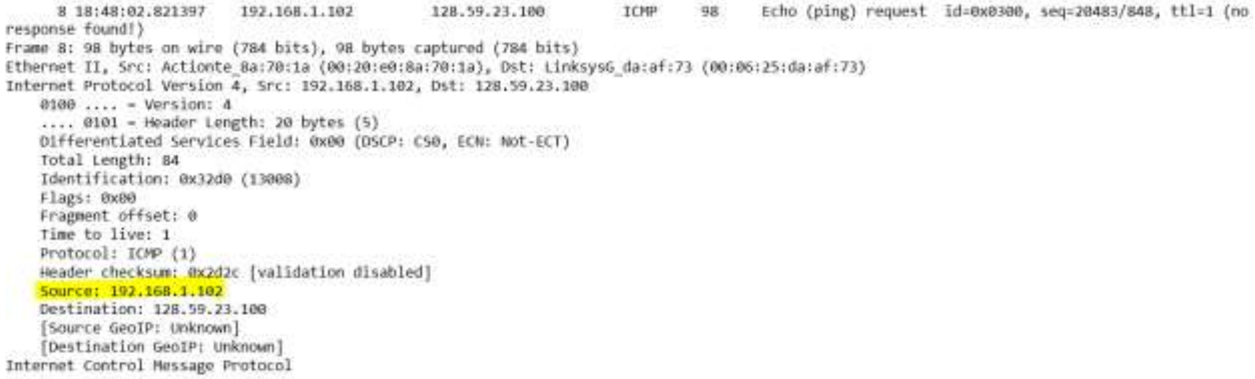
Rhea Mae Edwards
CS 372

Lab #4: IP

Capturing Packets from an Execution of Traceroute

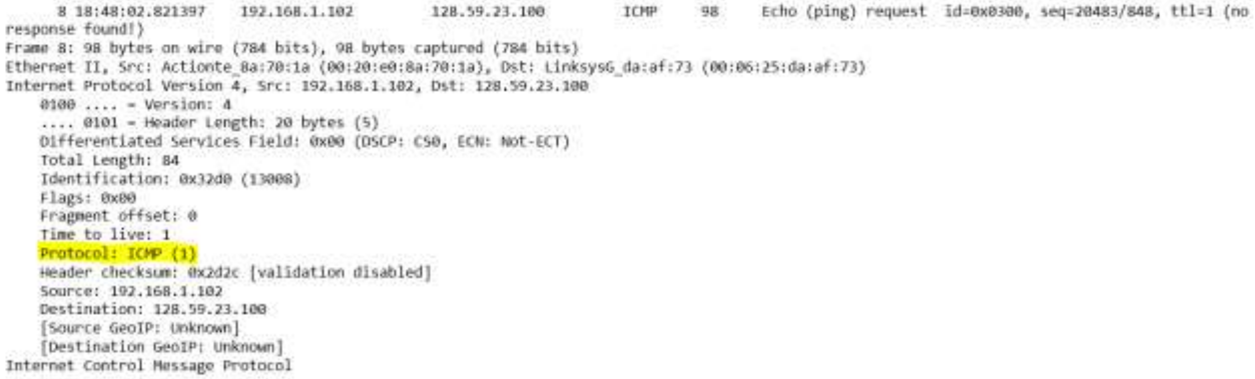
A Look at the Captured Trace

1. IP Address of My Computer: 192.168.1.102



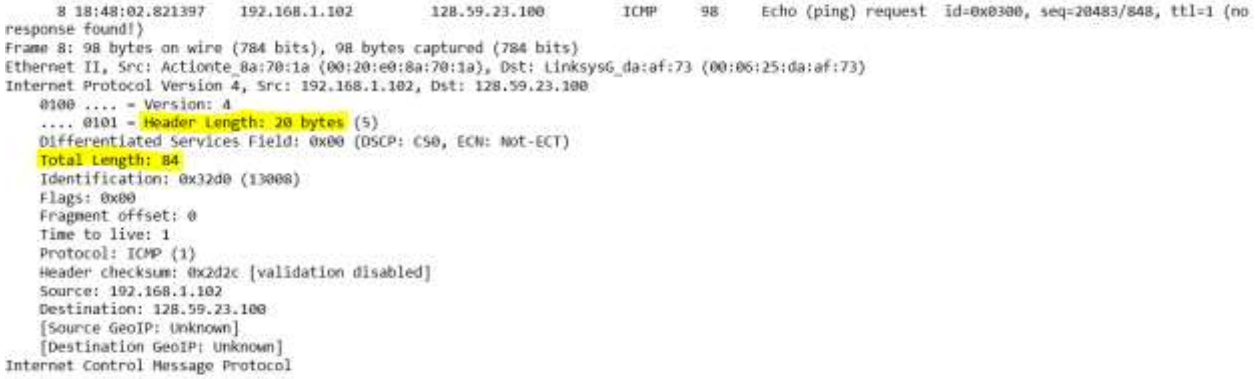
```
     8 18:48:02.821397    192.168.1.102        128.59.23.100        ICMP     98     Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no
response found!)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (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: 84
    Identification: 0x32d0 (13008)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
```

2. Value of the Upper Layer Protocol Field: 1



```
     8 18:48:02.821397    192.168.1.102        128.59.23.100        ICMP     98     Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no
response found!)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 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: 84
    Identification: 0x32d0 (13008)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
```

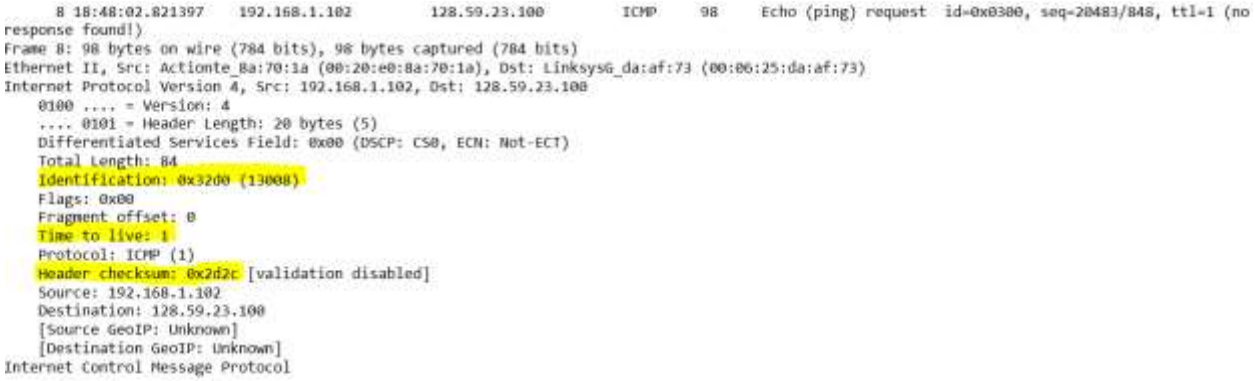
3. Bytes in the IP Header: 20 bytes
Bytes in the Payload of the IP Datagram: 84 – 20 = 64 bytes



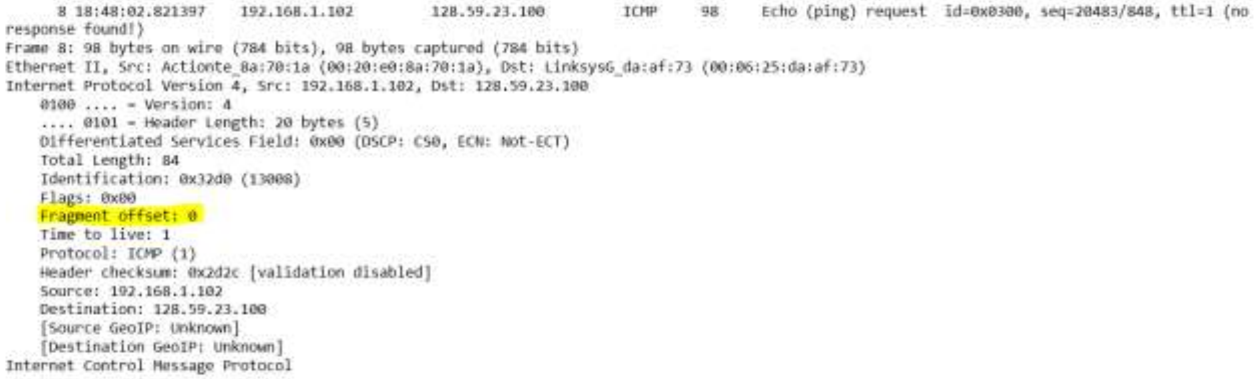
```
     8 18:48:02.821397    192.168.1.102        128.59.23.100        ICMP     98     Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no
response found!)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (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: 84
    Identification: 0x32d0 (13008)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
```

Rhea Mae Edwards
CS 372

4. This IP datagram has not been fragmented.
   Since the fragment offset section of the packets states the value of zero, was the indicator on how I determined that the datagram has not been fragmented.



```
     8 18:48:02.821397    192.168.1.102        128.59.23.100        ICMP     98     Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no
response found!)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 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: 84
    Identification: 0x32d0 (13008)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
```



```
     8 18:48:02.821397    192.168.1.102        128.59.23.100        ICMP     98     Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no
response found!)
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 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: 84
    Identification: 0x32d0 (13008)
    Flags: 0x00
    Fragment offset: 0
    Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x2d2c [validation disabled]
    Source: 192.168.1.102
    Destination: 128.59.23.100
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
```

5. The Identification, Time to Live, and Header Checksum fields in the IP datagram always change from one datagram to the next within this series of ICMP message sent by my computer.

6. Fields that Stay Constant:

- Version
- Header Length
- Differentiated Services Field
- Total Length
- Flags
- Fragment Offset
- Protocol
- Source
- Destination
- Source GeoIP
- Destination GeoIP

Fields that Must Stay Constant:

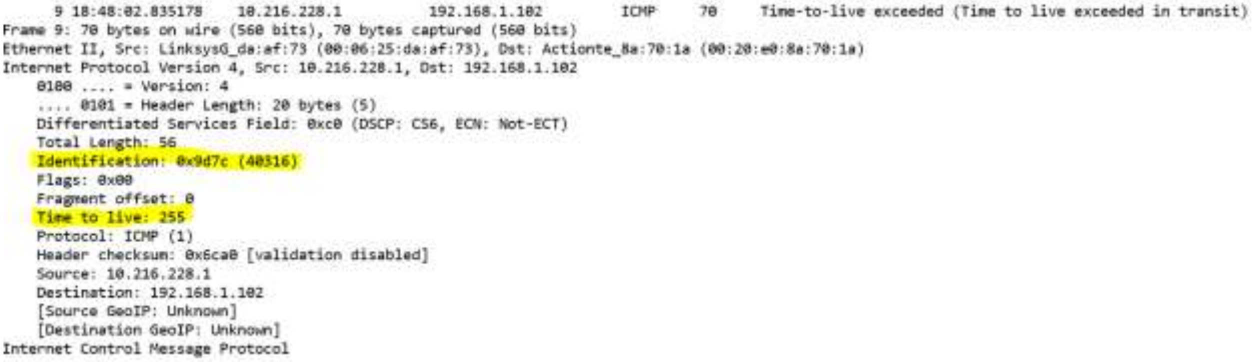
- Version [*IPv4 used for all packets*]
- Header Length [*All ICMP packets*]
- Differentiated Services Field [*Same type of service being used*]
- Total Length [*Similar payload*]
- Flags [*All Stated Not Set*]
- Protocol [*All ICMP packets*]
- Source [*All sent from my computer*]
- Destination [*All sent to the same destination*]
- Source GeoIP [*Stated Unknown*]
- Destination GeoIP [*Stated Unknown*]

Fields that Must Change:

- Identification [*Each packet have their own IDs*]
- Time to Live [*traceroute increments with each packet*]
- Header Checksum [*Along with header changes*]

7. The last two spaces of the IDs consist of the second to last one being a letter that decrements through the alphabet every sixteen packets, and the last space decrementing from letters f to a and then from digits 9 to 0 with every passing packet, and then cycling through again, with each ICMP Echo (ping) request.

8. Value in Identification Field: 0x9d7c (40316)
Value in TTL Field: 255

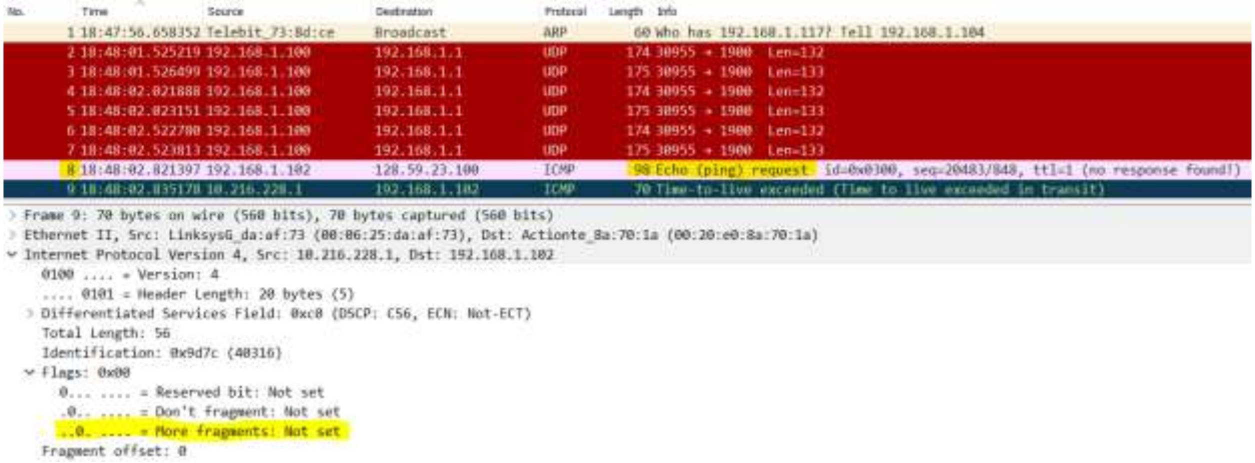


```
      9 18:48:02.835178    10.216.228.1         192.168.1.102        ICMP     70     Time-to-live exceeded (Time to live exceeded in transit)
Frame 9: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
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
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x6ca0 [validation disabled]
    Source: 10.216.228.1
    Destination: 192.168.1.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Internet Control Message Protocol
```

9. The value in the Identification field changes with each reply because they have their own individual id value, yet the value in the TTL field remains unchanged with each reply sent because the first hop router is the same/doesn't change.

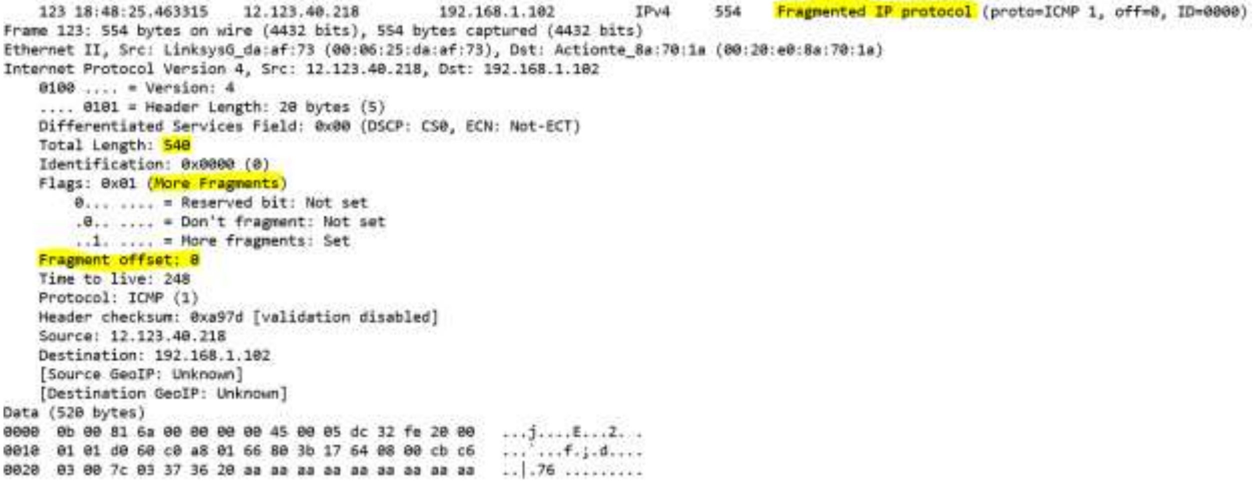
Fragmentation

10. The message has not been fragmented across more than one IP datagram.



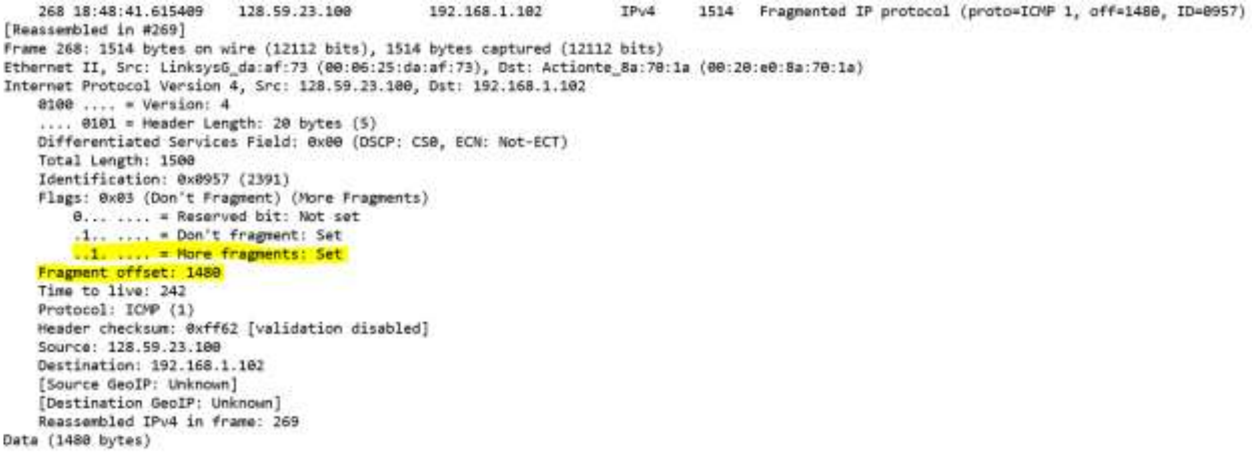
```
No.     Time                Source              Destination         Protocol  Length  Info
      1 18:47:56.658352 Telebit_73:8d:ce    Broadcast           ARP          60 Who has 192.168.1.117? Tell 192.168.1.104
      2 18:48:01.525219 192.168.1.100       192.168.1.1         UDP         174 30955 → 1900  Len=132
      3 18:48:01.526499 192.168.1.100       192.168.1.1         UDP         175 30955 → 1900  Len=133
      4 18:48:02.021888 192.168.1.100       192.168.1.1         UDP         174 30955 → 1900  Len=132
      5 18:48:02.023151 192.168.1.100       192.168.1.1         UDP         175 30955 → 1900  Len=133
      6 18:48:02.522780 192.168.1.100       192.168.1.1         UDP         174 30955 → 1900  Len=132
      7 18:48:02.523813 192.168.1.100       192.168.1.1         UDP         175 30955 → 1900  Len=133
      8 18:48:02.821397 192.168.1.102       128.59.23.100       ICMP         98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
      9 18:48:02.835178 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)
v 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)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
```

11. The title of the “Fragmented IP Protocol” along with the Flags section displaying the statement “More Fragments” are pieces of information in the IP header that indicates that the datagram has been fragmented. The fragment offset section of the datagram is valued at zero, which indicates that this fragment is the first one rather than a latter one. The datagram is 540 bytes long, including the header.



```
    123 18:48:25.463315    12.123.40.218        192.168.1.102        IPv4     554    Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
Frame 123: 554 bytes on wire (4432 bits), 554 bytes captured (4432 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: 12.123.40.218, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 540
    Identification: 0x0000 (0)
    Flags: 0x01 (More Fragments)
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..1. .... = More fragments: Set
    Fragment offset: 0
    Time to live: 248
    Protocol: ICMP (1)
    Header checksum: 0xa97d [validation disabled]
    Source: 12.123.40.218
    Destination: 192.168.1.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Data (520 bytes)
0000  0b 00 81 6a 00 00 00 00 45 00 05 dc 32 fe 20 00   ...j....E...2. .
0010  01 01 d0 60 c0 a8 01 66 80 3b 17 64 08 00 cb c6   ...`...f.;.d....
0020  03 00 7c 03 37 36 20 aa aa aa aa aa aa aa aa aa   ..|.76 .........
```

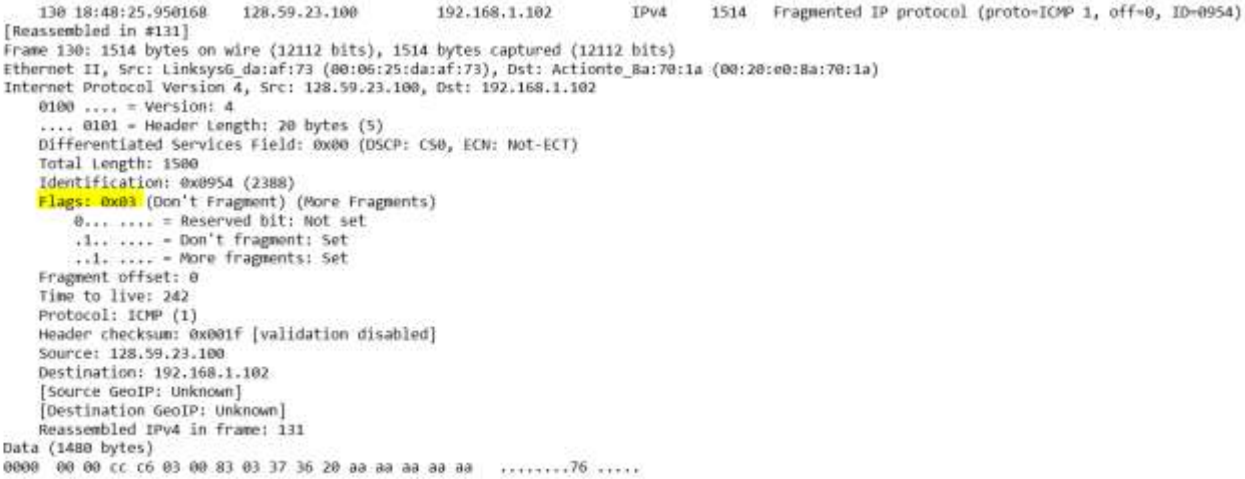
12. Since the fragment offset section of the datagram is set at the value of 1480, indicates that this is not the first datagram fragment. There are also more fragments because the more fragment section is set.



```
    268 18:48:41.615409    128.59.23.100        192.168.1.102        IPv4     1514   Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0957)
[Reassembled in #269]
Frame 268: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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: 128.59.23.100, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x0957 (2391)
    Flags: 0x03 (Don't Fragment) (More Fragments)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..1. .... = More fragments: Set
    Fragment offset: 1480
    Time to live: 242
    Protocol: ICMP (1)
    Header checksum: 0xff62 [validation disabled]
    Source: 128.59.23.100
    Destination: 192.168.1.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 269
Data (1480 bytes)
```

13. The total length, identification, flags, fragment offset, time to live, and header checksum are the fields that changes in the IP header between the first and second fragments.

14. 3 fragments were created from the original datagram, based off the value three stated within the flags section of the datagram.



```
    130 18:48:25.950168    128.59.23.100        192.168.1.102        IPv4     1514   Fragmented IP protocol (proto=ICMP 1, off=0, ID=0954)
[Reassembled in #131]
Frame 130: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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: 128.59.23.100, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x0954 (2388)
    Flags: 0x03 (Don't Fragment) (More Fragments)
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..1. .... = More fragments: Set
    Fragment offset: 0
    Time to live: 242
    Protocol: ICMP (1)
    Header checksum: 0x001f [validation disabled]
    Source: 128.59.23.100
    Destination: 192.168.1.102
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
    Reassembled IPv4 in frame: 131
Data (1480 bytes)
0000  00 00 cc c6 03 00 83 03 37 36 20 aa aa aa aa aa   ........76 .....
```

15. The fields that change in the IP header among the fragments are total length, identification, flags, fragment offset, time to live, and header checksum.