Assignment 1

Wireshark Fundamentals

Instructions

Wireshark software and a tutorial can be found using the link provided below. This assignment is divided into five parts. Each part will require you to analyze a different pcap file using Wireshark. **Please submit a single PDF document containing Wireshark output screenshots and filters used wherever necessary.**

https://www.wireshark.org/

Part 1: tr-chappellu.pcapng

a. Find the most active TCP conversation in the file (by bits per second).
b. What is the total amount of bytes transferred from A to B and from B to A in the most active TCP conversation? (Hint: right-click on the conversation, select Apply as Filter > Selected > A → B. Save the packets once the filter is applied)
c. Calculate the Round-Trip Time (RTT) between A and B by inspecting the TCP Handshake.
d. What are selective acknowledgments? Are they permitted in this conversation? Please justify your answer.

Part 2: tr-http-pcaprnet.pcapng

a. Use a filter to display the HTTP response time for each HTTP request.
b. Define and explain the significance of each HTTP response status code.
c. Apply a filter that lists packets wherein the HTTP response time is greater than one second.

Part 3: tr-ftpfail.pcapng

a. Use a filter to display the FTP request and response packets.
b. List the server and client IP addresses and port numbers.

c. Use another filter to display only the FTP response codes for the packets. Define and explain the significance of the response codes.
d. Is the FTP termination initiated by server or client? Please justify your answer.
e. How secure is FTP?

Part 4: tr-bootp.pcapng

a. What layer of the OSI model can DHCP Discover packets be found? What type of packet is DHCP Discover? List the source and destination IP addresses and port numbers.
b. How many DHCP packets are exchanged between the client and server before the client receives an IP address? Define and explain the commands used in the DHCP handshake.
c. What is the significance of DHCP Release packet?
d. Explain the communication flow between a DHCP client and server on a network that has two DHCP servers.

Part 5: tr-nameresolution.pcapng

a. Use a filter to display DNS traffic only.
b. Which transport layer protocol is used for DNS queries?
c. What is the response for the DNS query of packet number 1004? What is the reason for this response?

Remember to submit your work on NYU Classes as a single PDF document with all necessary screenshots and Wireshark filters. **Late assignments will not be accepted!**