北京邮电大学实验报告

实验名称	计算机网络实验一	学 院	网络空间安全	指导教师	程莉
班 级	班内序号	学 号	学生姓名	成绩	
2021211805	06	2021212039	黄达威		
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。				
学生实验报告(附页)	《详见下方“实验报告”》				
实验成绩评定	评语： 成绩： 指导教师签名： 年　　月　　日				

注：评语要体现每个学生的工作情况，可以加页。

实验报告

目录

实验一 应用层协议消息的捕获和解析

1. 实验内容和实验步骤描述

1.1 实验目的

深入理解典型的应用层协议——HTTP 和 SMTP 的要点。

1.2 实验内容

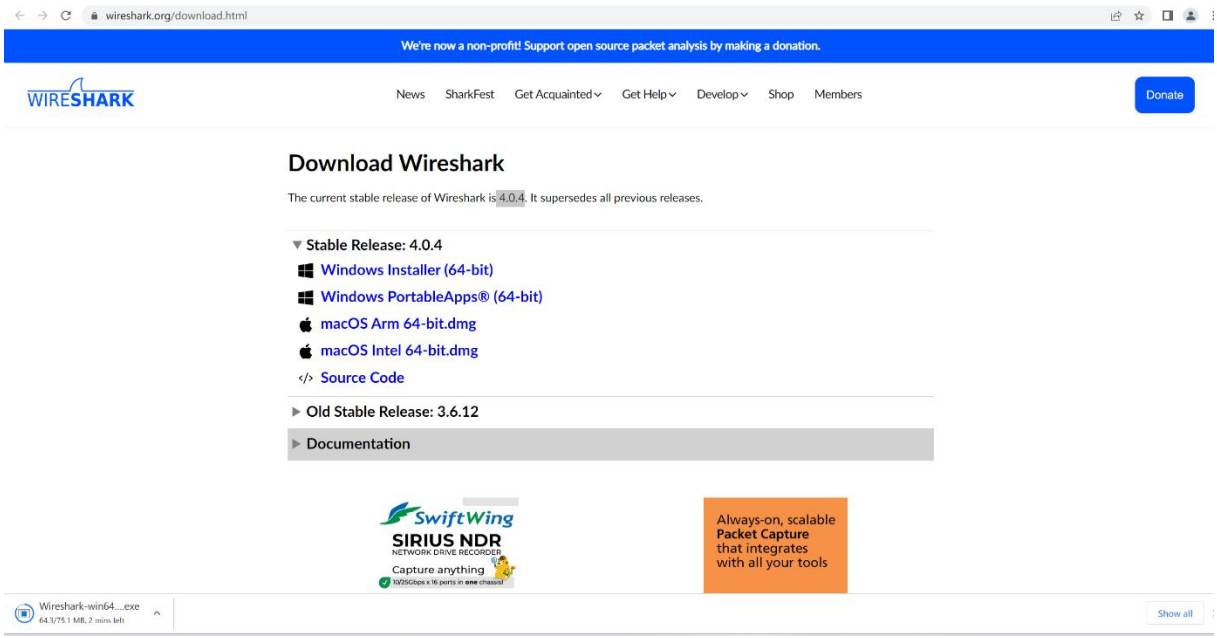
1） 使用 Wireshark 软件捕获 HTTP 消息，分析其消息头，理解 HTTP 的通信原理；
2） 使用 Wireshark 软件捕获一次从客户端发送 Email 的过程，分析 SMTP 消息，理解 Email 系统中 发送邮件的通信原理；
3）使用 Telnet 软件访问 Email 服务器，输入 SMTP 命令与 Email 服务器交互，理解 SMTP 的通信 过程和 Base64 编码的概念。

1.3 实验环境

- Microsoft Windows 11 *22H2*
- Wireshark *4.0.4*

1.4 实验步骤

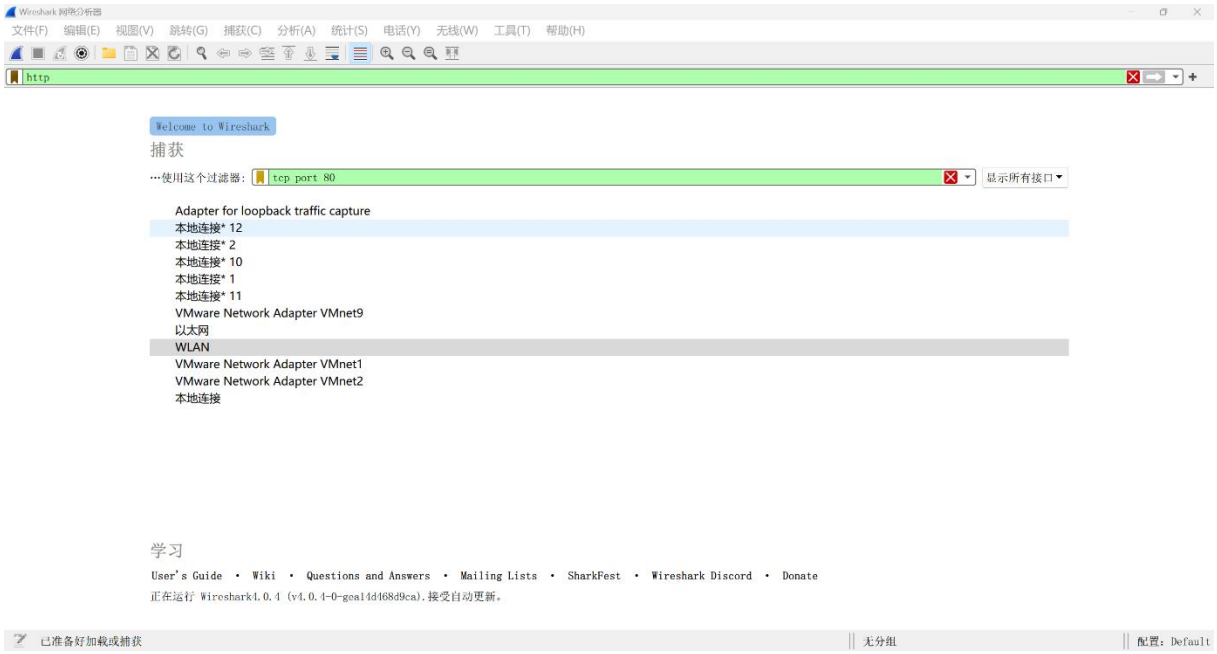
1）下载 Wireshark 软件并了解其功能和使用方法。



2） 确保计算机已经连接到网络

3）启动 Wireshark，选择捕获接口为联网的本机网卡（本地连接或 WLAN），设置合适的捕获
过滤器：

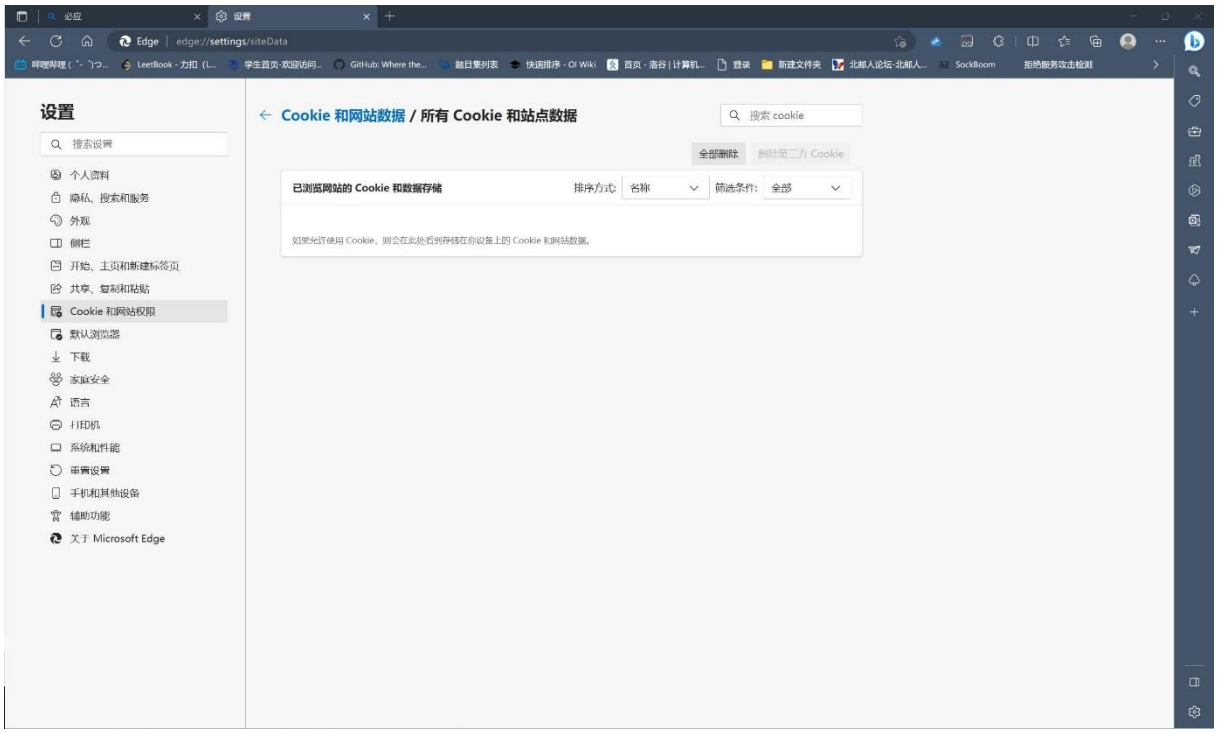
对于 HTTP 消息，设置捕获过滤器为 tcp port 80
对于 SMTP 消息，设置捕获过滤器为 tcp port 25

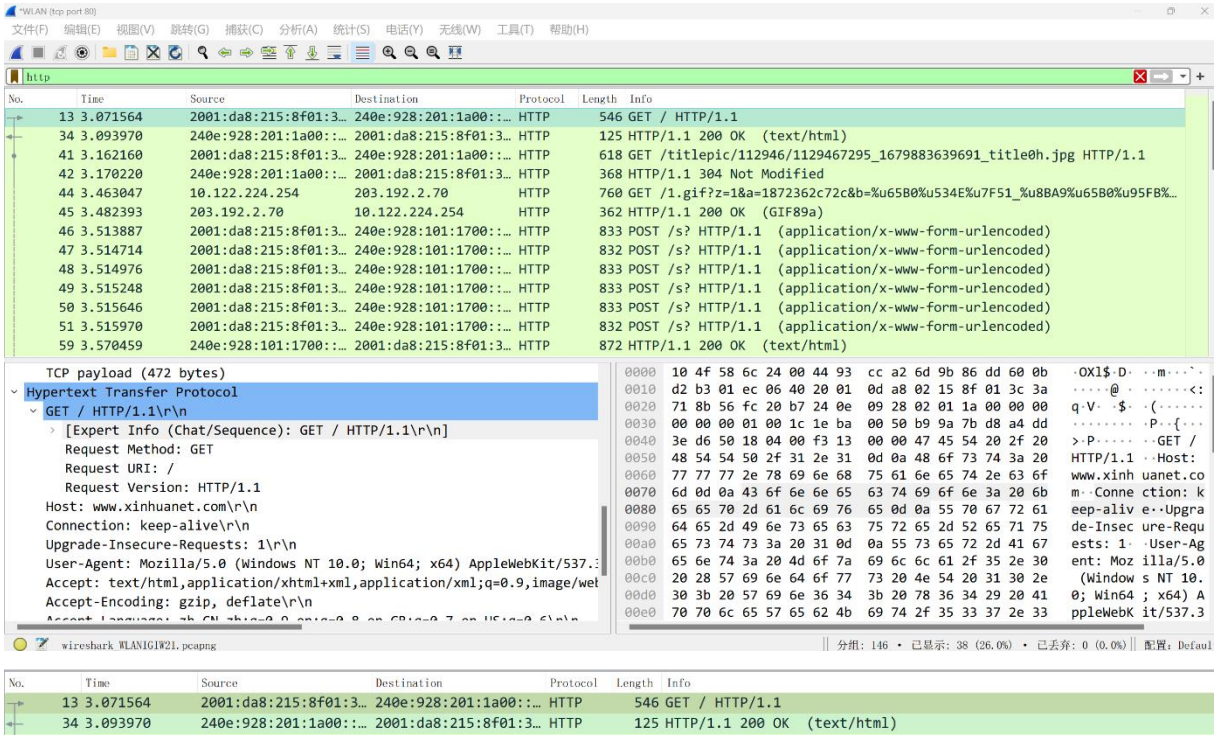


2.数据捕获

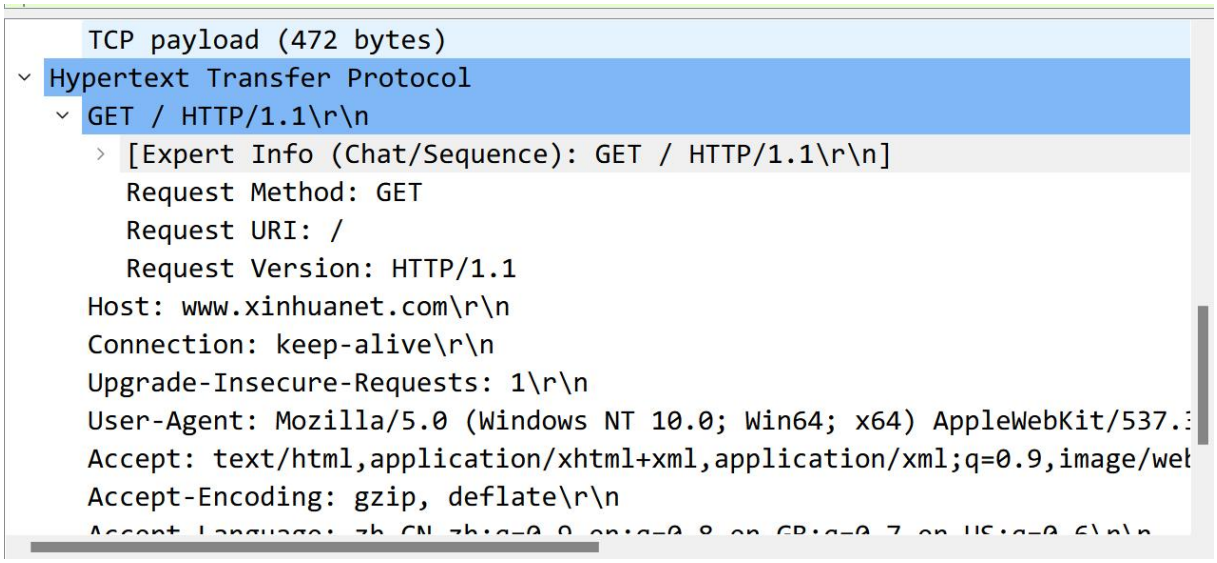
2.1 捕获 HTTP 协议数据

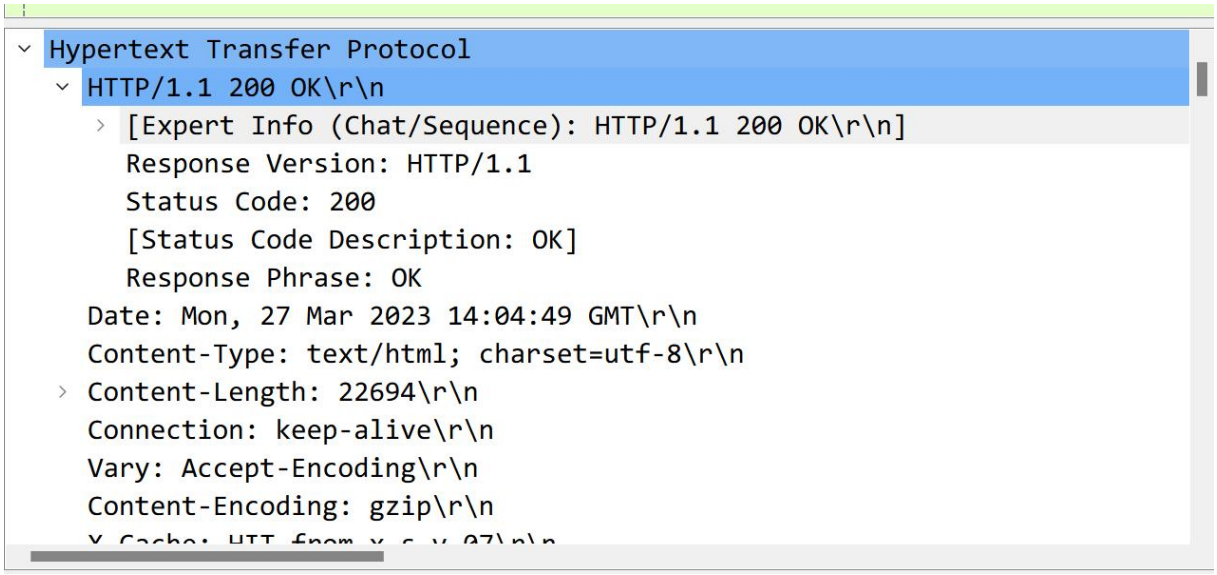
打开浏览器，从设置中清除 cookie 数据（访问记录），选择一个非 HTTPS 协议的网站，在
地址栏里输入其 URL，如 www.xinhuanet.com，网页全部显示后停止捕获。


设置
Cookie 和网站数据 / 所有 Cookie 和站点数据
搜索 cookie
全部删除
已浏览网站的 Cookie 和数据存储
排序方式: 名称
筛选条件: 全部
如果允许使用 Cookie，则会在此处看到存储在你设备上的 Cookie 和网站数据。
个人资料
隐私、搜索和服务
外观
侧栏
开始、主页和新建标签页
共享、复制和粘贴
Cookie 和网站权限
默认浏览器
下载
家庭安全
语言
打印机
系统和性能
重置设置
手机和其他设备
辅助功能
关于 Microsoft Edge


No. Time Source Destination Protocol Length Info
13 3.071564 2001:da8:215:8f01:3… 240e:928:201:1a00::… HTTP 546 GET / HTTP/1.1
34 3.093970 240e:928:201:1a00::… 2001:da8:215:8f01:3… HTTP 125 HTTP/1.1 200 OK (text/html)
41 3.162160 2001:da8:215:8f01:3… 240e:928:201:1a00::… HTTP 618 GET /titlepic/112946/1129467295_1679883639691_title0h.jpg HTTP/1.1
42 3.170220 240e:928:201:1a00::… 2001:da8:215:8f01:3… HTTP 368 HTTP/1.1 304 Not Modified
44 3.463047 10.122.224.254 203.192.2.70 HTTP 760 GET /1.gif?z=1&a=1872362c72c&b=%u65B0%u534E%u7F51_%u8BA9%u65B0%u95FB%…
45 3.482393 203.192.2.70 10.122.224.254 HTTP 362 HTTP/1.1 200 OK (GIF89a)
46 3.513887 2001:da8:215:8f01:3… 240e:928:101:1700::… HTTP 833 POST /s? HTTP/1.1 (application/x-www-form-urlencoded)
47 3.514714 2001:da8:215:8f01:3… 240e:928:101:1700::… HTTP 832 POST /s? HTTP/1.1 (application/x-www-form-urlencoded)
48 3.514976 2001:da8:215:8f01:3… 240e:928:101:1700::… HTTP 833 POST /s? HTTP/1.1 (application/x-www-form-urlencoded)
49 3.515248 2001:da8:215:8f01:3… 240e:928:101:1700::… HTTP 833 POST /s? HTTP/1.1 (application/x-www-form-urlencoded)
50 3.515646 2001:da8:215:8f01:3… 240e:928:101:1700::… HTTP 833 POST /s? HTTP/1.1 (application/x-www-form-urlencoded)
51 3.515970 2001:da8:215:8f01:3… 240e:928:101:1700::… HTTP 832 POST /s? HTTP/1.1 (application/x-www-form-urlencoded)
59 3.570459 240e:928:101:1700::… 2001:da8:215:8f01:3… HTTP 872 HTTP/1.1 200 OK (text/html)
TCP payload (472 bytes)
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Host: www.xinhuanet.com\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/we
Accept-Encoding: gzip, deflate\r\n
0000 10 4f 58 6c 24 00 44 93 cc a2 6d 9b 86 dd 60 0b ·OXl$·D· ··m···`·
0010 d2 b3 01 ec 06 40 20 01 0d a8 02 15 8f 01 3c 3a ·····@ · ·····<:
0020 71 8b 56 fc 20 b7 24 0e 09 28 02 01 1a 00 00 00 q·V· ·$· ·(·····
0030 00 00 00 01 00 1c 1e ba 00 50 b9 9a 7b d8 a4 dd ········ ·P··{···
0040 3e d6 50 18 04 00 f3 13 00 00 47 45 54 20 2f 20 >·P····· ··GET /
0050 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ··Host:
0060 77 77 77 2e 78 69 6e 68 75 61 6e 65 74 2e 63 6f www.xinh uanet.co
0070 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b m··Conne ction: k
0080 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 eep-aliv e··Upgra
0090 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ
00a0 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 ests: 1· ·User-Ag
00b0 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0
00c0 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e (Window s NT 10.
00d0 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 0; Win64 ; x64) A
00e0 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 ppleWebK it/537.3
wireshark_WLANIGIW21.pcapng
分组: 146 · 已显示: 38 (26.0%) · 已丢弃: 0 (0.0%)
配置: Defaul

No. Time Source Destination Protocol Length Info
13 3.071564 2001:da8:215:8f01:3… 240e:928:201:1a00::… HTTP 546 GET / HTTP/1.1
34 3.093970 240e:928:201:1a00::… 2001:da8:215:8f01:3… HTTP 125 HTTP/1.1 200 OK (text/html)



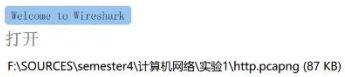


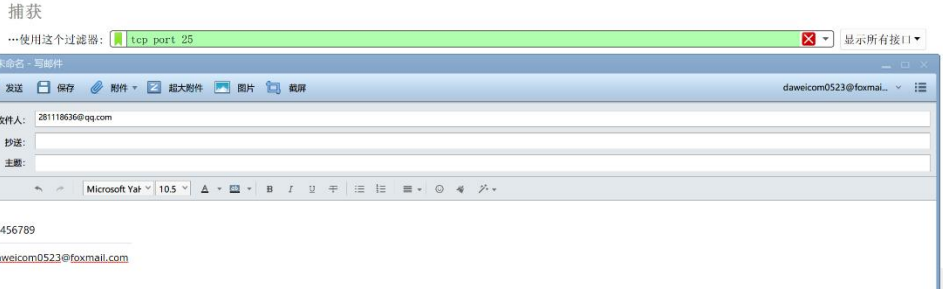
2.2 捕获 SMTP 协议数据

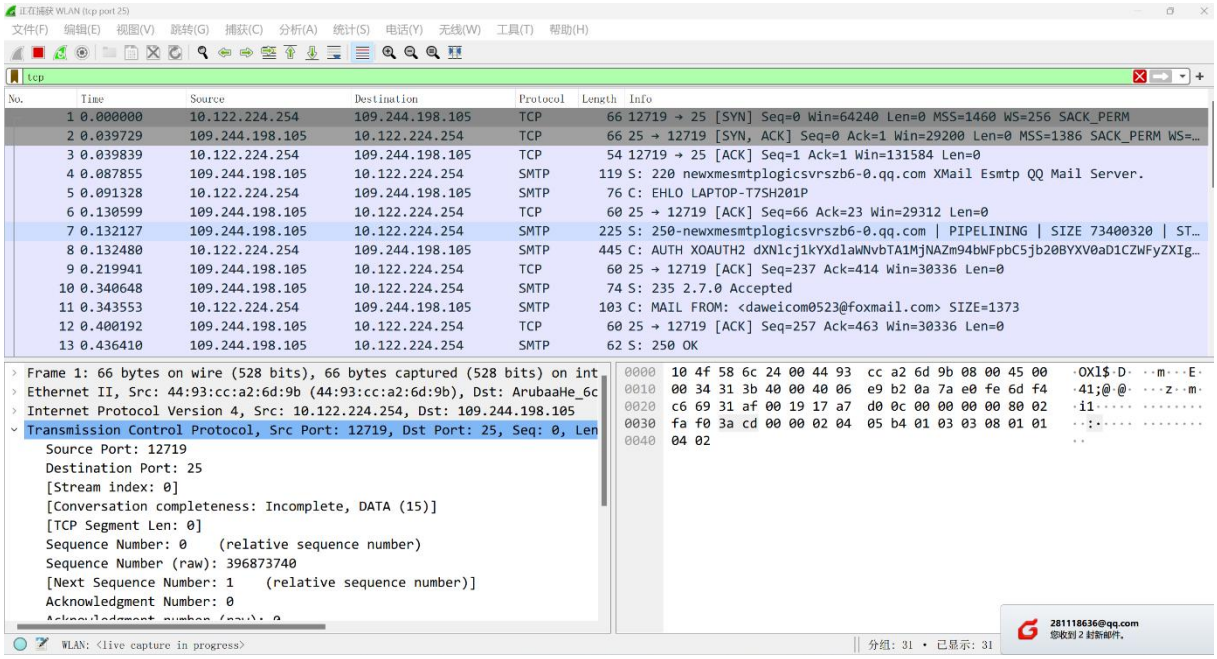
下载并安装邮件客户端软件(如 Foxmail),配置用户账户,设置发件服务器不选择 SSL,端口为 25。配置 wireshark，开始捕获，用 Foxmail 发送一封邮件，邮件发送成功后停止捕获。


系统设置
常用
帐号
写邮件
网络
反垃圾
插件
高级
有汰渍，没乌兹
设置
服务器
高级
邮箱类型：IMAP
帐号：daweicom0523@foxmail.com
收件服务器：imap.qq.com SSL 端口：993
发件服务器：smtp.qq.com SSL 端口：25
如果服务器支持，就使用STARTTLS加密传输(T)
本地备份：服务器删除邮件后，本地 保留
发件服务器身份验证：和收件服务器相同
通讯录和日历：通过ActiveSync同步
服务器：ex.qq.com
新建
导入
删除
确定
取消
应用(A)


文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
tcp

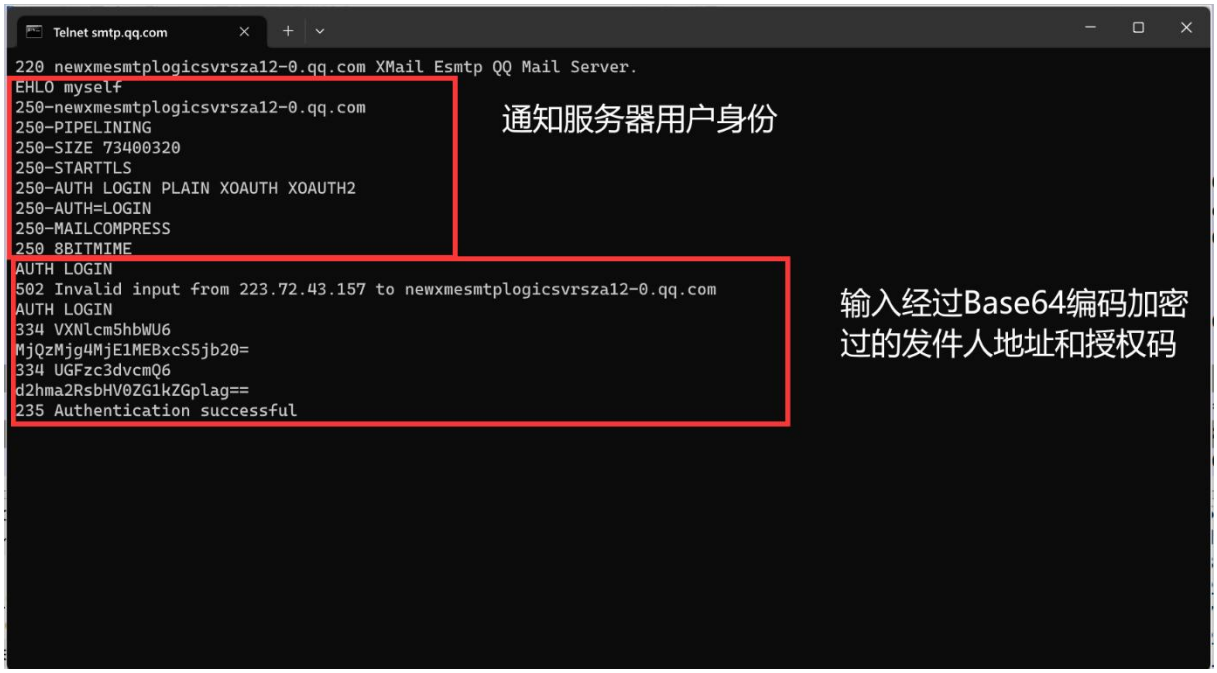

Welcome to Wireshark
打开
F:\SOURCES\semester4\计算机网络\实验1\http.pcapng (87 KB)


捕获
…使用这个过滤器：
tcp port 25
显示所有接口
发送
保存
附件
超大附件
图片
截屏
收件人：
281118636@qq.com
抄送：
主题：
123456789
daweicom0523@foxmail.com
配置：Default



2.3 使用 SMTP 命令与邮件服务器交互

在命令行模式，使用 telnet 程序连接到发件服务器，如 c:>telnet smtp.qq.com 25 在新窗口中，输入 SMTP 命令，与邮件服务器交互。结果如下图：

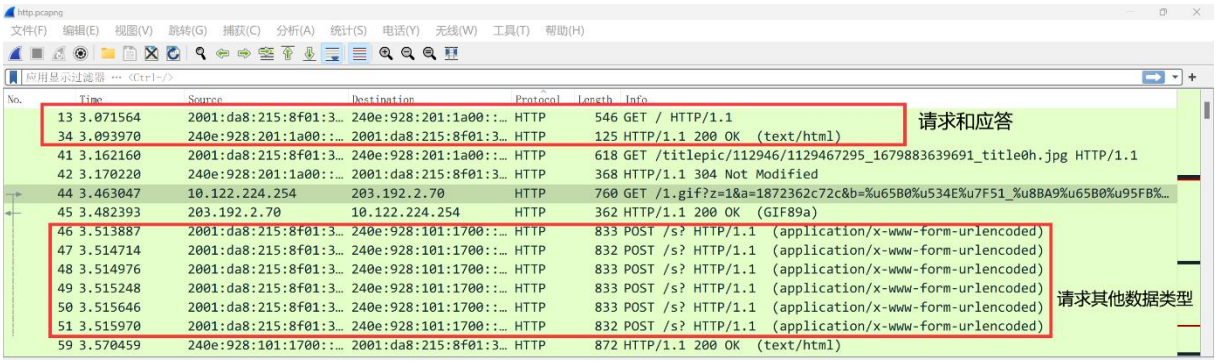


3.HTTP 协议分析

3.1HTTP 的功能和通信过程

3.1.1 HTTP 的功能

HTTP 是 WWW 的应用层协议，通过捕获到的消息可以看出，HTTP 负责浏览器和 Web 服务器之间的通信。浏览器向服务器发送 HTTP 请求消息，服务器返回 HTTP 响应消息。



3.1.2HTTP 的通信过程

1） 浏览器分析网页的 URL（即 www.xinhuanet.com），分析其协议名，如果是 http 或者默认则继续，否则调用对应协议的程序；

2） 浏览器提取出 Web 服务器的域名；

3） 浏览器调用 Resolver 进程，查询 Web 服务器的 IP 地址；

4） 浏览器和 Web 服务器建立 TCP 连接；

5） 浏览器向 Web 服务器发送 HTTP 请求消息，其中包含文件路径和文件名；

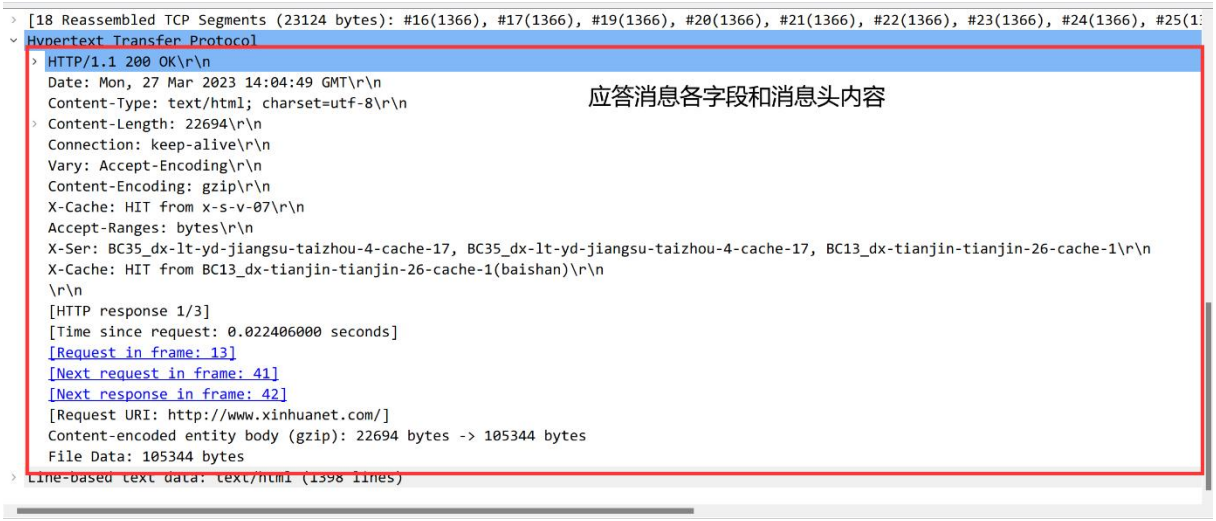
6） 收到 HTTP 请求后，Web 服务器从数据库中查找对应的文件，或者生成动态网页。

7） Web 服务器向浏览器发送 HTTP 响应消息，将网页文件或程序发送给浏览器；

8） 浏览器执行收到的程序或解释收到的网页文件，向用户显示；

9） 如果网页文件嵌有其他类型的数据，则向对应的服务器发送请求。

3.1.2.1 HTTP 请求和应答消息



字段/消息头	功能	现有值	现有值含义
请求行	说明请求方法，请求资源和协议版本	GET/HTTP/1.1\r\n	用 GET 方法请求网页，支持 HTTP1.1
Host	指定被请求的主机和端口号	www.xinhuanet.com	指定请求新华网的主机
Connection	请求结束后，TCP 连接是否关闭	keep-alive	保持 TCP 连接
Upgrade-Insecure-Requests	向服务器发送一个客户端对 HTTPS 加密和认证响应良好，并且可以成功处理的信号，可以请求所属网站所有的 HTTPS 资源。	1	页面包含了 HTTP 资源
User-Agent	让网络协议的对端来识别发起请求的用户代理软件的应用类型、操作系统、软件开发商及版本号	Mozilla/5.0 (Windows NT 10.0; Win64;x64) AppleWebKit/537.36 (KHTML,like Gecko) Chrome/95.0.4638.54 Safari/537.36 Edg/95.0.1020.30	让网络协议的对端来识别发起请求的用户代理软件的应用类型、操作系统、软件开发商及版本号。浏览器标识是 Mozilla 5.0 浏览器，操作系统版本是 Windows10 64 位，渲染引擎 AppleWebKit，537.36 版本（WebKit 又伪装是 KHTML，KHTML 伪装成

			Gecko 的），Chrome 希望能得到为 Safari 编写的网页，于是决定装成 Safari，真实的浏览器是 Edg ，版本号是 95.0.1020.30
Accept	指定客户端接受哪些类型的信息	Text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	客户端接收数据是 html,xhtml+xml,apng,webp,signed-exchange 类型的
Accept-Encoding	指定可接受的内容编码	Gzip,deflate	客户端接收 gzip 和 deflate 的压缩方式
Accept-Language	指定一种自然语言	zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6	客户端接收的首选语言是中文，其次是英语，英式英语和美式英语，q 代表了客户端对其的喜爱度。
Referer	指示一个请求是从哪里链接过来	http://www.xinhuanet.com/	指示请求从 www.xinhuanet.com 链接过来
空行	消息头结束		
响应消息			
状态行	指示响应的状态	HTTP/1.1 200 OK	HTTP 协议是 1.1 版本，网页请求成功
Server	说明服务器名	Tengine	www.xinhuanet.com 的服务器是 Tengine
Content-Length	指示资源总大小	22694	网页文件总大小是 22694 字节
Content-Type	指示资源的 MIME 类型	text/html	资源是 HTML 类型
Connection	说明请求结束后是否保持连接	keep-alive	TCP 保持连接
Date	消息生成的日期和时间	Date: Mon, 27 Mar 2023 14:04:49 GMT\r\n	消息是在 2023 年 3 月 27 日星期一 14:04:49 生成的
Vary	告知代理服务器如何应对以后的请求，是否可以使用缓存	Vary: Accept-Encoding	告诉代理服务器缓存两种版本的资源：压缩和非压缩
Content-Encoding	说明如何解码	gzip	使用 gzip 解码

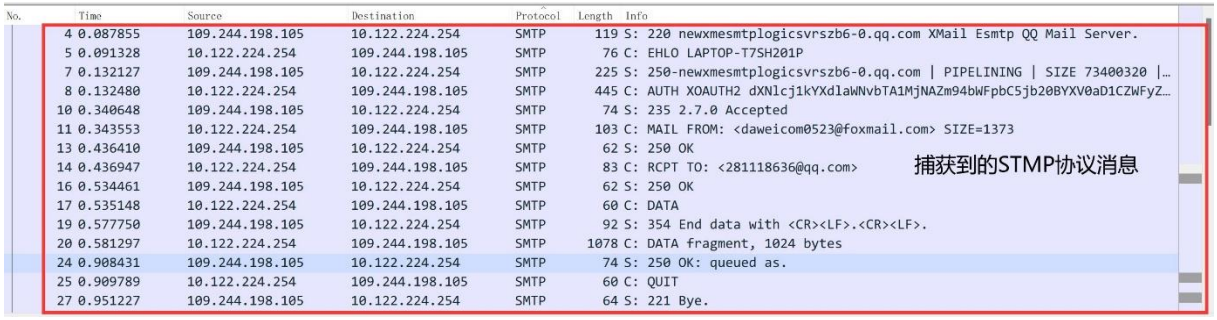
Accept-Ranges	指示服务器可以接受的范围	Accept-Ranges: bytes	服务器可以接受的范围是字节
X-Cache	指示浏览器从哪个代理缓存载入的网页文件	X-Cache: HIT from x-s-v-07\r\n	命中了 CDN 缓存，从 x-s-v-07 代理缓存载入
X-Ser	服务器	X-Ser: BC35_dx-lt-yd-jiangsu-taizhou-4-cache-17, BC35_dx-lt-yd-jiangsu-taizhou-4-cache-17, BC13_dx-tianjin-tianjin-26-cache-1	
Timing-Allow-Origin	用于指定特定站点，以允许其访问 Resource Timing API 提供的相关信息	Timing-Allow-Origin: *	所有域都可以访问
空行	响应头结束		
File Data:	文件总数据大小	105344 bytes	文件总数据大小为 105344 字节

4. SMTP 协议分析

4.1 SMTP 的功能和通信过程

4.1.1 SMTP 的功能

SMTP 是简单邮件传输协议，从捕获到的消息可以看出 SMTP 负责邮件的直接传输，直接从发信人的服务器传输到收信人的服务器。SMTP 通过与收信人的服务器的命令和应答方式实现交互。



4.1.2　SMTP 的通信过程

1）客户端与 SMTP 服务器建立 TCP 连接；

2）客户端向服务器发送 EHLO 命令标识发件人身份；

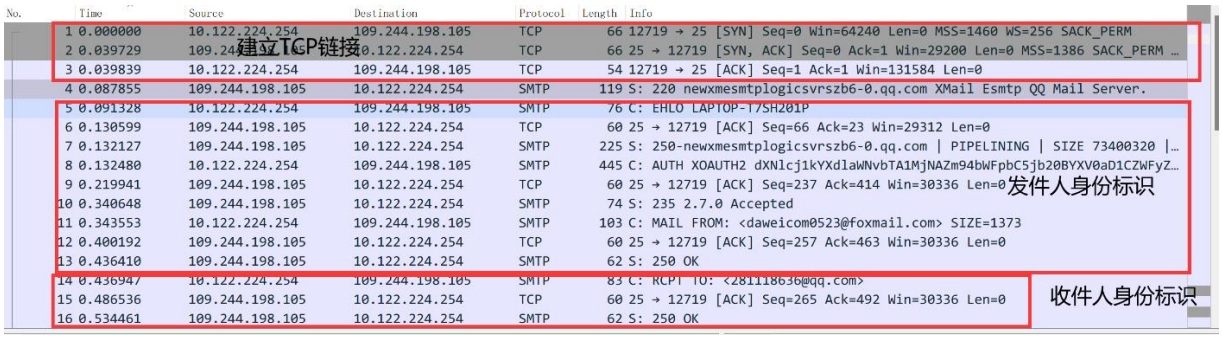
3）邮件服务器通过后，准备接受邮件；

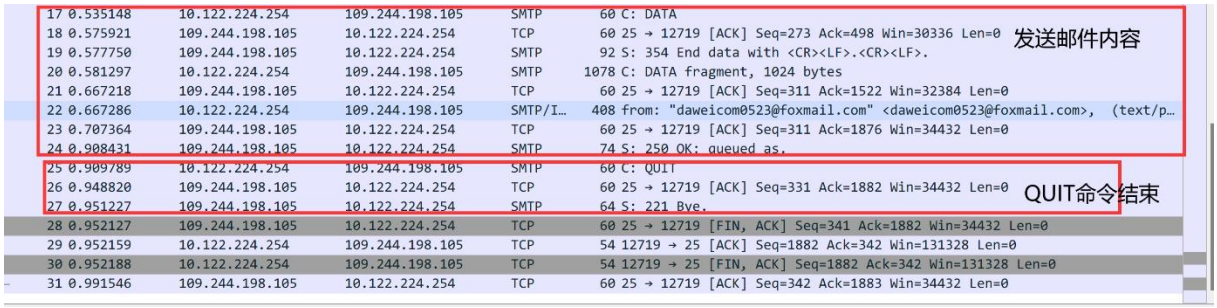
4）客户端向服务器发送 RCPT 命令标识收件人身份；

5）邮件服务器回复是否愿意接收；

6）如果服务器愿意接收，客户端用 DATA 命令将邮件内容分多次发送；

7）发送结束后，客户端用 QUIT 命令退出，结束通信。





4.2 SMTP 命令消息和状态码

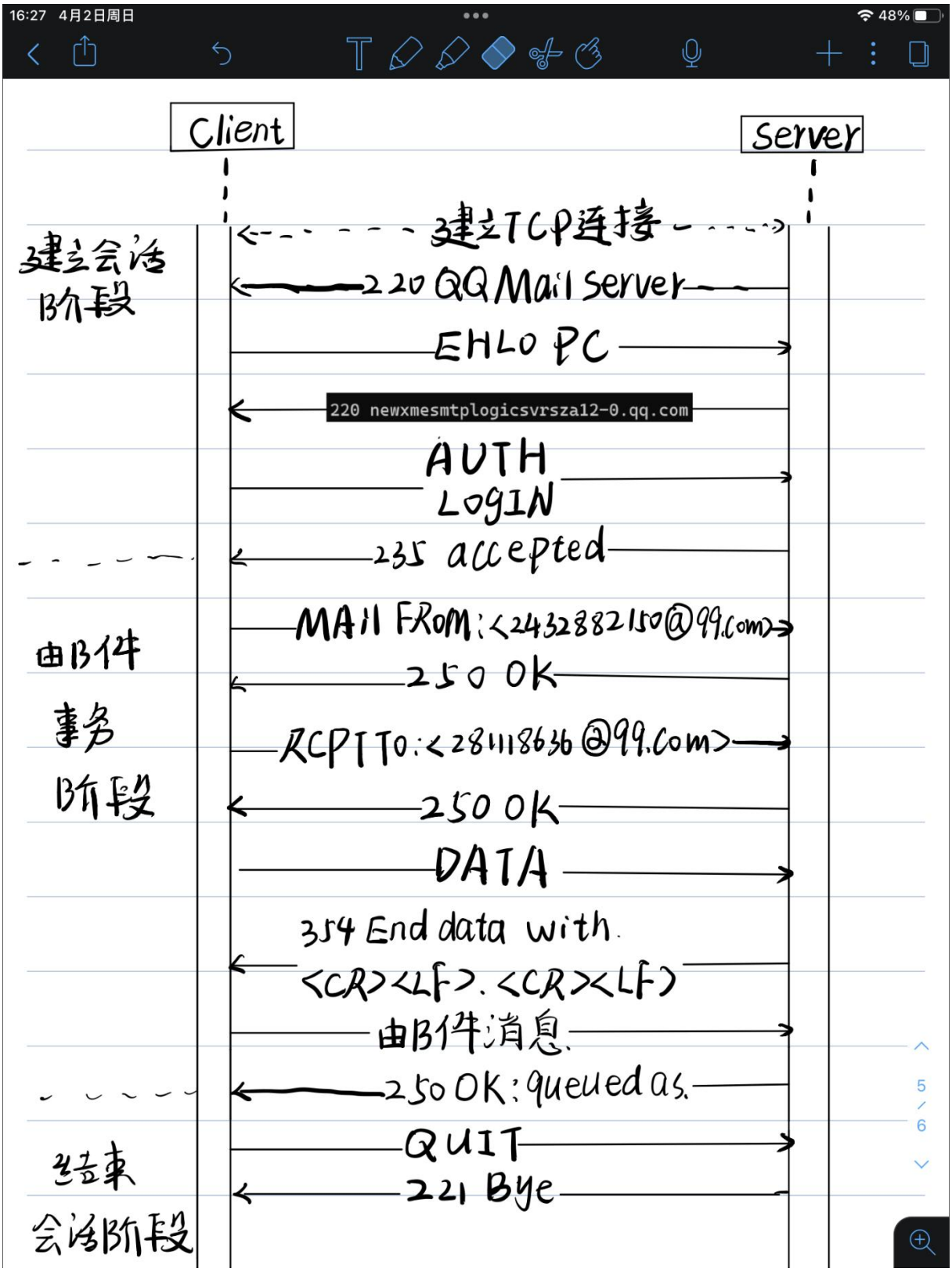
4.2.1 命令功能

命令	功能
EHLO	通知发件人的用户身份
AUTH	指出本地 SMTP 虚拟服务器支持 SMTP 身份验证服务扩展
MAIL FROM	通知服务器写信人的邮件地址，并开始邮件服务
RCPT TO	通知收信人地址
DATA	通知邮件正文开始
QUIT	要求关闭 TCP 连接

4.2.2 状态码

状态码	含义
220	可以提供邮件服务
250	命令成功执行
235	认证通过
354	通知客户端开始发送邮件，以只包含“.”的一行作为结束
221	服务器端结束传输，关闭 TCP 连接

4.2.3 消息序列图


16:27 4月2日周日
48%
Client
Server
建立TCP连接
建立会话阶段
220 QQ Mail Server
EHLO PC
220 newxmesmtplogicsvrsza12-0.qq.com
AUTH LOGIN
235 accepted
MAIL FROM:<2432882150@99.com>
由B件事务阶段
250 OK
RCPT TO:<2811118636@99.com>
250 OK
DATA
354 End data with <CR><LF>.<CR><LF>
由B件消息
250 OK: queued as.
QUIT
结束会话阶段
221 Bye

5. 实验结论和实验心得

5.1 遇到的问题

1）复制授权码时或者复制 QQ 邮箱名字时，导致多复制了一个空格，使得 Base64 编码多了一个=，导致一直无法登录。
2）使用 Wireshark 时，以为需要自己设置捕获器过滤（如下图 1 设置），一直无法准确捕捉对应的信息，实则仅需要在图 2 设置即可。

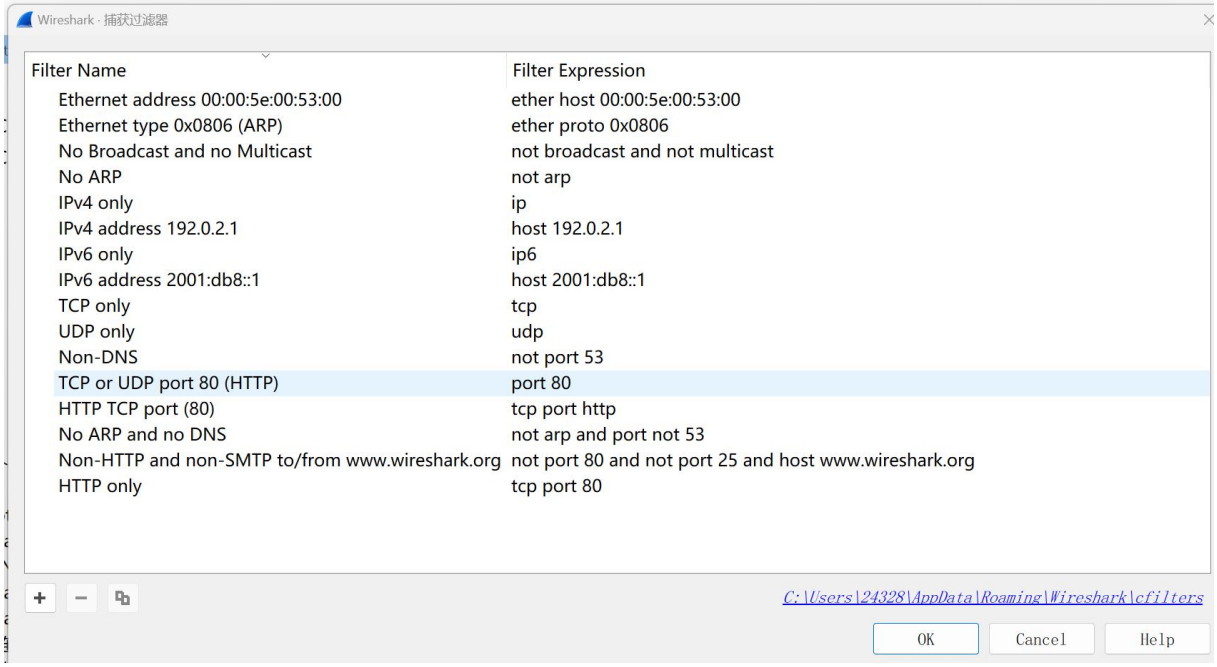


图 1

图 2

5.2 实验心得

通过以上实验，我深入了解了 HTTP 和 SMTP 两个协议的通信原理，并学习了如何使用 Wireshark 和 Telnet 工具进行网络数据包捕获和交互式通信。

在分析 HTTP 消息之后，我了解到 HTTP 是一种无状态的协议，客户端与服务器之间通过请求和响应来进行通信。通过分析消息头，我了解到 HTTP 消息头中包含许多元数据，如请求的方法、URI、请求头、响应状态码等，这些元数据对于实现有效的网络通信非常重要。

在分析 SMTP 消息之后，我认识到 SMTP 是一种用于发送邮件的协议，它是基于文本的协议，包含邮件头和邮件主体。通过分析 SMTP 消息，我了解到邮件的发送过程涉及到发送邮件服务器和接收邮件服务器之间的交互，这些交互包括 HELO/EHLO、MAIL

FROM、RCPT TO、DATA、QUIT 等命令，这些命令用于在邮件服务器之间传递邮件信息。在使用 Telnet 访问 Email 服务器时，我知道了 SMTP 命令是基于文本的协议，包括 ASCII 字符集和 Base64 编码。通过交互式地输入 SMTP 命令，我了解到 Base64 编码可以用于将二进制数据转换为文本数据，并在网络中进行传输。

这次实验不仅增强了我对教材和讲义中理论知识的理解与记忆，更让我用清晰简单的方式实现了邮件的接收与 HTTP 交互。同时，也通过这个看起来十分复杂，“羞涩难懂”的代码，使得我可以深入浅出地认识明白这些内容，能够对此有着更加透彻的学习与了解。