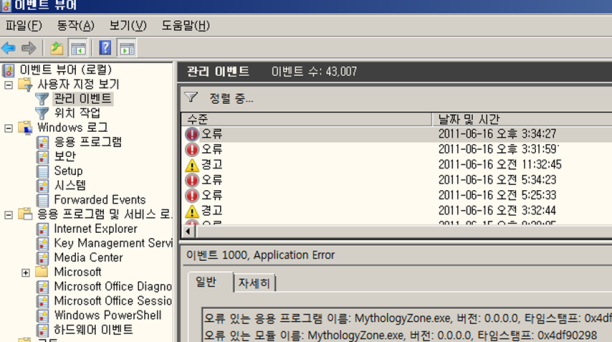
|  |  |
| --- | --- |
| ..symfix C:\SymStore  .sympath+ c:\SymStore  .reload /f |  |
| !sym noisy .reload /f !analyze -v |  |
| Lm  Lmvm myapp |  |
| .srcpath  .srcpath+ d:\Myapp  P // step over  T // step into  Locals // alt+3  Dv //로컬 변수. |  |
| dump -mfh d:\asdf.dmp  qd | 덤프생성.  프로세스 Debug종료. |
| ~\*kb  ~2s  Lsa eip  !address 07a4bff8  !handle  .ecxr |  |
|  |  |
| @rem http://support.microsoft.com/kb/286350  @mkdir c:\dump  @mkdir c:\dump\%1  adplus -quiet -crash -pn %1 -o c:\dump\%1  @rem adplus -crash -pmn %1 -o c:\dump\%1 | adplus |

이벤트뷰어에서 덤프파일 생성시 로그



**WinDbg**

<http://blog.naver.com/PostView.nhn?blogId=saram95&logNo=90093651287>

TaskMgr

|  |  |
| --- | --- |
| .symfix C:\SymStore  .sympath+ c:\SymStore  .sympath+ C:\OsSymbols  .symfix c:\SymStore  .sympath + c:\SymStore  .reload  SRV\* c:\ossymbols \*http://msdl.microsoft.com/download/symbols;c:\symstore; |  |

|  |  |
| --- | --- |
| **일반 명령** | r register  d memory  e memory 수정 |
| **메타명령** | .sympath |
| **확장명령.** | !sym noisy |

[www.osronline.com](http://www.osronline.com)

# 디펄트 덤프생성기 세팅

|  |
| --- |
| AeDebug원본-Win7.reg Windows Registry Editor Version 5.00  [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug]  "UserDebuggerHotKey"=dword:00000000  "Debugger"="\"C:\\Windows\\system32\\VSJitDebugger.exe\" -p %ld -e %ld"  [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug\AutoExclusionList]  "DWM.exe"=dword:00000001 |
| AeDebug-WinDbg용-Win7.reg Windows Registry Editor Version 5.00  [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug]  "UserDebuggerHotKey"=dword:00000000  "Debugger"="\"C:\\Program Files\\Debugging Tools for Windows (x64)\\ntsd.exe\" -p %ld -c \".dump /f /u c:\\Dump\\mydump.dmp;q\""  "Auto"="1"  [HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug\AutoExclusionList]  "DWM.exe"=dword:00000001 |

# 심볼로드

SRV\*C:\OsSymbols\*http://msdl.microsoft.com/download/symbols

.symfix c:\OsSymbols

.reload

.sympath

.sympath+ D:\test\book-cd-WinDbg로 쉽게 배우는 windows debugging

.sympath+ SRV\*C:\OsSymbols\*http://msdl.microsoft.com/download/symbols

.sympath+ D:\test\book-cd-WinDbg로 쉽게 배우는 windows debugging\Ch4\Bin

# 심볼 스토어

AddMySym.bat test.pdb

mkdir c:\SymStore

symstore add /f %1 /s c:\SymStore /t mech\_lib

AddMySym.bat D:\test\book-cd-WinDbg로 쉽게 배우는 windows debugging\Ch2\Bin\MyApp.pdb

# MyApp.exe 디버깅

File > Open Excutable메뉴

|  |  |
| --- | --- |
| g | Debug go |
| bp MyApp!CMyAppDlg::OnBreakPoint |  |
| bl | 브레이크포인트 리스트 |
| bd 0 | breakpoint disable |
| be 0 | enable |
| bc 0 | clear |
| bc \*  bc 3-5  bc 2,7,8 |  |
| bu | bp와 동일. 상태가 저장됨 |

### 콜스택

K //콜스택 alt+6

Kb // 파라미터도 포함한 콜스택

### 소스보기

.srcpath

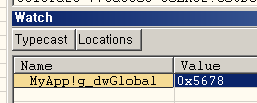
.srcpath+ d:\Myapp

P // step over

T // step into

Locals // alt+3

Dv //로컬 변수.



db MyApp!g\_dwGlobal // 전역변수보기

0:000:x86> db MyApp!g\_dwGlobal

0042d0a0 78 56 00 00 25 73 28 25-64 29 00 00 5c 00 00 00 xV..%s(%d)..\...

0042d0b0 2e 73 79 73 00 00 00 00-47 65 74 4d 6f 64 75 6c .sys....GetModul

0042d0c0 65 50 61 74 68 00 00 00-4d 79 44 72 76 00 00 00 ePath...MyDrv...

0042d0d0 52 65 67 69 73 74 65 72-44 72 69 76 65 72 20 45 RegisterDriver E

0042d0e0 72 72 6f 72 00 00 00 00-4d 79 44 72 76 00 00 00 rror....MyDrv...

0042d0f0 4d 79 44 72 76 00 00 00-53 74 61 72 74 44 72 76 MyDrv...StartDrv

0042d100 69 65 72 20 45 72 72 6f-72 00 00 00 53 74 61 72 ier Error...Star

0042d110 74 00 00 00 4d 79 44 72-76 00 00 00 53 74 6f 70 t...MyDrv...Stop

0:000:x86> dd MyApp!g\_dwGlobal

0042d0a0 00005678 25287325 00002964 0000005c

0042d0b0 7379732e 00000000 4d746547 6c75646f

0042d0c0 74615065 00000068 7244794d 00000076

0042d0d0 69676552 72657473 76697244 45207265

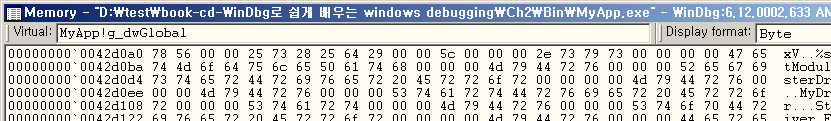
0042d0e0 726f7272 00000000 7244794d 00000076

0042d0f0 7244794d 00000076 72617453 76724474

0042d100 20726569 6f727245 00000072 72617453

0042d110 00000074 7244794d 00000076 706f7453

### 메모리창 alt+5



### 디버기 세팅

Boot.ini // xp

Bcdedit.exe // 비스타

Bootcfg.exe// IA64용 윈2003

# 덤프파일분석.

D:\test\book-cd-WinDbg로 쉽게 배우는 windows debugging\Ch3\Dump\UserMode Crash

.ecxr //예외 정보

K //스택

0:000> k

\*\*\* Stack trace for last set context - .thread/.cxr resets it

ChildEBP RetAddr

WARNING: Stack unwind information not available. Following frames may be wrong.

0012f8d4 00401c06 MyApp+0x1baf

0012f8f4 0041371b MyApp+0x1c06

0012f904 004138a8 MyApp+0x1371b

0012f934 00413c98 MyApp+0x138a8

0012f958 0041618e MyApp+0x13c98

### 심볼찾기.

Lm

0:000> lm

start end module name

00400000 00437000 MyApp C (no symbols)

4b540000 4b55a000 imekr61 (deferred)

5a480000 5a4b8000 uxtheme (deferred)

7d5a0000 7dd9c000 shell32 (deferred)

### Lmvm // 해당 모듈의 심볼정보.

0:000> lmvm MyApp

start end module name

00400000 00437000 MyApp C (no symbols)

Loaded symbol image file: MyApp.exe

Image path: Z:\WinDbgCD\Ch2\Bin\MyApp.exe

Image name: MyApp.exe

Timestamp: Tue Jun 02 23:41:45 2009 (4A253A29)

CheckSum: 00000000

ImageSize: 00037000

File version: 1.0.0.1

Product version: 1.0.0.1

File flags: 0 (Mask 3F)

File OS: 4 Unknown Win32

File type: 1.0 App

File date: 00000000.00000000

Translations: 0412.04b0

CompanyName:

ProductName: MyApp 응용 프로그램

InternalName: MyApp

OriginalFilename: MyApp.EXE

ProductVersion: 1, 0, 0, 1

FileVersion: 1, 0, 0, 1

PrivateBuild: 1, 0, 0, 1

SpecialBuild: 1, 0, 0, 1

FileDescription: MyApp MFC 응용 프로그램

LegalCopyright: Copyright (C) 2008

LegalTrademarks: Copyright (C) 2008

Comments: Copyright (C) 2008

### 심볼 맞추기

.symfix c:\SymStore

.sympath + c:\SymStore

.reload

### 심볼패스 설정

Set \_NT\_SYMBOL\_PATH=SRV\*C:\Symbol\*http://msdl.microsoft.com/download/symbols

또는

Windbg –y SRV\*C:\Symbol\*http://msdl.microsoft.com/download/symbols

또는 File > Warkspace로 저장.

### 심볼로딩 자세히 보기.

!sym noisy

!sym quiet

# 잘못된 메모리 사용 검출.

Gflags.exe

GFlags –I LabApp.exe +hpa

*This dump file has an exception of interest stored in it.*

*The stored exception information can be accessed via .ecxr.*

*(1034.f2c): Access violation - code c0000005 (first/second chance not available)*

*LabApp!CLabAppDlg::OnFreedheapaccessBtn+0x27:*

*00401687 c701ffffffff mov dword ptr [ecx],0FFFFFFFFh ds:002b:07a4bff8=????????*

0:000:x86> lsa eip

213: (SomeStructWhichNotInitialized\*)malloc(sizeof(SomeStructWhichNotInitialized));

214:

215: free(pInitializedStruct);

216:

> 217: **pInitializedStruct->MemoryBuffer = (PVOID)0xffffffff**;

218: }

!address *07a4bff8*

# 프로세스 CPU 100%점유 문제

### Process Explorer

### Perfmon.msc

: 데이터 수집기 집합 > 사용자 정의 > 새로 만들기 > “데이터 수집기 집합” >템플릿… >

### Kernrate Viewer (KrView) executable and documentation

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=d6e95259-8d9d-4c22-89c4-fad382eddcd1>

(xp , win2000)

c:\>Kernrate\_i386\_XP.exe

-----------------------------

Results for Kernel Mode:  
-----------------------------

OutputResults: KernelModuleCount = 135  
Percentage in the following table is based on the Total Hits for the Kernel

Time   13080 hits, 25000 events per hit --------  
 Module                                Hits   msec  %Total  Events/Sec  
amdk7                                  7381      35718    56 %     5166162  
***nv4\_disp***                               3834      35718    29 %     2683520

Kernrate\_i386\_XP.exe -z ntoskrnl

마지막으로 자신이 만든 모듈의 내부를 알고 싶다면

kernrate -z module -j <module심볼 패스>

**Windows Performance Toolkit**

<http://msdn.microsoft.com/en-us/performance>

Vista sp1, windows 2008 에대한 성능측정 도구.

x86, x64, ia64 버전별 설치.

W[indows 7 SDK (contains WPT 4.6)](http://www.microsoft.com/downloads/details.aspx?FamilyID=c17ba869-9671-4330-a63e-1fd44e0e2505) 에 포함되어 있음.

설명 문서 : <http://okprince.egloos.com/378793>

설명 동영상 : <http://www.microsoftpdc.com/2009/CL16>

설치 : <http://blog.naver.com/PostView.nhn?blogId=hakunamata2&logNo=90079315511>

## xperf.exe // 콘솔모드 성능측정.

xperf -on DiagEasy

xperf –d c:\test.etl

xperfview.exe // \*.etl파일 보기.

xperf -providers K // DiagEasy외의 더 많은 Flag확인.

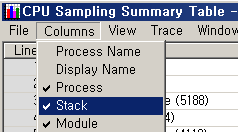
xperf -help symbols //심볼관련 환경변수 세팅정보 출력.

## Stack Tracing

xperf –help stackwalk

xperf -on latency -stackwalk Profile

1. Run the command, xperf -on latency -stackwalk Profile.
2. Run the application that you wish to analyze, then
3. You can end the trace by using the regular xperf –d <filename>.etl command.
4. Load the trace in the viewer and then select the **Load Symbols** from the Trace drop down menu.
5. Once the symbols are loaded, select an interesting region on the CPU sampling graph.
6. Right click and select **Summary Table**.



만약 다음과 같은 메시지가 나오면 레지스트리를 수정하자.

C:\Users\user>xperf -on latency -stackwalk Profile

xperf: warning: This system is not fully configured for x64 stack tracing.

Please modify the registry under:

**HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management**

and set the value:

**DisablePagingExecutive (REG\_DWORD) = 1**

Then reboot before retrying tracing.

## 심볼 캐쉬 폴더세팅.

Set \_NT\_SYMCACHE\_PATH=SRV\*c:\OsSymbols\*http://msdl.microsoft.com/download/symbols;c:\SymStore

**Visual Studio 2010에서 제공하는 Profiler**

# Thread Hang

~\*kb //모든 스레드(~\*)의 콜스텍.

~2s // 2번스레드로 제어변경. Set current thread

Lsa eip // 현제실행중인 명령주소(eip)의 소스코드 보기.

# 데드락검출

ProcessHangApp.exe

!handle // 프로세스의 핸들정보