shhqy82

< 2025年8月 >

日	一	二	三	四	五	六
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

昵称： shhqy82
园龄： 15年5个月
粉丝： 66
关注： 10
+加关注

搜索

找找看

常用链接

我的随笔
我的评论
我的参与
最新评论
我的标签

最新随笔

1.jqGrid选择列控件向右拖拽超出边界处理
2.强力推荐！那些你不能错过的 GitHub 插件和工具
3.GitHub 托管的10款免费开源 windows 工具
4.MT5：放大市场价格指标
5.wpf
6.2016年最佳Linux发行版排行榜
7.C++ 消息中间件（MQ4CPP）
8.使用VS2012调试ReactOS源码
9.Process Explorer使用图文教程
10.解决VS2015安装Android SDK 后文件不全及更新问题

积分与排名

积分 - 118117
排名 - 12995

随笔分类 (52)

.net(21)
js(4)
other(22)
sql server(2)
读书(3)

随笔档案 (53)

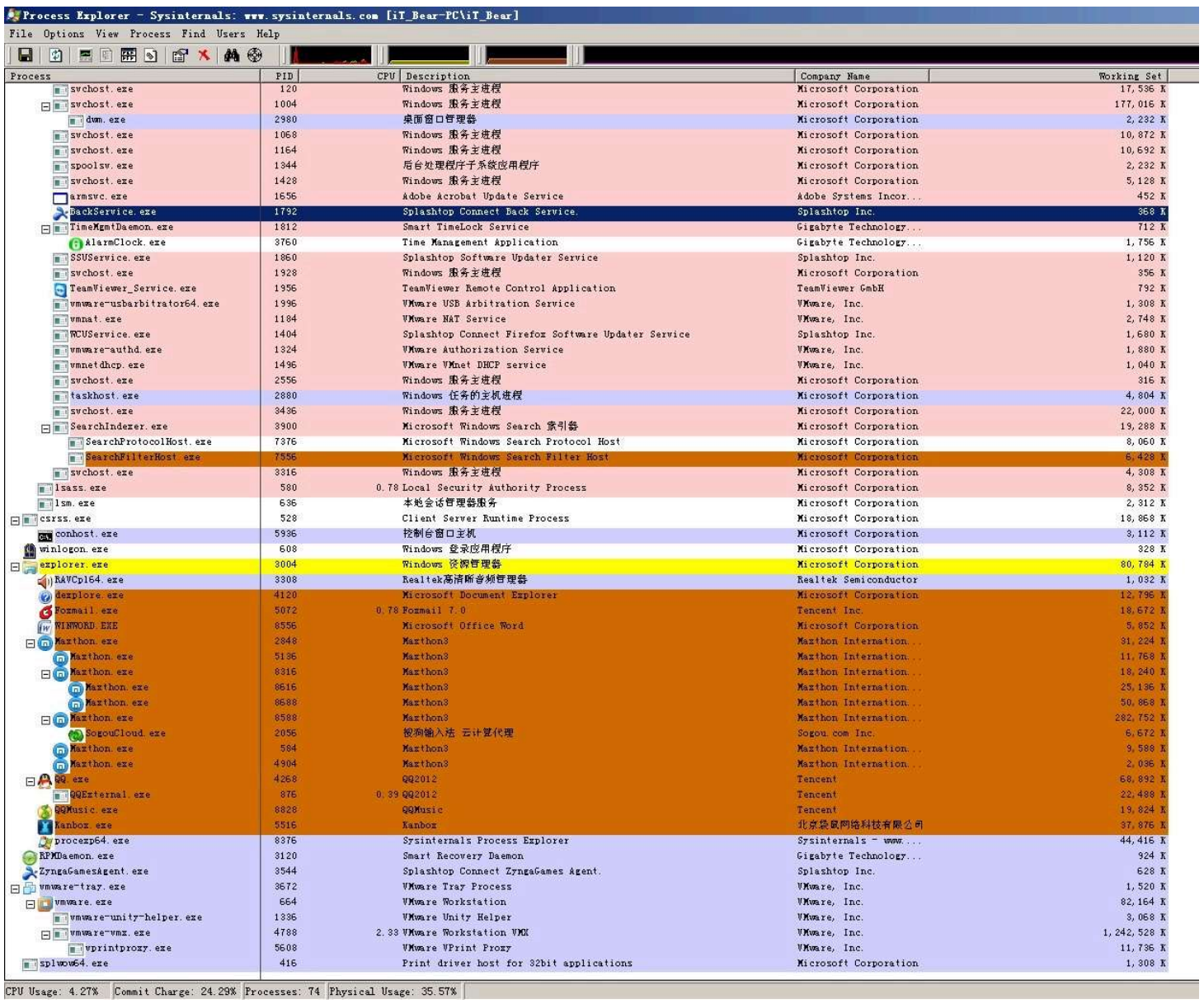
2019年4月(1)
2017年9月(2)

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、Process Explorer的树形结构界面



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

右键单击标题栏-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!

2016年4月(1)
2016年1月(2)
2015年12月(3)
2015年11月(1)
2012年12月(1)
2012年11月(1)
更多

相册 (0)

w(2)

阅读排行榜

1. 如何正确设置Proxy Switchy!(51140)
2. asp.net c# 打开新页面或页面跳转(43380)
3. C# winform 使用进度条(两种形式)(32855)
4. 完整opencv(emgucv)人脸、检测、采集、识别、匹配、对比(26673)
5. 将centos7打造成桌面系统(25616)
6. VMware虚拟机安装Mac OS X Lion(25355)
7. Process Explorer使用图文教程(21524)
8. 彻底卸载或删除office 2007(16980)
9. Android API 人脸检测（Face Detect）(14541)
10. 解决VS2015安装Android SDK 后文件不全及更新问题(11337)

评论排行榜

1. Neurotec Biometrics 人脸、检测、采集、识别、匹配、对比(8)
2. 完整opencv(emgucv)人脸、检测、采集、识别、匹配、对比(6)
3. C# winform 使用进度条(两种形式)(5)
4. C#导出数据到EXCEL方法谈(4)
5. MyEclipse bling 10.x 破解激活(3)

推荐排行榜

1. asp.net c# 打开新页面或页面跳转(5)
2. Neurotec Biometrics 人脸、检测、采集、识别、匹配、对比(3)
3. 完整opencv(emgucv)人脸、检测、采集、识别、匹配、对比(3)
4. 弄清.NET中复杂的文件类型(3)
5. VMware虚拟机安装Mac OS X Lion(3)

最新评论

1. Re:使用VS2012调试ReactOS源码

出现链接错误怎么办大佬，我也私信您了

--明亮有香气

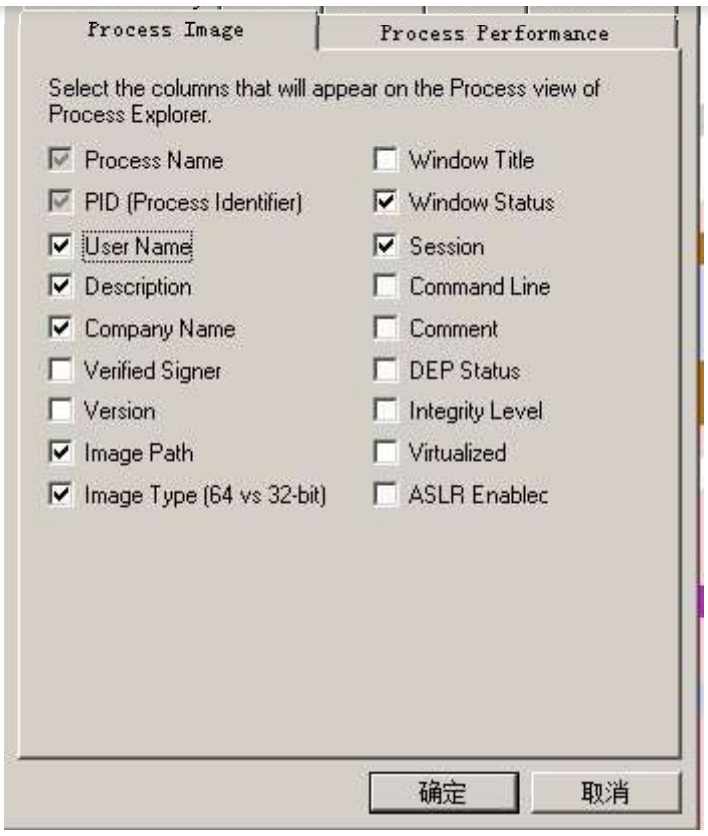
2. Re:C# winform 使用进度条(两种形式)

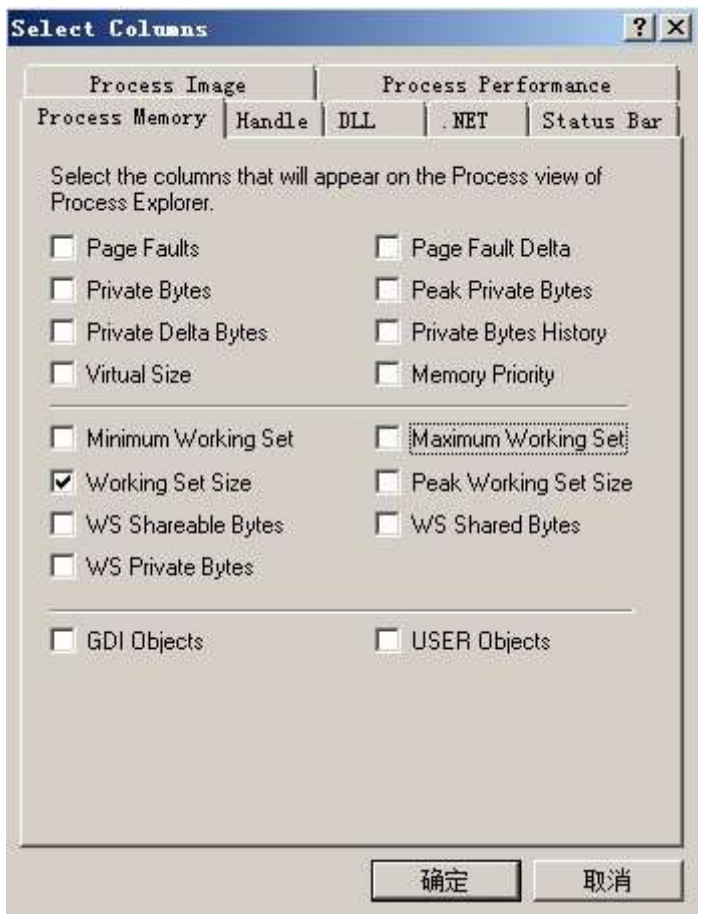
至少给个图吧，都不清楚结果咋样

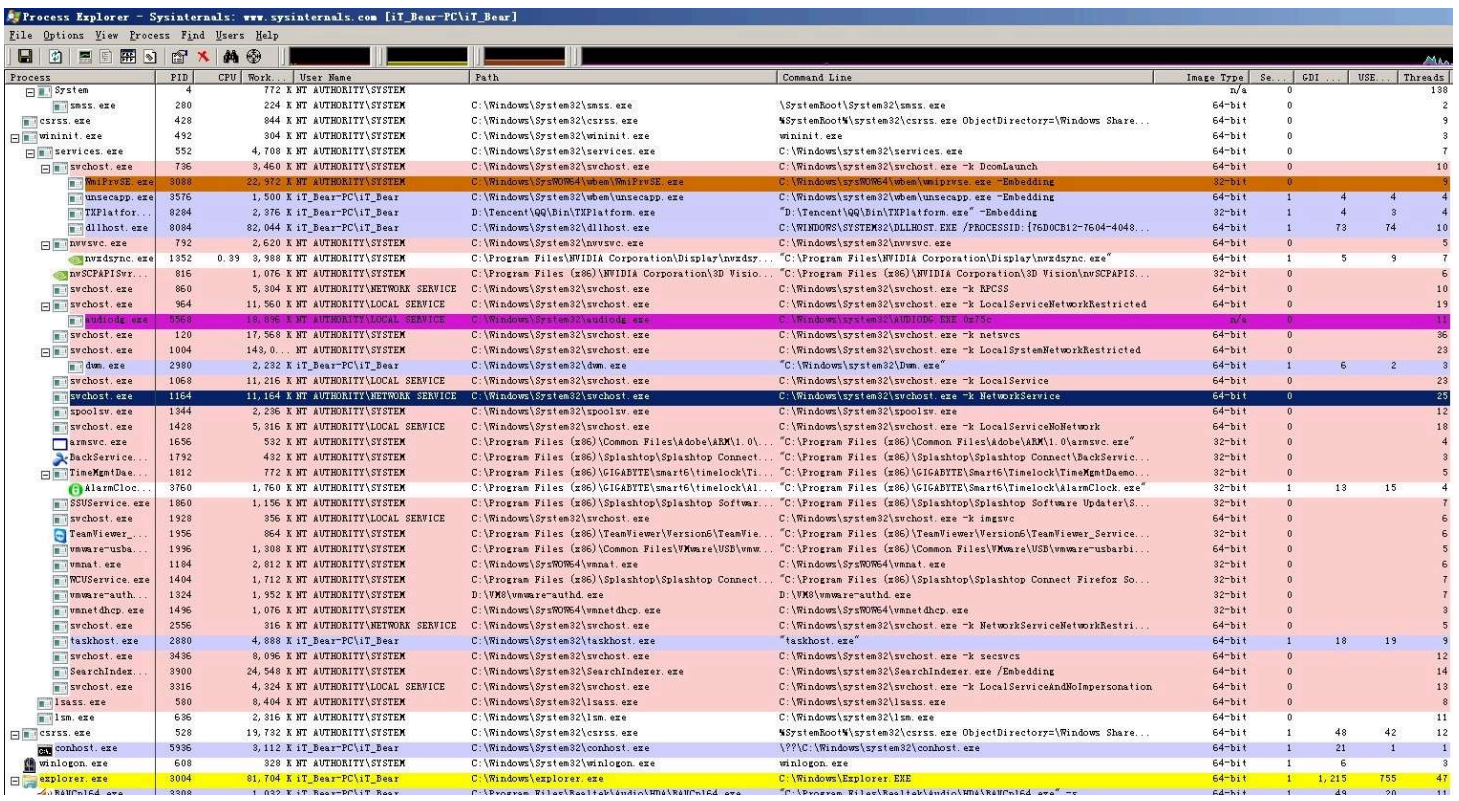
--PER10

3. Re:C# winform 使用进度条(两种形式)

楼主可以问个问题吗?我用第二种办法进度条出不来啊...我是想用进度条监听几个执行SQL语句的方法,要等执行结果出来







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）

--Anmen

4. Re:完整ASP.Net Excel导入程序（支持2007）

大牛，前台的ID标识给一下呀

--小通

5. Re:MT5：放大市场价格指标

好想学习

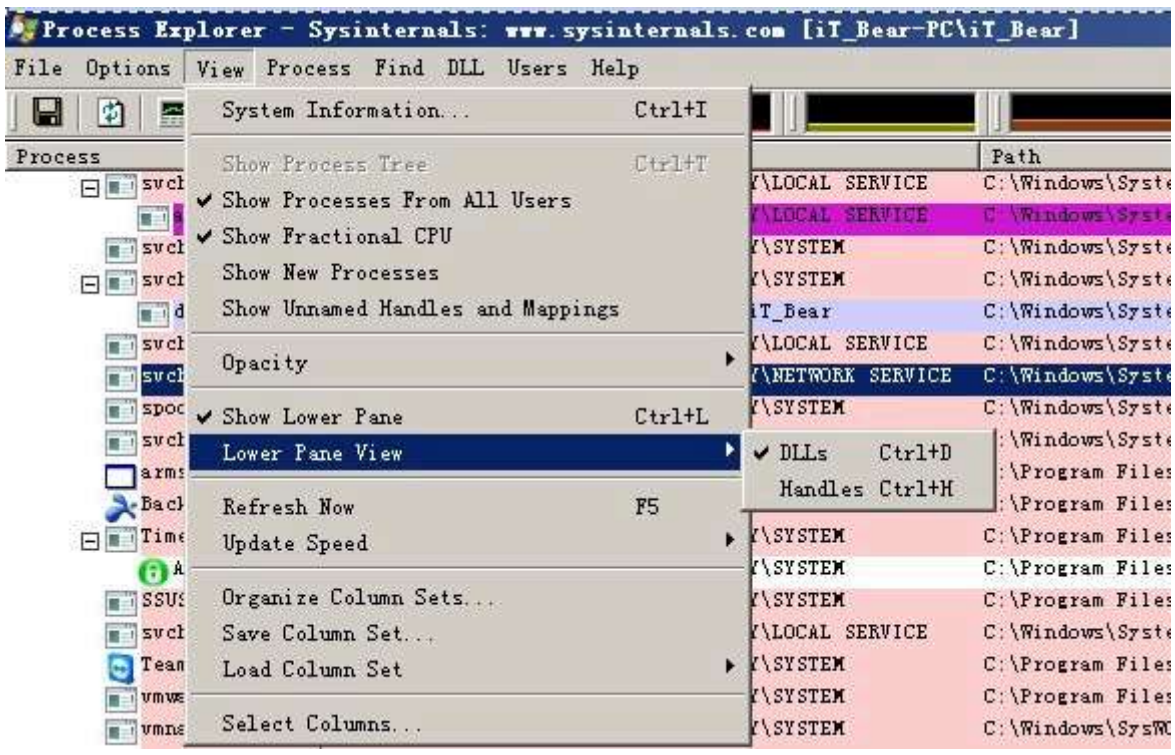
--落日赌城

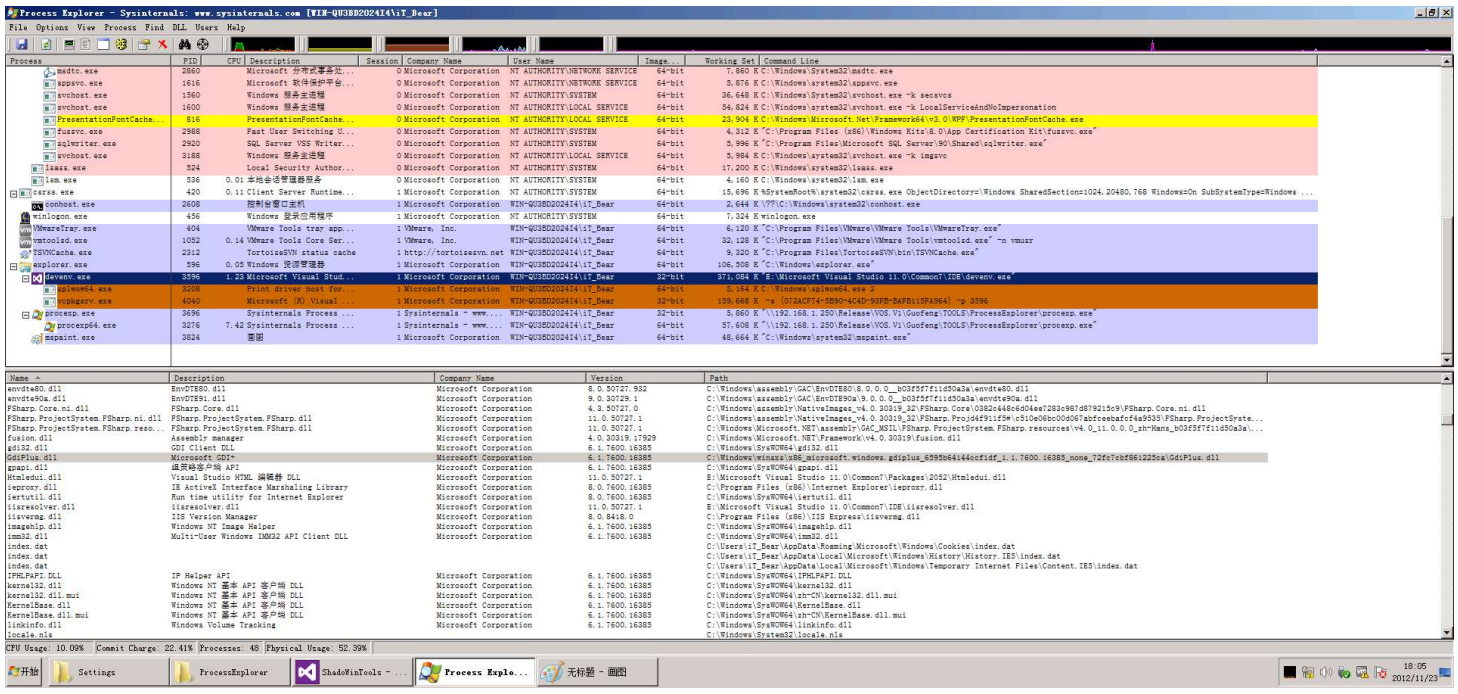
5.显示进程当前的权限，是系统用户权限还是网络管理员权限还是普通管理员权限（User Name）

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





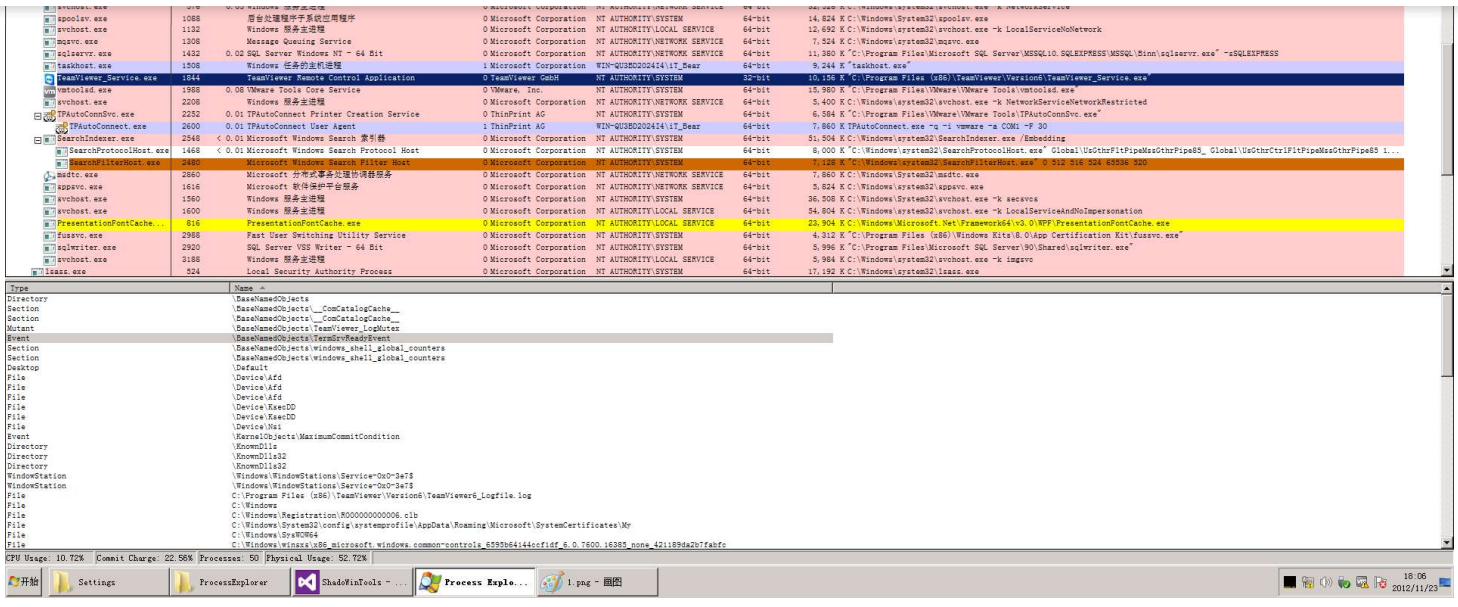
1.通过这种方式可以观察，我们的进程是否被其他程序注入DLL

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 —> DLLs



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。

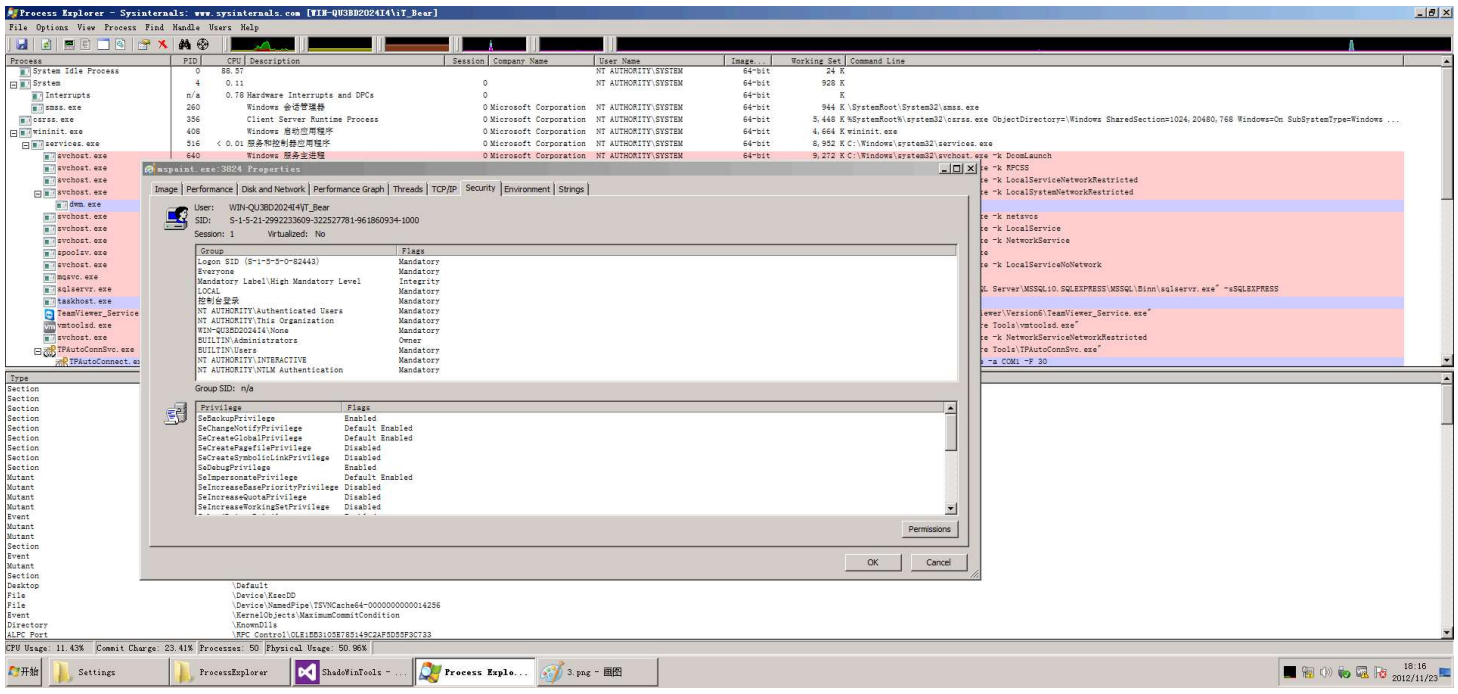
五、操控进程以及显示进程的内部信息（这类信息是属于当前进程的）

右键单击进程

1.可以结束当前进程，或者当前进程树

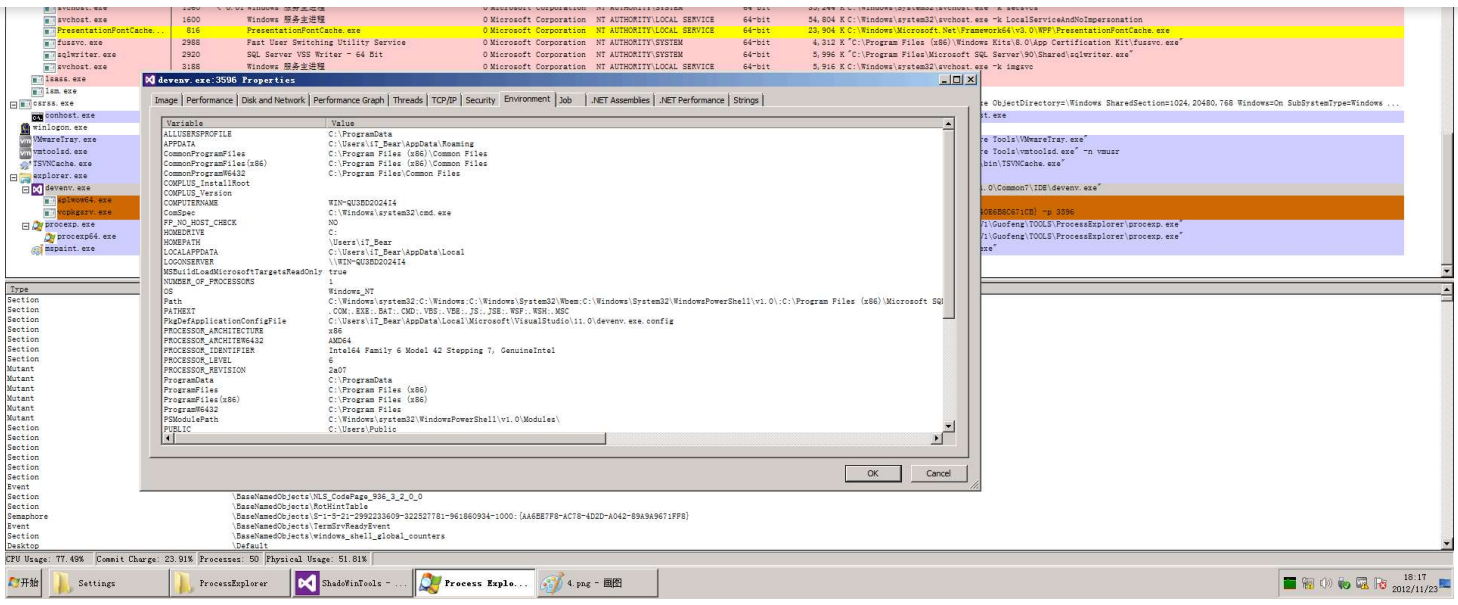
2.可以挂起、重启、从挂其中恢复一个进程

3.查看进程信息（如图-选择Properties）



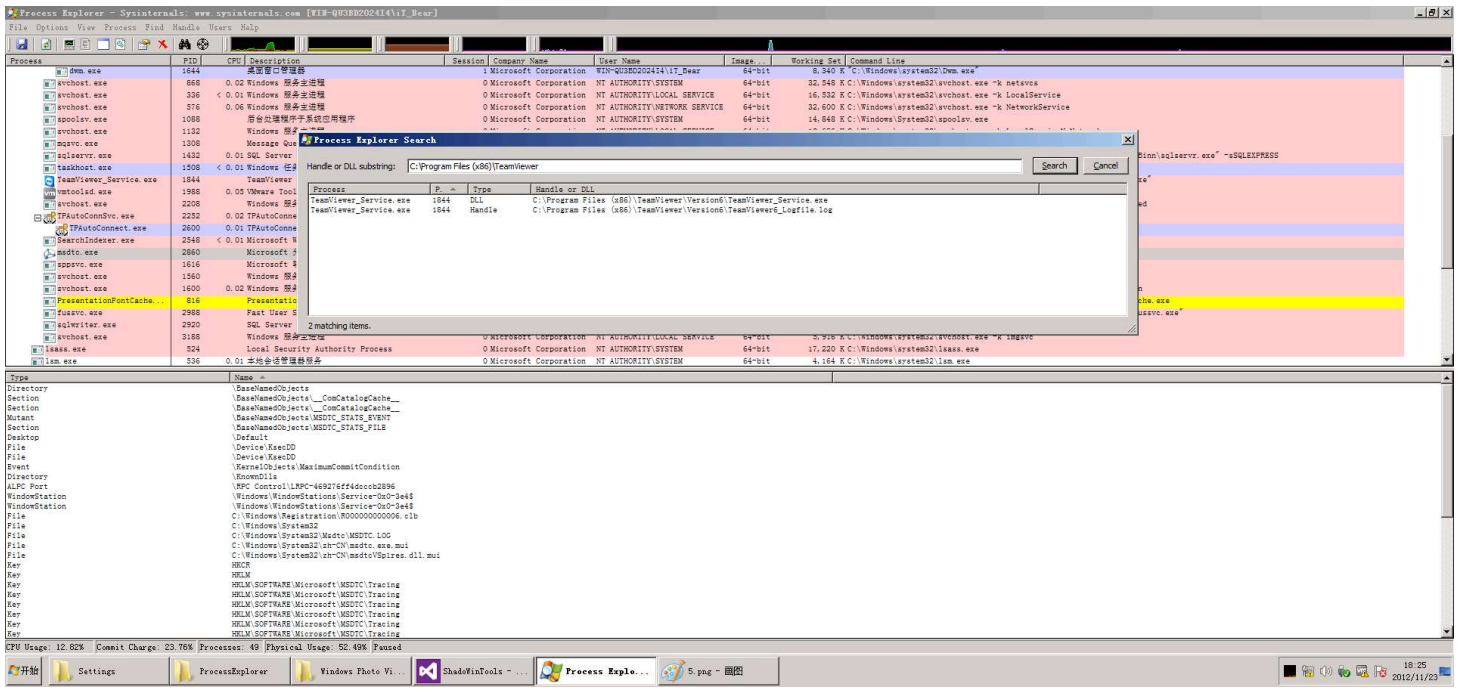
1.可以看到当前进程的用户组信息

2.可以看到当前进程申请了哪些特权



选择Environment选项卡，可以看到当前进程的环境变量，如果自动化编译或者使用一些开源软件，查看其环境变量是很重要的一环。

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

如图：TeamViewer这个文件夹正在被一个服务占用，这样我只需要把这个服务停止，就可以删除了，常见的还有U盘被占用不让卸载等等!

分类: other

shhqy82
粉丝 - 66 关注 - 10
+加关注

« 上一篇： 解决VS2015安装Android SDK 后文件不全及更新问题
» 下一篇： 使用VS2012调试ReactOS源码

posted on 2015-12-30 11:57 shhqy82 阅读(21524) 评论(0) 收藏 举报

自动补全

提交评论 退出 订阅评论 我的博客

[Ctrl+Enter快捷键提交]