Task 5:

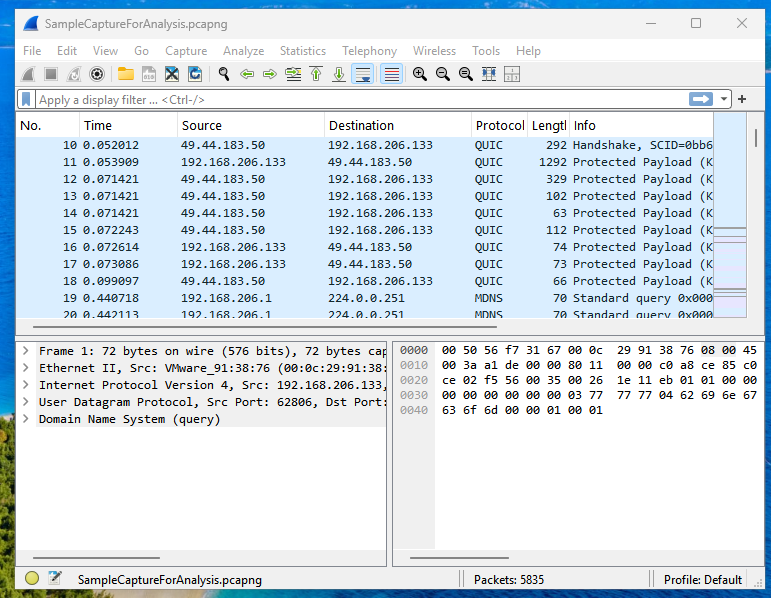
Capture and analyze Network Traffic using wireshark.

Steps:

1. I have used windows VM to perform the task.
2. I have downloaded Wireshark form the internet and installed it.
3. I have opened the wireshark and used my ethernet to capture the traffic.
4. I have saved the captured traffic in a file( uploaded in the repository)

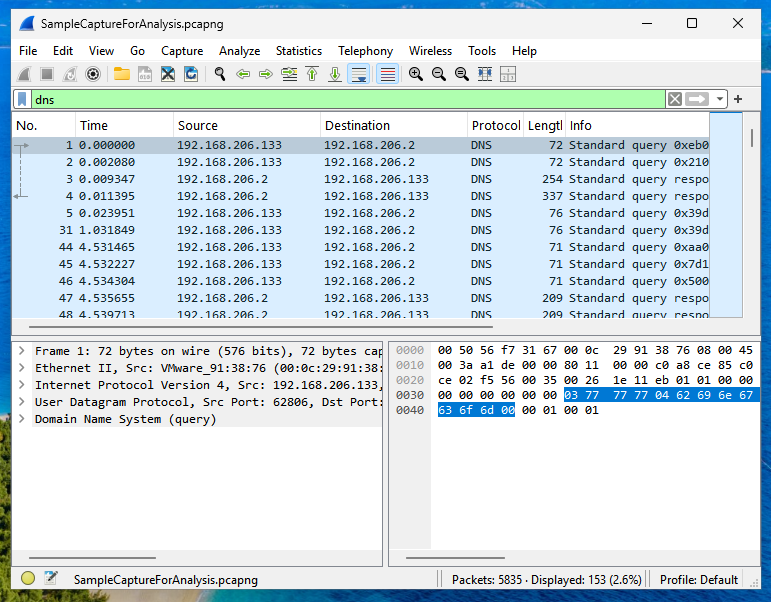
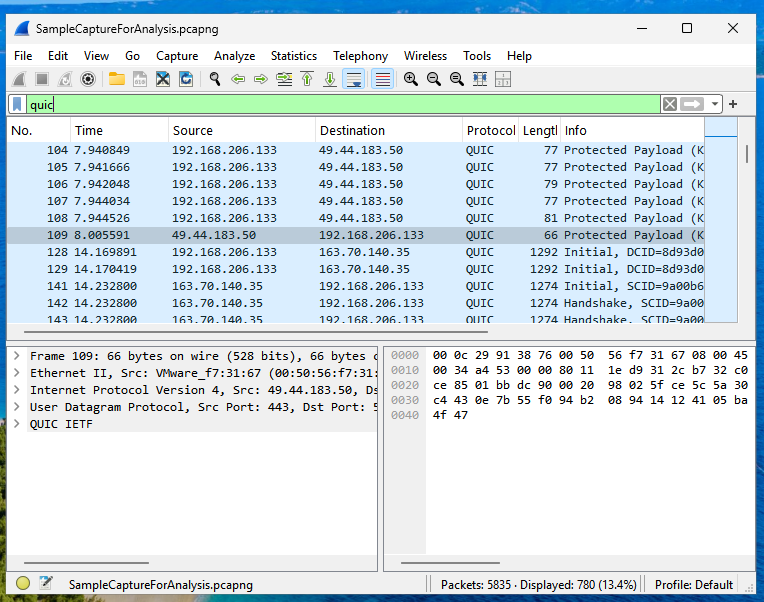
Sample outcome traffic screenshot below:

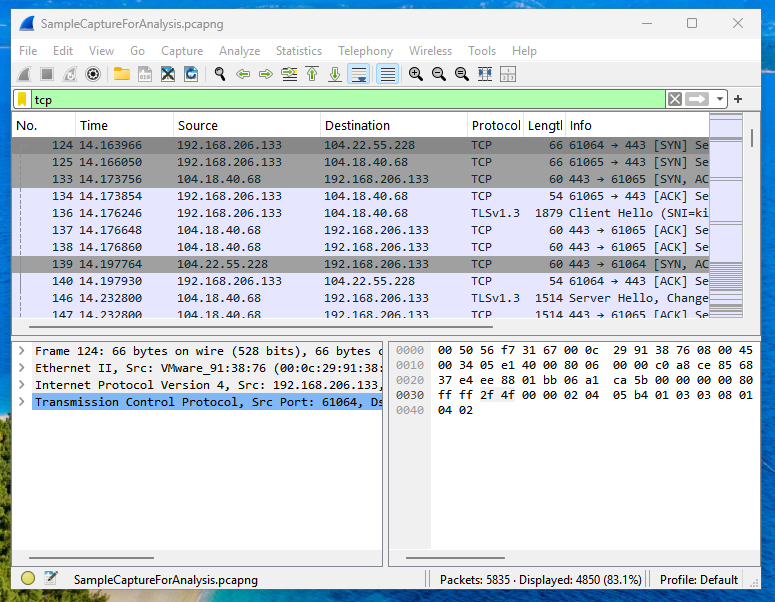
My pcap file has total of 5835 packets generated.



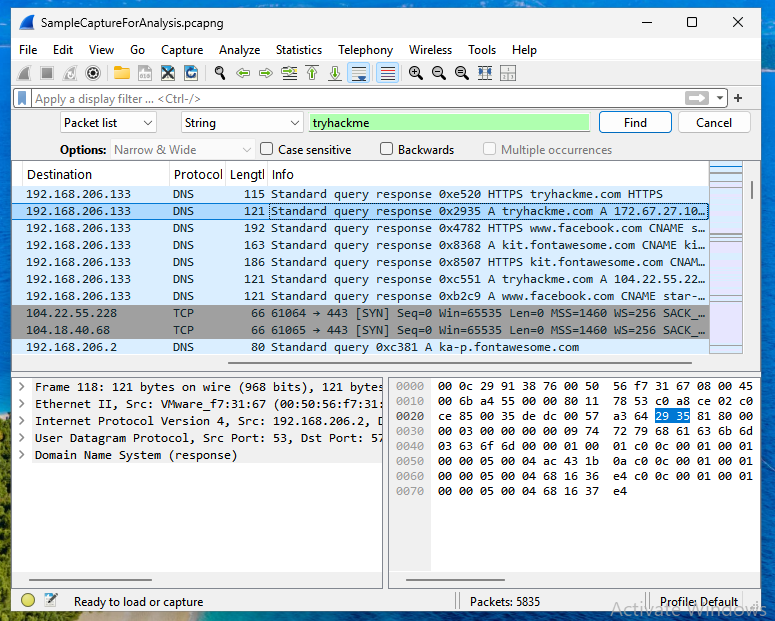
1. I have pinged <https://tryhackme.com> to generate the traffic.
2. After a minute, I have stopped the capture of the traffic and saved the pcap file as SampleCaptureForAnalysis.pcapng
3. Later, I have opened the saved pcap file for analysis.
4. First, I have identified 3 protocols generated in the wireshark traffic and filtered them using display filter (dns,tcp,quic protocols) DNS - 153 packets, TCP -4850 packets, QUIC – 780 packets generated

Screenshots below





1. As I have pinged tryhackme.com to generate traffic, I have used the Edit-> Find Packet option to filter and find the packet which pinged tryhackme, Screenshot below



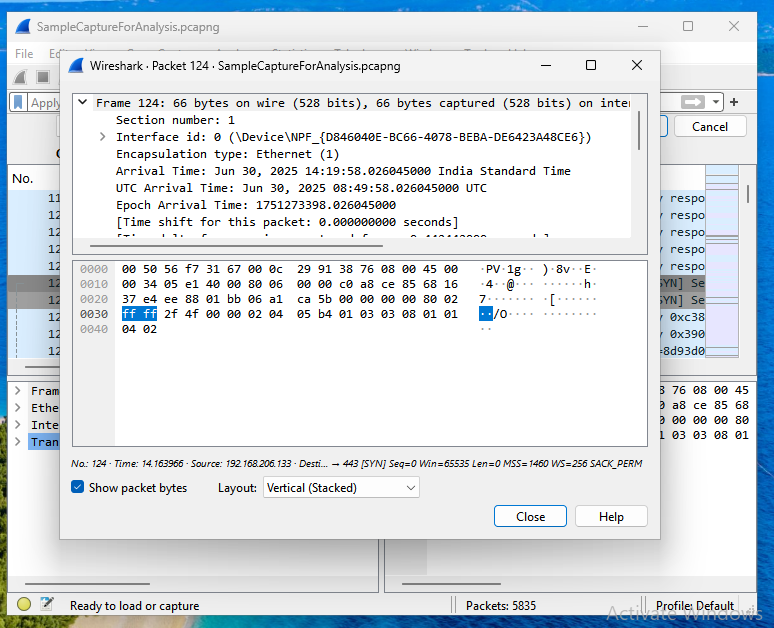
Summary:

Wireshark tool helps us to capture the network traffic. Live network traffic can be captured and wireshark allows us to save the traffic in a file format which can be used for analysis later.

It has many different options that lets us to filter protocols, strings we want to find, and also helps us to analyze each packet.

Each packet has details of the packet which represents OSI layer , where did the packet start , source mac, dest mac, ip address of source and destination, protocols used and the tcp headers, payload information, ttl etc.. everything can be seen when we click on a specific packet and expand each details shown in the packet.

Sample packet details screenshot:



When we double click on a packet , packet details will be opened in a new window, which can be helpful for further analysis. In the above screenshot, it shows Frame 124, i.e packet 124 details are shown , and the 1st layer of OsI model details like devicename, internet type are shown in the details.

Likewise we will get the details of all the layers.

This packet analysis can be helpful to identify if any downloads are made, payloads executed etc which are strong evidences to tell if an attack has happened.