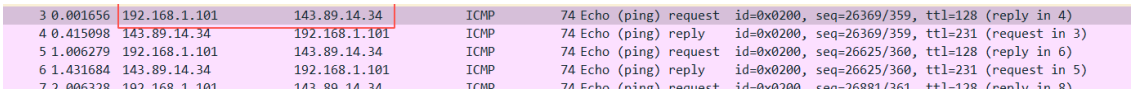
Lab8 Wireshark_ICMP

- 学号:1813075
- 姓名:刘茵

---

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



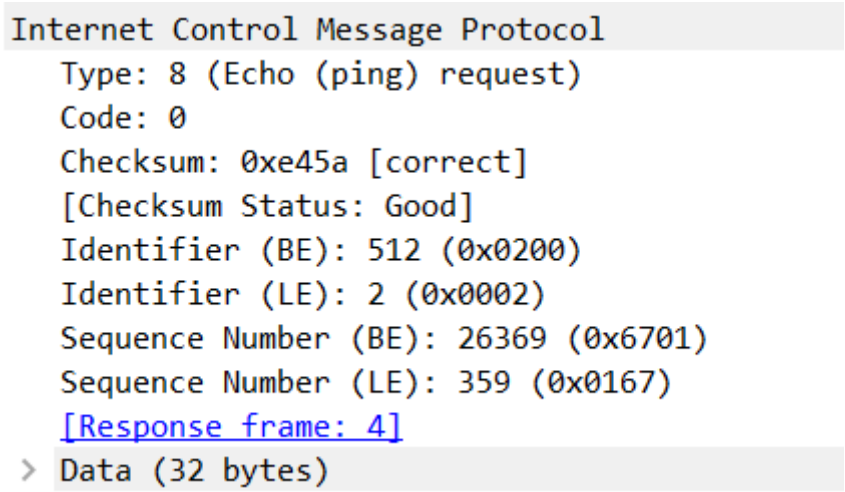
   答：主机IP：192.168.1.101

   目标IP：143.09.14.34

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

   答：因为 ICMP 协议是网络层的协议，它不需要传输层 TCP 和 UDP 承载， 直接使用 IP 报承载，因此不需要源端口号目的端口号，只需要目的地址即可。

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?

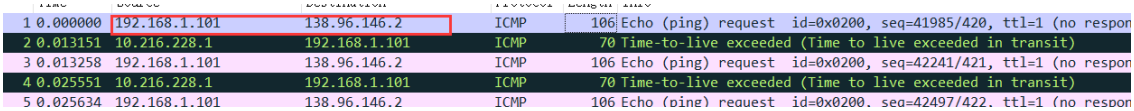


   答：ICMP类型：8(代表ICMP请求)，代码：0
   还有Checksum、Indetifier，Sequence number字段
   校验和(Checksum)：2个字节
   序列号(Sequence)：2个字节
   标识符(Identifier)：2个字节

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?

   答：ICMP类型：0(代表ICMP响应)，代码：0
   还有Checksum、Indetifier，Sequence number字段
   校验和(Checksum)：2个字节
   序列号(Sequence)：2个字节
   标识符(Identifier)：2个字节

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



答：主机IP：192.168.1.101

目标IP：138.96.146.2

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?

答：发送请求路由跟踪的数据包为UDP 数据包，IP协议号为17。

如果未发送UDP数据包，是ICMP协议为01。

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?

答：路由跟踪的 ICMP 的 Type 、Checknum, Sequence Number, Data不同于前半部分 ICMP 的 PING 的查询数据包。

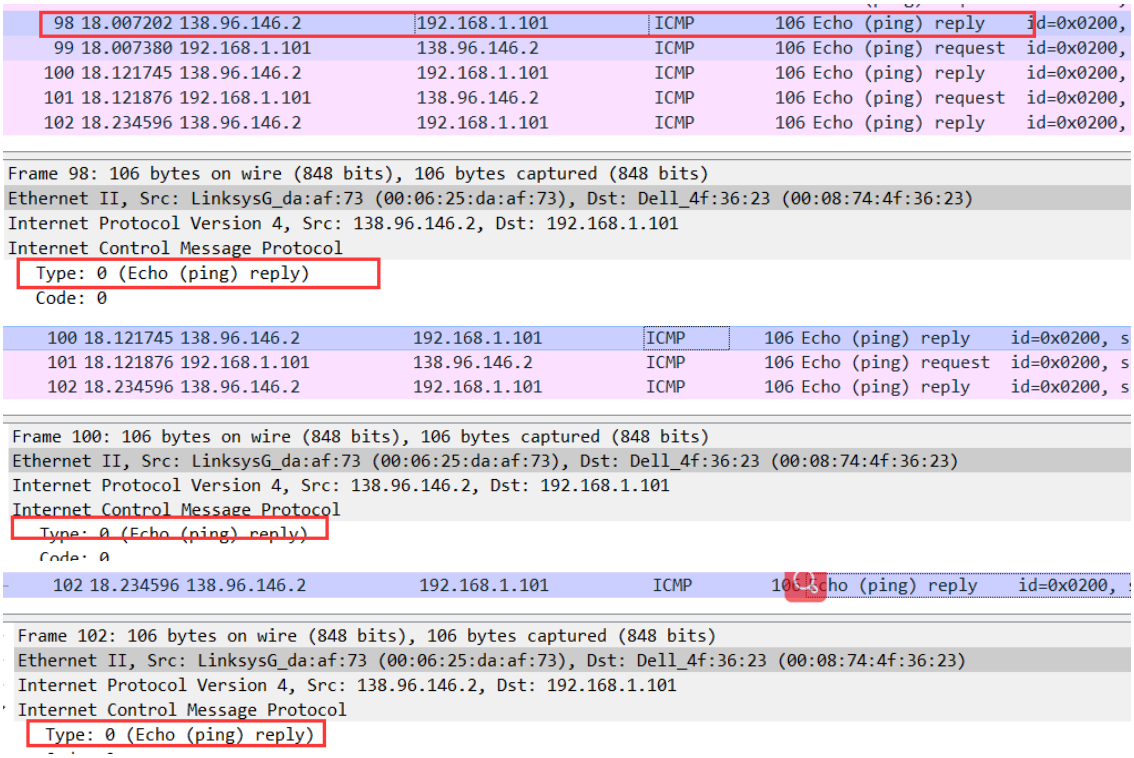
8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xec5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 512 (0x0200)
    Identifier (LE): 2 (0x0002)
    Sequence Number (BE): 26369 (0x6701)
    Sequence Number (LE): 359 (0x0167)
    [Request frame: 3]
    [Response time: 413.442 ms]
  > Data (32 bytes)
```

```
Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:2
Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.101
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x2c16 [correct]
    [Checksum Status: Good]
    Unused: 00 00 00 00
  > Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
  v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x51fe [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 512 (0x0200)
      Identifier (LE): 2 (0x0002)
      Sequence Number (BE): 41985 (0xa401)
      Sequence Number (LE): 420 (0x01a4)
```

答：多了 ICMP 的请求数据包的内容。

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?



答：**源主机收到的最后三个ICMP数据包是目的主机发送给我的ICMP回应数据包**，因为路由查询是使用逐渐递增TTL的查询数据包，最后的ICMP查询数据包的TTL已经大于到达目的主机中间路由跃点数，type为0，因此不会被目标主机丢弃来发送ICMP超时的数据包，所以只会收到ICMP响应数据包。