St. Vincent Pallotti College of Engineering & Technology, Nagpur
Department of Computer Engineering
Session 2023-24
Advanced Computer Networks (ACN) Lab Manual

Problem Statement 5: Installation, Understanding & Analyzing Different Protocols using Wireshark Packet Sniffer tool.

Aim 5a: Understand Wireshark Packet Sniffer Tool and display the following after the installation:

a. Select a capture interface and create the first PCAP file.
b. Navigate through menus and status bar
c. Finding a text string in a trace file
(Refer the attached PDF and display the outputs)

Aim 5b: Analyze 3-way Transmission Control Protocol using Wireshark Packet Analyzer.

To execute the mentioned points, students need to press the CAPTURE button of Wireshark tool, go to the browser & check for any website, go back to Wireshark tool & press STOP button to stop capture the packets (above 4000 to 5000 packets are to be captured). Save the PCAP file & use the attached TCP.pcapng file and start analyzing it for the mentioned points:

a. Identify the 3-way handshake TCP segments during establishment phase and note down the resp. Source IP address, Destination IP address and respective sequence numbers for a particular set of segments.
b. Identify the value of header calculation as mentioned in terms of the number of bytes.
c. Identify the flag values of SYN, SYN+ACK and ACK segments.
d. List down the 4 protocols that you identified from the live capture and explain each in 3 to 4 lines.
e. Identify the name of the protocols is used for Client Server communication from your live capture packet? Explain in your own words.
f. Identify the type of protocol that uses PSH flag for application data transfer.
g. Show the process to validate the TCP checksum value when its incorrect in the Packet detail panel.
h. Write down the Round-Trip Time (RTT) for SYN+ACK segment from your observation.
i. Observe and find Client and Server TCP MSS size.
j. Explain SACK option under TCP. How do you find whether SACK is permitted or not?
k. Observe and identify the connection termination phase for a sequence of segments. Explain the working of the identified segments in your own words.
l. Explain ICMPv6 neighbor solicitation and neighbor advertisement queries in your own words.