Windbg – Introduction to Commands

By Anand George

Command categories

- Native commands
  - Comes with the debugger engine.
  - Covers core debugger operations like breakpoint, read write memory and registers.
- Debugger meta commands
  - More of less like config for the debugger or debugger setting like commands.
  - Start with . (read as dot) example .reload.
- Extension commands
  - Exported by debugger extensions or plug-ins which enhance the capability of debugger engine.
  - Start with ! (read as bang)
  - You can create your own
- Others like command token etc
- More or less meta commands or kind of keywords in debugging command scripts - .for, .while, .continue etc

Lots of commands….

- Mastering all will be quite a job.
- In most cases debugging is not about knowing all the commands but about knowing the internal data structures, functions and relations between them.
- As matter for fact in the day to day "windbg life" we may use only a handful of commands

A few (Case Sensitive)

- .hh
- k
- dv
- dc
- x
- ln
- s
- dt
- r
- p
- t
- e
- u
- bp
- ~ (threads in user mode, processor in kernel mode)
- !process (kernel mode specific)
- !thread (kernel mode specific)

Did I miss !analyze –v ?

DML or "click" debugging

- Type of extensions.
- Click on the command window output links to execute next command.
- Very useful and intuitive with some fairly new debugger extensions.

Demo

Summary

- Debugger commands.

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

Thank you