**Task 5 :Wireshark Network Analysis Report**

**Setup and Traffic Capture**

* **Tool Used:** Wireshark
* **Interface:** Ethernet / Wi-Fi (depending on system)
* **Traffic Generation:** Opened a browser and visited example.com, then ran ping google.com
* **Capture Duration:** 1 minute
* **Result:** 500+ packets captured

**Filtering by Protocol**

Using Wireshark display filters:

| **Filter** | **Protocol Name** | **Description** |
| --- | --- | --- |
| http | HTTP | Web traffic (clear text) |
| dns | DNS | Domain name resolution |
| tcp | TCP | Transport layer traffic |

**Identified Protocols in the Capture**

**1. HTTP (HyperText Transfer Protocol)**

* **Purpose:** Used to load web pages
* **Packets Observed:** GET request to example.com, HTTP 200 OK response
* **Port:** 80 (clear text)
* **Info:** Included headers like Host, User-Agent, Accept

**2. DNS (Domain Name System)**

* **Purpose:** Resolves domain names to IP addresses
* **Packets Observed:** A query for google.com, response with multiple IPs
* **Port:** 53 (UDP)
* **Info:** Standard queries and responses

**3. TCP (Transmission Control Protocol)**

* **Purpose:** Manages reliable data transmission
* **Packets Observed:** TCP handshakes, acknowledgments
* **Ports:** 443, 80, 53, etc.
* **Info:** SYN, ACK, FIN flags were visible in the handshake and termination phases

**Others possibly found:**

* **ICMP:** Detected during ping google.com
* **TLSv1.3:** For encrypted HTTPS traffic

**Exported Packet Capture**

* **Filename:** traffic\_capture.pcap
* **Export Method:** File → Export Specified Packets → Save as .pcap

*Let me know if you’d like an example .pcap file generated for training.*

**Summary of Findings**

**📈 Traffic Overview:**

* 500+ packets captured in 1 minute
* Mix of TCP, DNS, and HTTP packets observed
* HTTPS traffic present, but encrypted (TLS handshake visible)
* Some ICMP packets visible from ping

**🔍 Key Packet Insights:**

| **Protocol** | **Key Fields** | **Notes** |
| --- | --- | --- |
| HTTP | Method: GET, Status: 200 OK | Web request to example.com |
| DNS | Query: google.com, Response: IP addresses | Domain resolution in action |
| TCP | Flags: SYN, ACK, FIN | Connection setup and teardown |

**📌 Conclusion and Learnings**

* **Wireshark** provides powerful filtering and inspection tools for protocol-level traffic analysis.
* Traffic types such as **DNS** and **HTTP** can reveal a lot in plaintext unless encrypted.
* **TCP** flags help track session behavior and detect issues or intrusions.
* **Exported .pcap files** are essential for offline analysis, replay, or collaboration.