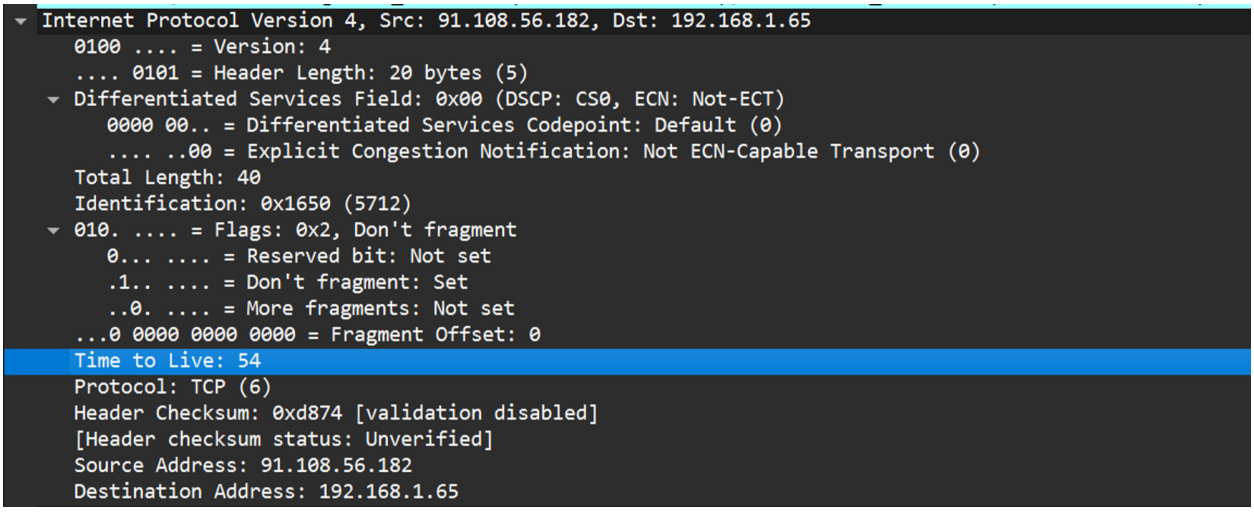
# Wireshark analysis of IPv4




In Wireshark, the term "IPv4 statistics" refers to statistical data about IPv4 (Internet Protocol version 4) packets in a network capture. One of the essential protocols used at the network layer to address and route packets over the Internet and many private networks is IPv4.

The IPv4 header is a critical part of the IPv4 packet structure, containing important information required for routing and delivering packets across an IP network. Below is a breakdown of the IPv4 header fields and their functions:

## IPv4 Header Format

1. **Version (4 bits)**:
   - Indicates the IP version. For IPv4, this value is 4.
2. **IHL (Internet Header Length) (4 bits)**:
   - Specifies the length of the IP header in 32-bit words. The minimum value is 5 (20 bytes), and the maximum is 15 (60 bytes).
3. **Type of Service (ToS) / Differentiated Services (DS) (8 bits)**:

- Used for specifying the quality of service and priority of the packet. It includes fields like DSCP (Differentiated Services Code Point) and ECN (Explicit Congestion Notification).

4. **Total Length (16 bits)**:
    - Specifies the total length of the IP packet, including the header and data, in bytes. The minimum length is 20 bytes, and the maximum is 65,535 bytes.
5. **Identification (16 bits)**:
    - Used to identify fragments of the original IP packet. Each packet sent from the source has a unique identification value.
6. **Flags (3 bits)**:
    - Controls or identifies fragments. It consists of:
        - Reserved bit (must be zero)
        - Don't Fragment (DF) bit
        - More Fragments (MF) bit
7. **Fragment Offset (13 bits)**:
    - Indicates the position of a fragment in the original IP packet. Measured in 8-byte units.
8. **Time to Live (TTL) (8 bits)**:
    - Specifies the maximum number of hops (routers) the packet can traverse. Decremented by 1 by each router; when it reaches 0, the packet is discarded.
9. **Protocol (8 bits)**:
    - Indicates the protocol used in the data portion of the IP packet. Common values include:
        - 1: ICMP (Internet Control Message Protocol)
        - 6: TCP (Transmission Control Protocol)
        - 17: UDP (User Datagram Protocol)

10. **Header Checksum (16 bits)**:
    - A checksum of the header to detect corruption in transit.
11. **Source Address (32 bits)**:
    - The IP address of the sender.
12. **Destination Address (32 bits)**:
    - The IP address of the receiver.
13. **Options (variable length, if any)**:
    - Optional fields for various purposes, such as security, timestamping, etc. If used, they increase the header length.
14. **Padding (variable length, if any)**:
    - Added to ensure the header length is a multiple of 32 bits.