

博客园 首页 新随笔 联系 管理 订阅 [HTML](#)

随笔- 53 文章- 0 评论- 63 阅读- 40万

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	PID	CPU	Description	Company Name	Working Set
svchost.exe	120	Windows	服务主进程	Microsoft Corporation	17,596 K
svchost.exe	1004	Windows	服务主进程	Microsoft Corporation	177,016 K
dum.exe	2980	桌面窗口管理器		Microsoft Corporation	2,232 K
svchost.exe	1068	Windows	服务主进程	Microsoft Corporation	10,872 K
svchost.exe	1164	Windows	服务主进程	Microsoft Corporation	10,872 K
spoolsw.exe	1844	后台处理程序	系统应用程	Microsoft Corporation	2,232 K
svchost.exe	1428	Windows	服务主进程	Microsoft Corporation	5,128 K
armsvc.exe	1656	Adobe Acrobat Update Service		Adobe Systems Incor...	452 K
BackService.exe	1792	SplashTop Connect Back Service.		SplashTop Inc.	368 K
TimeMgmtDaemon.exe	1812	Smart TimeLock Service		Gigabyte Technology...	712 K
AlarmClock.exe	3760	Time Management Application		Gigabyte Technology...	1,756 K
SSUService.exe	1860	SplashTop Software Updater Service		SplashTop Inc.	1,120 K
svchost.exe	1928	Windows	服务主进程	Microsoft Corporation	356 K
TeamViewer_Service.exe	1956	TeamViewer Remote Control Application		TeamViewer GmbH	792 K
vmware-usbarbitrator64.exe	1996	VMware USB Arbitration Service		VMware, Inc.	1,308 K
vmanit.exe	1184	VMware NAT Service		VMware, Inc.	2,748 K
RCUService.exe	1404	SplashTop Connect Firefox Software Updater Service		SplashTop Inc.	1,680 K
vmware-authd.exe	1324	VMware Authorization Service		VMware, Inc.	1,880 K
vmnetdhcp.exe	1496	VMware VMnet DHCP service		VMware, Inc.	1,040 K
svchost.exe	2556	Windows	服务主进程	Microsoft Corporation	316 K
taskhost.exe	2880	Windows 任务的主机进程		Microsoft Corporation	4,804 K
svchost.exe	3436	Windows	服务主进程	Microsoft Corporation	22,000 K
SearchIndexer.exe	3900	Microsoft Windows Search 引擎		Microsoft Corporation	19,288 K
SearchProtocolHost.exe	7376	Microsoft Windows Search Protocol Host		Microsoft Corporation	8,060 K
SearchFilterHost.exe	7356	Microsoft Windows Search Filter Host		Microsoft Corporation	6,428 K
svchost.exe	3316	Windows	服务主进程	Microsoft Corporation	4,308 K
lsass.exe	580	0.78 Local Security Authority Process		Microsoft Corporation	8,352 K
lsm.exe	636	本地会话管理器服务		Microsoft Corporation	2,312 K
csrss.exe	528	Client Server Runtime Process		Microsoft Corporation	18,868 K
conhost.exe	5936	控制台窗口主机		Microsoft Corporation	3,112 K
winlogon.exe	608	Windows 登录应用程序		Microsoft Corporation	328 K
explorer.exe	3004	Windows 资源管理器		Microsoft Corporation	80,784 K
RAVCp164.exe	3308	Realtek高清断音频管理器		Realtek Semiconductor	1,032 K
Reexplorer.exe	4120	Microsoft Document Explorer		Microsoft Corporation	12,796 K
formail.exe	5072	0.78 Formail 7.0		Tencent Inc.	18,672 K
WINWORD.EXE	8556	Microsoft Office Word		Microsoft Corporation	5,052 K
Marthon.exe	2848	Marthon3		Marthon Internation...	31,224 K
Marthon.exe	5136	Marthon3		Marthon Internation...	11,760 K
Marthon.exe	8316	Marthon3		Marthon Internation...	18,240 K
Marthon.exe	8616	Marthon3		Marthon Internation...	25,196 K
Marthon.exe	8688	Marthon3		Marthon Internation...	50,868 K
Marthon.exe	8598	Marthon3		Marthon Internation...	282,752 K
SogouCloud.exe	2056	搜狗输入法 云计算代理		Sogou.com Inc.	6,672 K
Marthon.exe	584	Marthon3		Marthon Internation...	9,598 K
Marthon.exe	4904	Marthon3		Marthon Internation...	2,036 K
qq.exe	4268	QQ2012	0.39 QQ2012	Tencent	68,892 K
QQExternal.exe	876	QQMusic		Tencent	22,488 K
QQMusic.exe	8826	QQMusic		Tencent	19,824 K
banbox.exe	5516	Kanbox		北京聚爱网络科技有限公司	37,876 K
procexp64.exe	8376	Sysinternals Process Explorer		Sysinternals - www...	44,416 K
RFMDaemon.exe	3120	Smart Recovery Daemon		Gigabyte Technology...	924 K
ZyngagamesAgent.exe	3544	SplashTop Connect ZyngaGames Agent.		SplashTop Inc.	628 K
vmware-tray.exe	3672	VMware Tray Process		VMware, Inc.	1,520 K
vmware.exe	654	VMware Workstation		VMware, Inc.	82,164 K
vmware-unity-helper.exe	1336	VMware Unity Helper		VMware, Inc.	9,068 K
vmware-vmx.exe	4788	2.33 VMware Workstation VMX		VMware, Inc.	1,242,528 K
vpriproxy.exe	5608	VMware VPrint Proxy		VMware, Inc.	11,736 K
sp1wo64.exe	416	Print driver host for 32bit applications		Microsoft Corporation	1,308 K

CPU Usage: 4.27% Commit Charge: 24.29% 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。

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)

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 人脸识别 (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

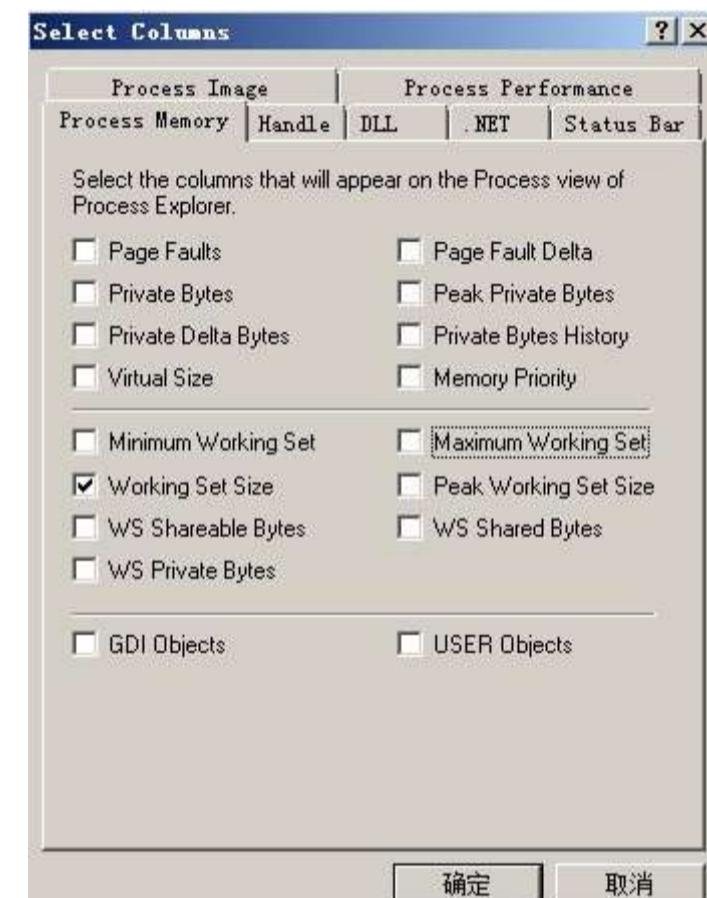
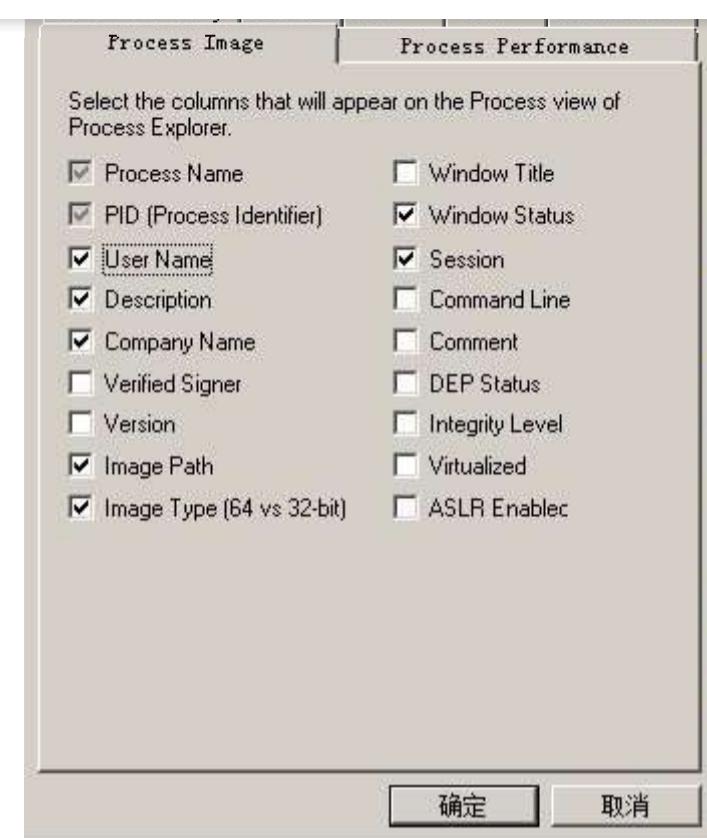
2. Re:C# winform 使用进度条(两种形式)

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



Process	FID	CPU	Work...	User Name	Path	Command Line	Image Type	Se...	GDI...	USE...	Threads
System	4	772	X NT AUTHORITY\SYSTEM		C:\Windows\System32\sms.exe	\SystemRoot\System32\sms.exe	n/a	0	0	138	
smss.exe	280	224	X NT AUTHORITY\SYSTEM		C:\Windows\System32\smss.exe	W\$SystemRoot\smss.exe ObjectDirectory\Windows Share...	64-bit	0	0	2	
crss.exe	428	844	X NT AUTHORITY\SYSTEM		C:\Windows\System32\crss.exe	wininit.exe	64-bit	0	0	9	
wininit.exe	492	304	X NT AUTHORITY\SYSTEM		C:\Windows\System32\wininit.exe	C:\Windows\System32\services.exe	64-bit	0	0	3	
services.exe	552	4,708	X NT AUTHORITY\SYSTEM		C:\Windows\System32\services.exe	C:\Windows\System32\svchost.exe	64-bit	0	0	7	
svchost.exe	736	3,460	X NT AUTHORITY\SYSTEM		C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k DcomLaunch	64-bit	0	0	10	
smss.exe	3098	22,372	X NT AUTHORITY\SYSTEM		C:\Windows\System32\smss.exe	C:\Windows\System32\smss.exe -Embedding	32-bit	0	0	9	
unscapp.exe	3576	1,500	X NT AUTHORITY\SYSTEM		C:\Windows\System32\unscapp.exe	C:\Windows\System32\unscapp.exe -Embedding	64-bit	1	4	4	
TTFHostFor...	8284	2,376	X NT AUTHORITY\SYSTEM		D:\Tencent\QQ\Bin\TTFHostFor.exe	D:\Tencent\QQ\Bin\TTFHostFor.exe -PROCESSID:7600CB12-7604-4048...	32-bit	1	4	3	4
dllhost.exe	8084	82,044	X NT AUTHORITY\SYSTEM		C:\Windows\System32\dlldhost.exe	C:\Windows\System32\DLLHOST.EXE /PROCESSID:7600CB12-7604-4048...	64-bit	1	73	74	10
nwsvc.exe	792	2,620	X NT AUTHORITY\SYSTEM		C:\Windows\System32\nwsvc.exe	C:\Windows\System32\nwsvc.exe	64-bit	0	0	5	
nwdrvnc.exe	1352	0,370	X NT AUTHORITY\SYSTEM		C:\Program Files\NVIDIA Corporation\Display\NvDrvDx...	"C:\Program Files\NVIDIA Corporation\Display\NvDrvDx.exe"	64-bit	1	5	9	7
nwSCAPI.Svr...	816	1,076	X NT AUTHORITY\SYSTEM		C:\Program Files\NVIDIA Corporation\3D Vision...	"C:\Program Files\NVIDIA Corporation\3D Vision\NvSCAPIS...	32-bit	0	0	6	
svchost.exe	860	5,304	X NT AUTHORITY\NETWORK SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k EPCS	64-bit	0	0	10	
svchost.exe	964	11,560	X NT AUTHORITY\LOCAL SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted	64-bit	0	0	19	
svchost.exe	976	16,806	X NT AUTHORITY\SYSTEM		C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystem	64-bit	0	0	11	
svchost.exe	120	17,569	X NT AUTHORITY\SYSTEM		C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k Network	64-bit	0	0	86	
dwm.exe	1004	143,0	X NT AUTHORITY\SYSTEM		C:\Windows\System32\dwm.exe	C:\Windows\System32\dwm.exe -k LocalSystemNetworkRestricted	64-bit	0	0	23	
dwm.exe	2390	2,232	X NT AUTHORITY\SYSTEM		C:\Windows\System32\dwm.exe	C:\Windows\System32\dwm.exe	64-bit	1	6	2	3
svchost.exe	1058	11,216	X NT AUTHORITY\LOCAL SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k LocalService	64-bit	0	0	23	
gvhost.exe	1164	11,164	X NT AUTHORITY\NETWORK SERVICE		C:\Windows\System32\gvhost.exe	C:\Windows\System32\gvhost.exe -k NetworkService	64-bit	0	0	25	
gvhost.exe	1344	2,236	X NT AUTHORITY\SYSTEM		C:\Windows\System32\gvhost.exe	C:\Windows\System32\gvhost.exe	64-bit	0	0	12	
gvhost.exe	1420	5,216	X NT AUTHORITY\LOCAL SERVICE		C:\Windows\System32\gvhost.exe	C:\Windows\System32\gvhost.exe	64-bit	0	0	19	
gvhost.exe	1856	532	X NT AUTHORITY\SYSTEM		C:\Program Files (x86)\Common Files\Adobe\ARM\1.0...	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\gvhost.exe"	32-bit	0	0	4	
BackService...	1792	432	X NT AUTHORITY\SYSTEM		C:\Program Files (x86)\SplashTop\SplashTop Connect...	"C:\Program Files (x86)\SplashTop\SplashTop Connect\BackService...	32-bit	0	0	3	
TimClock...	1812	772	X NT AUTHORITY\SYSTEM		C:\Program Files (x86)\GIGABYTE\SmartTime\TimClock...	"C:\Program Files (x86)\GIGABYTE\SmartTime\TimClock\TimClockDemos..."	32-bit	0	0	0	
alarmclock...	3760	1,760	X NT AUTHORITY\SYSTEM		C:\Program Files (x86)\SplashTop\SplashTop Software...	"C:\Program Files (x86)\SplashTop\SplashTop Software\Update\3...	32-bit	1	13	15	4
SSUService.exe	1860	1,156	X NT AUTHORITY\SYSTEM		C:\Program Files (x86)\SSUService.exe	C:\Windows\System32\svchost.exe	32-bit	0	0	7	
svchost.exe	1928	356	X NT AUTHORITY\LOCAL SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe	64-bit	0	0	6	
TeamViewer...	1956	864	X NT AUTHORITY\SYSTEM		C:\Program Files\TeamViewer\Version6\TeamVi...	C:\Program Files\TeamViewer\Version6\TeamViewer_Service...	32-bit	0	0	6	
vmmwareusb...	1996	1,308	X NT AUTHORITY\SYSTEM		C:\Program Files (x86)\Common Files\VMware\USB\vmw...	C:\Program Files (x86)\Common Files\VMware\USB\vmwareusb...	64-bit	0	0	5	
vmanat.exe	1184	2,812	X NT AUTHORITY\SYSTEM		C:\Windows\System32\vmanat.exe	C:\Windows\System32\svchost.exe	32-bit	0	0	6	
RCUService.exe	1404	1,712	X NT AUTHORITY\SYSTEM		C:\Program Files (x86)\Splashtop\Splashtop Connect...	"C:\Program Files (x86)\Splashtop\Splashtop Connect\RCUService...	32-bit	0	0	7	
vmmwareauth...	1324	1,352	X NT AUTHORITY\SYSTEM		D:\VMS\vmware-authd.exe	D:\VMS\vmware-authd.exe	32-bit	0	0	12	
vmmethdcp.exe	1496	1,076	X NT AUTHORITY\SYSTEM		C:\Windows\System32\vnethdcpc.exe	C:\Windows\System32\vnethdcpc.exe	32-bit	0	0	7	
svchost.exe	2556	2,112	X NT AUTHORITY\NETWORK SERVICE		C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k NetworkServiceNetworkRestricted	64-bit	0	0	3	
taskhost.exe	2880	4,888	X NT AUTHORITY\SYSTEM		C:\Windows\System32\taskhost.exe	C:\Windows\System32\taskhost.exe	64-bit	1	18	19	9
svchost.exe	3436	8,096	X NT AUTHORITY\SYSTEM		C:\Windows\System32\svchost.exe	C:\Windows\System32\svchost.exe -k seccvs	64-bit	0	0	12	
searchindexer...	3900	24,548	X NT AUTHORITY\SYSTEM		C:\Windows\System32\searchindexer.exe	C:\Windows\System32\searchindexer.exe - Embedding	64-bit	0	0	14	
lsass.exe	3116	4,424	X NT AUTHORITY\LOCAL SERVICE		C:\Windows\System32\lsass.exe	C:\Windows\System32\lsass.exe	64-bit	0	0	13	
lm.exe	580	8,404	X NT AUTHORITY\SYSTEM		C:\Windows\System32\lm.exe	C:\Windows\System32\lm.exe	64-bit	0	0	8	
csrss.exe	528	19,732	X NT AUTHORITY\SYSTEM		C:\Windows\System32\crss.exe	C:\Windows\System32\crss.exe ObjectDirectory\Windows Share...	64-bit	1	48	42	12
cnhost.exe	5395	3,112	X NT AUTHORITY\SYSTEM		C:\Windows\System32\cnhost.exe	C:\Windows\System32\cnhost.exe	64-bit	1	21	1	1
winlogon.exe	608	328	X NT AUTHORITY\SYSTEM		C:\Windows\System32\winlogon.exe	C:\Windows\System32\winlogon.exe	64-bit	1	6	3	
explorer.exe	3004	81,172	X NT AUTHORITY\SYSTEM		C:\Windows\explorer.exe	C:\Windows\explorer.exe	64-bit	1	215	755	47
win32kfull.exe	3204	1,052	X NT AUTHORITY\SYSTEM		C:\Windows\kernel32.dll	"C:\Windows\kernel32.dll"	64-bit	1	44	26	11

1. 显示进程的文件路径 (Image Path)



会员 众包 新闻

博问 闪存 赞助商 Trae Chat2DB



--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

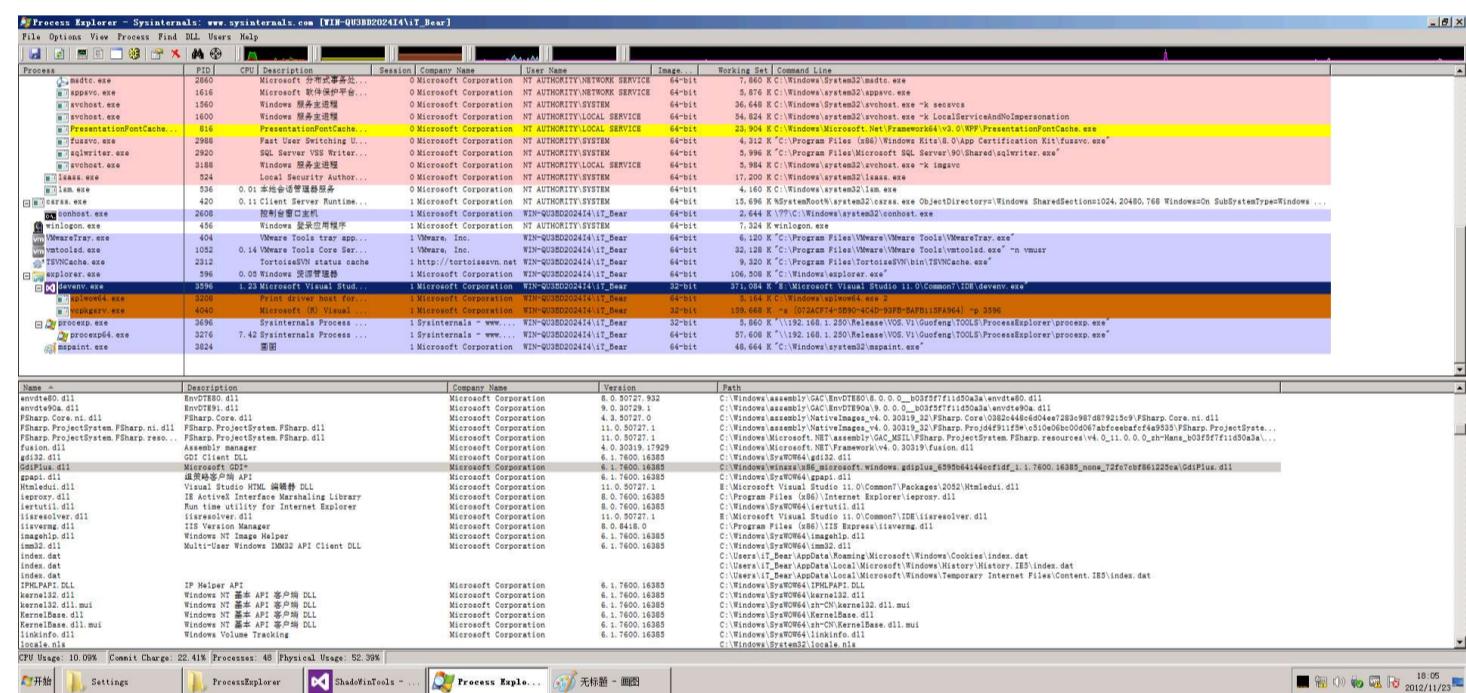
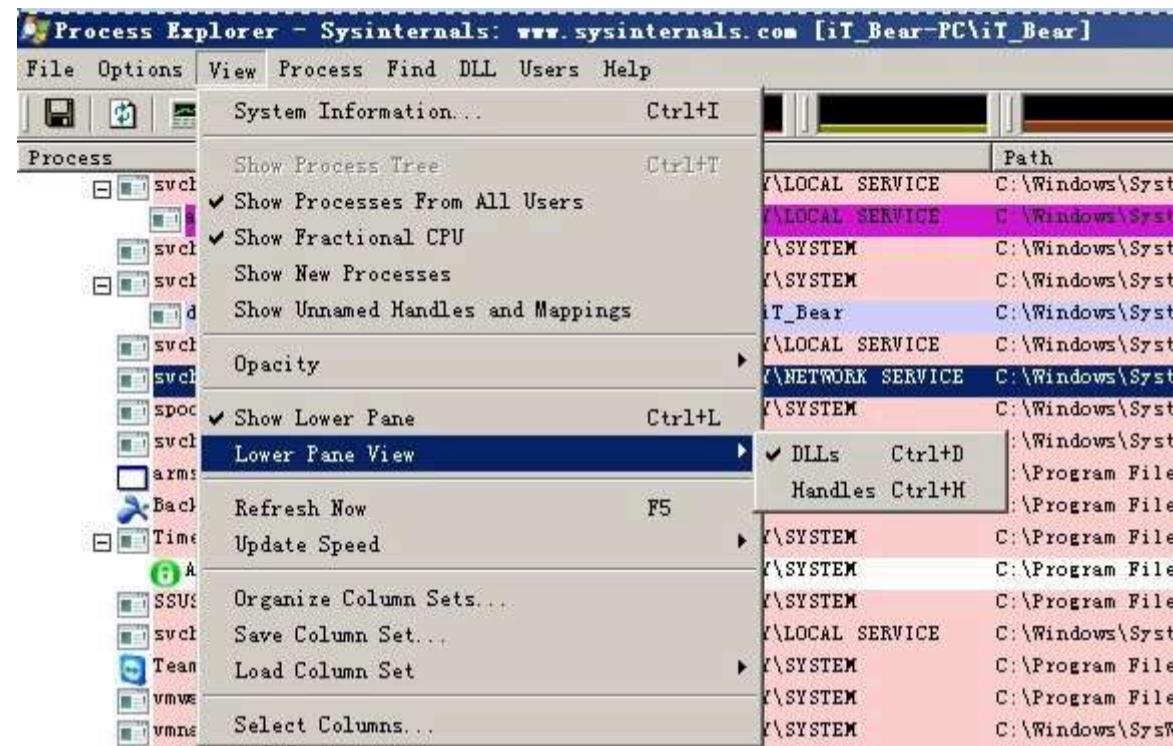
5. Re:MT5：放大市场价格指标

好想学习

--落日赌城

三、显示当前进程所加载的DLL

选择View → Lower Pane View → DLLs



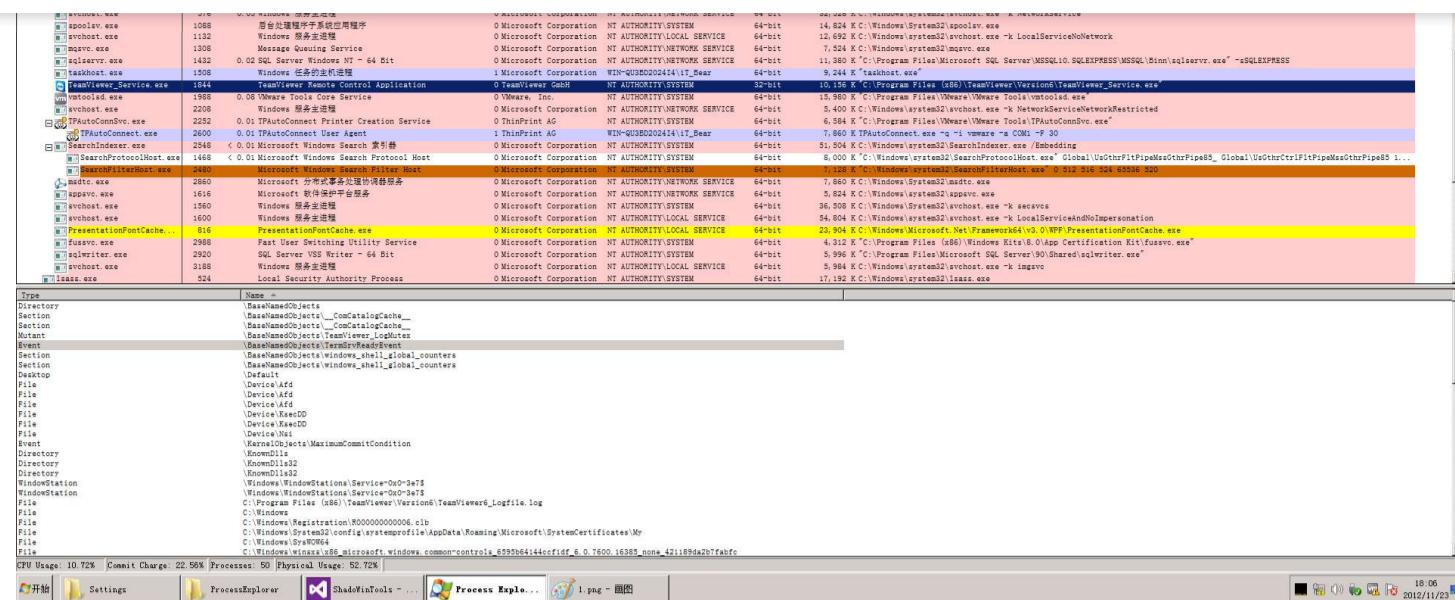
1.通过这种方式可以观察，我们的进程是否被其他程序注入DLL

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



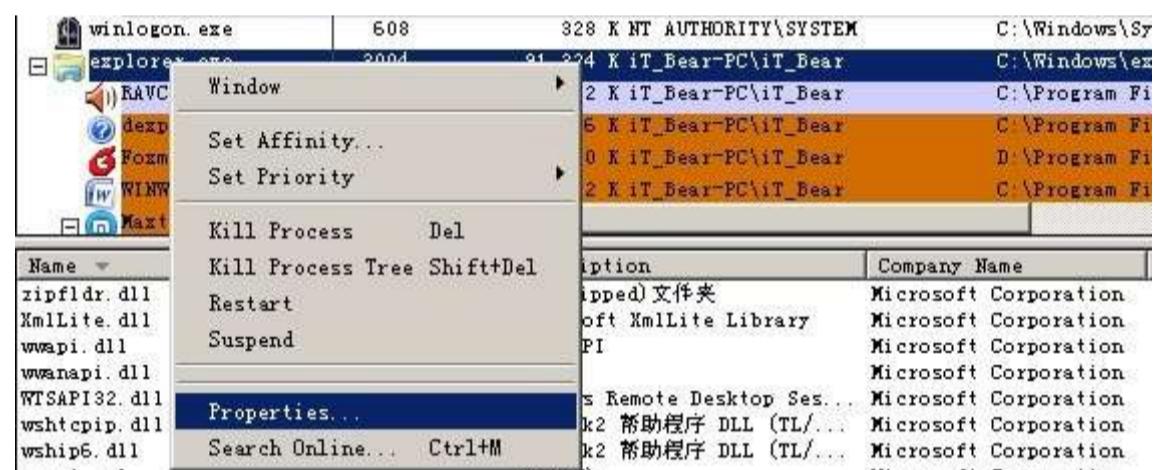
1.查看当前进程所占用的资源句柄表

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）

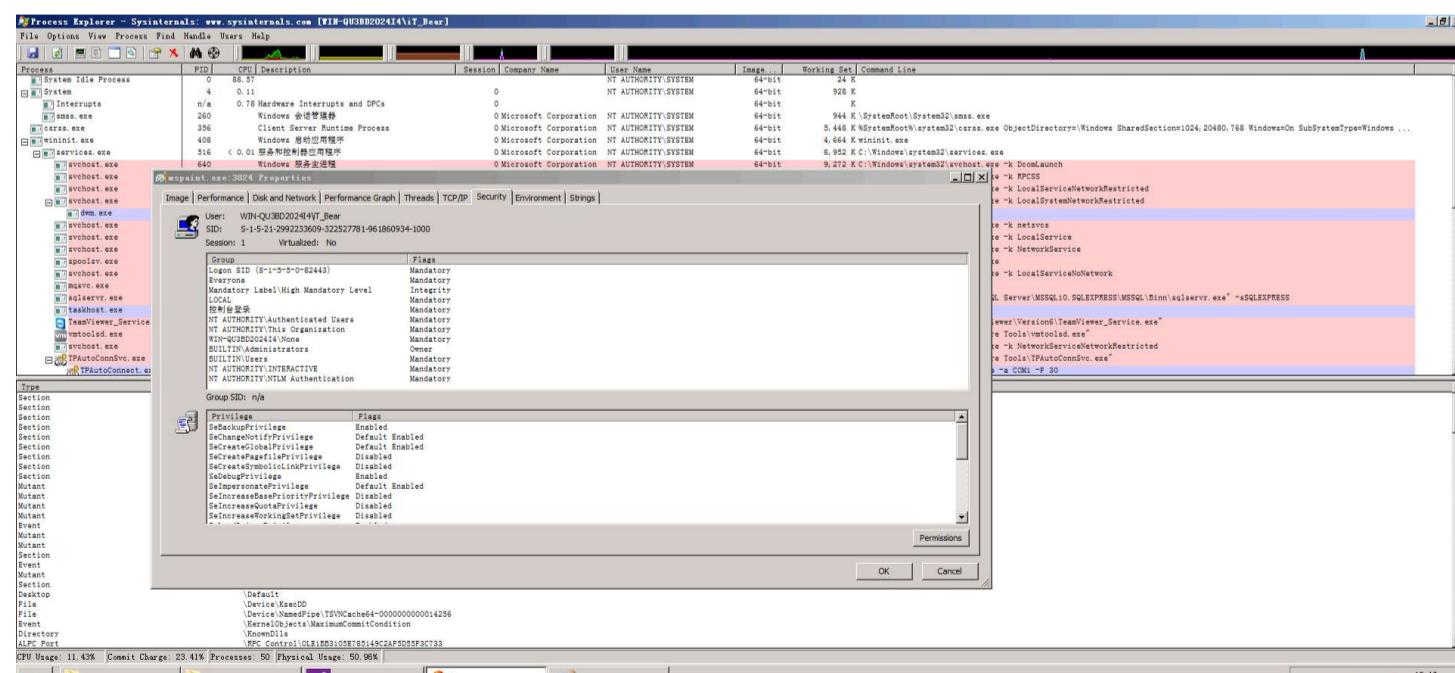
右键单击进程



1.可以结束当前进程，或者当前进程树

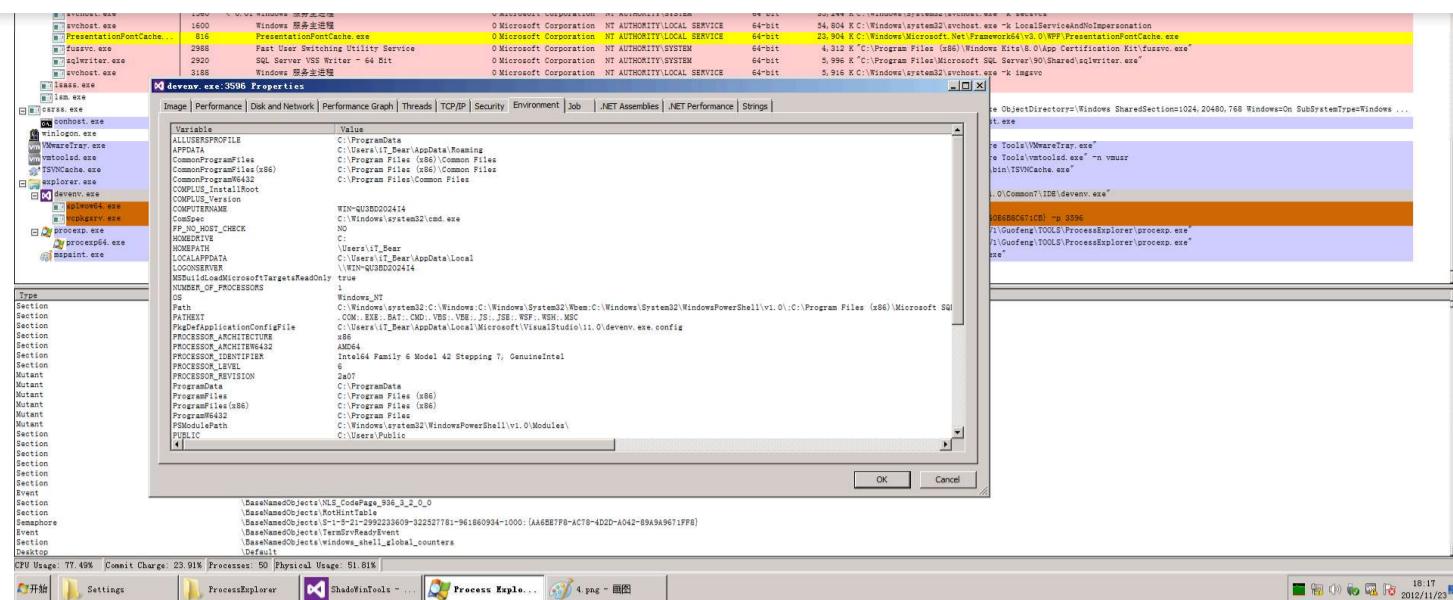
2.可以挂起、重启、从挂其中恢复一个进程

3.查看进程信息（如图-选择Properties）



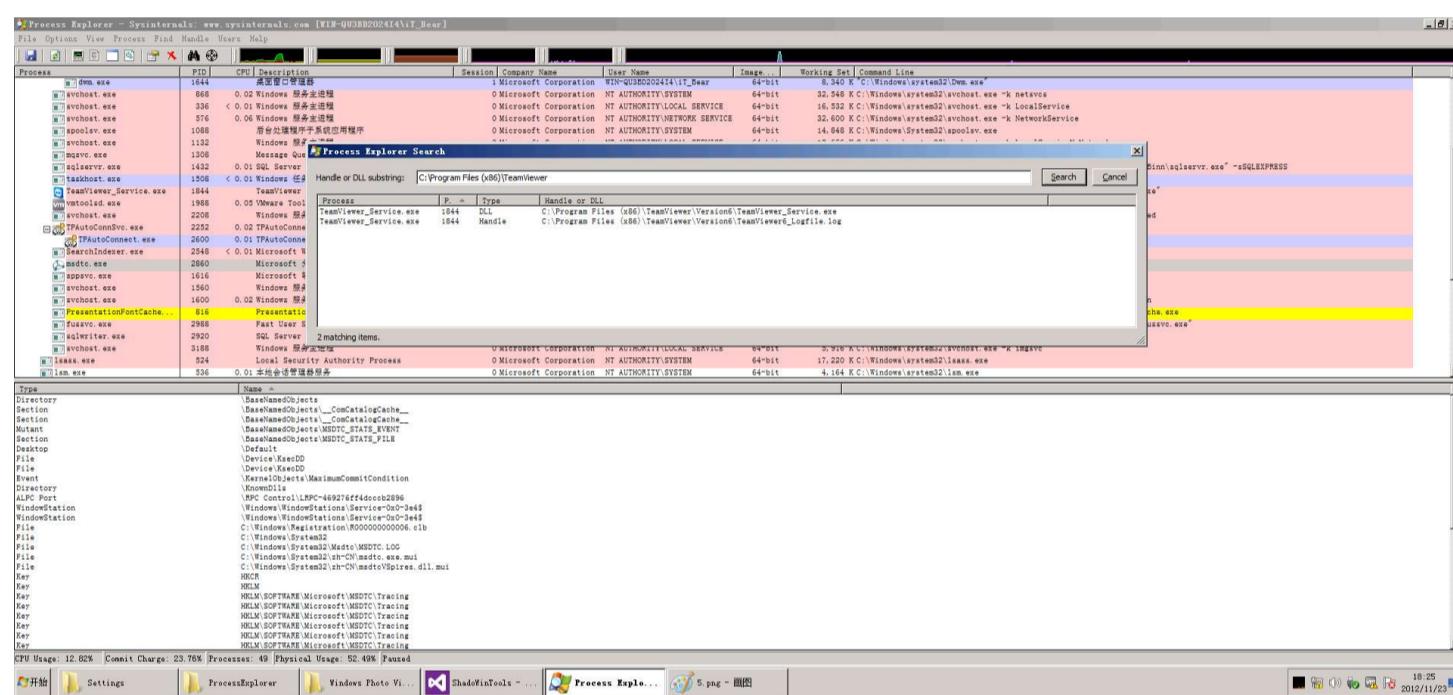
1.可以看到当前进程的用户组信息

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明呢，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



1 0

« 上一篇：解决VS2015安装Android SDK 后文件不全及更新问题

Page 6 of 16



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

博客园 © 2004-2025



浙公网安备 33010602011771号 浙ICP备2021040463号-3