**Title of the Lab:** Wireshark / DNS

**Name:** MITHUN MARAGIRI

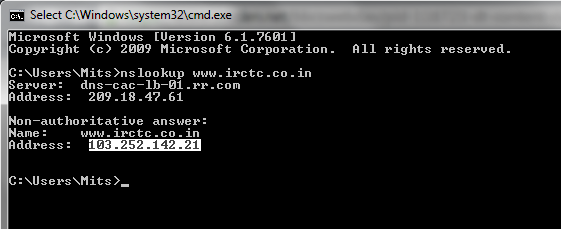
**Session #:** 2

**Course:** EE-450

1. Run nslookup to obtain the IP address of a Web Server in Asia. What is the IP address of that server?

Ans: The web server looked up is [www.irctc.co.in](http://www.irctc.co.in) which is based in India.

The IP address of this web server is “103.252.142.21”

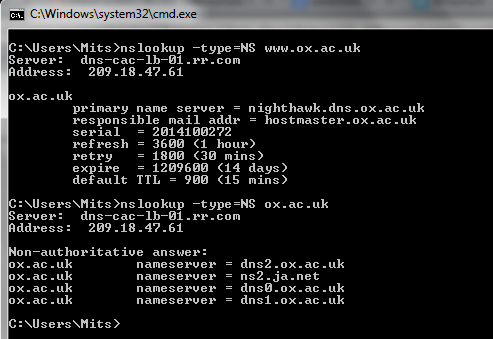


1. Run nslookup to determine the authoritative DNS servers for a university in Europe.

Ans: The university looked up is [www.ox.ac.uk](http://www.ox.ac.uk) which is the University of Oxford, United Kingdom.

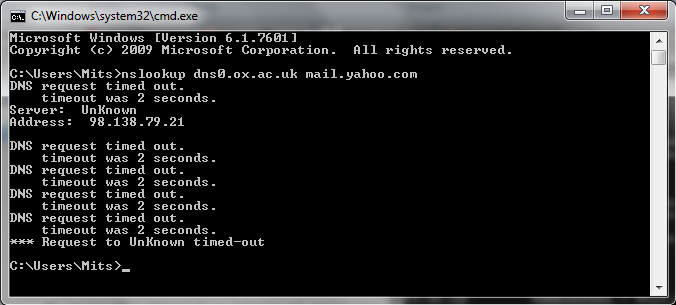
The authoritative DNS Servers are:

**dns2.ox.ac.uk; ns2.ja.net; dns0.ox.ac.uk; dns1.ox.ac.uk**



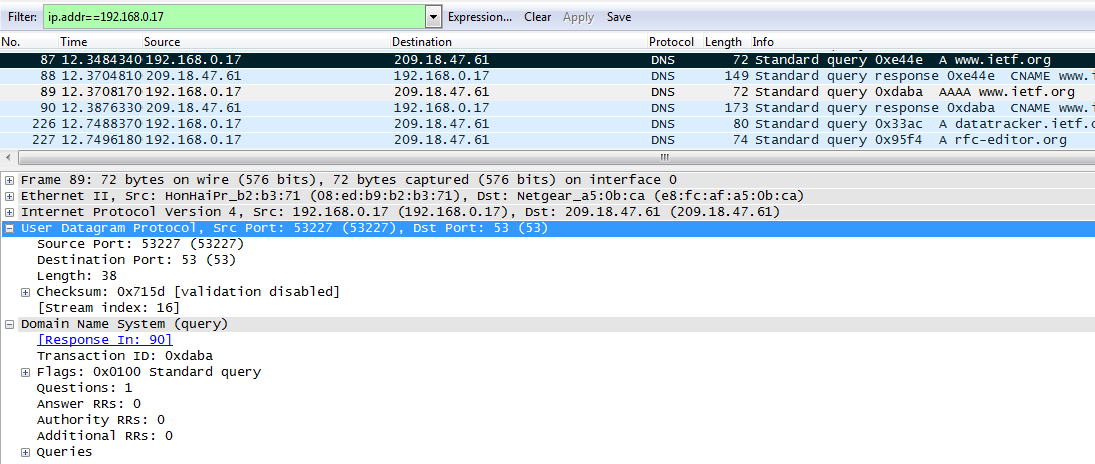
1. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! Mail. What is its IP address?

Ans: nslookup for name server **dns0.ox.ac.uk** is queried for **mail.yahoo.com** the mail server of yahoo. The IP address is **98.138.79.21**

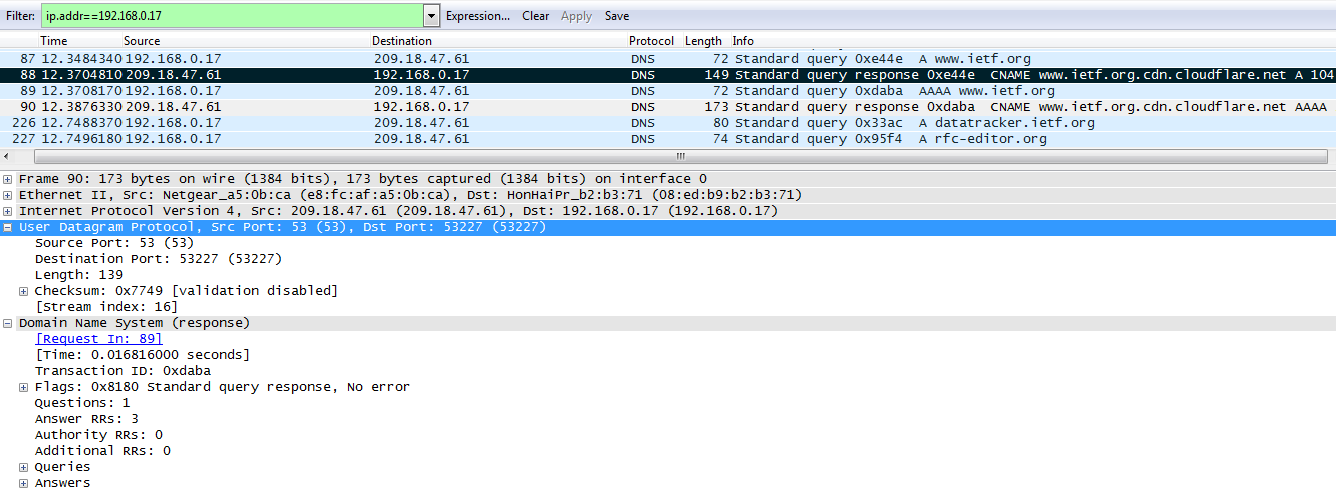


1. Locate the DNS query and response messages. Are they sent over UDP or TCP?

Ans: DNS Query message



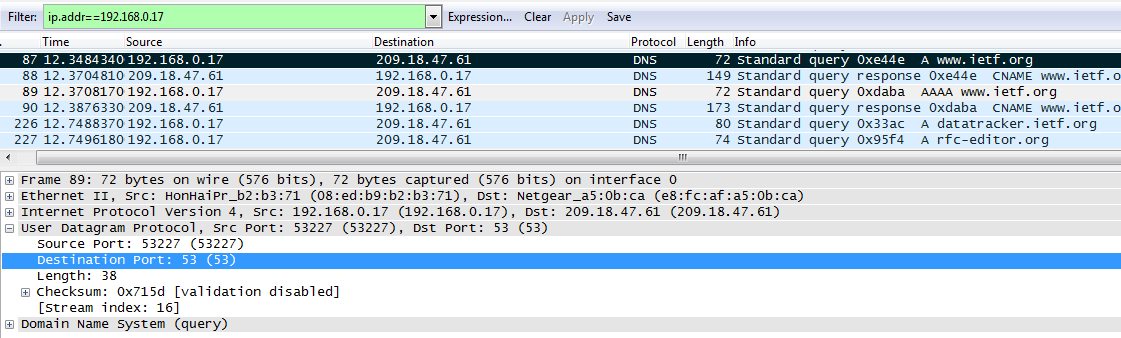
DNS Response Message



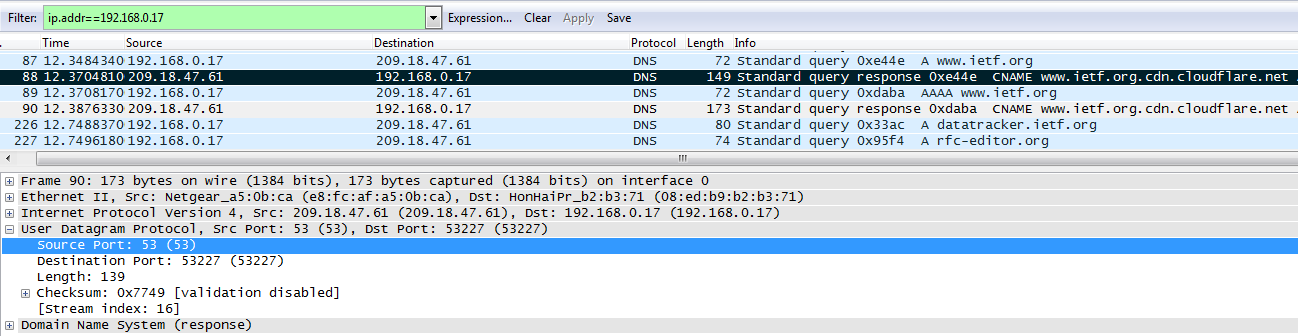
They are sent over UDP.

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

Ans: Destination port for DNS Query message is 53 which is the well known port number for DNS server.

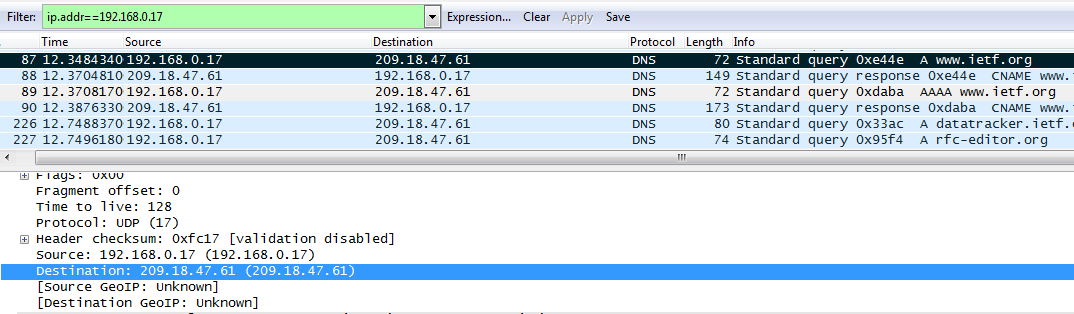


Source Port of DNS response message is 53 which is the well known port number for DNS server.

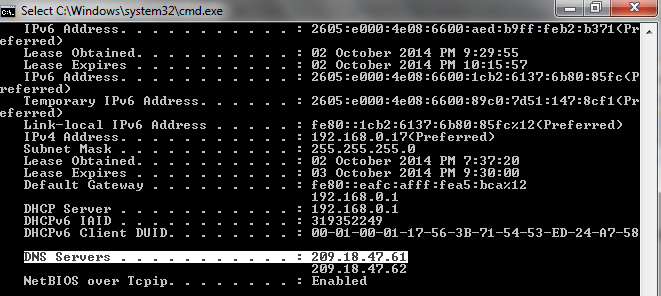


1. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these 2 IP addresses the same?

Ans: DNS query message is sent to 209.18.47.61

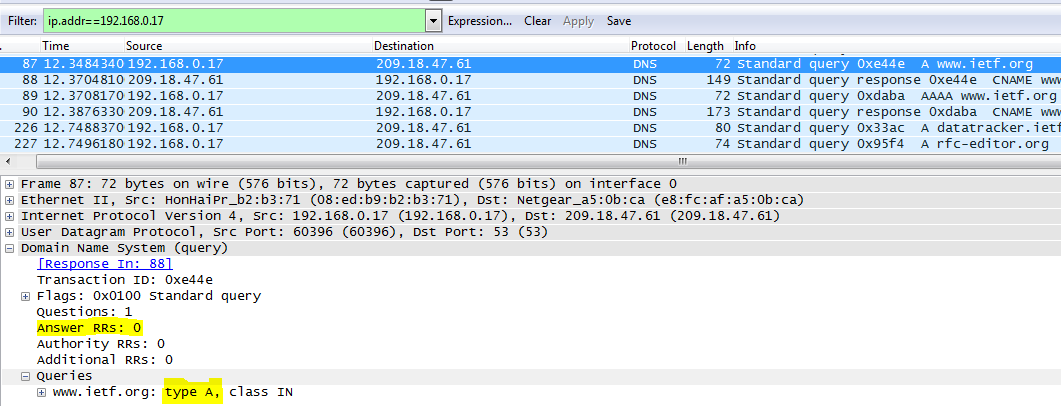


Yes. The IP address of my local DNS server determined by ipconfig is same 209.18.47.61

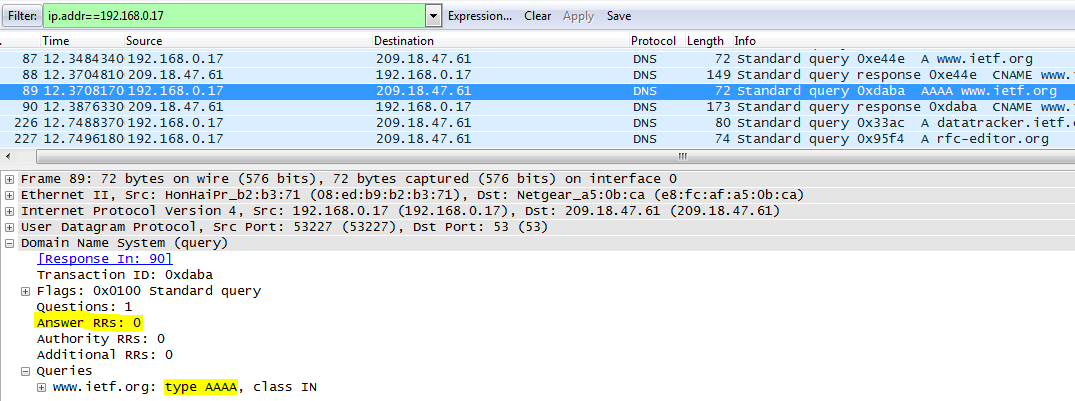


1. Examine the DNS query message. What “Type” of DNS query it is? Does the query message contain any “answers”?

Ans: DNS query Type is “A” (IPV4 address). No the query message does not contain any answers. The Answer RR (Resource Record) count is 0.



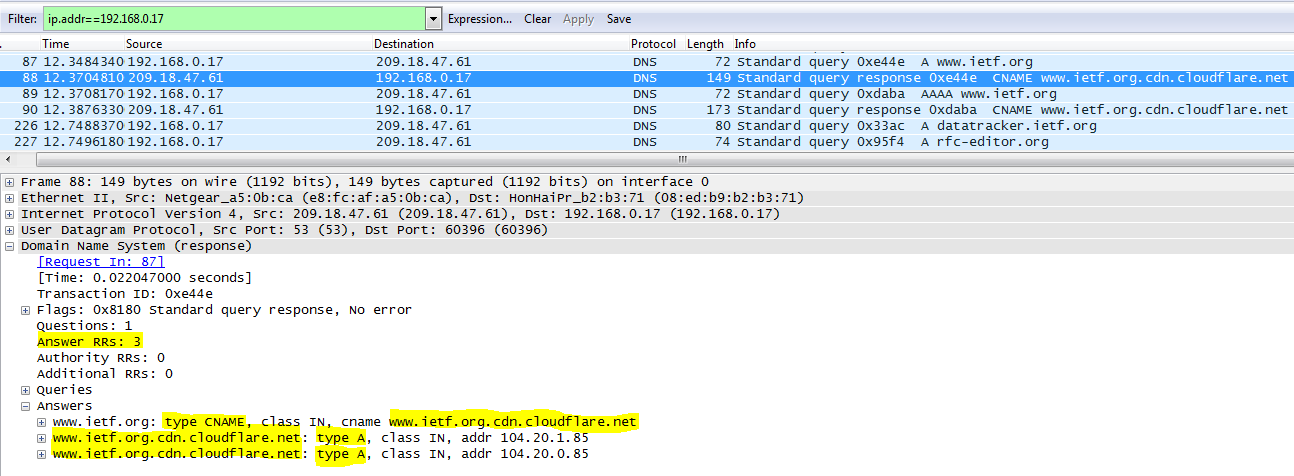
There is “AAAA” (IPV6 address) also being made to the DNS server.



1. Examine the DNS response message. How many “Answers” are provided? What does each of these answers contain?

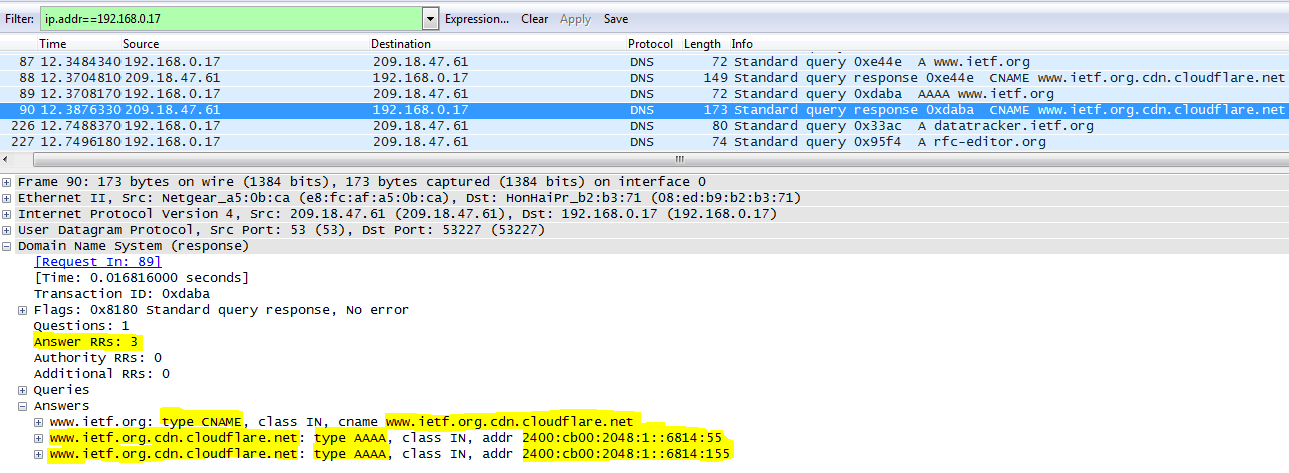
Ans: There are 3 answers in the DNS response message.

* There is 1 CNAME record (Canonical Name) in the answer which gives the canonical name of the server as [**www.ietf.org.cdn.cloudflare.net**](http://www.ietf.org.cdn.cloudflare.net)
* There are 2 A records (IPV4 addresses) corresponding to the canonical name of the DNS server. These IP addresses are **104.20.1.85** and **104.20.0.85**



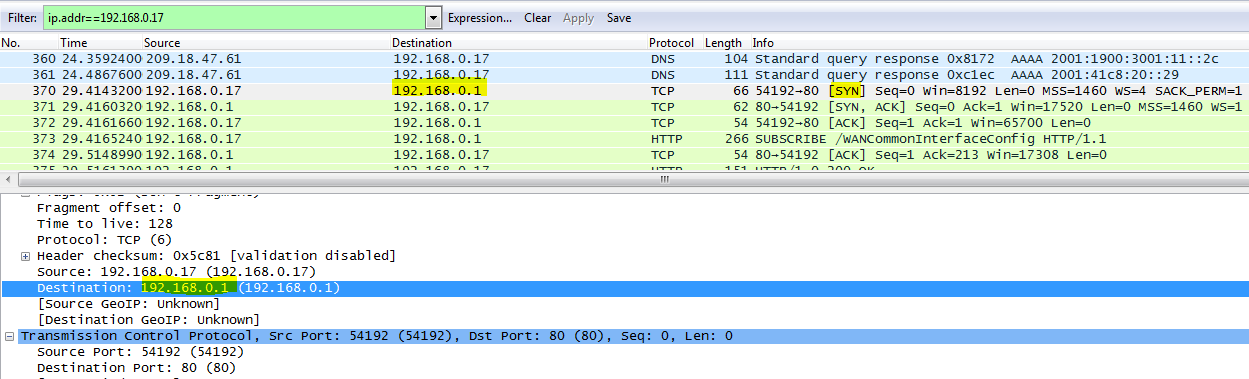
In the case of AAAA query, the response message consists of 2 IPV6 addresses

* **2400:cb00:2048:1::6814:55**
* **2400:cb00:2048:1::6814:155**

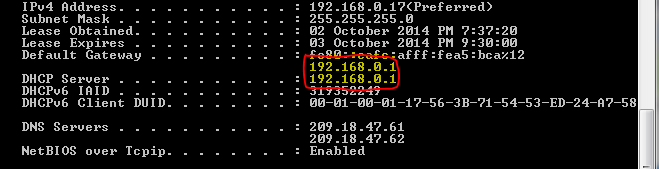


1. Consider the subsequent TCP SYN packet sent by your host. Does the IP address of the SYN packet corresponds to any of the IP addresses provided by the DNS response message?

Ans: The IP address of the SYN packet is the IP address of my Default Gateway 192.168.0.1. The SYN request is acknowledged by my Default Gateway.

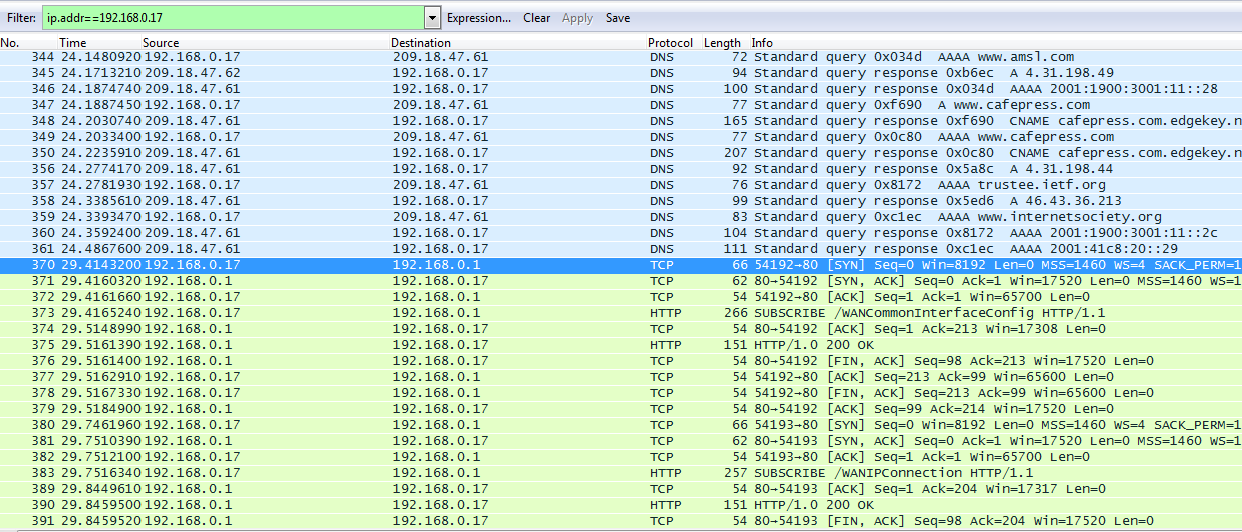


IP address of my default gateway: 192.168.0.1



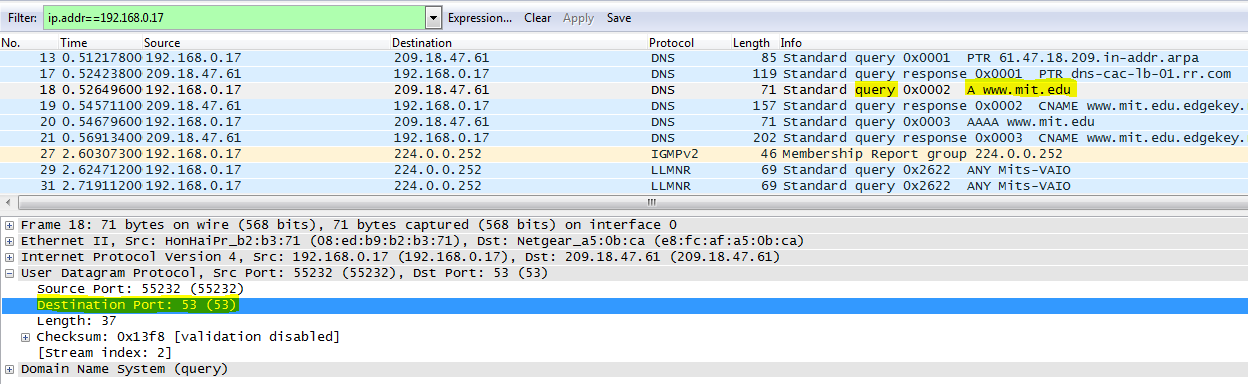
1. This webpage contains images. Before retrieving each image, does your host issue new DNS queries?

Ans: NO. There were no new DNS queries made before retrieving images

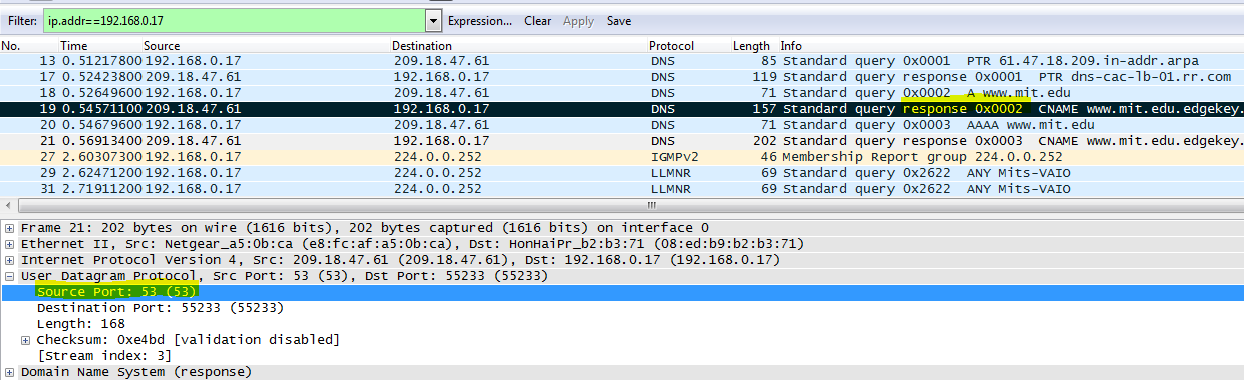


1. What is the destination port for DNS query message? What is the source port of DNS response message?

Ans: The destination Port for DNS query message is 53

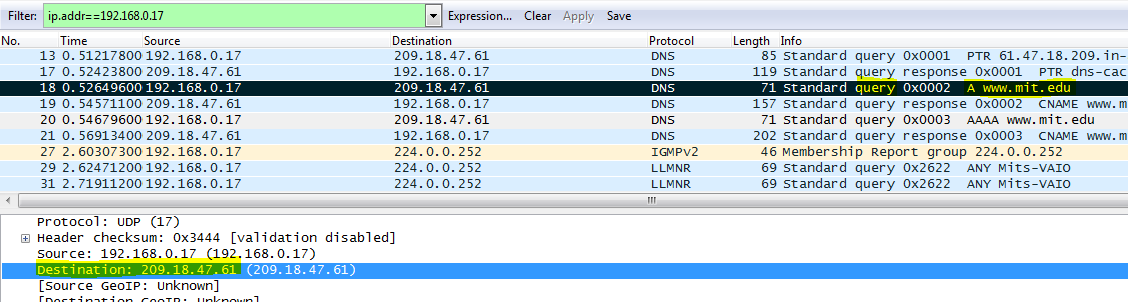


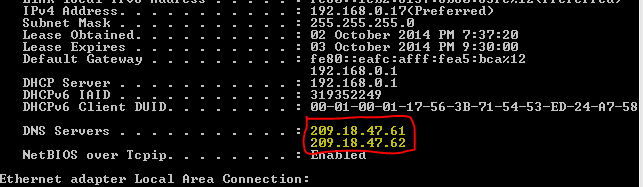
The source port of DNS response message is 53



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

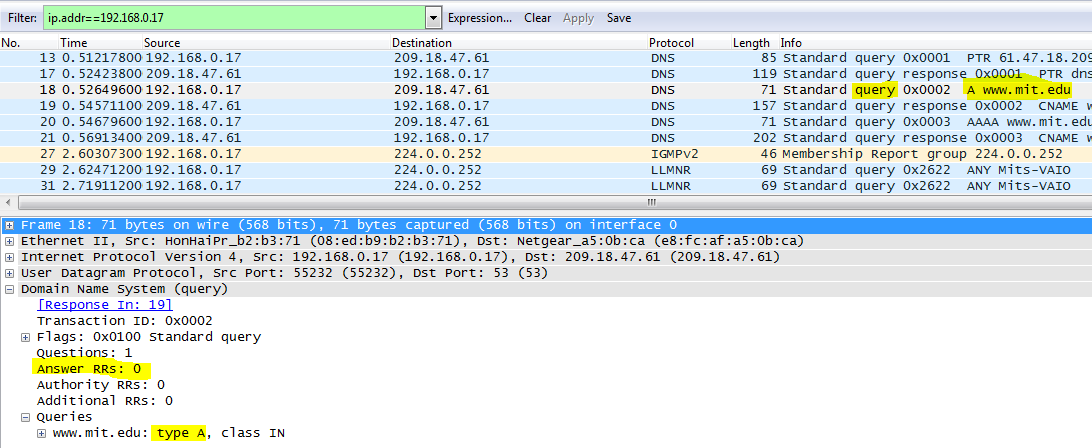
Ans: DNS query message is sent to the IP 209.18.47.61. Yes this is the IP address of my default local DNS server.





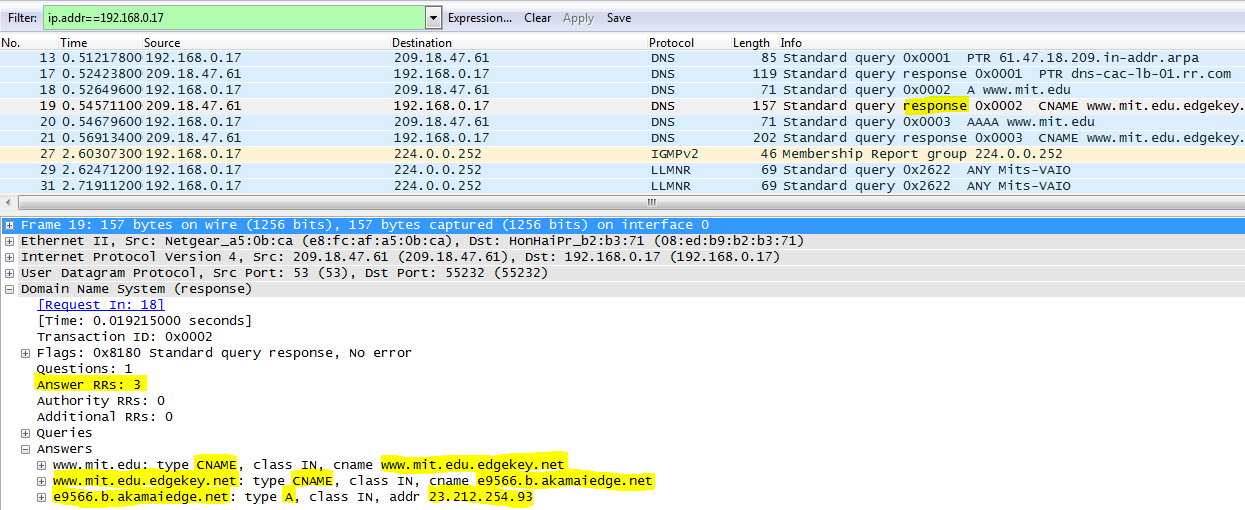
1. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any answers?

Ans: DNS Query type is “A” Query. NO the query message does not contain any answers. The answer record count is 0

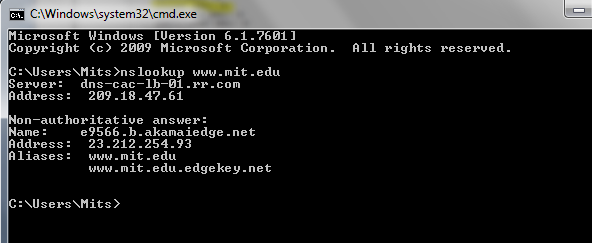


1. Examine the DNS response message. How many “Answers” are provided? What does each of these answers contain?

Ans: There are 3 answers in the DNS response message. The response has 2 CNAME resource records and 1 A resource record. The CNAME records are [**www.mit.edu.edgekey.net**](http://www.mit.edu.edgekey.net) and **e9566.b.akamaiedge.net** and the A record has the IP address **23.212.254.93.**



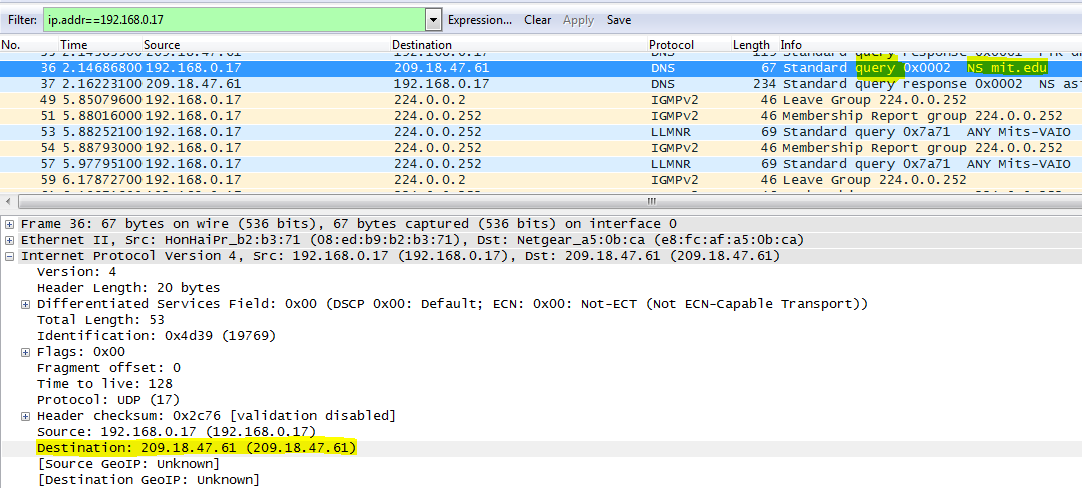
1. Provide a screen shot?



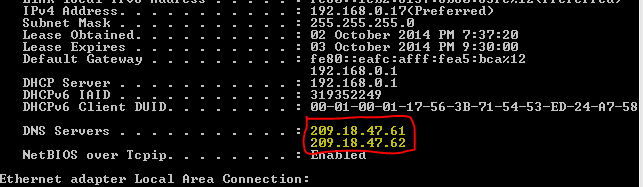
COMMAND: nslookup –type=NS mit.edu

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

Ans: DNS query message is sent to the IP 209.18.47.61. Yes it is the IP address of my default Local DNS server.

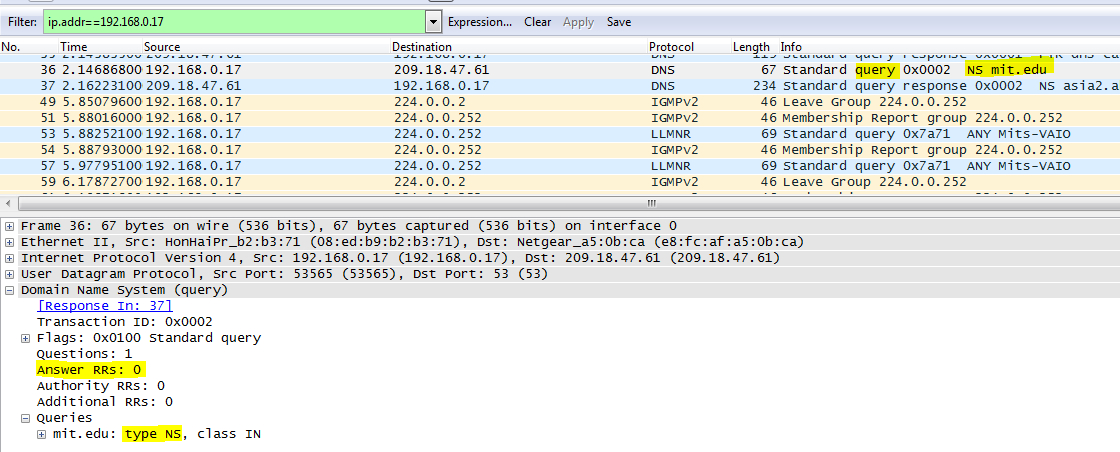


My default Local DNS server



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

Ans: DNS query type is “NS”. No the DNS query message does not contain any answers. The answer resource record count is 0.



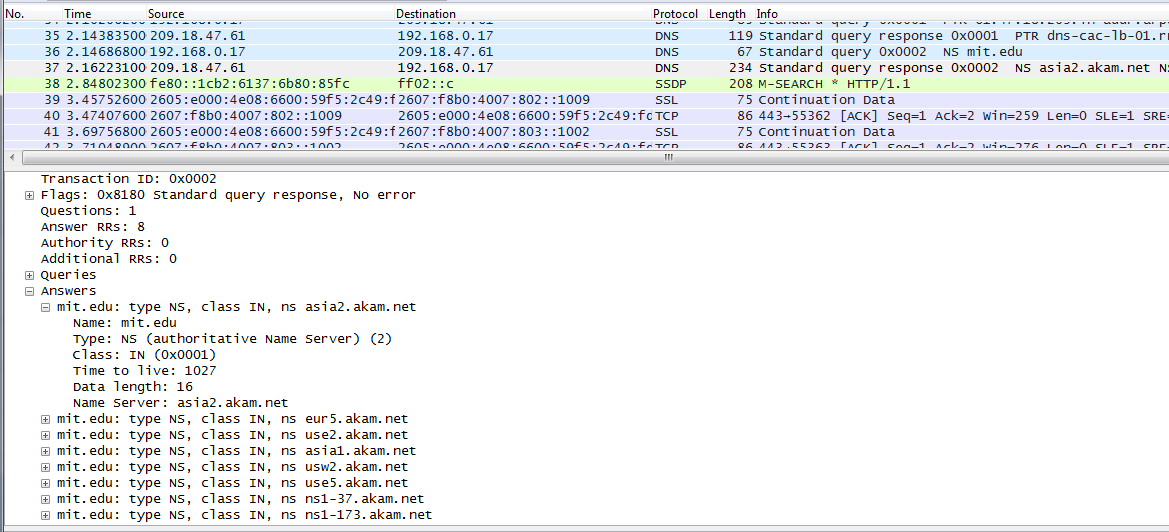
1. Examine the DNS response message. What MIT name servers does the response message provide? Does this response message also provide the IP addresses of MIT name servers?

Ans: Response message provides the following name servers:

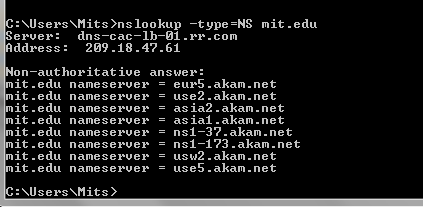
* **asia2.akam.net, eur5.akam.net, use2.akam.net, asia1.akam.net, usw2.akam.net, use5.akam.net, ns1-37.akam.net,**

**ns1-173.akam.net**

NO, the response message does not provide the IP addresses of MIT name servers.



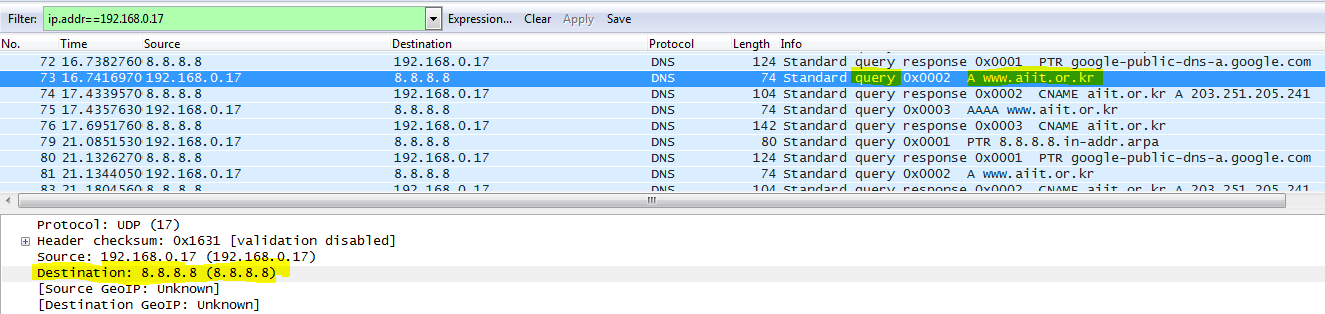
1. Provide a screen shot.



COMMAND: nslookup [www.aiit.or.kr](http://www.aiit.or.kr) 8.8.8.8

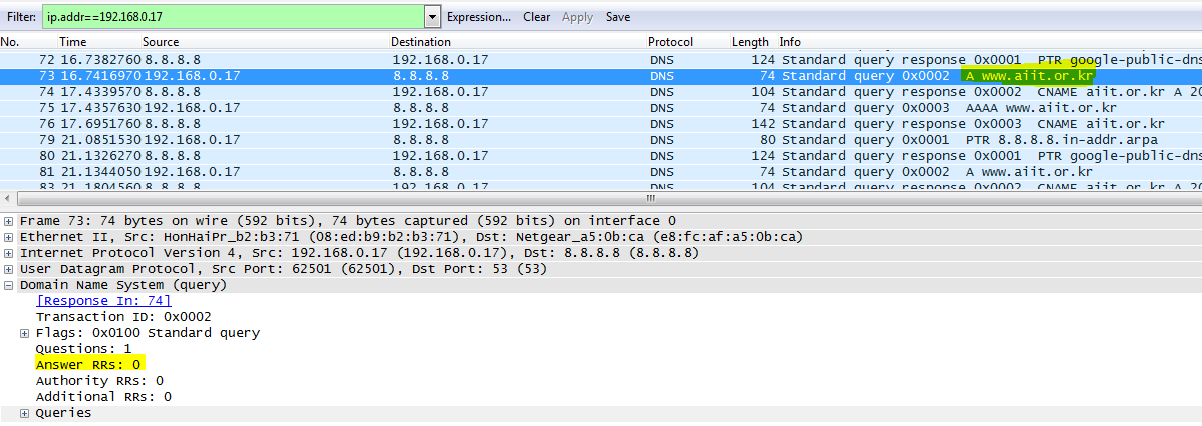
1. To what IP address is the DNS query message sent? Is this the IP address of your local DNS server? If not what does the IP address corresponds to?

Ans: The DNS query message was sent to the IP address 8.8.8.8. No this IP address is not my local DNS server. This IP address corresponds to the IP address of Google’s Public DNS server.



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

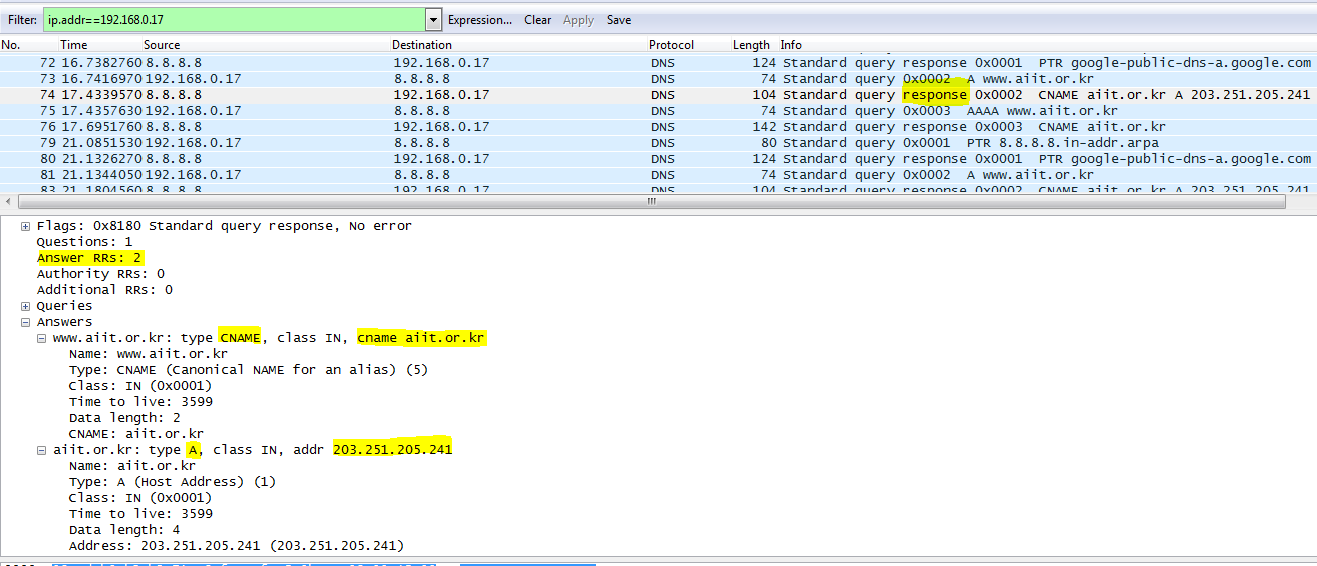
Ans: DNS query type is “A”. NO the query message does not contain answers. The answer resource record count is 0.



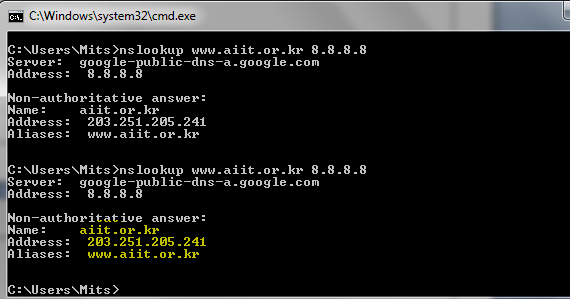
1. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

Ans: There are 2 answer resource records in the DNS response message.

These answers contain one CNAME resource record with CNAME aiit.or.kr and one A record with IP address 203.251.205.241



1. Provide a screen shot.



Wireshark Experience: The tool is very friendly in using and understanding. The description about how to do the assignment is also very clear and crisp. The concepts of DNS query types, DNS response types are clear after this experiment. The different ways in which DNS server can respond to the queries based on query types is quite interesting. One interesting point I noticed is when answering question3 where nslookup is made to the yahoo mail server. The response to the nslookup will contain server name as unknown by provides IP address followed by timeout messages. I tried running this command on multiple university website names and they all yielded the similar replies. Also when a nslookup is made to the ip address returned by command in question 3, I got a reply with the domain name of a yahoo mail server hence confirming it’s one of yahoo mail servers.

In question 3, the ip address of the DNS server returned is **98.138.79.21** whose DNS server name was Unknown.

nslookup for the same will return the DNS server name to be yahoo mail server.

