Wireshark

Submitted by Aleena Anna Plessey

Reg no: 21BCE5767

Course Program: B.Tech

Course code: BCSE308L

Course Title: Computer Networks

Batch:2021-25

Submitted to: Dr. Swaminathan A

Submitted on 09/07/2023

Problem Statement:

12.1. Capture the packets using Wireshark and depict the TCP connection establishment and termination process.

12.2. Filter the TCP packets that contain the request to terminate.

12.3. Depict the flowgraph and the I/O graph of TCP, UDP, ICMP, ARP, and TLS.

Aim and Objective:

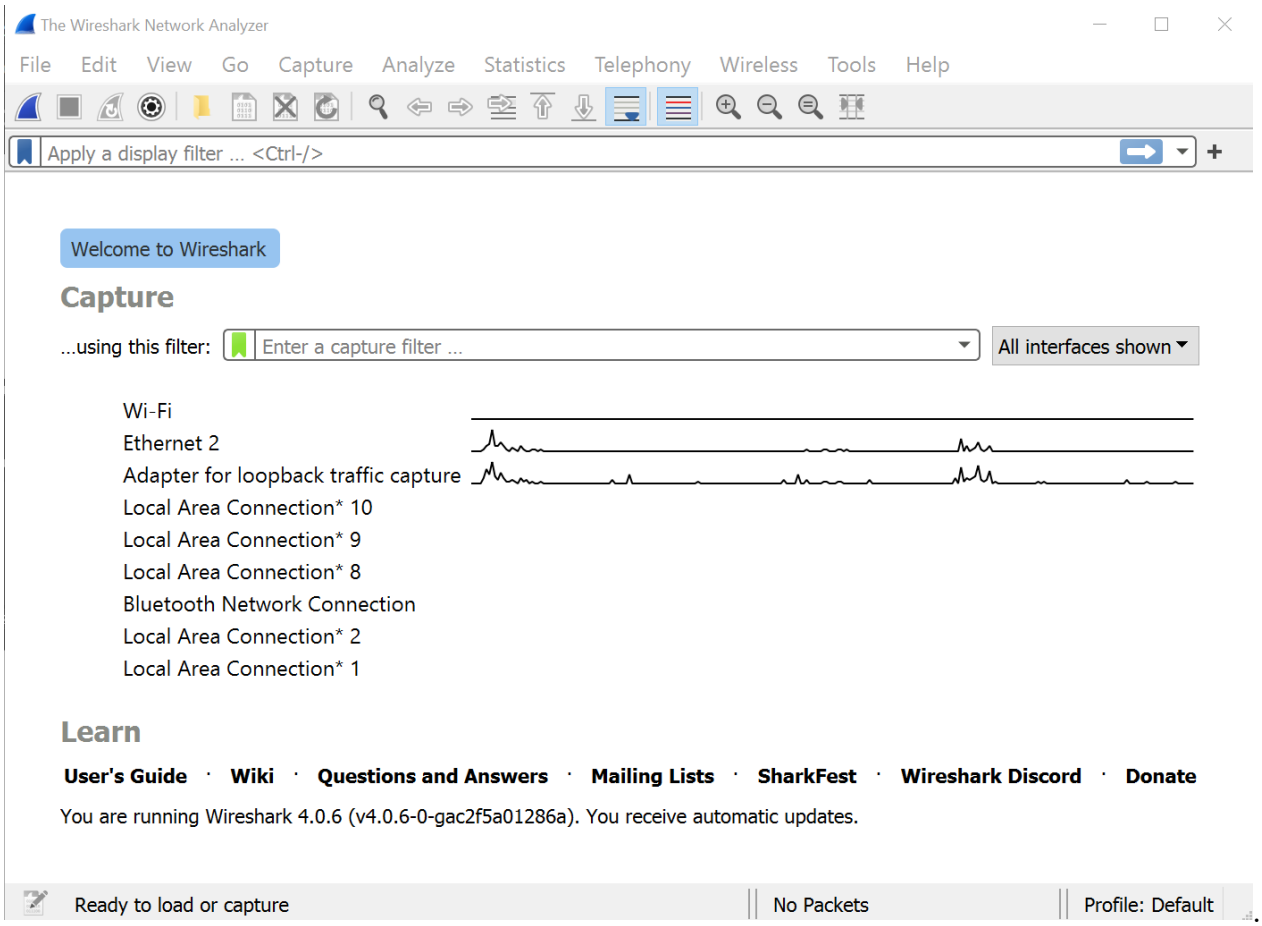
To understand the main use case of Wireshark and to understand its features and learn to capture packets to view the different properties of TCP packets.

Solutions:

12.1. Capture the packets using Wireshark and depict the TCP connection establishment and termination process

Procedure:

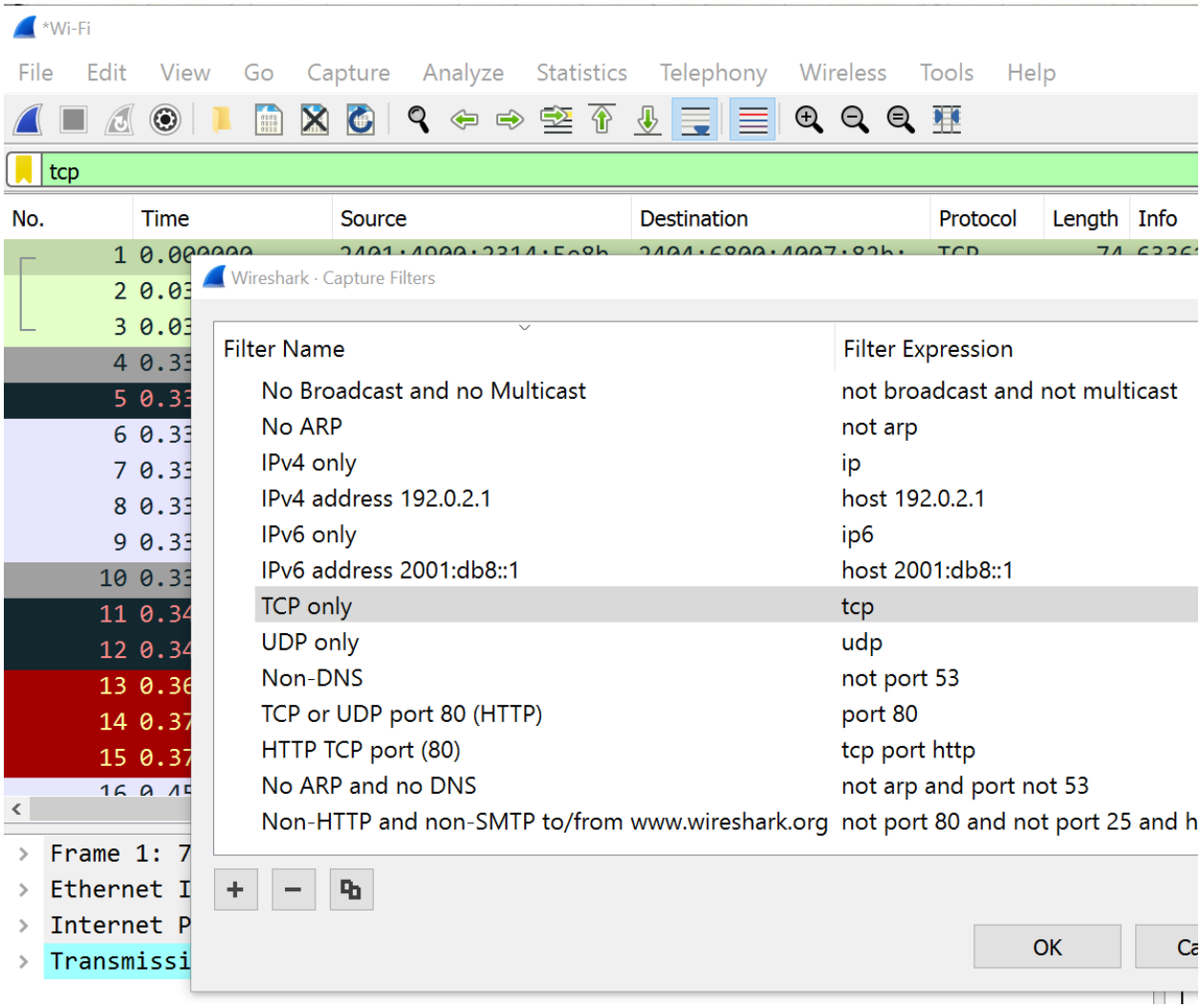
1)Open Wireshark whilst connected to a network and use the appropriate interface(Ethernet/WiFi)



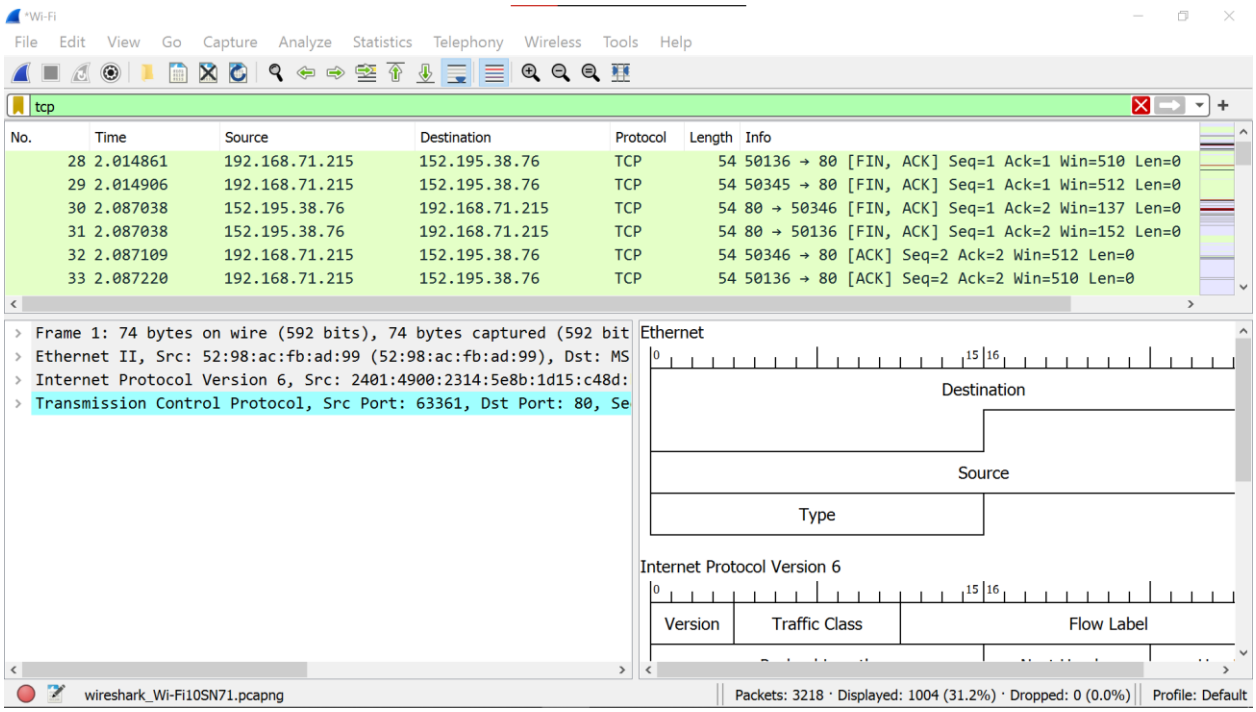
2)Press start and capture the packets for a few 5 to 10 minutes.

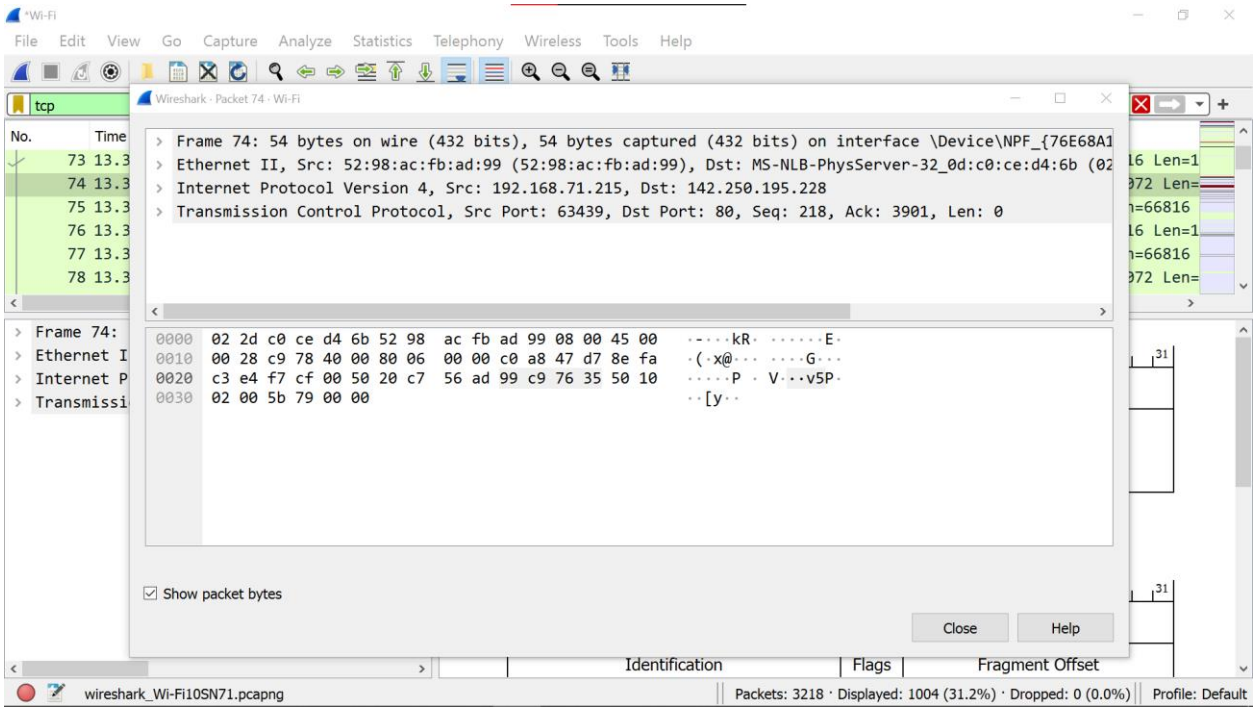
3)Press stop once enough packets have been gathered.

4)In the top right corner search for tcp only and filter out the packets.



Output:





12.2 Filter the TCP packets that contain the request to terminate.

Procedure:

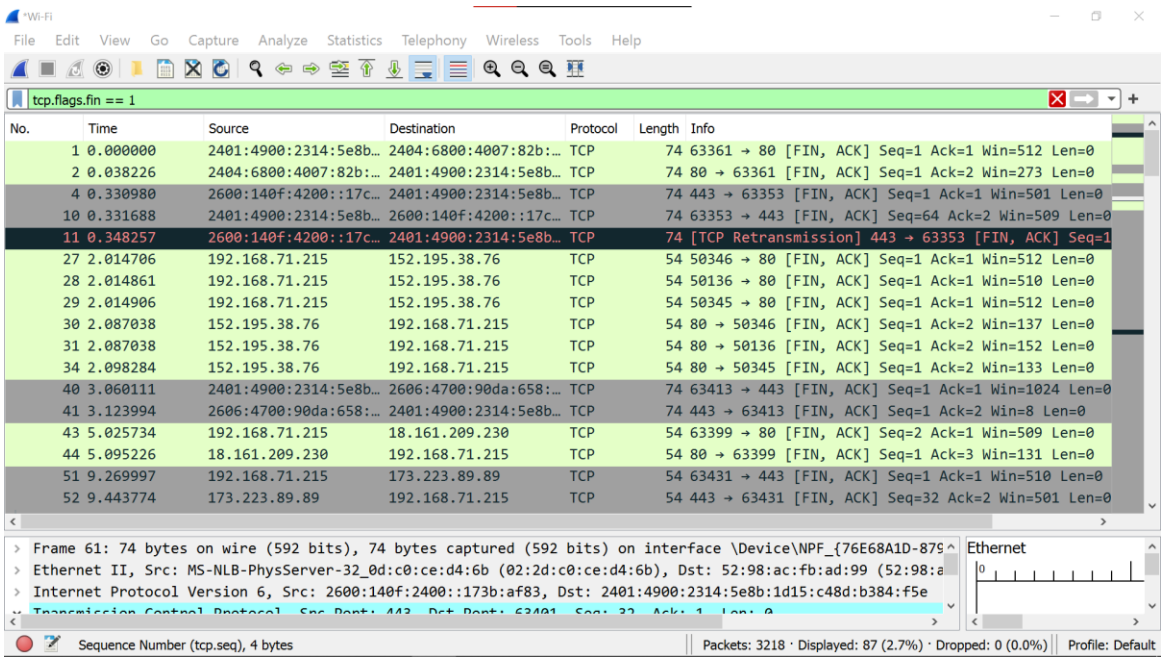
1)Open Wireshark whilst connected to a network and use the appropriate interface(Ethernet/WiFi)

2)Press start and capture the packets for a few 5 to 10 minutes.

3)Press stop once enough packets have been gathered.

4)In the top right corner set a filter “tcp.flags.fin==1” which will aid in particularily searching for tcp packets that have sent a request to terminate.These packets are usually grayed out.

Output:



We can see that all the packets displayed on the screen have FIN in their information status indicating that they have been sent to request to terminate.

12.3. Depict the flowgraph and the I/O graph of TCP, UDP, ICMP, ARP, and TLS.

Procedure:

1)Open Wireshark whilst connected to a network and use the appropriate interface (Ethernet/WiFi)

2)Press start and capture the packets for a few 5 to 10 minutes.

3)Press stop once enough packets have been gathered.

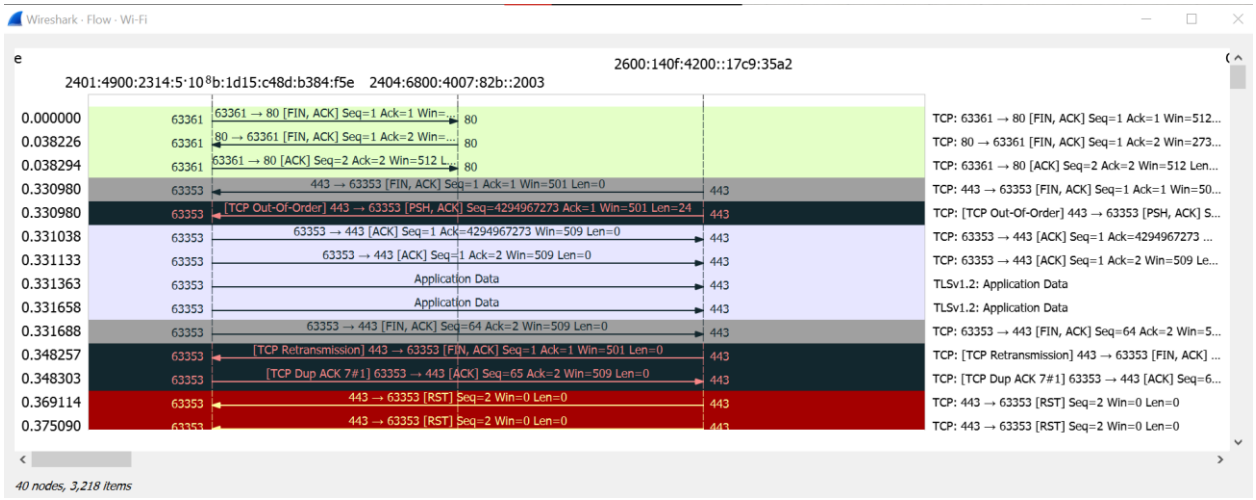
4)Go to statistics in the menu bar and select flow graph.

5)From there choose what packets to filter by to see the flow graph in each protocol

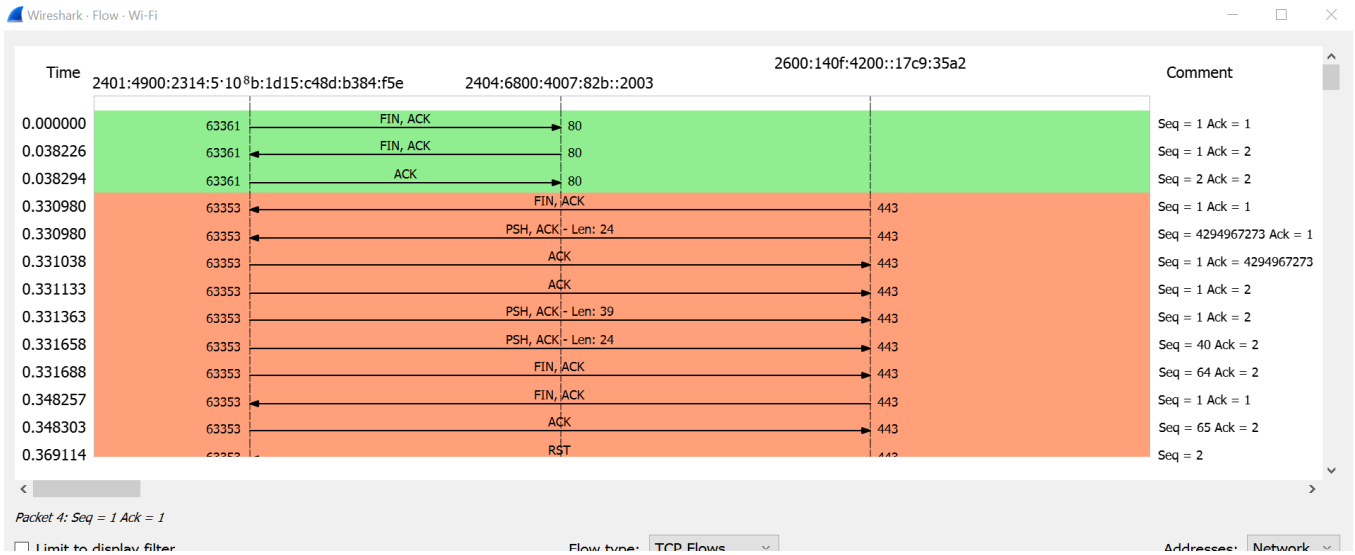
6)Similarly got to statistics->IO graph to see the IO graphs of the packets you require.

Output:

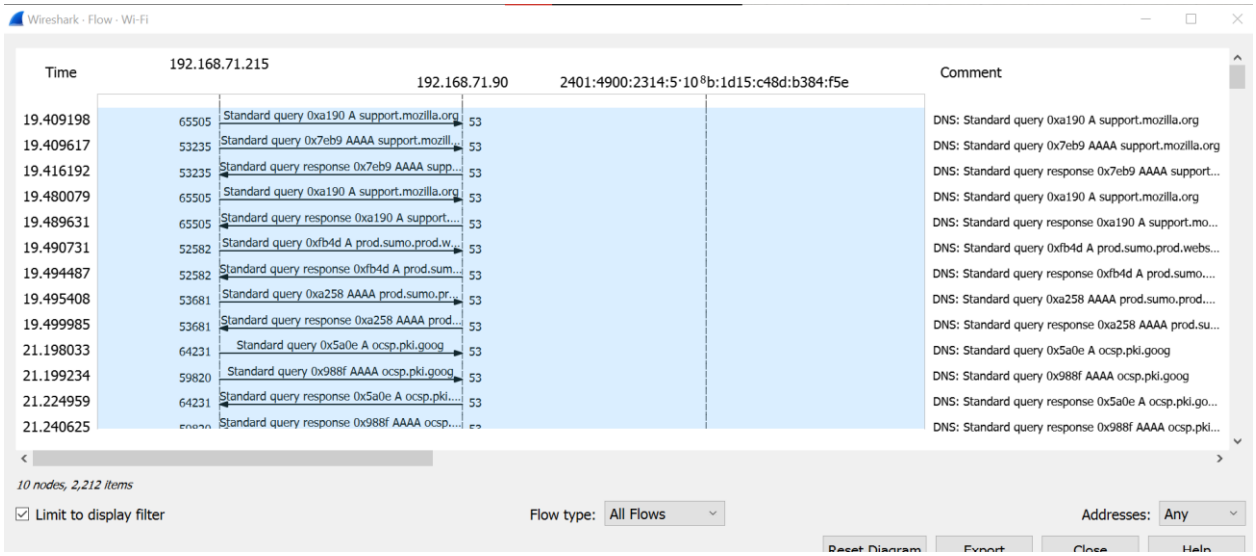
Overall



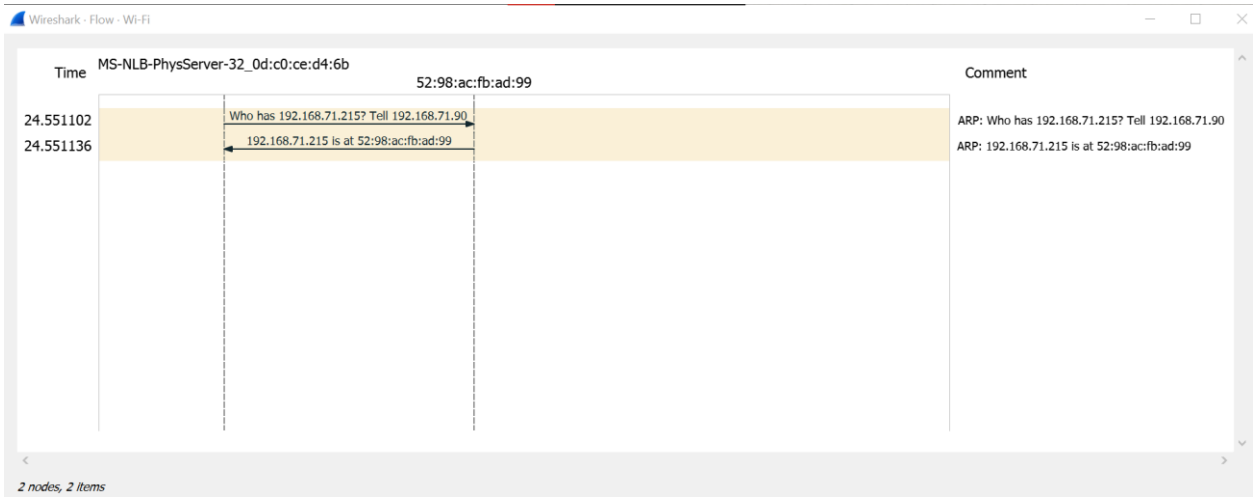
TCP



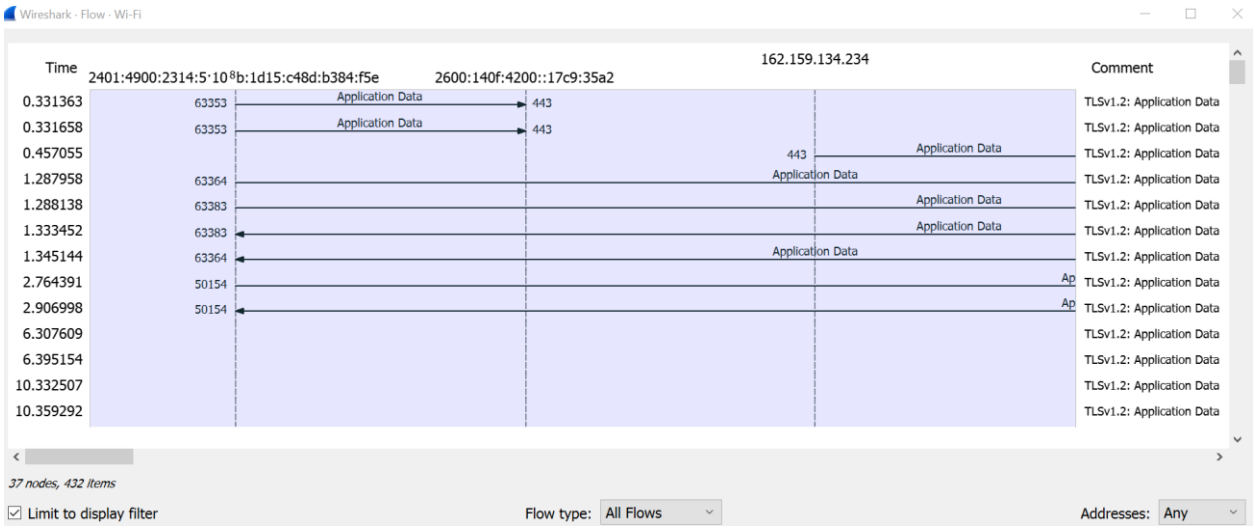
UDP



ARP

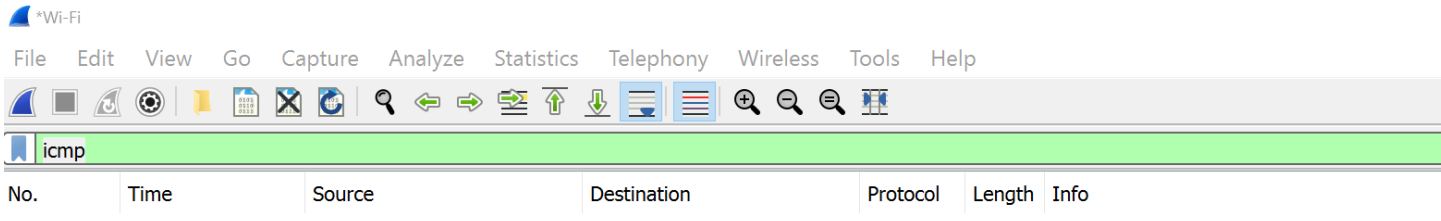


TLS

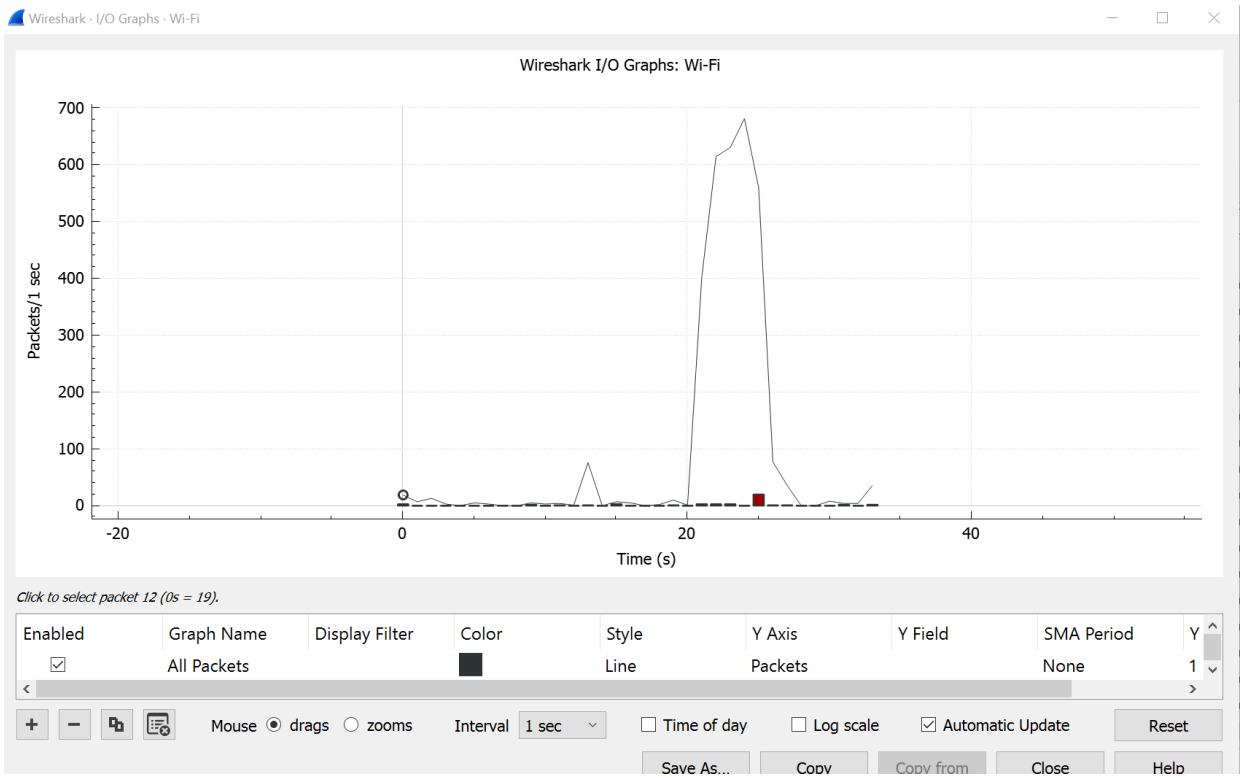


ICMP

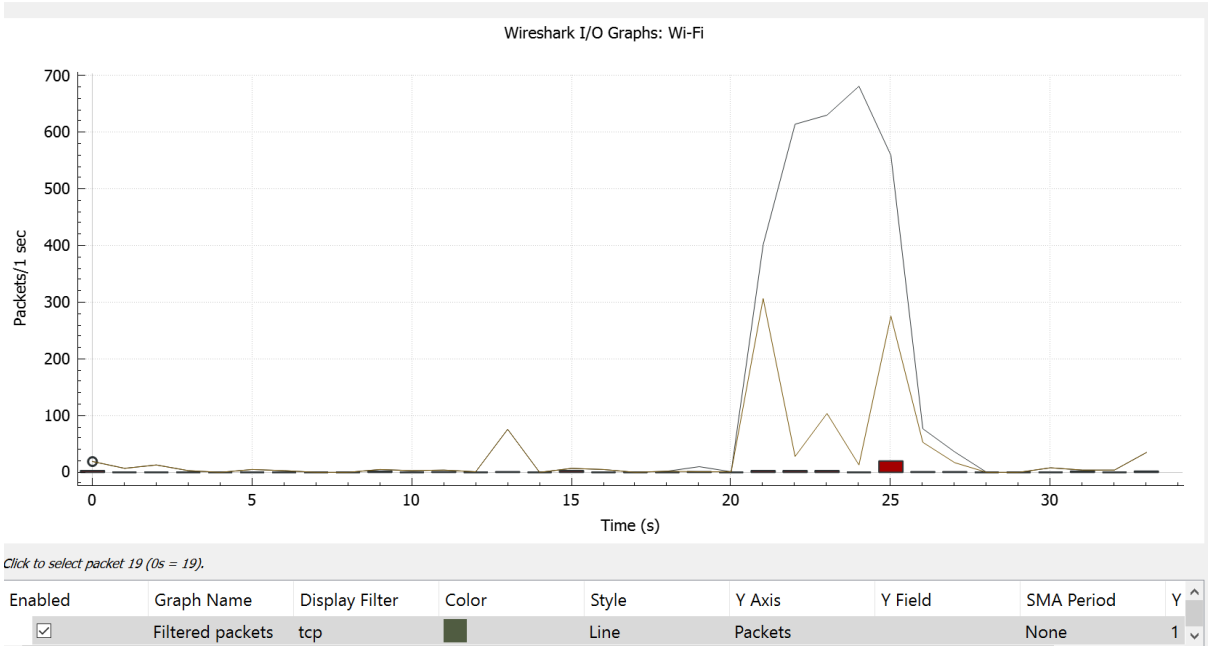
No packets compliying to ICMP were available in the packets that were collected as shown below.



IO Graph



TCP packets



Result:

Through these experiments I have successfully gained practical knowledge on how to effectively use Wireshark for capturing PDUs and filtering them according to the various demands as well as viewing and retrieving flow and IO graphs for different commonly used protocols.