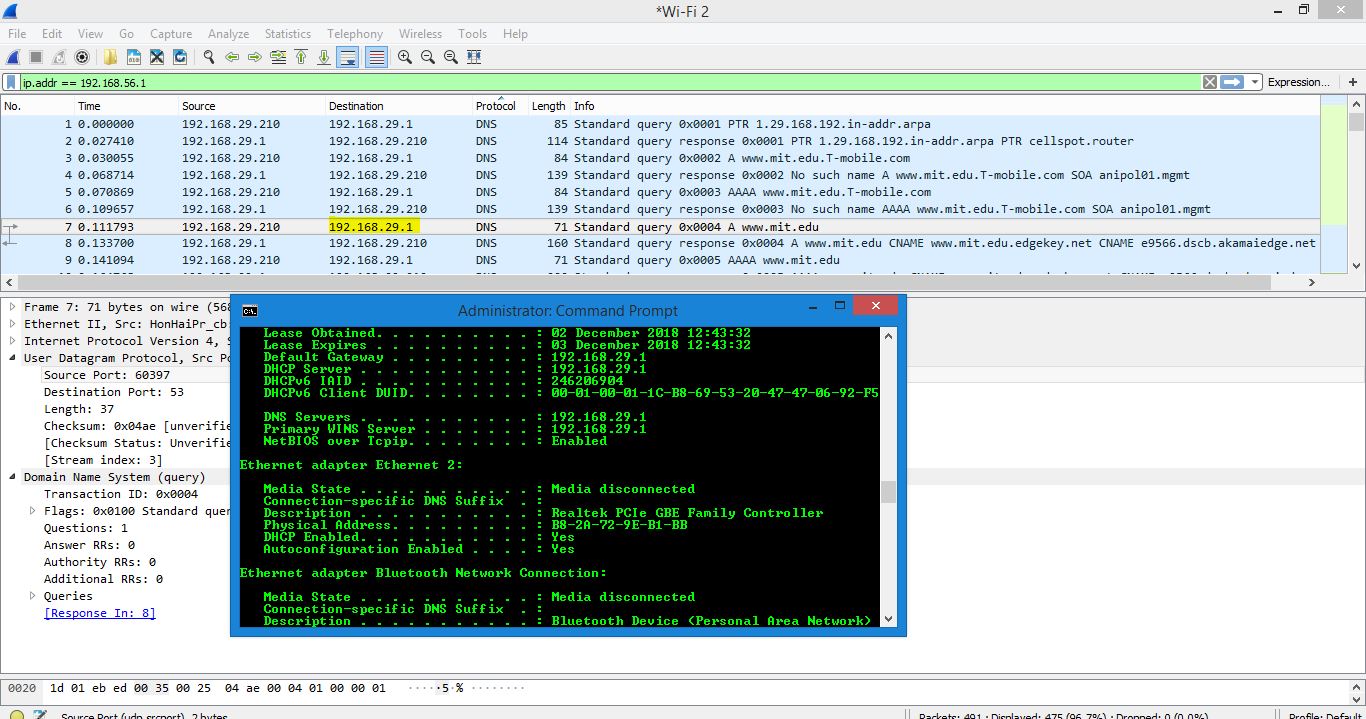


12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

Ans:

The message is sent to the IP address of my default local DNS server and the IP address is:

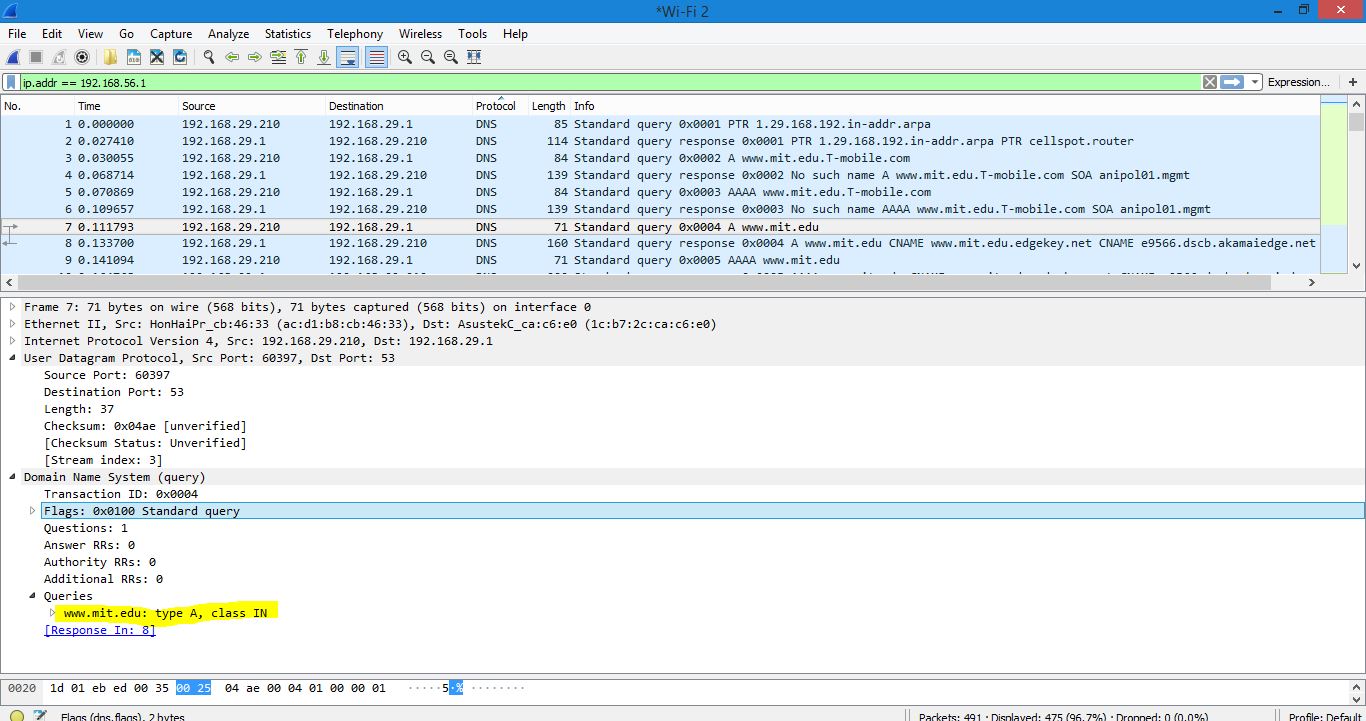
192.168.29.1.



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

Ans:

The Type is : A and it doesn’t contain any answers.



14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

Ans:

There are 2 answers and they contain:

[www.mit.edu](http://www.mit.edu): type CNAME, class IN , cname [www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net)

Name: [www.mit.edu](http://www.mit.edu)

Type: CNAME (canonical NAME for an alias) (5)

Class : IN (0x0001)

Time to live: 1800

Data length: 25

CNAME: [www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net)

[www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net): type CNAME, Class IN , cname e9566.dscb.akamaiedge.net

Name: [www.mit.edu.edgekey.net](http://www.mit.edu.edgekey.net)

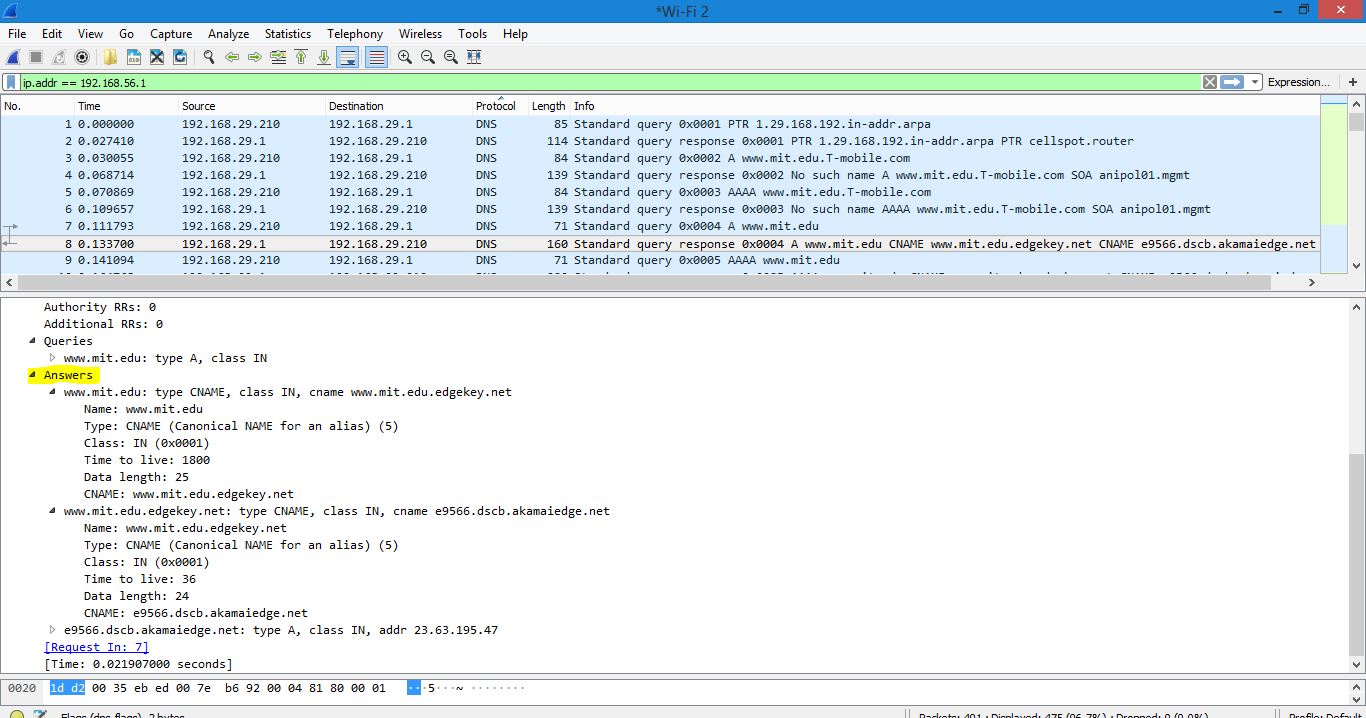
Type: CNAME (canonical NAME for an alias) (5)

Class : IN(0x0001)

Time to live: 36

Data length : 24

CNAME: e.9566.dscb.akamaiedge.net



**CONCLUSION:**

With the help of Wireshark, the packets generated by the ping program and the traceroute program have been captured. We were able to get a closer look on the client side of the DNS server. The lab helped us to get to know a lot of things like the use of Wireshark to capture packets and to get a in depth knowledge of the DNS server and also the traceroute and ping program.