CS425A: Assignment 3

Shrilakshmi S K (211012)

April 5, 2024

1 Question 1

In the captured IP packet header, the content of the upper layer protocol field is designated as 0x01. This specific value signifies that the protocol utilized in the upper layer corresponds to ICMP (Internet Control Message Protocol).

2 Question 2

In the packet capture provided, the IP header is 20 bytes long. To find out how many bytes the payload of the IP datagram contains, we subtract the length of the IP header from the IP datagram's total length. The total length of the IP datagram, as shown in the IP header, is 56 bytes. When we subtract the 20-byte IP header from this total, we get: 56 bytes - 20 bytes = 36 bytes. So, the payload of the IP datagram is 36 bytes. This was determined by taking the total length of the IP datagram and subtracting the length of the IP header, as outlined in the packet capture information.

3 Question 3

According to the provided packet data, there is no evidence to suggest that the IP datagram has undergone fragmentation. This assessment is made by examining the fragmentation offset field within the IP header, which holds a value of 0. In instances where an IP datagram is fragmented, this fragmentation offset field would present a value greater than 0, and the more fragments

flag, located in the flags field, would be marked as 1. However, in this particular packet, both the fragmentation offset and the more fragments flag are recorded as 0, signifying that the datagram has remained unfragmented.

4 Question 4

The Identification field holds a value of 0x80b2, which equates to 32946 in decimal notation. In the TTL (Time to Live) field, the value is set at 1.

5 Question 5

Yes, the message linked to the given packet has been fragmented. This conclusion is drawn from the "Info" column in the packet details, where the protocol is labeled as "Fragmented IP protocol" This point indicates that the original IP datagram was split into more than one piece during its transmission. Furthermore more protocol flag is set to 1.

6 Question 6

The presence of a 0 value in the fragment offset field, combined with the setting of the more fragments field to 1, serves as an indication that the datagram has undergone fragmentation.

7 Question 7

The fragment offset field, with a value of 0, signifies that this is the initial fragment of the datagram. Latter fragments will have non-zero offset values.

8 Question 8

The fragment offset, with a value of 1480 instead of 0, indicates that this fragment is not the initial one, but a latter one.

9 Question 9

No, there are no additional fragments. This conclusion is based on the fact that the more fragments field is unset, indicated by its value being 0.

10 Question 10

Between the first and second fragments, changes occur in four distinct fields within the IP header. These alterations, presented in their sequential appearance, include:

- Total Length: This field changes from an initial value of 1500 in the first fragment to 520 in the second. It signifies the overall length of the fragment, including the header and data.
- Flags: The modification here is from 0x02 in the first fragment to 0x00 in the second. The change is indicative of the "more fragments" flag; initially set to signal more fragments are to follow, and then cleared to indicate the final fragment.
- Fragment Offset: This field shifts from 0 in the first fragment to 1480 in the second fragment. The offset indicates the position of the fragment's data within the original data payload.
- Header Checksum: There's a change from 0xda69 in the first fragment to 0xfd84 in the second fragment. The checksum ensures integrity of the IP header; its change reflects the alterations in the header due to the fragmentation process.