

设为首页 收藏本站



论坛

排行榜

最新发表

最新回复

最新热门

捐助榜

升级权限

快速导航

用户名

☐ 自动登录

找回密码

密码

登录

注册

请输入搜索内容

搜索

论坛 :: 启动制作 :: 综合讨论区 对Catroot下签名文件精简的思路和尝试

发帖

返回列表

查看: 8899 | 回复: 27

Windows_Air

[原创] 对Catroot下签名文件精简的思路和尝试 [复制链接]

发表于 2019-2-4 12:06:03 | 只看该作者 | 只看大图

1# 电梯直达

本帖最后由 Windows_Air 于 2019-2-4 16:17 编辑

一、引言

对于PE(Portable Executable)文件，如果要校验其完整性或有效性，很容易地想到使用数字签名的办法。

常规 兼容性 数字签名 文件校验 安全 详细信息 以前的版本

签名列表

签名者姓名:	摘要算法	时间戳
Oracle Corpo...	sha1	2018年8月14日 19...
Oracle Corpo...	sha256	2018年8月14日 19...

详细信息(D)

不过，数字签名也有一定的缺陷。还有其他的办法吗？既能快速判断文件的完整性，又能兼容各种文件格式，并且提高安全性？使用安全编录文件是一个不错的代替方案，安全编录数据库存储和文件的哈希值，可以通过比对文件哈希与数据库中的条目，来判断文件的完整性。

一般地，系统中的安全编录文件储存于**Windows\System32\Catroot** 下，根据不同的GUID分别存储在不同的文件夹中。

> 此电脑 > 本地磁盘 (C:) > Windows > System32 > CatRoot

名称	修改日期	类型
{127D0A1D-4EF2-11D1-8608-00C04F...	2016/7/16 19:47	文件夹
{F750E6C3-38EE-11D1-85E5-00C04FC...	2019/1/28 10:00	文件夹
{FC451C16-AC75-11D1-B4B8-00C04F...	2019/2/1 17:00	文件夹

常见的GUID有以下几种:(具体请见[WinVerifyTrustEx](#))

01. {F750E6C3-38EE-11D1-85E5-00C04FC295EE} DRIVER_ACTION_VERIFY 驱动级别验证，最为常见的验证方式

02. {127D0A1D-4EF2-11D1-8608-00C04FC295EE} NULL 未指定信任提供程序时的默认值

复制代码

这里，我们主要讨论**{F750E6C3-38EE-11D1-85E5-00C04FC295EE}**(在一些环境中，有可能也是唯一选项)。进入到相应的路径中，可以看到这里标识了系统一些组件的签名文件：

Microsoft-Windows-Common-Drivers-minkernel-Package~31bf3856ad364e35~amd64~zh-CN~10.0....

Microsoft-Windows-Common-Drivers-net-Package~31bf3856ad364e35~amd64~~10.0.14393.0.cat

Microsoft-Windows-Common-Drivers-net-Package~31bf3856ad364e35~amd64~en-US~10.0.14393....

Microsoft-Windows-Common-Drivers-net-Package~31bf3856ad364e35~amd64~zh-CN~10.0.14393....

Microsoft-Windows-Common-Drivers-oncore-Package~31bf3856ad364e35~amd64~~10.0.14393.0....

Microsoft-Windows-Common-Drivers-oncore-Package~31bf3856ad364e35~amd64~en-US~10.0.14....

同样也包含一些Windows Update更新后遗留下的一些文件：

wuyou.net/forum.php?mod=viewthread&tid=413020

1/12

- Package_3181_for_KB4480961~31bf3856ad364e35~amd64~~10.0.1.3.cat
- Package_3182_for_KB4480961~31bf3856ad364e35~amd64~~10.0.1.3.cat
- Package_3183_for_KB4480961~31bf3856ad364e35~amd64~~10.0.1.3.cat
- Package_3184_for_KB4480961~31bf3856ad364e35~amd64~~10.0.1.3.cat
- Package_3185_for_KB4480961~31bf3856ad364e35~amd64~~10.0.1.3.cat

打开任意一个文件:
签名文件需要数字签名才能被系统接受:

安全目录

常规

安全目录

安全目录信息

该安全目录有效。

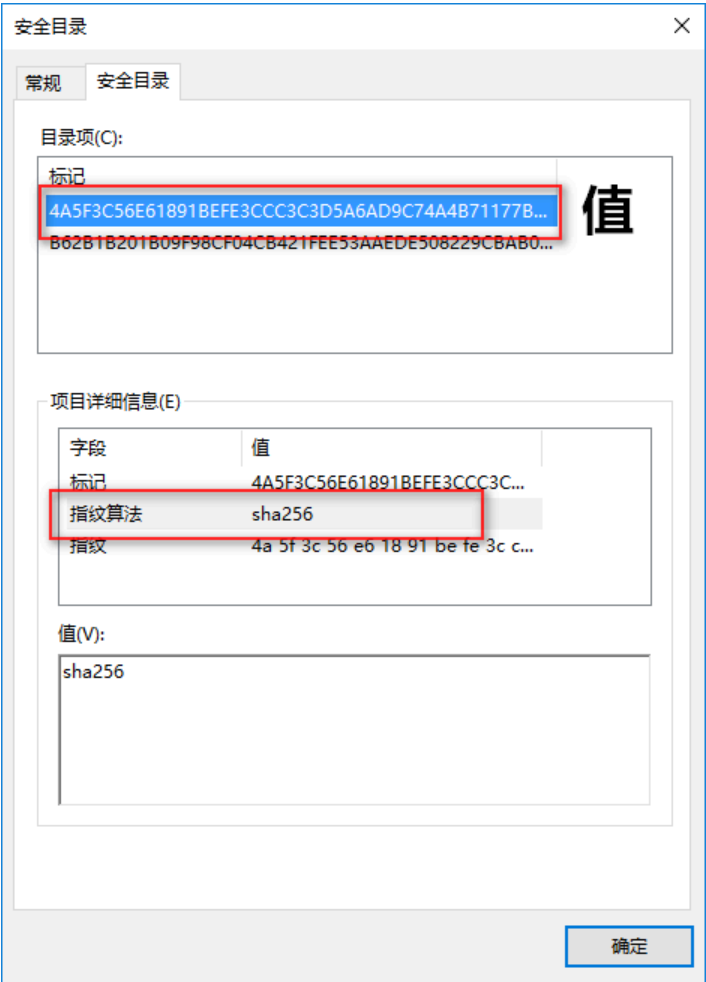
字段	值
版本	V1
使用者使用	1.3.6.1.4.1.311.12.1.1
列出标识符	8d 33 f0 60 3c bb 22 42 8a e8 ...
生效日期	2016年7月17日 3:11:43
使用者算法	1.3.6.1.4.1.311.12.1.3
1.3.6.1.4.1.311.1...	30 6b 1e 0c 00 4f 00 53 00 41 ...
指纹算法	sha1
指纹	97 d0 c3 a2 85 24 c2 1e 0e af ...

值(A):

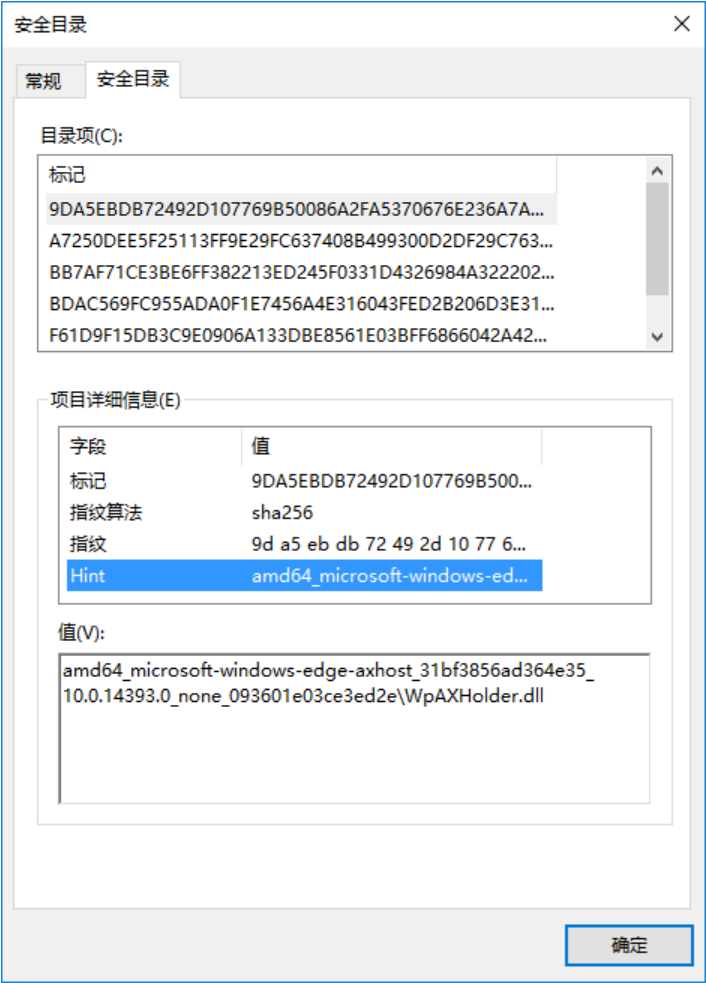
查看签名(V)

确定

查看目录项，可以看到存储的哈希值，在多数情况下，系统采用SHA256算法记录文件的哈希:



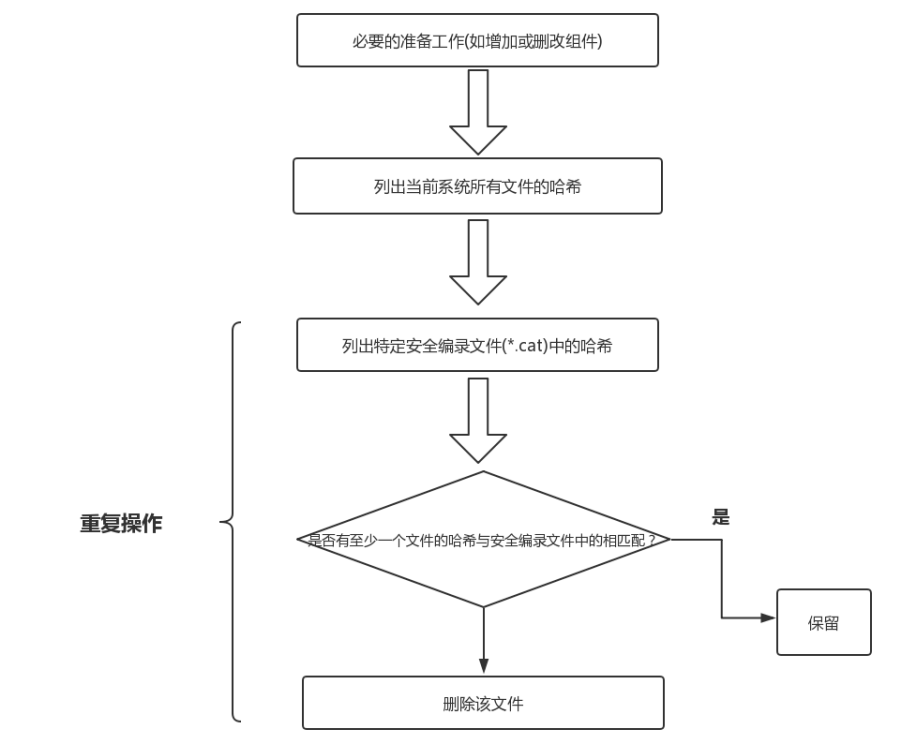
在大多数情况下，不能直观地判断特定Hash对应的文件。而在有些时候，你可以在详细信息中看到一个名为Hint的条目，记录对应的文件信息。



二、思路

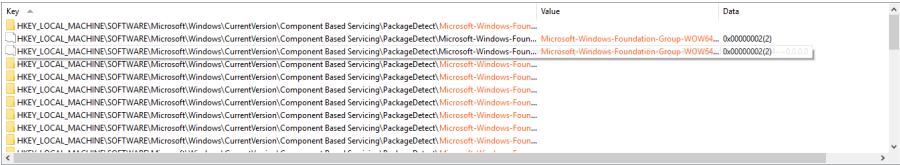
在Windows Update进行更新时，会在安全编录数据库中添加新的条目，以保证更新文件的完整性。在系统启动的过程中，同样会检验一些关键组件的校验信息。删除一些条目可能有利于加快启动时系统的加载进程，然而，随意删除更可能直接导致系统无法启动。

在实际的操作过程中，你可能想要删除掉一些“多余”的条目用以制作精简系统，那么具体应该如何操作才能保证能成功启动？可以尝试通过下面的方法进行精简：



在精简完文件后，你需要在 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing** 中删除相应的注册表项目，否则将导致启动过程中蓝屏。

举个例子，如果删除了 **Microsoft-Windows-Foundation-Group-WOW64-mincore-Package~31bf3856ad364e35~amd64~en-US~10.0.14393.0.cat** 文件，那么在该项中查找包含 "Microsoft-Windows-Foundation-Group-WOW64-mincore-Package" 的条目并删除之(可能需要留意语言区别)。



如果精简完后出现问题，检查下面项目：

01. *Client-Drivers-Package*

02. *Client-Drivers-drivers-Package*

03. *Client-Wired-Network-Drivers-Package*

04. *Common-Drivers-Package*

05. *DriverClasses-Package*

06. *SnippingTool-Package*

07. Adobe-Flash*

08. *Basic-Http*

09. Microsoft-Windows-Foundation-Package*

10. *CameraCaptureUI*

11.

复制代码

能不能进一步改进？如果不同的安全编录文件中包含相同的条目，能否保留其中一个？有些非pe的文件类型是否也存储在数据库中？有待进一步发掘。

三、尝试

试着写了个能列出可删除文件列表的小工具，精简后尚未发现问题。仍在继续测试中。

```
C:\Users\ChongKi\source\repos\catfile\x64\Release\catfile.exe

Enter the wim mount directory path
(example : D:\mount) : E:\test

Enter signature file(.cat) path
(example :K:\test\Windows\System32\Catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE} ) : C:\work\boot\windows\system32\catr
oot\{f750e6c3-38ee-11d1-85e5-00c04fc295ee}

Do you want to use the system default signature file database ?
(Default : no) (yes/no): n

Total : 897 files in mount path.
Total : 393 files in catroot path.
Add catalog file to system database...
[=====]100%


Searching in system database...
[=====]100%

Searching in current signature file...
[=====]100%

Done.

Now, a list of possible deletable files has been saved in the CatResult.txt file.
You can delete the {FC451C16-AC75-11D1-B4B8-00C04FB66EA0} folder under the Catroot folder to free up disk space.
请按任意键继续...
```

感兴趣的可以尝试下:

 [catfile.exe](#) (107.5 KB, 下载次数: 121)

○ 评分

参与人数	6	无忧币	+30	理由	收起
	Anson4	+ 5		赞一个!	
	xman00	+ 5		很给力!	
	chshrm	+ 5		论坛需要你这样的人才!	
	d9o	+ 5		很给力!	
	freesoft00	+ 5			
	sx3k	+ 5		很给力!	

查看全部评分

★ 收藏 12 👍 支持 ➡ 反对

回复 使用道具 举报

qitiandashe1020

 发表于 2019-2-4 12:29:38 | 只看该作者 2#

好高深啊。。。抢个沙发先

回复 使用道具 举报

红毛樱木

 发表于 2019-2-4 12:52:37 来自手机 | 只看该作者 3#

cat文件存储的文件信息也能读，厉害

bdfcy	<div>回复<div>使用道具</div><div>举报</div></div>
	<div><div>发表于 2019-2-4 17:47:03 只看该作者</div><div>4#</div><div>还不懂，先收藏一个，以后再学习</div></div>
sx3k	<div>回复<div>使用道具</div><div>举报</div></div>
	<div><div>发表于 2019-2-4 18:06:00 只看该作者</div><div>5#</div><div><div>本帖最后由 sx3k 于 2019-2-4 18:41 编辑</div><div>我正好需要，谢谢分享。 我用 catfile.exe精简slore的Wimbuilder2生成的PE下的Catroot下的文件。 Wimbuilder2-基于hta/vbs/js/bat的图形界面新的PE生成器 http://bbs.wuyou.net/forum.php?m ... &fromuid=678854 (出处: 无忧启动论坛) Re:WIN10XPE - 从零开始构建的PE+Admin双登录+MTP支持首发+19H1支持 http://bbs.wuyou.net/forum.php?m ... &fromuid=678854 (出处: 无忧启动论坛)</div><div><div>Windows 10 x64-2019-02-04-18-36-09.png (37.36 KB, 下载次数: 134)</div><div></div></div><div><div>点评</div><div><div>Windows_Air 效果如何？ 详情 回复 发表于 2019-2-6 11:00</div><div><div>slore 其实Re:WIN10XPE 自帶了精简Catroot列表。 D:\dev\wimbuilder2\Projects\WIN10XPE\00-Configures\Build\Catalog.bat 删除蓝色的部分就行了。不过为了保持兼容性，所以RS5暂时所有的文件都加了。不知道si 详情 回复 发表于 2019-2-4 23:07</div></div></div></div></div></div>
wangziqiang	<div>回复<div>使用道具</div><div>举报</div></div>
	<div><div>发表于 2019-2-4 20:49:13 只看该作者</div><div>6#</div><div>新年快乐 感谢分享</div></div>
slore	<div>回复<div>使用道具</div><div>举报</div></div>
	<div><div>发表于 2019-2-4 23:07:55 只看该作者</div><div>7#</div></div>

本帖最后由 slore 于 2019-2-4 23:15 编辑

[sx3k](#) 发表于 2019-2-4 18:06

我正好需要，谢谢分享。

我用 catfile.exe精简slore的Wimbuilder2生成的PE下的Catroot下的文件。

Wimbuil ...

其实Re:WIN10XPE 自带了精简Catroot列表。

D:\dev\wimbuilder2\Projects\WIN10XPE\00-Configures\Build\Catalog.bat

@echo off

if not "%opt[build.catalog]%"=="xfull" goto :CATALOG_ADDFILES

call AddFiles %0 :end_full_files

goto :end_full_files

:[Catalog_AddFiles_Info]**; Full Catalogs: \Windows\System32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}****; Use signtool.exe to find Catalogs ex: Signtool verify /kp /v /a****X:\Windows\System32\drivers*.sys > B:\SignDrivers.txt**

\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}

:end_full_files

goto :EOF

:CATALOG_ADDFILES

call AddFiles %0 :end_files

goto :end_files

@\Windows\System32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\

+ver >= 17763**; typo? this line make all catalog ?****\Windows\System32\catroot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}**

;skip

+ver = 0

Microsoft-Windows-Client-Desktop-Required-Package*.cat

Microsoft-Windows-Client-Desktop-Required-WOW64-Package*.cat

Microsoft-Windows-Client-Features-Package*.cat

...

; For updates**Package_***

:end_files

删除蓝色的部分就行了。不过为了保持兼容性，所以RS5暂时所有的文件都加了。

不知道signtool.exe的结果和楼主的catfile.exe有什么区别。

 点评**Windows_Air** 试了下，catfile还能节省1000...不清楚是不是姿势不对 [详情](#) [回复](#) 发表于 2019-2-6 11:45**Windows_Air** 不太清楚。。。估计又造轮子了 [详情](#) [回复](#) 发表于 2019-2-6 11:14[回复](#)[使用道具](#)[举报](#)

Windows_Air

楼主 | 发表于 2019-2-6 11:00:11 | 只看该作者

8#

sx3k 发表于 2019-2-4 18:06
我正好需要，谢谢分享。
我用 catfile.exe精简slore的Wimbuilder2生成的PE下的Catroot下的文件。
Wimbuil ...

效果如何？

点评

sx3k

slore的方法解决了我的问题，楼主你的工具如我的图片所示的内容是什么问题。 详情 回复 发表于 2019-2-6 11:52

回复

使用道具

举报

Windows_Air

楼主 | 发表于 2019-2-6 11:14:49 | 只看该作者

9#

slore 发表于 2019-2-4 23:07
其实Re:WIN10XPE 自带了精简Catroot列表。

D:\dev\wimbuilder2\Projects\WIN10XPE\00-Configures\Bu ...

不太清楚。。。估计又造轮子了

回复

使用道具

举报

Windows_Air

楼主 | 发表于 2019-2-6 11:45:06 | 只看该作者

10#

slore 发表于 2019-2-4 23:07
其实Re:WIN10XPE 自带了精简Catroot列表。

D:\dev\wimbuilder2\Projects\WIN10XPE\00-Configures\Bu ...

试了下，catfile还能节省1000...不清楚是不是姿势不对

回复

使用道具

举报

sx3k

发表于 2019-2-6 11:52:52 | 只看该作者

11#

Windows_Air 发表于 2019-2-6 11:00
效果如何？

slore的方法解决了我的问题，楼主你的工具如我的图片所示的内容是什么问题？

点评

Windows_Air

能把CBS.log删除后再重新运行看看文件里面有什么错误吗 详情 回复 发表于 2019-2-6 17:41

回复


使用道具

举报

Windows_Air

楼主 | 发表于 2019-2-6 17:41:17 来自手机 | 只看该作者

12#

xman00	sx3k 发表于 2019-2-6 11:52 slore的方法解决了我的问题，楼主你的工具如我的图片所示的内容是什么问题？	
	能把CBS.log删除后再重新运行看看文件里面有什么错误吗	
Windows_Air	<div>回复</div> <div>使用道具 举报</div>	
	<div> 发表于 2019-2-9 15:44:23 来自手机 只看该作者</div> <div>13#</div>	
xman00	想删除更多，前期的设想是干掉所有KB相关的(更新有关的)，结果失败。再通过错误日志补充，仍然不行。暂时没有安全精简的策略。希望得到更多指导。	
	<div>点评</div>	
Windows_Air	<div> Windows_Air 失败？具体指？ 详情 回复 发表于 2019-2-10 16:49</div> <div>回复</div> <div>使用道具 举报</div>	
	<div> 楼主 发表于 2019-2-10 16:49:11 只看该作者</div> <div>14#</div>	
xman00	<div>xman00 发表于 2019-2-9 15:44</div> <div>想删除更多，前期的设想是干掉所有KB相关的(更新有关的)，结果失败。再通过错误日志补充，仍然不行。暂时没 ...</div>	
	失败？具体指？	
Windows_Air	<div>回复</div> <div>使用道具 举报</div>	
	<div> 发表于 2019-2-10 18:36:56 来自手机 只看该作者</div> <div>15#</div>	
xman00	开机蓝屏	
	<div>点评</div>	
Windows_Air	<div> Windows_Air 有可能是注册表没删干净 详情 回复 发表于 2019-2-15 10:41</div> <div>回复</div> <div>使用道具 举报</div>	
	<div> 楼主 发表于 2019-2-15 10:41:41 只看该作者</div> <div>16#</div>	
xman00	<div>xman00 发表于 2019-2-10 18:36</div> <div>开机蓝屏</div>	
	有可能是注册表没删干净	
xman00	<div>点评</div>	
	<div> xman00 已确定和注册表无关，注册表清理得相当干净的。 详情 回复 发表于 2019-2-18 09:39</div> <div>回复</div> <div>使用道具 举报</div>	

10/12

Windows_Air	<div><div><div><div><div><div></div></div></div><div><div><div>楼主</div><div>发表于 2019-3-2 12:33:29</div><div>只看该作者</div></div></div></div></div><div>23#</div></div>
	<div><div><div><div><div><div></div></div></div><div><div><div>xman00 发表于 2019-2-18 09:40</div><div>因为我只关心*KB*相关的cat文件，经过各种尝试，结论就是这部分动不动~有危害或隐患的</div></div></div></div></div><div><div>那就比较神奇了，至少还是能处理掉不少的</div></div></div>
	<div><div><div>回复</div><div>使用道具</div><div>举报</div></div></div>
chshrm	<div><div><div><div><div><div></div></div></div><div><div><div>发表于 2019-3-18 20:10:47</div><div>只看该作者</div></div></div></div></div><div>24#</div></div>
	<div><div><div><div><div><div></div></div></div><div>如图所示，没找到那个划线部分的文件夹。只得到了一个可以精简的文件列表</div></div></div></div>
	<div><div><div><div><div><div></div></div></div><div><div><div>点评</div></div></div></div></div></div>
	<div><div><div><div><div><div></div><div>Windows_Air</div></div></div><div><div>不太清楚，原本是想静默删除的。。。 详情 回复 发表于 2019-4-21 00:11</div></div></div></div></div>
	<div><div><div>回复</div><div>使用道具</div><div>举报</div></div></div>
Anson4	<div><div><div><div><div><div></div></div></div><div><div><div>发表于 2019-3-19 14:36:43</div><div>只看该作者</div></div></div></div></div><div>25#</div></div>
	<div><div><div>感谢分享!</div></div></div>
	<div><div><div>回复</div><div>使用道具</div><div>举报</div></div></div>
Windows_Air	<div><div><div><div><div><div></div></div></div><div><div><div>楼主</div><div>发表于 2019-4-21 00:11:02</div><div>只看该作者</div></div></div></div></div><div>26#</div></div>
	<div><div><div><div><div><div></div></div></div><div><div><div>chshrm 发表于 2019-3-18 20:10</div><div>如图所示，没找到那个划线部分的文件夹。只得到了一个可以精简的文件列表</div></div></div></div></div><div><div>不太清楚，原本是想静默删除的。。。 </div></div></div>
	<div><div><div>回复</div><div>使用道具</div><div>举报</div></div></div>
weisusu	<div><div><div><div><div><div></div></div></div><div><div><div>发表于 2020-9-1 03:24:53 来自手机</div><div>只看该作者</div></div></div></div></div><div>27#</div></div>
	<div><div><div>800700c1然后一直卡1%，提示press any key to exit，请问啥原因?</div></div></div>

28[#][返回列表](#)

12/12