Matt Kennedy
Brent Thompson

CIS 457
Section 101
Lab 10

1. What frame number is this packet? And at what time was it sent?
8 bytes, 21:48:02

2. Within the IP packet header, what is the value in the upper layer protocol field?
0100

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.
IP Header has 20 bytes, payload of IP datagram has 36 bytes. There is a total of 56 bytes, so 56 - 20 = 36 bytes for the payload.

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
No, it has not been fragmented. The more fragments bit is 0.

5.Which fields in the IP datagram header always change from one datagram to the next within this series of ICMP messages sent by the sending computer?
The sequence number in the check zone always change from one datagram to the next.

6.Which fields stay constant? Why?
Version, header length, source IP, destination IP all stay constant.

7.Describe the pattern you see in the values in the Identification field of the IP datagram
IP Header identification fields are all incremented by 1 for every echo request.

8.What is the value in the Identification field and the TTL field?
TTL - 1, Identification - 13128.

9.Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to the sending computer by the nearest (first hop) router? Why?
No, the identification changes. The ID field is a unique value for each reply.

10.Has that message been fragmented across more than one IP datagram? Record the Wireshark's frames numbers.

Yes, 102, 104, 106

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?
There is a flag for more fragments, which is true.The datagram offset is 0. The 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 there more fragments? How can you tell?
The fragment offset is not 0. There are not more fragments, the more fragments flag is false.

13. What fields change in the IP header between the first and second fragment?
Total length, checksum, fragment offset, more fragments flag.

14. How many fragments were created from the original datagram? And what fields change in the IP header among the fragments?
3 fragments created. Fragment offset and checksum.

15.What is the anycast ip address and how it is used to implement load distribution, reduce service delay and reduce the potential of DoS attack?
From https://www.incapsula.com/blog/how-anycast-works.html: In anycast, a collection of servers share the same IP address and send data from a source computer to the server that is topographically the closest. The main principle of anycast is that an IP address range is advertised in the BGP messages of multiple routers. As routers become full, the recipient address can migrate to other servers or routers that are able to take the traffic, instead of slowing down traffic by staying. This also applies to DOS attacks.