**Moulik Tammana**

**Q2. Use Wireshark to capture and analyse DNS, TCP, UDP traffic and packet header, packet flow, options and flags.**

**Structure of a Packet Header:**

**1.Ethernet Header (Data Link Layer - Layer 2)**

* **Destination MAC Address:** The receiver’s MAC address.
* **Source MAC Address:** The sender’s MAC address.
* **EtherType:** Identifies the type of payload (e.g., IPv4, IPv6).

**2.IP Header (Network Layer - Layer 3)**

* **Version:** IPv4 (4) or IPv6 (6).
* **Header Length:** Length of the IP header.
* **Source IP Address:** The sender’s IP.
* **Destination IP Address:** The receiver’s IP.
* **Time to Live (TTL):** Limits the packet's lifetime.
* **Protocol:** Identifies the transport layer protocol (TCP = 6, UDP = 17).
* **Checksum:** Error-checking value.

**3.TCP Header (Transport Layer - Layer 4)**

For TCP packets:

* **Source Port & Destination Port:** Identifies applications.
* **Sequence Number:** Tracks packet order.
* **Acknowledgment Number:** Confirms received packets.
* **Flags:** Controls connection behavior.

**SYN:** Initiates a connection.

**ACK:** Acknowledges a packet.

**FIN:** Ends a connection.

**RST:** Resets a connection.

**PSH:** Pushes data immediately.

**URG:** Marks urgent data.

* **Window Size:** Controls flow of data.
* **Checksum:** Error-checking mechanism.

**4.UDP Header (Transport Layer - Layer 4)**

For UDP packets:

* **Source & Destination Ports:** Identifies applications.
* **Length:** Packet size.
* **Checksum:** Integrity check.

**5.DNS Header (Application Layer - Layer 7)**

For DNS packets:

* **Transaction ID:** Unique identifier for queries.
* **Flags:** Request/response, recursion.
* **Questions & Answers:** Query type (A, AAAA, CNAME).
* **TTL:** How long the response is valid.







