实验 3：ICMP

班级_____　学号　2021　姓名_____

一、 实验内容

在本实验中，我们将探讨 ICMP 协议的几个方面：

1. **Ping 程序生成的 ICMP 消息**
2. **Traceroute 程序生成的 ICMP 消息**
3. **ICMP 消息的格式和内容**

在进行本实验之前，我们鼓励您查看 text1 第 4.4.3 节中的 ICMP 资料。 我们在 Microsoft Windows 操作系统的中介绍此实验。 但是，将实验环境转换为 Unix 或 Linux 环境非常简单。

二、 实验操作步骤及结果

1、ICMP 和 Ping

（1）实验步骤

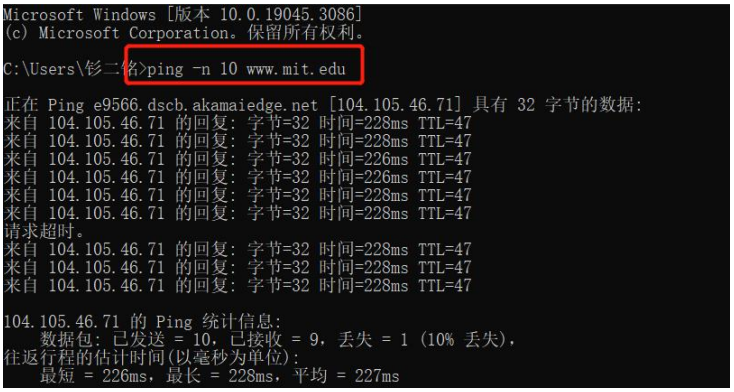
① 打开 Windows 命令提示符。

② 启动 Wireshark 数据包嗅探器，然后开始 Wireshark 包捕获。

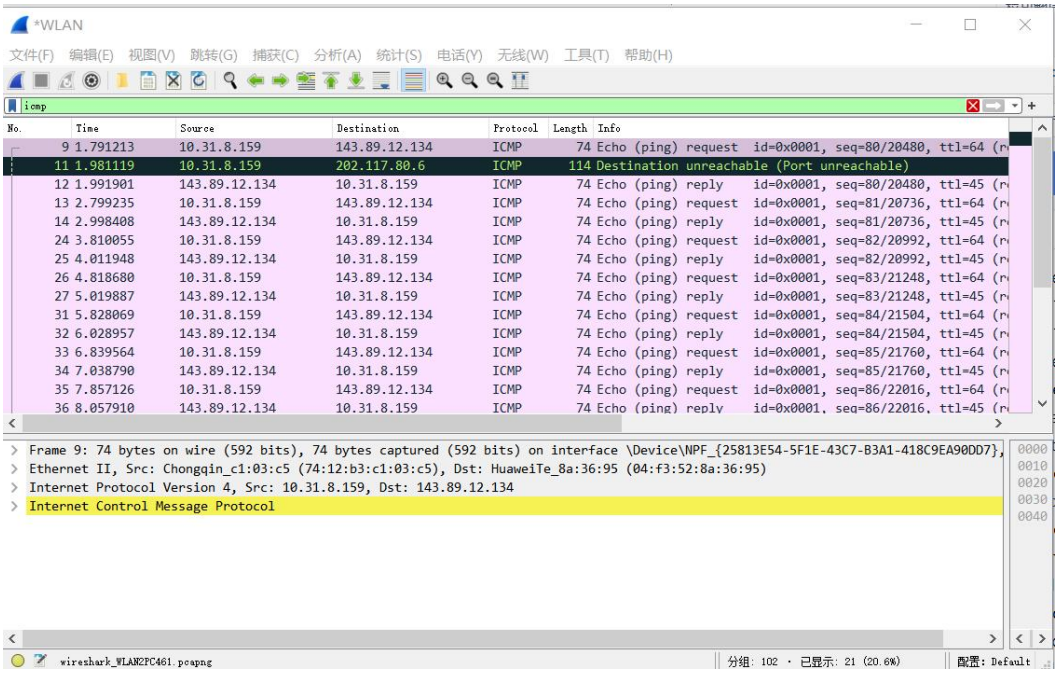
③ 在 MS-DOS 命令行中键入“ping－n 10 hostname”或“c:\windows\systems32\ping－n 10hostname”。然后键入 return 来运行 Ping 程序。

④ 当 Ping 程序终止时，停止 Wireshark 中的数据包捕获。

命令提示符中显示情况如下：



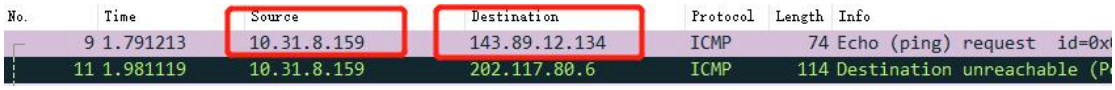
Wireshark 中数据包捕获情况如下：



（2）回答问题

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

我的主机 IP 地址为 10.31.8.159，目的 IP 地址为 143.89.12.134。如下图所示：



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

ICMP 是网络层的协议。它不须要传输层 TCP 或者 UDP 的承载，而是直接使用 IP 数据报承载。ICMP 报文有一个类型字段和一个编码字段，用来表示特定的消息被接收，它能够解释所有消息，所以 ICMP 在应用层不需要端口号。

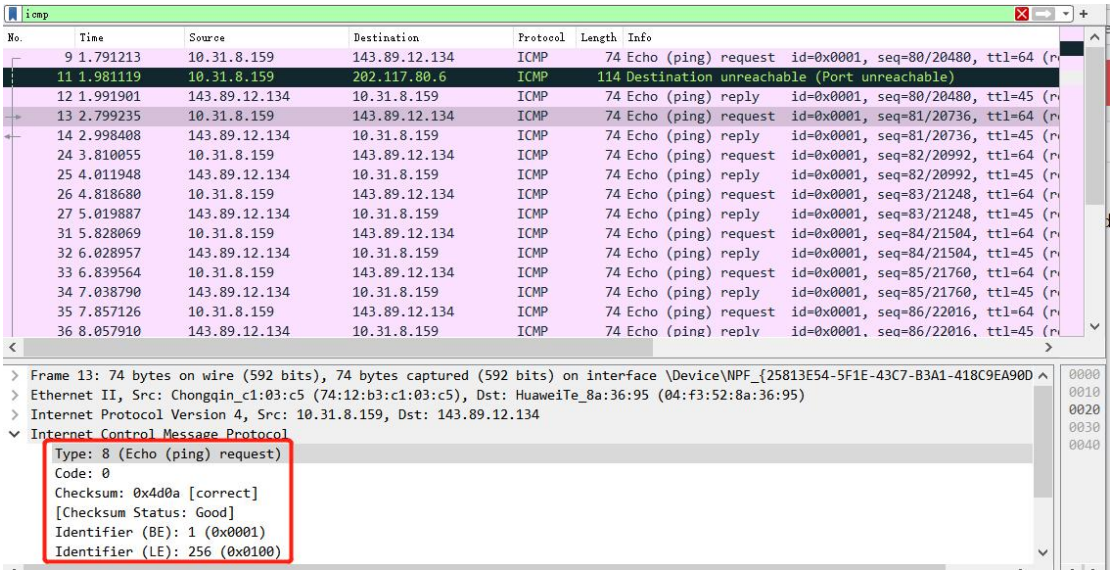
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

查看捕获到的请求数据包可知：

ICMP TYPE: 08　　CODE: 0　　Checksum: 2 bytes

Sequence number: 2 bytes　　Identifier: 2 bytes

如下图所示：

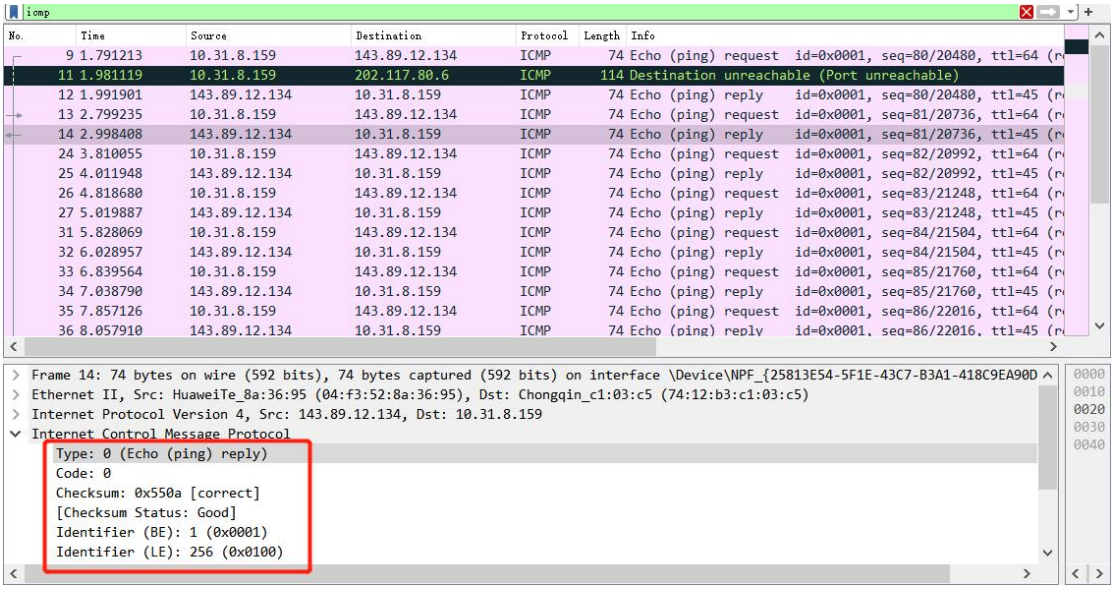


4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

查看捕获到的回复数据包可知：

ICMP TYPE: 0　　CODE: 0　　Checksum: 2 bytes

Sequence number: 2 bytes　　Identifier: 2 bytes



2、ICMP 和路由跟踪

（1）实验步骤

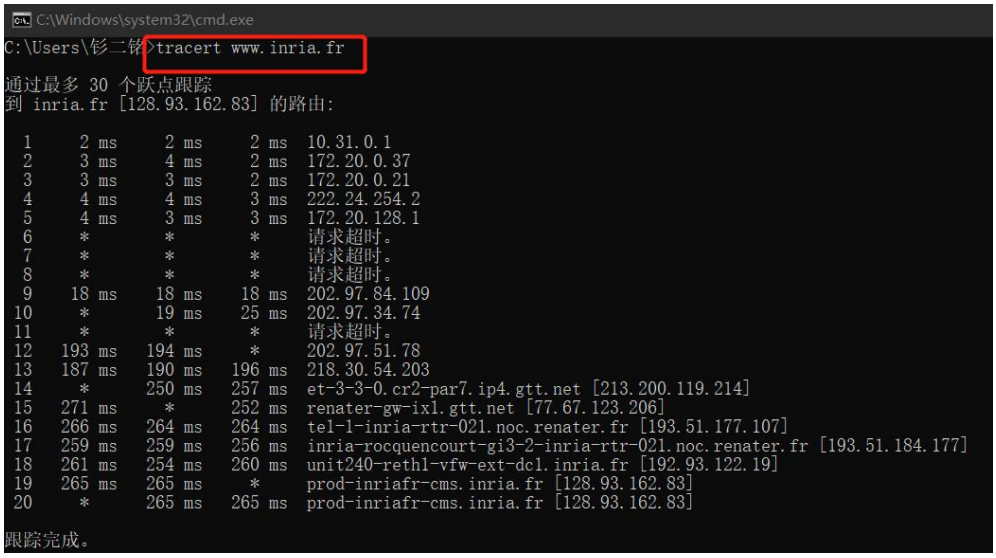
① 打开 Windows 命令提示符。

② 启动 Wireshark 数据包嗅探器，然后开始 Wireshark 包捕获。

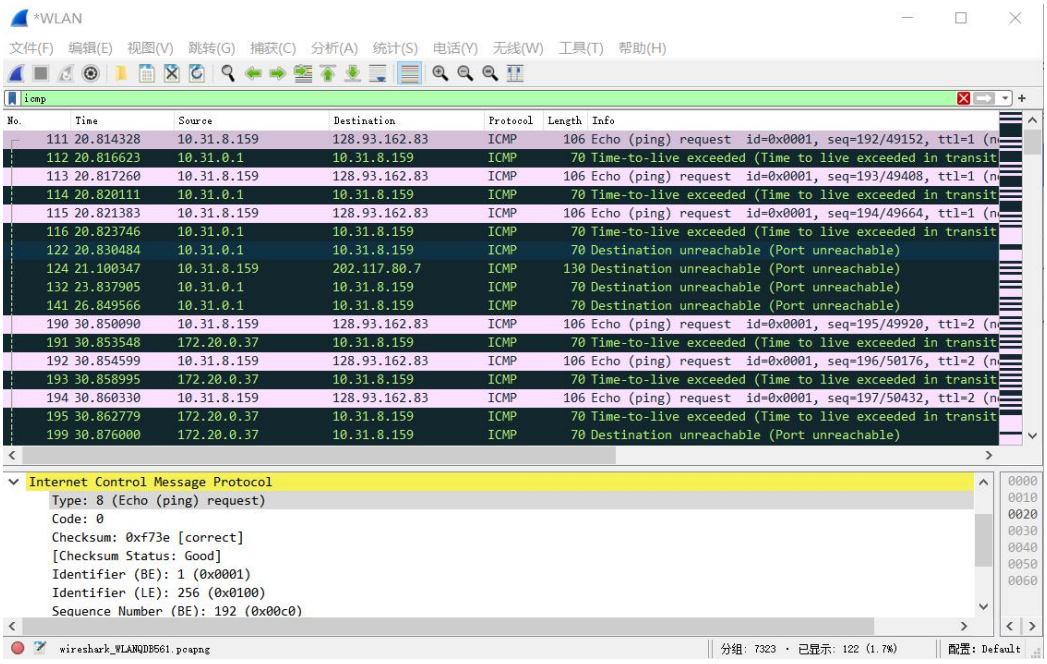
③ 在 MS-DOS 命令行中键入“tracert hostnam”或“c:\windows\systems32\tracert hostname”，其中 hostname 是另一个大陆上的主机。然后键入 return 来运行 Ping 程序。

④ 当 Ping 程序终止时，停止 Wireshark 中的数据包捕获。

命令提示符中显示情况如下：



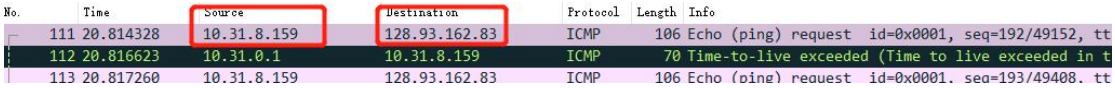
Wireshark 中数据包捕获情况如下：



（2）回答问题

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

我的主机 IP 地址：192.168.43.68　　目的主机 IP 地址为：128.93.162.83



No.	Time	Source	Destination	Protocol	Length	Info
111	20.814328	10.31.8.159	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=192/49152, tt
112	20.816623	10.31.0.1	10.31.8.159	ICMP	70	Time-to-live exceeded (Time to live exceeded in t
113	20.817260	10.31.8.159	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=193/49408, tt

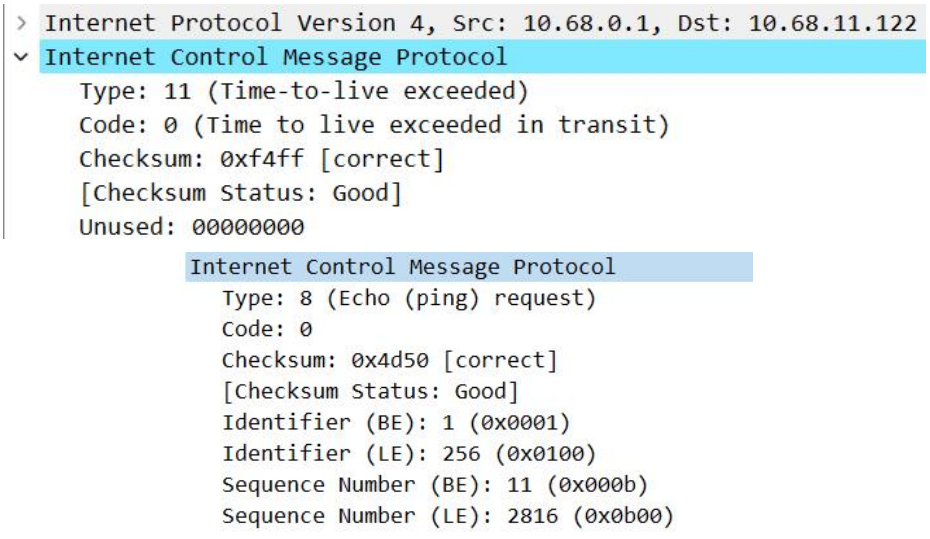
6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

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?

第一张图片显示了实验第一部分发布的 ICMP 包，第二张图片显示的是 tracert 发布的 ICMP 数据包。经过观察，我们可以发现第一张图片比第二张图片多了响应帧。响应包完整地包含 ICMP ping 请求包中的数据，以及发送方的 IP 地址、接收方的 IP 地址，时间戳和序列号。

比对的截图如下：



```
> Internet Protocol Version 4, Src: 10.68.0.1, Dst: 10.68.11.122
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 Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d50 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 11 (0x000b)
    Sequence Number (LE): 2816 (0x0b00)
```

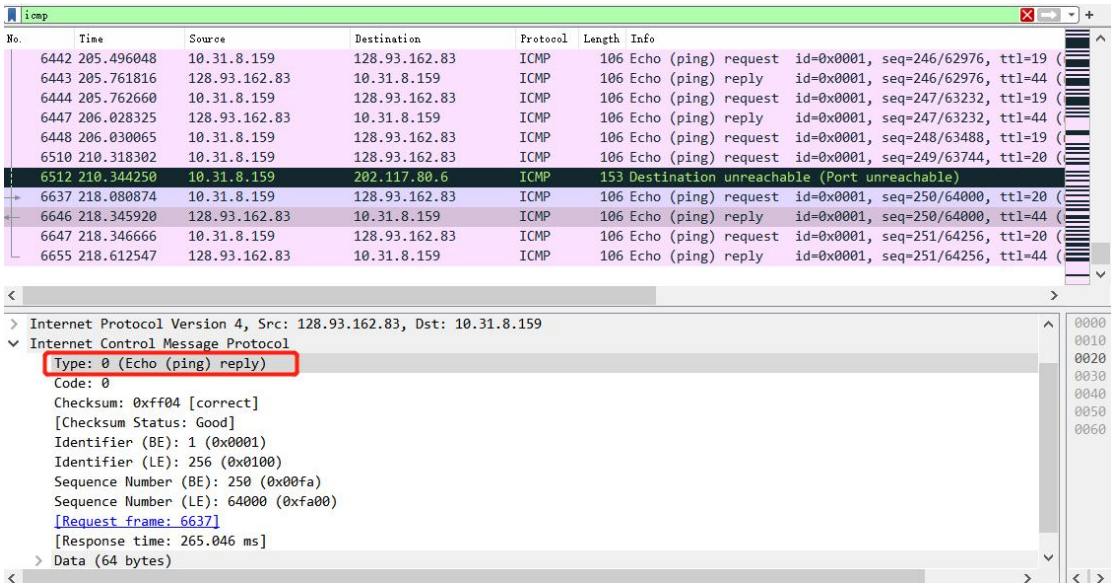
8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

ICMP 错误数据报包括：所有 IP 字段和原来的 ICMP 字段。如下图所示：

```
> Internet Protocol Version 4, Src: 10.68.0.1, Dst: 10.68.11.122
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: 10.68.11.122, Dst: 104.155.134.41
  > Internet Control Message Protocol
```

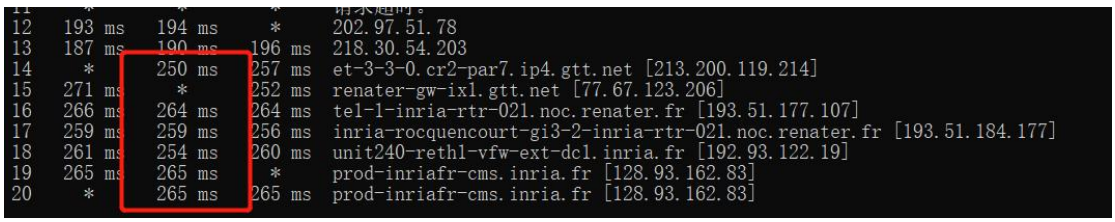
9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

最后三个 ICMP 数据报类型码都为 0，而不是 11（TTL 过期），它与错误报文段的不同之处是引文数据报在 TTL 过期之前已经全部送往目的地。如下图所示：

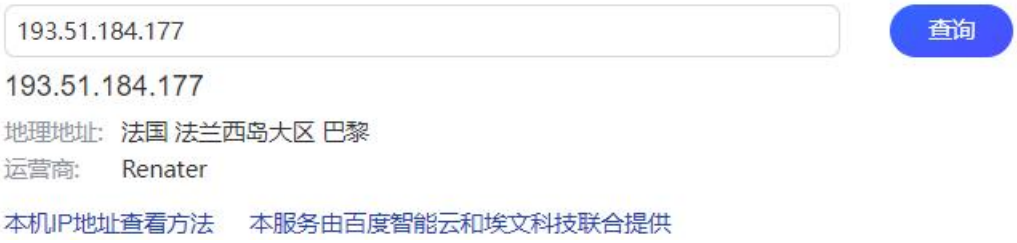


10. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this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

14-20 明显比其他链路延时大。如下图所示：



查询 IP 地址所属地区可知，对应节点位于外国（法国），因此延时很大。



三、实验中存在问题及分析

通过进行 ICMP 实验，我对计算机网络的理解有了进一步的提升，并且在解决问题时逐渐熟悉了 wireshark 软件，感到越发得心应手。然而，在解决问题的过程中，我曾经遇到了一些困扰。首先，由于 ICMP 反馈的信息过多，我在寻找特定信息的过程中遇到了问题，通过与同学的讨论，最终我成功地解决了这个问题。

另外，对实验文档的阅读一定要仔细，我在做实验的过程中几次因为审题不清遇到了问题，可以借助翻译插件阅读英文文档，减少误解。

总的来说，本次实验遇到的问题比前几次少，但是还由于对理论知识不够熟悉，导致我理解实验过程有些困难，需要将理论课和实验课结合起来。