Chris Banci

CS436

11/27/17

Lab 5 - Wireshark IP Layer

1. What is the IP address of your computer?

* 192.168.0.7

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.

* 36 bytes are in the payload of the IP datagram.
* It can be determined by subtracting the ip header (20 bytes) from the total length (56 bytes).

4. Has this IP datagram been fragmented? Explain how you determined whether or

not the datagram has been fragmented.

* No the IP datagram has not been fragmented because the more fragments field is not set.

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?

* The identification, header checksum, time to live fields always change from one datagram to the next.

6. Which fields stay constant? Which of the fields must stay constant? Which fields

must change? Why?

* The fields that must stay constant are :
  + Version (IPV4 always used)
  + Differentiated services (all ICMP packets)
  + Header length (all ICMP packets)
  + Source ip (sending from same source)
  + Destination ip (sending to the same destination)
  + Upper layer protocol (all ICMP packets)
* The fields that must change are:
  + Identification (must be unique)
  + Header checksum (must change since header changes)
  + Time to live (must increment)

7. Describe the pattern you see in the values in the Identification field of the IP

* The identification field is decreasing when source is in descending order for ICMP messages.

8. What is the value in the Identification field and the TTL field?

* Identification = 38230
* TTL = 64

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?

* The identification field changes because it must be a unique number, but TTL remains unchanged because the first hop is always the same.

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?

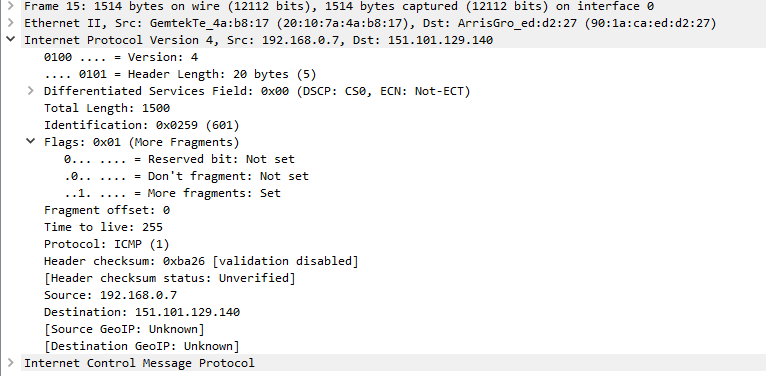
* Yes it has been fragmented across more than one IP datagram.

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?

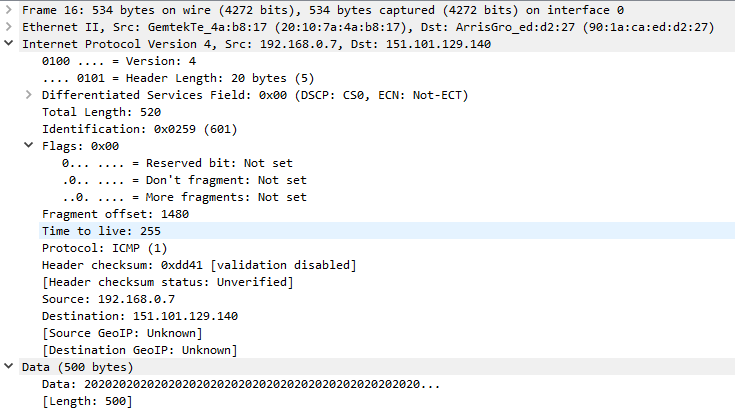


* The flag bit for more fragment being set indicates the datagram has been fragment.
* The fragment offset being 0 indicates this is the first fragment.
* The length of the IP datagram is indicated by the total length field which is 1500.

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 fragment offset (1480) indicates this is not the first datagram fragment.
* There are no more fragments because the flag bit for more fragments is not set.

13. What fields change in the IP header between the first and second fragment?

* The total length, fragment offset, the flag bit for more fragments.

14. How many fragments were created from the original datagram?

* Three fragments were created from the original datagram.

15. What fields change in the IP header among the fragments?

* Fragment 1 - 2 = the fragment offsets and checksums
* Fragment 2 - 3 = total length, more fragment flag bit and fragment offset.