Experiment 14

FAMILIARIZATION WITH WIRESHARK

14.1 Aim

Familiarisation of wireshark .

14.2 Theory

Wireshark is the most popular and commonly used network protocol analyzer in the world. It gives you the view of what's going on in your network. Wireshark is a network data capture application that "understands" the structure of various networking protocols. It can parse and display the fields, as well as the meanings of the fields, as defined by various networking protocols. Wireshark captures packets using pcap, hence it can only collect packets on networks that pcap.

In our computer lots of communication happends when connected to a network. We can see a lot of packages there and we can filter each one with the protocol specified there . When we visit a site, we obtain their IP address and wireshark can capture those IP addresses and the data transferred. But wireshark cannot obtain the encrypted data. websites that are not secured are vulnerable with wireshark. we can filter the packets based on various conditions. Here we are filtering TCP packets that contains google in it . Installation of wireshark in linux is as follows,

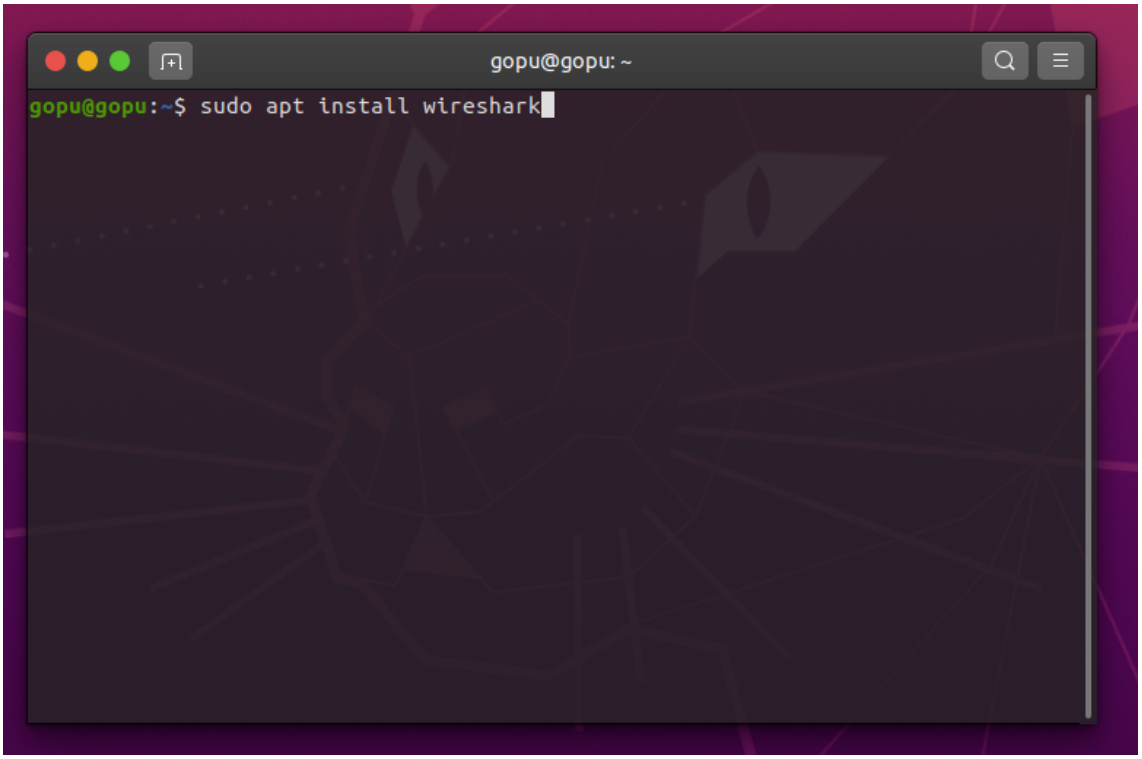

Figure 1: Installation of wireshark

After installation open wireshark with superuser permission to access our wireless or wired network interface. In the home page of the network adapter , we can see the network activites as soon as we hit capture.

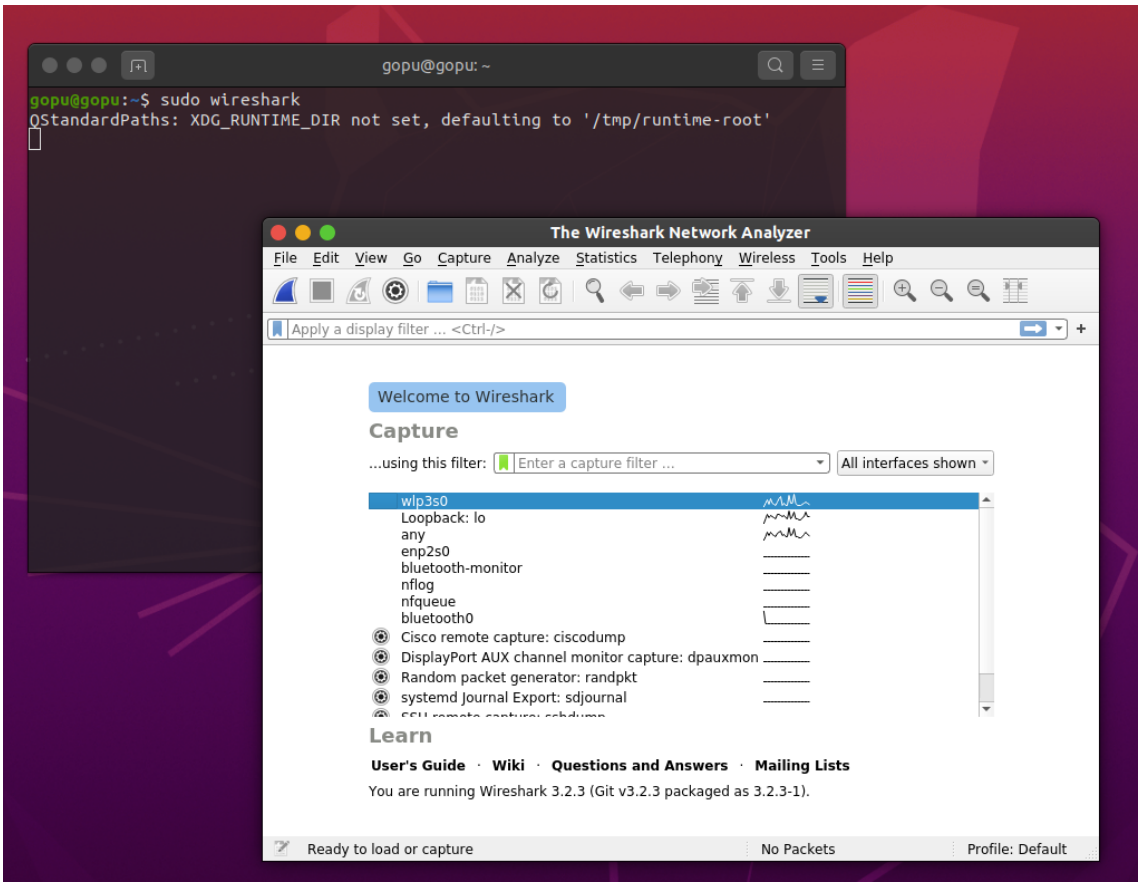

Figure 2: UI Interface of wireshark

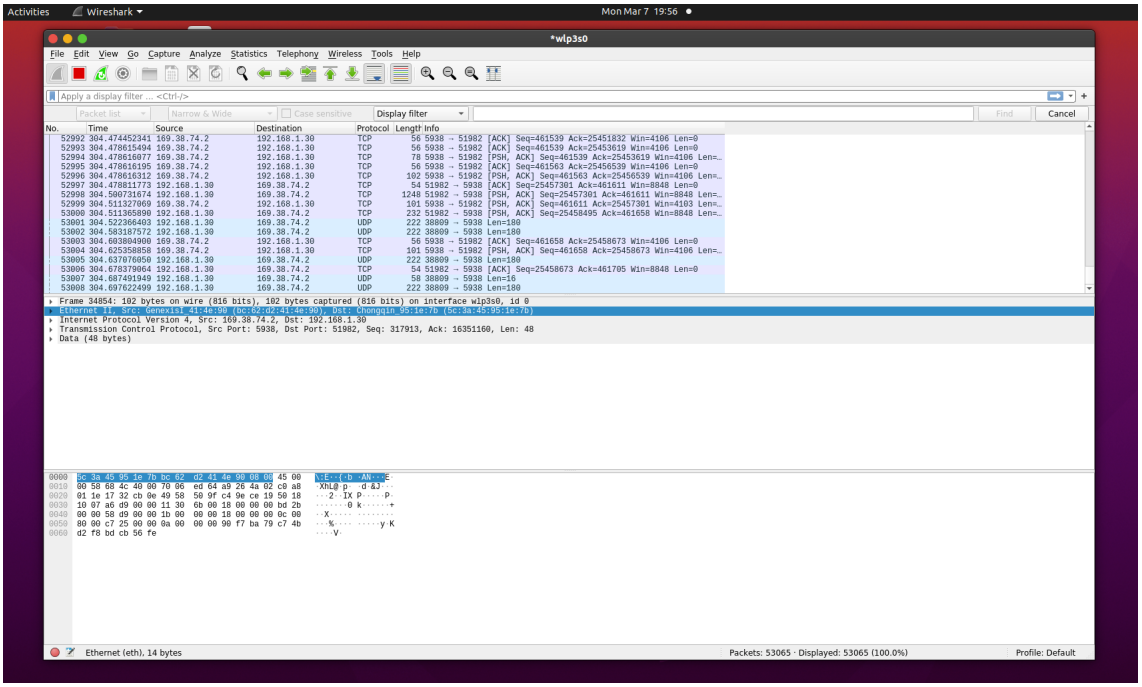

Figure 3: Capturing network packets with wireshark

We can see a list of packages generated while we are browsing google.com. These packets are encrypted and the data inside is hidden and safe.

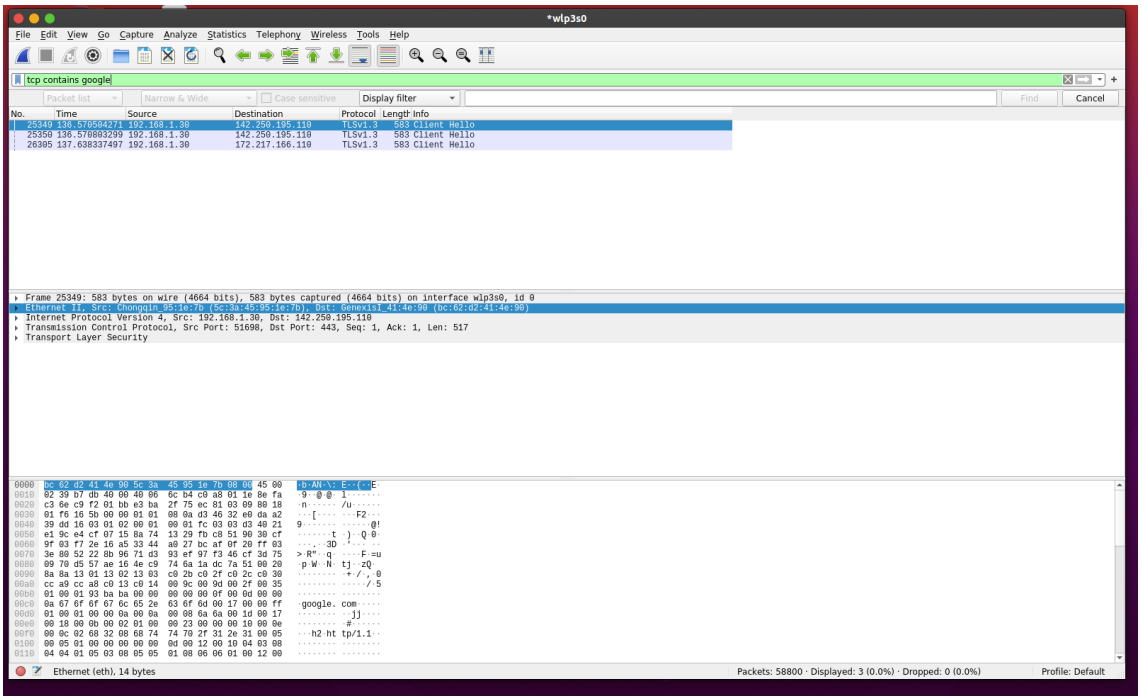

Figure 4: Filtering captured TCP network Packets

Wireshark filters are useful for identifying various wireless network attacks such as deauthentication, disassociation, beacon flooding or authentication denial of service attacks. Wireshark is a legal tool, but it becomes illegal when you monitor a network that you don't have authorization to monitor.

14.3 Result

Got Familiarized with wireshark .