무료 전자 책

배우기

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

windbg .

windbg . windbg .

WinDbg WinDbg. .

6.12 6.1 . (<100) , (> 6000) .

, Windows WinDbg Windows . WinDbg 10 Windows 7 . API . WinDbg .

6.12.0002.633	Windows 7 .NET Framework 4	2010-05-21
6.1.7600.16385		2009-07-24
6.2.8400.0	Windows 8 (?)	2012-06-23
6.2.9200.16384	Windows 8 .NET Framework 4.5	2012-11-15
6.3.9600.16384	Windows 8.1	2013-10-17
10.0.10075.9	Windows 10	2015-04-29
10.0.10586.567	Windows 10 , 1511	2015-10-30
10.0.14321.1024	Windows 10 , 1607	2016-07-29

Examples

Microsoft WinDbg 3 .

- WDK (Windows Driver Kit) ,
- SDK ( ) ,
- SDK "Debugging Tools for Windows"

WDK, WinDbg " " .

Codemachine .

. .

WinDbg "Windows " . :

WinDbg	

CDB	**C** onsole **d** e **b** ugger,
NTSD	**N** EW erminal ymbolic **D** ebugger, () **S t**
KD	currrently **k** ernel **d** ebugger
NTKD	**N** EW **t** erminal **K** ernel **D** ebugger

GUI .

WinDbg : https://riptutorial.com/ko/windbg/topic/1833/windbg-

2: DML ( )

Examples

/

.prefer_dml 1 dmlformat .

.prefer_dml 0 dmlformat .

DML ( ) : https://riptutorial.com/ko/windbg/topic/7987/dml-----

3: /

Examples

WinDbg . .

`.logopen`	
`.logclose`	.
`.dump`	( )

. WinDbg . WinDbg .

`.symfix`	Microsoft .
`.sympath`	
`.reload`	
`.symopt`	
`!sym`	
`x`	
`ln`	

( ) ( ).

`.exr`	
`.lastevent`	
`sx`	
`!analyze`	
`!avrf`	

.

| ()	
`lm`	

, ,

.

~	
r	
k	
d *	
e *	
s	
.formats	
?	
u *	
a	
!address	

.

g	/
gu	
p	
t	( )
bp	
bl	

.

.load	( )
.loadby	
.chain	
.unload	

q	.
qd	

.tlist	
.attach	
.create	
.childdbg	
.detach	
.kill	
.restart	.

WinDbg

.prefer_dml	
.effmach	

.cmdtree	.

.hh	WinDbg .

Windbg

.cmdtree .txt . .

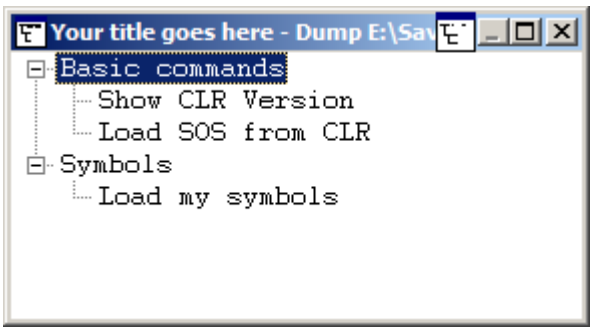
```
windbg ANSI Command Tree 1.0
title {"Window title"}
body
{"Group Heading"}
 {"Name of command to display"} {"command"}
 {"Name of command to display"} {"command"}
{"Group Heading"}
 {"Name of command to display"} {"command"}
```

1. Windbg .
2. {Group Heading} .
3. {Name of command to display} {command} .

```
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"}
```

UI

```
.cmdtree <path of your .txt file>   .
```



.

/ : https://riptutorial.com/ko/windbg/topic/5384/------

4:

Examples

- .server -
- .clients -
- .endsrv -
- .servers -
- .remote - remote.exe .
- .noshell -

: https://riptutorial.com/ko/windbg/topic/5977/-

5:

Examples

`.exr -1` .

`!analyze -v` .

.NET SOS `!pe` throw .NET .

: https://riptutorial.com/ko/windbg/topic/5389/-

6:

Examples

- ! -
- .process -
- ! peb -
- ! teb -
- ! locks -
- .dump - .

: https://riptutorial.com/ko/windbg/topic/6076/-

7:

Examples

SOS ( ) .NET Microsoft WinDbg . .NET Framework .

`.load x:\full\path\to\sos.dll` . .NET `mscorwks.dll` (.NET CLR 2), `clr.dll` (.NET CLR 4) `coreclr.dll` (Silverlight Universal apps) `coreclr.dll` .

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

`!help` .

SOSex

SOSex Microsoft Steve Johnson SOS . SOSex .

DLL `.load x:\full\path\to\sosex.dll` .

.NET `!dlk` .

SOSex `!help` .

PyKD

PyKD Python WinDbg . .

DLL `.load x:\full\path\to\pykd.pyd` . PYD Python DLL DLL.

PyKd

PyKD `!help` Codeplex . . Google .

WinDbg . .

`!py` REPL `!py x:\path\to\script.py` . .

```
from pykd import *
```

REPL PyKD . `exit()` `exit()` .

NetExt

NetExt .NET

-

LINQ (`!wselect !wfrom`)
- (`!wdict !whash`)
- ASP.NET / HTTP (`!wcookie` , `!wruntime` , `!whttp`)
-

DLL .load x : \ full \ path \ \ netext.dll.

WinDbg WinDbg :

	.NET (Microsoft)
SOSex	.NET (SOS)
CoSOS	.NET (SOS)
NetExt	.NET ( )
PyKD	
PDE	Windows ( )
PSSCOR	.
SDbgExt	.
MEX	.

CoSOS

CoSOS (SOS) .NET (`!gcview`) (`!wfo !tn`) WinDbg .

DLL `.load x:\full\path\to\cosos.dll` . SOS 32 .

: https://riptutorial.com/ko/windbg/topic/5391/-

S. No		Contributors
1	WinDbg	Community, Thomas Weller
2	DML ( )	Wang Zhengzhang
3	/	Piyush Parashar, Thomas Weller, X. Liu
4		Thomas Weller
5		Thomas Weller
6		Thomas Weller
7		Jason Evans, Lieven Keersmaekers, Thomas Weller