Wireshark IP Packet Analysis

Aayush Adhikari

June 23, 2024

Introduction

This report analyzes an IP packet captured using Wireshark, focusing on the structure and content of the IP header. The capture was performed while accessing google.com.

1 Packet Capture

Wireshark Capture Details

```
Frame 1382: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on
    interface en0, id 0
Ethernet II, Src: Apple_77:80:65 (10:bd:3a:77:80:65), Dst: FidaInternet_a3:e8
    :ec (90:61:0c:a3:e8:ec)
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 56555, Dst Port: 53
Domain Name System (query)
```

2 Hexadecimal Data

Captured Packet's Hexadecimal Data

```
0000  90 61 0c a3 e8 ec 10 bd 3a 77 80 65 08 00 45 00
0010  00 3c 28 2b 00 00 40 11 cf 2d c0 a8 01 07 c0 a8
0020  01 01 dc eb 00 35 00 28 cf a1 40 db 01 00 00 01
0030  00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c
0040  65 03 63 6f 6d 00 00 01 00 01
```

3 IP Header Analysis

IP Header (20 bytes)

```
45 00 00 3c 28 2b 00 00 40 11 cf 2d c0 a8 01 07 c0 a8 01 01
```

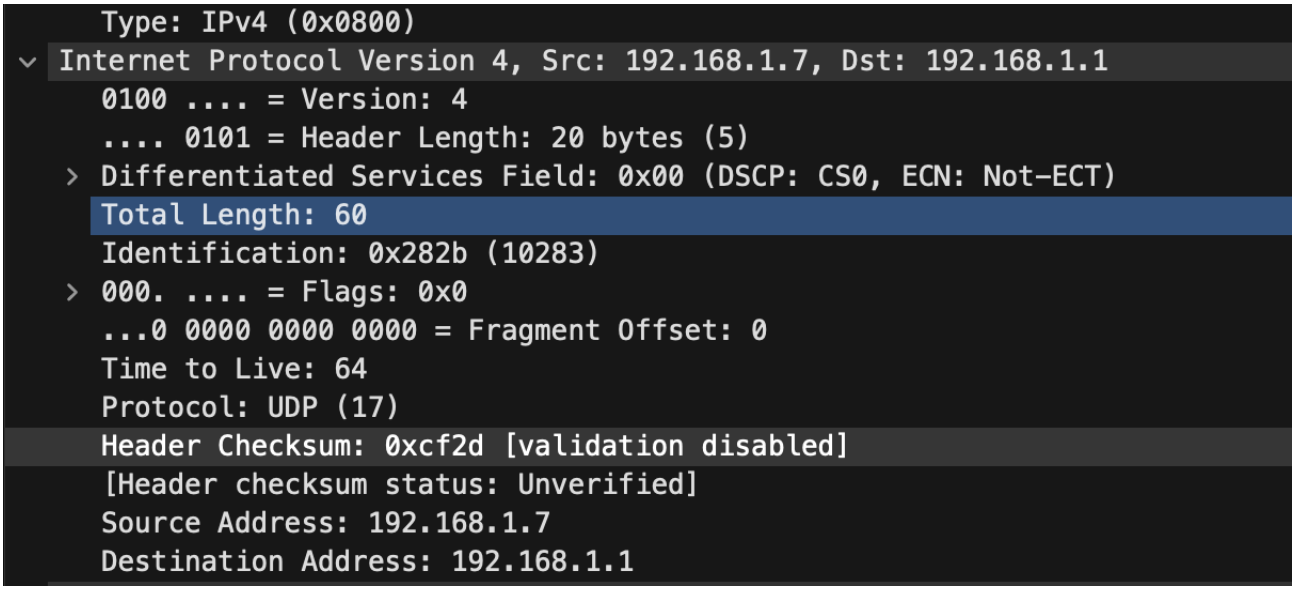

Figure 1: IP header fields in wireshark

Field	Value (Hex)	Value (Decoded)	Explanation
Version	4	4	IPv4
IHL	5	5	Header length 20 bytes
TOS	00	0	No special priority
Total Length	00 3c	60 bytes	Packet size
Identification	28 2b	10283	Packet identifier
Flags & Fragment Offset	00 00	0	No fragmentation
TTL	40	64	Max hops before discard
Protocol	11	17 (UDP)	Next level protocol
Header Checksum	cf 2d	53037	Error checking
Source IP	c0 a8 01 07	192.168.1.7	Source address
Destination IP	c0 a8 01 01	192.168.1.1	Destination address

Table 1: IP Header Fields

4 Explanation of Fields

Field Descriptions

- **Version**: Always 4 for IPv4 packets.
- **IHL (Internet Header Length)**: Measured in 32-bit words. Value 5 means 5 * 4 = 20 bytes.
- **TOS (Type of Service)**: Specifies priority and handling of the packet.
- **Total Length**: Sum of header and payload lengths in bytes.
- **Identification**: Unique identifier for fragments of the same packet.
- **Flags & Fragment Offset**: Control and indicate packet fragmentation.
- **TTL (Time to Live)**: Decremented at each hop, packet is discarded when it reaches 0.
- **Protocol**: Indicates the next level protocol (17 for UDP).
- **Header Checksum**: Error-checking calculated over the entire header.
- **Source/Destination IP**: IP addresses of sender and receiver.

5 Conclusion

Summary

This analysis demonstrates the structure and content of an IPv4 header from a captured DNS query packet. Understanding these fields is crucial for network troubleshooting and protocol analysis.