EBook Gratis

APRENDIZAJE WinDbg

Free unaffiliated eBook created from
Stack Overflow contributors.

#windbg

Tabla de contenido

Acerca de

You can share this PDF with anyone you feel could benefit from it, downloaded the latest version from: windbg

It is an unofficial and free WinDbg ebook created for educational purposes. All the content is extracted from Stack Overflow Documentation, which is written by many hardworking individuals at Stack Overflow. It is neither affiliated with Stack Overflow nor official WinDbg.

The content is released under Creative Commons BY-SA, and the list of contributors to each chapter are provided in the credits section at the end of this book. Images may be copyright of their respective owners unless otherwise specified. All trademarks and registered trademarks are the property of their respective company owners.

Use the content presented in this book at your own risk; it is not guaranteed to be correct nor accurate, please send your feedback and corrections to info@zzzprojects.com

Capítulo 1: Empezando con WinDbg

Observaciones

Esta sección proporciona una descripción general de qué es windbg y por qué un desarrollador puede querer usarlo.

También debe mencionar cualquier tema importante dentro de windbg y vincular a los temas relacionados. Dado que la Documentación para windbg es nueva, es posible que deba crear versiones iniciales de los temas relacionados.

Versiones

Versiones importantes de WinDbg, para versiones compatibles de WinDbg. Vea también una lista detallada con versiones históricas en línea.

Es importante tener en cuenta que hay un cambio en el esquema de versiones de la versión 6.12 anterior a la versión 6.1 más nueva. Las versiones anteriores tienen números bajos (<100) en el tercer lugar, mientras que las versiones más nuevas tienen números altos (> 6000).

En muchos casos, las versiones de WinDbg proporcionadas para las versiones más nuevas de Windows todavía funcionan en versiones anteriores en Windows, por ejemplo, la versión 10 de WinDbg todavía se puede usar en Windows 7. Sin embargo, algunos comandos pueden usar llamadas API que no están disponibles y, por lo tanto, fallan. Por lo tanto, es bueno tener varias versiones de WinDbg disponibles.

Versión	Descripción	Fecha de lanzamiento
6.12.0002.633	proporcionado para Windows 7 y .NET Framework 4	2010-05-21
6.1.7600.16385		2009-07-24
6.2.8400.0	actualización para Windows 8 (?)	2012-06-23
6.2.9200.16384	proporcionado para Windows 8 y .NET Framework 4.5	2012-11-15
6.3.9600.16384	proporcionado para Windows 8.1	2013-10-17
10.0.10075.9	proporcionado para Windows 10	2015-04-29
10.0.10586.567	proporcionado desde Windows 10, compilación 1511	2015-10-30
10.0.14321.1024	proporcionado desde Windows 10, compilación	2016-07-29

Versión	Descripción	Fecha de lanzamiento
	1607	

Examples

Instalación o configuración

Microsoft describe 3 formas de instalar WinDbg:

- como parte del WDK (Kit de controladores de Windows)
- como parte del SDK (Kit de desarrollo de software)
- con el instalador del SDK y deseleccionando todo lo demás excepto "Herramientas de depuración para Windows"

Para obtener el instalador, visite Descargar el WDK, WinDbg y las herramientas asociadas y desplácese hacia abajo a una sección llamada "Obtener herramientas de depuración".

Una fuente conocida y conveniente pero no oficial es Codemachine, donde también puede descargar versiones anteriores de las herramientas de depuración directamente.

La configuración en sí es sencilla. Haga clic a través del instalador hasta que termine.

Depuradores

WinDbg se usa a menudo como una abreviatura de "Herramientas de depuración para Windows". Contiene diferentes depuradores:

Depurador	Descripción
WinDbg	El depurador con una interfaz gráfica de usuario.
CDB	**c** onsole **d** e **b** ugger, depurador de modo de usuario que se ejecuta en la consola actualmente abierta
NTSD	**n** ew **t** erminal **s** ymbolic **d** ebugger, depurador de modo de usuario que abre un nuevo terminal (consola) como su nombre indica
KD	el **k** Ernel **d** ebugger, que se ejecuta en la consola currrently abierto
NTKD	**n** ew **t** erminal **k** ernel **d** ebugger, abre un nuevo terminal

Los comandos son idénticos, excepto que puede haber comandos relacionados con la GUI que no funcionan en las versiones de la consola.

Lea Empezando con WinDbg en línea: https://riptutorial.com/es/windbg/topic/1833/empezando-con-windbg

Capítulo 2: Análisis de colisiones

Examples

Análisis de fallas en modo usuario básico

`.exr -1` le da detalles sobre la última excepción lanzada.

`!analyze -v` generalmente hace un buen trabajo también.

Para .NET, el comando `!pe` de la extensión SOS muestra detalles sobre la excepción .NET que se lanzó.

Lea Análisis de colisiones en línea: https://riptutorial.com/es/windbg/topic/5389/analisis-de-colisiones

Capítulo 3: Depuración del núcleo

Examples

Comandos importantes

- ! proceso - lista los procesos en modo usuario
- .process - establece contexto de proceso
- ! peb - muestra el bloque de entorno de proceso
- ! teb - mostrar bloque de entorno de hilo
- ! bloqueos - análisis de interbloqueo
- .dump - guarda un archivo de volcado de caída en el disco

Lea Depuración del núcleo en línea: https://riptutorial.com/es/windbg/topic/6076/depuracion-del-nucleo

Capítulo 4: Depuración remota

Examples

Comandos importantes

- .server - crea un servidor de depuración
- .clients: muestra los clientes de depuración conectados al servidor
- .endsrv - termina un servidor de depuración
- .servers - lista las conexiones del servidor de depuración
- .remote - inicia un servidor remote.exe
- .noshell - previene comandos de shell

Lea Depuración remota en línea: https://riptutorial.com/es/windbg/topic/5977/depuracion-remota

Capítulo 5: DML (lenguaje de la marca del depurador)

Examples

Encender / apagar

.prefer_dml 1 activa la salida de dmlformat

.prefer_dml 0 desactiva la salida dmlformat

Lea DML (lenguaje de la marca del depurador) en línea:
https://riptutorial.com/es/windbg/topic/7987/dml--lenguaje-de-la-marca-del-depurador-

Capítulo 6: Extensiones

Examples

llamada de socorro

SOS (hijo de strike) es la extensión oficial de WinDbg de Microsoft para .NET. Se instala como parte del marco .NET y, por lo tanto, está disponible de forma predeterminada.

Como cualquier extensión, se puede cargar utilizando `.load x:\full\path\to\sos.dll` , pero hay formas más fáciles. Dependiendo de la versión de .NET, la extensión se encuentra lado a lado de `mscorwks.dll` (.NET CLR 2), `clr.dll` (.NET CLR 4) o `coreclr.dll` (aplicaciones Silverlight y Universal), por lo que una de las los siguientes comandos deberían funcionar:

```
.loadby sos clr
.loadby sos coreclr
.loadby sos mscorwks
```

Para obtener una lista de los comandos disponibles, consulte `!help` .

SOSex

SOSex es una extensión de SOS, escrita por Steve Johnson , un empleado de Microsoft. Proporciona SOSex para descargar de forma gratuita, pero no es de código abierto.

Por lo general, la extensión no está disponible una junto a otra DLL, por lo que generalmente se carga con `.load x:\full\path\to\sosex.dll` .

Además de simplificar la depuración de .NET, el comando `!dlk` también se puede usar en entornos nativos para verificar puntos muertos de secciones críticas.

Para obtener una lista de los comandos disponibles, consulte la `!help` de SOSex.

PyKD

PyKD es una extensión de WinDbg que te permite escribir scripts de Python. Es de código abierto.

Normalmente, la extensión no está disponible una al lado de otra DLL, por lo que generalmente se carga con `.load x:\full\path\to\pykd.pyd` , donde PYD es la extensión para una DLL de python, pero puede cambiar el nombre a DLL si lo desea.

Empezando con PyKd

PyKD no ofrece `!help` , así que busque la documentación en Codeplex. Muchos desarrolladores parecen ser de Rusia y la documentación más actualizada y completa probablemente esté en

ruso. El traductor de Google hace un trabajo decente.

Al igual que otras extensiones, use el bitness correcto de la extensión que corresponde a la de WinDbg. Además de eso, también debes tener Python instalado con el mismo bitness.

`!py` ejecuta un intérprete REPL y `!py x:\path\to\script.py` ejecuta un script en python. Los scripts deben usar

```
from pykd import *
```

como la primera línea para hacer uso de la funcionalidad de PyKD, mientras que esta línea no es necesaria en el intérprete REPL. Se puede salir del intérprete usando `exit()` .

NetExt

NetExt es una extensión para .NET que proporciona

- Consultas similares a LINQ para objetos en el montón (`!wselect !wfrom`)
- capacidades de visualización para objetos especiales como diccionarios y tablas hash (`!wdict !whash`)
- Comandos relacionados con ASP.NET / HTTP (`!wcookie !wruntime !whttp`)
- varios otros comandos relacionados con la red

Normalmente, la extensión no está disponible una al lado de otra DLL, por lo que generalmente se carga con .load x: \ full \ path \ to \ netext.dll

Resumen de extensiones

Una lista incompleta de las extensiones de WinDbg que no están instaladas con el propio WinDbg:

Extensión	Propósito
llamada de socorro	.NET (extensión oficial de Microsoft)
SOSex	.NET (extensión para SOS)
CoSOS	.NET (extensión para SOS)
NetExt	.NET (con enfoque en redes)
PyKD	Python scripting
PDE	Aplicaciones nativas y de tienda de Windows (excepciones almacenadas)
PSSCOR	.RED

Extensión	Propósito
SDbgExt	.RED
MEX	.RED

CoSOS

Cosos (primo del SOS) es una extensión de código abierto para WinDBG centrándose en la fragmentación de memoria .NET (`!gcview`) y roscado cuestiones (`!wfo` , `!tn`).

Normalmente, la extensión no está disponible una al lado de otra DLL, por lo que generalmente se carga con `.load x:\full\path\to\cosos.dll` . Requiere que SOS esté cargado y actualmente solo funciona con aplicaciones de 32 bits.

Lea Extensiones en línea: https://riptutorial.com/es/windbg/topic/5391/extensiones

Capítulo 7: Modo de usuario / depuración de aplicaciones

Examples

Comandos importantes

Documentando tu trabajo

Recuerda lo que has hecho y conserva salidas largas que no se pueden mantener en el búfer de WinDbg. Siempre es bueno tener un registro disponible para reproducir los pasos de depuración, por ejemplo, para hacer preguntas sobre el desbordamiento de pila.

Mando	Propósito
`.logopen`	crear un archivo de registro
`.logclose`	cierra el archivo de registro
`.dump`	guardar archivo de volcado de caída (instantánea de la sesión de depuración actual)

Trabajando con simbolos

Sin o con símbolos incorrectos, puede recibir información incorrecta y ser engañado. Asegúrese de estar familiarizado con estos comandos antes de comenzar a trabajar en WinDbg. Vea también Cómo configurar símbolos en WinDbg .

Mando	Propósito
`.symfix`	establecer o agregar símbolos a la ruta oficial de símbolos de Microsoft
`.sympath`	Establecer o añadir símbolos propios o de terceros.
`.reload`	recargar simbolos
`.symopt`	Definir las opciones de manejo de símbolos.
`!sym`	símbolo de control de carga
`x`	examinar simbolos
`ln`	lista de símbolos más cercanos

Análisis de colisiones

Averigüe qué ha sucedido (en los volcados) y cómo manejar los eventos (en la depuración en vivo).

Mando	Propósito
`.exr`	mostrar registro de excepción
`.lastevent`	mostrar el último evento
`sx`	definir manejo de excepciones
`!analyze`	analizar un choque o colgar
`!avrf`	verificador de la aplicación

El entorno

Compruebe el nombre del proceso y la información de la versión.

Mando	Propósito
| (tubo)	procesar informacion
`lm`	lista de módulos

Hilos, pilas de llamadas, registros y memoria.

Inspecciona los detalles.

Mando	Propósito
`~`	lista de hilos
`r`	registros
`k`	pila de llamadas
`d` *	memoria de pantalla
`e` *	editar memoria
`s`	memoria de búsqueda
`.formats`	convertir entre formatos de números

Mando	Propósito
`?`	evaluar expresión
`u` *	desmontar
`a`	montar
`!address`	información de la memoria

Controlando el objetivo

En la depuración en vivo, tomar el control de la ejecución.

Mando	Propósito
`g`	ir / continuar
`gu`	subir
`p`	un solo paso
`t`	traza (solo paso y registros de salida)
`bp`	establecer punto de interrupción
`bl`	lista de puntos de interrupción

Trabajando con extensiones

Las extensiones pueden proporcionar importantes ventajas y mejoras.

Mando	Propósito
`.load`	extensión de carga (ruta completa)
`.loadby`	extensión de carga relativa al módulo
`.chain`	mostrar extensiones cargadas
`.unload`	extensión de descarga

Dejar de depurar

Mando	Propósito
`q`	salir y terminar la aplicación

Mando	Propósito
`qd`	separar y dejar

Adjuntar y separar

Mando	Propósito
`.tlist`	lista de procesos
`.attach`	adjuntar al proceso
`.create`	crear un proceso y adjuntar
`.childdbg`	Definir el comportamiento de depuración del proceso hijo
`.detach`	desprenderse de un proceso
`.kill`	matar un proceso
`.restart`	reiniciar el proceso

Comportamiento de WinDbg

Mando	Propósito
`.prefer_dml`	configurar el manejo del lenguaje de marcado del depurador
`.effmach`	cambiar el bitness

Comandos de usabilidad

Mando	Propósito
`.cmdtree`	Carga un archivo de texto con comandos predefinidos en una ventana separada

Obtención de ayuda

Mando	Propósito
`.hh`	Muestra el manual de ayuda para los comandos de WinDbg

Crear una ventana de comando personalizada en Windbg

El comando `.cmdtree` permite abrir un archivo `.txt` con comandos predefinidos que puede simplemente hacer doble clic para ejecutar.

Cómo crear un archivo de comando

Crea el archivo usando esta plantilla

```
windbg ANSI Command Tree 1.0
title {"Window title"}
body
{"Group Heading"}
 {"Name of command to display"} {"command"}
 {"Name of command to display"} {"command"}
{"Group Heading"}
 {"Name of command to display"} {"command"}
```

Cosas para cuidar

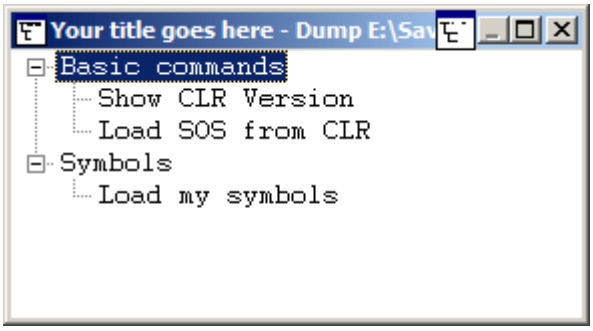
1. El formato de la plantilla debe seguirse precisamente para abrir el archivo en Windbg.
2. Se requiere la nueva línea después de cada `{Group Heading}` .
3. Cada par de `{Name of command to display} {command}` debe estar en una línea y debe ir seguido de una nueva línea.

Ejemplo de archivo de comando personalizado

```
windbg ANSI Command Tree 1.0
title {"Your title goes here"}
body
{"Basic commands"}
 {"Show CLR Version"} {"lmv m clr"}
 {"Load SOS from CLR"} {".loadby sos clr "}
{"Symbols"}
 {"Load my symbols"} {".sympath+ "c:\DebugSymbols" ; .reload"}
```

Cómo abrir el comando UI desde la ventana de comandos

Ejecute `.cmdtree <path of your .txt file>` para abrir la ventana. Verás una ventana como esta.



Haga doble clic en el comando para ejecutar.

Lea Modo de usuario / depuración de aplicaciones en línea:
https://riptutorial.com/es/windbg/topic/5384/modo-de-usuario---depuracion-de-aplicaciones

Creditos

S. No	Capítulos	Contributors
1	Empezando con WinDbg	Community, Thomas Weller
2	Análisis de colisiones	Thomas Weller
3	Depuración del núcleo	Thomas Weller
4	Depuración remota	Thomas Weller
5	DML (lenguaje de la marca del depurador)	Wang Zhengzhang
6	Extensiones	Jason Evans, Lieven Keersmaekers, Thomas Weller
7	Modo de usuario / depuración de aplicaciones	Piyush Parashar, Thomas Weller, X. Liu