

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：2021

上机实践成绩：

指导教师：张召

姓名：温兆和

学号：10205501432

上机实践名称：HTTP、SMTP、POP3 协议分析

上机实践日期：2022.04.15

上机实践编号：08

组号：001-432

上机实践时间：13: 00

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

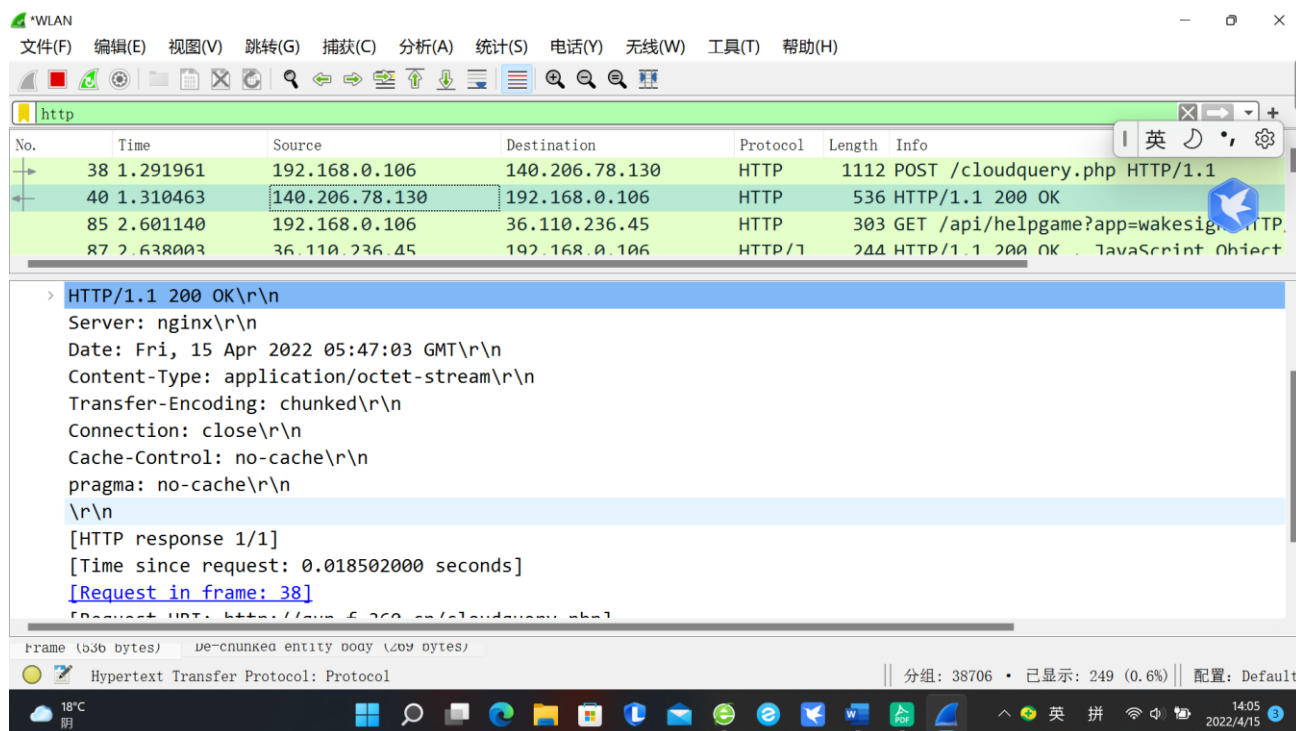
四、实验过程

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。

请求方法: POST, 协议版本: HTTP/1.1
User-Agent: Post_Multipart\r\n\r\n
Host: qup.f.360.cn\r\n\r\n
Accept: */*\r\n\r\n
Pragma: no-cache\r\n\r\n
X-360-Cloud-Security-Desc: Scan Suspicious File\r\n\r\n
x-360-ver: 4\r\n\r\n
> Content-Length: 1058\r\n\r\n
Content-Type: multipart/form-data; boundary=-----97e00365cc58\r\n\r\n
\r\n
[Full request URI: http://qup.f.360.cn/cloudquery.php]
[HTTP request: 1]
[Request body: 1058 bytes]

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。

上述请求网络包对应响应网络包的报文：



HTTP 请求网络包和响应网络包报文的区别：

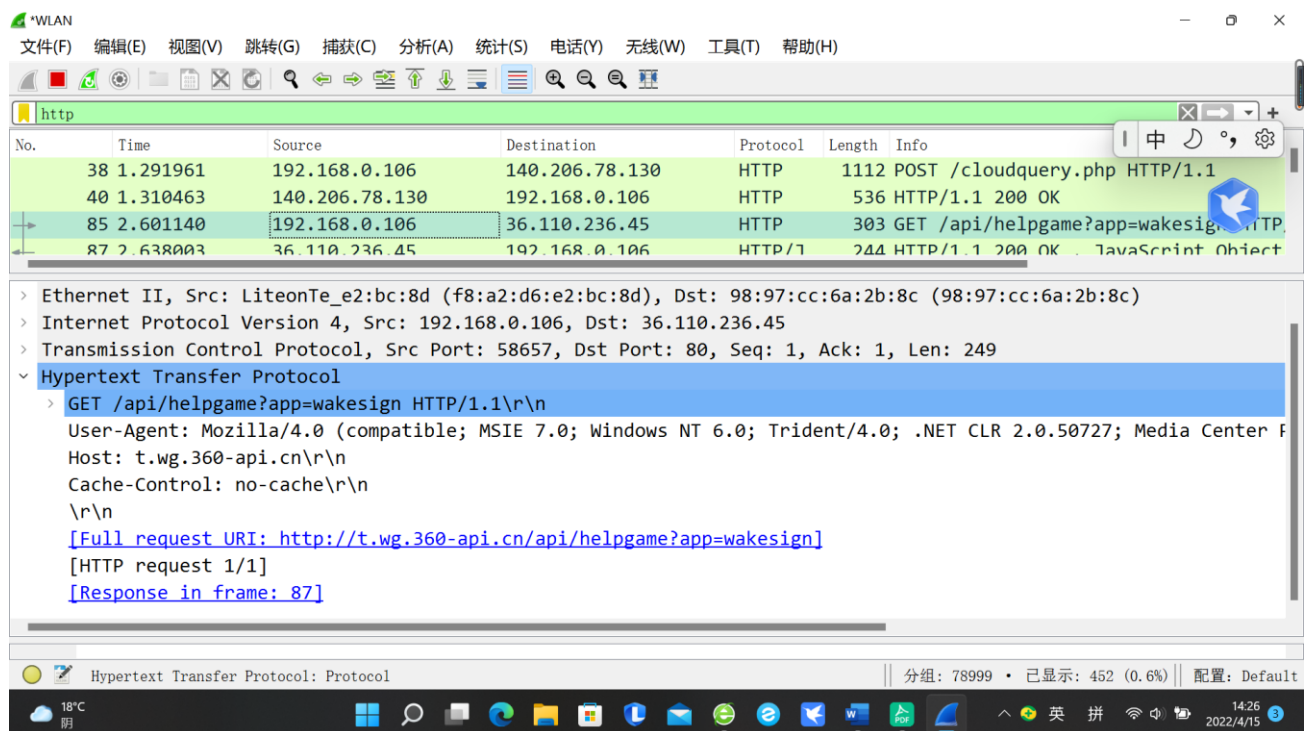
状态行：两者的状态行都会显示协议的版本（HTTP），但请求网络包状态行中会显示请求的方法和请求对象的标识，而响应网络包状态行中会显示请求的结果（状态码和短语）；

首部行：请求报文的首部行会指明对象所在的主机（Host）和向服务器发送请求的浏览器类型（User-Agent），而响应报文的首部行会指明报文生成的日期（Date）和产生报文的服务器的类型（Server）。两者的相同之处在于它们都会指出实体体中文件的类型（Content-Type）和字节长度（Content-Length）。

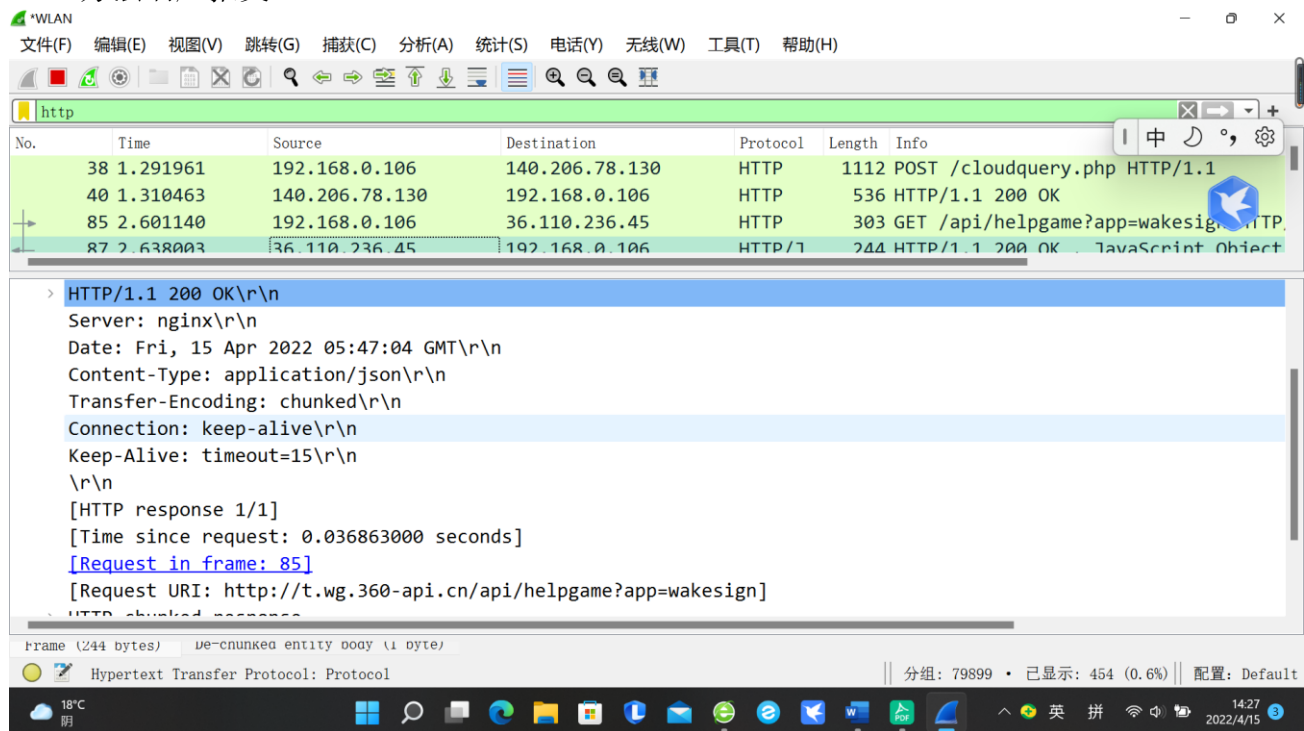
Task3. 学习了解 GET 和 POST 方法，请在实验报告中分析对比 GET 和 POST 方法的请求报文，以及 GET 和 POST 方法的响应报文之间的区别。

之前的请求和响应报文都是有关 POST 方法的。

GET 方法请求报文：



GET 方法响应报文:

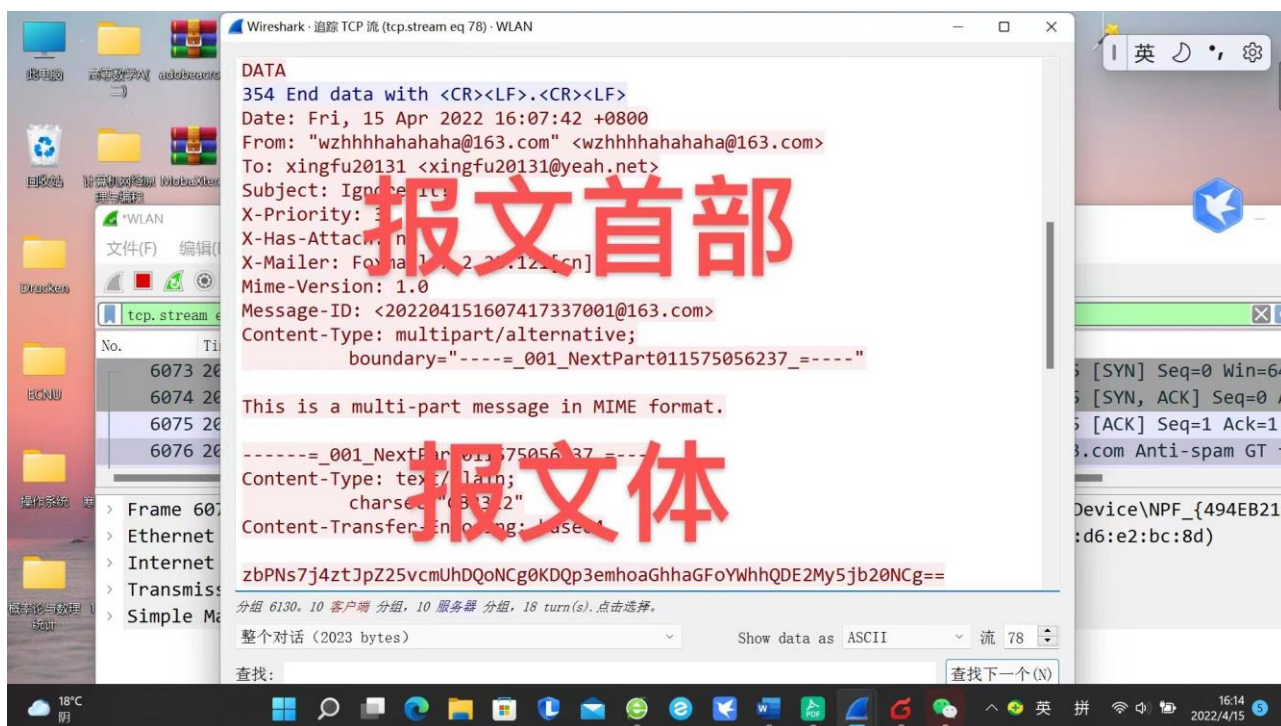


GET 和 POST 方法报文的区别:

GET 方法和 POST 方法请求报文最大的区别就在于 GET 方法请求报文的实体体为空，也就自然没有了 Content-Type 和 Content-Length 这两行，而 POST 方法请求报文中实体体不为空，首部行中会显示实体体中文件的类型和字节长度；在这个例子中，两种方法的响应报文结构区别不明显。

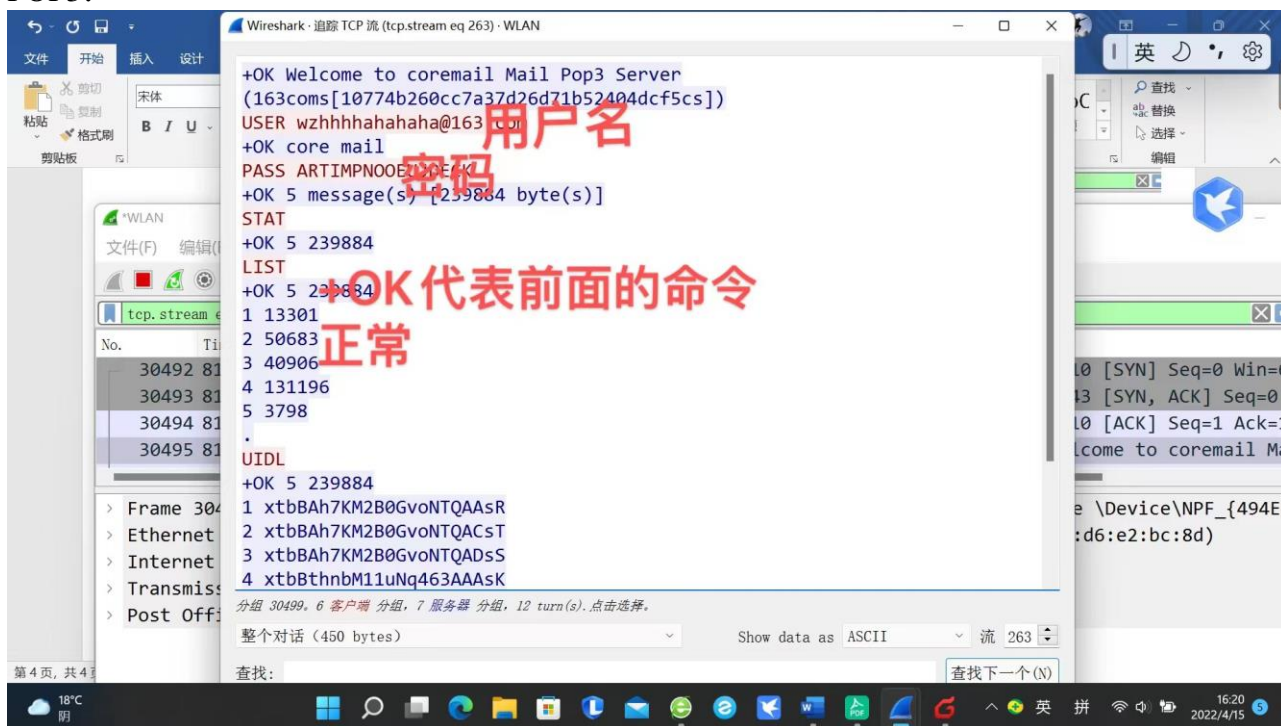
Task4. 利用 Wireshark 抓取 SMTP 和 POP3 网络包，分析 SMTP 和 POP3 数据包组成（要求根据报文结构正确标识每个部分），请将实验结果附在实验报告中。

SMTP:

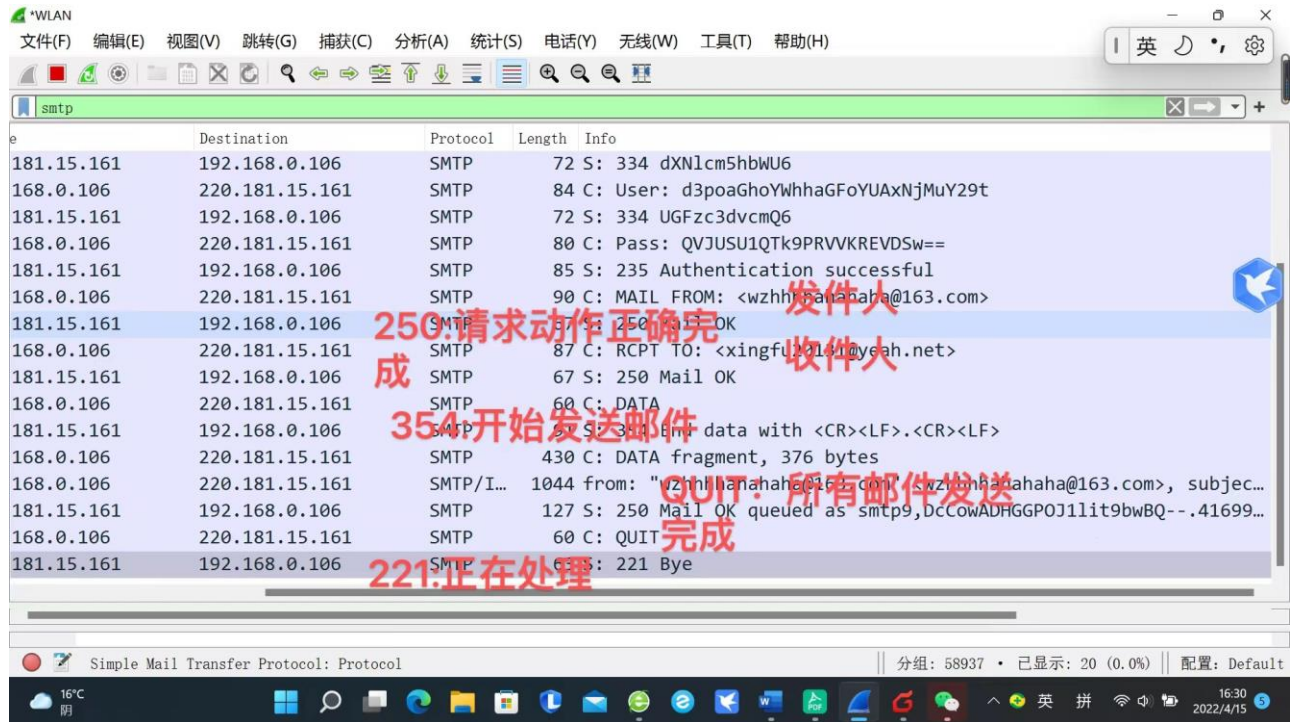


其中报文首部包含：发件人、收件人、主题、发送时间等。

POP3:



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
181	15.15.161	192.168.0.106	192.168.0.106	SMTP	72	S: 334 dXNlcm5hbWU6
168	0.106	220.181.15.161	220.181.15.161	SMTP	84	C: User: d3poaGhoYWhhaGfoYUAXNjMuY29t
181	15.161	192.168.0.106	192.168.0.106	SMTP	72	S: 334 UGFzc3dvcmQ6
168	0.106	220.181.15.161	220.181.15.161	SMTP	80	C: Pass: QVJUSU1QTk9PRVVKREVDsw==
181	15.161	192.168.0.106	192.168.0.106	SMTP	85	S: 235 Authentication successful
168	0.106	220.181.15.161	220.181.15.161	SMTP	90	C: MAIL FROM: <wzhhhahahahaha@163.com>
181	15.161	192.168.0.106	192.168.0.106	SMTP	74	S: 250 Mail OK
168	0.106	220.181.15.161	220.181.15.161	SMTP	87	C: RCPT TO: <xingfujia141@yeah.net>
181	15.161	192.168.0.106	192.168.0.106	SMTP	67	S: 250 Mail OK
168	0.106	220.181.15.161	220.181.15.161	SMTP	60	C: DATA
181	15.161	192.168.0.106	192.168.0.106	SMTP	257	S: 354 Begin data with <CR><LF>.<CR><LF>
168	0.106	220.181.15.161	220.181.15.161	SMTP	430	C: DATA fragment, 376 bytes
168	0.106	220.181.15.161	220.181.15.161	SMTP/I...	1044	from: "wzhhhahahahaha@163.com" (wzhhhahahahaha@163.com), subjec...
181	15.161	192.168.0.106	192.168.0.106	SMTP	127	S: 250 Mail OK queued as smtp9,DcCowADHGgPOJ1lit9bwBQ--.41699...
168	0.106	220.181.15.161	220.181.15.161	SMTP	60	C: QUIT
181	15.161	192.168.0.106	192.168.0.106	SMTP	63	S: 221 Bye

五、总结

通过本周的实验，我们通过抓取网络包并分析、观察其报文，熟悉了 HTTP、SMTP、POP3 的工作原理，直观地了解了它们在实际网络中的运行过程，巩固了课内知识，为以后的理论学习和实验项目打下了基础。