CN LAB
WIRESHARK

IT IS COMPULSORY TO ATTACH SCREENSHOT WITH EACH ANSWER.

1. List 5 different protocols that appear in the protocol column in the packet-listing window. Also describe each protocol in short.
2. Visit a http site and examine 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 packet listing in seconds)
   (Hint: Timestamp of http GET packet=10.25478, Timestamp of http OK packet=10.41478, Required answer = 10.41478-10.25478=0.16 s)
3. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   (Hint: First to know the http version of your browser: Select GET packet, Expand the http protocol, then expand the GET option, HTTP version information is listed in the item ‘Request Version’. To know the http version of server, follow same steps with http OK packet)
4. What languages does your browser indicate that it can accept to the server?
   (Hint: languages information is listed in the item ‘Accept-Language’ in the HTTP GET message).
5. What is the status code returned from the server to your browser? When was the HTML file that you are retrieving last modified at the server?
   (Hint: Analyse the http OK packet)
6. What is the IP address of the mnit.ac.in? What is the IP of your computer? What is the length of these IP addresses in bits? How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
7. Open a terminal on your PC, execute this command:
   “nslookup www.google.com 8.8.8.8” While capturing the packet in background, set your filter to “ip.addr == 8.8.8.8”.
8. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header.
9. Determine the length (in bytes) of each of the UDP header fields.
   (Hint: See the packet diagram)
10. The value in the Length field is the length of what? What is the length of UDP payload for your selected packet?
11. What is the largest possible source port number?
12. What is the protocol number for UDP?
    (Hint: To answer this question, you’ll need to look into the IP header.)
13. Establish TCP connection and name the 3 packets involved in the connection (TCP handshake). Determine what is the IP address of the client (the initiator of this TCP connection), and what is the server’s IP address? From which port the client initiates the connection, and what is the port number used for this connection on the server side?
14. During the handshaking of this connection, what is the length of the TCP header? What is the optional field(s) in the TCP header.

15. What is the sequence number of the TCP SYN that is used to initiate the TCP connection. What is the sequence number of the SYN-ACK segment? What is the initial buffer size (window size) advertised by the client?
16. Execute the command “ping www.mnit.ac.in” in terminal, Use WireShark to capture the generated ICMP packet (you can use filter “icmp”) and answer why is it that an ICMP packet does not have source and destination port numbers?
17. Choose one of the ping request packets sent by your host, what are the ICMP type and code numbers? Find the corresponding ping reply, what are the type and code numbers?
18. Apart from the ICMP headers, what is in the data field of these ICMP packets? Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer? And Which fields stay constant?
19. Enter the following URL into your browser
    http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html
    The username is “wireshark-students” (without the quotes), and the password is “network”. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
20. Extract credential from the second GET message.