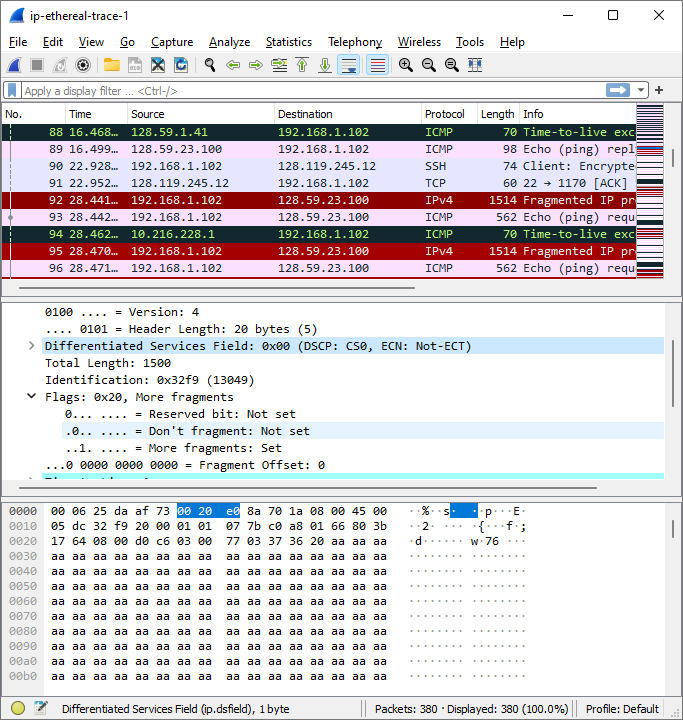
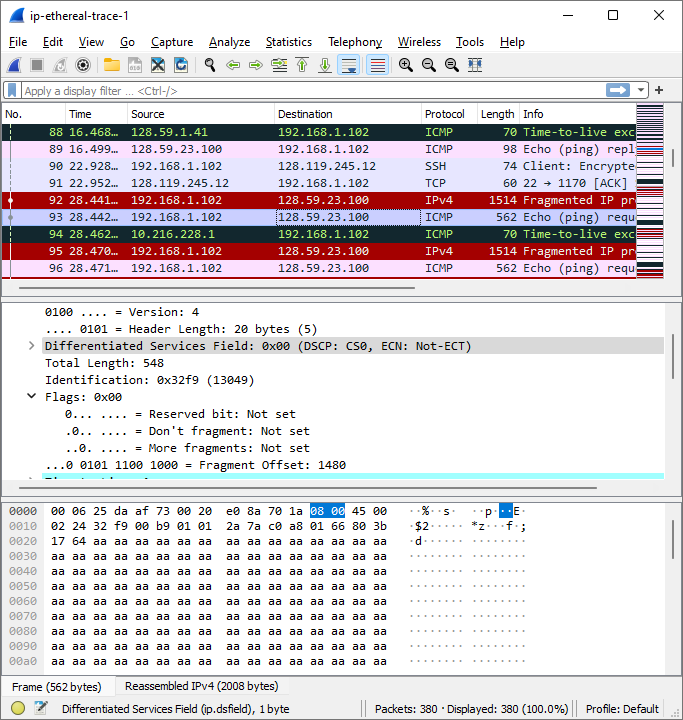
* 1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?
     1. My IP address is 192.168.1.100
  2. Within the IP packet header, what is the value in the upper layer protocol field?
     1. The value for the upper layer protocol is 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.
     1. There are 20 bytes in the IP header, and since the total length is 56 bytes, that means the payload is 36 bytes.
  4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.
     1. Since the more fragments bit is 0, that means that the data was not fragmented
  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?
     1. Time to Live, Header checksum, and identification seem to 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?
     1. Stay constant
        1. Version, header length, source and destination IP, Differentiated Services, Upper layer protocol
     2. Must stay constant
        1. Version, header length, source and destination IP, Differentiated Services, Upper layer protocol (They are the same as can stay constant)
     3. Must change
        1. Identification, Time to live, and Header checksum
  7. Describe the pattern you see in the values in the Identification field of the IP datagram
     1. The pattern that I see for the values in the identification field is that it increments by one after every echo request
  8. What is the value in the Identification field and the TTL field?
     1. The value for the identification field is 40316 and the value for the TTL field is 56
  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?
     1. The TTL field remains unchanged because the first hop router does not change. The identification field though changes because the identification value is a unique value and if they didn’t have a unique value then it means that they are fragments of a larger datagram.
  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?
      1. Yes, the message was 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?
      1. The information in the header that says the data is fragmented is that the flag for more fragments is now set. The way we know that this is the first is that the fragmentation offset is now set to 0 where latter it is 1480.The total length is 1500.
      2. 
  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?
      1. You can tell it is not the first fragment because the fragment offset is now 1480. There are no more fragments because the more fragments flag is no longer set.
      2. 
  13. What fields change in the IP header between the first and second fragment?
      1. Length, the more fragments flag, the fragment offset, header checksum
  14. How many fragments were created from the original datagram?
      1. Three fragments
  15. What fields change in the IP header among the fragments?
      1. The fragment offset, checksum are different between the three. Also though, the first two have lengths of 1500 and also have the more fragments flags set, but the last one has a length of 540 and no flag set.

**Trace 1**

C :\Users\kv str\Downloads\ip-ethereal-trace-1 380 total packets, 380 shown No. Time Source Destination Protocol Length Info 9 6.176826 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit) Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) Ethernet II, Src: LinksysG\_da:af:73 (00:06:25:da:af:73), Dst: Actionte\_8a:70:1a (00:20:e0:8a:70:1a) Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.102 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT) Total Length: 56 Identification: 0x9d7c (40316) Flags: 0x00 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 255 Protocol: ICMP (1) Header Checksum: 0x6ca0 [validation disabled] [Header checksum status: Unverified] Source Address: 10.216.228.1 Destination Address: 192.168.1.102 Internet Control Message Protocol Type: 11 (Time-to-live exceeded) Code: 0 (Time to live exceeded in transit) Checksum: 0xd946 [correct] [Checksum Status: Good] Unused: 00000000 Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100 0100 .... = Version: 4 .... 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 84 Identification: 0x32d0 (13008) Flags: 0x00 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 1 Protocol: ICMP (1) Header Checksum: 0xf616 [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.102 Destination Address: 128.59.23.100 Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0xf7ca [unverified] [in ICMP error packet] [Checksum Status: Unverified] Identifier (BE): 768 (0x0300) Identifier (LE): 3 (0x0003) Sequence Number (BE): 20483 (0x5003) Sequence Number (LE): 848 (0x0350)