**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 3 实验项目类型 验证型 实验地点 实B402

学生姓名 张景曦 学号 2019051098

学院 智能科学与工程学院 系 计算机 专业 信息安全

实验时间 2021 年 10 月 1 日 上 午～ 10 月 12 日 上午

温度 27 ℃ 湿度 70%

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。**
2. **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）
3. **主要仪器设备**
   * 局部网环境，计算机若干台。本实验不分组，独立完成。
4. **实验环境**

计算机网络实验平台以及校园网络环境。

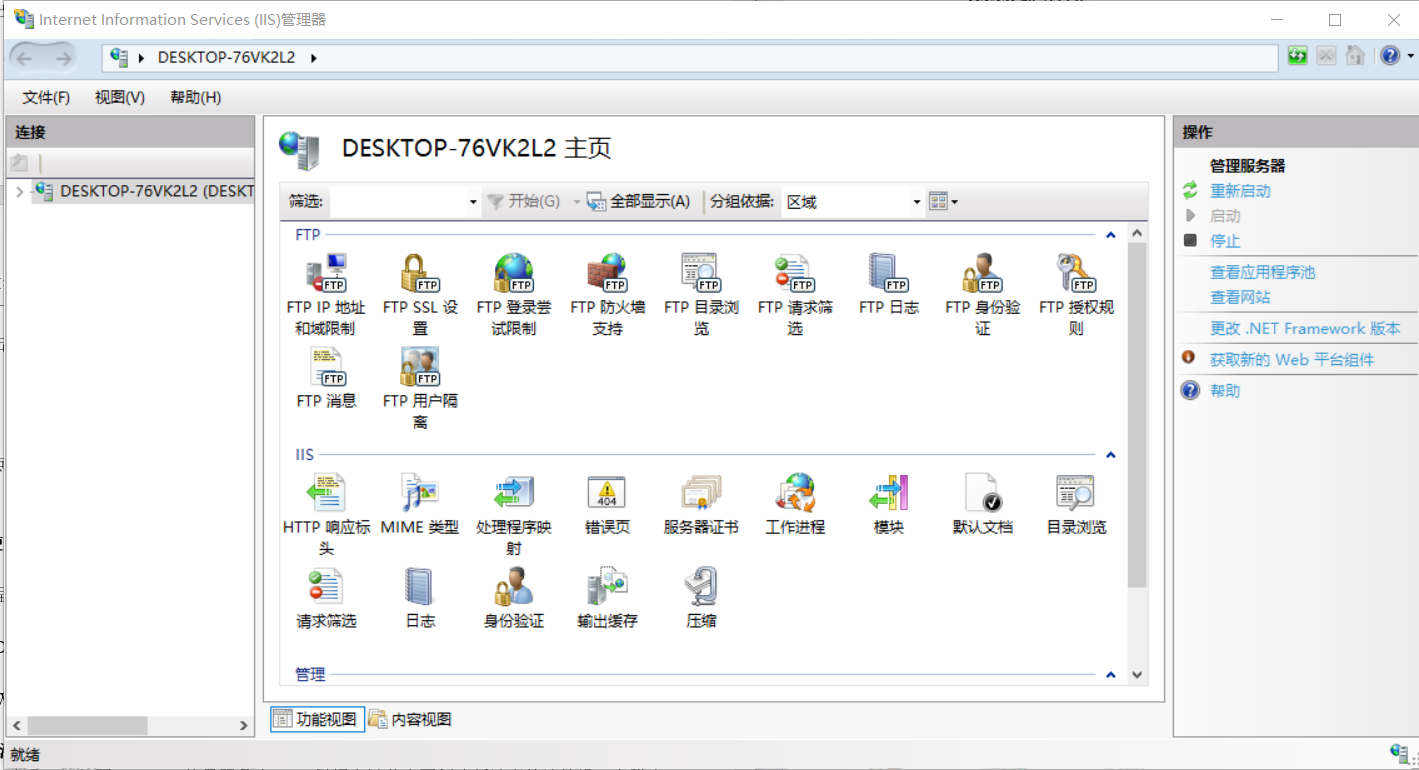
1. **实验步骤**

**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。

1. （如果访问的网站信息量太大，可以利用windows自带组件（如IIS））

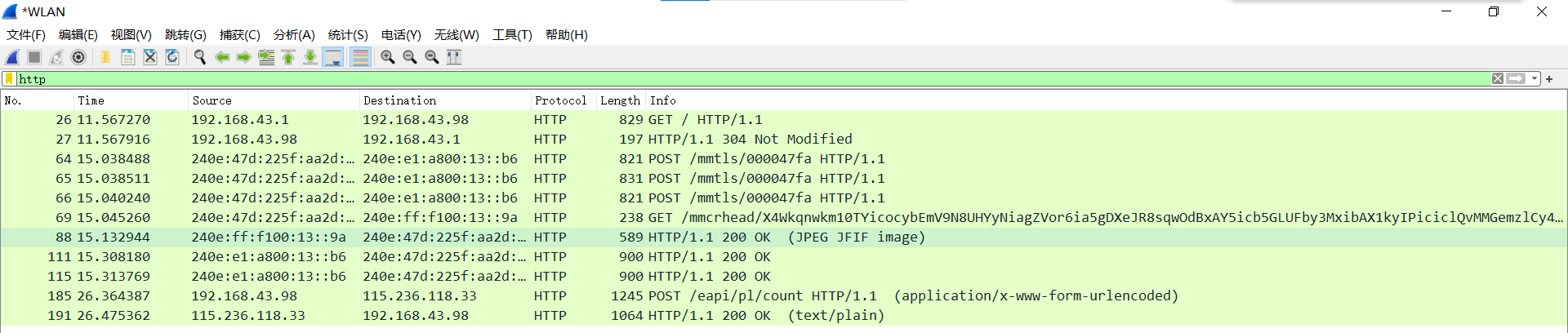
在控制面板中打开“添加或删除程序”，点击“启用或关闭Windows功能”打开选中Internet Information Services然后全部勾选点击确认下载。此时在管理工具中即可IIS管理器。此时服务器的WWW等服务会自动启动。



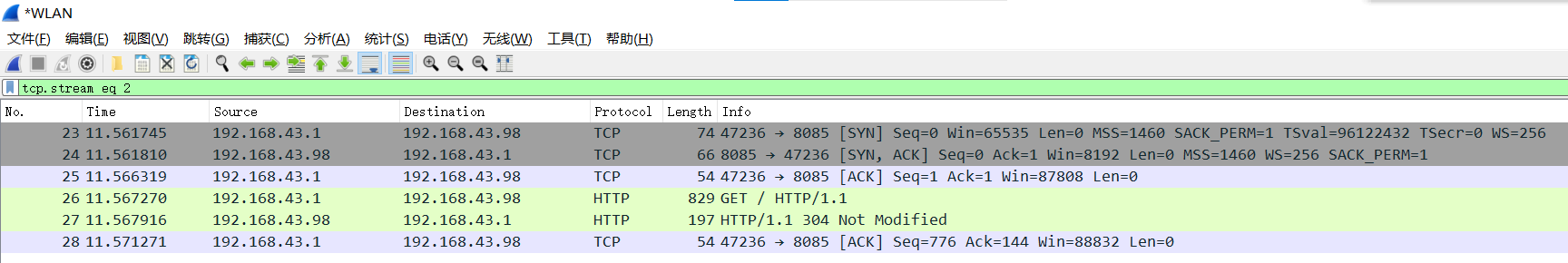
2.新建网站，然后用手机访问（使用同一局域网）



使用wireshark



选择追踪流的TCP流，做如下分析：



分析：

前三行：（三次握手）可以看见http请求报文发送前要和服务器建立TCP连接

第四行：请求报文



请求报文前面的GET /HTTP/1.1是请求行，接下来的是首行部，最后是实体主体。

GET / HTTP/1.1rn #请求行信息

Request Method: GET #请求方法为GET

Request URI: / #请求的URI

Request Version: HTTP/1.1 #请求的版本为HTTP/1.1

Host: 10.1.1.33:8080rn #请求的主机

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0rn #浏览器类型

Accept:text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8rn #请求的类型

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3rn #请求语言

Accept-Encoding: gzip, deflatern #请求的编码格式

Connection: keep-alivern #使用持久连接

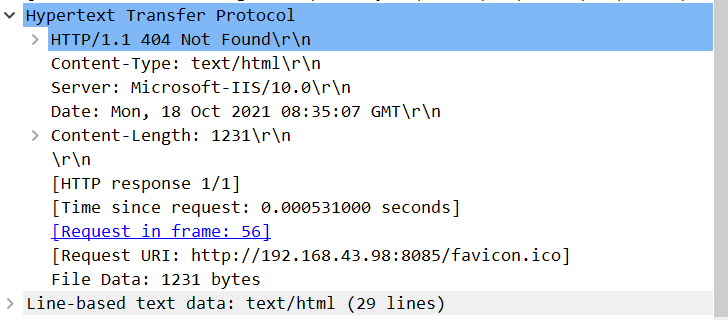
Full request URI: 请求的URI

Response in frame: 59 #应答是第59帧





第五行：响应报文



HTTP/1.1 200 OK\r\n #响应行信息 1.1是版本，200 OK是客户端请求成功，404是客户端请求失败

Content-Type: text/html\r\n #响应的内容类型

Content-Length: 1231\r\n #包的长度

Accept-Ranges: bytesrn #服务器支持的请求：字节

Server: Mivrodoft-IIS/10.0\r\n #服务器类型

\r\n #空行

HTTP response 1/1 #HTTP响应

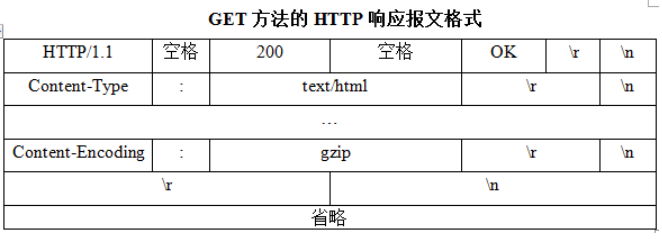
Time since request: 0.000531000 seconds #响应使用的时间

Request in frame: 56 #请求的帧号为56

Line-based text data: text/ html #基于行的文本数据

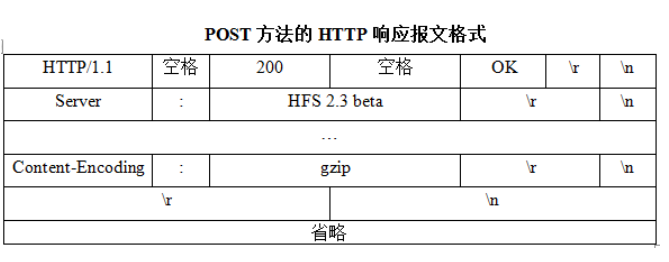
<1> GET方法

最常见的一种请求方式，当客户端要从服务器中读取文档时，当点击网页上的链接或者通过在浏览器的地址栏输入网址来浏览网页的，使用的都是GET方式。GET方法要求服务器将URL定位的资源放在响应报文的数据部分，回送给客户端。使用GET方法时，请求参数和对应的值附加在URL后面，利用一个问号（“?”）代表URL的结尾与请求参数的开始，传递参数长度受限制。例如，/index.jsp?id=100&op=bind,这样通过GET方式传递的数据直接表示在地址中，所以我们可以把请求结果以链接的形式发送给好友。



<2> POST方法

对于上面提到的不适合使用GET方式的情况，可以考虑使用POST方式，因为使用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。



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。

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。

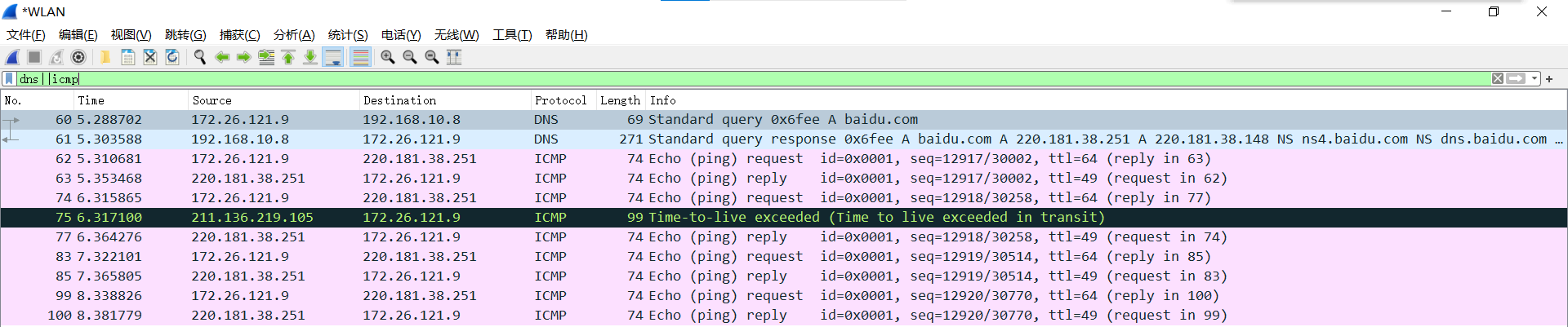
问：有时候可能捕获不到DNS解析过程，为什么？要仔细分析。

答：访问一次后储存了数据，下次访问就捕获不到DNS解析过程。

1.打开cmd命令行，ping一个网址



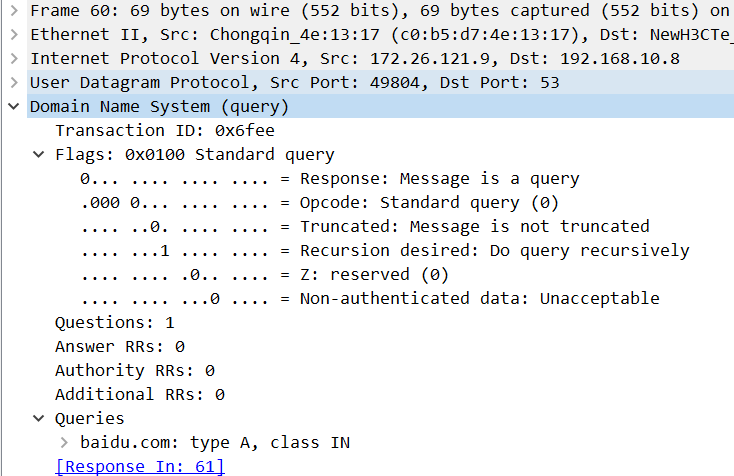
2.使用wireshark捕获数据包



分析：

总共有10个包，分别是2个DNS数据包（一次域名解析）和8个ICMP包（四次ping）。前面2个是dns数据包，分别是请求和响应。

3.打开第一个包，展开DNS数据：



可以发现DNS为应用层协议,下层传输层采用UDP,再下层网络层是IP协议,然后是数据链路层的以太网帧.需要关注的是应用层的实现也即DNS协议本身.第一个包是请求包,不可能直接包含DNS服务器地址。

第一个是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。

第二个是Flags标志字段,2字节,每一位的含义不同。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| QR | opcode | AA | TC | RD | RA | (zero) | Rcode |
| 1 | 4 | 1 | 1 | 1 | 1 | 3 | 4 |

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

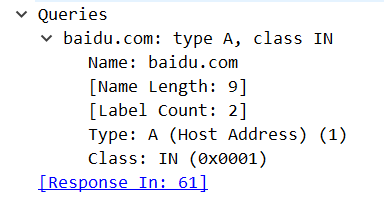
6 ~ 15 保留

紧接着标志位的是

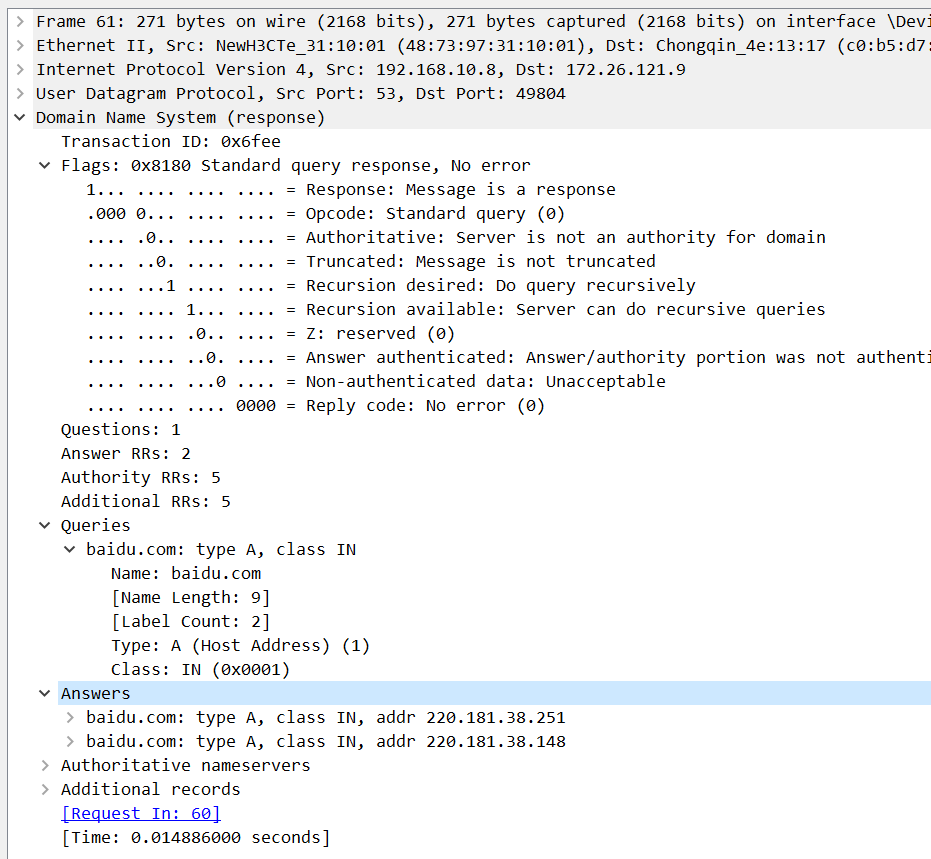
Quetions(问题数),2字节,通常为1

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

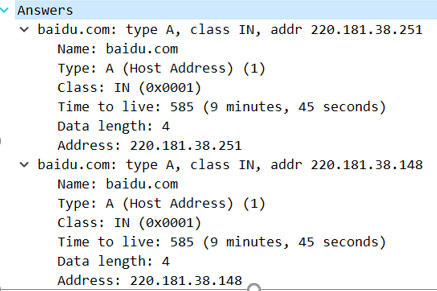


4.打开第二个包



和第一个请求包相比,响应包多出了一个Answers字段,同时Flags字段每一位都有定义.Flags中Answer RRs 为2说明对应的Answers字段中将会出现2项解析结果.

Answers字段可以看成一个List,集合中每项为一个资源记录,除了上面提到过的Name,Type,Class之外,还有Time to Live,Data length,Addr.



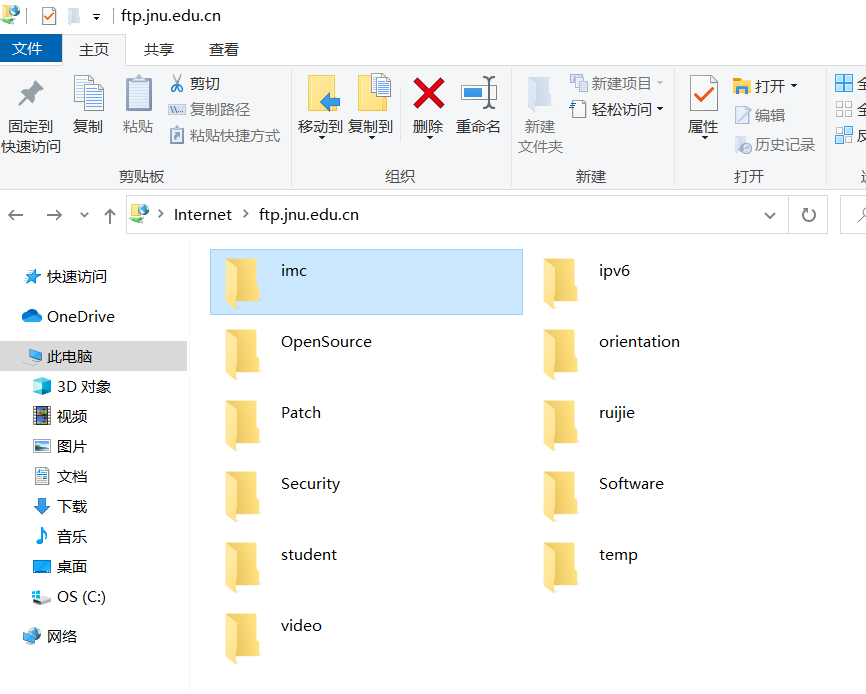
Time to Live(生存时间TTL):表示该资源记录的生命周期,从取出记录到抹掉记录缓存的时间,以秒为单位.

**三、FTP协议分析**

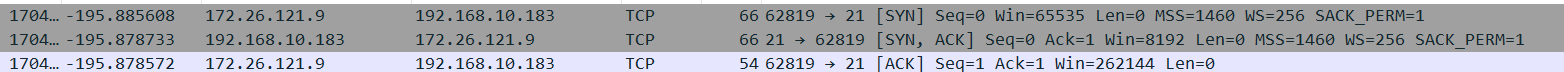
**1.**访问FTP服务器。如ftp://ftp.jnu.edu.cn

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。

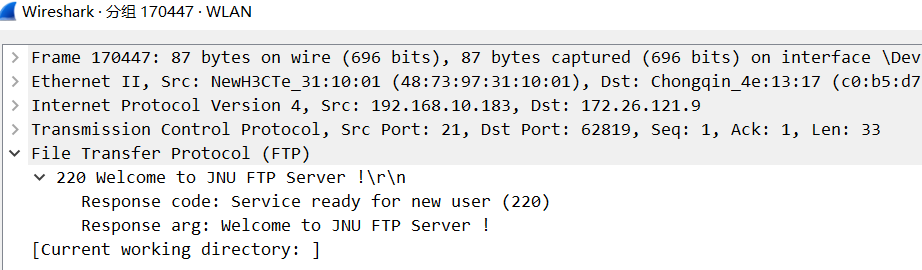
1.在“此电脑”搜索ftp://ftp.jnu.edu.cn



FTP是基于TCP协议的，首先经过三次握手建立连接：



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。

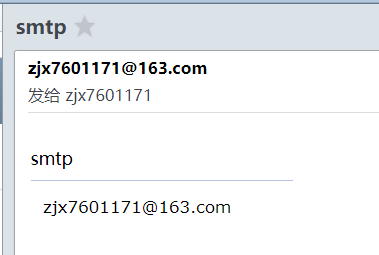
第五到十一个包分别是：客户端向服务器发送的确认，客户端输入用户名；服务器端确认并提示输密码；客户端确认；客户端发送密码；服务器端确认密码正确；客户端确认收到。

**四、 SMTP和POP协议分析**

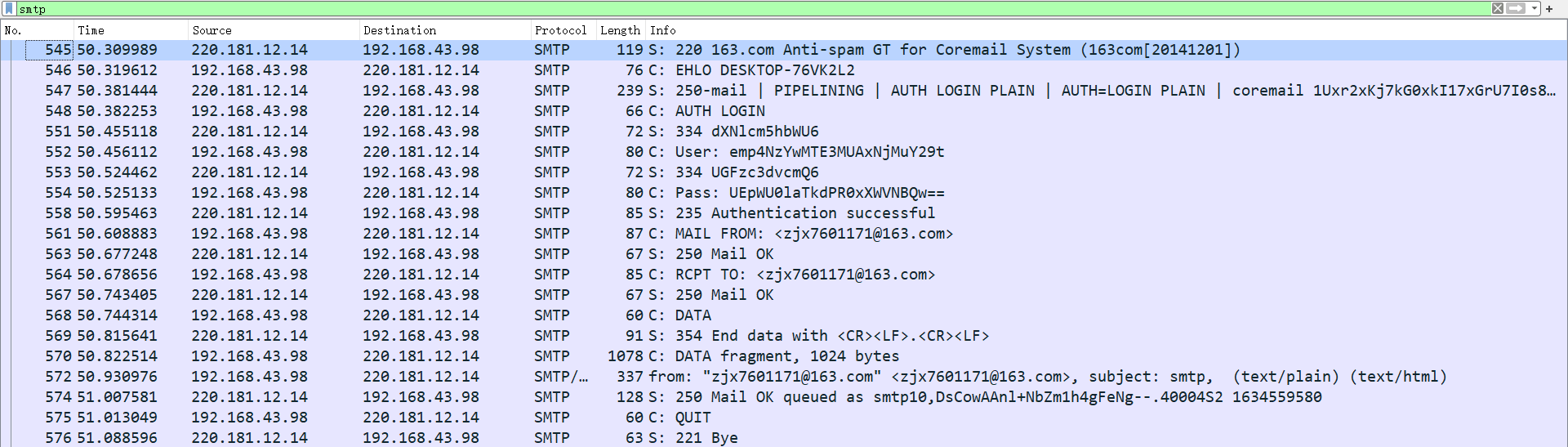
基于Web的邮件或客户端的邮件软件（如outlook）收发邮件，捕获数据报分析邮件收发过程和SMTP、POP3等协议格式和工作过程。

SMTP：简单邮件传输协议（SMTP）是发送邮件的标准，它被Microsoft Exchange 和Postfix等平台使用。与HTTP一样，SMTP由于实现方式、与客户端/服务器兼容性相关的一些列特性的不同，在数据包结构上存在多样性。

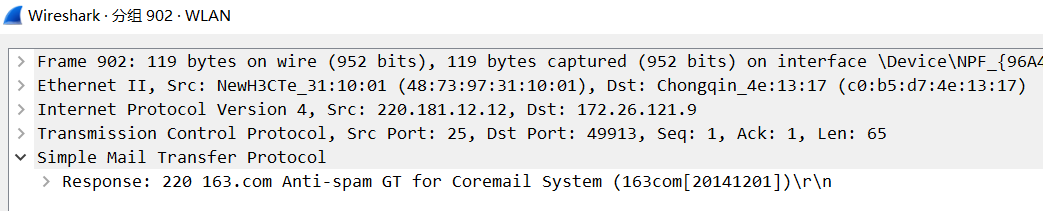
使用163邮箱发送邮件：



使用wirshark捕捉：

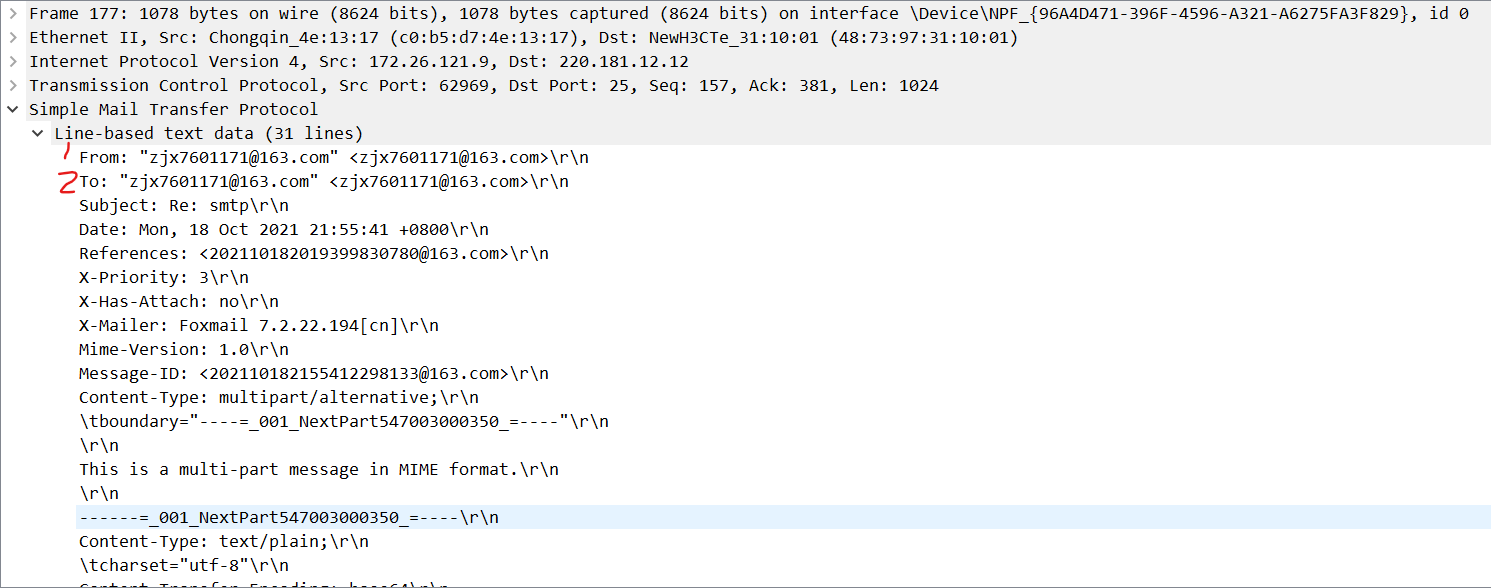


状态字220代表连接SMTP服务器成功：

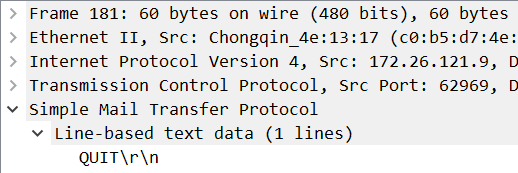


状态字250表示与服务器握手成功，235代表用户登录成功然后发送邮件。

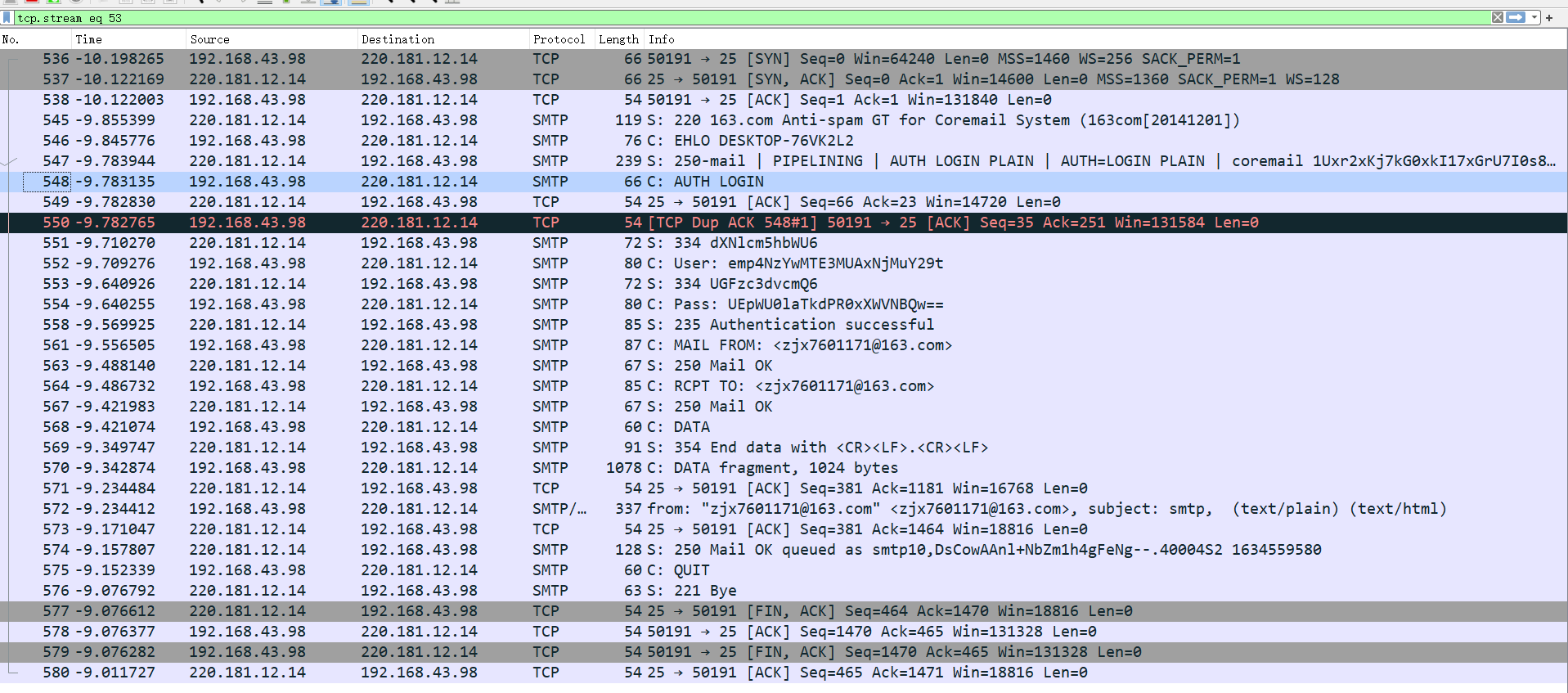
状态字334表示接受用户登录。



1位置是邮件发送者，2位置是邮件接收者。

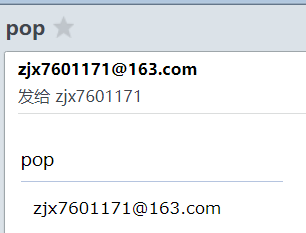


发送完成后quit推出smtp服务器。

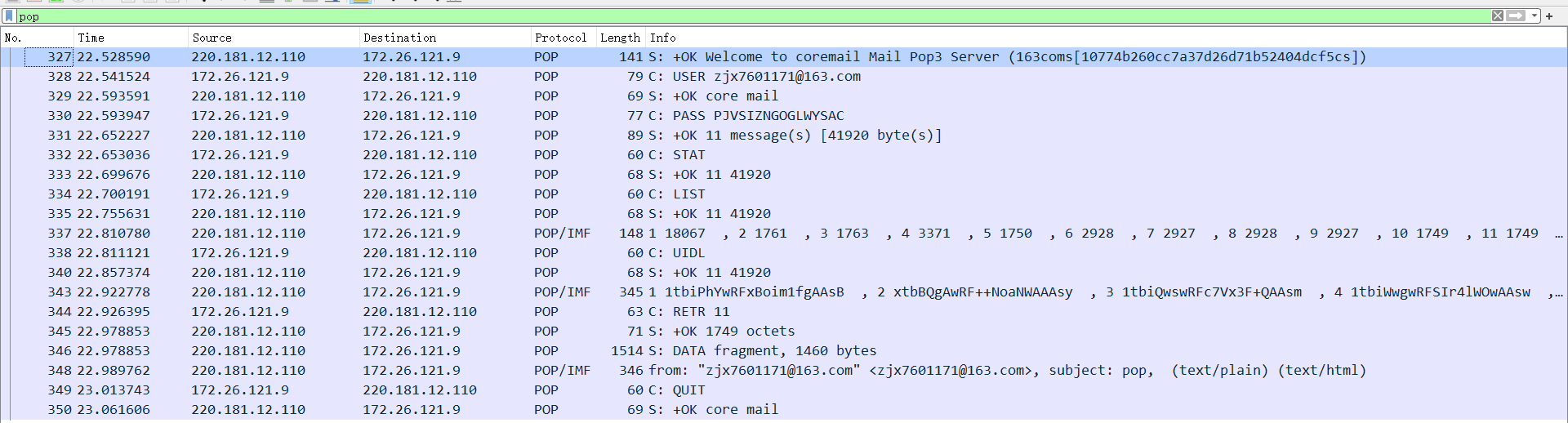


前面三个是三次握手，后面四个是四次挥手，中间的是数据。

POP：

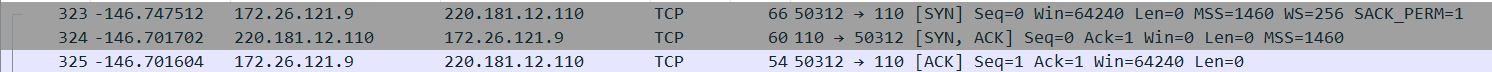


输入pop捕获：



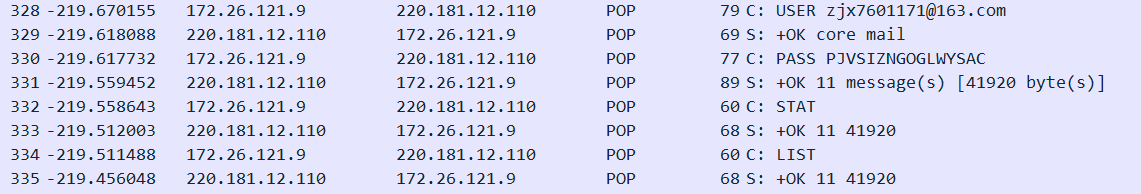
wireshark显示出了从客户端服务器之间三次握手建立tcp连接，到pop3认证，处理，更新，最后以tcp四次挥手结束这个过程的数据包。

(1) 由于POP3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。



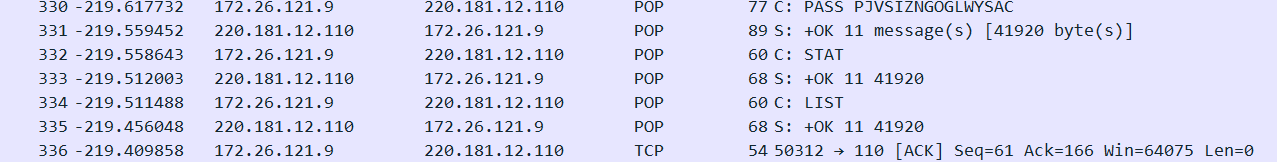
(2)客户端和服务器建立连接之后，pop3服务器会向pop3客户端吧发送一条消息，通知客户端服务器已经准备好了，客户端开始进行认证阶段。

(3) 客户端进入认证阶段后，向服务器发送 user xxx@qq.com，回车，pass 授权码（注意不是邮箱的登录密码），回车，服务器返回ok，表明认证成功，客户端由认证阶段进入处理阶段。



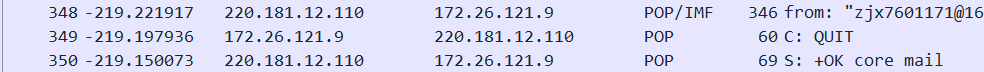
(4)处理阶段

客户端向服务器发送命令码list，服务器返回命令执行的状态（+ok表示命令执行成功，-err表示命令执行失败），邮件数量和每个邮件的大小。

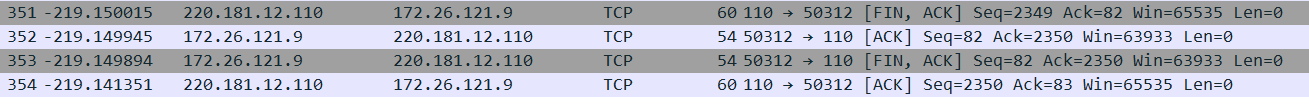


客户端向服务器发送命令码retr 28，表示客户端请求28标识的邮件的全部文本内容，服务器返回命令执行的状态以及28标识的邮件的全部内容。

客户端输入quit之后，退出处理状态进入更新状态，服务器将客户端标识为删除的邮件删除并退出pop3服务器。



(5)客户端服务器挥手断开连接。



问：什么情况下可以捕获POP或SMTP数据包？

答：发邮件时捕获到SMTP数据包，服务器采用pop协议然后收取邮件时会捕获到POP数据包。

1. **实验结果与分析**

**暨南大学本科实验报告专用纸(附页)**