Andrew Jenkins
Nathan Robertus

The Captured Trace

1. **Select the first ICMP Echo Request message sent by your computer, what is the IP address of your computer? (1pt)**
   - 192.168.1.102

2. **Within the IP packet header, what is the value in the upper layer protocol field? (1pt)**
   - 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. (2pts)**
   - Header - 20 bytes
   - Payload - 64 bytes
   - Total length was 84, minus 20 for header = 64 for payload

4. **Has this IP datagram been fragmented? Justify your answer. (1pt)**
   - No, the fragment bit isn't set

Sort the traced packets according to IP source address. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol portion in the "details of selected packet header" window. In the "listing of captured packets" window, you should see all of the subsequent ICMP messages below this first ICMP.

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? (1pt)**
   - Identification, TTL, Header Checksum

6. **Which fields stay constant? Which of these fields must stay constant? Which fields must change? Justify your answer. (2pts)**
   - Total length is constant here but could vary based on payload length.
   - All of the following are constant and must stay constant.
     - Version
       - ipv4 on all requests
     - Header Length
       - icmp has header length of 20
     - Source IP
       - sending from same source

    - Destination IP
        - sending to same destination
    - Differentiated Services
        - All ICMP use same services
    - Upper Layer Protocol
        - All ICMP use ICMP protocol
- Must change
    - Identification
        - each packet has to be unique
    - TTL
        - It gets incremented in between packets
    - Header checksum
        - Changes since ID and TTl change

7. **Describe the pattern you see in the values of the Identification field of the IP datagram. (1pt)**

- It increments by 1 each subsequent request

Find the series of ICMP TTL-exceeded replies sent to your computer by the first-hop router.

8. **What is the value in the Identification field and the TTL field? (1pt)**

- ID: 0x9d7c (40316)
- TTL: 255

9. **Do these values remain unchanged for all ICMP TTL-exceeded replies sent to your computer by the first-hop router? Justify your answer. (1pt)**

- ID changes because the Datagrams are separate, so each needs a unique identifier.
- TTL doesn't change because the TTL to the first hop router is always the same.

Fragmentation

Sort the packet listing according to time by clicking on the Time column.

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? (1pt)**

Yes, “more fragments” is shown in the packet.

11. **Look at 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? What is the length of this IP datagram? (2pts)**

The frag flag has been set, so that indicates that more are coming.

12. **Look at 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?**
Justify your answer. (3pts)

The offset is not zero, so that means it cannot be the first.

13. **What fields change in the IP header between the first and second fragments? (1pt)**

Length, flags, fragmentation offset, and the header checksum.

Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500.

14. **How many fragments were created from the original datagram? (1pt)**

2 fragments

15. **What fields change in the IP header among the fragments? (1pt)**

The offset and checksum change.