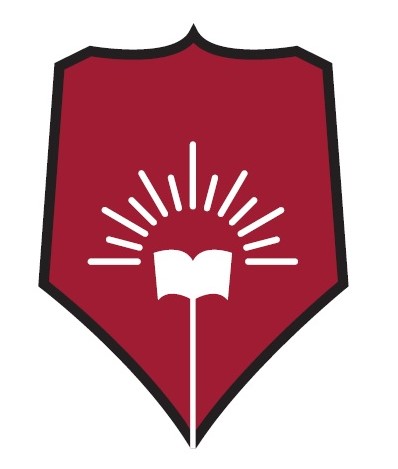
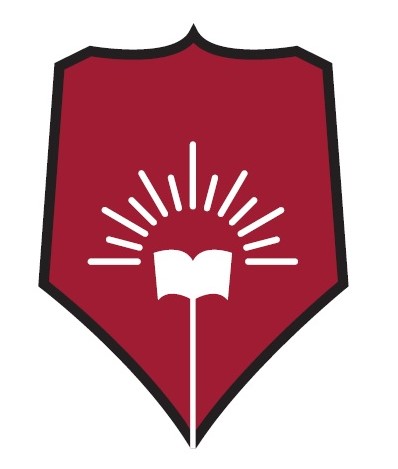
**Experiment No.: 8**

**Network Packet Analyzer**

**Understand the operation of TCP/IP layers**

****

**Aim**:Use **Wireshark** to understand the operation of TCP/IP layers :

* Ethernet Layer : Frame header, Frame size etc.
* Data Link Layer : MAC address, ARP (IP and MAC address binding)
* Network Layer : IP Packet (header, fragmentation), ICMP (Query and Echo)
* Transport Layer: TCP Ports, TCP handshake segments etc.
* Application Layer: DHCP, FTP, HTTP header formats

1. **Objectives:** To explore the network packet analyzer Wireshark on different TCP/IP layer. To introduce concepts and fundamentals of data communication and computer networks.
2. **Outcomes:** The learner will be able to

* Analyze the functioning of various protocols.
* Use of protocols in networks.
* Recognize the need for networking TCP/IP protocols.

1. **Hardware/Software required: Wireshark**
2. **Theory:**

**Wireshark** is a [free and open-source](http://en.wikipedia.org/wiki/Free_and_open_source_software) [packet analyzer](http://en.wikipedia.org/wiki/Packet_analyzer). It is used for [network](http://en.wikipedia.org/wiki/Computer_network) troubleshooting, analysis, software and [communications protocol](http://en.wikipedia.org/wiki/Communications_protocol) development, and education. Wireshark is very similar to [tcpdump](http://en.wikipedia.org/wiki/Tcpdump), but has a [graphical](http://en.wikipedia.org/wiki/Graphical_user_interface) [front-end](http://en.wikipedia.org/wiki/Front-end_and_back-end), plus some integrated sorting and filtering options.

Wireshark allows the user to put the network interfaces that support [promiscuous mode](http://en.wikipedia.org/wiki/Promiscuous_mode) into that mode, in order to see all traffic visible on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic. However, when capturing with a packet analyzer in promiscuous mode on a port on a [network switch](http://en.wikipedia.org/wiki/Network_switch), not all of the traffic traveling through the switch will necessarily be sent to the port on which the capture is being done, so capturing in promiscuous mode will not necessarily be sufficient to see all traffic on the network. [Port mirroring](http://en.wikipedia.org/wiki/Port_mirroring) or various [network taps](http://en.wikipedia.org/wiki/Network_tap) extend capture to any point on net; simple passive taps are extremely resistant to [malware](http://en.wikipedia.org/wiki/Malware) [tampering](http://en.wikipedia.org/wiki/Tamper_resistance).

Wireshark Installation steps:

1. Download wireshark
2. Double click on the wireshark icon. We get an open window as given below.

An example of a Wireshark capture

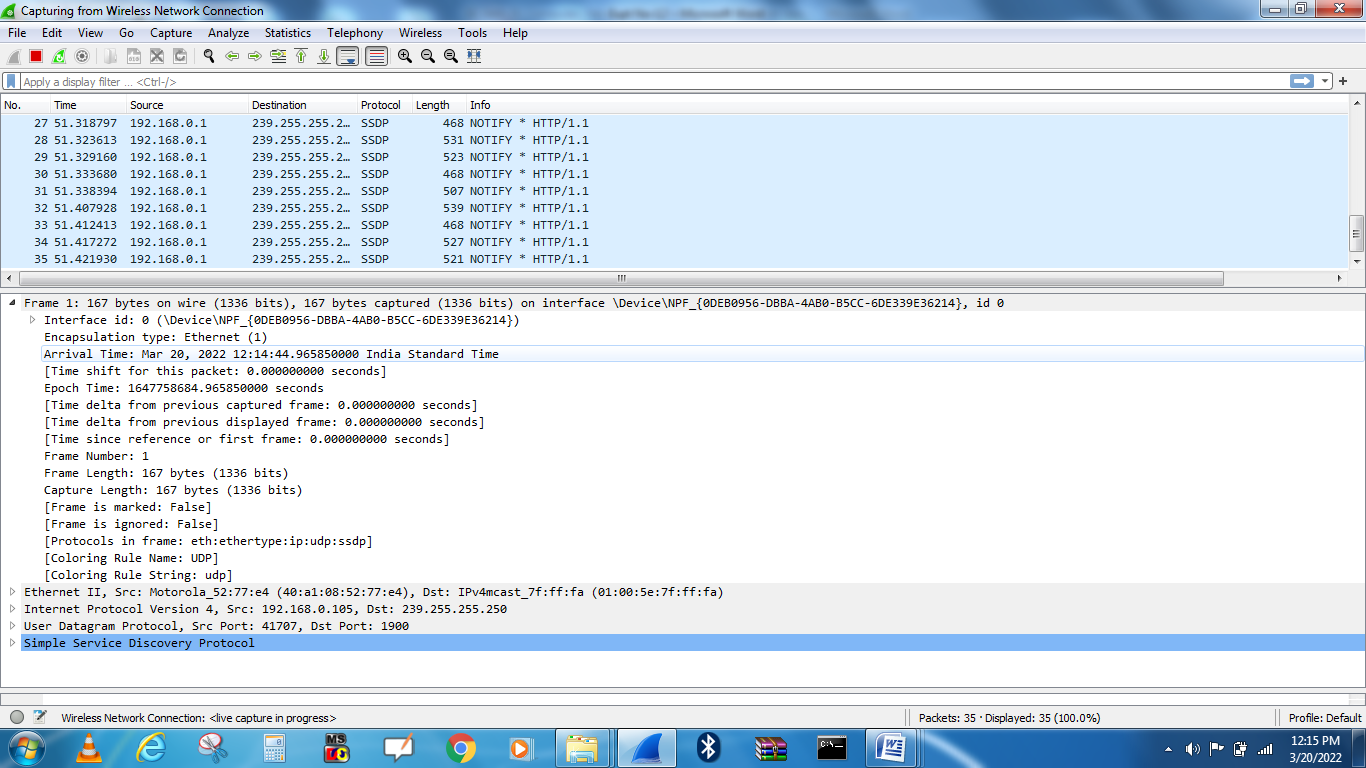


Figure 2. Frame format along with the Wireshark

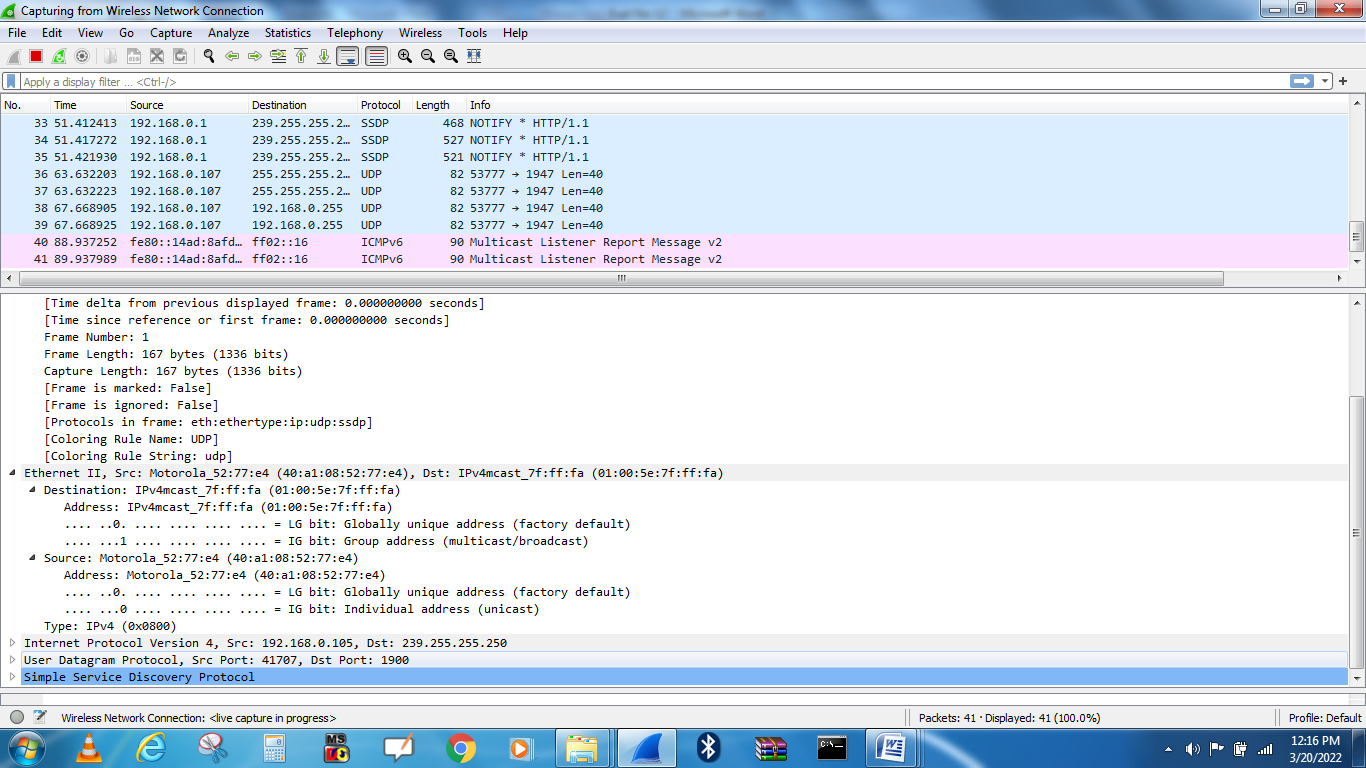
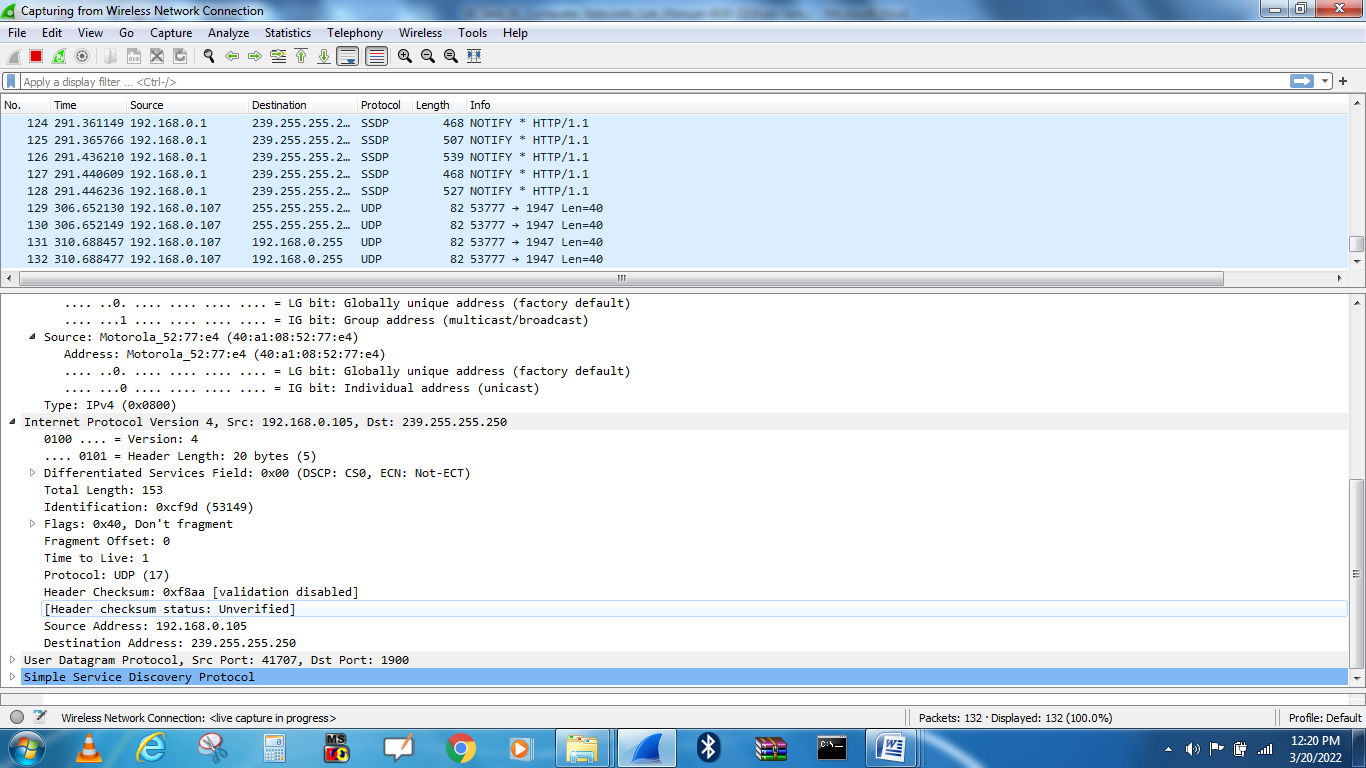
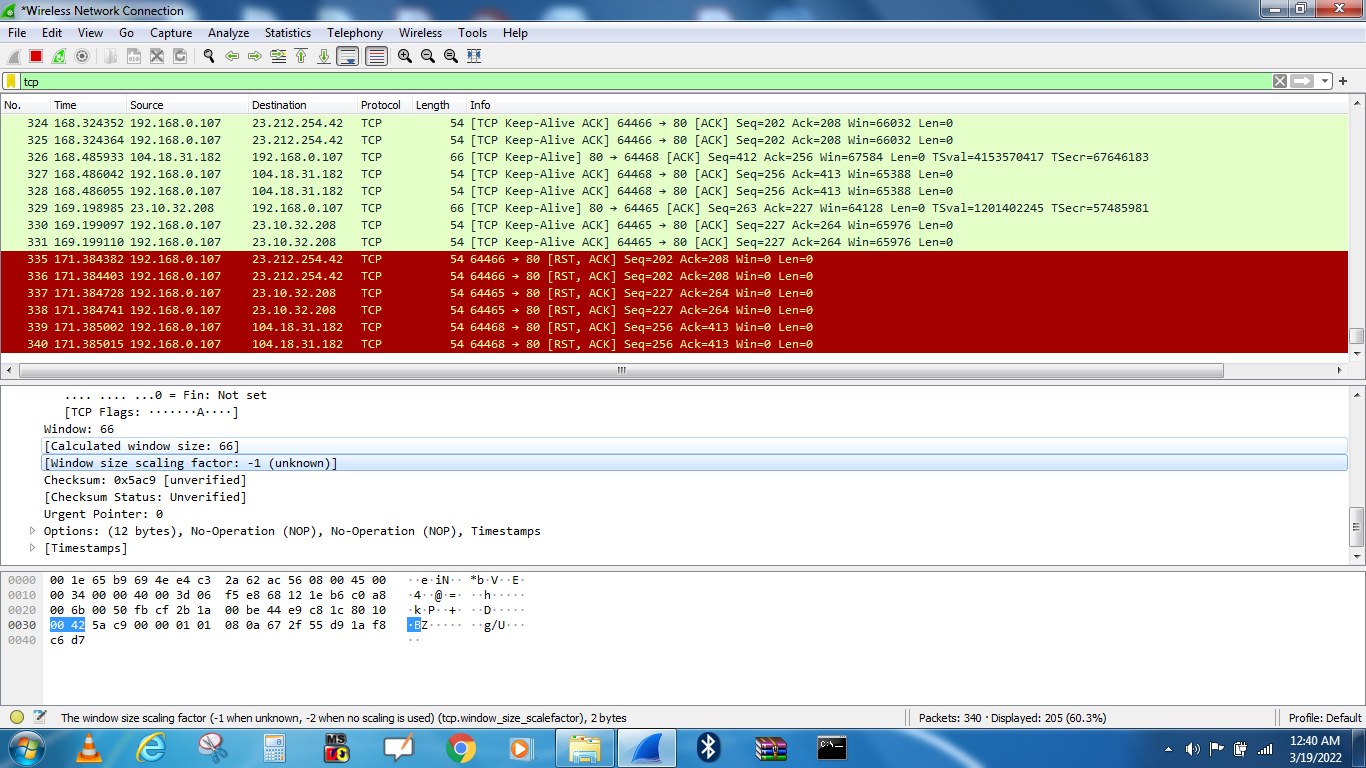


Figure 2. Ethernet II (Layer 2) header along with the Wireshark





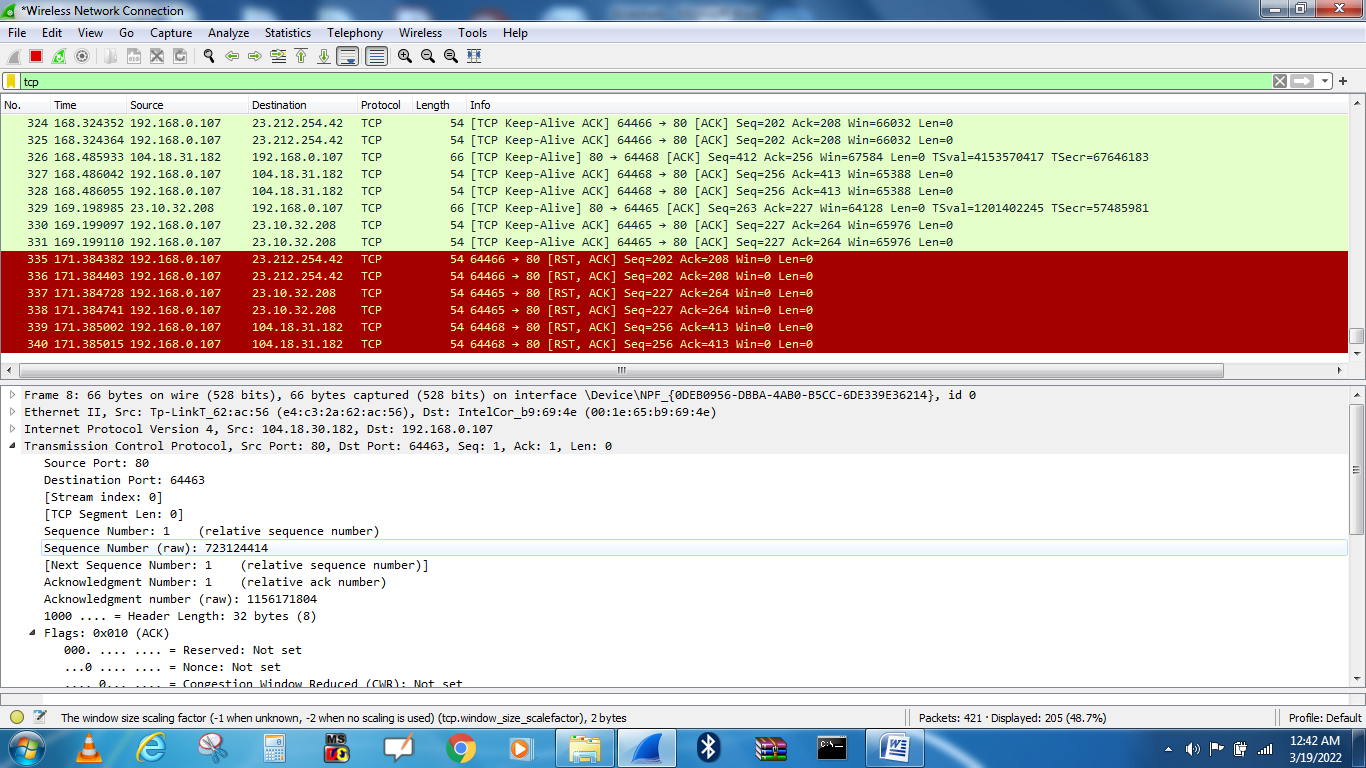
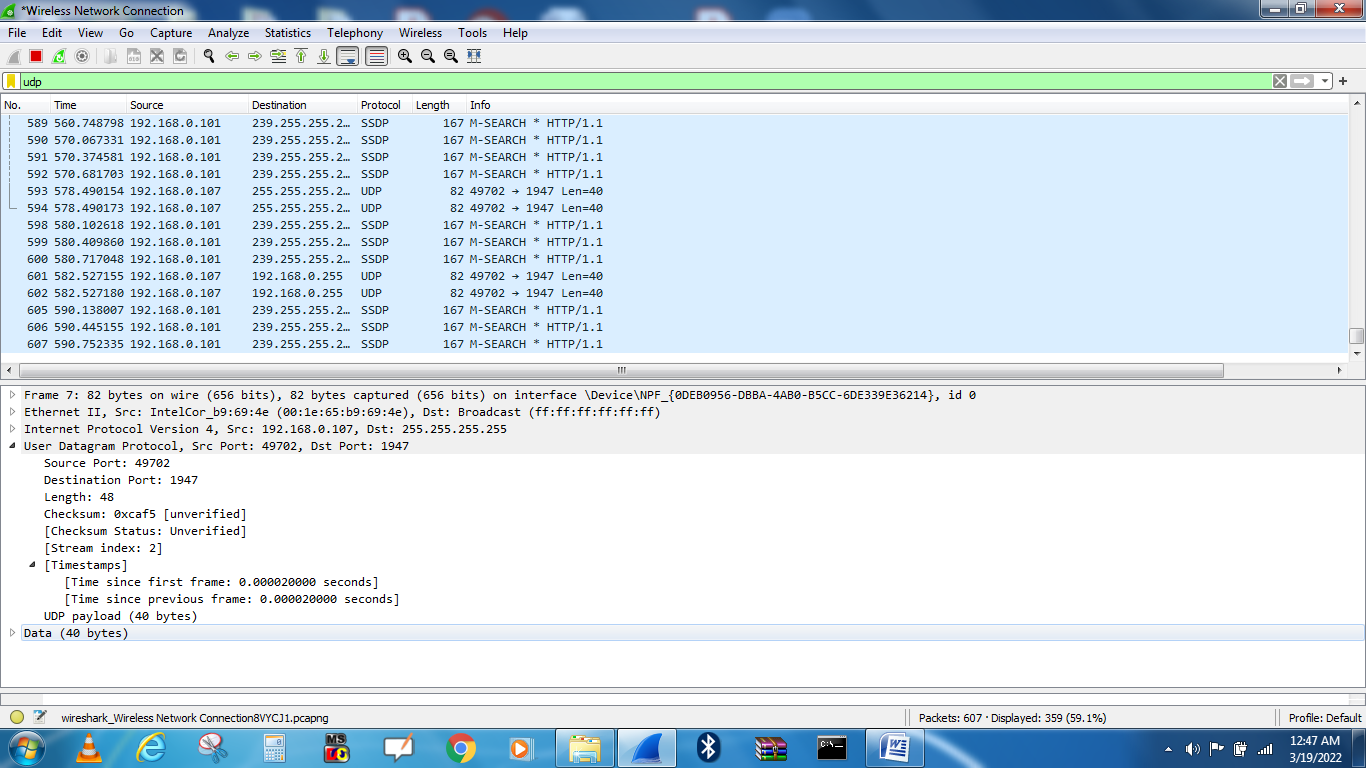


Figure 3. IP Header (Layer-3) along with the Wireshark



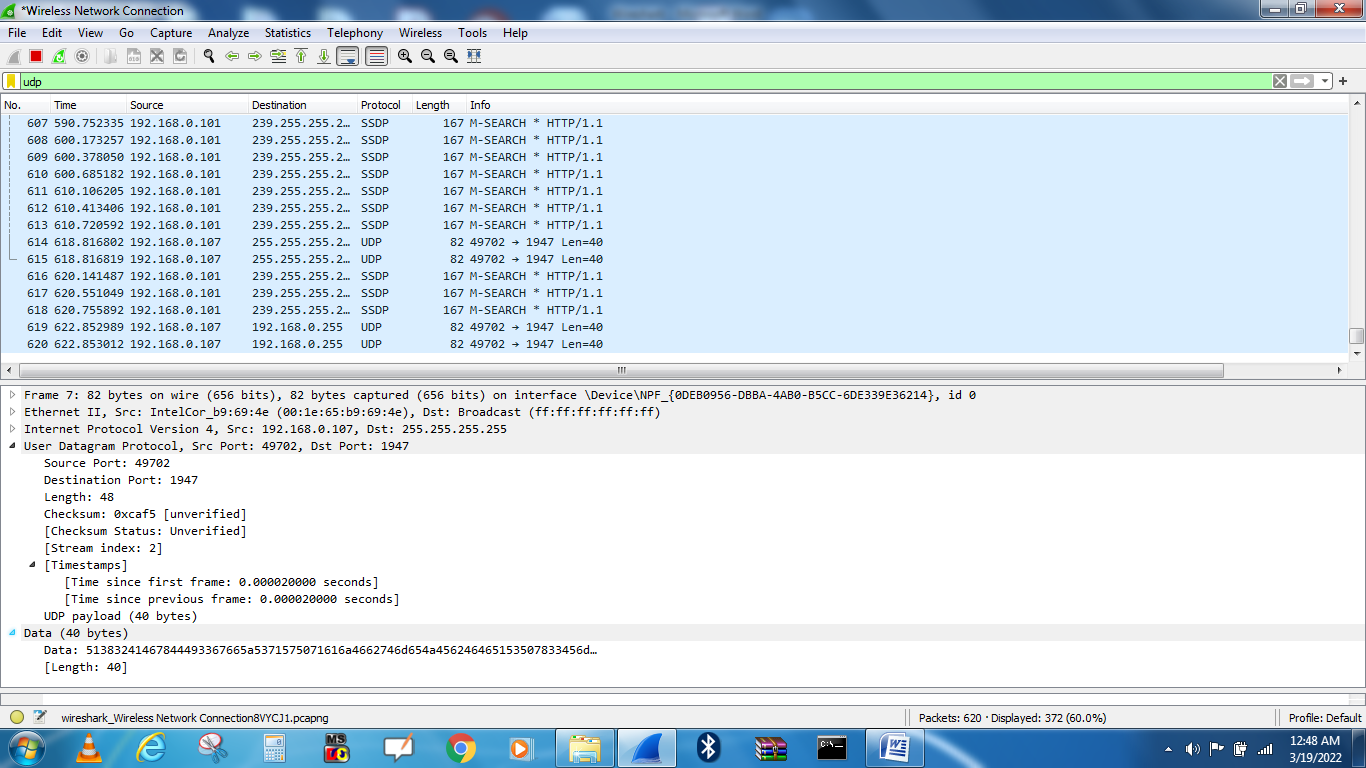
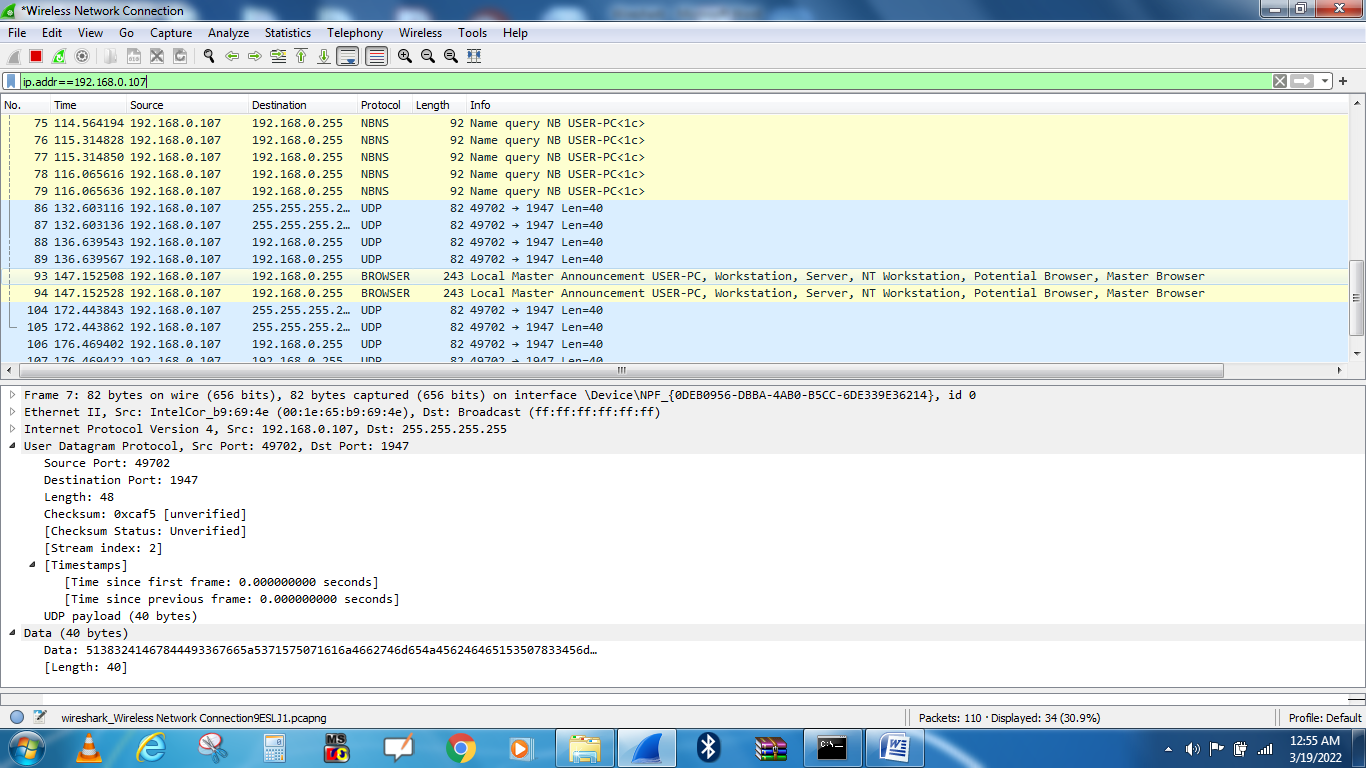
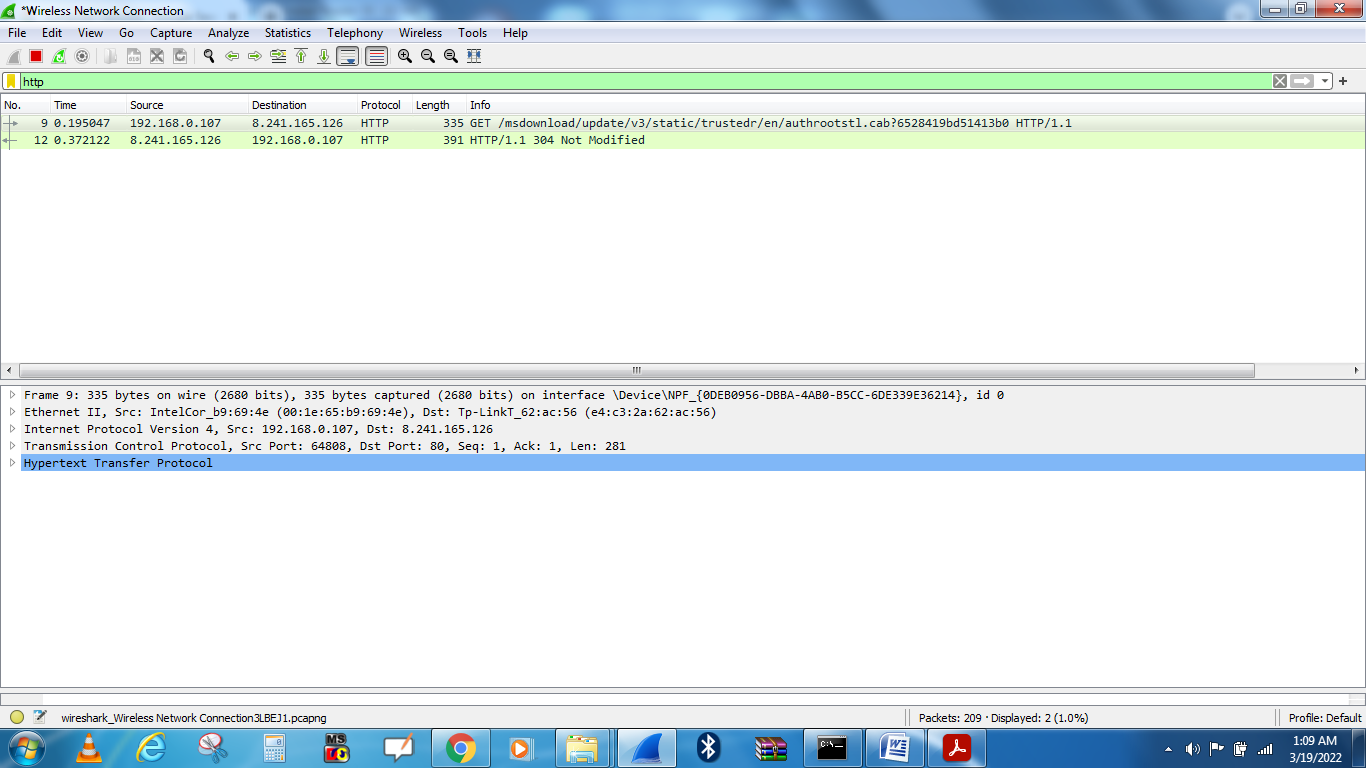
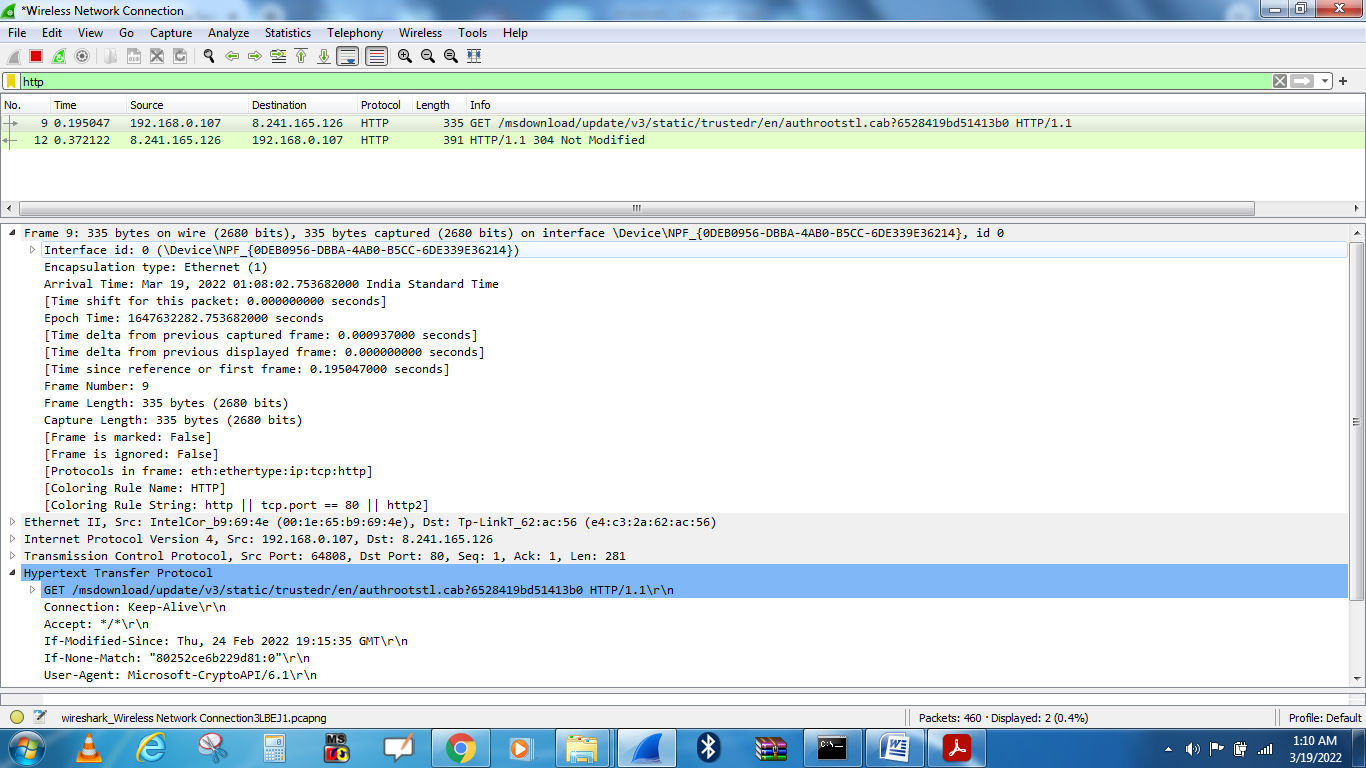
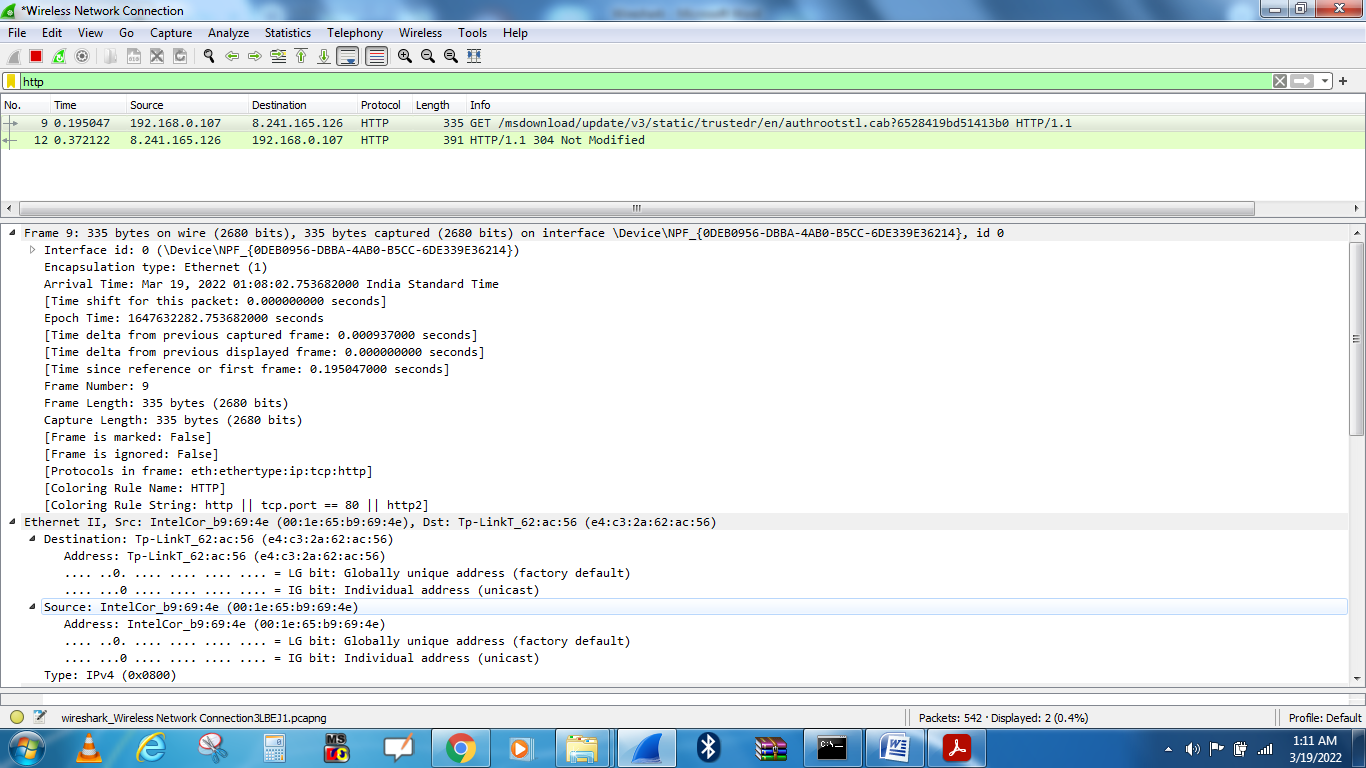


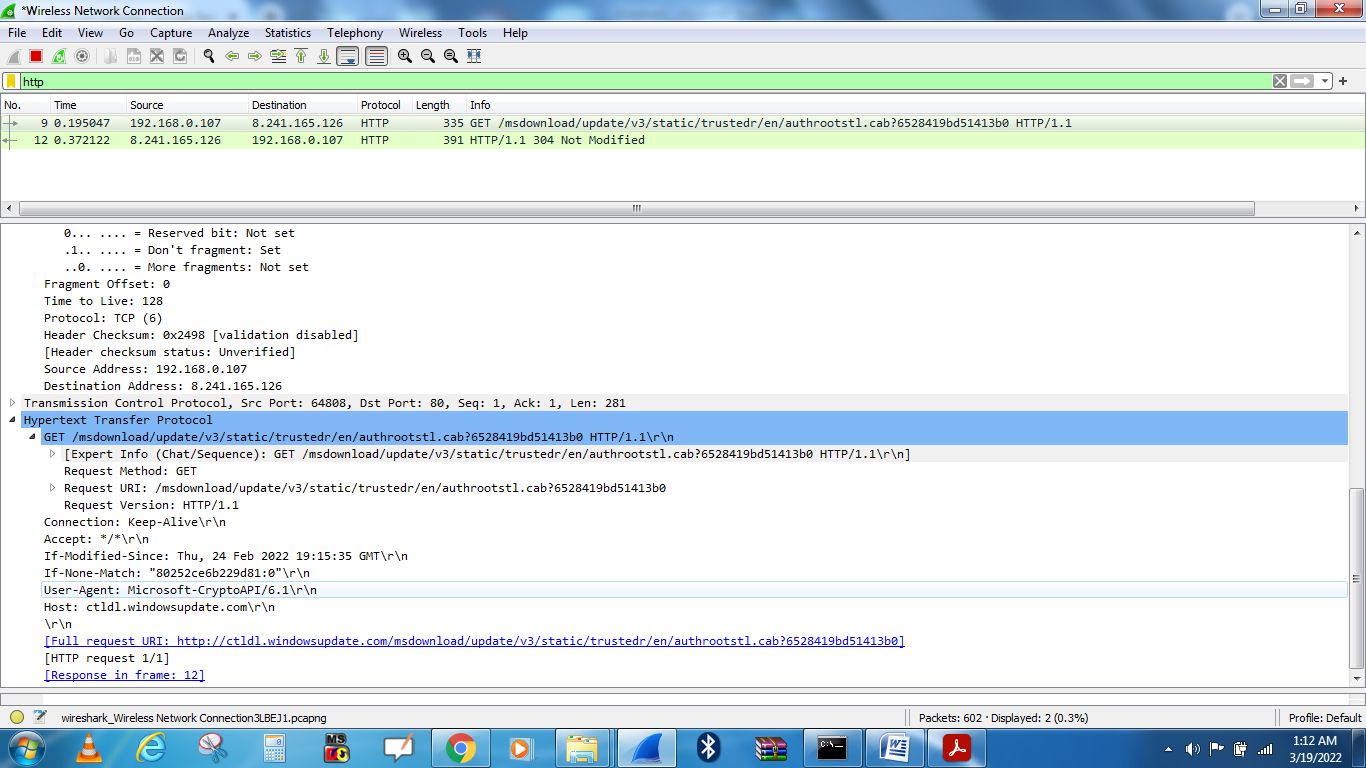
Figure 4. TCP/UDP Header (Layer-4) along with the Wireshark

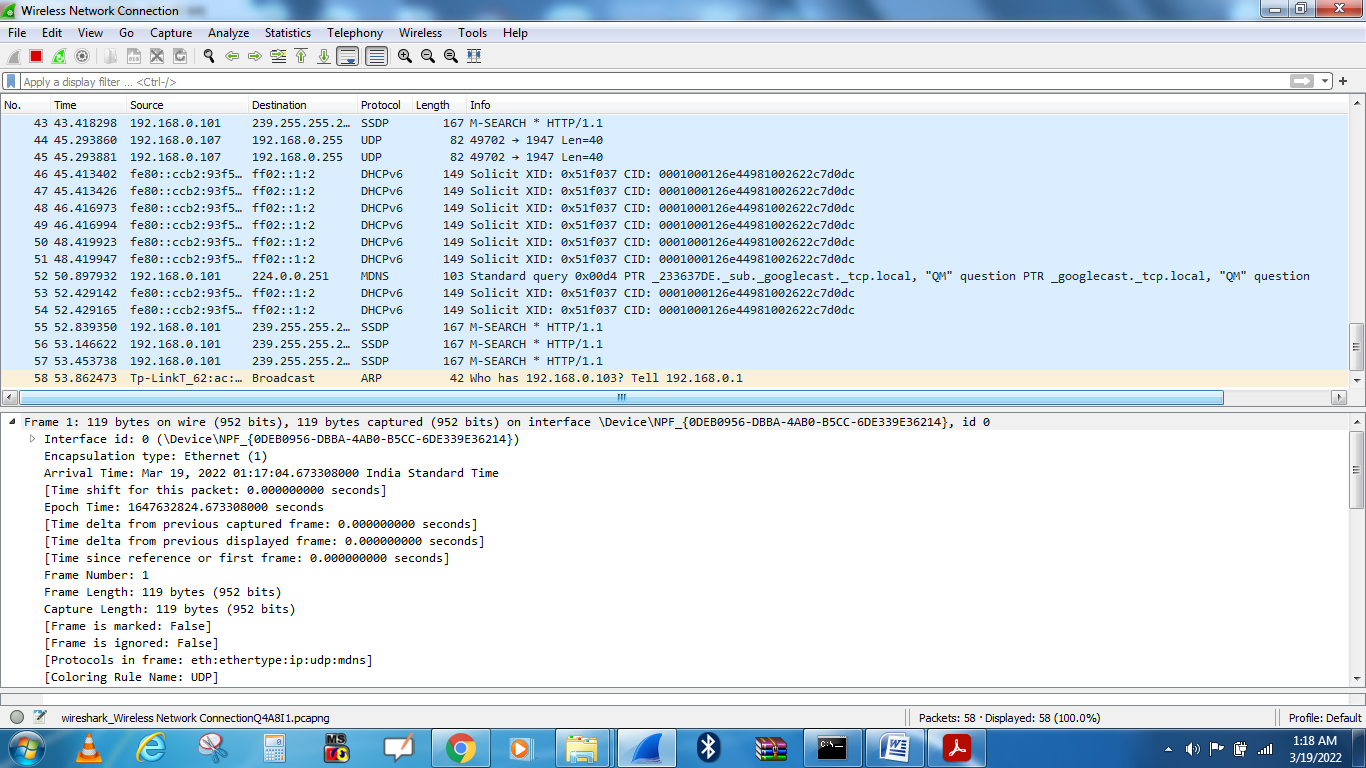












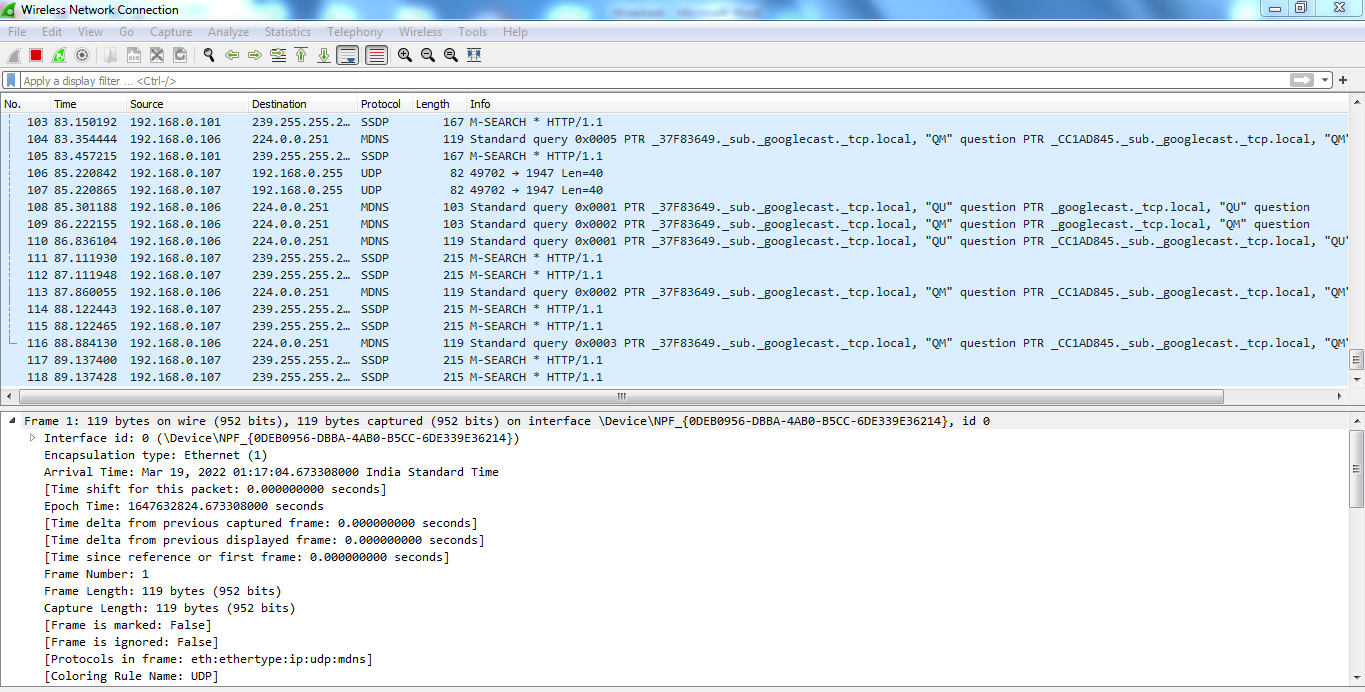
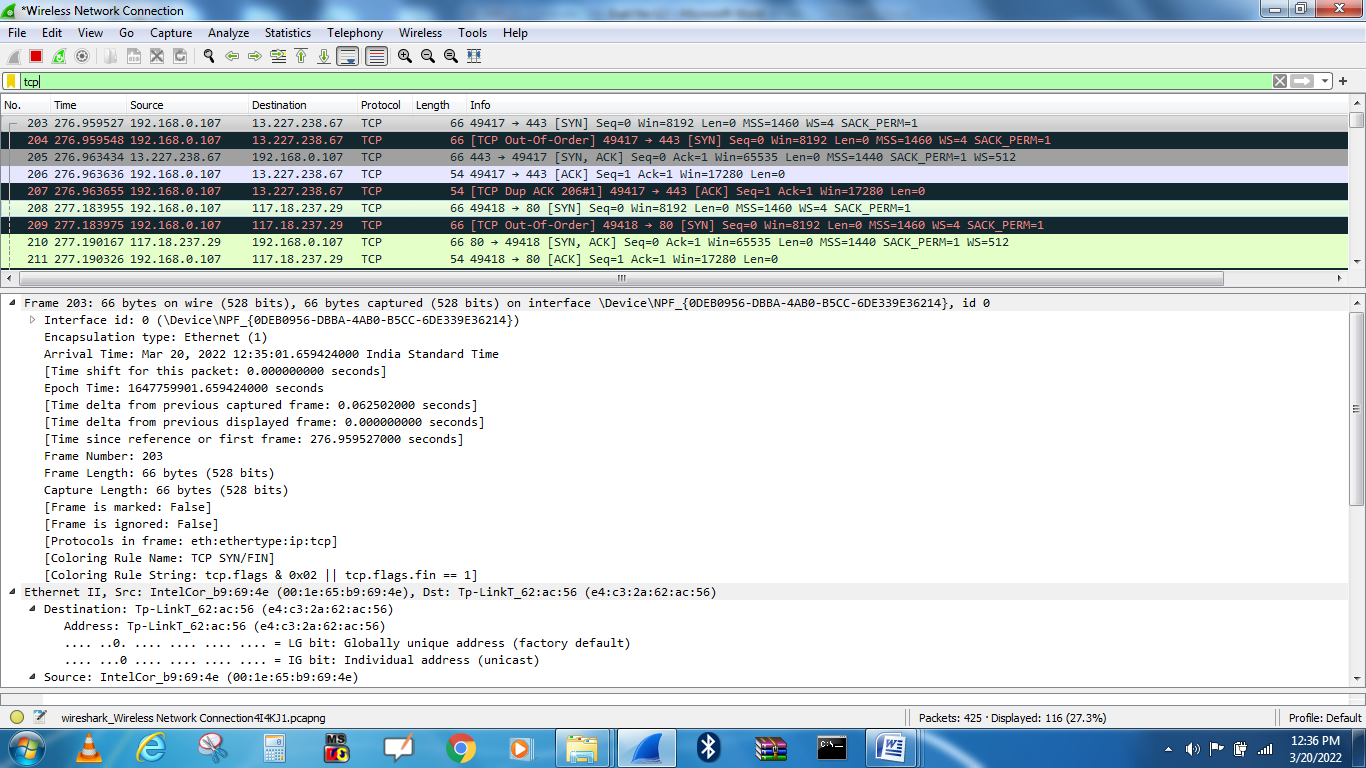


Figure 5. Application Layer: DHCP, FTP, HTTP header formats Header (Layer-5) along with the Wireshark

**TCP Three-way Handshake**

The delta value between frames 1 and 2 can be used as a TCP transport connect baseline value. Other important information gathered from this handshake: • Window Size • SACK • Maximum Segment Size • Window Scale Option value



1. **Output Analysis:**

(Students should write output analysis based on the working of different topology and different networking devices used in simulation. Specify each scenario explicitly with output analysis)

1. **Additional Learning:**

(Students should write additional learning on their own based on what additionally they learnt after performing the experiment)

1. **Conclusion :**

(Students should write conclusion on their own)

1. **Viva Questions:**

* State the header format of DLL, IP, TCP and UDP and put values of one the packet that you have captured using Wireshark
* Explain how layers are interrelated.

1. **References:**
   1. A.S. Tanenbaum, “Computer Networks”, Pearson Education, (4e)
   2. B.A. Forouzan, “Data Communications and Networking”, TMH (5e)
2. James F. Kurose & K W Ross: Computer Networking: A Top Down Approach, Pearson Education (LPE)