Practical 7: To analyze network traffic using Wireshark – capture ICMP packets and study their header fields.

Objectives

1. To capture and study ICMPv4 packets using Wireshark.
2. To understand how `ping` utility generates ICMP packets.
3. To identify and interpret the key fields in the ICMP header.
4. To observe Echo Request, and Echo Reply, and messages.

Lab Task

1. Capture ICMP Packets Generated by `ping`

1. Open Wireshark and start packet capturing on the active network interface.
2. Open Command Prompt and type:

   ```
   ping <hostname or IP address>
   ```

3. Stop capturing once replies are received.
4. Apply the display filter:

   ```
   icmp && ip.addr==destination ip address
   ```

   to view only ICMP packets of the particular destination IP address.
5. Observe the sequence of Echo Request (Type 8) and Echo Reply (Type 0) messages.
6. Examine each ICMP packet's header and note:
   - Type and Code
   - Checksum
   - Identifier
   - Sequence Number
   - Data length

Observation and Analysis

Ping – Part I

1	Destination IP address:
2	Number of ping messages sent:
3	Number of bytes of data sent with each ping message:
4	Round-trip time for each packet:
5	Minimum round-trip: Average round-trip: Maximum round-trip:

Ping – Part II

1	Destination IP address of Echo Request ICMP messages: Does the result agree with Part I?
2	Number of Echo Request ICMP packets: Number of Echo Reply ICMP packets: Does the result agree with Part I?
3	Number of bytes of data carried by each ICMP packet: Does the result agree with Part I?
4	Difference between the time the first Echo message was sent and the first reply message was received:
5	Fields that are **same** in Echo Request and Echo Reply: Reason:
6	Fields that are **different** in Echo Request and Echo Reply: Reason:

Report Submission Requirements

- Provide a screenshot of the `ping` command execution from the Command Prompt.
- Include a screenshot of the Wireshark capture window filtered with `icmp`.
- Submit the completed **Ping – Part I** observation table with all relevant data filled in.
- Submit the completed **Ping – Part II** observation table with all relevant data filled in.