Basic commands for Windbg - k

By Anand George

Concept of Callstack

- Callstack is the most important information for any kind of debugging.
- Stack of functions.
- A callstack is there for each thread in the OS.
- k is the command for callstack.
- Many variants – kb, kvn, kM
- Take 3 inputs optional which is esp, eip and ebp which is useful in some case like stack corruption.
- Correct symbols are needed to show the stack correctly.
- Works in both kernel mode and user mode.

Demo

Summary

- Callstack
- k command.

SourceLens
sourcelens.com.au/Training
sourcelens.com.au/Mentoring
sourcelens.com.au/Consult

Thank you