华东师范大学数据科学与工程学院实验报告

课程名称：计算机网络与编程	**年级**：21 级	**上机实践成绩**：
指导教师：张召	**姓名**：杨茜雅	**学号**：10215501435
上机实践名称：Lab06		**上机实践日期**：2023.4.7
上机实践编号：6	**组号**：	**上机实践时间**：4.7-4.14

一、 实验目的

熟悉HTTP协议的工作原理
了解HTTP协议在实际网络中的运行过程
熟悉SMTP和POP3协议的工作原理
了解 SMTP 和 POP3 协议在实际网络中的运行过程

二、 实验任务

通过Wireshark分析HTTP协议
通过 Wireshark 分析 SMTP 和 POP3 协议

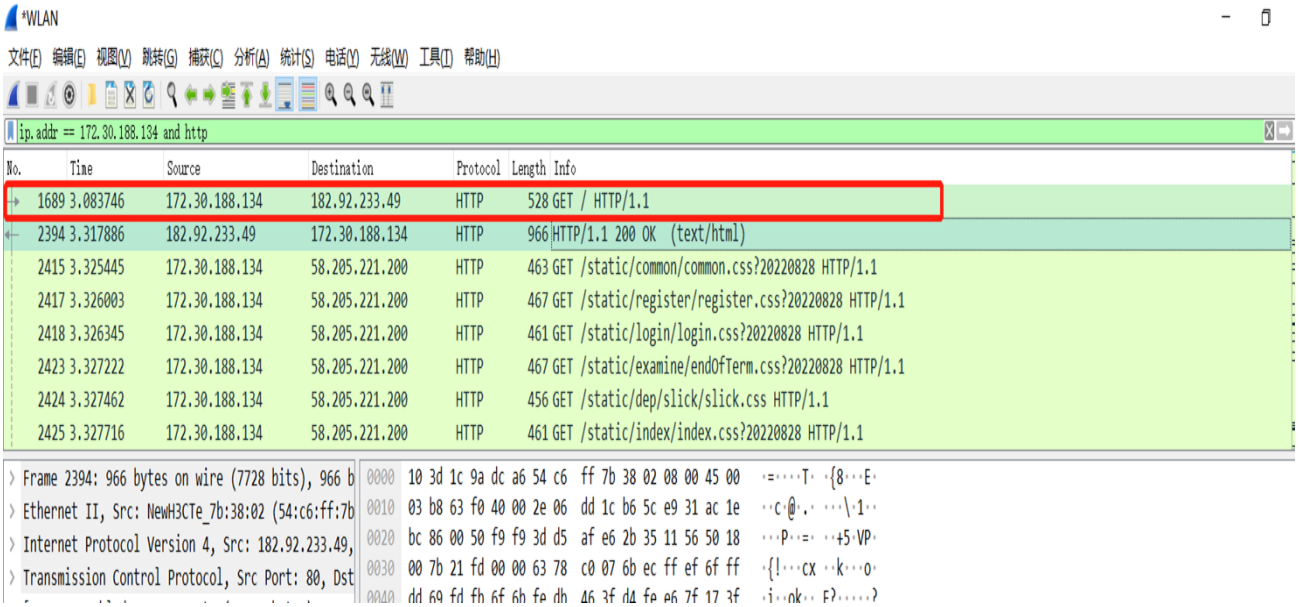
三、 使用环境

Wireshark

四、 实验过程

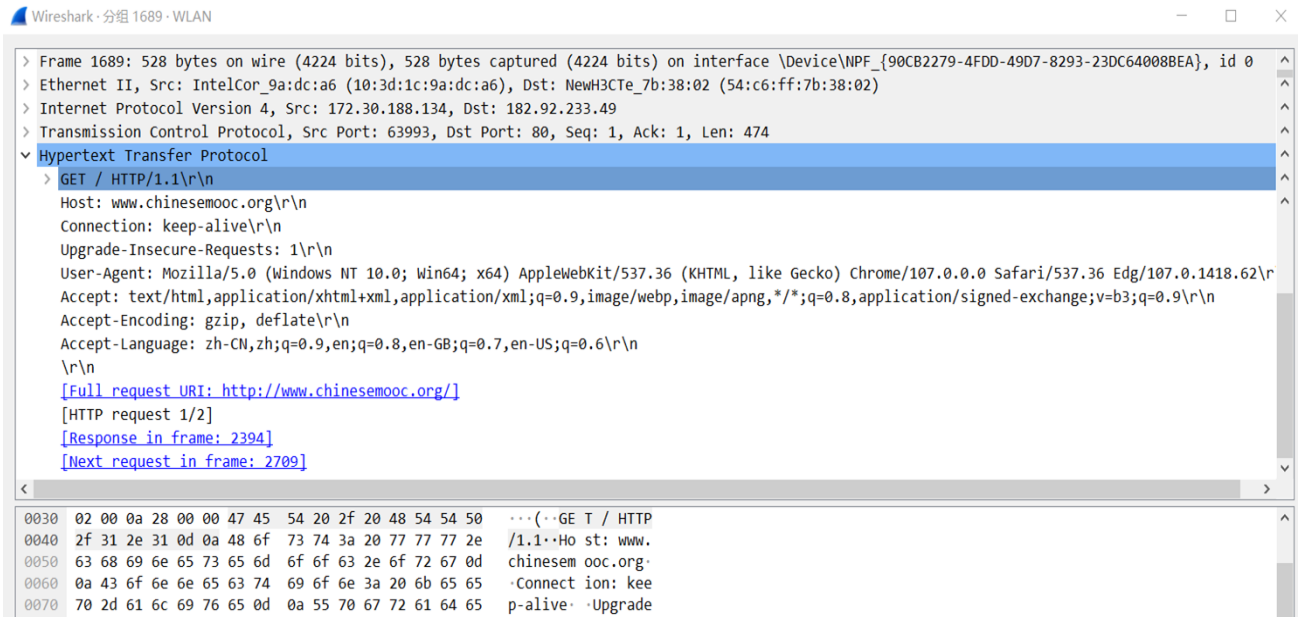
Task 1:
利用Wireshark抓取一条HTTP请求网络包，分析HTTP请求网络包的组成（要求根据报文结构正确标识每个部分），请将实验结果附在实验报告中。

为避免过多网络包影响分析，在显示过滤器栏输入ip.addr == 172.30.188.134 and http ，此时 Wireshark 会按照条件过滤网络包，我选择的 HTTP 请求网络包如下：



可以看出 info 为请求行，其中方法字段为 GET，是绝大部分 HTTP 请求报文使用的方法；URL 代表请求的对象，这里其实就是我们输入的网址 http://www.chinesemooc.org；HTTP 版本是 HTTP/1.1 版本。

接下来让我们看看网络包的组成：
HTTP 请求报文的全部内容为：



对照 HTTP 请求报文的通用格式：

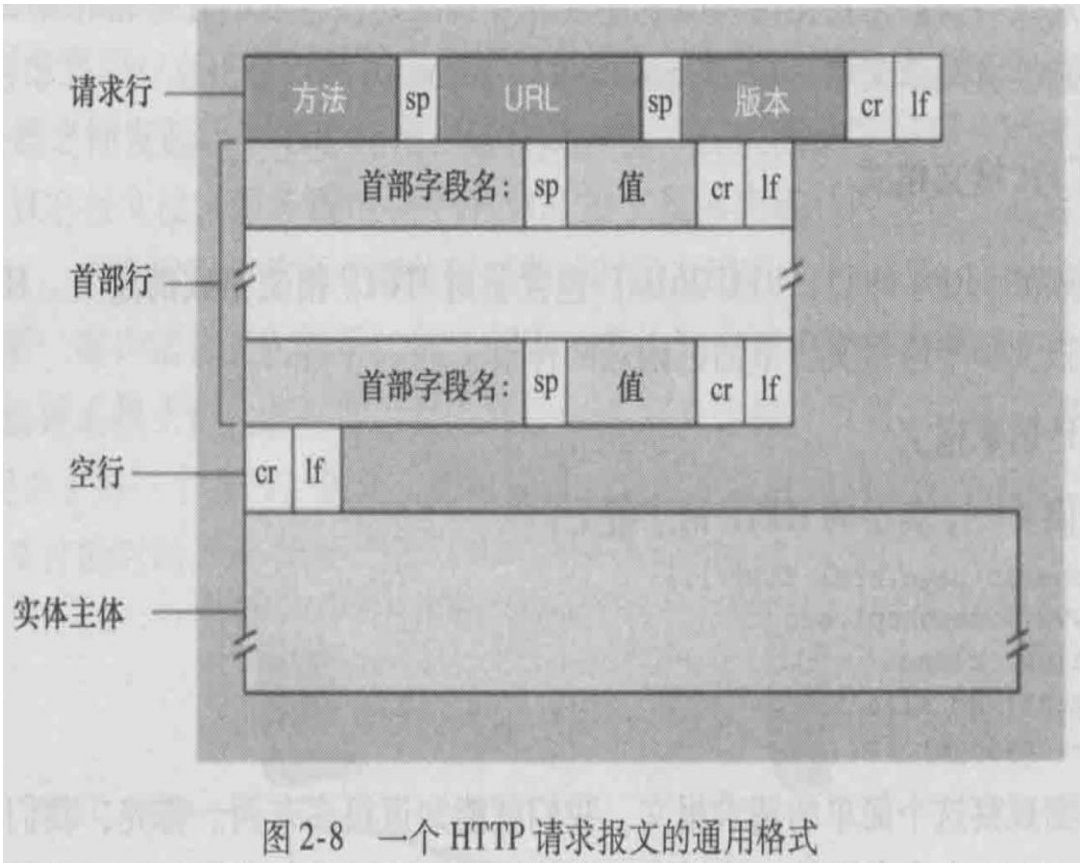
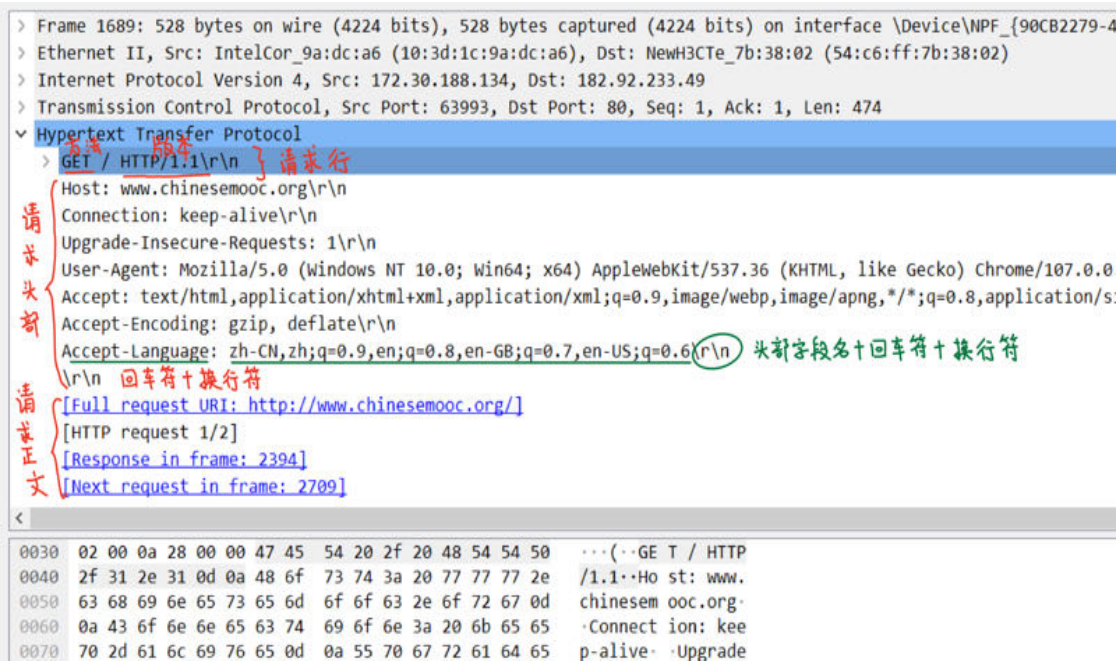


图 2-8　一个 HTTP 请求报文的通用格式

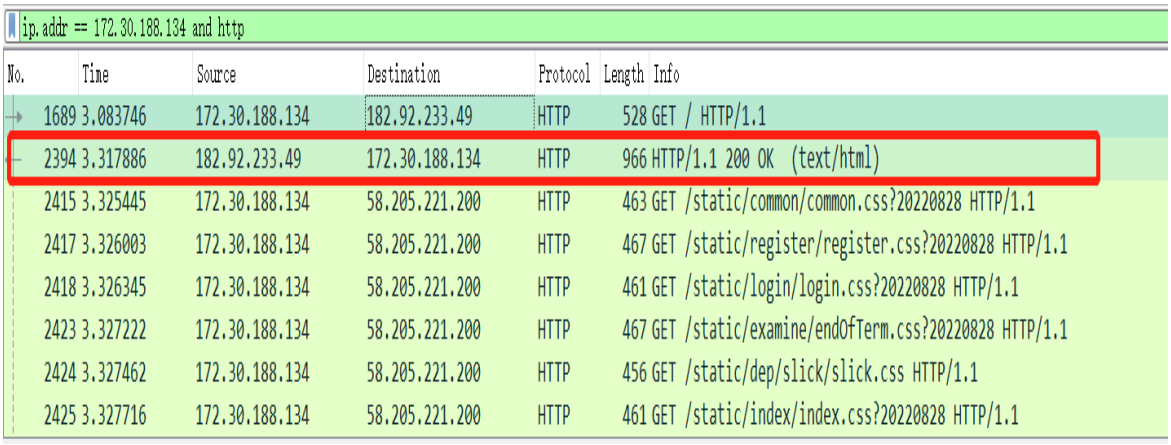
GET 方法的 HTTP 请求报文：



Task 2:

利用Wireshark找到上述请求网络包相对应的HTTP响应网络包，然后对比分析两个网络包的组成，请在实验报告中说明两者之间的区别。

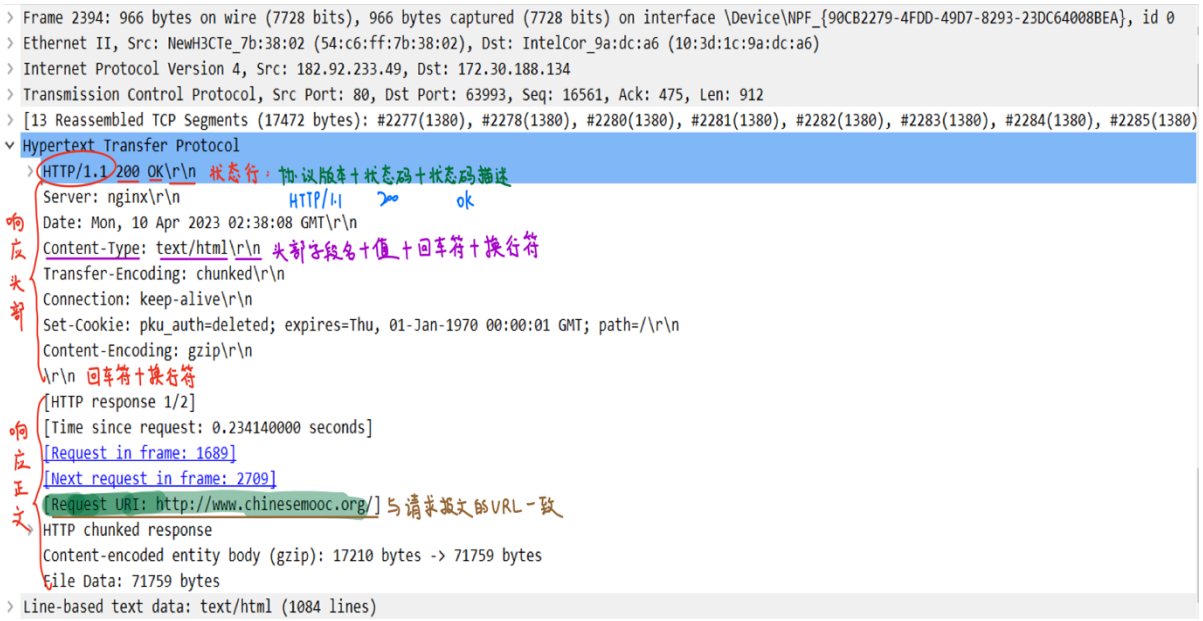
找到相对应的 HTTP 响应网络包：



对照 HTTP 相应报文的通用格式：

图2 HTTP响应报文

标识报文结构的每个部分：



对比两个网络包的组成，分析区别：
对比发现两者的主要区别在于请求行和状态行

请求行：


```
GET / HTTP/1.1\r\n
```

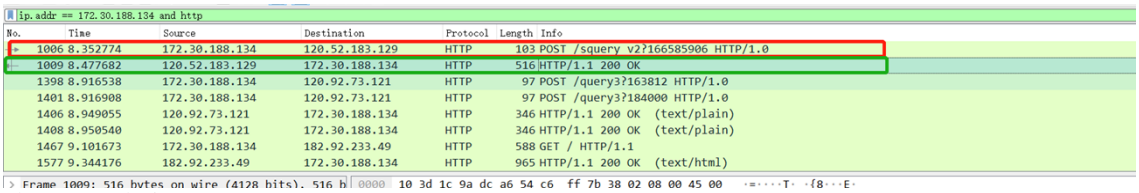
状态行


```
HTTP/1.1 200 OK  (text/html)
```

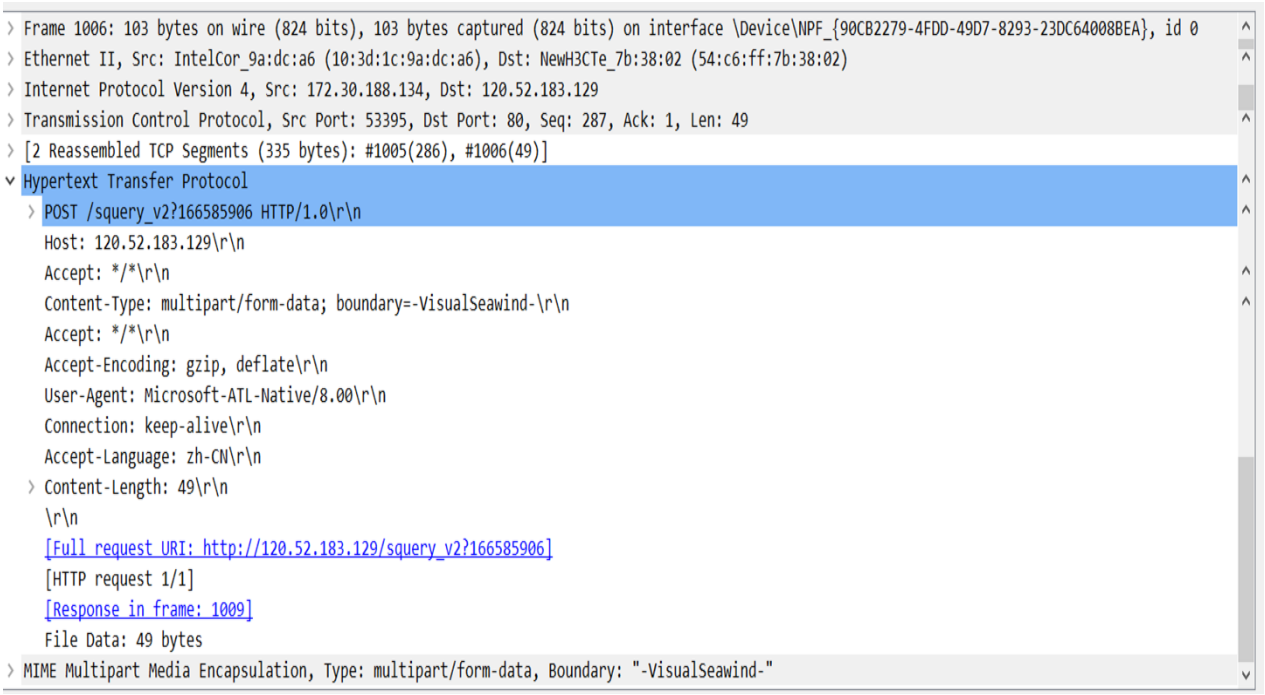
剩下的请求头部、请求正文以及响应头部、响应正文组成类似

Task 3：学习了解GET和POST方法，请在实验报告中分析对比GET和POST方法的请求报文，以及GET 和 POST 方法的和响应报文之间的区别。

POST 方法的请求和响应报文



请求报文内容如下：



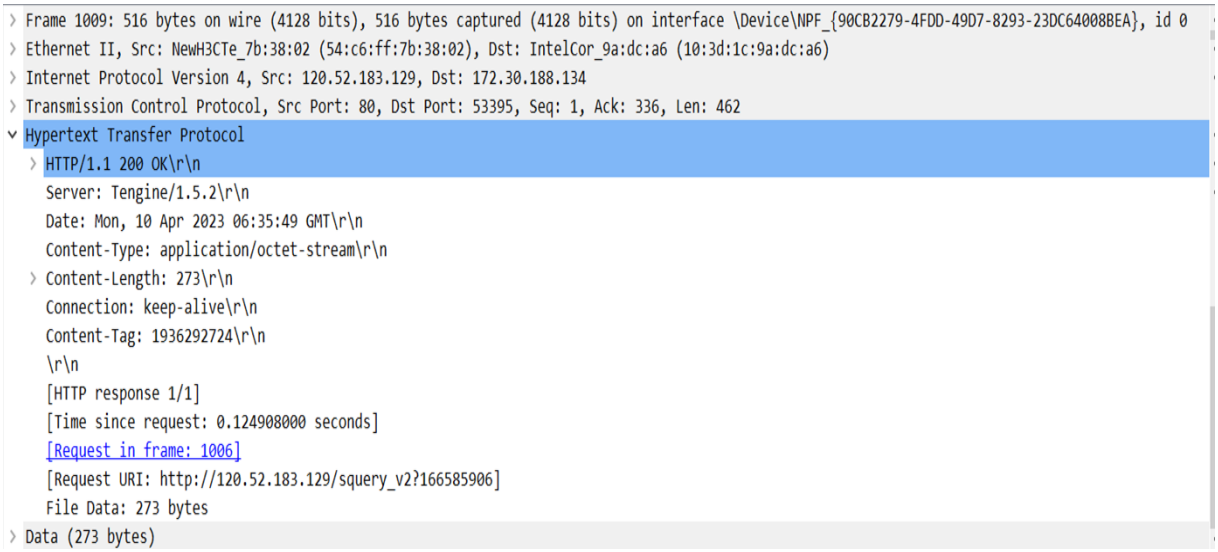
对比 GET 和 POST 方法的请求报文，可以发现：

1、 最直观的区别就是 GET 把参数包含在 URL 中，POST 通过 request body 传递参数。

2、 get 请求只能进行 url 编码（appliacation-x-www-form-urlencoded），post 请求支持多种（multipart/form-data 等）

3、 GET 比 POST 更不安全，因为参数直接暴露在 URL 上，所以不能用来传递敏感信息。

POST 方法的响应报文：



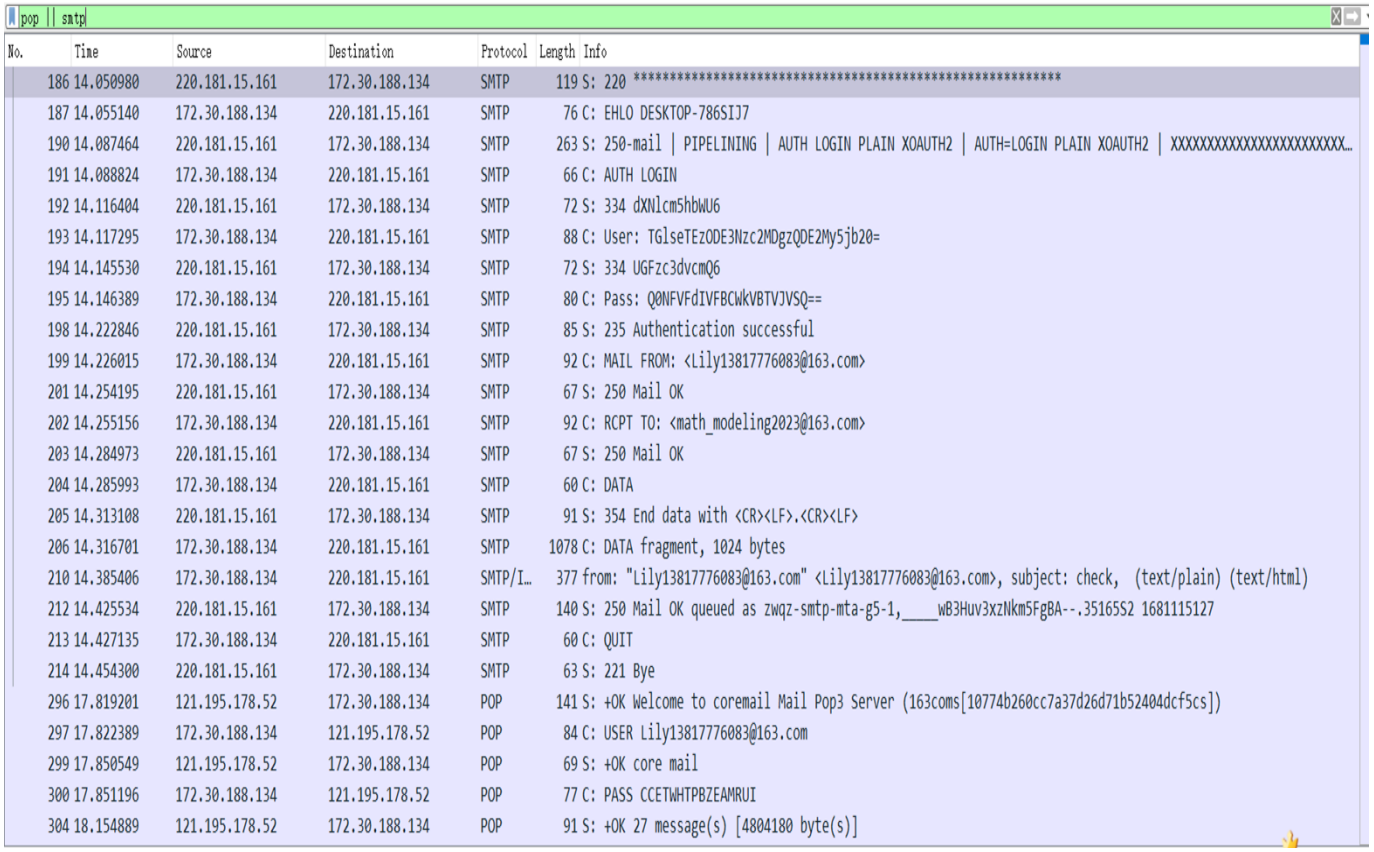
对比 GET 方法和 POST 方法的响应报文，可以发现：

1、 GET 表示从服务器获取资源，而POST 表示向指定的服务器资源提交数据。

2、 get 传送的数据量较小，不能大于2KB。post 传送的数据量较大，一般被默认为不受限制。

Task 4：利用Wireshark抓取SMTP和POP3网络包，分析SMTP和POP3数据包组成（要求根据报文结构正确标识每个部分），请将实验结果附在实验报告中。

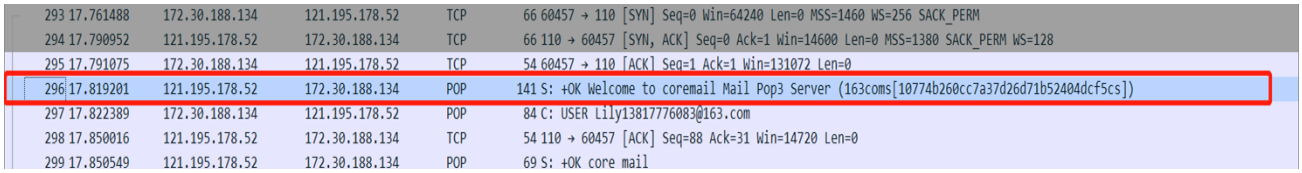
发送邮件后，利用Wireshark过滤SMTP和POP3协议的数据包



No.	Time	Source	Destination	Protocol	Length	Info
186	14.050980	220.181.15.161	172.30.188.134	SMTP	119	S: 220 **********
187	14.055140	172.30.188.134	220.181.15.161	SMTP	76	C: EHLO DESKTOP-786SIJ7
190	14.087464	220.181.15.161	172.30.188.134	SMTP	263	S: 250-mail | PIPELINING | AUTH LOGIN PLAIN XOAUTH2 | AUTH=LOGIN PLAIN XOAUTH2 | XXXXXXXXXXXXXXXXXXXXXXX…
191	14.088824	172.30.188.134	220.181.15.161	SMTP	66	C: AUTH LOGIN
192	14.116404	220.181.15.161	172.30.188.134	SMTP	72	S: 334 dXNlcm5hbWU6
193	14.117295	172.30.188.134	220.181.15.161	SMTP	88	C: User: TGlseTEzODE3Nzc2MDgzQDE2My5jb20=
194	14.145530	220.181.15.161	172.30.188.134	SMTP	72	S: 334 UGFzc3dvcmQ6
195	14.146389	172.30.188.134	220.181.15.161	SMTP	80	C: Pass: Q0NFVFdIVFBCWkVBTVJVSQ==
198	14.222846	220.181.15.161	172.30.188.134	SMTP	85	S: 235 Authentication successful
199	14.226015	172.30.188.134	220.181.15.161	SMTP	92	C: MAIL FROM: <Lily13817776083@163.com>
201	14.254195	220.181.15.161	172.30.188.134	SMTP	67	S: 250 Mail OK
202	14.255156	172.30.188.134	220.181.15.161	SMTP	92	C: RCPT TO: <math_modeling2023@163.com>
203	14.284973	220.181.15.161	172.30.188.134	SMTP	67	S: 250 Mail OK
204	14.285993	172.30.188.134	220.181.15.161	SMTP	60	C: DATA
205	14.313108	220.181.15.161	172.30.188.134	SMTP	91	S: 354 End data with <CR><LF>.<CR><LF>
206	14.316701	172.30.188.134	220.181.15.161	SMTP	1078	C: DATA fragment, 1024 bytes
210	14.385406	172.30.188.134	220.181.15.161	SMTP/I…	377	from: "Lily13817776083@163.com" <Lily13817776083@163.com>, subject: check, (text/plain) (text/html)
212	14.425534	220.181.15.161	172.30.188.134	SMTP	140	S: 250 Mail OK queued as zwqz-smtp-mta-g5-1,____wB3Huv3xzNkm5FgBA--.35165S2 1681115127
213	14.427135	172.30.188.134	220.181.15.161	SMTP	60	C: QUIT
214	14.454300	220.181.15.161	172.30.188.134	SMTP	63	S: 221 Bye
296	17.819201	121.195.178.52	172.30.188.134	POP	141	S: +OK Welcome to coremail Mail Pop3 Server (163coms[10774b260cc7a37d26d71b52404dcf5cs])
297	17.822389	172.30.188.134	121.195.178.52	POP	84	C: USER Lily13817776083@163.com
299	17.850549	121.195.178.52	172.30.188.134	POP	69	S: +OK core mail
300	17.851196	172.30.188.134	121.195.178.52	POP	77	C: PASS CCETWHTPBZEAMRUI
304	18.154889	121.195.178.52	172.30.188.134	POP	91	S: +OK 27 message(s) [4804180 byte(s)]

通过追踪流得到具体的交互信息：

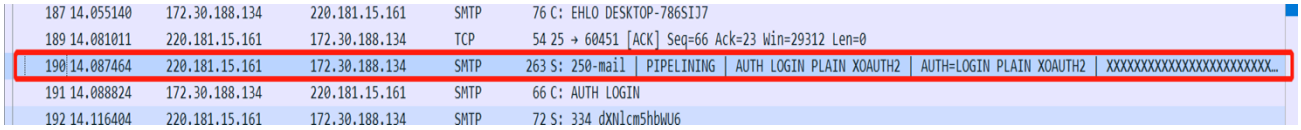
抓取POP3网络包：



293	17.761488	172.30.188.134	121.195.178.52	TCP	66	60457 → 110 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
294	17.790952	121.195.178.52	172.30.188.134	TCP	66	110 → 60457 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1380 SACK_PERM WS=128
295	17.791075	172.30.188.134	121.195.178.52	TCP	54	60457 → 110 [ACK] Seq=1 Ack=1 Win=131072 Len=0
296	17.819201	121.195.178.52	172.30.188.134	POP	141	S: +OK Welcome to coremail Mail Pop3 Server (163coms[10774b260cc7a37d26d71b52404dcf5cs])
297	17.822389	172.30.188.134	121.195.178.52	POP	84	C: USER Lily13817776083@163.com
298	17.850016	121.195.178.52	172.30.188.134	TCP	54	110 → 60457 [ACK] Seq=88 Ack=31 Win=14720 Len=0
299	17.850549	121.195.178.52	172.30.188.134	POP	69	S: +OK core mail

具体组成+分析如下：

抓取SMTP网络包：



具体组成+分析如下：

Wireshark · 追踪 TCP 流 (tcp.stream eq 24) · WLAN

```
220 ****************************************************************
EHLO DESKTOP-786SIJ7
250-mail
250-PIPELINING
250-AUTH LOGIN PLAIN XOAUTH2
250-AUTH=LOGIN PLAIN XOAUTH2
250-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXA
250-STARTTLS
250-XB
250 8BITMIME
AUTH LOGIN
334 dXNlcm5hbWU6
TGlseTEzODE3Nzc2MDgzQDE2My5jb20=
334 UGFzc3dvcmQ6
[redacted]
235 Authentication successful
MAIL FROM: <Lily13817776083@163.com>
250 Mail OK
RCPT TO: <math_modeling2023@163.com>
250 Mail OK
DATA
354 End data with <CR><LF>.<CR><LF>
Date: Mon, 10 Apr 2023 16:25:27 +0800
From: "Lily13817776083@163.com" <Lily13817776083@163.com>
To: math_modeling2023 <math_modeling2023@163.com>
Subject: check
X-Priority: 3
X-Has-Attach: no
X-Mailer: Foxmail 7.2.25.213[cn]
Mime-Version: 1.0
Message-ID: <202304101625269939761 3@163.com>
Content-Type: multipart/alternative;
        boundary="----=_001_NextPart450665583770_=----"

This is a multi-part message in MIME format.

------=_001_NextPart450665583770_=----
Content-Type: text/plain;
        charset="us-ascii"
Content-Transfer-Encoding: base64

DQpoZWxsbw0KDQoNCkxpbHkxMzgxNzc3NjA4M0AxNjMuY29tDQo=

------=_001_NextPart450665583770_=----
Content-Type: text/html;
        charset="us-ascii"
Content-Transfer-Encoding: quoted-printable

<html><head><meta http-equiv=3D"content-type" content=3D"text/html; charse=
t=3Dus-ascii"><style>body { line-height: 1.5; }body { font-size: 14px; fon=
t-family: "Microsoft YaHei UI"; color: rgb(0, 0, 0); line-height: 1.5; }</=
style></head><body>=0A<div><span></span><br></div>=0A<div>hello</div><hr s=
tyle=3D"width: 210px; height: 1px;" color=3D"#b5c4df" size=3D"1" align=3D"=
left">=0A<div><span><div style=3D"MARGIN: 10px; FONT-FAMILY: verdana; FONT=
-SIZE: 10pt"><div>Lily13817776083@163.com</div></div></span></div>=0A</bod=
y></html>
------=_001_NextPart450665583770_=------

.
250 Mail OK queued as zwqz-smtp-mta-g5-1,____wB3Huv3xzNkm5FgBA--.35165S2 1681115127
QUIT
221 Bye
```

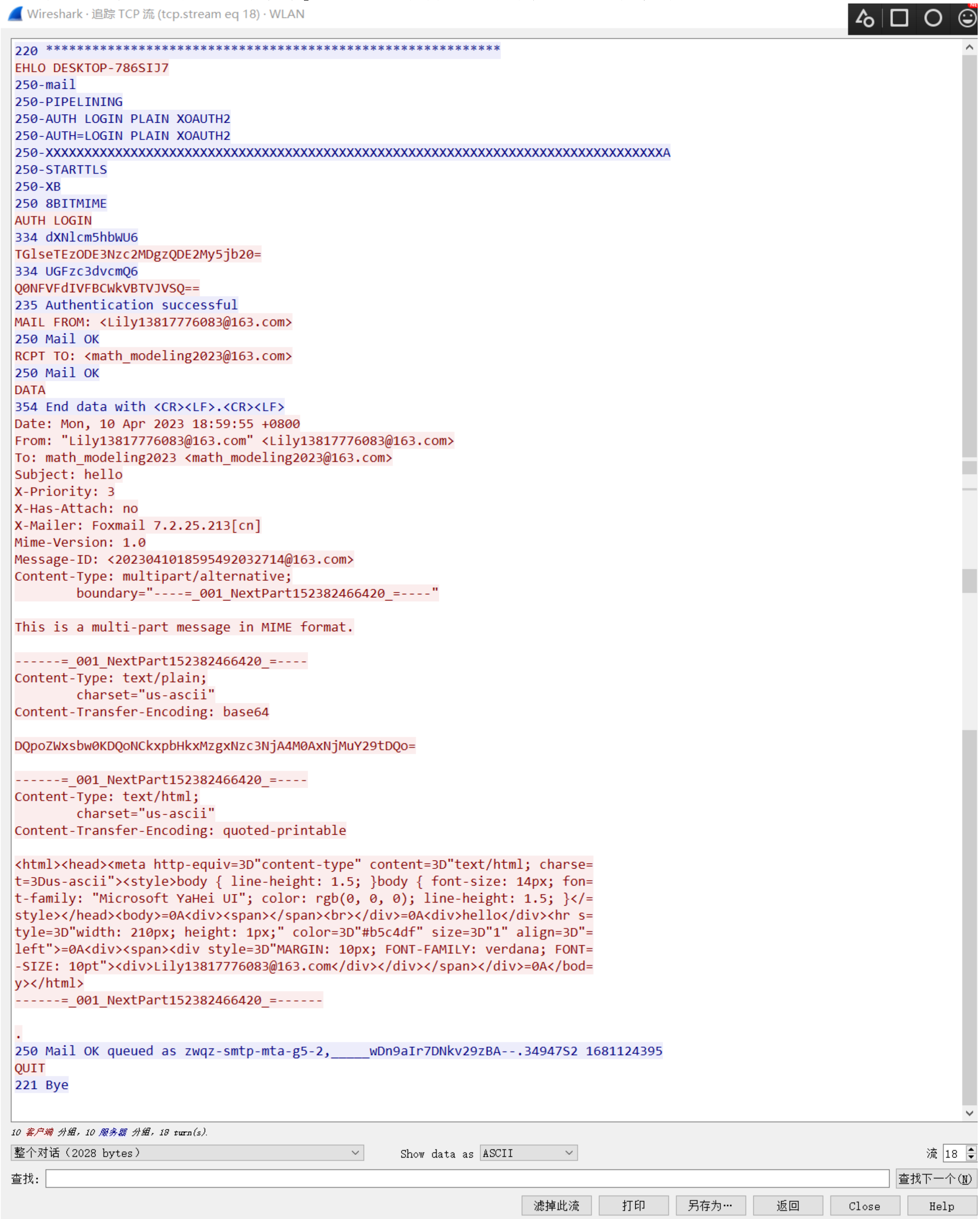
10 客户端 分组, 10 服务器 分组, 18 turn(s).

整个对话 (2028 bytes)　Show data as ASCII　流 24

查找:　查找下一个(N)

滤掉此流　打印　另存为…　返回　Close　Help

Task 5：利用Wireshark抓取SMTP网络包，分析一个在SMTP客户（C）和SMTP服务器（S）之间交换报文文本的例子（参考书本p77-78），请将实验结果附在实验报告中。



Wireshark · 追踪 TCP 流 (tcp.stream eq 18) · WLAN

```
220 ************************************************************
EHLO DESKTOP-786SIJ7
250-mail
250-PIPELINING
250-AUTH LOGIN PLAIN XOAUTH2
250-AUTH=LOGIN PLAIN XOAUTH2
250-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXA
250-STARTTLS
250-XB
250 8BITMIME
AUTH LOGIN
334 dXNlcm5hbWU6
TGlseTEzODE3Nzc2MDgzQDE2My5jb20=
334 UGFzc3dvcmQ6
Q0NFVFdIVFBCWkVBTVJVSQ==
235 Authentication successful
MAIL FROM: <Lily13817776083@163.com>
250 Mail OK
RCPT TO: <math_modeling2023@163.com>
250 Mail OK
DATA
354 End data with <CR><LF>.<CR><LF>
Date: Mon, 10 Apr 2023 18:59:55 +0800
From: "Lily13817776083@163.com" <Lily13817776083@163.com>
To: math_modeling2023 <math_modeling2023@163.com>
Subject: hello
X-Priority: 3
X-Has-Attach: no
X-Mailer: Foxmail 7.2.25.213[cn]
Mime-Version: 1.0
Message-ID: <2023041018595492032714@163.com>
Content-Type: multipart/alternative;
        boundary="----=_001_NextPart152382466420_=----"

This is a multi-part message in MIME format.

------=_001_NextPart152382466420_=----
Content-Type: text/plain;
        charset="us-ascii"
Content-Transfer-Encoding: base64

DQpoZWxsbw0KDQoNCkxpbHkxMzgxNzc3NjA4M0AxNjMuY29tDQo=

------=_001_NextPart152382466420_=----
Content-Type: text/html;
        charset="us-ascii"
Content-Transfer-Encoding: quoted-printable

<html><head><meta http-equiv=3D"content-type" content=3D"text/html; charse=
t=3Dus-ascii"><style>body { line-height: 1.5; }body { font-size: 14px; fon=
t-family: "Microsoft YaHei UI"; color: rgb(0, 0, 0); line-height: 1.5; }</=
style></head><body>=0A<div><span></span><br></div>=0A<div>hello</div><hr s=
tyle=3D"width: 210px; height: 1px;" color=3D"#b5c4df" size=3D"1" align=3D"=
left">=0A<div><span><div style=3D"MARGIN: 10px; FONT-FAMILY: verdana; FONT=
-SIZE: 10pt"><div>Lily13817776083@163.com</div></div></span></div>=0A</bod=
y></html>
------=_001_NextPart152382466420_=------

.
250 Mail OK queued as zwqz-smtp-mta-g5-2,_____wDn9aIr7DNkv29zBA--.34947S2 1681124395
QUIT
221 Bye
```

10 客户端 分组，10 服务器 分组，18 turn(s).

整个对话（2028 bytes）　Show data as ASCII　流 18

查找：　查找下一个(N)

滤掉此流　打印　另存为…　返回　Close　Help

S：220 **

C：EHLO DESKTOP-786SIJ7

S：250 Hello DESKTOP-786SIJ7，please to meet you

C：AUTH LOGIN

S：334 dXNlcm5hbWU6

C: MAIL FROM: <Lily13817776083@163.com>
S: 250 Mail OK
C: RCPT TO: <math_modeling@163.com>
S: 250 Mail OK
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: .
S: 250 Mail OK queued as zwqz-smtp-mta-g5-2,wDn9aIr7DNkv29ZBA--.34947S2 1681124395
C: QUIT
S: 221 Bye

五、 总结

通过本次实验，我熟悉了HTTP协议的工作原理，了解了HTTP协议在实际网络中的运行过程，熟悉了SMTP和POP3协议的工作原理，了解了SMTP和POP3协议在实际网络中的运行过程。同时实践上手通过Wireshark分析HTTP协议、SMTP和POP3协议，对书本上的理论知识有了更深刻的见解。