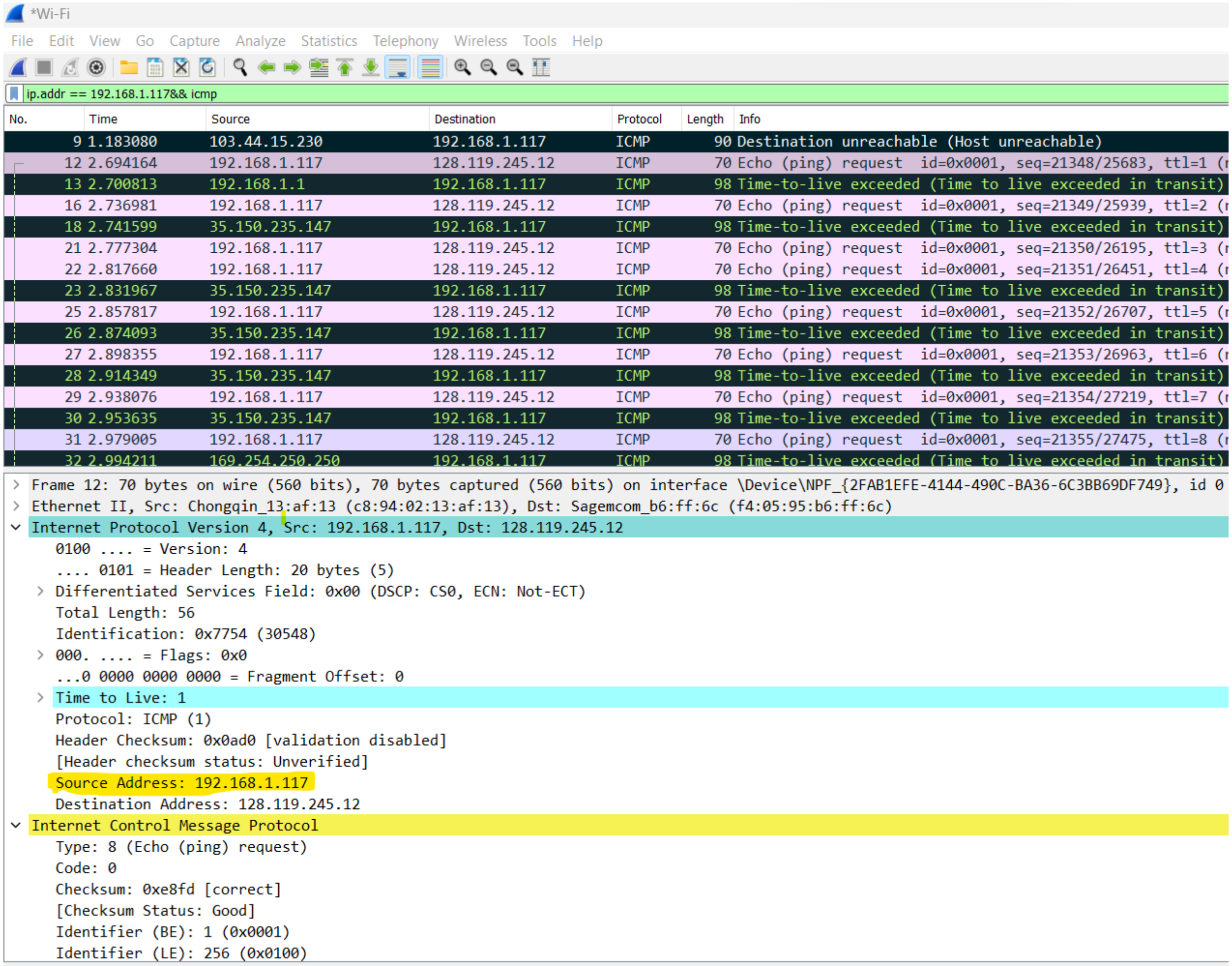
Computer Networks Assignment - 2

Submitted By: N V H Sowndarya
Email ID: sowndaryanoookala.vh@uga.edu

Submission Date: 26th March,23
UGA ID: 811594990

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?**

   The IP address of my computer is 192.168.1.117


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

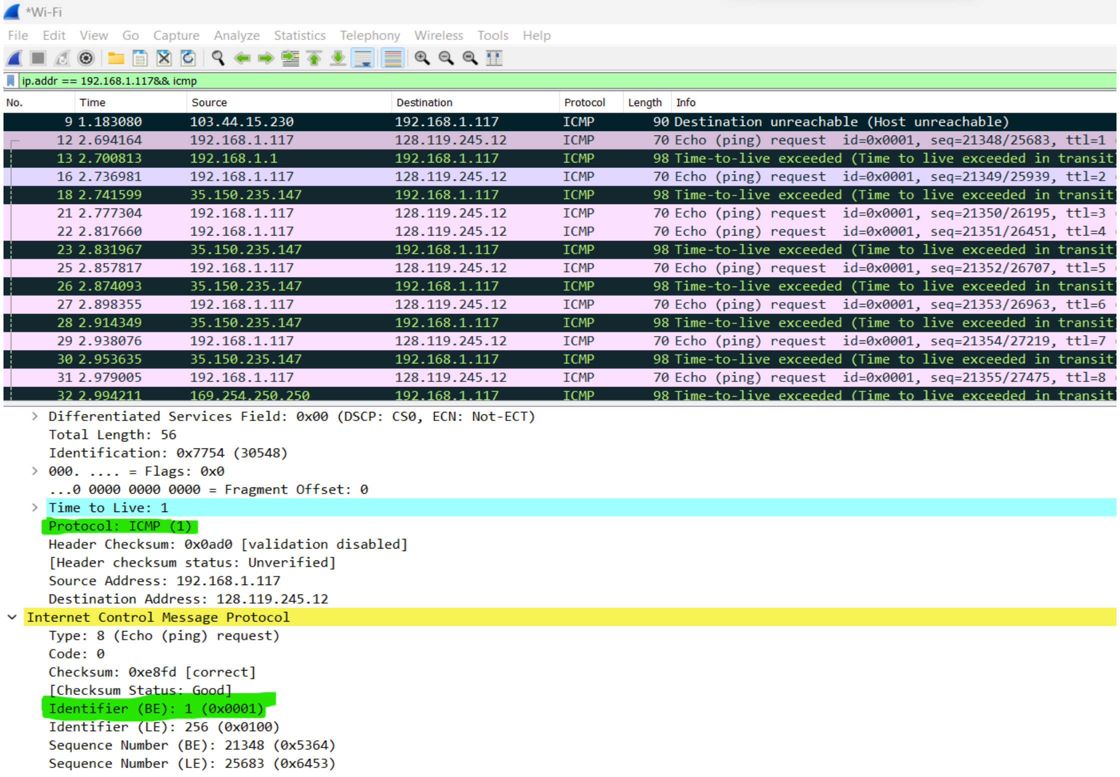
```
ip.addr == 192.168.1.117&& icmp
```

```
No.     Time       Source            Destination       Protocol  Length  Info
      9 1.183080   103.44.15.230     192.168.1.117     ICMP         90 Destination unreachable (Host unreachable)
     12 2.694164   192.168.1.117     128.119.245.12    ICMP         70 Echo (ping) request  id=0x0001, seq=21348/25683, ttl=1 (r
     13 2.700813   192.168.1.1       192.168.1.117     ICMP         98 Time-to-live exceeded (Time to live exceeded in transit)
     16 2.736981   192.168.1.117     128.119.245.12    ICMP         70 Echo (ping) request  id=0x0001, seq=21349/25939, ttl=2 (r
     18 2.741599   35.150.235.147    192.168.1.117     ICMP         98 Time-to-live exceeded (Time to live exceeded in transit)
     21 2.777304   192.168.1.117     128.119.245.12    ICMP         70 Echo (ping) request  id=0x0001, seq=21350/26195, ttl=3 (r
     22 2.817660   192.168.1.117     128.119.245.12    ICMP         70 Echo (ping) request  id=0x0001, seq=21351/26451, ttl=4 (r
     23 2.831967   35.150.235.147    192.168.1.117     ICMP         98 Time-to-live exceeded (Time to live exceeded in transit)
     25 2.857817   192.168.1.117     128.119.245.12    ICMP         70 Echo (ping) request  id=0x0001, seq=21352/26707, ttl=5 (r
     26 2.874093   35.150.235.147    192.168.1.117     ICMP         98 Time-to-live exceeded (Time to live exceeded in transit)
     27 2.898355   192.168.1.117     128.119.245.12    ICMP         70 Echo (ping) request  id=0x0001, seq=21353/26963, ttl=6 (r
     28 2.914349   35.150.235.147    192.168.1.117     ICMP         98 Time-to-live exceeded (Time to live exceeded in transit)
     29 2.938076   192.168.1.117     128.119.245.12    ICMP         70 Echo (ping) request  id=0x0001, seq=21354/27219, ttl=7 (r
     30 2.953635   35.150.235.147    192.168.1.117     ICMP         98 Time-to-live exceeded (Time to live exceeded in transit)
     31 2.979005   192.168.1.117     128.119.245.12    ICMP         70 Echo (ping) request  id=0x0001, seq=21355/27475, ttl=8 (r
     32 2.994211   169.254.250.250   192.168.1.117     ICMP         98 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{2FAB1EFE-4144-490C-BA36-6C3BB69DF749}, id 0
> Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
v Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x7754 (30548)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0ad0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.117
    Destination Address: 128.119.245.12
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xe8fd [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
```

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

   The value in the upper layer protocol field within the header, is ICMP 1(0x0001)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

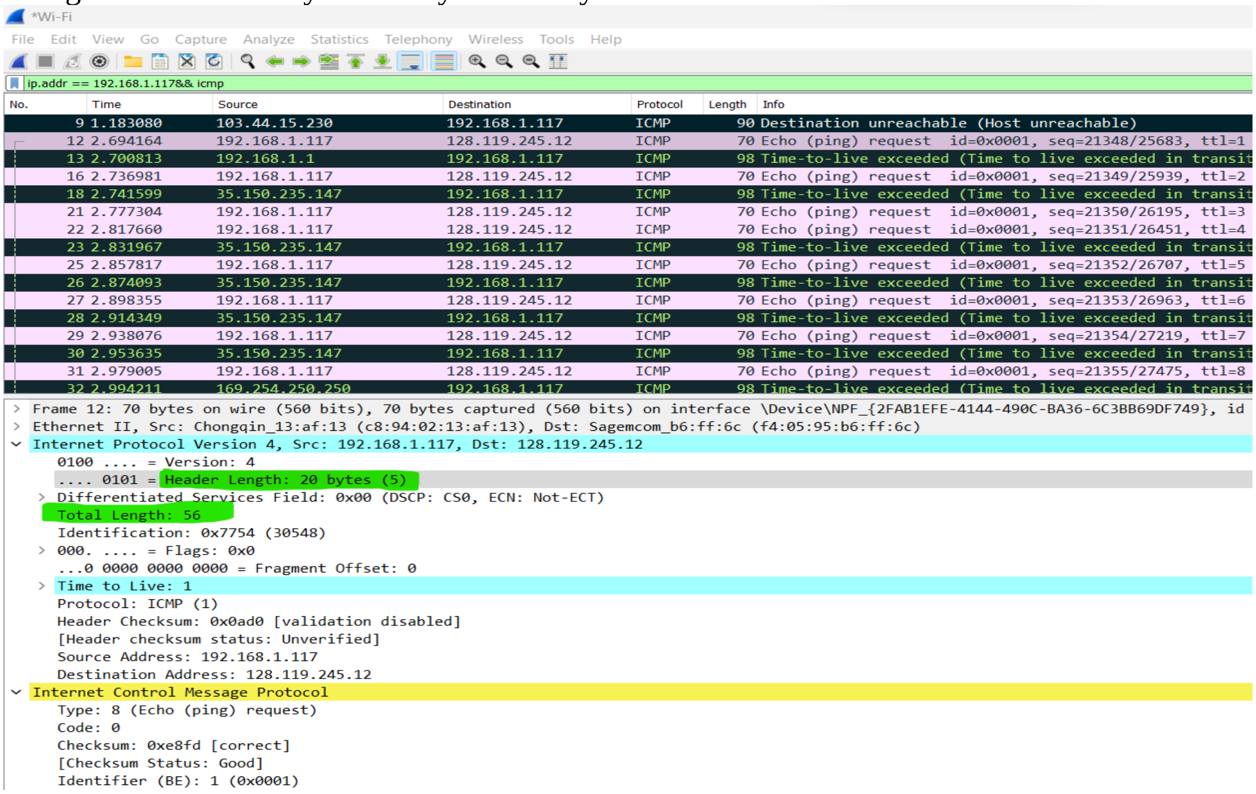
ip.addr == 192.168.1.117&& icmp

```
No.   Time      Source            Destination       Protocol  Length  Info
  9 1.183080    103.44.15.230     192.168.1.117     ICMP      90 Destination unreachable (Host unreachable)
 12 2.694164    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21348/25683, ttl=1
 13 2.700813    192.168.1.1       192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 16 2.736981    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21349/25939, ttl=2
 18 2.741599    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 21 2.777304    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21350/26195, ttl=3
 22 2.817660    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21351/26451, ttl=4
 23 2.831967    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 25 2.857817    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21352/26707, ttl=5
 26 2.874093    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 27 2.898355    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21353/26963, ttl=6
 28 2.914349    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 29 2.938076    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21354/27219, ttl=7
 30 2.953635    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 31 2.979005    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21355/27475, ttl=8
 32 2.994211    169.254.250.250   192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
```

```
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 56
     Identification: 0x7754 (30548)
   > 000. .... = Flags: 0x0
     ...0 0000 0000 0000 = Fragment Offset: 0
   > Time to Live: 1
     Protocol: ICMP (1)
     Header Checksum: 0x0ad0 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 192.168.1.117
     Destination Address: 128.119.245.12
 v Internet Control Message Protocol
     Type: 8 (Echo (ping) request)
     Code: 0
     Checksum: 0xe8fd [correct]
     [Checksum Status: Good]
     Identifier (BE): 1 (0x0001)
     Identifier (LE): 256 (0x0100)
     Sequence Number (BE): 21348 (0x5364)
     Sequence Number (LE): 25683 (0x6453)
```

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 header length is 20 bytes, and the total length is 56 bytes. Therefore, the payload of the IP datagram must be 56 bytes - 20 bytes = 36 bytes.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

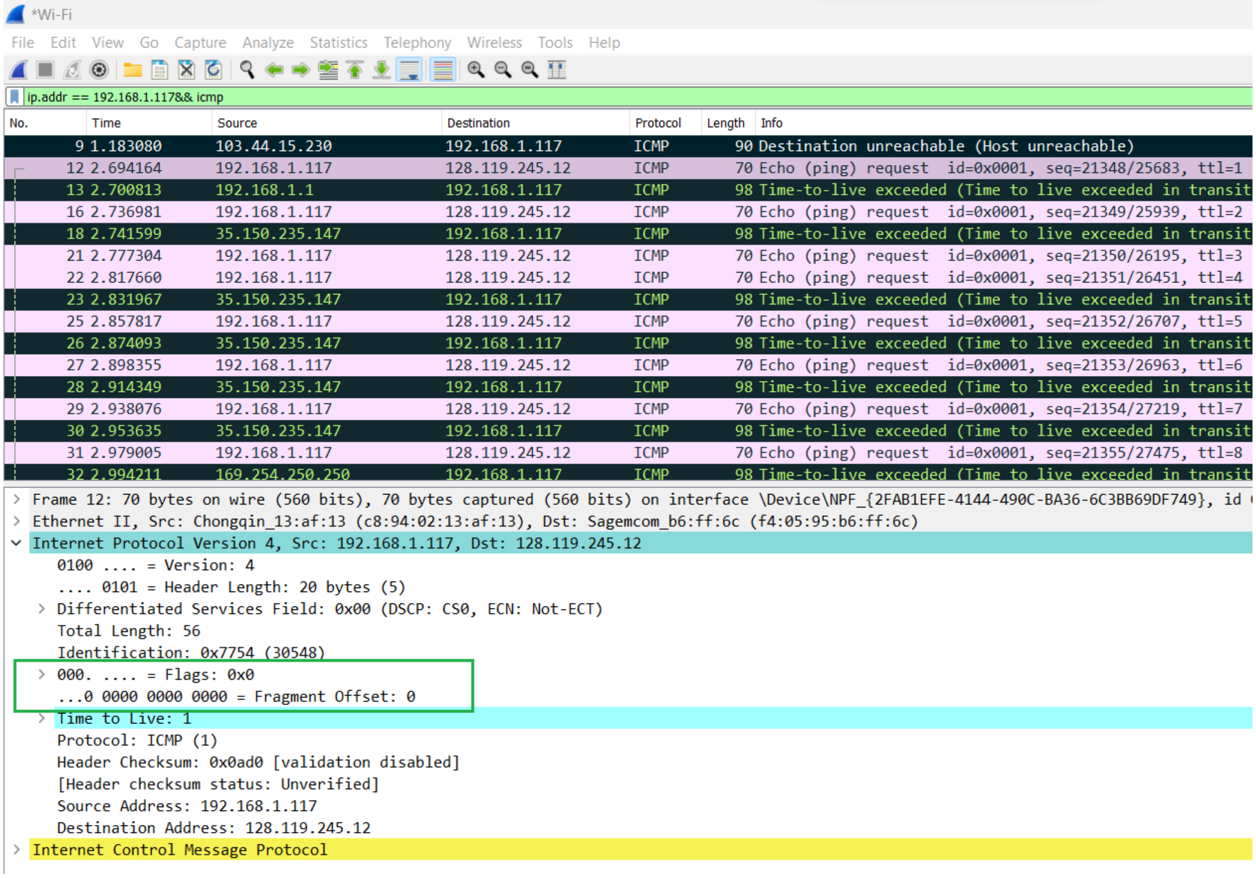
ip.addr == 192.168.1.117&& icmp

```
No.   Time      Source            Destination       Protocol  Length  Info
  9 1.183080    103.44.15.230     192.168.1.117     ICMP      90 Destination unreachable (Host unreachable)
 12 2.694164    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21348/25683, ttl=1
 13 2.700813    192.168.1.1       192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 16 2.736981    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21349/25939, ttl=2
 18 2.741599    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 21 2.777304    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21350/26195, ttl=3
 22 2.817660    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21351/26451, ttl=4
 23 2.831967    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 25 2.857817    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21352/26707, ttl=5
 26 2.874093    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 27 2.898355    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21353/26963, ttl=6
 28 2.914349    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 29 2.938076    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21354/27219, ttl=7
 30 2.953635    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
 31 2.979005    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21355/27475, ttl=8
 32 2.994211    169.254.250.250   192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
```

```
 > Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{2FAB1EFE-4144-490C-BA36-6C3BB69DF749}, id
 > Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
 v Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 56
     Identification: 0x7754 (30548)
   > 000. .... = Flags: 0x0
     ...0 0000 0000 0000 = Fragment Offset: 0
   > Time to Live: 1
     Protocol: ICMP (1)
     Header Checksum: 0x0ad0 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 192.168.1.117
     Destination Address: 128.119.245.12
 v Internet Control Message Protocol
     Type: 8 (Echo (ping) request)
     Code: 0
     Checksum: 0xe8fd [correct]
     [Checksum Status: Good]
     Identifier (BE): 1 (0x0001)
```

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

   In flags section, the more fragments bit = 0 and fragment offset is also set to 0, so we can conclude that the data is not fragmented.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

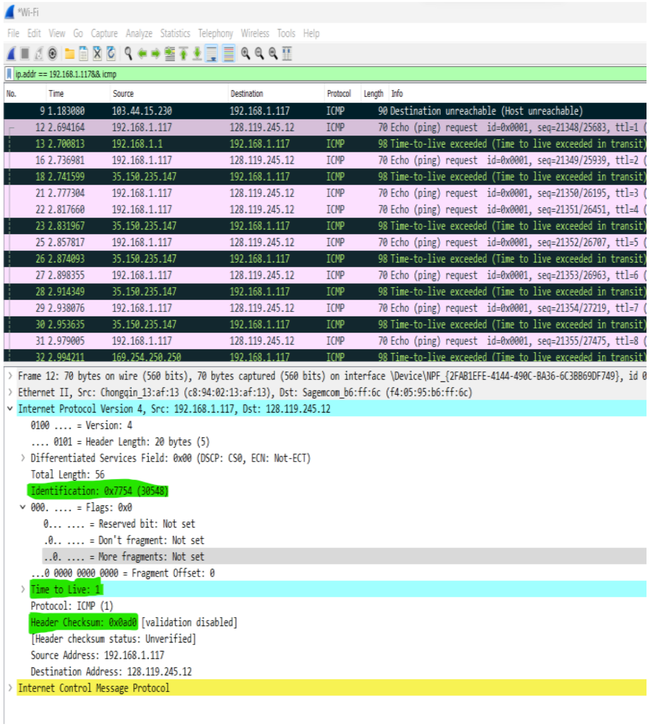
ip.addr == 192.168.1.117&& icmp

```
No.    Time       Source            Destination       Protocol  Length  Info
     9 1.183080   103.44.15.230     192.168.1.117     ICMP        90 Destination unreachable (Host unreachable)
    12 2.694164   192.168.1.117     128.119.245.12    ICMP        70 Echo (ping) request  id=0x0001, seq=21348/25683, ttl=1
    13 2.700813   192.168.1.1       192.168.1.117     ICMP        98 Time-to-live exceeded (Time to live exceeded in transit
    16 2.736981   192.168.1.117     128.119.245.12    ICMP        70 Echo (ping) request  id=0x0001, seq=21349/25939, ttl=2
    18 2.741599   35.150.235.147    192.168.1.117     ICMP        98 Time-to-live exceeded (Time to live exceeded in transit
    21 2.777304   192.168.1.117     128.119.245.12    ICMP        70 Echo (ping) request  id=0x0001, seq=21350/26195, ttl=3
    22 2.817660   192.168.1.117     128.119.245.12    ICMP        70 Echo (ping) request  id=0x0001, seq=21351/26451, ttl=4
    23 2.831967   35.150.235.147    192.168.1.117     ICMP        98 Time-to-live exceeded (Time to live exceeded in transit
    25 2.857817   192.168.1.117     128.119.245.12    ICMP        70 Echo (ping) request  id=0x0001, seq=21352/26707, ttl=5
    26 2.874093   35.150.235.147    192.168.1.117     ICMP        98 Time-to-live exceeded (Time to live exceeded in transit
    27 2.898355   192.168.1.117     128.119.245.12    ICMP        70 Echo (ping) request  id=0x0001, seq=21353/26963, ttl=6
    28 2.914349   35.150.235.147    192.168.1.117     ICMP        98 Time-to-live exceeded (Time to live exceeded in transit
    29 2.938076   192.168.1.117     128.119.245.12    ICMP        70 Echo (ping) request  id=0x0001, seq=21354/27219, ttl=7
    30 2.953635   35.150.235.147    192.168.1.117     ICMP        98 Time-to-live exceeded (Time to live exceeded in transit
    31 2.979005   192.168.1.117     128.119.245.12    ICMP        70 Echo (ping) request  id=0x0001, seq=21355/27475, ttl=8
    32 2.994211   169.254.250.250   192.168.1.117     ICMP        98 Time-to-live exceeded (Time to live exceeded in transit
```

```
> Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{2FAB1EFE-4144-490C-BA36-6C3BB69DF749}, id
> Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
v Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x7754 (30548)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0ad0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.117
    Destination Address: 128.119.245.12
> Internet Control Message Protocol
```

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?**

   From below two screenshots we can observe that the identification, time to live and the header checksum change from one datagram to next.

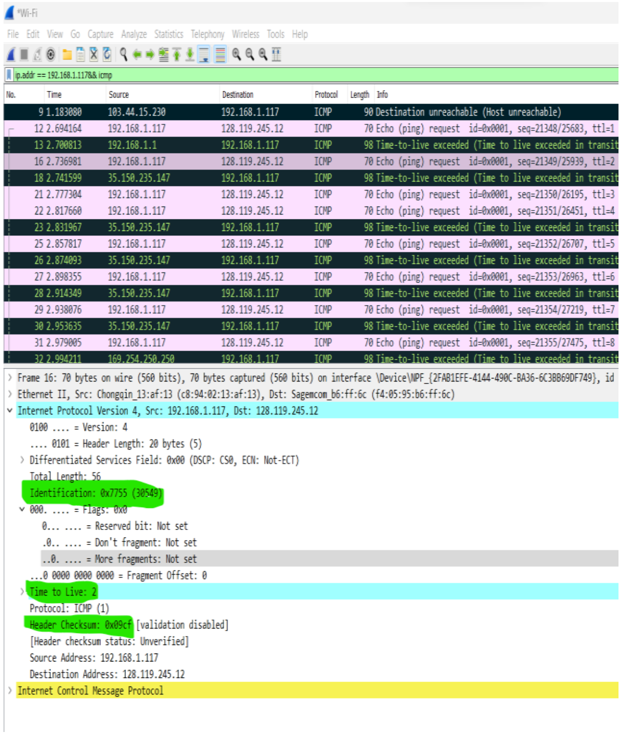


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.1.117&& icmp

No.     Time        Source            Destination       Protocol  Length  Info
      9 1.183080    103.44.15.230     192.168.1.117     ICMP      90 Destination unreachable (Host unreachable)
     12 2.694164    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21348/25683, ttl=1 (
     13 2.700813    192.168.1.1       192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
     16 2.736981    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21349/25939, ttl=2 (
     18 2.741599    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
     21 2.777304    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21350/26195, ttl=3 (
     22 2.817660    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21351/26451, ttl=4 (
     23 2.831967    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
     25 2.857817    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21352/26707, ttl=5 (
     26 2.874093    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
     27 2.898355    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21353/26963, ttl=6 (
     28 2.914349    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
     29 2.938076    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21354/27219, ttl=7 (
     30 2.953635    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)
     31 2.979005    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21355/27475, ttl=8 (
     32 2.994211    169.254.250.250   192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{2FAB1EFE-4144-490C-BA36-6C3BB69DF749}, id 0
> Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
v Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x7754 (30548)
  v 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0ad0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.117
    Destination Address: 128.119.245.12
> Internet Control Message Protocol
```



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.1.117&& icmp

No.     Time        Source            Destination       Protocol  Length  Info
      9 1.183080    103.44.15.230     192.168.1.117     ICMP      90 Destination unreachable (Host unreachable)
     12 2.694164    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21348/25683, ttl=1
     13 2.700813    192.168.1.1       192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
     16 2.736981    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21349/25939, ttl=2
     18 2.741599    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
     21 2.777304    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21350/26195, ttl=3
     22 2.817660    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21351/26451, ttl=4
     23 2.831967    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
     25 2.857817    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21352/26707, ttl=5
     26 2.874093    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
     27 2.898355    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21353/26963, ttl=6
     28 2.914349    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
     29 2.938076    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21354/27219, ttl=7
     30 2.953635    35.150.235.147    192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit
     31 2.979005    192.168.1.117     128.119.245.12    ICMP      70 Echo (ping) request  id=0x0001, seq=21355/27475, ttl=8
     32 2.994211    169.254.250.250   192.168.1.117     ICMP      98 Time-to-live exceeded (Time to live exceeded in transit

> Frame 16: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{2FAB1EFE-4144-490C-BA36-6C3BB69DF749}, id
> Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
v Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x7755 (30549)
  v 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 2
    Protocol: ICMP (1)
    Header Checksum: 0x09cf [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.117
    Destination Address: 128.119.245.12
> Internet Control Message Protocol
```

6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?

The fields that stay constant across the IP datagrams are:

- Version (IP version is 4 for all packets)
- Header Length (All are ICMP)
- Source IP (The requests are sent from same source)
- Destination IP (The requests are being sent to the same destination)
- Differentiated Services (ICMP packets use same Type of Service class)
- Upper Layer Protocol (All are ICMP packets)

The fields that must stay constant are:

- Version (IP version is 4 for all packets)
- Header Length (All are ICMP)
- Source IP (The requests are sent from same source)
- Destination IP (The requests are being sent to the same destination)
- Upper Layer Protocol (All are ICMP packets)
- Differentiated Services (ICMP packets use same Type of Service class)

The fields that must change are:

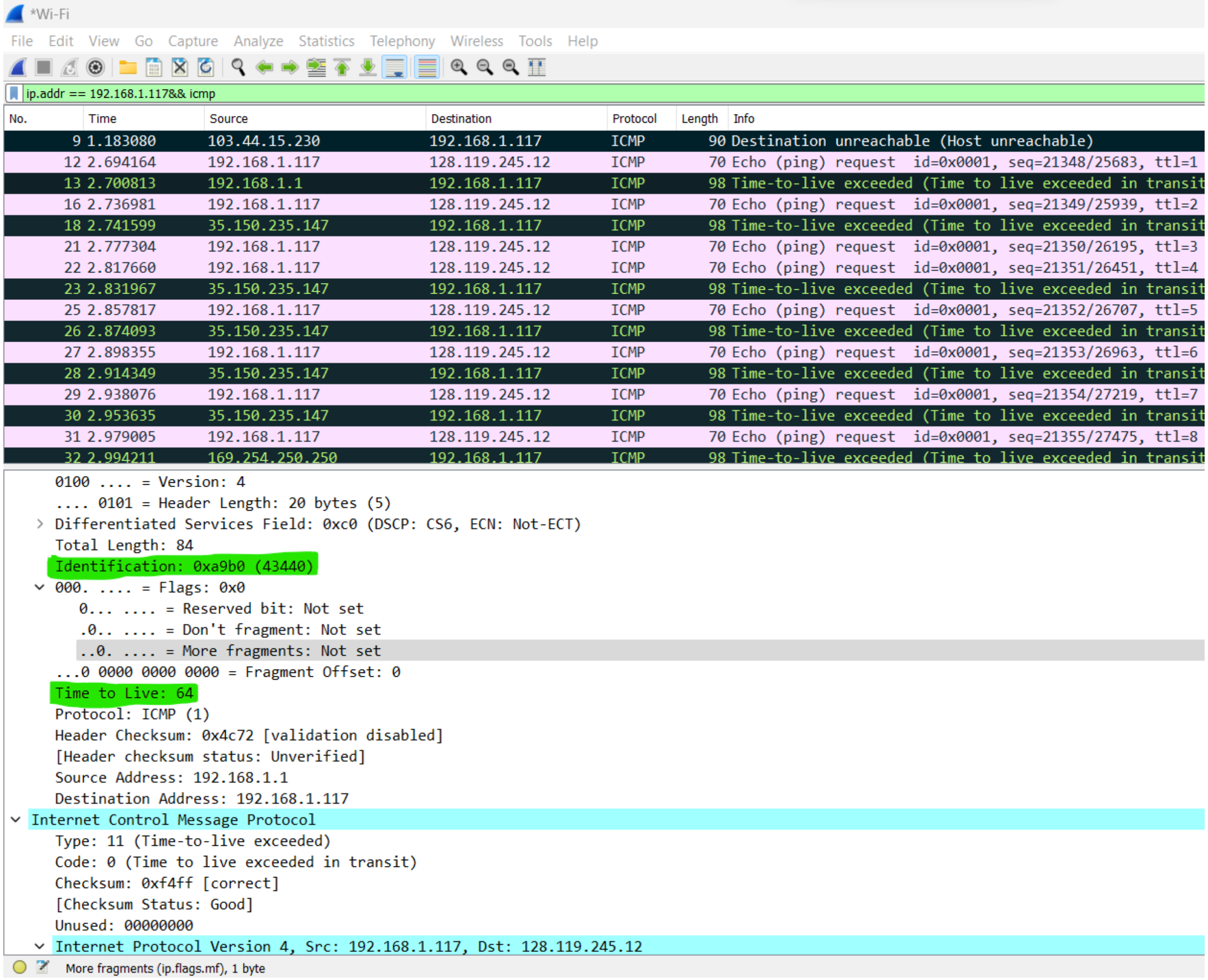
- Identification(IP packets must have different ids)
- Time to live (traceroute increments each subsequent packet)
- Header checksum (since header changes, so must checksum)

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

The pattern we can observe from the IP datagram is that the IP header Identification field increments by one from one request to another request.

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

From the pattern in the ICMP TTL exceeded replies sent to my computer by the nearest (first hop) router, we can observe that the,
Time to Live: 64
Identification: 0xa9b0 (43440)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.117&& icmp

No.	Time	Source	Destination	Protocol	Length	Info
9	1.183080	103.44.15.230	192.168.1.117	ICMP	90	Destination unreachable (Host unreachable)
12	2.694164	192.168.1.117	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=21348/25683, ttl=1
13	2.700813	192.168.1.1	192.168.1.117	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit
16	2.736981	192.168.1.117	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=21349/25939, ttl=2
18	2.741599	35.150.235.147	192.168.1.117	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit
21	2.777304	192.168.1.117	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=21350/26195, ttl=3
22	2.817660	192.168.1.117	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=21351/26451, ttl=4
23	2.831967	35.150.235.147	192.168.1.117	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit
25	2.857817	192.168.1.117	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=21352/26707, ttl=5
26	2.874093	35.150.235.147	192.168.1.117	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit
27	2.898355	192.168.1.117	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=21353/26963, ttl=6
28	2.914349	35.150.235.147	192.168.1.117	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit
29	2.938076	192.168.1.117	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=21354/27219, ttl=7
30	2.953635	35.150.235.147	192.168.1.117	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit
31	2.979005	192.168.1.117	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=21355/27475, ttl=8
32	2.994211	169.254.250.250	192.168.1.117	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xa9b0 (43440)
  v 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x4c72 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.1
    Destination Address: 192.168.1.117
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  v Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
```

More fragments (ip.flags.mf), 1 byte

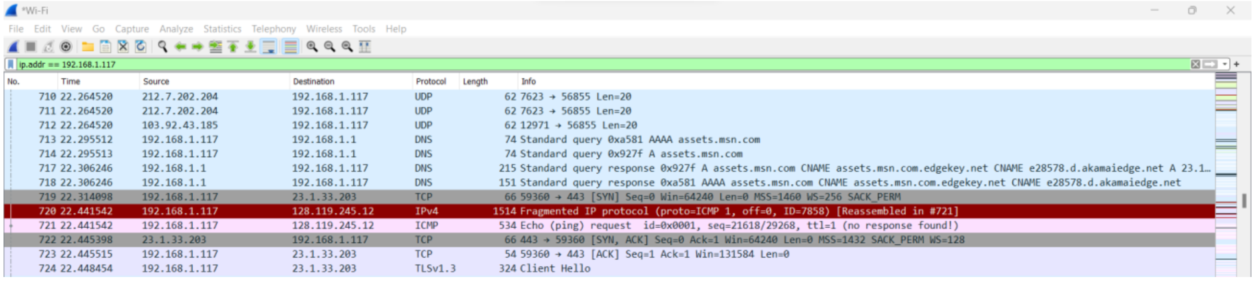
9. **Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?**

   From the data captured in Wireshark, we see that the identification field values for all the ICMP TTL-exceeded replies are different because a unique value is given to identify it for every response. If two or more IP datagrams have the same identification value, it means that they are fragments of one large IP packet.

   The TTL field remains unchanged because all the responses generated by the same hop router are 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?**

From the screenshot we can observe that the packet has been fragmented more than once in 720 line.

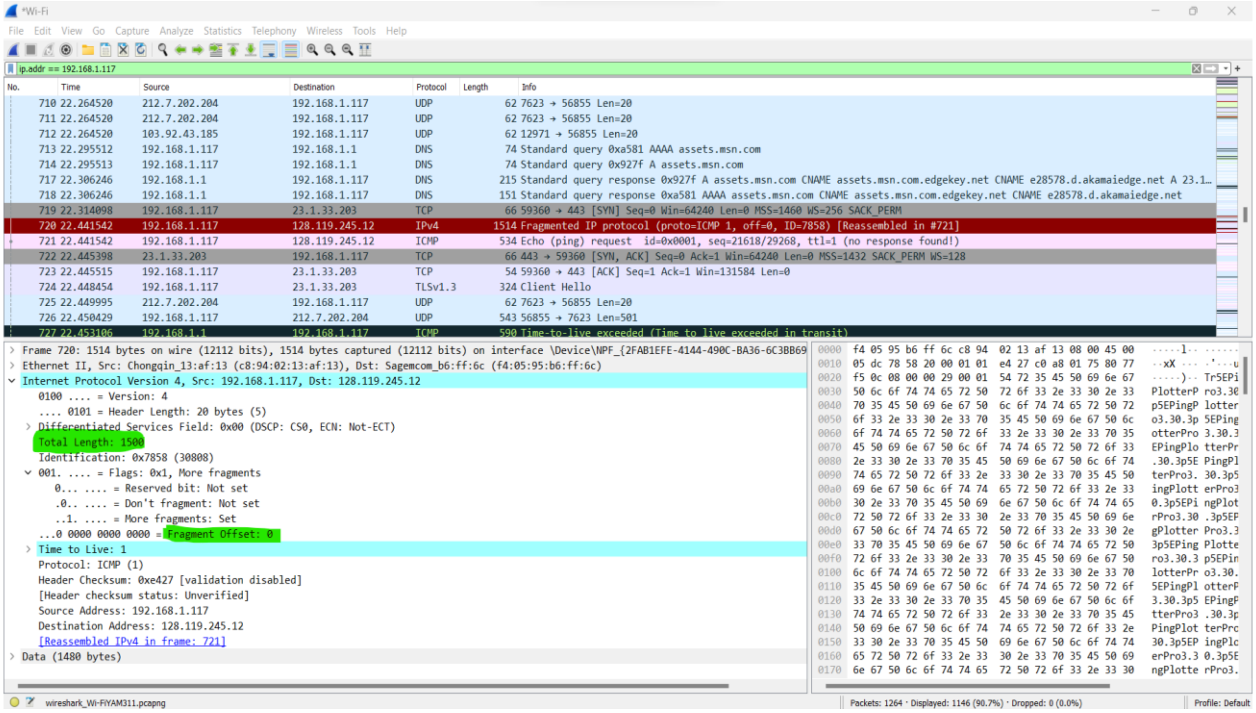

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.1.117

No.  Time       Source         Destination    Protocol Length Info
 710 22.264520  212.7.202.204  192.168.1.117  UDP        62 7623 → 56855 Len=20
 711 22.264520  212.7.202.204  192.168.1.117  UDP        62 7623 → 56855 Len=20
 712 22.264520  103.92.43.185  192.168.1.117  UDP        62 12971 → 56855 Len=20
 713 22.295512  192.168.1.117  192.168.1.1    DNS        74 Standard query 0xa581 AAAA assets.msn.com
 714 22.295513  192.168.1.117  192.168.1.1    DNS        74 Standard query 0x927f A assets.msn.com
 717 22.306246  192.168.1.1    192.168.1.117  DNS       215 Standard query response 0x927f A assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net A 23.1…
 718 22.306246  192.168.1.1    192.168.1.117  DNS       151 Standard query response 0xa581 AAAA assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net
 719 22.314098  192.168.1.117  23.1.33.203    TCP        66 59360 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 720 22.441542  192.168.1.117  128.119.245.12 IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7858) [Reassembled in #721]
 721 22.441542  192.168.1.117  128.119.245.12 ICMP      534 Echo (ping) request  id=0x0001, seq=21618/29268, ttl=1 (no response found!)
 722 22.445398  23.1.33.203    192.168.1.117  TCP        66 443 → 59360 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1432 SACK_PERM WS=128
 723 22.445515  192.168.1.117  23.1.33.203    TCP        54 59360 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
 724 22.448454  192.168.1.117  23.1.33.203    TLSv1.3   324 Client Hello
```

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?**

    In the below screenshot, we can observe that more fragments field has the value “set” under the flags section. The fragment offset is set to ‘0’ which indicates that it is the first segment. The first datagram has total length 1500.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.1.117

No.  Time       Source         Destination    Protocol Length Info
 710 22.264520  212.7.202.204  192.168.1.117  UDP        62 7623 → 56855 Len=20
 711 22.264520  212.7.202.204  192.168.1.117  UDP        62 7623 → 56855 Len=20
 712 22.264520  103.92.43.185  192.168.1.117  UDP        62 12971 → 56855 Len=20
 713 22.295512  192.168.1.117  192.168.1.1    DNS        74 Standard query 0xa581 AAAA assets.msn.com
 714 22.295513  192.168.1.117  192.168.1.1    DNS        74 Standard query 0x927f A assets.msn.com
 717 22.306246  192.168.1.1    192.168.1.117  DNS       215 Standard query response 0x927f A assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net A 23.1…
 718 22.306246  192.168.1.1    192.168.1.117  DNS       151 Standard query response 0xa581 AAAA assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akamaiedge.net
 719 22.314098  192.168.1.117  23.1.33.203    TCP        66 59360 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 720 22.441542  192.168.1.117  128.119.245.12 IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7858) [Reassembled in #721]
 721 22.441542  192.168.1.117  128.119.245.12 ICMP      534 Echo (ping) request  id=0x0001, seq=21618/29268, ttl=1 (no response found!)
 722 22.445398  23.1.33.203    192.168.1.117  TCP        66 443 → 59360 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1432 SACK_PERM WS=128
 723 22.445515  192.168.1.117  23.1.33.203    TCP        54 59360 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
 724 22.448454  192.168.1.117  23.1.33.203    TLSv1.3   324 Client Hello
 725 22.449995  212.7.202.204  192.168.1.117  UDP        62 7623 → 56855 Len=20
 726 22.450429  192.168.1.117  212.7.202.204  UDP       543 56855 → 7623 Len=501
 727 22.453106  192.168.1.1    192.168.1.117  ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
```

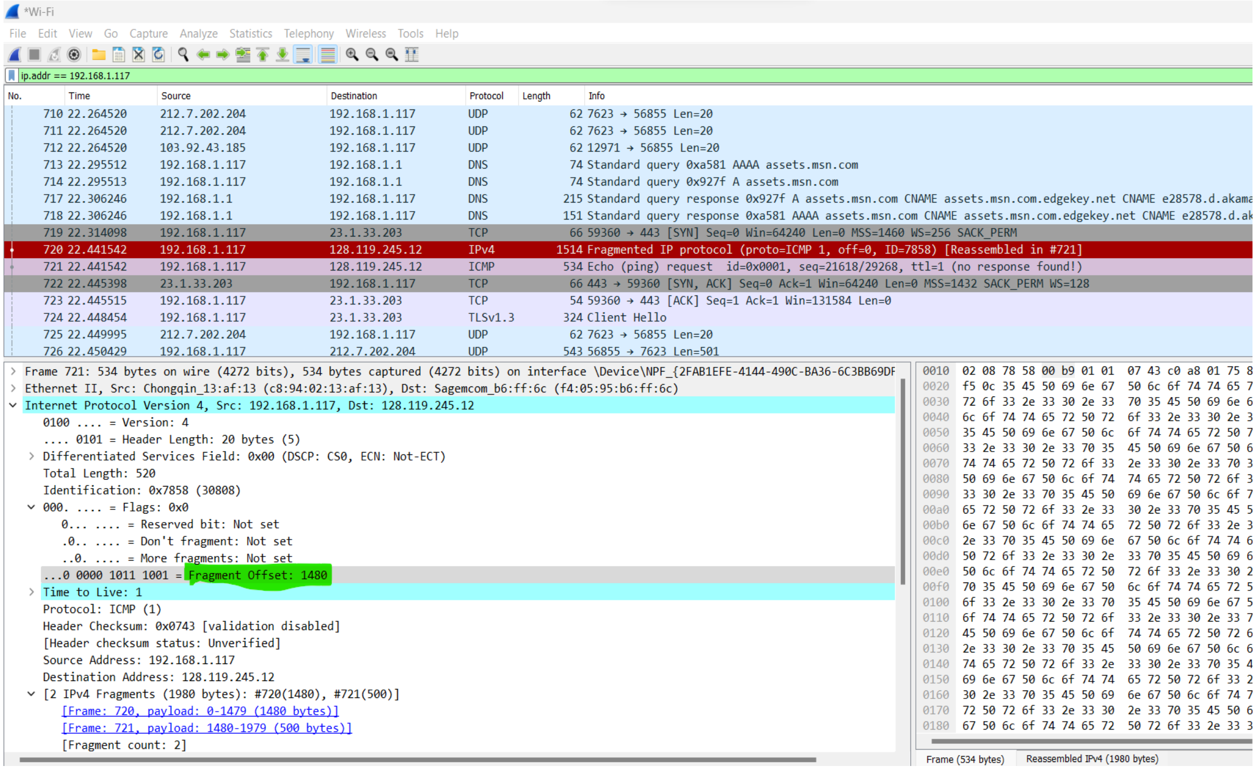
```
> Frame 720: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{2FAB1EFE-4144-490C-BA36-6C3BB69
> Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
v Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x7858 (30808)
  v 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0xe427 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.117
    Destination Address: 128.119.245.12
    [Reassembled IPv4 in frame: 721]
> Data (1480 bytes)
```

```
0000  f4 05 95 b6 ff 6c c8 94  02 13 af 13 08 00 45 00   ·····l·· ······
0010  05 dc 78 58 20 00 01 01  e4 27 c0 a8 01 75 80 77   ··xX ··· ·'···u
0020  f5 0c 08 00 00 29 00 01  54 72 35 45 50 69 6e 67   ·····)·· Tr5EPi
0030  50 6c 6f 74 74 65 72 50  72 6f 33 2e 33 30 2e 33   PlotterP ro3.30
0040  70 35 45 50 69 6e 67 50  6c 6f 74 74 65 72 50 72   p5EPingP lotter
0050  6f 33 2e 33 30 2e 33 70  35 45 50 69 6e 67 50 6c   o3.30.3p 5EPing
0060  6f 74 74 65 72 50 72 6f  33 2e 33 30 2e 33 70 35   otterPro 3.30.3
0070  45 50 69 6e 67 50 6c 6f  74 74 65 72 50 72 6f 33   EPingPlo tterPr
0080  2e 33 30 2e 33 70 35 45  50 69 6e 67 50 6c 6f 74   .30.3p5E PingPl
0090  74 65 72 50 72 6f 33 2e  33 30 2e 33 70 35 45 50   terPro3. 30.3p5
00a0  69 6e 67 50 6c 6f 74 74  65 72 50 72 6f 33 2e 33   ingPlott erPro3
00b0  30 2e 33 70 35 45 50 69  6e 67 50 6c 6f 74 74 65   0.3p5EPi ngPlot
00c0  72 50 72 6f 33 2e 33 30  2e 33 70 35 45 50 69 6e   rPro3.30 .3p5EP
00d0  67 50 6c 6f 74 74 65 72  50 72 6f 33 2e 33 30 2e   gPlotter Pro3.3
00e0  33 70 35 45 50 69 6e 67  50 6c 6f 74 74 65 72 50   3p5EPing Plotte
00f0  72 6f 33 2e 33 30 2e 33  70 35 45 50 69 6e 67 50   ro3.30.3 p5EPin
0100  6c 6f 74 74 65 72 50 72  6f 33 2e 33 30 2e 33 70   lotterPr o3.30.
0110  35 45 50 69 6e 67 50 6c  6f 74 74 65 72 50 72 6f   5EPingPl otterP
0120  33 2e 33 30 2e 33 70 35  45 50 69 6e 67 50 6c 6f   3.30.3p5 EPingP
0130  74 74 65 72 50 72 6f 33  2e 33 30 2e 33 70 35 45   tterPro3 .30.3p
0140  50 69 6e 67 50 6c 6f 74  74 65 72 50 72 6f 33 2e   PingPlot terPro
0150  33 30 2e 33 70 35 45 50  69 6e 67 50 6c 6f 74 74   30.3p5EP ingPlo
0160  65 72 50 72 6f 33 2e 33  30 2e 33 70 35 45 50 69   erPro3.3 0.3p5E
0170  6e 67 50 6c 6f 74 74 65  72 50 72 6f 33 2e 33 30   ngPlotte rPro3.
```

wireshark_Wi-FiYAM311.pcapng
Packets: 1264 · Displayed: 1146 (90.7%) · Dropped: 0 (0.0%)
Profile: Default

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?**

    Below is the screenshot of the second fragment of the datagram. The fragment offset has the value 1480 unlike the first fragment which has value 0 indicating that it is the second fragment. There are not more fragments because under the flag field the more segments has “Not set” value.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.1.117

No.  Time       Source          Destination     Protocol  Length Info
 710 22.264520  212.7.202.204   192.168.1.117   UDP         62 7623 → 56855 Len=20
 711 22.264520  212.7.202.204   192.168.1.117   UDP         62 7623 → 56855 Len=20
 712 22.264520  103.92.43.185   192.168.1.117   UDP         62 12971 → 56855 Len=20
 713 22.295512  192.168.1.117   192.168.1.1     DNS         74 Standard query 0xa581 AAAA assets.msn.com
 714 22.295513  192.168.1.117   192.168.1.1     DNS         74 Standard query 0x927f A assets.msn.com
 717 22.306246  192.168.1.1     192.168.1.117   DNS        215 Standard query response 0x927f A assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.akama
 718 22.306246  192.168.1.1     192.168.1.117   DNS        151 Standard query response 0xa581 AAAA assets.msn.com CNAME assets.msn.com.edgekey.net CNAME e28578.d.ak
 719 22.314098  192.168.1.117   23.1.33.203     TCP         66 59360 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 720 22.441542  192.168.1.117   128.119.245.12  IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=7858) [Reassembled in #721]
 721 22.441542  192.168.1.117   128.119.245.12  ICMP       534 Echo (ping) request  id=0x0001, seq=21618/29268, ttl=1 (no response found!)
 722 22.445398  23.1.33.203     192.168.1.117   TCP         66 443 → 59360 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1432 SACK_PERM WS=128
 723 22.445515  192.168.1.117   23.1.33.203     TCP         54 59360 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
 724 22.448454  192.168.1.117   23.1.33.203     TLSv1.3    324 Client Hello
 725 22.449995  212.7.202.204   192.168.1.117   UDP         62 7623 → 56855 Len=20
 726 22.450429  192.168.1.117   212.7.202.204   UDP        543 56855 → 7623 Len=501
```

```
> Frame 721: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface \Device\NPF_{2FAB1EFE-4144-490C-BA36-6C3BB69DF
> Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
v Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 520
    Identification: 0x7858 (30808)
  v 000. .... = Flags: 0x0
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 1011 1001 = Fragment Offset: 1480
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0743 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.117
    Destination Address: 128.119.245.12
  v [2 IPv4 Fragments (1980 bytes): #720(1480), #721(500)]
      [Frame: 720, payload: 0-1479 (1480 bytes)]
      [Frame: 721, payload: 1480-1979 (500 bytes)]
      [Fragment count: 2]
```

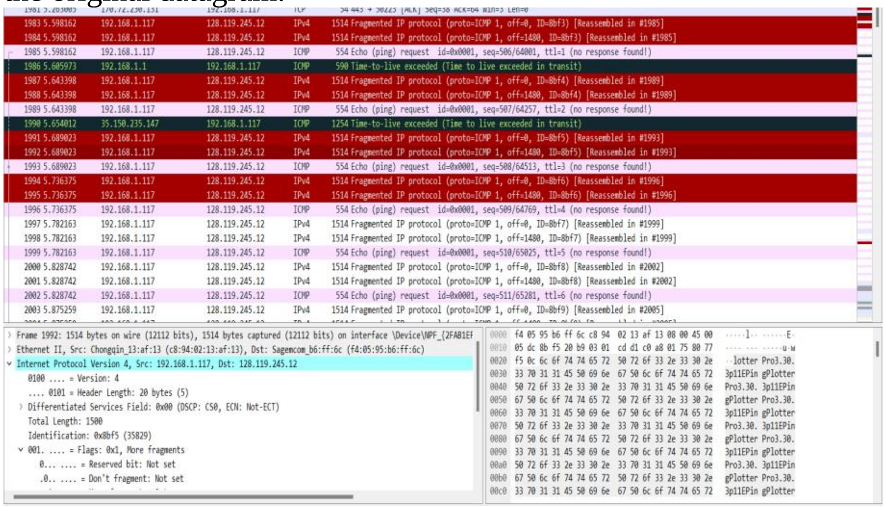
```
0010  02 08 78 58 00 b9 01 01  07 43 c0 a8 01 75 8
0020  f5 0c 35 45 50 69 6e 67  50 6c 6f 74 74 65 7
0030  72 6f 33 2e 33 30 2e 33  70 35 45 50 69 6e 6
0040  6c 6f 74 74 65 72 50 72  6f 33 2e 33 30 2e 3
0050  35 45 50 69 6e 67 50 6c  6f 74 74 65 72 50 7
0060  33 2e 33 30 2e 33 70 35  45 50 69 6e 67 50 6
0070  74 74 65 72 50 72 6f 33  2e 33 30 2e 33 70 3
0080  50 69 6e 67 50 6c 6f 74  74 65 72 50 72 6f 3
0090  33 30 2e 33 70 35 45 50  69 6e 67 50 6c 6f 7
00a0  65 72 50 72 6f 33 2e 33  30 2e 33 70 35 45 5
00b0  6e 67 50 6c 6f 74 74 65  72 50 72 6f 33 2e 3
00c0  2e 33 70 35 45 50 69 6e  67 50 6c 6f 74 74 6
00d0  50 72 6f 33 2e 33 30 2e  33 70 35 45 50 69 6
00e0  50 6c 6f 74 74 65 72 50  72 6f 33 2e 33 30 2
00f0  70 35 45 50 69 6e 67 50  6c 6f 74 74 65 72 5
0100  6f 33 2e 33 30 2e 33 70  35 45 50 69 6e 67 5
0110  6f 74 74 65 72 50 72 6f  33 2e 33 30 2e 33 7
0120  45 50 69 6e 67 50 6c 6f  74 74 65 72 50 72 6
0130  2e 33 30 2e 33 70 35 45  50 69 6e 67 50 6c 6
0140  74 65 72 50 72 6f 33 2e  33 30 2e 33 70 35 4
0150  69 6e 67 50 6c 6f 74 74  65 72 50 72 6f 33 2
0160  30 2e 33 70 35 45 50 69  6e 67 50 6c 6f 74 7
0170  72 50 72 6f 33 2e 33 30  2e 33 70 35 45 50 6
0180  67 50 6c 6f 74 74 65 72  50 72 6f 33 2e 33 3
```

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

The fields in the IP header that has changed between the first and second fragments are the total length, flags, checksum, and the fragment offset.

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

When the number of bytes is changed from 2000 to 3500 bytes, three fragments are created from the original datagram.



```
1981 5.263005  170.72.230.131  192.168.1.117   TCP    54 443 → 50225 [ACK] Seq=38 Ack=64 Win=3 Len=0
1983 5.598162  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=8bf3) [Reassembled in #1985]
1984 5.598162  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8bf3) [Reassembled in #1985]
1985 5.598162  192.168.1.117   128.119.245.12  ICMP  554 Echo (ping) request  id=0x0001, seq=506/64001, ttl=1 (no response found!)
1986 5.605973  192.168.1.1     192.168.1.117   ICMP  590 Time-to-live exceeded (Time to live exceeded in transit)
1987 5.643398  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=8bf4) [Reassembled in #1989]
1988 5.643398  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8bf4) [Reassembled in #1989]
1989 5.643398  192.168.1.117   128.119.245.12  ICMP  554 Echo (ping) request  id=0x0001, seq=507/64257, ttl=2 (no response found!)
1990 5.654012  35.150.235.147  192.168.1.117   ICMP 1254 Time-to-live exceeded (Time to live exceeded in transit)
1991 5.689023  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=8bf5) [Reassembled in #1993]
1992 5.689023  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8bf5) [Reassembled in #1993]
1993 5.689023  192.168.1.117   128.119.245.12  ICMP  554 Echo (ping) request  id=0x0001, seq=508/64513, ttl=3 (no response found!)
1994 5.736375  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=8bf6) [Reassembled in #1996]
1995 5.736375  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8bf6) [Reassembled in #1996]
1996 5.736375  192.168.1.117   128.119.245.12  ICMP  554 Echo (ping) request  id=0x0001, seq=509/64769, ttl=4 (no response found!)
1997 5.782163  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=8bf7) [Reassembled in #1999]
1998 5.782163  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8bf7) [Reassembled in #1999]
1999 5.782163  192.168.1.117   128.119.245.12  ICMP  554 Echo (ping) request  id=0x0001, seq=510/65025, ttl=5 (no response found!)
2000 5.828742  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=8bf8) [Reassembled in #2002]
2001 5.828742  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8bf8) [Reassembled in #2002]
2002 5.828742  192.168.1.117   128.119.245.12  ICMP  554 Echo (ping) request  id=0x0001, seq=511/65281, ttl=6 (no response found!)
2003 5.875259  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=8bf9) [Reassembled in #2005]
2004 5.875259  192.168.1.117   128.119.245.12  IPv4 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8bf9) [Reassembled in #2005]
```

```
> Frame 1992: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{2FAB1EF
> Ethernet II, Src: Chongqin_13:af:13 (c8:94:02:13:af:13), Dst: Sagemcom_b6:ff:6c (f4:05:95:b6:ff:6c)
v Internet Protocol Version 4, Src: 192.168.1.117, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x8bf5 (35829)
  v 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
```

```
0000  f4 05 95 b6 ff 6c c8 94  02 13 af 13 08 00 45 00   ·····l·· ······E·
0010  05 dc 8b f5 20 b9 03 01  cd d1 c0 a8 01 75 80 77   ···· ··· ·····u·w
0020  f5 0c 6c 6f 74 74 65 72  50 72 6f 33 2e 33 30 2e   ··lotter Pro3.30.
0030  33 70 31 31 45 50 69 6e  67 50 6c 6f 74 74 65 72   3p11EPin gPlotter
0040  50 72 6f 33 2e 33 30 2e  33 70 31 31 45 50 69 6e   Pro3.30. 3p11EPin
0050  67 50 6c 6f 74 74 65 72  50 72 6f 33 2e 33 30 2e   gPlotter Pro3.30.
0060  33 70 31 31 45 50 69 6e  67 50 6c 6f 74 74 65 72   3p11EPin gPlotter
0070  50 72 6f 33 2e 33 30 2e  33 70 31 31 45 50 69 6e   Pro3.30. 3p11EPin
0080  67 50 6c 6f 74 74 65 72  50 72 6f 33 2e 33 30 2e   gPlotter Pro3.30.
0090  33 70 31 31 45 50 69 6e  67 50 6c 6f 74 74 65 72   3p11EPin gPlotter
00a0  50 72 6f 33 2e 33 30 2e  33 70 31 31 45 50 69 6e   Pro3.30. 3p11EPin
00b0  67 50 6c 6f 74 74 65 72  50 72 6f 33 2e 33 30 2e   gPlotter Pro3.30.
00c0  33 70 31 31 45 50 69 6e  67 50 6c 6f 74 74 65 72   3p11EPin gPlotter
```

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

There are two fields that change: checksums and fragment offsets (0, 1480, 2960 for first, second, and third fragments, respectively). The first and second packets are 1500 bytes in length, and their more fragments flags are both set to "Set", but the third fragment is 540 bytes in length, and its flag value is "Not Set", indicating that it is the last fragment.