*Process Explorer* shows you information about which DLLs processes have loaded and which handles they have opened. This makes it a powerful tool for understanding the internal behavior of applications, as well as tracking down handle leaks and DLL version mismatches.

The *Process Explorer* display consists of two sub-windows. The top always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that *Process Explorer* is in: if it is in handle mode you'll see the handles (files on Windows 9x/Me) that the process selected in the top window has opened; if it is in DLL mode you'll see the DLLs that the process has loaded.

*Process Explorer* has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded, making it ideal for discovering which process has references that prevent a file, directory, or DLL from being deleted.

You can obtain equivalent command-line tools, *Handle* and *ListDLLs,* at the **Sysinternals** Web site (www.sysinternals.com).

*Process Explorer* works on Windows 9x/Me, Windows NT 4.0, Windows 2000, Windows XP, and Server 2003.

## Starting Process Explorer

Simply run the *Process Explorer* GUI (Procexp.exe).

Note: On Windows NT/WK/XP/2K3 *Process Explorer* requires that your account have the "load driver" and "debug" privileges.

When *Process Explorer* is started for the first time it will be in handle-mode. Menus, hot-keys, or toolbar buttons can be used to refresh the display or switch to DLL-mode.

*Process Explorer* will remember its window positions and the mode that it was in each time you exit it, and initialize with these settings when started again.

You can reorder columns in the process, handle and DLL views simply by clicking on their headers and dragging them to their new position. Use the **View|Select Columns** menu item to choose which columns you want *Process Explorer* to display in each view.

## Processes

You can sort processes by any of the columns in the process view, or click on the **View| Show Process Tree** menu item or toolbar button to have the process view represent the process creation tree. The tree represents the parent-child relationships of processes by indenting children underneath their parent.

If you right-click on a process *Process Explorer* will pop-up a context-menu that will let you view additional CPU and memory-related properties of the process, change the process' base priority, debug the process using the system's registered application debugger, or immediately terminate the process. If the *Dependency Walker* utility (www.dependencywalker.com - depends.exe) is on your path, you'll also see a menu item

that lets you launch Depends with the selected process as the target. If you have a debugger installed the **Debug** menu item will be enabled and have the same behavior of attaching the debugger to the process selected that Task Manager's corresponding menu item has. You can use toolbar buttons or menu entries to accomplish the same tasks. Use the tab key to move the focus between the process and the handle or DLL windows.

Select the **Options|Highlight Services** menu item for Process Explorer to highlight process that host services. You can see the services that are running in a process on the Services tab of a process' properties dialog.

To highlight your own processes, which might be useful in a Terminal Services environment, select the **Options|Highlight Own Processes**.

### Handle Mode

When *Process Explorer* is in handle mode you'll see the names of all the named objects that a selected process has open (note that Registry handles are not shown on Win9x/Me). You can view object properties for most object types to display additional information, such as the signal state of mutexes, semaphores, and events. Use the tab key to move the focus between the handle and process windows.

Select the **Options|Show Unnamed Handles** menu item or toolbar button to see all the process' handles, both named and un-named. You can toggle this mode on and off according to what you want to see. On NT/Win2K, right-clicking on a handle brings up a menu that lets you forcibly close a handle. You should only use this in extreme circumstances because doing so may result in an application or system crash.

Processes and threads are treated as named objects, so you will be shown the process name and, in parenthesis, the process identifier of processes referenced by handles. For thread handles you will be shown the corresponding thread's process name and ID, as well as the thread's ID.

### DLL Mode

Select the **View|View DLLs** menu item or the equivalent toolbar button to switch to DLL mode. In this mode loaded DLLs are listed in the bottom window. If you double-click on a DLL, or press the properties toolbar button, *Process Explorer* will present a properties dialog with detailed version information. You can use the tab key to move the focus between the DLL and process windows.

If you're running on Windows NT/2K, the "MM" column indicates whether the corresponding file has been memory-mapped rather than loaded as a module. This corresponds to an applications use of *MapViewOfFile*. If a file is memory-mapped the base and size columns indicate the virtual address range where the file has been mapped. If you are unable to delete a file and don't find any handle references to it, the file may have been memory mapped, since WinNT/2K does not let memory mapped files be deleted or portions of a file that have been mapped be truncated.

Select the **Options|Highlight Relocated DLLs** to have *Process Explorer* highlight any DLLs that were not loaded at their default base address in yellow. This feature is intended to help developers define base addresses for their DLLs that result in no conflicts and therefore speed load times.

### Refresh

The F5 key or the "Refresh" menu item will cause *Process Explorer* to rescan process, DLL and handle information.  When you perform a refresh *Process Explorer* highlights entries

that existed before the refresh but not after in red. *Process Explorer* shows entries that are new after the refresh in green. For example, if you start a new process, that process will display in green. This feature makes it easier to see what's changed across a refresh, and to find handle leaks.

## Searching

You can search for processes that have particular DLLs loaded or handles opened. The search dialog is activated with the search toolbar button or its menu item. Enter a substring in the edit box of the search dialog and select the "Search" button. If *Process Explorer* is in handle mode it will search for opened handles that contain the substring, but if it is in DLL mode it will search for loaded DLLs that have the substring in their path name. In either case, all handles or DLLs are scanned, not just those of the currently selected process.

Selecting an entry in the result-pane of the find dialog causes *Process Explorer* to locate and display in the process and handle or DLL view (as appropriate), the lines corresponding to the entry you select.

## Reporting Bugs and Feedback

If you encounter a problem while running *Process Explorer*, please visit to obtain the latest version. If you still have problems, please record all the information relevant to the problem. Determine if the problem is reproducible, and if so, how, and send this information to:

mark@sysinternals.com