**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

实验项目编号三 实验项目类型 验证型实验地点 计算机网络实验室

学生姓名 张诗宇 学号 2019054001

学院 智能科学与工程 系 专业 信息安全

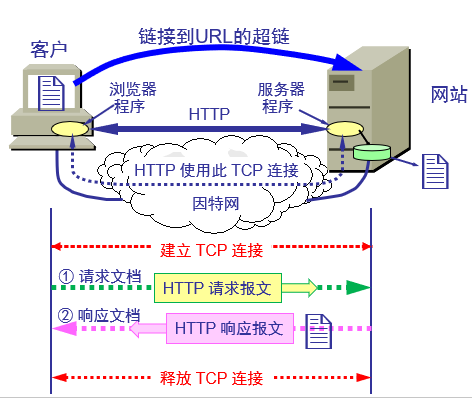
实验时间 2021 年 10 月 11 日 上 午～ 10 月 18 日 下 午

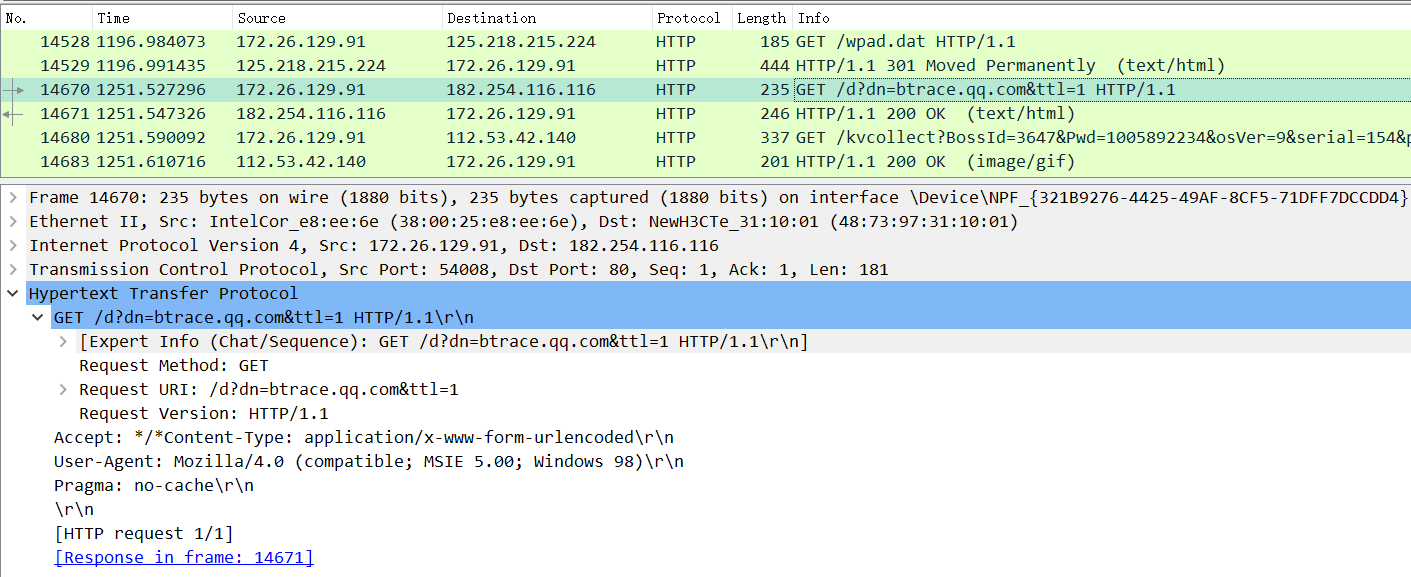
1. **实验目的**
2. 理解WWW 、 DNS服务、FTP服务、SMTP的作用和原理；
3. 学会使用wireshark分析HTTP、FTP、SMTP和DNS协议的工作过程，加深对协议格式和工作原理的理解。
4. **实验内容**
5. 通过域名访问WWW、FTP服务器，分析DNS、WWW、FTP工作过程，并使用WireShark分析相关协议格式；
6. 在客户端访问SMTP服务器，使用wireshark分析SMTP、POP3协议的工作过程。（可以在客户端安装outlook或使用QQ邮件服务器或自己编程）
7. **实验设备**

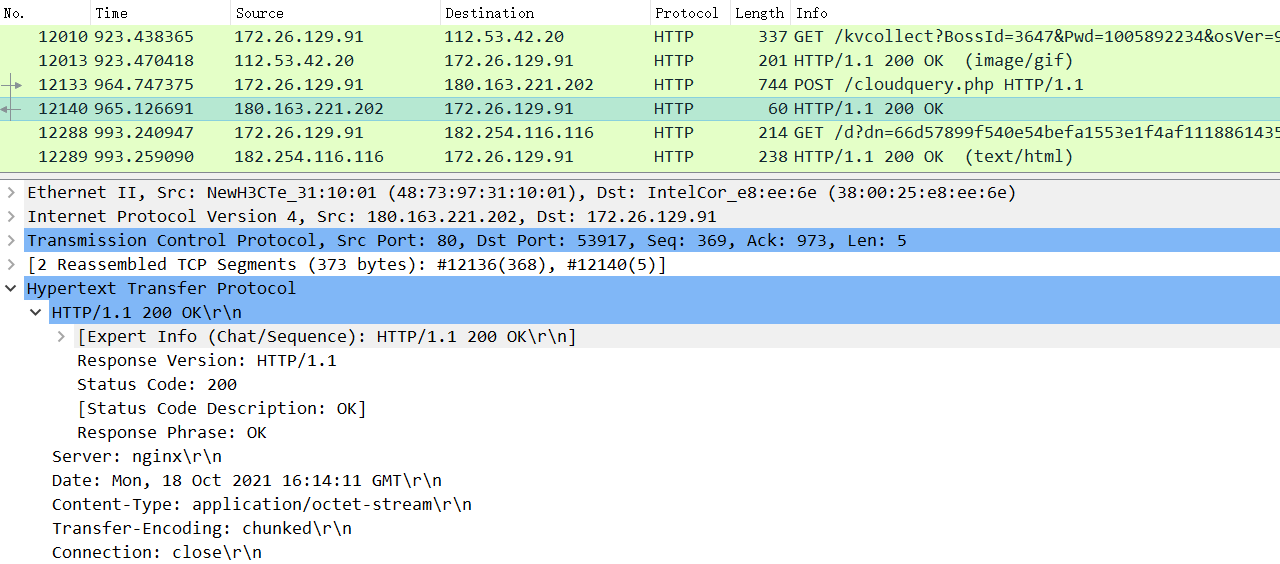
局部网环境，计算机若干台。本实验不分组，独立完成

1. **实验步骤**
2. 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







(1) 浏览器分析超链指向页面的 URL。

(2) 浏览器向 DNS 请求解析网站域名的 IP 地址。

(3) 域名系统 DNS 解析出服务器的 IP 地址。

(4) 浏览器与服务器建立 TCP 连接

(5) 浏览器通过HTTP发出取文件命令：如，GET /index.htm

(6) 服务器通过HTTP给出响应，把文件 index.htm 发给浏览器。

(7) TCP 连接释放。

(8) 浏览器显示网站主页文件 index.htm 中的所有文本。

HTTP首部字段根据实际用途分为4种类型：

通用首部字段： 请求报文和响应报文两方都会使用到的首部。

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。

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，补充了响应时的附加内容，也会要求客户端附加额外的内容信息。

实体首部字段： 针对请求报文和响应报文的实体部分使用到的首部，补充了资源内容更新时间等与实体有关的信息。

首部字段名 说明

Cache-Control 控制缓存行为

Connection 逐跳首部、连接的管理

Date 创建报文的日期时间

Pragma 报文指令

Transfer-Encoding 指定报文传输主体的编码方式

Upgrade 升级为其他协议

Via 代理服务器的相关信息

Warning 错误通知

Accept 用户代理可以处理的媒体类型

Accept-Charset 优先的字符集

Accept-Encoding 优先的内容编码

Authorization Web认证信息

Except 期待服务器的特定行为

Host 请求资源所在的服务器

if-Match 比较实体标记（ETag）

if-Modified-Since 比较资源的更新时间

Range 实体的字节范围请求

Refer 实体的字节范围请求

TE 传输编码的优先级

User-Agent HTTP客户端程序的信息

Accept-Ranges 是否接受字节范围请求

Age 推算资源创建经过的时间

ETag 资源的匹配信息

Location 令客户端重定向至指定UPI

Proxy-Authenticate 代理服务器对客户端的认证信息

WWW-Authenticate 服务器对客户端的认证信息

Server HTTP服务器的安装信息

Vary 代理服务器的管理信息

Allow 资源可支持的HTTP方法

Content-Encoding 实体主体适用的编码方式

Content-Language 实体主体的自然语言

Content-Length 实体主体的大小

Content-Location 替代对应资源的URI

Content-MD5 实体主体的报文摘要

Content-Range 实体主体的位置范围

Content-Type 实体主体的媒体类型

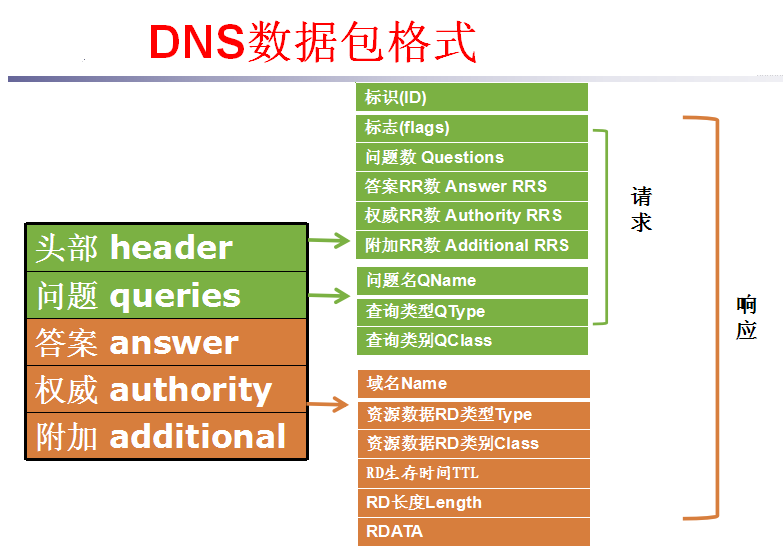
EXpires 实体主体过期的日期时间

Last-Modified 资源的最后修改日期时

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。

DNS格式如下：



标志flags（16位）



QR：0表示查询报文query，1表示响应报文response

Opcode：0-标准查询，1-反向查询（IP地址查域名，IP地址.in-addr.arpa.），2-服务器状态查询,3~15保留。

AA：授权应答(Authoritative Answer) - 在应答数据包中使用， 1表示授权回答，指出给出应答的服务器是授权解析服务器。

TC：截断（TrunCated），用来指出报文比允许的长度还要长，导致被截断。TC=1,表示大于512字节，被删减成512字节，置TC=0没截断。

RD：期望递归(Recursion Desired) -由客户端请求设置，应答的时候使用相同的值返回。 RD=1，就建议域名服务器进行递归解析。

RA： 支持递归(Recursion Available) - 在应答中设置或取消，用来代表服务器是否支持递归查询。  RA=1，表示可用递归。

Zero:保留值，占3位，必须为0

Rcode： 应答码 ，占4位。

0      没有错误。

1      报文格式错误(Format error) - 服务器不能理解请求的报文。

2   服务器失败(Server failure) - 因为服务器的原因导致没办法处理这个请求。

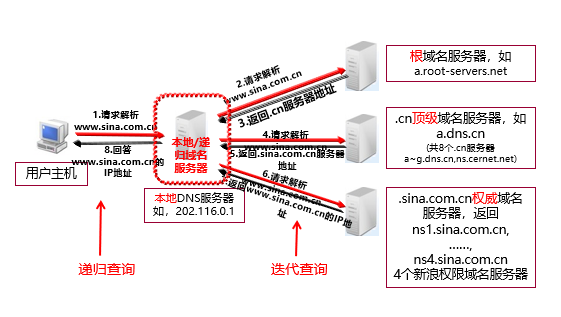
3      名字错误(Name Error) - 只有对授权域名解析服务器有意义，指出解析的域名不存在。

4      没有实现(Not Implemented) - 域名服务器不支持查询类型。

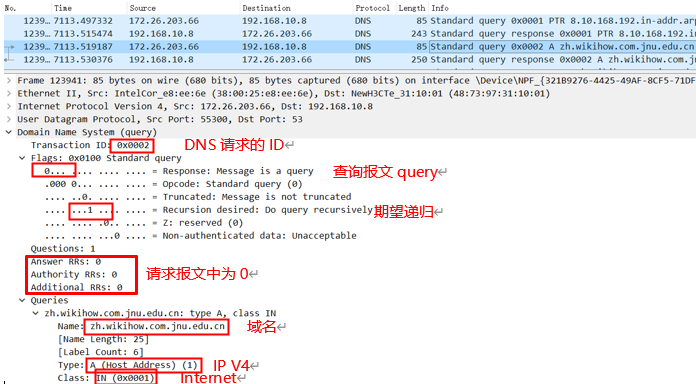
5      拒绝(Refused) - 服务器由于设置的策略拒绝给出应答。比如，服务器不希望对某些请求者给出应答，或者服务器不希望进行某些操作（比如区域传送zone transfer）。

6-15    保留值，暂时未使用。

DNS工作过程：



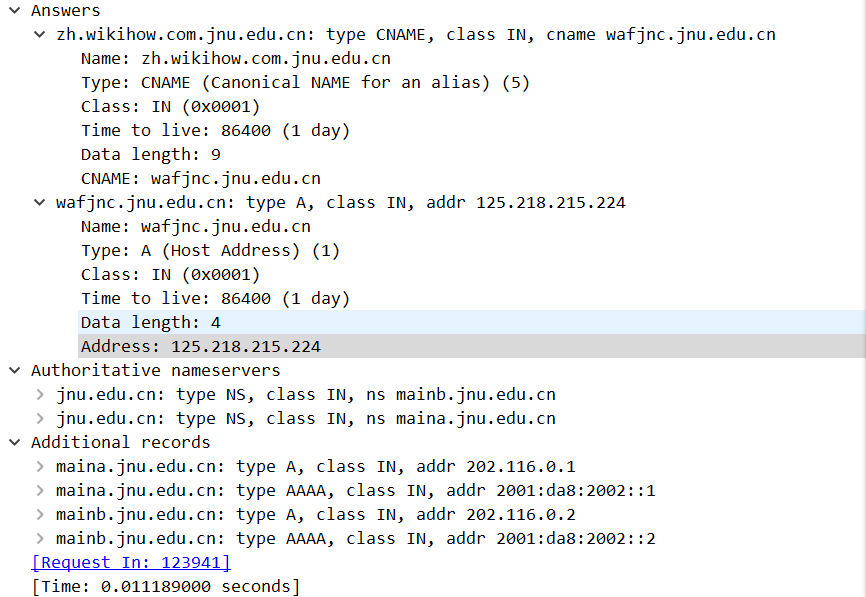
在谷歌浏览器访问zh.hikihow.com网站，捕获DNS数据包—查询请求：



浏览器先看本地是否有zh.wikihow.com的缓存，没有，并且本机文件中没有对应的IP地址，于是浏览器发出一个ID为0x0002的请求：在Internet上以递归方式查询zh.wikihow.com的IPV4地址。

捕获DNS数据包—查询应答：





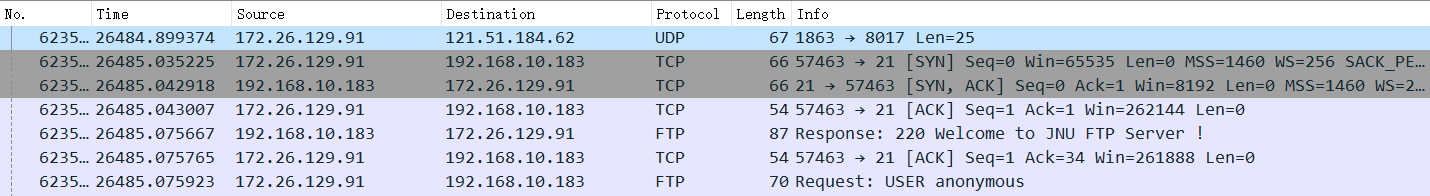
权威服务器给出的附加结果

两台权威服务器

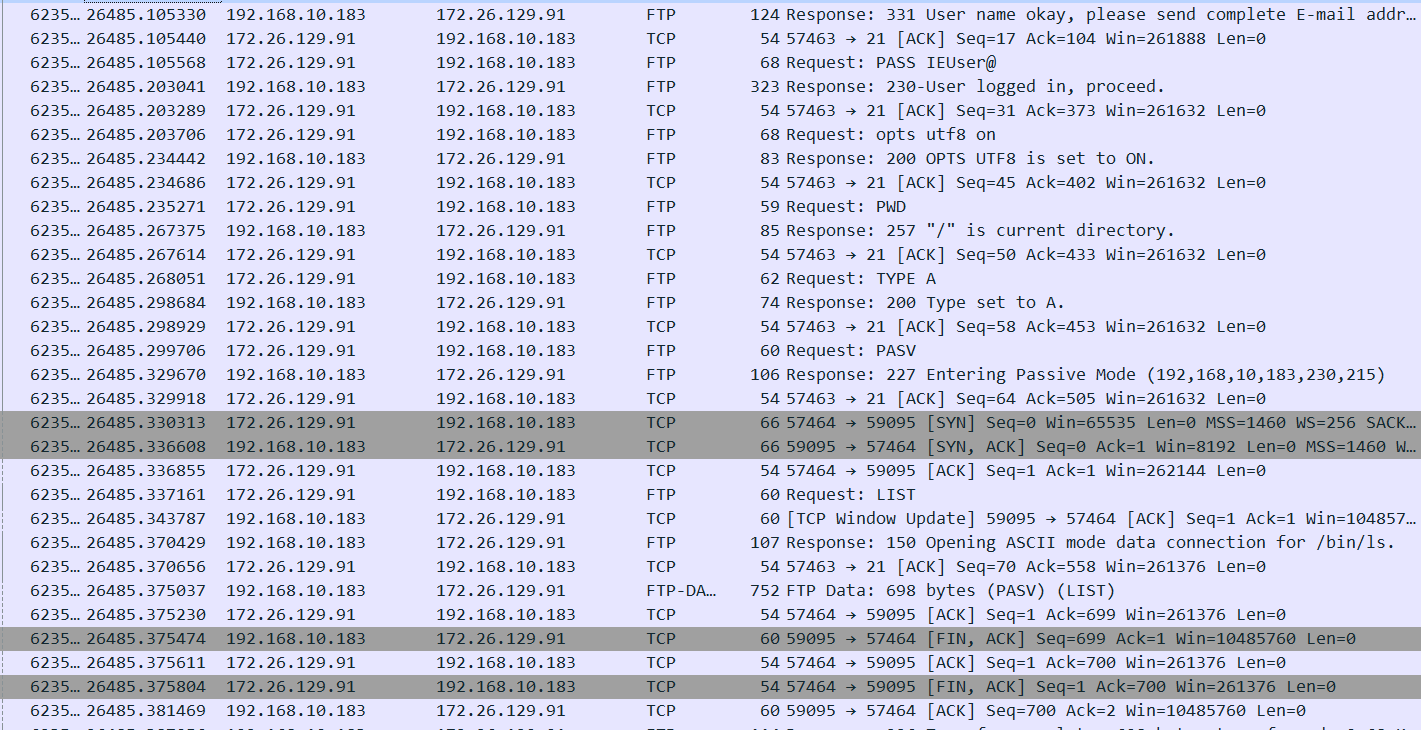
查询没有zh.wikihow.com的A记录，继续查询到zh.wikihow.com的NS记录，2个 zh.wikihow.com权威域名服务器，返回IP地址。

1. FTP协议分析

被动模式



三次握手建立控制连接：  
服务器：21 客户：57463



协商工作模式：被动模式PASV。

客户端发起协商工作模式，**服务器**数据连接端口：230\*256+215=59095

客户端发起建立数据连接：

服务器：50225--客户：53374+1

四次握手断开数据连接

1. 建立控制连接

三次握手建立TCP连接，客户端57463通过控制进程向服务器进程（21）发出建立连接请求，协商工作模式（被动PASV）、客户端或服务器端口号，用于建立数据传送连接。

1. 建立数据连接

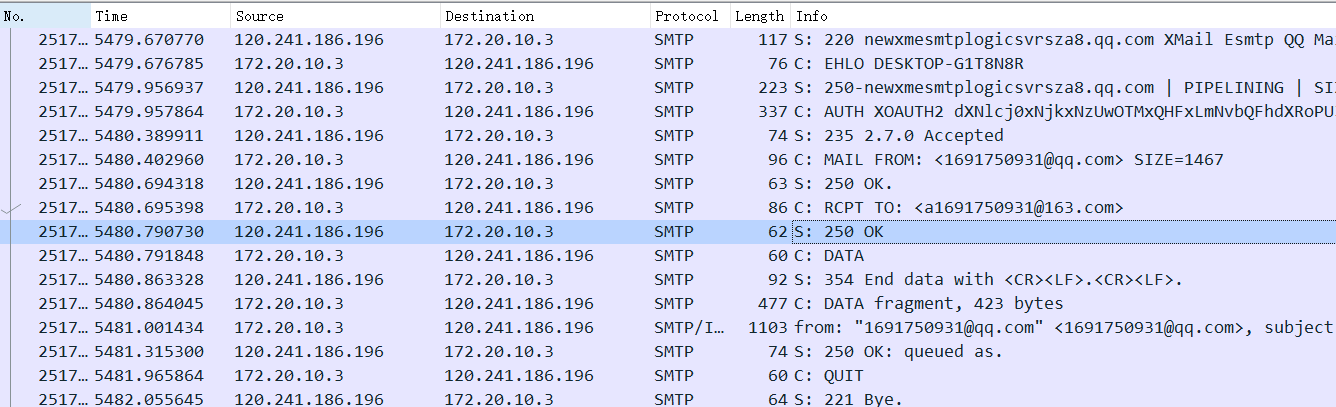
客户进程（端口号已协商好）发起与服务器进程（端口号：控制连接端口号+1）建立数据连接（TCP三次握手）

1. 关闭数据连接

数据传送进程完成实际的文件传送,传送完毕,关闭数据传送连接.控制连接不关闭。

主动模式

1. SMTP和POP协议分析



SMTP通信：

1）建立连接

SMTP客户周期性地从邮件缓冲区进行扫描，如果有邮件就SMTP熟知的端口25与目的主机的SMTP服务器建立TCP连接。不使用中间的邮件服务器，TCP连接是基于收发双方的两个邮件服务器，并非在收发人之间的连接。

2）邮件传送

从mail命令开始。如MAIL FROM:<XIEXIREN@TSINGHUA.ORG.CN>

3）释放连接

SMTP客户发送QUIT命令，服务器返回”221 (服务关闭)”表示SMTP统一释放连接。

1. **实验总结**

本次实验通过域名访问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。（在客户端安装了foxmail）

通过本次实验进一步理解了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，加深了对协议格式和工作原理的理解。

**暨南大学本科实验报告专用纸(附页)**