# Lab week-05 Application Layer

## Objectives

\* Explore and explain the nature of Application Layer packet structures

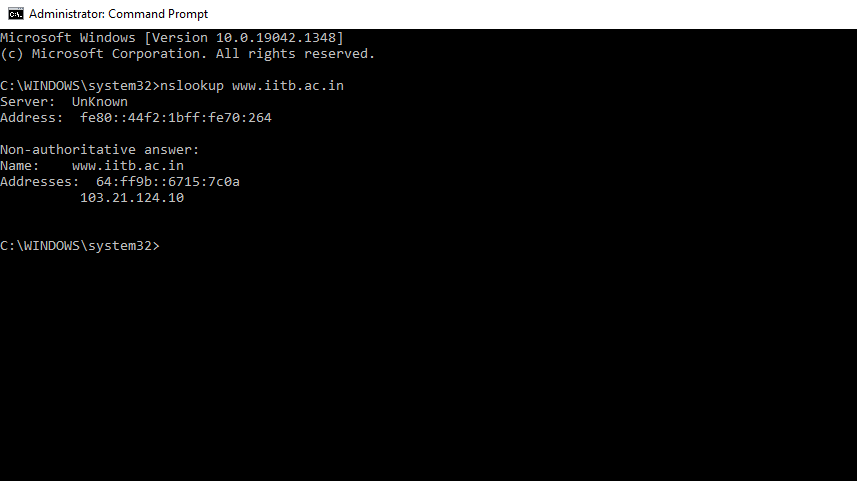
\* Explore and describe the use of commanline tools for networking use

\* Explain the internal concepts of the Application layer

### Questions

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](www.iitb.ac.in "IIT India"). What is the IP address of www.iitb.ac.in?

i)



103.21.124.10

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

i) Address: 172.20.10.1

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

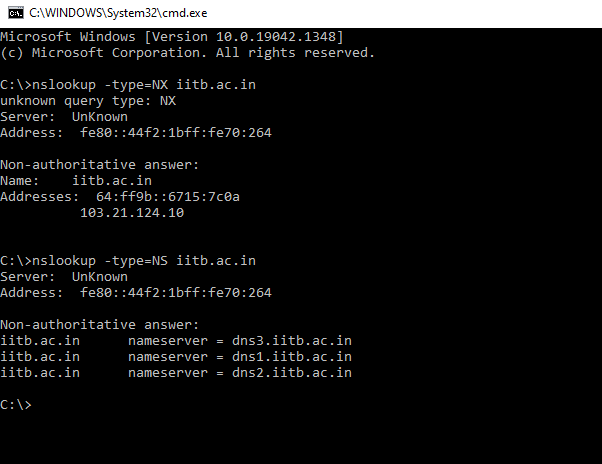
i)Non-authoritative answer:

Name: www.iitb.ac.in

Addresses: 103.21.124.10

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?

i)



iitb.ac.in nameserver = dns3.iitb.ac.in

iitb.ac.in nameserver = dns1.iitb.ac.in

iitb.ac.in nameserver = dns2.iitb.ac.in

These are the servers used by iitb.ac.in

On a Mac computer, you can enter the following command into a terminal window to clear your DNS resolver cache: `sudo killall -HUP mDNSResponder`

On Windows computer you can enter the following command at the command prompt: `ipconfig /flushdns`

\* Clear the DNS cache in your host, as described above.

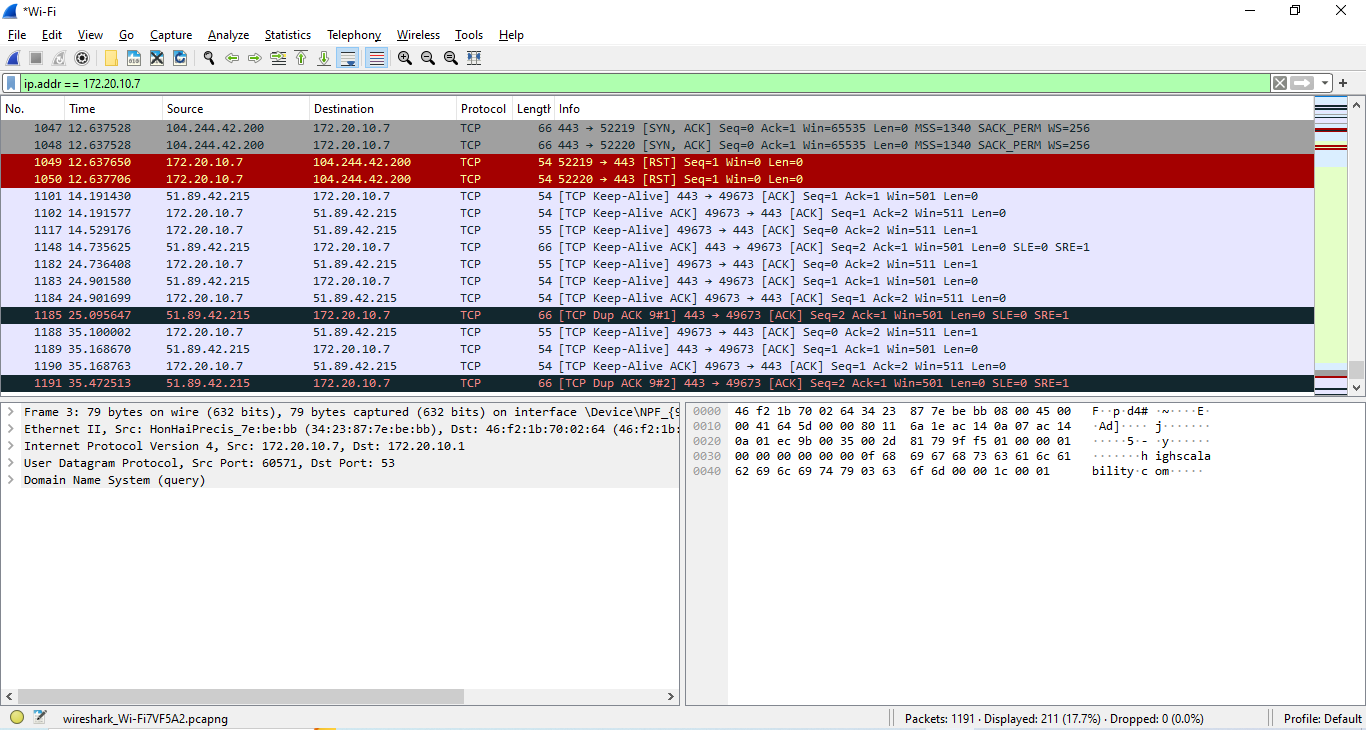
\* Open your Web browser and clear your browser cache.

\* Open Wireshark and enter ip.addr == <your\_IP\_address> into the display filter, where <your\_IP\_address> is the IPv4 address of your computer . With this filter, Wireshark will only display packets that either originate from, or are destined to,your host.

\* Start packet capture in Wireshark.

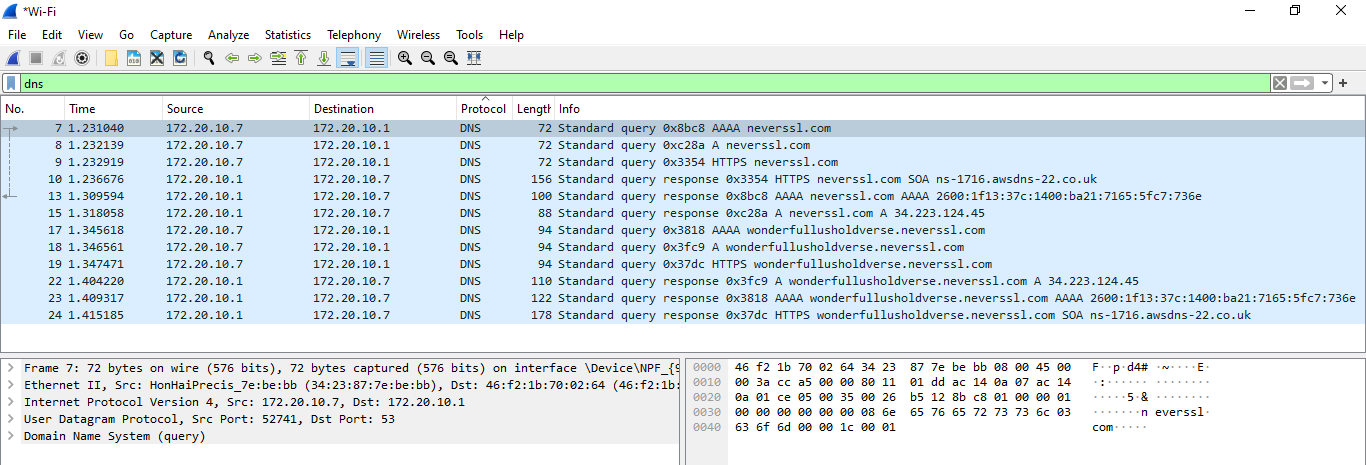
\* With your browser, visit the Web page: http://highscalability.com

\* Stop packet capture.

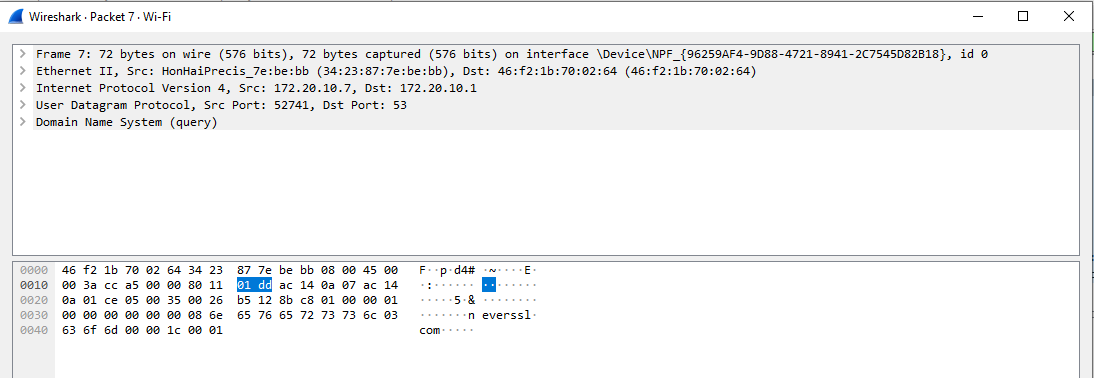


1. Locate the first DNS query message resolving the name neverssl.com. What is the packet number in the trace for the DNS query message? Is this query message sent over UDP or TCP?

i)



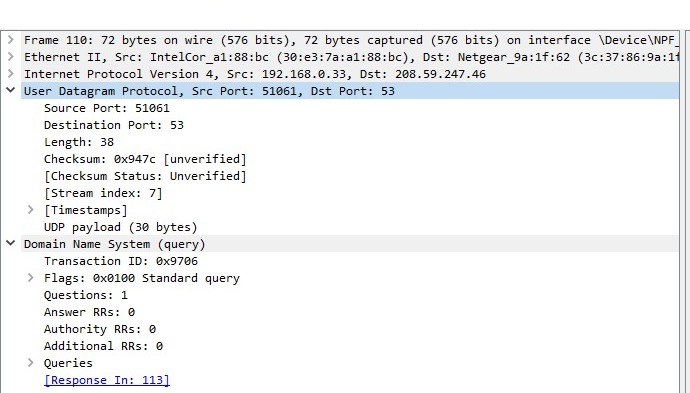
Packet No 7



The query Message sent Over UDP.

2. 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?

i)



In packet No 110 We got corresponding response from DNS 208.59.247.46 to our server 192.168.0.33

we got response through UDP.

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

i) In standard query Intitial request destination port is 53

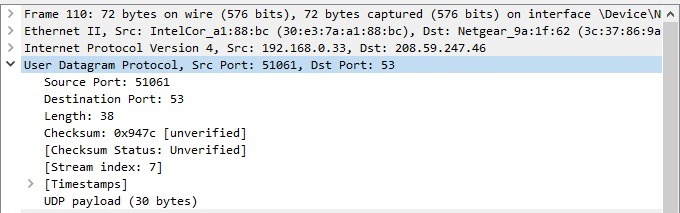
In response Destination port is 51061

In standard query Intitial request destination port is 53

In response Destination port is 58402 see the scree shot.In standard query Intitial request destination port is 53 In response Destination port is 58402

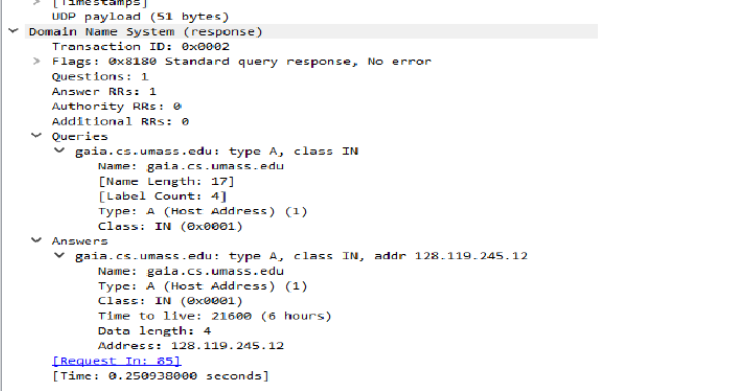
4. To what IP address is the DNS query message sent?

i)



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

i)It contains 1 Question and 1 Answer



## Deliverables

Place your answers to each question next to the \*i)\*. Copy this template into your own local private repo under the itmo-340 or itmo-540 folder. Create a subfolder called: `week-05` and place this document into that folder, push the code to GitHub and submit the URL to this document.