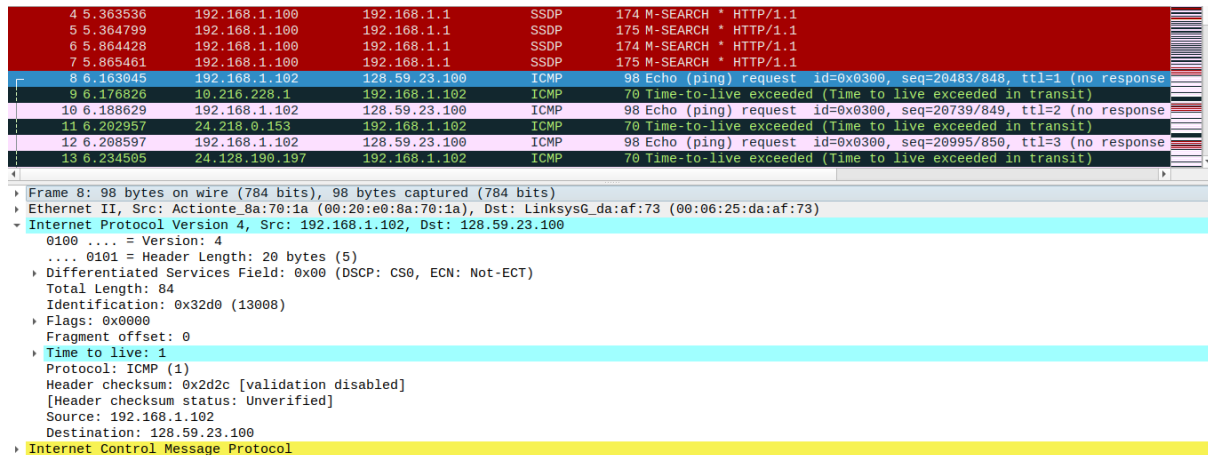


Lab_4a_Wireshark_IP_v8.0

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?

Answer:



The IP address of my computer is 192.168.1.162

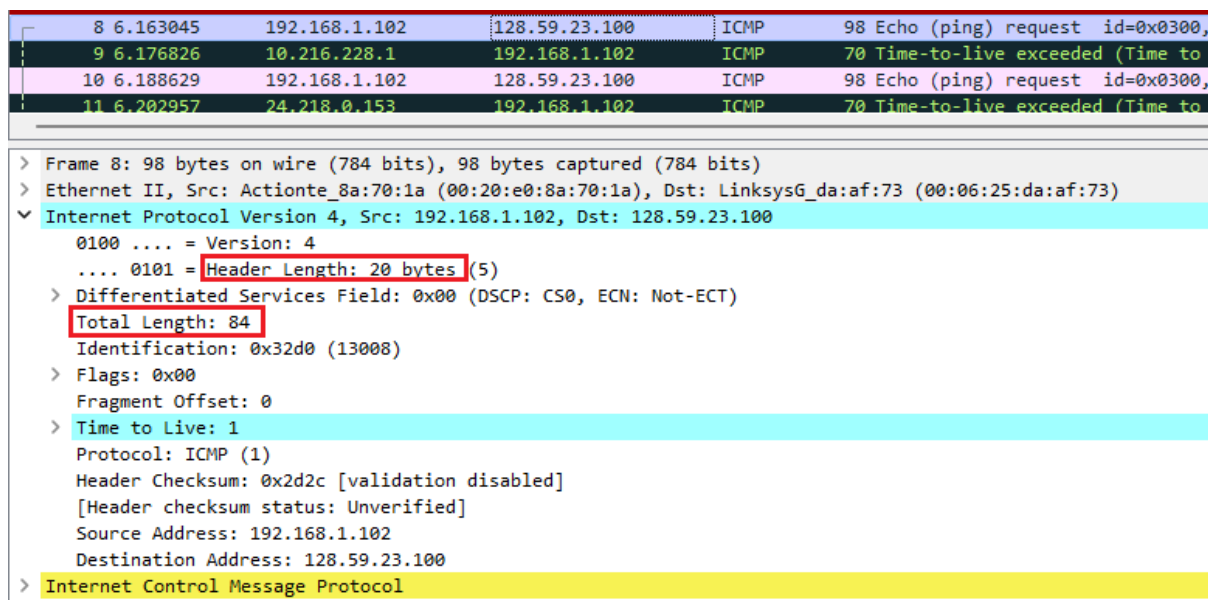
2. Within the IP packet header, what is the value in the upper layer protocol field?

Answer:

The value of the upper layer protocol field is 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.

Answer:



There are 20 bytes in the IP header which leaves 64 bytes for the payload of the IP datagram because we were sending a packet of length 84 bytes.

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

Answer: Not fragmented. b/c The more fragments bit = 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?

Answer:

Time to live, Identifier and header checksum 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?

Answer:

- The fields that stay constant are:
 - + Version (since we are using IPv4)
 - + Header length (since these are UDP packets)
 - + Source IP (since all packets are sent from my computer)
 - + Destination IP (since we are sending to the same host)
 - + Differentiated Services (since all packets are UDP)
 - + Upper Layer Protocol (since these are UDP packets)
- The fields that must stay constant are:
 - + Version (since we are using IPv4)
 - + Header length (since these are UDP packets)
 - + Source IP (since all packets are sent from my computer)
 - + Destination IP (since we are sending to the same host)
 - + Differentiated Services (since all packets are UDP)
 - + Upper Layer Protocol (since these are UDP packets)
- The fields that must change are:
 - + Identification (IP packets have different ids)
 - + Time to live (traceroute increments each packet)
 - + Header checksum (since header changes)

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

Answer:

The pattern in the identification field is that the field increases by one in each strand of echo requests.

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

Answer:

```

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: 0x0000
  Fragment offset: 0
  Time to live: 255
  Protocol: ICMP (1)
  Header checksum: 0x6ca0 [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.216.228.1
  Destination: 192.168.1.102
Internet Control Message Protocol

```

Identification: 40316

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?

Answer:

- The Identification field changes from all of the replies because this field has to have a unique value. If they(2 or more replies) have the same value then the replies must be fragments of a bigger packet.
- The TLL field does not change because the time to live to the first hop router 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? [Note: if you find your packet has not been fragmented, you should download the zip file

<http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.^{3]}

Answer:

This packet 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?

Answer:

82	16.393260	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request	id=0x0300, seq=29443/883, ttl=10 (no response found!)
83	16.413273	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request	id=0x0300, seq=29699/884, ttl=11 (no response found!)
84	16.418067	216.140.10.30	192.168.1.102	ICMP	70 Time-to-live exceeded	(Time to live exceeded in transit)
85	16.438258	67.99.58.194	192.168.1.102	ICMP	70 Time-to-live exceeded	(Time to live exceeded in transit)
86	16.443310	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request	id=0x0300, seq=29955/885, ttl=12 (no response found!)
87	16.463382	192.168.1.102	128.59.23.100	ICMP	98 Echo (ping) request	id=0x0300, seq=30211/886, ttl=13 (reply in 89)
88	16.468603	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded	(Time to live exceeded in transit)
89	16.499919	128.59.23.100	192.168.1.102	ICMP	98 Echo (ping) reply	id=0x0300, seq=30211/886, ttl=242 (request in 87)
90	22.928093	192.168.1.102	128.119.245.12	SSH	74 Client: Encrypted packet	(len=20)
91	22.952738	128.119.245.12	192.168.1.102	TCP	60 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0	
92	28.441511	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9)	[Reassembled in #93]
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request	id=0x0300, seq=30467/887, ttl=1 (no response found!)

```

Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
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: 1500
  Identification: 0x32f9 (13049)
  Flags: 0x0000, More fragments
  Fragment offset: 0
  Time to live: 1
  Protocol: ICMP (1)
  Header checksum: 0x077b [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.1.102
  Destination: 128.59.23.100
  Reassembled 1064 in frame: 93

```

- The Flags bit for more fragments is set, indicating that the datagram has been fragmented.
- Since the fragment offset is 0, we know that this is the first fragment.
- This first datagram has a total length of 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 there more fragments? How can you tell?

88	16.468603	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded	(Time to live exceeded in transit)
89	16.499919	128.59.23.100	192.168.1.102	ICMP	98 Echo (ping) reply	id=0x0300, seq=30211/886, ttl=242 (request in 87)
90	22.928093	192.168.1.102	128.119.245.12	SSH	74 Client: Encrypted packet	(len=20)
91	22.952738	128.119.245.12	192.168.1.102	TCP	60 22 → 1170 [ACK] Seq=1 Ack=21 Win=35040 Len=0	
92	28.441511	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9)	[Reassembled in #93]
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request	id=0x0300, seq=30467/887, ttl=1 (no response found!)
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded	(Time to live exceeded in transit)
95	28.470668	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa)	[Reassembled in #96]
96	28.471338	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request	id=0x0300, seq=30723/888, ttl=2 (no response found!)
97	28.490663	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fb)	[Reassembled in #98]
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562 Echo (ping) request	id=0x0300, seq=30979/889, ttl=3 (no response found!)

```

Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
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: 548
  Identification: 0x32f9 (13049)
  Flags: 0x00b9
    0... .. = Reserved bit: Not set
    .0.. .. = Don't fragment: Not set
    .0.. .. = More fragments: Not set
  Fragment offset: 1480
  Time to live: 1
  Protocol: ICMP (1)
  Header checksum: 0x2a7a [validation disabled]

```

Answer:

According to above screenshot, this is not the first fragment since the fragment offset is 1480 and this should be the last fragment, since the status of more fragments flag is not set.

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

Answer: Total length, flags, fragment offset, and checksum.

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

Answer: there are 3 packets created from the original datagram.

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

Answer:

211	39.164169	67.99.58.194	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
212	39.227649	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
213	39.314263	128.59.23.100	192.168.1.102	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562 Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
215	41.038658	192.168.1.102	199.2.53.206	TCP	62 [TCP Retransmission] 1483 - 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PER
216	43.466136	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	43.466808	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	43.467629	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219	43.485786	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
220	43.492284	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	43.492953	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222	43.493901	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)
223	43.530345	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]
0100 = Version: 4					
... 0101 = Header Length: 20 bytes (5)					
+ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 1500					
Identification: 0x3323 (13091)					
+ Flags: 0x2000, More fragments					
0... .. = Reserved bit: Not set					
.0... .. = Don't fragment: Not set					
..1... .. = More fragments: Set					
Fragment offset: 0					
+ Time to live: 1					
Protocol: ICMP (1)					
Header checksum: 0x0751 [validation disabled]					
[Header checksum status: Unverified]					
Source: 192.168.1.102					
Destination: 128.59.23.100					
Reassembled IPv4 in frame: 218					
211	39.164169	67.99.58.194	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
212	39.227649	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
213	39.314263	128.59.23.100	192.168.1.102	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562 Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
215	41.038658	192.168.1.102	199.2.53.206	TCP	62 [TCP Retransmission] 1483 - 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PER
216	43.466136	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	43.466808	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	43.467629	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219	43.485786	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
220	43.492284	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	43.492953	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222	43.493901	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)
223	43.530345	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]
0100 = Version: 4					
... 0101 = Header Length: 20 bytes (5)					
+ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 1500					
Identification: 0x3323 (13091)					
+ Flags: 0x20b9, More fragments					
0... .. = Reserved bit: Not set					
.0... .. = Don't fragment: Not set					
..1... .. = More fragments: Set					
Fragment offset: 1480					
+ Time to live: 1					
Protocol: ICMP (1)					
Header checksum: 0x0698 [validation disabled]					
[Header checksum status: Unverified]					
Source: 192.168.1.102					
Destination: 128.59.23.100					
211	39.164169	67.99.58.194	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
212	39.227649	128.59.1.41	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
213	39.314263	128.59.23.100	192.168.1.102	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
214	39.322566	128.59.23.100	192.168.1.102	ICMP	562 Echo (ping) reply id=0x0300, seq=40195/925, ttl=242 (request in 205)
215	41.038658	192.168.1.102	199.2.53.206	TCP	62 [TCP Retransmission] 1483 - 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PER
216	43.466136	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
217	43.466808	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
218	43.467629	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40451/926, ttl=1 (no response found!)
219	43.485786	10.216.228.1	192.168.1.102	ICMP	70 Time-to-live exceeded (Time to live exceeded in transit)
220	43.492284	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
221	43.492953	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
222	43.493901	192.168.1.102	128.59.23.100	ICMP	582 Echo (ping) request id=0x0300, seq=40707/927, ttl=2 (no response found!)
223	43.530345	192.168.1.102	128.59.23.100	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3325) [Reassembled in #225]
0100 = Version: 4					
... 0101 = Header Length: 20 bytes (5)					
+ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)					
Total Length: 568					
Identification: 0x3323 (13091)					
+ Flags: 0x0172					
0... .. = Reserved bit: Not set					
.0... .. = Don't fragment: Not set					
..0... .. = More fragments: Not set					
Fragment offset: 2960					
+ Time to live: 1					
Protocol: ICMP (1)					
Header checksum: 0x2983 [validation disabled]					
[Header checksum status: Unverified]					
Source: 192.168.1.102					
Destination: 128.59.23.100					
+ [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]					
Internet Control Message Protocol					

- The IP header fields that changed between all of the packets are: fragment offset, and checksum.
- The first two packets have a total length of 1500, with the more fragments bit set to 1
- The last packet has a total length of 568, with the more fragments bit set to 0.