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 数据报

学　　号：PB18111793

姓　　名：裴启智

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 20 日

一、 实验目的

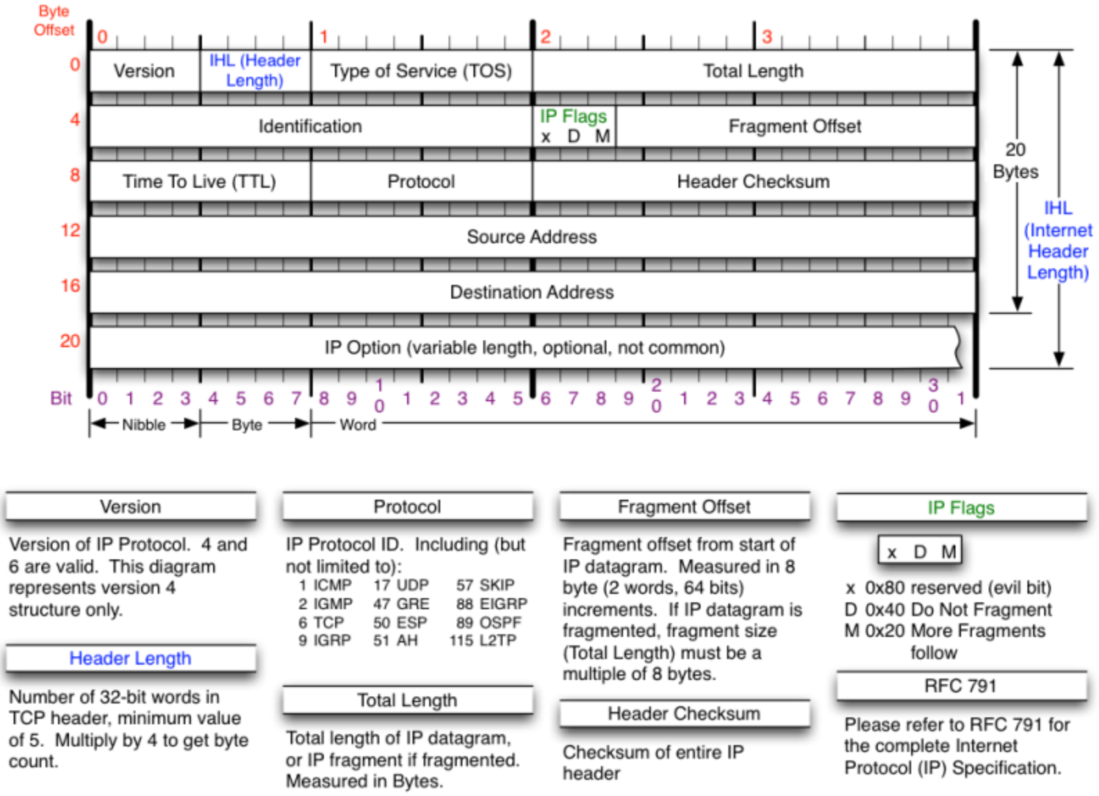
1. 捕获观察并分析 IP 数据报的结构。

2. 掌握 traceroute 的使用(Windows 下替换为 PingPlotter)。

3. 回答 pdf 中的 question 部分的问题

二、 实验原理

1、 IPv4 报文



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

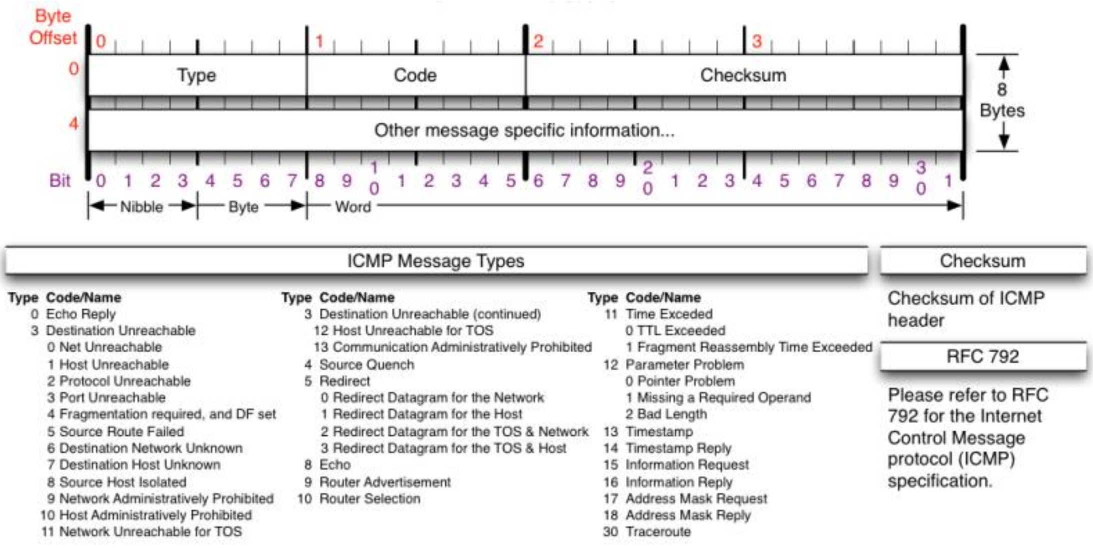
x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

2、 ICMP 报文结构



ICMP Message Types

Type	Code/Name
0	Echo Reply
3	Destination Unreachable
	0 Net Unreachable
	1 Host Unreachable
	2 Protocol Unreachable
	3 Port Unreachable
	4 Fragmentation required, and DF set
	5 Source Route Failed
	6 Destination Network Unknown
	7 Destination Host Unknown
	8 Source Host Isolated
	9 Network Administratively Prohibited
	10 Host Administratively Prohibited
	11 Network Unreachable for TOS
3	Destination Unreachable (continued)
	12 Host Unreachable for TOS
	13 Communication Administratively Prohibited
4	Source Quench
5	Redirect
	0 Redirect Datagram for the Network
	1 Redirect Datagram for the Host
	2 Redirect Datagram for the TOS & Network
	3 Redirect Datagram for the TOS & Host
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceded
	0 TTL Exceeded
	1 Fragment Reassembly Time Exceeded
12	Parameter Problem
	0 Pointer Problem
	1 Missing a Required Operand
	2 Bad Length
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
30	Traceroute

Checksum

Checksum of ICMP header

RFC 792

Please refer to RFC 792 for the Internet Control Message protocol (ICMP) specification.

3. IP 报文分片

MTU： Maximum Transmit Unit，最大传输单元，即物理接口（数据链路层）提供给其上层（通常是 IP 层）最大一次传输数据的大小；以普遍使用的以太网接口为例，缺省 MTU=1500 Byte，这是以太网接口对 IP 层的约束，如果 IP 层有<=1500 byte 需要发送，只需要一个 IP 包就可以完成发送任务；如果 IP 层有> 1500 byte 数据需要发送，需要分片才能完成发送

标识：唯一的标识主机发送的每一份数据报。通常每发送一个报文，它的值加一。当 IP 报文长度超过传输网络的 MTU（最大传输单元）时必须分片，这个标识字段的值被复制到所有数据分片的标识字段中，使得这些分片在达到最终目的地时可以依照标识字段的内容重新组成原先的数据。

4. TTL

TTL 是 IP 数据包在计算机网络中可以转发的最大跳数。TTL 字段由 IP 数据包的发送者设置，在 IP 数据包从源到目的的整个转发路径上，每经过一个路由器，路由器都会修改这个 TTL 字段值，具体的做法是把该 TTL 的值减 1，然后再将 IP 包转发出去。如果在 IP 包到达目的 IP 之前，TTL 减少为 0，路由器将会丢弃收到的 TTL=0 的 IP 包并向 IP 包的发送者发送 ICMP time exceeded 消息。

TTL 的主要作用是避免 IP 包在网络中的无限循环和收发，节省了网络资源，并能使 IP 包的发送者能收到告警消息。

TTL 是由发送主机设置的，以防止数据包不断在 IP 互联网络上永不终止地循环。转发 IP 数据包时，要求路由器至少将 TTL 减小 1。

三、 实验条件

1、 硬件条件：一台 PC 机：联想小新 pro13 2019

AMD 锐龙 5 3550H 2.1GHz

16G 内存

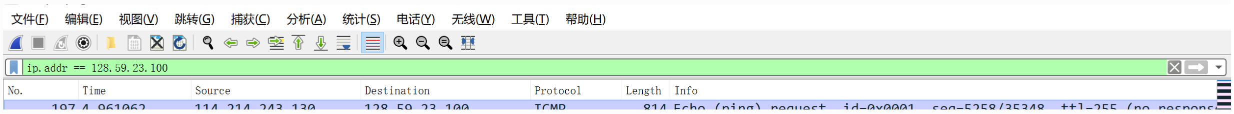
2、 软件条件：Windows10

Wireshark3.4.2

四、实验过程

1. 在官网下载 PingPlotter 专业版，安装14天试用版本

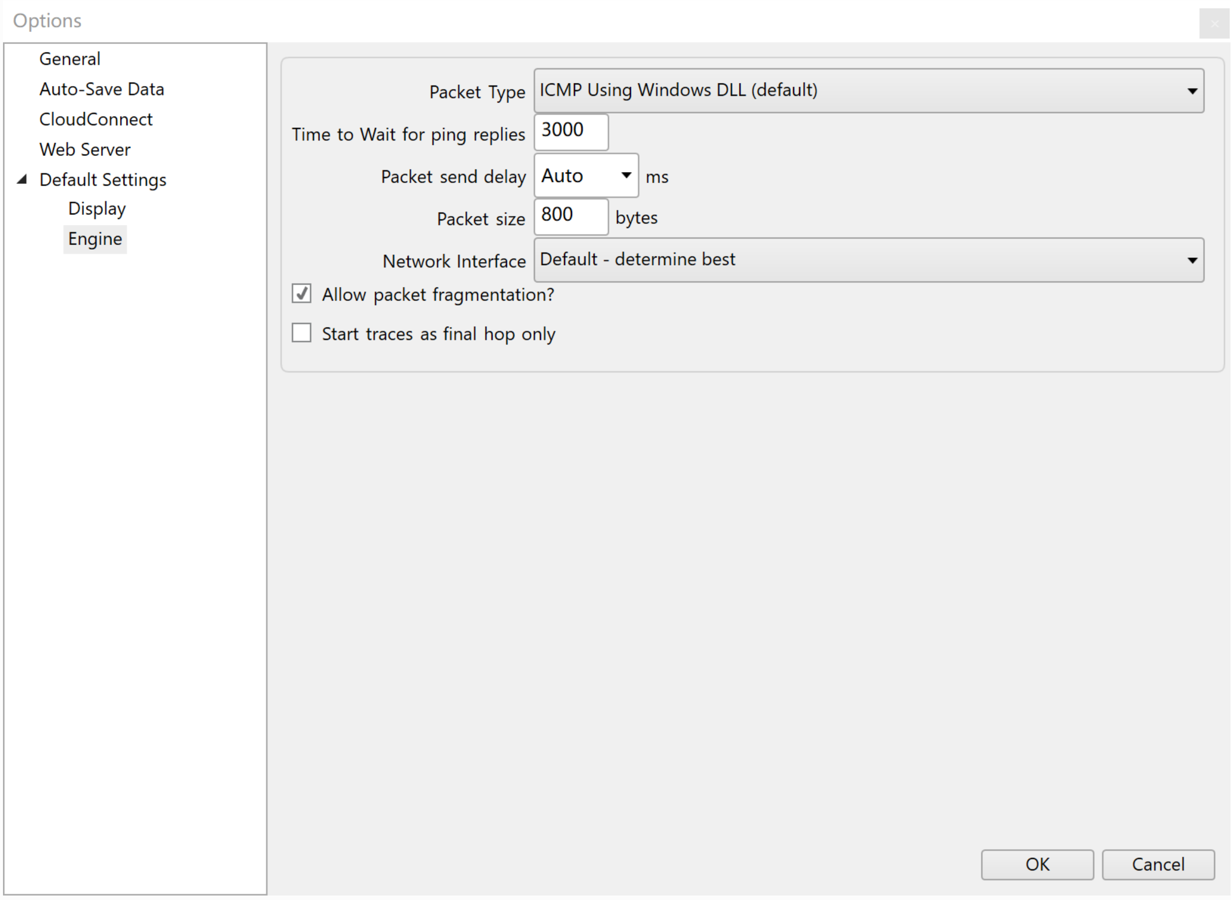
2. 打开Wireshark抓包，并设置过滤条件如下图


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.addr == 128.59.23.100

No.	Time	Source	Destination	Protocol	Length	Info
197	4.961062	114.214.243.130	128.59.23.100	ICMP	814	Echo (ping) request id=0x0001, seq=5258/35348, ttl=255 (no respons

3. 打开 PingPlotter，设置 Edit→Options→Default→Settings→Engine中的Packet size为800



Packet Type: ICMP Using Windows DLL (default)

Time to Wait for ping replies: 3000

Packet send delay: Auto ms

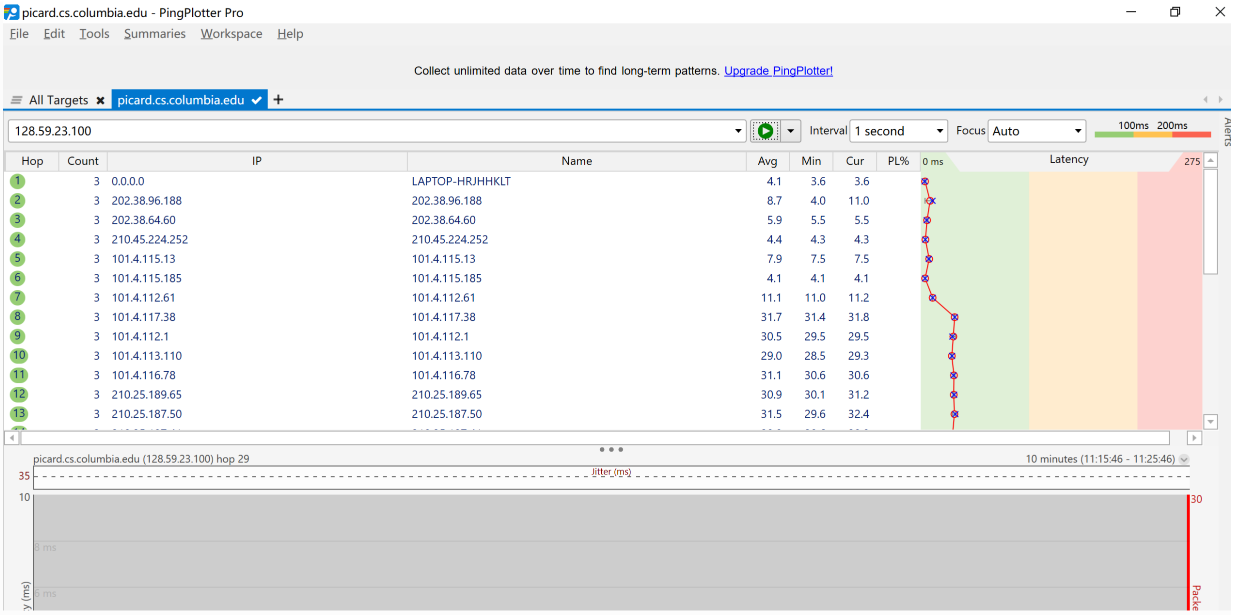
Packet size: 800 bytes

Network Interface: Default - determine best

☑ Allow packet fragmentation?

□ Start traces as final hop only

4. 输入ip地址 128.59.23.100进行跟踪，跟踪约3次（新版本的PingPlotter Pro好像不能设置“# of times to Trace”，只能手动停止，无法准确达到英文pdf中的“Enter 3 in the “# of times to Trace” field, so you don’t gather too much data”，不过不影响分析）



picard.cs.columbia.edu - PingPlotter Pro

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

picard.cs.columbia.edu

128.59.23.100

Interval 1 second

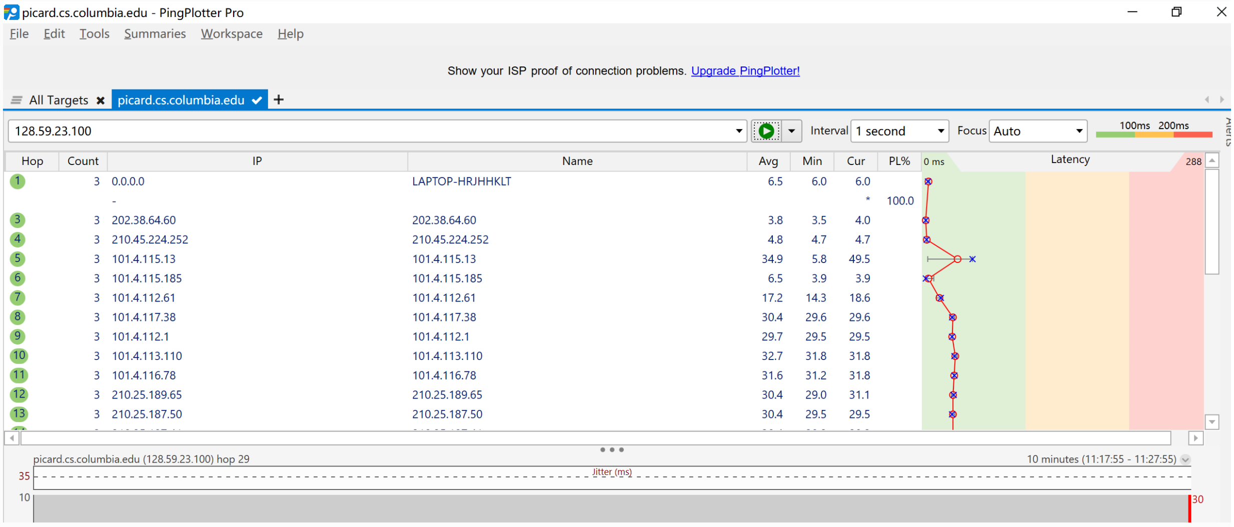
Focus Auto

Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	3	0.0.0.0	LAPTOP-HRJHHKLT	4.1	3.6	3.6	
2	3	202.38.96.188	202.38.96.188	8.7	4.0	11.0	
3	3	202.38.64.60	202.38.64.60	5.9	5.5	5.5	
4	3	210.45.224.252	210.45.224.252	4.4	4.3	4.3	
5	3	101.4.115.13	101.4.115.13	7.9	7.5	7.5	
6	3	101.4.115.185	101.4.115.185	4.1	4.1	4.1	
7	3	101.4.112.61	101.4.112.61	11.1	11.0	11.2	
8	3	101.4.117.38	101.4.117.38	31.7	31.4	31.8	
9	3	101.4.112.1	101.4.112.1	30.5	29.5	29.5	
10	3	101.4.113.110	101.4.113.110	29.0	28.5	29.3	
11	3	101.4.116.78	101.4.116.78	31.1	30.6	30.6	
12	3	210.25.189.65	210.25.189.65	30.9	30.1	31.2	
13	3	210.25.187.50	210.25.187.50	31.5	29.6	32.4	

picard.cs.columbia.edu (128.59.23.100) hop 29

10 minutes (11:15:46 - 11:25:46)

5. 重复3、4两步，将大小分别设置为1600、3200字节。在这期间保持Wireshark打开



picard.cs.columbia.edu - PingPlotter Pro

Show your ISP proof of connection problems. Upgrade PingPlotter!

picard.cs.columbia.edu

128.59.23.100

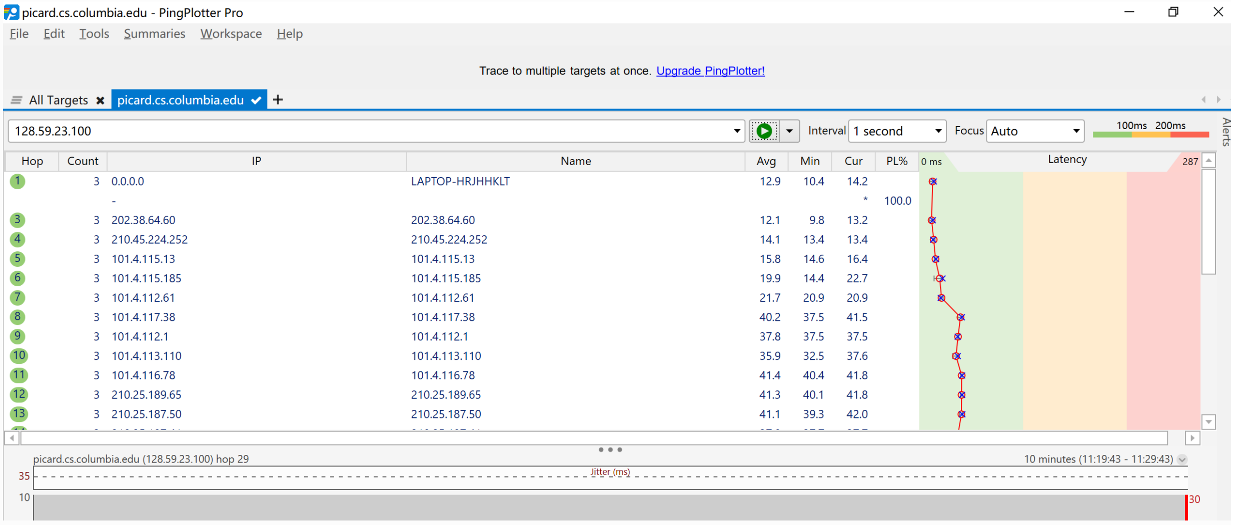
Interval 1 second

Focus Auto

Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	3	0.0.0.0	LAPTOP-HRJHHKLT	6.5	6.0	6.0	
		-				*	100.0
3	3	202.38.64.60	202.38.64.60	3.8	3.5	4.0	
4	3	210.45.224.252	210.45.224.252	4.8	4.7	4.7	
5	3	101.4.115.13	101.4.115.13	34.9	5.8	49.5	
6	3	101.4.115.185	101.4.115.185	6.5	3.9	3.9	
7	3	101.4.112.61	101.4.112.61	17.2	14.3	18.6	
8	3	101.4.117.38	101.4.117.38	30.4	29.6	29.6	
9	3	101.4.112.1	101.4.112.1	29.7	29.5	29.5	
10	3	101.4.113.110	101.4.113.110	32.7	31.8	31.8	
11	3	101.4.116.78	101.4.116.78	31.6	31.2	31.8	
12	3	210.25.189.65	210.25.189.65	30.4	29.0	31.1	
13	3	210.25.187.50	210.25.187.50	30.4	29.5	29.5	

picard.cs.columbia.edu (128.59.23.100) hop 29

10 minutes (11:17:55 - 11:27:55)



picard.cs.columbia.edu - PingPlotter Pro

Trace to multiple targets at once. Upgrade PingPlotter!

picard.cs.columbia.edu

128.59.23.100

Interval 1 second

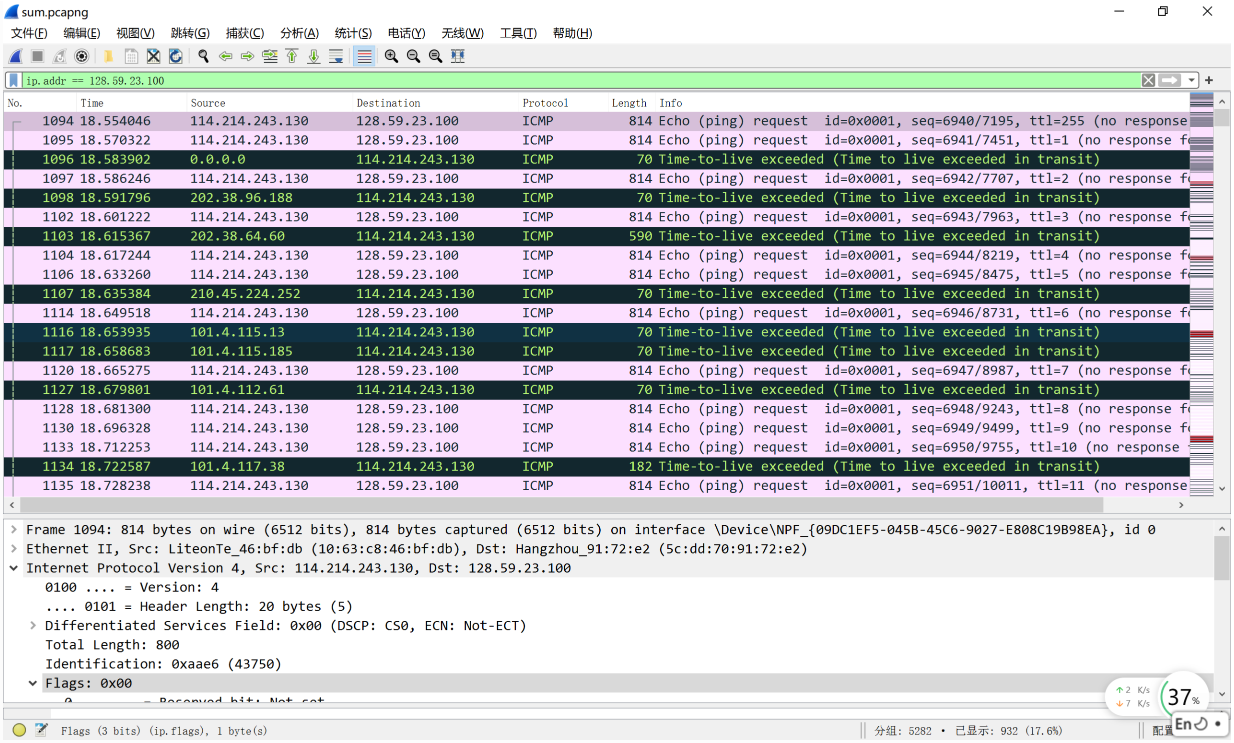
Focus Auto

Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	3	0.0.0.0	LAPTOP-HRJHHKLT	12.9	10.4	14.2	
		-				*	100.0
3	3	202.38.64.60	202.38.64.60	12.1	9.8	13.2	
4	3	210.45.224.252	210.45.224.252	14.1	13.4	13.4	
5	3	101.4.115.13	101.4.115.13	15.8	14.6	16.4	
6	3	101.4.115.185	101.4.115.185	19.9	14.4	22.7	
7	3	101.4.112.61	101.4.112.61	21.7	20.9	20.9	
8	3	101.4.117.38	101.4.117.38	40.2	37.5	41.5	
9	3	101.4.112.1	101.4.112.1	37.8	37.5	37.5	
10	3	101.4.113.110	101.4.113.110	35.9	32.5	37.6	
11	3	101.4.116.78	101.4.116.78	41.4	40.4	41.8	
12	3	210.25.189.65	210.25.189.65	41.3	40.1	41.8	
13	3	210.25.187.50	210.25.187.50	41.1	39.3	42.0	

picard.cs.columbia.edu (128.59.23.100) hop 29

10 minutes (11:19:43 - 11:29:43)

6. 停止捕获，保存trace文件。分析实验结果并回答问题


sum.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.addr == 128.59.23.100

```
No.    Time       Source           Destination      Protocol  Length Info
  1094 18.554046  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6940/7195, ttl=255 (no response
  1095 18.570322  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6941/7451, ttl=1 (no response fo
  1096 18.583902  0.0.0.0          114.214.243.130  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  1097 18.586246  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6942/7707, ttl=2 (no response fo
  1098 18.591796  202.38.96.188    114.214.243.130  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  1102 18.601222  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6943/7963, ttl=3 (no response fo
  1103 18.615367  202.38.64.60     114.214.243.130  ICMP      590 Time-to-live exceeded (Time to live exceeded in transit)
  1104 18.617244  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6944/8219, ttl=4 (no response fo
  1106 18.633260  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6945/8475, ttl=5 (no response fo
  1107 18.635384  210.45.224.252   114.214.243.130  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  1114 18.649518  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6946/8731, ttl=6 (no response fo
  1116 18.653935  101.4.115.13     114.214.243.130  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  1117 18.658683  101.4.115.185    114.214.243.130  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  1120 18.665275  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6947/8987, ttl=7 (no response fo
  1127 18.679801  101.4.112.61     114.214.243.130  ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  1128 18.681300  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6948/9243, ttl=8 (no response fo
  1130 18.696328  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6949/9499, ttl=9 (no response fo
  1133 18.712253  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6950/9755, ttl=10 (no response
  1134 18.722587  101.4.117.38     114.214.243.130  ICMP      182 Time-to-live exceeded (Time to live exceeded in transit)
  1135 18.728238  114.214.243.130  128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6951/10011, ttl=11 (no response
```

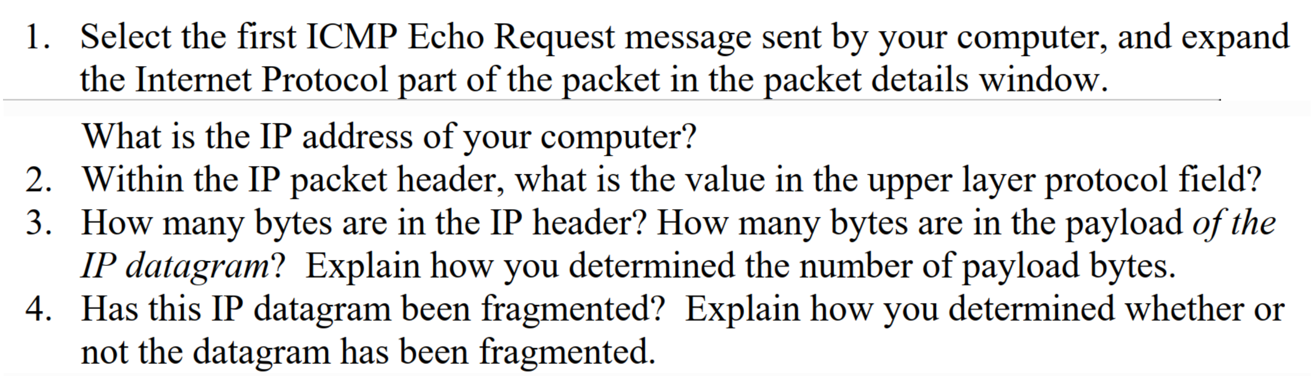
```
> Frame 1094: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits) on interface \Device\NPF_{09DC1EF5-045B-45C6-9027-E808C19B98EA}, id 0
> Ethernet II, Src: LiteonTe_46:bf:db (10:63:c8:46:bf:db), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
v Internet Protocol Version 4, Src: 114.214.243.130, 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: 0xaae6 (43750)
  v Flags: 0x00
      0... .... = Reserved bit: Not set
```

Flags (3 bits) (ip.flags), 1 byte(s)   分组: 5282 • 已显示: 932 (17.6%)   配置

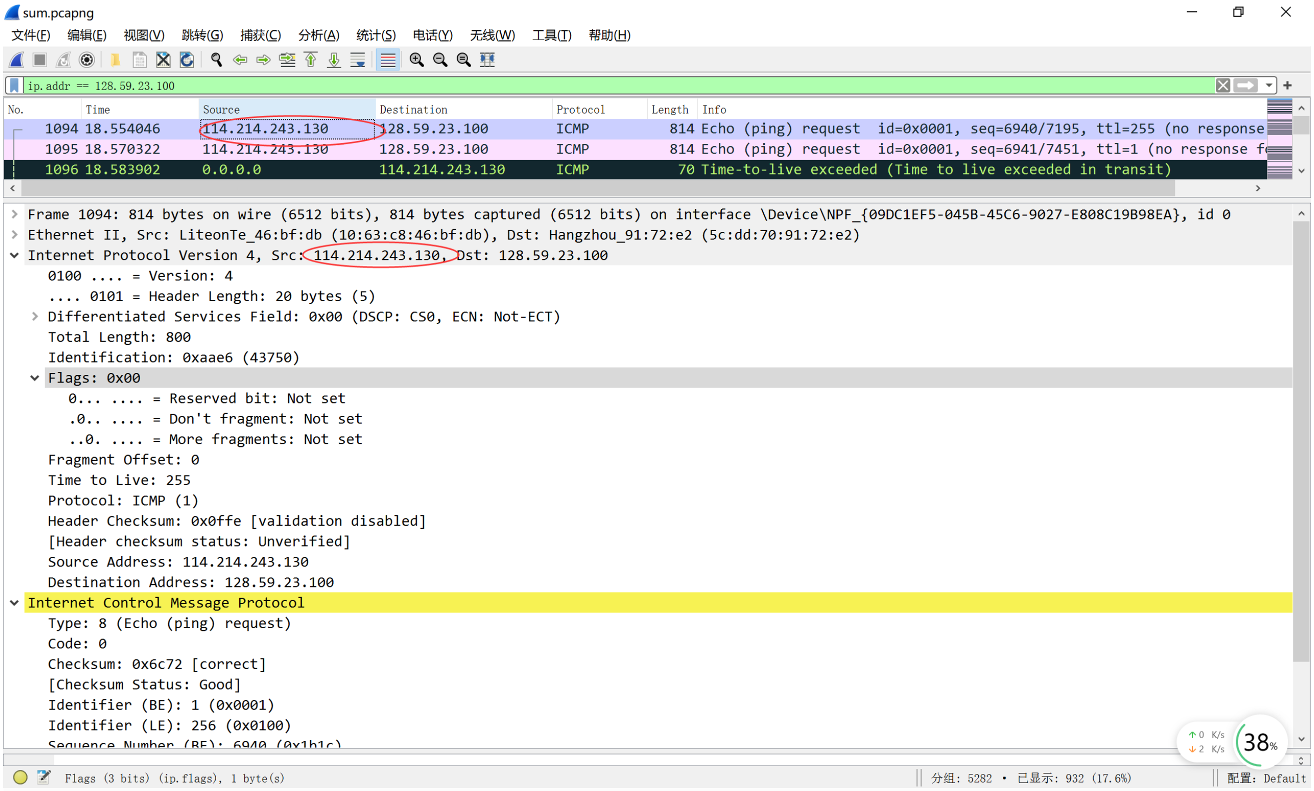
五、结果分析与回答问题

- PingPlotter通过ICMP协议发送连续的、TTL逐渐增大的ICMP报文，以此来得到位于源主机和目的主机之间的路由器数量和标识
- 有些路由出于安全方面的考虑可能不会回应ICMP message (type 11 – TTL-exceeded) ，而TTL会继续增加获取下一个路由的回复
- 先以800字节对应的结果进行分析

A look at the captured trace



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?
2. Within the IP packet header, what is the value in the upper layer protocol field?
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.
4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

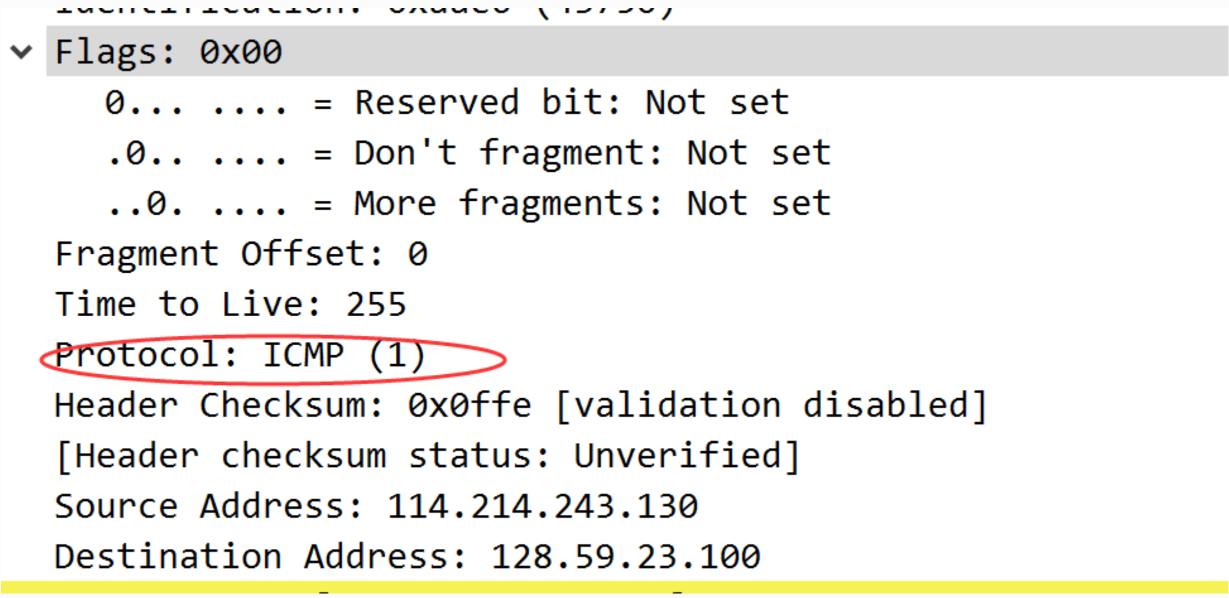

sum.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
ip.addr == 128.59.23.100

No.    Time        Source            Destination       Protocol   Length  Info
  1094 18.554046   114.214.243.130   128.59.23.100     ICMP         814 Echo (ping) request  id=0x0001, seq=6940/7195, ttl=255 (no response
  1095 18.570322   114.214.243.130   128.59.23.100     ICMP         814 Echo (ping) request  id=0x0001, seq=6941/7451, ttl=1 (no response f
  1096 18.583902   0.0.0.0           114.214.243.130   ICMP          70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
> Frame 1094: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits) on interface \Device\NPF_{09DC1EF5-045B-45C6-9027-E808C19B98EA}, id 0
> Ethernet II, Src: LiteonTe_46:bf:db (10:63:c8:46:bf:db), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
v Internet Protocol Version 4, Src: 114.214.243.130, 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: 0xaae6 (43750)
  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: 0x0ffe [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x6c72 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 6940 (0x1b1c)

Flags (3 bits) (ip.flags), 1 byte(s)        分组: 5282 · 已显示: 932 (17.6%)        配置: Default
```

1. 我的IP地址：114.214.243.130

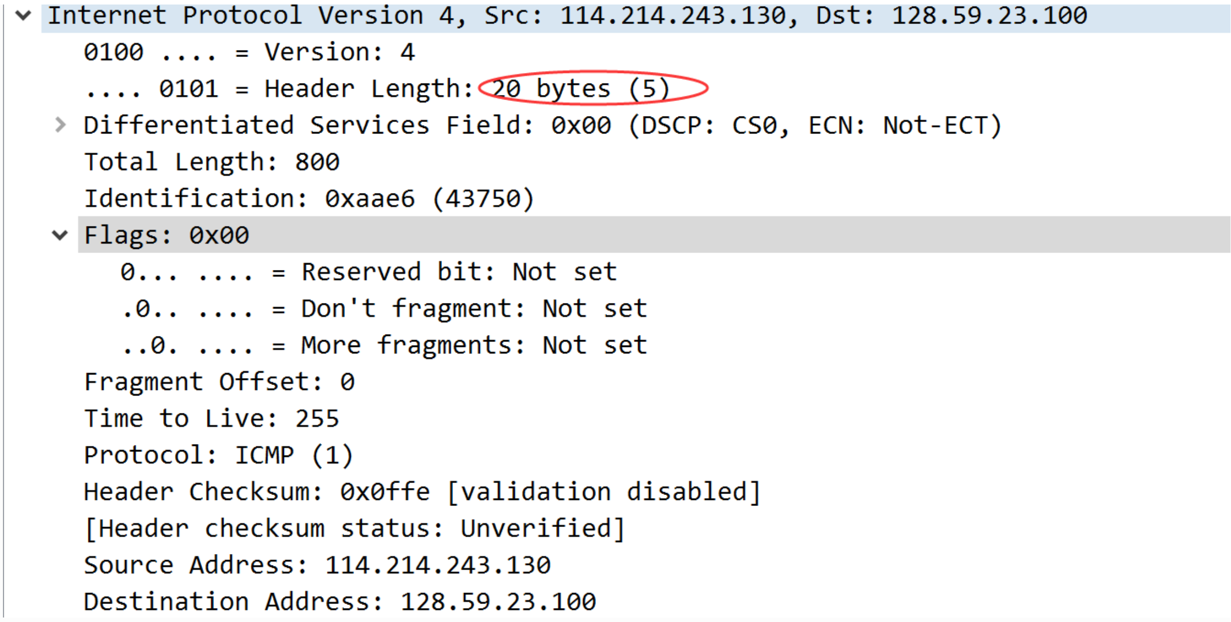
2.



```
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: 0x0ffe [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 114.214.243.130
  Destination Address: 128.59.23.100
```

上层协议为ICMP，值为1

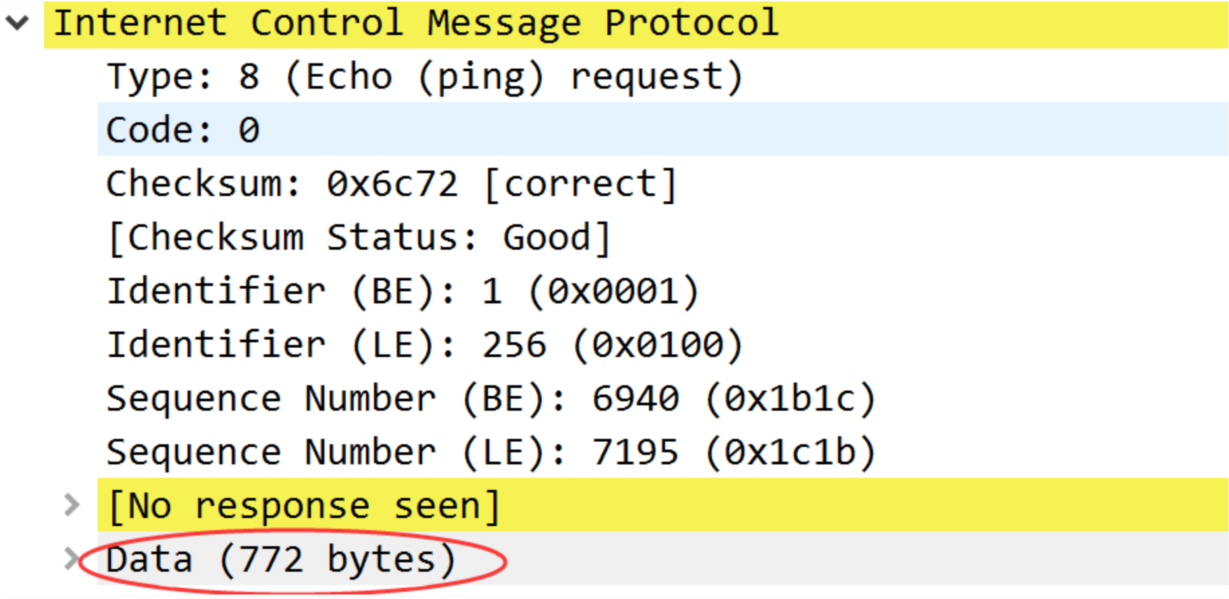
3.



```
v Internet Protocol Version 4, Src: 114.214.243.130, 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: 0xaae6 (43750)
  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: 0x0ffe [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
```

IP头部为20字节

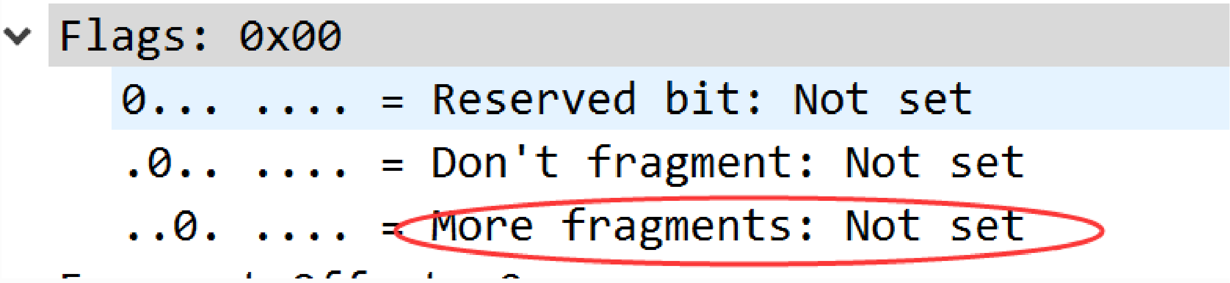
IP数据报的总长度为800字节，故IP数据报的有效荷载为800-20=780字节（封装了ICMP报文），这也可以从下图中得到验证



```
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x6c72 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 6940 (0x1b1c)
    Sequence Number (LE): 7195 (0x1c1b)
  > [No response seen]
  > Data (772 bytes)
```

可以看到ICMP数据部分为772字节，加上ICMP首部的8字节，总共780字节

4. 没有被分片。



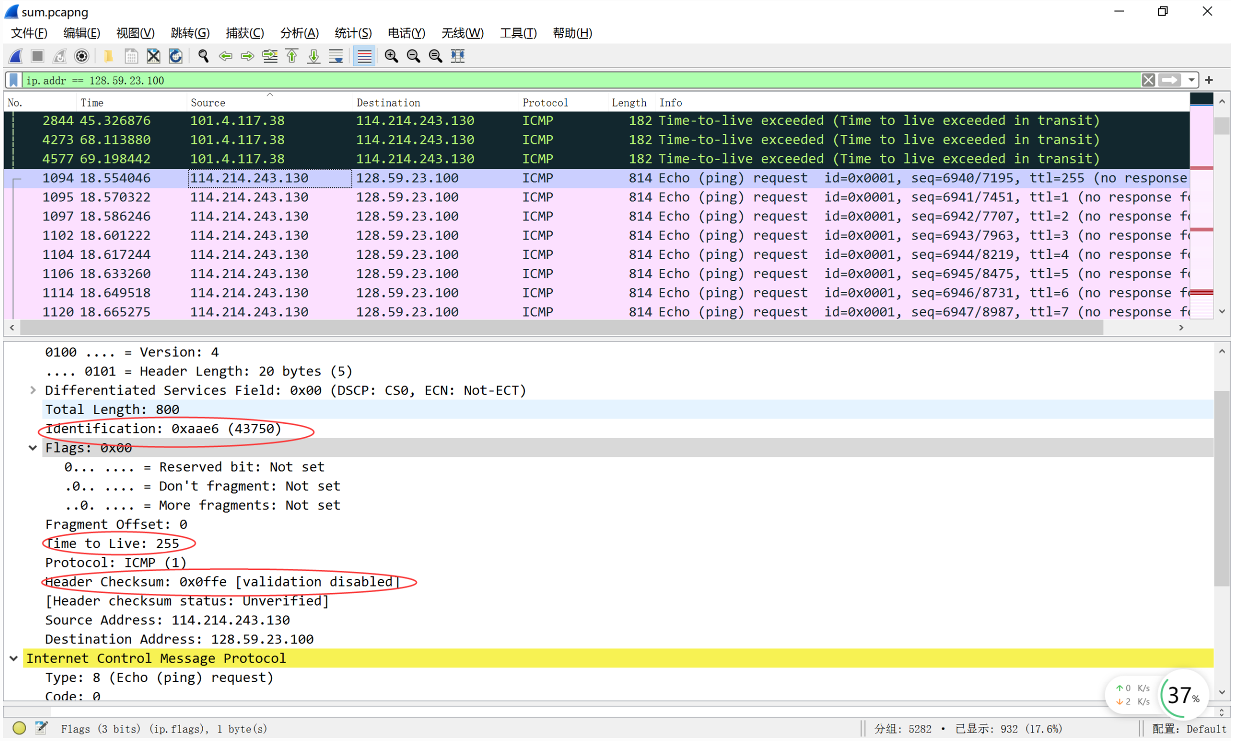
```
v Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
```

可以看到IP首部的标志字段的More fragments位没有被置为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?
6. Which fields stay constant? Which of the fields *must* stay constant? Which fields must change? Why?
7. Describe the pattern you see in the values in the Identification field of the IP datagram

5. IP数据首部的标识（Identification）、寿命（TTL）、首部检验和（Header Checksum）总是会变化。另外IP数据报的数据（Data）里面的ICMP报文的检验和、序号也会变化

下面是前两个ICMP Echo Request message对应的截图

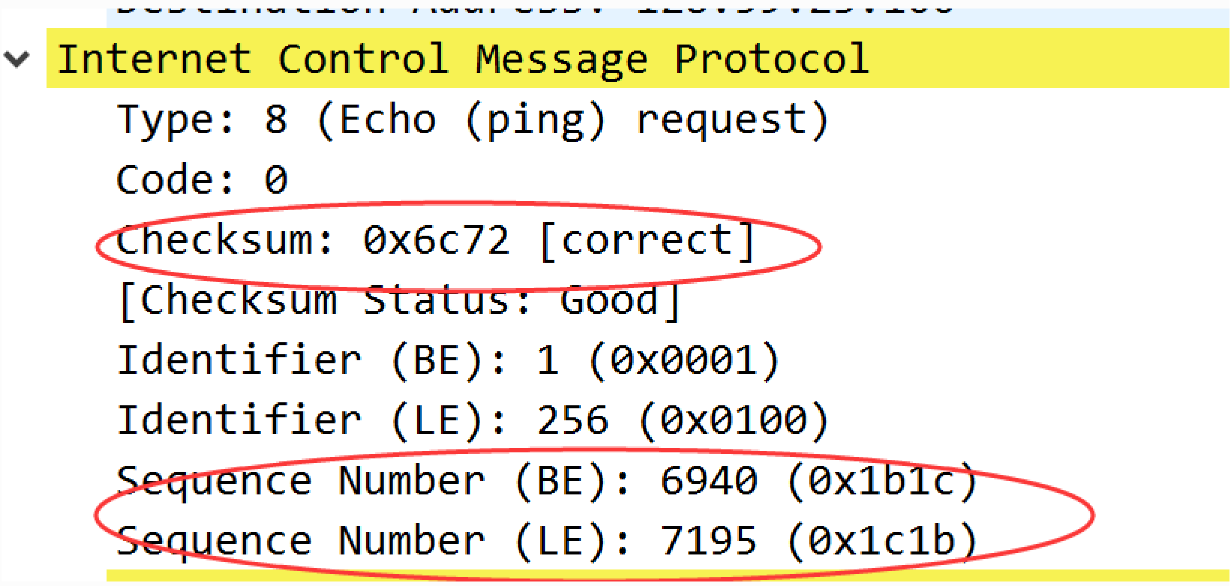


ip.addr == 128.59.23.100

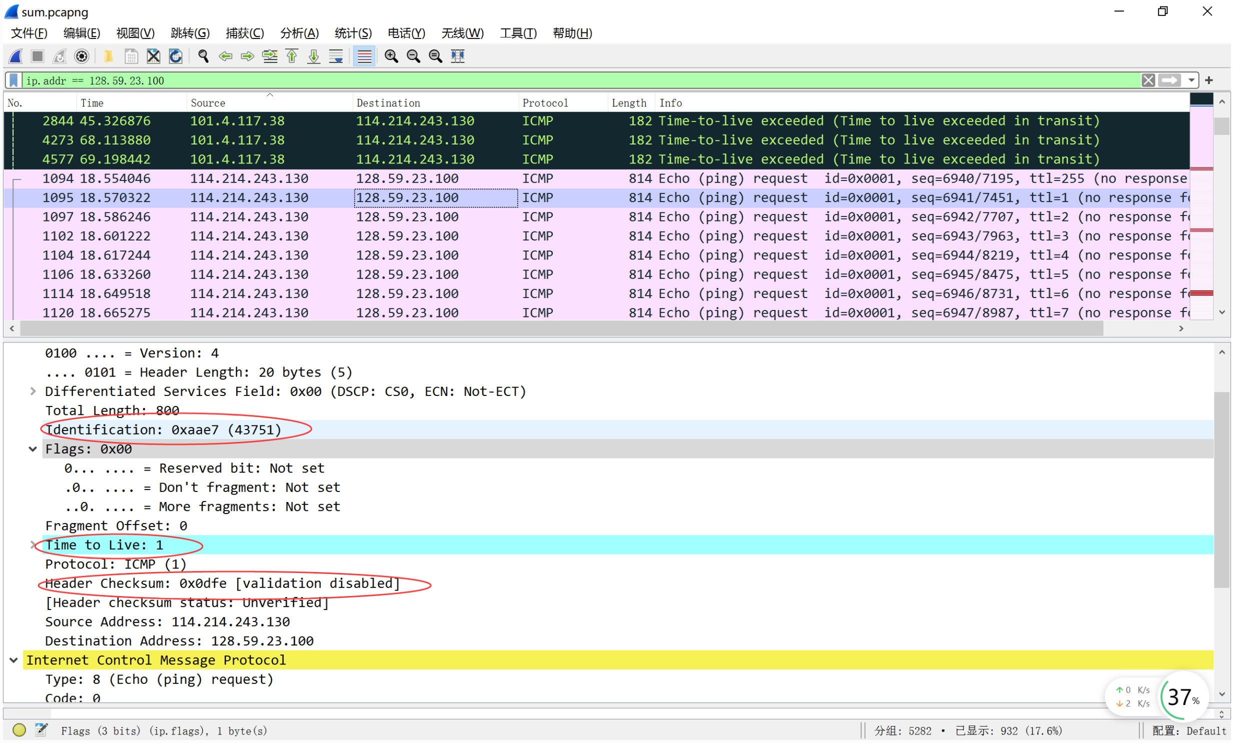
```
No.   Time          Source            Destination      Protocol  Length Info
 2844 45.326876     101.4.117.38      114.214.243.130  ICMP      182 Time-to-live exceeded (Time to live exceeded in transit)
 4273 68.113880     101.4.117.38      114.214.243.130  ICMP      182 Time-to-live exceeded (Time to live exceeded in transit)
 4577 69.198442     101.4.117.38      114.214.243.130  ICMP      182 Time-to-live exceeded (Time to live exceeded in transit)
 1094 18.554046     114.214.243.130   128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6940/7195, ttl=255 (no response
 1095 18.570322     114.214.243.130   128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6941/7451, ttl=1 (no response f
 1097 18.586246     114.214.243.130   128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6942/7707, ttl=2 (no response f
 1102 18.601222     114.214.243.130   128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6943/7963, ttl=3 (no response f
 1104 18.617244     114.214.243.130   128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6944/8219, ttl=4 (no response f
 1106 18.633260     114.214.243.130   128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6945/8475, ttl=5 (no response f
 1114 18.649518     114.214.243.130   128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6946/8731, ttl=6 (no response f
 1120 18.665275     114.214.243.130   128.59.23.100    ICMP      814 Echo (ping) request  id=0x0001, seq=6947/8987, ttl=7 (no response f
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 800
    Identification: 0xaae6 (43750)
  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: 0x0ffe [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

Flags (3 bits) (ip.flags), 1 byte(s) || 分组: 5282 • 已显示: 932 (17.6%) || 配置: Default



```
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x6c72 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 6940 (0x1b1c)
    Sequence Number (LE): 7195 (0x1c1b)
```

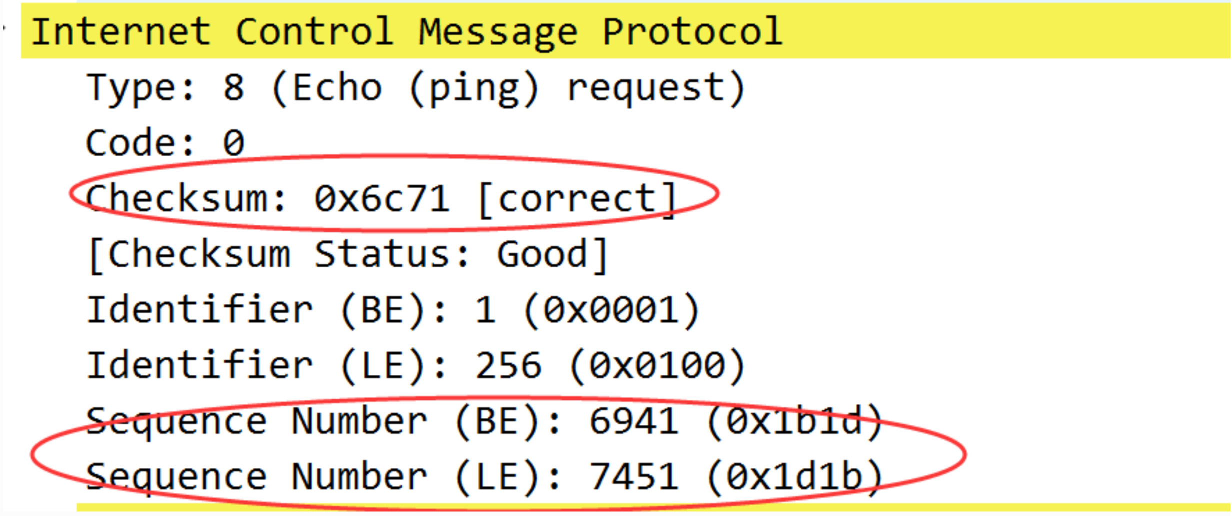

sum.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
0 K/s
2 K/s
37%

```
ip.addr == 128.59.23.100
```

```
No.     Time          Source           Destination      Protocol  Length  Info
   2844 45.326876     101.4.117.38     114.214.243.130  ICMP        182 Time-to-live exceeded (Time to live exceeded in transit)
   4273 68.113880     101.4.117.38     114.214.243.130  ICMP        182 Time-to-live exceeded (Time to live exceeded in transit)
   4577 69.198442     101.4.117.38     114.214.243.130  ICMP        182 Time-to-live exceeded (Time to live exceeded in transit)
   1094 18.554046     114.214.243.130  128.59.23.100    ICMP        814 Echo (ping) request  id=0x0001, seq=6940/7195, ttl=255 (no response
   1095 18.570322     114.214.243.130  128.59.23.100    ICMP        814 Echo (ping) request  id=0x0001, seq=6941/7451, ttl=1 (no response fo
   1097 18.586246     114.214.243.130  128.59.23.100    ICMP        814 Echo (ping) request  id=0x0001, seq=6942/7707, ttl=2 (no response fo
   1102 18.601222     114.214.243.130  128.59.23.100    ICMP        814 Echo (ping) request  id=0x0001, seq=6943/7963, ttl=3 (no response fo
   1104 18.617244     114.214.243.130  128.59.23.100    ICMP        814 Echo (ping) request  id=0x0001, seq=6944/8219, ttl=4 (no response fo
   1106 18.633260     114.214.243.130  128.59.23.100    ICMP        814 Echo (ping) request  id=0x0001, seq=6945/8475, ttl=5 (no response fo
   1114 18.649518     114.214.243.130  128.59.23.100    ICMP        814 Echo (ping) request  id=0x0001, seq=6946/8731, ttl=6 (no response fo
   1120 18.665275     114.214.243.130  128.59.23.100    ICMP        814 Echo (ping) request  id=0x0001, seq=6947/8987, ttl=7 (no response fo
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 800
    Identification: 0xaae7 (43751)
  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: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0dfe [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

```
Flags (3 bits) (ip.flags), 1 byte(s)        分组: 5282 • 已显示: 932 (17.6%)        配置: Default
```



```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x6c71 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 6941 (0x1b1d)
    Sequence Number (LE): 7451 (0x1d1b)
```

其中BE、LE是考虑到Windows系统和Linux系统发出的ping报文的字节顺序不同（Windows为LE：little-endian byte order，LInux为BE：big-endian byte order），Wireshark将它们都显示出来

6. - stay constant：
     - Total Length：共有三种不同的数据报长度
     - Flags：根据是否分片可能会有变化
     - Fragment offset：若不分片，则没有偏移；若分片，则除了第一片之外都有偏移
     - Source Address：源地址一直是114.214.243.130
     - Destination Address：目标地址一直是128.59.23.100
     - 以及下面must stay constant的部分
   - must stay constant：
     - Version：都是IPv4

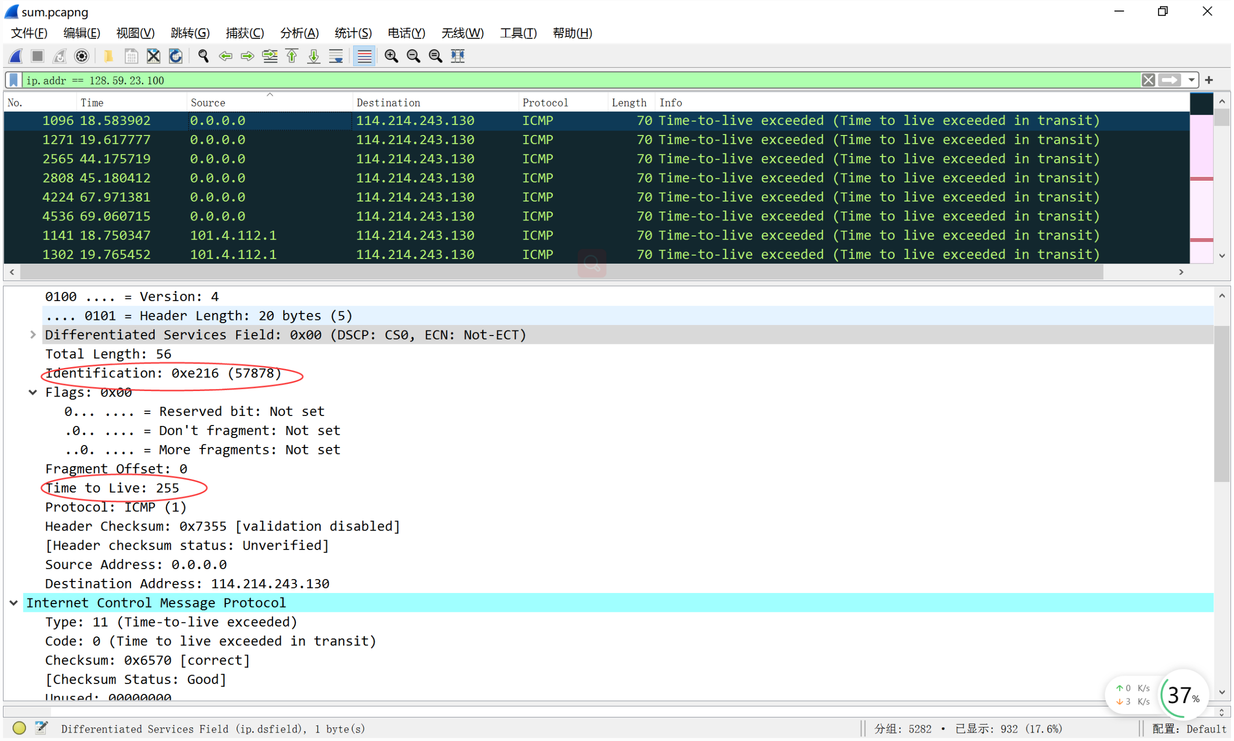
        - Protocol：都是ICMP
        - Header length：都是20字节，没有选项部分
        - Differentiated Services Field：都是ICMP类型
    - must change
        - TTL：每经过一个路由器TTL应减一
        - Identification：IP数据报之间的ID不同
        - Header Checksum：每次Header不同导致检验和也不同
        - Data：每次封装的ICMP报文的序列号、检验和会发生变化

7. 每个Identification都会比上一个增加1，用来区分每个IP数据报和处理IP分片，这从第5问的图中可以看出

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?
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?

8.



ip.addr == 128.59.23.100

```
No.     Time           Source        Destination      Protocol  Length Info
   1096 18.583902      0.0.0.0       114.214.243.130  ICMP          70 Time-to-live exceeded (Time to live exceeded in transit)
   1271 19.617777      0.0.0.0       114.214.243.130  ICMP          70 Time-to-live exceeded (Time to live exceeded in transit)
   2565 44.175719      0.0.0.0       114.214.243.130  ICMP          70 Time-to-live exceeded (Time to live exceeded in transit)
   2808 45.180412      0.0.0.0       114.214.243.130  ICMP          70 Time-to-live exceeded (Time to live exceeded in transit)
   4224 67.971381      0.0.0.0       114.214.243.130  ICMP          70 Time-to-live exceeded (Time to live exceeded in transit)
   4536 69.060715      0.0.0.0       114.214.243.130  ICMP          70 Time-to-live exceeded (Time to live exceeded in transit)
   1141 18.750347      101.4.112.1   114.214.243.130  ICMP          70 Time-to-live exceeded (Time to live exceeded in transit)
   1302 19.765452      101.4.112.1   114.214.243.130  ICMP          70 Time-to-live exceeded (Time to live exceeded in transit)
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xe216 (57878)
  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: 0x7355 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 0.0.0.0
    Destination Address: 114.214.243.130
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x6570 [correct]
    [Checksum Status: Good]
    Unused: 00000000
```

Differentiated Services Field (ip.dsfield), 1 byte(s) || 分组: 5282 • 已显示: 932 (17.6%) || 配置: Default

Identification为57878，TTL为255

9. Identification会发生变化，这些IP包彼此之间应该有不同的标识，相互独立

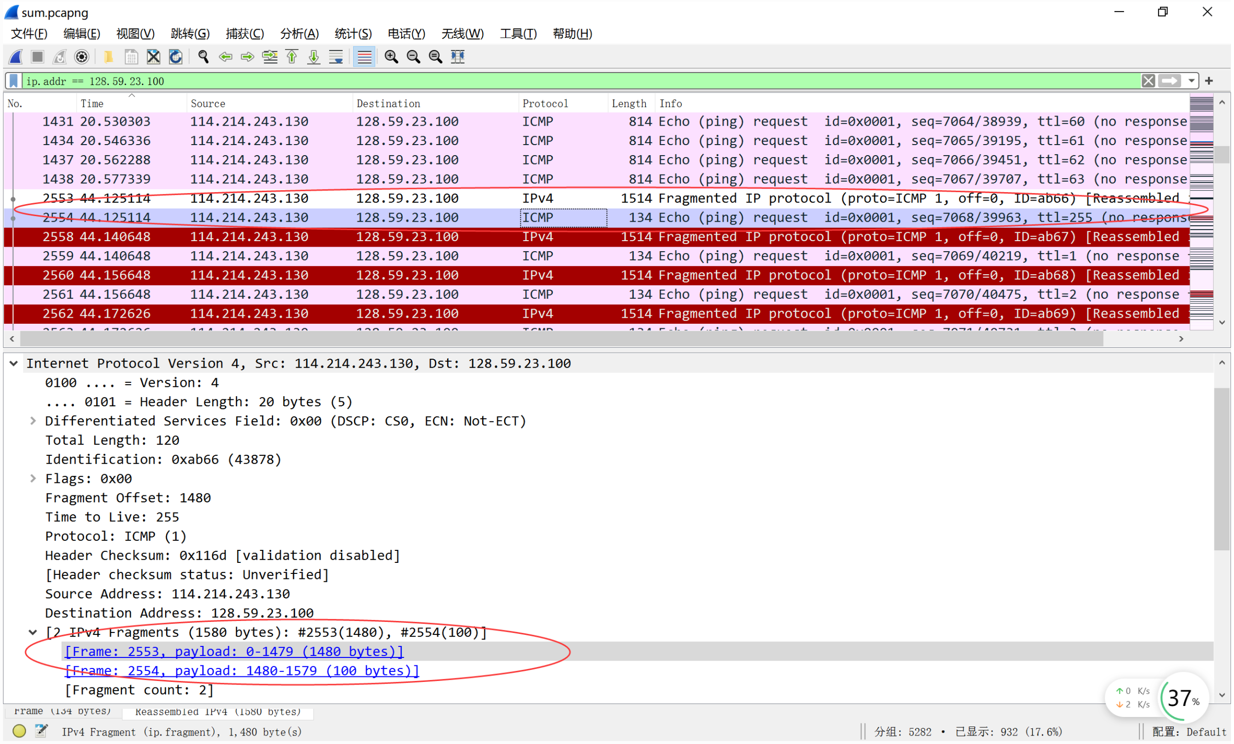
TTL不变，因为在实验的这段时间内，第一跳路由是没有发生变化的，TTL初始值为255，默认不会变化

Fragmentation

这一部分对应改为**1600字节**

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 *ip-ethereal-trace-1*packet trace. If your computer has an Ethernet interface, a packet size of 2000 *should* cause fragmentation.[3]]
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?
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?
13. What fields change in the IP header between the first and second fragment?

10. 它被分片为2个fragments。第一个数据报是协议为IPv4的IP破碎片，第二个数据报是协议为ICMP的剩余部分。在第二个数据报中可以看到统计结果



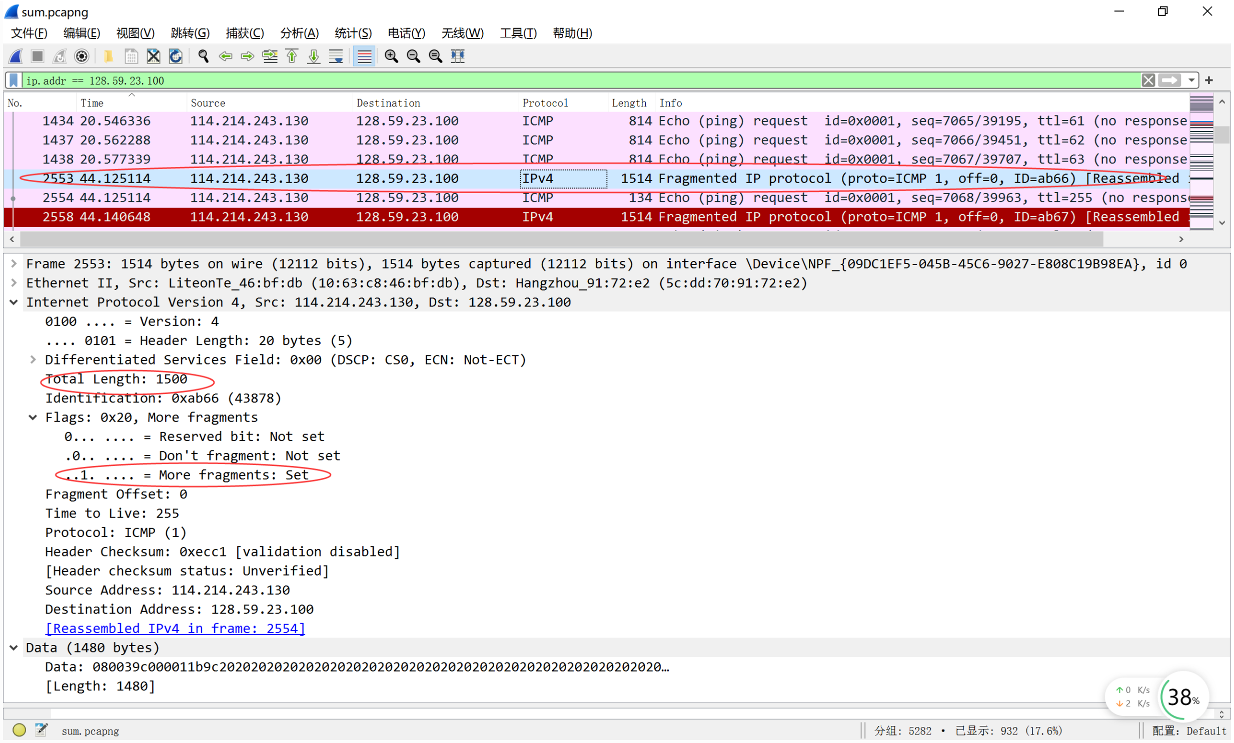
```
ip.addr == 128.59.23.100
```

```
No.   Time       Source           Destination    Protocol  Length Info
 1431 20.530303  114.214.243.130  128.59.23.100  ICMP       814 Echo (ping) request  id=0x0001, seq=7064/38939, ttl=60 (no response
 1434 20.546336  114.214.243.130  128.59.23.100  ICMP       814 Echo (ping) request  id=0x0001, seq=7065/39195, ttl=61 (no response
 1437 20.562288  114.214.243.130  128.59.23.100  ICMP       814 Echo (ping) request  id=0x0001, seq=7066/39451, ttl=62 (no response
 1438 20.577339  114.214.243.130  128.59.23.100  ICMP       814 Echo (ping) request  id=0x0001, seq=7067/39707, ttl=63 (no response
 2553 44.125114  114.214.243.130  128.59.23.100  IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ab66) [Reassembled
 2554 44.125114  114.214.243.130  128.59.23.100  ICMP       134 Echo (ping) request  id=0x0001, seq=7068/39963, ttl=255 (no response
 2558 44.140648  114.214.243.130  128.59.23.100  IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ab67) [Reassembled
 2559 44.140648  114.214.243.130  128.59.23.100  ICMP       134 Echo (ping) request  id=0x0001, seq=7069/40219, ttl=1 (no response
 2560 44.156648  114.214.243.130  128.59.23.100  IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ab68) [Reassembled
 2561 44.156648  114.214.243.130  128.59.23.100  ICMP       134 Echo (ping) request  id=0x0001, seq=7070/40475, ttl=2 (no response
 2562 44.172626  114.214.243.130  128.59.23.100  IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ab69) [Reassembled
```

```
v Internet Protocol Version 4, Src: 114.214.243.130, 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: 120
    Identification: 0xab66 (43878)
  > Flags: 0x00
    Fragment Offset: 1480
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x116d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
  v [2 IPv4 Fragments (1580 bytes): #2553(1480), #2554(100)]
      [Frame: 2553, payload: 0-1479 (1480 bytes)]
      [Frame: 2554, payload: 1480-1579 (100 bytes)]
      [Fragment count: 2]
```

```
Frame (134 bytes)   Reassembled IPv4 (1580 bytes)
IPv4 Fragment (ip.fragment), 1,480 byte(s)    分组: 5282 • 已显示: 932 (17.6%)    配置: Default
```

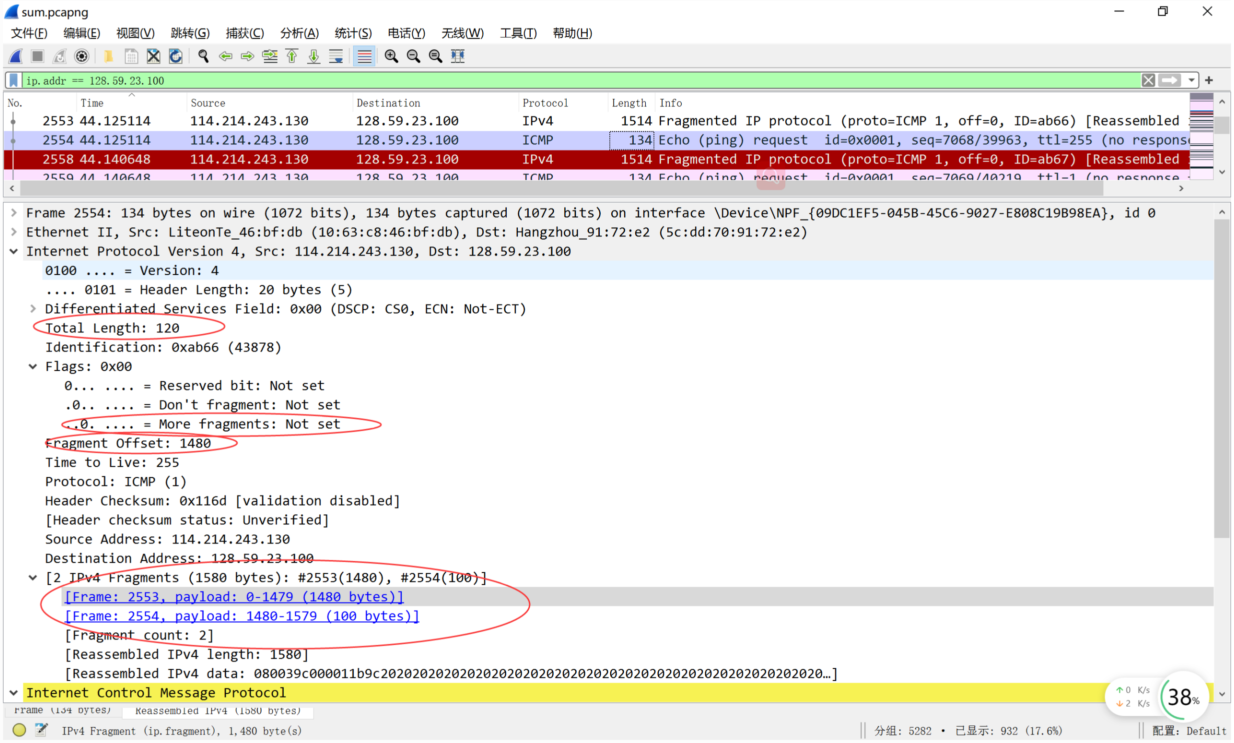
11.



sum.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.addr == 128.59.23.100

```
No.   Time       Source           Destination     Protocol  Length Info
 1434 20.546336  114.214.243.130  128.59.23.100   ICMP       814 Echo (ping) request  id=0x0001, seq=7065/39195, ttl=61 (no response
 1437 20.562288  114.214.243.130  128.59.23.100   ICMP       814 Echo (ping) request  id=0x0001, seq=7066/39451, ttl=62 (no response
 1438 20.577339  114.214.243.130  128.59.23.100   ICMP       814 Echo (ping) request  id=0x0001, seq=7067/39707, ttl=63 (no response
 2553 44.125114  114.214.243.130  128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ab66) [Reassembled
 2554 44.125114  114.214.243.130  128.59.23.100   ICMP       134 Echo (ping) request  id=0x0001, seq=7068/39963, ttl=255 (no respons
 2558 44.140648  114.214.243.130  128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ab67) [Reassembled

> Frame 2553: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{09DC1EF5-045B-45C6-9027-E808C19B98EA}, id 0
> Ethernet II, Src: LiteonTe_46:bf:db (10:63:c8:46:bf:db), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
v Internet Protocol Version 4, Src: 114.214.243.130, 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: 0xab66 (43878)
  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: 0xecc1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 2554]
v Data (1480 bytes)
    Data: 080039c000011b9c20202020202020202020202020202020202020202020202020202020…
    [Length: 1480]

sum.pcapng          分组: 5282 · 已显示: 932 (17.6%)          配置: Default
```

由上图可知More fragments被置为1表示数据报已经被分片。Fragment Offset为0表示这是第一片。这个IP数据报的长度为1500字节（20字节的IP首部加上1480字节的数据）

12. 

sum.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.addr == 128.59.23.100

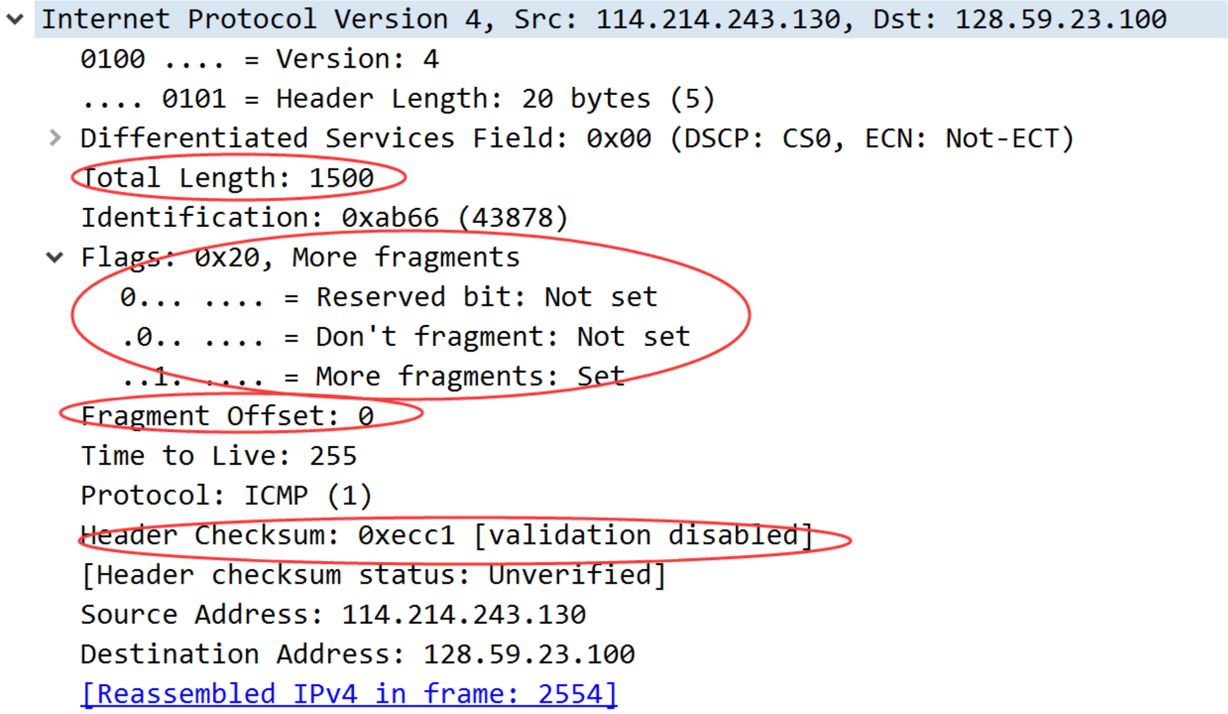
```
No.   Time       Source           Destination     Protocol  Length Info
 2553 44.125114  114.214.243.130  128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ab66) [Reassembled
 2554 44.125114  114.214.243.130  128.59.23.100   ICMP       134 Echo (ping) request  id=0x0001, seq=7068/39963, ttl=255 (no respons
 2558 44.140648  114.214.243.130  128.59.23.100   IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=ab67) [Reassembled
 2559 44.140648  114.214.243.130  128.59.23.100   ICMP       134 Echo (ping) request  id=0x0001, seq=7069/40219, ttl=1 (no response

> Frame 2554: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{09DC1EF5-045B-45C6-9027-E808C19B98EA}, id 0
> Ethernet II, Src: LiteonTe_46:bf:db (10:63:c8:46:bf:db), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
v Internet Protocol Version 4, Src: 114.214.243.130, 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: 120
    Identification: 0xab66 (43878)
  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: 0x116d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
  v [2 IPv4 Fragments (1580 bytes): #2553(1480), #2554(100)]
      [Frame: 2553, payload: 0-1479 (1480 bytes)]
      [Frame: 2554, payload: 1480-1579 (100 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 1580]
      [Reassembled IPv4 data: 080039c000011b9c2020202020202020202020202020202020202020202020202020…]
v Internet Control Message Protocol
 Frame (134 bytes)   Reassembled IPv4 (1580 bytes)

IPv4 Fragment (ip.fragment), 1,480 byte(s)          分组: 5282 · 已显示: 932 (17.6%)          配置: Default
```

Fragment Offset不为0表示这不是第一片

没有更多的分片了，因为More fragments被置为0，且根据偏移量和长度也可以判断。第一片的有效数据为1480字节，故这一片偏移量为1480字节。这一片总长度为120字节，减去首部长度20字节，有效数据为100字节。故总的有效数据位1480+100=1580字节，加上首部20字节，总长度为1600字节，这正好对应了之前的设置，故没有更多的片了

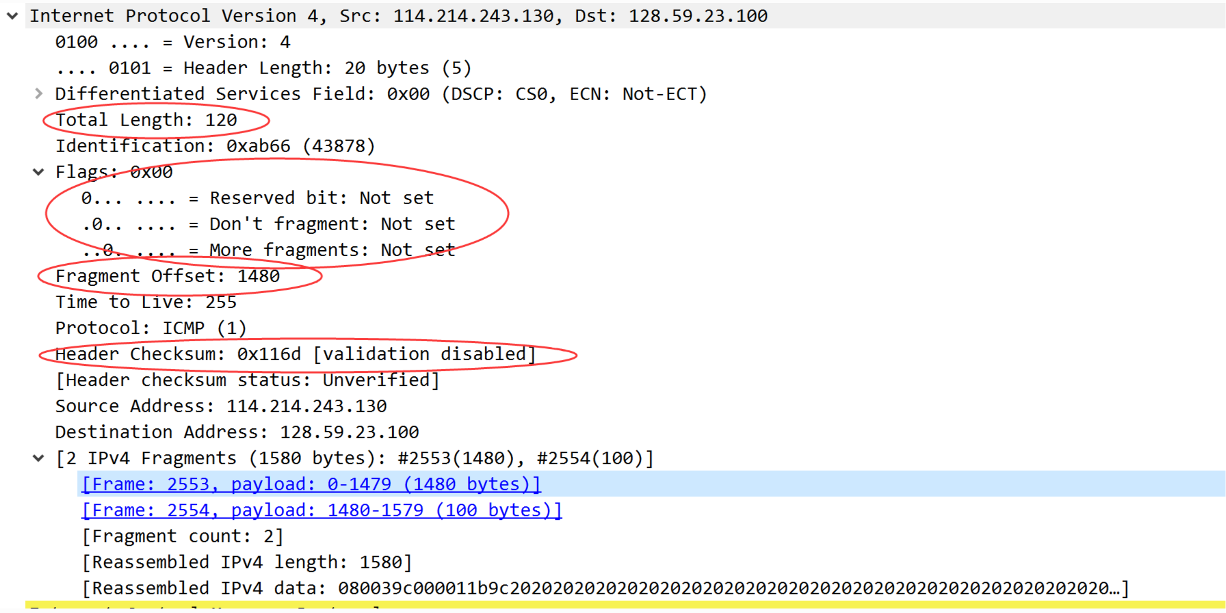
13. 变化：Total Length、Flags、Fragment offset、Header Checksum。具体如下图

第一片



```
⌄ Internet Protocol Version 4, Src: 114.214.243.130, 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: 0xab66 (43878)
  ⌄ 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: 0xecc1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 2554]
```

第二片

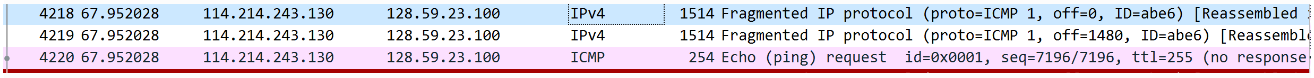


```
⌄ Internet Protocol Version 4, Src: 114.214.243.130, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 120
    Identification: 0xab66 (43878)
  ⌄ Flags: 0x00
      0... .... = 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: 0x116d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
  ⌄ [2 IPv4 Fragments (1580 bytes): #2553(1480), #2554(100)]
      [Frame: 2553, payload: 0-1479 (1480 bytes)]
      [Frame: 2554, payload: 1480-1579 (100 bytes)]
      [Fragment count: 2]
      [Reassembled IPv4 length: 1580]
      [Reassembled IPv4 data: 080039c000011b9c202020202020202020202020202020202020202020202020…]
```

这一部分对应改为**3200字节**

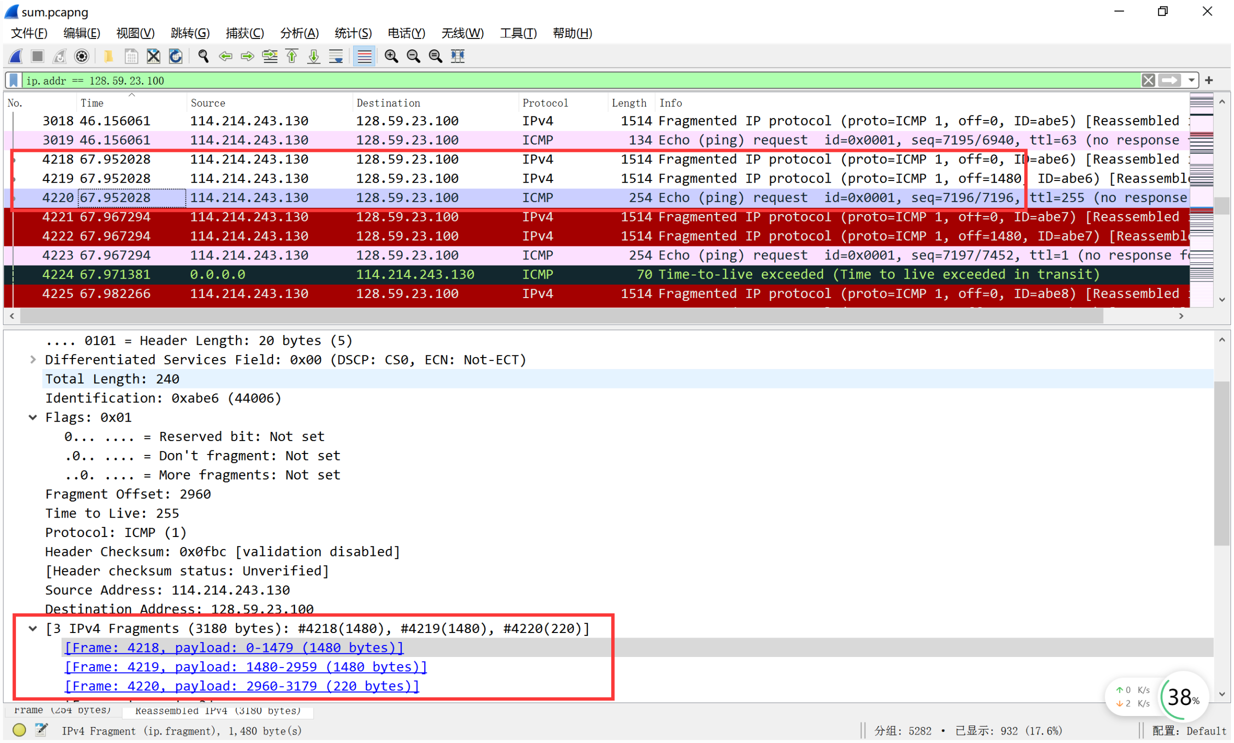
Now find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 3500.

14. How many fragments were created from the original datagram?
15. What fields change in the IP header among the fragments?



```
4218 67.952028   114.214.243.130   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=abe6) [Reassembled
4219 67.952028   114.214.243.130   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=abe6) [Reassembl
4220 67.952028   114.214.243.130   128.59.23.100   ICMP    254 Echo (ping) request  id=0x0001, seq=7196/7196, ttl=255 (no response
```

14. 3个

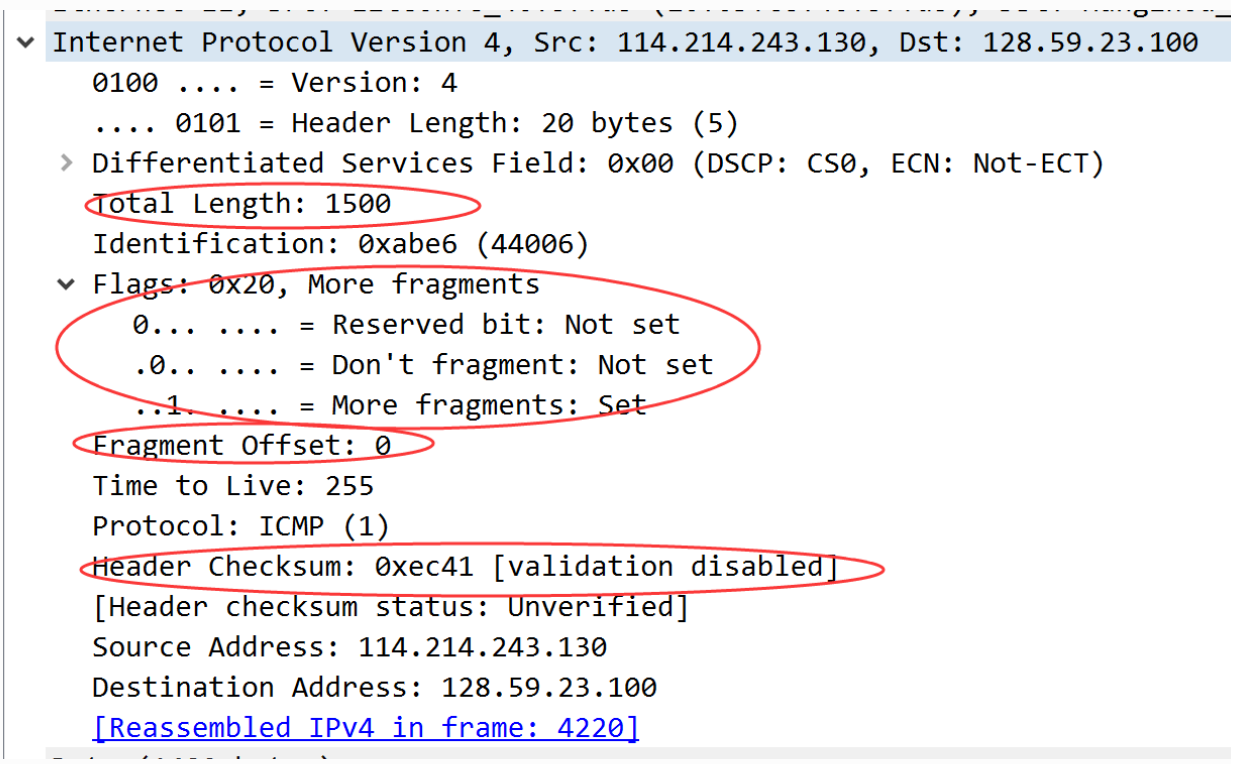


sum.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
ip.addr == 128.59.23.100

No.   Time       Source           Destination      Protocol  Length Info
 3018 46.156061  114.214.243.130  128.59.23.100    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=abe5) [Reassembled
 3019 46.156061  114.214.243.130  128.59.23.100    ICMP       134 Echo (ping) request  id=0x0001, seq=7195/6940, ttl=63 (no response
 4218 67.952028  114.214.243.130  128.59.23.100    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=abe6) [Reassembled
 4219 67.952028  114.214.243.130  128.59.23.100    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=abe6) [Reassembl
 4220 67.952028  114.214.243.130  128.59.23.100    ICMP       254 Echo (ping) request  id=0x0001, seq=7196/7196, ttl=255 (no response
 4221 67.967294  114.214.243.130  128.59.23.100    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=abe7) [Reassembled
 4222 67.967294  114.214.243.130  128.59.23.100    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=abe7) [Reassembl
 4223 67.967294  114.214.243.130  128.59.23.100    ICMP       254 Echo (ping) request  id=0x0001, seq=7197/7452, ttl=1 (no response f
 4224 67.971381  0.0.0.0          114.214.243.130  ICMP        70 Time-to-live exceeded (Time to live exceeded in transit)
 4225 67.982266  114.214.243.130  128.59.23.100    IPv4      1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=abe8) [Reassembled

    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 240
    Identification: 0xabe6 (44006)
  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: 0x0fbc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
  v [3 IPv4 Fragments (3180 bytes): #4218(1480), #4219(1480), #4220(220)]
      [Frame: 4218, payload: 0-1479 (1480 bytes)]
      [Frame: 4219, payload: 1480-2959 (1480 bytes)]
      [Frame: 4220, payload: 2960-3179 (220 bytes)]

Frame (254 bytes)   Reassembled IPv4 (3180 bytes)
IPv4 Fragment (ip.fragment), 1,480 byte(s)        分组: 5282 • 已显示: 932 (17.6%)        配置: Default
```

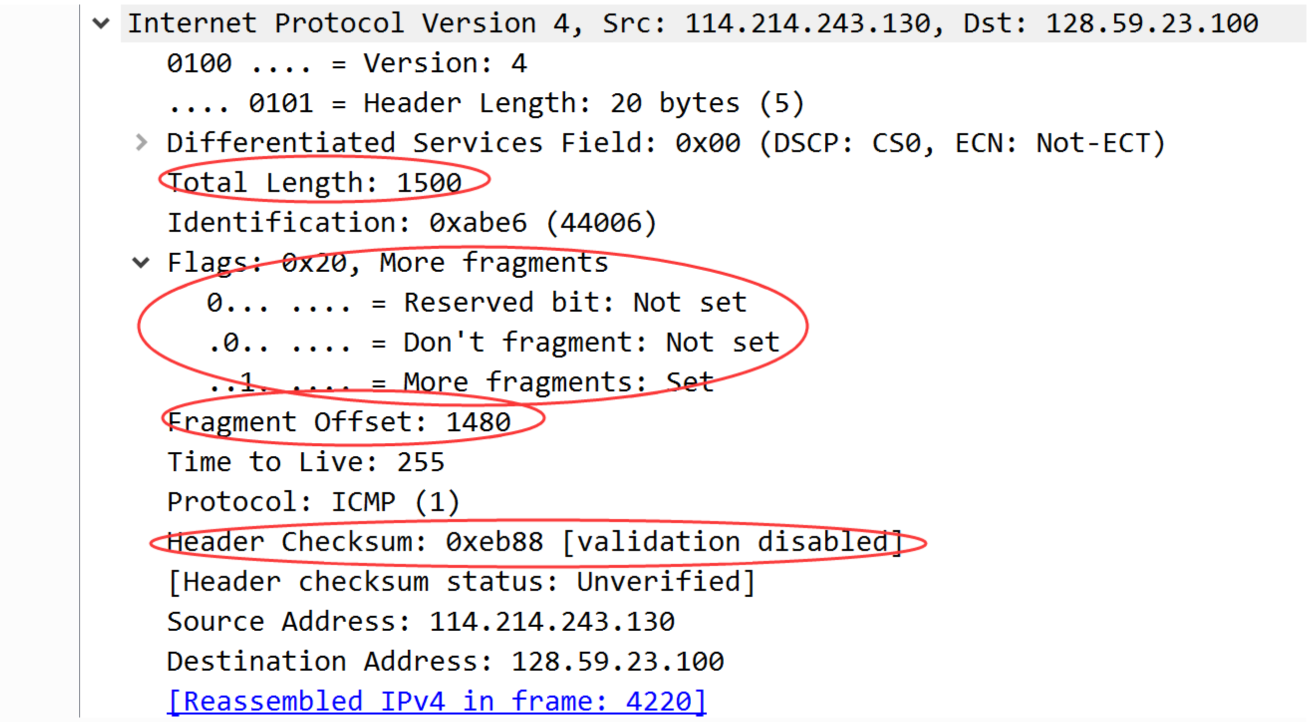
15. 变化：Total Length、Flags、Fragment offset、Header Checksum。具体如下图

第一片



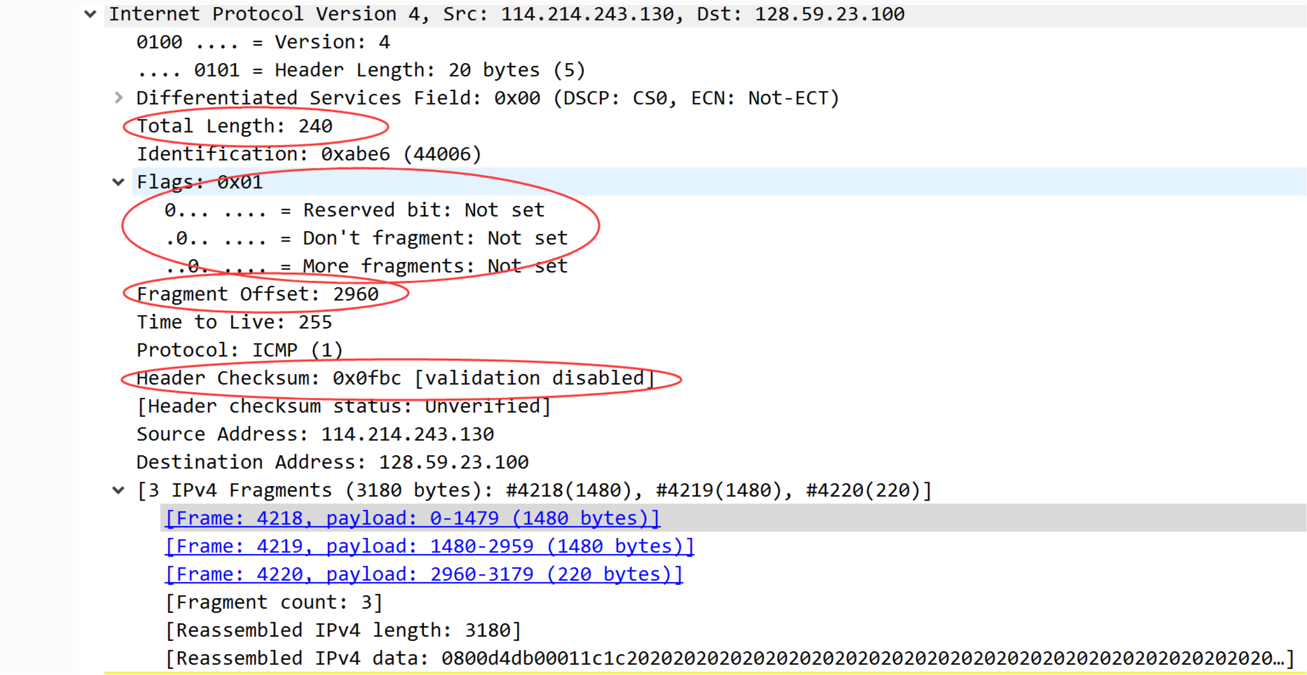
```
v Internet Protocol Version 4, Src: 114.214.243.130, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xabe6 (44006)
  v Flags: 0x20, More fragments
      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: 0xec41 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 4220]
```

第二片



```
Internet Protocol Version 4, Src: 114.214.243.130, 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: 0xabe6 (44006)
  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: 0xeb88 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
    [Reassembled IPv4 in frame: 4220]
```

第三片



```
Internet Protocol Version 4, Src: 114.214.243.130, 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: 0xabe6 (44006)
  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: 0x0fbc [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.243.130
    Destination Address: 128.59.23.100
  v [3 IPv4 Fragments (3180 bytes): #4218(1480), #4219(1480), #4220(220)]
        [Frame: 4218, payload: 0-1479 (1480 bytes)]
        [Frame: 4219, payload: 1480-2959 (1480 bytes)]
        [Frame: 4220, payload: 2960-3179 (220 bytes)]
        [Fragment count: 3]
        [Reassembled IPv4 length: 3180]
        [Reassembled IPv4 data: 0800d4db00011c1c202020202020202020202020202020202020202020202020202020202020…]
```