4. In wireshark locate an IPv6 packet and discuss the header present.

➢ When analyzing IPv6 packets in Wireshark, you will encounter several headers that are part of the IPv6 protocol suite. These headers provide important information about the packet's source, destination, payload, and other characteristics. Below is a detailed discussion of the headers you will see when locating an IPv6 packet in Wireshark:

A. Ethernet Header

- **Destination MAC Address**: The hardware address of the destination device.
- **Source MAC Address**: The hardware address of the source device.
- **EtherType**: Indicates the protocol encapsulated in the payload. For IPv6, this value is typically 0x86DD.

B. IPv6 Header

The IPv6 header is the primary header for IPv6 packets and includes the following fields:

- **Version**: (4 bits) Indicates the IP version (6 for IPv6).
- **Traffic Class**: (8 bits) Used for packet priority (similar to the Type of Service field in IPv4).
- **Flow Label**: (20 bits) Used to label packets of a specific flow for special handling.
- **Payload Length**: (16 bits) The length of the payload, including any extension headers.
- **Next Header**: (8 bits) Identifies the type of header following the IPv6 header (similar to the Protocol field in IPv4). This could be

a transport-layer protocol (e.g., TCP or UDP) or an IPv6 extension header.

- **Hop Limit**: (8 bits) Decrements by one at each hop; the packet is discarded when it reaches zero (similar to the TTL field in IPv4).
- **Source Address**: (128 bits) The IPv6 address of the packet's origin.
- **Destination Address**: (128 bits) The IPv6 address of the packet's intended recipient.

C. IPv6 Extension Headers

IPv6 allows for optional extension headers to be included between the IPv6 header and the payload. These headers provide additional functionality and information. Common extension headers include:

- **Hop-by-Hop Options Header**: Contains options that need to be examined by every router along the packet's path.
- **Destination Options Header**: Contains options that need to be examined only by the destination node(s).
- **Routing Header**: Lists one or more intermediate nodes to be visited on the way to the packet's destination.
- **Fragment Header**: Used for packet fragmentation and reassembly.
- **Authentication Header (AH)**: Provides packet integrity and authentication.
- **Encapsulating Security Payload (ESP) Header**: Provides confidentiality, data integrity, and authentication.

D. Transport Layer Headers

The transport layer headers follow the IPv6 and any extension headers. The most common transport layer protocols are:

- **TCP (Transmission Control Protocol)**:
  - **Source Port**: The port number of the sender.
  - **Destination Port**: The port number of the receiver.
  - **Sequence Number**: Used to ensure correct data reassembly.
  - **Acknowledgment Number**: Indicates the next sequence number expected by the sender.
  - **Data Offset**: The size of the TCP header.
  - **Flags**: Control flags such as SYN, ACK, FIN, etc.
  - **Window Size**: Flow control information.
  - **Checksum**: Used for error-checking the header and payload.
  - **Urgent Pointer**: Indicates if any data is urgent.
- **UDP (User Datagram Protocol)**:
  - **Source Port**: The port number of the sender.
  - **Destination Port**: The port number of the receiver.
  - **Length**: The length of the UDP header and payload.
  - **Checksum**: Used for error-checking the header and payload.