**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 钟颖谦 学号 2019051091

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 09 月 28上午～ 10月 12 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

无

## 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。

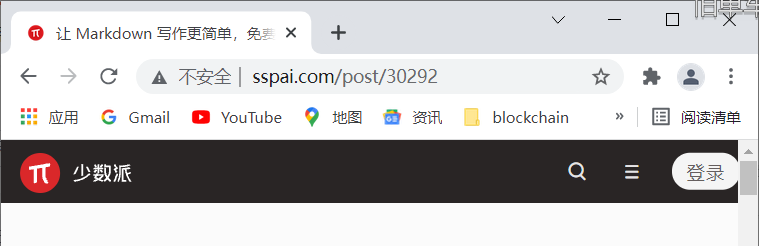
1．设置过滤条件

指定网络协议http

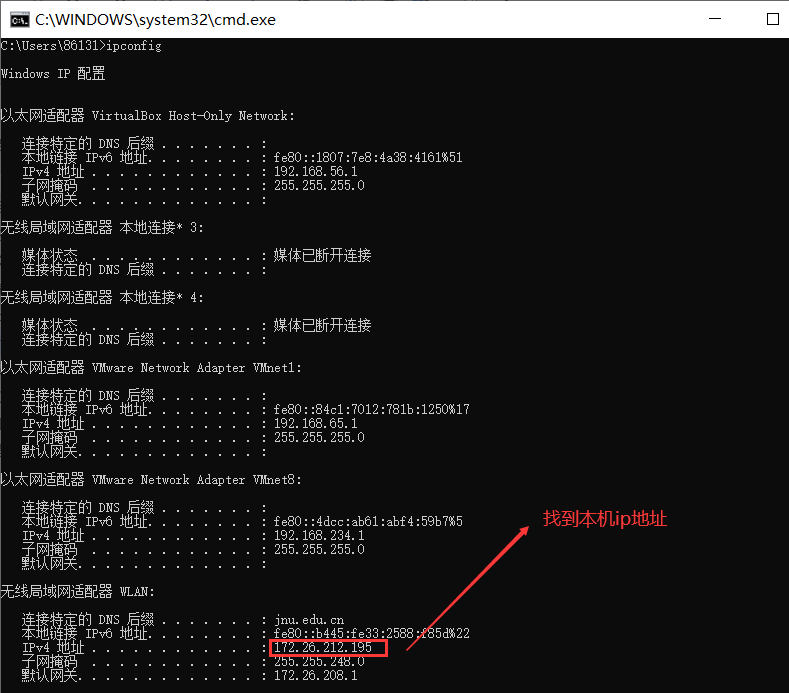


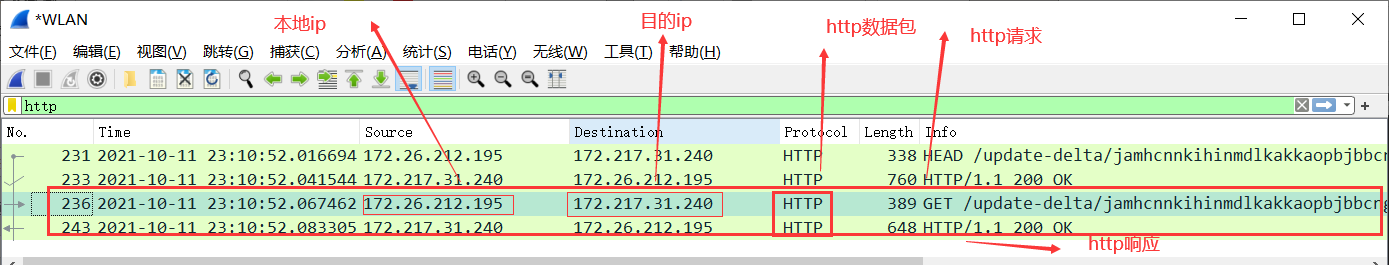
**2.打开Chrome浏览器输入网址**

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**

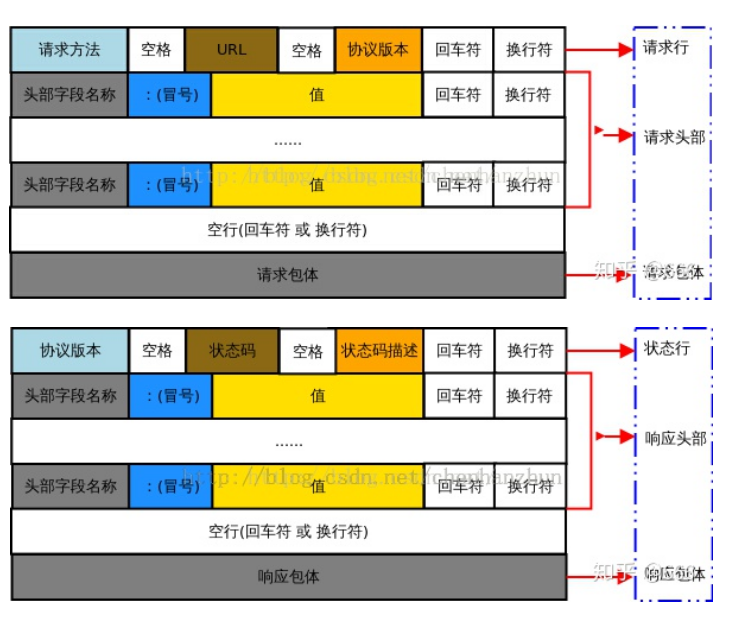




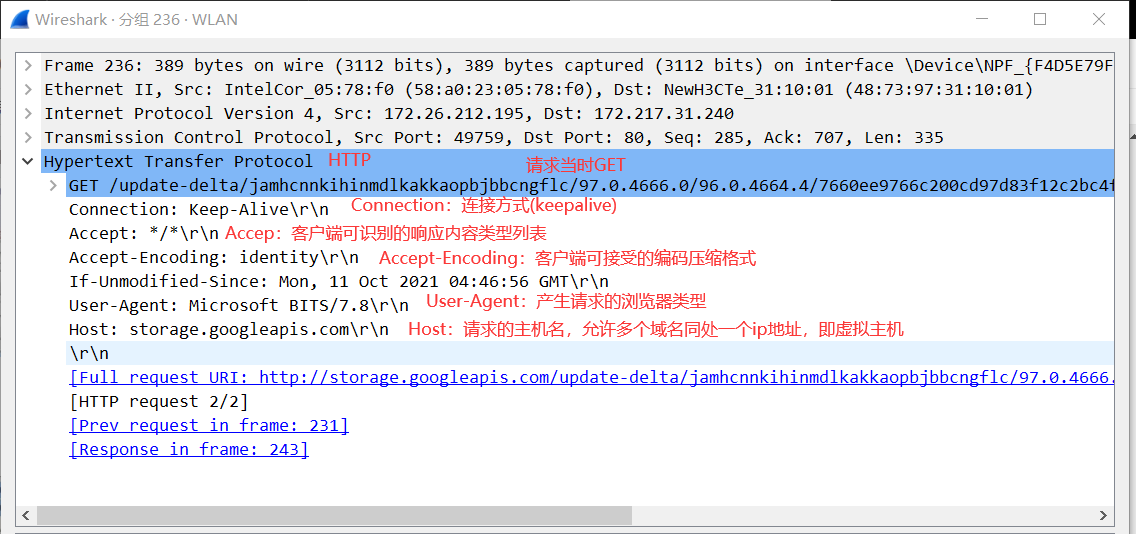
### HTTP数据包分析：



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。

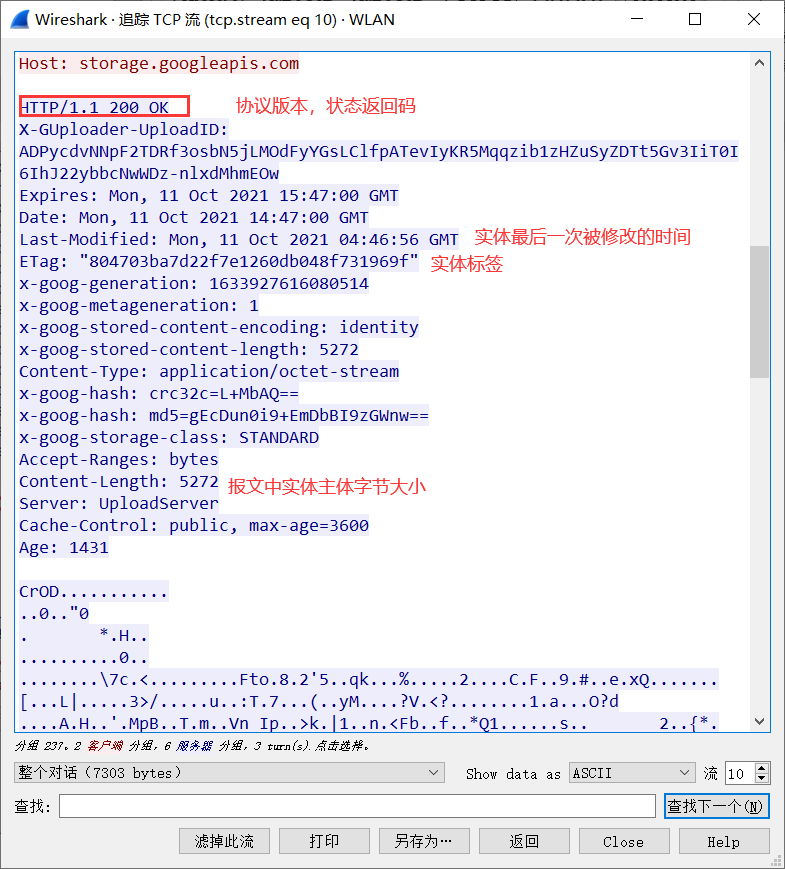
8）User-Agent：告诉服务器，Browser内核。

9）Cookie：

10）Connection：保持连续发完信息后，我不关闭连接。

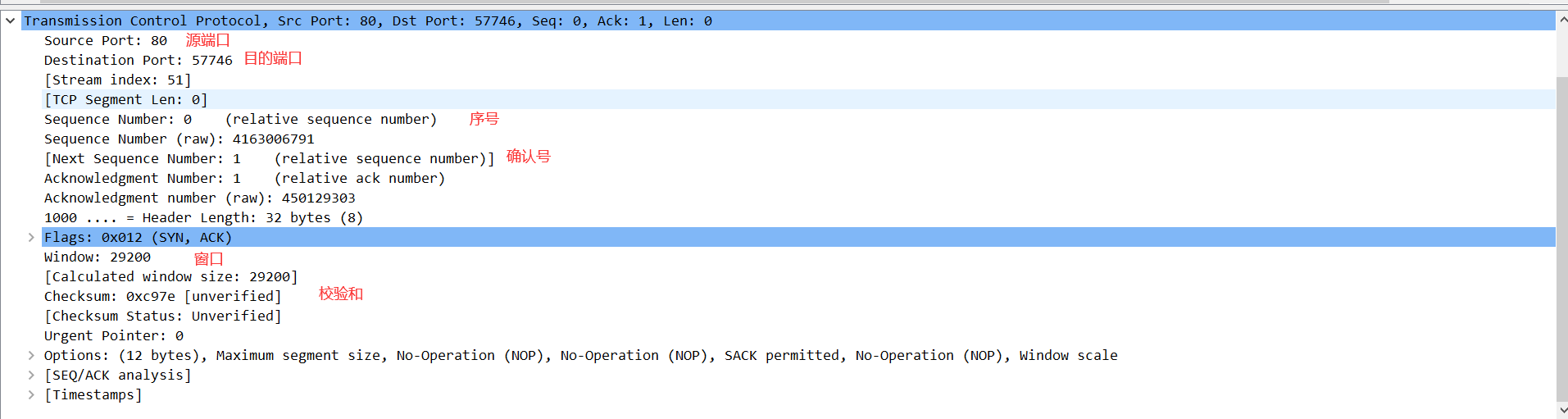
11）Date：Browser发送时间

### HTTP响应报文分析：

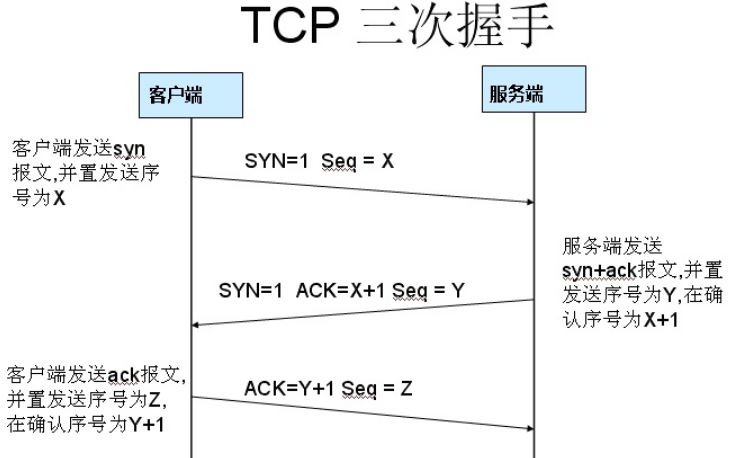


### 分析三次握手：

TCP数据包的具体内容：

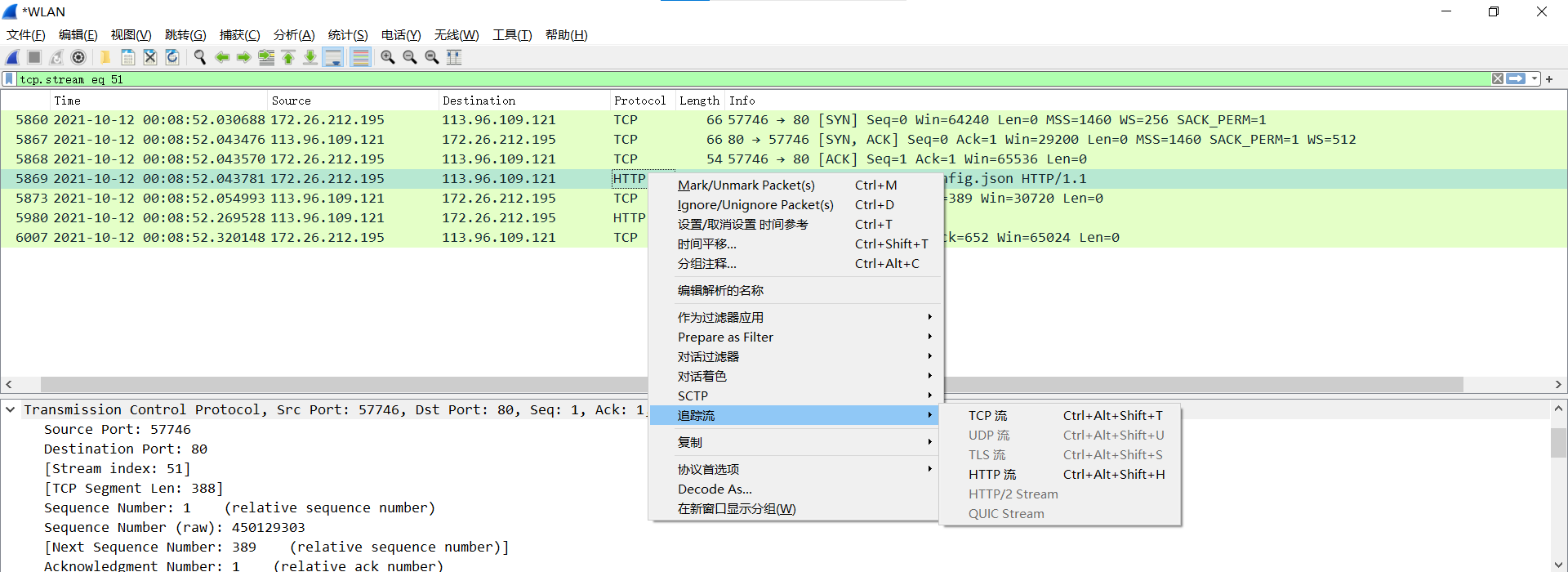


TCP三次握手过程：

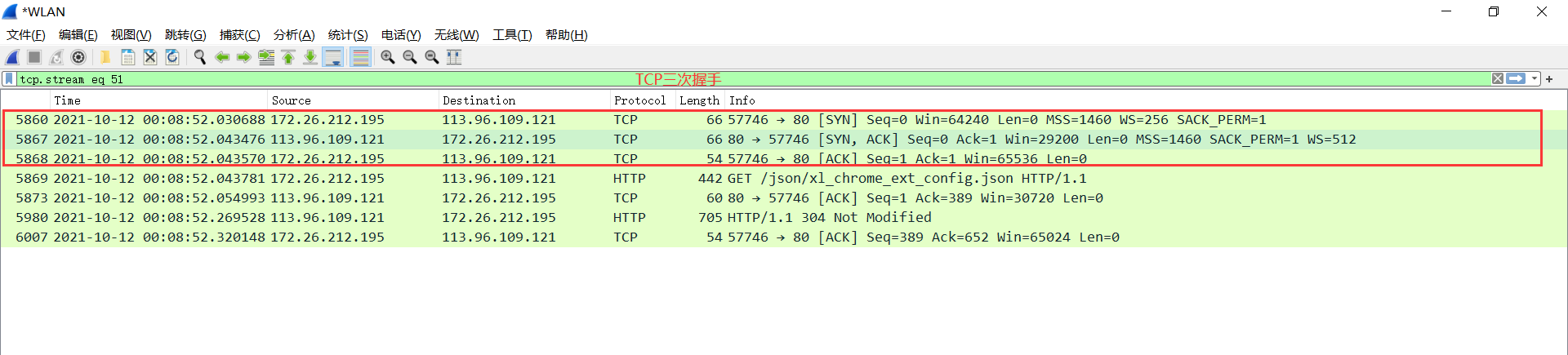


Wireshark中三次握手的具体情形：

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

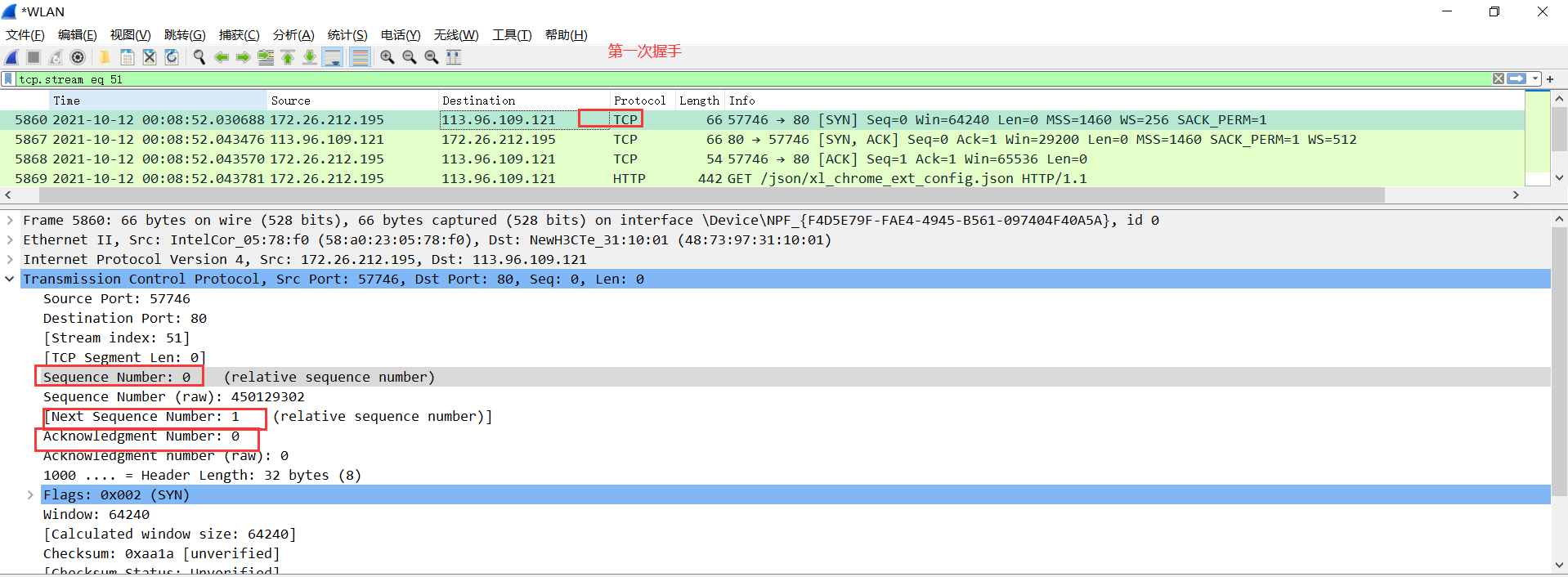


图中可以看到wireshark截获到了三次握手的三个数据包，第四个包才是HTTP的，这说明HTTP的确是使用TCP建立连接的。

#### 第一次握手数据包：

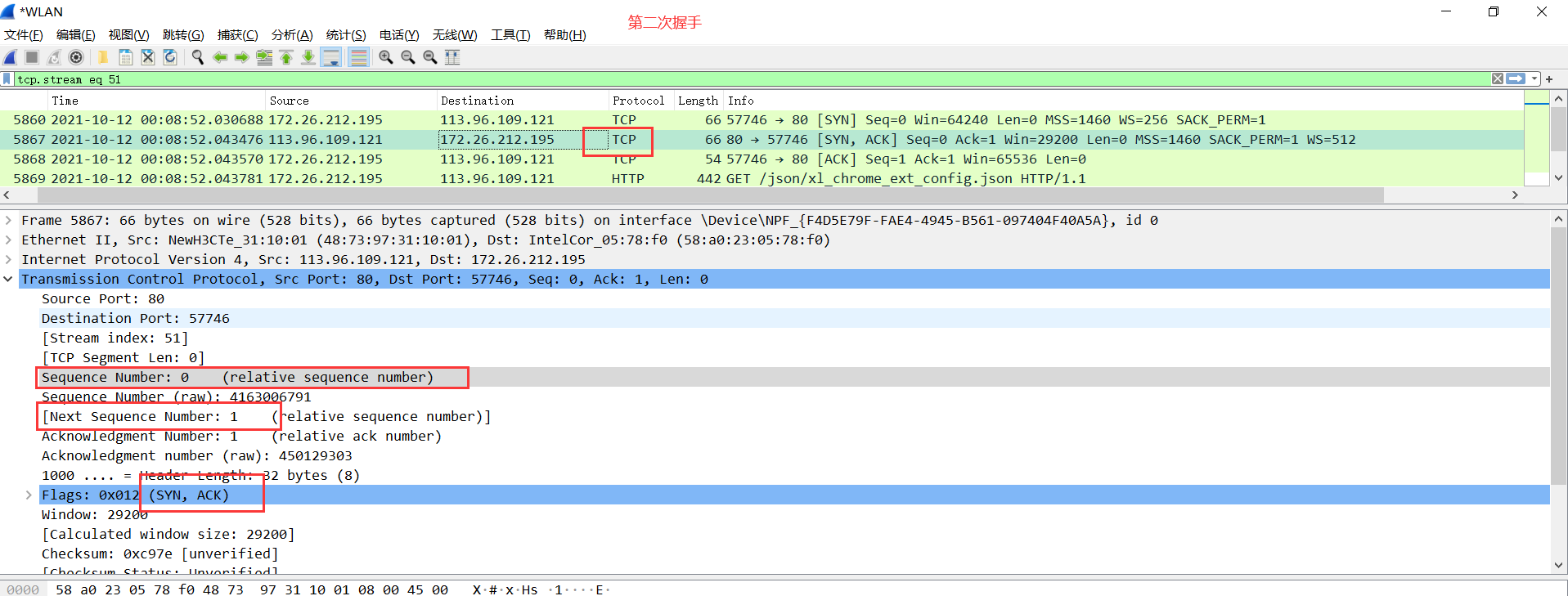
客户端发送一个TCP，标志位为SYN，序列号为0， 代表客户端请求建立连接。

如下图



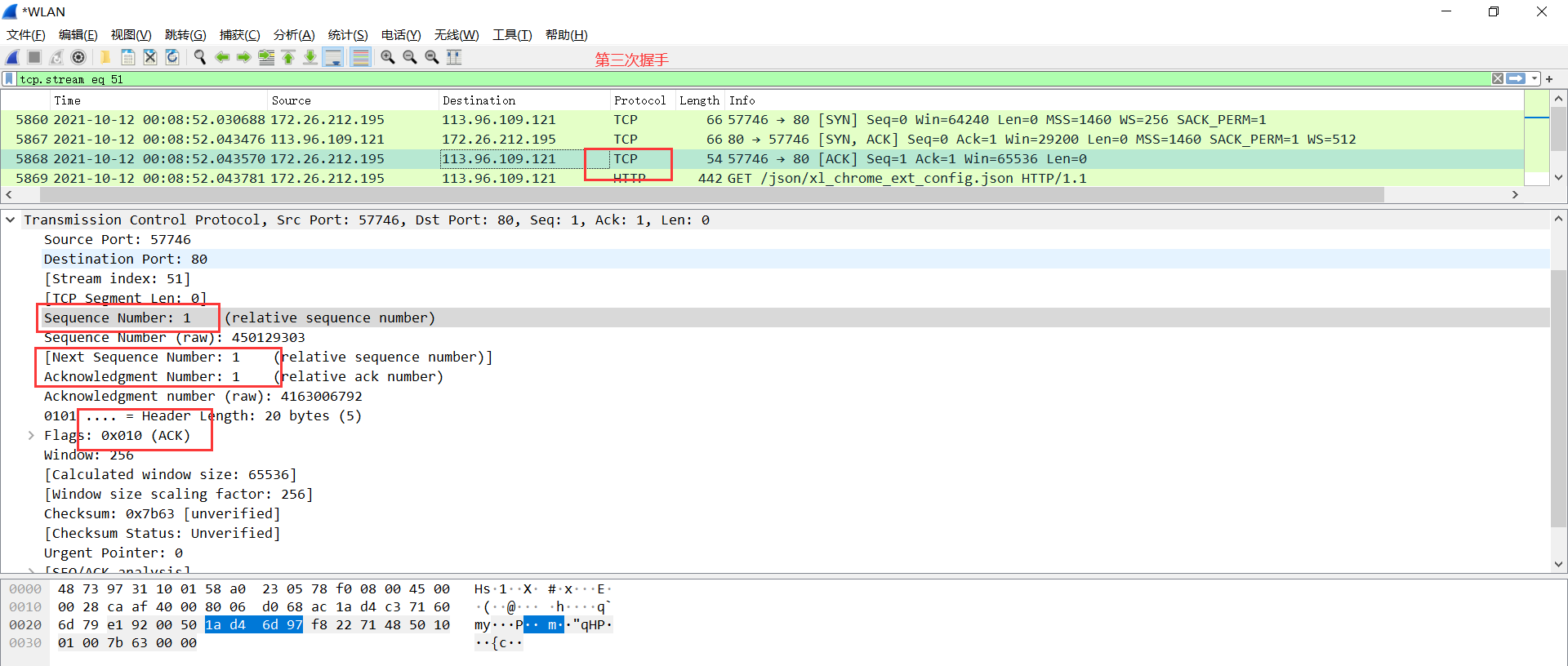
#### 第二次握手的数据包

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。

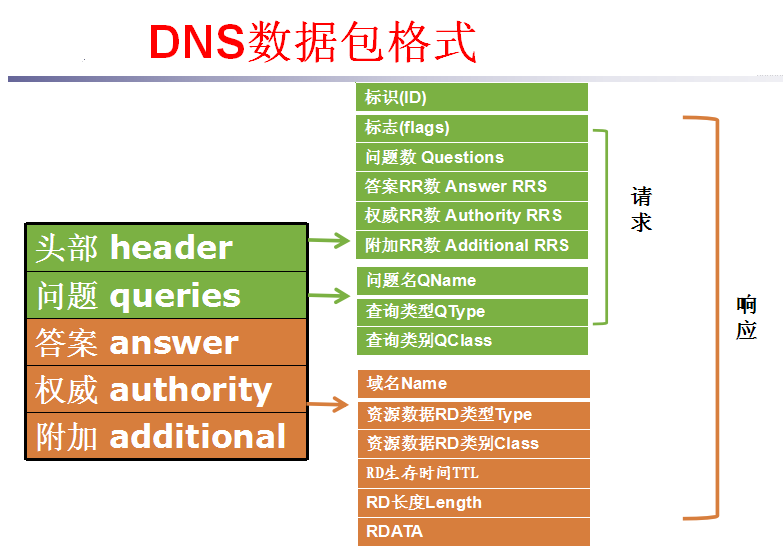
1）建立DNS服务器。

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）

3、附DNS数据包格式（细节见课件）



### 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。

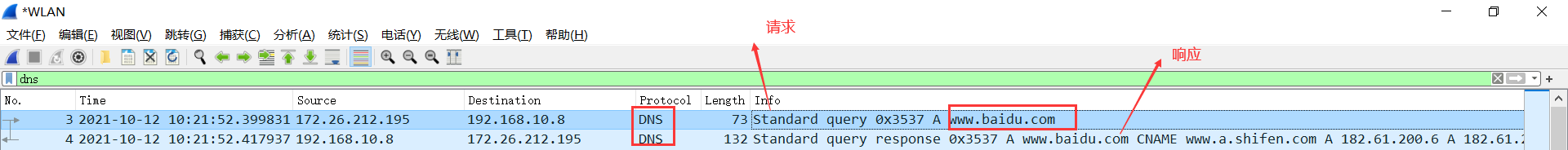
Header段中每个字段的含义：

* 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

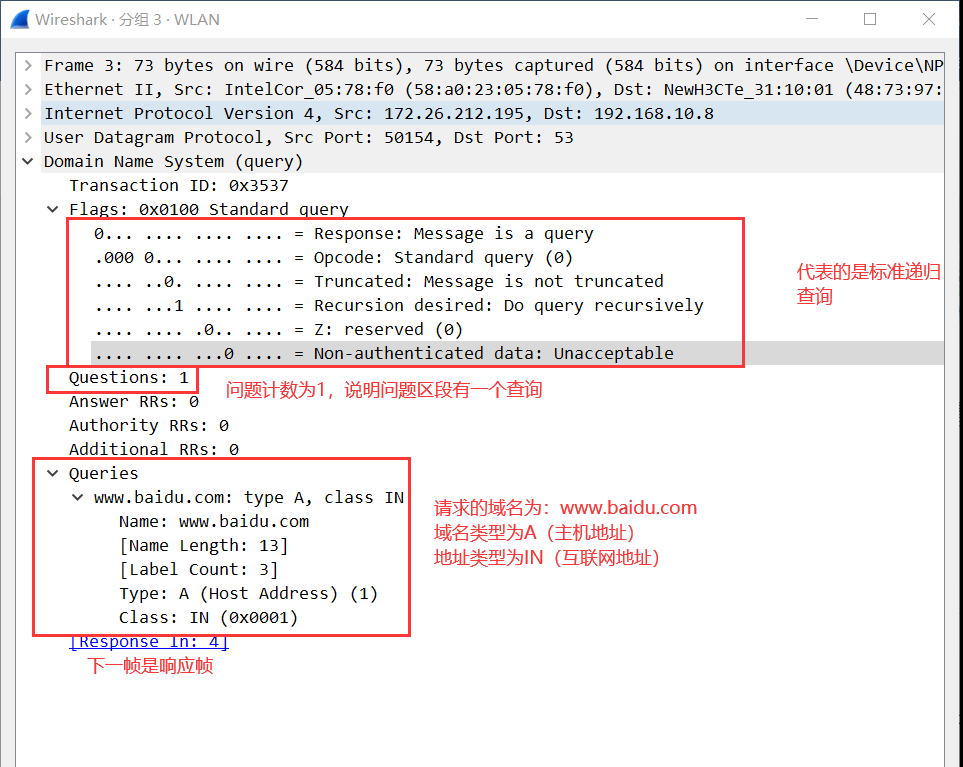
刘篮球输入网址[www.baidu.com，Wireshark](http://www.baidu.com，Wireshark)捕获DNS数据包





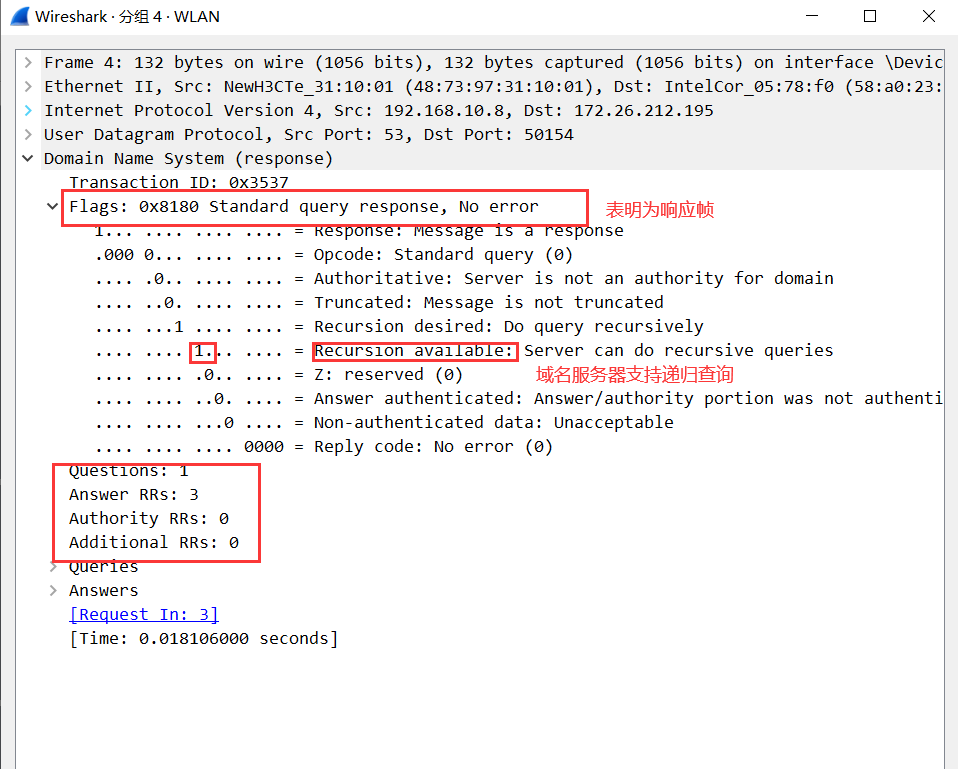
可以看到一个DNS请求帧，一个DNS响应帧

### 分析DNS请求帧

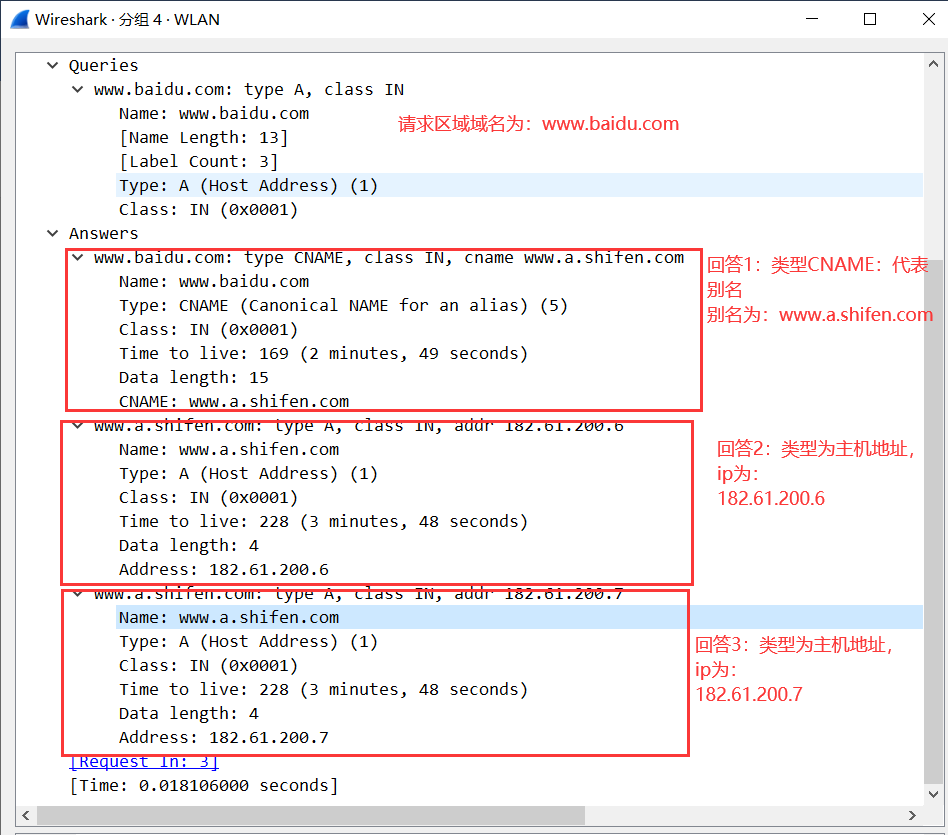


请求计数为1.请求的主机域名是：[www.baidu.com](http://www.baidu.com)

### 分析DNS响应帧



问题区段与回答区段：



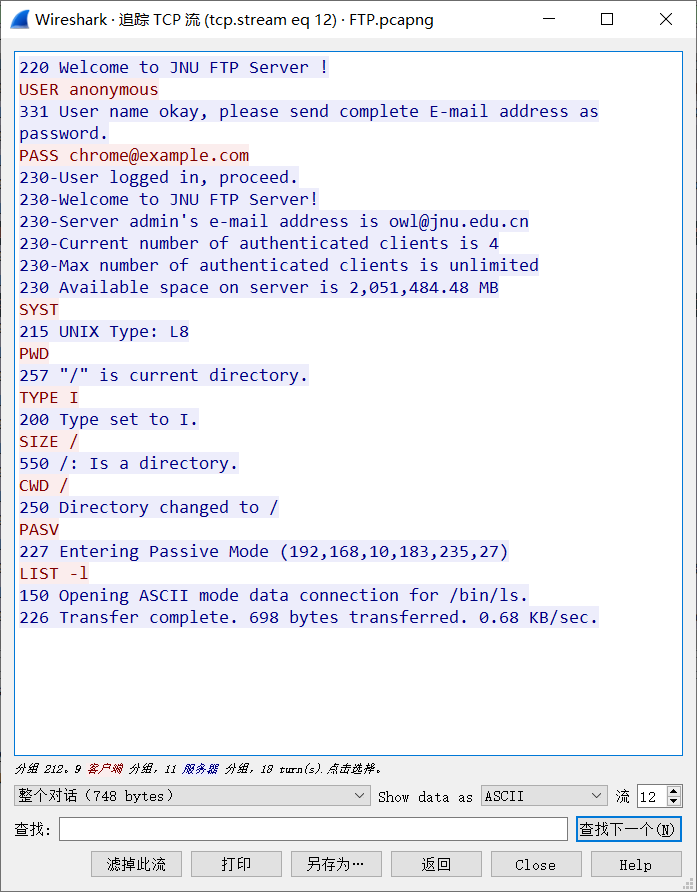
## 三、FTP协议分析

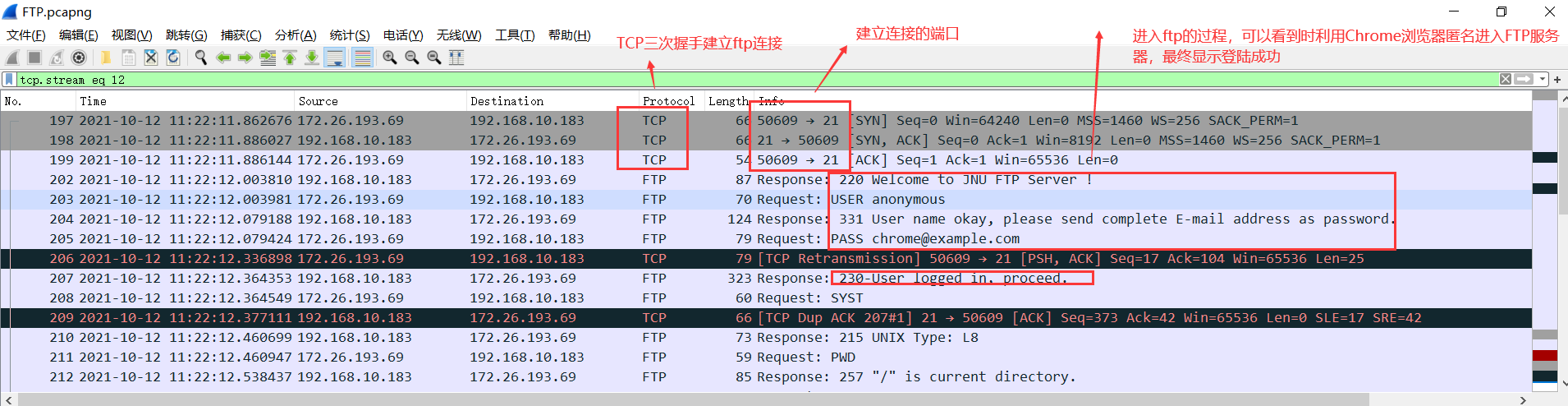
**1.**访问FTP服务器。如ftp://ftp.jnu.edu.cn

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。

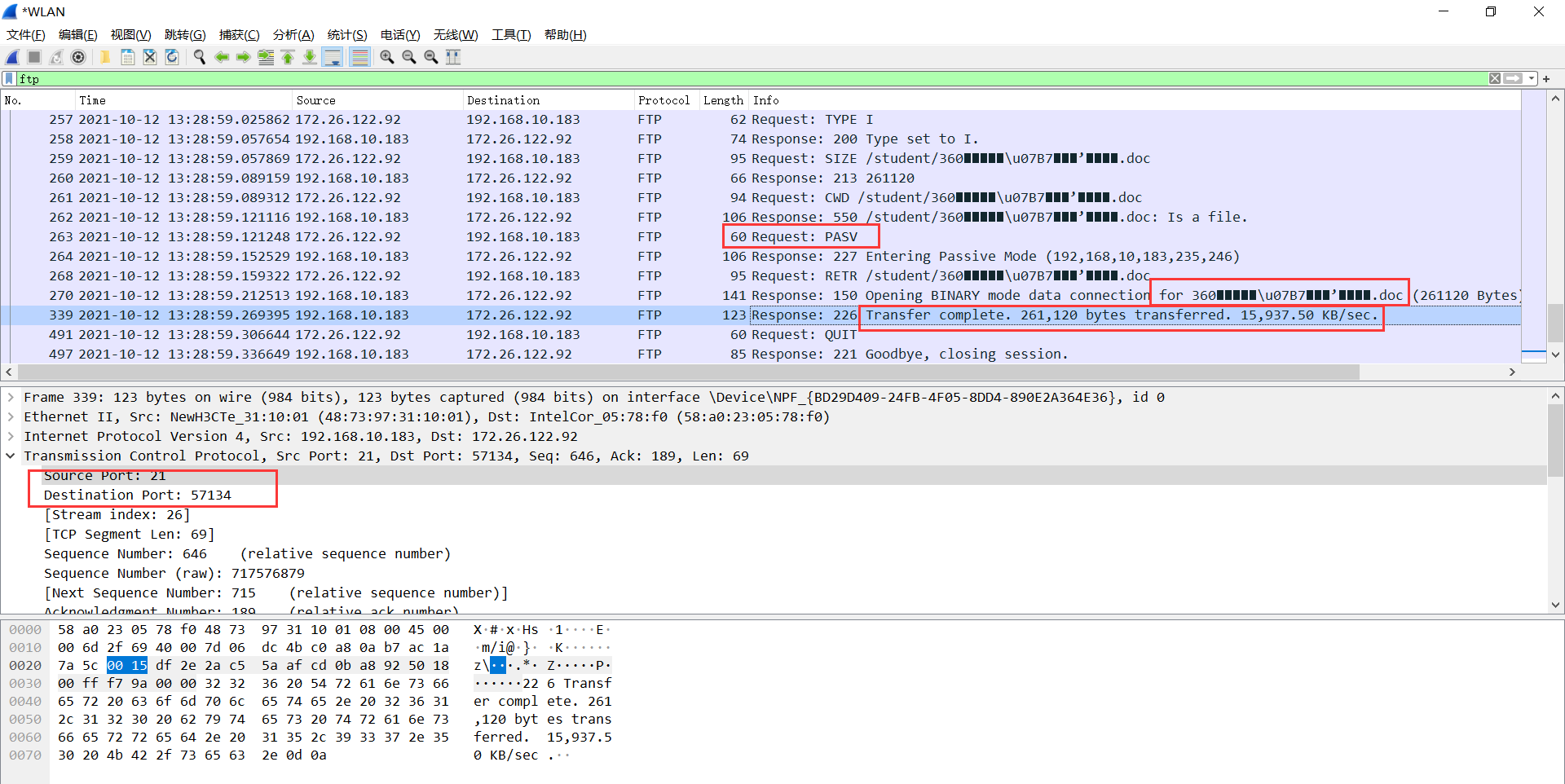
**注意：**可以利用Windows自带的FTP组件或下载FTP软件，建立FTP服务器，并进行配置，并访问分析FTP协议

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。

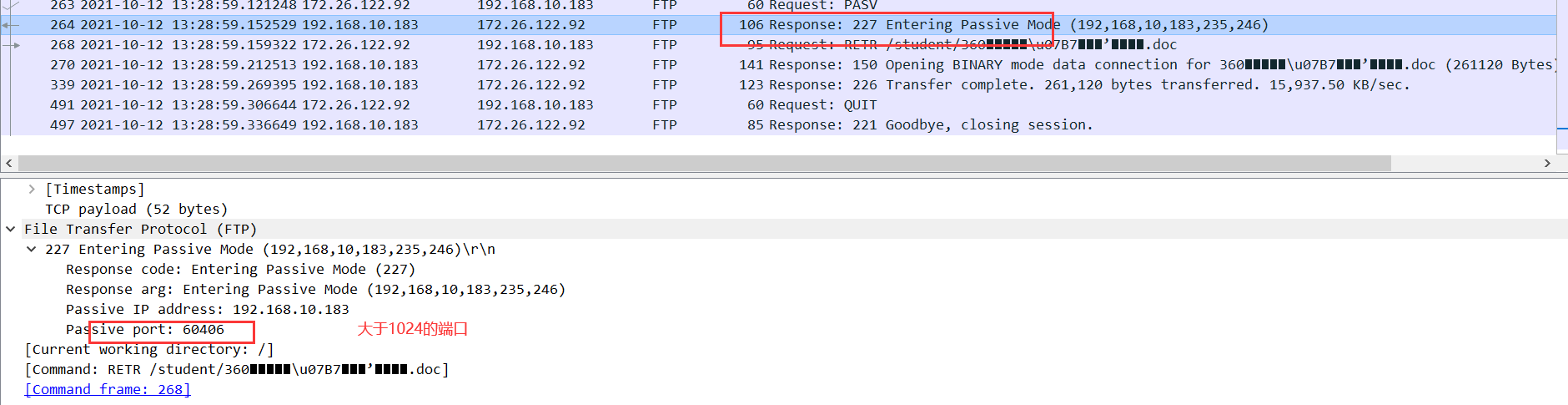




从中ftp下载了一个文件，可以看到如下图：

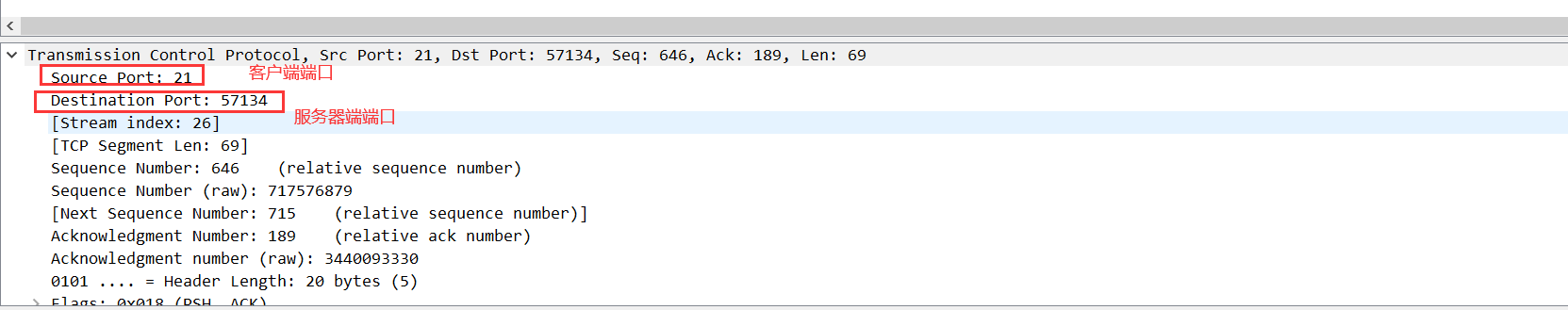


这里的是PASV被动模式抓包



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





查阅资料可知：

ftp的port和pasv模式最主要区别就是数据端口连接方式不同，ftp port模式只要开启服务器的21和20端口，而ftp pasv需要开启服务器大于1024所有tcp端口和21端口。从网络安全的角度来看的话似乎ftp port模式更安全，而ftp pasv更不安全，那么为什么RFC要在ftp port基础再制定一个ftp pasv模式呢？其实RFC制定ftp pasv模式的主要目的是为了数据传输安全角度出发的，因为ftp port使用固定20端口进行传输数据，那么作为黑客很容使用sniffer等探嗅器抓取ftp数据，这样一来通过ftp port模式传输数据很容易被黑客窃取，因此使用pasv方式来架设ftp server是最安全绝佳方案。

如果作为一个有经验的网络管理员就会发现使用ftp pasv方式会给网络安全很大隐患，那就是ftp pasv需要开启服务器tcp大于1024所有端口，这样对服务器的安全保护是非常不利的。

## 四、 SMTP和POP协议分析

基于Web的邮件或客户端的邮件软件（如outlook）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。

**注意：**

1、可以利用windows自带组件安装SMTP服务器，并配置邮件服务器，并访问。

2、 什么情况下可以捕获POP或SMTP数据包

回答：

POP：POP协议支持“离线”邮件处理。其具体过程是：邮件发送到服务器上，电子邮件客户端调用邮件客户机程序以连接服务器，并下载所有未阅读的电子邮件。这种离线访问模式是一种存储转发服务，将邮件从邮件服务器端送到个人终端机器上，一般是PC机或 MAC。一旦邮件发送到 PC 机或MAC上，邮件服务器上的邮件将会被删除。但POP3邮件服务器大都可以“只下载邮件，服务器端并不删除”，也就是改进的POP3协议。

也就是说在客户端进行收取邮件时可以捕获到POP数据包。

SMTP：SMTP是一种提供可靠且有效的电子邮件传输的协议。SMTP是建立在FTP文件传输服务上的一种邮件服务，主要用于系统之间的邮件信息传递，并提供有关来信的通知。SMTP独立于特定的传输子系统，且只需要可靠有序的数据流信道支持，SMTP的重要特性之一是其能跨越网络传输邮件，即“SMTP邮件中继”。使用SMTP，可实现相同网络处理进程之间的邮件传输，也可通过中继器或网关实现某处理进程与其他网络之间的邮件传输。

即在发送邮件时可以捕获到SMTP数据包。

接下来通过安装Foxmail，利用其进行收发软件，并通过Wireshark进行SMTP和POP3协议分析。

#### SMTP协议：

1. 安装好Foxmail后配置好Foxmail，本次实验为方便使用，我登陆了QQ邮箱和163邮箱的账户进行收发邮件。

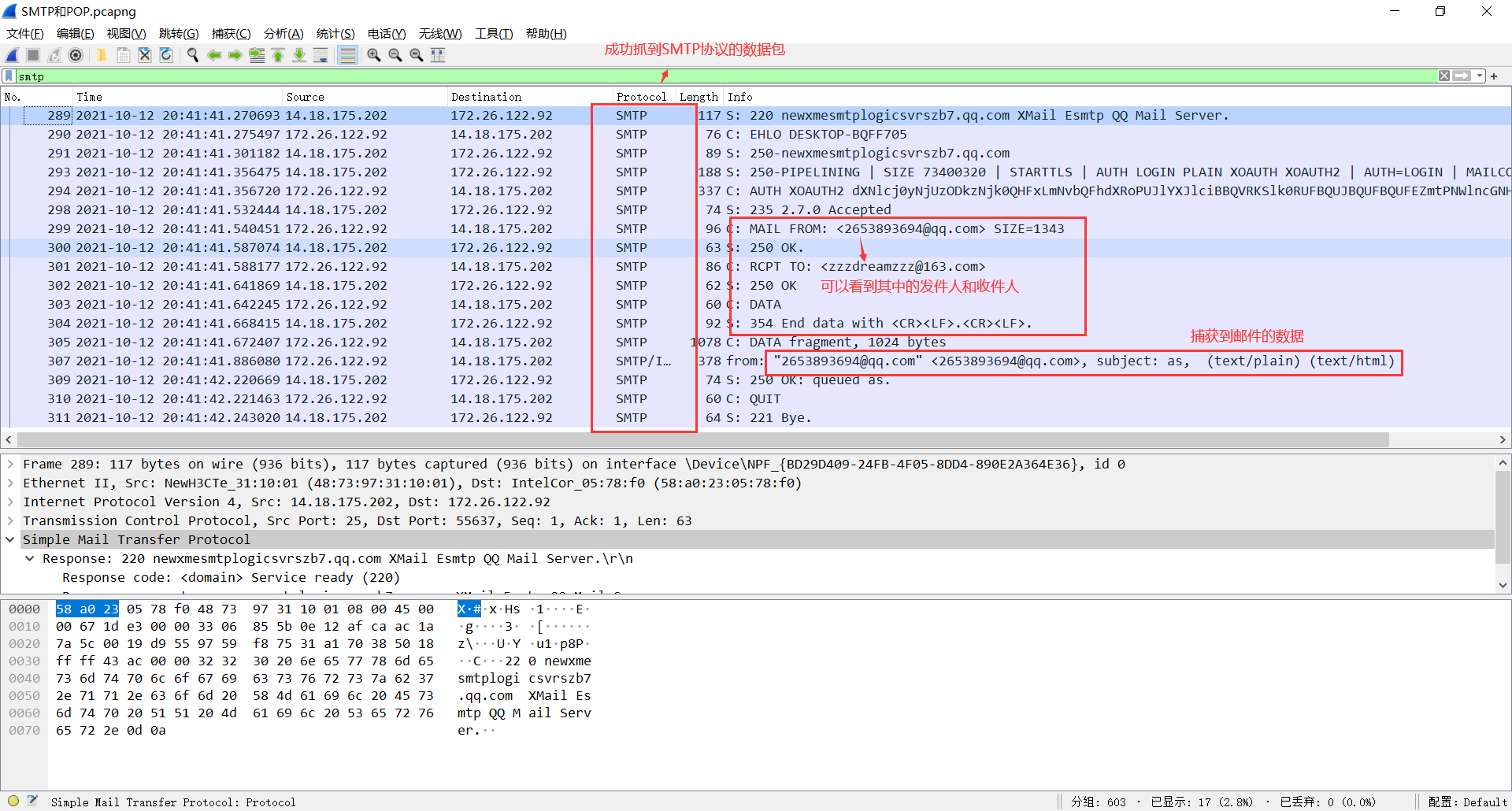


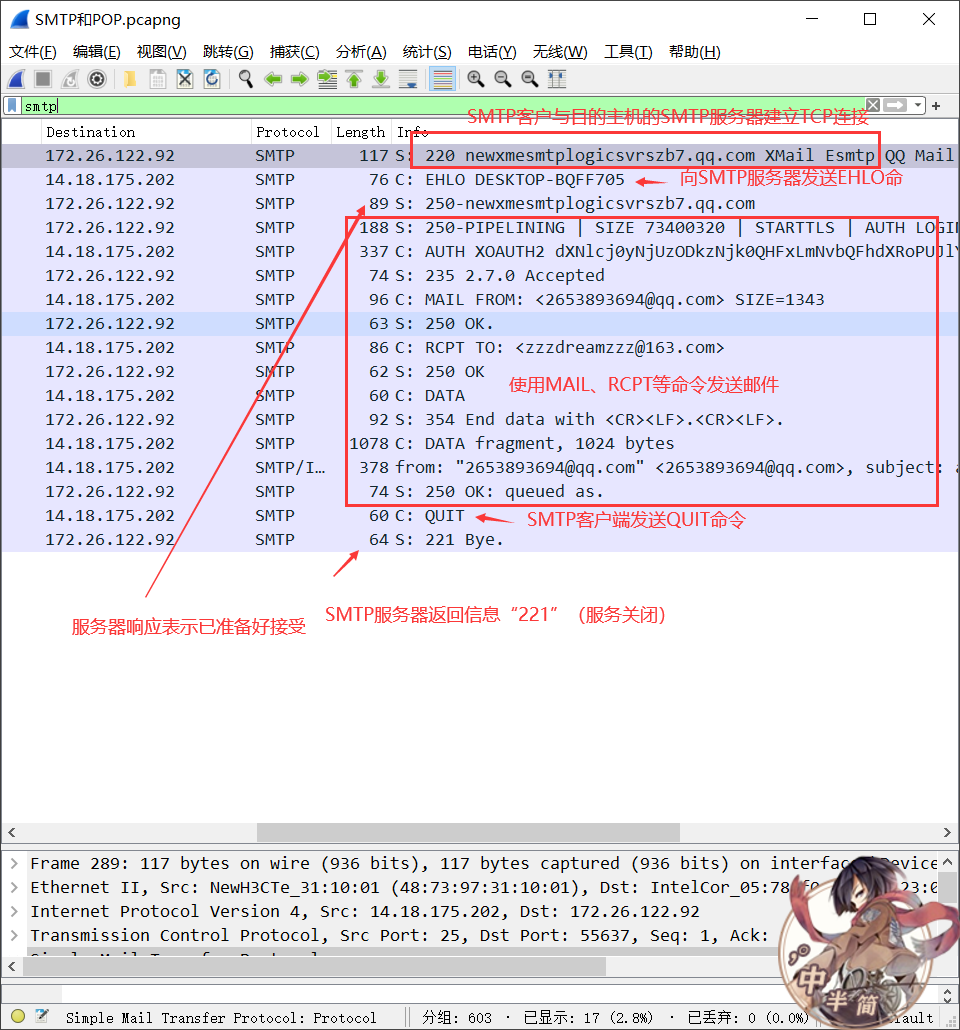
1. 配置成功后，利用Wireshark进行抓包

首先把在账户中SSL加密取消掉，这样才能让Wireshark捕获到SMTP和POP3协议

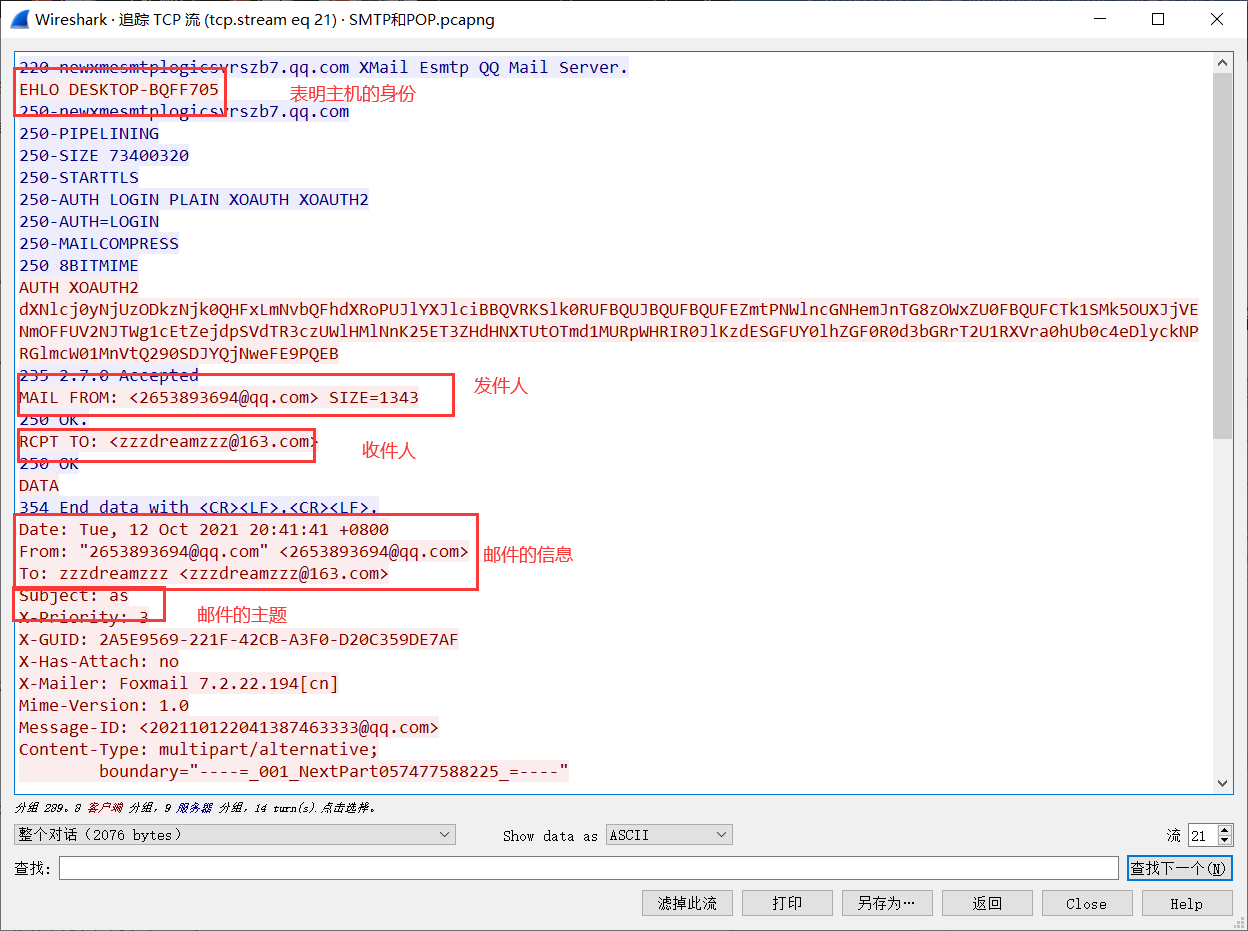


先写一封邮件，打开Wireshark进行捕获后再把邮件发送，发送完成后，这样就能捕获到SMTP协议，成功抓包。



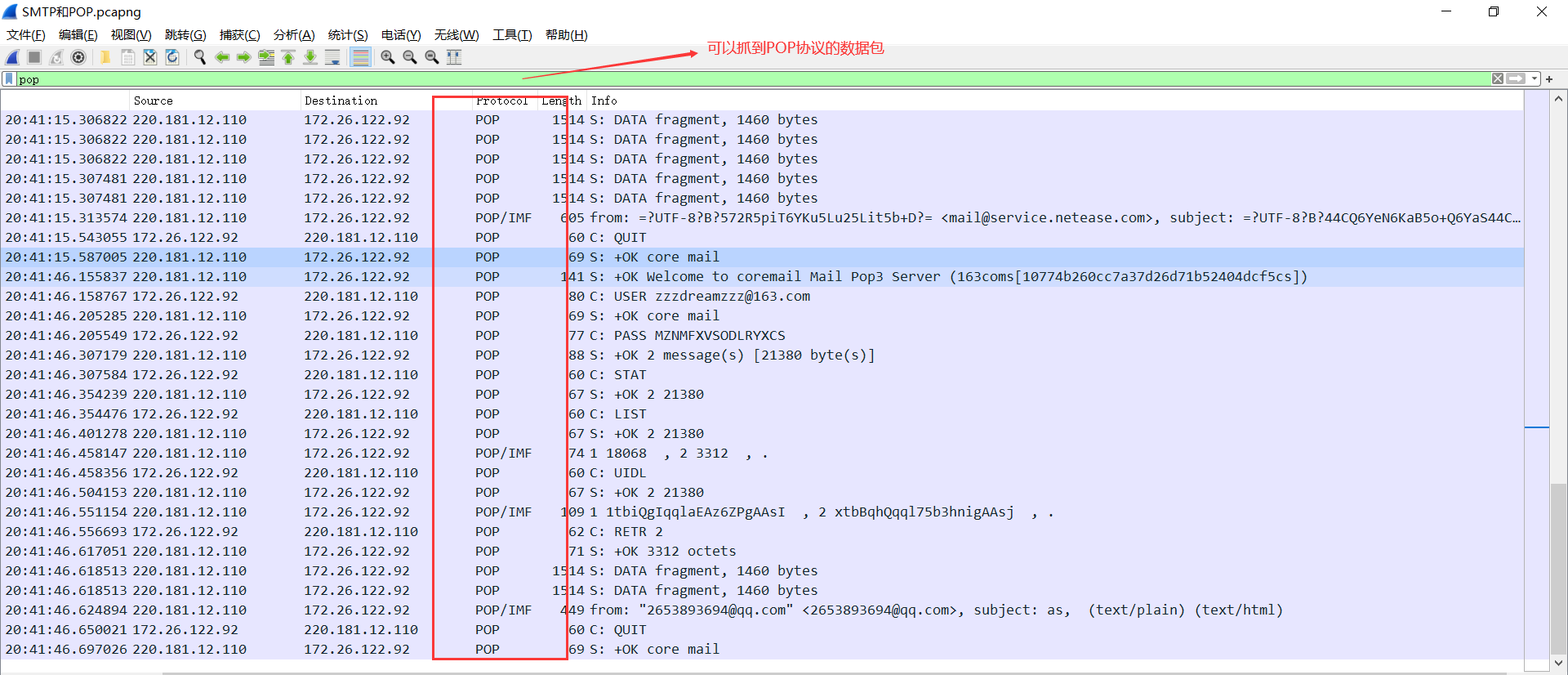


跟踪TCP流查看信息

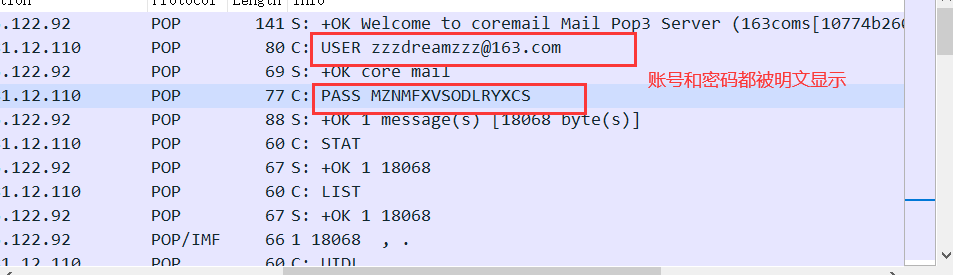


#### POP3协议：

1. .打开wireshark抓包并用Foxmail向163邮箱发一封邮件，发送成功后，在Foxmail页面点收取邮件，然后停止抓包



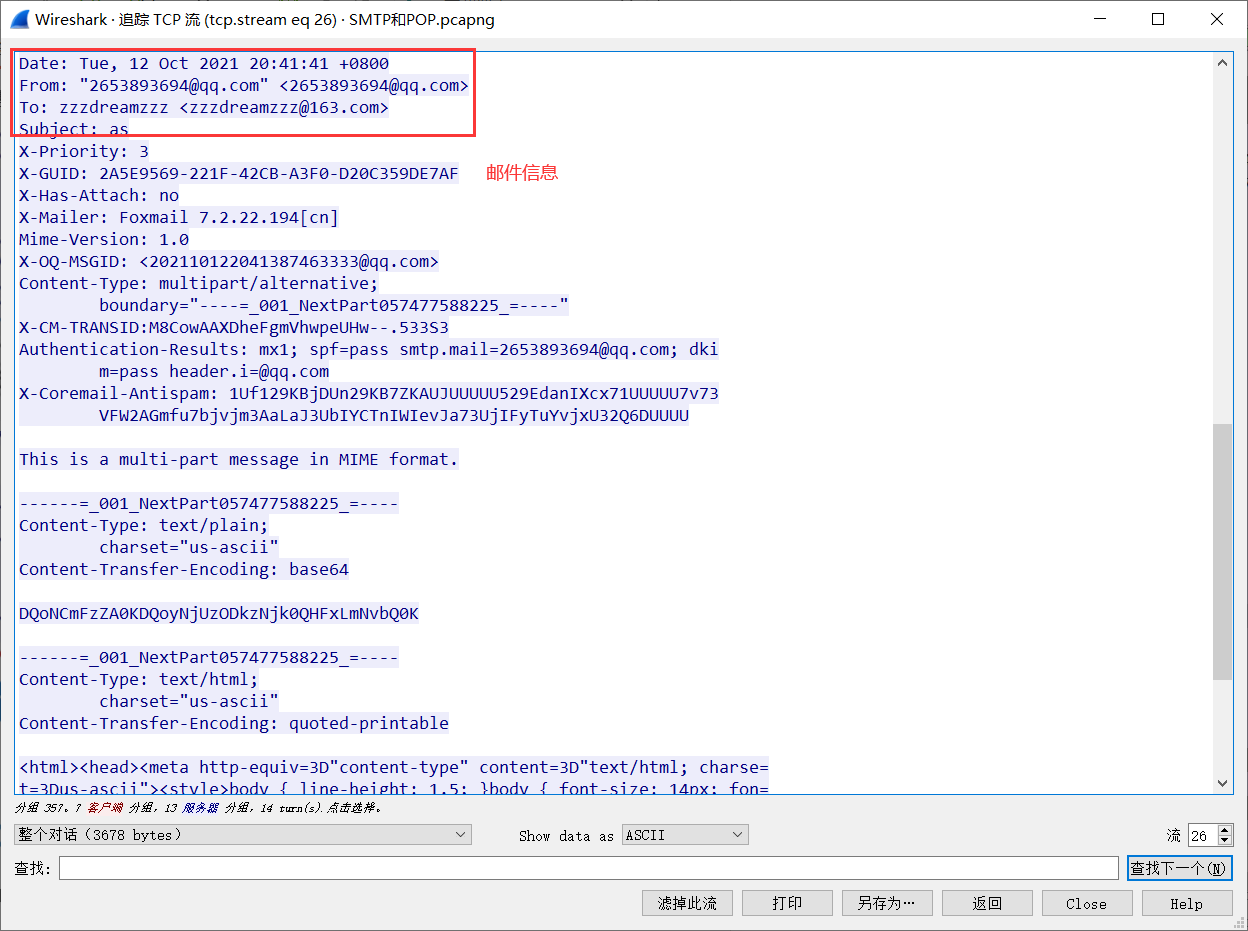
2.POP3协议分析





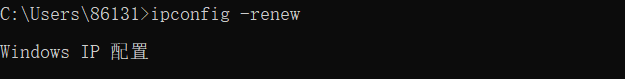
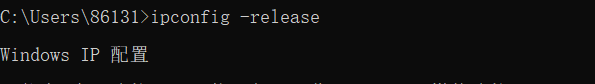
追踪TCP流查查看到收发人的账号等信息

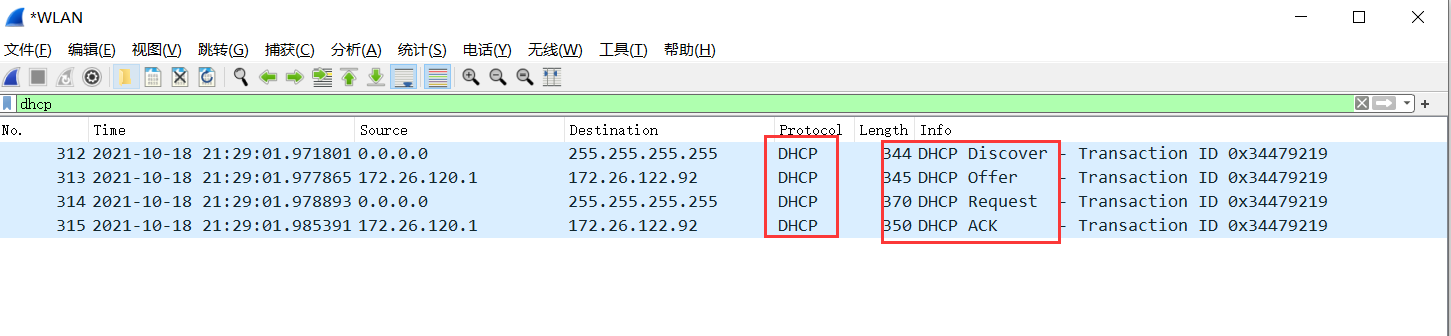




## 补充：DHCP协议捕捉

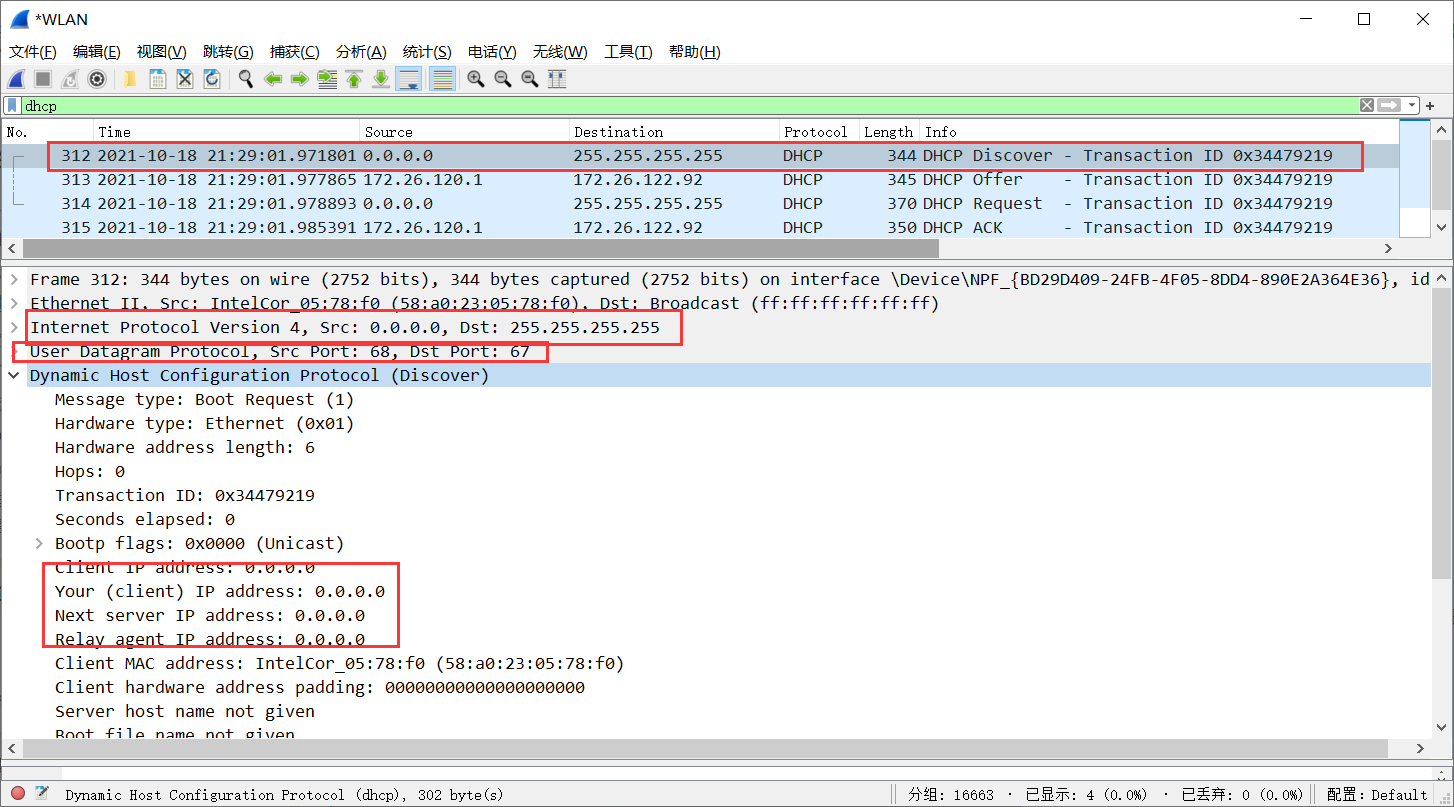
打开wireshark，然后在命令行中输入：ipconfig -release，再输入ipconfig -renew





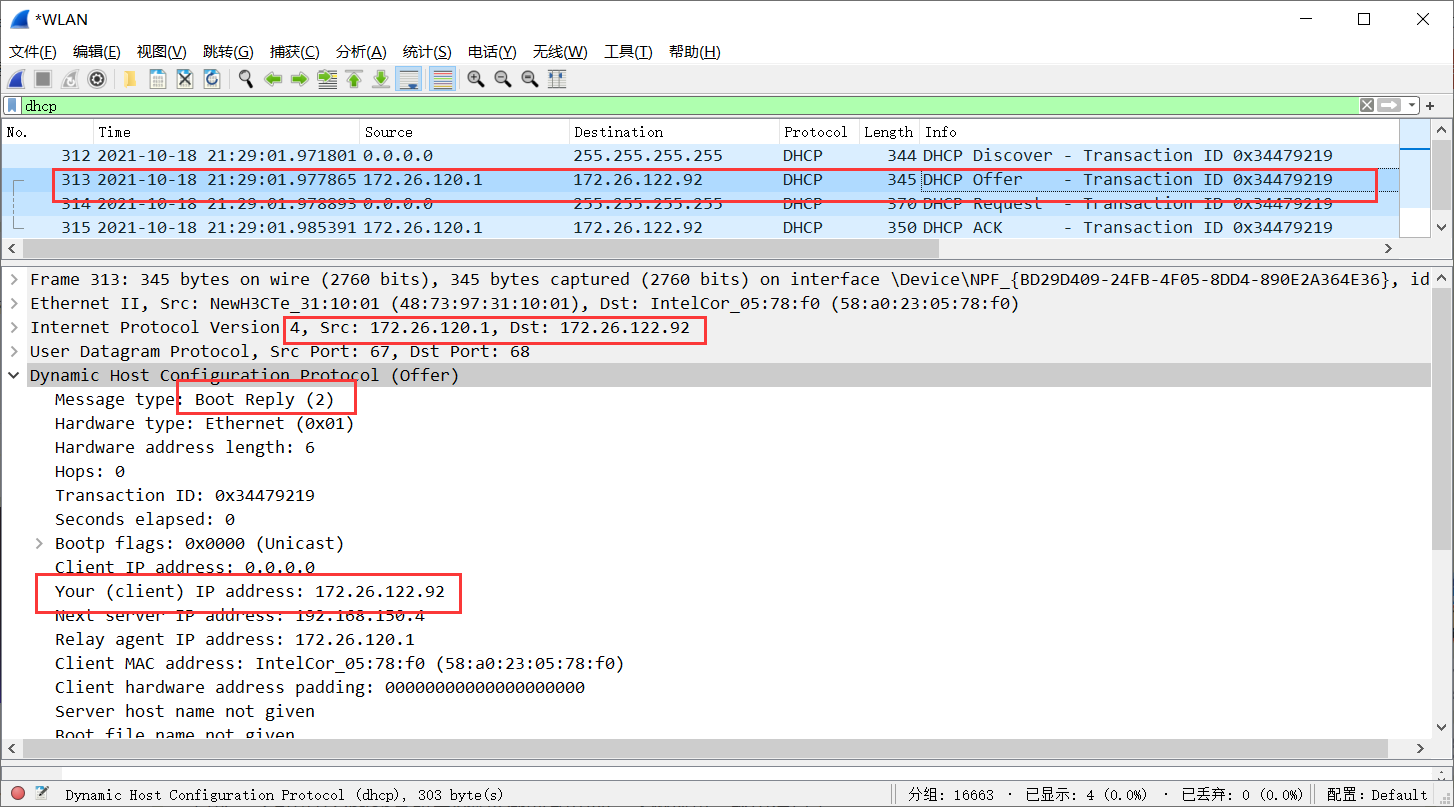
wireshark捕获了4个DHCP包，分别是discover、offer、request、ack。   
这刚好就对应着主机向DHCP服务器请求分配IP的4个过程：DHCP服务器发现、DHCP服务器提供、DHCP请求、DHCP ACK。   
接下来详细看看每个报文的具体内容：

### Discover：DHCP服务器发现

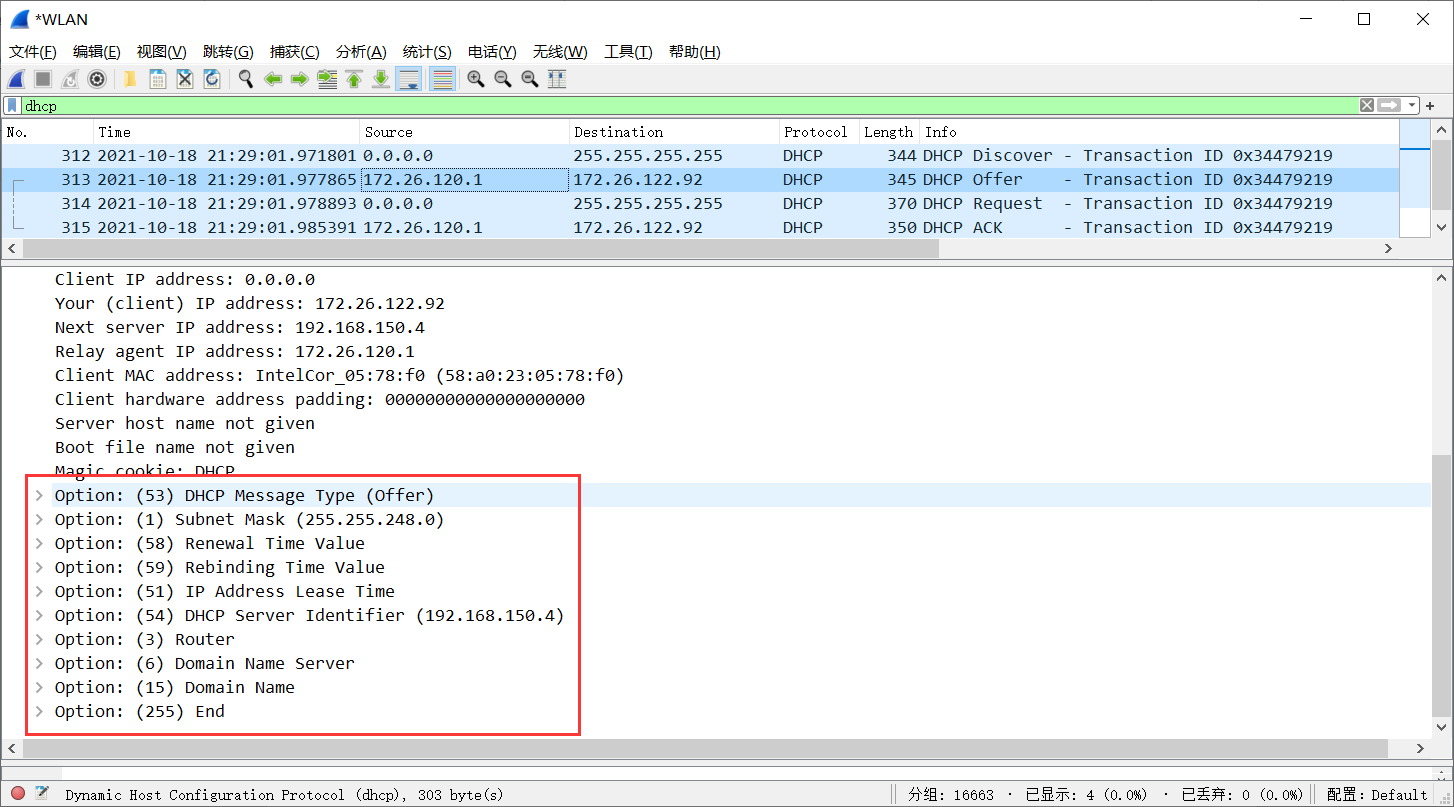


DHCP包的传输层协议是UDP，端口号是67。因为此时主机不知道自己的IP地址，也不知道DHCP服务器的地址，所以使用源地址0.0.0.0和广播目的地址255.255.255.255。

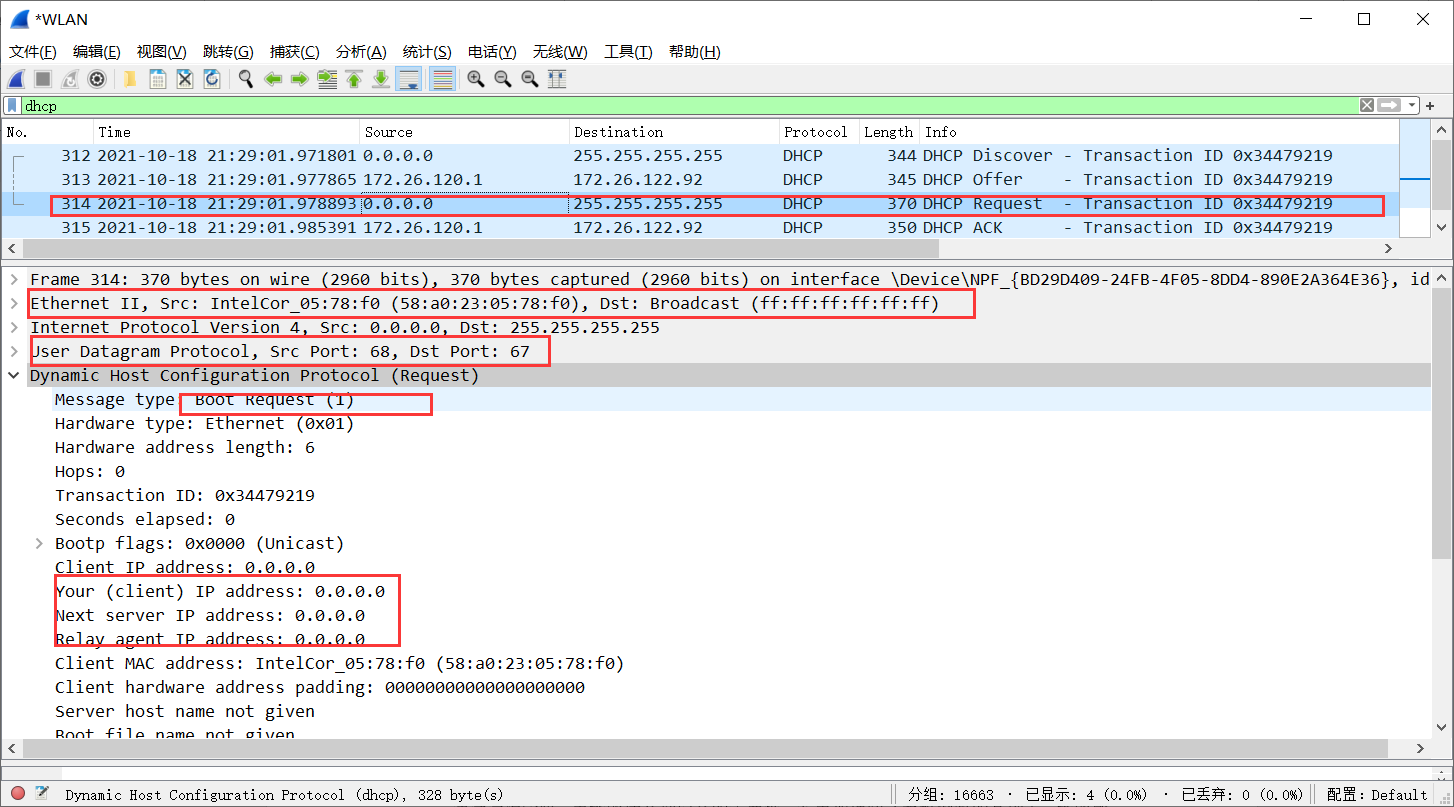
### Offer：DHCP服务器提供



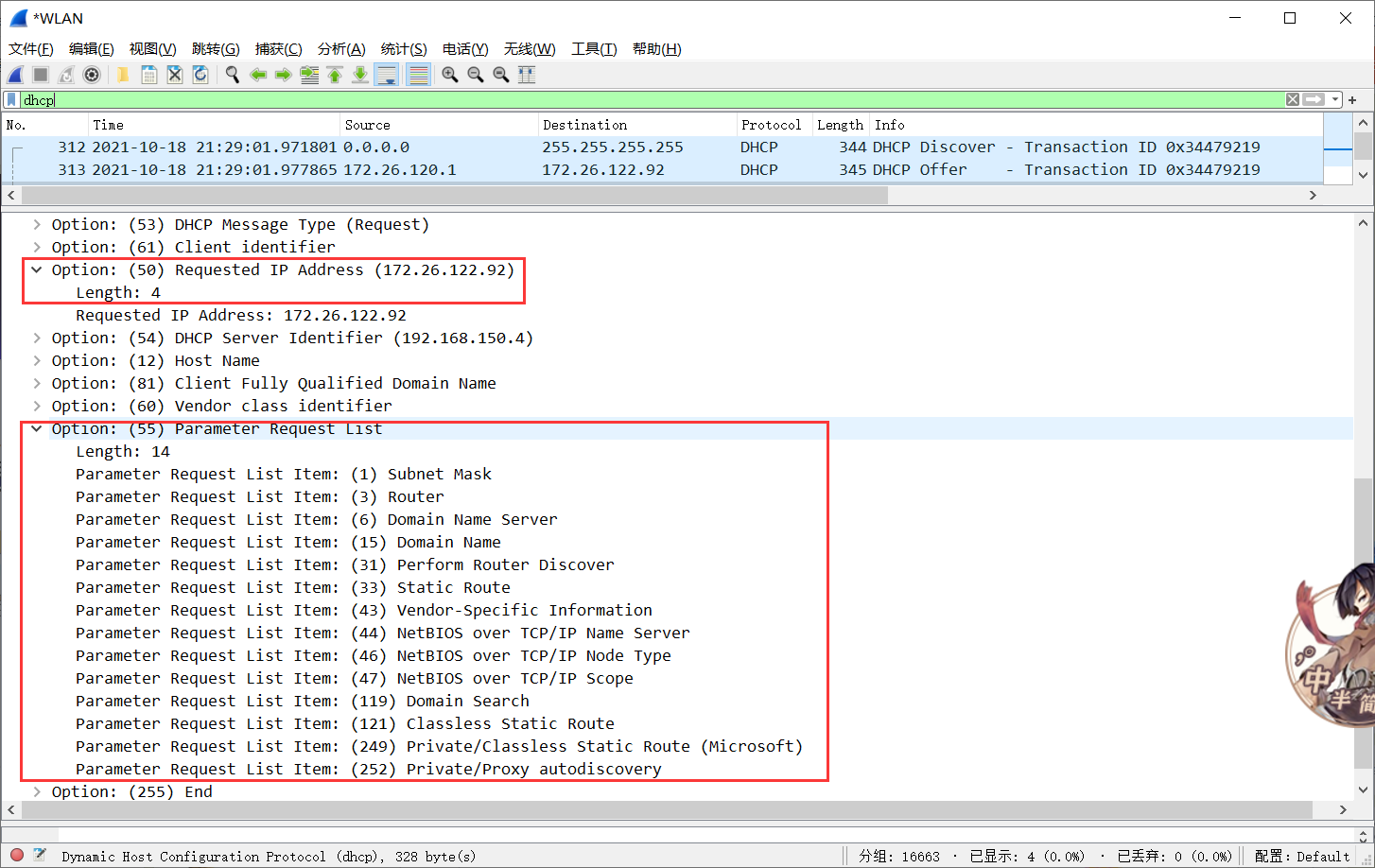
DHCP服务器收到一个DHCP发现报文后，用一个DHCP提供报文进行响应。从包中可以看出服务器IP地址为192.168.1.1，分配给主机的IP地址是192.168.1.103。该报文的事务ID是0x8100beb0，和上一个发现报文的事务ID是一样的。另外，还可以从Option字段里获得IP地址租用期、子网掩码、路由信息等。



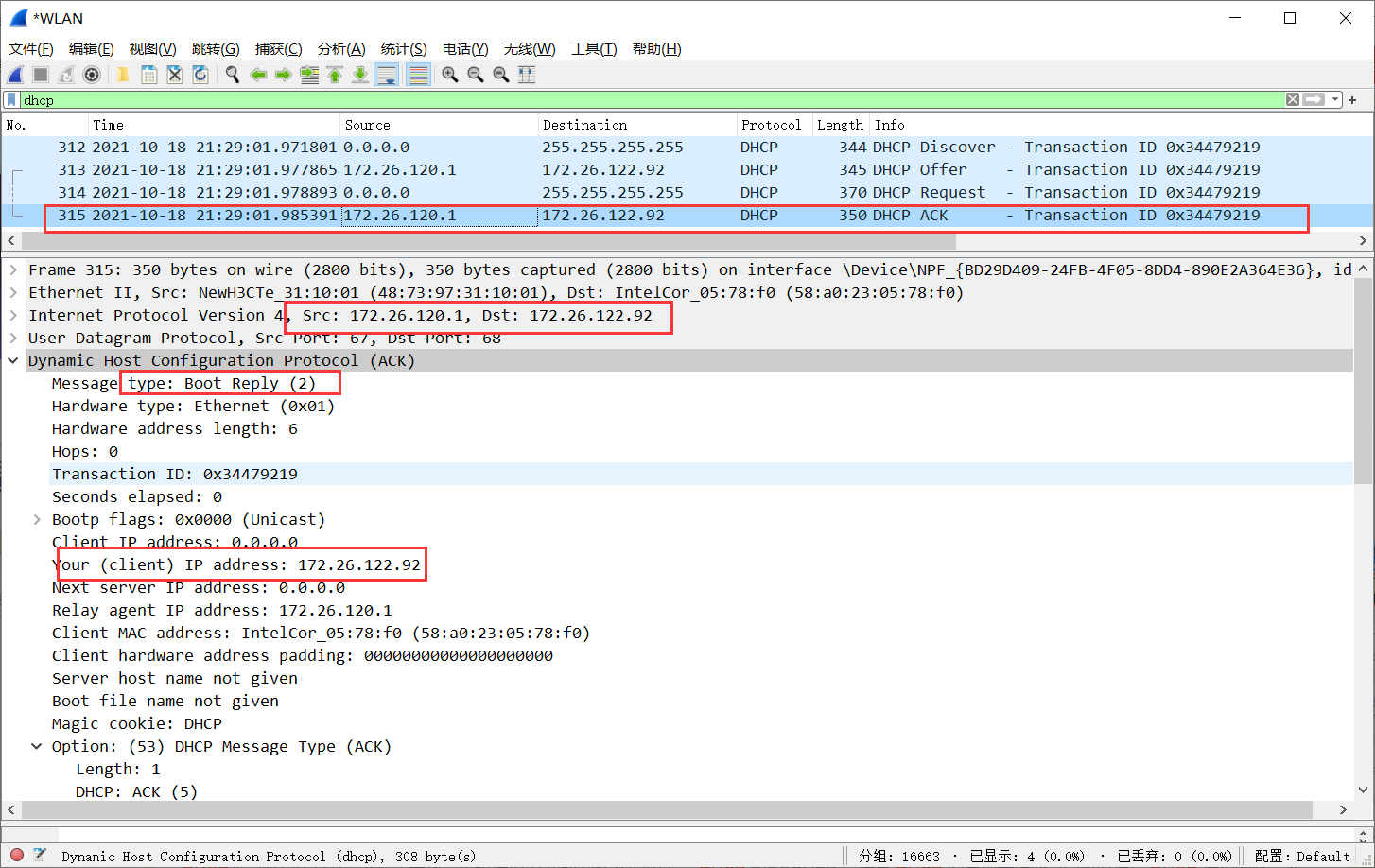
### Request：DHCP请求



主机收到Offer报文后，用一个DHCP请求报文进行响应，此时和DHCP发现报文一样，都是使用源地址0.0.0.0和广播目的地址255.255.255.255。并且重新选择一个新的事务ID以及回显配置参数。如请求的IP地址等。



### ACK：DHCP ACK应答



最后，服务器用DHCP ACK报文对DHCP请求报文进行响应，证实所要求的参数。，整个IP请求分配过程就完成了，客户端能够在租用期内使用DHCP分配的IP地址。

## （六）实验小结

通过本次实验，理解了WWW、DNS服务、FTP服务、SMTP的作用和原理，能够使用Wireshark分析HTTP、FTP、DNS、STMP和POP协议的工作过程。也通过补充，知道了DHCP协议的工作过程。

当然，一开始对于各种应用层的协议也只是停留在课本的内容上，虽然说知道其一二，但是没有在开始实验前，也只是对其有内容上的一知半解，在实验中通过对Wireshark的使用，捕获数据包，然后跟随实验提示和要求分析数据包，我对协议格式和工作原理有了更深的理解，对其各种协议的格式以及工作原理能够有更好的认识，更加明白了网络工作的过程，掌握各种应用层中的协议知识，更好地理解到了计算机网络的工作原理，在理解协议的细节后能够对网络有了底层思维上的理解，像是IP地址的获取有通过使用命令查看到学习WIFi的IP获取过程，又有域名服务解析出的IP地址是给予机器看的，而域名是给予我们用户看的这一类通俗而又形象的知识。

而最后，通过这次实验，其实对于学习信息安全本身来说，更加重要的是更能够体会到安全的重要性，在更加理解计算机网络的基础上，能够感受到Web安全，网络安全的重要性，知道计网的知识是进行安全学习的道路中必须掌握的，这对之后无论是学习还是工作来说，都掌握了必要的知识，同时实际上，也开拓了自己的视野，包括在底层网络运行上，和安全道路上，也在一定程度上，增大了自己学习的兴趣，了解到计网中协议的工作过程不是枯燥的，而是形象有趣的。

**暨南大学本科实验报告专用纸(附页)**