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：PB17081504

姓　　名：廖洲洲

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

2019年12月4日

一、 实验目的

1、捕获观察并分析IP数据报的结构。

2、掌握PingPlotter的使用方法。

二、 实验原理

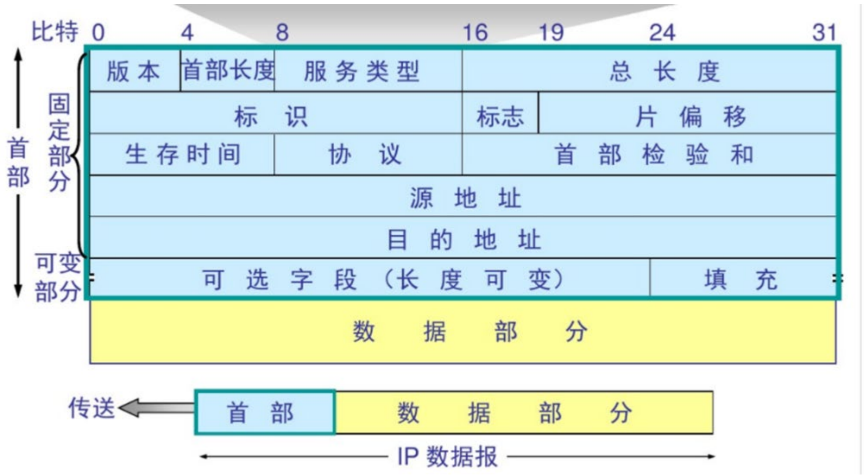
1、 Wireshark（前称Ethereal）是一个网络封包分析软件。网络封包分析软件的功能是抓取网络封包，并尽可能显示出最为详细的网络封包资料。 Wireshark使用WinPCAP作为接口，直接与网卡进行数据报文交换，监听共享网络上传送的数据包，但不能对其进行修改或者控制。

2、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。

3、 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。

4、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。

5、 IPv4数据报格式



三、 实验环境

1、 硬件

Lenovo XiaoXin CHA07000
Intel® Core ™ i7-8500U CPU 1.80GHZ
内存：8G
显卡：NVIDIA GEFORCE 940MX

2、 软件

wireshark和PingPlotter

四、 实验过程

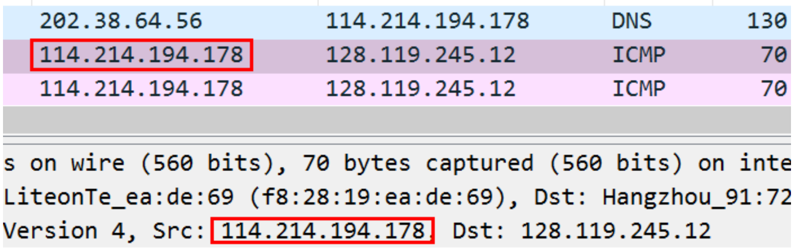
1） 实验步骤

a） 安装PingPlotter
b） 利用PingPlotter发包并用wireshark捕获，分别发送了56字节、2000字节、3500字节的数据报
c） 分析捕获的包

2） 实验分析

1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet details window. What is the IP address of your computer?

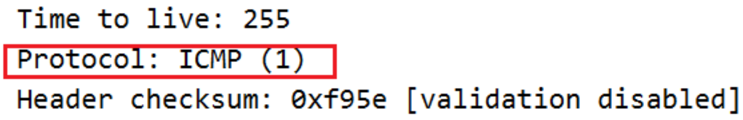
答：114.214.194.178



```
 202.38.64.56          114.214.194.178       DNS        130
 114.214.194.178       128.119.245.12        ICMP        70
 114.214.194.178       128.119.245.12        ICMP        70

s on wire (560 bits), 70 bytes captured (560 bits) on inte
LiteonTe_ea:de:69 (f8:28:19:ea:de:69), Dst: Hangzhou_91:72
Version 4, Src: 114.214.194.178, Dst: 128.119.245.12
```

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

答：1（表示ICMP）



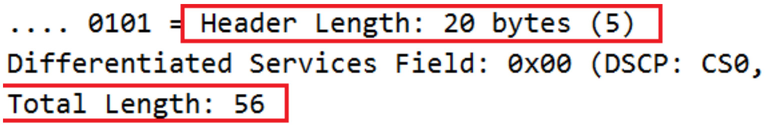
```
 Time to live: 255
 Protocol: ICMP (1)
 Header checksum: 0xf95e [validation disabled]
```

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：首部长度：20bytes

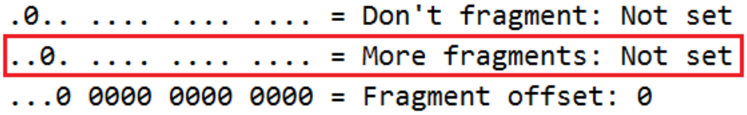
总长度56bytes,故payload=56-20=36bytes



```
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0,
Total Length: 56
```

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

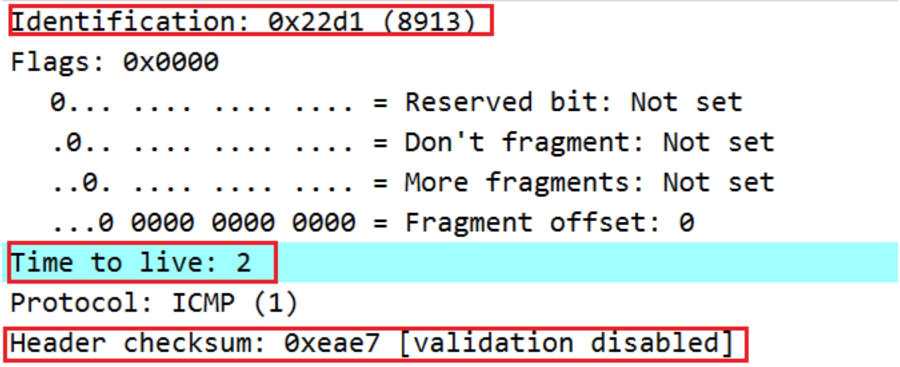
答：more fragments bit = 0,因此数据没有被分片



```
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
```

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：Identification, Time to live 和 Header checksum



```
Identification: 0x22d1 (8913)
Flags: 0x0000
   0... .... .... .... = Reserved bit: Not set
   .0.. .... .... .... = Don't fragment: Not set
   ..0. .... .... .... = More fragments: Not set
   ...0 0000 0000 0000 = Fragment offset: 0
Time to live: 2
Protocol: ICMP (1)
Header checksum: 0xeae7 [validation disabled]
```

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

- stay constant为：

（1）Version

（2）header length

（3）source IP

（4）destination IP

（5）Differentiated Services

（6） Upper Layer Protocol
（7） flags
（8） fragment offset,

- must stay constant为:

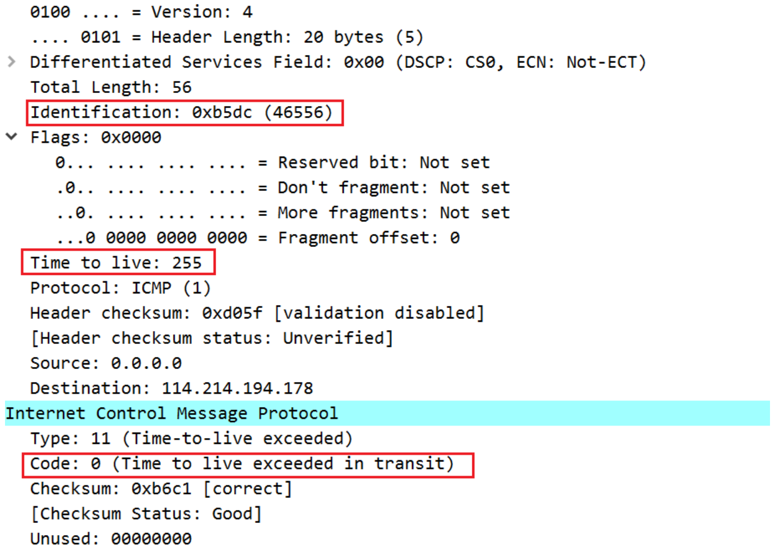
（1） Version (因为我们使用的数据报协议都为IPv4)
（2） header length (因为这些都是ICMP报文)
（3） source IP (因为我们从相同源发送报文)
（4） destination IP (因为我们报文发向相同目的地)
（5） Differentiated Services (ICMP报文使用相同的服务类型)
（6） Upper Layer Protocol (因为这些都是ICMP报文)

- must change:

（1） Identification(IP数据报之间要有不同的标识)
（2） Time to live (因为traceroute会改变ttl)
（3） Header checksum (因为头部改变了，故首部检验和会改变)

7. Describe the pattern you see in the values in the Identification field of the IP datagram.
   答：每个id比以前加1

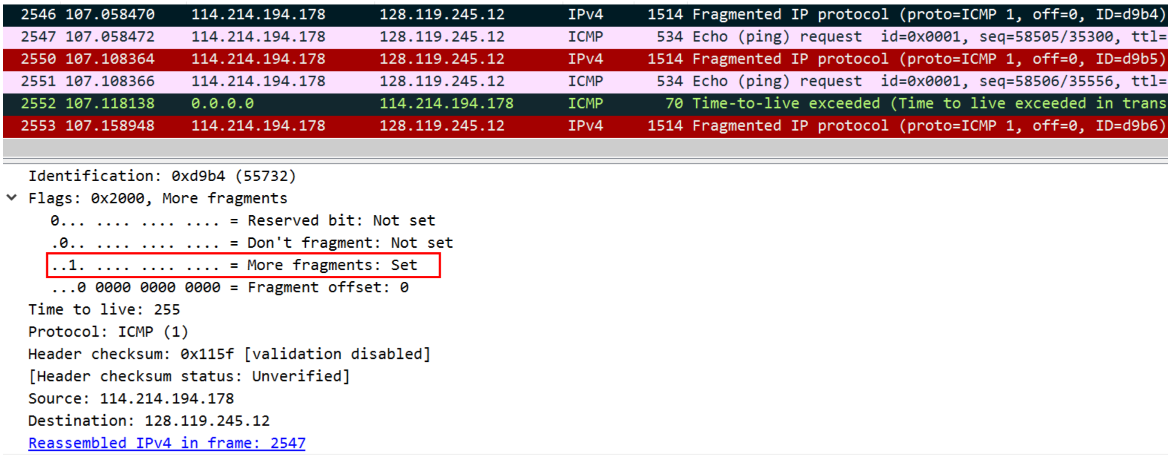
8. What is the value in the Identification field and the TTL field?
   答：id:46556 ttl:255



```
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 56
  Identification: 0xb5dc (46556)
v Flags: 0x0000
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..0. .... .... .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 255
  Protocol: ICMP (1)
  Header checksum: 0xd05f [validation disabled]
  [Header checksum status: Unverified]
  Source: 0.0.0.0
  Destination: 114.214.194.178
Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0xb6c1 [correct]
  [Checksum Status: Good]
  Unused: 00000000
```

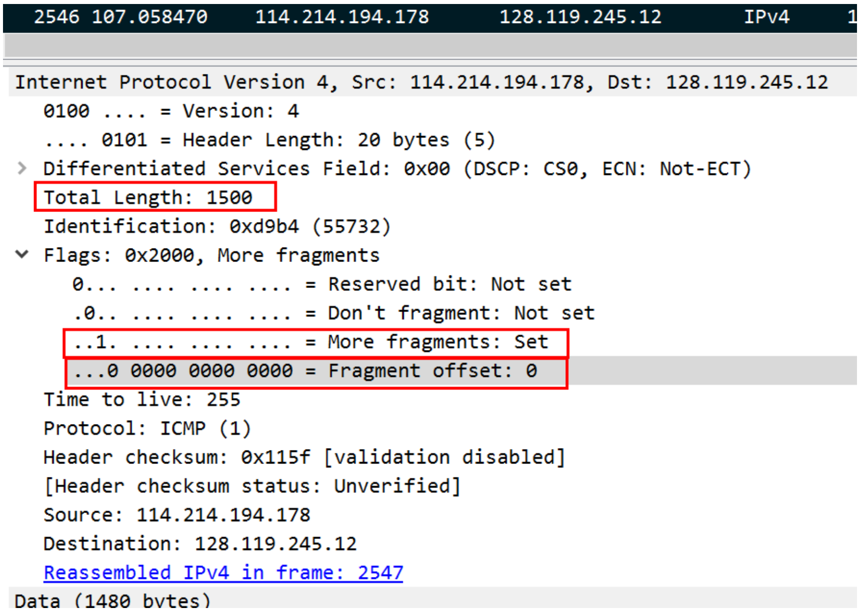
9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?
答：id变化，因为id值是一个独一无二的值，若id相同，则说明这些数据报实际上是同一较大数据报的片， 但它们不是，故会改变。TTL不变，因为第一跳路由的ttl总是相同的。

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?
答：被分片了，因为More fragments标志被置为1



```
2546 107.058470   114.214.194.178   128.119.245.12    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=d9b4)
2547 107.058472   114.214.194.178   128.119.245.12    ICMP     534 Echo (ping) request  id=0x0001, seq=58505/35300, ttl=
2550 107.108364   114.214.194.178   128.119.245.12    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=d9b5)
2551 107.108366   114.214.194.178   128.119.245.12    ICMP     534 Echo (ping) request  id=0x0001, seq=58506/35556, ttl=
2552 107.118138   0.0.0.0           114.214.194.178   ICMP      70 Time-to-live exceeded (Time to live exceeded in trans
2553 107.158948   114.214.194.178   128.119.245.12    IPv4    1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=d9b6)

  Identification: 0xd9b4 (55732)
v Flags: 0x2000, More fragments
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..1. .... .... .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 255
  Protocol: ICMP (1)
  Header checksum: 0x115f [validation disabled]
  [Header checksum status: Unverified]
  Source: 114.214.194.178
  Destination: 128.119.245.12
  Reassembled IPv4 in frame: 2547
```

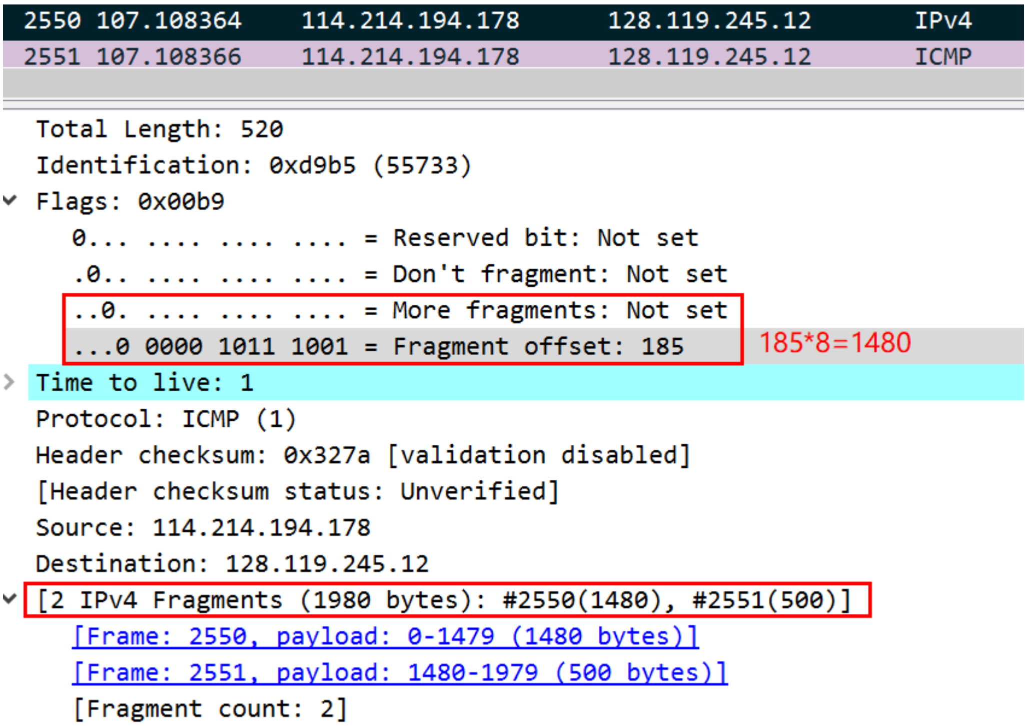
11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?
答：More fragments标志被置为1说明数据报被分片，偏移字段为0说明这是第一段，包括首部总共1500bytes。



```
2546 107.058470    114.214.194.178       128.119.245.12        IPv4       1

Internet Protocol Version 4, Src: 114.214.194.178, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0xd9b4 (55732)
  v Flags: 0x2000, More fragments
        0... .... .... .... = Reserved bit: Not set
        .0.. .... .... .... = Don't fragment: Not set
        ..1. .... .... .... = More fragments: Set
        ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
    Header checksum: 0x115f [validation disabled]
    [Header checksum status: Unverified]
    Source: 114.214.194.178
    Destination: 128.119.245.12
    Reassembled IPv4 in frame: 2547
Data (1480 bytes)
```

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：因为片偏移字段不为0，而是185*8=1480,没有更多的分片了，因为More fragments为0.



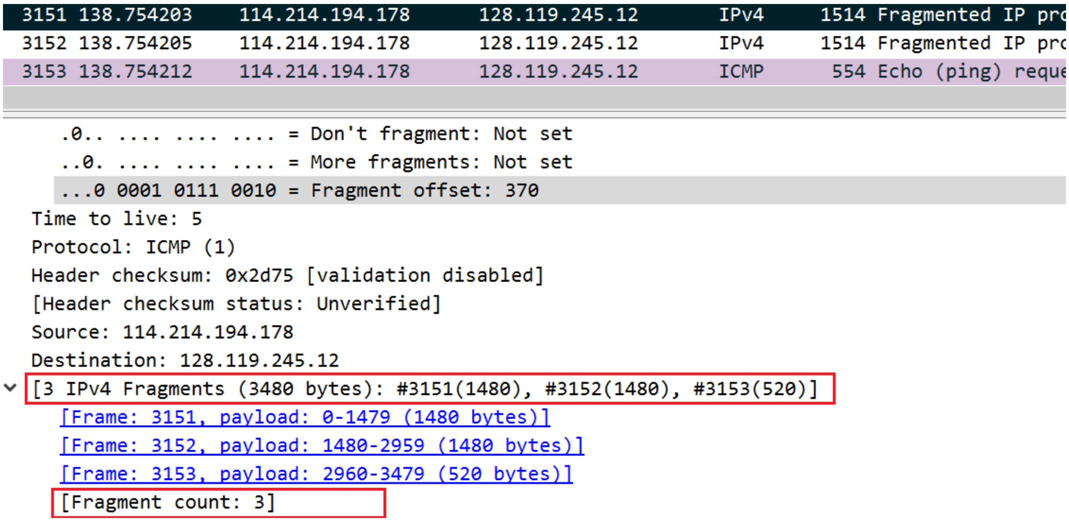
```
 2550 107.108364     114.214.194.178      128.119.245.12       IPv4
 2551 107.108366     114.214.194.178      128.119.245.12       ICMP

  Total Length: 520
  Identification: 0xd9b5 (55733)
v Flags: 0x00b9
     0... .... .... .... = Reserved bit: Not set
     .0.. .... .... .... = Don't fragment: Not set
     ..0. .... .... .... = More fragments: Not set
     ...0 0000 1011 1001 = Fragment offset: 185      185*8=1480
> Time to live: 1
  Protocol: ICMP (1)
  Header checksum: 0x327a [validation disabled]
  [Header checksum status: Unverified]
  Source: 114.214.194.178
  Destination: 128.119.245.12
v [2 IPv4 Fragments (1980 bytes): #2550(1480), #2551(500)]
     [Frame: 2550, payload: 0-1479 (1480 bytes)]
     [Frame: 2551, payload: 1480-1979 (500 bytes)]
     [Fragment count: 2]
```

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

答：total length, flags, fragment offset 和 checksum

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

答：3个，见下图



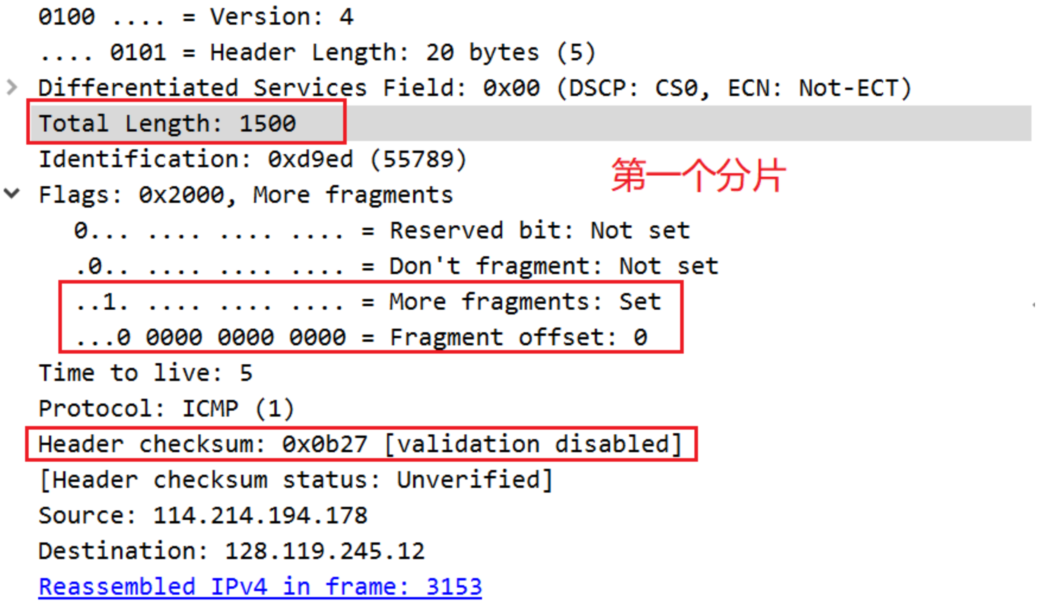
```
3151 138.754203   114.214.194.178   128.119.245.12   IPv4   1514 Fragmented IP pro
3152 138.754205   114.214.194.178   128.119.245.12   IPv4   1514 Fragmented IP pro
3153 138.754212   114.214.194.178   128.119.245.12   ICMP    554 Echo (ping) reque

     .0.. .... .... .... = Don't fragment: Not set
     ..0. .... .... .... = More fragments: Not set
     ...0 0001 0111 0010 = Fragment offset: 370
  Time to live: 5
  Protocol: ICMP (1)
  Header checksum: 0x2d75 [validation disabled]
  [Header checksum status: Unverified]
  Source: 114.214.194.178
  Destination: 128.119.245.12
v [3 IPv4 Fragments (3480 bytes): #3151(1480), #3152(1480), #3153(520)]
     [Frame: 3151, payload: 0-1479 (1480 bytes)]
     [Frame: 3152, payload: 1480-2959 (1480 bytes)]
     [Frame: 3153, payload: 2960-3479 (520 bytes)]
     [Fragment count: 3]
```

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

答：都不同的是：Fragment offset, Header checksum。

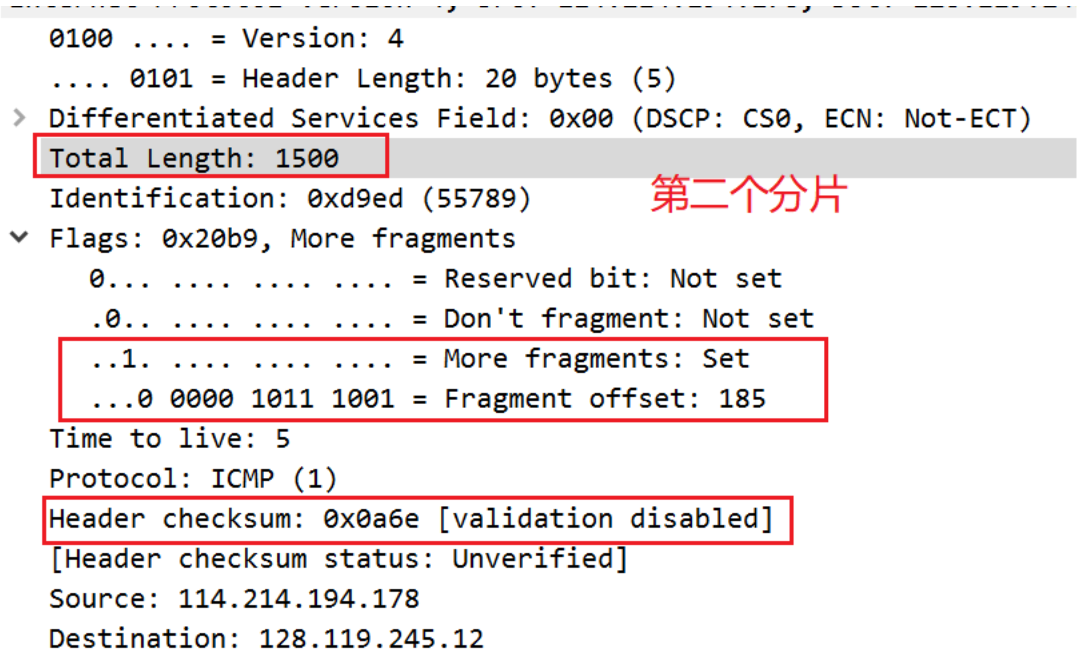
第一个和第二个分片除了上述两个别无不同。

前俩个和最后一个除了上述两个还有：Total length，flags 不同。



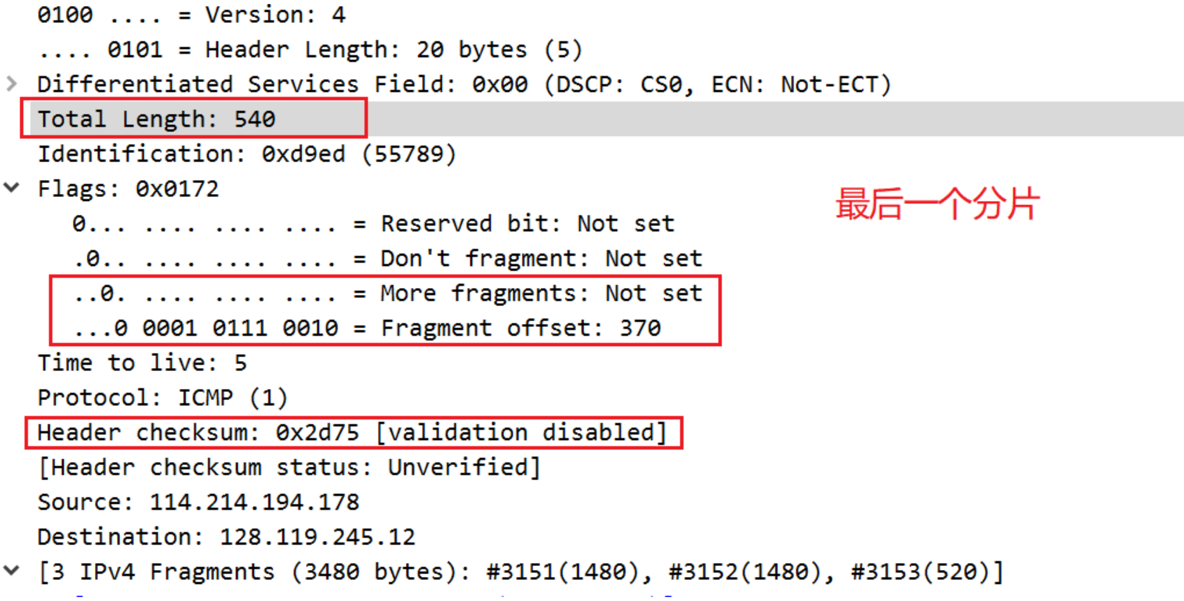
```
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1500
  Identification: 0xd9ed (55789)
v Flags: 0x2000, More fragments
     0... .... .... .... = Reserved bit: Not set
     .0.. .... .... .... = Don't fragment: Not set
     ..1. .... .... .... = More fragments: Set
     ...0 0000 0000 0000 = Fragment offset: 0
  Time to live: 5
  Protocol: ICMP (1)
  Header checksum: 0x0b27 [validation disabled]
  [Header checksum status: Unverified]
  Source: 114.214.194.178
  Destination: 128.119.245.12
  Reassembled IPv4 in frame: 3153
```

第一个分片



```
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 1500
  Identification: 0xd9ed (55789)
v Flags: 0x20b9, More fragments
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..1. .... .... .... = More fragments: Set
    ...0 0000 1011 1001 = Fragment offset: 185
  Time to live: 5
  Protocol: ICMP (1)
  Header checksum: 0x0a6e [validation disabled]
  [Header checksum status: Unverified]
  Source: 114.214.194.178
  Destination: 128.119.245.12
```

第二个分片



```
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 540
  Identification: 0xd9ed (55789)
v Flags: 0x0172
    0... .... .... .... = Reserved bit: Not set
    .0.. .... .... .... = Don't fragment: Not set
    ..0. .... .... .... = More fragments: Not set
    ...0 0001 0111 0010 = Fragment offset: 370
  Time to live: 5
  Protocol: ICMP (1)
  Header checksum: 0x2d75 [validation disabled]
  [Header checksum status: Unverified]
  Source: 114.214.194.178
  Destination: 128.119.245.12
v [3 IPv4 Fragments (3480 bytes): #3151(1480), #3152(1480), #3153(520)]
```

最后一个分片

五、 实验总结

1. 学习了软件PingPlotter的使用

2. 分析了IP数据报的结构，对IP数据报有了更加深入的理解。