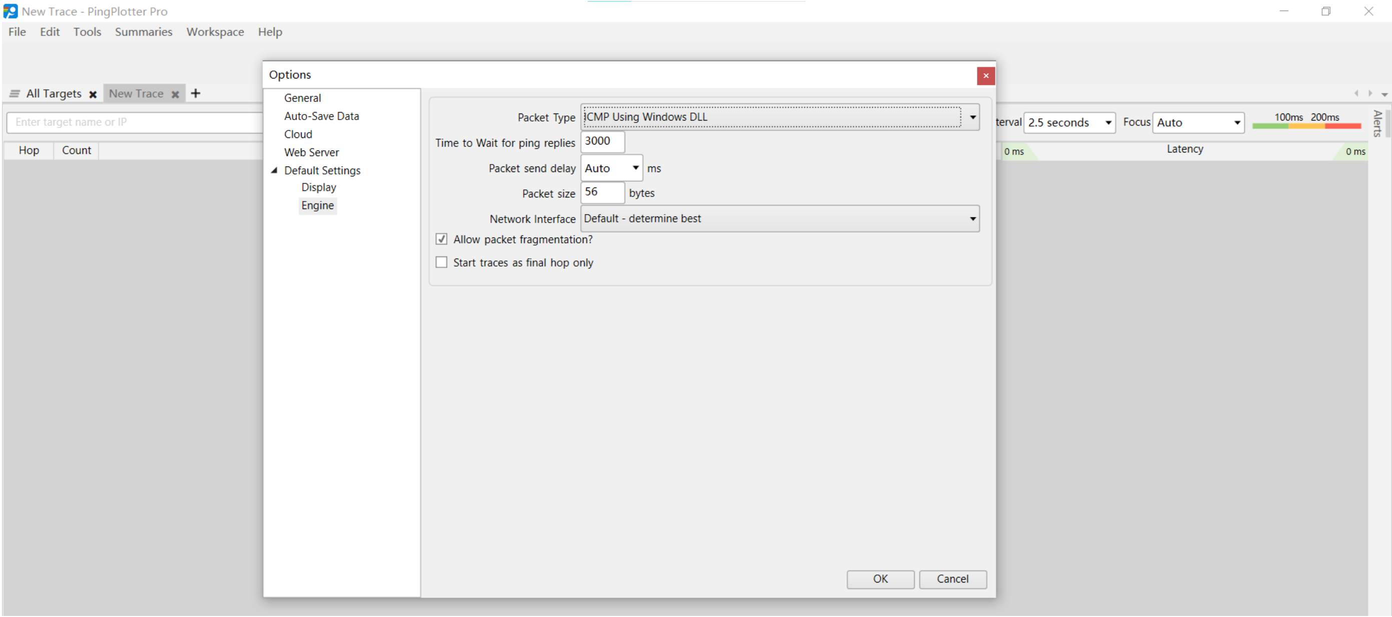
Computer Network Study Lab 6

- Author:PB19000362 钟书锐
- Time:2021.11.24

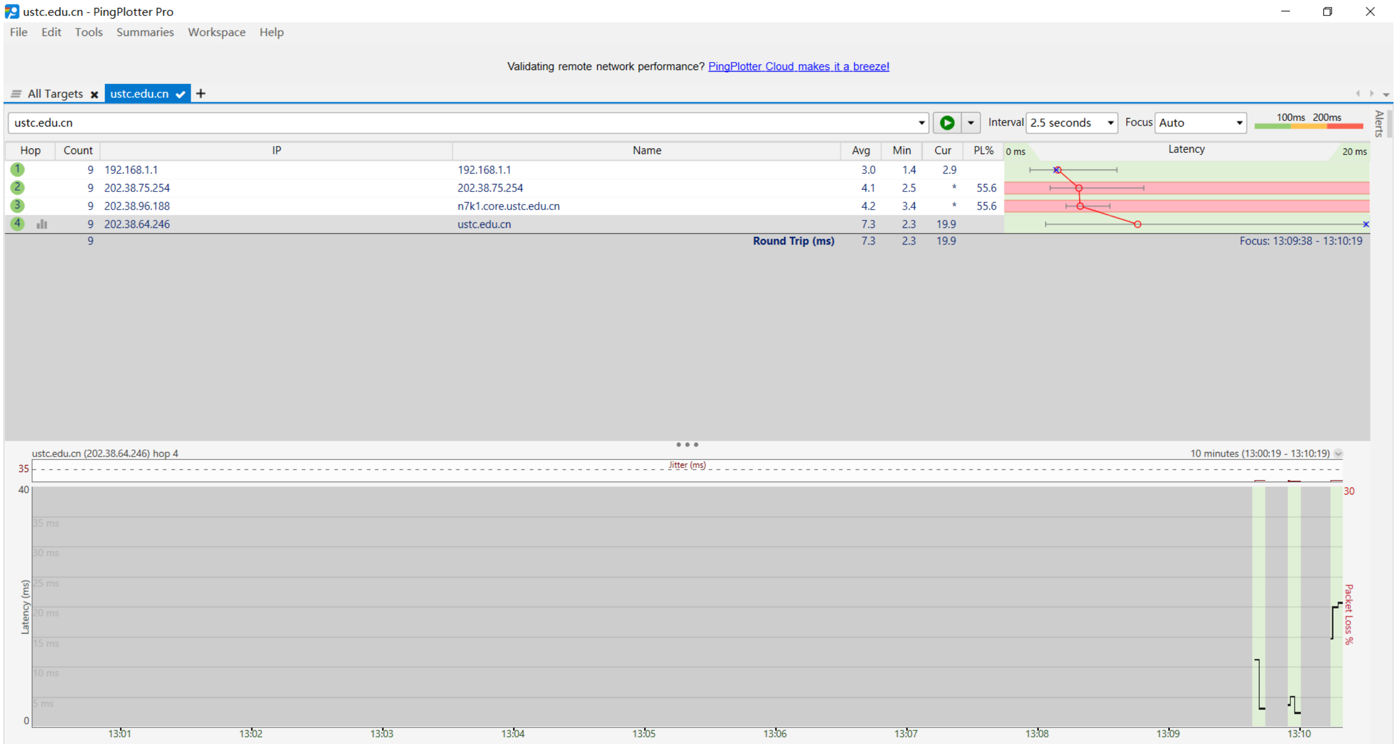
1. Capturing packets from an execution of traceroute

- 本人选择的网站为 ustc.edu.cn，对应ip地址为202.38.64.246
- 可以在pingplotter 中显式设置ICMP echo 请求消息的大小，默认数据包大小为56个字节。



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?
□ Start traces as final hop only

- 在pingplotter 三次不同Packet Size 发送之后结果



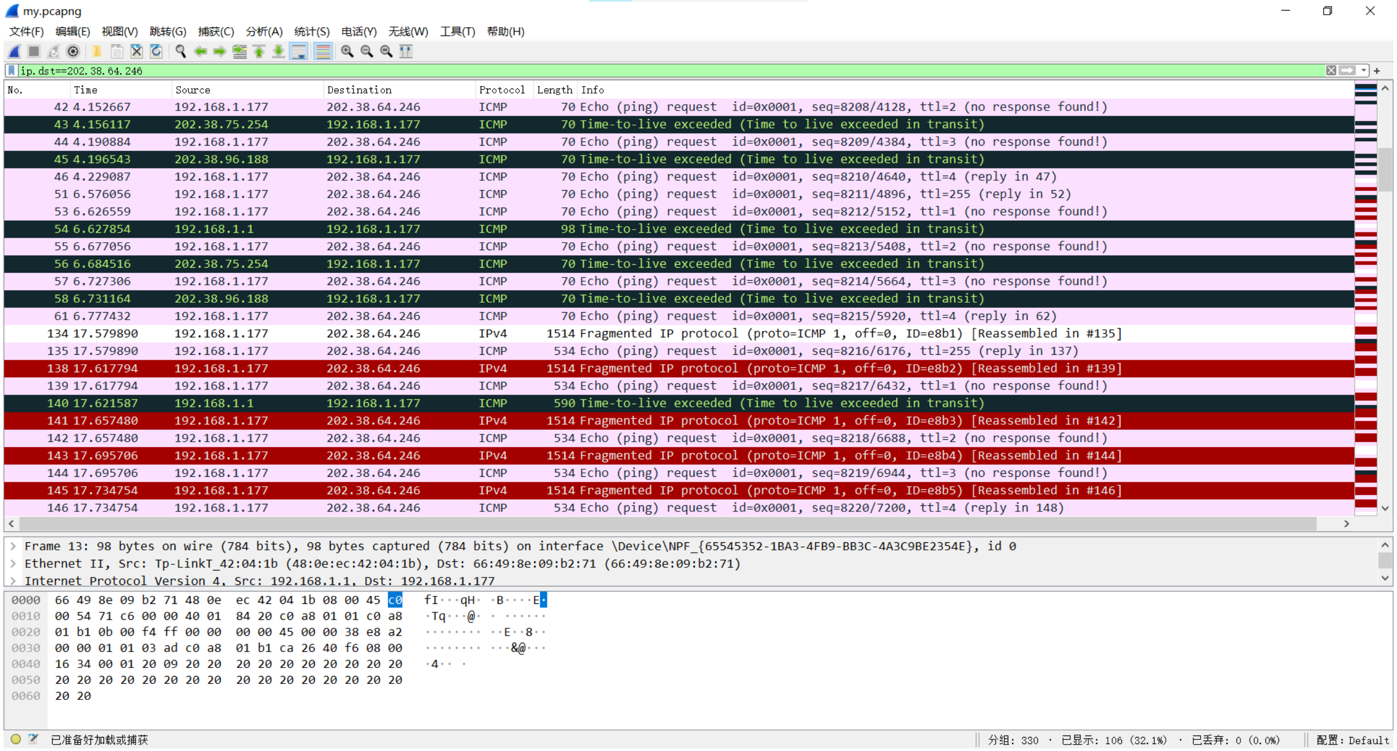
Validating remote network performance? PingPlotter Cloud makes it a breeze!

ustc.edu.cn

Interval 2.5 seconds Focus Auto

Hop	Count	IP	Name	Avg	Min	Cur	PL%	0 ms Latency 20 ms
1	9	192.168.1.1	192.168.1.1	3.0	1.4	2.9		
2	9	202.38.75.254	202.38.75.254	4.1	2.5	*	55.6	
3	9	202.38.96.188	n7k1.core.ustc.edu.cn	4.2	3.4	*	55.6	
4	9	202.38.64.246	ustc.edu.cn	7.3	2.3	19.9		
	9		Round Trip (ms)	7.3	2.3	19.9		Focus: 13:09:38 - 13:10:19

- wireshark抓包结果



ip.dst==202.38.64.246

```
No.  Time       Source         Destination    Protocol Length Info
  42 4.152667   192.168.1.177  202.38.64.246  ICMP       70 Echo (ping) request  id=0x0001, seq=8208/4128, ttl=2 (no response found!)
  43 4.156117   202.38.75.254  192.168.1.177  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  44 4.190884   192.168.1.177  202.38.64.246  ICMP       70 Echo (ping) request  id=0x0001, seq=8209/4384, ttl=3 (no response found!)
  45 4.196543   202.38.96.188  192.168.1.177  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  46 4.229087   192.168.1.177  202.38.64.246  ICMP       70 Echo (ping) request  id=0x0001, seq=8210/4640, ttl=4 (reply in 47)
  51 6.576056   192.168.1.177  202.38.64.246  ICMP       70 Echo (ping) request  id=0x0001, seq=8211/4896, ttl=255 (reply in 52)
  53 6.626559   192.168.1.177  202.38.64.246  ICMP       70 Echo (ping) request  id=0x0001, seq=8212/5152, ttl=1 (no response found!)
  54 6.627854   192.168.1.1    192.168.1.177  ICMP       98 Time-to-live exceeded (Time to live exceeded in transit)
  55 6.677056   192.168.1.177  202.38.64.246  ICMP       70 Echo (ping) request  id=0x0001, seq=8213/5408, ttl=2 (no response found!)
  56 6.684516   202.38.75.254  192.168.1.177  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  57 6.727306   192.168.1.177  202.38.64.246  ICMP       70 Echo (ping) request  id=0x0001, seq=8214/5664, ttl=3 (no response found!)
  58 6.731164   202.38.96.188  192.168.1.177  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  61 6.777432   192.168.1.177  202.38.64.246  ICMP       70 Echo (ping) request  id=0x0001, seq=8215/5920, ttl=4 (reply in 62)
 134 17.579890  192.168.1.177  202.38.64.246  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e8b1) [Reassembled in #135]
 135 17.579890  192.168.1.177  202.38.64.246  ICMP      534 Echo (ping) request  id=0x0001, seq=8216/6176, ttl=255 (reply in 137)
 138 17.617794  192.168.1.177  202.38.64.246  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e8b2) [Reassembled in #139]
 139 17.617794  192.168.1.177  202.38.64.246  ICMP      534 Echo (ping) request  id=0x0001, seq=8217/6432, ttl=1 (no response found!)
 140 17.621587  192.168.1.1    192.168.1.177  ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
 141 17.657480  192.168.1.177  202.38.64.246  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e8b3) [Reassembled in #142]
 142 17.657480  192.168.1.177  202.38.64.246  ICMP      534 Echo (ping) request  id=0x0001, seq=8218/6688, ttl=2 (no response found!)
 143 17.695706  192.168.1.177  202.38.64.246  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e8b4) [Reassembled in #144]
 144 17.695706  192.168.1.177  202.38.64.246  ICMP      534 Echo (ping) request  id=0x0001, seq=8219/6944, ttl=3 (no response found!)
 145 17.734754  192.168.1.177  202.38.64.246  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=e8b5) [Reassembled in #146]
 146 17.734754  192.168.1.177  202.38.64.246  ICMP      534 Echo (ping) request  id=0x0001, seq=8220/7200, ttl=4 (reply in 148)
```

```
> Frame 13: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: Tp-LinkT_42:04:1b (48:0e:ec:42:04:1b), Dst: 66:49:8e:09:b2:71 (66:49:8e:09:b2:71)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.177
```

```
0000  66 49 8e 09 b2 71 48 0e  ec 42 04 1b 08 00 45 c0   fI···qH· ·B····E·
0010  00 54 71 c6 00 00 40 01  84 20 c0 a8 01 01 c0 a8   ·Tq···@· · ······
0020  01 b1 0b 00 f4 ff 00 00  00 00 45 00 00 38 e8 a2   ········ ··E··8··
0030  00 00 01 01 03 ad c0 a8  01 b1 ca 26 40 f6 08 00   ········ ···&@···
0040  16 34 00 01 20 09 20 20  20 20 20 20 20 20 20 20   ·4·· ·
0050  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0060  20 20
```

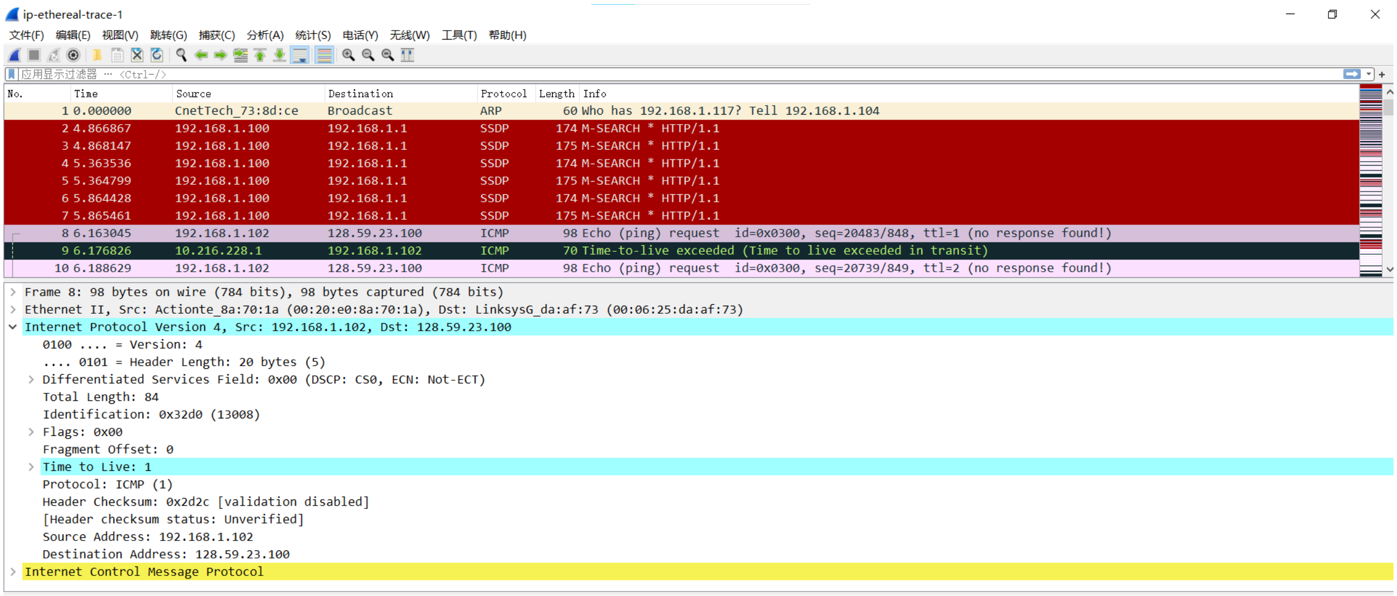
已准备好加载或捕获 | 分组: 330 · 已显示: 106 (32.1%) · 已丢弃: 0 (0.0%) | 配置: Default

2. A look at the captured trace

- **因为自己抓的包比较乱，以下回答基于下载的ip-ethereal-trace-1**

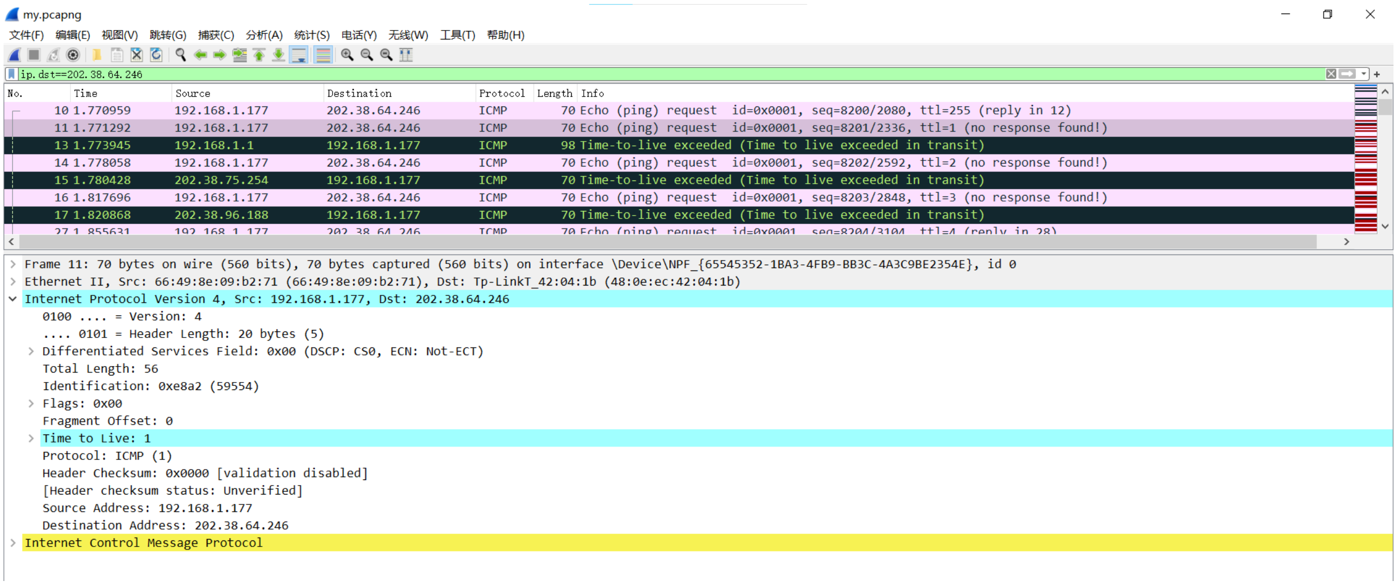
Q:1.Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet

in the packet details window.What is the IP address of your computer?

- 下载的ip-ethereal-trace-1
- 
ip-ethereal-trace-1
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
    1 0.000000   CnetTech_73:8d:ce   Broadcast        ARP         60 Who has 192.168.1.117? Tell 192.168.1.104
    2 4.866867   192.168.1.100       192.168.1.1      SSDP       174 M-SEARCH * HTTP/1.1
    3 4.868147   192.168.1.100       192.168.1.1      SSDP       175 M-SEARCH * HTTP/1.1
    4 5.363536   192.168.1.100       192.168.1.1      SSDP       174 M-SEARCH * HTTP/1.1
    5 5.364799   192.168.1.100       192.168.1.1      SSDP       175 M-SEARCH * HTTP/1.1
    6 5.864428   192.168.1.100       192.168.1.1      SSDP       174 M-SEARCH * HTTP/1.1
    7 5.865461   192.168.1.100       192.168.1.1      SSDP       175 M-SEARCH * HTTP/1.1
    8 6.163045   192.168.1.102       128.59.23.100    ICMP        98 Echo (ping) request  id=0x0300, seq=20483/848, ttl=1 (no response found!)
    9 6.176826   10.216.228.1        192.168.1.102    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   10 6.188629   192.168.1.102       128.59.23.100    ICMP        98 Echo (ping) request  id=0x0300, seq=20739/849, ttl=2 (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)
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
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
> Internet Control Message Protocol
```

- 自己抓取的包
- 
my.pcapng
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)

```
ip.dst==202.38.64.246
```

```
No.   Time       Source              Destination      Protocol  Length Info
   10 1.770959   192.168.1.177       202.38.64.246    ICMP        70 Echo (ping) request  id=0x0001, seq=8200/2080, ttl=255 (reply in 12)
   11 1.771292   192.168.1.177       202.38.64.246    ICMP        70 Echo (ping) request  id=0x0001, seq=8201/2336, ttl=1 (no response found!)
   13 1.773945   192.168.1.1         192.168.1.177    ICMP        98 Time-to-live exceeded (Time to live exceeded in transit)
   14 1.778058   192.168.1.177       202.38.64.246    ICMP        70 Echo (ping) request  id=0x0001, seq=8202/2592, ttl=2 (no response found!)
   15 1.780428   202.38.75.254       192.168.1.177    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   16 1.817696   192.168.1.177       202.38.64.246    ICMP        70 Echo (ping) request  id=0x0001, seq=8203/2848, ttl=3 (no response found!)
   17 1.820868   202.38.96.188       192.168.1.177    ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
   27 1.855631   192.168.1.177       202.38.64.246    ICMP        70 Echo (ping) request  id=0x0001, seq=8204/3104, ttl=4 (reply in 28)
```

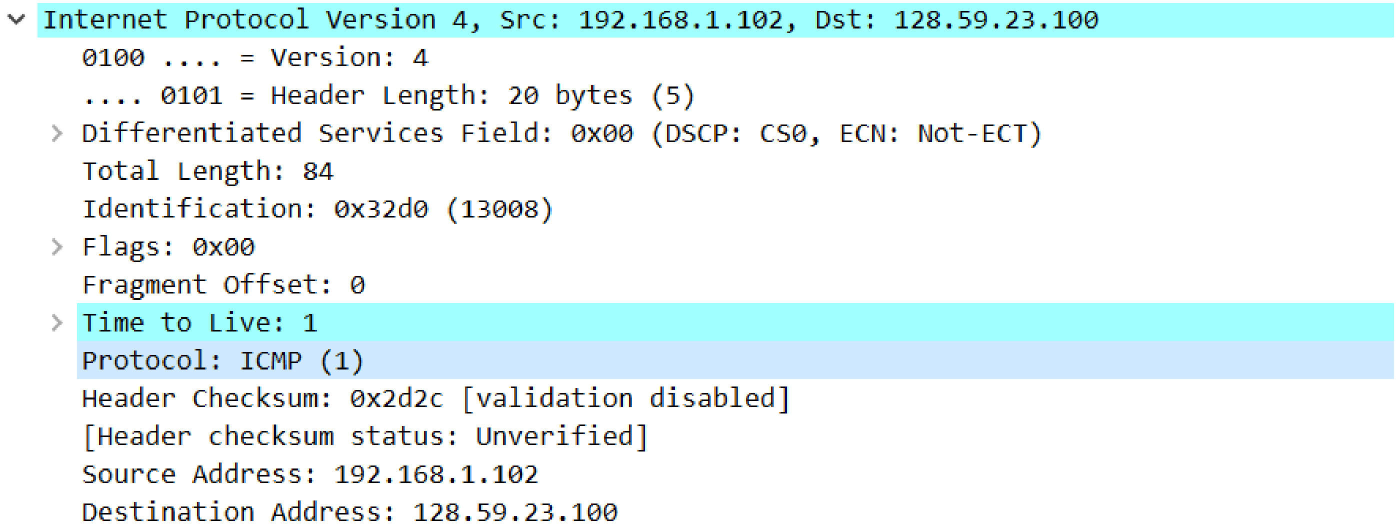
```
> Frame 11: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{65545352-1BA3-4FB9-BB3C-4A3C9BE2354E}, id 0
> Ethernet II, Src: 66:49:8e:09:b2:71 (66:49:8e:09:b2:71), Dst: Tp-LinkT_42:04:1b (48:0e:ec:42:04:1b)
v Internet Protocol Version 4, Src: 192.168.1.177, Dst: 202.38.64.246
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xe8a2 (59554)
  > Flags: 0x00
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.177
    Destination Address: 202.38.64.246
> Internet Control Message Protocol
```

- IP 地址 是 192.168.1.102（此处是下载到的包抓取人的ip地址）
- IP 地址 是 192.168.1.177

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

- `Protocol: ICMP (1)`
- 上层协议就是ICMP，值为1。 Protocol: ICMP (1)

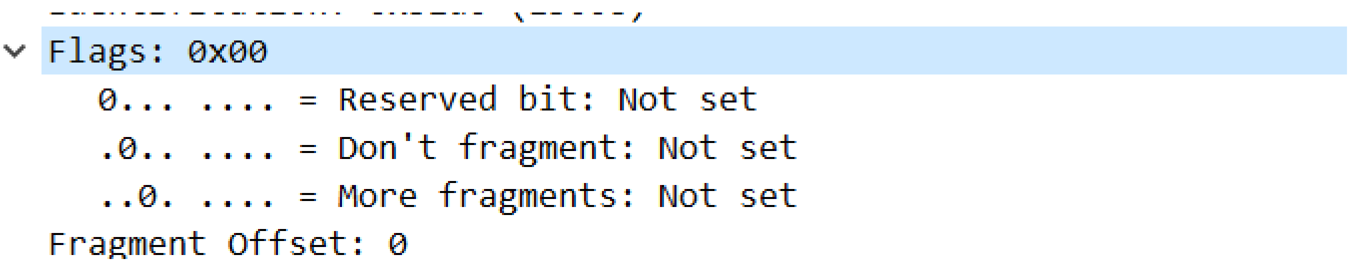
Q:3.How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes

- 

```
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
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x2d2c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
```

- Header Length：20 bytes
- IP datagram payload bytes：64bytes
- explain how:
  - IP数据报总长度 = IP头长度 + IP数据长度(payload bytes)
  - 已知IP头长度20bytes，总长度total lenth 84bytes
  - payload bytes为84-20=64bytes

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

- 

```
v Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment Offset: 0
```

- IP数据报没有被分段
- explain how:
  - Fragment Offset：该片偏移原始数据包开始处的位置。偏移的字节数是该值乘以8。
  - 此处Fragment offset = 0
  - More Fragment，“更多的片”，除了最后一片外，其他每个组成数据报的片都要把该比特置1。
  - 此处More Fragment = 0
  - 综上，既是第一片也是最后一片，所以没有进行分片

Q: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?

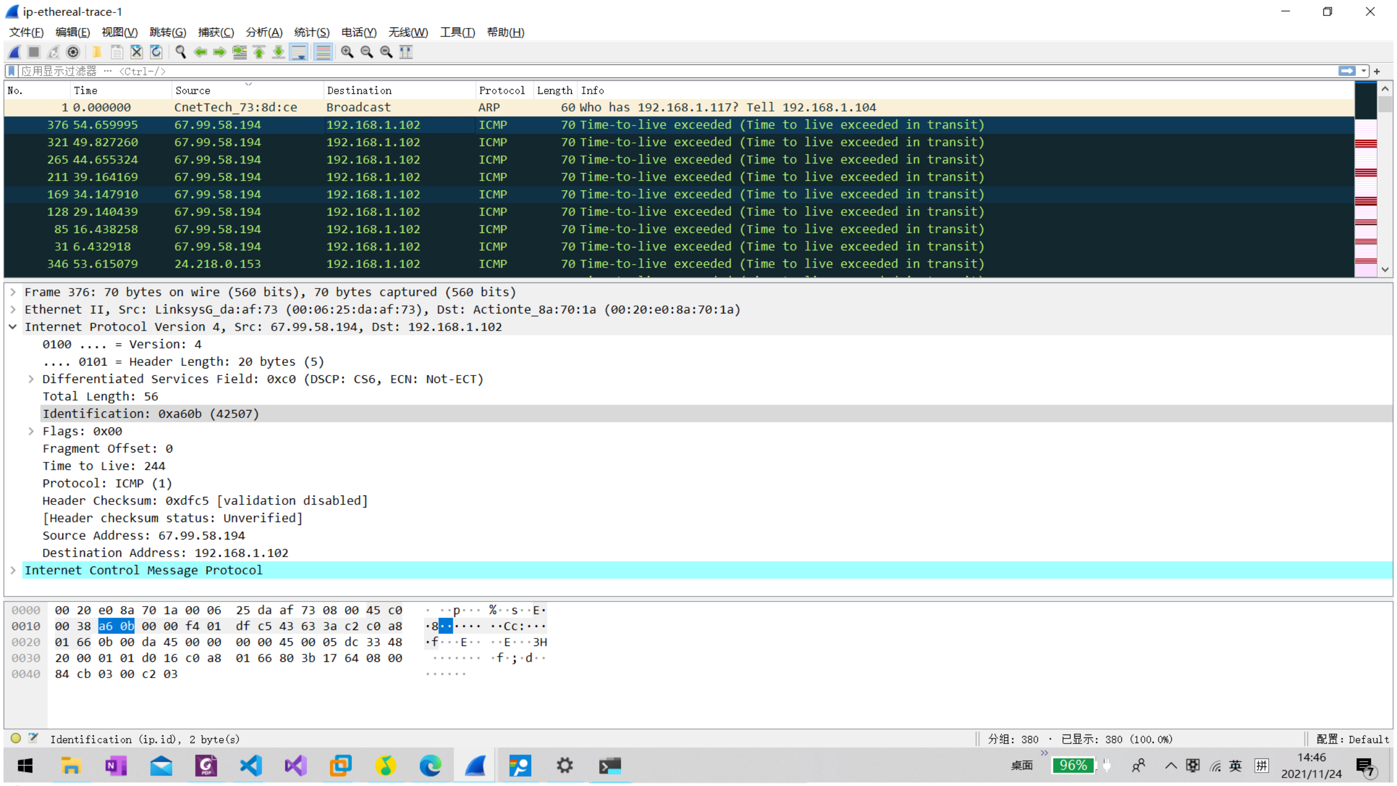
- 一直更改的:Header checksum, TTL, Identification, data

Q:6.Which fields stay constant? Which of the fields must stay constant? Which fields must change，Why?

- 一直不变的：Sources, Destination, Protocol, Header Length, Version
- 必须保持不变：Version, Header Length,
- 必须改变的是：Header checksum, Identification, data
- why：
  - 必须保持不变
    1. Version：占 4 bit,通信双方使用的版本必须一致，对于 IPv4 字段的值是4
    2. Header Length：占 4 bit,首部长度说明首部有多少个4字节
  - 必须改变的是
    1. 每发送一个datagram，Identification++；TTL++；Header Checksum随data变而变
    2. Identification：占 16bit,用来唯一地标识一个报文的所有分片,所以必须改变区分报文
    3. Header checksum：占 16bit,用来检验，和数据data关联
    4. TTL：TTL的作用是限制IP数据包在计算机网络中的存在的时间
    5. data：发送数据

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

-

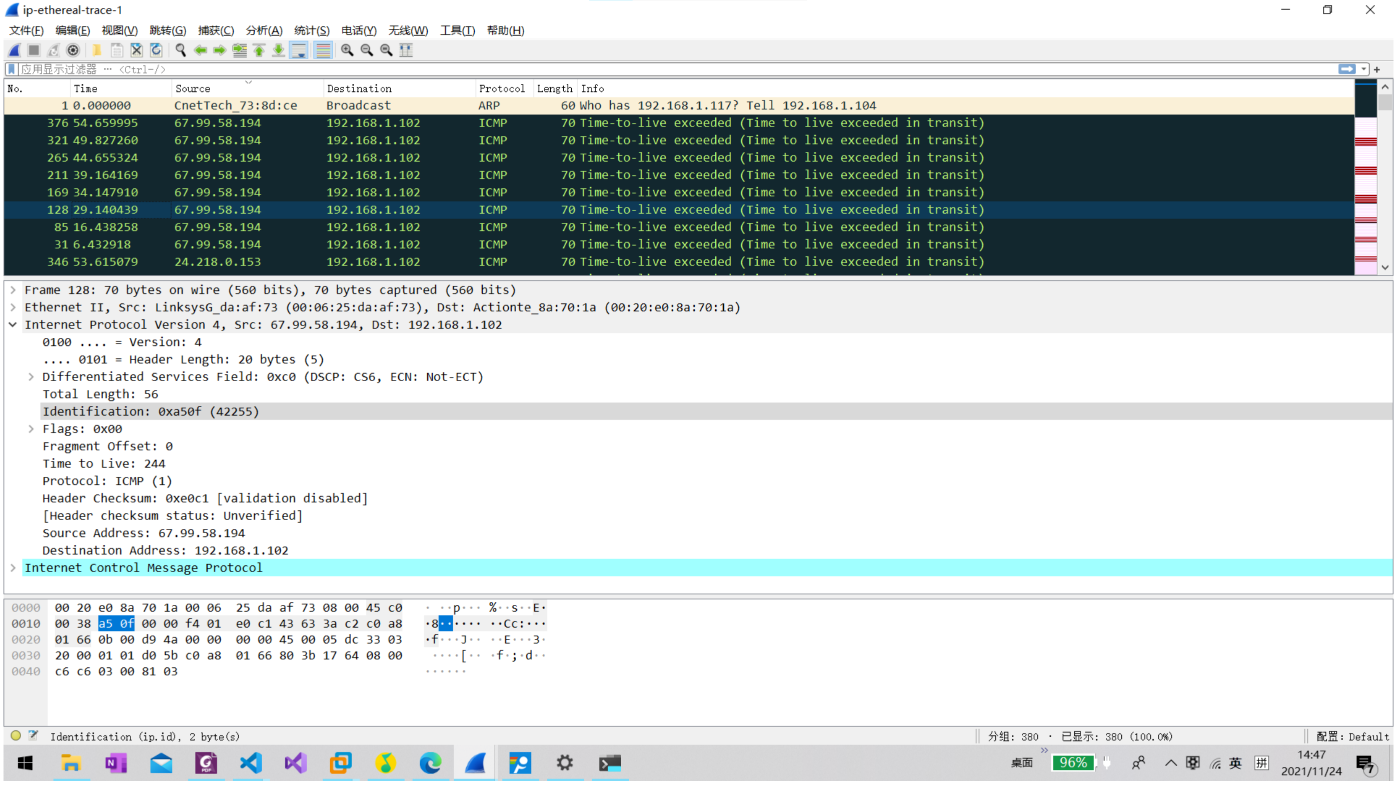

ip-ethereal-trace-1
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.    Time        Source            Destination    Protocol Length Info
     1 0.000000    CnetTech_73:8d:ce Broadcast      ARP      60 Who has 192.168.1.117? Tell 192.168.1.104
   376 54.659995   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   321 49.827260   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   265 44.655324   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   211 39.164169   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   169 34.147910   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   128 29.140439   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
    85 16.438258   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
    31 6.432918    67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   346 53.615079   24.218.0.153      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 376: 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: 67.99.58.194, 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: 0xa60b (42507)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 244
    Protocol: ICMP (1)
    Header Checksum: 0xdfc5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 67.99.58.194
    Destination Address: 192.168.1.102
> Internet Control Message Protocol
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   · ·p··· %··s··E·
0010  00 38 a6 0b 00 00 f4 01  df c5 43 63 3a c2 c0 a8   ·8······ ··Cc:···
0020  01 66 0b 00 da 45 00 00  00 00 45 00 05 dc 33 48   ·f···E·· ··E···3H
0030  20 00 01 01 d0 16 c0 a8  01 66 80 3b 17 64 08 00   ······· ·f·;·d··
0040  84 cb 03 00 c2 03                                  ······
```

Identification (ip.id), 2 byte(s)
分组: 380 · 已显示: 380 (100.0%)
配置: Default
桌面
96%
英
14:46
2021/11/24

- 
ip-ethereal-trace-1
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
     1 0.000000    CnetTech_73:8d:ce Broadcast      ARP      60 Who has 192.168.1.117? Tell 192.168.1.104
   376 54.659995   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   321 49.827260   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   265 44.655324   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   211 39.164169   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   169 34.147910   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   128 29.140439   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
    85 16.438258   67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
    31 6.432918    67.99.58.194      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
   346 53.615079   24.218.0.153      192.168.1.102  ICMP     70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 128: 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: 67.99.58.194, 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: 0xa50f (42255)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 244
    Protocol: ICMP (1)
    Header Checksum: 0xe0c1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 67.99.58.194
    Destination Address: 192.168.1.102
> Internet Control Message Protocol
```

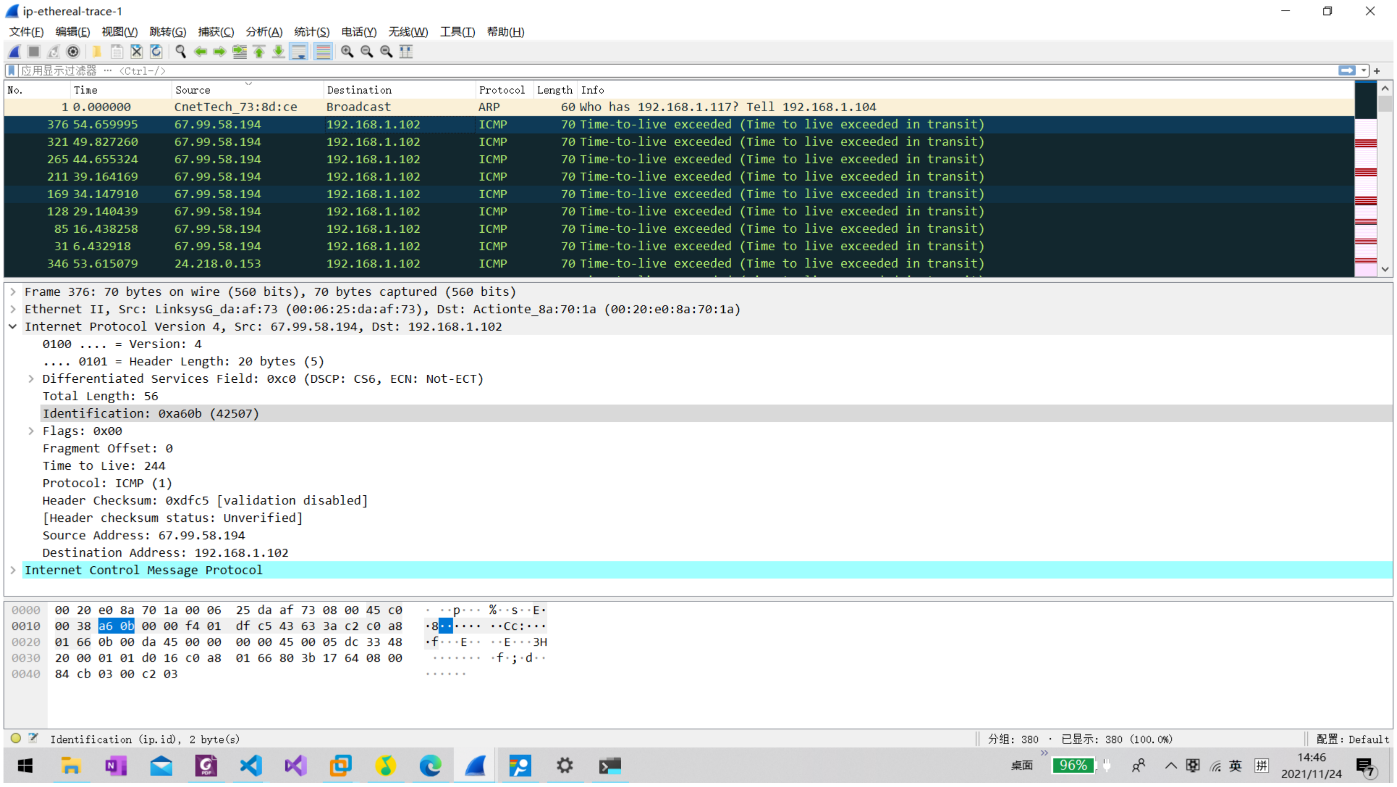
```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   · ·p··· %··s··E·
0010  00 38 a5 0f 00 00 f4 01  e0 c1 43 63 3a c2 c0 a8   ·8······ ··Cc:···
0020  01 66 0b 00 d9 4a 00 00  00 00 45 00 05 dc 33 03   ·f···J·· ··E···3·
0030  20 00 01 01 d0 5b c0 a8  01 66 80 3b 17 64 08 00   ····[·· ·f·;·d··
0040  c6 c6 03 00 81 03                                  ······
```

Identification (ip.id), 2 byte(s)
分组: 380 · 已显示: 380 (100.0%)
配置: Default
桌面
96%
英
14:47
2021/11/24

- 每个IP数据报的Identification是不同的，用来唯一地标识一个报文的所有分片和处理IP分片
- Identification 随数据报的发送而增长

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

-


ip-ethereal-trace-1
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-/>
桌面
96%
英
拼
14:46
2021/11/24

```
No.   Time        Source            Destination   Protocol Length Info
    1 0.000000    CnetTech_73:8d:ce Broadcast     ARP          60 Who has 192.168.1.117? Tell 192.168.1.104
  376 54.659995   67.99.58.194      192.168.1.102 ICMP         70 Time-to-live exceeded (Time to live exceeded in transit)
  321 49.827260   67.99.58.194      192.168.1.102 ICMP         70 Time-to-live exceeded (Time to live exceeded in transit)
  265 44.655324   67.99.58.194      192.168.1.102 ICMP         70 Time-to-live exceeded (Time to live exceeded in transit)
  211 39.164169   67.99.58.194      192.168.1.102 ICMP         70 Time-to-live exceeded (Time to live exceeded in transit)
  169 34.147910   67.99.58.194      192.168.1.102 ICMP         70 Time-to-live exceeded (Time to live exceeded in transit)
  128 29.140439   67.99.58.194      192.168.1.102 ICMP         70 Time-to-live exceeded (Time to live exceeded in transit)
   85 16.438258   67.99.58.194      192.168.1.102 ICMP         70 Time-to-live exceeded (Time to live exceeded in transit)
   31 6.432918    67.99.58.194      192.168.1.102 ICMP         70 Time-to-live exceeded (Time to live exceeded in transit)
  346 53.615079   24.218.0.153      192.168.1.102 ICMP         70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 376: 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: 67.99.58.194, 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: 0xa60b (42507)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 244
    Protocol: ICMP (1)
    Header Checksum: 0xdfc5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 67.99.58.194
    Destination Address: 192.168.1.102
> Internet Control Message Protocol
```

```
0000  00 20 e0 8a 70 1a 00 06  25 da af 73 08 00 45 c0   · ··p··· %··s··E·
0010  00 38 a6 0b 00 00 f4 01  df c5 43 63 3a c2 c0 a8   ·8······ ··Cc:···
0020  01 66 0b 00 da 45 00 00  00 00 45 00 05 dc 33 48   ·f···E·· ··E···3H
0030  20 00 01 01 d0 16 c0 a8  01 66 80 3b 17 64 08 00    ······· ·f·;·d··
0040  84 cb 03 00 c2 03                                  ······
```

```
Identification (ip.id), 2 byte(s)          分组: 380 · 已显示: 380 (100.0%)          配置: Default
```

- Identification: 0xa60b (42507)
- Time to Live: 255

Q: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?

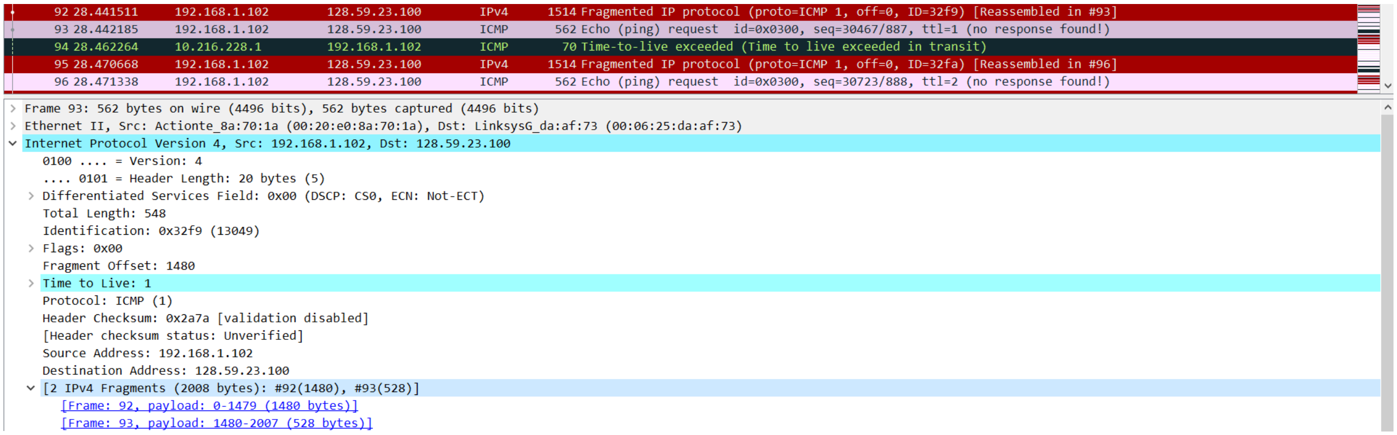
- Identification 字段改变
- Time to Live 字段不改变，为255
- why:

  1. Identification变，每发一个IP datagram，Identification++;

  2. TTL 为 255不变。TTL初始最大值为 255 ， TTL每经过一个router才减1，因为题干是 nearest router，所以和发送方之间一个其它router都没有，所以TTL不会减，一直是255

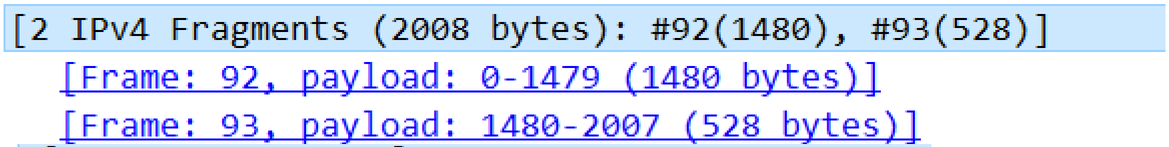
Q:10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram

-

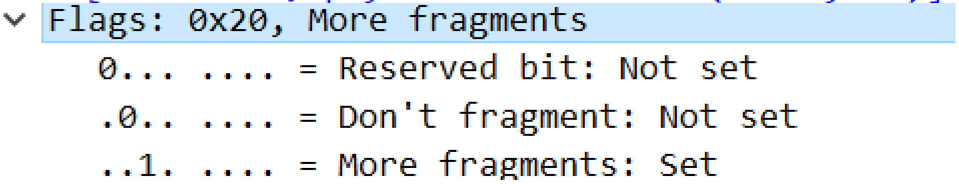


```
92 28.441511    192.168.1.102    128.59.23.100    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
93 28.442185    192.168.1.102    128.59.23.100    ICMP     562 Echo (ping) request  id=0x0300, seq=30467/887, ttl=1 (no response found!)
94 28.462264    10.216.228.1     192.168.1.102    ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
95 28.470668    192.168.1.102    128.59.23.100    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32fa) [Reassembled in #96]
96 28.471338    192.168.1.102    128.59.23.100    ICMP     562 Echo (ping) request  id=0x0300, seq=30723/888, ttl=2 (no response found!)
```

```
> Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 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)
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: 548
    Identification: 0x32f9 (13049)
  > Flags: 0x00
    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
  v [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
      [Frame: 92, payload: 0-1479 (1480 bytes)]
      [Frame: 93, payload: 1480-2007 (528 bytes)]
```

- 

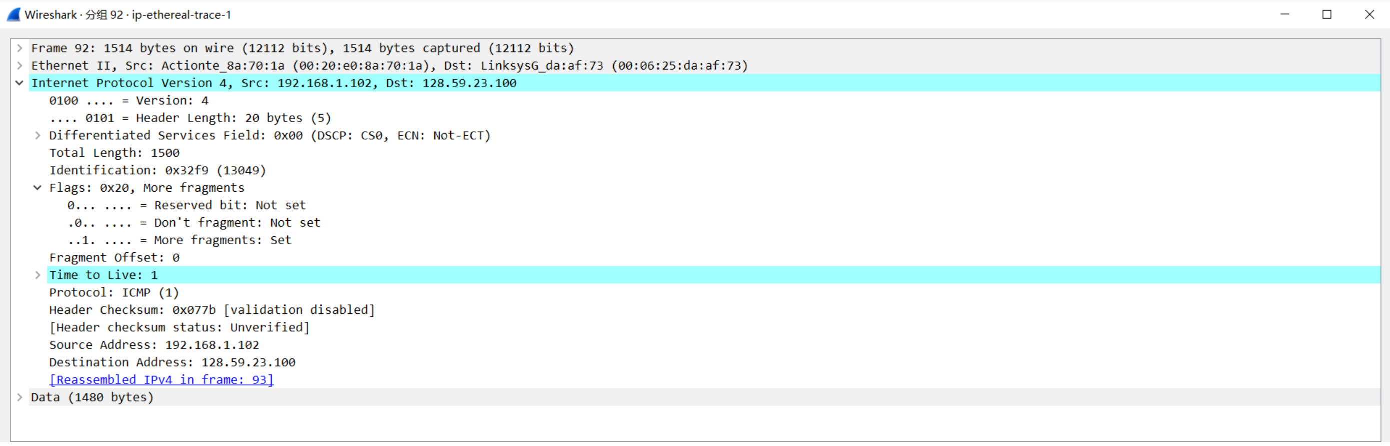
  ```
  [2 IPv4 Fragments (2008 bytes): #92(1480), #93(528)]
     [Frame: 92, payload: 0-1479 (1480 bytes)]
     [Frame: 93, payload: 1480-2007 (528 bytes)]
  ```

- 

  ```
  v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
  ```

- 从图中可以看到已经分成2片了
- [Frame: 92, payload: 0-1479 (1480 bytes)]
- [Frame: 93, payload: 1480-2007 (528 bytes)]
- Frame92 总共2000 bytes = 20bytes + 1480bytes
- Frame93 总共548 bytes = 20bytes + 528bytes
- 第一片的More fragments: Set 表明已经分片了

Q: 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?

- 

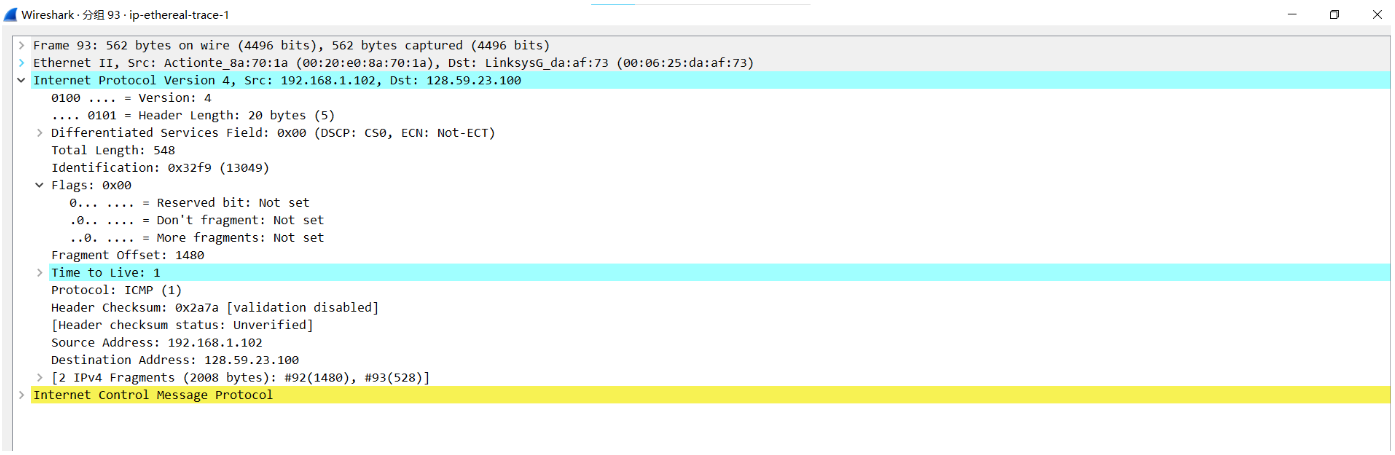
  Wireshark · 分组 92 · ip-ethereal-trace-1

  ```
  > Frame 92: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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)
  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: 1500
      Identification: 0x32f9 (13049)
    v Flags: 0x20, More fragments
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..1. .... = More fragments: Set
      Fragment Offset: 0
    > Time to Live: 1
      Protocol: ICMP (1)
      Header Checksum: 0x077b [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.1.102
      Destination Address: 128.59.23.100
      [Reassembled IPv4 in frame: 93]
  > Data (1480 bytes)
  ```

- IP头中 `..1. .... = More fragments: Set` 表示后面还有分片，所以已经被分片了。

- 根据Fragment Offset为 0 可以推出是第一个分片。
- 如果Fragment Offset不为 0，且More fragments为1，则表示为最后一个分片。
- Total Length: 1500 单位bytes，其中头部20 bytes，负载1480 bytes。

Q： 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?

- 

Wireshark · 分组 93 · ip-ethereal-trace-1

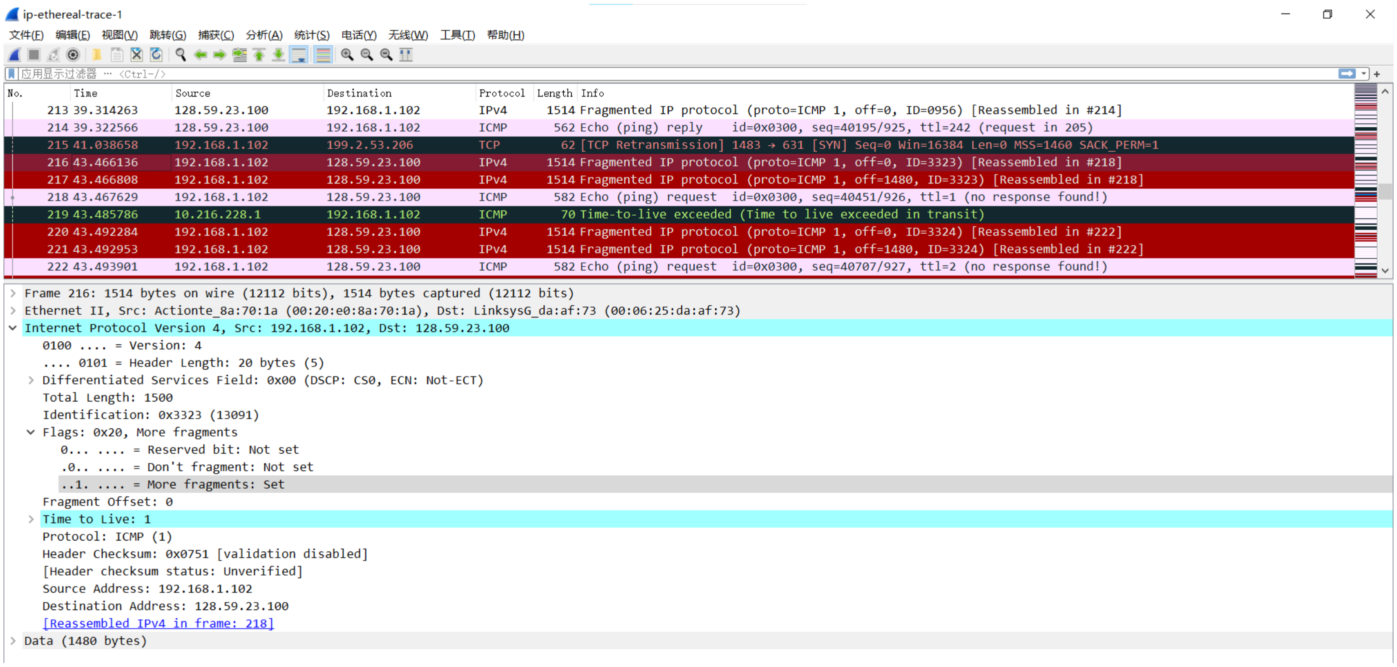
```
> Frame 93: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0x32f9 (13049)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    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
```

- Fragment Offset不为 0，而是 1480
- 没有更多的分片了，因为More fragments为0，More fragments: Not Set

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

- Frame
- Fragment Offset
- More fragments
- Total Length
- data
- header checksum
- 特别的：
    - flag的最后一位（More fragments）分别为：1 0
    - fragment offset分别为：0 1480
    - Total Length分别是 1500 548

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

- 

ip-ethereal-trace-1
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
  213 39.314263  128.59.23.100  192.168.1.102  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0956) [Reassembled in #214]
  214 39.322566  128.59.23.100  192.168.1.102  ICMP      562 Echo (ping) reply    id=0x0300, seq=40195/925, ttl=242 (request in 205)
  215 41.038658  192.168.1.102  199.2.53.206   TCP        62 [TCP Retransmission] 1483 → 631 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
  216 43.466136  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3323) [Reassembled in #218]
  217 43.466808  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3323) [Reassembled in #218]
  218 43.467629  192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=40451/926, ttl=1 (no response found!)
  219 43.485786  10.216.228.1   192.168.1.102  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  220 43.492284  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3324) [Reassembled in #222]
  221 43.492953  192.168.1.102  128.59.23.100  IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3324) [Reassembled in #222]
  222 43.493901  192.168.1.102  128.59.23.100  ICMP      582 Echo (ping) request  id=0x0300, seq=40707/927, ttl=2 (no response found!)
```

```
> Frame 216: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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)
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: 1500
    Identification: 0x3323 (13091)
  v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0751 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.102
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 218]
> Data (1480 bytes)
```

- 3个分片
- [3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
- [Frame: 216, payload: 0-1479 (1480 bytes)]
- [Frame: 217, payload: 1480-2959 (1480 bytes)]
- [Frame: 218, payload: 2960-3507 (548 bytes)]

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

- Frame
- Fragment Offset
- More fragments
- Total Length
- data
- header checksum
- 特别的：
  - flag的最后一位（More fragments）分别为：1 1 0
  - fragment offset分别为：0 1480 2960
  - Total Length分别是 1500 1500 568