**TCP三次握手实验1 : SMTP**

电子邮件是我们的生活工作中经常使用的一种服务，用来联系世界各地的朋友，客户。下面我们就用Wireshark对电子邮件进行抓包。

准备工作：

安装邮件客户端一款(Outlook,Foxmail,KooMail,...)

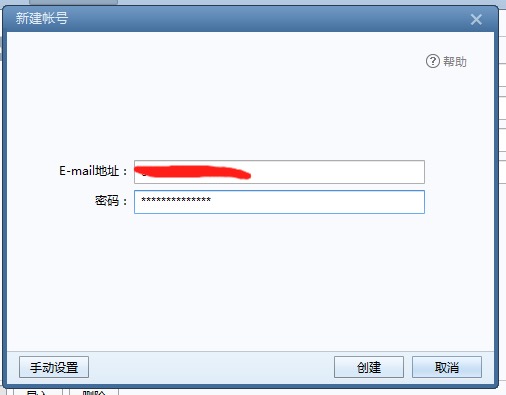
　　Wireshark

　　邮件测试账号两枚

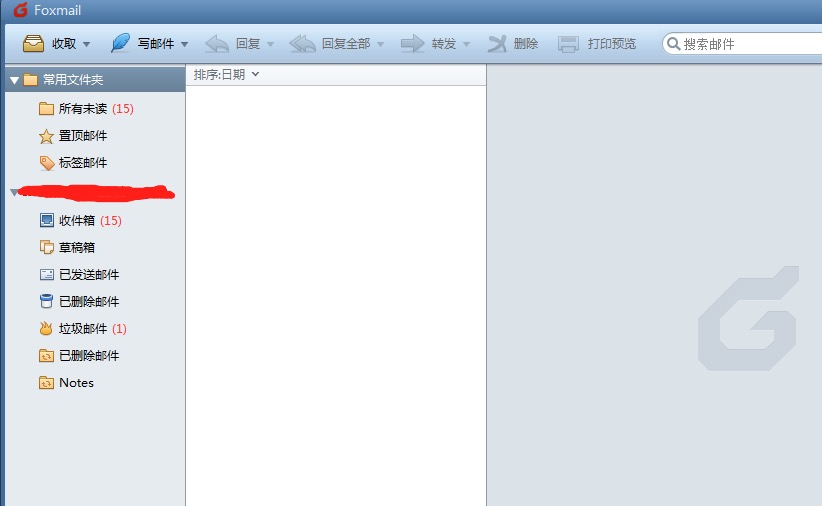
　　邮件相关协议知识([SMTP协议](http://baike.baidu.com/link?url=4YAhtE70bVlWyfksywoPQhlG-MAb3D7PaqbXafCCgF1POfErXFQwGF7r7j39OqOCrFuYuFMFUB1kP38GxbnM48vFiSx1_ejxoZPmv3NO5HMNzRAZwFMcY3X-lSIbC_qdSxmBIRJo9UCVvk5y3rWYiudyL6cUMrLR-3lkLS9tDwe)，[POP协议](http://baike.baidu.com/link?url=mIsWcDs29vo4Zx5q3YI7nSLO5sns53tMSWDBUEHsh8iayvwYmobIHMR3VoXZ93NsF8pc77ubX2MmJLS22XsaiK)，[IMAP协议](http://baike.baidu.com/view/17877.htm))

1.邮件客户端设置

　　[1].打开Foxmail 进行账号设置

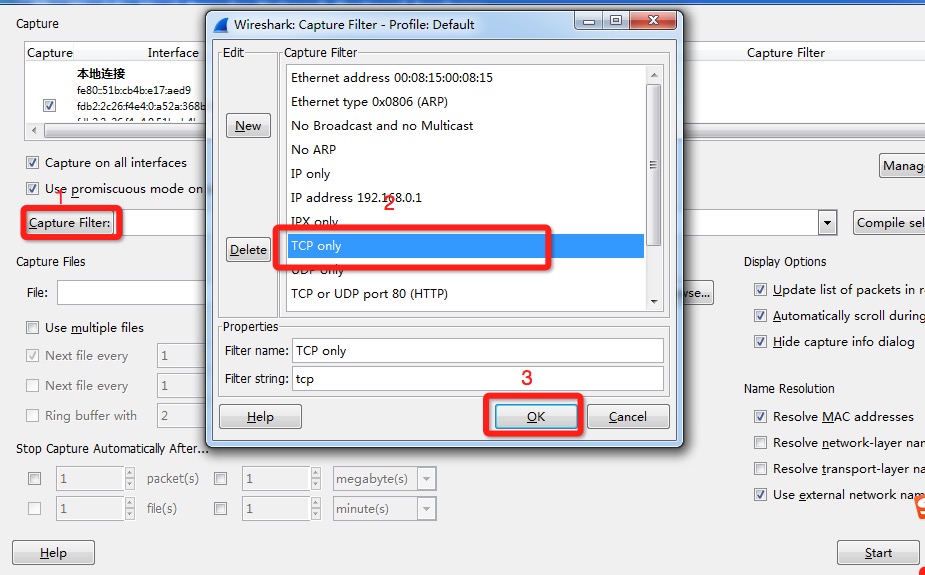


　　[2]设置成功后，写一封邮件先不要发送。



2.Wireshark 抓包前选项设置(主菜单->Caputre->Options)

　　[1].设置过滤器，减少信息干扰。

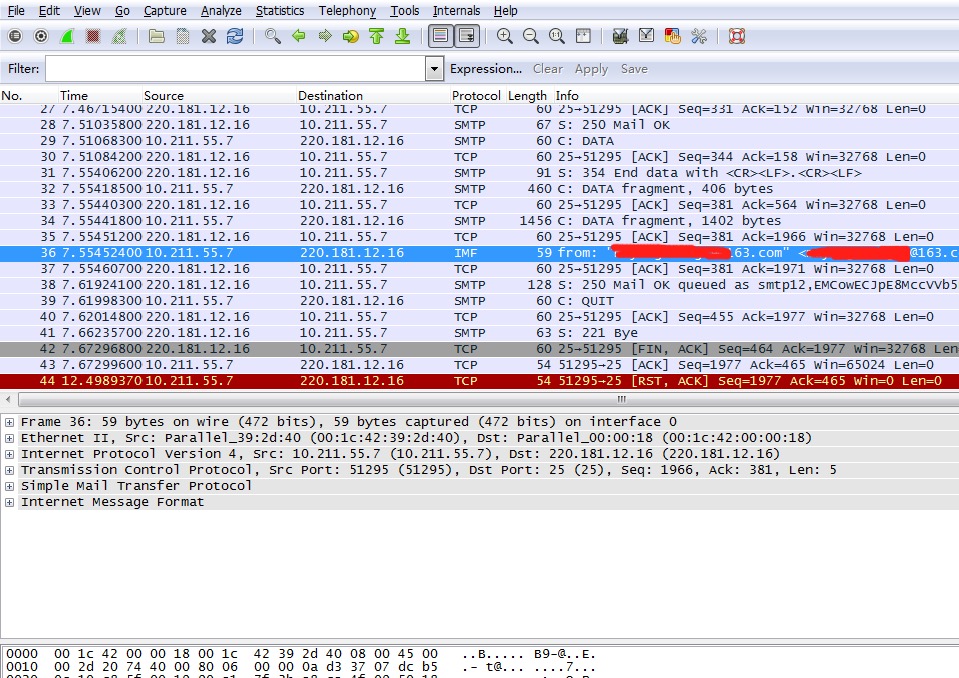


3.抓捕电子邮件数据包

　　[1].选项设置完后，点击Start开始抓捕数据包。

　　[2].在Foxmail中发送前面写好的邮件。

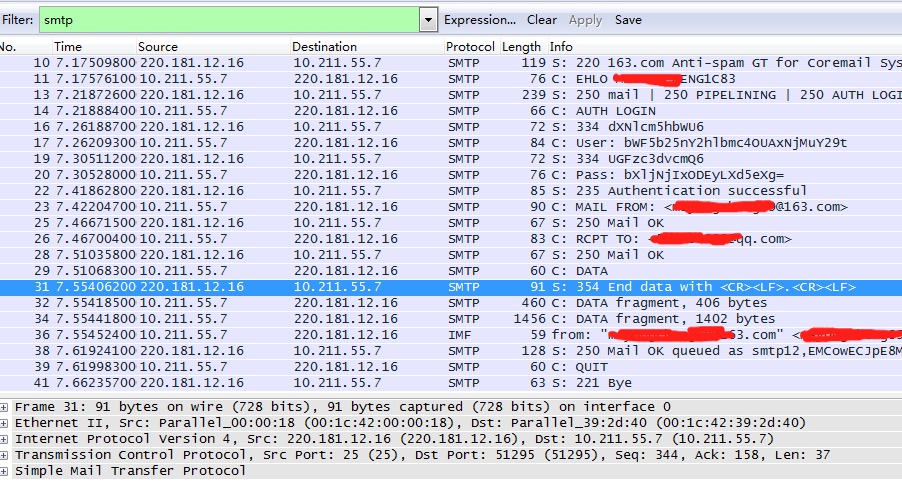
　　[3].邮件发送完成后，Wireshark 中点击 Stop 停止抓捕数据包



4.分析TCP和电子邮件数据包

[1]. 分析TCP三次握手，类似与HTTP的方法

　　[2].分析电子邮件：过滤SMTP方便查看。

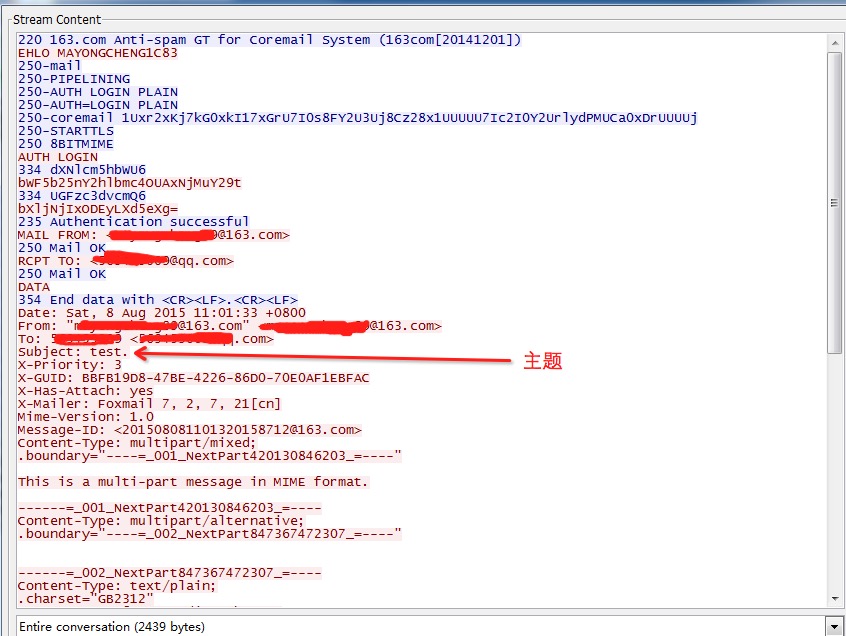


　　[3].分析SMTP 工作流程

* 第11帧Foxmail向服务器发送EHLO指令，表明身份，我们可以看到Foxmail客户端的主机名: xxxxENG1C83。
* 第17帧与第20帧,我们可以看到发送邮件的User和Pass，但是是经过base64加密的，因为SMTP不接收明文。
* 第23帧与第26帧,我们可以看到发送邮件的发送者和接受者，这个是明文的。
* 第32帧与第34帧,Foxmail客户端发送的数据大小。
* 第36帧是邮件的账户和主题信息。
* 第39帧断开服务器连接。

　　[4].查看电子邮件的内容

　　　选择任何想看的一帧数据包的详细内容，单击右键 选择Follow TCP Stream 即可进行查看。





　　　　经过Wireshark 分析，电子邮件个人信息基本泄露。