# LAB 2: Examining Packets using Wireshark

*PACKET SNIFFING USING WIRESHARK*

Q1)

A) TCP

B) IP addresses of first SYN packet are:

Source IP address: 10.196.6.245

Destination IP address: 10.250.200.7

Yes, the destination IP address is matching with iitgoa.ac.in.

C) Source Port:58012

Destination port: 443

D) UDP is the protocol that is in majority.

Q2)

A) for chrome it is UDP

B) for Firefox it is both UDP and TCP

Q3)

A) url: daystar.ac.ke
Application layer: HTTPS, NA
Transport layer: TCP, src port: 59813, Dst port:80
Network layer: - IPv4, src: 10.196.6.245, Dst:41.204.160.15
Data link layer: - IPv4, src: 78:af:08:9b:2d:05 , Dst: 00:04:96:9a:82:da
Physical layer:- NA

B) Total Data packets: 170
Time taken: 0.431ms

Bonus question

Q4)

First we connected our both laptops with same mobile network, then from one laptop we took ip address with the help of ifconfig, then in second laptop in wireshark we filtered with the help of ip.addr==<ip address of first of laptop>, and then the packets that were flowing in first laptop were shown in the second laptops wireshark.