**Wireshark Lab 4: IP**

**Group Details:**

Bahareh Farhadi 1003975282

Jingfeng Chen 1000411262

**Mark:**

|  |  |  |
| --- | --- | --- |
|  | **Question** | **Answer** |
| 1 | Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window.  What is the IP address of your computer? | 192.168.1.102 |
| 2 | Within the IP packet header, what is the value in the upper layer protocol field? | ICMP (1) |
| 3 | How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes. | 20 bytes |
| 4 | Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented. | I don’t think this datagram is fragmented because when ip.fragment is applied in Wireshark, this packet was filtered out. It is probably due to its size being smaller than MTU. |
| 5 | Which fields in the IP datagram always change from one datagram to the next  within this series of ICMP messages sent by your computer? | As the lab files indicated, the Identification field is being incremented 1 every time. |
| 6 | Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why? | The source IP and destination IP, the version number, and the protocol version stayed constant. The identification, checksum had to change are from different packets, therefore, they will have to change. |
| 7 | Describe the pattern you see in the values in the Identification field of the IP datagram | It is increased by one every time. |
| 8 | What is the value in the Identification field and the TTL field? | 0xa60b (43507)  244 |
| 9 | Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why? | Identification increases by one every time, but TTL value remains to be 244. It is because TTL has to remain the same for the return message to be delivered successfully. |
| 10 | Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram? | Yes, the packet is fragmented. |
| 11 | Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment?  How long is this IP datagram? | The more fragments is set to Set.  The fragment offset is 0.  The total length is 1500. |
| 12 | Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more  fragments? How can you tell? | The more fragment is set to Not set.  The fragment offset is not 0. |
| 13 | What fields change in the IP header between the first and second fragment? | More fragments, Fragment offset, checksum, and total length. |
| 14 | How many fragments were created from the original datagram? | 2 |
| 15 | What fields change in the IP header among the fragments? | More fragments, Fragment offset, checksum, and total length. |