

< 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 window s 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)

随笔- 53 文章- 0 评论- 63 阅读- 40万

博客园 首页 新随笔 联系 管理 订阅 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

Process Explorer - Sysinternals: www.sysinternals.com [iT_Bear-PC\iT_Bear]				
File Options View Process Find Users Help				
Process	PID	CPU	Description	Working Set
svchost.exe	120		Windows 服务主进程	17,936 K
svchost.exe	1004		Windows 服务主进程	177,016 K
explorer.exe	2980		桌面窗口管理器	2,232 K
svchost.exe	1068		Windows 服务主进程	10,872 K
svchost.exe	1164		Windows 服务主进程	10,692 K
spoolsv.exe	1344		后台处理程序子系统应用程序	2,232 K
svchost.exe	1428		Windows 服务主进程	5,128 K
armsvc.exe	1656		Adobe Acrobat Update Service	452 K
BackService.exe	1732		Splashtop Connect Back Service	368 K
TimeMgtDaemon.exe	1812		Smart TimeLock Service	712 K
AlarmClock.exe	3760		Time Management Application	1,756 K
SSUService.exe	1860		Splashtop Software Updater Service	1,120 K
svchost.exe	1928		Windows 服务主进程	356 K
TeamViewer_Service.exe	1956		TeamViewer Remote Control Application	792 K
vmtoolsd-usd-arbitrator64.exe	1996		VMware USB Arbitration Service	1,308 K
vmtoolsd.exe	1184		VMware NAT Service	2,748 K
PCUService.exe	1404		Splashtop Connect Firefox Software Updater Service	1,680 K
vmtoolsd-authd.exe	1324		VMware Authorization Service	1,880 K
vmtoolsd-dhcp.exe	1496		VMware VMnet DHCP service	1,040 K
svchost.exe	2556		Windows 服务主进程	316 K
taskhost.exe	2880		Windows 任务的主机进程	4,804 K
svchost.exe	3436		Windows 服务主进程	22,000 K
SearchIndexer.exe	3900		Microsoft Windows Search 索引器	19,288 K
SearchProtocolHost.exe	7376		Microsoft Windows Search Protocol Host	8,060 K
SearchFilterHost.exe	7556		Microsoft Windows Search Filter Host	6,428 K
svchost.exe	3316		Windows 服务主进程	4,308 K
lsass.exe	580	0.78	Local Security Authority Process	8,352 K
lsass.exe	636		本地会话管理器服务	2,312 K
csrss.exe	528		Client Server Runtime Process	18,868 K
conhost.exe	5936		控制台窗口主机	3,112 K
winlogon.exe	608		Windows 登录应用程序	328 K
explorer.exe	3004		Windows 资源管理器	80,784 K
RAVCpl64.exe	3308		Realtek高清音频管理器	1,032 K
explore.exe	4120		Microsoft Document Explorer	12,796 K
Formmail.exe	5072	0.78	Formmail 7.0	18,672 K
WINWORD.EXE	8556		Microsoft Office Word	5,852 K
Marthon.exe	2848		Marthon3	31,224 K
Marthon.exe	5136		Marthon3	11,768 K
Marthon.exe	8316		Marthon3	18,240 K
Marthon.exe	8616		Marthon3	25,136 K
Marthon.exe	8638		Marthon3	50,868 K
Marthon.exe	8588		Marthon3	282,752 K
SogouCloud.exe	2056		搜狗输入法 云计算代理	6,672 K
Marthon.exe	584		Marthon3	9,588 K
Marthon.exe	4904		Marthon3	2,036 K
QQ.exe	4268		QQ2012	68,892 K
QQExternal.exe	876	0.39	QQ2012	22,488 K
QQMusic.exe	8828		QQMusic	19,824 K
Kanbox.exe	5516		Kanbox	97,876 K
process64.exe	8876		Sysinternals Process Explorer	44,416 K
RFMDaemon.exe	3120		Smart Recovery Daemon	924 K
ZyngaGamesAgent.exe	3544		Splashtop Connect ZyngaGames Agent	628 K
vmtoolsd-tray.exe	3672		VMware Tray Process	1,520 K
vmtoolsd.exe	664		VMware Workstation	82,164 K
vmtoolsd-unity-helper.exe	1336		VMware Unity Helper	3,068 K
vmtoolsd-vmx.exe	4788	2.33	VMware Workstation VMX	1,242,528 K
vprintproxy.exe	5608		VMware VPrint Proxy	11,736 K
splwow64.exe	416		Print driver host for 32bit applications	1,308 K

CPU Usage: 4.27% | Commit Charge: 24.28% | Processes: 74 | Physical Usage: 35.57%

- 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 t) (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

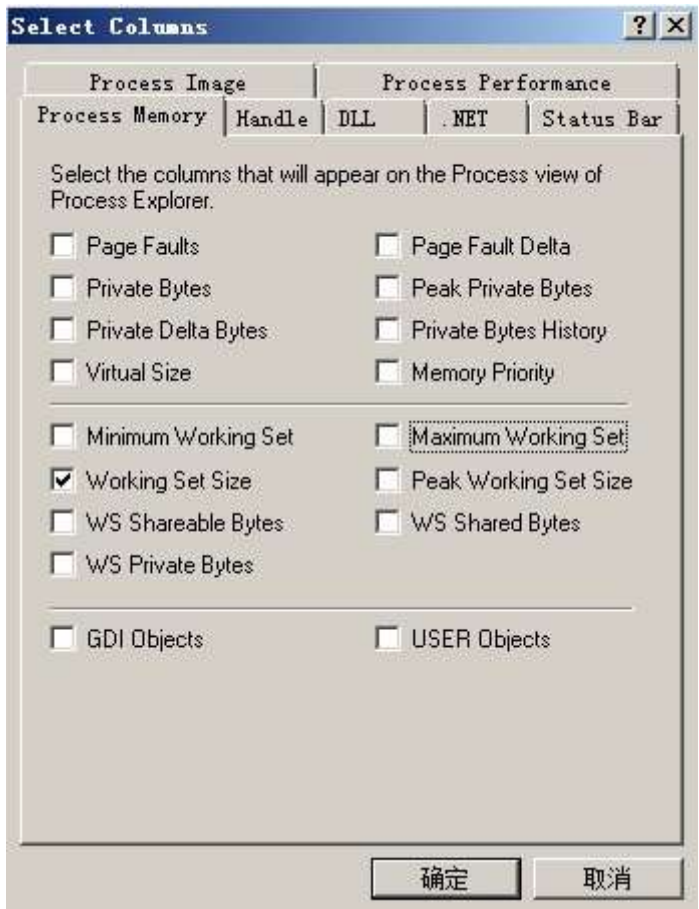
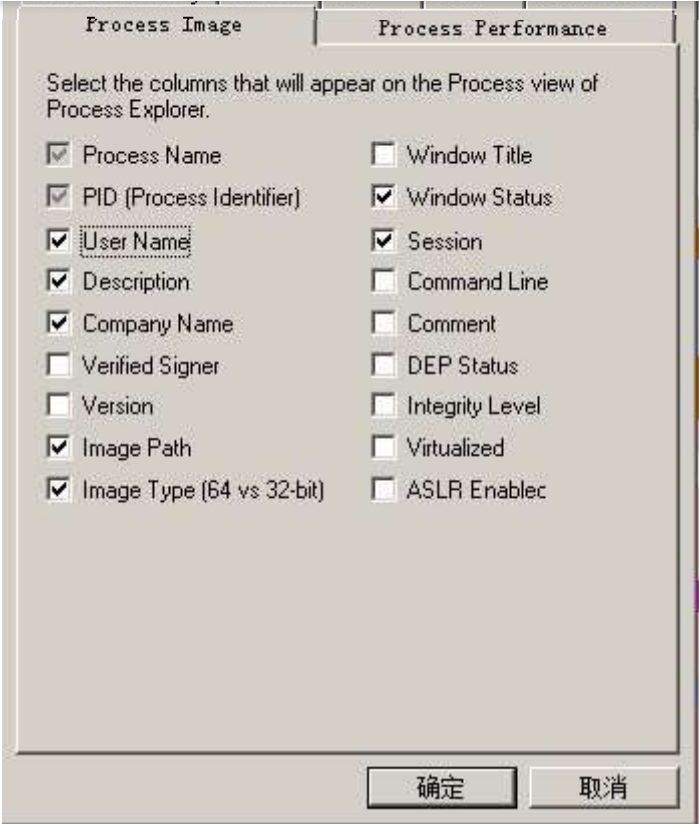
2. Re:C# winform 使用进度条(两种形式)

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



Process	PID	CPU	Work	User Name	Path	Command Line	Image Type	Se...	GDI ...	USE...	Threads
System	4		712 K NT AUTHORITY\SYSTEM								138
smss.exe	280		224 K NT AUTHORITY\SYSTEM		C:\Windows\System32\smss.exe	\\SystemRoot\System32\smss.exe	64-bit	0			2
csrss.exe	428		844 K NT AUTHORITY\SYSTEM		C:\Windows\System32\csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows Share...	64-bit	0			9
wininit.exe	492		804 K NT AUTHORITY\SYSTEM		C:\Windows\System32\wininit.exe	wininit.exe	64-bit	0			3
services.exe	552		4,708 K NT AUTHORITY\SYSTEM		C:\Windows\System32\services.exe	C:\Windows\system32\services.exe	64-bit	0			7
svchost.exe	736		3,460 K NT AUTHORITY\SYSTEM		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	64-bit	0			10
smss.exe	2088		224 K NT AUTHORITY\SYSTEM		C:\Windows\System32\smss.exe	C:\Windows\system32\smss.exe -Embedding	32-bit	0			3
smss.exe	2576		1,500 K IT_Bear-PC\IT_Bear		C:\Windows\System32\smss.exe	C:\Windows\system32\smss.exe -Embedding	64-bit	1	4	4	4
TPPlatform.exe	8284		2,376 K IT_Bear-PC\IT_Bear		D:\Tencent\QQ\Bin\TPPlatform.exe	"D:\Tencent\QQ\Bin\TPPlatform.exe" -Embedding	32-bit	1	4	3	4
dllhost.exe	8084		82,044 K IT_Bear-PC\IT_Bear		C:\Windows\System32\dlhost.exe	C:\WINDOWS\SYSTEM32\DLLHOST.EXE /PROCESSID:{76D0CB12-76D4-4048-...	64-bit	1	73	74	10
nvsvcs.exe	732		2,620 K NT AUTHORITY\SYSTEM		C:\Windows\System32\nvsvcs.exe	C:\Windows\system32\nvsvcs.exe	64-bit	0			5
nvazdync.exe	1952	0.39	3,988 K NT AUTHORITY\SYSTEM		C:\Program Files\NVIDIA Corporation\Display\nvazdync.exe	C:\Program Files\NVIDIA Corporation\Display\nvazdync.exe	64-bit	1	5	9	7
nvSCPAPISrv.exe	816		1,076 K NT AUTHORITY\SYSTEM		C:\Program Files (x86)\NVIDIA Corporation\3D Vision\nvSCPAPISrv.exe	"C:\Program Files (x86)\NVIDIA Corporation\3D Vision\nvSCPAPISrv.exe"	32-bit	0			6
svchost.exe	860		5,304 K NT AUTHORITY\NETWORK SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS	64-bit	0			10
svchost.exe	964		11,560 K NT AUTHORITY\LOCAL SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted	64-bit	0			19
svchost.exe	968		18,096 K NT AUTHORITY\LOCAL SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted	64-bit	0			13
svchost.exe	120		17,568 K NT AUTHORITY\SYSTEM		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k netsvc	64-bit	0			36
svchost.exe	1004		143.0... NT AUTHORITY\SYSTEM		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted	64-bit	0			23
dm.exe	2980		2,232 K IT_Bear-PC\IT_Bear		C:\Windows\System32\dm.exe	"C:\Windows\system32\dm.exe"	64-bit	1	6	2	3
svchost.exe	1068		11,216 K NT AUTHORITY\LOCAL SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k LocalService	64-bit	0			23
svchost.exe	1164		11,164 K NT AUTHORITY\NETWORK SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k NetworkService	64-bit	0			25
spoolsv.exe	1944		2,236 K NT AUTHORITY\SYSTEM		C:\Windows\System32\spoolsv.exe	C:\Windows\system32\spoolsv.exe	64-bit	0			12
svchost.exe	1428		5,316 K NT AUTHORITY\LOCAL SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNetwork	64-bit	0			18
armvsc.exe	1656		532 K NT AUTHORITY\SYSTEM		C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armvsc.exe	"C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armvsc.exe"	32-bit	0			4
BackService.exe	1732		432 K NT AUTHORITY\SYSTEM		C:\Program Files (x86)\Splashtop\Splashtop Connect\BackService.exe	"C:\Program Files (x86)\Splashtop\Splashtop Connect\BackService.exe"	32-bit	0			3
TimeMentDae.exe	1812		772 K NT AUTHORITY\SYSTEM		C:\Program Files (x86)\CIGABYTE\Smart6\TimeMentDae.exe	"C:\Program Files (x86)\CIGABYTE\Smart6\TimeMentDae.exe"	32-bit	0			5
AlarmClock.exe	2760		1,760 K NT AUTHORITY\SYSTEM		C:\Program Files (x86)\CIGABYTE\Smart6\AlarmClock.exe	"C:\Program Files (x86)\CIGABYTE\Smart6\AlarmClock.exe"	32-bit	1	19	15	4
CSOService.exe	1860		1,156 K NT AUTHORITY\SYSTEM		C:\Program Files (x86)\Splashtop\Splashtop Software Updater\CSOService.exe	"C:\Program Files (x86)\Splashtop\Splashtop Software Updater\CSOService.exe"	32-bit	0			7
svchost.exe	1928		356 K NT AUTHORITY\LOCAL SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k ingvsc	64-bit	0			6
TeamViewer.exe	1956		864 K NT AUTHORITY\SYSTEM		C:\Program Files (x86)\TeamViewer\Version6\TeamViewer.exe	"C:\Program Files (x86)\TeamViewer\Version6\TeamViewer_Service.exe"	32-bit	0			6
vmtoolsd.exe	1996		1,308 K NT AUTHORITY\SYSTEM		C:\Program Files (x86)\Common Files\VMware\USB\vmtoolsd.exe	"C:\Program Files (x86)\Common Files\VMware\USB\vmtoolsd.exe"	64-bit	0			5
vmtoolsd.exe	1184		2,812 K NT AUTHORITY\SYSTEM		C:\Windows\System32\vmtoolsd.exe	C:\Windows\system32\vmtoolsd.exe	32-bit	0			6
PCVService.exe	1404		1,712 K NT AUTHORITY\SYSTEM		C:\Program Files (x86)\Splashtop\Splashtop Connect\Firefox.exe	"C:\Program Files (x86)\Splashtop\Splashtop Connect\Firefox.exe"	32-bit	0			7
vmtoolsd-auth.exe	1324		1,952 K NT AUTHORITY\SYSTEM		D:\VM8\vmtoolsd-auth.exe	D:\VM8\vmtoolsd-auth.exe	32-bit	0			7
vmtoolsd-dhcp.exe	1496		1,076 K NT AUTHORITY\SYSTEM		C:\Windows\System32\vmtoolsd-dhcp.exe	C:\Windows\system32\vmtoolsd-dhcp.exe	32-bit	0			3
svchost.exe	2556		316 K NT AUTHORITY\NETWORK SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestri...	64-bit	0			5
taskhost.exe	2880		4,088 K IT_Bear-PC\IT_Bear		C:\Windows\System32\taskhost.exe	"taskhost.exe"	64-bit	1	18	19	9
svchost.exe	3436		8,096 K NT AUTHORITY\SYSTEM		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k secsvcs	64-bit	0			12
SearchIndexer.exe	3900		24,548 K NT AUTHORITY\SYSTEM		C:\Windows\System32\SearchIndexer.exe	C:\Windows\system32\SearchIndexer.exe /Embedding	64-bit	0			14
svchost.exe	3316		4,324 K NT AUTHORITY\LOCAL SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation	64-bit	0			13
lsass.exe	580		8,404 K NT AUTHORITY\SYSTEM		C:\Windows\System32\lsass.exe	C:\Windows\system32\lsass.exe	64-bit	0			8
lsim.exe	636		2,316 K NT AUTHORITY\SYSTEM		C:\Windows\System32\lsim.exe	C:\Windows\system32\lsim.exe	64-bit	0			11
csrss.exe	528		19,792 K NT AUTHORITY\SYSTEM		%SystemRoot%\system32\csrss.exe	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows Share...	64-bit	1	48	42	12
conhost.exe	5936		3,112 K IT_Bear-PC\IT_Bear		C:\Windows\System32\conhost.exe	\\?C:\Windows\system32\conhost.exe	64-bit	1	21	1	1
winlogon.exe	608		328 K NT AUTHORITY\SYSTEM		C:\Windows\System32\winlogon.exe	winlogon.exe	64-bit	1	6	3	3
explorer.exe	3004		81,704 K IT_Bear-PC\IT_Bear		C:\Windows\explorer.exe	C:\Windows\Explorer.exe	64-bit	1	1,215	755	47
svchost.exe	3208		1,000 K IT_Bear-PC\IT_Bear		C:\Windows\System32\svchost.exe	"C:\Windows\System32\svchost.exe"	64-bit	1	48	28	11

- 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

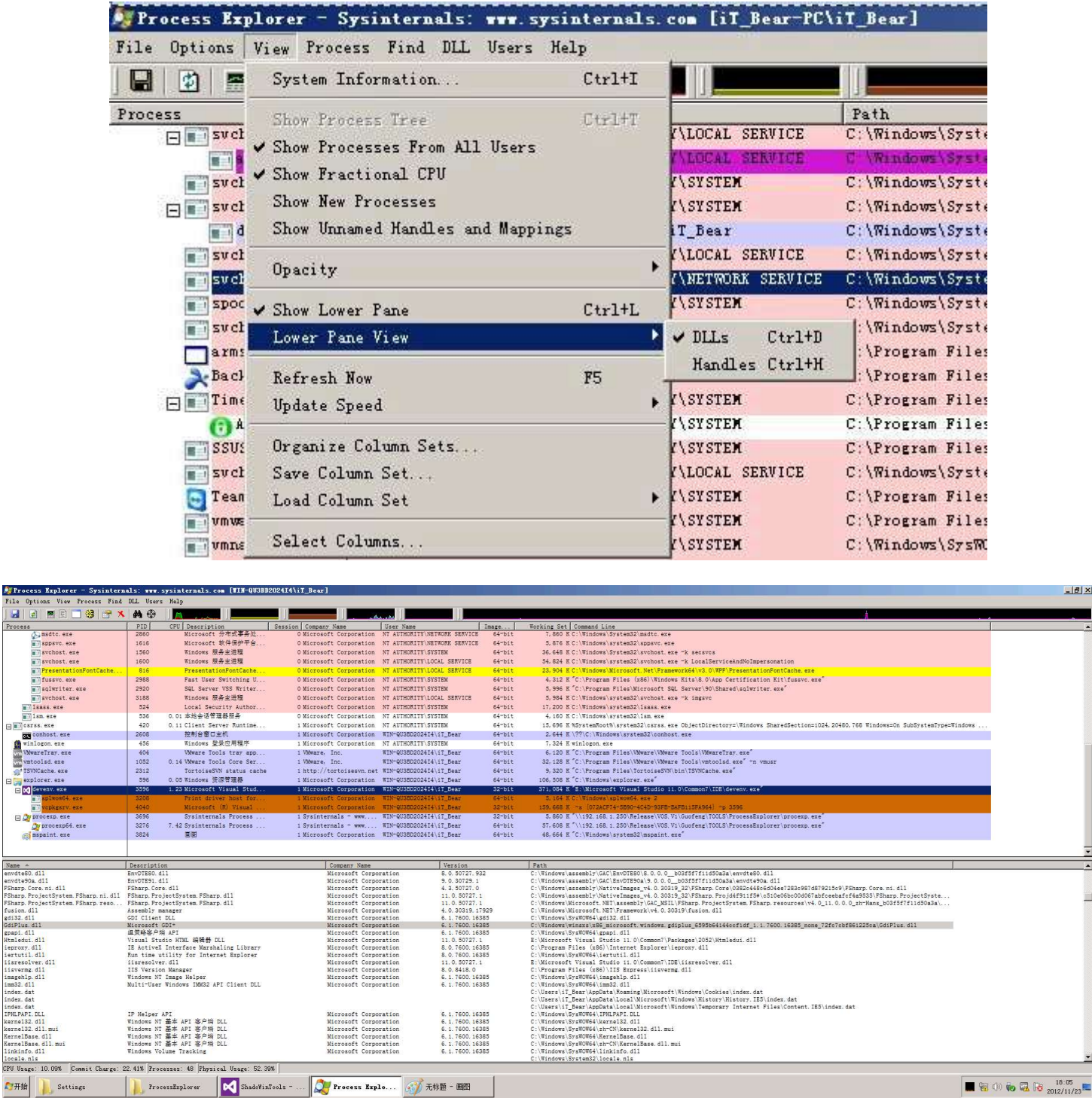
--落日赌城

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



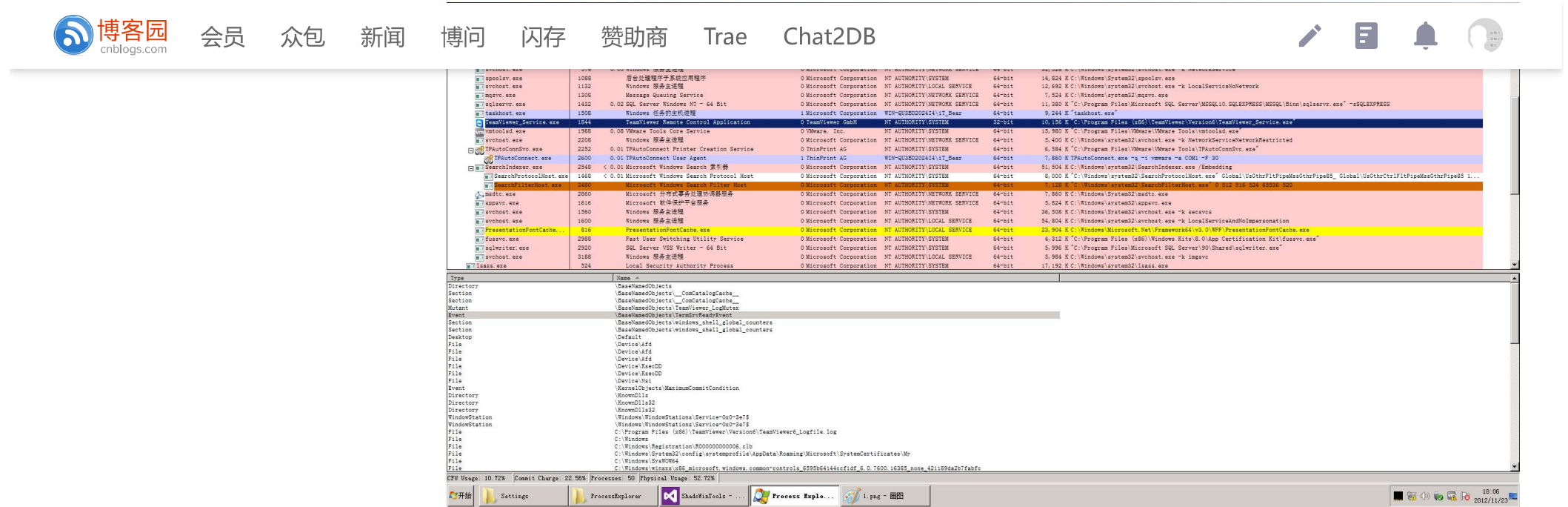
1.通过这种方式可以观察，我们的进程是否被其他程序注入DLL

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

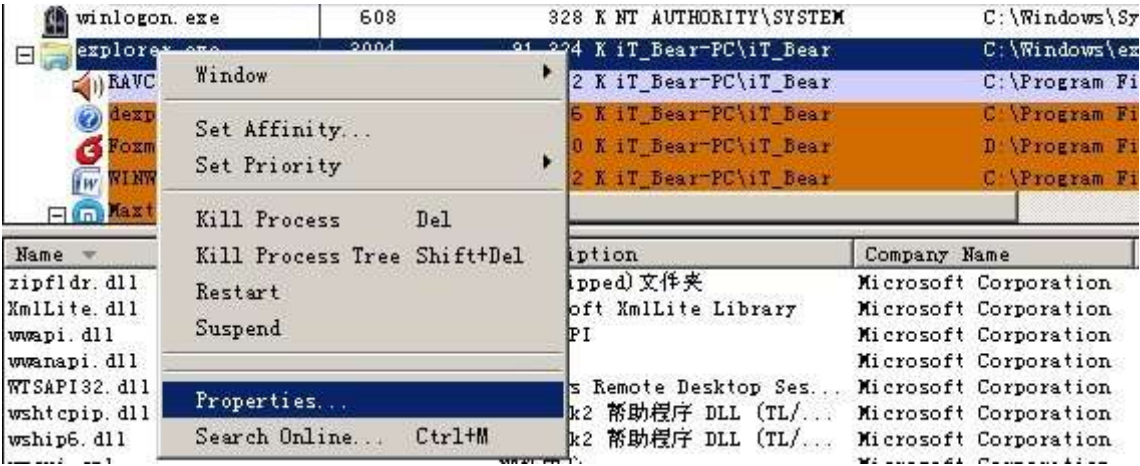
选择View —> Lower Pane View —> DLLs



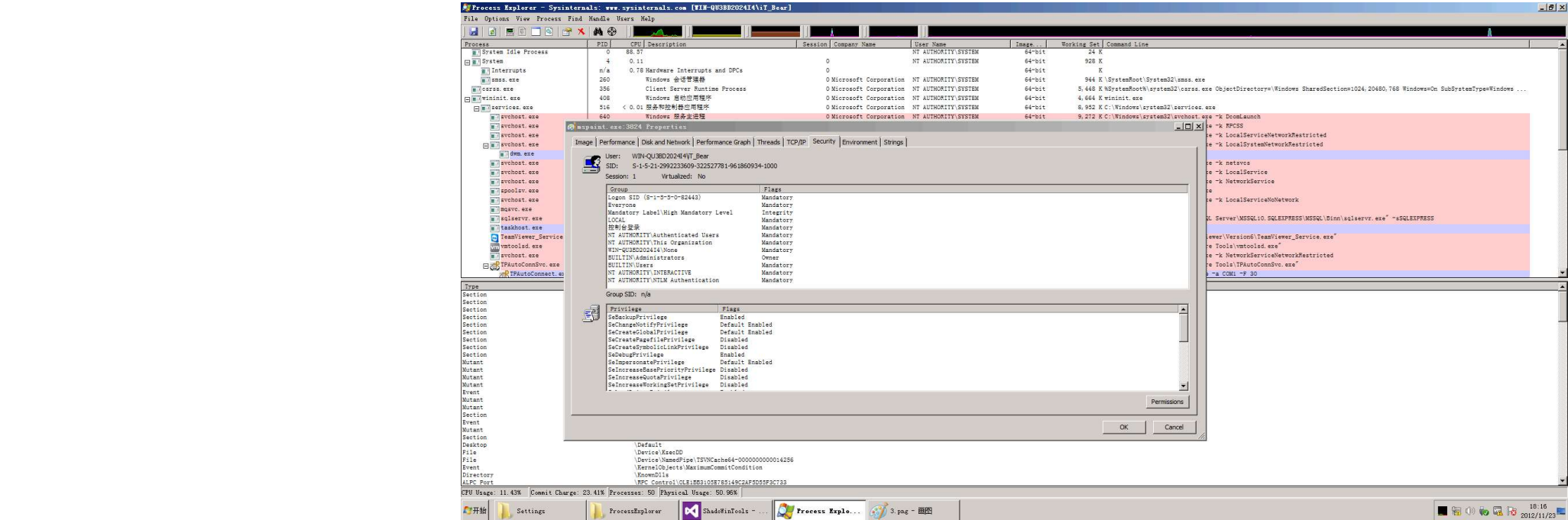
- 1.查看当前进程所占用的资源句柄表
- 2.可以分析进程的逻辑：如图当前TeamViewer的服务进程创建了一个Event事件，并且占用一个Log文件
- 3.可以检查自己的程序是否有内核句柄泄露。

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）

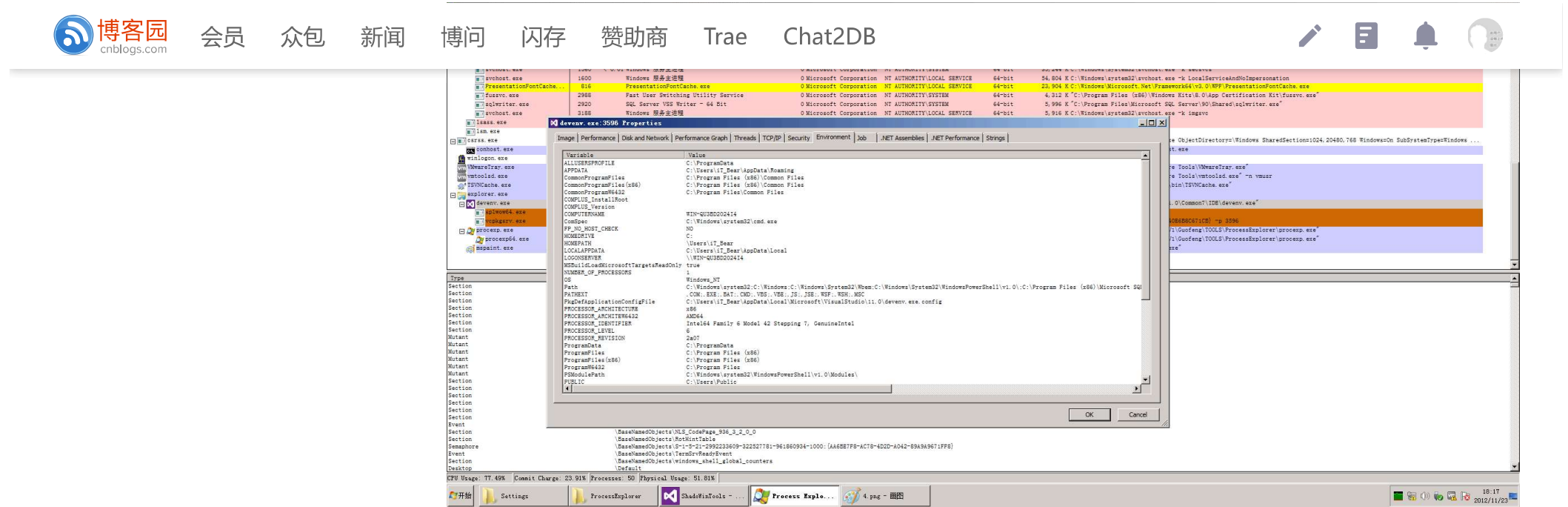
右键单击进程



- 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）

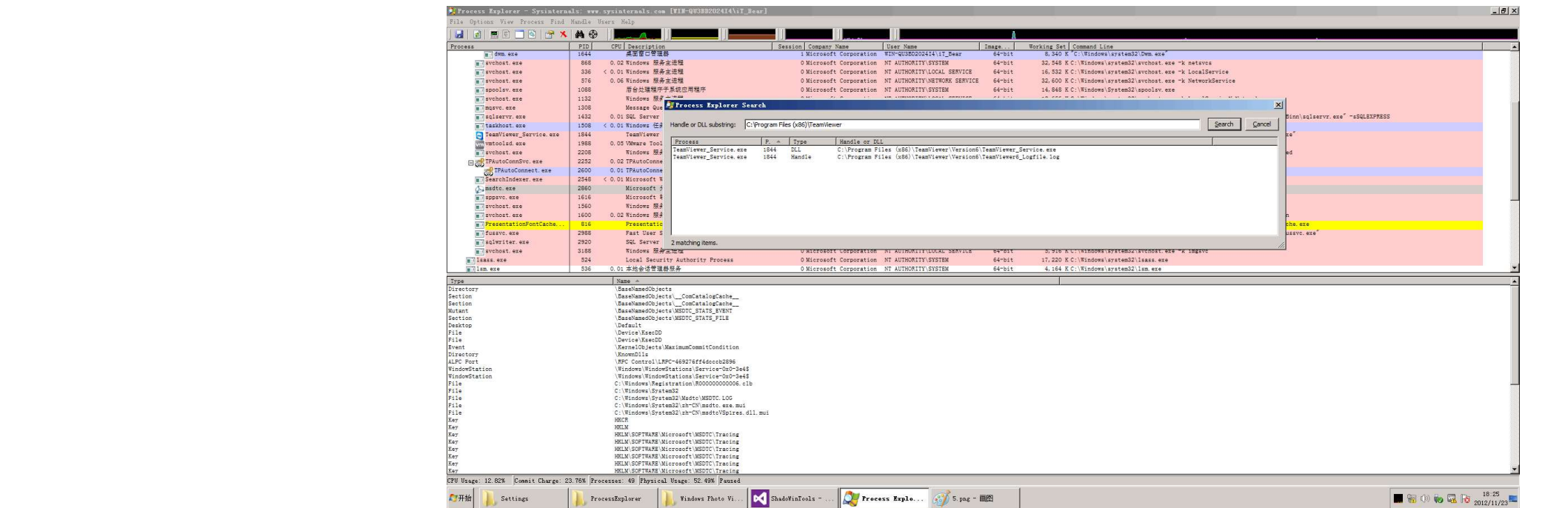


- 1.可以看到当前进程的用户组信息
- 2.可以看到当前进程申请了哪些特权



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

好文要顶

关注我

收藏该文

微信分享

shhqy82

粉丝 - 66 关注 - 10

+加关注

1

0

升级成为会员

« 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

刷新评论 刷新页面 返回顶部

发表评论 升级成为园子VIP会员

编辑 预览

B



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]

编辑推荐:

- 下划线字段在golang结构体中的应用
- SQL Server也能玩正则表达式?
- CUDA 编程初探
- 《C#高级GDI+实战：从零开发一个流程图》增加贝塞尔曲线
- AES 加密模式演进：从 ECB、CBC 到 GCM 的 C# 深度实践

阅读排行:

- 在本地部署Qwen大语言模型全过程总结
- 十年大厂员工终明白：MySQL性能优化的尽头，是对B+树的极致理解
- Coze工作流实战：一键生成历史人物一镜到底爆款短视频
- 程序员感觉工作没有成长，怎么破局？
- 记一次OOM

