**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

学生姓名 孙靖 学号 2019053750

学院 智能科学与工程/人工智能产业学院 系 专业 信息安全

实验时间 年 月 日 上 午～ 月 日 下 午

1. **实验目的**

1.了解WWW 、 DNS服务、FTP服务、SMTP的作用和原理；

2.掌握Windows下WWW 、 DNS、FTP服务的安装及相关配置方法；

3.了解建立网站的基本知识。

4.学会使用wireshark分析HTTP、FTP、SMTP和DNS协议的工作过程，加深对协议的理解。

**二、实验内容**

1.安装WWW，建立WWW站点；并进行访问测试。

2.安装DNS服务器，并进行正向解析设置；设置实验中建立的WWW服务器域名或FTP域名。

3.测试DNS解析效果，通过域名的方式访问实验中建立的WWW服务器。

4.安装FTP服务器，建立FTP站点，并配置匿名用户访问目录及权限。

5.测试FTP站点，上传或下载一个或多个文件。

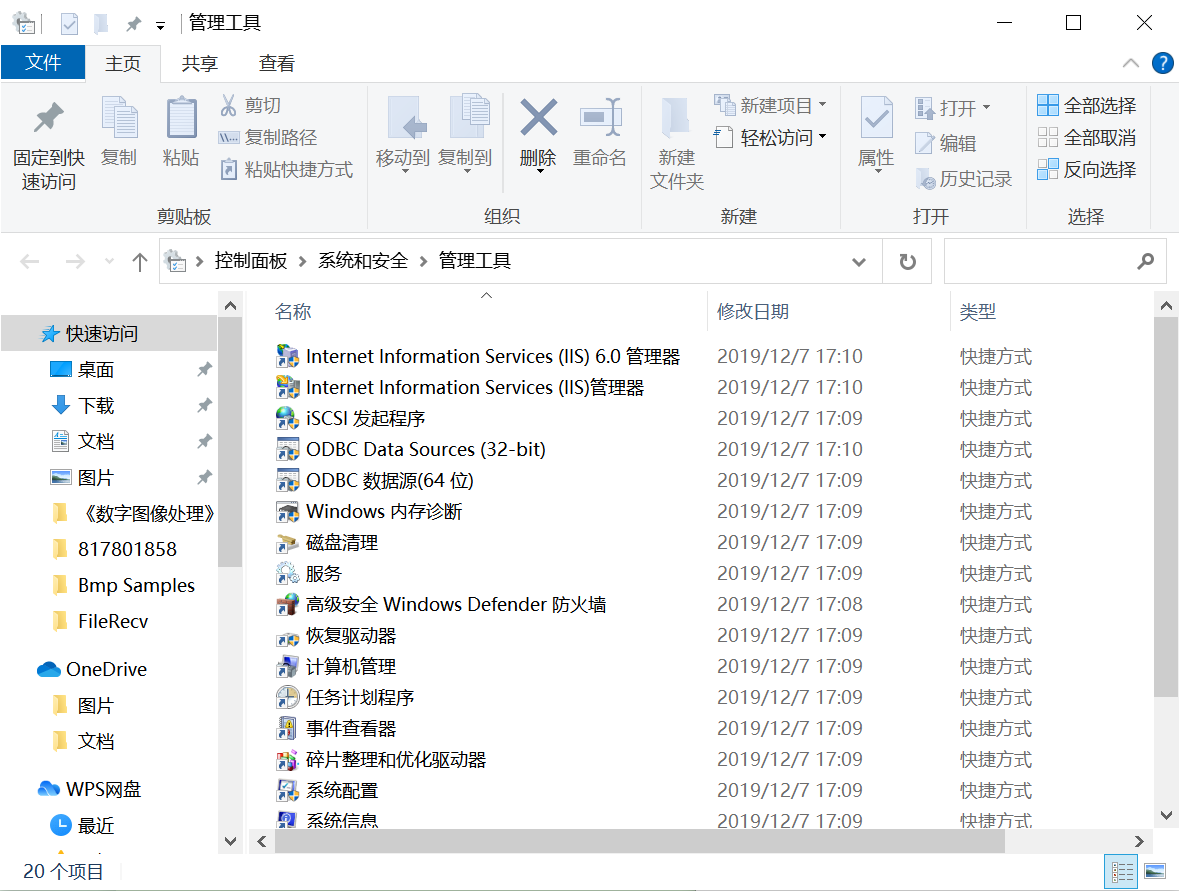
**三、实验设备**

局部网环境，计算机若干台。

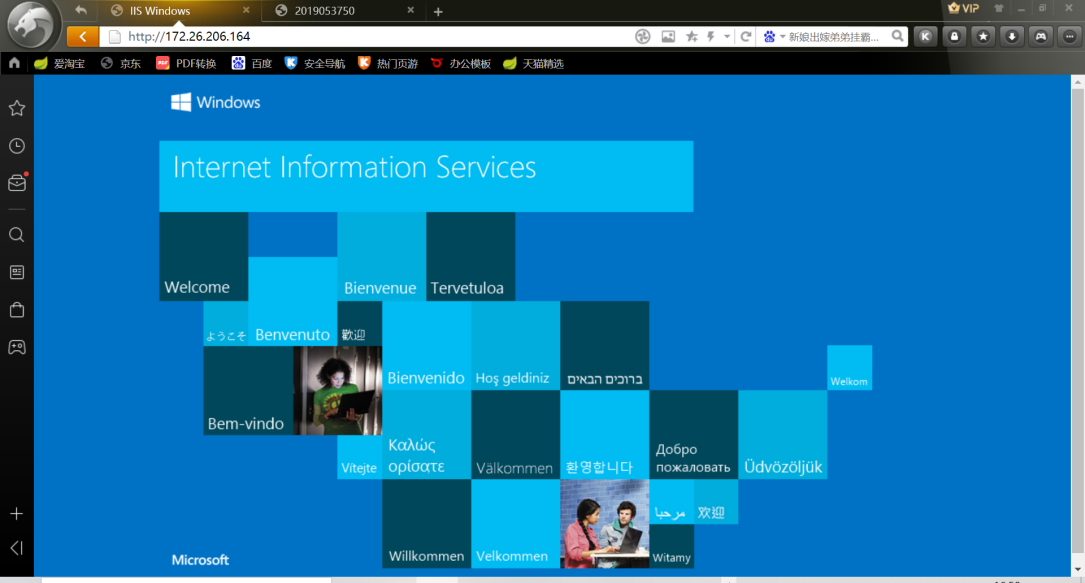
1. **实验步骤**
2. **、HTTP协议分析**

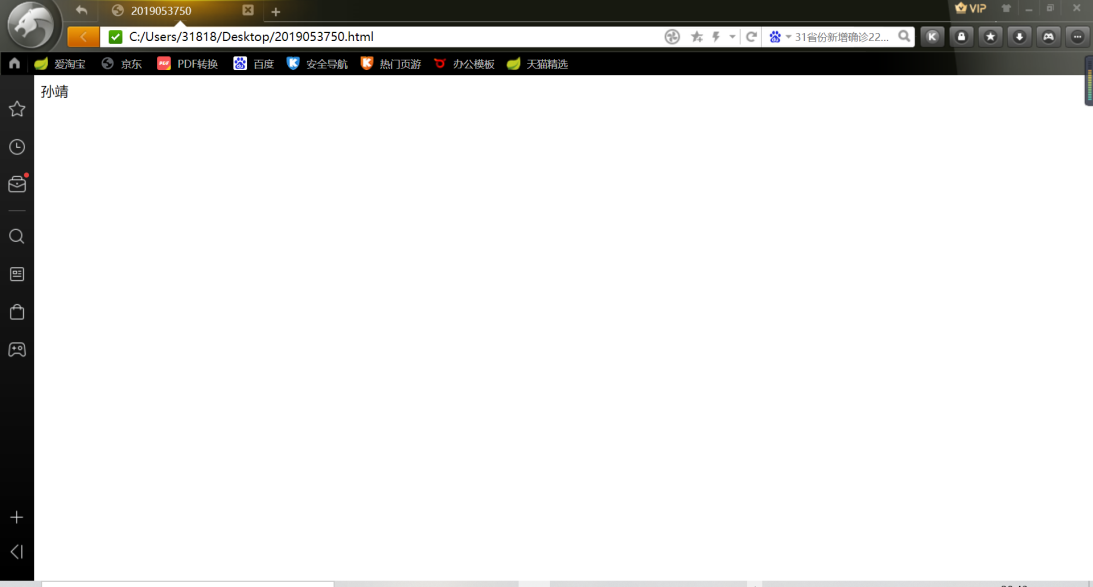
访问任意web站点，用wireshark分析HTTP协议的工作过程和HTTP协议格式。

1.安装IIS6.0



1. 使用IIS的默认站点

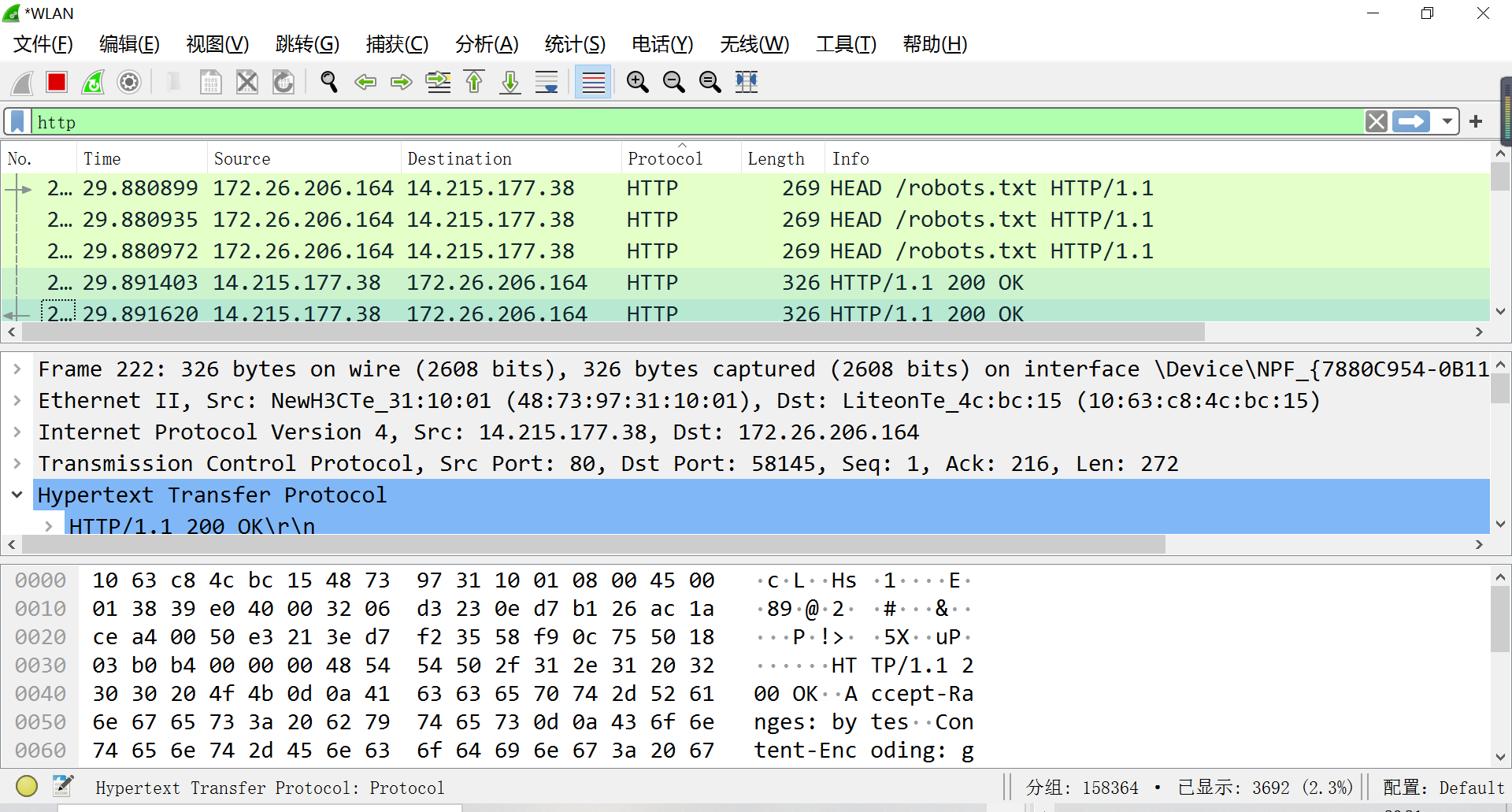


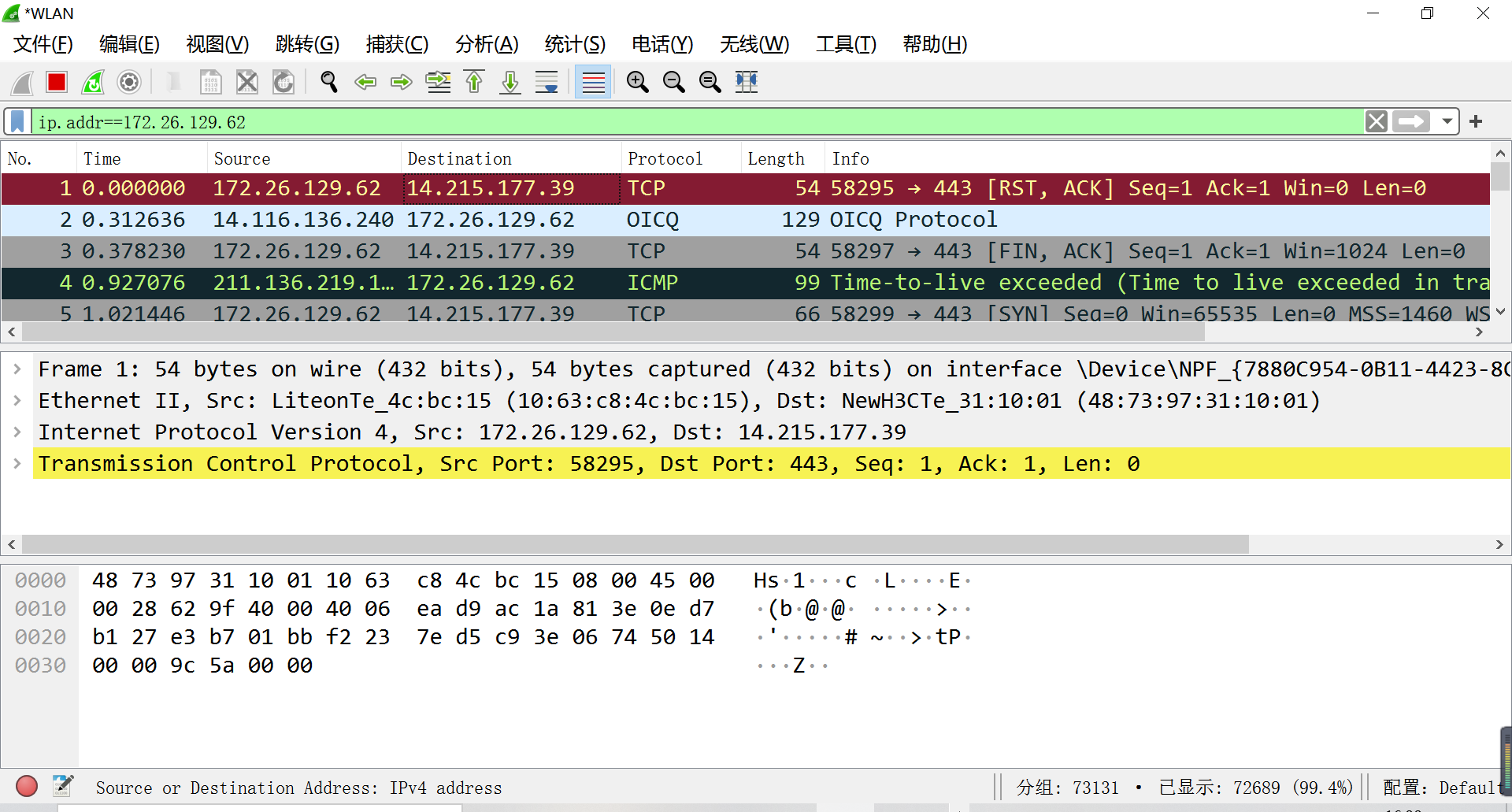


Web服务器安装成功，WWW服务运行正常。

1. 添加新的Web站点

4.访问建立的web站点，用wireshark分析网站的访问过程。

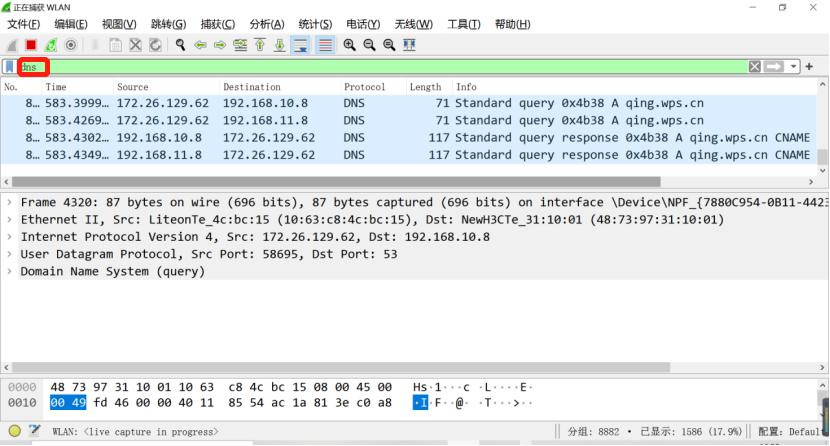




**（二）DNS协议分析**

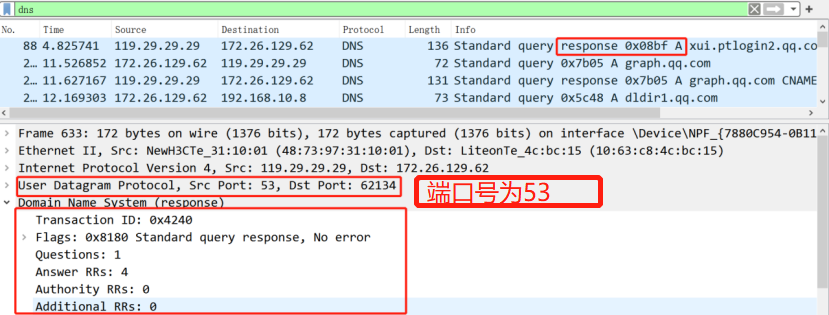
通过域名访问网站，用wireshark捕获DNS数据包，并分析DNS工作过程和DNS格式。

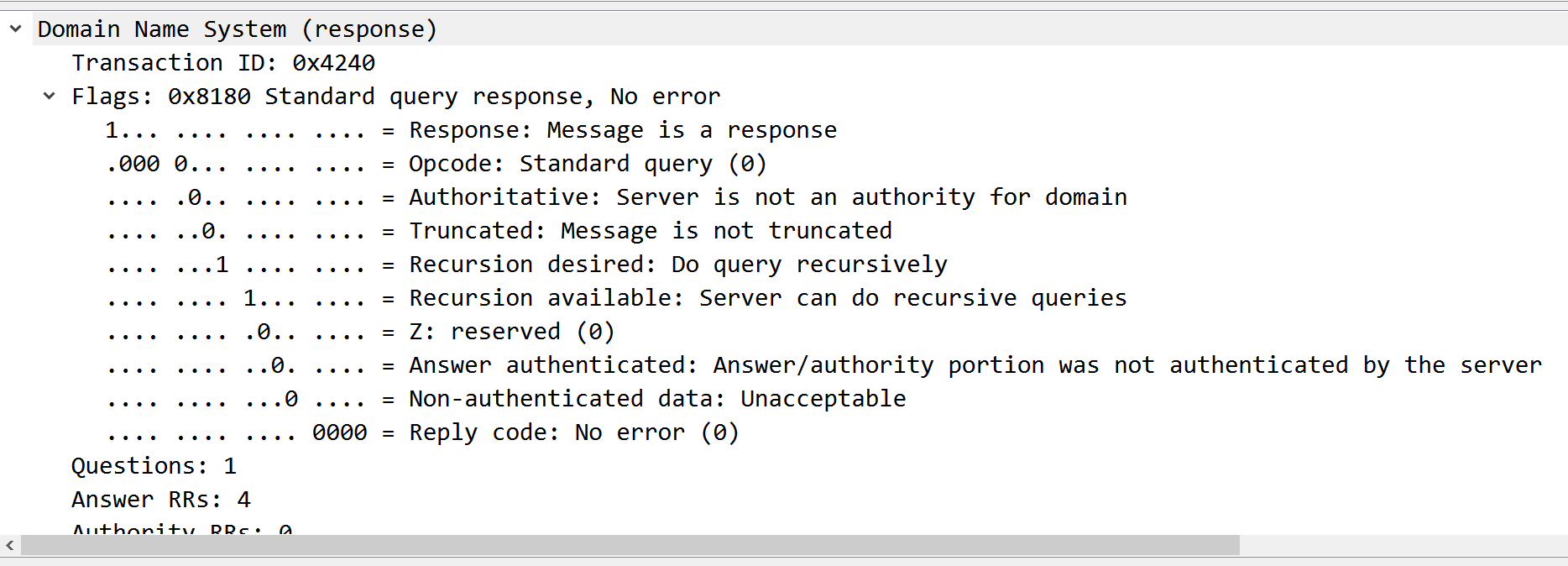
抓取数据

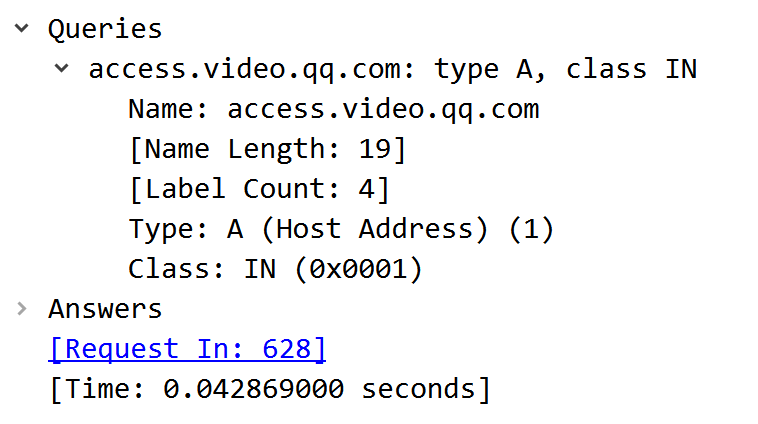




DNS报文数据





问题查询部分

标志（Flags）：DNS 报文中的标志字段。

问题计数（Questions）：DNS 查询请求的数目。

回答资源记录数（Answers RRs）：DNS 响应的数目。

权威名称服务器计数（Authority RRs）：权威名称服务器的数目。

附加资源记录数（Additional RRs）：额外的记录数目（权威名称服务器对应 IP 地址的数目）。

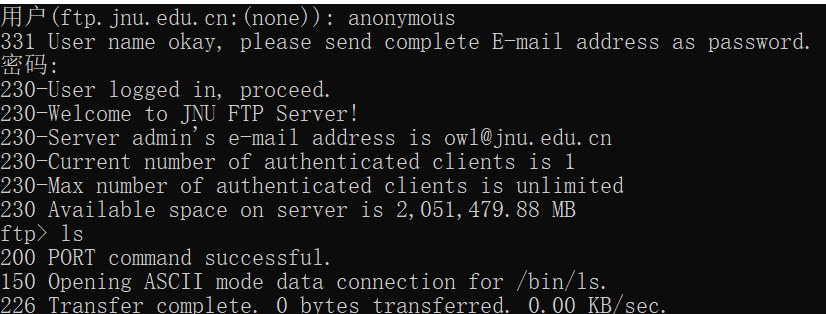
**（三）、FTP协议分析**

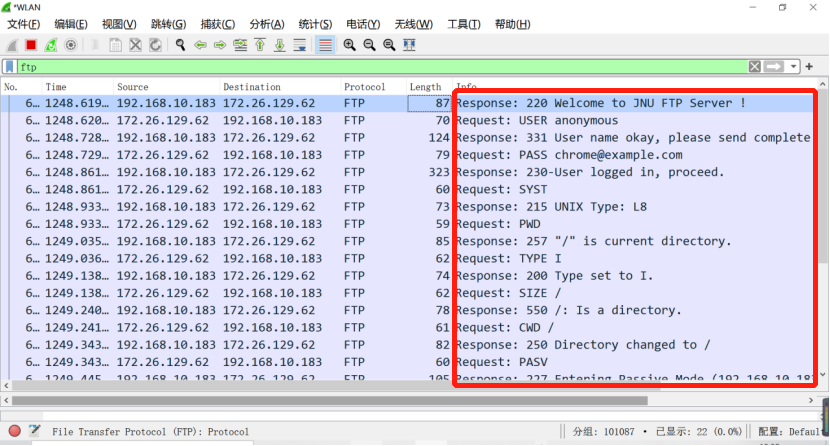
1.访问FTP服务器。如ftp://ftp.jnu.edu.cn



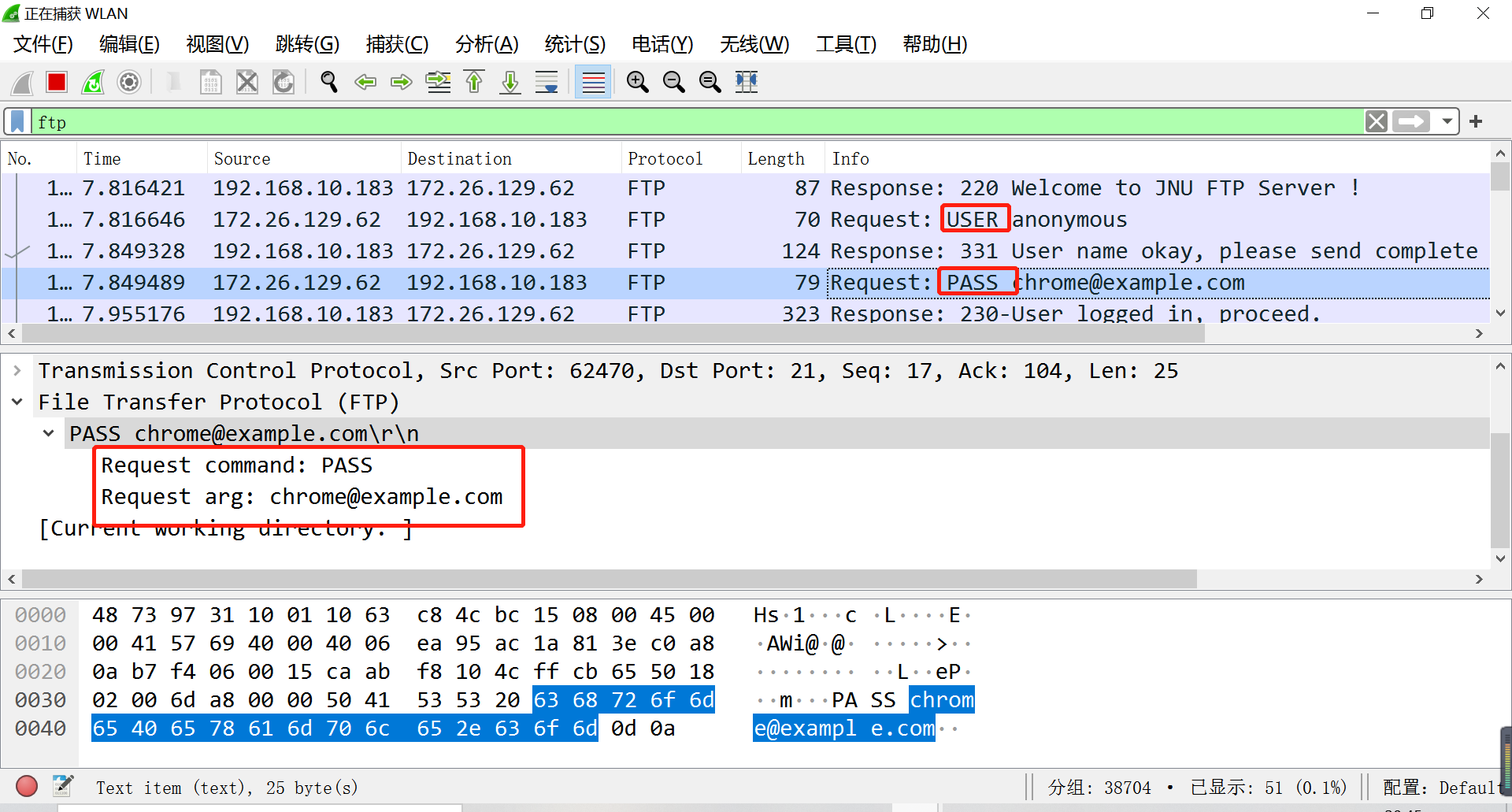
1. 用wireshark分析FTP的工作过程。

用Wireshark捕获到的数据包

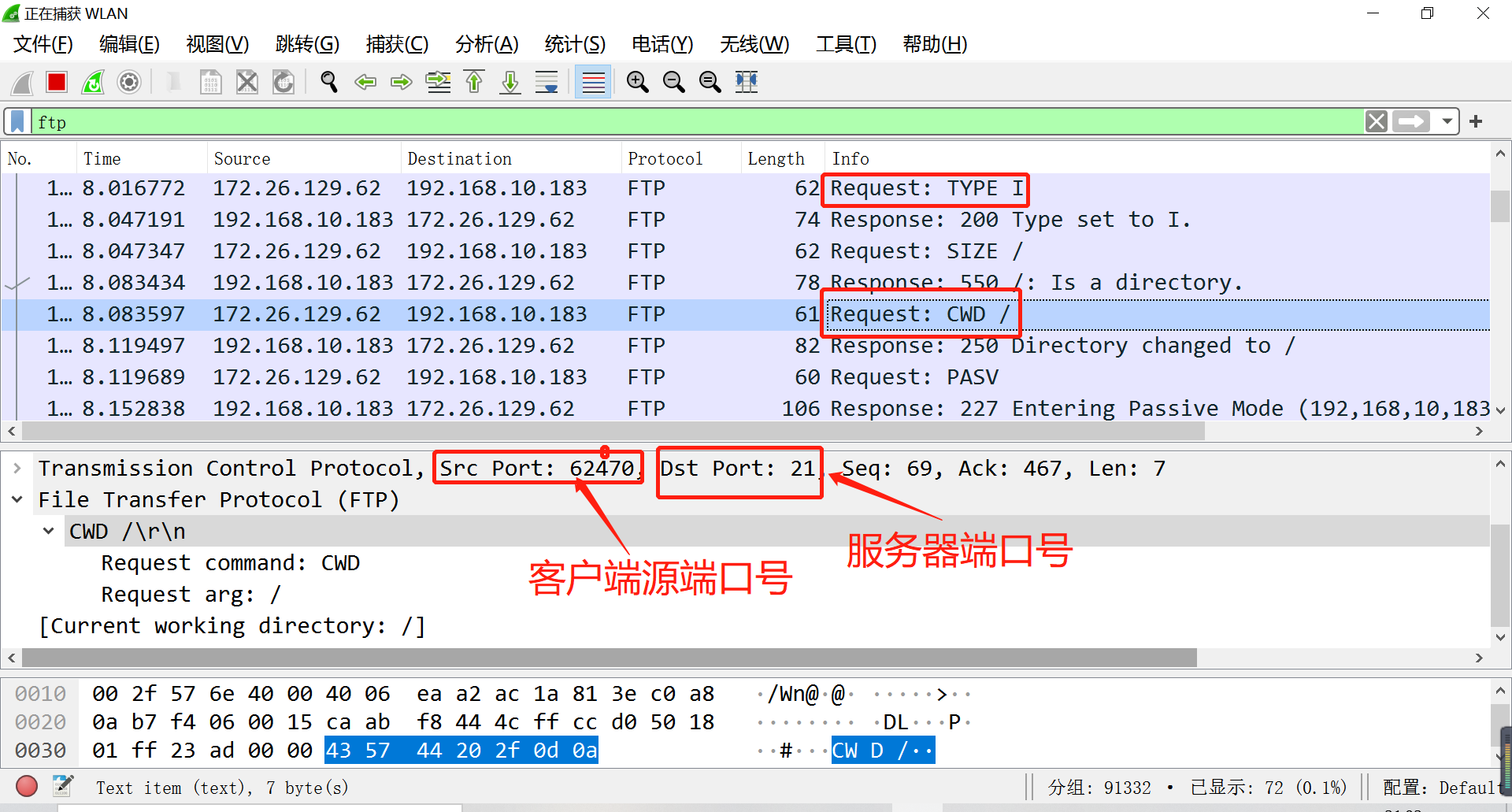




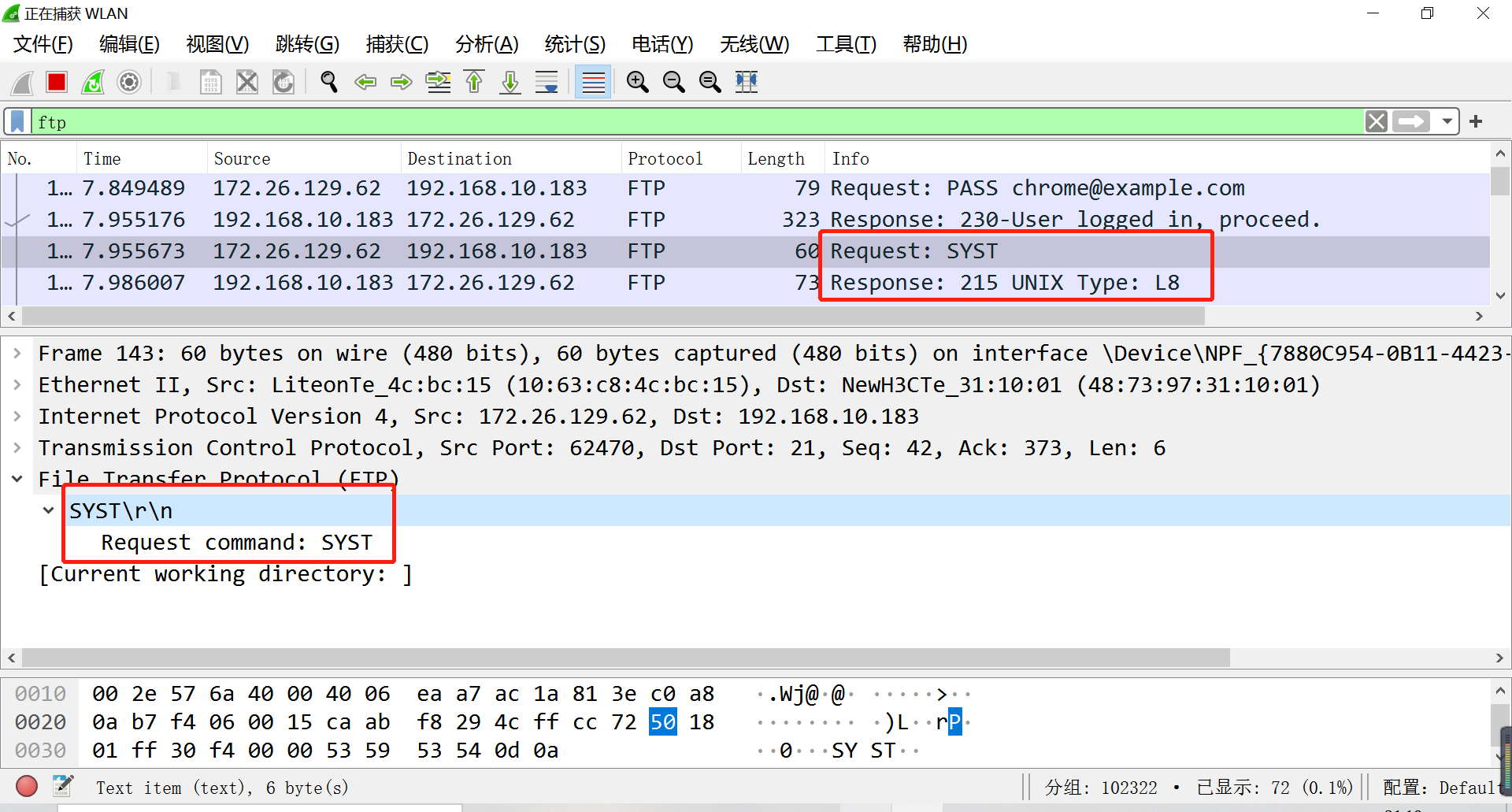
[图中显示数据包的Info列，在这里可以看到ftp传输的所有信息，因为FTP是明文形式传输数据包的，所有我们在InFo列里能看到登录FTP服务器的用户名、密码等。在上图中，登录FTP服务器的用户名为anonymous，密码为chrome@example.com。](mailto:图中显示数据包的Info列，在这里可以看到ftp传输的所有信息，因为FTP是明文形式传输数据包的，所有我们在InFo列里能看到登录FTP服务器的用户名、密码等。在上图中，登录FTP服务器的用户名为anonymous，密码为chrome@example.com。)



登录FTP服务器时，使用的控制命令是USER和PASS。根据这两个命令，可以看到登录的账号为anonymous，密码为chrome@example.com.

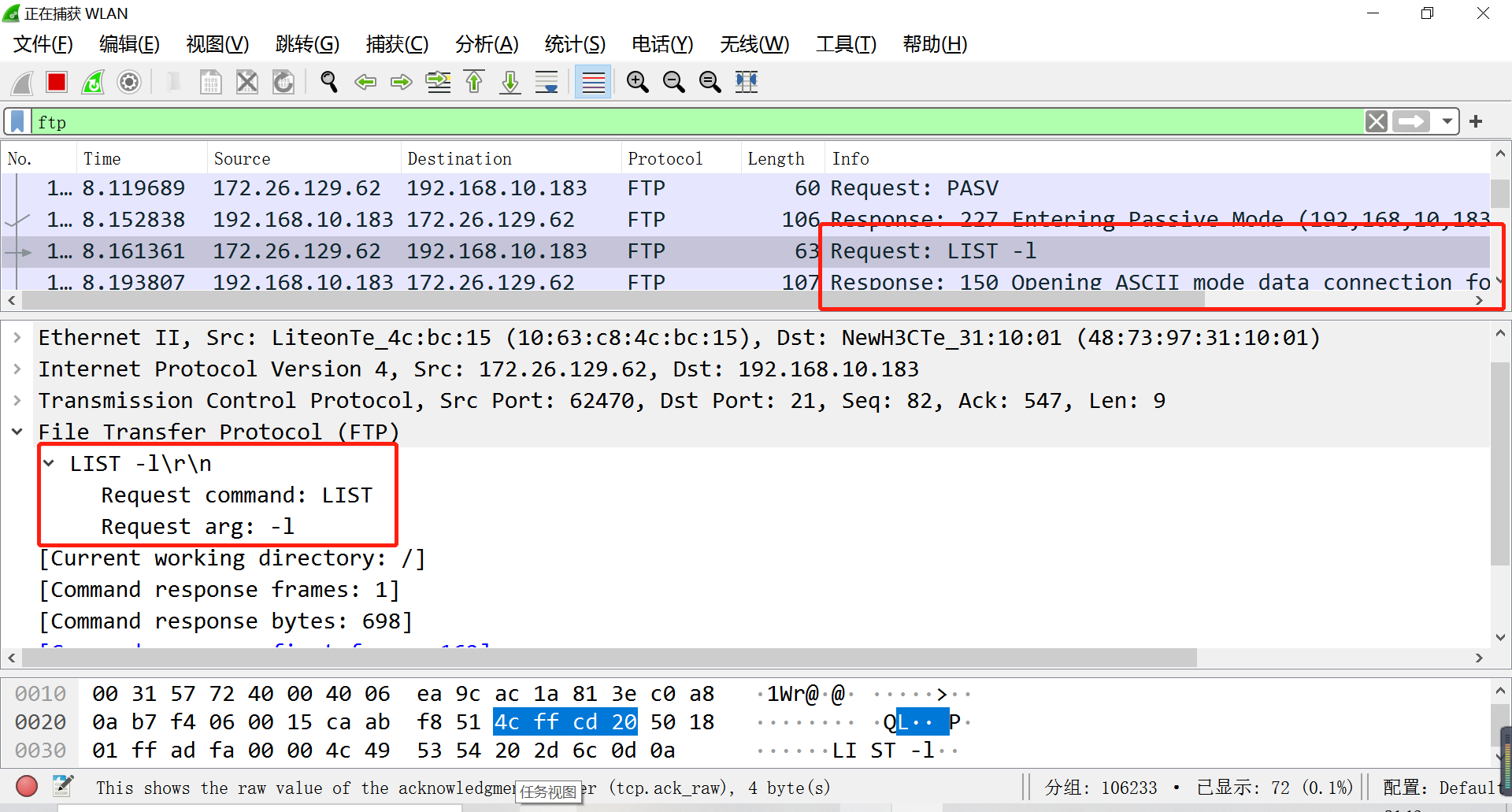


SYST



Response：服务器返回系统类型

LIST

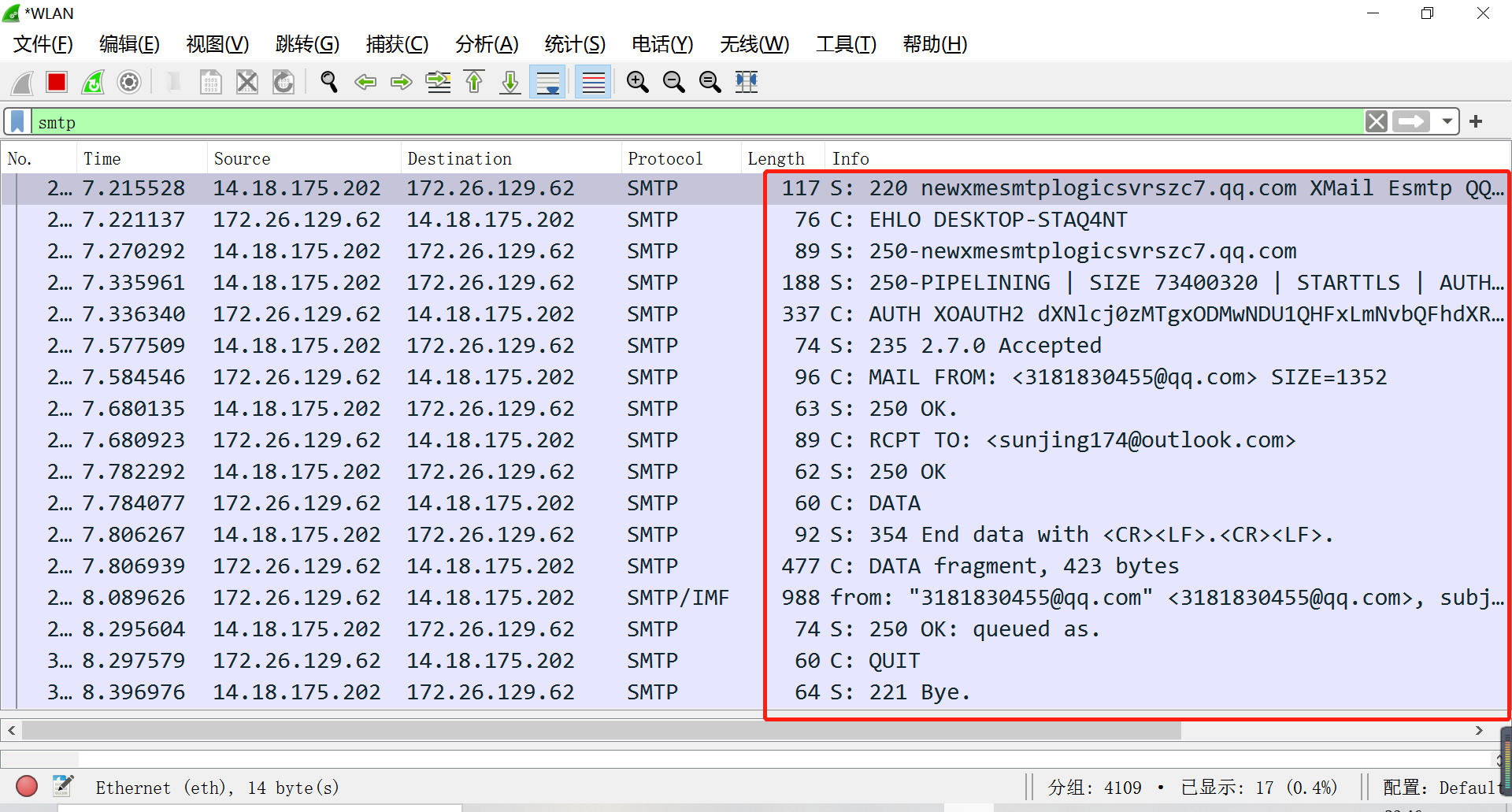


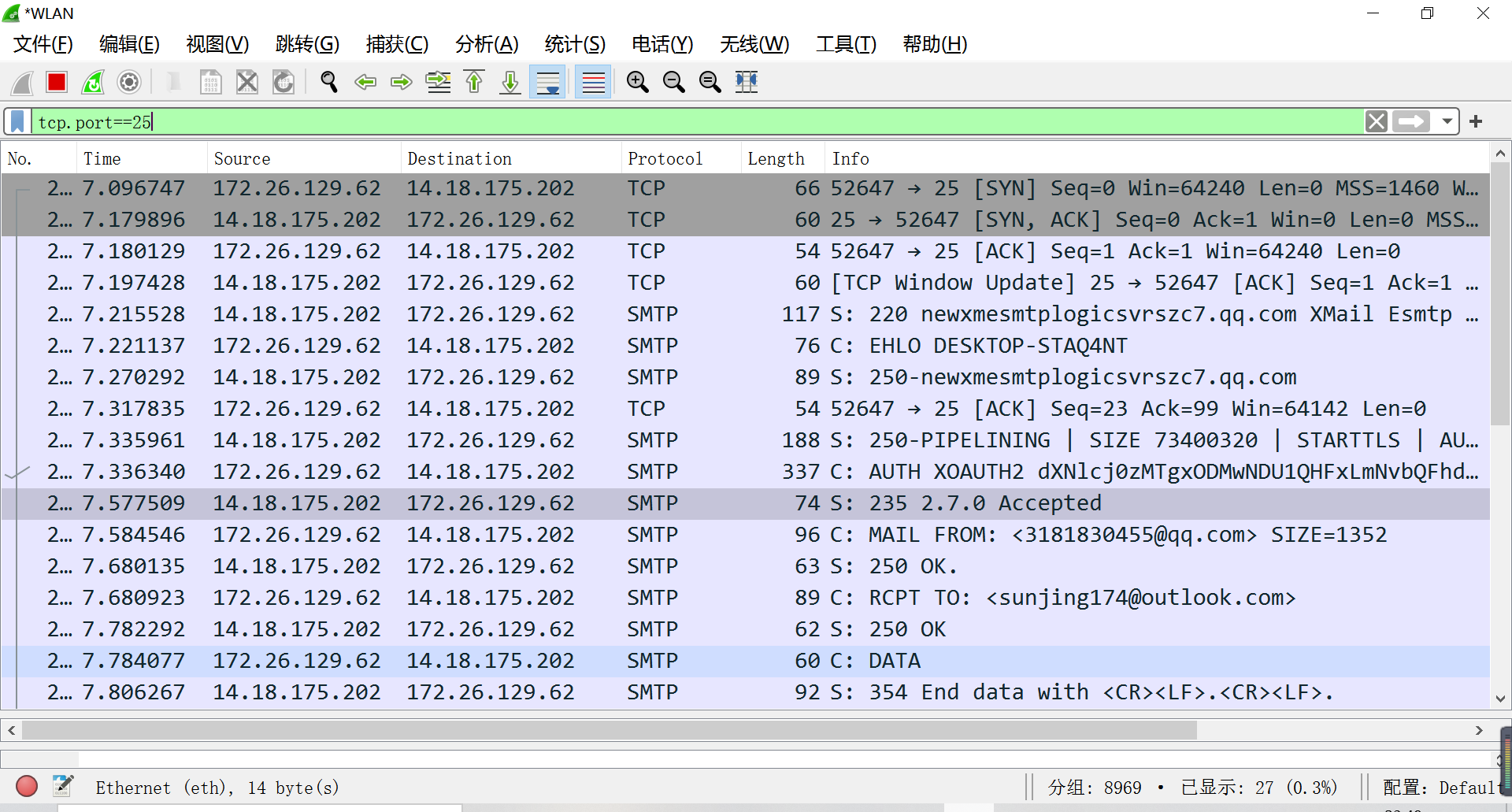
客户端开始发送LIST命令查询文件列表信息，服务器回复相应文件信息，并开始准备从数据连接发送文件。

**（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。

SMTP协议数据包如下：

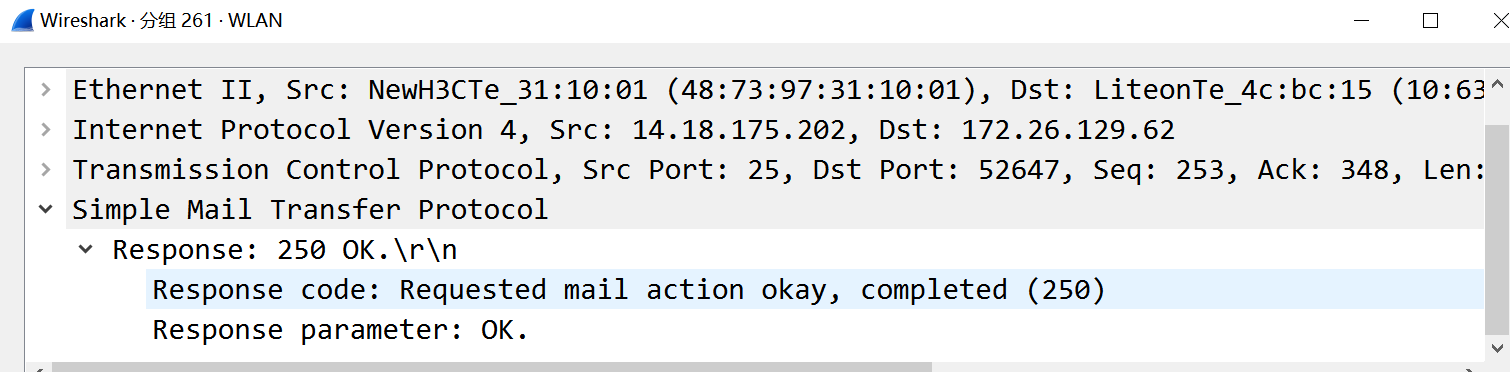




状态字220代表连接SMTP服务器成功



状态字250表示与服务器握手成功



用户登录命令

