Department of Electrical Engineering, UET Lahore
EE432 Computer Networks Lab

Course Instructor: Dr Naveed Nawaz	**Dated: 23/09/2024**
Session: Fall 2024	**Semester: 7th**

LAB 4 Analyzing the behavior of User Datagram Protocol (UDP)

Name	Roll. No.	Report Marks (10)	Viva Marks (5)	Total Marks (15)
Ayesha Ahmad	2021-EE-052			

Signature: ______________________________

Analyzing the behavior of User Datagram Protocol

4.1. Objectives

In performing this lab, students will

- Analyze the behavior of UDP in detail
- Determine 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

4.2. Background

4.2.1. 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.

4.2.2. UDP Datagrams

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.

4.2.2.1. 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; therefore, valid UDP port numbers range from 0 to 65535.

4.2.2.2. 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.

4.2.2.3. 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, checksumming is optional as opposed to TCP where checksums are mandatory.

4.3. Procedure

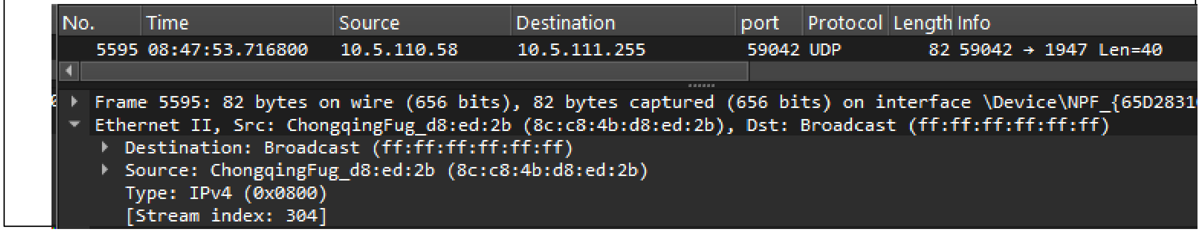
1. Start up the Wireshark software.
2. Begin packet capture, select the Capture pull down menu and select Options.
3. Select the network interface on which packets would be captured: You can use most of the default values in this window. The network interfaces (i.e., the physical connections) that your computer has to the network will be shown in the Interface pull down menu at the top of the Capture Options window.
4. Click Start. Packet capture will now begin.
5. Start up your favorite web browser, and type any site which uses the UDP packets for traffic flow in the packet listing window.
6. Stop the capture and inspect captured packets: After your browser has displayed the page, stop Wireshark packet capture

7. Filter the UDP packets.
8. Select the UDP messages shown in the packet-listing window and analyze by looking into the detail of packets pane.

4.4. Questions

1. Select one packet and determine the source MAC address of that UDP packet.

The source MAC address of the UDP packet is 8c:c8:4b:d8:ed:2b

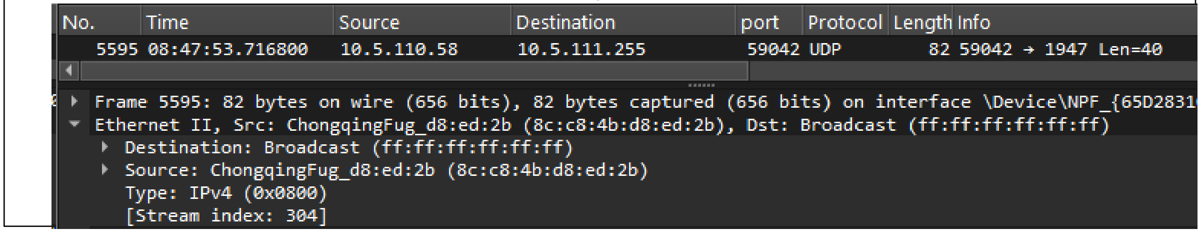


```
No.   Time             Source        Destination    port  Protocol Length Info
 5595 08:47:53.716800  10.5.110.58   10.5.111.255   59042 UDP        82 59042 → 1947 Len=40

▸ Frame 5595: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{65D2831
▾ Ethernet II, Src: ChongqingFug_d8:ed:2b (8c:c8:4b:d8:ed:2b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   ▸ Source: ChongqingFug_d8:ed:2b (8c:c8:4b:d8:ed:2b)
     Type: IPv4 (0x0800)
     [Stream index: 304]
```

2. Select one packet and determine the destination MAC address of that UDP packet.

The destination MAC address of the UDP packet is ff:ff:ff:ff:ff:ff

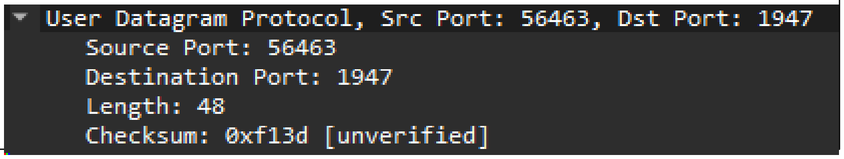


```
No.   Time             Source        Destination    port  Protocol Length Info
 5595 08:47:53.716800  10.5.110.58   10.5.111.255   59042 UDP        82 59042 → 1947 Len=40

▸ Frame 5595: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{65D2831
▾ Ethernet II, Src: ChongqingFug_d8:ed:2b (8c:c8:4b:d8:ed:2b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
   ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   ▸ Source: ChongqingFug_d8:ed:2b (8c:c8:4b:d8:ed:2b)
     Type: IPv4 (0x0800)
     [Stream index: 304]
```

3. Select one packet and determine how many fields are there in the UDP header.

There are 4 fields in the UDP header.

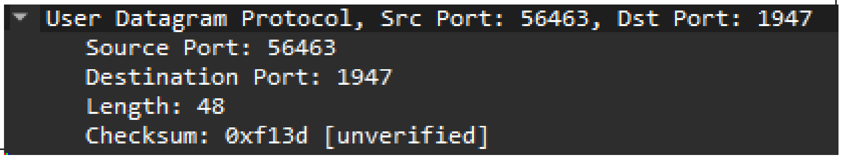


```
▾ User Datagram Protocol, Src Port: 56463, Dst Port: 1947
     Source Port: 56463
     Destination Port: 1947
     Length: 48
     Checksum: 0xf13d [unverified]
```

4. List the name of these fields.

The names of the UDP header fields are:

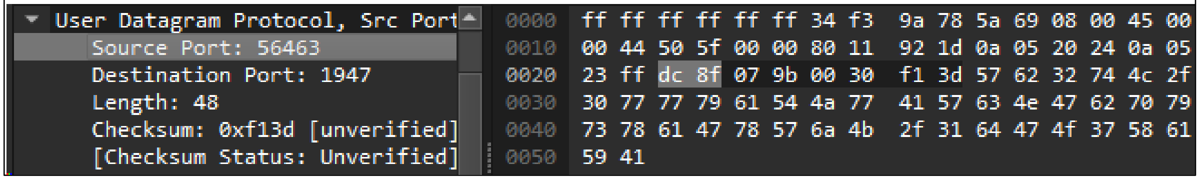
1. Source Port
2. Destination Port
3. Length
4. Checksum



```
▾ User Datagram Protocol, Src Port: 56463, Dst Port: 1947
     Source Port: 56463
     Destination Port: 1947
     Length: 48
     Checksum: 0xf13d [unverified]
```

5. From the packet content field, determine the length (in bytes) of each of the UDP header fields.

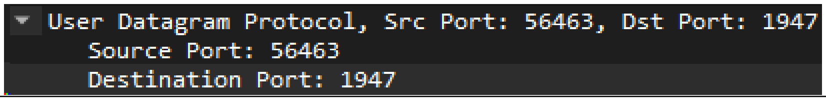
The length of the UDP header fields is 2 bytes each.



```
▾ User Datagram Protocol, Src Port     0000  ff ff ff ff ff ff 34 f3  9a 78 5a 69 08 00 45 00
     Source Port: 56463                0010  00 44 50 5f 00 00 80 11  92 1d 0a 05 20 24 0a 05
     Destination Port: 1947            0020  23 ff dc 8f 07 9b 00 30  f1 3d 57 62 32 74 4c 2f
     Length: 48                        0030  30 77 77 79 61 54 4a 77  41 57 63 4e 47 62 70 79
     Checksum: 0xf13d [unverified]     0040  73 78 61 47 78 57 6a 4b  2f 31 64 47 4f 37 58 61
     [Checksum Status: Unverified]     0050  59 41
```

6. What is the source and the destination port number of UDP packet.

The source and destination port numbers of the UDP packet are as follows,
Source Port : 56463
Destination Port : 1947

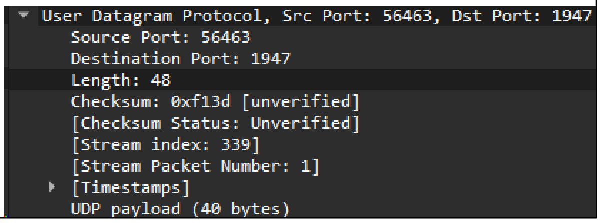


```
▾ User Datagram Protocol, Src Port: 56463, Dst Port: 1947
    Source Port: 56463
    Destination Port: 1947
```

7. 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.

The value in the Length field is the "Datagram length" which is the **number of bytes of the UDP header and payload combined.**

UDP header = (2 bytes x 4 fields) = 8 bytes
UDP payload = 40 bytes
Length = 8 + 40 = 48 bytes



```
▾ User Datagram Protocol, Src Port: 56463, Dst Port: 1947
    Source Port: 56463
    Destination Port: 1947
    Length: 48
    Checksum: 0xf13d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 339]
    [Stream Packet Number: 1]
  ▸ [Timestamps]
    UDP payload (40 bytes)
```

8. What is the maximum number of bytes that can be included in a UDP payload.

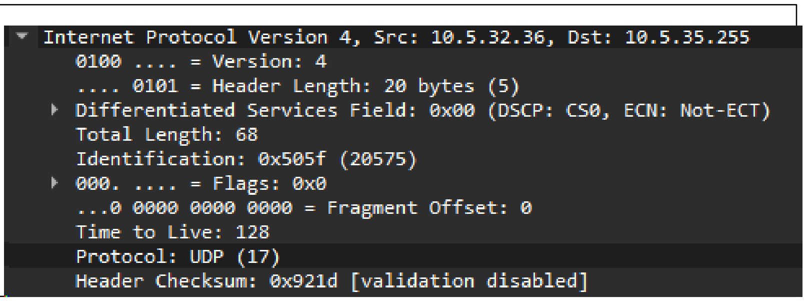
A UDP datagram is carried in a single IP packet so the maximum number of bytes in the payload for IPv4 is **65,507 bytes** and for IPv6 is 65,527 bytes.

9. What is the largest possible source port number?

The source/destination port numbers are defined as 2 bytes in the UDP header so the largest port number possible is 2^(16 bits) - 1 = 65,535.
Thus, UDP source port numbers can be between 0 and **65,535.**

10. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. (To answer this question, you'll need to look into the IP header.)

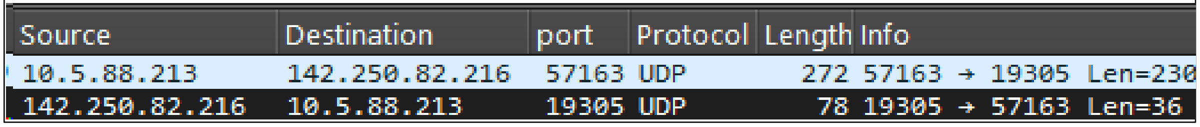
The Protocol Number for UDP is **17**.



```
▾ Internet Protocol Version 4, Src: 10.5.32.36, Dst: 10.5.35.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 68
    Identification: 0x505f (20575)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x921d [validation disabled]
```

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

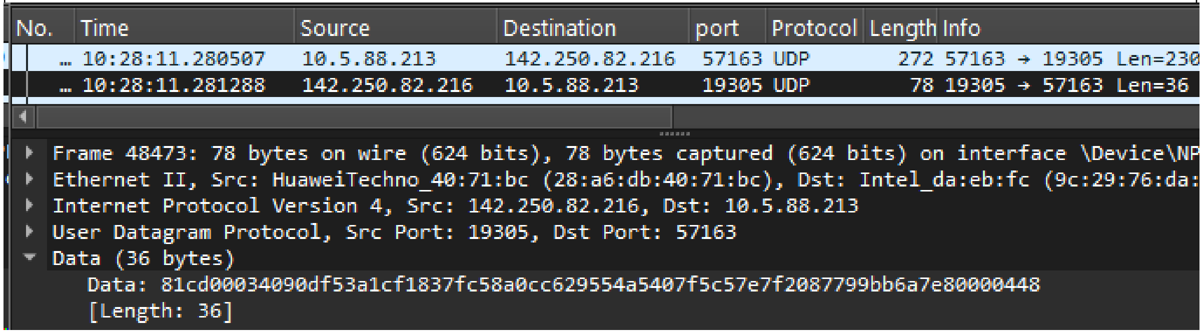
The source and destination port numbers get **switched** in the reply to the 1st packet.



```
Source           Destination      port  Protocol Length Info
10.5.88.213      142.250.82.216   57163 UDP         272 57163 → 19305 Len=230
142.250.82.216   10.5.88.213      19305 UDP          78 19305 → 57163 Len=36
```

12. Show the data attached to the UDP packet in both hexadecimal and decimal notation.

Hexadecimal:
81cd00034090df53a1cf1837fc58a0cc629554a5407f5c57e7f2087799bb6a7e80000448
Decimal:
252159940297551942098939914212021105023735056643498695743468927269684874417513334572104



```
No.  Time              Source           Destination      port  Protocol Length Info
 … 10:28:11.280507   10.5.88.213      142.250.82.216   57163 UDP         272 57163 → 19305 Len=230
 … 10:28:11.281288   142.250.82.216   10.5.88.213      19305 UDP          78 19305 → 57163 Len=36

▸ Frame 48473: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NP
▸ Ethernet II, Src: HuaweiTechno_40:71:bc (28:a6:db:40:71:bc), Dst: Intel_da:eb:fc (9c:29:76:da:
▸ Internet Protocol Version 4, Src: 142.250.82.216, Dst: 10.5.88.213
▸ User Datagram Protocol, Src Port: 19305, Dst Port: 57163
▾ Data (36 bytes)
    Data: 81cd00034090df53a1cf1837fc58a0cc629554a5407f5c57e7f2087799bb6a7e80000448
    [Length: 36]
```

Assessment Rubrics for
Computer Networks Lab 4

Student Name: ______________________________ Roll Number: _____________________________

Method:

Lab report evaluation and instructor observation during lab sessions.

Outcomes Assessed:

a. Ability to condut experiments as well as to analyze and interpret data
b. Ability to adhere to safety and disciplinary rules
c. Ability to use the techniques, skills and modern engineering tools necessary for engineering practice

Performance	Exceeds expectation (5-4)	Meets expectation (3-2)	Does not meet expectation (1)	Marks
Realization of experiment (a)	Downloads and installs required software and sets up the system according to the experiment requirements	Needs guidance to set up the system according to the experiment requirements	Incapable of selecting relevant software to the experiment and unable to setup the system with required software tools	
Conducting experiment (a, c)	Carries out each procedural step in a satisfactory manner and studies outputs of the software application rigorously	Needs assistance or guidance to proceed through experiment steps, studies outputs with minor errors in interpretation	Unable to carry out procedural steps and make any useful observations of outputs	
Laboratory safety and disciplinary rules (b)	Observes lab safety rules; adheres to the lab disciplinary guidelines aptly	Observes safety rules and disciplinary guidelines with minor deviations	Disregards lab safety and disciplinary rules	
Data collection (c)	Completes data collection from the experiment setup by following procedural steps, ensures that the data is entered in the lab manual according to the specified instructions	Completes data collection with minor error and enters data in lab manual with slight deviation from guidelines	Fails at collecting data by giving proper inputs and observing output states of experiment setup, unable to fill the lab manual properly	
Data analysis (a, c)	Analyzes the data obtained from experiment thoroughly and accurately verifies it with theoretical understanding, accounts for any discrepancy in data from theory with sound explanation	Analyzes data with minor error and correlates it with theoretical values reasonably. Attempts to account for any discrepancy in data from theory	Unable to establish the relationship between practical and theoretical values and lacks the theoretical understanding to explain any discrepancy in data	