

Re: Windows process table and process image.

Re: Windows process table and process image.

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2006-06/msg00237.htm>

- *From:* "Chris" <chrisforng@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 8 Jun 2006 16:55:57 -0700
-

Thanks Ivan.

In your example, the parent process is holding the handle of the child process, I can understand the child process won't go away as long as the parent process is alive. But what happens after the parent process is also killed? My understanding is that if a process is terminated, the OS will close all the handles it opened.

In my application, only the child process is listed in process list without process image. All other related(parent) processes are gone.

Thanks,
Chris

"Ivan Brugiolo [MSFT]" <Ivan.Brugiolo@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message [news:OfG\\$5M1iGHA.4504@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:OfG$5M1iGHA.4504@xxxxxxxxxxxxxxxxxxxxxxxx)

As long as there is one active referece to the process object, then the process will in the process list. Zombie processes are normally caused by a handle leak on some other process.

For example this code would cause that

```
HANDLE hProcess = OpenProcess(PID,...);  
TerminateProcess(hProcess,...);
```

You would need to call CloseHandle(hProcess) to remove your own reference to the process object.

--
--

This posting is provided "AS IS" with no warranties, and confers no rights.

Re: Windows process table and process image.

Use of any included script samples are subject to the terms specified at <http://www.microsoft.com/info/copyright.htm>

"Chris" <chrisforng@xxxxxxxxxxxxxxxxxxxx> wrote in message <news:%232burBliGHA.3816@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

Hi,

Please help me understand how Windows process is managed.

My application uses some utility programs such as nslookup and dnscmd. Fo some cases my application needs to kill those child process by calling TerminateProcess().

Here is something I cannot understand, after killing a process why the process is still in process table but its image is gone?

I used Process explorer to check, the process is listed but its image does not exist.

I tried windbg to connect to the process but windbg told me the process image is not there.

The process does hold some file handles so its current directory cannot be removed.

Is there a zambie process in Windows as unix? I cannot find any documents about Windows Zambie processes.

Thanks,
Chris