免費電子書

學習

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

windbg。

windbg。 windbg。

WinDbgWinDbg。 。

6.126.1。 <100> 6000。

WindowsWinDbgWindowsWinDbg10Windows 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	20121115
6.3.9600.16384	Windows 8.1	○
10.0.10075.9	Windows 10	2015429
10.0.10586.567	Windows 101511	○
10.0.14321.1024	Windows 101607	2016729

Examples

Microsoft WinDbg3

- WDKWindows
- SDK
- SDK“Windows”

WDKWinDbg“”。

Codemachine。

。 。

WinDbg“Windows”。

WinDbg	

CDB	**c** onsole **d** e **b** ugger
NTSD	**ÑEW** ymbolic **d** ebugger
KD	**k** ernel **d** ebugger
NTKD	**ÑEW ķernel d** ebugger

GUI。

WinDbg https://riptutorial.com/zh-TW/windbg/topic/1833/windbg

2: DML

Examples

/

.prefer_dml 1dmlformat

.prefer_dml 0dmlformat

DML https://riptutorial.com/zh-TW/windbg/topic/7987/dml--

3:

Examples

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

https://riptutorial.com/zh-TW/windbg/topic/6076/

4:

Examples

```
.exr -1
```

```
!analyze -v
```

.NETSOS`!pe`.NET

https://riptutorial.com/zh-TW/windbg/topic/5389/

5:

Examples

SOS

SOSMicrosoft for .NETWinDbg。.NET。

`.load x:\full\path\to\sos.dll` 。.NET`mscorwks.dll` .NET CLR 2 `clr.dll` .NET CLR 4`coreclr.dll` SilverlightUniversal `coreclr.dll`

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

`!help` 。

SOSex

SOSexSOS。SOSex 。

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

.NET`!dlk`。

SOSex`!help` 。

PyKD

PyKDWinDbgPython。 。

DLL.`load x:\full\path\to\pykd.pyd` PYDpython DLLDLL。

PyKd

PyKD`!help` Codeplex。 。 。

WinDbg。Python。

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

```
from pykd import *
```

PyKDREPL。`exit()`。

NetExt

NetExt.NET

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

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

WinDbgWinDbg

SOS	.NET
SOSex	.NETSOS
CoSOS	.NETSOS
NetExt	.NET
PyKD	Python
PDE	Windows
PSSCOR	。
SDbgExt	。
MEX	。

CoSOS

CoSOS SOSWinDbg.NET `!gcview !wfo !tn` 。

DLL`.load x:\full\path\to\cosos.dll` 。 SOS32。

https://riptutorial.com/zh-TW/windbg/topic/5391/

6: /

Examples

WinDbg。 Stack Overflow。

.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
.childddbg
.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"}
```

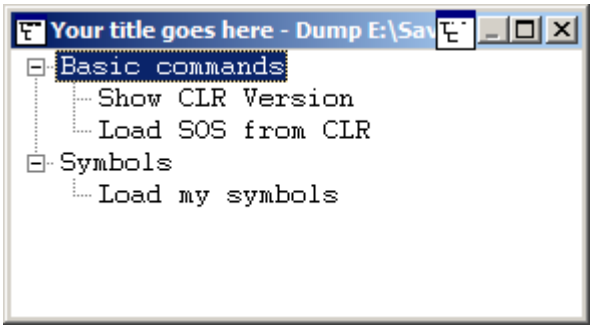
1. Windbg◦
2. {Group Heading}◦
3. {Name of command to display} {command}◦

```
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/zh-TW/windbg/topic/5384/-

7:

Examples

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

https://riptutorial.com/zh-TW/windbg/topic/5977/

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