시작 시 AMP 문제를 해결하기 위해 ProcMon 로그를 수집하는 방법

목차

소개

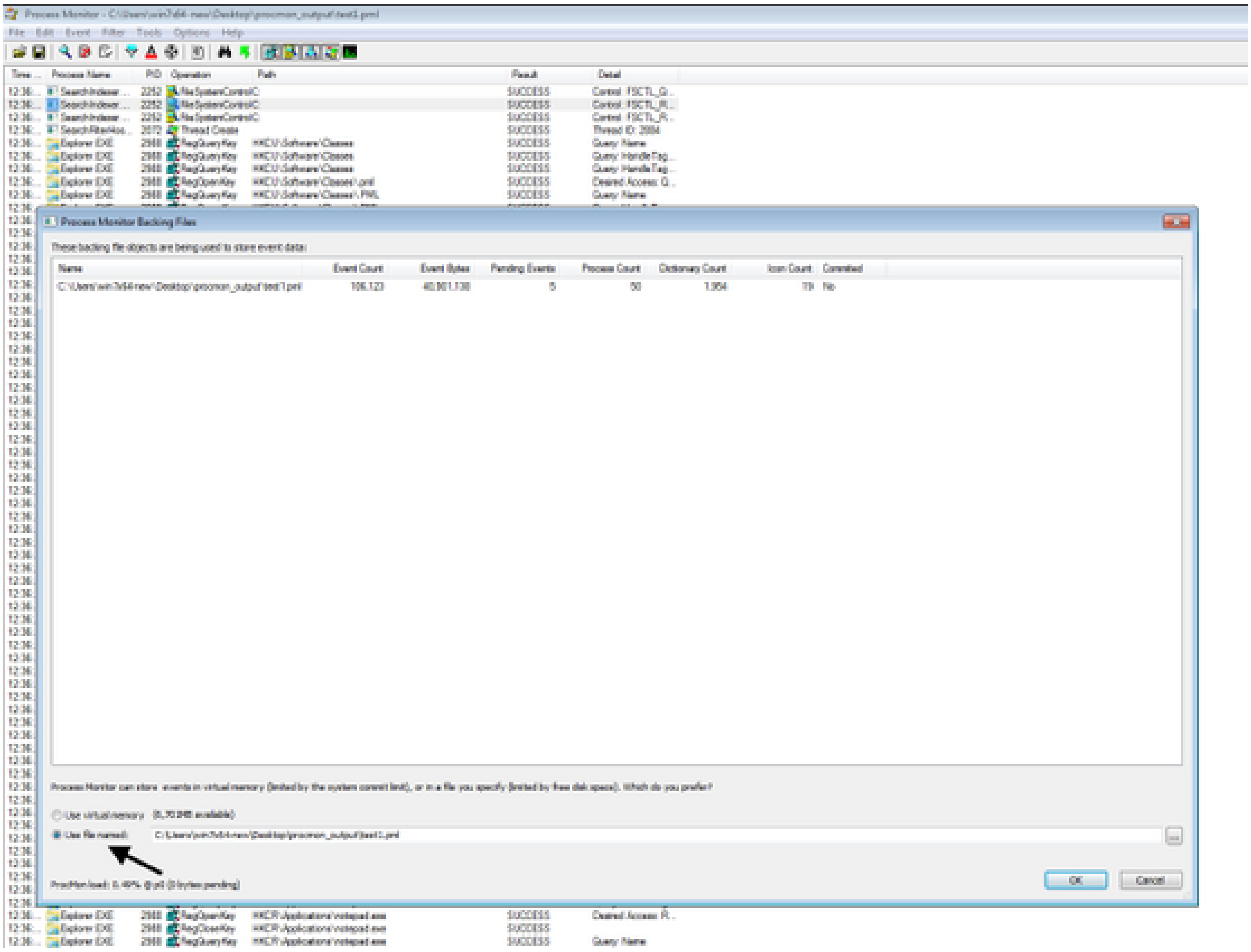
시스템 관리자는 프로세스 모니터(procmon.exe)를 사용하여 컴퓨터 시작 프로세스 중에 FireAMP 커넥터 환경이 중단되는지 여부를 확인하는 자세한 로그를 얻을 수 있습니다.이러한 로그는 Cisco TAC에서 이러한 문제를 해결하기 위해 요청합니다.Process Monitor는 여기에서 도움이 되는 무료 유틸리티입니다.이 파일은 https://docs.microsoft.com/en-us/sysinternals/downloads/procmon에서 무료로 다운로드할 수 있습니다.

이 문서에서는 시스템 부팅 프로세스 중에 문제가 발생할 경우(부팅 시 BSOD를 생성하는 중임) ProcMon 로그 및 메모리 덤프를 수집하는 방법에 대해 설명합니다. 이러한 로그는 부팅 중에 발생하는 시스템 이벤트를 캡처하는 데 필요합니다.

절차:

1. 문제가 쉽게 재현될 수 있도록 시험장치를 설정하는 방법

2. 관리자로 ProcMon 도구를 다운로드하여 실행합니다.File(**파일) -> Process Monitor Backing Files(프로세스 모니터 백업 파일)**로 이동하고 **경로**를 선택합니다.



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

Time ...	Process Name	PID	Operation	Path	Result	Detail
12:36:...	SearchIndexer ...	2252	FileSystemControlC:		SUCCESS	Control: FSCTL_Q...
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	40,901,130	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?

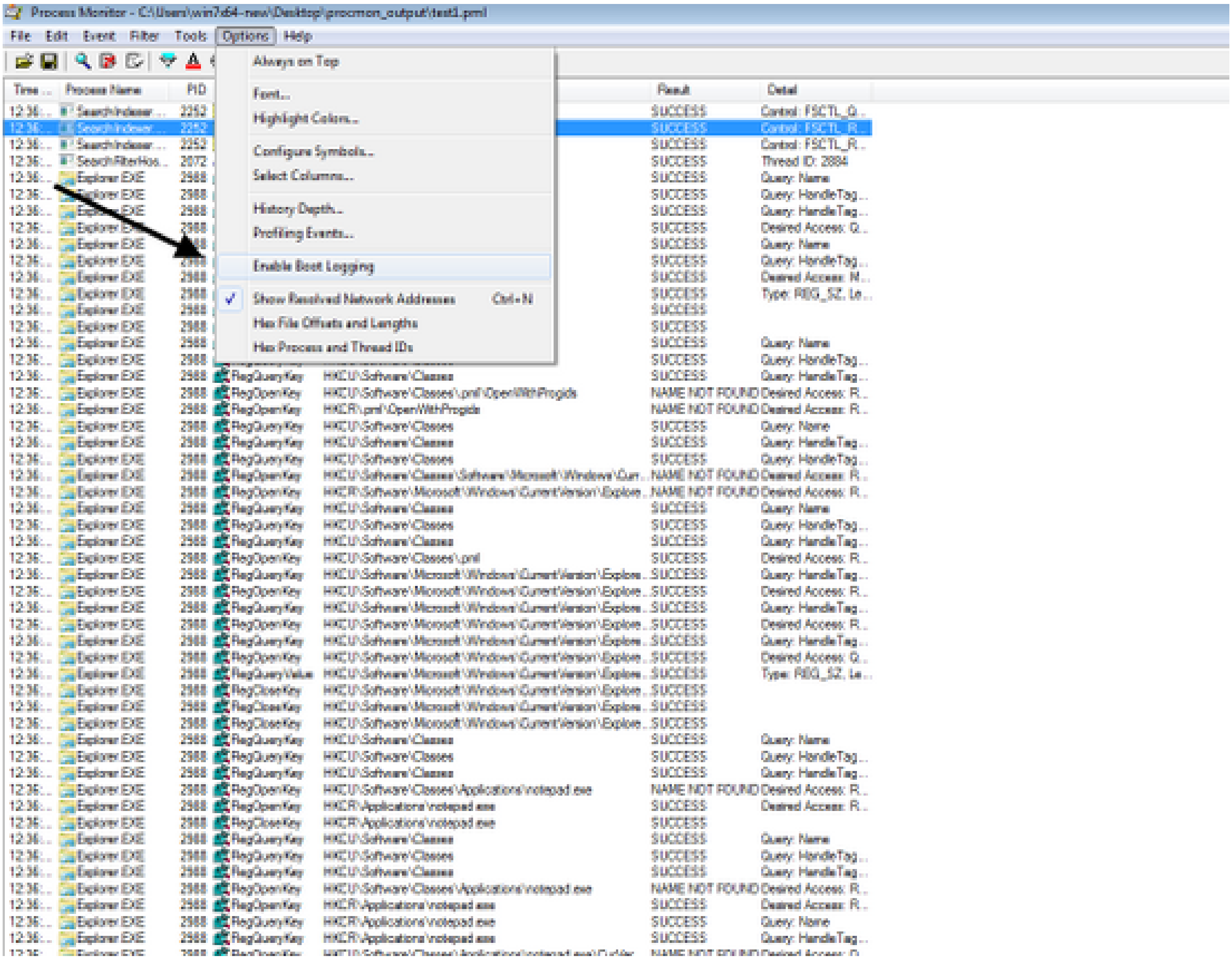
○ Use virtual memory (6,70 [illegible] available)

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

ProcMon load: 0.40% @ [illegible] (0 bytes pending)

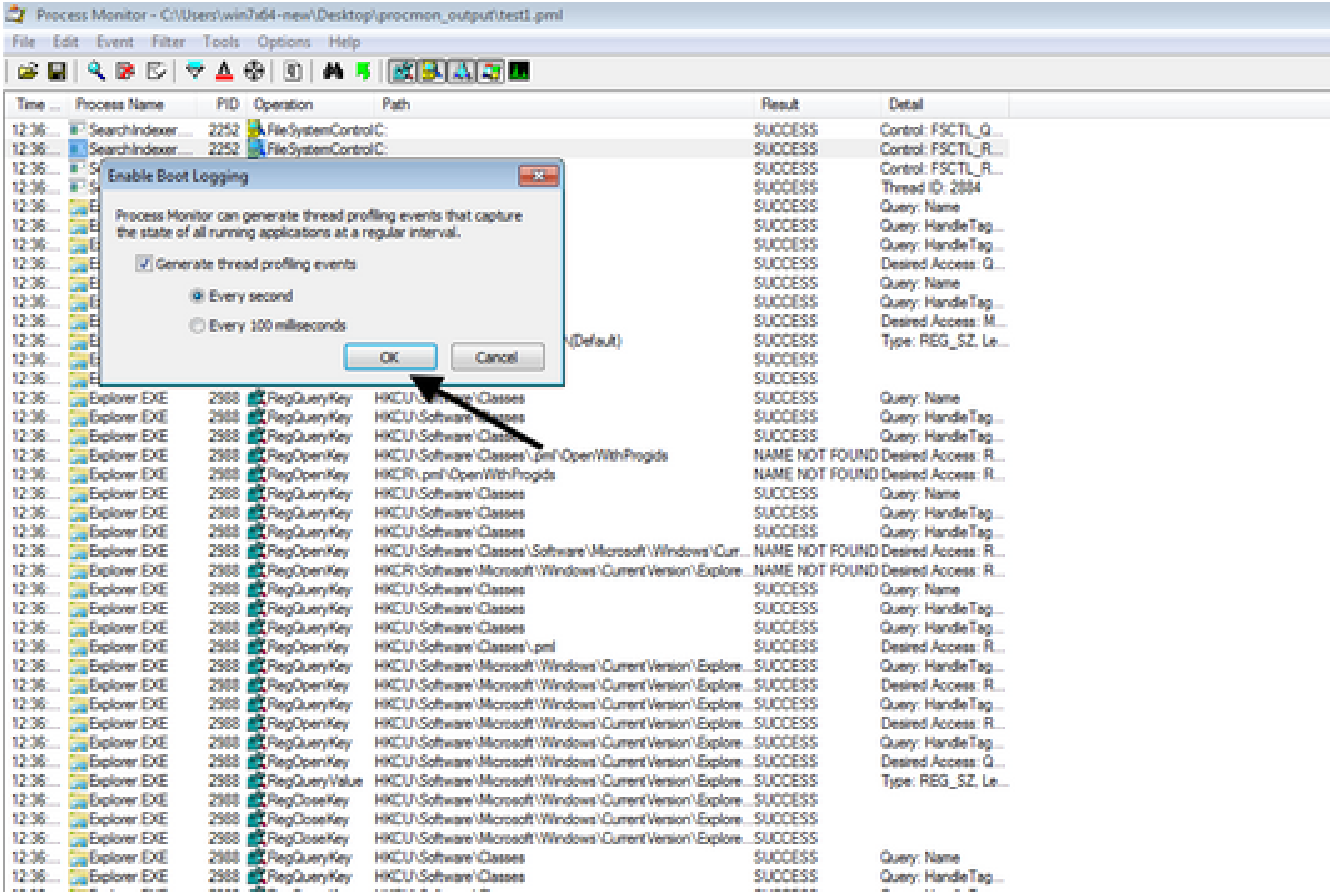
Time ...	Process Name	PID	Operation	Path	Result	Detail
12:36:...	Explorer.EXE	2988	RegOpenKey	HKCR\Applications\notepad.exe	SUCCESS	Desired Access: R...
12:36:...	Explorer.EXE	2988	RegCloseKey	HKCR\Applications\notepad.exe	SUCCESS	
12:36:...	Explorer.EXE	2988	RegQueryKey	HKCR\Applications\notepad.exe	SUCCESS	Query: Name

3. Process Tool에서 Options(옵션) **-> Enable Boot Logging(부팅 로깅 활성화)으로** 이동합니다.


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...
12:36:... Explorer.EXE        2988  RegOpenKey     HKCU\Software\Classes\Applications\notepad.exe\CurVer NAME NOT FOUND Desired Access: R...
```

4. Generate threat profiling events(**위협 프로파일링 이벤트 생성)** 및 **Every second를 선택합니다.**



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

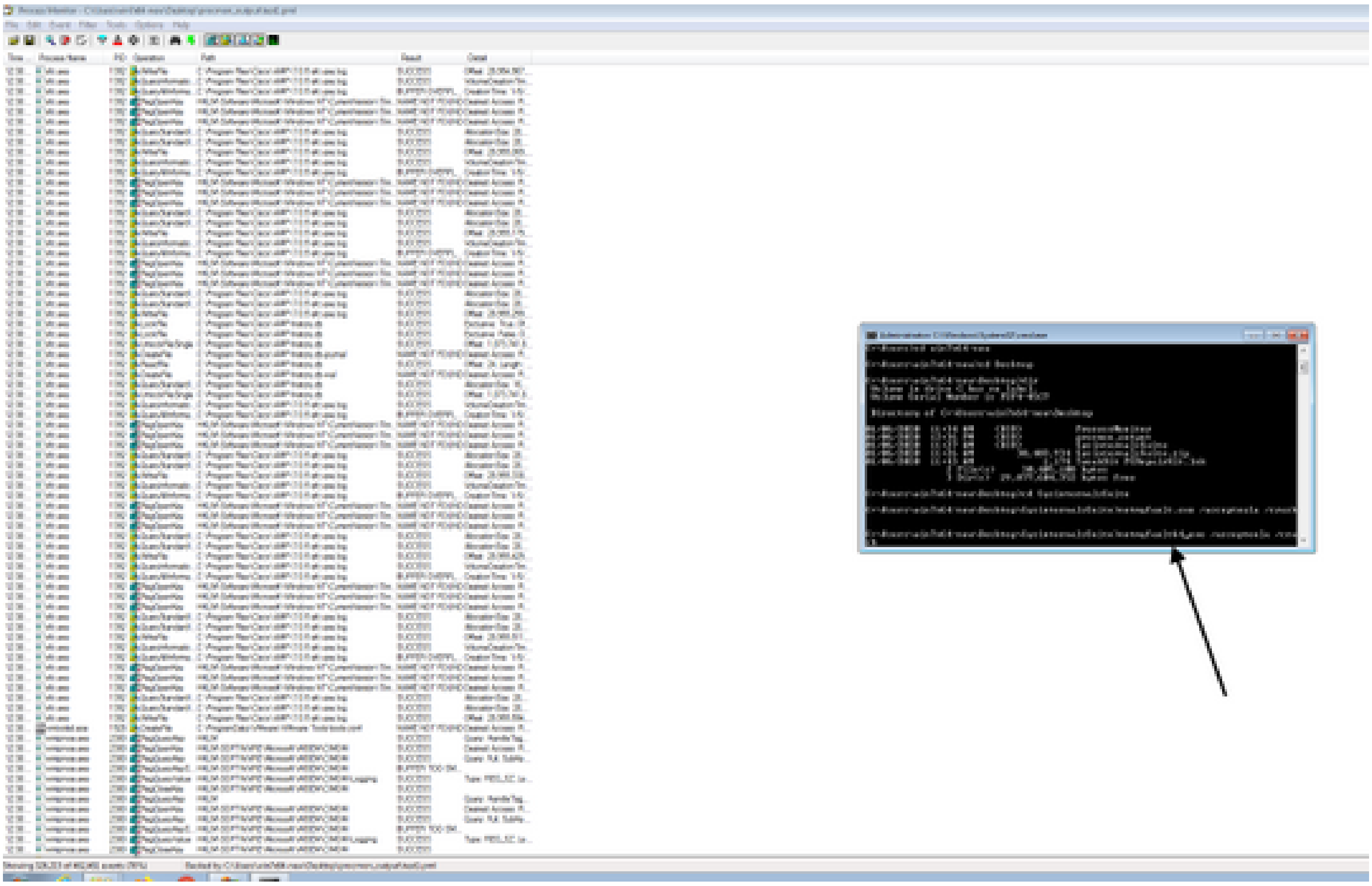
○ Every 100 milliseconds

```
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. 프로세스에서 모든 관련 필터를 선택하고 데이터를 수집해야 합니다.

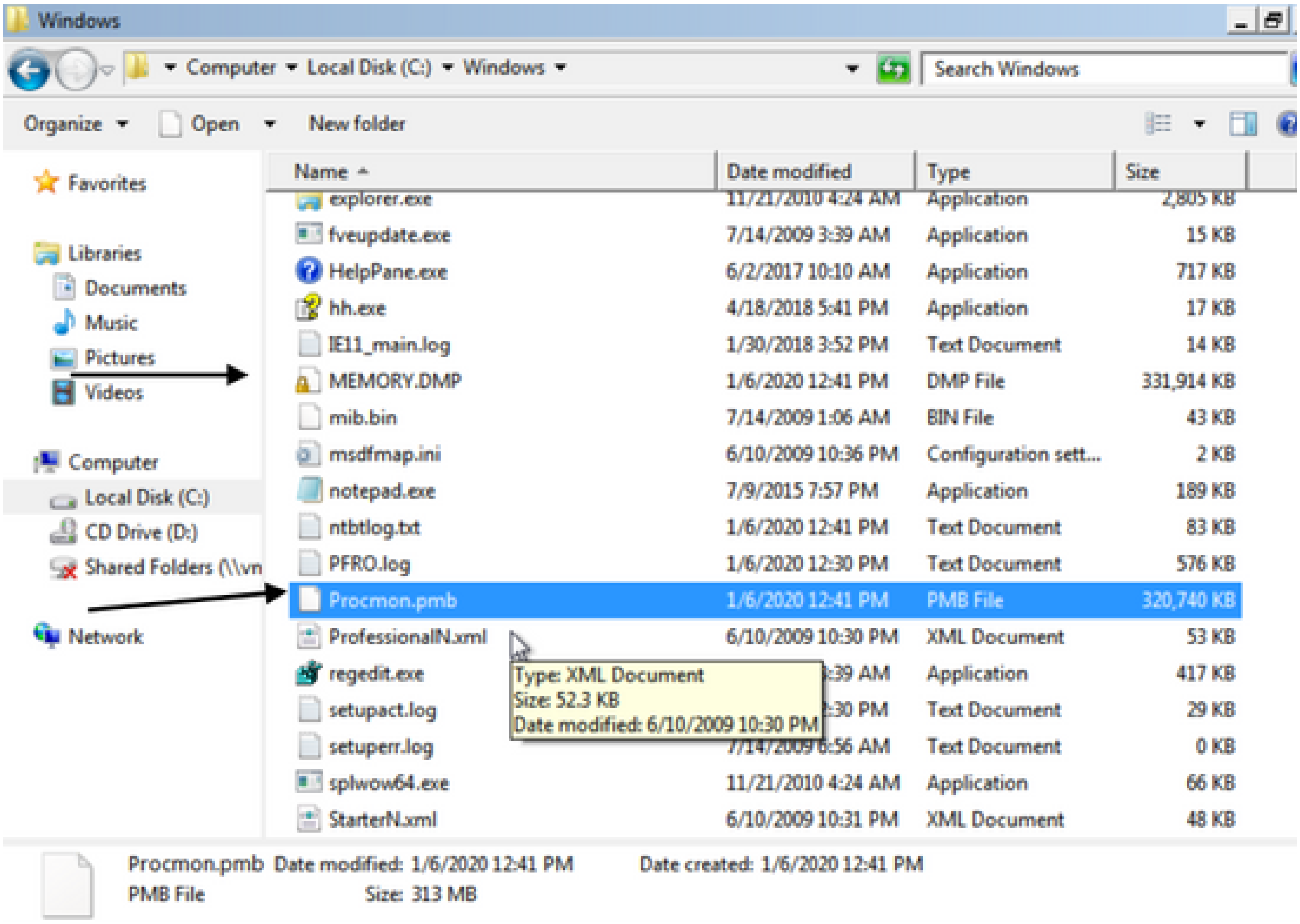
6. 충돌을 복제할 수 없는 경우 NotMyFault64.exe 유틸리티를 사용하여 충돌 Windows를 강제로 실행할 수 있습니다. https://live.sysinternals.com/files/

실행 방법에 대한 지침은 다음과 같습니다. https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump



7. 기계를 망가뜨리는 행위

8. 시스템을 안전 모드로 부팅하고 Procmon**.pmb** 및 **MEMORY.DMP를** 수동으로 수집합니다. 두 파일은 모두 C:\Windows folder에 있습니다.이러한 파일은 Cisco TAC와 공유됩니다.

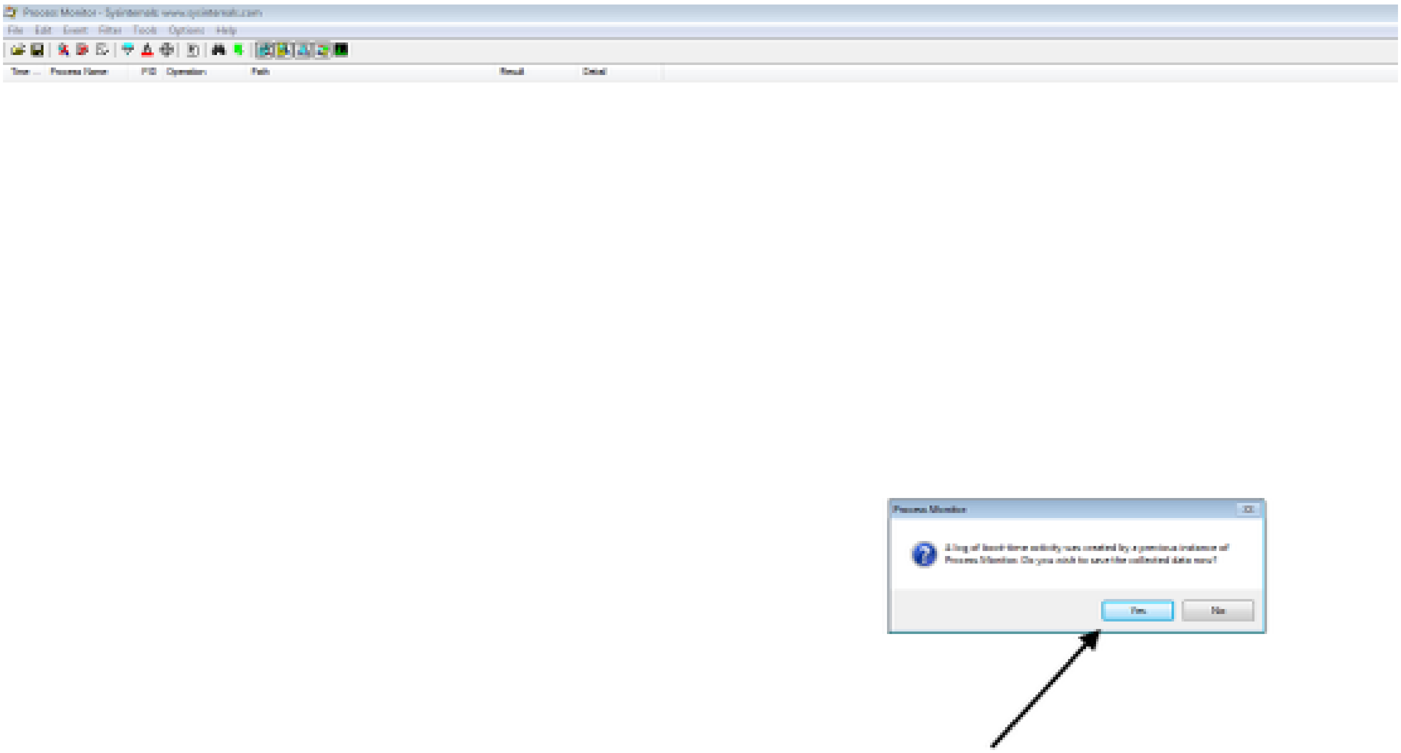


Name	Date modified	Type	Size
explorer.exe	11/21/2010 4:24 AM	Application	2,805 KB
fveupdate.exe	7/14/2009 3:39 AM	Application	15 KB
HelpPane.exe	6/2/2017 10:10 AM	Application	717 KB
hh.exe	4/18/2018 5:41 PM	Application	17 KB
IE11_main.log	1/30/2018 3:52 PM	Text Document	14 KB
MEMORY.DMP	1/6/2020 12:41 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

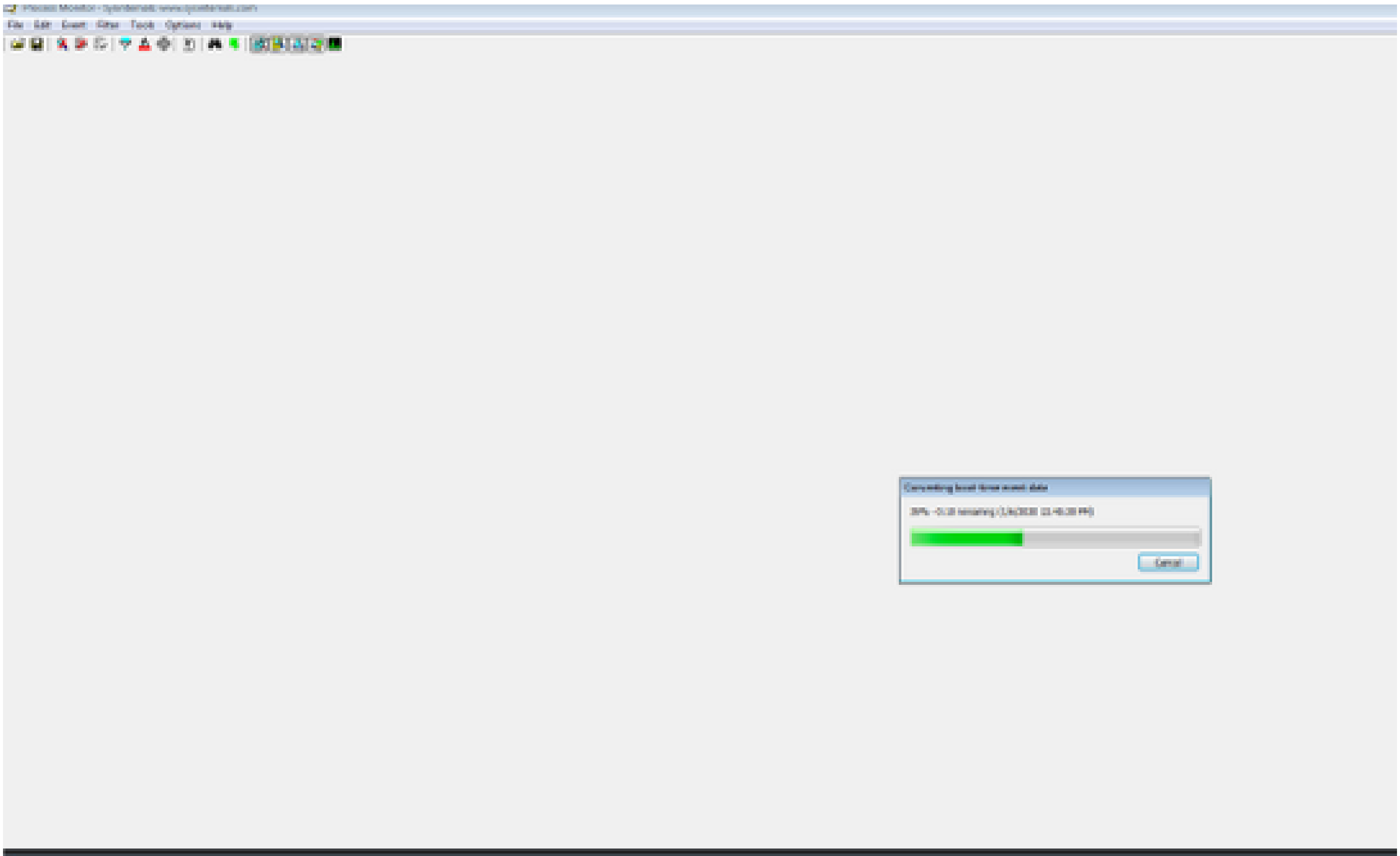
Procmon.pmb Date modified: 1/6/2020 12:41 PM Date created: 1/6/2020 12:41 PM
PMB File Size: 313 MB

7. 선택적으로, C:\Windows folder폴더에 PMB 파일이 생성된 경우 "일반 모드"로 부팅할 수 있는 경우 ProcMon을 다시 시작하면 다음 로그가 표시됩니다.여기에서 Save(저장) 버튼을 클릭하여 이벤트를 다시 저장할 수 있습니다.



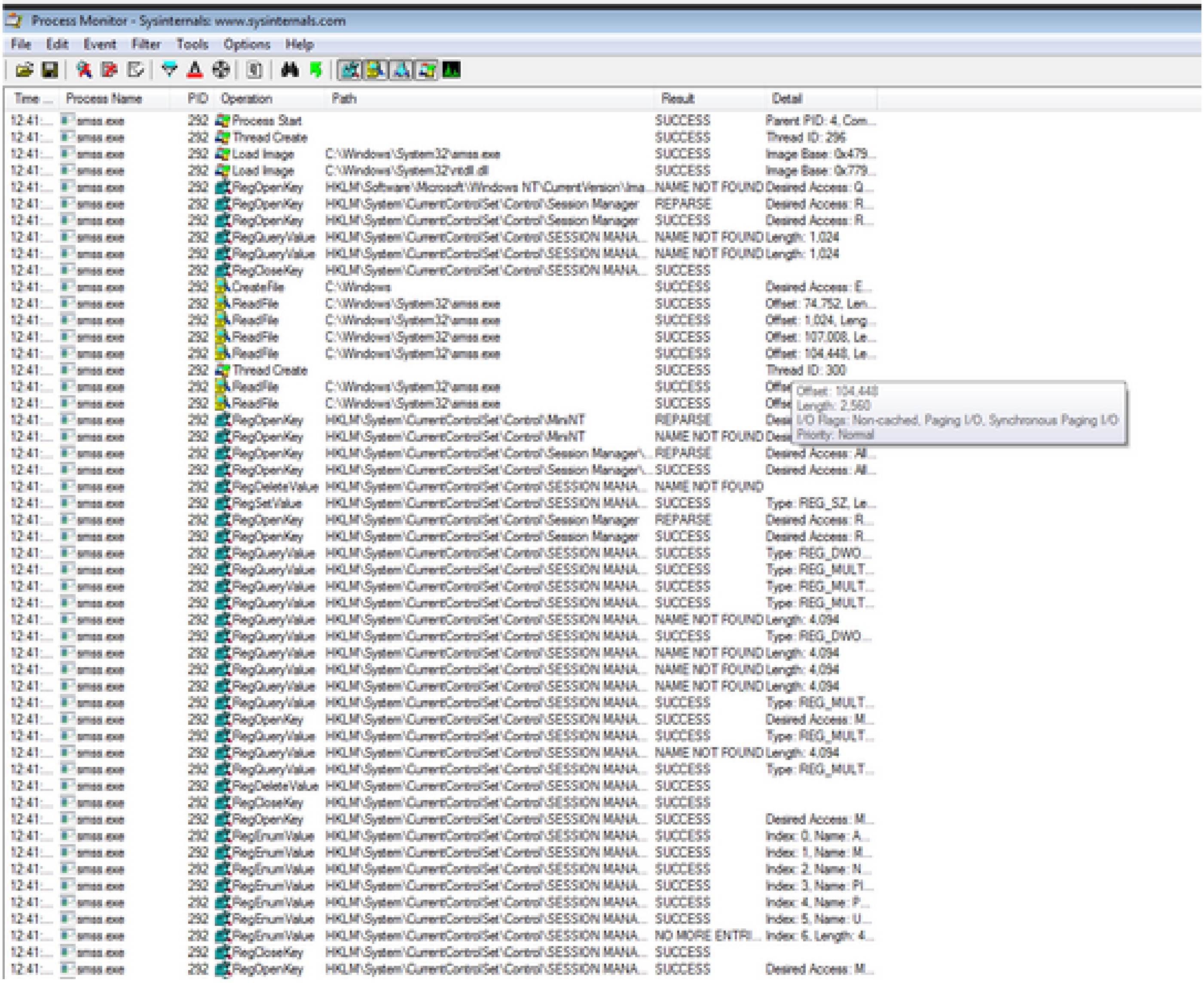
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
Process Monitor
Yes
No

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



Converting boot-time event data

[illegible]



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