The Windows Registry

What Is The Registry?

The Registry is a database used to store settings and options for the 32 bit versions of Microsoft Windows including Windows 95, 98, ME, NT/2000 and XP. It contains information and settings for all the hardware, software, users, and preferences of the PC. Whenever a user makes changes to a Control Panel settings, or File Associations, System Policies, or installed software, the changes are reflected and stored in the Registry.

The physical files that make up the registry are stored differently depending on your version of Windows; under Windows 95 & 98 it is contained in two hidden files in your Windows directory, called USER.DAT and SYSTEM.DAT, for Windows Me there is an additional CLASSES.DAT file, while under Windows NT/2000/XP the files are contained separately in the %SystemRoot%\System32\Config directory. You can not edit these files directly, you must use a tool commonly known as a "Registry Editor" to make any changes (using registry editors will be discussed later in the article).

The Registry Structure

The Registry has a hierarchal structure, although it looks complicated the structure is similar to the directory structure on your hard disk, with Regedit being similar to Windows Explorer.

Each main branch (denoted by a folder icon in the Registry Editor, see left) is called a Hive, and Hives contains Keys. Each key can contain other keys (sometimes referred to as sub-keys), as well as Values. The values contain the actual information stored in the Registry. There are three types of values; String, Binary, and DWORD - the use of these depends upon the context.

There are six main branches, each containing a specific portion of the information stored in the Registry. They are as follows:

- **HKEY_CLASSES_ROOT** - This branch contains all of your file association mappings to support the drag-and-drop feature, OLE information, Windows shortcuts, and core aspects of the Windows user interface.
- **HKEY_CURRENT_USER** - This branch links to the section of HKEY_USERS appropriate for the user currently logged onto the PC and contains information such as logon names, desktop settings, and Start menu settings.
- **HKEY_LOCAL_MACHINE** - This branch contains computer specific information about the type of hardware, software, and other preferences on a given PC, this information is used for all users who log onto this computer.

- **HKEY_USERS** - This branch contains individual preferences for each user of the computer, each user is represented by a SID sub-key located under the main branch.
- **HKEY_CURRENT_CONFIG** - This branch links to the section of HKEY_LOCAL_MACHINE appropriate for the current hardware configuration.
- **HKEY_DYN_DATA** - This branch points to the part of HKEY_LOCAL_MACHINE, for use with the Plug-&-Play features of Windows, this section is dynamic and will change as devices are added and removed from the system.

Each registry value is stored as one of five main data types:

- **REG_BINARY** - This type stores the value as raw binary data. Most hardware component information is stored as binary data, and can be displayed in an editor in hexadecimal format.
- **REG_DWORD** - This type represents the data by a four byte number and is commonly used for boolean values, such as "0" is disabled and "1" is enabled. Additionally many parameters for device driver and services are this type, and can be displayed in REGEDT32 in binary, hexadecimal and decimal format, or in REGEDIT in hexadecimal and decimal format.
- **REG_EXPAND_SZ** - This type is an expandable data string that is string containing a variable to be replaced when called by an application. For example, for the following value, the string "%SystemRoot%" will replaced by the actual location of the directory containing the Windows NT system files. (This type is only available using an advanced registry editor such as REGEDT32)
- **REG_MULTI_SZ** - This type is a multiple string used to represent values that contain lists or multiple values, each entry is separated by a NULL character. (This type is only available using an advanced registry editor such as REGEDT32)
- **REG_SZ** - This type is a standard string, used to represent human readable text values.

Editing The Registry

The Registry Editor (REGEDIT.EXE) is included with most version of Windows (although you won't find it on the Start Menu) it enables you to view, search and edit the data within the Registry. There are several methods for starting the Registry Editor, the simplest is to click on the Start button, then select Run, and in the Open box type "regedit", and if the Registry Editor is installed it should now open and look like the image below.

An alternative Registry Editor (REGEDT32.EXE) is available for use with Windows NT/2000/XP, it includes some additional features not found in the standard version, including; the ability to view and modify security permissions, and being able to

create and modify the extended string values REG_EXPAND_SZ & REG_MULTI_SZ.

Cleaning The Registry

Although it's possible to manually go through the Registry and delete unwanted entries, Microsoft provides a tool to automate the process, the program is called RegClean. RegClean analyzes Windows Registry keys stored in a common location in the Windows Registry. It finds keys that contain erroneous values, it removes them from the Windows Registry after having recording those entries in the Undo.Reg file.