如何收集ProcMon日志以排除启动时的AMP问题

目录

简介

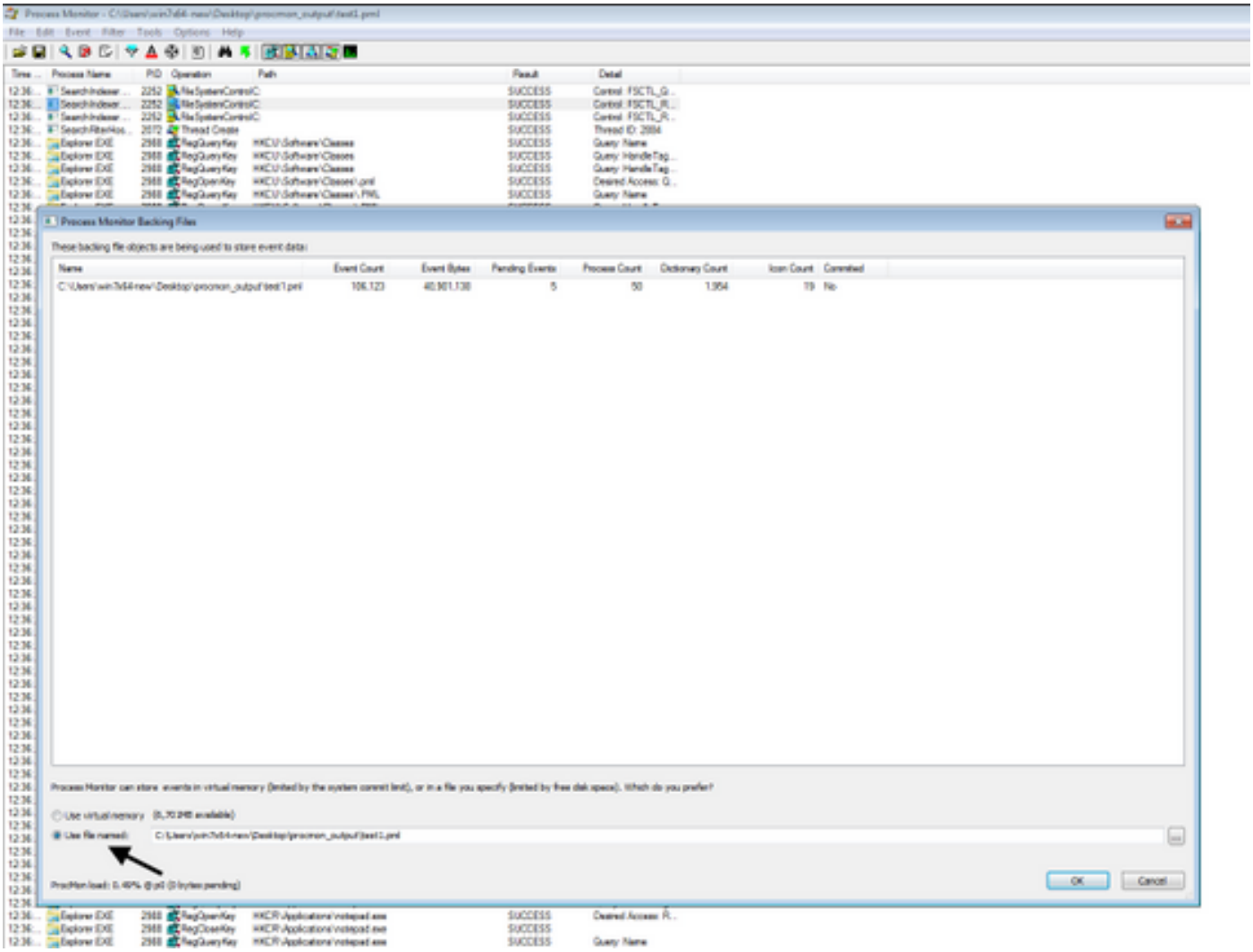
作为系统管理员，您可能希望使用进程监控器(procmon.exe)获取详细日志，以确定FireAMP连接器在计算机启动过程中是否出现挂起。思科TAC也会请求这些日志来排除此类问题。进程监控器是一个免费的实用程序，可帮助我们进行此操作。可以从https://docs.microsoft.com/en-us/sysinternals/downloads/procmon免费下载

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。

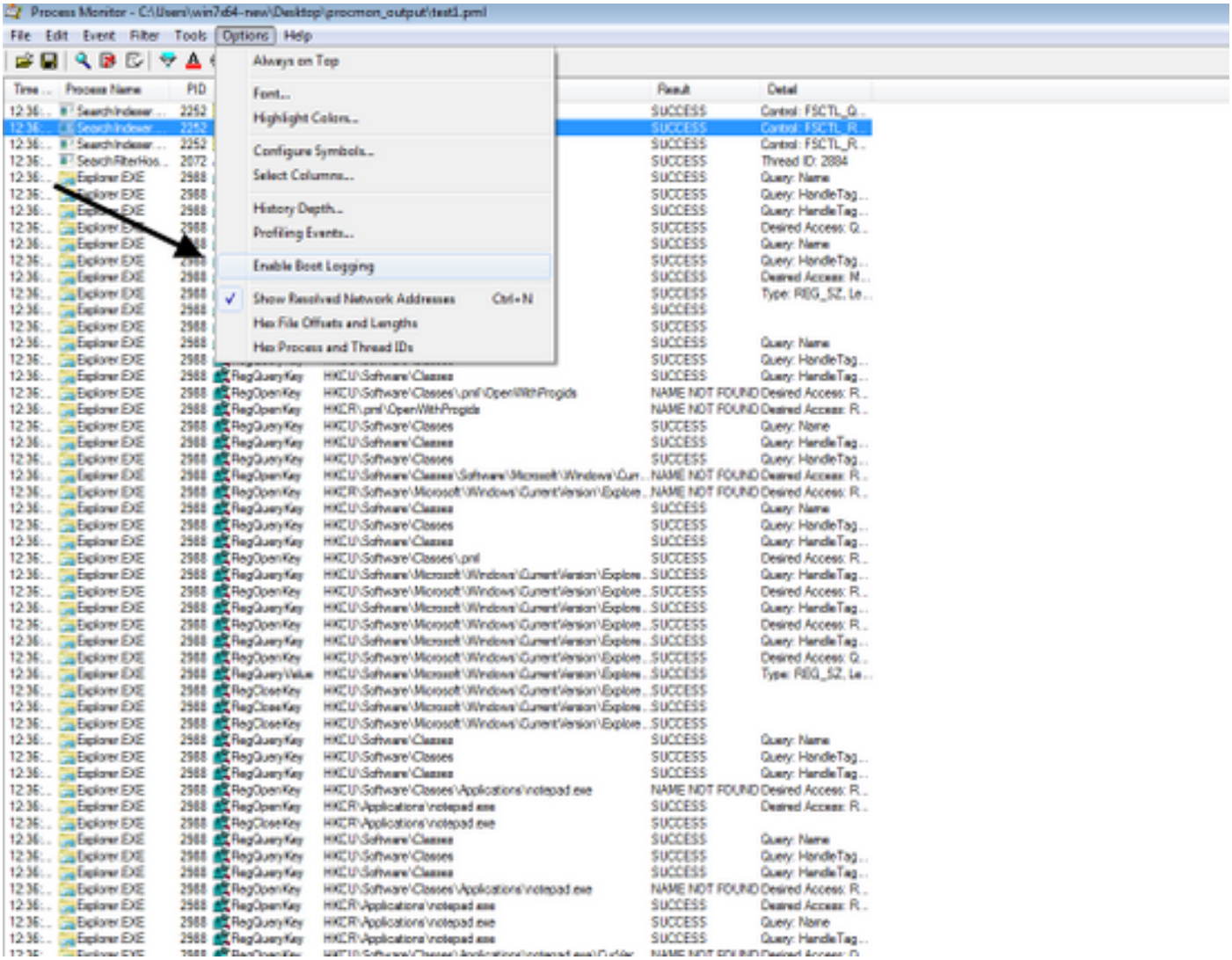
步骤:

1.以这种方式设置测试机，使问题易于重现。

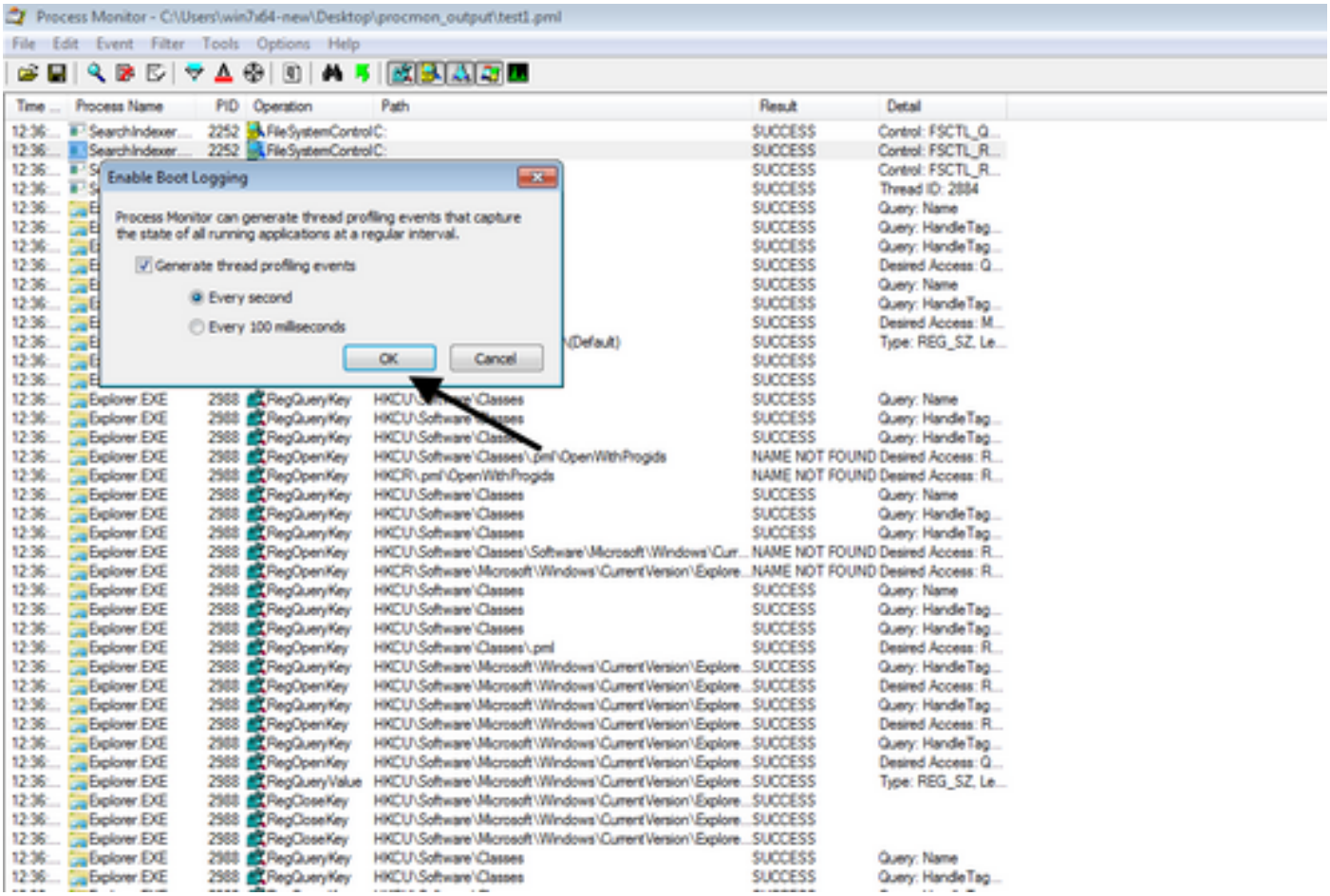
2.以管理员身份下载并运行ProcMon工具。转至“文**件” — >“进程监控器备份文**件”并选择**路径**。



3.在Procmon工具中，转到“选**项” — >“启用引导日志记录**”。



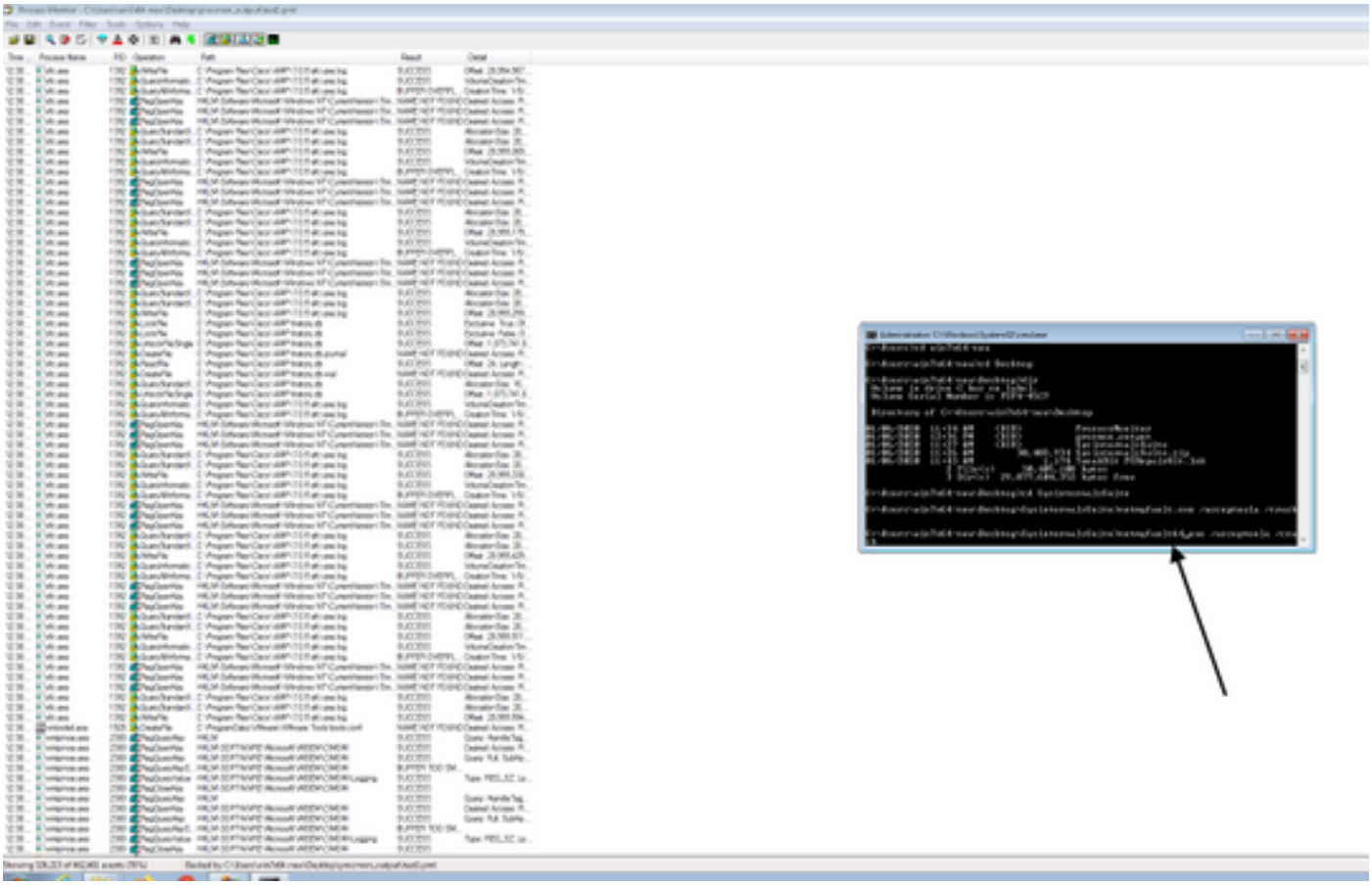
4.选择“生**成威胁分析事**件并**每秒**”。



5.确保在Procmon中选择所有相关过滤器并收集数据。

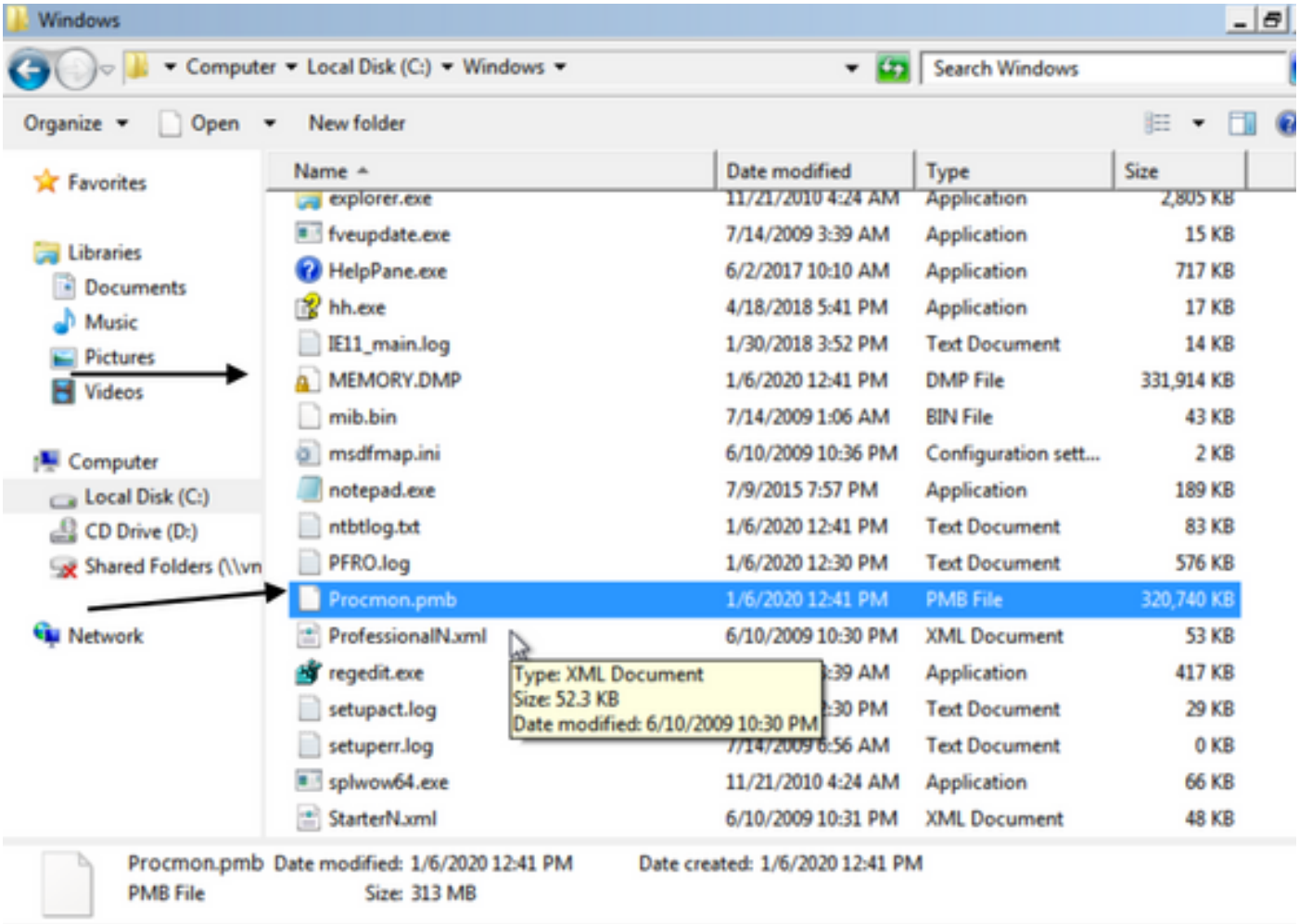
6.如果无法复制崩溃，则可以使用NotMyFault64.exe实用程序强制Windows崩溃，您可以从该实用程序获取 https://live.sysinternals.com/files/

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

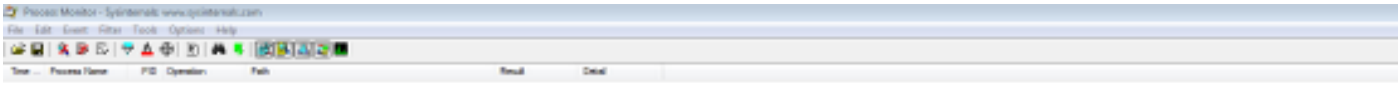


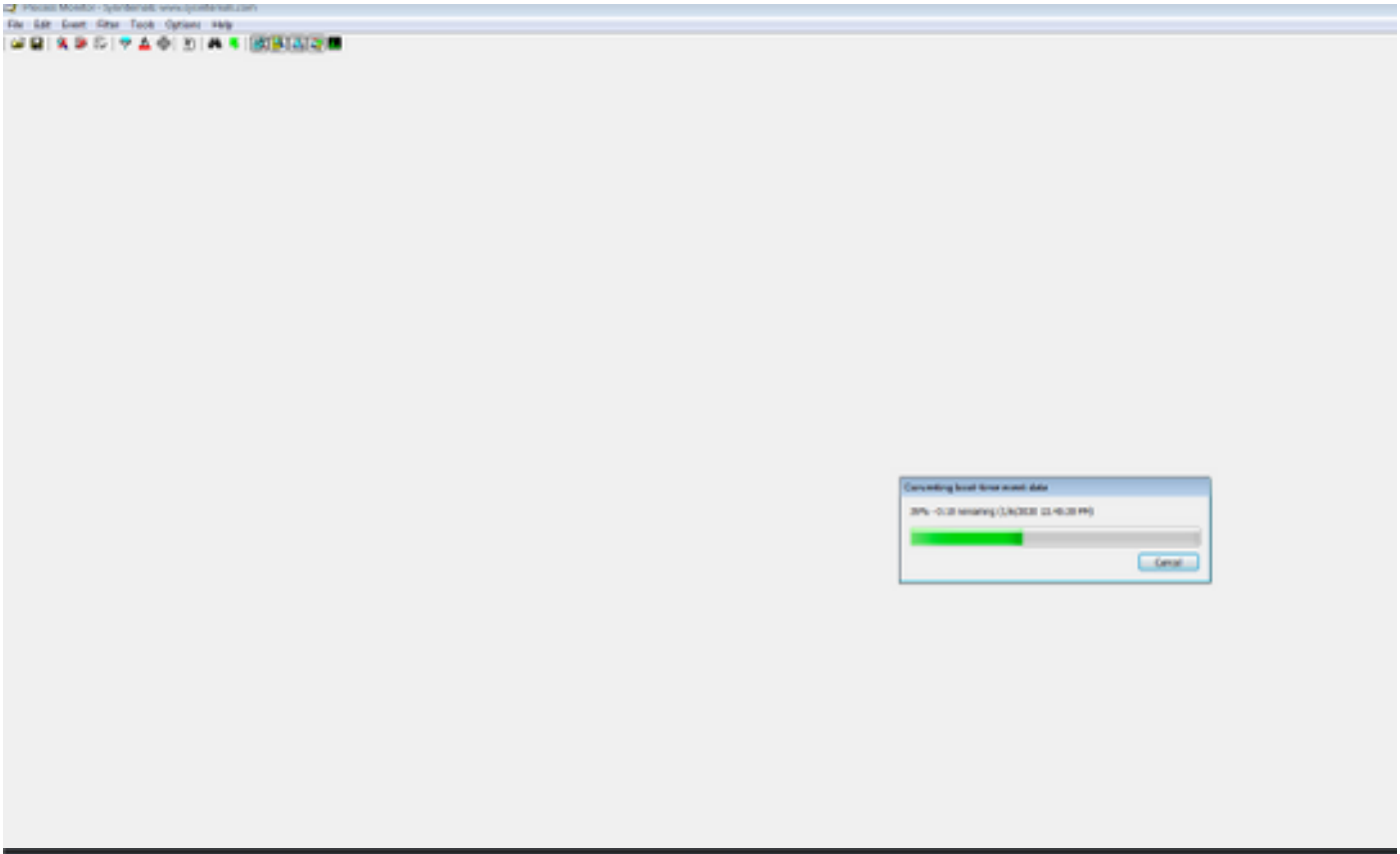
7.撞机。

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。





Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

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\ntdll.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 Length: 2,560 I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O Priority: Normal
12:41:...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 107,008, Le...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MiniNT	REPARSE	Desired Access: R...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MiniNT	NAME NOT FOUND	Desired Access: R...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\...	REPARSE	Desired Access: All...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\...	SUCCESS	Desired Access: All...
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: PI...
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...