kernel32 symbol in live kernel debug

Posted by Thongchai - 29 Aug 2011 - 18:04

Is it possible to load kernel32 or user32 symbol in live kernel debug?
Sorry for stupid question :O

==========

Re: kernel32 symbol in live kernel debug

Posted by Robert Kuster - 09 Oct 2011 - 14:47

Welcome Thongchai.

The kernel on 2000, XP, Vista, or Windows 7 never loads user32.dll or kernel32.dll. Both are user mode DLLs and thus get loaded by user-mode applications (generally speaking any Win32 process should load kernel32.dll; applications that have a GUI also load user32.dll).

Symbols are loaded into a debugger mainly for two purposes:to map raw addresses in the executable to source-code linesto analyze internal layout and data of applications What you are asking about somehow violates this basic principle and is simply not needed to debug an application or the kernel. You can still check out the Symbol Options for WinDbg or start your investigation by examining the ld or !lmi commands.

I hope this helps,
Robert

==========