

# Using Process Monitor

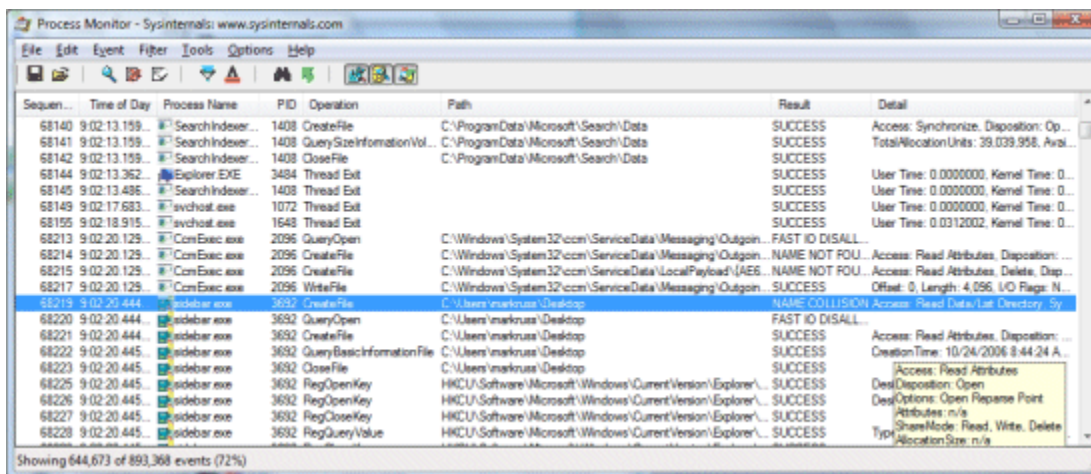
## Process Monitor Tutorial

This information was adapted from the help file for the program.

Process Monitor is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Process Monitor runs on Windows 2000 SP4 with Update Rollup 1, Windows XP SP2, Windows Server 2003 SP1, and Windows Vista as well as x64 versions of Windows XP, Windows Server 2003 and Windows Vista.

## Using Process Monitor



The screenshot shows the Process Monitor application window with a table of events. The table has columns for Sequence Number, Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The events listed include file system operations like CreateFile, QuerySizeInformation, CloseFile, and WriteFile, as well as registry operations like RegOpenKey, RegCloseKey, and RegQueryValue. The status bar at the bottom indicates 'Showing 644,673 of 893,368 events (72%)'.

Sequen...	Time of Day	Process Name	PID	Operation	Path	Result	Detail
68140	9:02:13.159	SearchIndexer...	1408	CreateFile	C:\ProgramData\Microsoft\Search\Dat...	SUCCESS	Access: Synchronize. Disposition: Op...
68141	9:02:13.159	SearchIndexer...	1408	QuerySizeInformationVol...	C:\ProgramData\Microsoft\Search\Dat...	SUCCESS	TotalAllocationUnits: 39,039,956, Avail...
68142	9:02:13.159	SearchIndexer...	1408	CloseFile	C:\ProgramData\Microsoft\Search\Dat...	SUCCESS	
68144	9:02:13.362	Explorer.EXE	3484	Thread Exit		SUCCESS	User Time: 0.0000000, Kernel Time: 0...
68145	9:02:13.496	SearchIndexer...	1408	Thread Exit		SUCCESS	User Time: 0.0000000, Kernel Time: 0...
68149	9:02:17.683	svchost.exe	1072	Thread Exit		SUCCESS	User Time: 0.0000000, Kernel Time: 0...
68155	9:02:18.915	svchost.exe	1548	Thread Exit		SUCCESS	User Time: 0.0312002, Kernel Time: 0...
68213	9:02:20.125	ConExec.exe	2096	QueryOpen	C:\Windows\System32\ccm\ServiceData\Messaging\Outgoin...	FAST IO DISALL...	
68214	9:02:20.125	ConExec.exe	2096	CreateFile	C:\Windows\System32\ccm\ServiceData\Messaging\Outgoin...	NAME NOT FOU...	Access: Read Attributes. Disposition: ...
68215	9:02:20.125	ConExec.exe	2096	CreateFile	C:\Windows\System32\ccm\ServiceData\LocalPayload\AEG...	NAME NOT FOU...	Access: Read Attributes. Delete, Disp...
68217	9:02:20.125	ConExec.exe	2096	WriteFile	C:\Windows\System32\ccm\ServiceData\Messaging\Outgoin...	SUCCESS	Offset: 0, Length: 4,096, I/O Flags: N...
68219	9:02:20.444	sidebar.exe	3692	CreateFile	C:\User\markrus\Desktop	NAME COLLISION	Access: Read Data/List Directory, Sy...
68220	9:02:20.444	sidebar.exe	3692	QueryOpen	C:\User\markrus\Desktop	FAST IO DISALL...	
68221	9:02:20.444	sidebar.exe	3692	CreateFile	C:\User\markrus\Desktop	SUCCESS	Access: Read Attributes. Disposition: ...
68222	9:02:20.445	sidebar.exe	3692	QueryBasicInformationFile	C:\User\markrus\Desktop	SUCCESS	CreationTime: 10/24/2006 8:44:24 A...
68223	9:02:20.445	sidebar.exe	3692	CloseFile	C:\User\markrus\Desktop	SUCCESS	Access: Read Attributes
68225	9:02:20.445	sidebar.exe	3692	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explor...	SUCCESS	DesiDisposition: Open
68226	9:02:20.445	sidebar.exe	3692	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explor...	SUCCESS	DesiOptions: Open Reparse Point
68227	9:02:20.445	sidebar.exe	3692	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explor...	SUCCESS	Attributes: n/a
68228	9:02:20.445	sidebar.exe	3692	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explor...	SUCCESS	ShareMode: Read, Write, Delete Type: AllocationSize: n/a

Executing Process Monitor requires local Administrative group membership. When you launch Process Monitor it immediately starts monitoring three classes of operation: file system, Registry and process.

- **File System**

Process Monitor displays file system activity for all Windows file systems, including local storage and remote file systems. Process Monitor automatically detects the arrival of new file system devices and monitors them. All file system paths are displayed relative to the user session in which a file system operation executes. For example, if user A has

mounted a share as drive letter Z:, any accesses they make to that share will display in Process Monitor as being relative to drive Z:.

To remove file system operations from the display de-select the file system push-button in the Process Monitor toolbar and to add back file system operations depress the button.

- **Registry**

Process Monitor logs all Registry operations and displays Registry paths using conventional abbreviations for Registry root keys (e.g. HKEY\_LOCAL\_MACHINE is represented as HKLM).

To remove Registry operations from the display de-select the Registry push-button in the Process Monitor toolbar and to add back Registry operations depress the button.

- **Process**

In its process/thread monitoring subsystem Process Monitor tracks all process and thread creation and exit operations as well as DLL and device driver load operations.

To remove Process operations from the display de-select the process push-button in the Process Monitor toolbar and to add back process operations depress the button.

- **Network**

Process Monitor uses Event Tracing for Windows (ETW) to trace and record TCP and UDP activity. Each network operation includes the source and destination addresses, as well as the amount of data sent or received, but does not include the actual data.

To remove Network operations from the display de-select the network push-button in the Process Monitor toolbar and to add back network operations depress the button.

- **Profiling**

This event class can be enabled from the Options menu. When active, Process Monitor scans all the active threads in the system and generates a profiling even for each one that records the kernel and user CPU time consumed, as well as the number of context switches executed, by the thread since its previous profiling event. *Note: the System process is not included in profiling.*

There are a number of basic options that control basic Process Monitor operation:

**Capture:** Use the Capture Events menu item in the File menu, capture toolbar button or Ctrl+E hotkey to toggle Process Monitor's monitoring.

Autoscroll: Select Autoscroll entry in the Edit menu, the autoscroll toolbar button or Ctrl+A hotkey to toggle Process Monitor's autoscroll behavior, which causes it to ensure that the most recent operation is visible in the display.

Clear: To clear the display of all items choose Clear Display from the Edit menu or use the Ctrl+X hotkey.

## Column Selection

You can drag columns to rearrange their order and customized the columns displayed by choosing Select Columns from the Options menu to open the column selection dialog. Columns that are available for selection include:

### *Application Details*

- Process Name The name of the process in which an event occurred.
- Image Path The full path of the image running in a process.
- Command Line The command line used to launch a process.
- Company Name The text of the company name version string embedded in a process image file. This text is optionally defined by the application developer.
- Description The text of the product description string embedded in a process image file. This text is optionally defined by the application developer.
- Version The product version number embedded in a process image file. This information is optionally specified by the application developer.

### *Event Details*

- Sequence Number The unique number Process Monitor assigns to an individual event.
- Event Class The class (File, Registry, Process) of the event.
- Operation The specific event operation (e.g. Read, RegQueryValue, etc.).
- Date & Time Both the date and the time of an operation.
- Time of Day Only the time of an operation.
- Path The path of the resource that an event references.
- Detail Additional information specific to an event.
- Result The status code of a completed operation.
- Relative Time The time of the operation relative to Process Monitor's start time or the last time that the Process Monitor display was cleared.
- Duration The duration of an operation that has completed.

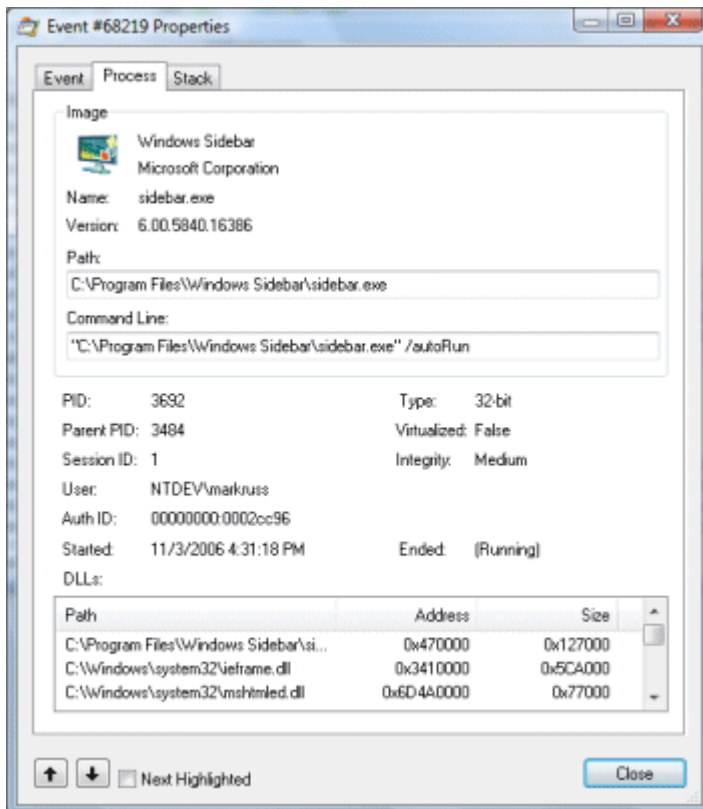
### *Process Management*

- User Name The name of the user account in which the process that performed an operation is executing.

- Session ID The Windows session in which the process that executed an operation is executing.
- Authentication ID The logon session in which the process that executed an operation is executing.
- Process ID The Process ID (PID) of the process that executed an operation.
- Thread ID The Thread ID (TID) of the thread that executed an operation.
- Integrity Level The integrity level at which the process that executed an operation is running (Windows Vista only).
- Virtualized The virtualization status of the process that executed an operation (Windows Vista only).

## Event Properties

You can access the properties for an individual event by double-clicking on the event, or by selecting the Properties menu item from the Event menu or the context menu when you right-click on an event. The Event Properties dialog consists of the Event, Process and Stack pages. You can move to the next or preceding displayed or highlighted event with the arrow buttons at the bottom of the Event Properties dialog.



## *Event*

The Event page displays information specific to an event, including its sequence number, issuing thread, event class and operation, result, timestamp, and if applicable, resource path. Only file system and Registry events define resource paths. The lower area of the Event page lists details collected for an event that are dependent on the event operation. The details are the same as shown for an event in the Detail column of the main display, but each detail is shown on a separate line.

## *Process*

An event's Process page shows information about the process that executed an event. Along with the data associated with a process' image, such as the path and version strings, the Process page shows process execution attributes like the process ID, user account in which the process is executing, and if the event was generated on a 64-bit Windows system, whether the process is 32-bit or 64-bit. For processes executing on Windows Vista systems, Process Monitor shows the integrity level of the process and whether or not it's virtualized.

The bottom area of the process page displays the list of images loaded, and the addresses at which they are loaded, in the process at the time the event executed. Double-click on an image in the list to view more information about the image, including its version information.

## *Stack*

The Stack page shows the thread stack of the thread when the event was recorded. The stack can be useful for determining the reason an event took place and the component responsible for the event. Kernel-mode frames of a stack are designated with the letter 'K' on the left of the frame and user-mode stacks (only available only on 32-bit systems prior to Vista SP1/Windows Server 2008) with the letter 'U'. If Process Monitor is able to locate symbols for images referenced in the trace it will attempt to resolve addresses to the functions in which they reside. Symbols resolution can take time if symbols must be retrieved from the network, for example from the Microsoft symbol server. Use the Symbol Configuration dialog, which you access from the [Options](#) menu, to configure symbols.

If you specify a path to source files in the Symbol Configuration dialog, the Stack dialog's Source button will enable for any frame for which line-number symbols information is available and the source file is present in the paths you include. Clicking on the Source button opens a text viewer that highlights the source code line referenced.

To view more information about an image listed in the stack trace either double-click on the frame or select the frame and press the Properties button below the stack trace area. Select the Stack menu entry from the Event menu to open the Event Properties dialog directly to the Stack page.

## Filtering and Highlighting

Process Monitor offers several ways to configure filters or highlighting.

### *Include and Exclude Filters*

You can specify event attributes such that Process Monitor will only display or exclude events with matching attribute values. All filters are non-destructive, meaning that they affect only which events Process Monitor displays, not the underlying event data.

When an event is selected the Include and Exclude sub-menus in the Event menu allows you to easily add one of the event's attributes to the configured Include or Exclude filters. For example, to only show events executed by a particular process name choose the Process Name entry from the Include submenu. You can also select multiple events and simultaneously configure an attribute filter for all of the unique values contained in the selected events.

Process Monitor ORs together all the filters that are related to a particular attribute type and ANDs together filters of different attribute types. For example, if you specified process name include filters for Notepad.exe and Cmd.exe and a path include filter for C:\Windows, Process Monitor would only display events originating in either Notepad.exe or Cmd.exe that specify the C:\Windows directory.

More complex filtering options are available in the Filter dialog, which you open by selecting Filter from the Tools menu or by clicking on the Filter toolbar button. A filter entry consists of an attribute field (e.g. Authentication ID, Process Name, etc.), a comparison operation, an attribute value, and a filter type of either Include or Exclude. For convenience, Process Monitor will automatically populate the attribute value drop-down with values that are present in the loaded trace data, but you can enter arbitrary values.

### *Filter Context Menu*

If you right-click on an item in the display Process Monitor displays a context menu that let's you view the item's properties or configure a filter based on the item's attributes. Further, quick-filter entries are added to the menu for the value of the column on which you click.

### *Destructive Filtering*

By default, Process Monitor filters apply to the data it displays, not what it saves. This allows you to change filters to obtain different views of data without affecting the excluded data. However, you can configure Process Monitor to delete any data that's excluded by a filter at the time the data is captured by toggling destructive filtering mode, which you do by choosing Drop Filtered Events from the Filter menu.

## **Include Process from Window**

The toolbar includes a button shaped like a target that you can drag off and drop onto a window to cause Process Monitor to add the process ID of the process that owns the window to the Include filter.

## *Basic vs. Advanced Mode*

The Filter menu's Enable Advanced Output menu item controls whether Process Monitor is operating in Basic or Advanced Mode. When in Basic mode Process Monitor configures built-in filters to exclude system-related activity from the display and uses intuitive names for internal file system operations. For example, Process Monitor shows the internal IRP\_MJ\_READ operation as Read when in Basic mode. Basic mode makes output easier to read and omits events usually not relevant for application troubleshooting.

## *Saving and Loading Filters*

Once you have configured a filter you can save it using the Save Filters menu item in the Tools menu. Process Monitor adds filters you save to the Load Filter menu for easy access and you can change the order in which the filters display in the menu using the Organize Filters dialog that you open with Organize Filters in the Tools menu. You can use the Organize Filter dialog to rename saved filters as well as to easily export filters to a format that you can then reimport using the Organize Filter dialog on other systems.

## *Highlighting*

Process Monitors highlighting filters enable you to specify event attributes that cause an event to be shown with a highlight color. The Highlight submenu in the Event menu provides quick access for defining highlight filter entries and the Highlight menu entry in the Tools menu opens the Highlight Filter dialog, which operates similarly to the Include/Exclude Filter dialog.

## **The Process Tree**

The Process Tree menu entry in the Tools menu opens the Process Tree dialog, which displays all of the processes referenced in the loaded trace in a hierarchy that reflects their parent-child relationships. Processes with the same parent are sorted according to their start time. Processes that are aligned along the left side of the window have parent processes that did not execute any event in the trace.

When you select a process in the tree a subset of the data Process Monitor has obtained about the process, such as its image path, user account, and start time, shows in the bottom of the dialog. To view more information about a process you can click on the Go To Event button, which results in Process Monitor locating and selecting the first visible item in the trace

executed by the process. Note that filters can prevent this operation from succeeding by excluding from the display all of the specified process' events.

### **Trace Summary Tools**

Process Monitor includes a number of dialogs that allow you to perform simple data mining on the events collected in a trace.

### **System Details**

Process Monitor captures some information about the system on which it collects a trace, including the machine name, the system root path, and whether the OS is 32-bit or 64-bit. You can access this information, which Process Monitor stores in log files, from the System Details dialog in the Tools menu.

### **Unique Values**

The Unique Values dialog, which you open using the corresponding menu entry in the Tools menu, lets you see the unique values for each of the different attribute values defined for events in a trace. For example, if you want quickly see all the paths referenced in the trace, choose Path in the selection entry.

Double-clicking on a displayed value or clicking on the Filter button adds an include filter for the currently selected value.

### **Count Occurrences**

Open the Count Occurrences dialog from the Tools menu. It displays the unique values seen in a trace for the attribute type you specify along with the number of times in the trace an event contained the value.

### **Process Summary**

This dialog summarizes the processes seen in the trace, including their process ID, image name, and command line.

### **File Summary**

The File Summary dialog lists each unique file system path present in the filtered trace, the amount of time spent performing I/O to the file, total number of events that referenced the path, and the count of individual operation types.



### *Registry Summary*

The Registry Summary dialog lists each unique Registry path present in the filtered trace, the amount of time spent performing I/O to the Registry path, total number of events that referenced the path, and the count of individual operation types.

### *Network Summary*

The Network Summary dialog lists each unique destination IP address present in the filtered trace and the number different types of events, including sends and receives, to each address.

### *Stack Summary*

Use the Stack Summary dialog to see individual instances of stack traces for each process, including the number of times the stack trace occurs and the total time spent in events that share the same trace.

### **Options**

A number of settings in the Options menu modify Process Monitor's behavior.

#### *Always on Top*

Selecting this option causes the Process Monitor window to remain on top of other windows.

#### *Font*

This option opens a font selection dialog where you can chose the font Process Monitor uses for its display.

#### *Highlight Colors*

Chose this entry to open a dialog to pick the text and background colors Process Monitor uses for entries that match the configured [highlight filters](#).

#### *Configure Symbols*

Process Monitor can use symbol information, if available, to show functions referenced on event stacks. You can find information on configuring symbols on the [Microsoft Debugging Tools for Windows](#) web page.

## *History Depth*

Process Monitor watches committed memory usage and turns itself off when virtual memory runs low, but the History Depth dialog let's you limit the number of entries it keeps so that you can leave Process Monitor running for long periods and ensure that it always keeps the most recent events.

## *Profiling Events*

Use this menu entry to open the thread profiling configuration dialog, where you enable thread profiling and the rate at which thread profiling events generate. When thread profiling is enabled, Process Monitor captures thread stack traces and CPU utilization that you can use to identify the source of CPU-related performance issues.

## *Enable Boot Logging*

Use this option to configure Process Monitor [boot logging](#).

## *Saving and Logging*

### *File Formats*

You can use the Save entry in the File menu to save Process Monitor data in native (PML), comma-delimited value (CSV), or XML formats. The PML format preserves all of the data captured so that you can reload it back into Process Monitor on the same system or a different one. CSV files are useful for importing into Excel or other data analysis applications. Finally, XML emits XML-formatted data that can be parsed by tools that manipulate XML.

### *Logging*

By default, Process Monitor uses virtual memory to store captured data. Use the Backing Files dialog, which you access from the File menu, to configure Process Monitor to store captured data in files on disk. Enabling this option has Process Monitor log data to the disk in its native PML format as it captures it.

The Backing Files dialog also displays diagnostic information, including the number of events captured, processes defined and the capture thread's load status.

### *Boot Logging*

Process Monitor can log activity from a point very early in the boot process during the initialization of boot-start device drivers. Configure Process Monitor to log the next boot by selecting Enable Boot Logging from the Options menu. Process Monitor's driver will log activity

at the next boot into a file in the %Windir% directory and will continue logging through the shutdown or until you run Process Monitor again. Thus, if you don't run Process Monitor during a boot session you will capture a trace of the entire boot to shutdown cycle.

When you run Process Monitor it looks to see if a previous boot log has been generated, and if so, asks you where you want to place the processed boot log output file. Process Monitor displays the trace after it has finished translating it. To see activity from the System process, which is the only process early in a boot, select Enable Advanced Output from the Options menu.

If you configure boot logging and the system crashes early in the boot you can deactivate boot logging by choosing the Last Known Good option from the Windows boot menu (which you access by pressing F8 during the boot).

*Note: network events, which are based on ETW (Event Tracing for Windows), are not available in boot logs.*

## Importing and Exporting Configuration

Once you have configured a filter you can save it using the Save Filters menu item in the Tools menu. Process Monitor adds filters you save to the Load Filter menu for easy access and you can change the order in which the filters display in the menu using the Organize Filters dialog that you open with Organize Filters in the Tools menu. You can use the Organize Filter dialog to rename saved filters as well as to easily export filters to a format that you can then reimport using the Organize Filter dialog on other systems.

You can also export Process Monitor's entire configuration, including filters, column selection, column order and size, log file settings, and debug help file path configuration, to a Process Monitor Configuration file (.PMC) using the Export Configuration menu entry in the File menu. Use the File menu's Import Configuration entry to load a saved configuration file.

## Command Line Options

Process Monitor supports several command line options:

### **/Openlog <saved PML log file>**

Directs Process Monitor to open and load the specified log file.

### **/Backingfile <log file name>**

Has Process Monitor create and use the specified file name as the logging file.

### **/Pagingfile**

Save events to the paging file.

**/Noconnect**

When this flag is present Process Monitor does not automatically start logging activity.

**/Nofilter**

Clears the filter at startup.

**/AcceptEula**

Automatically accepts the license and bypasses the EULA dialog.

**/Profiling**

Enables the thread profiling event class.

**/Minimized**

Starts Process Monitor with its window minimized to the task bar.

**/WaitForIdle**

Wait for an instance of Process Monitor to become ready.

**/Terminate**

Terminate all instances of Process Monitor and exit.

**/Quiet**

Don't confirm filter settings on startup.

**/Run32**

Uses this switch to run the 32-bit version of Process Monitor on 64-bit Windows to open logs generated on 32-bit systems

**/HookRegistry**

This switch, which is available only on 32-bit Vista and Server 2008, has Process Monitor use system-call hooking instead of the Registry callback mechanism to monitor Registry activity, which enables it to see Softgrid virtual Registry operations on these operating systems. This

option must be used the first time that Process Monitor is run on a system and should only be used to troubleshoot SoftGrid applications.

### *[/SaveAs](#), [/SaveAs1](#), [/SaveAs2](#)*

Use these switches with the `/OpenLog` switch to have Process Monitor export a log file into CSV, XML, or PML format. The `/SaveAs1` option includes stack information for export to XML format and the `/SaveAs2` option adds symbol information.

### **Scripting Process Monitor**

You can use Process Monitor command-line options to drive it with a batch file. Here is how your batch file should look to capture a trace of `notepad.exe`'s execution:

```
set PM=C:\sysint\procmon.exe  
start %PM% /quiet /minimized /backingfile C:\temp\notepad.pml  
%PM% /waitforidle  
notepad.exe  
%PM% /terminate
```

The first invocation of Process Monitor using `start` ensures that the process detaches from the console window, which allows it to run concurrently with the later commands. The second invocation with `/WaitForIdle` causes the batch file to pause until the first instance is up and running and actively capturing events. The final invocation with `/Terminate` tells the first instance to stop capturing, commit any outstanding data to the backing file and exit cleanly.