Practical: Capture and Analyze Network Traffic Using Wireshark

Aim: To capture live network packets and identify basic network protocols using Wireshark.

Apparatus/Requirements:

1. Computer System
2. Internet Connection
3. Wireshark Software
4. Web Browser

Theory:

Wireshark is a network protocol analyzer used to capture and analyze packets of data transmitted over a network. It helps in understanding how communication occurs between different devices and identifies protocols such as DNS, TCP, HTTP, HTTPS, and ICMP.

Procedure:

1. Install and open Wireshark software.
2. Select the active network interface (Wi-Fi/Ethernet).
3. Click on Start to begin packet capturing.
4. Open any website to generate network traffic.
5. Use command prompt and type: ping google.com
6. Allow capture for 60 seconds.
7. Stop the packet capture.
8. Apply filters such as DNS, TCP, HTTP, ICMP.
9. Observe different protocols in the captured packets.
10. Save the captured file in .pcap format.

Observation Table:

Protocol	Packet Details
DNS	Used for domain name resolution
TCP	Reliable communication between devices
HTTP	Web data transfer
HTTPS	Secure web data transfer
ICMP	Ping request and reply

Filters Used:

dns

tcp

http

https

icmp

Result:

Live network traffic was successfully captured using Wireshark. Different protocols such as DNS, TCP, HTTP, HTTPS, and ICMP were identified.

Precautions:

1. Ensure proper internet connectivity.
2. Select correct network interface.
3. Do not capture for a long time unnecessarily.
4. Apply appropriate filters.

Viva Questions:

1. What is Wireshark?
2. What is DNS protocol?
3. What is TCP?
4. What is ICMP?
5. What is HTTP and HTTPS?