Optimizing and Protecting Hard Drives - Chapter # 9

Amy Hissom

Key Terms

antivirus (AV) software — Utility programs that prevent infection or scan a system to detect and remove viruses. McAfee Associates' VirusScan and Norton AntiVirus are two popular AV packages.

backup — An extra copy of a file, used in the event that the original becomes damaged or destroyed.

boot sector virus — An infectious program that can replace the boot program with a modified, infected version of the boot command utilities, often causing boot and data retrieval problems.

buffer — A temporary memory area where data is kept before being written to a hard drive or sent to a printer, thus reducing the number of writes to the devices.

chain — A group of clusters used to hold a single file.

child, parent, grandparent backup method — A plan for backing up and reusing tapes or removable disks by rotating them each day (child), week (parent), and month (grandparent).

cross-linked clusters — Errors caused when more than one file points to a cluster, and the files appear to share the same disk space, according to the file allocation table.

defragment — To "optimize" or rewrite a file to a disk in one contiguous chain of clusters, thus speeding up data retrieval.

differential backup — Backup method that backs up only files that have changed or have been created since the last full backup. When recovering data, only two backups are needed: the full backup and the last differential backup.

disk cache — A method whereby recently retrieved data and adjacent data are read into memory in advance, anticipating the next CPU request.

disk cloning — *See* drive imaging.

disk compression — Compressing data on a hard drive to allow more data to be written to the drive.

disk imaging — *See* drive imaging.

drive imaging — Making an exact image of a hard drive, including partition information, boot sectors, operating system installation, and application software to replicate the hard drive on another system or recover from a hard drive crash. Also called *disk cloning* and *disk imaging*.

DriveSpace — A Windows 9x utility that compresses files so that they take up less space on a disk drive, creating a single large file on the disk to hold all the compressed files.

encrypting virus — A type of virus that transforms itself into a nonreplicating program in order to avoid detection. It transforms itself back into a replicating program in order to spread.

file virus — A virus that inserts virus code into an executable program file and can spread whenever that program is executed.

firewall — Hardware or software that protects a computer or network from unauthorized access.

fragmentation — The distribution of data files on a hard drive or floppy disk such that they are stored in noncontiguous clusters.

full backup — A complete backup, whereby all of the files on the hard drive are backed up each time the backup procedure is performed. It is the safest backup method, but it takes the most time.

hardware cache — A disk cache that is contained in RAM chips built right on the disk controller. Also called a buffer.

incremental backup — A time-saving backup method that only backs up files changed or newly created since the last full or incremental backup. Multiple incremental backups might be required when recovering lost data.

infestation — Any unwanted program that is transmitted to a computer without the user's knowledge and that is designed to do varying degrees of damage to data and software. There are a number of different types of infestations, including viruses, Trojan horses, worms, and logic bombs.

logic bomb — Dormant code added to software that is triggered by a predetermined time or event.

lost allocation units — *See* lost clusters.

lost clusters — File fragments that, according to the file allocation table, contain data that does not belong to any file. The command CHKDSK/F can free these fragments. Also called lost allocation units.

macro — A small sequence of commands, contained within a document, that can be automatically executed when the document is loaded, or executed later by using a predetermined keystroke.

macro virus — A virus that can hide in the macros of a document file.

memory-resident virus — A virus that can stay lurking in memory even after its host program is terminated.

multipartite virus — A combination of a boot sector virus and a file virus. It can hide in either type of program.

non-memory-resident virus — A virus that is terminated when the host program is closed. Compare to memory-resident virus.

polymorphic virus — A type of virus that changes its distinguishing characteristics as it replicates itself. Mutating in this way makes it more difficult for AV software to recognize the presence of the virus.

SMARTDrive — A hard drive cache program that came with Windows 3.x and DOS and can be executed as a TSR from the Autoexec.bat file (for example, Device=Smartdrv.sys 2048).

software cache — Cache controlled by software whereby the cache is stored in RAM.

stealth virus — A virus that actively conceals itself by temporarily removing itself from an infected file that is about to be examined, and then hiding a copy of itself elsewhere on the drive.

Trojan horse — A type of infestation that hides or disguises itself as a useful program, yet is designed to cause damage at a later time.

VCACHE — A built-in Windows 9x 32-bit software cache that doesn't take up conventional memory space or upper memory space as SMARTDrive did.

virus — A program that often has an incubation period, is infectious, and is intended to cause damage. A virus program might destroy data and programs or damage a disk drive's boot sector.

virus signature — A set of distinguishing characteristics of a virus used by antivirus software to identify the virus.

worm — An infestation designed to copy itself repeatedly to memory, on drive space or on a network, until little memory or disk space remains.

Review Questions

1.) What is the difference between a cross-linked cluster and a lost cluster? What can cause them?
Cross-linked clusters are errors caused when more than one file points to a cluster and the files appear to share the same disk space, according to the file allocation table. Lost clusters are file fragments that, according to the file allocation table, contain data that does not belong to any file. The command CHKDSK/F can free these fragments. Also called lost allocation units.

2.) What are two tools that Windows 9x/Me uses to check for cross-linked and lost clusters?
ScanDisk and Chkdsk

3.) What are two tools that Windows 2000/XP uses to check for cross-linked and lost clusters?
Chkdsk and ScanDisk

4.) Of the two tools used by Windows 2000/XP to check for cross-linked and lost clusters, which tool is available from the Recovery Console?
Chkdsk

5.) Explain two disadvantages of data compression.
1. Longer disk access time
2. Performance risks

6.) What file system is necessary to use if a volume is to be compressed under Windows 2000?
FAT32

7.) What is the name of the drive compression utility used by Windows 95/98?
DriveSpace

8.) How is a hardware cache different from software cache?
Hardware cache is built right into the controller circuit board and the software cache is a cache program stored on the hard drive like other software, and is usually locked into memory when the computer is booted.

9.) Name and define the method DOS used to speed up disk access?
Buffering. A buffer is a temporary memory area where data is kept before being written to a hard drive or sent to a printer, thus reducing the number of writes to the devices.

10.) How is disk cache accomplished in Windows XP? Windows 9x/Me? Windows 3.x with DOS?
Windows XP – uses automated disk caching as an inherited Windows component.
Windows 98/ME – Has a built-in 32-bit, protected-mode software cache called VCACHE, which is automatically loaded without entries in Config.sys or Autoexec.bat.
Windows 3.x – Used SmartDrive, a 16-bit, real-mode software cache utility.

11.) What is the difference between an incremental backup and a differential backup?
Differential backups don't consider whether other differential backups have been performed. Instead, they compare data only to the last full backup. Incremental backups compare data to the last backup even if the last backup was itself an incremental or full backup.

12.) What versions of Windows support incremental backups? Differential backups?
Incremental Backups – Windows NT/2000/XP and Windows 9x/Me
Differential Backups - Windows 98 and Windows NT/2000/XP

13.) What is the Windows Scripting Host utility used for, and what is the command line to execute it?

The Windows Scripting Host (WSH) uses Windows commands to execute scripts written in a scripting language such as VBScript or Jscript. It is also good for making backups. To execute it you must type ***wscript.exe filename*** in the run dialog box, substituting the name of the script file for ***filename***, or double-click the desktop icon. You can also make a script file run as a scheduled task.

14.) Explain the child, parent, grandparent method of making backups?

Child backup – Should have an on-site storage location and be performed daily in which to keep four daily backup tapes, to be rotated each week. You should label the four tapes Monday, Tuesday, Wednesday, and Thursday. A Friday daily (Child) backup is not made because on Friday you make the parent backup.

Parent Backup – Should have an off-site storage location and be performed weekly on Friday. You keep five weekly backup tapes, one for each Friday of the month, and rotate them each month. You should label the tapes Friday 1, Friday 2, Friday 3, Friday4, and Friday 5.

Grandparent Backup - Should be performed monthly on the last Friday of the month and be stored in an off-site location such as a fireproof vault. 12 tapes should be kept for each month and rotated each year. These 12 tapes should be labeled January, February, and so on.

15.) What must you do before you can use the Windows Backup utility on a Windows XP Home Edition PC?

Close all files before performing the backup because this utility only backs up files that are not currently in use.

16.) What process is used to replicate a hard drive to a new computer? When might you use this process, and what are some examples of software designed to perform it?

The process is called disk cloning, disk imaging, or drive imaging. Examples of software used to perform this process are Drive Image by PowerQuest, ImageCast by Innovative Software, and Norton Ghost by Symantec Corp.

17.) Why should you create a disaster recovery plan? What type of information would you include in it?

Because the damage from a disaster will most likely be greater than if you had made and followed disaster plans. Always record your regular backups in a table along with information pertaining to folders or drives backed up, the date of the backup, the type of backup, and a label identifying the tape, disk, or other media.

18.) Define and explain the differences between viruses, worms, logic bombs, and Trojan horses.

A virus is a program that replicates by attaching itself to other programs. The infected program must be executed for a virus to run. A worm is a program that spreads copies of itself throughout a network or the Internet without a host program. A Trojan horse is a third type of computer infestation that, like a worm, does not need a host program to work; rather it substitutes itself for a legitimate program. Most Trojan horses cannot replicate themselves, although there have been some exceptions. A logic bomb is a dormant code added to software and triggered at a predetermined time or by a predetermined event.

These four types of infestations differ in the way they spread, the damage they do, and the way they hide.

19.) Where can viruses hide?

In the boot sector program, in an executable program (.exe, .com, or .sys) or in a word processing document that contains a macro.

20.) What is the best way to protect a computer or network against worms?
By using a firewall.

21.) What is the best way to determine if an e-mail message warning about a virus is a hoax?
Check the Web sites of virus software manufactures or a search engine by using the name of the virus or virus warning

22.) Name three ways that a virus can hide from antivirus software.
1. by changing its distinguishing characteristics (its signature).
2. By attempting to mask its presence.
3. by not keeping the antivirus software up to date with virus definitions.

23.) Are boot sector viruses limited to hard drives? Explain.
No, because one of the most common ways a virus spreads is from a floppy disk used to boot a PC. On a floppy disk, a boot sector virus hides in the boot program of the boot sector.

24.) What is the most likely way that a virus will get access to your computer?
Via the Internet

25.) List 3 third-party utility programs used to support hard drives.
1. Norton Utilities by Symantec
2. Partition Magic by PowerQuest
3. SpinRite by Gibson Research

26.) List at least 4 causes of hard drive problems.
1. Viruses
2. Fragmented files and lost or cross-linked clusters
3. Long spans of inactivity while leaving the computer on
4. High humidity

27.) List 3 hardware components to check or examine if a hard drive does not boot.
1. Drive data cable
2. Drive adapter cord
3. Field replaceable units
4. Hard drive itself
5. Motherboard
6. Power supply

28.) What items must be intact in order for DOS or Windows to be able to access a hard drive using the FAT file system? List them in the order in which they are accessed.
1. The partition table
2. The boot record
3. The FAT
4. The root directory
5. The system files
6. Data and program files

29.) What error message might appear if the partition table is damaged? The boot record? The FAT? The system files?
Partition table - “Invalid drive or drive specification”
Boot record – “Invalid media type”, “Non-DOS disk”, or “Unable to read from drive C”
FAT – “Sector not found reading drive C, Abort, Retry, Ignore, Fail?”, “Bad sector”, and “Sector Not Found”

System files – “Non-system disk or disk error…” Invalid system disk…”, and “Command file not found”

30.) If a file header is lost or corrupted and an application needs that header to read the file, how can you recover the contents of the file?

By treating the file as an ASCII text file.

31.) Explain how lost clusters are caused and what can you do to recover from them.

They are caused when a program cannot properly close a file it has opened. Scandisk can be used to recover them.

32.) If an erased file is not found in the Recycle Bin, what command can you use at a command prompt to attempt to recover the file?

The unerase or undelete command

33.) Before you call the manufacturer’s technical support for a hard drive during installation, what should you have in hand?

1. Drive model and description
2. Manufacturer and model of your computer
3. Exact wording of error message, if any
4. Description of the problem
5. Hardware and software configuration for your system