Basic commands for Windbg – r and d*

By Anand George

r – show register

- Show registers.
- Some variants which control the amount of output – rarely used.
- Always show the saved CPU context of the thread even in kernel mode.

d* - dump memory

- dc, du,dd,dp,dq lot of variants.
- dps and dc (I use those more frequently).

Note

- dv and dt are different and not a variants of d*

Demo

Summary

- r
- d*

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

Thank you