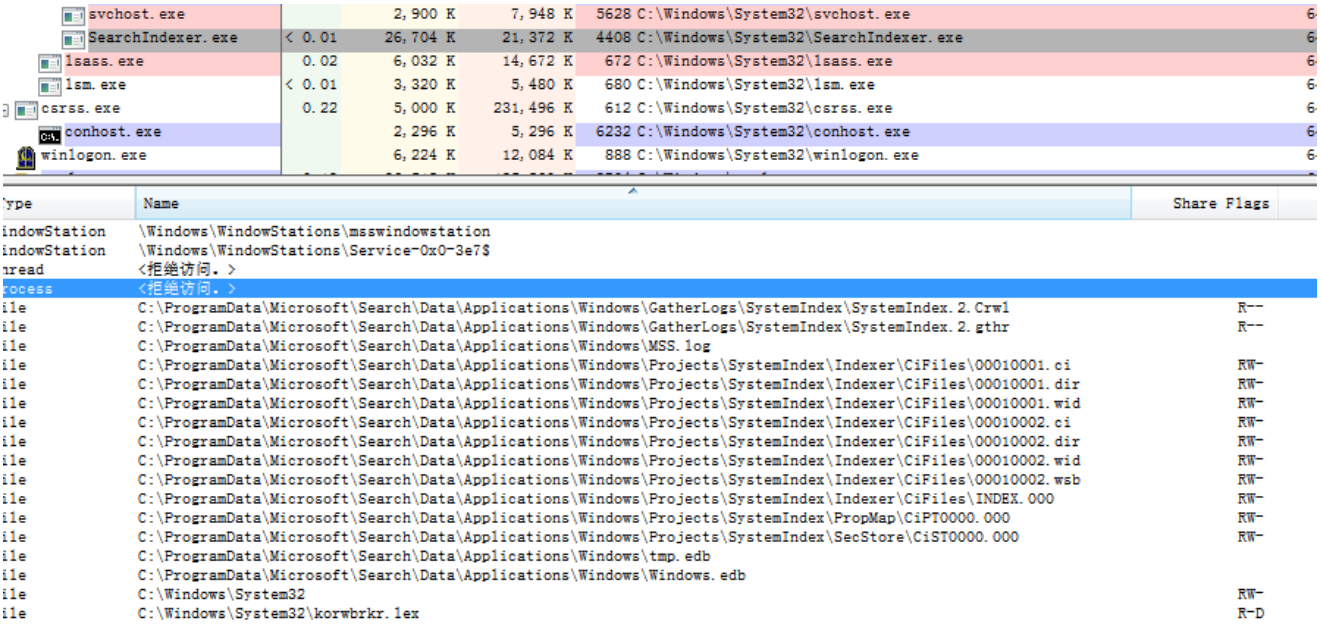
Windows任意文件下载的三个Tips -- zcgonvh

在群里面看到大家提出的两个思路，简单进行了一下测试，并附加一个新思路。

由于需要读取一些系统服务使用的文件或用户文件，一般来说需要 `SYSTEM` 或 `administrators` 权限。

WSearch服务

@Lz1y提出的思路，简单看了一下 `SearchIndexer` 的文件句柄，WSearch服务会将数据存放在 `%ProgramData%\Microsoft\Search\Data\Applications\Windows\Windows.edb` 中：



```
svchost.exe                  2,900 K     7,948 K   5628 C:\Windows\System32\svchost.exe
SearchIndexer.exe    < 0.01 26,704 K    21,372 K   4408 C:\Windows\System32\SearchIndexer.exe
lsass.exe             0.02   6,032 K    14,672 K    672 C:\Windows\System32\lsass.exe
lsm.exe              < 0.01  3,320 K     5,480 K    680 C:\Windows\System32\lsm.exe
csrss.exe             0.22   5,000 K   231,496 K    612 C:\Windows\System32\csrss.exe
conhost.exe                  2,296 K     5,296 K   6232 C:\Windows\System32\conhost.exe
winlogon.exe                 6,224 K    12,084 K    888 C:\Windows\System32\winlogon.exe
```

```
ype        Name                                                                                                  Share Flags
indowStation  \Windows\WindowStations\msswindowstation
indowStation  \Windows\WindowStations\Service-0x0-3e7$
ıread      <拒绝访问。>
rocess     <拒绝访问。>
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.2.Crwl                    R--
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex\SystemIndex.2.gthr                    R--
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.log
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010001.ci             RW-
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010001.dir            RW-
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010001.wid            RW-
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010002.ci             RW-
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010002.dir            RW-
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010002.wid            RW-
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\00010002.wsb            RW-
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\Indexer\CiFiles\INDEX.000               RW-
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\PropMap\CiPT0000.000                    RW-
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex\SecStore\CiST0000.000                   RW-
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\tmp.edb
ile        C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb
ile        C:\Windows\System32                                                                                               RW-
ile        C:\Windows\System32\korwbrkr.lex                                                                                  R-D
```

文件拓展名为edb，显然和 `ntds.dit` 相同，使用了EsentDB作为存储引擎。

~~所以只要下载回来还原即可~~ 那是不可能的，注意 `ShareFlag` 一栏，SearchIndexer选择以独占方式打开数据库，其他进程无法进行读取。

那么关注一下其他目录或文件， `%ProgramData%\Microsoft\Search\Data\Applications\Windows\GatherLogs\SystemIndex` 目录下存在一些 `Crwl` 与 `gthr` 文件，文件名类似 `SystemIndex.[数字序号].gthr` 。其中 `gthr` 文件中存在一些路径信息：

```
6a95c7f0  1d66041   4000001f  0 40d84   2 16  4294967295
6c1f2710  1d66041 file:C:/Users/   /Documents/WeChat Files/wxid_              /Attachment/4f01ae458b982331b437549d63a1756d_t.jpg  8000000
6c1f4e20  1d66041 file:C:/Users/   /Documents/WeChat Files/wxid_              /FavTemp/1b04d101/  8000000c  0 80041201    1 4294967295  2
6c2cbba0  1d66041 csc://{S-1-5-21-                                  3-1000}/  8000000c  2 80041201    2 16  3
6c2d57e0  1d66041 file:C:/Users/:  /Documents/Visual Studio 2017/Backup Files,                                    8000000c  0 800
6c2d7ef0  1d66041 file:C:/Users/:  /Documents/WeChat Files/wxid_2            ./Image/Image/2107078e03fae542d0dc42eca01c36c0.jpg 8000000c
9187b8a0  1d66041 file:C:/Users/:  /ntuser.dat.LOG1 8000000c  2 80070020    1 4294967295  117
9187dfb0  1d66041 file:C:/Users/:  /NTUSER.DAT  8000000c  2 80070020    1 4294967295  116
d91bb220  1d66041 file:C:/Users/:  /ntuser.dat.LOG1 8000000c  2 80070020    1 4294967295  117
d91bb220  1d66041 file:C:/Users/:  /NTUSER.DAT  8000000c  2 80070020    1 4294967295  116
df9c6e00  1d66041   40000020  0 40d84   2 16  4294967295
5bf0c770  1d66043 file:C:/Users/   /Documents/WeChat Files/mmTest_writable_weixin.txt 8000000c  0 80041201    1 4294967295  311
5ef1d270  1d66043 file:C:/Users/   /Documents/WeChat Files/wxid_2             /Msg/MicroMsg.db-journal  8000000c  0 80041201    1 4294967
5f0644d0  1d66043 file:C:/Users/   /Documents/WeChat Files/wxid_2             /Msg/ChatMsg.db-journal 8000000c  0 80041201    1 4294967295
```

如图，刚刚打开服务后，微信访问的图片、聊天数据库即被记录，甚至还有一个我的 `Sid` 。

另外一个文件里面有一些我的 `ie访问历史` ：

```
fbe92d01  1d22f30   4000001f  0 40d83   3 4 4294967295
69c15aad  1d22f31 iehistory://{S-1-5-21-                                -1000}/http://192.168.1.11/  8000000c  0 80004005    3 4 101
69c15aad  1d22f31 iehistory://{S-1-5-21-                                -1000}/http://192.168.1.11/  8000000c  0 80040d37    3 4 101
7559ad4e  1d22f31 iehistory://{S-1-5-21-                                -1000}/http://cn.bing.com/search?q=192.168.1.11&src=IE-SearchBox&
756f19ae  1d22f31 iehistory://{S-1-5-21-                                -1000}/http://192.168.1.11/Windows6.1-KB3138612-x64.msu  8000000c
7ce4286f  1d22f31   40000020  0 40d83   2 3 4294967295
7ce4286f  1d22f31   4000001f  0 40d84   2 5 4294967295
83cf2770  1d22f31 iehistory://{S-1-5-21-                               3-1000}/http://cn.bing.com/search?q=192.168.1.11&src=IE-SearchBox&
83cf2770  1d22f31 iehistory://{S-1-5-21-                               3-1000}/http://192.168.1.11/Windows6.1-KB3138612-x64.msu  8000000c
```

虚拟机中则记录了复制到桌面的mimikatz：

```
147f28c5  1d5e58d  file:C:/Users/User/Desktop/x64/mimidrv.sys
151aeb94  1d5e58d  file:C:/Users/User/Desktop/x64/mimikatz.exe
151d2bc7  1d5e58d  file:C:/Users/User/Desktop/x64/mimilib.dll8000000c
```

如果安装了 Outlook ，甚至会有 邮箱 、 附件名称 、 联系人 等信息。 (这里没有图，请自行检查)

之后再注意和windows.edb同目录的文件，其中 .jtx 是可以被打开的。查询msdn https://docs.microsoft.com/en-us/windows/win32/extensible-storage-engine/extensible-storage-engine-files 可知，此文件为数据库的 事务日志 ，文件名格式为 edb[从00000-fffff的五位十六进制数].jtx 。

研究过SqlServer的都应当想到，事务日志里面会保存未同步或未写入的数据，只要对文件内容进行分析即可。

实际上我们完全不需要去研究文件结构，windows下绝大部分情况下都以 UTF16-LE 编码进行保存，所以直接使用 strings 进行提取：

```
(u7b\
User\Desktop\windbg.exe -
_wc
.lnk
file:C:/Users/User/Desktop/windbg.exe -
_wc
.lnk
```

如果是一个常用机器，或者安装了outlook等，那么会有更多惊喜。

这种方式获取到的数据可能极为敏感，也可能完全没有， 效果取决于人品 ，而且需要进行文件名爆破。不过好在根据自己几个环境的统计，数据量很可观，而且需要爆破的序号并不大。

EventLog服务

@某个名字中有emoji的老哥（抱歉打不出来）提出的思路，之前做测试时候一致认为是独占式，今天仔细一看发现被打脸：

```
File            C:\Windows\System32\winevt\Logs\Application.evtx                                                                  R--
File            C:\Windows\System32\winevt\Logs\HardwareEvents.evtx                                                               R--
File            C:\Windows\System32\winevt\Logs\Internet Explorer.evtx                                                            R--
File            C:\Windows\System32\winevt\Logs\Key Management Service.evtx                                                       R--
File            C:\Windows\System32\winevt\Logs\Media Center.evtx                                                                 R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Problem-Steps-Recorder.evtx             R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx    R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Troubleshoote...  R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Inventory.evtx                  R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx                  R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Bits-Client%4Operational.evtx                                   R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Dhcp-Client%4Admin.evtx                                         R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Dhcpv6-Client%4Admin.evtx                                       R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4Operational.evtx                                 R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx                           R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripted%4Admin.evtx                                  R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-Scripted%4Operational.evtx                            R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%4Operational.evtx                       R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx                     R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Fault-Tolerant-Heap%4Operational.evtx                           R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-GroupPolicy%4Operational.evtx                                   R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-EventTracing%4Admin.evtx                                 R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Power%4Thermal-Operational.evtx                          R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx                               R--
File            C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4Errors.evtx                                        R--
```

日志文件存放于 %systemroot%\System32\winevt\Logs ，且允许共享读取 ~~真想打当时的我一顿~~

由于ETW文件名固定，我们直接根据已知列表进行下载即可：

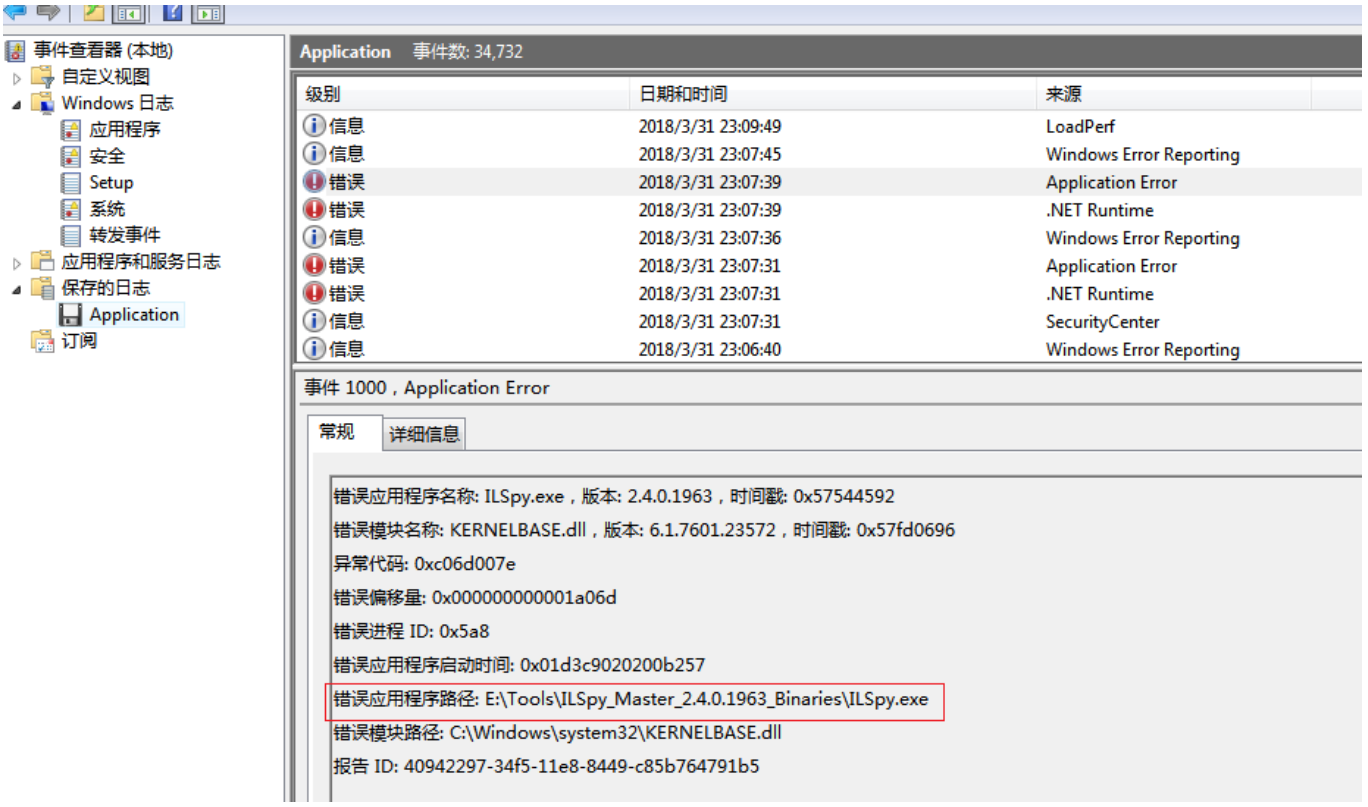
```
Application.evtx
ConnectionInfo.evtx
Error.evtx
HardwareEvents.evtx
Internet Explorer.evtx
Key Management Service.evtx
Media Center.evtx
Microsoft-Windows-API-Tracing%4Operational.evtx
Microsoft-Windows-AppID%4Operational.evtx
Microsoft-Windows-Application Server-Applications%4Admin.evtx
Microsoft-Windows-Application Server-Applications%4Operational.evtx
Microsoft-Windows-Application-Experience%4Problem-Steps-Recorder.evtx
Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx
Microsoft-Windows-Application-Experience%4Program-Compatibility-Troubleshooter.evtx
Microsoft-Windows-Application-Experience%4Program-Inventory.evtx
Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx
Microsoft-Windows-AppLocker%4EXE and DLL.evtx
Microsoft-Windows-AppLocker%4MSI and Script.evtx
Microsoft-Windows-Audio%4CaptureMonitor.evtx
Microsoft-Windows-Audio%4Operational.evtx
Microsoft-Windows-Authentication User Interface%4Operational.evtx
Microsoft-Windows-Backup.evtx
Microsoft-Windows-BitLocker-DrivePreparationTool%4Admin.evtx
Microsoft-Windows-BitLocker-DrivePreparationTool%4Operational.evtx
Microsoft-Windows-Bits-Client%4Operational.evtx
Microsoft-Windows-Bluetooth-MTPEnum%4Operational.evtx
Microsoft-Windows-BranchCache%4Operational.evtx
Microsoft-Windows-BranchCacheSMB%4Operational.evtx
Microsoft-Windows-CAPI2%4Operational.evtx
```

```
Microsoft-Windows-CodeIntegrity%4Operational.evtx
Microsoft-Windows-Compat-Appraiser%4Operational.evtx
Microsoft-Windows-CorruptedFileRecovery-Client%4Operational.evtx
Microsoft-Windows-CorruptedFileRecovery-Server%4Operational.evtx
Microsoft-Windows-DateTimeControlPanel%4Operational.evtx
Microsoft-Windows-DeviceSync%4Operational.evtx
Microsoft-Windows-Dhcp-Client%4Admin.evtx
Microsoft-Windows-DhcpNap%4Admin.evtx
Microsoft-Windows-Dhcpv6-Client%4Admin.evtx
Microsoft-Windows-Diagnosis-DPS%4Operational.evtx
Microsoft-Windows-Diagnosis-PCW%4Operational.evtx
Microsoft-Windows-Diagnosis-PLA%4Operational.evtx
Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx
Microsoft-Windows-Diagnosis-Scripted%4Admin.evtx
Microsoft-Windows-Diagnosis-Scripted%4Operational.evtx
Microsoft-Windows-Diagnosis-ScriptedDiagnosticsProvider%4Operational.evtx
Microsoft-Windows-Diagnostics-Networking%4Operational.evtx
Microsoft-Windows-Diagnostics-Performance%4Operational.evtx
Microsoft-Windows-DiskDiagnostic%4Operational.evtx
Microsoft-Windows-DiskDiagnosticDataCollector%4Operational.evtx
Microsoft-Windows-DiskDiagnosticResolver%4Operational.evtx
Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx
Microsoft-Windows-EapHost%4Operational.evtx
Microsoft-Windows-EventCollector%4Operational.evtx
Microsoft-Windows-Fault-Tolerant-Heap%4Operational.evtx
Microsoft-Windows-FMS%4Operational.evtx
Microsoft-Windows-Folder Redirection%4Operational.evtx
Microsoft-Windows-Forwarding%4Operational.evtx
Microsoft-Windows-GroupPolicy%4Operational.evtx
Microsoft-Windows-Help%4Operational.evtx
Microsoft-Windows-HomeGroup Control Panel%4Operational.evtx
Microsoft-Windows-HomeGroup Listener Service%4Operational.evtx
Microsoft-Windows-HomeGroup Provider Service%4Operational.evtx
Microsoft-Windows-IKE%4Operational.evtx
Microsoft-Windows-International%4Operational.evtx
Microsoft-Windows-International-RegionalOptionsControlPanel%4Operational.evtx
Microsoft-Windows-Iphlpsvc%4Operational.evtx
Microsoft-Windows-Kernel-EventTracing%4Admin.evtx
Microsoft-Windows-Kernel-Power%4Thermal-Operational.evtx
Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx
Microsoft-Windows-Kernel-WDI%4Operational.evtx
Microsoft-Windows-Kernel-WHEA%4Errors.evtx
Microsoft-Windows-Kernel-WHEA%4Operational.evtx
Microsoft-Windows-Known Folders API Service.evtx
Microsoft-Windows-LanguagePackSetup%4Operational.evtx
Microsoft-Windows-MCT%4Operational.evtx
Microsoft-Windows-MemoryDiagnostics-Results%4Debug.evtx
Microsoft-Windows-MUI%4Admin.evtx
Microsoft-Windows-MUI%4Operational.evtx
Microsoft-Windows-NCSI%4Operational.evtx
Microsoft-Windows-NetworkAccessProtection%4Operational.evtx
Microsoft-Windows-NetworkAccessProtection%4WHC.evtx
Microsoft-Windows-NetworkLocationWizard%4Operational.evtx
Microsoft-Windows-NetworkProfile%4Operational.evtx
Microsoft-Windows-NlaSvc%4Operational.evtx
Microsoft-Windows-NTLM%4Operational.evtx
Microsoft-Windows-OfflineFiles%4Operational.evtx
Microsoft-Windows-ParentalControls%4Operational.evtx
Microsoft-Windows-PeopleNearMe%4Operational.evtx
Microsoft-Windows-PowerShell%4Operational.evtx
Microsoft-Windows-PrintService%4Admin.evtx
Microsoft-Windows-ReadyBoost%4Operational.evtx
Microsoft-Windows-ReadyBoostDriver%4Operational.evtx
Microsoft-Windows-Recovery%4Operational.evtx
Microsoft-Windows-ReliabilityAnalysisComponent%4Operational.evtx
Microsoft-Windows-RemoteApp and Desktop Connections%4Admin.evtx
Microsoft-Windows-RemoteApp and Desktop Connections%4Operational.evtx
Microsoft-Windows-RemoteAssistance%4Admin.evtx
Microsoft-Windows-RemoteAssistance%4Operational.evtx
Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx
Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx
microsoft-windows-RemoteDesktopServices-RemoteDesktopSessionManager%4Admin.evtx
Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx
Microsoft-Windows-Resource-Exhaustion-Resolver%4Operational.evtx
Microsoft-Windows-Resource-Leak-Diagnostic%4Operational.evtx
Microsoft-Windows-RestartManager%4Operational.evtx
Microsoft-Windows-Security-Audit-Configuration-Client%4Operational.evtx
Microsoft-Windows-SMBServer%4Audit.evtx
Microsoft-Windows-SMBServer%4Operational.evtx
```

```
Microsoft-Windows-TerminalServices-ClientUSBDevices%4Admin.evtx
Microsoft-Windows-TerminalServices-ClientUSBDevices%4Operational.evtx
Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx
Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
Microsoft-Windows-TerminalServices-PnPDevices%4Admin.evtx
Microsoft-Windows-TerminalServices-PnPDevices%4Operational.evtx
Microsoft-Windows-TerminalServices-RDPClient%4Operational.evtx
Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx
Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
Microsoft-Windows-TerminalServices-ServerUSBDevices%4Admin.evtx
Microsoft-Windows-TerminalServices-ServerUSBDevices%4Operational.evtx
Microsoft-Windows-TZUtil%4Operational.evtx
Microsoft-Windows-UAC%4Operational.evtx
Microsoft-Windows-UAC-FileVirtualization%4Operational.evtx
Microsoft-Windows-User Profile Service%4Operational.evtx
Microsoft-Windows-VDRVROOT%4Operational.evtx
Microsoft-Windows-VHDMP%4Operational.evtx
Microsoft-Windows-WebDeploy%4ConnectionInfo.evtx
Microsoft-Windows-WebDeploy%4Error.evtx
Microsoft-Windows-WER-Diag%4Operational.evtx
Microsoft-Windows-WFP%4Operational.evtx
Microsoft-Windows-Windows Defender%4Operational.evtx
Microsoft-Windows-Windows Defender%4WHC.evtx
Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSecurity.evtx
Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
Microsoft-Windows-WindowsBackup%4ActionCenter.evtx
Microsoft-Windows-WindowsSystemAssessmentTool%4Operational.evtx
Microsoft-Windows-WindowsUpdateClient%4Operational.evtx
Microsoft-Windows-Winlogon%4Operational.evtx
Microsoft-Windows-WinRM%4Operational.evtx
Microsoft-Windows-Winsock-WS2HELP%4Operational.evtx
Microsoft-Windows-Wired-AutoConfig%4Operational.evtx
Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx
Microsoft-Windows-WPD-ClassInstaller%4Operational.evtx
Microsoft-Windows-WPD-CompositeClassDriver%4Operational.evtx
Microsoft-Windows-WPD-MTPClassDriver%4Operational.evtx
OAlerts.evtx
PreEmptive.evtx
Security.evtx
Setup.evtx
System.evtx
Windows PowerShell.evtx
```

（注意安装某些服务后可能会有更多日志，需要自行收集。）

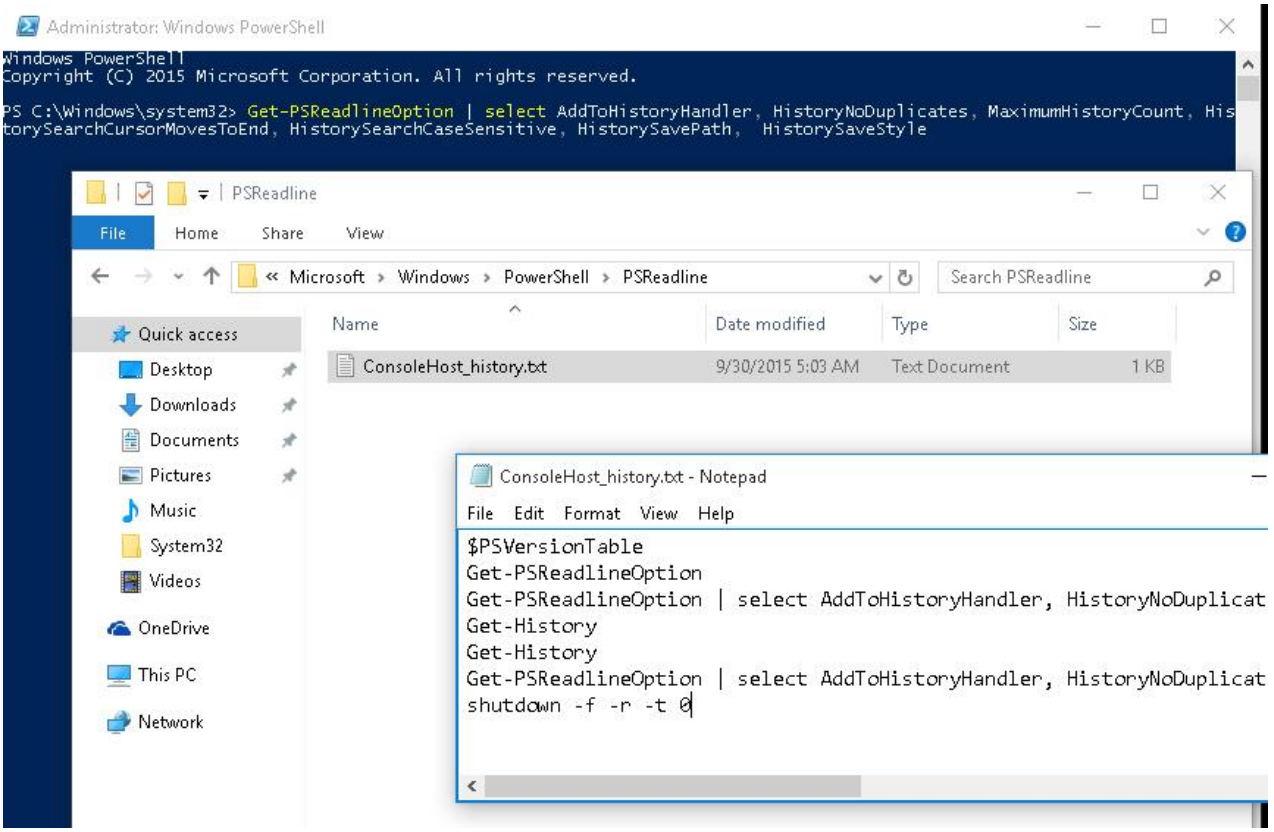
之后直接用事件查看器打开即可：



后续操作就各显神通了，例如 Application 里面的错误信息包含异常退出程序的 全路径 ； Powershell 日志包含执行的命令行； Security 日志包含 登陆信息 ； System 日志可能包含某些杀软的信息等等。

PowerShell命令历史记录

类似 .bash_history ， 高版本Powershell 会将历史记录保存
在 %userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt 中，里面可能包含一些敏感信息：



(图来自google)

美中不足的是需要爆破用户名，所以需要结合某些手段获取一些用户名--例如ETW日志中的登录信息，或是WSearch服务数据库中的信息等等。

小结

成年人了，放个论文式结尾总结没有意义，谈一谈过程中的体会。

技术是有连贯性的，不仅仅局限在某个操作系统领域，某些看似毫不相关的领域可能会碰撞出奇妙的交集。

例如WSearch服务获取信息的思路实际上就是 文件取证 ；ETW思路的后续则更类似安服 应急溯源 ，可能有不少自动化工具可用；PowerShell历史记录则可以和 linux信息 搜集形成类比。这些知识点综合起来，会让人有种莫名的爽快感。

再次回到本文主题，或许可以顺着这种思路问一下取证的朋友与安服的朋友，看看有没有什么其他可行的方案。找到领域咨询专业人员实际上是比自己研究靠谱得多的，虽然最终结果还是做渗透的事。