中国科学技术大学计算机学院

计算机网络实验报告

实验四
利用 Wireshark 观察 IP 报文

学　　号：PB18000006
姓　　名：范翔宇
专　　业：计算机科学与技术
指导老师：张信明

中国科学技术大学计算机学院

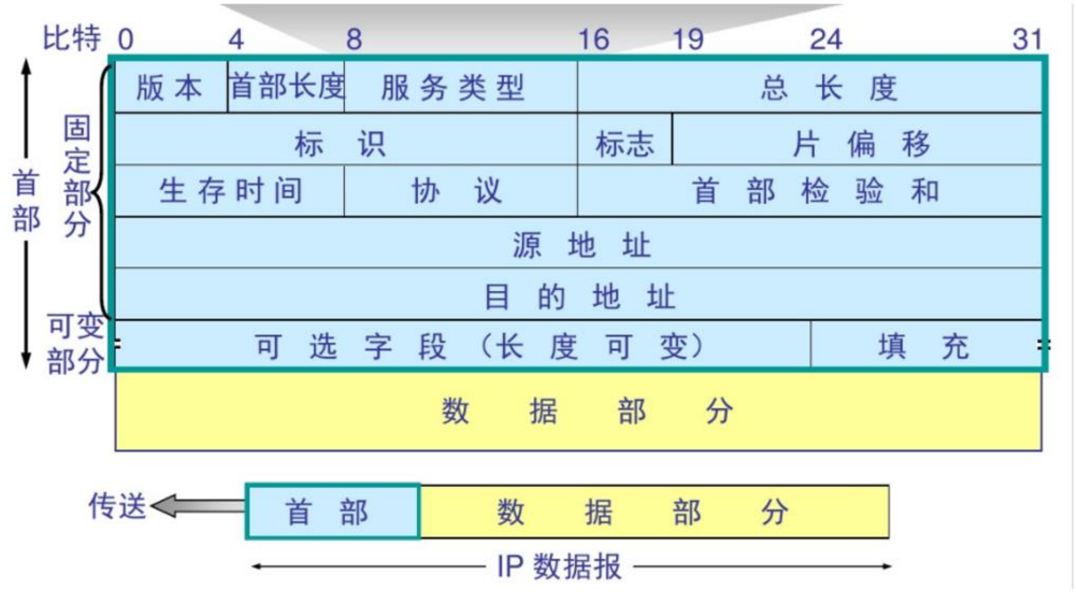
2020 年 12 月 26 日

一、 实验目的

1、　通过捕获观察并分析 IP 报文，理解 IP 的细节，掌握 traceroute 的使用。

二、 实验原理

Wireshark 是一个 packet 分析工具，可以抓取 packet，并分析出详细信息。Wireshark 使用 wincap 作为接口，直接与网卡进行 packet 交换，监听共享网络上传送的 packet。



IP 数据报首部的 TTL(Time to live)表示数据报的生存时间,每经过路由器转发一次,就至少减少 1,当减少到 0 的时候,会被路由器丢弃,并返回 ICMP 消息.

Traceroute 通过巧妙的设置 ttl,通过一次次的重传,与 ttl+1 来得到到目的地址的路径上的路由器的信息.

三、 实验条件

1、　硬件条件：　联想拯救者 Y7000：

i5-8300H 2.30GHz

16G 内存

Intel UHD Graphics 630

2、　软件条件：　Win10

Ubuntu 16.04

Wireshark3.4.0

PingPlotter5.18.3

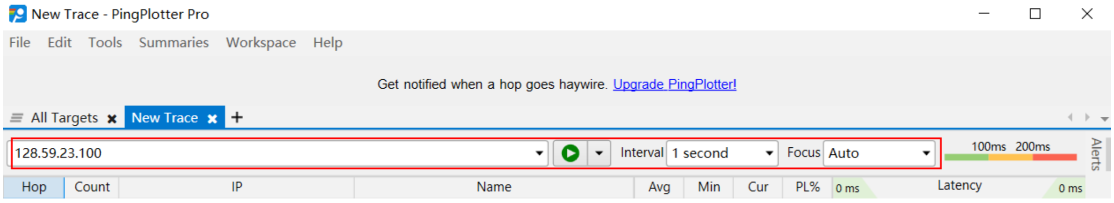
四、 实验过程

1、 安装 PingPlotter5

在官网https://www.pingplotter.com/download下载Windows版本。

2、 利用发包并用 wireshark 查看

输入 128.59.23.100



New Trace - PingPlotter Pro

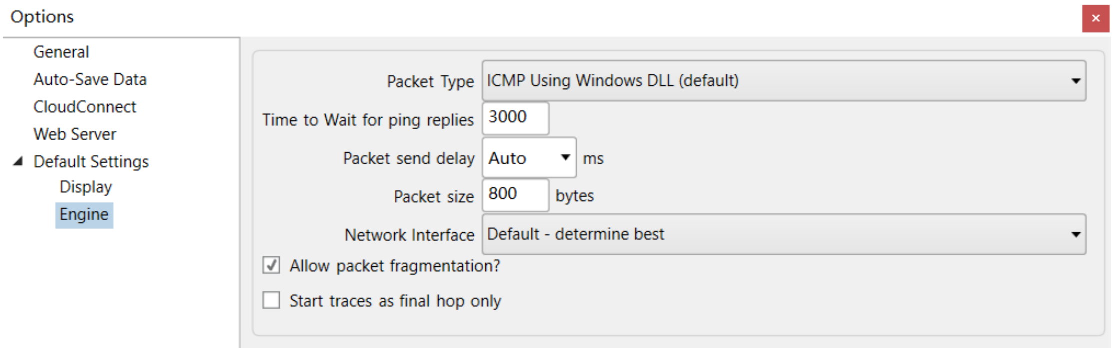
Get notified when a hop goes haywire. Upgrade PingPlotter!

128.59.23.100　Interval 1 second　Focus Auto

Hop	Count	IP	Name	Avg	Min	Cur	PL%	0 ms	Latency	0 ms

并且在 Edit->Options->Engine 设置 Packet Size 为 800 字节

用 wireshark 开始捕获，当 count 为 3 时，手动 pause。



Options

Packet Type: ICMP Using Windows DLL (default)

Time to Wait for ping replies: 3000

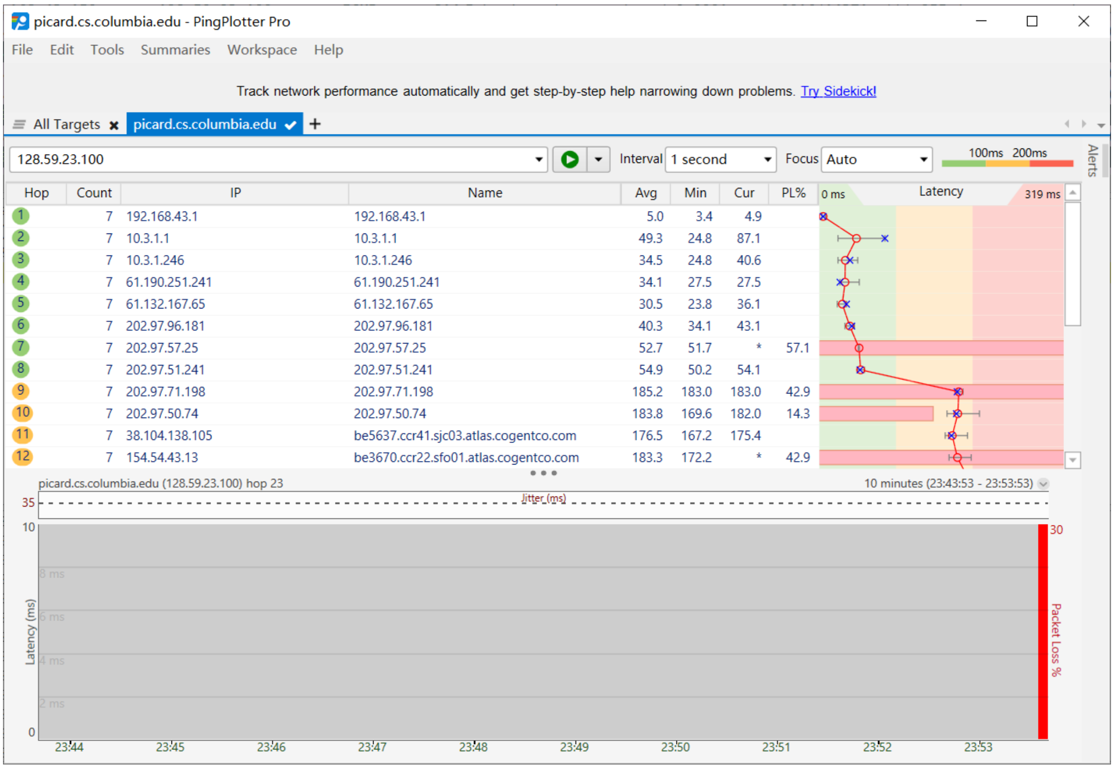
Packet send delay: Auto ms

Packet size: 800 bytes

Network Interface: Default - determine best

☑ Allow packet fragmentation?

☐ Start traces as final hop only



Track network performance automatically and get step-by-step help narrowing down problems. Try Sidekick!

128.59.23.100

Interval 1 second

Focus Auto

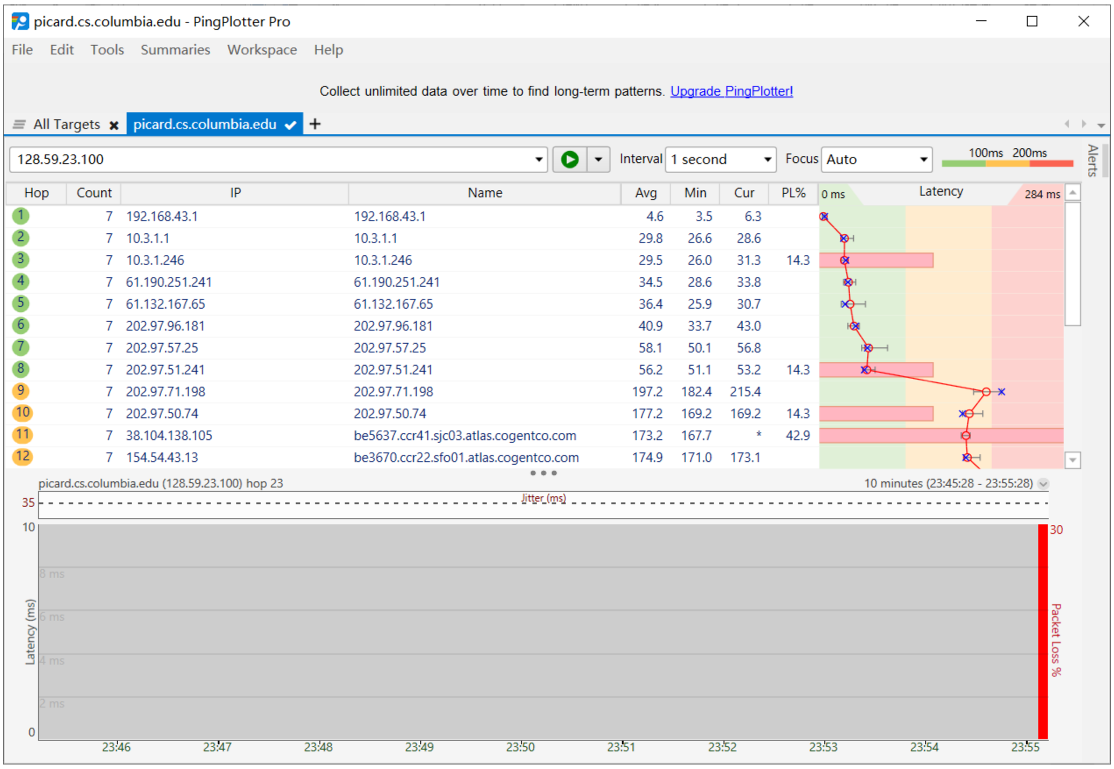
Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	7	192.168.43.1	192.168.43.1	5.0	3.4	4.9	
2	7	10.3.1.1	10.3.1.1	49.3	24.8	87.1	
3	7	10.3.1.246	10.3.1.246	34.5	24.8	40.6	
4	7	61.190.251.241	61.190.251.241	34.1	27.5	27.5	
5	7	61.132.167.65	61.132.167.65	30.5	23.8	36.1	
6	7	202.97.96.181	202.97.96.181	40.3	34.1	43.1	
7	7	202.97.57.25	202.97.57.25	52.7	51.7	*	57.1
8	7	202.97.51.241	202.97.51.241	54.9	50.2	54.1	
9	7	202.97.71.198	202.97.71.198	185.2	183.0	183.0	42.9
10	7	202.97.50.74	202.97.50.74	183.8	169.6	182.0	14.3
11	7	38.104.138.105	be5637.ccr41.sjc03.atlas.cogentco.com	176.5	167.2	175.4	
12	7	154.54.43.13	be3670.ccr22.sfo01.atlas.cogentco.com	183.3	172.2	*	42.9

picard.cs.columbia.edu (128.59.23.100) hop 23

10 minutes (23:43:53 - 23:53:53)

（手动 puase 可能会多传。。。

设置 Packet Size 为 1600、3200 字节，重复上述操作分别得



Collect unlimited data over time to find long-term patterns. Upgrade PingPlotter!

128.59.23.100

Interval 1 second

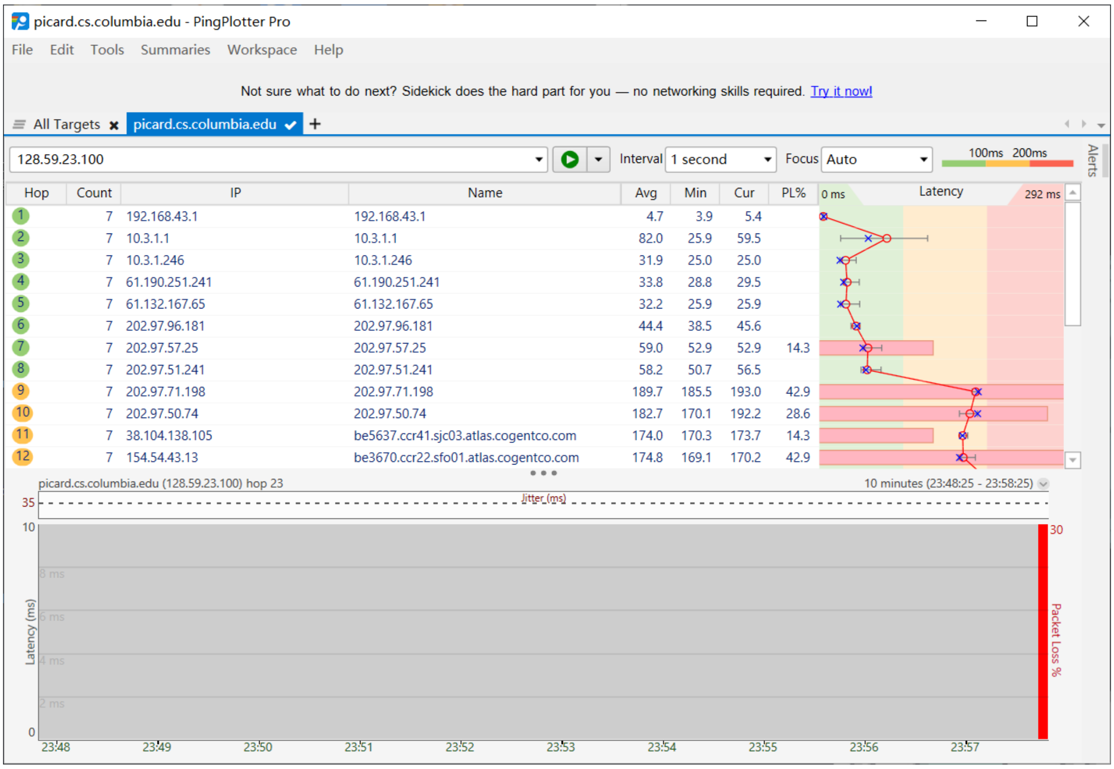
Focus Auto

Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	7	192.168.43.1	192.168.43.1	4.6	3.5	6.3	
2	7	10.3.1.1	10.3.1.1	29.8	26.6	28.6	
3	7	10.3.1.246	10.3.1.246	29.5	26.0	31.3	14.3
4	7	61.190.251.241	61.190.251.241	34.5	28.6	33.8	
5	7	61.132.167.65	61.132.167.65	36.4	25.9	30.7	
6	7	202.97.96.181	202.97.96.181	40.9	33.7	43.0	
7	7	202.97.57.25	202.97.57.25	58.1	50.1	56.8	
8	7	202.97.51.241	202.97.51.241	56.2	51.1	53.2	14.3
9	7	202.97.71.198	202.97.71.198	197.2	182.4	215.4	
10	7	202.97.50.74	202.97.50.74	177.2	169.2	169.2	14.3
11	7	38.104.138.105	be5637.ccr41.sjc03.atlas.cogentco.com	173.2	167.7	*	42.9
12	7	154.54.43.13	be3670.ccr22.sfo01.atlas.cogentco.com	174.9	171.0	173.1	

picard.cs.columbia.edu (128.59.23.100) hop 23

10 minutes (23:45:28 - 23:55:28)

(1600)



picard.cs.columbia.edu - PingPlotter Pro

Not sure what to do next? Sidekick does the hard part for you — no networking skills required. Try it now!

128.59.23.100 Interval 1 second Focus Auto

Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	7	192.168.43.1	192.168.43.1	4.7	3.9	5.4	
2	7	10.3.1.1	10.3.1.1	82.0	25.9	59.5	
3	7	10.3.1.246	10.3.1.246	31.9	25.0	25.0	
4	7	61.190.251.241	61.190.251.241	33.8	28.8	29.5	
5	7	61.132.167.65	61.132.167.65	32.2	25.9	25.9	
6	7	202.97.96.181	202.97.96.181	44.4	38.5	45.6	
7	7	202.97.57.25	202.97.57.25	59.0	52.9	52.9	14.3
8	7	202.97.51.241	202.97.51.241	58.2	50.7	56.5	
9	7	202.97.71.198	202.97.71.198	189.7	185.5	193.0	42.9
10	7	202.97.50.74	202.97.50.74	182.7	170.1	192.2	28.6
11	7	38.104.138.105	be5637.ccr41.sjc03.atlas.cogentco.com	174.0	170.3	173.7	14.3
12	7	154.54.43.13	be3670.ccr22.sfo01.atlas.cogentco.com	174.8	169.1	170.2	42.9

picard.cs.columbia.edu (128.59.23.100) hop 23

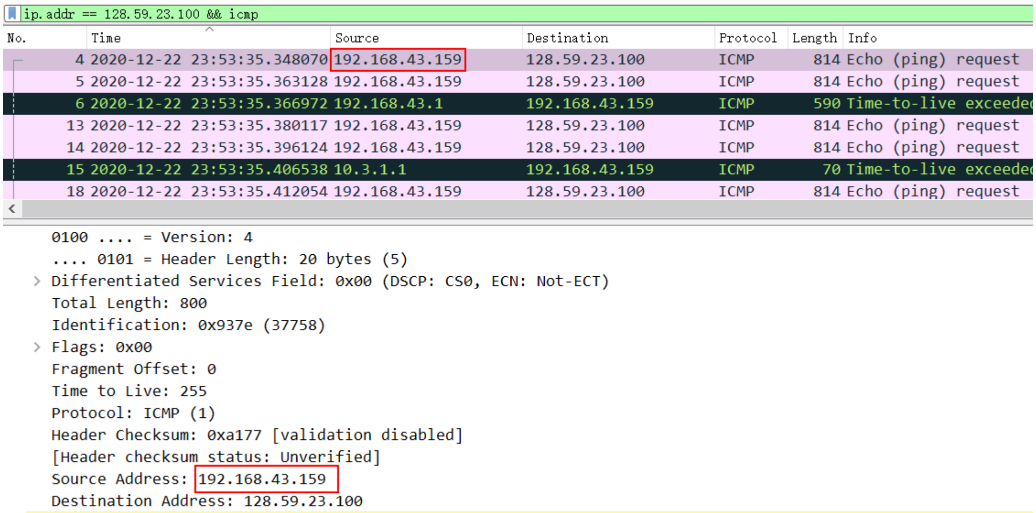
10 minutes (23:48:25 - 23:58:25)

（3200）

五、结果分析

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?

答：192. 168. 43. 159



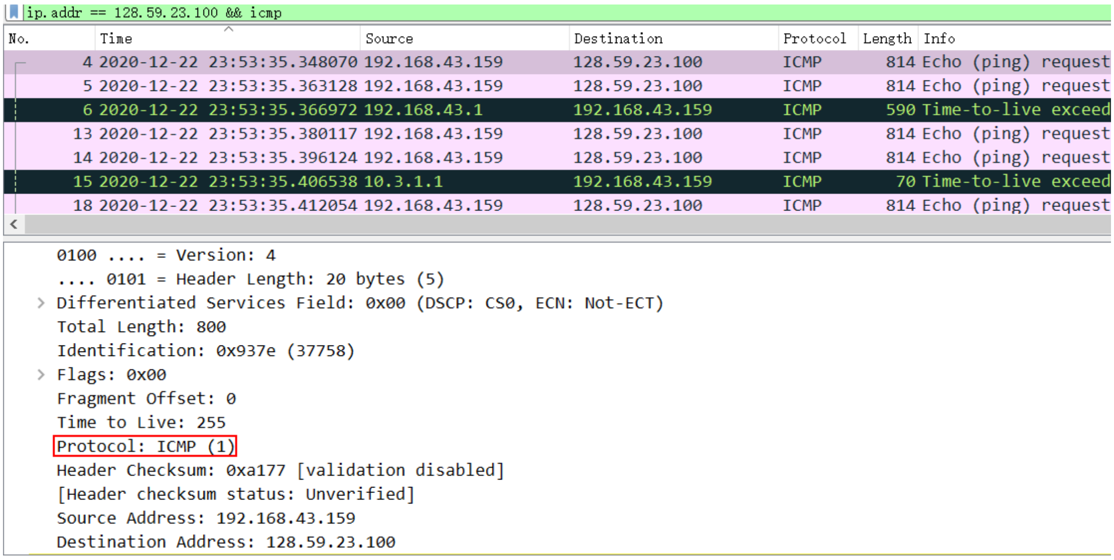
ip.addr == 128.59.23.100 && icmp

```
No.   Time                        Source          Destination     Protocol Length Info
    4 2020-12-22 23:53:35.348070 192.168.43.159  128.59.23.100   ICMP      814 Echo (ping) request
    5 2020-12-22 23:53:35.363128 192.168.43.159  128.59.23.100   ICMP      814 Echo (ping) request
    6 2020-12-22 23:53:35.366972 192.168.43.1    192.168.43.159  ICMP      590 Time-to-live exceeded
   13 2020-12-22 23:53:35.380117 192.168.43.159  128.59.23.100   ICMP      814 Echo (ping) request
   14 2020-12-22 23:53:35.396124 192.168.43.159  128.59.23.100   ICMP      814 Echo (ping) request
   15 2020-12-22 23:53:35.406538 10.3.1.1        192.168.43.159  ICMP       70 Time-to-live exceeded
   18 2020-12-22 23:53:35.412054 192.168.43.159  128.59.23.100   ICMP      814 Echo (ping) request
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 800
    Identification: 0x937e (37758)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xa177 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.159
    Destination Address: 128.59.23.100
```

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

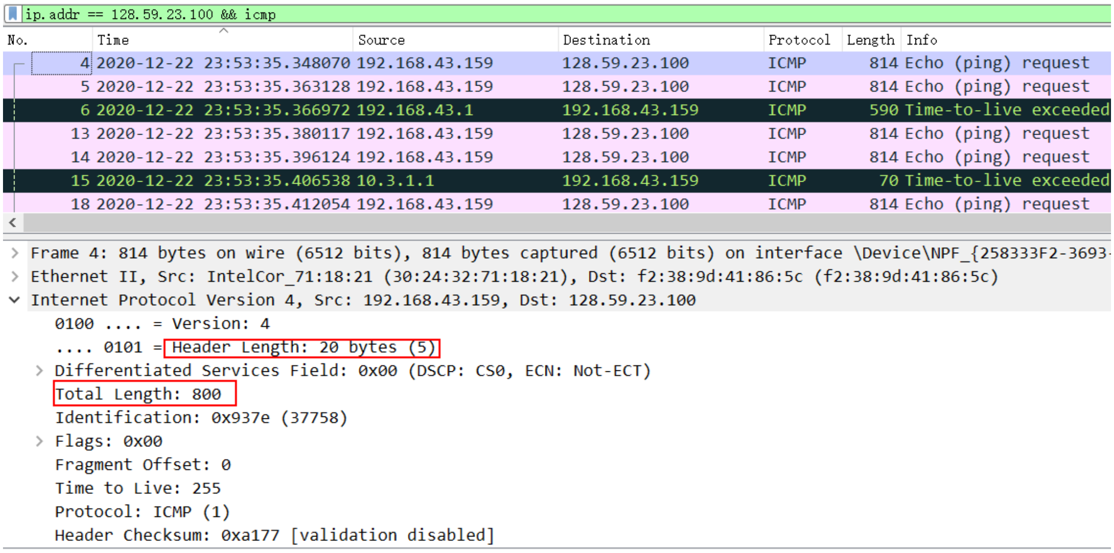
答： 1(表示ICMP)



```
ip.addr == 128.59.23.100 && icmp
No.   Time                         Source          Destination     Protocol  Length  Info
    4 2020-12-22 23:53:35.348070 192.168.43.159  128.59.23.100   ICMP       814 Echo (ping) request
    5 2020-12-22 23:53:35.363128 192.168.43.159  128.59.23.100   ICMP       814 Echo (ping) request
    6 2020-12-22 23:53:35.366972 192.168.43.1    192.168.43.159  ICMP       590 Time-to-live exceed
   13 2020-12-22 23:53:35.380117 192.168.43.159  128.59.23.100   ICMP       814 Echo (ping) request
   14 2020-12-22 23:53:35.396124 192.168.43.159  128.59.23.100   ICMP       814 Echo (ping) request
   15 2020-12-22 23:53:35.406538 10.3.1.1        192.168.43.159  ICMP        70 Time-to-live exceed
   18 2020-12-22 23:53:35.412054 192.168.43.159  128.59.23.100   ICMP       814 Echo (ping) request

    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 800
    Identification: 0x937e (37758)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xa177 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.159
    Destination Address: 128.59.23.100
```

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.

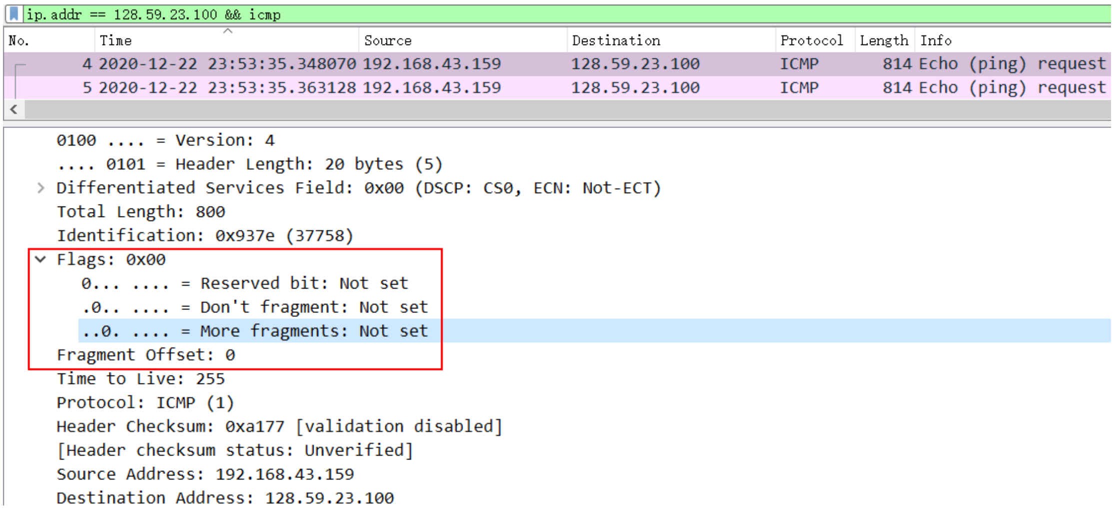
答： 780 字节,800-20=780 字节.payload 字节数就是总字节数减去 header 字节数.



```
ip.addr == 128.59.23.100 && icmp
No.   Time                         Source          Destination     Protocol  Length  Info
    4 2020-12-22 23:53:35.348070 192.168.43.159  128.59.23.100   ICMP       814 Echo (ping) request
    5 2020-12-22 23:53:35.363128 192.168.43.159  128.59.23.100   ICMP       814 Echo (ping) request
    6 2020-12-22 23:53:35.366972 192.168.43.1    192.168.43.159  ICMP       590 Time-to-live exceeded
   13 2020-12-22 23:53:35.380117 192.168.43.159  128.59.23.100   ICMP       814 Echo (ping) request
   14 2020-12-22 23:53:35.396124 192.168.43.159  128.59.23.100   ICMP       814 Echo (ping) request
   15 2020-12-22 23:53:35.406538 10.3.1.1        192.168.43.159  ICMP        70 Time-to-live exceeded
   18 2020-12-22 23:53:35.412054 192.168.43.159  128.59.23.100   ICMP       814 Echo (ping) request

> Frame 4: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits) on interface \Device\NPF_{258333F2-3693-
> Ethernet II, Src: IntelCor_71:18:21 (30:24:32:71:18:21), Dst: f2:38:9d:41:86:5c (f2:38:9d:41:86:5c)
v Internet Protocol Version 4, Src: 192.168.43.159, 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: 800
    Identification: 0x937e (37758)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xa177 [validation disabled]
```

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

答： 这里的 IP 数据报没有被分段， 因为 Fragment offset = 0，分段的偏移量为 0，所以没有分段，而且 More fragments 也是为 Not set，表示没有设置分段。如下:



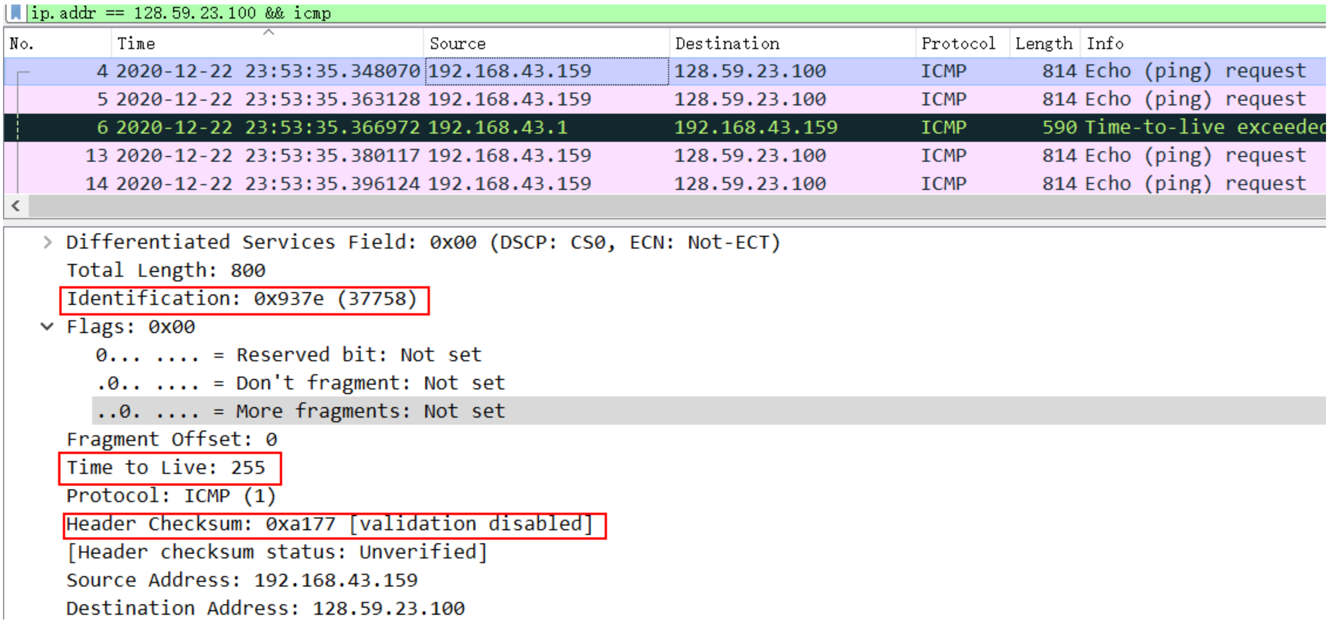
```
ip.addr == 128.59.23.100 && icmp
No.     Time                        Source          Destination     Protocol  Length  Info
      4 2020-12-22 23:53:35.348070 192.168.43.159  128.59.23.100   ICMP         814 Echo (ping) request
      5 2020-12-22 23:53:35.363128 192.168.43.159  128.59.23.100   ICMP         814 Echo (ping) request

    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 800
    Identification: 0x937e (37758)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xa177 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.159
    Destination Address: 128.59.23.100
```

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?

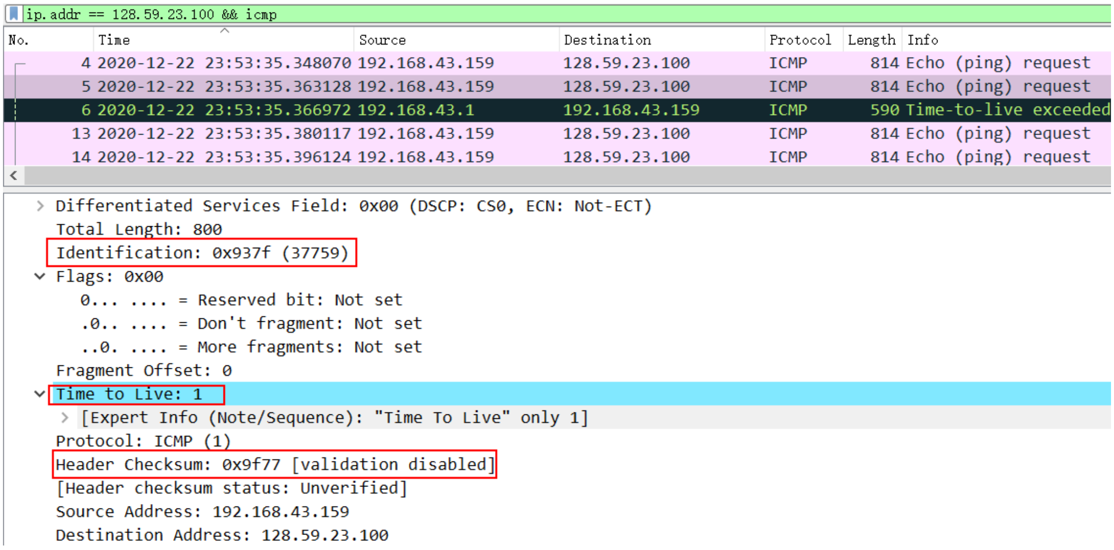
答:

从下面可以看出:

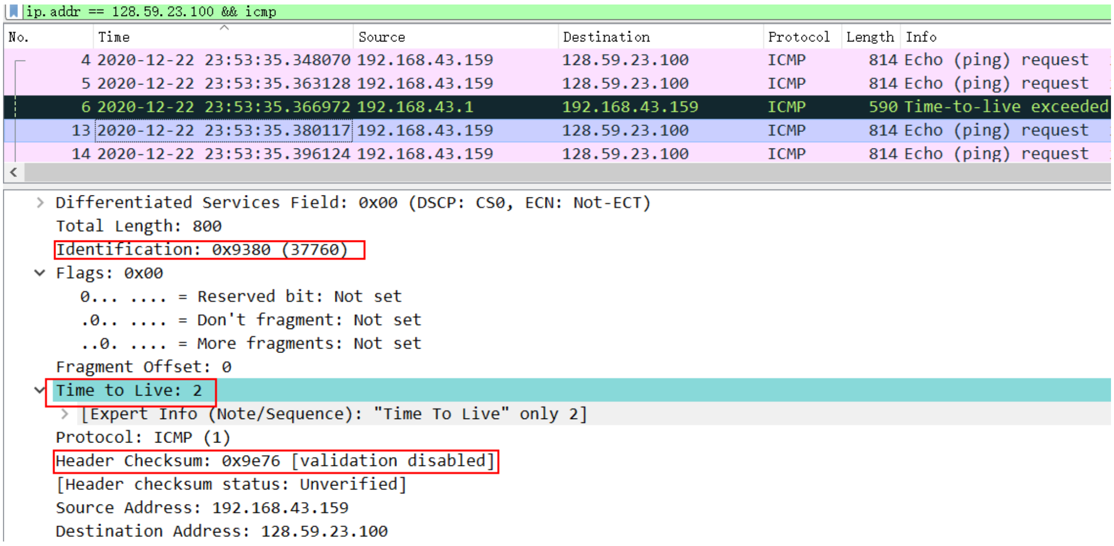
Header 中的 TTL,checksum,Identification 总改变



```
ip.addr == 128.59.23.100 && icmp
No.     Time                        Source          Destination     Protocol  Length  Info
      4 2020-12-22 23:53:35.348070 192.168.43.159  128.59.23.100   ICMP         814 Echo (ping) request
      5 2020-12-22 23:53:35.363128 192.168.43.159  128.59.23.100   ICMP         814 Echo (ping) request
      6 2020-12-22 23:53:35.366972 192.168.43.1    192.168.43.159  ICMP         590 Time-to-live exceeded
     13 2020-12-22 23:53:35.380117 192.168.43.159  128.59.23.100   ICMP         814 Echo (ping) request
     14 2020-12-22 23:53:35.396124 192.168.43.159  128.59.23.100   ICMP         814 Echo (ping) request

  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 800
    Identification: 0x937e (37758)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0xa177 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.159
    Destination Address: 128.59.23.100
```



```
ip.addr == 128.59.23.100 && icmp
No.  Time                          Source           Destination      Protocol  Length  Info
   4 2020-12-22 23:53:35.348070 192.168.43.159   128.59.23.100    ICMP       814 Echo (ping) request
   5 2020-12-22 23:53:35.363128 192.168.43.159   128.59.23.100    ICMP       814 Echo (ping) request
   6 2020-12-22 23:53:35.366972 192.168.43.1     192.168.43.159   ICMP       590 Time-to-live exceeded
  13 2020-12-22 23:53:35.380117 192.168.43.159   128.59.23.100    ICMP       814 Echo (ping) request
  14 2020-12-22 23:53:35.396124 192.168.43.159   128.59.23.100    ICMP       814 Echo (ping) request

 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 800
   Identification: 0x937f (37759)
 v Flags: 0x00
     0... .... = Reserved bit: Not set
     .0.. .... = Don't fragment: Not set
     ..0. .... = More fragments: Not set
   Fragment Offset: 0
 v Time to Live: 1
   > [Expert Info (Note/Sequence): "Time To Live" only 1]
   Protocol: ICMP (1)
   Header Checksum: 0x9f77 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 192.168.43.159
   Destination Address: 128.59.23.100
```



```
ip.addr == 128.59.23.100 && icmp
No.  Time                          Source           Destination      Protocol  Length  Info
   4 2020-12-22 23:53:35.348070 192.168.43.159   128.59.23.100    ICMP       814 Echo (ping) request
   5 2020-12-22 23:53:35.363128 192.168.43.159   128.59.23.100    ICMP       814 Echo (ping) request
   6 2020-12-22 23:53:35.366972 192.168.43.1     192.168.43.159   ICMP       590 Time-to-live exceeded
  13 2020-12-22 23:53:35.380117 192.168.43.159   128.59.23.100    ICMP       814 Echo (ping) request
  14 2020-12-22 23:53:35.396124 192.168.43.159   128.59.23.100    ICMP       814 Echo (ping) request

 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 800
   Identification: 0x9380 (37760)
 v Flags: 0x00
     0... .... = Reserved bit: Not set
     .0.. .... = Don't fragment: Not set
     ..0. .... = More fragments: Not set
   Fragment Offset: 0
 v Time to Live: 2
   > [Expert Info (Note/Sequence): "Time To Live" only 2]
   Protocol: ICMP (1)
   Header Checksum: 0x9e76 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 192.168.43.159
   Destination Address: 128.59.23.100
```

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

答：stay constant:

Version, header length, Differentiated Services Field, flags, fragment offset, protocol, source ip address, destination ip address.

必须不变的是

Version:因为都是 ipV4.

Protocol:都是 ICMP

Header length: 因为 protocol 不变，是 icmp，所以 header 不变

Differentiated Services:理由同上，都是 icmp 类型

source ip address,destination ip address:源，目的地址在这一过程不变

必须变的是:

TTL:因为 traceroute 会改变 ttl

Identification:IP 数据报之间要有不一样的 id

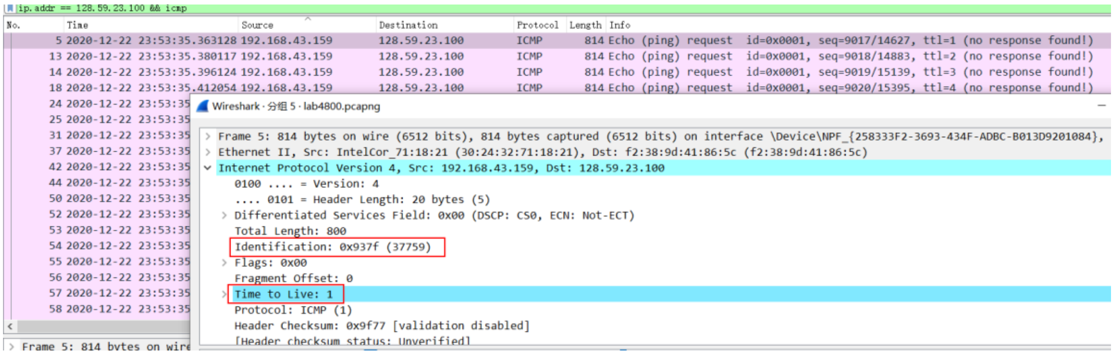
Header checksum:因为 header 每次都会不一样

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

答： 每个 id 会比前一个增加 1，每个 IP 数据报的标识号是不同的，用于区分每个 IP 数据报和处理 IP 分片。

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

答：



```
ip.addr == 128.59.23.100 && icmp
No.   Time                        Source          Destination    Protocol Length Info
    5 2020-12-22 23:53:35.363128 192.168.43.159  128.59.23.100  ICMP     814 Echo (ping) request  id=0x0001, seq=9017/14627, ttl=1 (no response found!)
   13 2020-12-22 23:53:35.380117 192.168.43.159  128.59.23.100  ICMP     814 Echo (ping) request  id=0x0001, seq=9018/14883, ttl=2 (no response found!)
   14 2020-12-22 23:53:35.396124 192.168.43.159  128.59.23.100  ICMP     814 Echo (ping) request  id=0x0001, seq=9019/15139, ttl=3 (no response found!)
   18 2020-12-22 23:53:35.412054 192.168.43.159  128.59.23.100  ICMP     814 Echo (ping) request  id=0x0001, seq=9020/15395, ttl=4 (no response found!)
   24 2020-12-22 23:53:35
   25 2020-12-22 23:53:35
   31 2020-12-22 23:53:35
   37 2020-12-22 23:53:35
   42 2020-12-22 23:53:35
   44 2020-12-22 23:53:35
   50 2020-12-22 23:53:35
   52 2020-12-22 23:53:35
   53 2020-12-22 23:53:35
   54 2020-12-22 23:53:35
   55 2020-12-22 23:53:35
   56 2020-12-22 23:53:35
   57 2020-12-22 23:53:35
   58 2020-12-22 23:53:35
> Frame 5: 814 bytes on wire

Wireshark · 分组 5 · lab4800.pcapng
> Frame 5: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits) on interface \Device\NPF_{258333F2-3693-434F-ADBC-B013D9201084},
> Ethernet II, Src: IntelCor_71:18:21 (30:24:32:71:18:21), Dst: f2:38:9d:41:86:5c (f2:38:9d:41:86:5c)
v Internet Protocol Version 4, Src: 192.168.43.159, 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: 800
    Identification: 0x937f (37759)
  > Flags: 0x00
    Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x9f77 [validation disabled]
    [Header checksum status: Unverified]
```

第一跳的id为0x937f (37759),ttl为1

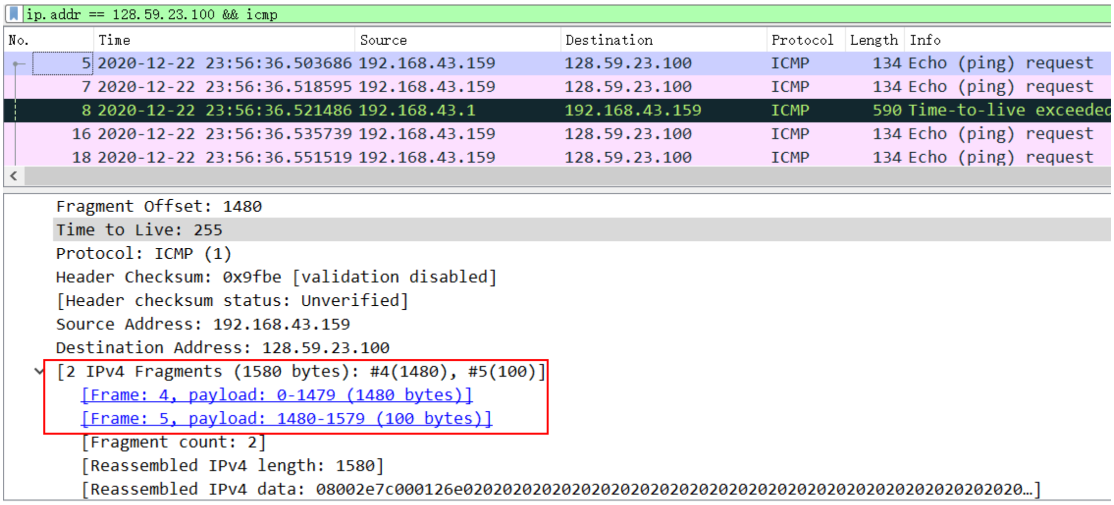
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

答： id变化,因为id相同表示ip包是同一个大包的fragment,这里的id需要独立.ttl不变.因为在一段时间内(排除电脑转移或者网络环

境彻底变化），电脑的第一跳路由是不变的，默认不会改变。

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? [Note: if you find your packet has not been fragmented, you should download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the *ipethereal-*
*trace-1*packet trace. If your computer has an Ethernet interface, a packet size of 2000 *should* cause fragmentation.3]

答：　是的，被分成了2份fragments.



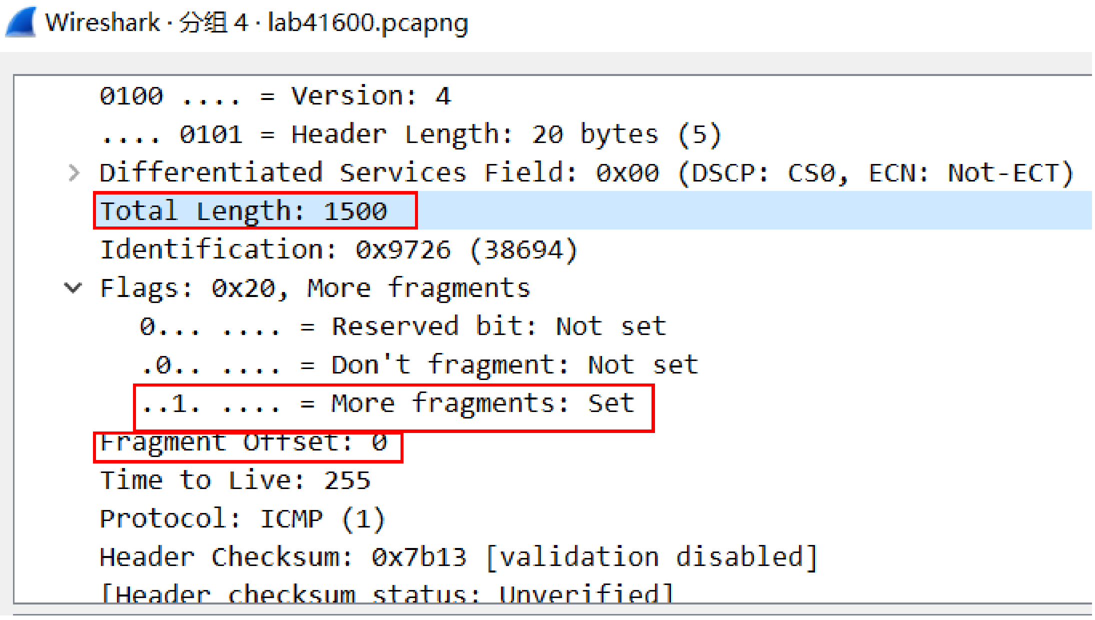
```
ip.addr == 128.59.23.100 && icmp
```

```
No.   Time                        Source          Destination     Protocol  Length  Info
    5 2020-12-22 23:56:36.503686 192.168.43.159  128.59.23.100   ICMP      134 Echo (ping) request
    7 2020-12-22 23:56:36.518595 192.168.43.159  128.59.23.100   ICMP      134 Echo (ping) request
    8 2020-12-22 23:56:36.521486 192.168.43.1    192.168.43.159  ICMP      590 Time-to-live exceeded
   16 2020-12-22 23:56:36.535739 192.168.43.159  128.59.23.100   ICMP      134 Echo (ping) request
   18 2020-12-22 23:56:36.551519 192.168.43.159  128.59.23.100   ICMP      134 Echo (ping) request
```

```
    Fragment Offset: 1480
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x9fbe [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.159
    Destination Address: 128.59.23.100
  ⌄ [2 IPv4 Fragments (1580 bytes): #4(1480), #5(100)]
      [Frame: 4, payload: 0-1479 (1480 bytes)]
      [Frame: 5, payload: 1480-1579 (100 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 1580]
      [Reassembled IPv4 data: 08002e7c000126e020202020202020202020202020202020202020202020202020202020…]
```

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?

答：　有上一题的图找到No. 4 frame，得到：



Wireshark · 分组 4 · lab41600.pcapng

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x9726 (38694)
  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: 255
    Protocol: ICMP (1)
    Header Checksum: 0x7b13 [validation disabled]
    [Header checksum status: Unverified]
```

其中flags中的 More fragments位被置为1.

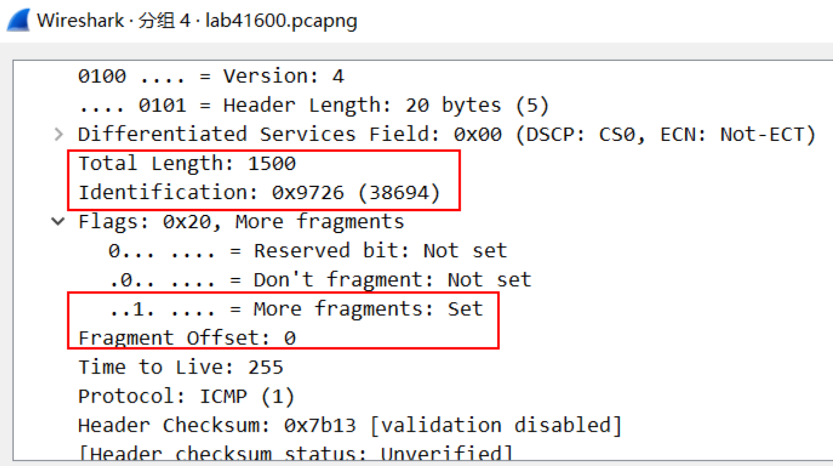
这里的fragment offset为0,

整个ip包的长度为1500字节.

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?

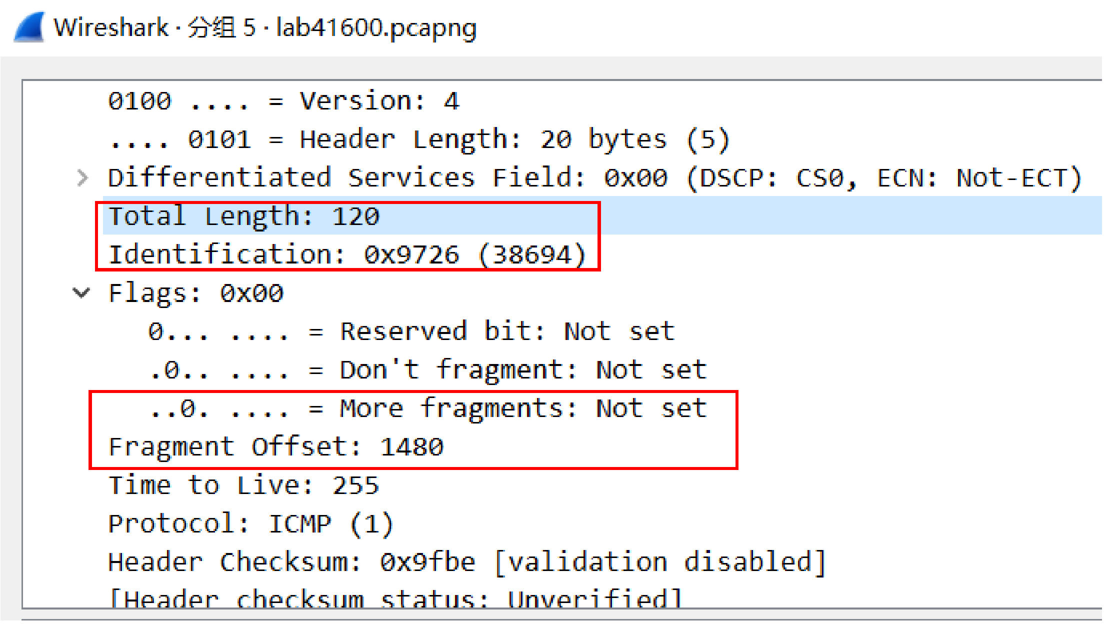
答：如下图所示.与No.4 frame相同id的No.5 frame,其fragment offset为1480,非0,表示不是第一个.

不能根据more fragments位判断是不是第一个,因为最后一个fragment的more fragments位也是0.



Wireshark · 分组 4 · lab41600.pcapng

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x9726 (38694)
  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: 255
    Protocol: ICMP (1)
    Header Checksum: 0x7b13 [validation disabled]
    [Header checksum status: Unverified]
```



Wireshark · 分组 5 · lab41600.pcapng

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 120
    Identification: 0x9726 (38694)
  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: 255
    Protocol: ICMP (1)
    Header Checksum: 0x9fbe [validation disabled]
    [Header checksum status: Unverified]
```

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

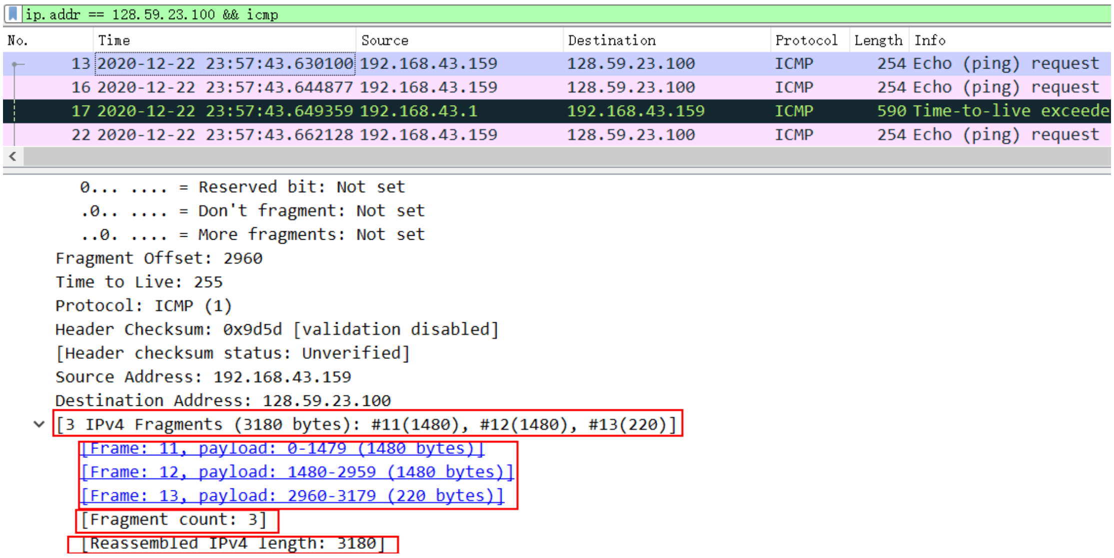
答：就这两个fragment来说的话,变的有:

Total length, flags, fragment offset, header checksum

对于所有的第一个fragment与第二个fragment来说的话,一般肯定变的有:Fragment offset和header checksum

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

答： 3个



ip.addr == 128.59.23.100 && icmp

```
No.   Time                        Source          Destination     Protocol  Length Info
   13 2020-12-22 23:57:43.630100 192.168.43.159  128.59.23.100   ICMP         254 Echo (ping) request
   16 2020-12-22 23:57:43.644877 192.168.43.159  128.59.23.100   ICMP         254 Echo (ping) request
   17 2020-12-22 23:57:43.649359 192.168.43.1    192.168.43.159  ICMP         590 Time-to-live exceede
   22 2020-12-22 23:57:43.662128 192.168.43.159  128.59.23.100   ICMP         254 Echo (ping) request
```

```
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 2960
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x9d5d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.159
    Destination Address: 128.59.23.100
  v [3 IPv4 Fragments (3180 bytes): #11(1480), #12(1480), #13(220)]
      [Frame: 11, payload: 0-1479 (1480 bytes)]
      [Frame: 12, payload: 1480-2959 (1480 bytes)]
      [Frame: 13, payload: 2960-3179 (220 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 3180]
```

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

答： 总长度Total Length、标志Flags、fragment offset、Header checksum等。

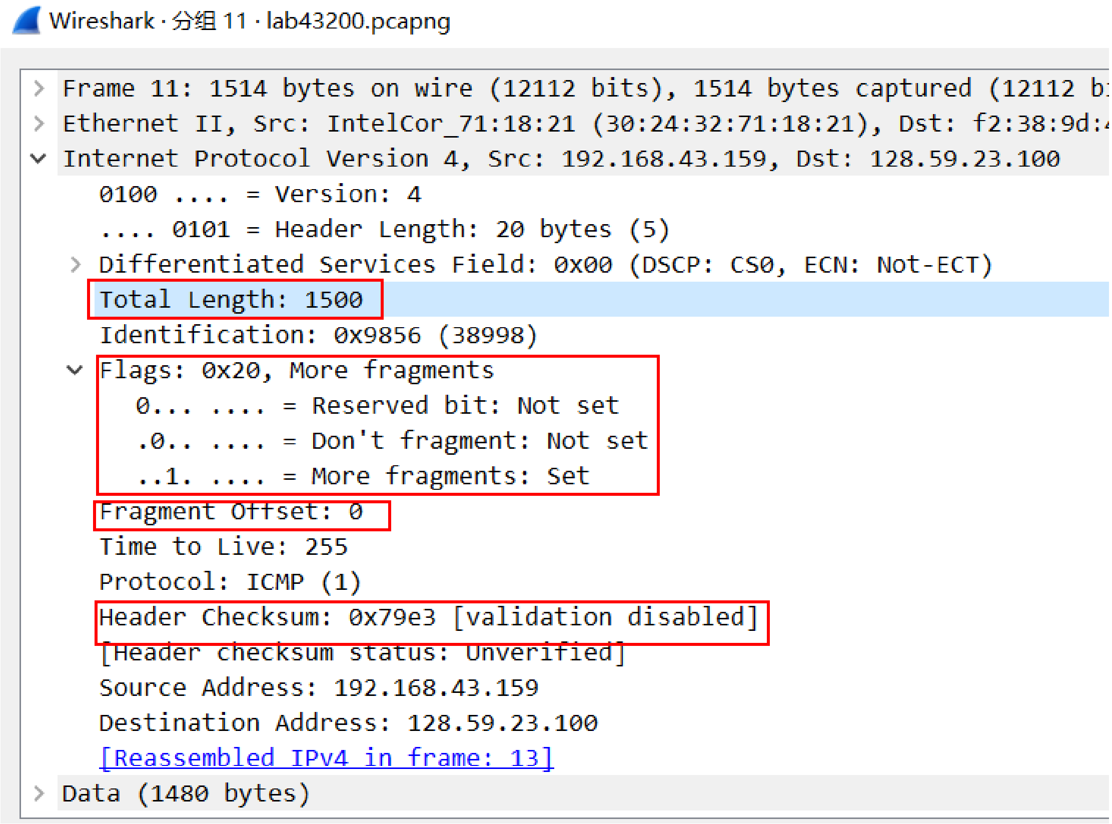
第一个是分组11、第二个是分组12、第三个是分组13

第一个第二个的Total Length是1500,第三个是240

在Flags中，第一个第二个的more fragments位是1,第三个是0

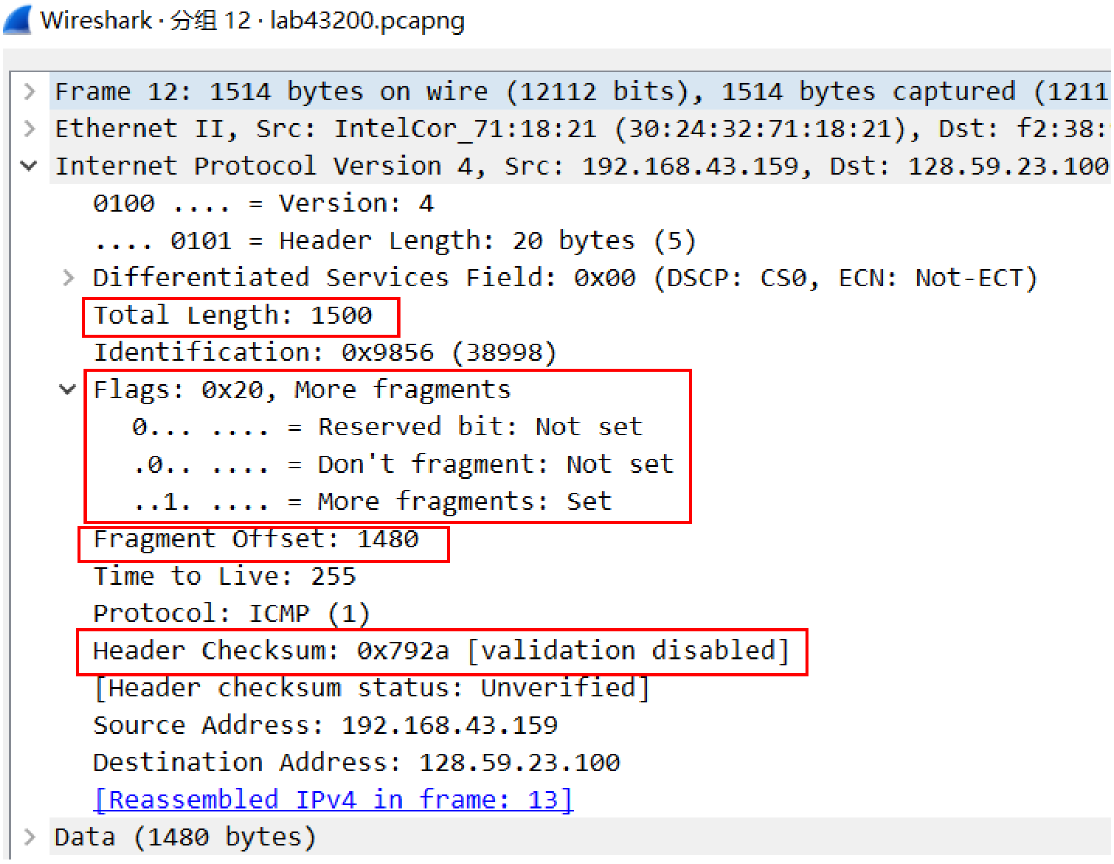
第一个的fragment offset是0，第二个是1480，第三个是2960

第一个的Header checksum是0x79e3、第二个是0x792a、第三个是0x9d5d



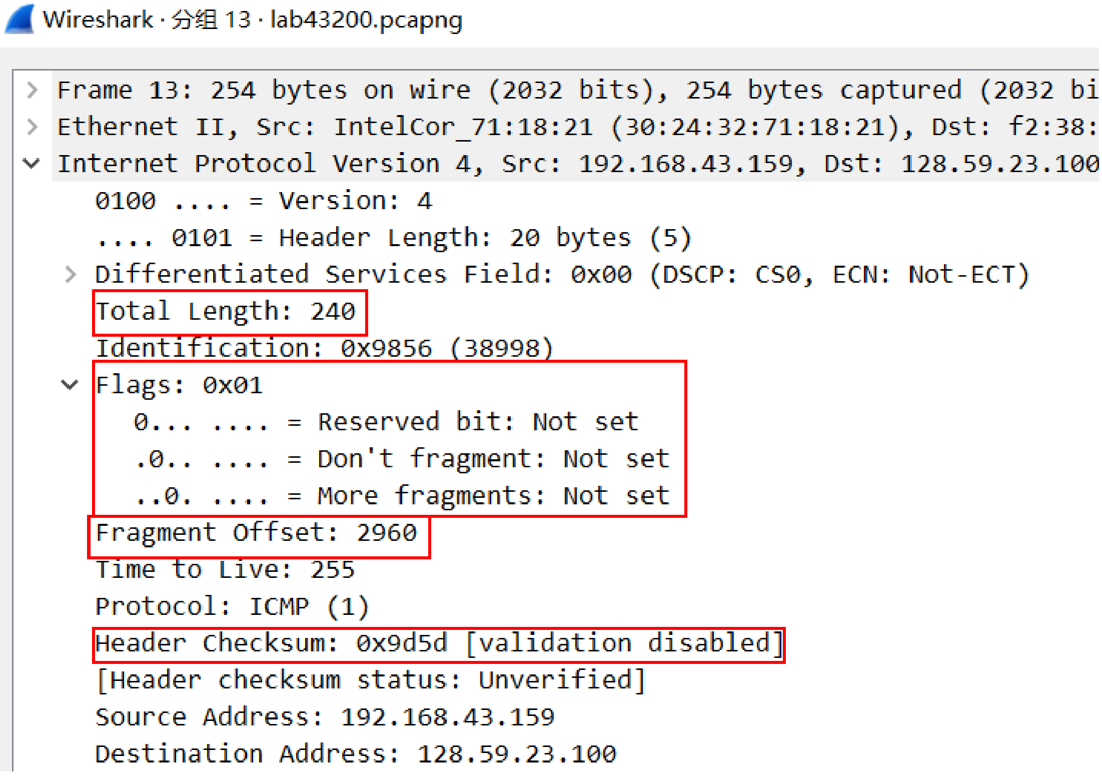
Wireshark · 分组 11 · lab43200.pcapng

```
> Frame 11: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bi
> Ethernet II, Src: IntelCor_71:18:21 (30:24:32:71:18:21), Dst: f2:38:9d:
v Internet Protocol Version 4, Src: 192.168.43.159, 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: 0x9856 (38998)
  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: 255
    Protocol: ICMP (1)
    Header Checksum: 0x79e3 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.159
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 13]
> Data (1480 bytes)
```



Wireshark · 分组 12 · lab43200.pcapng

```
> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (1211
> Ethernet II, Src: IntelCor_71:18:21 (30:24:32:71:18:21), Dst: f2:38:
v Internet Protocol Version 4, Src: 192.168.43.159, 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: 0x9856 (38998)
  v Flags: 0x20, More fragments
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
    Fragment Offset: 1480
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x792a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.159
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 13]
> Data (1480 bytes)
```



Wireshark · 分组 13 · lab43200.pcapng

```
> Frame 13: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bi
> Ethernet II, Src: IntelCor_71:18:21 (30:24:32:71:18:21), Dst: f2:38:
v Internet Protocol Version 4, Src: 192.168.43.159, 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: 240
    Identification: 0x9856 (38998)
  v Flags: 0x01
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment Offset: 2960
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x9d5d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.159
    Destination Address: 128.59.23.100
```