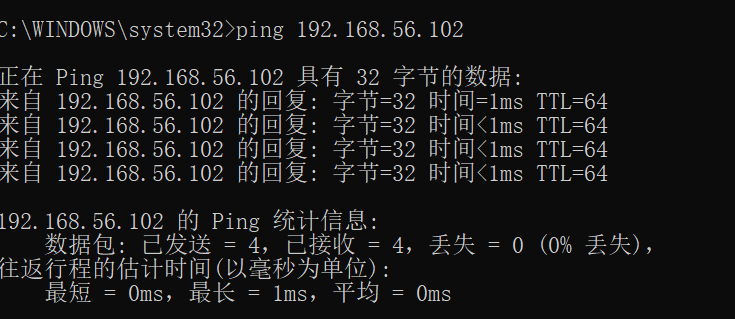
1. **实验目的：**
2. 掌握ping命令和tracert命令的用法，了解它们的工作过程
3. 通过抓包理解ICMP协议原理
4. **实验配置**

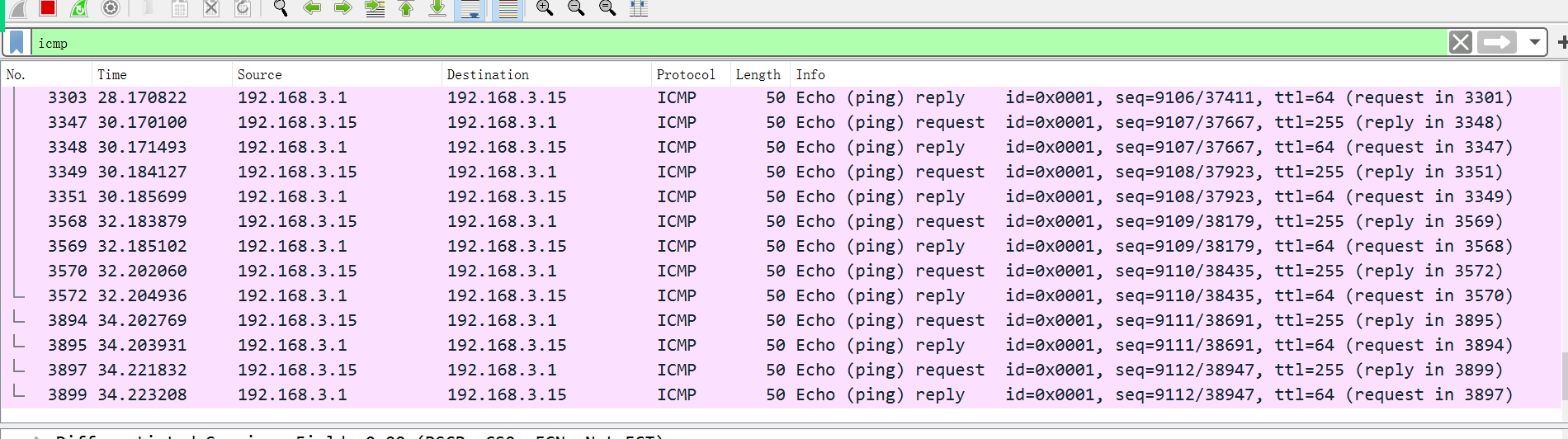
与因特网连接的计算机；

主机操作系统为windows；

Wireshark、IE等软件。

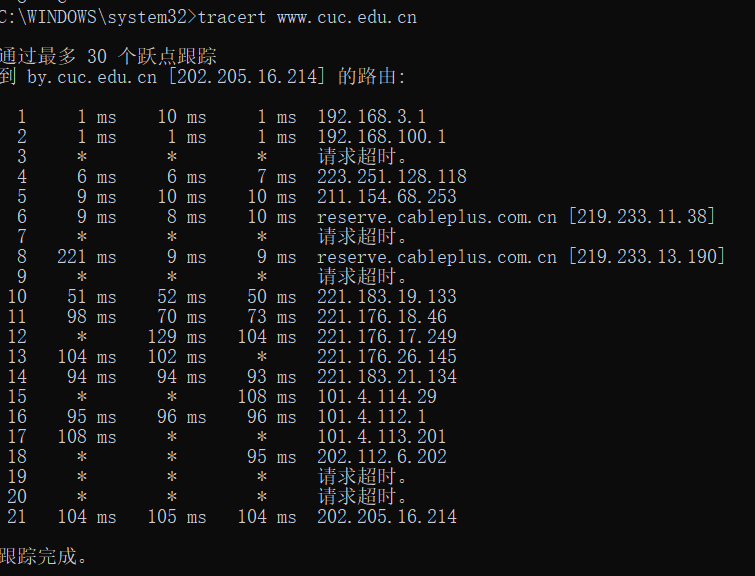
1. **实验内容：**
2. **Ping某个主机，并抓包找到ICMP的请求包和相应的回应包，分析ping命令的原理。**

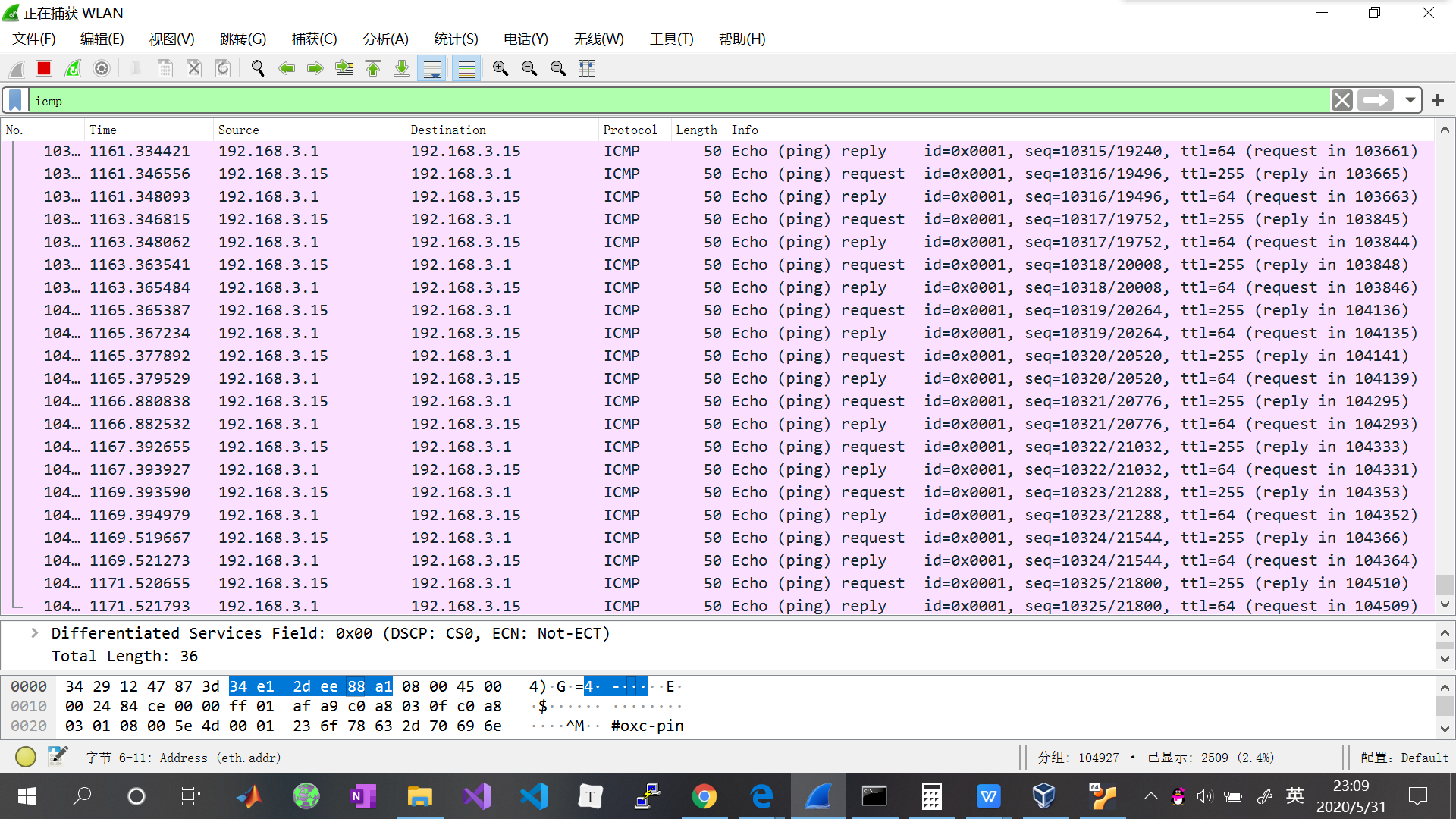




Ping命令会构建一个固定格式的ICMP请求数据包，然后由ICMP协议将这个数据包连同地址一起交给IP层协议，IP层协议将以本机IP地址作为源地址，加上一些其他的控制信息，构建一个IP数据包，并在一个映射表中查找出目的地址所对应的物理地址，一并交给数据链路层。

1. **Tracert主机www.cuc.edu.cn，抓取过程中的所有ICMP包，对应控制台上的显示信息，分析Windows系统上tracert命令的实现过程。**





可以看到途径路由器的IP地址：

192.168.3.1->192.168.100.1->223.251.128.118->211.154.68.253->219.233.11.38->219.233.13.190->221.138.19.133->221.176.18.46->221.176.17.249->221.176.26.145->221.183.21.134->101.4.144.29->101.4.112.1->101.4.113.201->202.112.6.202->202.205.16.214

中途\*的地方说明该次ICMP包返回时间超时。

本地主机通过各个路由器以及远程主机返回的这些ICMP报文，知道了这些路由信息，即目的主机所经过的路由器的IP地址，以及到达其中每一个路由器的往返时间。从而实现了跟踪的功能。

1. **说明Ping和Tracert命令执行时，命令行中显示的时间是怎么得出的。**

Tracert 每一跳同时发出3个TTL包 返回的三个时间都是你到达这个路由的时间，三个时间值都PING值  
 Tracert 先发送 TTL 为 1 的回应数据包，并在随后的每次发送过程将 TTL 递增 1，直到目标响应或 TTL 达到最大值，从而确定路由。通过检查中间路由器发回的“ICMP 已超时”的消息确定路由。某些路由器不经询问直接丢弃 TTL 过期的数据包，这在 Tracert 实用程序中看不到。

参考文献：

1. <https://jingyan.baidu.com/article/54b6b9c0081fbf6d593b4713.html>
2. <https://blog.csdn.net/dan15188387481/article/details/49893375>