综合验证性实验：

实验一、网络命令的使用

课程名称：组网工程 开课实验室：6313

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 专业班级 | 软件1603 | 学号 | 201616040310 | 姓名 | 张勋 |
| 实验项目名称 | 实验一：网络命令的使用 | | | 实验日期 | 2019.4.1 |
| 成绩评定 |  | | | | |

第一部分：子网划分与连通性测试

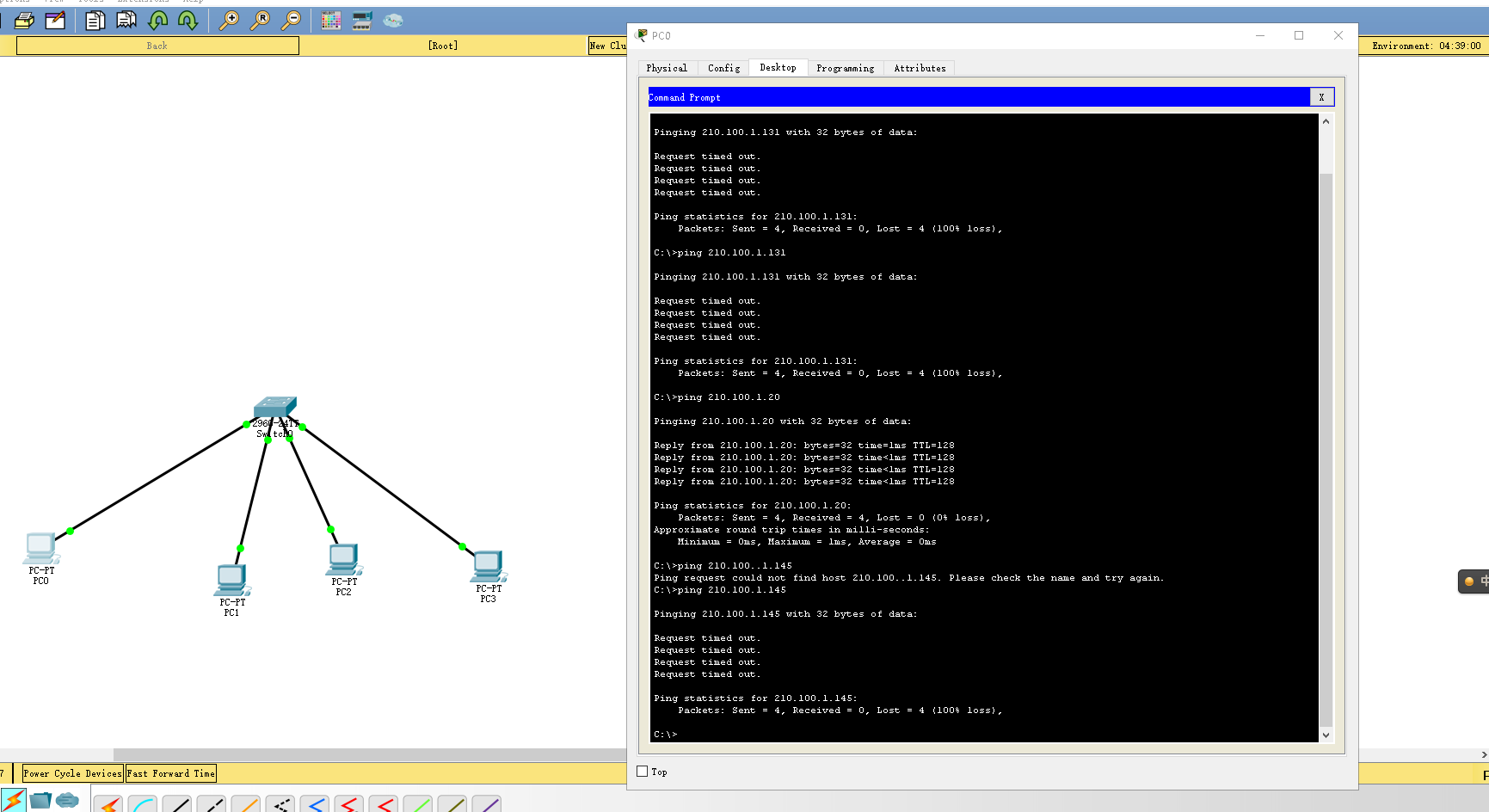
某单位一个局域网中，使用交换机连接了4台计算机，它们的网络参数（IP地址/子网掩码）配置如图所示，请完成如下问题：

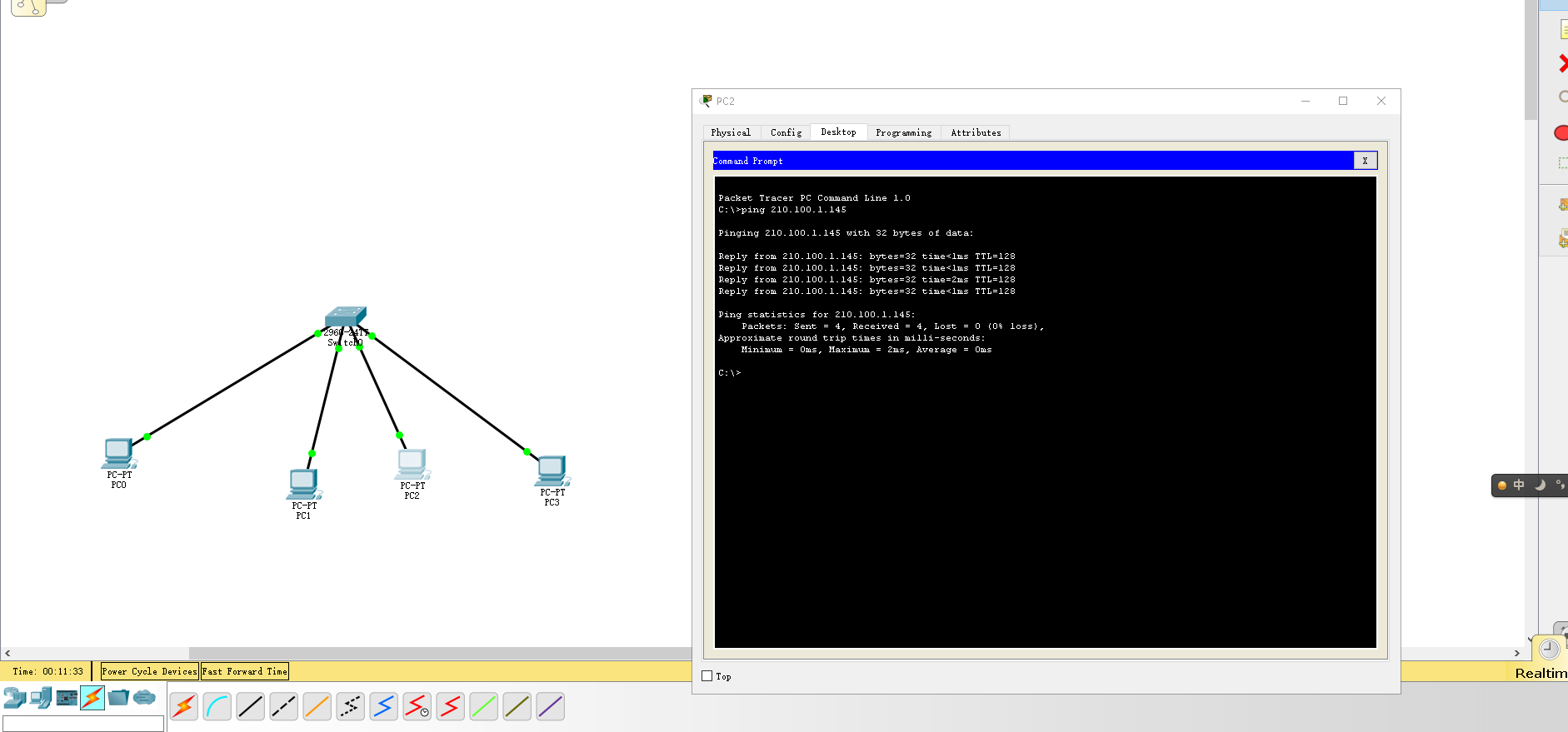
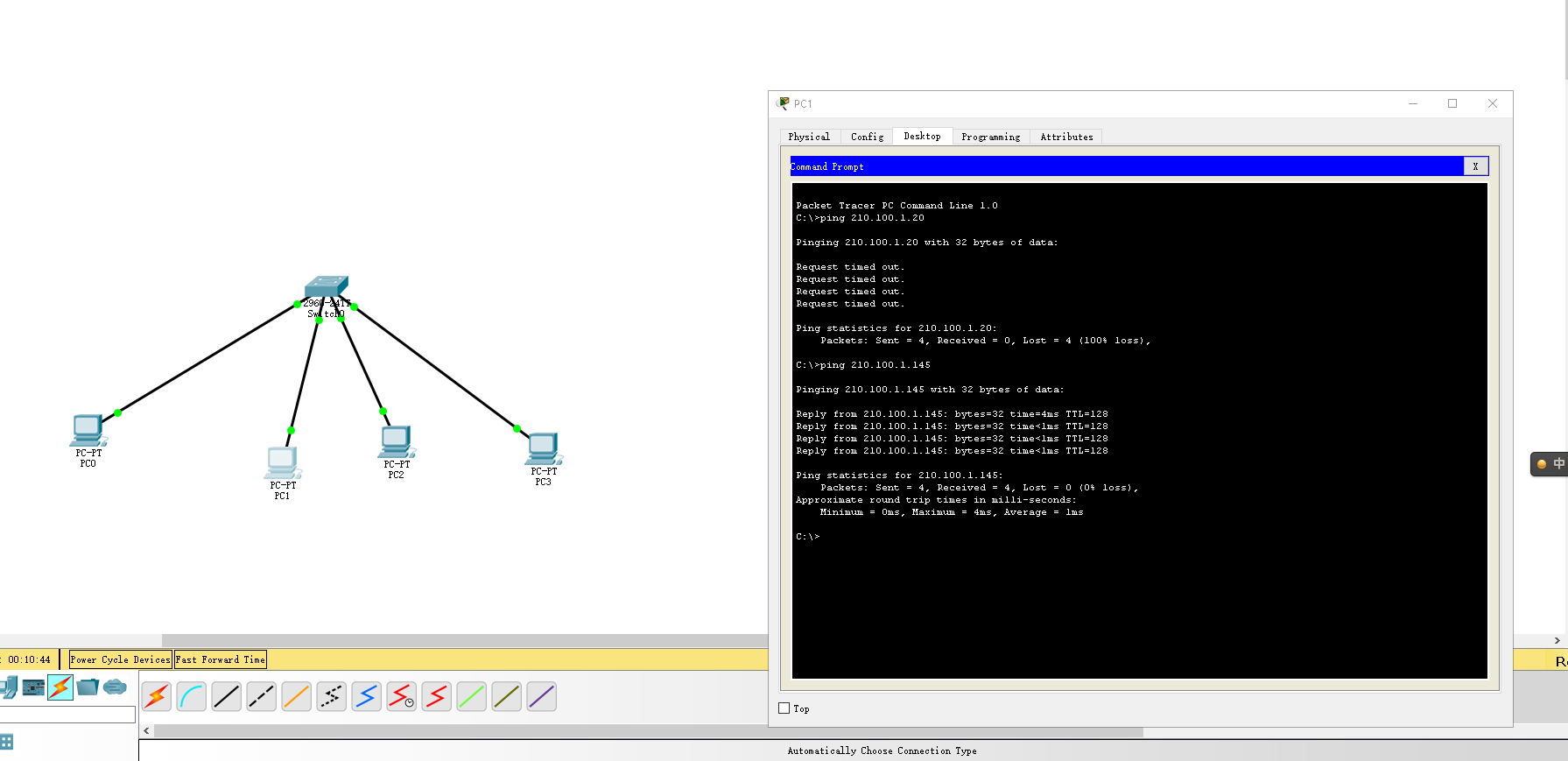
（1）对四个IP地址进行分析，哪些地址位于同一个子网，哪些地址网络地址相同，但是子网掩码不同。

表1-1 主机ip地址分析

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 主机号 | Ip地址 | 子网掩码 | 网络地址 | 网段 |
| A | 210.100.1.10 | 255.255.255.128 | 210.100.1.0 | 210.100.1.0-210.100.1.255 |
| B | 210.100.1.131 | 255.255.255.128 | 210.100.1.128 | 210.100.1.128-210.100.1.255 |
| C | 210.100.1.20 | 255.255.255.0 | 210.100.1.0 | 210.100.1.0-210.100.1.255 |
| D | 210.100.1.145 | 255.255.255.0 | 210.100.1.0 | 210.100.1.0-210.100.1.255 |

（2）主机之间互相ping，列出结果，并认真分析原因。

答：

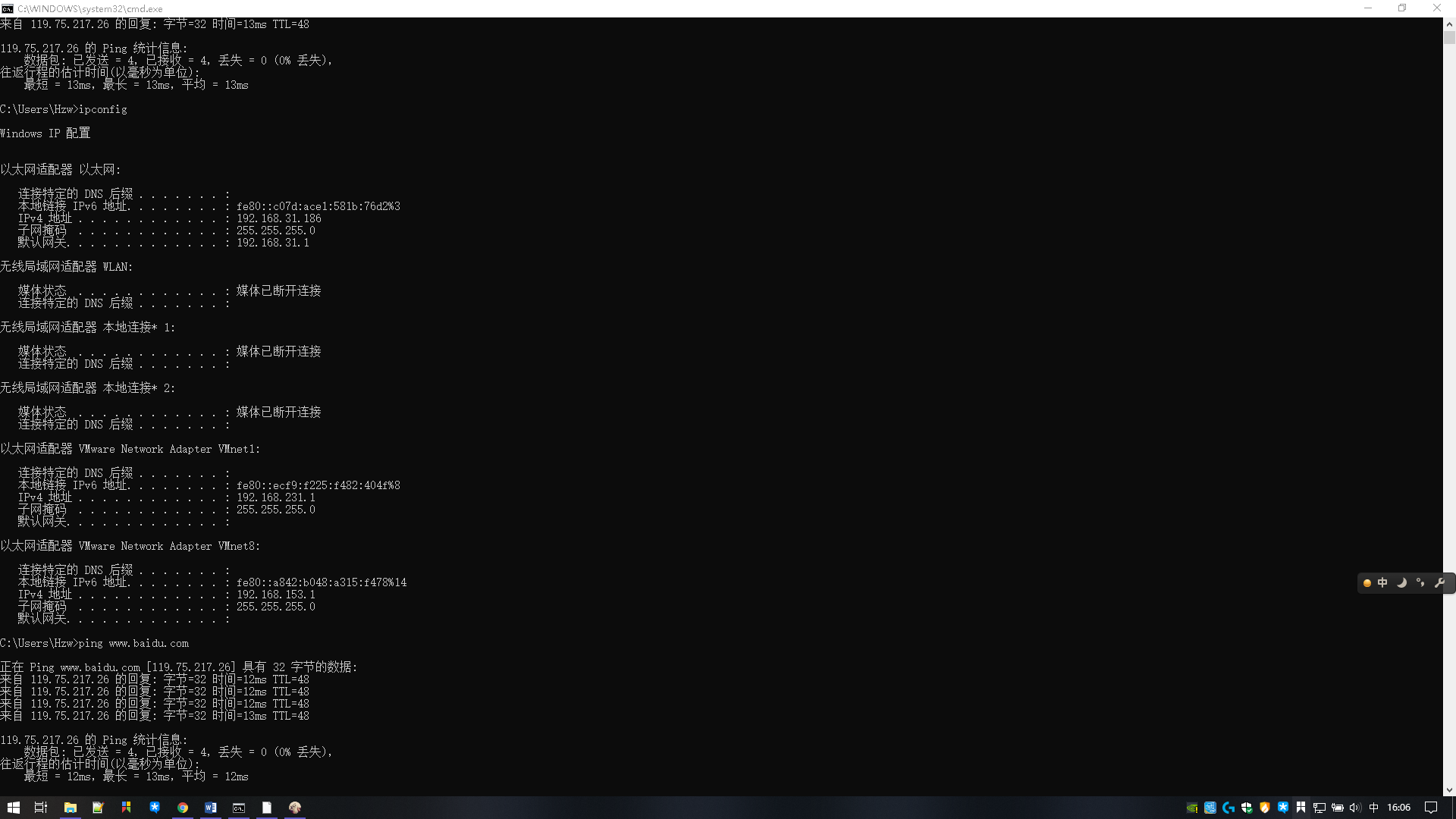


第二部分：深刻理解运输层协议

运输层是负责数据通信的最高层，充分理解和验证运输层协议有助于对数据通信、数据传输的深刻理解，以及对其下层协议的理解。请用Wireshark软件完成如下要求：

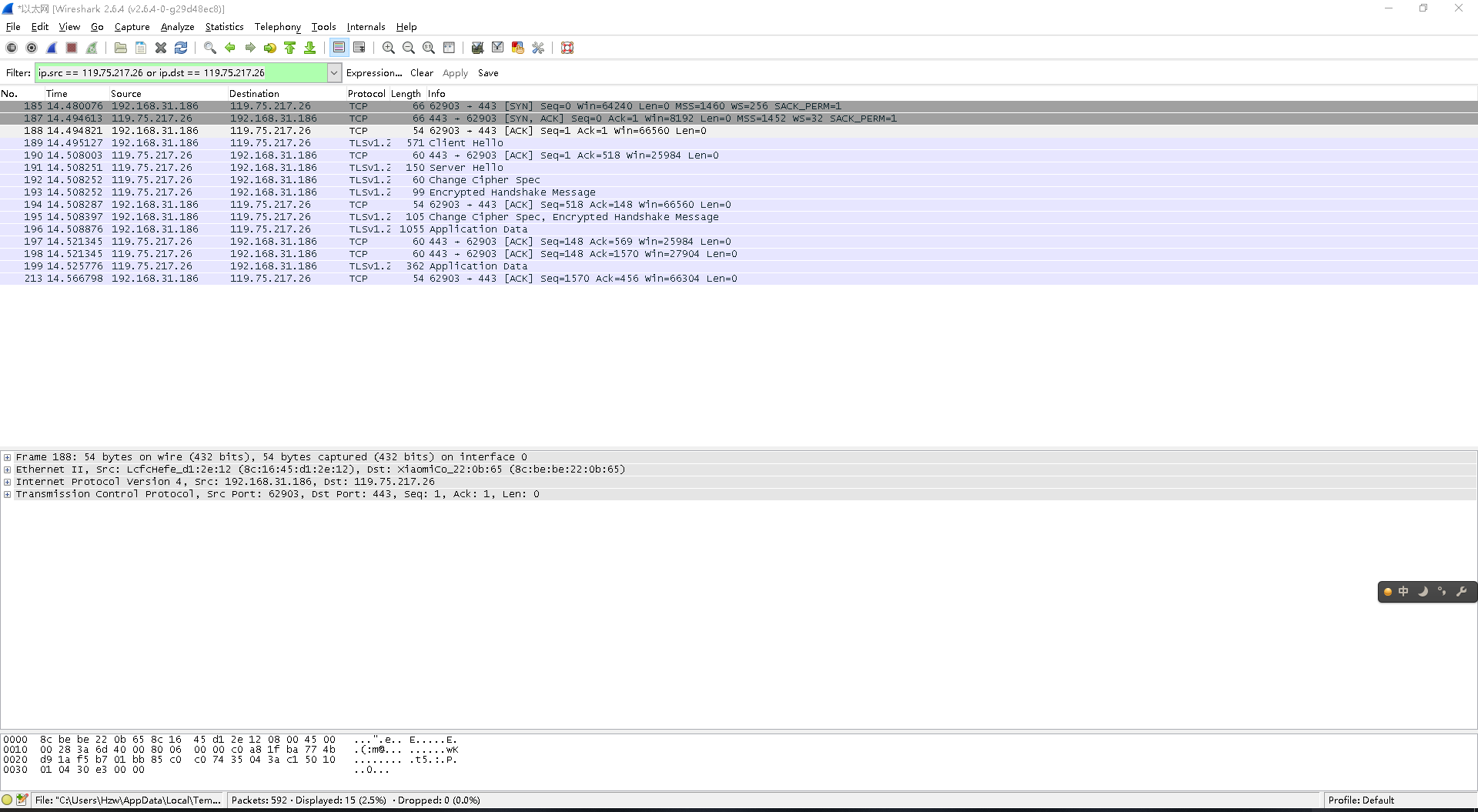
1. TCP三次握手全过程。三次交互。首部关键字段理解：序号、确认号、同步/确认开关量、接收窗口等。（知识点：TCP报文首部、TCP连接管理）

TCP三次握手过程：打开Wireshark，访问百度，然后查询本机和百度的IP地址



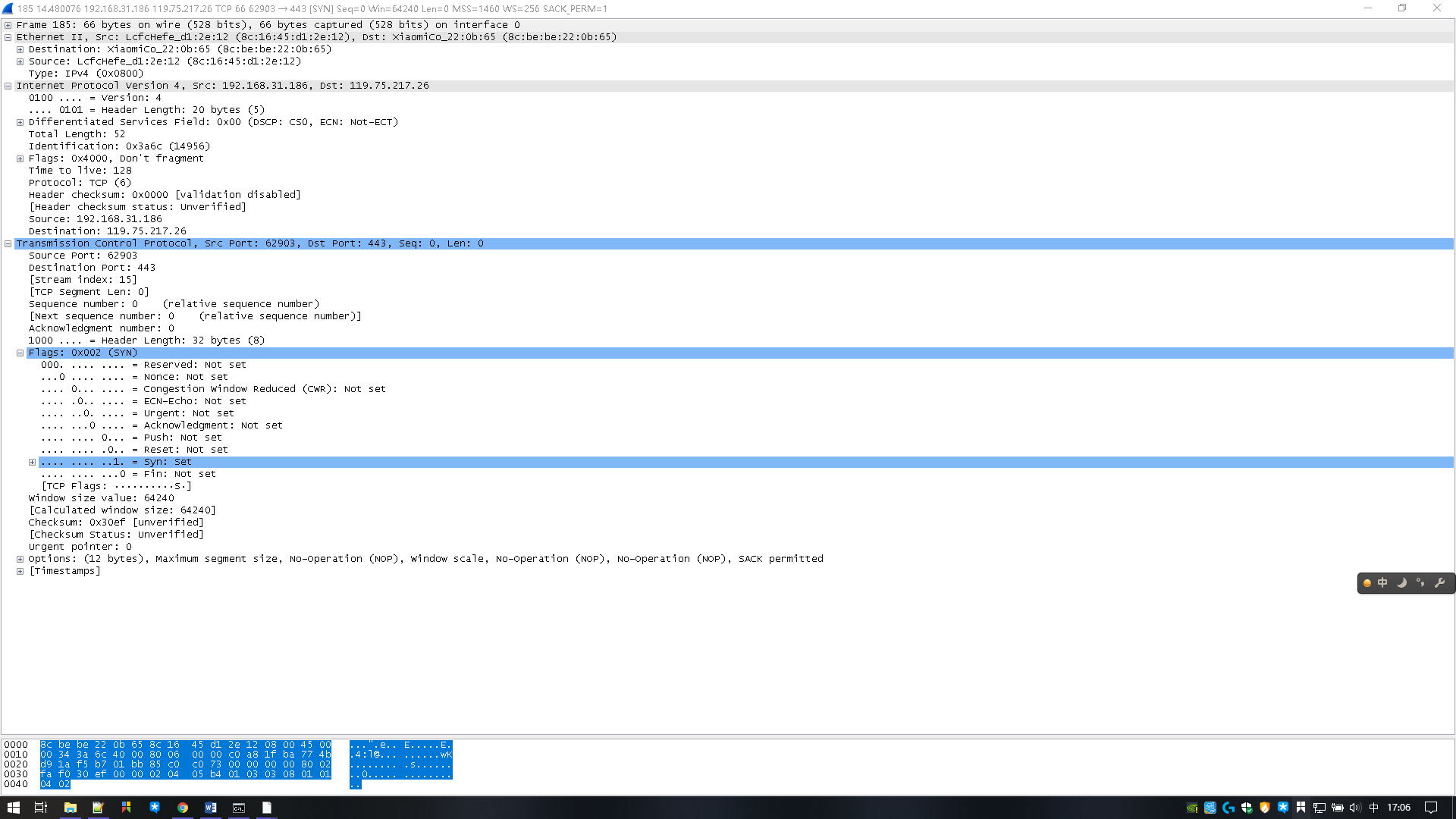
由于捕获数据过多，必须进行筛选

筛选表达式：ip.src == 119.75.217.26 or ip.dst == 119.75.217.26



图中可以看到。Wireshark截获了三次握手的三个数据报

**源主机向目的主机发送连接请求：**



报头：

源端口号：62903

目的端口号：http(443)

序列号：0（源主机选择0作为起始序号）

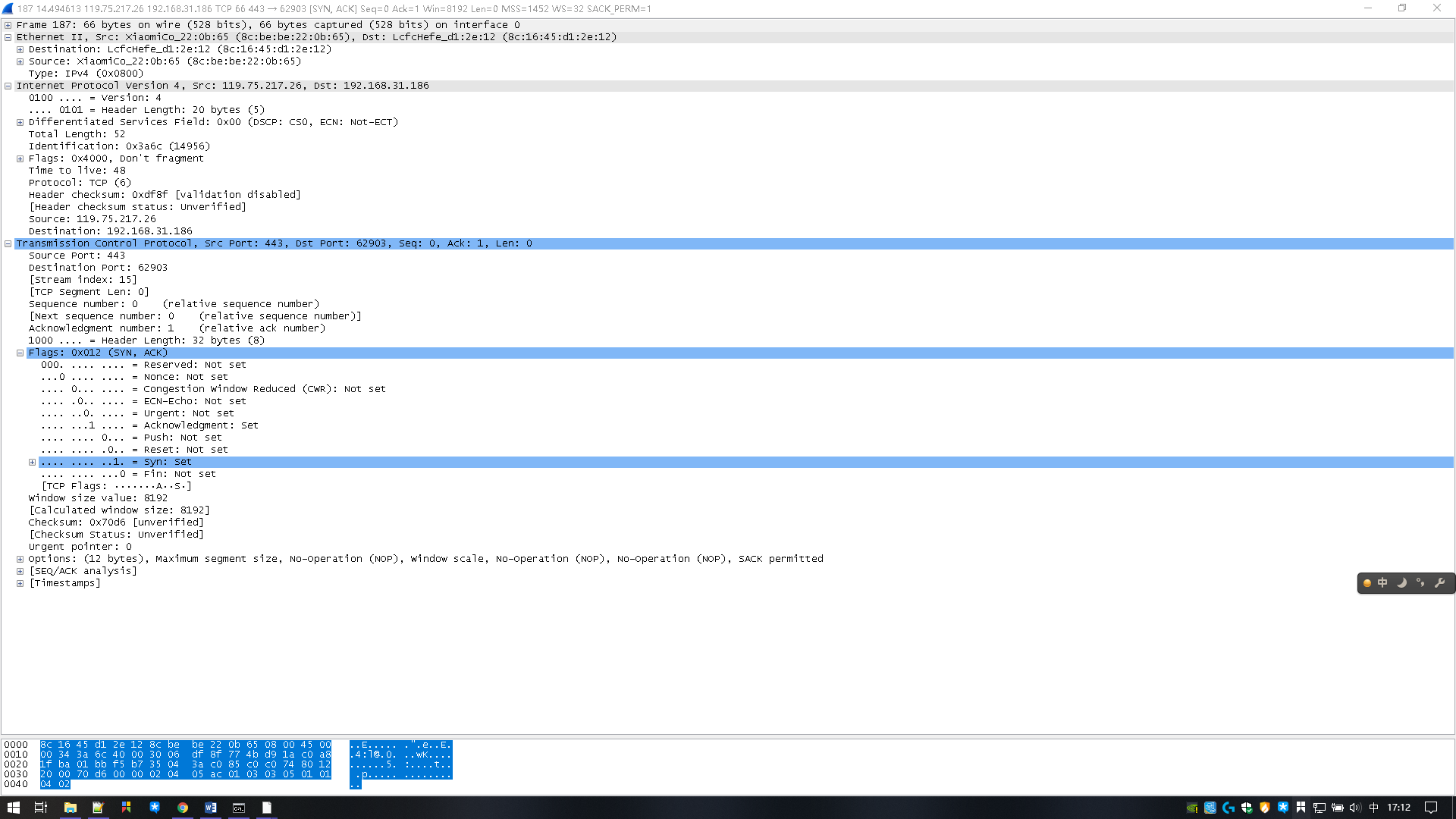
报头长度：32字节

标志位：仅SYN设为1，请求建立连接，ACK：not set

窗口大小：64240字节

选项字段：12字节

**目的主机返回确认信号：**



报头：

源端口号：http(443)

目的端口号：62903

序列号：0（目的主机选择0作为起始序号）

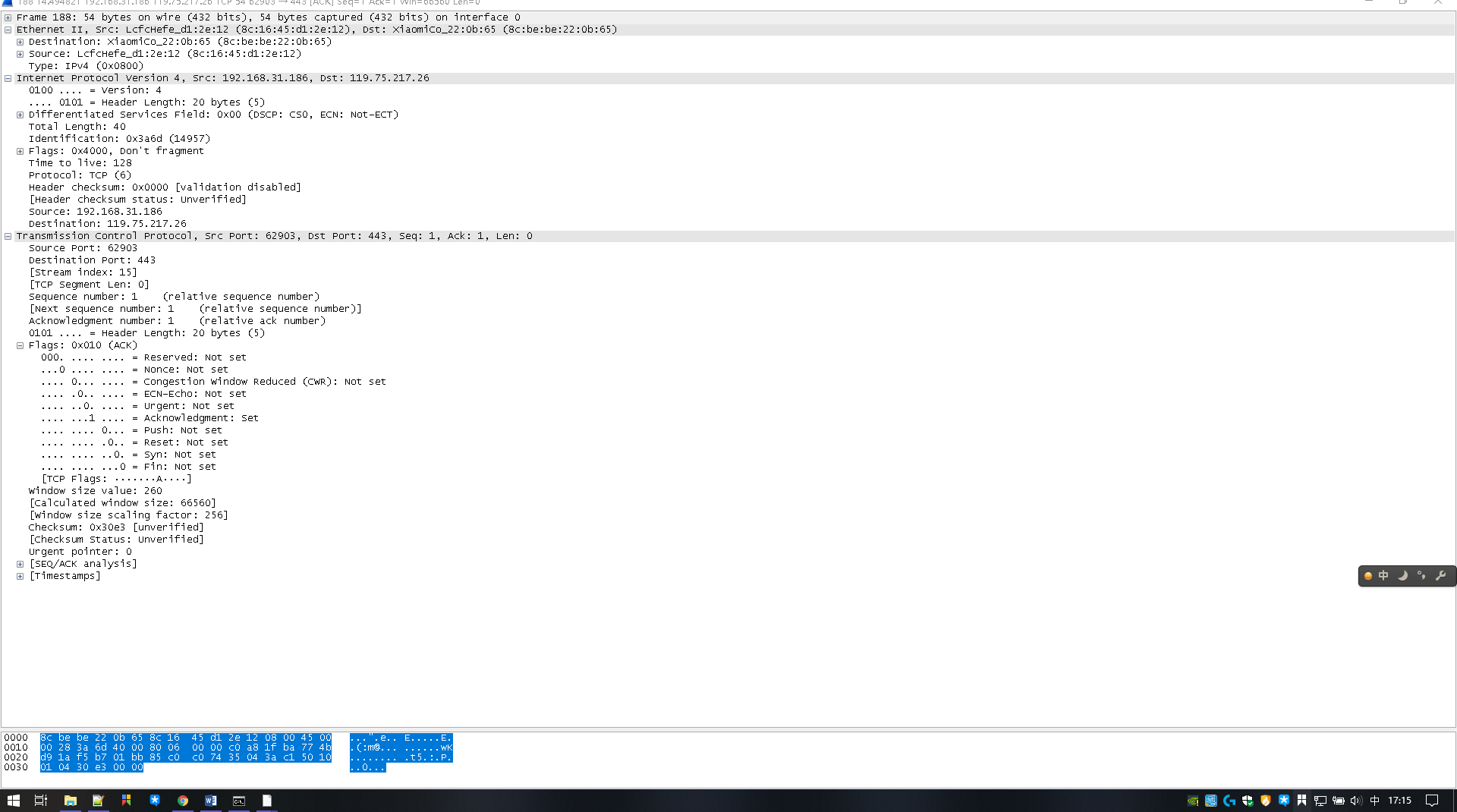
报头长度：32字节

标志位：SYN设为1，ACK设为1，确认允许建立连接

窗口大小：8192字节

选项字段：12字节

**源主机再次返回确认信息，并可以携带数据**



报头：

源端口号：62903

目的端口号：http(443)

序列号：1（发送的报文段编号）

报头长度：20字节

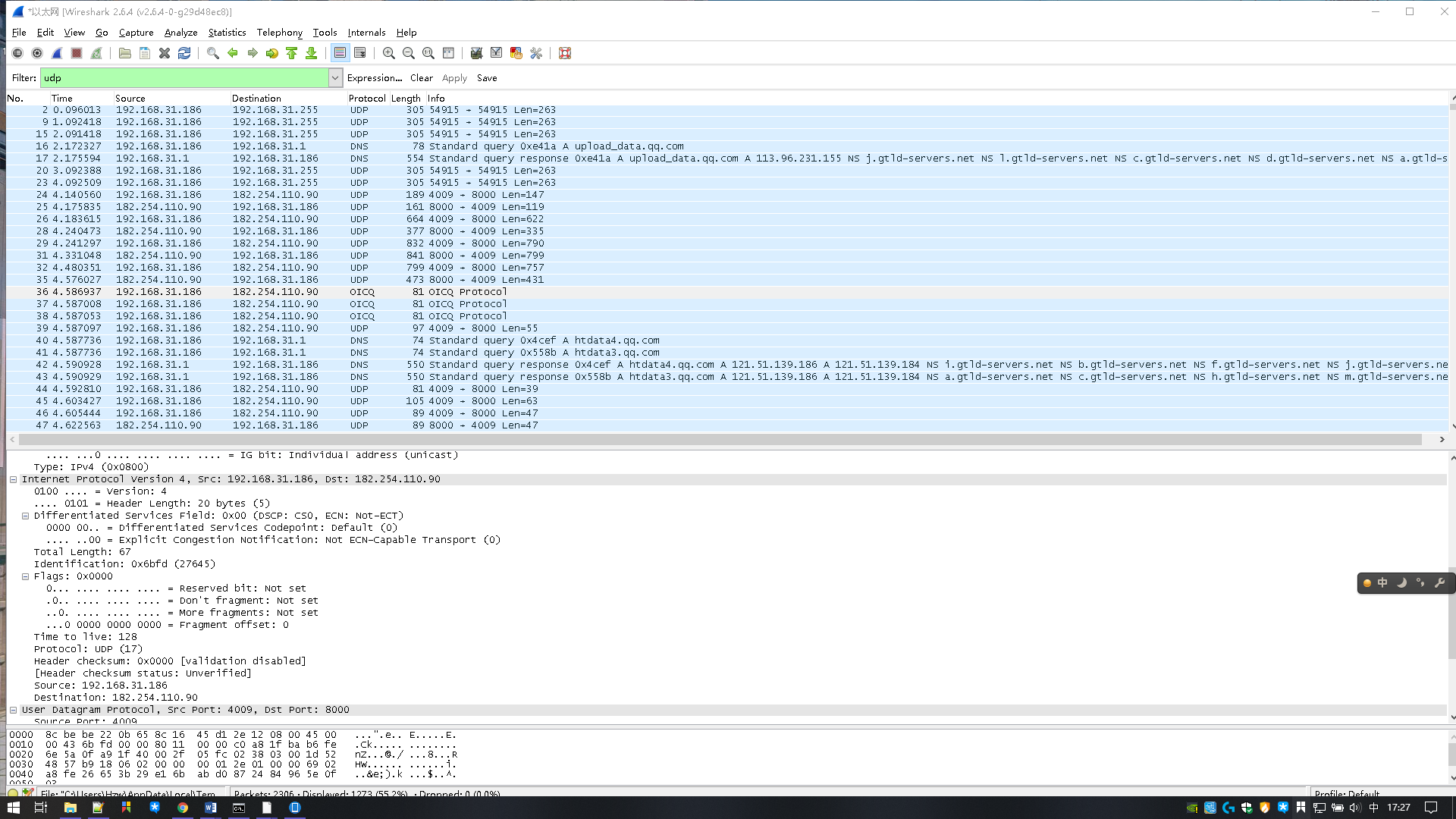
标志位：SYN=0，ACK=1

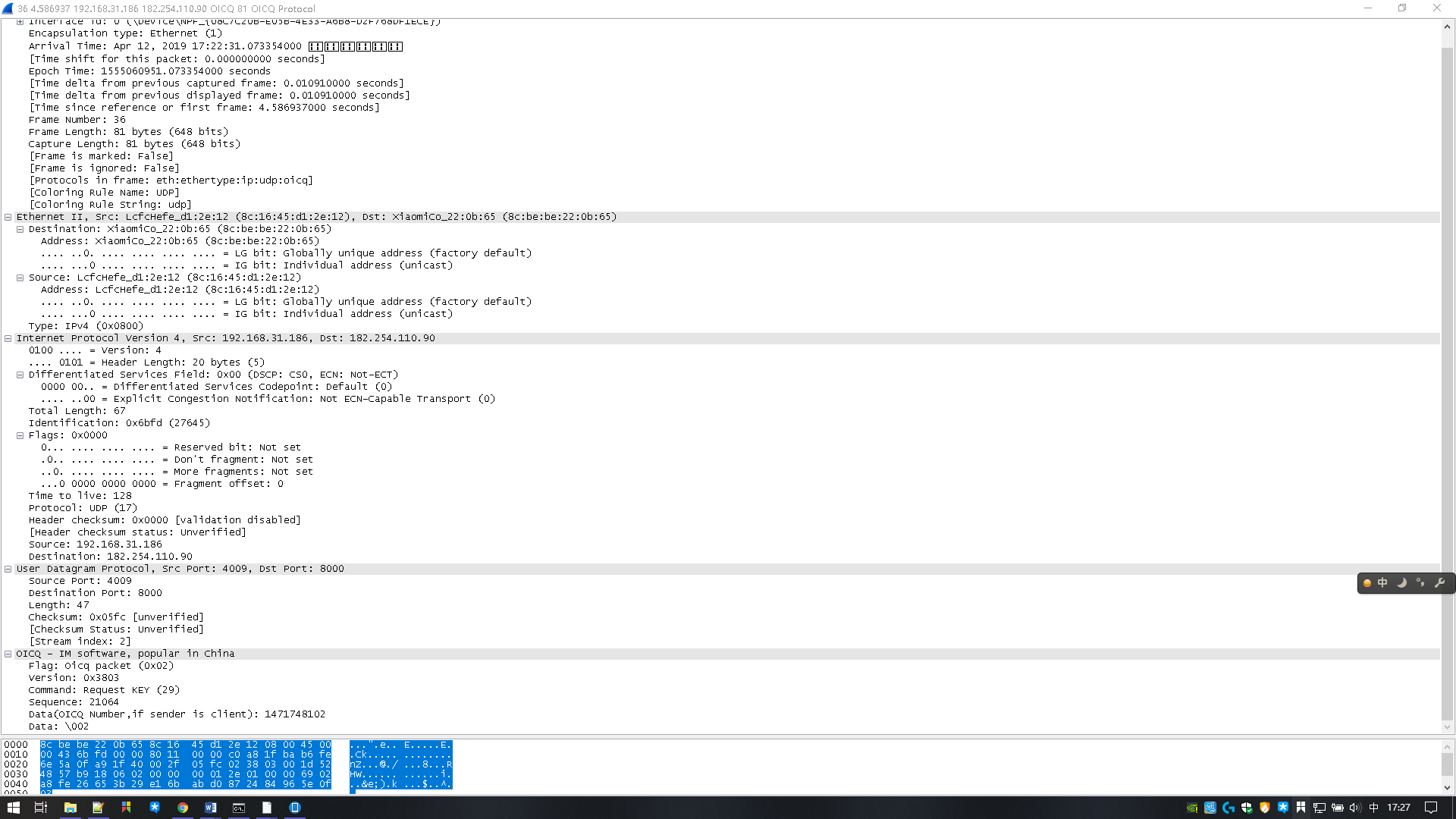
窗口大小：260字节

1. UDP报文传输，首部内容分析，端口等字段。（知识点：UDP协议）

UDP作为一种面向无连接服务的运输协议，报文格式很简洁，由抓包信息可知，UDP协议大多被DNS协议应用。

UDP协议分析：这里利用wireshark抓捕QQ登陆时候的UDP数据包，分析其中的协议





**UDP协议部分：**

源端口号：4009

目的端口号：8000

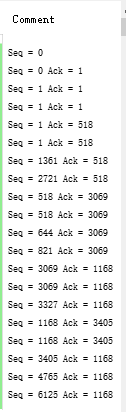
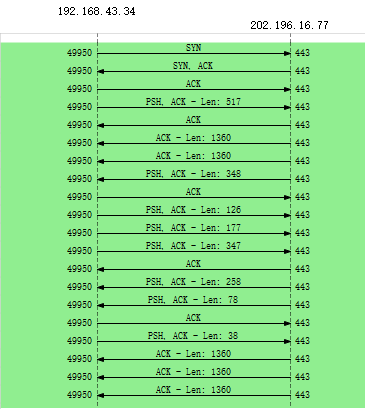
UDP首部和数据的长度：47

16进制校验和：0x05fc

UDP作为一种面向无连接服务的运输协议，报文格式很简洁，由抓包信息可知，UDP协议大多被DNS协议应用。

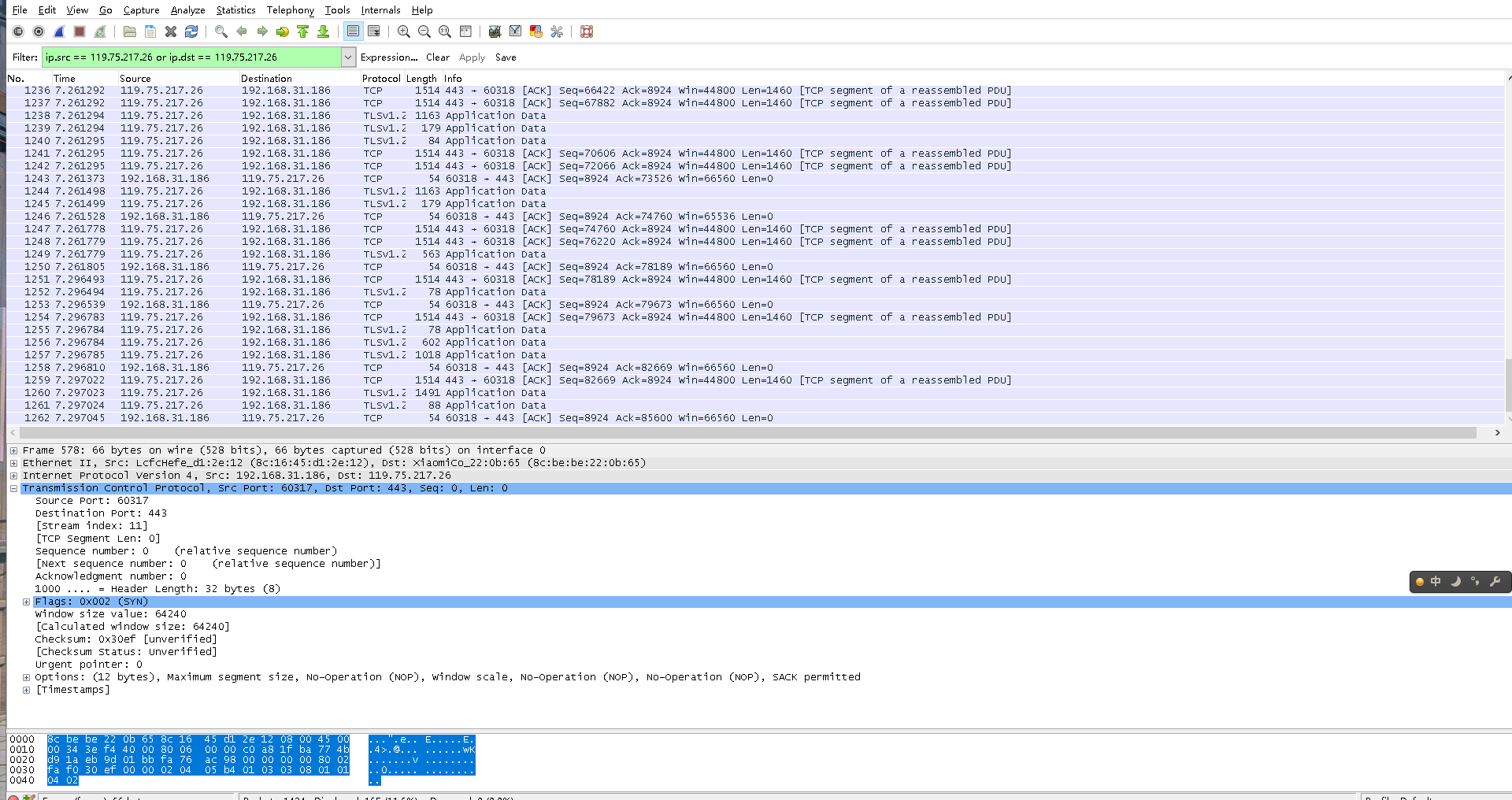
1. TCP停等协议，发送-确认交互，尤其观测是累计确认还是单一确认。（知识点：TCP可靠传输-停等协议）

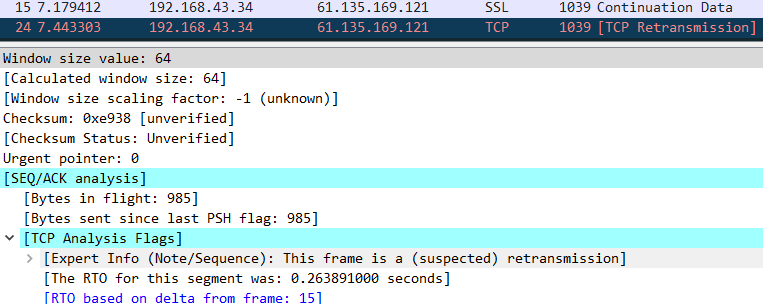
停止等待协议是tcp保证传输可靠的重要途径,”停止等待”就是指发送完一个分组就停止发送,等待对方的确认,只有对方确认过,才发送下一个分组。



1. TCP超时重传，能否设计出发送后超时重传，观察计时时间，重传报文段与第一次发送的报文段时间差。（知识点：TCP可靠传输-停等协议）

在发送一个数据之后，就开启一个定时器，若是在这个时间内没有收到发送数据的ACK确认报文，则对该报文进行重传，在达到一定次数还没有成功时放弃并发送一个复位信号。

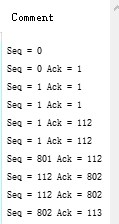
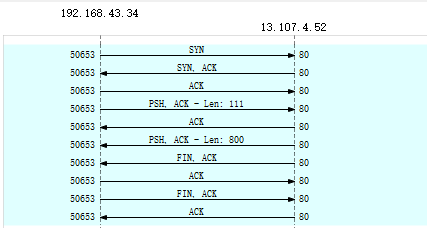




可看出重传时间差RTO：0.263891

1. TCP连接释放，能否捕获完成双向释放请求和确认，注意观察主机中协议端口状态。（知识点：TCP连接管理）

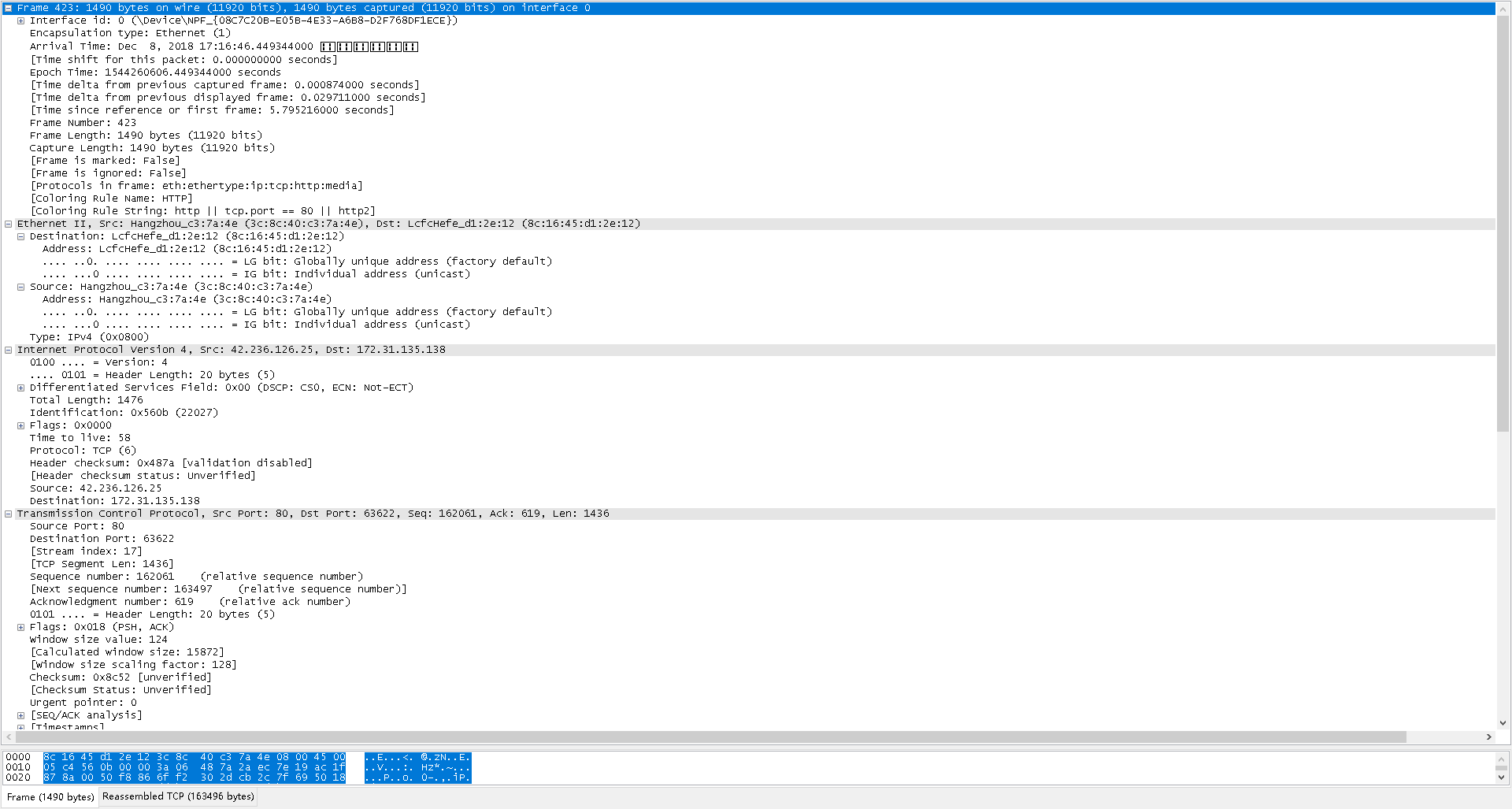
TCP协议是面向连接的协议，要传送数据，需要进行建立连接、传送数据、释放连接三个阶段。其中建立连接需要三次握手，而释放连接需要四次握手

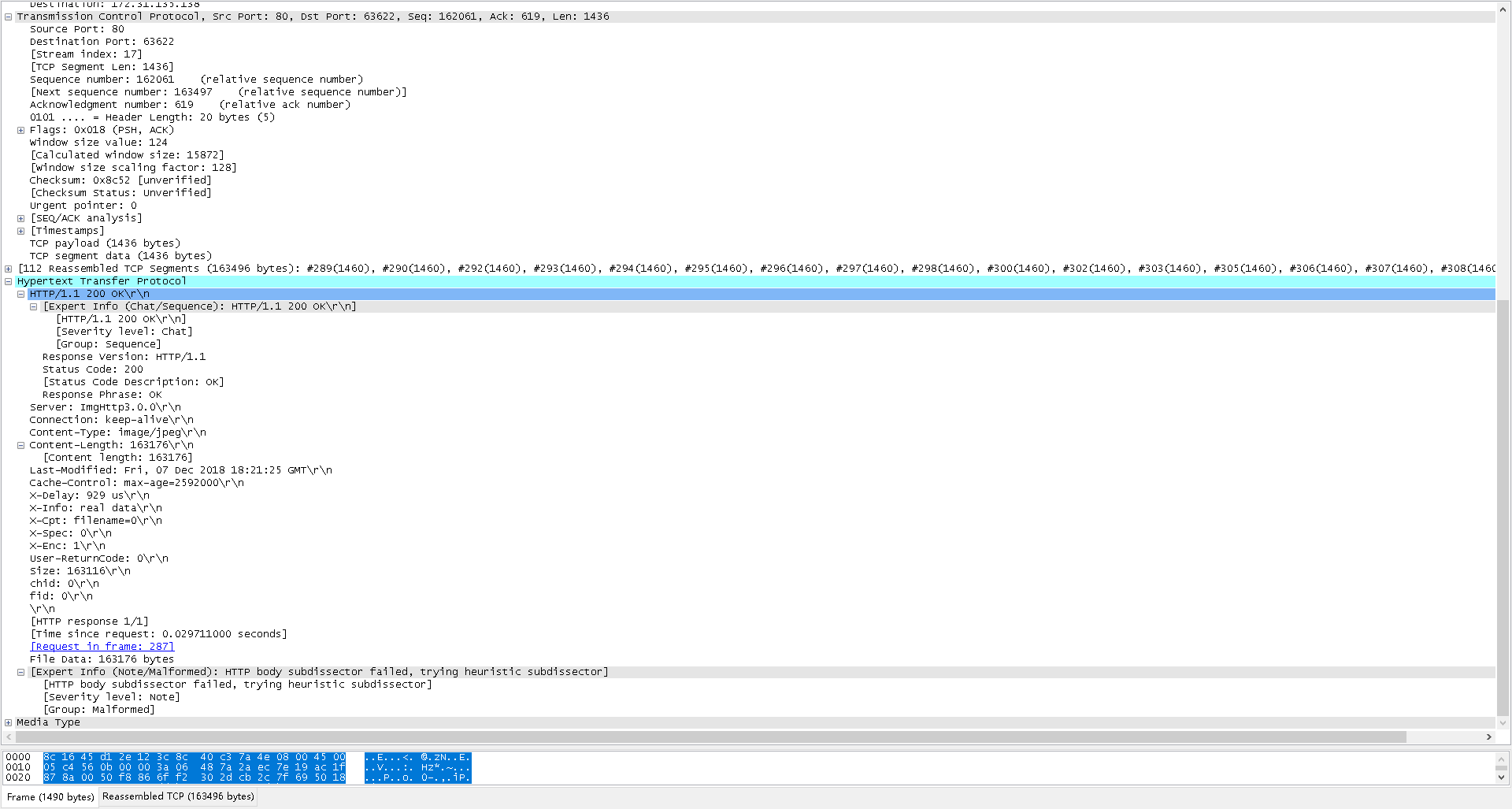


1. 不同高层协议在运输层的反映，如http、QQ、FTP等应用。（知识点：TCP、UDP协议及应用层协议）

捕获HTTP数据包分析：

|  |  |  |  |
| --- | --- | --- | --- |
| 源端口号 | 80 | 目的端口号 | 63622 |
| 源IP地址 | 42.236.126.25 | 目的IP地址 | 172.31.135.138 |
| 源MAC地址 | 3c:8c:40:c3:7a:4e | 目的MAC地址 | 8c:16:45:d1:2e:12 |
| 序号 | 162061 | 确认号 | 619 |
| 长度 | 1476 | 应用层协议 | HTTP |





捕获FTP数据包分析：

|  |  |  |  |
| --- | --- | --- | --- |
| 源端口号 | 62682 | 目的端口号 | 21 |
| 源IP地址 | 172.31.129.221 | 目的IP地址 | 172.18.53.220 |
| 源MAC地址 | 98:e7:f4:56:8a:f7 | 目的MAC地址 | 3c:8c:40:c3:7a:4e |
| 序号 | 1 | 确认号 | 9 |
| 长度 | 66 | 应用层协议 | FTP |