北京邮电大学实验报告

<table>
<tr><td>实验名称</td><td colspan="2">计算机网络实验一</td><td>学 院</td><td>网络空间
安全学院</td><td>指导教师</td><td>刘建毅</td></tr>
<tr><td>班 级</td><td>班内序号</td><td colspan="2">学 号</td><td>学生姓名</td><td colspan="2">成绩</td></tr>
<tr><td>2022211801</td><td>4</td><td colspan="2">2022211570</td><td>项 枫</td><td colspan="2"></td></tr>
<tr><td>实验内容</td><td colspan="6">1、使用 Wireshark 软件捕获 HTTP 消息，分析其消息头，理解 HTTP 的通信原理；

2、使用 Wireshark 软件捕获一次从客户端发送 Email 的过程，分析 SMTP 消息，理解 Email 系统中发送邮件的通信原理；

3、使用 Telnet 软件访问 Email 服务器，输入 SMTP 命令与 Email 服务器交互，理解 SMTP 的通信过程和 Base64 编码的概念。</td></tr>
<tr><td>学生实验报告
(附页)</td><td colspan="6"></td></tr>
<tr><td>实验成绩评定</td><td colspan="6">评语：

成绩：
指导教师签名：

年 月 日</td></tr>
</table>

注：评语要体现每个学生的工作情况，可以加页。

一、实验内容

1、使用 Wireshark 软件捕获 HTTP 消息，分析其消息头，理解 HTTP 的通信原理；

2、使用 Wireshark 软件捕获一次从客户端发送 Email 的过程，分析 SMTP 消息，理解 Email 系统中发送邮件的通信原理；

3、使用 Telnet 软件访问 Email 服务器，输入 SMTP 命令与 Email 服务器交互，理解 SMTP 的通信过程和 Base64 编码的概念。

二、实验环境

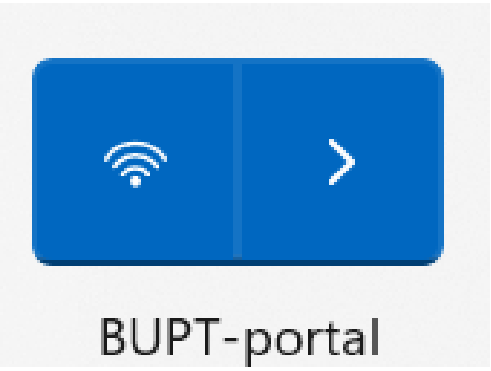
一台装有 MS Windows 系列操作系统的计算机，能够连接到因特网，并安装 Wireshark 软件。

三、实验步骤

（一）准备工作

1、下载 Wireshark 软件并了解其功能和使用方法。

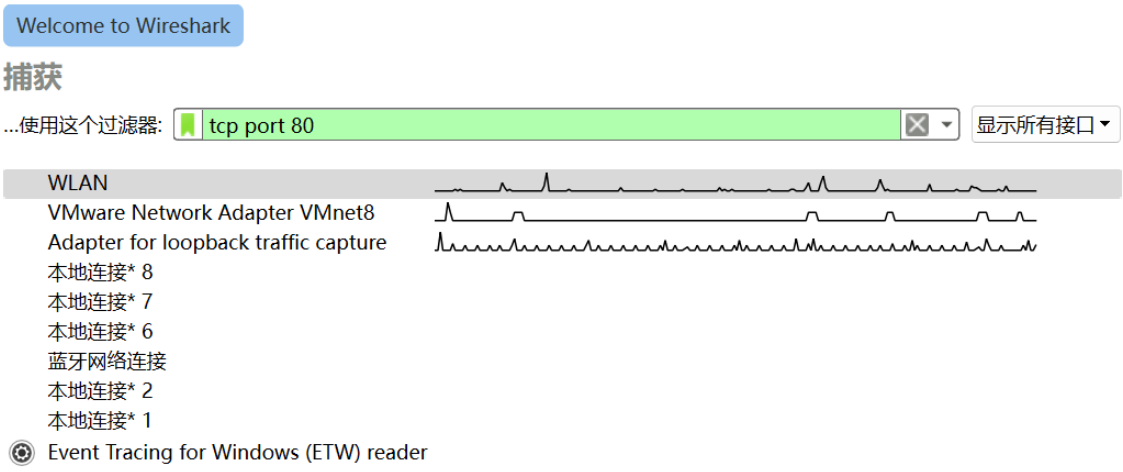
2、确保计算机已经连接到网络。



（二）捕获 HTTP 协议数据

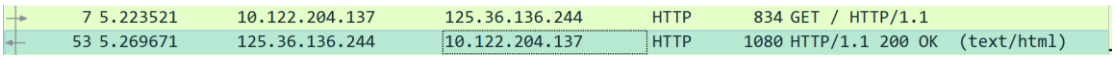
1、清除浏览器 cookie 数据。

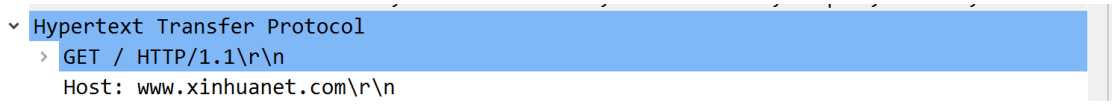
2、启动 Wireshark，选择捕获接口为 WLAN ，设置捕获过滤器为 tcp port 80。

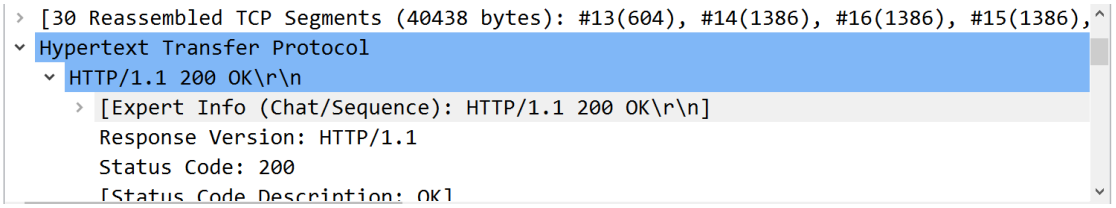


3、用浏览器打开 http://www.xinhuanet.com/。

4、抓包捕获 HTTP 协议数据。

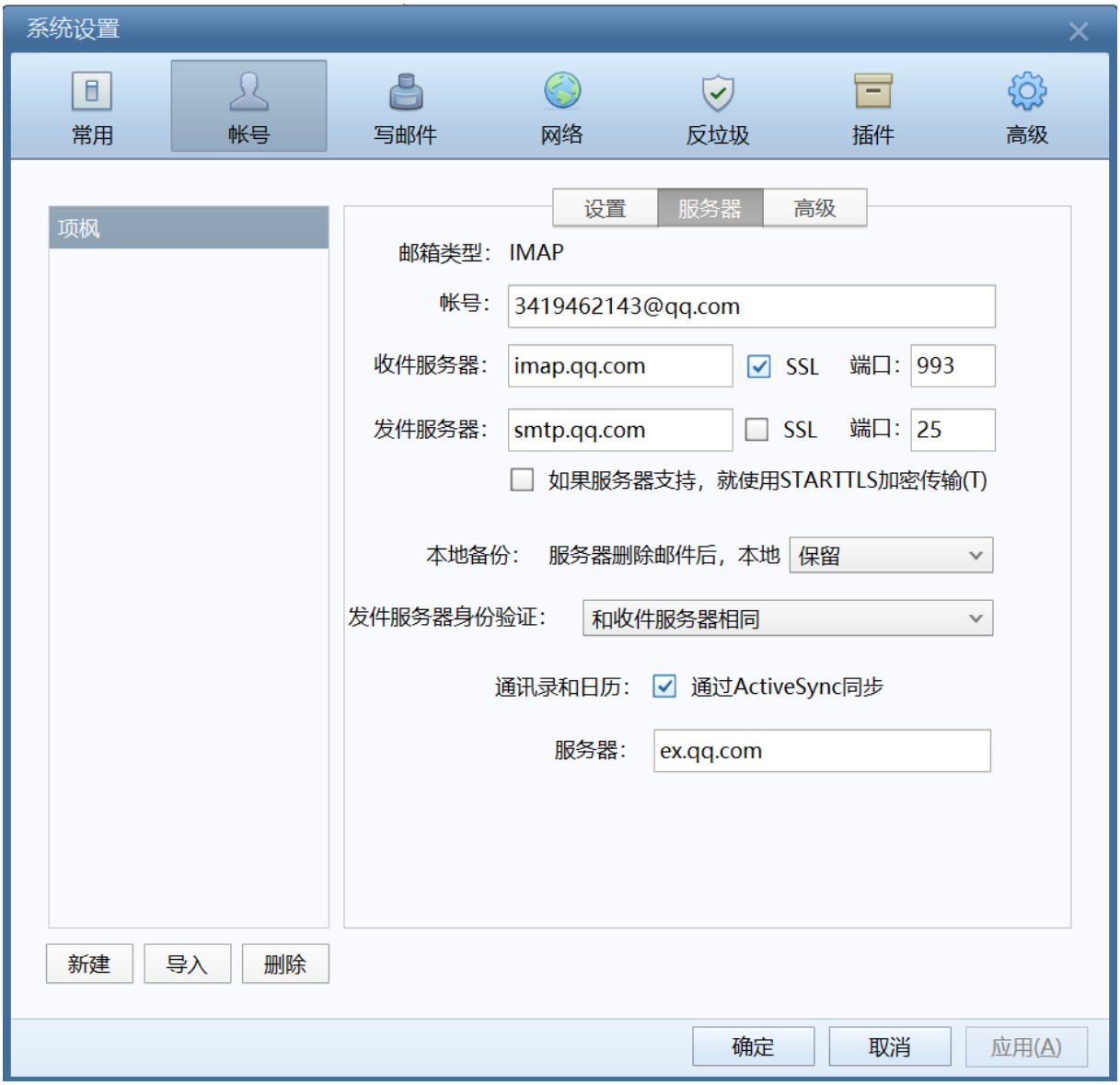






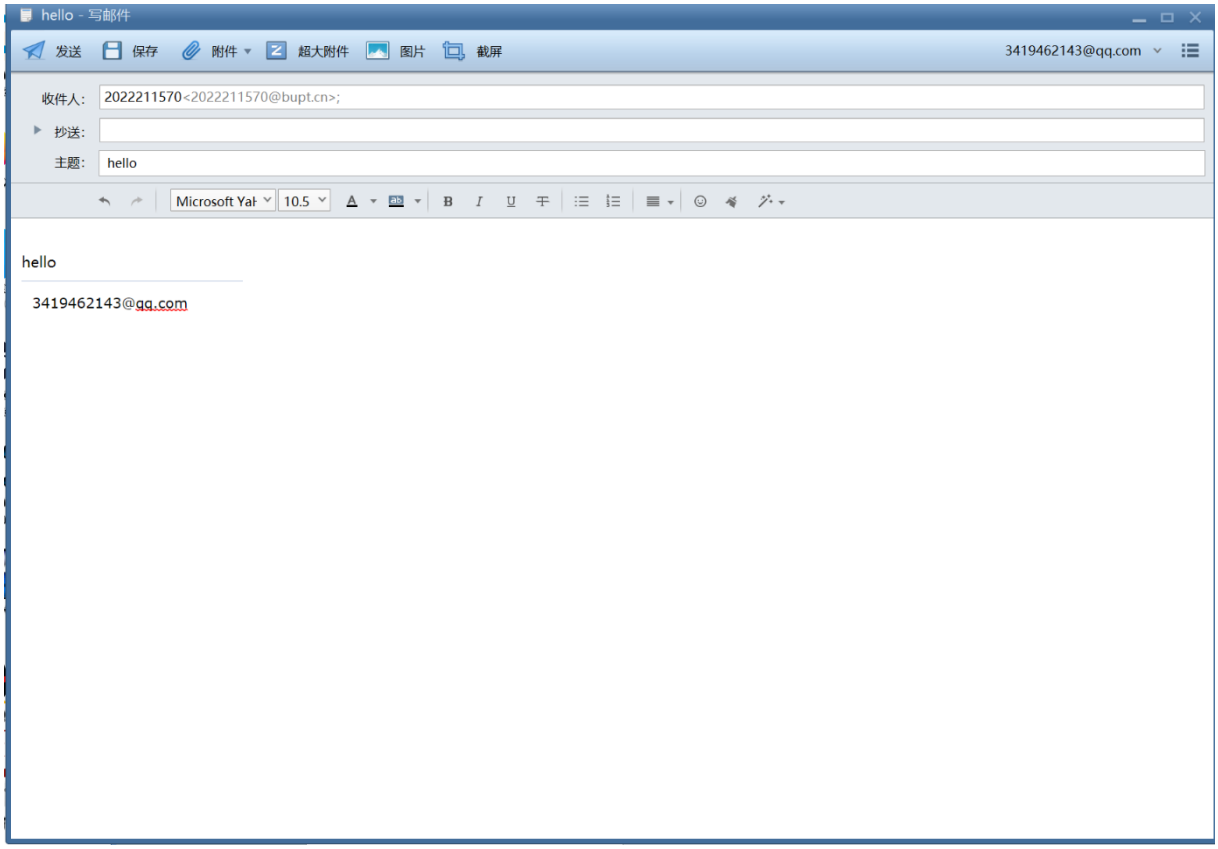
（三）捕获 SMTP 协议数据

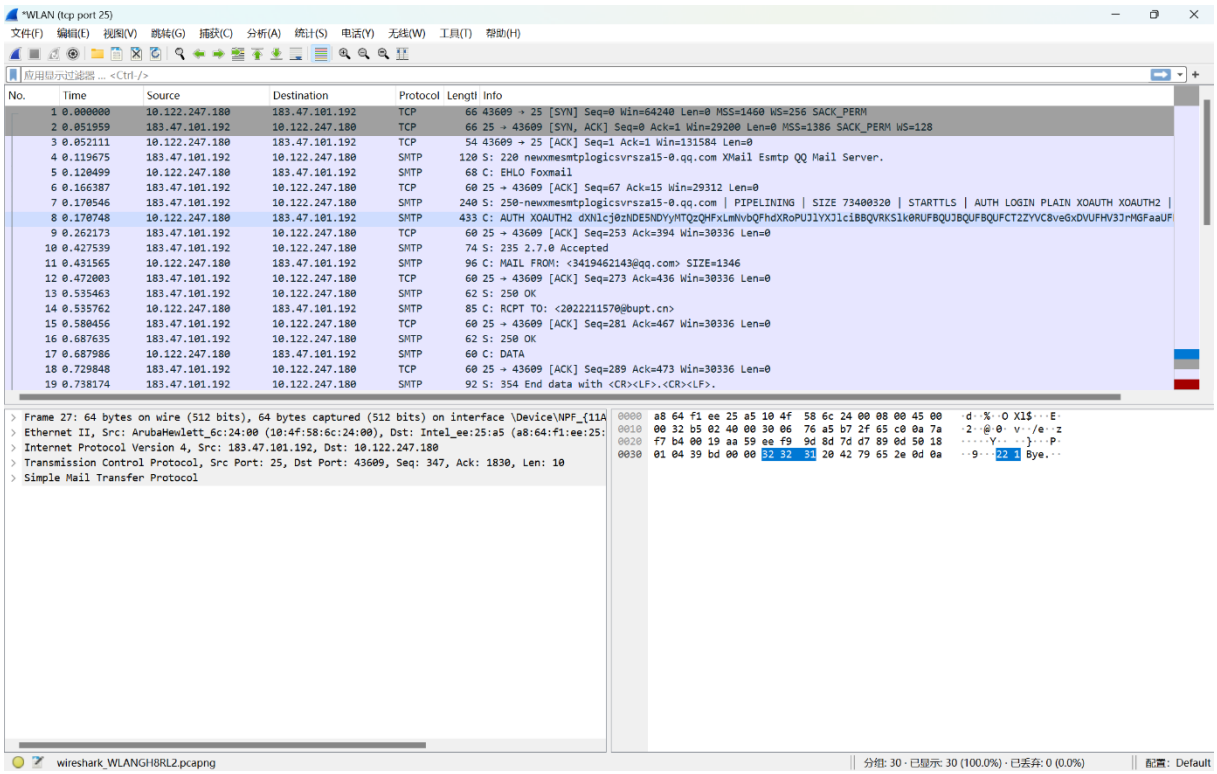
1、下载并安装邮件客户端软件 Foxmail，配置用户账户，设置发件服务器不选择 SSL， 端口为 25。



2、配置 wireshark ，设置捕获过滤器为 tcp port 25。

3、开始捕获，用 Foxmail 发送一封邮件，邮件发送成功后停止捕获。

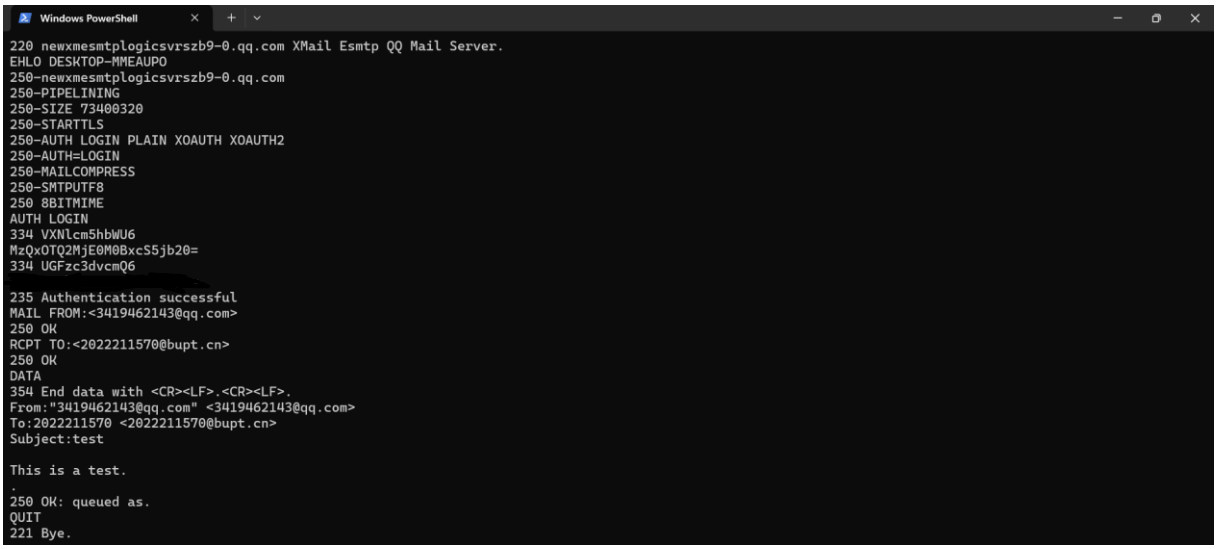




（四）使用 SMTP 命令与邮件服务器交互

1、在命令行模式，使用 telnet 程序连接到发件服务器。

2、在新窗口中，输入 SMTP 命令，与邮件服务器交互。



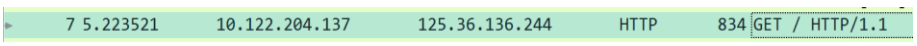
四、协议分析

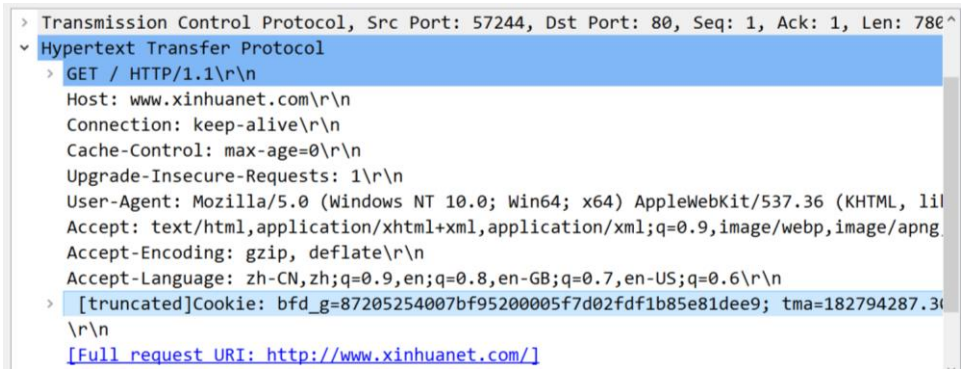
（一）HTTP 协议分析

1、设置了 tcp port 80，捕捉到的数据没有 DNS 类型的请求。浏览器先分析 URL 得到域名，再根据 DNS 得到新华网服务器的 IP 地址。

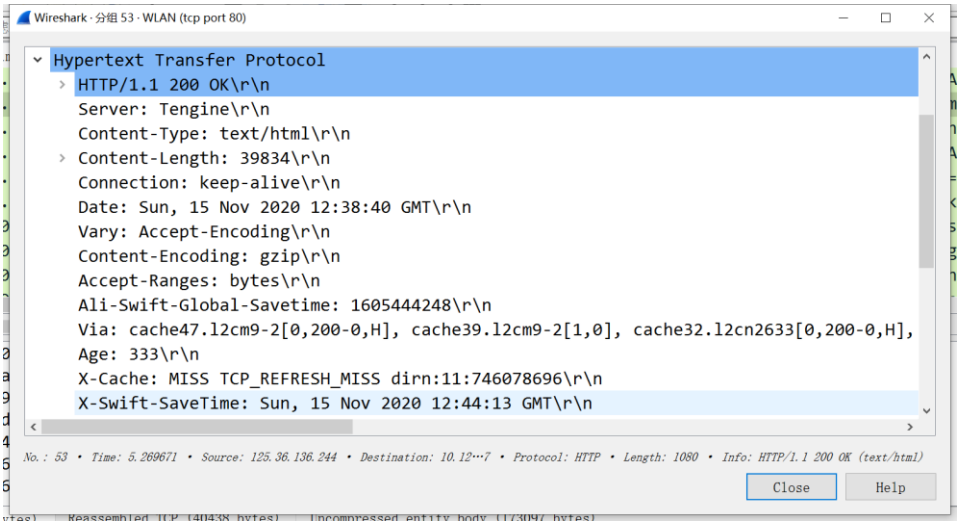
2、然后发生了 TCP 连接过程。发生了 TCP 三次握手，建立了本机和新华网服务器的 TCP 连接。

3、建立的 TCP 连接后，浏览器向服务器发送了 HTTP 类型的 GET 请求。GET 为 http 的方法，用于从服务器上下载 URL 对应的网页，接着每个 HTTP 消息头及其值如下图：





4、新华网的服务器接收到请求后，对于请求进行回应 200 OK，其中包含了网页文件的数据，消息头及其值如下图：

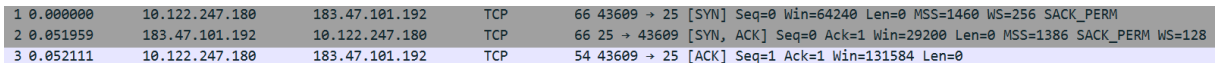


5、请求与应答消息中的各个字段与消息头的功能列表如下：

Host	请求	Web 服务器的域名
Cache-Control	请求	指定请求和响应遵循的缓存机制
Connection	两个消息都有	TCP 连接的类型
Upgrade	两个消息都有	发送方要使用的协议
User-Agent	请求	浏览器的类型
Accept	请求	浏览器能处理的网页类型
Accept-Encoding	请求	浏览器能处理的网页编码类型
Accept-Language	请求	浏览器能处理的自然语言
Server	响应	Web 服务器的类型
Date	两个消息都有	消息发送的日期时间
Content-type	响应	网页的 MIME 类型
Expires	响应	指定一个日期/时间
Transfer-Encoding	响应	表示实体传输给用户的编码形式
Location	响应	通知客户将请求发送给别的服务器
Content-Encoding	响应	内容的编码类型
Content-Language	响应	网页中的自然语言类型

（二）SMTP 协议分析

1、根据 ACK 和 SYN 确定第 1、2、3 行为客户与邮件服务器之间建立 TCP 连接。



2、第 4 行的数据是为服务器的回复：

```
4 0.119675      183.47.101.192      10.122.247.180      SMTP      120 S: 220 newxmesmtplogicsvrsza15-0.qq.com XMail Esmtp QQ Mail Server.
```

Server.表示可以提供服务并表明了邮件系统

3、第 5 行客户端接收到后回复 EHLO 通知发件人的邮件服务器域名，再加上操作 PC 信息，之后服务器端回复 250 表示连接成功

```
5 0.120499      10.122.247.180      183.47.101.192      SMTP      68 C: EHLO Foxmail
6 0.166387      183.47.101.192      10.122.247.180      TCP       60 25 → 43609 [ACK] Seq=67 Ack=15 Win=29312 Len=0
7 0.170546      183.47.101.192      10.122.247.180      SMTP      240 S: 250-newxmesmtplogicsvrsza15-0.qq.com | PIPELINING | SIZE 73400320 | STARTTLS | AUTH LOGIN PLAIN XOAUTH XOAUTH2 | AUTH…
```

4、第 8 行为用户发送 AUTH 用户登录命令给服务器。

```
8 0.170748      10.122.247.180      183.47.101.192      SMTP      433 C: AUTH XOAUTH2 dXNlcj0zNDE5NDYyMTQzQHFxLmNvbQFhdXRoPUJlYXJlciBBQVRKSlk0RUFBQUJBQUFBQUFCT2ZYVC8veGxDVUFHV3JrMGFaaUF
```

5、用户通过使用用户名和密码登录服务器，第 10 行中服务器回复 235，表示登陆成功 。

```
10 0.427539      183.47.101.192      10.122.247.180      SMTP      74 S: 235 2.7.0 Accepted
```

6、第 11 行是客户端发送 MAIL FROM，声明写信人的邮件地址，准备传输。之后第 13 行服务器回复 250 OK 表示命令成功。

```
11 0.431565      10.122.247.180      183.47.101.192      SMTP      96 C: MAIL FROM: <3419462143@qq.com> SIZE=1346
12 0.472003      183.47.101.192      10.122.247.180      TCP       60 25 → 43609 [ACK] Seq=273 Ack=436 Win=30336 Len=0
13 0.535463      183.47.101.192      10.122.247.180      SMTP      62 S: 250 OK
```

7、第 14 行客户端发送 RCPT TO 命令，注明收信人的地址。之后 16 行服务器回复 250 OK 表示命令成功。

```
14 0.535762      10.122.247.180      183.47.101.192      SMTP      85 C: RCPT TO: <2022211570@bupt.cn>
15 0.580456      183.47.101.192      10.122.247.180      TCP       60 25 → 43609 [ACK] Seq=281 Ack=467 Win=30336 Len=0
16 0.687635      183.47.101.192      10.122.247.180      SMTP      62 S: 250 OK
```

8、第 17 行客户端发送 DATA 命令通知正文开始，之后服务器回复 354，通知客户端可以发送正文了。

```
17 0.687986      10.122.247.180      183.47.101.192      SMTP      60 C: DATA
18 0.729848      183.47.101.192      10.122.247.180      TCP       60 25 → 43609 [ACK] Seq=289 Ack=473 Win=30336 Len=0
19 0.738174      183.47.101.192      10.122.247.180      SMTP      92 S: 354 End data with <CR><LF>.<CR><LF>.
```

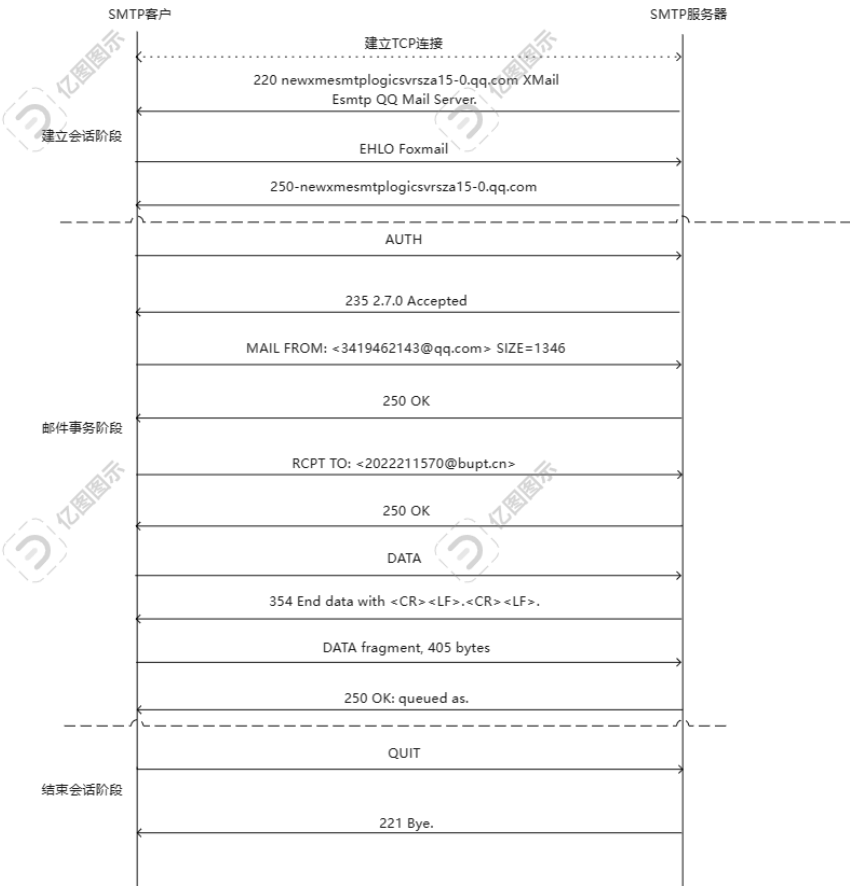
9、第 20 行客户端开始发送正文，并标明正文的大小，之后 24 行服务器发送 250 OK 表示确认收到了邮件。

```
20 0.738798      10.122.247.180      183.47.101.192      SMTP      459 C: DATA fragment, 405 bytes
21 0.841539      183.47.101.192      10.122.247.180      TCP       60 25 → 43609 [ACK] Seq=327 Ack=878 Win=31360 Len=0
22 0.841576      10.122.247.180      183.47.101.192      SMTP/I…   1000 from: "3419462143@qq.com" <3419462143@qq.com>, subject: hello,  (text/plain) (text/html)
23 0.882965      183.47.101.192      10.122.247.180      TCP       60 25 → 43609 [ACK] Seq=327 Ack=1824 Win=33280 Len=0
24 1.144768      183.47.101.192      10.122.247.180      SMTP      74 S: 250 OK: queued as.
```

10、第 25 行客户端发送 Quit 命令要求关闭 TCP 连接，之后 27 行显示服务器返回 221 Bye 表示服务器段结束传输，关闭 TCP。至此完成邮件传输。

```
25 1.145455      10.122.247.180      183.47.101.192      SMTP      60 C: QUIT
26 1.186137      183.47.101.192      10.122.247.180      TCP       60 25 → 43609 [ACK] Seq=347 Ack=1830 Win=33280 Len=0
27 1.193250      183.47.101.192      10.122.247.180      SMTP      64 S: 221 Bye.
```

11、画出通信的过程



五、实验结论和实验心得

（一）实验结论

两个应用层协议在运作时，首先都需要建立 TCP 连接，这就说明了下层为上层提供服务且脱离了传输层，应用层是无法运作的。

（二）实验心得

1、在进行 HTTP 协议分析时遇到了一些消息头不是教材中列出的部分消息头，于是我上网查找这些内容和功能。

2、在 SMTP 抓包时，最开始输入密码不正确，然后仔细阅读实验指导书发现是授权码。

3、通过实验，对这两个应用层协议在 C/S 交互中每一步的详细作用有了更深的理解，且掌握了使用 wireshark 进行简单抓包的技能。