

Lab 6: Analysis of UDP in Wireshark

Lab Title: Analysis of UDP in Wireshark

Name: Muhammad Rizwan Khalid

Regn No: 180459

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix  . : nust.edu.pk
Link-local IPv6 Address . . . . . : fe80::41ab:dcf1:1dd2:f4b2%11
IPv4 Address. . . . . : 10.7.44.55
Subnet Mask . . . . . : 255.255.252.0
Default Gateway . . . . . : 10.7.44.1
```

Objective of this lab:

In this lab, we will analyze the behavior of UDP in detail, determining the number of fields in UDP header, the value in the UDP header fields, and maximum number of bytes in UDP payload, source & destination port numbers etc.

Instructions:

- Read carefully before starting the lab.
- These exercises are to be done individually.
- You are supposed to provide the answers to the questions listed at the end of this document (substantiate your answers with screen shots of your Wireshark captures) and upload the completed report to your course's LMS site.
- Avoid plagiarism by copying from the Internet or from your peers. You may refer to source/text but you must paraphrase the original work.

Background:**1. Introduction to UDP:**

UDP (User Datagram Protocol) is a simple transport layer protocol for client/server network applications based on Internet Protocol (IP). UDP is the main alternative to TCP and one of the oldest network protocols in existence, introduced in 1980. UDP is often used in videoconferencing applications or computer games specially tuned for real-time performance. To achieve higher performance, the protocol allows individual packets to be dropped (with no retries) and UDP packets to be received in a different order than they were sent as dictated by the application.

2. UDP Datagrams:

Lab 6: Analysis of UDP in Wireshark

UDP network traffic is organized in the form of datagrams. A datagram comprises one message unit. The first eight (8) bytes of a datagram contain header information and the remaining bytes contain message data.

A UDP datagram header consists of four (4) fields of two bytes each: Source port number, Destination port number, Datagram size and checksum

- a. **UDP port number:** UDP port numbers allow different applications to maintain their own channels for data similar to TCP. UDP port headers are two bytes long.
- b. **Datagram size:** The UDP datagram size is a count of the total number of bytes contained in header and data sections. As the header length is a fixed size, this field effectively tracks the length of the variable-sized data portion (sometimes called payload). The size of datagrams varies depending on the operating environment but has a maximum of 65535 bytes.
- c. **Checksum:** UDP checksums protect message data from tampering. The checksum value represents an encoding of the datagram data calculated first by the sender and later by the receiver. Should an individual datagram be tampered with or get corrupted during transmission, the UDP protocol detects a checksum calculation mismatch. In UDP, check-summing is optional as opposed to TCP where checksums are mandatory.

Steps for performing this lab:

Do the following:

1. **Download** files *UDPCient.py* and *UDPServer.py* from your LMS site.
2. **Edit** these files. In *UDPCient.py* The serverIP address; use one of your neighbor and the message; as your name. In *UDPServer.py* use your own IP address
3. **Start up the Wireshark software.**
4. **Begin packet capture**, select the Capture pull down menu and select Options.
5. **Selecting the network interface on which packets would be captured:** You can use most of the default values in this window. The network interfaces (i.e., the physical connections) that your computer has to the network will be shown in the Interface pull down menu at the top of the Capture Options window. Click Start. Packet capture will now begin

Lab 6: Analysis of UDP in Wireshark**6. Run your UDPServer and UDPClient.**

7. Stopping the capture and inspecting captured packets: After you have received a welcome message, stop Wireshark packet capture

8. Filtering: Filter the UDP packets.

7. Details of a packet: Select the UDP messages shown in the packet-listing window and analyze by looking into the detail of packets pane and answer the questions given at the end of this document.

8. Obtaining credit for this lab: Now, please proceed to the questions section to answer the questions. You must note down your answers, along with screen shots in this file itself. Please note that you must upload this file (after duly filling in the answers) through the appropriate link at your LMS to obtain credit. Please clarify with your instructor/ lab engineer if you have any queries.

udp						
No.	Time	Source	Destination	Protocol	Length	Info
490	12.459306	10.7.44.55	10.7.40.255	UDP	75	55001 → 59680 Len=33
489	12.459012	10.7.40.255	10.7.44.55	UDP	58	59680 → 55001 Len=16
484	12.452026	10.7.44.82	230.0.0.1	UDP	92	61857 → 6666 Len=50
471	12.289664	10.7.40.97	230.0.0.1	UDP	92	52630 → 6666 Len=50
463	12.122926	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50
462	12.122925	10.7.32.227	230.0.0.1	UDP	92	61302 → 6666 Len=50
458	11.963920	10.7.40.69	230.0.0.1	UDP	92	56265 → 6666 Len=50
456	11.963919	10.7.40.202	230.0.0.1	UDP	92	55192 → 6666 Len=50
422	11.305876	10.7.9.6	230.0.0.1	UDP	92	59284 → 6666 Len=50
416	10.991677	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50
415	10.991677	10.7.32.227	230.0.0.1	UDP	92	61302 → 6666 Len=50
> Frame 490: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0 > Ethernet II, Src: SamsungE_14:ff:3e (50:b7:c3:14:ff:3e), Dst: HuaweiTe_40:6f:97 (28:a6:db:40:6f:97) > Internet Protocol Version 4, Src: 10.7.44.55, Dst: 10.7.40.255 > User Datagram Protocol, Src Port: 55001, Dst Port: 59680 > Data (33 bytes)						
0000	28 a6 db 40 6f 97 50 b7 c3 14 ff 3e 08 00 45 00	(..@oP...>..E..				
0010	00 3d 18 5c 00 00 80 11 b9 10 0a 07 2c 37 0a 07	..=\.......,7..				
0020	28 ff d6 d9 e9 20 00 29 aa 37 57 65 6c 63 6f 6d	(....)·7Welcom				
0030	65 20 41 42 44 55 4c 4c 41 48 20 52 41 46 41 51	e ABDULL AH RAFAQ				
0040	41 54 66 72 6f 6d 20 42 53 43 53	ATfrom B SCS				

Lab 6: Analysis of UDP in Wireshark**Questions:**

1. Select one UDP packet and determine the **Source IP, Source port No, Destination IP and Destination port No** of that UDP packet.

udp						
No.	Time	Source	Destination	Protocol	Length	Info
490	12.459306	10.7.44.55	10.7.40.255	UDP	75	55001 → 59680 Len=33
489	12.459012	10.7.40.255	10.7.44.55	UDP	58	59680 → 55001 Len=16
484	12.452026	10.7.44.82	230.0.0.1	UDP	92	61857 → 6666 Len=50
471	12.289664	10.7.40.97	230.0.0.1	UDP	92	52630 → 6666 Len=50
463	12.122926	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50
462	12.122925	10.7.32.227	230.0.0.1	UDP	92	61302 → 6666 Len=50
458	11.963920	10.7.40.69	230.0.0.1	UDP	92	56265 → 6666 Len=50
456	11.963919	10.7.40.202	230.0.0.1	UDP	92	55192 → 6666 Len=50
422	11.305876	10.7.9.6	230.0.0.1	UDP	92	59284 → 6666 Len=50
416	10.991677	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50
415	10.001677	10.7.32.227	230.0.0.1	UDP	92	61302 → 6666 Len=50
[Header checksum status: Unverified]						
Source: 10.7.44.55						
Destination: 10.7.40.255						
User Datagram Protocol, Src Port: 55001, Dst Port: 59680						
Source Port: 55001						
Destination Port: 59680						
Length: 41						
Checksum: 0xaa37 [unverified]						
[Checksum Status: Unverified]						
[Stream index: 188]						
> Data (33 bytes)						
0000	28 a6 db 40 6f 97 50 b7	c3 14 ff 3e 08 00 45 00	(..@o.P. ...>..E.			
0010	00 3d 18 5c 00 00 80 11	b9 10 0a 07 2c 37 0a 07	.=.\.... ..,7..			
0020	28 ff d6 d9 e9 20 00 29	aa 37 57 65 6c 63 6f 6d	(....) .7welcom			
0030	65 20 41 42 44 55 4c 4c	41 48 20 52 41 46 41 51	e ABDULL AH RAFAQ			
0040	41 54 66 72 6f 6d 20 42	53 43 53	ATfrom B SCS			

From the above figure,

Source IP Address: **10.7.44.55**

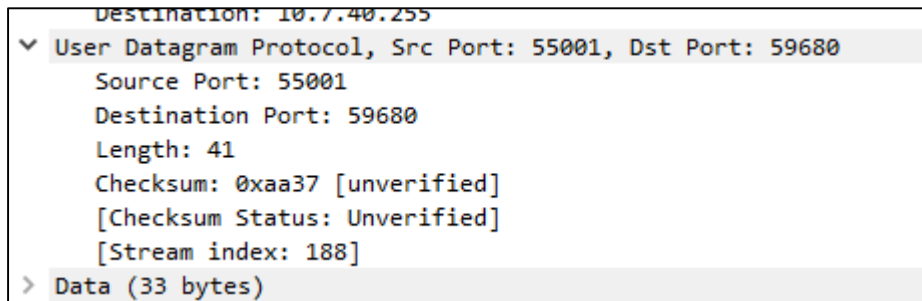
Destination IP Address: **10.7.40.255**

Source Port: **55001**

Destination Port: **59680**

Lab 6: Analysis of UDP in Wireshark

2. Select one UDP packet and determine how many **fields** are there in the UDP header. List **the name of these fields**.

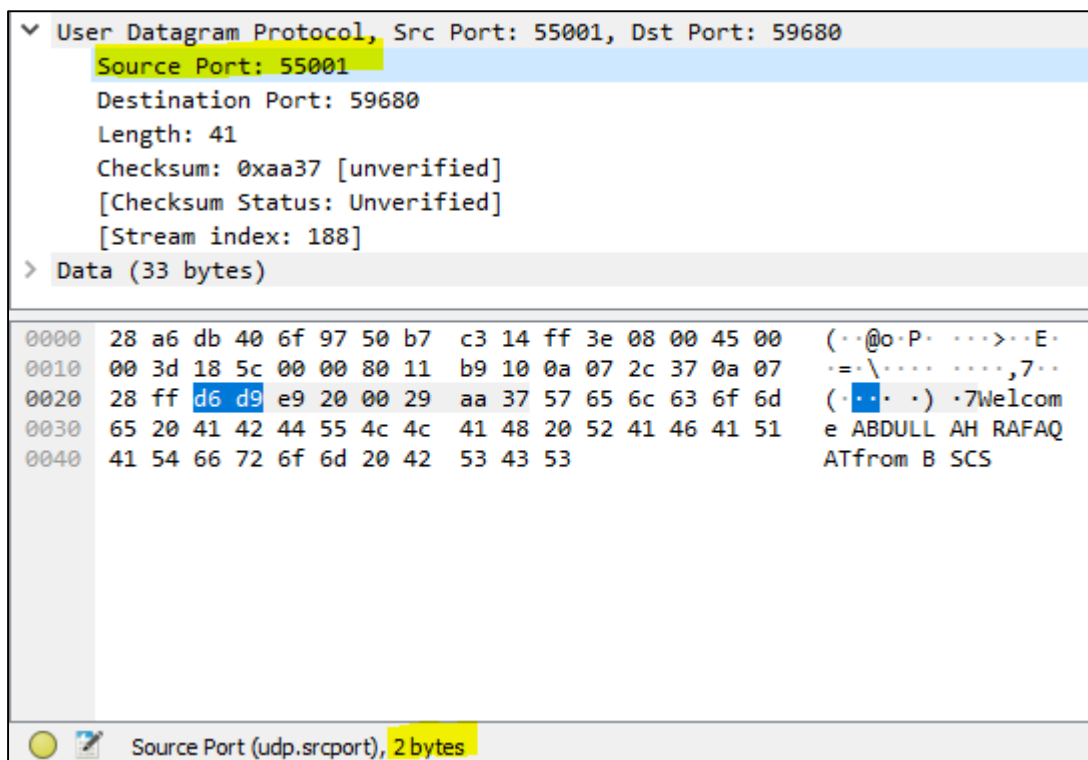


There are following fields in the UDP header:

1. **Source port**
 2. **Destination port**
 3. **Length**
 4. **Checksum**
3. From the packet content field, determine **the length (in bytes) of each of the UDP header fields**.

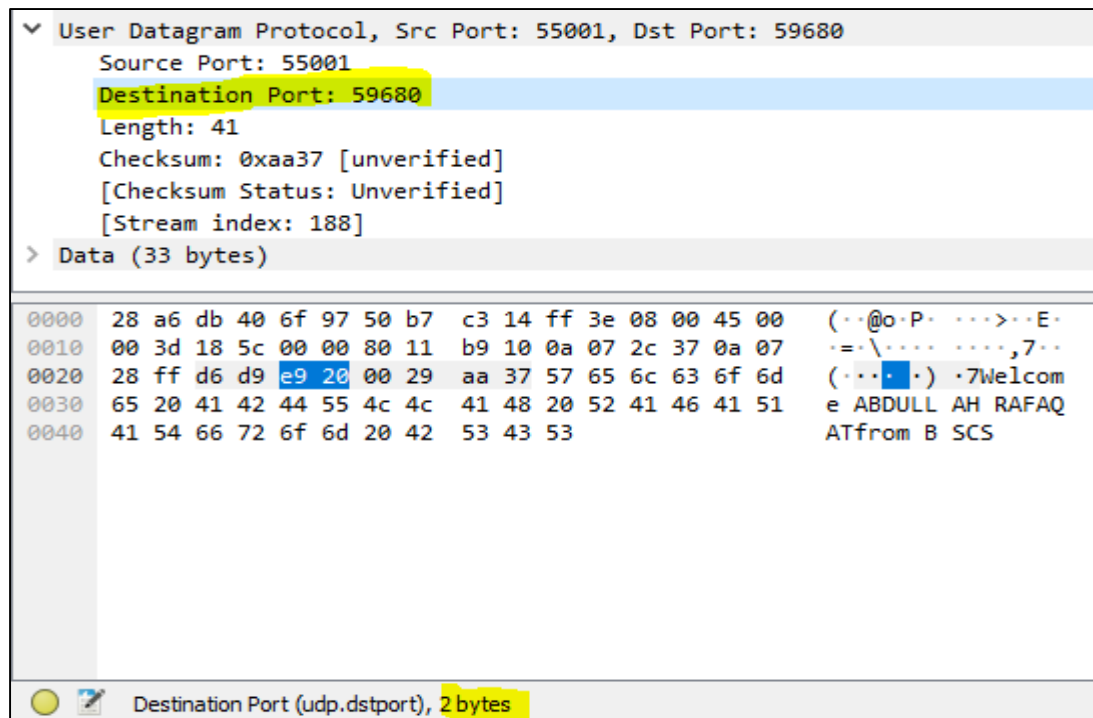
The size of header field of UDP is 8 bytes. Each field is divided as follow:

Source Port Field:



Lab 6: Analysis of UDP in Wireshark

The size of source port field is 2 bytes.

Destination Port Field:


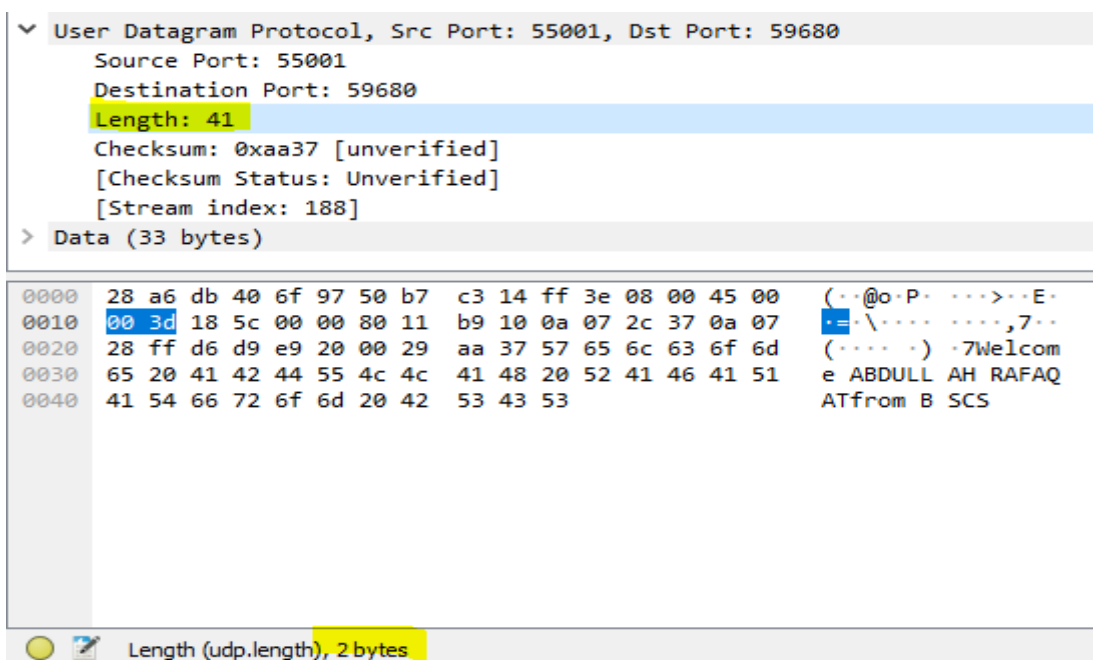
▼ User Datagram Protocol, Src Port: 55001, Dst Port: 59680

- Source Port: 55001
- Destination Port: 59680**
- Length: 41
- Checksum: 0xaa37 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 188]
- > Data (33 bytes)

0000	28 a6 db 40 6f 97 50 b7 c3 14 ff 3e 08 00 45 00	(..@o.P. ...>..E.
0010	00 3d 18 5c 00 00 80 11 b9 10 0a 07 2c 37 0a 07	..=\.... ..,7..
0020	28 ff d6 d9 e9 20 00 29 aa 37 57 65 6c 63 6f 6d	(... ..) .7Welcom
0030	65 20 41 42 44 55 4c 4c 41 48 20 52 41 46 41 51	e ABDULL AH RAFAQ
0040	41 54 66 72 6f 6d 20 42 53 43 53	ATfrom B SCS

Destination Port (udp.dstport), 2 bytes

The size of destination port field is 2 bytes.

Length Field:


▼ User Datagram Protocol, Src Port: 55001, Dst Port: 59680

- Source Port: 55001
- Destination Port: 59680
- Length: 41**
- Checksum: 0xaa37 [unverified]
- [Checksum Status: Unverified]
- [Stream index: 188]
- > Data (33 bytes)

0000	28 a6 db 40 6f 97 50 b7 c3 14 ff 3e 08 00 45 00	(..@o.P. ...>..E.
0010	00 3d 18 5c 00 00 80 11 b9 10 0a 07 2c 37 0a 07	..=\.... ..,7..
0020	28 ff d6 d9 e9 20 00 29 aa 37 57 65 6c 63 6f 6d	(... ..) .7Welcom
0030	65 20 41 42 44 55 4c 4c 41 48 20 52 41 46 41 51	e ABDULL AH RAFAQ
0040	41 54 66 72 6f 6d 20 42 53 43 53	ATfrom B SCS

Length (udp.length), 2 bytes

Lab 6: Analysis of UDP in Wireshark

The size of length field is also 2 bytes.

Checksum Field:

User Datagram Protocol, Src Port: 55001, Dst Port: 59680
 Source Port: 55001
 Destination Port: 59680
 Length: 41
 Checksum: 0xaa37 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 188]
 > Data (33 bytes)

0000	28 a6 db 40 6f 97 50 b7 c3 14 ff 3e 08 00 45 00	(..@o.P.>..E.
0010	00 3d 18 5c 00 00 80 11 b9 10 0a 07 2c 37 0a 07	..=\.....,7..
0020	28 ff d6 d9 e9 20 00 29 aa 37 57 65 6c 63 6f 6d	(....) 7Welcom
0030	65 20 41 42 44 55 4c 4c 41 48 20 52 41 46 41 51	e ABDULL AH RAFAQ
0040	41 54 66 72 6f 6d 20 42 53 43 53	ATfrom B SCS

Details at: http://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (udp.checksum), 2 bytes

The size of Checksum field is 2 bytes.

4. **Examine the pair of UDP packets** in which your host sends the first packet and the second packet is a reply to the first packet. Describe the relationship between the port numbers in the two packets.

No.	Time	Source	Destination	Protocol	Length	Info
490	12.459306	10.7.44.55	10.7.40.255	UDP	75	55001 → 59680 Len=33
489	12.459012	10.7.40.255	10.7.44.55	UDP	58	59680 → 55001 Len=16
484	12.452026	10.7.44.82	230.0.0.1	UDP	92	61857 → 6666 Len=50
471	12.289664	10.7.40.97	230.0.0.1	UDP	92	52630 → 6666 Len=50
463	12.122926	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50
462	12.122925	10.7.32.227	230.0.0.1	UDP	92	61302 → 6666 Len=50
458	11.963920	10.7.40.69	230.0.0.1	UDP	92	56265 → 6666 Len=50
456	11.963919	10.7.40.202	230.0.0.1	UDP	92	55192 → 6666 Len=50
422	11.305876	10.7.9.6	230.0.0.1	UDP	92	59284 → 6666 Len=50
416	10.991677	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50

> Frame 490: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
 > Ethernet II, Src: SamsungE_14:ff:3e (50:b7:c3:14:ff:3e), Dst: HuaweiTe_40:6f:97 (28:a6:db:40:6f:97)
 > Internet Protocol Version 4, Src: 10.7.44.55, Dst: 10.7.40.255
 > User Datagram Protocol, Src Port: 55001, Dst Port: 59680
 Source Port: 55001
 Destination Port: 59680
 Length: 41
 Checksum: 0xaa37 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 188]
 > Data (33 bytes)

0000	28 a6 db 40 6f 97 50 b7 c3 14 ff 3e 08 00 45 00	(..@o.P.>..E.
0010	00 3d 18 5c 00 00 80 11 b9 10 0a 07 2c 37 0a 07	..=\.....,7..
0020	28 ff d6 d9 e9 20 00 29 aa 37 57 65 6c 63 6f 6d	(....) 7Welcom
0030	65 20 41 42 44 55 4c 4c 41 48 20 52 41 46 41 51	e ABDULL AH RAFAQ
0040	41 54 66 72 6f 6d 20 42 53 43 53	ATfrom B SCS

Lab 6: Analysis of UDP in Wireshark

For the request packet, source port (Which is the client port) is set as: **59680** and the destination port (Which is server port to which it is requested) is set as: **55001**. Whereas, in response packet, ports are interchanged because this time server is source and client is destination. For that case, Source port is: **55001** and Destination port is: **59680**.

5. Analyze the UDP packet and answer that the **value in the Length field** is the length of what? Verify your claim with your captured UDP packet.

Length field shows the total number of bytes of the packet. For my case, it is: 24. Out of 24, We know that header field contains total of 8 bytes. So, remaining 16 bytes is for the data. As we can see in figure, Data contains 16 bytes which were exactly expected from the above calculation. The client send "**Abdullah Rafaqat**" as message. The message has 16 characters so the 16 bytes of data.

User Datagram Protocol, Src Port: 59680, Dst Port: 55001															
Source Port: 59680															
Destination Port: 55001															
Length: 24															
Checksum: 0x1e35 [unverified]															
[Checksum Status: Unverified]															
[Stream index: 188]															
> Data (16 bytes)															
0000	50	b7	c3	14	ff	3e	28	a6	db	40	6f	97	08	00	45 00
0010	00	2c	17	d8	00	00	7f	11	ba	a5	0a	07	28	ff	0a 07
0020	2c	37	e9	20	d6	d9	00	18	1e	35	41	62	64	75	6c 6c
0030	61	68	20	52	61	66	61	71	61	74					

6. What is the **maximum number of bytes** that can be included in a UDP payload? Why this is the maximum?

Since from above question, we realize that greatest length of the bundle can be: $2^{16} - 1$ since 2 bytes is the extent of length field in the header. Out of these length esteems, we realize that 8 bytes are saved for header in this way, for payload the size must be: $(2^{16} - 1) - 8$ Bytes. Additionally it contains some pseudo header of size 20 Bytes which should likewise be subtracted from above outcome to acquire the required bytes. In this way, Maximum number of Bytes that can be incorporated into UDP payload are:
 $2^{16} - 29$ Bytes = **65506 Bytes**.

Lab 6: Analysis of UDP in Wireshark7. What is the **largest possible source port number**?

Add up to size of the source port number field is: 2 Bytes (16 Bits). So these 16 Bits (2 Bytes) can speak to 2^{16} aggregate potential outcomes beginning from 0. Thus most extreme conceivable source port number is: $2^{16} - 1 = 65535$ port number

8. What is the **protocol number for UDP**? Give your answer in both hexadecimal and decimal notation.

No.	Time	Source	Destination	Protocol	Length	Info
490	12.459306	10.7.44.55	10.7.40.255	UDP	75	55001 → 59680 Len=33
489	12.459012	10.7.40.255	10.7.44.55	UDP	58	59680 → 55001 Len=16
484	12.452026	10.7.44.82	230.0.0.1	UDP	92	61857 → 6666 Len=50
471	12.289664	10.7.40.97	230.0.0.1	UDP	92	52630 → 6666 Len=50
463	12.122926	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50
462	12.122925	10.7.32.227	230.0.0.1	UDP	92	61302 → 6666 Len=50
458	11.963920	10.7.40.69	230.0.0.1	UDP	92	56265 → 6666 Len=50
456	11.963919	10.7.40.202	230.0.0.1	UDP	92	55192 → 6666 Len=50
422	11.305876	10.7.9.6	230.0.0.1	UDP	92	59284 → 6666 Len=50
416	10.991677	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50
415	10.991677	10.7.32.227	230.0.0.1	UDP	92	61302 → 6666 Len=50

0000	00..	= Differentiated Services Codepoint: Default (0)
....	..00	= Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 44		
Identification: 0x17d8 (6104)		
> Flags: 0x0000		
Time to live: 127		
Protocol: UDP (17)		
Header checksum: 0xbaa5 [validation disabled]		
[Header checksum status: Unverified]		
Source: 10.7.40.255		
Destination: 10.7.44.55		
> User Datagram Protocol Src Port: 59680 Dst Port: 55001		

0000	50 b7 c3 14 ff 3e 28 a6 db 40 6f 97 08 00 45 00	P....>(.@o...E.
0010	00 2c 17 d8 00 00 7f 11 ba a5 0a 07 28 ff 0a 07	,.....(...
0020	2c 37 e9 20 d6 d9 00 18 1e 35 41 62 64 75 6c 6c	,7....5Abdull
0030	61 68 20 52 61 66 61 71 61 74	ah Rafaq at

From the above figure, for my UDP packet, protocol number is:

Hexadecimal: **(11)₁₆**

Decimal: **(17)₁₀**

Lab 6: Analysis of UDP in Wireshark

9. Compare the **checksum values** in the UDP segment header sent from client to server and from the server to the client. Are they same or they differ? If the payload of each packet is same, would the checksum change?

Client to Server:

No.	Time	Source	Destination	Protocol	Length	Info
490	12.459306	10.7.44.55	10.7.40.255	UDP	75	55001 → 59680 Len=33
489	12.459012	10.7.40.255	10.7.44.55	UDP	58	59680 → 55001 Len=16
484	12.452026	10.7.44.82	230.0.0.1	UDP	92	61857 → 6666 Len=50
471	12.289664	10.7.40.97	230.0.0.1	UDP	92	52630 → 6666 Len=50
463	12.122926	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50
462	12.122925	10.7.32.227	230.0.0.1	UDP	92	61302 → 6666 Len=50
458	11.963920	10.7.40.69	230.0.0.1	UDP	92	56265 → 6666 Len=50
456	11.963919	10.7.40.202	230.0.0.1	UDP	92	55192 → 6666 Len=50
422	11.305876	10.7.9.6	230.0.0.1	UDP	92	59284 → 6666 Len=50
416	10.991677	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50
415	10.001677	10.7.33.227	230.0.0.1	UDP	92	61302 → 6666 Len=50

> Frame 489: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
 > Ethernet II, Src: HuaweiTe_40:6f:97 (28:a6:db:40:6f:97), Dst: SamsungE_14:ff:3e (50:b7:c3:14:ff:3e)
 > Internet Protocol Version 4, Src: 10.7.40.255, Dst: 10.7.44.55
 > User Datagram Protocol, Src Port: 59680, Dst Port: 55001
 Source Port: 59680
 Destination Port: 55001
 Length: 24
 Checksum: 0x1e35 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 188]
 > Data (16 bytes)

```

0000  50 b7 c3 14 ff 3e 28 a6 db 40 6f 97 08 00 45 00  P....>(.@o...E.
0010  00 2c 17 d8 00 00 7f 11 ba a5 0a 07 28 ff 0a 07  .,\.....,7...
0020  2c 37 e9 20 d6 d9 00 18 1e 35 41 62 64 75 6c 6c  ,7.....5Abdull
0030  61 68 20 52 61 66 61 71 61 74                   ah Rafaq at
  
```

Server to Client:

No.	Time	Source	Destination	Protocol	Length	Info
490	12.459306	10.7.44.55	10.7.40.255	UDP	75	55001 → 59680 Len=33
489	12.459012	10.7.40.255	10.7.44.55	UDP	58	59680 → 55001 Len=16
484	12.452026	10.7.44.82	230.0.0.1	UDP	92	61857 → 6666 Len=50
471	12.289664	10.7.40.97	230.0.0.1	UDP	92	52630 → 6666 Len=50
463	12.122926	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50
462	12.122925	10.7.32.227	230.0.0.1	UDP	92	61302 → 6666 Len=50
458	11.963920	10.7.40.69	230.0.0.1	UDP	92	56265 → 6666 Len=50
456	11.963919	10.7.40.202	230.0.0.1	UDP	92	55192 → 6666 Len=50
422	11.305876	10.7.9.6	230.0.0.1	UDP	92	59284 → 6666 Len=50
416	10.991677	10.7.9.7	230.0.0.1	UDP	92	56326 → 6666 Len=50
415	10.001677	10.7.33.227	230.0.0.1	UDP	92	61302 → 6666 Len=50

> Frame 490: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
 > Ethernet II, Src: SamsungE_14:ff:3e (50:b7:c3:14:ff:3e), Dst: HuaweiTe_40:6f:97 (28:a6:db:40:6f:97)
 > Internet Protocol Version 4, Src: 10.7.44.55, Dst: 10.7.40.255
 > User Datagram Protocol, Src Port: 55001, Dst Port: 59680
 Source Port: 55001
 Destination Port: 59680
 Length: 41
 Checksum: 0xaa37 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 188]
 > Data (33 bytes)

```

0000  28 a6 db 40 6f 97 50 b7 c3 14 ff 3e 08 00 45 00  (.@o.P....>...E.
0010  00 3d 18 5c 00 00 80 11 b9 10 0a 07 2c 37 0a 07  .-=\.....,7...
0020  28 ff d6 d9 e9 20 00 29 aa 37 57 65 6c 63 6f 6d  (.....)7welcom
0030  65 20 41 42 44 55 4c 4c 41 48 20 52 41 46 41 51  e ABDULL AH RAFAQ
0040  41 54 66 72 6f 6d 20 42 53 43 53                 ATfrom B SCS
  
```

For the two cases, Checksum esteems are distinctive as observed from the figure. For same payload, the checksum would in any case change on the grounds that UDP does not enjoy the arrangement of packets. So for similar information, arrangement of packets may change.

Lab 6: Analysis of UDP in Wireshark

10. Which fields are included in calculating the UDP checksum?

*To ascertain UDP checksum, we require **pseudo header field, data field, header field as checksum** is computed by taking 1s supplement of the aggregate of these fields.*