Using Retake

The most important asset on your computer is the information, or *data*, you create and store there. Over time, this data grows in size and value. The storage devices where you keep this information, although typically quite reliable, are still vulnerable to a wide range of environmental and human factors that can damage or destroy all or part of the data stored there.

Valuable and vulnerable disk organizational structure information is also stored in various places on a hard drive. This includes the boot sector, partition tables, directories, the FAT (file allocation table), and other structural components. These structural components are used by Windows to find data on the drive, organize it, and so on. If any one of these components is damaged or destroyed, you will not be able to access the data you've stored on the drive.

Let's take a closer look at one of these structural components, the file allocation table. The FAT, your drive's roadmap, points to the locations where your files are physically stored on the drive. Files can either be stored in contiguous locations or scattered in pieces in different places. Since files are not always stored contiguously, the FAT information becomes even more indispensable than if files were stored one after another, end to end. If a drive's file allocation table becomes corrupt or scrambled (such as may be caused by a virus), your computer will be unable to find and assemble all the pieces of your files. This is true even if all the files' data still exists.

Protected Volume Files (The Ultimate Backup Protection)

Safe & Sound's Retake utility allows you to create backup sets in protected volume files, which is the safest and preferred type of backup, and is unique to Safe & Sound. A *protected volume file* is a sectioned off portion of the drive, sometimes called a logical drive. Retake's protected volume files have some very special characteristics that let Retake reconstruct backup files sector by sector, even if the drive's standard FAT is damaged or completely lost. In fact, files can be largely reconstructed even if large parts of the drive are unreadable or erased.

The protected volume file also includes enough information in each directory entry to completely reconstruct a file's entire directory tree even if all its parent nodes are erased.

Retake provides internal redundancy in the protected volume file backups you create. It does this by marking each sector of each file that it backs up with identifying information about the sector's contents and the file that sector belongs to. Each sector in a protected volume file contains enough information to allow files to be reconstructed from their individual sectors.

Why You Should Make Regular Backups With Retake

Your data is very valuable and costly to recreate. This means that making frequent or even mirror backup copies of the important data on your drives is *crucial*. A *mirror* backup copy is always identical to the original information on the source drive.

Retake automates the back-up process, doing the time-consuming and repetitive work for you. It lets you decide which types of files to back up, how often to save them, and where you want the backup set located (on the same drive, another local drive, or on a shared network drive). With Retake, you can create mirror backup sets that are, at any given time, an exact replica of the files you've selected to back up on the source drive. You can also specify a short time delay in the backup, or back up manually by copying files to the backup set on your drive if you prefer.

All forms of data storage are susceptible to losing the information they hold. The most common types of data storage—hard drives, 3.5-inch disks, ZIP disks or SyQuest tapes—are often called *permanent storage* (thus differentiating them from the volatile storage in your computer's RAM, random access memory). Permanent storage means the information remains intact even when you turn off your computer. Permanent storage does not mean *eternal* storage.

Many things can cause the data on disks, tapes or drives to become garbled or lost: hardware malfunctions, worn out media, electrical storms, excessive heat, static electricity, magnets, loose cable or power cord connections, and so on. CD discs, though durable, can become scratched enough to damage their data. Human actions can also cause lost data, such as deleting the wrong folder or formatting the wrong drive. Even a well-designed application can sometimes cause its own files to become corrupt.

With so much at risk, you have everything to gain by letting Safe & Sound's Retake utility automatically make backup copies for you. You simply decide what information is important to you, how you want it to be backed up, and where you want the backup copy to be stored. Retake takes care of the rest!

How Retake Creates Automatic Backups

When you select to have Retake automatically create a backup set for you, it creates the first backup set while you are stepping through the Retake Wizard. Thereafter, while the Enable Automatic Backup option is selected, it continues to update your backup set at the time delay you've specified. If you chose to make Mirror backups, Retake updates your backup set at the same time that you resave the original source files.

If you select a write-behind delay longer than zero seconds (a Mirror backup), Retake updates the backup set at any time after the specified time delay when your PC is idle. This allows Retake to work in the background so that it does not interrupt the work you are doing. This is a good option to use with the protected volume file backup type since it eliminates any speed loss due to more frequent disk accesses and larger file sizes associated with the protected volume file backup type.

Defining Your Backup Strategy

After you decide which backup type you want to use (either a protected volume file or a directory backup set), the most important questions you must answer when defining your own backup strategy are:

- Where Will You Store The Backup Set?
- What Files are Important to You? (which files must be backed up?)
- How Often Should You Or Retake Make Backups?

Where Will You Store the Backup Set?

If the survival of your business depends upon your PC being up and running at all times (and if money is not an object), the ultimate way to protect the data on your PC would be to set up a redundant PC with identical sized drives. This backup PC's only job would be to mirror the data on your primary PC. It would be waiting in the wings should your first PC fail for any reason. And if that happened, you could simply switch your work to the second PC while the first one is repaired.

Often money is a consideration in deciding where you'll store your backup sets. The least expensive way of making backups has traditionally been to copy data to 3.5-inch disks, though this is the most labor intensive way of storing backups because it requires you to switch disks by hand.

In today's computer marketplace, you may discover that it is as cost effective to acquire a separate backup hard drive where you can keep a current mirror backup copy of one or more other drives that you use on your PC.

In addition, you may want the backup copy to be stored at a remote location, for increased protection. As long as Retake can access a logical drive mapped on your PC, it can store the backup set there. That is, the backup set can be stored on a shared network drive.

Note You can use the Map Network Drive command, available by Right-clicking My Computer, to assign (map) a drive letter to a location on a network drive. This makes that location a "logical drive" on your PC. For more details, see your Windows online Help.

Even if you cannot invest in another drive or disks for storing your backups, you can still create a backup copy of your data on the same drive. This offers the least protection should that drive fail, but the potential for data recovery is increased by having two sets of your most important information stored there. It is further enhanced if you select the protected volume file backup type, which allows recovery in many circumstances even with the drive physically damaged.

Note If your data usually resides on a server, you can make a local copy so you can access data even when the server goes down.

What Files Are Important to You?

Retake automatically selects files that are typically important to include in a backup set. However, you can select other files or types of files to include in your backup set.

In addition, you can create multiple backup sets of data for particular purposes. Each of these backup sets can be created when and where you specify. They can each include exactly the files or types of files that you choose. For example, you might create individual backup sets for each of your clients if you produce data for clients that is stored on your computer, such as advertising layouts, graphic images, books, or accounting data.

How Often Should You or Retake Make Backups?

The more recent your backup set, the happier you'll be if your PC does encounter a problem that compromises the data on your primary drives. However, you may want to keep the default Write-behind Delay of 20 minutes to give you time to recover a previous version of a file if you ever need to.

Note Save early, save often. While working in applications, you can almost always press CTRL-S to save your work as you go. The more often you save your work, the less you have to lose at any given point in time. You may also want to be sure the auto-save option is selected in your applications for more frequent backups.

Creating a Backup Set

Creating a backup set, either manually or to be updated automatically, in Retake is very easy. Retake's default choices should work fine, though you may want to add additional folders or file types to your backup list.

To create a backup set:

1. Click the Start button and do one of the following:
   - Choose the Safe & Sound command from the Start menu and click the Retake button.
   - Choose the Programs > Safe & Sound > Retake command.

   The Retake Wizard window appears.
2. Click the Next > button while the Create a New Backup Set radio button is selected.

   The Retake Wizard (Backup Type) windowappears.
3. Select whether to back up to a Protected Volume File or a Directory. Then click Next >.
4. Specify the target destination where the backup set will be created and click Next >.
5. Click the Settings button if you want to customize any of the settings for this backup set.

   The Retake Properties window appears.

   If you are not yet familiar with file types and want to see them, you can open My Computer or Windows Explorer, choose the Options command from the View menu, and click the File Types tab.
6. Click Apply to apply changes to a tab of information. Then click OK when you are done.

   If you want to make a backup set manually, deselect the Enable Automatic Backup check box.

   If you've selected your 3.5-inch drive or a removable media drive that provides less space than you'll need for your backup set, you'll need to follow the instructions on the screen and switch disks or tapes when instructed.
7. Click Next >, enter a name for your backup volume, and click Next > again.
8. Click OK.

Restoring Files From a Backup Set

If you encounter a problem with the information on your drive, you can restore one or more of the files in your Retake backup sets.

Note Unless you create a backup set that contains the entire contents of a drive, you should never drag and drop, or copy and paste, the contents of a Retake backup set's <drive letter> folder directly into your drive's window. Though the folder names match between a Directory type backup set and the folders on the drive, the contents of the two are most likely very different. By default, Retake only backs up files it considers essential and important, such as INI, TXT, RTF, DOC, and WRI files. It backs them up using the original hierarchical directory structure from the source drive. You will know where to restore each file, if you need to, based on its location in the backup set. It does not automatically back up your application files or DLL files, nor does it back up your Windows directory without your explicit instructions to do so.

To restore a backup set:

1. Open Windows Explorer or My Computer and open the backup set.

   If the backup set is a Directory type backup, the folder name (by default) is Backup_1, Backup_2, and so on. If the backup set is a Protected Volume File, it is located at the same level as your physical drives.

2. Find the files you want to restore and use Drag and Drop or Copy/ Paste to copy files from your backup set to the location where you want them.

Modifying an Existing Backup Set

To modify a backup set:

1. Click the Start button and do one of the following:
   - Choose the Safe & Sound command from the Start menu and click the Retake button.
   - Choose the Programs > Safe & Sound > Retake command.
2. Select the backup set to modify and click the Properties button.
3. Change the settings and click OK when you are done. Then click Finish.

Deleting a Backup Set

If you created a Retake backup set as a protected volume file, you cannot delete it in My Computer or Windows Explorer. You can *only delete the protected volume file* using Retake.

If you created a Retake backup set as a directory, you should still delete it using Retake; however, you can delete the backup directory via My Computer or Windows Explorer.

To delete a backup set:

1. Start Retake.
2. Click the Next > button while the Delete a Backup Set radio button is selected.
3. Select the backup set to delete and click Finish. Then click Yes to confirm the deletion.

Repairing and Rebuilding a Backup Set

If you encounter a problem with the backup set itself, you can repair (CHKVOL.EXE) or rebuild (REBUILD.EXE) it. For example, if your computer crashes while the backup is being created or updated automatically, the contents of the backup may be incomplete or damaged. Retake automatically checks the integrity of your backup when you start Windows. If it is damaged, Retake's Repair Utility starts and asks if you want to repair the backup set.

Repair

Rebuild

Repairing a backup set:

1. Start Safe & Sound's Retake utility and click Next > while the Repair or Rebuild Backup Set radio button is selected.
2. Click the Repair button and click Next > if you can see the backup set in My Computer or Windows Explorer, but the information is somehow damaged. For example, if a backup was not finished due to a power outage or computer crash.
3. Select the backup set that you want to check and click Start.

Retake Repair Utility (CHKVOL.EXE) command line options:

You may also execute the Retake Repair Utility using command line parameters.

chkvol.exe [volume filename [=volume label]...]

- /m remounts after checking
- /f autofix error
- /s start checking volumes

Rebuilding a Backup Set:

Note: Performing a Rebuild is a time-consuming process because Retake searches your entire system to find all backup sets and files that are stored there. Use Rebuild to restore a volume that can no longer be mounted because of corruption. You can also use Rebuild to restore backups from a previous installation of Retake.

1. Start Safe & Sound's Retake utility and click Next > while the Repair or Rebuild Backup Set radio button is selected.

2. Click the Rebuild button and click Next > if you can no longer see the backup set (for example if the protected volume file is no longer visible in My Computer or Windows Explorer).

3. Select the drives that contain a protected volume file you want to restore. Then click Next >.

It is recommended that you select a logical drive when searching for volumes to rebuild. If for some reason you cannot access your logical drives, select a physical drive instead.

Wait while the Restore utility searches the selected drives for protected volume files or backup directories. If it finds a protected volume file, it displays a message that it found a protected volume file with its creation date and time and asks if you want to Save As, Ignore, or Ignore All.

Save As
Saves this found volume and continues to search for others. When you select this option, rebuild displays the saved volume on the window marked "Volumes located." An LED type graphic indicator shows the status of the volume. A yellow light indicates that all files in the backup set have not been found. If the searching bar graph is active, be patient, rebuild is still trying to complete the set. A green light indicates that all files in the backup set have been located.

Ignore
Ignores this found volume and continues to search for others.

Ignore All
Ignores this found volume and skips searching for other volumes. If you have selected to save a found backup previously, It continues to search the drive to complete the backup set.

Tip: Make sure to keep track of the creation date and time of when you create the backup volumes. This is the only way rebuild can you show

4. Click the Save As button and select where you want the restored volume file to be placed. Then click Save. Retake displays all saved volume sets on the "Volumes located" list.

5. Rebuild will continue searching for other volumes and files for the backup sets that you chosen to save. Rebuild will prompt you each time it finds a backup set. If it has already found the backup set that you want, select "Ignore All" to skip searching for other volumes.

Tip: You can highlight a found set and press the DEL key to delete any of the found volume set listed on the "Volume located" list while Retake is searching for more volumes.

6. After Rebuild finishes rebuilding all backup sets that it found and saved, it displays the "Volume to reactivate" list. Select the volume(s) you want reactivated by checking off the checkbox to the left of the volume name.

Recovering a backup set manually:
An alternate way to recover an existing backup is to edit the RETAKE.INI file. This is recommended if the following criterias are met:

1. You know the name of the backup volume filename or backup folder.

2. You are familiar with using a text editor and editing files.

3. Use the following format:

[Volumes]

filename=volume label

[filename]

type=1 for backup folder/2 for backup volume

drive=x:

mount=yes/no

For example: If you have an existing backup volume file called backup001.vol located in the folder called C:\MY BACKUP, use the following setting steps to restore the backup:

1. Edit RETAKE.INI
2. Add the following line under the [Volumes] section:

   [Volumes]

   c:\my backup\backup001.vol=This is my backup
3. Add a section using the backup volume filename:

   [c:\my backup\backup001.vol]

   type=2

   drive=d:

   mount=yes

Retake Wizard Window

The Retake Wizard window steps you through the process of creating a backup set. It starts by offering you these options:

Create a New Backup Set
Select this radio button and click Next > to create new backup set (either a protected volume file or directory type backup).

The Retake Wizard (Backup Type) window appears.

Modify an Existing Backup Set's Properties
Select this radio button and click Next > to modify the backup set you select.

Delete a Backup Set
Select this radio button and click Next > to delete the backup set you select.

Repair or Rebuild Backup Set
Select this radio button and click Next > to repair or rebuilt a backup set.

Cancel
Click the Cancel button to close Retake without finishing the backup procedure.

< Back
Click the < Back button to step backward through the Retake Wizard windows.

Retake Wizard (Backup Type) Window

This Retake Wizard window offers these options:

Protected Volume File
The Protected Volume File is the preferred backup type. A protected volume file is a sectioned off portion on the drive. It has special characteristics to ensure that even if organizational structures, such as the file allocation table on the drive is corrupted or lost, or the data becomes scrambled, the files in the backup set can be reconstructed. Retake stores extra information (in each sector for each file and also in a separate directory) to provide this level of protection. For details, see the “Protected Volume Files (The Ultimate Backup Protection)”.

Note You can copy files into a protected volume file manually using My Computer or Windows Explorer to add them to your backup set and instantly protect them.

There are two drawbacks to using a protected volume file backup type. The first drawback is that three percent more storage space is required for the extra information that will be used to reconstruct the files in the event of a problem. The second drawback is that a protected volume file is slightly slower because it has to manipulate more information in more areas on the disk and more disk accesses are required. This is a marginal performance degradation, which you can eliminate by also selecting a Write-behind Delay of seconds or minutes.

Directory
The Directory backup type makes another copy of the files and directories selected for backup in a different location. This type of backup creates no performance drain on the system and it’s simple to manage the backup area. You can use My Computer or Windows Explorer to cut or copy files in or out of the backup location or delete the files. The drawback of selecting a directory backup type is that the files are no more protected than if you had created a backup copy yourself.

Retake Properties Window

This Retake Properties window offers these options:

Backup Type
Displays the currently selected backup type (Protected Volume File or Directory).

Enable Automatic Backup
While this check box is selected, Retake automatically updates this backup set as you update the files it contains based on the time delay you specify.

Name of Backup Set
If you are saving this backup set to a non-Windows 95/98 or NT drive (such as to a UNIX server on your network) be sure to follow the 8.3 naming convention for this name.

Write-behind Delay
Select the Mirror (0) write-behind delay if you want your backup set to remain in constant synchronization with the original files as you change them. Select a write-behind delay in seconds or minutes if you want your backup to be created during times when your PC is idle starting at any time after the time delay you select.

Note A write-behind delay in seconds or minutes is recommended if you are using the protected volume file backup type and want to eliminate the slight speed reduction caused by extra disk accesses in more locations on the drive.

Protected Volume Drive Letter
The drive letter you want to use for the Protected Volume File backup set. (*Available only for backup sets stored as a Protected Volume File*).

Keep Deleted Files For
Select how long you want the backup set to keep files whose original counterparts have been deleted from your system.

Limit Size of Backup Volume
Drag the slider left to reduce the backup volume size limit or right to increase the backup volume size limit.

Backup Drive
Drive and Directory Folders appear in the Backup Drive list so you can select any of the ones you want to add to your backup set. Click folders to open and close them. Click the check boxes to place a check mark beside the drives or directories that you want to back up.

Document Types
You can select groups of files that you want to include in your backup set by selecting their file type. The file type, such as TXT (for a text file), indicates the file's purpose. Retake displays a list of all the registered file types in Windows 95/98. The file types with check marks show the types of files that will be included in your backup set.

Retake obtains its list of registered file types from Windows. You can view or add registered file types in My Computer or Windows Explorer.

If you are not yet familiar with file types and want to see them, you can open My Computer or Windows Explorer, choose the Options command from the View menu, and click the File Types tab.

In the Options dialog box you will be able to examine the list of the registered file types on your system. These are the file types that will be available to you in Retake. You can add new registered file types in the Options dialog box to make them available to Safe & Sounds' Retake utility the next time you run it.

Many file types are standard, such as BMP and PCX which are used by paint applications like Microsoft Paint, or TIF which is a standard file type used for TIF or TIFF graphic image files.

Each application's documents typically have a file type (which may or may not be registered in Windows). For example, Microsoft Word document files may be stored using the registered file types of DOC, RTF or TXT, depending upon the file type you select when saving the document.

Note You can also view file types directly in My Computer or Windows Explorer. Choose the Options command from the View menu, click the View tab, and make sure the HIDE MS-DOS FILE EXTENSIONS FOR FILE TYPES THAT ARE REGISTERED check box is deselected. Registered file types are also listed in the File Types tab in the Options dialog box. The other place where file types appear is in the Save As dialog box of Windows applications.

Address Space

The sum total of all possible memory addresses available at a given time. This is 4 GB (gigabytes) on a 386 or later PC in protected mode.

Launch Pad

The Launch Pad is a window where you can place application and document icons so you can conveniently access them.

Benchmarks

A benchmark is a standardized task that tests various devices for measurements, such as speed.

BIOS

The BIOS (or Basic Input/Output System) contains buffers for sending information from an application to the hardware device, such as a printer, where the information should go.

Buffers

A buffer is a temporary storage location for information being sent or received.

Bytes

A byte is eight bits of information composed of zeros and ones, one of which may be a parity bit. Most character sets, such as ASCII, use one byte to represent each character (letter, number, or special symbol).

Cache

A cache is part of the computer's memory used to temporarily store recently accessed information. A cache is designed on the premise that recently used information may be needed again soon. Keeping information available in cache reduces the time it takes for an application to obtain the information again.

Cluster

A cluster is a unit of storage allocation usually consisting of four or more 512-byte sectors.

Conventional Memory

Conventional memory is the first 640 K (kilobytes) of RAM (random access memory).

CPU (Central Processing Unit)

The “brain” of your computer. This is main computer chip that controls all activity that takes place on a computer.

Diagnostics

Diagnostics are tests run to detect faults in a computer system. Diagnostics tests are run to detect faults before they become serious problems so the faults can be corrected.

Directories

Directories are locations within a volume on a drive where you can store files or subdirectories. In Windows, directories are equivalent to folders that appear on the desktop in a drive window.

Discardable Memory

Discardable memory is memory used by an application that it has marked as discardable. Windows can reallocate the discardable memory to a different application if it needs to.

DLLs (Dynamic Link Libraries)

A DLL is an executable code module that can be loaded on demand and linked at run time. DLLs can be shared among multiple applications and independently updated, transparent to the applications. DLLs can also be unloaded when they are no longer needed.

DMA (Direct Memory Access)

DMA is a fast method of moving information from a storage device or LAN interface card directly to RAM which speeds processing time. DMA is direct memory access by a peripheral device that by-passes the CPU to save time.

Expanded Memory

DOS running on the Intel 80286, 80386, or 80486 family of computers can only address one megabyte of memory at one time. Expanded memory is the memory located between the base memory (either 512 K or 640 K) and one megabyte. Expanded memory is reserved by DOS for housekeeping tasks, such as managing information that appears on the screen.

Extended Memory

Memory above one megabyte in 80286 and higher PCs. Extended memory can be used for RAM disks, disk caches, or Windows, but it requires the CPU to run in a special mode (protected mode or virtual real mode).

FAT (File Allocation Table)

The FAT is an index to the location where all the information is stored on a floppy disk or hard drive. The FAT is extremely important because the system uses it to store and retrieve files containing information.

GDT (General Description Table)

The GDT is a table that is basic to the operation of protected mode. This table contains data structures (descriptors) that describe various regions of memory and how they may be accessed. Windows uses the GDT for system devices. *See LDT.*

Global Heap

The Global Heap is the general pool of memory available to Windows applications.

GPF (General Protection Fault)

An error condition caused by an application when it attempts to perform an operation not allowed by the operating system. Windows uses GPFs to determine and control the state of the currently executing application. GPFs that are unexpected by Windows cause a system error message to appear.

HMA (High Memory Area)

The HMA is the first 64 K of extended memory. If you use DOS 5.0, you can save memory by loading DOS into the HMA. Do this by adding the DOS=HIGH setting to your CONFIG.SYS file and restarting your PC.

Interrupt

A temporary suspension of a process caused by an event outside that process. More specifically, an interrupt is a signal or call to a specific routine. Interrupts allow peripheral devices, such as printers or modems, to send a call to the CPU requesting attention.

I/O (Input/Output) Device

An I/O device is any piece of computer hardware that can exchange information with the CPU. Examples of I/O devices include network cards, printers, speakers or other sound devices, or devices connected to the serial or parallel ports of your PC such as external modems.

Kernel

The Kernel is the part of a computer operating system that performs basic functions such as switching between tasks.

LDT (Local Descriptor Table)

The LDT is a secondary data structure table that contains additional information about various regions of memory and how they can be accessed. Windows uses the LDT for programs.

Linear Memory

Linear memory is the currently defined address space of the system that Windows uses to allocate memory to Windows applications.

Local Heap

The Local Heap is a region of memory allocated for local use by an application.

Locked Memory

Locked memory is memory used by an application that cannot be relocated or discarded by Windows.

Mapping

Mapping is the process of assigning physical memory (RAM) to a particular linear address range.

Mode Switch

A mode switch is a transition made by the CPU when changing from one mode of operation to another. For example, switching from real or protected mode, or a transition between different levels of protection. *See Ring 0, 1, 2, 3*.

Modules

A module is a device driver loaded by Windows.

Paging

The process of saving information stored in RAM to the swap file on the system hard drive so Windows can make the RAM available at a different linear address.

Parallel Port

The parallel port is a connector on the back of your PC and on some peripheral devices. With the appropriate driver software installed and a parallel cable connected to the parallel ports on your PC and a peripheral device, the two can communicate with each other. Parallel transmissions have no EIA standard, but most equipment follows a quasi-standard called the Centronics Parallel Standard.

PCI (Peripheral Component Interconnect) Bus

The PCI Bus is a local motherboard specification (that provides connector slots on the motherboard for installing peripheral cards). The PCI Bus, designed by Intel, offers a high performance, peripheral component level interface to the CPU bus.

Physical Memory

Physical memory is the RAM (Random Access Memory) installed in your PC. *See Random Access Memory (RAM).*

Protected Mode

A mode of operation of 80286 or later CPUs which allows access to more than 1 MB of memory.

RAM (Random Access Memory)

RAM (Random Access Memory) is also called physical memory. It is installed in your PC on SIMMs (Single Inline Memory Modules) or DIMMs (Dual Inline Memory Modules). RAM is volatile, extremely high-speed storage used by your computer for processing information.

Real Mode

A mode of 80286 or later CPUs, where the CPU operates substantially like an older 8086 CPU and can address directly only 1 MB of memory.

Resources

Resources are objects that Windows and its applications can use, such as the buttons on the screen that you can click.

Ring 0, 1, 2, 3

Different levels of protection in protected mode, where programs having varying degrees of freedom of operation. Ring 0 (zero) is least protected and has direct access to all hardware in the system.

Sector

A sector is a pie-shaped portion of a hard disk. A disk is divided into tracks and sectors. Tracks are complete circuits and are divided into sectors. Under DOS, a sector is 512 bytes.

Serial Port

A serial port is an input/output port (connector) that allows the transmission of information out at one bit at a time, as opposed to parallel which transmits eight bits, or one byte at a time.

Swap File

The swap file is created by Windows on the system hard disk. It uses the swap file to copy information stored in part of the linear address space so it can reallocate the RAM used at that location to another linear address space.

Swapping

Swapping is the process of saving to disk or restoring from disk the contents of RAM so that the RAM can be used elsewhere in linear memory.

System Resources

System resources are a series of data structures kept by Windows. System resources are managed by the Windows User and GDI programs and maintain information about objects that appear on your screen.

32BDA (32-Bit Disk Access)

32BDA is a process in Windows where the device driver that accesses the disk runs entirely as a 32-bit program at Ring 0 (zero).

32BFA (32-Bit File Access)

32BFA is a process in Windows where the DOS file operations are controlled by a program, or set of devices, that operate entirely as 32-bit programs at Ring 0 (zero).

Unlocked Memory

Unlocked memory is physical memory that Windows can copy to the swap file on disk, and whose linear address can be changed whenever Windows chooses.

UMB (Upper Memory Block)

The UMB is the area in memory between 640 K and 1 MB that have RAM mapped into them by memory managers, such as Network Associates' Netroom or MemMaker. *See Expanded memory.*

V86 Mode (Virtual 8086 Mode)

V86 mode is a mode of operation of 80386 or later CPUs where programs, originally designed to run in real mode, can run as sub-programs to a protected mode control program or operating system.

Video Memory

Video memory, called VRAM, is physical memory installed on your PC's video card that is used for displaying information on the screen.

Virtual Memory

Virtual memory is the amount of memory that exists either as physical memory (RAM) or on the hard drive (in the swap file). When a part of memory that is located in the swap file is accessed by an application, Windows reads the information into RAM.

VMs (Virtual Machines)

Virtual machines (also called Virtual DOS machines or VDMs) are created in Windows 95/98 when you open a MS-DOS Prompt window. The VDM is a software emulation of a separate computer, offering all the services that the DOS application expects of a PC.

VxDs (Virtual Device Drivers)

VxDs are used in Windows to communicate with all physical hardware in the system. This prevents any application from having direct access to a piece of hardware. Instead, it communicates only through the VxD for that hardware.

Windows Registry

The Windows 95/98 Registry file contains user, application, and computer-specific configuration information in a central location that was kept in various .INI files in Windows 3.1. The Registry contains settings that determine how your computer runs.