

Wireshark CN Assignment – 5

Submitted By: Stuti Garg (SE22UCSE263)

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields.

- The number of fields under the UDP header are 4.
- They are namely- Source Port, Destination Port, Length and Checksum.

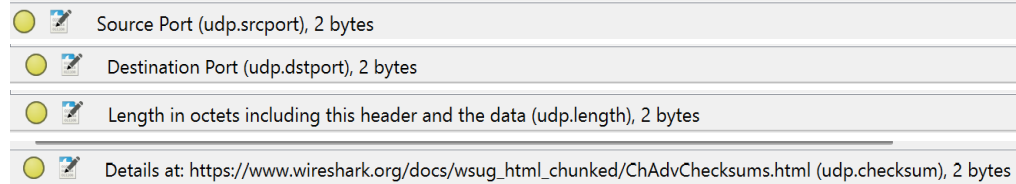
▼ User Datagram Protocol, Src Port: 52957, Dst Port: 53

Source Port: 52957
Destination Port: 53
Length: 38
Checksum: 0x6a15 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
[Stream Packet Number: 1]
> [Timestamps]
UDP payload (30 bytes)

- > Domain Name System (query)

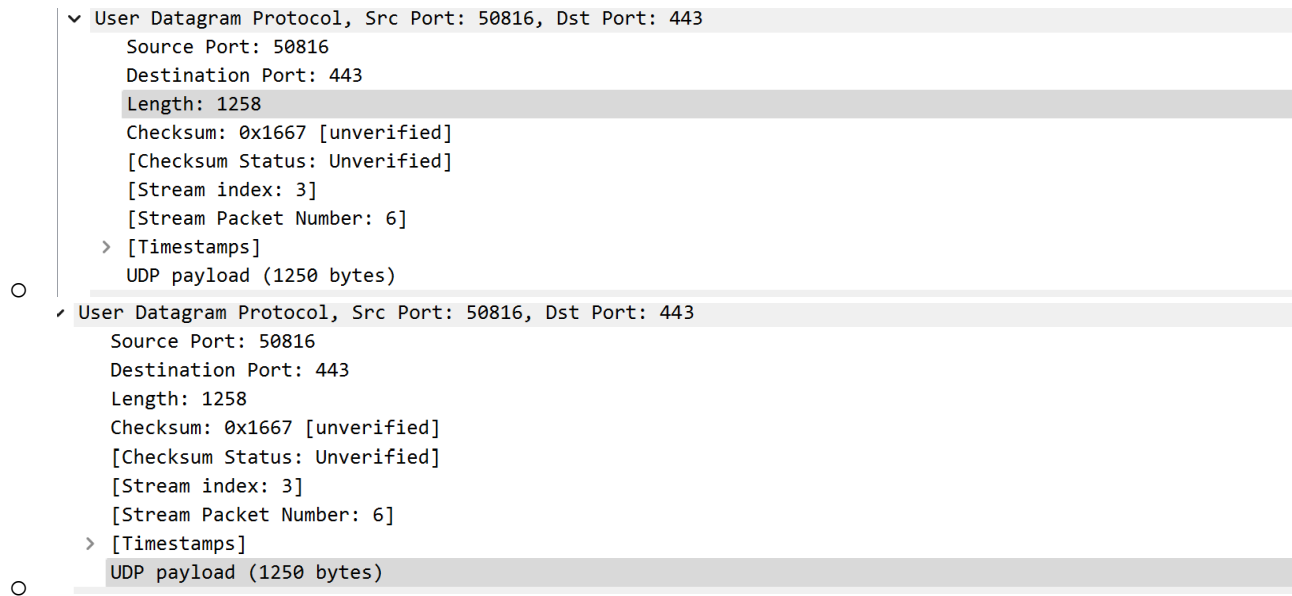
2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

- The length of each field under UDP header (Source Port, Destination Port, Length and Checksum): are each of 2 bytes.
- Therefore, total UDP header size is $2 + 2 + 2 + 2 = 8$ bytes

- 

3. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

- The Length field indicates the total length of the UDP segment, which includes the 8-byte header and the UDP payload.
- Length = 1258 bytes, UDP payload = 1250 bytes
- Therefore, length = 8 byte header + UDP payload
- Implies, $1258 = 8 + 1250$ satisfied.



4. What is the maximum number of bytes that can be included in a UDP payload?
- The UDP Length field is 16 bits, allowing it to represent a maximum value of 65,535 bytes. However, this total length includes the 8-byte UDP header.
 - As a result, the largest possible UDP payload size is: $65,535 - 8 = 65,527$ bytes.
5. What is the largest possible source port number?
- The port number field is also 16 bits, so the largest possible value is:
 - $(2^{16}) - 1 = 65,535$
6. 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 Protocol field of the IP datagram containing this UDP segment.
- Under the Protocol field of the IP datagram containing this UDP segment, the protocol number for UDP in decimal is 17.
 - In hexadecimal, it is 0x11.

```

> Frame 20373: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{8F984505-D
> Ethernet II, Src: Microsoft_7f:ad:fc (70:bc:10:7f:ad:fc), Dst: 12:01:00:00:01:00 (12:01:00:00:01:00)
✓ Internet Protocol Version 4, Src: 10.70.60.31, Dst: 4.155.233.194
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 84
        Identification: 0x2df3 (11763)
    > 000. .... = Flags: 0x0
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 128
        Protocol: UDP (17)
        Header Checksum: 0xd7e3 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 10.70.60.31
        Destination Address: 4.155.233.194
        [Stream index: 26]
✓ User Datagram Protocol, Src Port: 57811, Dst Port: 37174
    Source Port: 57811
    Destination Port: 37174
    Length: 64
    Checksum: 0xf9bd [unverified]
    [Checksum Status: Unverified]
    [Stream index: 10]

```

7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.

- While capturing, packet 4914 is a UDP packet sent from the host, and packet 4977 is the response to it. The source port in the outgoing packet (54845) turns into the destination port in the reply, while the destination port in the original packet (53) becomes the source port in the response.
- This shows the port-swapping behavior-
The request goes from a random high port to port 53 (DNS server).
The reply comes back from port 53 to the original source port (54845).
- Hence, the UDP swaps the source and destination ports, matching the request.

No.	Time	Source	Destination	Protocol	Length	Info
4914	1.676953	10.70.60.31	10.59.121.144	DNS	91	Standard query 0x2f73 A browser.pipe.aria.microsoft.com
4977	1.700075	10.59.121.144	10.70.60.31	DNS	212	Standard query response 0x2f73 A browser.pipe.aria.microsoft.com CNAME browser.events.data.trafficmanager.net CNAME onedscolprdeus00

```
> Frame 4914: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{8F984505-D5
> Ethernet II, Src: Microsoft_7f:ad:fc (70:bc:10:7f:ad:fc), Dst: 12:01:00:00:01:00 (12:01:00:00:01:00)
v Internet Protocol Version 4, Src: 10.70.60.31, Dst: 10.59.121.144
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 77
        Identification: 0xef30 (61232)
    > 000. .... = Flags: 0x0
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 128
        Protocol: UDP (17)
        Header Checksum: 0x813f [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 10.70.60.31
        Destination Address: 10.59.121.144
        [Stream index: 11]
v User Datagram Protocol, Src Port: 54845, Dst Port: 53
    Source Port: 54845
    Destination Port: 53
    Length: 57
    Checksum: 0x0601 [unverified]
    [Checksum Status: Unverified]

> Frame 4977: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits) on interface \Device\NPF_{8F984505-D5}
> Ethernet II, Src: Hewlett-Packard_01:00:ec:67:94:fb (01:00:ec:67:94:fb:01:00), Dst: Microsoft_7f:ad:fc (70:bc:10:7f:ad:fc)
v Internet Protocol Version 4, Src: 10.59.121.144, Dst: 10.70.60.31
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 198
        Identification: 0xd6d2 (54994)
    > 000. .... = Flags: 0x0
        ...0 0000 0000 0000 = Fragment Offset: 0
        Time to Live: 127
        Protocol: UDP (17)
        Header Checksum: 0x9a24 [validation disabled]
        [Header checksum status: Unverified]
        Source Address: 10.59.121.144
        Destination Address: 10.70.60.31
        [Stream index: 11]
v User Datagram Protocol, Src Port: 53, Dst Port: 54845
    Source Port: 53
    Destination Port: 54845
    Length: 178
    Checksum: 0x0fc9 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 5]
```