计算机网络实验作业 4

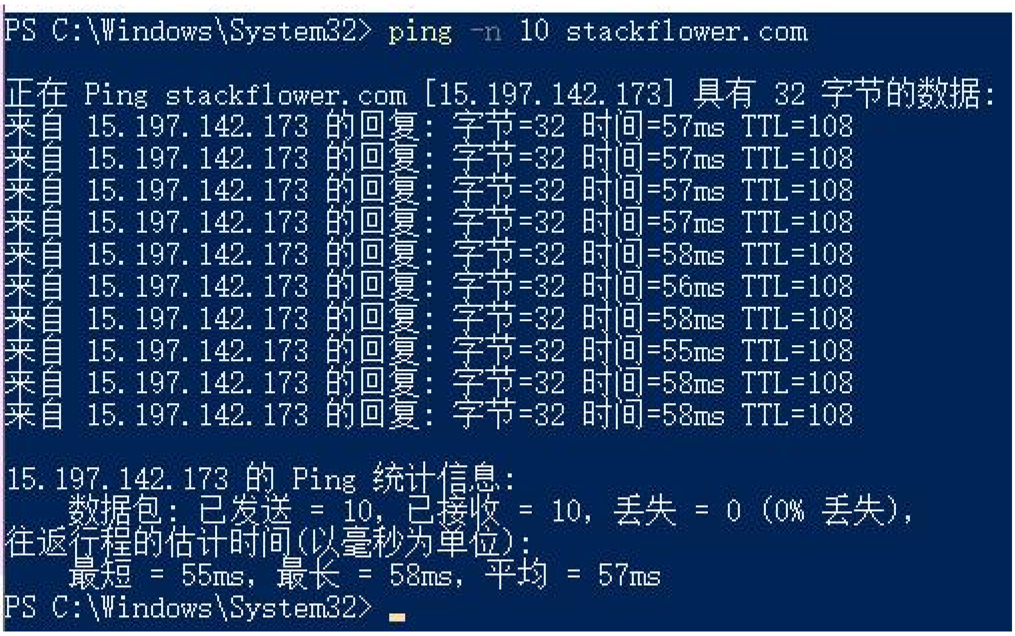
学号：19020011038　姓名：岳宇轩

一．ICMP and Ping

打开 wireshark，在 C:\Windows\System32 下打开 windows powershell 窗口，键入：

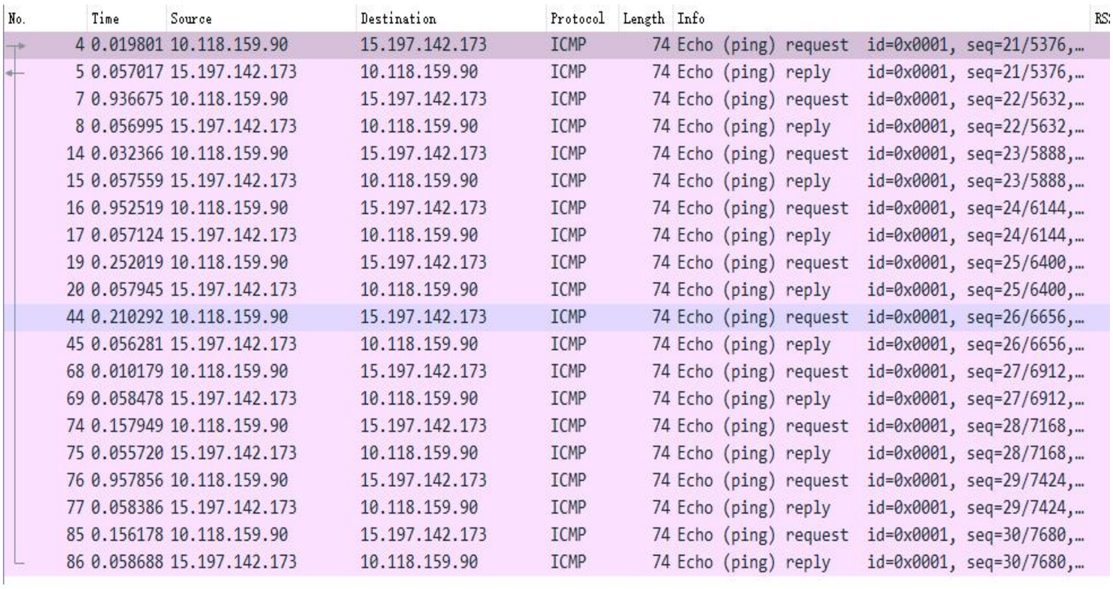
ping -n 10 stackflower.com，

得到下图所示结果：



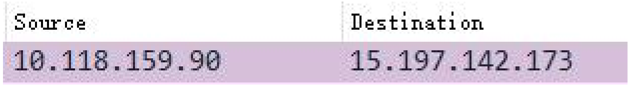
```
PS C:\Windows\System32> ping -n 10 stackflower.com

正在 Ping stackflower.com [15.197.142.173] 具有 32 字节的数据:
来自 15.197.142.173 的回复: 字节=32 时间=57ms TTL=108
来自 15.197.142.173 的回复: 字节=32 时间=57ms TTL=108
来自 15.197.142.173 的回复: 字节=32 时间=57ms TTL=108
来自 15.197.142.173 的回复: 字节=32 时间=57ms TTL=108
来自 15.197.142.173 的回复: 字节=32 时间=58ms TTL=108
来自 15.197.142.173 的回复: 字节=32 时间=56ms TTL=108
来自 15.197.142.173 的回复: 字节=32 时间=58ms TTL=108
来自 15.197.142.173 的回复: 字节=32 时间=55ms TTL=108
来自 15.197.142.173 的回复: 字节=32 时间=58ms TTL=108
来自 15.197.142.173 的回复: 字节=32 时间=58ms TTL=108

15.197.142.173 的 Ping 统计信息:
    数据包: 已发送 = 10, 已接收 = 10, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 55ms, 最长 = 58ms, 平均 = 57ms
PS C:\Windows\System32>
```

停止 wireshark 抓包，查看 ICMP 分组如下：



No.	Time	Source	Destination	Protocol	Length	Info	RS:
4	0.019801	10.118.159.90	15.197.142.173	ICMP	74	Echo (ping) request id=0x0001, seq=21/5376,…	
5	0.057017	15.197.142.173	10.118.159.90	ICMP	74	Echo (ping) reply id=0x0001, seq=21/5376,…	
7	0.936675	10.118.159.90	15.197.142.173	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632,…	
8	0.056995	15.197.142.173	10.118.159.90	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632,…	
14	0.032366	10.118.159.90	15.197.142.173	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888,…	
15	0.057559	15.197.142.173	10.118.159.90	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888,…	
16	0.952519	10.118.159.90	15.197.142.173	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144,…	
17	0.057124	15.197.142.173	10.118.159.90	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144,…	
19	0.252019	10.118.159.90	15.197.142.173	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400,…	
20	0.057945	15.197.142.173	10.118.159.90	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400,…	
44	0.210292	10.118.159.90	15.197.142.173	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656,…	
45	0.056281	15.197.142.173	10.118.159.90	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656,…	
68	0.010179	10.118.159.90	15.197.142.173	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912,…	
69	0.058478	15.197.142.173	10.118.159.90	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912,…	
74	0.157949	10.118.159.90	15.197.142.173	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168,…	
75	0.055720	15.197.142.173	10.118.159.90	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168,…	
76	0.957856	10.118.159.90	15.197.142.173	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424,…	
77	0.058386	15.197.142.173	10.118.159.90	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424,…	
85	0.156178	10.118.159.90	15.197.142.173	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680,…	
86	0.058688	15.197.142.173	10.118.159.90	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680,…	

1.What is the IP address of your host? What is the lP address of the destination host?



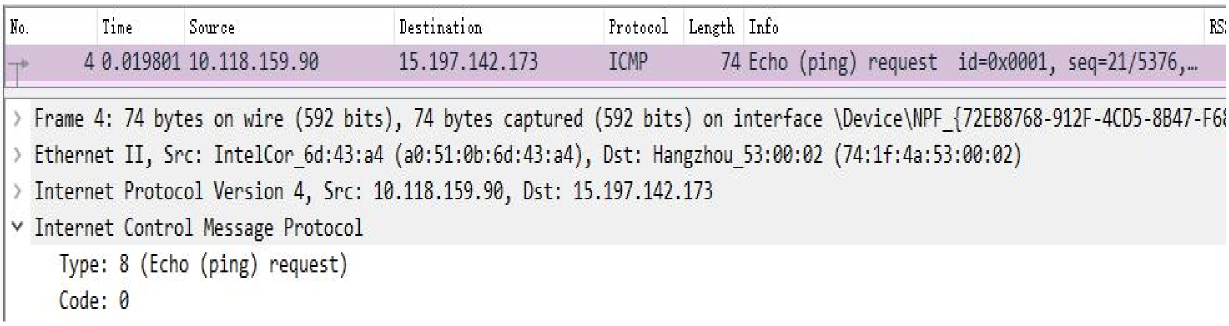
Source	Destination
10.118.159.90	15.197.142.173

通过 wiresharp 抓取的包中的 source 字段和 destination 字段分析可知，本机 IP 地址为 10.118.159.90,stackflower 的 IP 地址是 15.197.142.173

2.Why is it that an ICMP packet does not have source and destination port numbers?

ICMP 是 IP 层的协议，ICMP 报文直接封装到 IP 数据报中，而端口号是运输层才有的,网络层是没有端口，所以 ICMP 包里没有源地址和目的地址的端口号。

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? Howmany bytes are the checksum, sequence number and identifier fields?

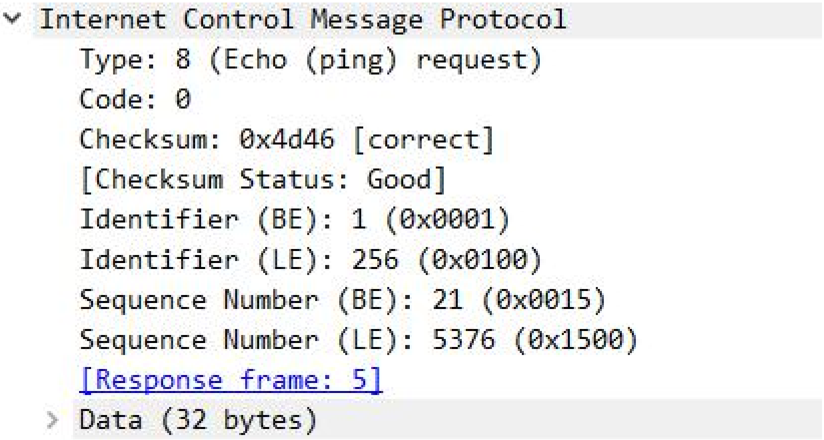


```
No.    Time      Source         Destination     Protocol  Length  Info                                              RS
     4 0.019801  10.118.159.90  15.197.142.173  ICMP          74  Echo (ping) request  id=0x0001, seq=21/5376,…

> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{72EB8768-912F-4CD5-8B47-F6
> Ethernet II, Src: IntelCor_6d:43:a4 (a0:51:0b:6d:43:a4), Dst: Hangzhou_53:00:02 (74:1f:4a:53:00:02)
> Internet Protocol Version 4, Src: 10.118.159.90, Dst: 15.197.142.173
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

ICMP type: 8(Echo(ping)request)

Code:0

ICMP 请求分组含有的其他字段:



```
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d46 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 21 (0x0015)
    Sequence Number (LE): 5376 (0x1500)
    [Response frame: 5]
  > Data (32 bytes)
```

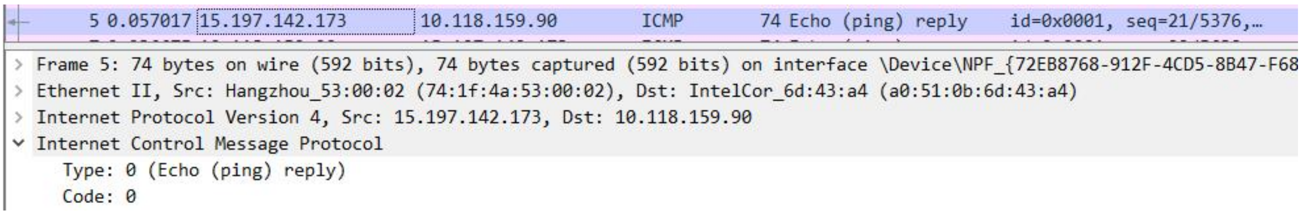
Checksum:校验和 2 字节

Idenifier:标识符 2 字节

Sequence Number:序列号 2 字节

Data:数据 32 字节

4. Examine the corresponding ping reply packet. What are the ICMP type and codenumbers? What other fields does this ICMP packet have?How many bytes are thechecksum, sequence number and identifier fields?

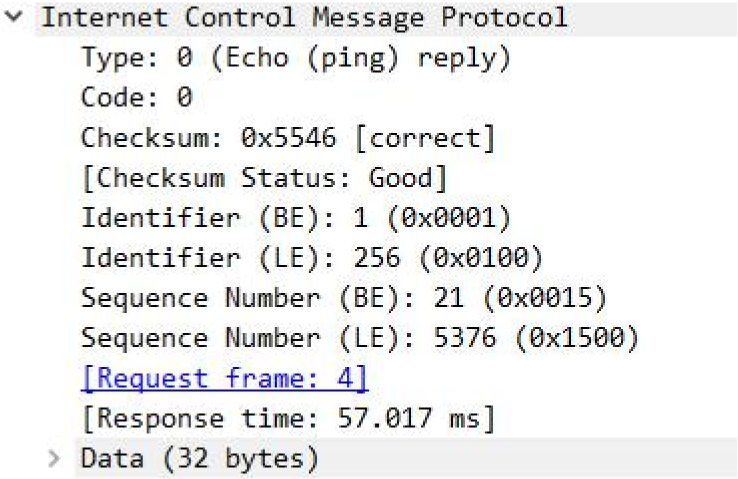


```
      5 0.057017 15.197.142.173        10.118.159.90         ICMP         74 Echo (ping) reply     id=0x0001, seq=21/5376,…
> Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{72EB8768-912F-4CD5-8B47-F68
> Ethernet II, Src: Hangzhou_53:00:02 (74:1f:4a:53:00:02), Dst: IntelCor_6d:43:a4 (a0:51:0b:6d:43:a4)
> Internet Protocol Version 4, Src: 15.197.142.173, Dst: 10.118.159.90
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
```

ICMP type: 0 (Echo(ping) reply)

Code:0

ICMP 应答分组含有的其他字段：



```
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5546 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 21 (0x0015)
    Sequence Number (LE): 5376 (0x1500)
    [Request frame: 4]
    [Response time: 57.017 ms]
  > Data (32 bytes)
```

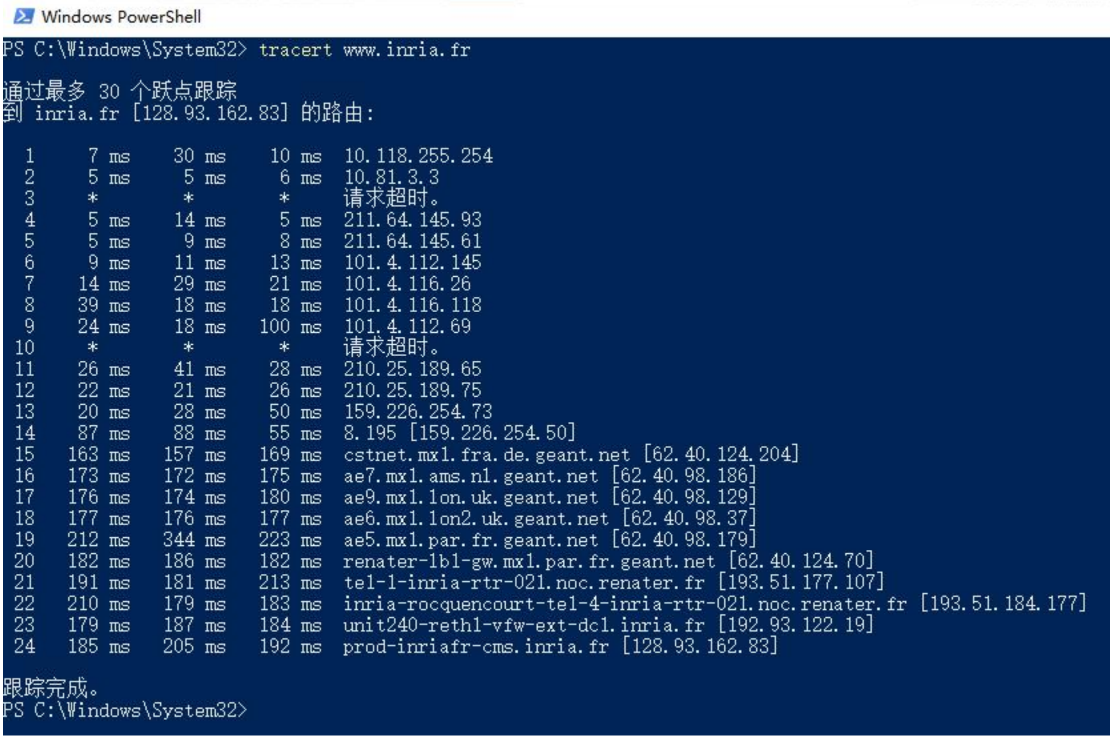
Checksum:校验和 2 字节

Identifier:标识符 2 字节

Sequence Number:序列号 2 字节

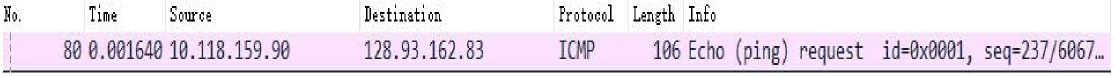
Data:数据 32 字节

二． ICMP and Traceroute



```
PS C:\Windows\System32> tracert www.inria.fr

通过最多 30 个跃点跟踪
到 inria.fr [128.93.162.83] 的路由:

  1     7 ms    30 ms    10 ms  10.118.255.254
  2     5 ms     5 ms     6 ms  10.81.3.3
  3     *        *        *     请求超时。
  4     5 ms    14 ms     5 ms  211.64.145.93
  5     5 ms     9 ms     8 ms  211.64.145.61
  6     9 ms    11 ms    13 ms  101.4.112.145
  7    14 ms    29 ms    21 ms  101.4.116.26
  8    39 ms    18 ms    18 ms  101.4.116.118
  9    24 ms    18 ms   100 ms  101.4.112.69
 10     *        *        *     请求超时。
 11    26 ms    41 ms    28 ms  210.25.189.65
 12    22 ms    21 ms    26 ms  210.25.189.75
 13    20 ms    28 ms    50 ms  159.226.254.73
 14    87 ms    88 ms    55 ms  8.195 [159.226.254.50]
 15   163 ms   157 ms   169 ms  cstnet.mx1.fra.de.geant.net [62.40.124.204]
 16   173 ms   172 ms   175 ms  ae7.mx1.ams.nl.geant.net [62.40.98.186]
 17   176 ms   174 ms   180 ms  ae9.mx1.lon.uk.geant.net [62.40.98.129]
 18   177 ms   176 ms   177 ms  ae6.mx1.lon2.uk.geant.net [62.40.98.37]
 19   212 ms   344 ms   223 ms  ae5.mx1.par.fr.geant.net [62.40.98.179]
 20   182 ms   186 ms   182 ms  renater-lb1-gw.mx1.par.fr.geant.net [62.40.124.70]
 21   191 ms   181 ms   213 ms  tel-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 22   210 ms   179 ms   183 ms  inria-rocquencourt-tel-4-inria-rtr-021.noc.renater.fr [193.51.184.177]
 23   179 ms   187 ms   184 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 24   185 ms   205 ms   192 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

跟踪完成。
PS C:\Windows\System32>
```

5. What is the IP address of your host? What is the IP address of the target destination host?



No.	Time	Source	Destination	Protocol	Length	Info
80	0.001640	10.118.159.90	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=237/6067…

my host: 10.118.159.90

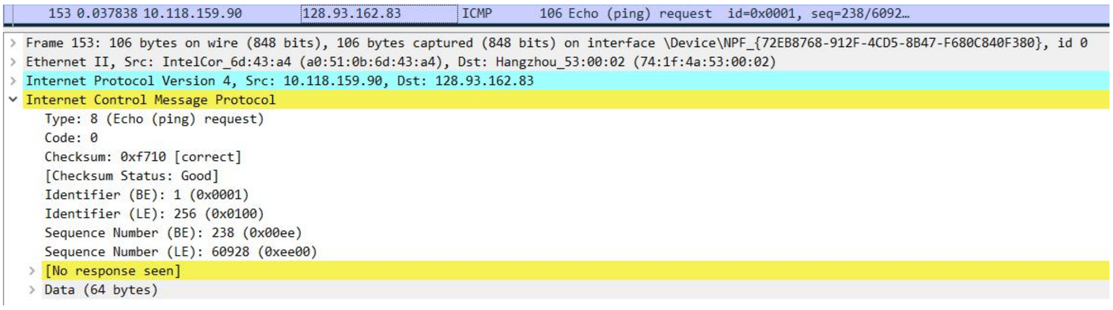
target destination host: 128.93.162.83

6.If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

有不同的协议号

如果 ICMP 发送 UDP 数据报,IP 协议号应该为 0x11.十进制为 17,表明交给 UDP。

7.Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?

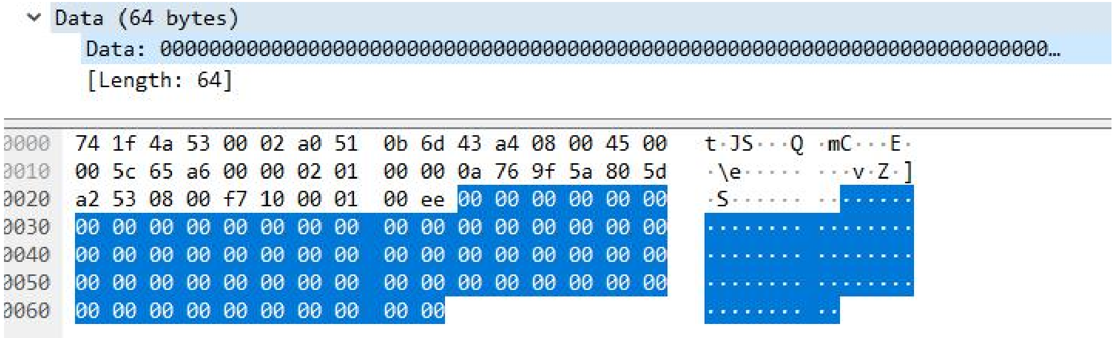


```
   153 0.037838 10.118.159.90        128.93.162.83        ICMP      106 Echo (ping) request  id=0x0001, seq=238/6092…
> Frame 153: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{72EB8768-912F-4CD5-8B47-F680C840F380}, id 0
> Ethernet II, Src: IntelCor_6d:43:a4 (a0:51:0b:6d:43:a4), Dst: Hangzhou_53:00:02 (74:1f:4a:53:00:02)
> Internet Protocol Version 4, Src: 10.118.159.90, Dst: 128.93.162.83
v Internet Control Message Protocol
     Type: 8 (Echo (ping) request)
     Code: 0
     Checksum: 0xf710 [correct]
     [Checksum Status: Good]
     Identifier (BE): 1 (0x0001)
     Identifier (LE): 256 (0x0100)
     Sequence Number (BE): 238 (0x00ee)
     Sequence Number (LE): 60928 (0xee00)
   > [No response seen]
   > Data (64 bytes)
```

字段是一致的，包内容是不同的

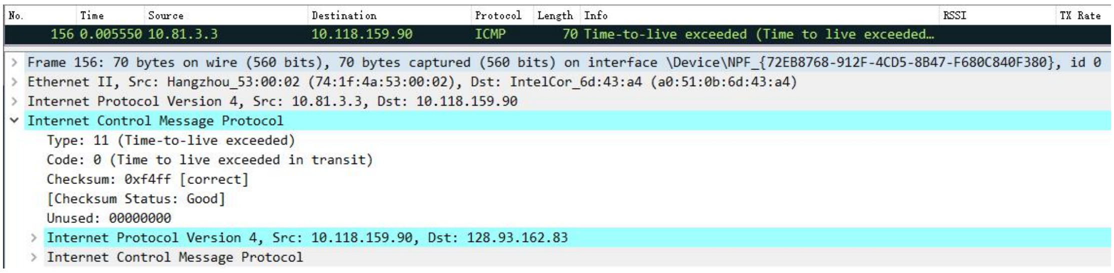
ICMP 报文的格式为 1 个字节的 type，1 个字节的 code,2 个字节的 checksum，4 个字节的由类型决定的部分 option，以及剩下的数据部分 data。由于 type 是 8/0，那么由类型决定的部分就是 2 个字节的 identifier 和 2 个字节的 sequence。所以只要协议类型相同，那么包包含的字段就是相同的。

这里的数据部分全部都是 0。(checksum, sequence 一般每个包都不同，identifier MacOS/Linux 和进程号相同, Windows 固定)



```
v Data (64 bytes)
     Data: 000000000000000000000000000000000000000000000000000000000000000000000000…
     [Length: 64]

0000  74 1f 4a 53 00 02 a0 51  0b 6d 43 a4 08 00 45 00   t·JS···Q ·mC···E·
0010  00 5c 65 a6 00 00 02 01  00 00 0a 76 9f 5a 80 5d   ·\e····· ···v·Z·]
0020  a2 53 08 00 f7 10 00 01  00 ee 00 00 00 00 00 00   ·S······ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··
```

8.Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet.What is included in those fields?

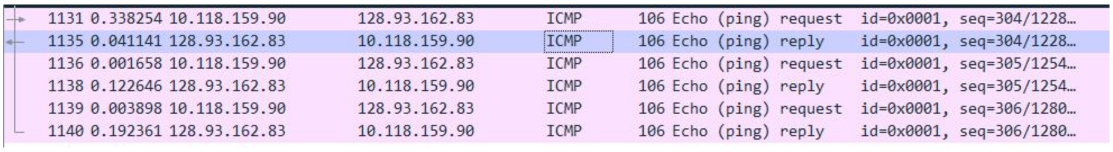


```
No.   Time     Source      Destination    Protocol Length Info                                                RSSI   TX Rate
  156 0.005550 10.81.3.3   10.118.159.90  ICMP         70 Time-to-live exceeded (Time to live exceeded…

> Frame 156: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{72EB8768-912F-4CD5-8B47-F680C840F380}, id 0
> Ethernet II, Src: Hangzhou_53:00:02 (74:1f:4a:53:00:02), Dst: IntelCor_6d:43:a4 (a0:51:0b:6d:43:a4)
> Internet Protocol Version 4, Src: 10.81.3.3, Dst: 10.118.159.90
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 10.118.159.90, Dst: 128.93.162.83
  > Internet Control Message Protocol
```

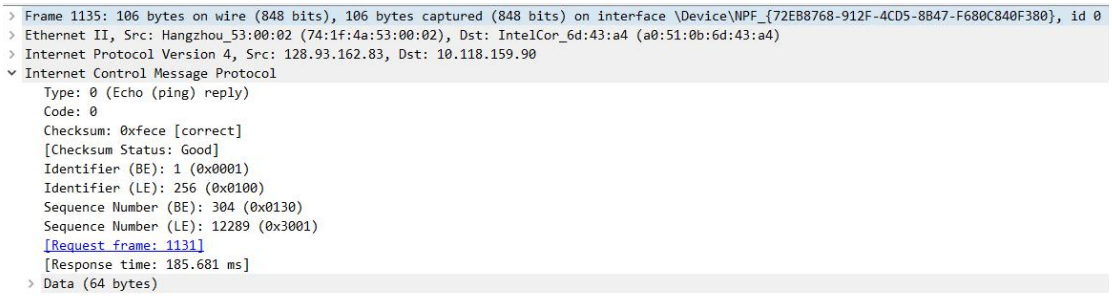
ICMP 错误数据报包括;所有 IP 字段和原来的 ICMP 字段。

只不过这里的 type 为 11，表示 time-to-live exceeded TTL 过期, code 是 0，由类型决定的部分为全 0 的填充，数据部分为 TTL 减至 0 的那个 IP 报文的全部。

9. Examine the last three ICMP packets received by the source host. How are thesepackets different from the ICMP error packets? Why are they different?



```
1131 0.338254 10.118.159.90   128.93.162.83   ICMP   106 Echo (ping) request  id=0x0001, seq=304/1228…
1135 0.041141 128.93.162.83   10.118.159.90   ICMP   106 Echo (ping) reply    id=0x0001, seq=304/1228…
1136 0.001658 10.118.159.90   128.93.162.83   ICMP   106 Echo (ping) request  id=0x0001, seq=305/1254…
1138 0.122646 128.93.162.83   10.118.159.90   ICMP   106 Echo (ping) reply    id=0x0001, seq=305/1254…
1139 0.003898 10.118.159.90   128.93.162.83   ICMP   106 Echo (ping) request  id=0x0001, seq=306/1280…
1140 0.192361 128.93.162.83   10.118.159.90   ICMP   106 Echo (ping) reply    id=0x0001, seq=306/1280…
```

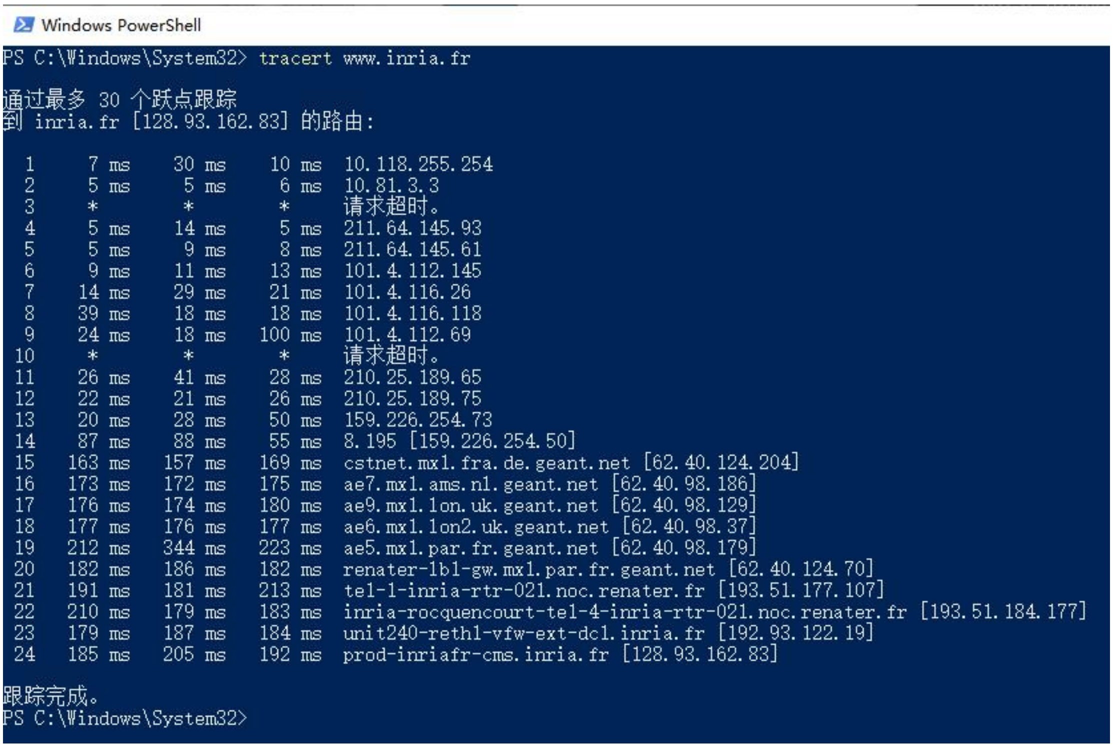


```
> Frame 1135: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{72EB8768-912F-4CD5-8B47-F680C840F380}, id 0
> Ethernet II, Src: Hangzhou_53:00:02 (74:1f:4a:53:00:02), Dst: IntelCor_6d:43:a4 (a0:51:0b:6d:43:a4)
> Internet Protocol Version 4, Src: 128.93.162.83, Dst: 10.118.159.90
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xfece [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 304 (0x0130)
    Sequence Number (LE): 12289 (0x3001)
    [Request frame: 1131]
    [Response time: 185.681 ms]
  > Data (64 bytes)
```

最后三个 ICMP reply 数据报的 Type 和 Code 都是 0，表示回显回答，而不是 11 (TTL 过期)，在 TTL 为 24 时恰能把包送到目的地址

10. Within the tracert measurements, is there a link whose delay is

significantlylonger than others?Refer to the screenshot in Figure 4, is there a link whosedelay is significantly longer than others? On the basis of the router names, canyou guess the location of the two routers on the end of this link?



```
PS C:\Windows\System32> tracert www.inria.fr

通过最多 30 个跃点跟踪
到 inria.fr [128.93.162.83] 的路由:

  1     7 ms    30 ms    10 ms  10.118.255.254
  2     5 ms     5 ms     6 ms  10.81.3.3
  3     *        *        *     请求超时。
  4     5 ms    14 ms     5 ms  211.64.145.93
  5     5 ms     9 ms     8 ms  211.64.145.61
  6     9 ms    11 ms    13 ms  101.4.112.145
  7    14 ms    29 ms    21 ms  101.4.116.26
  8    39 ms    18 ms    18 ms  101.4.116.118
  9    24 ms    18 ms   100 ms  101.4.112.69
 10     *        *        *     请求超时。
 11    26 ms    41 ms    28 ms  210.25.189.65
 12    22 ms    21 ms    26 ms  210.25.189.75
 13    20 ms    28 ms    50 ms  159.226.254.73
 14    87 ms    88 ms    55 ms  8.195 [159.226.254.50]
 15   163 ms   157 ms   169 ms  cstnet.mx1.fra.de.geant.net [62.40.124.204]
 16   173 ms   172 ms   175 ms  ae7.mx1.ams.nl.geant.net [62.40.98.186]
 17   176 ms   174 ms   180 ms  ae9.mx1.lon.uk.geant.net [62.40.98.129]
 18   177 ms   176 ms   177 ms  ae6.mx1.lon2.uk.geant.net [62.40.98.37]
 19   212 ms   344 ms   223 ms  ae5.mx1.par.fr.geant.net [62.40.98.179]
 20   182 ms   186 ms   182 ms  renater-lb1-gw.mx1.par.fr.geant.net [62.40.124.70]
 21   191 ms   181 ms   213 ms  tel-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 22   210 ms   179 ms   183 ms  inria-rocquencourt-tel-4-inria-rtr-021.noc.renater.fr [193.51.184.177]
 23   179 ms   187 ms   184 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 24   185 ms   205 ms   192 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

跟踪完成。
PS C:\Windows\System32>
```

从上图可以看出第 18 跳到第 19 跳延迟最大

62.40.98.37 法国巴黎

62.40.98.179 英国

这条链接连接法国巴黎的路由器和英国的路由器