Introduction to Windbg – Part2 Symbols

By Anand George

What is a debug symbol?

- Generated by linker.
- Have PDB extensions.
- Mainly contains type details, function details.
- Contains a subset of information which is there in the source code.
- Not needed for running the binary.
- Needed for debugging to understand what is what.

PDB

- Format is undocumented.
- Can be accessed via Debugger Interface Access SDK from msdn.

http://msdn.microsoft.com/en-us/library/x93ctkx8.aspx

Microsoft symbols

- Pdb file for Microsoft binaries like ntoskrnl, ntdll, hal etc.
- Is stripped down and very less information and there for called "public symbols".
- Always function locals variable information and argument details missing.
- Some of the symbols has some global variable's type information.
- Need for some commands to work and show the Microsoft part of the stack correctly.
- Path is
  - http://msdl.microsoft.com/download/symbols

Demo

- Setting symbol path.
- Understanding the difference.
- ln and x commands.
- lmvm to see if symbols are loaded.
- sympath
- symfix

Summary

- Symbols
- Setting

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

Thank you