Experiment Title: Network Packet Capture and Analysis using Wireshark

Objective:

- To understand the structure of network packets.
- To capture and analyze different types of network traffic using Wireshark.
- To study the behavior of protocols such as HTTP, DNS, TCP, UDP, and ICMP.

Requirements:

- A computer with internet access
- Wireshark installed (latest version recommended)
- Basic understanding of TCP/IP protocol suite

Theory:

Wireshark is a network protocol analyzer that lets you capture and interactively browse traffic running on a computer network. It provides detailed information about each packet including protocol type, source and destination IP, ports, flags, etc.

Common Protocols:

- **HTTP** – HyperText Transfer Protocol
- **DNS** – Domain Name System
- **TCP/UDP** – Transport layer protocols
- **ICMP** – Internet Control Message Protocol

Procedure:

Part A: Capturing Packets

1. Open **Wireshark**.
2. Select the correct **network interface** (e.g., Ethernet or Wi-Fi).
3. Click **"Start Capture"**.

4. Open a browser and visit a few websites like www.google.com, www.wikipedia.org.
5. Open a command prompt and try:
    - ping www.google.com
    - nslookup www.google.com
6. Let the capture run for 1-2 minutes, then click **"Stop"** in Wireshark.

Part B: Analysing Packets

1. HTTP Analysis

- Apply filter: http
- Locate an HTTP GET or POST request.
- Right-click → Follow → HTTP stream.

2. DNS Analysis

- Apply filter: dns
- Find queries and responses.
- Note the domain names and resolved IPs.

3. TCP/UDP Traffic

- Apply filters: tcp and udp
- Observe 3-way handshake: SYN, SYN-ACK, ACK.
- View TCP sequence and acknowledgment numbers.

4. ICMP Analysis

- Filter: icmp
- Analyze echo requests and replies (from ping command).

Observations:

Record the following:

Protocol	**Source IP**	**Destination IP**	**Info (e.g., Request Type, Flags)**
HTTP	192.168.1.10	142.250.190.78	GET /index.html HTTP/1.1
DNS	192.168.1.10	8.8.8.8	https://search.brave.com/search?q=the+importance+of+WHOIS+data+in+VAPT.
TCP	192.168.1.10	142.250.190.78	Flags: SYN, Seq=0, Win=64240
ICMP	192.168.1.10	192.168.1.1	Echo (ping) request id=0x0001, seq=1/256

Result:

Thus we successfully used wireshark for understanding behavior of different network protocols.

Theory Questions:

1. What is Wireshark used for?
2. How can you filter packets by protocol?
3. What is the purpose of a TCP handshake?
4. What's the difference between TCP and UDP?
5. What does the nslookup command do?
