# 21级计算机科学与技术2班

# 计算机网络 实验六

**6.1 TCP协议分析：**

【目的】 利用wireshark 分析 TCP服务；

【要求】

**实验6.1.1**

1）启动wireshark 抓包,设置过滤显示TCP和SSL/TLS 相关的信息；

2）打开 http://[www.sohu.com](http://www.sohu.com) ；

3） 截图显示传输层及TCP，SSL/TLS 相关的连接建立、及关闭的过程。观察期间数据传输；

4） 分析并解释以上实验结果。

5） 将以上 第2）步的网址改成 <http://www.ucdavis.edu，重做以上实验>。

**6.2 UDP协议分析**

【目的】 利用wireshark 分析 UDP服务；

【要求】

**实验6.2.1**

1）启动wireshark 抓包,设置过滤显示UDP相关的信息；

2） 运行命令 traceroute 命令（windows 的是 tracert）

Tracert www.ucdavis.edu

3） 截图显示传输层及UDP 相关的信息；观察期间数据传输；

4） 分析并解释以上实验结果。

**实验6.2.2**

1）启动wireshark 抓包,设置过滤显示UDP相关的信息；

2） 运行命令 ping www.sina.com 命令

3） 观察期间数据传输；截图显示以上命令是否触发传输层及UDP 相关的数据段传输；

4） 分析并解释以上实验结果。

## 实验6.1.1

启动wireshark 抓包,设置过滤显示UDP相关的信息

过滤信息可设置为以下两者过滤方式的一种:

f8b9e4082e333d3016f635b629ac514

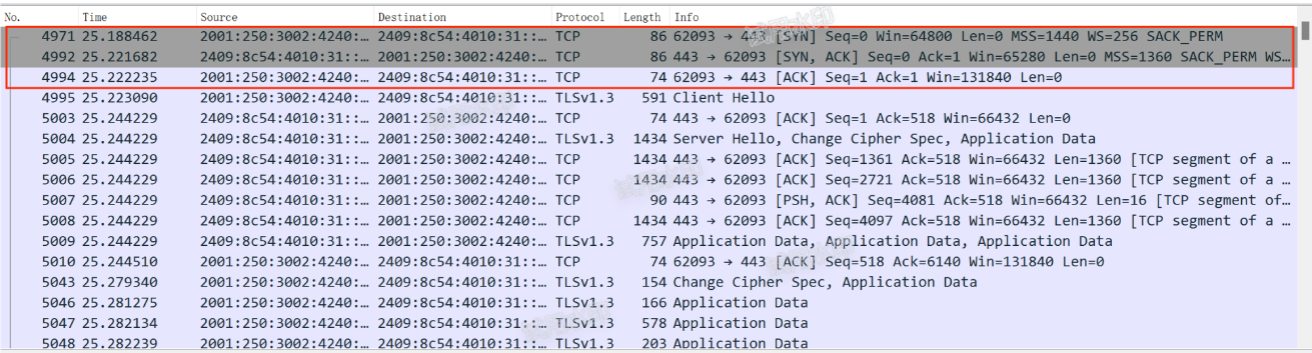
fad95c55f733eeb0409f76d742b4508

**打开http://www.sohu.com，过一段时间关闭,追踪TCP相关的信息**

**抓包信息为:**

**分析抓包信息:**

**1.首先tcp的三次握手**



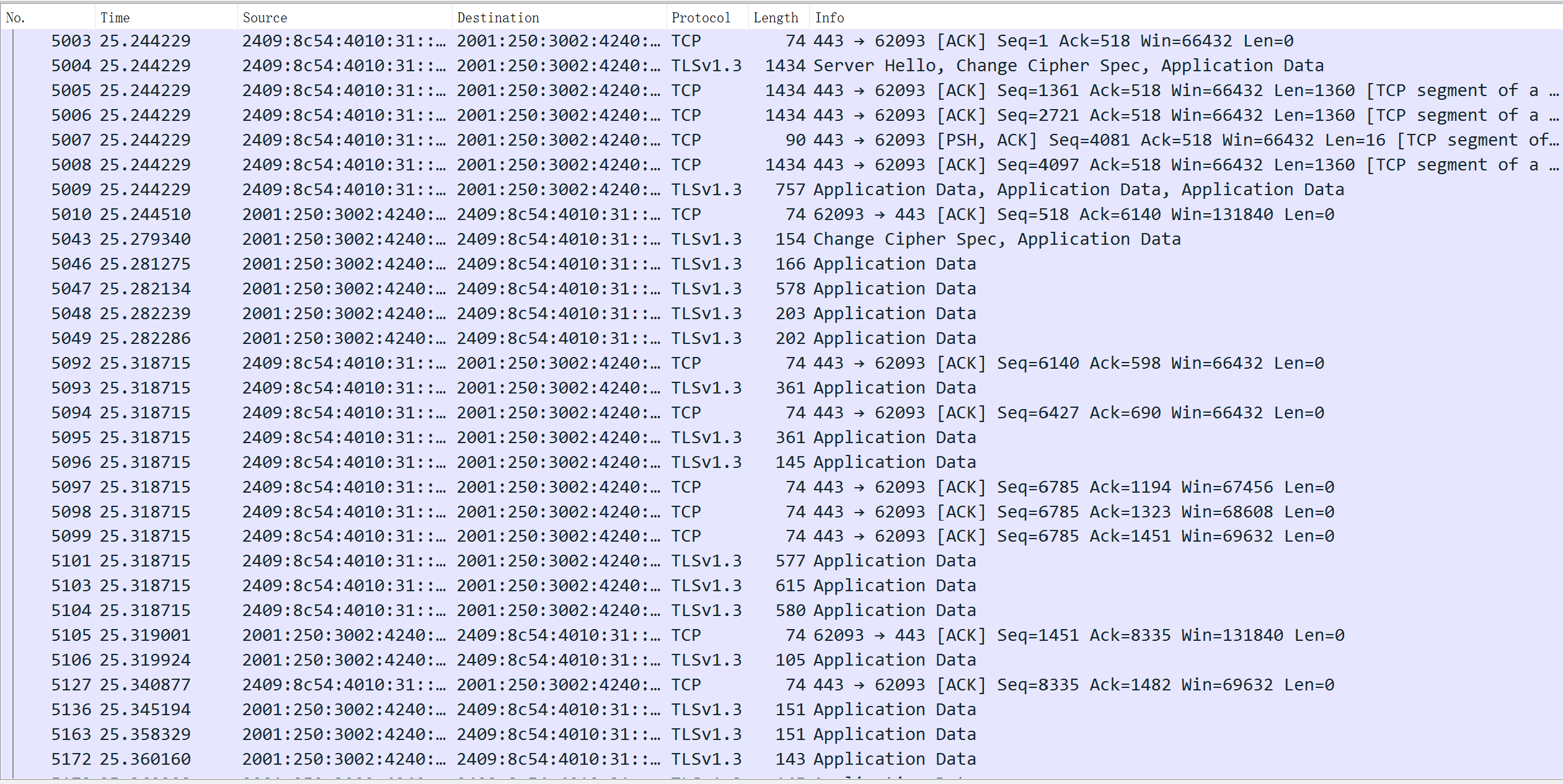
**首先客户端先向服务端发送SYN=1，请求建立连接，发送的Seq=0**

**然后服务端接收到，回复客户端的SYN 发送SYN=1与ACK=1 服务器端发送Seq=0**

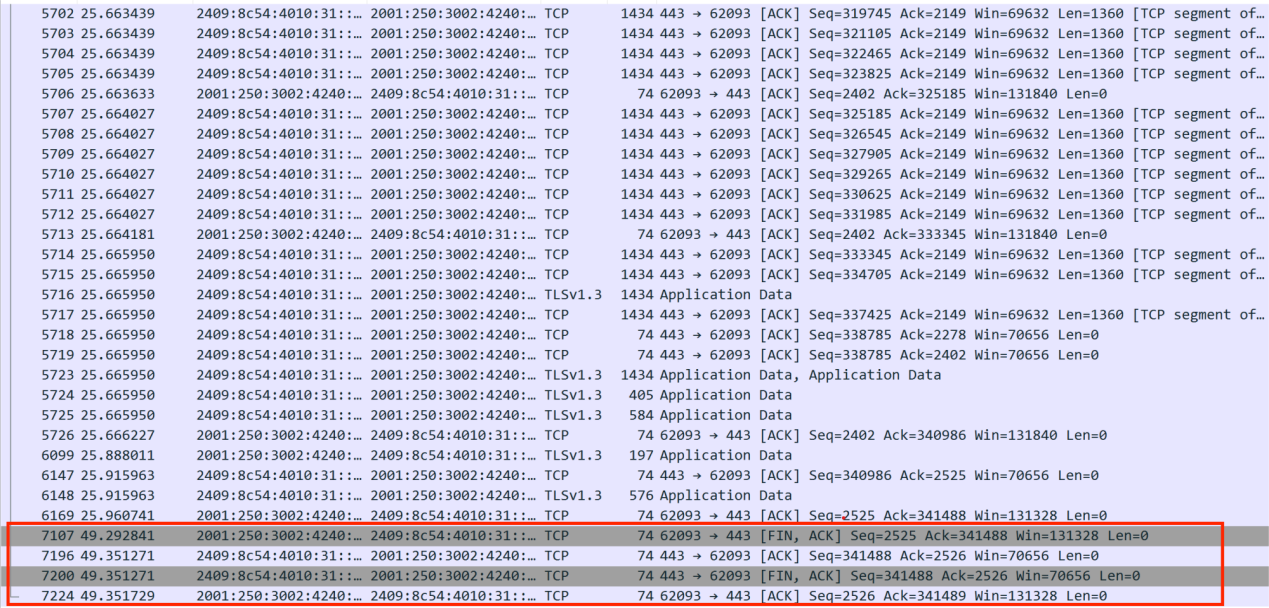
**客户端接收到 ，检测回复信息后 给服务端发送一个ACK=1 表示TCP连接已经建立**

**在TCP连接建立后，客户端向服务器发出的TLS问候消息"ClientHello" ，包含了与建立安全连接相关的信息和参数，表示两者可以进行数据传输。**

**2.TCP连接建立后，服务端和客户开始互传数据:**



**3.TCP的四次挥手：**



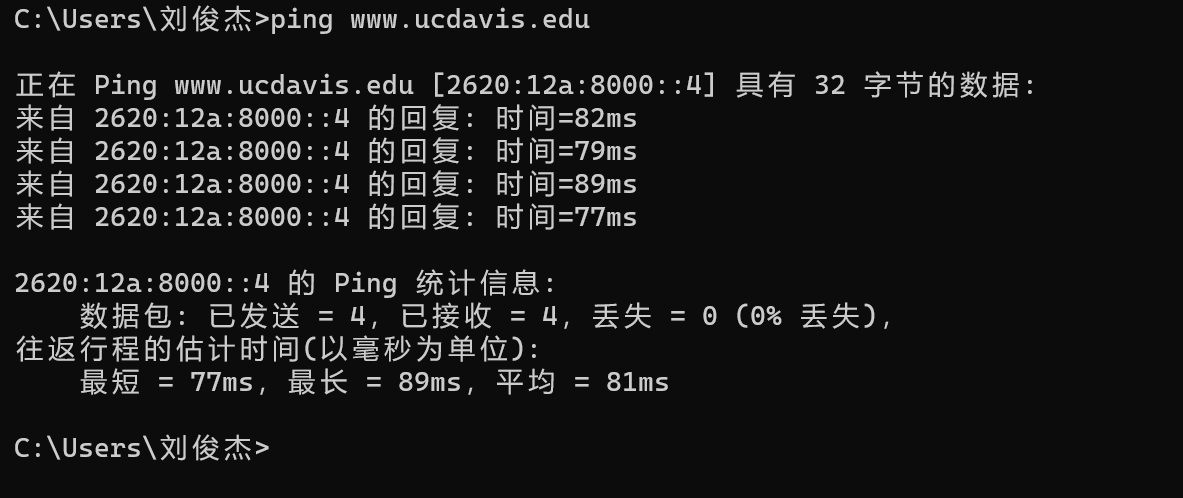
**在浏览器关闭网页后 客户机向服务端发起了[FIN ACK]中断连接的请求**

**服务端接到客户端发来的中断连接的请求，发送ACK回复，同时自己进入了半关闭状态**

**接着服务器端发送FIN给客户机，告诉客户机它不再有数据要发送。**

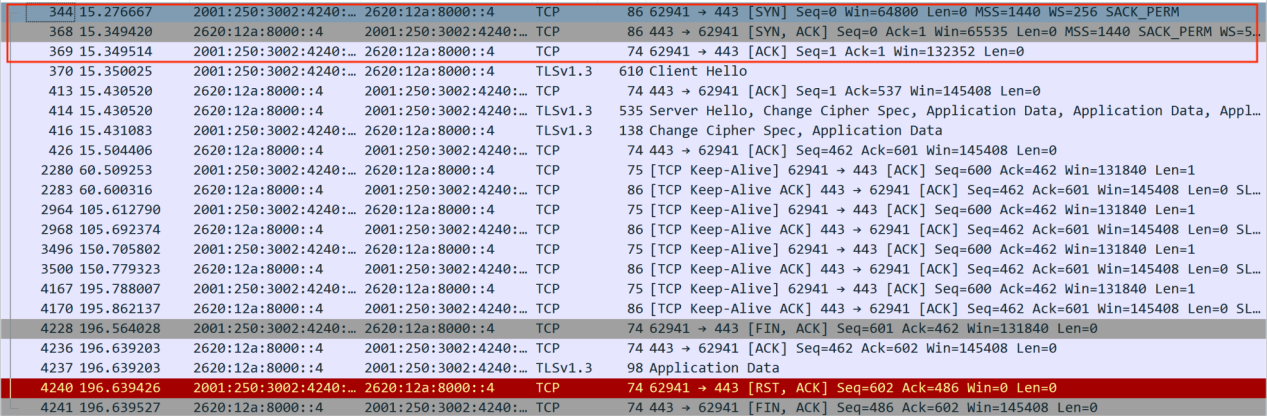
**客户机接收到服务端的FIN报文后，发送一个确认ACK报文，以确认已经接收到了被动关闭方的FIN。此时，客户机进入TIME\_WAIT状态。在TIME\_WAIT状态下，主动关闭方等待一段时间（两个最大段生存期的时间，以确保被动关闭方收到ACK），然后关闭连接，进入CLOSED状态。**

## 将网站换为http://www.ucdavis.edu



## 查询得到http://www.ucdavis.edu的IP地址

**1.TCP连接的3次握手:**



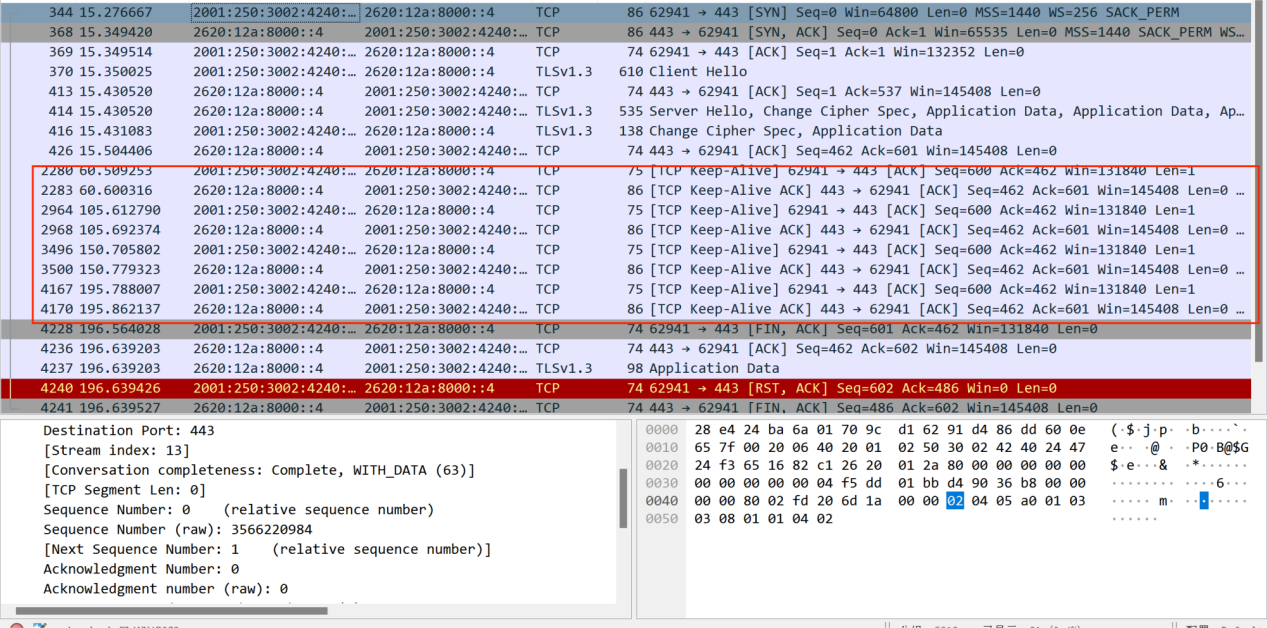
**首先客户端先向服务端发送SYN=1，请求建立连接，发送的Seq=0**

**然后服务端接收到，回复客户端的SYN 发送SYN=1与ACK=1 服务器端发送Seq=0**

**客户端接收到 ，检测回复信息后 给服务端发送一个ACK=1 表示TCP连接已经建立**

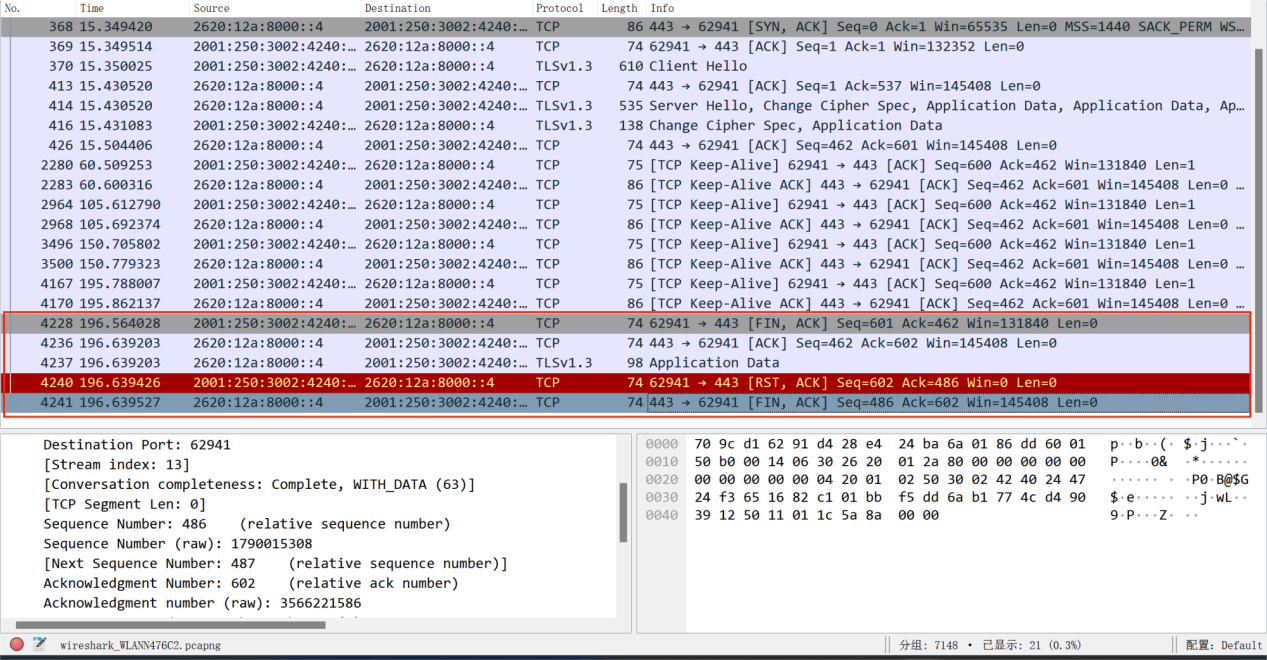
**在TCP连接建立后，客户端向服务器发出的TLS问候消息"ClientHello" ，包含了与建立安全连接相关的信息和参数，表示两者可以进行数据传输。**

**2.TCP连接建立后 两者开始数据传输**



**从上图可见，中间的数据传输采用的时TCP的持续连接**

1. **TCP断开连接 4次挥手**



**在浏览器关闭网页后 客户机向服务端发起了[FIN ACK]中断连接的请求**

**服务端接到客户端发来的中断连接的请求，发送ACK回复，同时自己进入了半关闭状态**

**可以看到还进行了一次服务端向客户端的应用数据传输**

**接着服务器端发送FIN给客户机，告诉客户机它不再有数据要发送。**

**问题:最后一次挥手 即最后一步客户端向服务机端的ACK回复未被捕获到。**

## 实验6.2.1

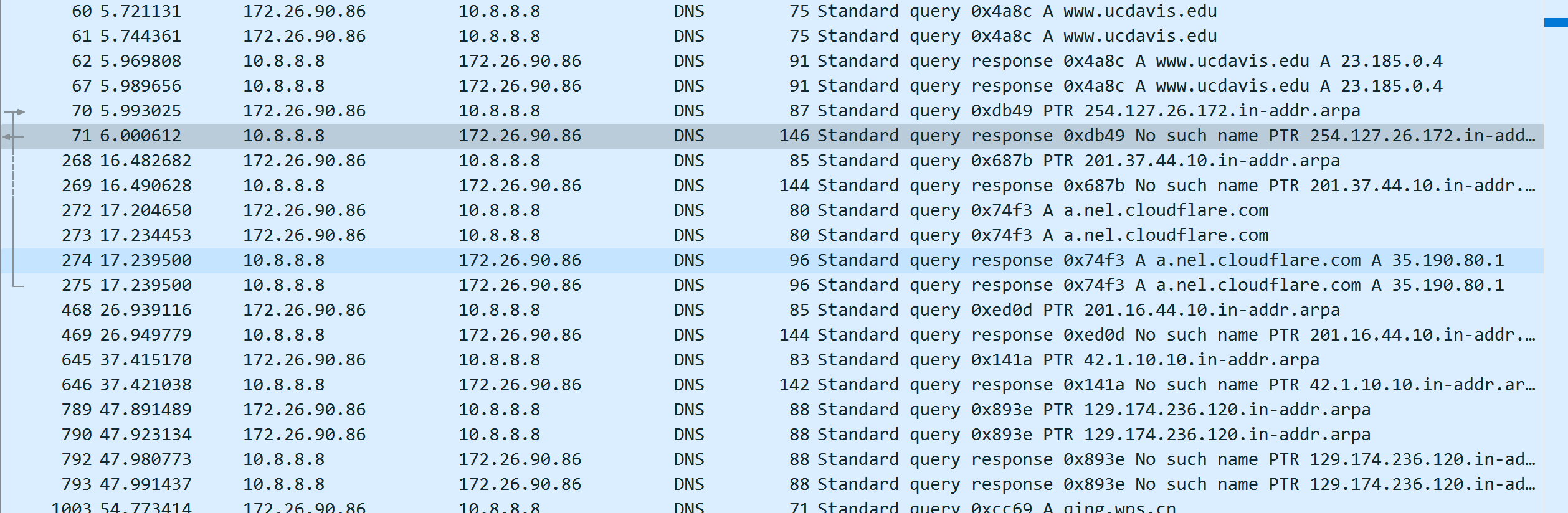
## 

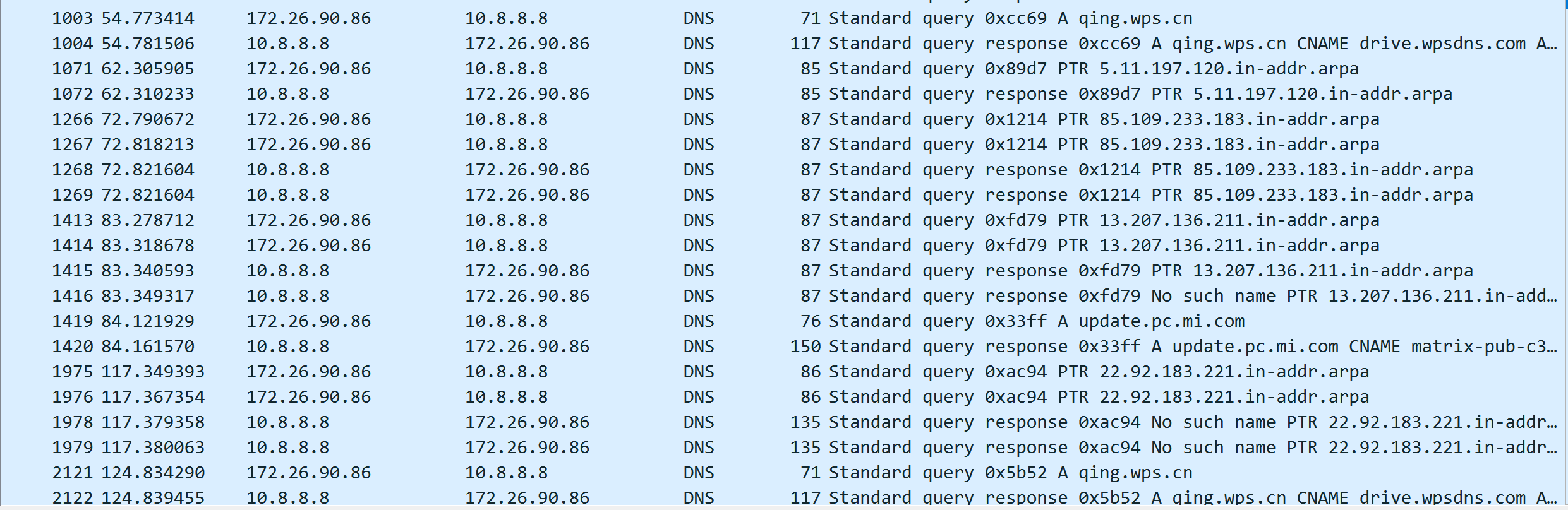
**先执行一次tracert指令，获得网站的IP地址 23.185.0.4**

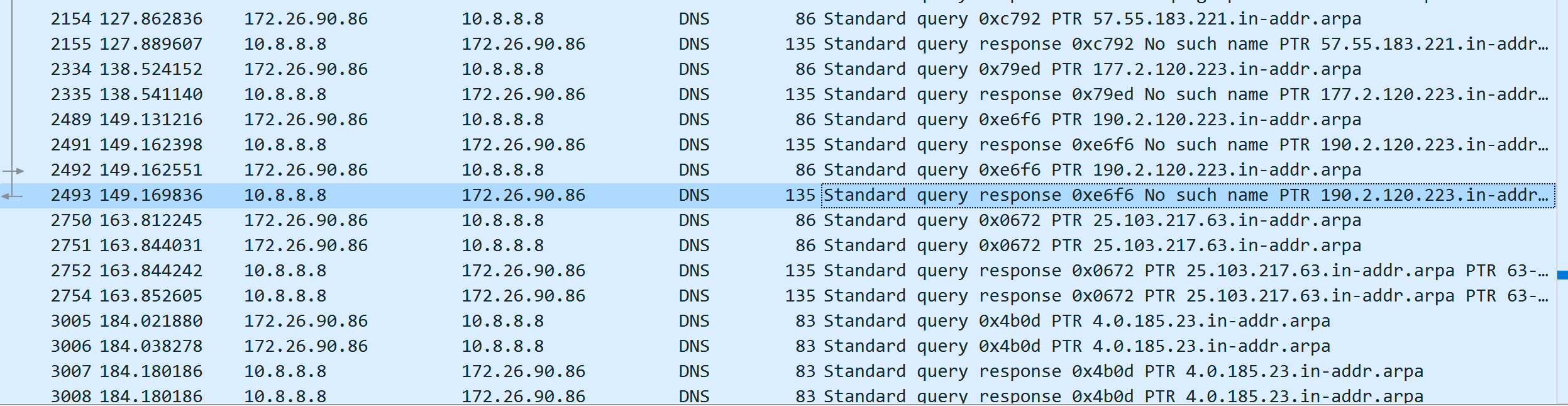
**再执行tracert 并启动wireshark抓包**

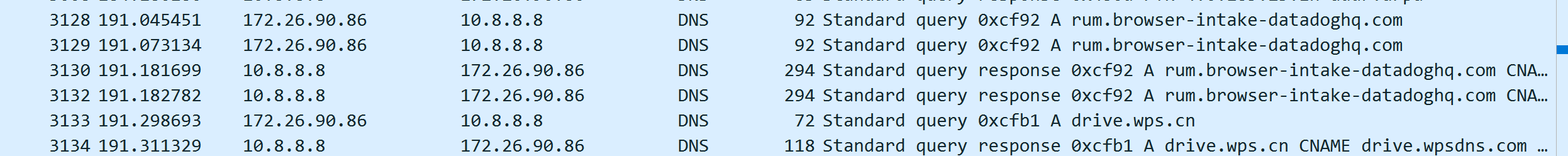
**通过查询资料得知和UDP有关的报文为DNS和ICMP**

**捕获到的DNS报文:**

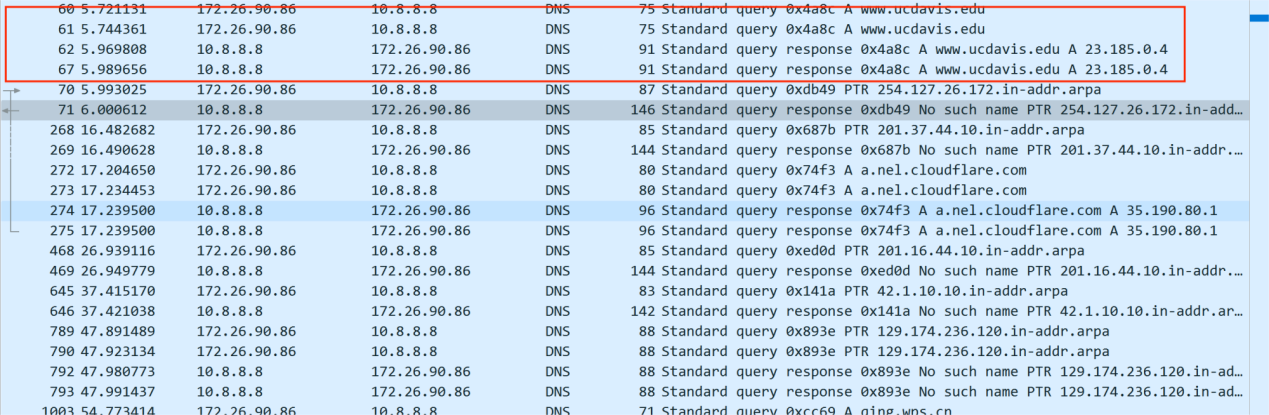




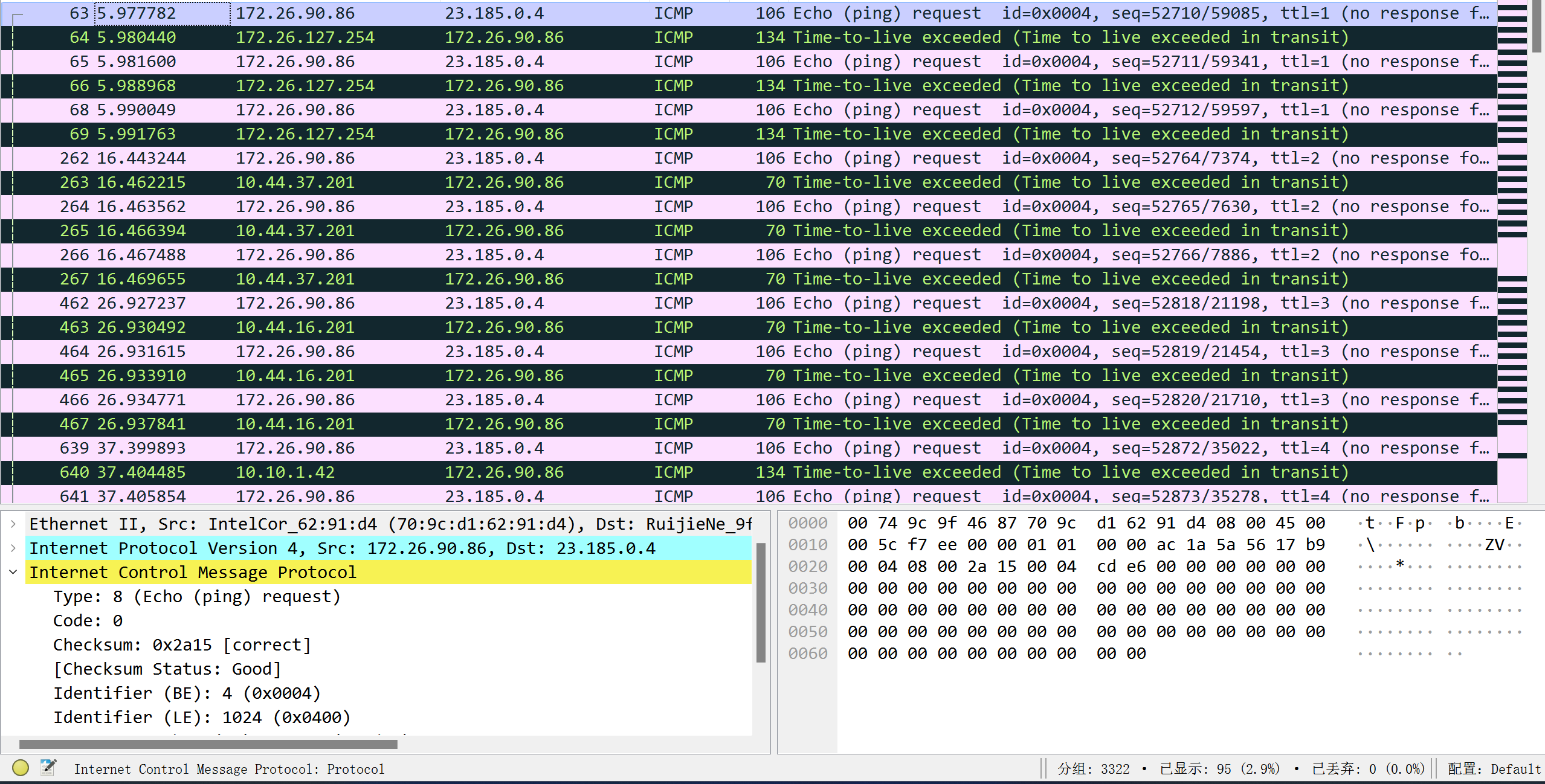




可以看到其中有关于查询目的网址的DNS报文



**捕获到的icmp报文:**



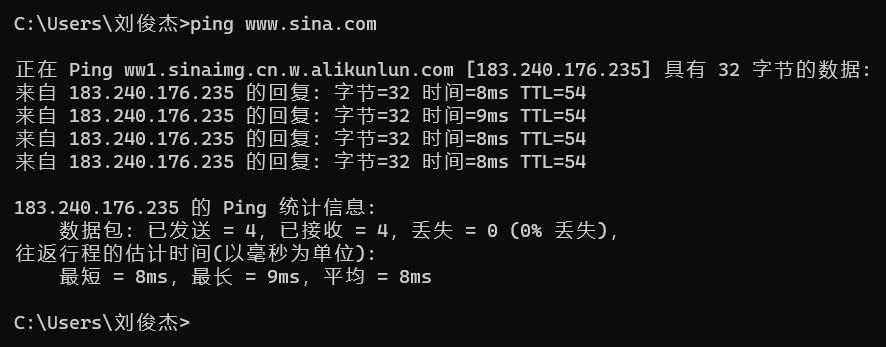
选取一部分分析:

该报文的作用是使用 ICMP 报文来跟踪数据包在网络中的路径，并显示每个节点的响应时间。

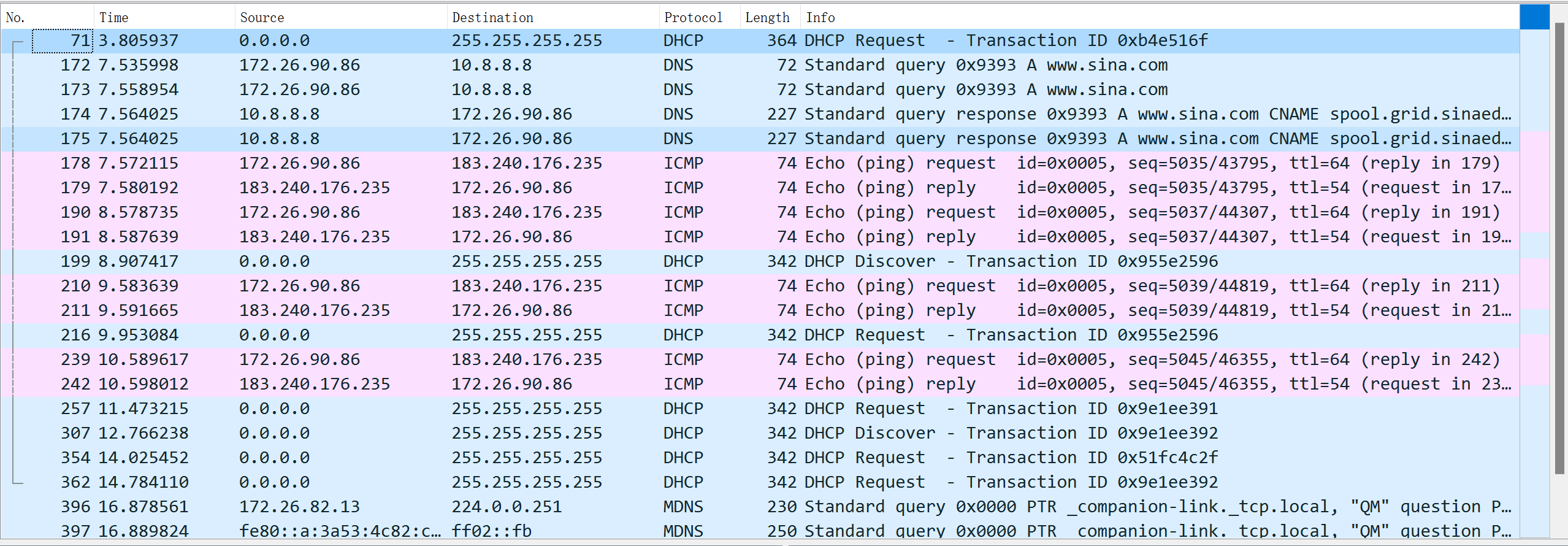
此外，还可以看到报文的Time to Live为1，说明该报文最多可以经过1个路由器。

如果TTL在某个节点减为0，该节点将丢弃数据包并发送一个"Time Exceeded"（时间超限）的ICMP消息给源主机，以通知它数据包已经被丢弃。

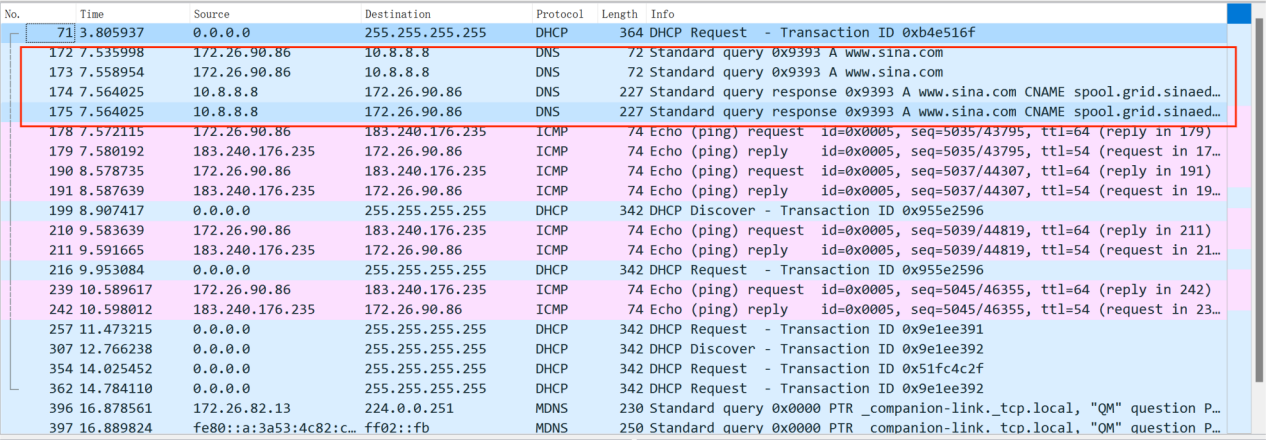
## 实验6.2.2



捕获到的UDP信报:



首先可以看到查询www.sina.com的IP的DNS信报:



其次是测试四次连通的ICMP信报：

