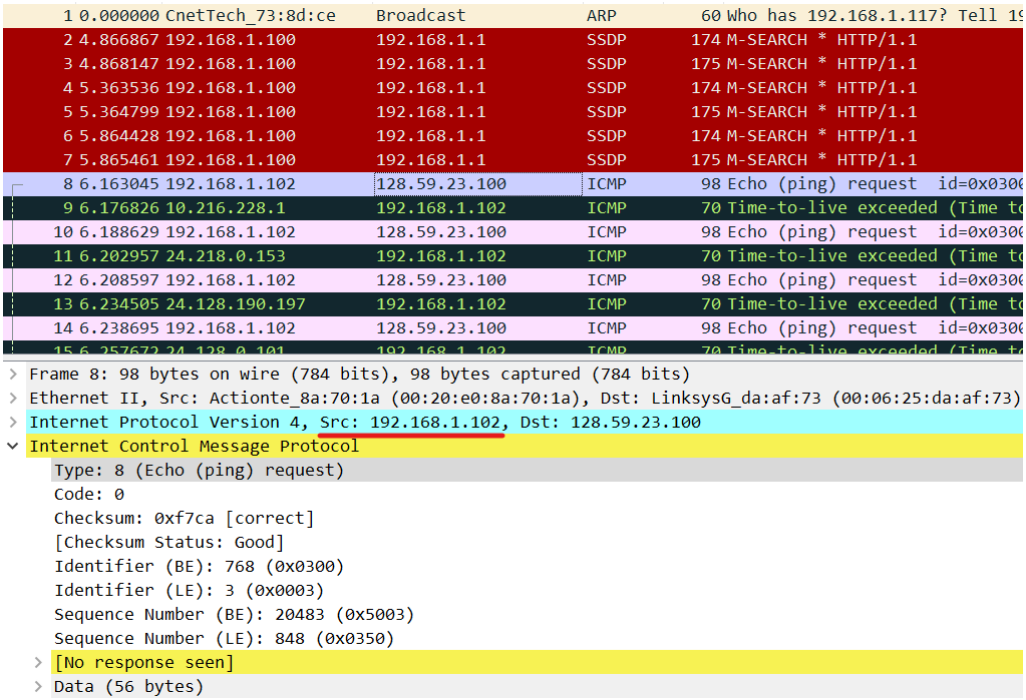
IP 实验报告

PB20111689 蓝俊玮

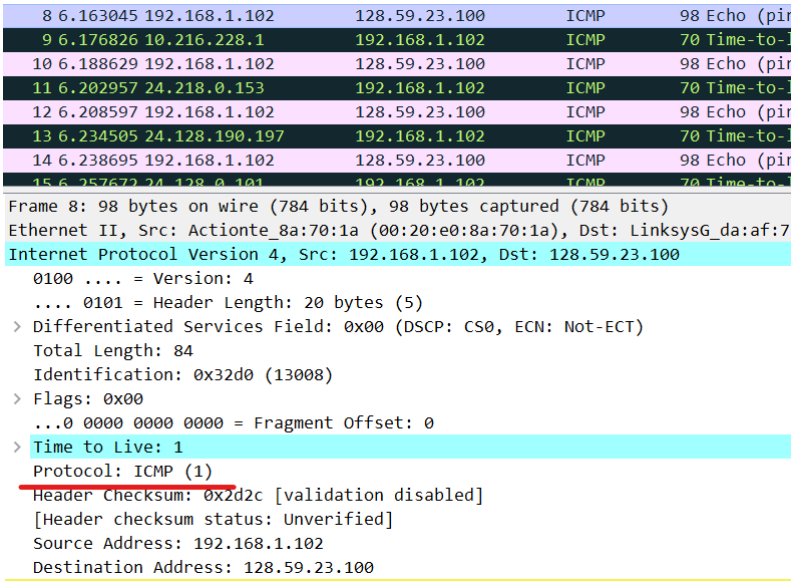
本次实验所分析的包是由实验文档提供的 http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip 的 ip-ethereal-trace-1 包

A look at the captured trace

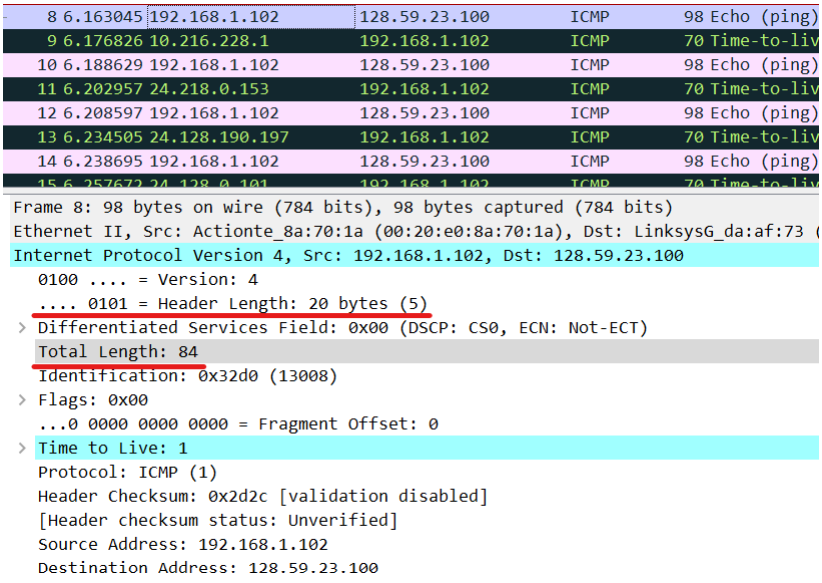
1. 我（文档）的电脑的 IP 地址是 **192.168.1.102**



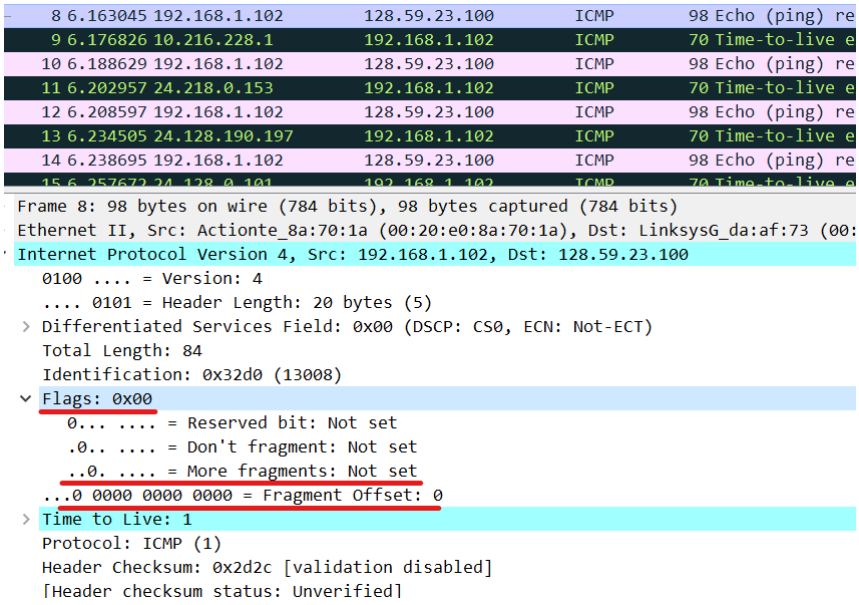
2. 在 IP 分组的首部中，上层协议是 **ICMP**，且它的值是 **1**。



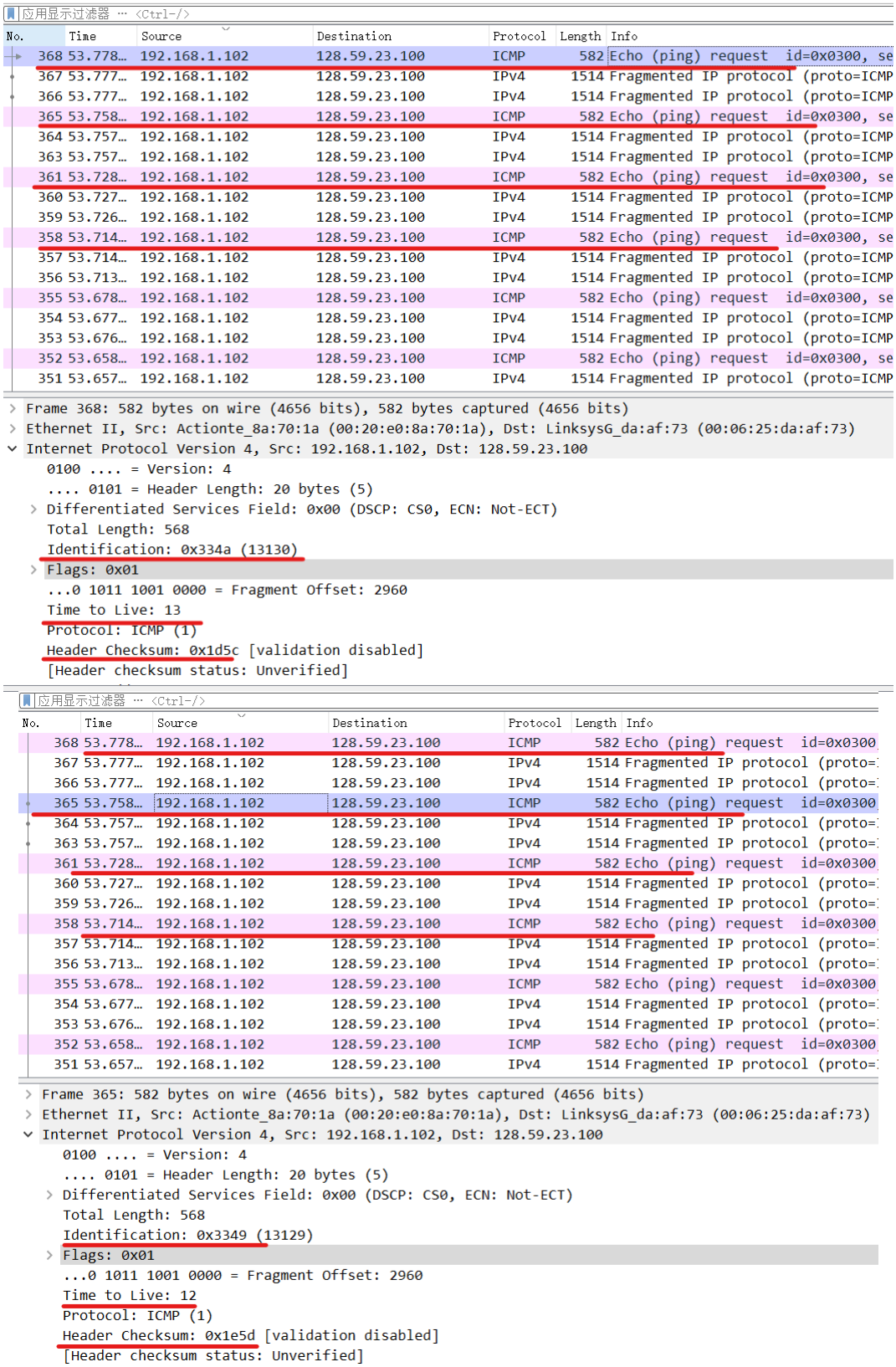
3. IP 首部一共有 **20** 字节。而有效载荷的字节数为数据报长度减去 IP 首部长度而得，所以为 $84 - 20 = 64$ 字节



4. 这个 ip 数据报并没有被分片。因为它的 flags 标志为 0，同时它的偏移量 offset 也为0，说明该数据报是第一个数据报分片也是最后一个数据报分片。所以它并没有被分片。



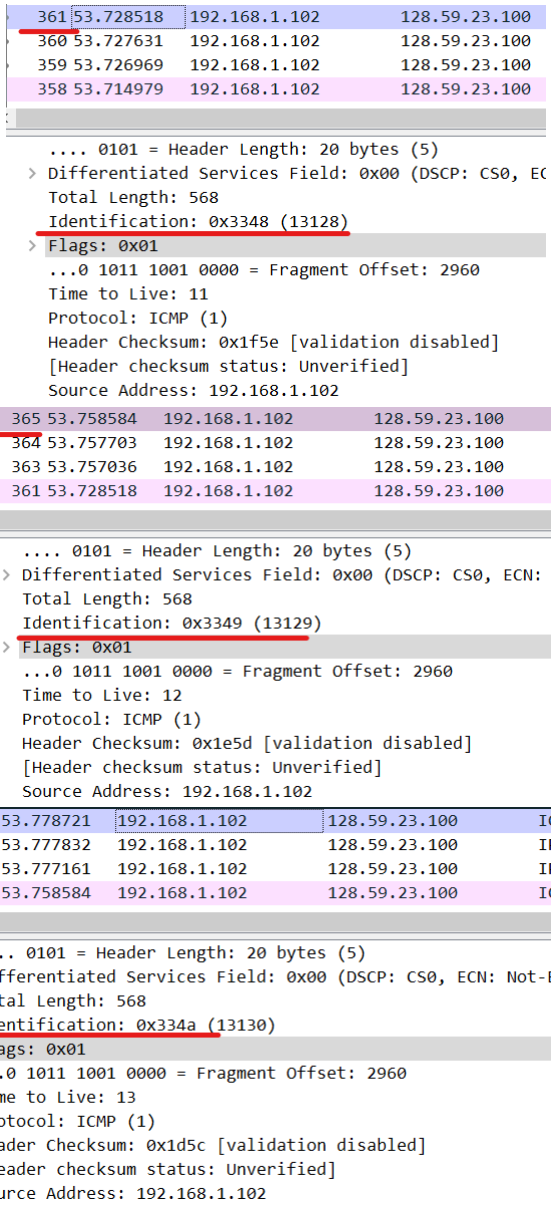
5. 从一个数据报到另一个数据报（不考虑同个数据报分片的情况）总是改变的是：**标识 Identification**，**寿命 Time-To-Live**，**首部检验和 Header Checksum**。



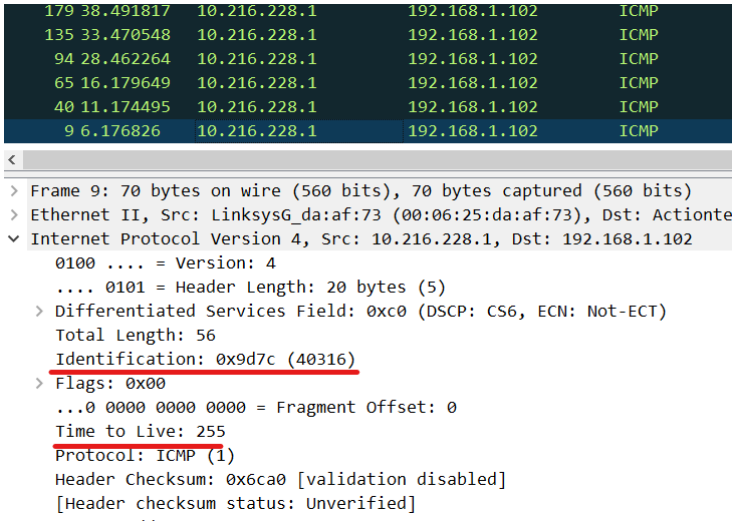
6. 这些字段一直保持不变：**版本 Version**，**首部长度 Header Length**，**源 IP**，**目的 IP**，**服务类型 Differentiated Services**，**上层协议 Protocol**。同时这些也都是必须保持不变的。而 **标识 Identification**，**寿命 Time-To-Live**，**首部检验和 Header Checksum** 都是必须变的。

   这是因为在不同数据报中，标识 Identification 是肯定要变化的，而根据实验需求，我们要通过 Traceroute 确认每个路由器的名字和它的 IP 地址，所以寿命 TTL 肯定也是需要变化的，而这些一旦变化，则首部检验和 Header Checksum 肯定也会变化。同时在进行这个服务的时候，其他字段都是不能变化的。

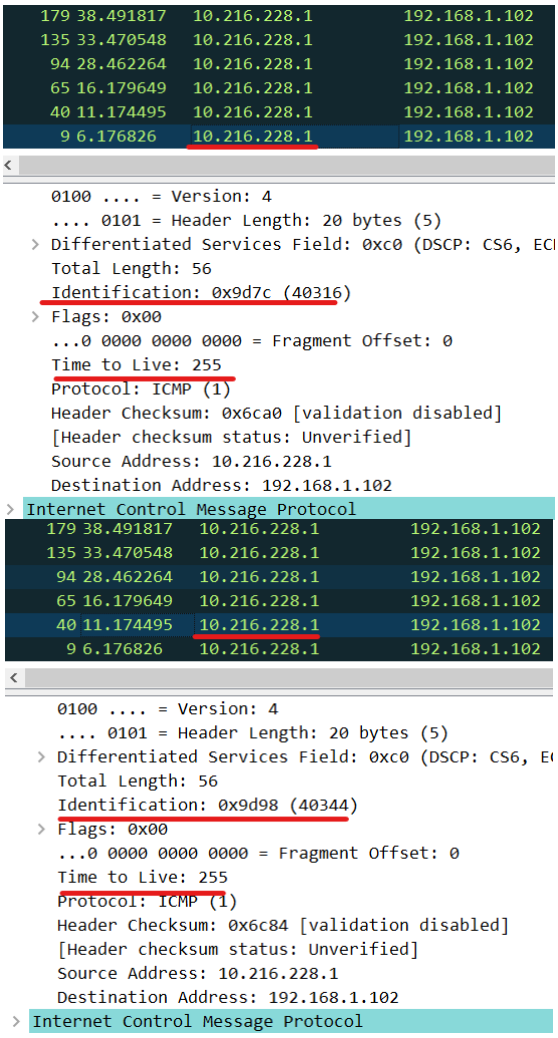
7. 该模式是 IP 首部中的标识 Identification 字段随着每个 ICMP Echo (ping) 请求而增加（从时间顺序来看）。



8. 标识 Identification 字段是 **0x9d7c（40316）**，寿命 TTL 字段是 **255**。



9. **标识 Identification 是会一直变化的，而寿命 TTL 是会保持不变的。**因为标识是一个独一无二的值，而每次返回的 ICMP TTL-exceeded 回复都是一个新的数据报，所以其标识是一直会变化的。而寿命 TTL 是保持不变是因为第一跳返回的 TTL 总是相等的。

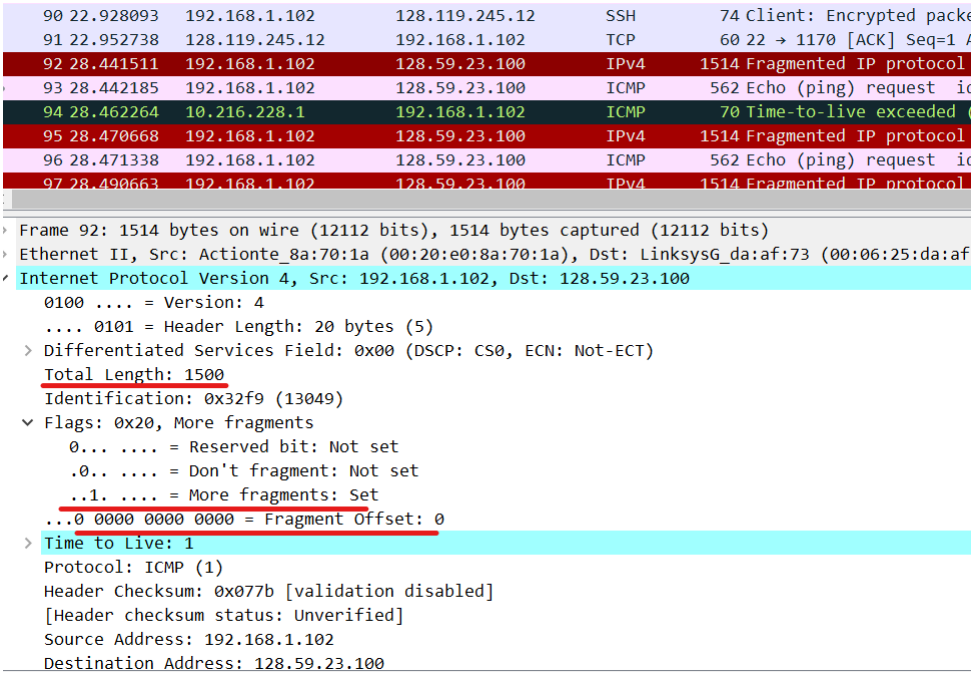


Fragment

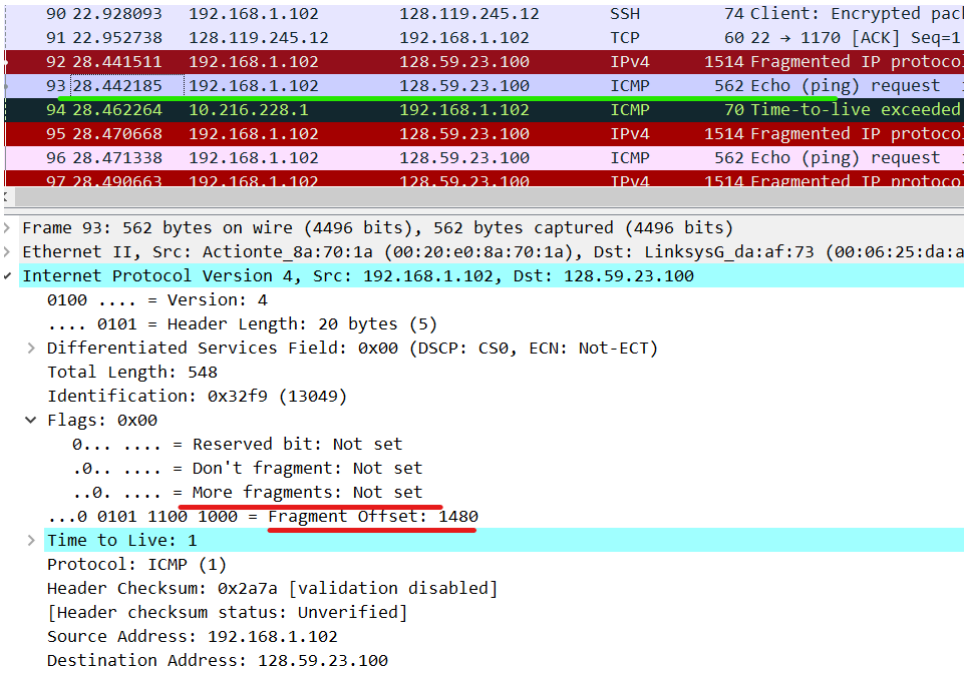
10. 可以看到，在重新发送更大报文之后，**数据报被分片了。**

No.	Time	Source	Destination	Protocol	Length	Info
85	16.438258	67.99.58.194	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to li
86	16.443310	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, s
87	16.463382	192.168.1.102	128.59.23.100	ICMP	98	Echo (ping) request id=0x0300, s
88	16.468603	128.59.1.41	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to li
89	16.499919	128.59.23.100	192.168.1.102	ICMP	98	Echo (ping) reply id=0x0300, s
90	22.928093	192.168.1.102	128.119.245.12	SSH	74	Client: Encrypted packet (len=20)
91	22.952738	128.119.245.12	192.168.1.102	TCP	60	22 → 1170 [ACK] Seq=1 Ack=21 Win=
92	28.441511	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICM
93	28.442185	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, s
94	28.462264	10.216.228.1	192.168.1.102	ICMP	70	Time-to-live exceeded (Time to li
95	28.470668	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICM
96	28.471338	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, s
97	28.490663	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICM
98	28.491323	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, s
99	28.520729	192.168.1.102	128.59.23.100	IPv4	1514	Fragmented IP protocol (proto=ICM
100	28.521393	192.168.1.102	128.59.23.100	ICMP	562	Echo (ping) request id=0x0300, s

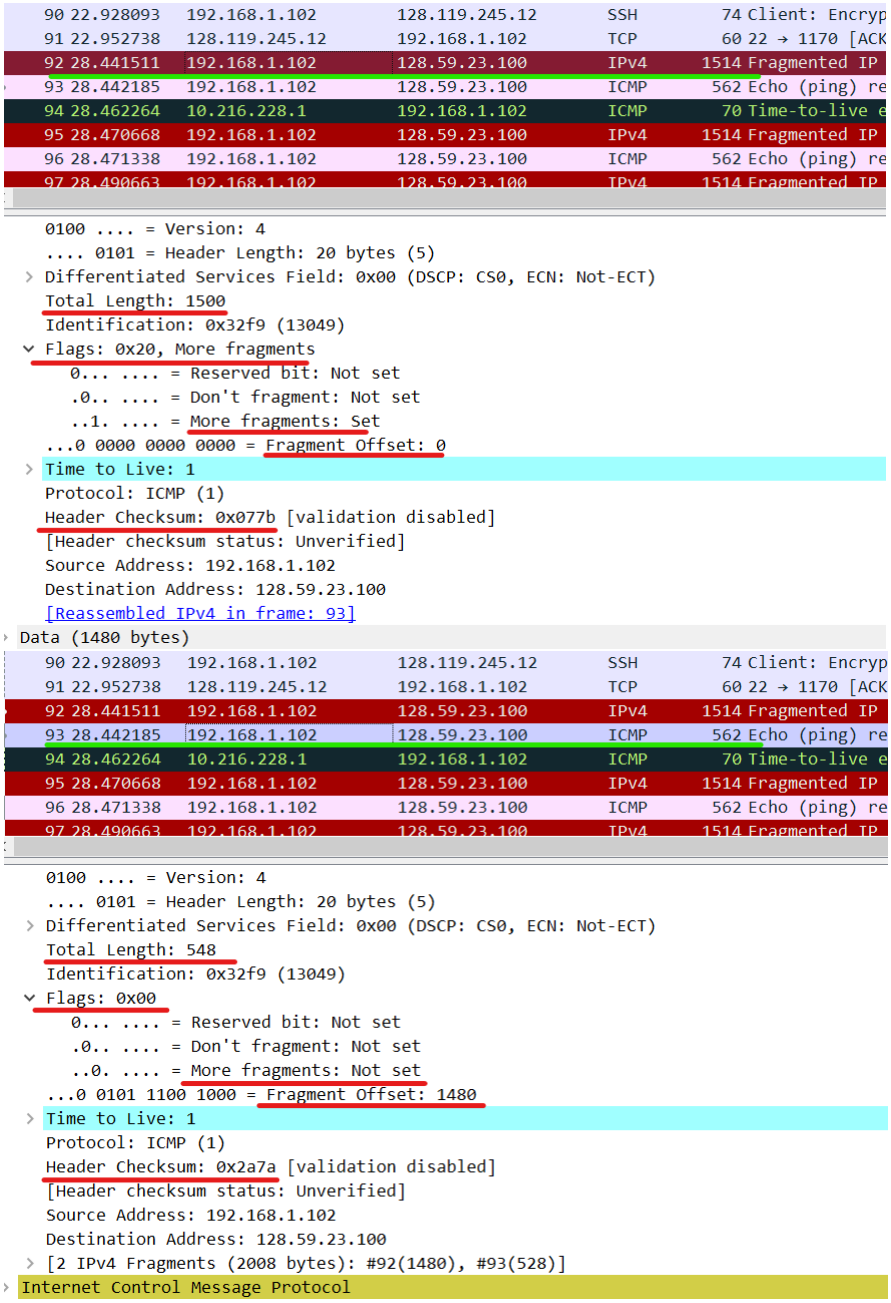
11. 可以看到，首部中的标志 Flags 被置位，其中 More Fragment 被置位为 1，说明数据报已经被分片。而其中的分片偏移量 Fragement Offset 为 0，说明**它是第一个分片，而不是最后一个分片。**同时如果它是最后一个分片的话，则它的标志位应该为 0，而不是 1。同时从数据报长度 Total Length 可以看出该数据报的长度为 **1500** 字节。



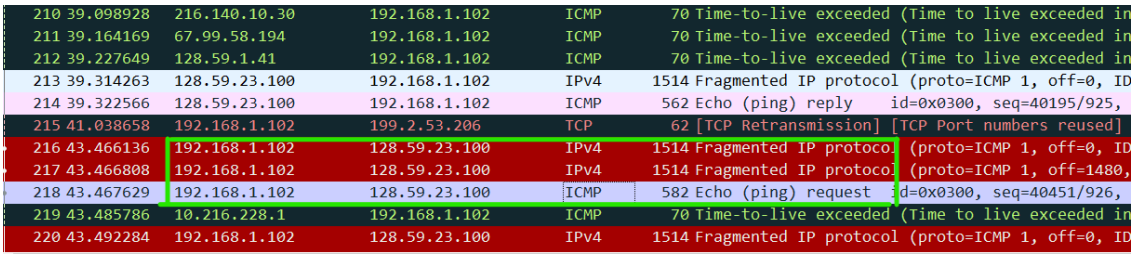
12. 从 IP 首部中的标志 Flags 可以看出，它**不是**数据报的第一个分片，因为此时它的标志为 0，表示它是最后一个分片，所以没有更多的分片。同时从它的分片偏移量 Fragement Offset 为 1480 也可以看出，它**不是**数据报的第一个分片。



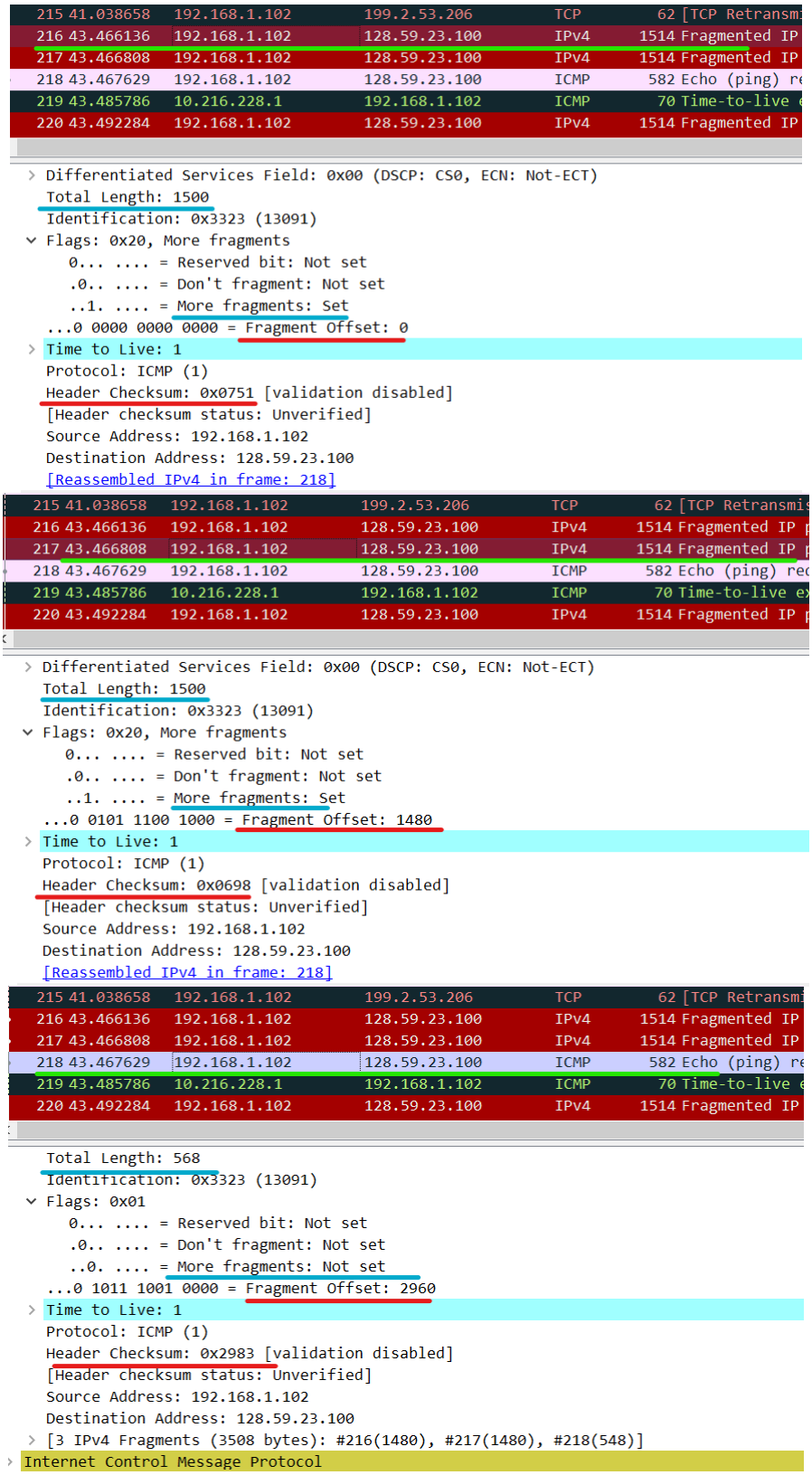
13. 两个分片之间的**数据报长度 Total Length**，**标志 Flags**，**首部检验和 Header Checksum** 有改变。



14. 会产生 **3** 个数据报分片。



15. 在这些数据报分片中都变化了的是**分片偏移量 Fragement Offset** 和 **首部检验和 Header Checksum**。而前两个分片的**数据报长度 Total Length** 和**更多分片 More Fragement** 都是一样的，分别为 1500 和 1，与最后一个分片的不一样，最后一个分片的是 568 和 0。


215 41.038658 192.168.1.102 199.2.53.206 TCP 62 [TCP Retransmi
216 43.466136 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP
217 43.466808 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP
218 43.467629 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) re
219 43.485786 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live
220 43.492284 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3323 (13091)
Flags: 0x20, 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
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]
215 41.038658 192.168.1.102 199.2.53.206 TCP 62 [TCP Retransmis
216 43.466136 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP
217 43.466808 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP
218 43.467629 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) re
219 43.485786 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live
220 43.492284 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1500
Identification: 0x3323 (13091)
Flags: 0x20, More fragments
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..1. .... = More fragments: Set
...0 0101 1100 1000 = Fragment Offset: 1480
Time to Live: 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]
215 41.038658 192.168.1.102 199.2.53.206 TCP 62 [TCP Retransmi
216 43.466136 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP
217 43.466808 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP
218 43.467629 192.168.1.102 128.59.23.100 ICMP 582 Echo (ping) re
219 43.485786 10.216.228.1 192.168.1.102 ICMP 70 Time-to-live
220 43.492284 192.168.1.102 128.59.23.100 IPv4 1514 Fragmented IP
Total Length: 568
Identification: 0x3323 (13091)
Flags: 0x01
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 1011 1001 0000 = Fragment Offset: 2960
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x2983 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.102
Destination Address: 128.59.23.100
[3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
Internet Control Message Protocol