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

Basic commands for Windbg – u for Unassemble

By Anand George

SourceLens.Com.Au - Training, Consulting and Mentoring -Sydney, NSW, Australia All Rights Reserved



u* – Unassemble

- To see the disassembly of the code.
- uf for unassembled a function
 - Some times wont work mostly if you have post build optimization.
- ub unassemble backwards very frequently used to understand how the code reached to the current execution point. Helps like an "airplane black box" combined with the information in stack.



Demo

- uf
- ub
- uf /c
- .asm no_code_bytes

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

Summary

- Disassembly in windbg
- a (assemble) opposite rarely used.

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

Thank you

SourceLens.Com.Au - Training, Consulting and Mentoring -Sydney, NSW, Australia All Rights Reserved