Introduction to Windbg

By Anand George

Windbg

“He’s not a hero… he is a silent guardian, a watchful protector, a dark knight.”

Courtesy - Dark Knight - Christopher Nolan

Windbg

- The single most powerful tool in windows platform.
- A debugging tool for Microsoft OS and applications.
- Free download - comes with SDK/WDK at the time of this presentation.
- Like visual studio debugger we can put breakpoints, watch and execute code step by step.
- But much more powerful than older versions of Visual Studios like VS 2010.

Demo

- Basic debugging in Windbg
- Breakpoints
- Stepping.
- UI
- Command Window.

Advantages

- A lot - but an incomplete list of few.
  - Very light weight, we can copy to a production environment and debug.
  - Huge number of commands and extensions.
  - Endless opportunities to understand and resolve the most difficult problems in windows.
  - Understand OS and software running in that in depth
  - Dump analysis.

Challenges

- Most of the features are command driven and no menu or UI.
- Poor documentation.
- Not everything works as it is to be.
- Microsoft private symbols are needed for advanced debugging which is not available outside.
- Very few inputs from community / forums etc.

Summary

- Windbg as a debugger.
- Pros and cons
- Last and no least - We will be using this tool a lot from now.

Thank you