数据通信和网络lab1 应逸雯12210159

• Run all the demos on your PC.

• Use Wireshark to capture and analyze the packets when running the demos, list the source IPs, source port numbers, destination IPs, destination port numbers and response’s status code of each connections.

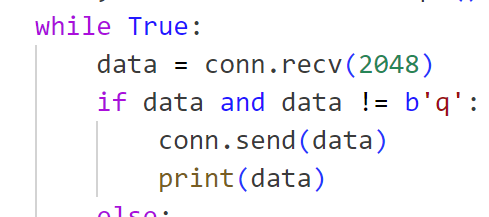
demo1.py

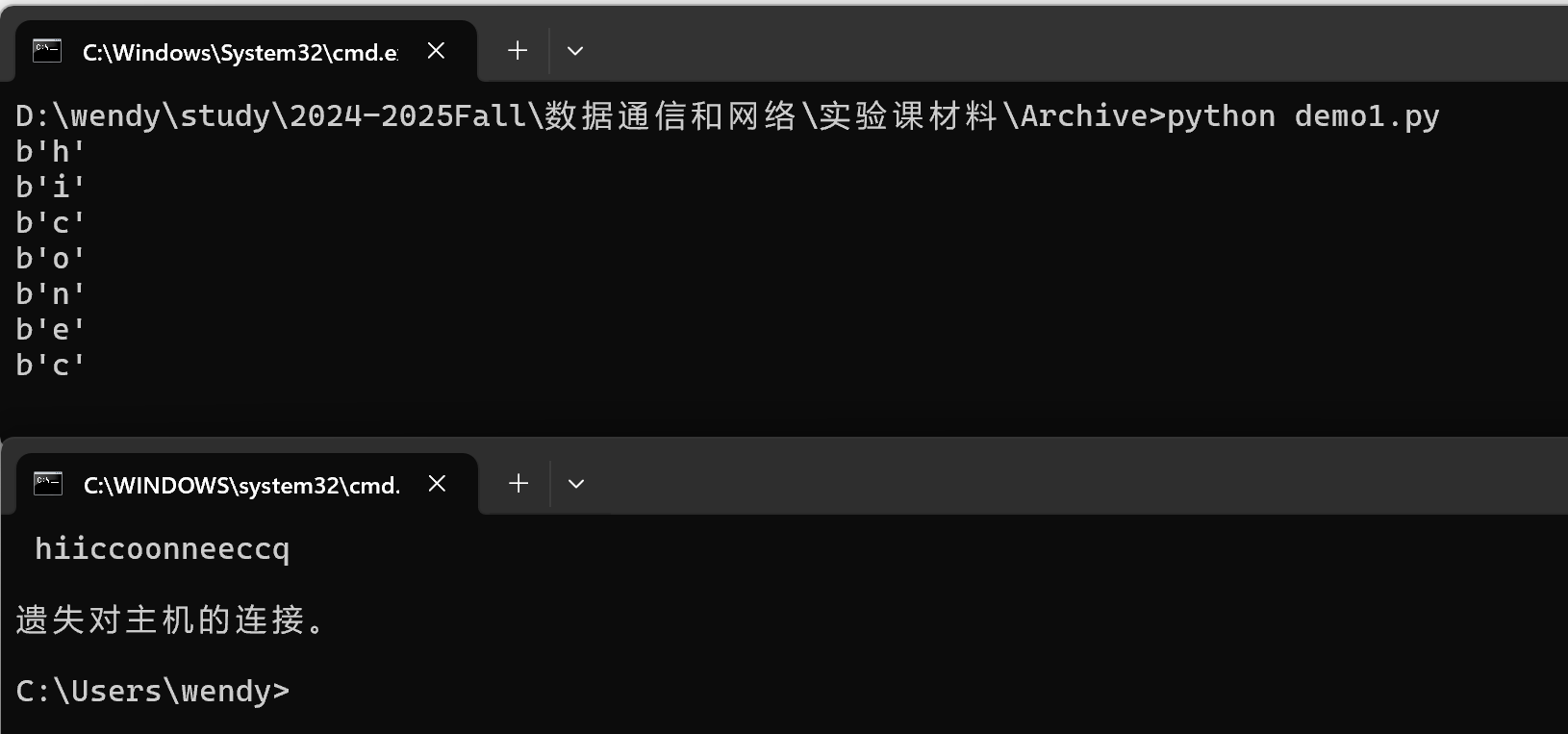
python demo1.py运行server

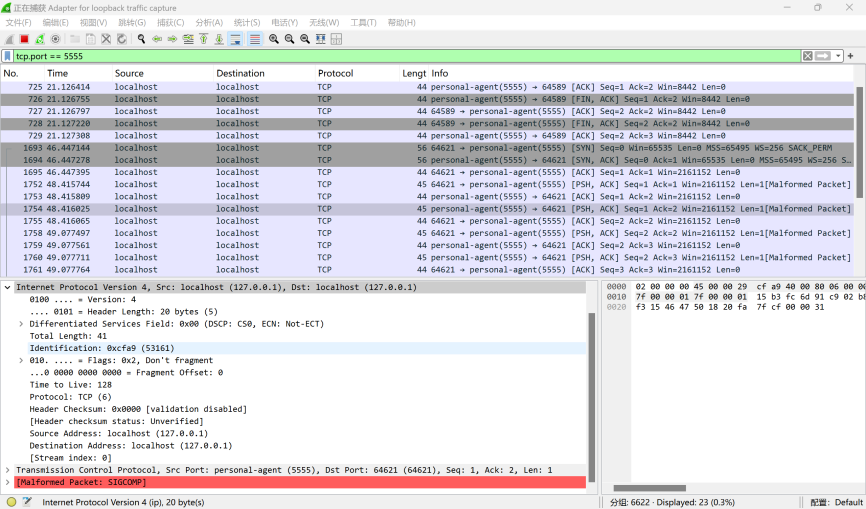
telnet 127.0.0.1 5555 运行client

client发送消息，server接收并打印、返回，client收到消息并打印；如遇到q则退出

（修改代码，退出条件为q，而非exit，以符合输入逻辑）







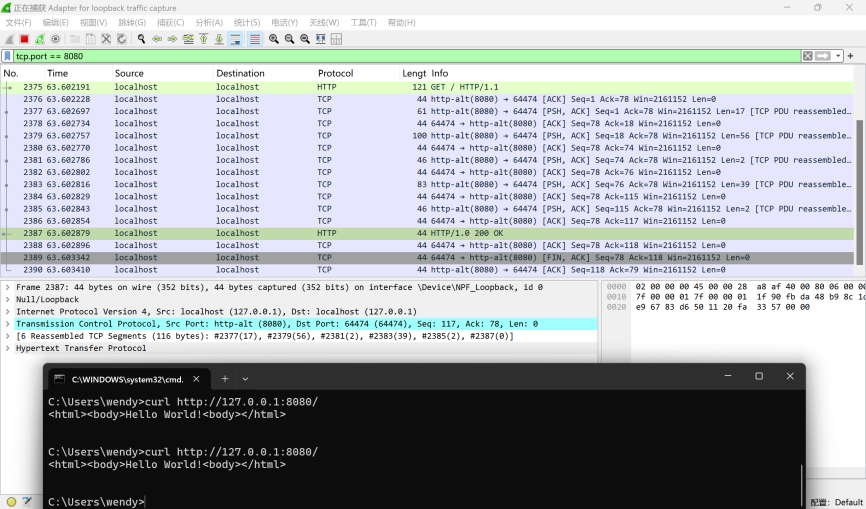
source ip: 127.0.0.1 source port: 5555，源于代码中的设定，ip地址127.0.0.1，端口5555

destination ip: 127.0.0.1 destination port: 64621，源于telnet中连接了127.0.0.1，随机分配端口为64621

demo2.py

python demo2.py启动服务器

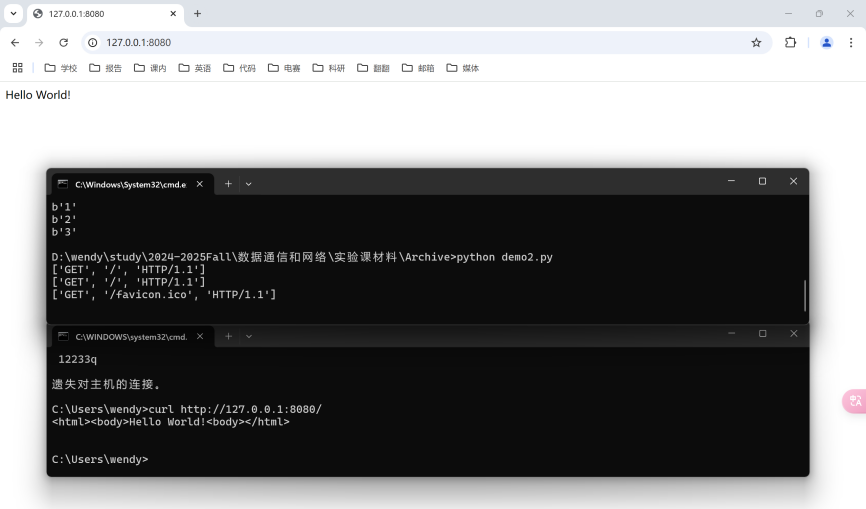
curl <http://127.0.0.1:8080/> 访问服务器



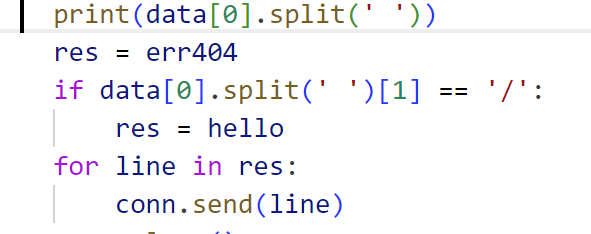
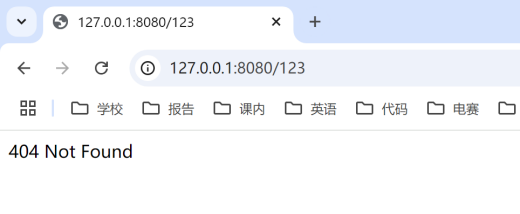
source ip: 127.0.0.1 source port: 8080（代码中设置）

destination ip: 127.0.0.1 destination port 64474（浏览器访问时ip为127.0.01，随机分配端口）

在浏览器中输入 <http://127.0.0.1:8080/> 访问服务器，符合解析地址“/”，正常返回Hello World!



在浏览器中输入 http://127.0.0.1:8080/123测试404错误，因为8080/123的地址不是解析到只有“/”，根据代码，会返回err404的信息。



Capture DNS query sent from your computer

– Using capture filter udp port 53

– Using display filter (any domain filter is ok)

Try to catch and explain a complete DNS query flow via Wireshark

Try to catch an authoritative RR response

在首页选择自己定义的捕获过滤器“udp”，其中内容为“udp port 53”

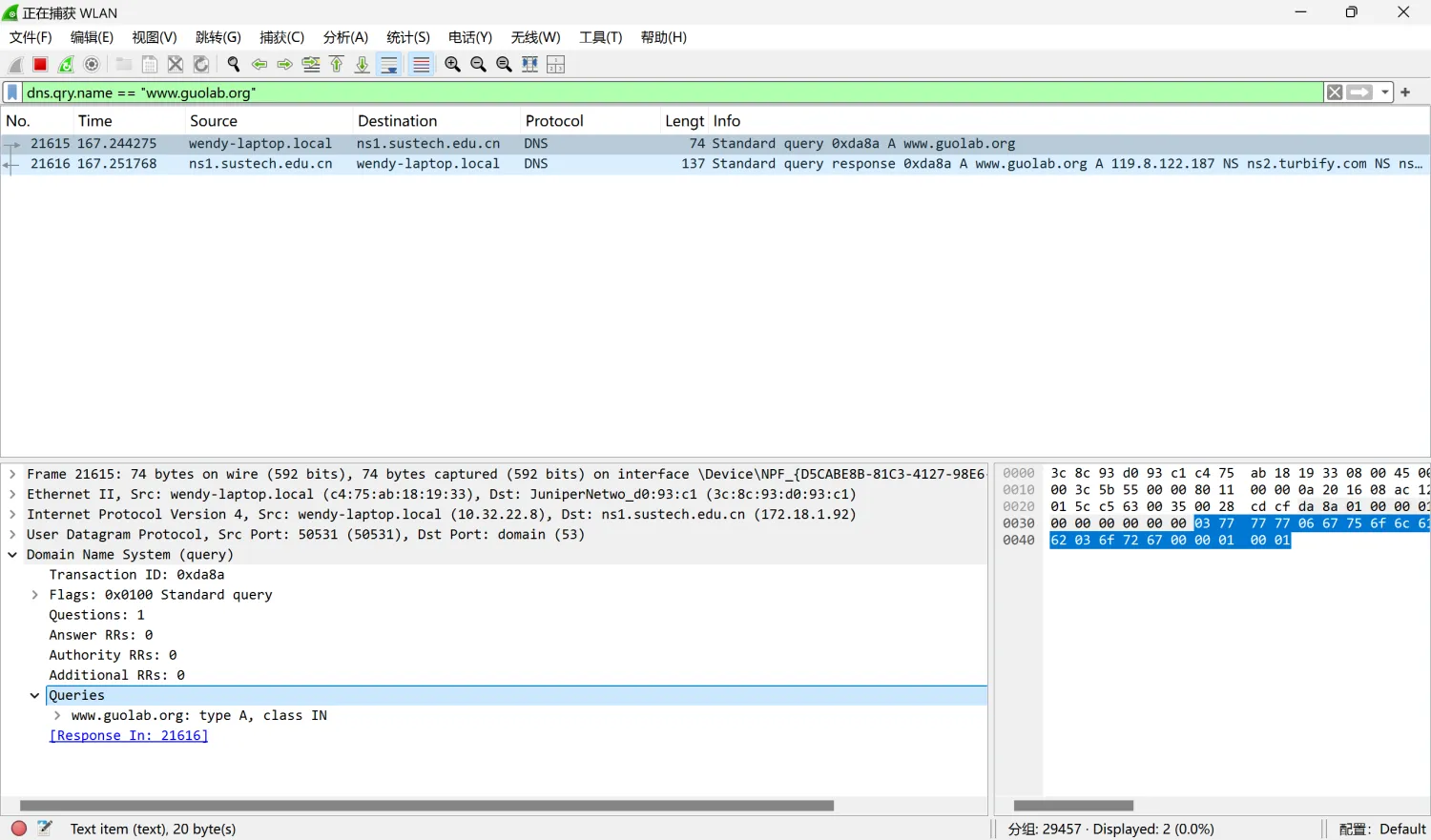
开始捕获，运行浏览器页面。

捕获完成后设置显示过滤器“dns.qry.name == “www.guolab.org””

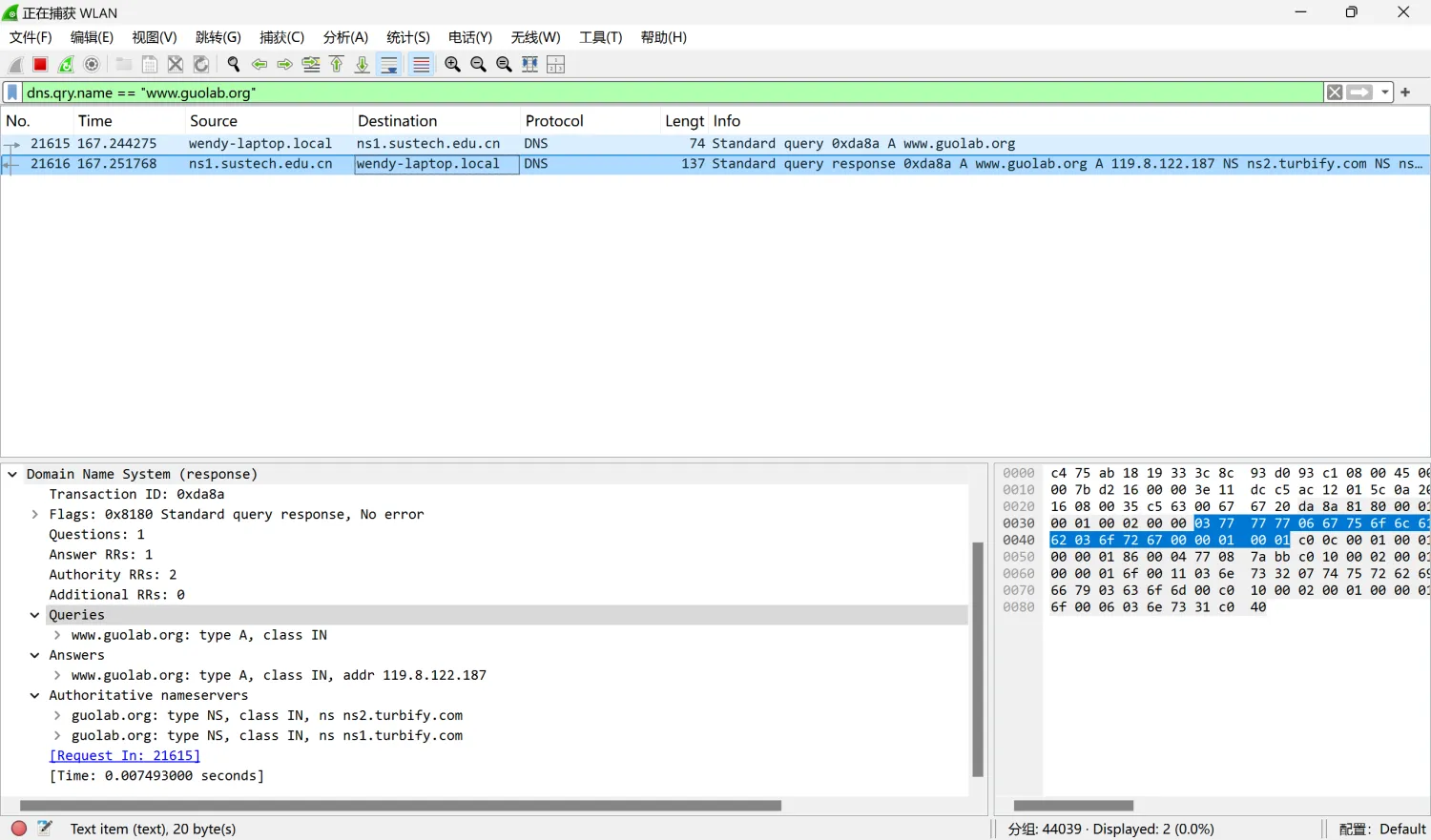
分析捕获结果，可以看到Query Name：请求的域名，Query Type：查询类型（如 A，表示IP地址），Answer Section：包含域名的IP地址或其他信息。

要捕获权威应答，可以观察 DNS 响应中的字段 Authoritative，如果该字段为 1，说明该应答是从权威DNS服务器返回的。

客户向DNS服务器发送请求，查询某个域名的ip地址。



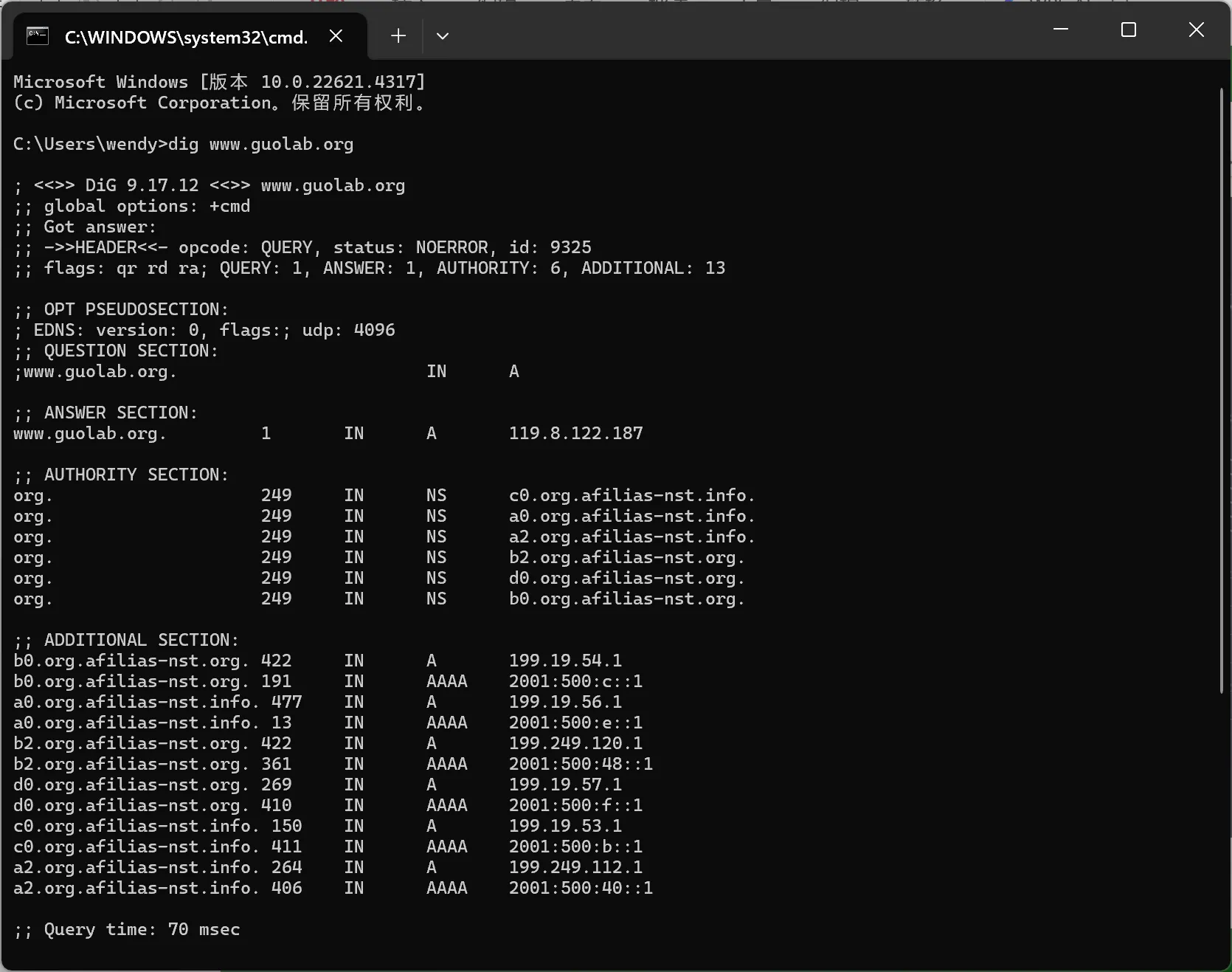
DNS服务器返回应答，包含域名的ip地址。

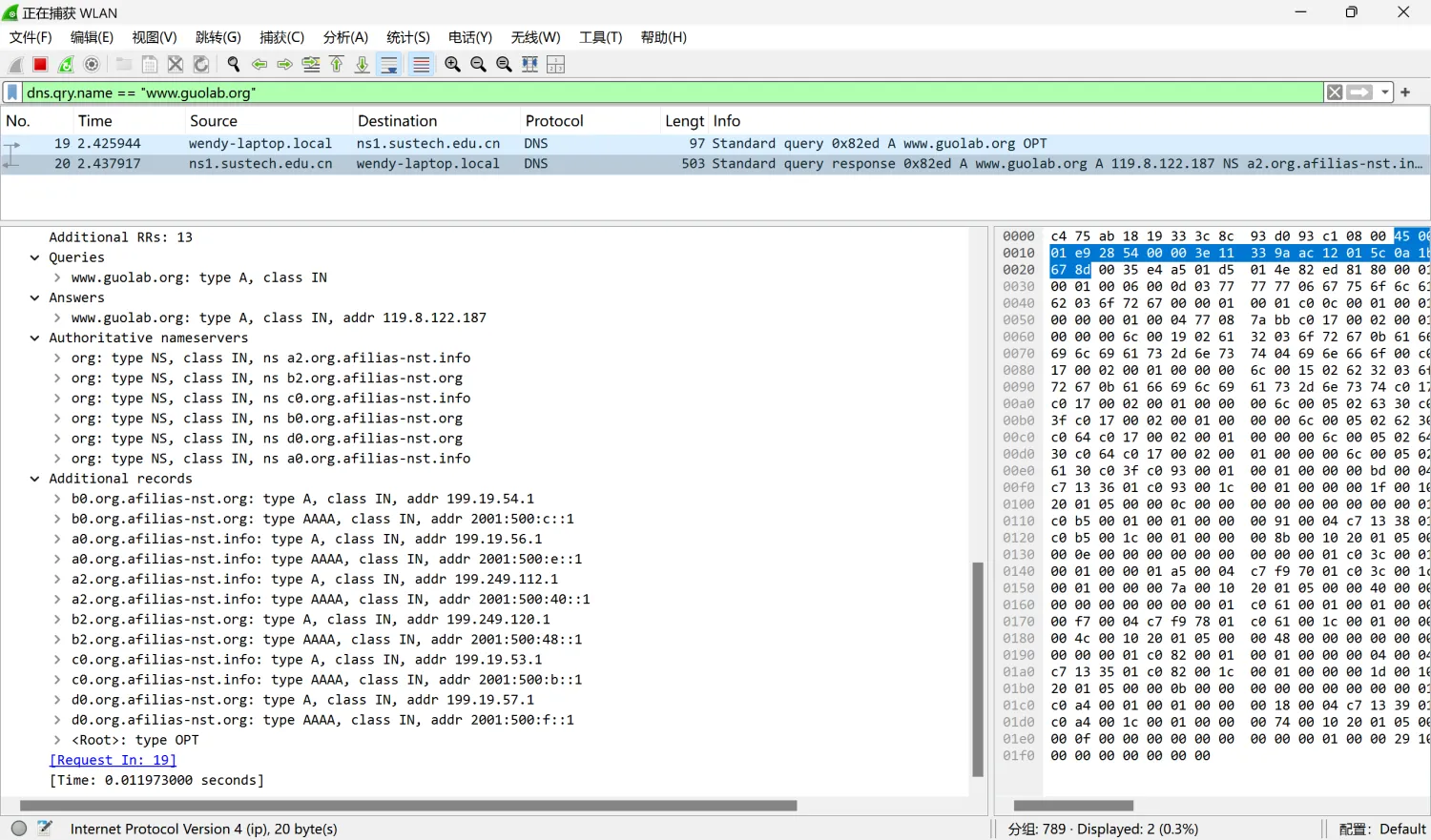


1. DNS查询包（Packet No. 21615）  
   Source: wendy-laptop.local (客户端)  
   Destination: ns1.sustech.edu.cn (本地DNS服务器)  
   Protocol: DNS (使用UDP端口53)  
   Query: 查询 www.guolab.org 的 A 记录，即请求该域名对应的IPv4地址。  
   Transaction ID: 0xda8a8（标识DNS请求与响应的对应关系）  
   Questions: 1 个查询请求，查询的域名为 www.guolab.org，查询类型为 A 记录，类为 IN（互联网）。
2. DNS响应包（Packet No. 21616）  
   Source: ns1.sustech.edu.cn (本地DNS服务器)  
   Destination: wendy-laptop.local (客户端)  
   Protocol: DNS (使用UDP端口53)  
   Response: 包含 www.guolab.org 域名的 A 记录和权威记录。  
   Transaction ID: 0xda8a8（与请求包的ID匹配）  
   Flags: 0x8180，表明这是一个标准查询响应且无错误。  
   Answer RRs: 1 个答案资源记录，返回 www.guolab.org 的 IPv4 地址为 119.8.122.187。  
   Authority RRs: 2 个权威资源记录，提供了权威DNS服务器信息，分别是 ns2.turbify.com 和 ns1.sustech.edu.cn。

客户端 (wendy-laptop.local) 向 DNS 服务器 (ns1.sustech.edu.cn) 发送了一个查询 www.guolab.org 的请求。DNS 服务器响应了请求，返回了 119.8.122.187 以及权威DNS服务器的信息。由于本地DNS服务器存储了地址，故能够直接返回，不会向根服务器等查询地址。

使用dig可以看到权威服务器。得到的IP地址等与wireshark抓包所见相同，但dig可以观察到，经过了6个权威DNS服务器，分别是c0.org.afilias-nst.info，a0.org.afilias-nst.info，a2.org.afilias-nst.info，b2.org.afilias-nst.org，d0.org.afilias-nst.org，b0.org.afilias-nst.org。





Implement your own SMTP client. Refer to the document we provide in BB.

Use Wireshark to capture SMTP packets.

将代码中fromAddress, toAddress, username, license\_key设置为自己的。

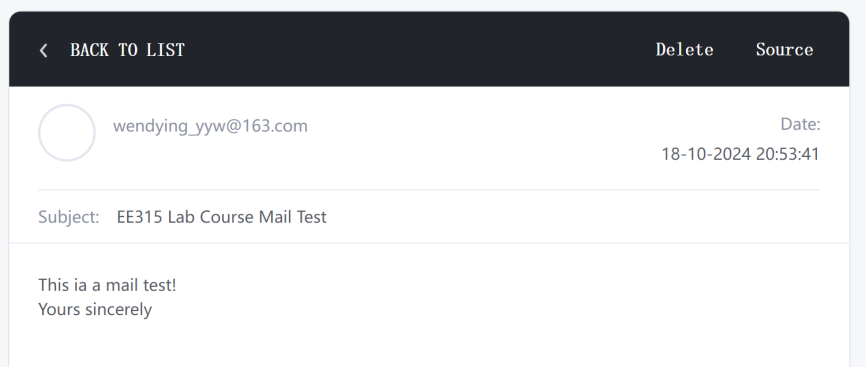
在163邮箱中打开SMTP服务。记录授权码。

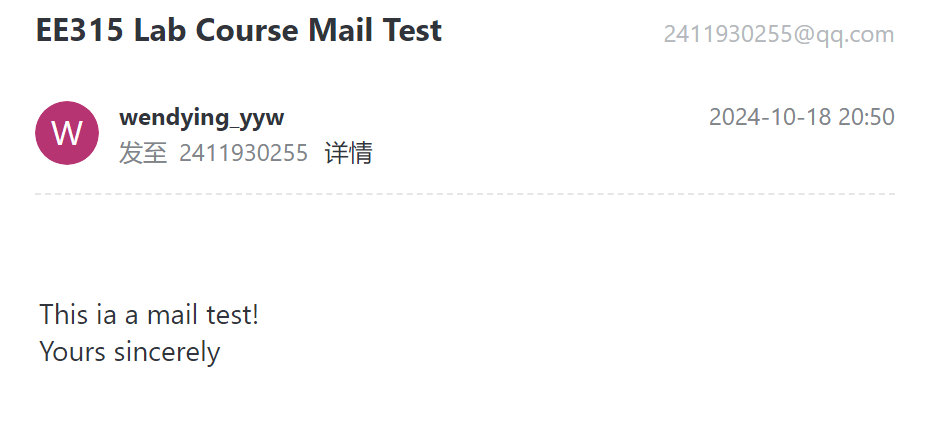
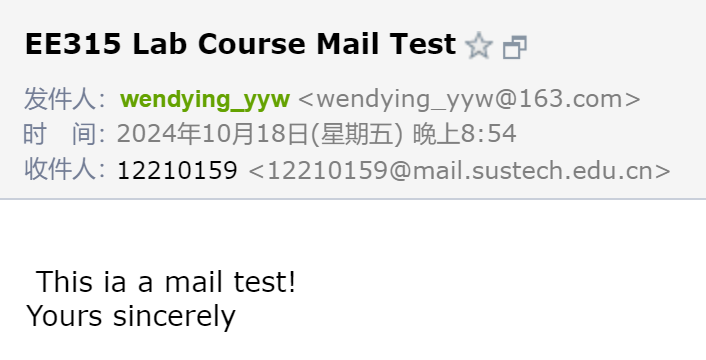
端口号等设置可以与其他客户端应用比照选择（使用了网易邮箱大师）。

命令行返回

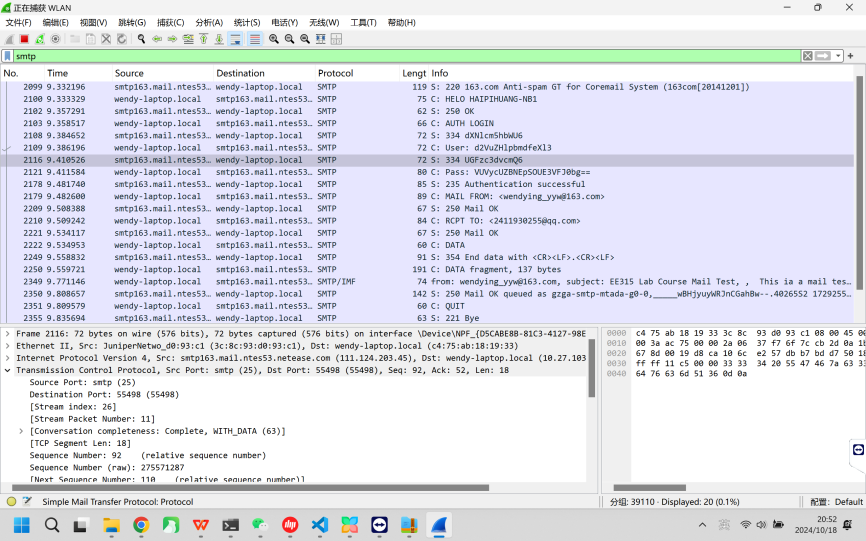


接收邮件方结果





wireshark抓包结果，记录了每次通信的状态码，如250,354,221。



修改邮件内容

