PRACTICAL - 1

AIM: Study Network Analysis Tool Wireshark. Filter TCP, UDP, ICMP Packet Format and extract OSI model.

➔ Introduction to Wireshark network analysis tool

Wireshark is open source tool.Wireshark is the world's widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions.

- 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.
- It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

➔ Capturing Data packets on Wireshark:

When you open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor. You also have a capture filter field, so you only capture the network traffic you want to see.

Fig 1.1 wireshark

Capturing from wifi :

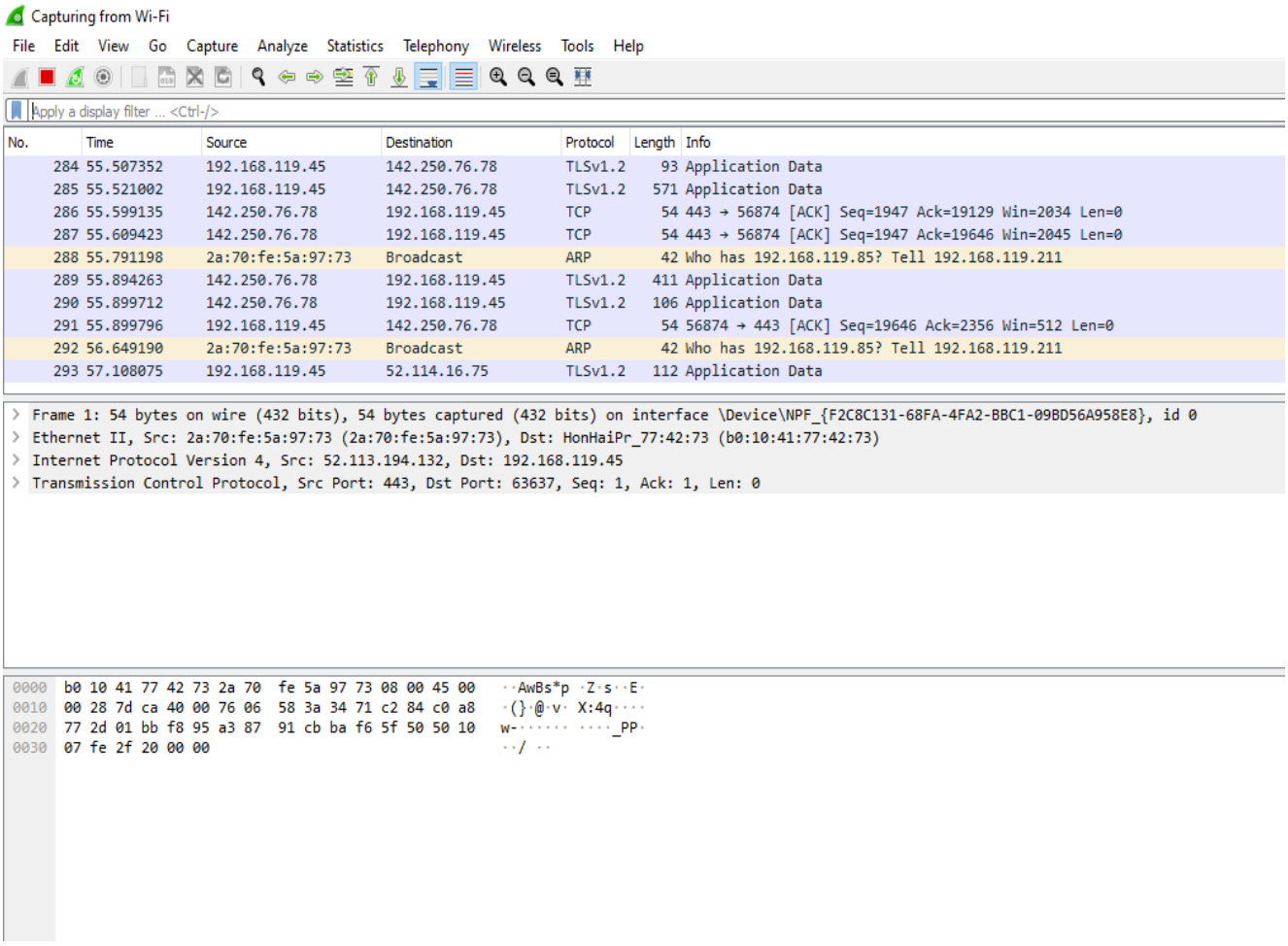

Fig 1.2 capturing from wifi

➔ Filtering Packets by Tcp:

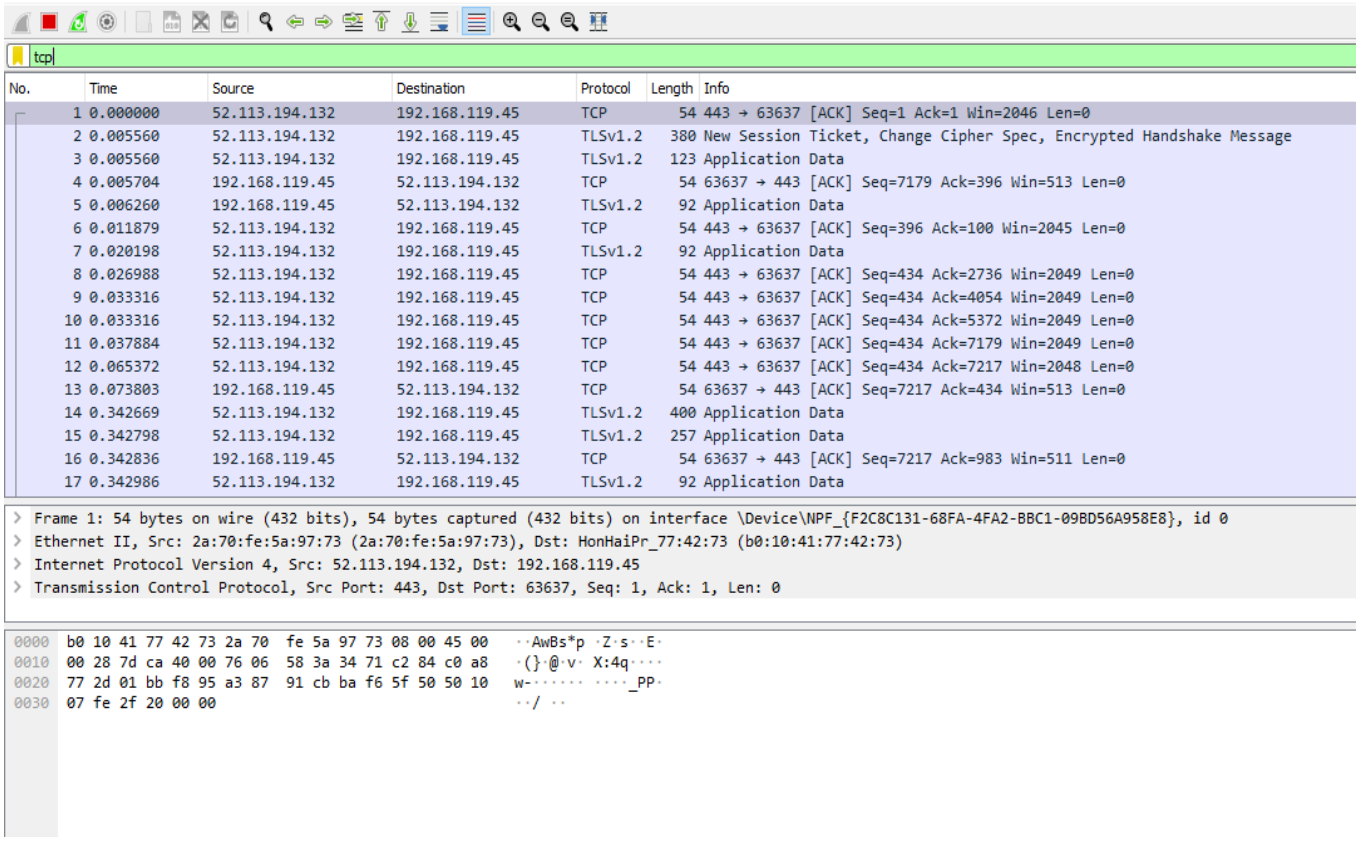

Fig 1.3 Tcp packet capturing

➔ Filtering Packets by Udp:

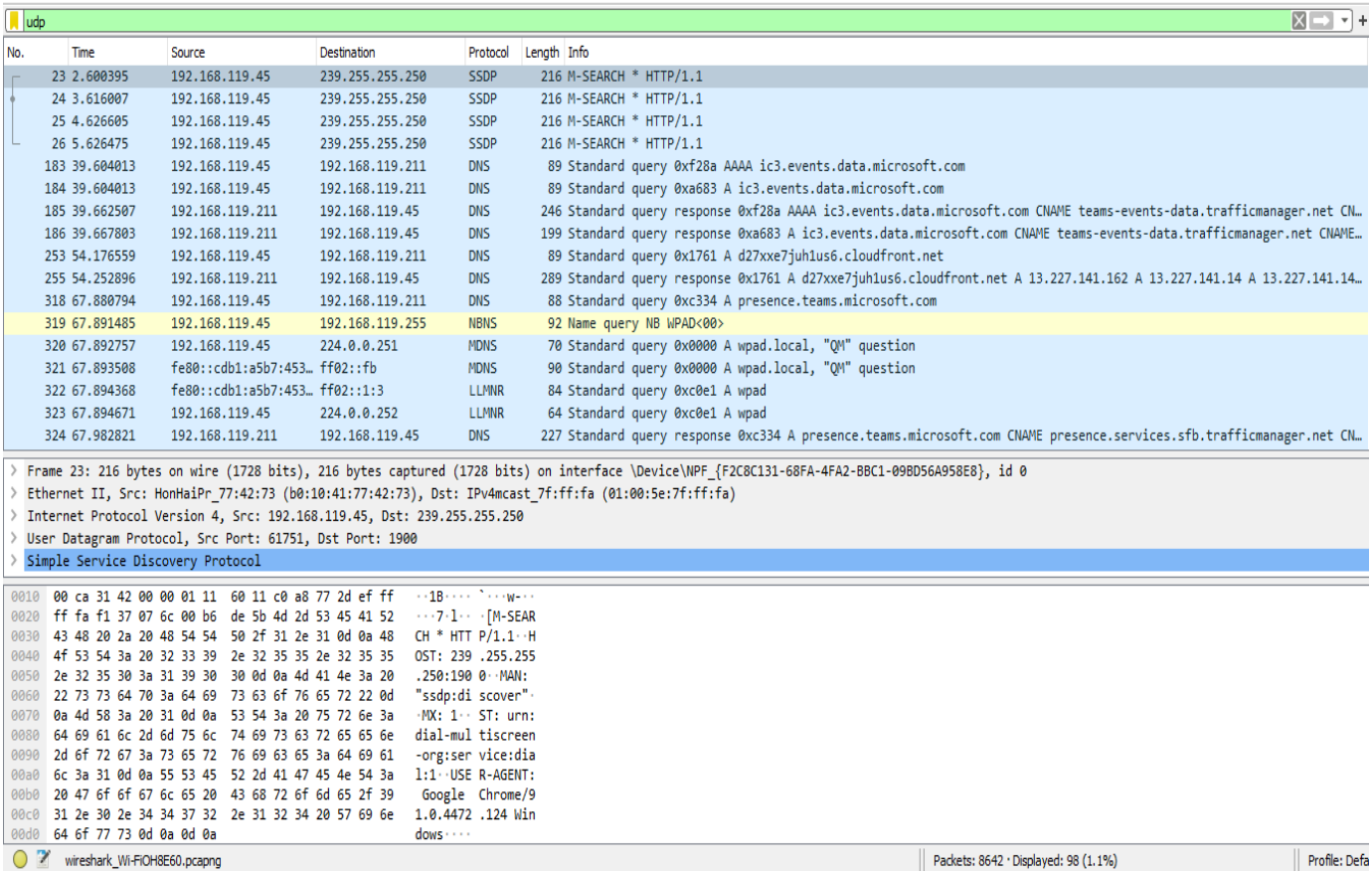

Fig 1.4 Udp packet capturing

➔ Filtering Packets by Icmp:

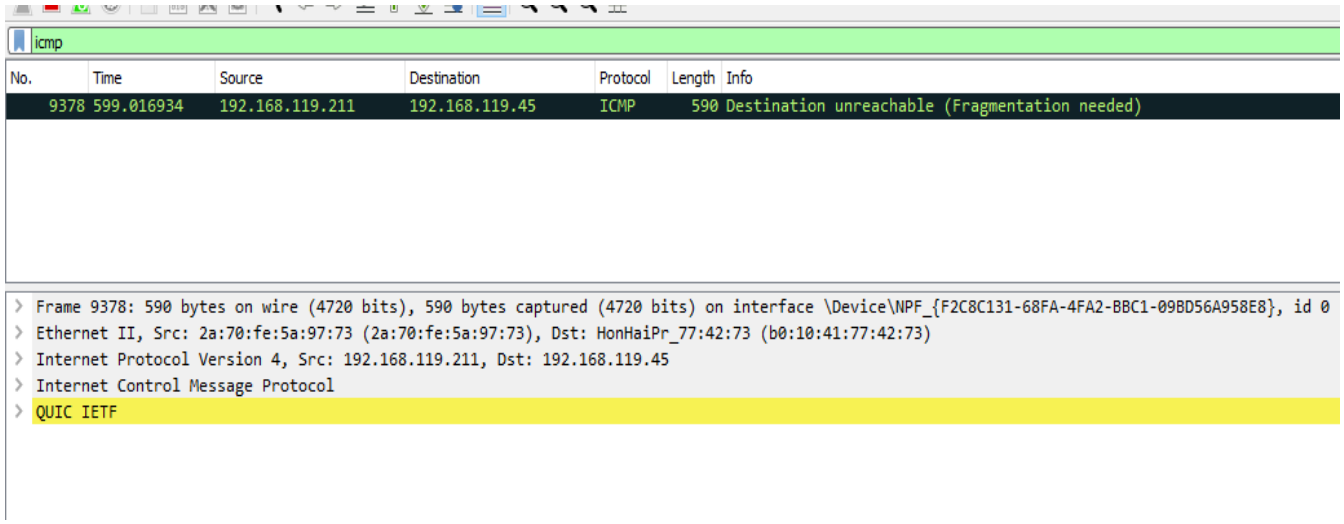

Fig 1.5 Udp packet capturing

➔ Filtering Packets by Arp:

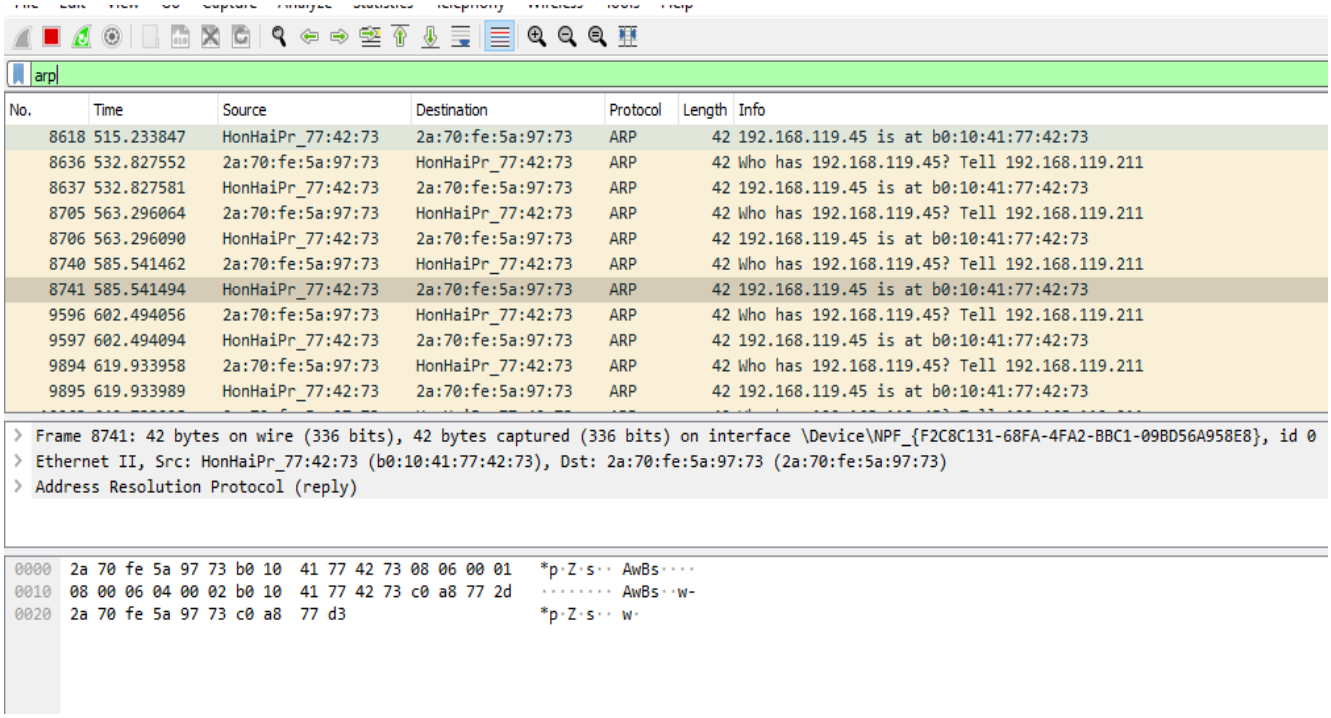

Fig 1.6 Arp packet capturing

➔ Osi model format:

As Wireshark decodes packets at Data Link layer so we will not get physical layer information always. In some cases, capturing adapter provides some physical layer information and can be displayed through Wireshark.
So here are the sequence layers seen in Wireshark:

- Data link layer
- Network layer
- Transport layer
- Application layer

Wireshark is just showing in reverse order. If physical layer information is given to Wireshark then that time we should see physical layer information on top of Data link. See below examples.

HTTP [It has 4 layers]:

You can follow below link to understand HTTP through Wireshark

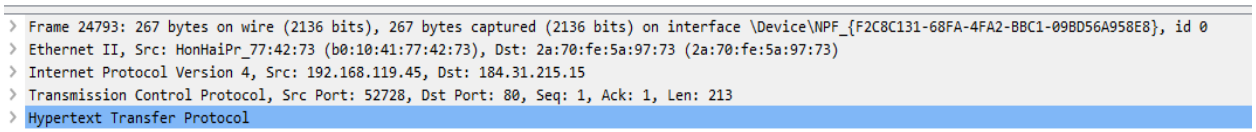

Fig 1.7 http osi format

TCP [It has 4 layers]:

Here is the screenshot of a TCP packet where we can see 4 layers.

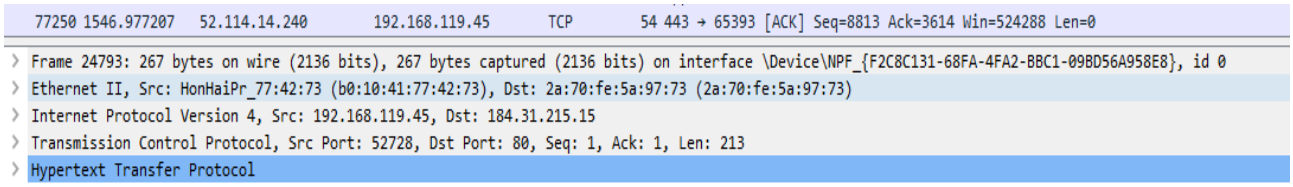

Fig 1.7 Tcp osi format

ICMP [It has 2 layers]:

Here is the screenshot of a TCP packet where we can see 2 layers.

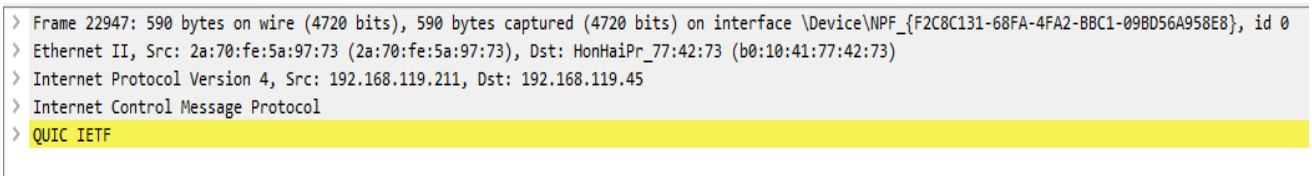

Fig 1.7 Icmp osi format