

# 如何收集ProcMon日志以排除启动时的AMP问题

## 目录

[简介](#)

[步骤:](#)

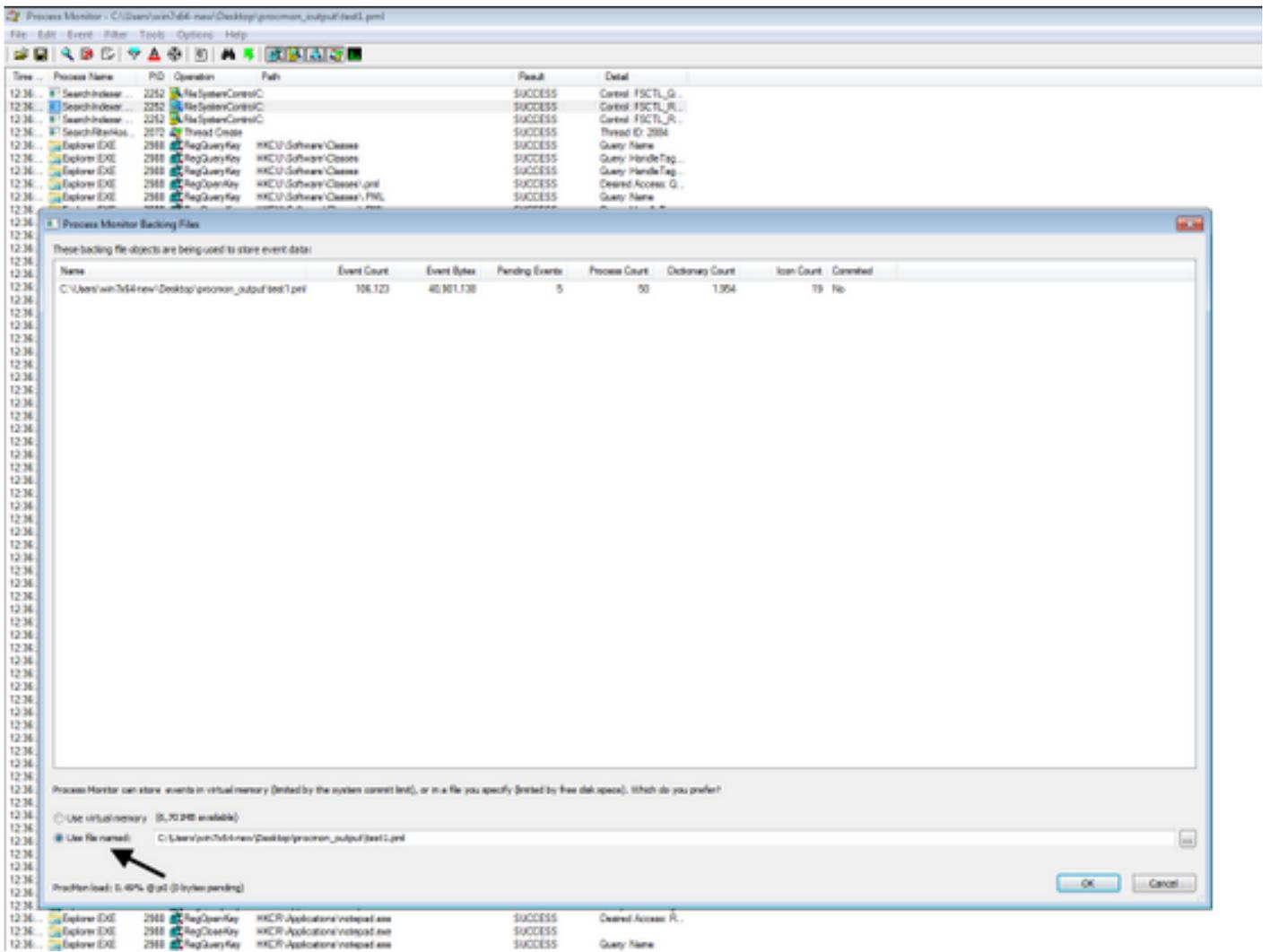
## 简介

作为系统管理员，您可能希望使用进程监控器(procmon.exe)获取详细日志，以确定FireAMP连接器在计算机启动过程中是否出现挂起。思科TAC也会请求这些日志来排除此类问题。进程监控器是一个免费的实用程序，可帮助我们进行此操作。可以从<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>免费下载

本文档介绍在系统引导过程中出现问题时如何收集ProcMon日志和内存转储（这意味着它在引导时生成BSOD）的步骤。需要这些日志来捕获引导期间发生的系统事件。

## 步骤:

- 1.以这种方式设置测试机，使问题易于重现。
- 2.以管理员身份下载并运行ProcMon工具。转至“文件” —>“进程监控器备份文件”并选择路径。



3.在Procmon工具中，转到“选项” —>“启用引导日志记录”。

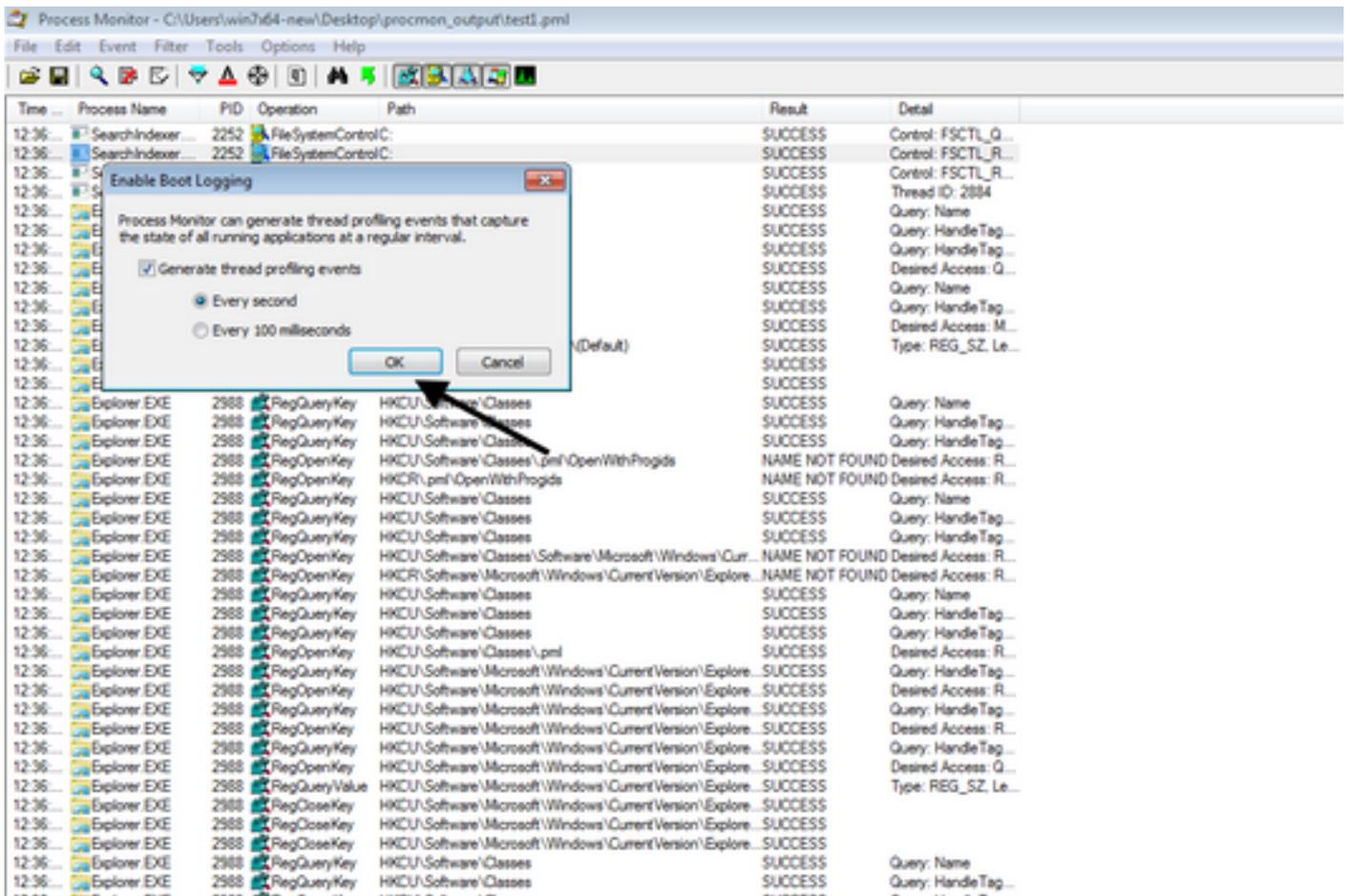
Process Monitor - C:\Users\win764-new\Desktop\procomon\_output\test1.pml

File Edit Event Filter Tools Options Help

Always on Top  
 Font...  
 Highlight Colors...  
 Configure Symbols...  
 Select Columns...  
 History Depth...  
 Profiling Events...  
 Enable Boot Logging  
 Show Resolved Network Addresses Ctrl+N  
 Hex File Offsets and Lengths  
 Hex Process and Thread IDs

Time	Process Name	PID	Operation	Path	Result	Detail
12:36...	SearchIndexer	2252	Control-FSCTL_G...		SUCCESS	Control-FSCTL_G...
12:36...	SearchIndexer	2252	Control-FSCTL_R...		SUCCESS	Control-FSCTL_R...
12:36...	SearchIndexer	2252	Control-FSCTL_R...		SUCCESS	Control-FSCTL_R...
12:36...	SearchFilterHost	2072	Thread ID: 2894		SUCCESS	Thread ID: 2894
12:36...	Explorer EXE	2988	Query Name		SUCCESS	Query Name
12:36...	Explorer EXE	2988	Query HandleTag...		SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Query HandleTag...		SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Desired Access: G...		SUCCESS	Desired Access: G...
12:36...	Explorer EXE	2988	Query Name		SUCCESS	Query Name
12:36...	Explorer EXE	2988	Query HandleTag...		SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Desired Access: N...		SUCCESS	Desired Access: N...
12:36...	Explorer EXE	2988	Type: REG_SZ, Le...		SUCCESS	Type: REG_SZ, Le...
12:36...	Explorer EXE	2988	Query Name		SUCCESS	Query Name
12:36...	Explorer EXE	2988	Query HandleTag...		SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Query HandleTag...		SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	NAME NOT FOUND	HKCU\Software\Classes\pnf\OpenWithProgid	NAME NOT FOUND	Desired Access: R...
12:36...	Explorer EXE	2988	NAME NOT FOUND	HKCR\pnf\OpenWithProgid	NAME NOT FOUND	Desired Access: R...
12:36...	Explorer EXE	2988	Query Name	HKCU\Software\Classes	SUCCESS	Query Name
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Classes	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Classes	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	NAME NOT FOUND	HKCU\Software\Classes\Software\Microsoft\Windows\Cur...	NAME NOT FOUND	Desired Access: R...
12:36...	Explorer EXE	2988	NAME NOT FOUND	HKCU\Software\Microsoft\Windows\CurrentVersion\Explo...	NAME NOT FOUND	Desired Access: R...
12:36...	Explorer EXE	2988	Query Name	HKCU\Software\Classes	SUCCESS	Query Name
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Classes	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Classes	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Desired Access: R...	HKCU\Software\Microsoft\Windows\CurrentVersion\Explo...	SUCCESS	Desired Access: R...
12:36...	Explorer EXE	2988	Query Name	HKCU\Software\Classes	SUCCESS	Query Name
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Classes	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Desired Access: R...	HKCU\Software\Classes\pnf	SUCCESS	Desired Access: R...
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Microsoft\Windows\CurrentVersion\Explo...	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Desired Access: R...	HKCU\Software\Microsoft\Windows\CurrentVersion\Explo...	SUCCESS	Desired Access: R...
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Microsoft\Windows\CurrentVersion\Explo...	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Desired Access: R...	HKCU\Software\Microsoft\Windows\CurrentVersion\Explo...	SUCCESS	Desired Access: R...
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Microsoft\Windows\CurrentVersion\Explo...	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Desired Access: G...	HKCU\Software\Microsoft\Windows\CurrentVersion\Explo...	SUCCESS	Desired Access: G...
12:36...	Explorer EXE	2988	Type: REG_SZ, Le...	HKCU\Software\Microsoft\Windows\CurrentVersion\Explo...	SUCCESS	Type: REG_SZ, Le...
12:36...	Explorer EXE	2988	Query Name	HKCU\Software\Classes	SUCCESS	Query Name
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Classes	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Classes	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	NAME NOT FOUND	HKCU\Software\Classes\Applications\notepad.exe	NAME NOT FOUND	Desired Access: R...
12:36...	Explorer EXE	2988	Desired Access: R...	HKCR\Applications\notepad.exe	SUCCESS	Desired Access: R...
12:36...	Explorer EXE	2988	Query Name	HKCR\Applications\notepad.exe	SUCCESS	Query Name
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Classes	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	Query HandleTag...	HKCU\Software\Classes	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	NAME NOT FOUND	HKCU\Software\Classes\Applications\notepad.exe	NAME NOT FOUND	Desired Access: R...
12:36...	Explorer EXE	2988	Desired Access: R...	HKCR\Applications\notepad.exe	SUCCESS	Desired Access: R...
12:36...	Explorer EXE	2988	Query Name	HKCR\Applications\notepad.exe	SUCCESS	Query Name
12:36...	Explorer EXE	2988	Query HandleTag...	HKCR\Applications\notepad.exe	SUCCESS	Query HandleTag...
12:36...	Explorer EXE	2988	NAME NOT FOUND	HKCU\Software\Classes\Applications\notepad.exe\Cur...	NAME NOT FOUND	Desired Access: R...

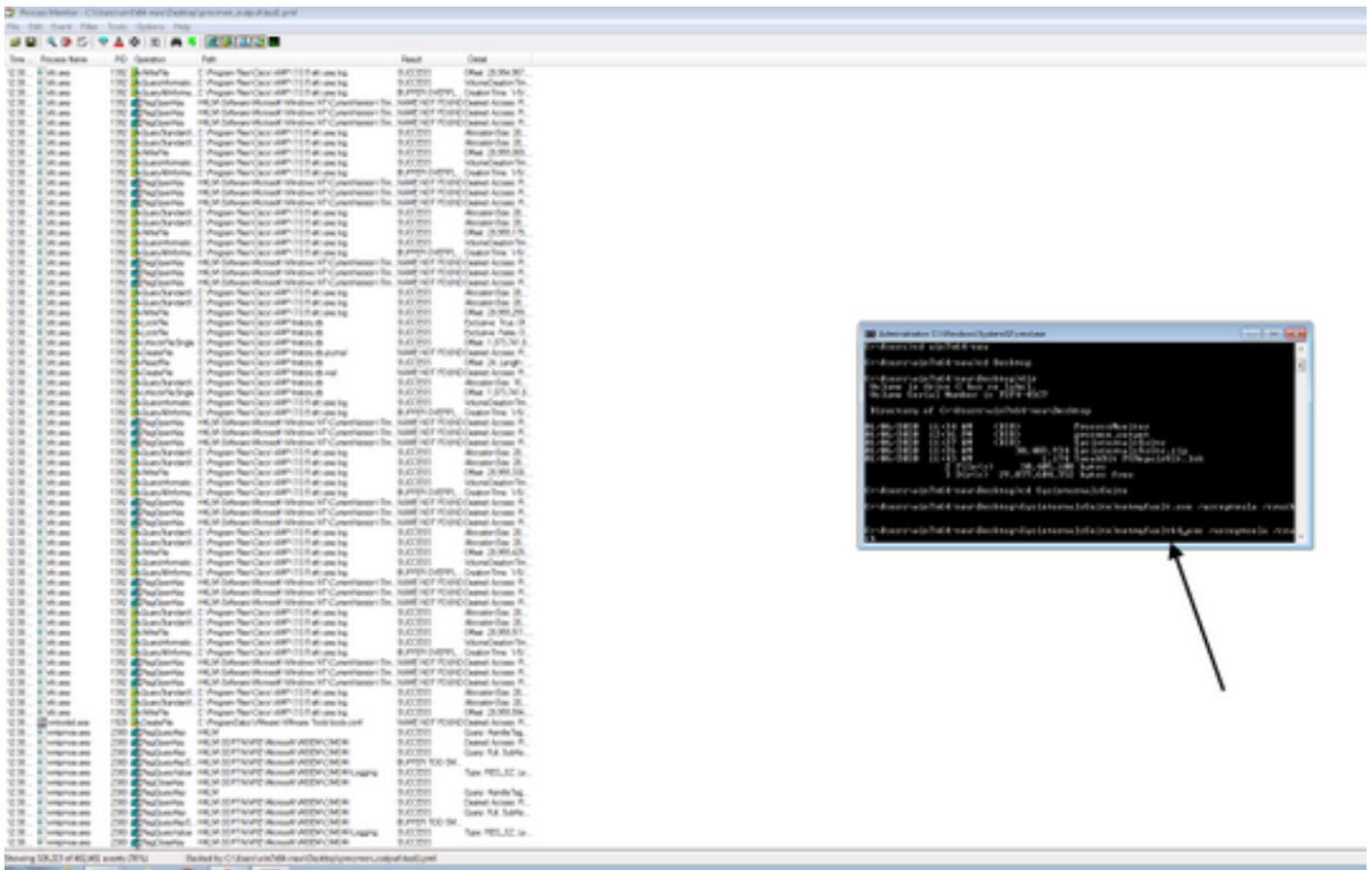
4.选择“生成威胁分析事件并每秒”。



5. 确保在Procmon中选择所有相关过滤器并收集数据。

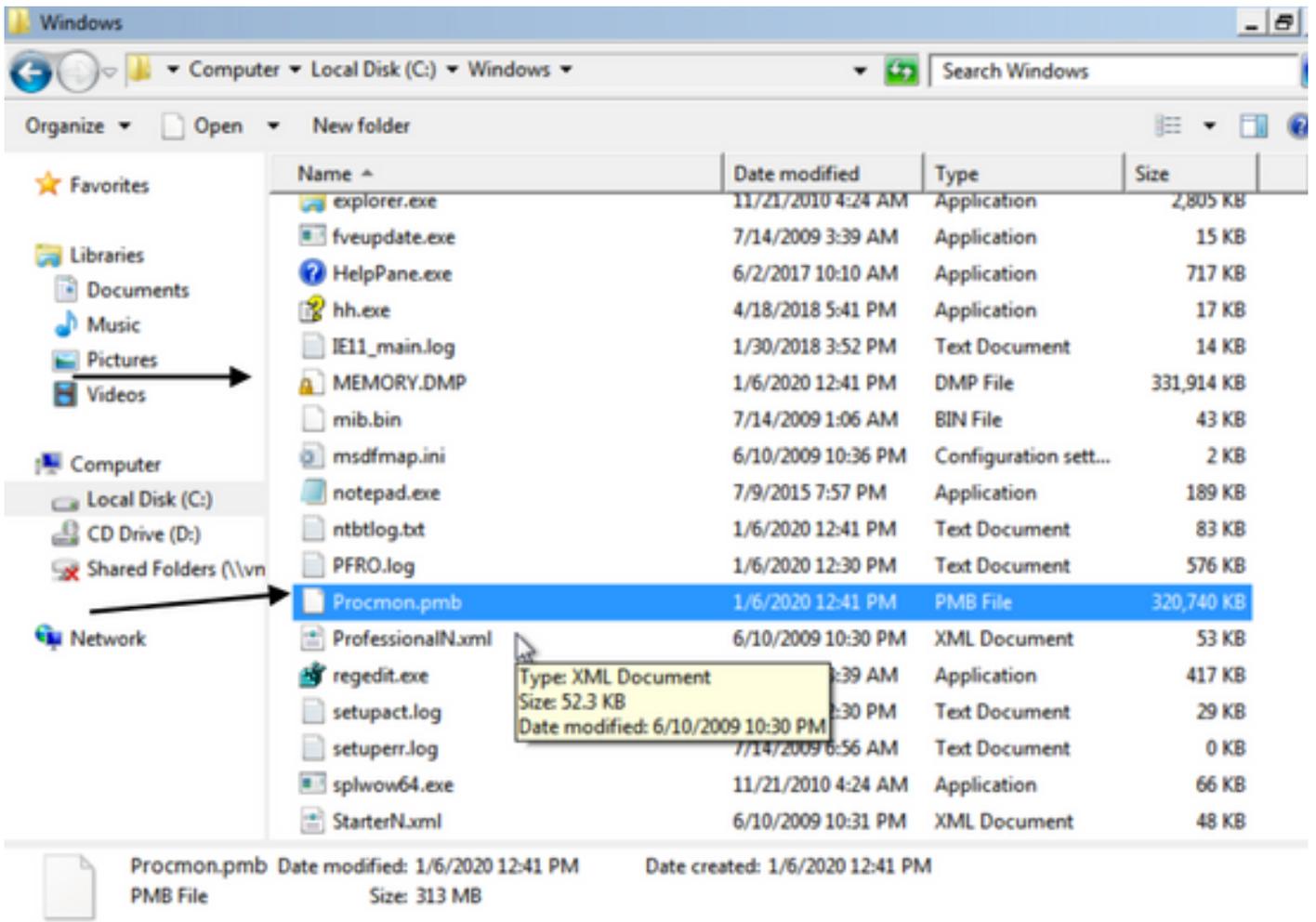
6. 如果无法复制崩溃，则可以使用NotMyFault64.exe实用程序强制Windows崩溃，您可以从该实用程序获取 <https://live.sysinternals.com/files/>

有关如何运行这些命令的说明如下：<https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump>



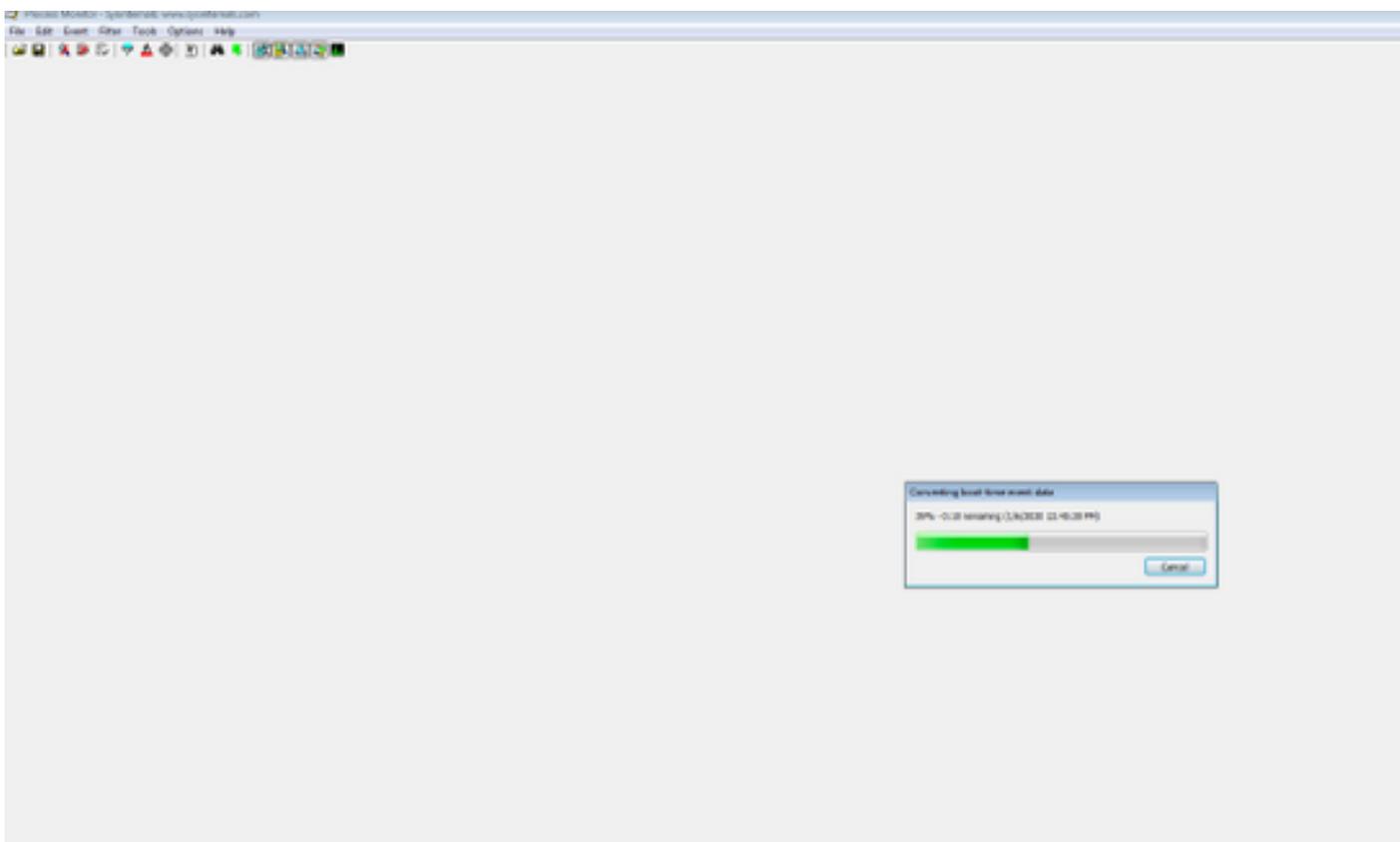
7.撞机。

8.将计算机引导到安全模式并手动收集Procmon.pmb和MEMORY.DMP，两个文件都在C:\Windows folder中。这些文件将与思科TAC共享。



7.或者，如果PMB文件在C:\Windows folder文件中生成，则如果能够将其引导到“正常模式”，则如果再次启动ProcMon，将看到以下日志。从而，您可以通过点击Save按钮重新保存事件。





Time	Process Name	PID	Operation	Path	Result	Detail
12:41...	smss.exe	292	Process Start		SUCCESS	Parent PID: 4, Com...
12:41...	smss.exe	292	Thread Create		SUCCESS	Thread ID: 296
12:41...	smss.exe	292	Load Image	C:\Windows\System32\smss.exe	SUCCESS	Image Base: 0x479...
12:41...	smss.exe	292	Load Image	C:\Windows\System32\ntldr.dll	SUCCESS	Image Base: 0x779...
12:41...	smss.exe	292	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\ima...	NAME NOT FOUND	Desired Access: Q...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	REPARSE	Desired Access: R...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	SUCCESS	Desired Access: R...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 1,024
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 1,024
12:41...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 74,752, Len...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 1,024, Leng...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 107,008, Le...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 104,448, Le...
12:41...	smss.exe	292	Thread Create		SUCCESS	Thread ID: 300
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 104,448
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset Length: 2,560
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MinNT	REPARSE	Desired I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MinNT	NAME NOT FOUND	Desired I/O Flags: Normal
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	REPARSE	Desired Access: Al...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	SUCCESS	Desired Access: Al...
12:41...	smss.exe	292	RegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	
12:41...	smss.exe	292	RegSetValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_SZ, Le...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: R...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_DWO...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_DWO...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 0, Name: A...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 1, Name: M...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 2, Name: N...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 3, Name: Pl...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 4, Name: P...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 5, Name: U...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NO MORE ENTRI...	Index: 6, Length: 4...
12:41...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...