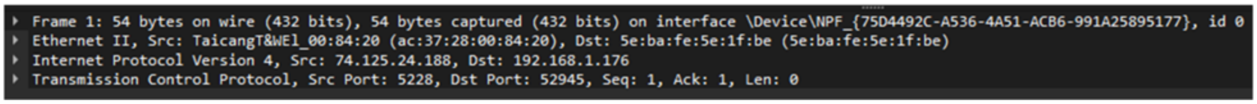
Wireshark IP Packet Analysis

Introduction

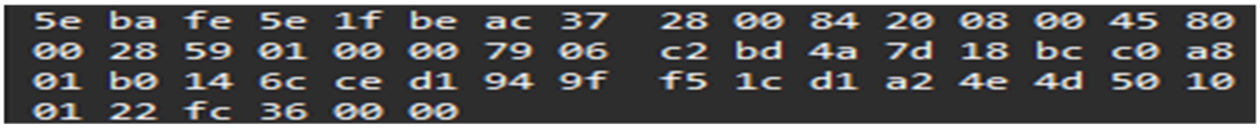
This report analyzes an IP packet captured using Wireshark, focusing on the structure and content of the IP header.

1 Packet Capture



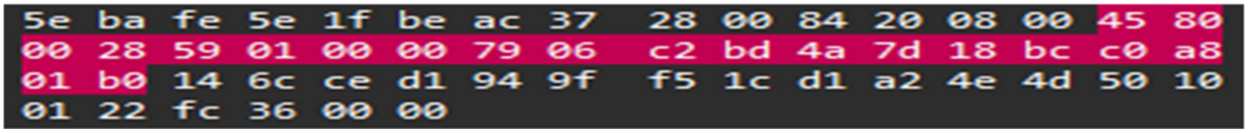
```
▸ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{75D4492C-A536-4A51-ACB6-991A25895177}, id 0
▸ Ethernet II, Src: TaicangT&WEl_00:84:20 (ac:37:28:00:84:20), Dst: 5e:ba:fe:5e:1f:be (5e:ba:fe:5e:1f:be)
▸ Internet Protocol Version 4, Src: 74.125.24.188, Dst: 192.168.1.176
▸ Transmission Control Protocol, Src Port: 5228, Dst Port: 52945, Seq: 1, Ack: 1, Len: 0
```

2 Hexadecimal Data



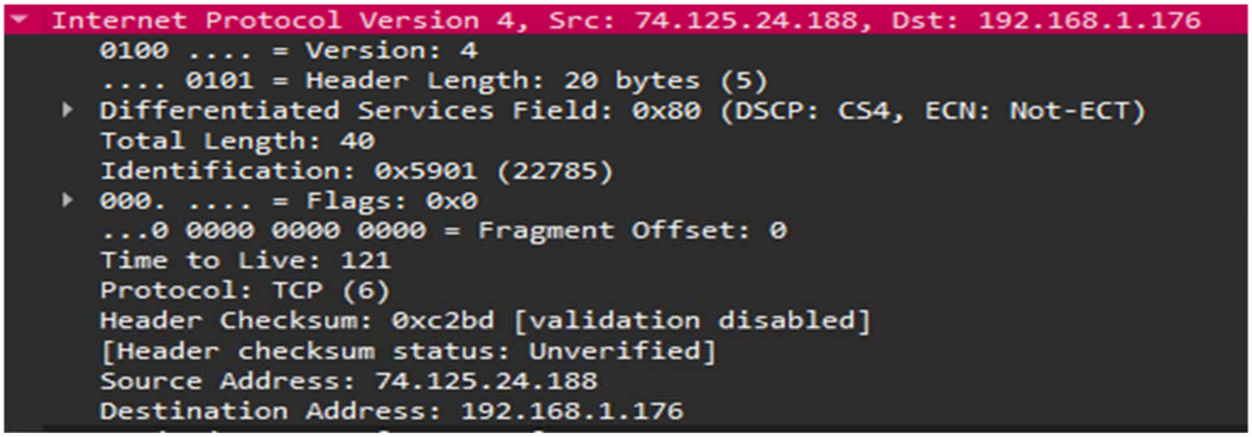
```
5e ba fe 5e 1f be ac 37  28 00 84 20 08 00 45 80
00 28 59 01 00 00 79 06  c2 bd 4a 7d 18 bc c0 a8
01 b0 14 6c ce d1 94 9f  f5 1c d1 a2 4e 4d 50 10
01 22 fc 36 00 00
```

3 IP Header Analysis



```
5e ba fe 5e 1f be ac 37  28 00 84 20 08 00 45 80
00 28 59 01 00 00 79 06  c2 bd 4a 7d 18 bc c0 a8
01 b0 14 6c ce d1 94 9f  f5 1c d1 a2 4e 4d 50 10
01 22 fc 36 00 00
```

4 Wireshark IP packet Analysis



```
▾ Internet Protocol Version 4, Src: 74.125.24.188, Dst: 192.168.1.176
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    ▸ Differentiated Services Field: 0x80 (DSCP: CS4, ECN: Not-ECT)
      Total Length: 40
      Identification: 0x5901 (22785)
    ▸ 000. .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 121
      Protocol: TCP (6)
      Header Checksum: 0xc2bd [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 74.125.24.188
      Destination Address: 192.168.1.176
```

Figure: IP header fields in Wireshark

5 Explanation of each field of IPv4

Field	Value (Hex)	Value (Decoded)	Explanation
Version	4	4	IPv4
IHL	5	5	Header length 20 bytes
TOS	80	128	No special priority
Total Length	00 28	40 bytes	Packet Size
Identification	59 01	22785	Packet Identifier
Flags & Fragment Offset	00 00	0	No fragmentation
TTL	79	121	Max hops before discard
Protocol	06	6 TCP	Next level protocol
Header Checksum	c2 bd	49853	Error checking
Source IP	4a 7d 18 bc	74.125.24.188	Source address
Destination IP	c0 a8 01 b0	192.168.1.176	Destination address

Table: IP Header fields

6 Explanation of Fields

- **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 packets
- **Total Length:** Sum of header and payload lengths in bytes.
- **Identification:** Unique identifier for fragments of the same packet.
- **Flags and Fragment Offset:** Control and indicate packet fragmentation.
- **TTL (Time to Leave):** Decremented at each hop. Packet is discarded when it reaches 0.
- **Protocol:** Indicates the next level protocol (6 for TCP).
- **Header Checksum:** Error-checking calculated over the entire header.
- **Source/Destination IP:** IP addresses of sender and receiver.