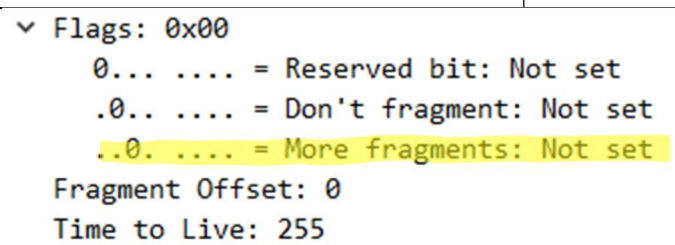
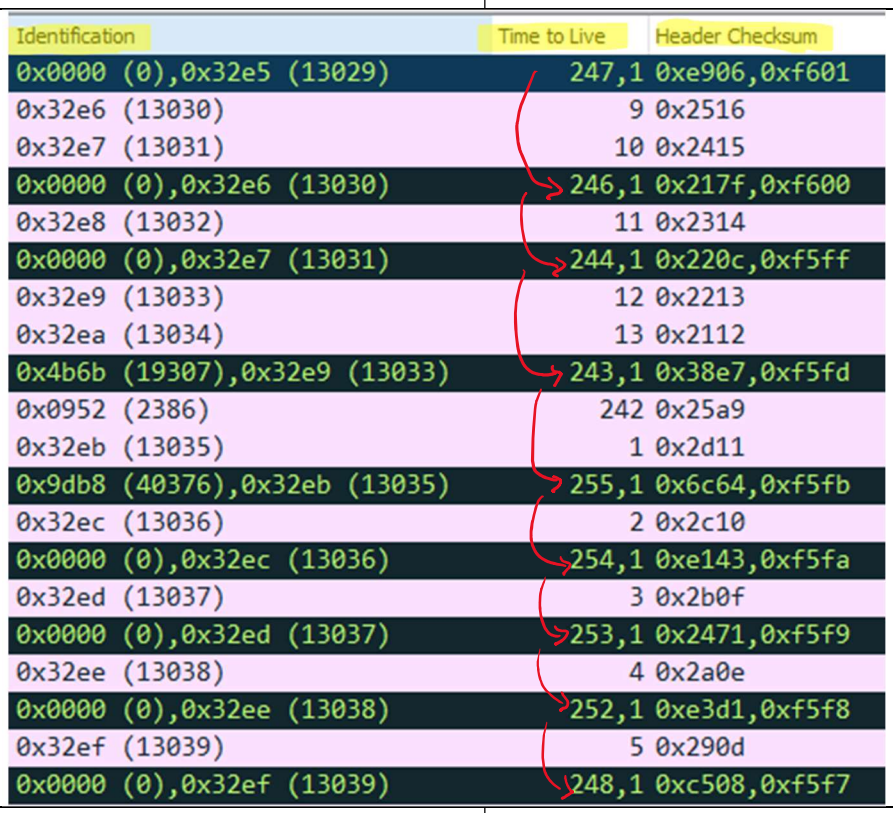
# Wireshark Lab 1: IP

**Group Details:** Shayshu NR – 1005035196, Johnathan Yan - 1004745476

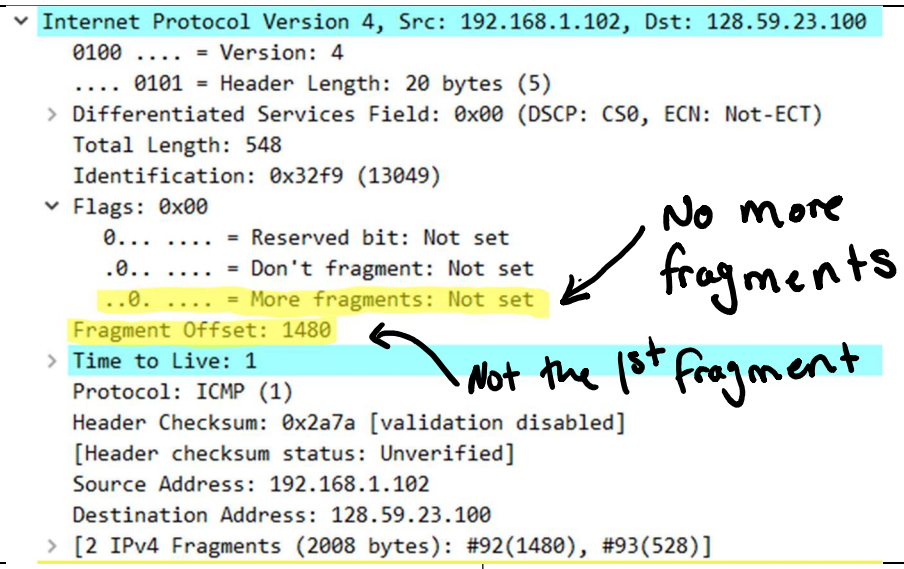
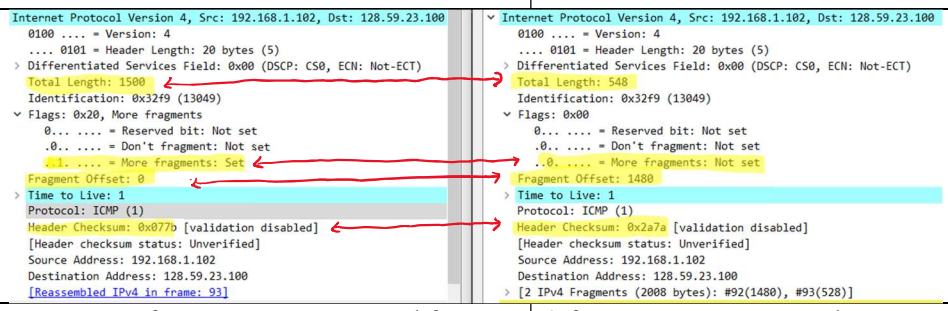
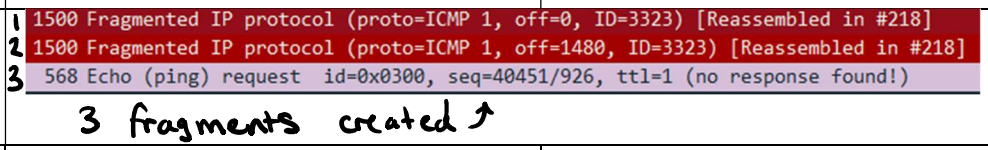
**Mark:**

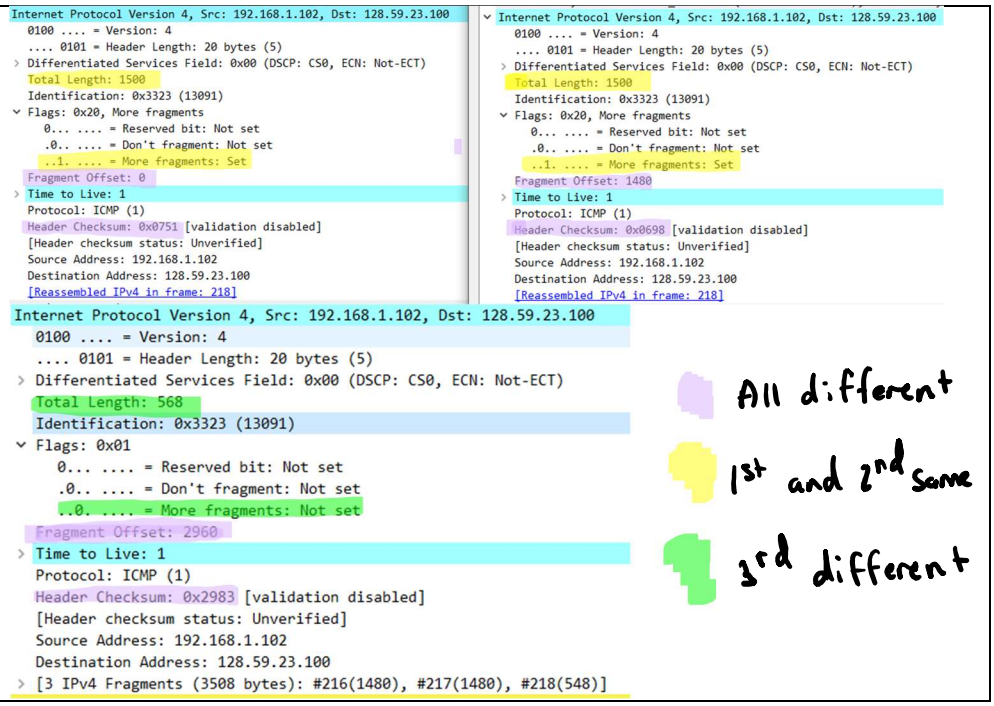
| | Question | Answer |
|---|---|---|
| 1 | Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer? | My Ip address is 10.0.0.230 |
| Annotated Screenshot (if needed) | Internet Protocol Version 4, Src: 10.0.0.230, Dst: 104.244.42.193<br>0100 .... = Version: 4<br>.... 0101 = Header Length: 20 bytes (5)<br>> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)<br>Total Length: 56<br>Identification: 0xc5fb (50683)<br>> Flags: 0x00<br>Fragment Offset: 0<br>Time to Live: 255<br>Protocol: ICMP (1)<br>Header Checksum: 0x0000 [validation disabled]<br>[Header checksum status: Unverified]<br>Source Address: 10.0.0.230 ← My IP<br>Destination Address: 104.244.42.193 | |
| 2 | Within the IP packet header, what is the value in the upper layer protocol field? | The protocol is ICMP |
| Annotated Screenshot (if needed) | See above | |
| 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 has 20 bytes, and the total message has 56 bytes of data. So, the payload is only 36 bytes. |
| Annotated Screenshot (if needed) | > Data (56 bytes)<br>↑ 20 bytes for header<br>∴ 56 - 20 = 36 byte Payload | |

| | | |
|---|---|---|
| 4 | Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented. | No because the more fragments flag is not set and the fragment offset is 0. |
| Annotated Screenshot (if needed) |  | |
| 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 time to live field, the header checksum, and the identification fields will always change |
| Annotated Screenshot (if needed) |  | |
| 6 | Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why? | The version, source address, destination address, header length, the differentiated services field, and the protocol type all stay constant.<br><br>The above also must stay constant. The checksum, identification, and time to live must change. |
| Annotated Screensho | | |

| | | |
|---|---|---|
| t (if needed) | | |
| 7 | Describe the pattern you see in the values in the Identification field of the IP datagram. | The identification field increases by one for every ping request sent out |
| Annotated Screenshot (if needed) | | |
| 8 | What is the value in the Identification field and the TTL field? | Identification 0x9d7c, time to live 255. |
| Annotated Screenshot (if needed) | Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.102<br>0100 .... = Version: 4<br>.... 0101 = Header Length: 20 bytes (5)<br>Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)<br>Total Length: 56<br>Identification: 0x9d7c (40316)<br>Flags: 0x00<br>Fragment Offset: 0<br>Time to Live: 255<br>Protocol: ICMP (1)<br>Header Checksum: 0x6ca0 [validation disabled]<br>[Header checksum status: Unverified]<br>Source Address: 10.216.228.1<br>Destination Address: 192.168.1.102 | |
| 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 time to live values stay consistent but the identification values change. |
| Annotated Screenshot (if needed) | Identification / Time to Live<br>0x9d7c (40316),0x32d0 (13008) 255,1<br>0x9d98 (40344),0x32de (13022) 255,1<br>0x9db8 (40376),0x32eb (13035) 255,1<br>0x9e06 (40454),0x32f9 (13049) 255,1<br>0x9e2c (40492),0x3307 (13063) 255,1<br>0x9e5a (40538),0x3315 (13077) 255,1<br>0x9e7c (40572),0x3323 (13091) 255,1<br>0x9e95 (40597),0x3330 (13104) 255,1<br>0x9ebb (40635),0x333e (13118) 255,1<br>Changing<br>constant | |
| 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 was fragmented |

| | | |
|---|---|---|
| Annotated Screenshot (if needed) | 1500 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]<br>548 Echo (ping) request id=0x0300, seq=30467/887, ttl=1 (no response found!)<br>56,1500 Time-to-live exceeded (Time to live exceeded in transit)<br>1500 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]<br>548 Echo (ping) request id=0x0300, seq=30723/888, ttl=2 (no response found!)<br>1500 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb) [Reassembled in #98]<br>548 Echo (ping) request id=0x0300, seq=30979/889, ttl=3 (no response found!)<br>1500 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fc) [Reassembled in #100]<br>548 Echo (ping) request id=0x0300, seq=31235/890, ttl=4 (no response found!) | |
| 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?<br>How long is this IP datagram? | The More fragments flag is set.<br>The fragment offset is set to zero.<br>The first one is 1500 bytes, this size includes the size of the header. |
| Annotated Screenshot (if needed) | Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100<br>0100 .... = Version: 4<br>.... 0101 = Header Length: 20 bytes (5)<br>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)<br>Total Length: 1500 ← Size of datagram<br>Identification: 0x32f9 (13049)<br>Flags: 0x20, More fragments<br>0... .... = Reserved bit: Not set<br>.0.. .... = Don't fragment: Not set<br>..1. .... = More fragments: Set ← Tells us there are more fragments<br>Fragment Offset: 0<br>Time to Live: 1<br>Protocol: ICMP (1)<br>Header Checksum: 0x077b [validation disabled]<br>[Header checksum status: Unverified]<br>Source Address: 192.168.1.102<br>Destination Address: 128.59.23.100<br>[Reassembled IPv4 in frame: 93] | |
| 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<br>fragments? How can you tell? | The fragment offset is non-zero.<br>There are no more fragments because the More fragments flag is not set. |

| | | |
|---|---|---|
| Annotated Screenshot (if needed) |  | |
| 13 | What fields change in the IP header between the first and second fragment? | The more fragments flag, the checksum, the fragment offset field, and the total length. |
| Annotated Screenshot (if needed) |  | |
| 14 | How many fragments were created from the original datagram? | 3 fragments were created |
| Annotated Screenshot (if needed) |  | |
| 15 | What fields change in the IP header among the fragments? | The total length, the more fragments flag, the fragment offset, and the checksum change. Note that the total length only differs between the 3rd fragment. And the more fragments flag is only set to 0 in the 3rd fragment. |

| | |
|---|---|
| Annotated Screenshot (if needed) |  Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100<br>0100 .... = Version: 4<br>.... 0101 = Header Length: 20 bytes (5)<br>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)<br>Total Length: 1500<br>Identification: 0x3323 (13091)<br>Flags: 0x20, More fragments<br>0... .... = Reserved bit: Not set<br>.0.. .... = Don't fragment: Not set<br>..1. .... = More fragments: Set<br>Fragment Offset: 0<br>Time to Live: 1<br>Protocol: ICMP (1)<br>Header Checksum: 0x0751 [validation disabled]<br>[Header checksum status: Unverified]<br>Source Address: 192.168.1.102<br>Destination Address: 128.59.23.100<br>[Reassembled IPv4 in frame: 218]<br>Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100<br>0100 .... = Version: 4<br>.... 0101 = Header Length: 20 bytes (5)<br>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)<br>Total Length: 1500<br>Identification: 0x3323 (13091)<br>Flags: 0x20, More fragments<br>0... .... = Reserved bit: Not set<br>.0.. .... = Don't fragment: Not set<br>..1. .... = More fragments: Set<br>Fragment Offset: 1480<br>Time to Live: 1<br>Protocol: ICMP (1)<br>Header Checksum: 0x0698 [validation disabled]<br>[Header checksum status: Unverified]<br>Source Address: 192.168.1.102<br>Destination Address: 128.59.23.100<br>[Reassembled IPv4 in frame: 218]<br>Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100<br>0100 .... = Version: 4<br>.... 0101 = Header Length: 20 bytes (5)<br>Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)<br>Total Length: 568<br>Identification: 0x3323 (13091)<br>Flags: 0x01<br>0... .... = Reserved bit: Not set<br>.0.. .... = Don't fragment: Not set<br>..0. .... = More fragments: Not set<br>Fragment Offset: 2960<br>Time to Live: 1<br>Protocol: ICMP (1)<br>Header Checksum: 0x2983 [validation disabled]<br>[Header checksum status: Unverified]<br>Source Address: 192.168.1.102<br>Destination Address: 128.59.23.100<br>[3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]<br>All different<br>1st and 2nd same<br>3rd different |