**EE 5360 DATA COMMUNICATIONS**

PROJECT ASSIGNMENT REPORT

**University of Texas at Arlington**

**Department of Electrical Engineering**

**Spring 2016**

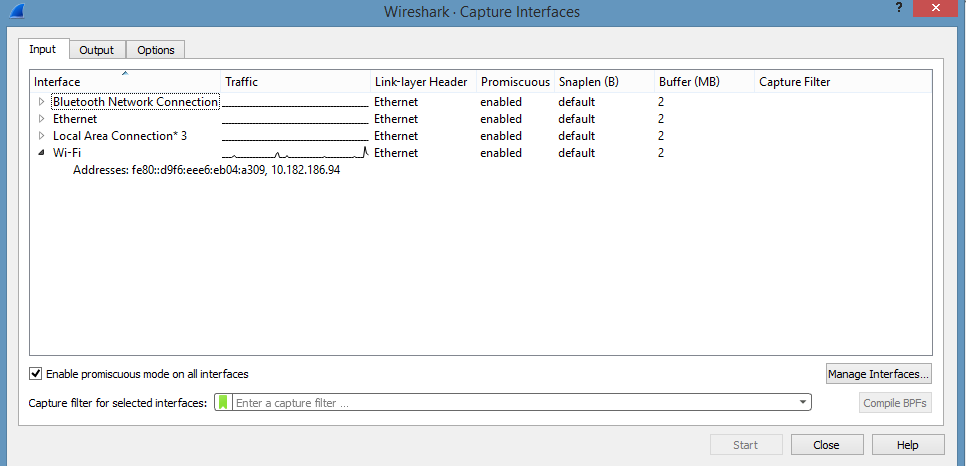
**By**

**PAVAI ARCHIMEDES**

**1001233996**

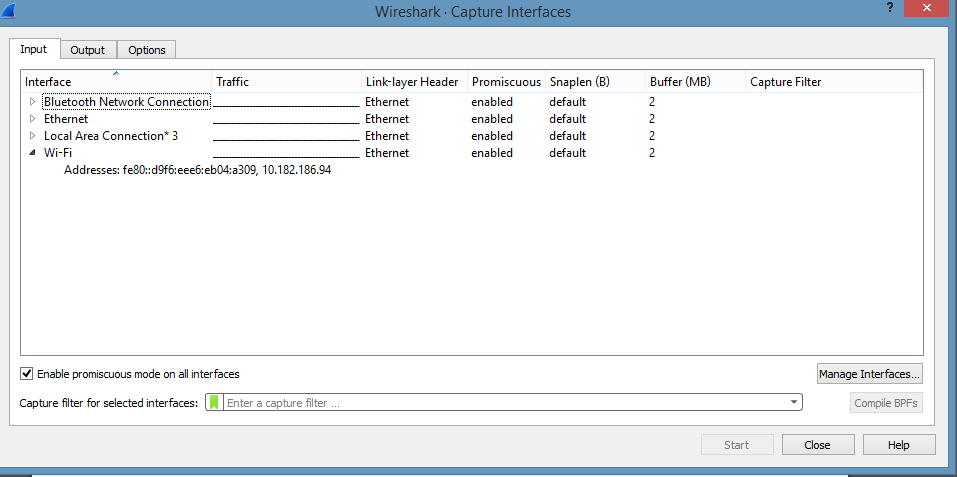
**WIRESHARK STARTUP:**

1. By connecting wireshark to the internet( wifi) the following observations were made

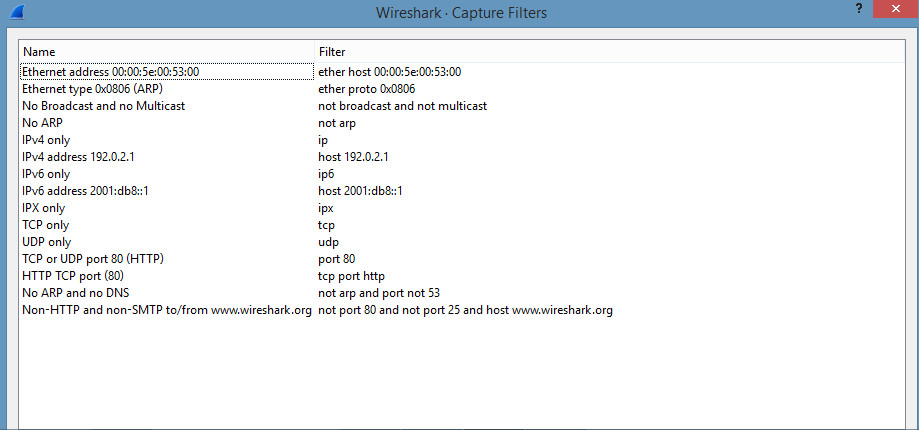


The wifi part is collecting data soon after connected to the internet.

1. By disconnecting from internet the following observations were made



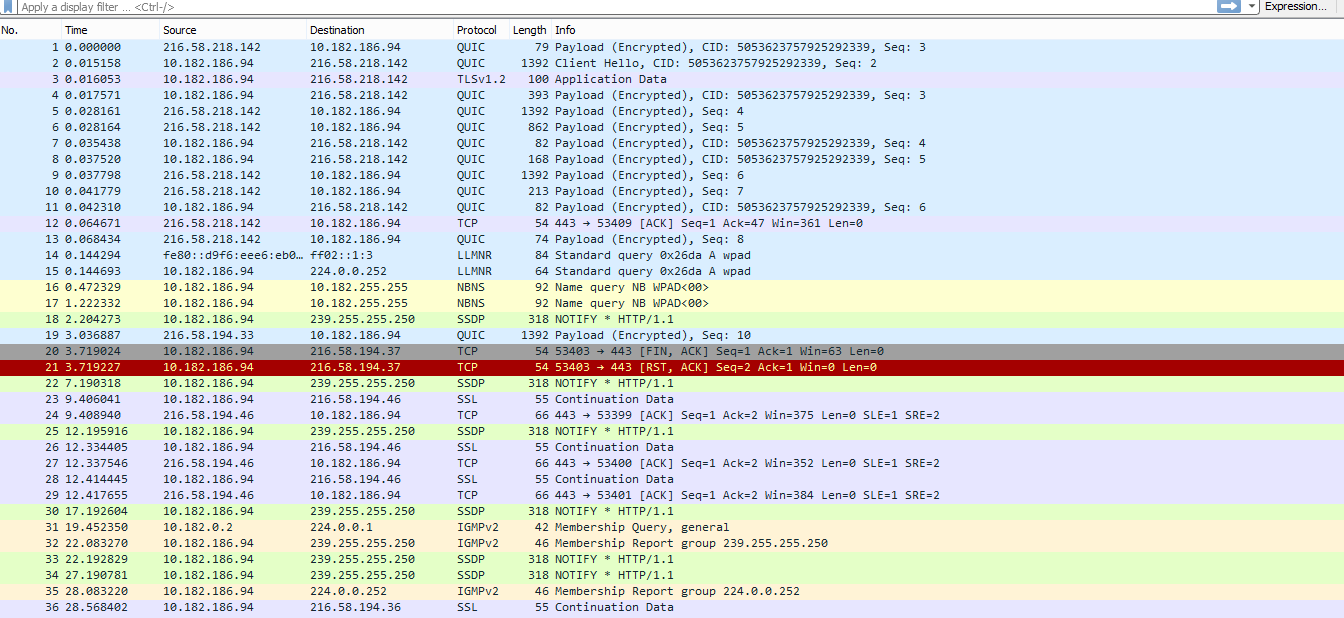
3.Collection for the port that was receiving data. Capture → Interfaces → Start



By again reconnecting to internet wireshark started to collect data.

**STEP 1**

Wireshark is used to capture the traffic while using web browser to visit a web page



* The computer is connected to the internet.
* Wireshark has started to collect data as follows

Frame 1 :QUIC

QUIC supports a set of multiplexed connections between two endpoints over User Datagram Protocol. ACK is sent

Frame 2: QUIC

Estimates bandwidth in each direction. ACK is sent.

Frame 3:TLSV1.2

Transport Layer Security is used to provide communication security over a computer network. This is an advanced version of TLS.

Frame 4-11: QUIC

Both query and response are made during this time frame.

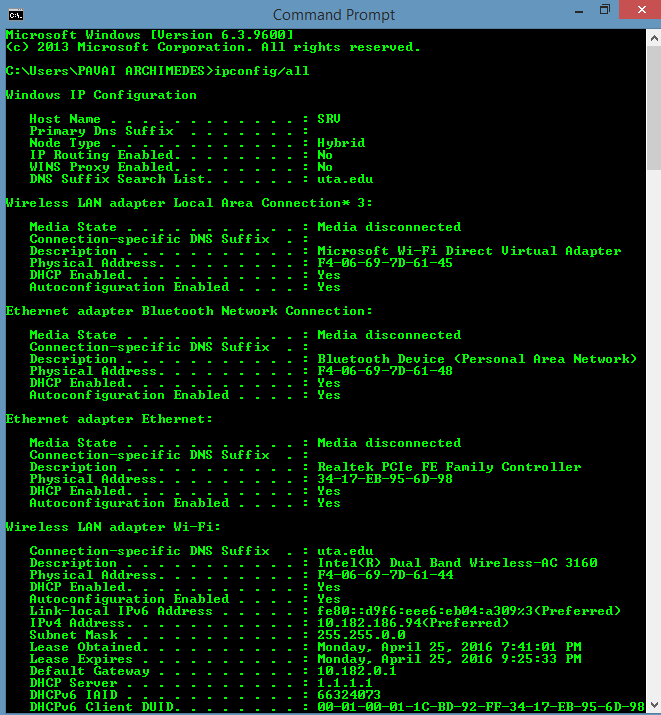
Frame 12:TCP

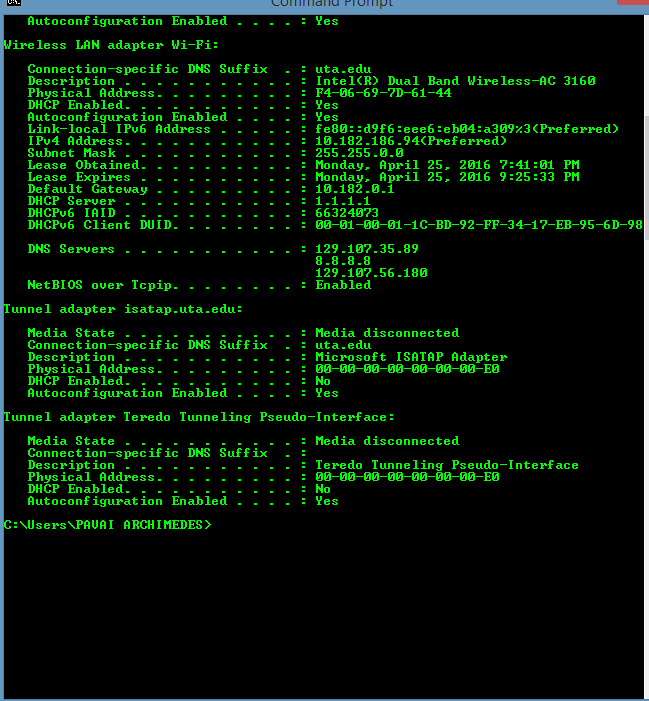
This is used to establish connection

It means that Wireshark thinks the packet in question contains part of a packet (PDU - "Protocol Data Unit") for a protocol that runs on top of TCP.

**STEP 2**

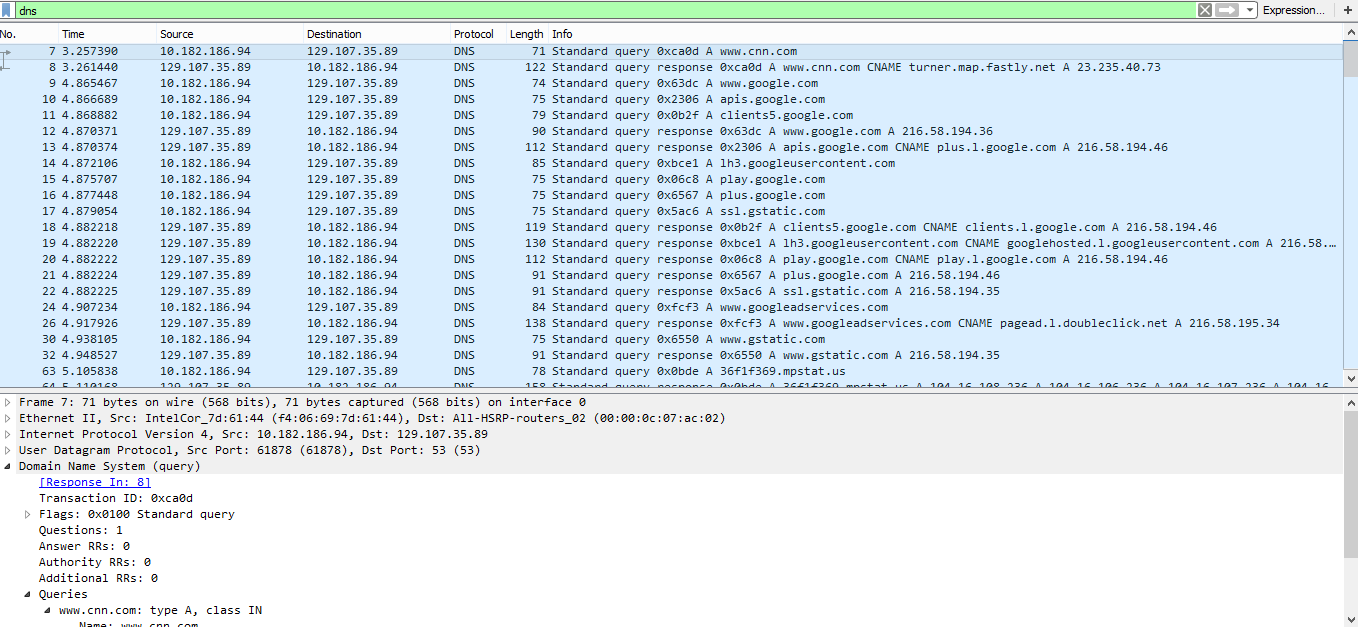
By Using appropriate Command Console command the following are found:

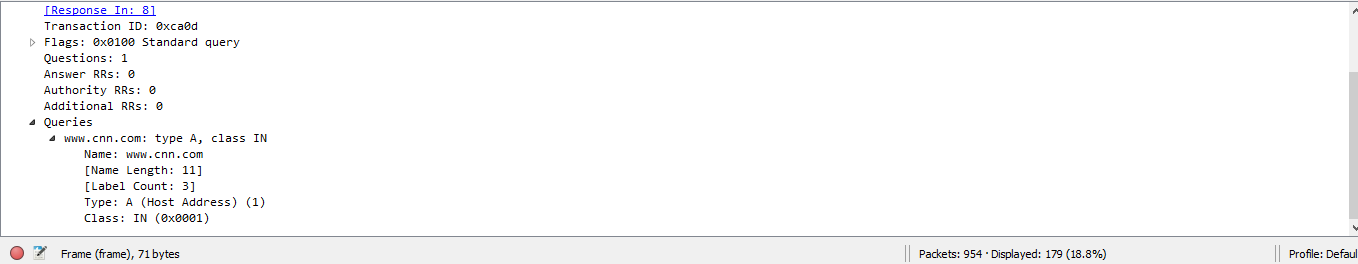


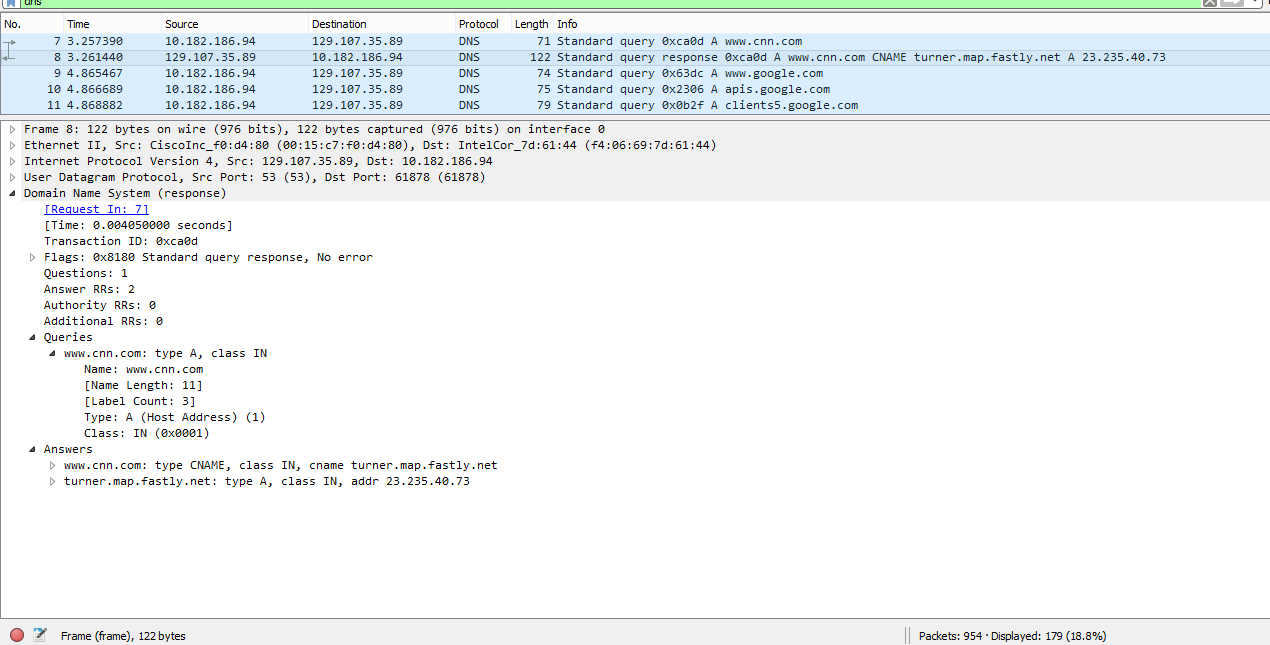


Wireshark data collection for [www.cnn.com](http://www.cnn.com)

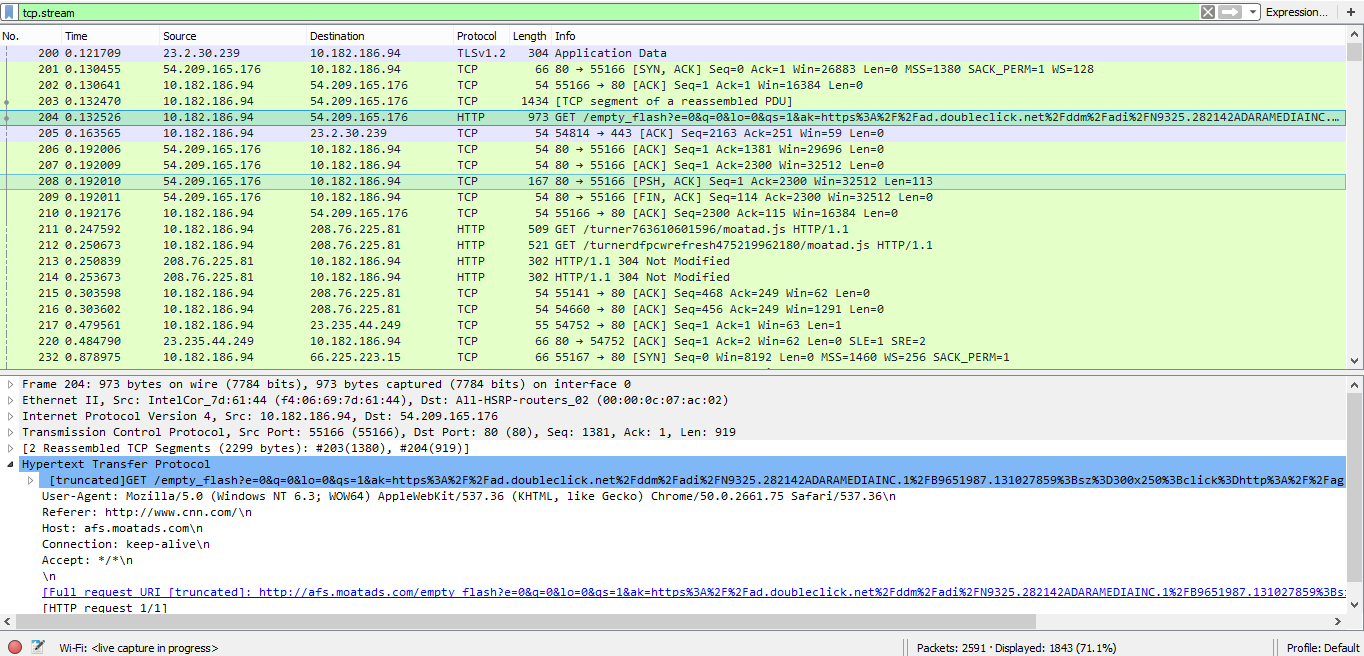
Dns query and response:







Which tcp protocol is used?

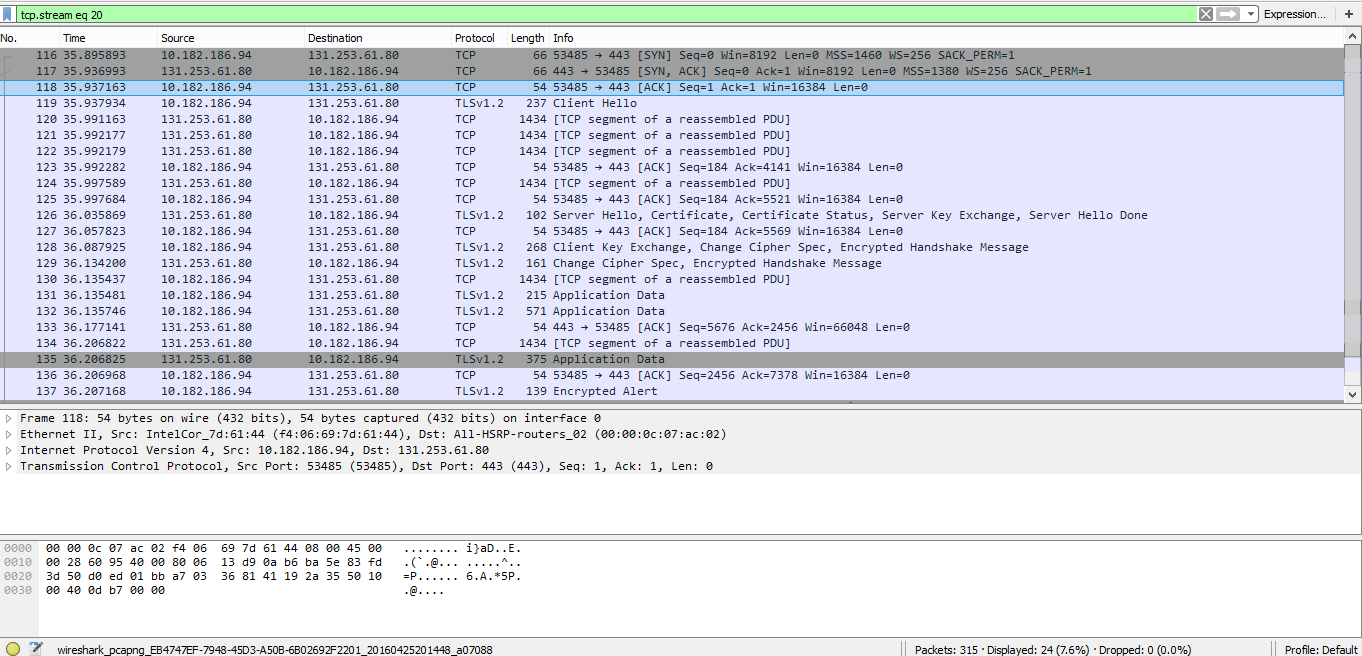


THE TCP PROTOCOL USED IS HTTP AND 2 ANSWERS ARE provided.

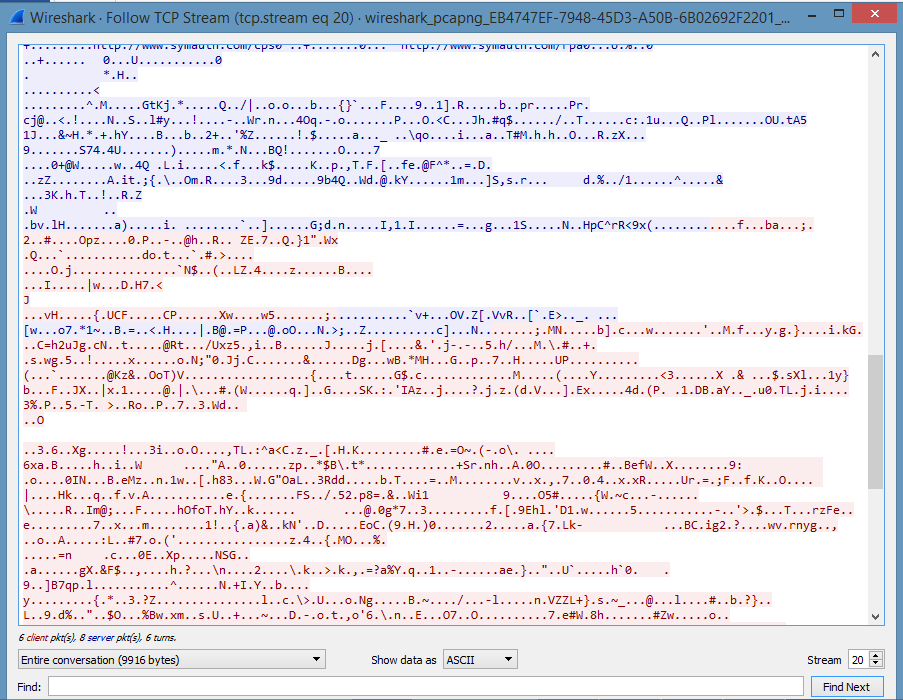
The dns query and response are noted.

**STEP 3**

Here a youtube video of 2 minutes duration is observed. Data is collected using wireshark.



Wireshark following tcp stream:



Frame 118 is observed here:

Window size: 16384

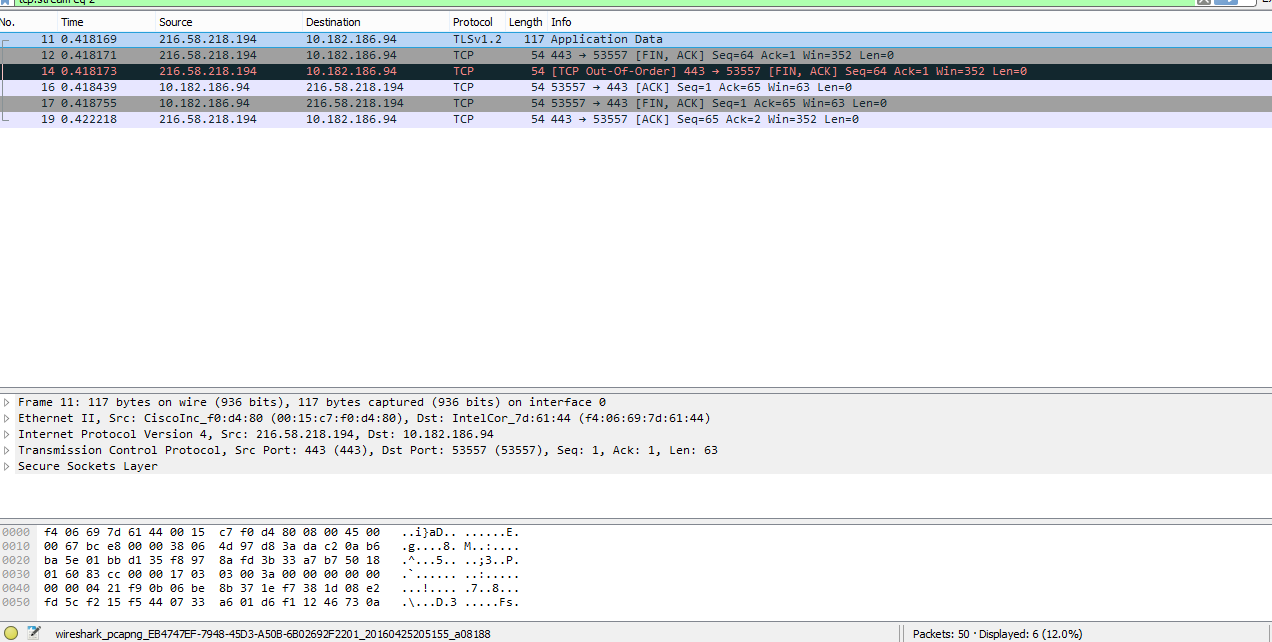
Entire data transmission takes place between 53485- 443 ( upstream and downstream) ports.

Entire conversation bytes: 9916

Ip address: source- 10: 182:186:94

Ip address destination: 131:253: 61:80

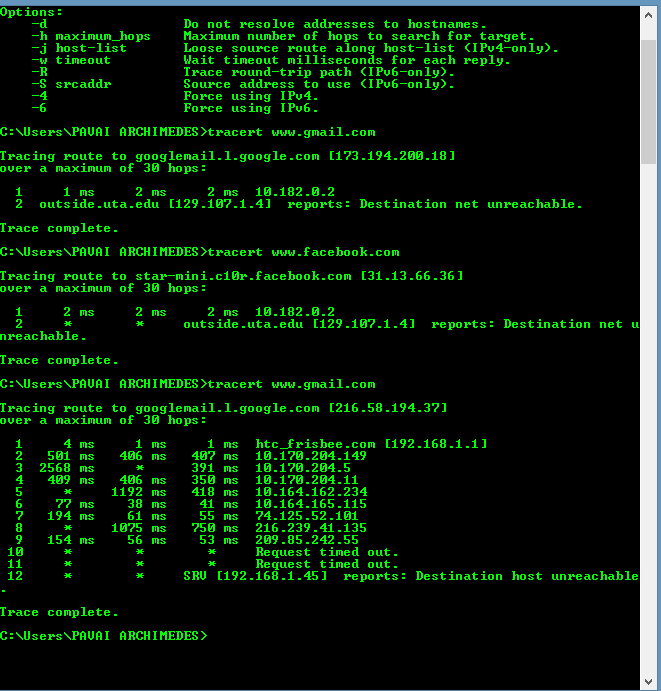
ERROR DURING AND RECOVERY:

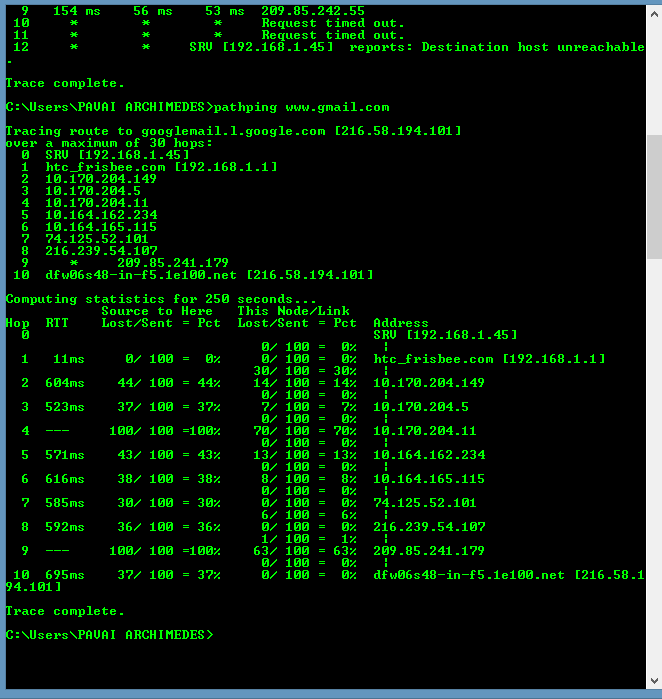


At frame 14 TCP went out of order which was recovered in the very next frame.

**STEP 4:**

By using tracert and pathping in command prompt the following observations are made:





|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Hop** | **%loss** | **IP Address** | **Node Name** | **Location** | **Avg. time(ms)** | **Network** |
| 1 | 0 | 192.168.1.45 | ------------------ | Arlington, TX, USA | 11ms | Htc frisbee |
| 2 | 44 | 192.168.1.11 | ------------------ | Arlington,Tx,  USA | 604ms | Htc frisbee |
| 3 | 37 | 10.172.204.149 | ------------------ | Arlington, Tx,USA | 523ms | Htc frisbee |
| 4 | 100 | 10.172.204.5 | ------------------ | Arlington, Tx,  USA | ------- | Htc frisbee |
| 5 | 43 | 10.172.204.11 | ------------------ | Arlington, Tx,  USA | 571ms | Htc frisbee |
| 6 | 38 | 10.164.162.234 | ------------------- | Arlington, Tx,  USA | 616 ms | Htc frisbee |
|  |  |  |  |  |  |  |