**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 成绩评定

实验项目名称 TCP/IP协议配置与网络实用命令 指导教师 潘冰

实验项目编号 3 实验项目类型 验证型 实验地点

学生姓名 梁峻铭 学号 2019051103

学院 智能科学与工程 系 专业 信息安全

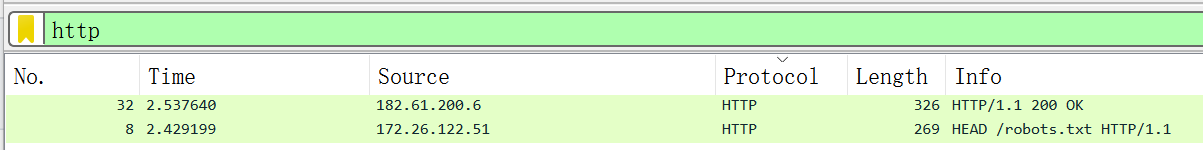
实验时间 2021 年 10 月 17 日 下 午～ 10 月 17 日 下 午

1. **实验目的**
   * 理解WWW 、 DNS服务、FTP服务、SMTP的作用和原理；
   * **学会使用wireshark分析HTTP、FTP、SMTP和DNS协议的工作过程，加深对协议格式和工作原理的理解。**
2. **实验内容**
   * 通过域名访问WWW、FTP服务器，分析DNS、WWW、FTP工作过程，并使用WireShark分析相关协议格式；
   * 在客户端访问SMTP服务器，使用wireshark分析SMTP、POP3协议的工作过程。（可以在客户端安装outlook或使用QQ邮件服务器或自己编程）
3. **实验步骤**

**1、HTTP协议分析**

访问任意web站点，用wireshark分析HTTP协议的工作过程和HTTP协议格式。（协议首部含义需要查询了解）

以下为过滤http后的列表：



工作过程：

浏览器向服务器建立连接请求后，通过三次握手建立连接，建立后，浏览器向服务器发出访问某个页面的请求，服务器返回请求的页面作为响应。

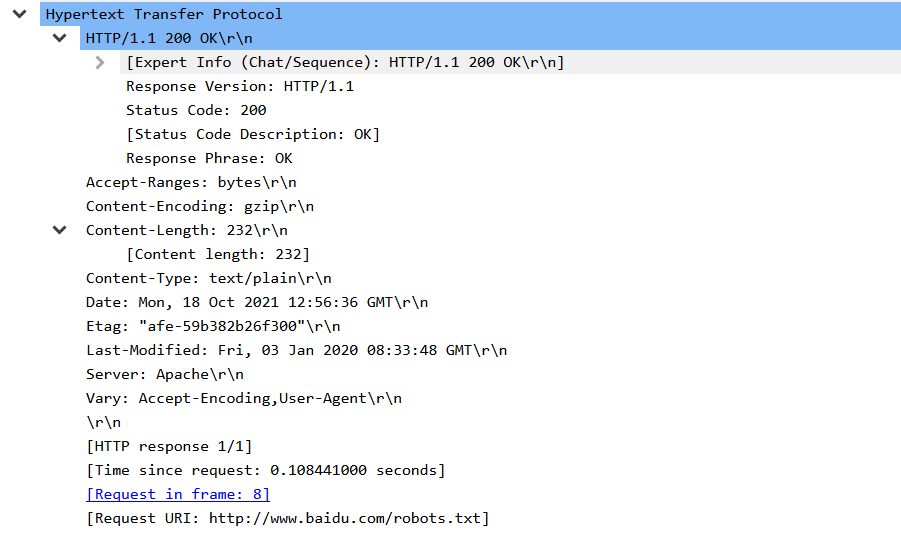
请求报文：

该报文为请求报文，使用了HEAD方法用于请求读取由URL所标志的信息的首部。接着是URL和版本号，\r\n表示回车换行。接着是各个首部字段名（用户代理、主机域名等）和及它们的值。



响应报文：

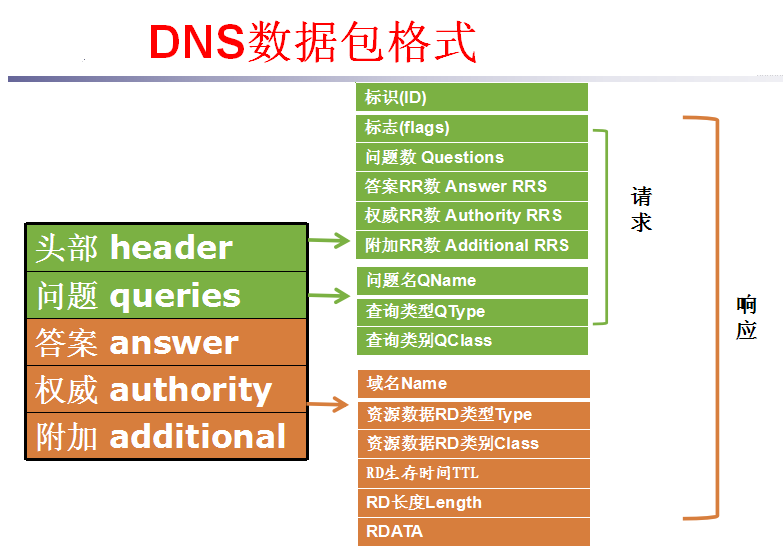
收到请求报文后，能收到响应报文。以下图为例，第一行为状态行（包括版本号、状态码以及解释状态码的简单短语）。其中状态码为三位的数字，以图中为例，200表示成功，如接受或知道了。

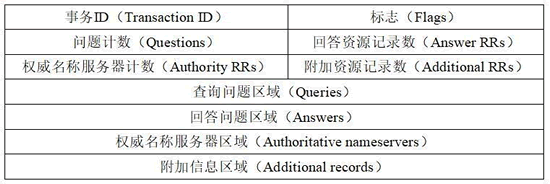


**2、DNS协议分析**

通过域名访问某网站，用wireshark捕获DNS数据包，并分析DNS工作过程和DNS格式。

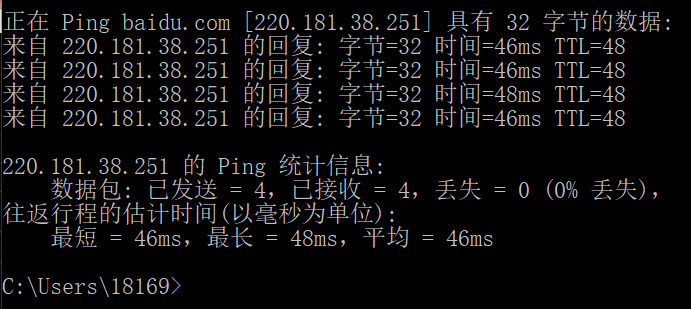
DNS格式如下：



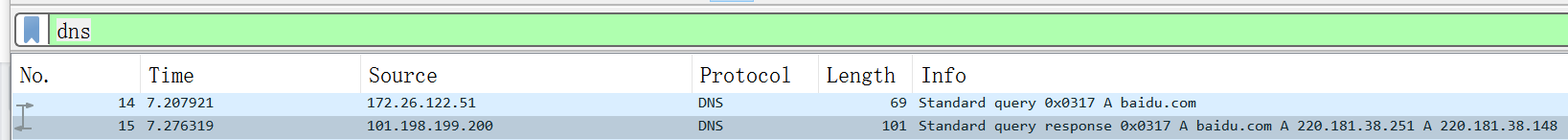




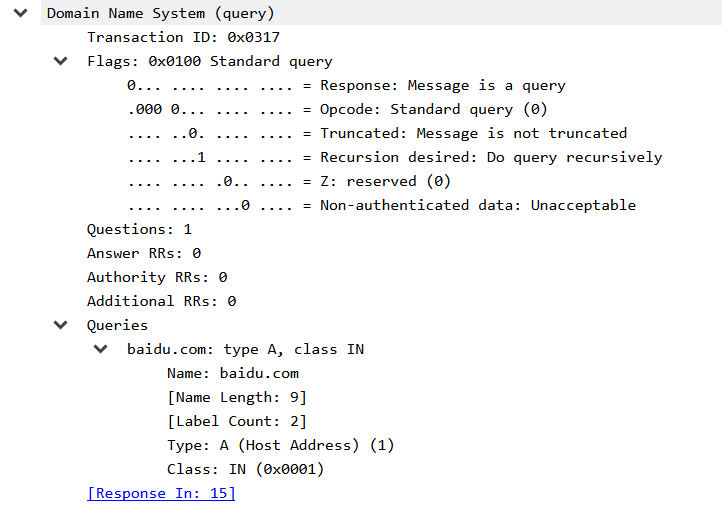
通过CMD来ping www.baidu.com：



通过WIRESHARK捕捉，以下为过滤dns后的列表：



查询请求：



该部分中每个字段含义如下。

事务 ID：DNS 报文的 ID 标识。对于请求报文和其对应的应答报文，该字段的值是相同的。通过它可以区分 DNS 应答报文是对哪个请求进行响应的。

标志：DNS 报文中的标志字段。

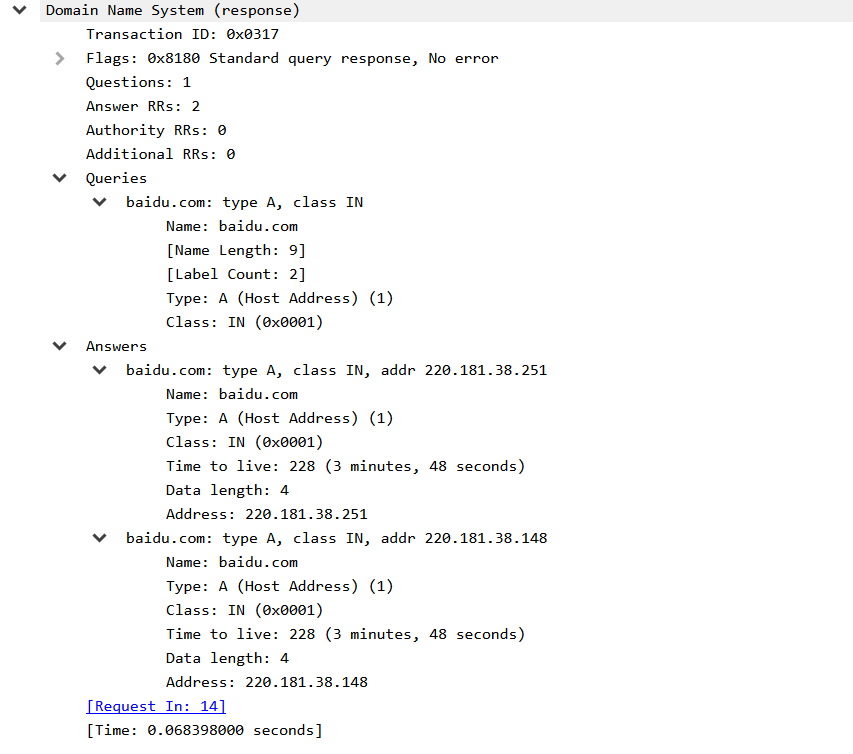
问题计数：DNS 查询请求的数目。

回答资源记录数：DNS 响应的数目。

权威名称服务器计数：权威名称服务器的数目。

附加资源记录数：额外的记录数目（权威名称服务器对应 IP 地址的数目）。

查询响应：



标志字段如下：

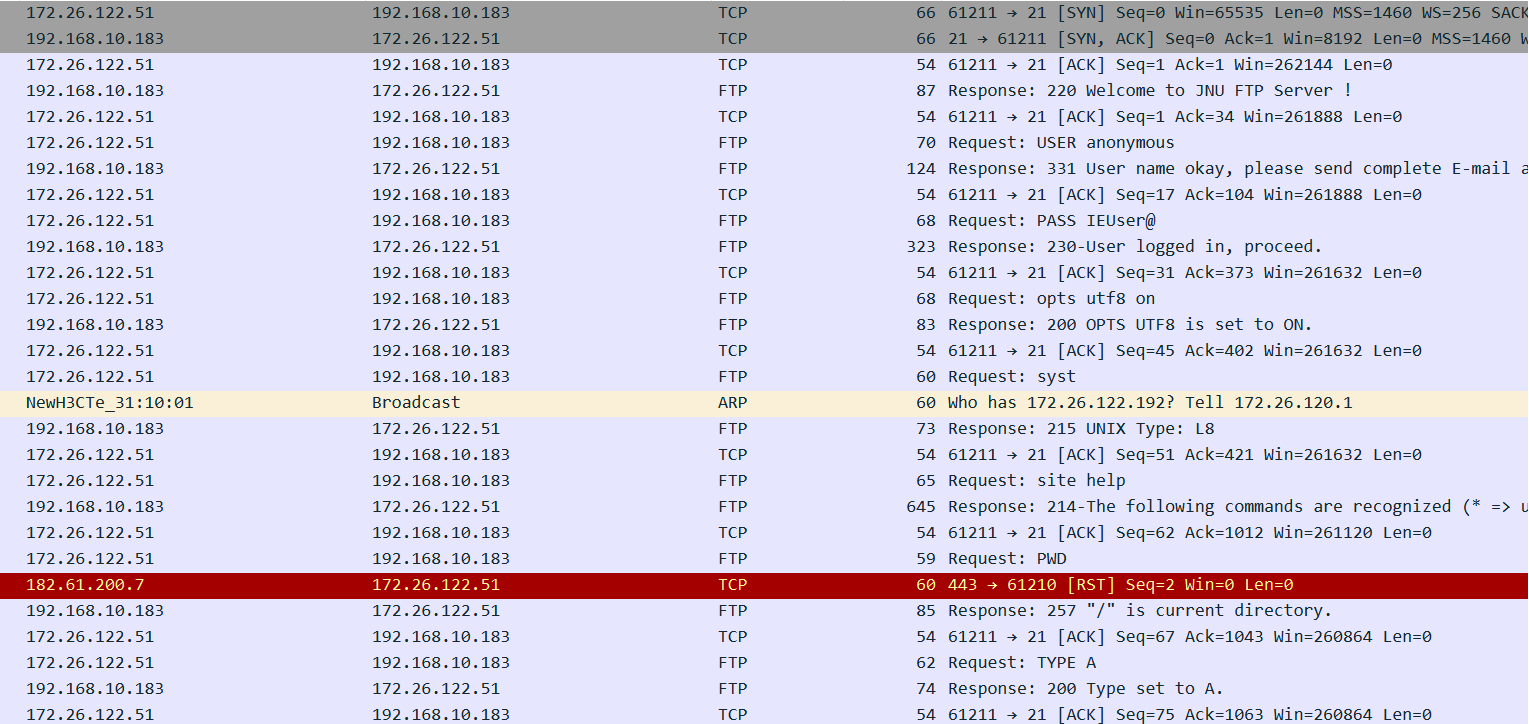
IMG_256

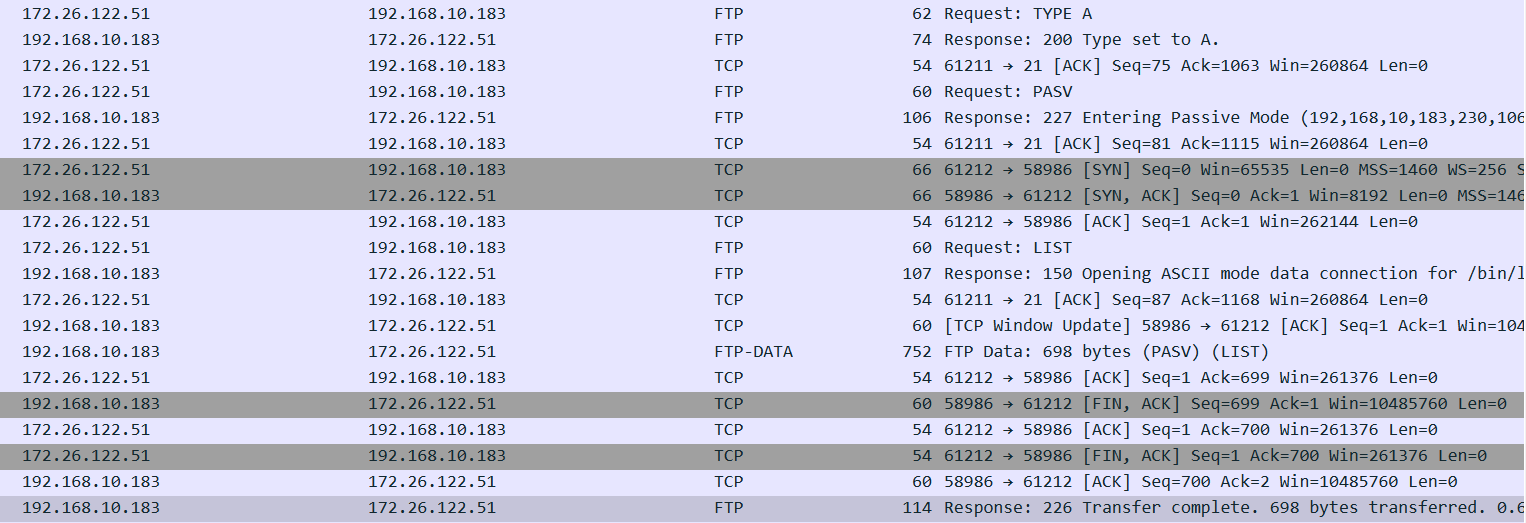
**3、FTP协议分析**

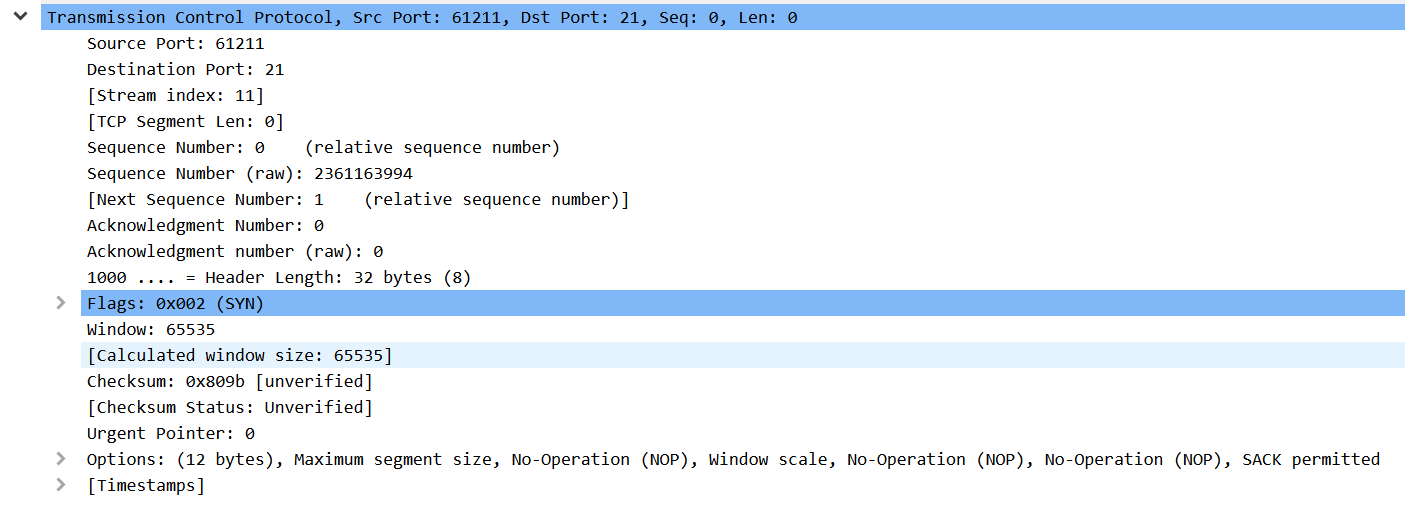
**1.**访问FTP服务器。如ftp://ftp.jnu.edu.cn

2.用wireshark分析FTP的工作过程。注意观察FTP的工作模式，用于控制连接的端口和数据连接的端口。

访问后用wireshark进行捕获：







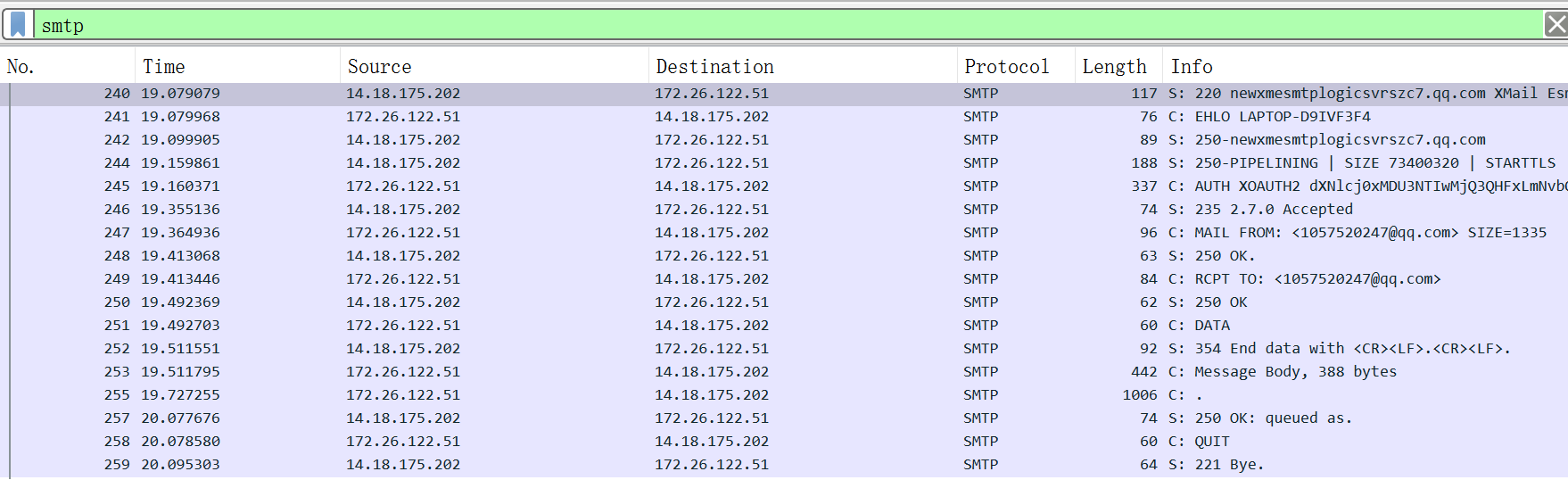
可以观察到，首先服务器和客户建立传输控制块，然后客户进程向服务器发出连接请求报文段，服务器收到连接请求报文后，如同意见已连接则向客户发送确认，客户进程收到服务器的确认后还要向服务器给出确认。

协商工作模式（PASV被动模式）：FTP的服务器进程打开21端口让客户进程连接。以图中的信息为例，61211即为客户，此时服务器收到PASV命令后处于被动模式。服务器收到命令后会开放一个大于1024的端口进行监听，再通知客户端，客户端收到名令后，通过N+1然后在两个端口之间进行数据传输。

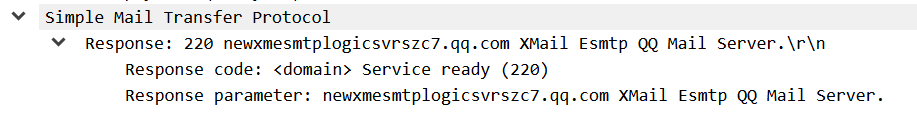
**4、 SMTP和POP协议分析**

基于Web的邮件或客户端的邮件软件（如outlook）收发邮件，捕获数据报分析邮件收发过程和SMTP、POP3等协议格式和工作过程。

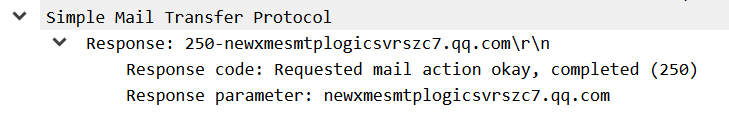
利用FIREFOX客户端发送邮件，用WIRESHARK捕捉。



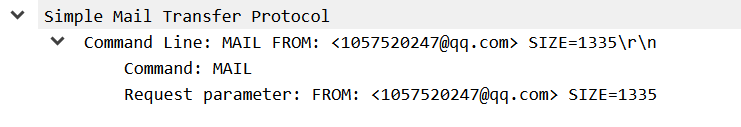
建立TCP连接后，SMTP服务器向客户发送了回应答码220，为客户端提供了服务器的域名。



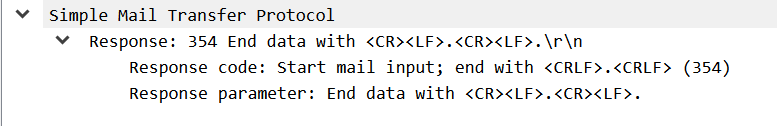
250表示连接建立成功，客户端返回了250码并且附带了身份验证方式。



记录收信人的邮箱和域名。



服务器回应354表示可以输入邮件。



1. **实验设备与环境**

局部网环境，计算机若干台。本实验不分组，独立完成。

1. **实验总结**

**通过本次实验，初步的了解和巩固了HTTP、DNS、FTP、SMTP的工作方式和协议格式。通过对不同协议的研究，能够发现它们的区别，同时加深了对其工作原理的印象。同时，在实验过程中存在理论知识的空白，在一定程度上也回顾和巩固了课上的相关知识，相信这次实验学到的学习经验和学习成果也能在以后的工作和研究生活中发挥其积极作用。**