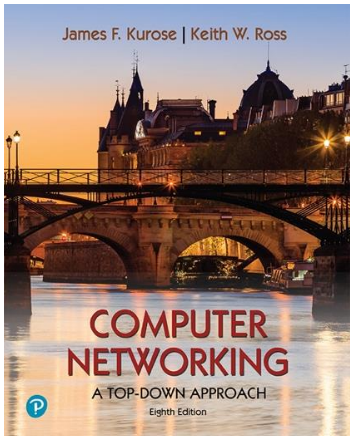
Wireshark Lab:
ICMP v8.0

Supplement to *Computer Networking: A Top-Down Approach*, *8th ed.*, J.F. Kurose and K.W. Ross

“Tell me and I forget. Show me and I remember. Involve me and I understand.” Chinese proverb

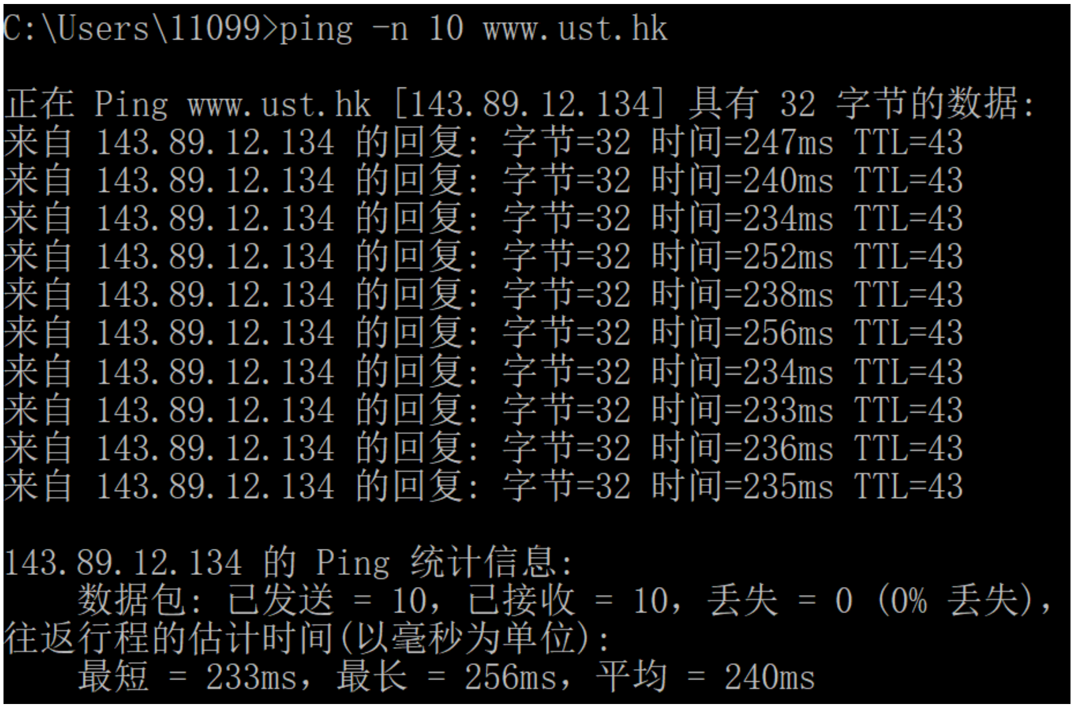


0. Academic integrity

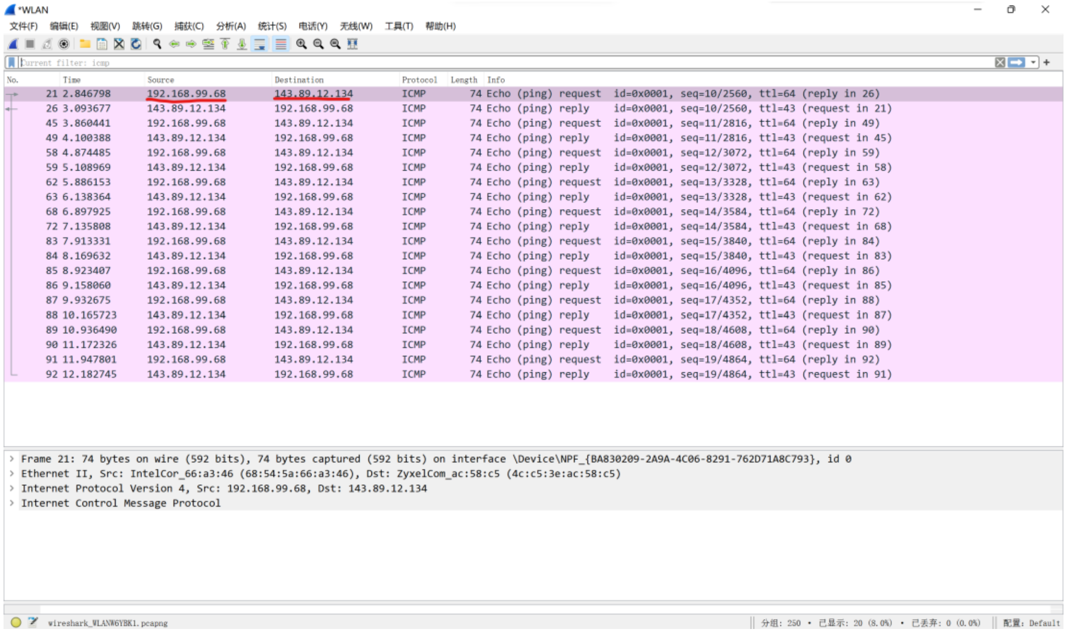
I have read and understood the course academic integrity policy.

1. ICMP and Ping

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



```
C:\Users\11099>ping -n 10 www.ust.hk

正在 Ping www.ust.hk [143.89.12.134] 具有 32 字节的数据:
来自 143.89.12.134 的回复: 字节=32 时间=247ms TTL=43
来自 143.89.12.134 的回复: 字节=32 时间=240ms TTL=43
来自 143.89.12.134 的回复: 字节=32 时间=234ms TTL=43
来自 143.89.12.134 的回复: 字节=32 时间=252ms TTL=43
来自 143.89.12.134 的回复: 字节=32 时间=238ms TTL=43
来自 143.89.12.134 的回复: 字节=32 时间=256ms TTL=43
来自 143.89.12.134 的回复: 字节=32 时间=234ms TTL=43
来自 143.89.12.134 的回复: 字节=32 时间=233ms TTL=43
来自 143.89.12.134 的回复: 字节=32 时间=236ms TTL=43
来自 143.89.12.134 的回复: 字节=32 时间=235ms TTL=43

143.89.12.134 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 = 233ms，最长 = 256ms，平均 = 240ms
```


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Current filter: icmp

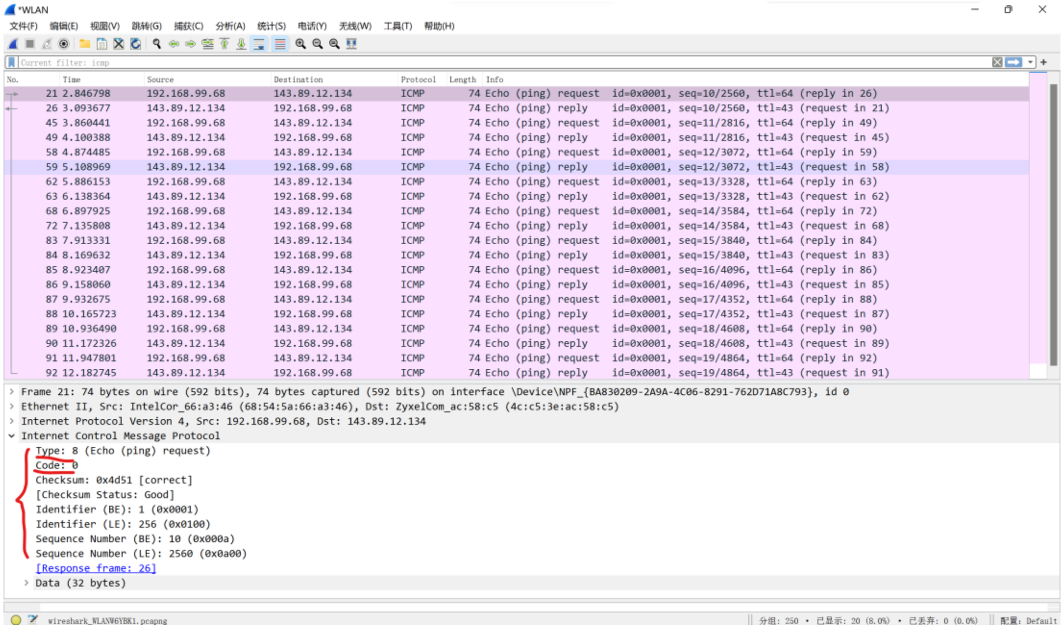
```
No.   Time        Source          Destination     Protocol Length Info
   21 2.846798    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=10/2560, ttl=64 (reply in 26)
   26 3.093677    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=10/2560, ttl=43 (request in 21)
   45 3.860441    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=11/2816, ttl=64 (reply in 49)
   49 4.100388    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=11/2816, ttl=43 (request in 45)
   58 4.874485    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=12/3072, ttl=64 (reply in 59)
   59 5.108969    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=12/3072, ttl=43 (request in 58)
   62 5.886153    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=64 (reply in 63)
   63 6.138364    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=13/3328, ttl=43 (request in 62)
   68 6.897925    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=14/3584, ttl=64 (reply in 72)
   72 7.135808    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=14/3584, ttl=43 (request in 68)
   83 7.913331    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=15/3840, ttl=64 (reply in 84)
   84 8.169632    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=15/3840, ttl=43 (request in 83)
   85 8.923407    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=16/4096, ttl=64 (reply in 86)
   86 9.158060    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=16/4096, ttl=43 (request in 85)
   87 9.932675    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=17/4352, ttl=64 (reply in 88)
   88 10.165723   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=17/4352, ttl=43 (request in 87)
   89 10.936490   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=18/4608, ttl=64 (reply in 90)
   90 11.172326   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=18/4608, ttl=43 (request in 89)
   91 11.947801   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=19/4864, ttl=64 (reply in 92)
   92 12.182745   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=19/4864, ttl=43 (request in 91)

> Frame 21: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{BA830209-2A9A-4C06-8291-762D71A8C793}, id 0
> Ethernet II, Src: IntelCor_66:a3:46 (68:54:5a:66:a3:46), Dst: ZyxelCom_ac:58:c5 (4c:c5:3e:ac:58:c5)
> Internet Protocol Version 4, Src: 192.168.99.68, Dst: 143.89.12.134
> Internet Control Message Protocol

wireshark_WLANW6YBK1.pcapng        分组: 250 • 已显示: 20 (8.0%) • 已丢弃: 0 (0.0%)   配置: Default
```

The IP address of my host is 192.168.99.68, and the IP address of the destination host is 141.89.12.134.

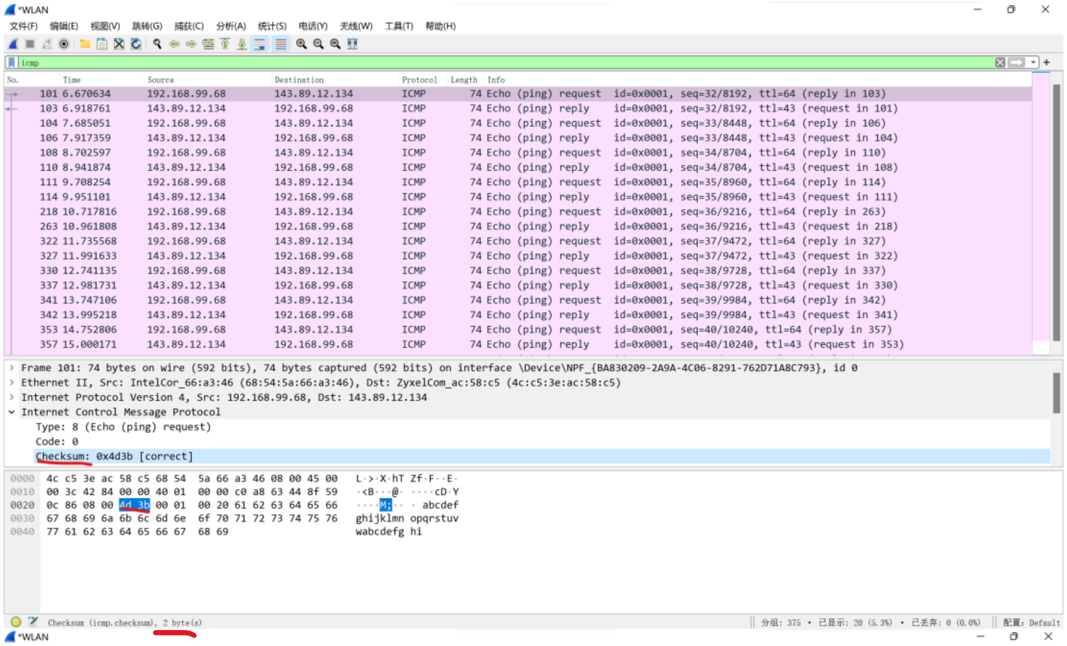
2. Why is it that an ICMP packet does not have source and destination port numbers?

   ICMP doesn’t care TCP or UDP information. It is an IP-dependent protocol, and it only use IP datagram.

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? How many bytes are the checksum, sequence number and identifier fields?


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Current filter: icmp

```
No.   Time        Source          Destination     Protocol Length Info
   21 2.846798    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=10/2560, ttl=64 (reply in 26)
   26 3.093677    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=10/2560, ttl=43 (request in 21)
   45 3.860441    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=11/2816, ttl=64 (reply in 49)
   49 4.100388    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=11/2816, ttl=43 (request in 45)
   58 4.874485    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=12/3072, ttl=64 (reply in 59)
   59 5.108969    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=12/3072, ttl=43 (request in 58)
   62 5.886153    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=64 (reply in 63)
   63 6.138364    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=13/3328, ttl=43 (request in 62)
   68 6.897925    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=14/3584, ttl=64 (reply in 72)
   72 7.135808    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=14/3584, ttl=43 (request in 68)
   83 7.913331    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=15/3840, ttl=64 (reply in 84)
   84 8.169632    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=15/3840, ttl=43 (request in 83)
   85 8.923407    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=16/4096, ttl=64 (reply in 86)
   86 9.158060    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=16/4096, ttl=43 (request in 85)
   87 9.932675    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=17/4352, ttl=64 (reply in 88)
   88 10.165723   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=17/4352, ttl=43 (request in 87)
   89 10.936490   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=18/4608, ttl=64 (reply in 90)
   90 11.172326   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=18/4608, ttl=43 (request in 89)
   91 11.947801   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=19/4864, ttl=64 (reply in 92)
   92 12.182745   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=19/4864, ttl=43 (request in 91)

> Frame 21: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{BA830209-2A9A-4C06-8291-762D71A8C793}, id 0
> Ethernet II, Src: IntelCor_66:a3:46 (68:54:5a:66:a3:46), Dst: ZyxelCom_ac:58:c5 (4c:c5:3e:ac:58:c5)
> Internet Protocol Version 4, Src: 192.168.99.68, Dst: 143.89.12.134
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d51 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 10 (0x000a)
    Sequence Number (LE): 2560 (0x0a00)
    [Response frame: 26]
  > Data (32 bytes)

wireshark_WLANW6YBK1.pcapng        分组: 250 • 已显示: 20 (8.0%) • 已丢弃: 0 (0.0%)   配置: Default
```

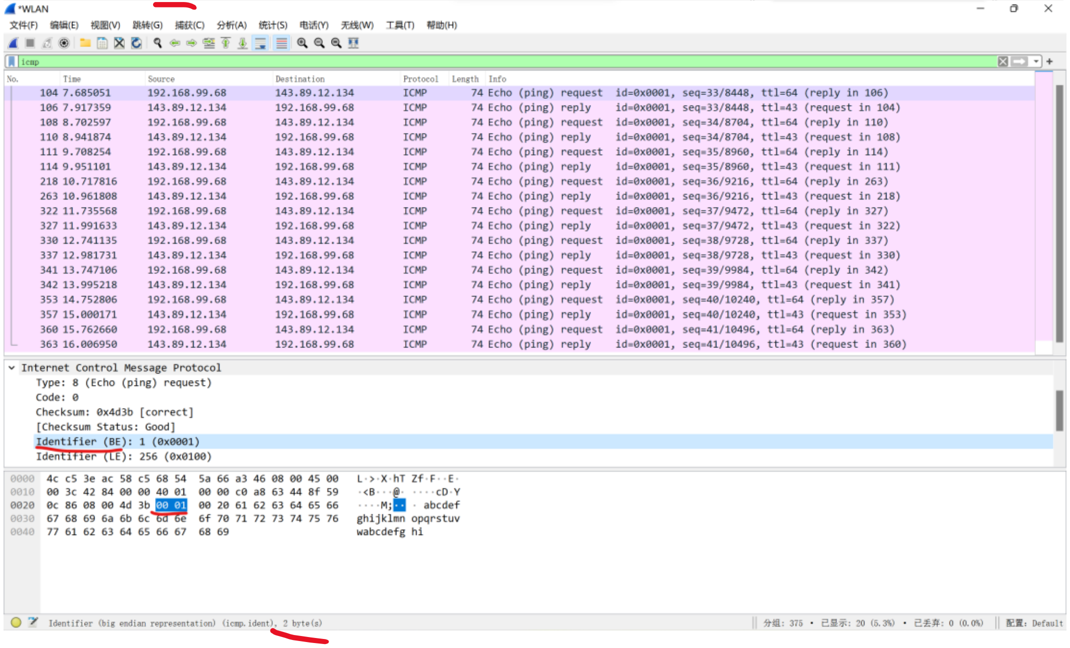

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
icmp

```
No.   Time        Source          Destination     Protocol Length Info
  101 6.670634    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=32/8192, ttl=64 (reply in 103)
  103 6.918761    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=32/8192, ttl=43 (request in 101)
  104 7.685051    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=33/8448, ttl=64 (reply in 106)
  106 7.917359    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=33/8448, ttl=43 (request in 104)
  108 8.702597    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=34/8704, ttl=64 (reply in 110)
  110 8.941874    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=34/8704, ttl=43 (request in 108)
  111 9.708254    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=35/8960, ttl=64 (reply in 114)
  114 9.951101    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=35/8960, ttl=43 (request in 111)
  218 10.717816   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=36/9216, ttl=64 (reply in 263)
  263 10.961808   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=36/9216, ttl=43 (request in 218)
  322 11.735568   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=37/9472, ttl=64 (reply in 327)
  327 11.991633   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=37/9472, ttl=43 (request in 322)
  330 12.741135   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=38/9728, ttl=64 (reply in 337)
  337 12.981731   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=38/9728, ttl=43 (request in 330)
  341 13.747106   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=39/9984, ttl=64 (reply in 342)
  342 13.995218   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=39/9984, ttl=43 (request in 341)
  353 14.752806   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=40/10240, ttl=64 (reply in 357)
  357 15.000171   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=40/10240, ttl=43 (request in 353)
```

```
> Frame 101: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{BA830209-2A9A-4C06-8291-762D71A8C793}, id 0
> Ethernet II, Src: IntelCor_66:a3:46 (68:54:5a:66:a3:46), Dst: ZyxelCom_ac:58:c5 (4c:c5:3e:ac:58:c5)
> Internet Protocol Version 4, Src: 192.168.99.68, Dst: 143.89.12.134
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d3b [correct]
```

```
0000  4c c5 3e ac 58 c5 68 54  5a 66 a3 46 08 00 45 00   L·>·X·hT Zf·F··E·
0010  00 3c 42 84 00 00 40 01  00 00 c0 a8 63 44 8f 59   ·<B···@· ····cD·Y
0020  0c 86 08 00 4d 3b 00 01  00 20 61 62 63 64 65 66   ····M;·· · abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

```
Checksum (icmp.checksum), 2 byte(s)    分组: 375 • 已显示: 20 (5.3%) • 已丢弃: 0 (0.0%)    配置: Default
```

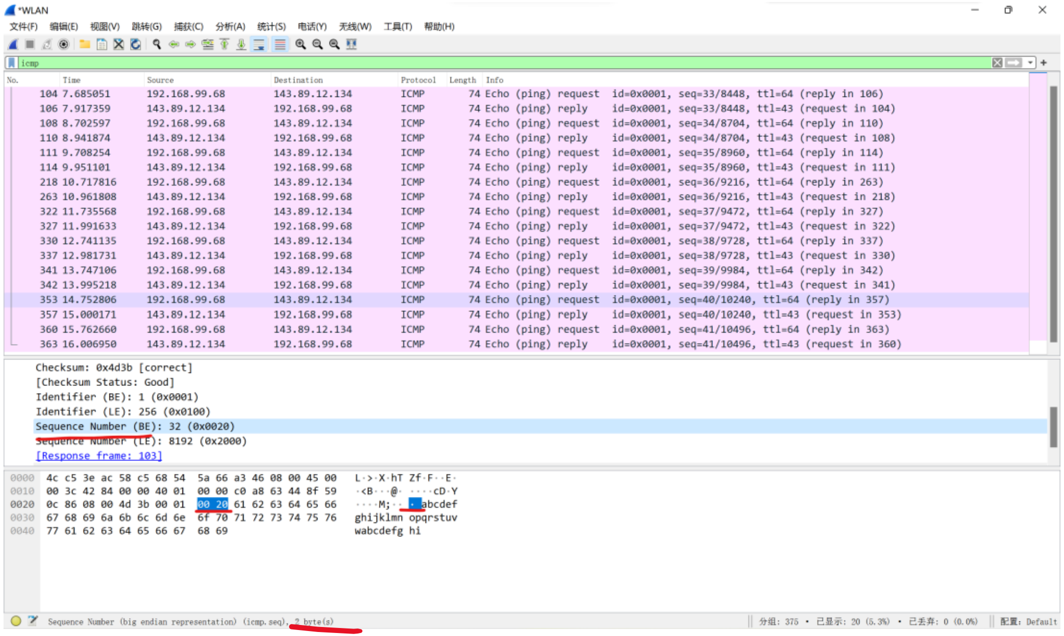

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
icmp

```
No.   Time        Source          Destination     Protocol Length Info
  104 7.685051    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=33/8448, ttl=64 (reply in 106)
  106 7.917359    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=33/8448, ttl=43 (request in 104)
  108 8.702597    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=34/8704, ttl=64 (reply in 110)
  110 8.941874    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=34/8704, ttl=43 (request in 108)
  111 9.708254    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=35/8960, ttl=64 (reply in 114)
  114 9.951101    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=35/8960, ttl=43 (request in 111)
  218 10.717816   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=36/9216, ttl=64 (reply in 263)
  263 10.961808   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=36/9216, ttl=43 (request in 218)
  322 11.735568   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=37/9472, ttl=64 (reply in 327)
  327 11.991633   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=37/9472, ttl=43 (request in 322)
  330 12.741135   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=38/9728, ttl=64 (reply in 337)
  337 12.981731   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=38/9728, ttl=43 (request in 330)
  341 13.747106   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=39/9984, ttl=64 (reply in 342)
  342 13.995218   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=39/9984, ttl=43 (request in 341)
  353 14.752806   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=40/10240, ttl=64 (reply in 357)
  357 15.000171   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=40/10240, ttl=43 (request in 353)
  360 15.762660   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=41/10496, ttl=64 (reply in 363)
  363 16.006950   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=41/10496, ttl=43 (request in 360)
```

```
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d3b [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
```

```
0000  4c c5 3e ac 58 c5 68 54  5a 66 a3 46 08 00 45 00   L·>·X·hT Zf·F··E·
0010  00 3c 42 84 00 00 40 01  00 00 c0 a8 63 44 8f 59   ·<B···@· ····cD·Y
0020  0c 86 08 00 4d 3b 00 01  00 20 61 62 63 64 65 66   ····M;·· · abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

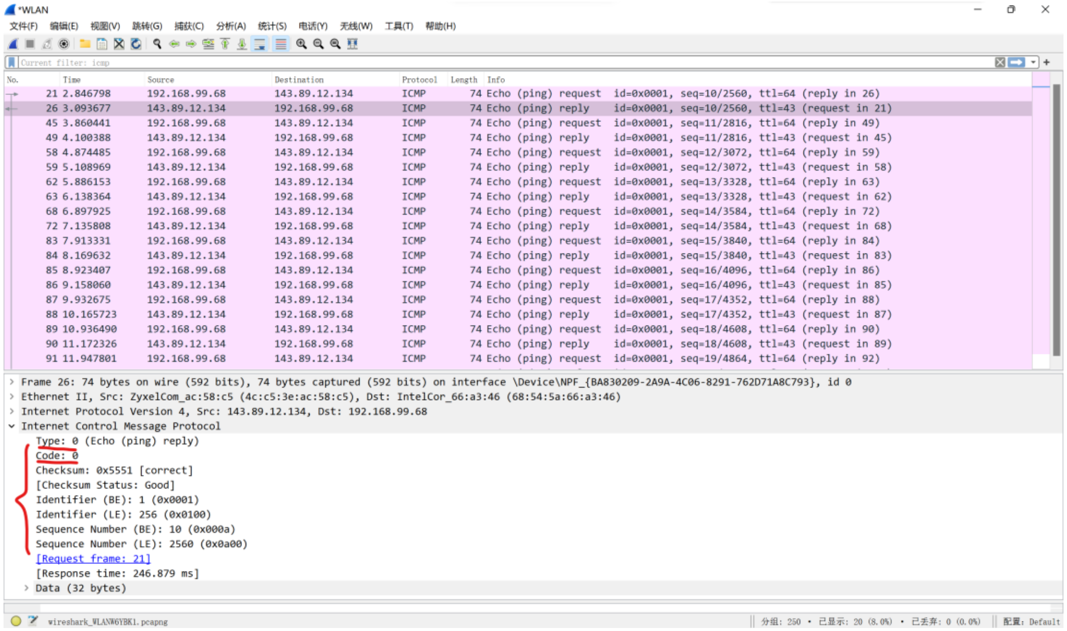
```
Identifier (big endian representation) (icmp.ident), 2 byte(s)    分组: 375 • 已显示: 20 (5.3%) • 已丢弃: 0 (0.0%)    配置: Default
```


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
icmp
No.     Time         Source          Destination     Protocol  Length Info
  104 7.685051      192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=33/8448, ttl=64 (reply in 106)
  106 7.917359      143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=33/8448, ttl=43 (request in 104)
  108 8.702597      192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=34/8704, ttl=64 (reply in 110)
  110 8.941874      143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=34/8704, ttl=43 (request in 108)
  111 9.708254      192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=35/8960, ttl=64 (reply in 114)
  114 9.951101      143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=35/8960, ttl=43 (request in 111)
  218 10.717816     192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=36/9216, ttl=64 (reply in 263)
  263 10.961808     143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=36/9216, ttl=43 (request in 218)
  322 11.735568     192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=37/9472, ttl=64 (reply in 327)
  327 11.991633     143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=37/9472, ttl=43 (request in 322)
  330 12.741135     192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=38/9728, ttl=64 (reply in 337)
  337 12.981731     143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=38/9728, ttl=43 (request in 330)
  341 13.747106     192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=39/9984, ttl=64 (reply in 342)
  342 13.995218     143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=39/9984, ttl=43 (request in 341)
  353 14.752806     192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=40/10240, ttl=64 (reply in 357)
  357 15.000171     143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=40/10240, ttl=43 (request in 353)
  360 15.762660     192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=41/10496, ttl=64 (reply in 363)
  363 16.006950     143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=41/10496, ttl=43 (request in 360)

    Checksum: 0x4d3b [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 32 (0x0020)
    Sequence Number (LE): 8192 (0x2000)
    [Response frame: 103]

0000  4c c5 3e ac 58 c5 68 54  5a 66 a3 46 08 00 45 00   L·>·X·hT Zf·F··E·
0010  00 3c 42 84 00 00 40 01  00 00 c0 a8 63 44 8f 59   ·<B···@· ····cD·Y
0020  0c 86 08 00 4d 3b 00 01  00 20 61 62 63 64 65 66   ····M;·· · abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi

Sequence Number (big endian representation) (icmp.seq), 2 byte(s)    分组: 375 · 已显示: 20 (5.3%) · 已丢弃: 0 (0.0%)    配置: Default
```

The type is 8 and the code number is 0. It also has checksum, checksum status, identifier(BE), identifier(LE), sequence number(BE) and sequence number(LE). They are all 2 bytes.

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

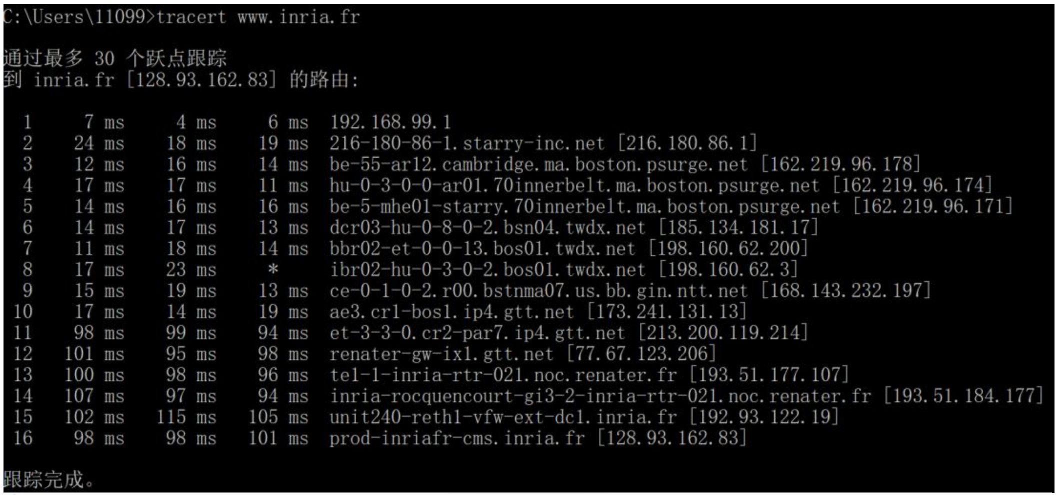

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
Current filter: icmp
No.     Time         Source          Destination     Protocol  Length Info
   21 2.846798      192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=10/2560, ttl=64 (reply in 26)
   26 3.093677      143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=10/2560, ttl=43 (request in 21)
   45 3.860441      192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=11/2816, ttl=64 (reply in 49)
   49 4.100388      143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=11/2816, ttl=43 (request in 45)
   58 4.874485      192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=12/3072, ttl=64 (reply in 59)
   59 5.108969      143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=12/3072, ttl=43 (request in 58)
   62 5.886153      192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=64 (reply in 63)
   63 6.138364      143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=13/3328, ttl=43 (request in 62)
   68 6.897925      192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=14/3584, ttl=64 (reply in 72)
   72 7.135808      143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=14/3584, ttl=43 (request in 68)
   83 7.913331      192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=15/3840, ttl=64 (reply in 84)
   84 8.169632      143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=15/3840, ttl=43 (request in 83)
   85 8.923407      192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=16/4096, ttl=64 (reply in 86)
   86 9.158060      143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=16/4096, ttl=43 (request in 85)
   87 9.932675      192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=17/4352, ttl=64 (reply in 88)
   88 10.165723     143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=17/4352, ttl=43 (request in 87)
   89 10.936490     192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=18/4608, ttl=64 (reply in 90)
   90 11.172326     143.89.12.134   192.168.99.68   ICMP        74 Echo (ping) reply    id=0x0001, seq=18/4608, ttl=43 (request in 89)
   91 11.947801     192.168.99.68   143.89.12.134   ICMP        74 Echo (ping) request  id=0x0001, seq=19/4864, ttl=64 (reply in 92)

> Frame 26: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{BA830209-2A9A-4C06-8291-762D71A8C793}, id 0
> Ethernet II, Src: ZyxelCom_ac:58:c5 (4c:c5:3e:ac:58:c5), Dst: IntelCor_66:a3:46 (68:54:5a:66:a3:46)
> Internet Protocol Version 4, Src: 143.89.12.134, Dst: 192.168.99.68
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5551 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 10 (0x000a)
    Sequence Number (LE): 2560 (0x0a00)
    [Request frame: 21]
    [Response time: 246.879 ms]
  > Data (32 bytes)

wireshark_WLANW6YBK1.pcapng    分组: 250 · 已显示: 20 (8.0%) · 已丢弃: 0 (0.0%)    配置: Default
```

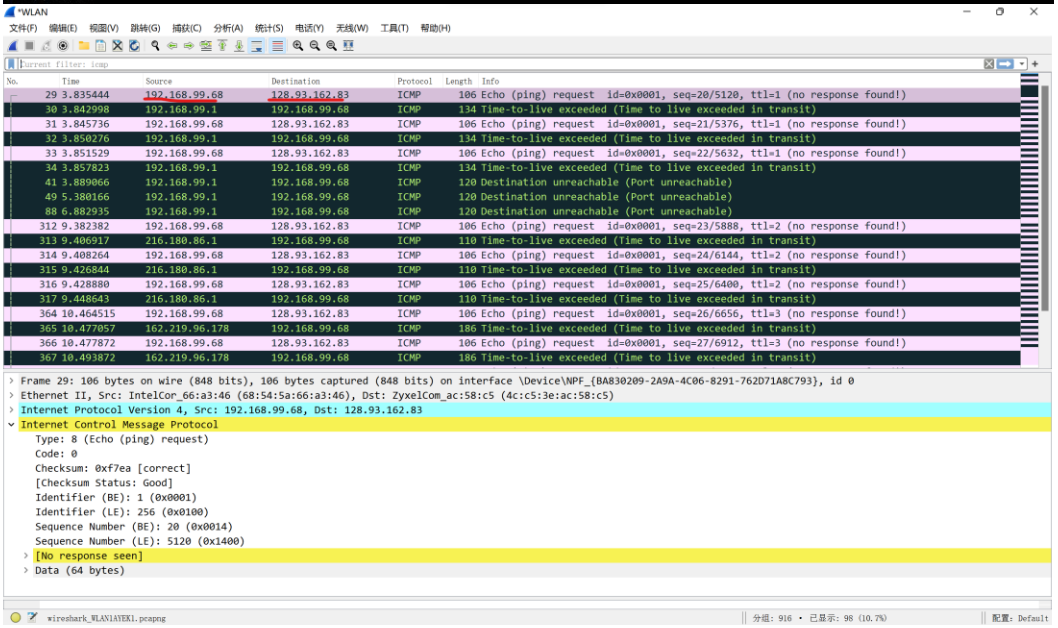
The type is 0 and the code number is 0. It also has checksum, checksum status, identifier(BE), identifier(LE), sequence number(BE) and sequence number(LE). The same as problem 3’s screenshot, they are all 2 bytes.

2. ICMP and Traceroute

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



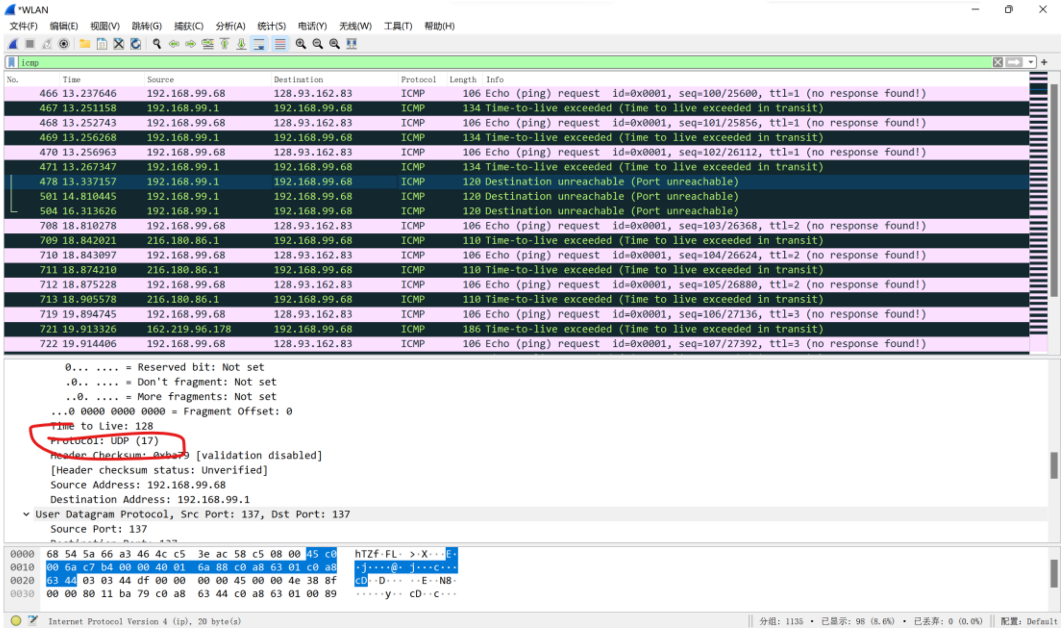
```
C:\Users\11099>tracert www.inria.fr

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

  1     7 ms     4 ms     6 ms  192.168.99.1
  2    24 ms    18 ms    19 ms  216-180-86-1.starry-inc.net [216.180.86.1]
  3    12 ms    16 ms    14 ms  be-55-ar12.cambridge.ma.boston.psurge.net [162.219.96.178]
  4    17 ms    17 ms    11 ms  hu-0-3-0-0-ar01.70innerbelt.ma.boston.psurge.net [162.219.96.174]
  5    14 ms    16 ms    16 ms  be-5-mhe01-starry.70innerbelt.ma.boston.psurge.net [162.219.96.171]
  6    14 ms    17 ms    13 ms  dcr03-hu-0-8-0-2.bsn04.twdx.net [185.134.181.17]
  7    11 ms    18 ms    14 ms  bbr02-et-0-0-13.bos01.twdx.net [198.160.62.200]
  8    17 ms    23 ms     *     ibr02-hu-0-3-0-2.bos01.twdx.net [198.160.62.3]
  9    15 ms    19 ms    13 ms  ce-0-1-0-2.r00.bstnma07.us.bb.gin.ntt.net [168.143.232.197]
 10    17 ms    14 ms    19 ms  ae3.cr1-bos1.ip4.gtt.net [173.241.131.13]
 11    98 ms    99 ms    94 ms  et-3-3-0.cr2-par7.ip4.gtt.net [213.200.119.214]
 12   101 ms    95 ms    98 ms  renater-gw-ix1.gtt.net [77.67.123.206]
 13   100 ms    98 ms    96 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 14   107 ms    97 ms    94 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 15   102 ms   115 ms   105 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 16    98 ms    98 ms   101 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

跟踪完成。
```



```
No.   Time        Source          Destination     Protocol  Length  Info
   29 3.835444    192.168.99.68   128.93.162.83   ICMP      106 Echo (ping) request  id=0x0001, seq=20/5120, ttl=1 (no response found!)
   30 3.842998    192.168.99.1    192.168.99.68   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   31 3.845736    192.168.99.68   128.93.162.83   ICMP      106 Echo (ping) request  id=0x0001, seq=21/5376, ttl=1 (no response found!)
   32 3.850276    192.168.99.1    192.168.99.68   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   33 3.851529    192.168.99.68   128.93.162.83   ICMP      106 Echo (ping) request  id=0x0001, seq=22/5632, ttl=1 (no response found!)
   34 3.857823    192.168.99.1    192.168.99.68   ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
   41 3.889066    192.168.99.1    192.168.99.68   ICMP      120 Destination unreachable (Port unreachable)
   49 5.380166    192.168.99.1    192.168.99.68   ICMP      120 Destination unreachable (Port unreachable)
   88 6.882935    192.168.99.1    192.168.99.68   ICMP      120 Destination unreachable (Port unreachable)
  312 9.382382    192.168.99.68   128.93.162.83   ICMP      106 Echo (ping) request  id=0x0001, seq=23/5888, ttl=2 (no response found!)
  313 9.406917    216.180.86.1    192.168.99.68   ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  314 9.408264    192.168.99.68   128.93.162.83   ICMP      106 Echo (ping) request  id=0x0001, seq=24/6144, ttl=2 (no response found!)
  315 9.426844    216.180.86.1    192.168.99.68   ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  316 9.428880    192.168.99.68   128.93.162.83   ICMP      106 Echo (ping) request  id=0x0001, seq=25/6400, ttl=2 (no response found!)
  317 9.448643    216.180.86.1    192.168.99.68   ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
  364 10.464515   192.168.99.68   128.93.162.83   ICMP      106 Echo (ping) request  id=0x0001, seq=26/6656, ttl=3 (no response found!)
  365 10.477057   162.219.96.178  192.168.99.68   ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
  366 10.477872   192.168.99.68   128.93.162.83   ICMP      106 Echo (ping) request  id=0x0001, seq=27/6912, ttl=3 (no response found!)
  367 10.493872   162.219.96.178  192.168.99.68   ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)

> Frame 29: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{BA830209-2A9A-4C06-8291-762D71A8C793}, id 0
> Ethernet II, Src: IntelCor_66:a3:46 (68:54:5a:66:a3:46), Dst: ZyxelCom_ac:58:c5 (4c:c5:3e:ac:58:c5)
> Internet Protocol Version 4, Src: 192.168.99.68, Dst: 128.93.162.83
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7ea [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 20 (0x0014)
    Sequence Number (LE): 5120 (0x1400)
  > [No response seen]
  > Data (64 bytes)

wireshark_WLAN1AYEK1.pcapng          分组: 916 · 已显示: 98 (10.7%)          配置: Default
```

The IP address of my host is 192.168.99.68, and the IP address of the destination host is 128.93.162.83.

6. Answer one of them depending on the OS you used.
If you used Windows tracert: If tracert sent UDP packets instead (as in Unix/Linux), what would the IP protocol number be for the probe packets? If you used Unix/Linus traceroute: If traceroute sent ICMP ping query packets instead (as in Windows), what would the IP protocol number be for the probe packets?


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
icmp

```
No.  Time       Source          Destination     Protocol Length Info
466 13.237646   192.168.99.68   128.93.162.83   ICMP     106 Echo (ping) request  id=0x0001, seq=100/25600, ttl=1 (no response found!)
467 13.251158   192.168.99.1    192.168.99.68   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
468 13.252743   192.168.99.68   128.93.162.83   ICMP     106 Echo (ping) request  id=0x0001, seq=101/25856, ttl=1 (no response found!)
469 13.256268   192.168.99.1    192.168.99.68   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
470 13.256963   192.168.99.68   128.93.162.83   ICMP     106 Echo (ping) request  id=0x0001, seq=102/26112, ttl=1 (no response found!)
471 13.267347   192.168.99.1    192.168.99.68   ICMP     134 Time-to-live exceeded (Time to live exceeded in transit)
478 13.337157   192.168.99.1    192.168.99.68   ICMP     120 Destination unreachable (Port unreachable)
501 14.810445   192.168.99.1    192.168.99.68   ICMP     120 Destination unreachable (Port unreachable)
504 16.313626   192.168.99.1    192.168.99.68   ICMP     120 Destination unreachable (Port unreachable)
708 18.810278   192.168.99.68   128.93.162.83   ICMP     106 Echo (ping) request  id=0x0001, seq=103/26368, ttl=2 (no response found!)
709 18.842021   216.180.86.1    192.168.99.68   ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
710 18.843097   192.168.99.68   128.93.162.83   ICMP     106 Echo (ping) request  id=0x0001, seq=104/26624, ttl=2 (no response found!)
711 18.874210   216.180.86.1    192.168.99.68   ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
712 18.875228   192.168.99.68   128.93.162.83   ICMP     106 Echo (ping) request  id=0x0001, seq=105/26880, ttl=2 (no response found!)
713 18.905578   216.180.86.1    192.168.99.68   ICMP     110 Time-to-live exceeded (Time to live exceeded in transit)
719 19.894745   192.168.99.68   128.93.162.83   ICMP     106 Echo (ping) request  id=0x0001, seq=106/27136, ttl=3 (no response found!)
721 19.913326   162.219.96.178  192.168.99.68   ICMP     186 Time-to-live exceeded (Time to live exceeded in transit)
722 19.914406   192.168.99.68   128.93.162.83   ICMP     106 Echo (ping) request  id=0x0001, seq=107/27392, ttl=3 (no response found!)
```

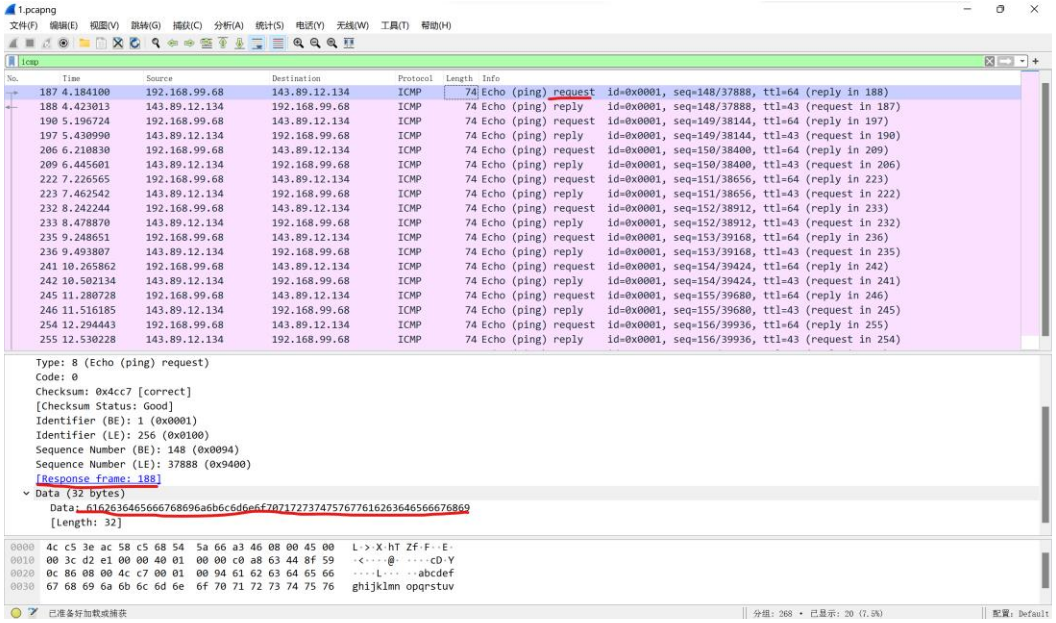
```
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xba79 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.99.68
    Destination Address: 192.168.99.1
  User Datagram Protocol, Src Port: 137, Dst Port: 137
    Source Port: 137
```

```
0000  68 54 5a 66 a3 46 4c c5  3e ac 58 c5 08 00 45 c0   hTZf·FL· >·X···E·
0010  00 6a c7 b4 00 00 40 01  6a 88 c0 a8 63 01 c0 a8   ·j····@· j···c···
0020  63 44 03 03 44 df 00 00  00 00 45 00 00 4e 38 8f   cD··D··· ··E··N8·
0030  00 00 80 11 ba 79 c0 a8  63 44 c0 a8 63 01 00 89   ·····y·· cD··c···
```

```
Internet Protocol Version 4 (ip), 20 byte(s)    分组: 1135 · 已显示: 98 (8.6%) · 已丢弃: 0 (0.0%)    配置: Default
```

I used Windows tracert. Clicked the “Destination unreachable” packet and the number was 17.

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?

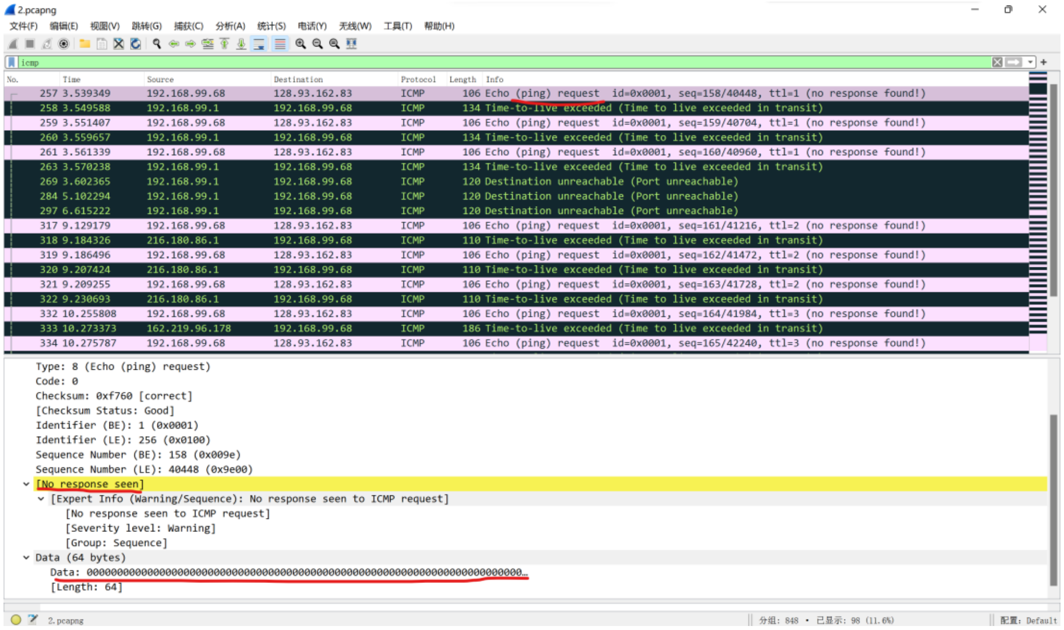

1.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
icmp

```
No.  Time       Source          Destination     Protocol Length Info
187 4.184100    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=148/37888, ttl=64 (reply in 188)
188 4.423013    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=148/37888, ttl=43 (request in 187)
190 5.196724    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=149/38144, ttl=64 (reply in 197)
197 5.430990    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=149/38144, ttl=43 (request in 190)
206 6.210830    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=150/38400, ttl=64 (reply in 209)
209 6.445601    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=150/38400, ttl=43 (request in 206)
222 7.226565    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=151/38656, ttl=64 (reply in 223)
223 7.462542    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=151/38656, ttl=43 (request in 222)
232 8.242244    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=152/38912, ttl=64 (reply in 233)
233 8.478870    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=152/38912, ttl=43 (request in 232)
235 9.248651    192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=153/39168, ttl=64 (reply in 236)
236 9.493807    143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=153/39168, ttl=43 (request in 235)
241 10.265862   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=154/39424, ttl=64 (reply in 242)
242 10.502134   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=154/39424, ttl=43 (request in 241)
245 11.280728   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=155/39680, ttl=64 (reply in 246)
246 11.516185   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=155/39680, ttl=43 (request in 245)
254 12.294443   192.168.99.68   143.89.12.134   ICMP     74 Echo (ping) request  id=0x0001, seq=156/39936, ttl=64 (reply in 255)
255 12.530228   143.89.12.134   192.168.99.68   ICMP     74 Echo (ping) reply    id=0x0001, seq=156/39936, ttl=43 (request in 254)
```

```
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4cc7 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 148 (0x0094)
    Sequence Number (LE): 37888 (0x9400)
    [Response frame: 188]
  Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

```
0000  4c c5 3e ac 58 c5 68 54  5a 66 a3 46 08 00 45 00   L·>·X·hT Zf·F··E·
0010  00 3c d2 e1 00 00 40 01  00 00 c0 a8 63 44 8f 59   ·<····@· ····cD·Y
0020  0c 86 08 00 4c c7 00 01  00 94 61 62 63 64 65 66   ····L··· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
```

```
已准备好加载或捕获    分组: 268 · 已显示: 20 (7.5%)    配置: Default
```

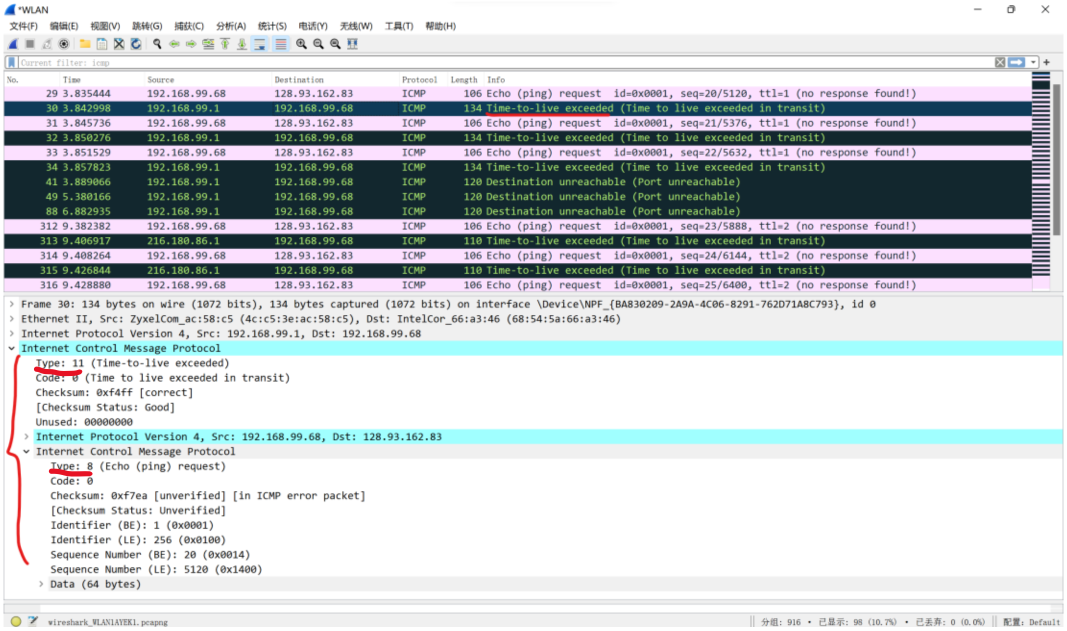

2.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
icmp

```
No.      Time        Source           Destination      Protocol  Length  Info
    257 3.539349     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=158/40448, ttl=1 (no response found!)
    258 3.549588     192.168.99.1     192.168.99.68    ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
    259 3.551407     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=159/40704, ttl=1 (no response found!)
    260 3.559657     192.168.99.1     192.168.99.68    ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
    261 3.561339     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=160/40960, ttl=1 (no response found!)
    263 3.570238     192.168.99.1     192.168.99.68    ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
    269 3.602365     192.168.99.1     192.168.99.68    ICMP      120 Destination unreachable (Port unreachable)
    284 5.102294     192.168.99.1     192.168.99.68    ICMP      120 Destination unreachable (Port unreachable)
    297 6.615222     192.168.99.1     192.168.99.68    ICMP      120 Destination unreachable (Port unreachable)
    317 9.129179     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=161/41216, ttl=2 (no response found!)
    318 9.184326     216.180.86.1     192.168.99.68    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
    319 9.186496     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=162/41472, ttl=2 (no response found!)
    320 9.207424     216.180.86.1     192.168.99.68    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
    321 9.209255     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=163/41728, ttl=2 (no response found!)
    322 9.230693     216.180.86.1     192.168.99.68    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
    332 10.255808    192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=164/41984, ttl=3 (no response found!)
    333 10.273373    162.219.96.178   192.168.99.68    ICMP      186 Time-to-live exceeded (Time to live exceeded in transit)
    334 10.275787    192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=165/42240, ttl=3 (no response found!)
```

```
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf760 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 158 (0x009e)
    Sequence Number (LE): 40448 (0x9e00)
  ⌄ [No response seen]
    ⌄ [Expert Info (Warning/Sequence): No response seen to ICMP request]
        [No response seen to ICMP request]
        [Severity level: Warning]
        [Group: Sequence]
  ⌄ Data (64 bytes)
      Data: 00000000000000000000000000000000000000000000000000000000000000000000…
      [Length: 64]
```

ICMP echo packet had a different field called ‘No response seen’ and ICMP ping packet had ‘Response frame’. Also the “Data” was different, one had 32 bytes, the other had 64 bytes filled with zero.

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


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Current filter: icmp

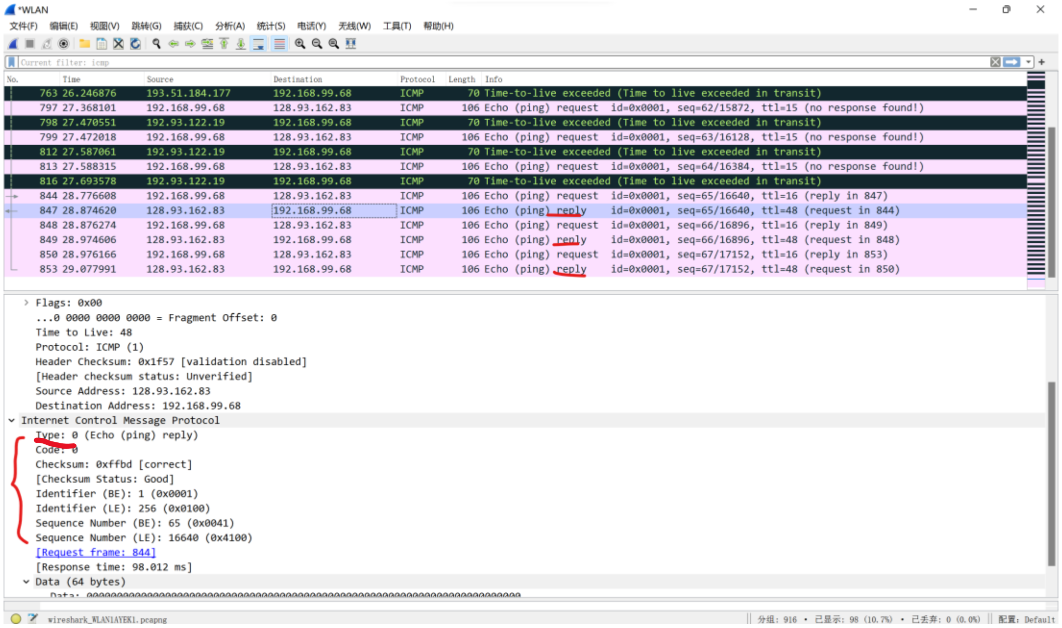
```
No.      Time        Source           Destination      Protocol  Length  Info
     29 3.835444     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=20/5120, ttl=1 (no response found!)
     30 3.842998     192.168.99.1     192.168.99.68    ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
     31 3.845736     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=21/5376, ttl=1 (no response found!)
     32 3.850276     192.168.99.1     192.168.99.68    ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
     33 3.851529     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=22/5632, ttl=1 (no response found!)
     34 3.857823     192.168.99.1     192.168.99.68    ICMP      134 Time-to-live exceeded (Time to live exceeded in transit)
     41 3.889066     192.168.99.1     192.168.99.68    ICMP      120 Destination unreachable (Port unreachable)
     49 5.380166     192.168.99.1     192.168.99.68    ICMP      120 Destination unreachable (Port unreachable)
     88 6.882935     192.168.99.1     192.168.99.68    ICMP      120 Destination unreachable (Port unreachable)
    312 9.382382     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=23/5888, ttl=2 (no response found!)
    313 9.406917     216.180.86.1     192.168.99.68    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
    314 9.408264     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=24/6144, ttl=2 (no response found!)
    315 9.426844     216.180.86.1     192.168.99.68    ICMP      110 Time-to-live exceeded (Time to live exceeded in transit)
    316 9.428880     192.168.99.68    128.93.162.83    ICMP      106 Echo (ping) request  id=0x0001, seq=25/6400, ttl=2 (no response found!)
```

```
> Frame 30: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{BA830209-2A9A-4C06-8291-762D71A8C793}, id 0
> Ethernet II, Src: ZyxelCom_ac:58:c5 (4c:c5:3e:ac:58:c5), Dst: IntelCor_66:a3:46 (68:54:5a:66:a3:46)
> Internet Protocol Version 4, Src: 192.168.99.1, Dst: 192.168.99.68
⌄ 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: 192.168.99.68, Dst: 128.93.162.83
  ⌄ Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf7ea [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 20 (0x0014)
      Sequence Number (LE): 5120 (0x1400)
    > Data (64 bytes)
```

wireshark_WLAN1AYEK1.pcapng
分组: 916 • 已显示: 98 (10.7%) • 已丢弃: 0 (0.0%)
配置: Default

I choosed “Time-to-live exceeded” error packet. It had 1 more fields. 2 fields respectively contained different two types (11 and 8), two code names (0 and 0) and two checksums (0xf4ff and 0xf7ea).

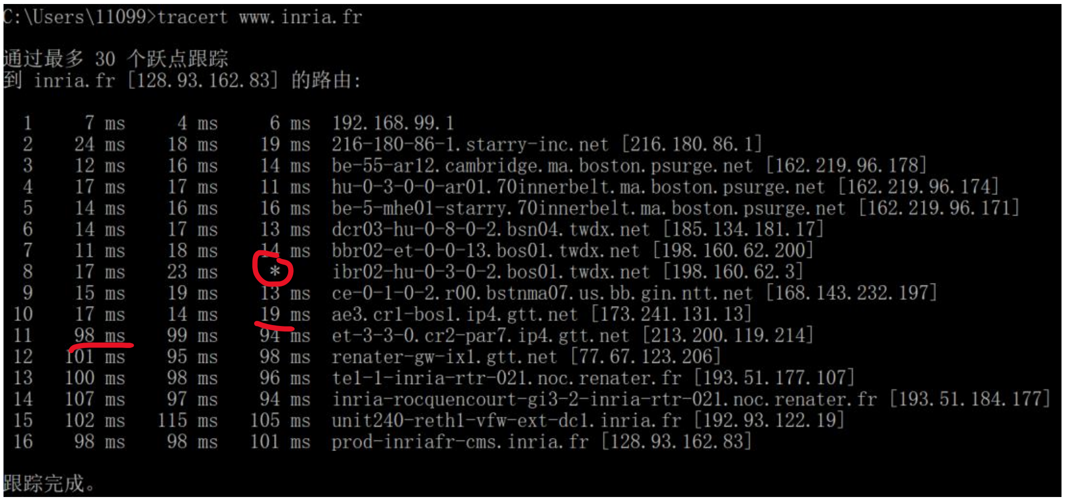
9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
Current filter: icmp

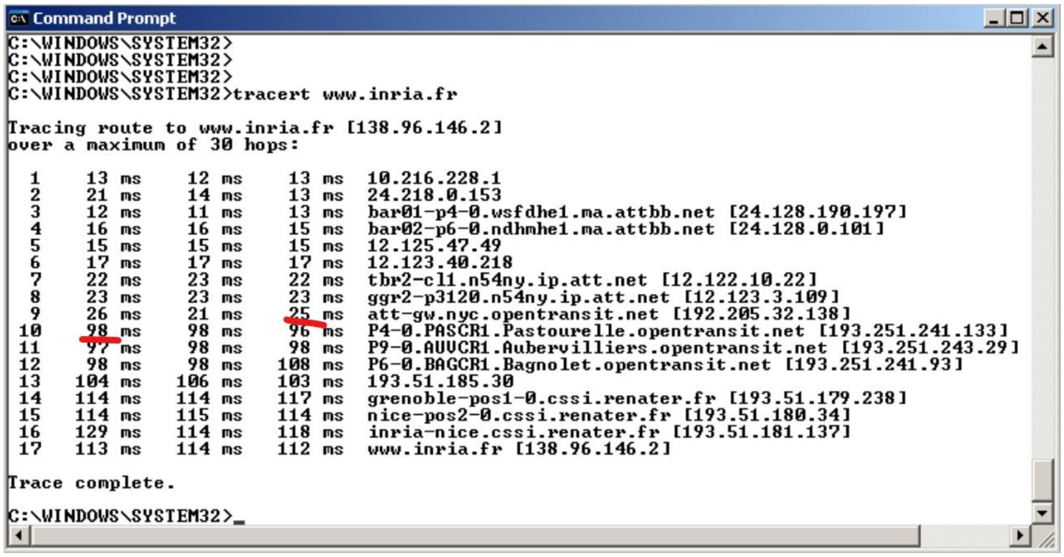
```
No.   Time          Source            Destination       Protocol  Length  Info
  763 26.246876     193.51.184.177    192.168.99.68     ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  797 27.368101     192.168.99.68     128.93.162.83     ICMP      106 Echo (ping) request  id=0x0001, seq=62/15872, ttl=15 (no response found!)
  798 27.470551     192.93.122.19     192.168.99.68     ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  799 27.472018     192.168.99.68     128.93.162.83     ICMP      106 Echo (ping) request  id=0x0001, seq=63/16128, ttl=15 (no response found!)
  812 27.587061     192.93.122.19     192.168.99.68     ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  813 27.588315     192.168.99.68     128.93.162.83     ICMP      106 Echo (ping) request  id=0x0001, seq=64/16384, ttl=15 (no response found!)
  816 27.693578     192.93.122.19     192.168.99.68     ICMP       70 Time-to-live exceeded (Time to live exceeded in transit)
  844 28.776608     192.168.99.68     128.93.162.83     ICMP      106 Echo (ping) request  id=0x0001, seq=65/16640, ttl=16 (reply in 847)
  847 28.874620     128.93.162.83     192.168.99.68     ICMP      106 Echo (ping) reply    id=0x0001, seq=65/16640, ttl=48 (request in 844)
  848 28.876274     192.168.99.68     128.93.162.83     ICMP      106 Echo (ping) request  id=0x0001, seq=66/16896, ttl=16 (reply in 849)
  849 28.974606     128.93.162.83     192.168.99.68     ICMP      106 Echo (ping) reply    id=0x0001, seq=66/16896, ttl=48 (request in 848)
  850 28.976166     192.168.99.68     128.93.162.83     ICMP      106 Echo (ping) request  id=0x0001, seq=67/17152, ttl=16 (reply in 853)
  853 29.077991     128.93.162.83     192.168.99.68     ICMP      106 Echo (ping) reply    id=0x0001, seq=67/17152, ttl=48 (request in 850)

  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 48
    Protocol: ICMP (1)
    Header Checksum: 0x1f57 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.93.162.83
    Destination Address: 192.168.99.68
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xffbd [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 65 (0x0041)
    Sequence Number (LE): 16640 (0x4100)
    [Request frame: 844]
    [Response time: 98.012 ms]
  v Data (64 bytes)
      Data: 0000000000000000000000000000000000000000000000000000000000000000000000

wireshark_WLAN1AYEK1.pcapng        分组: 916 · 已显示: 98 (10.7%) · 已丢弃: 0 (0.0%)    配置: Default
```

The type of three reply packets is 0. Because they all reply to the request correctly, thus they don’t need to preserve ICMP error type like 11.

10. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?



```
C:\Users\11099>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     4 ms     6 ms  192.168.99.1
  2    24 ms    18 ms    19 ms  216-180-86-1.starry-inc.net [216.180.86.1]
  3    12 ms    16 ms    14 ms  be-55-ar12.cambridge.ma.boston.psurge.net [162.219.96.178]
  4    17 ms    17 ms    11 ms  hu-0-3-0-0-ar01.70innerbelt.ma.boston.psurge.net [162.219.96.174]
  5    14 ms    16 ms    16 ms  be-5-mhe01-starry.70innerbelt.ma.boston.psurge.net [162.219.96.171]
  6    14 ms    17 ms    13 ms  dcr03-hu-0-8-0-2.bsn04.twdx.net [185.134.181.17]
  7    11 ms    18 ms    14 ms  bbr02-et-0-0-13.bos01.twdx.net [198.160.62.200]
  8    17 ms    23 ms     *     ibr02-hu-0-3-0-2.bos01.twdx.net [198.160.62.3]
  9    15 ms    19 ms    13 ms  ce-0-1-0-2.r00.bstnma07.us.bb.gin.ntt.net [168.143.232.197]
 10    17 ms    14 ms    19 ms  ae3.cr1-bos1.ip4.gtt.net [173.241.131.13]
 11    98 ms    99 ms    94 ms  et-3-3-0.cr2-par7.ip4.gtt.net [213.200.119.214]
 12   101 ms    95 ms    98 ms  renater-gw-ix1.gtt.net [77.67.123.206]
 13   100 ms    98 ms    96 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 14   107 ms    97 ms    94 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 15   102 ms   115 ms   105 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 16    98 ms    98 ms   101 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

跟踪完成。
```



```
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>tracert www.inria.fr

Tracing route to www.inria.fr [138.96.146.2]
over a maximum of 30 hops:

  1     13 ms    12 ms    13 ms  10.216.228.1
  2     21 ms    14 ms    13 ms  24.218.0.153
  3     12 ms    11 ms    13 ms  bar01-p4-0.wsfdhe1.ma.attbb.net [24.128.190.197]
  4     16 ms    16 ms    15 ms  bar02-p6-0.ndhmhe1.ma.attbb.net [24.128.0.101]
  5     15 ms    15 ms    15 ms  12.125.47.49
  6     17 ms    17 ms    17 ms  12.123.40.218
  7     22 ms    23 ms    22 ms  tbr2-cl1.n54ny.ip.att.net [12.122.10.22]
  8     23 ms    23 ms    23 ms  ggr2-p3120.n54ny.ip.att.net [12.123.3.109]
  9     26 ms    21 ms    25 ms  att-gw.nyc.opentransit.net [192.205.32.138]
 10     98 ms    98 ms    96 ms  P4-0.PASCR1.Pastourelle.opentransit.net [193.251.241.133]
 11     97 ms    98 ms    98 ms  P9-0.AUVCR1.Aubervilliers.opentransit.net [193.251.243.29]
 12     98 ms    98 ms   108 ms  P6-0.BAGCR1.Bagnolet.opentransit.net [193.251.241.93]
 13    104 ms   106 ms   103 ms  193.51.185.30
 14    114 ms   114 ms   117 ms  grenoble-pos1-0.cssi.renater.fr [193.51.179.238]
 15    114 ms   115 ms   114 ms  nice-pos2-0.cssi.renater.fr [193.51.180.34]
 16    129 ms   114 ms   118 ms  inria-nice.cssi.renater.fr [193.51.181.137]
 17    113 ms   114 ms   112 ms  www.inria.fr [138.96.146.2]

Trace complete.

C:\WINDOWS\SYSTEM32>_
```

According to my experiment screenshot, it's between step 10 and 11 (19ms ~ 98ms).

According to Figure 4, it's between step 9 and 10 (25ms ~ 98ms). The first router's name contains "nyc" = "newyork city"? so I guess it's America. The second router's name contains "Pastourelle", so I guess it's France.