

60-367

Lab 3

Ryan Lebeau, Calvin Moras

07/11/18

Part 1: ICMP

1. Host IP address is 192.168.1.101 and the IP address of the destination host is 143.89.14.34
2. There are no source and destination port numbers in an ICMP packet since it is designed to communicate between network layers which only require a Type and Code combination.
3. ICMP type numbers 8 and code number 0, there are also identifier (both BE and LE), sequence numbers (BE/LE), checksum field, and data fields. The checksum bytes are 2, the identifier bytes are 2, and sequence number bytes are 2.

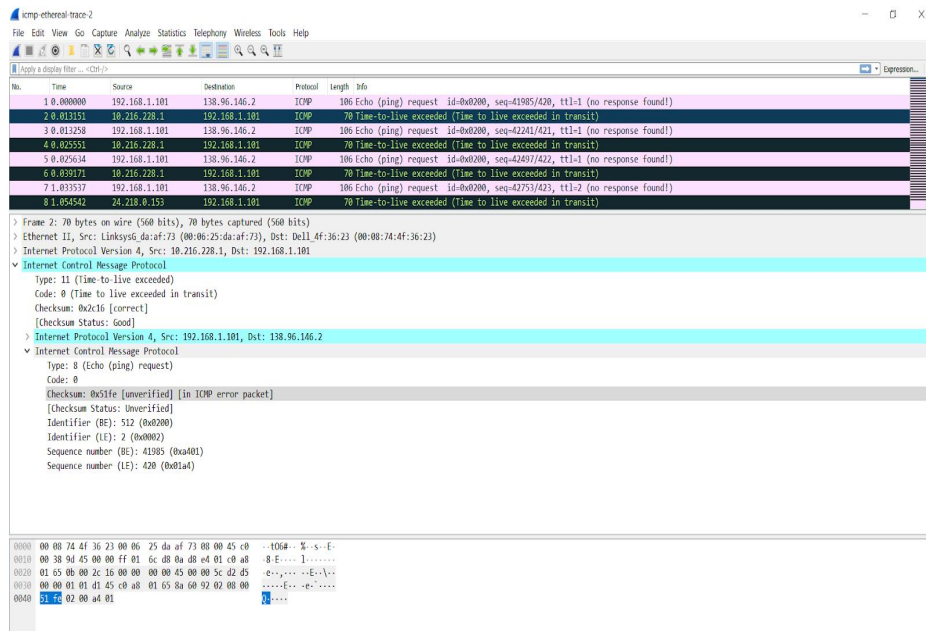
The image shows a Wireshark packet capture titled 'icmp-ethereal-trace-1'. The packet list pane shows several ICMP Echo (ping) requests and replies. The selected packet is packet 3, an ICMP Echo (ping) request from 192.168.1.101 to 143.89.14.34. The packet details pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Dell_4f:36:23	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.101
2	0.001649	LinksysG_da:af:73	Dell_4f:36:23	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001656	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26369/359, ttl=128 (reply in 4)
4	0.415998	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26369/359, ttl=231 (request in 3)
5	1.006279	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26625/360, ttl=128 (reply in 6)
6	1.431684	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26625/360, ttl=231 (request in 5)
7	2.006328	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26881/361, ttl=128 (reply in 8)
8	2.324479	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26881/361, ttl=231 (request in 7)

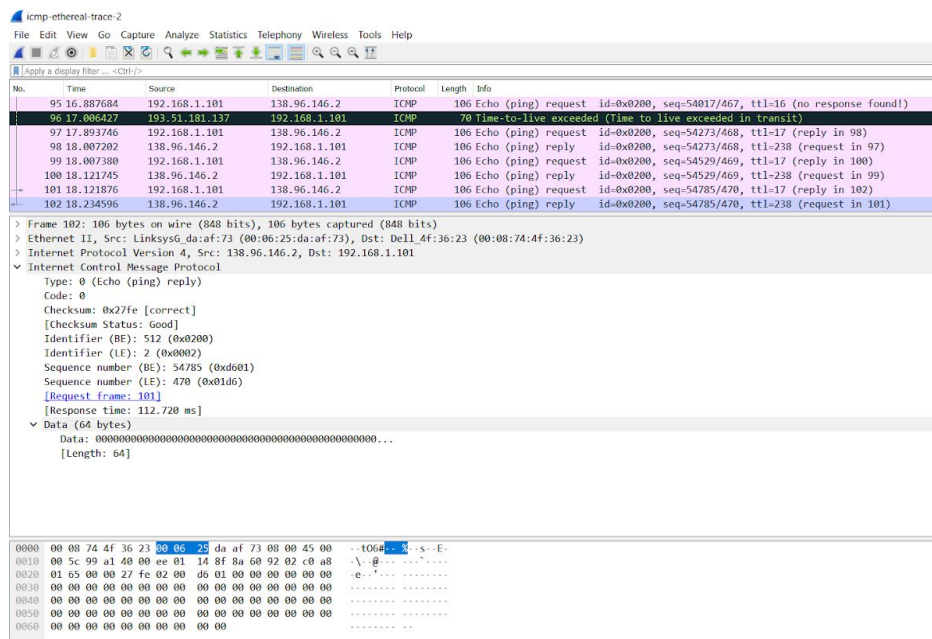
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 143.89.14.34
▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xe45a [correct]
[Checksum Status: Good]
Identifier (BE): 512 (0x0200)
Identifier (LE): 2 (0x0002)
Sequence number (BE): 26369 (0x6701)
Sequence number (LE): 359 (0x0167)
[Response frame: 4]
▼ Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f707172737475767768...
[Length: 32]

4. The ICMP type number 0 and code number 0, there are also identifier (both BE and LE) and sequence numbers (BE/LE), checksum field, and data fields. The checksum bytes are 2, the identifier bytes are 2, and sequence number bytes are 2.

8. The ICMP error packet contains the type, code, checksum, identifier, and sequence number of the original ICMP echo packet.



9. The last three ICMP packets are reply messages to the request packet instead of error packets, they have type number 0.



10. There is a significant longer link between step 11 and 12. The link is from New York to Aubervilliers, France.

Part 2: IP

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area shows a list of captured packets. The selected packet is 78, which is an ICMP Echo (ping) request from 192.168.1.8 to 151.101.125.140. The details pane on the right shows the structure of the packet: Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The IP header details are expanded, showing fields like Version, Header Length, Total Length, Identification, Flags, Time to live, Protocol, Header checksum, Source, and Destination. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
78	4.912779	192.168.1.8	151.101.125.140	ICMP	70	Echo (ping) request id=0x0001, seq=16
80	4.926446	151.101.125.140	192.168.1.8	ICMP	70	Echo (ping) reply id=0x0001, seq=16
83	4.930083	192.168.1.8	151.101.125.140	ICMP	70	Echo (ping) request id=0x0001, seq=16
84	4.930480	192.168.1.1	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live ex
86	4.947922	192.168.1.8	151.101.125.140	ICMP	70	Echo (ping) request id=0x0001, seq=16
87	4.965725	192.168.1.8	151.101.125.140	ICMP	70	Echo (ping) request id=0x0001, seq=16
88	4.981616	192.168.1.8	151.101.125.140	ICMP	70	Echo (ping) request id=0x0001, seq=11
89	4.981665	24.226.4.61	192.168.1.8	ICMP	110	Time-to-live exceeded (Time to live ex

Frame 78: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: Giga-Byt_1f:e1:d5 (40:8d:5c:1f:e1:d5), Dst: Netgear_2e:da:17 (74:44:01:2e:da:17)
> Internet Protocol Version 4, Src: 192.168.1.8, Dst: 151.101.125.140
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 56
 Identification: 0x1edd (7901)
 > Flags: 0x0000
 Time to live: 255
 Protocol: ICMP (1)
 Header checksum: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.8
 Destination: 151.101.125.140
> Internet Control Message Protocol

0000 74 44 01 2e da 17 40 8d 5c 1f e1 d5 08 00 45 00 tD...@. \.....E.

Source (ip.src), 4 bytes Packets: 5222 · Displayed: 1362 (26.1%) · Dropped: 0 (0.0%) Profile: Default

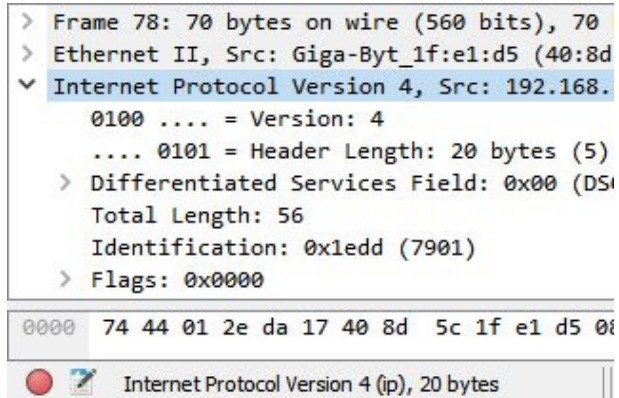
1.

The IP address of my computer is 192.168.1.8.

2. The value in the Protocol field of the IP Header is ICMP (1).

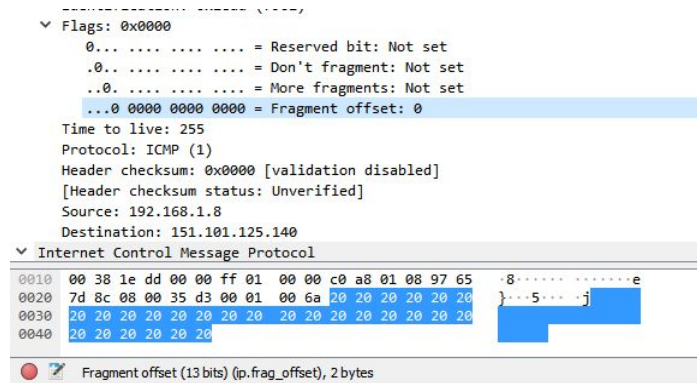
3. The IP header itself contains 20 bytes, the payload of the IP datagram is 36 bytes. This is because the total length field tells us the overall length is 56 bytes, so $56 - 20 = 36$. This

can be verified by checking the length of the ICMP field in wireshark as well.



4. This IP datagram has not been fragmented. This can be seen by the fragment offset flag

having a value of 0:



5. The only two values two change from one datagram to the next for me, were the Identification and Time to Live values. However it is worth noting that my installation of wireshark had checksum validation disabled by default, and had it been enabled at the

time of capture, the checksum of each header should have differed.

No.	Time	Source	Destination	Protocol	Length	Info
148	3.272921	206.108.35.30	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
133	2.272478	206.108.35.30	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
112	1.268141	206.108.35.30	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
93	0.101500	206.108.35.30	192.168.1.8	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
5152	142.661273	192.168.1.8	151.101.125.140	ICMP	554	Echo (ping) request id=0x0001, seq=924/39939, ttl=6 (no response found!)
5149	142.610689	192.168.1.8	151.101.125.140	ICMP	554	Echo (ping) request id=0x0001, seq=923/39683, ttl=5 (no response found!)
5145	142.560424	192.168.1.8	151.101.125.140	ICMP	554	Echo (ping) request id=0x0001, seq=922/39427, ttl=4 (no response found!)
5139	142.509895	192.168.1.8	151.101.125.140	ICMP	554	Echo (ping) request id=0x0001, seq=921/39171, ttl=3 (no response found!)
5135	142.459295	192.168.1.8	151.101.125.140	ICMP	554	Echo (ping) request id=0x0001, seq=920/38915, ttl=2 (no response found!)
5131	142.408634	192.168.1.8	151.101.125.140	ICMP	554	Echo (ping) request id=0x0001, seq=919/38659, ttl=1 (no response found!)
5128	142.358086	192.168.1.8	151.101.125.140	ICMP	554	Echo (ping) request id=0x0001, seq=918/38403, ttl=255 (no response found!)
5118	141.660584	192.168.1.8	151.101.125.140	ICMP	554	Echo (ping) request id=0x0001, seq=917/38147, ttl=6 (no response found!)
5115	141.610066	192.168.1.8	151.101.125.140	ICMP	554	Echo (ping) request id=0x0001, seq=916/37891, ttl=5 (no response found!)
5111	141.559387	192.168.1.8	151.101.125.140	ICMP	554	Echo (ping) request id=0x0001, seq=915/37635, ttl=4 (no response found!)

Ethernet II, Src: Giga-Byt_1f:e1:d5 (40:8d:5c:1f:e1:d5), Dst: Netgear_2e:da:17 (74:44:01:2e:da:17)

Internet Protocol Version 4, Src: 192.168.1.8, Dst: 151.101.125.140

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 540
Identification: 0x220f (8719)
> Flags: 0x0172
Time to live: 6
Protocol: ICMP (1)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.8
Destination: 151.101.125.140
> [3 IPv4 Fragments (3480 bytes): #5150(1480), #5151(1480), #5152(520)]
> Internet Control Message Protocol

0010 02 1c 22 0f 01 72 06 01 00 00 c0 a8 01 08 97 65 ...
0020 7d 8c 20 20 20 20 20 20 20 20 20 20 20 20 20 20 }
0030 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 }

Frame (554 bytes) Reassembled IPv4 (3480 bytes)
Header checksum (ip.checksum), 2 bytes

Packets: 5222 · Displayed: 1362 (26.1%) · Dropped: 0 (0.0%) Profile: Default

- Source, Destination, Protocol / version, upper layer protocol, Differentiated Services Field (including sub-entries), and Header Length all remain constant. The source and destination must remain constant so long as the same two devices are communicating, both types of protocols must remain constant since IPV4 is being used and all packets are ICMP packets, which means they will all also use the same services. Identification must change so as to uniquely identify each packet, time to live changes due to the traceroute's incrementation of each packet, and once again although it did not on mine, due to the nature of checksums, the header checksum would change each time as well, as each packet's checksum is a product of the information its header contains.
- Each identification number is a sequential hex value from the previous packet's identification number (these values are technically ascending each packet, we are just viewing in descending order).

8. The Identification field's value is 0x2aad (10925 in decimal). The TTL value is 64.

The image shows a Wireshark packet capture of ICMP Echo (ping) requests. The packet list shows several requests from 192.168.1.8 to 151.101.125.140. The details pane for frame 5132 shows the following fields:

- Frame 5132: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
- Ethernet II, Src: Netgear_2e:da:17 (74:44:01:2e:da:17), Dst: Giga-Byt_1f:e1:d5 (40:8d:5c:1f:e1:d5)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.8
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
 - Total Length: 576
 - Identification: 0x2aad (10925)
 - Flags: 0x0000
 - Time to live: 64
 - Protocol: ICMP (1)
 - Header checksum: 0xc9f6 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.1.1
 - Destination: 192.168.1.8
- Internet Control Message Protocol

The packet bytes pane shows the raw data of the packet, including the IP header and ICMP header.

9. The identification value should not remain unchanged as it is meant to uniquely identify each packet. The TTL remains unchanged because the TTL for the first hop router always remains the same, and since the TTL was exceeded in transit, the request was sent again to the same first hop router.

10. As indicated by both the fragment flag and the wireshark populated “IP Fragments” field, this message has been fragmented.

1566	45.396097	151.101.125.140	192.168.1.8	ICMP	70 Echo (ping) reply
2189	58.762530	192.168.1.8	151.101.125.140	ICMP	534 Echo (ping) request
2192	58.779962	192.168.1.8	151.101.125.140	ICMP	534 Echo (ping) request
2193	58.780735	192.168.1.1	192.168.1.8	ICMP	590 Time-to-live exceeded
2196	58.797093	192.168.1.8	151.101.125.140	ICMP	534 Echo (ping) request
2198	58.814914	192.168.1.8	151.101.125.140	ICMP	534 Echo (ping) request
2199	58.830326	24.226.4.61	192.168.1.8	ICMP	110 Time-to-live exceeded

..0..	= Don't fragment: Not set
..0.	= More fragments: Not set
...0	0000	1011	1001		= Fragment offset: 185

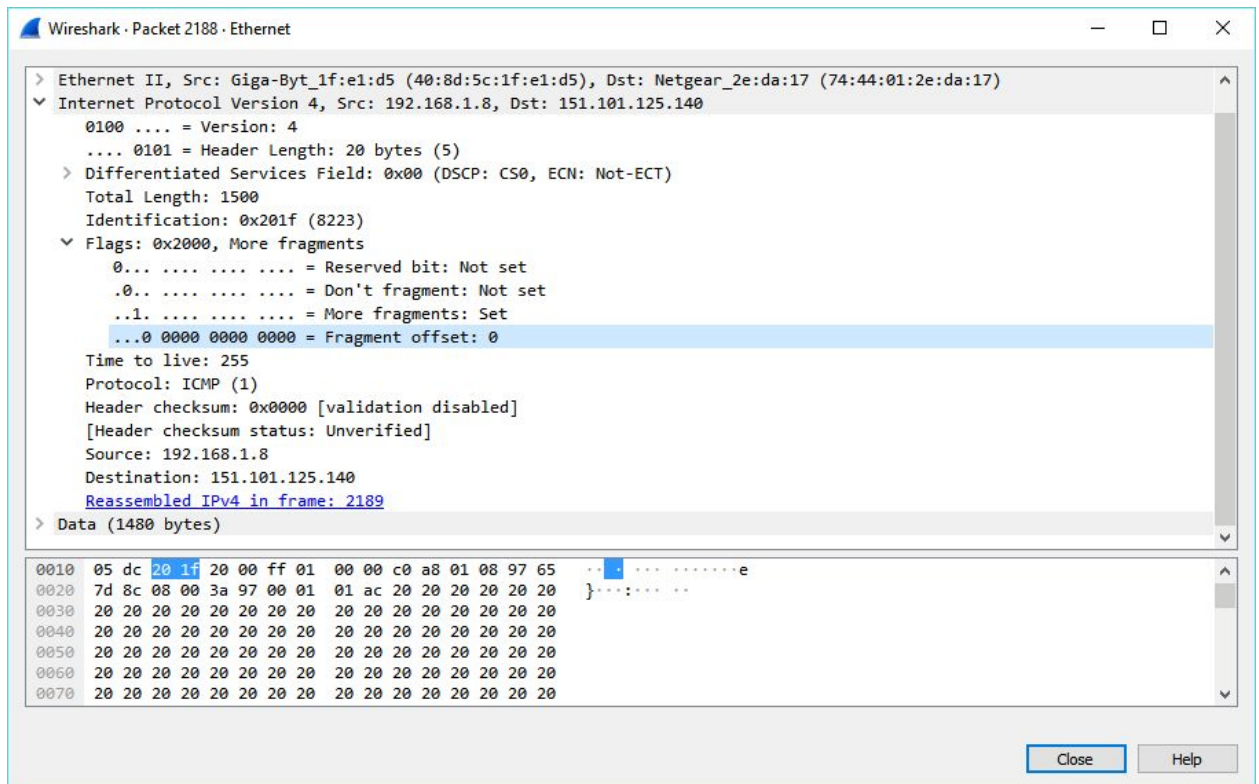
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.8
Destination: 151.101.125.140

▼ [2 IPv4 Fragments (1980 bytes): #2188(1480), #2189(500)]

[Frame: 2188, payload: 0-1479 (1480 bytes)]
[Frame: 2189, payload: 1480-1979 (500 bytes)]
[Fragment count: 2]
[Reassembled IPv4 length: 1980]

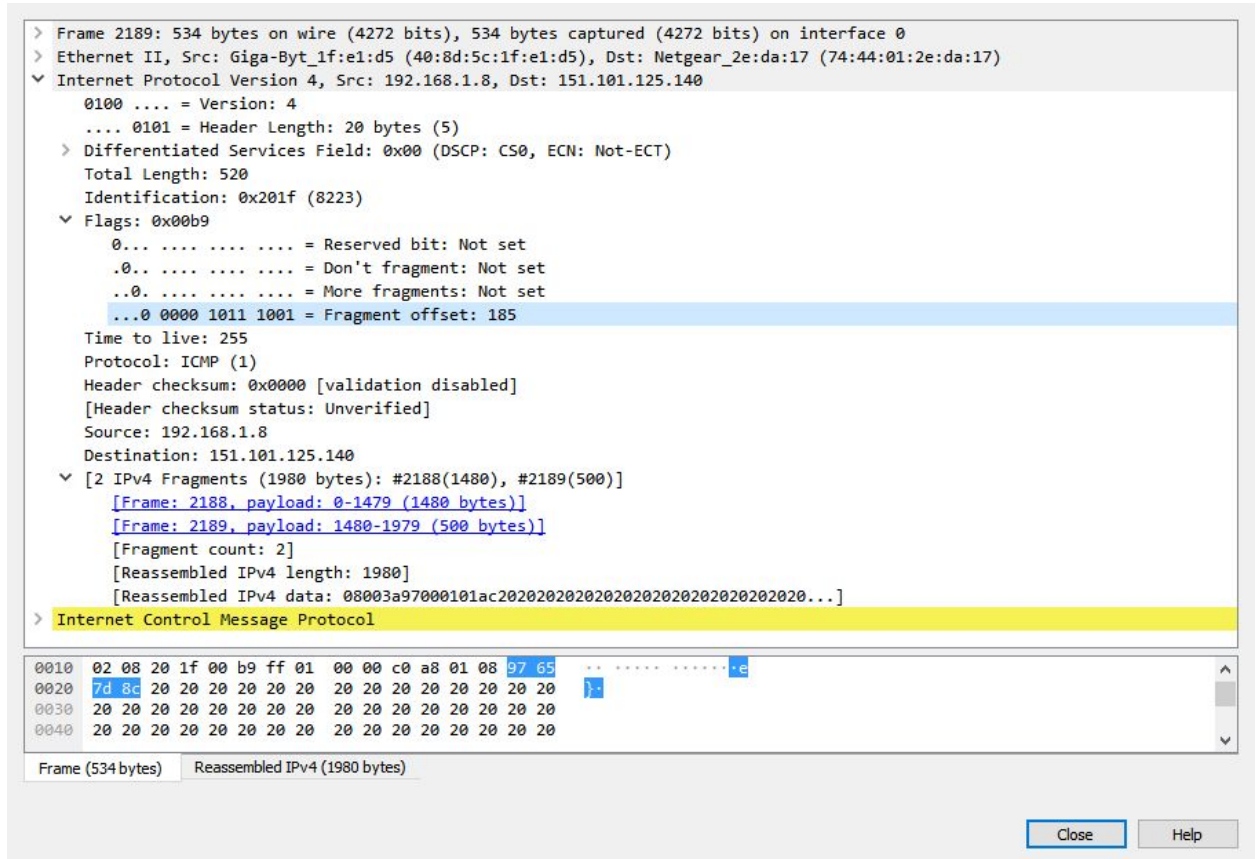
11. Although the fragment offset is set to 0, we can see the datagram has been fragmented because the more fragments flag is set. The fragment offset of 0 also tells us that this is the first fragment in the message. This IP datagram has a total length of 1500 bytes. The remaining 500 bytes are contained in the latter fragment, adding to a total of 2000 bytes.

This can also be seen in the frame sizes in the image above.



12. The second fragment has a non-zero fragment offset of 185. This tells us it is a fragment and not the first one. There are no more fragments after this one because the “More

fragments" flag is not set.



13. The only fields to change between the two fragments are the total length and any appropriate fragment flags such as the “more fragments” flag or the fragment offset, and once again, checksum would change in this case as well, since information in the IP header differs again.

14. When the packet size was set to 3500 bytes, 3 fragments were created from the original datagram.

3452	107.310807	192.168.1.8	151.101.125.140	ICMP	554 Echo (ping) request	id=0x0001, seq=673/41218, ttl=255 (no response found!)
3456	107.328237	192.168.1.8	151.101.125.140	ICMP	554 Echo (ping) request	id=0x0001, seq=674/41474, ttl=1 (no response found!)
3457	107.329088	192.168.1.1	192.168.1.8	ICMP	590 Time-to-live exceeded	(Time to live exceeded in transit)
3461	107.346174	192.168.1.8	151.101.125.140	ICMP	554 Echo (ping) request	id=0x0001, seq=675/41730, ttl=2 (no response found!)
3464	107.362017	192.168.1.8	151.101.125.140	ICMP	554 Echo (ping) request	id=0x0001, seq=676/41986, ttl=3 (no response found!)
3465	107.376426	24.226.4.61	192.168.1.8	ICMP	110 Time-to-live exceeded	(Time to live exceeded in transit)
3468	107.379798	192.168.1.8	151.101.125.140	ICMP	554 Echo (ping) request	id=0x0001, seq=677/42242, ttl=4 (no response found!)
3471	107.395713	192.168.1.8	151.101.125.140	ICMP	554 Echo (ping) request	id=0x0001, seq=678/42498, ttl=5 (no response found!)
3472	107.396925	10.0.18.73	192.168.1.8	ICMP	110 Time-to-live exceeded	(Time to live exceeded in transit)

...0 0001 0111 0010 = Fragment offset: 370
 Time to live: 255
 Protocol: ICMP (1)
 Header checksum: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source: 192.168.1.8
 Destination: 151.101.125.140

[3 IPv4 Fragments (3480 bytes): #3450(1480), #3451(1480), #3452(520)]

- [Frame: 3450, payload: 0-1479 (1480 bytes)]
- [Frame: 3451, payload: 1480-2959 (1480 bytes)]
- [Frame: 3452, payload: 2960-3479 (520 bytes)]

[Fragment count: 3]
 [Reassembled IPv4 length: 3480]
 [Reassembled IPv4 data: 00001b84000102a120202020202020202020202020202020...]

Internet Control Message Protocol

15. Once again, between the three fragments, the different fragment flags change (offset, more), the total length differs between either the cap of 1500 bytes, or the total remaining number of bytes in the last fragment (in my case 540, the extra 40 bytes of course, coming from the 20 bytes in each previous IP header in each fragment). Checksum would also change each time due to the changes in each IP header, though once again, not in mine as this was not enabled at the time of the trace.

Three Wireshark packet capture screenshots showing ICMP Echo (ping) requests. The first packet (3450) is a standard Echo request. The second packet (3451) is an Echo request with the 'More fragments' flag set. The third packet (3452) is an Echo request with the 'More fragments' flag set and a fragment offset of 370.

Packet Number	Length	Identification	Flags	Fragment Offset
3450	1500	0x2114 (8468)	0x2000, More fragments	0
3451	1500	0x2114 (8468)	0x20b9, More fragments	185
3452	540	0x2114 (8468)	0x0172	370