

# UDP

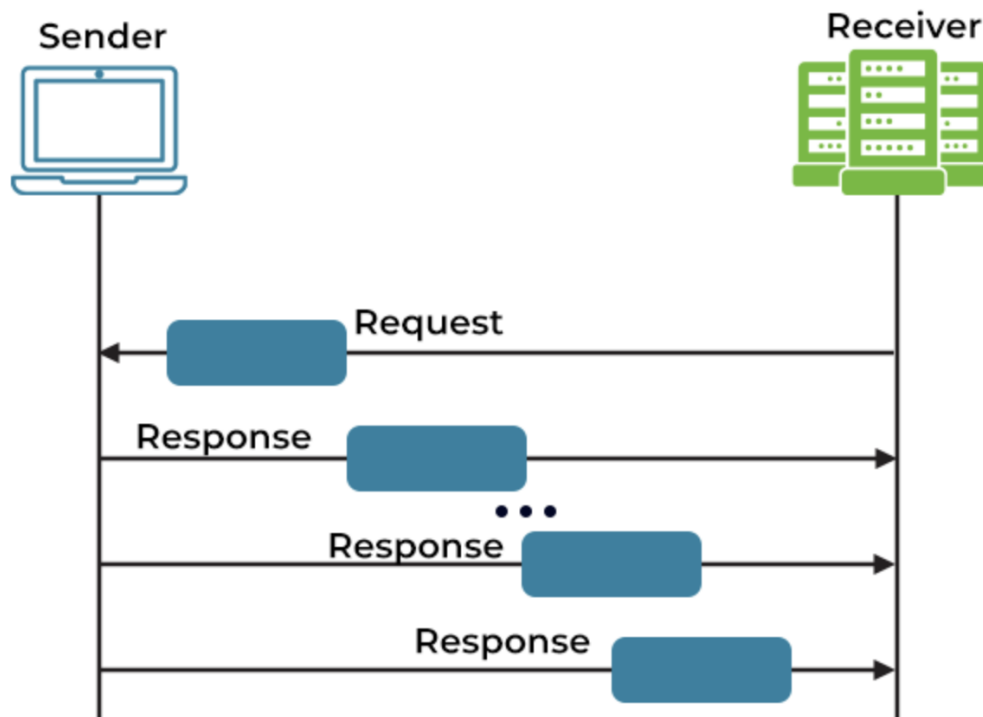
**How many bytes are in the UDP header? its different fields? How are values set? verify in Wireshark.**

Let's first talk about **UDP**

## **User Datagram Protocol**

- a message-oriented communication protocol that allows computing devices and applications to send data over a network
- doesn't verify it's delivery

## FUNCTIONING OF USER DATAGRAM PROTOCOL (UDP)



**UDP enables continuous data transmission (i.e., response) without acknowledging or confirming the connection**

- No connection is established
- directly sends packets to a target computer without establishing a connection first
- doesn't ensure the delivery of data packets from the server
- not concerned whether or not the client receives the data

### **Real-life use cases**

- Real-time applications like broadcasting

- multitasking network traffic

**UDP** wraps datagrams with a **UDP** header, which contains four fields up to eight bytes long.

The fields in the **UDP** header are explained below:

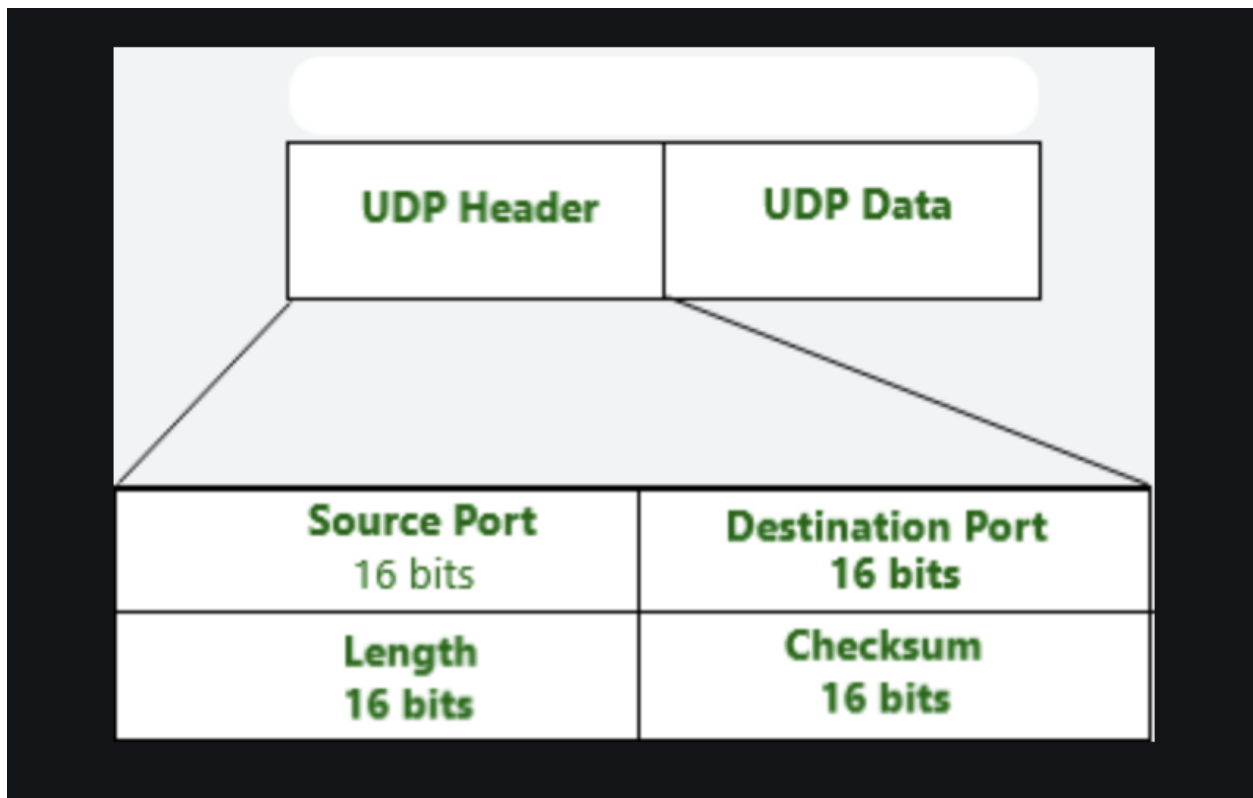
**a) Source port** ( port of device sending the data ) **16bits**

**b) Destination port** ( port of device receiving the data ) **16bits**

UDP port numbers can be from **0 to 65535**

**c) Length** ( specifies the number of bytes comprising the UDP header and the UDP payload data ) **16bits**

**d) Checksum** ( allows the receiving device to verify the integrity of the packet header and payload ) **16bits**



**How are values set?**

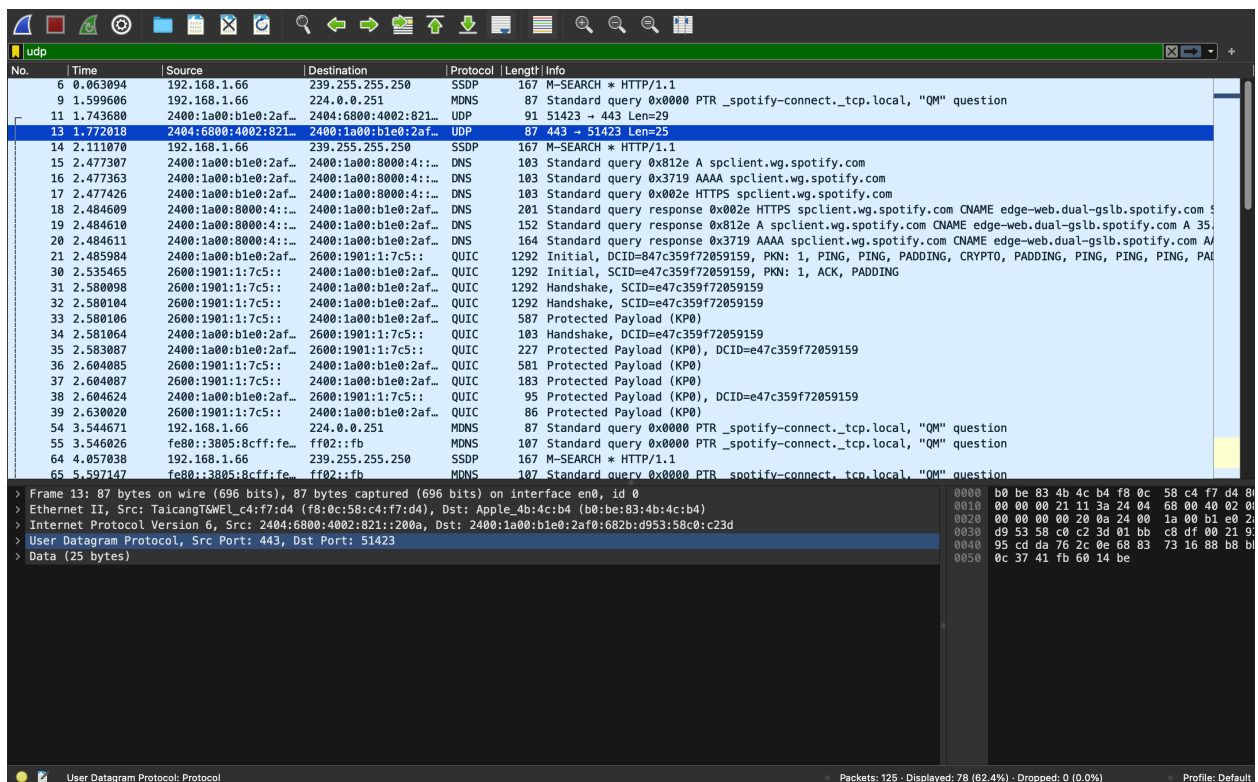
a) **Source port** ( set by applications sending the datagram )

b) **Destination port** ( set by sending applications based on the port number of the receiving applications )

c) **Length** ( calculated by the sending application )

d) **Checksum** ( calculated by the sending application which is used for error checking )

I captured packets on my network interface using Wireshark and obtained the following results:



No.	Time	Source	Destination	Protocol	Length	Info
6	0.063094	192.168.1.66	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
9	1.599606	192.168.1.66	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
11	1.743680	2400:1a00:b1e0:2af...	2404:6800:4002:821...	UDP	91	51423 → 443 Len=29
13	1.772018	2404:6800:4002:821...	2400:1a00:b1e0:2af...	UDP	87	443 → 51423 Len=25
14	2.111070	192.168.1.66	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
15	2.477307	2400:1a00:b1e0:2af...	2400:1a00:8000:4:...	DNS	103	Standard query 0x812e A spclient.wg.spotify.com
16	2.477363	2400:1a00:b1e0:2af...	2400:1a00:8000:4:...	DNS	103	Standard query 0x3719 AAAA spclient.wg.spotify.com
17	2.477426	2400:1a00:b1e0:2af...	2400:1a00:8000:4:...	DNS	103	Standard query 0x002e HTTPS spclient.wg.spotify.com
18	2.484609	2400:1a00:8000:4:...	2400:1a00:b1e0:2af...	DNS	201	Standard query response 0x002e HTTPS spclient.wg.spotify.com CNAME edge-web.dual-gslb.spotify.com
19	2.484610	2400:1a00:8000:4:...	2400:1a00:b1e0:2af...	DNS	152	Standard query response 0x812e A spclient.wg.spotify.com CNAME edge-web.dual-gslb.spotify.com A 35.
20	2.484611	2400:1a00:8000:4:...	2400:1a00:b1e0:2af...	DNS	164	Standard query response 0x3719 AAAA spclient.wg.spotify.com CNAME edge-web.dual-gslb.spotify.com A
21	2.485984	2400:1a00:b1e0:2af...	2600:1901:1:7c5:...	QUIC	1292	Initial, DCID=e47c359f72059159, PKN: 1, PING, PING, PADDING, CRYPTO, PADDING, PING, PING, PING, PING
22	2.535465	2600:1901:1:7c5:...	2400:1a00:b1e0:2af...	QUIC	1292	Handshake, SCID=e47c359f72059159, PKN: 1, ACK, PADDING
31	2.580098	2600:1901:1:7c5:...	2400:1a00:b1e0:2af...	QUIC	1292	Handshake, SCID=e47c359f72059159
32	2.580104	2600:1901:1:7c5:...	2400:1a00:b1e0:2af...	QUIC	587	Protected Payload (KP0)
33	2.580106	2400:1a00:b1e0:2af...	2600:1901:1:7c5:...	QUIC	103	Handshake, DCID=e47c359f72059159
34	2.581064	2400:1a00:b1e0:2af...	2600:1901:1:7c5:...	QUIC	227	Protected Payload (KP0), DCID=e47c359f72059159
35	2.583087	2600:1901:1:7c5:...	2400:1a00:b1e0:2af...	QUIC	581	Protected Payload (KP0)
36	2.604085	2600:1901:1:7c5:...	2400:1a00:b1e0:2af...	QUIC	183	Protected Payload (KP0)
37	2.604087	2600:1901:1:7c5:...	2400:1a00:b1e0:2af...	QUIC	95	Protected Payload (KP0), DCID=e47c359f72059159
38	2.604624	2600:1901:1:7c5:...	2400:1a00:b1e0:2af...	QUIC	86	Protected Payload (KP0)
39	2.630020	2600:1901:1:7c5:...	2400:1a00:b1e0:2af...	QUIC	87	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
54	3.544671	192.168.1.66	224.0.0.251	MDNS	107	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
55	3.546026	fe80::3805:8cfe:f...	ff02::fb	MDNS	167	M-SEARCH * HTTP/1.1
64	4.057038	192.168.1.66	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
65	5.597147	fe80::3805:8cfe:f...	ff02::fb	MDNS	107	Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question

> Frame 13: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface en0, id 0

> Ethernet II, Src: TaicangTWEI\_c4:f7:d4 (f8:0c:58:c4:f7:d4), Dst: Apple\_4b:4c:b4 (b0:be:83:4b:4c:b4)

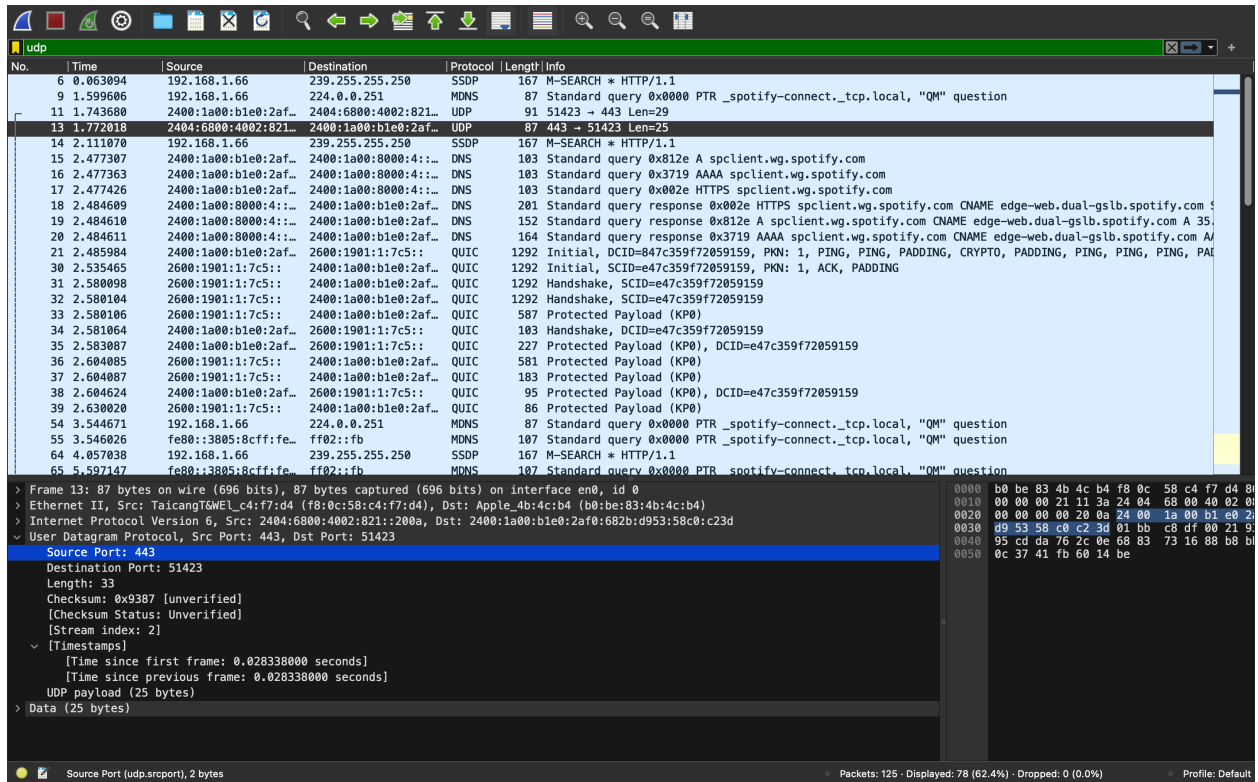
> Internet Protocol Version 6, Src: 2404:6800:4002:821::200a, Dst: 2400:1a00:b1e0:2af0:682b:d953:58c0:c23d

> User Datagram Protocol, Src Port: 443, Dst Port: 51423

> Data (25 bytes)

0000 b0 be 83 4b 4c b4 f8 0c 58 c4 f7 d4 81  
0010 00 00 00 21 11 3a 24 04 68 00 40 02 01  
0020 00 00 00 00 20 0a 24 00 1a 00 b1 e0 2:  
0030 d9 53 58 c0 c2 3d 01 bb c8 df 00 21 9:  
0040 95 cd da 76 2c 0e 68 83 73 16 88 b8 b:  
0050 0c 37 41 fb 60 14 be

User Datagram Protocol: Protocol      Packets: 125 - Displayed: 78 (62.4%) - Dropped: 0 (0.0%)      Profile: Default



In Wireshark, the following is the information about the UDP headers:

- Source port: 443
- Destination port: 51423
- Length: 33bytes
- Checksum: 0x9387 [unverified]
- UDP payload length: 25bytes
- Data: 25bytes