1 Wireshark exercise

In each of the following questions you have to mention steps used to achieve the output in sufficient detail. Also mention any additional observations, that you have made.

1. Capture packets while opening http://intranet.iiit.ac.in/ and see the information exchanged between your machine and intranet machine. Use 'Follow TCP Stream' option to observe application level data that was exchanged. Learn about HTTP request and response headers from the captured information.

   Now use telnet (Windows-7 users can use putty for telnet) and connect to intranet.iiit.ac.in on port 80 and send different types of HTTP requests. Mention the shortest request through which you can obtain the intranet page.

2. Intranet page refers to css file named 'index.css'. Download the contents of this file using your knowledge of HTTP protocol using telnet. You are not supposed to use any download manager or browser to achieve the task.

3. Configure thunderbird / evolution / outlook express etc. for checking your IIIT email account using IMAP. Try to send email using configured client and capture the packets in Wireshark. Compare the captured output with protocol described at following URL.

   Now send email to yourself using only telnet, without using any browser or email client.

4. Study about POP3 protocol using RFC at http://www.ietf.org/rfc/rfc1939.txt. Try to use POP3 protocol to check your email through telnet.

   Compare the difference in ease of learning various protocols using Wireshark by observing their useful parts versus learning protocol in detail using RFCs.

5. Learn the use of nmap command for port scanning. Find out IP addresses of machines that are working in your subnet. Start wireshark to capture packets. Now use 'arp -d' command to delete ARP entry of some neighbour. Then try to ping neighbour whose ARP entry you have deleted and observe the ARP protocol that gets used.

   Restart wireshark capture. Now add delete the entry for the same neighbour again. Then add a static ARP entry for the neighbour using

'arp -s' command. Then try to ping to neighbour whose ARP entry has just been added. Observe the difference between packets captured now with respect to packets captured when static entry was not added.