# Malaviya National Institute of Technology Jaipur
# Computer Networks
# Lab Tasks#2

---

**Problem 1: Learn use of Display Filters**

1. Write the syntax for the ethereal command which capture filter so that all IP datagrams with a source or destination IP address equal to 172.17.4.116 (use some valid system IP of lab) are recorded.

2. Write the syntax for an ethereal display filter that show IP datagrams with their destination IP address equal to 172.17.4.100 (use a valid system IP of lab) and frame size is greater than 400 bytes.

3. Write the syntax for an ethereal display filter for packets containing TCP segments with the source and destination IP address equal to 172.17.4.116 and using port no 23.

4. Write the syntax for an ethereal display filter that shows packets containing ICMP segments with a source or destination IP address equal to 172.17.4.116 and frame numbers between 15 and 30?

5. Give the output of the following ethereal capture filter expression
   ip. addr =172.17.4.116\ tcp .port> 23?

6. Include file in print format and give difference between saving file by TCP dump and ethereal?

7. Use the data captured with ethereal. Support the answers by including the from the saved ethereal captures.

**Problem 2:**

Start up your web browser. Then start up the wireshark (i.e. ethereal) packet sniffer and then begin ethereal packet capture. Next, enter into your browser few websites of your interest. Wait for some time before you stop the capture for some interesting packets. Specify filter "http" in display-filter-specification window, so that only captured http messages will be displayed later in the packet-listing window. Find out the answer of following questions by observations:

**i)** List the different protocols that appear in the protocol column in the unfiltered packet-listing window.

**ii)** Locate the HTTP GET and response messages. What is the status code and phrase associated with the response to the HTTP GET request?

**iii)** Your browser running which of the HTTP version 1.0 or 1.1? Which version of HTTP is running by the server?

**iv)** What languages (if any) does your browser indicate that it can accept to the server?

**v)** Find out the IP address of your computer on which browser is running ? What is IP address of your entered url of website server?

**vi)** Find out the status code returned from the server to your browser?

**vii)** Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

**viii)** Find out when was the HTML file that you are retrieving last modified at the server?

**ix)** Find out how many bytes of content are being returned to your browser?

**x)** By inspecting the raw data in the packet content window, if you see any headers within the data that are not displayed in the packet-listing window write few name?

**xi)** What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

**xii)** How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day)