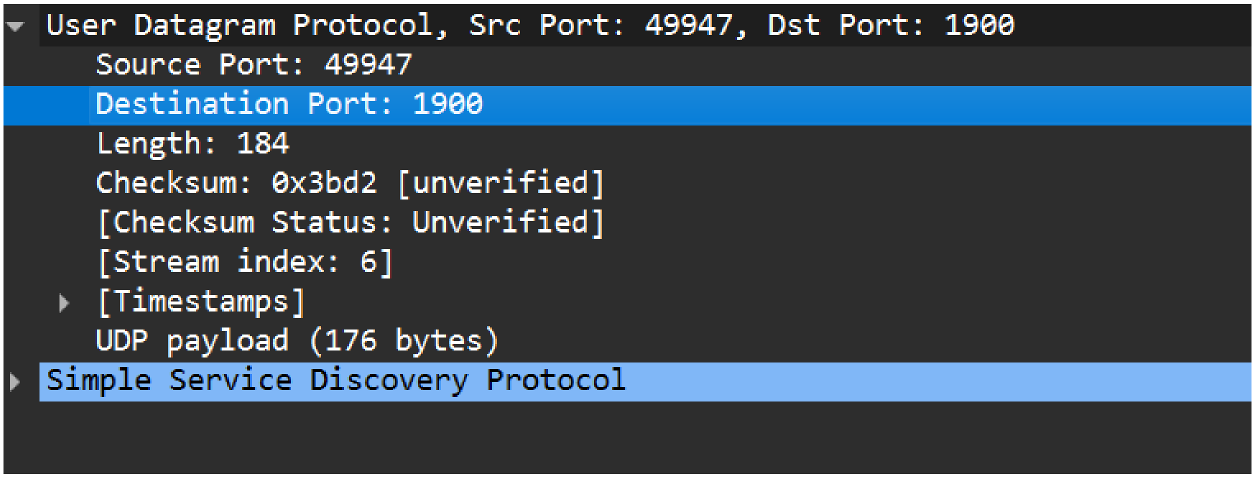
UDP wireshark and analysis



```
▾ User Datagram Protocol, Src Port: 49947, Dst Port: 1900
      Source Port: 49947
      Destination Port: 1900
      Length: 184
      Checksum: 0x3bd2 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 6]
    ▸ [Timestamps]
      UDP payload (176 bytes)
▸ Simple Service Discovery Protocol
```

In, UDP (User Datagram Protocol) is a simpler, connectionless protocol that does not require a handshake to establish a connection and does not guarantee packet delivery, ordering, or error checking. Here's a guide on capturing and analyzing UDP packets in Wireshark:

Capturing UDP Packets

1. **Open Wireshark**: Start Wireshark and select the network interface you want to capture traffic on.
2. **Start Capture**: Click the "Start Capturing Packets" button (the shark fin icon).
3. **Apply Filter**: Use a filter to capture only UDP packets. The filter expression is `udp`.

Analyzing UDP Packets

When you capture UDP packets, you can see detailed information about each packet. Here are the main components of a UDP packet in Wireshark:

Packet Details Pane

- **Frame**: Information about the captured frame, including the frame number and length.
- **Ethernet II**: Ethernet header information, including source and destination MAC addresses.
- **Internet Protocol Version 4 (IPv4) or Version 6 (IPv6)**: IP header information, including source and destination IP addresses.
- **User Datagram Protocol (UDP)**: Detailed UDP header information:
  - **Source Port**: The port number on the source device.
  - **Destination Port**: The port number on the destination device.
  - **Length**: The length of the UDP header and payload in bytes.
  - **Checksum**: Used for error-checking the UDP header and payload.

Common UDP Packet Types

- **DNS**: Domain Name System queries and responses.
- **DHCP**: Dynamic Host Configuration Protocol messages for IP address assignment.
- **SNMP**: Simple Network Management Protocol messages for network management.
- **TFTP**: Trivial File Transfer Protocol messages for simple file transfers.
- **VoIP**: Voice over IP traffic, often using protocols like SIP and RTP.

Following UDP Streams

While UDP is connectionless and does not establish streams in the same way as TCP, Wireshark allows you to follow UDP "conversations":

1. **Select a Packet**: Right-click on a UDP packet and select "Follow" > "UDP Stream".
2. **View the Conversation**: Wireshark will display the conversation between the two endpoints in a separate window.