|  |
| --- |
| **Lovely Professional University** Logo  Description automatically generated |

**Name: Mohammad Ashad khan**

**Reg no: 11907101**

**Roll no: 20 (KE057)**

**Faculty: Navjot Kaur**

Q.25)

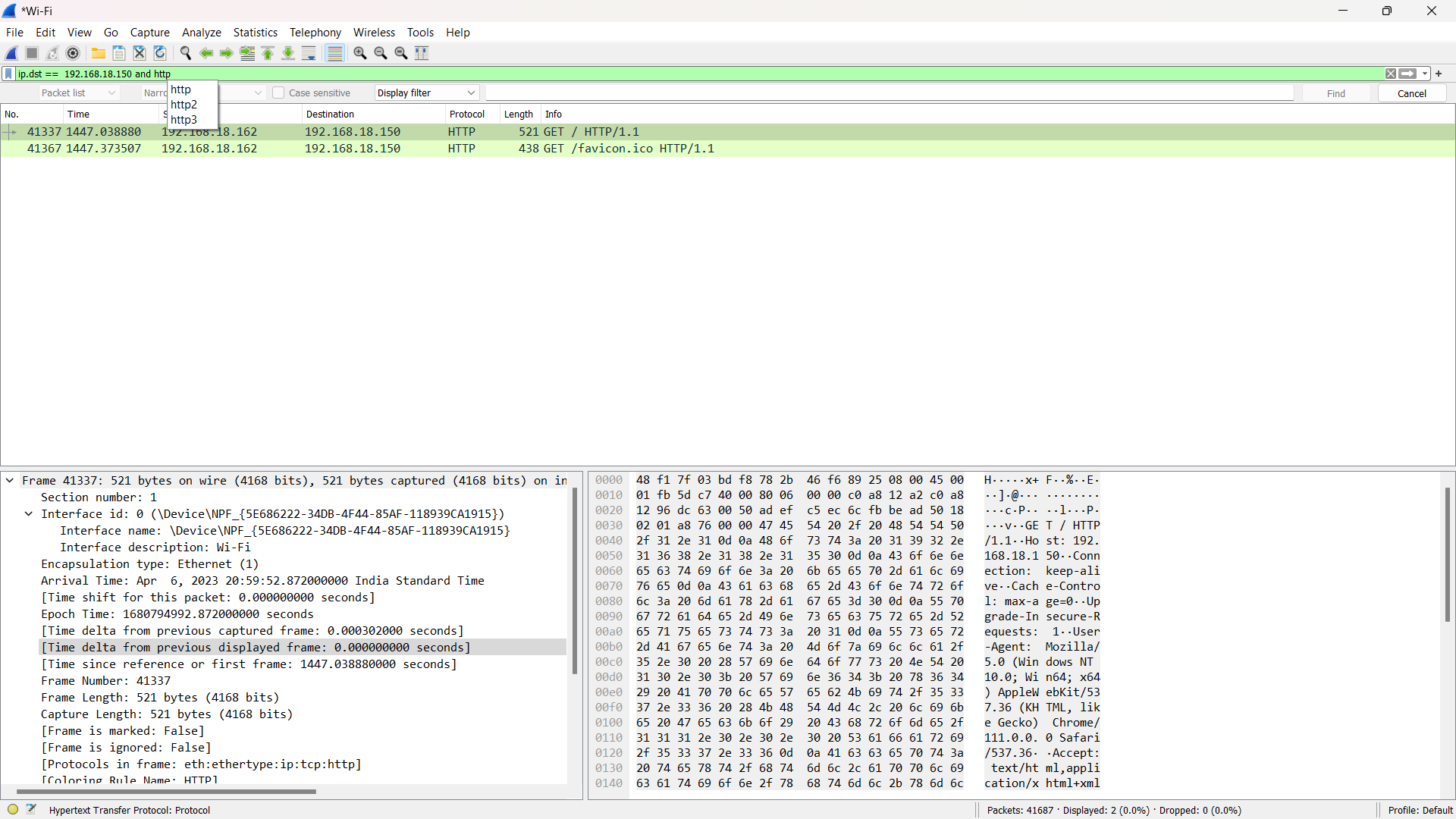
Use any open source software to generate report to capture packets from a network connection, trace connections, view the contents of suspect network transactions and identify bursts of network traffic.

In order to compete this following task above I’ve used an Open Source Tool named “Wireshark”

**Capturing packets from a network connection**.

I connected to the network I wanted to capture packets from after installing Wireshark. I then launched Wireshark and chose the network interface from which I wanted to gather packets. I had a Wi-Fi connection, so.

The "Capture" button will cause it to begin capturing packets. In addition A display filter can be used to filter the packets being captured. To capture packets from a specific destination IP address, I entered the address below. I used the filters "http and ip.dst == 192.168.18.150"



**2. To trace then network connections:**

Now we can trace the connection by following the TCP stream after identifying the sync packet. Right-click the packet and choose "Follow TCP Stream" to accomplish this. This will open a separate window where all of the connection's packets will be visible.

Graphical user interface

Description automatically generated

**3. To view the contents of suspect network transactions.**

After simply clicking on follow or TCP stream we can easily get access to all the content of the the suspect network .

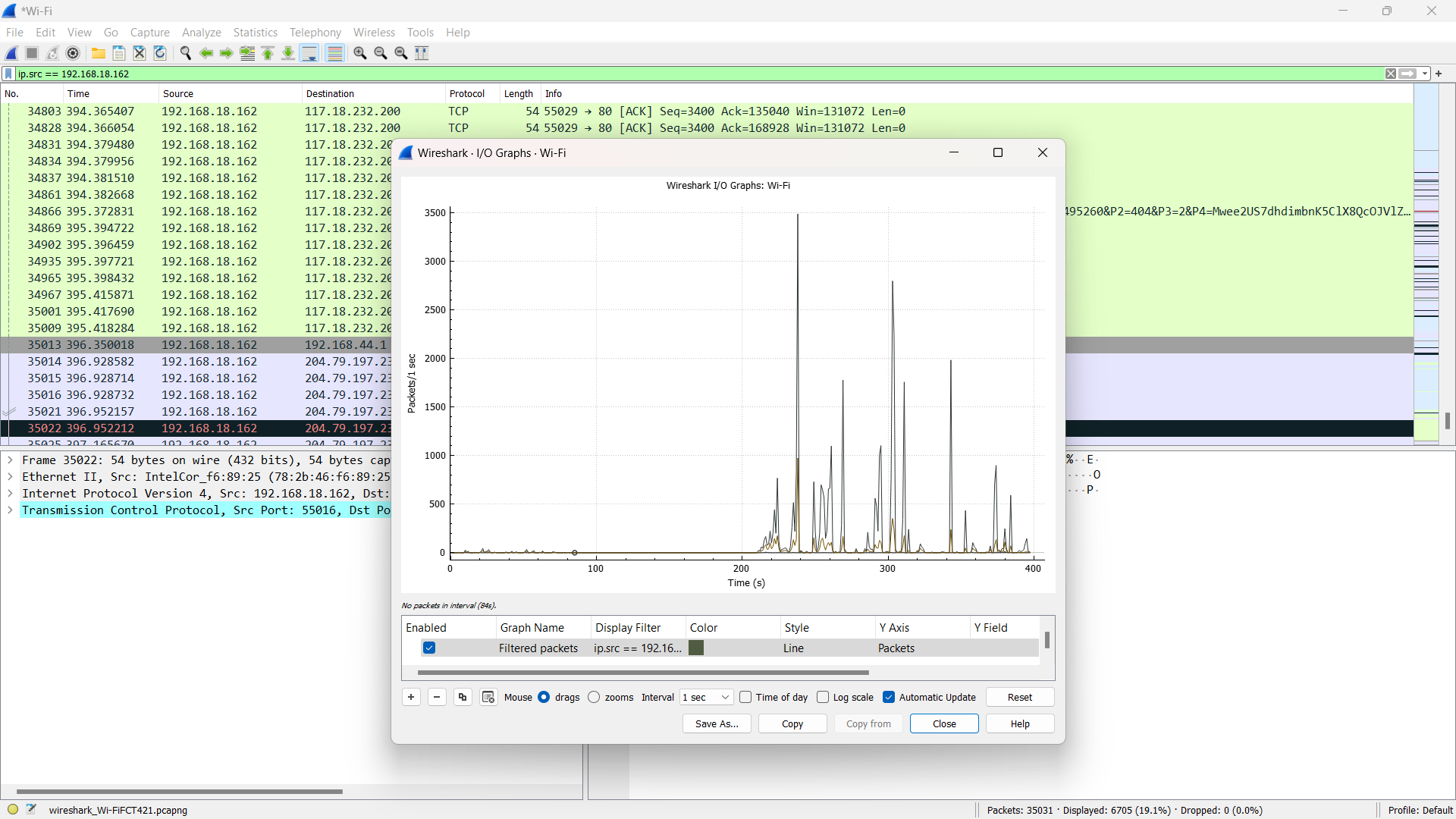
Graphical user interface, text

Description automatically generated

**4. Identification of network bursts traffic.**

This term usually means identifying the traffic occurring on a specific network of an filtered or desired ip address.

Real time analysis of network traffic.

****

Traffic on a network pr second.

**GitHub Link:** [**https://github.com/xashad/Opensource**](https://github.com/xashad/Opensource.git)