**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应用层与应用层协议分析 指导教师 潘冰

实验项目编号 实验项目类型 实验地点

学生姓名 钱子仪 学号 2019052855

学院 智能科学与工程学院 专业 信息安全

实验时间2021年 月 日 上午～ 月 日上午

**实验目的**

1.理解WWW 、 DNS服务、FTP服务、SMTP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。

1. **实验内容和要求**

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）

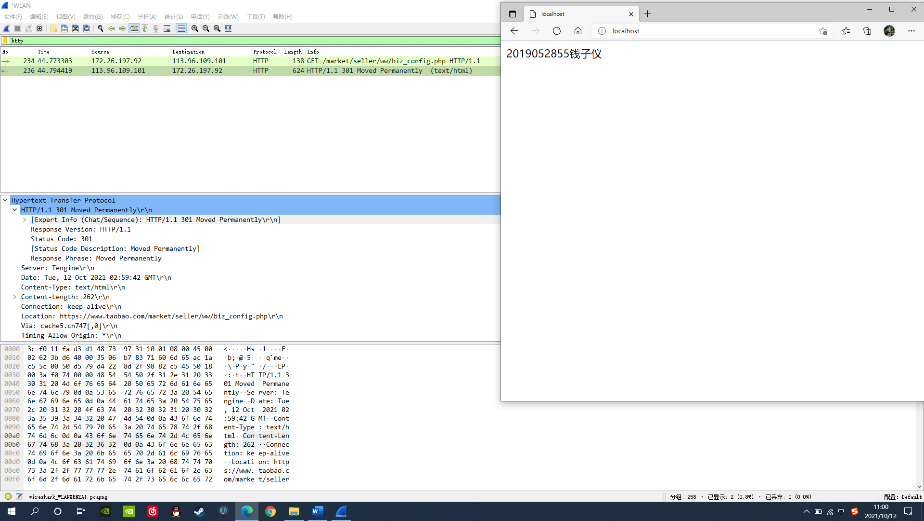
1. **主要仪器设备**

**仪器：**计算机

**实验环境：局部网环境**

1. **实验步骤与调试**

一、HTTP协议分析



如图，使用wireshark截获了自行创建的www站点的http协议。内容为：

HTTP/1.1 301 Moved Permanently响应行信息

Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently 专家信息

HTTP/1.1 301 Moved Permanently #HTTP响应信息，响应码为301

Response Version: HTTP/1.1 请求版本

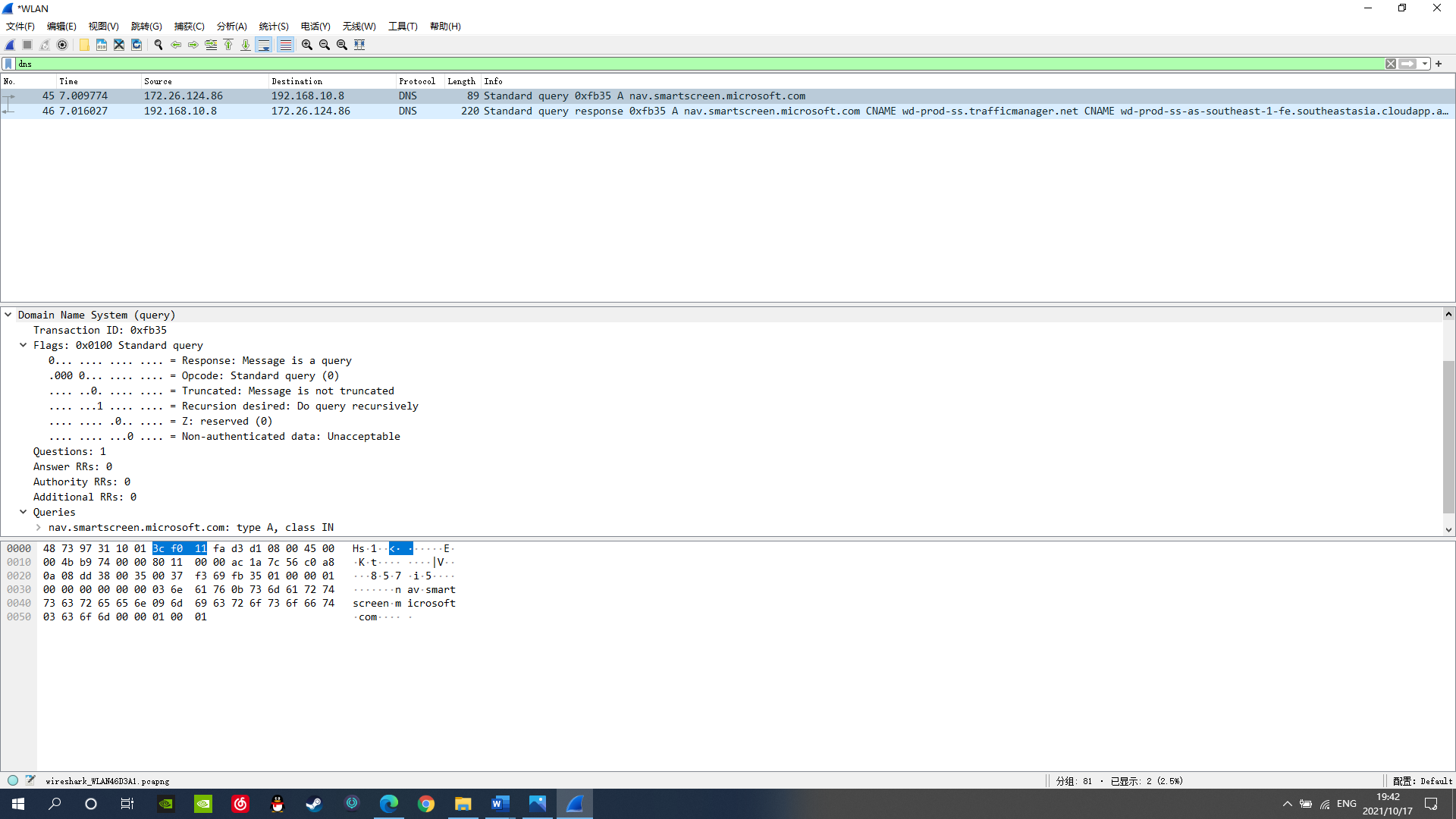
Status Code: 301 状态码

Response Phrase: Moved Permanently 响应短语

Content-Type: text/html 响应的内容类型

Content-Length: 262 包的长度

二、DNS协议分析



如图，用wireshark捕获了自己建立的网站的DNS

第一行transaction ID为标识字段，用于辨别DNS应答报文是哪个请求的回应。

第二行是Flags标志字段

Questions为问题数,通常为1

Answer RRs为资源记录数,Authority RRs为授权资源记录数,Additional RRs为额外资源记录数，三者通常为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)是ping后的参数,不定长度以0结束

DNS协议的工作过程：第一步：客户机提出域名解析请求,并将该请求发送给本地 域名服务器。

第二步：当本地 域名服务器收到请求后,就先查询本地 缓存,如果 该纪录项,则本地 域名服务器就直接把查询 结果返回。

第三步：如果本地 缓存中没 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,然后根域名服务器再返回给本地域名服务器一个所查询域(根 子域) 主域名服务器 地址。

第四步：本地服务器再向 一步返回 域名服务器发送请求,然后接受请求 服务器查询自己 缓存,如果没 该纪录,则返回相关 下级 域名服务器 地址。

第五步：重复第四步,直到找到正确 纪录。

第六步：本地域名服务器把返回 结果保存到缓存,以备下一次使用,同时还将结果返回给客户机。

三、FTP协议分析

FTP是客户端-服务器协议，它依赖于客户端和服务器之间的两个通信通道。一个用于控制对话的命令通道和一个用于传输文件内容的数据通道。客户端通过请求下载文件来启动与服务器的对话。客户端可以使用FTP上传、下载、删除、重命名、移动和复制服务器上的文件。用户通常需要登录FTP服务器FTP服务一般运行在20和21两个端口。端口20用于在客户端和服务器之间传输数据流，而端口21用于传输控制流。并且是命令通向ftp服务器的进口。

控制连接（TCP 21端口）主要用于实现FTP协议控制信令传送，服务器端打开TCP 21端口被动等待客户端发起连接命令。一旦建立连接，数据就会通过这些客户端和服务器端口进行传输。

数据连接（TCP 20端口）主要用于实现应用数据传送，服务器的数据连接端使用端口20。一旦建立连接，数据就会通过这些客户端和服务器端口进行传输。

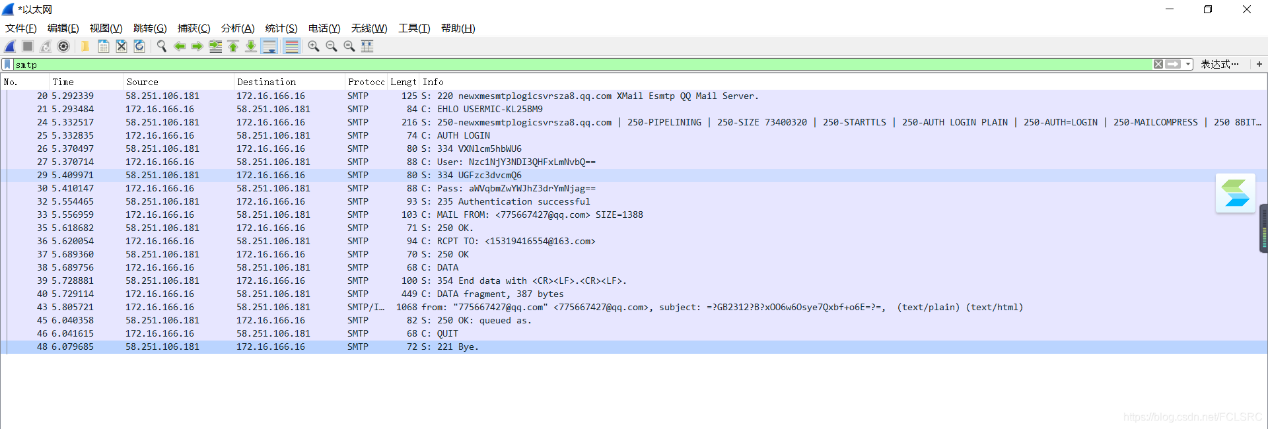
四、SMTP协议

协议工作过程：

(1)建立连接：在这一阶段，SMTP客户请求与服务器的25端口建立一个TCP连接。一旦连接建立，SMTP服务器和客户就开始相互通告自己的域名，同时确认对方的域名。

(2)邮件传送：利用命令，SMTP客户将邮件的源地址、目的地址和邮件的具体内容传递给SMTP服务器，SMTP服务器进行相应的响应并接收邮件。

(3)连接释放：SMTP客户发出退出命令，服务器在处理命令后进行响应，随后关闭TCP连接。



五、POP协议

用户从邮件服务器上接收邮件的典型通信过程如下。

1)        用户运行用户代理（如Foxmail, Outlook Express）。

2)        用户代理（以下简称客户端）与邮件服务器（以下简称服务器端）的110端口建立TCP连接。

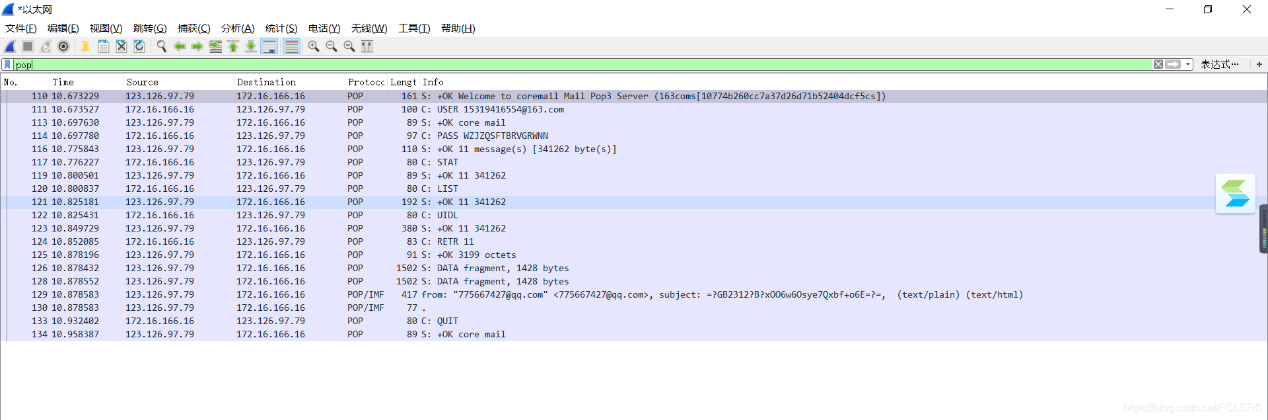
3)        客户端向服务器端发出各种命令，来请求各种服务（如查询邮箱信息，下载某封邮件等）。

4)        服务端解析用户的命令，做出相应动作并返回给客户端一个响应。

5)        3）和4)交替进行，直到接收完所有邮件转到步骤6)，或两者的连接被意外中断而直接退出。

6)        用户代理解析从服务器端获得的邮件，以适当地形式（如可读）的形式呈现给用户。

其中2)、3）和4）用POP3协议通信。

****

**（三）实验结果与分析**

本次实验通过wireshark抓包，结合网络资料了解了FTP、SMTP和POP协议的工作方式以及协议细节。除了抓包http协议使用了自己搭建的站点之外，其他都使用已有网站或服务器完成抓包。