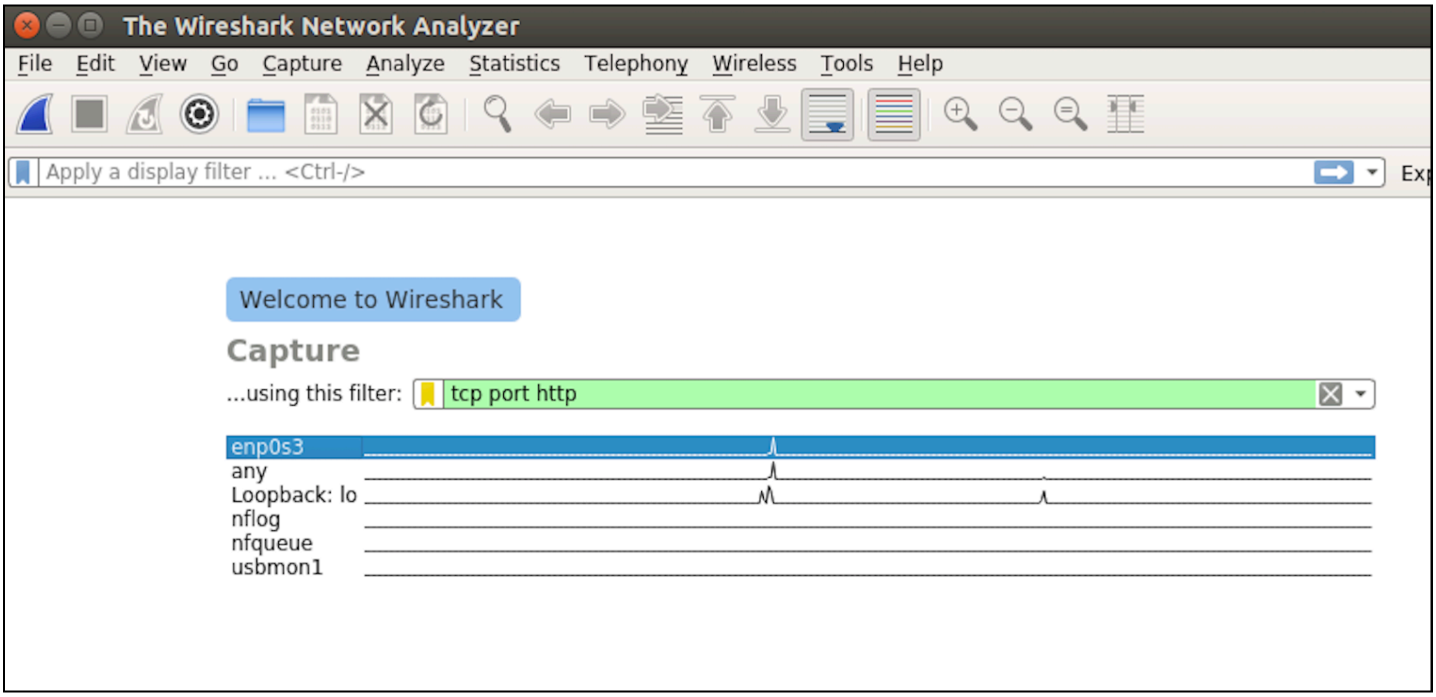
Exercise 1 : Wireshark

- open a new terminal windows and type `sudo wireshark`
- select an appropriate interface such as `eth0` or `wln0` , enter a valid filter
- start the capture


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Exp
Welcome to Wireshark
Capture

...using this filter: tcp port http

enp0s3
any
Loopback: lo
nflog
nfqueue
usbmon1

- **Layer 7 [Application Layer]**
  - (a) HTTP
    - start the capture with appropriate interface and filter as `tcp port http`
    - goto http://dayanandasagar.edu from web browser
    - stop the capture
    - identify HTTP headers such as version, protocol, User-Agent?
  - (b) DNS
    - start the capture with appropriate interface and filter as `port 53`
    - open a new terminal window, execute `nslookup google.com` , `nslookup dayanandasagar.edu`
    - stop the capture
    - identify DNS flags, queries, answers?
  - (c) SSH (Secure Shell)
    - start the capture with appropriate interface and filter as `port 22`
    - start the capture

        - open a new terminal window, ssh into another system `ssh <username>@<ip-addr>`
        - example `ssh netlab@10.1.12.188`
        - stop the capture and analyse
        - identify ssh protocol, key-exchange algorithm, packet lengths?

- **Layer 4 [Transport Layer]**

    - (a) UDP

        - start the capture with appropriate interface and filter as `udp`
        - on one system execute `nc -u -l <port-no>`
        - example `nc -u -l 9999`
        - on another system execute `nc -u <ip-addr> <same-port-no>`
        - example `nc -u 10.1.12.188 9999`
        - stop the capture and analyse
        - identify source port, destination port, data?

    - (b) TCP

        - start the capture with appropriate interface and filter as `tcp`
        - open a new terminal window on first system and execute `nc -l <port-no> > <filename>`
        - example `nc -l 1234 > hello.txt`
        - from the second system execute `nc <ip-addr-first-system> <same-port-no> < <filname>`
        - example `nc 10.1.12.188 1234 < hello.txt`
        - stop the capture and analyse
        - identify source port, destination port, flags?

    - (c) TLS

        - start the capture with appropriate interface and filter as `port 443`
        - goto any https website from web browser
        - stop the capture
        - identify version, length, content-type, application-data-protocol?

- **Layer 3 [Network Layer]**

    - (a) Ping

        - start the capture with appropriate interface and filter as `icmp`
        - open a new terminal window and ping a system `ping <ip-addr>`
        - example `ping 10.1.12.188`
        - stop the capture and analyse
        - identify ICMP Requests and Replies, sequence number, type, code?

- (b) Traceroute
    - start the capture with appropriate interface and filter as `icmp`
    - open a new terminal and execute `traceroute <ip-addr>/<website>`
    - example `traceroute www.google.com`
    - if traceroute is not installed, install is using `sudo apt install traceroute`
    - stop the capture and analyse
    - identify number of hops, time elapsed and path taken?
- (c) ARP
    - start the capture with appropriate interface and filter as `arp`
    - ping a system which is not in your network
    - example `ping 10.1.12.189`
    - stop the capture and analyse
    - identify sender mac address, sender IP address, Target IP address, Opcode?

- **Layer 2 [Data Link Layer]**
    - examine the ethernet layer for the above captures
    - identify source mac address, destination mac-address, Type?