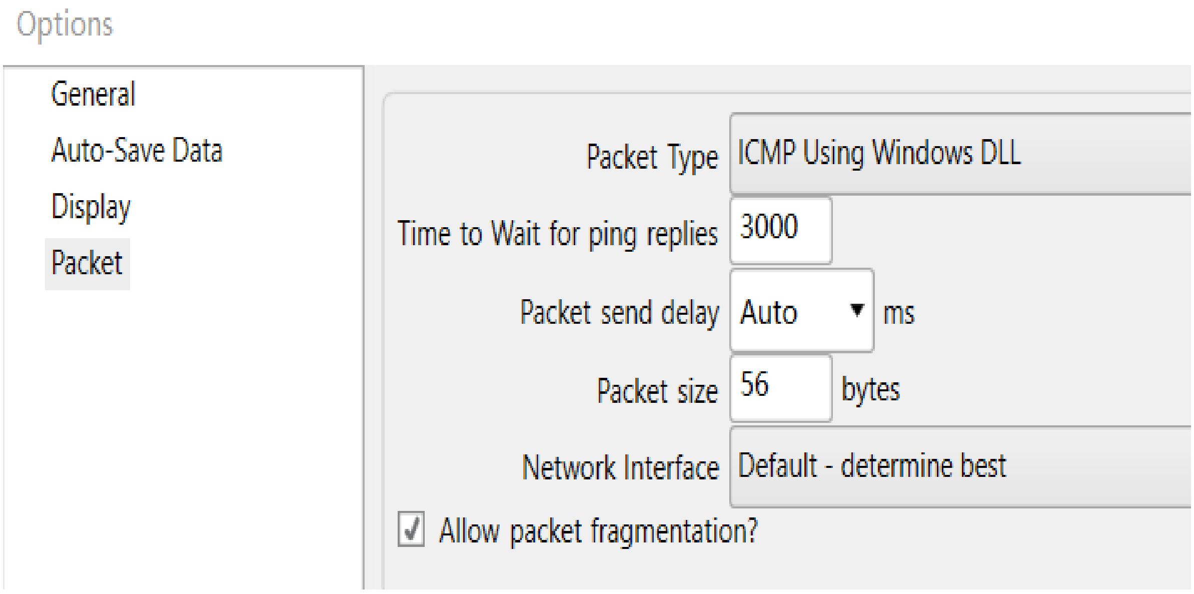
Wireshark Lab: IP v7.0

实验步骤：

1.开始wireshark捕获

2.在pingplotter中要跟踪的地址窗口一栏中填入地址，此处我填入的是gaia.cs.umass.edu，将packet size修改为56，接下来再将packet size修改为2000以捕获大一点的数据报



Options

Packet Type: ICMP Using Windows DLL

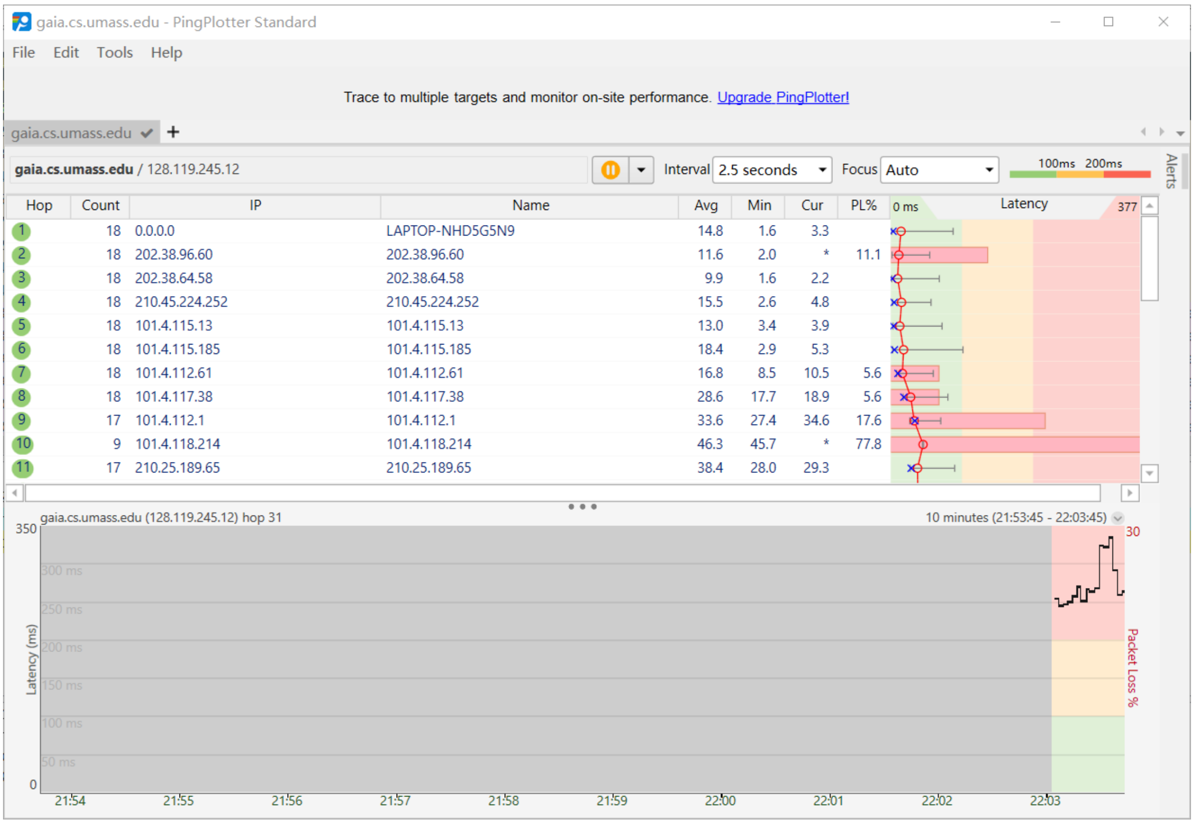
Time to Wait for ping replies: 3000

Packet send delay: Auto ms

Packet size: 56 bytes

Network Interface: Default - determine best

☑ Allow packet fragmentation?



gaia.cs.umass.edu - PingPlotter Standard

Trace to multiple targets and monitor on-site performance. Upgrade PingPlotter!

gaia.cs.umass.edu / 128.119.245.12

Interval: 2.5 seconds

Focus: Auto

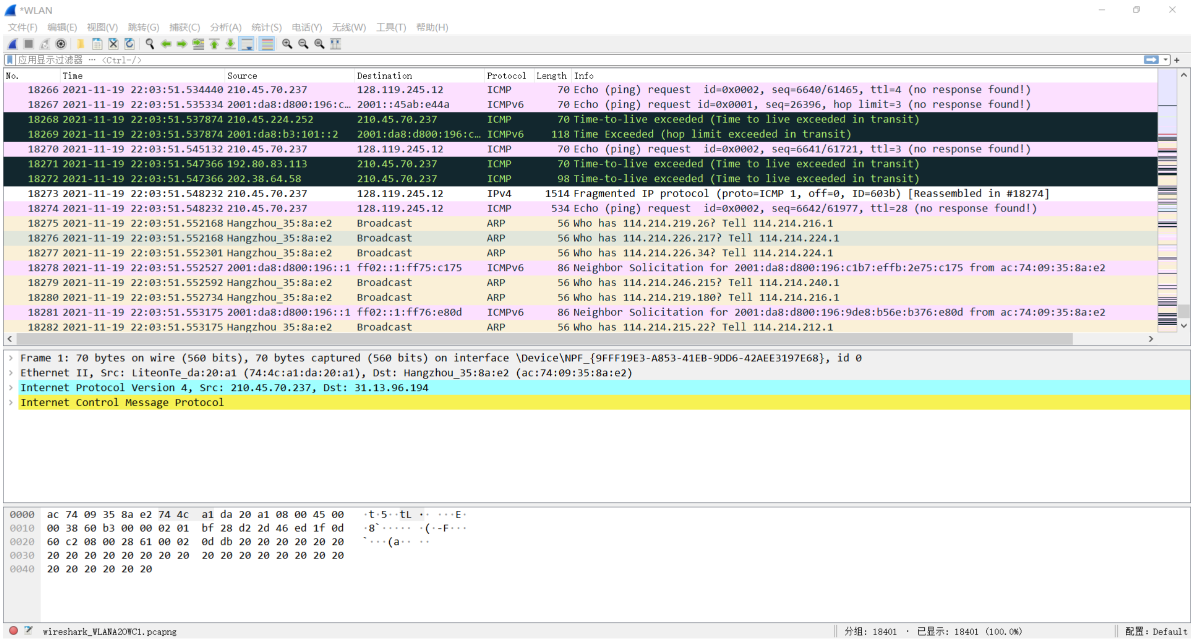
Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	18	0.0.0.0	LAPTOP-NHD5G5N9	14.8	1.6	3.3	
2	18	202.38.96.60	202.38.96.60	11.6	2.0	*	11.1
3	18	202.38.64.58	202.38.64.58	9.9	1.6	2.2	
4	18	210.45.224.252	210.45.224.252	15.5	2.6	4.8	
5	18	101.4.115.13	101.4.115.13	13.0	3.4	3.9	
6	18	101.4.115.185	101.4.115.185	18.4	2.9	5.3	
7	18	101.4.112.61	101.4.112.61	16.8	8.5	10.5	5.6
8	18	101.4.117.38	101.4.117.38	28.6	17.7	18.9	5.6
9	17	101.4.112.1	101.4.112.1	33.6	27.4	34.6	17.6
10	9	101.4.118.214	101.4.118.214	46.3	45.7	*	77.8
11	17	210.25.189.65	210.25.189.65	38.4	28.0	29.3	

gaia.cs.umass.edu (128.119.245.12) hop 31

10 minutes (21:53:45 - 22:03:45)

3.停止wireshark捕获

以下为我捕获到的包：

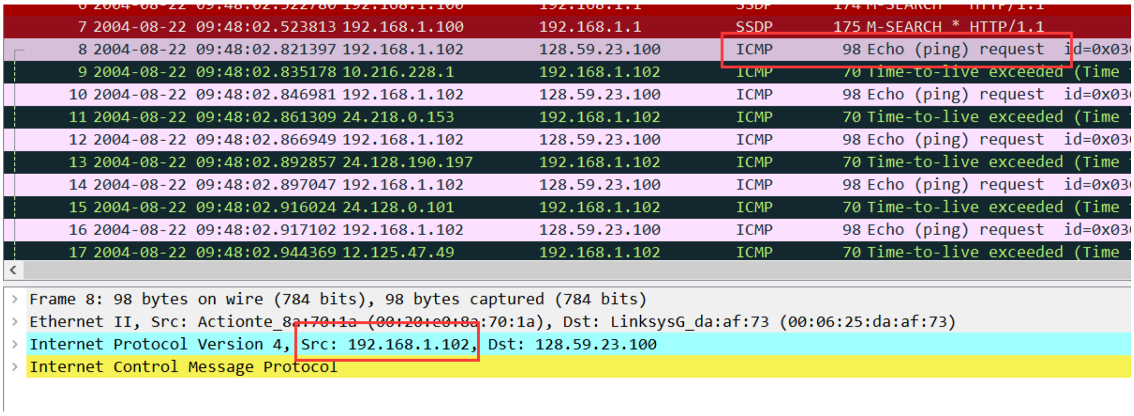


```
*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
No.   Time                       Source                 Destination            Protocol Length Info
18266 2021-11-19 22:03:51.534440 210.45.70.237          128.119.245.12         ICMP        70 Echo (ping) request  id=0x0002, seq=6640/61465, ttl=4 (no response found!)
18267 2021-11-19 22:03:51.535334 2001:da8:d800:196:c…   2001::45ab:e44a        ICMPv6      70 Echo (ping) request id=0x0001, seq=26396, hop limit=3 (no response found!)
18268 2021-11-19 22:03:51.537874 210.45.224.252         210.45.70.237          ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
18269 2021-11-19 22:03:51.537874 2001:da8:b3:101::2     2001:da8:d800:196:c…   ICMPv6     118 Time Exceeded (hop limit exceeded in transit)
18270 2021-11-19 22:03:51.545132 210.45.70.237          128.119.245.12         ICMP        70 Echo (ping) request  id=0x0002, seq=6641/61721, ttl=3 (no response found!)
18271 2021-11-19 22:03:51.547366 192.80.83.113          210.45.70.237          ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
18272 2021-11-19 22:03:51.547366 202.38.64.58           210.45.70.237          ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
18273 2021-11-19 22:03:51.548232 210.45.70.237          128.119.245.12         IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=603b) [Reassembled in #18274]
18274 2021-11-19 22:03:51.548232 210.45.70.237          128.119.245.12         ICMP       534 Echo (ping) request  id=0x0002, seq=6642/61977, ttl=28 (no response found!)
18275 2021-11-19 22:03:51.552168 Hangzhou_35:8a:e2      Broadcast              ARP         56 Who has 114.214.219.26? Tell 114.214.216.1
18276 2021-11-19 22:03:51.552168 Hangzhou_35:8a:e2      Broadcast              ARP         56 Who has 114.214.226.217? Tell 114.214.224.1
18277 2021-11-19 22:03:51.552301 Hangzhou_35:8a:e2      Broadcast              ARP         56 Who has 114.214.226.34? Tell 114.214.224.1
18278 2021-11-19 22:03:51.552527 2001:da8:d800:196::1   ff02::1:ff75:c175      ICMPv6      86 Neighbor Solicitation for 2001:da8:d800:196:c1b7:effb:2e75:c175 from ac:74:09:35:8a:e2
18279 2021-11-19 22:03:51.552592 Hangzhou_35:8a:e2      Broadcast              ARP         56 Who has 114.214.246.215? Tell 114.214.240.1
18280 2021-11-19 22:03:51.552734 Hangzhou_35:8a:e2      Broadcast              ARP         56 Who has 114.214.219.180? Tell 114.214.216.1
18281 2021-11-19 22:03:51.553175 2001:da8:d800:196::1   ff02::1:ff76:e80d      ICMPv6      86 Neighbor Solicitation for 2001:da8:d800:196:9de8:b56e:b376:e80d from ac:74:09:35:8a:e2
18282 2021-11-19 22:03:51.553175 Hangzhou_35:8a:e2      Broadcast              ARP         56 Who has 114.214.215.22? Tell 114.214.212.1

> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{9FFF19E3-A853-41EB-9DD6-42AEE3197E68}, id 0
> Ethernet II, Src: LiteonTe_da:20:a1 (74:4c:a1:da:20:a1), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
> Internet Protocol Version 4, Src: 210.45.70.237, Dst: 31.13.96.194
> Internet Control Message Protocol

0000  ac 74 09 35 8a e2 74 4c  a1 da 20 a1 08 00 45 00   ·t·5··tL ·· ···E·
0010  00 38 60 b3 00 00 02 01  bf 28 d2 2d 46 ed 1f 0d   ·8`····· ·(·-F···
0020  60 c2 08 00 28 61 00 02  0d db 20 20 20 20 20 20   `···(a·· ··
0030  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0040  20 20 20 20 20 20

wireshark_WLANA20WC1.pcapng          分组: 18401 · 已显示: 18401 (100.0%)          配置: Default
```

以下用的都是作者抓的数据包：

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?**

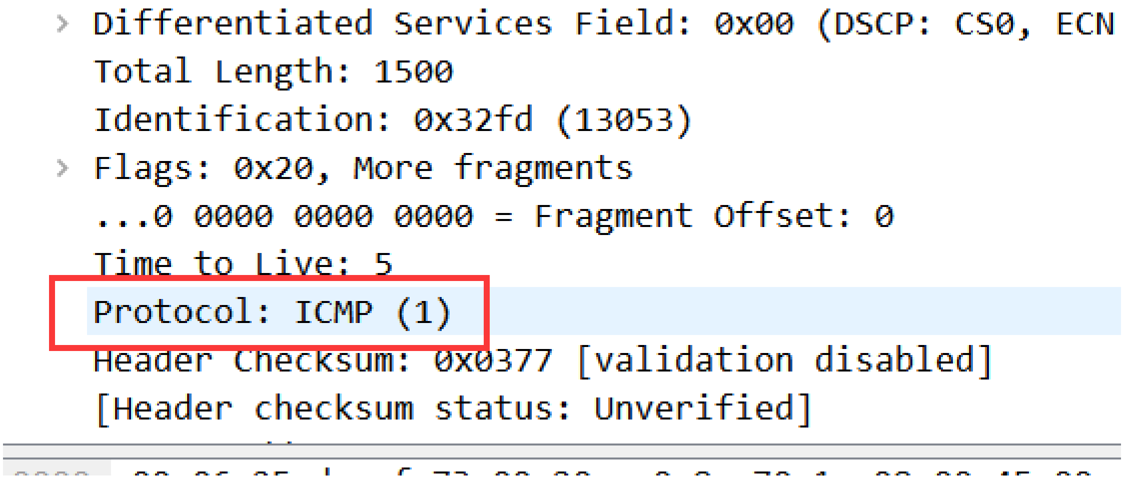
   192.168.1.102



```
 6 2004-08-22 09:48:02.522780 192.168.1.100   192.168.1.1    SSDP   174 M-SEARCH * HTTP/1.1
 7 2004-08-22 09:48:02.523813 192.168.1.100   192.168.1.1    SSDP   175 M-SEARCH * HTTP/1.1
 8 2004-08-22 09:48:02.821397 192.168.1.102   128.59.23.100  ICMP    98 Echo (ping) request  id=0x03
 9 2004-08-22 09:48:02.835178 10.216.228.1    192.168.1.102  ICMP    70 Time-to-live exceeded (Time
10 2004-08-22 09:48:02.846981 192.168.1.102   128.59.23.100  ICMP    98 Echo (ping) request  id=0x03
11 2004-08-22 09:48:02.861309 24.218.0.153    192.168.1.102  ICMP    70 Time-to-live exceeded (Time
12 2004-08-22 09:48:02.866949 192.168.1.102   128.59.23.100  ICMP    98 Echo (ping) request  id=0x03
13 2004-08-22 09:48:02.892857 24.128.190.197  192.168.1.102  ICMP    70 Time-to-live exceeded (Time
14 2004-08-22 09:48:02.897047 192.168.1.102   128.59.23.100  ICMP    98 Echo (ping) request  id=0x03
15 2004-08-22 09:48:02.916024 24.128.0.101    192.168.1.102  ICMP    70 Time-to-live exceeded (Time
16 2004-08-22 09:48:02.917102 192.168.1.102   128.59.23.100  ICMP    98 Echo (ping) request  id=0x03
17 2004-08-22 09:48:02.944369 12.125.47.49    192.168.1.102  ICMP    70 Time-to-live exceeded (Time

> 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
> Internet Control Message Protocol
```

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

   1，表示ICMP

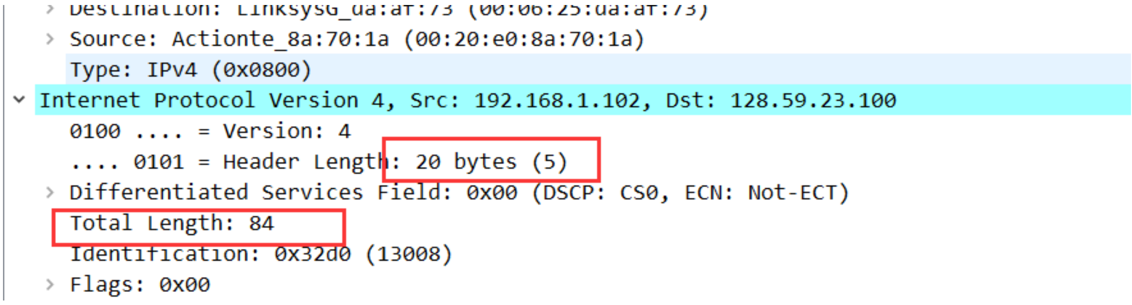


```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN
  Total Length: 1500
  Identification: 0x32fd (13053)
> Flags: 0x20, More fragments
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 5
  Protocol: ICMP (1)
  Header Checksum: 0x0377 [validation disabled]
  [Header checksum status: Unverified]
```

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.**

   报头长度为20 bytes，总长度为84 bytes，故有效负载为 84 - 20 = 64 bytes

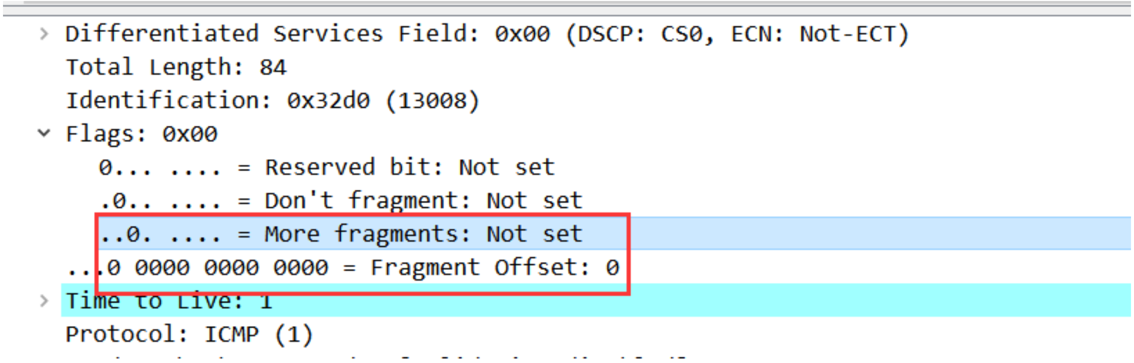
   有效负载为总长度减去报头的长度



```
  > Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
  > Source: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
    Type: IPv4 (0x0800)
v 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
```

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

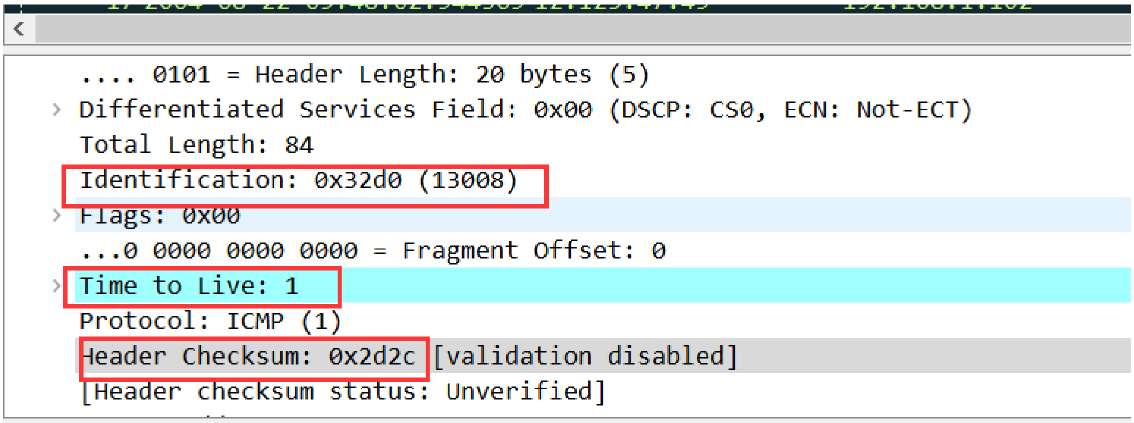
   没有分片，more fragments设为not set



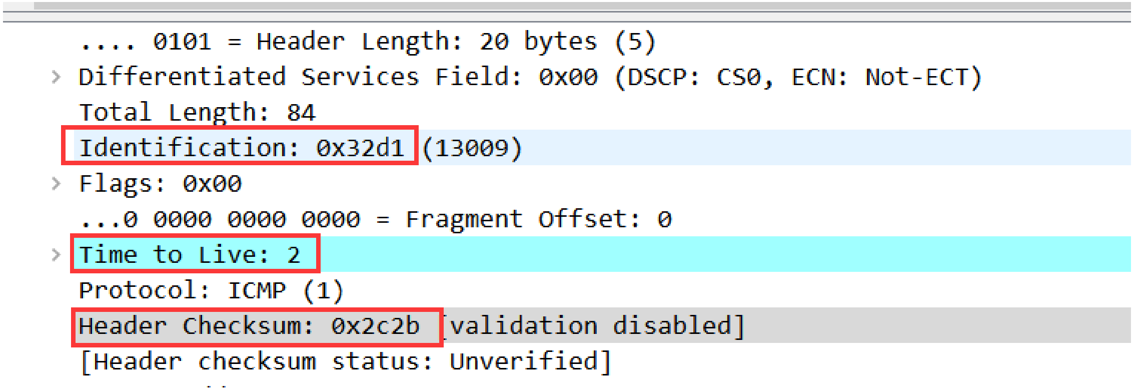
```
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
```

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?**

   标识、寿命、首部检验和



```
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d0 (13008)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
```



```
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x32d1 (13009)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 2
    Protocol: ICMP (1)
    Header Checksum: 0x2c2b [validation disabled]
    [Header checksum status: Unverified]
```

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

   保持不变：数据报长度、标志、片偏移、源ip地址、目的ip地址、选项

   在同一个传输中，发送方和接收方不变，故源ip地址、目的ip地址保持不变。此处数据报长度均为84，没有分片。

   必须保持不变：版本、首部长度、服务类型、上层协议

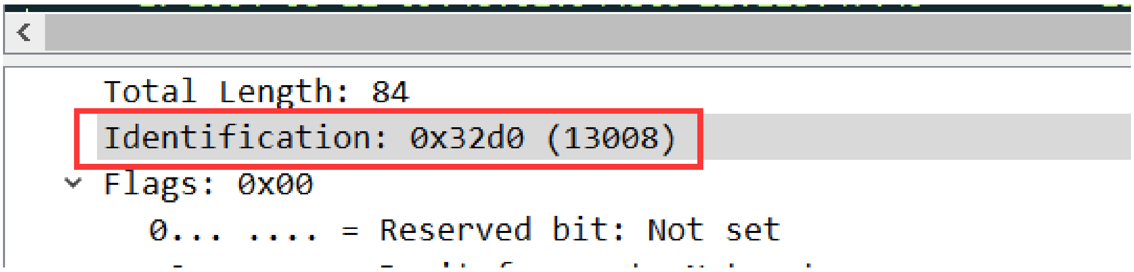
   版本都为ipv4，首部长度为20，上层协议为IMCP。

   一定改变：标识、寿命、首部检验和、数据

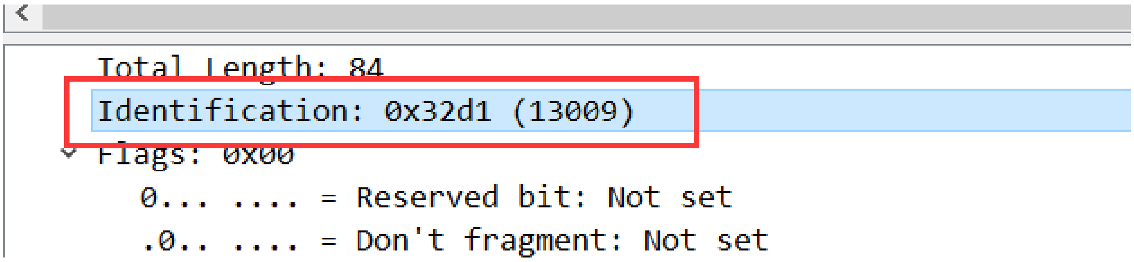
   不同的数据报的标识、寿命均不同，装载的数据也不同，故首部检验和也会有所不同。

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

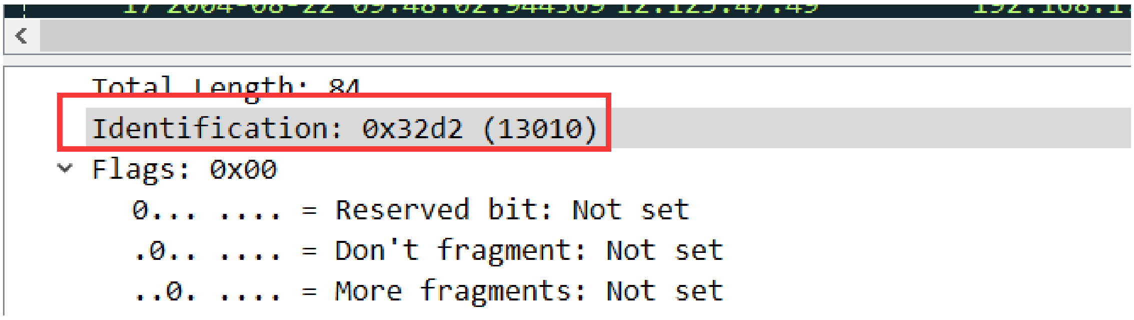
   标识号每次加1



```
Total Length: 84
Identification: 0x32d0 (13008)
Flags: 0x00
    0... .... = Reserved bit: Not set
```



```
Total Length: 84
Identification: 0x32d1 (13009)
Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
```

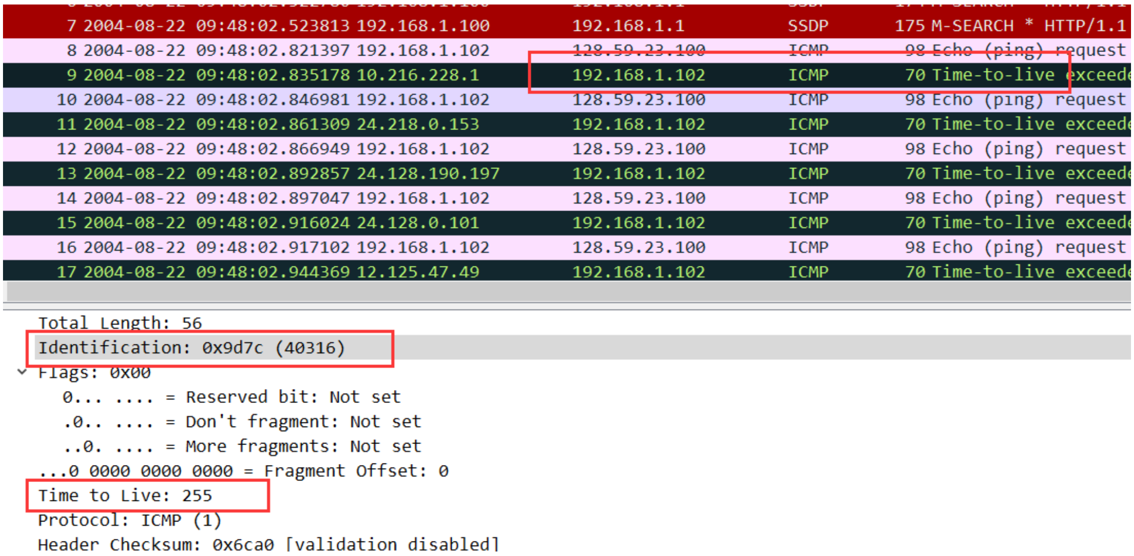


```
Total Length: 84
Identification: 0x32d2 (13010)
Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
```

Next (with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to your computer by the nearest (first hop) router.

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

   标识：0x9d7c　　寿命：255

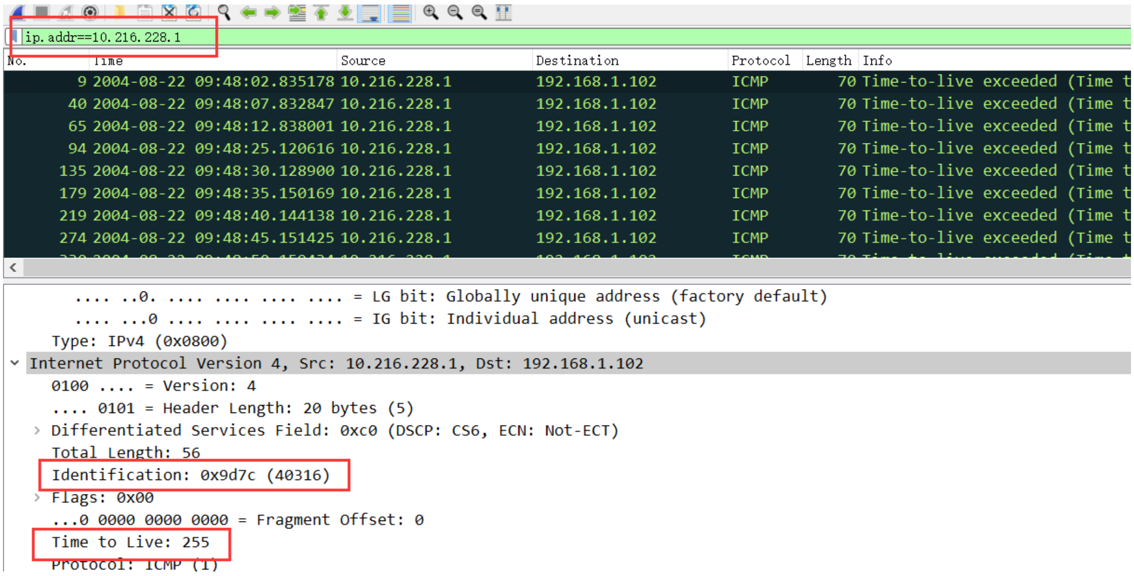


```
  7 2004-08-22 09:48:02.523813 192.168.1.100     192.168.1.1       SSDP      175 M-SEARCH * HTTP/1.1
  8 2004-08-22 09:48:02.821397 192.168.1.102     128.59.23.100     ICMP       98 Echo (ping) request
  9 2004-08-22 09:48:02.835178 10.216.228.1      192.168.1.102     ICMP       70 Time-to-live exceede
 10 2004-08-22 09:48:02.846981 192.168.1.102     128.59.23.100     ICMP       98 Echo (ping) request
 11 2004-08-22 09:48:02.861309 24.218.0.153      192.168.1.102     ICMP       70 Time-to-live exceede
 12 2004-08-22 09:48:02.866949 192.168.1.102     128.59.23.100     ICMP       98 Echo (ping) request
 13 2004-08-22 09:48:02.892857 24.128.190.197    192.168.1.102     ICMP       70 Time-to-live exceede
 14 2004-08-22 09:48:02.897047 192.168.1.102     128.59.23.100     ICMP       98 Echo (ping) request
 15 2004-08-22 09:48:02.916024 24.128.0.101      192.168.1.102     ICMP       70 Time-to-live exceede
 16 2004-08-22 09:48:02.917102 192.168.1.102     128.59.23.100     ICMP       98 Echo (ping) request
 17 2004-08-22 09:48:02.944369 12.125.47.49      192.168.1.102     ICMP       70 Time-to-live exceede

    Total Length: 56
    Identification: 0x9d7c (40316)
  ∨ Flags: 0x00
      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: 0x6ca0 [validation disabled]
```

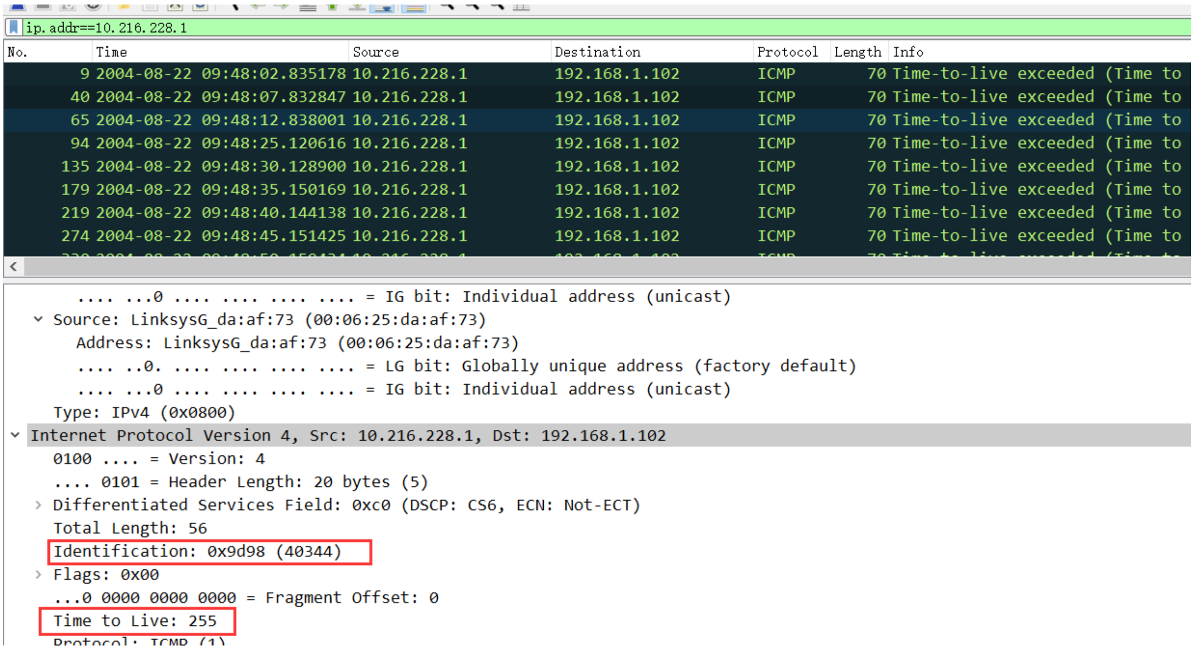
9. **Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why**

寿命不变，一个路由器有着固定的TTL值。

标识改变，标识相同表示的是同一个数据包的分片。



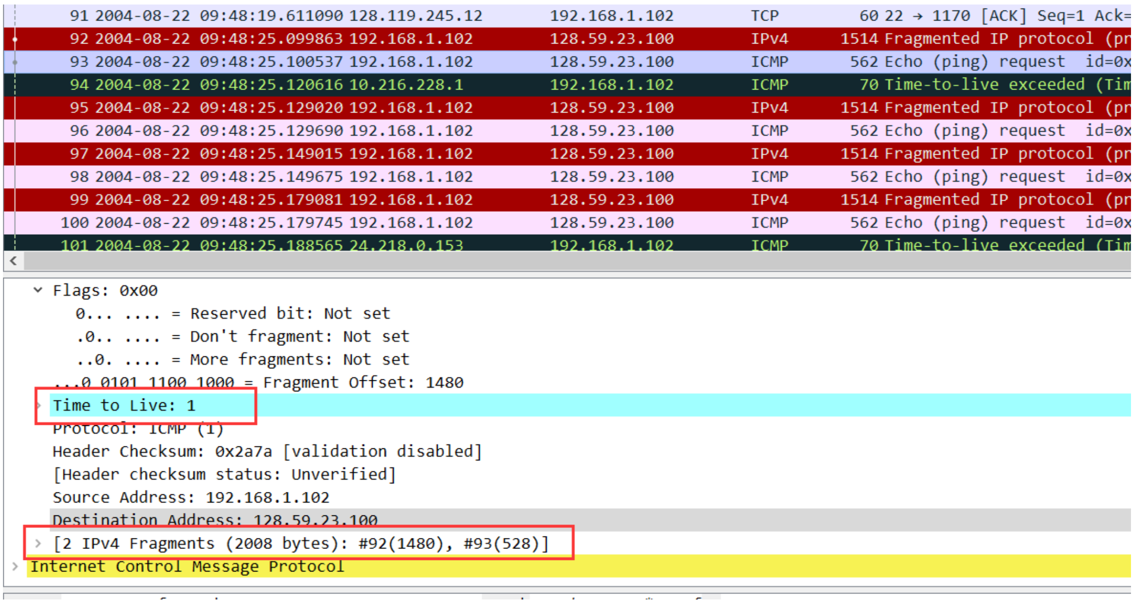
```
ip.addr==10.216.228.1
No.   Time                          Source          Destination     Protocol  Length  Info
    9 2004-08-22 09:48:02.835178 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time t
   40 2004-08-22 09:48:07.832847 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time t
   65 2004-08-22 09:48:12.838001 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time t
   94 2004-08-22 09:48:25.120616 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time t
  135 2004-08-22 09:48:30.128900 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time t
  179 2004-08-22 09:48:35.150169 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time t
  219 2004-08-22 09:48:40.144138 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time t
  274 2004-08-22 09:48:45.151425 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time t

      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
  ∨ 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
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 255
      Protocol: ICMP (1)
```



```
ip.addr==10.216.228.1
No.   Time                          Source          Destination     Protocol  Length  Info
    9 2004-08-22 09:48:02.835178 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time to
   40 2004-08-22 09:48:07.832847 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time to
   65 2004-08-22 09:48:12.838001 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time to
   94 2004-08-22 09:48:25.120616 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time to
  135 2004-08-22 09:48:30.128900 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time to
  179 2004-08-22 09:48:35.150169 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time to
  219 2004-08-22 09:48:40.144138 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time to
  274 2004-08-22 09:48:45.151425 10.216.228.1    192.168.1.102   ICMP        70 Time-to-live exceeded (Time to

      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ∨ Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
∨ 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: 0x9d98 (40344)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
```

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?**

    是的，被分成了两片

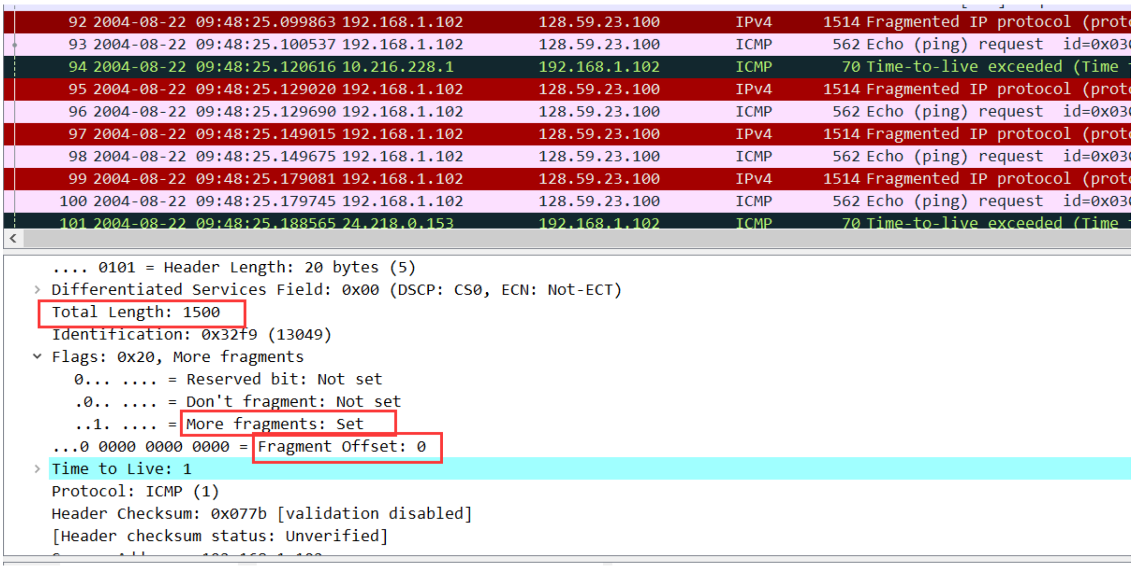


```
 91 2004-08-22 09:48:19.611090 128.119.245.12   192.168.1.102   TCP     60 22 → 1170 [ACK] Seq=1 Ack=
 92 2004-08-22 09:48:25.099863 192.168.1.102    128.59.23.100   IPv4  1514 Fragmented IP protocol (pr
 93 2004-08-22 09:48:25.100537 192.168.1.102    128.59.23.100   ICMP   562 Echo (ping) request  id=0x
 94 2004-08-22 09:48:25.120616 10.216.228.1     192.168.1.102   ICMP    70 Time-to-live exceeded (Tim
 95 2004-08-22 09:48:25.129020 192.168.1.102    128.59.23.100   IPv4  1514 Fragmented IP protocol (pr
 96 2004-08-22 09:48:25.129690 192.168.1.102    128.59.23.100   ICMP   562 Echo (ping) request  id=0x
 97 2004-08-22 09:48:25.149015 192.168.1.102    128.59.23.100   IPv4  1514 Fragmented IP protocol (pr
 98 2004-08-22 09:48:25.149675 192.168.1.102    128.59.23.100   ICMP   562 Echo (ping) request  id=0x
 99 2004-08-22 09:48:25.179081 192.168.1.102    128.59.23.100   IPv4  1514 Fragmented IP protocol (pr
100 2004-08-22 09:48:25.179745 192.168.1.102    128.59.23.100   ICMP   562 Echo (ping) request  id=0x
101 2004-08-22 09:48:25.188565 24.218.0.153     192.168.1.102   ICMP    70 Time-to-live exceeded (Tim
```

```
  ˅ Flags: 0x00
       0... .... = Reserved bit: Not set
       .0.. .... = Don't fragment: Not set
       ..0. .... = More fragments: Not set
    ...0 0101 1100 1000 = Fragment Offset: 1480
  › Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2a7a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  › [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
› Internet Control Message Protocol
```

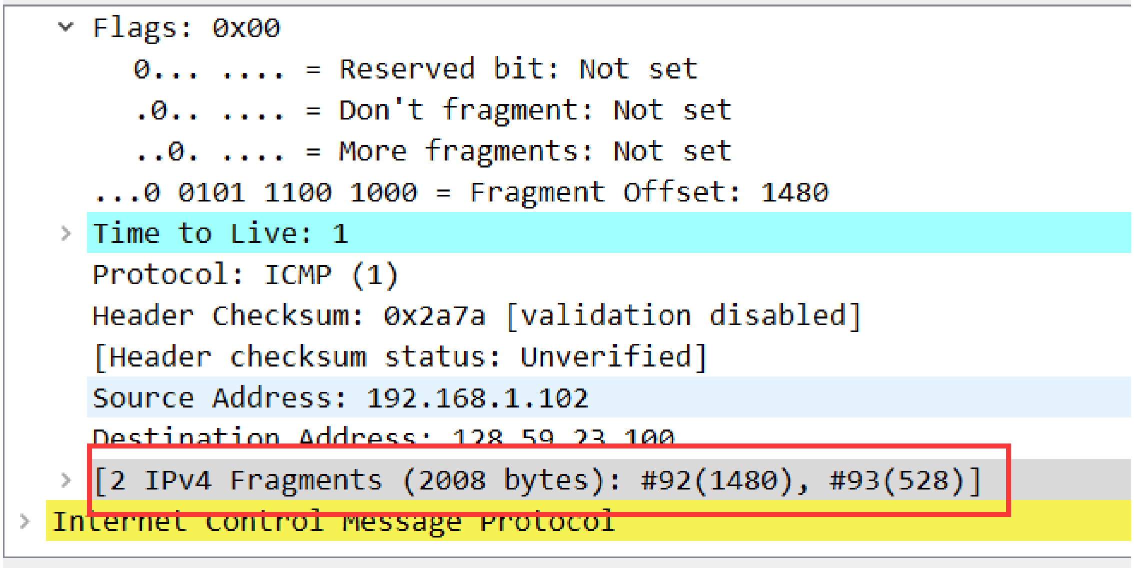
11. **Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram**

    more fragments设为了set表示数据报被分片，fragment offset为0表示这是第一个分片，这个分片所在的数据报的长度为1480+528+20 = 2028 bytes



```
 92 2004-08-22 09:48:25.099863 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (prot
 93 2004-08-22 09:48:25.100537 192.168.1.102   128.59.23.100   ICMP   562 Echo (ping) request  id=0x03
 94 2004-08-22 09:48:25.120616 10.216.228.1    192.168.1.102   ICMP    70 Time-to-live exceeded (Time
 95 2004-08-22 09:48:25.129020 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (prot
 96 2004-08-22 09:48:25.129690 192.168.1.102   128.59.23.100   ICMP   562 Echo (ping) request  id=0x03
 97 2004-08-22 09:48:25.149015 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (prot
 98 2004-08-22 09:48:25.149675 192.168.1.102   128.59.23.100   ICMP   562 Echo (ping) request  id=0x03
 99 2004-08-22 09:48:25.179081 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP protocol (prot
100 2004-08-22 09:48:25.179745 192.168.1.102   128.59.23.100   ICMP   562 Echo (ping) request  id=0x03
101 2004-08-22 09:48:25.188565 24.218.0.153    192.168.1.102   ICMP    70 Time-to-live exceeded (Time
```

```
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x32f9 (13049)
  ˅ Flags: 0x20, 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: 0x077b [validation disabled]
    [Header checksum status: Unverified]
```



```
  ⌄ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0101 1100 1000 = Fragment Offset: 1480
  › Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2a7a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  › [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
› Internet Control Message Protocol
```

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?**

    fragment offset为1480表示这不是第一个分片，通过more fragments为not set可知没有更多分片

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

    flags、fragment offset、header checksum、total length

    第一个分片的more fragments设为set，fragment offset为0，总长度为1500，

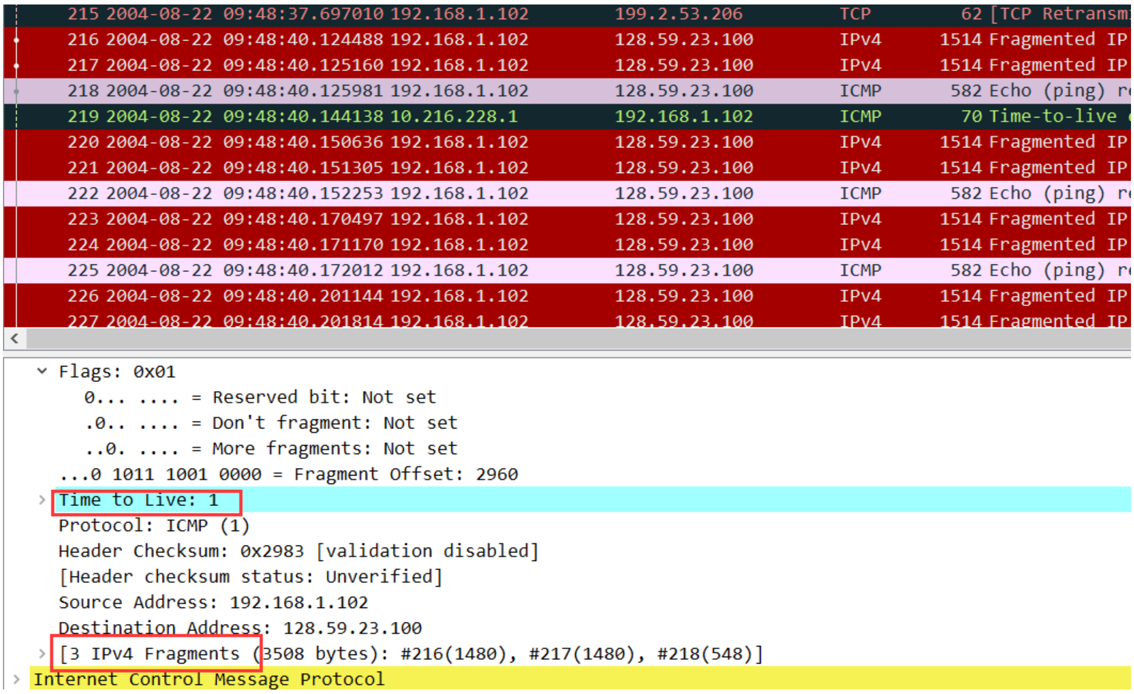
    而第二个more fragments为not set，fragment offset为1480，总长度为548；

    由于数据的不同，故首部检验和也不同

Now find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 3500.

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

    3个



```
215 2004-08-22 09:48:37.697010 192.168.1.102   199.2.53.206    TCP     62 [TCP Retransm
216 2004-08-22 09:48:40.124488 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP
217 2004-08-22 09:48:40.125160 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP
218 2004-08-22 09:48:40.125981 192.168.1.102   128.59.23.100   ICMP   582 Echo (ping) r
219 2004-08-22 09:48:40.144138 10.216.228.1    192.168.1.102   ICMP    70 Time-to-live
220 2004-08-22 09:48:40.150636 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP
221 2004-08-22 09:48:40.151305 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP
222 2004-08-22 09:48:40.152253 192.168.1.102   128.59.23.100   ICMP   582 Echo (ping) r
223 2004-08-22 09:48:40.170497 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP
224 2004-08-22 09:48:40.171170 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP
225 2004-08-22 09:48:40.172012 192.168.1.102   128.59.23.100   ICMP   582 Echo (ping) r
226 2004-08-22 09:48:40.201144 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP
227 2004-08-22 09:48:40.201814 192.168.1.102   128.59.23.100   IPv4  1514 Fragmented IP
```

```
  ⌄ Flags: 0x01
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 1011 1001 0000 = Fragment Offset: 2960
  › Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2983 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
  › [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
› Internet Control Message Protocol
```

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

    flags、fragment offset、header checksum、total length

    第一个分片的more fragments设为set，fragment offset为0，总长度为1500，

    第二个分片的more fragments设为set，fragment offset为1480，总长度为1500，

    最后一个分片的more fragments为not set，fragment offset为2960，总长度为568；

    由于数据的不同，故首部检验和也不同