**Networking Lab**

**Lab Experiment No 6**

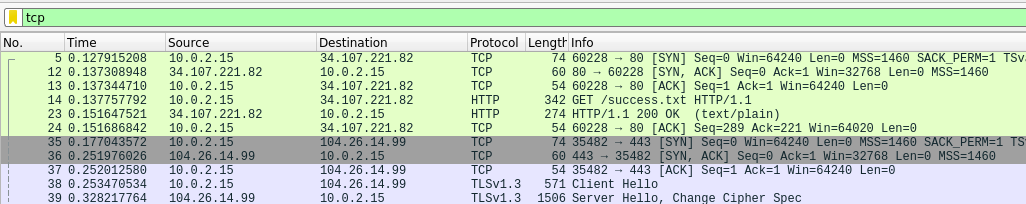
Name: Iyer Sreekesh Subramanian Roll No. 24

**Aim**: Installation of Wireshark (Network protocol analyzer) and analyze the traffic

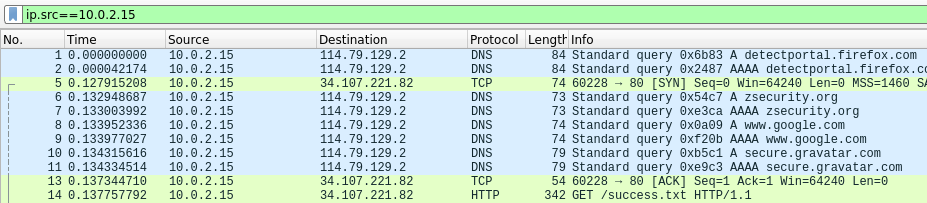
1. What is Wireshark?  
     
   Wireshark is the world’s foremost and widely-used network protocol analyzer. It lets you see what’s happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions.

## What filter would you use?

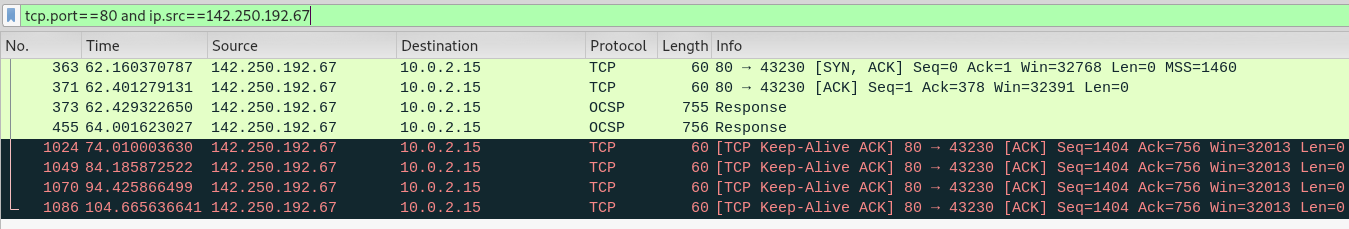
## To monitor all TCP packets

**tcp**

## To monitor and display all incoming packets from a specific IP address **ip.src==<source\_ip\_address> Eg. ip.src==10.0.2.15**



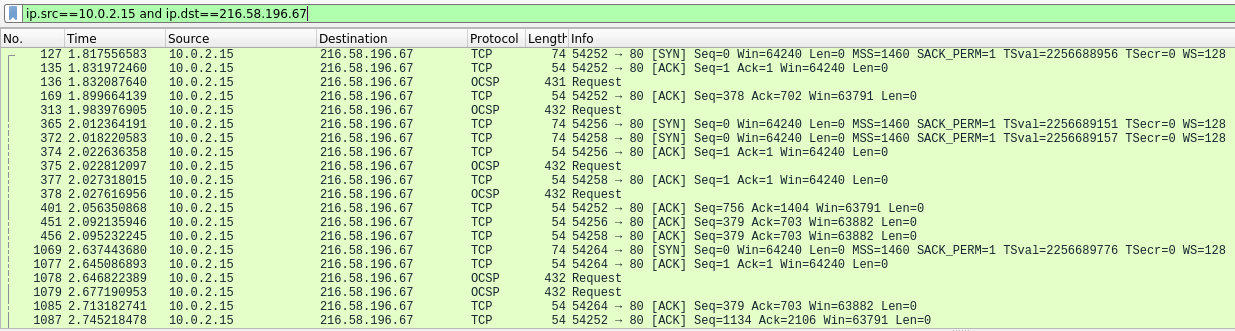
* 1. To check all requests to and response received from an HTTP Web server.

**tcp.port==80 and ip.src==142.250.192.167**  


## To monitor all packets exchanged between 2 IP addresses.

**ip.src==<source\_ip\_address> and ip.dst==<destination\_ip\_address>**

**Eg. ip.src==10.0.2.15 and ip.dst==216.68.196.67**



## Check all incoming requests to an HTTPS Web Server **tcp.port==443 and ip.src==10.0.2.15**

