**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 验证型

实验地点 计算机网络实验室

学生姓名 许铭燊 学号 2019051106

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 下 午～ 10 月 12 日 下 午

**【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。**

**【实验内容】**

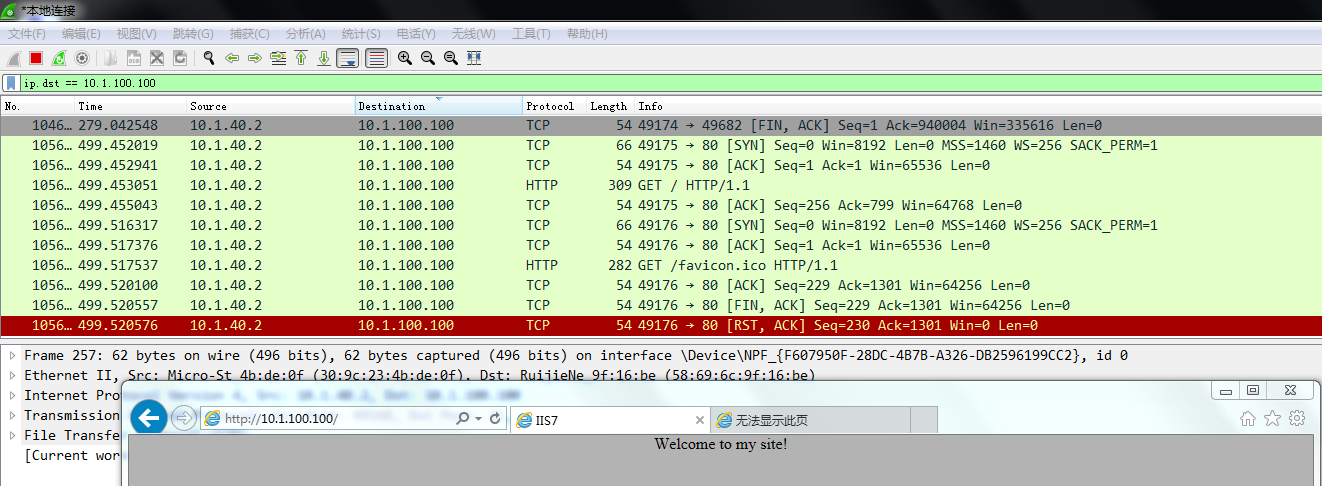
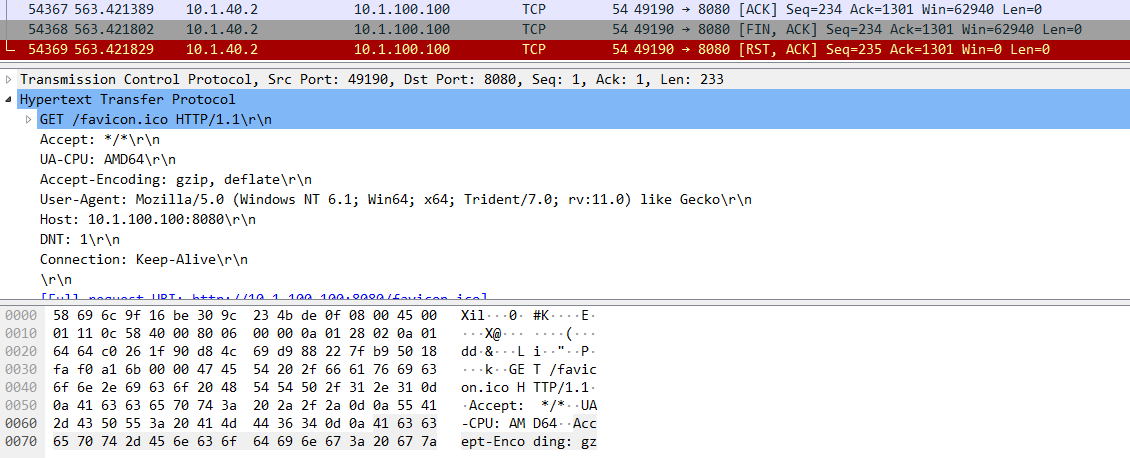
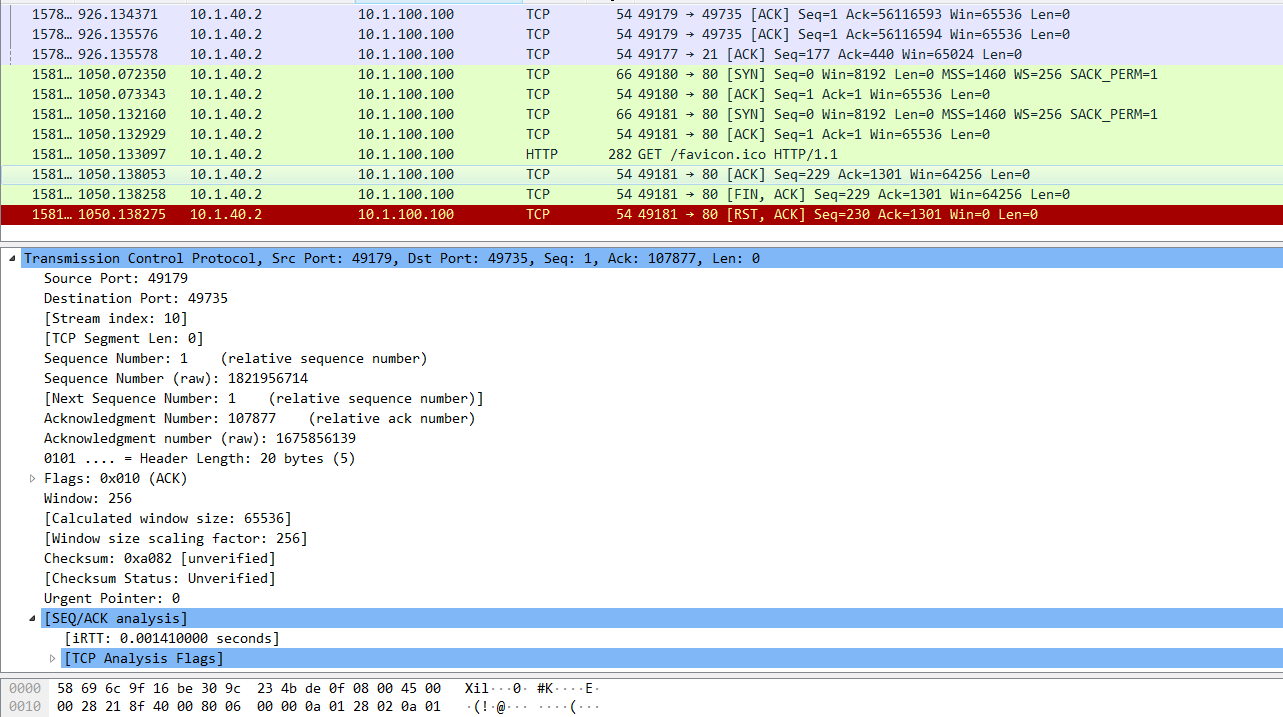
* + 通过域名访问WWW、FTP服务器，分析DNS、WWW、FTP工作过程，并使用WireShark分析相关协议格式；
  + 在客户端访问SMTP服务器，使用wireshark分析SMTP、POP3协议的工作过程。（可以在客户端安装outlook或使用QQ邮件服务器或自己编程）

**【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。

**【实验步骤】**

**一、HTTP协议分析**



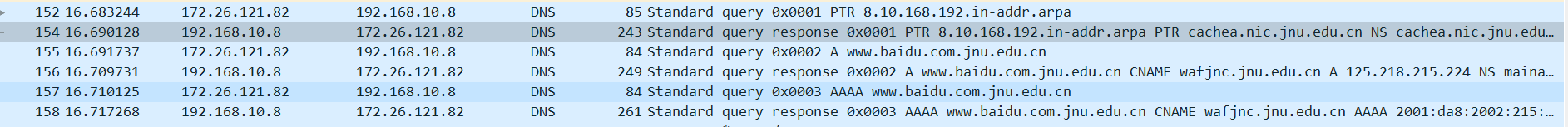
键入http：//10.1.100.100,使用wireshark对10.1.100.100进行嗅探，得出如上信息，可见http协议一共分如上四步，即，客户与服务器建立连接；客户向服务器提出请求；服务器接受请求，并根据请求返回相应的文件作为应答；客户与服务器关闭连接。

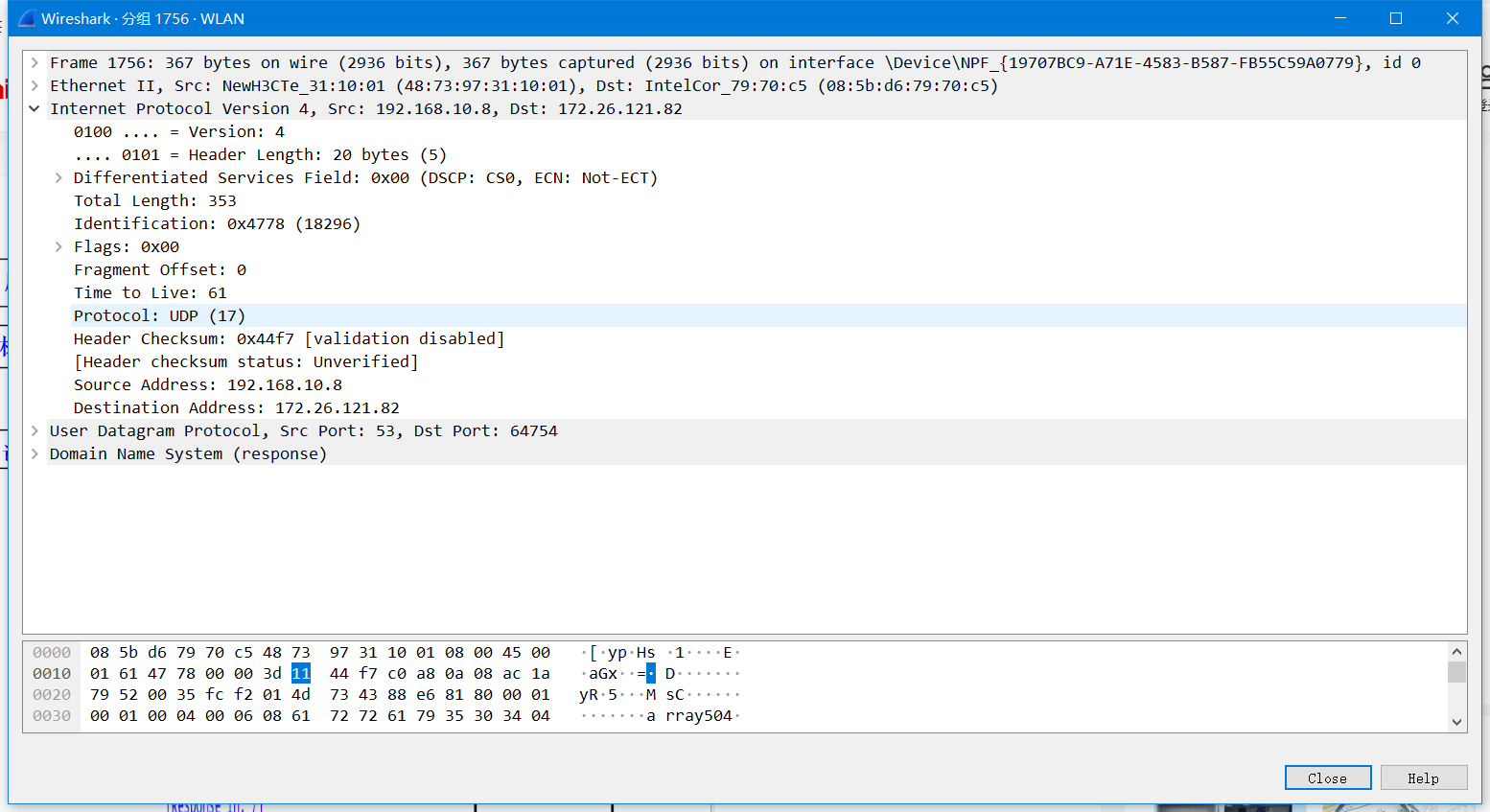
1. **DNS协议分析**

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。

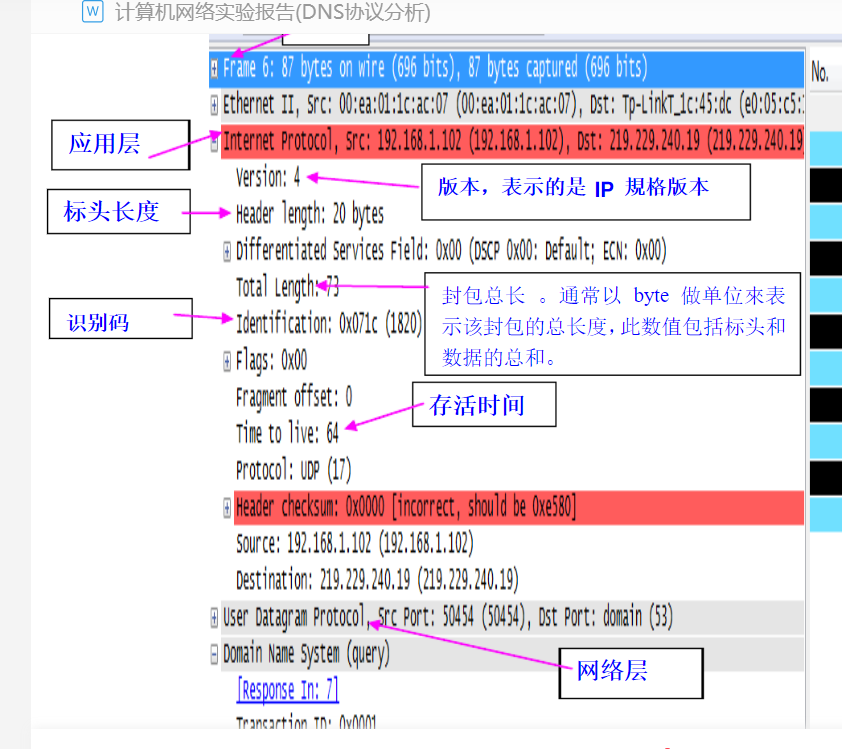


我们以www.baidu.com为例。使用wireshark分析如下

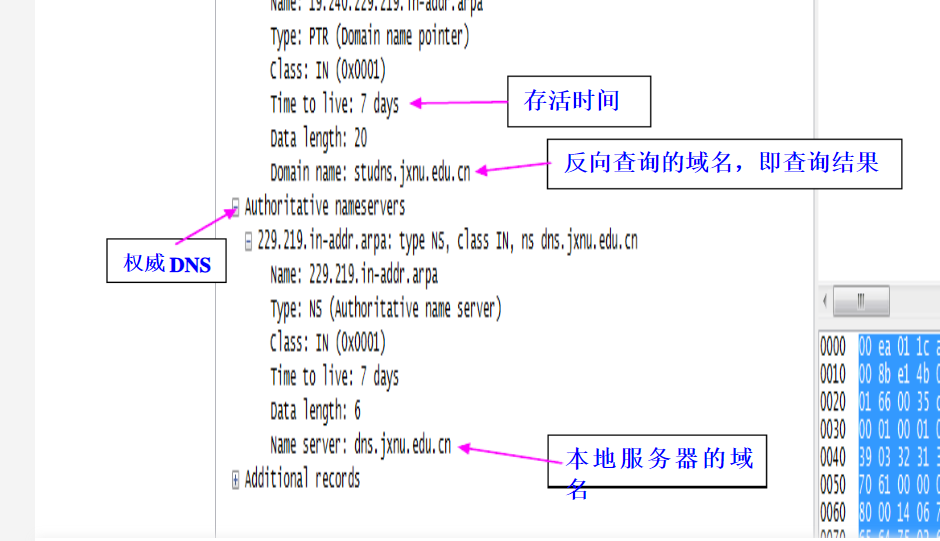




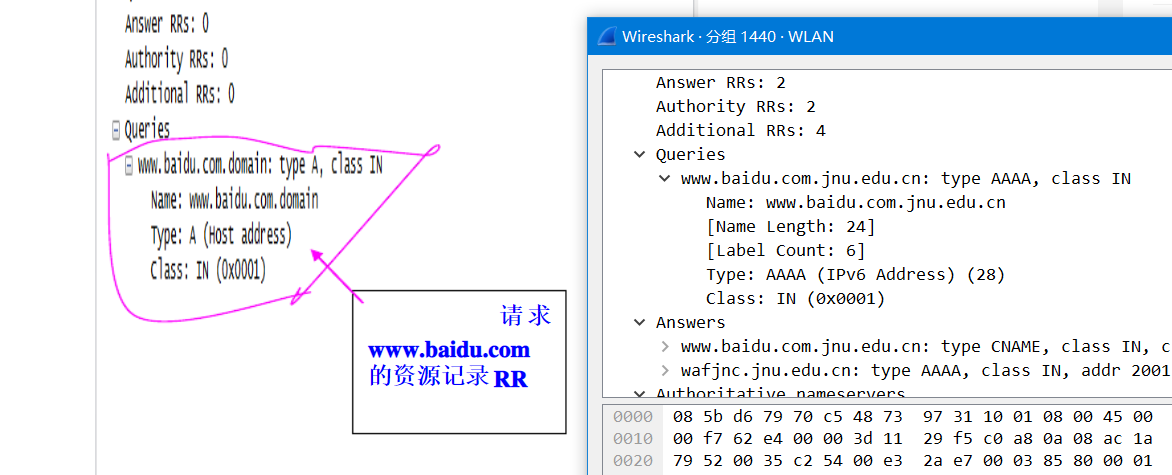
查阅百度，我们可以得知部分关键信息



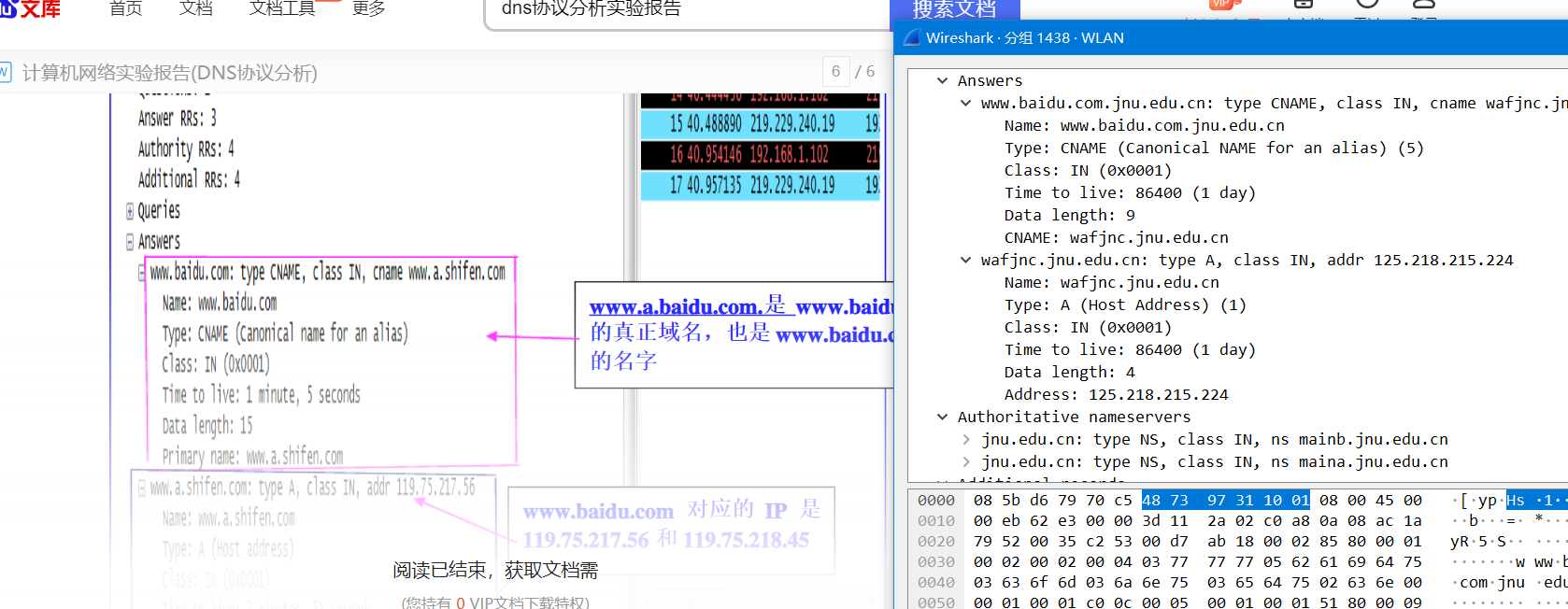
以上则是第一帧信息，我们可以得知第一帧是发送给本地dns服务器的反向查询，目的是获得本地dns服务器的名字。



可见，第二帧是返回的相应帧



根据百度的对照，我们得知，第三帧是客户端发给本地dns服务器的dns请求报文，用于请求百度的对应ip地址。

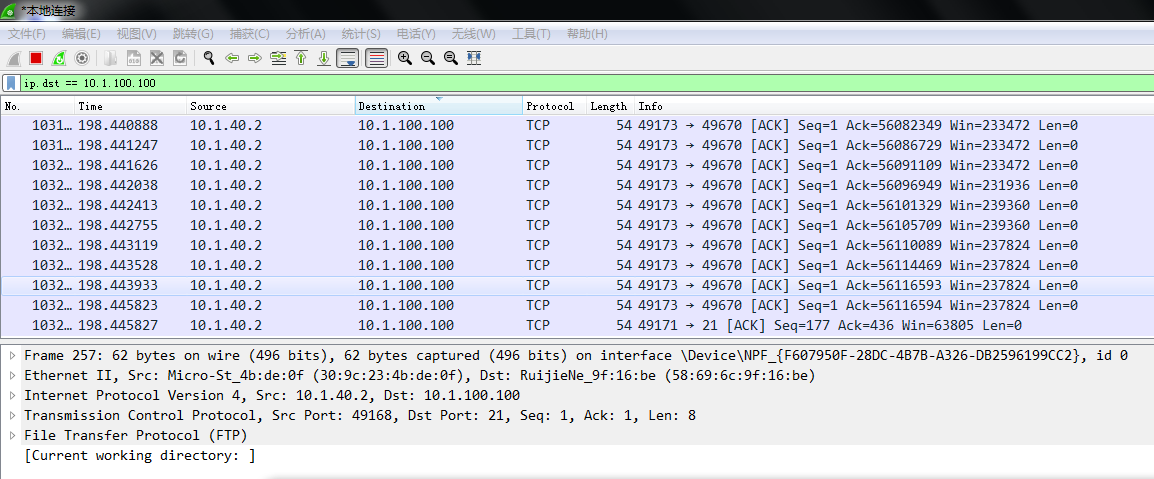
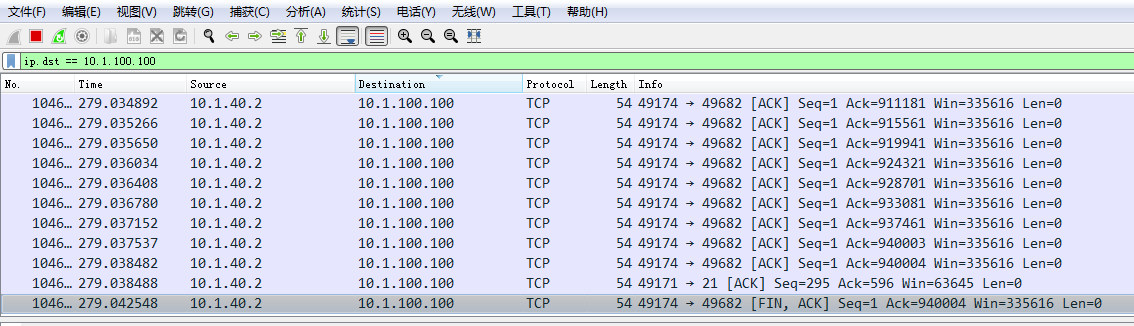


同样根据查阅百度资料对比，我们可以得知第四帧的作用是本地dns服务器发给客户端的报文，同时包含百度真正域名和名字。

**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。

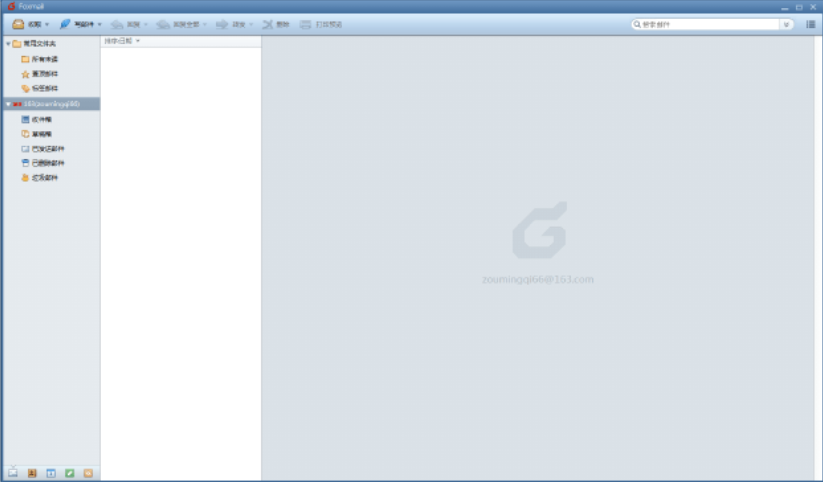
ftp

键入ftp：//10.1.100.100，下载一个文件，同时嗅探，得出如上信息，分析得出ftp协议使用时保持网络畅通，如上将文件逐步传送。

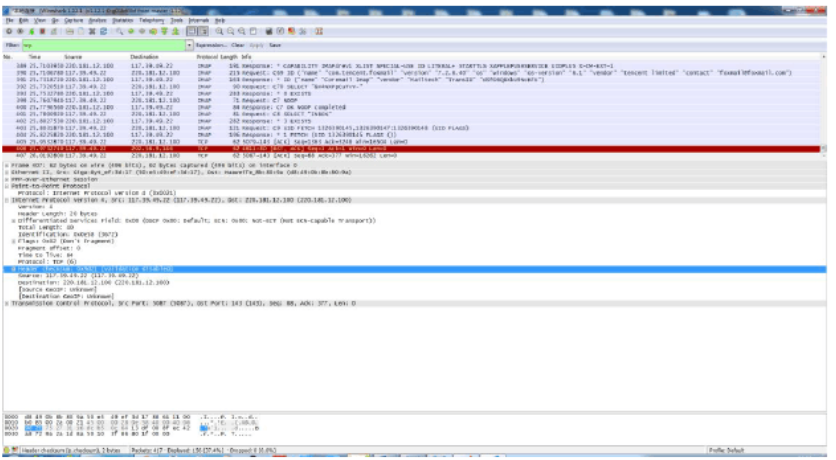
**四、 SMTP和POP协议分析**

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。

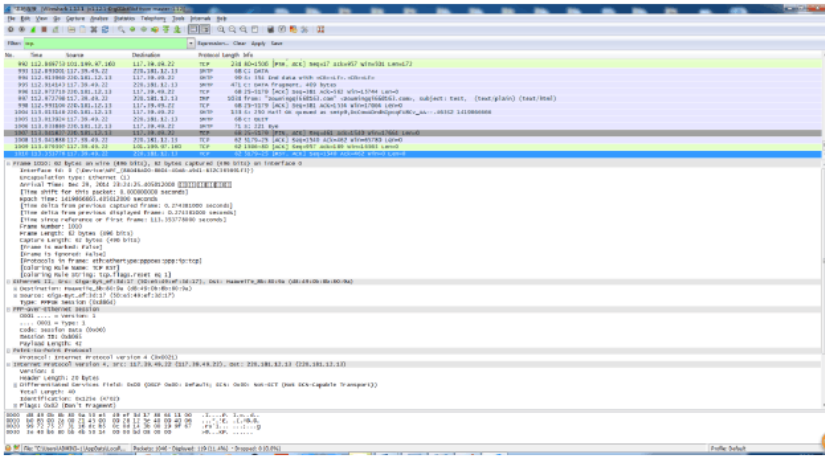
创建foxmail如下

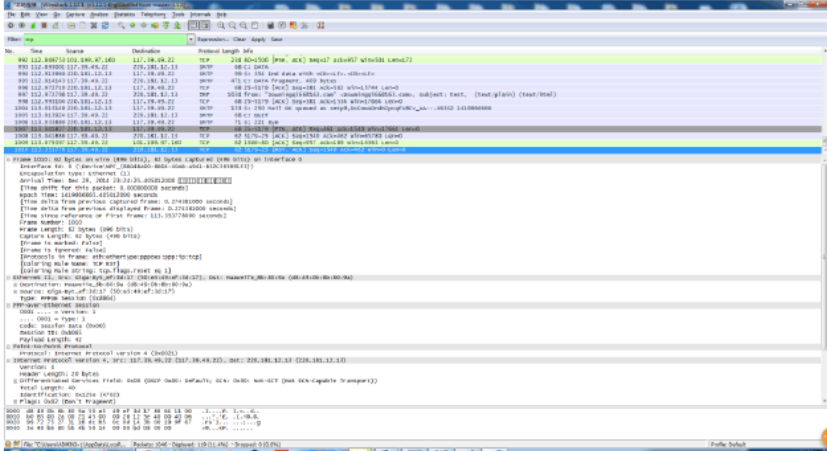


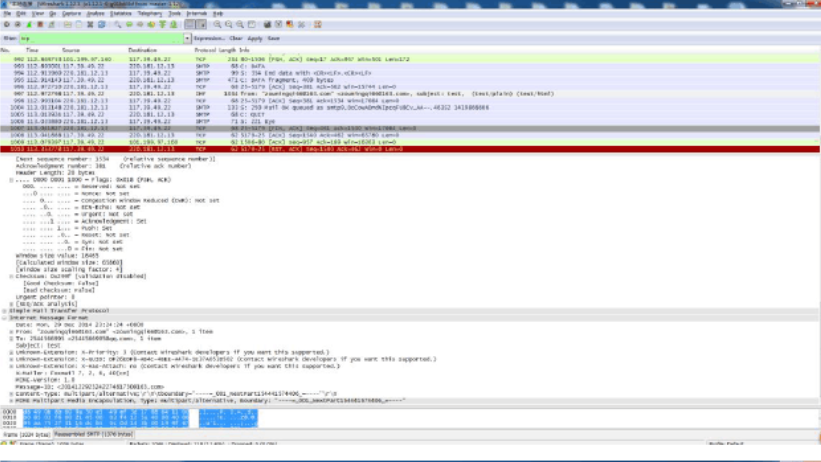
使用wireshark嗅探。

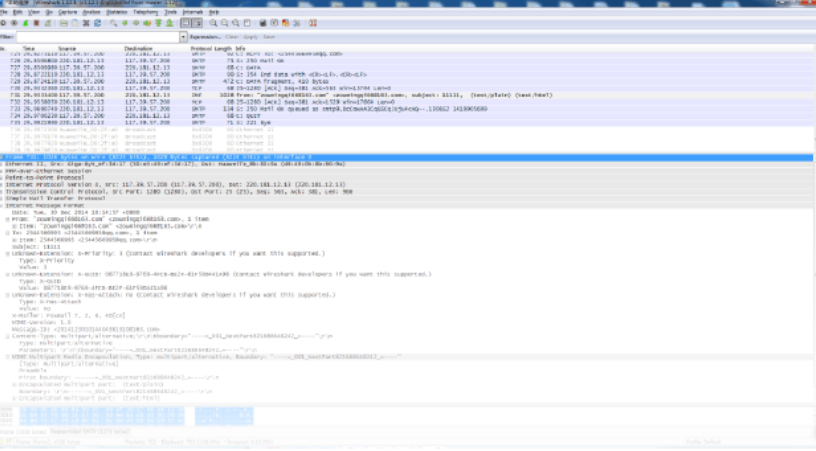


发送一封邮件









由图可知邮件的具体内容