Como coletar registros ProcMon para solucionar problemas de AMP na inicialização

Contents

Introduction

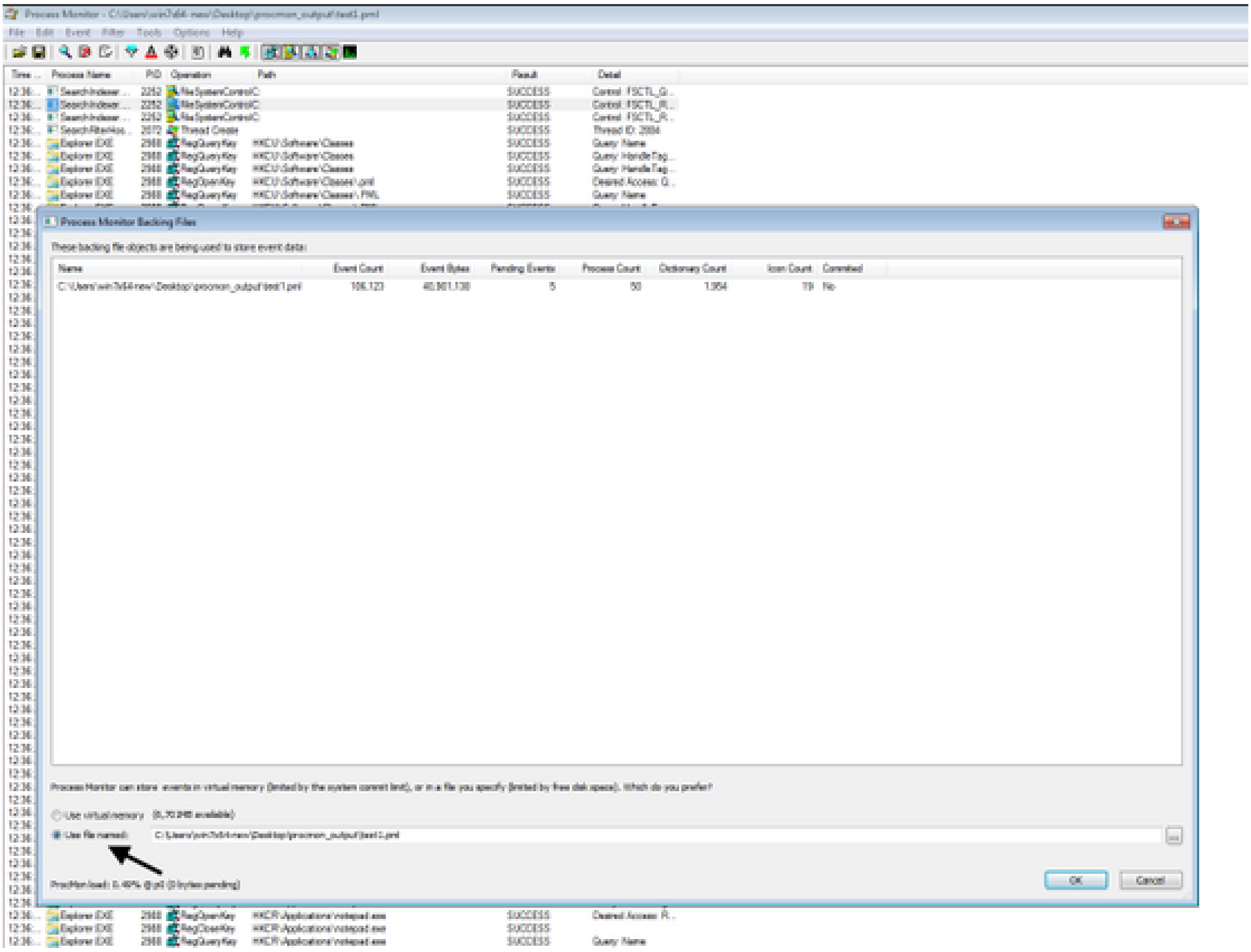
Como administrador de sistema, você pode querer obter registros detalhados usando o Process Monitor (procmon.exe) para determinar se o conector FireAMP trava durante o processo de inicialização do computador. Esses registros também serão solicitados pelo Cisco TAC para solucionar esses problemas. O Process Monitor é um utilitário gratuito que pode nos ajudar aqui. Pode ser baixado gratuitamente em https://docs.microsoft.com/en-us/sysinternals/downloads/procmon

Este documento descreve as etapas sobre como coletar registros ProcMon e despejo de memória se o problema ocorrer durante um processo de inicialização do sistema (o que significa que ele está gerando BSODs na inicialização). Esses registros são necessários para capturar os eventos do sistema que ocorrem durante a inicialização.

Procedimento:

1. Configurar as máquinas de ensaio de modo a que o problema possa ser facilmente reproduzido.

2. Baixe e execute a ferramenta ProcMon como administrador. Vá para **File -> Process Monitor Backing Files** e selecione um **Path**.



Process Monitor - C:\Users\win7x64-new\Desktop\procmon_output\test1.pml

```
Time ...  Process Name    PID   Operation          Path                               Result   Detail
12:36...  SearchIndexer... 2252 FileSystemControlC                                    SUCCESS  Control: FSCTL_G...
12:36...  SearchIndexer... 2252 FileSystemControlC                                    SUCCESS  Control: FSCTL_R...
12:36...  SearchIndexer... 2252 FileSystemControlC                                    SUCCESS  Control: FSCTL_R...
12:36...  SearchFilterHos... 2072 Thread Create                                       SUCCESS  Thread ID: 2884
12:36...  Explorer.EXE    2988  RegQueryKey        HKCU\Software\Classes              SUCCESS  Query: Name
12:36...  Explorer.EXE    2988  RegQueryKey        HKCU\Software\Classes              SUCCESS  Query: HandleTag...
12:36...  Explorer.EXE    2988  RegQueryKey        HKCU\Software\Classes              SUCCESS  Query: HandleTag...
12:36...  Explorer.EXE    2988  RegOpenKey         HKCU\Software\Classes\.pml         SUCCESS  Desired Access: Q...
12:36...  Explorer.EXE    2988  RegQueryKey        HKCU\Software\Classes\.PML         SUCCESS  Query: Name
```

Process Monitor Backing Files

These backing file objects are being used to store event data:

Name	Event Count	Event Bytes	Pending Events	Process Count	Dictionary Count	Icon Count	Committed
C:\Users\win7x64-new\Desktop\procmon_output\test1.pml	106.123	40.901.138	5	50	1.954	19	No

Process Monitor can store events in virtual memory (limited by the system commit limit), or in a file you specify (limited by free disk space). Which do you prefer?

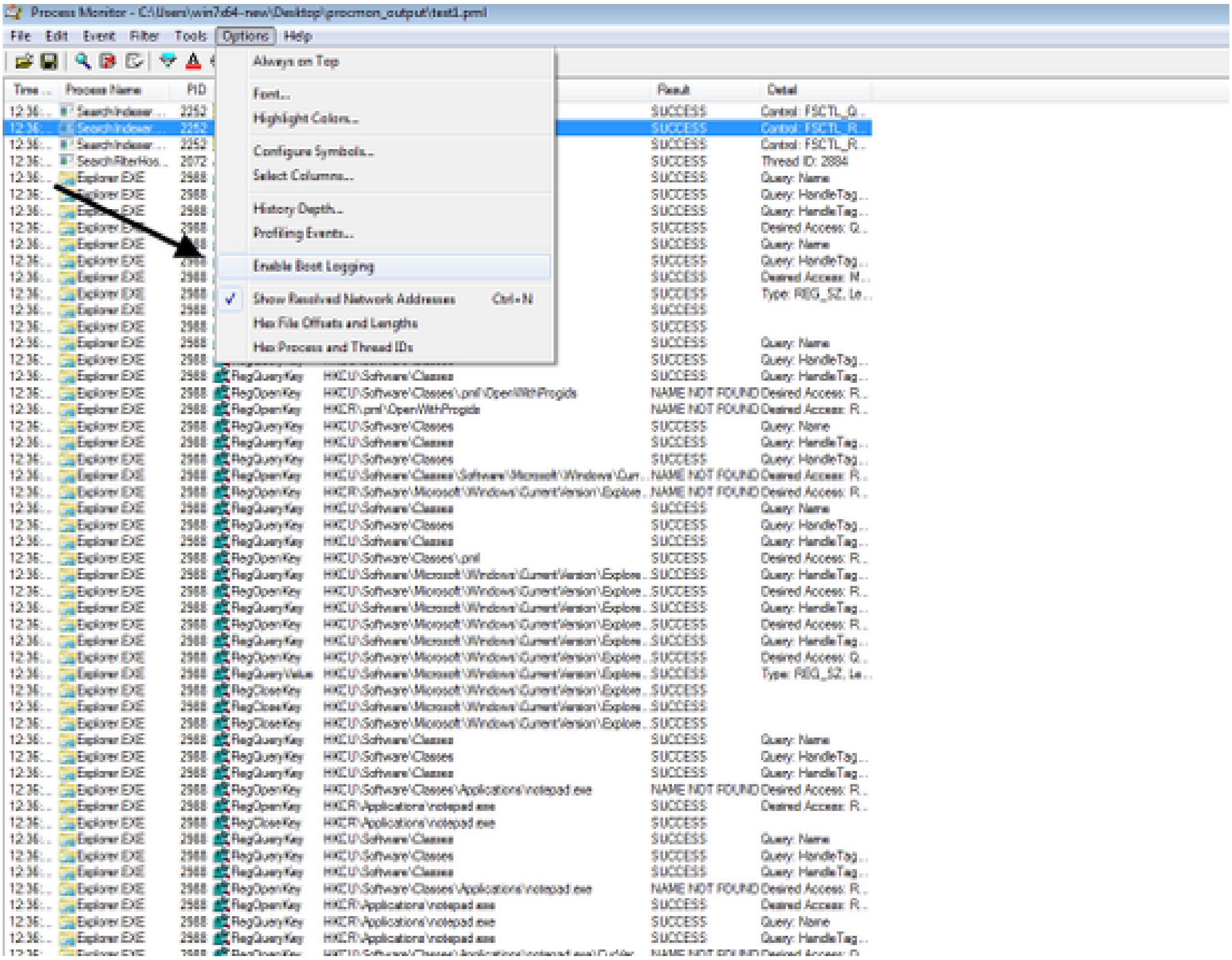
○ Use virtual memory (6.70 [illegible] available)

● Use file named: C:\Users\win7x64-new\Desktop\procmon_output\test1.pml

ProcMon load: 0.49% @ [illegible] (0 bytes pending)

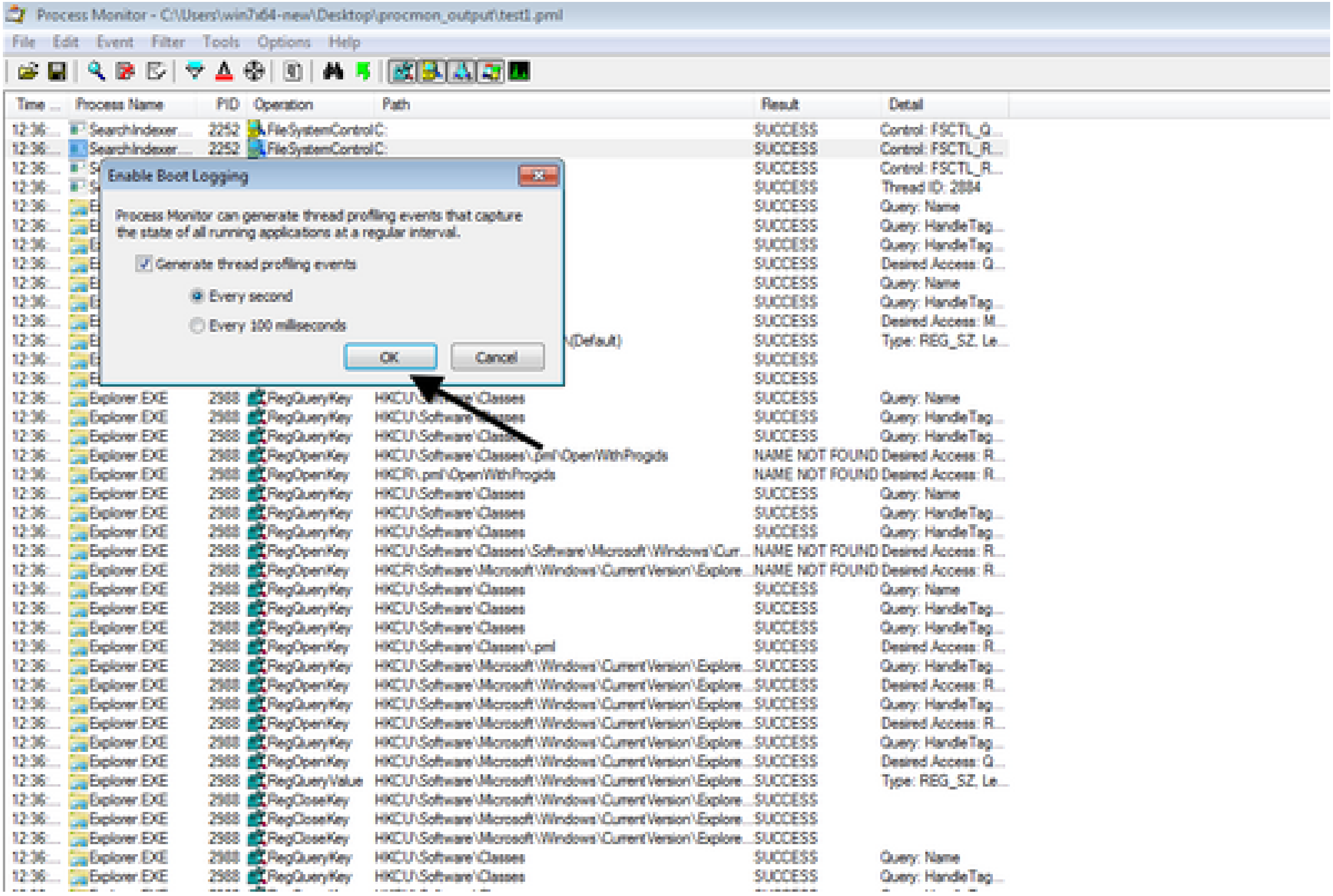
```
12:36...  Explorer.EXE    2988  RegOpenKey         HKCR\Applications\notepad.exe      SUCCESS  Desired Access: R...
12:36...  Explorer.EXE    2988  RegCloseKey        HKCR\Applications\notepad.exe      SUCCESS
12:36...  Explorer.EXE    2988  RegQueryKey        HKCR\Applications\notepad.exe      SUCCESS  Query: Name
```

3. Na ferramenta Procmon, vá para **Options -> Enable Boot Logging (Opções -> Ativar registro de inicialização)**.


Process Monitor - C:\Users\win7x64-new\Desktop\procmon_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                                                                                   Result          Detail
12:36:... SearchIndexer ...  2252                                                                                  SUCCESS         Control: FSCTL_Q...
12:36:... SearchIndexer ...  2252                                                                                  SUCCESS         Control: FSCTL_R...
12:36:... SearchIndexer ...  2252                                                                                  SUCCESS         Control: FSCTL_R...
12:36:... SearchFilterHos... 2072                                                                                  SUCCESS         Thread ID: 2884
12:36:... Explorer.EXE       2988                                                                                  SUCCESS         Query: Name
12:36:... Explorer.EXE       2988                                                                                  SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988                                                                                  SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988                                                                                  SUCCESS         Desired Access: Q...
12:36:... Explorer.EXE       2988                                                                                  SUCCESS         Query: Name
12:36:... Explorer.EXE       2988                                                                                  SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988                                                                                  SUCCESS         Desired Access: M...
12:36:... Explorer.EXE       2988                                                                                  SUCCESS         Type: REG_SZ, Le...
12:36:... Explorer.EXE       2988                                                                                  SUCCESS
12:36:... Explorer.EXE       2988                                                                                  SUCCESS
12:36:... Explorer.EXE       2988                                                                                  SUCCESS         Query: Name
12:36:... Explorer.EXE       2988                                                                                  SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCU\Software\Classes\.pml\OpenWithProgids                         NAME NOT FOUND  Desired Access: R...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCR\.pml\OpenWithProgids                                          NAME NOT FOUND  Desired Access: R...
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: Name
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCU\Software\Classes\Software\Microsoft\Windows\Curr...           NAME NOT FOUND  Desired Access: R...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCR\Software\Microsoft\Windows\CurrentVersion\Explore...          NAME NOT FOUND  Desired Access: R...
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: Name
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCU\Software\Classes\.pml                                         SUCCESS         Desired Access: R...
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...          SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...          SUCCESS         Desired Access: R...
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...          SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...          SUCCESS         Desired Access: R...
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...          SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...          SUCCESS         Desired Access: Q...
12:36:... Explorer.EXE       2988 RegQueryValue HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...          SUCCESS         Type: REG_SZ, Le...
12:36:... Explorer.EXE       2988 RegCloseKey   HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...          SUCCESS
12:36:... Explorer.EXE       2988 RegCloseKey   HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...          SUCCESS
12:36:... Explorer.EXE       2988 RegCloseKey   HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...          SUCCESS
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: Name
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCU\Software\Classes\Applications\notepad.exe                     NAME NOT FOUND  Desired Access: R...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCR\Applications\notepad.exe                                      SUCCESS         Desired Access: R...
12:36:... Explorer.EXE       2988 RegCloseKey   HKCR\Applications\notepad.exe                                      SUCCESS
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: Name
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegQueryKey   HKCU\Software\Classes                                              SUCCESS         Query: HandleTag...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCU\Software\Classes\Applications\notepad.exe                     NAME NOT FOUND  Desired Access: R...
12:36:... Explorer.EXE       2988 RegOpenKey    HKCR\Applications\notepad.exe                                      SUCCESS         Desired Access: R...
12:36:... Explorer.EXE       2988 RegQueryKey   HKCR\Applications\notepad.exe                                      SUCCESS         Query: Name
12:36:... Explorer.EXE       2988 RegQueryKey   HKCR\Applications\notepad.exe                                      SUCCESS         Query: HandleTag...
```

4. Selecione **Gerar perfis de ameaças** e **a cada segundo.**


Process Monitor - C:\Users\win7x64-new\Desktop\procmon_output\test1.pml
File Edit Event Filter Tools Options Help

Enable Boot Logging

Process Monitor can generate thread profiling events that capture the state of all running applications at a regular interval.

☑ Generate thread profiling events

● Every second

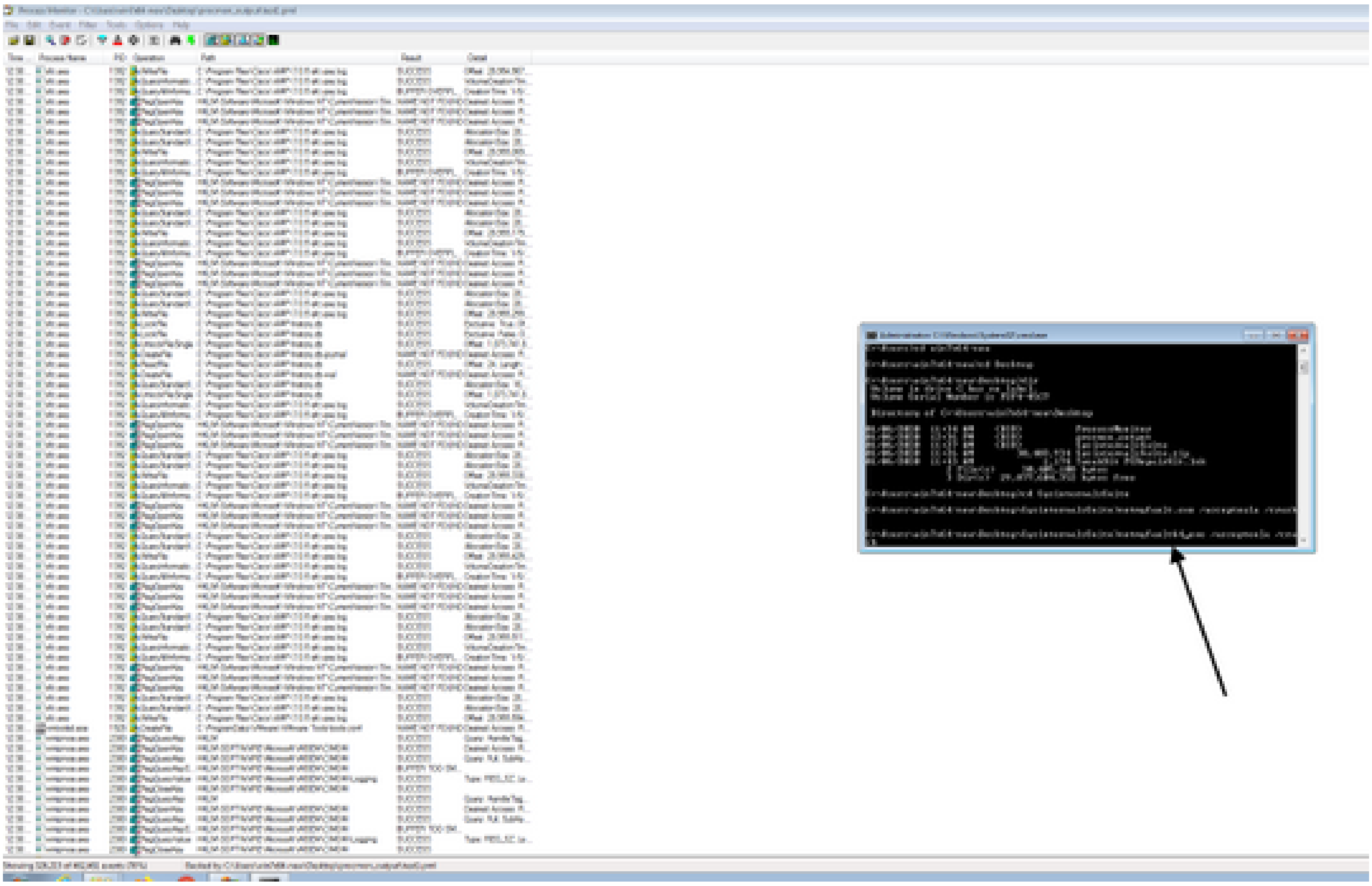
○ Every 100 milliseconds

Time ...	Process Name	PID	Operation	Path	Result	Detail
12:36:...	SearchIndexer...	2252	FileSystemControl	C:	SUCCESS	Control: FSCTL_Q...
12:36:...	SearchIndexer...	2252	FileSystemControl	C:	SUCCESS	Control: FSCTL_R...
12:36:...	S				SUCCESS	Control: FSCTL_R...
12:36:...	S				SUCCESS	Thread ID: 2884
12:36:...	E				SUCCESS	Query: Name
12:36:...	E				SUCCESS	Query: HandleTag...
12:36:...	E				SUCCESS	Query: HandleTag...
12:36:...	E				SUCCESS	Desired Access: Q...
12:36:...	E				SUCCESS	Query: Name
12:36:...	E				SUCCESS	Query: HandleTag...
12:36:...	E				SUCCESS	Desired Access: M...
12:36:...	E			\(Default)	SUCCESS	Type: REG_SZ, Le...
12:36:...	E				SUCCESS	
12:36:...	E				SUCCESS	
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:36:...	Explorer.EXE	2988	RegOpenKey	HKCU\Software\Classes\.pml\OpenWithProgids	NAME NOT FOUND	Desired Access: R...
12:36:...	Explorer.EXE	2988	RegOpenKey	HKCR\.pml\OpenWithProgids	NAME NOT FOUND	Desired Access: R...
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:36:...	Explorer.EXE	2988	RegOpenKey	HKCU\Software\Classes\Software\Microsoft\Windows\Curr...	NAME NOT FOUND	Desired Access: R...
12:36:...	Explorer.EXE	2988	RegOpenKey	HKCR\Software\Microsoft\Windows\CurrentVersion\Explore...	NAME NOT FOUND	Desired Access: R...
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:36:...	Explorer.EXE	2988	RegOpenKey	HKCU\Software\Classes\.pml	SUCCESS	Desired Access: R...
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...	SUCCESS	Query: HandleTag...
12:36:...	Explorer.EXE	2988	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...	SUCCESS	Desired Access: R...
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...	SUCCESS	Query: HandleTag...
12:36:...	Explorer.EXE	2988	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...	SUCCESS	Desired Access: R...
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...	SUCCESS	Query: HandleTag...
12:36:...	Explorer.EXE	2988	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...	SUCCESS	Desired Access: Q...
12:36:...	Explorer.EXE	2988	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...	SUCCESS	Type: REG_SZ, Le...
12:36:...	Explorer.EXE	2988	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...	SUCCESS	
12:36:...	Explorer.EXE	2988	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...	SUCCESS	
12:36:...	Explorer.EXE	2988	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explore...	SUCCESS	
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...

5. Verifique se todos os filtros relevantes estão selecionados em Procmon e se os dados estão sendo coletados.

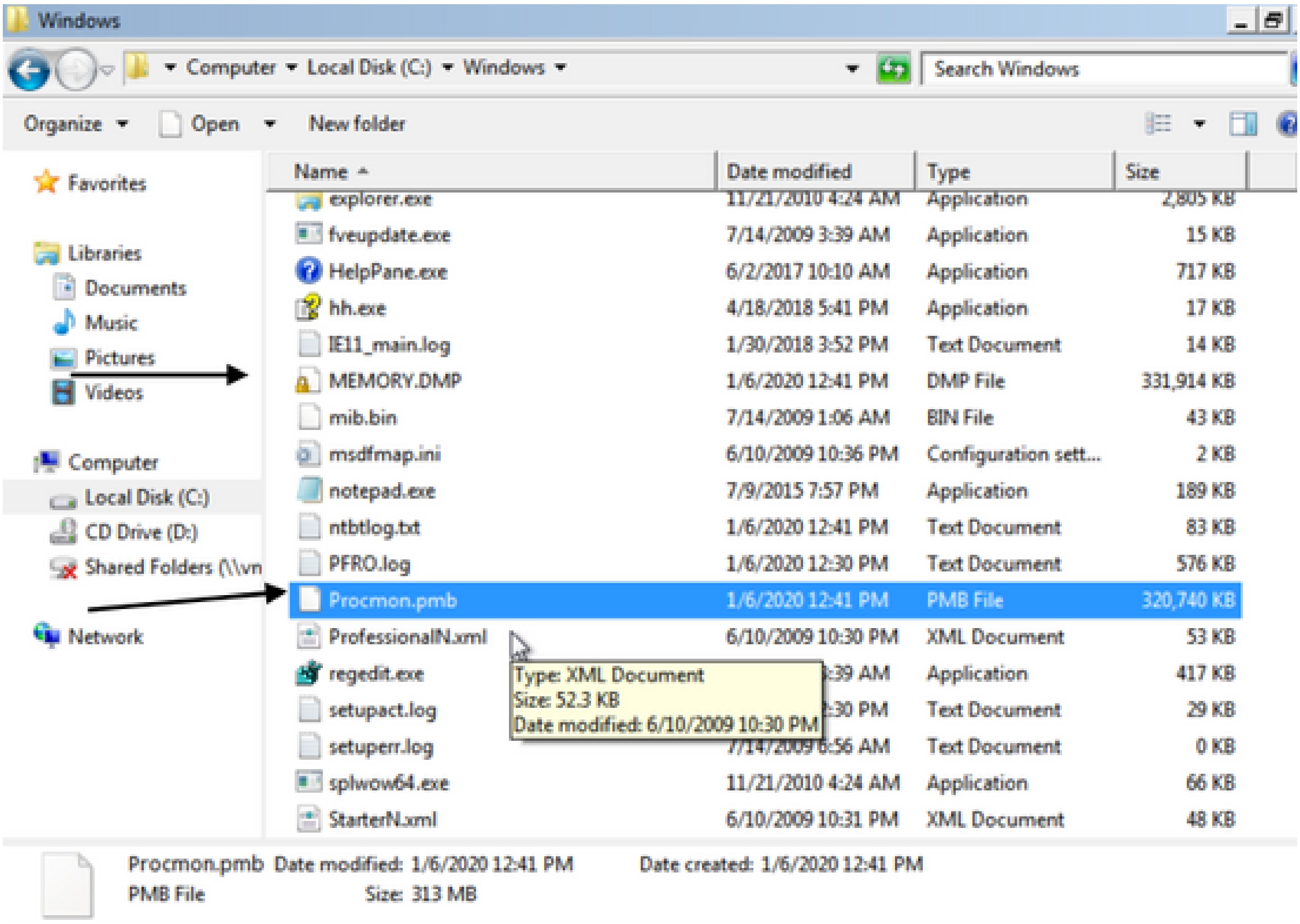
6. Se você não conseguir replicar o travamento, você pode forçar o travamento do Windows usando o utilitário NotMyFault64.exe que você pode obter do https://live.sysinternals.com/files/

As instruções sobre como executar estão aqui: https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump



7. Quebre a máquina.

8. Inicialize a máquina no modo de segurança e colete manualmente **Procmon.pmb** e **MEMORY.DMP**, ambos os arquivos estão em C:\Windows folder. Esses arquivos devem ser compartilhados com o Cisco TAC.

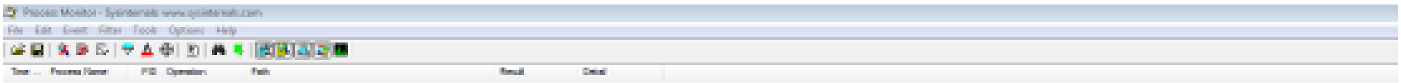


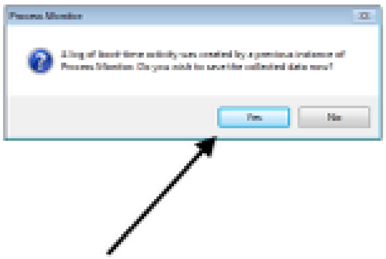
Name	Date modified	Type	Size
explorer.exe	11/21/2010 4:24 AM	Application	2,805 KB
fveupdate.exe	7/14/2009 3:39 AM	Application	15 KB
HelpPane.exe	6/2/2017 10:10 AM	Application	717 KB
hh.exe	4/18/2018 5:41 PM	Application	17 KB
IE11_main.log	1/30/2018 3:52 PM	Text Document	14 KB
MEMORY.DMP	1/6/2020 12:41 PM	DMP File	331,914 KB
mib.bin	7/14/2009 1:06 AM	BIN File	43 KB
msdfmap.ini	6/10/2009 10:36 PM	Configuration sett...	2 KB
notepad.exe	7/9/2015 7:57 PM	Application	189 KB
ntbtlog.txt	1/6/2020 12:41 PM	Text Document	83 KB
PFRO.log	1/6/2020 12:30 PM	Text Document	576 KB
Procmon.pmb	1/6/2020 12:41 PM	PMB File	320,740 KB
ProfessionalN.xml	6/10/2009 10:30 PM	XML Document	53 KB
regedit.exe	:39 AM	Application	417 KB
setupact.log	:30 PM	Text Document	29 KB
setuperr.log	7/14/2009 6:56 AM	Text Document	0 KB
splwow64.exe	11/21/2010 4:24 AM	Application	66 KB
StarterN.xml	6/10/2009 10:31 PM	XML Document	48 KB

Type: XML Document
Size: 52.3 KB
Date modified: 6/10/2009 10:30 PM

Procmon.pmb Date modified: 1/6/2020 12:41 PM Date created: 1/6/2020 12:41 PM
PMB File Size: 313 MB

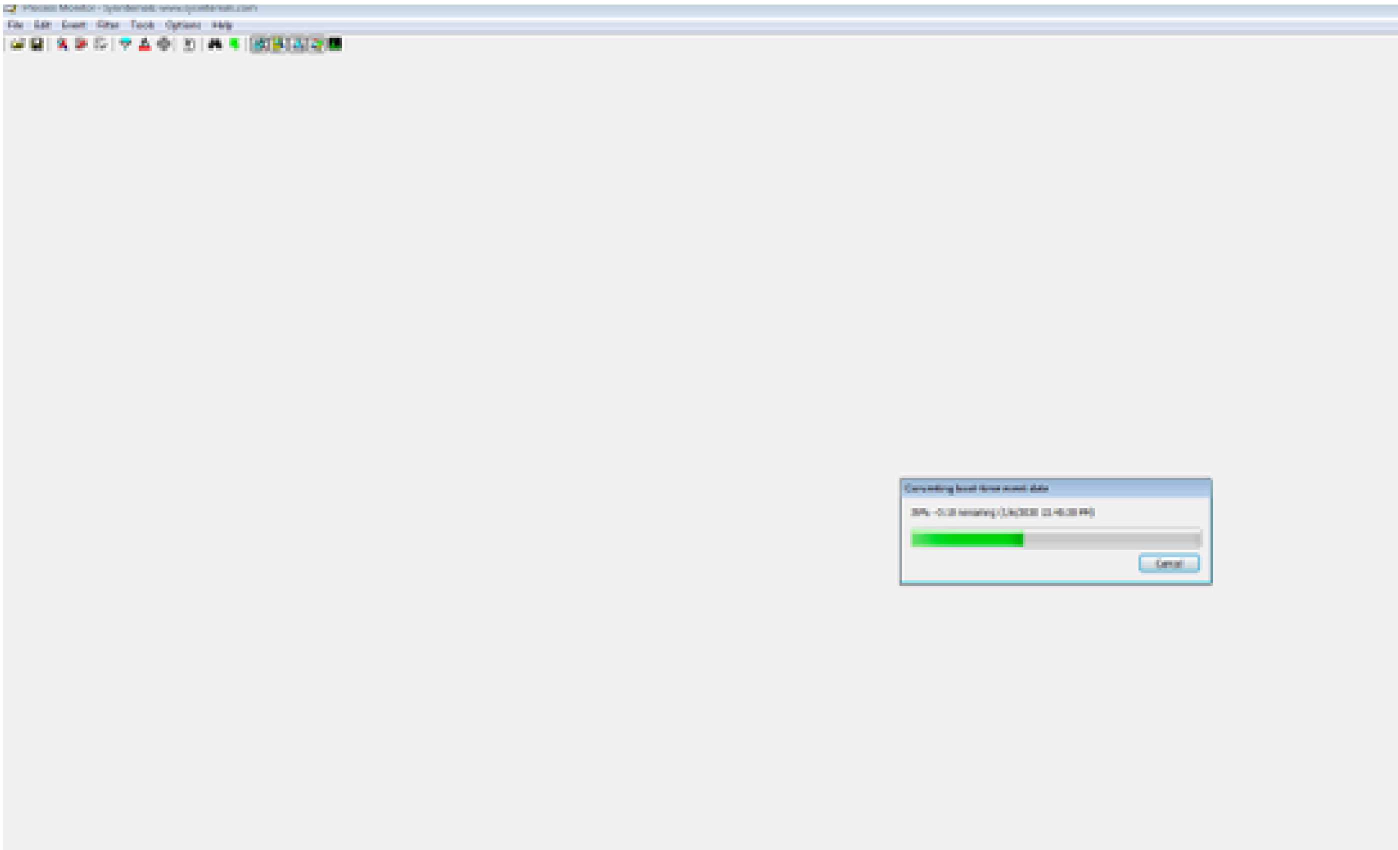
7. Opcionalmente, se você puder inicializá-lo no "modo normal" se os arquivos PMB forem gerados no diretório C:\Windows folder, se você iniciar o ProcMon novamente, verá os seguintes registros. A partir disso, você pode salvar novamente os eventos clicando no botão Salvar.

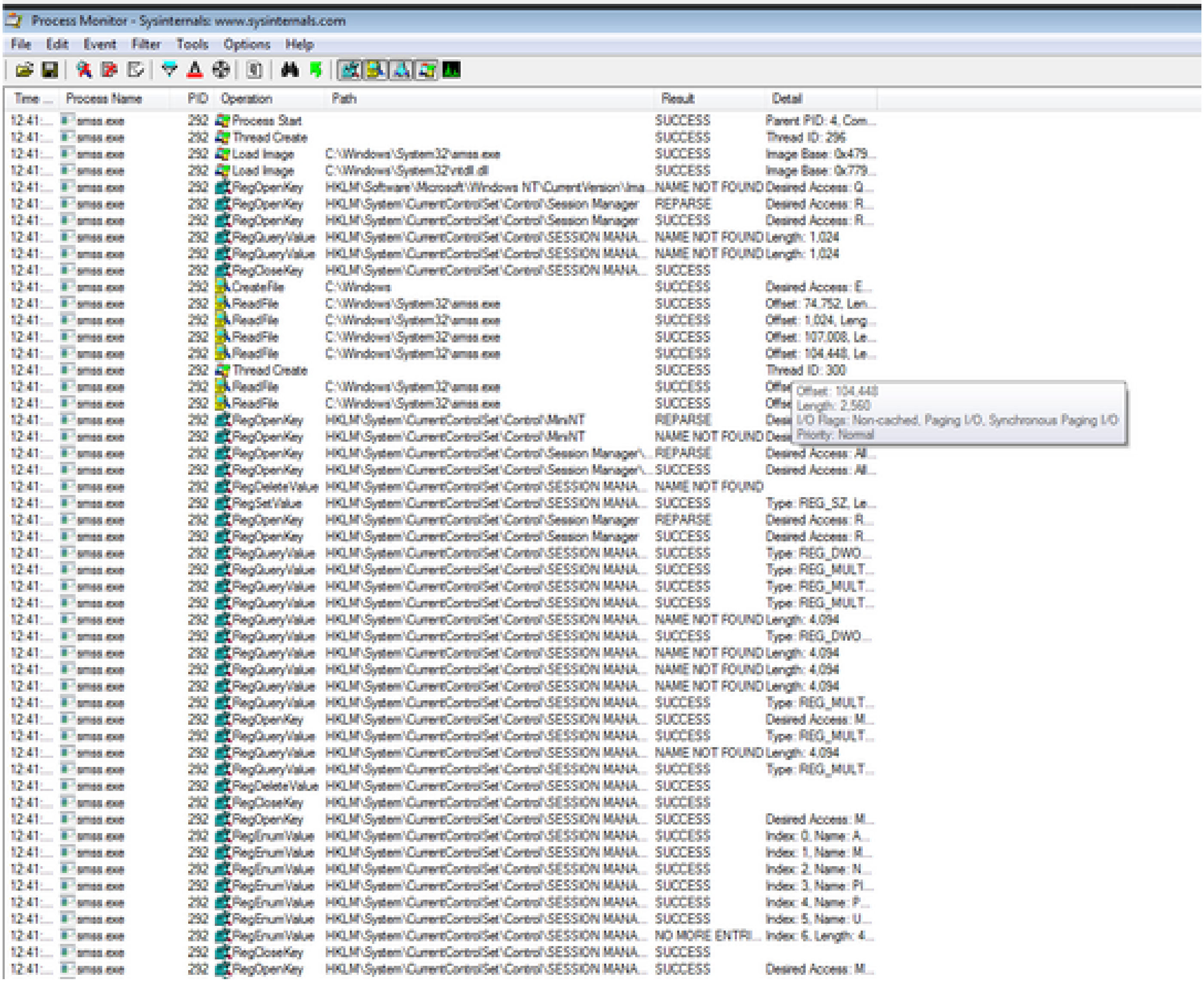




Process Monitor

A log of boot-time activity was created by a previous instance of Process Monitor. Do you wish to save the collected data now?


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Converting boot time event data
[illegible]
Cancel


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	Offse
12:41:...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offse
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...	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...

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