**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 Internet应用与应用层协议分析 指导教师 潘冰

实验项目编号 03 实验项目类型 实验地点 B402

学生姓名 张强 学号 2019053448

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 10 月 5上午～ 10月 17 日上午 温度 ℃湿度

## （一）实验目的

1. 理解WWW、DNS服务、FTP服务、SMTP的作用和原理；
2. 学会使用wireshark分析HTTP、FTP、SMTP和DNS协议的工作过程，加深对协议格式和工作原理的理解

## （二）实验内容和要求

1. 通过域名访问WWW、FTP服务器，分析DNS、WWW、FTP工作过程，并使用WireShark分析相关协议格式；
2. 在客户端访问SMTP服务器，使用wireshark分析SMTP、POP3协议的工作过程。（可以在客户端安装outlook或使用QQ邮件服务器或自己编程）

**说明：**

1、本实验重点放在协议分析上，包括协议格式和工作过程。

2、在网上查询并理解FTP、SMTP和POP协议细节；查询并理解HTTP请求和响应的首部信息（不同的请求响应，首部信息不同）。

3、所有需要建立的服务器不是必须的，建议有兴趣的同学花些时间建立服务器，能帮助更深刻地理解相关原理。

## （三）主要仪器设备

**仪器：**局部网环境，计算机若干台

**实验环境：wireshark&cmd**

## （四）源程序

## 实验步骤与调试

## 一、HTTP协议分析

访问任意web站点，用wireshark分析HTTP协议的工作过程和HTTP协议格式。（协议首部含义需要查询了解）

**注意：**

如果访问的网站信息量太大，可以利用windows自带组件（如IIS）或自行下载WWW服务器软件，建立并配置WWW站点，主页内容需要包含姓名、学号等个人信息，然后访问自己建立的网站。

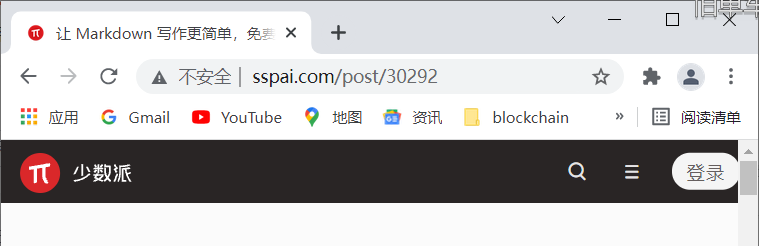
1．设置过滤条件

指定网络协议http

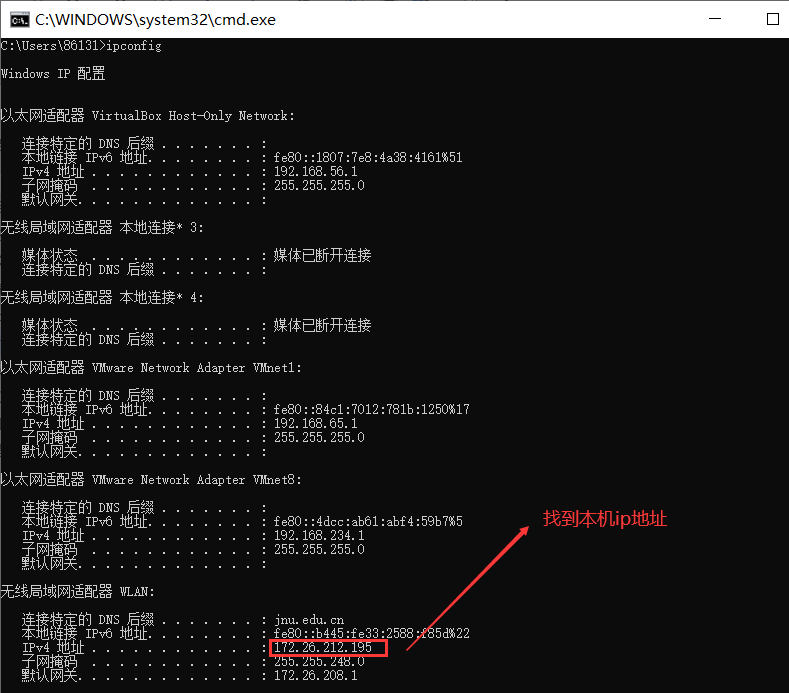


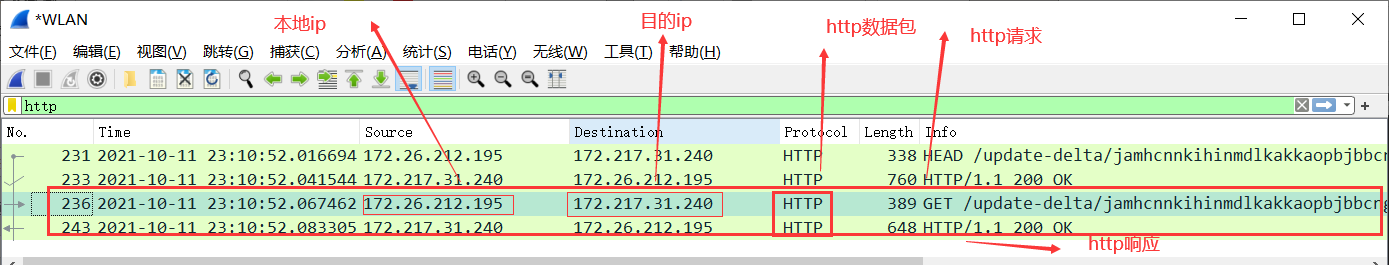
**2.打开浏览器输入网址**

在浏览器输入如下网站



**在抓获得包中得到两个数据包，分别是HTTP请求以及HTTP响应**

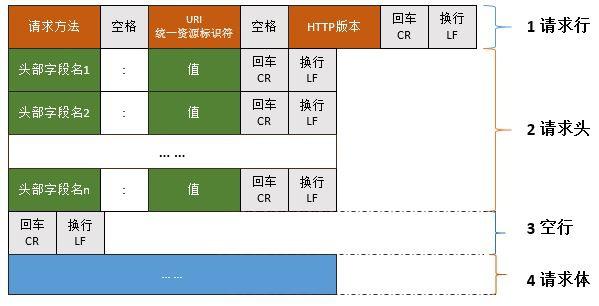




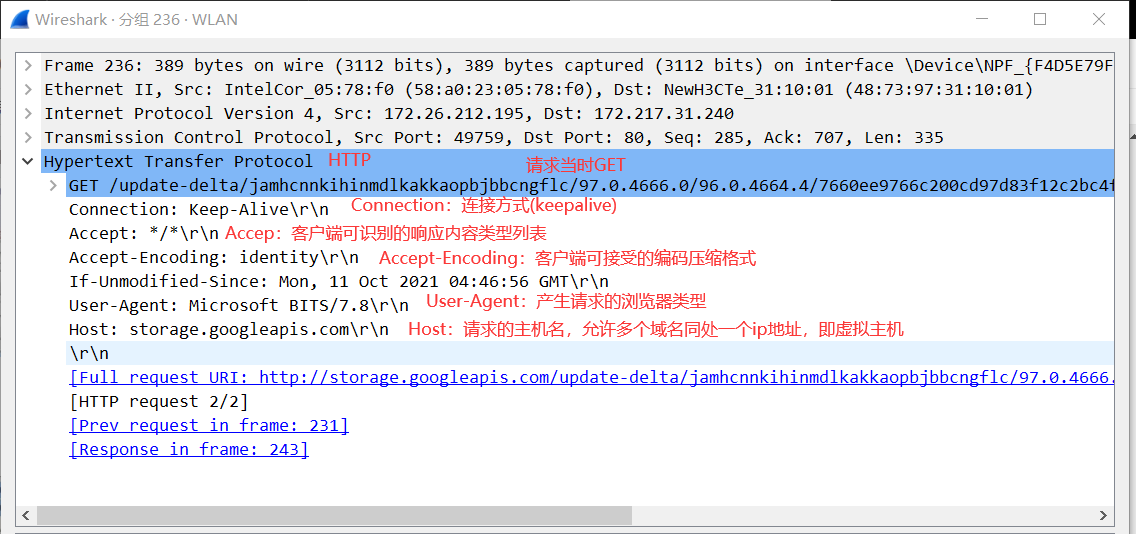
### HTTP数据包分析：



HTTP请求报文AND响应报文：



### HTTP请求报文分析：



Http协议包分析：

- HTTP请求消息头

1）Accept：call服务器，可以接收文件、网页和图片。

2）Accept-Charset：所接收的字符编码。

3）Accept-Encoding：可接收（）压缩后的数据。

4）Accept-Language：Browser支持中、英文。

5）Host：要找的主机是。

6）If-Modified-Since：告诉服务器我们的缓冲中有这个资源文件，该文件的时间是，，

7）Referer：告诉服务器，我来自哪里。

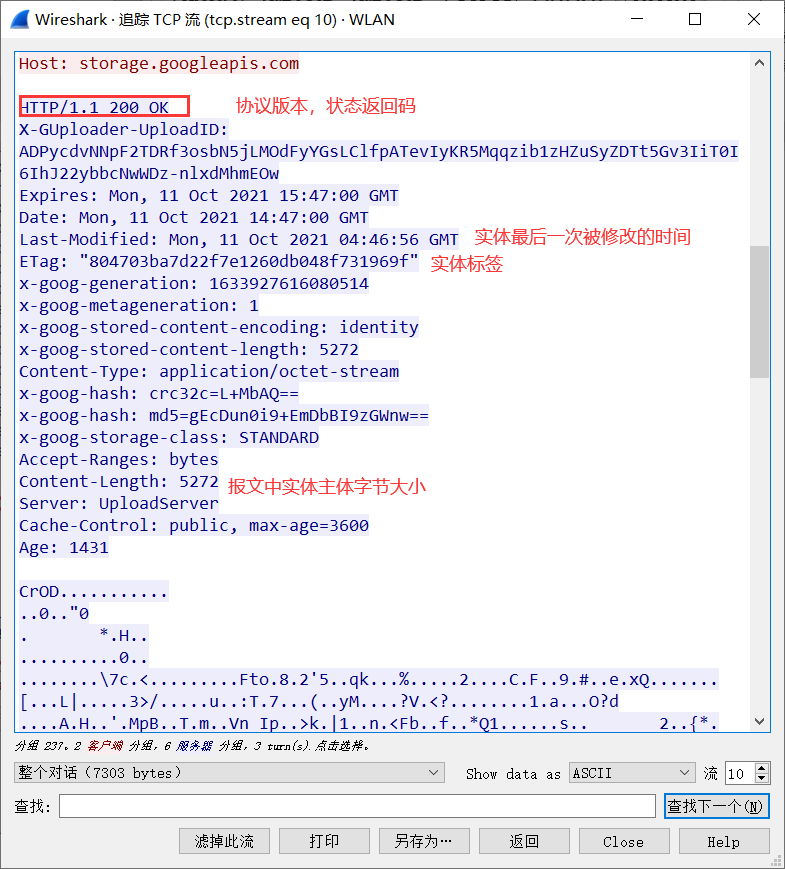
8）User-Agent：告诉服务器，Browser内核。

9）Cookie：

10）Connection：保持连续发完信息后，我不关闭连接。

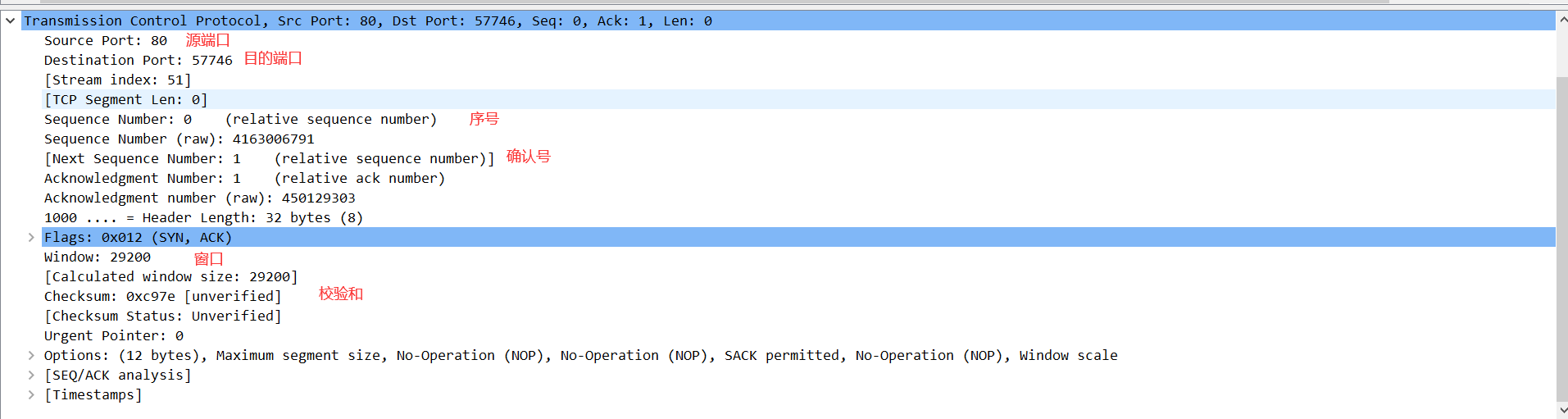
11）Date：Browser发送时间

### HTTP响应报文分析：

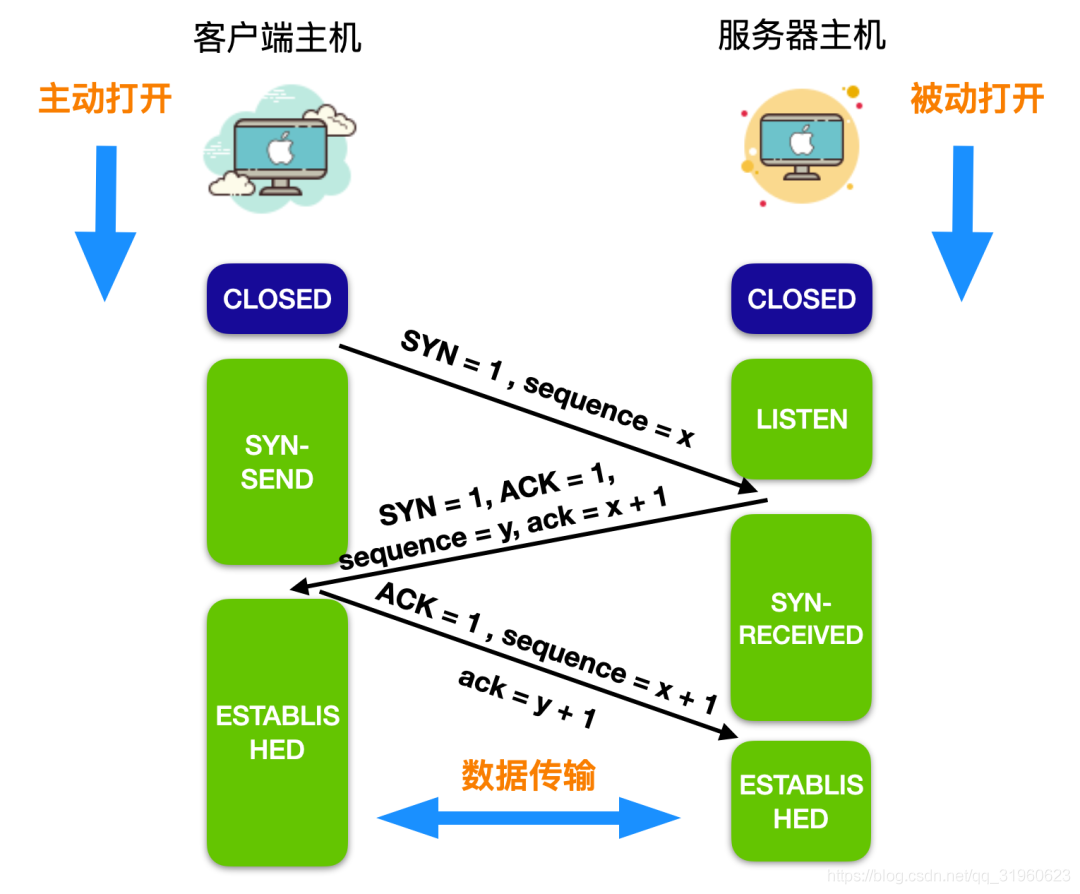


### 分析三次握手：

TCP数据包的具体内容：

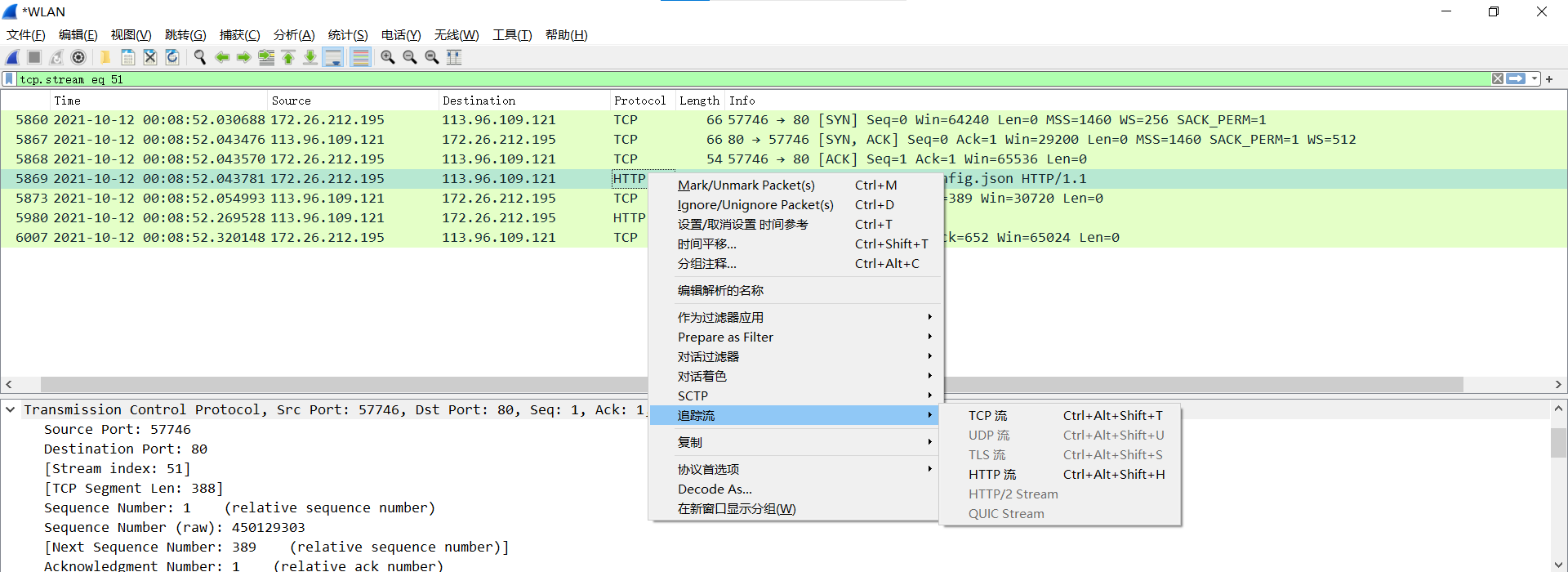


TCP三次握手过程：

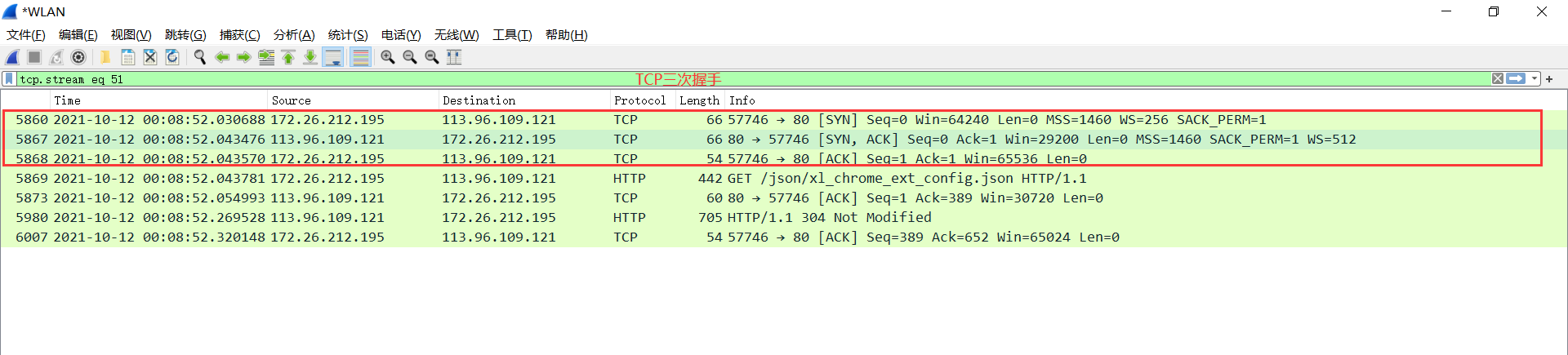


Wireshark中三次握手的具体情形：

在wireshark中输入http过滤，然后选中GET……HTTP/1.1的那条记录，右键然后点击"Follow TCP Stream"



目的是为了得到与浏览器打开网站相关的数据包，将得到如下图

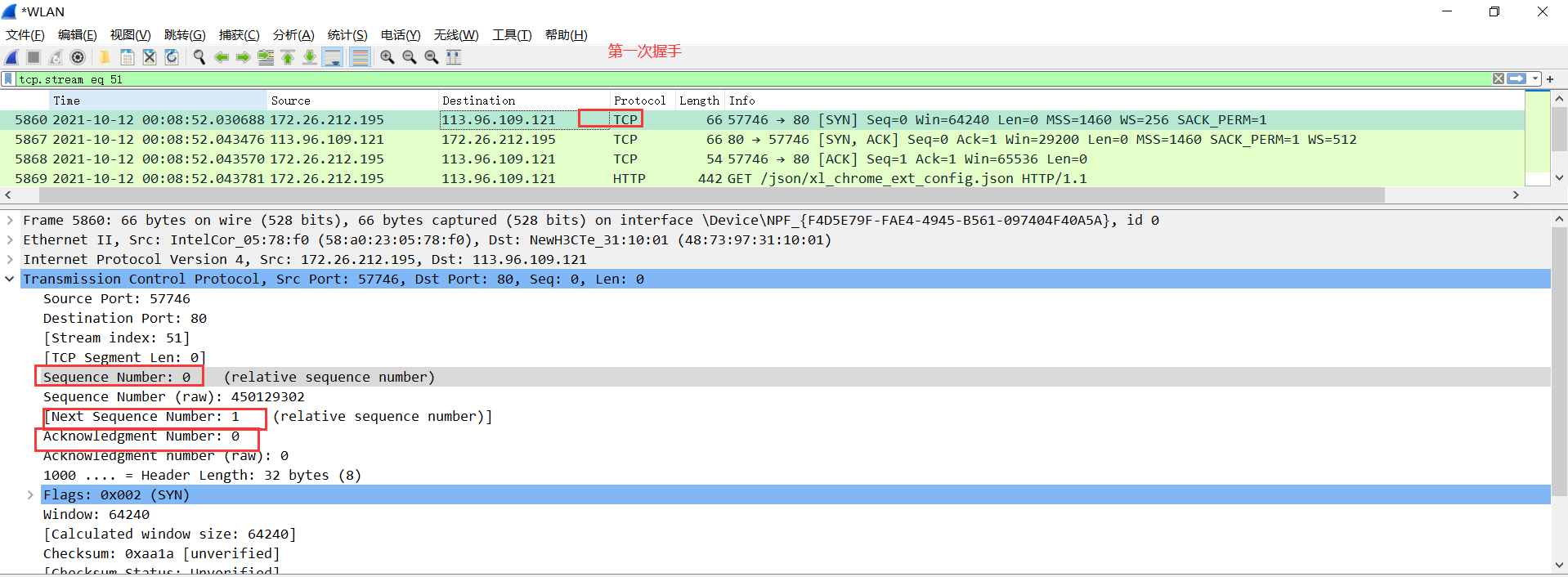


图中可以看到wireshark截获到了三次握手的三个数据包，第四个包才是HTTP的，这说明HTTP的确是使用TCP建立连接的。

#### 第一次握手数据包：

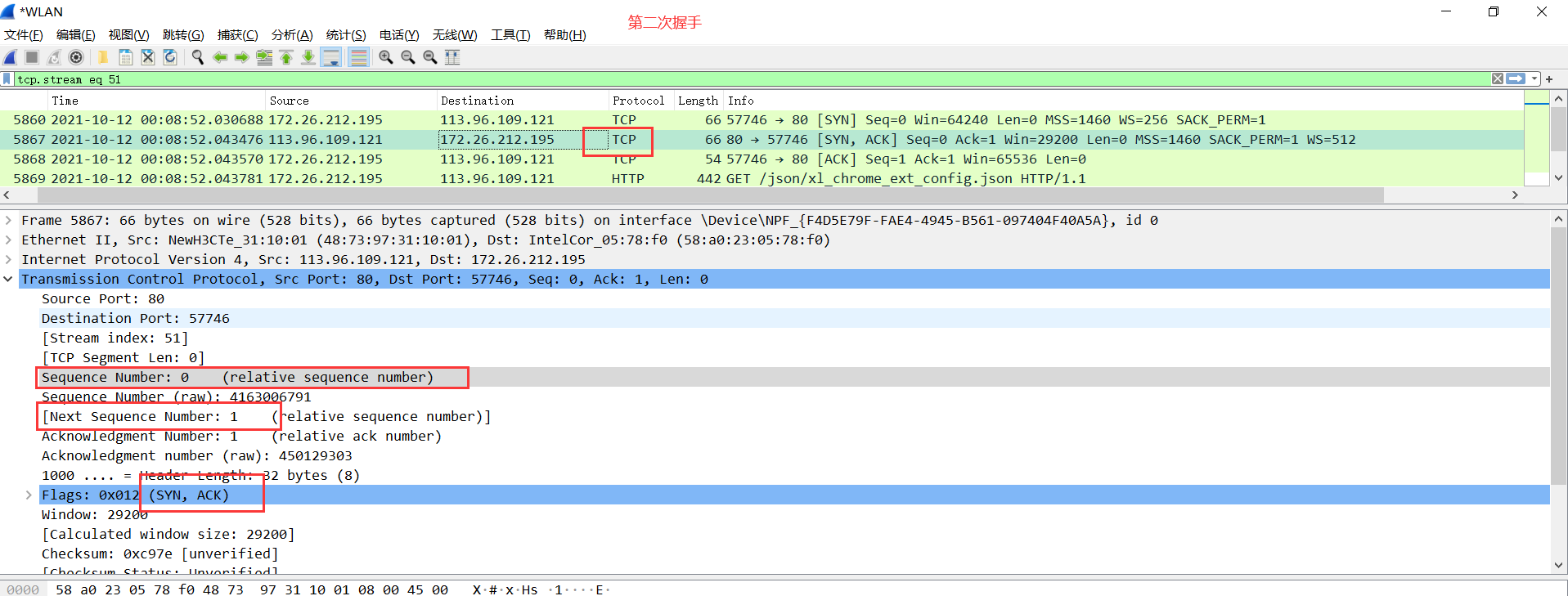
客户端发送一个TCP，标志位为SYN，序列号为0， 代表客户端请求建立连接。

如下图



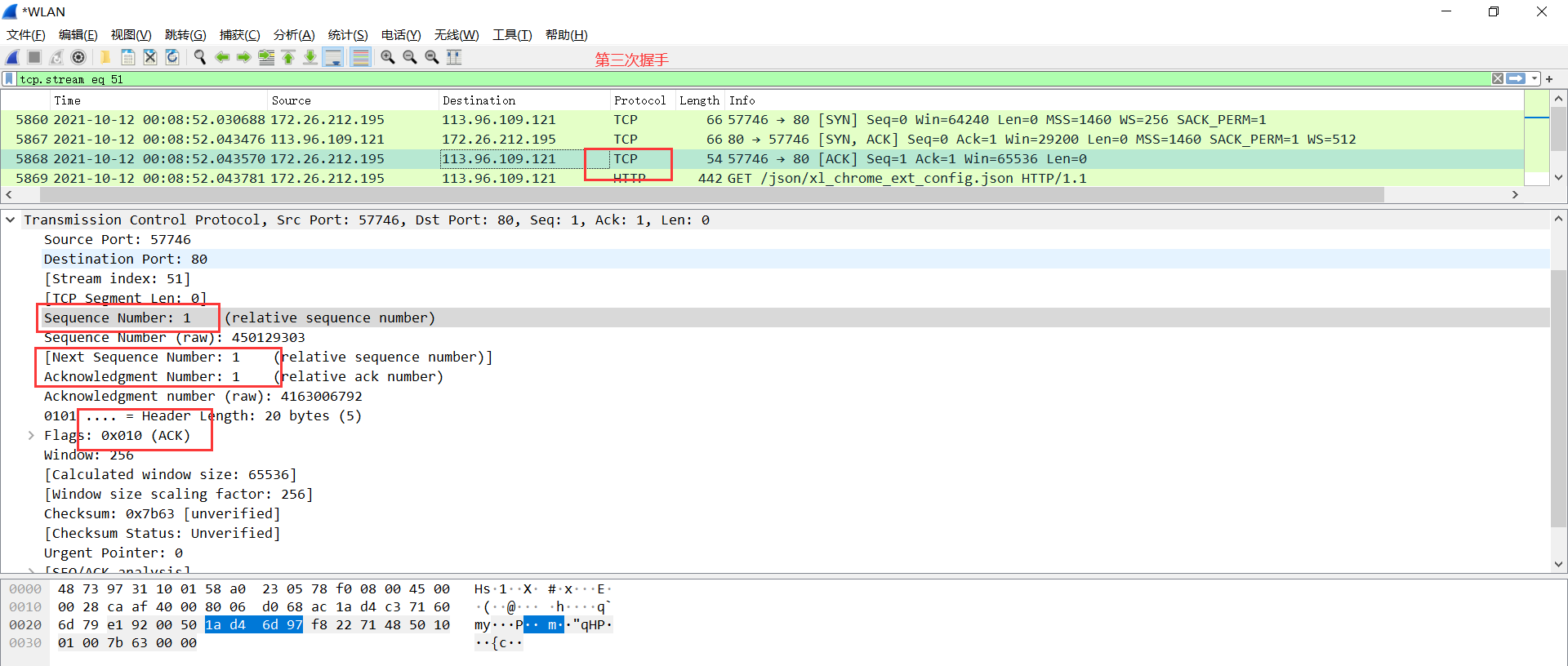
#### 第二次握手的数据包

服务器发回确认包, 标志位为 SYN,ACK. 将确认序号(Acknowledgement Number)设置为客户的ISN加1，即0+1=1, 如下图



#### 第三次握手的数据包

客户端再次发送确认包(ACK) SYN标志位为0,ACK标志位为1.并且把服务器发来ACK的序号字段+1,放在确定字段中发送给对方。并且在数据段放写ISN的+1，如下图:



## 二、DNS协议分析

通过域名访问某网站，用wireshark捕获DNS数据包，并分析DNS工作过程和DNS格式。

**注意：**

1. 有时候可能捕获不到DNS解析过程，为什么？要仔细分析。

回答：本机与DNS服务器之间的网络出现异常导致无法正常访问，从而无法正常进行DNS解析导致无法捕获。

1. 可以自己建立DNS服务器并使用它进行域名解析。

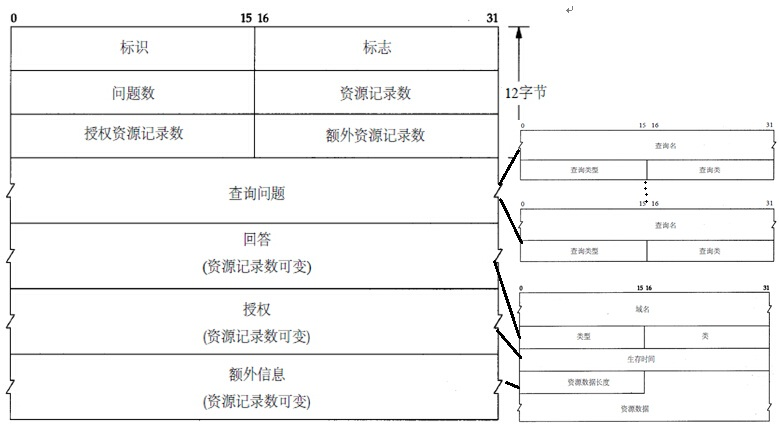
1）建立DNS服务器。

利用windows自带组件或下载DNS软件（如**ntbind**），建立DNS服务器，并对DNS服务器的配置（建立域名-IP地址的解析关系）。

2）使用DNS

在任意一台计算机上配置TCP/IP协议，将DNS服务器配置成上述DNS服务器（注意该DNS服务器的IP地址是静态的），用该DNS服务器中设置的器域名访问该WWW服务，并与用IP地址访问的结果进行比较。（注意该客户机的IP地址最好与DNS服务器地址同一个网段，即网络号相同）

### DNS报文格式



DNS报文格式分为五大部分。分别为：报文头Header，问题区段（Question），回答区段（Answer），权威区段（Authority），额外信息区段（Additional）。但是不是五个段必须存在，只有Header必须存在，别的段在不同情况下不存在。

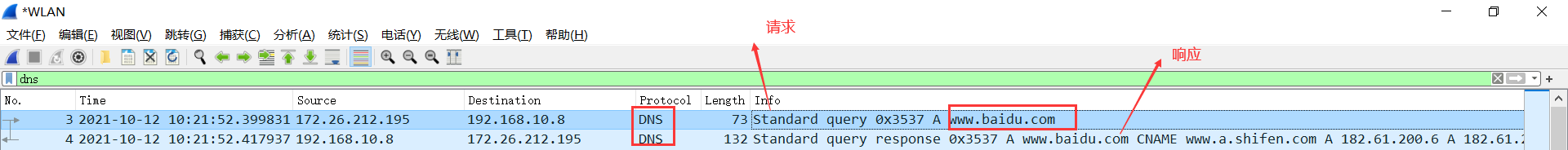
Header段中每个字段的含义：

* DNS ID号（DNS ID Number）：用来对应DNS查询和DNS响应
* 查询/响应（Query/Response，QR）：用来指明这个报文是DNS查询还是响应，占1个比特位。为1代表响应，0代表查询
* 操作代码（OpCode）：用来定义消息中请求的类型
* 权威应答（Authoritative Answer， AA）：这个比特位在响应的时候才有意义。则说明这个响应是由域内权威域名服务器发出的
* 截断（Truncation，TC）：用来指出报文比允许的长度还要长，导致被截断
* 期望递归（Recursion Desired, RD）：如果设置了RD，就建议域名服务器进行递归解析，递归查询的支持是可选的。
* 支持递归（Recursion Available， RA）： 当响应中设定了这个值，说明域名服务器支持递归查询
* 保留（Z）：未使用，用0表示
* 响应代码（Response Code）：在DNS响应中指明错误，占4个比特位。
* 问题计数（Question Count）：问题区段中的问题记录数
* 回答计数（Answer Count）：回答区段中的回答记录数
* 域名服务计数（Name Server Count）：权威区段中的记录数
* 额外记录数（Additional Records Count）：在额外信息区段中的记录数
* 问题区段（Question Section）：包含有被发送到DNS服务器的一条或者多条信息
* 回答区段（Answer Section）：含有用来回答查询的一条或者多条资源记录
* 权威区段（Authority Section）：包含权威域名服务器的资源记录
* 额外信息区段（Additional Information Section）：包含资源记录且大小可变的区段。

### 捕获DNS数据包

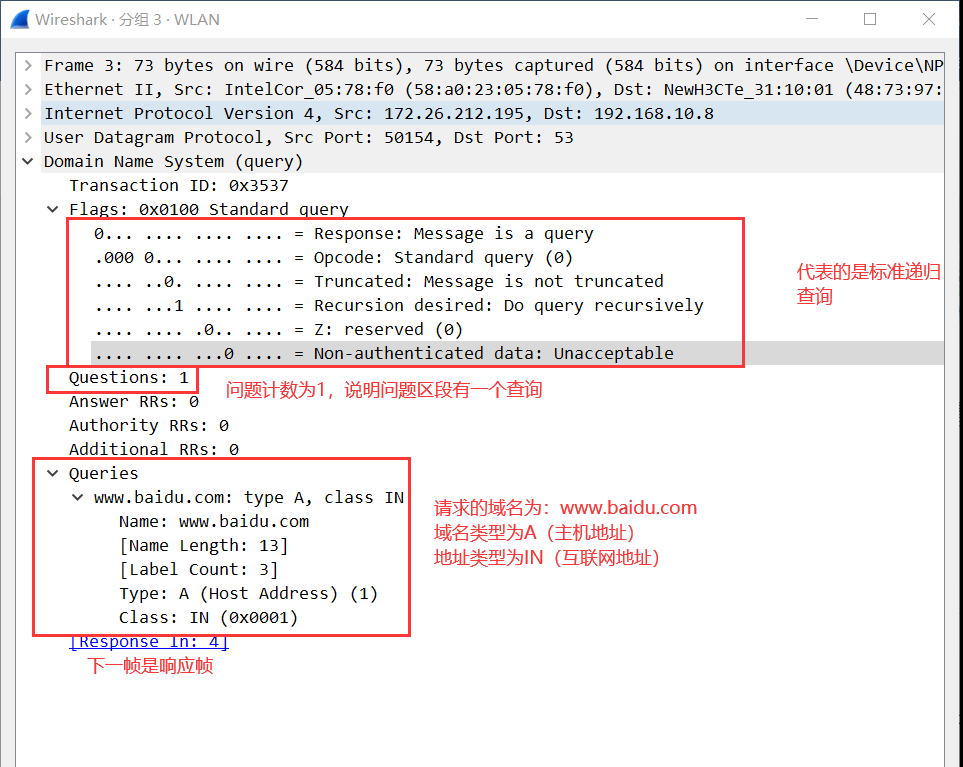
刘篮球输入网址[www.baidu.com，Wireshark](http://www.baidu.com，Wireshark)捕获DNS数据包





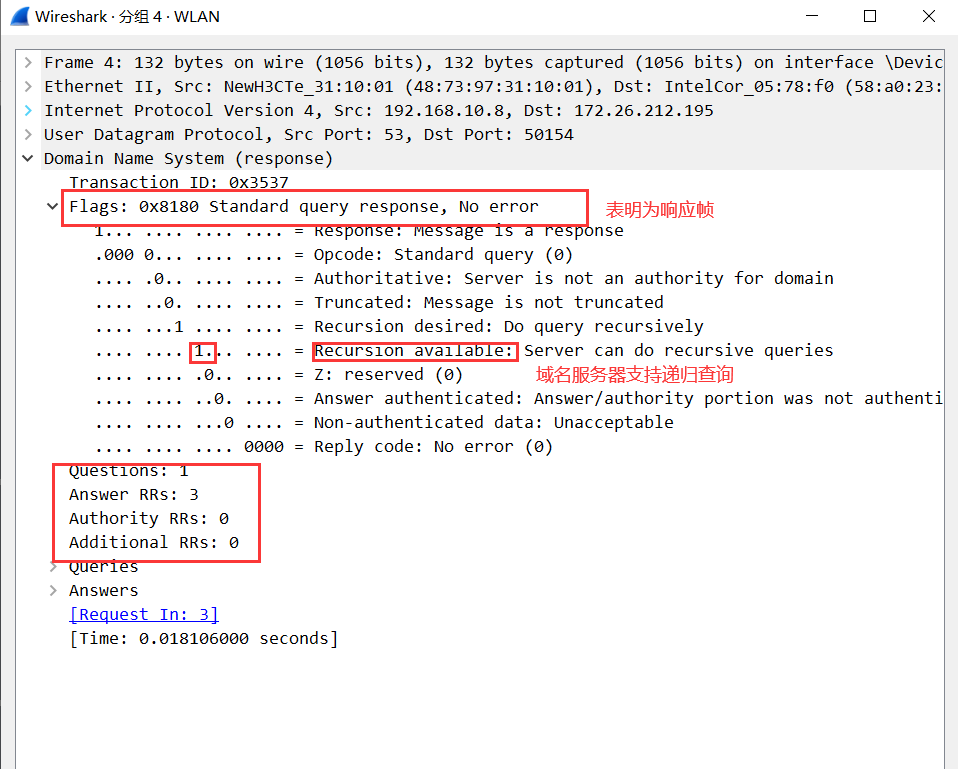
可以看到一个DNS请求帧，一个DNS响应帧

### 分析DNS请求帧

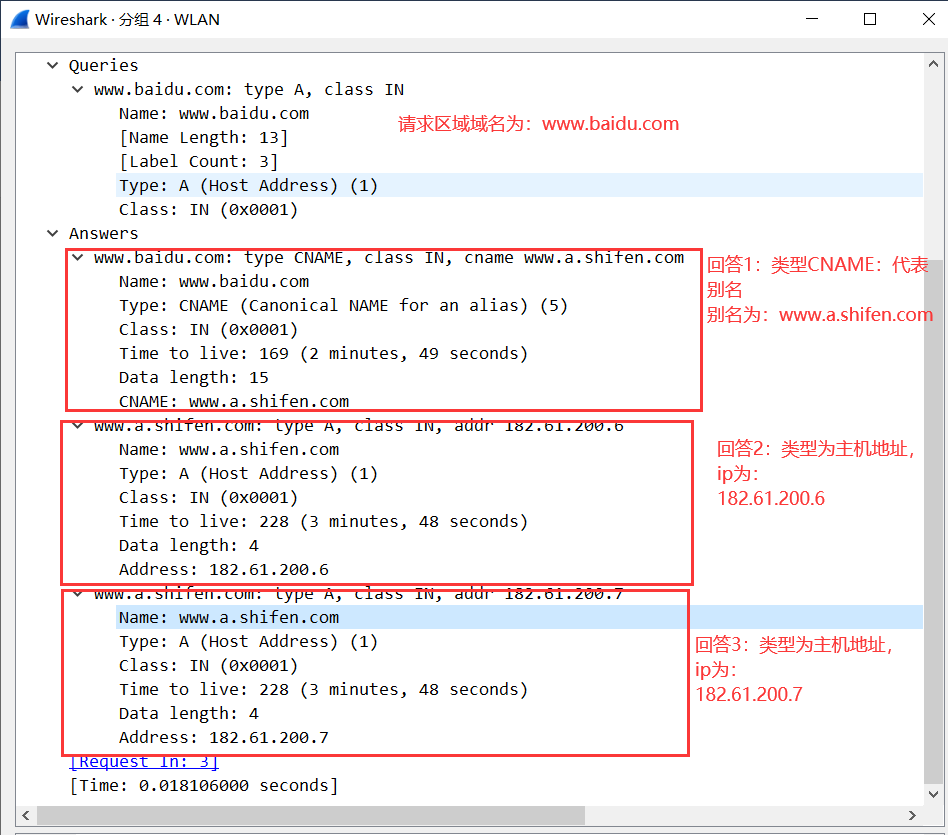


请求计数为1.请求的主机域名是：[www.baidu.com](http://www.baidu.com)

### 分析DNS响应帧



问题区段与回答区段：



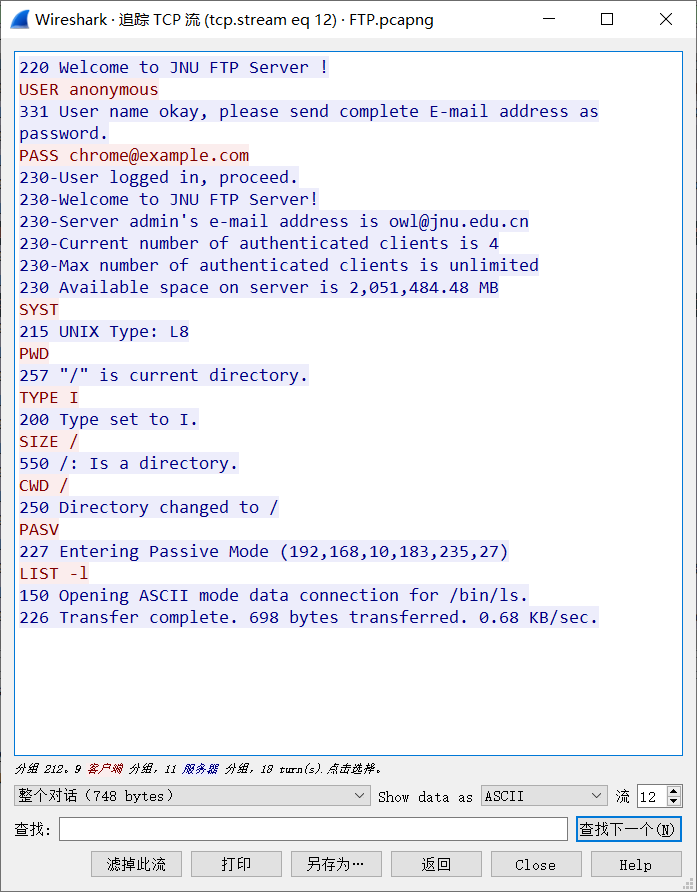
## 三、FTP协议分析

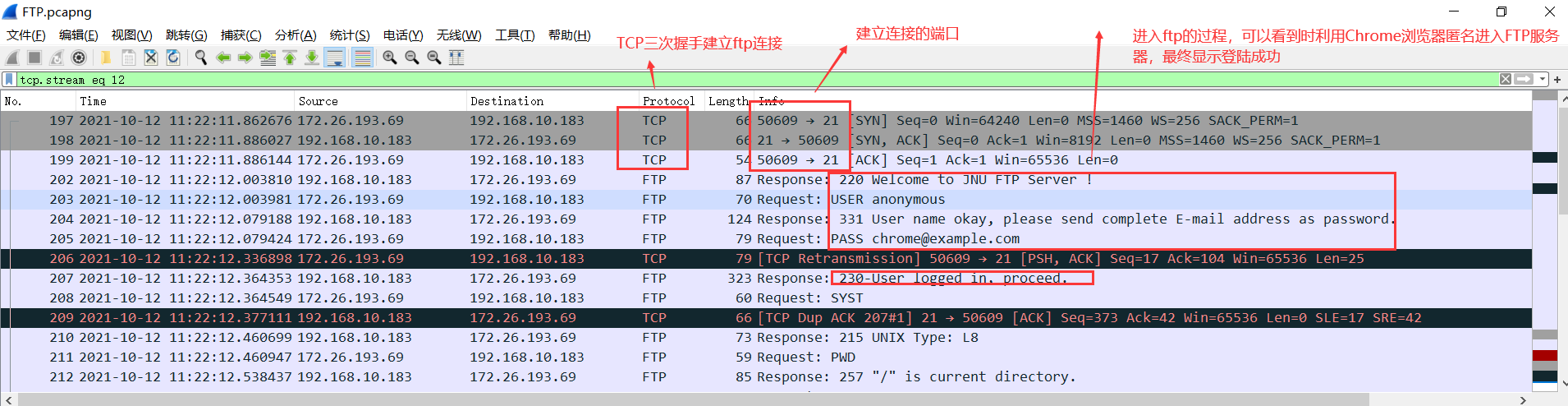
**1.**访问FTP服务器。如ftp://ftp.jnu.edu.cn

2.用wireshark分析FTP的工作过程。注意观察FTP的工作模式，用于控制连接的端口和数据连接的端口。

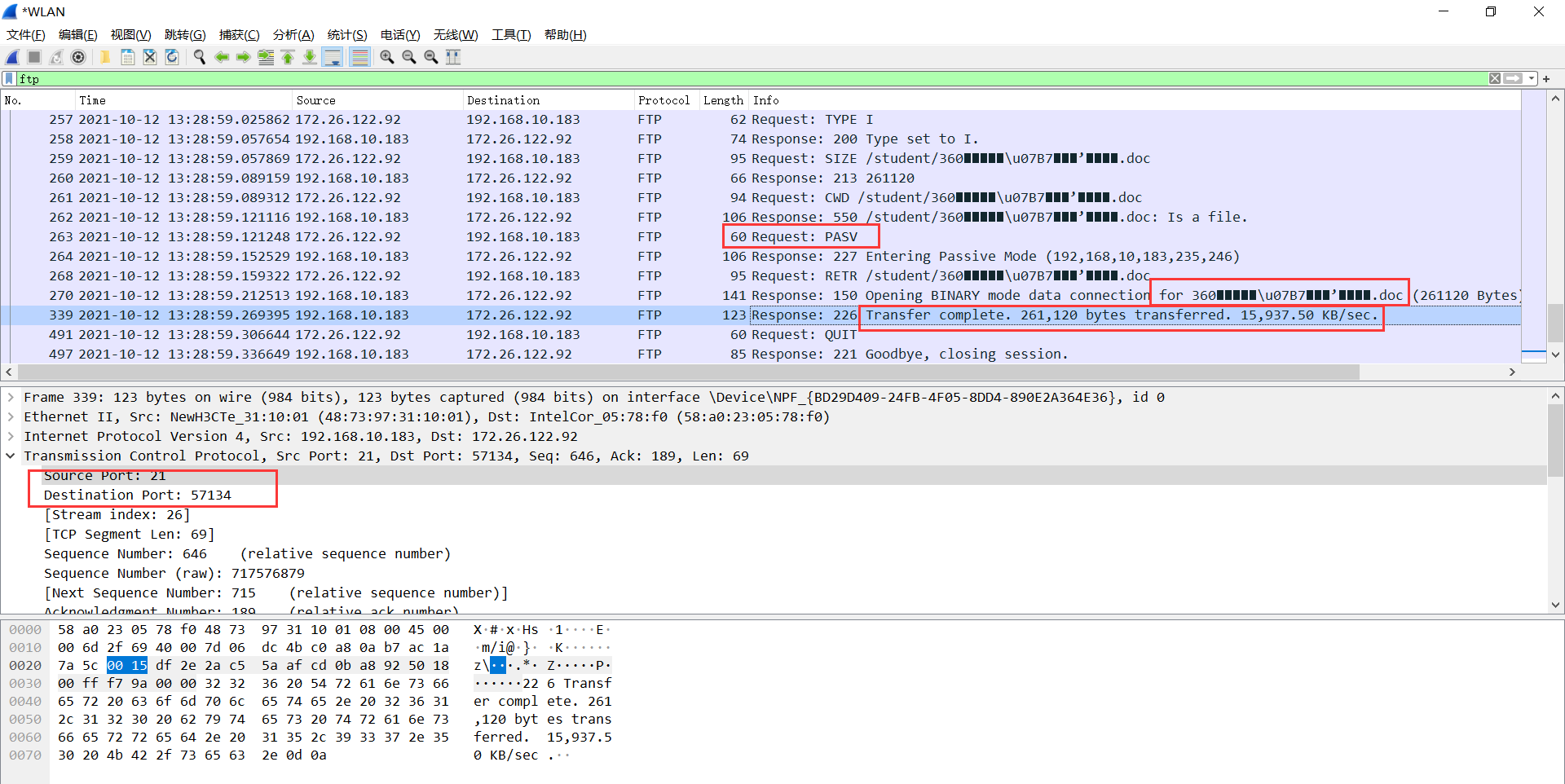
**注意：**可以利用Windows自带的FTP组件或下载FTP软件，建立FTP服务器，并进行配置，并访问分析FTP协议

用浏览器访问<ftp://ftp.jnu.edu.cn/>的ftp服务器，再视同wireshark分析ftp工作过程。

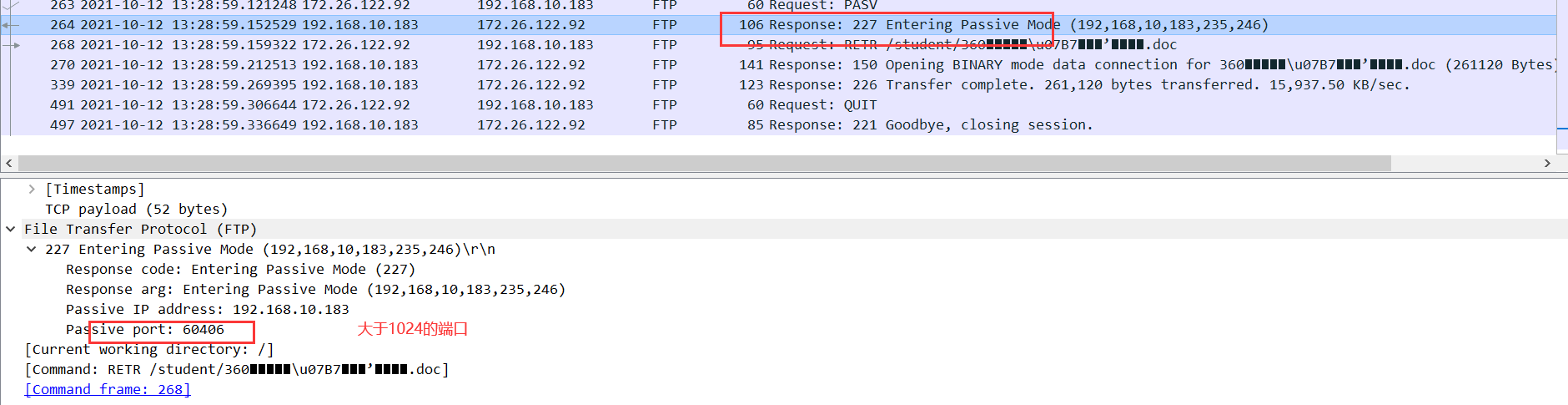




从中ftp下载了一个文件，可以看到如下图：

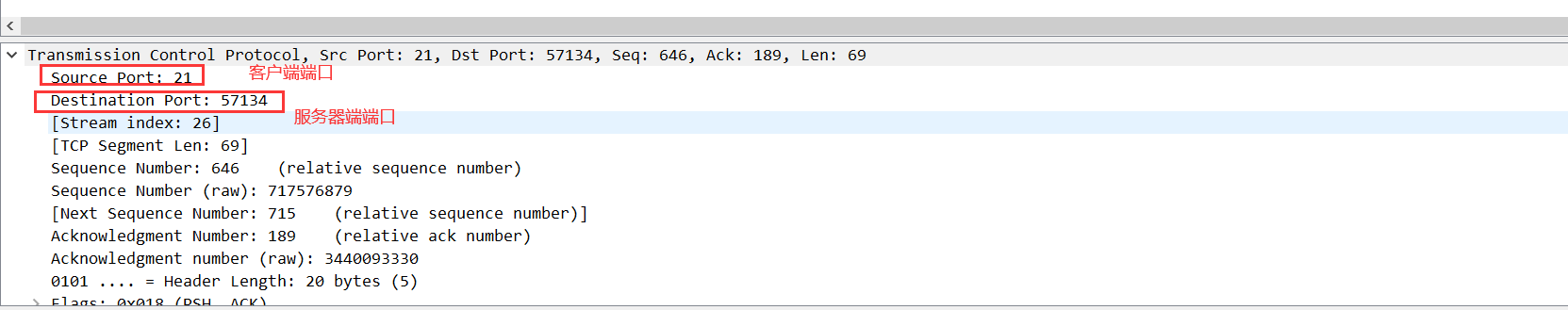


这里的是PASV被动模式抓包



这里也显示在打开文档，就是进行了数据通道中的数据传送



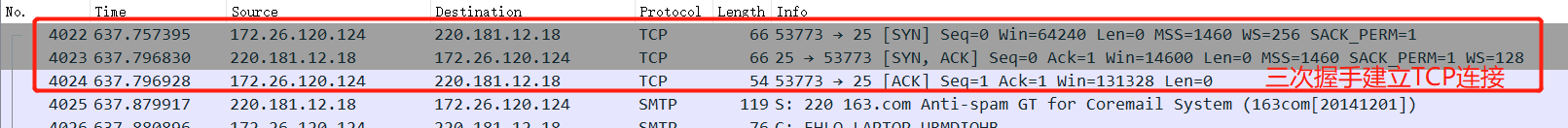


## 四、 SMTP和POP协议分析

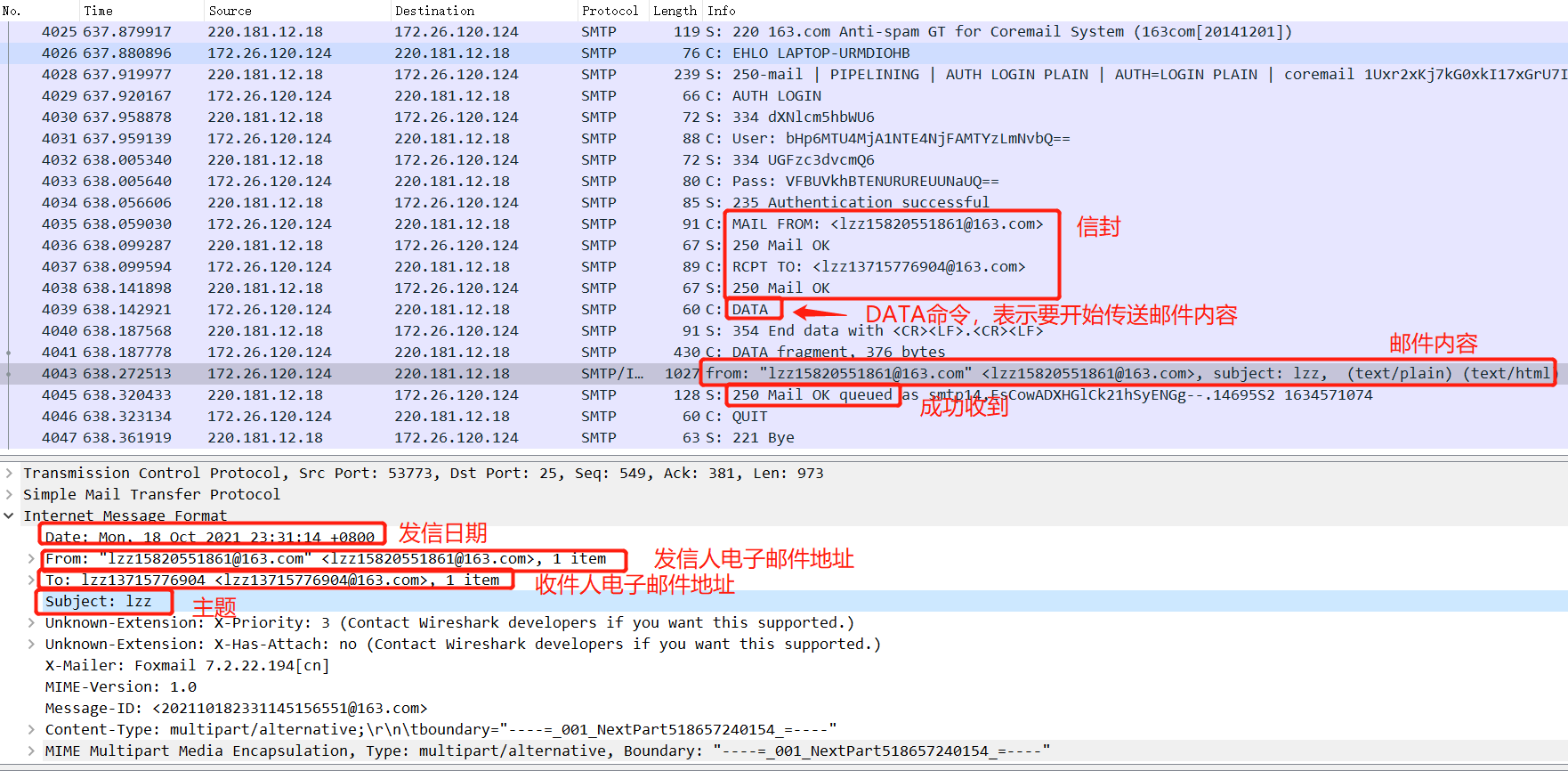
用客户端的邮件软件foxmail收发邮件，捕获数据报分析邮件收发过程和SMTP、POP3等协议格式和工作过程。

SMTP协议的工作过程可分为如下3个过程：

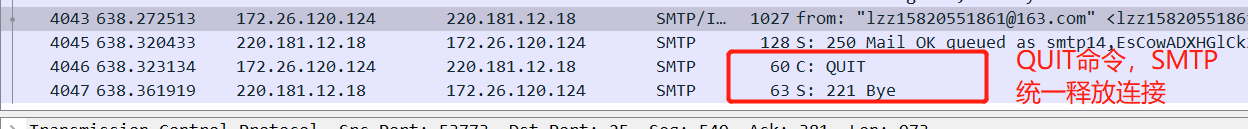
1. 建立连接：在这一阶段，SMTP客户请求与服务器的25端口建立一个TCP连接。



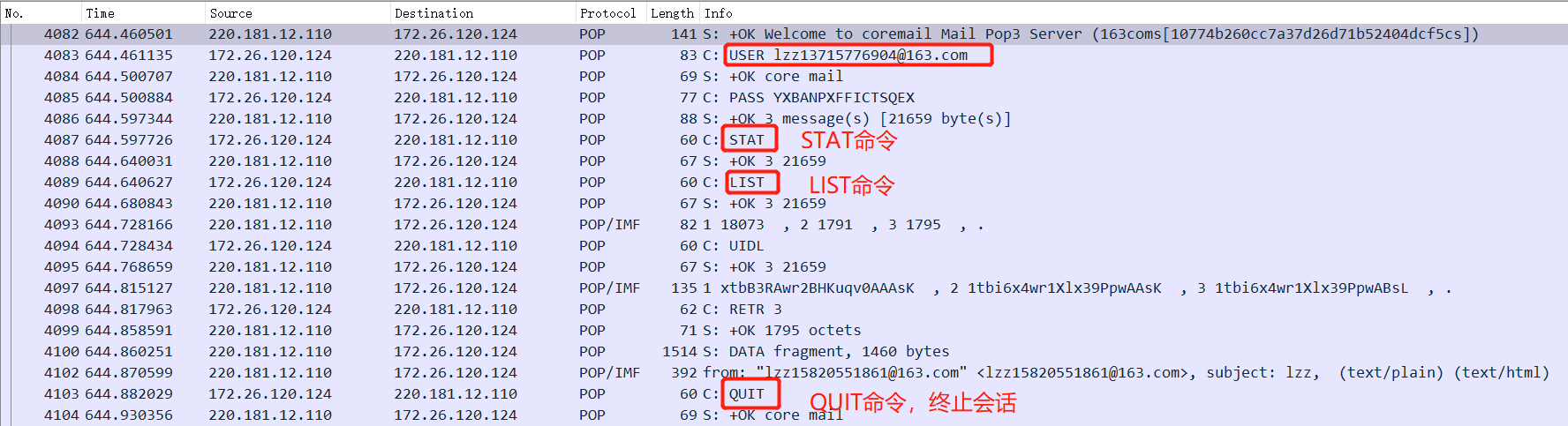
1. 邮件传送：利用命令，SMTP客户将邮件的源地址、目的地址和邮件的具体内容传递给SMTP服务器，SMTP服务器进行相应的响应并接收邮件。从mail命令开始。



(3)连接释放：SMTP客户发出退出命令，服务器在处理命令后进行响应，随后关闭TCP连接。



POP协议的工作过程：



## (六)：实验小结

这次实验我们学习了HTTP协议，DNS协议，FTP协议，SMTP协议和POP协议，理解了这些协议的作用和原理，并学会了通过wireshark来分析HTTP，DNS，FTP，SMTP，POP协议的工作过程，使得我们对协议的格式以及原理有了更深的理解。通过这次实验，我们将更加了解应用层的这些协议，这将有助于我们今后的计算机网络的学习。

**暨南大学本科实验报告专用纸(附页)**