AMITY SCHOOL OF ENGINEERING & TECHNOLOGY

DATA COMMUNICATION & COMPUTER NETWORK LAB

LABWORK – 02

(Experiment: Packet Capture and Analysis Using Wireshark)

COURSE NAME: DCCN Lab

COURSE CODE: CSE2306

DEPARTMENT: Computer Science & Engineering

FACULTY NAME: Dr. Sarang Maruti Patil

SUBMITTED BY

STUDENT NAME:

ENROLLMENT NUMBER:

CLASS:

SEMESTER:

DATE OF SUBMISSION:

Aim:

Experiment: Packet Capture and Analysis Using Wireshark

Objective:

To capture and analyze network packets using the **Wireshark** tool and understand the working of basic protocols like **ICMP** through a **ping operation**.

Tools Required:

- A computer with an internet connection
- **Wireshark** installed (Download: https://www.wireshark.org)

Theory:

Introduction

In computer networks, data is transmitted in the form of **packets**. To understand how data travels through a network and how different protocols operate, we need to observe and analyze these packets. **Wireshark** is a powerful and widely used **network protocol analyzer** that allows users to capture, inspect, and analyze data packets flowing over a network in real time.

What is Wireshark?

Wireshark is an open-source packet analysis tool that captures the traffic flowing over a network and displays detailed protocol information. It supports hundreds of protocols, including TCP, UDP, HTTP, DNS, ARP, and ICMP.

Key features include:

- Real-time packet capturing
- Protocol decoding and filtering
- Deep packet inspection
- Exporting and saving captured files (.pcap format)

Importance of Packet Analysis

Packet analysis helps in:

- Network troubleshooting
- Performance monitoring
- Security auditing
- Protocol behavior analysis
- Educational understanding of network communication

Internet Control Message Protocol (ICMP)

The **ICMP** protocol is used by network devices to send control messages, such as **ping** requests and replies. It is primarily used to test network connectivity between two devices.

Types of ICMP Messages:

- **Type 8 (Echo Request):** Sent by the source to test connectivity.
- **Type 0 (Echo Reply):** Sent by the destination as a response to the Echo Request.

The ping command uses ICMP to check if a host is reachable and how long the response takes.

Packet Structure in ICMP (as seen in Wireshark)

A captured ICMP packet typically includes:

- **Ethernet Header** (Layer 2)
- **IP Header** (Layer 3)
- **ICMP Header** (Layer 4)
    - Type (Request or Reply)
    - Code (0 for normal ping)
    - Checksum (for error checking)
    - Identifier and Sequence Number (to match requests and replies)

◆ Filters in Wireshark

To narrow down traffic, Wireshark provides a filter bar to view specific types of packets:

- icmp – to filter ICMP traffic (used by ping)
- dns – for domain name lookups
- http – for web browsing traffic

Use Case: Ping with Wireshark

By performing a ping to a known IP or domain (e.g., google.com) and using Wireshark to observe the packets:

- **ICMP Echo Request** packets are sent from your PC to the server.

- **ICMP Echo Reply** packets are sent back by the server.

Wireshark shows these in real time, helping students understand how the ping command works at the protocol level.

Procedure

Step 1: Start Wireshark

- Open the Wireshark application.
- Select your active network interface (e.g., Ethernet, Wi-Fi).
- Click **Start** to begin capturing packets.

Step 2: Generate Network Traffic (Ping)

- Open the **Command Prompt (Windows)** or **Terminal (Linux/Mac)**.
- Type the following command:

  ```
  ping google.com
  ```

  This sends ICMP Echo Request and receives Echo Reply packets.

Step 3: Apply Filter in Wireshark

- In the top filter bar, type:

Step 4: Analyze the Packets

- Click on any **ICMP Echo Request** or **Echo Reply** packet.
- Expand the following protocol layers:
  - **Internet Protocol Version 4 (IPv4)**
  - **Internet Control Message Protocol**
- Observe fields like:
  - Source IP
  - Destination IP
  - Type (Echo Request = 8, Echo Reply = 0)
  - Checksum
  - Identifier and Sequence Number

Observation Table

S.No	Packet Type	Source IP	Destination IP	ICMP Type	Description
1	Echo Request	192.168.1.10	8.8.8.8	8	Ping sent
2	Echo Reply	8.8.8.8	192.168.1.10	0	Ping response

Result

The ICMP Echo Request and Echo Reply packets were successfully captured and analyzed using Wireshark. The packet headers showed details such as IP addresses, ICMP types, and identifiers.