|  |
| --- |
| Lovely Professional University |

Name: Mohammad Ashad khan

Reg no: 11907101

Roll no: 20 ( KE057)

Faculty: Navjot Kaur

Q.25)

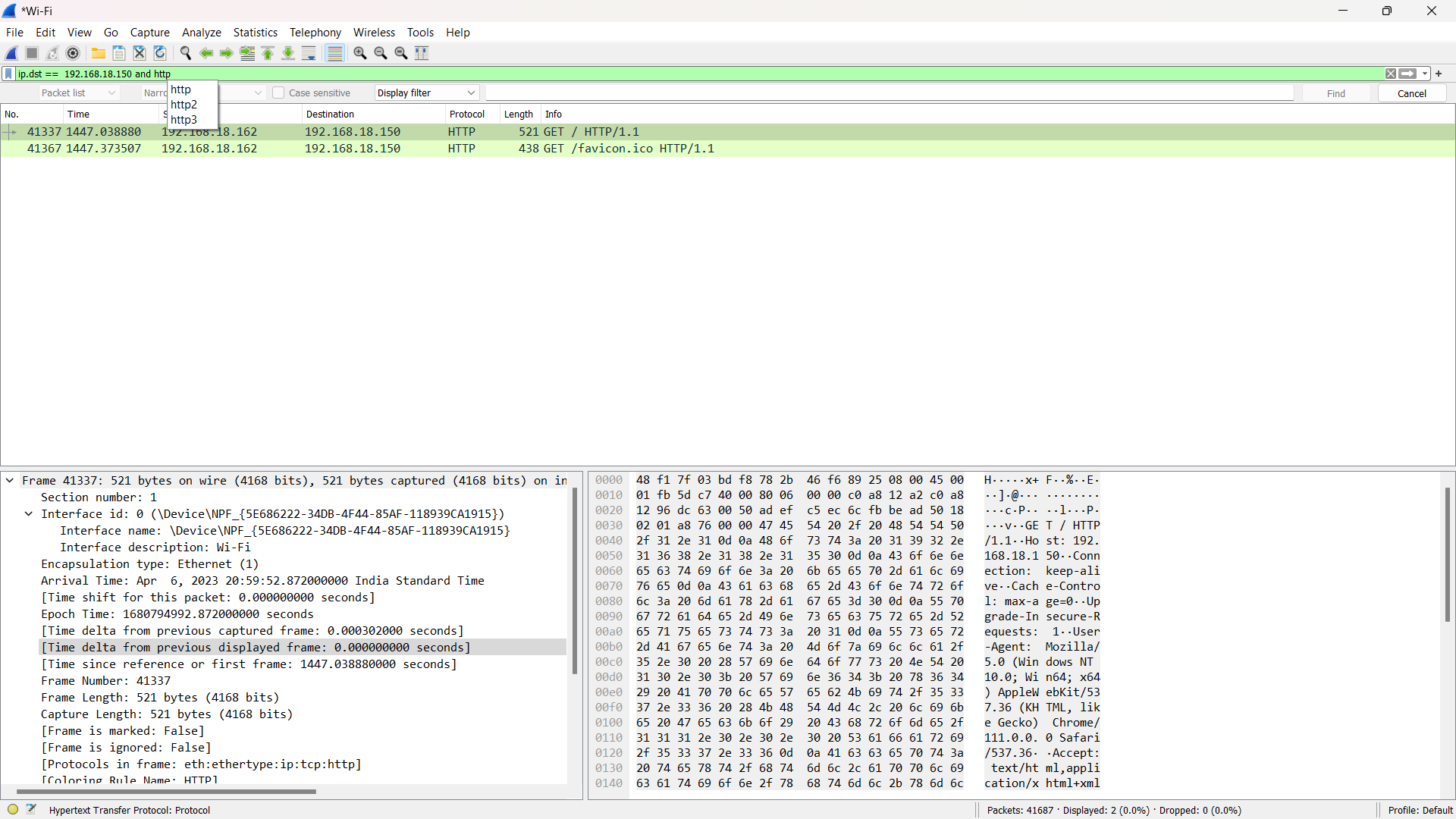
Use any open source software to generate report to capture packets from a network connection, trace connections, view the contents of suspect network transactions and identify bursts of network traffic.

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

**1.Capture packets from a network connection**.

After installing Wireshark, I Connected to the network that I want to capture packets from. And I opened Wireshark and selected the network interface that I want to capture packets from. As I was connected to a Wi-Fi.

By clicking on the "Capture" button it will start capturing packets. And further If we want to filter the packets being captured, we can use a display filter. As I entered the address below to capture packets from a specific destination IP address . I used the filter " ip.dst == 192.168.18.150 and http “



**2. To trace connections:**

After identifying the SYN packet, you can follow the TCP stream to trace the connection. To do this, right-click on the packet and select "Follow TCP Stream". This will display all the packets related to the connection in a separate window.

Graphical user interface

Description automatically generated

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

Graphical user interface, text

Description automatically generated

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