Basic commands for Windbg – dv .frame
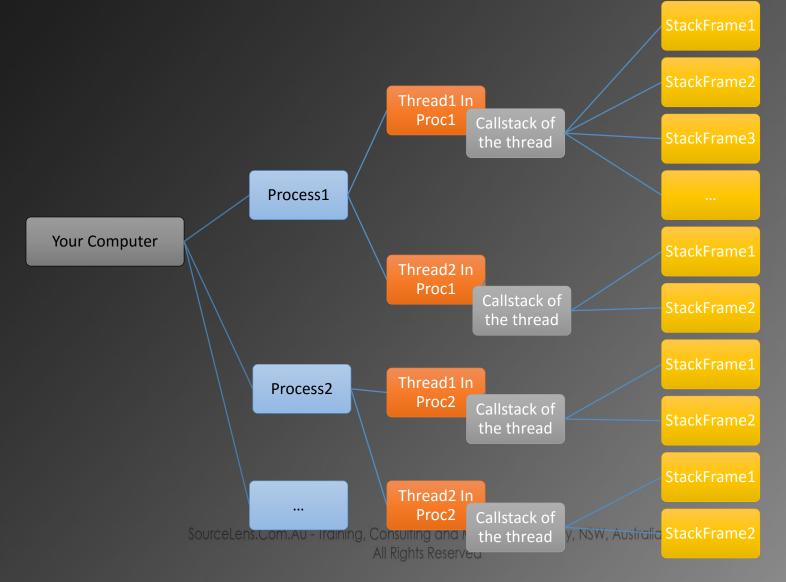
By Anand George

Note

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

- dv command will give incorrect result in fast calling convention and calling conventions similar to that - like 64 bit calling conventions.

- So this limits the user of .frame command as well.

- Works best in the case of x86 calling convention with each frame has the saved ebp (no frame pointer optimization).

Concept of Stack frame

Stack Frame

Arguments Passed

Return Address

Saved EBP

LocalVariables

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

.frame <framenumber>

- Switch to the given frame.

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

dv

- Dump locals and arguments passed for the current frame.

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

Demo

- We can use kM which has the DML for both .frame and dv combined.

Summary

- Stack frame
- .frame
- dv.

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

Thank you