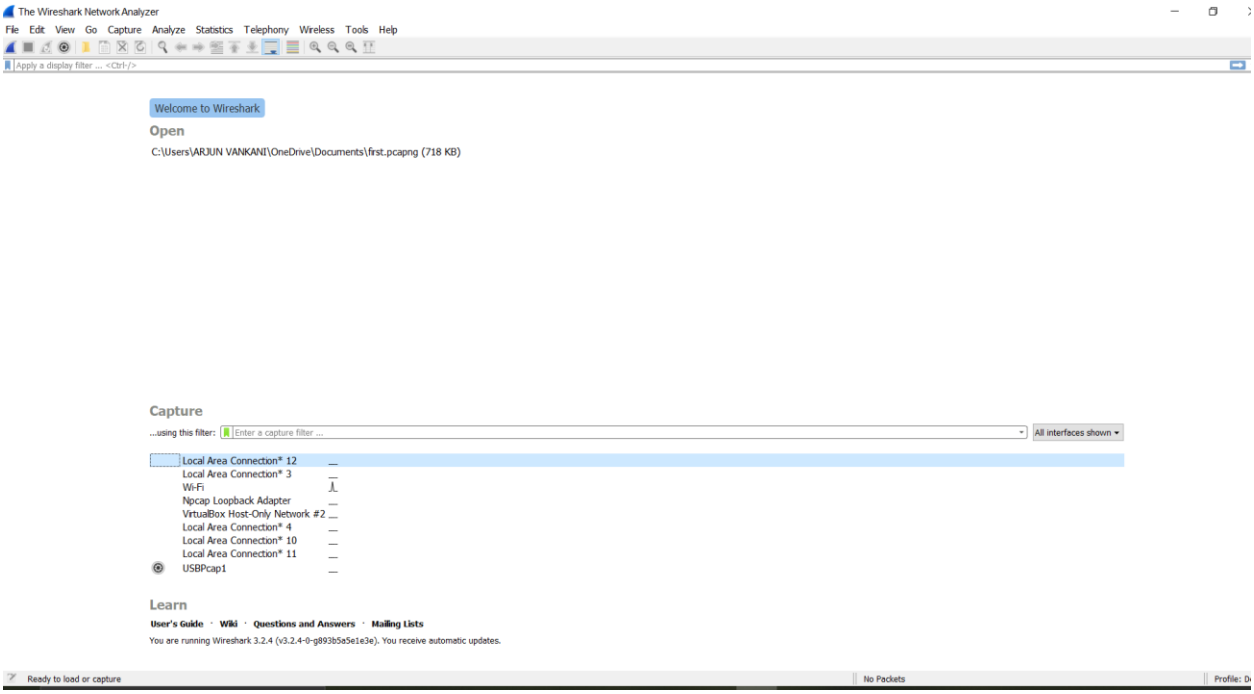
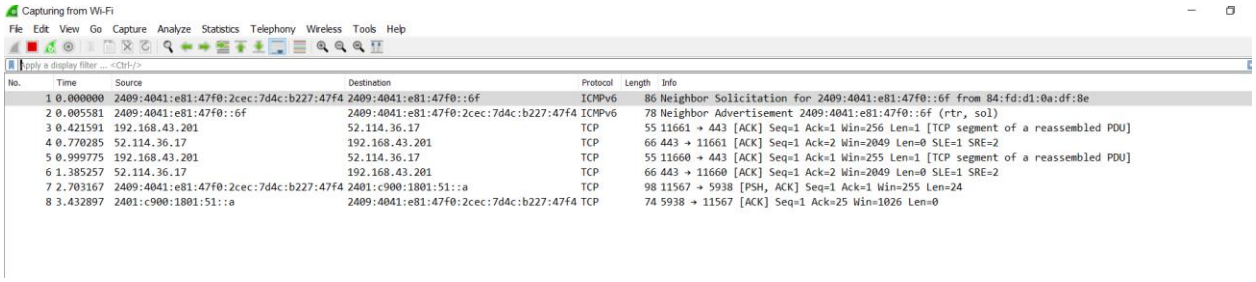
Computer Network LAB (Session -8)

- Packet capture and header analysis by Wireshark
- **Download and install Wireshark(https://www.wireshark.org/).**
- First, we have to download Wireshark is the world's foremost and widely-used network protocol analyzer.
- And mostly it used for Ip tracing as well as all know about all layer's handshaking and data transfer protocol.

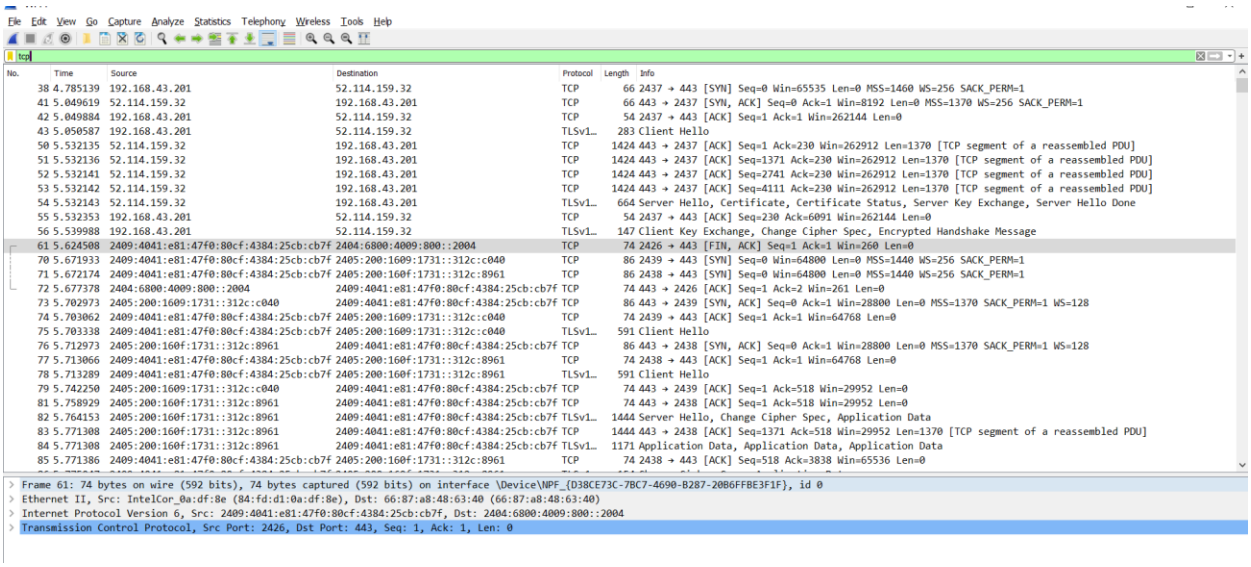


- This is Wireshark, if we want to analysis protocol then clicks on Wi-Fi connection and Start capture.
- After Start kernel that was shown below



Q-A) Access a website and capture the protocol message being exchanged between your web browser and the web server.

- Frist, we requesting for URL to send data that why opening browser and search for website.



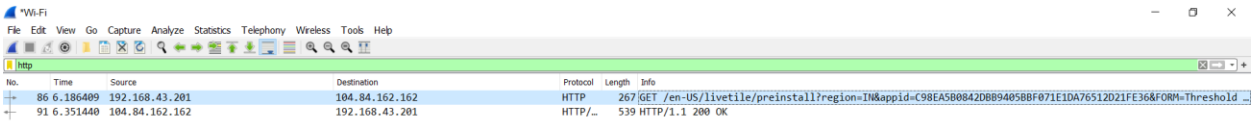
- TCP means transmission control protocol.

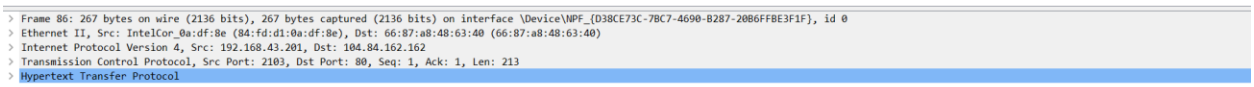
- This is Ipv4 and data bytes are (600bits) where UDP source port 58453 and destination port 53 length 41.

- For message and query requesting for seq num and ack is shown above figure for Client say Hello
- Seq =1, ack =230, Len =1370
  Seq = 1371, ack=230, Len=1370
  And after Server say Hello
  Seq = 230, Ack=6091, Len =0
  Now Encrypted handshaking for message.

Q-B) Explore different aspect of HTTP protocol, GET/reply interaction, HTTP message format, persistent and non-persistent HTTP connections.

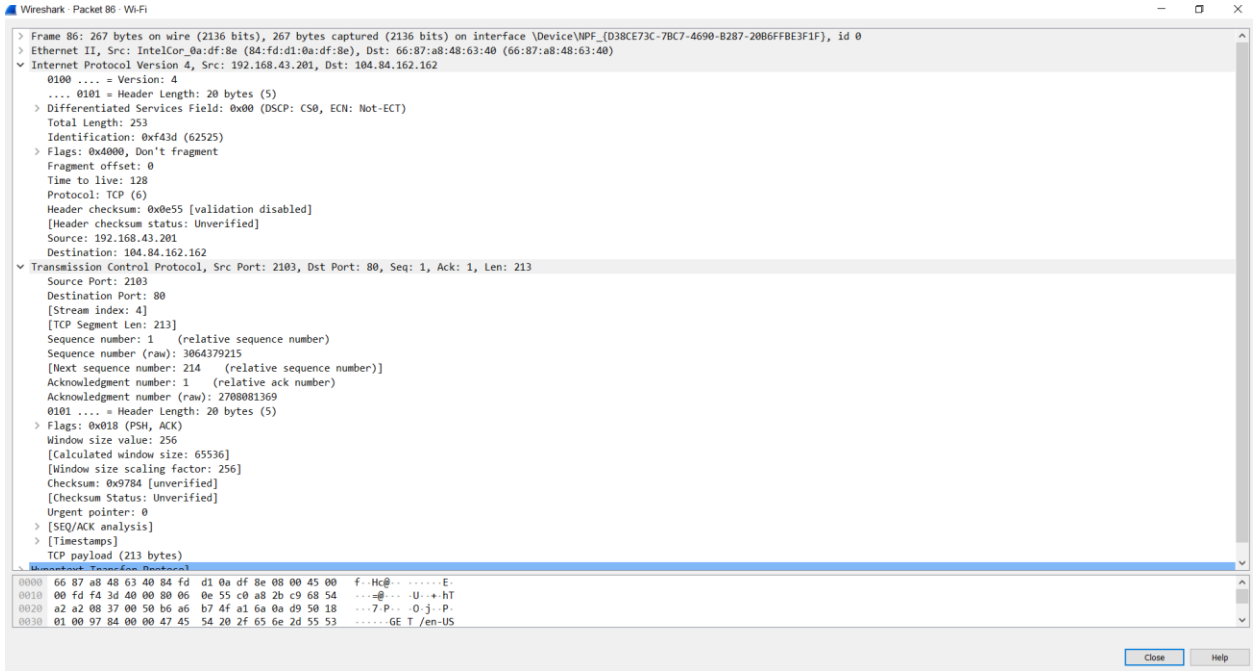
- Http stands for Hypertext transfer protocol.
- Where we start website and it req for HTTP ok response. After that cache will shown our web data if we are going to second time on this website.





- Here, Fig shows source ip 192.168.43.201 when we req to load data at that time GET method is used and data Length 267.

After second server is source when it gives OK response to us that is why both source and destination changed.



- Data length is 2136 bits and IPv4 with source-ip 192.168.43.201 and destination-ip 104.84.162.162 for Hotstar-ip, with source-port: 2103 and des-port :80 For HTTP. 1.1 version represent connection close and Persistent connection.
- In HTTP/1.0 the connection is non-persistent by default unless you add the Connection: keep-alive.
- In HTTP/1.1 the connection is persistent by default unless you add the Connection: close

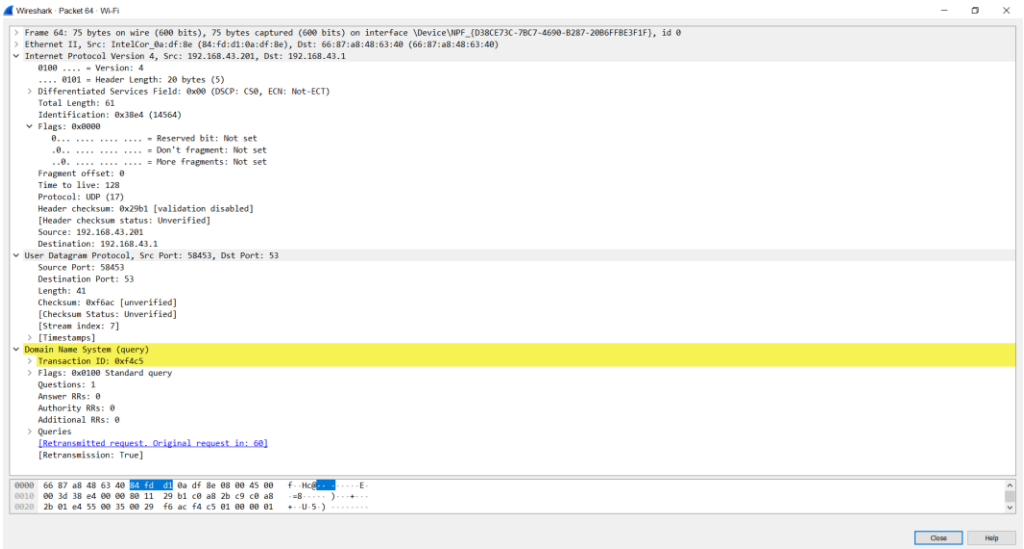
Q-C) Explore the process of resolving a DNS query, recursive/iterative communication between different DNS servers and DNS response from different DNS servers.

dns

No.	Time	Source	Destination	Protocol	Length	Info
57	5.621489	192.168.43.201	192.168.43.1	DNS	75	Standard query 0x4ebf A www.hotstar.com
58	5.621490	192.168.43.201	192.168.43.1	DNS	87	Standard query 0xd57b A secure-media.hotstarext.com
59	5.621843	192.168.43.201	192.168.43.1	DNS	87	Standard query 0x4a8b AAAA secure-media.hotstarext.com
60	5.621858	192.168.43.201	192.168.43.1	DNS	75	Standard query 0xf4c5 AAAA www.hotstar.com
62	5.660069	192.168.43.1	192.168.43.201	DNS	189	Standard query response 0x4ebf A www.hotstar.com CNAME www.hotstar.com-sni.edgekey.net CNAME e35862…
63	5.664263	192.168.43.201	192.168.43.1	DNS	87	Standard query 0xd57b A secure-media.hotstarext.com
64	5.664265	192.168.43.201	192.168.43.1	DNS	75	Standard query 0xf4c5 AAAA www.hotstar.com
65	5.664267	192.168.43.201	192.168.43.1	DNS	87	Standard query 0x4a8b AAAA secure-media.hotstarext.com
66	5.669731	192.168.43.1	192.168.43.201	DNS	203	Standard query response 0xd57b A secure-media.hotstarext.com CNAME wildcard.hotstarext.com.edgesuite…
67	5.670289	192.168.43.1	192.168.43.201	DNS	227	Standard query response 0x4a8b AAAA secure-media.hotstarext.com CNAME wildcard.hotstarext.com.edgesu…
68	5.670472	192.168.43.1	192.168.43.201	DNS	297	Standard query response 0xf4c5 AAAA www.hotstar.com CNAME www.hotstar.com-sni.edgekey.net CNAME e358…
69	5.670737	192.168.43.1	192.168.43.201	DNS	206	Standard query response 0xd57b A secure-media.hotstarext.com CNAME wildcard.hotstarext.com.edgesuite…

- DNS is Domain name server.

- Now we are opening Google browser and https://www.hotstar.com/ search this URL for capturing query and response.
- DNS req is going through many sources and also destination is more than one. Shown above figure
- DNS server firstly req query to server and waiting for its response or ack.
- Here, Source ip is 192.168.43.1 Which is our laptop ip address and Destination ip is 192.168.43.201



- Ipv4 with source and destination share UDP source-port: 58453 and destination-port: 53 where length 41 (600bits) sending. And All flag shown above as Question: 1, Answer: 0, Authority: 0, Additional:0, as well as Queries requesting for answer

- OSI Model shown below work with Wireshark.

1) Application layer as HTTP format

- Which is shown above Hypertext transfer protocol. The HTTP is our Application layer, with its own headers. HTTP is an application protocol for distributed, collaborative, hypermedia information systems.

2) Transport layer as TCP/UDP

- TCP is connection oriented and a connection between client and server is established before data can be sent. UDP uses a simple connectionless communication model with a minimum of protocol mechanisms.

3) Network Layer

- It includes the process of ICMP protocols, ICMP stands for Internet control message protocol.

4) Data link layer

- The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the physical layer. ARP stands for address resolution protocol works with data link layer.