实验一 SMTP 与 POP3 消息的捕获与分析

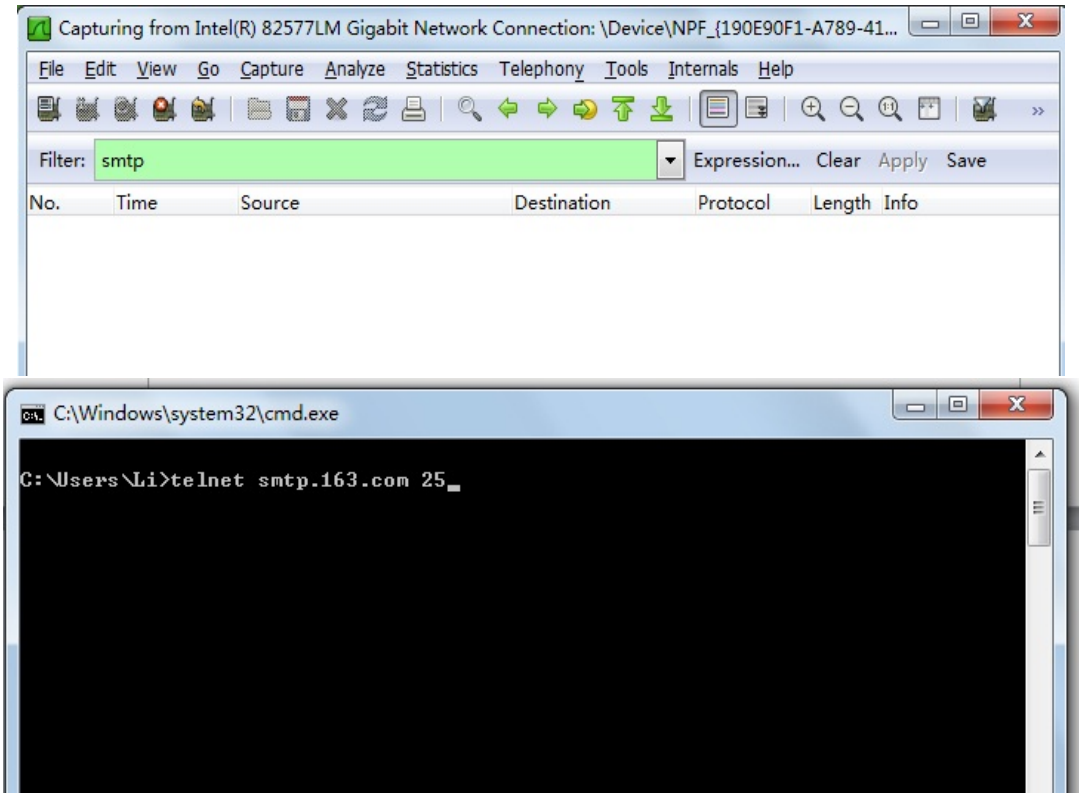
SMTP 消息和 POP3 消息的捕获需要使用在 Windows 命令行下使用 Telnet 命令登陆邮件提供商的 SMTP 和 POP3 服务器。本文使用 SMTP 命令访问 163 邮箱为例，供同学们参考。

1. 首先申请一个 163 邮箱，进入主界面后，点击页面上方的“设置”进入设置页面。

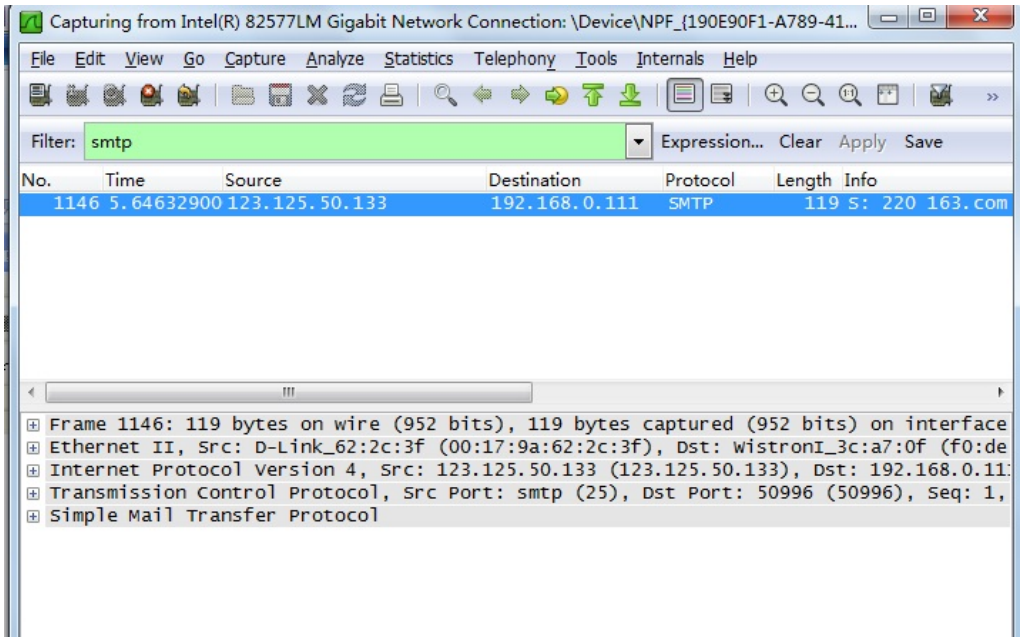
2. 进入邮箱中心——客户端授权密码，选择开启，并记住授权码，该授权码后面为用来登陆邮箱的密码。

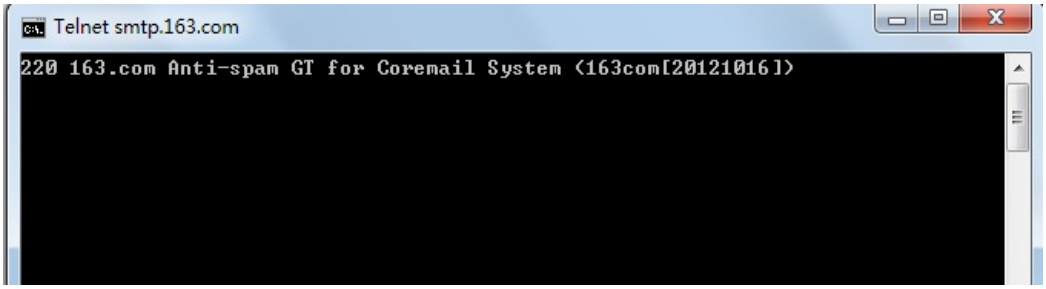
3. 选择 POP/SMTP/IMAP 选项，记下 POP/SMTP 服务器的地址。

4. 然后打开 wireshark 抓包软件，在显示过滤条件行中输入 smtp 并且开始抓包，同时在命令行窗口输入：telnet smtp.163.com 25。



5. 敲击回车后，Wireshark 显示和命令行的显示结果如下图所示：





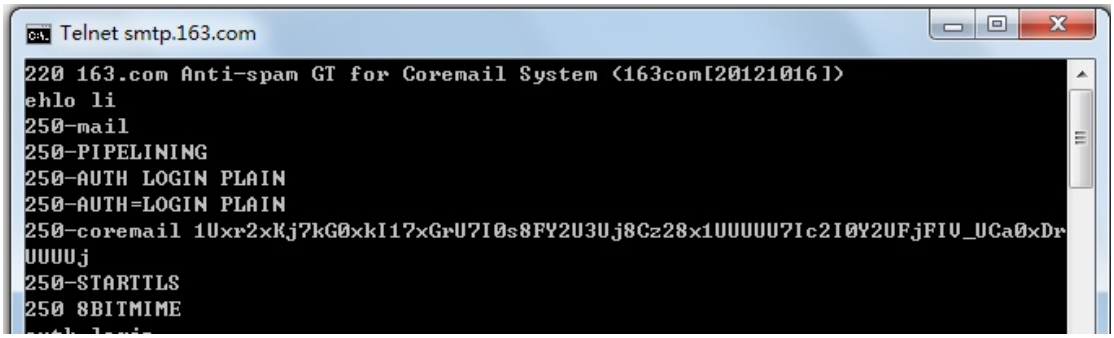
6. 上图中的 220 是邮件服务器返回给客户的响应状态码，它表示邮件服务器准备就绪(service ready)；163.com 则表示邮件服务器的域名。
这些提示信息表明网易的 SMTP 服务器登录成功，用户可以通过输入 SMTP 命令与邮件服务器进行通信，并用 wireshark 捕获到的报文进行格式和内容的分析。

与发送邮件相关的 SMTP 命令如下表所示：

SMTP 命令及格式	说明
ehlo<SP><domain><CRLF>	ehlo 命令是 SMTP 邮件发送程序与 SMTP 邮件接收程序建立连接后必须发送的第一条 SMTP 命令。参数<domain>表示 SMTP 邮件发送者的主机名。ehlo 命令用于替代传统 SMTP 协议中的 helo 命令
auth<SP><para><CRLF>	如果 SMTP 邮件接收程序需要 SMTP 邮件发送程序进行认证时，它会向 SMTP 邮件发送程序提示它所采用的认证方式，SMTP 邮件发送程序接着应该使用这个命令回应 SMTP 邮件接收程序，参数<para>表示回应的认证方式，通常是 SMTP 邮件接收程序先前提示的认证方式。
mail<SP>from:<reverse-path><CRLF>	此命令用于指定邮件发送者的邮箱地址，参数<reverse-path>表示发件人的邮箱地址。
rept<SP>to:<forword-path><CRLF>	此命令用于指定邮件接收者的邮箱地址，参数<forword-path>表示接收者的邮箱地址。如果邮件要发送多个接收者，那么应使用多条 rept<SP>to 命令来分别指定每一个接收者的邮箱地址。
data<CRLF>	此命令用于表示 SMTP 邮件发送程序准备开始传送邮件内容，在这个命令后面发送的所有数据都将被当做邮件内容，直至遇到“<CRLF>.<CRLF>”标志符，则表示邮件内容结束。
quit<CRLF>	此命令表示要结束邮件发送过程，SMTP 邮件接收程序接收到此命令后，将关闭与 SMTP 邮件发送程序的网络连接。

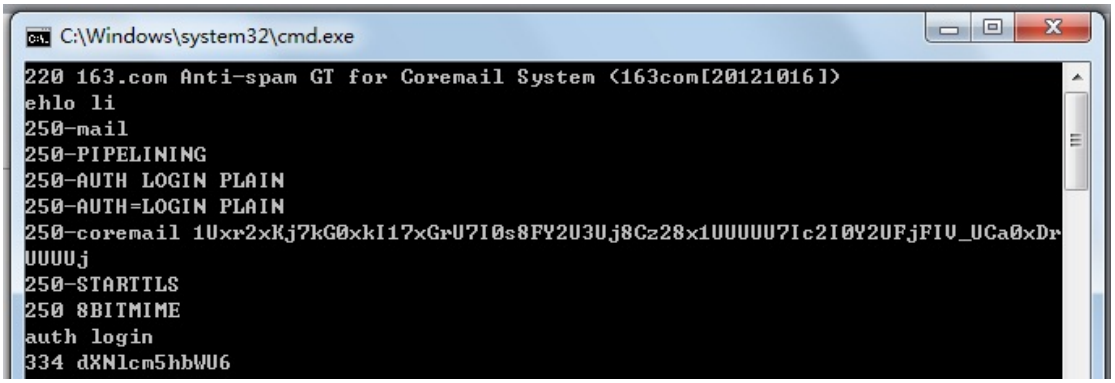
7. 使用 SMTP 命令的通信过程实例

1）建立连接后，用户（邮件的发送方）首先应该使用 ehlo 命令向 SMTP 服务器接收程序发送问候信息。由于当前运行 Telnet 程序的计算机没有在 Internet 上注册的主机名，这里随便使用一个名称“Li”来表示 ehlo 命令中主机名。发送 ehlo 命令后，邮件服务器返回的信息如下图所示：



2）接着输入命令：auth login

SMTP 服务器返回的响应信息如下图所示：

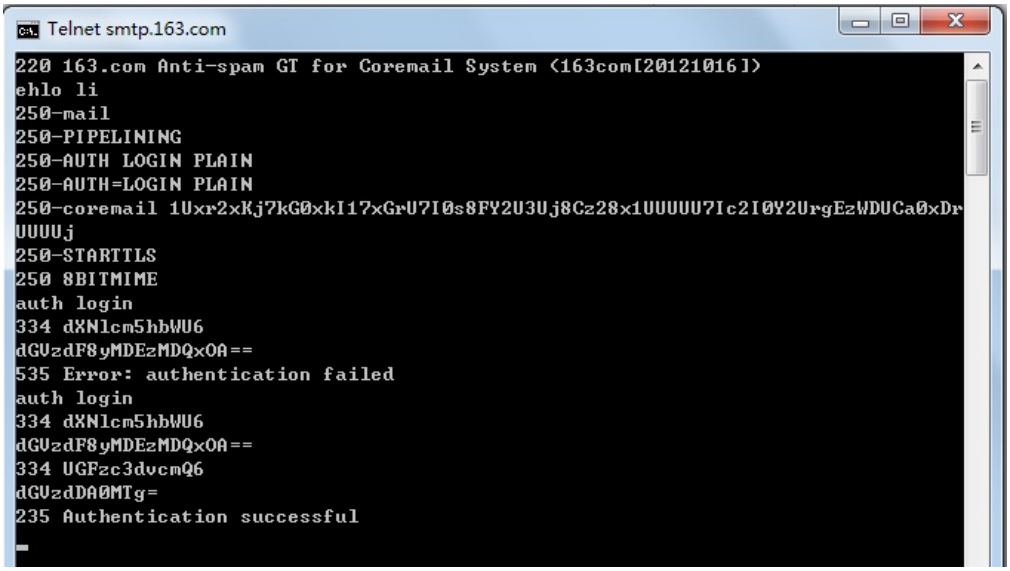


要注意：上图中的状态码 334 提示用户应输入帐户名和密码，后面跟的是 BASE64 编码。

同学们可以使用在线转码的网站，如 http://www1.tc711.com/tool/BASE64.htm，来进行 ASCII 码和 BASE64 编码的转换。

3）用户输入的帐户名和授权码同样需要先转换成 BASE64 编码，如下图所示，在上面的文本框里输 163 邮箱的 Email 账户 test_20130418，点击编码，下面的文本框就显示出对应的 BASE64 编码。

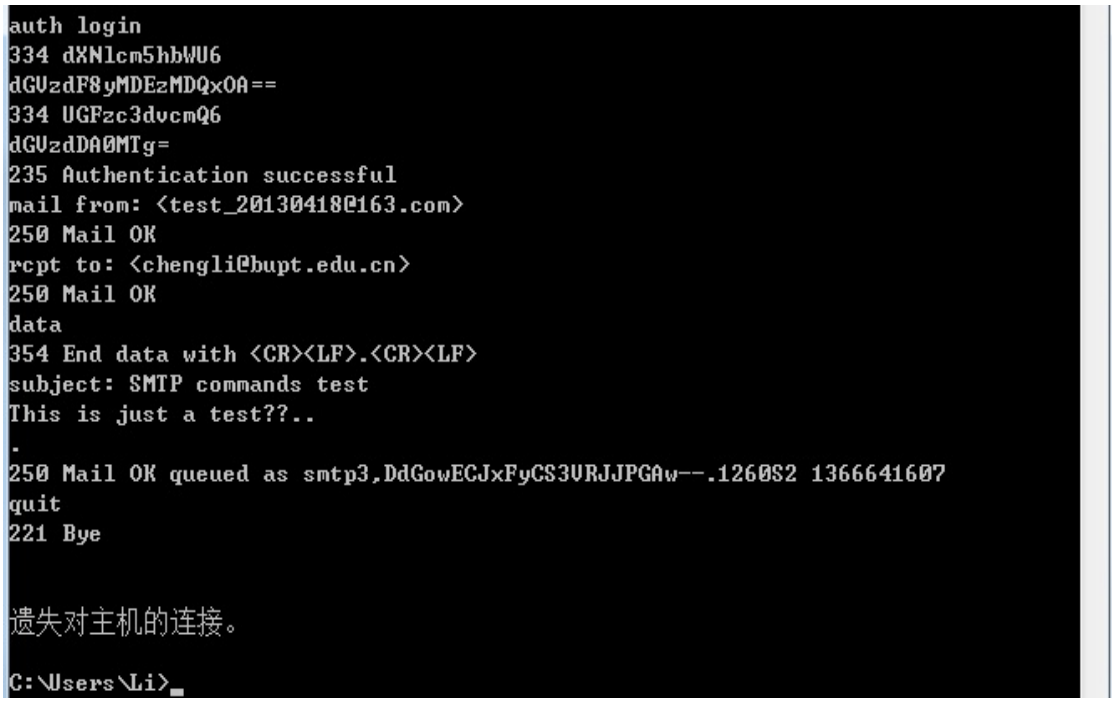
4）将账户名对应的 BASE64 编码复制粘贴到命令行窗口中，回车，可见返回的是状态码 334，表示账户名正确，提示输入密码。同样需要先将密码转换成 BASE64 编码，然后再复制粘贴到命令行窗口中。如下图所示，此时，服务器返回状态码 235，提示登录成功，可以开始发送邮件了。



5）输入 mail from 命令，告诉服务器发件人账户。

然后输入 rcpt to 命令，告诉服务器收件人的 Email 地址。

再使用 data 命令开始发送邮件内容。

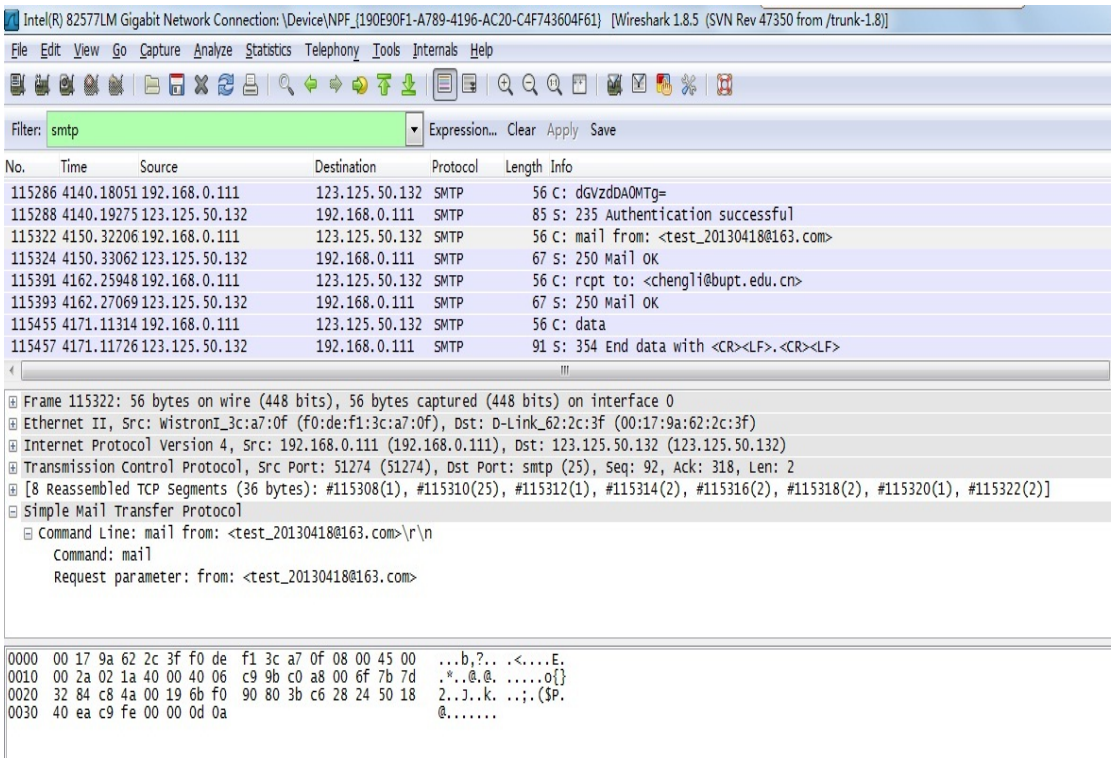


注意，邮件消息是以单独占一行的一个“.”来标志结束的。

邮件发送结束后，使用 quit 命令拆除与邮件服务器的连接。

还要注意一点，命令行环境下不支持退格键，因此一旦输入错误，无法更改。同学们可以把要输入的命令事先保存在一个文本文件中，逐一复制粘贴到命令行中，以减少输入错误。

在上述的试验用例中，使用 Wireshark 可以捕获到全部的 SMTP 协议消息，可以从中分析 SMTP 协议的格式和内容，并且都是明文传输，如下图所示：



对于 POP3 命令，同样可以在命令行状态下，使用 telnet 连接到邮件服务器（端口号为 110），通过手工输入 POP3 命令，来捕获 POP3 消息。具体的命令和返回信息可以参照教材 p57 的示例。

注意：在 POP3 中，用户名和密码不需要用 base64 编码，且密码仍然为授权码

附： Wireshark 软件使用说明

本次实验使用的是 Wireshark 软件，其早期版本称为 Ethereal。Wireshark 是一个网络包分析工具，它可以捕获网络中传输的数据包，对于数据包进行解析，并显示包中各协议数据的详细内容，是目前最好的开源网络分析软件之一。Wireshark 可以应用在下列情形：

- 帮助网络管理员解决网络问题
- 帮助网络安全工程师检测安全隐患
- 帮助开发人员测试其开发的协议的执行情况
- 帮助学生学习网络协议

1.1 Wireshark 软件的安装

在 http://www.wireshark.org 下载 Wireshark 安装包并执行，安装选项可以选择默认配置。Wireshark 安装包中已包含 WinPcap，无需单独下载安装。

1.2 运行 Wireshark 并设置捕获条件

运行 Wireshark 软件（对于 windows vista 和 windows 7，要以管理员身份运行），在启动页或者菜单中选择 ***Capture Options***，如图 1 所示，需要配置的参数为：

- 选择待捕获的接口（***Interface***），即以太网网卡或无线网卡；
- 选中混杂模式（***promiscuous mode***）捕获，即捕获所有的数据；
- 设置好后，按 ***Start*** 即开始捕获。

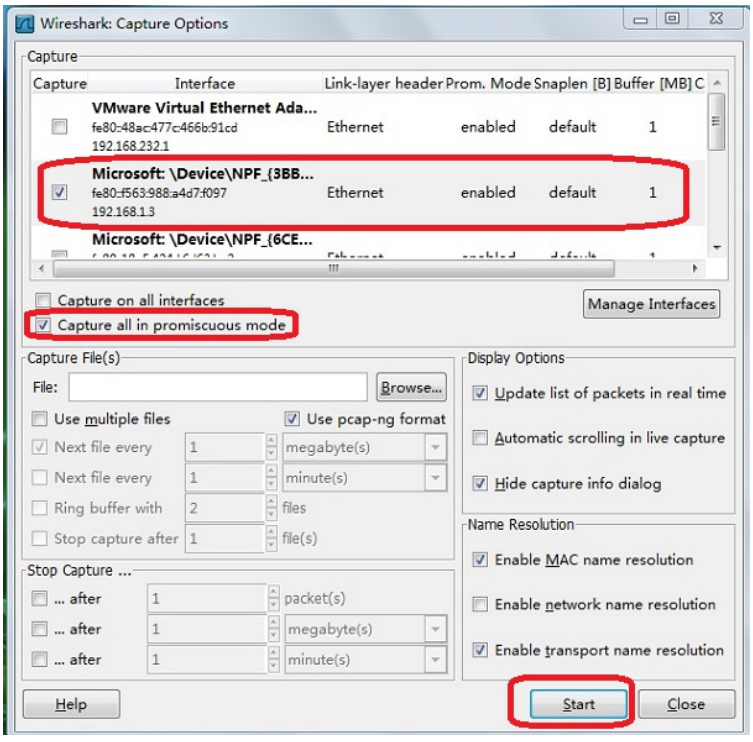


图 1 Wireshark 的捕获条件设置示例

1.3 解码分析

启动捕获之后，运行相应的网络通信程序，Wireshark 即可以捕获到网卡发送和接收到的符合捕获条件的数据，并在显示在如图 2 所示的主窗口中。

注：在显示过滤器中进行设置，可以只显示需要的消息，例如图 2 中，dns 表示只显示

DNS 消息。要显示 HTTP 消息，可以设置为 http。如果要观察连接的建立和释放，则应该设置为 tcp.port==80，以便同时截获 TCP 的连接建立和释放报文段。

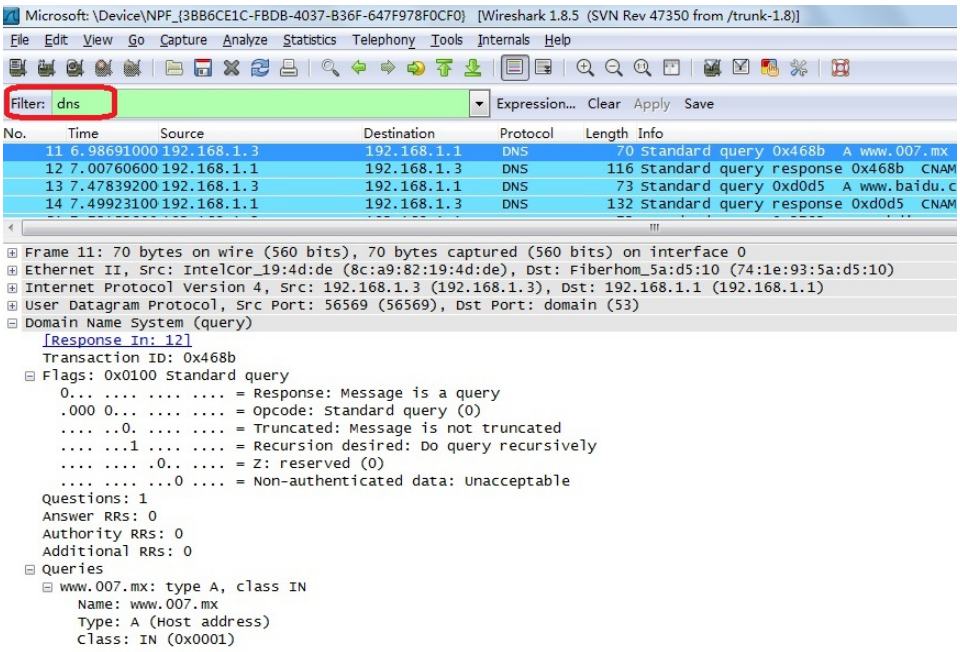


图 2 Wireshark 主窗口示例

Wireshark 的数据显示窗口分为 Packet List、Packet Detail 和 Packet Byte 三部分。

1. PacketList：显示所捕获到的所有数据包，每行显示一个数据包。如果选中一行，在下面的 Packet Detail 和 Packet Byte 窗口中显示对应的详细信息。

默认情况下，PacketList 显示包括下面各列：

- **No.** ：表示包的序号
- **Time**：表示包的时间戳
- **Source**：显示包的源 IP 地址。
- **Destination**：显示包的目的 IP 地址
- **Protocal**：显示包内数据的协议类型
- **Length**：消息长度
- **Info**：包内容的主要信息，例如对于 DNS 消息，将包括：消息类型、消息标识、解析类型、域名等信息。

2. PacketDetail：显示在 PacketList 窗口中所选中的数据包解析后的详细信息，包括每个协议字段的含义及其值。PacketList 窗口中的显示是从数据链路层开始，每层协议显示一行概要信息，包括协议的源地址和目的地址。如图 2 示例的 DNS 消息，概要信息分别显示了以太网帧地址、IP 包地址和 UDP 数据报端口号。
   每层协议的细节信息是以树状方式组织的，可以展开，如图 2 示例，对 DNS 的协议消息进行了展开，可以看到每个协议字段的名字、值和补充信息。
3. Packet Byte：以十六进制的方式在 PacketList 和 PacketDetail 窗口中所选中的部分对应的数据值。该窗口分为 3 部分，左侧分栏显示选中数据在整个帧中的偏移量，中间分栏显示 16 进制的对应值，右侧分栏显示对应的 ASCII 字符值。

关于 Wireshark 的详细功能和具体使用说明，请参照教师提供的的 Wireshark 用户手册。