编号：_____

| 实验 | 一 | 二 | 三 | 四 | 五 | 六 | 七 | 八 | 总评 | 教师签名 |
|---|---|---|---|---|---|---|---|---|---|---|
| 成绩 | | | | | | | | | | |

武汉大学国家网络安全学院

# 课程实验(设计)报告

课程名称 ：软件安全实验

实验内容 ：实验四 恶意软件样本行为分析

专业(班) ：_____

学　　号 ：_____

姓　　名 ：_____

任课教师 ：_____

# 目 录

# 实验 4　恶意软件样本行为分析

## 4.1 实验名称

## 4.2 实验目的

## 4.3 实验步骤及内容

**第一阶段：熟悉 Process Moniter 的使用**

- 利用 Process Moniter 监视 WinRAR 的解压缩过程。
- 利用 Process Moniter 分析 WinRAR 的临时文件存放在哪个文件夹中。
- WinRAR 压缩包内文件直接打开后，有两种关闭方式：先关闭打开的文件，再关闭打开的压缩包。另外一种方式是先关闭打开的压缩包，再关闭打开的文件。利用 Process Moniter 分析上述两种方式的异同点。

**第二阶段：熟悉抓包工具 Wireshark 的使用**

- 熟悉 Wireshark 软件的使用，着重掌握 Wireshark 的过滤器使用。
- 使用 Wireshark 抓取登录珞珈山水 BBS 的数据包，并通过分析数据包获得用户名和密码。

**第三阶段：VMware 的熟悉和使用**

- 着重掌握 VMware 的网络设置方式，主要有 NAT 连接、桥接和 Host-Only 模式。
- 配置自己的木马分析环境。

**第四阶段：灰鸽子木马的行为分析**

- 熟悉灰鸽子木马的使用，利用灰鸽子木马控制虚拟机。
- 利用 Process Moniter 监控感染灰鸽子木马的被控端的文件行为和注册表行为。
- 利用 Wireshark 监控灰鸽子木马与控制端的网络通信。
- 提出灰鸽子木马的清除方案。

**第五阶段：课后习题思考与实践**

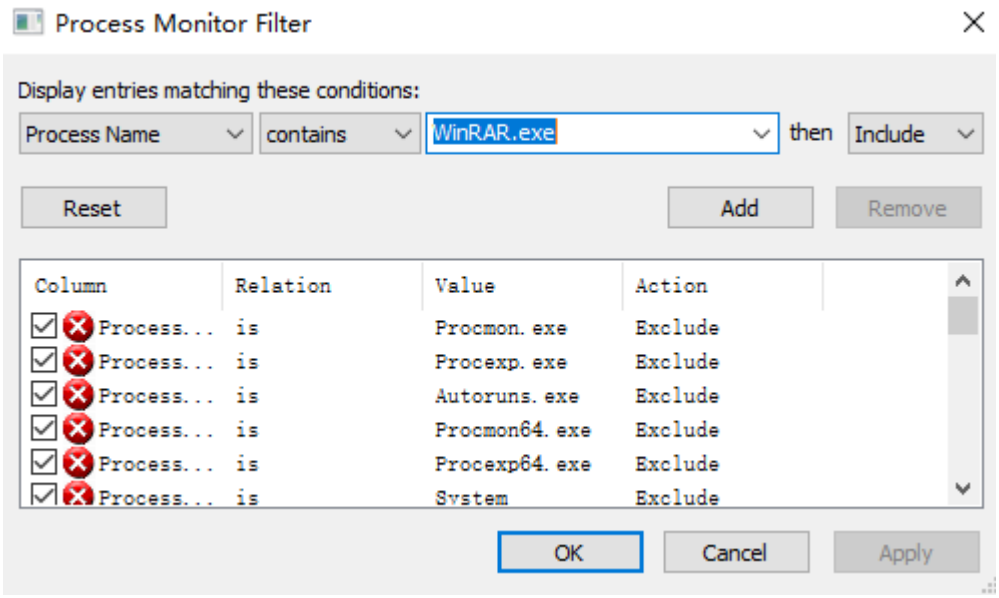
- 尝试对大白鲨木马或 PCShare 木马进行行为分析。

## 4.4 实验关键过程、数据及其分析

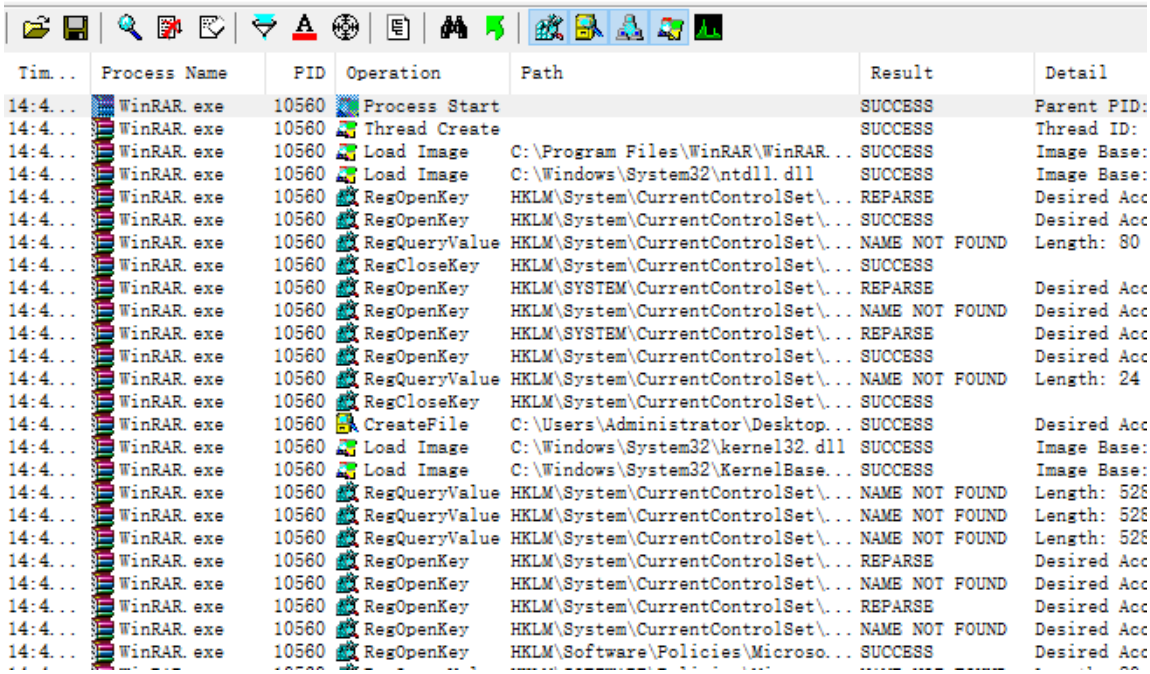
**第一阶段：熟悉 Process Moniter 的使用**

- 利用 Process Moniter 监视 WinRAR 的解压缩过程。

打开 Process Monitor,设置过滤器，选择 Process Name 指定为 WinRAR



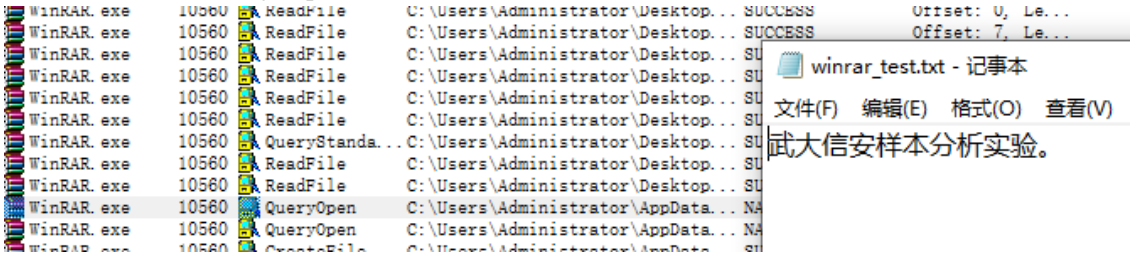

接着测试解压实验工具中的 winrar_test.rar 压缩包，同时检测 Process Monitor 的监控信息，可以发现成功捕获到了 WinRAR 解压缩过程。



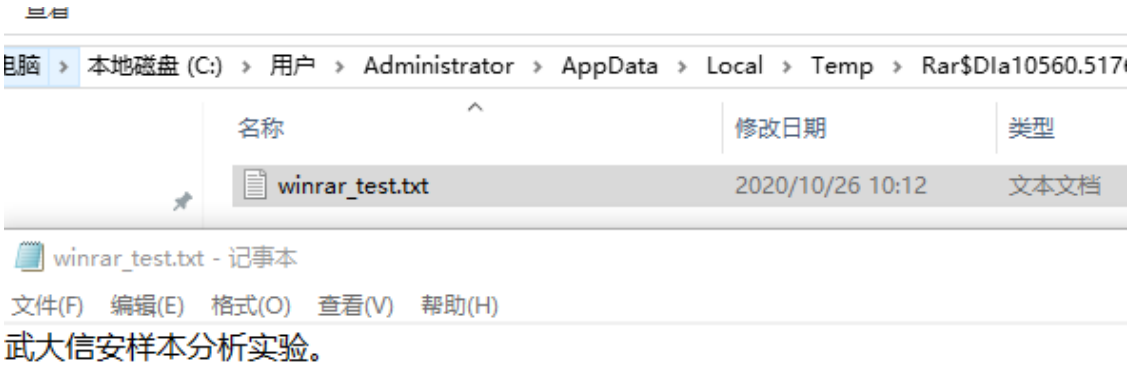
| Tim... | Process Name | PID | Operation | Path | Result | Detail |
|---|---|---|---|---|---|---|
| 14:4... | WinRAR.exe | 10560 | Process Start | | SUCCESS | Parent PID: |
| 14:4... | WinRAR.exe | 10560 | Thread Create | | SUCCESS | Thread ID: |
| 14:4... | WinRAR.exe | 10560 | Load Image | C:\Program Files\WinRAR\WinRAR... | SUCCESS | Image Base: |
| 14:4... | WinRAR.exe | 10560 | Load Image | C:\Windows\System32\ntdll.dll | SUCCESS | Image Base: |
| 14:4... | WinRAR.exe | 10560 | RegOpenKey | HKLM\System\CurrentControlSet\... | REPARSE | Desired Acc |
| 14:4... | WinRAR.exe | 10560 | RegOpenKey | HKLM\System\CurrentControlSet\... | SUCCESS | Desired Acc |
| 14:4... | WinRAR.exe | 10560 | RegQueryValue | HKLM\System\CurrentControlSet\... | NAME NOT FOUND | Length: 80 |
| 14:4... | WinRAR.exe | 10560 | RegCloseKey | HKLM\System\CurrentControlSet\... | SUCCESS | |
| 14:4... | WinRAR.exe | 10560 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\... | REPARSE | Desired Acc |
| 14:4... | WinRAR.exe | 10560 | RegOpenKey | HKLM\System\CurrentControlSet\... | NAME NOT FOUND | Desired Acc |
| 14:4... | WinRAR.exe | 10560 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\... | REPARSE | Desired Acc |
| 14:4... | WinRAR.exe | 10560 | RegOpenKey | HKLM\System\CurrentControlSet\... | SUCCESS | Desired Acc |
| 14:4... | WinRAR.exe | 10560 | RegQueryValue | HKLM\System\CurrentControlSet\... | NAME NOT FOUND | Length: 24 |
| 14:4... | WinRAR.exe | 10560 | RegCloseKey | HKLM\System\CurrentControlSet\... | SUCCESS | |
| 14:4... | WinRAR.exe | 10560 | CreateFile | C:\Users\Administrator\Desktop... | SUCCESS | Desired Acc |
| 14:4... | WinRAR.exe | 10560 | Load Image | C:\Windows\System32\kernel32.dll | SUCCESS | Image Base: |
| 14:4... | WinRAR.exe | 10560 | Load Image | C:\Windows\System32\KernelBase... | SUCCESS | Image Base: |
| 14:4... | WinRAR.exe | 10560 | RegQueryValue | HKLM\System\CurrentControlSet\... | NAME NOT FOUND | Length: 528 |
| 14:4... | WinRAR.exe | 10560 | RegQueryValue | HKLM\System\CurrentControlSet\... | NAME NOT FOUND | Length: 528 |
| 14:4... | WinRAR.exe | 10560 | RegQueryValue | HKLM\System\CurrentControlSet\... | NAME NOT FOUND | Length: 528 |
| 14:4... | WinRAR.exe | 10560 | RegOpenKey | HKLM\System\CurrentControlSet\... | REPARSE | Desired Acc |
| 14:4... | WinRAR.exe | 10560 | RegOpenKey | HKLM\System\CurrentControlSet\... | NAME NOT FOUND | Desired Acc |
| 14:4... | WinRAR.exe | 10560 | RegOpenKey | HKLM\System\CurrentControlSet\... | REPARSE | Desired Acc |
| 14:4... | WinRAR.exe | 10560 | RegOpenKey | HKLM\System\CurrentControlSet\... | NAME NOT FOUND | Desired Acc |
| 14:4... | WinRAR.exe | 10560 | RegOpenKey | HKLM\Software\Policies\Microso... | SUCCESS | Desired Acc |

- 利用 Process Moniter 分析 WinRAR 的临时文件存放在哪个文件夹中。

通过查看创建文件的操作对进程过滤，可以发现 WinRAR 相关的文件开启进程操作，进而发现临时路径，右键 jump to，跳转到改路径

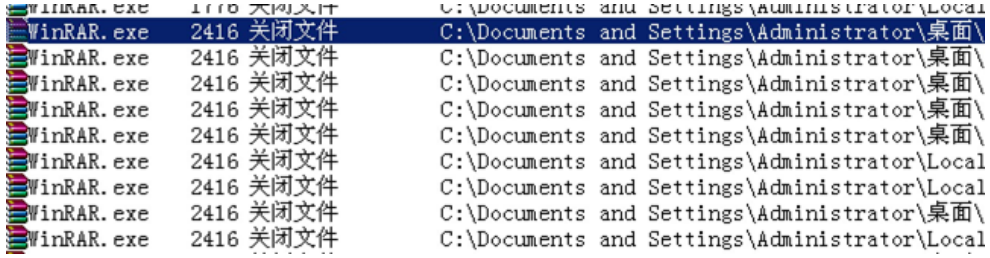



可以看到 WinRAR 的解压缩临时路径如下：

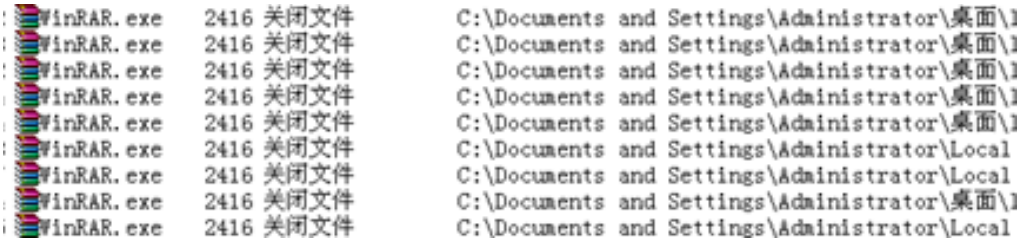



- WinRAR 压缩包内文件直接打开后，有两种关闭方式：先关闭打开的文件，再关闭打开的压缩包。另外一种方式是先关闭打开的压缩包，再关闭打开的文件。利用 Process Moniter 分析上述两种方式的异同点。

测试先关闭文件，再关闭压缩包，PM 检测情况如下：




测试先关闭压缩包，再关闭文件，PM 检测情况如下：



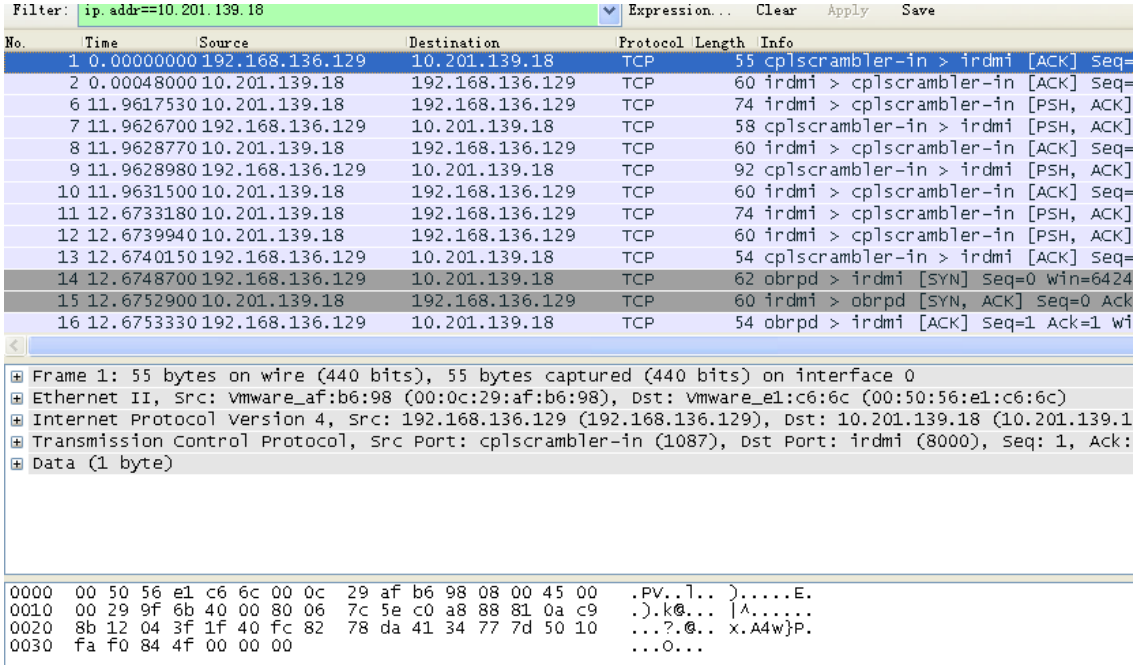

实验结果显示文件是.txt 时两种方式没有明显的区别。两种方式 WinRAR 的文件临时保存地

址略有不同。另外，若文件是.doc 类型，如果先关闭压缩包再关闭 doc 文档会导致文件存储失败。

**第二阶段：熟悉抓包工具 Wireshark 的使用**

- 熟悉 Wireshark 软件的使用，着重掌握 Wireshark 的过滤器使用。

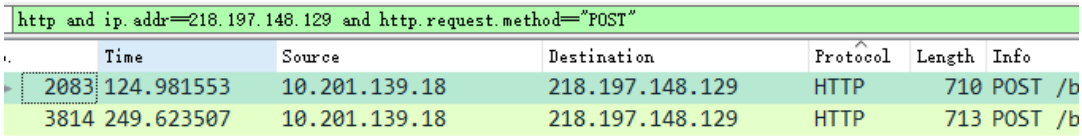
进入 Wireshark 主界面选择以太网，点击 start 即开始抓包。



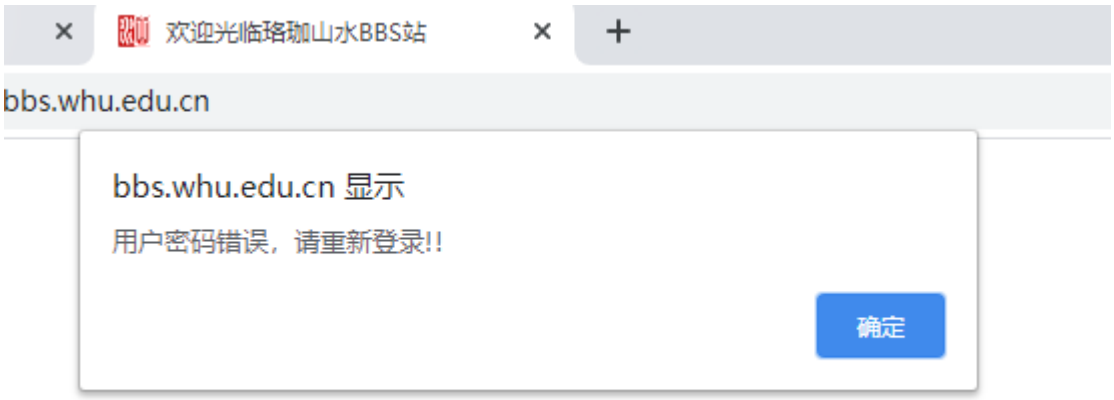

- 使用 Wireshark 抓取登录珞珈山水 BBS 的数据包，并通过分析数据包获得用户名和密码。

使用浏览器访问 bbs.whu.edu.cn，开始抓包

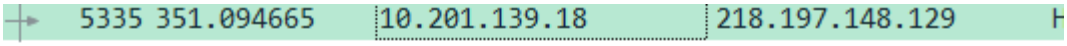

通过站长之家查看 bbs 的 ip，配置 Wireshark 的过滤器，仅抓取指定的包如下：




随便输入一串用户名和密码，抓取 POST 包，BBS 反馈密码错误



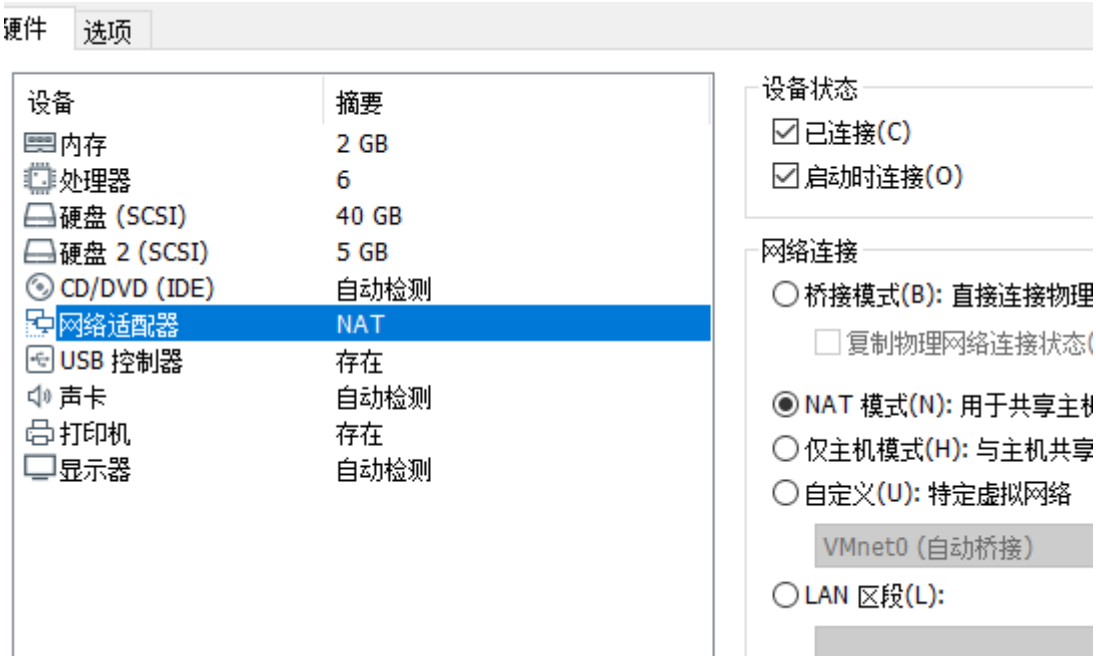

打开 Wireshark，浏览刚才抓到的指定过滤类型包，可以看见成功抓取了用户名和密码




**第三阶段：VMware 的熟悉和使用**

- 着重掌握 VMware 的网络设置方式，主要有 NAT 连接、桥接和 Host-Only 模式。

启动 VMWare，进入虚拟机配置界面，将虚拟机配置成 NAT 模式




使用 cmd+ipconfig 查看客户端机的 IPv4 地址并记录，为接下来的木马安装做好准备

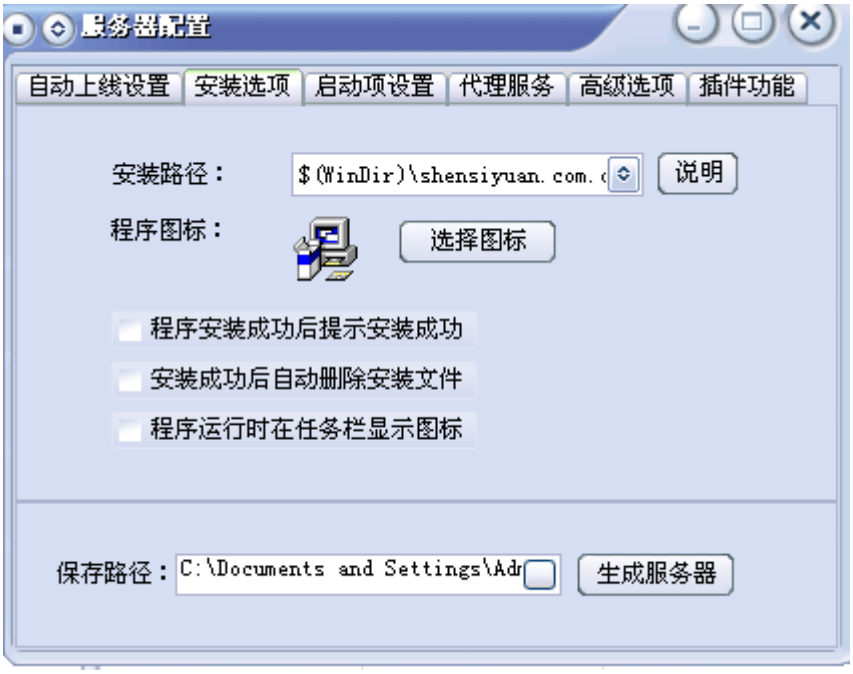
- 配置自己的木马分析环境。

在本次实验中，木马受害机处于 VMware 虚拟机中，主机为客户端机。为虚拟机安装 Wireshark，Process Monitor 用于木马行为分析。

**第四阶段：灰鸽子木马的行为分析**

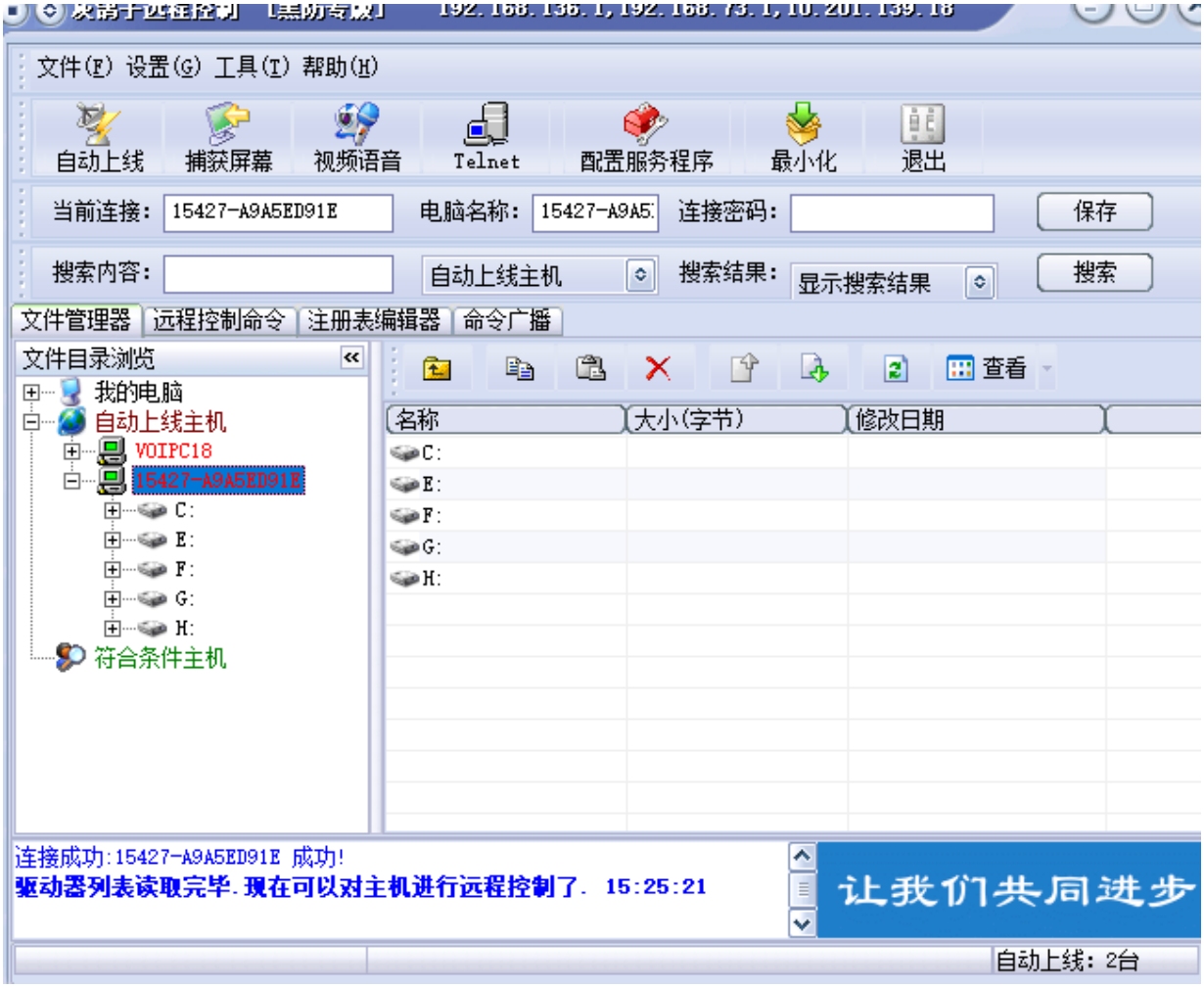
- 熟悉灰鸽子木马的使用，利用灰鸽子木马控制虚拟机。

主机安装灰鸽子客户端，进入主界面，选择服务器配置，根据前一节获取的主机 ip 地址，配置服务器如下




将生成的 server.exe 发送到受害机，点击运行，显示成功安装，此时受害机已经成功感染木马。

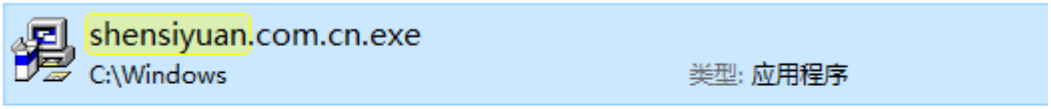
在主机中打开客户端可以看到木马机已经上线可以对其进行控制。




测试捕获屏幕，可以发现已经实现了对受害机的完全控制。

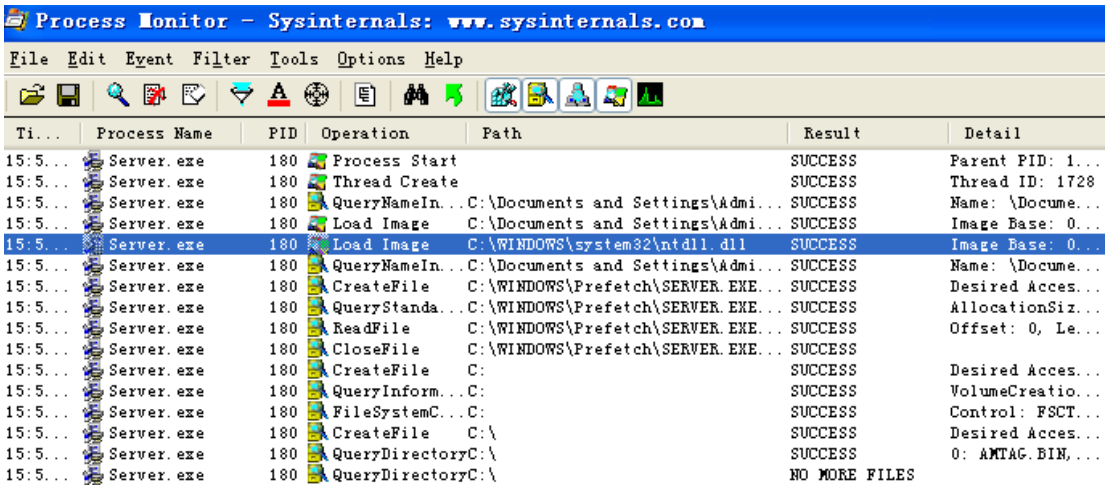
- 利用 Process Moniter 监控感染灰鸽子木马的被控端的文件行为和注册表行为。

查看系统目录下由灰鸽子生成的程序文件，这里使用了我的姓名作为名称



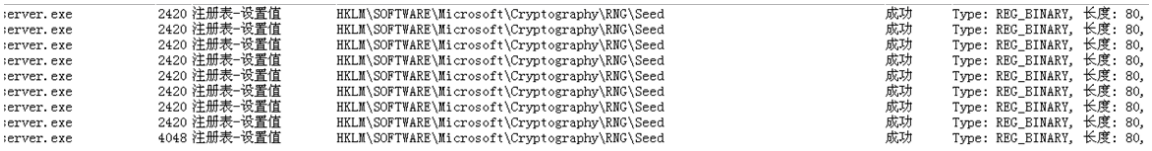
```
shensiyuan.com.cn.exe
C:\Windows                                   类型: 应用程序
```

在 Process Moniter 过滤器中设置过滤行为，过滤出包口 server 的进程,查看服务端



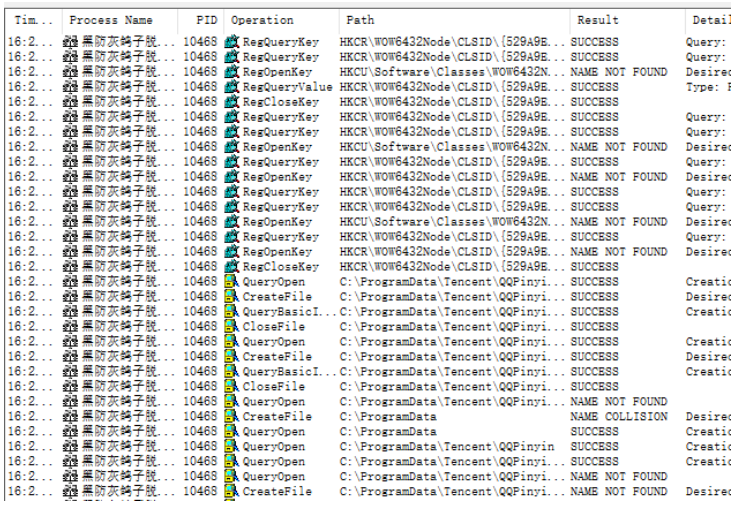
```
Ti...  Process Name  PID  Operation       Path                               Result         Detail
15:5... Server.exe   180  Process Start                                      SUCCESS        Parent PID: 1...
15:5... Server.exe   180  Thread Create                                      SUCCESS        Thread ID: 1728
15:5... Server.exe   180  QueryNameIn...C:\Documents and Settings\Admi...    SUCCESS        Name: \Docume...
15:5... Server.exe   180  Load Image    C:\Documents and Settings\Admi...    SUCCESS        Image Base: 0...
15:5... Server.exe   180  Load Image    C:\WINDOWS\system32\ntdll.dll        SUCCESS        Image Base: 0...
15:5... Server.exe   180  QueryNameIn...C:\Documents and Settings\Admi...    SUCCESS        Name: \Docume...
15:5... Server.exe   180  CreateFile    C:\WINDOWS\Prefetch\SERVER.EXE...    SUCCESS        Desired Acces...
15:5... Server.exe   180  QueryStanda...C:\WINDOWS\Prefetch\SERVER.EXE...    SUCCESS        AllocationSiz...
15:5... Server.exe   180  ReadFile      C:\WINDOWS\Prefetch\SERVER.EXE...    SUCCESS        Offset: 0, Le...
15:5... Server.exe   180  CloseFile     C:\WINDOWS\Prefetch\SERVER.EXE...    SUCCESS
15:5... Server.exe   180  CreateFile    C:                                   SUCCESS        Desired Acces...
15:5... Server.exe   180  QueryInform...C:                                   SUCCESS        VolumeCreatio...
15:5... Server.exe   180  FileSystemC...C:                                   SUCCESS        Control: FSCT...
15:5... Server.exe   180  CreateFile    C:\                                  SUCCESS        Desired Acces...
15:5... Server.exe   180  QueryDirectoryC:\                                  SUCCESS        0: AMTAG.BIN,...
15:5... Server.exe   180  QueryDirectoryC:\                                  NO MORE FILES
```

观察其注册表行为



```
erver.exe    2420 注册表-设置值    HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed    成功    Type: REG_BINARY, 长度: 80,
erver.exe    2420 注册表-设置值    HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed    成功    Type: REG_BINARY, 长度: 80,
erver.exe    2420 注册表-设置值    HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed    成功    Type: REG_BINARY, 长度: 80,
erver.exe    2420 注册表-设置值    HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed    成功    Type: REG_BINARY, 长度: 80,
erver.exe    2420 注册表-设置值    HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed    成功    Type: REG_BINARY, 长度: 80,
erver.exe    2420 注册表-设置值    HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed    成功    Type: REG_BINARY, 长度: 80,
erver.exe    2420 注册表-设置值    HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed    成功    Type: REG_BINARY, 长度: 80,
erver.exe    2420 注册表-设置值    HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed    成功    Type: REG_BINARY, 长度: 80,
erver.exe    4048 注册表-设置值    HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed    成功    Type: REG_BINARY, 长度: 80,
```

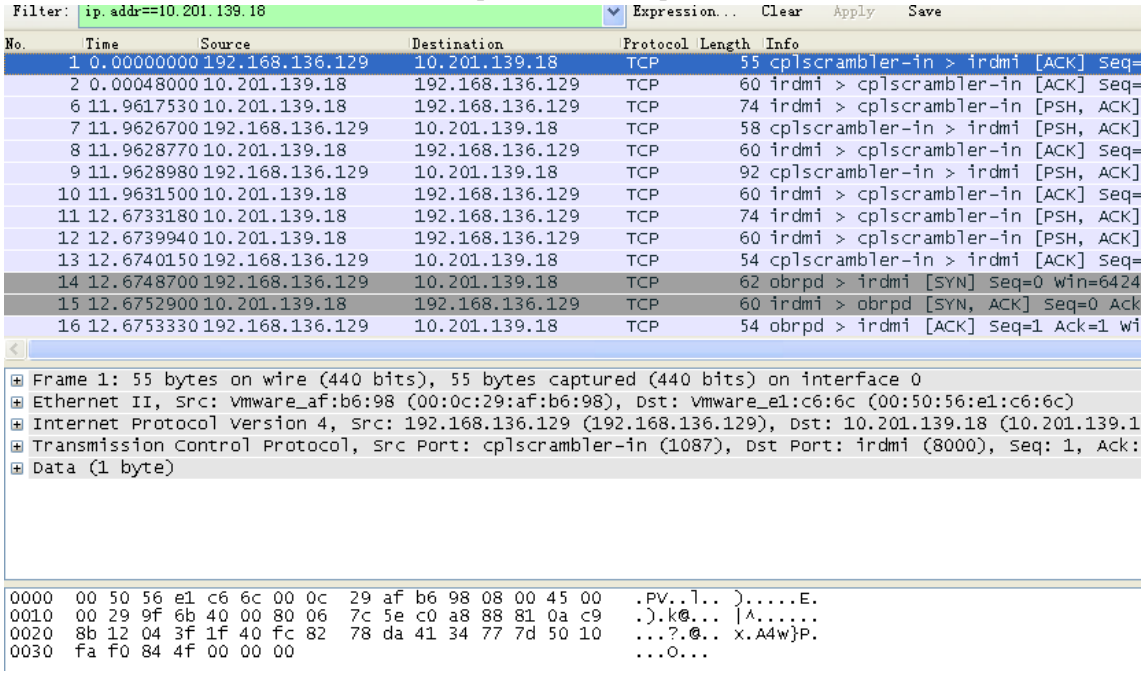
观察客户端文件操作行为



```
Tim...  Process Name      PID    Operation      Path                                Result            Detai
16:2... 黑防灰鸽子脱...  10468  RegQueryKey    HKCR\WOW6432Node\CLSID\{529A9E...   SUCCESS           Query:
16:2... 黑防灰鸽子脱...  10468  RegQueryKey    HKCR\WOW6432Node\CLSID\{529A9E...   SUCCESS           Query:
16:2... 黑防灰鸽子脱...  10468  RegOpenKey     HKCU\Software\Classes\WOW6432N...   NAME NOT FOUND    Desire
16:2... 黑防灰鸽子脱...  10468  RegQueryValue  HKCR\WOW6432Node\CLSID\{529A9E...   SUCCESS           Type:
16:2... 黑防灰鸽子脱...  10468  RegCloseKey    HKCR\WOW6432Node\CLSID\{529A9E...   SUCCESS
16:2... 黑防灰鸽子脱...  10468  RegQueryKey    HKCR\WOW6432Node\CLSID\{529A9E...   SUCCESS           Query:
16:2... 黑防灰鸽子脱...  10468  RegQueryKey    HKCR\WOW6432Node\CLSID\{529A9E...   SUCCESS           Query:
16:2... 黑防灰鸽子脱...  10468  RegOpenKey     HKCU\Software\Classes\WOW6432N...   NAME NOT FOUND    Desire
16:2... 黑防灰鸽子脱...  10468  RegQueryKey    HKCR\WOW6432Node\CLSID\{529A9E...   SUCCESS           Query:
16:2... 黑防灰鸽子脱...  10468  RegOpenKey     HKCR\WOW6432Node\CLSID\{529A9E...   NAME NOT FOUND    Desire
16:2... 黑防灰鸽子脱...  10468  RegQueryKey    HKCR\WOW6432Node\CLSID\{529A9E...   SUCCESS           Query:
16:2... 黑防灰鸽子脱...  10468  RegQueryKey    HKCR\WOW6432Node\CLSID\{529A9E...   SUCCESS           Query:
16:2... 黑防灰鸽子脱...  10468  RegOpenKey     HKCU\Software\Classes\WOW6432N...   NAME NOT FOUND    Desire
16:2... 黑防灰鸽子脱...  10468  RegQueryKey    HKCR\WOW6432Node\CLSID\{529A9E...   SUCCESS           Query:
16:2... 黑防灰鸽子脱...  10468  RegOpenKey     HKCR\WOW6432Node\CLSID\{529A9E...   NAME NOT FOUND    Desire
16:2... 黑防灰鸽子脱...  10468  RegCloseKey    HKCR\WOW6432Node\CLSID\{529A9E...   SUCCESS
16:2... 黑防灰鸽子脱...  10468  QueryOpen      C:\ProgramData\Tencent\QQPinyi...   SUCCESS           Creati
16:2... 黑防灰鸽子脱...  10468  CreateFile     C:\ProgramData\Tencent\QQPinyi...   SUCCESS           Desire
16:2... 黑防灰鸽子脱...  10468  QueryBasicI... C:\ProgramData\Tencent\QQPinyi...   SUCCESS           Creati
16:2... 黑防灰鸽子脱...  10468  CloseFile      C:\ProgramData\Tencent\QQPinyi...   SUCCESS
16:2... 黑防灰鸽子脱...  10468  QueryOpen      C:\ProgramData\Tencent\QQPinyi...   SUCCESS           Creati
16:2... 黑防灰鸽子脱...  10468  CreateFile     C:\ProgramData\Tencent\QQPinyi...   SUCCESS           Desire
16:2... 黑防灰鸽子脱...  10468  QueryBasicI... C:\ProgramData\Tencent\QQPinyi...   SUCCESS           Creati
16:2... 黑防灰鸽子脱...  10468  CloseFile      C:\ProgramData\Tencent\QQPinyi...   SUCCESS
16:2... 黑防灰鸽子脱...  10468  QueryOpen      C:\ProgramData\Tencent\QQPinyi...   NAME NOT FOUND
16:2... 黑防灰鸽子脱...  10468  CreateFile     C:\ProgramData                      NAME COLLISION    Desire
16:2... 黑防灰鸽子脱...  10468  QueryOpen      C:\ProgramData                      SUCCESS           Creati
16:2... 黑防灰鸽子脱...  10468  QueryOpen      C:\ProgramData\Tencent\QQPinyin     SUCCESS           Creati
16:2... 黑防灰鸽子脱...  10468  QueryOpen      C:\ProgramData\Tencent\QQPinyi...   SUCCESS           Creati
16:2... 黑防灰鸽子脱...  10468  QueryOpen      C:\ProgramData\Tencent\QQPinyi...   NAME NOT FOUND
16:2... 黑防灰鸽子脱...  10468  CreateFile     C:\ProgramData\Tencent\QQPinyi...   NAME NOT FOUND    Desire
```

- 利用 Wireshark 监控灰鸽子木马与控制端的网络通信。

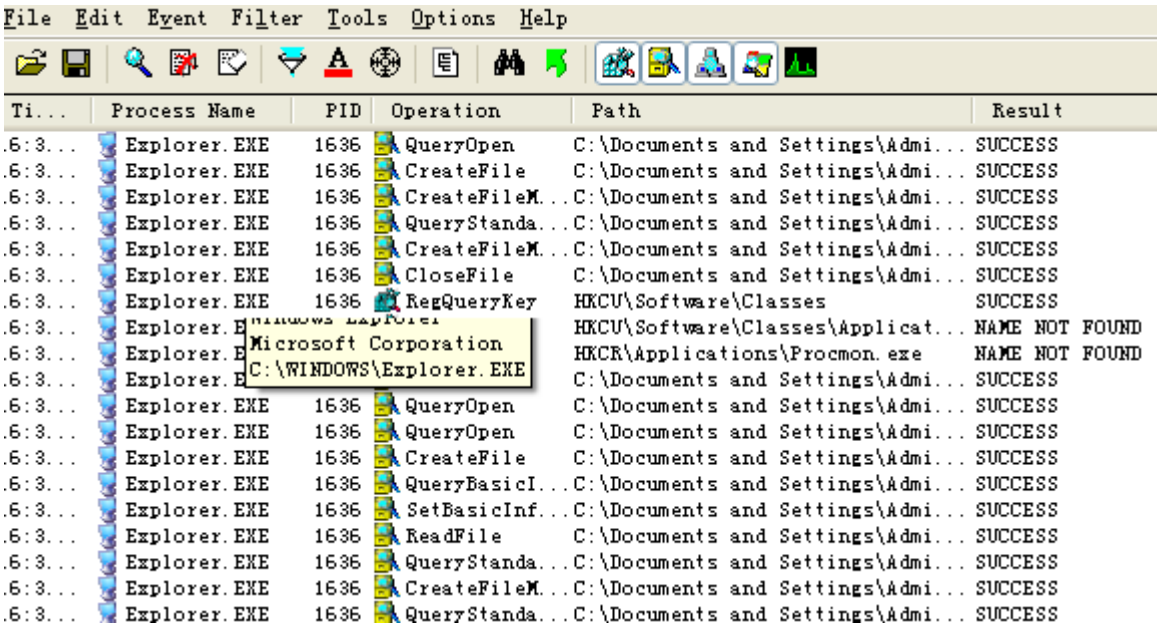
在 Wireshark 中，设置过滤器，指定 ip 地址为主机 ip，查看数据包



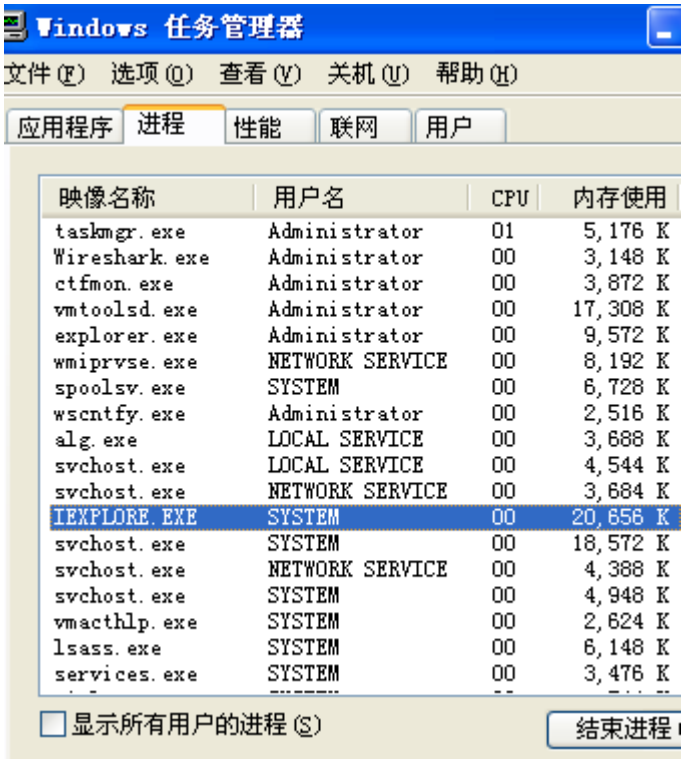

这说明灰鸽子木马采用的是 TCP 协议进行的通信。

- 提出灰鸽子木马的清除方案。

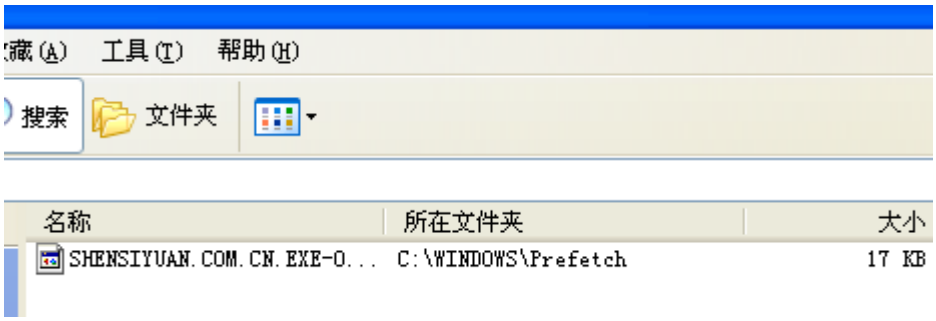
灰鸽子默认使用的是 EXPLORER.EXE 作为自己的隐藏进程，打开 PM 进行检测



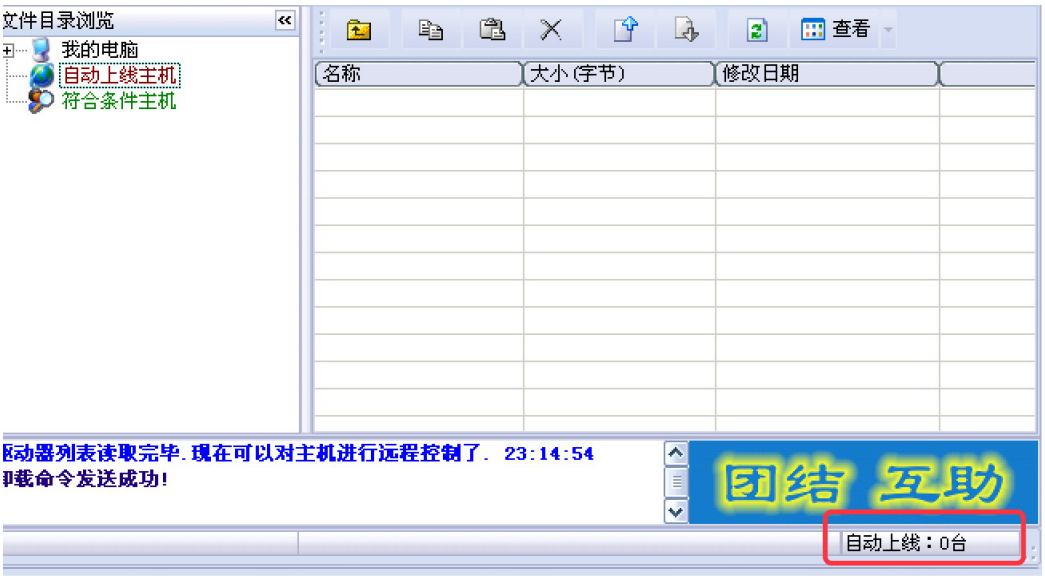

打开系统任务管理器，中止该进程，




进入系统 C 盘目录，搜索服务端程序



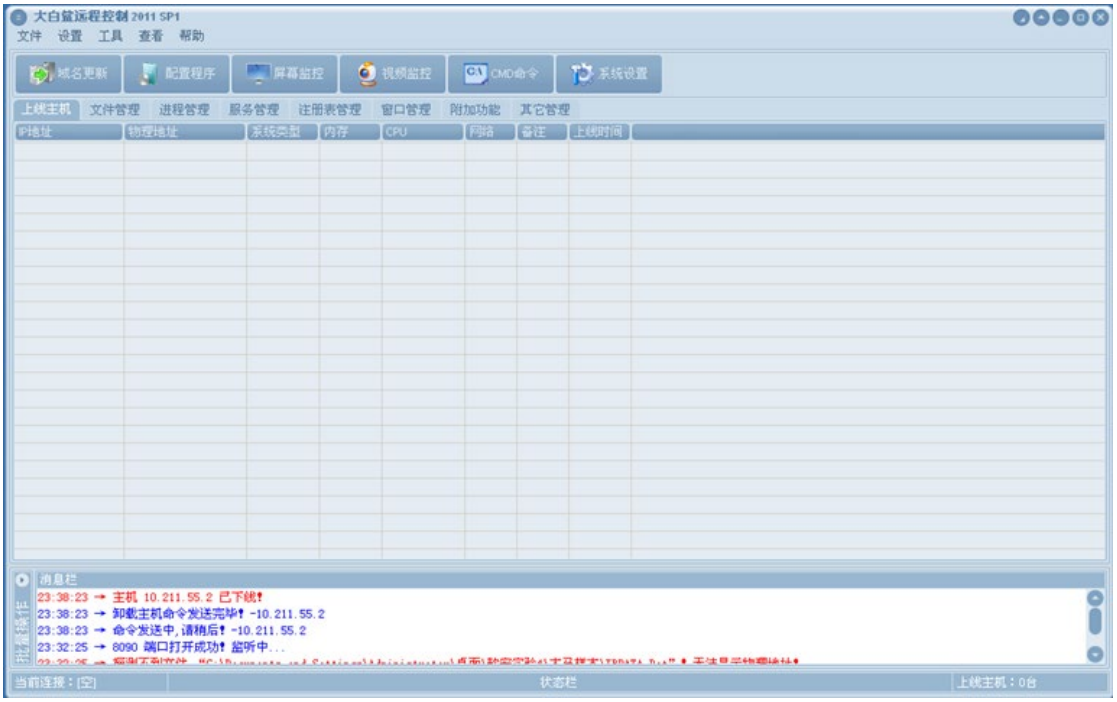

删除服务端程序，再次打开主机操作界面，可以发现此时受害机已经自动下线。



**第五阶段：课后习题思考与实践**

- 尝试对大白鲨木马或 PCShare 木马进行行为分析。

打开大白鲨木马主界面




木马配置方式与灰鸽子类似


配置完成后在受害机中安装，打开主机客户端，发现受害机上线成功

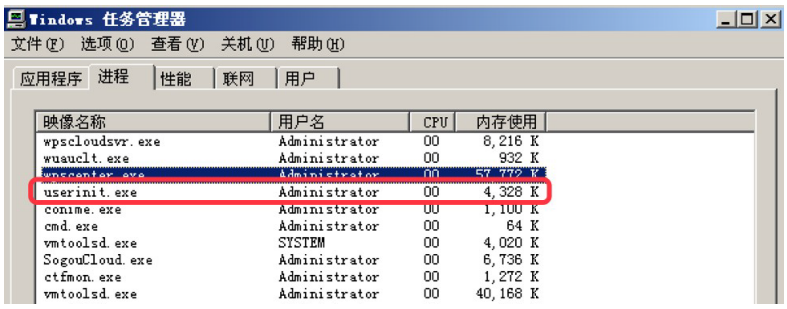

使用 Process Monitor 监控木马进程，信息如下：

| | | | | | |
|---|---|---|---|---|---|
| server.exe | 2252 | 关闭文件 | C:\WINDOWS\liuside.EXE | 成功 | |
| server.exe | 2252 | 注册表-创建项 | HKLM\SOFTWARE\Microsoft\DBS | 成功 | 访问期望: 允许的最大值 |
| server.exe | 2252 | 设置文件末尾信息-文件 | C:\WINDOWS\system32\config\software.LOG | 成功 | 文件末尾: 20,480 |
| server.exe | 2252 | 设置文件末尾信息-文件 | C:\WINDOWS\system32\config\software.LOG | 成功 | 文件末尾: 24,576 |
| server.exe | 2252 | 设置文件末尾信息-文件 | C:\WINDOWS\system32\config\software.LOG | 成功 | 文件末尾: 28,672 |
| server.exe | 2252 | 设置文件末尾信息-文件 | C:\WINDOWS\system32\config\software.LOG | 成功 | 文件末尾: 32,768 |
| server.exe | 2252 | 注册表-关闭项 | HKLM\SOFTWARE\Microsoft\DBS | 成功 | |
| server.exe | 2252 | 注册表-打开项 | HKLM\SOFTWARE\Microsoft\DBS | 成功 | 访问期望: 设置值 |
| server.exe | 2252 | 注册表-设置值 | HKLM\SOFTWARE\Microsoft\DBS\InstallTime | 成功 | Type: REG_SZ, 长度: 38, 数据: 2017 |
| server.exe | 2252 | 注册表-关闭项 | HKLM\SOFTWARE\Microsoft\DBS | 成功 | |
| server.exe | 2252 | 注册表-打开项 | HKLM\System\CurrentControlSet\Control\Session... | 成功 | 访问期望: 查询值 |
| server.exe | 2252 | 注册表-查询值 | HKLM\System\CurrentControlSet\Control\Session... | 名称未... | 长度: 16 |
| server.exe | 2252 | 注册表-关闭项 | HKLM\System\CurrentControlSet\Control\Session... | 成功 | |
| server.exe | 2252 | 查询-打开 | C:\WINDOWS\liuside.EXE | 成功 | 创建时间: 2017-5-30 23:40:27, 最后 |
| server.exe | 2252 | 查询-打开 | C:\WINDOWS\liuside.EXE | 成功 | 创建时间: 2017-5-30 23:40:27, 最后 |
| server.exe | 2252 | 创建文件 | C:\WINDOWS\liuside.EXE | 成功 | 访问期望: 读取数据/列出目录, 执行/ |
| server.exe | 2252 | 查询标准信息-文件 | C:\WINDOWS\liuside.EXE | 成功 | 分配的大小: 118,784, 文件末尾: 118, |
| server.exe | 2252 | 注册表-打开项 | HKLM\System\CurrentControlSet\Control\Session... | 名称未... | 访问期望: 查询值 |
| server.exe | 2252 | 注册表-打开项 | HKLM\System\CurrentControlSet\Control\Session... | 成功 | 访问期望: 查询值 |
| server.exe | 2252 | 注册表-查询值 | HKLM\System\CurrentControlSet\Control\Session... | 名称未... | 长度: 20 |
| server.exe | 2252 | 注册表-关闭项 | HKLM\System\CurrentControlSet\Control\Session... | 成功 | |
| server.exe | 2252 | 查询-打开 | C:\WINDOWS\system32\apphelp.dll | 成功 | 创建时间: 2008-4-14 20:00:00, 最后 |
| server.exe | 2252 | 创建文件 | C:\WINDOWS\system32\apphelp.dll | 成功 | 访问期望: 执行/遍历, 同步, 安排: 打 |
| server.exe | 2252 | 查询标准信息-文件 | C:\WINDOWS\system32\apphelp.dll | 成功 | 分配的大小: 126,976, 文件末尾: 125, |
| server.exe | 2252 | 关闭文件 | C:\WINDOWS\system32\apphelp.dll | 成功 | |
| server.exe | 2252 | 查询-打开 | C:\WINDOWS\system32\apphelp.dll | 成功 | 创建时间: 2008-4-14 20:00:00, 最后 |
| server.exe | 2252 | 创建文件 | C:\WINDOWS\system32\apphelp.dll | 成功 | 访问期望: 执行/遍历, 同步, 安排: 打 |
| server.exe | 2252 | 关闭文件 | C:\WINDOWS\system32\apphelp.dll | 成功 | |
| server.exe | 2252 | 加载映像 | C:\WINDOWS\system32\apphelp.dll | 成功 | 映像基址: 0x76d70000, 映像大小: 0x |
| server.exe | 2252 | 注册表-打开项 | HKLM\Software\Microsoft\Windows NT\CurrentVer... | 名称未... | 访问期望: 读取 |
| server.exe | 2252 | 创建文件 | C:\WINDOWS\AppPatch\sysmain.sdb | 成功 | 访问期望: 正常读取, 安排: 打开, 选 |
| server.exe | 2252 | 查询标准信息-文件 | C:\WINDOWS\AppPatch\sysmain.sdb | 成功 | 分配的大小: 1,204,224, 文件末尾: 1, |
| server.exe | 2252 | 查询标准信息-文件 | C:\WINDOWS\AppPatch\sysmain.sdb | 成功 | 分配的大小: 1,204,224, 文件末尾: 1, |
| server.exe | 2252 | 查询标准信息-文件 | C:\WINDOWS\AppPatch\sysmain.sdb | 成功 | 分配的大小: 1,204,224, 文件末尾: 1, |
| server.exe | 2252 | 创建文件 | C:\WINDOWS\AppPatch\systest.sdb | 名称未... | 访问期望: 正常读取, 安排: 打开, 选 |
| server.exe | 2252 | 注册表-打开项 | HKLM\System\WPA\TabletPC | 名称未... | 访问期望: 查询值, WOW64_64Key |
| server.exe | 2252 | 注册表-打开项 | HKLM\SYSTEM\WPA\MediaCenter | 成功 | 访问期望: 查询值, WOW64_64Key |
| server.exe | 2252 | 注册表-查询值 | HKLM\SYSTEM\WPA\MediaCenter\Installed | 成功 | Type: REG_DWORD, 长度: 4, 数据: 0 |
| server.exe | 2252 | 注册表-关闭项 | HKLM\SYSTEM\WPA\MediaCenter | 成功 | |
| server.exe | 2252 | 创建文件 | C:\WINDOWS | 成功 | 访问期望: 读取数据/列出目录, 同步, |
| server.exe | 2252 | 查询目录 | C:\WINDOWS\liuside.EXE | 成功 | 过滤器: liuside.EXE, 1: liuside.E |

与灰鸽子类似，大白鲨也在系统盘复制了客户端程序。

使用 Wireshark 对大白鲨木马进行抓包，同样发现其采用的也是 TCP 协议。

清除大白鲨木马，与灰鸽子无法删除不同，大白鲨可以直接删除客户端程序。但是进入主机客户端发现仍然能够控制受害机。打开进程管理器。发现存在一个名叫 userinit 的进程




将其结束，回到主机服务端发现受害机已经自动下线。

## 4.5 实验体会和拓展思考

本次实验我学会了 Process Monitor 进程监视器和抓包工具 Wireshark 的使用。知道了如何利用 PM 去监视一个程序的各个进程以及执行过程。学会了如何利用工具抓包截取明文传输的信息。也让我进一步体会到了 Web 安全的重要性。一个简单的 BBS 网站采用明文传输攻击者就可以轻而易举的获取用户的明文密码，这无疑是非常危险的。

而学习灰鸽子等木马的使用则让我体会到了木马程序的威力。一个来路不明的 exe 文件仅仅执行一次就可以让恶意攻击者获取整个电脑的权限，而利用上述的工具又让我了解到了木马是如何工作的，它们的通信机制是什么。而学习木马的清除也提升了自己的安全意识。相信这些对我今后的学习和工作会有很大的帮助。