Task 5: Capture and Analyze Network Traffic Using Wireshark

Author: Robith Abraham
Date: 2025-09-29
Tool: Wireshark

Objective:

The objective of this task is to capture live network packets using Wireshark and identify at least three different protocols (e.g., HTTP, DNS, TCP, ICMP) to understand basic network communication.

Tools Used:

Wireshark (Free, Open Source)

Procedure:

1. Installed Wireshark on the system with required drivers (Npcap on Windows).
2. Opened Wireshark and selected the active network adapter (Wi-Fi).
3. Started live capture by clicking the shark fin icon.
4. Generated traffic: - Opened a browser and visited example.com (created HTTP and DNS traffic).
- Used 'ping 8.8.8.8' to generate ICMP traffic.
- Observed TCP handshakes when establishing connections.
5. Stopped capture after ~1 minute.
6. Applied protocol filters (dns, http, tcp, icmp) to analyze packets.
7. Saved capture file as Task5_Wireshark_Capture.pcap.
8. Prepared findings report with identified protocols.

Findings:

The following protocols were identified:

- **DNS (Domain Name System):** Used for resolving example.com to its IP.
- **HTTP (Hypertext Transfer Protocol):** Used for web traffic when accessing a website.
- **TCP (Transmission Control Protocol):** Ensures reliable communication with the server.
- **ICMP (Internet Control Message Protocol):** Observed during ping commands.

Protocol	Source IP	Destination IP	Description
DNS	192.168.1.10	8.8.8.8	DNS query for example.com
HTTP	192.168.1.10	93.184.216.34	GET request for web page
TCP	192.168.1.10	93.184.216.34	TCP 3-way handshake observed
ICMP	192.168.1.10	8.8.8.8	Ping echo request and reply observed

Conclusion:

The packet capture demonstrated multiple protocols in action. Using Wireshark filters made it possible to isolate and analyze each protocol. This task improved understanding of how data flows between clients and servers and the role of different network protocols.