Computer Networks Laboratory
IT 3095

Lab instructions
On

Introduction to Wireshark Protocol Analyzer and exploring its features

Part- A

© Prof. (Dr.) Amitkumar V. Jha, School of Electronics Engineering, KIIT-DU, Bhubaneswar-751024

Aim of the Experiment: To understand the functionalities of the Wireshark protocol analyzer and its applications in networking such as packet capturing, sniffing, network traffic interpretation, etc.

Objective: To understand the basic functionalities of Wireshark such as configuration, preferences, capture filter, display filter, data interpretation, encapsulation/decapsulation, etc.

Software Required: Wireshark Protocol Analyzer

Procedure:

- Start capturing packets on your Wi-Fi interface or Ethernet (if you are using wired LAN).
- Visit a few websites from your browser.
- Stop the capture.
- Notice that thousands of packets are captured. List out various application-level protocol used in those packets. Make sure you notice at least one HTTP and DNS packet.
- Use display filters to only see the packets you are interested in. For example, a display filter of "**dns**" would only show you DNS packets.
- Discard the captured packets and start fresh.
- This time use capture filters to capture only specific packets. For example, a capture filterof "**port 53**" will only capture DNS traffic. This is different from display filters. Here you are filtering at the time of capture itself.
- Start capture.
- Visit some different websites (other than the ones you visited in the first run).
- Stop capture and notice that only DNS packets have been captured.
- Click on any packet and notice how, in the middle area, encapsulation and decapsulation work. You should be able to see the raw frame, the Ethernet part from it, the IP part from the Ethernet part, the UDP part from the IP part, and the DNS part from the UDP part.
- Now change the bottom pane view style to packet diagram through **Edit → Preferences → Layout → Pane 3 → Packet Diagram**. And observe the encapsulation /decapsulation using the packet diagram.

Observations: (Take Screen-shorts for putting Outputs in the Record)

- Take a screenshot of your Wireshark application without applying any filter showing all three panes.

  Note: *Pane 3 can be viewed either in the* ***packet diagram*** *or* ***packet bytes*** *view.*
- Take a screenshot of your Wireshark application by applying a display filter showing all three panes.

  Note: *Pane 3 can be viewed either in the* ***packet diagram*** *or* ***packet bytes*** *view.*
- Take a screenshot of your Wireshark application with Capture filter showing all three panes.

  Note: *Pane 3 can be viewed either in the* ***packet diagram*** *or* ***packet bytes*** *view.*
- Take a screenshot of your Wireshark application with Capture as well as display filters showing all three panes.

  Note: *Pane 3 must be shown in* ***Packet diagram*** *format only to visualize encapsulation and decapsulation.*

Conclusion: After the experiment, you must be able to write a conclusion in your own words. The conclusion may be based on the following observations: how to configure Wireshark, significance of capture filter, significance of display filter, data analysis and interpretation, encapsulation/decapsulation, etc.

Outcomes:

- Students should be able to demonstrate that they can operate Wireshark without much help.
- Students should be able to understand encapsulation and decapsulation properly and should be able to demonstrate how it works in Wireshark.
- Students should be able to understand the difference between capture and display filters.They should also identify basic filters.

***