Version

This field specifies the version of the IP protocol being used. It helps routers and hosts to understand how to interpret the packet. In my packet the value is 4, which means the packet is using IPv4

Header Length

Specifies the length of the IP header in 32-bit words. This allows the receiving device to know where the actual data begins, as the header length can vary. In my packet the header size is 20 bytes, so the value is 5 (20 bytes / 4 = 5 words).

Type of Service

Indicates the quality of service desired for this packet. It can be used for prioritizing certain types of traffic, such as VoIP (Voice over IP), video, or other real-time applications. My ToS value is 0x00 in hexadecimal, which translates to a decimal value of 0.

Total Length

Specifies the total size of the IP packet, including both the header and the data, in bytes. This allows the recipient to determine the full size of the packet and process it correctly. My total length is 61 so it is 61 bytes long

Identification

Used to uniquely identify fragments of a packet. When a large packet is fragmented into smaller pieces (for transmission over networks with size limits), each fragment carries the same identification number so they can be reassembled at the destination.

Flags

Used to control or provide information about the fragmentation of packets. It consists of three flags. The first bit is reserved (always 0). The second bit is the DF (Don't Fragment) flag, which indicates that the packet should not be fragmented. The third bit is the MF (More Fragments) flag, which indicates that more fragments are coming.

Fragment Offset

Indicates the position of the fragment within the original packet. It is used to help reassemble fragmented packets in the correct order at the destination.

Time to Live (TTL) (8 bits)

Sets the maximum number of hops (routers) the packet can pass through before being discarded. Each router that forwards the packet decrements this value. If it reaches zero, the packet is discarded. This prevents infinite loops. My packet has a Time To Live value of 128 which means the packet can go through 128 routers before being dropped.

Protocol

Identifies the protocol used in the data portion of the packet, such as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). This tells the recipient how to interpret the data portion of the packet. My packet has a Protocol value of 17 which indicates that the data is using UDP

Header Checksum

Provides error-checking for the IP header to ensure data integrity during transmission. It helps detect corruption in the header during the packet's transit. If the checksum is incorrect, the packet is discarded.

Source IP Address

Specifies the IP address of the device that sent the packet. This is used for routing responses back to the sender. 149.153.106.64

Destination IP Address

Specifies the IP address of the intended recipient. Routers use this field to forward the packet to the correct destination. 10.199.10.10

Options

his field is optional and can be used for various special options like security settings, timestamps, or source routing (where the sender specifies the path the packet should take). This field increases the header length if used.

Data

The payload of the packet, which contains the actual data being sent. This is the application data or higher-layer protocol data (like TCP, UDP, or ICMP). The size of this field is determined by the Total Length minus the header length.