

Windows process table and process image.

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2006-06/msg00235.htm>

- *From:* "Chris" <chrisforng@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 8 Jun 2006 16:08:13 -0700
-

Hi,

Please help me understand how Windows process is managed.

My application uses some utility programs such as nslookup and dnscmd. For 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 zombie process in Windows as unix? I cannot find any documents about Windows Zombie processes.

Thanks,
Chris