**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 成绩评定

实验项目名称 TCP/IP协议配置与网络实用命令 指导教师 潘冰

实验项目编号 2 实验项目类型 实验地点 计算机网络实验室

学生姓名 罗清 学号 2019053295

学院 智能科学与工程学院 系 专业 信息安全

实验时间 2021 年 9 月 7 日 午～ 9 月7 日 午温度 ℃湿度

**一、实验目的**

1. 熟悉TCP/IP协议的配置；

2. 熟悉常见网络命令的使用；

3. 加深对TCP/IP协议的认识并对简单网络故障诊断和网络分析；

4. 进一步熟悉使用Wireshark捕获信息，初步了解ping、tracert命令的工作过程；

5. 培养使用Wireshark对网络工作过程进行跟踪分析的习惯，为计算机网络（和网络安全）课程的学习打下基础。

**二、实验内容**

1.以Windows或Linux系统为例，对TCP/IP协议进行安装和配置；

2.利用ipconfig查看主机接口的配置，并理解其含义；

3.利用route查看本机路由，并了解其含义；

4.利用netstat查看当前主机上网络简介统计信息，了解其含义；

5.利用ping对网络故障诊断与分析，用Wireshark分析其工作过程；

6.利用tracert跟踪数据包在传输过程中经过的路径，用Wireshark分析其工作过程。

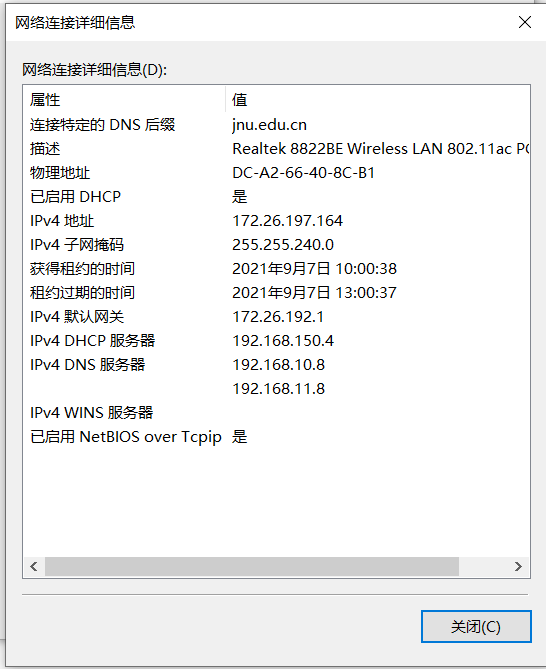
**三、实验环境**

一台处于校园网网络环境、具有正常网络功能的PC机。

**四、实验步骤**

**1、TCP/IP协议的安装和配置**

Windows 10系统在初次启动时就自动安装配置了TCP/IP协议，可以直接进行网络的连接使用。

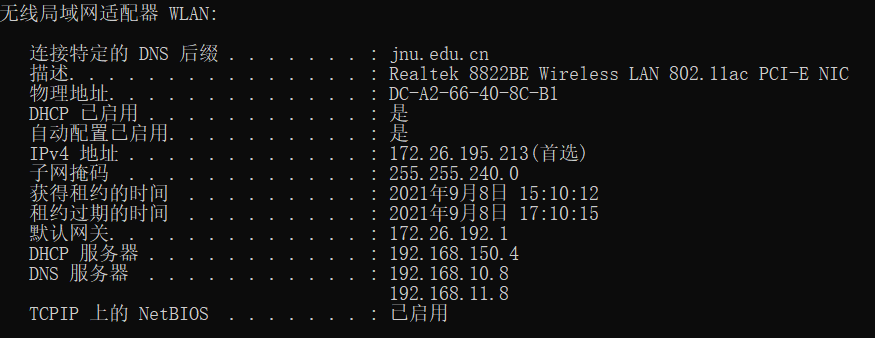


上网查询资料了解相关含义：

1. **IP地址**：IPv4协议规定给连接在网络上的每台计算机都分配一个唯一的IP地址（IPv4由于32位IP地址有限，通常配合子网掩码使用），地址分为4部分，每部分取值0~255。每个IP地址由于配合子网掩码使用又分为两部分，一个称为网络地址（Network Address），用来表示计算机所属网络的网络号；另一个称为主机地址（Node Address），用来表示某个网络上某个特定主机的主机号。
2. **子网掩码**：又称为网络掩码、地址掩码，用来与IP地址计算得到网络号，标识哪些位表示主机号。如上图为本PC机的网络连接属性，IP地址为172.26.197.164就被子网掩码为255.255.240.0分为网络号172.26.192.0和主机号0.0.5.164。
3. **网关**：网关在网络层以上实现网络互连，用于两个高层协议不同的网络互连，是数据的中转站。与网桥不同，网关不只是简单地传递信息，还要对收到的信息进行重新封装数据包以适应目的系统的需求。
4. **DNS服务器**：即域名系统，由解析器和域名服务器组成。域名服务器保存有该网络中所有主机的域名和对应IP地址，并且具有将域名转换为IP地址返回的功能。

**2、常见网络命令**

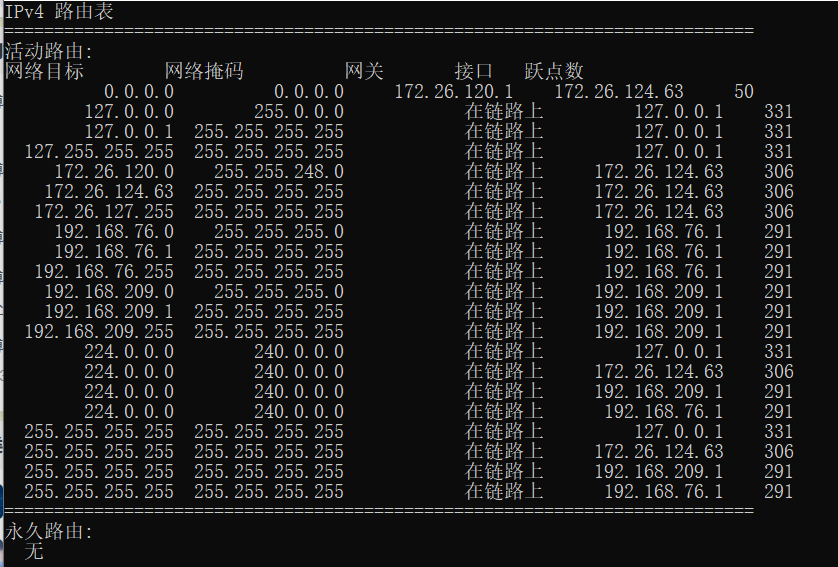
（1）ipconfig



1. **连接特定的DNS后缀**：PC机从DHCP server获取地址时，如果配置了该项，那么在用nslookup查询dns时，PC机会先尝试在域名后面加上这个后缀查询，如果查询失败，则再发起一次正常查询。
2. **物理地址**：即MAC地址，工作在数据链路层，是传输数据时真正标识主机的地址。
3. **DHCP/自动配置已启用**：即动态主机配置协议，指由服务器控制一段IP地址，客户机登录服务器时就可以自动获得服务器分配的IP地址和子网掩码。
4. **默认网关**：连接子网和外网的的设备，通常是一个路由器。

（2）route

打开cmd界面输入route print命令查看本机路由表如下



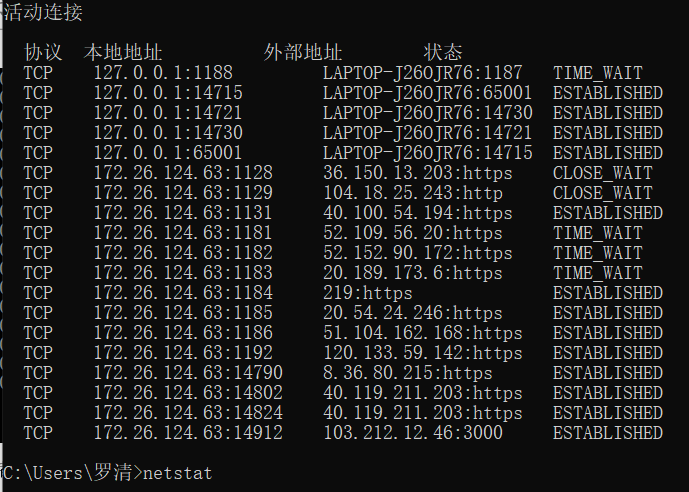
分成五部分，分别是网络目标、网络掩码、网关、接口、跃点数。

网络目标即目的IP地址，网络掩码即子网掩码，网关第一行即默认网关，接口代表数据包从哪个地方出去，跃点数则代表在路径选择过程中信息的可信度（跃点数越小，可信度越高）。

其中，第一条表项中网络目标的的0.0.0.0表示这样一个集合：所有不清楚的主机和目的网络。注意到子网掩码全0，故IP地址与子网掩码运算结果也为全0，即数据匹配不到时就一定会转发到默认网关172.26.120.1进行路由。

（3）netstat

打开cmd界面输入netstat命令查看网络协议的统计结果（连接和侦听端口的状态）如下



注意到本次统计用到的端口协议都为TCP，第二列为本PC机地址以及使用的端口（套接字），第三列为外部地址，第四列则为该端口目前的状态，有CLOSE\_WAIT，TIME\_WAIT，ESTABLISHED。其中CLOSE\_WAIT代表端口关闭后进入时间等待，TIME\_WAIT代表主动关闭TCP连接的一方会进入的时间等待状态，ESTABLISHED则代表打开（或已建立）的状态。

此外，TCP建立过程其实还会有LISTENING、FIN\_WAIT、LAST\_ACK等状态，此次统计没有给出。

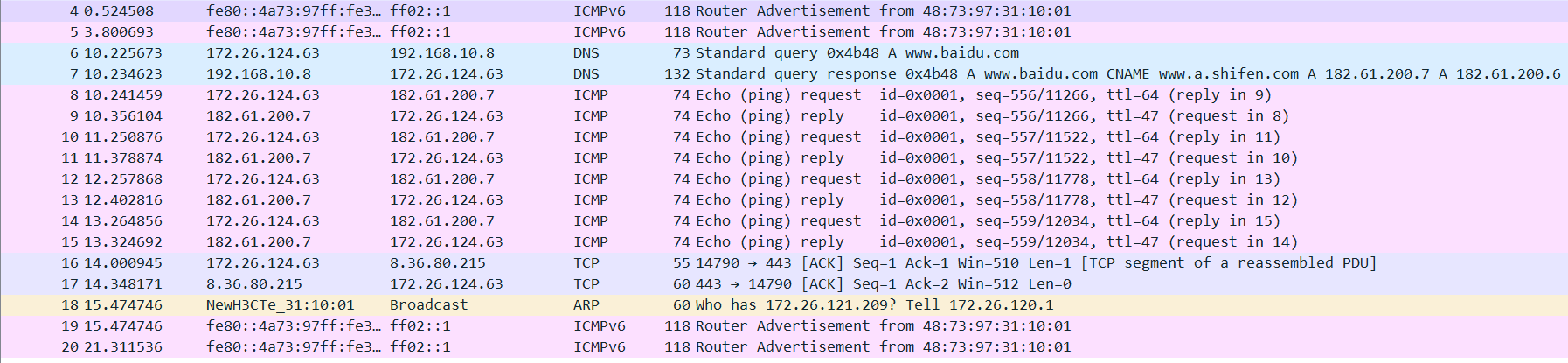
（4）ping

打开cmd界面输入ping IP地址或域名查看ping的结果如下

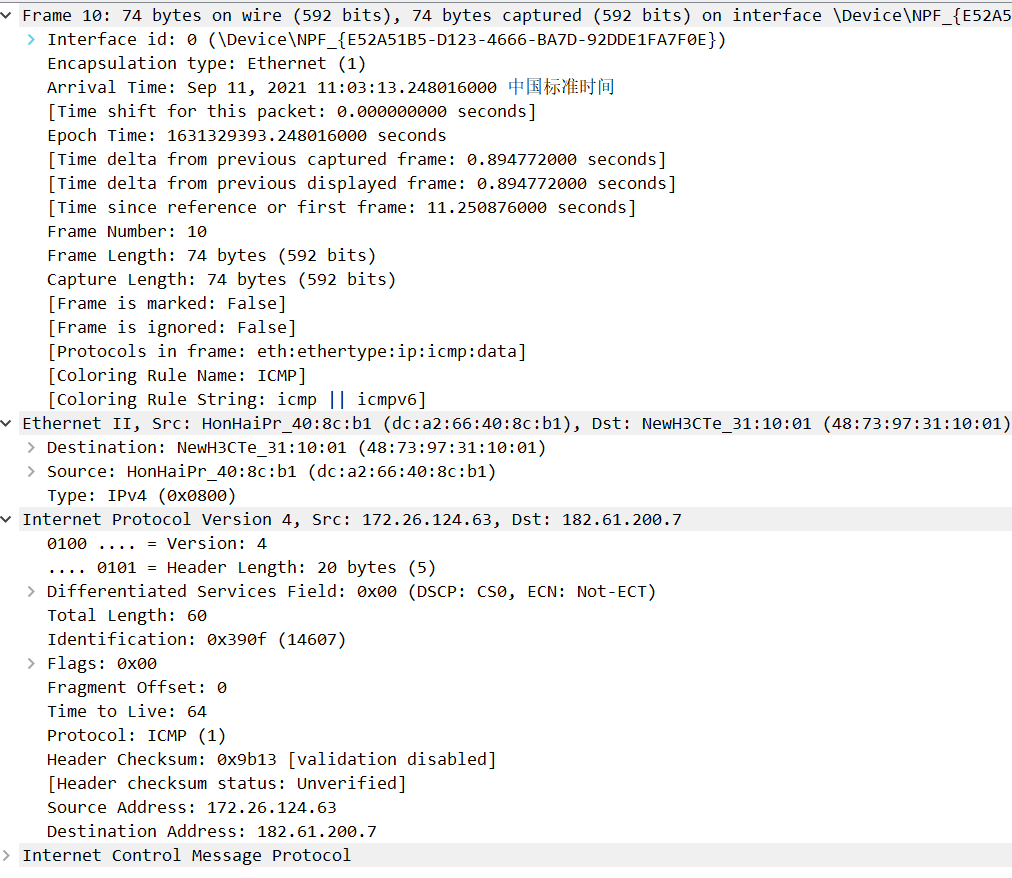


下面对上述ping过程作说明：

1. 这是一次成功的ping
2. ping百度的域名，DNS服务器会自动解析IP地址为182.61.200.7
3. 没有设置参数时，默认发送32字节的数据包
4. 默认发送了四个数据包，在接受到第四个回应的数据包后结束命令
5. 统计结果返回耗时时间的统计（最短时间、最长时间、平均时间），丢包率等



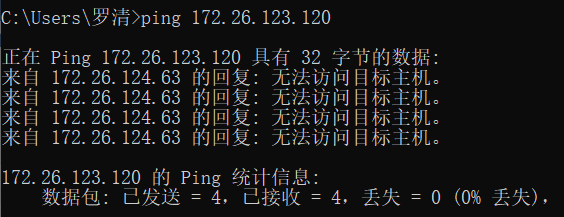
在WireShark中进行分析，可以发现此次ping开始时需要进行DNS的解析（本机发送一个请求，收到一个回复），ping的过程发送接受的是ICMP数据包（四次对应八个），打开一个进行查看。



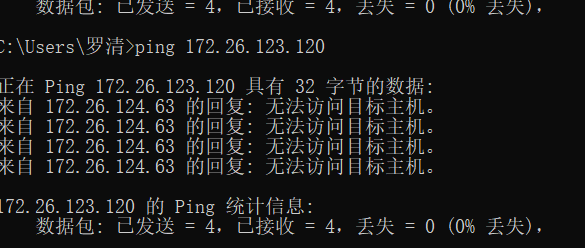
可以容易得到，ICMP数据包作为一个网络层的包，可以看到网络层、数据链路层和物理层的信息（有具体数据data、时间、协议、版本号、正误等信息）。

接下来进行无法成功的ping（让室友连接校园网与本PC机处于同一网段，开启防火墙，由我来先后进行ping（分为室友接上网、室友断开网两种情况））

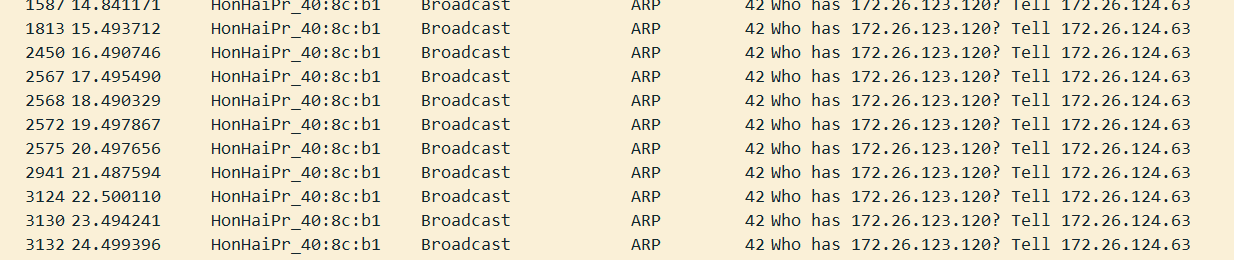
1. 室友接上网络



1. 室友断开网络



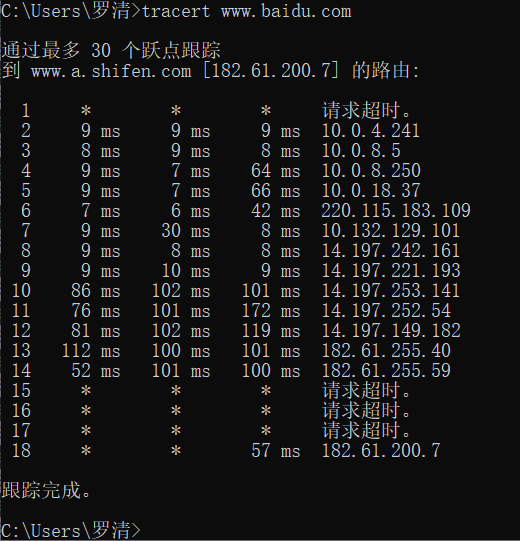
发现两种情况的ping结果相同，在WireShark中对该过程抓到的包进行查看



这里的172.26.124.63是本PC机的IP地址，即最终返回的都是ARP广播未果的结果，不能从这里判断目标主机是开启了防火墙还是根本不在网络上。

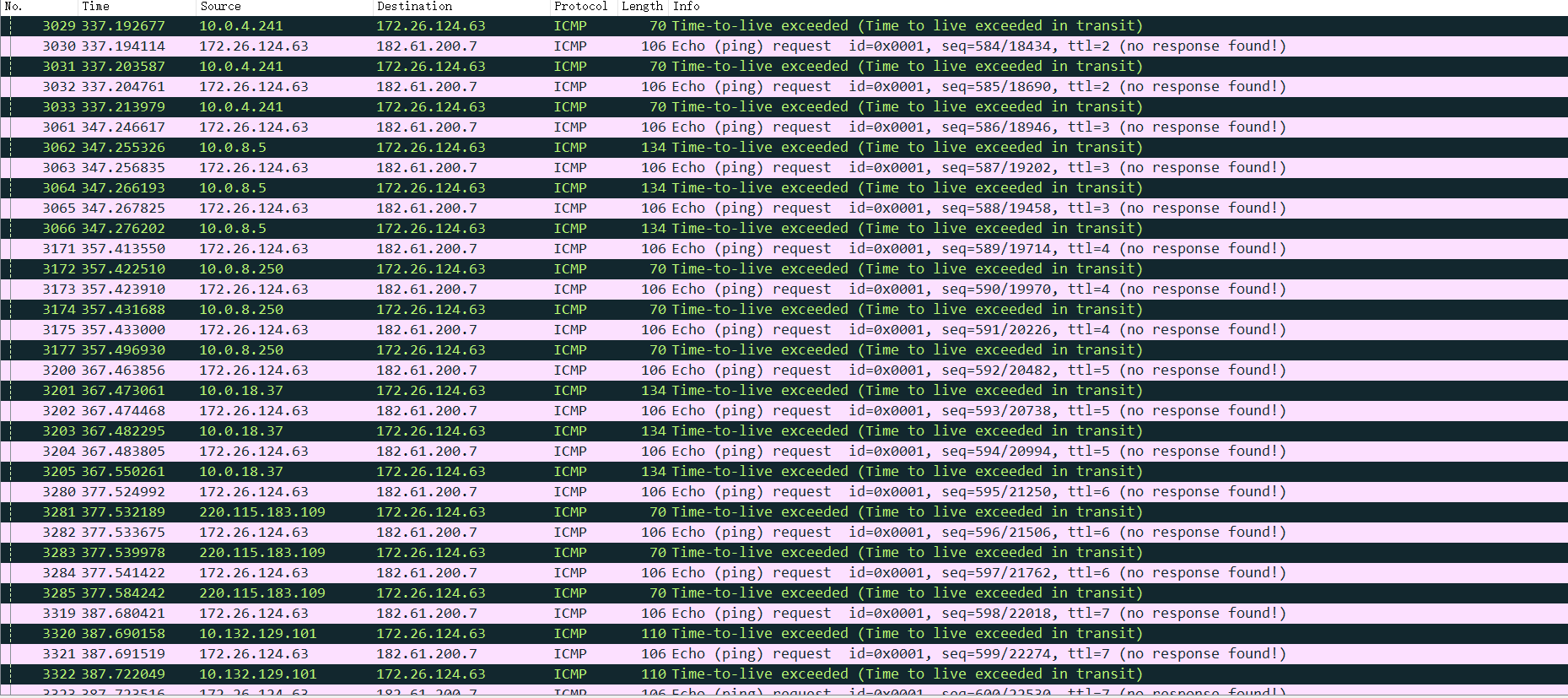
（5）tracert

打开cmd界面输入tracert IP地址或主机名查看用户数据经过路径上各个路由器的信息如下



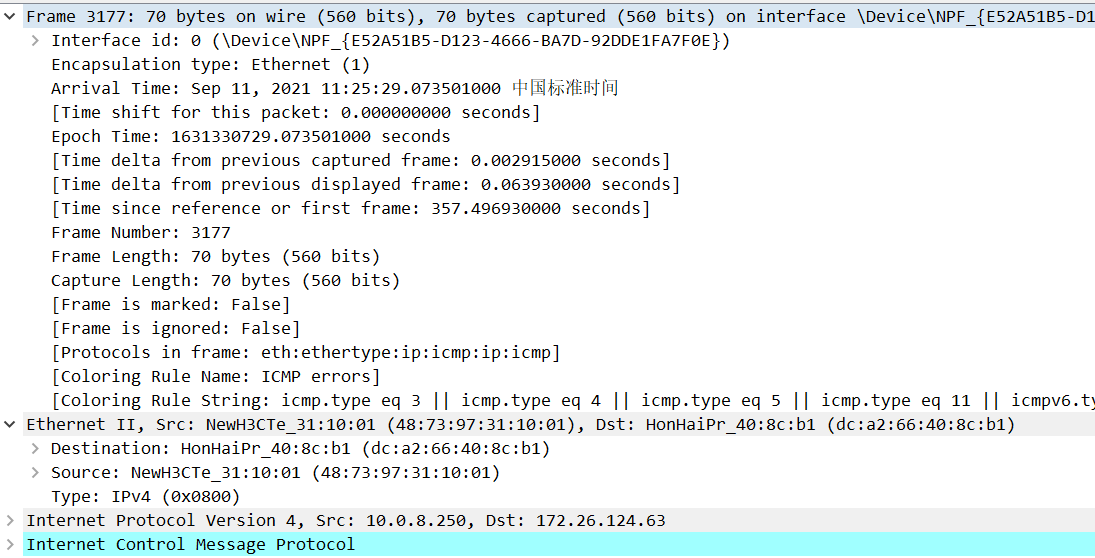
下面对上述tracert过程作说明：

1. 同样是跟踪到百度的路由，首先进行DNS的解析得到百度服务器的IP地址。
2. 从截图看出本次访问百度总共经过了18个节点，其中第一个为本PC机所在网络网关（请求超时，可以得到它设置了禁ping），最后一个为目的地址。
3. 15、16、17节点请求超时，可能是其服务器出现问题或是设置了禁ping，但没有影响总体的路由跟踪。



接下来对上述过程在WireShark中抓到的包进行分析。

可以得到黑色的ICMP包就是tracert得到的节点返回的包（Source和路由器节点对应得上）。之所以这些ICMP包是黑色的，是因为它们都刚好完成了生存时间的最后一跳（即time to live exceed），这也是tracert所应用的原理。



打开一个ICMP包进行查看，与ping过程得到的ICMP包内容类似，有从网络层到物理层的详细信息。

**五、实验思考题**

1、TCP/IP协议配置中的“网关”作用是什么？

答：网关（Gateway）是连接基于不同通信协议的网络的设备，使得数据能在这些网络之间传输。网关除了单纯的数据转发之外，还有能将数据转化为目标网络所使用的协议认可的数据形式，在实际应用中网关通常使用路由器。总的来说，网关就是一个网络连接到另一个网络的“关口”。

2、如何用ping 检测网络中的故障点？用ping 测试网络连通性时，若出现“Destination host unreahable”，则意味着什么？“Destionation host unreachable”和“Time out”的区别是什么？

答：（1）检测网络中故障点的步骤：

1. 首先，对于网站检查代理是否开启；
2. 其次，检测DNS服务是否出错。ping一个域名，如不能ping通，则表示DNS解析出现问题。
3. ping本地回环地址（127.0.0.1），如不能ping通，则表示计算机的TCP/IP协议出现错误或是网卡损坏；
4. 打开cmd输入ipconfig查看本地IP地址后ping之，如不能ping通，则表示本机的网络适配器（网卡）出现故障；
5. ping处于同一网段的计算机的IP或路由器在本网段端口的IP，如不能ping通，则表示通信线路出现故障；
6. 如果③能ping通，则ping处于不同网段的计算机的IP，如不能ping通，则表示路由器（网关）出现故障；

（2）“Destination host unreahable”即目标主机不能到达，意味着对方主机不存在或对方主机没有和网络建立连接。如果路由所经过的路由器的路由表中具有到达目标主机的路由，而因为其它原因导致目标不可到达，这时候会导致“Time out”；而如果路由表中连到达目标主机的路由都没有，这时候就会导致“Destination host unreahable”。