**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 实验地点 计算机网络实验室

学生姓名 贺萱 学号 2019054616

学院 智能科学与工程学院 系 专业 信息安全

实验时间2021年 9月28日上午～10月18日下午温度 ℃湿度

1. **实验目的**
2. 理解WWW、DNS服务、FTP服务、SMTP的作用和原理；
3. 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。
4. **实验内容**
5. 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；
6. 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）
7. **主要仪器设备**

**仪器：**一台具有网络功能的PC 机

**实验环境：**局部网环境

1. **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）

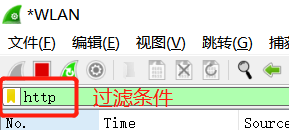
**注意：**

如果访问的网站信息量太大，可以利用windows自带组件（如IIS）或自行下载WWW服务器软件，建立并配置WWW站点，主页内容需要包含姓名、学号等个人信息，然后访问自己建立的网站。

**实验步骤：**

1. **适的过滤条件，开始抓包，使用的网站为**

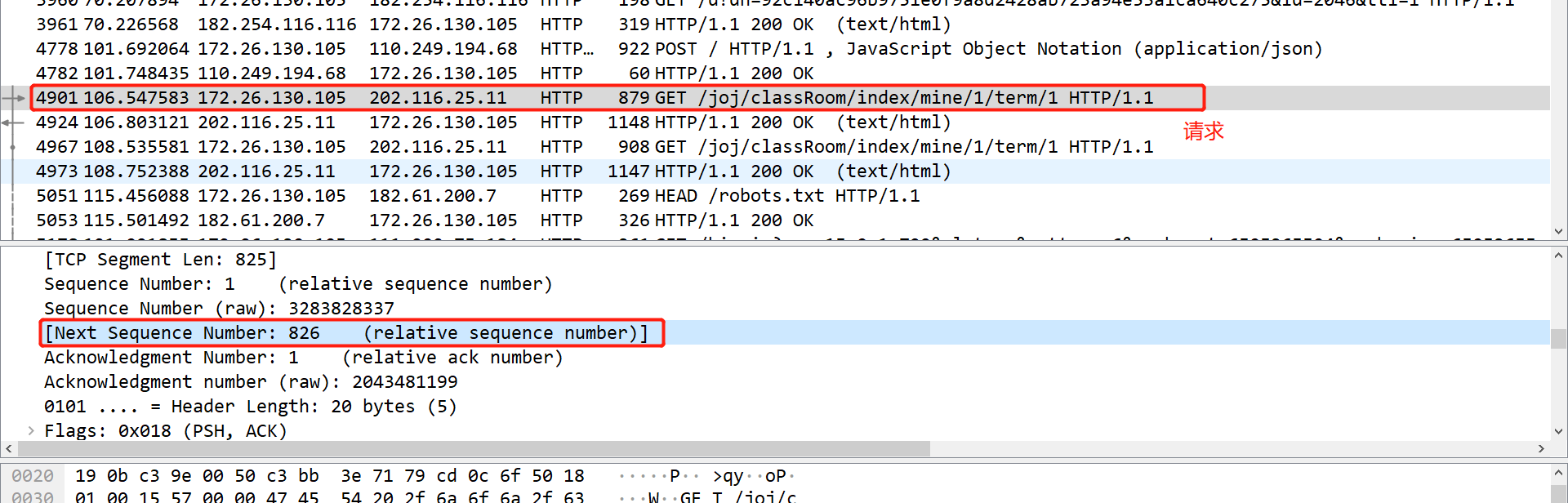
<http://www.jiaozuoye.com/joj/classRoom/index/mine/1/term/1>



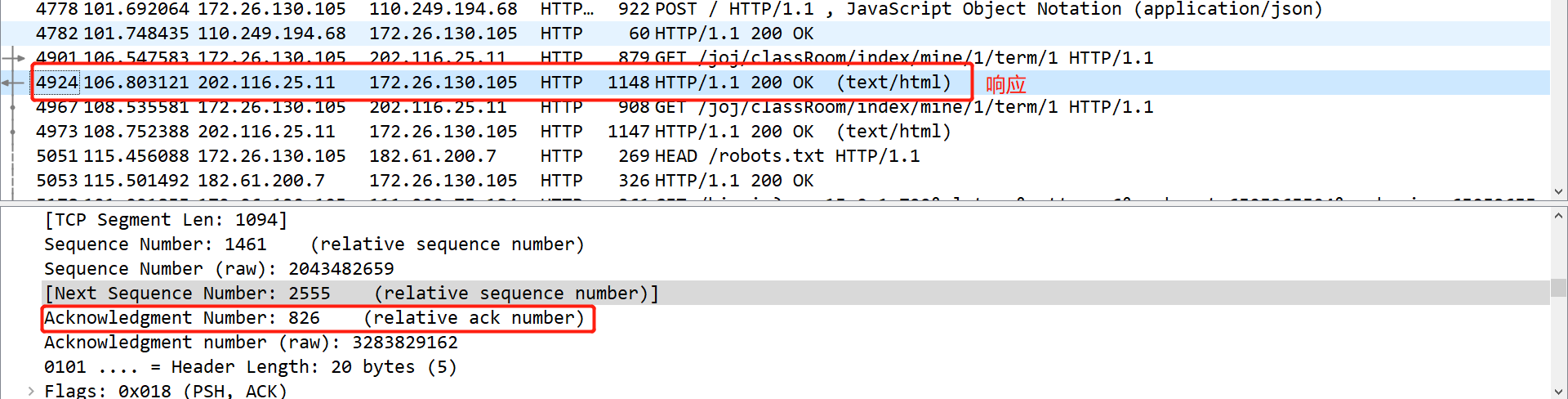


1. **辨别请求和响应包**

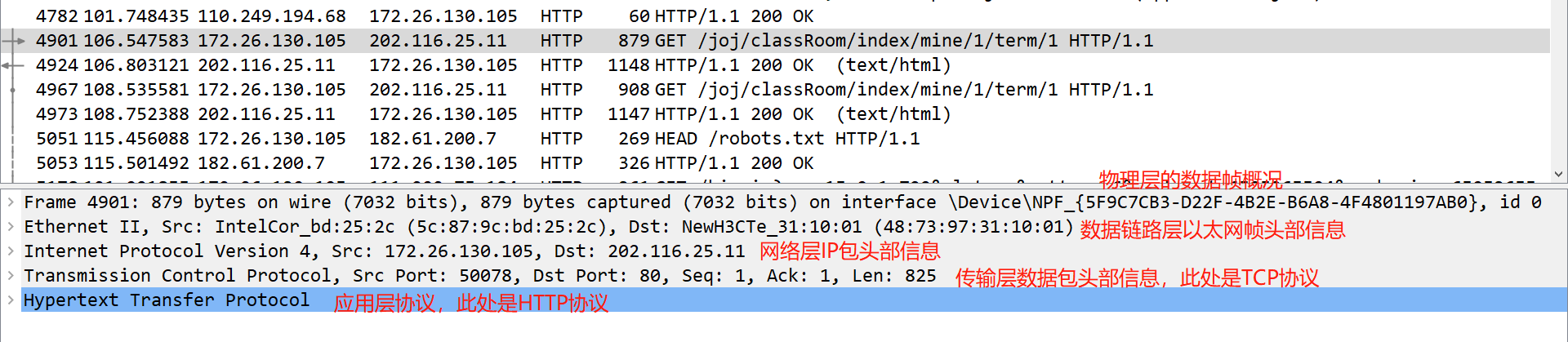
请求：



响应：



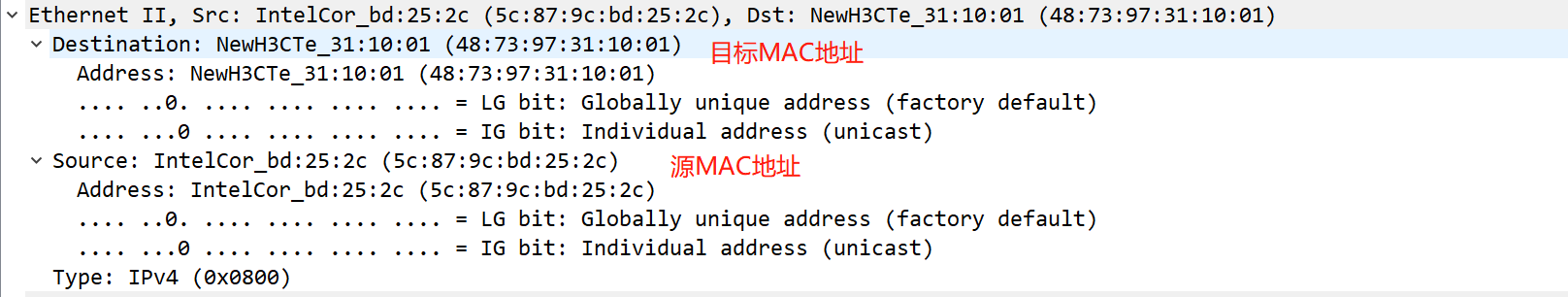
1. **对抓取的http进行分析**



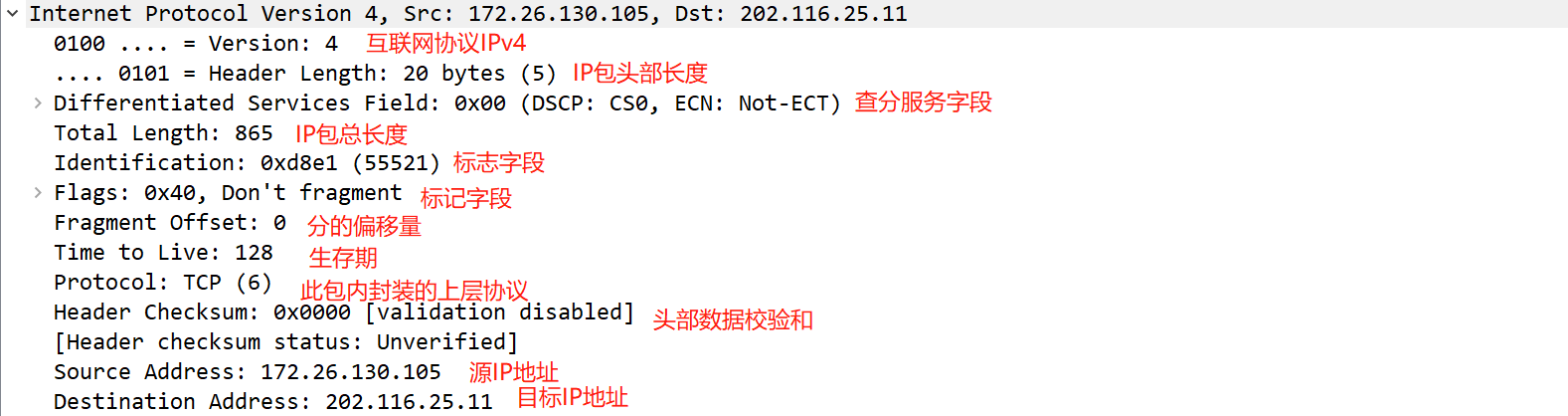
1. 物理层数据帧概要



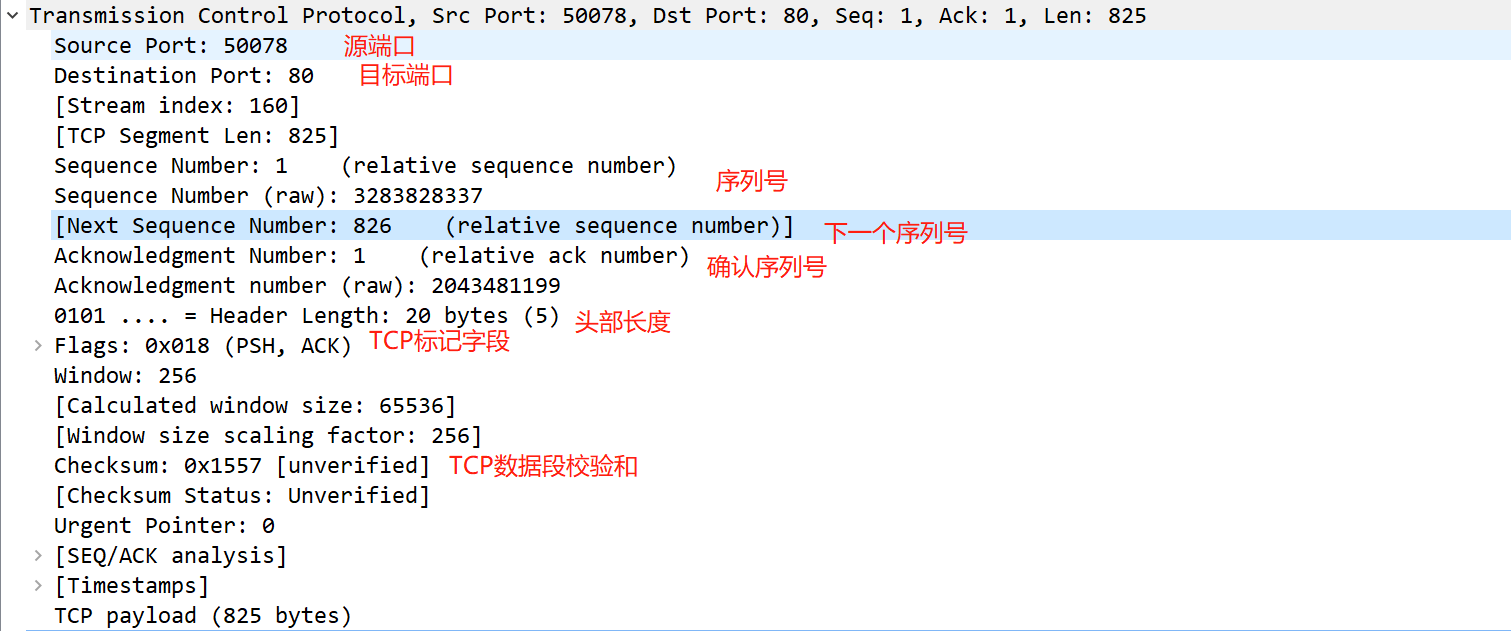
1. 数据链路曾以太网帧的头部信息



1. 网络层IP头部包信息



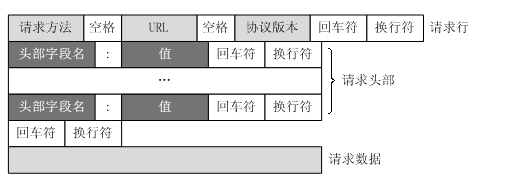
1. 传输层数据包头部信息



1. 应用层分析（HTTP协议分析）

①请求报头：

请求报文的结构：



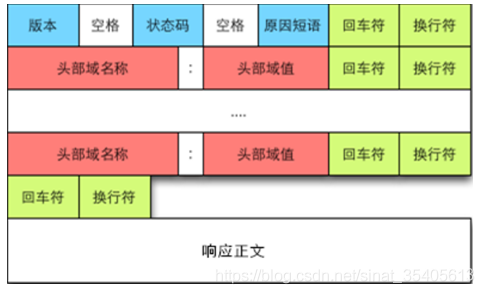
报文分析：



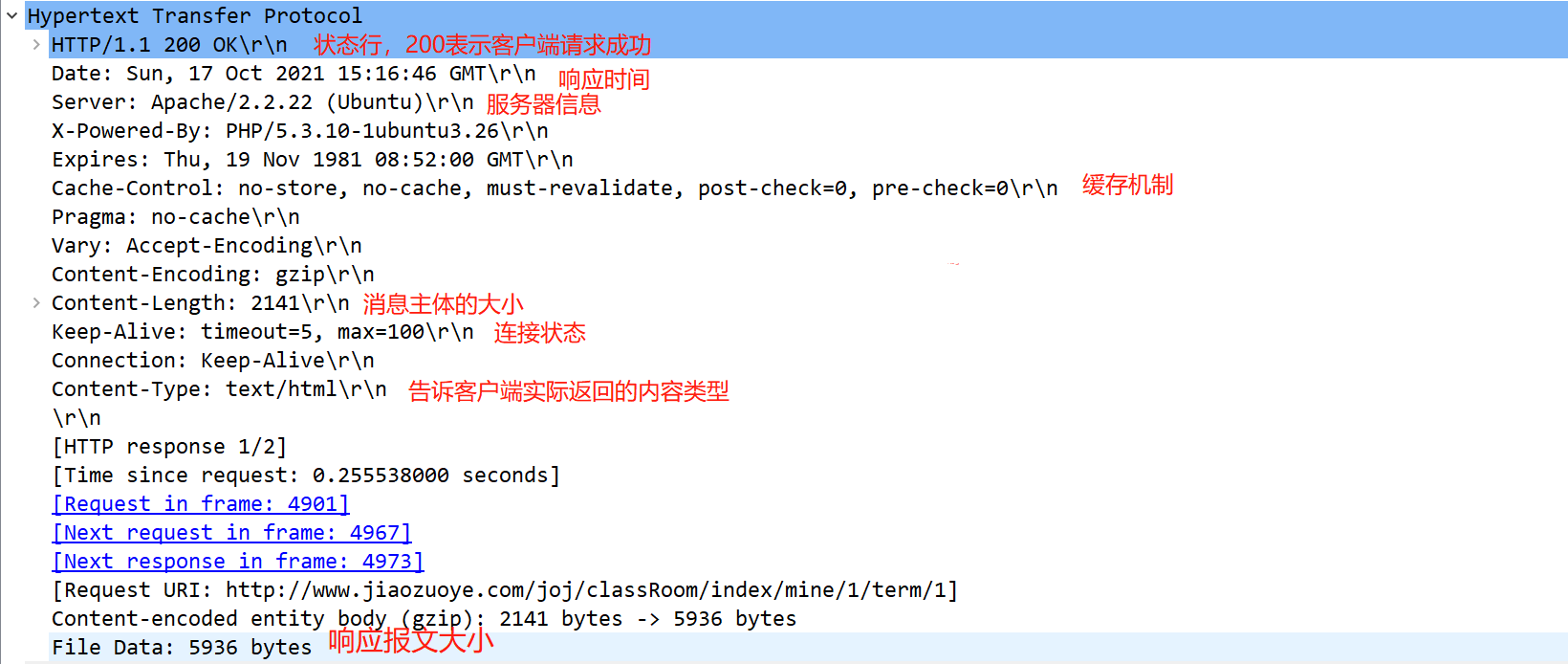
请求头请求方式不同，数据传输不一样，如，Get/Post

②响应报文

响应报文的结构：



报文分析：



1. **http协议首部含义**

（1）首部字段的作用

首部字段是构成HTTP报文的要素之一，在服务器与客户端之间的HTTP通信过程中都会使用首部字段，他能起到传递额外重要信息的作用。

首部字段提供了报文主体大小，所使用的语言，认证信息等内容。

（2）首部字段的结构

格式为： 首部字段名：字段值。例如：Content-Type:text/html。并且，一个首部字段名可以对应多个字段值。

（3）四种首部字段的类型

①通用首部字段：请求报文和响应报文都会是使用的首部。

②请求首部字段：从客户端向服务器发送请求报文时使用的首部。补充了请求的附加内容，客户端信息，响应内容相关优先级等信息。

③响应首部字段：从服务器端向客户端返回响应报文时使用的首部。补充了响应的附加内容，也会要求客户端添加额外的内容信息。

④实体首部字段：针对请求报文和响应报文的实体部分使用的首部。补充了资源内容的更新时间等于实体有关的信息。

（4）HTTP通用首部字段



（5）请求首部字段





1. 响应首部字段



1. 实体首部字段



1. **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。

**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。
2. 可以自己建立DNS服务器并使用它进行域名解析。

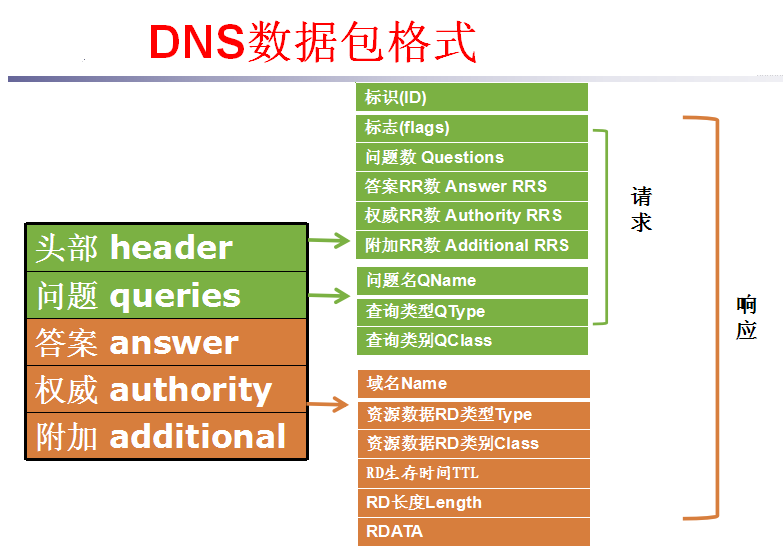
1）建立DNS服务器。

利用windows自带组件或下载DNS软件（如ntbind），建立DNS服务器，并对DNS服务器的配置（建立域名-IP地址的解析关系）。

2）使用DNS

在任意一台计算机上配置TCP/IP协议，将DNS服务器配置成上述DNS服务器（注意该DNS服务器的IP地址是静态的），用该DNS服务器中设置的器域名访问该WWW服务，并与用IP地址访问的结果进行比较。（注意该客户机的IP地址最好与DNS服务器地址同一个网段，即网络号相同）

3、附DNS数据包格式（细节见课件）

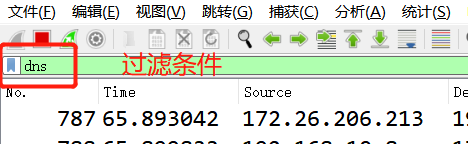


**实验步骤：**

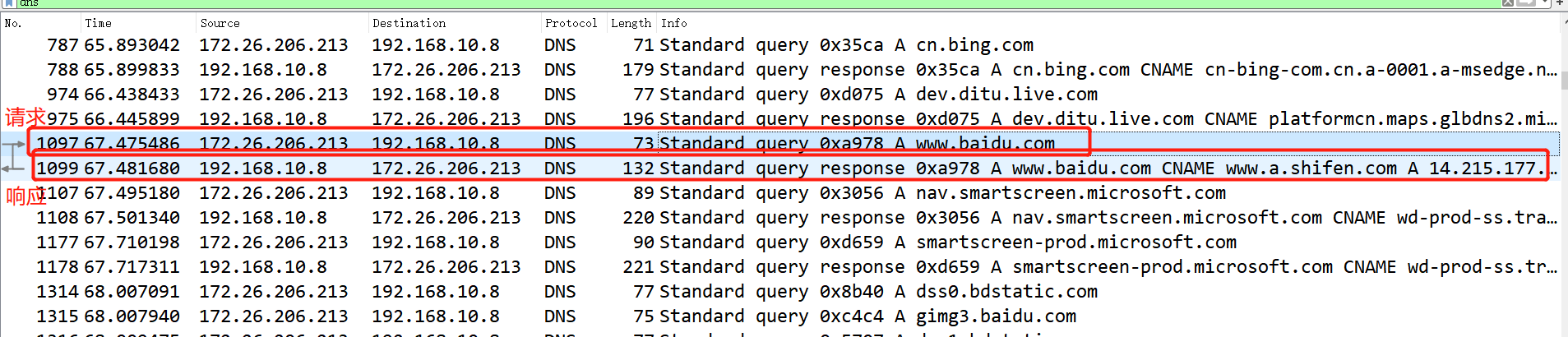
1. **适的过滤条件，开始抓包，使用的网站为**

<https://www.baidu.com/>



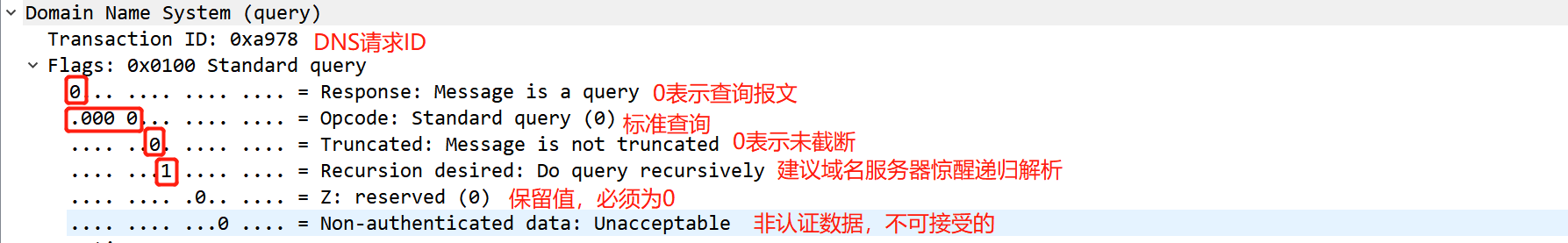


1. **辨别请求和响应包**



1. **对抓取的dns进行分析**
2. 请求包





1. 响应包



DNS利用递归查询的方式解析域名，向主机发送请求报文，解析地址14.215.177.39和14.215.177.38

DNS工作过程分为递归查询和迭代查询，主机向本地域名服务器查询采用递归查询，本地服务器向根服务器查询采用迭代查询，本实验解析www.baidu.com是主机向本地域名服务器查询所以问递归查询



由两个域名指向同一个IP地址和类型名CNAME可知，二者是同一个域名，一个是别名

1. **有时候可能捕获不到DNS解析过程，为什么？**

初次访问www.baidu.com时，Wireshark能捕获到DNS解析过程；但随后再次访问相同网站时，Wireshark捕获不到。是因为在第一次访问之后，本机（浏览器或系统）进行了DNS缓存，第二次访问时直接从本机缓存中得到IP，不需要再与本地DNS服务器进行通信，因此Wireshark捕获不到解析过程。若在第一次访问之后清除本机缓存，再进行第二次访问，那么两次都应该可以捕获到DNS解析过程。通过重启浏览器的方式清除浏览器的DNS缓存，通过ipconfig/flushdns命令清除系统的DNS缓存。DNS缓存既存在于浏览器中，也存在于系统中，域名解析将优先查找这两处的缓存；只有当需要解析的域名在这两处地方都没有缓存记录时，才会向本地DNS服务器通信请求解析。此外，浏览器和系统的DNS缓存都不是一直存在的，有设定的TTL，只有在TTL内发起第二次访问，才会无法捕获；若间隔一段时间再访问，不需要清除本机DNS缓存也能捕获解析过程。

**三、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。

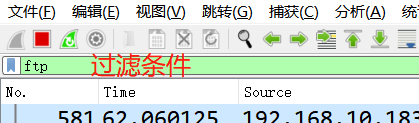
**注意：**

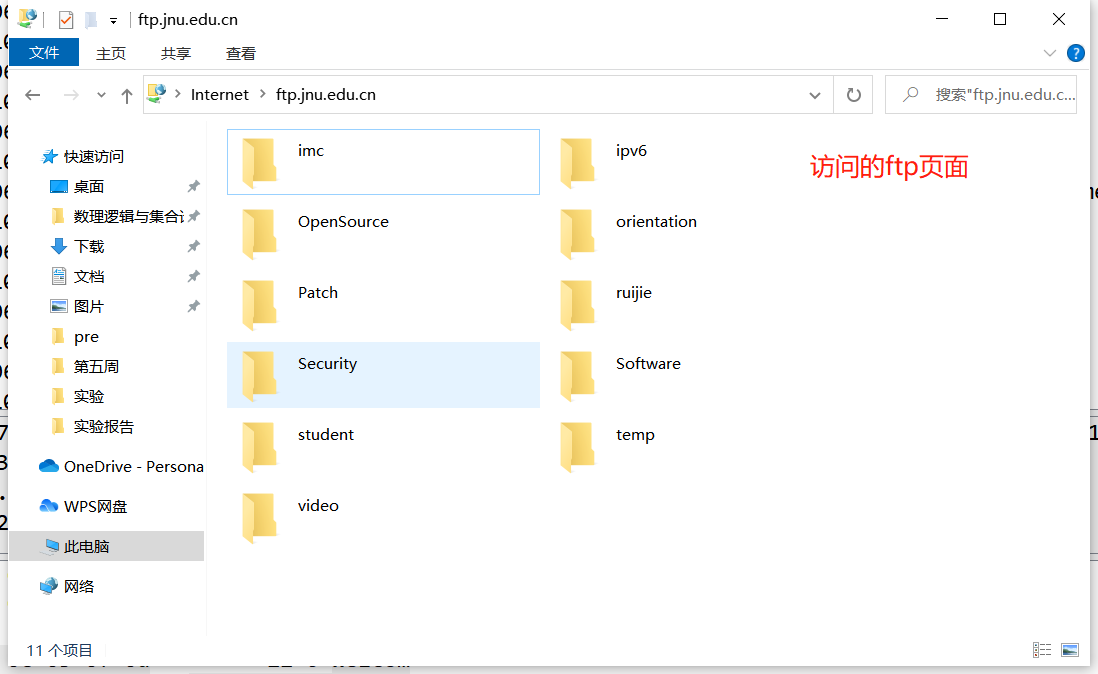
可以利用Windows自带的FTP组件或下载FTP软件，建立FTP服务器，并进行配置，并访问分析FTP协议

**实验步骤：**

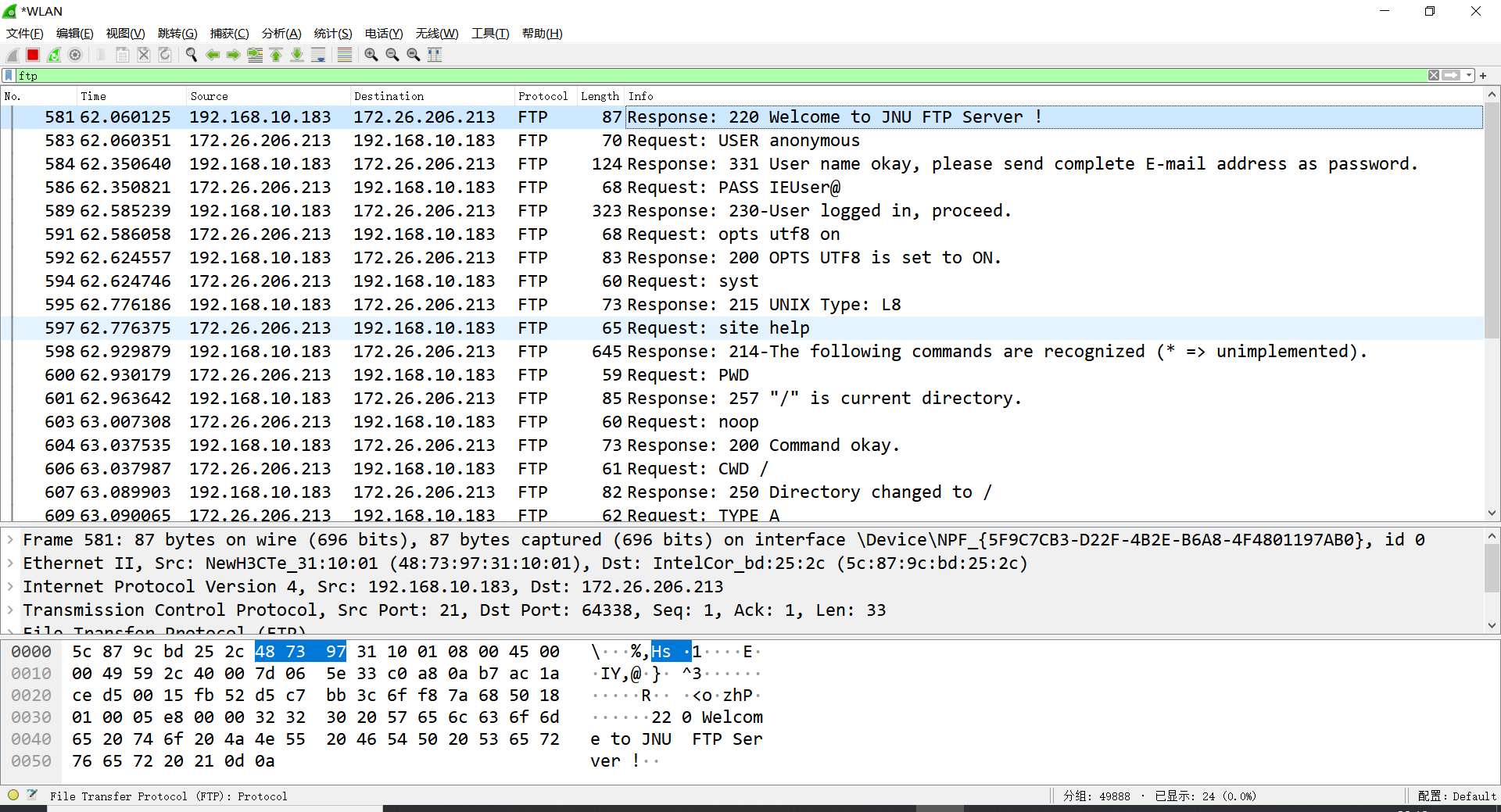
1. **访问FTP服务器。如ftp://ftp.jnu.edu.cn**

**适的过滤条件，开始抓包**





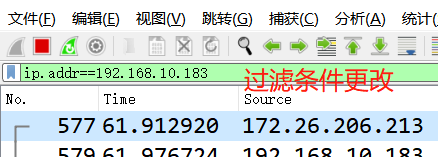
1. **捕获内容**



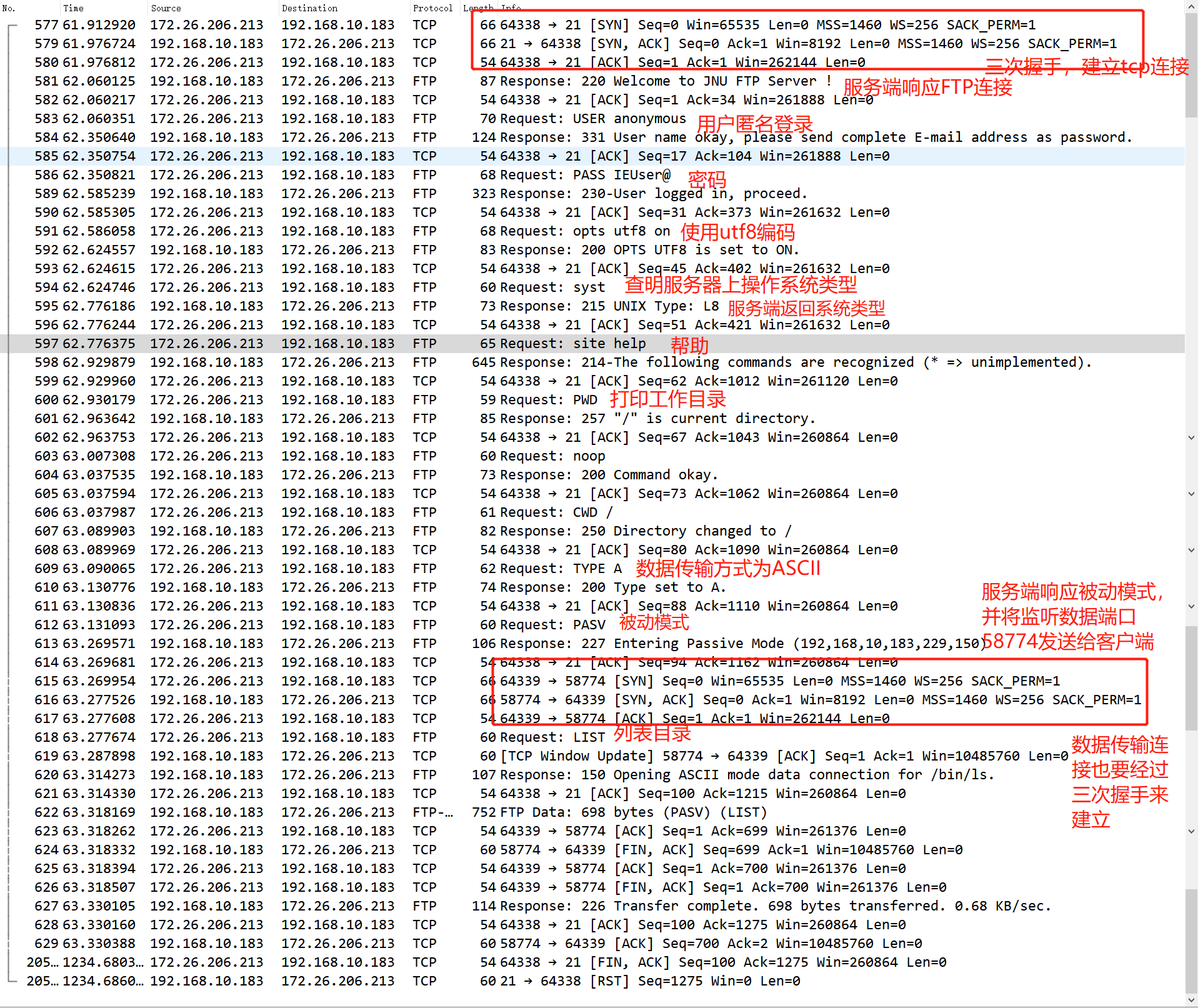
发现数据中并没有3次握手，经过查询后发现FTP的客户和服务器之间需要建立TCP连接，所以重新设置过滤条件，[ftp.jnu.edu.cn](ftp://ftp.jnu.edu.cn)的IP地址192.168.10.183。

1. **更改过滤条件重新捕获**

更改过滤器条件为ip.addr==192.168.10.183，以此捕获访问ftp的所有数据包



1. **对抓取的FTP进行分析**



控制连接的端口：

**客户端172.26.206.213首先经由端口64338**与**FTP服务器192.168.10.183端口21**经过TCP三次握手建立连接，建立连接成功后，FTP服务器返回状态码220，表示服务就绪。登陆过程首先由终端向FTP服务器发送匿名用户并等待验证。用户名验证通过后，FTP服务器返回状态码331，表示用户名验证已通过并需要输入密码。终端将登陆密码发送给FTP服务器，FTP服务器验证后返回状态码230，表示用户已经登陆。终端向FTP服务器发送命令“TYPE A”，表示设置文件传输类型为ASCII，FTP服务器返回状态码 200，表示命令执行成功。

数据连接的端口：

客户端请求被动模式，FTP服务器通过21端口返回227 Entering Passive Mode (192，168，10，183，229，150)，**服务器将开放端口58774**接受来自**客户端64339的数据连接**，客户端则将使用端口进行数据连接。

1. **命令端口和数据端口**

一般来说，客户端有一个 Socket 用来连接 FTP 服务器的相关端口，它负责 FTP 命令的发送和接收返回的响应信息。一些操作如“登录”、“改变目录”、“删除文件”，依靠这个连接发送命令就可完成。服务器的命令端口号一般是21。

对于有数据传输的操作，主要是显示目录列表，上传、下载文件，我们需要依靠另一个Socket来完成。

如果使用被动模式，通常服务器端会返回一个端口号。客户端需要用另开一个Socket来连接这个端口，然后我们可根据操作来发送命令，数据会通过新开的一个端口传输。

如果使用主动模式，通常客户端会发送一个端口号给服务器端，并在这个端口监听。服务器需要连接到客户端开启的这个数据端口，并进行数据的传输。主动模式下，服务器的数据端口号一般是20。

**四、 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。

注意：

1、可以利用windows自带组件安装SMTP服务器，并配置邮件服务器，并访问。

2、 什么情况下可以捕获POP或SMTP数据包

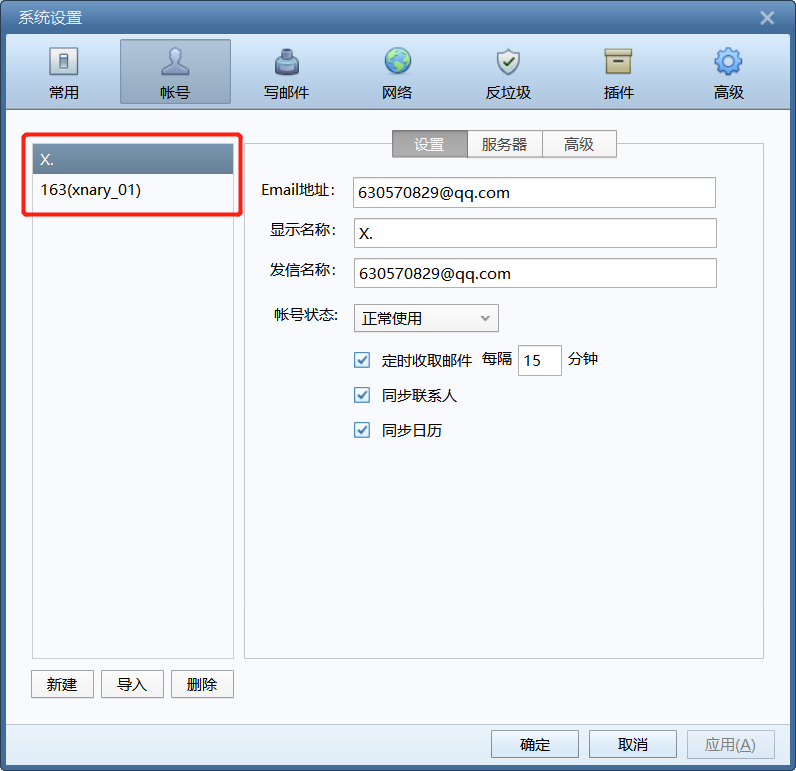
**实验步骤：**

1. **在qq邮箱和163邮箱开启相关服务**





1. **下载并配置Foxmail**
2. 下载Foxmail
3. 绑定163邮箱和qq邮箱账号



1. 本次实验从qq邮箱发送邮件到163邮箱，所以配置如下

163邮箱需手动配置



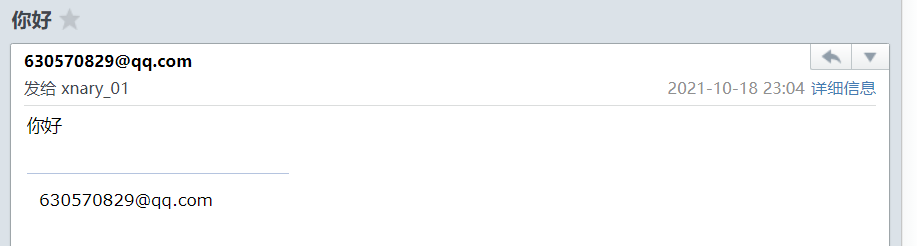
qq邮箱配置



163邮箱配置



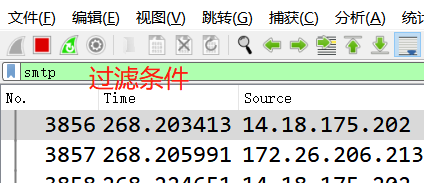
1. 发送邮件



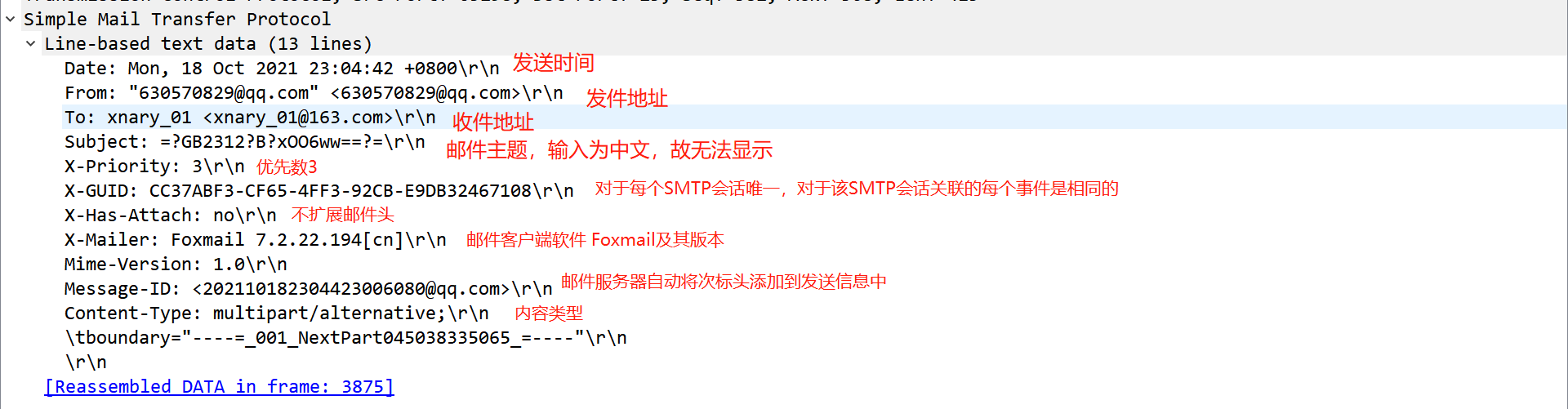
1. **利用Wireshark进行捕获，并分析**

过滤条件

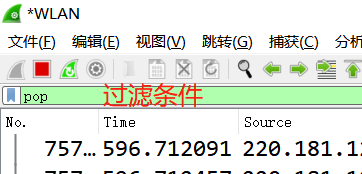
发件过程：

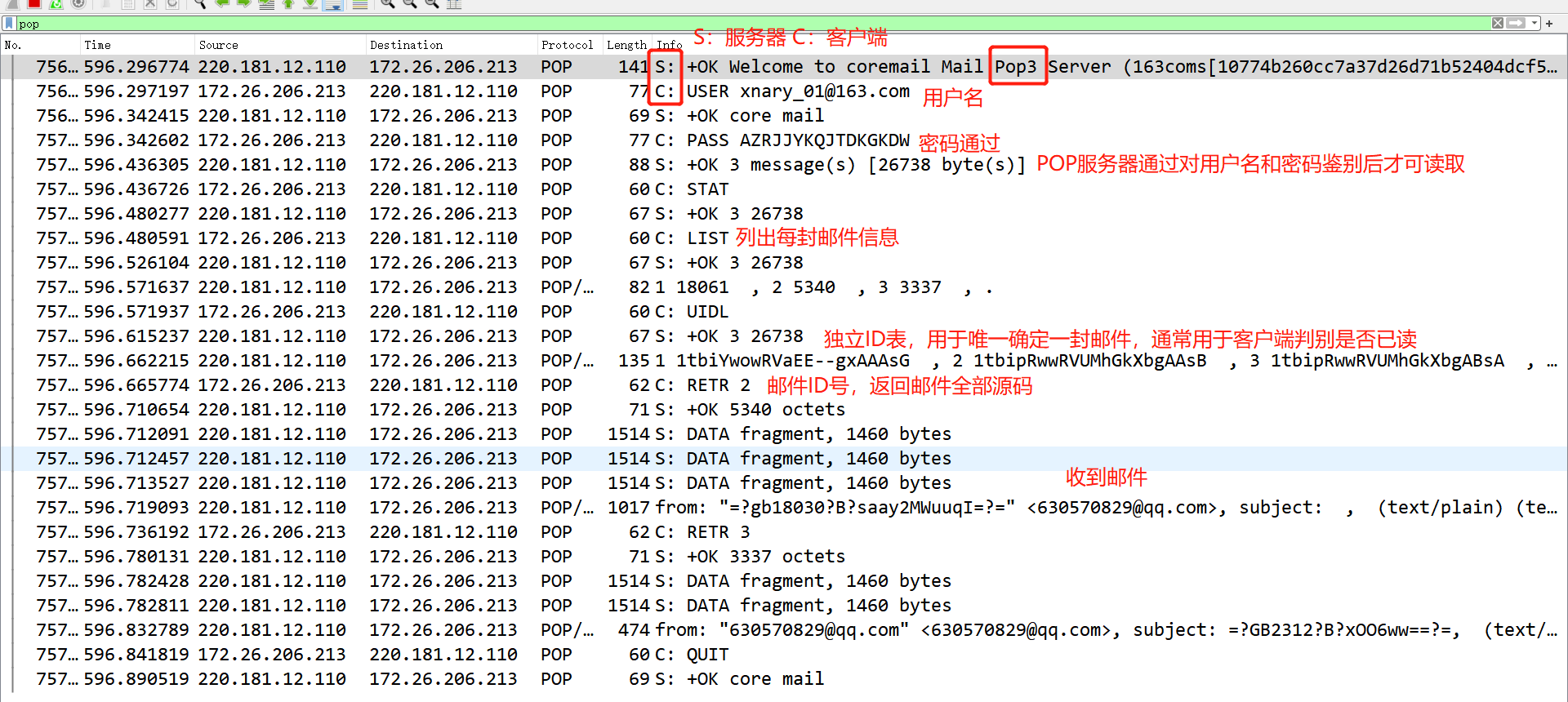






收件过程：





1. **什么情况下可以捕获POP或SMTP数据包**

在配置邮箱时，不勾选SSL可以捕获

在Foxmail中配置邮件服务器时勾选SSL则POP和SMTP不再使用默认端口，经过试验，勾选SSL后再次从qq邮箱发送邮件到163网易邮箱，wireshark中未能捕获到POP或SMTP数据包

SSL是Secure Sockets Layer 安全套接字协议，是一个不依赖于平台和运用程序的协议，位于TCP/IP协议与各种应用层协议之间，为数据通讯提供安全支持。SSL协议可分为两层： SSL记录协议（SSL Record Protocol）：它建立在可靠的传输协议（如TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。 SSL握手协议（SSL Handshake Protocol）：它建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等

1. **实验总结**

通过实验，加深理解WWW、DNS服务、FTP服务、SMTP的作用和原理，并学会使用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。

通过对HTTP协议分析，加深对HTTP协议的理解，了解其首部字段，及不同首部字段的含义，对请求报文和响应报文的结构和内容组成进一步加深

通过对DNS协议分析，对DNS请求和相应包进行理解分析，了解其中的迭代查询和递归查询，加深对DNS数据包的理解和掌握，同时弄清楚了为什么有时候能捕捉到DNS数据包，有时候捕捉不到数据包的原因

通过对FTP协议分析，了解FTP协议以及底层TCP协议的结构，更改过滤条件后对TCP协议三次握手进行分析，对FTP协议的了解着重于对服务器和客户端的控制端口和数据端口据的分析

通过对SMTP和POP协议分析，配置了邮箱发件服务器和邮箱收件服务器，进一步了解SMTP和POP的工作原理和结构，同时当对邮箱服务器进行SSL加密时，Wireshark则不能捕获其数据