Tevin Jeffrey – CS 356

**Wireshark Lab 4**

**1. Select one packet. From this packet, determine how many fields there are in the UDP header. (Do not look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.**

*User Datagram Protocol, Src Port: 443 (443), Dst Port: 53274 (53274)*

*Source Port: 443*

*Destination Port: 53274*

*Length: 1358*

*Checksum: 0x1671 [validation disabled]*

*[Stream index: 7]*

The fields are:

* Source Port
* Destination Port
* Length
* Checksum

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

The UDP header fields are two byes each.

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

The length is the number of bytes in payload minus 8 bytes (The size of the headers itself!).

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

The practical limit for the data length which is imposed by the underlying IPv4 protocol is 65,507 bytes (65,535 − 8 byte UDP header − 20 byte IP header). From what I’ve gathered you don’t want to send a packet that large as it may lead to fragmentation. e.g Ethernet has a MTU of 1500 bytes.

*Source: TCP/IP: Protocol Suite, 1st ed. New Delhi, India: Tata McGraw-Hill Publishing Company Limited.*

**5. What is the largest possible source port number?**

2 bytes = 28 or 65536 possible values.

**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.)**

Protocol 1710, or 1116

**7. Search “UDP” in Google and determine the fields over which the UDP checksum is calculated.**

Checksum is the 16-bit one's complement of the one's complement sum of a pseudo header of information from the IP header, the UDP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Source: RFC 768 https://tools.ietf.org/html/rfc768

**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.**

*Packet 1: User Datagram Protocol, Src Port: 62485 (62485), Dst Port: 59786 (59786)*

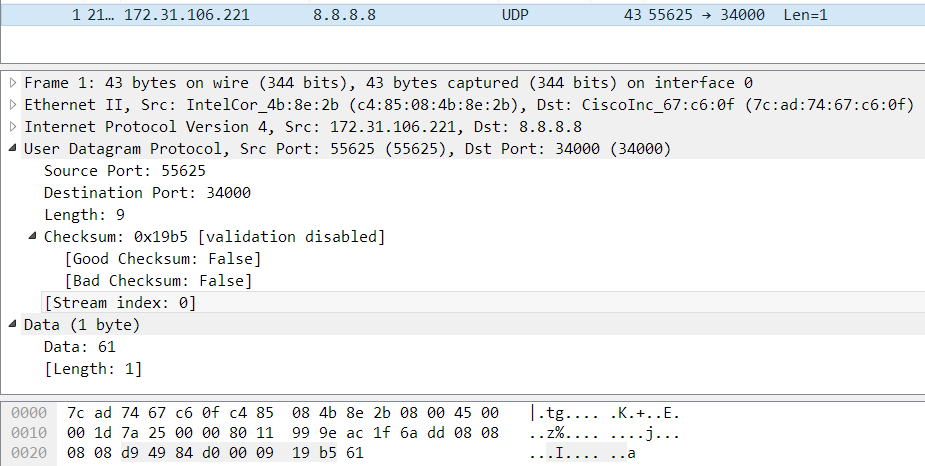
*Packet 2: User Datagram Protocol, Src Port: 59786 (59786), Dst Port: 62485 (62485)*

It seems as though the request and reply were on corresponding ports.

**Extra Credit 1. Capture a small UDP packet. Manually verify the checksum in this packet. Show all work and explain all steps.**

I used netcat to send a single ascii char to 8.8.8.8:34000

*echo -n ‘a’ | nc -4u -w1 8.8.8.8 34000*



Divided into 16-bit chunks.

**Source ip address (172.31.106.221):** 0xAC1F, 0x6ADD | 1010110000011111, 0110101011011101

**Destination ip address (8.8.8.8):** 0x0808, 0x0808 | 0000100000001000, 0000100000001000

**Zero padded protocol:** 0x0011 | 0000000000010001

**UDP length, which is 8 bytes header + 1 byte payload:** 0x0009 | 0000000000001001

**UDP source port (55625):** 0xD949 | 1101100101001001

**UDP destination port (34000):** 0x84D0 | 1000010011010000

**UDP length, which is 8 bytes header + 1 byte payload:** 0x0009 | 0000000000001001

**UDP payload (which is the ascii char ‘a’):** 0x0061 | 0000000001100001

Adding them up should = the checksum.