WinDbg by examples

Advanced techniques in debugging . Net apps

What is WinDbg?

```
File Edit View Debug Window Help
     Command
                                                                              >_ ×
Microsoft (R) Windows Debugger Version 6.2.9200.20512 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.
Loading Dump File [C:\Users\Sergey\AppData\Local\Temp\w3wp (2).DMP]
User Mini Dump File with Full Memory: Only application data is available
Symbol search path is: SRV*C:\Symbols\LocalCache*http://msdl.microsoft.com/downloa
Executable search path is:
Windows 8 Version 9600 MP (8 procs) Free x64
Product: WinNt, suite: SingleUserTS Personal
Built by: 6.3.9600.16384 (winblue rtm.130821-1623)
Machine Name:
Debug session time: Wed Feb 19 19:32:09.000 2014 (UTC + 3:00)
System Uptime: 5 days 22:33:40.531
Process Uptime: 0 days 0:17:51.000
Loading unloaded module list
*** ERROR: Symbol file could not be found. Defaulted to export symbols for ntdll.
*** ERROR: Symbol file could not be found. Defaulted to export symbols for KERNEL
ntdll!ZwWaitForSingleObject+0xa:
00007ffe`633d65ba c3
0:000>
                                     Ln 0. Col 0 Sys 0:C:\User Proc 000:3a4c Thrd 000:4a98 ASM OVR CAPS NUM
```

```
| $6.40 | $6.50 | $6.60 | $6.50 | $6.60 | $6.50 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.60 | $6.6
     (29% 3-65) Prok instruction exception - code 80000003 (first chance)

***EBBR: Symbol file could not be found. Defaulted to export symbols for C:\WINDOWS\SYSTEM32\ntdll.dll -
ntdlllDbgFres#Foint:
00007ffe*633d80a0 cc int 3
0:046/
```



How to use WinDbg?

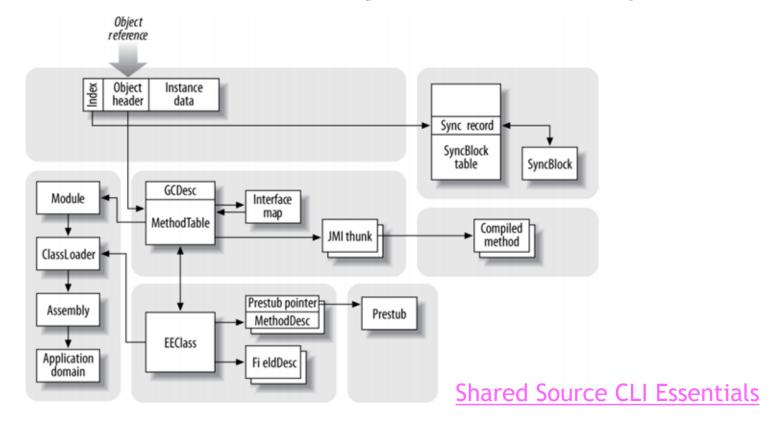
Install WinDbg from WDK or SDK

- Attach to process or open memory dump (crash dump)
- Load extensions: sos, sosex or netext

- Execute commands: !DumpHeap, !ClrStack, !Threads, !runaway, !FinalizeQueue or !Help
- Analyze output



Internal structure of CLR objects in memory



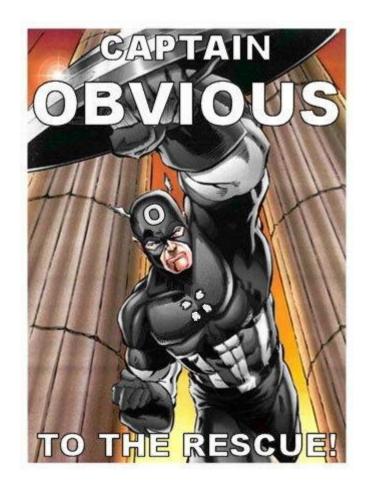


Demo

Case of unexplained redirect

Case of high CPU usage

Case of high memory consumption





Summary

WinDbg is useful for:

- Post mortem debugging
- Debugging on production server
- Understanding internals of applications and frameworks

shchegrikovich@gmail.com

