Solution to Wireshark Lab: UDP

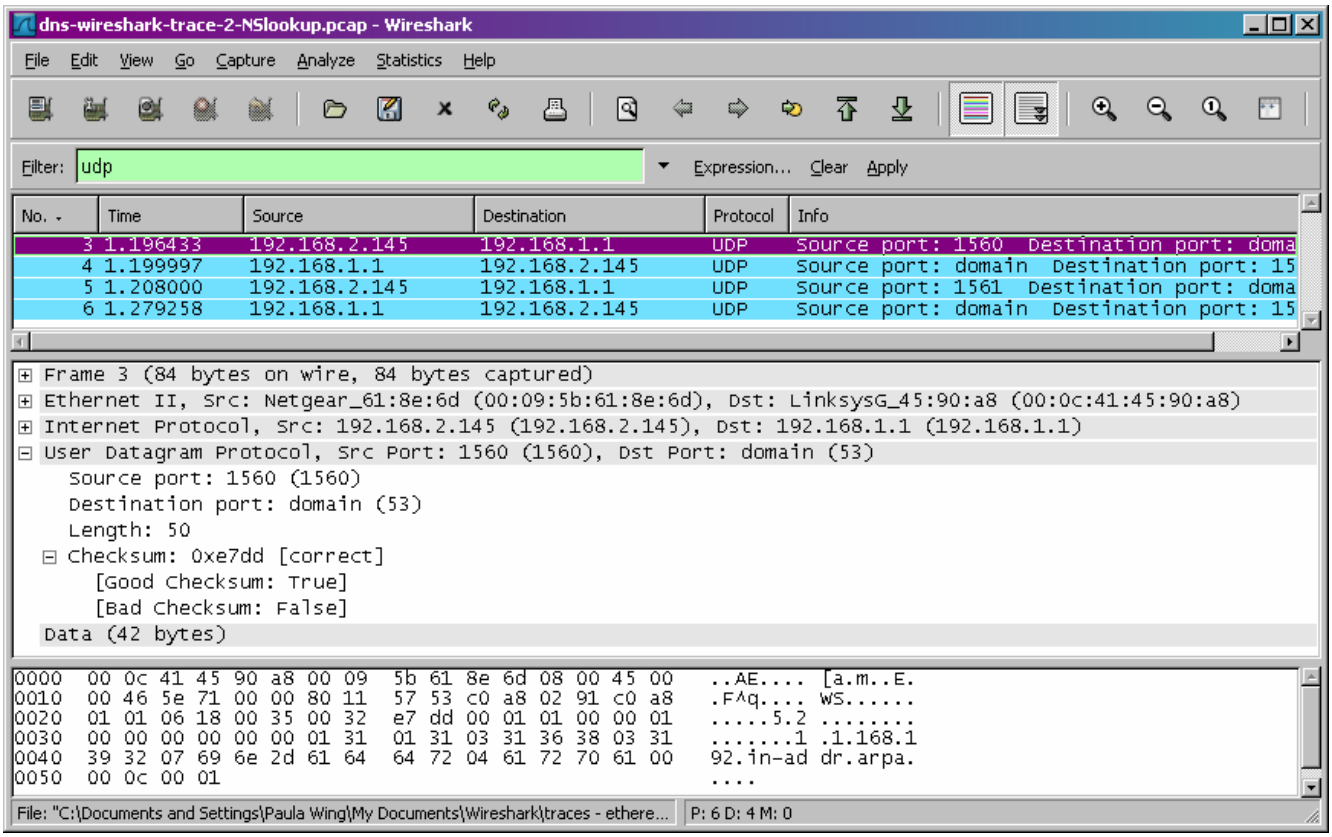

Fig. 1: UDP Header Fields

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.

   The UDP header contains 4 fields: source port, destination port, length, and checksum.

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

   Each of the UDP header fields is 2 bytes long.

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 sum of the 8 header bytes, plus the 42 encapsulated data bytes.

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

   The maximum number of bytes that can be included in a UDP payload is $2^{16} - 1$ less the header bytes. This gives 65535 – 8 = 65527 bytes.

5. What is the largest possible source port number?

   The largest possible source port number is $2^{16} - 1 = 65535$.

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 IP protocol number for UDP is 0x11 hex, which is 17 in decimal value.

7. Search "UDP" in Google and determine the fields over which the UDP checksum is calculated.

   The UDP checksum is calculated as 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. This is padded as needed with zero bytes at the end to make a multiple of two bytes. If the checksum is computed to be 0, it must be set to 0xFFFF

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.

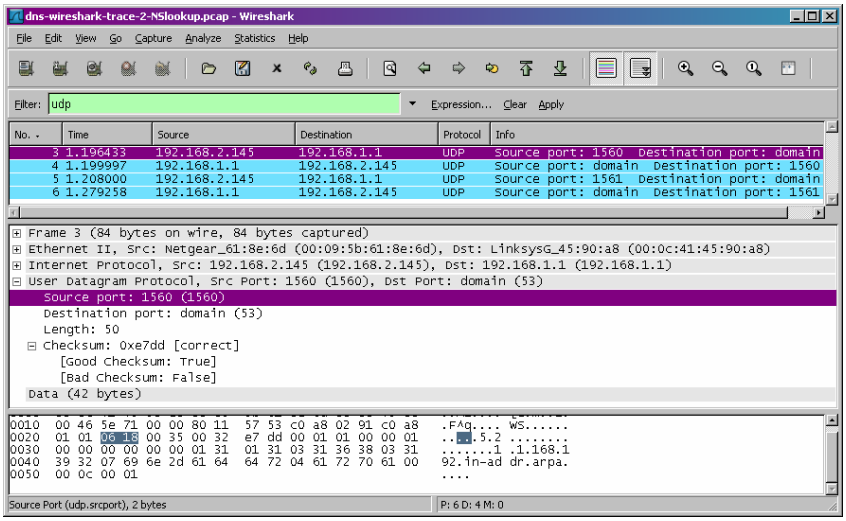

Fig. 2: UDP sent by my host

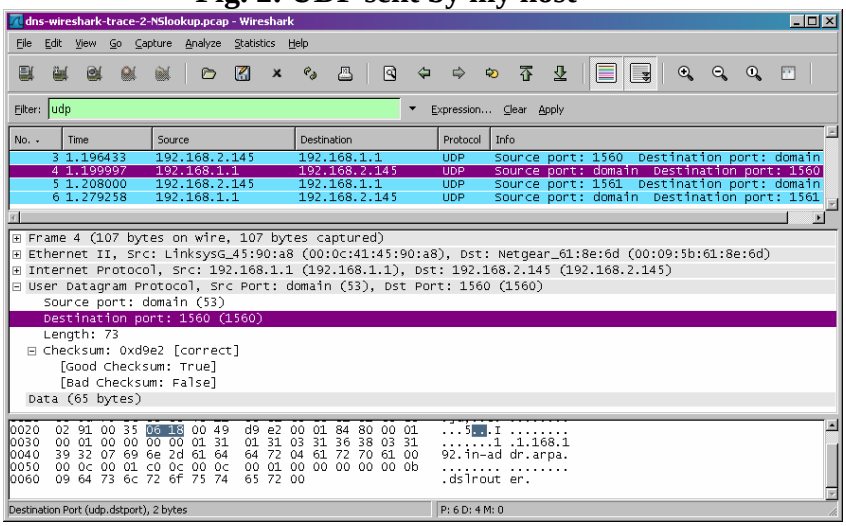

Fig. 3: UDP reply to my host

The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.

Extra Credit

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

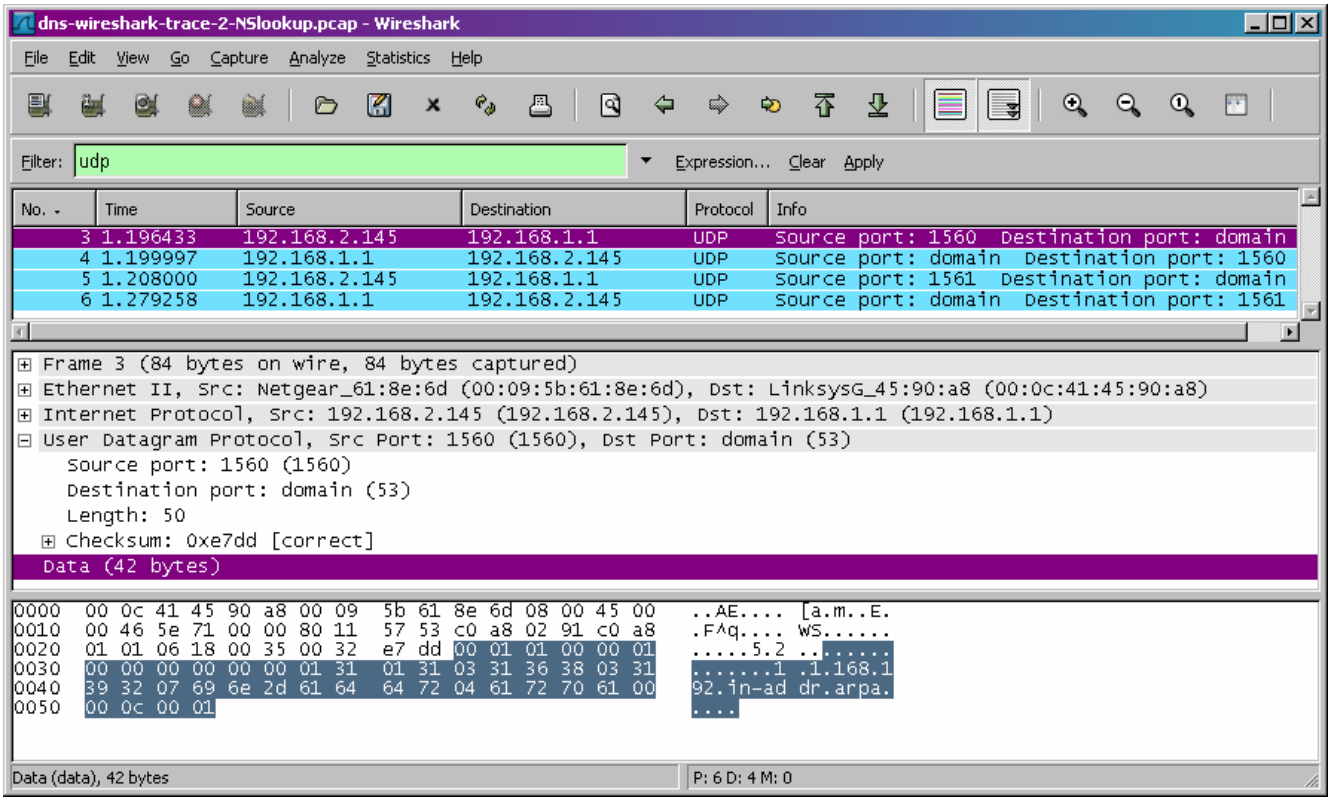

Fig. 4: UDP packet for checksum calculation

Take the following fields from the packet containing 42 bytes of data shown in figure 4 above. All calculations are done using the hex values.

Field	Hex value
IP header: Source IP address	c0a8
…	0291
IP header: Destination IP address	c0a8
…	0101
IP header: Protocol number(zero padded on left)	0011
16 bit UDP Length	0032
UDP header: source port	0618
UDP header: destination port	0035
UDP header: length	0032
UDP Data	0001
…	0100
	0001
	0000
	0000
	0000
	0131
	0131
	0331
	3638
	0331
	3932
	0769
	6e2d
	6164
	6472
	0461
	7270
	6100
	000c
	0001
Sum all hex values	181e
Carry	4
Add in the carry	1822
1s complement = checksum!	E7dd