山东大学 计算机 学院

计算机网络 课程实验报告

学号：	姓名：	班级：
实验题目： 实验九 IP		
实验学时：2h	实验日期： 2023.04.24	
实验目的： 学习 IP 的相关内容		
硬件环境： Windows10 家庭版		
软件环境： Wireshark		

实验步骤与内容：

实验内容：

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.

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

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?

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?

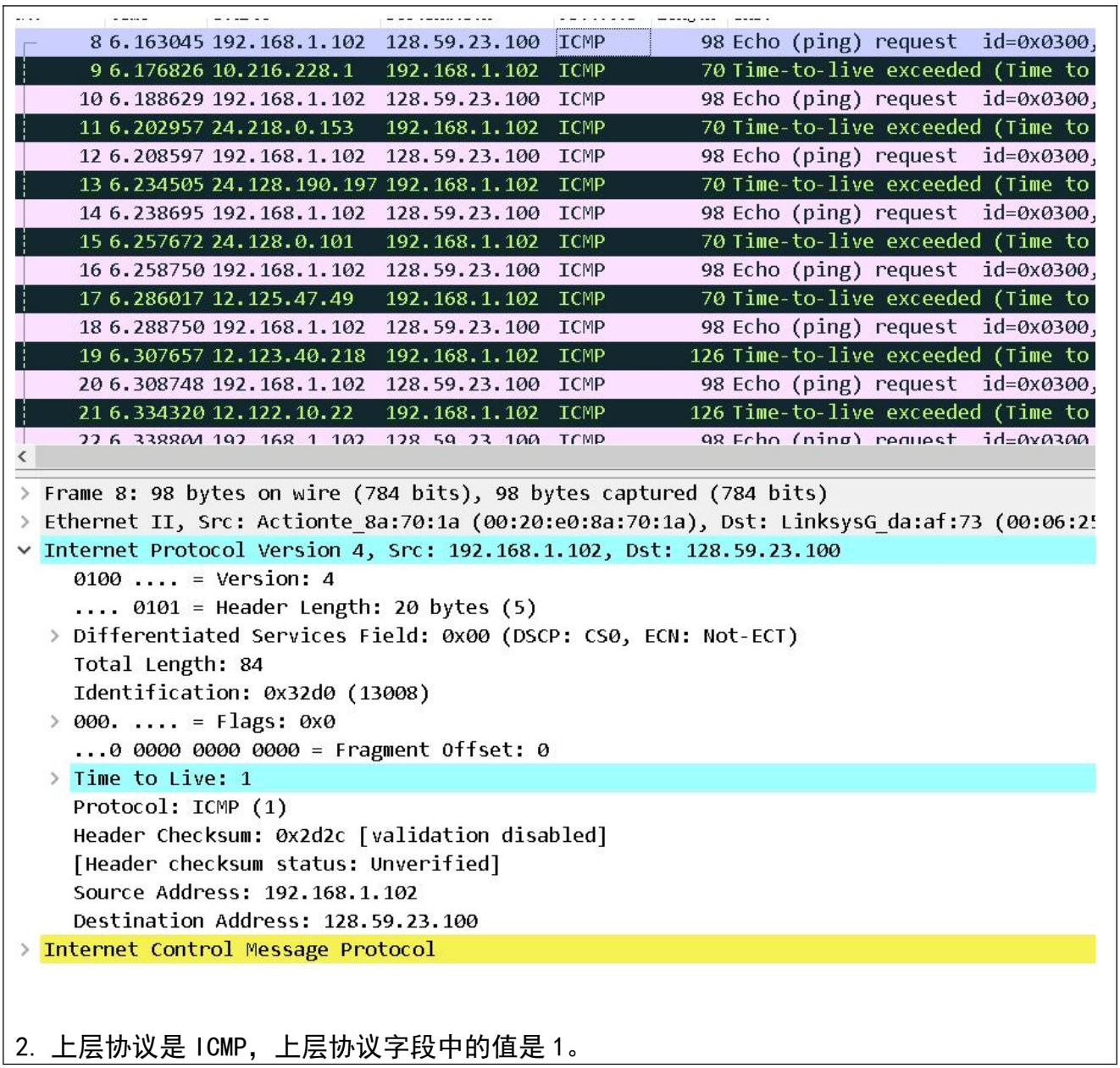
13. What fields change in the IP header between the first and second fragment?

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

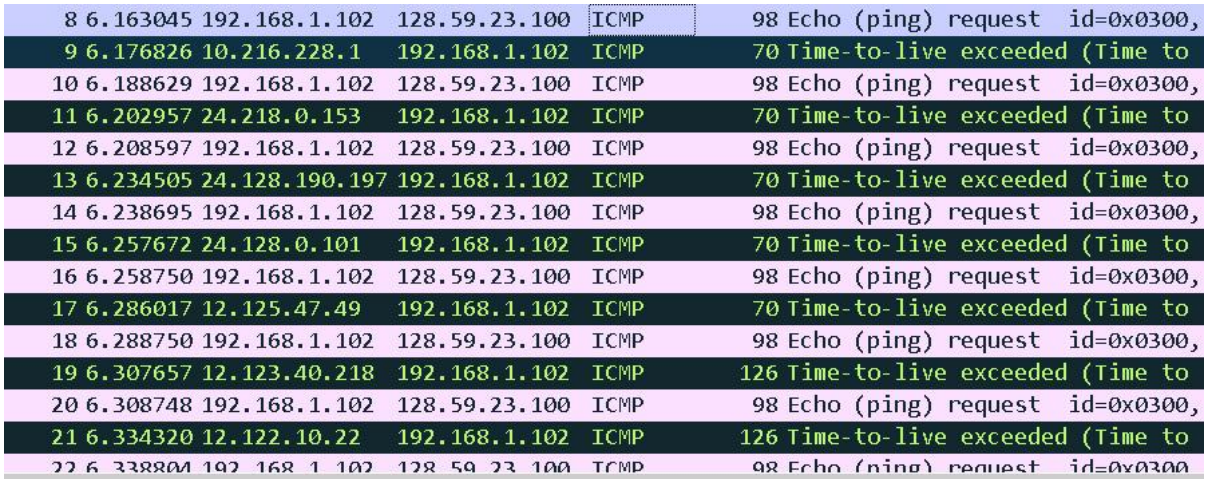
15. What fields change in the IP header among the fragments?

实验步骤：
本实验主要学习 IP，需要下载 PingPlotter 来对 IP 数据包进行跟踪，同时在跟踪过程中还需修改数据包大小。

1. 本机的 IP 地址是 192.168.1.102。



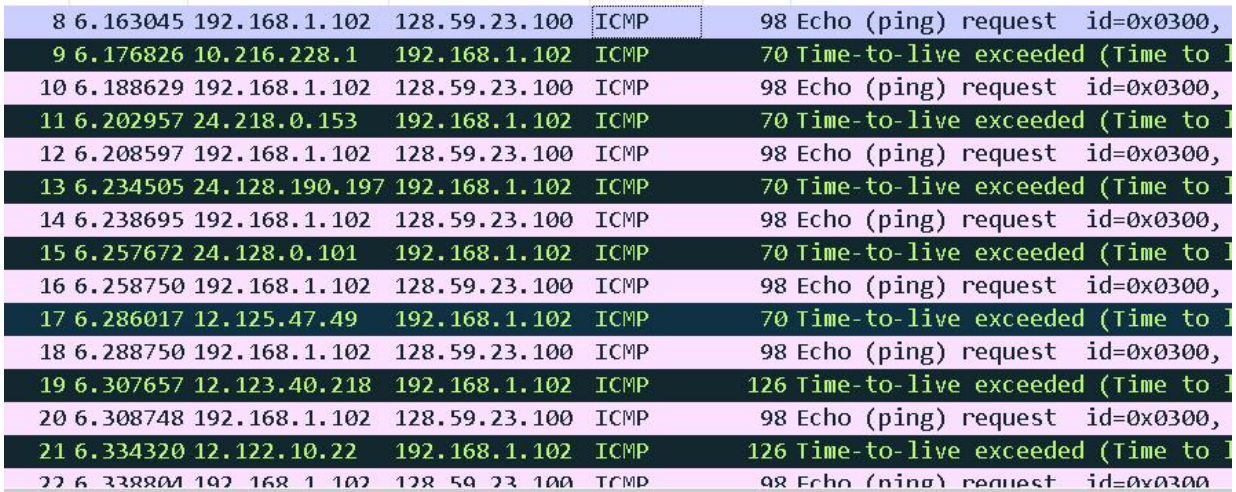
2. 上层协议是 ICMP，上层协议字段中的值是 1。



```
    8 6.163045 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
    9 6.176826 10.216.228.1   192.168.1.102  ICMP      70 Time-to-live exceeded (Time to
   10 6.188629 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   11 6.202957 24.218.0.153   192.168.1.102  ICMP      70 Time-to-live exceeded (Time to
   12 6.208597 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   13 6.234505 24.128.190.197 192.168.1.102  ICMP      70 Time-to-live exceeded (Time to
   14 6.238695 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   15 6.257672 24.128.0.101   192.168.1.102  ICMP      70 Time-to-live exceeded (Time to
   16 6.258750 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   17 6.286017 12.125.47.49   192.168.1.102  ICMP      70 Time-to-live exceeded (Time to
   18 6.288750 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   19 6.307657 12.123.40.218  192.168.1.102  ICMP     126 Time-to-live exceeded (Time to
   20 6.308748 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   21 6.334320 12.122.10.22   192.168.1.102  ICMP     126 Time-to-live exceeded (Time to
   22 6.338804 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300
```

```
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
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)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: ICMP (1)
```

3. IP 标头有 20 字节，IP 数据包有 64 字节，有效负载字节数等于总长度减去标头长度。



```
    8 6.163045 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
    9 6.176826 10.216.228.1   192.168.1.102  ICMP      70 Time-to-live exceeded (Time to
   10 6.188629 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   11 6.202957 24.218.0.153   192.168.1.102  ICMP      70 Time-to-live exceeded (Time to
   12 6.208597 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   13 6.234505 24.128.190.197 192.168.1.102  ICMP      70 Time-to-live exceeded (Time to
   14 6.238695 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   15 6.257672 24.128.0.101   192.168.1.102  ICMP      70 Time-to-live exceeded (Time to
   16 6.258750 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   17 6.286017 12.125.47.49   192.168.1.102  ICMP      70 Time-to-live exceeded (Time to
   18 6.288750 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   19 6.307657 12.123.40.218  192.168.1.102  ICMP     126 Time-to-live exceeded (Time to
   20 6.308748 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300,
   21 6.334320 12.122.10.22   192.168.1.102  ICMP     126 Time-to-live exceeded (Time to
   22 6.338804 192.168.1.102  128.59.23.100  ICMP      98 Echo (ping) request  id=0x0300
```

```
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:
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)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
```

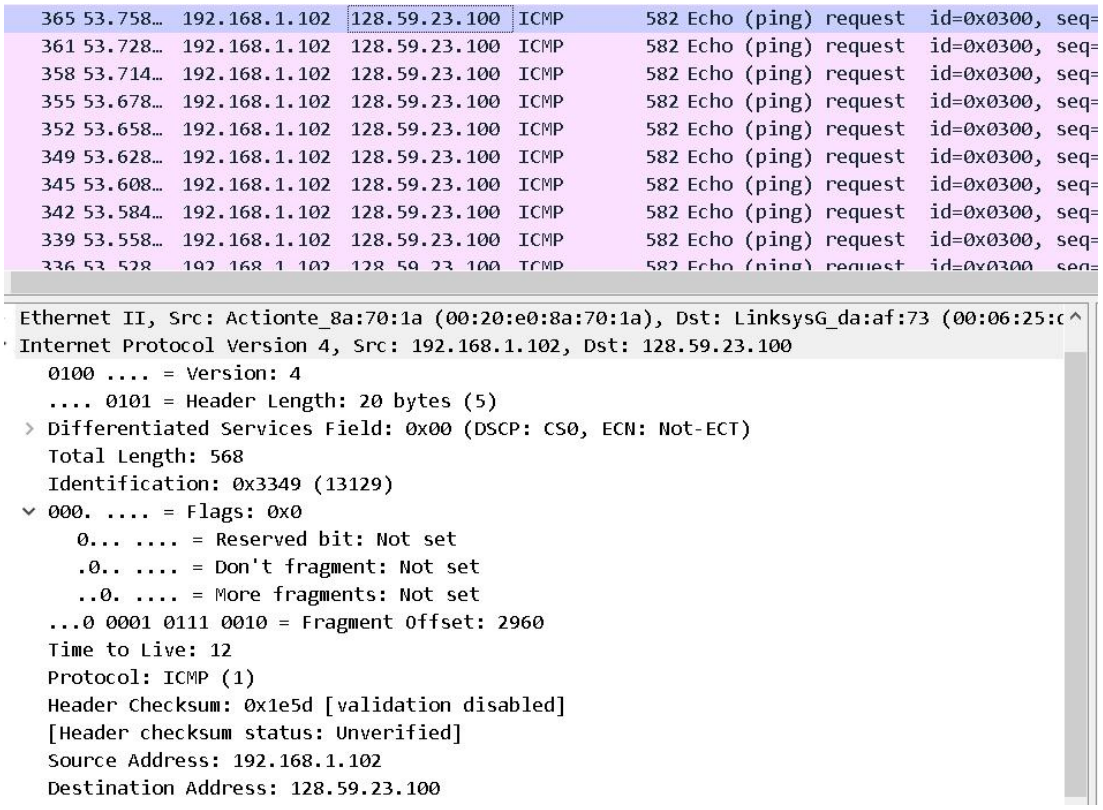
4. IP 数据包没有分片，因为 Flag 中最后一位为 0，且 Fragment offset 为 0，这意味着该包是最后一个分片，且偏移量为 0，一个包就装下了所有的 data。

8	6.163045	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300,
9	6.176826	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
10	6.188629	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300,
11	6.202957	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
12	6.208597	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300,
13	6.234505	24.128.190.197	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
14	6.238695	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300,
15	6.257672	24.128.0.101	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
16	6.258750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300,
17	6.286017	12.125.47.49	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to
18	6.288750	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300,
19	6.307657	12.123.40.218	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to
20	6.308748	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300,
21	6.334320	12.122.10.22	192.168.1.102	ICMP	126	Time-to-live exceeded (Time to
22	6.338804	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300

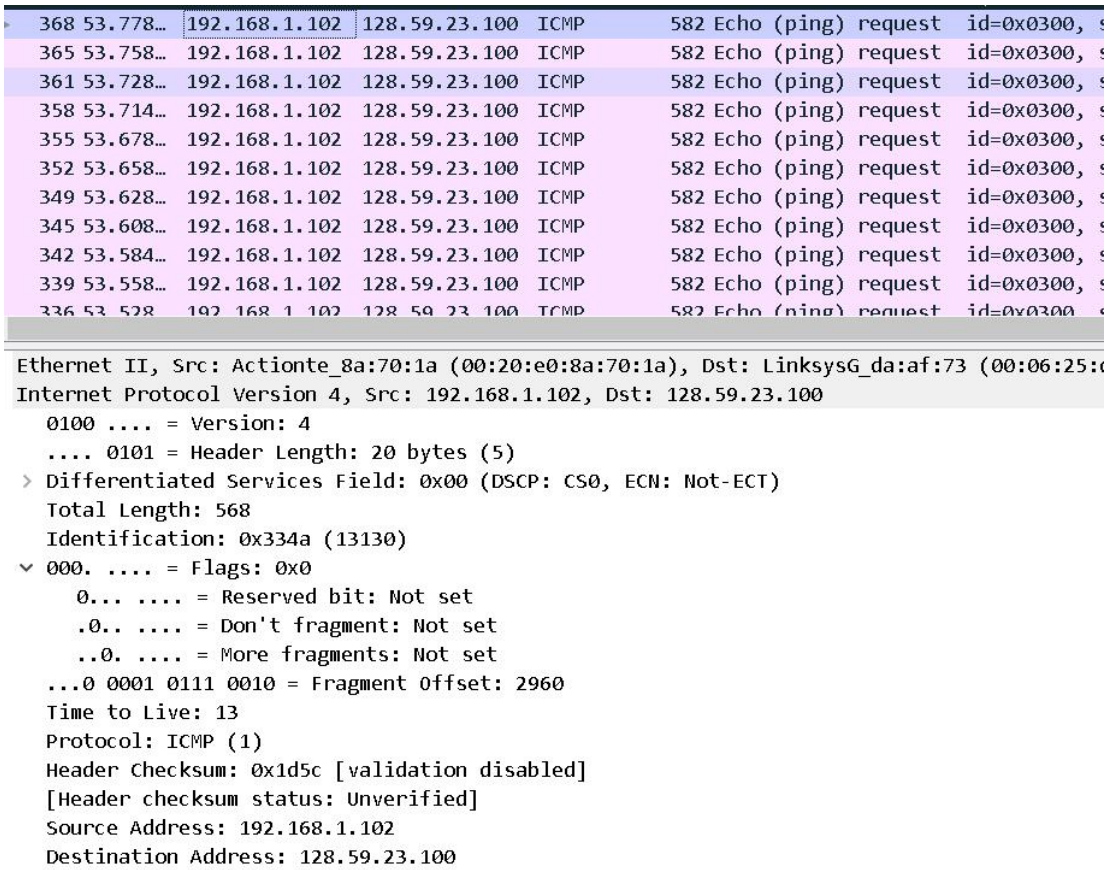
```
Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25
Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x32d0 (13008)
v 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
```

5. Identification、TTL、Checksum 都会发生改变，如下图所示。

第一条消息：



第二条消息：

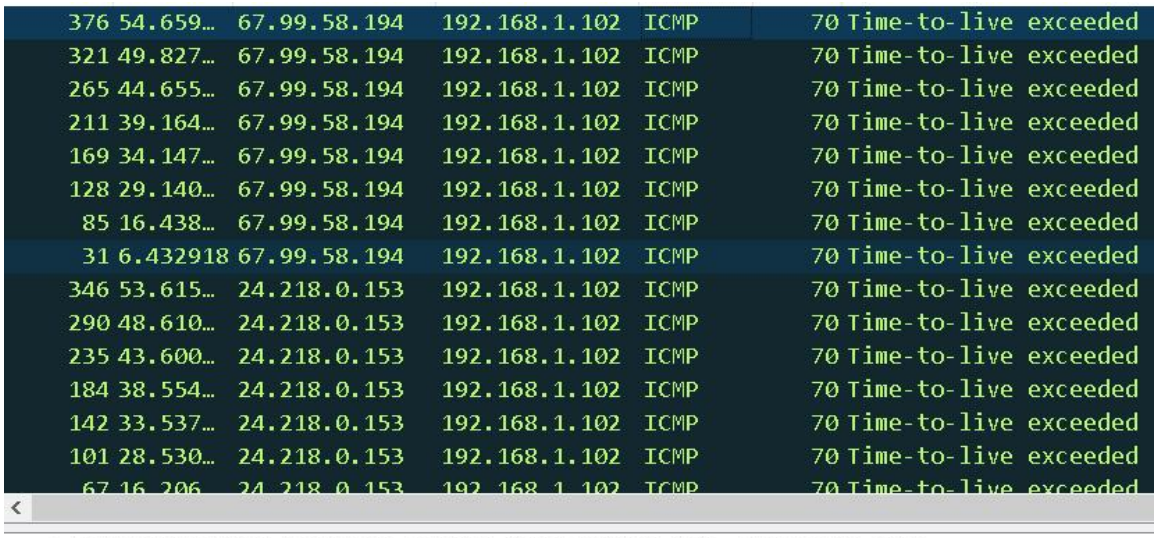


6. Version、Header Length、Total Length、source IP、Destination IP 不变，TTL、Header Checksum、Identification 变。因为发送方每发送一个 datagram，TTL++，Checksum 会随

datagram 中其他字节的变化而变化，Identification 也会++。

7. 标识号是不同的，用于区分每个 IP 数据包和处理 IP 分片。

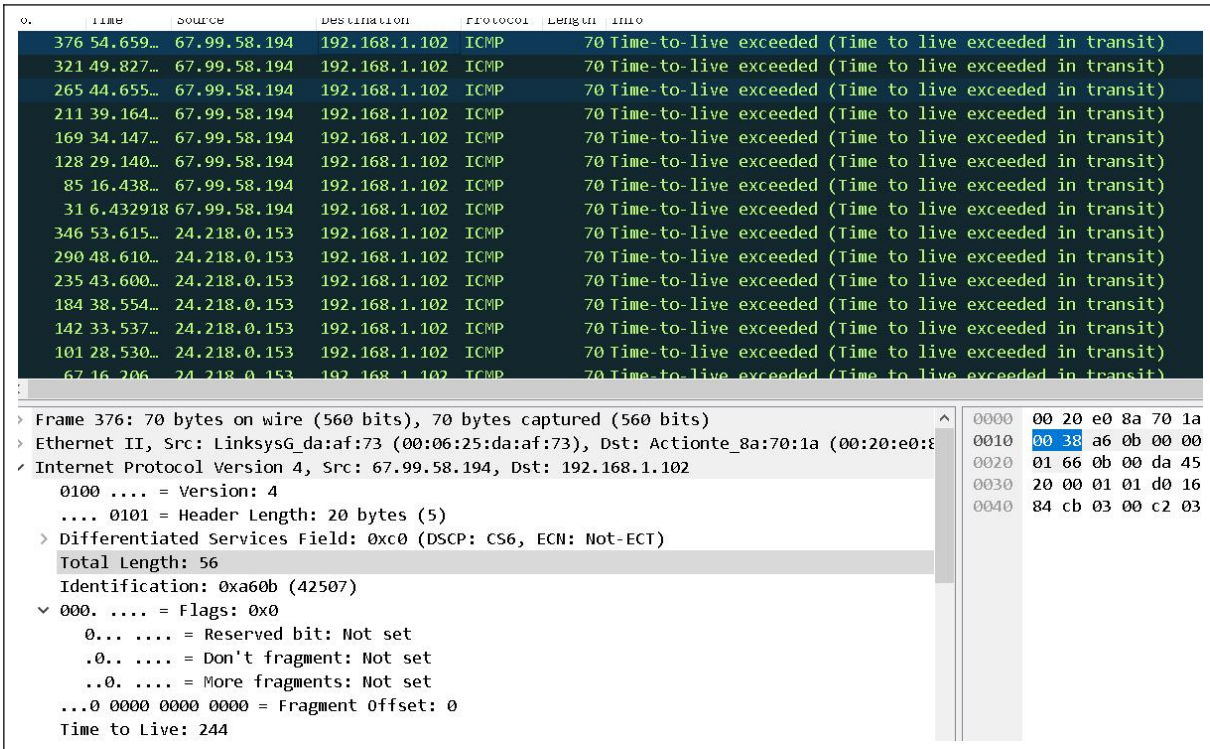
8. Identification 的值是 42507，TTL 是 224。



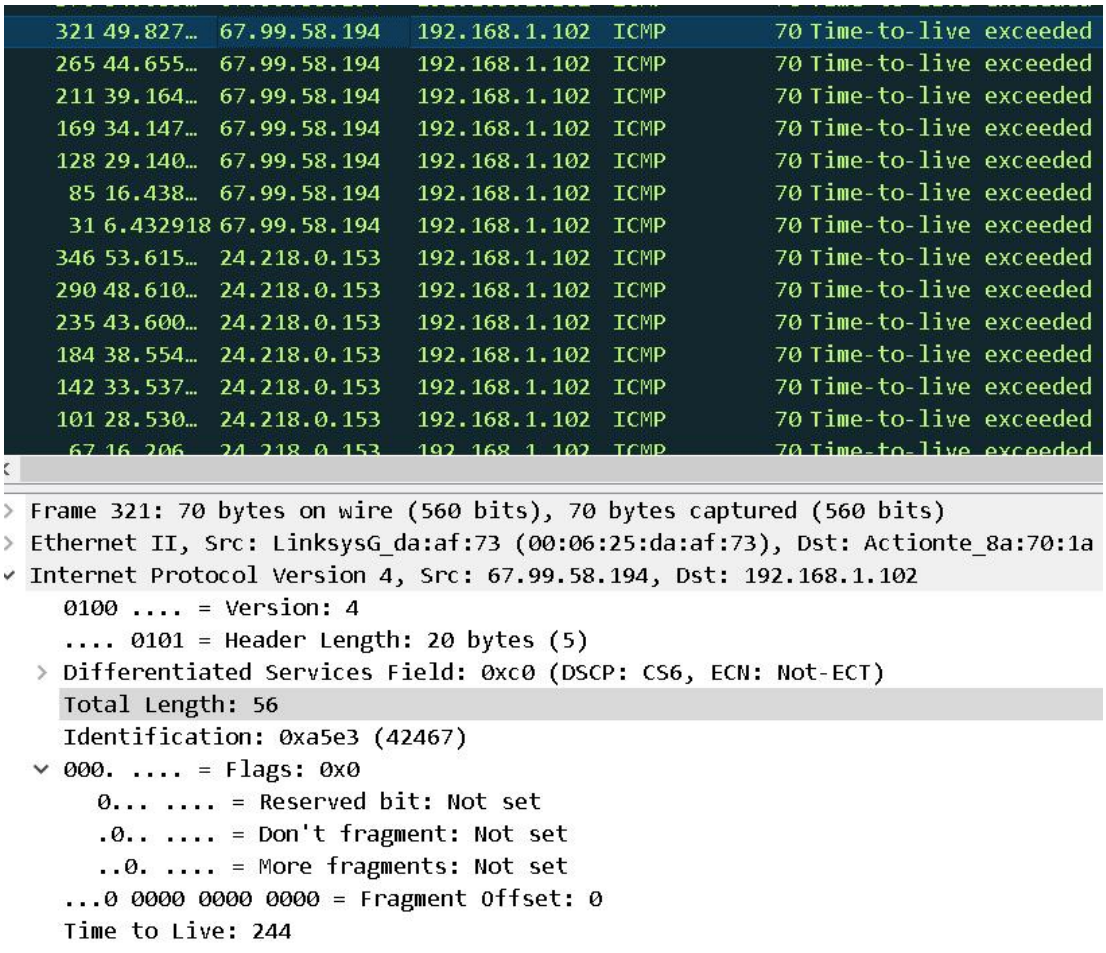
376	54.659…	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded
321	49.827…	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded
265	44.655…	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded
211	39.164…	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded
169	34.147…	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded
128	29.140…	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded
85	16.438…	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded
31	6.432918	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded
346	53.615…	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded
290	48.610…	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded
235	43.600…	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded
184	38.554…	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded
142	33.537…	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded
101	28.530…	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded
67	16.206…	24.218.0.153	192.168.1.102	ICMP	70	Time-to-live exceeded

```
> Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
  Total Length: 56
  Identification: 0xa60b (42507)
v 000. .... = Flags: 0x0
    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: 244
  Protocol: ICMP (1)
```

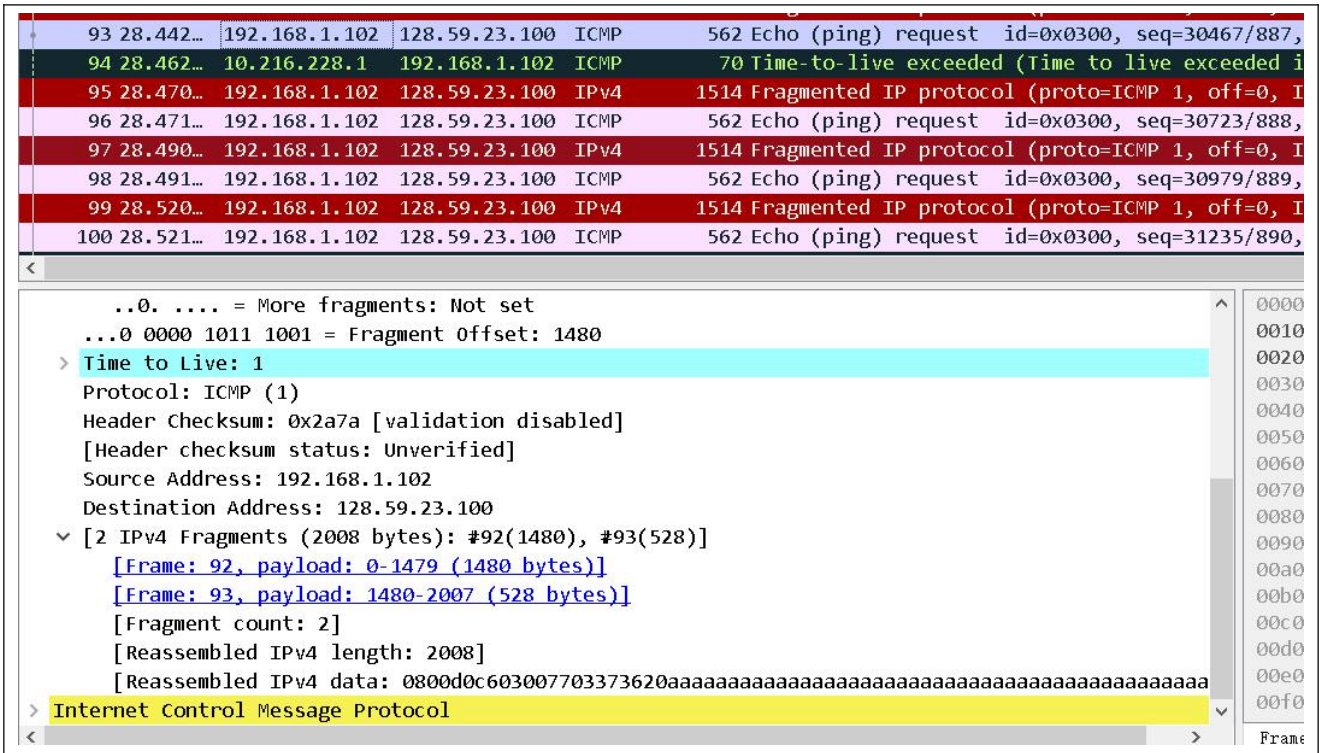
9. 标识字段都会更改，因为标识字段是唯一值。当两个或多个 IP 数据报具有相同的标识值时，则意味着这些 IP 数据报是单个大型 IP 数据报的片段。TTL 字段保持不变，因为第一跳路由器的 TTL 始终相同。
第一条消息：



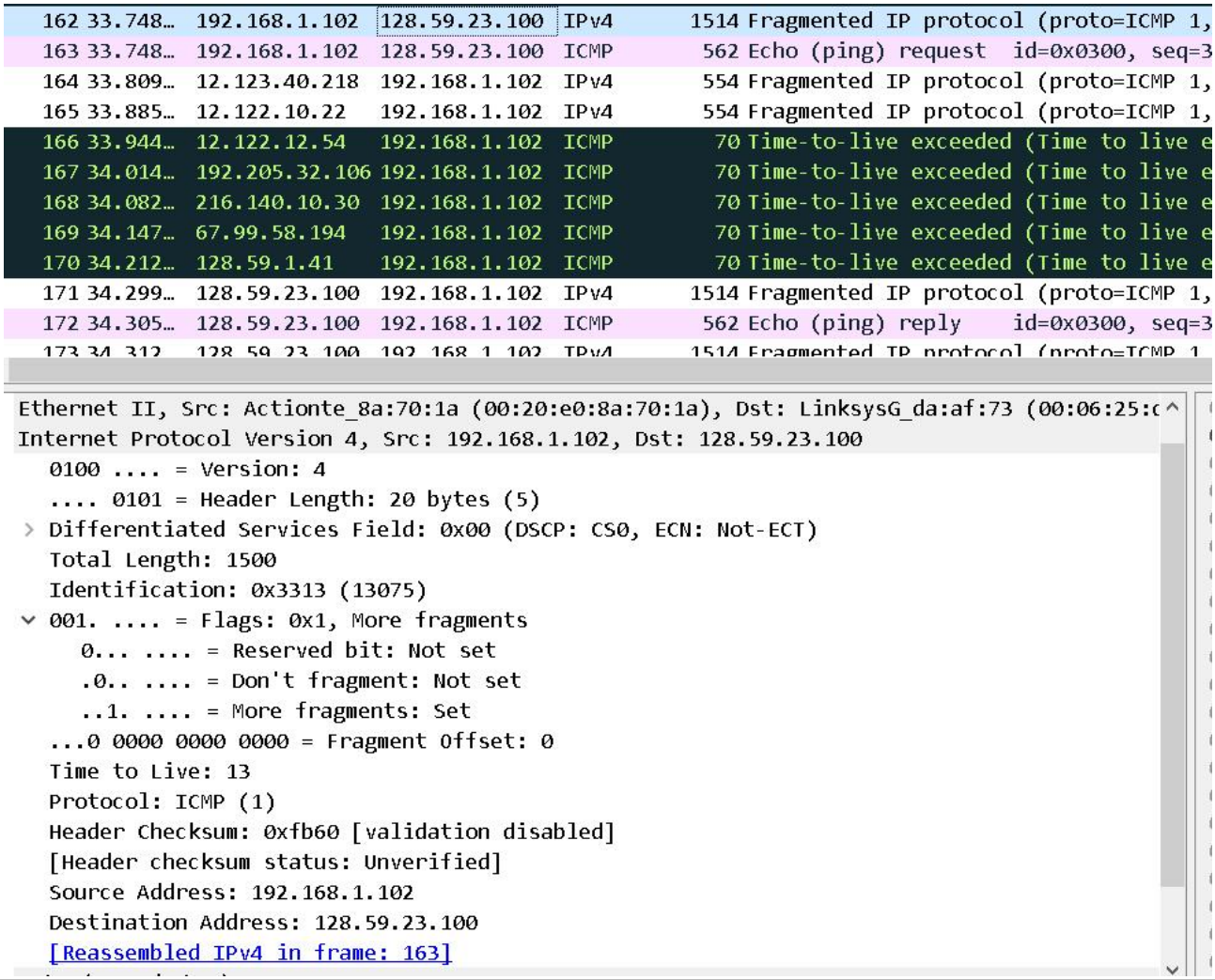
第二条消息：



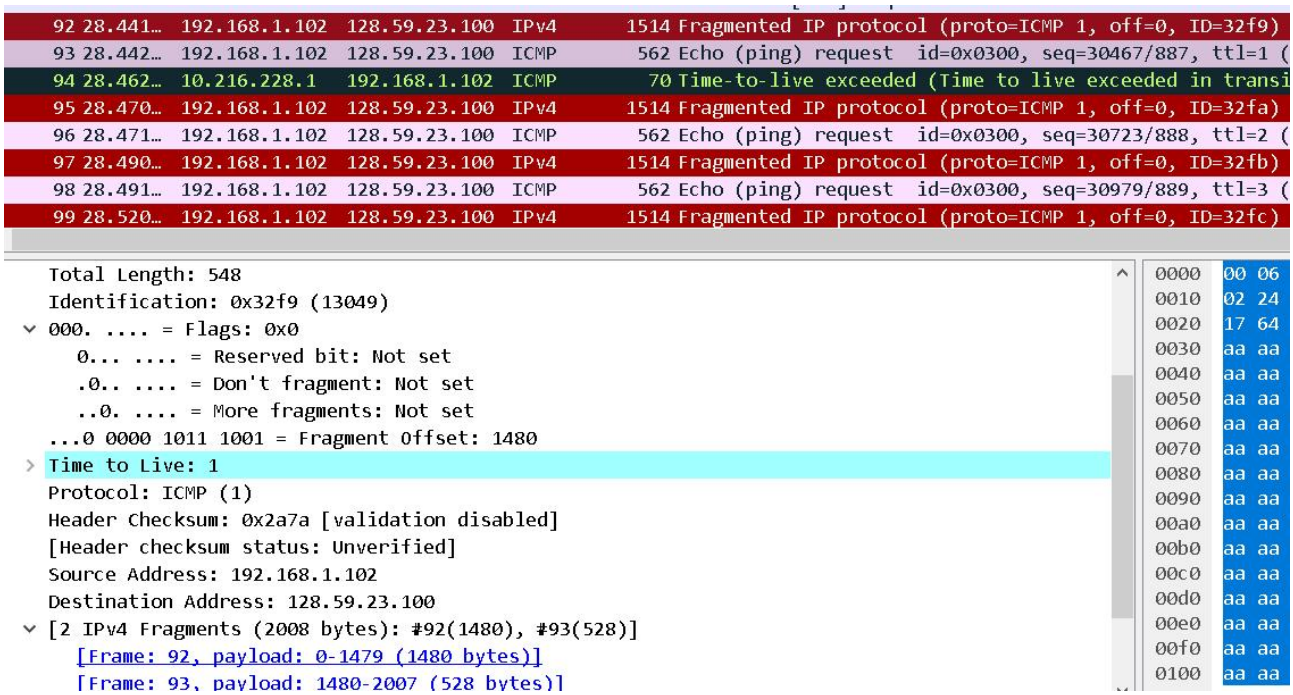
10. 信息会被分段，因为收集跟踪的计算机中最大 IP 数据包长度为 1500 个字节。



11. Flags 中的 More fragment 不为 0 表示数据报分段，而 Fragment offset 为 0 表示是第一个片段，该数据报长度为 1480。

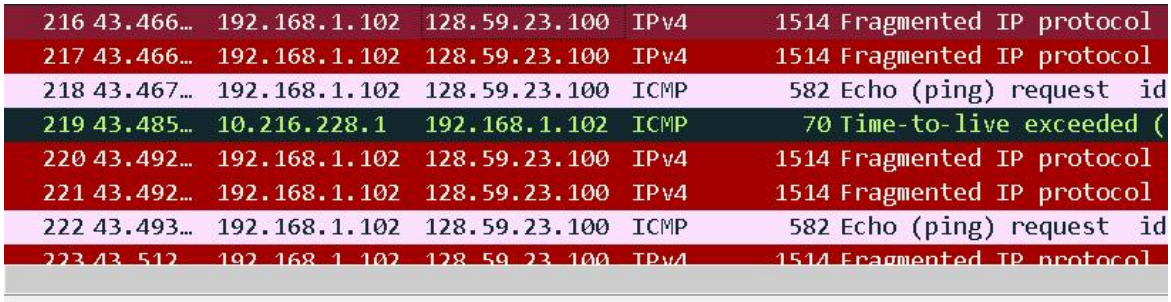


12. 由 Fragment offset 为 1480 可知这是第二个数据报片段，而又因为 Flags 为 0 可表明之后没有其他片段，该数据报长度为 528。

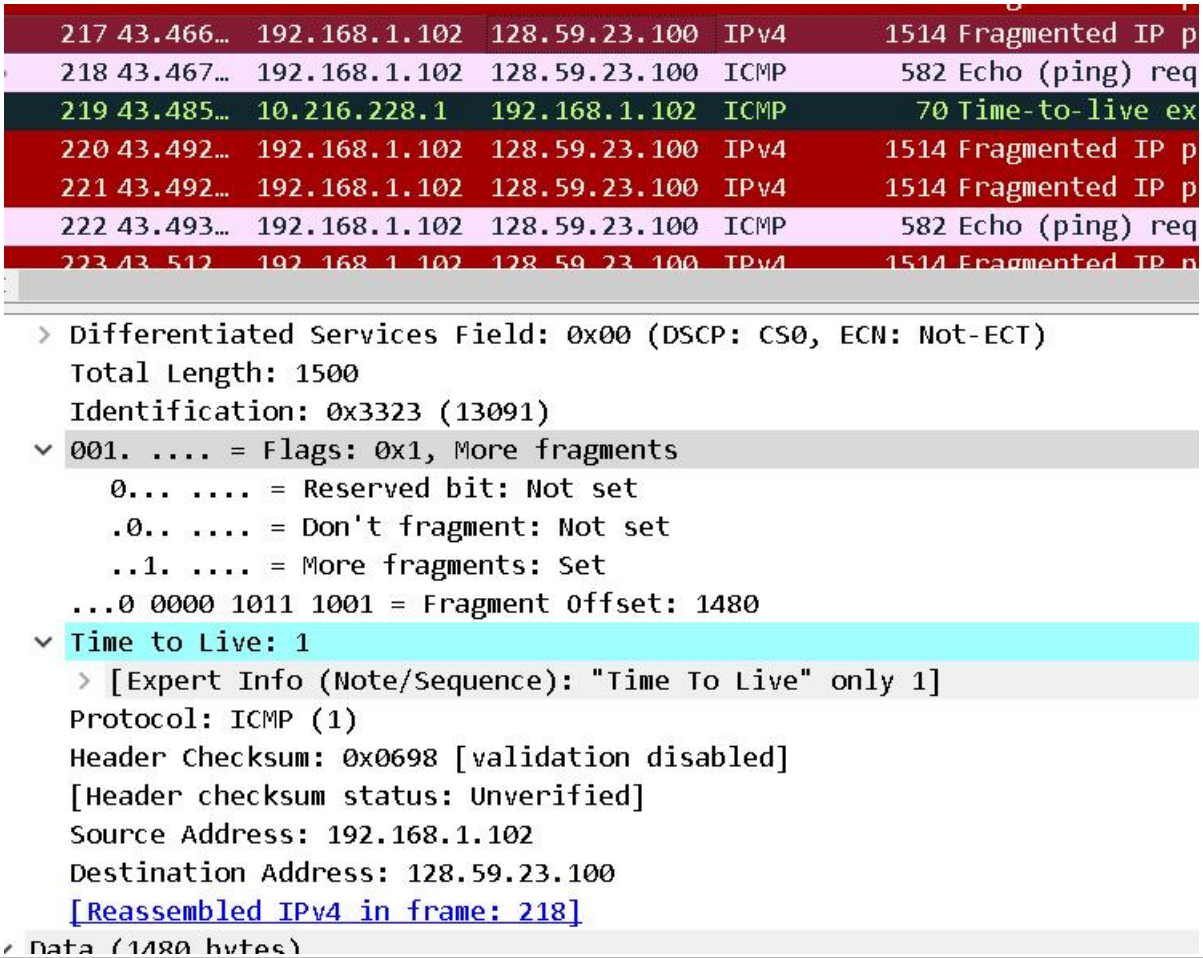


13. Fragment Offser 和 Header Checksum 会发生改变。

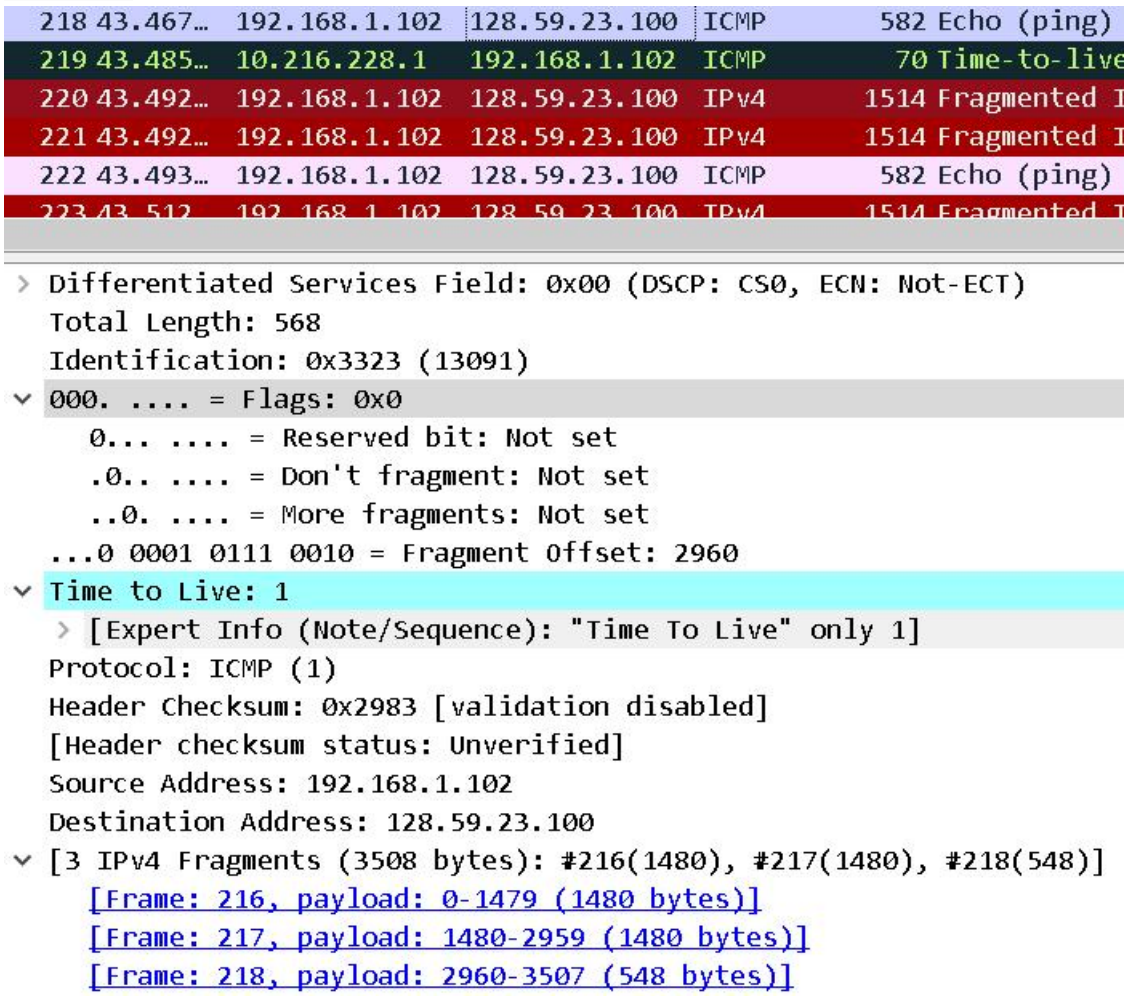
14. 共有三个分片。
第一个：


216 43.466… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol
217 43.466… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol
218 43.467… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id
219 43.485… 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live exceeded (
220 43.492… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol
221 43.492… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP protocol
222 43.493… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) request id
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3323 (13091)
001. .... = Flags: 0x1, More fragments
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..1. .... = More fragments: Set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
[Expert Info (Note/Sequence): "Time To Live" only 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)

第二个：


217 43.466… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP p
218 43.467… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) req
219 43.485… 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live ex
220 43.492… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP p
221 43.492… 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP p
222 43.493… 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) req
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3323 (13091)
001. .... = Flags: 0x1, More fragments
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..1. .... = More fragments: Set
...0 0000 1011 1001 = Fragment Offset: 1480
Time to Live: 1
[Expert Info (Note/Sequence): "Time To Live" only 1]
Protocol: ICMP (1)
Header Checksum: 0x0698 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[Reassembled IPv4 in frame: 218]

第三个：



15. Fragment Offser 和 Header Checksum 会发生改变。

结论分析与体会：

通过本次实验，学习了 IP 的相关内容，巩固了课堂所学。通过具体查看相应封包，对数据包分段传送有了更清楚的认识。通过查看具体的数据报中的内容，来学习 IP 的知识，对 IP 相关知识的记忆更加直观和清晰。