WinDbg : User Mode

Installation and Overview

: Available on Microsoft Store

Types Of Commands:

1. Built in commands/ regular command/ native commands

e.g g, k etc

1. Meta commands / dot commands (.)

e.g. .cls, .reboot etc

3) Extension Commands (!)

e.g. !threads

Symbols :

🡺Binary generated by linker do not have variable or function name

🡺In order to access the information from executable, we need pdb files which contain symbol information

Modules :

Process :

Threads :

Breakpoints :

Tracing & Stepping :

Call Stack :

Memory :