华东师范大学数据科学与工程学院上机实践报告

课程名称：计算机网络原理与编程	年级：2018	上机实践成绩:
指导教师：张召	姓名：孙秋实	学号：10185501402
上机实践名称：Wireshark Lab: IP		上机实践日期：2020/6/1
上机实践编号：Exp8	组号：	上机实践时间：

Part 1
实验目的

- 研究 IP 协议，重点关注 IP 数据报 (IP datagram)
- 研究 IP datagram 中的各个字段 (fields)
- 详细研究 IP fragmentation 的方法

Part 2
实验任务

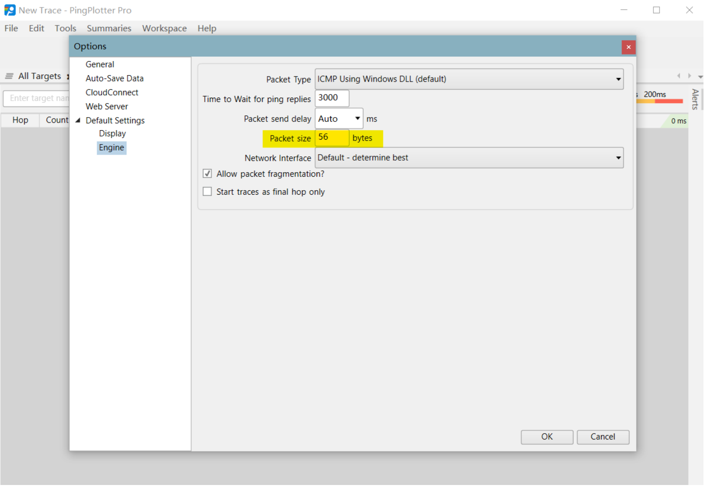
- 访问一个网站并捕获数据包
- 分析 IP 数据报

Part 3
使用环境

- Wireshark v7.0

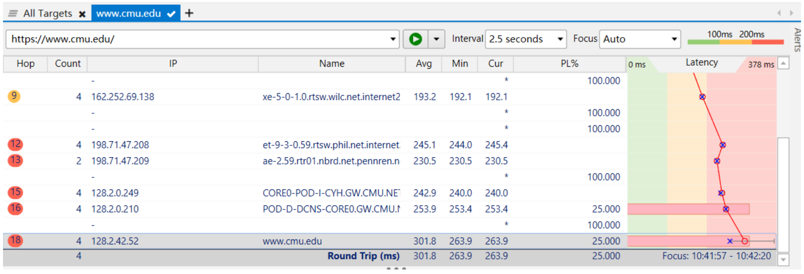
Part 4
实验过程

在一切开始前，先安装 PingPlotter，在 Option 中将包大小设置为 56bytes



Packet Type: ICMP Using Windows DLL (default)
Time to Wait for ping replies: 3000
Packet send delay: Auto ms
Packet size: 56 bytes
Network Interface: Default - determine best
☑ Allow packet fragmentation?
☐ Start traces as final hop only

然后打开 https://www.cmu.edu (卡内基 • 梅隆大学的主页) 的跟踪

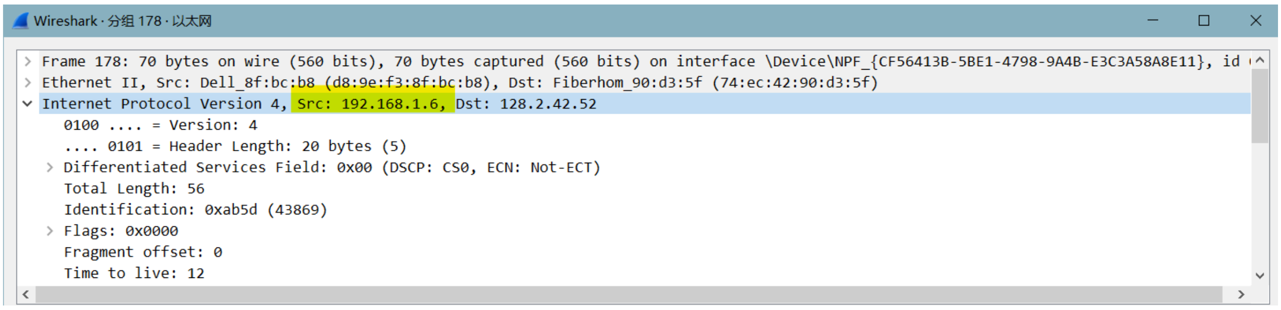


https://www.cmu.edu/ Interval 2.5 seconds Focus Auto

Hop	Count	IP	Name	Avg	Min	Cur	PL%
		-				*	100.000
9	4	162.252.69.138	xe-5-0-1.0.rtsw.wilc.net.internet2	193.2	192.1	192.1	
		-				*	100.000
		-				*	100.000
12	4	198.71.47.208	et-9-3-0.59.rtsw.phil.net.internet	245.1	244.0	245.4	
13	2	198.71.47.209	ae-2.59.rtr01.nbrd.net.pennren.n	230.5	230.5	230.5	
		-				*	100.000
15	4	128.2.0.249	CORE0-POD-I-CYH.GW.CMU.NE	242.9	240.0	240.0	
16	4	128.2.0.210	POD-D-DCNS-CORE0.GW.CMU.N	253.9	253.4	253.4	25.000
		-				*	100.000
18	4	128.2.42.52	www.cmu.edu	301.8	263.9	263.9	25.000
	4		Round Trip (ms)	301.8	263.9	263.9	25.000

Task 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.



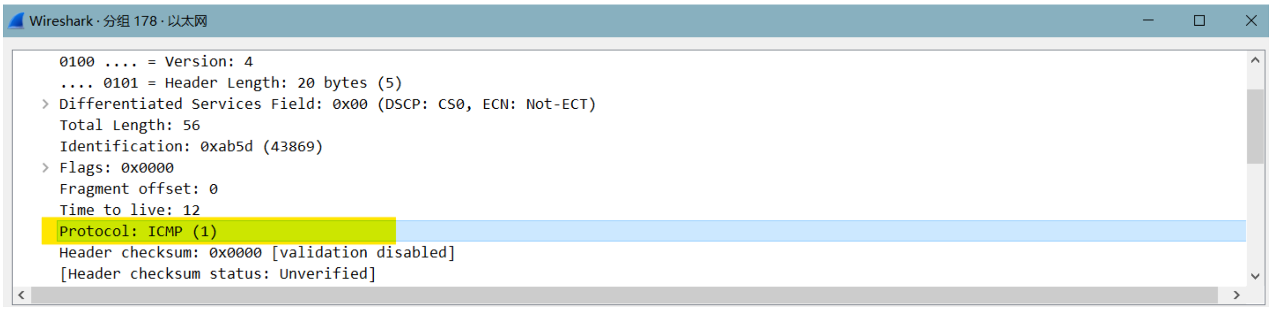
```
> Frame 178: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{CF56413B-5BE1-4798-9A4B-E3C3A58A8E11}, id
> Ethernet II, Src: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8), Dst: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f)
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.2.42.52
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xab5d (43869)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 12
```

如图所示，我的 IP 地址为 192.168.1.6

Task 2

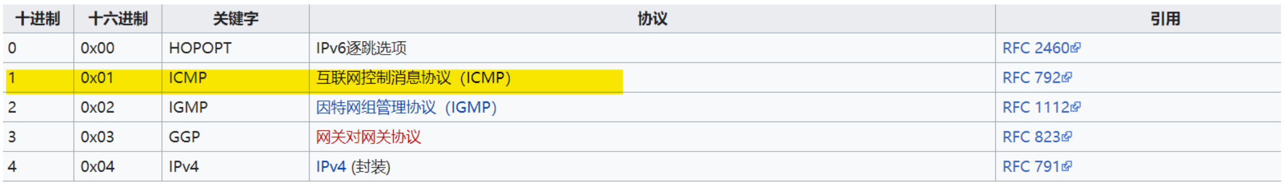
Within the IP packet header, what is the value in the upper layer protocol field?

如下图所示，上层协议是 ICMP，上层协议字段值是 1



```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xab5d (43869)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 12
    Protocol: ICMP (1)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
```

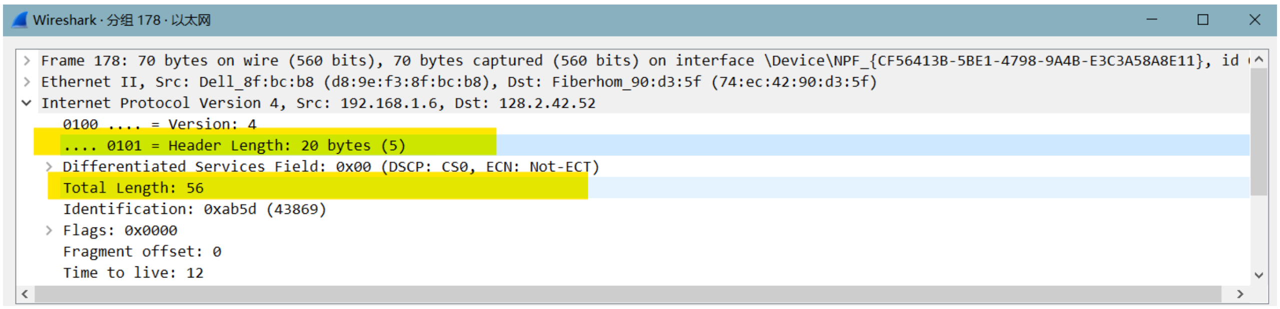
查询了协议号列表，ICMP 协议关键字值为 1



十进制	十六进制	关键字	协议	引用
0	0x00	HOPOPT	IPv6逐跳选项	RFC 2460
1	0x01	ICMP	互联网控制消息协议（ICMP）	RFC 792
2	0x02	IGMP	因特网组管理协议（IGMP）	RFC 1112
3	0x03	GGP	网关对网关协议	RFC 823
4	0x04	IPv4	IPv4 (封装)	RFC 791

Task 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.

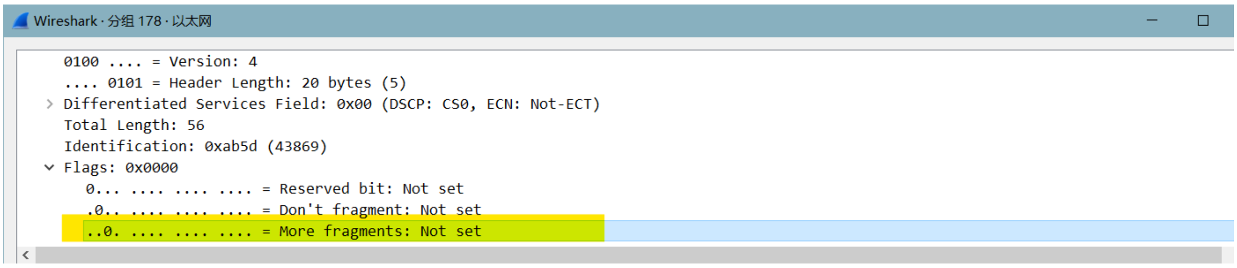


```
> Frame 178: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{CF56413B-5BE1-4798-9A4B-E3C3A58A8E11}, id
> Ethernet II, Src: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8), Dst: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f)
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.2.42.52
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xab5d (43869)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 12
```

如上图所示，IP Header 长度有 20bytes，IP 报文总长度为 56bytes，有效长度（payload）为 36bytes

Task 4

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

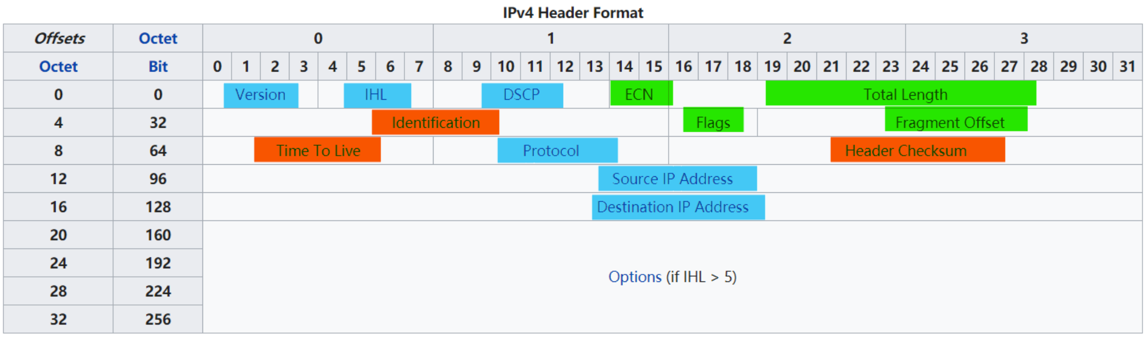


```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xab5d (43869)
  v Flags: 0x0000
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
```

More Fragments 位设位 0，故没有被分段

Task 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?



IPv4 Header Format

Offsets	Octet	0	1	2	3
Octet	Bit	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
0	0	Version IHL	DSCP ECN	Total Length	
4	32	Identification		Flags Fragment Offset	
8	64	Time To Live	Protocol	Header Checksum	
12	96	Source IP Address			
16	128	Destination IP Address			
20	160	Options (if IHL > 5)			
24	192				
28	224				
32	256				

上图为 IPv4 协议报头节构，其中橙红色部分总是改变

(1) Identification(标识符)

(2) Time To Live(存活时间)

(3) Header Checksum(报头校验和)

Task 6

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

保持不变的信息如下所示（节构如 Task5 中的图所示的蓝色部分不变，绿色部分可能下次改变）

(1) Version(版本)

(2) 发送端 IP

(3) 接收端 IP

(4) Protocol(协议)

(5) Differentiated Services(区分服务，下次可能改变)

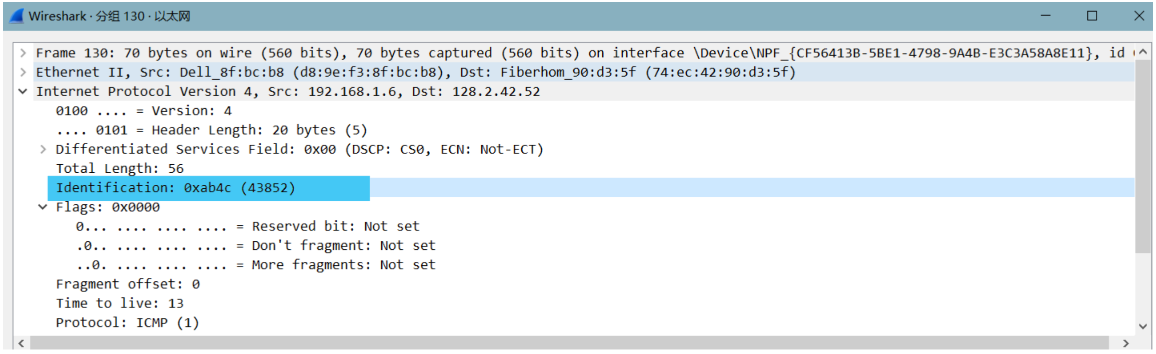
(6) Total Length(总长度，下次可能改变)

(7) Flags(标志位，下次可能改变)

Task 7

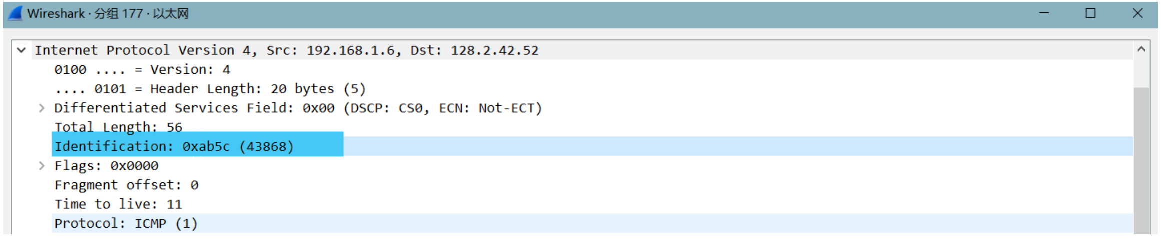
Describe the pattern you see in the values in the Identification field of the IP datagram

下图为分组 130



```
> Frame 130: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{CF56413B-5BE1-4798-9A4B-E3C3A58A8E11}, id
> Ethernet II, Src: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8), Dst: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f)
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.2.42.52
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xab4c (43852)
  v Flags: 0x0000
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..0. .... .... .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 13
    Protocol: ICMP (1)
```

下图为分组 170(发生在 130 之后)



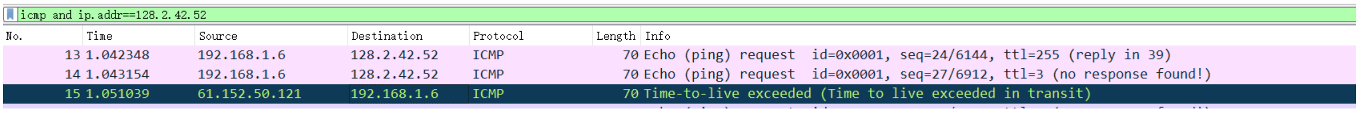
```
v Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.2.42.52
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xab5c (43868)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 11
    Protocol: ICMP (1)
```

如图所示 IP 报文头的 Identification（ID 字段）是递增的

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.

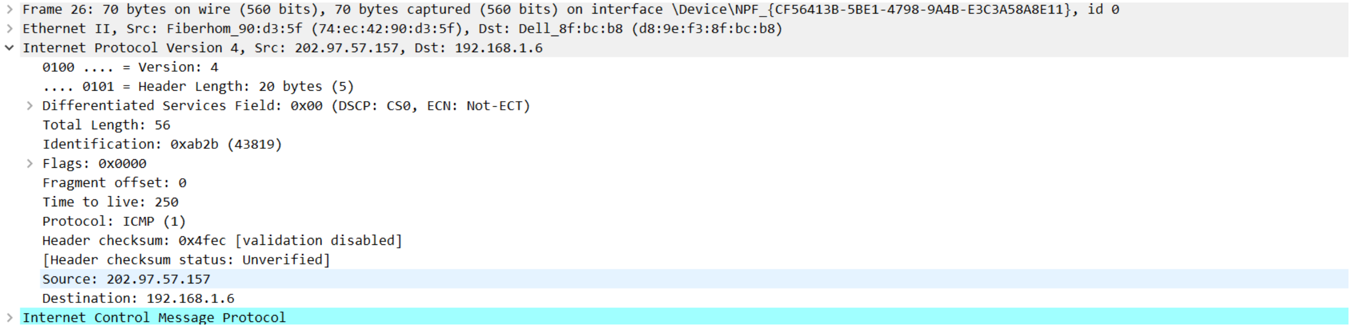
Task 8

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



```
icmp and ip.addr==128.2.42.52
No.     Time        Source          Destination     Protocol    Length Info
     13 1.042348    192.168.1.6     128.2.42.52     ICMP            70 Echo (ping) request  id=0x0001, seq=24/6144, ttl=255 (reply in 39)
     14 1.043154    192.168.1.6     128.2.42.52     ICMP            70 Echo (ping) request  id=0x0001, seq=27/6912, ttl=3 (no response found!)
     15 1.051039    61.152.50.121   192.168.1.6     ICMP            70 Time-to-live exceeded (Time to live exceeded in transit)
```

找到的第一个返回超时路由返回给我们的 IP 数据报



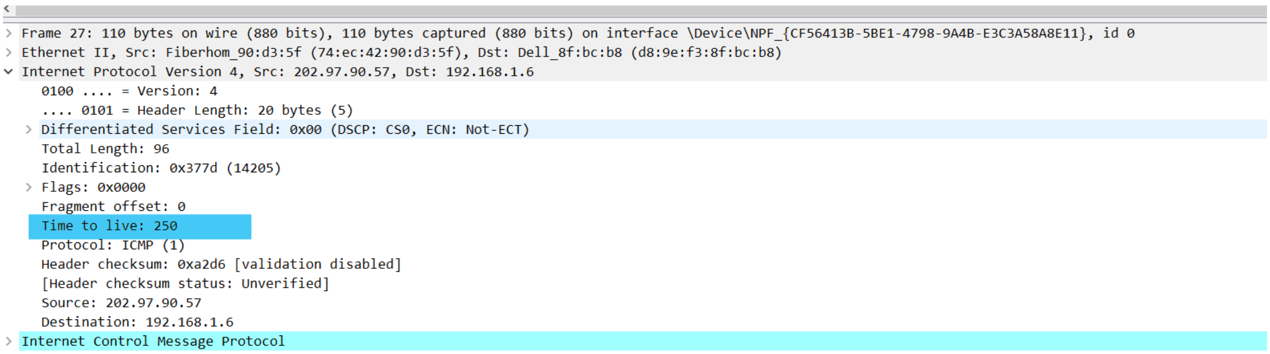
```
> Frame 26: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{CF56413B-5BE1-4798-9A4B-E3C3A58A8E11}, id 0
> Ethernet II, Src: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f), Dst: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
v Internet Protocol Version 4, Src: 202.97.57.157, Dst: 192.168.1.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0xab2b (43819)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 250
    Protocol: ICMP (1)
    Header checksum: 0x4fec [validation disabled]
    [Header checksum status: Unverified]
    Source: 202.97.57.157
    Destination: 192.168.1.6
> Internet Control Message Protocol
```

如图所示，ID 字段为 43819,TTL=250

Task 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?

观察多个超时数据报后，发现 ID 字段（Identification）对每一个超时数据报均改变，查询资料（自己抓的包没有被分段）知此处如果两个 IP 数据报拥有相同的 ID 字段，那么说明他们是一个大数据报拆分而成的，IP 数据报的 TTL 不改变（如下图所示），TTL 等于 IP 数据包能经历的最大跳（hop）数，而非数据包传输时间

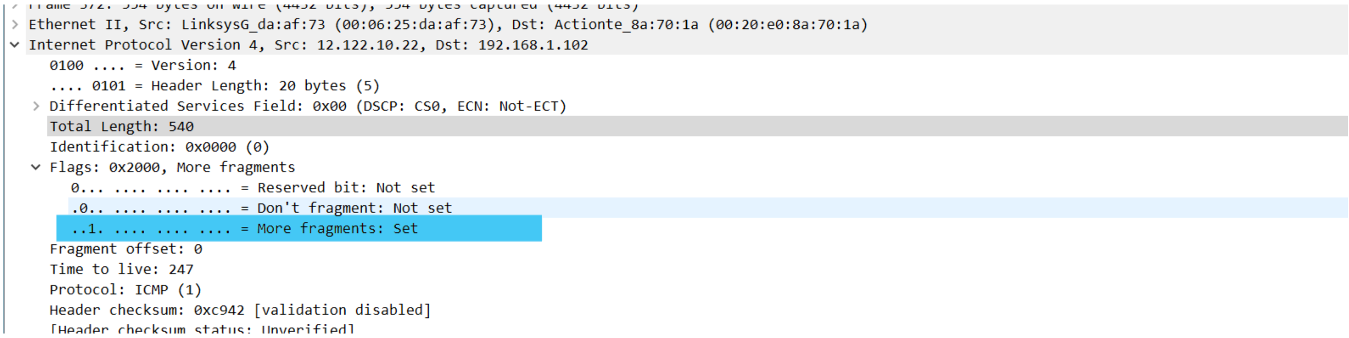


```
> Frame 27: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{CF56413B-5BE1-4798-9A4B-E3C3A58A8E11}, id 0
> Ethernet II, Src: Fiberhom_90:d3:5f (74:ec:42:90:d3:5f), Dst: Dell_8f:bc:b8 (d8:9e:f3:8f:bc:b8)
v Internet Protocol Version 4, Src: 202.97.90.57, Dst: 192.168.1.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 96
    Identification: 0x377d (14205)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 250
    Protocol: ICMP (1)
    Header checksum: 0xa2d6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 202.97.90.57
    Destination: 192.168.1.6
> Internet Control Message Protocol
```

因为我自己抓到的包没有出现数据包被分割的情况，所以开始跟踪作者已经抓取好的包

Task 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?



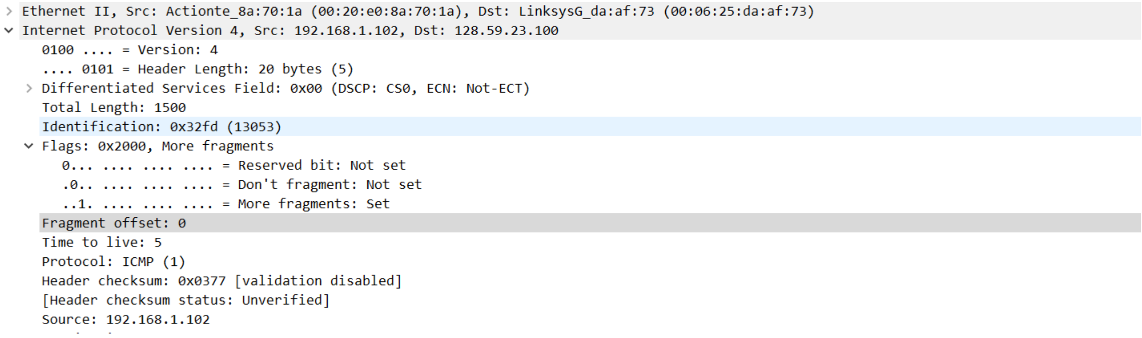
```
> Frame 572: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Actionte_8a:70:1a (00:20:e0:8a:70:1a)
v Internet Protocol Version 4, Src: 12.122.10.22, Dst: 192.168.1.102
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 540
    Identification: 0x0000 (0)
  v Flags: 0x2000, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
    Fragment offset: 0
    Time to live: 247
    Protocol: ICMP (1)
    Header checksum: 0xc942 [validation disabled]
    [Header checksum status: Unverified]
```

如图所示，这个消息已经碎片化为 ≥2 个数据报

Task 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?

如图所示，抓取到的第一个碎片数据报长度为 1500（1514=1500+14bytes 以太网头），观察 offset==0 可知这是前一个片段

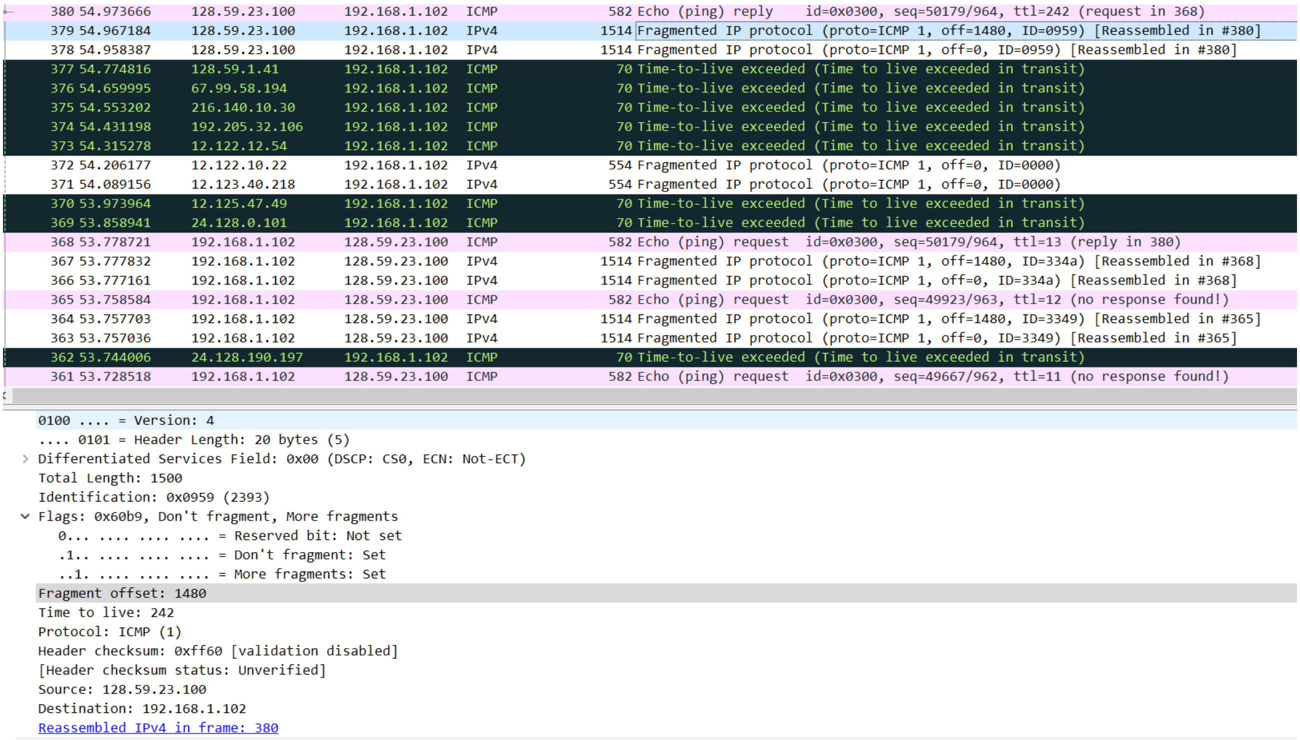


```
> Ethernet II, Src: Actionte_8a:70:1a (00:20:e0:8a:70:1a), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
v Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x32fd (13053)
  v Flags: 0x2000, More fragments
      0... .... .... .... = Reserved bit: Not set
      .0.. .... .... .... = Don't fragment: Not set
      ..1. .... .... .... = More fragments: Set
    Fragment offset: 0
    Time to live: 5
    Protocol: ICMP (1)
    Header checksum: 0x0377 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
```

Task 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?

在抓包结果中寻找



```
380 54.973666  128.59.23.100   192.168.1.102  ICMP   582 Echo (ping) reply    id=0x0300, seq=50179/964, ttl=242 (request in 368)
379 54.967184  128.59.23.100   192.168.1.102  IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=0959) [Reassembled in #380]
378 54.958387  128.59.23.100   192.168.1.102  IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0959) [Reassembled in #380]
377 54.774816  128.59.1.41     192.168.1.102  ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
376 54.659995  67.99.58.194    192.168.1.102  ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
375 54.553202  216.140.10.30   192.168.1.102  ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
374 54.431198  192.205.32.106  192.168.1.102  ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
373 54.315278  12.122.12.54    192.168.1.102  ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
372 54.206177  12.122.10.22    192.168.1.102  IPv4   554 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
371 54.089156  12.123.40.218   192.168.1.102  IPv4   554 Fragmented IP protocol (proto=ICMP 1, off=0, ID=0000)
370 53.973964  12.125.47.49    192.168.1.102  ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
369 53.858941  24.128.0.101    192.168.1.102  ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
368 53.778721  192.168.1.102   128.59.23.100  ICMP   582 Echo (ping) request  id=0x0300, seq=50179/964, ttl=13 (reply in 380)
367 53.777832  192.168.1.102   128.59.23.100  IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=334a) [Reassembled in #368]
366 53.777161  192.168.1.102   128.59.23.100  IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=334a) [Reassembled in #368]
365 53.758584  192.168.1.102   128.59.23.100  ICMP   582 Echo (ping) request  id=0x0300, seq=49923/963, ttl=12 (no response found!)
364 53.757703  192.168.1.102   128.59.23.100  IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3349) [Reassembled in #365]
363 53.757036  192.168.1.102   128.59.23.100  IPv4  1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=3349) [Reassembled in #365]
362 53.744006  24.128.190.197  192.168.1.102  ICMP    70 Time-to-live exceeded (Time to live exceeded in transit)
361 53.728518  192.168.1.102   128.59.23.100  ICMP   582 Echo (ping) request  id=0x0300, seq=49667/962, ttl=11 (no response found!)

    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x0959 (2393)
  v Flags: 0x60b9, Don't fragment, More fragments
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..1. .... .... .... = More fragments: Set
    Fragment offset: 1480
    Time to live: 242
    Protocol: ICMP (1)
    Header checksum: 0xff60 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.59.23.100
    Destination: 192.168.1.102
    Reassembled IPv4 in frame: 380
```

如上图所示，offset 为 1480，是第二个碎片，more fragments 的状态是 set，所以认为在该碎片后至少还有一个碎片。

Task 13

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

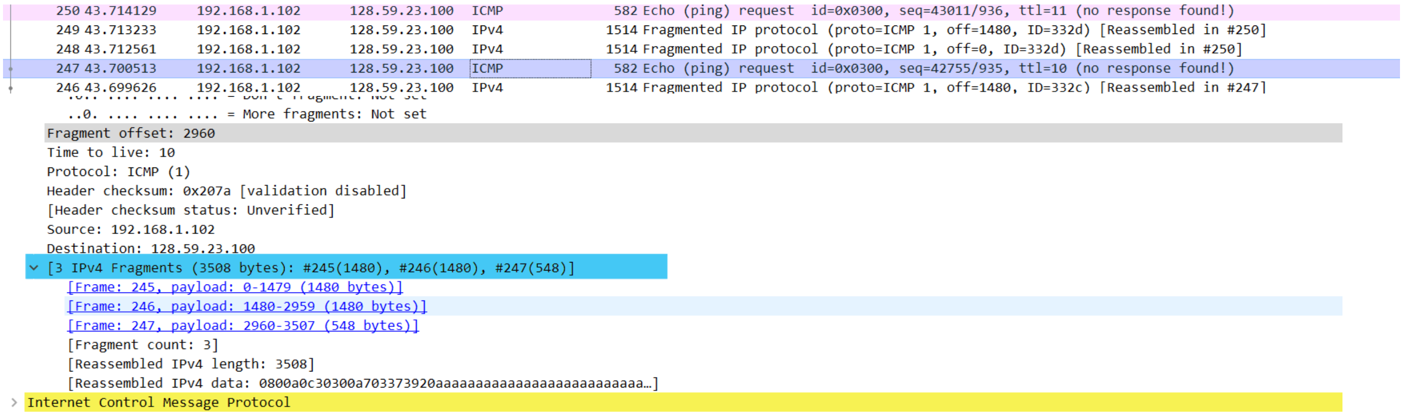
如 Task13 和 Task13 的截图所示，ID 字段，标志位和 checksum 发生了变化

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

Task 14

How many fragments were created from the original datagram?

如下图所示，切换到 3500 后，从原始数据报创建 3 个片段



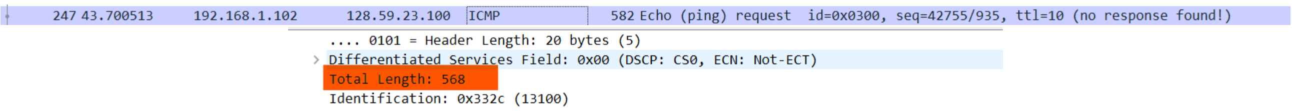
```
 250 43.714129   192.168.1.102    128.59.23.100   ICMP      582 Echo (ping) request  id=0x0300, seq=43011/936, ttl=11 (no response found!)
 249 43.713233   192.168.1.102    128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=332d) [Reassembled in #250]
 248 43.712561   192.168.1.102    128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=332d) [Reassembled in #250]
 247 43.700513   192.168.1.102    128.59.23.100   ICMP      582 Echo (ping) request  id=0x0300, seq=42755/935, ttl=10 (no response found!)
 246 43.699626   192.168.1.102    128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=332c) [Reassembled in #247]
       .0.. .... .... .... = Don't fragment: Not set
       ..0. .... .... .... = More fragments: Not set
     Fragment offset: 2960
     Time to live: 10
     Protocol: ICMP (1)
     Header checksum: 0x207a [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.102
     Destination: 128.59.23.100
   ⌄ [3 IPv4 Fragments (3508 bytes): #245(1480), #246(1480), #247(548)]
       [Frame: 245, payload: 0-1479 (1480 bytes)]
       [Frame: 246, payload: 1480-2959 (1480 bytes)]
       [Frame: 247, payload: 2960-3507 (548 bytes)]
       [Fragment count: 3]
       [Reassembled IPv4 length: 3508]
       [Reassembled IPv4 data: 0800a0c30300a703373920aaaaaaaaaaaaaaaaaaaaaaaa…]
 > Internet Control Message Protocol
```

Task 15

What fields change in the IP header among the fragments?

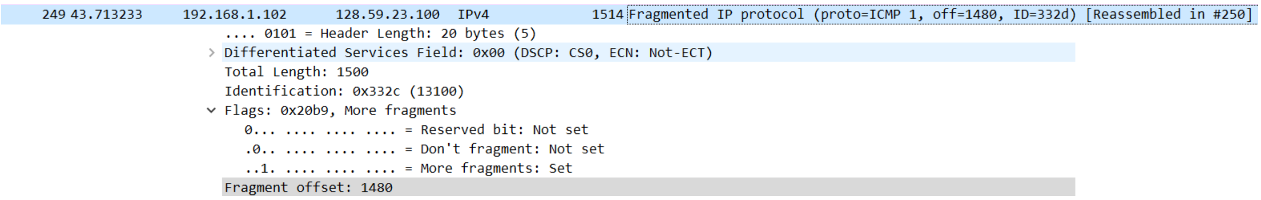
截取了一个 total length 改变的例子

(1)Length=568



```
 247 43.700513   192.168.1.102    128.59.23.100   ICMP      582 Echo (ping) request  id=0x0300, seq=42755/935, ttl=10 (no response found!)
                                    .... 0101 = Header Length: 20 bytes (5)
                                  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
                                    Total Length: 568
                                    Identification: 0x332c (13100)
```

(2)Length=1500



```
 249 43.713233   192.168.1.102    128.59.23.100   IPv4     1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=332d) [Reassembled in #250]
                           .... 0101 = Header Length: 20 bytes (5)
                         > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
                           Total Length: 1500
                           Identification: 0x332c (13100)
                         ⌄ Flags: 0x20b9, More fragments
                             0... .... .... .... = Reserved bit: Not set
                             .0.. .... .... .... = Don't fragment: Not set
                             ..1. .... .... .... = More fragments: Set
                           Fragment offset: 1480
```

片段中 IP 标头中发生变化的字段有

(1) Fragment offset（每个碎片的位移）

(2) Checksum

(3) Total Length