

**Assignment 2****Due: 11/9/21****Total: 20marks****Questions:**

1. Open Wireshark and start capturing packets. In your web browser type <https://intranet.cb.amrita.edu/> and let the web page load. Once you see the TLSv1.3 packets being captured in Wireshark, wait for a while and stop the packet capture and save it.

(5 marks)

- a. What is the IP address of the client and server?
  - b. Show the TCP three way handshake in the list of packets captured in Wireshark and explain
  - c. When does the TLSv1.3 occur in the list? Explain during with HTTPS point of view
  - d. Explain the TLSv1.3 Client Hello and Server Hello steps here.
  - e. Show the web page name in the packet content
  - f. In which step in TLSv1.3 does the webpage name occur in the packet content?
- 
2. Open Wireshark and start capturing packets. In your web browser type <http://mininet.org> and let the web page load. Once you see the HTTP packets being captured in Wireshark, wait for a while and stop the packet capture.

(5marks)

- a. Explain the HTTP protocol from the packets captured. i.e the GET and response
- b. Is it a secure connection or not and how will you identify the same?
- c. What is the HTTP status code and phrase returned from the server in response to the second HTTP GET? Did the server explicitly return the contents of the file? Explain.
- d. Explain the role of DNS here and show the relevant packets captured

- e. Locate the DNS query and response messages. Are then sent over UDP or TCP?  
Explain the same
  - f. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
3. Implement the following topologies using Cisco Packet tracer (10 Marks)
- Show the transfer of packets from one end system to another using both simulation and ping command
- a. Star
  - b. Ring
  - c. Bus
  - d. Hybrid

The IP address of the devices should contain the Roll numbers of group members.

Eg: CB.EN.U4AIE1900**1**, CB.EN.U4AIE1900**2**, CB.EN.U4AIE1900**3** and  
CB.EN.U4AIE1900**4**.

Then the IP address of your end systems should contain their respective roll numbers.

192.17.2.**1**, 192.17.2.**2**, 192.17.2.**3** and 192.17.2.**4**

Note: The number of end systems can vary depending upon the network you configure