**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 赖智聪 学号 2019051118

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。** |

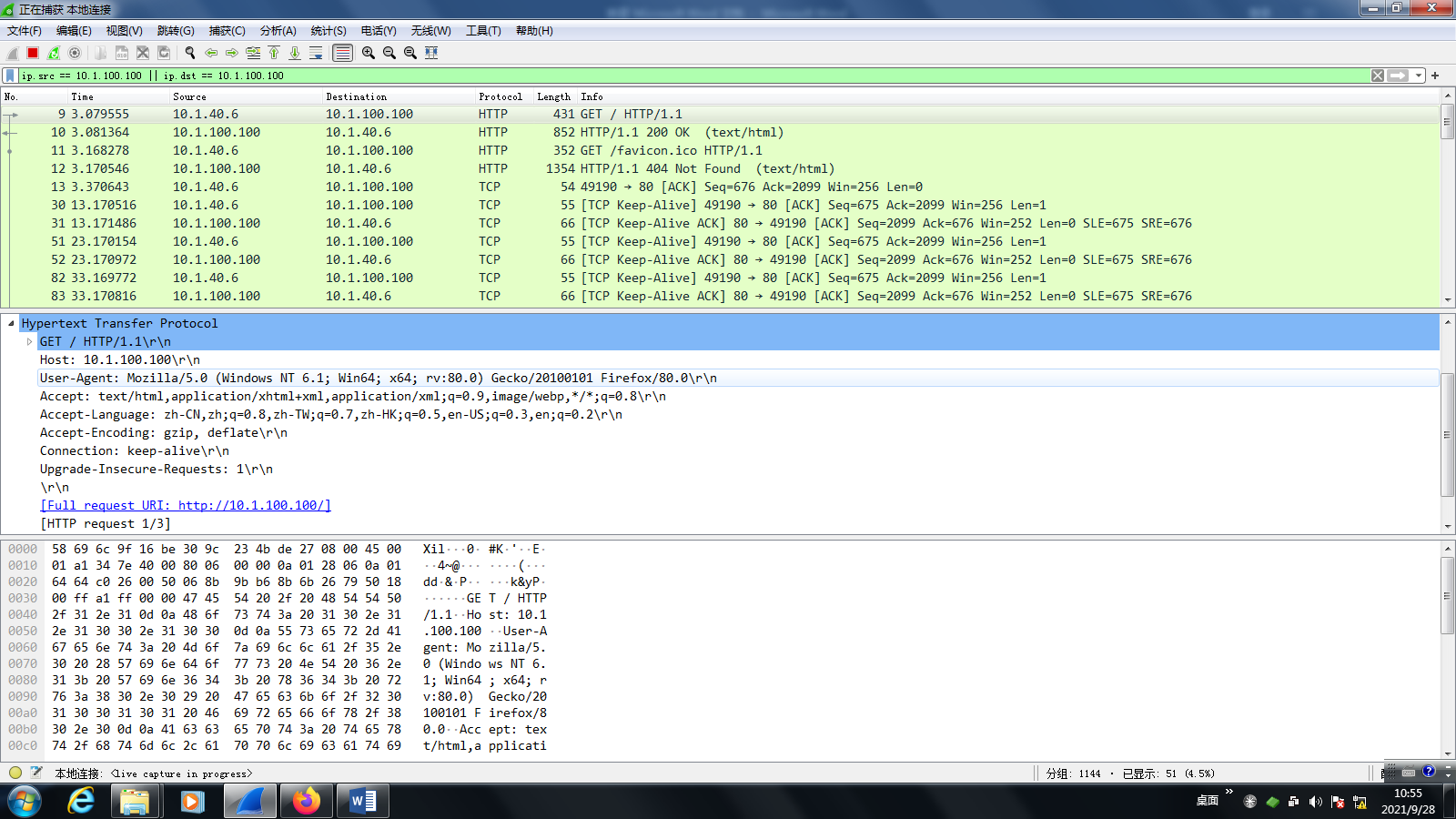
|  |
| --- |
| **二、实验环境** |
| 局部网环境，计算机若干台。本实验不分组，独立完成。 |
| **三、实验内容**   * + 通过域名访问WWW、FTP服务器，分析DNS、WWW、FTP工作过程，并使用WireShark分析相关协议格式；   + 在客户端访问SMTP服务器，使用wireshark分析SMTP、POP3协议的工作过程。（可以在客户端安装outlook或使用QQ邮件服务器或自己编程） |

**四、实验及分析**

一、http协议分析

访问网站，得到的是http请求（GET），还有TCP三次握手和释放TCP

请求报文：



对其报文进行分析：

首部GET表示是请求报文，版本是http/1.1；

Host字段体现了请求的IP地址；

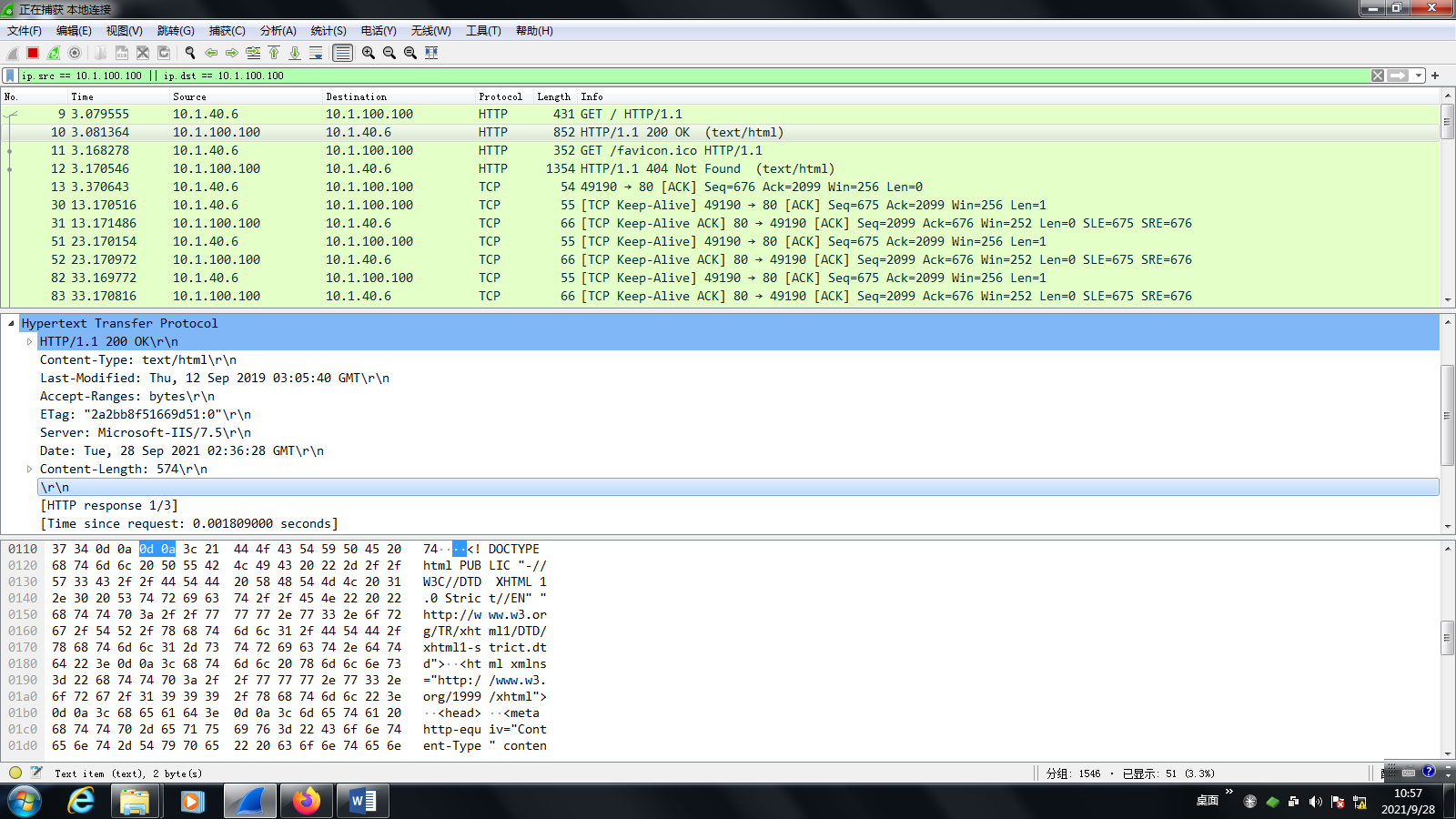
Accept字段：表明了可以接受的响应类型；

Connection字段：表明是一个持续的连接；

Upgrade-Insecure-Requests字段：Upgrade-Insecure-Requests:1表示浏览器告诉服务器，它能读懂服务器发过来的信息；

倒数第二行表明URI的全称，最后一行表示请求进度。

响应报文：



大致内容和请求报文类似，但存在一些差别：

第二含200表示状态OK

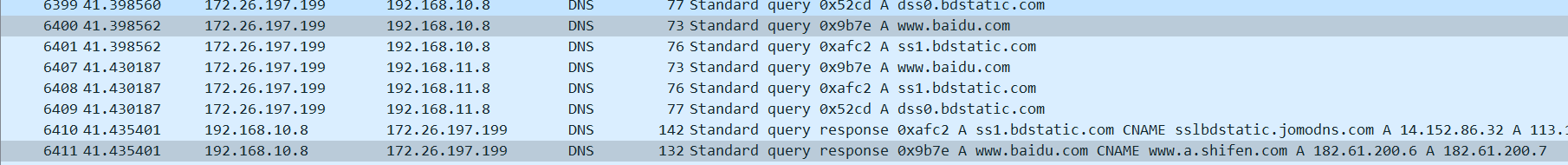
Etag：资源实体的指纹，以确定两个版本的资源是否相同。

Server：表明服务器的名称。

1. DNS协议分析

访问[www.baidu.com](http://www.baidu.com)，通过wireshark抓包进行分析

可以得到下图中的情况，黑色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。

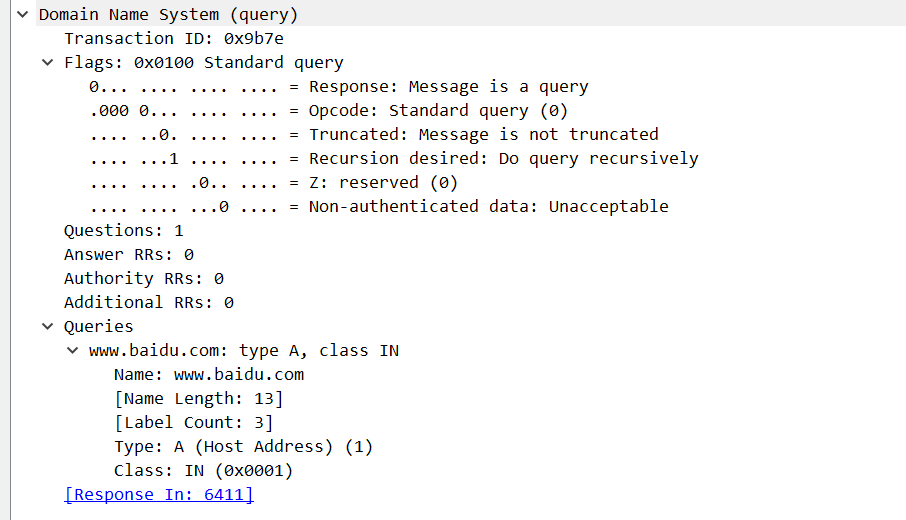
第三步：根域名服务器再返回给本地域名服务器一个所查询域(根的子域) 的主域名服务器的地址。本地服务器再向上一步返回的域名服务器发送请求，然后接受请求的服务器查询自己的缓存，如果没有该纪录，则返回相关的下级的域名服务器的IP地址。

第四步：重复第三步，直到找到正确的纪录。

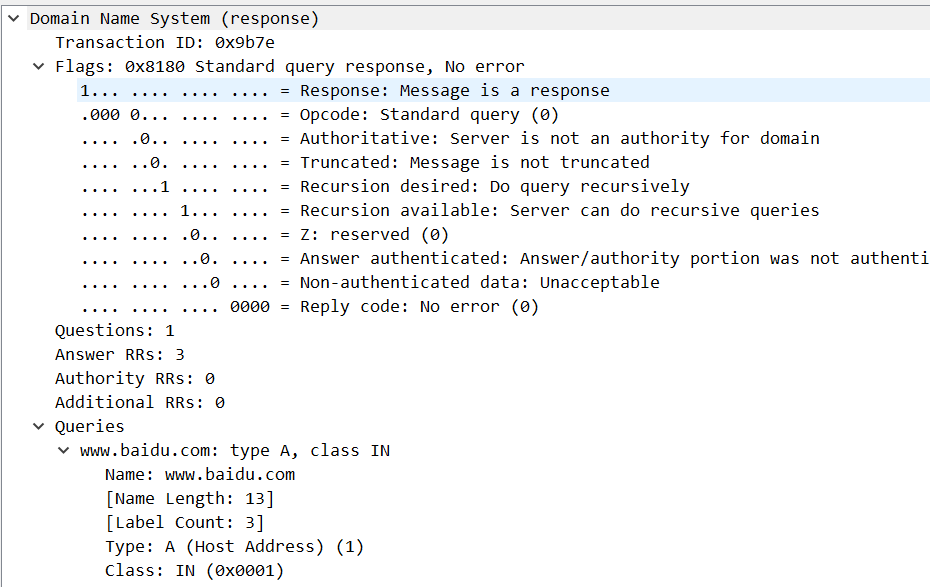
第五步：本地域名服务器把返回的结果保存到缓存，以备下一次使用.

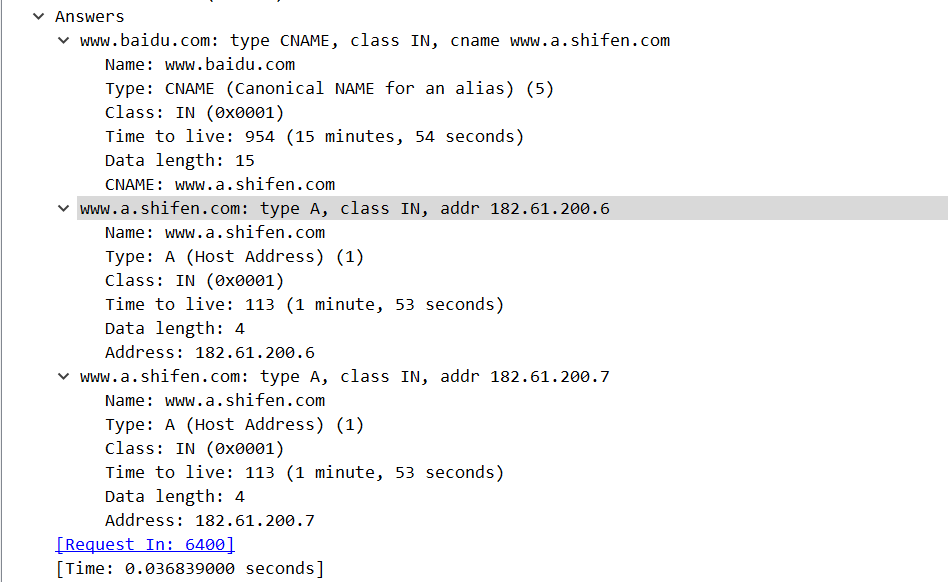
DNS报文分析：

请求：



回答：



**基础结构部分**：

Transaction ID字段：即事务ID，请求报文和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字段为0，表示这是一个请求报文，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；

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；

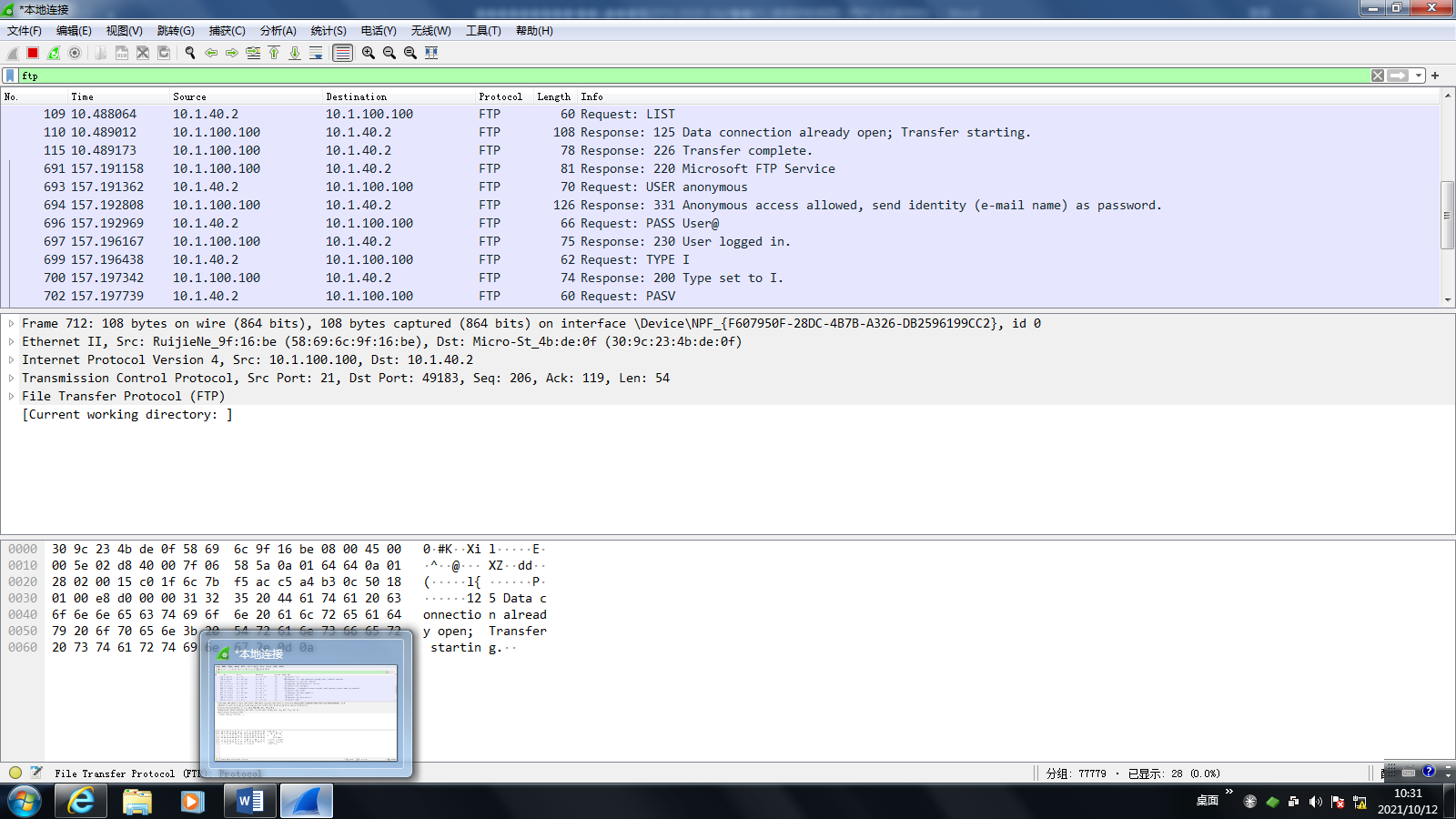
**问题部分：**

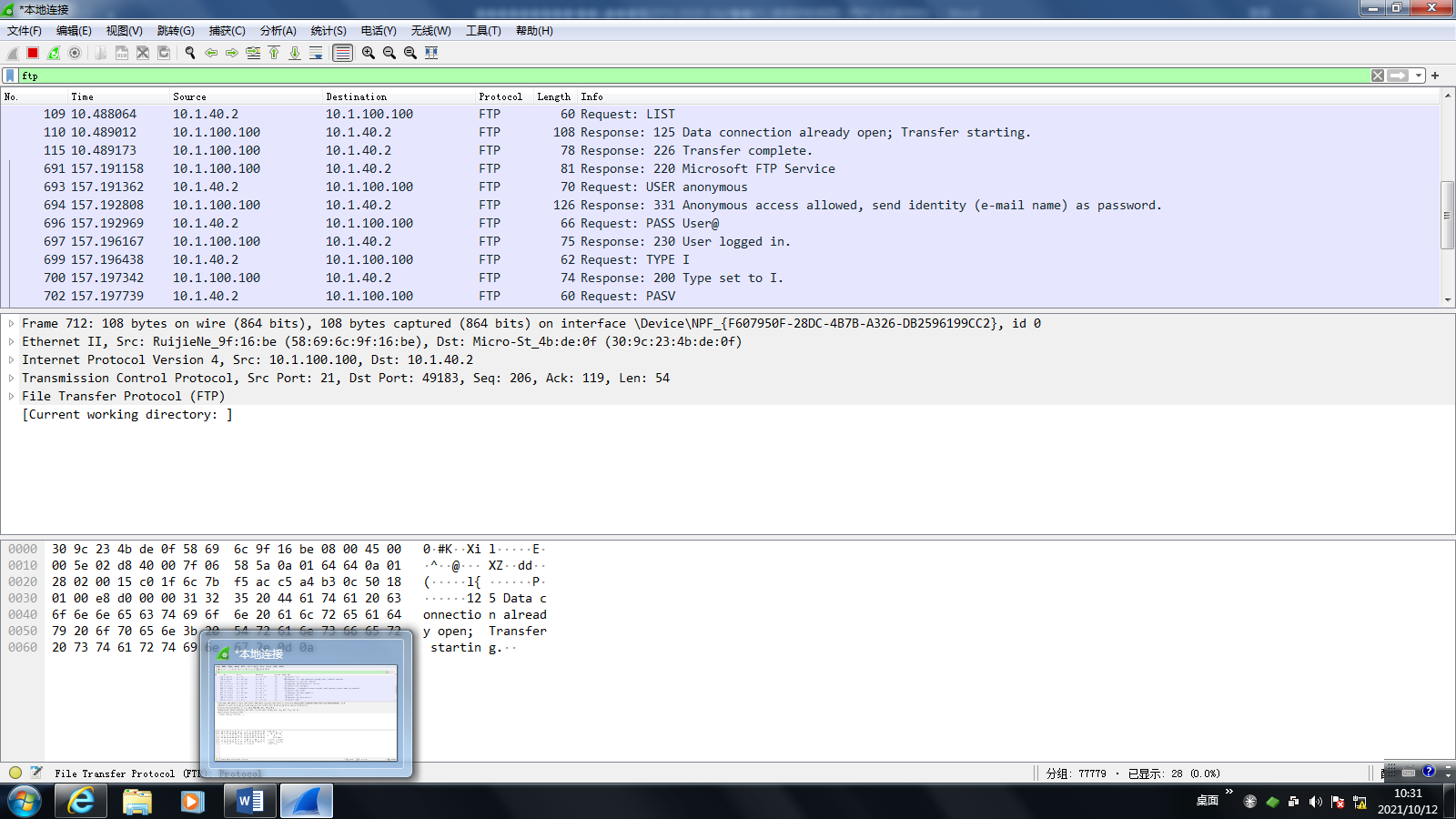
www.baidu.com是所需要请求解析的域名，type A表示由域名（Host Address）获取对应的 IP 地址，class IN表示地址类型为互联网地址。最后一行的是对应的应答报文或请求报文所在的帧。

1. FTP协议分析

进入<ftp://ftp.jnu.edu.cn>，并使用wireshark进行抓包分析。

首先通过TCP三次握手建立连接，然后进入身份认证阶段，通过后进入ftp会话从而处于命令交互阶段，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。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。



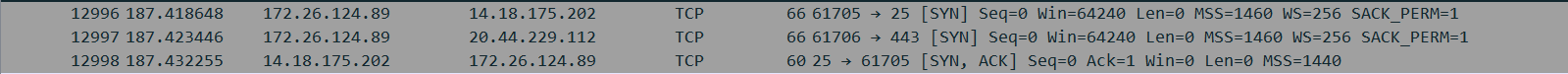


1. SMTP和POP协议分析

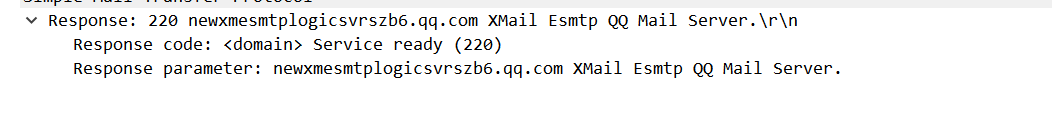
使用QQ邮箱，从一个用户发送一封测试邮件给另一个QQ邮箱用户，并利用wireshark抓包。

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



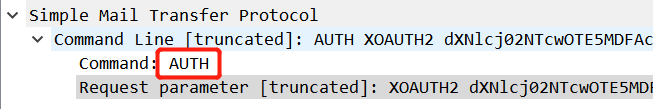
连接建立后，SMTP服务器发出状态“220”，即第一个STMP数据包，表示服务已经就绪：



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

接下来用户发送AUTH命令进行身份认证。



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

之后开始邮件传送，邮件的传送从MAIL命令开始，后面跟有发件人的地址：

服务器回复“250 OK”，表示已准备好接收邮件。

下面跟着一条RCPT命令，表示邮件的收件人地址：

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。

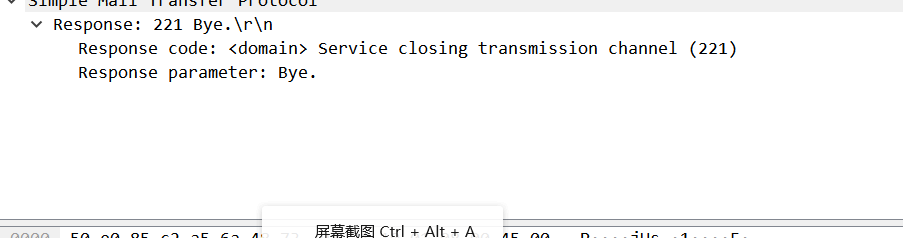
SMTP返回的信息如下，354代表服务器为这封邮件创建了缓冲区，客户可以开始邮件传输：

接着就开始发送邮件的内容：

SMTP/INF数据包里有邮件的日期，主题等信息。

SMTP服务器回复“250 OK”，表示邮件收到了。

邮件发送完毕后，SMTP客户发送QUIT命令，SMTP服务器回复的信息是221服务关闭，表示同意释放连接：



**五、实验总结**

通过使用wireshark对相关协议的数据包进行分析，更好地了解了www，DNS服务，FTP服务，SMTP的工作原理和过程。