**WIRESHARK**

**Task 5** : Capture and Analyze Network Traffic Using Wireshark.

Objective: Capture live network packets and identify basic protocols and traffic types.

Tools: Wireshark (free).

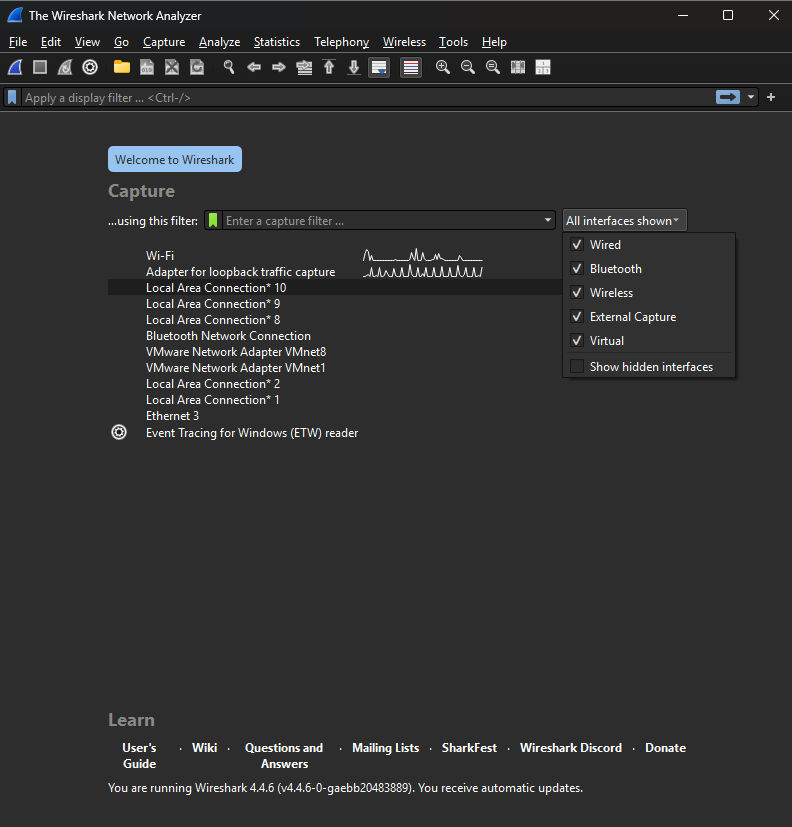
Deliverables: A packet capture (.pcap) file and a short report of protocols identified

**Process:**

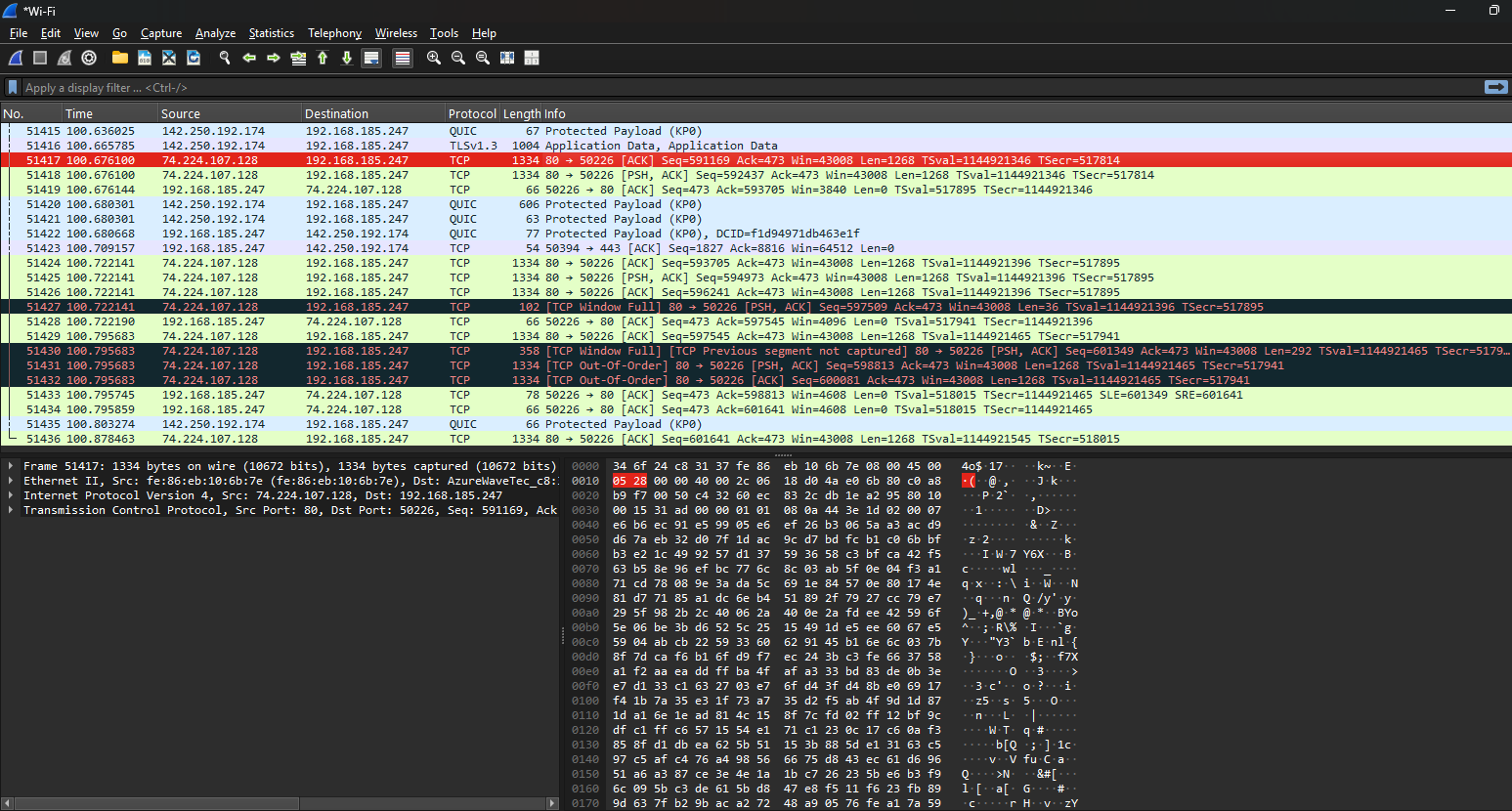
1. Install Wireshark

* I am using online platforms install wireshark tool.

1. Start capturing on active network interface



**This is the interface of wireshark**



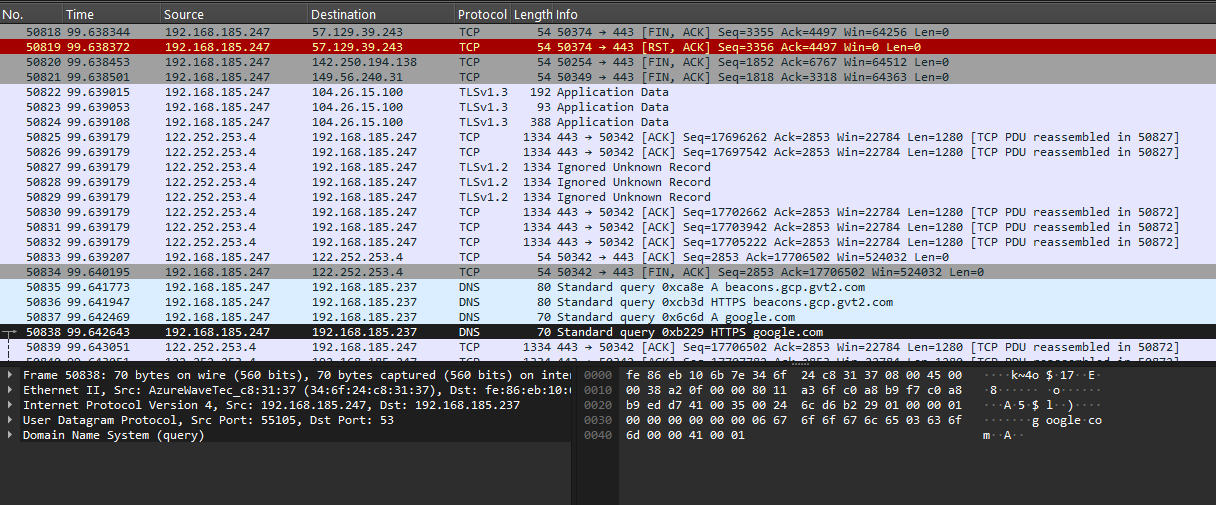
* Capture the information of our active network.

3.Browse a website or ping a server to generate traffic

* I Am search in firefox ( google.com)

4.Stop capture after a minute.

* Am try to understand what type of data capture the wireshark
* Member of protocols
* Timing
* Destination
* Protocols
* Length of information and
* In the Bellow have particular protocol information view.

****

**In 50837 capture the google.com**

5.Filter captured packets by protocol

6.Identify at least 3 different protocols in the capture.

(TCP,DNS,TLSV,QUIC,UDP, ARP …)

* Search a particular protocol after the stopping capturing

.ex: TCP search in search box display all TCP protocols only

7.Export the capture as a .pcap file.

Save as a name of( example.pcap) file

**NOTE: WE WANT TO MORE INFORMATION ABOUT WIRESHARK , IF**

**YOU POSSIBLE CONDECT A CLASS THIS TOPIC OR SUGGEST**

**ANY GOOD MENTER CLASSES ME .**