**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 实验四 实验项目类型 实验地点

学生姓名 李芷靖 学号 2019051114

学院 智能科学与工程学院 系 专业 信息安全

实验时间 2021年 10 月 12 日 上午～ 月 日 午 温度 ℃湿度

## 【实验目的】

* + 理解WWW 、 DNS服务、FTP服务、SMTP的作用和原理；
  + **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。**

## 【实验内容】

* + 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；
  + 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）

## 【实验设备】

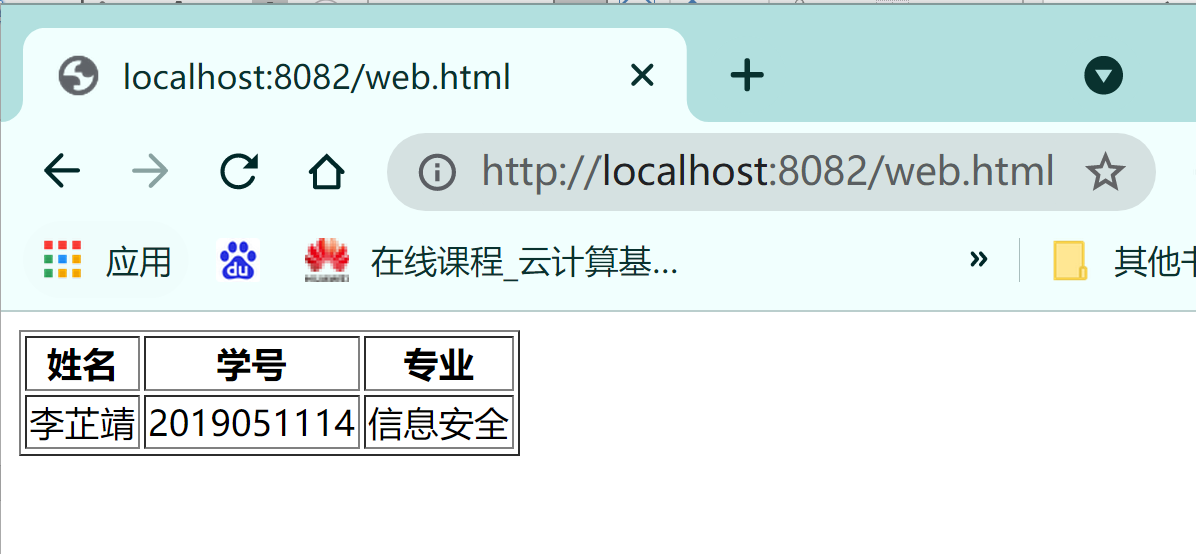
局部网环境，计算机若干台。本实验不分组，独立完成。

## 【实验步骤】

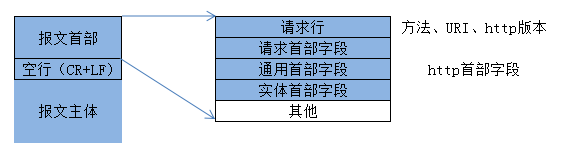
**一、HTTP协议分析**

1. 配置www站点

利用windows自带组件IIS建立并配置WWW站点。

1. 报文首部



经查阅资料得知，报文首部中包含了请求行以及一些首部字段，请求和响应中都存在，并涵盖http报文相关的内容。

其中几种

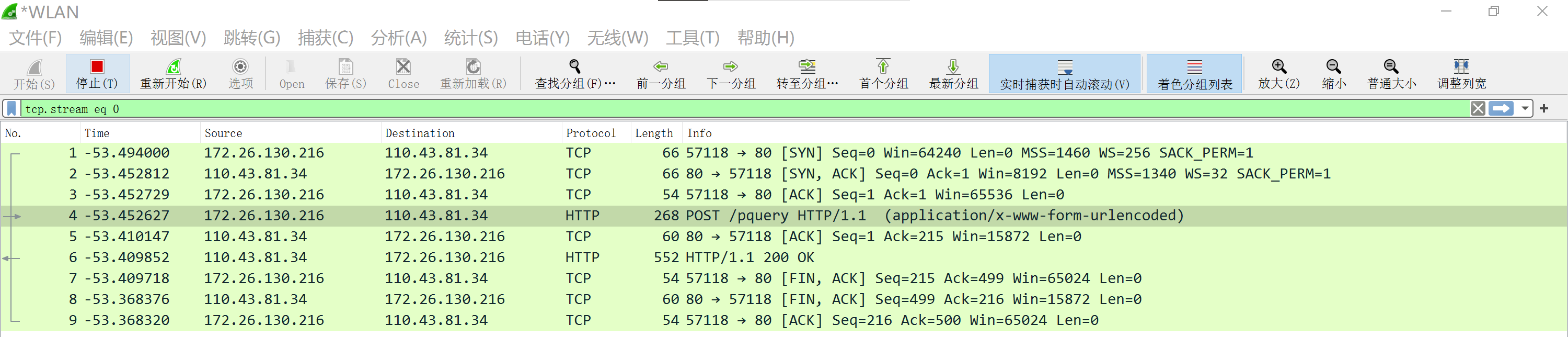
通用首部字段 定义：请求和响应报文都会使用的首部。

请求首部字段 定义：从客户端向服务器发送请求报文时使用的首部，补充了请求的附加内容、客户端信息、相应内容相关优先级信息。

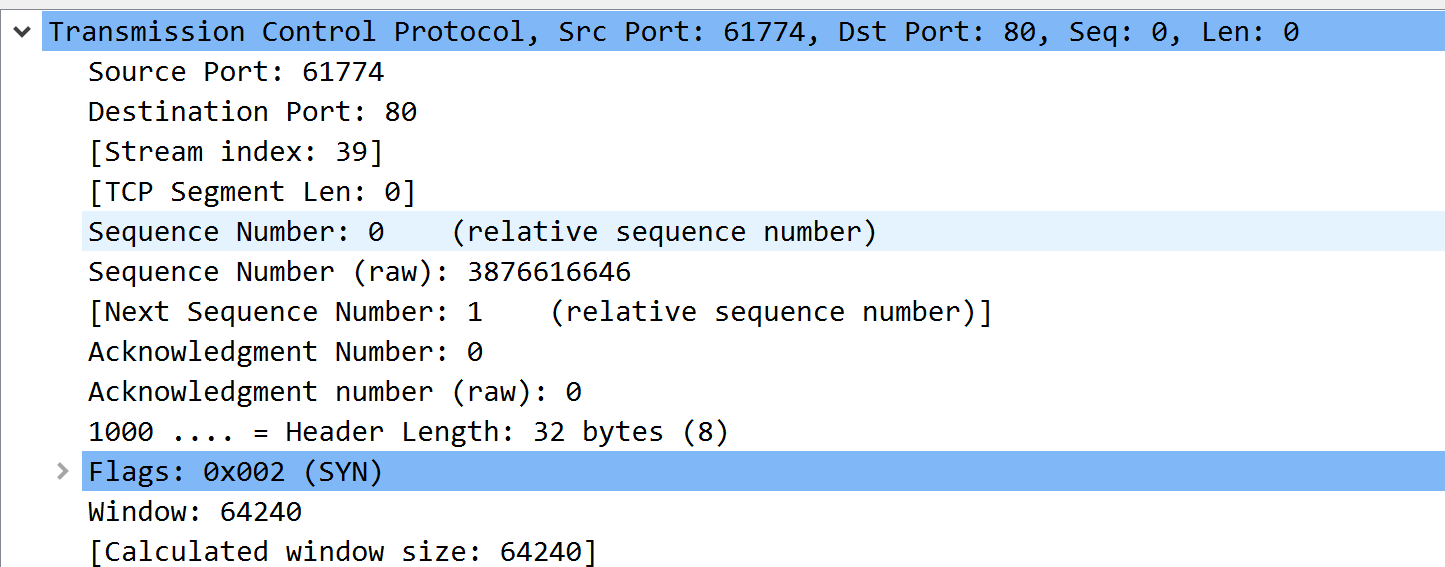
响应首部字段 定义：从服务器向客户端返回响应报文时使用的首部。补充了资源内容更新时间等与实体有关的信息。

实体首部字段 定义：针对请求报文和响应报文的实体部分使用的首部，补充了资源内容更新时间与实体有关的信息。

1. 抓包分析HTTP工作过程

* 建立TCP连接

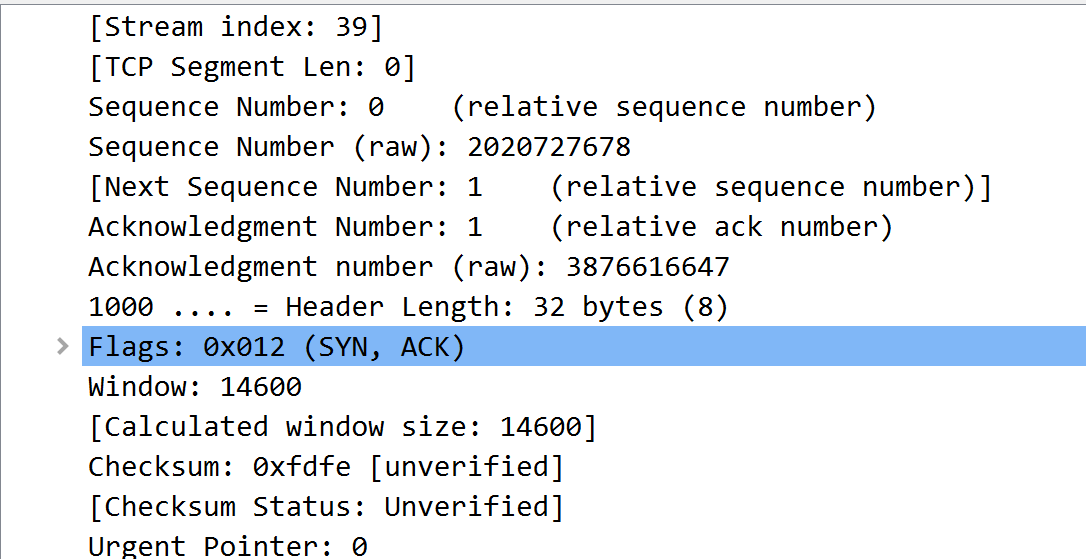
第一次连接：发送端发送一个带SYN标志的数据包给对方



Sequence Number序号和Acknowledgment Number确认号都为0；

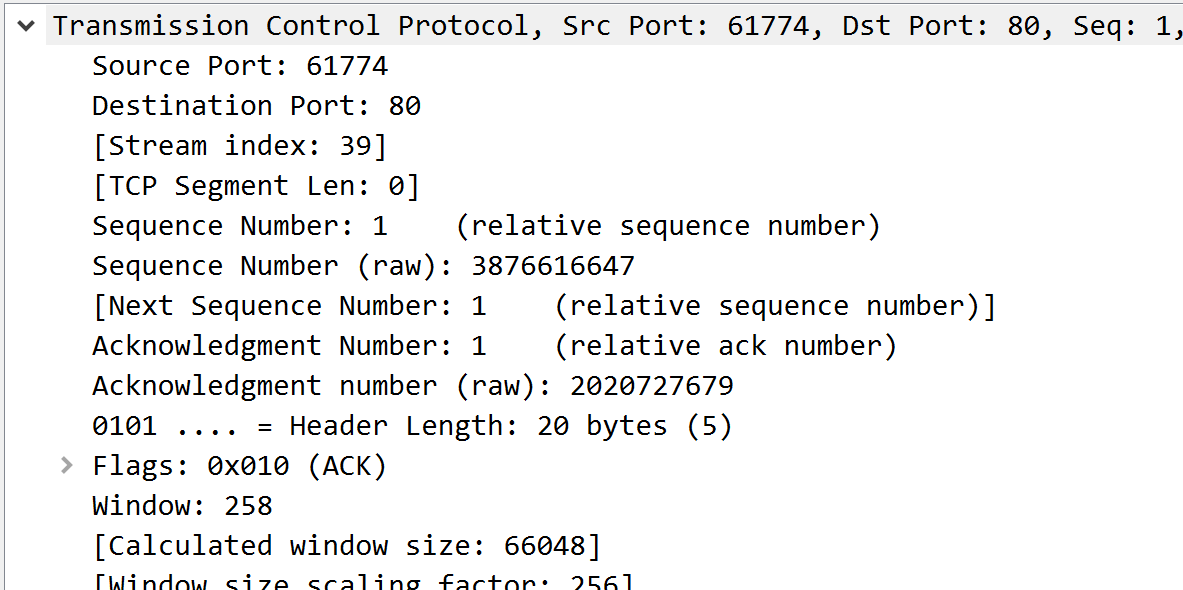
代表客户端请求建立连接。

第二次连接，接收端回传一个带有SYN和ACK标志的数据包以示传达确认信息



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I S N加1即0+1=1

第三次连接发送端再回传一个带ACK标志的数据包，代表“握手结束”



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,

* 发起HTTP请求（HTTP请求报文）

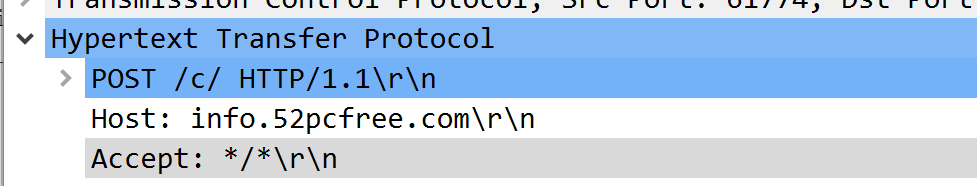
HTTP超文本传输协议，由请求和响应构成。

请求报文分为三部分:首行,请求头,请求体.

首行包括:请求类型,URL,HTTP版本.

请求头部保存一些键值对的属性.

请求体保存具体内容,一般为POST类型的参数.



请求行由请求方法字段、URL字段和HTTP协议版本字段3个字段组成，它们用空格分隔。例如，POST/c/HTTP/1.1\r\n

HTTP协议的请求方法有GET、POST、HEAD、PUT、DELETE、OPTIONS、TRACE、CONNECT。

本次实验中使用的是POST请求方法使用POST方法可以允许客户端给服务器提供信息较多。POST方法将请求参 数封装在HTTP请求数据中，以名称/值的形式出现，可以传输大量数据，这样POST方式对传送的数据大小没有限制，而且也不会显示在URL中。POST方式请求行中不包含数据字符串，这些数据保存在”请求内容”部分，各数据之间也是使用”&”符号隔开。

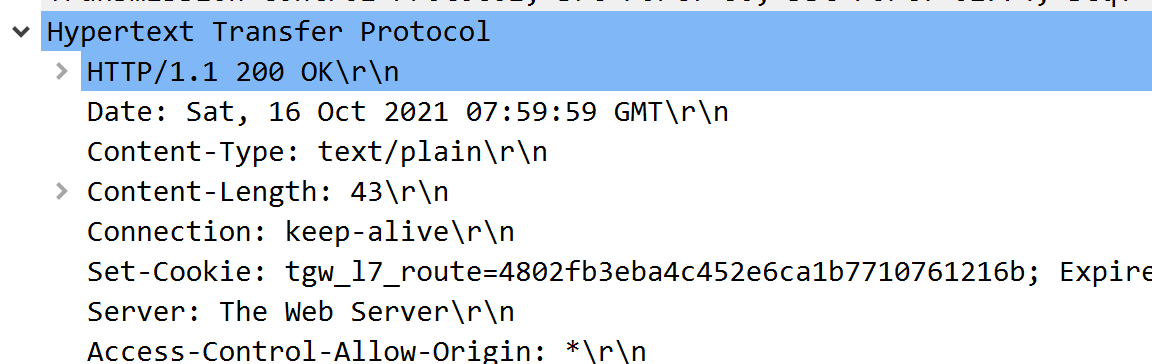
请求头部由关键字/值对组成，每行一对，关键字和值用英文冒号“:”分隔。请求头部通知服务器有关于客户端请求的信息，典型的请求头有：

请求头部User-Agent：产生请求的浏览器类型。Accept：客户端可识别的内容类型列表。Host：请求的主机名，允许多个域名同处一个IP地址，即虚拟主机。

* HTTP响应（响应报文）

响应报文也由三部分组成，首行，响应头，响应体。

首行分为报文协议及版本，响应码及状态描述



分析首行中的响应码和状态表示

状态行格式：HTTP-Version Status-Code Reason-Phrase CRLF

其中，HTTP-Version表示服务器HTTP协议的版本；Status-Code表示服务器发回的响应状态代码；Reason-Phrase表示状态代码的文本描述。状态代码由三位数字组成，第一个数字定义了响应的类别，且有五种可能取值。

1xx：指示信息--表示请求已接收，继续处理。

2xx：成功--表示请求已被成功接收、理解、接受。

3xx：重定向--要完成请求必须进行更进一步的操作。

4xx：客户端错误--请求有语法错误或请求无法实现。

5xx：服务器端错误--服务器未能实现合法的请求。

常见状态代码、状态描述的说明如下。

200 OK：客户端请求成功。

400 Bad Request：客户端请求有语法错误，不能被服务器所理解。

401 Unauthorized：请求未经授权，这个状态代码必须和WWW-Authenticate报头域一起使用。

403 Forbidden：服务器收到请求，但是拒绝提供服务。

404 Not Found：请求资源不存在，举个例子：输入了错误的URL。

500 Internal Server Error：服务器发生不可预期的错误。

503 Server Unavailable：服务器当前不能处理客户端的请求，一段时间后可能恢复正常。

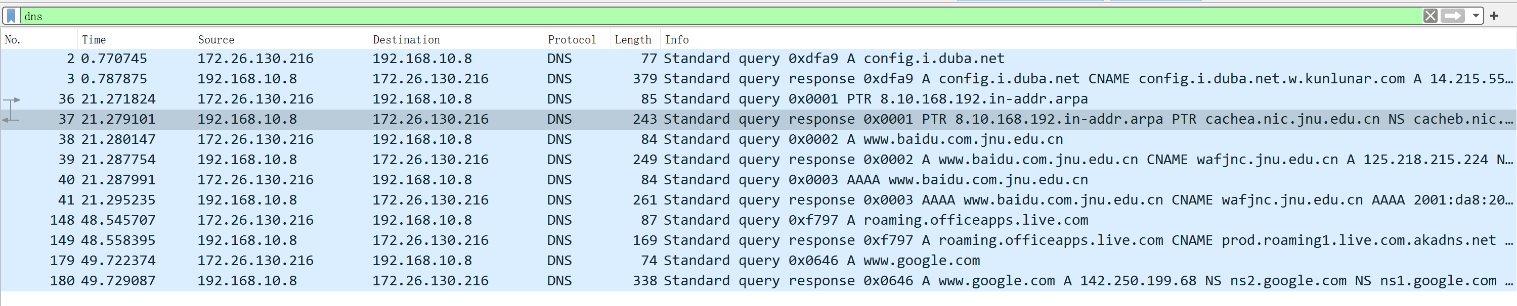
如实验结果中显示：HTTP/1.1 200 OK\r\n。

1. **DNS协议分析**

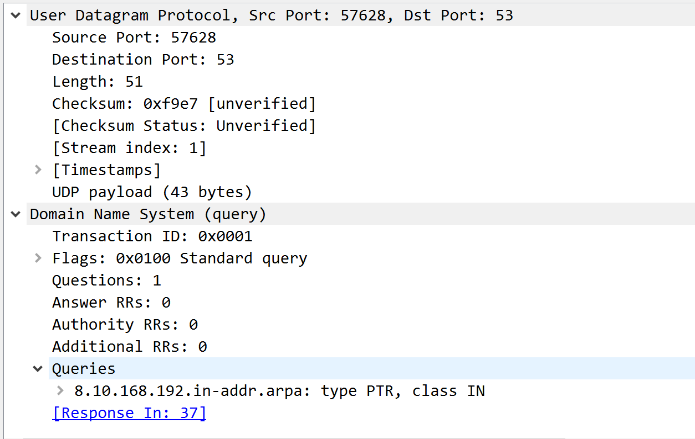
通过域名访问某网站，用wireshark捕获DNS数据包，并分析DNS工作过程和DNS格式。DNS（Domain Name System，域名系统）, DNS通过域名和IP地址相互映射的一个分布式数据库，使易记的域名替代了枯燥的IP地址。在因特网中向主机提供域名解析服务的机器即为DNS服务器。DNS是基于IP协议中的UDP协议，端口号为53。目前，DNS分布式查询方式一般采用递归或递归迭代相结合的方法获得域名和对应的IP。

1. 首先通过nslookup命令进行DNS查询工作：

这里可以看到，我的本地DNS服务器为cachea.nic.jnu.edu.cn，IP地址为192.168.10.8。我所搜索的百度（www.baidu.com）真实域名为wafjnc,jnu.edu.cn（但这一域名地址无法ping通，也不能直接访问），IP地址有125.218.215.224和119.75.218.77，别名仍为www.baidu.com.jnu.edu.cn。

1. 通过wireshark获取DNS数据包

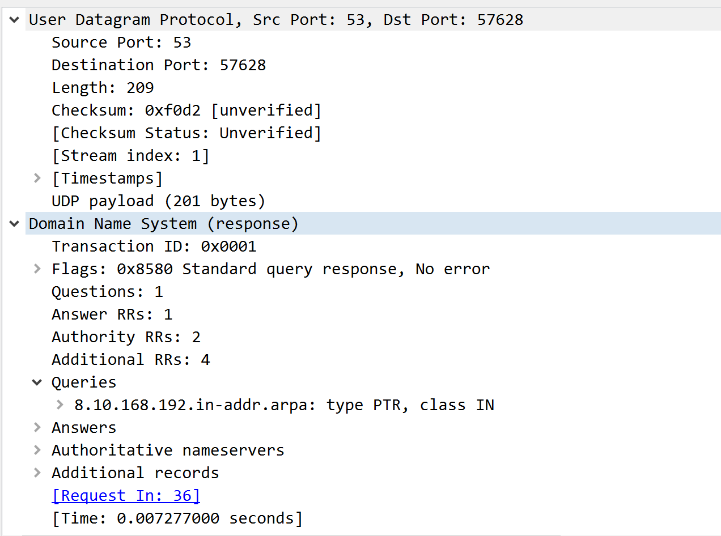
* 向本地DNS服务器发送了一个请求帧

源端口：57628，我电脑上的端口号；

目的端口：domain(53)，DNS默认端口号；

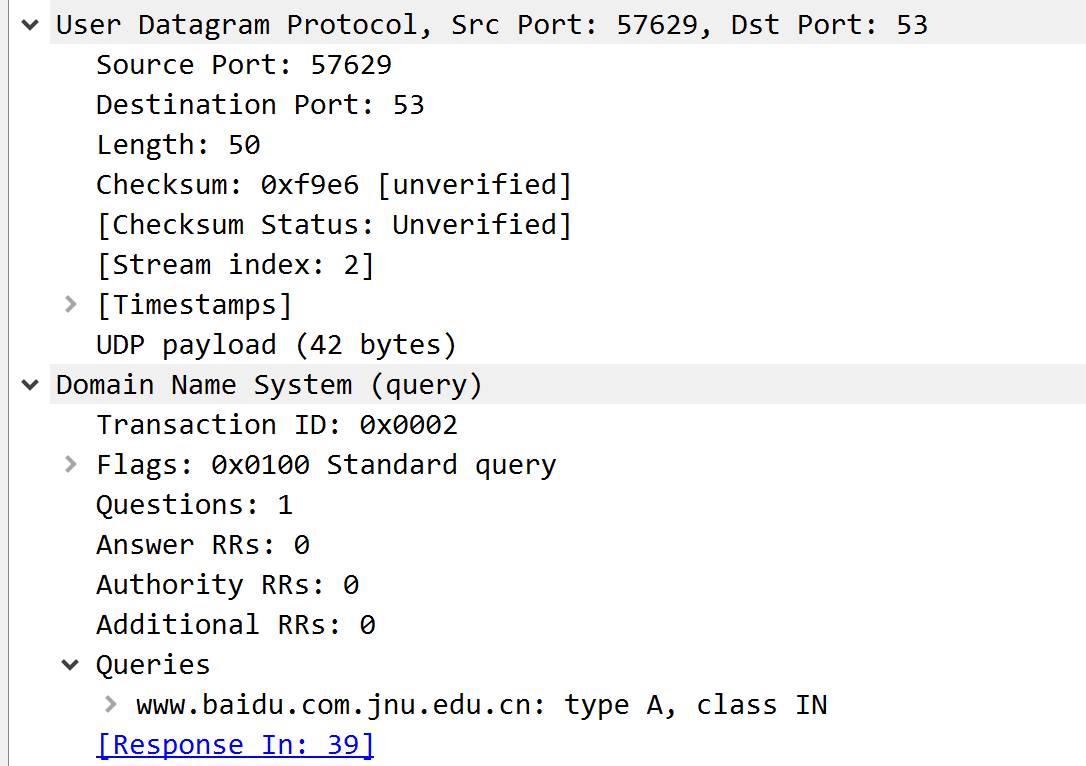
请求：8.10.168.192.in-addr.arpa：type PTR，class IN，反向域名解析，请求获得本地DNS服务器域名；

* 本地DNS服务器返回一个响应帧



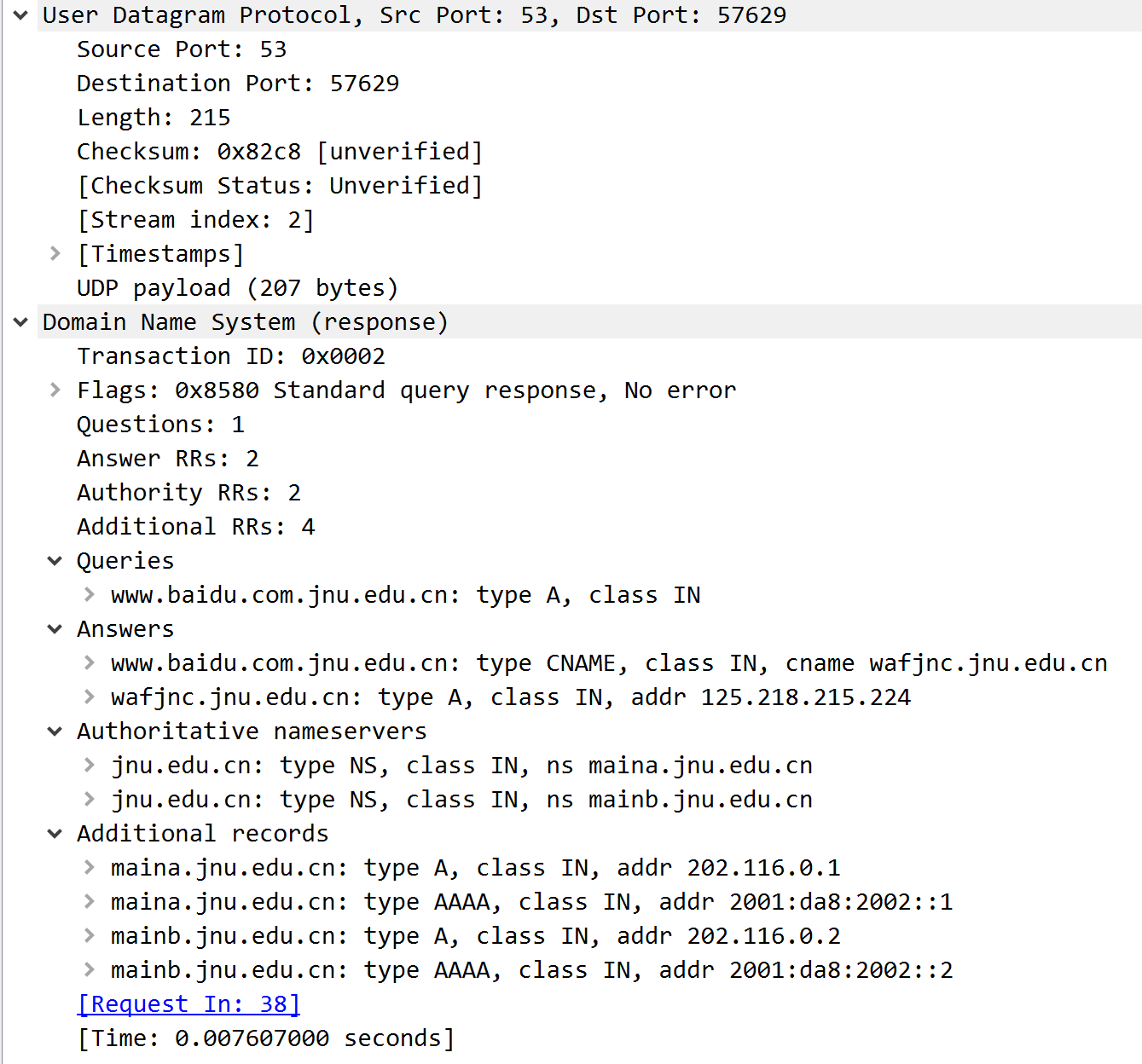
Answers一行数据即显示了响应帧的回复内容，本地DNS服务器域名为：cachea.nic.jnu.edu.cn。

* 向服务器请求获得www.baidu.com的IP地址



请求：请求获得www.baidu.com的主机IP地址；

* 本地DNS服务器返回一个响应帧



得到了我想要的IP地址

名称: wafjnc.jnu.edu.cn

Addresses:

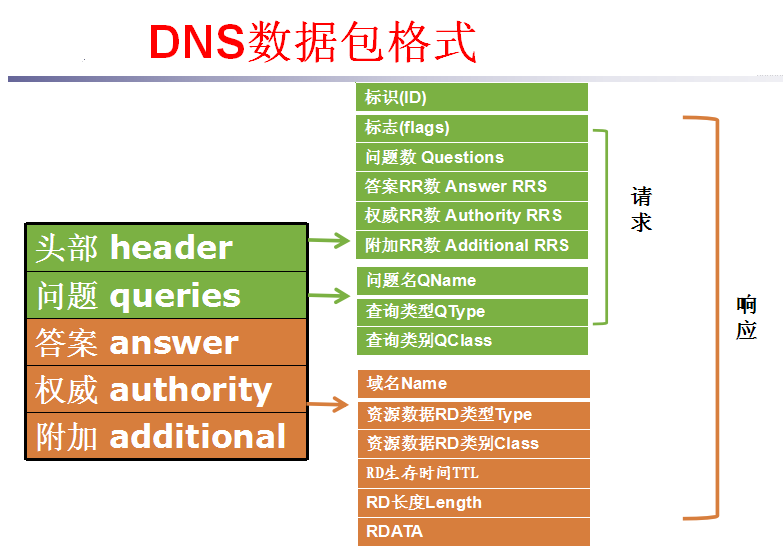
2001:da8:2002:215::224

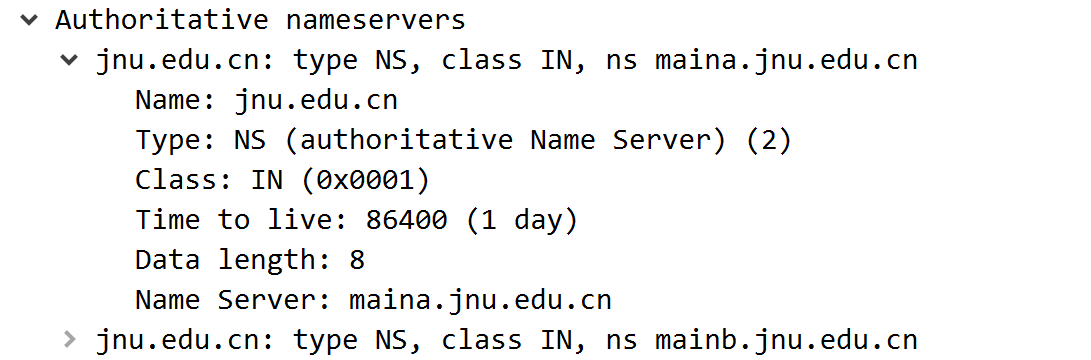
125.218.215.224

Aliases:

[www.baidu.com.jnu.edu.cn](http://www.baidu.com.jnu.edu.cn)

1. 附DNS数据包格式（细节见课件）





**注意：**

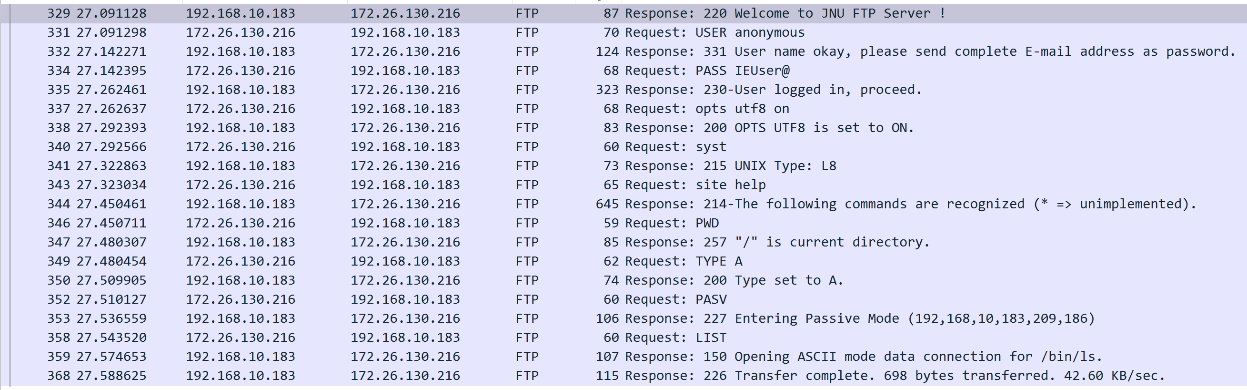
1. 有时候可能捕获不到DNS解析过程，为什么？要仔细分析。

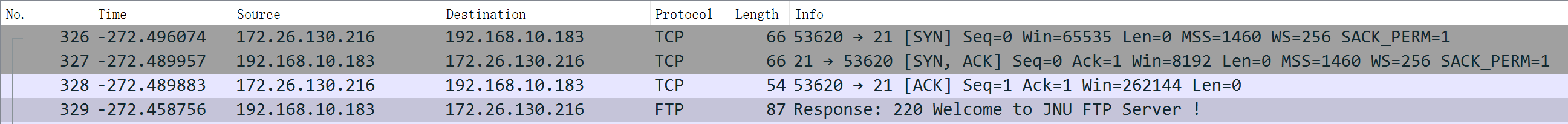
**三、FTP协议分析**

**在实验中尝试了使用IIS建立ftp服务器，成功创建，但是在用户使用登陆上出现了问题。在创建用户和组时每一次电脑界面都会自动闪退。**

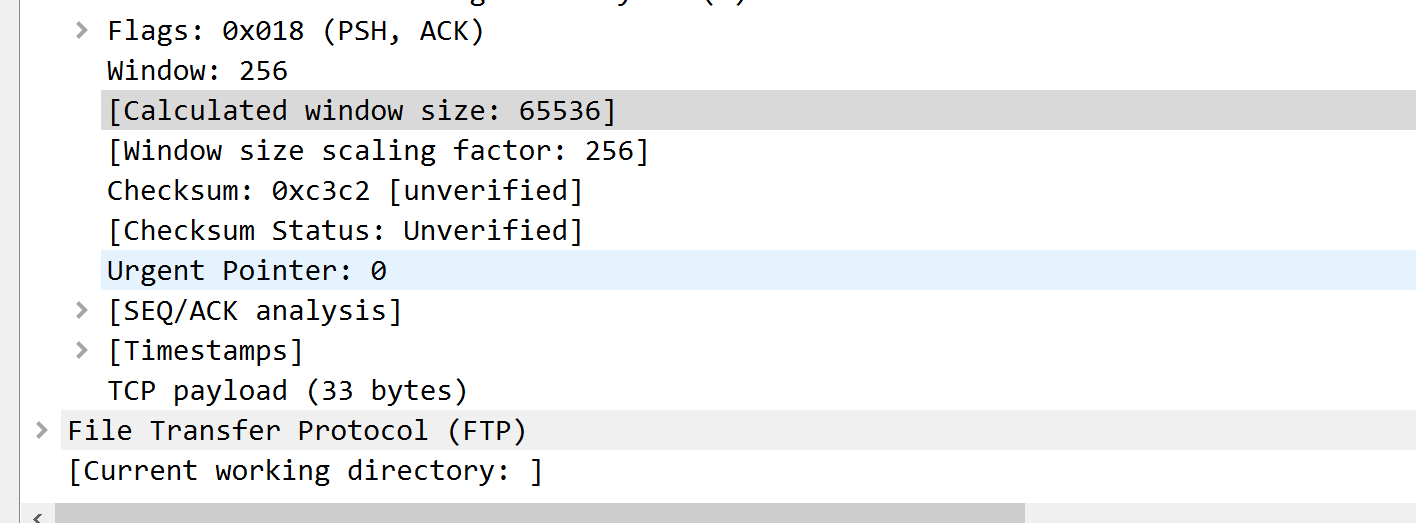
**1.**访问FTP服务器。如<ftp://ftp.jnu.edu.cn>先分析连接登录过程

使用wireshark对访问ftp进行数据包抓取。

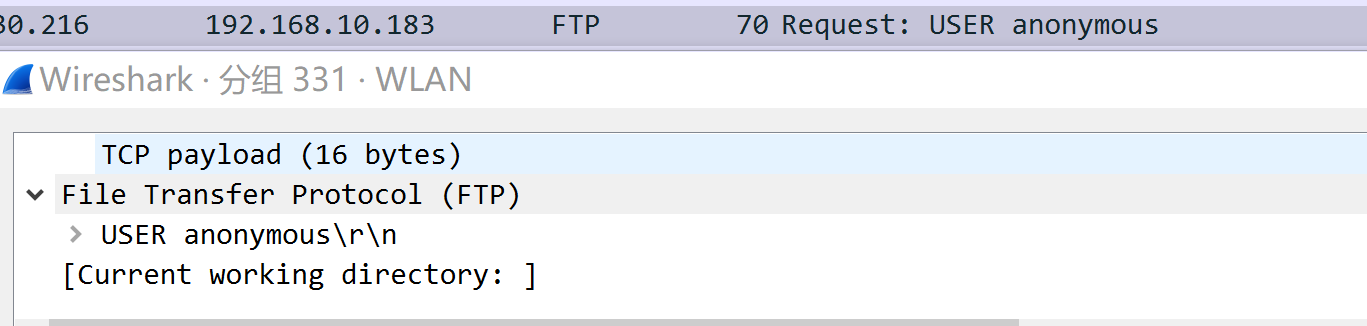


ftp是基于tcp的，所以也需要tcp三次握手，才能建立连接。

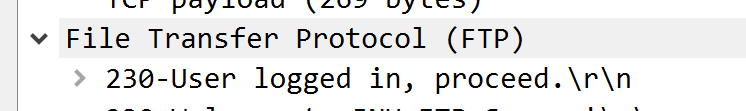
连接成功后，向ftp服务器发送请求，发送自己的相关信息，后面的状态码220表示服务准备就绪。



FTP中进行登录操作，显示是匿名用户登录。



登陆响应，显示成功登录



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。

据查阅资料得知，FTP有两种工作模式，主动模式和被动模式，有两个端口，数据端口和控制端口。控制端口一般为21，而数据端口不一定是20，这和FTP的应用模式有关，如果是主动模式，应该为20，如果为被动模式，由服务器端和客户端协商而定。

PORT(主动)方式的连接过程是：客户端向服务器的FTP端口(默认是21)发送连接请求，服务器接受连接，建立一条命令链路。当需要传送数据时，客户端在命令链路上用PORT命令告诉服务器：“我打开了XXXX端口，你过来连接我”。于是服务器从20端口向客户端的XXXX端口发送连接请求，建立一条数据链路来传送数据。

PASV(被动)方式的连接过程是：客户端向服务器的FTP端口(默认是21)发送连接请求，服务器接受连接，建立一条命令链路。当需要传送数据时，服务器在命令链路上用PASV命令告诉客户端：“我打开了XXXX端口，你过来连接我”。于是客户端向服务器的XXXX端口发送连接请求，建立一条数据链路来传送数据。

**四、 SMTP和POP协议分析**

1. 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。

实验中我选择使用的用户代理是Outlook

* SMTP协议

SMTP(Simple Mail Transfer Protocol)：简易邮件传输通讯协议 SMTP是互联网上的一种通讯协议，主要功能是用在传送电子邮件，当我们通过电子邮件程序，寄E-mil给另外一个人时，必须通过SMTP通讯协议，将邮件送到对方的邮件服务器上，等到对方上网的时候，就可以收到你所寄的信。

* 1. SMTP格式

C：telnet smtp.126.com 25 /\*　以telnet方式连接126邮件服务器　\*/

S：220 126.com Anti-spam GT for Coremail System (126com[071018])　/\* 220为响应数字，其后的为欢迎信息，会应服务器不同而不同\*/

C：HELO smtp.126.com /\* HELO 后用来填写返回域名，但该命令并不检查后面的参数 \*/

Ｓ：250 OK

C: MAIL FROM: bripengandre@126.com /\* 发送者邮箱 \*/

S：250 … ./\* “…”代表省略了一些可读信息 \*/

C：RCPT TO: bripengandre@smail.hust.edu.cn　/\* 接收者邮箱 \*/

S：250 … ./\* “…”代表省略了一些可读信息 \*/

C：DATA /\* 请求发送数据 \*/

S：354 Enter mail, end with "." on a line by itself

C：Enjoy Protocol Studing

C：.

S：250 Message sent

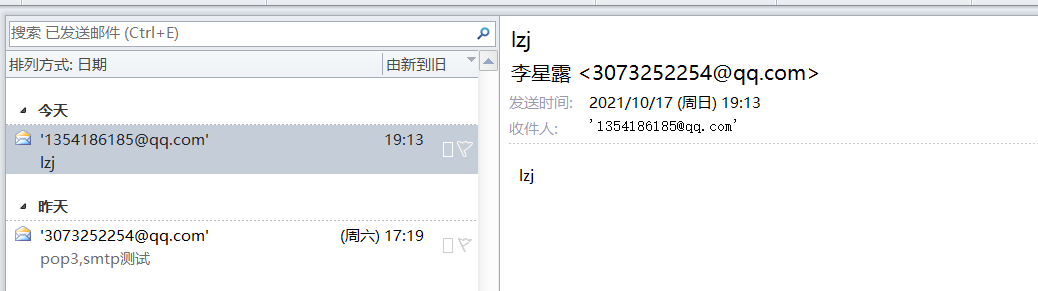
C：QUIT /\* 退出连接 \*/

S：221 Bye

分析上面的过程可参考注释进行，这里要补充如下几点。

“C：”开头的行(不包括"C：")是客户端的输入，而以“S：”开头的行(不包括"S：")则是服务器的输出。上述的命令并不一定会一次性成功，服务器会返回错误响应，客户端应该按照协议规定的时序，来输入后续的命令（或重复执行失败的命令，或重置会话，或退出会话等等）。

* 1. SMTP代理和SMTP服务器的通信过程分析



使用Outlook发送邮件

下图是我用WireShark抓取的一次Outlook代理和SMTP服务器的通信过程（由于SMTP是一种简单的传输协议，并且在这个例子通信过程为明文传输，因此可以跟踪TCP流）

分为三个步骤

**第一步：客户端至本地邮件服务器**

**第二步：本地邮件服务器至远程服务器**

**第三步：远程邮件服务器至远程客户端**

从用户在邮件客户端上点击“发送”按钮开始，用户计算机和本地邮件服务器在前三个数据包中完成握手连接建立后，客户端使用SMTP将邮件发送至本地邮件服务器

1、SMTP协议是基于TCP/IP协议的，所以通讯开始要进行tcp握手。

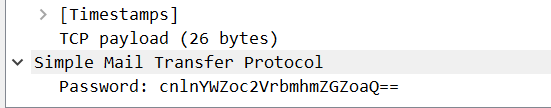
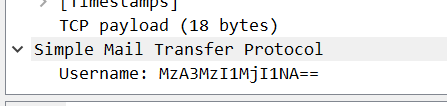
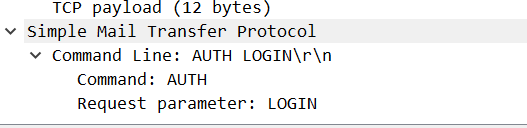
2、SMTP服务器向客户端发送200 newxmesmtplogicsvrsza8.qq.com Xmail Esmtp QQ Mail Server，表示服务器准备就绪。

3、客户端发送C: EHLO LAPTOP0S1S99NJ交换身份信息，打开通道。LAPTOP0S1S99NJ是客户端主机名。

4、服务器发送需要进行认证的信息。

5、进行用户名和密码认证

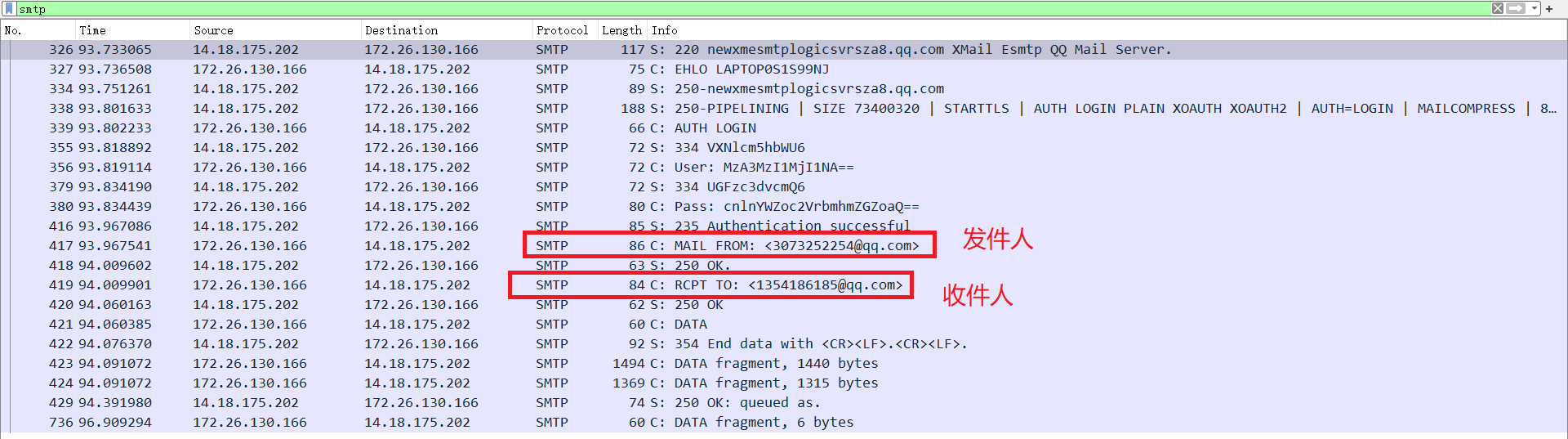
PC发送给邮件服务器的报文，这边是用户登录命令, 邮件服务器发送给PC的报文，状态码是334，代表接受用户登录, PC发送给邮件服务器的报文，包含了登陆的用户名的信息, 邮件服务器接受用户登录,PC发送给邮件服务器的报文，包含了用户登录服务器的密码,邮件服务器发送给PC的报文，状态字235代表用户登录成功。

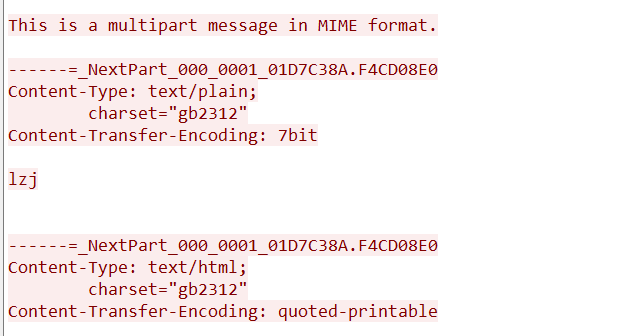


以上是用户登陆的信息包，用户名和密码是经过base64加密过后的。

6、发送邮件

邮件传送从MAIL命令开始，MAIL命令后面有发信人的地址。若SMTP服务器准备好接收邮件，在回答“250 OK”，否则，返回一个差错代码。随后跟着一个或多个RCPT 命令，再后面是DATA命令。





上图是传输邮件的具体文本内容

7、关闭信道，服务器返回总共收到的字节数，邮件发送完毕后，SMTP客户应发送QUIT命令。SMTP服务器返回的信息是“221”，表示同意释放TCP连接

8、TCP四次挥手，通讯结束

四次挥手并没有具体截图，但是和之前HTTP协议分析中的TCP三次连接一样有序号和确认号（状态号）。

1）客户端进程发出连接释放报文，并且停止发送数据。释放数据报文首部，FIN=1，其序列号为seq=u（等于前面已经传送过来的数据的最后一个字节的序号加1），此时，客户端进入FIN-WAIT-1（终止等待1）状态。 TCP规定，FIN报文段即使不携带数据，也要消耗一个序号。

2）服务器收到连接释放报文，发出确认报文，ACK=1，ack=u+1，并且带上自己的序列号seq=v，此时，服务端就进入了CLOSE-WAIT（关闭等待）状态。TCP服务器通知高层的应用进程，客户端向服务器的方向就释放了，这时候处于半关闭状态，即客户端已经没有数据要发送了，但是服务器若发送数据，客户端依然要接受。这个状态还要持续一段时间，也就是整个CLOSE-WAIT状态持续的时间。

3）客户端收到服务器的确认请求后，此时，客户端就进入FIN-WAIT-2（终止等待2）状态，等待服务器发送连接释放报文（在这之前还需要接受服务器发送的最后的数据）。

4）服务器将最后的数据发送完毕后，就向客户端发送连接释放报文，FIN=1，ack=u+1，由于在半关闭状态，服务器很可能又发送了一些数据，假定此时的序列号为seq=w，此时，服务器就进入了LAST-ACK（最后确认）状态，等待客户端的确认。

5）客户端收到服务器的连接释放报文后，必须发出确认，ACK=1，ack=w+1，而自己的序列号是seq=u+1，此时，客户端就进入了TIME-WAIT（时间等待）状态。注意此时TCP连接还没有释放，必须经过2∗∗MSL（最长报文段寿命）的时间后，当客户端撤销相应的TCB后，才进入CLOSED状态。

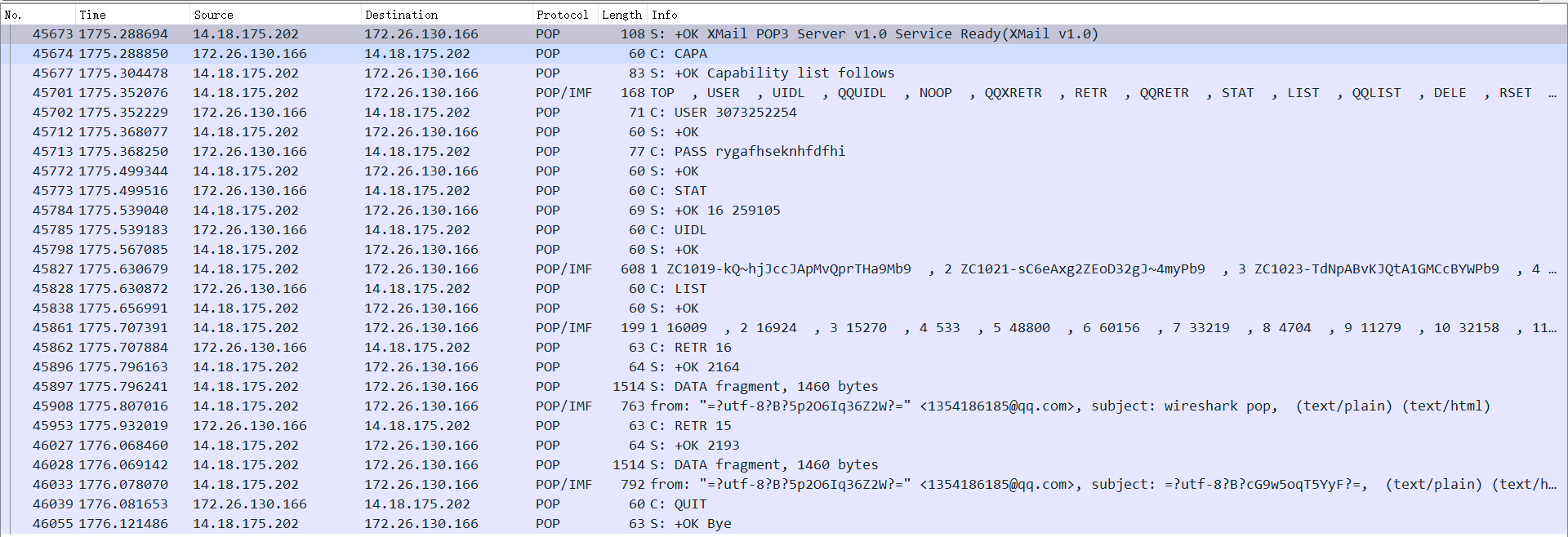
6）服务器只要收到了客户端发出的确认，立即进入CLOSED状态。同样，撤销TCB后，就结束了这次的TCP连接。可以看到，服务器结束TCP连接的时间要比客户端早一些。

* POP协议

与SMTP同时出现的还有POP，不同的是SMTP是负责邮件服务器与邮件服务器之间的寄信的通讯协定， POP则是负责邮件程序和邮件服务器收信的通讯协定

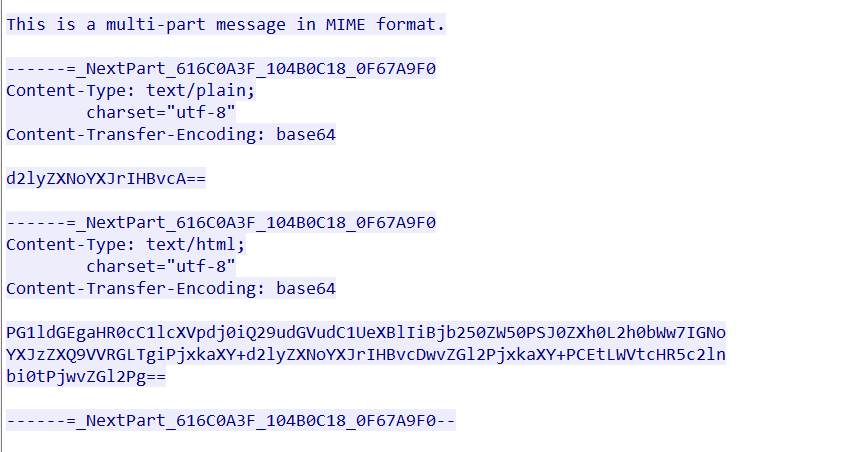
1. POP协议格式



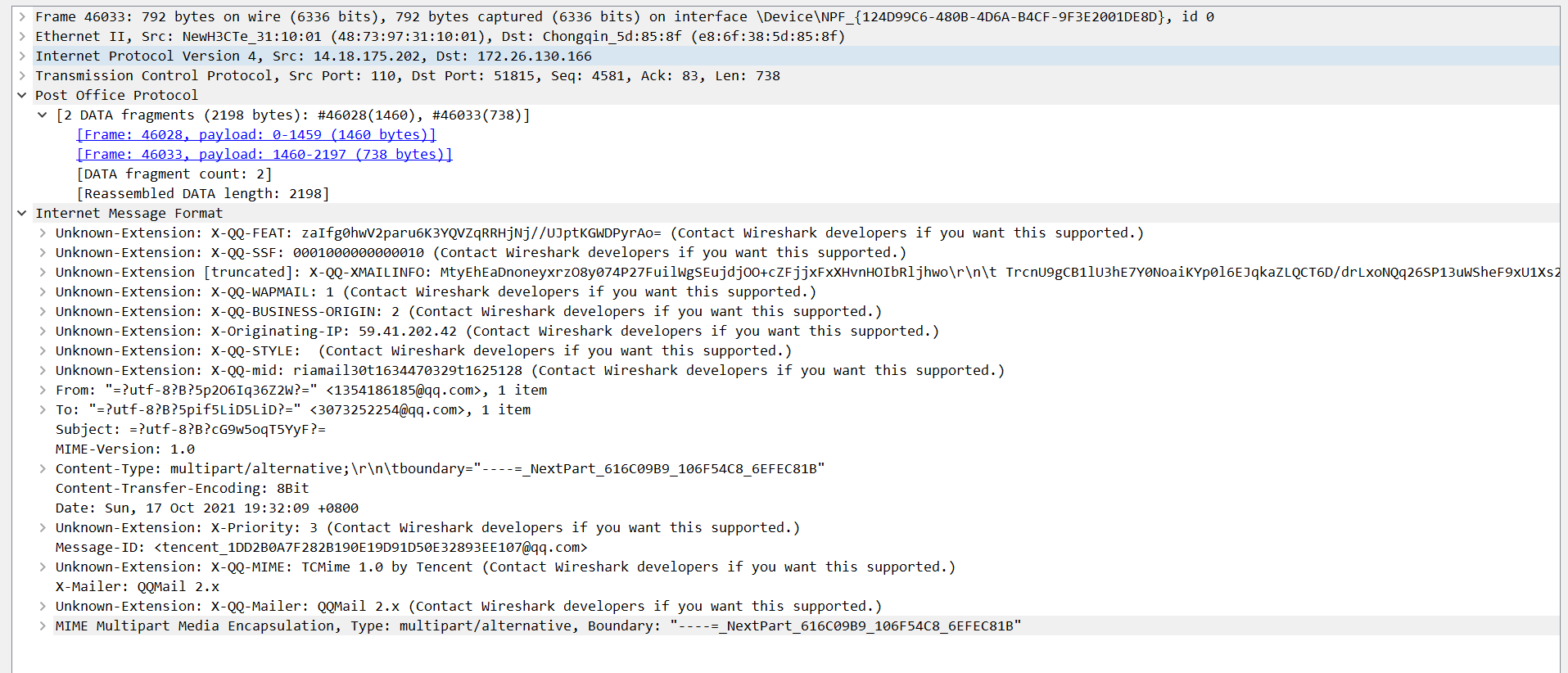
1. POP协议分析

由于POP协议默认的传输协议是TCP协议，因此，客户端连接服务器需要先进行三次握手建立端到端的连接。在客户端和服务器建立了连接之后，pop服务器回向pop客户端发送 带有OK的信息，通知客户端，服务器已经准备就绪，请开始认证阶段。

还是参照上图，客户端会向服务器发送用户名、授权码，邮箱服务器也会返回OK作为回应接下来客户端向服务器发送 LIST指令，服务器会返回邮件数量的大小。



这是具体接收到邮件的文本内容，该文本内容是经过base64加密后的显示结果。



**实验总结：**

通过本次实验，使得我对HTTP，FTP，DNS以及邮件的发送和接收过程有了一定的了解，锻炼了我的工具使用和分析协议的能力，也加深了我对网络协议的兴趣，让我觉得分析协议是一件很好玩的事情，网络协议看似很复杂， 但相互之间还是有很多的联系，认真的研宄真的会产生很多的乐趣。因为对网络协议分析还不是很了解，查找资料的过程中难免会存在一些理解上的偏差，有些地方的分析会显得很肤浅甚至是错误的，而且本次实验重点分析了协议的过程，而对每个包的详细分析还显得不够，所以还需要后续更深入的学习。

在做实验之前，在网上搜寻了很多创建邮件服务器的文章和做法，也尝试了很多方法，一开始是在网页上进行邮件的发送，但wireshark并不能捕获到有关SMTP以及POP协议的数据包，（因为在网页上使用邮件服务是封装在HTTP协议中的），也尝试过使用foxmail,创建不了用户，后来是使用了同学的电脑，还是发现在接收文件过滤POP协议数据包时，接受的速度很慢。

其实每一次在机房中做实验，就要珍惜好用机房电脑的机会，多次实验发现，其实电脑机房的数据捕获比在自己电脑上要更快。所以应该每次在实验课之前，就要做好相关的预习，这样在机房上实验课时对实验更快的上手，也不用再快下时间做其他的无用功。