Wireshark Lab 2: UDP

Group Details:

Leo Hanxu 1006045067 Shaoyang Zhang 1005751660

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 4 main fields including Source port, Destination port, Length, Checksum. There are also other fields like Stream Index, Timestamps.
Annotated Screenshots (if needed)	<pre>VUser Datagram Protocol, Src Port: 50004, Dst Source Port: 50004 Destination Port: 49553 Length: 1153 Checksum: 0x1c4d [unverified] [Checksum Status: Unverified] [Stream index: 0] V[Timestamps] [Time since first frame: 0.0000000000 sec [Time since previous frame: 0.00000000000 UDP payload (1145 bytes)</pre>	conds]
2	From the packet content field, determine the length (in bytes) of each of the UDP header fields.	Each field contain 2 bytes
Annotated Screenshots (if needed)	> Frame 18: 212 bytes on wire (1606 bits), 212 bytes captured (1606 bits) on interface \Deviorable 1 thermet II, sec: 80:00:00 00:00:00 (80:00:00:00:00), but: intellor_16:ac:10 (f8:59:71:10:00:00), but: intellor_16:ac:10 (f8:59:71:10:00:00:00:00:00:00:00:00:00:00:00:00	eV 000 fig 59 71 k1 es 10 90 eV 000 90 eV 00 eV

3	The value in the Length field is the length of what? Verify your claim with your captured UDP packet.	This is the sum of the length of the UDP header which is 8 byte and the length of the data. 1153=8+1145
Annotated Screenshots (if needed)	<pre>V User Datagram Protocol, Src Port: 50004, Source Port: 50004 Destination Port: 49553 Length: 1153 Checksum: 0x40c0 [unverified] [Checksum Status: Unverified] [Stream index: 0] * [Timestamps] [Time since first frame: 0.000000000 [Time since previous frame: 0.0000000 UDP payload (1145 bytes) Data (1145 bytes) Data: 9065f9d0ebdd6a8b0000d11cbede0003 [Length: 1145]</pre>	seconds]
4	What is the maximum number of bytes that can be included in a UDP payload.	The maximum length $2^{16} - 1 = 65535$ bytes Excluding the length of the header, the maximum number of payload is 65527 bytes
Annotated Screenshots (if needed)		
5	What is the largest possible source port number?	largest port number is $2^{16} - 1 = 65535$
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.)	17, or 0x11

Annotated Screenshots (if needed)	<pre>Internet Protocol Version 4, Src: 109.200.210.38, Dst: 192.168.0.14 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 1173 Identification: 0x8ec3 (36547) Flags: 0x40, Don't fragment Fragment Offset: 0 Time to Live: 57 Protocol: UDP (17) Header Checksum: 0xadef [validation disabled] [Header checksum status: Unverified] Source Address: 109.200.210.38 Destination Address: 192.168.0.14</pre>	
7	Search "UDP" in Google and determine the fields over which the UDP checksum is calculated.	the entire payload, and the other fields in the header, and some fields from the IP header
Annotated Screenshots (if needed)		
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 and the destination port will be exchanged
Annotated Screenshots (if needed)		200.210.38 UDP 98 49553 + 50004 Len=56 168.0.14 UDP 1180 50004 + 49553 Len=1138