起動時にAMPの問題をトラブルシューティングするためにProcMonログを収集する方法

内容
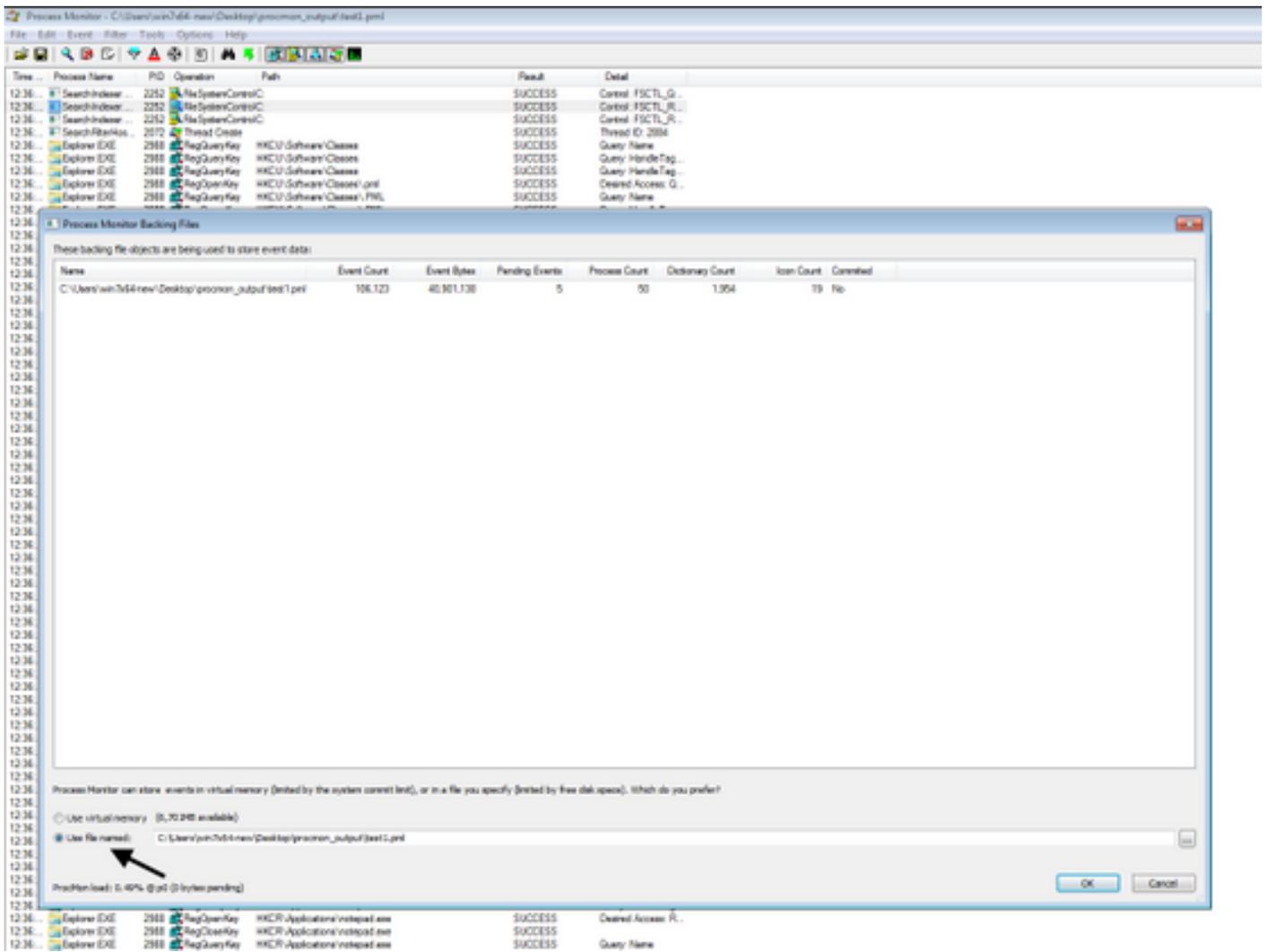
概要

システム管理者は、プロセスモニタ(procmon.exe)を使用して詳細なログを取得し、コンピュータの起動プロセス中にFireAMPコネクタがハングするかどうかを確認できます。これらのログは、このような問題のトラブルシューティングのためにCisco TACから要求されます。Process Monitorは無料のユーティリティで、ここで役立ちます。これはhttps://docs.microsoft.com/en-us/sysinternals/downloads/procmonから自由にダウンロードで[きます](#)
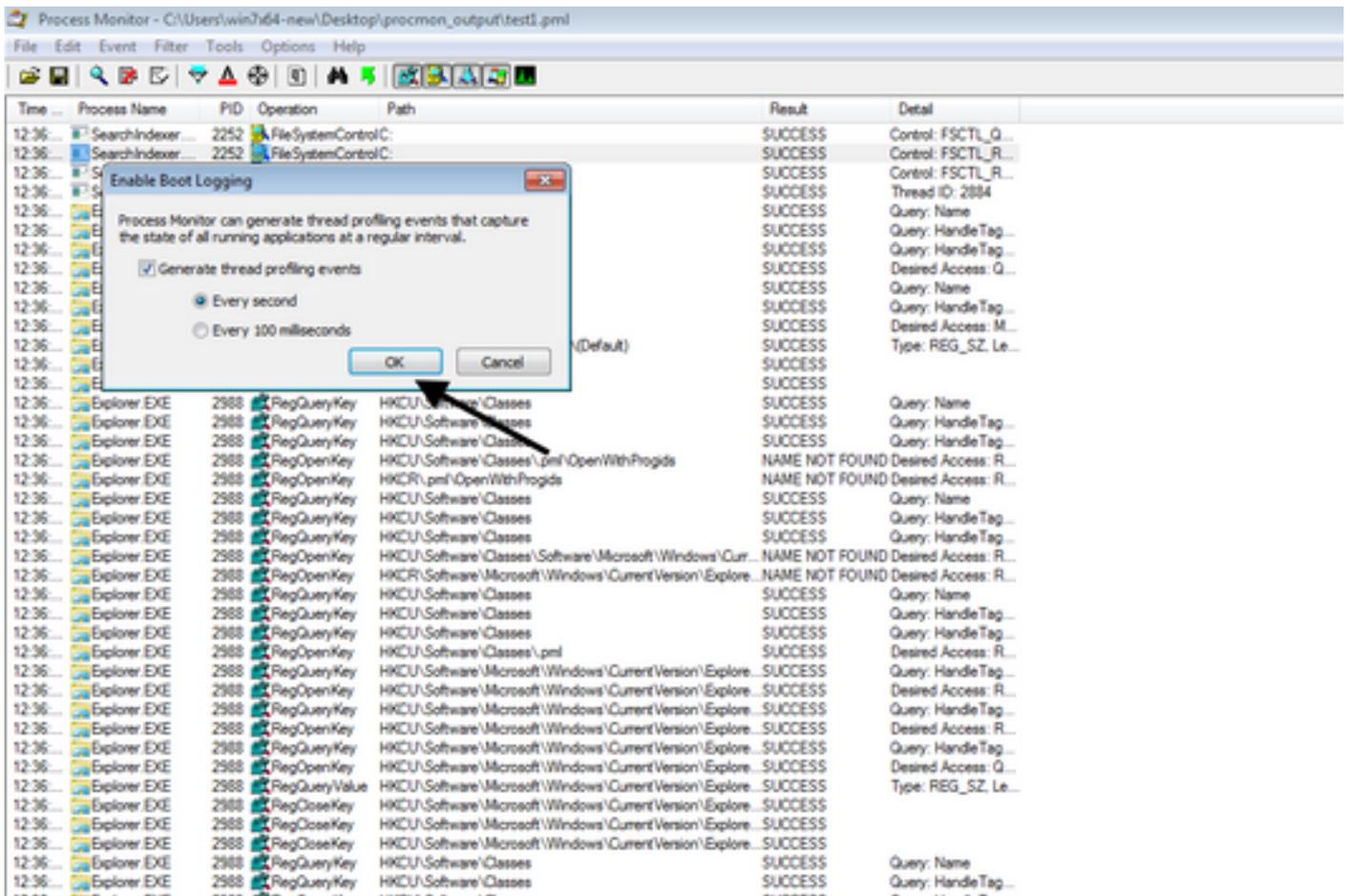
このドキュメントでは、システムブートプロセス中に問題が発生した場合（つまり、ブート時にBSODを生成している場合）に、ProcMonログとメモリダンプを収集する手順について説明します。 これらのログは、ブート中に発生するシステムイベントをキャプチャするために必要です。

手順：

1.試験機を簡単に再現できるようにセットアップする。

2.管理者としてProcMonツールをダウンロードして実行します。[File] -> [Process Monitor] [Backing Files]の順に選択し、[Path]を選択します。
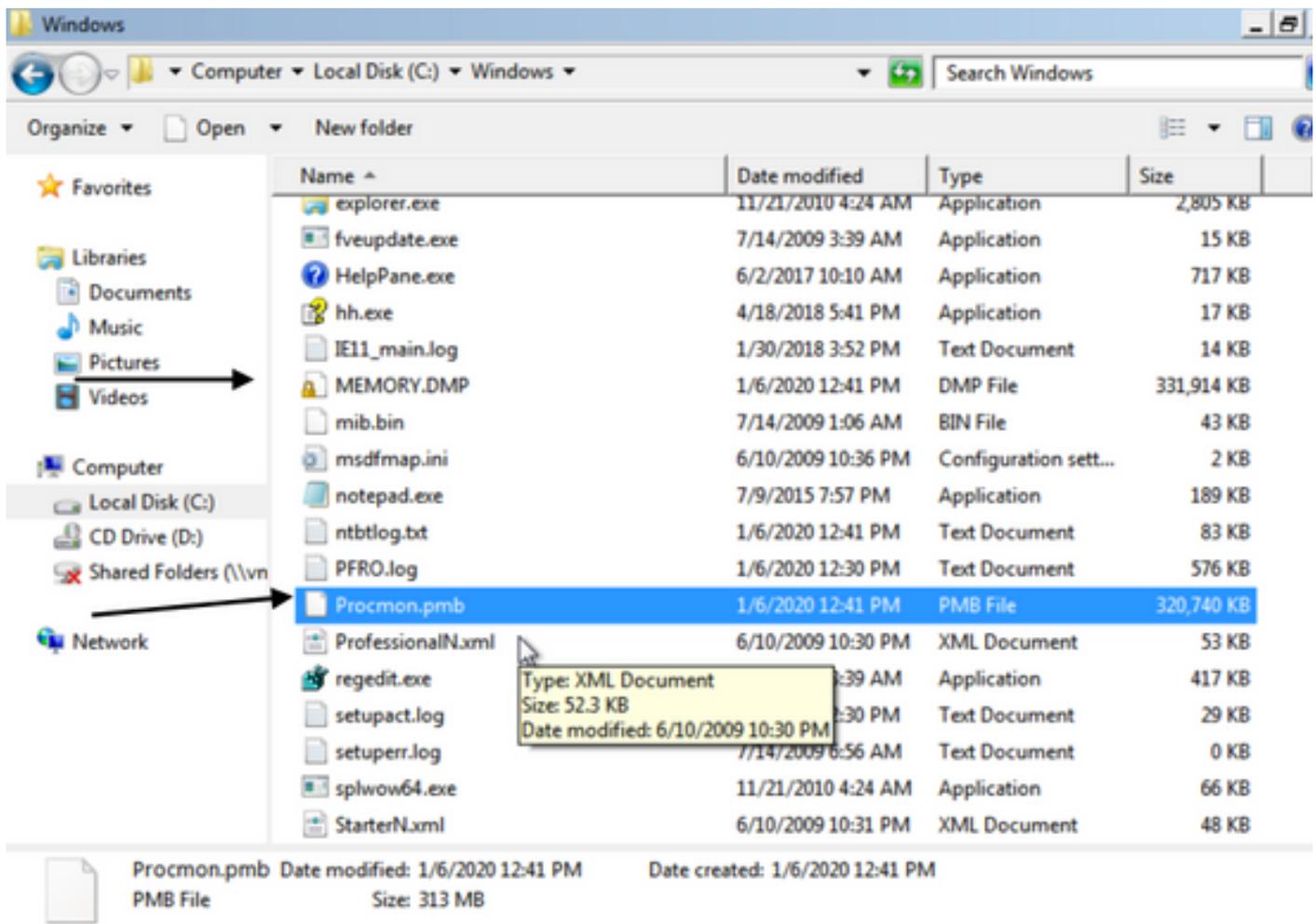
3. Procmonツールで、[Options] -> [Enable Boot Logging]に移動します。

4. [Generate threat profiling events]と[Every second]を選択します。
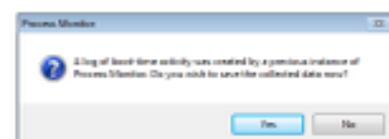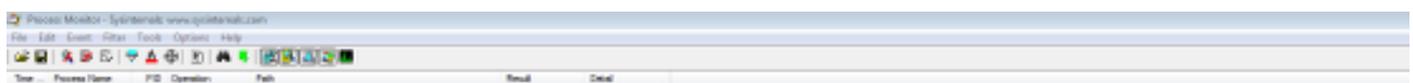
5.関連するすべてのフィルタがProcmonで選択され、データが収集されていることを確認します。
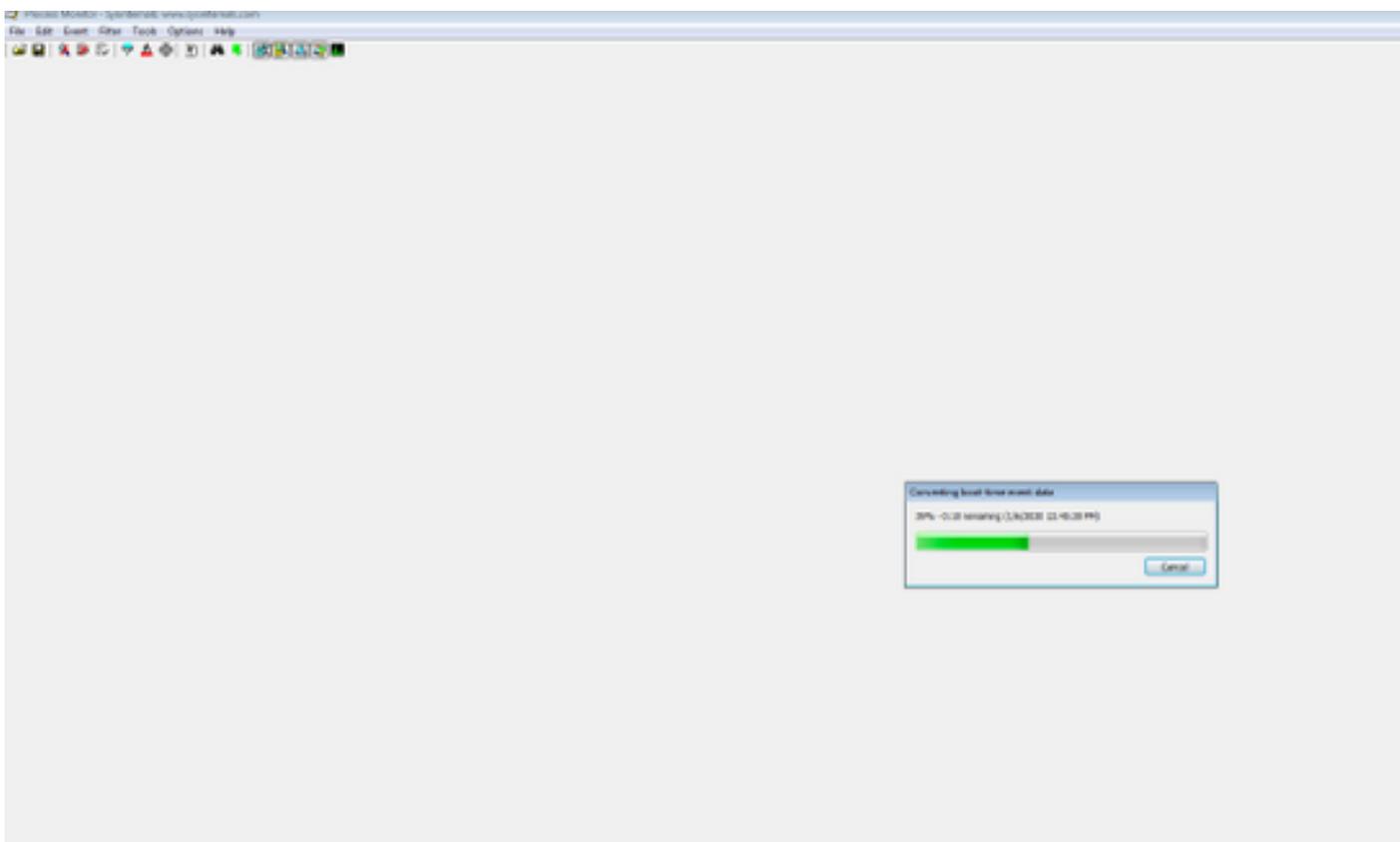
6.クラッシュを複製できない場合は、NotMyFault64.exeユーティリティを使用してWindowsを強制的にクラッシュさせることができます。このユーティリティは、Windowsから取得できます https://live.sysinternals.com/files/

これを実行する手順は次のとおりです。 https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump

7.マシンをクラッシュさせます。

8.マシンをセーフモードで起動し、**Procmon.pmb**と**MEMORY.DMP**を手動で収集します。両方の
ファイルは**C:\Windows folder**にあります。これらのファイルは、Cisco TACと共有する必要があ
ります。

7.オプションとして、C:\Windows folderディレクトリにPMBファイルが生成された場合に通常モードで起動できる場合、ProcMonを再起動すると、次のログが表示されます。[保存]ボタンをクリックすると、イベントを再保存できます。

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: ...
12:41:...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: ...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MiniNT	REPARSE	Desi...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MiniNT	NAME NOT FOUND	Desi...
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...	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: P...
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...

Tooltip:
Offset: 104,448
Length: 2,560
I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
Priority: Normal