無料電子ブック

学習

WinDbg

Free unaffiliated eBook created from
Stack Overflow contributors.

#windbg

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.

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

1: WinDbgをいめる

このセクションでは、windbgのと、なぜがそれをいたいのかをします。

また、windbgのきなテーマについてもし、トピックにリンクするがあります。 windbgのドキュメンテーションはしいので、それらのトピックのバージョンをするがあります。

バージョン

WinDbgのサポートされているバージョンのWinDbgのなバージョン。 なバージョンのオンラインでなリストもごください。

いバージョン6.12からしい6.1バージョンへのバージョニングスキームのがあることにすることがです。いバージョンは3にい<100をち、しいバージョンはい> 6000をっています。

くの、しいWindowsバージョンにされたWinDbgのバージョンはWindowsのバージョンでもします。たとえば、WinDbgのバージョン10はWindows 7でもできます。ただし、のコマンドではできないAPIびしがされるがあります。したがって、WinDbgのいくつかのバージョンをすることはいことです。

バージョン		
6.12.0002.633	Windows 7および.NET Framework 4にされています	2010-05-21
6.1.7600.16385		2009-07-24
6.2.8400.0	Windows 8のプログラム	2012-06-23
6.2.9200.16384	Windows 8および.NET Framework 4.5にされています	2012-11-15
6.3.9600.16384	Windows 8.1に	20131017
10.0.10075.9	Windows 10に	2015-04-29
10.0.10586.567	Windows 10、1511をビルド	2015-10-30
10.0.14321.1024	Windows 10、1607を	2016-07-29

Examples

インストールまたはセットアップ

マイクロソフトでは、WinDbgをインストールする3つのについてしています 。

- WDKWindows Driver Kitのとして、
- SDKソフトウェアキットのとして、
- SDKのインストーラをして「Debugging Tools for Windows」のすべてのをします

インストーラをするには、WDK、WinDbg、およびツールをダウンロードし、「Get debugging tools」セクションまでスクロールしてください。

よくられていてですがのソースは、デバッグツールのいバージョンをダウンロードできるコーデックマシーンです。

セットアップはです。インストーラがするまでクリックします。

デバッガ

WinDbgは「Windowsデバッグツール」のとしてよくわれます。さまざまなデバッガがまれています

デバッガ	
WinDbg	グラフィカルユーザインタフェースをえたデバッガ
CDB	**c** onsole **d** e **b** ugger、いているコンソールでされるユーザモードデバッガ
NTSD	**N** EW **T** erminal **S** ymbolic **D** ebugger、がするように、しいコンソールをき、ユーザモードデバッガ
K D	いよくいているコンソールでする**k** ernel **d** ebugger
NTKD	**N** EW **T** erminal **K** ernel **D** ebugger、しいをい

コンソールのバージョンではしないGUIのコマンドがあることをいて、コマンドはじです。

オンラインでWinDbgをいめるをむ https://riptutorial.com/ja/windbg/topic/1833/windbgをいめる

2: DMLデバッガマーク

Examples

オン/オフをりえる

.prefer_dml 1 dmlformatをオンにする

.prefer_dml 0 dmlformatのをオフにする

オンラインでDMLデバッガマークをむ https://riptutorial.com/ja/windbg/topic/7987/dml-デバッガマーク-

3: カーネルデバッグ

Examples

なコマンド

- process - ユーザーモードプロセスをする
- .process - プロセスコンテキストをする
- peb - プロセスブロックをする
- teb - スレッドブロックをする
- locks - デッドロック
- .dump - クラッシュダンプファイルをディスクにする

オンラインでカーネルデバッグをむ https://riptutorial.com/ja/windbg/topic/6076/カーネルデバッグ

4: クラッシュ

Examples

なユーザーモードのクラッシュ

`.exr -1`は、スローされたのについてのをします。

`!analyze -v`は、よくきます。

.NETの、SOSの`!pe`コマンドは、スローされた.NETにするをします。

オンラインでクラッシュをむ https://riptutorial.com/ja/windbg/topic/5389/クラッシュ

5: ユーザーモード/アプリケーションのデバッグ

Examples

なコマンド

あなたのをする

あなたがやったことをえて、WinDbgのバッファにできないいをしてください。スタックオーバーフローにするなど、デバッグステップをするためのログをすることは、にいことです。

コマンド	
`.logopen`	ログファイルをする
`.logclose`	ログファイルをじる
`.dump`	クラッシュダンプファイルをするのデバッグセッションのスナップショット

をってする

ったがいていない、またはしくないと、ったをけりをくことがあります。 WinDbgでをするに、これらのコマンドにしていることをしてください。 WinDbgでシンボルをするもしてください。

コマンド	
`.symfix`	Microsoftのシンボルパスにシンボルをまたはする
`.sympath`	またはのシンボルをまたはする
`.reload`	シンボルをリロードする
`.symopt`	シンボルオプションをする
`!sym`	のみみ
`x`	シンボルをべる
`ln`	もいをする

クラッシュ

がきたのかクラッシュダンプので、イベントをどのようにするかライブデバッグ

コマンド	
.exr	レコードをする
.lastevent	のイベントをする
sx	をする
!analyze	クラッシュやハングアップをする
!avrf	アプリケーションプログラム

プロセスとバージョンをしてください。

コマンド	
| パイプ	プロセス
lm	モジュールリスト

スレッド、コールスタック、レジスタ、メモリ

をべます。

コマンド	
~	スレッドリスト
r	レジスタ
k	コールスタック
d*	メモリ
e*	メモリをする
s	メモリ
.formats	の
?	をする
u*	する

コマンド	
a	アセンブル
!address	メモリ

ターゲットの

ライブデバッグでは、をします。

コマンド	
g	く/ける
gu	がる
p	
t	トレースステップおよびレジスタ
bp	ブレークポイントをする
bl	ブレークポイントリスト

をってする

は、きなとをするがあります。

コマンド	
.load	フルパス
.loadby	モジュールにする
.chain	みんだをする
.unload	アンロード

デバッグをする

コマンド	
q	アプリケーションをしてする
qd	りしてする

アタッチとデタッチ

コマンド	
.tlist	プロセスリスト
.attach	プロセスにアタッチする
.create	プロセスをしてする
.childddbg	プロセスのデバッグをする
.detach	プロセスからりす
.kill	プロセスをす
.restart	プロセスをする

WinDbgの

コマンド	
.prefer_dml	デバッガマ―クァップをする
.effmach	ビットのりえ

ユ―ザビリティコマンド

コマンド	
.cmdtree	みのコマンドをむテキストファイルをのウィンドウにみみます

けをる

コマンド	
.hh	WinDbgコマンドのヘルプマニュアルをします。

Windbgでカスタムコマンドウィンドウをする

.cmdtreeコマンドをすると、みのコマンドで.txtファイルをくことができます。このコマンドは、

ダブルクリックしてするだけです。

コマンドファイルの

このテンプレートをしてファイルをする

```
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"}
```

になること

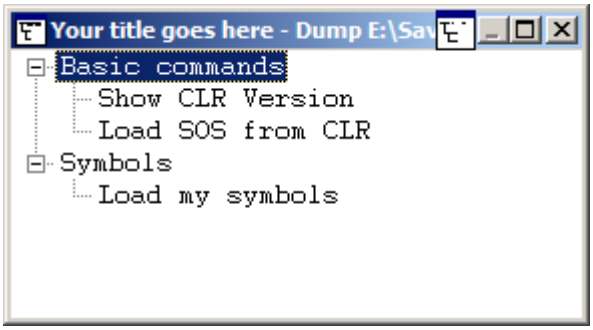
1. Windbgでファイルをくには、テンプレートをにわなければなりません。
2. `{Group Heading}`にがです。
3. `{Name of command to display} {command}`ペアは、1にするがあります。しいがかなければなりません。

カスタムコマンドファイルの

```
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"}
```

コマンドウィンドウからコマンドUIをく

`.cmdtree <path of your .txt file>`をしてウィンドウをきます。このようなウィンドウがされます



するコマンドをダブルクリックします。

オンラインでユーザーモード/アプリケーションのデバッグをむ
https://riptutorial.com/ja/windbg/topic/5384/ユーザーモード-アプリケーションのデバッグ

6: リモートデバッグ

Examples

なコマンド

- .server - デバッグサーバをする
- .clients - サーバにされたデバッグクライアントをする
- .endsrv - デバッグサーバをする
- .servers - デバッグサーバーをする
- .remote - remote.exeサーバーをする
- .noshell - シェルコマンドをする

オンラインでリモートデバッグをむ https://riptutorial.com/ja/windbg/topic/5977/リモートデバッグ

7:

Examples

SOS

SOSストライキのは、Microsoftの.NETのWinDbgです。 .NET Frameworkのとしてインストールされるため、でできます。

のとに、 `.load x:\full\path\to\sos.dll`をしてロードできますが、よりながあります。 .NETのバージョンにじて、は`mscorwks.dll` .NET CLR 2、 `clr.dll` .NET CLR 4、または`coreclr.dll` SilverlightおよびUniversalアプリケーションに`coreclr.dll`でいるため、のコマンドをするがあります

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

なコマンドのリストについては、consult `!help`してください。

SOSex

SOSexはMicrosoftのであるSteve Johnsonによってかれたsosのです。はでSOSexをダウンロードしてしていますが、オープンソースではありません。

、はのDLLとべてできないため、は`.load x:\full\path\to\sosex.dll`ます。

.NETのデバッグをするだけでなく、 `!dlk`コマンドをネイティブでして、クリティカルセクションのデッドロックをチェックすることもできます。

なコマンドのリストについては、SOSexの`!help`にしてください。

PyKD

PyKDは、PythonスクリプトをくためのwinDbgです。オープンソースです。

、はのDLLとべてできないため、は`.load x:\full\path\to\pykd.pyd`はPython DLLのですが、それはあなたがきならDLLに。

PyKdをいめる

PyKDはHelp `!help`していないので、Codeplexのドキュメントをしてください。くのはロシアのようですが、のなはおそらくロシアでかれています。 Googleはまともなをしています。

のとに、WinDbgのにするしいビットをします。それにえて、じビットでPythonをインストールするがあります。

`!py`はREPLインタプリタをし、 `!py x:\path\to\script.py`はPythonスクリプトをします。スクリプトでするがあります

```
from pykd import *
```

このはREPLインタープリタではないが、PyKDのをするためにはのである。インタプリタは`exit()`をして`exit()`できます。

NetExt

NetExtは.NETのであり、

- ヒープのオブジェクトにするLINQのようなクエリ `!wselect`、 `!wfrom`
- やハッシュテーブルなどのなオブジェクトの `!wdict`、 `!whash`
- ASP.NET / HTTPのコマンド `!wcookie`、 `!wruntime`、 `!whttp`
- いくつかののネットワークのコマンド

、はのDLLとべてできないため、は.load x¥full¥path¥to¥netext.dllがロードされます

の

WinDbgでインストールされていないWinDbgのなリスト

SOS	.NETMicrosoftエクステンション
SOSex	.NETSOSの
CoSOS	.NETSOSの
NetExt	.NETネットワーキングをに
PyKD	Pythonスクリプト
PDE	Windowsのネイティブアプリケーションとストアアプリケーションされている
PSSCOR	。ネット
SDbgExt	。ネット
MEX	。ネット

CoSOS

CoSOS SOSのいとこは、.NETメモリの `!gcview` とスレッドの `!wfo` 、 `!tn` にをてたWinDbgのオープンソースです。

、はのDLLとべてできないため、は`.load x:\full\path\to\cosos.dll`ます。 SOSがロードされ、は32ビットアプリケーションでのみすることがです。

オンラインでをむ https://riptutorial.com/ja/windbg/topic/5391/

クレジット

S. No		Contributors
1	WinDbgをいめる	Community, Thomas Weller
2	DMLデバッガマーク	Wang Zhengzhang
3	カーネルデバッグ	Thomas Weller
4	クラッシュ	Thomas Weller
5	ユーザーモード/アプリケーションのデバッグ	Piyush Parashar, Thomas Weller, X. Liu
6	リモートデバッグ	Thomas Weller
7		Jason Evans, Lieven Keersmaekers, Thomas Weller