EXPERIMENT NO. 4

AIM: Using wireshark understand the operations of TCP/IP layers:
Ethernet Layer: Frame header,Frame size tec.
Data Link Layer: MAC address, ARP.
Network Layer: IP packet(Header, fragmentation, ICMP).
Transport Layer: TCP Ports, TCP handshake segments etc.
Application Layer: FTP .,DHCP,HTTP header formats

Theory:

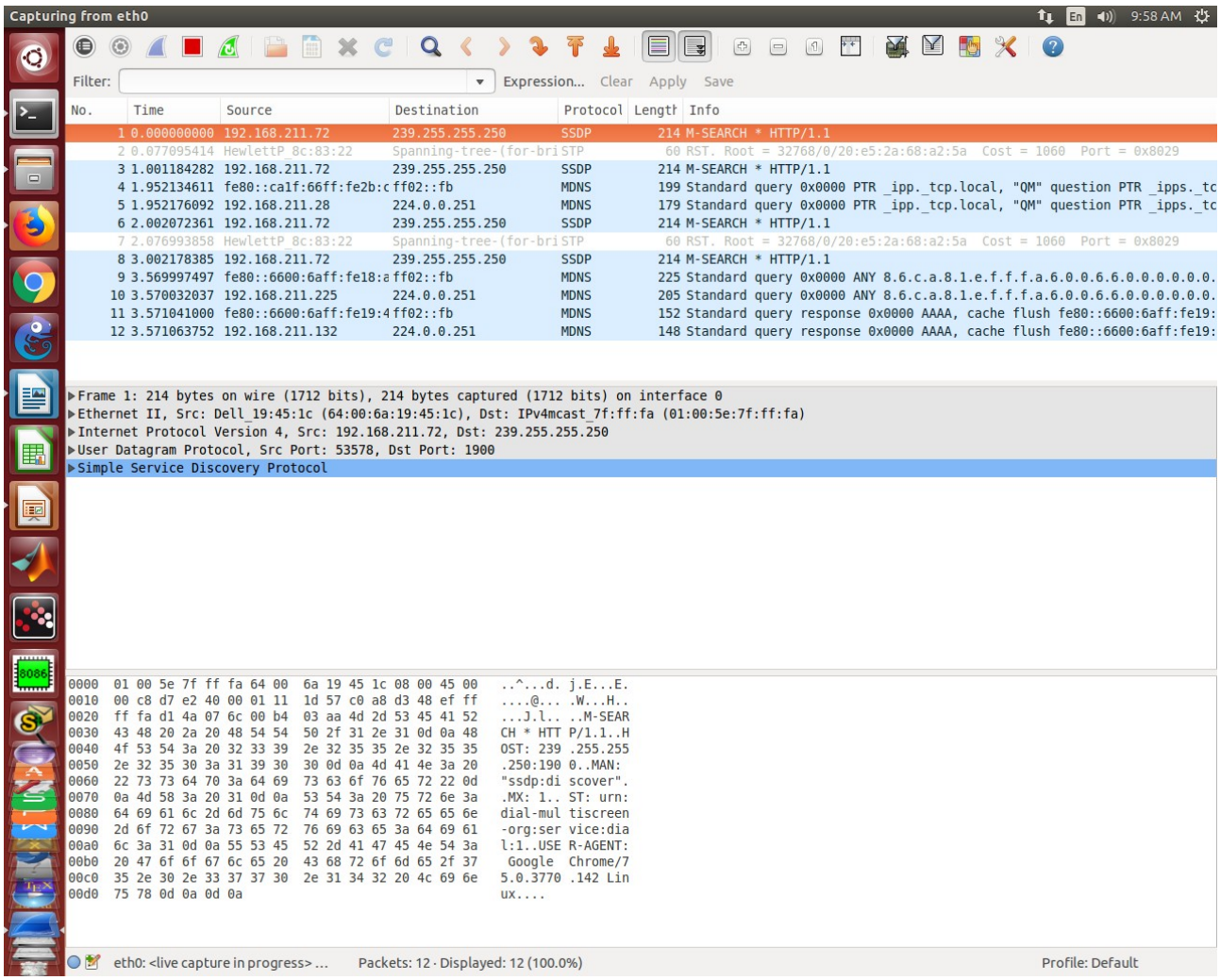
Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

Wireshark is a network or protocol analyzer (also known as a network sniffer) available for free at the Wireshark website. It is used to analyze the structure of different network protocols and has the ability to demonstrate encapsulation. The analyzer operates on Unix, Linux and Microsoft Windows operating systems, and employs the GTK+ widget toolkit and pcap for packet capturing. Wireshark and other terminal-based free software versions like Tshark are released under the GNU General Public License.

Wireshark shares many characteristics with tcpdump. The difference is that it supports a graphical user interface (GUI) and has information filtering features. In addition, Wireshark permits the user to see all the traffic being passed over the network.

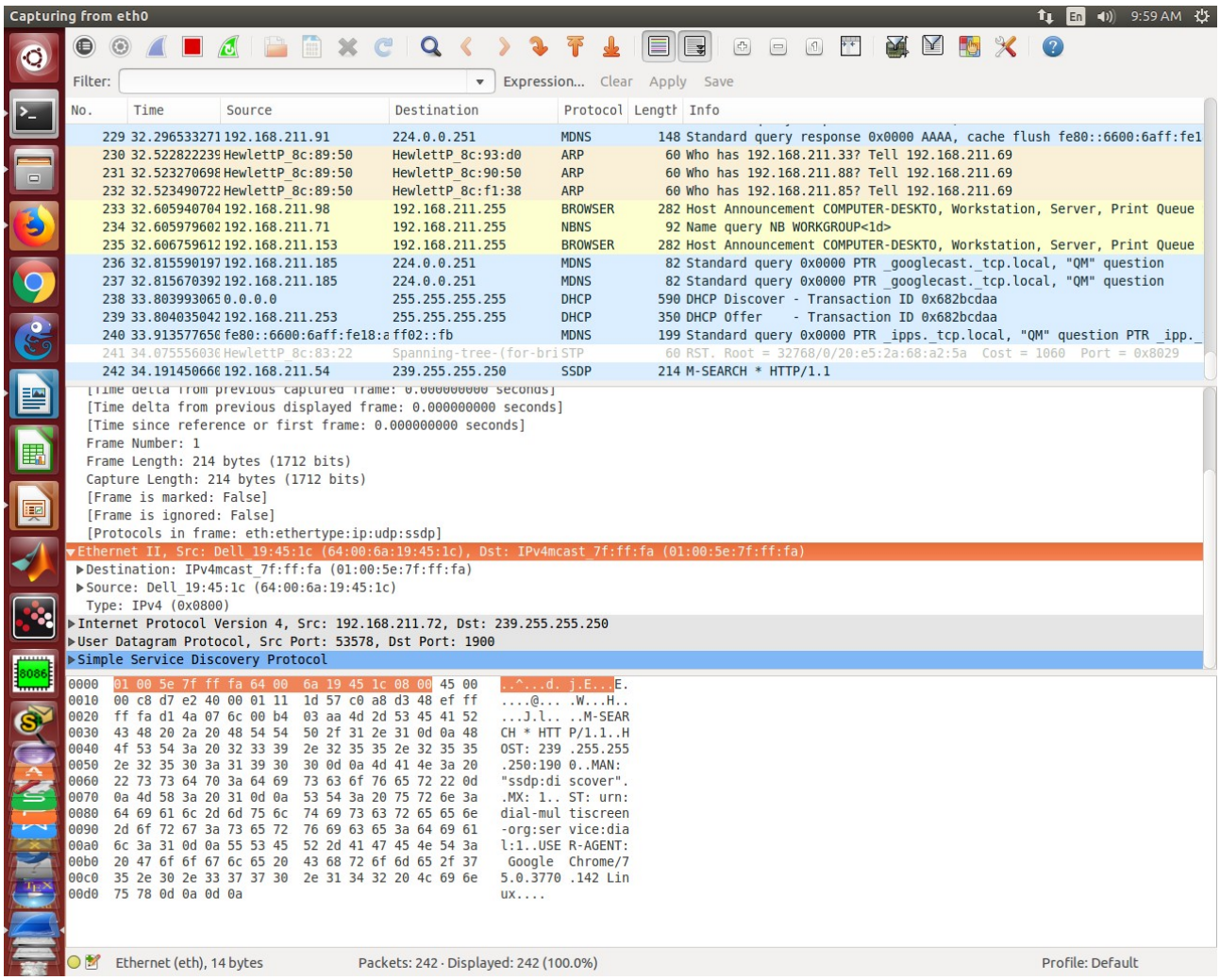
Features of Wireshark include:

- Data is analyzed either from the wire over the network connection or from data files that have already captured data packets.
- Supports live data reading and analysis for a wide range of networks (including Ethernet, IEEE 802.11, point-to-point Protocol (PPP) and loopback).
- With the help of GUI or other versions, users can browse captured data networks.
- For programmatically editing and converting the captured files to the editcap application, users can use command line switches.
- Display filters are used to filter and organize the data display.
- New protocols can be scrutinized by creating plug-ins.
- Captured traffic can also trace Voice over Internet (VoIP) calls over the network.
- When using Linux, it is also possible to capture raw USB traffic.



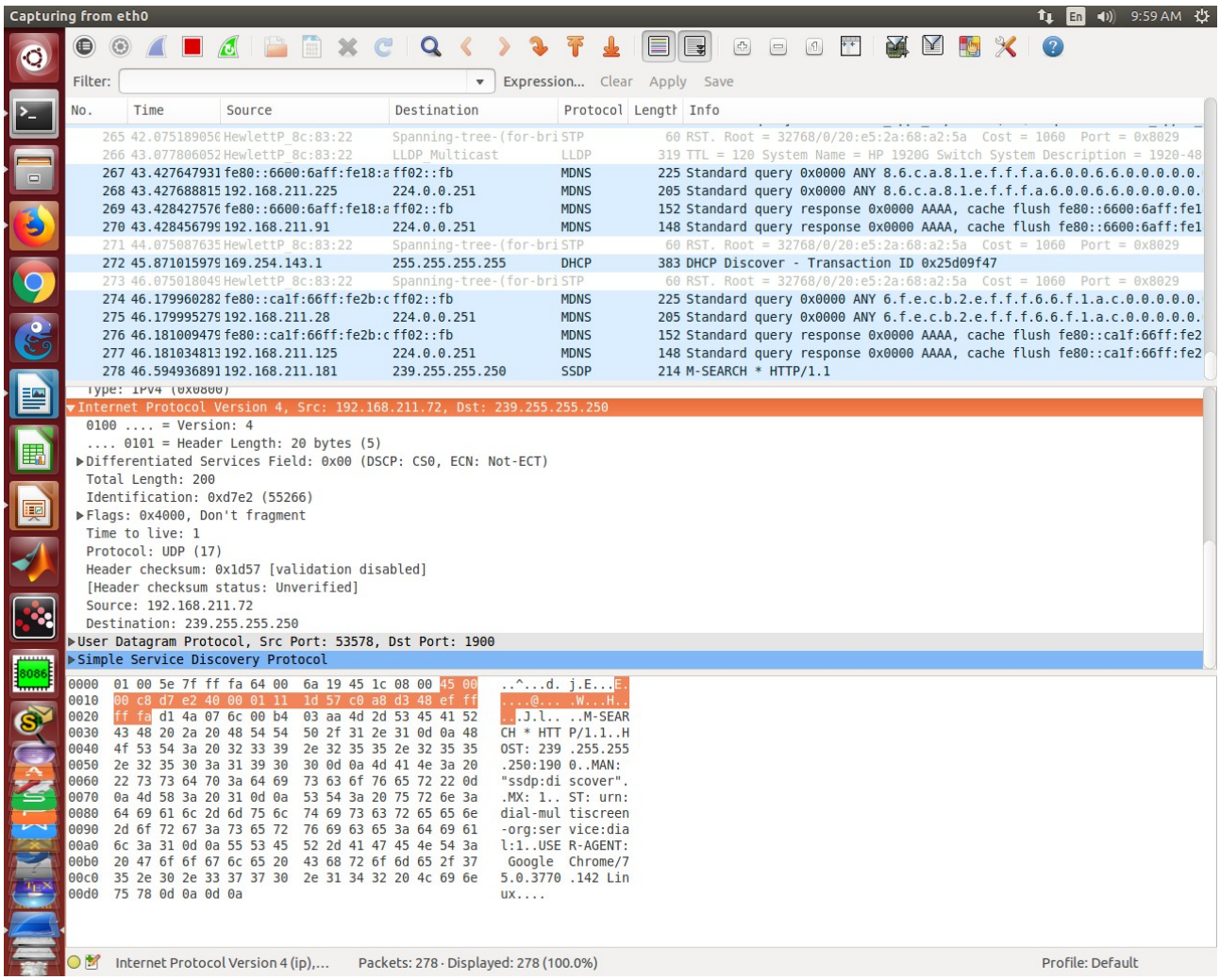
Ethernet Layer :

Ethernet layer 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.



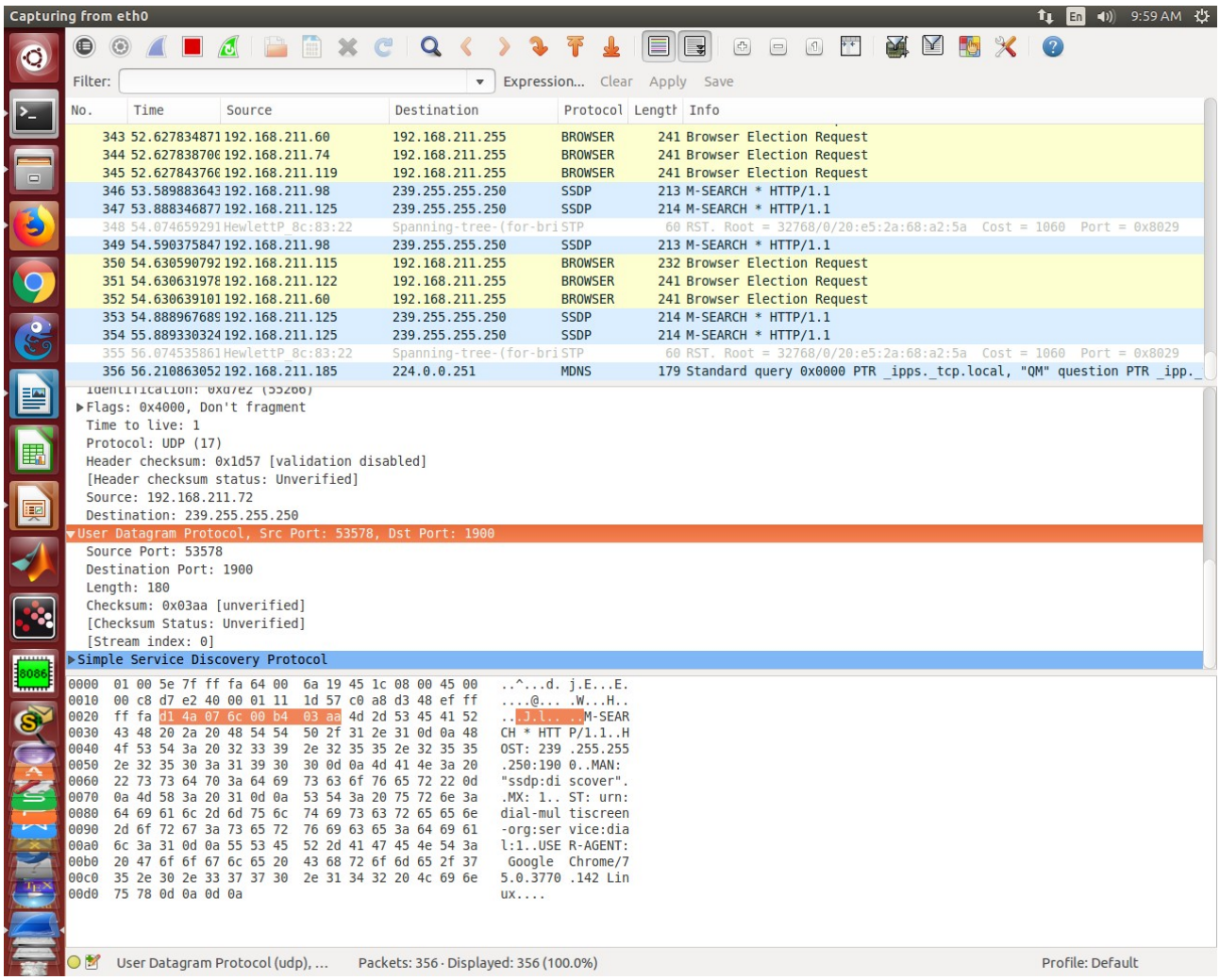
Network Layer:

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). We 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.



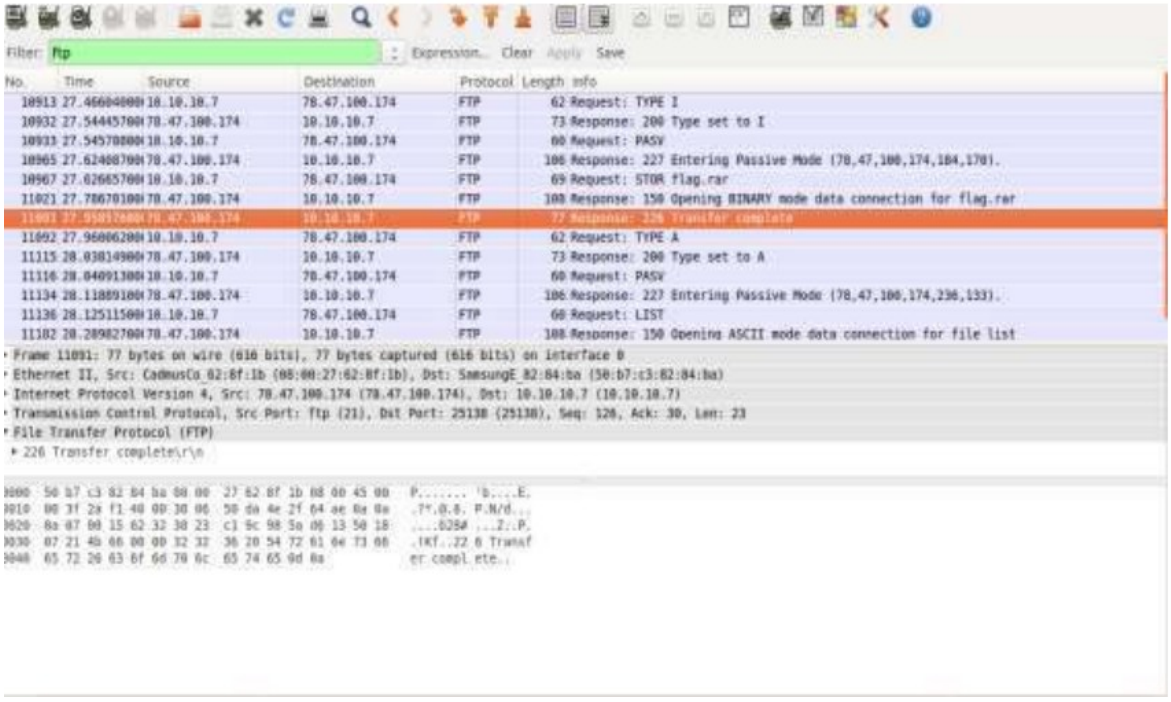
Transport Layer:

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.



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.



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 .