COMP 3721 **Assignment 4**

Note:

- Submit a single PDF file.
- Answer the questions according to textbook, lecture notes and class discussions, not ChatGPT or Google.

The beginning bytes of two IP packets are shown as follows. Data are in hexadecimal.

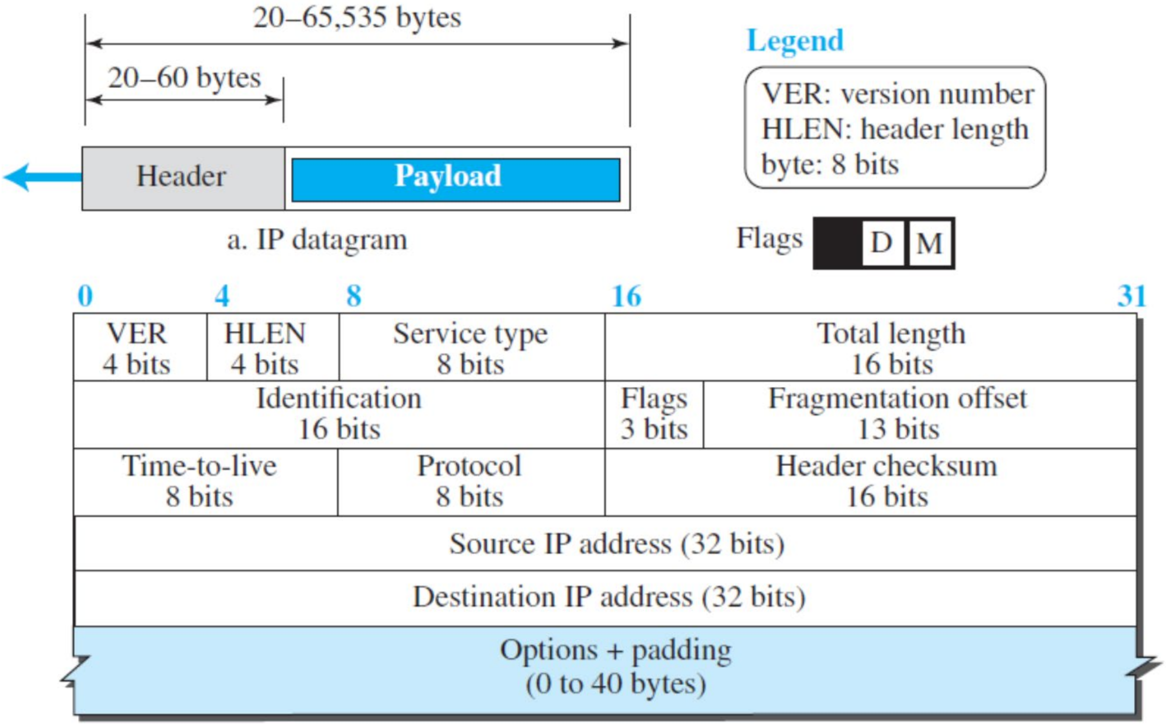
Packet 1:

```
45 00 05 DC
A5 E5 20 00
80 01 00 00
51 1C 9A 62
17 D5 E6 9A …
```

Packet 2:

```
45 00 05 DC
A5 E5 00 B9
80 01 00 00
51 1C 9A 62
17 D5 E6 9A …
```

The IP datagram format is shown below for your reference.



a. IP datagram

b. Header

Flags (3-bit field):
R: Reserved. Always 0.
D: If set to 1, the datagram must not be fragmented
M: 0 for the last or only fragment

Some protocol values:

ICMP:	01
TCP:	06
UDP:	17

Q1:

Find the following for packet 1.

(a) Version number
(b) Header length (in bytes)
(c) Confirm that service type is 0.
(d) Total length of IP packet (in bytes)
(e) Identification number (in decimal)
(f) Can we fragment this IP packet?
(g) Are there more fragments following this IP packet?
(h) Fragmentation offset of this packet (in decimal)
(i) Time-to-live (in decimal)
(j) Protocol (e.g., ICMP, TCP, UDP, etc.)
(k) Check that the header checksum is 0x0000 (not calculated). Calculate the checksum according to the lecture notes. Write the answer in hexadecimal.
(l) Source IP address (in dotted decimal)
(m) Destination IP address (in dotted decimal)

Q2:

Find the following for packet 2.

(a) Version number
(b) Header length (in bytes)
(c) Confirm that service type is 0.
(d) Total length of IP packet (in bytes)
(e) Identification number (in decimal)
(f) Can we fragment this IP packet?
(g) Are there more fragments following this IP packet?
(h) Fragmentation offset of this packet (in decimal)
(i) Time-to-live (in decimal)
(j) Protocol (e.g., ICMP, TCP, UDP, etc.)
(k) Check that the header checksum is 0x0000 (not calculated). Calculate the checksum according to the lecture notes. Write the answer in hexadecimal.
(l) Source IP address (in dotted decimal)
(m) Destination IP address (in dotted decimal)

Q3:

(a) Assuming that these two packets are the fragments that belong to the same packet (note the identification numbers), which packet is the first fragment and which is the last? Why?
(b) Using Wireshark, find the above packets in the given “icmp.cap” file. Show the filter used in Wireshark, and identify their frame numbers (e.g., packet 1 is frame 64 and packet 2 is frame 100).
(Note 1: Use the answer(s) you have in Q1 and Q2 to construct suitable filter(s).)
(Note 2: Frame number is the first column in Wireshark, denoted as “No.”.)

— End of Assignment 4 —