**sudo tcpdump**

**sudo tcpshark**

To see link-layer information of all available devices (which have a driver loaded) use the command:

**ip link show.**

tcpdump

-i live traffic from interface

-r read from trace file

-w write into trace file

dns port 53

**tcpdump "udp dst port 53" //captures packets for which dst port is 53**

**tcpdump "udp src port 53" //captures packets for which src port is 53**

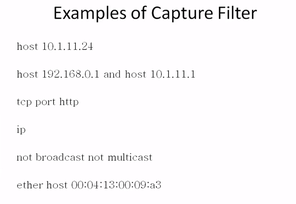
**tcpdump "udp port 53" //captures packets for which src or dst port is 53**

**tcpdump "dst host buet.ac.bd" //captures packets for which destination is //buet.ac.bd**

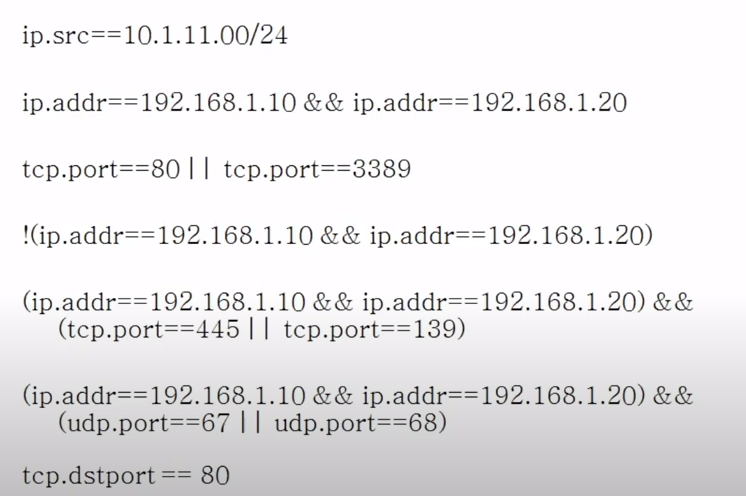
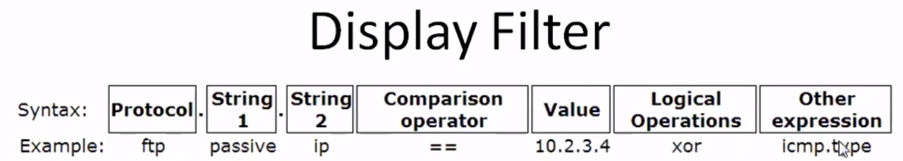
**tcpdump "(tcp and host buet.ac.bd) or udp port 53" //captures tcp packets for which**

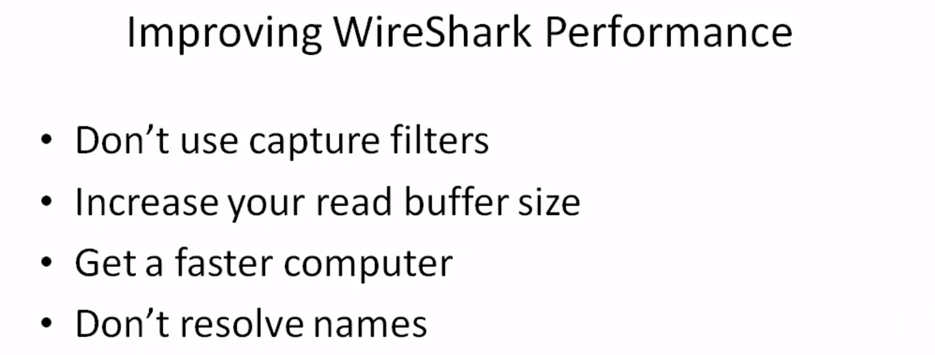
**//src or dest is buet.ac.bd and udp packets for which port is 53**

**wireshark**



Another type of filter: display filter(post filter)





Advanced Networking Lecture 1

