

这是作者的网络安全自学教程系列，主要是关于安全工具和实践操作的在线笔记，特分享出来与博友们学习，希望您们喜欢，一起进步。前文分享了Cracer教程的第一篇文章，详细讲解了安全术语、Web渗透流程和Windows基础、注册表及黑客常用DOS命令。本文将分享Procmon软件基本用法及文件进程、注册表查看，这是一款微软推荐的系统监视工具，功能非常强大可用来检测恶意软件。基础性文章，希望对您有所帮助。

作者作为网络安全的小白，分享一些自学基础教程给大家，主要是关于安全工具和实践操作的在线笔记，希望您们喜欢。同时，更希望您能与我一起操作和进步，后续将深入学习网络安全和系统安全知识并分享相关实验。总之，希望该系列文章对博友有所帮助，写文不易，大神们不喜勿喷，谢谢！如果文章对您有帮助，将是我创作的最大动力，点赞、评论、私聊均可，一起加油喔~

PS：本文参考了安全网站和参考文献中的文章（详见参考文献），并结合自己的经验和实践进行撰写，也推荐大家阅读参考文献。

下载地址：<https://github.com/eastmountyxz/NetworkSecuritySelf-study>

工具地址：<https://github.com/eastmountyxz/Security-Software-Based>

文章目录

一.Process Monitor

1.基本介绍

2.使用场景

3.新闻事件

二.Procmon分析可执行文件

1.常见用法

2.实例分析

三.Promon分析压缩包

四.总结

前文学习：

[网络安全自学篇] 一.入门笔记之看雪Web安全学习及异或解密示例

[网络安全自学篇] 二.Chrome浏览器保留密码功能渗透解析及登录加密入门笔记

[网络安全自学篇] 三.Burp Suite工具安装配置、Proxy基础用法及暴库示例

[网络安全自学篇] 四.实验吧CTF实战之WEB渗透和隐写术解密

[网络安全自学篇] 五.IDA Pro反汇编工具初识及逆向工程解密实战

[网络安全自学篇] 六.OllyDbg动态分析工具基础用法及Crakeme逆向

[网络安全自学篇] 七.快手视频下载之Chrome浏览器Network分析及Python爬虫探讨

[网络安全自学篇] 八.Web漏洞及端口扫描之Nmap、ThreatScan和DirBuster工具

[网络安全自学篇] 九.社会工程学之基础概念、IP获取、IP物理定位、文件属性

[网络安全自学篇] 十.论文之基于机器学习算法的主机恶意代码

[网络安全自学篇] 十一.虚拟机VMware+Kali安装入门及Sqlmap基本用法

[网络安全自学篇] 十二.Wireshark安装入门及抓取网站用户名密码（一）

[网络安全自学篇] 十三.Wireshark抓包原理（ARP劫持、MAC泛洪）及数据流追踪和图像抓取（二）

[网络安全自学篇] 十四.Python攻防之基础常识、正则表达式、Web编程和套接字通信（一）

[网络安全自学篇] 十五.Python攻防之多线程、C段扫描和数据库编程（二）

[网络安全自学篇] 十六.Python攻防之弱口令、自定义字典生成及网站暴库防护

[网络安全自学篇] 十七.Python攻防之构建Web目录扫描器及ip代理池（四）

[网络安全自学篇] 十八.XSS跨站脚本攻击原理及代码攻防演示（一）

[网络安全自学篇] 十九.Powershell基础入门及常见用法（一）

[网络安全自学篇] 二十.Powershell基础入门及常见用法（二）

[网络安全自学篇] 二十一.GeekPwn极客大赛之安全攻防技术总结及ShowTime

[网络安全自学篇] 二十二.Web渗透之网站信息、域名信息、端口信息、敏感信息及指纹信息收集

[网络安全自学篇] 二十三.基于机器学习的恶意请求识别及安全领域中的机器学习

[网络安全自学篇] 二十四.基于机器学习的恶意代码识别及人工智能中的恶意代码检测

[网络安全自学篇] 二十五.Web安全学习路线及木马、病毒和防御初探

[网络安全自学篇] 二十六.Shodan搜索引擎详解及Python命令行调用

[网络安全自学篇] 二十七.Sqlmap基础用法、CTF实战及请求参数设置（一）

[网络安全自学篇] 二十八.文件上传漏洞和Caidao入门及防御原理（一）

[网络安全自学篇] 二十九.文件上传漏洞和IIS6.0解析漏洞及防御原理（二）

[网络安全自学篇] 三十.文件上传漏洞、编辑器漏洞和IIS高版本漏洞及防御（三）

[网络安全自学篇] 三十一.文件上传漏洞之Upload-labs靶场及CTF题目01-10（四）

[网络安全自学篇] 三十二.文件上传漏洞之Upload-labs靶场及CTF题目11-20（五）

[网络安全自学篇] 三十三.文件上传漏洞之绕狗一句话原理和绕过安全狗（六）

[网络安全自学篇] 三十四.Windows系统漏洞之5次Shift漏洞启动计算机

[网络安全自学篇] 三十五.恶意代码攻击溯源及恶意样本分析

[网络安全自学篇] 三十六.WinRAR漏洞复现（CVE-2018-20250）及恶意软件自启动劫持

[网络安全自学篇] 三十七.Web渗透提高班之hack the box在线靶场注册及入门知识

[网络安全自学篇] 三十八.hack the box渗透之BurpSuite和Hydra密码爆破及Python加密Post请求（二）

[网络安全自学篇] 三十九.hack the box渗透之DirBuster扫描路径及Sqlmap高级注入用法（三）

[网络安全自学篇] 四十.phpMyAdmin 4.8.1后台文件包含漏洞复现及详解（CVE-2018-12613）

[网络安全自学篇] 四十一.中间人攻击和ARP欺骗原理详解及漏洞还原

[网络安全自学篇] 四十二.DNS欺骗和钓鱼网站原理详解及漏洞还原

[网络安全自学篇] 四十三.木马原理详解、远程服务器IPC\$漏洞及木马植入实验

[网络安全自学篇] 四十四.Windows远程桌面服务漏洞（CVE-2019-0708）复现及详解

[网络安全自学篇] 四十五.病毒详解及批处理病毒制作（自启动、修改密码、定时关机、蓝屏、进程关闭）

[网络安全自学篇] 四十六.微软证书漏洞CVE-2020-0601 (上)Windows验证机制及可执行文件签名复现

[网络安全自学篇] 四十七.微软证书漏洞CVE-2020-0601 (下)Windows证书签名及HTTPS网站劫持

[网络安全自学篇] 四十八.Cracer第八期——(1)安全术语、Web渗透流程、Windows基础、注册表及黑客常用DOS命令

前文欣赏：

[渗透&攻防] 一.从数据库原理学习网络攻防及防止SQL注入

[渗透&攻防] 二.SQL MAP工具从零解读数据库及基础用法

[渗透&攻防] 三.数据库之差异备份及Caidao利器

[渗透&攻防] 四.详解MySQL数据库攻防及Fiddler神器分析数据包

声明：本人坚决反对利用教学方法进行犯罪的行为，一切犯罪行为必将受到严惩，绿色网络需要我们共同维护，更推荐大家了解它们背后的原理，更好地进行防护。

一.Process Monitor

1.基本介绍

Process Monitor是微软推荐的一款系统监视工具，能够实时显示文件系统、注册表（读写）、网络连接与进程活动的高级工具。它整合了旧的Sysinternals工具、Filemon与Regmon，其中Filemon专门用来监视系统中的任何文件操作过程，Regmon用来监视注册表的读写操作过程。

- Filemon：文件监视器
- Regmon：注册表监视器

同时，Process Monitor增加了进程ID、用户、进程可靠度等监视项，可以记录到文件中。它的强大功能足以使Process Monitor成为您系统中的核心组件以及病毒探测工具。



Procmon.exe

Process Monitor可以帮助使用者对系统中的任何文件、注册表操作进行监视和记录，通过注册表和文件读写的变化，有效帮助诊断系统故障或发现恶意软件、病毒及木马。

Github下载地址：<https://github.com/eastmountyxz/Security-Software-Based>

CSDN下载链接：<https://download.csdn.net/download/lxiao428/10711509>

2.使用场景

运行Process Monitor建议使用管理员模式，当你启动Process Monitor后，它就开始监听三类操作，包括：文件系统、注册表、进程。

- **文件系统**

Process Monitor显示所有的Windows文件系统活动，包括本地磁盘和远程文件系统。它会自动探测到新的文件系统设备并监听它们。所有的系统路径都会被显示为相对于在用户会话中的一个文件系统操作的执行。想在列表中清除文件系统的操作，在Process Monitor工具栏上反选“文件系统”按钮，再按下可以增加对文件系统的监听。

- **注册表**

Process Monitor记录所有的注册表操作并显示使用常见的注册表根键缩写来显示注册表路径（如HEKY_LOCAL_MACHINE 缩写为HKLM）。想在列表中清除注册表的操作，在Process Monitor工具栏上反选“注册表”按钮，再次按下可以增加对注册表的监听。

- **进程**

在Process Monitor的进程/线程监听子系统中，它将跟踪所有进程/线程的创建和退出操作，包括DLL和设备驱动程序的加载操作。想在列表中清除进程的操作，在Process Monitor工具栏上反选“进程”按钮，再次按下可以增加对进程的监听。

- **网络**

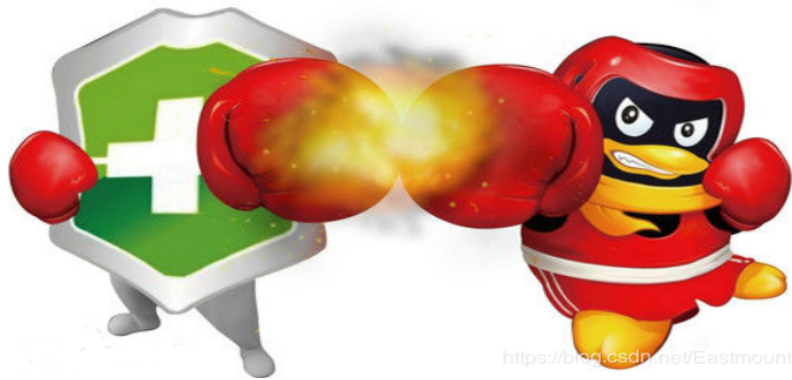
Process Monitor使用“Windows事件跟踪(ETW)”来跟踪并记录TCP和UDP活动。每个网络操作包括源地址和目标地址，还有发送和接受到的一些数量的数据，但不包括真实的数据。想在列表中清除网络的操作，在Process Monitor工具栏上反选“网络”按钮，再次按下可以增加对网络的监听。

• 性能分析

这个事件类可以在“选项”菜单中启用。当处于“启用”状态，Process Monitor扫描系统中所有活动的线程并为每个线程生成一个性能分析事件，记录了内核模式和用户模式的CPU时间消耗，还有许多在上个性能分析事件后已被线程执行的环境开关。

3.新闻事件

关于Procmon软件的传闻：曾经360隐私保护器曝出腾讯“窥私门”事件。当年的QQ聊天工具在暗中密集扫描电脑硬盘、窥视用户的隐私文件，另两款聊天工具MSN和阿里旺旺则没有类似行为。随即有网友爆料称，早有人通过微软Procmon（进程监视工具）发现QQ窥私的秘密。



据悉，微软这款Windows系统进程监视工具Procmon，通过对系统中的任何文件和注册表操作进行监视和记录，也能帮助用户判断软件是否存在“越轨”行为。与360隐私保护器相比，Procmon采用了类似的原理，但是监测对象更广泛，适合具备一定电脑知识的用户使用。

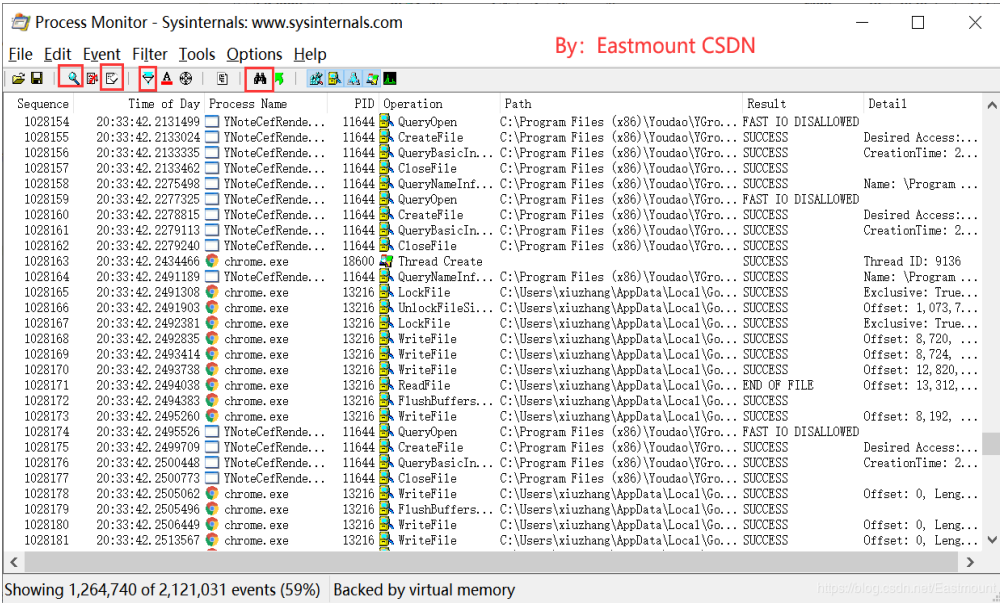
Procmon监测记录表明，当时的QQ会自动访问许多与聊天无关的程序和文档，例如“我的文档”等敏感位置，上网记录等。随后，QQ还会产生大量网络通讯，很可能是将数据上传到腾讯服务器。短短10分钟内，它访问的无关文件和网络通讯数量多达近万项！正常的聊天工具行为是只访问自身文件和必要的系统文件。

二.Procmon分析可执行文件

1.常见用法

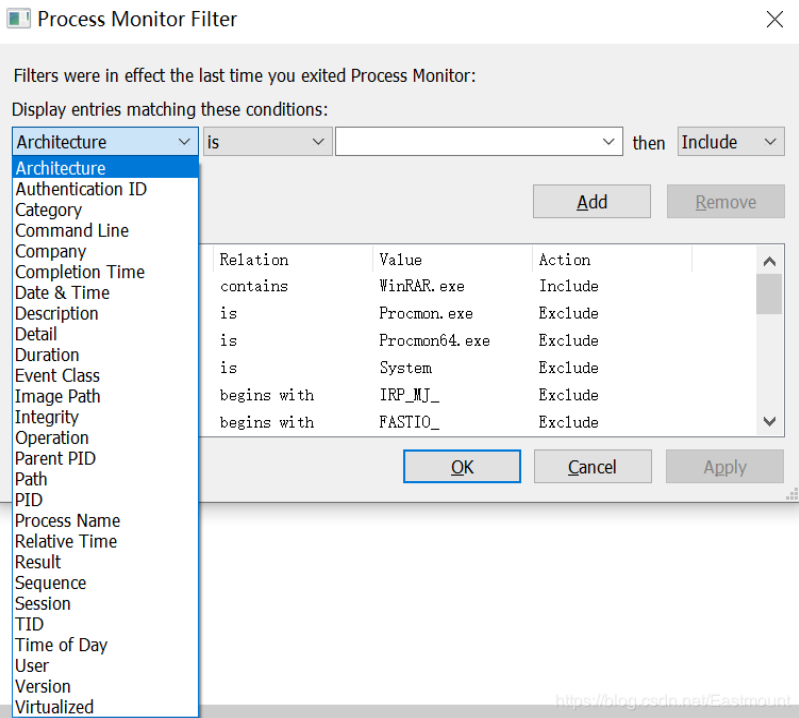
下载Procmon.exe软件后，直接双击启动，Procmon会自动扫描分析系统当前程序的运行情况。其中，下图框出来的4个常用按钮作用分别为：捕获开关、清屏、设置过滤条件、查找。最后5个并排的按钮，是用来设置捕获哪些类型的事件，分别表示注册表的读

写、文件的读写、网络的连接、进程和线程的调用和配置事件。一般选择前面2个，分别为注册表和文件操作。



输出结果中包括序号、时间点、进程名称、PID、操作、路径、结果、描述等，监控项通常包括：

- 文件系统
- 注册表
- 进程：跟踪所有进程和线程的创建和退出操作
- 剖析事件：扫描系统中所有活动线程，为每个线程创建一个剖析事件，记录它耗费的核心和用户CPU时间，以及该线程自上次剖析事件以来执行了多少次上下文转换



为了更好地定制选择，可以在过滤器中进行设置（见上图），也可以在Options菜单中选择Select Columns选项，然后通过弹出的列选择对话框来定制列的显示。常用列的选择包括：

- **Application Details**

- Process Name：产生事件的那个进程的名字
- Image Path：进程镜像的完整路径
- Command Line：命令行，用于启动进程
- Company Name：进程镜像文件中的企业名称。这个文本是由应用程序的开发者来定义的
- Description：进程镜像文件中的产品描述信息。这个文本是由应用程序的开发者定义的
- Version：进程镜像文件中的产品版本号。这个文本是由应用程序的开发者定义的

- **Event Details**

- Sequence Number：操作在全体事件中的相对位置，也包括当前的过滤
- Event Class：事件的类别（文件，注册表，进程）
- Operation：特殊事件操作，比如Read、RegQueryValue等
- Date & Time：操作的日期和时间
- Time of Day：只是操作的时间
- Path：一个事件引用资源的路径
- Detail：事件的附加信息
- Result：一个完成了的操作的状态码
- Relative Time：一个操作相对于Process Monitor的启动后的时间，或者相对于Process Monitor的信息清除后的时间
- Duration：一个已经完成了的操作所持续的时间

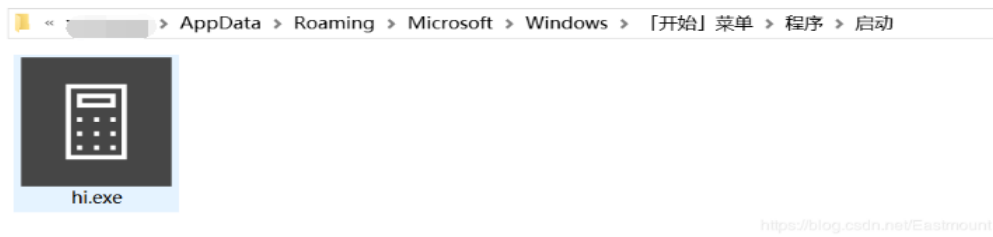
- **Process Management**

- User Name：正在执行操作的进程的用户账户名
- Session ID：正在执行操作的进程的Windows会话ID
- Authentication ID：正在执行操作的进程的登录会话ID
- Process ID：执行了操作的进程的进程ID
- Thread ID：执行了操作的线程的线程ID
- Integrity Level：正在运行的进程执行操作时的可信级别（仅支持Vista以上系统）
- Virtualized：执行了操作的进程的虚拟化状态

2.实例分析

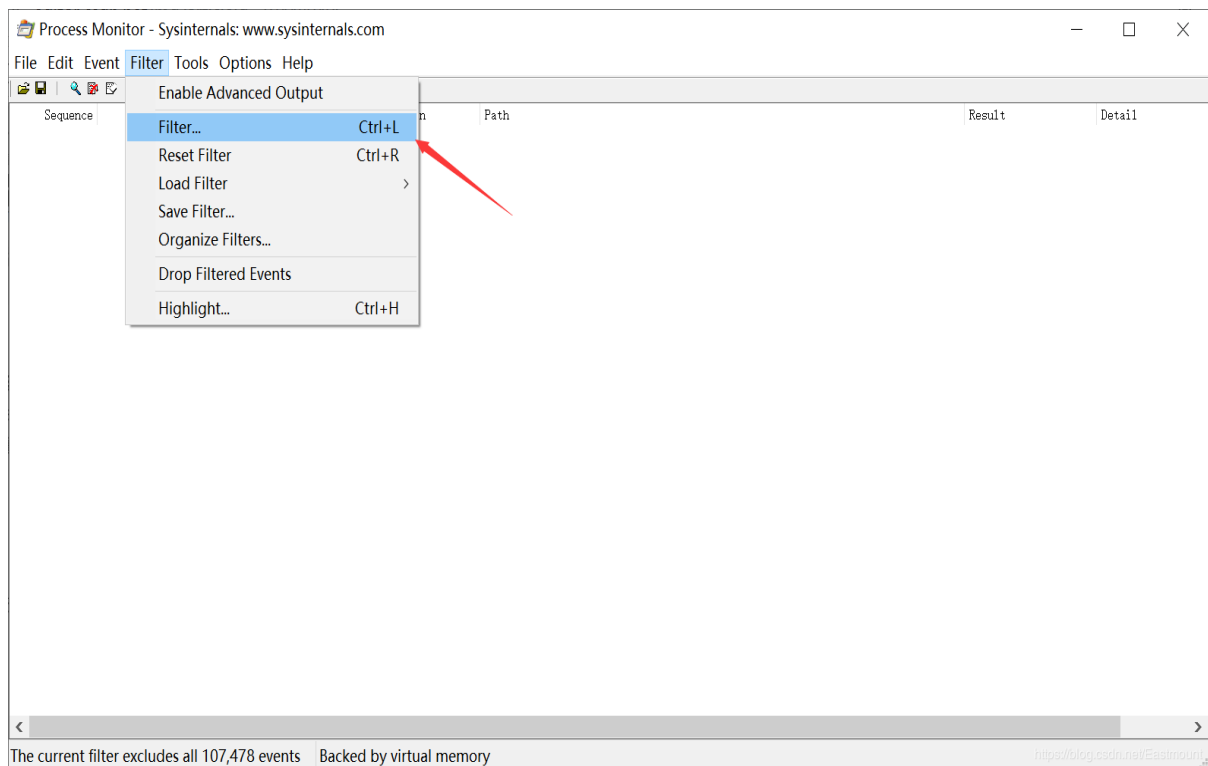
下面我们采用分析开机自启动的某个“hi.exe”程序。注意，作者之前第36篇文章CVE漏洞复现文章中，将“hi.exe”恶意加载至自启动目录，这里分析它。

C:\Users\xxxx\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

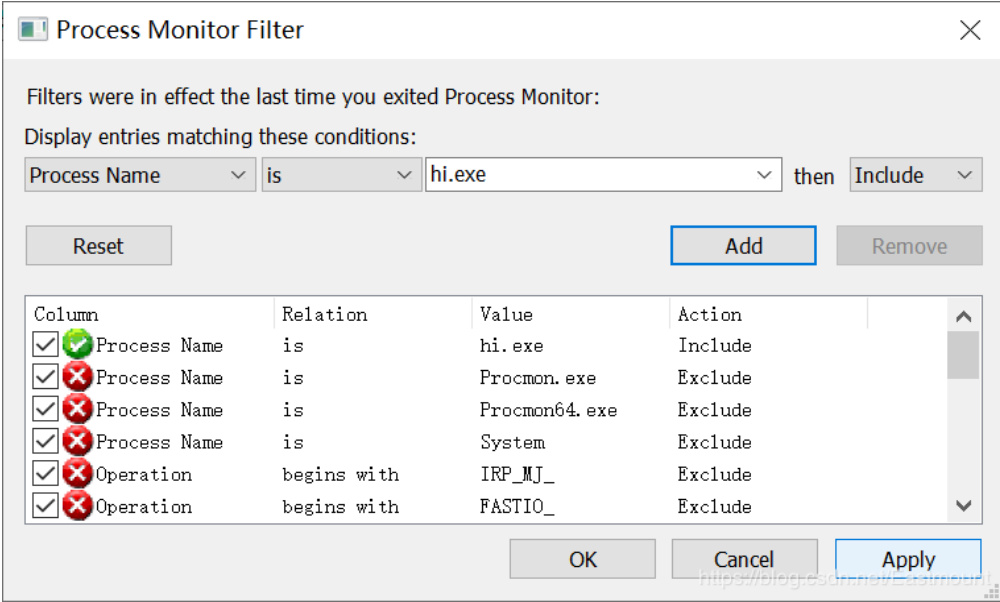


第一步，设置过滤器。

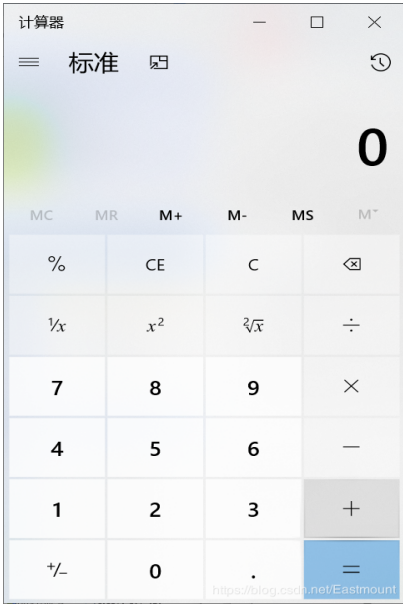
打开软件Process Monitor，并点击filter->filter。



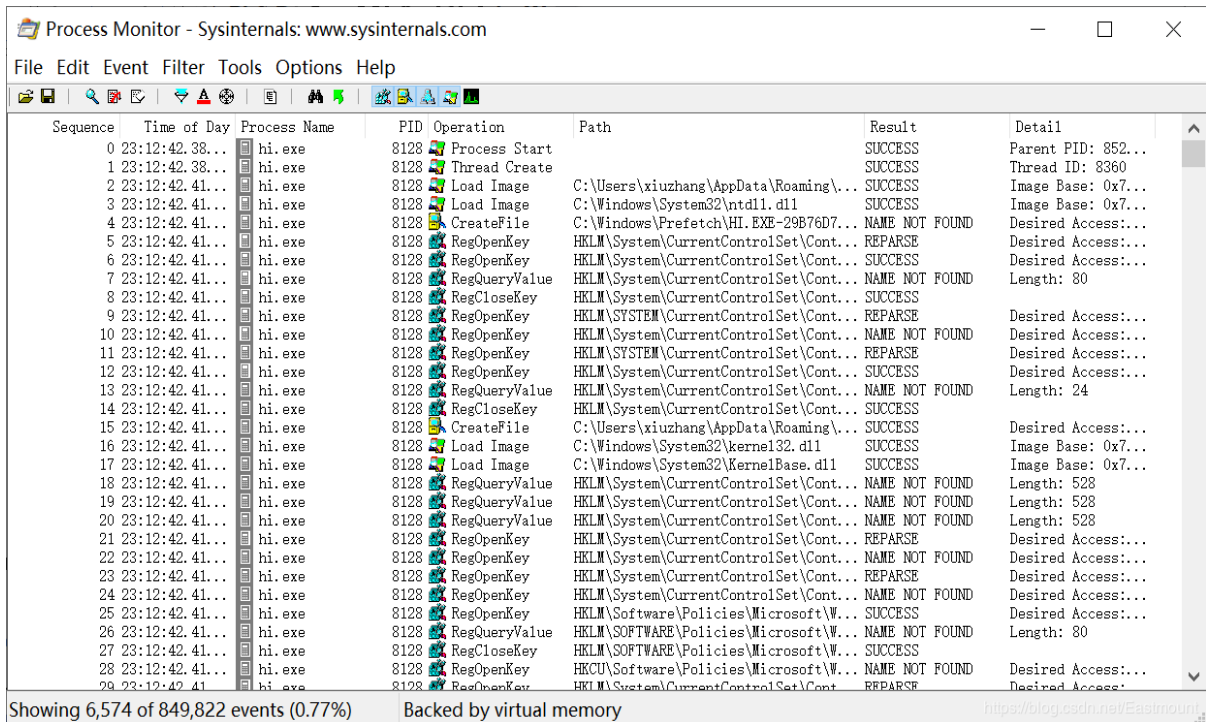
在弹出的对话框中Architecture下拉框，选择Process Name填写要分析的应用程序名字，点击Add添加，最后点击右下角的Apply。



第二步，执行被分析的应用。
双击应用程序会弹出“计算器”。



可以看到Process Mointor监控到应用的行为。

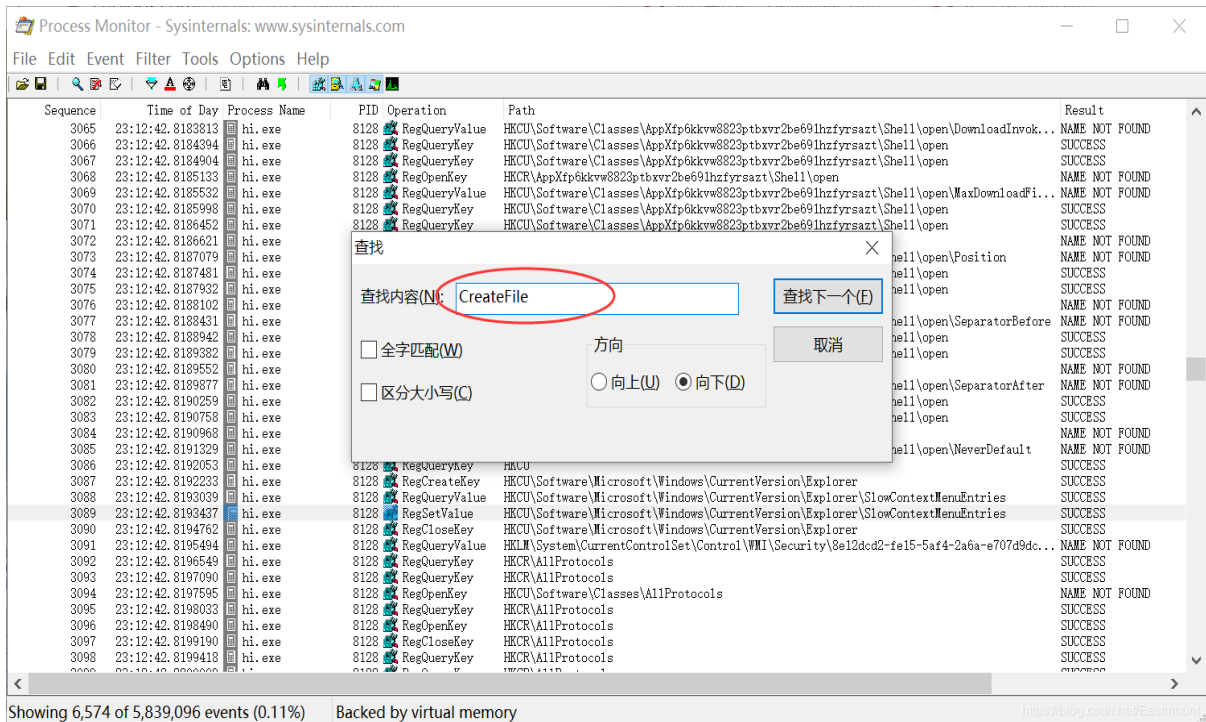


Sequence	Time of Day	Process Name	PID	Operation	Path	Result	Detail
0	23:12:42.38...	hi.exe	8128	Process Start		SUCCESS	Parent PID: 852...
1	23:12:42.38...	hi.exe	8128	Thread Create		SUCCESS	Thread ID: 8360
2	23:12:42.41...	hi.exe	8128	Load Image	C:\Users\xiuzhang\AppData\Roaming\...	SUCCESS	Image Base: 0x7...
3	23:12:42.41...	hi.exe	8128	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7...
4	23:12:42.41...	hi.exe	8128	CreateFile	C:\Windows\Prefetch\HI.EXE-29B76D7...	NAME NOT FOUND	Desired Access:...
5	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\System\CurrentControlSet\Cont...	REPARSE	Desired Access:...
6	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\System\CurrentControlSet\Cont...	SUCCESS	Desired Access:...
7	23:12:42.41...	hi.exe	8128	RegQueryValue	HKLM\System\CurrentControlSet\Cont...	NAME NOT FOUND	Length: 80
8	23:12:42.41...	hi.exe	8128	RegCloseKey	HKLM\System\CurrentControlSet\Cont...	SUCCESS	
9	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Cont...	REPARSE	Desired Access:...
10	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\System\CurrentControlSet\Cont...	NAME NOT FOUND	Desired Access:...
11	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Cont...	REPARSE	Desired Access:...
12	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\System\CurrentControlSet\Cont...	SUCCESS	Desired Access:...
13	23:12:42.41...	hi.exe	8128	RegQueryValue	HKLM\System\CurrentControlSet\Cont...	NAME NOT FOUND	Length: 24
14	23:12:42.41...	hi.exe	8128	RegCloseKey	HKLM\System\CurrentControlSet\Cont...	SUCCESS	
15	23:12:42.41...	hi.exe	8128	CreateFile	C:\Users\xiuzhang\AppData\Roaming\...	SUCCESS	Desired Access:...
16	23:12:42.41...	hi.exe	8128	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7...
17	23:12:42.41...	hi.exe	8128	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7...
18	23:12:42.41...	hi.exe	8128	RegQueryValue	HKLM\System\CurrentControlSet\Cont...	NAME NOT FOUND	Length: 528
19	23:12:42.41...	hi.exe	8128	RegQueryValue	HKLM\System\CurrentControlSet\Cont...	NAME NOT FOUND	Length: 528
20	23:12:42.41...	hi.exe	8128	RegQueryValue	HKLM\System\CurrentControlSet\Cont...	NAME NOT FOUND	Length: 528
21	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\System\CurrentControlSet\Cont...	REPARSE	Desired Access:...
22	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\System\CurrentControlSet\Cont...	NAME NOT FOUND	Desired Access:...
23	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\System\CurrentControlSet\Cont...	REPARSE	Desired Access:...
24	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\System\CurrentControlSet\Cont...	NAME NOT FOUND	Desired Access:...
25	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\Software\Policies\Microsoft\W...	SUCCESS	Desired Access:...
26	23:12:42.41...	hi.exe	8128	RegQueryValue	HKLM\Software\Policies\Microsoft\W...	NAME NOT FOUND	Length: 80
27	23:12:42.41...	hi.exe	8128	RegCloseKey	HKLM\Software\Policies\Microsoft\W...	SUCCESS	
28	23:12:42.41...	hi.exe	8128	RegOpenKey	HKCU\Software\Policies\Microsoft\W...	NAME NOT FOUND	Desired Access:...
29	23:12:42.41...	hi.exe	8128	RegOpenKey	HKLM\System\CurrentControlSet\Cont...	REPARSE	Desired Access:...

Showing 6,574 of 849,822 events (0.77%) Backed by virtual memory

第三步，查看可执行文件的位置。

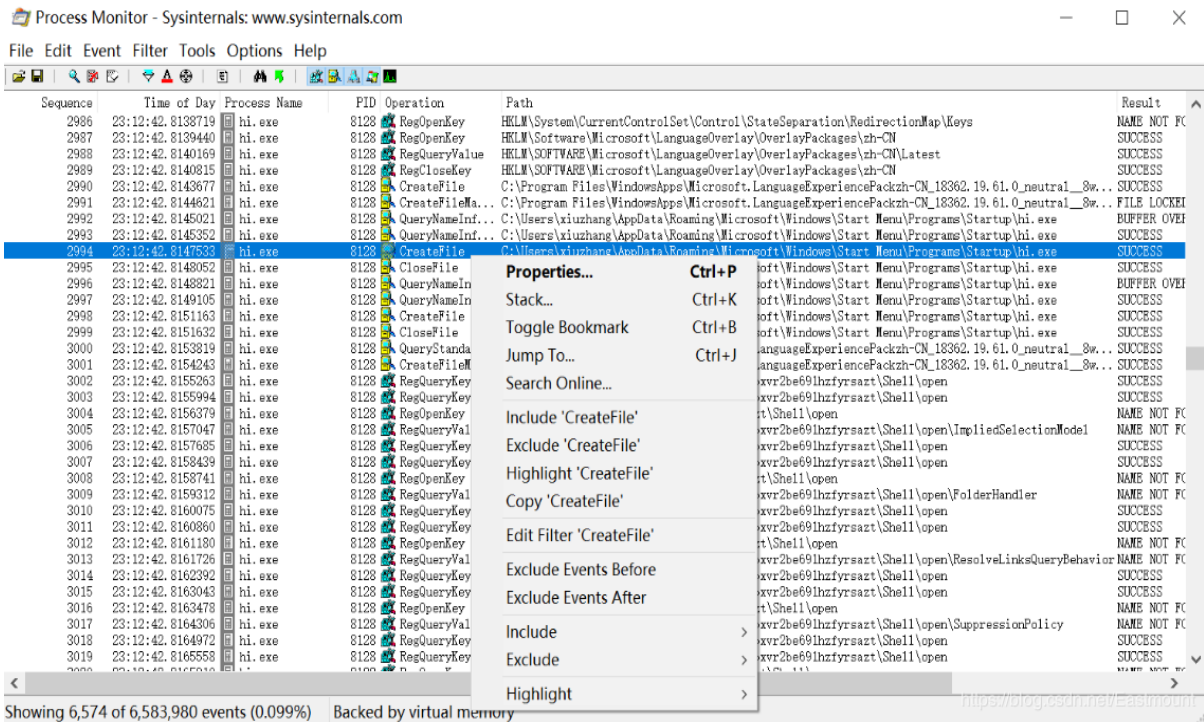
点击查找按钮，然后输入“CreateFile”。



Sequence	Time of Day	Process Name	PID	Operation	Path	Result	Detail
3065	23:12:42.8183813	hi.exe	8128	RegQueryValue	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open\DownloadInvok...	NAME NOT FOUND	
3066	23:12:42.8184394	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	SUCCESS	
3067	23:12:42.8184904	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	SUCCESS	
3068	23:12:42.8185133	hi.exe	8128	RegOpenKey	HKCR\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	NAME NOT FOUND	
3069	23:12:42.8185532	hi.exe	8128	RegQueryValue	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open\MaxDownloadFi...	NAME NOT FOUND	
3070	23:12:42.8185998	hi.exe	8128	RegQueryValue	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	SUCCESS	
3071	23:12:42.8186452	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	SUCCESS	
3072	23:12:42.8186621	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	NAME NOT FOUND	
3073	23:12:42.8187079	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	NAME NOT FOUND	
3074	23:12:42.8187481	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	SUCCESS	
3075	23:12:42.8187932	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	SUCCESS	
3076	23:12:42.8188102	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	NAME NOT FOUND	
3077	23:12:42.8188431	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	NAME NOT FOUND	
3078	23:12:42.8188942	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	SUCCESS	
3079	23:12:42.8189382	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	SUCCESS	
3080	23:12:42.8189552	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	NAME NOT FOUND	
3081	23:12:42.8189877	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	NAME NOT FOUND	
3082	23:12:42.8190259	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	SUCCESS	
3083	23:12:42.8190758	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	SUCCESS	
3084	23:12:42.8190968	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	NAME NOT FOUND	
3085	23:12:42.8191329	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	NAME NOT FOUND	
3086	23:12:42.8192053	hi.exe	8128	RegQueryKey	HKCU\Software\Classes\AppXfp6kkw8823ptbxvr2be691hzfysazt\Shell\open	SUCCESS	
3087	23:12:42.8192233	hi.exe	8128	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	
3088	23:12:42.8193039	hi.exe	8128	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries	SUCCESS	
3089	23:12:42.8193437	hi.exe	8128	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SlowContextMenuEntries	SUCCESS	
3090	23:12:42.8194762	hi.exe	8128	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	
3091	23:12:42.8195494	hi.exe	8128	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\8e12dcd2-fe15-5af4-2a6a-e707d9dc...	NAME NOT FOUND	
3092	23:12:42.8196549	hi.exe	8128	RegQueryKey	HKCR\AllProtocols	SUCCESS	
3093	23:12:42.8197090	hi.exe	8128	RegQueryKey	HKCR\AllProtocols	SUCCESS	
3094	23:12:42.8197595	hi.exe	8128	RegOpenKey	HKCU\Software\Classes\AllProtocols	NAME NOT FOUND	
3095	23:12:42.8198033	hi.exe	8128	RegQueryKey	HKCR\AllProtocols	SUCCESS	
3096	23:12:42.8198490	hi.exe	8128	RegOpenKey	HKCR\AllProtocols	SUCCESS	
3097	23:12:42.8199190	hi.exe	8128	RegCloseKey	HKCR\AllProtocols	SUCCESS	
3098	23:12:42.8199418	hi.exe	8128	RegQueryKey	HKCR\AllProtocols	SUCCESS	

Showing 6,574 of 5,839,096 events (0.11%) Backed by virtual memory

找到该选项之后，我们右键点击“Jump To”。



我们可以去到该文件所在的文件夹下，即：

Win 7/10: C:\Users\xxxx\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Win XP: C:\Documents and Settings\Administrator\「开始」菜单\程序\启动

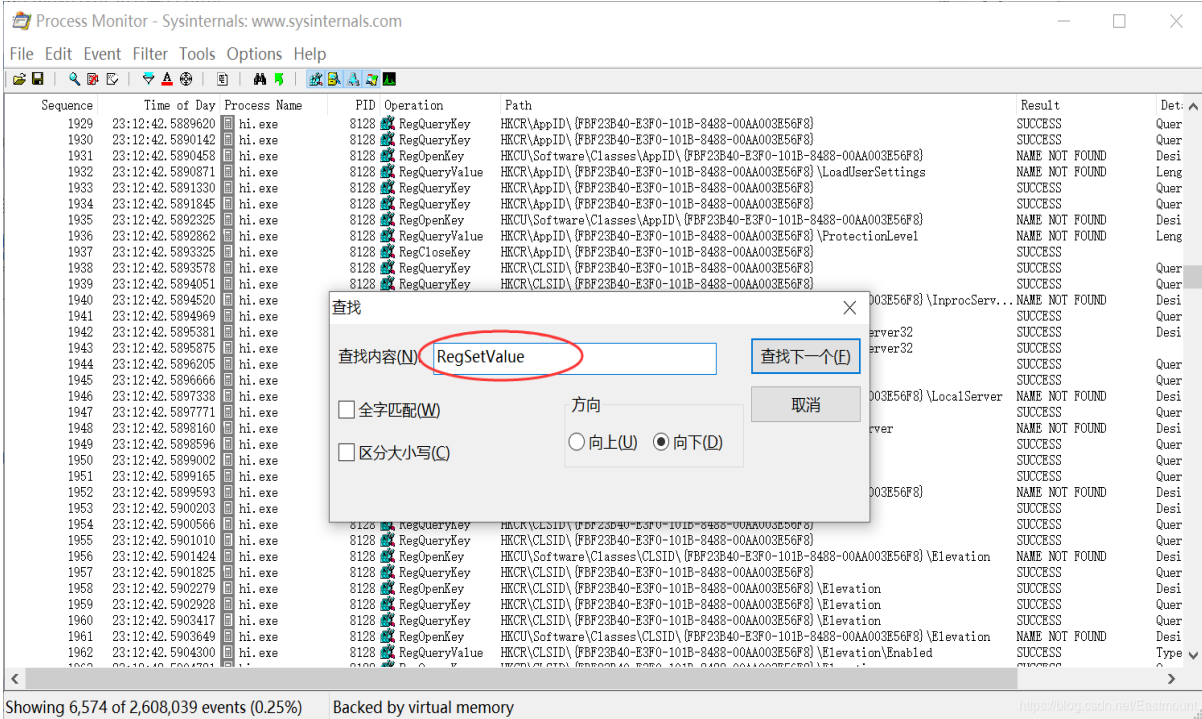
« AppData > Roaming > Microsoft > Windows > 「开始」菜单 > 程序 > 启动



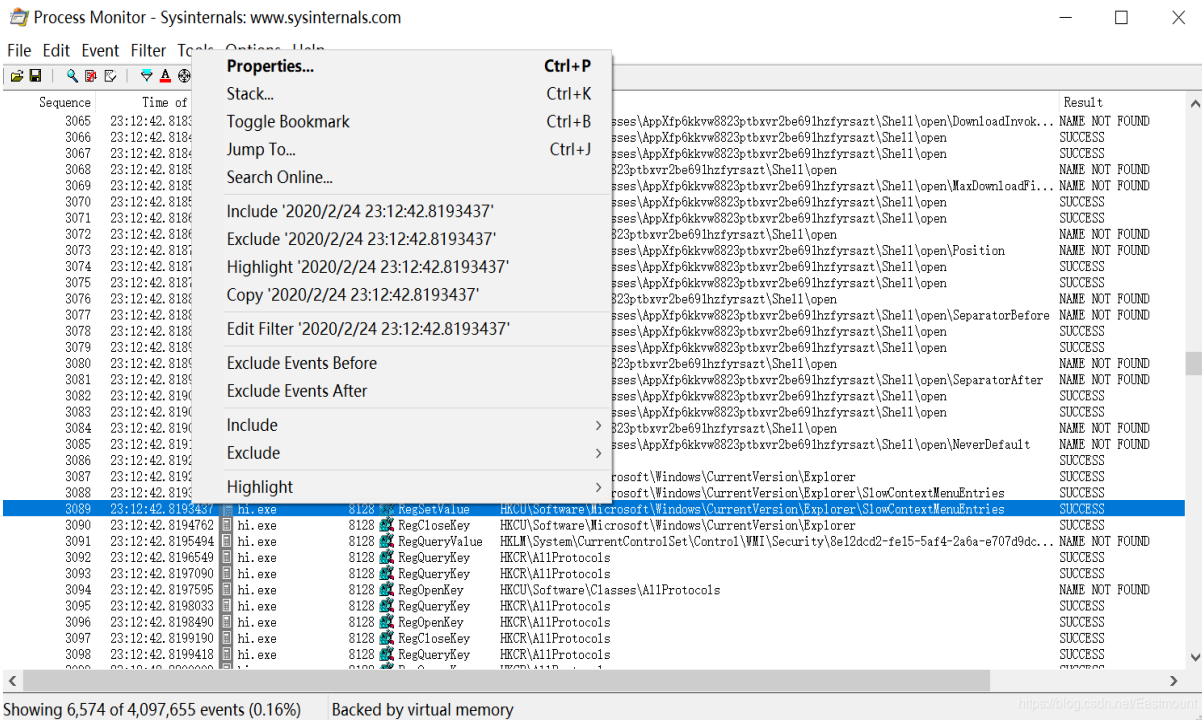
hi.exe

<https://blog.csdn.net/Eastmount>

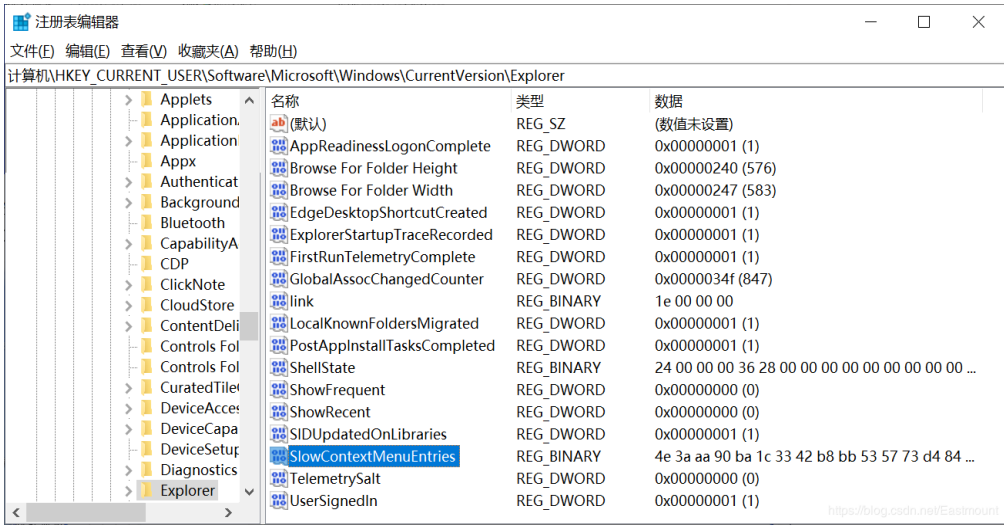
第四步，查看注册表选项。
查寻文件“RegSetValue”。



右键选择jump to跳转到注册表。



可以看到注册表的内容，如果自启动还能看到相关键对的设置。



Windows自动重启运行的程序可以注册在下列任一注册表的位置。

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

三.Promon分析压缩包

接着我们分析该压缩包。



blog02-pyecharts.rar

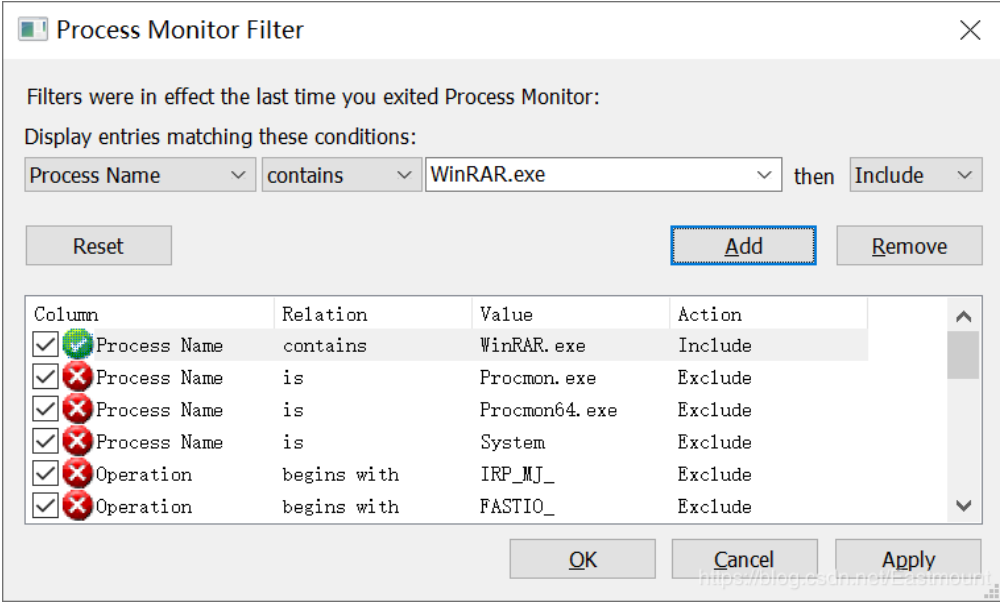


Procmon.exe

<https://blog.csdn.net/Eastmount>

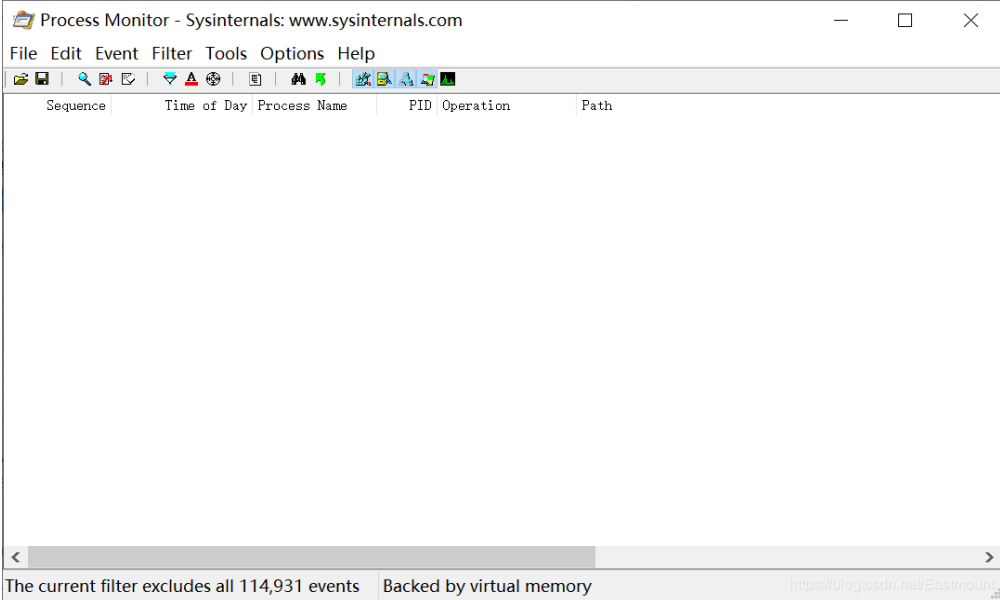
第一步，过滤器设置。

打开软件Process Monitor，并点击filter->filter。在弹出的对话框中Architecture下拉框，选择Process Name填写要分析的应用程序名字，点击Add添加、Apply应用。注意，也可以增加其他过滤规则。

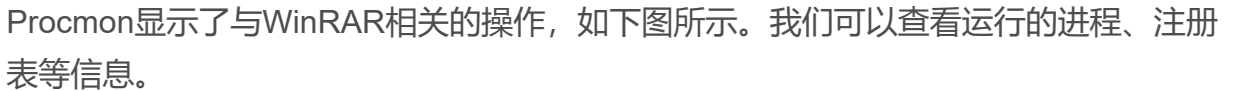


第二步，打开压缩包及某个文件。

未打开压缩包前运行结果如下图所示：



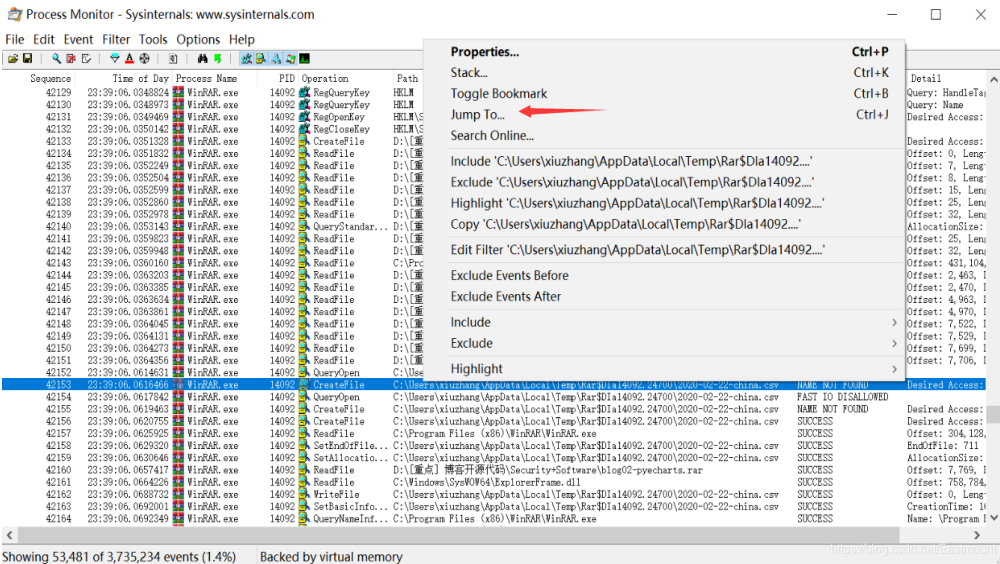
打开该压缩包中的“2020-02-22-china.csv”文件，这是作者Python大数据分析武汉疫情的
开源代码，也推荐感兴趣的读者阅读。



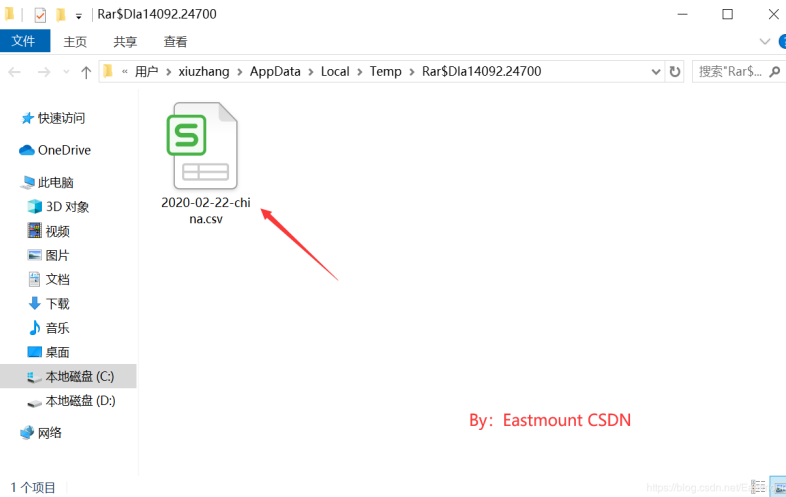
可以看到临时文件，其路径为：

C:\Users\xxxx\AppData\Local\Temp\Rar\$Dla14092.24700

第四步，右键点击“Jump To”跳转查看文件。

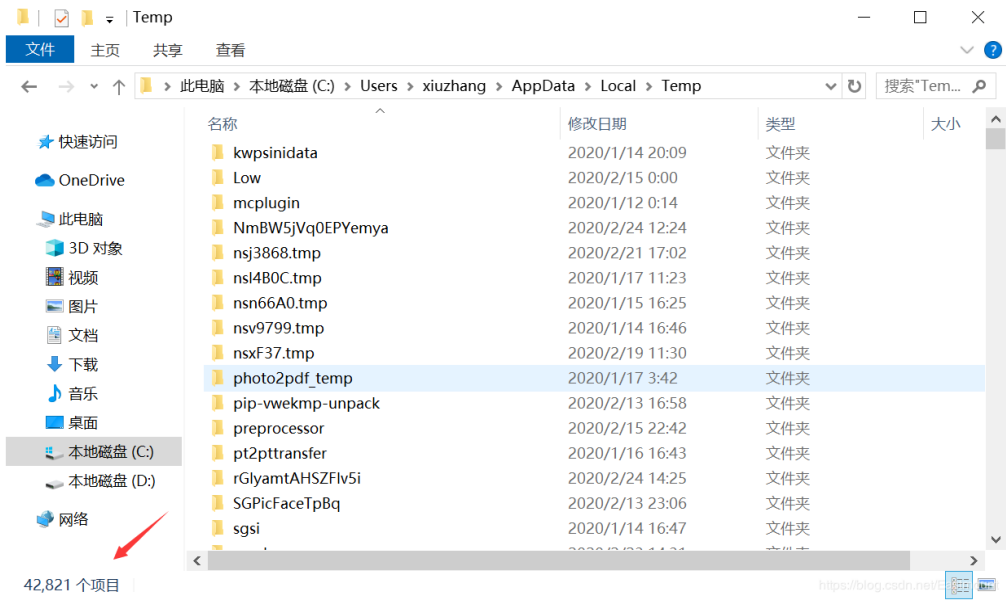


跟踪这个目录，在C盘对应目录下找到了这个文件，打开之后和本来打开的文件内容相同。



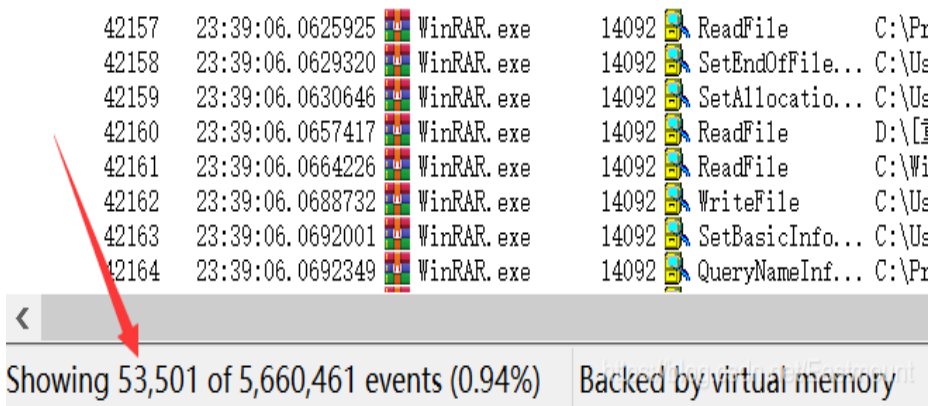
AppData\Local\Temp

它是电脑Windows系统临时存储的文件夹，会把浏览者浏览过的网站或者其它记录保存在这里。如果下次打开相应的地址，电脑会更快提取文件，甚至在没有网络时也能查看到。这是不安全的，你保密的文件文件也可能存在该位置，建议及时删除。

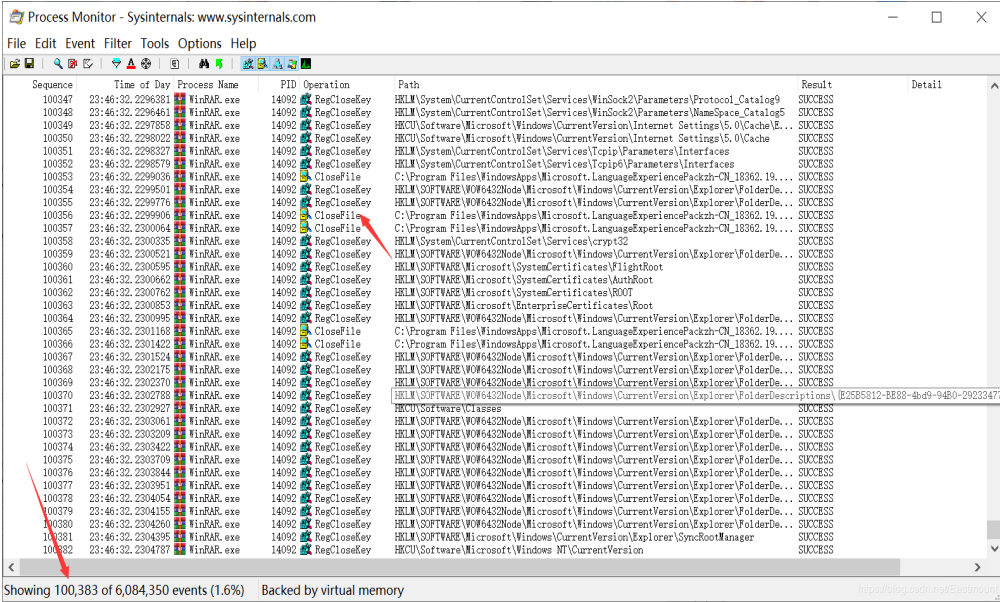


第五步，WinRAR压缩包内文件直接打开后，有两种关闭方式：先关闭打开的文件，再关闭打开的压缩包。另外一种方式是先关闭打开的压缩包，再关闭打开的文件。建议大家利用Process Monitor分析上述两种方式的不同点。

打开压缩包时加载的文件个数如下图所示。



先关闭word文件，再关闭winrar。注意，关闭word文件后，Process Monitor监测到了事件；再关闭winrar，Process Monitor也监测到了事件。



这仅是一篇基础性用法文章，更多实例作者希望深入学习后分享出来。比如监控某个目录下文件的创建、修改、删除、访问操作，从而保存日志为文件，以便日后分析。

Column	Relation	Value	Action	
<input checked="" type="checkbox"/>	Operation	is	WriteFile	Include
<input checked="" type="checkbox"/>	Operation	is	SetDispositionInformationFile	Include
<input checked="" type="checkbox"/>	Operation	is	SetRenameInformationFile	Include
<input checked="" type="checkbox"/>	Operation	is	SetEndOfFileInformationFile	Include
<input checked="" type="checkbox"/>	Operation	is	SetAllocationInformationFile	Include
<input checked="" type="checkbox"/>	Operation	is	ReadFile	Include
<input checked="" type="checkbox"/>	Path	contains	C:\eclipse	Include

- WriteFile：写操作，依照文件大小可能产生多条
- ReadFile：读操作，一次读会产生很多条
- SetAllocationInformationFile：改写文件时触发
- SetEndOfFileInformationFile：改写文件时触发
- SetRenameInformationFile：重命名时触发
- SetDispositionInformationFile：删除文件时触发

四.总结

写到这里，这篇文章就介绍完毕，主要包括三部分内容：

- Procmon软件介绍

- Procmon分析可执行文件
- Procmon分析压缩包文件加载项，包括进程和注册表

接下来，作者将采用该工具在虚拟机中分析恶意样本，涉及知识点包括：

- 文件活动行为分析：Procmon监控木马客户端的文件行为
- 注册表活动行为分析：Procmon监控木马客户端的注册表设置值行为
- 网络活动行为分析：Wireshark监控网络行为、TCP三次握手连接、被控端与控制端之间的通信过程

希望这系列文章对您有所帮助，真的感觉自己技术好菜，要学的知识好多。这是第49篇原创的安全系列文章，从网络安全到系统安全，从木马病毒到后门劫持，从恶意代码到溯源分析，从渗透工具到二进制工具，还有Python安全、顶会论文、黑客比赛和漏洞分享。未知攻焉知防，人生漫漫其路远兮，作为初学者，自己真是爬着前行，感谢很多人的帮助，继续爬着，继续加油！

欢迎大家讨论，是否觉得这系列文章帮助到您！如果存在不足之处，还请海涵。任何建议都可以评论告知读者，共勉~

武汉加油！湖北加油！中国加油！！！！

(By:Eastmount 2020-02-26 晚上12点写于贵阳 <http://blog.csdn.net/eastmount>)

参考文献：

- [1] 《软件安全》实验之恶意样本行为分析
- [2] <https://github.com/eastmountyxz/Security-Software-Based>
- [3] Process Monitor分析某个应用行为 - cui0x01
- [4] <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>
- [5] <https://wenku.baidu.com/view/aaf324150b4e767f5acfcec4.html>
- [6] Process Monitor中文手册 - D_R_L_T
- [7] ProcessMonitor文件以及注册表监视器的使用 - Amrecs
- [8] Process Monitor监控目录 - 监控文件被哪个进程操作了 - kendyjh9999