

Debug Windows Kernel

Information Security Inc.



Contents

- Windows Architecture
- Debugging Lab
- Setting up the Debugger
- Setting up the Debugee
- Setting up and testing the connection between Debugger and Debugee
- References



Windows Architecture

O User-mode and Kernel-mode

- In user-mode, an application starts a user-mode process which comes with its own private virtual address space and handle table
- In kernel mode, applications share virtual address space.
- © Relationship of application components for user-mode and kernel-mode.





Debugging Lab

◎ Lab components

- ▲ Vmware workstation 12 pro
- ▲ Two virtual machines: Windows 10 64bit (one will be the Debugger and one will be the Debugee)

Edition	Windows 10 Pro
Version	1703
OS Build	15063.540

WinDbg (https://developer.microsoft.com/en-us/windows/downloads/windows-10-sdk)



Setting up the Debugger

◎ Debugger is the machine form where we will be watching the Debugee

 Download WinSDK and install WinDbg (https://developer.microsoft.com/enus/windows/downloads/windows-10-sdk)



The Windows 10 SDK (10.0.15063.468) provides the late apps. The Windows 10 SDK, when used in conjunction v building apps for Windows- allowing you to take advar Creators Update.

In addition to targeting the Windows 10 Creators Upda as well as desktop apps on all versions of Windows 10. Windows 7 SP1, Windows Server 2016, and Windows Sv Phone SDKs, see the Archive page.

Note: Windows 10 app development targeting Window not be discovered by previous versions of Visual Studic

For your convenience you can either download and run



Select the features you want to install Click a feature name for more information.

Windows Software Development Kit - Windows 10.0.15063.468

Windows Performance Toolkit	Debugging Tools for Window	WS
Debugging Tools for Windows	Size: 277.5 MB	
Application Verifier For Windows	Kernel and user-mode debuggers as well	as help and tips
.NET Framework 4.7 Software Development Kit	for using Debugging Tools for Windows.	
Windows App Certification Kit		
MSI Tools		
Windows SDK Signing Tools for Desktop Apps		
Windows SDK for UWP Managed Apps		
Windows SDK for UWP C++ Apps		
Windows SDK for UWP Apps Localization		
Windows SDK for Desktop C++ x86 Apps		
Windows SDK for Desktop C++ amd64 Apps		
Windows SDK for Desktop C++ arm Apps		
Windows SDK for Desktop C++ arm64 Apps	Estimated disk space required: Disk space available:	277.5 MB 85.8 GB
	Back	tall Cancel



×

Setting up the Debugger

Adding the Debbuging Symbols (<u>https://en.wikipedia.org/wiki/Symbol_(programming)</u>)
 Assign a new variable called _NT_SYMBOL_PATH

System Properties	× Environment Varia	bles ×	
You must be logged on as an Administrator to make most of these changes.	User variables for	User3	
Performance	Variable	Value	
Visual effects, processor scheduling, memory usage, and virtual memory	OneDrive	C: \Users\User3\OneDrive	
Settings	TEMP	%USERPROFILE%\AppData\Local\Temp %USERPROFILE%\AppData\Local\Temp	
User Profiles		New Edit Delete	
Settings	Edit System Varia	ble	×
Startup and Recovery	Variable name:	_NT_SYMBOL_PATH	
System startup, system failure, and debugging information	Variable value:	SRV*C:\Symbols*https://msdl.microsoft.com/download/symbols	ols
Settings			OK Cancel
Environment Variables		New Edit Delete	
OK Cancel Apply		OK Cancel	



Setting up the Debugee

Adding one more option in a boot menu using bcdedit

- ▲ Copy the current settings into a new entry called "ForDebug"
- ▲ Enable debugging on the created entry "ForDebug"
- ▲ Verify the debugging interface settings

C:\.bcdedit /cop	v {current} /d "ForDebug"
The entry was su	ccessfully copied to {346d1950-9395-11e7-9bde-00505623a295}
C:\∙bcdedit /deb	ug {346d1950-9395-11e7-9bde-00505623a295} on
The operation co	mpleted successfully.
C:\.bcdedit /dbg	settings
debugtype	Serial
debugport	1
baudrate	115200
The operation co	mpleted successfully.



O Debugger and Debugge will be communicating via Serial Port COM1, that will be emulated in the host system by a Named Pipe (<u>https://en.wikipedia.org/wiki/Named_pipe</u>)

◎ Debugger and the debuggee need to have the same pipe name set

 Debugger will be creating the pipe, while the Debuggee will be connecting to the existing one (Debugger needs to run first)

▲ Debugger config

\\.\pipe\com_1	
This end is the client.	
The other end is a virtual m	achine.



O Debugger and Debugge will be communicating via Serial Port COM1, that will be emulated in the host system by a Named Pipe (<u>https://en.wikipedia.org/wiki/Named_pipe</u>)

◎ Debugger and the debuggee need to have the same pipe name set

 Debugger will be creating the pipe, while the Debuggee will be connecting to the existing one (Debugger needs to run first)

▲ Debugee config





Testing the connection

▲ File -> Kernel Debug

File	Edit	View	Debug	Window	Help
	Open	Source	File		Ctrl+0
	Close	Current	t Window	1	Ctrl+F4
	Open	Executa	able		Ctrl+E
	Attack	h to a Pi	rocess		F6
	Open	Crash E	Dump		Ctrl+D
	Conn	ect to R	emote Se	ssion	Ctrl+R
	Conn	ect to R	emote St	ub	
	Kerne	Debug	hu		Ctrl+K

Choosing debugging interface

ernel	Debugg	ing				?	×
NET	USB	1394	Local	COM			
Keme Baud 1152 Port: com1	Idebugg Rate: 00	ing over	a COM p	ort or virtual serial] Pipe] Reconnect esets:	device		
				ОК	Cancel	He	łp

Debugee connects back to the Debugger

Microsoft (R) Windows Debugger Version 10.0.15063.468 AMD64 Copyright (c) Microsoft Corporation. All rights reserved. Opened \\.\com1 Waiting to reconnect... Connected to Windows 10 15063 x64 target at (Thu Sep 7 00:53:29.003 2017 (UTC - 7:00)), ptr64 TRUE Kernel Debugger connection established. ************* Symbol Path validation summary *************** Response Time (ms) Location Deferred SRV*C:\Symbols*https://msdl.microsoft.com/download/symbols Symbol search path is: SRV*C:\Symbols*https://msdl.microsoft.com/download/symbols Executable search path is: Windows 10 Kernel Version 15063 MP (1 procs) Free x64 Built by: 15063.0.amd64fre.rs2 release.170317-1834 Machine Name: Kernel base = 0xfffff800`1d299000 PsLoadedModuleList = 0xfffff800`1d5e55c0 System Uptime: 0 days 0:00:00.070



◎ Testing the connection

▲ Interrupting the Debugee, clicking Debug -> Break

Debug Window Help	
Go	F5
Go Unhandled Exception	
Go Handled Exception	
Restart	Ctrl+Shift+F5
Stop Debugging	Shift+F5
Detach Debuggee	
Break	Ctrl+Break

▲ kd prompt shows -> Debugger is in control of the Debugee

* THIS IS	NOT A BUG OR A S	SYSTEM CRASH	*
*			*
* If you did not intend to H * press the "Enter" key now. * does, press "g" and "Enter *	This message m " again.	bugger, press the "g" key, hight immediately reappear.	then * If it * *
******	******	******	*******
nt!DbgBreakPointWithStatus: fffff803`f777dfd0 cc kd>	int 3		
4			



© Examine EPROCESS Structure (https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/eprocess)

kd> ! process 0 0

**** NT ACTIVE PROCESS DUMP ****

PROCESS ffff930fa1299040

SessionId: none Cid: 0004 Peb: <u>00000000</u> ParentCid: <u>0000</u> DirBase: 001aa000 ObjectTable: ffffa60a88c03280 HandleCount: 1. Image: System

kd> dt nt	! EPROCESS ffff930fa	a1299040	
+0x000	Pcb :	KPROCESS	
+0x2d8	ProcessLock :	EX PUSH LOCK	
+0x2e0	UniqueProcessId :	0x0000000`0000004 Void	
+0x2e8	ActiveProcessLinks	: LIST ENTRY [0xfffff803`f7951fe0 - 0xfffff803`f7951fe0]
+0x2f8	RundownProtect :	EX RUNDOWN REF	



◎ List all processes

kd> !process 0 0
***** NT ACTIVE PROCESS DUMP ****
PROCESS ffff930fal299040
SessionId: none Cid: 0004 Peb: 00000000 ParentCid: 0000
DirBase: 001aa000 ObjectTable: ffffa60a88c03280 HandleCount: 2723.
Image: System

PROCESS ffff930fa2ea0400

SessionId: none Cid: 027c Peb: <u>5770e24000</u> ParentCid: <u>0004</u> DirBase: 02ec6000 ObjectTable: ffffa60a88ed2ec0 HandleCount: 52. Image: smss.exe

Show process full details (wordpad.exe)

kd>	!process 0 / wordpad.exe	
PRO	CESS ffff930fa4ca17c0	
	SessionId: 1 Cid: 01fc Peb:	b431ae6000 ParentCid: 1670
	DirBase: 147d00000 ObjectTable:	ffffa60a942ead00 HandleCount: 338.
	Image: wordpad.exe	
	VadRoot ffff930fa34e19b0 Vads 41	5 Clone 0 Private 2329. Modified 62037. Locked 0.
	DeviceMap ffffa60a903e7050	
	Token	ffffa60a947c6060
	ElapsedTime	00:00:33.262
	UserTime	00:00:00.000
	KernelTime	00:00:00.000
	OuotaPoolUsage [PagedPool]	401776
	QuotaPoolUsage [NonPagedPool]	56632
	Working Set Sizes (now, min, max)	(10739, 50, 345) (42956KB, 200KB, 1380KB)
	PeakWorkingSetSize	10924
	VirtualSize	2097370 Mb
	PeakVirtualSize	2097378 Mb
	PageFaultCount	75634
	MemoryPriority	BACKGROUND
	BasePriority	8
	CommitCharge	3080



References

InfoSec

http://resources.infosecinstitute.com/windows-architecture-and-userkernel-mode/#gref

• Wikipedia

https://en.wikipedia.org/wiki/Architecture_of_Windows_NT

• WinDbg

http://www.windbg.org/

