Lab report no 6

Spring 2022

CSE303L Data Communication Network

Submitted by: **Muhammad Ali**

Registration No: - 19pwcse1801

Class Section: A

Submitted to:

Engr. Faizullah

Date: Friday 5, 2022

Department of Computer Systems Engineering

University of Engineering and Technology, Peshawar

CSE 303L: Data Communication and Computer Networks

Demonstration of Concepts	**Poor (Does not meet expectation (1))** The student failed to demonstrate a clear understanding of the assignment concepts	**Fair (Meet Expectation (2-3))** The student demonstrated a clear understanding of some of the assignment concepts	**Good (Exceeds Expectation (4-5)** The student demonstrated a clear understanding of the assignment concepts	**Score** **30%**
Accuracy	The student mis-configured enough network settings that the lab computer couldn't function properly on the network	The student configured enough network settings that the lab computer partially functioned on the network	The student configured the network settings that the lab computer fully functioned on the network	**30%**
Following Directions	The student clearly failed to follow the verbal and written instructions to successfully complete the lab	The student failed to follow the some of the verbal and written instructions to successfully complete all requirements of the lab	The student followed the verbal and written instructions to successfully complete requirements of the lab	**20%**
Time Utilization	The student failed to complete even part of the lab in the allotted amount of time	The student failed to complete the entire lab in the allotted amount of time	The student completed the lab in its entirety in the allotted amount of time	**20%**

Credit Hours: 1

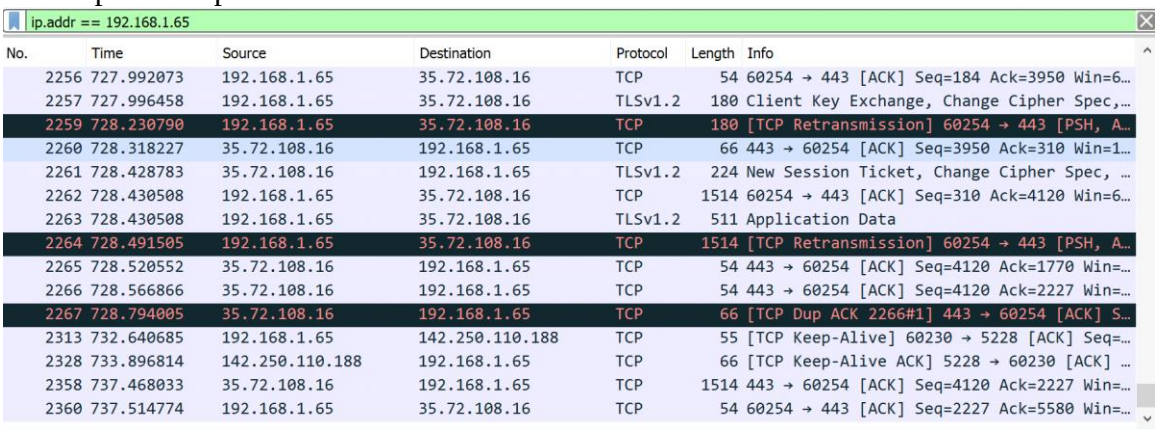
Lab 06

- **The Domain Name System (DNS)** translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll take a closer look at the client side of DNS. Recall that the client's role in the DNS is relatively simple – a client sends a query to its local DNS server, and receives a response back.

The hierarchical DNS servers communicate with each other to either recursively or iteratively resolve the client's DNS query. From the DNS client's standpoint, however, the protocol is quite simple – a query is formulated to the local DNS server and a response is received from that server.

Tracing DNS with Wireshark

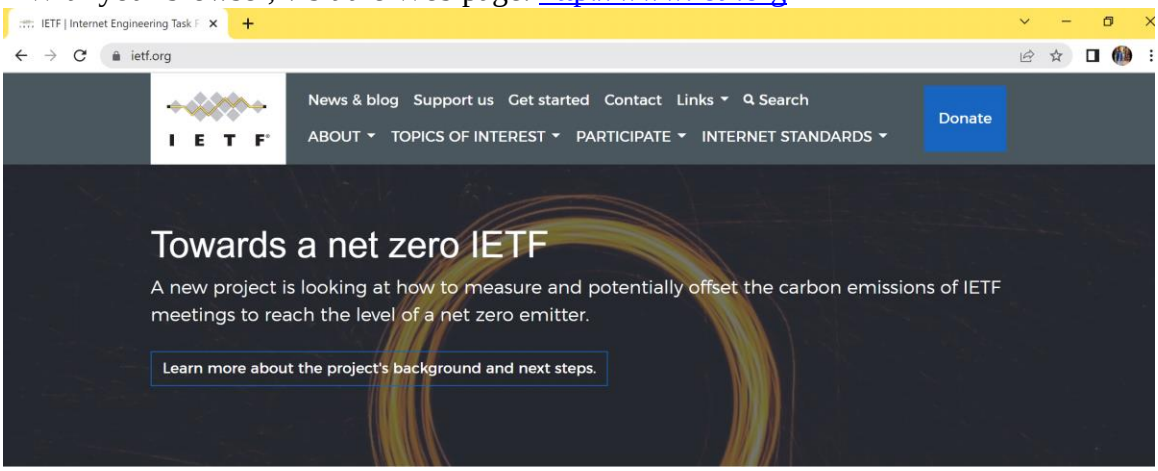
• Open Wireshark and enter "ip.addr == your_IP_address" into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.
• Start packet capture in Wireshark.



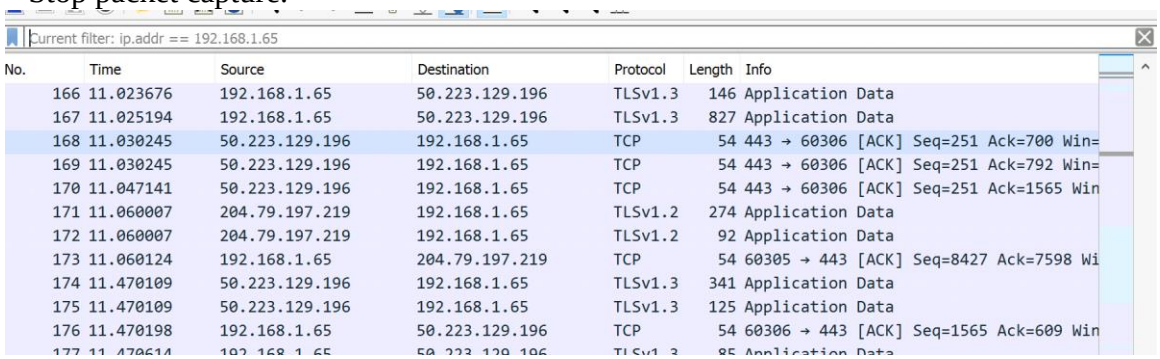
ip.addr == 192.168.1.65

No.	Time	Source	Destination	Protocol	Length	Info
2256	727.992073	192.168.1.65	35.72.108.16	TCP	54	60254 → 443 [ACK] Seq=184 Ack=3950 Win=6…
2257	727.996458	192.168.1.65	35.72.108.16	TLSv1.2	180	Client Key Exchange, Change Cipher Spec,…
2259	728.230790	192.168.1.65	35.72.108.16	TCP	180	[TCP Retransmission] 60254 → 443 [PSH, A…
2260	728.318227	35.72.108.16	192.168.1.65	TCP	66	443 → 60254 [ACK] Seq=3950 Ack=310 Win=1…
2261	728.428783	35.72.108.16	192.168.1.65	TLSv1.2	224	New Session Ticket, Change Cipher Spec, …
2262	728.430508	192.168.1.65	35.72.108.16	TCP	1514	60254 → 443 [ACK] Seq=310 Ack=4120 Win=6…
2263	728.430508	192.168.1.65	35.72.108.16	TLSv1.2	511	Application Data
2264	728.491505	192.168.1.65	35.72.108.16	TCP	1514	[TCP Retransmission] 60254 → 443 [PSH, A…
2265	728.520552	35.72.108.16	192.168.1.65	TCP	54	443 → 60254 [ACK] Seq=4120 Ack=1770 Win=…
2266	728.566866	35.72.108.16	192.168.1.65	TCP	54	443 → 60254 [ACK] Seq=4120 Ack=2227 Win=…
2267	728.794005	35.72.108.16	192.168.1.65	TCP	66	[TCP Dup ACK 2266#1] 443 → 60254 [ACK] S…
2313	732.640685	192.168.1.65	142.250.110.188	TCP	55	[TCP Keep-Alive] 60230 → 5228 [ACK] Seq=…
2328	733.896814	142.250.110.188	192.168.1.65	TCP	66	[TCP Keep-Alive ACK] 5228 → 60230 [ACK] …
2358	737.468033	35.72.108.16	192.168.1.65	TCP	1514	443 → 60254 [ACK] Seq=4120 Ack=2227 Win=…
2360	737.514774	192.168.1.65	35.72.108.16	TCP	54	60254 → 443 [ACK] Seq=2227 Ack=5580 Win=…

• With your browser, visit the Web page: http://www.ietf.org



• Stop packet capture.

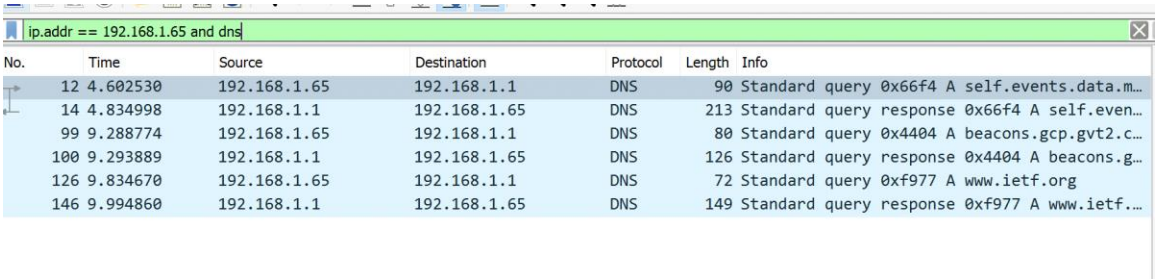


Current filter: ip.addr == 192.168.1.65

No.	Time	Source	Destination	Protocol	Length	Info
166	11.023676	192.168.1.65	50.223.129.196	TLSv1.3	146	Application Data
167	11.025194	192.168.1.65	50.223.129.196	TLSv1.3	827	Application Data
168	11.030245	50.223.129.196	192.168.1.65	TCP	54	443 → 60306 [ACK] Seq=251 Ack=700 Win=
169	11.030245	50.223.129.196	192.168.1.65	TCP	54	443 → 60306 [ACK] Seq=251 Ack=792 Win=
170	11.047141	50.223.129.196	192.168.1.65	TCP	54	443 → 60306 [ACK] Seq=251 Ack=1565 Win
171	11.060007	204.79.197.219	192.168.1.65	TLSv1.2	274	Application Data
172	11.060007	204.79.197.219	192.168.1.65	TLSv1.2	92	Application Data
173	11.060124	192.168.1.65	204.79.197.219	TCP	54	60305 → 443 [ACK] Seq=8427 Ack=7598 Wi
174	11.470109	50.223.129.196	192.168.1.65	TLSv1.3	341	Application Data
175	11.470109	50.223.129.196	192.168.1.65	TLSv1.3	125	Application Data
176	11.470198	192.168.1.65	50.223.129.196	TCP	54	60306 → 443 [ACK] Seq=1565 Ack=609 Win

To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

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



ip.addr == 192.168.1.65 and dns

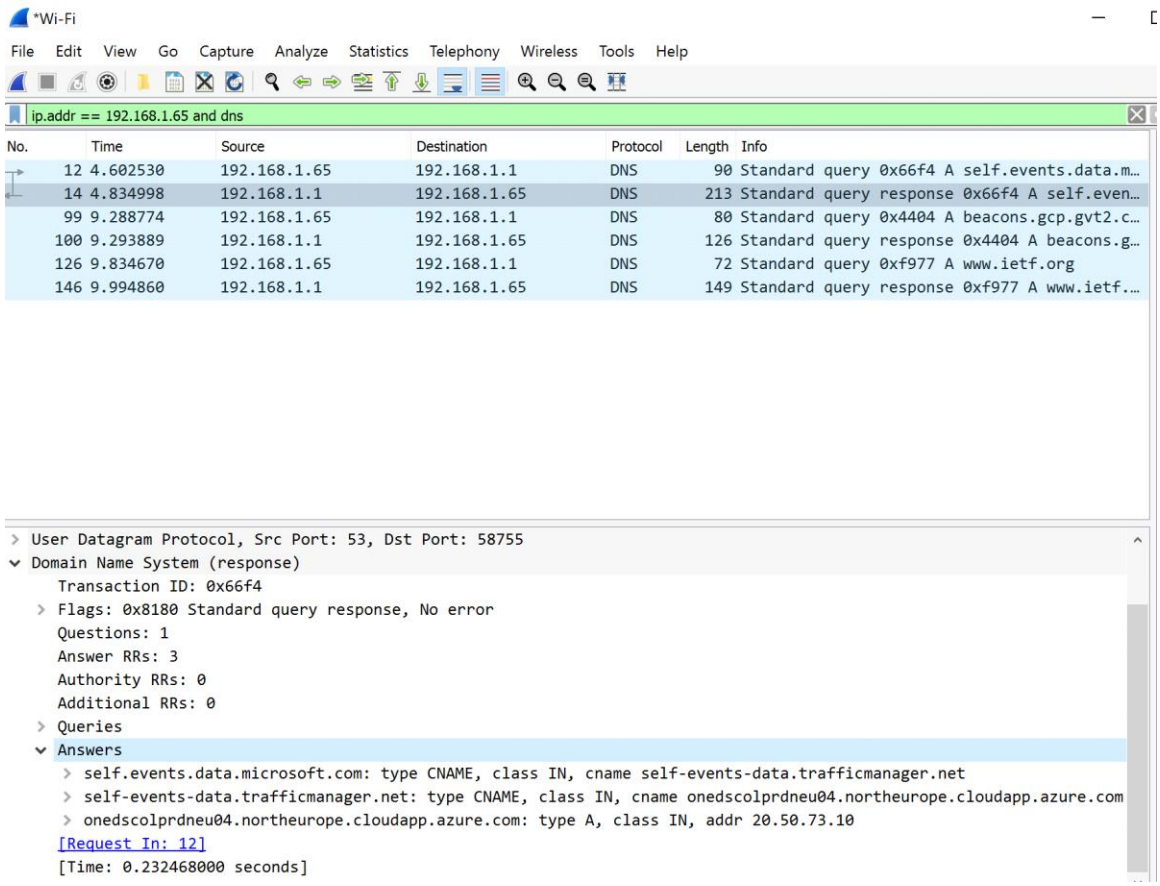
No.	Time	Source	Destination	Protocol	Length	Info
12	4.602530	192.168.1.65	192.168.1.1	DNS	90	Standard query 0x66f4 A self.events.data.m…
14	4.834998	192.168.1.1	192.168.1.65	DNS	213	Standard query response 0x66f4 A self.even…
99	9.288774	192.168.1.65	192.168.1.1	DNS	80	Standard query 0x4404 A beacons.gcp.gvt2.c…
100	9.293889	192.168.1.1	192.168.1.65	DNS	126	Standard query response 0x4404 A beacons.g…
126	9.834670	192.168.1.65	192.168.1.1	DNS	72	Standard query 0xf977 A www.ietf.org
146	9.994860	192.168.1.1	192.168.1.65	DNS	149	Standard query response 0xf977 A www.ietf.…

-
- What is the destination port for the DNS query message? What is the source port of DNS response message?
  Ans: Destination port is 53 for DNS message response and also
  Sourse port is 53 for DNS response.

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

Ans:Yes both are same in command promt and wireshark query message.my dns ip address is 192.168.1.65.

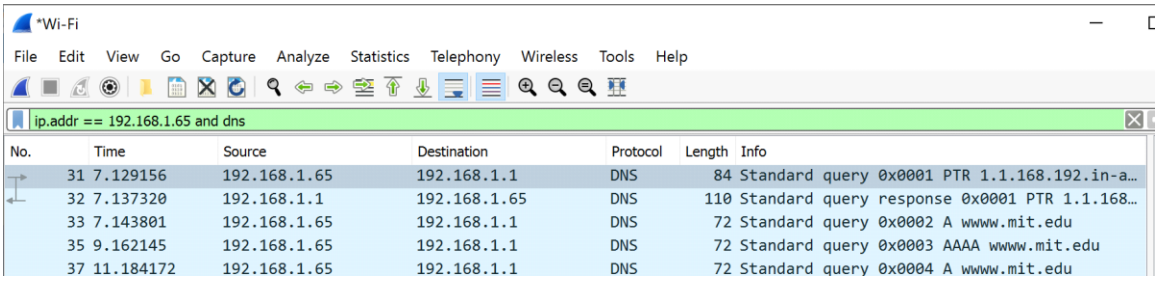
- Examine the DNS query message. What “Type” of DNS query is it? Does the query message contains any “answers”?
  Ans:It is a standard query type.it contains no answer.
- Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?



Now let's play with *nslookup*.

- Start packet capture.
- Do an *nslookup* on www.mit.edu
- Stop packet capture.

You should get a trace that looks something like the following:



We see from the above screenshot that *nslookup* actually sent three DNS queries and received three DNS responses. For the purpose of this assignment, in answering the following questions, ignore the first two sets of queries/responses, as they are specific to *nslookup* and are not

normally generated by standard Internet applications. You should instead focus on the last query and response messages.

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

Ans: Both are 53 .

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

Ans: 192.168.1.1 its my default DNS server IP address.

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

Ans: it is a query message and contains no messages.

```
Queries
> www.mit.edu: type AAAA, class IN
```

- Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

Ans: it contains 4 Answers

- Provide a screenshot.aa

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.65 and dns

No.	Time	Source	Destination	Protocol	Length	Info
27	15.464054	192.168.1.65	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-a…
28	15.488976	192.168.1.1	192.168.1.65	DNS	110	Standard query response 0x0001 PTR 1.1.168…
29	15.494932	192.168.1.65	192.168.1.1	DNS	71	Standard query 0x0002 A www.mit.edu
30	15.888707	192.168.1.1	192.168.1.65	DNS	160	Standard query response 0x0002 A www.mit.e…
31	15.898900	192.168.1.65	192.168.1.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
32	15.914497	192.168.1.1	192.168.1.65	DNS	200	Standard query response 0x0003 AAAA www.mi…

```
Domain Name System (response)
    Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    > www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:a1:6b1::255e
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2a02:26f0:a1:696::255e
    [Request In: 31]
    [Time: 0.015597000 seconds]
```