Registry Disassembled a basic tutorial

The registry is a hierarchical database that contains virtually all information about your computer's configuration. Under previous version of Windows, those setting where contained in files like config.sys, autoexec.bat, win.ini, system.ini, control.ini and so on. From this you can understand how important the registry is. The structure of the registry is similar to the ini files structure, but it goes beyond the concept of ini files because it offers a hierarchical structure, similar to the folders and files on hard disk. In fact the procedure to get to the elements of the registry is similar to the way to get to folders and files.
In this section I would be examing the Win95\98 registry only although NT is quite similar.

The Registry Editor

The Registry Editor is a utility by the filename regedit.exe that allows you to see, search, modify and save the registry database of Windows. The Registry Editor doesn't validate the values you are writing: it allows any operation. So you have to pay close attention, because no error message will be shown if you make a wrong operation.
To launch the Registry Editor simply run RegEdit.exe (under WinNT run RegEdt32.exe with administer privileges).
The registry editor is divided into two sectios in the left one there is a hierarchical structure of the database (the screen looks like Windows Explorer) in the right one there are the values.

The registry is organized into keys and subkeys. Each key contains a value entry , each one has a name, a type or a class and the value itself. The name is a string that identifies the value to the key. The length and the format of the value is dependent on the data type.

As you can see with the Registry Editor, the registry is divided into five principal keys: there is no way to add or delete keys at this level. Only two of these keys are effectively saved on hard disk: HKEY_LOCAL_MACHINE and HKEY_USERS. The others are jusr branches of the main keys or are dynamically created by Windows.

HKEY_LOCAL_MACHINE

This key contains any hardware, applications and services information. Several hardware information is updated automatically while the computer is booting. The data stored in this key is shared with any user. This handle has many subkeys:

Config
Contains configuration data for different hardware configurations.
Enum
This is the device data. For each device in your computer, you can find information such as the device type, the hardware manufacturer, device drivers and the configuration.
Hardware
This key contains a list of serial ports, processors and floating point processors.
Network
Contains network information.
Security
Shows you network security information.
Software
This key contains data about installed software.
System
It contains data that checks which device drivers are used by Windows and how they are configured.

HKEY_CLASSES_ROOT

This key is an alias of the branch HKEY_LOCAL_MACHINE\Software\Classes and contains OLE, drag'n'drop, shortcut and file association information.

HKEY_CURRENT_CONFIG
This key is also an alias. It contains a copy of the branch HKEY_LOCAL_MACHINE\Config, with the current computer configuration.

HKEY_DYN_DATA
Some information stored in the registry changes frequently, so Windows maintains part of the registry in memory instead of on the hard disk. For example it stores PnP information and computer performance. This key has two sub keys

Config Manager
This key contains all hardware information problem codes, with their status. There is also the sub key HKEY_LOCAL_MACHINE\Enum, but written in a different way.
PerfStats
It contains performance data about system and network

HKEY_USERS
This important key contains the sub key .Default and another key for each user that has access to the computer. If there is just one user, only .Default key exists. . Each sub key maintains the preferences of each user, like the desktop colors, the fonts used, and also the settings of many programs. If you open a user subkey you will find five important subkeys:

AppEvent
It contains the path of audio files that Windows plays when some events happen.
Control Panel
Here are the settings defined in the Control Panel. They used to be stored in win.ini and control.ini.
Keyboard Layouts
It contains some advanced code which identifies the actual keyboard disposition how it is set into the Control Panel.
Network
This key stores subkeys that describe current and recent network shortcuts.
RemoteAccess
The settings of Remote Access are stored here.
Software
Contains all software settings. This data was stored in win.ini and private .ini files.

HKEY_CURRENT_USER
It is an alias to current user of HKEY_USERS. If your computer is not configured for multi-users usage, it points to the subkey .Default of HKEY_USERS.

Description of .reg file

Here I am assuming that you already have a .reg file on your hard disk and want to know more about how it is structured.Now do not double click the .reg file or it's content will be added to the registry, of course there will be warning message that pops up. Now to view the properties of the .reg file open it in notepad.
To do so first launch notepad by going to Start>Programs>Accessories>Notepad.
Then through the open menu open the .reg file.
Now the thing that differentiates .reg files from other files is the word REGEDIT4. It is found to be the first word in all .reg files. If this word is not there then the registry editor cannot recognize the file to be a .reg file.
Then follows the key declaration which has to be done within square brackets and with the full path.If the key does not exist then it will be created.

After the key declaration you will see a list of values that have to be set in the particular key in the registry.The values look like this:

"value name"=type:value

Value name is in double commas. Type can be absent for string values, dword: for dword values and hex: for binary values. For all other values you have to use the code hex(#): , where # indicate the API code of the type.
So:

"My string" = "string value" is a string
"My dword" = dword:123456789 is a dword
"My binary" = hex:AA,BB,CC is a standard binary
"My other type" = hex(2):AA,BB,00 is an expand string

Important Note: expand string has API code = 2 and extended string has API code = 7.

As you can see, strings are in double quotes, dword is hexadecimal and binary is a sequence of hexadecimal byte pairs, with a comma between each. If you want to add a back slash into a string remember to repeat it two times, so the value "c:\Windows" will be "c:\\Windows".
Before write a new .reg file, make sure you do this else you will get an error message.

Command Line Registry Arguments

FILENAME.REG to merge a .reg file with the registry
/L:SYSTEM to specify the position of SYSTEM.DAT
/R:USER to specify the position of USER.DAT
/e FILENAME.REG [KEY] to export the registry to a file. If the key is specified, the whole branch will be exported.
/c FILENAME.REG to substitute the entire registry with a .reg file
/s to work silently, without prompt information or Warnings.

That wraps up the Windows Registry.