Secret Diagnostic Tools from the Windows XP CD for a More Stable Windows Setup

With the information in this article you can:

- **Discover 70 extra tools you never knew you had!**
- **Track down and repair Windows errors using these professional precision tools**
- **Safely remove settings left by incomplete software uninstallation**

On your original Windows XP installation CD, you can find many utility programs that are not documented anywhere. These utilities are also not automatically installed on to your XP system when you initially setup Windows. These 'hidden' tools can prove to be extremely useful, however, and can help you get to the root of some of the most annoying XP problems. They can also be used to cure incorrect settings and to configure Windows XP to be more stable. And the best thing about them is that they are free, and easy to access. This article introduces these tools, and tells you which to use to trace errors and optimise your PC – some of them will prove indispensable!

Richard Hunt:

"By using these advanced tools with care, they can help you to solve some tricky Windows problems, whether you're using them for general Windows maintenance, or for solving a specific error."

Solve Problems Fast with Windows Support Tools

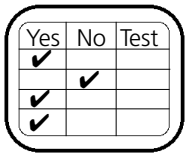
Installing the Windows Support Tools.

The Windows XP installation CD contains over 70 extra tools to help you identify and troubleshoot Windows errors. Because these tools are not installed by default with Windows, many users aren't able to make use of them as they don't even realise they have them. The first step is to install the new tools. To do so follow the instructions below:

1. Insert the Windows XP CD, select **Perform Additional Tasks > Browse this CD** from the menu.
2. Go to the folder **Support** > **Tools** on the CD and double-click on the file **SUPTOOLS.MSI**.
3. Confirm the user license and enter your name and the name of your company, as necessary.
4. Select **Complete**, then click **Continue**.

Once the Support Tools have been installed they can be launched by clicking **All Programs** > **Windows Support Tools** > **Command Prompt**. Further information can be found under **Support Tools Help** and **Release Notes**. Alternatively, you can find more information by opening the command prompt and typing: ***<tool name>*** **/?** Where ***<tool name>*** is the name of the program. You can find a list of the main programs given in the table below.

The most important tools at a glance.



Support Tools Help acts as a control centre, providing not only information about the functions and syntax for the individual tools but you can also start the majority of the tools directly from there. Several utilities can be started only from the command prompt. The following table lists the most useful problem solving Support Tools:

Tool Name	Description
APIMON	Analyses which .DLL files a program uses.
APMSTAT	This tool allows you to view information about APM (Advanced Power Management). This program is not relevant if an ACPI kernel is being used.

Tool Name	Description
BINDIFF	Identifies differences between files or directories at byte level. This can establish whether two different .EXE files are in fact the same program.
CABARC	Lists content of a cabinet archive, creates a new cabinet file in .CAB archive format, or extracts file(s) from an existing cabinet.
CLIPBRD	Allows you to manage, save and view the contents of the clipboard. The data can be saved in a .CLP file.
DEPENDS	Displays the dependency of .EXE, .DLL or .OCX files on other program libraries and shows the exported functions and types belonging to a selected module. This can prove very useful when trying to find out which .DLL files belong to a specific program.
DIRUSE	Provides reports and information on the folders stored on your hard drive, for example, files that exceed a particular size.
DSKPROBE	Allows you to view and edit hard drive sectors and partition tables such as NTFS and FAT16. Be very careful when using this program, as it has the potential to erase data from your hard drive.
DUPFINDER	Allows you to find duplicated files on your system. This can take a long time if you have many subfolders. If you only compare by filename you should check any duplicates found by size to confirm they really are identical. You can delete duplicated files directly from the list, rename them or place them in another directory.
DUMPCHK	A debugging tool for reading information in memory dumps – useful when trying to track down the cause of a crash.
FILEVER	This shows the file version of a file, providing it has a version mark (for example, .EXE or .DLL file).

Tool Name	Description
MSICUU	Removes any remains of a program in the registry following the uninstallation of an application previously installed with MS Installer.
NETCAP	Records a log file of the network traffic for a chosen network adaptor and time frame.
PMON	Allows you to view several different measurements of the processor and memory use of your system. Similar to the Task Manager viewer but operated from a command prompt.
PSTAT	Gives detailed information on the status and memory use of the current running programs. Use the command **PSTAT | MORE** to force a page break otherwise you see only the last part of the information as it scrolls too fast!
PVIEWER	A viewer for showing running programs, their priorities and memory use. It can also be used to terminate programs and alter their priority.
RASDIAG	Allows you to analyse network RAS connections. It collects diagnostic information about remote services and places it in a file.
REG	Adds, changes and displays subkey information and values of registry entries using command line. Also allows you to save individual subkeys in an external file. Very similar to REGEDIT but operated from the command prompt.
REMOTE	This allows you to control PCs remotely over a network. Start the server end of REMOTE on the PC which is to be controlled remotely by typing: **REMOTE /S CMD REMSERV**. In this case, the connection will be called REMSERV. On the client PC that you are connecting from, type: **REMOTE /C *<PC name>* REMSERV,** where *<PC name>* is the name of the remote computer. You can create many connections at the same time, using

	individual connection names for each one. You can end the connection by entering the command **@K** or **@Q** (which leaves the remote server running) on the remote computer or simply by closing the remote window by typing: **exit**.
SETX	This allows you to set up environmental variables in the user or the system environment from the command prompt. It can also get the values of registry keys and write them to a text file.
SPCHECK	Checks the various service packs installed on your PC. To run SPCHECK, the file SPCHECK.INI must be available. You can find the latest version of this file by clicking on the link on the CD accompanying this update.
VFI	Shows information on the current file, which you can save in a tab separated text file for future comparison.
WINDIFF	Direct comparison between two text files or folders where the differences are displayed or saved in a text file.

Compare Files and Folders Using WINDIFF

Launch with **Start > Run.**

As well as comparing the contents of folders, the WINDIFF tool also compares the content of text files. If you have two folders from two different drives which at first glance contain the same information, then WINDIFF will indicate any differences. You can start the program directly from the command prompt, or by going to **Start > Run** and typing in **windiff** then pressing Enter.

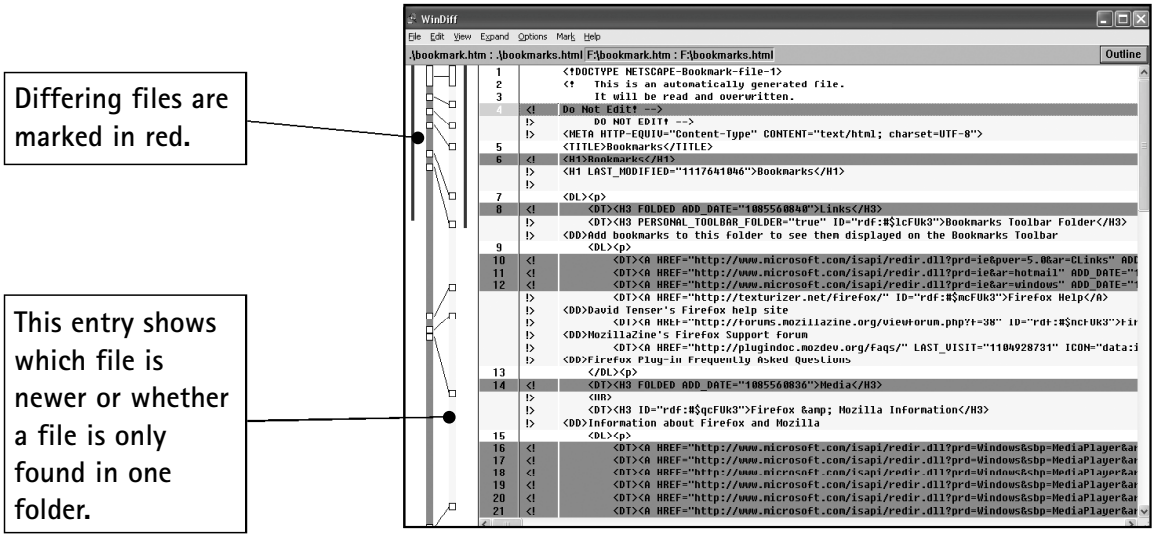
Comparing folders.

As an example, run WINDIFF and select **File > Compare Directories**. This opens a dialogue box in which you give the path of both directories you want to compare. Choose whether subfolders should also be examined by checking or clearing the **Include subfolders** check box. When you click **OK**, WINDIFF compares the directories, looks at every file by name and examines whether the file is newer or older than the one in the comparison directory.

Comparing text files.

The comparison of text files is much simpler. By selecting **File > Compare files**, WINDIFF brings up the **File > Open** dialogue box twice, in which you select the files to compare.

A summary of the comparison is then displayed. Double-click on this summary, or click **Expand**, and WINDIFF brings up the details on to the screen. In the left column is a graphical representation of both files with the positions marked where the files differ from each other. On the right-hand side, WINDIFF lists the lines of the file, including the line number. In this way, you can see at a glance where the differences lie.



The results of a comparison between two files

The Windows Clipboard Viewer.

Controlling the Clipboard with Clipboard Viewer

All data that you copy using **Edit > Copy** is placed on the clipboard. Normally, whatever is stored on the clipboard cannot be seen unless you paste it somewhere. This can be a problem, if you are not sure what is on the clipboard. Windows offers a hidden tool, the Clipboard Viewer CLPBRD.EXE, which you can use to view and organise the contents of the Clipboard.

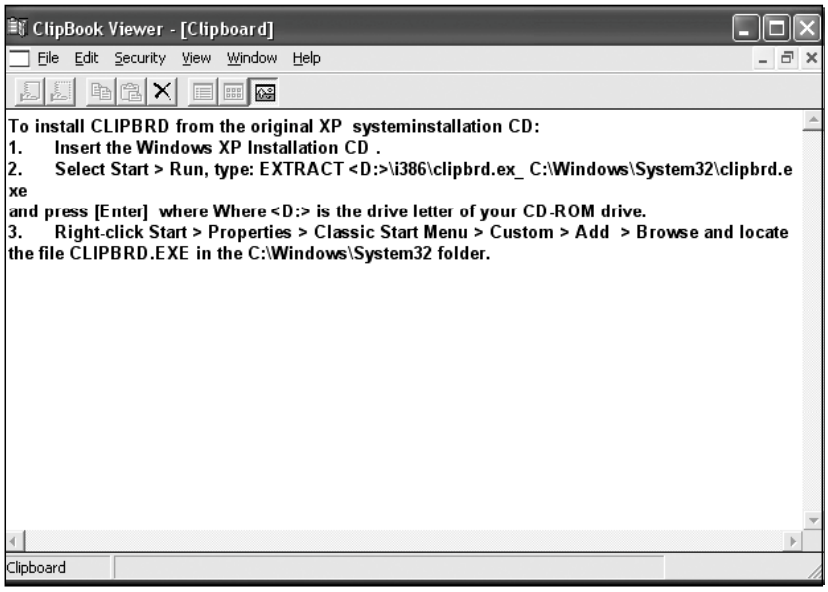
To open the tool select **Start > Run**, enter the command:

CLIPBRD then click **OK**. As Windows does not necessarily install this application automatically, you may have to take the following steps to install it.

To install CLIPBRD from the original XP installation CD:

1. Insert the Windows XP Installation CD.
2. Select **Start > Run**, type:
   EXTRACT <D:>\i386\clipbrd.ex_ C:\Windows\System32\clipbrd.exe
   and press Enter.
   Where <D:> is the drive letter of your CD-ROM drive.
3. Right-click **Start > Properties > Classic Start Menu > Custom > Add > Browse** and locate the file **CLIPBRD.EXE** in the **C:\Windows\System32** folder.
4. Click **OK** > **Next** and select the location **Accessories**.
5. Click **Next** again, rename the object Clipboard Viewer and press **Finish**.
6. Press **Cancel** two or three times to exit Properties.

You can now open the Viewer by selecting **Start** > **All Programs** > **Accessories** > **Clipboard Viewer**.



The Windows Clipboard Viewer in operation

Here you can see the actual content of the clipboard.

You can save the content in separate files by selecting File > Save As.

If you are on a network, you have the ability to share clipboard contents with other users on the network. On a standalone PC, you are restricted to performing operations on your local clipboard.

Windows Installer does not operate cleanly.

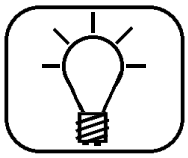
Boost Performance: Clean the Registry Using MSICUU

Microsoft has developed a Windows Installer service program called MSICUU (Microsoft Installer Clean Up Utility) which can help you safely remove traces left behind by programs that were installed with Windows Installer. You can use this tool to remove the elements from the registry which were not properly deleted following the removal of the original application. This program does not:

MSICUU does not delete any files.

- Remove the Windows Installer itself
- Remove any files installed by Windows Installer, such as Microsoft Word

To start Clean Up, select **Start > Run,** enter **msicuu** and then click **OK**. Once it's running, simply select the application which you wish to delete the entries in the registry, then click **Remove**.



What to do if you remove an application in error.

If you remove an application with this tool in error, you will have to re-install it to make it work again. If you need to do this you should re-install it in the same folder as the original installation, to prevent files being duplicated on your hard drive.

You will note that not every application installed on your PC is displayed by this tool, only those that used the Windows Installer for installation. Applications that used their own installer program are not listed in this tool.

Fix Faulty Windows Power Management with APMSTAT

Windows supports two power management methods:

- ACPI – Advanced Configuration and Power Interface
- APM – Advanced Power Management

APM stands for Advanced Power Management.

ACPI is the preferred method, but when it is not available the older APM is used. The APMSTAT.EXE program is used only to control the APM status of your PC.

APM is automatically installed by Windows when it is supported by your PC's hardware. You may experience some mysterious crashes which point to APM as the culprit. In practice, APM-related problems usually manifest themselves in the following ways:

- The computer will not switch off
- Problems with hardware devices after going into standby mode
- General stability problems associated with power management

You have to be ready to deal with these problems.

APMSTAT clearly informs you if APM support was installed or not. If you are running an ACPI machine you will see the message:

```
This is an ACPI machine, APM is not relevant on this machine.
```

Handle errors associated with APM.

Start APMSTAT by opening a Command Prompt window as follows:

1. Select **Start > All Programs > Windows Support Tools > Command Prompt**.
2. Enter the command: **apmstat -v** in the Command Prompt window and press Enter.

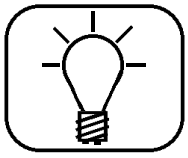
Start by typing apmstat -v to check your PC status.

The parameter '-v' shows that APMSTAT.EXE should be run in verbose (show all details) mode. APMSTAT.EXE gives a clear message with corresponding instructions as to how you can solve the problem, such as:

Error report with appropriate solution.

`This is a multiprocessor computer. APM does not function on multiprocessor computers.`

The computer appears in the Auto-Enable APM list section of the BIOSINFO.INF file. APM must have been activated at installation and can probably be manually deactivated. Check the APM tab under Power Options in the Control Panel.



Often a faulty or incorrect driver is the cause of APM problems. Check carefully whether all of your hardware drivers are listed as being Windows XP compatible.

If problems do occur when you try to use the APM functions (for example, if you put the computer into standby mode and try to restart), uninstall or deactivate all of the Windows hardware drivers one at a time. If the error no longer appears then you need to install an up-to-date driver for the offending device.

DiskProbe: Fix Low-level Hard Drive Problems

The DiskProbe tool is a disk sector editor. It allows a user with Administrator privileges to modify data directly on the hard drive, bypass the operating system, and correct problems that cannot be addressed in any other way.

You should use the DiskProbe editor with great caution so as not to create any serious problems. When you are working with the DiskProbe on a hard drive at sector level, you are not just making small changes. There is potential for you to make your disk and data *permanently* unusable when directly editing sectors. Therefore, before any use of DiskProbe, ensure you have a complete and reliable backup of the drive.

DiskProbe can help in emergencies.

While you must take care when using this program, there are some emergency situations where only DiskProbe can help, such as:

When the hard drive fails ...

... or data is deleted.

- The Disk Management tool allows you to configure and monitor your hard drives. If you have a hard drive problem that results in Disk Management reporting your system or boot drive has an error, such as 'A basic or dynamic disk's status is unreadable', then DiskProbe can be used to help you fix it.
- If your operating system is working, the original dynamic boot disk could still be listed as faulty or offline. All volumes on the faulty hard drive may be listed as failed, even though the operating system seems to be working. In this case DiskProbe can help restore access to your drive.
- Hard drive problems can also occur if Windows XP was recently installed and during setup a partition on a dynamic hard drive was erased or restored. Again, in this situation, DiskProbe can be used to restore access to your drive.
- When you try to set up a new partition with FDISK you encounter problems and have to use DiskProbe to restore access.

Hard drive problems manifest themselves as soon as you try to restart the faulty hard drive with an error message that the dynamic disk partition is unreadable or cannot be found. Furthermore, the system event log may contain an entry similar to the one below for every defective dynamic disk partition held on the missing drive:

```
Event ID: 3
Event Source: dmboot
Description: dmboot: Failed to start Volume
Sysdrive (C:)
```

If you want to recover this dynamic disk drive and all of its data, then it is important to note that a new hard drive cannot be installed or formatted at this time on your system. Also, do not delete any missing or offline dynamic disk partitions. On removing a dynamic disk partition, Disk

Management will delete the boot sector of the drive's file system and remove the drive entry from the local disk database.

NTFS and FAT32 keep a duplicate copy of the boot sector.

The other dynamic disk partitions remain intact (including the data), for the moment. Both FAT32 file systems and NTFS keep a duplicate copy of the boot sector, you can use this to restore your drive by reinstating your boot sector.

How to restore a deleted NTFS drive:

1. Click **Start** > **Run**, type: **dskprobe** and click **OK** to open the DiskProbe tool. As this is a dynamic drive you must look for the duplicate boot sector with DiskProbe.
2. Select the faulty drive, then from the menu click on **Tools** > **Search Sectors** to search for the boot sector on the hard drive.
3. Exit DiskProbe and the NTFS boot sector will be rewritten.
4. Click **Start** > **Run**, type: **diskmgmt.msc** and click **OK** to open Disk Management.
5. Click **File** > **Read New Hard Drives**. Your drive is ready to be used again.

How to restore a deleted FAT32 drive:

1. Set up a partition the same size as the faulty one using Disk Management, but do not format it.
2. Click **Start** > **Run**, type: **dskprobe** and click **OK** to open DiskProbe. Use it to copy the duplicate boot sector of the FAT32 drive from sector 6 of the logical drive and write it to sector 0 of the logical drive.
3. Click **Start** > **Run**, type: **diskmgmt.msc** and click **OK** to open Disk Management.
4. Click **File** > **Read New Hard Drives**. Your drive is ready to be used again.

Use the Small memory dump (Minidump) tool.

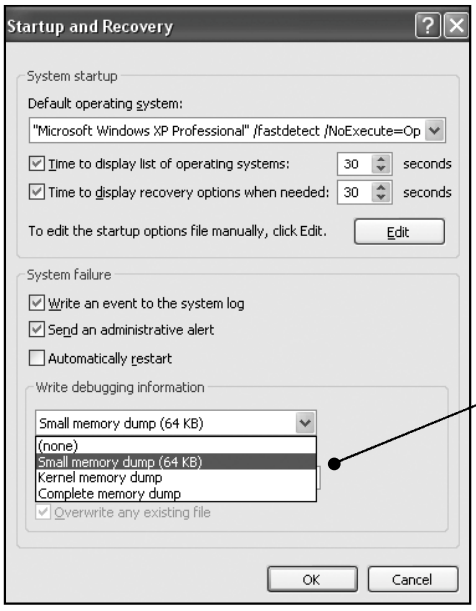
Track Down the Cause of Error Messages with DUMPCHK

An error is not always simple to pinpoint, especially when your system usually functions perfectly and the error occurs only sporadically. Windows provides a memory dump (that is, it copies the contents of the memory into a file) following a STOP error which can provide the information you need to track down the cause of the error.

First you must set your Startup and Recovery rules:

Set up the memory dump.

1. Select **Start** > **Control Panel** and click the **System** icon.
2. Click the **Advanced** tab, and then the **Settings** button under Startup and Recovery.
3. So that you can make a note of any STOP error code and associated information, ensure that the **Automatically restart** check box is blank.
4. Under **Write debugging information**, select the type of memory dump you would like (**Small memory dump** should suffice).



Set the size of the memory dump under **Write debugging information.**

The Small Memory Dump (Minidump) is excellent for analysing most errors

The Minidump records useful information as to why your system has produced an unexpected kernel error or a STOP error. The Minidump requires a paging file of at least 2 MB on the boot volume of your PC. This dump file type includes the following information:

- The Stop message and its parameters and other data
- A list of loaded drivers
- The processor context (PRCB) for the processor that stopped
- The process information and kernel context (EPROCESS) for the process that stopped
- The process information and kernel context (ETHREAD) for the thread that stopped
- The Kernel-mode call stack for the thread that stopped

The last three items are of most use to programmers debugging programs, but can also provide handy clues when looking for the source of an error. Following a crash, Windows will create an individual folder, **C:\Windows\minidump**, where you can see a history of dump information. If you tick the **Overwrite any existing file** box in the Startup and Recovery dialogue, Windows always writes to the same filename.

How to read the information from the Minidump

Download WINDBG and KD.EXE.

To read information in a Minidump file, you need a specific program, DUMPCHK. This is a command line program which displays information about the error contained in the file. As well as DUMPCHK you can also use the Windows tools WINDBG, a Windows debugging tool, or KD, another command prompt debugging tool, similar to WINDBG.

Links to debugging tools can be found on the CD.

You can install these last two tools from the Windows Debugging Tools package, by clicking on the link on the CD accompanying this update.

Once installed you will find them under **Start > All Programs > Debugging Tools for Windows**. For good

The associated symbol package.

measure, DUMPCHK is included in this package as well as in the Support Tools. You will also need to install the appropriate symbol package for your version of Windows, which translates the bugs in the Minidump file into meaningful errors. Click on the link on the CD to download the appropriate symbol package for your version of XP.

WINDBG can be accessed from the Start menu, but KD and DUMPCHK should be started from the command prompt. Be sure to include all necessary arguments and full file paths.

DUMPCHK syntax.

The command syntax for **DUMPCHK** is:

dumpchk [options] <*Minidump File*>

Options for DUMPCHK.

To find the possible options type: **dumpchk /?** at the command prompt. <*Minidump File*> is the name of the Minidump file created when the computer crashed.

Analysing errors with WINDBG and KD

Syntax for WINDBG and KD.

The command syntax for both WINDBG and KD.EXE is:

windbg -y <*SymbolPath*> -i <*ImagePath*> -z <*DumpFilePath*>
kd -y <*SymbolPath*> -i <*ImagePath*> -z <*DumpFilePath*>

The parameters explained.

The parameters of the commands are described in the table below:

Parameter	Description
<*SymbolPath*>	Either the local path where the symbol package has been downloaded or the URL to the symbol server path, including a cache folder (example below). Because a small memory dump file contains limited information, the actual binary files must be loaded together with the symbols for the dump file to be correctly read.
<*ImagePath*>	The path to the program file being debugged. For most Windows components the path will be C:\Windows\System32.
<*DumpFilePath*>	The path and name of the Minidump file to be examined.

To run KD using a debugging file located on Microsoft's web server, you would use the following command:

Use a remote symbol file to avoid downloading one.

kd -y srv*C:\symbols*http://msdl.microsoft.com/download/symbols -i C:\Windows\system32 -z C:\Windows\minidump\minidump.dmp

Sample syntax of WINDBG is identical. Make sure you include the **-y**, **-i** and **–z** arguments with these codes. If you prefer the graphical version of the debugger instead of the command line version, type the following command instead:

WINDBG has a graphical interface.

windbg -y srv*C:\symbols*http://msdl.microsoft.com/download/symbols -i C:\Windows\System32 -z C:\Windows\minidump\minidump.dmp

Making sense of the memory dump

How to evaluate the BugCheckCode.

In the results displayed, you will find an entry for **BugCheckCode**. This indicates the nature of the error, and the codes used for this are explained in the table below:

Error Code	Meaning
0x00000000	Division by 0 error.
0x00000001	Start of the system debugger.
0x00000003	Breakpoint of the debugger.
0x00000004	Register overflow from mathematical operations.
0x00000005	Reached the memory limit.
0x00000006	Invalid operation.
0x00000007	Call up of a function not supported by the co-processor.
0x00000008	Emergence of an error during error processing.
0x0000000A	A program with task status causes an error.
0x0000000B	Application tries to access an unavailable memory segment.
0x0000000C	Memory access attempt which lies outside of the permitted area.
0x0000000D	Unknown error.

Most of these errors indicate that the application's programmers have made an error, and the details of the error should be reported to them, via the support section of their website if possible.

There are some further WINDBG commands with which you can collect additional information about a dump file, by including them in the command line listed above:

Additional commands.

Command	Description
!analysis -show	Shows the STOP error code (also known as the BugCheckCode) and its parameters.
!analysis -v	Displays verbose information.
lm N T	Lists the modules running at the time of the system crash.

Speed Up the Debugging Process

Make it easier by using a batch file.

After you identify the correct command you need to load memory dumps, you can create a batch file to examine a memory dump quickly. When you want to analyse a memory dump, you can simply type the name of the batch file, rather than writing out the long command. To create a batch file follow these steps:

DUMP.BAT

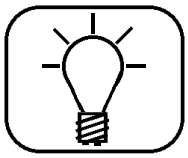
1. Open My Computer and navigate to the folder C:\Windows.
2. Click **File** > **New** > **Text Document**.
3. Double-click on NEW TEXT DOCUMENT.TXT. When the file opens in Notepad type the following:
   cd "c:\program files\debugging tools for windows"
   kd -y srv*c:\symbols*http://msdl.microsoft.com/download/symbols -i <d:>\windows\i386 -z %1
4. Click **File** > **Save** then **File** > **Exit**.
5. Right-click on the file NEW TEXT DOCUMENT.TXT and choose **Rename**. Name the file **dump.bat** and press Enter.

Run the batch file with this command.

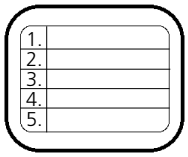
When you want to examine a dump file, you can now type the following command to launch the debugger from the batch file:

DUMP C:\Windows\minidump*<Minidump File>*

where ***<Minidump File>*** is the name of your dump file.



If you double-click on the WINDBG file icon, the tool opens and you can set Symbol and Image paths, and open the Minidump file directly using the Windows interface.



The tools described in this article are very powerful and let you take control of Windows features at a very deep level. For that reason you should use them with caution, and always read the command's help description before you use it. As always, ensure you have a full and reliable backup of any drive you are working on, and do not be surprised if you have to restore from that backup when all else fails.

If you are plagued with the sorts of problems described in this article, however, using the free diagnostic tools included on the original Windows XP installation CD should help you trace and repair many types of fault on your machine that would otherwise have required a full system re-install.