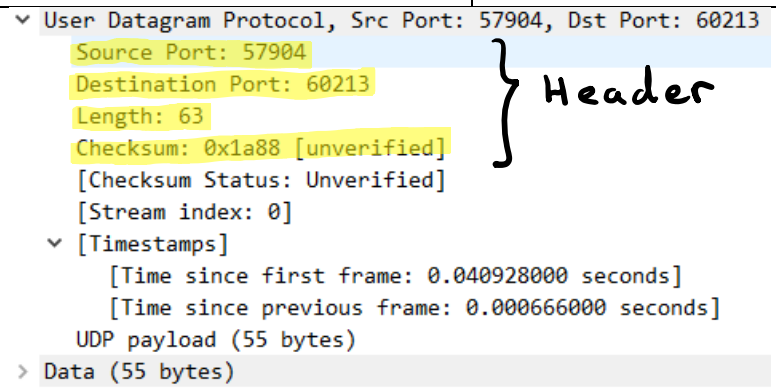
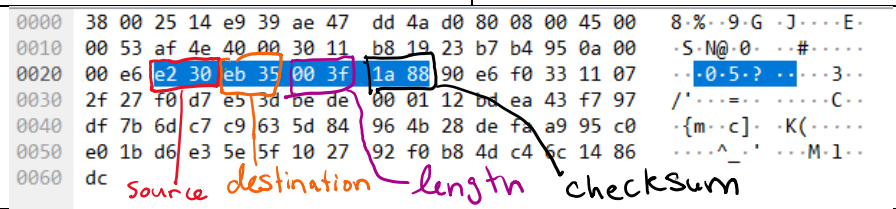
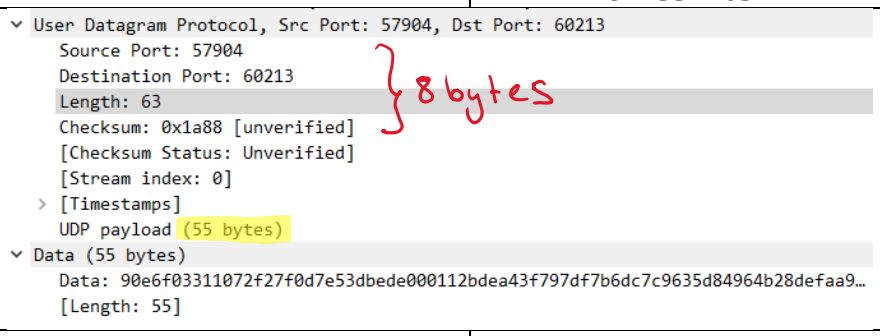
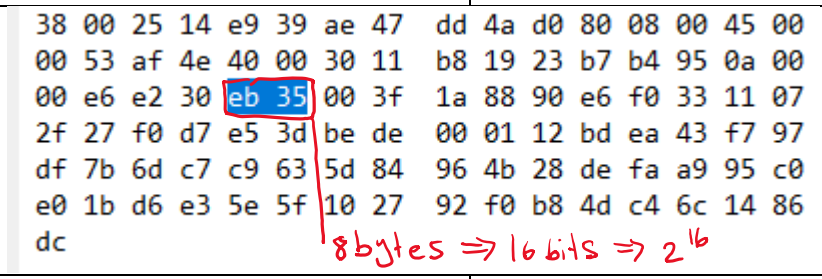
Wireshark Lab 2: UDP

Group Details:
Shayshu Nahata-Ragubance – 1005035196
Johnathan Yan - 1004745476

Mark:

	Question	Answer
1	Select one packet. From this packet, determine how many fields there are in the UDP header. Name these fields.	There are 8 fields: • Source port • Destination port • Length • Checksum
Annotated Screenshots (if needed)		
2	From the packet content field, determine the length (in bytes) of each of the UDP header fields.	The header is 8 bytes: • Source port: 2 bytes • Destination port: 2 bytes • Length: 2 bytes • Checksum: 2 bytes
Annotated Screenshots (if needed)		

3	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 size of the header plus the size of the UDP payload. Length = Header + payload = 8 + 55 = 63
Annotated Screenshots (if needed)		
4	What is the maximum number of bytes that can be included in a UDP payload.	The maximum size of a UDP segment is 65, 535 bytes, so the payload can be at most 65, 527 bytes
Annotated Screenshots (if needed)		
5	What is the largest possible source port number?	The highest available port number is 65, 535, this is because the port size is 2 bytes thus allowing for 2^16 – 1 values.
Annotated Screenshots (if needed)		
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 IP header.)	The protocol number is 17 or 0x11.

<table>
<tr><td>Annotated Screenshots (if needed)</td><td colspan="2">Time to Live: 48
Protocol: UDP (17) } decimal
Header Checksum: 0xb
38 00 25 14 e9 39 ae 47 dd 4a d0 80 08 00 45 00
00 53 af 4e 40 00 30 11 b8 19 23 b7 b4 95 0a 00
00 e6 e2 30 eb 35 00 3f 1a 88 90 e6 f0 33 11 07
2f 27 f0 d7 e5 3d be de 00 01 12 bd ea 43 f7 97
df 7b 6d c7 c9 63 5d 84 96 4b 28 de fa a9 95 c0
e0 1b d6 e3 5e 5f 10 27 92 f0 b8 4d c4 6c 14 86
dc
hexidecimal</td></tr>
<tr><td>7</td><td>Search “UDP” in Google and determine the fields over which the UDP checksum is calculated.</td><td>The checksum is calculated by summing up all the 16-bit words using one’s compliment, then one is complementing that sum it yields the checksum. The sum is calculated all the 16-bit words in the IP and UDP header, plus the payload:
Source IP (IP)
Destination IP (IP)
Protocol (IP)
Length (IP)
Source port (UDP)
Destination port (UDP)
Length (UDP)
Payload (UDP)</td></tr>
<tr><td>Annotated Screenshots (if needed)</td><td colspan="2">Internet Protocol Version 4, Src: 35.183.180.149, Dst: 10.0.0.230
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
› Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 189
Identification: 0xaf4d (44877)
› Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 48
Protocol: UDP (17)
Header Checksum: 0xb7b0 [validation disabled]
[Header checksum status: Unverified]
Source Address: 35.183.180.149
Destination Address: 10.0.0.230
User Datagram Protocol, Src Port: 57904, Dst Port: 60213
Source Port: 57904
Destination Port: 60213
Length: 169
Checksum: 0x9165 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
› [Timestamps]
UDP payload (161 bytes)</td></tr>
</table>

8	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 port of the first packet is the destination port of the second packet, and the destination port of the first packet is the source port of the second packet.
Annotated Screenshots (if needed)