Function offsets and return address in callstack

Posted by Oliver - 09 May 2012 - 00:14

Hello there,

I have a question :

Given a callstack for example :

0007f5b0 00c13e82 000f0406 0007f624 00000111 notepad!InvokeOpenDialog+0x25 (FPO:)
0007f62c 00c1164a 000f0406 00000002 00000000 notepad!NPCommand+0x165 (FPO:)
0007f650 7795f8d2 000f0406 00000111 00000002 notepad!NPWndProc+0x4cf (FPO:)
0007f67c 7795f794 00c1146c 000f0406 00000111 USER32!InternalCallWinProc+0x23
0007f6f4 77960008 00000000 00c1146c 000f0406 USER32!UserCallWinProcCheckWow+0x14b (FPO:)
0007f758 77960060 00c1146c 00000000 0007f79c USER32!DispatchMessageWorker+0x322 (FPO:)
0007f768 00c11465 0007f780 00000000 00c1a21c USER32!DispatchMessageW+0xf (FPO:)
0007f79c 00c1195d 00c10000 00000000 002226c2 notepad!WinMain+0xe3 (FPO:)
0007f82c 77374911 7ffd6000 0007f878 77ace4b6 notepad!_initterm_e+0x1a1 (FPO:)

I would like to know if frame notepad!WinMain+0xe3 after address calculation along with offset +0xe3 represents return address for the frame above with address 00c11465 ?
Is this always rule when inspecting callstack information for a thread in windbg (assuming callstack information is valid and also correct symbols are loaded)? An example of this would be very appreciated!

Thanks in advance!
Cheers!

==========