**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 验证型 实验地点 B402

学生姓名 叶世翔 学号 2019051122

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 9 月 28 日 下 午～ 9 月 29 日 下 午

1. **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。**

1. **实验内容**

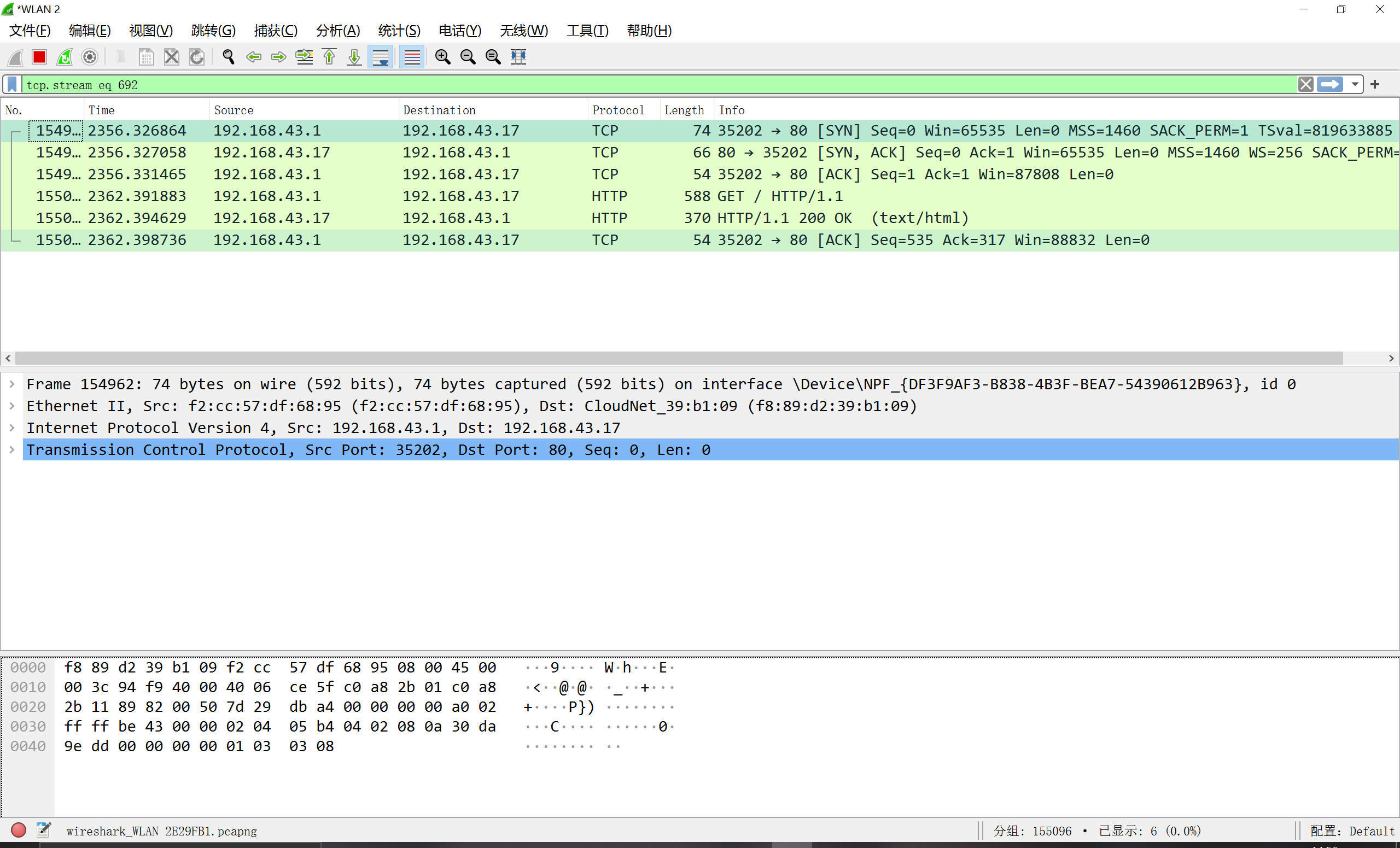
* 通过域名访问WWW、FTP服务器，分析DNS、WWW、FTP工作过程，并使用WireShark分析相关协议格式；
* 在客户端访问SMTP服务器，使用wireshark分析SMTP、POP3协议的工作过程。（可以在客户端安装outlook或使用QQ邮件服务器或自己编程）

1. **实验设备**

* 一台具有网络功能的PC 机

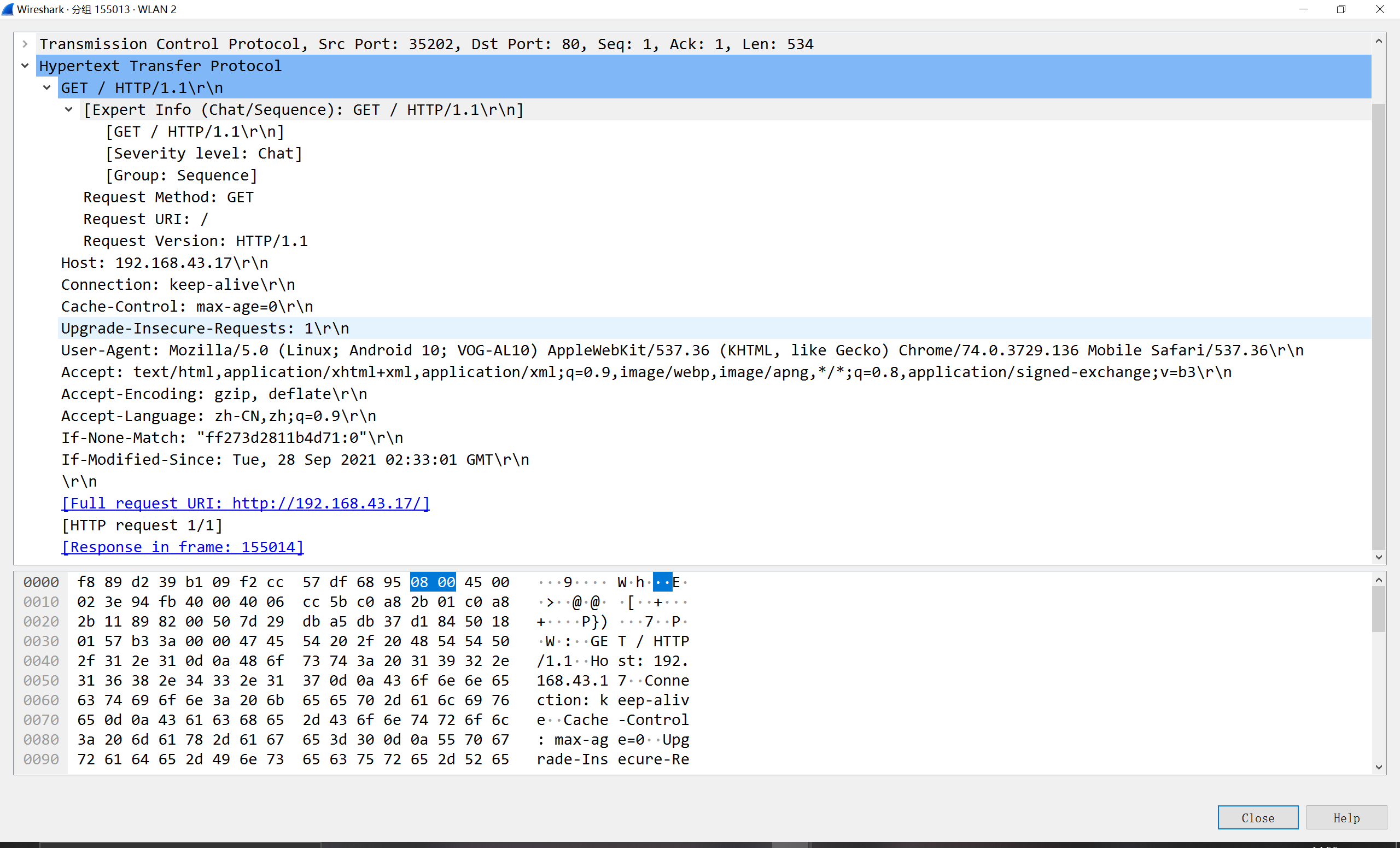
1. **实验步骤**
2. **HTTP协议分析**

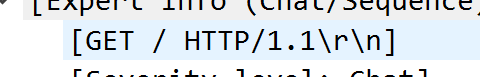
用电脑连上手机热点，利用windows自带组件IIS，建立并配置WWW站点，主页内容需要包含姓名、学号等个人信息，然后用手机访问自己建立的网站。



**网页做得比较简单，因此只有简单的get和ok的过程**

**报文分析：**





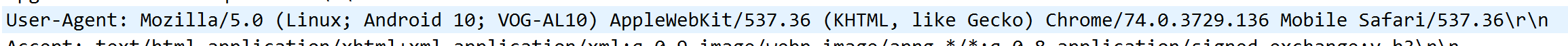
**此行为状态行，报文请求的是一个对象，该对象为空**

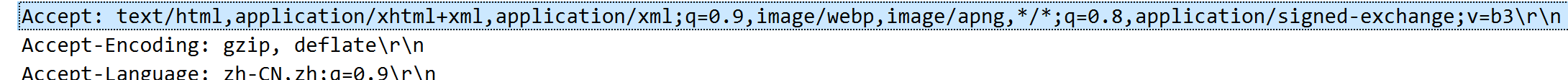


**激活连接**

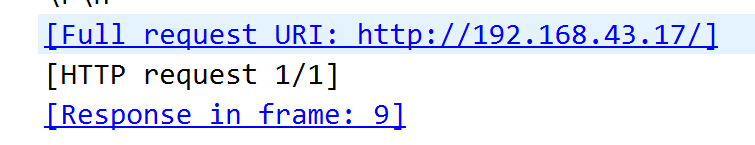


**缓存控制，告知服务器，客户端希望接受一个存在时间不超过0s的资源**

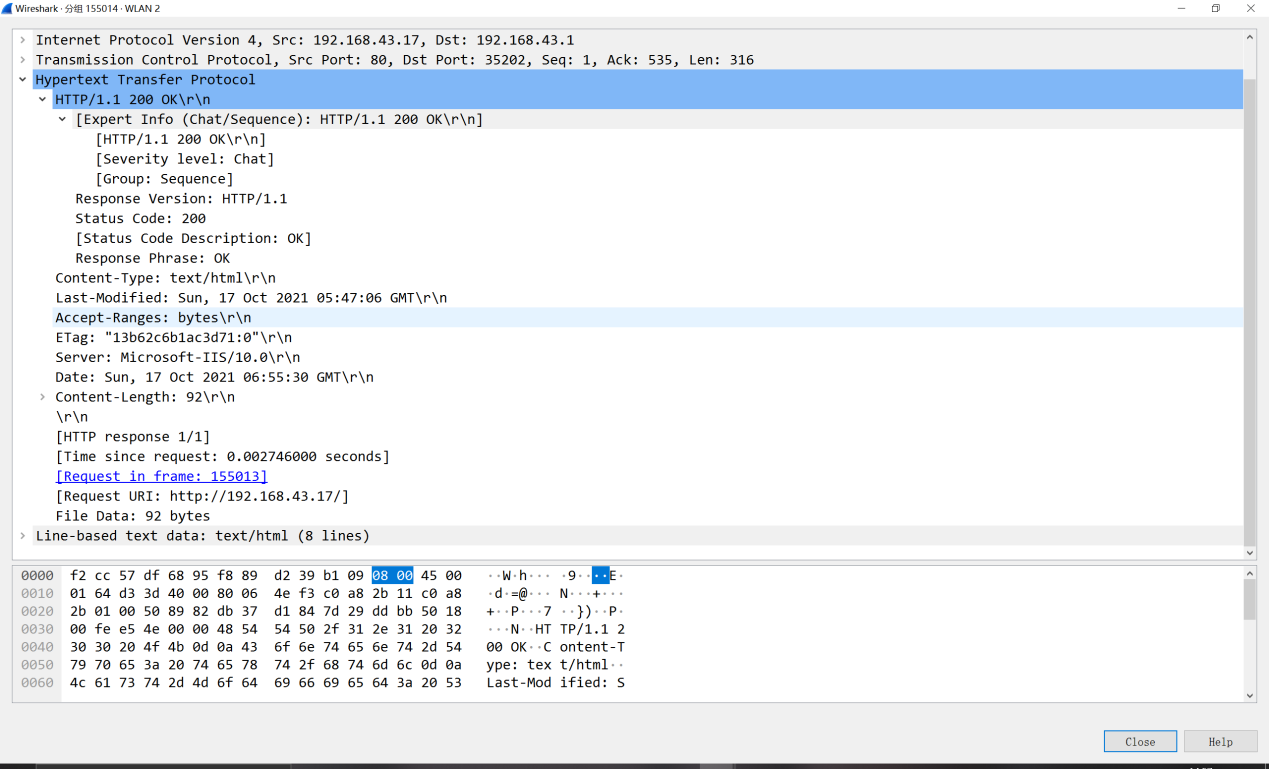
**浏览器的类型**

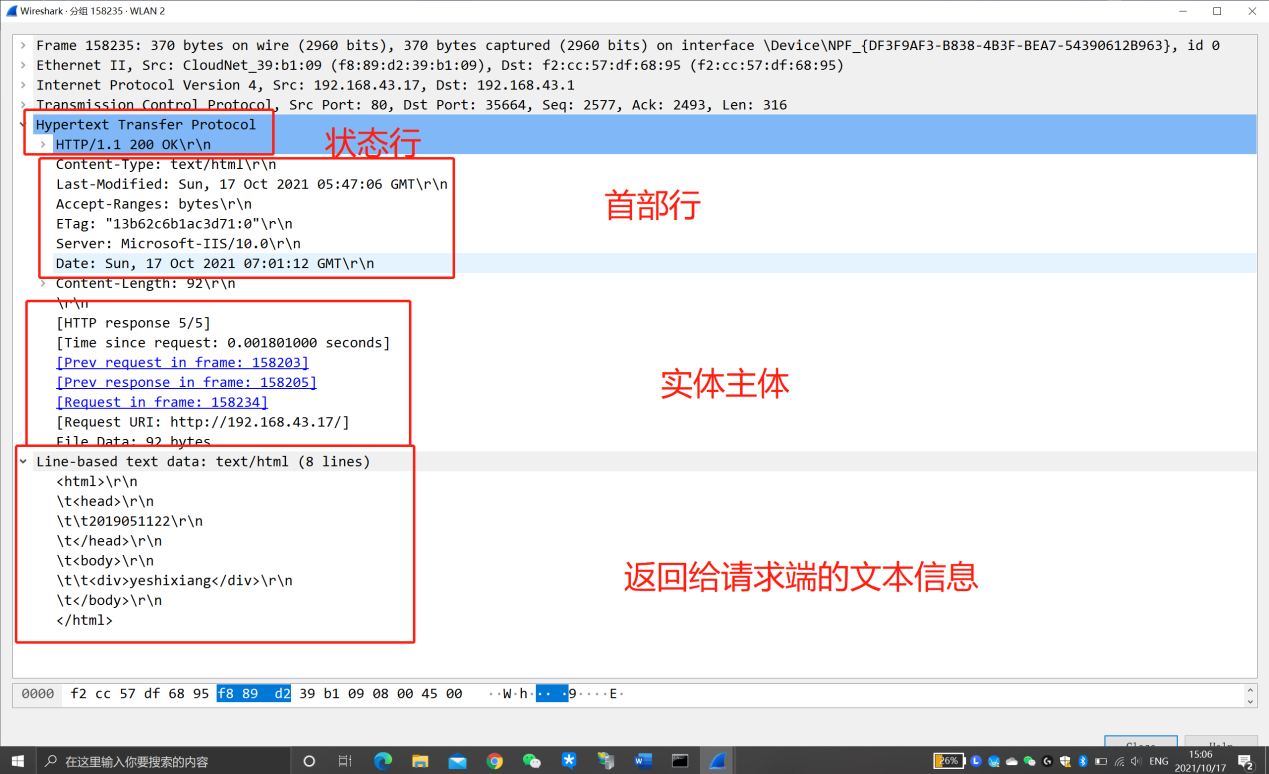


**分别为请求的类型、请求的编码格式、请求的语言**



**第一行位请求的url 第三行表示在第9帧应答**







**状态行中HTTP/1.1是版本字段，200 OK是表示客户端请求成功**

**Content-Type：表示后面的文档属于什么MIME类型**

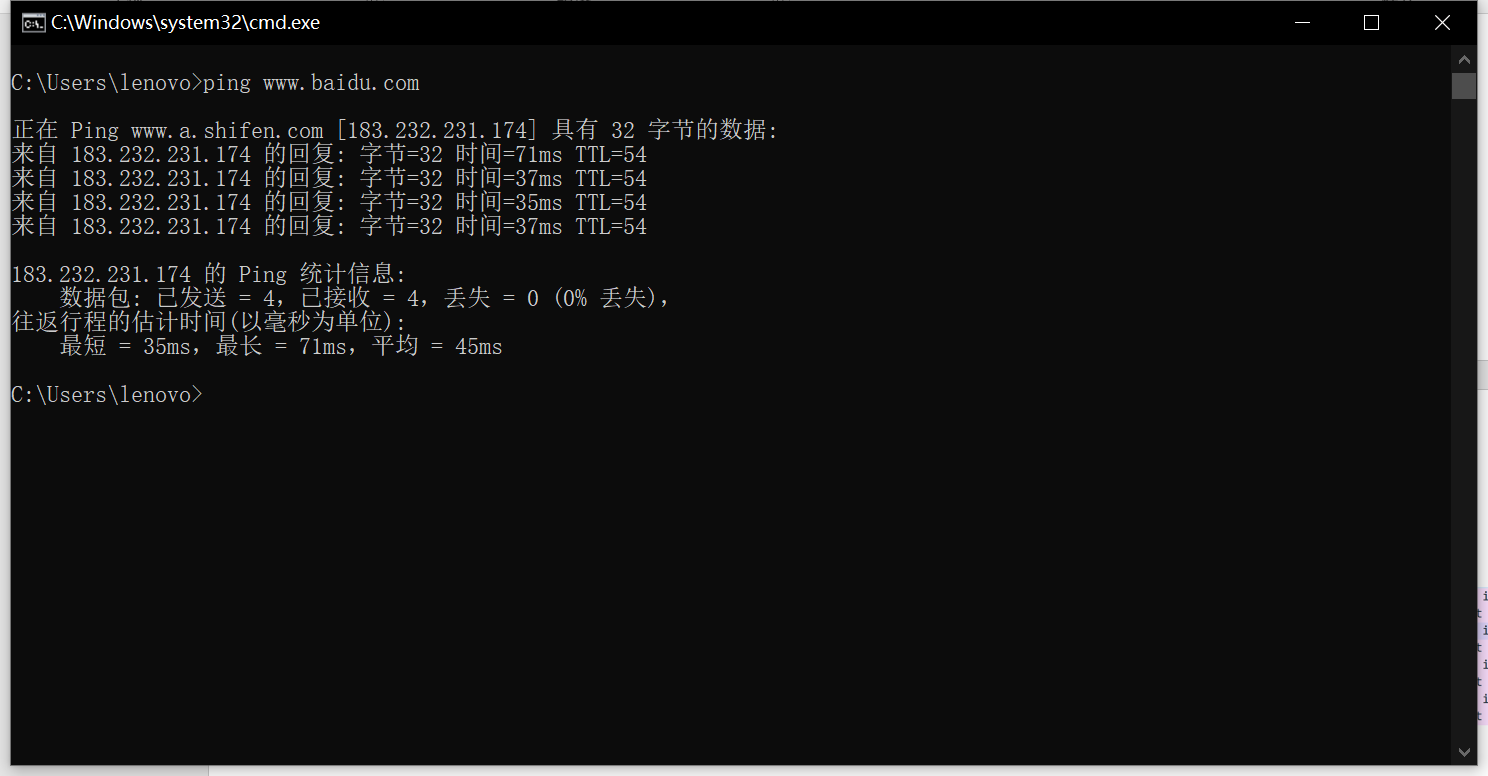
**Server：服务器名字**

**Date：当前GMT时间**

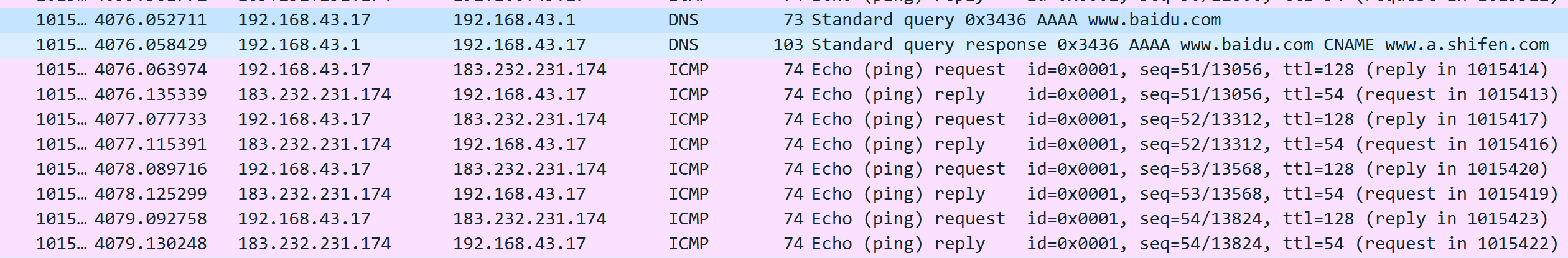
**Content-Length：表示内容长度**

1. **DNS协议分析**

先ping [www.baidu.com](http://www.baidu.com)

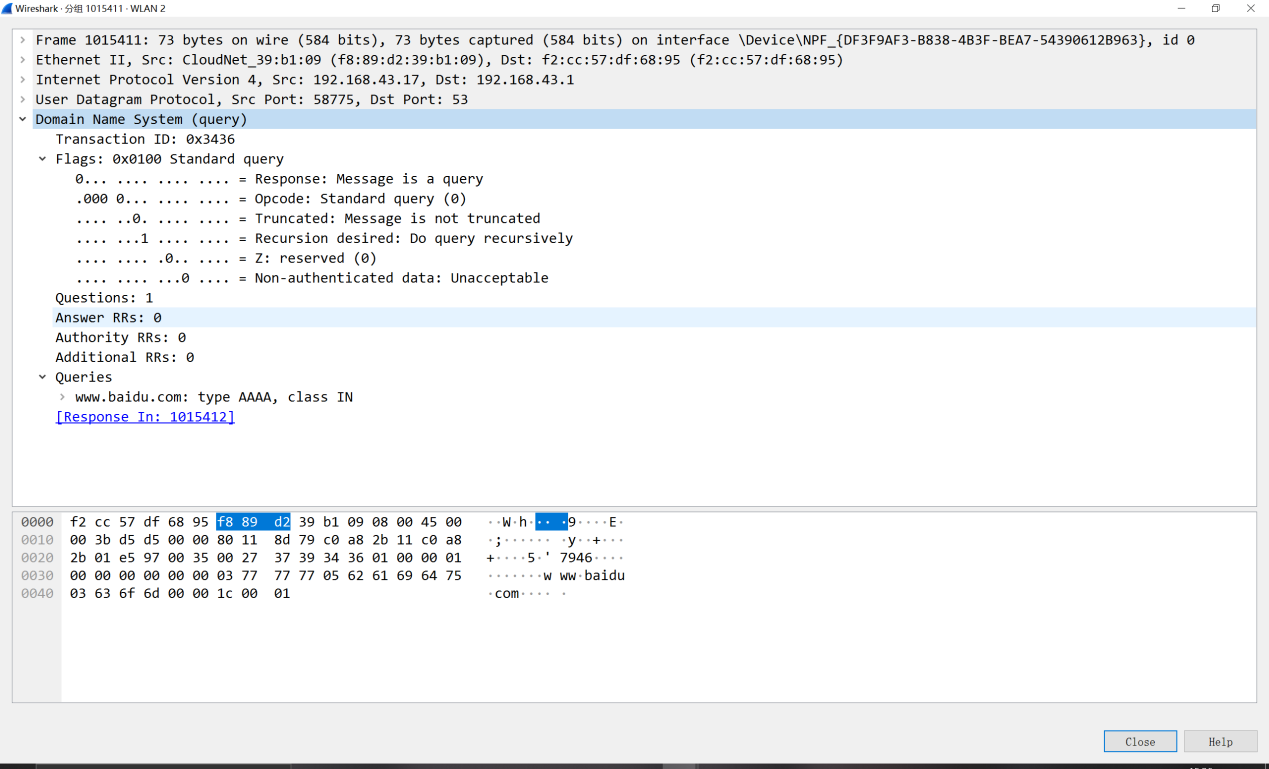


用wireshark进行抓包



可以看到两个DNS包和八个ICMP包，因为ping了四次，发送了四个包，接受了四个包。

点开第一个DNS包，也就是请求包，发送方是本机，接收方是本地域名服务器



Transaction ID为标识字段,2字节,用于辨别DNS应答报文是哪个请求报文的响应

Flags标志字段,2字节,每一位的含义不同:

IMG_256

QR: 查询/响应,1为响应,0为查询

Opcode: 查询或响应类型,这里0表示标准,1表示反向,2表示服务器状态请求

AA: 授权回答,在响应报文中有效,待会儿再看

TC: 截断,1表示超过512字节并已被截断,0表示没有发生截断

RD: 是否希望得到递归回答

RA: 响应报文中为1表示得到递归响应

zero: 全0保留字段

rcode: 返回码,在响应报文中,各取值的含义:

0 - 无差错

1 - 格式错误

2 - 域名服务器出现错误

3 - 域参照问题

4 - 查询类型不支持

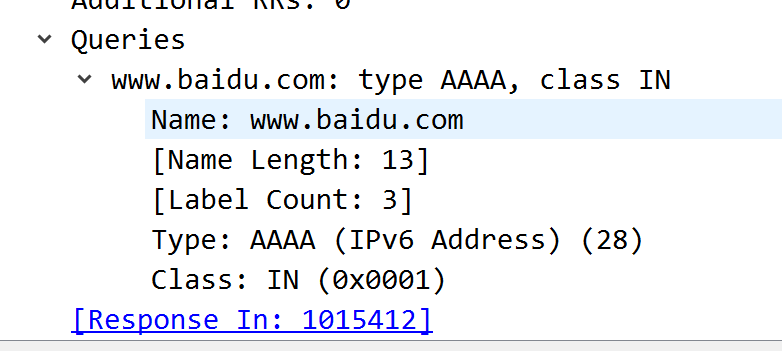
5 - 被禁止

6 ~ 15 保留

Quetions(问题数),2字节,通常为1

Answer RRs(资源记录数),Authority RRs(授权资源记录数),Additional RRs(额外资源记录数)通常为0

字段Queries为查询或者响应的正文部分,分为Name 、Type 、Class



Name：要查询的域名，如果是IP地址则代表反向查询

Type：DNS查询请求的资源类型。常见的有：

A类型：IPv4地址

AAAA类型：IPv6地址

NS：名字服务器  
ANY：对所有记录的请求

CLASS：地址类型，通常为互联网(IN)，值为1

事务 ID（Transaction ID）：DNS 报文的 ID 标识。对于请求报文和其对应的应答报文，该字段的值是相同的。通过它可以区分 DNS 应答报文是对哪个请求进行响应的。

标志（Flags）：DNS 报文中的标志字段。

问题计数（Questions）：DNS 查询请求的数目。

回答资源记录数（Answers RRs）：DNS 响应的数目。

权威名称服务器计数（Authority RRs）：权威名称服务器的数目。

附加资源记录数（Additional RRs）：额外的记录数目（权威名称服务器对应 IP 地址的数目）。

   其中Flags字段中每个字段的含义如下：

QR（Response）：查询请求/响应的标志信息。查询请求时，值为 0；响应时，值为 1。

Opcode：操作码。其中，0 表示标准查询；1 表示反向查询；2 表示服务器状态请求。

AA（Authoritative）：授权应答，该字段在响应报文中有效。值为 1 时，表示名称服务器是权威服务器；值为 0 时，表示不是权威服务器。

TC（Truncated）：表示是否被截断。值为 1 时，表示响应已超过 512 字节并已被截断，只返回前 512 个字节。

RD（Recursion Desired）：期望递归。该字段能在一个查询中设置，并在响应中返回。该标志告诉名称服务器必须处理这个查询，这种方式被称为一个递归查询。如果该位为 0，且被请求的名称服务器没有一个授权回答，它将返回一个能解答该查询的其他名称服务器列表。这种方式被称为迭代查询。

RA（Recursion Available）：可用递归。该字段只出现在响应报文中。当值为 1 时，表示服务器支持递归查询。

Z：保留字段，在所有的请求和应答报文中，它的值必须为 0。

rcode（Reply code）：返回码字段，表示响应的差错状态。

当值为 0 时，表示没有错误；

当值为 1 时，表示报文格式错误（Format error），服务器不能理解请求的报文；

当值为 2 时，表示域名服务器失败（Server failure），因为服务器的原因导致没办法处理这个请求；

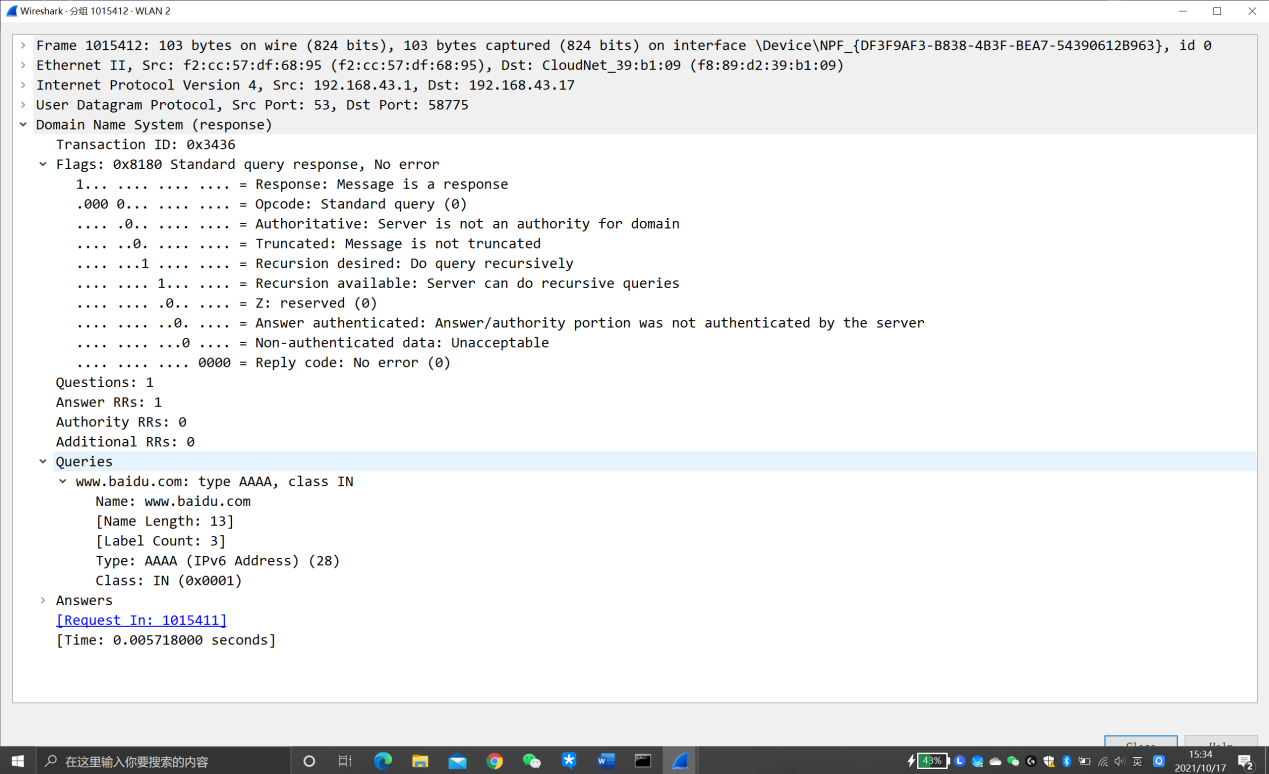
当值为 3 时，表示名字错误（Name Error），只有对授权域名解析服务器有意义，指出解析的域名不存在；

当值为 4 时，表示查询类型不支持（Not Implemented），即域名服务器不支持查询类型；

当值为 5 时，表示拒绝（Refused），一般是服务器由于设置的策略拒绝给出应答，如服务器不希望对某些请求者给出应答，，或者服务器不希望进行某些操作（比如区域传送zone transfer）；

6-15 保留值，暂时未使用。

点开第二个DNS包，响应包



对比请求报文发现，响应报文“基础结构部分”和请求报文结构对应相同，并返回字段说明服务器支持递归查询（RA=1），服务器响应记录的名称服务器为非权威服务器（AA=0）,产生了4条响应记录（Answers RRs = 4），响应报文中多了answers字段且有4条数据

响应报文中，Queries字段完全和请求报文相同，answers字段为**DNS资源记录部分**的内容。

每个字段含义如下：

Name：DNS 请求的域名。

Type：资源记录的类型，与问题部分中的查询类型值是一样的。

Class：地址类型，与问题部分中的查询类值是一样的。

Time to live：生存时间，以秒为单位，表示资源记录的生命周期，一般用于当地址解析程序取出资源记录后决定保存及使用缓存数据的时间。它同时也可以表明该资源记录的稳定程度，稳定的信息会被分配一个很大的值。

Data length：资源数据的长度。

资源数据：表示按查询段要求返回的相关资源记录的数据。（如 Address :IP地址，CNAME:服务器别名 ，等）

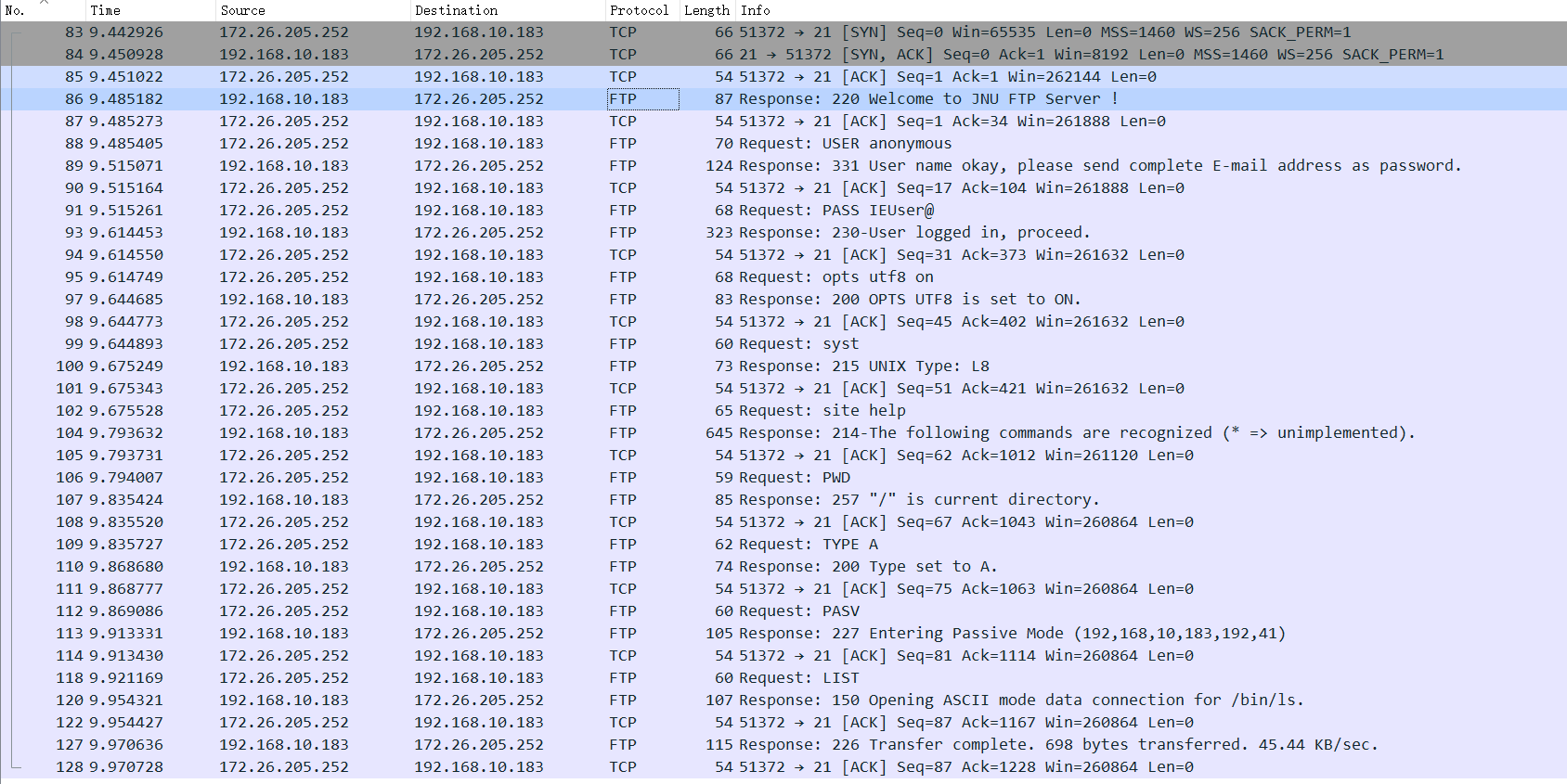
注意：

1、有时候可能捕获不到DNS解析过程，为什么？要仔细分析。

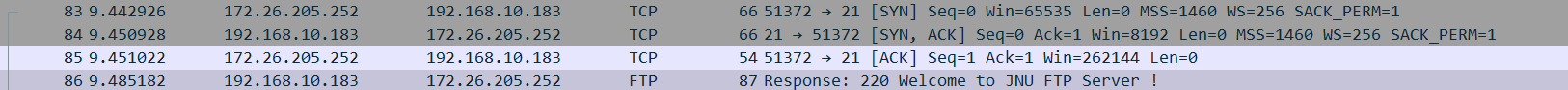
因为最近访问过这个网站，该网站的ip地址会被浏览器，操作系统缓存起来，再次访问该网站则直接从缓存中获取ip地址。

**三、FTP协议分析**

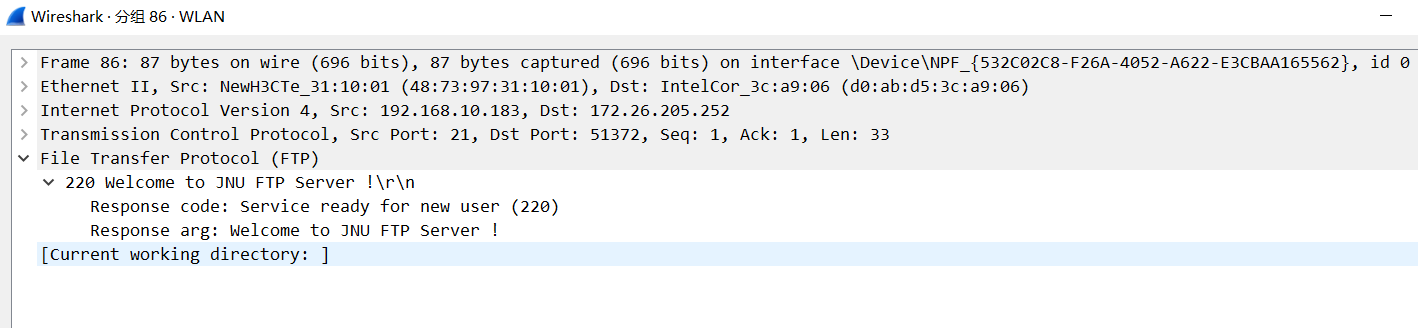
访问学校FTP服务器ftp://ftp.jnu.edu.cn，并进行抓包分析：



1-3是tcp包，tcp三次握手建立连接，可以看出ftp是基于tcp的



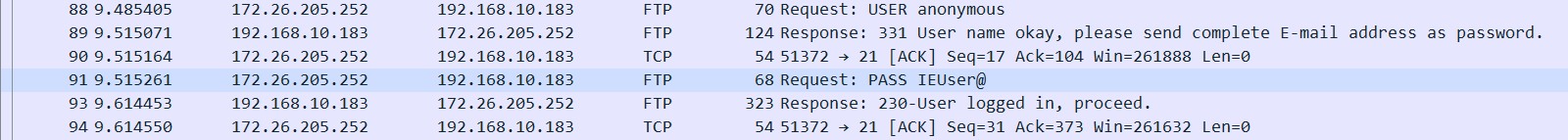
第四个包是FTP包，是服务器的响应报文，状态码220表示建立连接成功，并以ascii码方式明文传输数据



第五个包是客户端向服务器发送的确认。

第六到十一个包分别是：客户端输入用户名；服务器端确认并提示输密码；客户端确认；客户端发送密码；服务器端确认密码正确；客户端确认收到。

其中，密码和用户名都是明文的，如下图

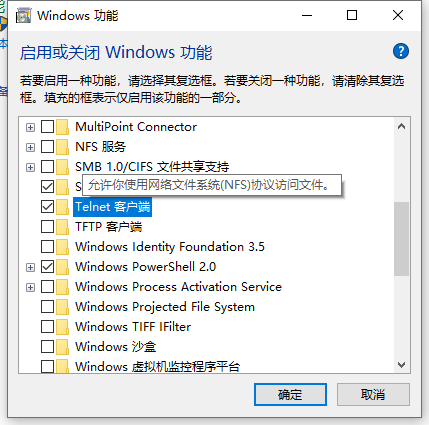


FTP响应代码



**四、 SMTP和POP协议分析**

先启用windows功能 Telnet客户端

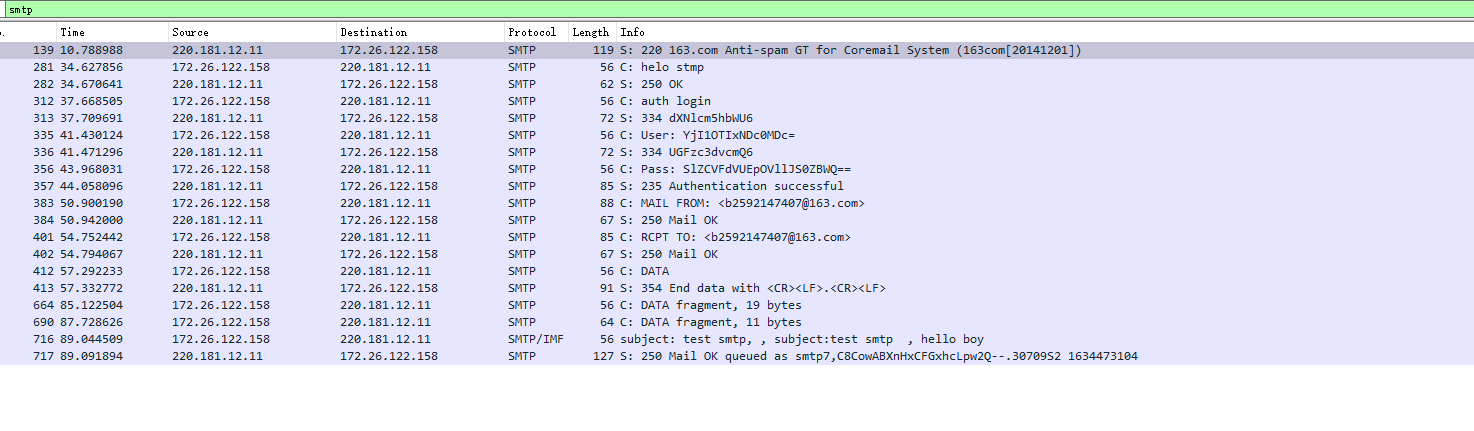


重启后输入一下命令

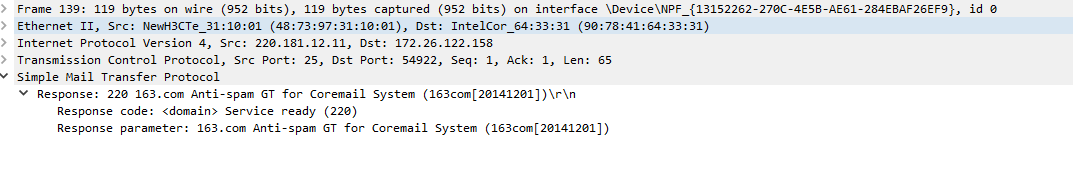


然后登陆邮箱

用wireshark捕获smtp包

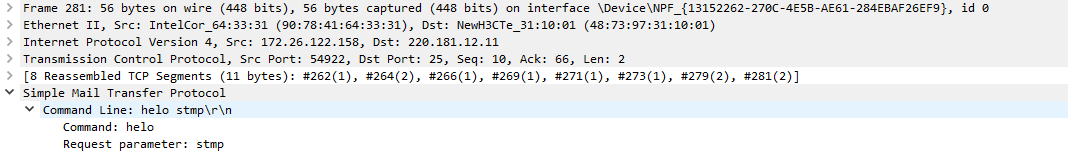


需这里筛掉了TCP协议，因此最开始的TCP三次握手建立连接在这里是看不到的，因此在图中的第一个包就是SMTP的服务器端发送给客户端的数据包



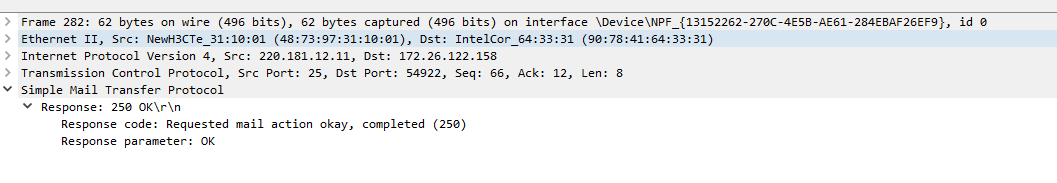
响应代码220表示连接建立成功，后面的Anti-spam表明是该邮件系统的反垃圾邮件模块，即猜测在这里就有反垃圾邮件模块来抵挡垃圾邮件的攻击

服务端返回220代码之后，客户端继续发送请求，首先是发送helo命令：

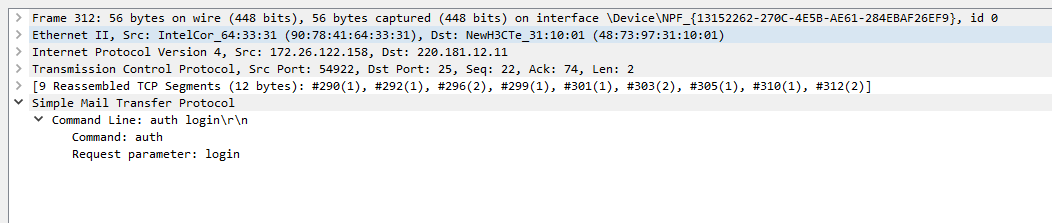


一般来说客户端和SMTP服务端建立连接之后就需要发送EHLO或者是HELO命令，后面附带的参数是<domain>，即相当于客户端的主机域名或者是主机名，这一步的主要作用是声明身份，EHLO/HELO命令相当于是HELLO命令，两者之间的主要区别是EHLO带身份验证而HELO不带身份验证，因此EHLO要更加安全

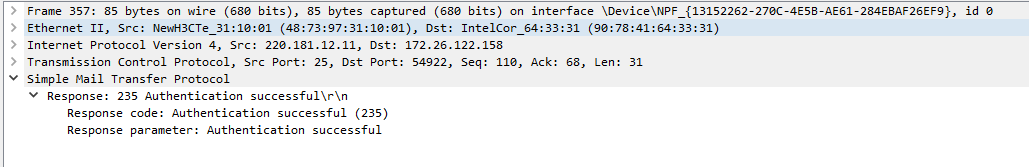
服务端接收到客户端的EHLO请求之后，返回了一个250代码.



客户端使用auth lgoin命令进行身份验证：



身份验证成功后会返回235的成功代码：



接下来客户端发送MAIL FROM命令声明邮件的发件人：

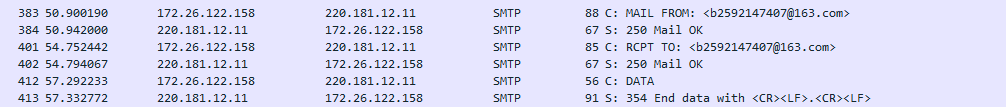
服务器返回250代码确定操作成功：

然后客户端发送RCPT TO命令声明邮件的收件人：

服务器返回250代码确定操作成功：

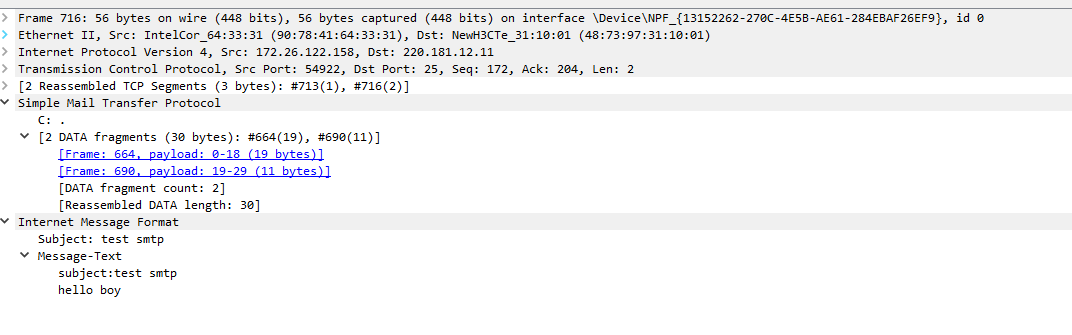
客户端使用DATA命令，告知服务器要开始传输邮件的正文内容：

服务端返回354代码，告知邮件的内容结束以<CR><LF>.<CR><LF>为标记：



客户端接收到254代码后，开始传输邮件内容：





我们可以看到在上面的数据包中包含了SMTP和IMF两个部分，因为抓包发送的邮件内容都是文本，所以直接使用[IMF协议](https://link.zhihu.com/?target=https://wiki.wireshark.org/IMF" \t "https://zhuanlan.zhihu.com/p/_blank)就可以传输，而SMTP协议中的报文内容则是DATA命令的终止标志.

服务器在接受到数据之后会返回250代码表示接受成功。

SMTP协议的工作过程：

SMTP的连接建立阶段

当SMTP需要身份验证时，此过程可能还包括AUTH等命令

SMTP客户与目的主机的SMTP服务器建立TCP连接，在TCP连接建立后,SMTP服务器要发出“220(服务就绪)”。

SMTP客户向SMTP服务器发送HELO命令,附上发送方的主机名。

SMTP服务器若有能力接收邮件，则回答:“250OK”，表示已准备好接收。

邮件的传送过程

SMTP连接建立后，就准备开始邮件的传送。邮件的传送从MAIL命令开始。MAIL 命令后面有发信人的地址。

SMTP服务器回答“2500K"。否则返回-个错误代码,指出原因。

下面跟着一个或多个RCPT命令,它取决于将同一个邮件发给一一个或多个收信人。

邮件服务器每收到一个RCPT命令，都会返回相应的信息。如“250 0K”或“550 Nosuch user here”。

接着是SMTP客户向SMTP服务器发送DATA命令，此命令表示要开始传送邮件的内容了。

若SMTP服务器能够接收邮件，则返回信息“354”,否则，返回信息“421”或“500”。

SMTP 客户发送邮件的内容，发送完毕后，再发送\r\n. \r\n表示邮件内容结束。

SMTP服务器返回信息“250OK"，表示邮件收到。

SMTP的连接释放过程

邮件发送完毕后,SMTP客户应发送QUIT命令。

SMTP服务器返回信息“221”(服务关闭)。

SMTP定义了14个命令，本次实验主要用到的命令有：

HELO–发件方问候收件方，后面是发件人的服务器地址或标识。收件方回答OK时标识自己的身份。问候和确认过程表明两台机器可以进行通信，同时状态参量被复位，缓冲区被清空。

MAIL–这个命令用来开始传送邮件，它的后面跟随发件方邮件地址（返回邮件地址）。它也用来当邮件无法送达时，发送失败通知。

RCPT–这个命令告诉收件方收件人的邮箱。

DATA–收件方把该命令之后的数据作为发送的数据。数据被加入数据缓冲区中，以单独一行是"."的行结束数据。

QUIT–SMTP要求接收方必须回答OK，然后中断传输；在收到这个命令并回答OK前，收件方不得中断连接，即使传输出现错误。发件方在发出这个命令并收到OK答复前，也不得中断连接。

POP3工作原理

POP3全称为Post Office Protocol version3，即邮局协议第3版。它被用户代理用来邮件服务器取得邮件，采用的也是C/S通信模型。

用户从邮件服务器上接收邮件的典型通信过程如下。

用户运行用户代理（如Foxmail, Outlook Express）。

用户代理（以下简称客户端）与邮件服务器（以下简称服务器端）的110端口建立TCP连接。

客户端向服务器端发出各种命令，来请求各种服务（如查询邮箱信息，下载某封邮件等）。

服务端解析用户的命令，做出相应动作并返回给客户端一个响应。

3和4交替进行，直到接收完所有邮件转到步骤6，或两者的连接被意外中断而直接退出。

用户代理解析从服务器端获得的邮件，以适当地形式（如可读）的形式呈现给用户。

其中2、3和4用POP3协议通信。

POP3协议中有三种状态，认证状态，处理状态，和更新状态。命令的执行可以改变协议的状态，而对于具体的某命令，它只能在具体的某状态下使用。客户机与服务器刚与服务器建立连接时，它的状态为认证状态；一旦客户机提供了自己身份并被成功地确认，即由认可状态转入处理状态； 在完成相应的操作后客户机发出QUIT命令，则进入更新状态，更新之后又重返认可状态；当然在认可状态下执行QUIT命令，可释放连接。状态间的转移如图所示。

