Name: Aditya R Sawant
Class: TE4
Roll No.: 46
Batch: D
Subject: Computer Networks

Experiment No. 5

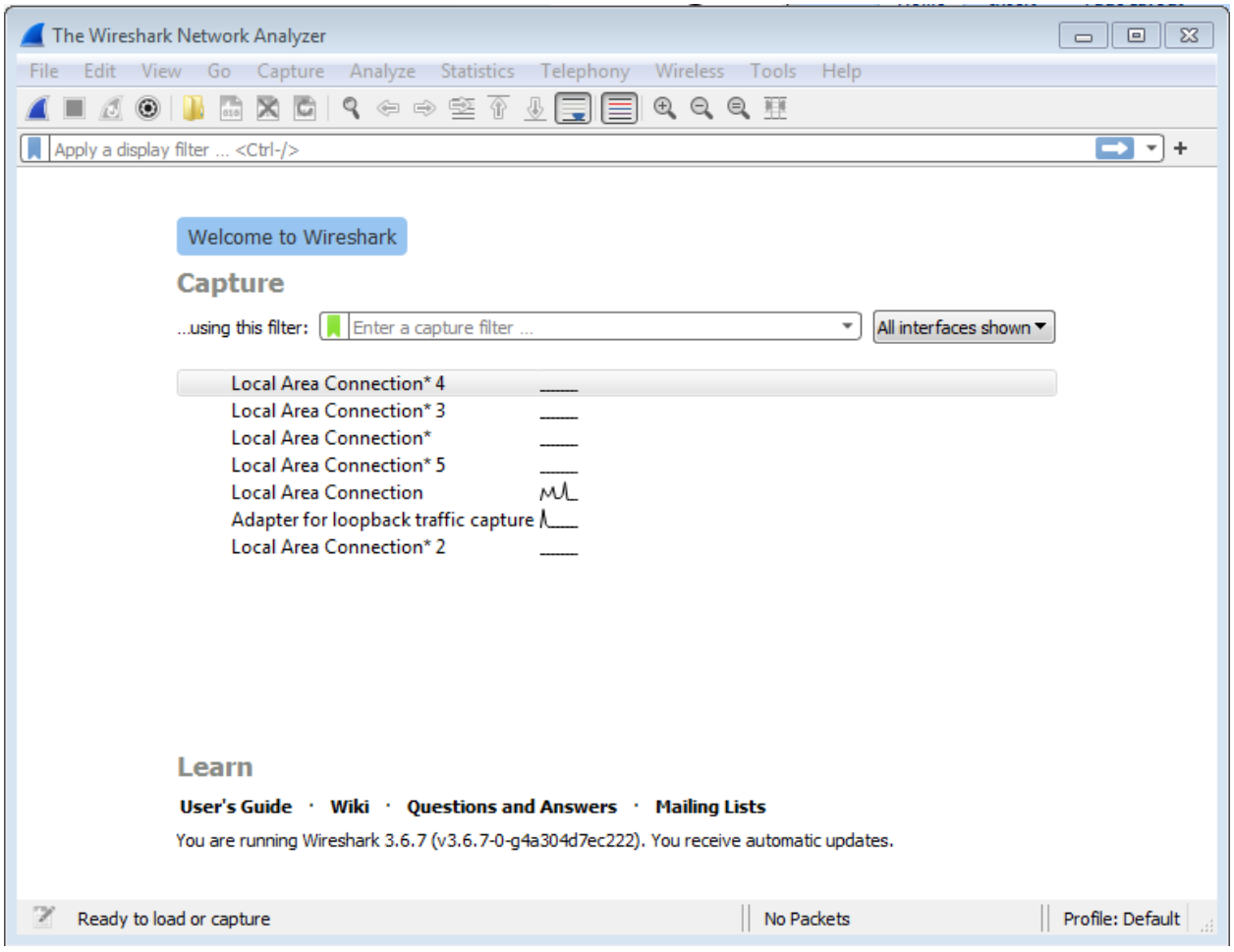
Aim: Using Wireshark understand the operations of TCP/IP layers:
Ethernet Layer: Frame header, rame size tec.
Data Link Layer: MAC address, ARP.
Network Layer: IP packet(Header, fragmentation, ICMP).
Transport Layer: TCP Ports, TCP handshake.
Application Layer: FTP header format.

Theory: Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets. Wireshark can be downloaded from their official website (https://www.wireshark.org/). For the linux users wireshark can be installed from package repositories.

Capturing the packets:

After installing the wireshark go to the terminal in ubuntu and type wireshark.The following page will open browser.

Fig 1: Wireshark home page



Double-click the name of a network interface under Capture to start capturing packets on that interface. As soon ass any interface's name is clicked, the packets start to appear in real time. Wireshark captures each packet sent to or from your system. Click the red "Stop" button near the top left corner of the window when you want to stop capturing traffic.

Color Coding

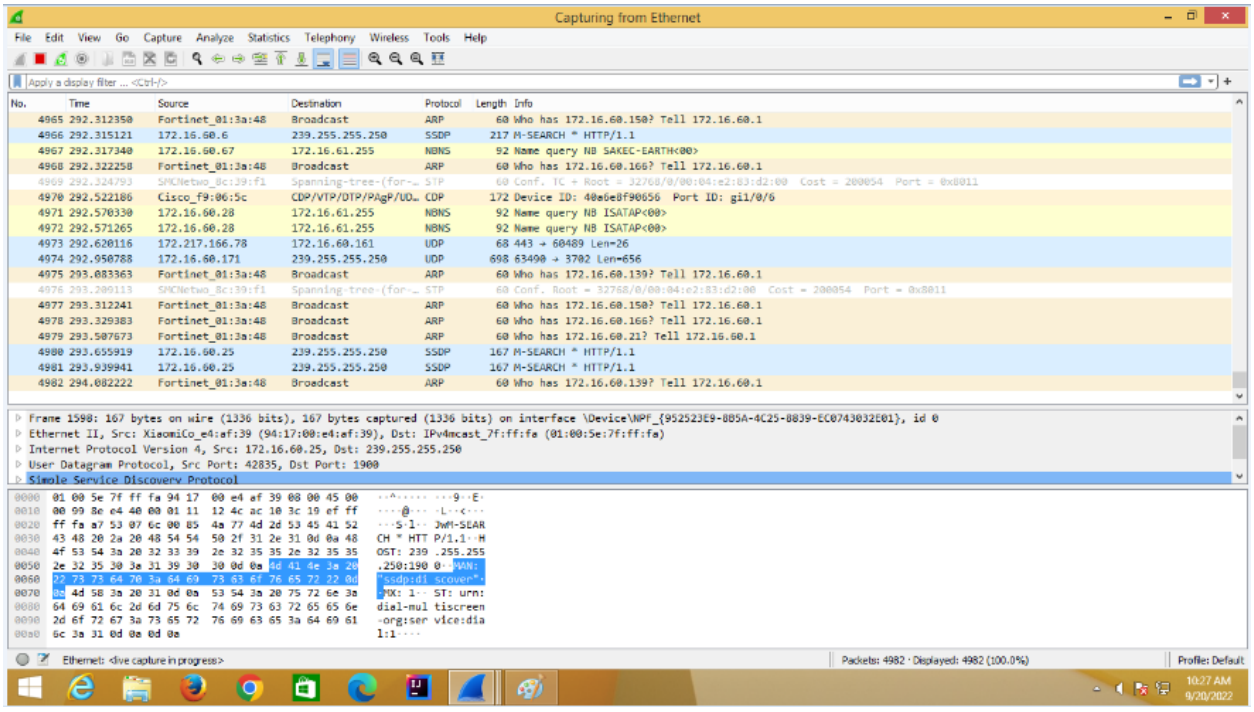
The packets are highlighted in a variety of different colors. Wireshark uses colors to identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors, for example, packets delivered out of order.
To view exactly what the color codes mean, click View > Coloring Rules. We can also customize and modify the coloring rules.

Filtering Packets

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type “dns” and you’ll see only DNS packets. When you start typing, Wireshark will help you auto complete your filter.

Ethernet Layer

Fig 2:Ethernet header captured by wireshark

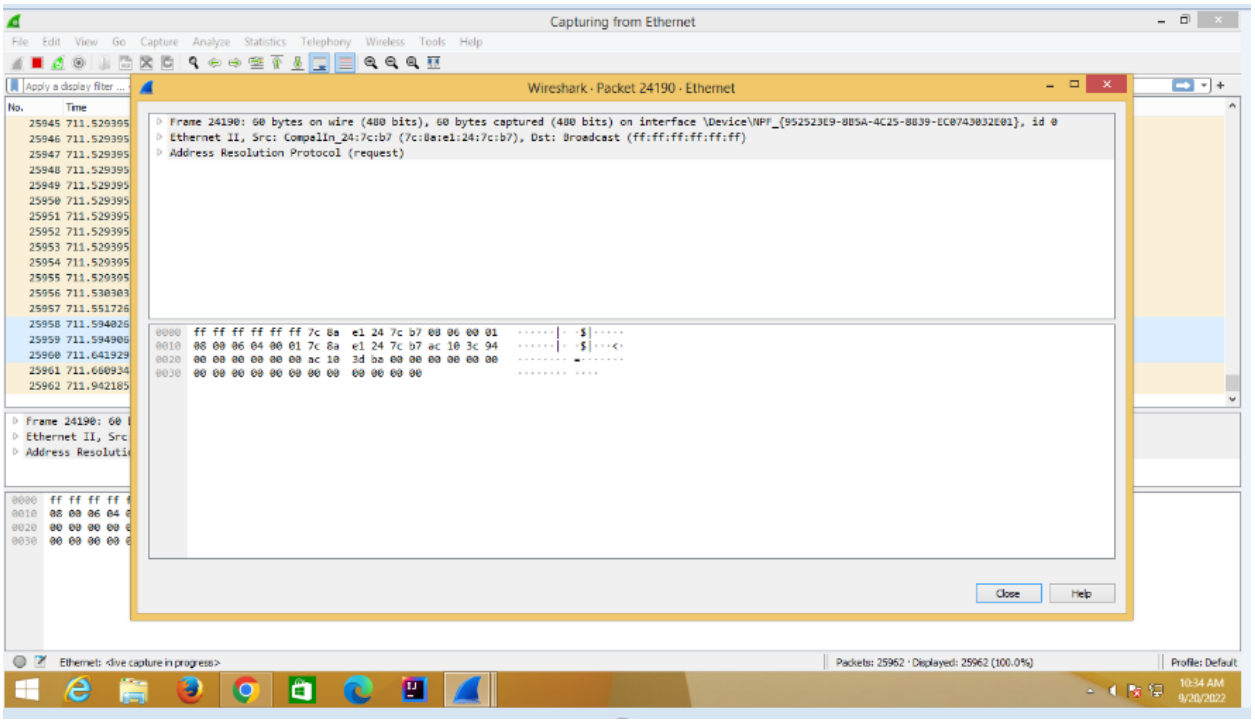


Ethernet layer (figure 2) is very simple. It contains a destination address and a source address. The data link layer is relatively simple in that it is only concerned with getting a frame to the next adjacent node on the physical medium.

Network Layer

The Ethernet layer is concerned with node to node. The IP layer is concerned with moving between networks, hence the original meaning of the term internetwork, from whence Internet was derived. Highlighting the network layer shows more details. From Figure C, we can see the source and destination IP addresses as well as the IP header length (20 bytes in this case). We1 can also see the Differentiated Services (DiffServ) area. This would be where extra information relating to the packet's type of service goes. For most packets on a LAN this is set to zero, which means best effort.

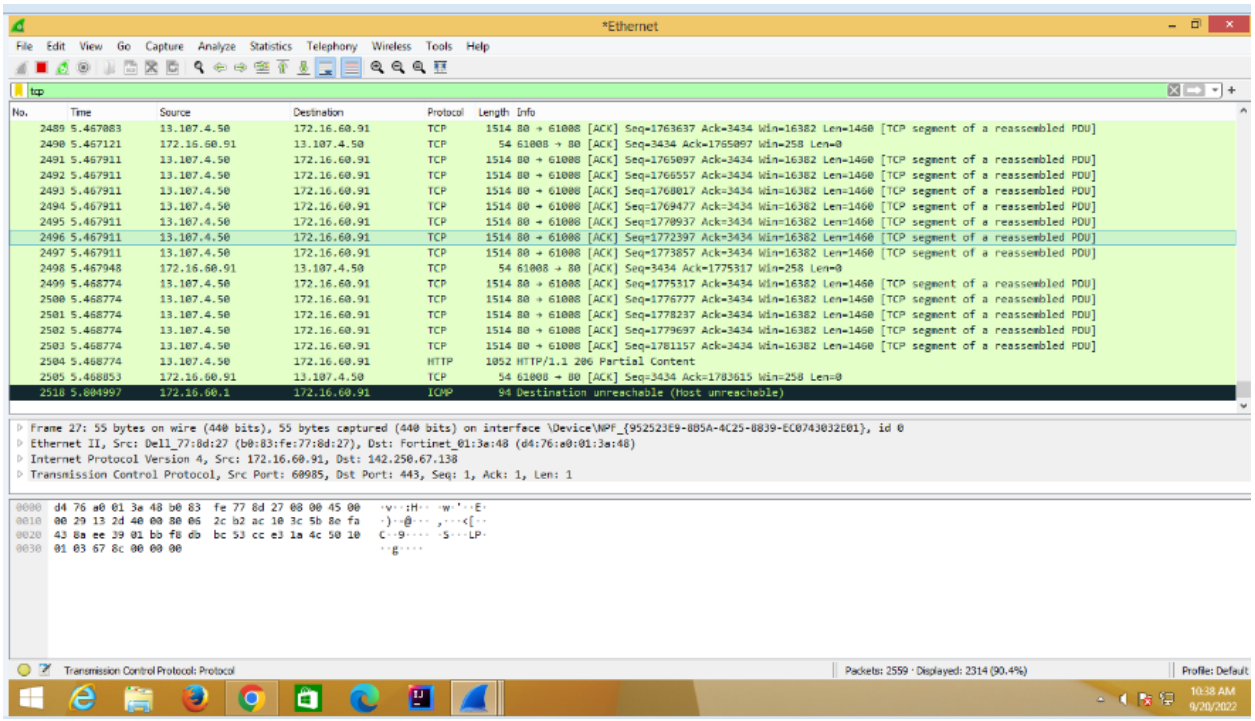
Fig 3: IP header captured by wireshark



Transport Layer

The transport layer is where applications communicate via the use of ports. Figure 4 will show the source port i.e 40519 and the destination port i.e 5001. The header length (32 bytes in this case) and the sequence number are displayed. The sequence number generally will change for each packet.

Fig 4: Transport layer header captured by wireshark

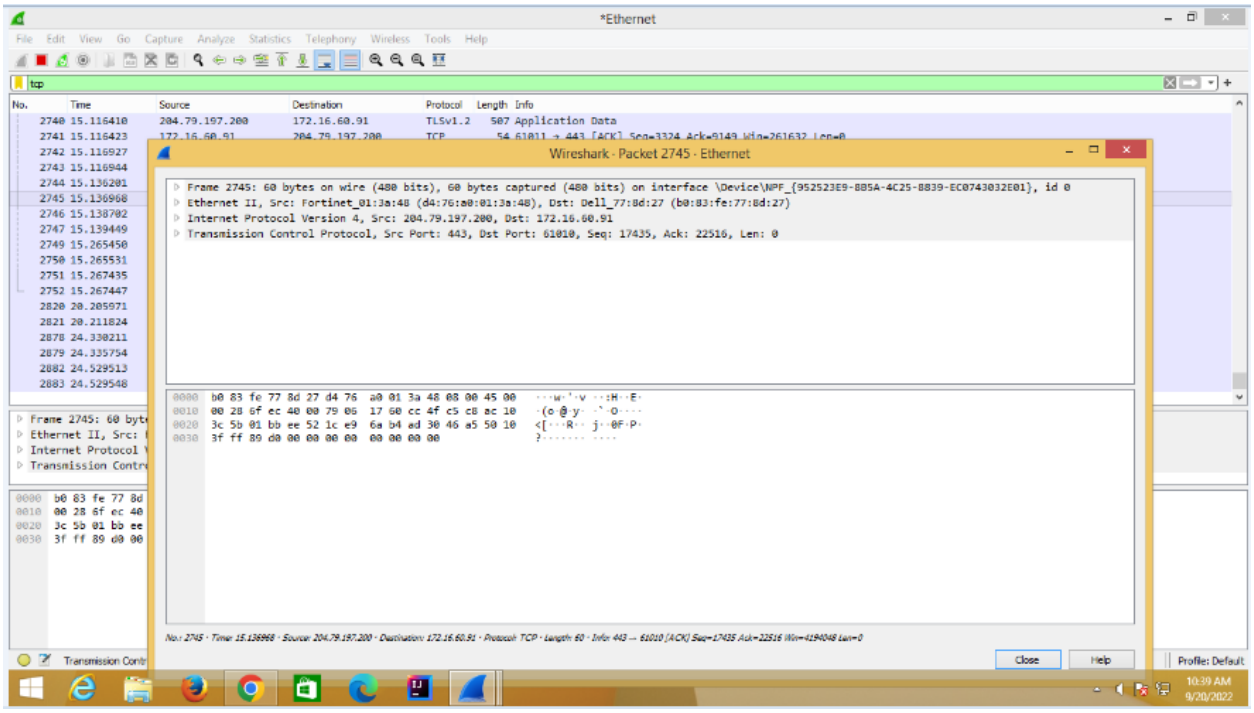


Application layer (FTP header)

FTP stands for File transfer protocol, which is used to transfer files from one host to other. It makes use of two separate connections (Control and Data connections) before transferring files. It uses TCP as its underlying network.

The figure below shows wiresharks captures when a file is transferred using FTP.

Fig 5: FTP File Transfer captured by wireshark



Firstly, the Client (10.10.10.7) makes a request to the Server (78.47.100.174) for transferring a file. After that, 4 to 5, request and response messages are transferred between the two machines. Take a close look at Packet No. 10967, the client makes a request to the server for getting a file named “flag.rar”. In the next packet, server tries to send the file to the requested machine. Finally packet no 11091 indicates the transfer of file named “flag.rar” to 10.10.10.7.

Conclusion: Wireshark is used to capture data packets and allows us to perform more precise analysis. The main focus of this tool is observing the data traffic within a network. This tool allows the user to examine their own computer, for protocol errors, problems within the network architecture, discovering and stopping hacker attacks.