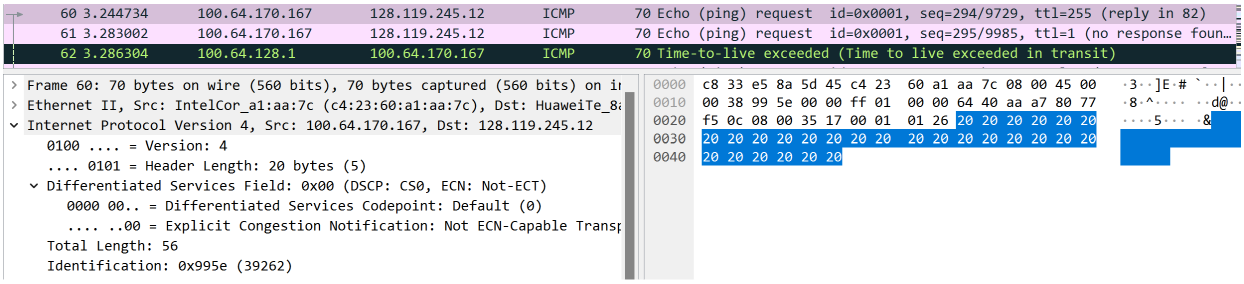
Wireshark:ip

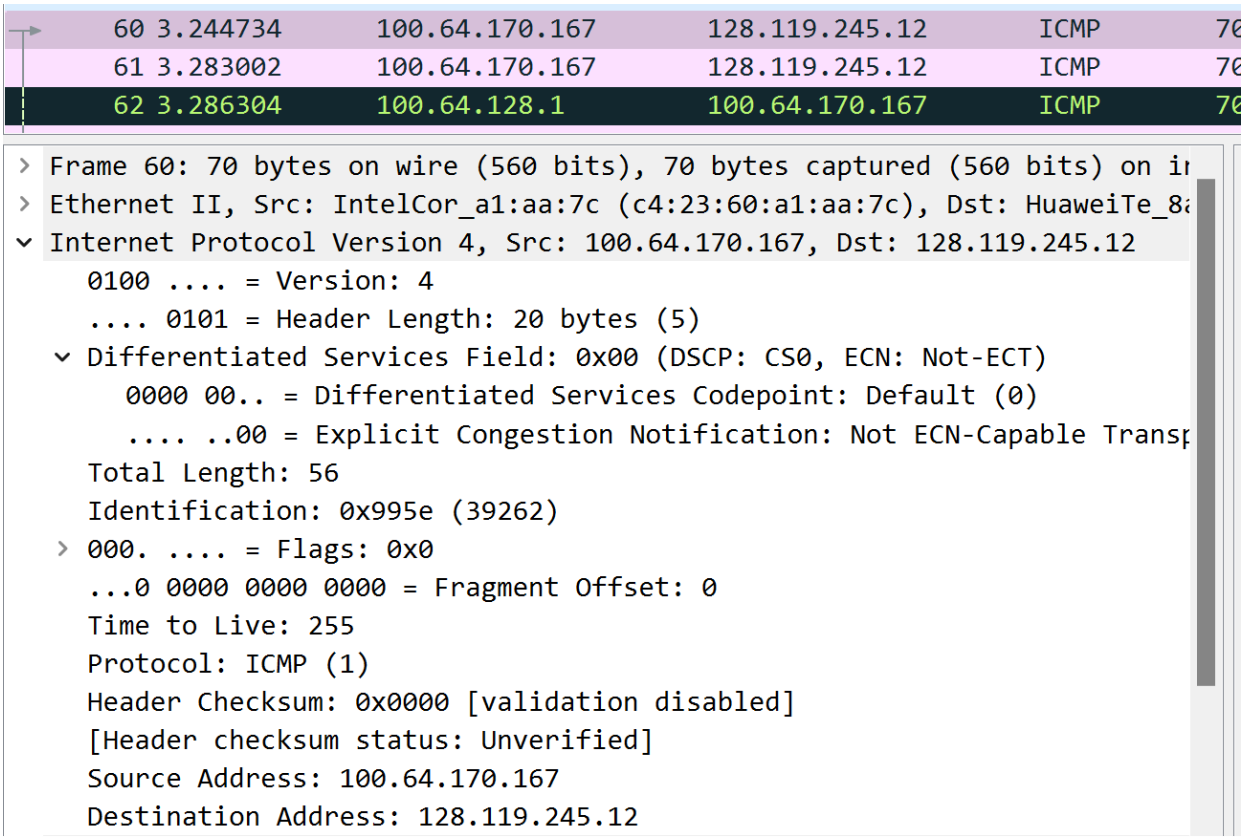
A look at the captured trace

1-7

1.Src是100.64.170.167



2.上层协议是ICMP协议，字段值为1。



3.IP头为20字节，IP数据报的数据负载为36字节，这里的判断方法是用total length(56)-header length(20)=36字节

```
    60 3.244734     100.64.170.167    128.119.245.12    ICMP    70
    61 3.283002     100.64.170.167    128.119.245.12    ICMP    70
    62 3.286304     100.64.128.1      100.64.170.167    ICMP    70
```

```
> Frame 60: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on i
> Ethernet II, Src: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c), Dst: HuaweiTe_8
v Internet Protocol Version 4, Src: 100.64.170.167, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transp
    Total Length: 56
    Identification: 0x995e (39262)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 100.64.170.167
    Destination Address: 128.119.245.12
```

4.没有分段，根据信息中Fragment Offset为0可知，根据Not set辅助可知。

```
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: 255
  Protocol: ICMP (1)
```

5.对比可知：数据报中一直在改变的数据有：标识号、校验和、存活时间以及有效负载的数据

```
> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 56
  Identification: 0x03e2 (994)
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: 255
  Protocol: ICMP (1)
  Header Checksum: 0xc3f9 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 100.64.128.1
  Destination Address: 100.64.170.167
```

```
> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 56
  Identification: 0x0151 (337)
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: 255
  Protocol: ICMP (1)
  Header Checksum: 0xc68a [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 100.64.128.1
  Destination Address: 100.64.170.167
```

6.保持不变：

显式拥塞通告、全长、 标识符、分片偏移 、源地址 、目的地址、选项

必须保持不变：version(版本)、header length(首部长度)、differentiated service(区别服务)、protocol(协议)

必须改变：标识号、校验和、存活时间、有效负载的数据

```
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 56
  Identification: 0x0151 (337)
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: 255
  Protocol: ICMP (1)
  Header Checksum: 0xc68a [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 100.64.128.1
  Destination Address: 100.64.170.167
```

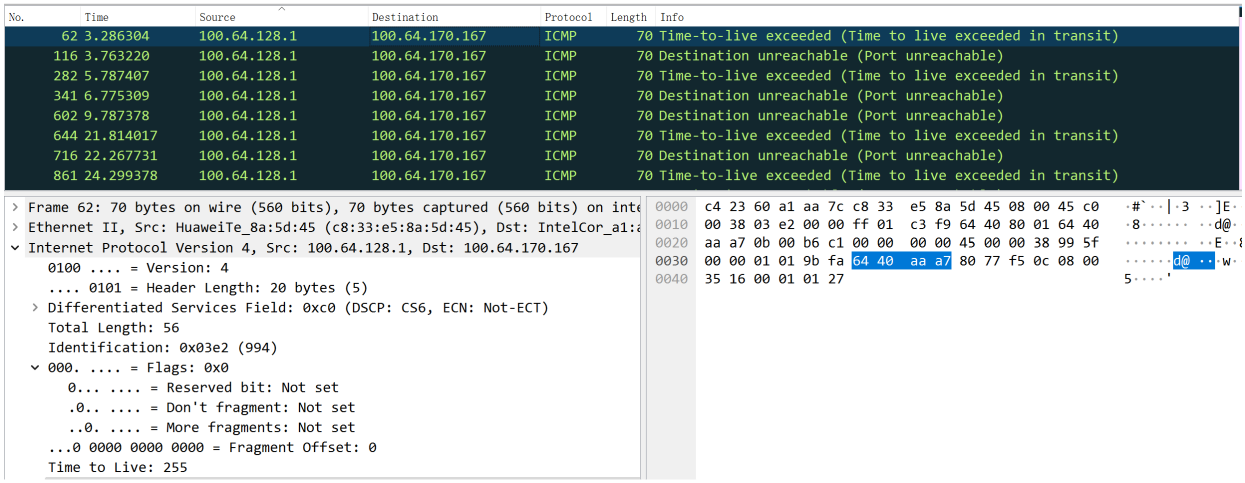
7.所有从本地电脑发向同一目的地址的IP数据报的标识符是连续递增的，且每次增加1

```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 56
  Identification: 0x995e (39262)
v 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
```

```
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 56
  Identification: 0x995f (39263)
v 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 56
  Identification: 0x9960 (39264)
v 000. .... = Flags: 0x0
```

8-9

8.标识号为0X03e2，TTL为225



No.	Time	Source	Destination	Protocol	Length	Info
62	3.286304	100.64.128.1	100.64.170.167	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
116	3.763220	100.64.128.1	100.64.170.167	ICMP	70	Destination unreachable (Port unreachable)
282	5.787407	100.64.128.1	100.64.170.167	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
341	6.775309	100.64.128.1	100.64.170.167	ICMP	70	Destination unreachable (Port unreachable)
602	9.787378	100.64.128.1	100.64.170.167	ICMP	70	Destination unreachable (Port unreachable)
644	21.814017	100.64.128.1	100.64.170.167	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
716	22.267731	100.64.128.1	100.64.170.167	ICMP	70	Destination unreachable (Port unreachable)
861	24.299378	100.64.128.1	100.64.170.167	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

```
> Frame 62: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on inte
> Ethernet II, Src: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45), Dst: IntelCor_a1:a
v Internet Protocol Version 4, Src: 100.64.128.1, Dst: 100.64.170.167
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x03e2 (994)
  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: 255
```

```
0000  c4 23 60 a1 aa 7c c8 33  e5 8a 5d 45 08 00 45 c0   ·#`··|·3 ··]E·
0010  00 38 03 e2 00 00 ff 01  c3 f9 64 40 80 01 64 40   ·8······ ··d@··
0020  aa a7 0b 00 b6 c1 00 00  00 00 45 00 00 38 99 5f   ·····E··8·
0030  00 00 01 01 9b fa 64 40  aa a7 80 77 f5 0c 08 00   ·····d@ ···w····
0040  35 16 00 01 01 27                                 5····'
```

9.标识号改变，但TTL不变，因为一个路由中的数据包具有相同的寿命，而除了来自同一分段的数据会有相同标识外，其他数据包都会有唯一的标识。而对我们现在分析的IP数据报没有分段，显然每个响应中的标识号应该不同。

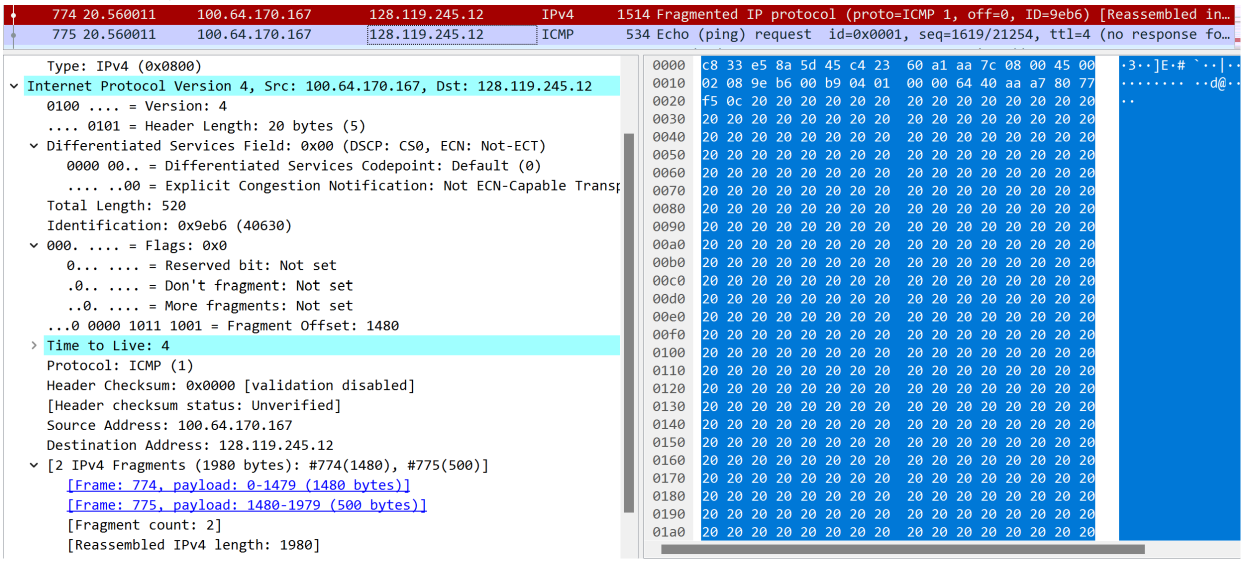
```
  Identification: 0x03e2 (994)
v 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 255
  Protocol: ICMP (1)
```

```
   Identification: 0x0151 (337)
 ⌄ 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: 255
   Protocol: ICMP (1)
   Identification: 0x03fc (1020)
 ⌄ 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: 255
   Protocol: ICMP (1)
```

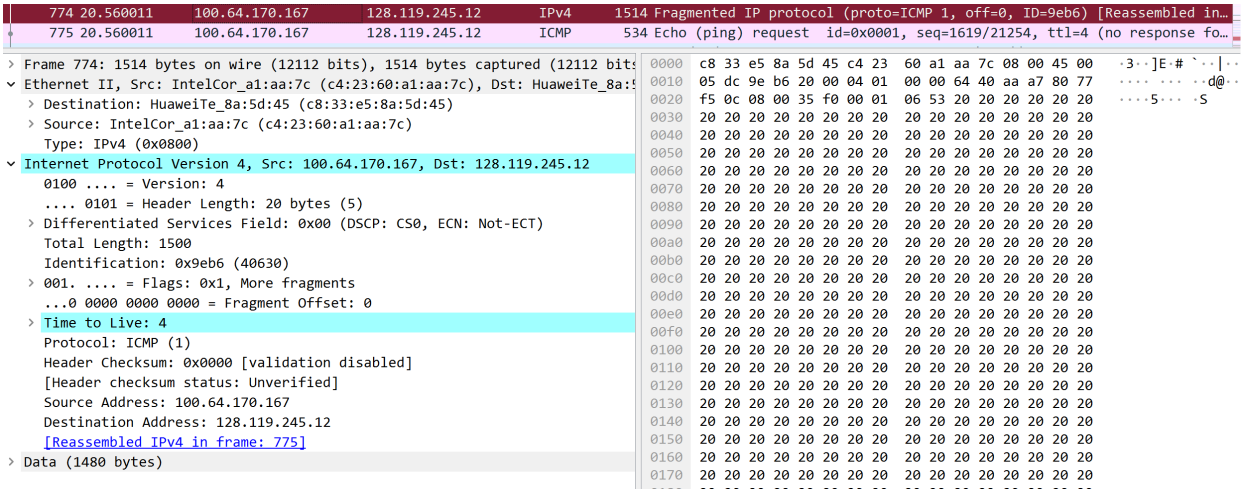
Fragmentation

10-13

10.发送2000bytes的数据后进行了分片，分为了两片



11.由flag=0x1可知，有分片，由more fragments可知，后面还有其它分片，这个ip数据报长1500字节。



12.Fragment Offset: 1480看出来这不是第一个分片，flag=0看出这是最后一个分片。且由于包大小为2000bytes，一个分片最大为1500字节，2000字节只能够分成两个片，故后面不会再有更多的分片。

```
Ethernet II, Src: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c), Dst: HuaweiTe_8a
  > Destination: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
  > Source: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 100.64.170.167, 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: 0x9eb6 (40630)
  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: 4
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 100.64.170.167
    Destination Address: 128.119.245.12
  v [2 IPv4 Fragments (1980 bytes): #774(1480), #775(500)]
      [Frame: 774, payload: 0-1479 (1480 bytes)]
      [Frame: 775, payload: 1480-1979 (500 bytes)]
```

13.总长度、标志、校验和字段发生了变化

14-15

14.3个

```
    Destination Address: 128.119.245.12
  v [3 IPv4 Fragments (3480 bytes): #5779(1480), #5780(1480), #5781(520)]
      [Frame: 5779, payload: 0-1479 (1480 bytes)]
      [Frame: 5780, payload: 1480-2959 (1480 bytes)]
      [Frame: 5781, payload: 2960-3479 (520 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 3480]
      [Reassembled IPv4 data: 080016c70001075e2020202020202020202020202020
```

15.总长度、标志、校验和字段发生了变化

```
Ethernet II, Src: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c), Dst: HuaweiTe_8a
  > Destination: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
  > Source: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 100.64.170.167, 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: 0x9fc1 (40897)
  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: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 100.64.170.167
    Destination Address: 128.119.245.12
    [Reassembled IPv4 in frame: 5781]
Ethernet II, Src: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c), Dst: HuaweiTe_8a
  > Destination: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
  > Source: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 100.64.170.167, 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: 0x9fc1 (40897)
  v 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 100.64.170.167
    Destination Address: 128.119.245.12
    [Reassembled IPv4 in frame: 5781]
Ethernet II, Src: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c), Dst: HuaweiTe_8a
  > Destination: HuaweiTe_8a:5d:45 (c8:33:e5:8a:5d:45)
  > Source: IntelCor_a1:aa:7c (c4:23:60:a1:aa:7c)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 100.64.170.167, 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: 540
Identification: 0x9fc1 (40897)
v 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
...0 0001 0111 0010 = Fragment Offset: 2960
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 100.64.170.167
Destination Address: 128.119.245.12
v [3 IPv4 Fragments (3480 bytes): #5779(1480), #5780(1480), #5781(520)]
```