

Exp-26. Transport layer protocol header analysis using Wire shark- UDP

The image displays a Wireshark packet capture window titled "Capturing from Wi-Fi". The packet list pane shows a series of packets, including QUIC and DNS traffic. The packet details pane is expanded for a selected packet, showing the following structure:

- Frame 77: 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits) on interface \Device\NPF_{34206...}
- Ethernet II, Src: Intel_13:4c:82 (6c:f6:da:13:4c:82), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
- Internet Protocol Version 4, Src: 192.168.38.29, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 49692, Dst Port: 1900
- Source Port: 49692
- Destination Port: 1900
- Length: 353
- Checksum: 0x8c3c [unverified]
- [Checksum Status: Unverified]
- [Stream index: 0]
- [Stream Packet Number: 1]
- [Timestamps]
- UDP payload (345 bytes)
- Simple Service Discovery Protocol

The packet bytes pane shows the raw hex and ASCII data for the selected packet, starting with 0000 01 00 5e 7f ff fa 6c f6 da 13 4c 82 08 00 45 00.