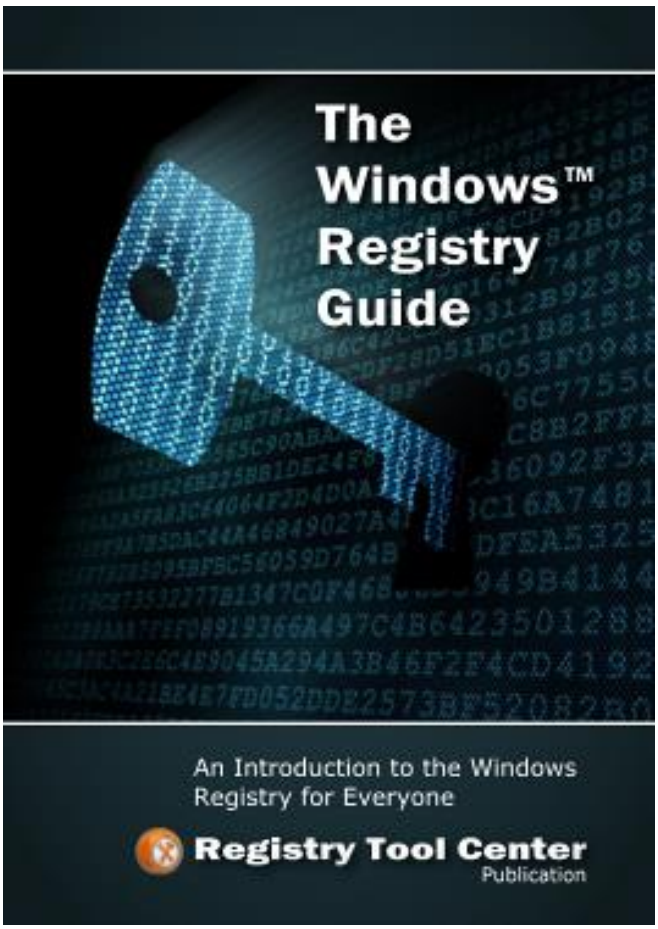

The
Windows™
Registry
Guide
An Introduction to the Windows
Registry for Everyone
Registry Tool Center
Publication

Table of Contents

Disclaimer

1 The Windows Registry Guide

Welcome to the Registry Tool Center Guide to the Windows Registry.

Our aim is to help Microsoft Windows PC users better understand the role of the registry which was first introduced in Windows 95.

We believe the registry is possibly the most important piece of software installed on any Windows PC released since Windows 95. If you truly want to understand how your PC works then learning about the registry is vital.

What does Microsoft say about the registry?

> **"Warning:** Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. **Modify the registry at your own risk**."
>
> Source: Microsoft.com *http://support.microsoft.com/kb/256986*

So as a reader of this book you have made a very sensible first step to understanding the importance of the registry and why you need to be extra careful with any update to this critical part of your Windows PC.

The Team

The Registry Tool Center

Let's have a look at the chapters within this ebook…

Chapter	Chapter Title	Description
1	Introduction	This chapter!
2	A History of Microsoft Windows	Understand how Windows has developed since the first release way back in 1985.
3	A History of the Windows Registry	How and why the registry was developed for Windows 95?
4	What does the Registry do?	What exactly is the role the registry plays?
5	Pros and Cons of the Registry	What is good and bad about the registry?
6	The Registry and PC Security	What are the security issues regarding the registry?
7	Registry Backup & Restore	The most important thing is to backup your registry… we'll tell you how.
8	Maintaining the Registry – Manual or Automatic	How to effortlessly keep your registry up to date and error free
9	Types of Registry Error	What are the different types of registry error and what do they mean?
10	Beyond RegEdit	What are the best advanced registry tools for expert PC users?
11	Registry Tips & Tricks	5 top tips to optimize your registry and improve your Windows PC performance
12	Further Reading	We highlight some great books for learning more about the registry
13	Registry Cleaning Suggestions	A selection of articles describing the benefits of registry cleaning
14	Online References	Where to go online to find out more about the registry and improving your PC

Our aim is to inform and allow PC users to make up their own minds regarding the registry. Should you leave well alone or do you want to explore the finer points of the most powerful software on every Windows PC? Read this book to find out more.

We wish you happy and safe computing!

2 The History of Microsoft Windows

Nowadays, we are exposed to different kinds of computers such as the PC desktop, PC laptops, netbooks, ultrabooks and even tablets, mp3 players and smart phones. They run different operating systems and work in different ways but since it was first announced in 1985, Microsoft Windows (in some form or the other) has found its way on to all of these devices.

This chapter will help you understand the basic components of personal computers and how Microsoft Windows has evolved over the years to play a crucial role in how we use PCs today.

2.1 A System of Two Halves – Hardware and Software

OK, so on to the basics. We can say computers consist of hardware and software components.

An example of the hardware components would be the wiring, memory chips, processor chips and semi-conductor boards that are physically inside the computer case.

The software components are computer instructions and commands that are programmed in the processor chips within the computer. Software can be classified into system software and application software.

The system software, also known as the 'Operating System', is the software that that controls how the computer works. A computer must have an operating system in order to work. Microsoft Windows is the most popular PC computer operating system in history.

The application software is specific computer programs that typically provide a service to the user. For instance, Microsoft Word provides a means for people to create letters, reports and newsletters. Adobe Reader allows people to view PDF files. Mozilla Firefox is a web browser that helps people surf the Internet. All of these programs rely on the operating system for them to work properly.

2.2 The Operating System… the Heart of the Machine

The main system software is the Operating System (OS). It has a set of programs that manage the hardware components and software programs in the computer. Some people refer to it as the conductor who directs the orchestra. Others consider it the heart of the computer.

The operating system checks the integrity of the computer memory; it prioritizes program instructions, controls the hardware devices, manages the system and data files and ensures the proper functioning of the network.

Put simply, if the operating system fails, the computer fails.

The Operating System is essential for the proper operation of a computer. This is no different for Microsoft Windows. Windows is the center of everything when it comes to running your PC. Hundreds of millions of people every day switch on their computer and Microsoft Windows will quietly check everything is working OK and allow them to do their work, send email, surf the web and play games.

2.3 Windows through the Years

If we go back to the 1970's and 1980's, the large computers used in corporations required huge and complex operating systems to handle the numerous business tasks they were programmed to do. It required many technicians and expensive computer rooms to house these large machines.

In the early 1980's, with the advent of the smaller-sized personal computers (from Apple and then IBM), there was a need to develop an operating system that could fit in the memory of the small PCs and still function with optimum efficiency.

Bill Gates and Paul Allen (and their fledgling company, Microsoft) assured their success by striking a deal with IBM to adopt their operating system (Microsoft DOS also known as MS-DOS) for the new IBM PC. The fact they had not actually created MS-DOS and had purchased it from another company is the stuff of legend.

MS-DOS was the start of a series of Microsoft operating systems. Succeeding versions of Microsoft operating systems carried the name Windows or MS Windows. Microsoft did develop an operating system for IBM called OS/2 (Operating System 2) after MS-DOS but this was not a commercial success for either organisation and subsequently Microsoft put all its efforts into Windows.

2.4 Windows 1.0 - The Journey Begins

Windows 1.0 was launched in 1985 and gave users the facility of using a mouse instead of typing the system commands. Drop-down menus made it easy to point and click with the mouse. This was a definite change for PC users who were used to a keyboard based operating system and applications.

The growing popularity of the Apple Mac and its graphics (not text based) approach for it operating system was putting pressure on Microsoft to develop Windows. Windows 1.0 was a pale imitation of the Apple Macintosh interface and was not widely adopted.

2.5 Windows 2.0 – Windows improves…

Released in November 1987 Windows 2.0 improved upon Windows 1.0 with new features such as overlapping Windows. Other tools that came with Windows 2.0 were a simple painting program called 'Paintbrush', a simple word processor called 'Write' and something called 'PIFEdit' which could be said to be one of the ancestors of today's Windows registry.

As computer manufacturers developed PCs with additional computer memory and faster processing speed, Microsoft made use of these hardware enhancements to improve on their operating system. Graphics displays were enhanced.

With the release by Intel of the 286 and 386 processors, Microsoft customised Windows in 1988 into a Windows/286 version and a Windows/386 version. This differentiation allowed Windows to take advantage of the extra power in the 386 processor which improved multi-tasking (running more than one program at a time).

2.6 Windows 3.x – The Breakthrough

Windows 3.0 was released in May 1990. Windows supported 256 colors on the screen at the same time if you had a graphics card that could support that large number of colors. Today, PC screens can support millions of colors but back in 1990, you got 256 colors if you were lucky.

However, this was all progress at the time and Windows 3.x proved to be the version of Windows that was widely adopted by PC users. It has to be said that MS-DOS was still popular, particularly for home users who liked to play games. Windows was known as a poor operating system for computer game players. That of course has now changed.

For corporate users Windows for Workgroups 3.11 provided networking support, thus allowing PC users to join together as workgroups. In the early 1990's, Local Area Networks (LANs) were being installed in many companies and being able to network with Windows was very important.

2.7 Windows NT – The Older, more Serious Brother

Launched in July 1993, Windows NT (New Technology) 3.1 was a more sophisticated version of Windows aimed at corporate users who required a quicker and more powerful operating system to run business, engineering and scientific applications.

Windows 2000 was the successor to Windows NT 4 when it was released in February 2000. It was subsequently replaced by Windows XP on the desktop and Windows 2003 as a server operating system.

Windows NT was the first Windows operating system to communicate via TCP/IP (which is how all computers on the Internet communicate). It is a little known fact that computer code from Windows NT is still at the heart of Windows 7 which was released in 2009, some 16 years after NT was first launched.

2.8 Windows 9.x – Windows is now the 800 Pound Gorilla

Microsoft released Windows 95 in August 1995 with a massive launch involving the use of the Rolling Stones track 'Start Me Up' in adverts around the world. This was reference to the new 'Start' button introduced to the bottom left corner

of the Windows desktop screen. If Windows 3.x had been the breakthrough release, the Windows 95 version cemented Windows' position as the dominant desktop operating system in the world.

Windows 95 offered many features and functions for the Internet. It had plug and play capabilities, making it easy to install and remove hardware components. It included facilities for mobile computing and integrated networks. The Internet Explorer 2.0 browser software was also released in 1995 with an update for Windows 95.

Windows 98 and Windows 98 ME (ME for Media Edition) were evolutionary versions of Windows 95 with enhancements and extra programs. In 2003, over 27% of all searches on Google were from Windows 98 machines.

2.9 Windows XP – Learning from Experience

Windows XP (eXPerience) was released in October 2001 and with over 400 million copies sold was a great success for Microsoft. At its peak in 2007, Windows XP held just over 70% of the PC operating system market worldwide.

The user interface was improved over Windows 9.X and a range of speed and usability improvements included in the version.

As with all new versions of Windows, the recommended and high end hardware specifications rose to accommodate the new features. 1.5 Gb of disk space was required to install Windows XP and eventually a further 3.3 Gb was required for the 3 service packs issued by Microsoft.

Windows XP presented improvements in networking and stability that made it popular in the corporate world as a new standard operating system for company PCs. All in all, Microsoft had yet again improved Windows but Apple's OSX operating system was still seen as the benchmark to be judged against. How would Microsoft continue to respond?

2.10 Windows Vista – Where did it all go Wrong?

There were high hopes for Windows Vista which was more than ever pitched against the Apple Mac. Introduced in January 2007 with an updated look and feel, nicknamed 'Aero', Vista was expected to improve upon Windows XP in the areas of security, multimedia support and networking amongst many other features.

However, the security warnings for users got in the way of actually using the PC and security flaws in early releases of Vista that showed Microsoft still had a way to go to keep hackers and viruses at bay. Windows Vista was also not considered as reliable and friendly as Windows XP.

Windows Vista sold 330 million copies by 2009 which in any other company's books would have been a huge success. For Microsoft though, this was a failure, selling fewer copies than the previous version, not least because the corporate

world did not upgrade to Vista en mass, they kept with their Windows XP machines hoping for something better.

It was up to Microsoft to learn some lessons and improve Windows in the next version. Would they do it?

2.11 Windows 7 – Back on Form

Microsoft chose to learn from the Vista experience and over the course of building Windows 7, had 8 million people test and give feedback on their new version of Windows.

Released in October 2009 the aim was to provide people with more of an upgrade experience rather than a swathe of new features as was presented in the release of Windows Vista. This more gradual change in the operating system may have contributed to greater acceptance of Windows 7 by users when compared to Windows Vista.

The windows taskbar sitting at the bottom of the screen was revitalized and provided a place for users to easily pin applications to the taskbar.

2.12 Windows 8 – A Brave New World

Come the release of Windows 8 in October 2012, the world of the operating system had changed considerably from those early days in the 1980's. The Windows operating system now had to account not just for PCs but tablets and smart phones in a seamless user experience.

Microsoft has developed a new design language, code named 'Metro', for how the screen displays information in Windows 8. This look and feel applies to all devices and has met with critical success from the fickle early adopters in the PC user community.

Windows 8 brings deeper integration with the online world and Microsoft services such as SkyDrive, Xbox Live and Outlook email.

2.13 Let's not forget the Registry

One of the most important developments in the design of Windows was the introduction of the Windows Registry in Windows 95.

It was with Windows 95 that Microsoft made the effort to create a centralised register (a registry) of all the configuration data for a PC in an orderly, organized and well-structured manner.

Since the mid 1980's Microsoft Windows has grown to become the dominant operating system for personal computers and defines much of what we do with computers today. The registry has played an increasingly important role in this operating system.

3 A Short History of the Registry

It began with .INI files.

The earlier versions of Windows (up until Windows 3.x) made use of initialization files, more commonly known as .INI files, to help manage the configuration of the system and application software. Many applications would have their own individual .INI file with their own specific settings.

The .INI files are formatted as text files which are human-readable. The .INI files were located with the application files which meant the .INI files were kept in locations that were difficult to find and access for the average user.

Since the personal computers at the start were intended for an individual, it was logical to keep the information inaccessible to prevent the user from accidentally damaging or corrupting the information. However, it made it difficult to optimize the PC configuration. The users had to accept the default settings or customize the .INI files for each application.

3.1 Multiplying .INI management

When a PC was connected to a network, users needed to access the .INI files so they could specify their desired settings for their computer network environment.

In the corporate environment in the early 1990's this meant that the use of .INI files was multiplying within companies as they networked more and more of their Windows 3.x PCs to Local Area networks (LANs).

The computer support departments in companies all over the world were finding it increasingly difficult to keep track of .INI settings across hundreds, if not thousands, of PCs within their organizations.

The .INI file had come to a point where more applications, more users and more PCs was making it incredibly difficult for large scale organizations to manage their PC configurations. A solution was needed.

3.2 Next Came the Registry

Microsoft introduced the registry as part of Windows 95 in August 1995. The registry was a replacement for .INI files and was designed to centralize the configuration of each PC in one location.

The registry defines various kinds of users and their rights and privileges when using the computer and application software systems. It provides information to configure software applications and connected hardware components. The registry defines the rules and restrictions in mathematical and logical computer operations.

The registry contains settings for low-level machine operations to high-level applications systems. Since all settings are centralized in the registry, it is easier for applications to access the information for their processing needs. All applications refer to the registry.

The centralization aspect also makes it convenient for users to locate the information that they want to adjust. The registry size is much larger and complex than the collection of individual text based .INI files.

Experienced users and administrators can maintain the registry over the network. This is particularly necessary in large scale computing environments such as corporations and government departments where all PCs require a standard configuration.

Effective management of the registry (which is really a hierarchical database) ensures these organizations have fewer computer errors. The registry needs to be managed over the network so a computer support person in one location can update and edit the registry on a user's PC in another location.

Checks and balances, like firewall rules and consistency policies ensure there are no conflicting operations among the users in the network. There is better integrity within the system since the registry is created similar to a hierarchical database. It is easier to determine and establish the properties for the different functions and operations.

3.3 The Family Tree

An ancestor of the registry was first seen in Windows 3.1, it was a simple file called REG.DAT. It was used to store configuration data and information about linking and embedding application objects (OLE). It facilitated adding data from different applications to a single document, such as putting images and spreadsheets in a text document.

Configuration data for windows and the operating system were still maintained in INI files. It was intended for a single-user environment.

When Microsoft released Windows 95, the registry was released and the data more organized.

Although the registry was not required for use in a Windows application, it was logical and practical to compile in one location all the settings and data that were previously contained in REG.DAT and the other INI files.

Some application software still kept their configuration settings within files where the executable application software is located.

People refer to the registry as a single file. Actually, there are the SYSTEM.DAT and the USER.DAT files. These files hold information relevant to the computer and the user respectively and are usually kept in the windows directory.

As memory size increases, the opportunity to enhance the registry also increases. With the worldwide proliferation of personal computers, workstations

and networking, it is becoming essential for users and companies to perform their own systems maintenance.

3.4 Registry Differences across the Versions

Although the registry did not seem to have significant changes over the succeeding desktop versions, it appeared that enhancements were made to address the objectives of the various operating systems.

For instance, in a network environment, the system administrator would place the file USER.DAT in the login directory of the user to enable them to log in from other work stations.

In Windows NT, the registry is spread over several files called hives. The hives are in the SYSTEM32\CONFIG directory and not in the Windows directory. This is the same location for Windows 2000, XP, Server 2003 and Vista.

There are 3 registry files in Windows ME; namely Classes.dat, User.dat, and System.dat. Most registry transformations were done due to networking requirements.

3.5 Using Registry and INI files

Microsoft advocates the use of registry over INI files because the registry was proven to be more robust, had better handling of functionalities and was in a centrally accessible location.

It is easier for technical users to access and update the registry rather than .INI files.

Despite the move to the registry, many applications continue using .INI files as a means to achieve backward compatibility with old versions of Windows systems. This helps users execute their application software on various Windows operating systems that may require using .INI files.

3.6 Registry Cleaning Software

The registry is not completely perfect.

There are instances when the system will encounter registry-related problems. You should back up the registry regularly so you can recover the settings in case of emergencies or fortuitous events. You can do a manual or automated backup.

You can use the registry editor software provided by Microsoft or choose from registry editor software in the marketplace that support cleaning, backing up and restoring the registry. Since the registry will remain part of the computer system for several more years it is a good idea to select registry cleaning software to maintain your registry.

4 So what does the Registry Actually Do?

The registry has been an important part of Windows since Windows 95.

The registry contains the configuration settings required for the execution of low-level machine operations up to the processing of high-level applications software.

If the Registry Fails… Your PC fails!

This section describes the various functions of the registry that make it so important.

4.1 Start Up

Every hardware component and software program set up in the computer will most likely have its configuration defined in the registry.

When you start Windows, the system refers to the registry to determine what drivers should be loaded, what the settings should be at start up and the resources needed to make the computer function properly. This information is essential for the successful start-up of your PC and it the registry is at the center of it all.

Without the registry you would not be able to start your Windows PC!

4.2 Default Settings

When the Windows operating system is first installed on a computer, it uses the default settings defined in the registry. The default settings are usually a reflection of the settings that will work for the majority of users. Once the operating system is installed, the user can edit the default settings.

Default registry settings (sometimes called 'factory settings') are important as they define the configuration of s standard Windows PC. The default settings will work in 99% of the cases and allow someone to buy a computer, switch it on and have it work right away.

The default settings in the registry help provide a base configuration for all Windows PCs – a configuration that works in a new computer or one that has to be rebuilt.

4.3 Your Personalized Computer

Aside from the settings needed for the operating system functions, the registry contains information related to user needs and user application software. For instance, the font settings you want to use every time you activate the Microsoft word processor or the Windows startup logo and background screen can be defined in the registry and activated every time you start the Windows system.

The registry also contains the directory location where you want files to be downloaded automatically.

The registry contains the information that makes your PC personal to you – wallpaper, screen options, file locations and lots more.

4.4 Advanced Users

Given the registry holds so much important information regarding the PC configuration it is an important source of information for expert PC users, PC specialists, developers and programmers.

Developers can control the registry configuration data to optimize the system operations. They can enable hardware and system software components to interface in varying ways with application software.

If there are problems with a PC then PC engineers will often check the registry to ensure there are no errors or to repair registry file corruption.

When testing a software application it is possible for a developer to monitor the registry and track changes that occur in the registry while a program, such as Microsoft Word, is running. This can help debug errors and improve how programs work with the registry. Visit The Registry Tool Center to find out more about advanced programs to manage the registry.

The registry is a critical component of every PC. Advanced users need to know how the registry works, how the registry is configured and how it can be used to improve the performance of a PC and installed software programs.

4.5 What if the Registry is Damaged or Corrupted?

The contents in the registry are so encompassing and complete that any error in the registry could result in total failure of the computer system. Minor errors could result in the malfunctioning of specific operations and routines while more major errors could mean the non-operability of the operating system.

Since Windows allows the registry to be maintained by users, it is critical that users handle the maintenance of the registry with extreme caution.

No matter how careful the person may be, there exists the possibility of committing an error accidentally. It is highly recommended that backups of the registry be done on a regular basis.

If you are an expert PC user and plan to do extensive editing on the registry, you must backup the registry after completing several edits. In this way, restarting your work from the last backup will not take too much time and effort.

It is critical that backups of the registry are kept in case of registry corruption or registry errors arising.

4.6 PC Performance

The registry holds so much important configuration information that the speed of a Windows PC is directly affected by the health of the registry.

Errors within the registry (for instance information stored in the registry is out of date or is linked to files that have since been deleted) can slow down a PC by making it difficult for Windows or programs to access the configuration information.

The ultimate problem is when the registry is completely corrupted and this will stop a PC working completely.

Maintaining your registry is a great way to keep your Windows PC running at top speed and error free.

5 Pros and Cons of the Registry

When Windows 95 was released the registry was a big step forward for Windows computers in many ways.

However, over the years PC users have developed a love/hate relationship with the registry. Users appreciate the registry is a single place to configure a PC but at the same time it is not the easiest aspect of Windows to manage and edit.

This section will describe the major advantages and disadvantages of the registry.

5.1 Registry Advantages

The main advantages are as follows:

5.2 Eliminates multiple INI files

As mentioned in a previous chapter, before the registry .INI files were used by applications to control configuration settings. Many applications had their own .INI file and it was difficult to keep track of multiple .INI files. System conflicts could arise from different system settings in different .INI files in different locations on a Windows computer.

The registry improves this situation by providing one place to store configuration information rather than have it distributed across multiple files in multiple locations. This consistency in the registry reduces the number of errors that occur and ensures that the PC is working at optimum speed.

5.3 Store standard configuration information

The registry is now the standard place Microsoft, application developers and hardware manufacturers look to store configuration information. This information is held and described in standard formats that all parties are agreed on.

Standardizing the location and format of Windows configuration information makes it easier for PC professionals and developers to know where and how to search for registry information and update the information in the correct formats.

5.4 Manage thousands of PC configurations

Large organizations with thousands, if not tens of thousands, of PC users can use the registry settings on each PC to manage the security, features and desktop appearance of their company computers.

The registry will help control which users can do which tasks on a given PC.

5.5 Simpler Backup & Restore of Configuration Settings

Backing up and restoring registry files is much simpler than backing up multiple .INI files since all the settings are effectively in one central database. If the registry is backed up, then the main configuration settings for the PC are backed up.

The Registry is not easily accessible to the Average User

The registry, although accessible, editable and fully documented, is normally published with warnings that errors could result in a complete computer malfunction.

This is intended to deter average users from accidentally accessing and corrupting the registry.

5.6 Registry Disadvantages

The main disadvantages of the registry are as follows:

5.7 A Single Point of Failure

In the IT world, the term 'Single Point of Failure' describes that part of a system that should it break down, the whole system breaks down.

So in a car, the engine is a single point of failure. If the engine is not working, the car will not go anywhere. With a Windows PC, if the registry is missing or contains corrupt information, the PC will stop working.

We say it elsewhere in this ebook but it is worth saying again:

If the Registry Fails... The PC Fails!

The registry is one of the biggest single points of failure on a PC. It is all well and good centralizing configuration information in one place, in standard formats everyone can refer to but when something goes wrong, it can be catastrophic.

This is why at the Registry Tool Center we recommend you schedule automatic cleaning and backup of the registry on your PC.

5.8 Navigation of the Registry

While it is an advantage to make the registry difficult to use for the average user, it actually hinders the advanced users who need access to registry information to troubleshoot problems, develop software and manage PC on networks.

Microsoft's registry editor (RegEdit) is a very basic tool and does not provide an advanced search functionality or means to track changes to the registry.

This has meant that some enterprising software companies have developed advanced registry tools to fill this gap. However, you have to know where to go to download these registry tools.

Visit the Registry Tool Center to find a selection of the best registry tools available for free download.

5.9 Security Vulnerability

Since the registry is a critical part of every PC it has been targeted by computer virus and trojan programs.

Each Windows PC has a registry and so if a virus is successful in making changes to the registry it could potentially do an awful lot of damage to configuration information, making the PC unusable or even to the point of destroying user data.

5.10 Summary

The registry is the standard configuration database Microsoft has used since 1995 and it has its benefits as well as its disadvantages.

In our opinion, the registry has helped standardize configuration management on Windows PCs and improved reliability, consistency and performance of these machines. As long as you look after your registry, it will look after you.

6 The Windows Registry and PC Security

6.1 Types of Viruses

In this section we will give an overview of security threats to your PC from certain types of program and how this can affect your registry and PC in general.

Generally speaking a virus is a computer routine or program that can reproduce itself and spread across computers. All viruses should be considered harmful and the degree of harm depends on the kind of virus.

Malware means 'MALicious softWARE' and covers all types of viruses such as trojan horses and worms as well as spyware. People create all kinds of malware to corrupt the computer system or to extract confidential data.

Worm viruses exploit security weaknesses to spread across networks within organizations or over the Internet. Trojan horse programs grant hackers entry into the computer system. Boot sector viruses are activated upon boot-up of the computer. Macro viruses infect documents like Word or Excel and can spread to other similar documents.

Some viruses stay in a computer's memory and use up the memory. Polymorphic viruses can replicate and change its digital identity every time it reproduces. It makes this malware difficult to detect. Time bomb viruses become active based on specific dates or events. Spyware gathers data about the computer and the users using the computer.

All in all, these types of programs are not generally healthy for your computer! Some of these programs attack the registry directly and seek to exploit any registry weaknesses.

6.2 The Effect of Viruses

Viruses can damage your computer, operating system functions, applications programs and data files in a whole range of ways, including:

- Changing the registry keys and system settings to allow entry of more viruses into the system
- Disabling access to the registry to prevent edit and maintenance of the files
- Erasing or corrupting the data in the disk drives
- Displaying strange messages on the computer screen; or blanking out the screen entirely
- Altering computer programs to produce erroneous information
- Using all RAM memory to degrade computer performance, causing the computer to slow down and eventually crash

Some viruses that can change or delete registry and system settings are W32.Beagle.CO, Adware.win32.Adkubru and Redirect.clickshield. Clickshield can change your registry entries and settings of the hardware, software, security, firewall, and startup configurations.

6.3 How does Malware Enter the System?

Viruses can enter your system through emails, infected multimedia codecs, websites, infected external media, and through the network. Malware programs can be disguised as legitimate files or programs.

Malware routines can be inserted in the codes of other legitimate programs. The malware enters the computer when you download software or access software from external sources. Attachments in the emails, website advertisements, games and programs downloaded from the web page can contain the malware.

The malware becomes active once you open the attachment file or start the software. The malware replicates or attaches itself to other files in your computer, such as config files.

Before a malware can be effective, it has to be executed first. It does this by becoming part of the configuration files that are executed upon startup, such as the autoexec.bat, config.sys, and registry files.

Any command embedded here will open when any exe file is executed. Another way for a malware to take charge over the systems is by modifying the association of commonly used file extensions, such as EXE, .DLL and, .COM.

Another location that could contain autostart registries which can be exploited by viruses is \HKEY_CURRENT_USER\ Software\ Microsoft\Windows\CurrentVersion.

So the registry is vulnerable to some viruses. The absolute best defense is to have an up to date anti-virus program running on your machine. We recommend www.avg.com which has both a free and a paid anti-virus program.

6.4 Securing the Registry

Another aspect to security of the registry is restricting the user to edit the registry. This is especially necessary in large organizations that have multiple users who will require the PC for different reasons.

In a Vulnerability Note issued by the US-CERT (Computer Emergency Response Team) agency on 26 November 2010 it was identified that a user could execute arbitrary software code with system privileges via the registry. For further information, click on this link: US Cert Vulnerability Note VU#529673

You can inhibit users from editing the registry by allowing the "prevent access to registry editing tools" policy or by applying restriction policies. Technical users can circumvent it by using 3rd party tools.

We can try securing the registry more effectively by inhibiting entry into the computer itself. By stopping the entry into the computer, you are effectively preventing the registry from getting corrupted. This would be accomplished by putting a password on the computer or even using a finger print recognition system (as some laptops have these days).

7 Backup and Restore the Registry

Being able to backup and restore the registry is possibly the most important thing you can do with your PC. Since the configuration of your PC is held within the registry, you need to be able to restore it if it becomes corrupted or contains errors.

7.1 The Manual Approach to Registry Backup and Restore

If you are an organized type of person, then it is perfectly possible to run your own backups of the registry.

It is always good to go to the source and we have selected the key support links from Microsoft for backing up the registry in 3 different versions of Windows (XP, Vista and 7).

This involves using RegEdit to save a copy of the registry on your PC.

Windows Version	Microsoft Support Link
Windows XP	http://support.microsoft.com/kb/322756
Windows Vista	http://windows.microsoft.com/en-us/windows-vista/Back-up-the-registry
Windows 7	http://windows.microsoft.com/en-us/windows7/Back-up-the-registry

7.2 The Automatic Approach – PC Backup Software

It is recommended that all users (beginners and experts alike) take the automatic approach to backing up the registry. The manual approach can work in ad hoc or one off situations but is not recommended for regular, scheduled backups.

If you are already using some sort of backup software on your PC (you often find that hard drive manufacturers such as Western Digital or Seagate include backup software with their products), then make sure you include the registry as part of the backup. In fact backup software is included as part of Windows.

The registry location information shown below is taken from Wikipedia at the following link: http://en.wikipedia.org/wiki/Windows_Registry. Use the information to identify the location of the registry for your particular version of Windows.

File Locations

The Registry is physically stored in several files, which are generally obfuscated from the user-mode APIs used to manipulate the data inside the Registry. Depending upon the version of Windows, there will be different files and different locations for these files, but they are all on the local machine. The location for system Registry files in Windows NT is \Windows\System32\Config; the user-specific HKEY_CURRENT_USER user registry hive is stored in `Ntuser.dat` inside the user profile. There is one of these per user; if a user has a roaming profile, then this file will be copied to and from a server at logout and login respectively. A second user-specific Registry file named UsrClass.dat contains COM registry entries and does not roam by default.

Windows NT-based operating systems (NT, XP, Vista, 7)

Windows NT-based systems store the registry in a binary file format which can be exported, loaded and unloaded by the Registry Editor in these operating systems. The following system Registry files are stored in: `%SystemRoot%\System32\Config\`:

`Sam` – HKEY_LOCAL_MACHINE\SAM

`Security` – HKEY_LOCAL_MACHINE\SECURITY

`Software` – HKEY_LOCAL_MACHINE\SOFTWARE

`System` – HKEY_LOCAL_MACHINE\SYSTEM

`Default` – HKEY_USERS\.DEFAULT

`Userdiff` – Not associated with a hive. Used only when upgrading operating systems.

The following file is stored in each user's profile folder:

`%UserProfile%\Ntuser.dat` – HKEY_USERS\<User SID> (linked to by HKEY_CURRENT_USER)

For Windows 2000, Server 2003 and Windows XP, the following additional user-specific file is used for file associations and COM information:

`%UserProfile%\Local Settings\Application Data\Microsoft\Windows\Usrclass.dat` (path is localized) – HKEY_USERS\<User SID>_Classes (HKEY_CURRENT_USER\Software\Classes)

For Windows Vista and later, the path was changed to:

`%UserProfile%\AppData\Local\Microsoft\Windows\Usrclass.dat` (path is not localized) alias `%LocalAppData%\Microsoft\Windows\Usrclass.dat` – HKEY_USERS\<User SID>_Classes (HKEY_CURRENT_USER\Software\Classes)

Windows 2000 kept an alternate copy of the registry hives (.ALT) and attempts to switch to it when corruption is detected. Windows XP and Windows Server 2003 do not maintain a `System.alt` hive because NTLDR on those versions of Windows can process the `System.log` file to bring up to date a System hive that has become inconsistent during a shutdown or crash. In addition,

the %SystemRoot%\Repair folder contains a copy of the system's registry hives that were created after installation and the first successful startup of Windows.

Each registry data file has an associated file with a ".log" extension that acts as a transaction log that is used to ensure that any interrupted updates can be completed upon next startup. Internally, registry files are split into 4k "bins" that contain collections of "cells".

Windows 95, 98, and Me

The registry files are stored in the %WINDIR% directory under the names USER.DAT and SYSTEM.DAT with the addition of CLASSES.DAT in Windows Me. Also, each user profile (if profiles are enabled) has its own USER.DAT file which is located in the user's profile directory in %WINDIR%\Profiles\<username>\.

Windows 3.11

The only registry file is called REG.DAT and it is stored in the %WINDIR% directory.

Refer to the above information from Wikipedia to include the registry location in your regular PC backups.

The main challenge with this approach is when you need to restore the registry you need to be able to find the exact registry files you need amongst the entire backup. A PC backup will typically run to thousands of files so make sure you have a note of the location of all the registry files you require.

7.3 The Automatic Approach – Registry Cleaner Software

If you do not use backup software on your PC to backup the registry then you can always use the registry backup and restore features of a registry cleaner program.

Visit our website at The Registry Tool Center to see our latest recommendation for registry cleaner software.

What you can expect is for the registry cleaner software to make a backup of the registry after a registry scan. Before any registry errors are fixed, the registry is first backed up and a copy of the registry saved. The errors will be fixed and the PC should now be error free.

If you then make a change to the registry that causes problem, you can simply load up the registry software, find the most recent registry backup and restore the registry settings immediately.

It is usually free to download the registry software on a 'try before you buy' basis. You can try out the registry software to see if it meets your registry backup needs.

Summary: Whether you choose a manual or automatic approach make sure you are fully protected and have your registry backed up.

8 Maintaining the Registry – Auto or Manual?

Hopefully we have established that the registry is an important part of your PC that requires looking after.

8.1 The Do Nothing Approach

The standard way for the majority of users is to do nothing. This has the benefit of requiring no thought or effort but the downside is that errors (such as shared DLL or COM/ActiveX errors) will creep into the registry over time. This can slow down your PC, produce seemingly random error messages or simply stop some programs from working.

Summary: Your PC is more important than this.

8.2 The Hand Crafted, Manual Approach

You could take the manual approach to registry maintenance. However, this approach does require an in depth knowledge of the workings of the Windows operating system and in particular an understanding of the registry. Technical terms such as root keys, hives, HKLM and HKCR should all be familiar.

Further Warning: If you want to edit the registry manually, make sure you have a backup of the registry and know how to restore the registry in the event of a problem. Remember: If the registry fails… your PC fails!

The tool supplied by Microsoft for manually editing the registry is called RegEdit. This tool can be run from the command line and give the user (if they have sufficient rights) access to the entire registry.

If you are to manually maintain the registry then make sure you have a well-organized system to backup and restore the registry.

Visit the Registry Tool center at RegistryTool.net to find a selection of advanced registry tools that are free to download and use on your PC. These tools can assist you in the manual management and maintenance of the registry.

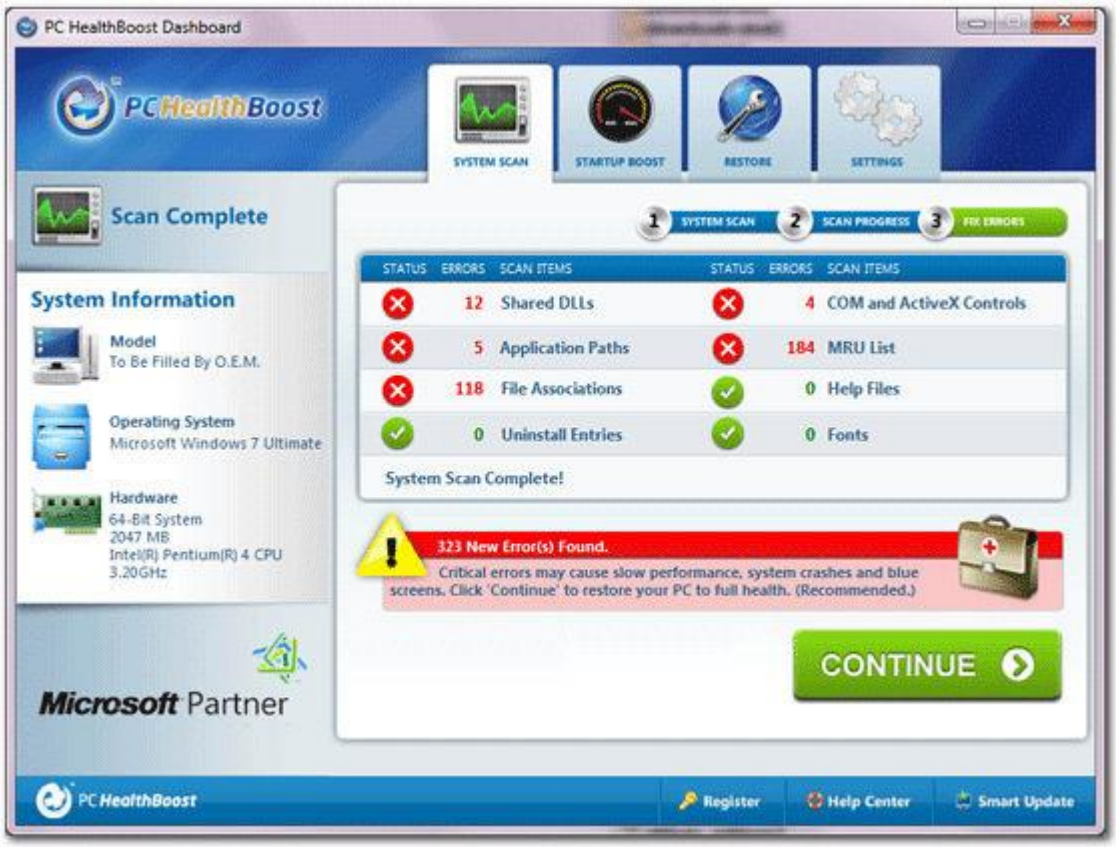
Summary: If you're a PC expert who regularly works with registry settings and can confidently backup and restore the registry, this option could be for you.

8.3 The Automatic, Sleep Well at Night Approach

This approach suits all types of users – from the newest owner of a PC to the most experienced Windows expert.

The automatic approach makes use of a PC registry tool called a registry cleaner. This type of software program you download to your PC will scan the registry and within minutes spot all the errors contained within the registry.

See the screenshot below to see a Registry Cleaner screen finding errors on a PC.



You can then have all the errors automatically repaired by the registry tool or for the experts; they can choose which errors to repair individually. This saves hours of effort that would otherwise be required to identify where the errors are located. In fact trying to find all the registry errors manually is like looking for a needle in a haystack and is not the best use of anyone's time.

Any good registry cleaner software will provide the feature to allow the registry scan and repair to be automatically scheduled. This means that you, the PC users, do not have to think about running a scan to check the health of your PC.

Before and after the scheduled repair a backup is automatically made of the registry. This means you do not have to manually copy the registry on a regular basis. The software will do it for you.

Registry cleaning software should be able to do this every day of the week or on a weekly basis. Either way, you have automatic registry backup. A PC expert would appreciate this as much as a beginner PC user.

Summary: Download and install a registry cleaning tool on your Windows PC and your registry will now be automatically scanned, repaired and backed up. As a result your PC is likely to run quicker and experience fewer or no errors at all.

9 Types of Registry Error

The registry plays such an important role in every Windows PC that, if not looked after, it can generate many different types of error message. In this section, we look at the main types of registry error and what they mean.

9.1 Shared DLLs

A Dynamic Link Library (DLL) holds shared code or data for an application in a file with the extension '.DLL'. A shared DLL is used by multiple applications.

There is a situation on Windows PC's called 'DLL Hell' (find out more with this excellent Wikipedia explanation http://en.wikipedia.org/wiki/DLL_hell).

The problem occurs when there are different versions of the same DLL on a PC, when there are unused versions of a DLL that get mixed up with live versions or where one DLL is not compatible with another. This can cause error messages, programs not working and system problems in Windows.

While Microsoft COM and .Net initiatives have gone some way to solving this situation, it is still possible to find DLL errors on even the latest Windows PCs.

9.2 Application Paths

An application path is a way of describing the location of an application such as Microsoft Word on a Windows computer's hard disk. This is the 'path' to find an application.

This location is stored in the application path variable in the registry. This means the Windows PC has a central record of where every application is located.

It is possible for this information to become corrupted or missing which can cause problems when a user tries to run an application. An application error is generated and the user will have to manually locate the application on the hard disk.

9.3 File Associations

Microsoft Windows defines different types of files by a file extension which is a short code after a period at the end of a file name. Some of the most common extensions you may know about are '.doc', '.xls' and '.jpg'.

Associated to each type of file is a program on the computer. For instance '.doc' are typically associated with Microsoft Word, '.xls' is usually associated with Microsoft Excel and '.jpg' for a graphics / picture program such as Picasa.

The file association information is stored in the registry and held centrally. If the file association becomes corrupt or lost, it is not possible to automatically open a

file with a double click. Windows will not know which program to automatically run to open the file correctly.

It is important to keep file associations up to date and accurate to avoid file association errors.

A regular scan of the registry will clean up file association errors on your PC.

9.4 Uninstall Entries

When most programs are installed on a Windows PC they update the registry with new information to ensure the program works correctly and does not have conflicts with other applications installed on the computer. The fact the registry acts as a central place for all applications to store and share configuration information is a key benefit of the registry.

However, whenever the time comes to uninstall a program, usually via the Windows control panel program uninstall feature, registry errors can occur.

Uninstall entry errors occur when the program being uninstalled does not delete some of its configuration settings within the registry. This may be down to poor programming on the part of the application developer or because of a conflict with another program that does not allow a registry entry to be deleted.

This leaves the registry with entries, values and keys that do not link to any program. Errors can occur when Windows tries to match this information with an application that has since been uninstalled.

9.5 COM and ActiveX Entries

Component Object Technology (COM) and ActiveX are programming technologies from Microsoft that allow programs and features within programs to be built from mini blocks of computer code.

The use of ActiveX is widespread across Microsoft Windows applications and consequently errors can occur in many different programs and situations.

As an example ActiveX controls can be embedded within web pages and sometimes it is desirable to block the ActiveX controls. See the help file from Microsoft on how to achieve this manually:

http://support.microsoft.com/kb/240797

While ActiveX errors are not terminal for a Windows PC and typically restricted to a particular situation for a particular application, it is worth ensuring the registry is scanned and cleaned regularly to avoid the errors in the first place.

9.6 MRU List

The Most Recently Used (MRU) list is a list of the documents that have been most recently opened within a specific application. For instance in Microsoft Word 2003, in the File menu option, you will see at the bottom of the menu a list that shows the most recently opened Word document. This is the MRU list.

This MRU list is held within the registry and updated every time a document is opened and closed.

If there is a problem with the application such as an unexpected shut down or if the file is moved from one folder to another, then the MRU list will be out of date and display an error message when you try to load a document in the list.

A regular clean of the registry will remove this type of error.

9.7 Help Files

Microsoft has specific file formats for help files. One of those file formats is the '.CHM' format. Most programs will have help information stored in a Windows compatible format and the registry records where the help information is kept for each application.

See Microsoft's site http://support.microsoft.com/kb/917607 for further advice about Help file related errors.

It is possible for the help file information for an application to become corrupted or missing if an application is upgraded or re-installed. In this event, the user is unable to find the required help information, usually at a critical time!

9.8 Fonts

Font information for Windows PCs is stored within the registry in the format of registry keys.

Fonts are vital to programs such as Microsoft Word that allow the user to use different typefaces (fonts) within their documents. Fonts are also used in the user interface of programs.

If a user or a program uninstalls a font incorrectly then this will create a font error within the registry. You can view the installed fonts in Control Panel or in the Windows registry. The font list can be found in the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Fonts

The implementation of fonts in Windows has evolved over time. In earlier versions of Windows TrueType fonts could be added with the use of a tool called FontReg. See this Microsoft support note describing the use of this utility. http://support.microsoft.com/kb/133732

Regular registry scans will keep the registry font information up to date.

10 RegEdit and Beyond

As we keep mentioning in this ebook, the registry needs to be edited with care.

The registry edit tool that Microsoft includes with Windows is called RegEdit and this provides a basic way to manage the registry. However the software is not meant to be 100% user friendly with easy to change settings. The intention is for the vast, vast majority of users to leave the registry well alone.

Our view at the Registry Tool Center is by all means, use an automatic registry cleaner but avoid manual edits of the registry that will get you into trouble.

Now, with all that said and warnings given, in this section we will show you a selection of the expert level tools you can download (for free) to help you manually edit the registry.

As we mentioned, Microsoft did not make RegEdit super easy to use and this has opened up an entire market for software developers to create registry utilities to help search, backup, restore and compare registry settings.

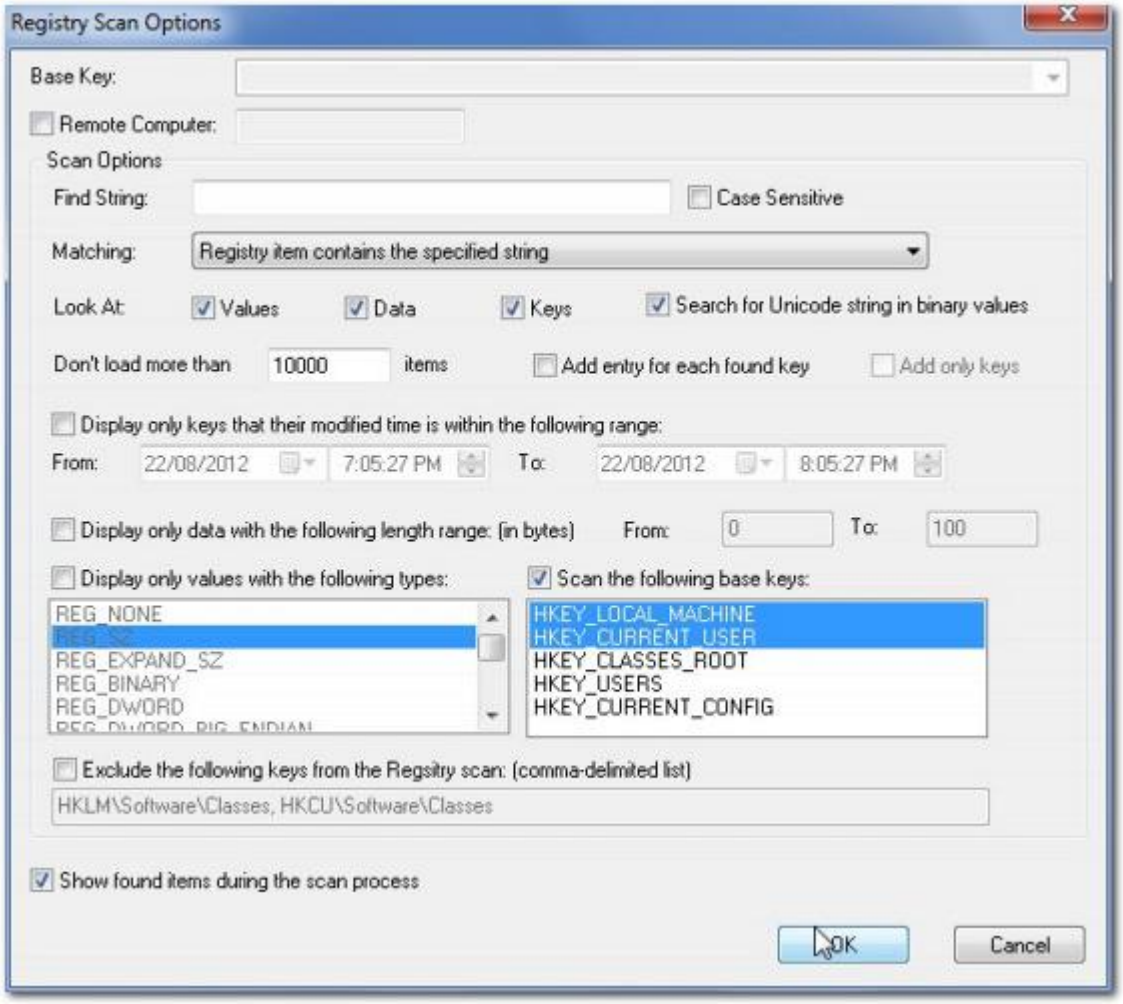
Let's have a look at a few of the advanced registry utilities available at the Registry Tool Center.

10.1 Reg Scanner

A useful registry utility Reg Scanner 1.90 allows you to scan the registry based on specific criteria and with a double click jump to the value within Regedit, saving time and effort getting to the information you need.

There are a wide range of options including scanning of the registry on a remote computer, using a wide range of matching options for a scan and displaying data within a specific size in bytes.

The Registry Scan options within Reg Scanner are displayed in the screen shot below.



The Reg Scanner software has the following features:

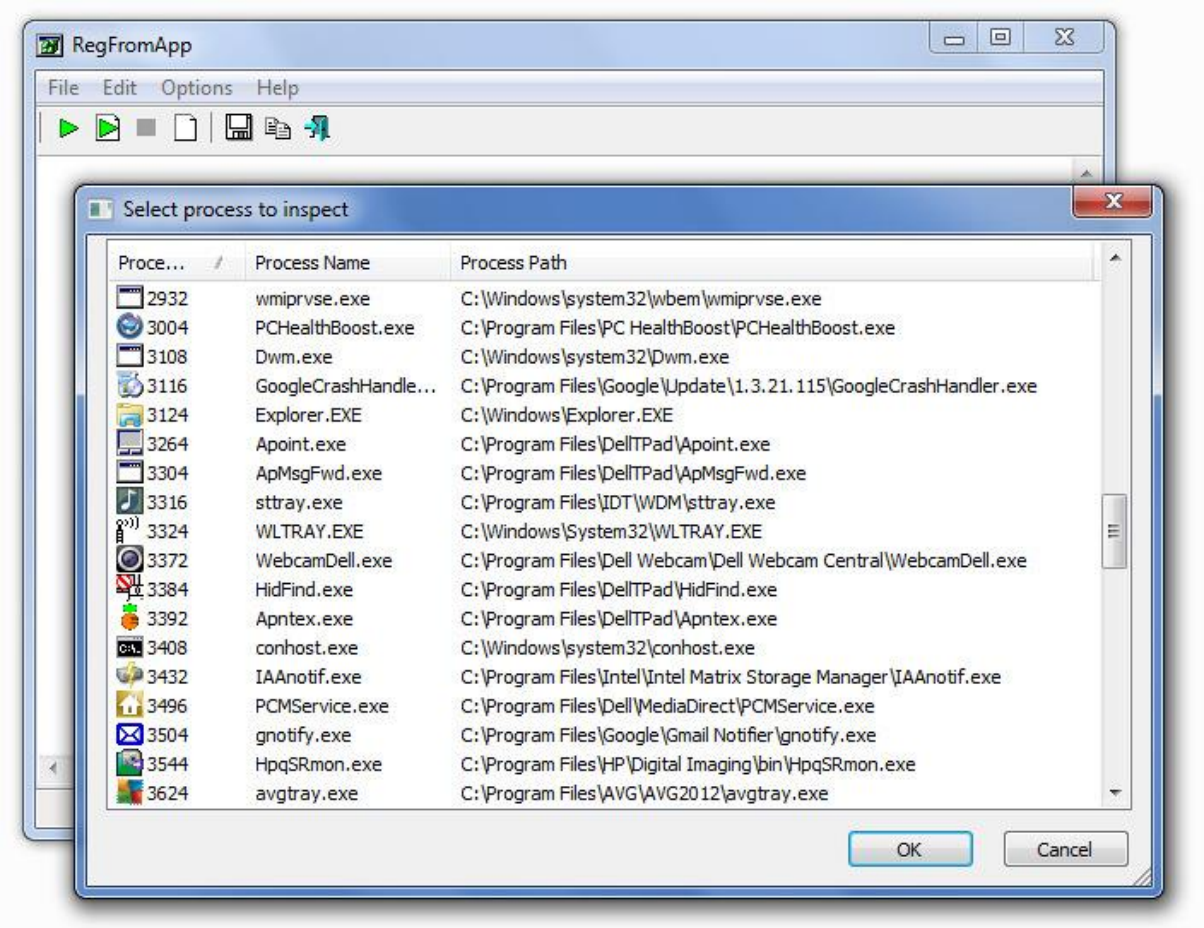
- Find a registry value by a wide range of means e.g.; value type, data length and modified date of key
- All search results are displayed at once, no need for the F3 to cycle through the results
- Searches can be case sensitive
- Enhanced search presentation with registry key displayed instead of Regedit dialog box of 'Scanning the Registry'.
- Delete selected keys or values. Warning! This is an advanced feature for expert users. Manual deletion of Registry keys could result in your PC or software on your PC displaying errors.
- Use the command line option with Regedit
- Export values to a .reg file for use within Regedit
- Find a unicode string within a binary value
- The program runs as a stand-alone executable, no installation required, just run
- Easy to use interface
- 100% free of spyware, Adware or Viruses
- Compatible with Windows NT/2000/XP/2003/Vista/7 (separate version for 64 bit PC)

10.2 RegFromApp

Select an application on your computer and then use RegFromApp to monitor changes to the Registry made by the application. A standard RegEdit file will be created of the changes and this can be imported into the Registry as required.

Once you have started RegFromApp you are able to select a process to monitor. Every time the process writes a value into the Registry, the written value will be shown in the main window of RegFromApp in .reg file format.

See the screen shot below to choose an existing process once you have loaded RegFromApp.



Once the values have been displayed, it is then your choice to either cut and paste the value into another Registry file or choose 'Save As' to save the changes into a .reg file.

RegFromApp has 2 display modes. The default display mode is 'Show Last Modified Values' where the last modified changes to the Registry are shown. The second display mode is 'Show Original Values' where the original Registry values, before any changes, are displayed.

RegFromApp features are shown below:

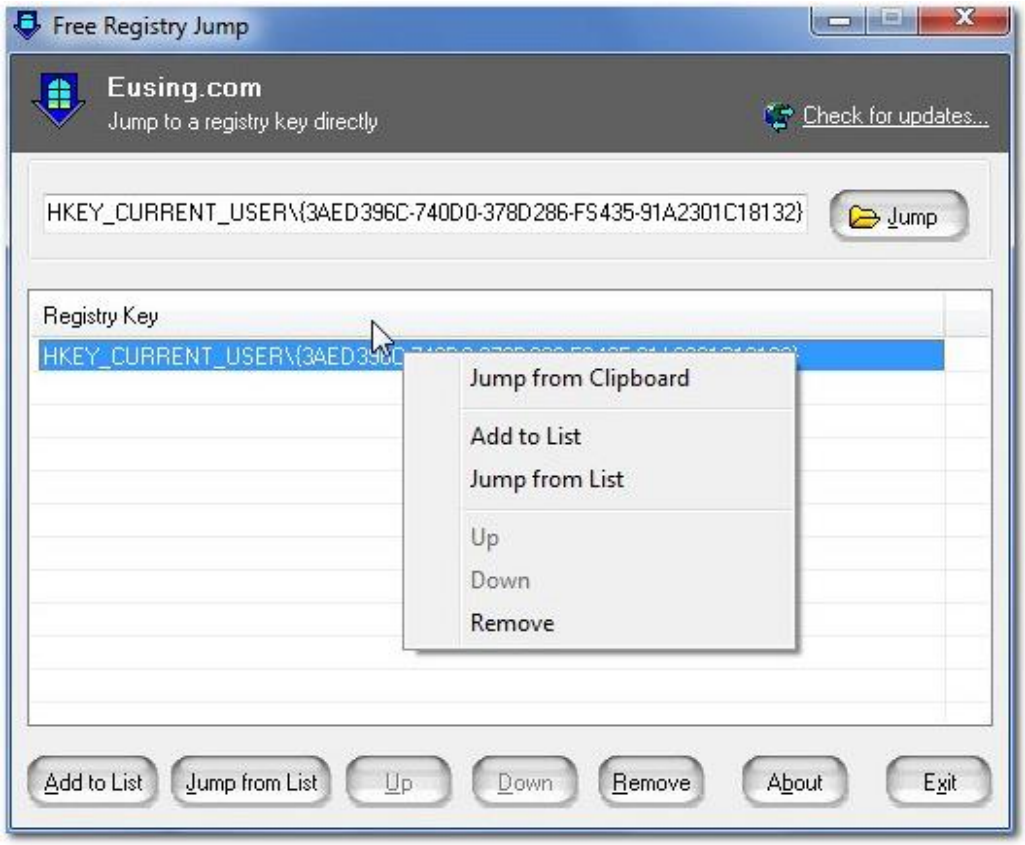
- 32 bit and 64 bit versions
- Monitor effect of application processes on Registry
- 2 display modes: Show Last Modified Values' and 'Show Original Values'
- Cut and paste registry changes to another registry file
- Save registry changes to a .reg file
- Upload changes to the Registry from a saved .reg file
- Command line support
- Works on both Windows desktops and Windows servers
- 100% Spyware FREE, does not contain any Spyware, Adware or Viruses
- Platforms: Windows XP/Vista/7 and Windows Server 2000/2003/2008

10.3 Registry Jump

Registry Jump 1.0 helps you jump directly to a particular registry key without manually navigating the paths using RegEdit. This program is a time saver if you edit the registry manually on a regular basis.

Registry Jump enables you to jump to a certain registry key or value instantly. You can just enter the registry key or value you wish to jump to. You also can manage and directly jump to frequently accessed registry keys.

Registry Jump accepts root keys in standard (e.g. HKEY_LOCAL_MACHINE) and abbreviated form (e.g. HKLM). It also can jump to a key you've copied to the clipboard.



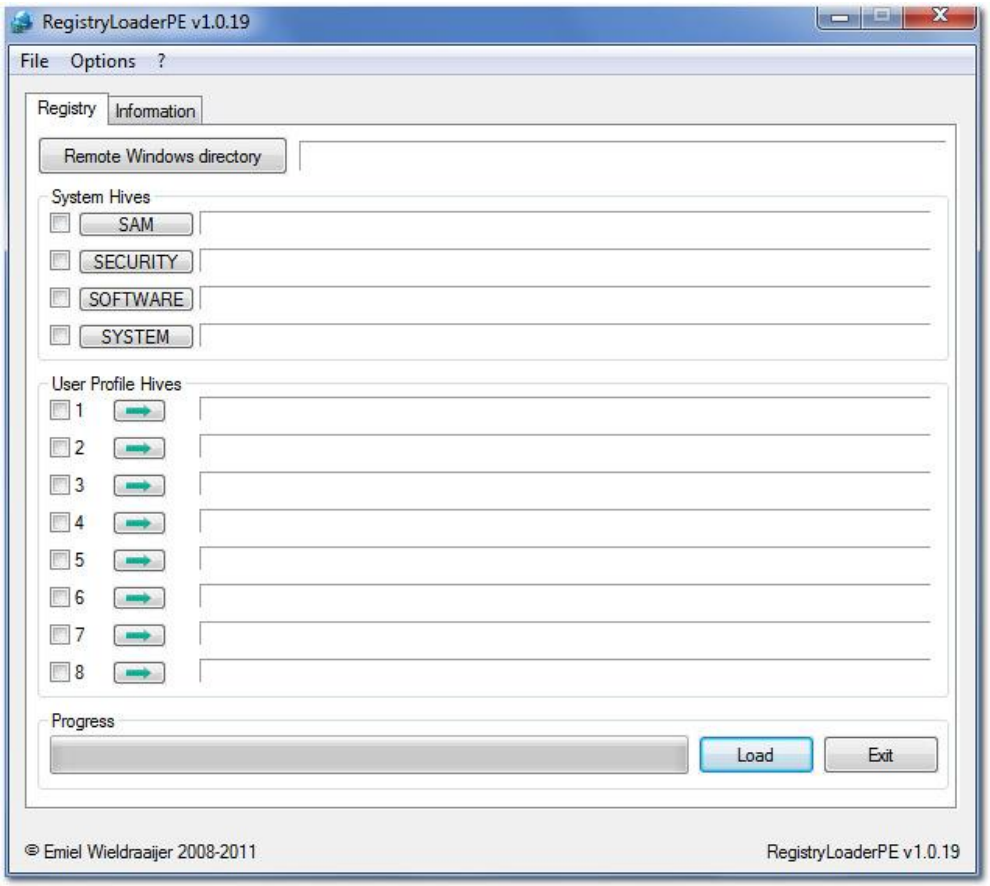
A summary of Registry Jump features are shown below:

- Directly jump to a registry key
- Directly jump to a saved registry key in Windows RegEdit
- Directly jump to a registry key copied to the clipboard
- Accepts root keys in standard (e.g. HKEY_LOCAL_MACHINE) and abbreviated form (e.g. HKLM)
- A simple, well designed user interface
- Tray Icon – easy-to-use
- Completely portable – copy to a USB stick and run on any PC with no installation
- 100% Spyware FREE, NOT contain any Spyware, Adware or Viruses
- Platforms: Windows 9x/Me/NT/2000/XP/2003/Vista/7

10.4 Registry Loader PE

Load registry files from offline systems, very useful if you are trying to recover a system that cannot boot and the registry needs to be edited to resolve the issue. An example problem would be a corrupt hardware driver.

RegistryLoaderPE only works for Windows NT/2000/XP/2003/2008/7 registry hives. The software will not work on Windows 95 / 98.



The software works with the Microsoft Windows Preinstallation Environment (Windows PE) which is based on the Windows Vista kernel.

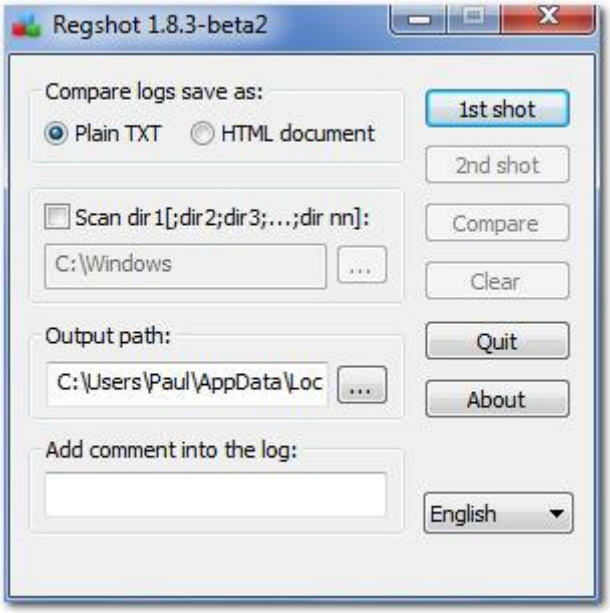
Microsoft defines Windows PE as "Windows PE is a modified version of the Windows operating system that is designed to support installing Windows and troubleshooting and recovering an installation that can no longer boot."

BartPe plugin creation from within the program is possible.

10.5 RegShot

RegShot is a registry compare utility that helps users take a snapshot of the registry before and after running a process or an application. This assists in identifying changes to the Registry as the result of a particular activity or program.

The changes identified by RegShot can be output as text or html and will contain a list of all modifications between the two versions. See the main screenshot below:



The software is also able to scan multiple folders if you delimit them with ';'. Sub-folders will also be scanned for changes.

A field is provided to add a comment into the log to assist with the recording the comparison process.

A summary of RegShot features are shown below:

- Compare two snapshots of registry and identify the differences
- Save reports in text or html format
- Utility available to convert version 1.8.2 hives to 1.8.3 version

- Works for 32- bit and 64 bit version of Windows
- Program does NOT contain any Spyware, Adware or Viruses
- Platforms: Windows 9x/Me/NT/2000/XP/2003/Vista/7

11 Registry Tips and Tricks

In this section we provide a number of tips and tricks when using the registry. This should help with any registry related activities you plan to undertake. Of course, make sure you have a current registry backup before you make a change. Here are our top 5 suggestions:

11.1 Edit the Registry with no need to restart the PC

This is a Windows XP tip for making a change to the registry and rather than having to reboot the PC in order for the change to take effect you can have the change take place without a reboot.

1. Make sure you have saved all your work.
2. Press Alt, Ctrl + Del to bring up the Task Manager.
3. Choose the 'Processes' tab, highlight 'Explorer.exe' and click on 'End Process'. You will see all windows and desktop icons disappear except for the Task Manager.
4. Choose the 'File' menu in Task Manager.
5. Select 'New Task… Run' and type in 'explorer'.
6. Explorer will be re-launched along with your updated registry settings.

11.2 Who needs 2 Naming Conventions?

The legacy of MS –DOS lives on.

DOS required all files to adhere to what is known as the 8.3 naming convention. This means, all files had 8 characters in their name and 3 characters for an extension. So a Word document might be called 'letter.doc' in DOS but it could not be called 'new_letter.docx' as the file name and extension are both too long.

When it came to later versions of Windows, the naming convention was far more flexible. However, there was a need for backward compatibility with MS-DOS so each file would effectively have 2 file names; an 8.3 file name and a Windows XP file name.

This means there is an overhead for Windows to manage 2 names for each file. If you are running Windows XP and have no need to run DOS based programs on your computer then you could use this registry edit to remove the DOS 8.3 naming from your Windows PC.

1. Open RegEdit (Click on Start, choose Run and type 'regedit')
2. Within the registry find the following key:
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem
3. Change the value of the NtfsDisable8dot3NameCreation key to '1'

The DOS 8.3 naming convention is now removed from your Windows XP PC.

11.3 Not all Memory is Created Equal

Your computer may have 1Gb or more of memory in RAM and that may seem enough to handle all the basic tasks you need your computer to complete. In order to help even further, Windows XP is configured to swap information out of RAM to a 'Page File' which is a slower type of virtual memory. However, if important operating system information is swapped to a page file the PC can slow down.

In order to keep your PC running as fast as possible, you can force Windows XP to keep important information in RAM and not move it to the slower page file.

1. Open RegEdit (Click on Start, choose Run and type 'regedit')
2. Within the registry find the following key: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Session Manager\Memory Management.
3. Change the DisablePagingExecutive value to '1'

11.4 Unwanted Baggage

Dynamic Link Libraries (DLLs) are used by many programs running in Windows. They are typically small sized files that have data used by one or many programs. The DLLs are loaded into memory as they are needed but they are not unloaded from memory when the associated program is closed.

This can leave a number of DLLs in memory that take up space and slow the performance of the computer. This is more likely if a computer is not switched off for a number of weeks and programs are loaded and unloaded throughout the day.

1. Open RegEdit (Click on Start, choose Run and type 'regedit')
2. Within the registry find the following key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer.
3. Create a new key named 'AlwaysUnloadDLL' and set the default value to equal '1.'

11.5 Increase Internet Browsing Speed

When you browse the Internet, details of frequently accessed websites are held on your PC. This helps speed up your access to these websites as you do not have to wait to find them on the Internet, your PC already has the details and can provide them to you right away.

This information is kept for a finite period of time. You can increase the space for this information so more website information is retained for longer. Just follow these adjustments on your Windows XP computer.

1. Open RegEdit (Click on Start, choose Run and type 'regedit')

2. Within the registry find the following key: 'HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters'
3. Create the following DWORD values:

   CacheHashTableBucketSize = 1

   CacheHashTableSize = 180

   MaxCacheEntryTtlLimit = ff00

   MaxSOACacheEntryTtlLimit = 12d

4. Exit RegEdit and restart your computer.

12 Further Reading

The following information is taken from www.amazon.com and is reproduced for your further research and reference.

12.1 Microsoft Windows Registry Guide, Second Edition

From the Publisher

Expert guidance and ready-to-use files and templates for modifying and managing the Windows registry.

Key Book Benefits

Learn how to customize and manage the Windows registry—and get your systems running the way you want Apply best practices for backing up, managing, modifying, restoring, and troubleshooting the registry Get 100+ registry files and templates plus a complete eBook on the CD

Get the in-depth information you need to modify—and seamlessly manage—the Windows registry. Written for IT professionals and power users, this vital resource reveals little-known registry techniques, tricks, tips, and secrets to make your job easier. Understand the inner workings of the Windows operating system—and use the registry to get Windows Server 2003 and Windows XP to run the way you want, on a single desktop or across the network.

You'll learn how to pinpoint registry settings and script registry changes, deal with registry permissions, use Windows Installer, and map Tweak UI settings. Also, find best practices for how to back up, restore, and maintain registry settings with confidence. The CD includes 100+ registry files for customizing operating system appearance and behavior, and the complete eBook.

You'll learn how to: Apply best practices to back up, restore, manage, and modify the registry Customize group and system policies to manage multiple PCs and users remotely Track down registry settings and script changes Optimize server services, including network connections and authentication Deploy user profiles and Microsoft Office program settings Configure security services, including Windows Firewall, templates, and service pack features Troubleshoot the registry—resolving common problems and corruption issues

About the Author

Jerry Honeycutt, MVP for Windows, is a popular author with more than 25 books to his credit, including Microsoft Windows Desktop Deployment Resource Kit. In addition, he is a columnist for Windows XP Expert Zone and Microsoft TechNet.

Paperback: 608 pages

Publisher: Microsoft Press; 2nd edition (September 14, 2005)

Language: English

ISBN-10: 0735622183

ISBN-13: 978-0735622180

12.2 Mastering Windows XP Registry

Expert Advice for Windows XP Power Users

Created for Windows power users and anyone who aspires to be one, *Mastering Windows XP Registry* provides focused, practical coverage of Windows' most important—and most challenging—element: the registry. Inside, you'll learn to customize Windows XP, optimize the network, and avoid scores of potential disasters, all by working with registry settings. If you're a power user, a system administrator, programmer, or consultant, this guide is absolutely essential.

Coverage includes:

- Understanding registry keys and data types
- Applying the secrets of the most important registry keys
- Adjusting the Windows GUI through registry settings
- Using the registry in networking
- Optimizing performance by editing registry settings
- Working with registry tools
- Recovering from disasters
- Eliminating unwanted keys, entries, applications, and files
- Taking advantage of the registry in your own programs
- Tracking registry changes made by applications
- Navigating registry entries

About the Author

Peter D. Hipson is an author, consultant, and teacher. When not writing computer books, he can often be found teaching computer science at the local college, where he says he "ruins the lives of hundreds of unsuspecting college students every year."

Paperback: 672 pages

Publisher: Sybex; 1st edition (May 15, 2002)

Language: English

ISBN-10: 0782129870

ISBN-13: 978-0782129878

12.3 Windows 7 Tweaks

Written by bestselling author and the creator of tweaks.com Steve Sinchak, this unique guide provides you with the ultimate collection of hidden gems that will enable you to get the most out of Windows 7.

Packed with more than 400 pages of insider tips, the book delves beneath the surface to reveal little-known ways to tweak, modify, and customize Windows 7 so you can get every ounce of performance from your operating system.

Regardless of your experience with tweaking your system, you'll find fascinating and fun tips and tricks for getting under the hood of Windows 7 that will allow you to optimize its appearance, speed, usability, and security.

Bestselling author and creator of tweaks.com shows you how to tweak, modify, customize, and take complete control of the new Windows 7 operating system

Unlocks hidden gems for optimizing the appearance, speed, usability, and security of the Windows 7 OS

Shows you how to customize boot and login screens, supercharge your network and online speed, get rid of features that drive you nuts, fine tune your User Account Protection, and more

So roll up your sleeves and take off your gloves so you can take total control over your Windows 7 OS!

About the Author

Steve Sinchak has repeatedly been honored with Microsoft's MVP (Most Valuable Professional) award. He manages several Web sites geared toward computer enthusiasts, most notably tweaks.com and wingeek.com. Steve is the author of *Hacking Windows Vista* and *Hacking Windows XP*, both from Wiley.

Paperback: 408 pages

Publisher: Wiley; 1 edition (December 2, 2009)

Language: English

ISBN-10: 0470525916

ISBN-13: 978-0470525913

12.4 Windows Registry Forensics

Harlan Carvey brings readers an advanced book on Windows Registry. The first book of its kind EVER -- *Windows Registry Forensics* provides the background of the Registry to help develop an understanding of the binary structure of Registry hive files. Approaches to live response and analysis are included, and tools and techniques for post mortem analysis are discussed at length.

Tools and techniques will be presented that take the analyst beyond the current use of viewers and into real analysis of data contained in the Registry.

The Windows Registry is perhaps one of the least understood sources of digital evidence on a Windows system. Unfortunately, bad guys have used specific locations in the Registry to remain persistent on systems a lot longer than many

analysts actually realize. I think that what most analysts don't realize is that the Registry is an excellent source of both direct and indirect artefacts.

Don Weber, a friend and fellow IBM alum who's now with InGuardians, was on an engagement where he found that the bad guys were actually storing executable files in binary Registry values. His find makes me wonder how many times this has occurred but not been "seen" because no one was looking.

Intrusions aside, I've also dug into the Registry to perform malware detection. As sometimes happens, malware files will change and avoid detection, but as with malware such as Conficker, some Registry artefacts remained relatively stable across the family. The same has been true for the examinations I've performed that involved Zeus, or Z-bot. Understanding this has allowed me and others to determine that malware was on a system, when multiple AV scans were negative.

Finally, the Registry contains a wealth of time stamped data, that when taken in context, can be extremely valuable to an analyst.

About the Author

Harlan Carvey's interest in computer and information security began while he was an officer in the U.S. military, and a student at the Naval Postgraduate School, earning his MSEE. After leaving military service, he began working in the field of commercial and government information security consulting, performing vulnerability assessments and penetration tests. While employed at one company, he was the sole developer of a program for collecting security-specific information (i.e., Registry entries, file information, configuration settings, etc.) from Windows NT systems during vulnerability assessments.

Paperback: 248 pages

Publisher: Syngress; 1 edition (February 7, 2011)

Language: English

ISBN-10: 1597495808

ISBN-13: 978-1597495806

12.5 Windows 7 Annoyances: Tips, Secrets, and Solutions

Windows 7 may be faster and more stable than Vista, but it's a far cry from problem-free. David A. Karp comes to the rescue with the latest in his popular Windows Annoyances series.

This thorough guide gives you the tools you need to fix the troublesome parts of this operating system, plus the solutions, hacks, and timesaving tips to make the most of your PC.

- Streamline Windows Explorer, improve the Search tool, eliminate the Green Ribbon of Death, and tame User Account Control prompts

- Explore powerful Registry tips and tools, and use them to customize every aspect of Windows and solve its shortcomings
- Squeeze more performance from your hardware with solutions for your hard disk, laptop battery, CPU, printers, and more
- Stop crashes, deal with stubborn hardware and drivers, fix video playback issues, and troubleshoot Windows when it won't start
- Protect your stuff with permissions, encryption, and shadow copies
- Secure and speed up your wireless network, fix networking woes, make Bluetooth functional, and improve your Web experience

--Jon Jacobi, *PC World*

"To use Windows is to be annoyed -- and this book is the best way to solve any annoyance you come across. It's the most comprehensive and entertaining guide you can get for turning Windows into an operating system that's a pleasure to use."

About the Author

David A. Karp is the author of twelve power-user books, including the bestselling Windows Annoyances series of books and O'Reilly's eBay Hacks. David's books are available in ten languages, and can be found under the short legs of tables around the world.

David is the founder of Annoyances.org, one of the most respected and popular computer help sites on the Interwebs. He writes for PC Magazine, but they're curiously reluctant to publish photos of his bicycle. Notable recognition has come from PC Computing, Windows Magazine, the San Francisco Examiner, and the New York Times.

Paperback: 722 pages

Publisher: O'Reilly Media; 1 edition (May 11, 2010)

Language: English

ISBN-10: 0596157622

ISBN-13: 978-0596157623

13 Registry Cleaning Suggestions

We have gathered a selection of articles explaining how to maintain the registry on your PC and the benefits you will see in your computer's performance.

13.1 What is the Purpose of a Registry Cleaner?

If you have ever heard of a tool called a registry cleaner or heard someone mention that they are going to clean up the registry on their computer, then you may not know what that means. However, cleaning the registry of your Windows PC is a great way to keep the performance of your computer in good shape and prevent your computer from becoming slow.

Actually, cleaning the registry on a computer can solve multiple problems. Here are a few of the things that a registry clean up can do for your computer:

- Speed your computer up
- Create more space on your computer
- Remove unneeded, unwanted or unnecessary files or information from your computer
- Fix corrupted or broken files on your computer

By running a registry clean up on your computer, you can do a lot of good for your computer. Not only can you boost the speed of your computer but you can also free up space on your computer as well. A registry clean up can also resolve errors and repair broken or corrupt files which may be preventing your computer from running properly.

As you can see, the main purpose of a registry cleaner is to tidy up the registry of a computer. The cleaner will eliminate files and information that the computer does not use or need. In addition to this, the cleaner will also "tidy up" files and pieces of information that need to remain on the computer.

For instance, if a file is damaged, the cleaner can repair the file so that the file works properly. A registry cleaner is a great tool for the general upkeep of your computer and should be used on your computer on a regular basis in order to keep your computer running effectively and efficiently.

13.2 How to Extend the Life of your Computer

With all of the things that people use computers for these days, it is no surprise that over time they begin to deplete. However, if you do not take steps to maintain the life and quality of your computer then your computer will slow down in what seems like no time at all.

As technology continues to advance, it is likely that your computer will seem much slower than new computers. In order to avoid purchasing a new computer much sooner than necessary, it is important to take care of your computer. This is not different to your car. If you do not take care of your car, it is going to breakdown on you at the worst possible moment!

Extending the life of your computer may seem like a daunting task, but it truly is not. One of the easiest and most effective ways of extending the life of your Windows computer is to run a scheduled registry clean on a regular basis. Depending on how often you use your computer and how many programs you install and uninstall on the PC this could be anywhere from a daily registry scan to once a month. All of this can be automated for you by registry cleaning software.

You may be wondering "how does a registry clean up extend the life of my computer?" Here are a few of those ways:

- Any unnecessary files or information in your computer's registry will be removed.
- Any broken or corrupted files will be removed from the registry.
- Duplicated files or information will be eliminated from the registry.

As a result of this, your computer will end up having more disk space than it did prior to the registry clean up. After the registry clean up, your computer will also run faster due to the removal of any files or information that was no longer needed. The registry clean-up will also fix any broken or corrupted files which means that there will be less errors or problems with the operation of programs.

A registry clean up will leave your computer with faster speeds, more space, and improved overall performance. All of these things will help to extend the life and the quality of your computer which means that you will be able to enjoy your computer for longer.

At the Registry Tool Center we recommend registry tools for expert users as well as the average PC user. We find that an automatic, scheduled registry scan works for both experts and regular users alike. Click here to find out more.

13.3 Is a Registry Cleaner a Virus Remover?

Technology is a wonderful tool. However, there are those individuals who like to abuse technology instead of use it for the greater good. These individuals are usually behind those annoying viruses unwittingly downloaded from the internet. Unfortunately, viruses are all too common and can be picked up from places that you thought were secure. Fortunately, these viruses can all be taken care of and eliminated from your computer.

You probably know that a registry cleaner is a scan that takes place in the computer's registry and removes unnecessary or unused files and other pieces of information from the computer's registry. For instance, if a file has become damaged or corrupted, then a registry scan will repair the damages to the file in order to repair it back to normal.

With this in mind, many people are curious as to whether or not a registry cleaner scan can remove a virus from a computer. To answer this question, it is possible that a virus could be removed from a computer during a registry clean up scan. However, it is not guaranteed and it all depends on where the virus has been placed.

A registry cleaner scan could scan through the entire registry of the computer and not catch on to a virus if the file containing the virus is not damaged or does not send out any sort of signal that the registry has been tampered with.

A virus could be removed from a computer using a registry cleaner if:

- The file containing the virus has become damaged or corrupted.
- The file containing the virus sets off some sort of signal that the file has been tampered with or contains foreign information.

A registry cleaner should not be used as a virus cleaner or virus protection since it is not a dependable virus remover.

If you are looking to protect your computer from viruses or remove a virus from your computer, you need to rely on a program that is made specifically for virus protection since this will be the best way to detect and remove a virus.

Summary: An actual virus protection program will be more dependable when detecting and removing a virus from a computer.

14 Online References

There is a tremendous amount of information available on the Internet regarding the registry. We have gathered some of the most relevant links and references we could find.

14.1 Microsoft

The following links will give you a great start to exploring the registry links on the Microsoft website.

- Microsoft – Windows Registry
- How to Modify the Windows Registry
- Microsoft Windows XP – Registry Editor overview
- Microsoft Windows XP – Using Regedit.exe

14.2 About.com

This is a great website to get tips and short answers to common problems. We have selected some of the best links related to the registry.

- What is the registry?
- What is a registry key?
- What is a registry value?
- What is a registry hive?
- What is the registry editor?
- How to backup the registry in Windows XP
- How to restore the registry in Windows XP
- How to delete registry keys in Windows XP
- How to backup the registry in Windows 7
- How to restore the registry in Windows 7
- How to delete registry keys in Windows 7
- How to backup the registry in Windows Vista
- How to restore the registry in Windows Vista
- How to delete registry keys in Windows Vista

14.3 Forensic Analysis

The Windows registry plays a key role for computer forensic investigators to reveal the activities that have been happening on a PC

- ForensicsWiki website focused on computer forensics - registry article
- Edith Cowan university research paper (PDF) on Windows 7 registry
- Forensic Focus - a site for computer forensic professionals – Windows registry article
- Registry forensic analysis tool