**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 3 实验项目类型 实验地点 机房

学生姓名 罗清 学号 2019053295

学院 智能科学与工程学院 系 专业 信息安全

实验时间 年 月 日 午～ 月 日 午温度 ℃湿度

# 一、实验目的

1. 理解WWW、DNS服务、FTP服务、SMTP服务的作用和原理；
2. 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。

# 实验内容

1. 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；
2. 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）

# 实验环境

局域网环境，计算机若干台。

# 实验步骤

## HTTP协议分析

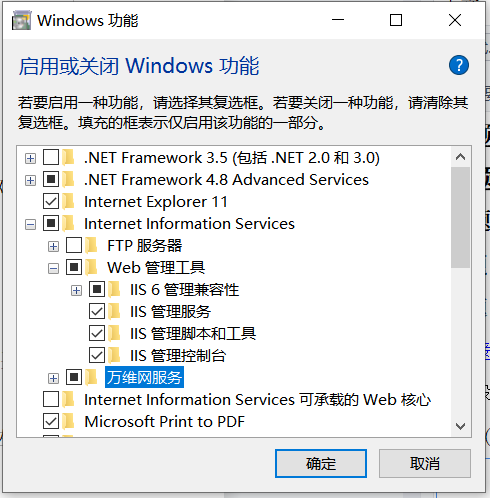
本次实验采用利用windows自带组件（IIS）安装配置WWW站点，并对站点进行访问、通过WireShark对网络进行抓包、分析网站的访问过程。

### WWW的安装和配置

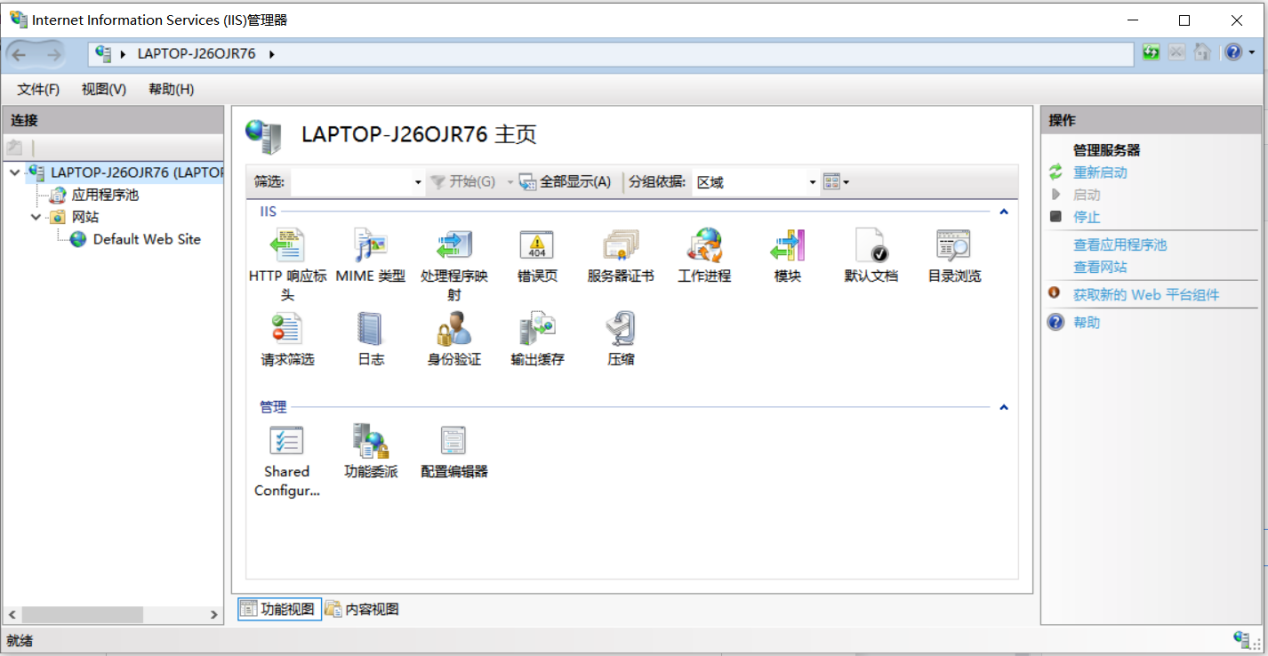
首先进行IIS6.0的安装与开启（经过查看，本机预先已安装好IIS6.0必要组件，故接下来介绍如何查看相关组件及如何开启）

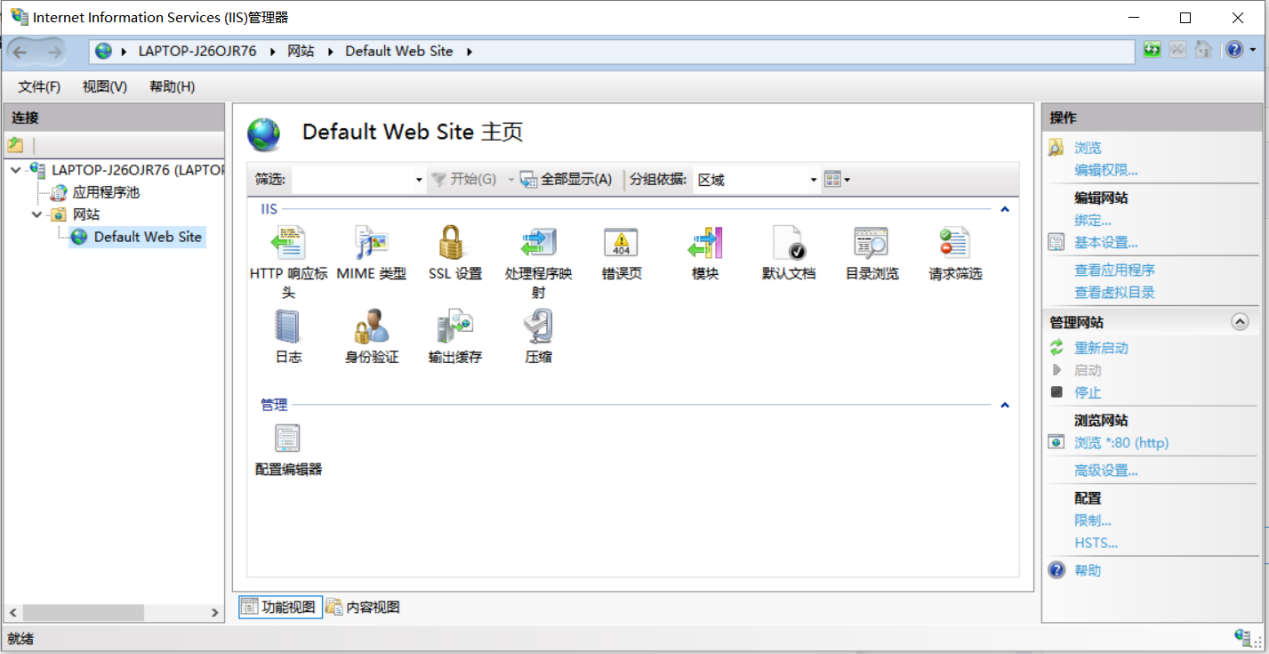
①将控制面板查看方式设置为大图标，点击“程序和功能”按钮，点击左侧“启用或关闭Windows功能”，打开Windows功能界面。

②将Internet Infomation Services下的IIS选项和万维网选项全部打开，如图所示。



③回到“控制面板”，点击“管理工具”，打开“Internet Infomation Service管理器”，可以看到窗口中有两个Web站点，分别是管理Web站点及默认Web站点。



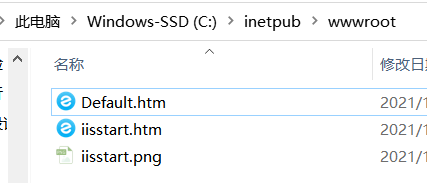


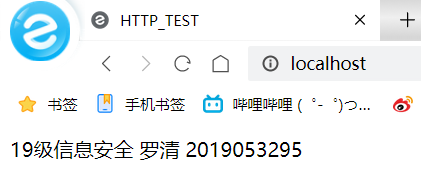
### 使用IIS默认站点

①将制作好的主页文件（html文件）复制到\inetpub\wwwroot目录下（即安装程序默认Web站点所在目录，可以通过默认站点右侧栏的“浏览”打开）。

②将主页文件名称改为Default.htm（IIS默认打开的主页文件是Default.htm或Default.asp，而不是一般常用的Index.htm）。

③打开浏览器，在地址栏中输入此计算机IP地址来浏览站点，测试Web服务器是否安装成功，WWW服务是否运行正常。







可见，输入localhost或本地IP地址都能够成功访问WWW站点。

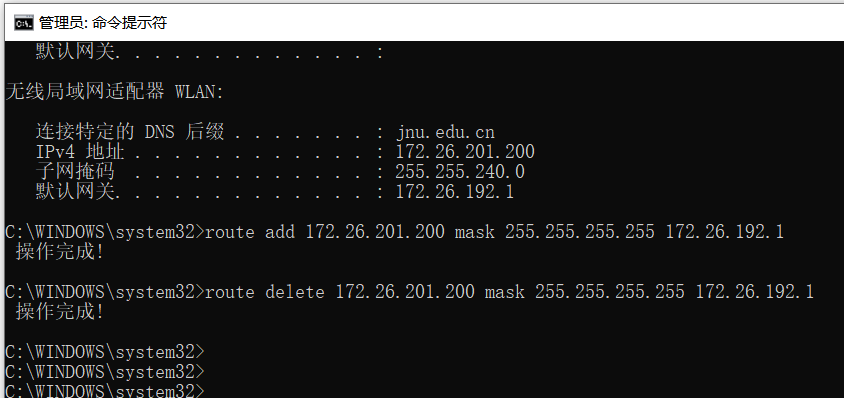
### 访问默认WWW站点，用WireShark分析网站的访问过程

打开WireShark开启混杂模式进行抓包，打开浏览器通过localhost访问默认WWW站点，结果发现抓不到对应源地址和目标地址都为本地IP地址的包。百度原因是WireShark只能抓取经过电脑网卡的包，由于访问默认WWW站点使用的是localhost或127.0.0.1，数据包不经过网卡，所以WireShark无法抓取相应的包，解决办法如下：

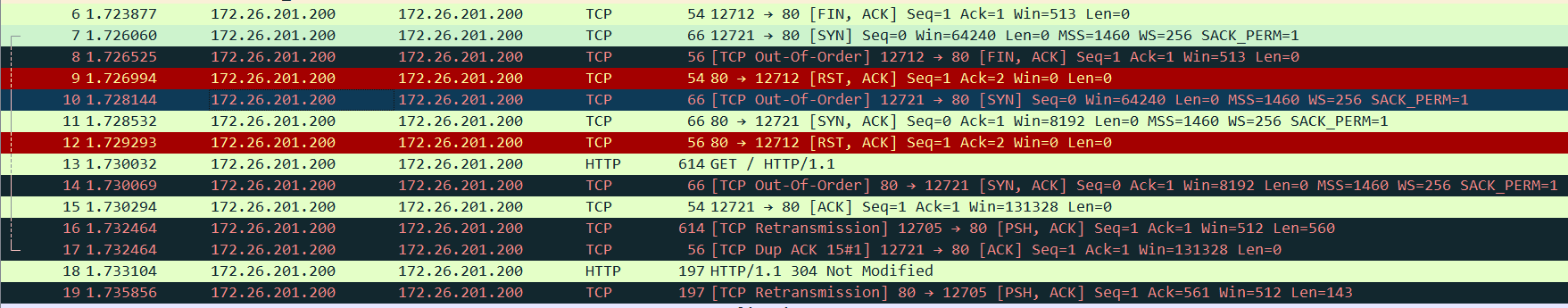
①以管理员身份打开命令提示符

②输入route add 本机IP mask 255.255.255.255 网关IP（在实验结束后使用route delete 本机IP mask 255.255.255.255 网关IP 来删除更改，否则本机的所有报文都会先经过电脑网卡再回到本机，会增加性能的消耗）

③使用WireShark即可抓到本地包。

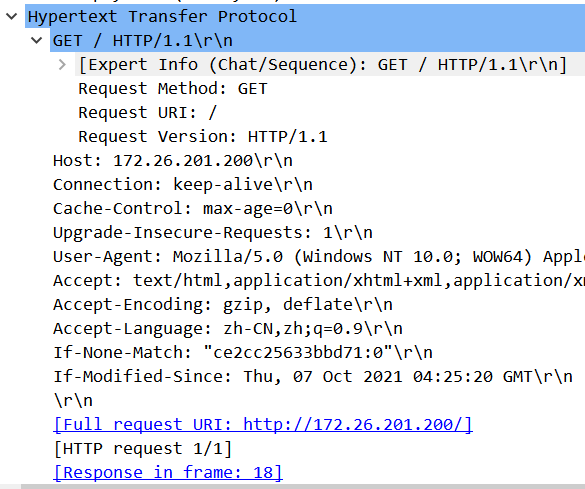


抓包结果如下



可以看到访问默认WWW站点获取HTTP服务需要首先进行三次握手建立连接，此处由客户端端口12721发送给HTTP默认端口80一个标志位为SYN的TCP连接请求，Seq=0，然后服务器通过端口80返回响应包Seq=0，ACK=1，由客户端再通过端口12721返回相应包Seq=1，ACK=1，建立TCP连接。然后发送HTTP的GET命令获取网页内容。

以GET命令为例的HTTP报文格式如下：



一个HTTP请求报文由请求行、请求头部、空行和请求数据4个部分组成。

**请求行：**如GET / HTTP/1.1\r\n打开后，有请求方法Request Method、HTTP协议版本Request Version和URL Request URI三个字段。

**请求头部：**由关键字/值对组成，每行一对，关键字和值用英文冒号“:”分隔。请求头部通知服务器有关客户端请求的信息，如User-Agent：产生请求的浏览器类型；Accept：客户端可识别的内容类型列表；Host：请求的主机名（允许多个域名同处一个IP地址，即虚拟主机）。

**空行：**最后一个请求头之后是一个空行，发送回车符和换行符，通知服务器以下不再有请求头。

**请求数据：**请求数据不在GET方法中使用，而是在POST方法中使用，POST适用于需要客户填写表单的场景。

## DNS协议分析

### 1、DNS报文格式分析

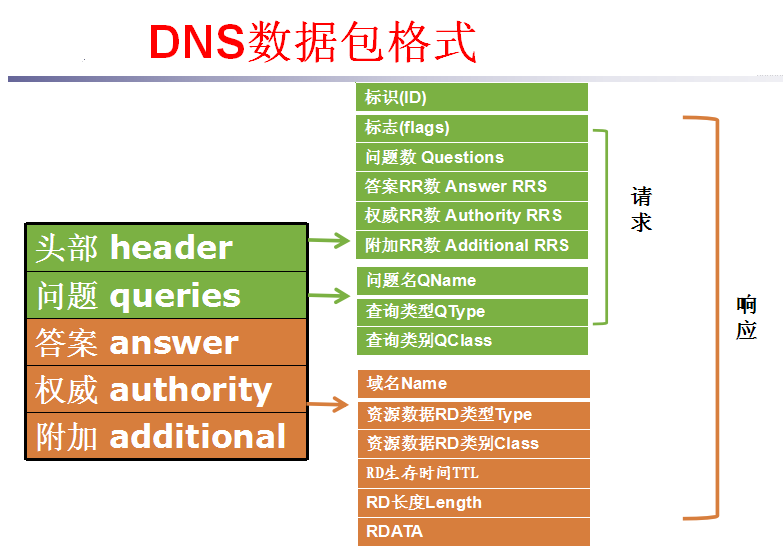
由于Win10系统的IIS无法使用DNS（无法自己搭建并配置），故本次实验直接使用正常网络中的DNS数据包进行DNS协议分析。

首先抛出DNS报文格式如下图所示：

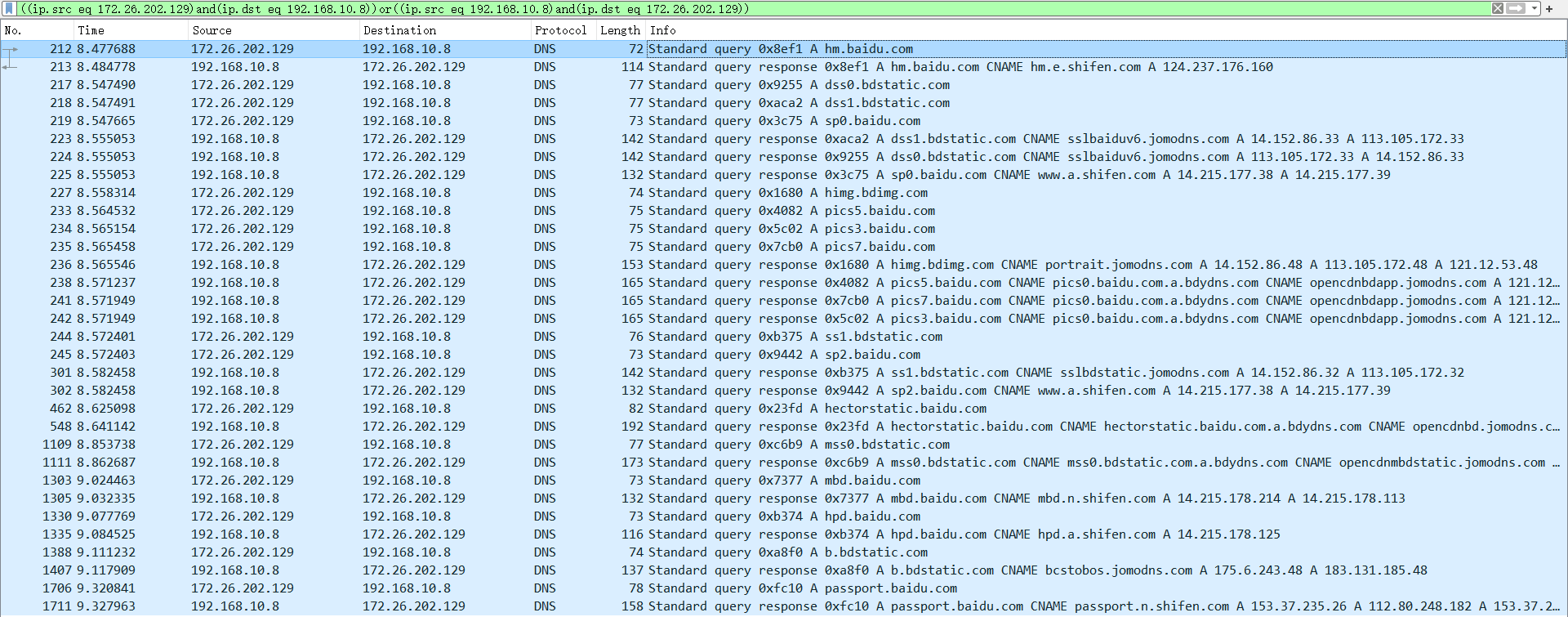
****

DNS报文格式分为5部分，分别是header、问题区段、回答区段、权威区段和额外信息区段，其中的header是必要的。

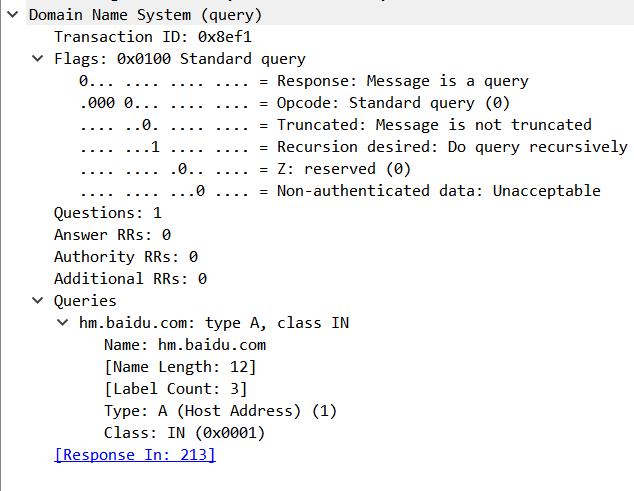
接下来给出DNS数据包格式各部分具体字段的总结，如下图所示：



打开浏览器，在网址栏输入www.baidu.com通过域名访问百度，同时利用WireShark对过程产生的数据包进行抓包，从而进行协议分析。设置显示过滤后，抓包的大致情况如下图所示：



打开任意一个DNS数据包



其中，Queries以上部分是DNS报文中的基础结构部分

①Transaction ID：是事务ID。

②Flags：是报文中的标志字段。

③Response：是QR字段，查询请求时值为0，响应时值为1。

④Opcode：是Opcode字段，操作码。0表示标准查询，1表示反向查询，2表示服务器状态请求。

⑤Truncated：是TC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，只返回前512个字节。

⑥Recursion desired：是RD字段，即期望递归。该字段能在一个查询中设置，并在响应中返回。该标志告诉名称服务器必须处理这个查询，这种方式被称为一个递归查询。如果该位为0，且被请求的名称服务器没有一个授权回答，它将返回一个能解答该查询的其他名称服务器列表。这种方式被称为迭代查询。

⑦Questions：是问题计数。

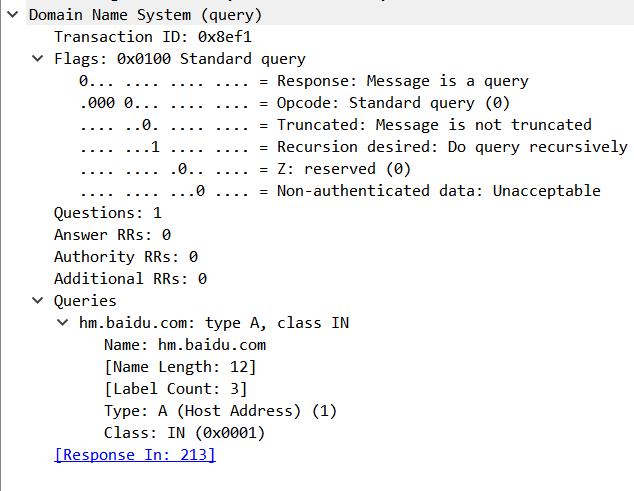
⑧Answer RRs：是回答资源记录数。

⑨Authority RRs：是权威名称服务器计数。

⑩Additional RRs：是附加资源记录数。

（需要注意！！在请求中Questions的值不可能为0；Answer RRs，Authority RRs，Additional RRs的值都为0，因为在请求中还没有响应的查询结果信息）

Queries即报文中的问题部分，是用来显示DNS查询请求的问题，通常只有一个问题。该部分包含正在进行的查询信息，包含查询名（被查询主机的名字）、查询类型和查询类。此处再此用上图作说明。

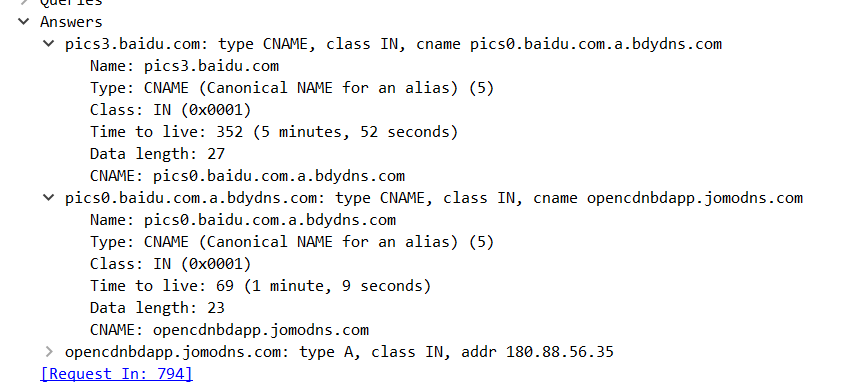


①Name：查询名字段，此处请求域名hm.baidu.com。

②Type：查询类型字段，这里为A类型。

③Class：查询类字段，这里为IN，即互联网地址。

由于资源记录部分只在DNS响应包中出现，故下面通过DNS响应包来进一步了解资源记录部分的字段信息。



其中各字段说明如下：

①pisc3.baidu.com：为资源记录部分。

②Name：为域名字段，这里请求的域名为pisc3.baidu.com。

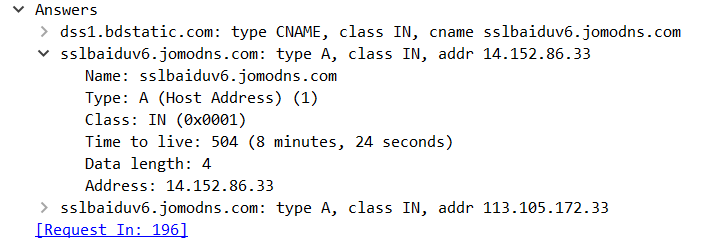
③Type：类型字段，这里为CNAME类型。

④Class：类字段。

⑤Time to live：生存时间。

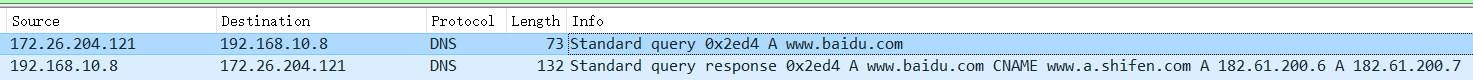
⑥Data length：数据长度

⑦CNAME：资源数据，这里为CNAME即规范域名。当为Type为A时此处返回IP地址，表示获取域名对应的IP地址。如下图所示：

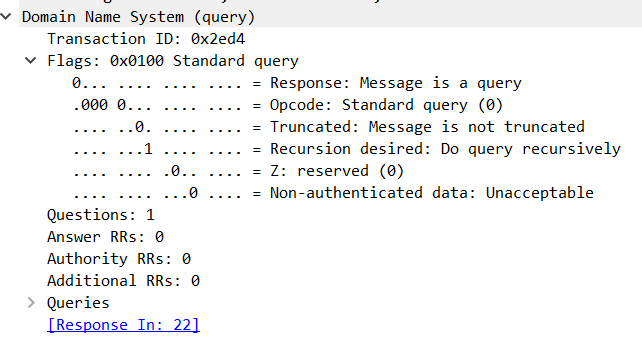


### DNS工作过程分析

接下来对www.baidu.com的域名访问的DNS工作过程做分析。首先列出最基本的相应数据包如下：



展开请求包

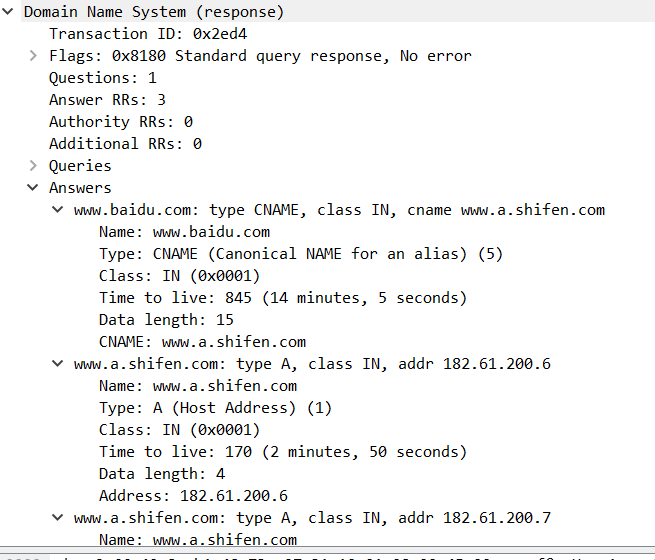


可以看到DNS请求报文的RD字段为1，说明要求采用递归查询，即要求直接得到域名解析的最终结果，解析过程由DNS服务器完成。为了验证192.168.10.8是本地DNS服务器，打开命令控制符输入ipconfig -all得到结果如下：



符合预期。

展开对应的DNS响应包如下：



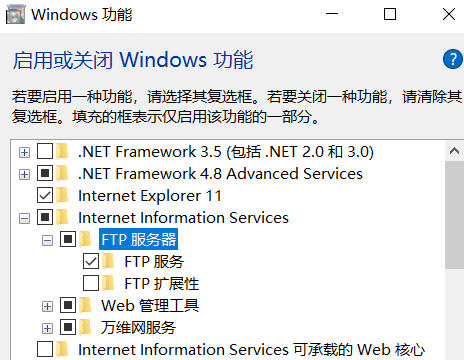
可以看到DNS为输入的域名作了规范化，并返回了最终的IP地址（有2个结果，一个是182.61.200.6，另一个是182.61.200.7）。

## FTP协议分析

本次实验采用自己安装配置FTP服务器，并对其进行访问，其中利用WireShark抓包来对FTP协议进行分析，分析FTP访问过程。

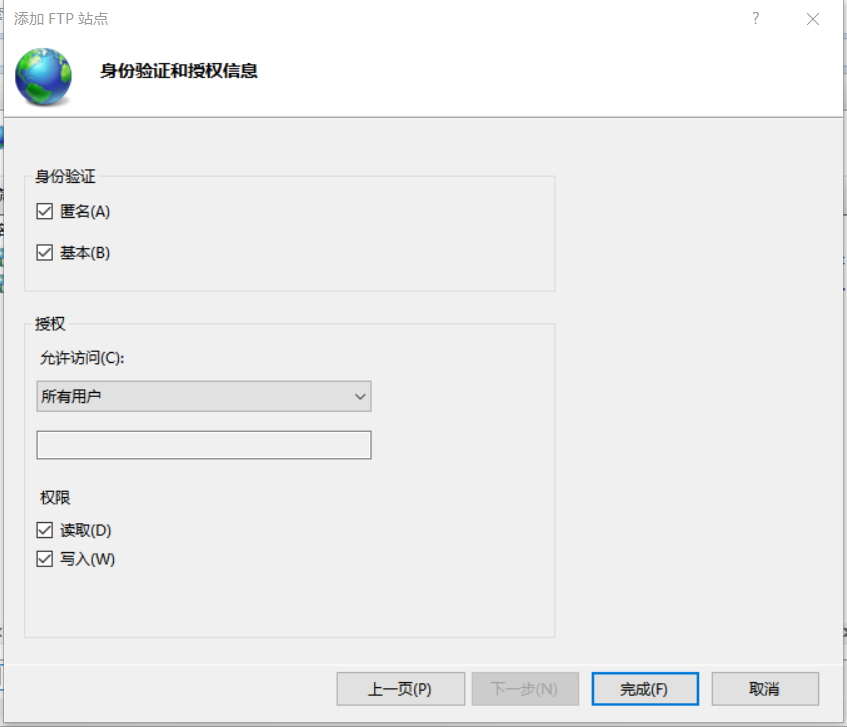
### 安装FTP服务器

打开控制面板，将查看方式设置为大图标，点击“程序和功能”，点击左侧“启动或关闭Windows功能”，展开Internet Infomation Services，选中开启FTP服务器，确认更新即可。



### 配置

安装更新完成后，FTP服务器就开始自动运行了，但是还需要进行一些配置工作。打开控制面板，将查看方式设置为大图标，点击“管理工具”，点击“Internet Infomation Services管理器”，在网站的操作界面点击“添加FTP站点...”，在站点信息界面填写FTP站点名称和物理路径（FTP服务器在本机上的内容目录）；在绑定和SSL界面绑定IP地址（由于我使用校园网，故绑定WLAN的IPv4地址），为了便于实现对FTP服务器的登录访问，此处选择不设置SSL证书；在身份验证和授权信息界面选择匿名或基本，赋予所有用户访问权限和读写权限，详细界面如下：



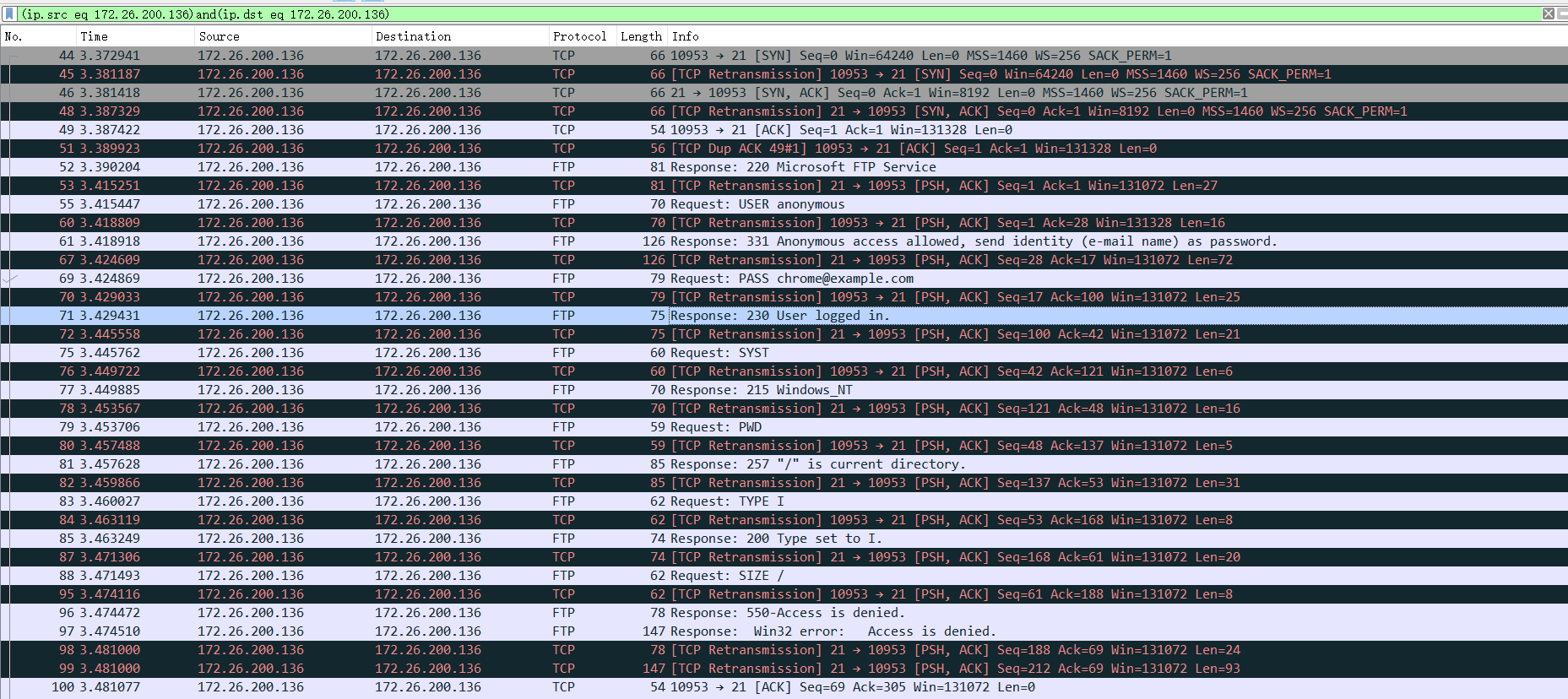
创建完毕后，FTP服务器站点随之生效，可以通过浏览器网址输入行或文件资源管理器目录行输入ftp://+绑定的IP地址来对FTP服务器进行访问，因为赋予了匿名用户最大权限，故可不登录（即匿名登录）对FTP内容文件进行访问。

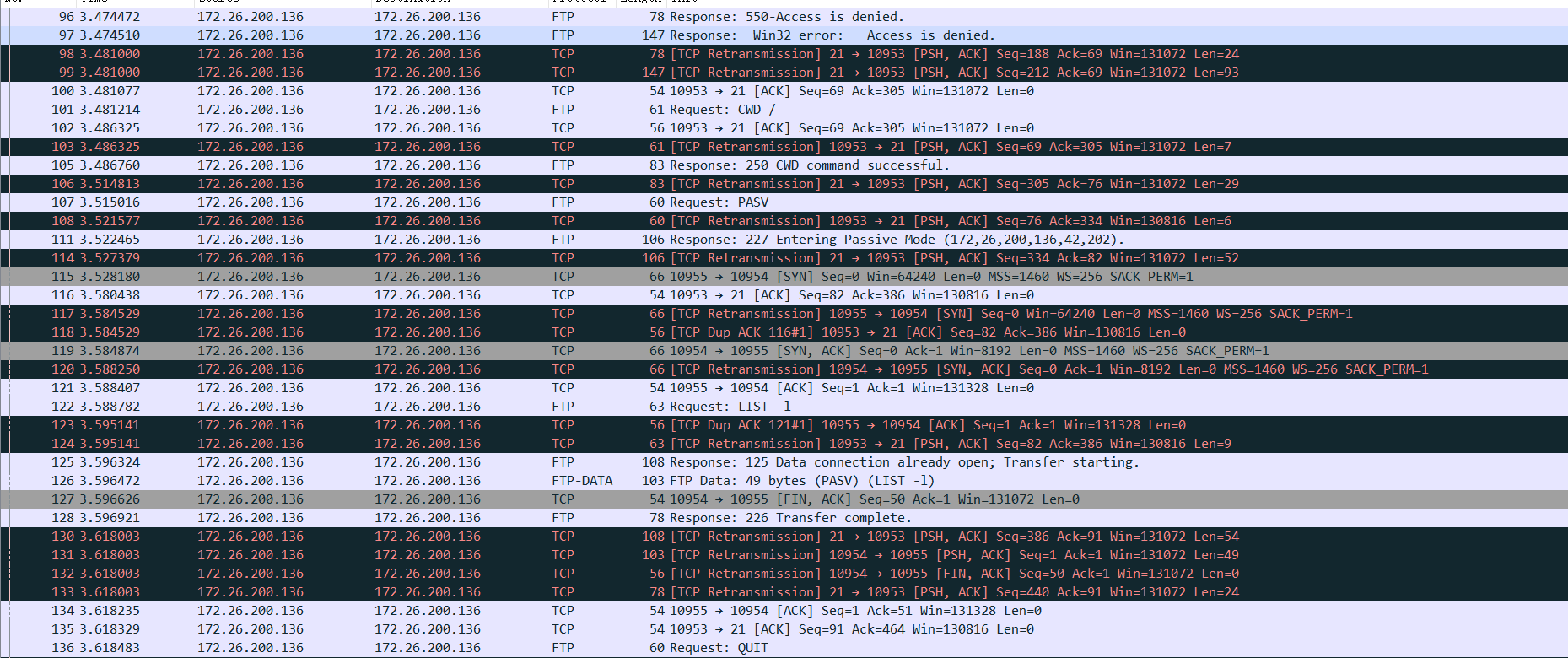
### 访问FTP服务器，用WireShark抓包分析

在创建的FTP站点绑定的文件夹下新建一个test.txt用于更直观的判断是否访问成功。打开WireShark开始抓包，打开浏览器，在网址栏输入ftp://172.26.200.136（我做本次实验时的IP地址），回车访问，此时遇到2个问题，下面逐一作介绍。

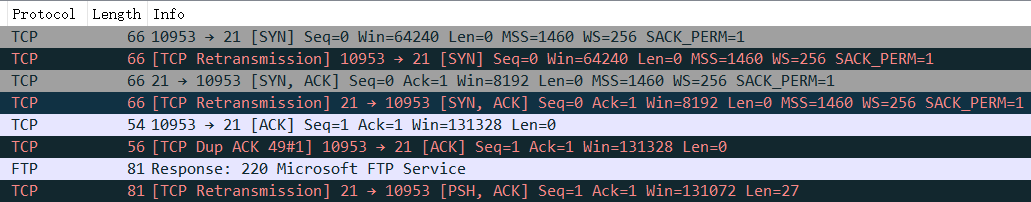
第一个问题是，对FTP站点的访问成功了，但是没有抓到相关的TCP和FTP数据包，分析过后得出原因是：与HTTP协议分析时相同，由于要访问的目标IP地址是本机IP地址，故数据包走本地回环，根本没有发送到真实网络上（即没有经过电脑网卡），故WireShark无法抓到相应的包。解决办法同HTTP协议分析：①以管理员身份打开命令控制符；②输入route add 本机IP地址 mask 255.255.255.255 网关IP地址；③再进行抓包即可；④抓包完成后删除添加的路由。

此后遇到了第二个问题，添加路由后连接FTP服务器失败，分析过后得出原因是：防火墙设置不当，阻碍了TCP的连接。解决办法如下：打开控制面板，打开Windows Defender防火墙，点击左侧高级设置，新建入站规则，设置规则类型为端口-适用于TCP-所有本地端口，理论上就可以使得连接FTP服务器成功。结果也的确如此。设置显示过滤后（源地址和目的地址都是本地IP地址），浏览抓到的包的大致情况如下：

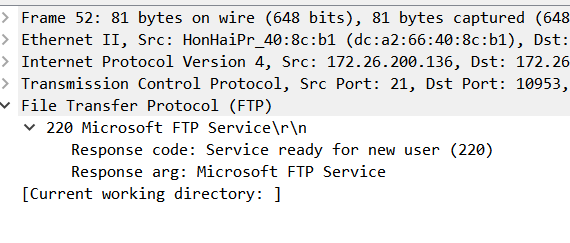




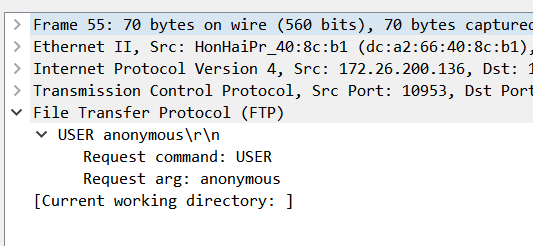
接下来进行访问FTP站点的过程分析及FTP协议分析。



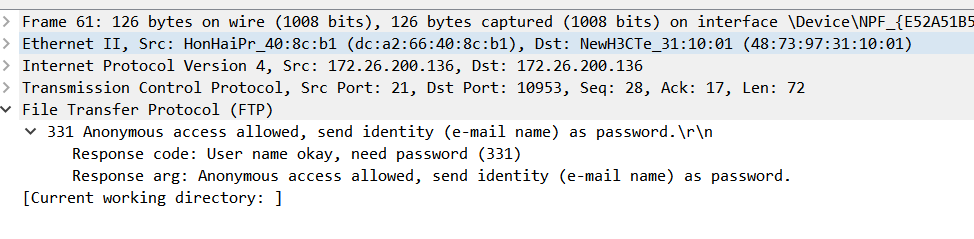
可以看到，FTP客户端本次利用10953号端口，首先与FTP默认21号端口进行三次握手建立控制连接，连接成功后FTP默认站点从21号端口返回一个FTP数据包，响应码为220，包内含有服务器的信息，客户端接收到该FTP包后返回一个ACK确认。FTP数据包如下：



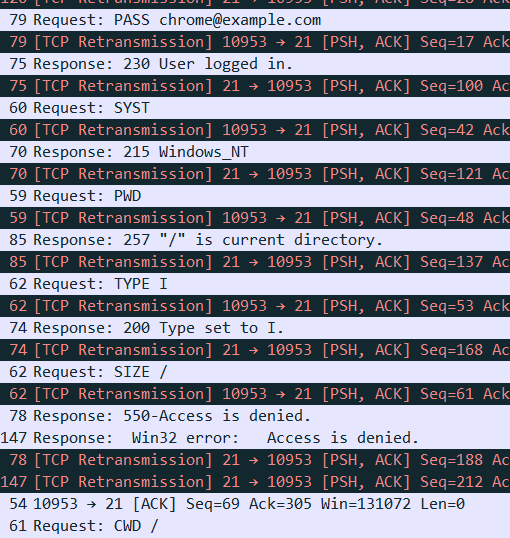
接下来进行登陆操作。



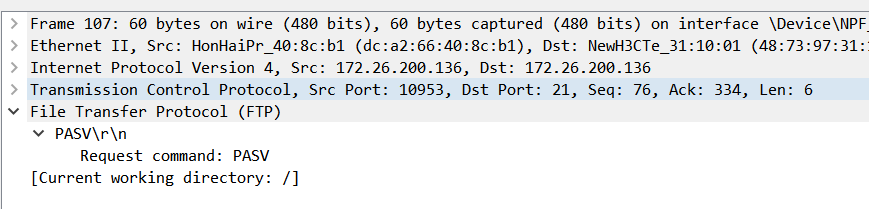
客户端发送USER请求登录，匿名用户登录。服务器返回FTP应答用户名正确，状态码331，然后客户端发送ACK确认包。



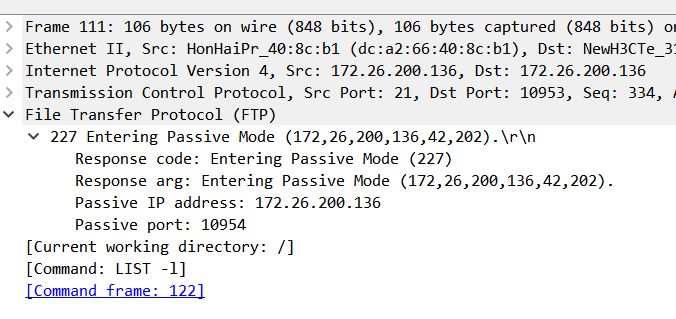
接下来是客户端请求一系列参数，如PASS、SYST、PWD等等，FTP服务器对每个参数请求做回应，客户端接收到回应后返回ACK确认包。



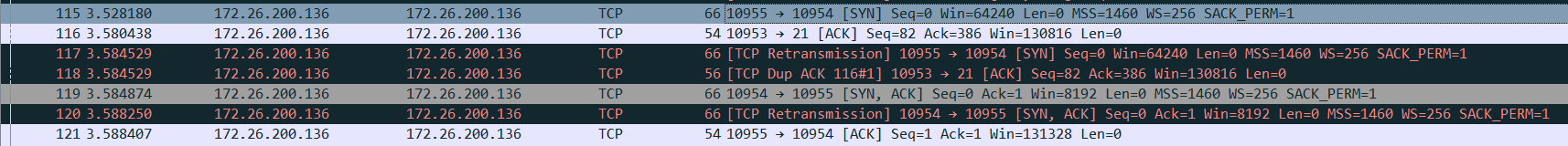
接下来可以看到客户端发送FTP请求，命令是PASV，为请求被动模式，然后服务器就会在本地随机开放一个端口（1024以上），把开放的端口告诉客户端，客户端再连接到服务器开放的端口进行数据传输。



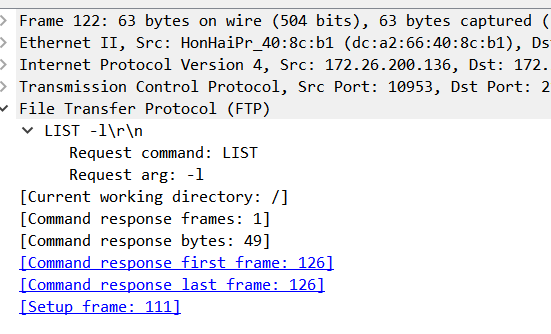
查看随后21端口返回的FTP数据包，很容易看到FTP服务器返回的被动模式连接用的IP地址和端口号，开放的端口号为10954，响应码为227。



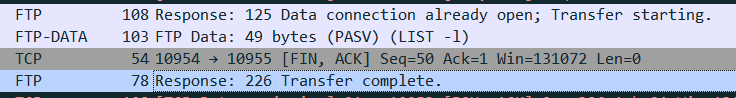
随后客户端采用10955号端口与10954端口三次握手建立TCP连接用于数据传输。



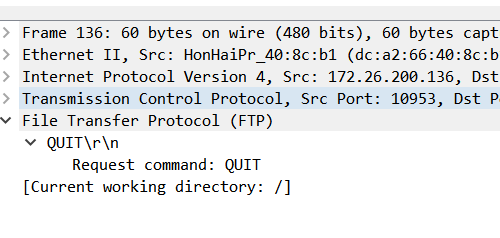
这条TCP连接建立成功后，客户端发送FTP请求命令为LIST到21端口，列目录。



随后开始传输数据：



传输完毕后断开连接到FTP服务器10954号端口的TCP连接。



至此结束。

总结：连接FTP时，首先会建立一个控制连接（连接到服务器的21号端口），然后客户端发送FTP请求设置各种参数和执行一些命令，服务器相应的给予响应（响应完毕后客户端发送ACK确认包）。当客户端请求PASV被动模式后，FTP服务器声明一个新的端口，客户端和服务器用不同于控制连接的端口建立TCP连接，然后就可以传输数据。数据传输完毕后，仍需发送ACK确认包。直接退出，控制连接和数据连接都会断开。

## SMTP和POP协议分析

本实验采用自己搭建SMTP服务器、配置邮件服务器，并在测试SMTP服务器功能的过程中用WireShark对相关协议包进行抓取分析的方法对SMTP和POP协议进行分析。

### 安装SMTP服务器

打开“控制面板”的“添加/删除程序”-“打开或关闭Windows服务”，打开“Internet

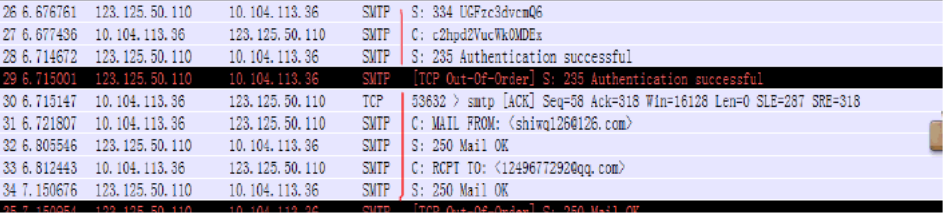
Infomation Services（IIS）”的“SMTP Service”，根据提示安装邮件服务器，默认会在systemroot://Inetpub//mailroot目录下生成7个子文件夹：①Badmail：存放错误的信件。②Drop：是本地邮件（Local Mail）的存放处，每一封信由一个文件表示，扩展名为elm。③Pickup：当SMTP服务器收到信件时会先存放在Pickup文件夹中，然后由系统检查该文件夹，当发现Pickup文件夹中存在文件时就立即处理。④Queue：邮件处理中的临时文件夹。⑤Mailbox⑥Route⑦SortTemp：上述三个文件夹都是邮件服务器在整理、分类邮件时使用的文件夹。

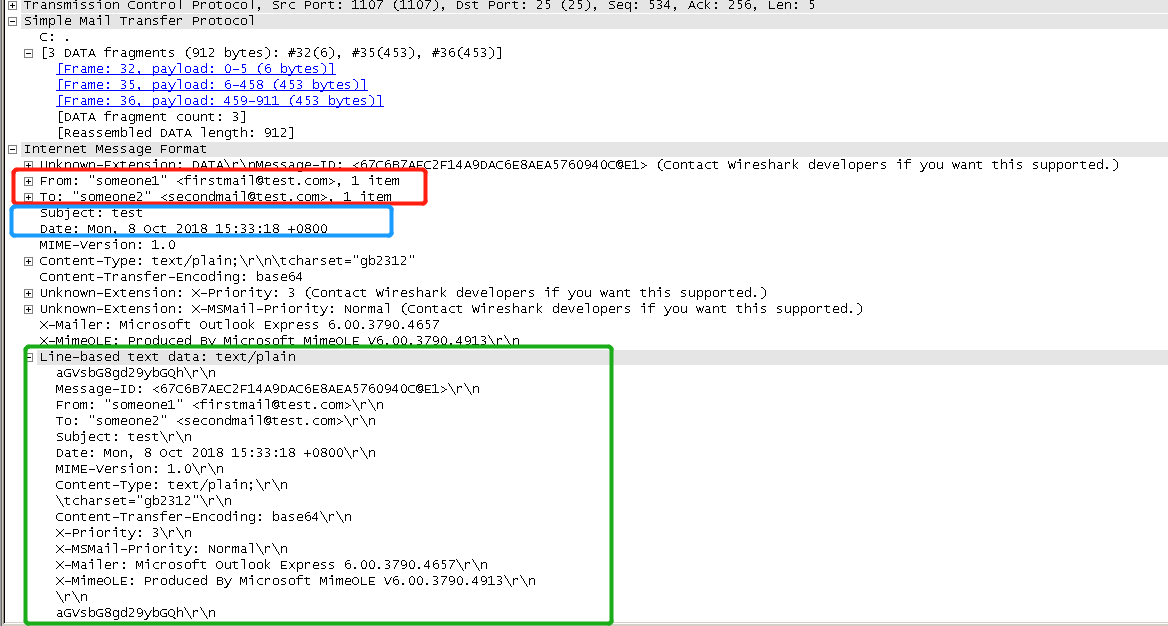
### 配置邮件服务器

IIS在安装时已自动创建默认的SMTP站点。此处我新建一个SMTP站点。

1. 选择新建站点的“属性”，在打开的对话框中修改IP地址。在“高级”中还可以设置多个IP和修改默认端口。
2. 在访问页面中，可以设置身份验证方法、连接控制以及中继控制。若要让SMTP服务器拥有中继邮件的功能则可以选择“中继”中的“选择可以通过此虚拟服务器进行中继的计算机”单选框中选择“仅以下列表除外”。则SMTP服务器可以中继除了列表之外的计算机的邮件。
3. 在邮件的属性页，可以限制邮件的大小，进而提高整体的效率。
4. 在Outlook等软件下发送本地邮件或远程邮件进行SMTP服务的测试，如果服务正常，则本地邮件会保存在“Drop”文件夹下，远程邮件会得以正常的转发。

### 邮件收发过程与相关协议分析





在邮件数据发送前，SMTP客户端需要先与SMTP服务器通过三次握手建立TCP连接。上图所示的包序号为39，是邮件所在的SMTP包。红色框内是收件人和发送人的域名信息，蓝色框是所发送邮件的邮件主题和发送时间，而绿色框则是邮件内容，其中text/plain代表文件设置为纯文本的形式，是一种内容类型。

在得出此实验结果前，我曾尝试直接用web的qq邮箱发送邮件，并试图抓包，但是失败了。通过百度，得出原因可能是这类邮件软件将邮件内容及其报文封装在其他应用层数据包中进行保护，故无法看到SMTP数据包。

# 实验总结

本次实验对WWW、DNS、FTP、SMTP等应用层服务协议的工作过程和协议格式作了分析，内容较多。个人认为难点在于相关服务器的搭建和环境的配置（如防火墙的设置等），且Win10的IIS服务不提供某些搭建服务（如DNS），耗费了一定的时间。但是实验的重点我认为无疑在于HTTP、DNS等应用层协议的分析，通过WWW服务器搭建、FTP服务器搭建和SMTP服务器搭建，为WireShark抓包进行协议分析、加深理解提供了加成和帮助。

通过本次实验，我解决配置问题的能力得到了提升，并且对应用层协议的工作过程有了较深刻的理解，在计算机网络学习的道路上又迈进了一步。