Cómo recopilar registros de ProcMon para resolver problemas de AMP al inicio

Contenido

Introducción

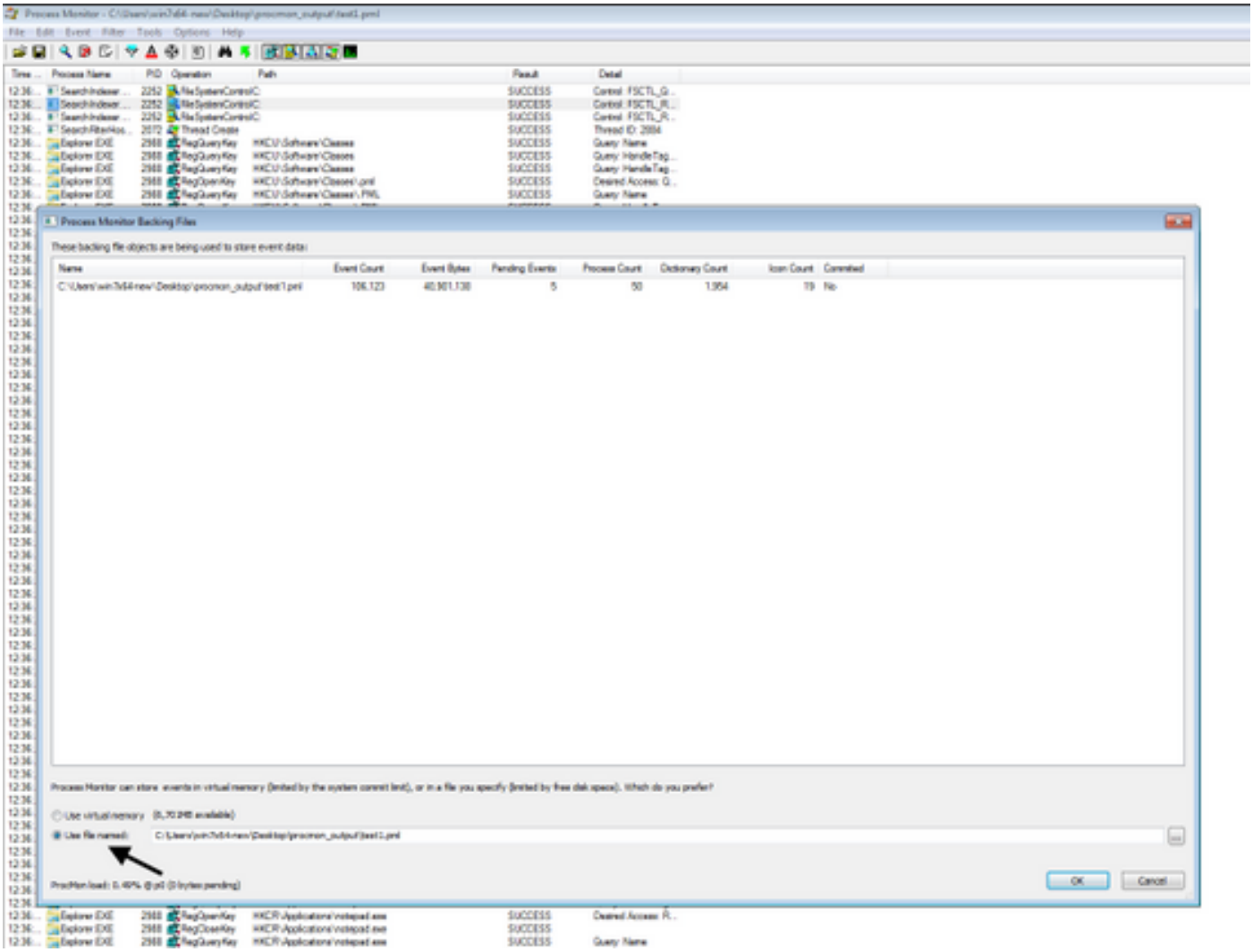
Como administrador del sistema, es posible que desee obtener registros detallados mediante el Monitor de procesos (procmon.exe) para determinar si el conector de FireAMP se bloquea durante el proceso de inicio del equipo. El TAC de Cisco también solicitará estos registros para resolver tales problemas. Process Monitor es una utilidad gratuita que puede ayudarnos aquí. Esto se puede descargar libremente desde https://docs.microsoft.com/en-us/sysinternals/downloads/procmon

Este documento describe los pasos sobre cómo recopilar registros ProcMon y vaciado de memoria si el problema ocurre durante un proceso de arranque del sistema (lo que significa que está generando BSODs en el arranque). Estos registros son necesarios para capturar los eventos del sistema que tienen lugar durante el arranque.

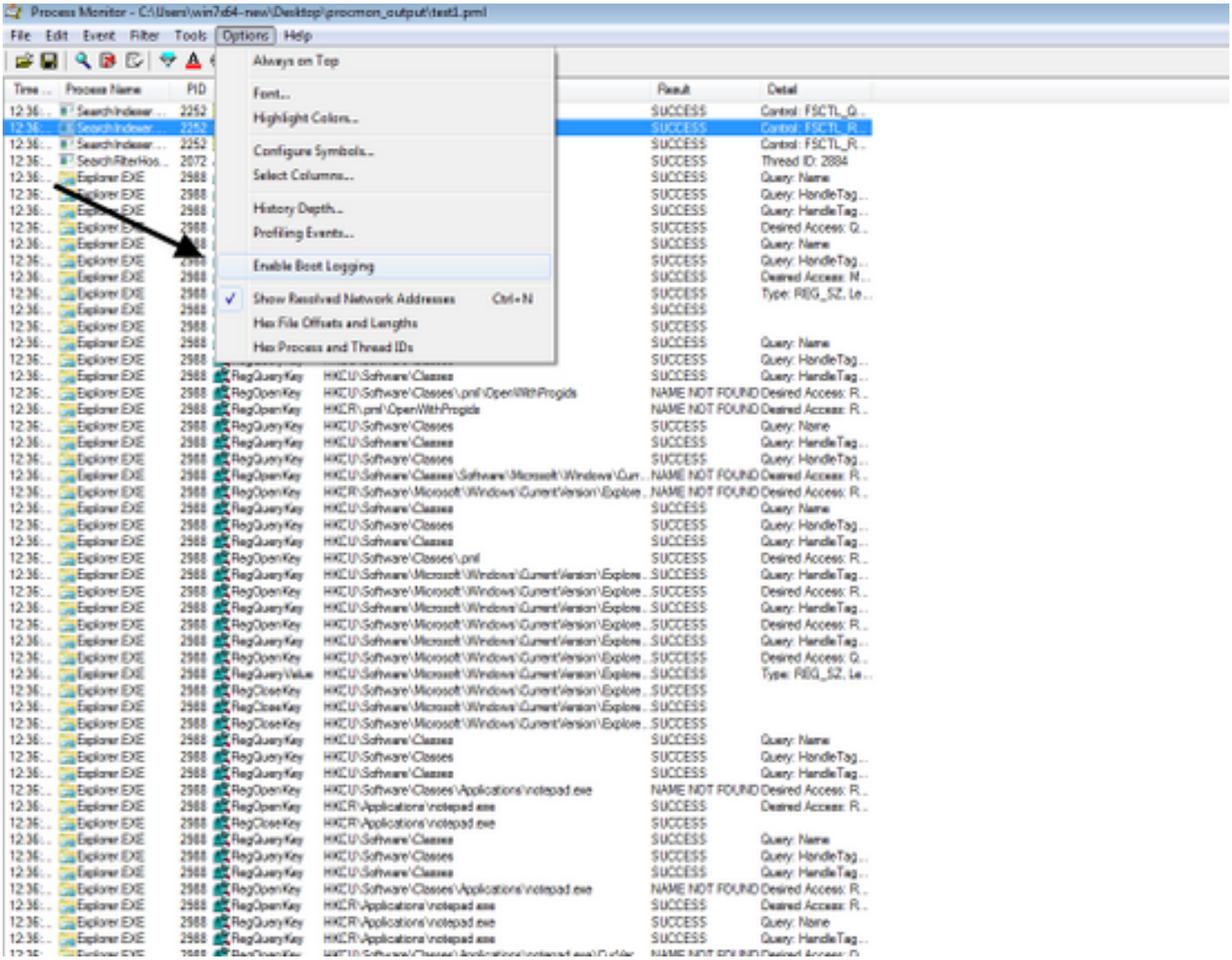
Procedimiento:

1. Configure las máquinas de ensayo de tal manera que el problema pueda reproducirse fácilmente.

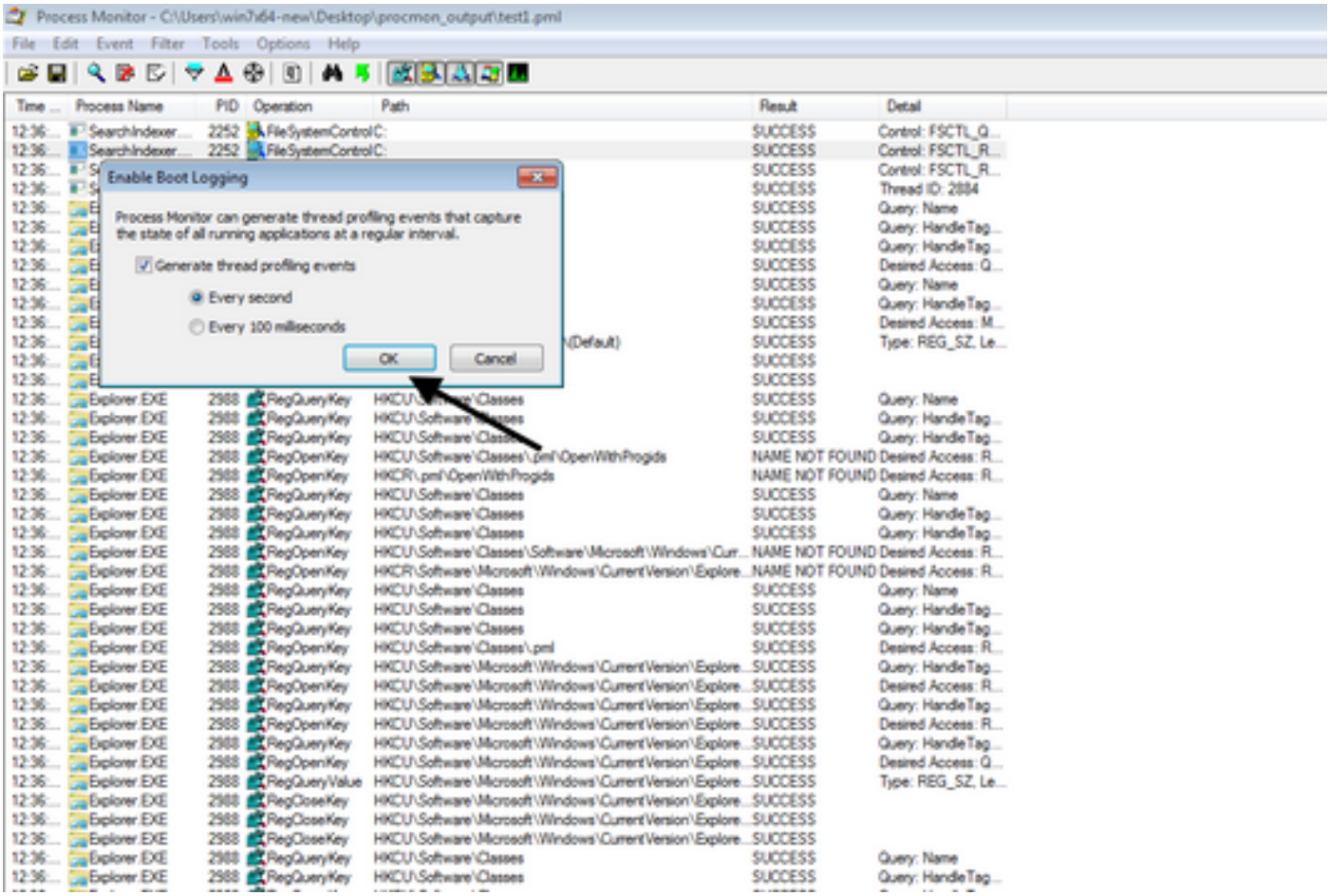
2. Descargue y ejecute la herramienta ProcMon como administrador. Vaya a **File -> Process Monitor Backing Files** y seleccione una **Path**.



3. En Procmon Tool, vaya a **Options -> Enable Boot Logging**.



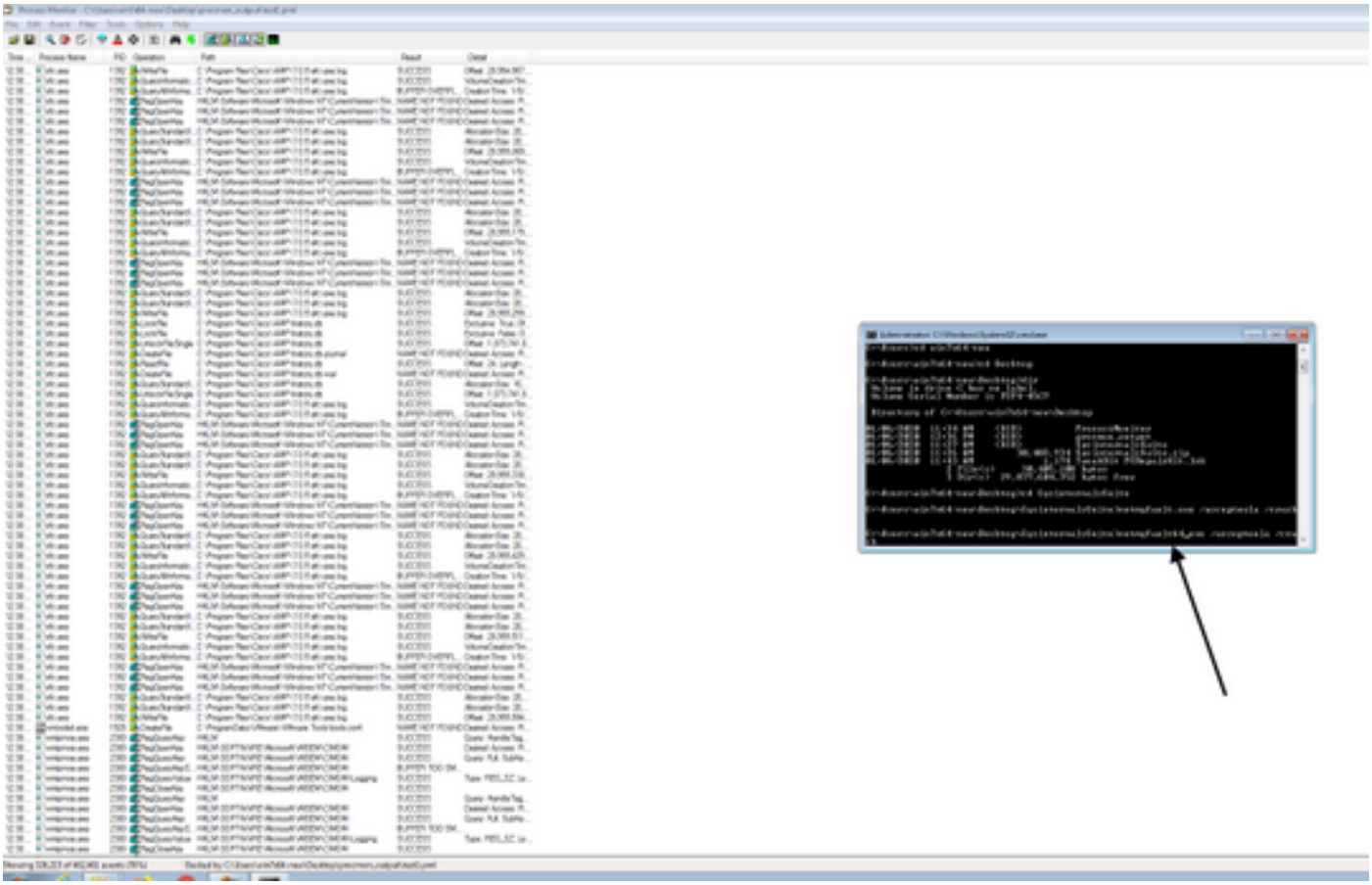
4. Seleccione **Generar eventos de perfiles de amenazas** y **Cada segundo.**



5. Asegúrese de que todos los filtros relevantes estén seleccionados en Procmon y que se estén recopilando datos.

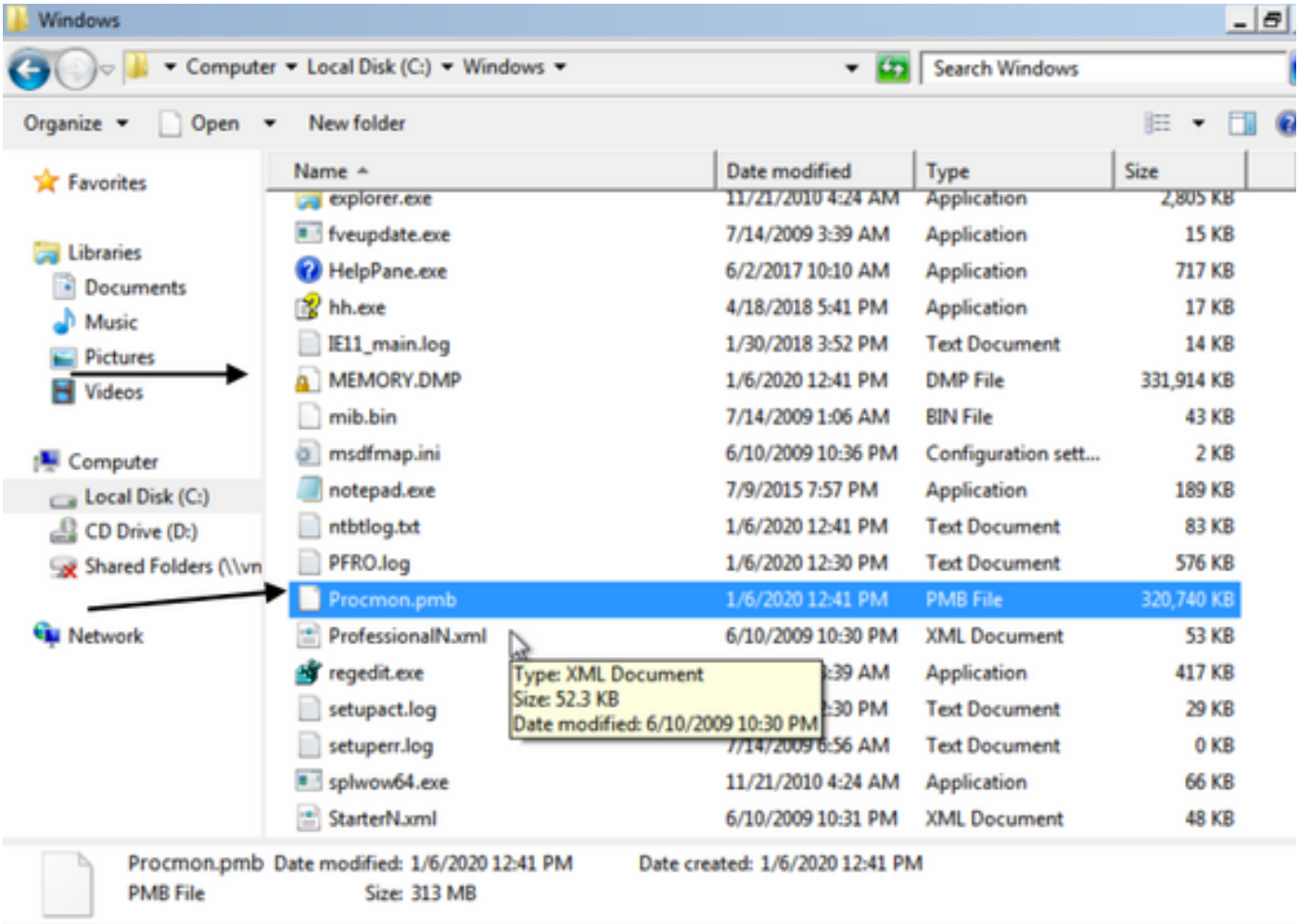
6. Si no puede replicar el desperfecto, puede forzar el desperfecto de Windows utilizando la utilidad NotMyFault64.exe que puede obtener de https://live.sysinternals.com/files/

Las instrucciones sobre cómo ejecutarlas aquí: https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump

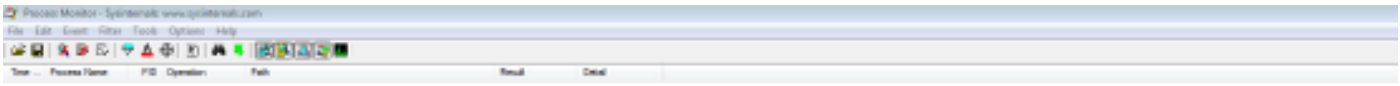


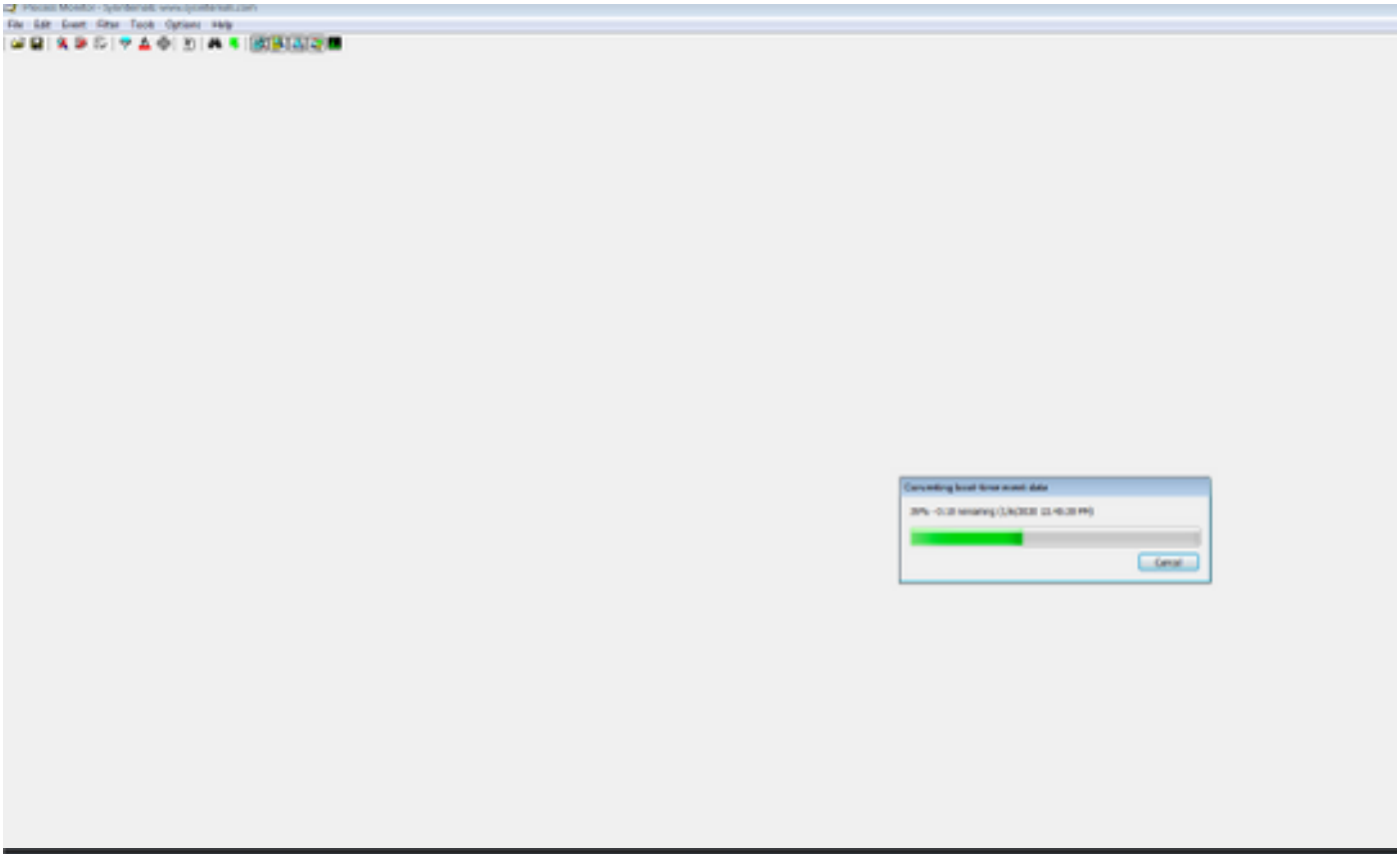
7. Acelere la máquina.

8. Inicie la máquina en el modo seguro y recopile manualmente **Procmon.pmb** y **MEMORY.DMP**, ambos archivos están en C:\Windows folder. Estos archivos se compartirán con Cisco TAC.



7. Opcionalmente, si puede arrancarlo en "modo normal" si los archivos PMB se generan en el C:\Windows folder, entonces si inicia ProcMon de nuevo, verá los siguientes registros. En este caso, puede volver a guardar los eventos haciendo clic en el botón Guardar.





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...