digit

August 2006

Fast Track *to*
THE WINDOWS REGISTRY

Some **Background**

Regedit: Hands-On

Beyond Regedit
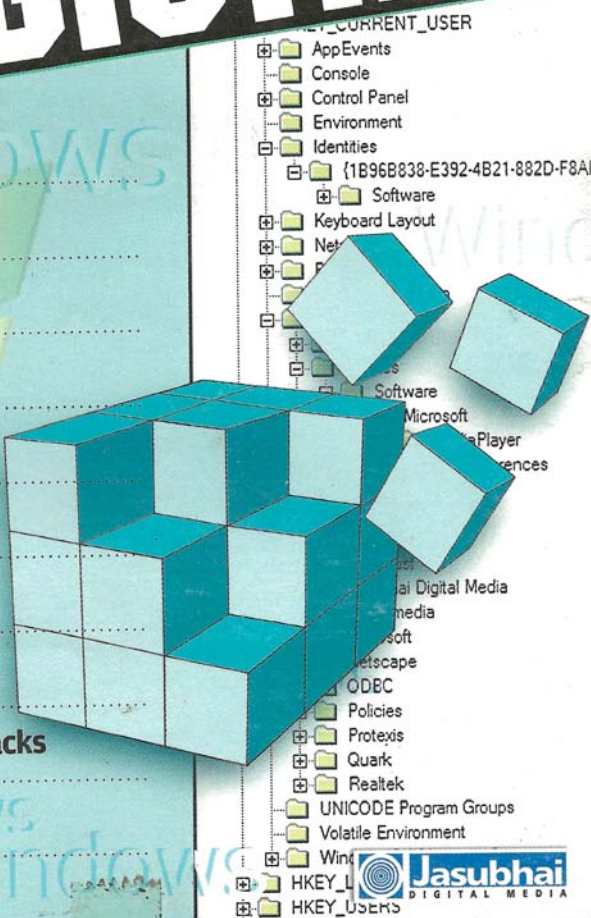
Hacks For **Windows XP**

Hacks For **MS Office**

Internet Software

Hardware

Security & **Network Hacks**

Irritants

HKEY_CURRENT_USER
- AppEvents
- Console
- Control Panel
- Environment
- Identities
  - {1B96B838-E392-4B21-882D-F8AF
    - Software
- Keyboard Layout
- Net
- ...
- Software
- Microsoft
- ...Player
- ...rences
- ...i Digital Media
- ...media
- ...soft
- ...tscape
- ODBC
- Policies
- Protexis
- Quark
- Realtek
- UNICODE Program Groups
- Volatile Environment
- Win...
- HKEY_L...
- HKEY_USERS

Jasubhai DIGITAL MEDIA

YOUR HANDY GUIDE TO EVERYDAY TECHNOLOGY

Fast Track
to
The Windows Registry

By Team Digit

Credits

The People Behind This Book

EDITORIAL
Deepak Ajwani Editor
Robert Sovereign-Smith Copy Editor
Ram Mohan Rao Writer, Copy Editor
Nimish Chandiramani Copy Editor
Jayesh Limaye Writer
Abey John Writer

DESIGN AND LAYOUT
Vijay Padaya Layout Designer
Sivalal S Cover Design
Harsho Mohan Chattoraj Illustrator

It's Your Computer

One size doesn't fit all, as you know all too well. Though most of us don't go so far as to name our computers, each Windows computer is unique - except in the case of some offices where people do nothing on them except word processing and spreadsheeting.

It's the Windows Registry that holds your personal settings - so that's where you should be headed if you want to make your computer your own.

We can think of at least five good reasons why you should tinker with the Registry. First, customisation: XP, more so than Windows 98, can be customised to one's heart's content, and Vista reportedly will be even more customisable. But customising via menus is (a) limited, and (b) not so much fun. Second, security restrictions: you don't want people to mess with your computer. Third, performance: Windows should ideally ship with a performance-tuning Wizard, but it doesn't, so we need to resort to Registry hacks. Fourth, using the Registry Editor and other tools we mention gives you a feeling of control over your computer - it's a good feeling. And finally, making Registry edits is good, clean fun. Except when you break something, of course.

In this book, we have collated a whole bunch of Registry edits. In addition, for those new to the Registry, we introduce it in terms of what it is and how it works. Then there's a chapter on how to work with Registry files and such, and another on third-party tools that give you more user-friendly control over the Registry. Included in this, the third chapter, are tools that help you optimise and repair the Registry as well. Then follow the tweaks.

There will be several more disclaimers to come, but here's the first: handle the all-powerful Registry with care!

DISCLAIMER

This book contains information on how you can modify your Windows Registry. It is always recommended that you take a back-up of the Registry before proceeding with an edit, because, as you should be aware, an improperly executed hack could cause strange behaviour, and at worst, could even entirely corrupt your Windows installation, requiring you to reinstall Windows.

We encourage you to try out the following hacks, but only if you know what you're doing - and if you do it with care.
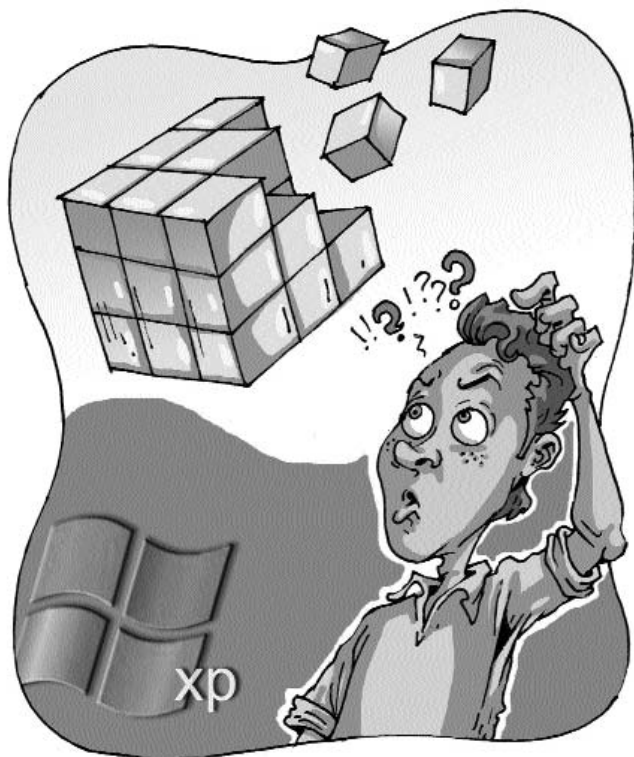
Neither Jasubhai Digital Media nor its employees and affiliates can be held responsible for *any* damage you may cause to your system as a result of taking *any* action suggested in the following pages. You are solely accountable for any negative consequences arising from changes you make to your Windows Registry as suggested in this book.

Contents

Some Background

The Registry has to be one of the least understood aspects of the Windows operating system family. Even seasoned professionals approach it with a degree of caution, knowing that a wrong entry can potentially wreak havoc on the system. To understand the Registry is to get to the heart of controlling and modifying your Windows system. With a detailed understanding of what you are doing, you can turn your machine into a lean performance machine, customise and personalise its appearance, and get fine-grained control over nearly every aspect of how Windows XP behaves.

1.1 Some History

The Registry was introduced as a way out of the "INI files mess" that plagued early versions of Windows. Configuration information regarding the operating system, application files, hardware, and so on were stored in INI files scattered all over the system. For example, when an application is installed, it needs to know various parameters regarding the operating system and the available hardware. Much of this information is common to other applications as well. However, if there was any change in the hardware or operating system software, updating the application's INI files used to be hell.

The Registry was conceived as a way out of this madness. It is a hierarchical database that stores information regarding the hardware, operating system software, application software, users preferences and system preferences. The hierarchy separates the machine information, user information and the software information into logically discrete units that can be manipulated with greater ease. Any changes made by users, the operating system, newly installed software, and hardware are all updated and reflected in the Registry.

During system startup, Windows uses the registry to get configuration data regarding the hardware, software and other peripherals that have been configured. It also maintains a backup copy of the registry with which the system had successfully started up last. Hence, if it encounters a problem with the current startup, it can then use the configuration information from the backup to attempt to start the system. Some of the information stored in the registry is specific to the particular startup session only, and is mostly user-specific. When a user installs new software, Windows will either make the installation user-specific or system-wide. In some software, the user is given the option to select whether the installation should or not be available to everyone else who uses the system. In other cases, the software will install itself system-wide and save user specific information separately, making entries in the registry that are both user-specific as well as system-wide.

For example, when you install Yahoo! Messenger, the program is installed system-wide, but the user information is specific to the currently logged-in user. Any preferences that are made are stored under the username in the registry. If another user logs in and starts Yahoo! Messenger, the default preferences are initialised, and a new entry is created in the Registry under this username.

This flexibility has deeper significance when considering a networked scenario. Administrators can specify user rights and access to various system and network components. They can control what users can and cannot do on their machines with a fair degree of granular control. For example, Administrators can specify that users are not allowed to install new applications on their machines. A Registry entry disabling the users' right to install would secure the system. And a Registry entry can be made to prevent unauthorized access to the registry itself!

However, the Registry has not done away entirely with the legacy of INI files, partially due to Microsoft's commitment to backward compatibility and partially because in some cases the Registry wouldn't be available—as in the case of the boot process, when the boot.ini file is used to get the initial startup information.

Critics of the Registry concept point to it as a "single point of failure." If the Registry is damaged, XP will fail to start up, and in most cases will require a complete reinstall. It is for this reason that the Registry is hidden deep in the system, and any discussion on the tweaking the Registry is accompanied by dire warnings of disaster if one does anything wrong. Also, if an application doesn't uninstall correctly, it can leave traces in the registry, which over time will increase its size and affect performance.

Physically, the Registry information in XP is stored in multiple files in the **\System32\Config** folder of the operating system (or root) folder—usually **C:\Windows** or **C:\WINNT.** These files cannot be edited directly; they have to be accessed through a Registry-editing program such as Regedit.exe or Regedt32.exe.

1.2 The Structure And Working Of The Registry

Registry editors visually depict the logical hierarchy into which the entire Registry is organised. Similar to the folder and sub-folder structure in Explorer, the Registry is divided into six main branches called hives.

Each of these hives contain keys, sub-keys and perhaps sub-sub-keys. Visualise this as sub-folders under a main folder. Each key or sub-key can also contain values. These values are where the information regarding software, hardware, and users is stored. The values are categorised into three primary types: **DWORD**, **String**, and **Binary**. These and some expansions based on them are used depending on the context of the key. "String" is used for human-readable text entries, "binary" for most hardware and device settings data in raw binary entered in hexadecimal format, and DWORD is allowed for Boolean entries where the option is a list of choices, each of which could invoke a different behaviour by the relevant section of the operating system, hardware, or the application.
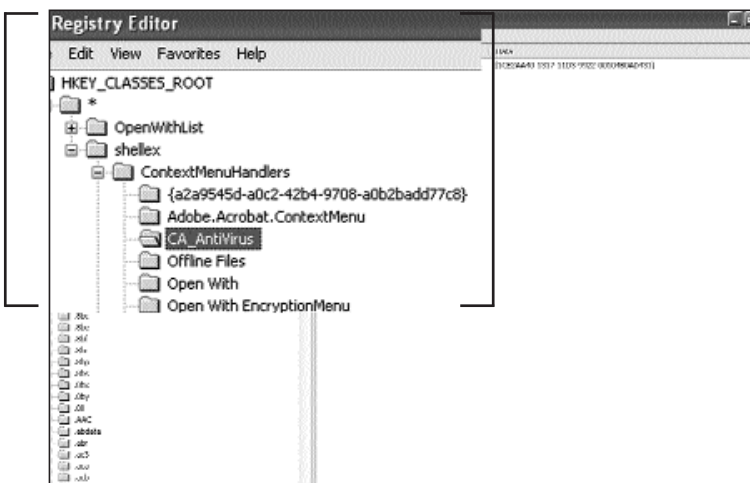
Much of the Registry looks like this—keys, sub-keys, and sub-sub-keys

In the image on the previous page the hive **HKEY_CLASSES_ROOT** has a key called "*****"; this key has a sub-key called "**shellex**", which in turn has a sub-key called "**ContextMenuHandlers**", which again has a sub-key called avast. The CA_antivirus sub-key, created by the anti-virus program, contains values that tell Windows to include it in the right-click context menu. The program will also have other information—stored elsewhere in the Registry—addressing different aspects of the program's functioning.

Each of the six hives serve a different function, storing information specific to the hive's function. Thus:

HKEY_CLASSES_ROOT contains all the information related to fundamental aspects of the Windows user interface, file association mappings for drag and drop functionality, shortcuts, and OLE (Object Linking and Embedding) information. In XP it is a compilation of the information found in **HKEY_CURRENT_USER \Software\Classes** and **HKEY_LOCAL_MACHINE\Software\Classes**. When a value in a sub-key of the same name is present in both hives, the one in **HKEY_CURRENT_USER** is used.

HKEY_CURRENT_USER contains all the information related to the current user logged into the system including such things as Desktop settings, logon names, and other user- specific information. This information is a copy of the currently logged-in user's configuration and other information merged in from the section of the **HKEY_USERS** hive relevant to the currently-logged in user.

HKEY_LOCAL_MACHINE contains all the information regarding the hardware, software, and other PC-specific preferences that are common to all the users who log in to the machine.

HKEY_USERS contains all the information related to specific preferences of individual users, who are each identified by a unique security identifier called the SID. This SID is unique for the life of the system. If a user is deleted and another created with the

same name, the SIDs will be different. An SID once used will not be repeated. All information regarding each and every user who has ever logged into the system is stored under the SID and is copied over to the **HKEY_CURRENT_USER** hive at login. This is particularly useful when a user crosses domains in a multi-domain organisation, or is one with a roaming profile. The particular Registry information is stored on the sever in case the user has a roaming profile, and is initialised when he logs in from anywhere on the network. If the user should become part of another domain, a new SID will be created, which will contain information pertinent to that domain—but which will also contain the old SID from the previous domain along with all the information associated with that domain.

HKEY_CURRENT_CONFIG contains all the information gathered when the computer boots up, and is copied and merged in from portions of **HKEY_LOCAL_MACHINE** relevant to the current hardware profile. This information is not stored: it is regenerated every time the computer starts up.

HKEY_DYN_DATA contains all the information relevant to plug-n-play devices, and is linked in from relevant portions of **HKEY_LOCAL_MACHINE**. Like in **HKEY_CURRENT_CONFIG**, this information is dynamic, and changes as devices are added or removed.

1.3 Value Types

As mentioned above, each of these hives contain keys and sub-keys, which in turn can contain further sub-keys or values. These values are of three major types: DWORD, Binary and String.

REG_DWORD (a DWORD Value) is usually used for Boolean values and is a four-byte number. Many device drivers and services use DWORD values to toggle between options. For example, the UpdateMode setting that controls refresh rates can have a setting of either 0 (disabled) or 1 (enabled). If the DWORD value is set to 0, refreshing does not take place. Each setting has a specific default DWORD value that is used by the system.

REG_BINARY (a Binary Value) is used to store information as raw binary data, and is usually used for hardware components.

The String Value type, however, has expansions to accommodate variables and multiple values. The Value types are denoted as:

REG_SZ is the standard string used to display human-readable text.

REG_EXPAND_SZ is an expandable data string that permits storing of variables that can be replaced by actual values by the application calling the key. For example, an application may refer to a particular key in a hive to obtain the location of a system file. The key would contain a setting for that system file, and a string value which is, say, **%systemroot%\filename**. The **%systemroot%** will be replaced by the location of the XP operating system folder, which on most machines will be **C:\Windows** or **C:\WINNT**.

REG_MULTI_SZ is used to store lists or multiple values, each entry being separated by a NULL character. This is analogous to arrays in programming. For example, a Registry entry could be created to store the IP addresses of multiple timeservers. An application program would then refer to this Registry entry and cycle through the list of IP addresses.

Regedit: Hands-On
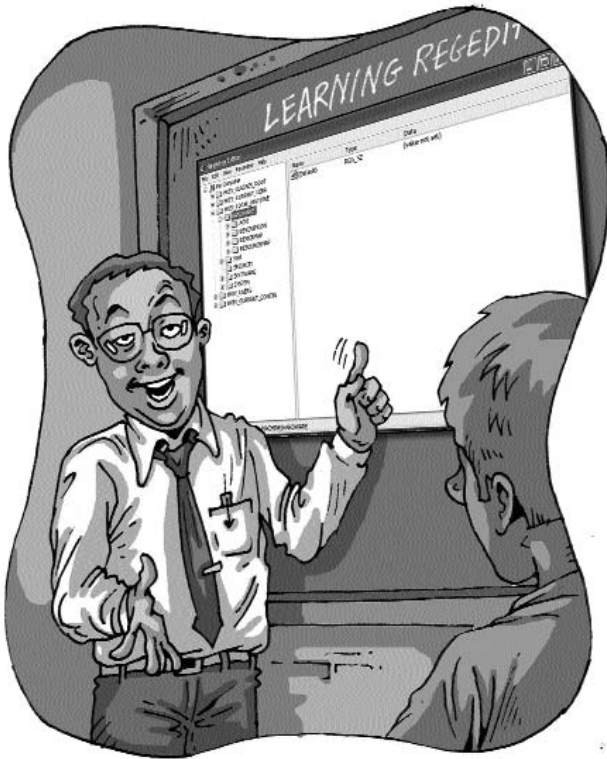
Regedit is a program you can use to access and edit the Registry. It normally ships with the default Windows installation and can be launched from the Run command box in the Start Menu by typing in "regedit" or "regedit.exe". Editing the Registry should be done with care, and with as much understanding as possible as to why and where you are making a change. Additionally, it is strongly recommended that you back up the Registry immediately prior to making a change. You also need to understand how to restore the Registry in case things go awry. The following sections deal with how to back up and restore the Registry

2.1 Backup And Restore

There are two things you can do in terms of backing up the Registry: either back up the entire Registry, or export the specific key you are going to edit.

To export a Registry key, open Regedit using the Run command box. Find the key or sub-key you want to edit and select it by clicking on it. Choose **File > Export**. In the dialog box, select the location where you want to save the key, select to save it as a .reg file, and select the "Selected Branch" option. Give a name for the file and click Save. It will be saved as a .reg file.

If you want to back up the entire Registry, use the backup utility provided with XP. It is generally not recommended to export the entire Registry or a hive using the "export" method, as any changes or accidental erasures while working with .reg file may have disastrous consequences. (Please bear with our warnings—you might just be glad you did!) Open the backup software from **All Programs > Accessories > System Tools > Backup**. Select the checkbox that says "System State Data". This will back up the registry, boot files, and the COM+ class registration database.

At any later point, you can either restore the individual key you exported using the method above, or the entire system state. Restoring the individual key is a simple double-click on the .reg file you saved.

To restore the system state, open the Backup utility, click Advanced Mode and select the Restore and Manage Media tab. Select the backed up system state file you want to restore. Check the System State box. In the "Restore Files to" box, select Original Location. In the Tools menu, select Options, and click on "Always replace the file on my computer", then on OK. (If you don't do this, you will be asked for a confirmation for each and every file during the restore process.) Click "Start Restore". You will get a warning that says: "Restoring System State will always overwrite current

System State unless restoring to an alternative location"; click OK to overwrite. Click OK in the Confirm Restore dialog box. The restore operation will start showing you the progress of the restore. When it completes, click Close and accept the prompt to restart the computer.

2.2 Editing The Registry

Using Regedit you can add, delete, edit or rename a sub-key or value. Navigate to the appropriate section of the Registry that you wish to edit. This is similar to the folder and sub-folder concept in Explorer, and clicking on the hive's "+" sign will make it expand to show the keys. Clicking on the "+" sign for each key will further expand them to show the sub-keys, and so on. If you are following instructions from a manual, the hive names are sometimes abbreviated as follows:

HKEY_CLASSES_ROOT: HKCR
HKEY_CURRENT_USER: HKCU
HKEY_LOCAL_MACHINE: HKLM
HKEY_USERS: HKU

Thus, the hive location **HKEY_CURRENT_USER\Control Panel\Accessibility\HighContrast** will be abbreviated as **HKCU\Control Panel\Accessibility\HighContrast**.

Note: In all the Registry hacks that begin in Chapter 4, we have used the following abbreviations:
HKEY_CLASSES_ROOT: "HCR"
HKEY_CURRENT_USER: "HCU"
HKEY_LOCAL_MACHINE: "HLM"

Clicking on a key or sub-key will show, in the right pane, the values it holds. If it contains no values, at the minimum it will show a "(Default)" setting entry, which will not contain any data. Double-

click each individual setting to open its data values. You can then edit the value as required.

Double click setting to edit value

To add a key, right-click on the parent key (similar to the parent folder in Explorer) and select **New > Key**. Enter the name of the key and press [**Enter**]. To add a value, select the key, right-click and select **NEW**, and the data type for the new value. Give a name for the value and press [**Enter**]. Double-clicking the value will enable you to modify it.

New Key

As mentioned in *Chapter 1*, the value type is determined by the context, and there are three basic data types: String, DWORD, and Binary.

New key created

"String" is a human-readable text entry and is used for most user-defined entries such as text, filenames, file paths, and so on. DWORD is a Boolean entry, which is usually a set of values such as yes, no, 0, 1, 2, 3, and so forth. Binary is raw binary data stored directly as 1s and 0s (binary format) and is entered either in binary or in hexadecimal format.

Adding a Key value setting
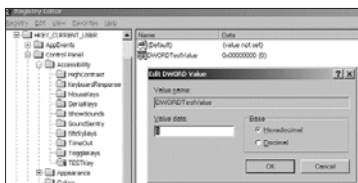
Modifying a newly added value setting

2.3 Creating And Using .Reg Files

Now that you have an understanding of how the Registry operates, you are ready to start hacking it! Hackers are not just those who create malicious viruses or attempt to break into systems. In fact, anyone who decides to get under the hood of any system to discover how it works, tweaks it to gain some advantage, or does it just out of curiosity to see what happens when something is changed, can be considered as a hacker. The hacker is more interested in the mechanics of the hack rather than the result. Once you get into the Registry and change things around, you may want to create your own .reg files to distribute to friends or publish it on your Web site or blog. Use this capability with caution, and be extra sure of what you are doing. A wrong entry here can potentially wreak havoc on a user's system.

The .reg file is actually a text file which will open in any ASCII editor like Notepad. It uses a specific syntax that the registry recognizes. Following the rules of this syntax you can create and publish your own registry hack.

The .reg file uses the syntax:
RegistryEditorVersion
Blank line
[RegistryPath1]
"DataItemName1"="DataType1:DataValue1"
"DataItemName2"="DataType2:DataValue2"
Blank line
[RegistryPath2]
"DataItemName3"="DataType3:DataValue3"

For Windows XP and Windows 2000, the header **RegistryEditorVersion** should always read "Windows Registry Editor Version 5.00". You can also create .reg files for use on older Windows 98 and Windows NT4.0 systems. **REGEDIT4** is the version entry in the header of the .reg file for Windows 98 and NT4.0 systems. A .reg file with the REGEDIT4 header will work both on

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER]

[HKEY_CURRENT_USER\Control Panel]

[HKEY_CURRENT_USER\Control Panel\International]
"Locale"="00000409"
"sShortDate"="dd/MMM/yy"
"iDate"="1"

[HKEY_CURRENT_USER\Control Panel\Appearance]
"Current"="Windows 2000"
"CustomColors"=hex:ff,ff,ff,00,ff,ff,ff,00,ff,ff,ff,00,ff,ff,ff,00,ff,ff,ff,00,\
  ff,ff,ff,00,ff,ff,ff,00,ff,ff,ff,00,ff,ff,ff,00,ff,ff,ff,00,ff,ff,ff,00,ff,\
  ff,ff,00,ff,ff,ff,00,ff,ff,ff,00,ff,ff,ff,00,ff,ff,ff,00
```

Typical entries in a .reg file

Windows XP/2000 as well as on Windows 98/NT4.0 systems, since the Registry is backwards-compatible. However, .reg files with the header "Windows Registry Editor Version 5.00" will only work on Windows XP/2000 based systems.

Note that when creating a hack on Windows XP/2000 targeted at earlier versions of Windows, you should always test whether these hacks will work on those earlier OSes. If you are unable to test it on earlier Windows versions, release the .reg file with the header "Windows Registry Editor Version 5.00" to prevent accidental updates into the registries of those earlier Windows versions. If you are quite certain that the hack is harmless to Windows 98/NT4.0 machines, and you do want to release it to that group of users as well, then at the very least, include a disclaimer such as "Not tested on Windows 98/NT4.0; deploy at your own risk!" so that the user is sufficiently warned about what he is about to do.

The *Blank line* informs the Registry of the start of a new Registry path. Every key and sub-key starts with a new Registry path and helps you identify the location of each of the entries in the registry when examining the contents of the .reg file.

RegistryPathx is the path to the location in the Registry of the particular key or sub-key whose values you will be adding, modi-

fying or deleting. The path has to be enclosed in square brackets, and each sub-key level is separated by a backslash. For example: [**HKEY_CURRENT_USER\Control Panel\International**]. If the sub-key in the path does not exist, it will be created—hence it is important that you follow the correct order in specifying the path. For example, if you erroneously create the path as [**HKEY_CUR-RENT_USER\International\Control Panel**], then a new key called International will be created under **HKEY_CURRENT_USER** with a sub-key called Control Panel. Multiple entries in the .reg file will each start with their own paths separated by blank lines.

The **"DataItemName1"="DataType1:DataValue1"** determines the specific values of the key (or sub-key). Each key can have one or more **DataItemName**. This is the specified name of the data, and is enclosed in quotation marks. It is immediately followed by an equals sign. To the right of the equals sign, the data type (DWORD or hexadecimal) is specified, followed by the actual data. If the data is of the String type, then no data type is specified, and the Registry will understand that the data type is String. The data type and the data value are separated by colons, and the entire entry is enclosed in quotations. Here's an example.

[**HKEY_CURRENT_USER\Control Panel\Appearance**]
"Current"="Windows 2000"
"PreviewMode"=hex:04,00,00,00
"ShowNewProcesses"=dword:00000000

Here, the data name **Current** has a string value: **"Windows 2000"**. The data name **PreviewMode** has a binary value represented in hexadecimal. The data name **ShowNewProcesses** has a DWORD value of **00000000**.

If the data name does not exist it will be created in the sub-key specified in the path; if it exists, it will overwrite the existing value with the new values. If you want to delete entries in the Registry with a .reg file, you can use the hyphen symbol. For example, [-**HKEY_CURRENT_USER\Control Panel\Test**] will delete the

"Test" key in the specified path. To delete a value, put the hyphen symbol immediately after the equals sign of the data name. For example...

> [HKEY_CURRENT_USER\Control Panel\Test]
> "TestItem"=-

...will delete the TestItem data name in the Test sub-key of the Control Panel key in the **HKEY_CURRENT_USER** hive.

To rename an entry, first delete the entry using the above procedure, then specify the new name and values in the same .reg file. Both entries have to be separated by blank lines. An example:

> [-HKEY_CURRENT_USER\Software\Yahoo\Pager\IMVironments\baseball3]
>
> [HKEY_CURRENT_USER\Software\Yahoo\Pager\IMVironments\baseball4]
> "promo"=dword:00000002
> "name"="Precious Moments"
>
> [HKEY_CURRENT_USER\Software\Yahoo\Pager\IMVironments\baseball4]
> "promo"=dword:00000002
> "name"=-

In this example, the sub-key "**baseball3**" will get deleted first. Then, the sub-key "**baseball4**" will be created with the data names "**promo**" and "**name**" containing a **DWORD** value of **00000002**, and a **String** value called "**Precious Moments**" respectively. Then the data name "**name**" will get deleted from the sub-key "**baseball4**".

It is good practice to distribute your .reg file as a zipped archive to prevent accidental insertion into the Registry. Even though the user will be prompted before adding the .reg file to the registry,

using the archive method will act as double insurance against carelessness on the user's part. The user will need to unzip the .reg file and double-click on it. Then, he will be prompted to add the information in the .reg file to the Registry.

If you right click on a .reg file, the first three options will allow you to either Merge the file with the Registry (which is the same as double-clicking on it), print out the text, or edit it with your text editor—usually Notepad or WordPad.

To even make it safer still, you might want to change the default double-click action of merging the .reg file with the Registry to be changed to open it in Notepad. Look for this tweak in what follows!

Beyond Regedit
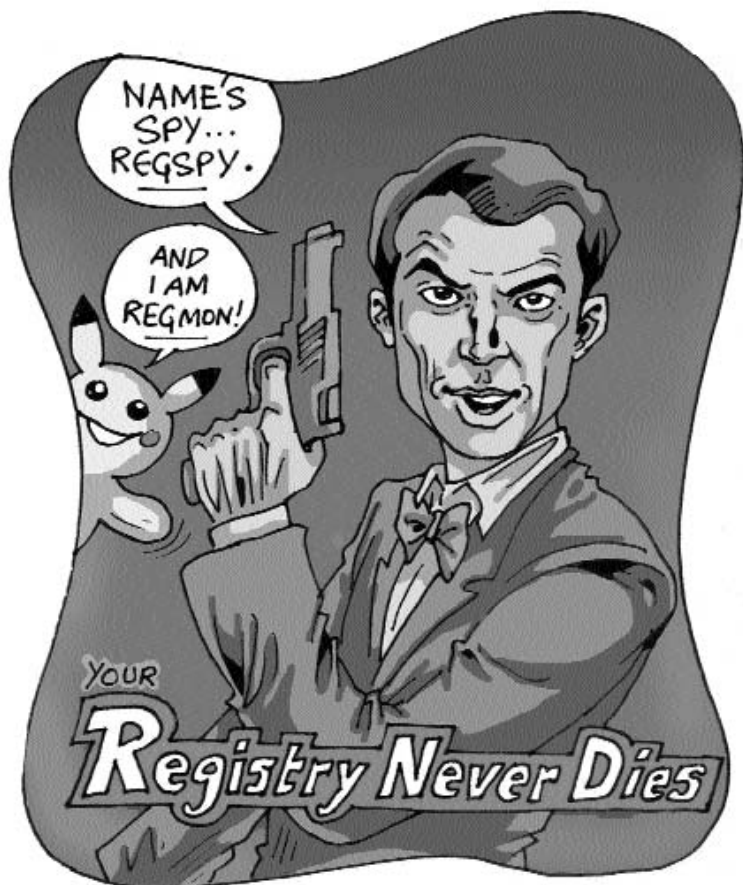
Regedit is fine as long as you don't tinker with the registry much, but there are several reasons you might want other Registry-related software. Here we explain why you can't do with just Regedit, what software are available, and what they do.

Once you get into editing the Registry regularly, you will notice a whole lot of things that you want to do differently or in a better way. You will want to move around the Registry faster, and speed up searches within the Registry, for example. You will also want to find out what applications are using the Registry and how, what changes are being made, and by which application. Then, of course, you will notice the continual bloating of the Registry due to entries left over from uninstalled applications that have not deleted their entries, from changes made by users, hardware additions, hardware removal, system configuration changes, and so forth.

You might, therefore, need tools beyond Regedit. There are three classes of applications we talk about now: third-party Registry editors, Registry trackers, and Registry cleaners.

3.1 Third-party Registry Editors

Regedit is a pretty basic tool provided by Microsoft. In most cases this should be more than sufficient for the job, since the Registry is not accessed regularly in most cases. But Registry hackers dispel with that convention in pursuit of the ultimate fine-tuned Registry, and in the pursuit of wanting to get things done faster! This is where third-party Registry editors step in.

These editors extend the standard functionality of Regedit by including powerful productivity enhancements such as faster search, cut/copy/paste functions, bookmarks, and undo options, amongst others.

Here, we take a look at three editors: Registry Commander, RegEditX (with its companion Registry search engine called Registry Crawler), and Registry Workshop. Registry Commander and RegEditX are freeware, while Registry Crawler and Registry Workshop are shareware.

3.1.1 Registry Commander

This software is a replacement for Regedit that uses a differently styled user interface to access the Registry. While the lack of the familiar explorer-style Registry tree may seem a bit disconcerting at first, users may find that having the key and its values in the same window is more intuitive.

A little known fact about the Registry is that it supports 12 data types. Most other Registry editors show only five of these twelve, and in this book, we've only dared to elaborate on three! (You're better off this way before you really get down to commanding the Registry!) Registry Commander exposes you to all twelve, which in turn means that you have to exercise due—or even undue—caution when using it. This is a very powerful tool in the hands of the advanced Registry hacker.

Registry Commander is downloadable from **http://www.aezay.dk**.
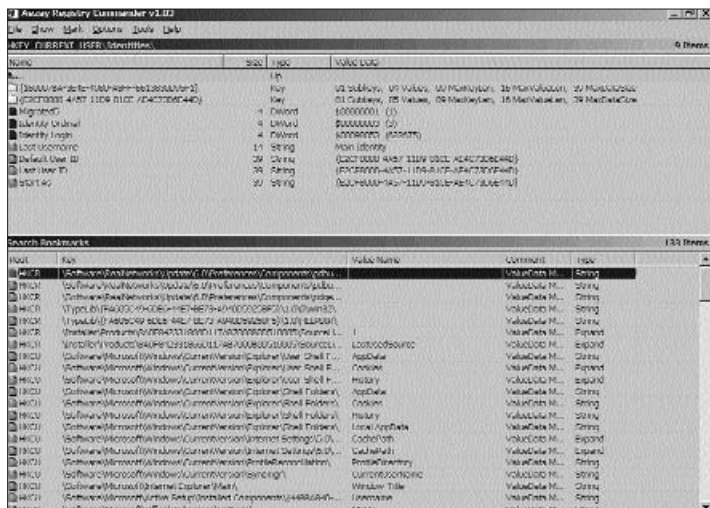
Registry Commander doesn't have the familiar Explorer-like interface, but you'll get used to it

Using this software, you can do all the following:
- Copy or move keys and values from sections of the Registry
- Jump back and forth between Registry locations using the history list
- Search through the Registry and get a result list with all the keys and values where your keywords are mentioned,
- Bookmark keys and maintain their history
- Copy data to the clipboard and maintain a history list of the all the data copied or cut into the clipboard, and view one type of data in another format—for example, binary data can be viewed in the String format so you can read the data (if possible) in text format

While the search function works at about the same speed as a Regedit search, it goes one step further by collating a list of all the keys where the keywords appear. Additionally, not only can you search by data type as in Regedit, you can search by size of the Registry entry as well.

If you're looking for a freeware utility that will give you some enhanced functionality over the staid operations of Regedit, Registry Commander is a good choice. However, like we mentioned, because Registry Commander exposes all data types supported by the Registry, it does have the potential to cause damage if used without care.

3.1.2 RegEditX (With Registry Crawler)

RegEditX sports an interface similar to Regedit, with one important exception: it has an Explorer-style address bar. This makes it easy to navigate through the Registry if you know the complete key path. Rather than click through the key hierarchy in the left pane, you can simply type out or paste the entire key path into the address bar, and it will instantly jump to the location. Additionally, it remembers the list of keys you have visited, making it easy to jump back and forth between keys by simply selecting one from the drop-down.

RegEditX also has the standard Regedit functionality of allowing you to add oft-visited keys to the Favorites menu, which
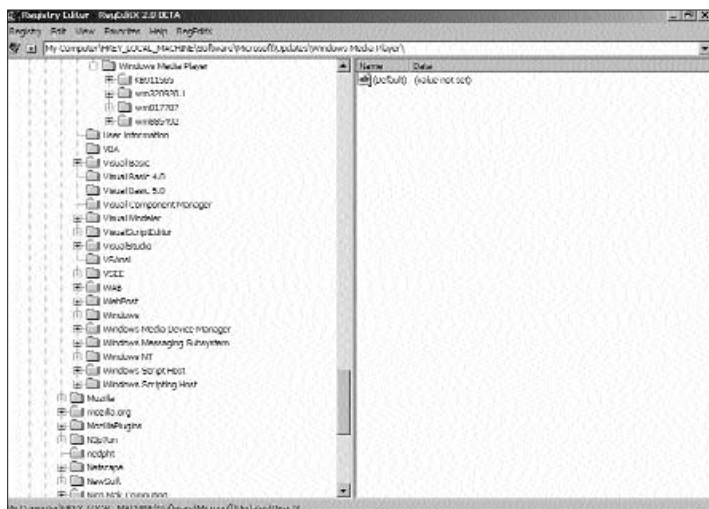
RegEditX has an Explorer-like address bar, making it easy to get right to that key you are looking for

enables you to quickly select the key when you next open RegEditX.

RegEditX and Registry Crawler are downloadable from **www.regeditx.com**.

RegEditX seems like a simple enhancement to Regedit, but the real power of the tool is unlocked with the shareware application called Registry Crawler. As the name suggests, this has a fast search algorithm that quickly scans the Registry for any keyword you type, and lists all the references to the keywords in a single screen. You can then right-click on any key and perform a variety of operations on the particular key entry—including opening the location in the Registry, editing the data, bookmarking the key, and deleting it.

In addition, Registry Crawler serves as a powerful tool to system administrators who can go through the Registries of multiple computers on the network, returning a list of Registry entries for
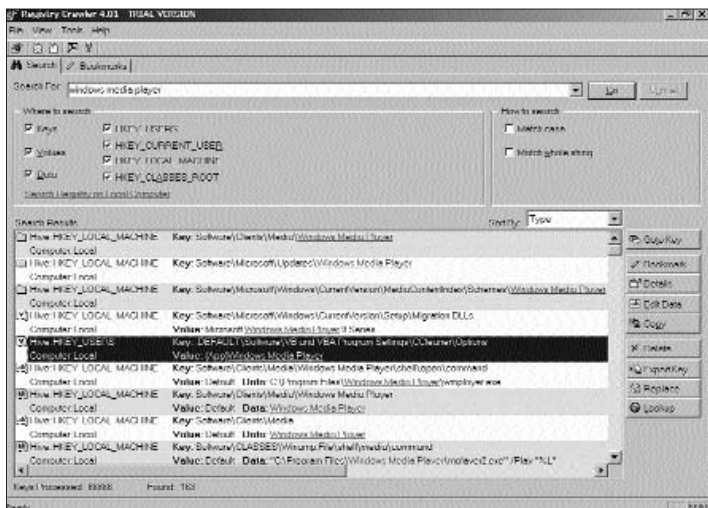
Registry Crawler will make registry editing a breeze

the chosen keywords. Both the local computer and network search results can then be exported into an HTML or text file report.

Another useful option for system administrators is information on "Access Denied" errors when scanning the Registry. This can serve as a warning flag, which they can investigate to verify if the access denial was legitimate, or a hack by an unruly user—or worse, a compromise of the Registry by a virus or other malware.

The only downside to this tool is the lack of the Undo functionality. Like Regedit, any changes to the Registry are permanent, with no record of the history of changes. This can make it cumbersome to roll back any edits when multiple changes to the Registry are being made.

3.1.3 Registry Workshop
Where Registry Workshop comes out ahead of the other Registry editors mentioned here is the Undo functionality. This, more than anything else, is a must-have capability for the avid Registry hacker. Many a time, even with all precautions taken, wrong Registry
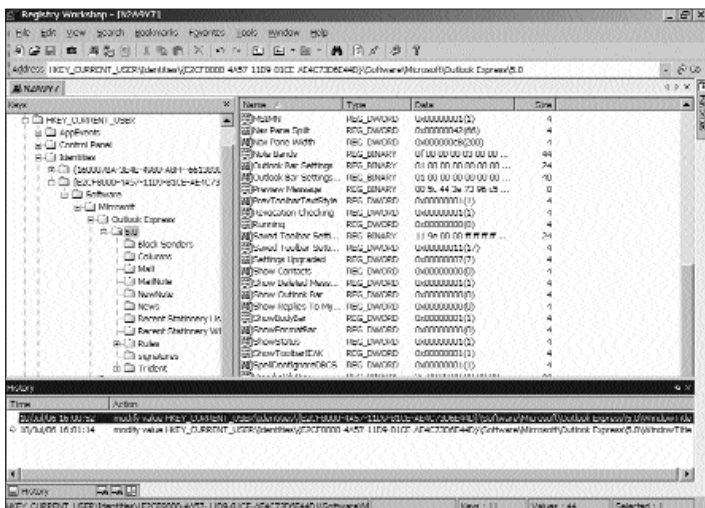
Registry Workshop

edits may be accidentally applied. Registry Workshop's undo list gives a complete history of the all the edits done on the Registry, making restoration a simple right-click rollback.

Registry Workshop is downloadable from **www.torchsoft.com**.

Like Registry Commander, Registry Workshop, too, supports all 12 data types, and has an interesting search feature where you can compare the results of two searches. This can be useful when searching for similar keys from different hives. It also supports bookmarks, Favorites, connecting to a network computer's Registry, and other functionalities found in the other editors.

Registry Workshop can take a snapshot of the local Registry. This can be useful if you want to compare changes to the Registry before and after installing an application which you suspect to be unruly, or if you want to inspect the Registry after a major change (like Registry cleaning) has happened. It also has the ability to open .reg files in the standard Registry tree structure view.

Opening a .reg file in the traditional tree structure will immediately reveal any inconsistencies in the syntax, while enabling you to add and delete values without being too careful to follow the syntax that needs to be followed when working with the .reg file in text mode.

3.2 Registry Trackers

Registry trackers are tools that enable you to view interactions with the Registry in real time. Such tools become very useful in troubleshooting and pinpointing application activity and interaction with the Registry. Registry Monitor and MultiMon are two such Registry tracking tools.

3.2.1 Registry Monitor

Much like a CPU monitor, Registry Monitor continuously monitors interaction with the Registry. It captures, in real-time, information regarding applications accessing the Registry, reading from it and writing to it.

Registry monitor is downloadable from **www.sysinternals.com/ Utilities/Regmon.html**.

This is a standalone .exe application. Using the menu and toolbar buttons, monitoring can be turned on or off and event capturing disabled. During Registry monitoring, the entries being captured can scroll through too fast for the eye. A useful feature controls the speed of the scrolling view, which can be slowed down to allow for online inspection of the entries, and the contents can be saved to an ASCII file for "offline" analysis.

There are usually many legal calls to the registry that Registry Monitor captures. These can number in the hundreds in a very short span of time, and can be daunting to wade through when trying to track down a specific problem. Registry Monitor has an

inbuilt filter, which can be used to narrow down the view list to only relevant entries. The highlight feature can be used to specify keywords that should be highlighted in scroll viewing. Additionally, you can directly access the location of the key in the Registry with a simple double-click. This will launch Regedit and directly navigate to the location of the key. You can then modify the Registry values as required.

3.2.2 MultiMon

MultiMon, a shareware application, can be thought of as the Swiss Army knife of monitoring software. It is a monitoring tool for your System, Devices, Files, Registry, Network, Keyboard, User and Clipboard. The interface is highly intuitive, with clear, self-explanatory labels that will have you up and running in a minute or two. While we will limit our discussion here to the Registry monitoring functionality, feel free to explore the other areas too!

MultiMon is downloadable from **www.resplendence.com/multimon**.

MultiMon's Registry monitoring is similar in functionality to that of Registry Monitor. However, the user interface is more intuitive, with checkboxes in the left pane enabling you to filter out the Registry activity of irrelevant processes. This will allow you to quickly concentrate on only the most relevant data.

Each application, when it launches, is assigned a process ID. This enables the CPU to keep track of all the tasks being processed for the application. Each process will have one or more threads that are each assigned an identifier by the system. This way an application can send multiple threads to the CPU for near-parallel processing. Knowing the thread ID and the process ID can help in monitoring an application's activity across the system.

In addition to the Registry keys' information, MultiMon also captures the process ID of the application that launched the interaction with the Registry, as well as the thread ID of the thread that

initiated the action. This information can be very useful when tracking down runaway processes and threads that hide themselves deep within the system and the Registry.

3.3 Registry Cleaners

One of the inherent problems with the Windows Registry is the number of obsolete entries it will accumulate over the life of the system. Applications that are uninstalled according to Microsoft's guidelines are required to remove themselves from the Registry as well. However, not all applications follow these guidelines, and more often than not, traces of the application will be left over in the Registry. This might not pose much of a problem in the beginning, but over time—especially if you are prone to installing and uninstalling a lot of applications—the pile of obsolete entries will begin to grow, and there will be a performance impact on the Registry, which in turn will impact the overall performance of the system. Also, if the software's uninstall program is sloppy, some Registry references may create problems for other installed applications or fresh software installations.

Registry cleaners attempt to solve this problem by scanning the Registry to fix and correct errors. These could include things like missing references to shared DLLs, unused file extensions, ActiveX and Class issues, obsolete software, shortcut paths, and more. There are no clear guidelines on how to effectively clean the Registry; as a result, developers of Registry cleaning software attempt their own methods. Some take an aggressive approach and attempt to clean everything that looks remotely obsolete or bad, which in some cases can do more harm than good. Others go for the middle path and exclude cleaning out entries for which there is some doubt.

A cleaned registry will improve system performance, since obsolete and erroneous entries will no longer slow down access to the Registry—thus improving application response time.

There are many popular freeware and shareware Registry cleaners. Each has its own fan following. While the jury is still out on how to effectively clean the Registry, we advise caution as the wiser course. Better to have a slightly slower system than break something, which "ain't broke" in the first place!

One approach is to not rely entirely on a single cleaner, and to use two or three cleaners that look at the Registry from different perspectives.

When choosing a Registry cleaner, there are two key factors to consider. One, the cleaner shouldn't be overly aggressive, as this can potentially cause more problems than solve them. Second, the cleaning should work consistently: that is, after cleaning once, when running the cleaner a second time, it shouldn't come up with the same (or a similar) number of errors.

Many cleaners, in a bid to show that they are superior to other cleaners, tend to include irrelevant results in their cleaning scan. This invariably gets repeated on subsequent scans, giving the impression that these cleaners are doing something special, while the fact is they are just picking up irrelevant results.

Ideally, you should start the computer, run the cleaner immediately (before opening any other applications), then reboot and do a second scan, and if warranted reboot again for a third scan. By the third scan, only low-severity persistent errors should be reported by the cleaner. These errors are, strictly speaking, not errors, but "ghost" entries left over from the normal working of the Registry—and are usually safe to ignore.

The cleaners we review here fulfil both the above conditions. One, they are not too aggressive in their scans; and two, once the cleaner has run through its scan once, a second or third scan will only pick up a minuscule number of entries that did not get reported during the first scan.

3.3.1 CCleaner

CCleaner (**www.ccleaner.com**) is a freeware system optimisation tool with an inbuilt Registry cleaner. It is light and fast, and can run through your Registry in minutes. It has a clean, user-friendly interface with a one-click operation to start the Registry scan. It takes a conservative approach to cleaning, and the errors discovered are listed for manual review. The problems discovered are classified under various heads such as Unused File Extension, Obsolete Software Key, Missing Shortcut Reference, and other issues. You can choose to skip fixing (or deleting) any of the entries that you feel are valid. Before fixing the Registry, CCleaner also prompts you to save a backup of the Registry prior to cleaning.

3.3.2 Easy Cleaner

Available from **http://personal.inet.fi/business/toniarts /ecleane.htm**, Easy Cleaner is another free and fast system cleaner that includes Registry cleaning. Like CCleaner, it takes a conservative approach to cleaning the Registry. The start-up screen gives you various cleaning options for different aspects of the system, including the Registry. Again, a single-click on the Find button starts the scan process. The results listed are a bit cryptic: Easy Cleaner doesn't attempt to classify the problems. This may be a bit confusing for the novice, though it does use green and red indicators against the entries that are safe (green) to delete and those (red) that are not. It is more aggressive than CCleaner, but it is usually safe to delete all the entries Easy Cleaner picks out. Nevertheless, it is advisable to review the results before deleting.

3.3.3 jv16 Power Tools

This is another collection of system optimisation tools that includes Registry cleaning. The latest version—jv16 Power Tools 2006, available from **www.jv16.org**—is a fully- functional 30-day trial product that must be purchased if you wish to use it beyond the trial period. They also have an older freeware version which is still available for download "in the wild." Run a Google search for "jv16 Power Tools 1.3.0.195" to find download sites for this product version.

Both versions are quite aggressive but safe, with the 2006 version providing superior results in its cleaning scan. The user interface is slightly advanced, and one can choose whether to opt for an automated cleaning session (not recommended) or for the manual procedure that allows you to review and select the entries to be fixed. Like in Easy Cleaner, the results have green and red indicators, but selecting any item will bring up extra details in the top part of the application interface. This can be very useful in making an informed decision whether to delete, fix or ignore the key change.

The above is not a definitive list, but rather a representative sample of what is out there and what to expect from Registry cleaning software. Overall, the cleaners mentioned here do a satisfactory job, with jv16 Power Tools giving the most options to the power user. One thing we haven't mentioned is that all these cleaners, either automatically or through a user prompt, back up the Registry before cleaning it. This should enable you quickly roll back should anything go wrong. Ensure you know the backup locations, and if you're curious, you can use an advanced Registry editor such as Registry Workshop to compare the state of the Registry before and after the cleaning operation.

Remember!

In what follows—the Registry hacks we're presenting—please bear the following in mind:

1. Often, references are made to keys in both HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER. The first is system-wide, and the changes indicated must be made there. The changes under HKEY_CURRENT_USER are user-specific.
2. If we say to navigate to a particular key and you find it doesn't exist, you'll need to create it.
3. Even if we haven't explicitly mentioned it, if you find a hack doesn't seem to work, try restarting your computer.

Hacks For Windows XP

This book covers a range of Registry edits, ranging from those for Internet software, to those related to personal computer security, and so forth. Included in this chapter, therefore, are those hacks that are applicable to XP but which don't fall into any other category.

So you're ready now—a little basic knowledge goes a long way. You want to speed things up, you want to make XP more intuitive to your personal way of doing things, you want to make it look pretty and impress your *khandhan* and friends...

But needless to say (at least now, after a dozen warnings!), delving into the Registry is not for the careless or faint of heart. The first and last rule when hacking XP's innards is to *back up* before doing anything. Ideally, keep a little notebook with you. Note down the changes you're making and the backup file prior to the change. This will help you quickly roll back to an earlier backup if things should go wrong.

A few general rules: if you make a change, it is best to reboot. If you are going to make a bunch of changes, do them all at one go and reboot. In most cases, you shouldn't face any problems. If you do, roll back to the last backup and go through the list again one by one between each reboot, until you reach the offensive hack. Sometimes you will need to re-create the String / DWORD / Binary values under a key, or even the key itself.

If a setting does not work as discussed, or, even worse, does the opposite of what was intended, reset it to the previous setting.

4.1 Performance

Eking the last bit of performance out of your XP machine is what this section is all about. Here's a list of some of favourite performance hacks.

Load Applications Faster

The Windows prefetcher aims to load applications faster by "prefetching" the application and storing it in the pre-fetch cache. You can speed up application loading by changing the default value of one the settings under the relevant key.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

The default value for the **EnablePrefetcher** setting is **3**. Change this value to **5** to make applications load faster. You can experiment with higher values—up to 9—and see if you get a further improvement.

Name	Type	Data
(Default)	REG_SZ	(value not set)
EnablePrefetcher	REG_DWORD	0x00000001 (1)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session ...

Since this relates to the system, a reboot is required for the change to take effect.

Optimisation Of The Boot Files

Normal file fragmentation scatters the pieces of a file all over your hard disk. This invariably also affects the files that load at boot time. You can defragment the files that load at system startup to enable faster loading.

Navigate to:
HLM\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction

A setting called **Enable** under this key needs to be set to **Y** (for Yes). This setting defragments the boot files, and it *might* relocate startup files into contiguous clusters on the volume, reducing the movement of the disk head when reading the volume.

With the setting at **Y**, boot file optimisation occurs automatically if the system is idle for 10 minutes. A reboot is required for the change to take effect.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Enable	REG_SZ	"Y"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunct ...

Prioritise!

Normally, multiple instances of the same application (such as multiple windows in Internet Explorer) will share a single process thread. If you have stability problems or slow application loads, launching each application in its own process will improve stability and speed up load times.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\PriorityControl

Optimise XP's process priority control by setting the DWORD Value for **Win32PrioritySeperation** to... well, the default is **2**, and **27, 28, 37, 38**, and more have all been quoted as good values (in decimal). Experiment a little. But after doing this, open My Computer, go to Folder Options under the Tools menu, choose the View tab, and check "Launch folder windows in a separate process."

This will run each application window in a separate process. However, note that that each process will consume the same amount of memory: this hack is therefore only recommended if you have 512 MB or more of system RAM. Ideally, a restart is not required.

Unload Unused DLLs

After an application is closed, XP has the annoying habit of leaving the associated DLL files in memory. This can hog precious resources and memory, and also cause stability problems. Make the DLLs unload themselves from memory after the program is done running.

Navigate to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\AlwaysUnloadDLL

Name	Type	Data
(Default)	REG_SZ	""

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion...

If the DWORD **AlwaysUnloadDLL** is not present, you will need to create it. Set the Value of the "(Default)" setting to **1**. Application-associated DLLs will get unloaded when the application is closed.

Run 16-bit Apps In Their Own Processes
Use this hack if you have more than one 16-bit application left over from the days of your nostalgia. XP runs all 16-bit applications in a single process. Having a separate process for each application can increase their stability and process.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\WOW

Browse to the String **DefaultSeparateVDM**. If it's not there, you'll need to create it. Set its value to **Yes**.

Disable User Tracking
Useless to most users—except perhaps for system administrators—XP's inbuilt user tracking system uses up precious resources.

The system keeps track of the programs run by a user, the paths followed, and the documents used. (Did you know your XP was spying on you all this while?) Disable this to free up system resources.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Set the DWORD **NoInstrumentation** to **1**. This will disable *most* of the user tracking features of XP.

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisableThumbnailCache	REG_DWORD	0x00000001 (1)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\...

Disable Thumbnail Caching

One of Explorer's features is to display a thumbnail of images and the first frame of the video when seen in Thumbnail view. Explorer can either create it when you access the folder or fetch it from the thumbnail cache. Fetching thumbnails from the cache is significantly faster, but will consume a lot of hard disk space, especially if your system is chock-full of images and video.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

Set the DWORD Value **DisableThumbnailCache** to **1** if you are low on hard disk space. Otherwise, it makes sense to leave it at zero—the thumbnail cache can indeed be useful.

Load Kernel Into RAM

In Windows 98, programs could be loaded and kept in RAM for as long as you wanted. You could even load a video clip into RAM directly and have it play from there! XP is much more restrictive, mostly due to security reasons. But when it comes to the Windows XP kernel, there's something you can do. By default, XP only loads the required parts of the kernel into RAM at boot time, and calls the other parts as and when needed. Having the entire kernel available in memory speeds up processing.

Navigate to:
HLM\System\CurrentControlSet\Control\Session Manager\Memory Management

Set the value of the **DisablePagingExecutive** key to **1**. This will make the entire kernel be loaded in memory. A reboot is required for the changes to take effect.

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisablePagingExecutive	REG_DWORD	0x00000001 (1)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session ...

Only use this hack if you have sufficient memory. Recommended: 512 MB or more. Also, this hack may affect some programs that use the Windows swap file directly, such as Adobe Photoshop.

Edit The Startup Programs List

Many of the programs that start up at boot time do not figure in the Startup folder. If you want to stop more than one application from loading at bootup, you will normally need to go and turn off the preference in each application one by one. Tedious and time consuming. This hack can help you do this in one go.

Navigate to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
And to:
HCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

All the programs that load at boot time will be specified under these two keys. Review the applications listed in this list and delete all the entries you don't want started up at boot time. Next bootup, they'll be gone.

Be careful not to delete needed programs such as anti-virus and anti-spyware programs. You should be able to identify them by their path if not by the file name.

Optimise The System Cache

Desktop systems are normally optimised for applications, and servers for file caching. Depending on how you use your system, you may want to optimise your system for either.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

Find the setting LargeSystemCache. Set this DWORD value to 1 for server behaviour or to 0 for desktop behaviour.

Some programs such as SQL Server and Exchange Server set this value during installation and override the change.

Turn Off Windows Animation

Windows animations—like those that happen when you minimise or maximise windows—look good, but only if you have the processing power and/or RAM. To get the most performance out of your system turn off this setting. You could do it via a host of settings in the GUI, but this Registry hack does it all in one fell swoop.

Navigate to:
HCU\Control Panel\Desktop\WindowMetrics

Change the value called **MinAnimate** to **0** to disable Windows Animation. A restart is required.

Disable The Desktop Cleanup Wizard

By default the Desktop Cleanup Wizard runs every 60 days to clean up unused shortcuts and other desktop items. Do you need this over-friendly tool? At any rate, you don't want it to run automatically—use this hack.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\ Explorer\Desktop\CleanupWiz

Modify the DWORD Value called **NoRun** to **0**, or to **1** to bring back the poor Wizard if you begin to pity it.

Control Master File Table Zone Reservation

On NTFS-enabled XP systems, you can control the amount of space allocated to the MFT. The MFT contains reference entries to all the files on the system. This can get fragmented over time and affect system performance. Use this hack to allocate sufficient space for the MFT.

Navigate to:
HLM\System\CurrentControlSet\Control\FileSystem

Modify **NtfsMftZoneReservation** to a value between **1** and **4**. For most users, a value of **2** is good enough. However, in this day of humongous hard disks, a better bet would be to set it at 4.

To be completely effective, this setting should be specified at the time the volume is formatted.

Automatic Window Refresh
Normally, there is a small delay after some information changes before it reflects in the GUI. If you need to see the information right away, you would need to press [**F5**]. The following will enable the system to do faster updates.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\Update

For faster updates, change the DWORD value called **UpdateMode** to **0**. The default is **1**.

A reboot will be required for the changes to take effect. Note that there is a likelihood of conflict if this setting is applied with system policies running: the UpdateMode value is used by system policies to Disable, Automatically or Manually check for a connection to the NETLOGON share of a domain controller. Change it back to the default if you are running system policies or are connected to a domain controller.

Die A Faster Death
If an application does not respond during shutdown, XP will normally wait for a while to see if open applications shut down safely.

Use this hack to shut down straightaway and not wait for any response from the application.

Navigate to:
HCU\Control Panel\Desktop
And to:
HKEY_USERS\.DEFAULT\Control Panel\Desktop

Name	Type	Data
(Default)	REG_SZ	(value not set)
AutoEndTasks	REG_SZ	"1"
WaitToKillAppTimeout	REG_SZ	"10000"

The first key is user-specific, and the second is system-wide. In both these locations, change the String value called **AutoEndTasks** to **1** to kill the application immediately, or **0** to prompt for user action. **WaitToKillAppTimeout** controls the default time, in milliseconds, before killing the application. Reduce this time to further speed up the process.

Control Auto-Reboot After A Crash
When Windows crashes due to application, hardware or any other system fault, it is by default set to automatically reboot. In some cases, if the crashing is persistent and you want to troubleshoot your PC, you might not want the system to go into auto-reboot mode.

Name	Type	Data
(Default)	REG_SZ	(value not set)
AutoReboot	REG_DWORD	0x00000001 (1)

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashCon...

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\CrashControl
Change the value of **AutoReboot** to **0** to prevent an automatic reboot after a crash.

Change Certain Folder Locations
Special folders such as My Documents, Desktop, and so on can be changed to any other location from that set by the default instal-

lation. There's a way to do this without a registry hack, but using the following hack is simpler. First, just move the required folders to the new locations. Then...

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

Open this Registry key and edit the full path for each special folder with the corresponding new path. For example, the default location of the My Documents folder is **"C:\Documents and Settings\username\My Documents**. Move the folder to, say, **"F:\Documents"**, and update the value for the **"Personal"** setting with the new path, that is, **"F:\My Documents"**, without the quotes.

The change should take effect immediately.

Change The Location Of The Windows Installation Files

If you installed XP from a CD and then copied the installation discs to your hard disk, use this hack to change the default installation folder that XP will look for when it searches for additional setup files later.

Navigate to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup

Change the String Value called SourcePath to one specifying the path to where the XP setup files are now stored. When you next need to access any setup files, XP will first look in this new location, instead of you having to click "browse" and browsing to there.

Disable The Search Assistant

The new search assistant is an annoyance to many people. Not only does it have a weird number of counter-intuitive search options, it also connects to the Microsoft site without the user's permission,

opening a potential door for compromise of privacy. Use this hack to disable the new search assistant and use the classic search interface.

Navigate to:
HCU\Software\Microsoft\Internet Explorer\Main
Set the String value for **Use Search Asst** to **"no"**. The default is **"yes"**.

Modify The Default Search Options

An incredibly useful hack! You've probably gone through the drill more than once—search, then specify that it's case-sensitive, then specify that you want to search subfolders, and so on and so forth. Use this hack to specify the search parameters that makes it most comfortable for you to search your system.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explorer

Set any of the following DWORD Values to 1 or to 0. What to set them to is obvious.

CaseSensitive: Do a case-sensitive search
IncludeSubFolders: Search subfolders
SearchHidden: Search hidden files and folders
SearchSlowFiles: Search tape backup
SearchSystemDirs: Search system folders

The next time you conduct a search, you won't need to enter a single parameter!

Change The Program Files And Common Files Directory

Change the default location where software will be installed and where the "common files" will be stored. These are normally found in **C:\Program Files** and **C:\Program Files\Common Files**. Both can be on independent volumes. This can be useful if, say, you're running out of space on the **C:** drive, and want to instruct

Windows to forever look elsewhere while installing programs. Removes the burden of pressing **"browse"** and browsing to the desired location.

Navigate to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion

Specify the String Value of the path of the new directories. For Common Files the setting is **CommonFilesDir**, and for Program

Name	Type	Data
(Default)	REG_SZ	(value not set)
CommonFilesDir	REG_SZ	C:\Program Files\Common File
ProgramFilesDir	REG_SZ	C:\Program Files

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion

Files the setting is **ProgramFilesDir**. All new software that is installed will refer to this key to identify where the common files and program files should be stored by default.

Control CPU Task Priorities

It is not possible to explain this tweak without getting into many technical details. But what it does is, it forces short processor time-slices to be allocated to foreground processes three times more often than the time-slices given to background processes.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\PriorityControl

Set the DWORD **Win32PrioritySeparation** to, well, any of a number of values.

3 (the default): Foreground and background tasks have equal priority.

2: Foreground tasks have higher priority than background tasks

1: Foreground tasks have maximum priority

0 (not recommended): Foreground tasks run in real-time. This

will most likely make your system hang, and is primarily to be used in mission-critical environments with supporting hardware.

This particular tweak should not be applied to a system running either SQL Server or IIS unless you're certain that you want to slow down those background processes.

4.2 Visual Enhancements

Once you've tuned your machine, you'll want to turn your attention to control how XP looks and behaves. This section shows you some of the best hacks to control the appearance of your XP box.

Add A Command-Prompt Right-Click To Every Folder

If you use the command line window a lot, this hack will let you open a command prompt at the selected directory.

Navigate to:
HCR\Directory\shell

Create a new sub-key called **Command** under the main key (that is, the new key will be **HCR\Directory\shell\Command**). Change the value of **"(Default)"** within that key to the text you'd like on the right-click menu, for example, **"Open A Prompt Here!"**

Create another, new sub-key under the key created above, again called "command" (so this key will be **HCR\Directory\shell\Command\command**). Change the value of **"(Default)"** here to **"cmd.exe /k cd %1"**, without the quotes. Now right-click on a folder, and voila!

Name	Type	Data
(Default)	REG_SZ	command.com /k cd "%1"
HKEY_CLASSES_ROOT\Directory\shell		

A Hotkey For Command Line Directory Completion

If you work at the command line for a considerable length of time, you will want this hack. Specify a key, which when pressed, will complete the directory name.

Navigate to:
HCU\Software\Microsoft\Command Processor

And to:
HLM\Software\Microsoft\Command Processor

The first key above is user-specific, the second is system-wide. Change the setting of **PathCompletionChar** to the DWORD hexadecimal value of the control character. For example, the value for the [**Tab**] key is **9**, [**Ctrl**] + [**D**] is **4**, and so on... each key or key combination has a value associated.

The complete list of possible control characters can be found at **http://en.wikipedia.org/wiki/ASCII**. The representation is in the form *^letter*, where the caret character represents the [**Ctrl**] key. Thus **^Z** = [**Ctrl**] + [**Z**], and has a hexadecimal value of **26**.

At the command prompt, when you type in the first letter or letters of a directory and press the completion key, it will display the first directory path matching your entry. Press the key multiple times to scroll through the choices.

Use this in conjunction with "A Command Line Command Completion Hotkey."

A Command Line Command Completion Hotkey

This is a hack of the UNIX shell command completion feature. You can type in the first few characters of a file name and then press a key to have the system complete it.

Navigate to:
HCU\Software\Microsoft\Command Processor

And to:
HLM\Software\Microsoft\Command Processor

Set the DWORD Value **CompletionChar** to equal the hexadecimal value of the control character for the required keyboard stroke. The hex values for the key combinations are as in *"A Hotkey For Command Line Directory Completion."*

Use any hex values corresponding to the desired control character. The complete list of possible control characters can be found at **http://en.wikipedia.org/wiki/ASCII**. The representation is in the form ^*letter*, where ^ represents the [**Ctrl**] key. Thus **^Z** = [**Ctrl**] + [**Z**], and has a hex value of **26**.

Type in the first few characters of the filename and press the key to complete it. If you have multiple files that begin with the same character string, press the [**Ctrl**] key multiple times to cycle through the available list of files.

Use this in conjunction with "A Hotkey For Command Line Directory Completion."

Name	Type	Data
(Default)	REG_SZ	(value not set)
CompletionChar	REG_DWORD	0x00000009 (9)

HKEY_CURRENT_USER\Software\Microsoft\Command Processor

Disable The Passport Balloon Reminder

A balloon reminder will annoyingly keep popping up asking you to enter your MSN Messenger username and password. Once you enter it, it will be stored—forever! If you don't want to be nagged by the balloon, use this hack to disable the reminder forever.

Navigate to:
HCU\Software\Microsoft\MessengerService

Change the Binary Value **PassportBalloon** to **"0a 00 00 00"** to permanently disable the reminder.

Control The Behaviour Of The Logon Screensaver

At the logon screen, Windows launches the specified (or default) screen saver after a specified timeout. Use this hack to disable, change or adjust the timeout of the screensaver.

Navigate to:
HKEY_USERS\.DEFAULT\Control Panel\Desktop

Modify the value of **ScreenSaveActive** to **1** or **0** to enable or disable the screensaver. Under **"SCRNSAVE.EXE"**, change the path to the **.scr** screensaver file you want. Adjust the value of the screensaver timeout in **ScreenSaveTimeOut** to your desired number (in seconds).

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ab ScreenSaveActive	REG_SZ	1
ab ScreenSaveTimeOut	REG_SZ	600
ab SCRNSAVE.EXE	REG_SZ	login.scr

HKEY_USERS\DEFAULT\Control Panel\Desktop

Control Capitalisation In File And Folders Names

With this hack, if you enter a file or folder name in upper case, Windows will change the entry to upper and lower case to make it more visually appealing.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

Modify the DWORD Value **DontPrettyPath** to **0**, and Windows will adjust the capitalisation. Set it to **1** and Windows will accept the capitalisation as entered. A restart might be required for the change to take effect.

Start Menu: Scrolling Or Columns?

By default, Start Menu items are cascaded as columns across the screen. This can get annoying and inconvenient when your Start

Menu list becomes large. This hack will enable you to switch the default Start Menu display mode to a scrolling menu.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

And to:
HLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ab StartMenuScrollPrograms	REG_SZ	Yes

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\...

To enable Start Menu scrolling, change the value of **StartMenuScrollPrograms** to "**Yes**". Set the value to "**No**" for the default multiple-column display. Reboot or log out and back in for the change to take effect.

Suppress Error Messages When Booting
This hack will suppress all pop-ups informing you that a device is not working or is causing an error. You might want to temporarily apply this edit if you know that a certain device isn't working, and you don't want to keep getting reminded.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\Windows

Change the value of the DWORD called **NoPopupsOnBoot** to **1**. This will suppress all error messages, but remember, you will not be warned even if the error is serious. If the pop-up is too annoying and you can't do anything about it, go ahead and suppress the error messages, but ensure that you periodically review the event logs to see that there's nothing going seriously wrong with your system.

If you do wish to be warned of critical errors, you can use another setting called **"Error Mode"**. Set the DWORD Value to **0** for no error suppression, **1** for suppressing system errors, and **2** for suppressing all errors.

The "New" Right-Click Command Goes Missing

After a Windows update, the much-used **"New"** option in the right-click could go missing. This hack will fix it.

Navigate to:
HCR\Directory\Background\shellex\ContextMenuHandlers \New

Add the following String Value:
{D969A300-E7FF-11d0-A93B-00A0C90F2719} to the **"(Default)"** setting under that key. If the "New" key is not present, create it and add the value.

Name	Type	Data
ab (Default)	REG_SZ	{D969A300-E7FF-11d0-A93B-0

HKEY_CLASSES_ROOT\Directory\Background\shellex\ContextMenuHa...

Display Attributes

This is something *nix folks have had all the time—the Attributes of files and folders. In Windows, if you want to see the file and folder attributes in Detailed View in Explorer, you'll need to use this hack.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explor er\Advanced

Set the DWORD Value called **ShowAttribCol** to 1 to enable a spanking new "Attributes" column.

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ShowAttribCol	REG_DWORD	0x00000001 (1)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\...

Don't Show Common Program Groups

If you don't want to see the "common groups" in the Start Menu, use this hack to disable it from getting displayed.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policie s\Explorer

And to:

HLM\Software\Microsoft\Windows\CurrentVersion\Policie s\Explorer

The first value above, as you know by now, is user-specific, and the second is the system-wide setting.

Change the DWORD Value of **NoCommonGroups** to **0** to disable the display, and to **1** to re-enable it.

Disable The Frequent Programs List

Use this hack if you don't want the list of frequently used programs in the Start Menu to show up.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policie s\Explorer

And to:

HLM\Software\Microsoft\Windows\CurrentVersion\Policie s\Explorer

Change the DWORD value of **NoStartMenuMFUprogramsList** to **1** to disable the display of the frequent programs list. If that DWORD doesn't exist, create it.

This will only work with the XP Start Menu, not the Classic Start Menu.

Remove Pinned Programs

Don't like the pinned program list in the Start Menu? We do—so we don't need to scroll—but some people don't like it. Use this Registry edit to get rid of it.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policie s\Explorer
And to:
HLM\Software\Microsoft\Windows\CurrentVersion\Policie s\Explorer

Change the DWORD value of **NoStartMenuPinnedList** to **1** to remove the pinned programs list. The default is **0**. The change should happen immediately, but as usual, if it doesn't, just restart!

This will also remove the Internet and E-mail Programs. Also, it only applies to the XP Start Menu and not the Classic Start Menu.

Name	Type	Data
(Default)	REG_SZ	(value not set)
NoStartMenuPinnedList	REG_DWORD	0x00000001 (1)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\...

Restore Folders Upon Startup

Another very useful hack! You can specify whether the folders that were open at the point of the last shutdown should re-open when the system starts up next. You can now reboot in the middle of exploring your computer, safe in the knowledge that all the windows will come back up when you restart.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explor er\Advanced

Change the DWORD value **PersistBrowsers** to **0** to *not* re-open

the folders when the system restarts. A value of **1** should be speci-
fied if the folders are to be re-opened.

Name	Type	Data
(Default)	REG_SZ	(value not set)
PersistBrowsers	REG_DWORD	0x00000001 (1)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\...

Hide Control Panel Applets

There are so many applets in the Control Panel that you never use!
This hack will let you hide any of the applets in the Control Panel.

Name	Type	Data
(Default)	REG_SZ	(value not set)
fax.cpl	REG_SZ	"No"
powercfg.cpl	REG_SZ	"No"

HKEY_CURRENT_USER\Control Panel\don't load

Navigate to:
HCU\Control Panel\don't load

(Yes, surprisingly, that key has an apostrophe!)

To hide the applets, you need to create a String Value for the
filename of the applet in question, and set the value of the setting
to No—or delete the key entirely to display the applet. The file-
names of most of the common applets are as below, for quick ref-
erence. You might or might not find all the following on your sys-
tem, and conversely, there could be applets on your system not
mentioned here.

access.cpl - Accessibility Applet
appwiz.cpl - Add/Remove Programs Applet
console.cpl - Console Applet
timedate.cpl - Date and Time Applet
desk.cpl - Display Properties Applet
fax.cpl - Fax Applet

hdwwiz.cpl - Hardware Wizard Applet
irprops.cpl - Infrared Port Applet
intl.cpl - International and Regional Settings Applet
inetcpl.cpl - Internet Settings Applet
joy.cpl - Joystick Applet
liccpa.cpl - Licensing Applet
main.cpl - Mouse and Keyboard Applet
mlcfg32.cpl - Mail Applet
mmsys.cpl - Sound and Multimedia Applet
modem.cpl - Modem and Phone Applet
ncpa.cpl - Network and Connectivity Applet
netcpl.cpl - Network and Dial-up Connectivity Applet
nwc.cpl - Netware Client Applet
odbccp32.cpl - ODBC Applet
devapps.cpl - PC Card Applet
ports.cpl - Ports Applet
powercfg.cpl - Power Management Applet
sticpl.cpl - Scanner and Camera Applet
srvmgr.cpl - Server Manager Applet
sapi.cpl - Speech Properties Applet
sysdm.cpl - System Applet
telephon.cpl - Telephony Applet
tweakui.cpl - TweakUI Applet (if you have TweakUI installed)
nusrmgr.cpl - User Manager Applet
wspcpl32.cpl - WSP Client Applet
quicktime.cpl - QuickTime Applet
S32LUCP1.cpl - Norton Live Update Applet

Get Rid Of The Hand

When you share a local resource on the network, a "hand" icon is placed under the item to show that it's shared. You can remove the icon if you want to.

Navigate to:
HCR\Network\SharingHandler

Find the **SharingHandler** key. To remove the "hand," clear the

current data from the "(Default)" value, which is a String Value. To restore the icon to the default, enter **"ntshrui.dll"** there. Restart Windows for the change to take effect.

Implement A User-Based Custom Shell
Windows allows you to selectively specify the system shell based on the logged-in user. For example, this allows one user to use the standard Explorer interface, and another to use the legacy "progman" shell.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
And to:
HLM\Software\Microsoft\Windows\CurrentVersion\Policies\System

The second value is the system-wide setting, and the first value is for the currently logged-in user.

Create or modify the String Value called Shell and set it to the filename of the replacement shell.

4.3 Just For Fun

Now that you've got XP purring along and it looks and behaves exactly as you want it to, here's some fun stuff you can still do when you're bored!

Change Registered Owner And Organisation Name

If you've accepted the default owner name (computer name) in office, say, or if you've entered the wrong information during installation—or if you just want to change it to something funny!—you can use this hack to change the details.

Name	Type	Data
(Default)	REG_SZ	(value not set)
RegisteredOwner	REG_SZ	"Joe Bloggs"
RegisteredOrganization	REG_SZ	"ACME, Inc."

Navigate to:
HLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Modify the String Values **RegisteredOwner** and **RegisteredOrganization** as required. Put in the new values without the quotes.

Create Your Own Tips

If you are getting bored of the Windows tutorial tips that appear when you log in to windows, use this hack to change and add your own tips.

Navigate to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Tips

The tips are listed in alphabetical or numerical sequence. You can either replace the string values in the existing tips, or create your own tips, or increment the existing letters or numbers and

enter a string value with your own tip. For example, if the last tip is designated "**Y**", the next tip could be "**Z**" with your String Value text.

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ab Z	REG_SZ	"Don't forget to visit ..."

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion...

You can use any message in the String Value; it needn't be a tip! For example, try "**Don't forget to call home!**" as a tip and see how it appears when you next log in.

Hide The Username On The Start Menu

Use this hack to hide the Username that is usually displayed in the XP start menu—not the Classic Start Menu, where the username is not displayed.

Navigate to:

HCU\Software\Microsoft\Windows\CurrentVersion\Policie s\Explorer

And to:

HLM\Software\Microsoft\Windows\CurrentVersion\Policie s\Explorer

Change the DWORD Value **NoUserNameInStartMenu** to **1** to hide the username display. The default is **0**.

Remove Or Change The Shortcut Arrow Icon

A tiny little modification to XP. If you prefer not to see the short-cut arrow icon in the bottom corner of the shortcut, use this hack to change it—or even remove it.

Name	Type	Data
ab (Default)	REG_SZ	(value not set)
ab 28	REG_SZ	"c:\windows\system\shell32.dll,

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion...

To delete the icon, remove the entry **IsShortCut** from the following keys:

HCR\lnkfile (in "lnkfile", it's a small "ell," not an "I")
HCR\piffile
HCR\InternetShortcut

To change the icon, go to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Icons

Change the String Value entries for the setting **"29"** to the path and filename of the new icon. Setting this value to blank has the same effect as deleting them, but without any side effects.

By deleting the icon, Windows no longer considers these shortcuts as shortcuts. There maybe some side effect in using the shortcuts after this change: in some cases, deleting the arrow for .LNK files leads to duplicate items in the Explorer context menu. Ideally, rather than deleting the icon, just remove the file path to be on the safe side.

Add A Custom Folder To My Computer Or The Desktop

This hack will create a custom folder—like the special My Documents folder—and one that cannot be deleted or renamed!

Navigate to:
HCR\CLSID

Create a new key with a Globally Unique Identifier (GUID). The GUID is a 128-bit identifier that is usually generated by Windows. This can be a random number that is used to uniquely identify COM objects when required for a Registry entry. Examples of GUIDs are:

{**25892e17-80f6-415f-9c65-7395632f0223**}
{**a53e98e4-0197-4513-be6d-49836e406aaa**}
{**e33898de-6302-4756-8f0c-5f6c5218e02e**}

These GUIDs should only be used on personal machines as their uniqueness cannot be guaranteed. GUIDs are usually generated by Windows, and not manually entered as we're doing here. If the GUID is distributed in runtime apps, there is the probability—however remote—of it clashing with the existing GUIDs.

For this example, we'll use a random GUID: **{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}**.

Hence, the key value will be: **HCR\CLSID\{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}**

Set the value of the "(Default)" setting for this key to the name of the folder—say "Digit Archive". Create a new sub-key under the main key and call it **"DefaultIcon"**. That is, create a key called:

H C R \ C L S I D \ { F D 4 D F 9 E 0 - E 3 D E - 1 1 C E - B F C F - ABCD1DE12345}\DefaultIcon

Set the value of the **"(Default)"** setting to the filename and path of the icon file you want to use for this folder. For example, **"C:\digiticon.ico"**, without the quotes. If you don't specify a path to an icon file, Windows will use its default folder icon.

Create another sub-key under the main key called **"InProcServer32"**, that is, create the key called:
H C R \ C L S I D \ { F D 4 D F 9 E 0 - E 3 D E - 1 1 C E - B F C F - ABCD1DE12345}\InProcServer32

Set the **"(Default)"** setting here to **"shell32.dll"**. Create another String Value called **ThreadingModel**, with the value set to **"Apartment"**.

There's more! Create another sub-key called

H C R \ C L S I D \ { F D 4 D F 9 E 0 - E 3 D E - 1 1 C E - B F C F - ABCD1DE12345}\Shell\Open My Folder\Command
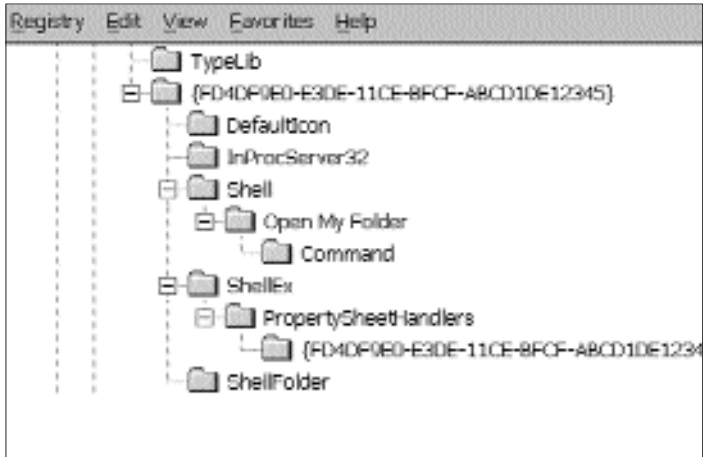
Set the "**(Default)**" value here to the command that should be executed when the folder is clicked. In this case, it would be "**explorer /root, c:\Digit Archive**"

Create another set of sub-keys called

H C R \ C L S I D \ { F D 4 D F 9 E 0 - E 3 D E - 1 1 C E - B F C F - ABCD1DE12345}\ShellEx\PropertySheetHandlers\{FD4DF9E0- E3DE-11CE-BFCF-ABCD1DE12345}

Then create another sub-key called

H C R \ C L S I D \ { F D 4 D F 9 E 0 - E 3 D E - 1 1 C E - B F C F - ABCD1DE12345}\ShellFolder

Under this key, create a new Binary Value called **Attributes** with the value "**00 00 00 00**".

To put the folder on the Desktop, add the following key: **HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\Desktop\NameSpace\{FD4DF9E0-E3DE-11CE-BFCF- ABCD1DE12345}**

To place the folder in My Computer, add the following key:
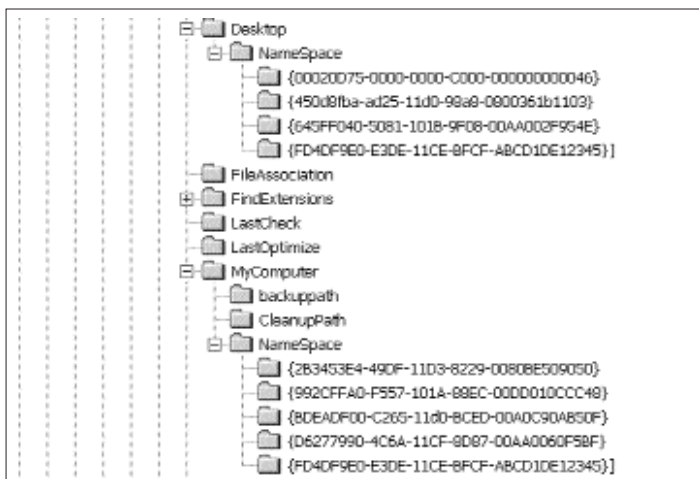
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\MyComputer\NameSpace\{FD4DF9E0-E3DE-11CE-BFCF-ABCD1DE12345}

The folder cannot now be removed or renamed without reversing the above steps.

Change The Window Title In WMP
Use this hack if you want to give the Windows Media Player window title something descriptive and/or creative, for example, **"WMP"**. (This is a non-creative, non-descriptive title, but you can do better.)

Navigate to:
HCU\Software\Policies\Microsoft\WindowsMediaPlayer
And to:
HLM\Software\Policies\Microsoft\WindowsMediaPlayer

Set the String Value for the setting TitleBar to the required text you wish to display, in our sad case, "WMP". To revert to the default title, delete the TitleBar setting entirely. Just restart WMP to see the effect.

Pop Up A Banner When Windows Boots

You might want to have a banner pop up when a user is going to log on, a banner that contains any kind of message you want to display. This can be used to display the company's policy, for example. Or a warning message to trespassers telling them to buzz off!

Navigate to:
HLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ WinLogon

Create a new String Value here called **LegalNoticeCaption**. Enter whatever you want to see in the bar at the top. Now create another new String Value called **LegalNoticeText**. Modify it to the message you want to display each time Windows boots.

Name	Type	Data
(Default)	REG_SZ	(value not set)
TitleBar	REG_SZ	"My Media Player"

HKEY_CURRENT_USER\Software\Policies\Microsoft\WindowsMediaPl...

The message will be displayed at the next logon.

Remove Items From The System Tray

We can't think of a really good use for this one, and it's just for fun that we're including it here. We all use the System Tray in the Taskbar, but you can get prevent any items from appearing there - except the time, if you've set the clock to appear in the System Tray! So once you apply this hack, the System Tray will be blank except for the time.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer

And to:

HLM\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer

Create a DWORD Value in both locations called NoTrayItemsDisplay. Set it to 1 to make items in the System Tray vanish. Come to think of it, this is a cool prank hack! Just log out and back on for the change to take effect.

Remove "File" From Explorer

Ever used the File menu in a Windows Explorer window? We're guessing not. In fact, did you even know it was there? It's useless. But equally useless is this hack, which removes the menu.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer

And to:

HLM\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer

Create a DWORD Value in both locations called NoFileMenu. Set it to 1, or back to 0 if you want the File menu to reappear.

Make DLLs Display Their Icons

By default, Windows Explorer displays a generic icon for all DLL files. Some poor DLLs actually offer their own icons. So if you'd like to know at a glance which ones have icons, you'll need to go through the following procedure. Remember that this tweak will cause the first icon contained in a DLL to be displayed in Windows Explorer.

Navigate to:
HCR\dllfile\DefaultIcon

Back up the key you are about to modify: highlight "(Default)"

in the right frame and select Export Registry File... . Save the file to the location of your choice, so if you don't like the results of this tweak, double-click the exported file to undo the changes you are about to make.

Then, right click "(Default)" and choose Modify. Replace all the information contained in the Value data: field with %1. Now reboot and launch Windows Explorer. Look at the file called Shell.dll in C:\Windows\System and note that it - and many other DLLs - now display an icon of their own!

Increase Balloon Tip Notify Time
Frankly, a silly hack - just for fun! This one will, of course, increase the time for which balloon tips will be displayed.

Navigate to:
HCR\Software\Microsoft\Windows\CurrentVersion\Explorer\TrayNotify

Create or modify the DWORD called BalloonTip to reflect a value of 0000000a. You might need to restart for the change to take effect.

Add Copy to / Move to To The Right-Click
An extremely useful hack, which adds "Copy to folder" and "Move to folder" to the right-click menu of every file and folder. When you select, say, "Copy to folder," you'll get an Explorer-style menu where you can navigate and choose the destination folder.

Navigate to:
HCR\AllFilesystemObjects\shellex\ContextMenuHandlers

Create a new key here called "Copy To". Change the "(default)" value to
{C2FBB630-2971-11D1-A18C-00C04FD75D13}

Then, in the same key (HCR\AllFilesystemObjects\shellex

\ContextMenuHandlers), create a new key called "Move To". Change its "(default)" value to

    {C2FBB630-2971-11D1-A18C-00C04FD75D13}

The change will be effective immediately.

Hacks For
Microsoft Office

Who doesn't want to hack Office? The thing is, many changes and customisations for Office are possible from within the Options, so here, we're only including those changes that need a Registry edit.

Greek And Latin

You might have seen some characters in MS Word getting printed out as little square boxes—such characters include Greek symbols and such. This happens on printers that don't support Unicode characters. Here's a hack to make those gammas and lambdas print out properly.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Word\Options

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

Create a new String value (or modify the existing value) called **NoWideTextPrinting**. Set it to **1** to enable the interesting characters. The default is **0**.

When you use this setting, print quality may be lower than when you have direct Unicode support.

If You Like Four-Digit Dates

Excel, like everything pre-2000, shows dates in the two-digit format. Many people use four digits for the year these days, and you can force Excel to do the same.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Excel\Options

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

Create a new DWORD value (or modify it if it's already there) called **EnableFourDigitYearDisplay**. Set it to **1** for four digits, and to **0** for two digits.

The change should be effective immediately; if it's not, restart Windows.

Which Wastebasket?

If, in Outlook 2003, you have deletion privileges for the mailbox of another user. When you delete items from his or her Mailbox folder, the items go into *your* Deleted Items rather than his or hers—which is the intuitive thing to happen. Here's how to bring in that behaviour into Outlook. First, exit Outlook.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Outlook\Options\ General

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

There should be a DWORD value called **DelegateWastebasketStyle**. If there isn't, create it.

Edit the value. Make it **8** to store items in your own folder (Outlook's default behaviour), or **4** to make the deleted items go into the mailbox owner's folder.

You only need to restart Outlook for the change to take effect.

Make sure you have at least Author Level rights for the Deleted Items folder of the owner's Mailbox.

Those Pesky Little Clipboards!

Office 2000 onwards, when you select multiple items and copy them to the clipboard at the same time, you get this little box with several smaller boxes inside it—saying "1 of 12", "2 of 12" and so on. It's irritating when you copy something, use it, then copy something else—the thing pops up! In fact, we'd bet you never even use the multiple clipboards feature. Disable that dialog box.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Common\General

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

Here, find the DWORD **AcbControl** (or create it if it doesn't exist.) Set it to **1**. (And to **0** later if you actually need to use multiple clipboards and want the dialog box.

Simply start (or restart) any Office application and the change will be effective.

Prevent Office Help From Stealing Space

This is a little weird—on some systems, the following doesn't happen at all, and on some, it does. If Office resizes the main application window when you access the Help, you might want to turn off that behaviour.

While in an Office application, press [**F1**]. If your main window gets resized and you don't like it...

Navigate to:
HCU\Software\Microsoft\Office\11.0\Common\HelpViewer

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

In all probability, a DWORD called **IsFloating** won't be present; create it and set its value to **1**. (If it's already there, it's probably set to **0**—reset it to **1**.)

To see the change, exit the Registry Editor and start (or restart) any Office program. Naturally, to reset what you've done, you can either delete the key or set it back to **0**.

Save To Where You Want To

You probably find the Places bar in XP very useful—the one that pops up when you do a **File > Save As** or a **File > Open** operation. You get My Documents, Desktop, and more. It's so very conven-

ient—just press Desktop instead of navigating.

But did you know you could add any drive whatsoever to this places bar? Like, say, a folder called **"My Latest Documents"**, or **"Office Work"** or something? Here's how to accomplish this.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Common\Open Find\Places\UserDefinedPlaces

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

Create a sub-key under **UserDefinedPlaces** called **Place{Number}**. Replace "**{Number}**" with any number starting with **1**, so you have **Place1**, **Place2**, and so on.

Under **Place{Number}**, create two String Values called **Name** and **Path**. As you might expect, the **Name** is what you want to appear in the Places bar, and the **Path** is the full path to where you want documents saved—for example, "**F:\OfficeWork**", with the quotes.

Close the Registry Editor, start or restart an Office application, and voila—a new place to click on and save to instantly!

Trim The Places Bar

This Registry edit is a companion to the previous one. If you never save to, say, the Desktop, you can remove "Desktop" from the places bar. Or "My Documents". Or anything else that's there by default, and you can also use it to remove places you added yourself using the previous Registry edit. Say you want to remove "Desktop".

Navigate to:
HCU\Software\Microsoft\Office\11.0\Common\Open Find\Places\StandardPlaces

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

Select the sub-key called Desktop, and there, create a new DWORD value called Show. Set it to 0. If you want to bring back that place, you'll need to either delete the sub-key or (the smarter way of doing it) resetting it to 1.

Start or restart any Office program to see the changes.

Kill 'em All!

If you're like most people, you hate the Office assistants. Now, there's an option within each Office program to stop using the Office assistant, but if you want to derive joy out of annihilating the Assistants, and do it for all Office programs in one go...

Navigate to:
HCU\Software\Microsoft\Office\11.0\Common\Assistant

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

Delete *all* the DWORD values in that key. Yes, it sounds drastic, but that's what you need to do. Clippy and the gang are now dead.

Hide The (Useless) Help Field

In every Office application, unless you've meddled around with some setting we don't know of, you'll see a space where you can "Type a question for help." What's the need for the bar when you can just press [**F1**]? In any case, it's not fair that the bar should be there all the time, since we don't use Help every single session. Remove it. Here's how.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Common\Toolbars\Settings

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

Unfortunately, you can't kill five or six birds with one stone: you'll need to create DWORD values for each Office program. For example, to make the change in Word, Create a DWORD value called **"Microsoft Word AWDropdownHidden"**. Note that you shouldn't put in the quotes, and note the spaces. Before the **"AWDropdownHidden"** comes **"Access"** for Microsoft Access, and so on. For PowerPoint, it's **"Powerpoint"** (note that the second "p" is in lowercase.)

Then, of course, set all these values to **1**, and back to **0** if you want the box back. Start or restart any Office program to see the changes.

Make Office Use The System Font

This is a silly hack, but it's interesting. You just might want to use the standard system font for the Office UI, instead of Microsoft Office's own fonts. The standard system font is what you set in the system properties by, for example, right-clicking on the Desktop, going to Appearance, and choosing "Large Fonts" (or something else).

To make Office use the font you selected as the system font, do the following.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Common\General

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

You should find a DWORD Value called **UseOfficeUIFont**. No prizes: set this to **0** to use the Windows system font, or to **1** to make Office use its own fonts. Start or restart any Office program to see the changes.

Disable Hyperlink Warnings

Depending on your settings, when you click on a hyperlink in a document, Office might display a warning. When you click on, say, a picture linked to an executable, Office will almost certainly display a warning. You might want to disable these messages, since we're assuming you know what you're doing. These warnings happen only in Office 2003, so the following is applicable only to that version.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Common

Here you should find a key called Security. Create it if it's not there. Select the newly-created key, and there, create a DWORD called **DisableHyperlinkWarning**, and set it to **1**, of course, to disable the warning messages.

You also need to navigate to:
HCU\Software\Policies\Microsoft\Office\11.0\Common

Do the same thing as above—finding or creating a key called **Security**, and the DWORD Value. Set it to the same value (**0** or **1**) as you did in the previous entry. Start or restart any Office program to see the changes.

I, Me, Mine

Office 2000 and XP allow you to change the company and individual the product is registered to, via two registry edits.

Navigate to:

(For Office 2000)
HLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\{00000409-78E1-11D2-B60F-006097C998E7}
(For Office XP)
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{90280409-6000-11D3-8CFE-0050048383C9}

Here, change the values of **RegCompany** and **RegOwner** to what you need.

Then, navigate to:
HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\ Common
("10.0" is for Office XP; it would be "9.0" for Office 2000.)

Here, rename the **UserInfo** sub-key to **OldUserInfo**.

Close all Office programs and restart one of them. The values should reflect both in the splash screen and in the About dialog box.

Optimise Find Fast In Office 2000

This edit seems to apply only to the 2000 version of Office. Office 2000 comes with a Find Fast Indexer that helps in increasing file search speed. This, however, may not be a good thing on large drives; the system may slow down when an index is being created or updated. Use the following Registry edit to delay the indexing for a specified amount of time between index updates—which, in turn, will reduce heavy system activity and improve performance.

Navigate to:
HLM\Software\Microsoft\Office\9.0\Find Fast

Create or modify a DWORD called **SlowDown** and set it to the delay time in milliseconds. The default is **1000** (1 second).

Take Charge Of Your Minions

If you don't not like the Office Assistants and haven't disabled them entirely, here's how to control their behaviour.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Common\Assistant

Here, create or modify DWORD values as follows.

AsstAssistWithWizards: Should the Assistants help with Office wizards? 0 or 1.

AsstAssistWithHelp: Should the Assistants help with help? 0 or 1.

AsstAssistWithAlerts: Should the Assistants open for Office alerts? 0 or 1.

AsstGuessHelp: Should the Assistants try and guess what help topics are shown? 0 or 1.

AsstKeyboardShortcutTips: Should tips about keyboard shortcuts be shown? 0 or 1.

AsstFeatureTips: Should tips about using features more effectively be shown? 0 or 1.

AsstMouseTips: Should tips about using the mouse more effectively be shown? 0 or 1.

AsstMoveWhenInTheWay: Should the assistants move when in the way? 0 or 1.

AsstOnlyHighPriorityTips: Specifies that only high priority tips be shown. 0 or 1.

AsstShowTipOfDay: Specifies whether the Assistants should show the tip of the day at startup. 0 or 1.

AsstSounds: God again knows you want to set this to 0, but this key specifies whether the Assistants are allowed to make sounds. 0 or 1.

AsstTipTimeout: Useful. This specifies the number of seconds before the tip bulb is brought down. Time in seconds.

Disable Error Reporting

You can turn off the error reporting feature in Office, which sends debug information to MS if and when a program crashes.

Navigate to:
HCU\Software\Policies\Microsoft\Office\11.0\Common

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively. However, the key doesn't exist on some Office 2003 installations, in which case you're better off not trying this hack.)

Create four DWORD Values as below, and set them all to **1**:
DWNeverUpload
DWNoExternalURL
DWNoFileCollection
DWNoSecondLevelCollection

Also navigate to:
HLM\Software\Policies\Microsoft\Office\10.0\Common

...and do the same thing as above.

You just need to restart your Office program for the change to take effect.

Don't Restrict My Attachments!

In Outlook 2002 and 2003, you can't open some attachments. .exe attachments are fine for this, but what about, say, .reg files? Or, for that matter, what do you do if you *want* to send an EXE? The sender has to go through some trouble—save him that trouble using this Registry edit.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Outlook\Security

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

Create or modify the String Value called **Level1Remove**. Set its value to a semi-colon-separated list of the extensions you want Outlook to deliver. For example, if you want to allow .exes, .bats and .inf files, set the value to **".exe;.bat;.inf"**—without the quotes. Restart Outlook for the change to take effect—there's no need to restart Windows.

Here's the list of attachments blocked by Outlook 2002 and 2003 by default: **.ade, .adp, .asx, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .hta, .inf, .ins, .isp, .js, .jse, .lnk, .mda, .mdb, .mde,**

.mdz, .msc, .msi, .msp, .mst, .pcd, .pif, .prf, .reg, .scf, .scr, .sct, .shb, .shs, .url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh.

Paranoia: Delete Them For Good

If you're paranoid, you won't be delighted to know that when you delete an item from Outlook, some parts of it may still be accessible from the .pst files (where Outlook stores data). Fortunately, there's a Registry hack to get around this problem. If it's a problem for you, that is.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Outlook\PST

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively. However, the key doesn't exist on some Office 2003 installations, in which case you're better off not trying this hack.)

Create or modify the DWORD value called **PSTNullFreeOnClose**. Set it to **1** to purge deleted data. **0** is the default, but we recommend you change that post haste.

Log out of Windows and log back in for the change to take effect, but since you're paranoid enough to have applied this hack, a better idea would be to restart Windows.

Set A Dedicated Directory

Attachments that you open in Outlook have been saved in a pre-existing, known folder, whose names go something like **"djj392u9d0dwh."** This isn't gibberish; those folders have certain known names, and that fact makes for a potential security threat. Make a dedicated folder to save your attachments to before you view them.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Outlook\Security

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

Create or modify the String Value called **OutlookSecureTempFolder**. Set its value to the folder you want, such as **"H:\OutlookAttach"**—without the quotes.

You might need to restart Windows for this to begin working, though logging out and back in might do it.

Tired Of The Same Outlook Today?

Did you know you could set any URL you want to be displayed instead of the usual Outlook Today page? The URL can be on the Internet or on your intranet. Here's how you set this.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Outlook\Today

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

If the **"Today"** key doesn't exist, you'll need to create it under **"Outlook"**. Now, create a String Value called **Url** and set it to whatever you want. For example, if you want Digit's homepage, you'd type in **"http://www.thinkdigit.com"** without the quotes.

You only need to restart Outlook to see the results.

Have Word Help You A Little Less

In Word, in the Open, Save, or Save As dialogs, the program tries to complete the filename you're entering. If you like this, skip this hack, but many of us don't. Here's how to disable this auto-complete feature.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Common\General

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

Create or modify the String Value called **Use AutoComplete**. Set it to either **Yes** or **No**, depending, obviously, on what you want. You'll need to either log off and back on, or restart Windows for the change to take effect.

If you have Office 2000, install the Office 2000 SR-1/SR-1a Update for this tweak to be able to take effect.

Repair Word The Easy Way

There's no need to panic if Word behaves oddly in respect to your customisations. For example, you created a toolbar and it's gone missing, or you personalised Word in some other way and those settings aren't retained. Simply reset Word to its default settings and start over, via this Registry edit.

Navigate to:
HCU\Software\Microsoft\Office\11.0\Word\Data

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

This key is what you need to get rid of. But don't get rid of it entirely—just rename it, by right-clicking on the key and selecting Rename. You can rename it to anything you want.

You just need to start or restart Word for the change to take effect. The edit will clear your list of recently accessed documents, too. Also, if you find something amiss, simply go back to the renamed key and rename it to **"Data"**.

Too Many Cooks...

On a network, when you open a Word document that's locked for editing by someone else, you have the option to edit a local copy and merge the changes later. You can disable this feature if you'd

like only one person to use a document at a time, navigate to:
HCU\Software\Microsoft\Office\11.0\Word\Options

(Here, the "11.0" is for Office 2003; for Office XP and Office 2000, it's 10.0 and 9.0 respectively.)

Create or modify the DWORD value called **NoPromptToForkDocuments**. Give it a value of **1**. (Or to **0** if you want to revert to the default.)

Log off and back on, or restart Windows, for the change to take effect.

Internet Software

Haccio
Lumos MS
Expresso !*

* IT MEANS: 'HACKER, SHED LIGHT
ON OUTLOOK EXPRESS, NOW!'

Here's an assortment of hacks—some useful, some just for fun—for Internet Explorer, Outlook Express and Windows/MSN Messenger. Tweaks for browsers such as Firefox do not figure here—this chapter is dedicated to what came bundled with Windows. (For some Firefox and Opera hacks, refer *Tips & Tricks* in this, the August 2006 issue.)

6.1 Internet Explorer

Use An Alternate Source Viewer With IE
When you view source in Internet Explorer, Notepad is launched as the text editor. If you want to change this, here's how.

Navigate to:
HLM\SOFTWARE\Microsoft\Internet Explorer\View Source Editor\Editor Name

If the "Editor Name" key does not exist, create it. Set the "(Default)" value to equal the full path and filename of the required text editor, for example, "D:\Program Files\MyEditor".

Just restart Internet Explorer for the change to take effect.

Change Auto-Complete Mode
In Windows Explorer as well as in Internet Explorer, the Auto Complete does two things: it appends the text it suggests to what you've already typed, and also displays a drop-down list from which you can choose an address. You can choose what you want.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explore\AutoComplete

Here, create or modify the String Value called Append Completion. Set it to Yes if you want Explorer (or IE) to append the suggested text as you type, or to No if you only want to see a drop-down list.

You'll need to restart Windows for the change to take effect.

That Irritating Floating Thing!
IE 5.5 onwards, when an image is displayed and you hover your mouse over it, a little floating toolbar comes up—with buttons to save, print, and do other things with the image. It's pretty use-

less, since you can do a right-click on the image—and since you do the right-click anyway out of habit. Prevent that toolbar from appearing!

Navigate to:
H C U \ S o f t w a r e \ P o l i c i e s \ M i c r o s o f t \ I n t e r n e t Explorer\PhotoSupport

Here, create or modify the DWORD Value called MyPics_Hoverbar. Set it to 0 to allow the thing to come up, and to 1 to prevent it from coming up.

Restart Windows or log out and log back in for the change to take effect.

Download ActiveX Files To A Specific Location

The default path where the ActiveX files are installed when you download an ActiveX control is Windows\Downloaded Program Files. It might be a good idea to change this location.

Navigate to:
H L M \ S O F T W A R E \ M i c r o s o f t \ W i n d o w s \ CurrentVersion\Internet Settings

Change the ActiveXCache String Value to the desired download location, for example, "F:\MyActiveX".

Also navigate to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ActiveX Cache

Here, change the "0" value to the same folder you specified in the other location.

You just need to restart IE for the change to take effect.

Get Rid Of The "Links" Folder

Persistently popping-up things are always irritating, especially if they're useless! IE creates a folder called Links in the Favorites menu. Delete it and it comes back. Plus, in all likelihood, you don't need it. Get rid of it.

Navigate to:
HCU\Software\Microsoft\Internet Explorer\Toolbar

Here, set the LinksFolderName String Value to a blank string. Then open IE and delete the Links folder from the Favorites menu. That'll be the last time you'll be doing it!

Edit With What You Want

IE, by default, attempts to detect the program that was originally used to create an HTML document, and modifies the Edit option so the same program is used for editing the document later. You'd probably want to use your default editor, which you've set, so you might want to not make IE check what program was used.

Navigate to:
HCU\Software\Microsoft\Internet Explorer\Main

Create or modify the String Value called CheckDocumentForProgID. Set it to Yes or No.

Restart Windows or log out and back in for the change to take effect.

Disabling the feature will cause Internet Explorer to use the default HTML editor for all editing.

No Tabbed Browsing Is A Pain...

Unless you're using the IE7 beta, the default behaviour is for Internet shortcuts to open in an existing window, without creating a new one. In many cases, you might want a new window spawned.

Navigate to:
HCU\Software\Microsoft\Internet Explorer\Main

Create or modify the DWORD value called AllowWindowReuse. Set it to, of course, 0 to make IE spawn a new window for each hyperlink clicked, and to 1 to use an existing window. You may need to restart Windows or log out and back in for the change to take effect.

TIFFS With IE
IE has many things to not like, and there are also several tweaks to modify its behaviour, as you've gathered by now. For example, when you click a link to a Tagged Information File Format (TIFF) image, the Open button in the File Download dialog box may be disabled. If you want to open the image in Internet Explorer...

Navigate to:
HCR\.tif

Change the String Value "(Default)" to Imaging.Document.

Then, navigate to:
HCR\.tiff

Here, do the same thing you did above. You'll need to restart Windows for the change to take effect.

Manage The Partial Address Feature In IE
The Internet Explorer partial address feature scans common domains for a match to a keyword entered in the address bar. The feature is limited by default to searching only .com, .net, .org and .edu domains. This tip allows you to add new domains and modify their priorities.

Navigate to:
H L M \ S O F T W A R E \ M i c r o s o f t \ I n t e r n e t Explorer\Main\UrlTemplate

The values listed under that key control which domains are auto-searched for matches to the keyword entered in the address bar. To add a new domain, simply create a new String Value and name it a sequential number (for example, "5"). Set the data of the new value to equal the domain you want to search; for example, to also search .co.uk domains, add the value "www.%s.co.uk" (with the quotes).

(Here, "%s" just represents the keyword; you can leave it as "%s" to include the entire domain).

To change their priorities, simply rename the values with sequential numbers, where "1" is the site to be checked first. This includes the existing domains (.com, .net, .org and .edu).

Text Only, Please

In IE 5 and greater, the "Text/Plain" Content-Type header field may not be used, and text files may not open properly. The following edit forces IE to treat files with that header as text files.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\ Internet Settings

Create or modify the DWORD Value called IsTextPlainHonored, and set it to 1 to treat those pages as text files. 0 is the default. Restart or log out of Windows and log back in for the change to take effect.

Control the IE Script Debugger

When Internet Explorer detects an error on a page it has the ability to launch a script debugger to diagnose the problem. If you have no use for the script debugger, you could use the "yes" value below.

Navigate to:
HCU\Software\Microsoft\Internet Explorer\Main

Create or modify the String Value called "Disable Script Debugger" and set it to either "yes" to disable the debugger or "no" to enable it.

Just restart Internet Explorer for the change to take effect.

Control Internet Explorer's Error Reporting

This setting allows you to control whether the error reporting tool, which reports browser debugging errors to Microsoft, is active in Internet Explorer 6.0.

Navigate to:
HLM\Software\Microsoft\Internet Explorer\Main

Create a new DWORD value called IEWatsonDisabled and set it to 1. Create another DWORD value called IEWatsonEnabled and set it to 0.

Just restart Internet Explorer for the changes to take effect.

The Sound Of Music

Here's a just-for-fun hack. When you start navigating a site in IE, it plays a WAV file—the default is that click sound you've heard so often. If it irritates you, get rid of it. To freak out your friends, make it play a tune!

Navigate to:
HCU\AppEvents\Schemes\Apps\Explorer\Navigating\
.current

Create or modify the String Value called "(Default)" and set it to the full path name of the sound you want to play. Leave it blank to force no sounds to emanate from IE when you're browsing.

Restart or log out of Windows and back in for the change to take effect.

Disable Internet Explorer Download Notification

This setting is used to disable download completion notification in Internet Explorer. The following can be useful if the checkbox next to "Close this dialog box..." is disabled and cannot be manually un-checked.

Navigate to:
HCU\Software\Microsoft\Internet Explorer\Main

Create or modify the String Value called NotifyDownloadComplete and set it to "yes" or "no", without the quotes, according to what you want. Restart or log out and back on for the change to take effect.

Make IE Not Mess With FTP

When you enter an FTP command at the command prompt—for example, "FTP ftp.somesite.com"—IE might intercept the command and launch itself, instead of allowing the DOS-based FTP program to launch. You might want this, or you might not. Here's the Registry edit for this.

Navigate to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\URL\Prefixes

To disable IE from launching, delete the "ftp" value there. To re-enable the interception by IE, create a new String Value called ftp and set it to "ftp://"

Checking For Internet Explorer Updates...

Internet Explorer 5 and higher have the ability to automatically check for updates. This tweak controls that feature.

Navigate to:
HCU\Software\Microsoft\Internet Explorer\Main

Create or modify the DWORD value called NoUpdateCheck and

set it to 1 to disable the update check, or to 0 to enable it. Just restart Internet Explorer for the change to take effect.

The Default Download Directory
As with many programs, you might want to specify a default download directory for Internet Explorer.

Navigate to:
HCU\Software\Microsoft\Internet Explorer

Here, create or modify the String Value called Download Directory and set it to the full path name of the directory you want to set, for example, "D:\Downloads". Restart or log out of Windows and back in for the change to take effect.

Specify The Location Of The Online Support Site
When a user selects "Online Support" from the Internet Explorer help menu, he or she is usually redirected to a Microsoft Web page. This tweak allows you to specify an alternate URL. This could be used as a prank hack.

Navigate to:
H L M \ S O F T W A R E \ M i c r o s o f t \ I n t e r n e t Explorer\Help_Menu_Urls

Create or modify the String Value called Online_Support and set it to the URL you wish to redirect the user to.

You may need to restart or log out and back on for the change to take effect.

This tweak can also be applied on a per-user basis under the [HKEY_CURRENT_USER] hive, that is, the same location as above with HLM changed to HCU.

Lots Of Settings For Controlling IE

These settings allow you to control a wide range of IE's features.

Navigate to:
H C U \ S o f t w a r e \ P o l i c i e s \ M i c r o s o f t \ I n t e r n e t Explorer\Restrictions

And to:
H L M \ S o f t w a r e \ P o l i c i e s \ M i c r o s o f t \ I n t e r n e t Explorer\Restrictions

In both these locations, set the following DWORD Values to 0 to disable and to 1 to enable the settings.

AlwaysPromptWhenDownload: Always prompt the user when downloading files. Useful in the event of a mistaken click.

NoBrowserBars: Disable changes to the browser's scrollbars. Some sites could change the default scrollbars.

NoBrowserContextMenu: Disable the right-click context menu. Useful as a prank hack—or to prevent people saving, say, images.

NoBrowserOptions: Disable the Tools > Internet Options menu. Comes in handy when you don't want people messing with settings.

NoBrowserSaveAs: Disable the ability to "Save As." Also, on some systems, this also disables the "Save" functionality. Good if you want people on your computer to just browse, get their work done with, and leave.

NoNavButtons: Disables the Forward and Back navigation buttons. A prank hack, of course.

NoPrinting: Remove Print and Print Preview from the File menu. Useful if, in an office, you want to impose restrictions such that only certain applications are allowed to print.

NoSelectDownloadDir: Disable the option to select a download directory. Since this would force all downloads to the default directory, you have an easy way of checking what has been downloaded.

Change The Internet Explorer Search Assistant
Use this hack to change IE's search assistant from the default to any engine you wish to use.

Navigate to:
HLM\SOFTWARE\Microsoft\Internet Explorer\Search

Change the String Value "SearchAssistant" to a URL of your choice.

Change The Internet Explorer Window Title
You can change the title of the Internet Explorer window and call it anything you like, for example, "Sucks But I Need To Use It Sometimes."

Navigate to:
HCU\Software\Microsoft\Internet Explorer\Main

Change the String Value called "Window Title" to any text you like. To change it back to the default, delete the "Window Title" entry.

Disable Internet Explorer Downloads
To disable file downloads via Internet Explorer...

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

And to:
HLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

In both these locations, set the value of the setting "1083" to a DWORD value of 3 to disable downloads. To re-enable downloads, change this value to 0.

Disable IE's Custom Search Page

When you click on the search button on IE's standard toolbar, a customisable search page opens on the left. This hack disables IE's inbuilt search page. Almost none of us use it anyway.

Navigate to:
HCU\Software\Microsoft\Internet Explorer\Main

Change the value of "Use Custom Search URL" to 0 to disable the custom search.

6.2 Outlook Express

A New Look For OE

If you want, you can change the page that Outlook Express loads in the right-hand window when it starts-up, or, the page that appears under "Outlook Express" if you've set it to go to the Inbox directly.

Navigate to:
HCU\Identities\[Identity]\Software\Microsoft\Outlook Express\5.0

Create or modify the String value called FrontPagePath. Set it to the URL or filename of what you wish to be displayed. Restart or log out of Windows and back in for the change to take effect.

Sick Of The OE Splash Screen?

If you're like us, you're tired of the OE splash screen—especially so because you probably open OE several times a day. One Registry key gets rid of it.
Navigate to:
HCU\Identities\{Unique   Identity}\Software\Microsoft\ Outlook Express\5.0

Here, create a new DWORD Value called NoSplash. Obviously, set it to 1 to disable the splash screen, and back to 0 when you start missing it. Just restart OE, and the blue thing won't show up.

Back Up OE Blocked Senders and Mail Rules

Here's how to back up and restore your Blocked Senders list and other mail rules in Outlook Express 5 and later.

For The Blocked Senders List:
Navigate to:
HCU\Identities\{GUID}\Software\Microsoft\Outlook Express\5.0\Block Senders

"GUID" represents the unique user identifier. In the Registry menu, click Export Registry File. Save the file to a known location.

For Other Mail Rules:
Navigate to:
HCU\Identities\{GUID}\Software\Microsoft\Outlook Express\5.0\Rules\Mail
On the Registry menu, click Export Registry File, and save the file to a known location.

If multiple Identities are in use for Outlook Express, these steps should be repeated for each Identity. The GUID cannot be immediately identified, but looking in, for example, the Mail Rules, should give you an idea of what corresponds to whom.

Too Little Of A Good Thing

With Outlook Express, you can normally view and save all attachments, including .exe files. You just might want to change this. Of course, if you want to download an exe, go back to the key and temporarily reset what you changed.

Navigate to:
HLM\SOFTWARE\Microsoft\Outlook Express

Create or modify the DWORD value called BlockExeAttachments. Set it to 1, and back to 0 at any time you want to allow .exe attachments to get through. Restart or log out of Windows and back in for the change to take effect.

Change The Location Of The WAB

Just as you might want to change the location where your mails are stored, you might also want to change where your Windows Address Book (WAB) is stored.

Navigate to:
HCU\Software\Microsoft\WAB\WAB4\Wab File Name

Create or modify the String value called "(Default)" and set it to the location you want, such as "F:\MyAddBook", without the quotes. You may need to restart or log out and back on for the change to take effect.

The WAB used by Outlook Express is normally located in [Windows]\Application Data\Microsoft\Address Book.

Use Smooth Scrolling In OE
If you want to enable smooth scrolling when viewing messages in Outlook Express 5.0 and above, here's a simple Registry edit.

Navigate to:
HCU\Identities\{Unique   Identity}\Software\Microsoft\ Outlook Express\5.0\Trident\Main

Create or modify the DWORD value called SmoothScroll and set it to 1 to enable smooth scrolling, or to 0 to disable it.

You may need to restart or log out and back on for the change to take effect.

This feature may slow down Outlook Express when navigating messages with lots of graphics.

Prevent Account Changes In OE
Use the following hack to prevent users from creating or modifying any of the OE accounts for mail, news or directories.

Navigate to:
HLM\SOFTWARE\Microsoft\Outlook Express

Change the DWORD Value "No Modify Accts" to 1 to enable the restriction. 0 is the default and allows unfettered access.

Change Internet Auto-Dial Settings
When the dial-up password is saved and the "Connect

Automatically" setting is enabled in the dialler, Internet Explorer can automatically launch the dial-up connection whenever a browser window is opened. Control the auto-dial features of Internet Explorer (and therefore Outlook Express) with this tweak.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\ Internet Settings

Change the DWORD Value EnableAutodial to 0 to disable auto-dial, and to 1 to enable it.

Decouple MSN Messenger From Outlook Express

When you open OE, and MSN Messenger is enabled, you are also automatically logged into Messenger. This can be very irritating. Here's how to do away with that.

Navigate to:
HLM\SOFTWARE\Microsoft\Outlook Express

Change the DWORD Value "Hide Messenger" to 2 to remove Messenger from Outlook Express. This hack is also applicable to AOL Instant Messenger.

6.3 Windows/MSN Messenger

MSN Instant Messenger Restrictions

These restrictions are used to disable various features of MSN Instant Messenger.

Navigate to both these keys:

HCU\Software\Policies\Microsoft\Messenger\Client
HLM\Software\Policies\Microsoft\Messenger\Client

Do the following in both these locations. For each restriction from the list below, create a new DWORD value and set the value to 1 to enable the restriction.

DisableCollaborationApps
DisableFileTransfer
DisablePC2PCAudio
DisablePC2Phone
DisableVideo
PreventAutoUpdate
PreventBackgroundDownload
PreventRun

Restart MSN Messenger for the changes to take effect.

Here's a description of the above values.

DisableCollaborationApps determines whether the Whiteboard and application sharing features in Windows Messenger are enabled or disabled.

DisableFileTransfer determines whether the file transfer feature in Messenger is enabled or disabled.

DisablePC2PCAudio determines whether the computer-to-computer calling feature in Messenger is enabled or disabled.

DisablePC2Phone determines whether the computer-to-phone calling feature in Messenger is enabled or disabled.

DisableVideo determines whether the video feature in Messenger is enabled or disabled.

PreventAutoUpdate disables the automatic update feature in Messenger.

PreventBackgroundDownload is used to enable or disable silent download of any file in the background when Messenger is running.

PreventRun determines whether Messenger is enabled or disabled.

I *Know* You're There!

When you minimise MSN Messenger by pressing the top-right cross, it very helpfully (or not so much) tells you via a pop-up that it's still running. Why?

Navigate to:
HCU\Software\Microsoft\MessengerService

Create or modify the Binary Value called DSBkgndMode. Set it to

01 00 00 00

to disable that useless pop-up. The default is 00 00 00 00.

Restart or log out of Windows and back in for the change to take effect.

My Card Number's Safe, Thank You

MSN Messenger gives you a warning every time you start it: "Never give out your password or credit card number in an instant mes-

sage conversation." You can customise this message just for fun, or if you have a company, you can make the message reflect company policy. You can also make a blank message appear, of course.

Navigate to:
HLM\SOFTWARE\Microsoft\MessengerService\Policies

Create or modify a String Value called IMWarning. Set it to whatever text you want to show up as the warning.

Restart or log out of Windows and back in for the change to take effect.

A New-Look Messenger
You always see those two rounded characters in the MSN Messenger window—change that picture to whatever you want!

First, locate the installation directory for MSN Messenger, which could be, for example, C:\Program Files\Messenger. This location can be found in the Registry.

Navigate to:
HLM\SOFTWARE\Microsoft\MessengerService

Look at the InstallationDirectory value. That's where your file is. Then go to that folder, and rename the "lvback.gif" file there to "lvback.old", just for a backup. Then copy your desired image (this should be a GIF) to the folder and name it "lvback.gif."

Just restart MSN Messenger for the change to take effect.

Remove Windows Messenger From IE
This tweak can be used to remove the integration of Windows Messenger into Internet Explorer: it will remove both the toolbar icon and Tools menu item.

Navigate to:
HLM\SOFTWARE\Microsoft\Internet Explorer\Extensions\
{FB5F1910-F110-11d2-BB9E-00C04F795683}

Highlight the key and select Edit > Rename, then add a minus symbol ("-") to the start of the key name so that it is now called "-{FB5F1910-F110-11d2-BB9E-00C04F795683}".

Restart Internet Explorer for the change to take effect. To re-enable Messenger integration, rename the key and remove the minus symbol.

Hardware
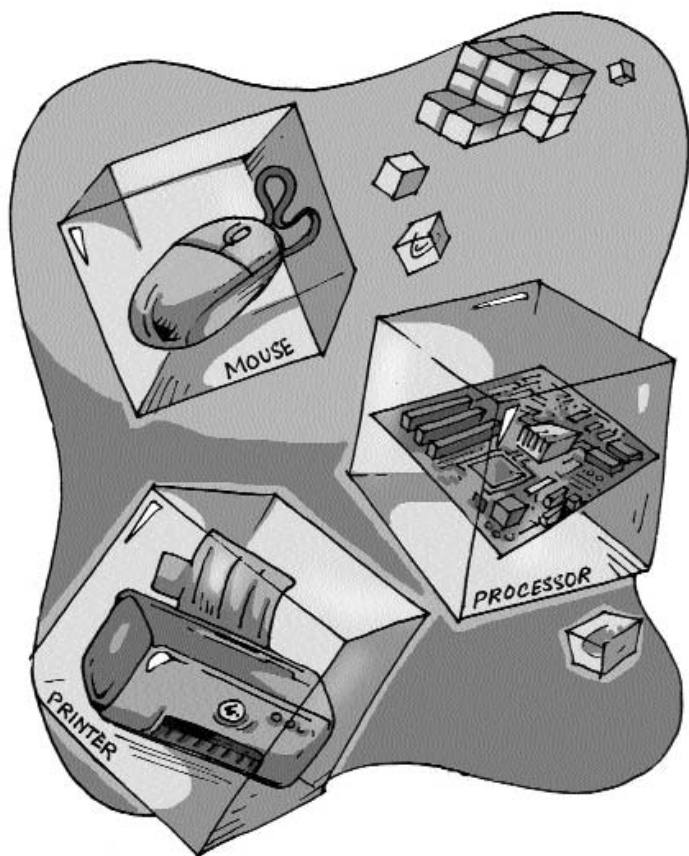
Covered here are hacks related to peripheral devices. You might want to change the behaviour of your mouse or keyboard, or make printing more efficient. With a couple of exceptions, the Registry edits we mention here do have something to do with the Windows interface or with Windows itself, but each of them is related to a peripheral.

No More DVDs!

You can make your computer pretend not to have a DVD drive. The following tweak is useful if, say, you have kids at home and you don't want them to play DVDs on the computer. Or, you have a large CD/DVD collection, you're away from home, and you don't want your friends messing with your collection.

Navigate to:
HCU\Software\Microsoft\MediaPlayer\Player\Settings

The value name of interest here is EnableDVDUI. It should be a String Value (REG_SZ). Create it if it's not there, or modify it according to what you want. "No" will disable the drive, and "Yes" will enable it.

A reboot is required for the changes to take effect. This hack has been found not to work on some systems, so you'll just have to take pot luck. If it doesn't work, just delete the value (EnableDVDUI) you created!

Reclaim Your Optical Drive

This hack might help if your optical drive isn't being detected. This hack is applicable if your drives disappear after you uninstall Adaptec Easy CD Creator versions 5.01 and earlier, or DirectCD version 3.01 or 3.01c. It should also work if your drives have disappeared for no apparent reason, or after various program installations and/or upgrades. In any case, it doesn't hurt to try it. You'll need to restart to see your drive again—if the hack works, that is.

Navigate to:
HLM\System\CurrentControlSet\Control\Class\{4D36E965-E325-11CE-BFC1-08002BE10318}

Delete the values inside the keys UpperFilters and LowerFilters. If that doesn't seem to work, go ahead and delete the keys themselves. You'll need to reboot to see if you've had any luck after that.

Enable UDMA66 Or UDMA100 Mode

DMA stands for Direct Memory Access, and refers to the capability to transfer data directly between, say, two hard disks, without the need for the CPU to interfere (hence "direct"). Now, as hard disks became faster, and as the need to increase transfer speeds came up, it was found that increasing the speed of the interface itself caused problems. The efficiency of the interface itself had to be improved in addition, and what resulted was the creation of new types of DMA transfer modes called Ultra DMA modes. UDMA66 is also called Ultra DMA Mode 4, and also Ultra ATA/66.

If you have an Intel chipset that supports UDMA66 or UDMA100 (you can find this out from the manual), you might find that that mode is disabled by default—and you might certainly want to enable it! You could use the Device Manager to do this, but in some cases, that doesn't work—in which case you'll need to modify the Registry. *Make sure* your Intel chipset supports one of the two modes mentioned above, *otherwise bad things might happen*. Naturally, since this is a low-level hardware hack, you'll need to restart after making the change.

Navigate to:
HLM\System\CurrentControlSet\Control\Class\
{4D36E96A-E325-11CE-BFC1-08002BE10318}\0000

Create a new DWORD value called EnableUDMA66 (or EnableUDMA100, as the case may be). Set its value to 1 to enable the ultra DMA mode, or to 0 to disable it.

Convert a FireWire Device To A Dynamic Disk Drive

A dynamic disk is a physical disk that provides features that "basic" disks do not, such as support for volumes spanning multiple disks. Such a disk contains dynamic volumes—such as simple volumes, spanned volumes, striped volumes, mirrored volumes, and RAID-5 volumes. Note that dynamic disks are not supported on notebooks or in XP Home Edition. This hack is for converting a FireWire disk to a dynamic disk.

Navigate to:
HLM\System\CurrentControlSet\Services\Dmadmin\
Parameters

Create a new DWORD value here called EnableDynamicConversionFor1394 if it doesn't exist, or if it does, modify the existing value. 0 is the default value; set it to 1 to enable the conversion to a dynamic disk. You may need to restart or log out for the change to take effect.

Do not convert FireWire disk drives to dynamic disk drives if they will be moved to other hosts.

Juggle The Keys Around

How often do you use the Windows key that's found on almost all keyboards today? Probably not too often, except when a program setup takes up the entire screen and you need to access your icons. If you press it accidentally, you need to press [Esc], which is a minor irritant. There's a registry hack to disable the Windows key should you wish to do so.

Navigate to:
HLM\System\CurrentControlSet\Control\Keyboard Layout

Here, create a new Binary value (or modify the existing value) called "Scancode Map" and set it to the following. Don't bother with what appears in the editing box—just type in the value below exactly as it is (you don't need to use the spacebar):

00 00 00 00 00 00 00 00 03 00 00 00 00 00 5B E0 00 00 5C E0 00 00 00 00

Logging out and logging back in should bring the change into effect, but you might need to restart.

In fact, you can change any key to any other! Essentially, each key has a code, and you need to specify how many keys you are

remapping. Apart from lots of zeroes, you specify the code of the key you're going to press, and you specify the code of the key you want it to become. For example:

The left [Alt] key is 38 00.
[Backspace] is 0E 00.
So the remapping of left [Alt] to [Backspace] would be 0e 00 38 00. Note the order.

Now, there are eight pairs of zeroes at the beginning of the Scancode map, and four ending pairs of zeroes. Since we're changing only one key, we need to use 02 00 00 00. (Two keys would be 03 00 00 00). After that comes the mapping, then the ending zeroes.

So, to remap left [Alt] to [Backspace] would be

00 00 00 00 00 00 00 00 02 00 00 00 0E 00 38 00 00 00 00 00

Just visit www.usnetizen.com/fix_capslock.html for a complete list of Scancode maps. Also remember that the value to use to disable a key is, of course, 00 00. Here are a few useful values.

[Caps Lock]: 3A 00
Left [Ctrl]: 1D 00
[Tab]: 0F 00
[Enter]: 1C E0
Left [Shift]: 2A 00
Right [Shift]: 36 00

Disabling [Caps Lock] would therefore be eight leading pairs of zeroes, followed by 02 00 00 00, followed by 00 00 (for the disabling), followed by 3A 00 (for [Caps Lock]), followed by four pairs of zeroes. Try changing someone's [Enter] key to [Backspace]!

Make Your NIC Do Some Work

This applies only if your network adapter has an onboard processor: you can find out from the spec sheet whether or not it does. If it does, it has been designed to offload network processing computations from the CPU. This hack can reduce system slowdown during high-speed data transfers.

Navigate to:
HLM\System\CurrentControlSet\Services\Tcpip\Parameters

Create a new DWORD value called DisableTaskOffload and set it to 0 to enable the NIC's processor. Of course, if the key exists and is set to 1, reset it to 0.

A restart is required for the change to take effect.

Take Control Of Your Modem

You've probably experienced this if you're on dial-up: if remote connections are enabled, your computer initiates an Internet connection—at startup or when an application demands it—and you find your modem dialling all on its own. Here's how to disable that behaviour.

Navigate to:
HLM\SOFTWARE\Microsoft\Ole

Create a new String value (or modify the existing value) called EnableRemoteConnect. Set it to N to disable your modem stealing control. Of course, you can always set it to Y if bad things happen after you do this.

A restart is required for the change to take effect.

Change The Priority Of The Print Spooler

The "priority" of a task is the degree of urgency that the task presents to the processor—requests from a task with higher priority are served earlier. Now, the default setting for the Print Spooler is to

run at normal priority. Now if you mostly use your computer for printing, use this hack to change the priority class of the Print Spooler.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\Print

Create a new DWORD value called SpoolerPriority and set it according to what value you want (or if it exists, just set the value):

0xFFFFFFFF for Idle Priority
0 for Normal Priority
1 for High Priority

Print Scheduler Priority
Here's how to control the priority of the Print Scheduler.

Navigate to
HLM\System\CurrentControlSet\Control\Print

Create a new DWORD value called SchedulerThreadPriority and set it to one of the following. Note that the value might already exist.

0 is for Normal
1 is for Above Normal
ffffffff (eight "F"s) is for Less Than Normal

Log off and log back in, or restart, for the change to take effect.

Beep On Print Job Errors
Ever wished you'd get some kind of warning when there's a job error on a remote print server? Here's the hack to make your computer beep repeatedly when this happens.

Navigate to
HLM\SYSTEM\CurrentControlSet\Control\Print

Here, a (new or existing) DWORD value called BeepEnabled needs to be set to 1.

Log off and log back in, or restart, for the change to take effect.

Spool Elsewhere

This hack allows you to change the default Print Spool directory. You could possibly relocate it to a more spacious disk. The default directory is %SystemRoot%\system32\spool\printers. There are two things you can do here—set a new directory for all printers, or only for a specific printer. First, restart your computer, or alternatively, stop and start the Spooler service.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\Print\Printers

Here, change the value of the String Value DefaultSpoolDirectory to the full path of the newly created directory, for example, "F:\NewSpool" (with the quotes).

To change the spool directory only for one printer, under the above key, find the sub-key that corresponds to the printer in question. Here, modify the value of the String Value SpoolDirectory to the full path of the folder you want to use.

Remember to create the directory first; if it does not exist when you edit the Registry, Windows will use the default path.

Print Job Pop-Ups

You might or might not, by default, be receiving a notification (by way of a pop-up message) when your print job has been completed. If you do and it's an irritant, or if you don't and you need it, use this Registry edit.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\Print\Providers

Here, create or modify a (the) DWORD value called NetPopup. Set its value to 1 to enable the pop-up notifications, and to 0 to disable them.

Restart the Print Spooler service for the change to take effect. You might need to restart Windows if that doesn't work.

Save Processor Power
Your processor polls your USB ports once every millisecond. It keeps doing this, even if you aren't going to attach any USB devices. You can increase the polling interval—essentially by enabling "USB idling"—thus allowing some processors to enter power-saving mode.

Navigate to:
HLM\System\CurrentControlSet\Control\Class\{36FC9E60-C465-11CF-8056-444553540000}\0000

Create a new DWORD value called IdleEnable and set it to 1 to enable USB idling, thus increasing the polling interval.

Restart Windows for the change to take effect.

Native Processor Performance Control In XP
The following tweak applies to processors with either Intel SpeedStep or AMD PowerNow! processor performance control technologies. Windows includes inbuilt processor performance control to utilise it more efficiently. Some CPUs that support the aforementioned technologies have trouble with random hangs under XP. Even if you've installed an updated CPU driver, XP might not have enabled it. This hack is for such cases.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\P3\Parameters

Here, create a new DWORD value (or modify the existing value) called HackFlags, and edit its value according to the following.

0: Disables native XP support

1: Use settings inherited from Intel software during your XP upgrade

5: Allow XP to support all modes when on battery

You will need to restart for the change to take effect.

Games Hanging On An Athlon Processor?

If you have an AMD Athlon, and if Windows often hangs when you run a game, it could be due to the memory allocated by the video adapter driver having become corrupted. Use the following edit to correct this.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

Create a new DWORD called LargePageMinimum and set it to 0xffffffff in hexadecimal. Restart Windows and hope for the best!

The problem described above is known to occur with the NVIDIA GeForce 256 and the Matrox G400 video adapters on AMD Athlon processors. It might be applicable to other cards as well.

Enable 48-bit Logical Block Addressing Support

If your ATAPI hard disk is bigger than 137 GB, Windows XP (without any service pack) will be unable to take full advantage of it due to its default 32-bit LBA support. This tweak allows you to use 48-bit LBA.

Navigate to:
HLM\System\CurrentControlSet\Services\Atapi\Parameters

The tweak involves changing the value of the DWORD called EnableBigLba to 1.

WARNING: Your system *must* meet these requirements:

❍ You must have a 48-bit LBA compatible BIOS
❍ Your hard disk must be larger than 137 GB

Performing the tweak on systems that do not meet these requirements WILL result in data losss! You have been warned!

Speed Up The COM Port

By default, all Windows 95/98/NT4/2000/ME/XP releases allow only up to 9600 bps on all serial ports: COMx = COM1—COM9 [BIOS (hardware) ports: COM1—COM4 ; Virtual (emulated) ports: COM5—COM9].

These settings enable serial (analogue) modem throughput over 9600 bps, to *possibly* speed up Internet access.

H L M \ S O F T W A R E \ M i c r o s o f t \ W i n d o w s NT\CurrentVersion\Ports

Modify the default String Value of the port. For example, COM1 is "9600,n,8,1" by default; you can modify it to "921600,n,8,1,p".

WARNING: Do this ONLY IF using dial-up (analogue) modems (e.g. 56K, ISDN) connected ONLY to a Serial Port (COMx), NOT IF using xDSL, Cable, Satellite, CNR, USB or Network (digital) modems! If using internal modems located in the Communication Networking Riser (CNR) slot, do NOT use these settings! Such cards are incompatible with these settings.

Also, please don't *expect* your Internet access speeds to improve—if they do, well and good!

Security And Network Hacks
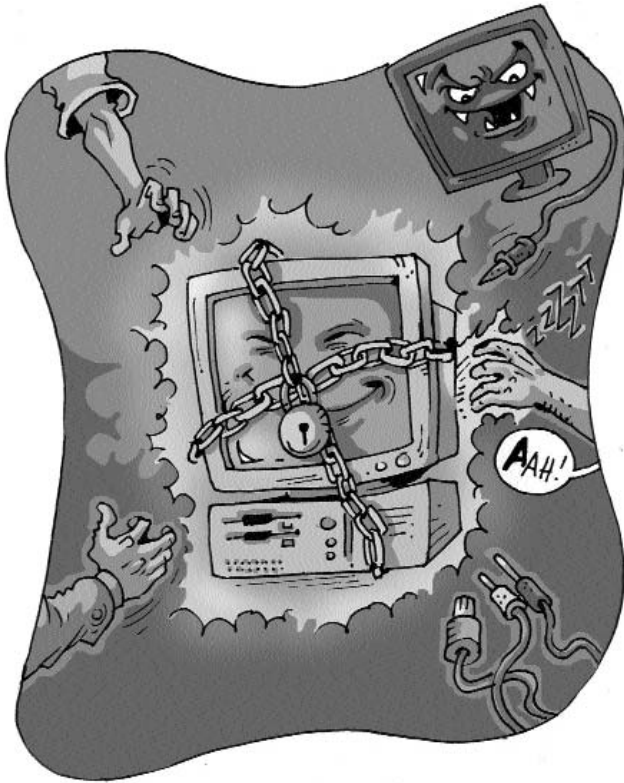
Here we cover two different topics—they've been bundled together in one chapter because there's a considerable overlap between "network" and "security." The first part relates to securing your computer against outsiders, and the second part relates to how you want your network to behave—and also how to protect it against certain kinds of attacks.

8.1 Security-Related Hacks

Secure Your Desktop Icons And Settings

Prevent your friends from playing with the desktop settings on your computer!

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Here, create a DWORD Value called NoSaveSettings. Set its value to 1. You'll need to restart Windows for the change to take effect.

A Barren My Computer

To entirely prevent access to your drives, you *could* try hiding them. This hack disables the display of local and networked drives in My Computer.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

In the right pane, create a new DWORD and name it NoDrives. Modify its value to 03ffffff (in hexadecimal). Press [F5] to refresh. Now when you click on My Computer, no drives will be shown. To re-enable the display of the drives, simply delete the DWORD you created.

No More Regedit!

This restriction removes the ability to run Microsoft Registry editing tools such as Regedit and REGEDT32. Be careful with this setting; once you enter the following key into the registry, you will not be able to use Regedit to undo the change! Be careful not to lock yourself out of the Registry: create a .reg file that will re-enable access to the registry editor. The file should have the value of DisableRegistryTools set to 1.

Navigate to:
HCU\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System

Create a new DWORD value called DisableRegistryTools and set
its value to 1 to disable the Registry editing functions.

Restart Windows for the change to take effect.

*Digit is not responsible if you take the above action and lock yourself
out of the Registry.*

Prevent Access To Certain Drives

This restriction prevents users from using My Computer or the
Windows Explorer to access the content of selected drives. Also,
they will not be able to use Run, Map Network Drive, or the "Dir"
command to view the directories on these drives.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

And to:
HLM\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

Create a new DWORD in both these locations called
NoViewOnDrive. That value uses a 32-bit bitmask to define local
and network drive access for each logical drive on the computer.
The lower 26 bits of the 32-bit word correspond to drive letters
A through Z. Drives are visible when set to 0 and hidden when
set to 1.

If you're not comfortable working in hexadecimal, add these
decimal numbers to hide the drive(s).

A: 1, B: 2, C: 4, D: 8, E: 16, F: 32, G: 64, H: 128, I: 256, J: 512, K:

1024, L: 2048, M: 4096, N: 8192, O: 16384, P: 32768, Q: 65536, R: 131072, S: 262144, T: 524288, U: 1048576, V: 2097152, W: 4194304, X: 8388608, Y: 16777216, Z: 33554432, All Drives: 67108863

For example, to hide drive A and drive C, you would add 1 (for A) + 4 (for C) to get 5, and the value of NoViewOnDrive should be set to 5. To disable all drives, set the value to 67108863.

You'll need to restart Windows for the change to take effect.

Disable Shutting Down

You can prevent users from being able to shut down the computer. This might be useful in cases such as when you're running a server and you don't want anyone to shut it down inadvertently.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer

And to:
HLM\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer

In these locations, create or modify the DWORD value called NoClose and set it to 1. Reset it to 0 to enable shutting down.

Log out and log back in, or restart Windows, for the change to take effect.

Restrict Access To Windows Update

Again, if you don't want your friends (or enemies) to make any changes to your system, you can consider, amongst other things, changing a Registry setting to restrict access to Windows Update.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer

And to:
HLM\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

In both these locations, create a new DWORD value named
NoWindowsUpdate and set it to 1.

The restriction can also be enforced by setting the
DisableWindowsUpdateAccess DWORD Value to 1 in the follow-
ing key:

HCU\Software\Microsoft\Windows\CurrentVersion\Policies\
WindowsUpdate

Refresh your Desktop or restart your Windows session for the
change to take effect.

Restrict Users Running Applications
If, for example, you run a cyber café, you can control what appli-
cations your users can run.

First navigate to:
HLM\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

Create a new DWORD value called RestrictRun set its value to
1 to enable application restrictions. Reset it to 0 to allow all appli-
cations to run.

Then navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion
\Policies\Explorer

And do the same thing as above.

After this, create a new sub-key called RestrictRun at the same
location as above (HCU\Software\Microsoft \Windows\

CurrentVersion\Policies\Explorer). Here, define the applications that are allowed, by creating a new String Value for each application, named as consecutive numbers, and setting the value to the filename to be allowed, for example, "regedit.exe", with the quotes.

For example, create a new String Value within RestrictRun called 1, and set it to "regedit.exe" with the quotes. Then, another String Value called 2, and set it to "iexplore.exe". And so on.

Restart Windows for the changes to take effect.

If it's you who applies Group Policy (the Administrator), you should not apply this restriction to yourself. If applied, this can prevent even administrators from running Group Policy or the registry editors. So once applied, there is no way to change undo this except by reinstalling Windows. This means that you should log in as the user you want to apply the restrictions to, then make the changes in HKEY_CURRENT_USER.

Digit is not responsible if you lock yourself out of any programs by taking the action above.

Disable Account Changes in Outlook Express
This setting disables the ability for users to create or modify any mail, news or directory accounts in Outlook Express.

Navigate to:
HLM\SOFTWARE\Microsoft\Outlook Express

Create a new DWORD value called "No Modify Accts". Set it to 1 to enable the restriction, or to 0 (the default) to allow users to modify accounts. Restart Outlook Express for the change to take effect.

Change Alternative Installation Credential Settings
If you want users to be prompted for alternate logon credentials—username, password and domain—when installing software as

non-administrative users, you need to apply this Registry edit.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

And to:
HLM\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

Create two new DWORD values in these locations. The first is NoRunasInstallPrompt, and should be set to 1 to disable the alternate credentials option—and to 0, which is the default, to request alternate credentials. The second is PromptRunasInstallNetPath. Here, setting it to 1 will make Windows request alternate credentials when installing from a network share, and 0, which is the default, will disable the alternate credentials option.

Restart Windows for the change to take effect.

Restrict Changes To Folder Locations

Use the following hack if you don't want users changing the location of user-specific folders such as My Documents, My Music, My Pictures and the Favorites.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

And to:
HLM\Software\Microsoft\Windows\CurrentVersion
\Policies\Explorer

In each of these, create new DWORD values from the following list and set them to 1 to restrict the changes or to 0 to allow them.

DisablePersonalDirChange: Restrict changes to My Documents
DisableMyPicturesDirChange: Restrict changes to My Pictures
DisableMyMusicDirChange: Restrict changes to My Music
DisableFavoritesDirChange: Restrict changes to the Favorites

Log off and back on, or restart Windows, for the change to take effect.

Disable Run Commands Specified in the Registry

This restriction is used to disable the ability to run startup programs specified in the registry when Windows launches.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

And to:
HLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Create new DWORD Values in these locations for each of the optional values below, depending on which Run function to stop, and set their values to 1 to disable the startup. For a description of what Run and RunOnce mean in the Windows XP Registry, visit http://support.microsoft.com/kb/314866/EN-US/

DisableLocalMachineRun
DisableLocalMachineRunOnce
DisableCurrentUserRun
DisableCurrentUserRunOnce

You'll need to restart Windows for the changes to take effect.

Miscellaneous Security-Related Hacks

Under the following key:
HCU\Software\Microsoft\CurrentVersion\Policies

There will be a key called Explorer. Under that key, create new DWORD Values and modify their values to 1 to impose the following restrictions. If and when you want to remove these restrictions, simply delete the respective DWORD Values, or change their values to 0. Here's a list of DWORD Values that can be created under the Explorer key.

NoDeletePrinter: Disables deletion of already installed printers
NoAddPrinter: Disables addition of new printers
NoRun: Disables or hides the Run Command
NoSetFolders: Removes folders from the Settings option in the Start Menu (Control Panel, Printers, Taskbar)
NoRecentDocsHistory: Removes the Recent Document system folder from the Start Menu
ClearRecentDocsOnExit: Clears the Recent Documents system folder on Exit

Under the same key, you can create new sub-keys other than the Explorer key. Create a new sub-key and name it System. Under this key, you can create the following new DWORD values, setting them to 1 for enabling the option and to 0 for disabling it.

NoDispCPL: Hides Control Panel
NoDispBackgroundPage: Hides the Background page
NoDispScrsavPage: Hides the Screen Saver page
NoDispAppearancePage: Hides the Appearance page
NoDispSettingsPage: Hides the Display Settings page
NoPwdPage: Hides Password Change Page
NoAdminPage: Hides the Remote Administration page
NoProfilePage: Hides the User Profiles page
NoDevMgrPage: Hides the Device Manager page
NoConfigPage: Hides the Hardware Profiles page
NoFileSysPage: Hides the File System button
NoVirtMemPage: Hides the Virtual Memory button

If you create a new sub-key named WinOldApp, you can add the following DWORD values under it, and set them to 1 for enabling the option and to 0 for disabling it.

Disabled: Disable the MS-DOS Prompt
NoRealMode: Disable Single-Mode MS-DOS

8.2 Network-Related Hacks

Stop Automatically Detecting Network Connection Speed
Windows will normally attempt to detect the time-out on network links to determine their speed (high or low). This functionality can be disabled if Windows is having problems determining the speed of your link.

Navigate to:
HLM\SOFTWARE\Microsoft\Windows   NT\CurrentVersion \Winlogon

Create   or   modify   the   DWORD   value   called SlowLinkDetectEnabled and set it to 0 to disable the functionality or to 1 to enable it.

Log out and back in, or restart Windows, for the change to take effect.

Define The Slow Link Time-Out
Windows uses the "Slow Link Time-Out" value to define what should be classified as low-speed and what a high-speed connection is. The default time-out is 2000 milliseconds; any connection slower is considered a low-speed link.

To elaborate, if the server storing a user's profile does not respond before the time specified in the value of this entry, then the link to the server is considered to be slow, and it offers the user

the option of using a profile stored on the local computer instead of waiting for the server.

You can increase the value of SlowLinkTimeOut (as below) to favour the server-based profile. This is particularly useful for clients using addresses assigned by DHCP, or for computers accessing server-based profiles over slow WAN connections, such as dial-up connections.

Navigate to:
H L M \ S O F T W A R E \ M i c r o s o f t \ W i n d o w s NT\CurrentVersion\Winlogon

Create or modify the DWORD Value called SlowLinkTimeOut and set it to the value in milliseconds.

You might need to restart or log out and back in for the change to take effect.

Specify The Users To Receive Administrative Alerts
This setting is used to specify a list of users and/or computers that should receive administrative alerts.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\Alerter\Parameters

Here, modify the REG_MULTI_SZ Value called AlertNames, and enter, as its value, the users or computers to receive the alerts. For example, you could set its value to "rajeshk rajeshm johna". Restart Windows for the change to take effect.

Manage QoS Packet Queuing
This setting specifies the maximum number of outstanding packets permitted on the system. When the number of outstanding packets reaches this limit, the Packet Scheduler postpones all submissions to network adapters until the number falls below this limit.

Navigate to:
HLM\SOFTWARE\Policies\Microsoft\Windows\Psched

Create or modify the DWORD Value called
MaxOutstandingSends and set it to the maximum number of
packets. The default is 65535.

Either log out and back in, or restart Windows, for the change
to take effect.

Manage Reserved QoS Bandwidth

This setting determines the percentage of connection bandwidth
that the system can reserve for QoS traffic. By default, the Packet
Scheduler limits the system to 20 per cent of the bandwidth of a
connection.

Navigate to:
HLM\SOFTWARE\Policies\Microsoft\Windows\Psched

Create a new DWORD value called NonBestEffortLimit and set
it to the percentage (in decimal) of the bandwidth to reserve for
QoS packets. (The default is 20.) Restart Windows.

This can be changed on an adapter-by-adapter basis by creating
the same value in the following key:

HLM\SYSTEM\CurrentControlSet\Services\Psched\Parameters\A
dapters\{Adapter-ID}

Manage The Network Bridge Feature

The feature in XP called Network Bridge lets you connect disparate
media types—10/100, Gigabit, etc.—into one seamless network. This
tweak allows you to control forwarding and settings associated
with this feature.
Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\BridgeMP

Create or modify the DWORD values from the following, and set them to 1 to disable the feature, or 0 (which is the default) to enable it.

DisableForwarding: Disables forwarding
DisableSTA: Disables the spanning tree algorithm

Restart Windows for the change to take effect.

Display Network Error Statistics

This tweak allows you display error statistics on the Network Connection Status page for LAN and WAN connections. This information could be useful in diagnosing the network reliability.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Control\Network\Connecti ons\StatMon

Create or modify the DWORD Value called ShowLanErrors and set it to 1 to enable the error count. 0 is the default.

Restart Windows for the change to take effect.

Increase Network Performance And Throughput

If you increase the number of buffers the network redirector reserves for network performance, it could increase your network throughput. Each extra execution thread you configure will take 1K of additional non-paged free memory, but only if your applications actually use them. Increasing this value will improve network throughput especially if you are running applications that perform more than 15 operations simultaneously.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstati on\Parameters

Create or modify DWORD values as follows:

MaxCmds: The range is 0 to 255 (some sources say the default is 15, some say it is 50)

MaxThreads: Set it to the same value as MaxCmds

You may also want to increase the value of MaxCollectionCount. This value represents the buffer for character-mode named pipes writes. The default is 16, and the range is 0 to 65535.

Specify The Schedule For The Alerter Service

This setting is used to specify how often the server checks alert conditions and sends any required alert messages to administrative users.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Create or modify the DWORD value called "AlertSched, ErrorThreshold, NetworkErrorThreshold" (without the quotes) and set it to a value in minutes between 1 and 65535. Restart Windows, or log out and back in, for the change to take effect.

By default, alert messages are sent every five minutes, unless 10 alerts are pending or 5 per cent of all network operations generate an error.

Specify The Server Announcement Frequency

This Registry edit specifies how often a non-hidden server announces itself to the network. More frequent announcements keep client server tables more up to date, but may increase network overhead and processing on client computers, because the clients must process every announcement.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Create or modify the DWORD Value called Announce and set it to a value in seconds between 1 and 65535. The default is 240.

You may need to restart or log out and back in for the change to take effect.

Include A Comment In The Server Announcement
This setting allows you to specify a comment that will be sent in server announcements and returned to NetServerGetInfo requests. (The NetServerGetInfo function retrieves current configuration information for the specified server.)

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Par ameters

Create or modify the String value called Comment and set it to the text string you want as the comment. You may need to restart or log out and back in for the change to take effect.

Browse Lists For Multiple Domains
By default, the Computer Browser service only maintains a list of servers on the local network. To allow clients to browse computers on other domains you may need to add the other domains names using this tweak.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\LanmanWorkstati on\Parameters

Modify or create a new REG_MULTI_SZ value called OtherDomains and edit it to add the names of the domains you want to browse, one after the other, with spaces between them.

Restart Windows for the change to take effect.

Optimise The Windows Server Service

This setting can be used to manually optimise for file server functionality. By selecting the appropriate value, you can optimise the service for memory usage, network throughput, or a balance of both.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

Create or modify the DWORD value called Size and set it according to the below values:

1: Minimise memory
2: Balance
3: Maximise network throughput

You may need to restart or log out and back in for the change to take effect.

Control Automatic DNS Server Cache Updates

This value disables that automatic cache updated from the DNS root servers. This can be useful when there is a problem with the root servers, or if you want to completely control DNS updates.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters

Create or modify the DWORD value called AutoCacheUpdate and set it to 0 to disable automatic updates. Restart Windows for the change to take effect.

Change LAN Auto-Disconnect Timeout

Windows can be configured to automatically disconnect idle LAN sessions are a set number of minutes.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Par
ameters

Modify or create the String Value called Autodisconnect and set it to equal the time in minutes before a session is disconnected. This can be between 0 and 4294967295 (0xffffffff in hexadecimal). Restart Windows for the change to take effect.

Set the value to 0xffffffff to disable the disconnection function.

Specify The Idle Timeout For Server Connections
You can specify the amount of idle time that a circuit is allowed before being disconnected. If this parameter is set to a low value, it saves server resources, but reduces performance because of the client overhead in reconnecting.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Par
ameters

Create or modify the DWORD value called Disc. Set it to the value in minutes—from 0 to as high as you want. The default is 15.

You may need to restart or log out and back in for the change to take effect.

Specify The Server Announcement Variation
You can specify the time by which the server announcement period can vary. This helps to prevent several servers from continuously announcing simultaneously, thereby reducing network load peaks.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Par
ameters

Create or modify the DWORD value called AnnDelta and set it to a value in milliseconds between 0 and 65535. The default is 3000. Log out and back in, or restart Windows, for the change to take effect.

Search For Network Folders And Printers
There is a setting that controls whether Windows should automatically attempt to locate available file shares and printers over the local network.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

Create or modify the DWORD value called NoNetCrawling. Set it to 1 to disable the searching, or to 0 to enable it.

You may need to restart or log out and back in for the change to take effect.

Change The Number Of Simultaneous HTTP Sessions
Windows normally limits the number of simultaneous connections made to a single Web server. This behaviour can be seen in IE when downloading multiple files from a site: only a certain number will be active at any one time. Windows limits connections to a single HTTP 1.0 server to four simultaneous connections. Connections to a single HTTP 1.1 server will be limited to two simultaneous connections.

The HTTP 1.1 specification mandates the two-connection limit, while the four-connection limit for HTTP 1.0 is a self-imposed restriction that coincides with the standard used by some popular Web browsers. To change this behaviour...

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Create two new DWORD values, or modify the existing values, called MaxConnectionsPerServer and MaxConnectionsPer1_0Server. Change the values to equal the number of simultaneous requests allowed to a single HTTP server. The default values are 2 and 4 respectively. Restart Windows for the change to take effect.

By changing these settings you are causing Windows to break the HTTP protocol specification for any Internet applications running on your machine. Also, this affects all Windows Internet applications that use the standard API, including Internet Explorer.

Protect Against SYN Flood Attacks

Windows includes protection that allows it to detect and adjust when the system is being targeted with a SYN flood attack—a type of denial of service attack. When enabled, the connection responses time out more quickly in the event of an attack. (This value causes TCP to adjust retransmission of SYN-ACKS.)

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Create a new DWORD value called SynAttackProtect and set it to either 0, 1 or 2, based on the following.

0 (the default): Typical protection against SYN attacks
1: Better protection against SYN attacks that uses the advanced values mentioned below.
2 (the recommended value): Best protection against SYN attacks. This value adds additional delays to connection indications, and TCP connection requests quickly timeout when a SYN attack is in progress.

For extra control, you can create these additional DWORD values in the same key for each of the items below. They are not required for SynAttackProtect to be effective.

TcpMaxHalfOpen: The default value is 100.
TcpMaxHalfOpenRetried: The default value is 80.
TcpMaxPortsExhausted: The default value is 5.
TcpMaxConnectResponseRetransmissions: The default is 3.

When SynAttackProtect is using the best protection option, then Scalable windows and TCP parameters that are configured on each adapter (including Initial RTT and window size) are no longer available.

Harden The TCP/IP Stack
These following settings can be used to increase the ability of Windows to defend against Denial of Service attacks when connected directly to the Internet.

Navigate to:
HLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Create the following DWORD values and set them as indicated.

EnableDeadGWDetect
Set this to 0. The default is 1.
This disables dead-gateway detection as an attack could force the server to switch gateways.

EnableICMPRedirect
Set this to 0. The default is 1.
This stops Windows from altering its route table in response to ICMP redirect messages. Some documentation has this listed as EnableICMPRedirects, but according to Microsoft it should be EnableICMPRedirect (with no "s".)

EnablePMTUDiscovery
Set this to 0. The default is 1.
This disables maximum transmission unit (MTU) discovery as an attacker could force the MTU value to a very small value and overwork the stack.

KeepAliveTime

Set this to 300000. The default is 7200000 (2 hours).

This reduces how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet.

NoNameReleaseOnDemand

Set this to 1. The default is 0.

This protects the computer against malicious NetBIOS name-release attacks.

PerformRouterDiscovery

Set this to 0. The default is 1.

This disables ICMP Router Discovery Protocol (IRDP) where an attacker remotely adds default route entries on a remote system.

SynAttackProtect

Set this to 2. The default is 0.

This automatically adds additional delays to connection indications, and TCP connection requests quickly timeout when a SYN attack is in progress.

Restart Windows for the changes to take effect.

These values will not give the best performance due to additional checking and less optimisation, but they will provide greater protection against attacks.

Disable Password Caching

When a user first logs on to the computer, the password is cached by Windows. There is a security risk with the password being stored on the computer. This hack disables the password cache on the local computer.

Navigate to:

HCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network

And to:

HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policie s\Network

Here, setting the DWORD value DisablePwdCaching to 0 will disable the cache. The change will be effective the next time you log on.

Disabling the cache also prevents the network password from going out of sync with the server.

Remove The "Properties" Option From My Computer
Use this hack to hide the System Properties screen and remove the Properties option from My Computer. Useful if you don't want anyone messing around with, well, Your Computer!

Navigate to:

HCU\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer

And to:

HLM\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer

Set the DWORD Value NoPropertiesMyComputer to 1 to hide the Properties option. Reset it to 0 to re-enable what you disabled.

Restart or log off and back on for the change to take effect.

Disable The Folder Options Menu
Again, if you're leaving your computer alone for a while and you don't want to see things changed when you return, one of the things you can do is to disable the Folder Options.

Navigate to:

HCU\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer

And to:

HLM\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

Here, create or modify the DWORD Value called
NoFolderOptions, and set it to 1 to hide the Folder Options. Reset
it to 0 to enable the options. A restart might be required to see the
changes.

Disable Right-Click On The Start Button

As part of securing the desktop, disable the ability to right-click on
the Start button and select the command options Open, Explore,
and Find.

Navigate to:
HCR\Directory\shell

And to:
HCR\Folder\shell

For both these keys, rename "shell" to "shell.old". Exit the
Registry Editor and right-click on the Start button: the options
will not be available. To re-enable them, simply remove the ".old"
suffix.

Disable Web Content And More

This hack will disable Web content and Web tasks in Explorer, and
will remove the Desktop item from the Display properties!

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

And to:
HLM\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

In both these keys, change the value of the DWORD ClassicShell to 1 to enable the Classic Desktop, which does not support Web content. To revert to the default, change it to 0.

This hack disables all the desktop features in newer releases of Windows including Active Desktop, Web View, Thumbnail View and the Quick Launch toolbar.

Disable Right-Clicking On The Desktop Altogether
The following hack will disable the context menu from appearing when clicking anywhere on the Desktop, or in the right pane of an Explorer window.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer

And to:
HLM\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer

Set the DWORD Value NoViewContextMenu to 1 to disable the right-click context menu, or to 0 to enable it.

Clear Cached Commands In "Run"
Use this hack to clear the cache of the MRU (Most Recently Used) list of command line entries in the Run dialog box.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explorer \RunMRU

Delete the values you want to remove from the list, or the entire RUNMRU key to delete the list altogether.

Limit Users From Changing User Folder Locations
The following will prevent unruly people from changing the fold-

er locations of My Documents, My Pictures, My Music, and the Favorites.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer

And to:
HLM\Software\Microsoft\Windows\CurrentVersion\Policies\ Explorer

Change the following DWORD Values to 1—or if they're not there, create them and set them to 1—to limit changes to these directories. The settings for each folder are as follows.

DisablePersonalDirChange: Limit changes to My Documents
DisableMyPicturesDirChange: Limit changes to My Pictures
DisableMyMusicDirChange: Limit changes to My Music
DisableFavoritesDirChange: Limit changes to the Favorites

The defaults for all these are 0. Reboot for the changes to take effect.

Clean Out The NetMeeting Call History
Another hack for the paranoid.

Navigate to:
HCU\Software\Microsoft\Conferencing\UI\CallMRU

Delete CallMRU altogether. Restart NetMeeting for the change to take effect.

Hide The Last Username
By default, XP displays the last successfully logged in username in the login dialog box. To prevent people with access to the computer from knowing who logged in last, use this hack.

Navigate to:
HLM\Software\Microsoft\Windows\CurrentVersion\Policies\
System

Change the DWORD Value called DontDisplayLastUserName to
0 to disable the feature.

Disable "Log On Using Dialup"
Use this hack to stop users from connecting to a domain via dial-up.

Navigate to:
H L M \ S O F T W A R E \ M i c r o s o f t \ W i n d o w s
NT\CurrentVersion\Winlogon

Set the String Value RasDisable to 1 to disable the checkbox. 0
will re-enable it.

Set A Minimum Password Length
It's a very useful security measure to force users to use a certain
minimum password length, and prevent blank passwords.

Navigate to:
HCU\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\Network

And to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\Network

The first is for the user currently logged in, and the second is
the system-wide setting.

Set the value for MinPwdLen to the minimum number of char-
acters that the user must use for his password. Obviously, zero-
length passwords will be disallowed if you enter any value greater
than zero. *This does not apply to existing passwords—only to new or
changed ones.*

Hide "All Programs"

Use this hack to hide the All Programs button, which displays a list of all installed applications.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

And to:
HLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Change the DWORD value of the setting NoStartMenuMorePrograms to 1 to hide the button. Default is 0.

This, obviously, applies only to the XP Start Menu and not the Classic Start Menu.

Irritants
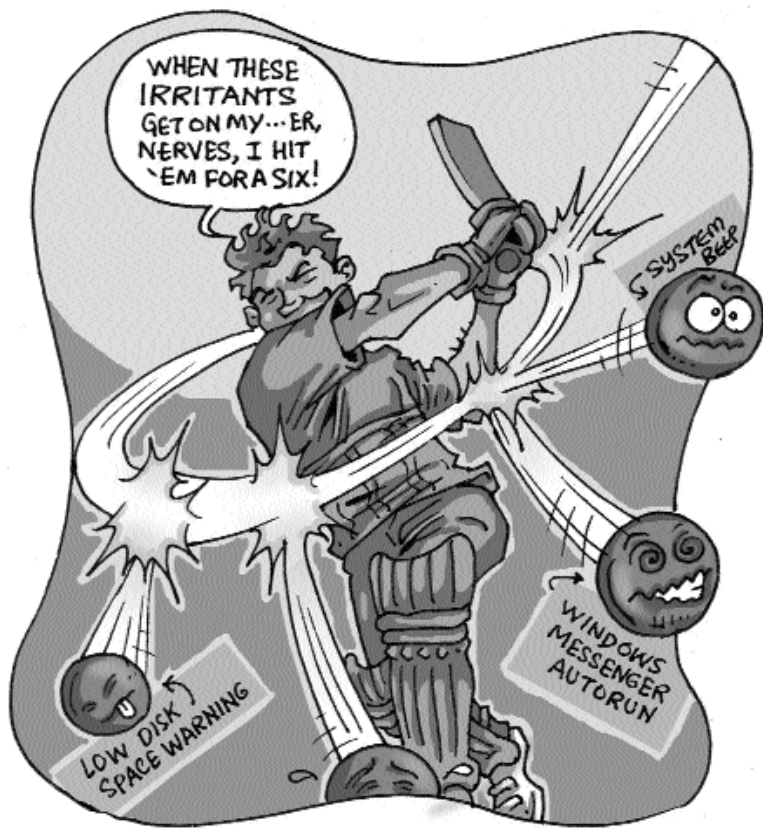
These are probably the Registry edits you'd want to make first thing after installing Windows! Who needs pop-ups telling you that new programs have been installed? And how do you feel when an application spawns and steals focus even as you're typing?

Yes, Windows has more than its fair share of irritants, and here's how to get rid of some of them.

Begone, Pop-Ups!

Don't you just hate it when Windows brings up a pop-up that serves no function whatsoever? Like something telling you you've installed a new program and so on; there's an easy way to get rid of such notifications.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

Here add a DWORD value called EnableBalloonTips. Set it to 0 to, of course, disable all balloon tips, and later to 1 if you get the feeling that those balloons were lovable little things you now can't live without.

This particular change to the Registry will only disable *most* balloon tips. A little more work is required to eliminate them all. Look for the following DWORD Values and change them to 0 to disable the balloon tips they refer to:

HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\FolderContentsInfoTip

HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip

HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\tips\Show

To Send Or Not To Send...

If you're overly devoted to Microsoft, or if you're plain eager to please, you might click "Send" when some program crashes and Windows asks you if you want to report the error. Most of us, though, don't have this attitude, and click "Don't Send" How often have you had to do that?

Navigate to:
HLM\SOFTWARE\Microsoft\PCHealth\ErrorReporting

Here, edit the DoReport value. Set it to 0 to disable the error reporting dialog—once and for all.

Zip Around
If you're fast at your mouse and just can't stand waiting for a few milliseconds for a menu to pop up, use the following hack.

Navigate to:
HCU\Control Panel\Desktop

Simply change the value of MenuShowDelay to 0. Increase the value if you think that's too fast for you!

The change should be effective immediately.

Clearing The Clutter #1
The "Documents" on the Start Menu, like the Favorites, never picked up in terms of usage. No-one seems to use it, even though it can indeed be pretty useful, and it's a sort of infringement on your privacy when someone else sits at your computer and opens up the Documents! Take it off for good.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

Set the DWORD NoRecentDocsMenu to 1. If you feel the need for the Documents item, you can bring it back by resetting it to 0.

Clearing The Clutter #2
Why do Start > Search > Files or Folders when you can just press [**Windows**] + [**F**]? Yes, that's the keyboard shortcut. And do you ever use the "Search" to find "people"? Or for "Internet Audio and Radio" or whatever is added by apps to the menu? Remove it for

good, and start using [**Windows**] + [**F**] when you need to do a file search!

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Set the DWORD NoFind (create it if it doesn't exist) to 1 to remove the "Search" item. A cleaner Start Menu!

Note: The above two hacks are best applied only if you're using the Classic Start Menu in Windows XP. You don't need the registry to clear these two items if you're using the XP Start Menu.

Killing 'Em Softly

XP is a lot more stable than 98, of course, but there's still a lot of scope for programs crashing. And then you need to bring up the task manager, arrange the processes by name, then end-task the non-responsive program. Automate this! Have non-responding programs shut down all by themselves...

Navigate to:
HCU\Control Panel\Desktop

Modify the String Value AutoEndTasks to 1.

This hack not only takes away the burden of ending tasks yourself, it can also help in cases where you can't delete a file because some process is using it—in *most* cases, this is a non-responding program. Windows will silently kill it.

Note that we said "most" cases; in some cases, you might wind up killing an application that is only temporarily unresponsive, as happens often when applications are performing particularly intensive calculations. To prevent this, you can instead set a lower threshold at which the system prompts you to manually end a hung task. The default is 5000 (milliseconds), meaning Windows

waits five seconds for an application to respond before deciding that it's hung and asking you to manually end it.

Navigate to the same key:
HCU\Control Panel\Desktop

Change the HungAppTimeout String Value from the default 5000 to, say, 2000, or even 1000. Be careful, though. If you have a program that runs slowly, XP, with this new value, could wrongly determine that a task has hung. If that seems to happen, increase the HungAppTimeout value in increments until false alarms stop.

The Most-Hated Balloon Of Them All

Why the incessant balloon warnings when you run low on disk space? It's not like these balloons help anyway—they offer to clear a few KB, and if you're lucky a couple of MB—of space by deleting temp files, clearing the Recycle Bin and such, depending on your settings. (As if you couldn't think of deleting files yourself!) Here's the warning we're talking about:

"You are running out of disk space on [drive]. To free space on this drive by deleting old or unnecessary files, click here."

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

Create or modify the DWORD called NoLowDiskSpaceChecks. Make it 1 to disable the alerts, and if you miss them, make the value 0 to have them return in all their glory.

Die!

This doesn't happen often, but when it does, it can be a major irritant—especially if you like your Windows all nice and neat. Some programs don't vanish from the Add/Remove Programs list even after you delete them. You can manually remove these from the list.

Navigate to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Unin
stall

Look for the program name there, and delete the key.

If you can't find the program, look in one of the sub-keys whose names start with a curly brace. Then look for the program name in the DisplayName sub-key within that key. Delete the entire key (the one whose name begins with a curly brace).

Use this hack with care—you don't want to mess with Windows by deleting a wrong key.

Silence Those Beeps

System beeps can be useful. And they can be quite irritating.

Navigate to:
HCU\Control Panel\Sound

You'll find the String Value called Beep on the right. Modify it to "no" to disable beeps, or to "yes" to enable them. A restart is required for the change to take effect.

Do Away With The List

OK. How often have you come across a file with a non-standard extension, wanted to view its contents, and then selected Notepad from the list of available programs? Here's how to associate all unknown-extension files with Notepad, so they open with that program by default.

Navigate to:
HCR\Unknown\shell

Create a new key called "notepad" (without the quotes). Right-click this key and create a sub-key called "command". Now set the "(Default)" String Values of the following as below, without quotes:

HCR\Unknown\shell:
"notepad"

HCR\Unknown\shell\notepad:
"Open Using The Wonderful Notepad Application" (or whatever you want!)

HCR\Unknown\shell\notepad\command:
"C:\WINDOWS\NOTEPAD.EXE %1"

Now, not only will double-clicking a file with an unknown extension cause it to be opened in Notepad, you'll also get "Open Using The Wonderful Notepad Application" in the context menu when you right-click the file. When you choose that option, the file, well, opens in Notepad!

Don't Hog The Limelight
It's irritating when an application steals focus. You're typing, and all of a sudden you find you're not... because there's some other window that's blinking blue on the taskbar, begging to be noticed. Here's how to prevent windows from stealing focus.

Navigate to:
HCU\Control Panel\Desktop

Create or modify the DWORD called ForegroundLockTimeout. Give it a value of... no, not 1 or 0; the value to give this DWORD is 00030D40. This is in hexadecimal, so when you get the "modify" box, make sure "Hexadecimal" is selected.

I'll Read My Mail, Thank You
In XP, you get a message at the logon screen that tells you how many unread mail messages you have. This isn't very useful: if you do care how many unread mails you have, you'll probably be getting to your Inbox soon enough! It can be a mild irritant if you log off and back on frequently, and you see that same number there. Anyway, here's how you can get rid of the intimation altogether.

Navigate to:
HLM\Software\Microsoft\Windows\CurrentVersion\
UnreadMail

Here, modify the DWORD called MessageExpiryDays. Give it a value of 0. You can see what the key means, so set it to whatever you want, just for the inane fun of it—but 0 will, of course, disable it. You'll see the change the next time you log on.

IE: A Bad Choice For Bitmaps
You right-click a bitmap image intending to open it with Photoshop, and you see a whole bunch of programs offered to you to open the file with. Not only is it plain irritating to see Internet Explorer in the list, it also takes more time for the list to come up when there are a lot of programs. So say you want to remove "Internet Explorer" from the list of "open with" programs when you right-click a .bmp file.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explorer
\FileExts

You'll see a whole bunch of file extensions. Find the extension you want—in this case, .bmp. Expand it further. You should see a key called OpenWithList. Inside that key lie all (well, most of) the programs that will come up in the "open with" list. Note down their order, which is displayed in the "MRUList" key. Delete the program names you don't need, including, in our case, Internet Explorer.

Do a good job of cleaning up by renaming the remaining keys in order of a,b,c, etc., and then rename the MRUList.

Like we said, this is for most, but not all, the programs. Some happen to be stubborn.

Navigate to:
HCR\.xxx\OpenWithList

Replace ".xxx" with the file extension in three-letter format that you want to delete. So in our case, go to HCR\.bmp\OpenWithList. Delete the Internet Explorer *key* entirely.

Usually, the first action as above does not require a restart, and the second does.

In addition, our consciences would hate us if we didn't tell you this: there exist a *few* programs for which neither of the above will work, but to remove those involves a dangerous Registry hack, which we won't get into here.

Windows Forgetting Your Settings?

This may seem a bug at first, but it turns out it's not a bug—it's more of an irritant, which is much less likely in XP SP2. Windows sometimes forgets your folder customisations: their positions and display options, and in addition, if you've customised them by setting a picture as a background for them, and such. This happens because XP remembers the settings for only 400 folders by default, and when you customise more folders, the 400 mark is reached, and the old settings are lost.

XP happens to allow a maximum of 8000 instead of that 400. Here's how to set it to any value up to 8000.

Navigate to:
HCU\Software\Microsoft\Windows\Shell

And to:
HCU\Software\Microsoft\Windows\ShellNoRoam

In both these keys, find the value called BagMRU. Increase it to whatever you want, all the way to 8000. (This is in decimal; make sure "decimal" is chosen when you're making the change. God

knows what'll happen if you set it to 8000 in hexadecimal.)

SP2 increases the oddly-named Bag value to 5000, but if you have a terabyte of data, you might just want to increase the size of the Bag to 8000.

When Startups Fail

It can be a major irritant if you place items in the Startup folder so they'll be run at startup, and they don't. There are two things you need to do in the Registry to rectify this.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Explorer \User Shell Folders

On the right, you'll see a REG_EXPAND_SZ Value called Startup. Set the data there to

"%USERPROFILE%\Start Menu\Programs\Startup" (without the quotes).

Then, navigate to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explor er\User Shell Folders

Here, set the Startup value on the right to
"%ALLUSERSPROFILE%\Start Menu\Programs\Startup" (without the quotes).

That should fix the problem.

Beyond Tiled And Centred

Ever set a wallpaper centred, depicting a face, to find the chin chopped off by your taskbar? Ever wished you had options other than Tiled and Centered for your wallpaper? Or perhaps you want to set a strip at the bottom of your Desktop as the wallpaper? Well, you can set a wallpaper at whatever position you want. Here's how.

Navigate to:
HCU\Control Panel\Desktop

Here, there are two String Values that probably won't be there, and you'll have to create them. They have helpful names: WallpaperOriginX and WallpaperOriginY. They are the horizontal and vertical offsets—in pixels—for the wallpaper, measured from the left and from the top respectively.

You don't need a restart—just change your wallpaper from the Control Panel after closing the Registry Editor. If you choose Centered, you'll get what you need. If you choose Tiled, you'll get the image at the desired position, with the image also tiled in the remaining space. And if you choose Stretch, it looks something like Centered, with the position being maintained but the size being different.

It's My Business
It happens on some computers, and not on some others. We're talking about a minor irritant here, something that infringes on your privacy—if you're a really private person, that is.

When you do a [Windows] + [L], the number of programs you have open is displayed: something like "10 programs running." As for you, you either know it or don't care; as for everyone around you, why should they know? Anyway, if you do want to disable that line from appearing, here's how to do it.

Navigate to:
HCU\SessionInformation

Look for ProgramCount in the right pane and set it to 0. Then there's something a little advanced: right-click SessionInformation. You'll get a menu; select Permissions. In the box that comes up, click the Advanced button, then click Add. Type in your Windows username in the box at the bottom. As soon as you do that, you'll get a new box with Allow and Deny columns. Select Deny for the Set

Value row. Click OK several times to finish up.

Despite our disclaimer, we need to stress again that you use the above procedure at your own risk. If you do the above, Windows can't update the ProgramCount, and any programs that depend on that value might fail!

Remove My Network Places

My Network Places is one of the items in the Windows Explorer that you might want to remove if you're on a home computer not connected to a network. Sometimes, an attempt to delete it followed by the opening of a fresh Explorer window will cause it to re-spawn. Here's how to get rid of it for good.

Navigate to:
H C R \ C L S I D \ { 2 0 8 D 2 C 6 0 - 3 A E A - 1 0 6 9 - A 2 D 7 - 08002B30309D}\ShellFolder

We urge you to back up this key; export it to a .reg file. Then, create a new DWORD value called Attributes. Assign it a value of 20180000 (in hexadecimal).

The change will be effective immediately. Make a note of the change you made—if ever you get on a network, you might want to delete that Attributes value and get My Network Places back.

A Vanishing Act

This sometimes happens to unlucky folks: when you log off or restart, the Run menu gets cleared all on its own, and you need to retype your program names. This *could* be due to a certain Registry value: be aware that the following edit may or may not solve the problem.

One thing we must mention here is that if you have TweakUI installed, you might want to check if you've ticked "Clear document history on exit" under Explorer. If you haven't, try the following.

Navigate to:
HCU\Software\Microsoft\Windows\CurrentVersion\Policies\
Explorer

Find the ClearRecentDocsOnExit value, and set it to 0 if you find it's at 1.

I'll Do It Myself

On some machines with XP—we don't know why not on all installations—Windows Media Player keeps prompting you to update it. Well, when there's a newer version available, you'll probably hear about it—and you *will* update it at your leisure! Here's how to disable the prompts.

Navigate to:
HLM\SOFTWARE\Microsoft\MediaPlayer\PlayerUpgrade

Create or modify the String Value called AskMeAgain, and set it to No to disable the prompts. If you're cut off from civilisation and want WMP to prompt you again, set it to Yes.

Another Irritating Pop-Up

When Windows is unable to contact a domain controller during a user's login, a pop-up error message could be displayed. If this is happening too often to you, the message can be controlled by modifying the following setting.

The message in question is:

"A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes made to your profile since you last logged on may not be available."

There are two things you need to do here. For the Per-User Parameter, navigate to:

H C U \ S o f t w a r e \ M i c r o s o f t \ W i n d o w s NT\CurrentVersion\Winlogon

Create or modify the DWORD value called ReportDC and set it to 0 to suppress the message.

For the System-Wide Parameter, navigate to:
H L M \ S O F T W A R E \ M i c r o s o f t \ W i n d o w s NT\CurrentVersion\Winlogon

(On Windows 2000 and above, this message is suppressed by default. To modify this, in the above key, create a new String Value called ReportControllerMissing. Set it to TRUE to report the errors, or to "FALSE" to suppress the errors.

Restart Windows for the change to take effect.

Clean Up The Add/Remove Programs list

Sometimes, when you uninstall a program from the Add/Remove programs list, the application gets uninstalled, but the entry for it in the Add/Remove Programs list remains. This can be an irritant depending on how particular you are about keeping your computer nead and tidy. Use this hack to remove extinct programs from the list.

Navigate to:
HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Uninstall

Find the Application sub-key under this key. There should be at least two entries for each application: "DisplayName", which shows the name that is displayed in the Add/Remove Programs list, and "UninstallString", which is the path to the uninstall program file. To remove the stubborn program from the list, select the Application sub-key and simply press [Delete].

Fix The Disk Cleanup Tool

When you try to compress old files, the Disk Cleanup tool may stop responding, and you could receive a message like the following:

"Disk Cleanup is calculating how much space you will be able to free on (C:).
This may take a few minutes to complete.
Scanning: Compress old files"

This happens when there's an incorrect entry in the registry that is used by the Disk Cleanup utility to locate compressed files.

Navigate to:

HLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\VolumeCaches

Delete the "Compress old files" registry key and you're done.

Notes

....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....

....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....
....