Subject: Re: howto see assembly code?
Posted by mr_ped on Wed, 23 Nov 2005 00:06:18 GMT
View Forum Message <> Reply to Message

hm... calling breakpoint interrupt and rewriting memory at address 0 with 0 is really not the equivalent. INT 3 summons breakpoint interrupt in DOS (Win16/32), and after resume the thread will continue, while "*(int *)0 = 0;" does rewrite protected memory, so the thread will crash. Maybe minor difference when you want to check the code, but can be helpfull when you are just steping trough some code.

I wonder why linux does not implement (or does it?) "INT 3" as breakpoint, because AFAIK (at least in the age of 286/386/486 CPUs) int 3 is the only 1B long interrupt instruction, and the main purpose for this instruction was exactly ability to use breakpoints easily in debuggers. (at least the code should *not* crash at linux, as the INT 3 should be simple RET interrupt when no debugger is running)