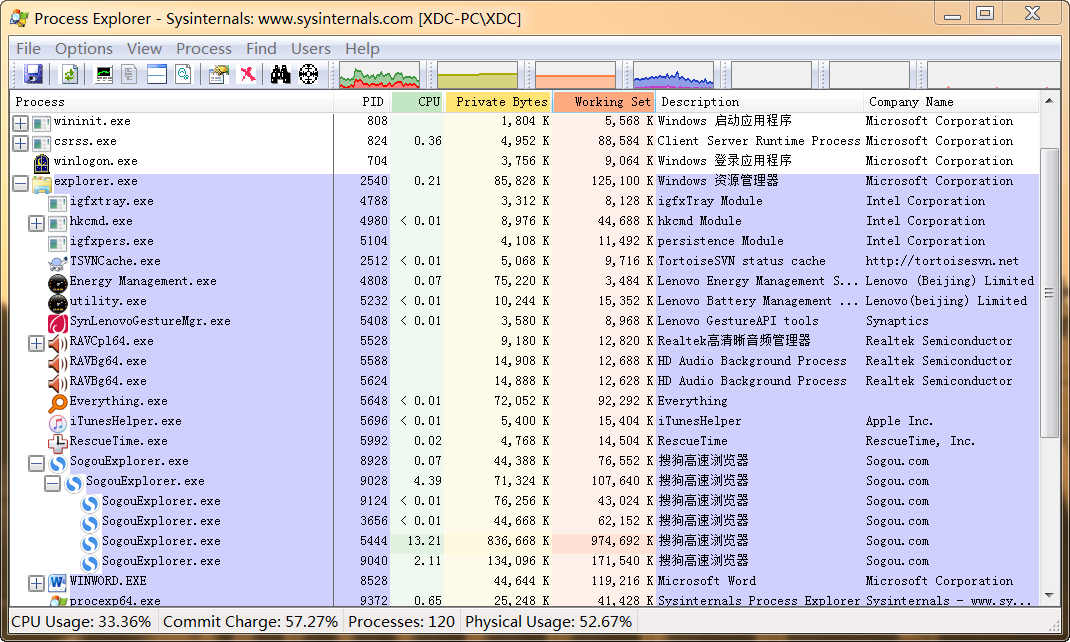
摘自：http://www.cr173.com/html/18315\_all.html

Process Explorer使用图文教程

这是一款由Sysinternals开发的Windows系统和应用程序监视工具，目前Sysinternals已经被微软收购，此款不仅结合了文件监视和注册表监视两个工具的功能，还增加了多项重要的增强功能，此工具支持64位Windows系统。

很多人可能把这款工具只当成TaskManager(任务管理器)的替代品，其实这样只能说是高射炮打蚊子，大材小用了，作为windows开发工程师，我极力推荐在[编码](http://www.cr173.com/k/bmzh/" \t "_blank)和调试过程中使用此工具，下面介绍一下Process Explorer在开发过程中的用处。

**一、树形结构界面**

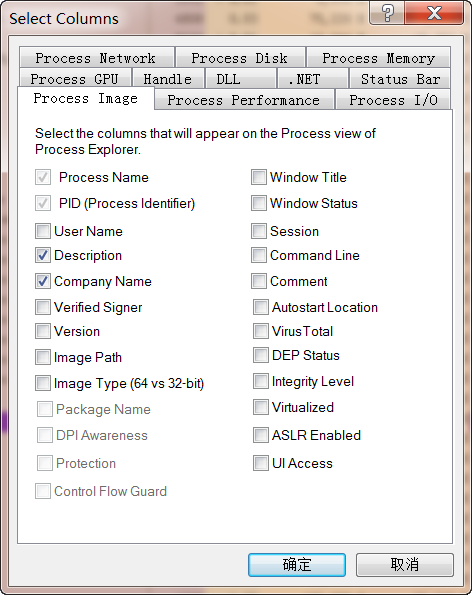


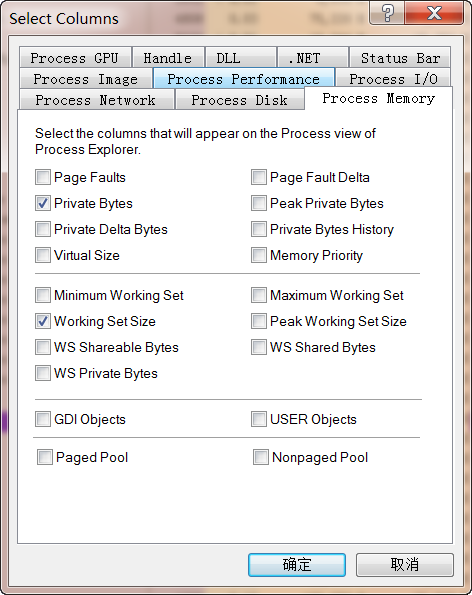
1.准确的显示的进程的父子关系。

2.通过颜色可以判断此进程处于的状态和类型，是挂起还是正在退出，是服务进程还是普通进程。

**二、显示进程的系统信息**

右键标题栏--选择Select Columns项，选择你要观察进程的某种特定的信息，这里有几个选项，常用的有Process Image和Process Memory这两个选项卡，其他的我就不截图举例了!





1.显示进程的文件路径（Image Path）

2.显示进程命令行参数(Command Line)

3.显示进程是64位进程还是32位的（Image Type）

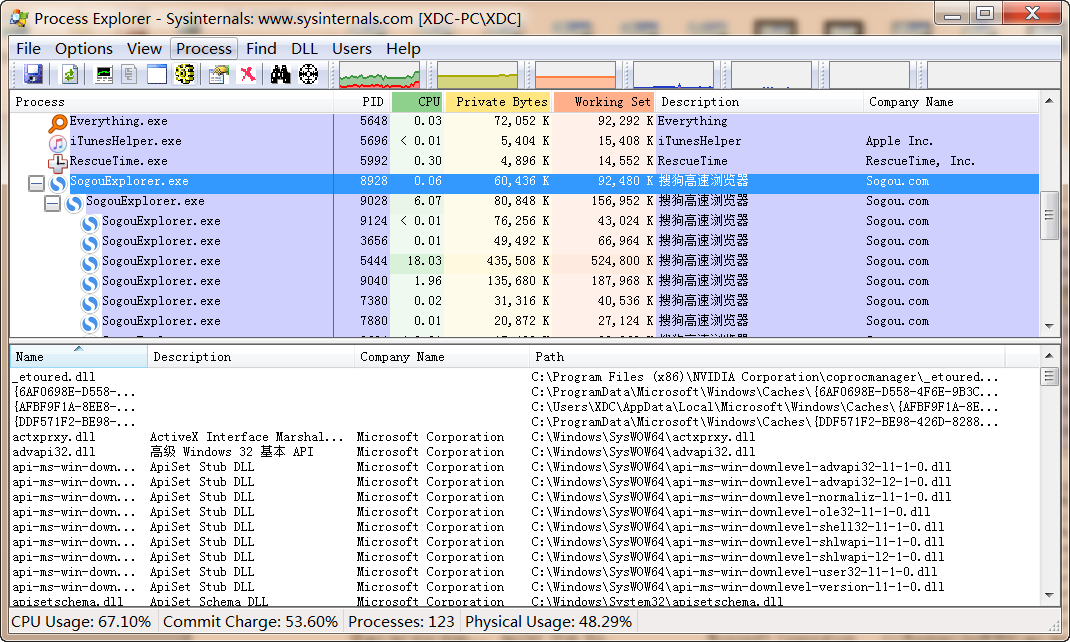
4.显示进程当前所在的Session ID（session ID）

5.显示进程当前的权限，是系统用户权限还是网络管理员权限还是普通管理员权限（User Name）

6.显示当前进程的Gdi对象个数，内核对象个数，线程个数。

**三、显示当前进程所加载的DLL**

选择View--Lower Pane View--DLLs



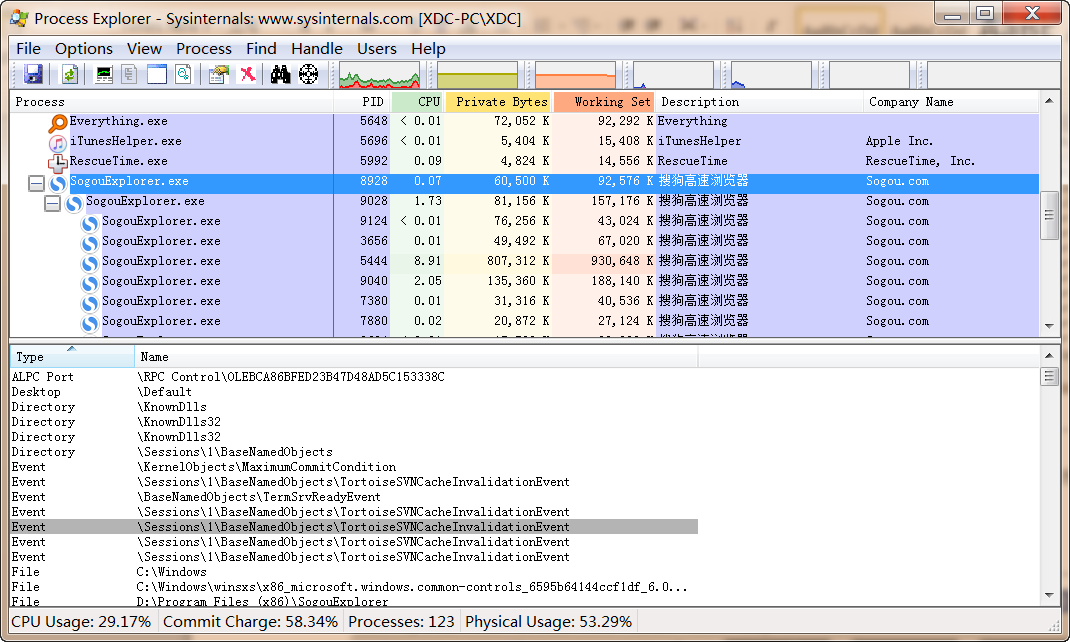
1.通过这种方式可以观察，我们的进程是否被其他程序注入DLL。

2.通过这种方式了解当前进程使用了那些编程技术，如图可见当前进程用到了Gdi+。

3.可以修改Pane View的选项卡，让其显示更多的内容，比如DLL基地址，DLL内存相关信息等。

**四、显示当前进程所占用的系统资源句柄**

选择View —> Lower Pane View —> Handles

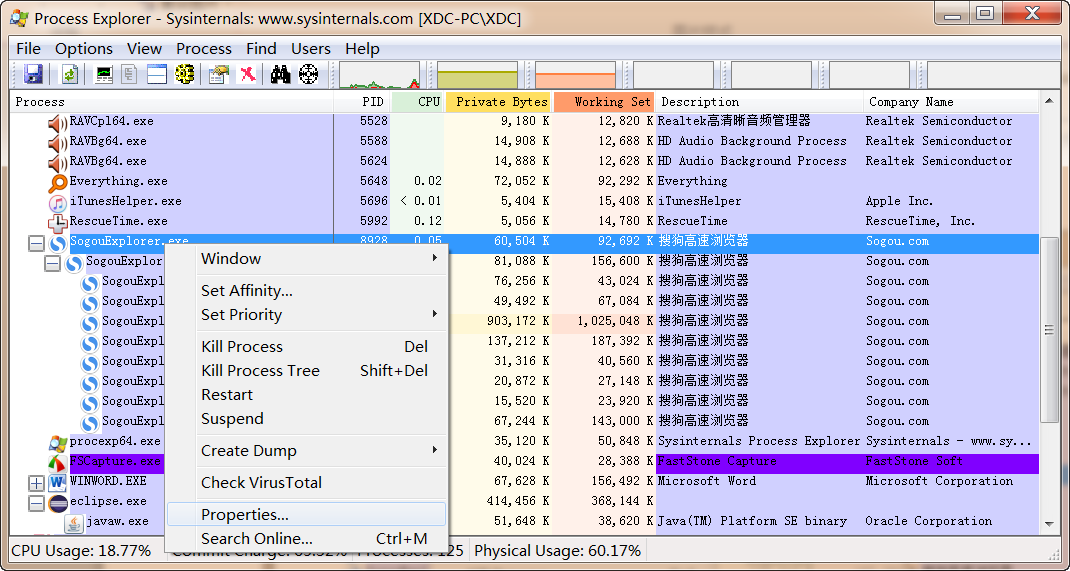


1.查看当前进程所占用的资源句柄表。

2.可以分析进程的逻辑：如图当前TeamViewer的服务进程创建了一个Event事件，并且占用一个Log文件。

3.可以检查自己的程序是否有内核句柄泄露。

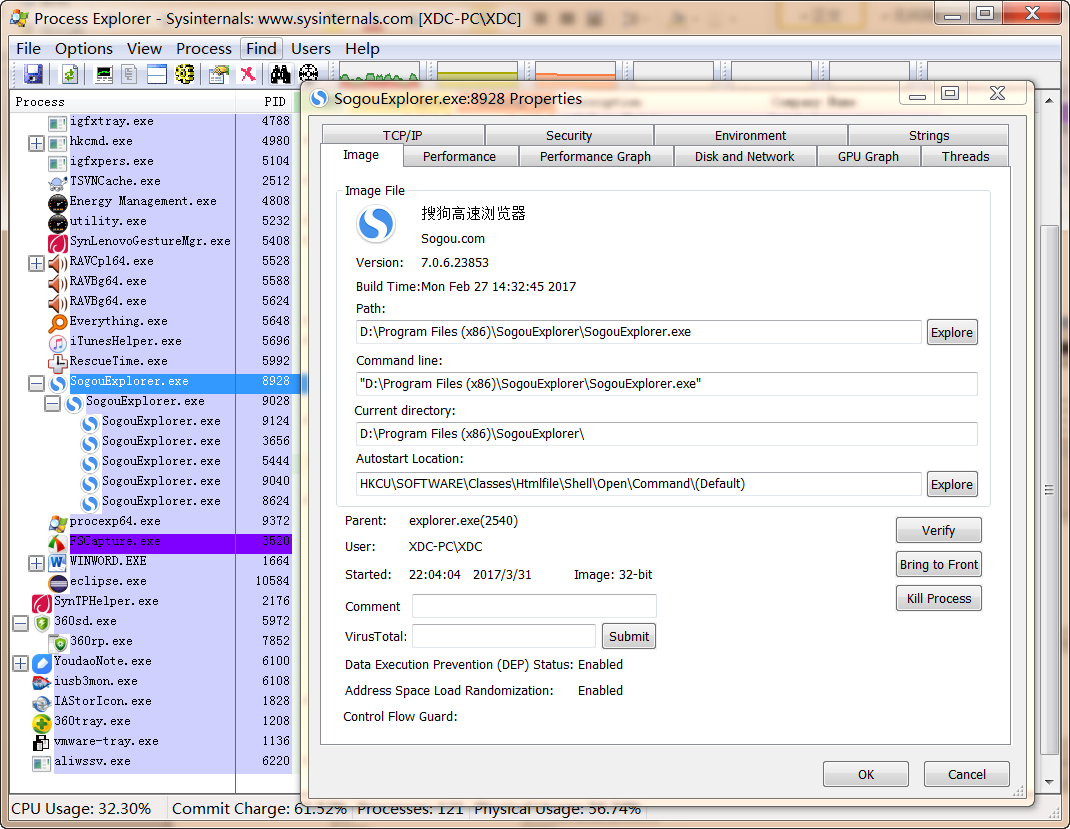
**五、操控进程以及显示进程的内部信息（这类信息是属于当前进程的）**



1.可以结束当前进程，或者当前进程树。

2.可以挂起、重启、从挂其中恢复一个进程。

3.查看进程属性信息（选择Properties）。



3.1可以看到当前进程的用户组信息。

3.2可以看到当前进程申请了哪些特权。

3.3可以看到当前进程的环境变量。

3.4可以看到当前进程的线程信息，这个很重要。

**六、搜索功能（Ctrl+F）**

为什么搜索功能单独拉出来说呢，我个人觉得这个功能在很多地方都可以用到，编码的时候可以查看哪个事件被谁占用了，你直接搜事件名称就可以了，如果你像删除一个目录怎么也删除不掉，就是说某某文件被人占用，那你可以搜索一下你需要删除的目录路径