**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 实验项目类型 实验地点 计算机网络实验室

学生姓名 梁伟希 学号 2019051117

学院 智能科学与工程 系 专业 信息安全

实验时间 2021 年 10 月 12 日 上 午～ 10 月 12 日 上 午

|  |
| --- |
| **一、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。** |

|  |
| --- |
| **二、实验环境** |
| 局部网环境，计算机若干台。本实验不分组，独立完成。 |
| **三、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） |

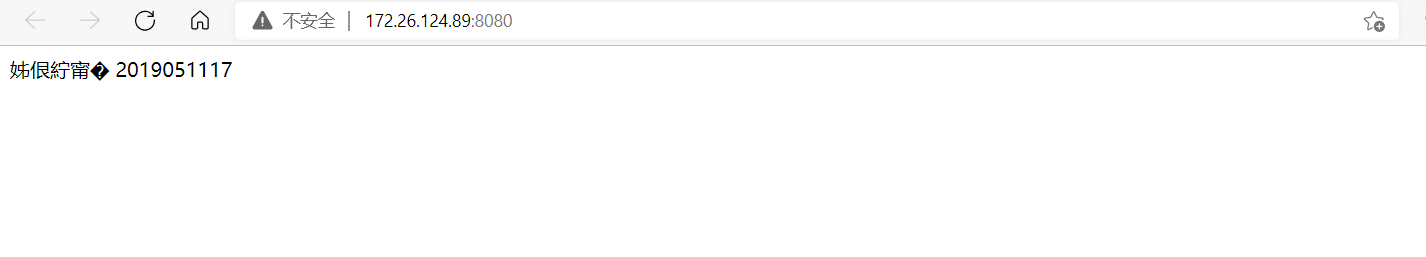
**四、实验及分析**

**【实验步骤】**

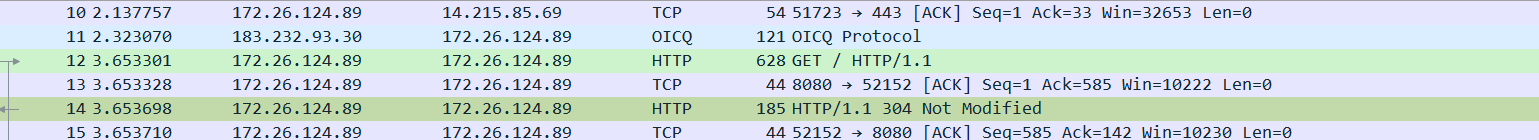
**一、HTTP协议分析**

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）

访问了http：//[172.26.124.89:8080](http://172.26.124.89:8080/)，



应用wireshark抓取HTTP协议数据包，得到了是HTTP请求（GET），HTTP响应，还有TCP的三次握手和释放TCP连接。

下面仅分析HTTP协议的工作过程和HTTP协议格式：

工作过程：

  (1) 服务器持续监听TCP端口80，监听到来自客户的连接建立请求后，与客户建立TCP连接，即浏览器与服务器建立 TCP 连接

  (2) 浏览器发出读取文档的命令，发送一个http请求

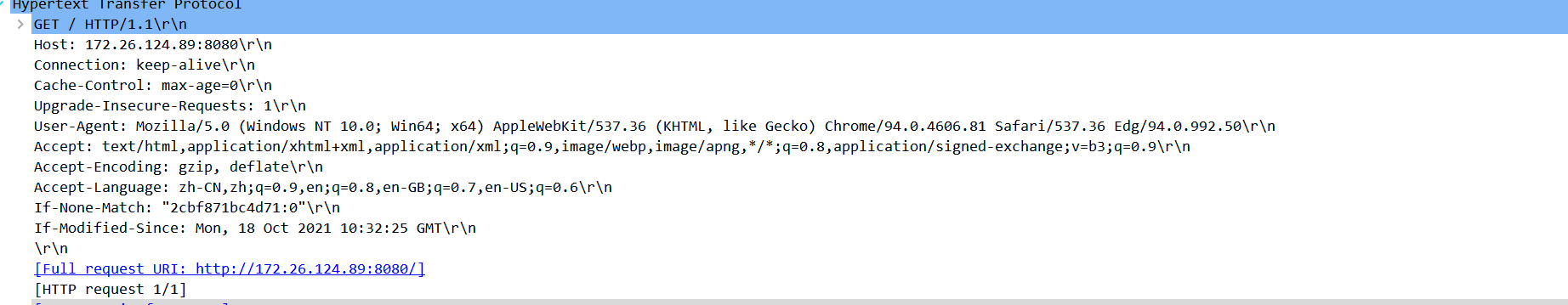
(3) 服务器给出响应，把文件 index.htm 发给浏览器，并发送了http响应

  (4) TCP 连接释放。

  (5) 浏览器显示文件 index.htm 中的所有文本。

HTTP协议格式：

1. **请求报文的分析如下：**

****

**请求行：**

GET方法表示这是一个请求报文，http协议的版本是HTTP/1.1。

**首部信息：**

Host字段：指定请求服务器的IP地址和端口号，这里是172.26.124.89，端口为8080

Connection字段：浏览器与服务器之间连接的类型，上图中的keep-alive表示建立了一个持续的连接。

Upgrade-Insecure-Requests字段：Upgrade-Insecure-Requests:1这个字段表示当前的浏览器告诉服务器，它能读懂服务器发过来的信息，但是请他下一次发送的时候用https，故浏览器加入了一个‘Upgrade-Insecure-Requests: 1’。

User-Agent： 浏览器的身份标识字符串。可用于区分用户是否为爬虫

Accept字段：告诉服务器浏览器可接受的响应内容类型。

Accept-Encoding字段：浏览器可处理的压缩编码类型。

Accept-Language字段：表示浏览器支持的语言

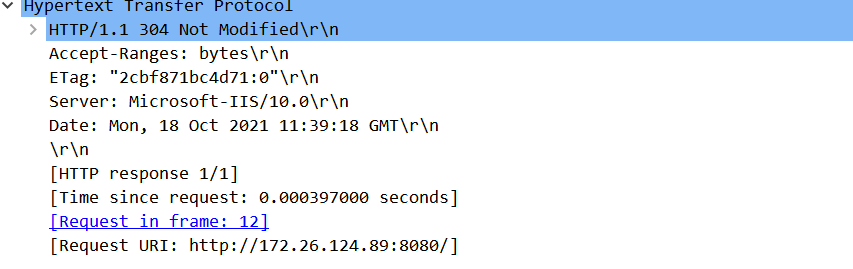
**实体主体：**

Full request URI:请求的URI全称。，这里为http://172.26.124.89:8080/

倒数第二行表示HTTP请求进度

倒数第一行表示响应帧，对应14。

1. **响应报文的分析如下：**

****

有一些字段和请求报文中的不一样

状态行HTTP/1.1是协议版本；304是状态码，表示状态没有改变；后面的英文短句是对状态码的简单解释

Etag：资源实体的指纹，并且他们能够被快速地被比较，以确定两个版本的资源是否相同。

Server：服务器的名称。这里是微软的ISS服务

Date：表示当前的标准时间。

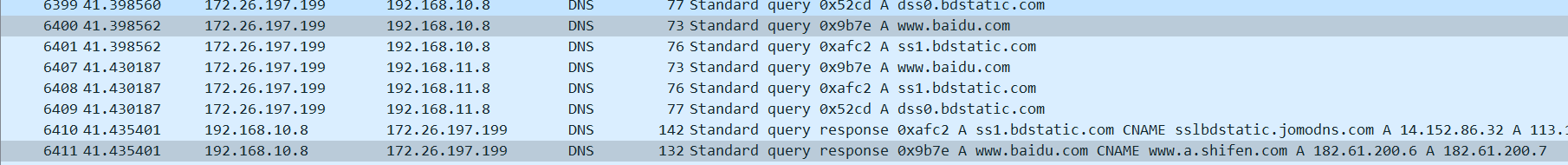
HTTP response 1/1表示HTTP响应进度；Time since request响应时间；

Request in frame表示请求帧，12；

**2、DNS协议分析**

1. 访问www.baidu.com,:
2. 通过wireshark抓包进行分析

可以得到下图中的情况，标黑的二者分别是请求帧和响应帧。



1. 分析DNS工作过程和DNS报文格式：

DNS的工作过程：

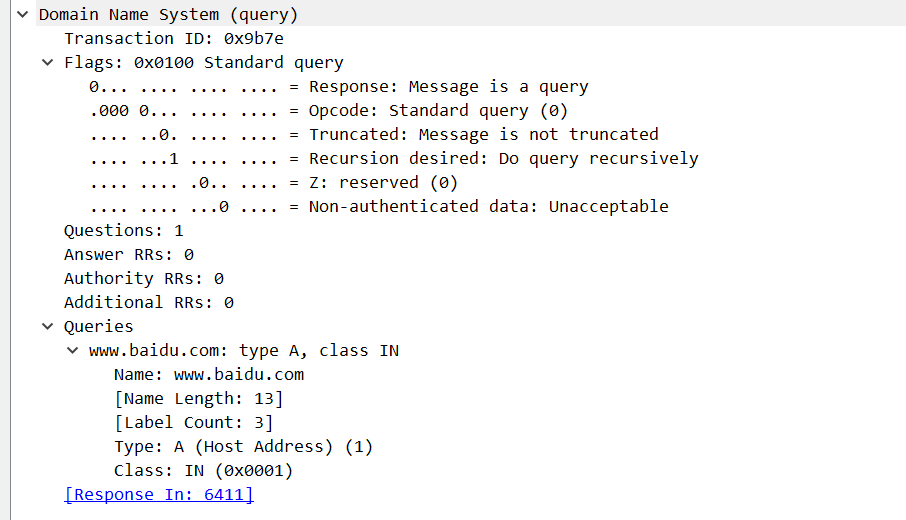
第一步：客户机提出域名解析请求，并将该请求发送给本地的域名服务器（发送递归请求）。

第二步：当本地的域名服务器收到请求后，就先查询本地的缓存，如果有该纪录项，则本地的域名服务器就直接把查询的结果返回。 如果本地的缓存中没有该纪录，则本地域名服务器就直接把请求发给根域名服务器.

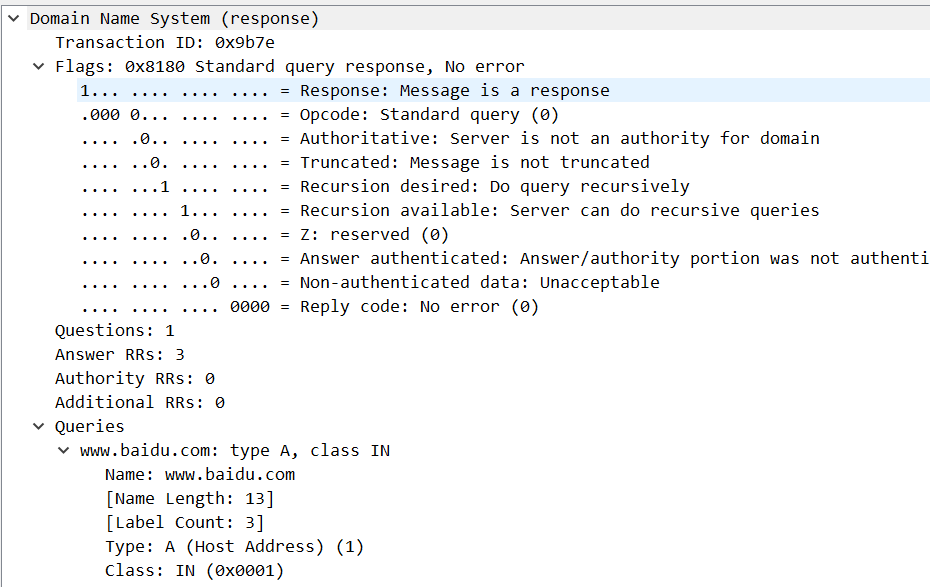
第三步：根域名服务器再返回给本地域名服务器一个所查询域(根的子域) 的主域名服务器的地址。本地服务器再向上一步返回的域名服务器发送请求，然后接受请求的服务器查询自己的缓存，如果没有该纪录，则返回相关的下级的域名服务器的IP地址。

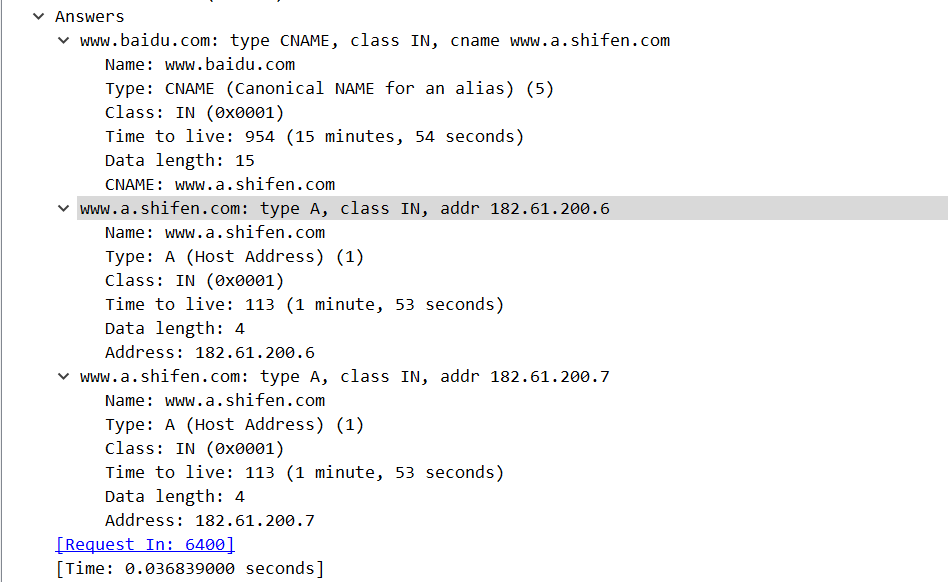
第四步：重复第三步，直到找到正确的纪录。本地域名服务器把返回的结果保存到缓存，以备下一次使用.DNS报文分析（这里主要对报文的基础结构部分和问题部分进行分析）

**请求：**



**回答：**



**基础结构部分**：

Transaction ID字段：即事务ID，请求报文跟其相对应应答报文中的ID相同。

Flags字段：标志字段。其中各行均有不同含义。Response字段若为0，表示这是一个请求报文，若为1即表示应答； Opcode字段若为0表示标准查询/响应； Truncated字段表示是否被截断，值为 1 时，表示响应已超过 512 字节，并已被截断，返回前 512 个字节；Recursion Desired字段为1，表示这里进行递归查询；Z作为一个保留字段，它的值必须为0。on-authenticated data: Unacceptable

，保留字段, 值为0

Answer RRs表示回答资源记录数

Authority RRs表示权威名称服务器计数

Additional RRs表示附加资源记录数

值得注意的是，在响应报文中以上三个均不为0了

Questions字段表示问题计数, 这里有1个问题，对应着下面的Queries字段。

响应报文中特有的字段有Authoritative: Server is not an authority for

domain AA字段和Recursion available: Server can do recursive queries 即RA字段

**问题部分：**

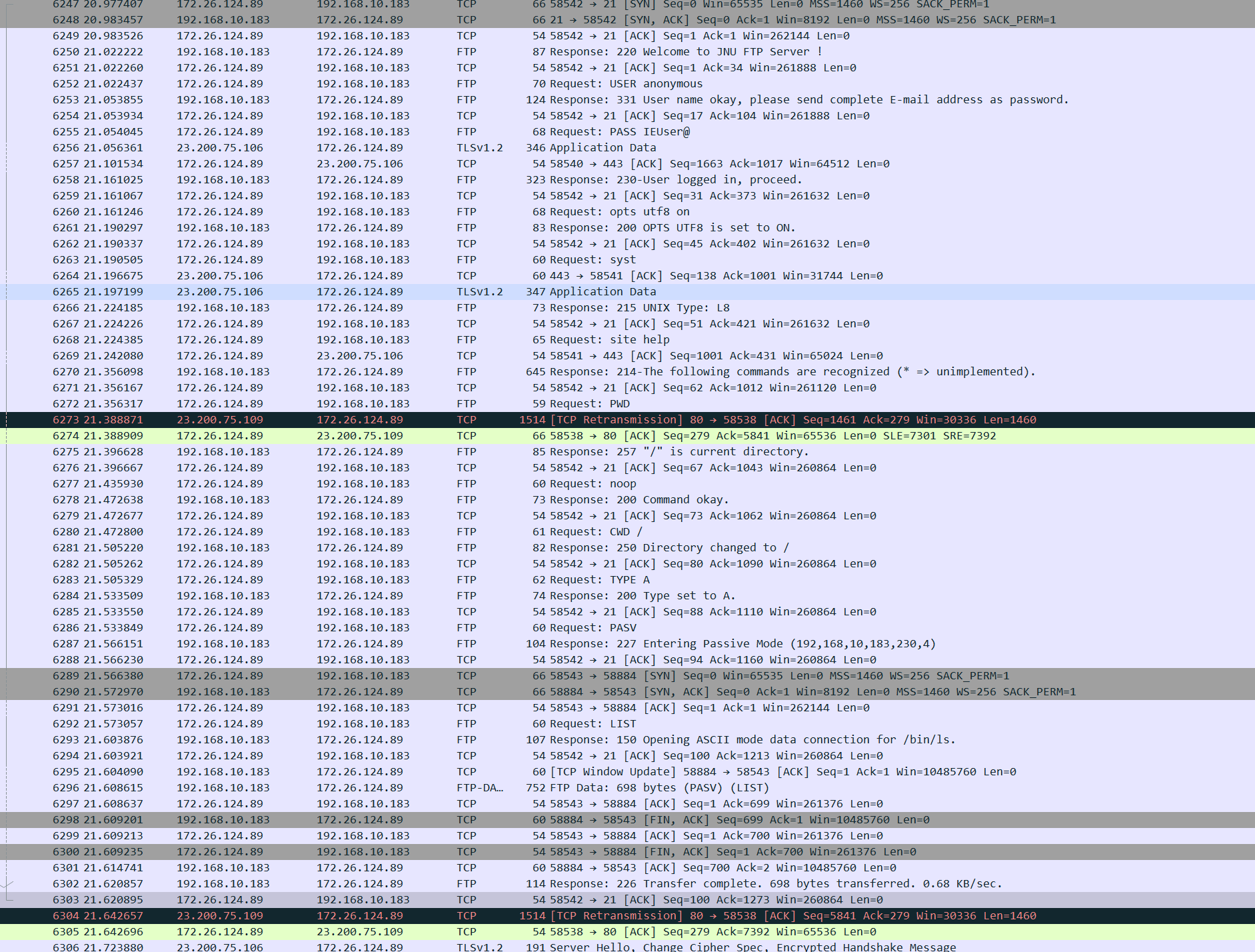
www.baidu.com是所需要请求解析的域名，type A表示由域名（Host Address）获取对应的 IP 地址，class IN表示地址类型为互联网地址。

最后一行的是对应的应答报文或请求报文所在的帧。

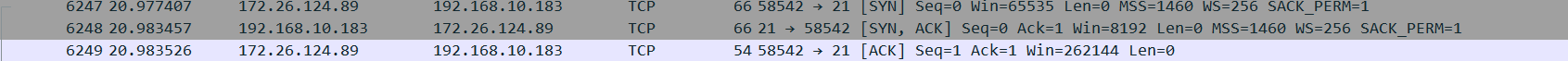
**3、FTP协议分析**

1.使用文件进入暨南大学的ftp，ftp://ftp.jnu.edu.cn

2.使用wireshark进行抓包，由于报文过多且后面有英文短句作为描述，这里不句句都解析，关键是理解ftp协议工作过程

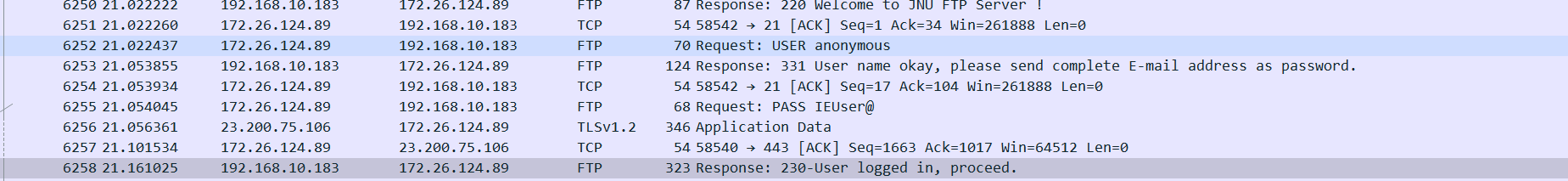
****

建立连接阶段：



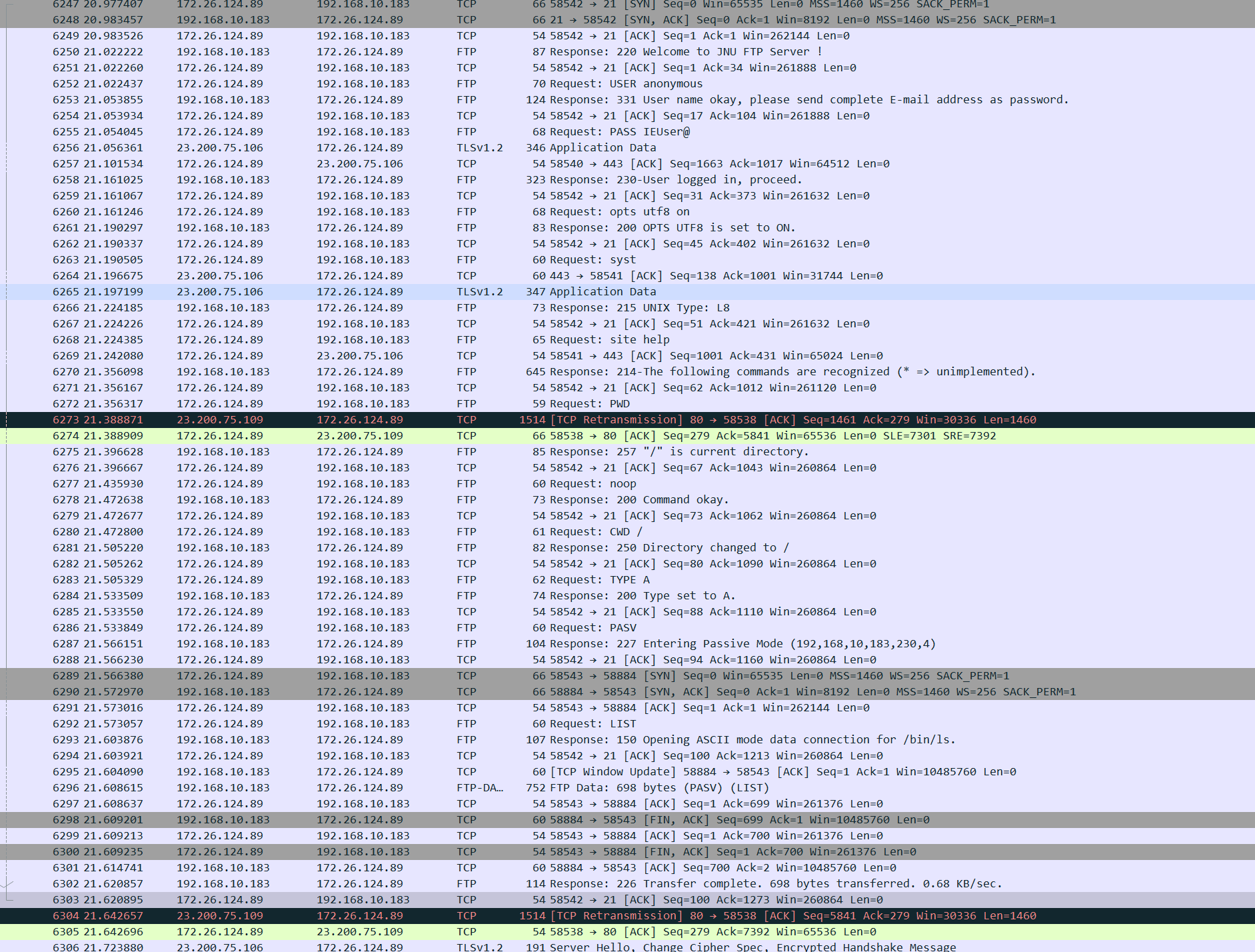
TCP三次握手建立控制连接（6247-6249），58542是客户端随机开启的一个端口，21是文件传输服务器端口。

身份认证阶段：



即输入账户密码等来验证用户身份。如果正确，将进入ftp会话。

命令交互阶段：

****

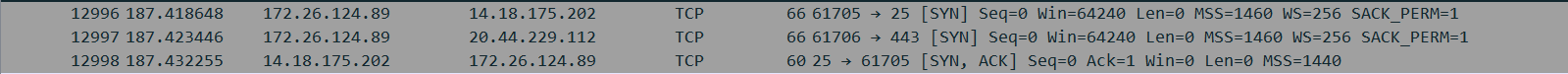
在这个阶段中，客户端输入要执行的 FTP 命令后，服务器同样会给出应答。如果输入的执命令正确，服务器会将命令的执行结果返回给客户端。执行结果返回完成后，服务器继续给出应答。这里协商了工作模式，将变为PASV，即被动模式，在被动模式下，FTP客户端向服务器发送PASV命令，通知服务器自己处于被动模式。值得注意的是，当服务器收到这个命令后，会开放一个大于1024的端口P进行监听(上图中是58884)，然后通知客户端。客户端收到命令后，会通过58543（即58542+1）号端口与服务器的端口建立数据连接(也是要进行三次握手)，然后在两个端口之间进行数据传输。

断开连接阶段：

当客户端不再与 FTP 服务器进行文件传输时，需要断开连接。客户端向 FTP 服务器发送断开连接请求，服务器收到断开连接后给出相应的应答。

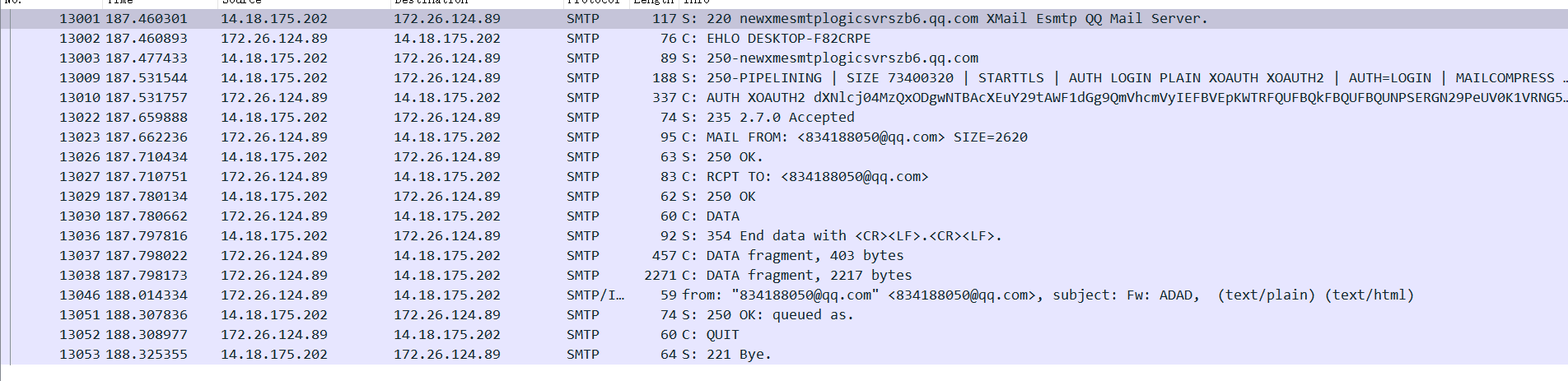
在断开时，TCP进行了四次挥手。

1. **SMTP和POP协议分析**
2. 使用QQ邮箱，从用户834188050@qq.com发送一封测试邮件给另一个QQ邮箱用户，并利用wireshark抓包。
3. **SMTP协议的工作过程及协议格式：**

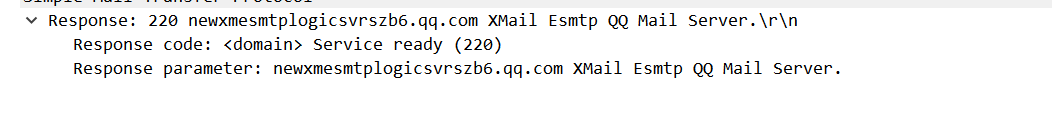


这里的14.18.175.202是SMTP服务器的IP地址

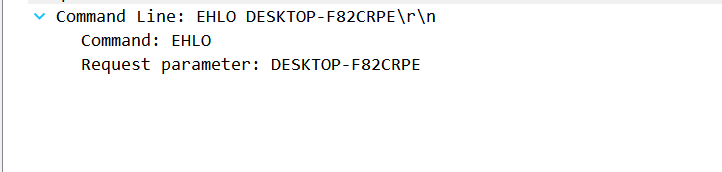
1. 首先是本机（172.26.124.89）与SMTP服务器三次握手建立TCP连接。



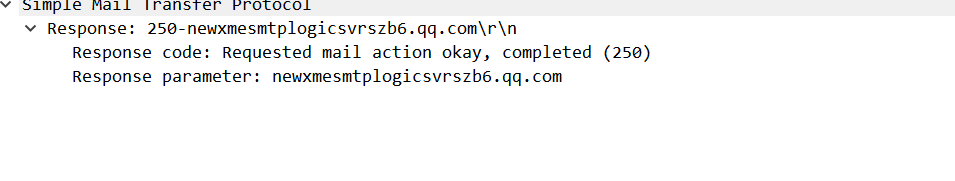
连接建立后，SMTP服务器发出状态“220”，即第一个STMP数据包，表示服务已经就绪：



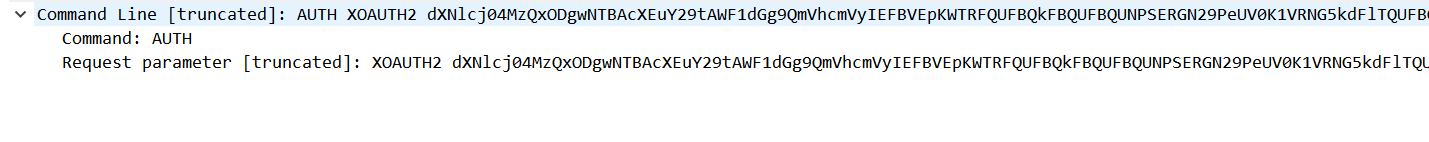
然后发送EHLO命令，即进行身份验证：



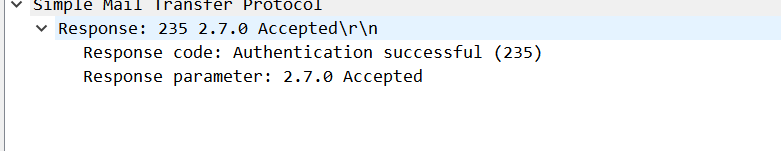
服务器回复“250”即代表有能力进行邮件回复



发送AUTH命令来进行身份验证

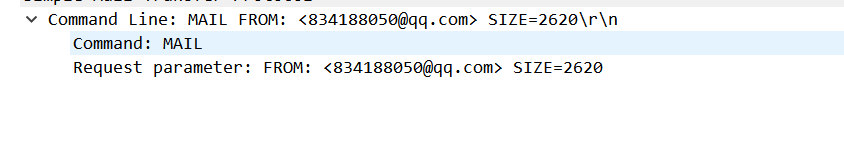


服务器回复“235 Authorization successful”即Accepted，身份验证成功。



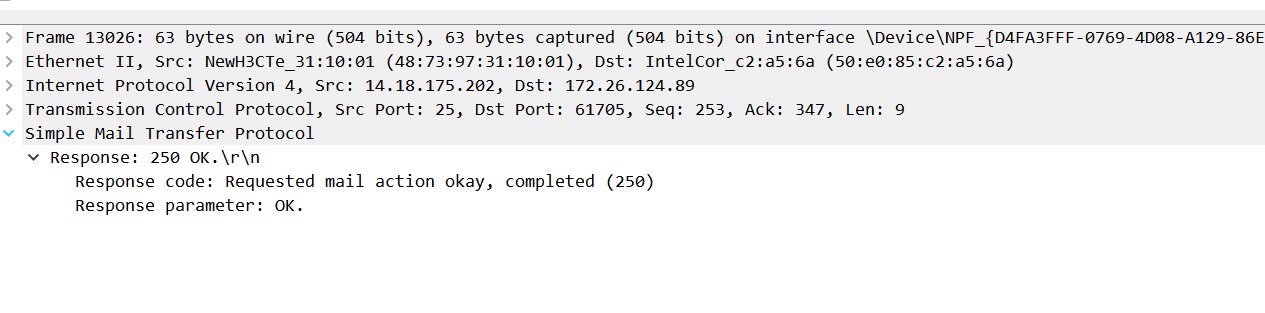
之后进入邮件的传送部分：

这一部分从发送MAIL命令开始

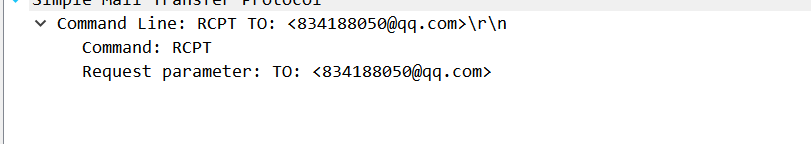


后面跟有发送者的邮件地址。

服务器回复“250 OK”，表示已做好准备接收邮件：

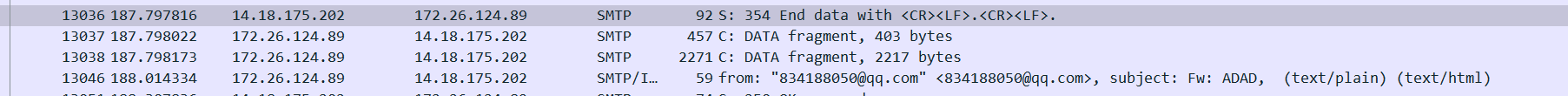


RCPT命令，应该是表示邮件的收件人地址，但这里不知为何是自己的邮箱



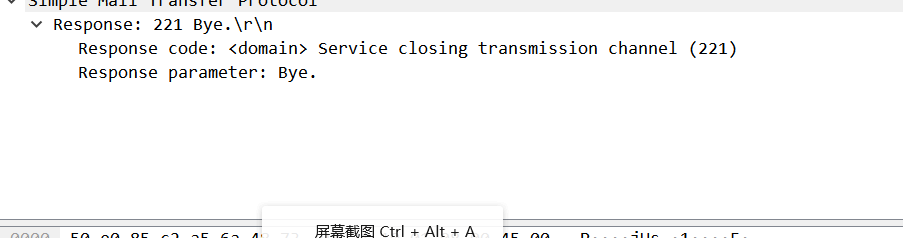
服务器回复“250 OK”

再下面就是DATA命令，表示要开始传送邮件内容了，之后的几行应该表示的是邮件的内容和相关设置

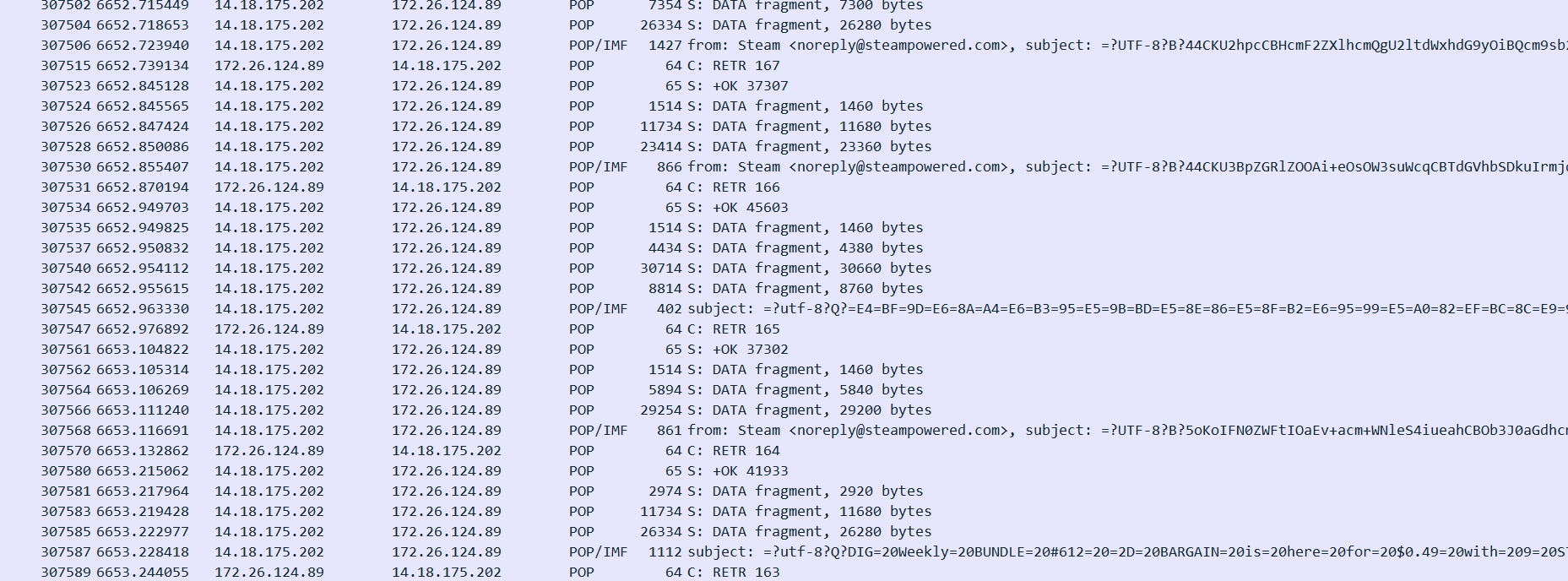


在发送邮件之后，SMTP服务器回复“250 OK”，表示已经收到了邮件。

邮件发送完毕后，SMTP客户端发送QUIT命令，服务器回复221 Bye，即表示释放连接



POP协议的工作方式，与smtp大同小异，这里不做过多的叙述



**五、实验总结**

本次实验分析了多种十分重要的应用层协议，了解了它们的报文格式，分析了它们的工作方式。知晓了它们之间的异同，也知道了tcp和udp等协议的重要性。这几种协议，都需要客户服务器以工作。通过完成本次实验，加深理解之后，在日后的学习与工作中，必定受益匪浅，影响深远。