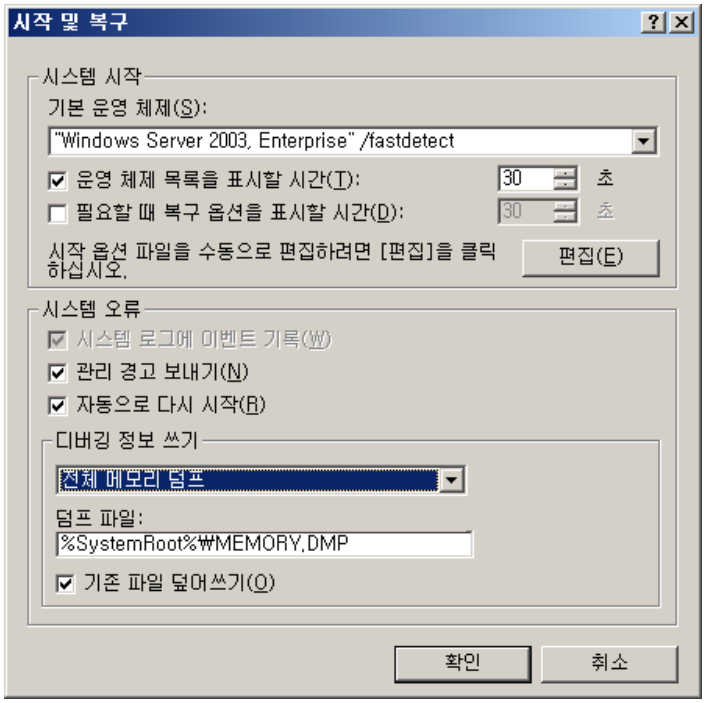
Memory.dmp 파일 만드는 방법 및 확인 방법 **작성자 : 이완주**

시스템에 장애가 발생하게 되면 우리는 덤프를 분석한다고 말을 한다. 그러나 실제로 덤프를 분석할 능력을 가진 사람은 많지 않다.
그러나 여기서 기본적인 덤프 생성 방법을 배우고 뒤에 실제 문제를 해결 할 때 사용 방법을 익힘으로써 시스템 정보 확인 차원의 덤프 분석은 가능 할 거 같다.
물론 덤프를 통해 장애를 처리하기 위해서는 많은 선수 지식이 필요하고 많은 노력이 뒤 따라야만 한다.

다음과 같은 경우에 덤프를 사용하여 문제를 해결 할 수 있다.
- 프로세스가 응답을 중지하는 경우
- 프로세스가 CPU 를 단일 프로세서 컴퓨터에서 100%, 이중 프로세서 컴퓨터에서 50%, 사중 CPU 컴퓨터에서 25% 사용할 경우
- 프로세스가 예기자 않게 충돌하거나 종료될 경우

메모리 덤프를 만드는 여러가지 방법
덤프를 만들게 되면 저장되는 기본 위치는 %SystemRoot% 위치이며 위치는 바꿀 수 있다.

마우스 오른쪽 단추로 내 컴퓨터를 누른 다음 속성(Windows 2000 의 경우, 등록 정보) 고급 탭을 누른 다음 시작 및 복구 에서 디버깅 정보 쓰기를 누른 다음 전체 메모리 덤프, 커널 메모리 덤프 또는 작은 메모리 덤프 중에서 선택.



디버깅 정보 쓰기에서 시스템이 예상치 않게 멈출 경우 Windows 에서 기록할 정보 유형을 선택합니다.

작은 메모리 덤프(64KB)
문제를 확인할 수 있도록 돕는 가장 작은 양의 정보를 기록합니다. 이 옵션을 사용하려면 컴퓨터의 부팅 볼륨에 2MB 이상의 페이징 파일이 있어야 합니다. 이 옵션을 선택하면 Windows 는 시스템이 예상치 않게 멈출 때마다 64KB 크기의 새로운 파일을 만듭니다. 이러한 파일에 대한 기록은 작은 덤프 디렉토리 아래에 나열된 디렉터리에 저장됩니다.
커널 메모리 덤프
커널 메모리만 기록하므로 작은 메모리 덤프보다 더 많은 정보를 저장하지만 시스템이 예상치 않게 멈출 때 전체 메모리를 덤프하는 것보다 짧은 시간 내에 작업을 완료할 수 있습니다. 파일은 덤프 파일 아래에 나열된 디렉터리에 저장됩니다. 이 옵션을 선택하는 경우 부팅 볼륨에 충분한 크기의 페이징 파일이 있어야 합니다. 필요한 크기는 컴퓨터의 RAM 크기에 따라 다릅니다. 커널 메모리 덤프의 경우 사용할 수 있는 최대 공간 크기는 2,060MB 입니다. 다음 표는 페이징 파일 크기에 대한 지침을 제공합니다.

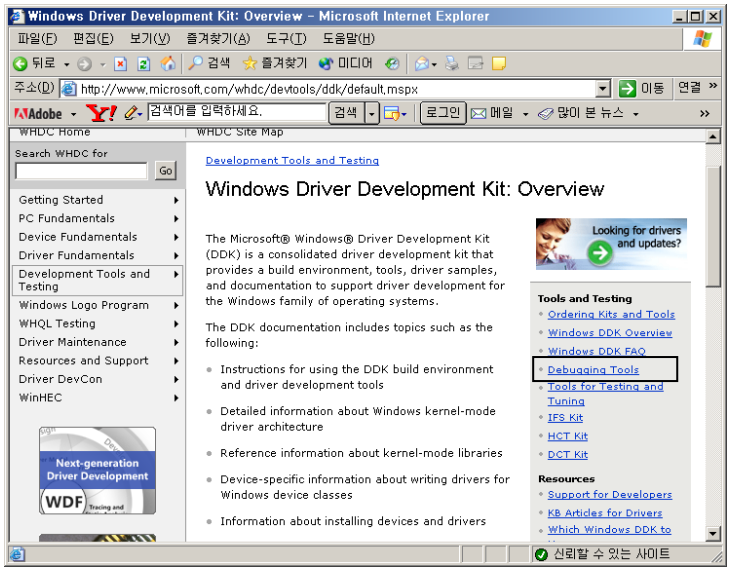
RAM 크기	페이징 파일 최소 크기
256MB-1,373MB	RAM 크기의 1.5 배
1,374MB 이상	2,060MB(커널 메모리 덤프의 최대 데이터 양)

전체 메모리 덤프
RAM 크기가 2GB 이상인 컴퓨터에서는 사용할 수 없습니다. 시스템이 예상치 않게 멈출 때 시스템 메모리의 전체 내용을 기록합니다. 이 옵션을 선택하는 경우 실제 RAM 에 1MB 를 더한 크기를 모두 보관하기에 충분한 페이징 파일이 부팅 볼륨에 있어야 합니다. 파일은 덤프 파일 아래에 나열된 디렉터리에 저장됩니다.

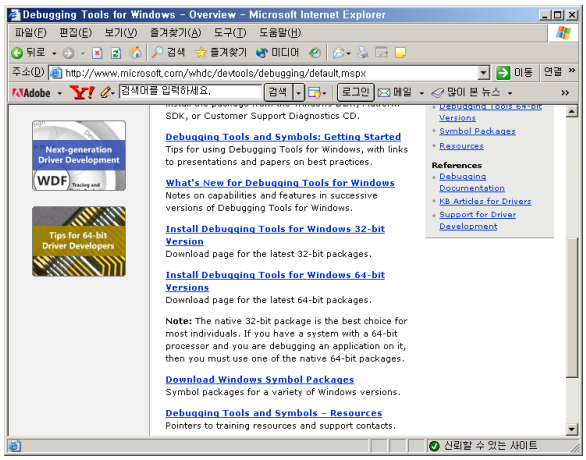
Windbg

가장 많이 사용되는 GUI 도구이며 User Mode, Kernel Mode Debug 등이 가능하다.

http://www.microsoft.com/ddk
해당 사이트에서 Debug Tool 다운로드 함



해당 사이트에서 OS 의 Version 에 맞게 다운 받으면 됨.
최신버전 확인해서 받으면 됨.

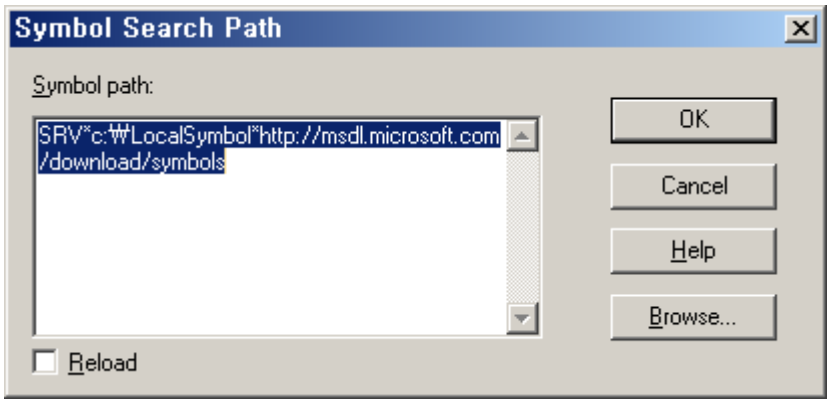


다운받고 설치 하면 아래의 위치에

C:₩Program Files₩Debugging Tools for Windows 설치가 됨

Windbg 에 가장 중요한 것은 Symbol 을 설정 하여야 한다.
http://support.microsoft.com/default.aspx?scid=kb;ko;315263

File -> Symbol File Path 에서 아래와 같이 지정 해야 한다.



Symbol 을 저장해 놓은 서버를 Symbol Store 라고 함
Symbol Server 라고 하지 않음

Private Symbol Store (마이크로소프트 내부 직원용) ₩₩symbols₩symbols
가 있으며 해당 소스 코드 및 소스 코드의 몇 번째 라인인지도 나타남
Public 에는 나타나지 않는 정보가 나타나게 됨.

Public Symbol Store (일반인이 접할 수 있는 심볼)
http://msdl.microsoft.com/download/symbols

srv* 을 Symbol Server 라고 하며 해당 위치로 변경하여 해당 Symbol 을 Download 하게 함
srv*로컬캐쉬 위치주소*심볼스토어 위치

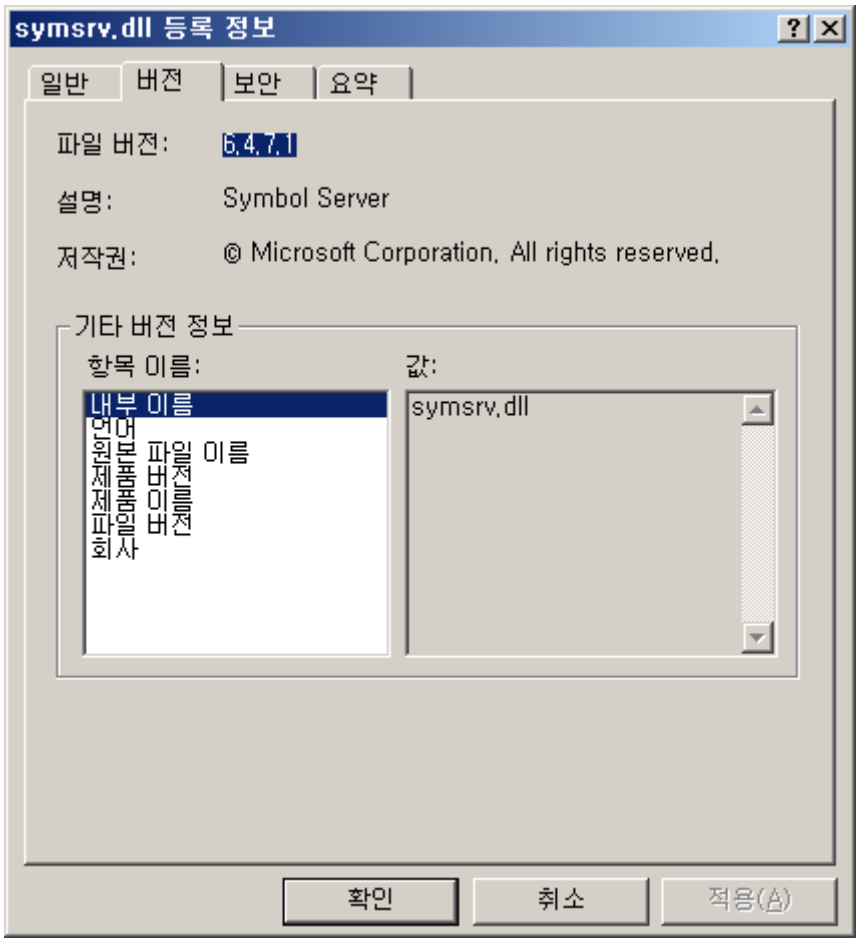
예) srv*c:₩LocalSymbols*http://msdl.microsoft.com/download/symbols
위에서 c:₩symbolcache local cache 위치 (임의의 값을 설정한 것임)

즉 Symbol store 를 지정할 경우는 반드시 앞에 srv*를 붙여야 한다.
물론 로컬일 경우는 생략 가능
캐쉬를 하지 않으면 매번 해당 서버에서 다운 받기 때문에 속도가 느릴 수 있다.
이것도 재산이므로 캐쉬를 두는 것이 좋다.

예 c:₩localsymbol 이라면 srv* 생략가능

C:₩Program Files₩Debugging Tools for Windows₩symsrv.dll

이 Dll 이 srv* 역할을 하는 Symbol Server 라고 함



Symbol Server 가 Symbol Store 에 가서 Symbol 을 가져오는 역할을 하게 됨

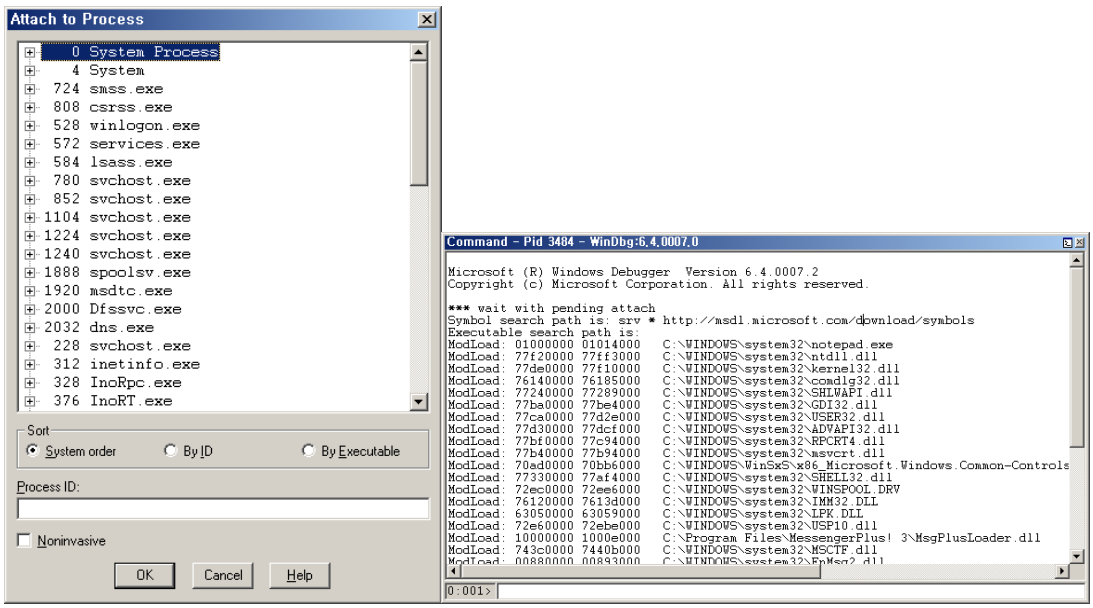
Symbol 은 상당히 중요한 역할을 하는 것이므로 반드시 알아 두어야 함.

심볼을 설정하였다면 로컬 컴퓨터의 특정 프로세스의 예를 들어 Notepad.exe 와 같이 로컬 컴퓨터의 실행되고 있는 프로세스의 값을 확인 할 수 있다.

이 방법은 굳이 덤프를 만들지 않고 지금 실행하고 있는 프로세스의 값을 확인 하고자 할 때 유용하게 사용할 수 있다.

Windbg 도구에서 현재 실행하고 있는 프로그램의 정보를 확인하고 싶다면..

File -> Attach to Process 에서 살펴보면 된다.



위의 화면은 실제 Notepad.exe 파일을 실행한 결과를 Windbg 로 실행한 결과 이다.

Windbg 는 그 밖에도 기존에 덤프 파일을 불러와 분석 할 때도 유용하게 사용되는 도구이다.

Windbg 를 설치 하게 되면 C:₩Program Files₩Debugging Tools for Windows 에는 아래의 도구는 명령어 기반의 도구들이 설치 되며 명령어 기반으로 관리 할 때 사용되는 도구들이다.

Command Tool

kd.exe : Kernel Mode Debug

cdb.exe : User Mode Debug

ntst.exe : User Mode Debug

Userdump.exe
http://support.microsoft.com/default.aspx?scid=kb;ko;241215
UserDump 및 해당 설명서는 OEM Support Tools 패키지의 일부이며. 다음 웹 사이트에서 복사본을 구할 수 있음.
http://download.microsoft.com/download/win2000srv/Utility/3.0/NT45/EN-US/Oem3sr2.zip

Userdump.exe 도구를 사용하면 예외 오류와 함께 종료되거나 더 이상 응답하지 않는 프로세스의 사용자 덤프를 생성할 수 있습니다.

일반적으로 LSASS.EXE 의 과도한 사용으로 인한 문제가 발생하는 경우
LSASS.EXE 는 인증과 관련된 문제들 예를 들어 특정시간에 도메인 인증이 집중되거나 아니면 2 대의 DC 가 NLB 역할을 제대로 하지 못하는 경우 등에 이러한 현상이 발생할 수 있으며 이러한 현상이 나오는 경우 정확한 분석을 위해 Userdump.exe 명령어를 실행하여 메모리 덤프를 통해 분석할 수 있게 된다.

Adplus

ADPlus는 콘솔 기반의 Microsoft Visual Basic 스크립트로, Microsoft CDB 디버거를 자동화하여 하나 이상의 프로세스 디버그 출력을 포함하는 메모리 덤프와 로그 파일을 생성

IIS와 관련된 문제 등의 경우에 많이 이용되는 툴이다.

ADPlus는 프로세스나 응용 프로그램이 응답을 중지하거나 예기치 않게 종료되었을 때 문제를 해결할 수 있도록 Microsoft 고객 기술지원부(PSS)에서 제공하는 도구입니다. ADPlus(ADPlus.vbs)는 Microsoft Internet Information Server(IIS) Exception Monitor(6.1/7.1)와 사용자 모드 프로세스 덤프(User Mode Process Dump)를 대체할 수 있는 도구로 자주 사용됩니다. 이러한 두 도구는 Microsoft Windows DNA 환경에서 프로세스가 응답을 중지하거나 예기치 않게 종료되는 이유를 찾기 위해 PSS에서 자주 사용하는 개별 도구입니다.

Microsoft Debugging Tools for Windows에 포함되어 있음.
C:₩Program Files₩Debugging Tools for Windows₩adplus.퓬

http://support.microsoft.com/default.aspx?scid=kb;ko;286350
명령어에 대한 자세한 사용 방법은 위의 사이트 참조

키보드를 이용한 강제로 메모리덤프 만들기

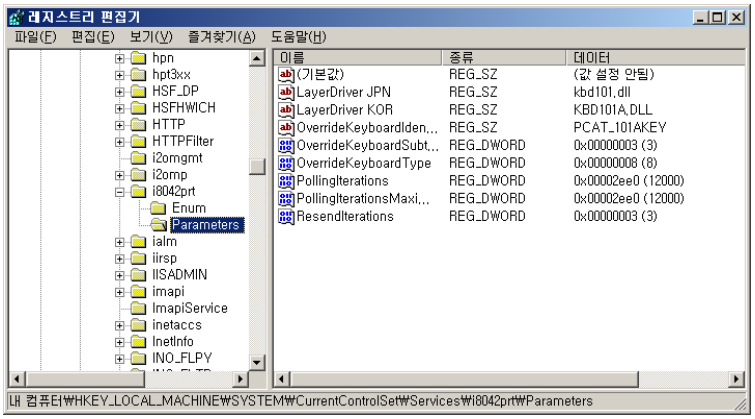
http://support.microsoft.com/?id=244139

키보드 스페이스 바 오른쪽에 있는 Ctrl 키와 함께 Scroll Lock 를 두번 누르게 되면
키보드 에러로 인식 시켜 강제로 덤프를 만드는 방법으로 강제 덤프 생성하는 방법이다.
단 아래의 단계는 USB 키보드를 사용하는 컴퓨터와 같은 레거시가 없는 컴퓨터에서는
작동하지 않는다. 이러한 컴퓨터의 경우 디버거를 연결해서 직접 모니터링을 하여야 한다.

아래의 사항은 레지스트리를 변경하는 방법이다.

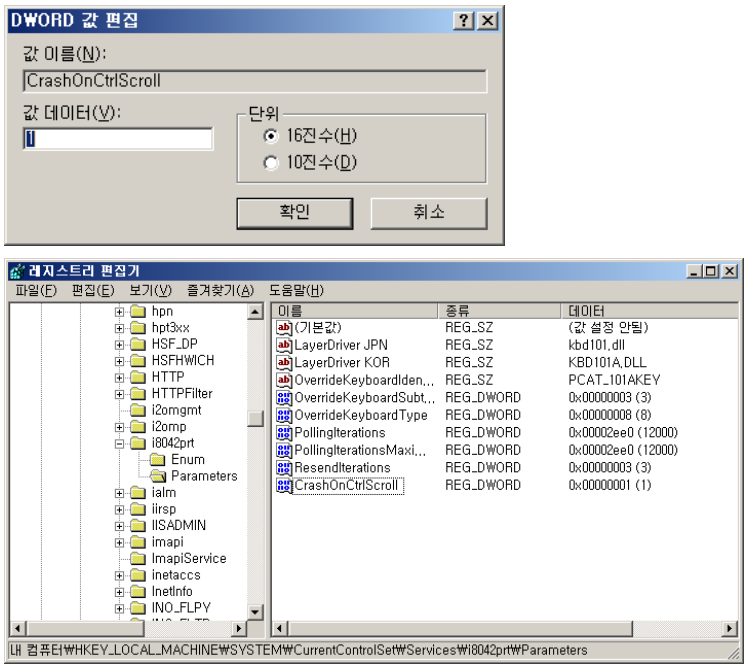
레지스터 편집기를 실행한다. (regedt32.exe 혹은 regedit.exe)

2. HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩i8042prt₩Parameters
키를 찾는다.



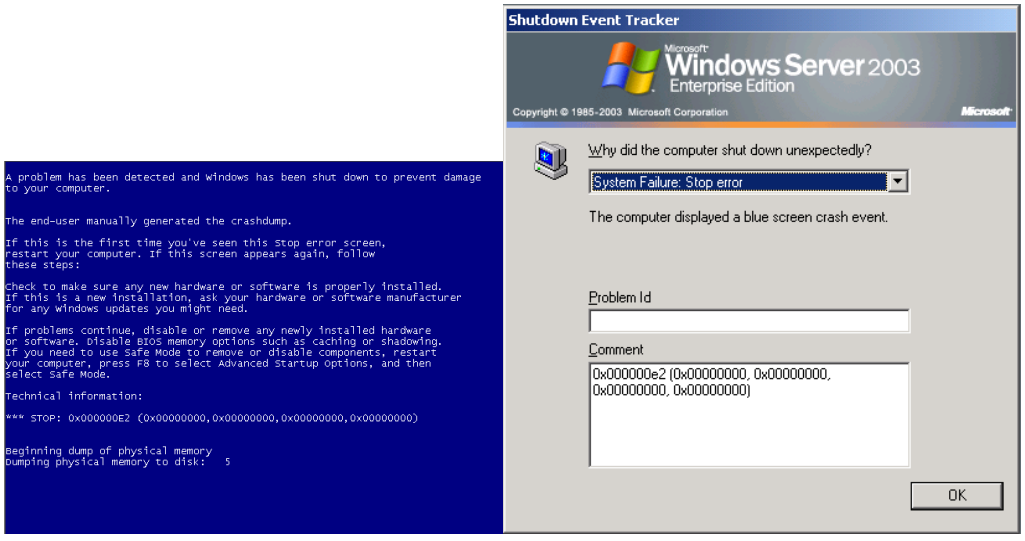
편집 -> 새로만들기 -> DWORD

CrashOnCtrlScroll 값 1을 추가 한다.



강제 메모리 덤프를 생성하기 위해서는 레지스트리 키를 바꾸고 컴퓨터를 리부팅하여야만 한다.

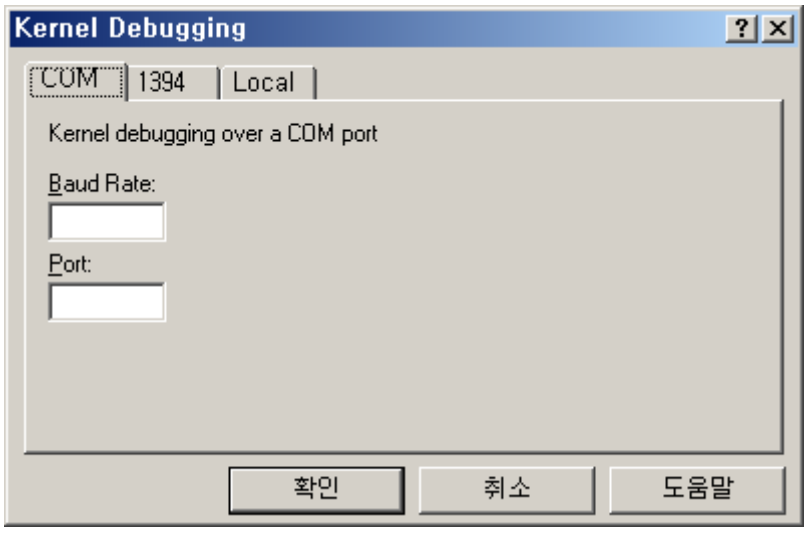
리부팅 후 Ctrl 키를 누른 상태에서 Scroll Lock를 두번 누르면 아래와 같이 화면이 바뀌면서 Memory.dmp 파일을 만들게 된다.



로그온 후 키보드 관련 시스템 장애가 발생했다고 알려주는 이벤트 메시지가 나타나게 된다.

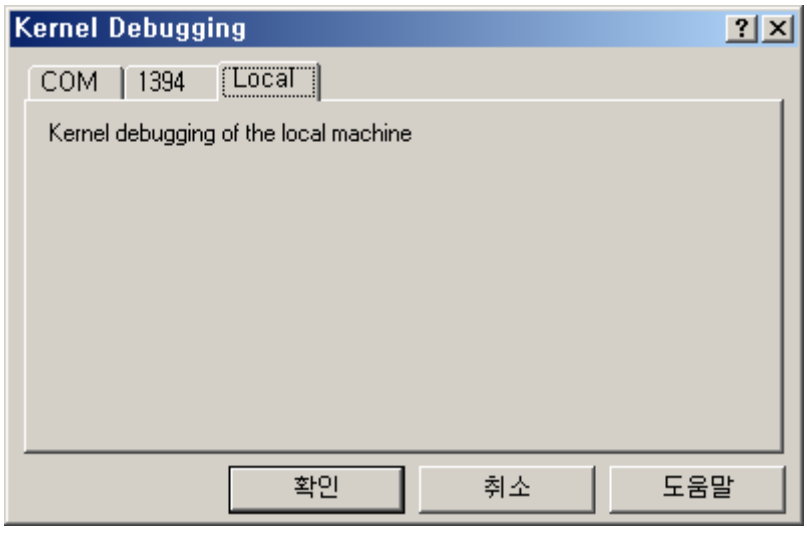
Kernel Debug 을 통해 Local Debug 방법

File -> Kernel Debug



COM, 1394 2 개는 원격에서 시리얼로 접근하여 처리 할 경우 사용

여기서는 Local 을 선택



로컬은 실제 debug 는 할 수 없고 정보만 확인 할 수 있음

Windows XP 이상에서만 이 도구를 통해서 로컬 사용 가능

Windows 2000 이라면 livekd tool 을 이용하여 정보를 확인할 수 있음

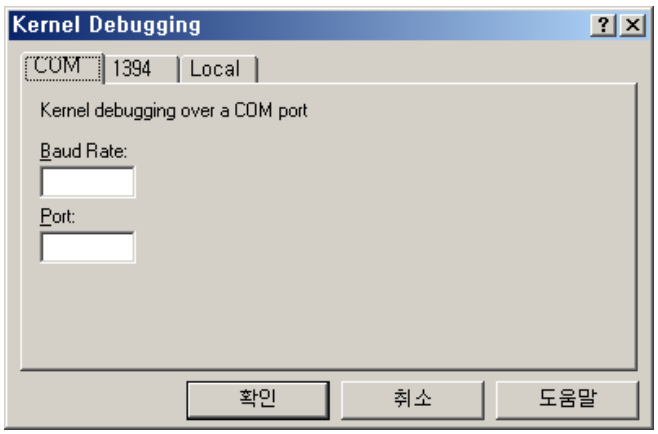
(livekd 는 http://www.sysinternals.com 에서 다운가능)

단 로컬인 경우는 시스템 상태만 확인 할 수 있음.

Kernel Mode 를 모니터링하고자 한다면

두대의 컴퓨터가 필요하다 대체로 노트북을 이용하여 모니터링을 하게 된다.
이 경우는 문제가 된 컴퓨터를 Target Machine 라고 하고 문제를 해결하고자 하는 컴퓨터를 Host machine 라고 한다.

두대의 컴퓨터에는 Null Modem Cable 로 연결하거나 1394 로 연결 할 수 있다.



Target Machine 은 Boot.ini 를 통해 부팅 설정을 하여야 한다.

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)WWINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)WWINDOWS="Windows Server 2003, Enterprise"
/fastdetect
multi(0)disk(0)rdisk(0)partition(1)WWINDOWS="Windows Server 2003, Enterprise"
/fastdetect /debug port=com1 /baudRate=115200
```

위와 같이 Boot.ini 를 설정하여야만 한다.
일반적으로 전송속도는 115200 을 많이 이용한다.

설정이 끝나면 Target Machine 은 컴퓨터 부팅을 다시 하여 위에 설정된 값으로 부팅을 하면 Host Machine(노트북) 에서는 windbg 를 실행하고 있어서 정보를 받아내게 되고 문제를 해결 할 수 있다.