CN LAB ASSIGNMENT 04

ANTRIKSH SHARMA 13-08-2022
CS-A1
20070122021

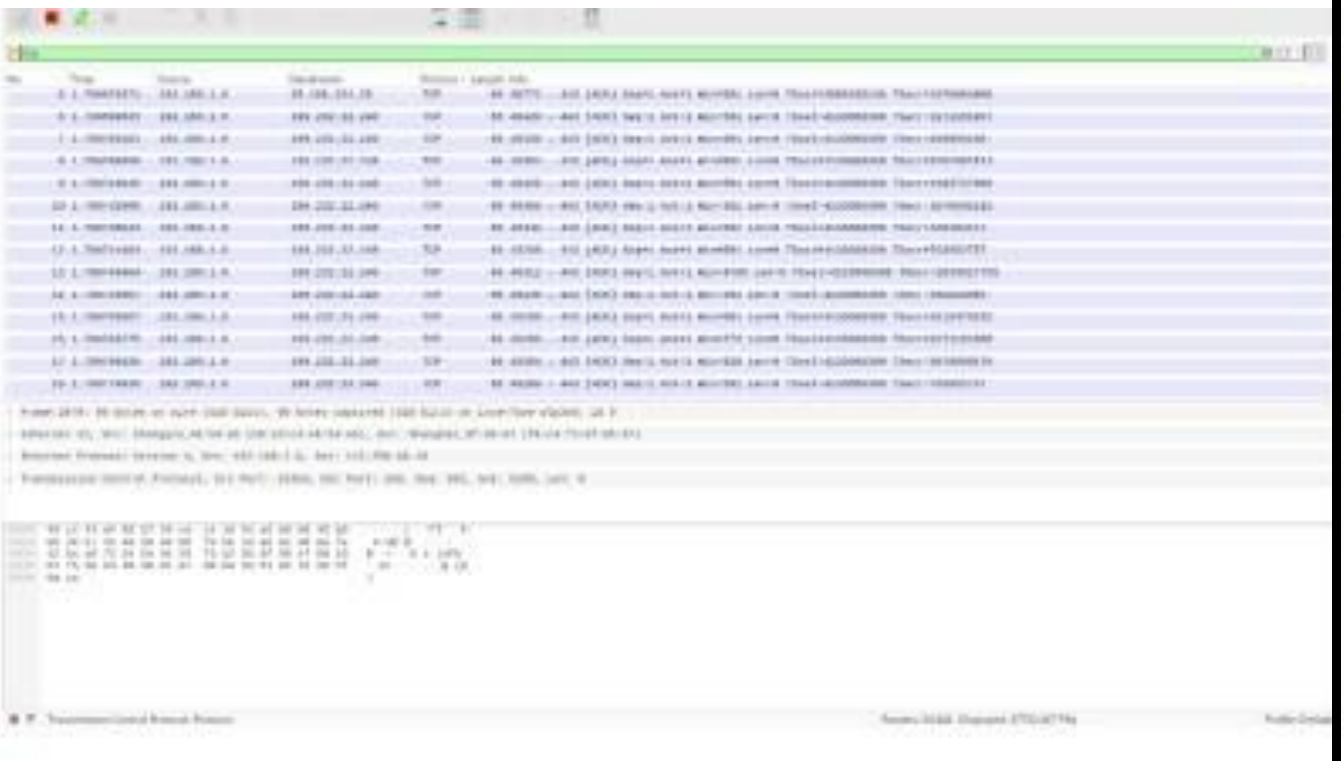
Aim: Packet Capture using Wireshark software filters.

Theory:

Packets to be captured are:
1. TCP
2. UDP
3. ARP

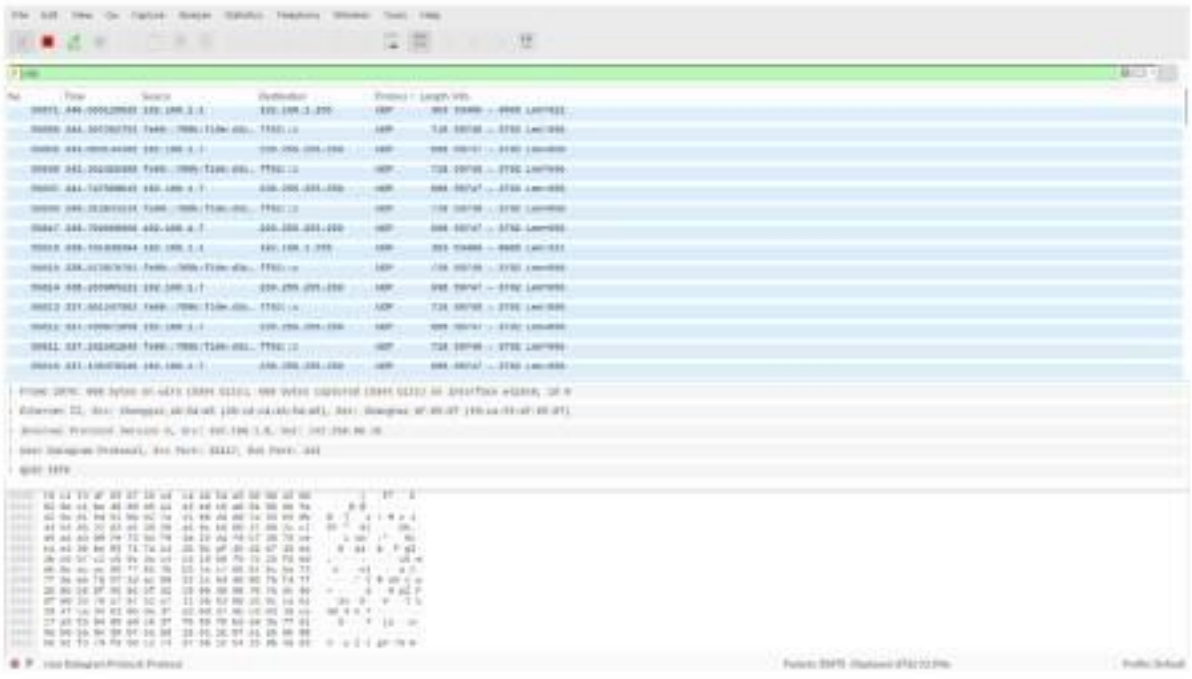
TCP

The Transmission Control Protocol (TCP) is a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks.



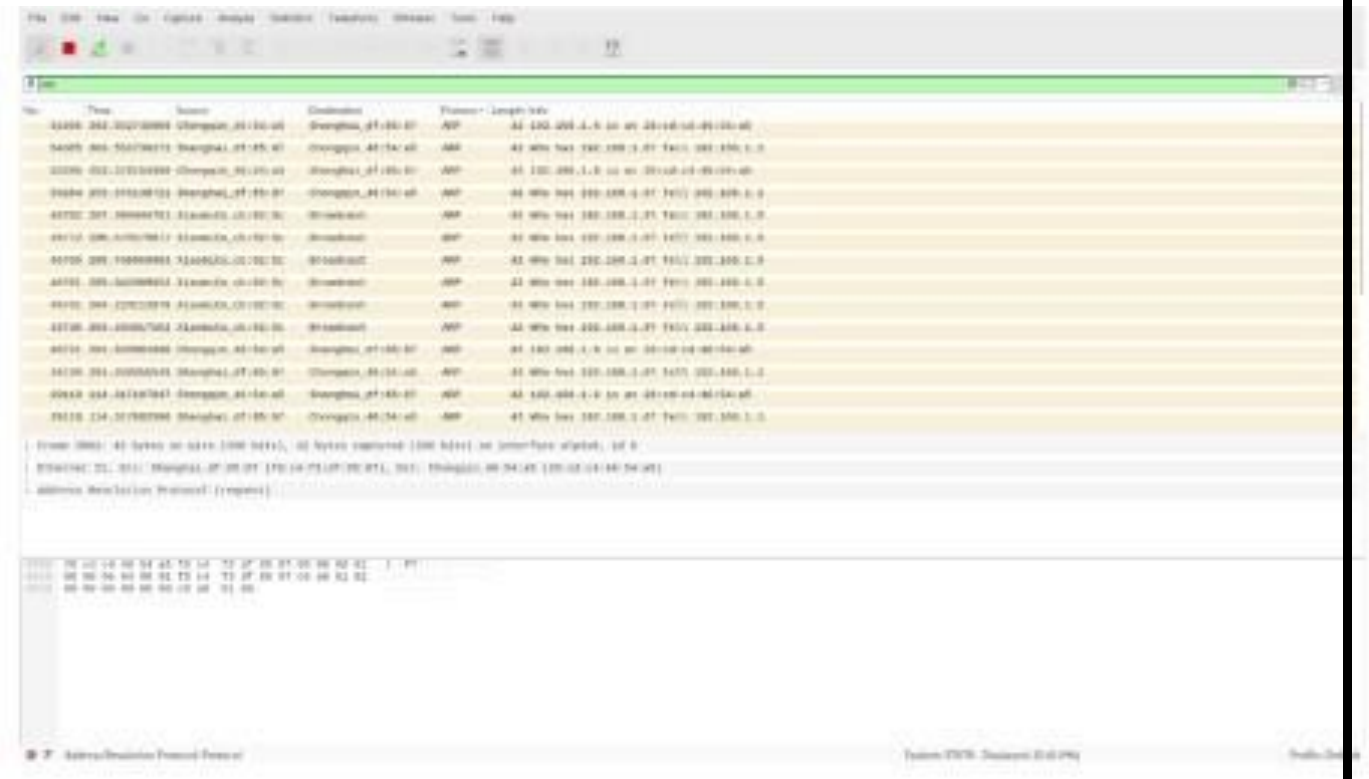
UDP

UDP divides messages into packets, called datagrams, which can then be forwarded by the devices in the network –switches, routers, security gateways– to the destination application/server.



ARP

The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.



Observations:

Answer the following questions after observing the Wireshark filter for TCP, UDP and ARP protocols.

The significance of different color for messages in Wireshark

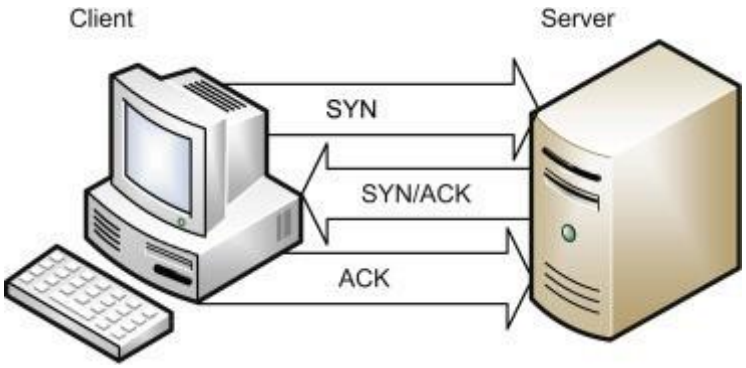
Color coding is used for us to differentiate between various types of traffics immediately. Purple is TCP, Blue is UDP, yellow is ARP and Black is for errors.

Observations in difference between UDP and TCP protocol using Wireshark.

In UDP, the packets are continuously sent irrespective of the fact if the user receives it or not. But in TCP the a confirmation is sent to the sender after receiving the packet from the sender, from the receiver. This makes TCP a bit slower than UDP but more reliable.

What is 3-way handshaking in TCP protocol?

The algorithm used by TCP to establish and terminate the connection is called a 3 way handshake. It consists of 3 parts: SYN, SYN + ACK & ACK.



Step 1 (SYN): In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN (Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with

Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement (ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with

Step 3 (ACK): In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer

Port addresses of TCP and UDP protocol

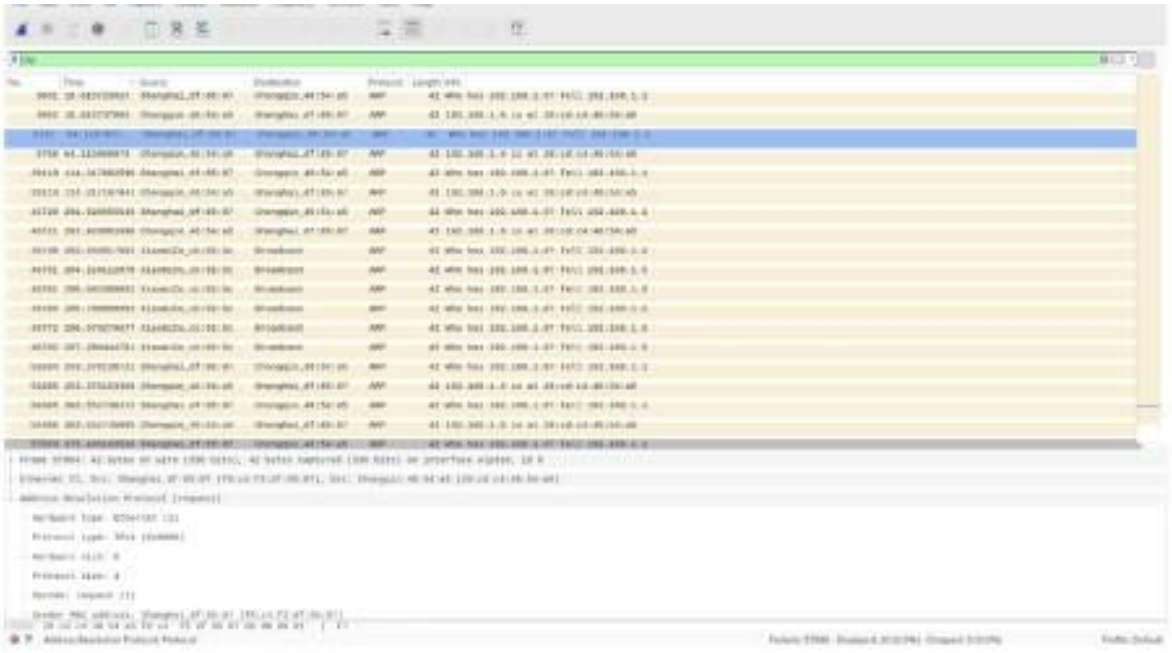
For UDP and TCP/IP respectively

```
Source Port: 53466
Destination Port: 9995
```

```
Source Port: 58482
Destination Port: 443
```

Define ARP protocol and observe Messages in ARP protocol using Wireshark.

ARP or address resolution protocol is a procedure that connects a changing IP address to a fixed physical machine address, also known as media acess control (MAC) address on a LAN.



ARP is essectially a bunch of requests and response between the network router and the connected device where the router asks which machine has a logical IP address assigned by the router. The device which has been assigned the IP address responds with it’s mac address.

Conclusion:
In this lab session, we were taught the difference between TCP/IP and UDP, about ARP protocols and how to identify them using Wireshark. The color codes and respective parameters were understood.