What Makes It Page? Sample Programs

This ReadMe file describes the sample programs package accompanying *What Makes It Page?*

The samples package includes both the source code and a built executable for each program.

Important Warning

The programs provided in this package are *experimental software* and can cause instability and even system crashes. In particular, the WrkEvent driver can only be used with Windows 7 x64 RTM, with no service packs and no updates installed. *Using it with any other version of the kernel will almost for sure crash the system. The WrkEvClient program loads this driver when starting.*

Built Executables

The built executables for user mode programs and kernel mode drivers can be found in the BuiltExecutables subdirectory of the package, together with their debug symbols. These executables are ready to use.

Visual Studio Solution for the Samples

The samples are organized as a solution workspace created with Visual C++ 2008 Express Edition. However, they can be used without VC 2008 installed, since the executables are not built with the IDE. VC 2008 can be used as a handy way to browse through the various source files provided, but any editor can be used in its place.

About the Programs

MemColls

MemColls is a program to test in-paging collisions. It is meant to be used together with the WrkEvent driver, to cause collisions and analyze them. See Chapter 35 of the book.

The source files for this program are located in the MemColls subdirectory of the package.

MemTests and KrnlAllocs

MemTests can be used to perform a number of test calls to memory management APIs and has been used for many experiments described in the book.

This program also allows to experiment (at one's own risk) with kernel mode DDIs for memory management, by means of the companion KrnlAllocs kernel mode driver. The *System range tests* submenu includes options to load and unload the driver and to call DDIs through it.

The source files for these programs are located under the MemTests directory of the package. MemTests\Memtests contains the program source and MemTests\KrnlAllocs the driver one.

WrkEvent and WrkEvClient

WrkEvent is a kernel mode driver which allocates synchronization objects used in the in-paging collision tests. It is meant to be used in conjunction with MemColls to experiment on the concepts explained in Chapter 35 of the book.

WrkEvClient is a user mode program used to load/unload the driver and call its functions.

The source files for these programs can be found in the WorkEvent\Driver and WorkEvent\Client directories.

Building the Programs

All the programs have been built with the following environments:

Windows® Software Development Kit (SDK) for Windows 7 and .NET Framework 3.5 Service Pack 1 has been used for the user mode ones.

Windows Driver Kits 7.1.0 has been used for the kernel mode drivers.

The Visual C++ 2008 express IDE has not been used to build any of these programs.

Each user mode program comes with a makefile which can be used to build it, located in the same directory of the source file. As an example, for the MemTests program:

source file: MemTests\MemTests\main.cpp

makefile: MemTests\MemTests\Makefile

To build a program, open the Windows SDK command shell and run nmake.

For each driver, a directory named W7Build located under the one of the source file contains the files needed to build it with the WDK build utility. E.g., for the KrnlAllocs driver we have:

source file: MemTests\KrnlAllocs\DrvMain.CPP

build files dir: MemTests\KrnlAllocs\W7Build

To build the driver, open the WDK build environment for Windows 7 x64 and run the build utility.