Assignment003-1

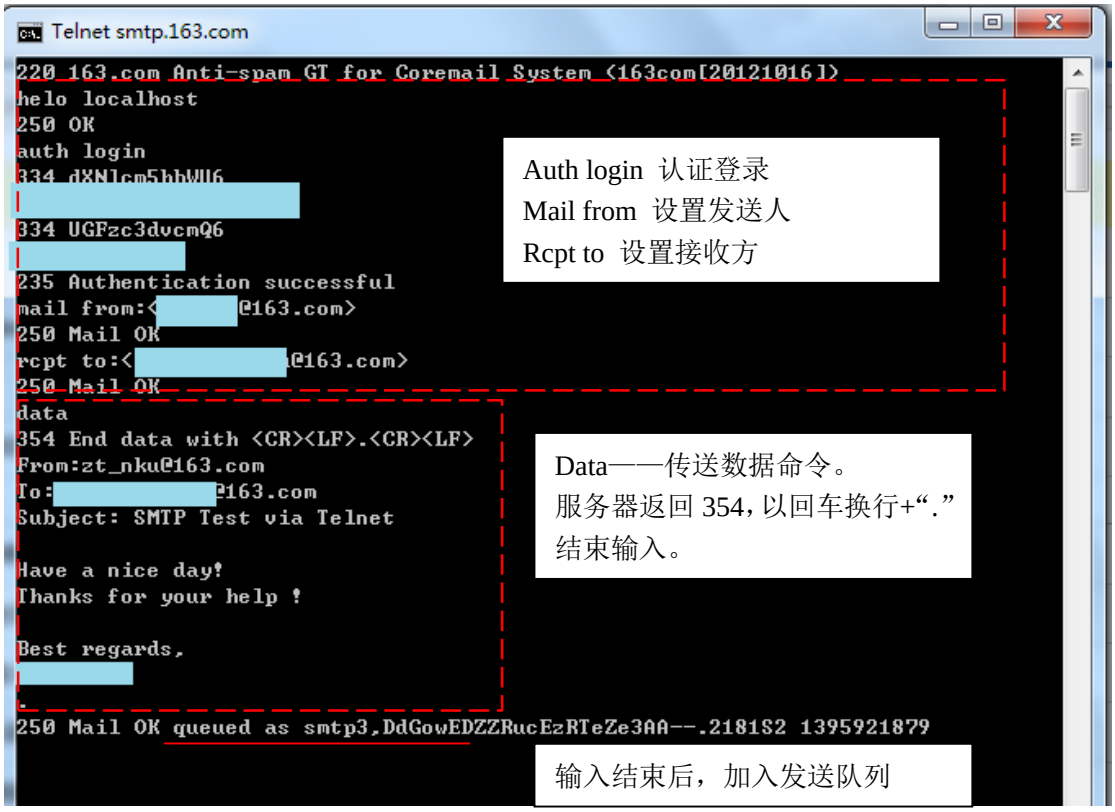
- **通过 Telnet TCP 25 端口，观察 SMTP 命令和响应的交互过程，给出截图。**

  实验中，采用 163 的服务器，进行 SMTP 的实验。

  实验命令如下：

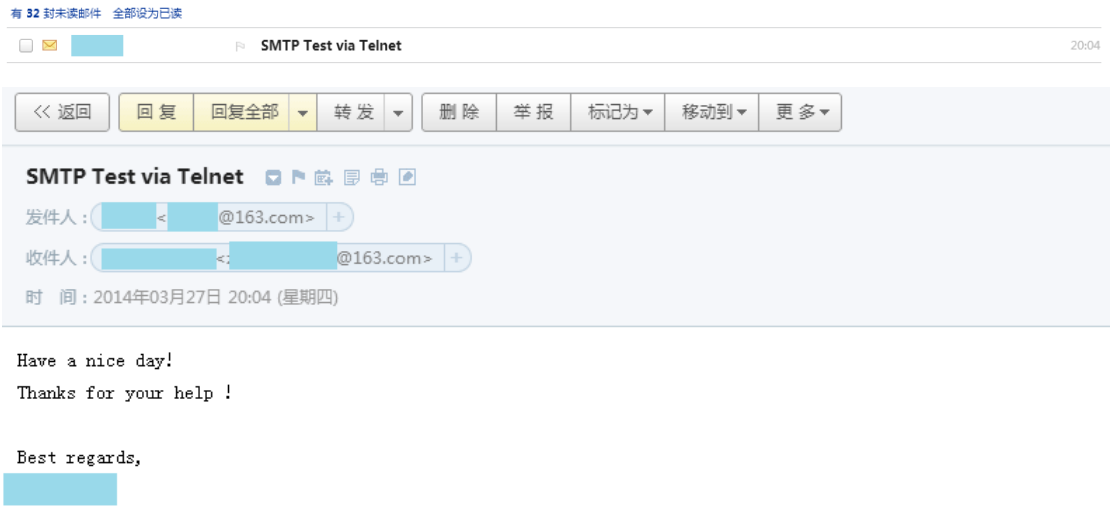
从下图可以看到，使用 SMTP 时，客户端首先发送 HELO 命令至服务器，像服务器标识身份，服务器返回 250 命令，标识可以连接。用户再通过 AUTH　LOGIN 命令，输入加密后的用户名和密码，服务器返回 235 命令，权限认证成功。这之后用户便可以开始用 SMTP 发送邮件。用户在输入合法有效的收/发地址后，便可以输入要传送的数据。

待完成数据输入后，以回车换行+“.”结束，该邮件会被加入发送方的服务器的发送队列中。



完成实验后，发送方的发件箱中出现了上图中发送的邮件，如下图所示：

接收方的收件箱也收到了该邮件，如下图所示：



通过 Telnet TCP 110 端口，观察 POP3 命令和响应的交互过程，给出截图。

实验中采用 163 的服务器进行 POP3 实验，实验命令如下：

实验中的命令和响应如下图所示：

从该图中可以看到，和 SMTP 类似，在进行命令响应交互之前，需要进行身份验证。图中 STAT 命令，返回邮箱中的邮件总数和邮件总大小

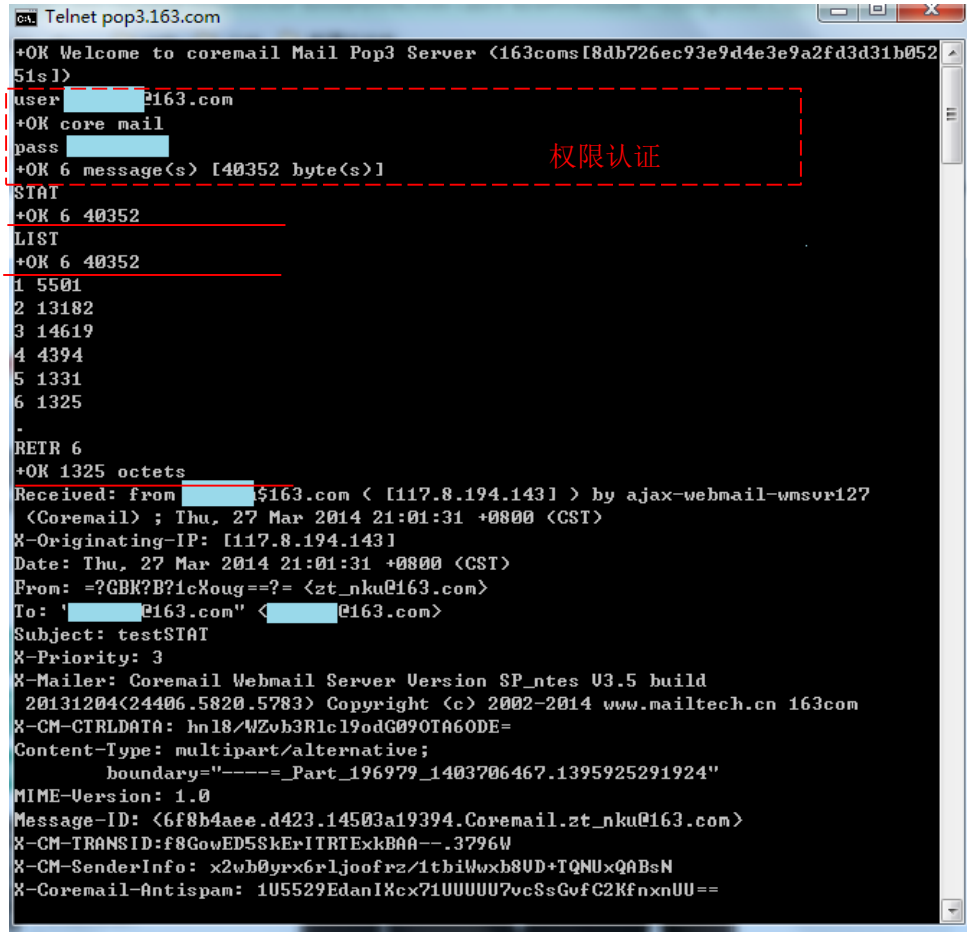
LIST 命令，在 STAT 的基础上，返回了每个邮件的大小

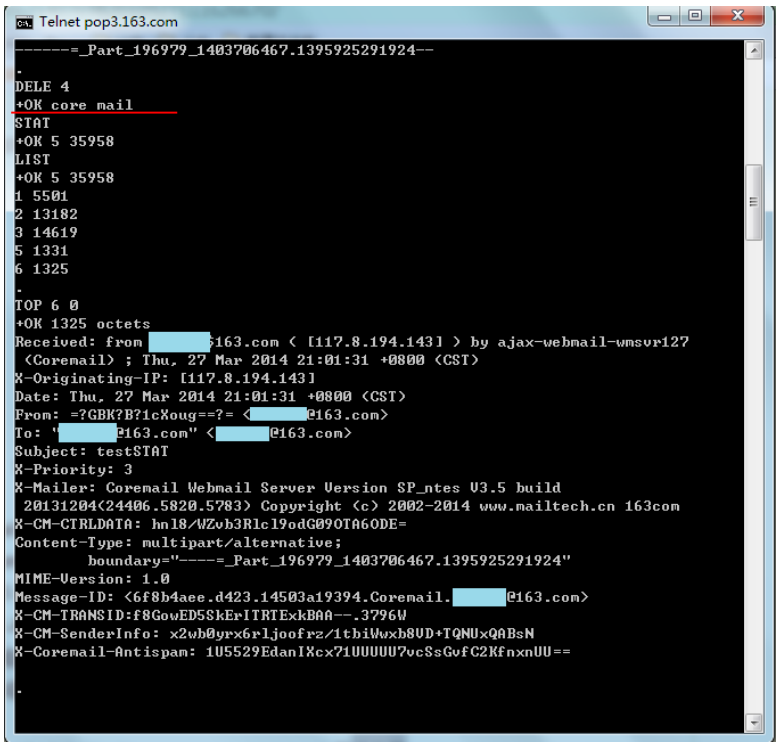
RETR 命令，返回指定邮件的全部文本

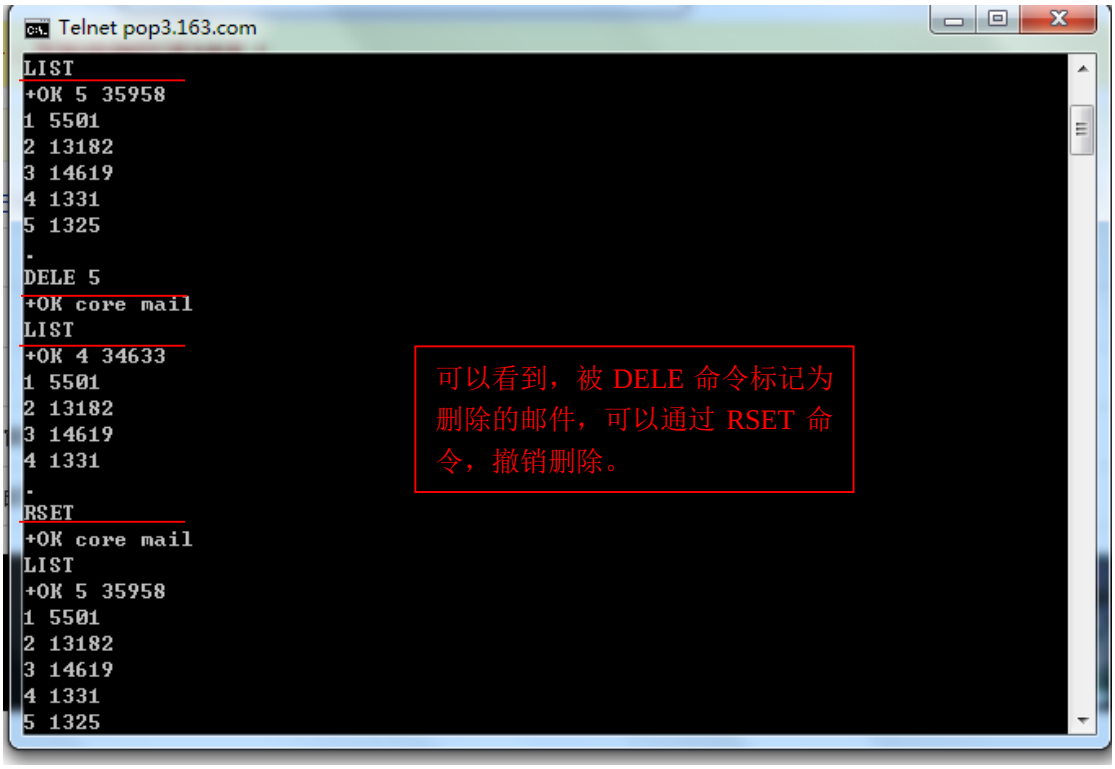
DELE 命令，将邮箱中的指定文件标记为删除，

RSET 命令，撤回 DELE 命令。

TOP 命令，返回邮件先 n 行的命令，如果 n=0，则返回邮件的 head 部分。


Telnet pop3.163.com
+OK Welcome to coremail Mail Pop3 Server (163coms[8db726ec93e9d4e3e9a2fd3d31b052
51s])
user [redacted]@163.com
+OK core mail
pass [redacted]
+OK 6 message(s) [40352 byte(s)]
权限认证
STAT
+OK 6 40352
LIST
+OK 6 40352
1 5501
2 13182
3 14619
4 4394
5 1331
6 1325
.
RETR 6
+OK 1325 octets
Received: from [redacted]$163.com ([117.8.194.143]) by ajax-webmail-wmsvr127
(Coremail) ; Thu, 27 Mar 2014 21:01:31 +0800 (CST)
X-Originating-IP: [117.8.194.143]
Date: Thu, 27 Mar 2014 21:01:31 +0800 (CST)
From: =?GBK?B?1cXoug==?= <zt_nku@163.com>
To: "[redacted]@163.com" <[redacted]@163.com>
Subject: testSTAT
X-Priority: 3
X-Mailer: Coremail Webmail Server Version SP_ntes V3.5 build
20131204(24406.5820.5783) Copyright (c) 2002-2014 www.mailtech.cn 163com
X-CM-CTRLDATA: hnl8/WZvb3Rlcl9odG09OTA6ODE=
Content-Type: multipart/alternative;
boundary="-----=_Part_196979_1403706467.1395925291924"
MIME-Version: 1.0
Message-ID: <6f8b4aee.d423.14503a19394.Coremail.zt_nku@163.com>
X-CM-TRANSID:f8GowED5SkErITRTExkBAA--.3796W
X-CM-SenderInfo: x2wb0yrx6rljoofrz/1tbiWwxb8VD+TQNUxQABsN
X-Coremail-Antispam: 1U5529EdanIXcx71UUUUU7vcSsGvfC2KfnxnUU==


Telnet pop3.163.com
------=_Part_196979_1403706467.1395925291924--
.
DELE 4
+OK core mail
STAT
+OK 5 35958
LIST
+OK 5 35958
1 5501
2 13182
3 14619
5 1331
6 1325
.
TOP 6 0
+OK 1325 octets
Received: from [redacted]$163.com ([117.8.194.143]) by ajax-webmail-wmsvr127
(Coremail) ; Thu, 27 Mar 2014 21:01:31 +0800 (CST)
X-Originating-IP: [117.8.194.143]
Date: Thu, 27 Mar 2014 21:01:31 +0800 (CST)
From: =?GBK?B?1cXoug==?= <[redacted]@163.com>
To: "[redacted]@163.com" <[redacted]@163.com>
Subject: testSTAT
X-Priority: 3
X-Mailer: Coremail Webmail Server Version SP_ntes V3.5 build
20131204(24406.5820.5783) Copyright (c) 2002-2014 www.mailtech.cn 163com
X-CM-CTRLDATA: hnl8/WZvb3Rlcl9odG09OTA6ODE=
Content-Type: multipart/alternative;
boundary="-----=_Part_196979_1403706467.1395925291924"
MIME-Version: 1.0
Message-ID: <6f8b4aee.d423.14503a19394.Coremail.[redacted]@163.com>
X-CM-TRANSID:f8GowED5SkErITRTExkBAA--.3796W
X-CM-SenderInfo: x2wb0yrx6rljoofrz/1tbiWwxb8VD+TQNUxQABsN
X-Coremail-Antispam: 1U5529EdanIXcx71UUUUU7vcSsGvfC2KfnxnUU==
.



Assignment003-2

- **配置域名服务器，理解资源记录的使用**

1. 配置 **sever**：

1）配置 ip 参数：如果网络中已有 DNS 服务器，则把 DNS 服务器一栏指向该服务器 ip，否则指向本机 ip 地址或 127.0.0.1；

2）运行 dcpromo 命令，弹出 Active Directory 安装向导；

3）根据 Active Directory 安装向导开始安装，主要选择“新域的域控制器”、“新林中的域”，并输入域的 DNS 全名等。相关内容根据向导都可完成，此处不再赘述；

4） 安装完成后，重启计算机，输入 dsa.msc 可以看到 Active Directory 用户和计算机。

2. 配置 client：

1） 配置 ip 参数；

2） 打开计算机属性——选择——计算机名——点"更改"，点域并输入域名（在 sever 配置中设定的域名）；

3） 输入域控制器管理员用户名和密码，直到完成，并重启；

4） 重启后就可以看到登录到域和计算机的选项。至此，域名服务器配置完成。

通过阅读**RFC1034**，可以知道：资源记录主要服务器用来解析域名的，每个区域数据库文件都是由资源记录构成的。

标准的资源记录具有其基本格式：**[name] [ttl] IN type rdata**

具体格式说明如下：

name:名称字段，此字段是资源记录引用的域对象名（一台单独的主机或整个域均可）。字段值："."是根域，@是默认域，即当前域；

ttl：生存时间字段，它以秒为单位定义该资源记录中的信息存放在**DNS**缓存中的时间长度。通常此字段值为空，表示采用SOA记录中的最小TTL值(即1小时)。

IN：此字段用于将当前记录标识为一个**INTERNET**的DNS资源记录。

type：类型字段，用于标识当前资源记录的类型。

资源记录类型及其作用说明如下：

A (host)，即是 A 记录(主机记录)，是 DNS 名称到 IP 地址的映射，用于正向解析

SOA：在一个区域的开始使用，SOA 记录后的所有信息均是用于控制这个区域的，每个区域数据库文件都必须包括一个 SOA 记录，并且必须是其中的第一个资源记录，用以标识 DNS 服务器管理的起始位置，SOA 可以指明这个区域的 DNS 服务器中哪个是主服务器。

MX （mail exchange）：邮件交换器记录，用于告知邮件服务器进程将邮件发送到指定的另一台邮件服务器

NS：NS 记录，用于标识区域的 DNS 服务器，即指明负责此 DNS 区域的权威名称服务器（用哪一台 DNS 服务器来解析该区域）

radata: 数据字段用于指定与当前资源记录有关的数据，数据字段的内容取决于类型字段

CNAME：CNAME 记录（别名记录），用于定义 A 记录的别名

PTR：是 IP 地址到 DNS 名称的映射，用于反向解析。

- **考虑 DNS/UDP 的可靠性如何实现**

从 RFC1035 中可以看到：互联网支持在服务器端口 53 上使用 TCP 的名称服务器的访问，并且支持在 UDP 端口 53 上使用 UDP 的数据报访问。使用 UDP 用户服务器端口 53 发送的消息：由 UDP 携带的消息被限制在 512 字节(不包括 IP 首部或 UDP 首部)。

区域传递不适合使用 UDP，但是互联网中推荐的标准查询方法是 UDP。使用 UDP 发送的查询可能丢失，因此需要采用重传策略。查询或查询响应可能会被网络重新排序，或者会被名称服务器重新排序，所以解析器（resolver）不能依赖按顺序返回的响应。

最优 UDP 重传策略将随互联网性能和客户端需求改变，用以下的方法可以优化：

1.在向服务器的特定地址进行重复查询前，客户端应当尝试其他服务器和服务器的其他地址；

2.如果可能，重传的时间间隔应当基于前面的统计量。过于频繁的重传一般会导致。

- **DNS 消息中的 ID 号的作用？**

查看 RFC1035 第四部分 messages。可以看到，DNS 的消息包含五部分：Header、Question、Answer、Authority 和 Additional；而消息的 ID 号包含在 Header 中。Header 格式如下：

```
The header contains the following fields:

                                    1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      ID                       |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR|   Opcode  |AA|TC|RD|RA|   Z    |   RCODE   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    QDCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ANCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    NSCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ARCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

可以看到，消息的 ID 为 16 位。根据 RFC 文档介绍，ID 号标识一次正常的交互，该 ID 由消息请求者设置，消息响应者回复请求时带上该 ID，请求者通过该 ID 号匹配好的查询结

果。

在 DNS 中，任何客户端都可以向服务器发起请求查询，服务器通常需要返回大量查询结果，客户端如何判断接收到的数据包是否为自己需要的查询结果呢？这就是消息的 ID 号的作用，相当于一个验证码实现应答与请求的匹配验证。同时，服务器也可以检测是否存在重复请求者，一定程度上避免不必要的重复查询以及恶意攻击。

当然，仅仅通过一个 ID 验证码作为查询结果与请求的验证是存在安全性风险的——攻击者可以猜测 ID 号从而在真实的查询请求到达前发出其他请求或者给客户端返回一个匹配 ID 的应答。这也就是 DNS 会遭到欺骗攻击的原因。