Indian Institute of Technology, Bhilai

CSL351: Computer Networks

Assignment - 3 (Wireshark)

Full Marks: 35 *Deadline: 26/01/2026, 11;59PM*

Submission Instructions:

1) Answer all the questions.
2) Deliverables in a .zip:
   a) Submission Guidelines: Upload the **Assignment Report**, **pcap** in .zip.
   b) Readable Report **[1 Point for report quality]** enumerating steps followed with screenshots for each of the important steps:
      i) Pcap trace collected and mention the command/tool used.
      ii) Put the screenshots (**mandatory**) to validate your answers in the report. ○ Clear and concise writing.
3) Follow the instructions carefully given in the question.
4) You can use latex/word to make the pdf.
5) The naming of the file should strictly follow the given format: <Roll_No>_<Name>_<Assignment No>. If your name is Alex, your roll number is B23CS055, then the filename should be: B23CS055_Alex_03.zip
6) **Any plagiarism case will be considered unethical practice, and appropriate action will be taken against them.**

Objectives:

1. Develop hands-on expertise in capturing and analyzing network packets using Wireshark.
2. Perform Comprehensive Packet Analysis
3. Utilize Filters and Statistical Tools
4. Generate Graphs and Analyze Network Metrics

Description:

This assignment focuses on developing practical expertise in using Wireshark, a powerful network analysis tool. You will learn to capture and analyze packets, apply advanced filtering techniques, and utilize statistical features for effective network troubleshooting. Additionally, you will generate I/O graphs and extract key metrics to evaluate network performance visually.

COMMON GUIDELINES FOR THIS ASSIGNMENT

- Follow the Installation guidelines mentioned in the PPT for wireshark installation and packet capture.
- You can use the following documentation related to Wireshark. (https://www.wireshark.org/docs/wsug_htmlchunked/)_

Open Wireshark and capture traffic for 10 or more minutes. During traffic capture, visit iitbhilai.ac.in, send an email to your personal mail ID using mailbox and web (separate emails to be sent from both the interface), download the Student Handbook from iitbhilai.ac.in, watch a video in youtube.com, Ping tesla.com (with packet size >=2500) and invoke traceroute to iitbhilai.ac.in

PART 1: BASIC ANALYSIS [10 Points]

1. How many packets were captured? Plot the graph showing a precise distribution of different protocols captured by Wireshark. **[2 Points]**
2. Which is the most common application layer protocol observed in the packet list, and how many times have those protocols been used? **[1 Point]**
3. Does Wireshark capture packets of the activities performed by the user only? YES or NO? If No, explain the reason with proof. **[2 Points]**
4. Identify and filter the packets received while downloading the Student Handbook. How many data packets were captured? **[1 Point]**
5. Can you Identify the packets used to ping tesla.com? If yes, How many packets (including both request and response) per ping request have been captured? Verify the information using the terminal output of the ping command. **[1 Point]**
6. Save your packet capture as a .pcap file and give the file name as your roll number. Explain why saving captures in .pcap format is useful. **[1 Point]**
7. Combine filters to display only DNS and HTTP traffic. What filter expression did you use? How many packets match this combined filter? **[2 Points]**

PART 2: STATISTICS [24 Points]

1. Draw the flow graph of packets captured while downloading a Student Handbook file. **[1 Point]**
2. Describe the process of file downloading using the flow graph and packets captured by Wireshark. (Explain on protocol level and mention all the protocols used.) **[3 Points]**
3. Fill the following table with the data extracted from Wireshark: **[5 Points]**

Total Packets Capture	
Total Number of HTTP/HTTPS connections established	
Average Throughput of streaming videos	

How many DNS queries were resolved?	
Average throughput of QUIC Protocols	
Total Number of SMTP packets captured	
Average Packet Length	
Average Packet Length of TCP Traffic	
What is the average time spent on TLS Message Exchange?	
How many packets are retransmitted?	

4. Draw the flow chart of the traceroute command using Wireshark and explain how the traceroute works. **[3 Points]**
5. Can you identify the protocols used for sending emails for both methods? If yes, explain the flow using relevant screenshots/flow graphs. Also, list the protocols used in sequential order. **[2 Points]**
6. Plot the I/O graph for the following: **[5 Points]**
    a. For complete packets captured
    b. For HTTP/HTTPS traffic
    c. For All the ARP, DNS/MDNS, and ICMP Queries
    d. For TCP/TLS Protocols
    e. For UDP protocol
7. Plot Flow Graphs for the following: **[5 Points]**
    a. For Youtube.com
    b. For Accessing iitbhilai.ac.in
    c. DNS Query
    d. ARP Query
    e. Pinging tesla.com

Check Web sources for more information.