Joshua Larkin

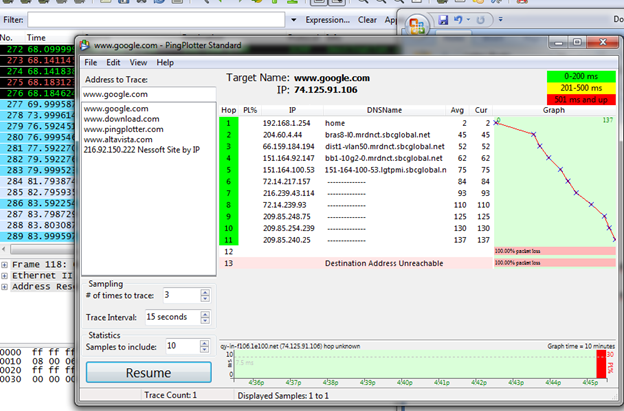
CSC 251

Net-Centric

Spring 2012

**Wireshark Lab 4: IP**

**1. Capturing packets from an execution of traceroute:**

****

**2. A look at the captured trace:**

**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?**

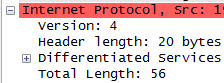
*My IP address is 192.168.1.69.*

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

*ICMP.*

**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.**

*The IP header is 20 bytes. The payload is 36 bytes. This is found by subtracting the Total Length of the IP datagram by the header:*

****

**4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.**

*The IP datagram has not been fragmented. This was determined by looking at the More Fragments Flag, which is set to 0.*

**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 field, the Header checksum field and the Time to live field.*

**6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?**

*The destination must stay constant because we are attempting a trace over a series of packets to one source. The Time to live must increase because this is what generates the return packets we're interested in. The Header checksum and Identification fields must change because these are unique for each packet.*

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

*It increases proportionally to the change in the Time to live value.*

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

*Identification: 0x408d.*

*TTL: 255.*

**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?**

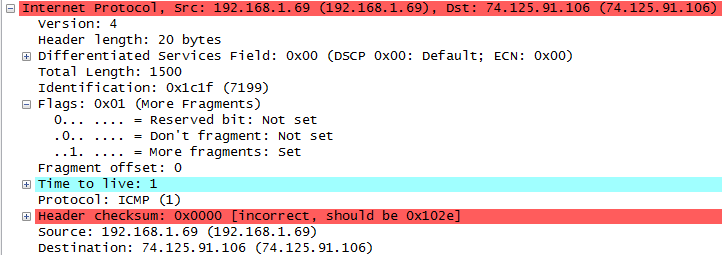
*The Identification field changes because this must be unique, but the TTL field stays at 255. This is because the router wants the packet to return to us and puts the highest limit it can on how much time the packet stays alive.*

**Fragmentation:**

**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?**

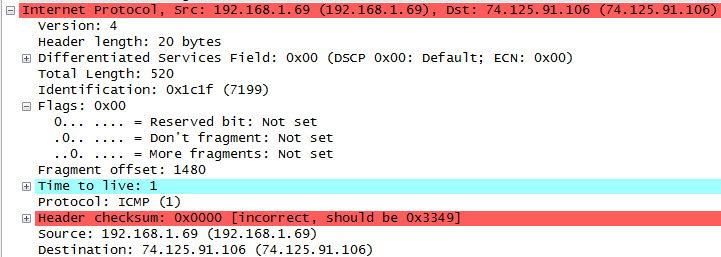
*Yes. The More fragments flag is set to 1.*

**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 flag lets us know that it is fragmented. The fragment offset is 0 so we know it is the first fragment. The IP datagram is 1500 bytes.*

**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?**

****

*This is not the first datagram fragment because it has an offset. There are no more fragments after this one because the More fragments flag is not set.*

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

*Total Length, Flags, and Offset.*

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

*Three.*

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

*Total Length, Flags, and Offset.*