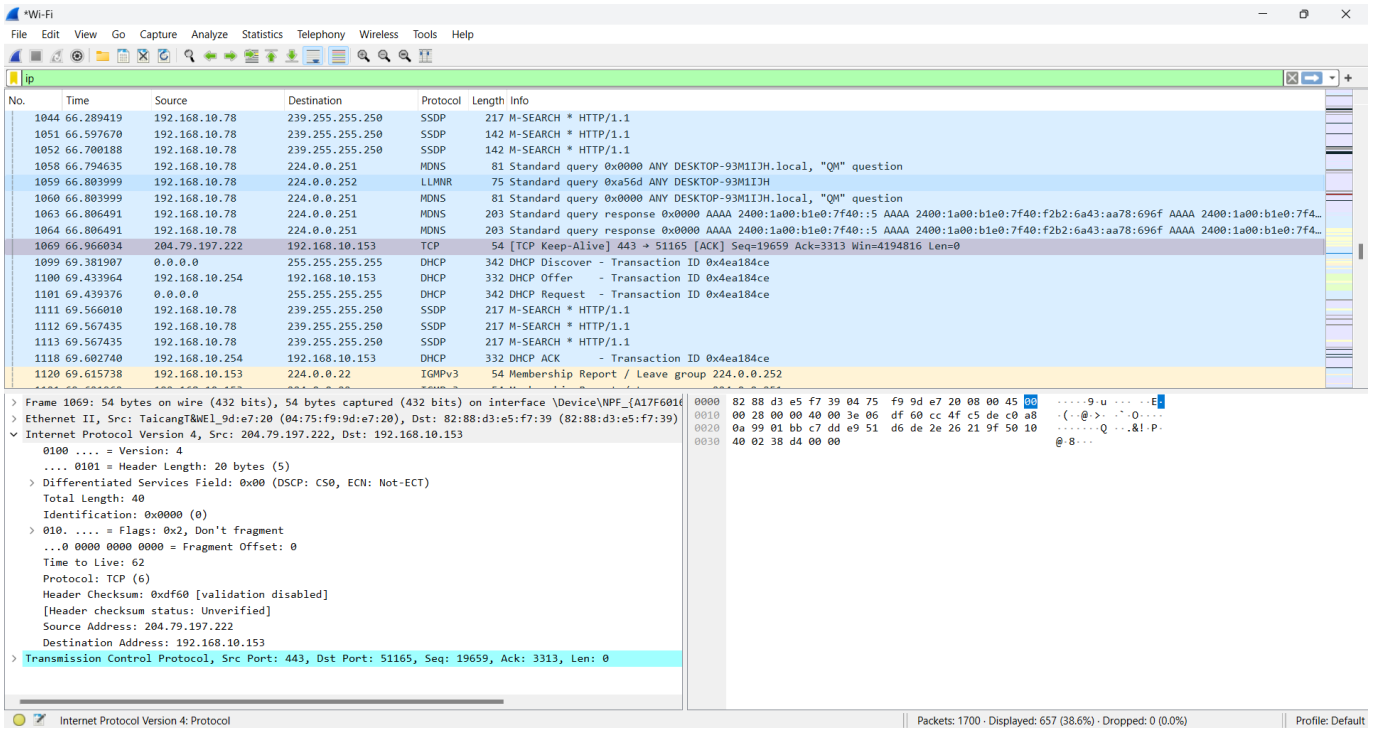
# 1. Capture an ip packet on Wireshark , what is the value of each of the header fields. Explain why the value is what it is.




## Analyzing IP Header Fields

Let's break down the IP header fields and their possible values, using a packet.

1. **Version**:
    - **Value**: 4 or 6
    - **Explanation**: Indicates the IP version. IPv4 is the most common and will show a value of 4. IPv6 packets will show a value of 6.
2. **Header Length**:
    - **Value**: Typically 20 bytes (5 in the header length field, indicating 5*4 = 20 bytes)
    - **Explanation**: Specifies the length of the IP header. The value is in 32-bit words, so a minimum value of 5 means 20 bytes.
3. **Type of Service (ToS)**:
    - **Value**: Varies

- **Explanation**: Indicates the priority of the packet and the type of service expected. The value can vary depending on the Quality of Service (QoS) needed.

4. **Total Length**:
    - **Value**: Varies
    - **Explanation**: Specifies the total length of the IP packet, including the header and data. The value is given in bytes.
5. **Identification**:
    - **Value**: Varies
    - **Explanation**: A unique value identifying the group of fragments of a single IP datagram.
6. **Flags**:
    - **Value**: 0, 1, or 2
    - **Explanation**: Contains flags such as "Don't Fragment" (DF) and "More Fragments" (MF). The most significant bit is always 0.
7. **Fragment Offset**:
    - **Value**: Varies
    - **Explanation**: Indicates where in the datagram this fragment belongs. It is measured in units of 8 bytes.
8. **Time to Live (TTL)**:
    - **Value**: Typically between 1 and 255
    - **Explanation**: Specifies the maximum time the packet is allowed to remain in the network before being discarded. It decreases by 1 for each hop.
9. **Protocol**:
    - **Value**: E.g., 6 (TCP), 17 (UDP)
    - **Explanation**: Identifies the protocol used in the data portion of the IP datagram.
10. **Header Checksum**:

- **Value**: Varies
- **Explanation**: Used for error-checking the header. It's recalculated and verified at each hop.

11. **Source IP Address**:
    - **Value**: Depends on the sender
    - **Explanation**: The IP address of the originator of the packet.
12. **Destination IP Address**:
    - **Value**: Depends on the recipient
    - **Explanation**: The IP address of the intended recipient.
13. **Options** (if any):
    - **Value**: Optional
    - **Explanation**: May contain various control options. Not always present and typically not used.