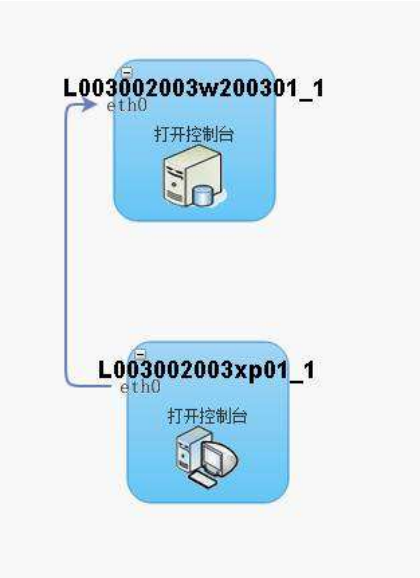
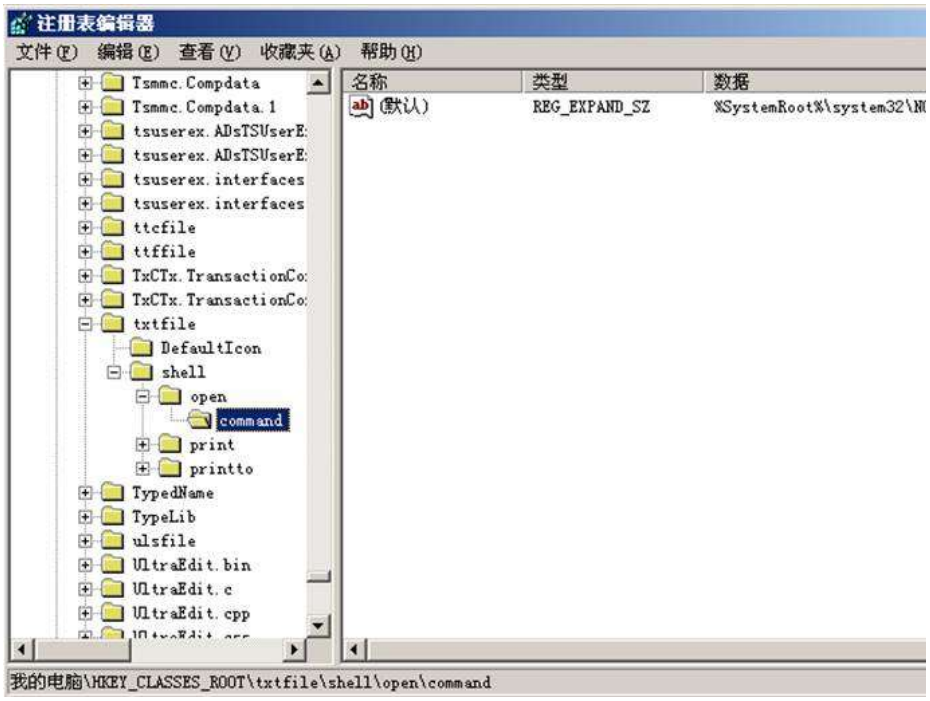
<table>
<tr><td colspan="3">课程编写</td></tr>
<tr><td colspan="2">类别</td><td>内容</td></tr>
<tr><td colspan="2">实验课题名称</td><td>测试冰河木马</td></tr>
<tr><td colspan="2">实验目的与要求</td><td>本次实验学习冰河木马远程控制软件的使用，通过实验可以了解木马和计算机病毒的区别，熟悉</td></tr>
<tr><td colspan="2"></td><td>络攻击的原理和方法。</td></tr>
<tr><td rowspan="4">实验环境</td><td>VPC1(虚拟PC)</td><td>操作系统类型：windows server 2003和windows XP professional，网络接口：本地连接</td></tr>
<tr><td>VPC1 连接要求</td><td>PC 网络接口，本地连接与实验网络直连</td></tr>
<tr><td>软件描述</td><td>1、学生机要求安装java环境
2、windows server 2003系统和windows XP professional，冰河木马软件（服务器和客户端）。</td></tr>
<tr><td>实验环境描述</td><td>1、 学生机与实验室网络直连；
2、 VPC1与实验室网络直连；
3、 学生机与VPC1物理链路连通；</td></tr>
<tr><td colspan="2">预备知识</td><td>1. 会打开注册表
2. 会查看ip地址</td></tr>
<tr><td colspan="2">实验内容</td><td>本次实验学习冰河木马远程控制软件的使用，通过实验可以了解木马和计算机病毒的区别，熟
行网络攻击的原理和方法。</td></tr>
<tr><td colspan="2">实验步骤</td><td>学生登录实验场景的操作
1、学生单击 “网络拓扑”进入实验场景，单击windows2003中的“打开控制台”按钮，进入目标
示：
 

2、学生输入账号Administrator ，密码123456，登录到实验场景中的目标主机。如图所示:</td></tr>
</table>

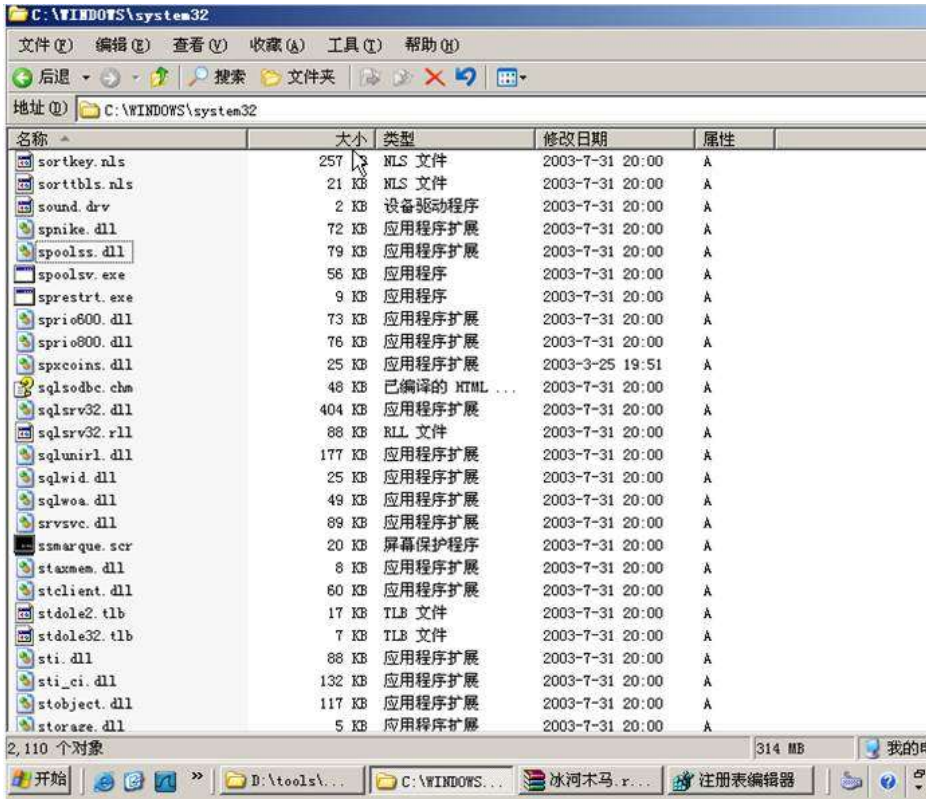
3、 进入到“D:\tools\冰河木马\冰河木马”文件夹，如下图所示：

4、冰河木马共有两个应用程序，见图，其中win32.exe是服务器程序，属于木马受控端程序，种
将该程序放入到受控端的计算机中，然后双击该程序即可；另一个是木马的客户端程序，属于
序。

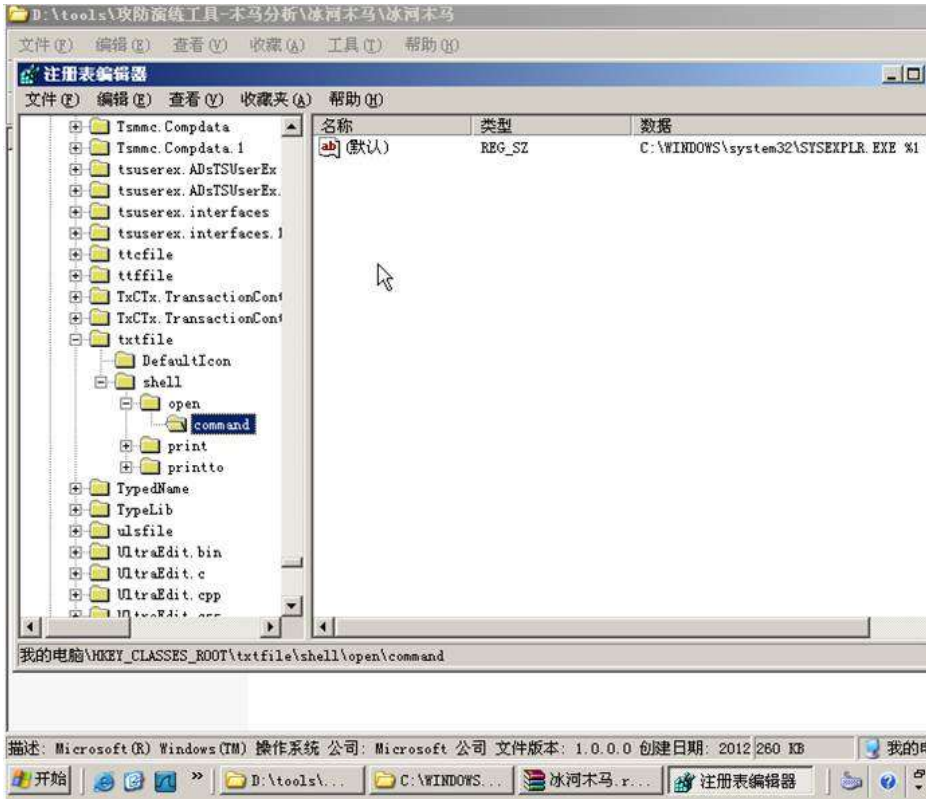
5、在种木马之前，我们在受控端计算机中打开注册表，查看打开txtfile的应用
HKEY_CLASSES_ROOT\txtfile\shell\open\command ， 可以看到打开 .txt 文件
c:\winnt\system32\notepad.exe%1，见图。



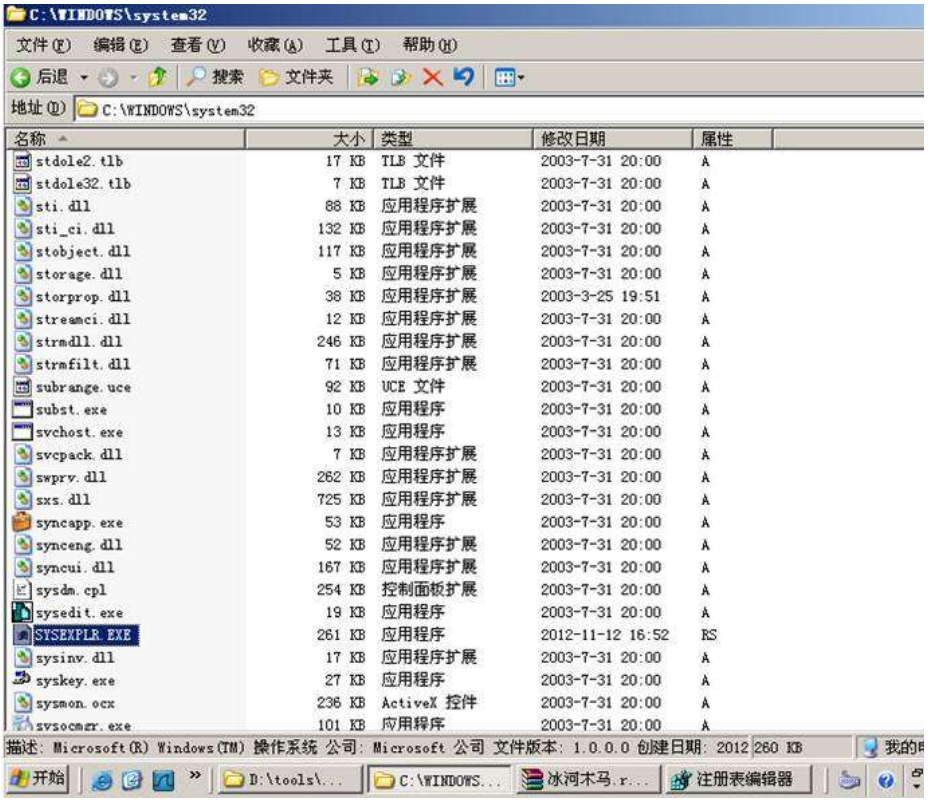
6、再打开受控端计算机的c:\winnt\system32文件夹（XP系统为C:\windows\system32），sysexplr.exe文件，如图所示。



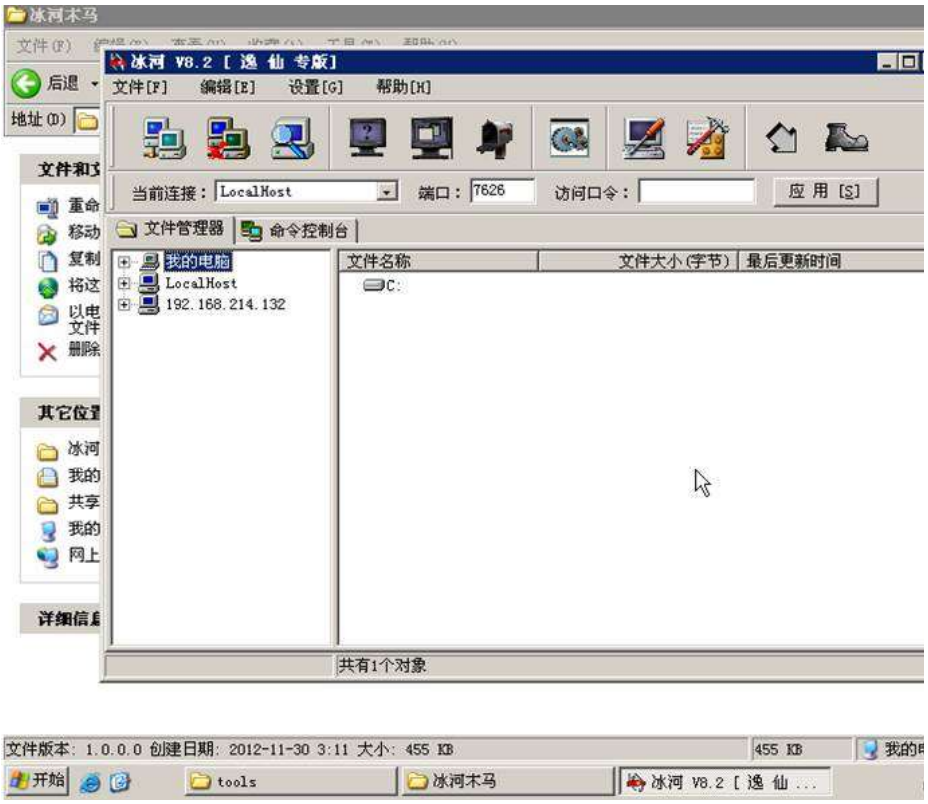
7、现在我们在受控端计算机中双击Win32.exe图标，将木马种入受控端计算机中，表面上好像没发生。（此时cpu使用率为100%）我们也可以打开受控端计算机的注册表，查看打开.txt文件的应用程序HKEY_CLASSES_ROOT\txtfile\shell\open\command，可以发现，这时它为C:\winnt\system32\sysexplr.exe%1，见图。



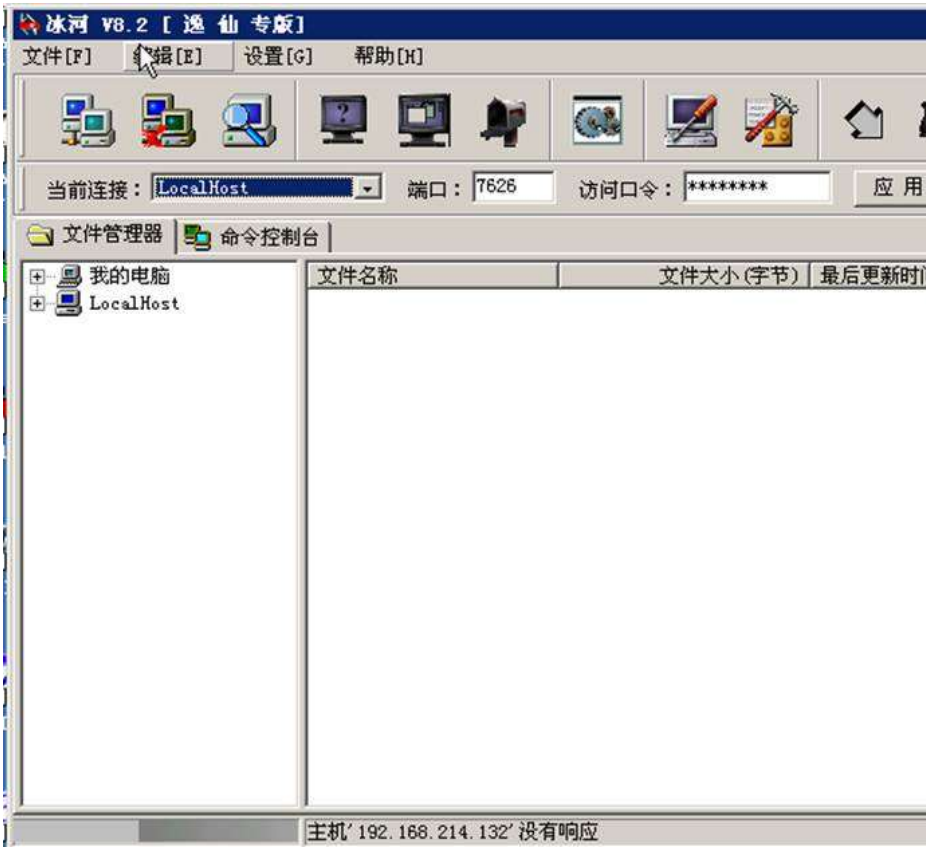
8、我们再打开受控端计算机的C:\WINNT\System32文件夹，这时我们可以找到sysexplr.exe文件，



9、我们在主控端计算机中，双击Y_Client.exe图标，打开木马的客户端程序（主控程序）。可以
面。



10、我们在该界面的【访问口令】编辑框中输入访问密码：12211987，设置访问密码，然后点击
图。



11、点击【设置】->【配置服务器程序】菜单选项对服务器进行配置，弹出图11所示的服务器配置

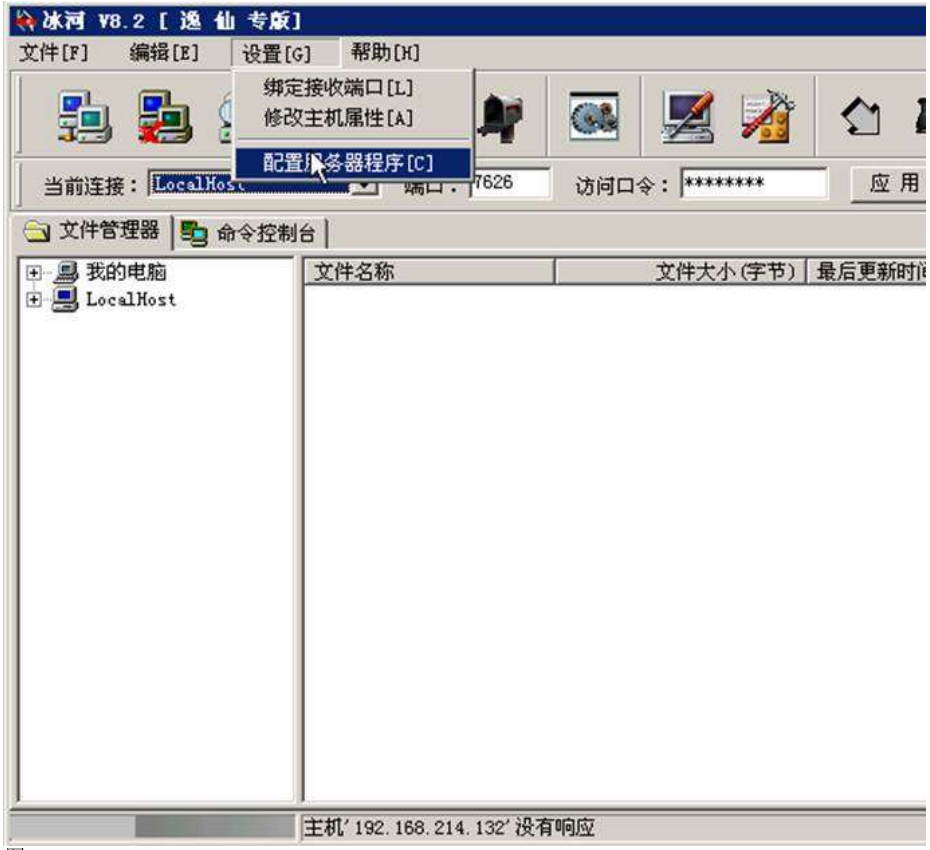
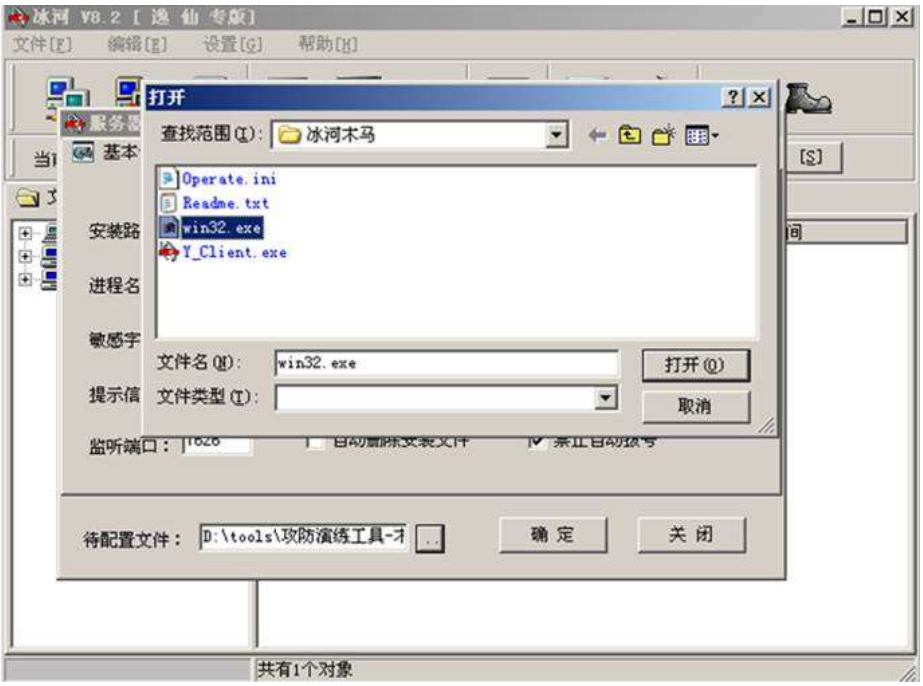
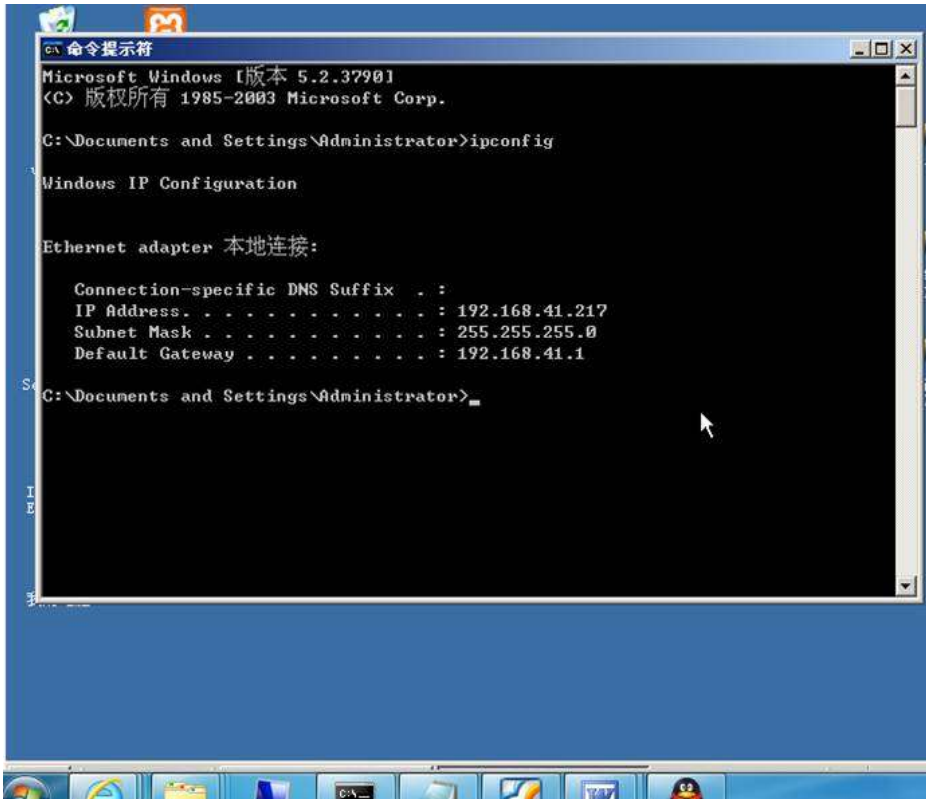


图11:

12、在服务器配置对话框中对待配置文件进行设置，如图11点击该按钮，找到服务器程序文件win3
文件；再在访问口令框中输入12211987，然后点击【确定】，就对服务器已经配置完毕，关闭对话

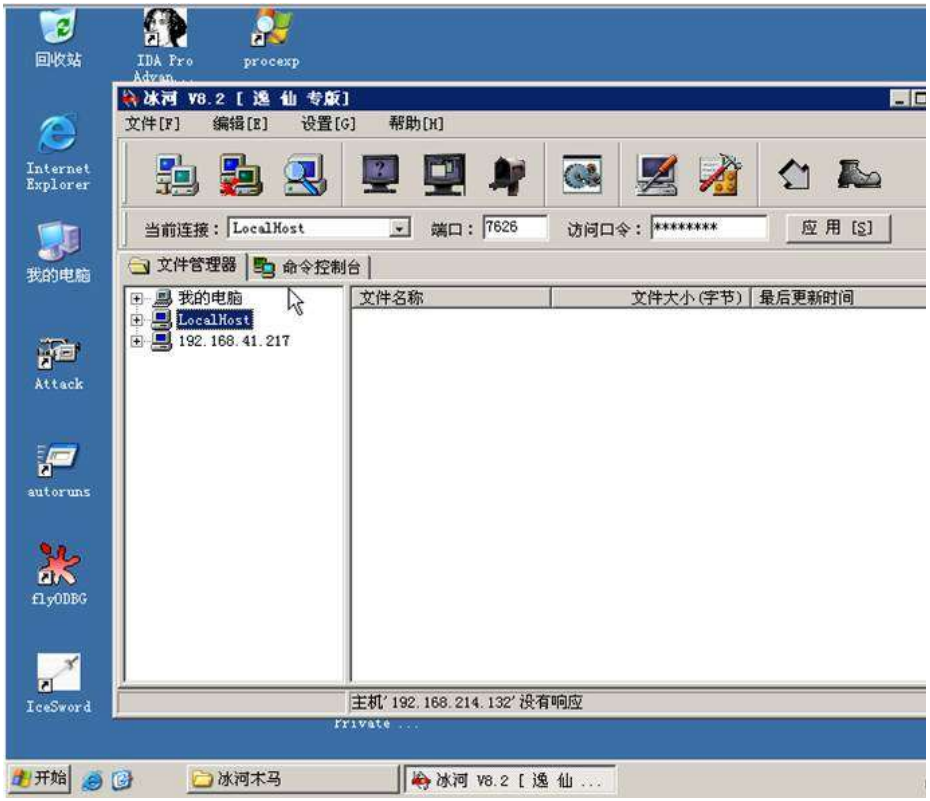


13、现在在主控端程序中添加需要控制的受控端计算机，我们先在受控端计算机中查看其IP地址（172.16.8.62）。



14、这时可以在我们的主控端计算机程序中添加受控端计算机了，详细过程见图

15、当受控端计算机添加成功之后，我们可以看到图所示界面。



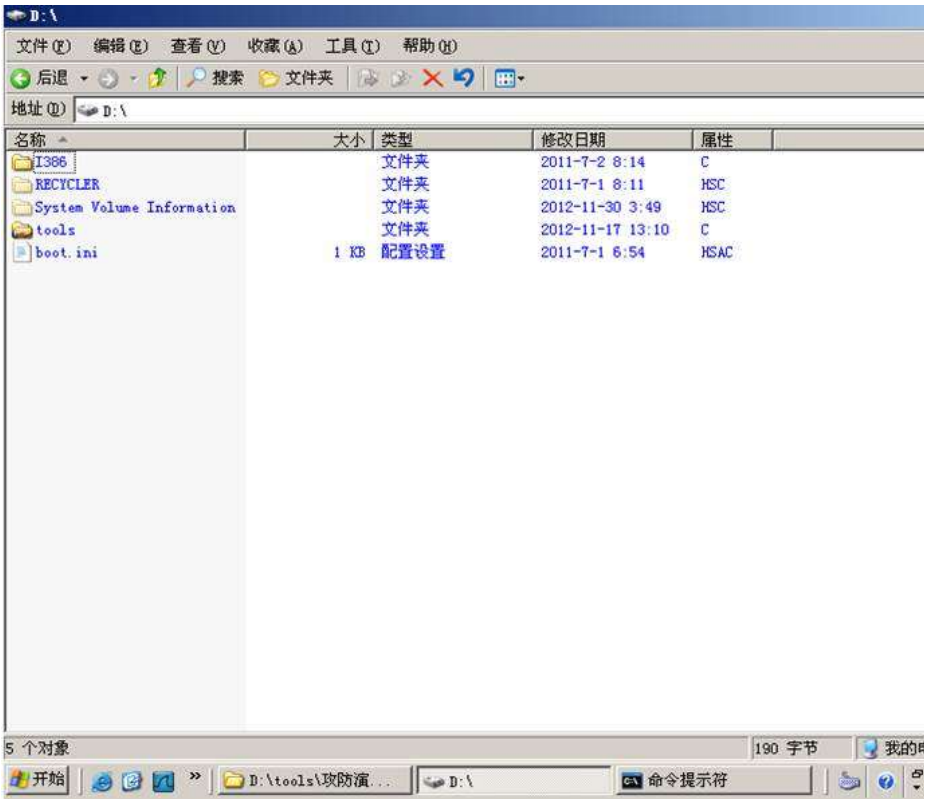
16、我们也可以采用自动搜索的方式添加受控端计算机，方法是点击【文件】->【自动搜索】，
话框。

17、搜索结束时，我们发现在搜索结果栏中IP地址为172.16.8.62的项旁状态为OK，表示搜
172.16.8.62的计算机已经中了冰河木马，且系统自动将该计算机添加到主控程序中。

18、将受控端计算机添加后，我们可以浏览受控端计算机中的文件系统

19、我们还可以对受控端计算机中的文件进行复制与粘贴操作，把C盘中的boot.ini文件拷贝到D盘

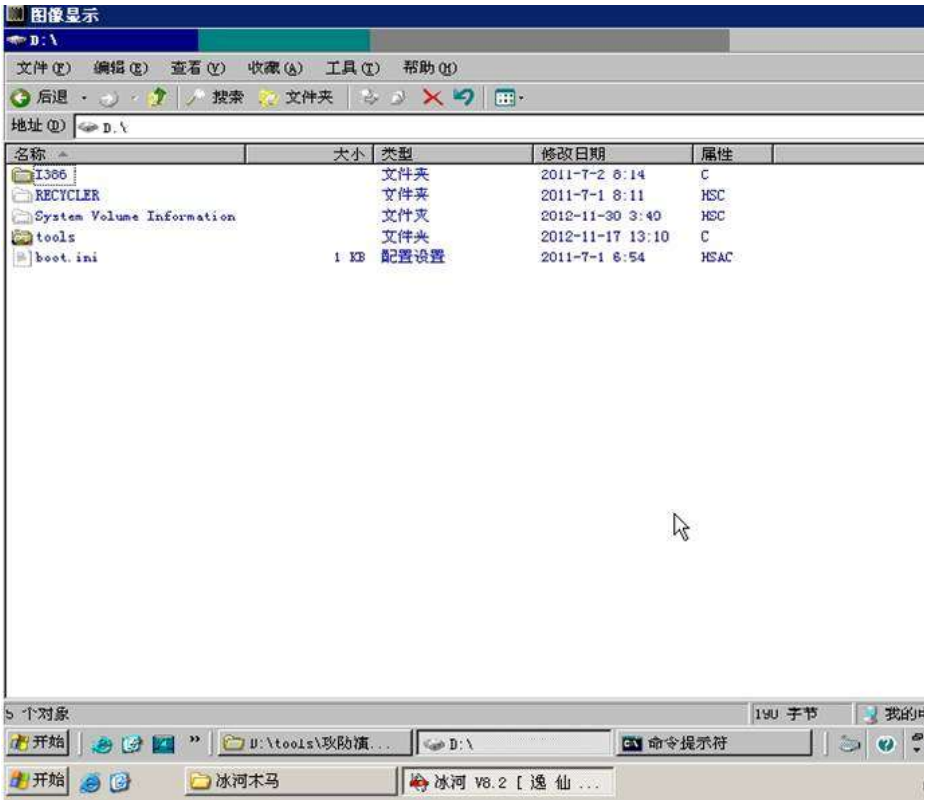
20、在受控端计算机中进行查看，可以发现在相应的文件夹中确实多了一个刚复制的文件，该图
中文件夹。



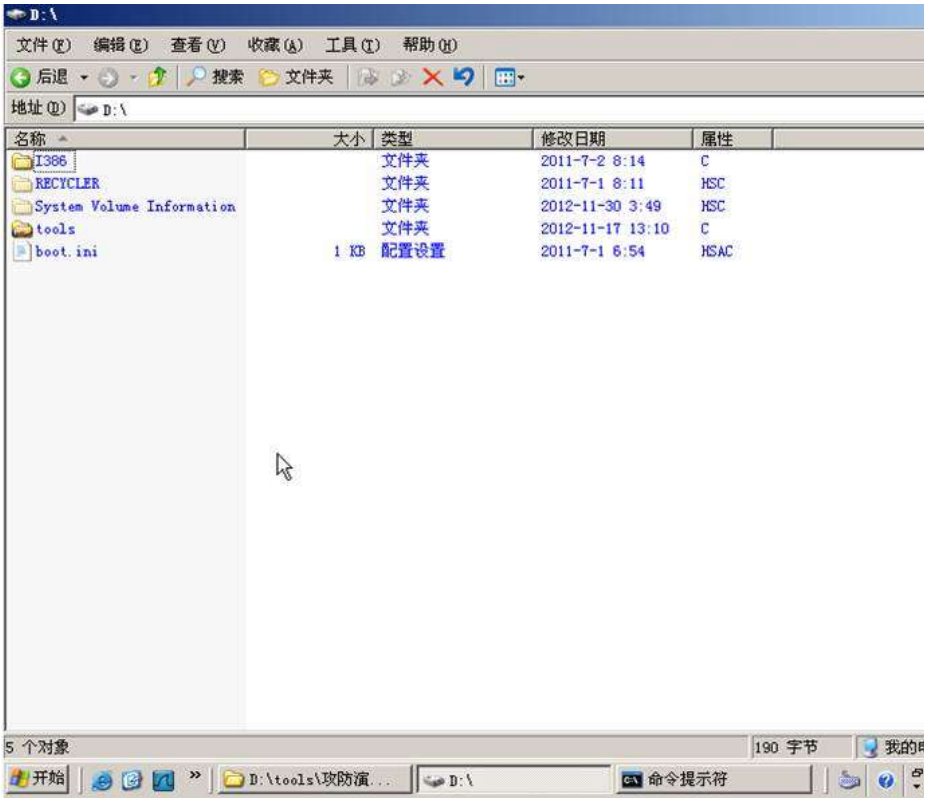
21、我们可以在主控端计算机上观看受控端计算机的屏幕，方法见图

22、这时在屏幕的左上角有一个窗口，该窗口中的图像即受控端计算机的屏幕。

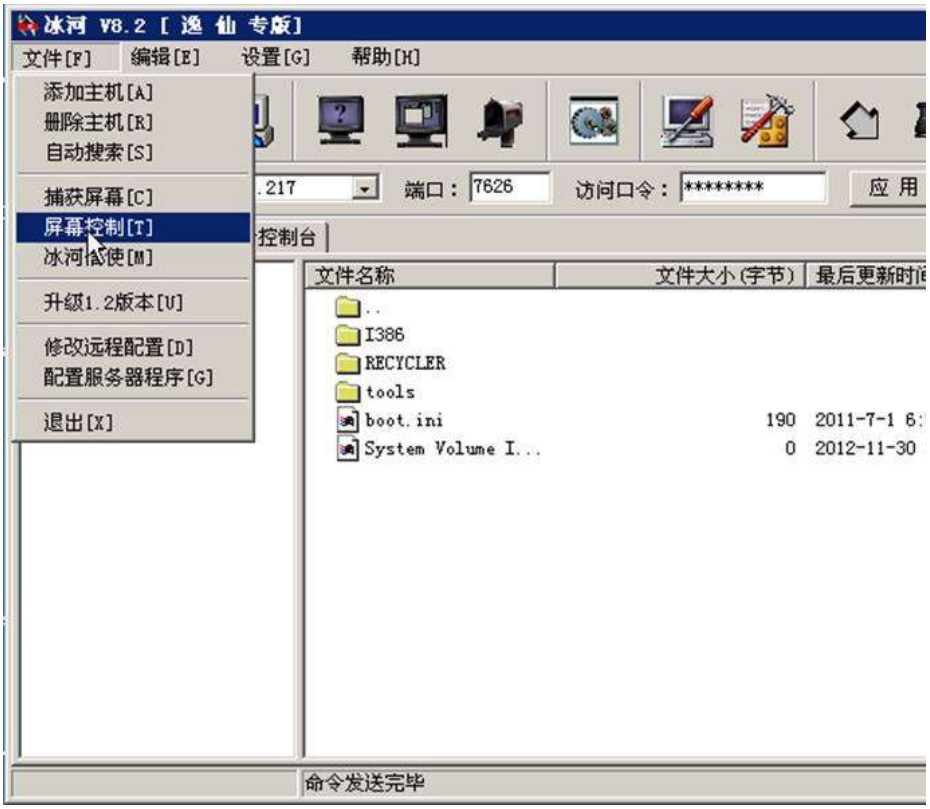
23、我们将左上角的窗口全屏显示，可得如图所示（屏幕的具体状态应视具体实验而不同）。

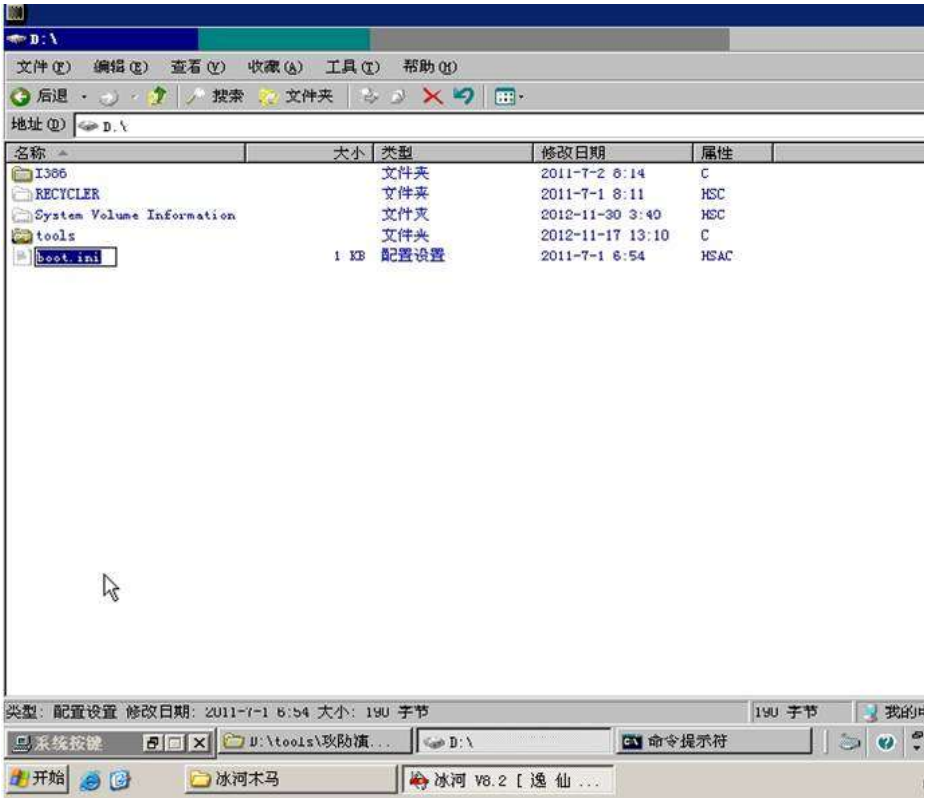


24、我们在受控端计算机上进行验证发现：主控端捕获的屏幕和受控端上的屏幕非常吻合。见图



25、我们可以通过屏幕来对受控端计算机进行控制，方法见图，进行控制时，我们会发现操作远程
在本地机进行操作一样。

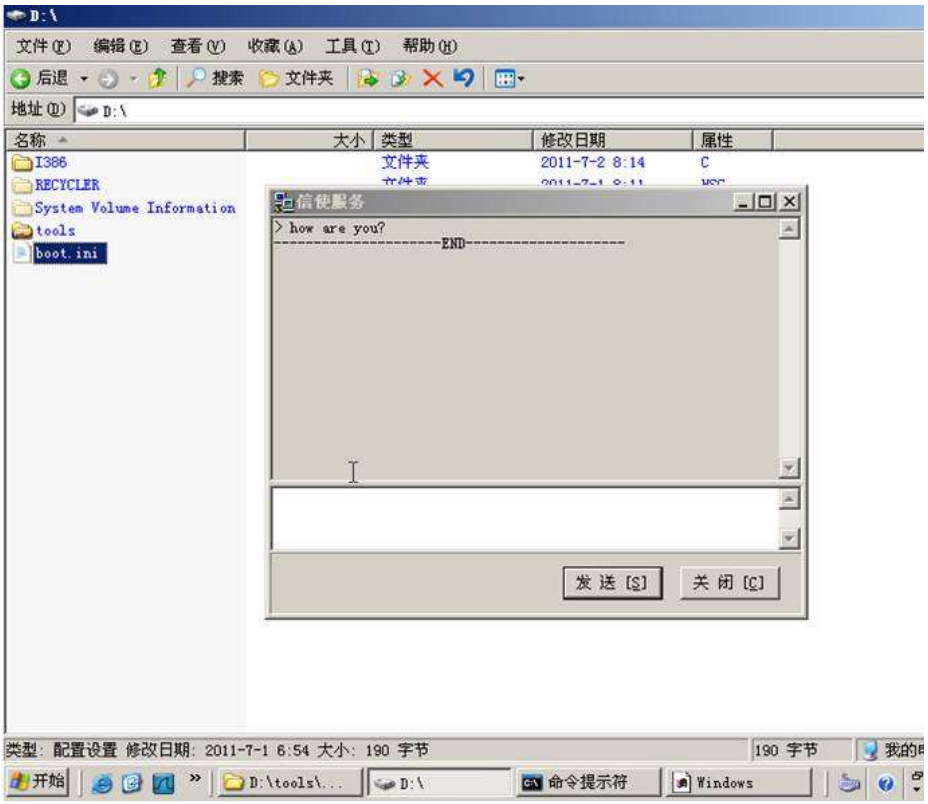




26、我们还可以通过冰河信使功能和服务器方进行聊天，具体见图，当主控端发起信使通信之后，向主控端发送消息了。


冰河 V8.2 [逸 仙 专版]
文件[F] 编辑[E] 设置[G] 帮助[H]
添加主机[A]
删除主机[R]
自动搜索[S]
捕获屏幕[C]
屏幕控制[T]
冰河信使[M]
升级1.2版本[U]
修改远程配置[D]
配置服务器程序[G]
退出[X]
端口：7626
访问口令：********
应 用 [S]
控制台
文件名称
文件大小(字节)
最后更新时间
I386
RECYCLER
tools
boot.ini 190 2011-7-1 6:54:34
System Volume I... 0 2012-11-30 3:49:02
命令发送完毕


冰河信使
> how are you?
----------END----------
发 送 [S]
关 闭 [C]
信息已被接收



27、 实验小结

通过本次实验，我们可以学会冰河木马的使用，从而理解木马的工作原理及木马的本来面目。