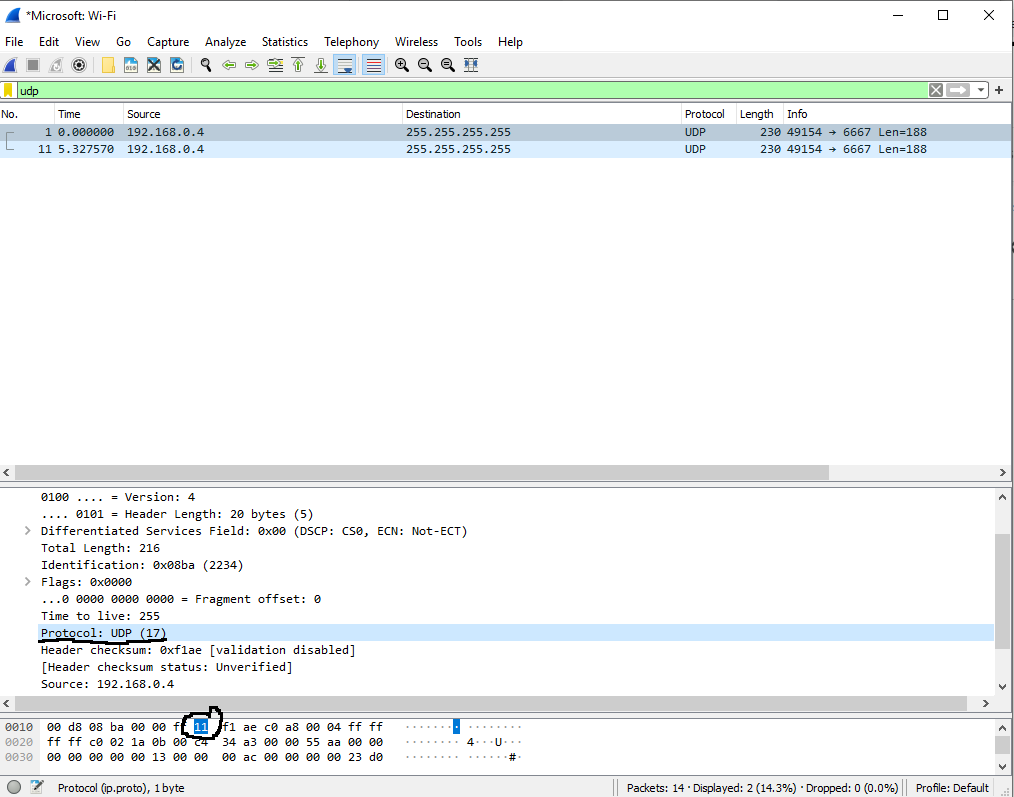
**COMPSCI-4C03 Networks and Security Assignment 3**

**Question 1: Understanding UDP Protocol**

**#1-A: Add the answer to q6 in UDP lab. To support your answer, add the screen shot and highlight the field from where you figured out the answer.**

*What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation?*

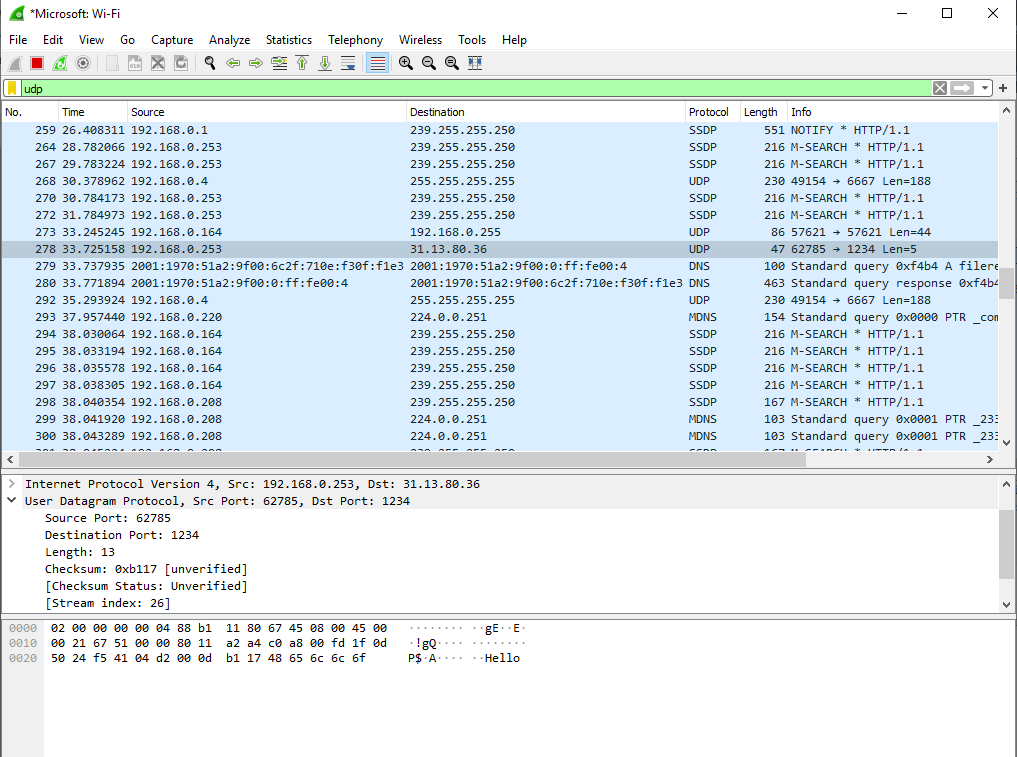
****

As clearly seen in the above screenshot, UDP’s protocol number is 17 as a decimal, and 0x11 in hexadecimal notation. I have highlighted these fields in the wireshark packet contents body above.

**#1-B: Select the smallest UDP segment from the trace that you have analysed in this assignment. Using the content of this segment, explain the process of checksum calculation for this segment. Use hexadecimal numbers to simplify the calculations.**

To calculate UDP checksum, we first must know that in addition to its own header, UDP checksum uses a pseudo header, consisting of the original source IP, destination IP, reserved (0000 0000), protocol (0x11), and the length from the UDP header. This get’s added with the actual UDP header, consisting of a source port, destination port, length, and actual data.

The following screenshot illustrates the UDP packet I used for this question. It has as it’s data the string “Hello.”



|  |  |  |
| --- | --- | --- |
| **Byte #** | **Data/Content (in hex)** | **Current rolling sum** |
| **PSEUDO HEADER** | **PSEUDO HEADER** | 0 |
| 26-29 (Source IP) | C0A8  00FD | C1A5 |
| 30-33 (Destination IP) | 1F0D  5024 | 130D6 -> 30D7 (after overflow) |
| 23 (UDP Protocol) plus reserve | 0011 | 30E8 |
| 38-39 (UDP Length) | 000D | 30F5 |
| **UDP HEADER** | **UDP HEADER** | 30F5 |
| 34-35 (UDP Source port) | F1AA | 1229F -> 22A0 (after overflow) |
| 36-37 (UDP Destination port) | 04D2 | 2772 |
| 38-39 (UDP Length) | 000D | 277F |
| 42-46 (UDP Data) | 4865  6c6c  6f00 | 4B51 |
| **TAKE ONE’S COMPLEMENT** |  | **FFFF – 4B51 = B4AE (Calculated Checksum)** |
| 40-41 (Actual Checksum) | 0xB4AE | **CORRECT!!!!** |

Comparing my calculated checksum with the actual wireshark captured checksum, we can verify that my solution was correct.