**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 Internet应用与应用层协议分析 指导教师 潘冰

实验项目编号 03 实验项目类型 验证型 实验地点 B402

学生姓名 许梓弘 学号 2019051107

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 9 月 28 日 下 午～ 9 月 29 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。**

1. **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）

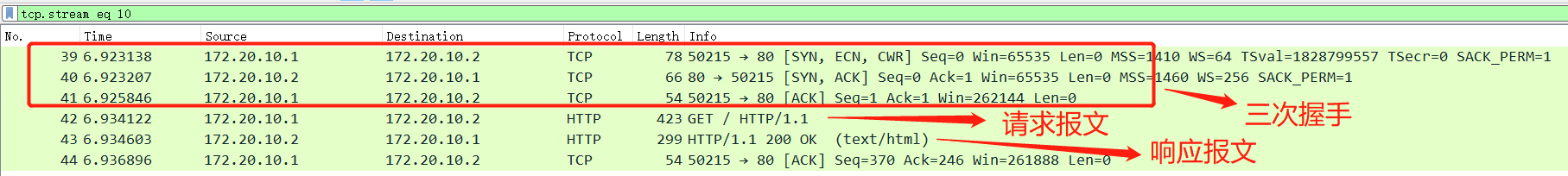
1. **实验设备**

* 一台具有网络功能的PC 机

1. **实验步骤**

**一、HTTP协议分析**

用IIS制作了一个自己的网站主页，将ip地址设为电脑的ip地址172.20.10.2，端口设为80，手机和电脑置于同一个局域网，手机的ip地址为172.20.10.1，用手机访问建立的web站点，用wireshark对其访问过程进行抓包：

可以看到http请求报文发送前需要和服务器建立TCP连接，即三次握手。

点开请求报文进行分析：

请求行由三部分组成，GET是方法，斜杠/是相对url，与下面的Host结合，这里我们访问的是主页，HTTP/1.1是版本。

Host：要访问的主机

Accept：指明浏览器接收对象的顺序，优先接收text/html文件

User-Agent：指明发出请求的用户代理的浏览器的一些信息

Accept-Language：指明了该浏览器支持的语言类型，支持zh-cn

Accept-Encoding：说明该浏览器支持的编码格式，这里是压缩编码的方式

Connection：keep-alive是持续连接，即不用再次握手，用同一个TCP进行连接接受文件，还有个值是close,即非持续连接，每次接受文件都需要进行TCP连接。

点开响应报文进行分析：



状态行中HTTP/1.1是版本字段，200 OK是表示客户端请求成功

Content-Type：表示后面的文档属于什么MIME类型

Server：服务器名字

Date：当前GMT时间

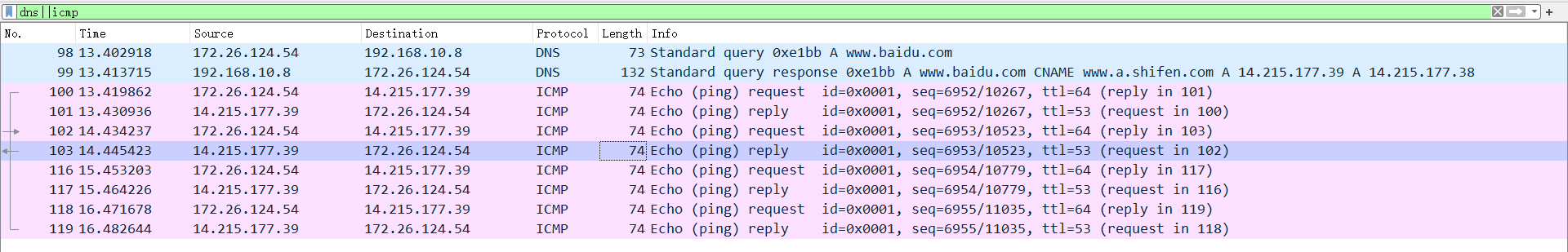
Content-Length：表示内容长度

1. **DNS协议分析**

打开cmd，ping www.baidu.com

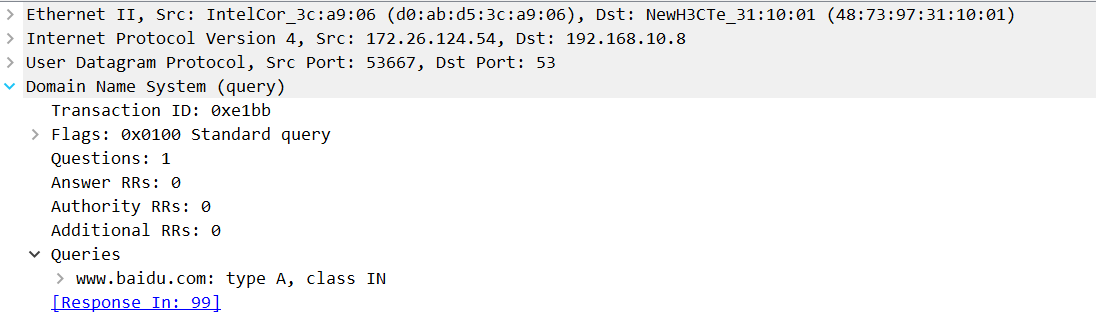


用wireshark进行抓包：



可以看到两个DNS包和八个ICMP包，因为ping了四次，发送了四个包，接受了 四个包。

点开第一个包，即DNS请求包，发送方是本机，接收方是本地域名服务器



第一个是Transaction ID为标识字段,2字节,用于辨别DNS应答报文是哪个请求报文的响应.

第二个是Flags标志字段,2字节,每一位的含义不同:

IMG_256

QR: 查询/响应,1为响应,0为查询

Opcode: 查询或响应类型,这里0表示标准,1表示反向,2表示服务器状态请求

AA: 授权回答,在响应报文中有效,待会儿再看

TC: 截断,1表示超过512字节并已被截断,0表示没有发生截断

RD: 是否希望得到递归回答

RA: 响应报文中为1表示得到递归响应

zero: 全0保留字段

rcode: 返回码,在响应报文中,各取值的含义:

0 - 无差错

1 - 格式错误

2 - 域名服务器出现错误

3 - 域参照问题

4 - 查询类型不支持

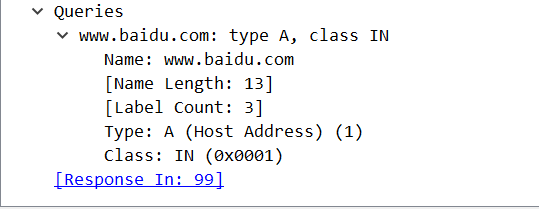
5 - 被禁止

6 ~ 15 保留

Quetions(问题数),2字节,通常为1

Answer RRs(资源记录数),Authority RRs(授权资源记录数),Additional RRs(额外资源记录数)通常为0

字段Queries为查询或者响应的正文部分,分为Name Type Class

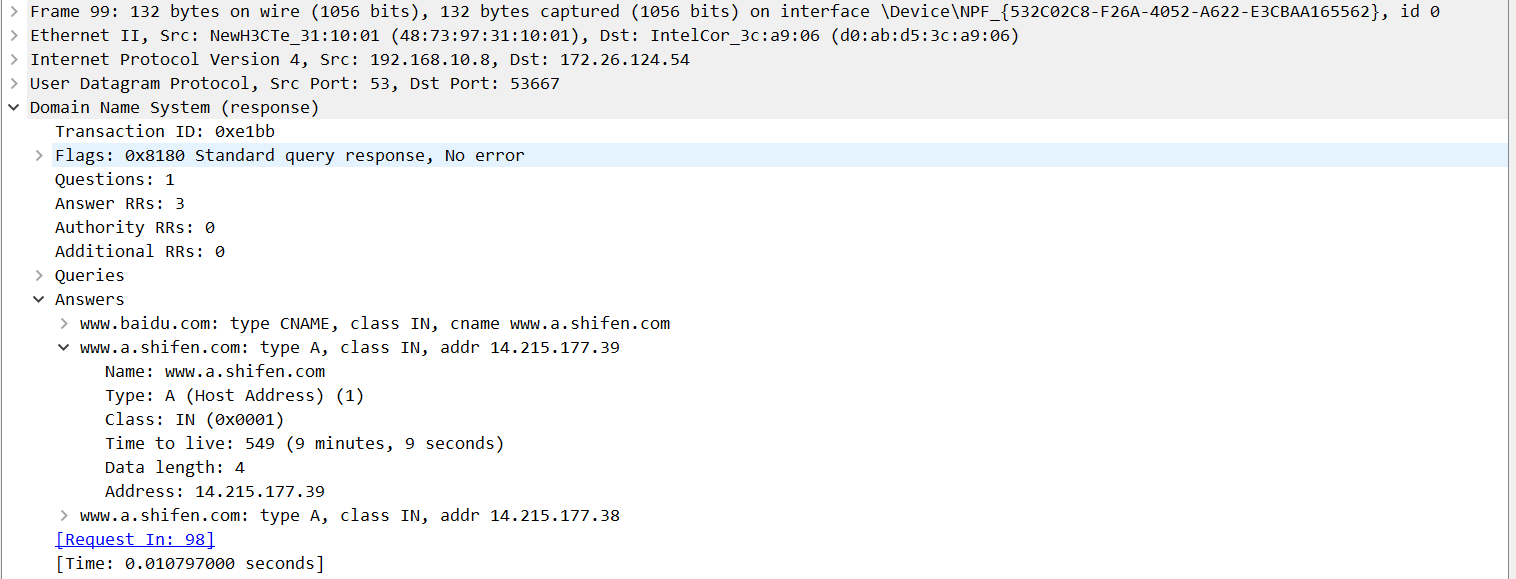


Name(查询名称):这里是ping后的参数,不定长度以0结束

Type(查询类型):2字节,这里是主机A记录，表示**IPv4地址。**

Class(类):2字节,IN表示Internet数据,通常为1

点开第二个DNS包，即相应包

与DNS请求包类似，只是多了个Answers字段，并且Flags有了定义。

Answers字段可以看成一个List,集合中每项为一个资源记录,除了上面提到过的Name,Type,Class之外,还有Time to Live,Data length,Addr.

第一行www.baidu.com的type是CNAME，就是定义了一个别名，即www.a.shifen.com，我们点开下面一行的，type是A，即有我们要找的ip地址

Time to Live(生存时间TTL):表示该资源记录的生命周期,从取出记录到抹掉记录缓存的时间,以秒为单位.这里是0x00 00 00 fd 合计253s.

Data length(资源数据长度):以字节为单位,这里的4表示IP地址的长度为4字节.也就是下面Addr字段的长度.

Addr(资源数据): 返回的IP地址,就是我们想要的结果.

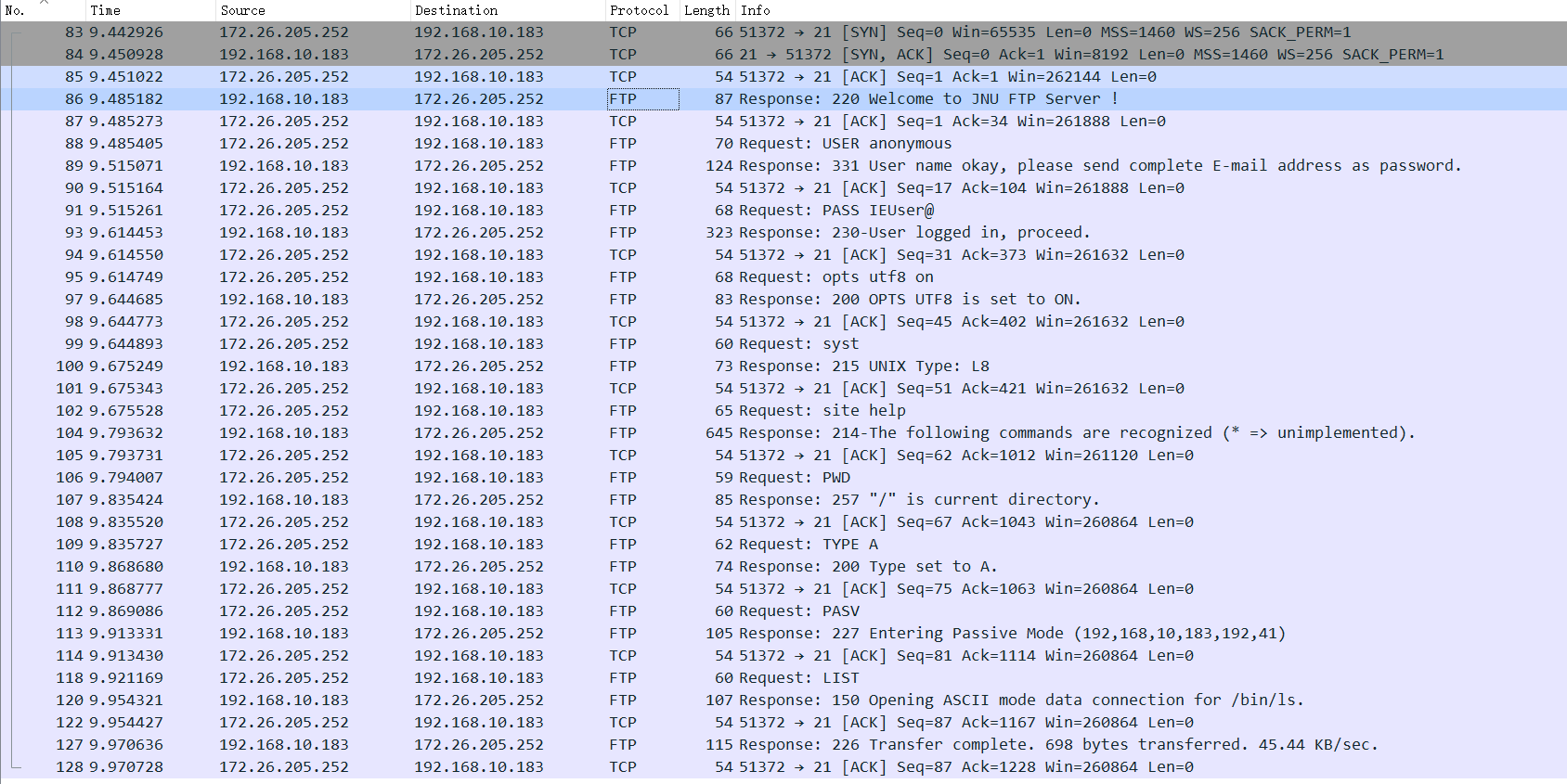
**注意：**

1. 有时候可能捕获不到DNS解析过程，为什么？要仔细分析。

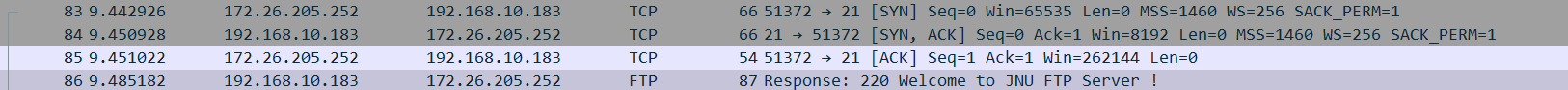
因为最近访问过这个网站，该网站的ip地址会被浏览器，操作系统缓存起来，再次访问该网站则直接从缓存中获取ip地址。

**三、FTP协议分析**

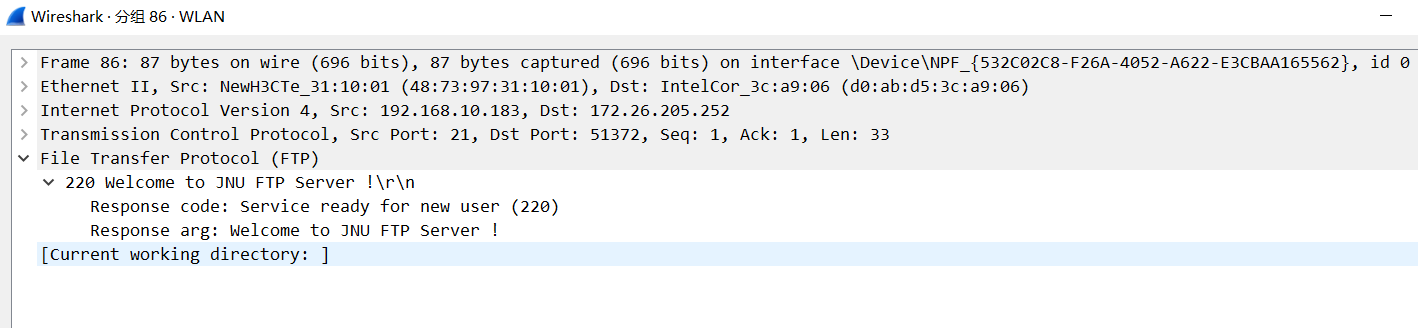
访问学校FTP服务器ftp://ftp.jnu.edu.cn，并进行抓包分析：



1-3是tcp包，tcp三次握手建立连接，可以看出ftp是基于tcp的



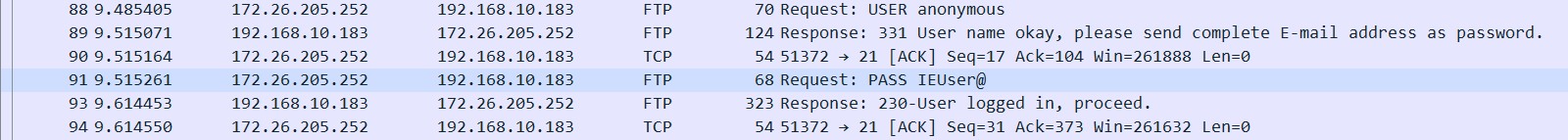
第四个包是FTP包，是服务器的响应报文，状态码220表示建立连接成功，并以ascii码方式明文传输数据



第五个包是客户端向服务器发送的确认。

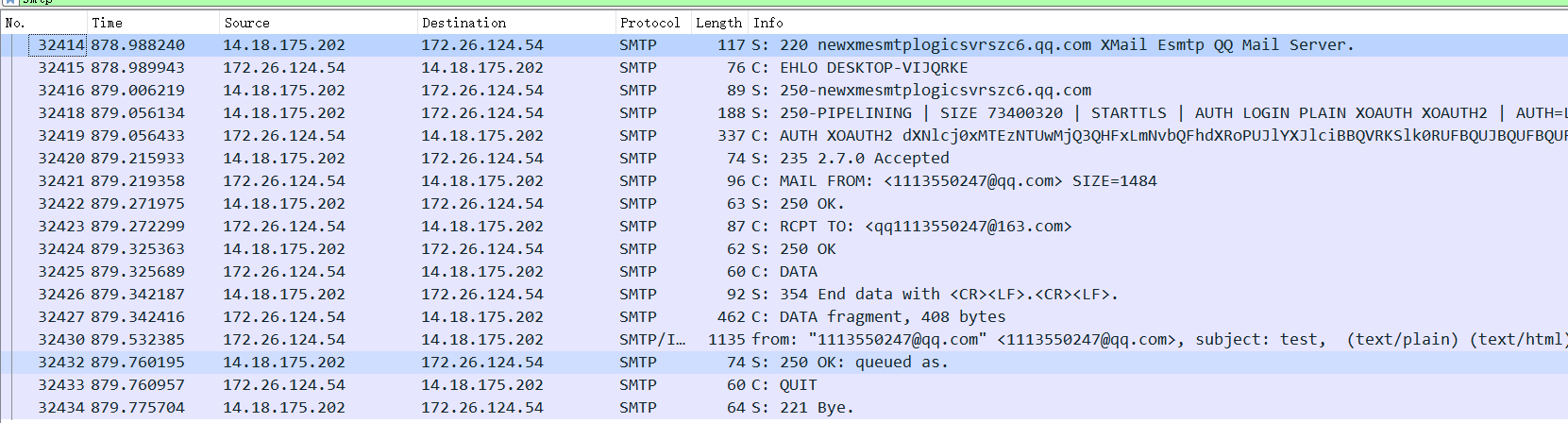
第六到十一个包分别是：客户端输入用户名；服务器端确认并提示输密码；客户端确认；客户端发送密码；服务器端确认密码正确；客户端确认收到。

其中，密码和用户名都是明文的，如下图

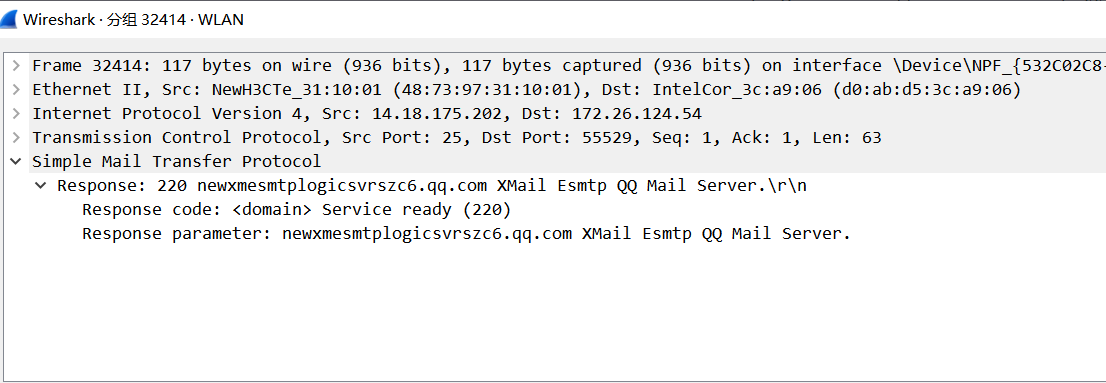


**四、 SMTP和POP协议分析**

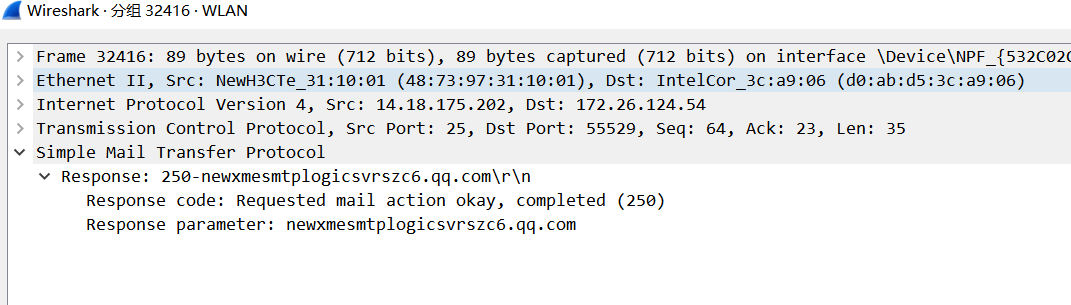
用foxmail登陆邮箱后发送邮件，用wireshark捕获SMTP包：



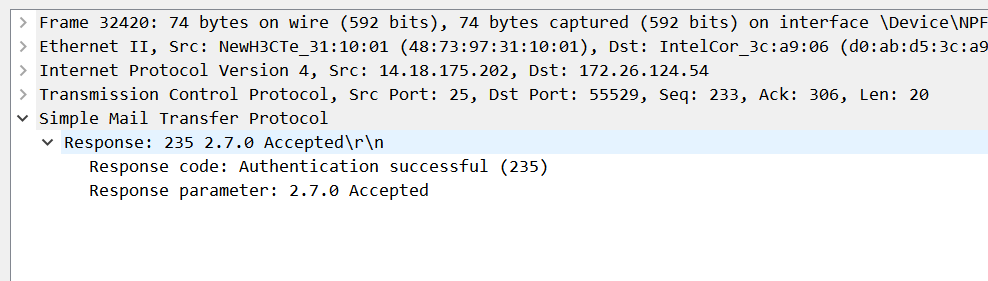
状态字220代表连接SMTP服务器成功：



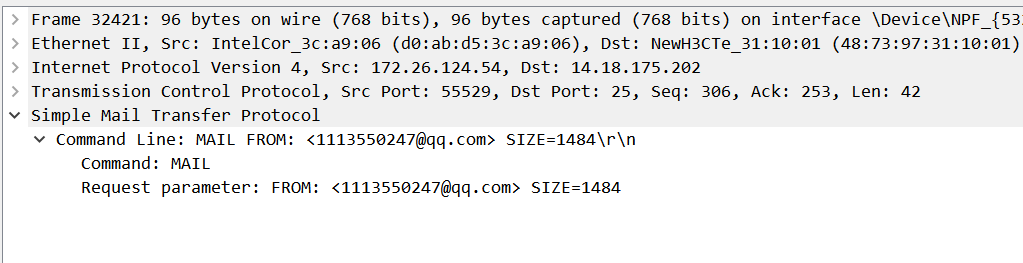
状态字250表示与服务器握手成功：



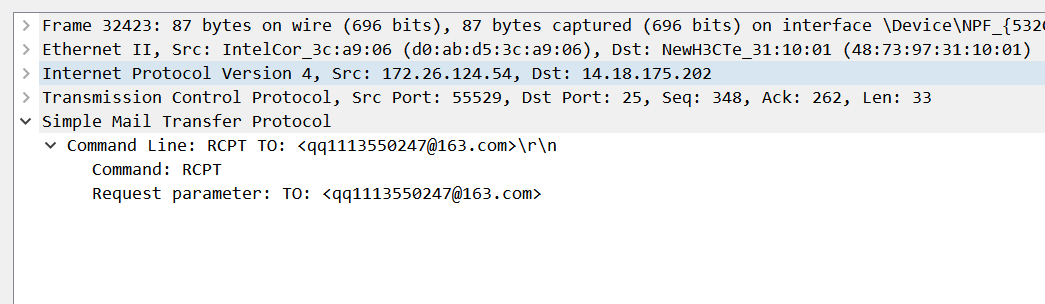
状态字235代表用户登录成功：



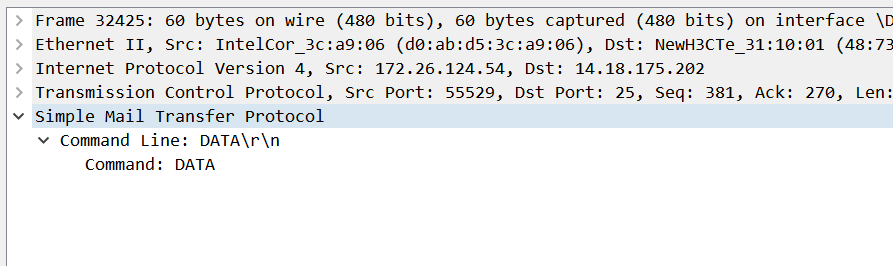
该字段记录邮件的发送者，必须存在且完全正确：



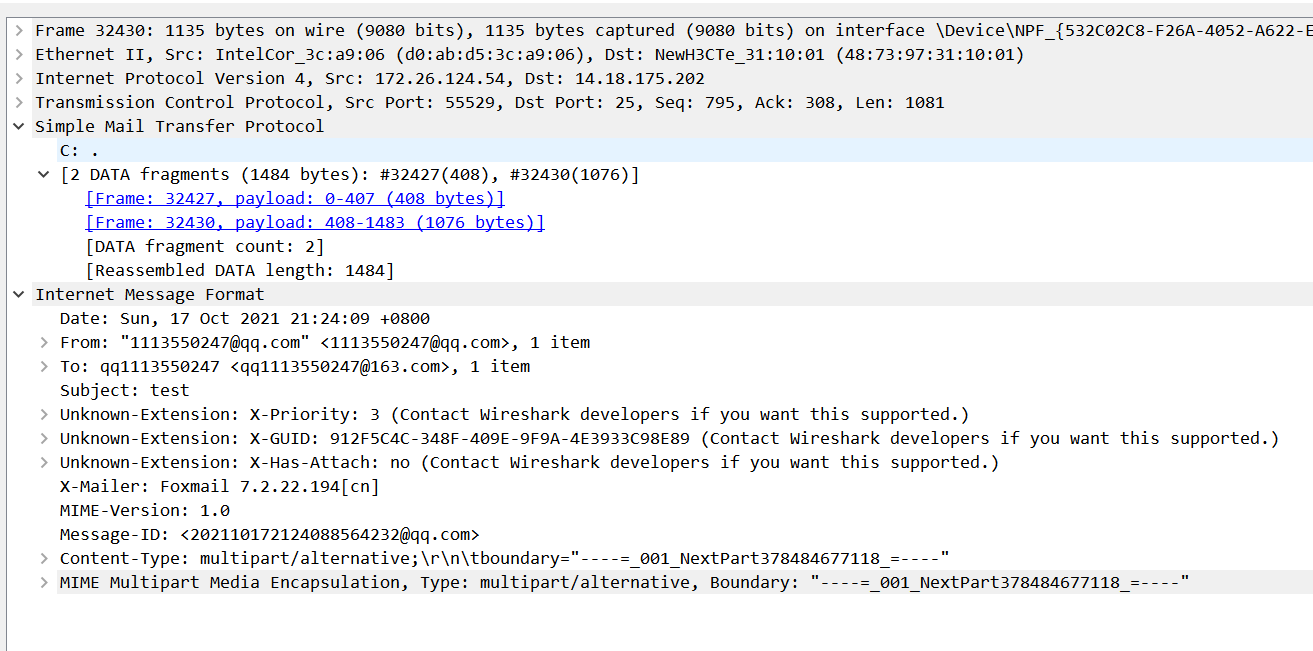
邮件的接收方：

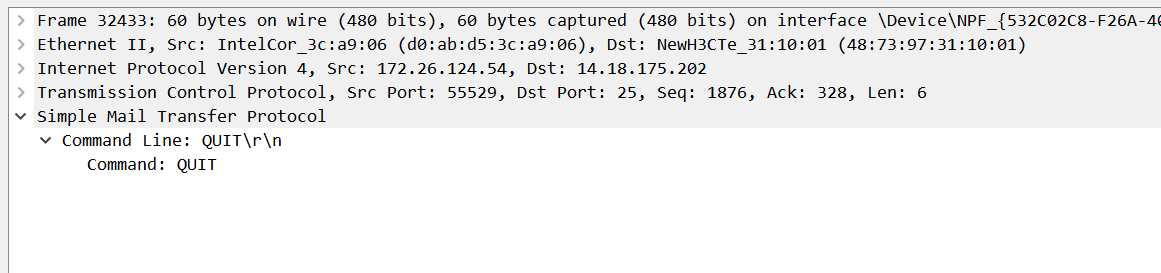


DATA明令表示以下为邮件正文：



这个数据包包含了SMTP和IMF两个部分，因为抓包发送的邮件内容都是文本，所以直接使用[IMF协议](https://link.zhihu.com/?target=https://wiki.wireshark.org/IMF" \t "https://zhuanlan.zhihu.com/p/_blank)就可以传输，而SMTP协议中的报文内容则是DATA命令的终止标志：

退出SMTP服务器：



**五、实验结果与分析**

**对协议有了更深的了解，能够清楚报文的结构及其内容。**