

Week6: HTTP、SMTP、POP3协议分析

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、实验过程

3.1 预备知识

- HTTP协议

HTTP协议(超文本传输协议HyperText Transfer Protocol)，它是基于TCP协议的应用层传输协议，简单来说就是客户端和服务端进行数据传输的一种规则。HTTP 是一种无状态 (stateless) 协议，HTTP协议本身不会对发送过的请求和相应的通信状态进行持久化处理。这样做的目的是为了保持HTTP协议的简单性，从而能够快速处理大量的事务，提高效率。然而，在许多应用场景中，我们需要保持用户登录的状态或记录用户购物车中的商品。由于HTTP是无状态协议，所以必须引入一些技术来记录管理状态，例如Cookie。

- SMTP协议

SMTP (Simple Mail Transfer Protocol) 即简单邮件传输协议,它是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP协议属于TCP/IP协议簇，它帮助每台计算机在发送或中转信件时找到下一个目的地。通过SMTP协议所指定的服务器,就可以把E-mail寄到收信人的服务器上了，整个过程只要几分钟。SMTP服务器则是遵循SMTP协议的发送邮件服务器，用来发送或中转发出的电子邮件。SMTP是一种TCP协议支持的提供可靠且有效电子邮件传输的应用层协议。

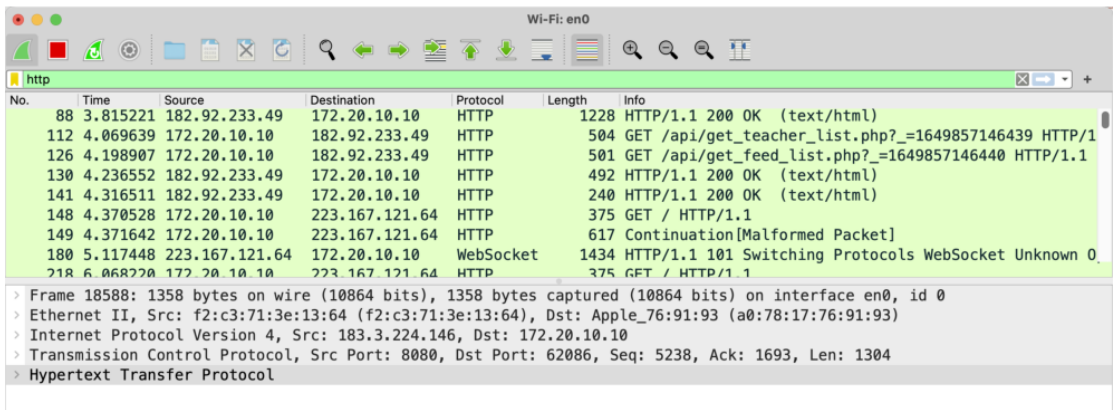
- POP3协议

POP3 (Post Office Protocol version3)：邮局协议第三版本，协助用户代理（即客户端）从邮件服务器上获取邮件。POP3允许用户从服务器上把邮件存储到本地主机（即自己的计算机）上，同时删除保存在邮件服务器上的邮件，而POP3服务器则是遵循POP3协议的接收邮件服务器，用来接收电子邮件的。

3.2 HTTP数据包抓取及分析

3.2.1 操作步骤

1. 清空Web浏览器的缓存，保证数据是从网络中获取的
2. 启动Wireshark，开始Wireshark抓包
3. 在浏览器地址栏中前往网址 <http://www.chinesemooc.org>
4. 单击浏览器中的“刷新”按钮
5. 停止Wireshark分组俘获，过滤筛选处输入“http”显示捕获到的HTTP报文



3.2.2 HTTP报文格式

HTTP由请求和响应两部分组成，所以对应的也有两种报文格式。

- HTTP请求报文分析



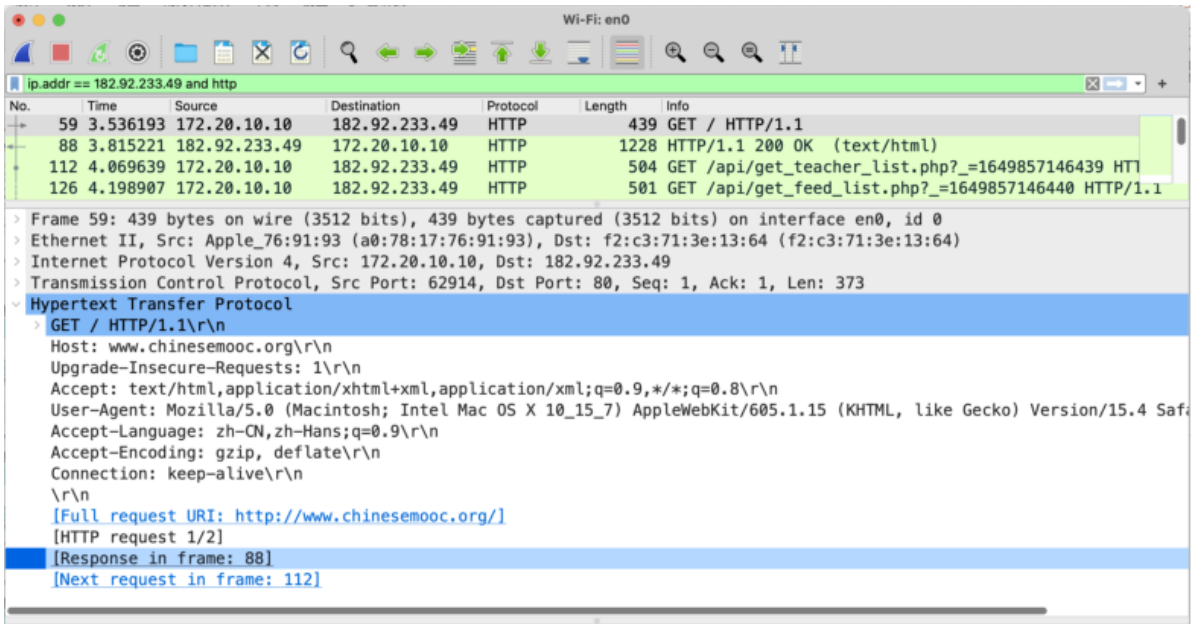
图1 HTTP请求报文

- HTTP响应报文分析



图2 HTTP响应报文

- 为避免过多网络包影响分析，可在显示过滤器栏输入 ip.addr == ip地址 and http，此时Wireshark会按照条件过滤网络包。



task1: 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。

task2: 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。

- 对比分析GET和POST方法的请求和响应报文

GET	空格	/	空格	HTTP/1.1	\r	\n
Accept	:	text/html,application/xhtml+xml,application/xml		\r	\n	
...						
Connection	:	keep-alive		\r	\n	
\r			\n			
Full request URI: http://10.1.1.33:8080/						

图3 GET方法的HTTP请求报文

HTTP/1.1	空格	200	空格	OK	\r	\n
Content-Type	:	text/html		\r		\n
...						
Content-Encoding	:	gzip		\r		\n
\r			\n			
省略						

图 4 GET方法的HTTP响应报文

POST	空格	/hfs2_3b287/	空格	HTTP/1.1	\r	\n
Accept	:	text/html,application/xhtml+xml,application/xml		\r		\n
...						
Content-Length	:	367		\r		\n
\r			\n			
忽略						

图 5 POST方法的HTTP请求报文

HTTP/1.1	空格	200	空格	OK	\r	\n
Server	:	HFS 2.3 beta		\r		\n
...						
Content-Encoding	:	gzip		\r		\n
\r			\n			
省略						

图 6 POST方法的HTTP响应报文

task3: 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。

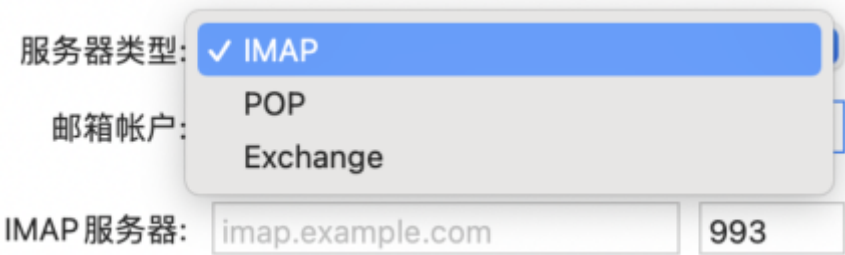
3.3 SMTP和POP3数据包抓取及分析

3.3.1 操作步骤:

1. 邮箱账户配置，本地用foxmail（或其他邮件app）登录两个邮箱，用A邮箱发送邮件给B邮箱，（为保证统一性此处将采用foxmail进行示范，且采用一个163邮箱账号进行模拟，其他邮箱类似）
2. 在绑定163账户至foxmail前，需前往网易邮箱设置中确认开启POP3/SMTP服务以保证能正确收到POP3协议包，默认开启的是IMAP/SMTP服务



3. 在foxmail中添加账户->其他邮箱->高级设置->修改服务器类型为POP，在进行下方账号信息填写



为保证后续Wireshark能正确捕获数据包，需取消安全连接的☑，填写用户名信息，注意这里的密码是在网易邮箱设置里面授权密码管理得到的，不是你的账户密码

服务器类型: POP

邮箱帐户: example@163.com

POP3 服务器: pop.163.com 995

用户名: example@163.com

密码:

☐ 安全连接

SMTP 服务器: smtp.example.com 465

用户名:

密码:

☐ 安全连接 ☒ 使用鉴定

网络代理: 设置

返回 继续

授权密码管理: 授权码是用于登录第三方邮件客户端的专用密码。
适用于登录以下服务: 您开启的服务 (例如POP3/IMAP/SMTP)、Exchange/CardDAV/CalDAV服务。

登录账号后, 选择邮箱帐户右击“设置/服务器”中取消SSL勾选。

系统设置

常用 帐号 写邮件 网络 反垃圾 插件 高级

163(m19370572258)
贾金萍
163(m15651788235_2)

设置 服务器 高级

邮箱类型: POP3

帐号: m15651788235_2@163.com

收件服务器: pop.163.com ☐ SSL 端口: 110

发件服务器: smtp.163.com ☐ SSL 端口: 25

☐ 如果服务器支持, 就使用STARTTLS加密传输(T)

服务器备份: 邮件收取后, 在服务器上 永久保留

发件服务器身份验证: 和收件服务器相同

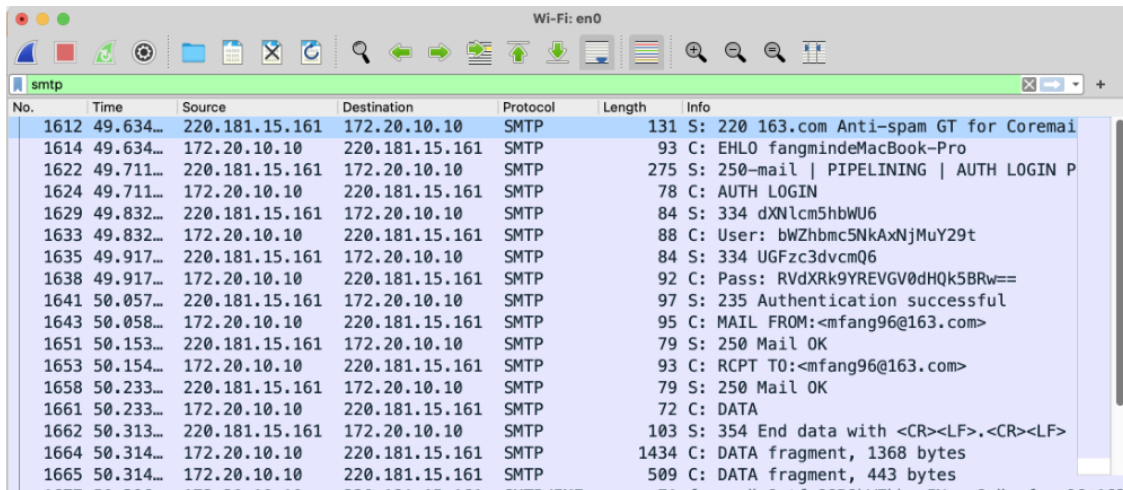
通讯录和日历: ☒ 通过ActiveSync同步

服务器: i.163.com

4. 邮箱账户配置完成后, 打开Wireshark, 开始捕获网络包
5. 通过foxmail (或其他邮件app) 用A邮箱发送邮件给B邮箱, 然后利用Wireshark过滤SMTP和POP3协议的数据包

task4: 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。

task5: 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。



No.	Time	Source	Destination	Protocol	Length	Info
1612	49.634...	220.181.15.161	172.20.10.10	SMTP	131	S: 220 163.com Anti-spam GT for Coremai
1614	49.634...	172.20.10.10	220.181.15.161	SMTP	93	C: EHLO fangmindeMacBook-Pro
1622	49.711...	220.181.15.161	172.20.10.10	SMTP	275	S: 250-mail PIPELINING AUTH LOGIN P
1624	49.711...	172.20.10.10	220.181.15.161	SMTP	78	C: AUTH LOGIN
1629	49.832...	220.181.15.161	172.20.10.10	SMTP	84	S: 334 dXNlcm5hbWU6
1633	49.832...	172.20.10.10	220.181.15.161	SMTP	88	C: User: bWZhbmMc5NkAxNjMuY29t
1635	49.917...	220.181.15.161	172.20.10.10	SMTP	84	S: 334 UGFzc3dvcmQ6
1638	49.917...	172.20.10.10	220.181.15.161	SMTP	92	C: Pass: RVdXRk9YREVGV0dHQk5BRw==
1641	50.057...	220.181.15.161	172.20.10.10	SMTP	97	S: 235 Authentication successful
1643	50.058...	172.20.10.10	220.181.15.161	SMTP	95	C: MAIL FROM:<mfang96@163.com>
1651	50.153...	220.181.15.161	172.20.10.10	SMTP	79	S: 250 Mail OK
1653	50.154...	172.20.10.10	220.181.15.161	SMTP	93	C: RCPT TO:<mfang96@163.com>
1658	50.233...	220.181.15.161	172.20.10.10	SMTP	79	S: 250 Mail OK
1661	50.233...	172.20.10.10	220.181.15.161	SMTP	72	C: DATA
1662	50.313...	220.181.15.161	172.20.10.10	SMTP	103	S: 354 End data with <CR><LF>.<CR><LF>
1664	50.314...	172.20.10.10	220.181.15.161	SMTP	1434	C: DATA fragment, 1368 bytes
1665	50.314...	172.20.10.10	220.181.15.161	SMTP	509	C: DATA fragment, 443 bytes