**TASK-5**

**Capture and Analyze Network Traffic Using Wireshark.**

**1. Objective**

Capture live network packets and identify basic protocols and traffic types.

**2. Tools Used**

* Wireshark (Free network protocol analyzer)

**3. Methodology**

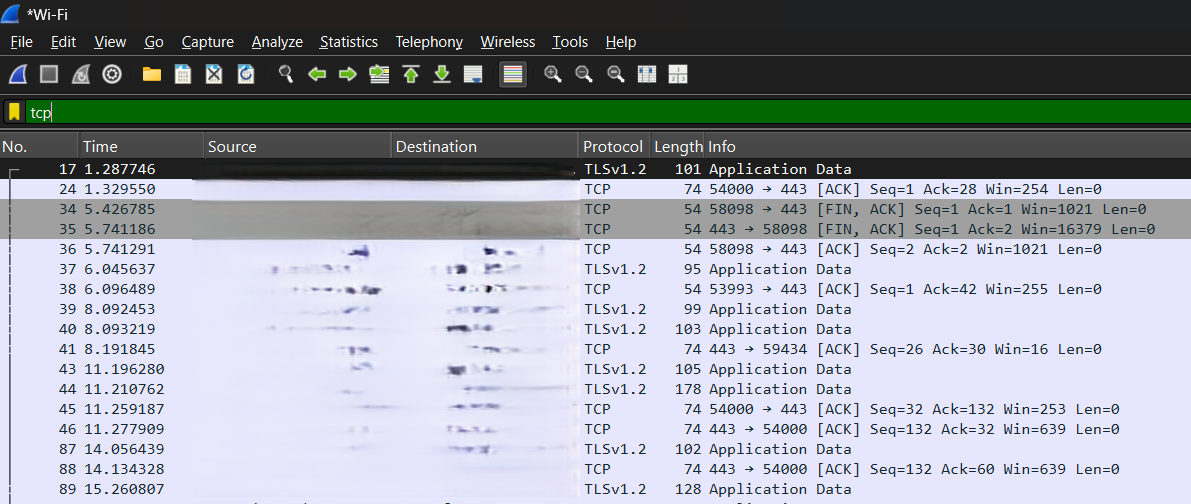
* Installed Wireshark on my computer.
* Started capturing packets on my active network interface (Wi-Fi/Ethernet).
* Generated traffic by browsing websites and pinging a server.
* Stopped capture after approximately 1 minute.
* Applied protocol filters (http, dns, tcp) in Wireshark to analyze traffic.
* Saved the capture as a .pcap file.
* Anonymized the capture to protect my IP address.

**4. Screenshots**

**A screenshot of a computer

AI-generated content may be incorrect.**

Screenshot-1

****

Screenshot-2

**A screenshot of a computer

AI-generated content may be incorrect.**

Screenshot-3

**A screenshot of a computer

AI-generated content may be incorrect.**

Screenshot-4

Example:

* Screenshot 1: HTTP filter applied in Wireshark.
* Screenshot 2: TCP filter applied in Wireshark.
* Screenshot 3: TLS filter applied in Wireshark.
* Screenshot 3: ICMP filter applied in Wireshark.

**5. Protocols Identified**

* **HTTP (Hypertext Transfer Protocol)** – Used for web communication when browsing websites.
* **TCP (Transmission Control Protocol)** – Ensures reliable delivery of packets between client and server.
* **TLS (Transport Layer Security)** – Provides encryption and security for HTTPS traffic.
* **ICMP (Internet Control Message Protocol)** – Used for diagnostic messages such as ping requests and replies.

6. Observations

* HTTP packets were captured, showing unencrypted web traffic requests and responses.
* TCP packets formed the backbone of communication, handling connection establishment and reliable transmission.
* TLS packets indicated secure HTTPS connections, ensuring encrypted data exchange with websites.
* ICMP traffic was seen when performing network diagnostics (e.g., ping), confirming connectivity.
* Anonymization was applied to the .pcap file, so IP addresses are hidden, but protocol-level insights remain visible.

**7. Conclusion**

The packet capture exercise using Wireshark successfully demonstrated how to collect and analyze live network traffic. Multiple protocols — HTTP, TCP, TLS, and ICMP — were identified, each serving different purposes such as web communication, secure transmission, and connectivity testing. By applying protocol filters, it became easier to isolate and study specific traffic types.

NOTE:

The .pcap file provided has been anonymized to protect sensitive information like IP addresses, while screenshots clearly show the analysis steps and results. Overall, this task improved hands-on skills in packet analysis and built awareness of commonly used network protocols.