Batch: A1	Roll No.: 16010120015
Experiment / assignment / tutorial No.___10_____	
Grade: AA / AB / BB / BC / CC / CD /DD	
Signature of the Staff In-charge with date	

Experiment No.:10

TITLE: Study of Packet Analyzer tool: Wireshark

AIM: To study and analyse various Protocols using Packet Analyzer tool: Wireshark

---

Expected Outcome of Experiment:

CO: Study about the function of the wireshark analyser tool such as

Deep inspection of hundreds of protocols, with more being added all the time

- Live capture and offline analysis
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- The most powerful display filters in the industry

Books/ Journals/ Websites referred:

1. A. S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition
2. B. A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition

---

Pre Lab/ Prior Concepts:

IPv4 Addressing, Subnetting, Link State Protocol, Router configuration Commands

---

New Concepts to be learned: Packet Analyzer tool: Wireshark.

THEORY:

Wireshark

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

- It is used to track the packets so that each one is filtered to meet our specific needs.
- It is commonly called as a sniffer, network protocol analyzer, and network analyzer.
- It is also used by network security engineers to examine security problems.

It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Uses of Wireshark:

- It is used by network security engineers to examine security problems.
- It allows the users to watch all the traffic being passed over the network.
- It is used by network engineers to troubleshoot network issues.
- It also helps to troubleshoot latency issues and malicious activities on your network.
- It can also analyze dropped packets.

Features of Wireshark

- It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.

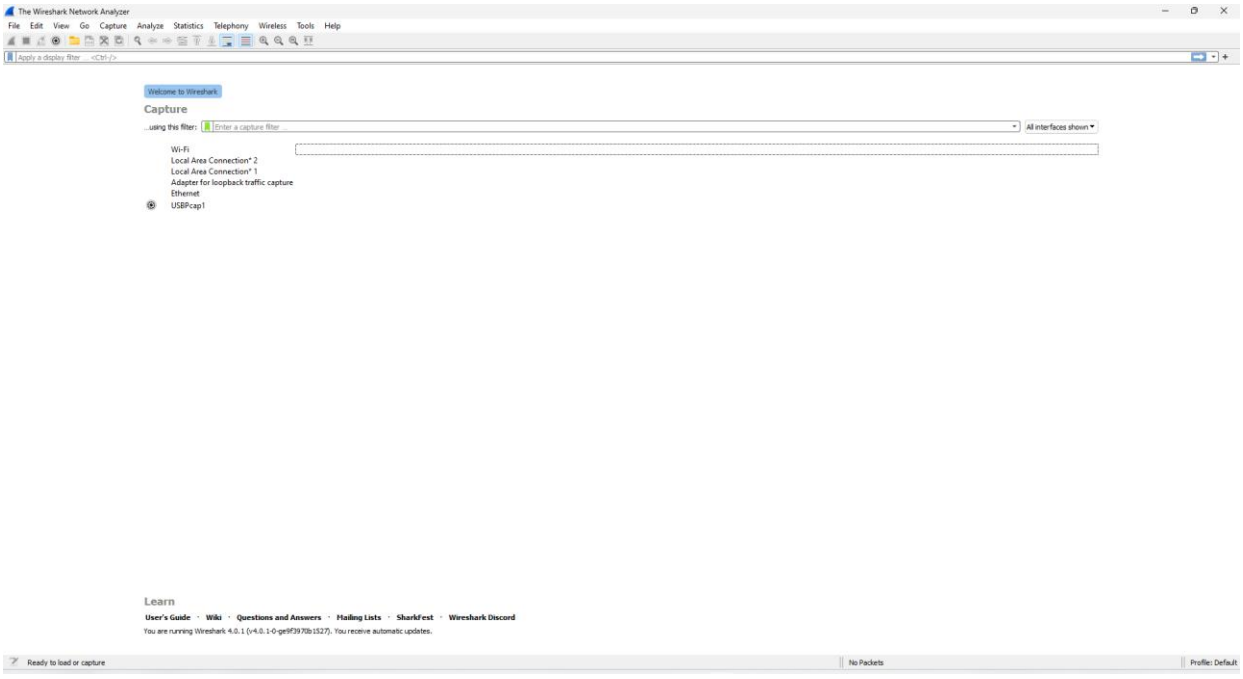
- It has sort and filter options which makes ease to the user to view the data.
- It is also useful in VoIP analysis.

Wireshark does three things:

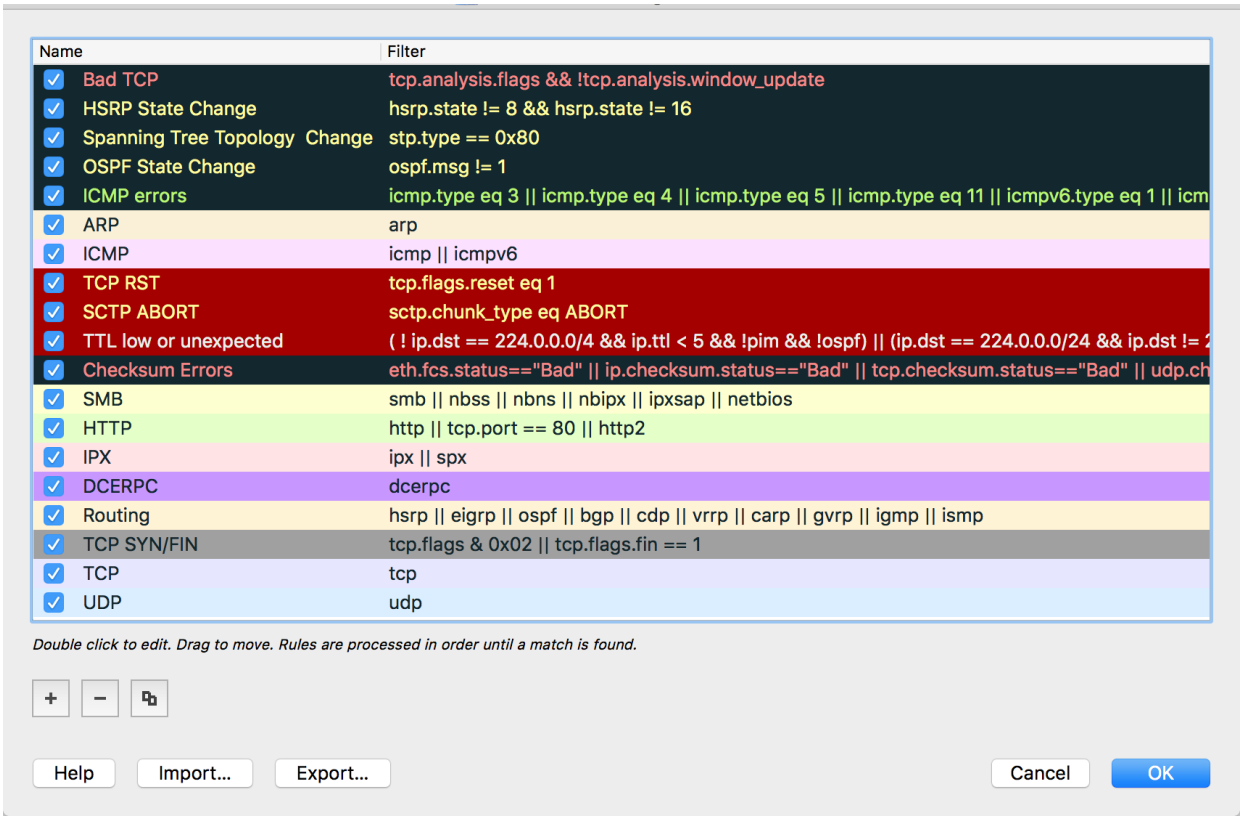
1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

IMPLEMENTATION:

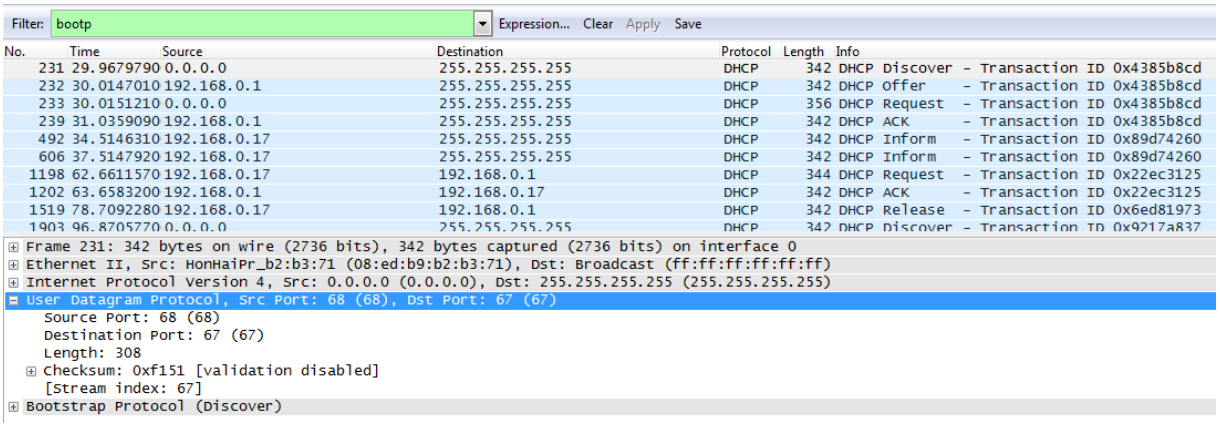
Home Page of Wireshark



Colouring Rules in Wireshark :



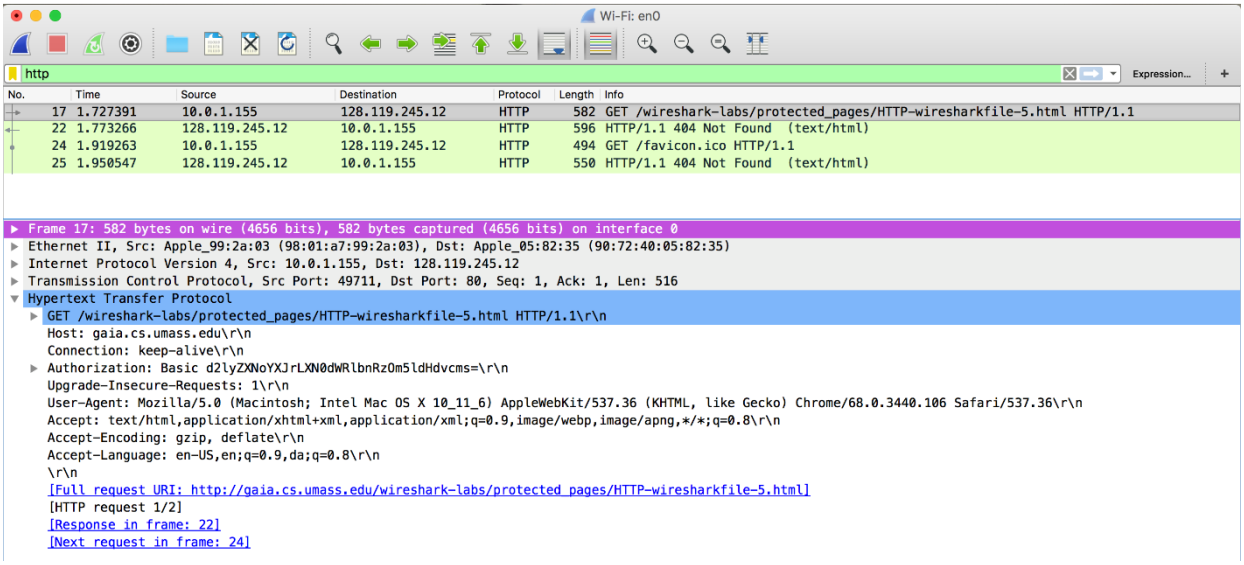
1) DHCP packets (Dynamic Host Configuration Protocol)
   - Responsible for dynamically assigning IP addresses and any other necessary parameters to each device on a network



As highlighted in the above snapshot, User Datagram Protocol is used as the transport layer protocol with src port (client port) as 68 and Dst port (Server port) as 67.

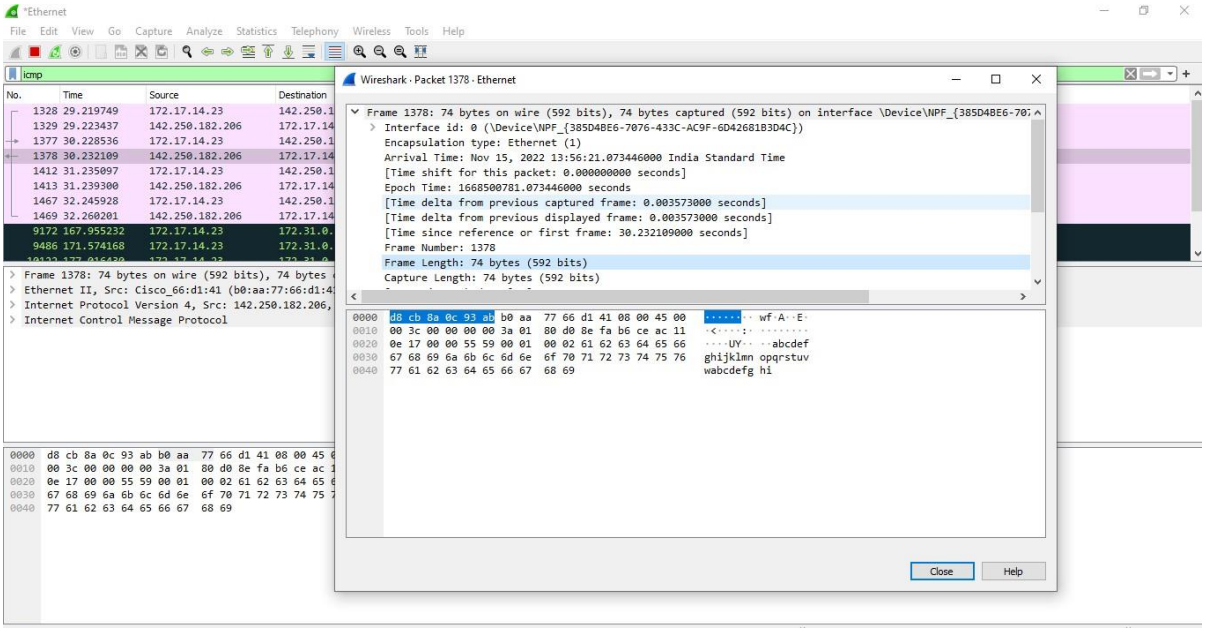
Http Packets (Hypertext Transfer Protocol)

- This is what actually transfers the website to the user in the form of instructions like a text document



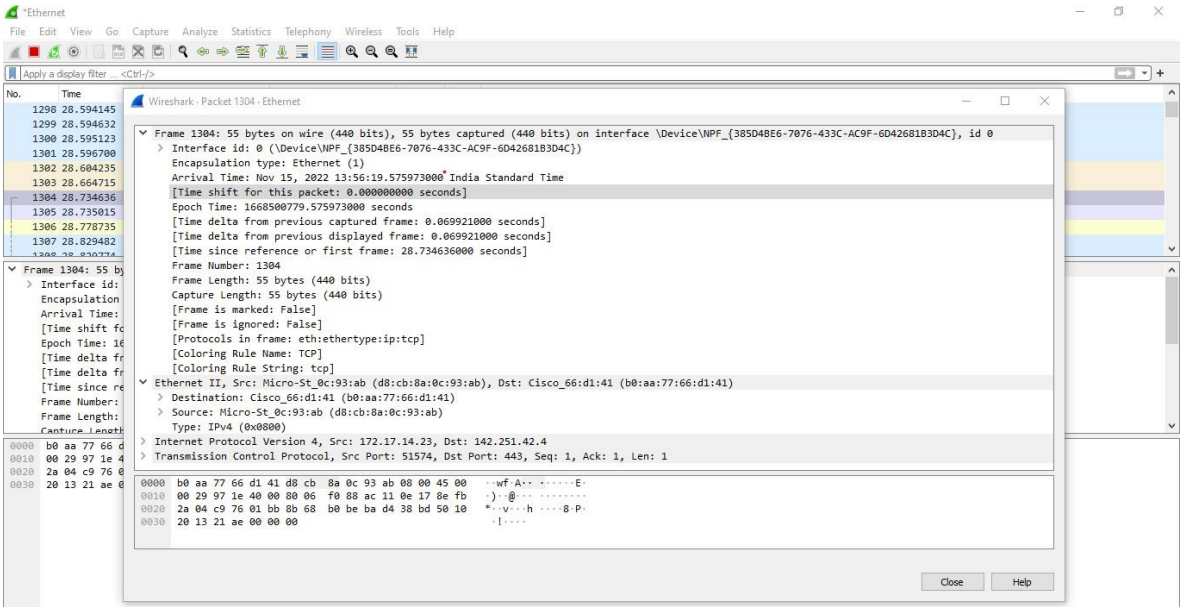
ICMP Packets (Internet Control Message Protocol)

ICMP messages also contain the entire IP header from the original message, so the end system knows which packet failed



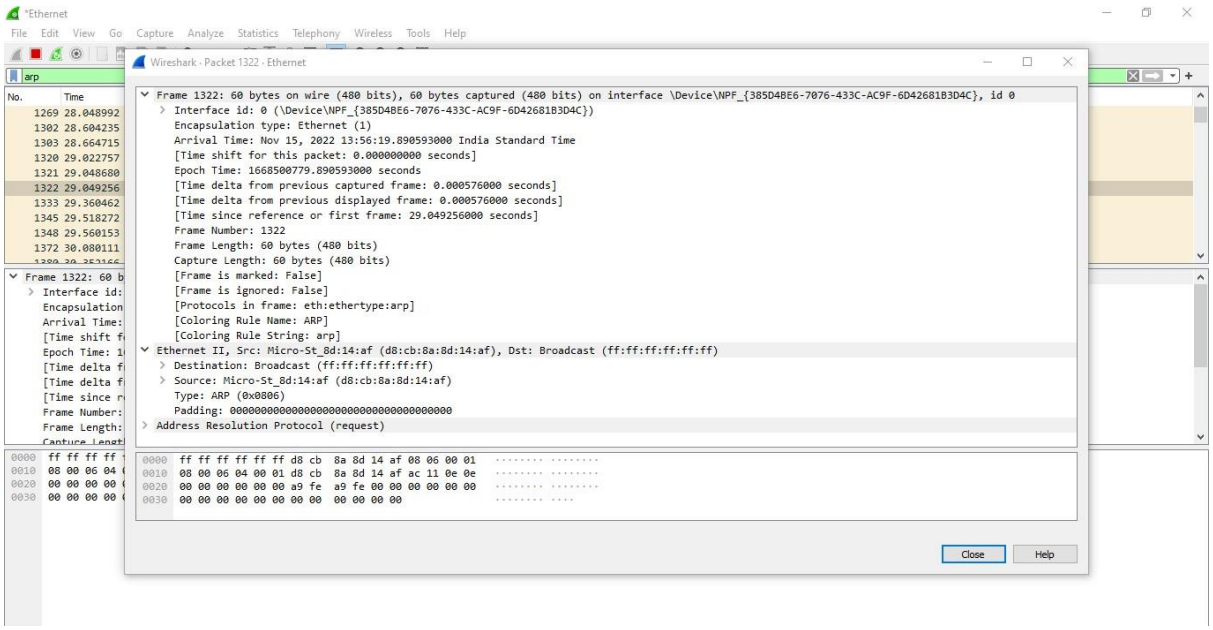
FTP Packets (File transfer protocol)

- The way to download, upload, and transfer files from one location to another on the Internet and between computer systems.

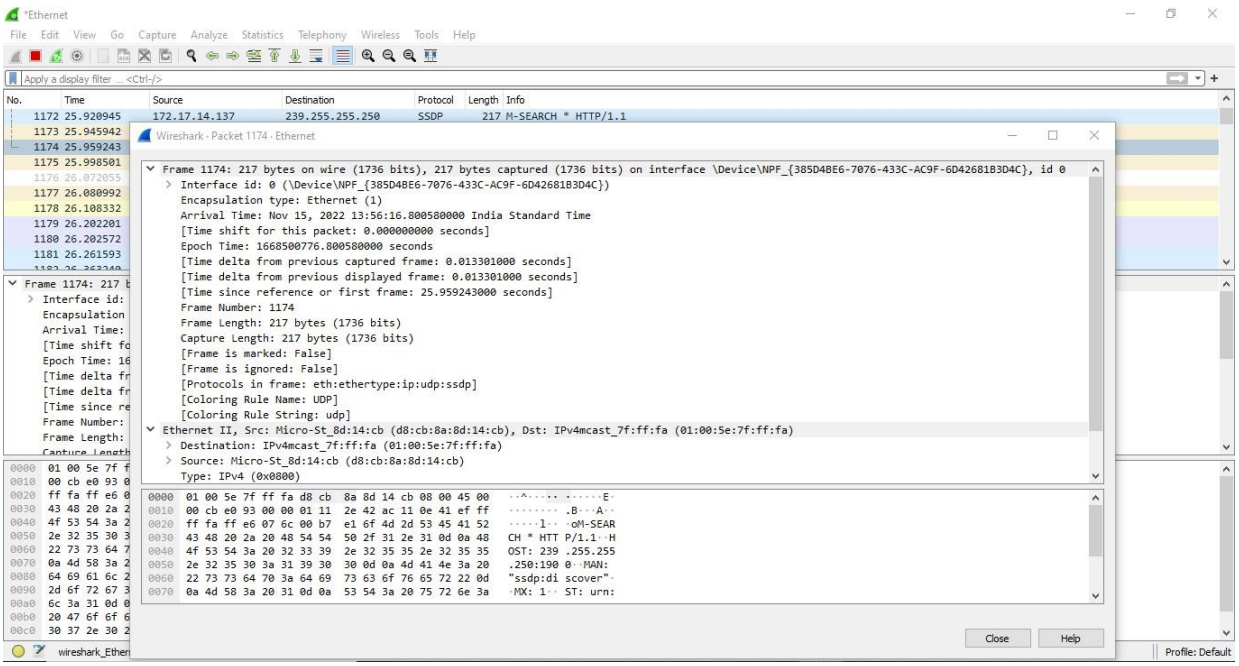


ARP Packets (Address Resolution Protocol)

- Responsible for discovering MAC (media access control) address

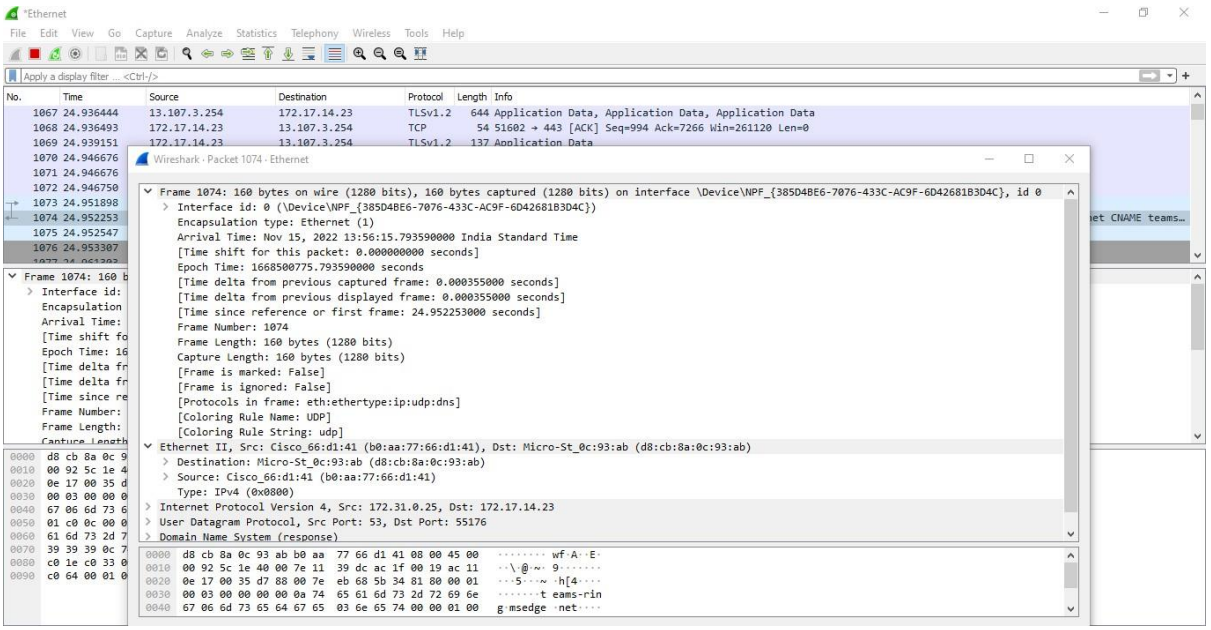


SSDP Packets



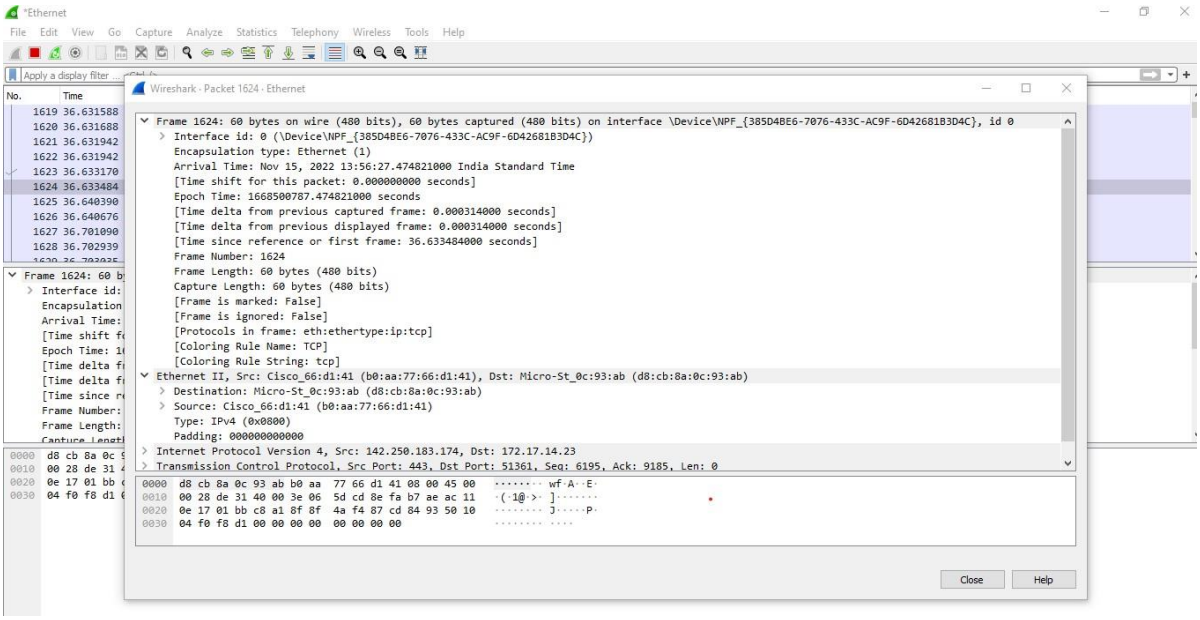
1) TCP packets (Transmission Control Protocol)

Delivers bytes between applications running on hosts



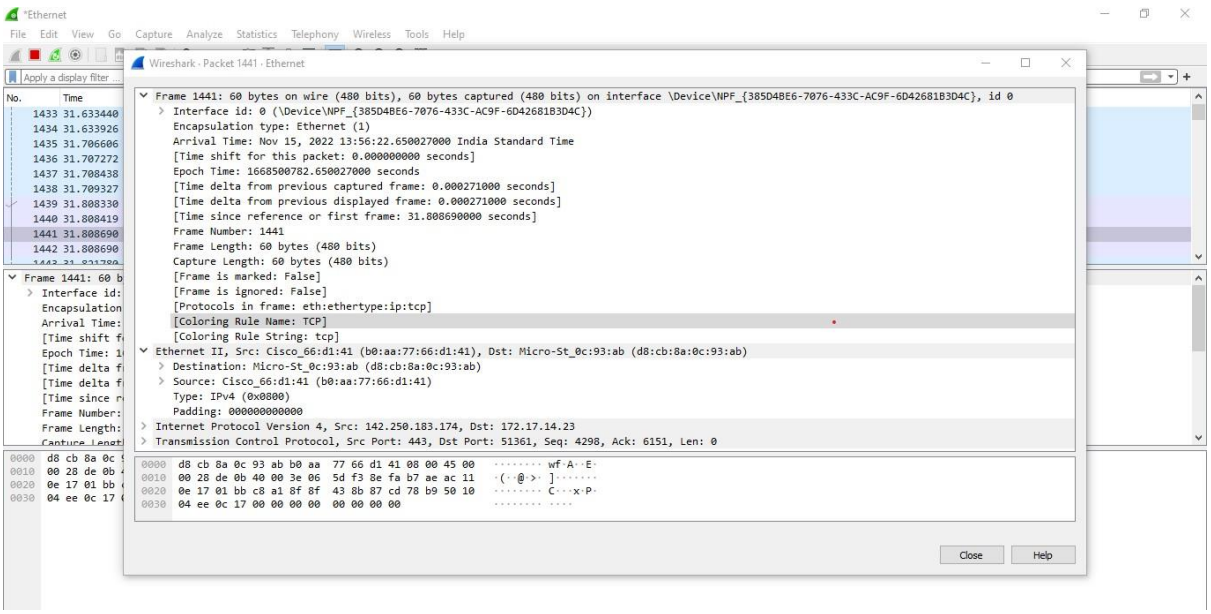
DNS Packets (Domain Name System)

- Translates memorized domain names into numerical IP addresses



Telnet Packet

- Terminal emulation programs that allow you to log into a remote host.



CONCLUSION:

Hence we have implemented and successfully studied about Wireshark

Wireshark basically Which captures packets from a network connection, such as from your computer to your home office or the internet.. Wireshark is the most often-used packet sniffer

Post Lab Questions:

Date:___15/11/2022____ **Signature of faculty in-charge**