Windows Data Recovery

Recovering lost data can be as simple as opening the Windows Recycle Bin, or it might require spending hundreds of dollars on specialized data recovery software or services. In the worst-case scenario, you might even need to send your drive to a data recovery center. Several factors affect the degree of difficulty you might encounter in recovering your data, including

- How the data was deleted
- Which file system was used by the drive on which the data was stored
- Whether the drive uses magnetic, optical, magneto-optical, or flash memory to store data
- Which version of Windows or other OS you use
- Whether you already have data-protection software installed on your system
- Whether the drive has suffered physical damage to heads, platters, or circuit board

The Windows Recycle Bin and File Deletion

The simplest data recovery of all takes place when you send files to the Windows Recycle Bin (a standard part of Windows since Windows 95). Pressing the Delete key or clicking the Delete button when you have a file or group of files highlighted in Windows Explorer or My Computer sends files to the Recycle Bin. Although a file sent to the Recycle Bin is no longer listed in its normal location by Windows Explorer, the file is actually protected from being overwritten. By default, Windows 95 and above reserve 10% of the disk space on each hard disk for the Recycle Bin (removable-media drives don't have a Recycle Bin). Thus, a 100GB drive reserves about 10GB for its Recycle Bin. In this example, as long as less than 10GB of files has been sent to the Recycle Bin, a so-called deleted file is protected by Windows. However, after more than 10GB of files has been sent to the Recycle Bin, Windows allows the oldest files to be overwritten. Thus, the quicker you realize that a file has mistakenly been sent to the Recycle Bin, the more likely it is you can retrieve it.

To retrieve a file from the Recycle Bin, open the Recycle Bin, select the file, right-click it, and select Restore. Windows lists the file in its original location and removes it from the Recycle Bin.

If you hold down the Shift key when you select Delete or press the Delete key, the Recycle Bin is bypassed. Retrieving lost data at this point requires third-party data recovery software.

Recovering Files That Are Not in the Recycle Bin

The Recycle Bin is a useful first line of defense against data loss, but it is quite limited. As you learned in the previous section, it can be bypassed when you select files for deletion, and files stored in the Recycle Bin are eventually kicked out by newer deleted files. Also, the Recycle Bin isn't used for files deleted from a command prompt or when an older version of a file is replaced by a newer version.

Products such as Norton UnErase (part of the Norton Utilities and Norton SystemWorks) are necessary if you want to retrieve files not in the Recycle Bin. However, the effectiveness of Norton UnErase and how you should use it depends on the version of Windows you use and the file system used by your drives.

Norton UnErase and Norton Protected Recycle Bin—Win 9x/Me

With Windows 9x/Me, which use the FAT file system, retrieving data from a drive that doesn't have Norton Utilities installed isn't difficult. However, installing Norton Utilities before you start to delete files that you might want to retrieve makes it even easier. You can run Norton UnErase from the bootable CD included in current versions, and run it as a command-prompt program if you don't

have it already installed and need to retrieve erased data. You will need to provide the first letter of each file you want to unerase.

Caution

Do *not* install data-recovery software to a drive you are attempting to retrieve data from because you might overwrite the data you are attempting to retrieve. If you are trying to recover data from your Windows startup drive, install another hard disk into your system, configure it as a boot drive in the system BIOS, install a working copy of Windows on it, boot from that drive, and install your data recovery software to that drive. If possible, install a drive large enough (at least 10GB or larger) so that you have several GB of free space on it for storing recovered data.

However, if you have already installed Norton Utilities, you probably have the Norton Protected Recycle Bin on your desktop in place of the regular Recycle Bin. Compared to the Windows standard-model Recycle Bin, the Norton Protected Recycle Bin protects files that have been replaced with newer versions and files that were deleted from a command prompt. To retrieve a file stored in the Norton Protected Recycle Bin, open the Recycle Bin, select the file you want to retrieve, right-click it, and select Retrieve to put it back in its original location.

Alternatively, you can start the Norton Unerase Wizard from the Norton Utilities menu. You can search for recently deleted files (these files are stored in the Recycle Bin), all protected files on local drives (also stored in the Recycle Bin), and any recoverable files on local drives. When you select the last option, you can narrow down the search with wildcards or file types and specify which drives to search. You must supply the first letter of the filename for files that were not stored in the Recycle Bin; you can also see which files were deleted by a particular program. To undelete a file with the Unerase Wizard, select the file, provide the first letter of the filename if necessary, click Quick View to view the file (if your file viewer supports the file format), and click Recover to restore the file to its original location.

With Windows 9x/Me, you can search both hard and removable-media (floppy, flash memory) drives for lost files, although the Recycle Bin works only for hard drives.

Norton UnErase and Norton Protected Recycle Bin—Win 2000/XP

Norton UnErase and Norton Protected Recycle Bin work in a similar fashion with Windows 2000/XP as with Windows 9x/Me, but with a significant exception: The Unerase Wizard can search only hard drives. Removable-media drives are not supported.

Alternatives to Norton UnErase

VCOM's System Suite 4.0 (previously sold by Ontrack) is an integrated utility suite that offers an undelete feature similar in many ways to Norton UnErase. However, System Suite's FileUndeleter works with removable-media drives as well as hard drives under all supported versions of Windows, including Windows XP.

Although it's not an automatic tool, you can use Norton's Disk Editor (DISKEDIT.COM) to retrieve lost data from hard, floppy, and most types of removable-media drives under any file system and most operating systems, including Linux. See the section "Using the Norton Disk Editor," later in this chapter.

Undeleting Files in NTFS

Because the file structure of NTFS is much more complex than any FAT file system version and some files might be compressed using NTFS's built-in compression, you should use an NTFS-specific file undeletion program to

attempt to recover deleted files from an NTFS drive. For example, you should use a version of Norton Utilities or Norton SystemWorks compatible with NTFS, such as the 2002 or later versions. Also, you should enable the Norton Protection feature, which stores deleted files for a specified period of time before purging them from the system. Using Norton Protection will greatly enhance Norton UnErase's capability to recover deleted files.

If you need to recover deleted files and have not already installed an undelete program such as Norton Utilities or Norton SystemWorks' Norton UnErase, you should consider a standalone file recovery program, such as

- *Active Undelete.* This series of products also works with flash memory cards; more information and a free demo are available from http://www.active-undelete.com.
- *Restorer 2000.* Available in FAT, NTFS, and Professional versions; more information and a free demo are available from http://www.bitmart.net/r2k.shtml.
- *Ontrack EasyRecovery.* More information and a free demo are available from http://www.ontrack.com.

Tip

Some file-undelete products for NTFS can undelete only files created by the currently logged-in user, whereas others require the administrator to be logged in. Check the documentation for details, particularly if you are trying to undelete files from a system with more than one user.

Retrieving Data from Partitioned and Formatted Drives

When a hard disk, floppy disk, or removable-media drive has been formatted, its file allocation table, which is used by programs such as Norton UnErase or VCOM System Suite's FileUndeleter to determine the location of files, is lost. If a hard drive has been repartitioned with FDISK or another partitioning program (such as Windows 2000/XP's Disk Management), the original file system and partition information is lost (as is the FAT).
In such cases, more powerful data-recovery tools must be used to retrieve data. To retrieve data from an accidentally formatted drive, you have two options:

- Use a program that can unformat the drive.
- Use a program that can bypass the newly created FAT and read disk sectors directly to discover and retrieve data.

To retrieve data from a drive that has been partitioned, you must use a program that can read disk sectors directly.

Norton Unformat and Its Limitations

Norton Utilities and Norton SystemWorks offer Norton Unformat, which can be launched from the bootable CD to unformat an accidentally formatted FAT drive. However, Norton Unformat has significant limitations with today's file systems and drive types, including the following:

- *Norton Un format doesn't support NTFS drives.* This means many Windows 2000 and XP-based systems can't use it for data recovery.
- *Norton Un format cannot be used with drives that require device drivers to function, such as removable-media drives.*

- *Norton Unformat works best if the Norton Image program has been used to create a copy of the FATs and root directory.* If the image file is out-of-date, Unformat might fail; if the image file is not present, Unformat cannot restore the root directory and the actual names of folders in the root directory will be replaced by sequentially numbered folder names.
- *Norton Unformat cannot copy restored files to another drive or folder.* It restores data back to the same drive and partition. If Unformat uses an out-of-date file created by Norton Image to determine where data is located, it could overwrite valid data on the drive being unformatted.

For these reasons, Norton Unformat is not the most desirable method for unformatting a drive. You can use the powerful, but completely manual, Norton Disk Editor (DISKEDIT) to unformat a drive or retrieve data from a formatted drive, but other alternatives are simpler.

Retrieving Lost Data to Another Drive

Many products on the market can retrieve lost data to another drive, even if the data loss was due to accidental formatting or disk partitioning. One of the best and most comprehensive products is the EasyRecovery product line from Ontrack DataRecovery Services, a division of Kroll Ontrack, Inc. The EasyRecovery product line includes the following products:

- *EasyRecovery DataRecovery.* Recovers data from accidentally formatted or deleted hard, floppy, and removable-media drives and repairs damaged or corrupted Zip and Microsoft Word files. Local and network folders can be used for recovered files.
- *EasyRecovery FileRepair.* Repairs and recovers data from damaged or corrupted Zip and Microsoft Office (Word, Excel, Access, PowerPoint, and Outlook) files. Local and network folders can be used for recovered files.
- *EasyRecovery Professional.* Combines the features of DataRecovery and FileRecovery and adds features such as file type search, RawRecovery, and user-defined partition parameters to help recover data from more severe forms of file system corruption and accidental partitioning. A free trial version displays files that can be recovered (and repairs and recovers Zip files at no charge); it can be downloaded from the Ontrack website (http://www.ontrack.com).

An earlier version of EasyRecovery Data Recovery Lite can recover up to 50 files and is included as part of VCOM's System Suite (previously sold by Ontrack).

When you start EasyRecovery Professional, you can choose from several recovery methods, including these:

- *DeletedRecovery.* Recovers deleted files
- *FormatRecovery.* Recovers files from accidentally formatted drives
- *RawRecovery.* Recovers files with direct sector reads using file-signature matching technology
- *AdvancedRecovery.* Recovers data from deleted or corrupted partitions

In each case, you need to specify another drive to receive the retrieved data. This read-only method preserves the contents of the original drive and enables you to use a different data-recovery method if the first method doesn't recover the desired files.

Which options are best for data recovery? Table 11.1 shows the results of various data-loss scenarios and recovery options when EasyRecovery Professional was used to recover data from a 19GB logical drive formatted with the NTFS file system under Windows XP.

Table 11.1 Data Recovery Options and Results with EasyRecovery Professional

Type of Data Loss	Data Recovery Method	Data Recoverable?	Details	Notes
Deleted folder	DeletedRecovery	Yes	All files recovered.	All long file and folder names preserved.
Formatted drive (full format)	FormatRecovery	Yes	All files recovered.	New folders created to store recovered files; long filenames preserved for files and folders beneath root folder level.
Logical drive deleted with Disk Management	AdvancedRecovery	Yes	All files and folders recovered.	All long file and folder names preserved.
Formatted drive with new data copied to it	FormatRecovery	Partial	Files and folders that were not overwritten were recovered.	Long filenames and folders preserved.
Formatted, repartitioned drive reformatted as FAT32 (117MB Disk 1)	AdvancedRecovery	No	Could not locate any files to recover.	
	RawRecovery	Partial	Nonfragmented files recovered.	Original directory structure and filenames lost; each file type stored in a separate folder and files numbered sequentially.
Formatted, repartitioned drive formatted as NTFS (18.8GB Disk 2)	AdvancedRecovery	No	Could not locate any files to recover.	
	RawRecovery	Partial	Nonfragmented files recovered.	Original directory structure and filenames lost; each file type stored in a separate folder and files numbered sequentially.

As Table 11.1 makes clear, as long as the data areas of a drive are not overwritten, complete data recovery is usually possible—even if the drive has been formatted or repartitioned. Thus, it's critical that you react quickly if you suspect you have partitioned or formatted a drive containing valuable data. The longer you wait to recover data, the less data will be available for recovery. In addition, if you must use a sector-by-sector search for data (a process called RawRecovery by Ontrack), your original folder structure and long filenames will not be saved. You will therefore need to re-create the desired directory structure and rename files after you recover them—a very tedious process.

Tip

If you use EasyRecovery Professional or EasyRecovery DataRecovery to repair damaged Zip or Microsoft Office files, use the Properties menu to select a location for repaired files (the original location or another drive or folder). By default, repaired Outlook files are copied to a different folder, whereas other file types are repaired in place unless you specify a different location.

As you can see from this example, dedicated data-recovery programs such as Ontrack EasyRecovery Professional are very powerful. However, they are also very expensive. If you have Norton Utilities or Norton SystemWorks and don't mind taking some time to learn about disk structures, you can perform data recovery with the Norton Disk Editor.

Using the Norton Disk Editor

In my PC Hardware (Upgrading and Repairing) and Data Recovery/Computer Forensics seminars, I frequently use the Norton Disk Editor—an often-neglected program that's part of the Norton Utilities and Norton SystemWorks—to explore drives. I also use Disk Editor to retrieve lost data. Because Disk Editor is a manual tool, it can sometimes be useful even when friendlier automatic programs don't work correctly or are unavailable. For example, in physical sector mode, Disk Editor can be used with any drive regardless of what file system was used, since at that level it is working underneath the OS. Additionally, because Disk Editor displays the structure of your drive in a way other programs don't, it's a perfect tool for learning more about disk drive structures as well as recovering lost data. This section discusses two of the simpler procedures you can perform with Disk Editor:

- Undeleting a file on a floppy disk
- Copying a deleted file on a hard disk to a different drive

If you have Norton SystemWorks, SystemWorks Professional, or Norton Utilities for Windows, you have Norton Disk Editor. To determine whether it's installed on your system, look in the Norton Utilities folder under the Program Files folder for the following files: `DISKEDIT.EXE` and `DISKEDIT.HLP`. If you don't find these files on your hard disk, you can run them directly from the Norton installation CD. If you have SystemWorks or SystemWorks Professional, look for the CD folder called `\ NU` to locate these files.

Disk Edit is a command prompt program designed primarily to access FAT-based file systems such as FAT12 (floppy disks), FAT16 (MS-DOS and early Windows 95 hard disks), and FAT32 (Windows 95B/Windows 98/Me hard disks). You can use Disk Edit with Windows NT, Windows 2000, and Windows XP if you prepared the hard disks with the FAT16 or FAT32 file systems. Disk Edit will also work on NTFS volumes; however, in that case it can only be used in physical sector mode.

I strongly recommend that you first use Disk Editor with floppy disks you have prepared with noncritical files before you use it with a hard disk or vital files. Because Disk Editor is a completely manual program, the opportunities for error are high.

The Disk Edit files can easily fit on a floppy disk, but if you are new to the program, you might want to put them on a different drive from one you will be examining or repairing. *Never* copy Disk Edit files (or any other data recovery program) to a drive that contains data you are trying to recover because the files might overwrite the data area and destroy the files you want to retrieve. For example, if you are planning to examine or repair floppy disks, create a folder on your hard disk called `Disk Edit` and copy the files to that folder.

You can use Disk Editor without a mouse by using keyboard commands, but if you want to use it with a mouse, you can do so if your mouse attaches to the serial or PS/2 mouse ports (USB mice generally don't work from the command prompt, but if your USB mouse has a PS/2 mouse port adapter, you can use it by plugging the mouse and adapter into the PS/2 port). You must load an MS-DOS mouse driver (usually MOUSE.COM) for your mouse before you start Disk Editor. If you have a Logitech mouse, you can download an MS-DOS mouse driver from the Logitech website. If you have a Microsoft mouse, Microsoft doesn't provide MS-DOS drivers you can download, but you can get them from the following website:
http://www.bootdisk.com/readme.htm#mouse

For other mice, try the Microsoft or Logitech drivers, or contact the vendor for drivers. Keep in mind that scroll wheels and other buttons won't work with an MS-DOS driver. I recommend you copy your mouse driver to the same folder in which Disk Editor is located.

Using Disk Editor to Examine a Drive

To start Disk Editor:

1. Boot the computer to a command prompt (not Windows); Disk Editor needs exclusive access to the drives you plan to examine. If you use Windows 9x, press F8 or Ctrl to bring up the startup menu and select Safe Mode Command Prompt, or use the Windows 9x/Me Emergency Startup disk (make one with Add/Remove Programs). If you use Windows 2000 or XP, insert a blank floppy disk into drive A:, right-click drive A: in My Computer, and select Format. Select the Create an MS-DOS Startup Disk option and use this disk to start your computer.
2. Change to the folder containing your mouse driver and Disk Editor.
3. Type MOUSE (if your mouse driver is called MOUSE.COM or MOUSE.EXE; otherwise, substitute the correct name if it's called something else). Then press Enter to load the mouse driver.
4. Type DISKEDIT and press Enter to start the program. If you don't specify a drive, Disk Editor scans the drive on which it's installed. If you are using it to work with a floppy disk, enter the command DISKEDIT A: to direct it to scan your floppy disk. Disk Editor scans your drive to determine the location of files and folders on the disk.
5. The first time you run Disk Editor, a prompt appears to remind you that Disk Editor runs in read-only mode until you change its configuration through the Tools menu. Click OK to continue.

After Disk Editor has started, you can switch to the drive you want to examine or recover data from. To change to a different drive, follow these steps:

1. Press Alt+O to open the Object menu.
2. Select Drive.
3. Select the drive you want to examine from the Logical Disks menu.
4. The disk structure is scanned and displayed in the Disk Editor window.

Disk Editor normally starts in Directory mode, but you can change it to other modes with the View menu. When you view a drive containing data in Directory mode, you will see a listing similar to the one shown in Figure 11.1.

The Name column lists the names of the directory entries, and the .EXT column lists the file/folder extensions (if any). The ID column lists the type of directory entry, including

- *Dir.* A directory (folder).
- *File.* A data file.
- *LFN.* A portion of a Windows long filename. Windows stores the start of the LFN before the actual filename. If the LFN is longer than 13 characters, one or more additional directory entries is used to store the rest of the LFN. The next three columns list the file size, date, and time.

The Cluster column indicates the cluster in which the first portion of the file is located. Drives are divided into clusters or allocation units when they are formatted, and a *cluster* (allocation unit) is the smallest unit that can be used to store a file. Cluster sizes vary with the size of the drive and the file system used to format the drive.

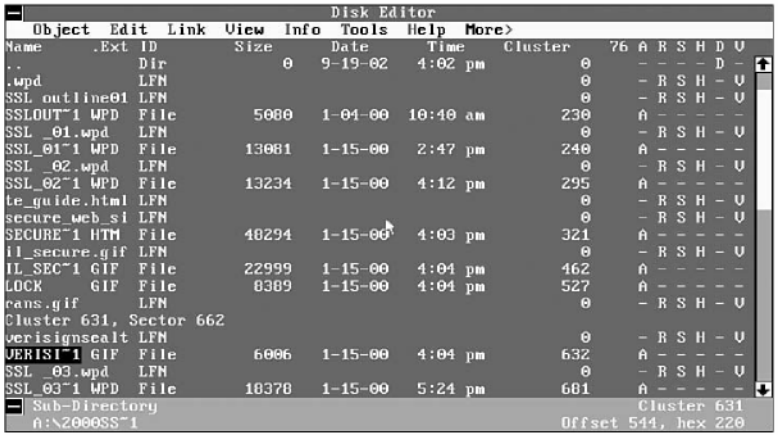

Figure 11. 1 The Norton Disk Editor directory view of a typical floppy disk.

The letters *A, R, S, H, D,* and *V* refer to attributes for each directory entry. *A* (archive) means the file hasn't been backed up since it was last modified. *R* is used to indicate that the directory entry is read-only, and *S* indicates that the directory entry has the System attribute. *H* indicates that the directory entry has the Hidden attribute, whereas *D* indicates that the entry is a directory. Finally, *V* is the attribute for an LFN entry.

The file `VER ISI~1 .GIF` (highlighted in black near the bottom of Figure 11.1) is interesting for several reasons. The tilde (~) and number at the end of the filename indicate that the file was created with a 32-bit version of Windows. 32-bit versions of Windows (Windows 9x/Me, 2000, and XP) allow the user to save a file with a long (more than eight characters) filename (plus the three-character file extension such as `.EXE`, `.BMP`, or `.GIF`). In addition, long filenames can have spaces and other characters not allowed by earlier versions of Windows and MS-DOS. The process used by various versions of Windows to create LFN entries is discussed in Chapter 10, in the section called "VFAT and Long Filenames."

When you view the file in Windows Explorer or My Computer, you see the long filename. To see the DOS alias name within the Windows GUI, right-click the file and select Properties from My Computer or Windows Explorer. Or, you can use the `DIR` command in a command-prompt window. The LFN is stored as one or more separate directory entries just before the DOS alias name. Because the actual long name for `VERISI~1 .GIF` (`Verisignsealtrans.gif`) is 21 characters, two additional directory entries are required to store the long filename (each directory entry can store up to 13 characters of an LFN), as shown in Figure 11.1.

Determining the Number of Clusters Used by a File

As discussed earlier in this chapter, an area of the disk called the file allocation table stores the starting location of the file and each additional cluster used to store the file. `VERISI~1 . GIF` starts at cluster 632. Clusters are the smallest disk structures used to store files, and they vary in size depending on the file system used to create the disk on which the files are stored and on the size of the drive. In this case, the file is stored on a 1.44MB floppy disk, which has a cluster size of 512 bytes (one sector). The cluster size of the drive is very important to know if you want to retrieve data using Disk Editor.

To determine the cluster size of a drive, you can open a command-prompt window and run CHKDSK C: to display the allocation unit size (cluster size) and other statistics about the specified drive.

To determine how many clusters are used to store a file, look at the size of the file and compare it to the cluster size of the drive on which it's stored. The file VERISI~1.GIF contains 6,006 bytes. Because this file is stored on a floppy disk that has a cluster size of 512 bytes, the file must occupy several clusters. How many clusters does it occupy? To determine this, divide the file size by the number of clusters and round the result up to the next whole number. The math is shown in Table 11.2.

Table 11.2 Determining the Number of Clusters Used by a File

File Size (FS) of VERISI~1 .GIF	Cluster Size (CS)	Result of (FS) Divided by (CS) Equals (CR)	(CR) Rounded Up to Next Whole Number
6,006	512	11.73046875	12

From these calculations, you can see that VER ISI~1.GIF uses 12 clusters on the floppy disk; it would use fewer clusters on a FAT16 or FAT32 hard disk (the exact number depends on the file system and size of the hard disk). The more clusters a file contains, the greater the risk is that some of its data area could be overwritten by newer data if the file is deleted. Consequently, if you need to undelete a file that was not sent to the Windows Recycle Bin or was deleted from a removable-media drive or floppy drive (these types of drives don't support the Recycle Bin), the sooner you attempt to undelete the file, the more likely it is that you can retrieve the data.

The normal directory display in Norton Disk Editor shows the starting cluster (632) for VERISI~1.GIF. If a file is stored on a drive with a lot of empty space, the remainder of the clusters will probably immediately follow the first two—a badly fragmented drive might use noncontiguous clusters to store the rest of the file. Because performing data recovery when the clusters are contiguous is much easier, I strongly recommend that you defragment your drives frequently.

To see the remainder of the clusters used by a file, move the cursor to the file, press Alt+L or click the Link menu, and select Cluster Chain (FAT); you can also press Ctrl+T to go directly to this view. The screen changes to show the clusters as listed in the FAT for this file, as shown in Figure 11.2. The clusters used by the file are highlighted in red, and the filename is shown at the bottom of the screen. The symbol <EOF> stands for *end of file,* indicating the last cluster in the file.

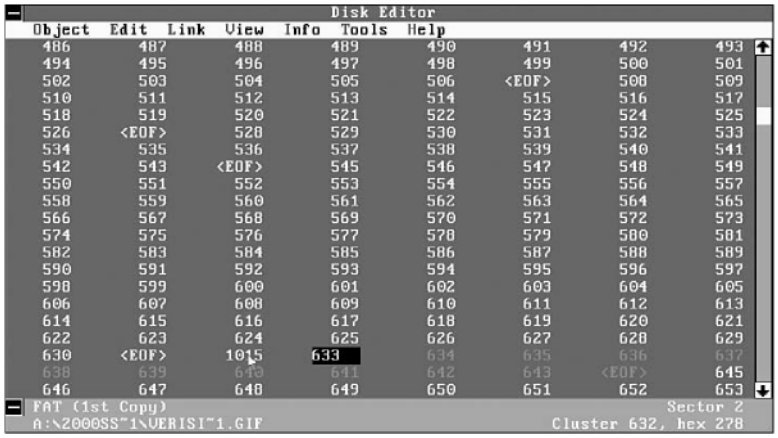

Figure 11.2 The FAT view of VERISI~1.GI F. All its clusters are contiguous.

How the Operating System Marks a File When It Is Deleted

If a file (VERISI~1.GIF, in this example) is deleted, the following changes happen to the disk where the file is stored, as shown in Figure 11.3:

- The default directory view shows that the first character of the filename (V) has been replaced with a σ (lowercase sigma) character.
- There are now two new types of entries in the ID column for this file and its associated LFN:
  - *Erased.* An erased file
  - *Del LFN.* An LFN belonging to an erased file

Note also that the beginning cluster (632) is still shown in the Cluster column.

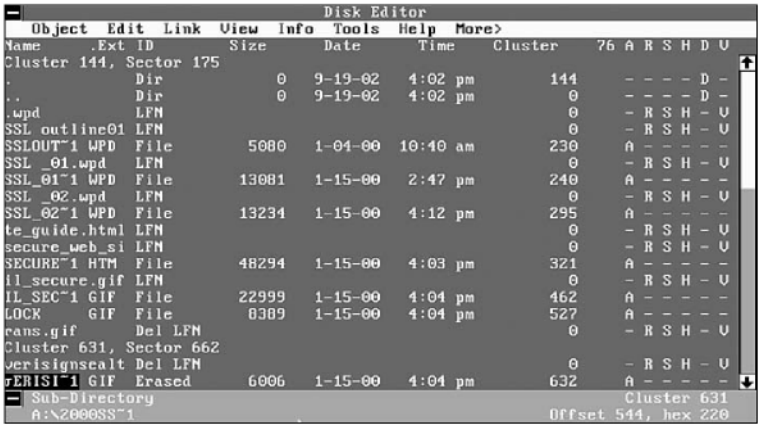

Figure 11.3 The Directory view after VERISI~1 .GIF has been deleted.

Zeroes have also replaced the entries for the cluster locations after the beginning cluster in the FAT. This indicates to the operating system that these clusters are now available for reuse. Thus, if an undelete process is not started immediately, some or all of the clusters could be overwritten by new data. Because the file in question is a GIF graphics file, the loss of even one cluster will destroy the file.

As you can see from analyzing the file-deletion process, the undelete process involves four steps:

- Restoring the original filename
- Locating the clusters used by the file
- Re-creating the FAT entries for the file
- Relinking the LFN entries for the file to the file

Of these four, the most critical are locating the clusters used by the file and re-creating the FAT entries for the file. However, if the file is a program file, restoring the original name is a must for proper program operation (assuming the program can't be reloaded), and restoring the LFN entries enables a Windows user accustomed to long filenames to more easily use the file.

If you want to make these changes to the original disk, Disk Editor must be configured to work in Read-Write mode.

To change to Read-Write mode, follow these steps:

1. Press Alt+T to open the Tools menu.
2. Press N to open the Configuration dialog box.
3. Press the spacebar to clear the check mark in the Read Only option box.
4. Press the Tab key until the Save box is highlighted.
5. Press Enter to save the changes and return to the main display.

Caution

As a precaution, I recommend that you use DISKCOPY to make an exact sector-by-sector copy of a floppy disk before you perform data recovery on it, and you should work with the copy of the disk, not the original. By working with a copy, you keep the original safe from any problems you might have; plus, you can make another copy if you need to.

After you change to Read-Write mode, Disk Editor stays in this mode and uses Read-Write mode every time you use it. To change back to Read-Only mode, repeat the previously listed steps but check the Read-Only box. If you are using Disk Editor in Read-Write mode, you will see the message `Drive` *x* `is Locked` when you scan a drive.

Undeleting an Erased File

After you have configured Disk Editor to work in Read-Write mode, you can use it to undelete a file.

To recover an erased file, follow this procedure:

1. To change to the folder containing the erased file, highlight the folder containing the erased file and press Enter. In this example, you will recover the erased file `VERISI~1.GIF`.
2. Place the cursor under the lowercase sigma symbol and enter a letter to rename the file.
3. If the keyboard is in Insert mode, the lowercase sigma will move to the right; press the Delete key to delete this symbol.
4. This restores the filename, but even though the ID changes from Erased to File, this does *not* complete the file-retrieval process. You must now find the rest of the clusters used by the file. To the right of the filename, the first cluster used by the file is listed.
5. To go to the next cluster used by the file, press Ctrl+T to open the Cluster Chain command. Because you changed the name of the file, you are prompted to write the changes to the disk before you can continue. Press W or click Write to save the changes and continue.
6. Disk Editor moves to the first cluster used by the deleted file. Instead of cluster numbers, as shown earlier in Figure 11.2, each cluster contains a zero (0). Because this file uses 12 clusters, there should be 12 contiguous clusters that have been zeroed out if the file is unfragmented.
7. To determine whether these are the correct clusters for the file, press Alt+O or click Object to open the Object menu. Press C to open the Cluster dialog box (or press Alt+C to go to the Cluster dialog box). Enter the starting cluster number (632 in this example) and the ending cluster number (644 in this example). Click OK to display these clusters.
   Disk Editor automatically switches to the best view for the specified object, and in this case, the best view is the Hex view (see Figure 11.4). Note that the first entry in cluster 632 is GIF89a (as shown in the right column). Because the deleted file is a GIF file, this is what we expected. Also, a GIF file is a binary graphics file, so the rest of the information in the specified sectors should not be human-readable. Note that the end of the file is indicated by a series of 0s in several disk sectors before another file starts.

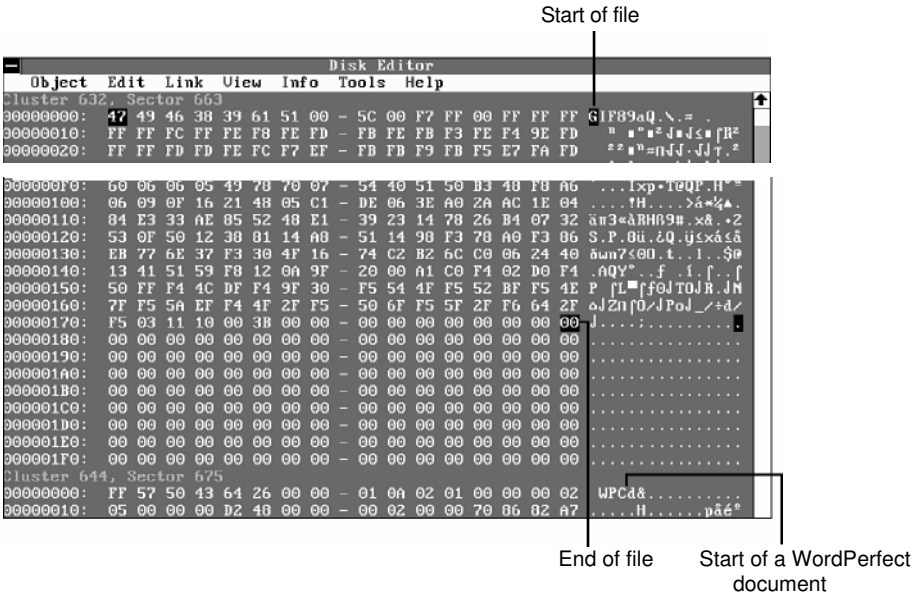

Figure 11.4 The start and end of the file `VERISI~1 .GIF`.

Because the area occupied by the empty clusters (632–644) contains binary data starting with GIF89a, you can feel confident that these clusters contain the data you need.

8. To return to the FAT to fill in the cluster numbers for the file, open the Object menu and select Directory. The current directory is selected, so click OK.
9. Move the cursor down to the entry for `VERISI~1.GIF`, open the Link menu, and click Cluster Chain (FAT). The Cluster Chain refers to the clusters after the initial cluster (632); enter **633** in the first empty field, and continue until you enter **643** and place the cursor in the last empty field. This field needs to have the `<EOF>` marker placed in it to indicate the end of the file. Press Alt+E to open the Edit menu and select Mark (or press Ctrl+B). Open the Edit menu again and select Fill. Then, select End of File from the menu and click OK. Refer to Figure 11.2 to see how the FAT looks after these changes have been made.
10. To save the changes to the FAT, open the Edit menu again and select Write. When prompted to save the changes, click Write; then click Rescan the Disk.
11. To return to Directory view, open the Object menu and select Directory. Click OK.
12. The LFN entries directly above the `VERISI~1.GI F` file are still listed as Del LFN. To reconnect them to `VERISI~1 .GIF`, select the first one (`verisignsealt`), open the Tools menu (press Alt+T), and select Attach LFN. Click Yes when prompted. Repeat the process for `rans.gif`.
13. To verify that the file has been undeleted successfully, exit Disk Editor and open the file in a compatible program. If you have correctly located the clusters and linked them, the file will open.

As you can see, this is a long process, but it is essentially the same process that a program such as Norton UnErase performs automatically. However, Disk Editor can perform these tasks on all types of disks that use FAT file systems, including those that use non-DOS operating systems; it's a favorite of advanced Linux users.

Retrieving a File from a Hard Disk or Flash Memory Card

What should you do if you need to retrieve an erased file from the hard disk or a flash memory card? It's safer to write the retrieved file to another disk (preferably a floppy disk if the file is small enough) or to a different drive letter on the hard disk. You can also perform this task with Disk Editor.

Tip

If you want to recover data from a hard disk and copy the data to another location, set Disk Editor back to its default Read-Only mode to avoid making any accidental changes to the hard disk. If you use Disk Editor in a multitasking environment such as Windows, it defaults to Read-Only mode.

The process of locating the file is the same as that described earlier:

1. Determine the cluster (allocation unit) size of the drive on which the file is located.
2. Run Disk Editor to view the name of the erased file and determine which clusters contain the file data.

However, you don't need to restore the filename because you will be copying the file to another drive.

The clusters will be copied to another file, so it's helpful to use the Object menu to look at the clusters and ensure that they contain the necessary data. To view the data stored in the cluster range, open the Object menu, select Cluster, and enter the range of clusters that the cluster chain command indicates should contain the data. In some cases, the first cluster of a particular file indicates the file type. For example, a GIF file has `GI F89a` at the start of the file, whereas a WordPerfect document has `WPC` at the start of the file.

Tip

Use Norton Disk Editor to view the starting and ending clusters of various types of files you create before you try to recover those types of files. This is particularly important if you want to recover files from formatted media. You might consider creating a database of the hex characters found at the beginning and ending of the major file types you want to recover.

If you are trying to recover a file that contains text, such as a Microsoft Word or WordPerfect file, you can switch Disk Edit into different view modes. To see text, press F3 to switch to Text view. However, to determine where a file starts or ends, use Hex mode (press F2 to switch to this mode). Figure 11.5 shows the start of a Microsoft Word file in Text format and the end of the file in Hex format.

To copy the contents of these clusters to a file safely, you should specify the sectors that contain the file. The top of the Disk Editor display shows the sector number as well as the cluster number. For example, the file shown in Figure 11.5 starts at cluster 75207, which is also sector 608470. The end of the file is located in sector 608503.

To write these sectors to a new file, do the following:

1. Open the Object menu.
2. Select Sector.
3. Specify the starting and ending sectors.
4. Click OK.
5. Scroll through the sectors to verify that they contain the correct data.

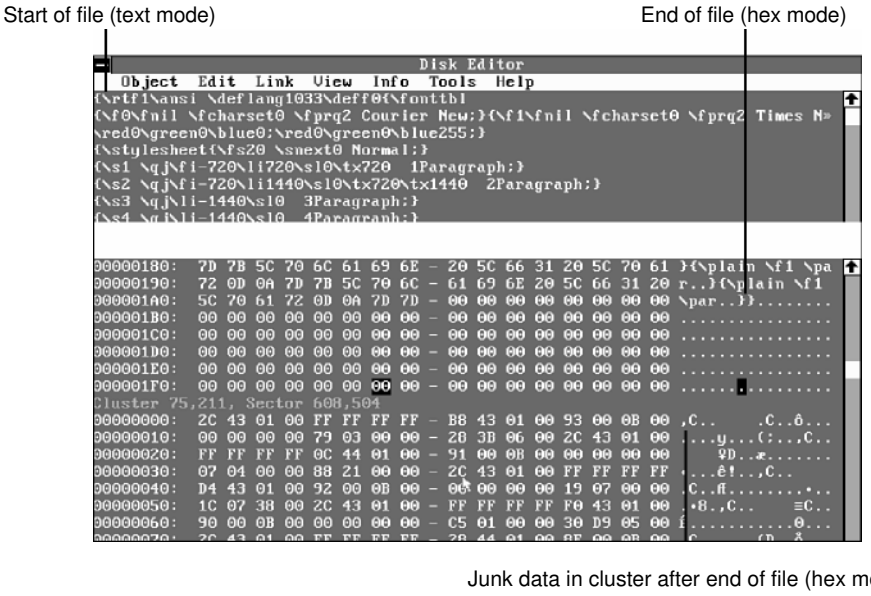

Figure 11.5 Scrolling through an erased file with Disk Editor.

6. Open the Tools menu.
7. Click Write Object To.
8. Click To a File.
9. Click the drive on which you want to write the data.
10. Specify a DOS-type filename (8 characters plus a 3-character extension); you can rename the file to a long filename after you exit Disk Edit.
11. Click OK, and then click Yes to write the file. A status bar appears as the sectors are copied to the file.
12. Exit Disk Edit and open the file in a compatible program. If the file contains the correct data, you're finished. If not, you might have specified incorrect sectors or the file might be fragmented.

Norton Disk Editor is a powerful tool you can use to explore drives and retrieve lost data. However, your best data recovery technique is to avoid the need for data recovery. Think before you delete files or format a drive, and make backups of important files. That way, you won't need to recover lost data very often.

Data Recovery from Flash Memory Devices

Flash memory devices such as USB keychain drives and cards used in digital cameras and digital music players present a unique challenge to data recovery programs. Although, from a user standpoint, these devices emulate conventional disk drives, have file allocation tables similar to those found on floppy disks, and can usually be formatted through the Windows Explorer, many data recovery programs that work well with conventional drives cannot be used to recover data from flash memory devices—especially when the device has been formatted.

Under several conditions, data loss can occur with a flash memory device. Some of them, such as formatting of the media or deletion of one or more photos or files, can occur when the device is connected to the computer through a card reader or when the flash memory device is inserted into a digital camera. When photos are deleted, the file locations and name listings in the file allocation tables are changed in the same way as when files are deleted from magnetic media: The first character of the filename is changed to a lowercase sigma, indicating the file has been erased. Just as with magnetic media, undelete programs that support removable-media drives and the Norton Disk Editor can be used to retrieve deleted files on flash memory devices in the same way that they retrieve deleted files from magnetic media. Note that Disk Editor must be run in Read-Only mode and works best on systems running Windows 9x/Me. Data files can also be damaged if the flash memory card is removed from a device before the data-writing process is complete.

However, retrieving data from a formatted flash memory device, whether it has been formatted by a digital camera or through Windows, is much more difficult. Traditional unformat programs such as the command-line Norton Unformat program provided with Norton Utilities and Norton SystemWorks can't be used because flash memory devices are accessible only from within the Windows GUI, and command-line programs are designed to work with BIOS-compatible devices such as hard and floppy drives.

Programs that rely on the file system, such as Ontrack EasyRecovery Personal Edition Lite (incorporated into VCOM System's Suite) and Ontrack EasyRecovery Personal Edition, do not work either because the previous file system is destroyed when the flash memory devices are formatted.

Note

When a digital camera formats a flash memory card, it usually creates a folder in which photos are stored. Some cameras might also create another folder for storing drivers or other information.

If you need to recover data from a formatted flash memory device, the following programs work extremely well:

- *Ontrack EasyRecovery Professional Edition;* free evaluation and more information are available from http://www.ontrack.com
- *PhotoRescue;* free evaluation and more information are available from http://www.datarescue.com/photorescue/

Norton Disk Editor (incorporated into Norton SystemWorks and Norton SystemWorks Pro) can also be used to recover data if you can determine the starting and ending clusters used by the data stored on the device.

To recover data from a formatted flash memory card with EasyRecovery Professional Edition, the RawRecovery option (which recovers data on a sector-by-sector basis) must be used. This option bypasses the file system and can be used on all supported media types. A built-in file viewer enables you to determine whether the recovered data is readable.

PhotoRescue, which works only with standard photo image types such as JPG, BMP, and TIF, can access the media in either logical drive mode (which worked quite well in our tests) or physical drive mode. Physical mode uses a sector-by-sector recovery method somewhat similar to that used by EasyRecovery Professional Edition. PhotoRescue also displays recovered photos in a built-in viewer. With both products, you might recover data from not just the most recent use before format, but also leftover data from previous uses. As long as the data area used by a particular file hasn't been overwritten, the data can be recovered—even if the device has been formatted more than once.

Table 11.3 provides an overview of our results when trying to recover data from two common types of flash memory devices: a Compact Flash card used in digital cameras and a USB keychain storage device.

Table 11.3 Retrieving Lost Data from Flash Memory Devices—Results by Data-Recovery Program

Device	Cause of Data Loss	Norton Utilities	Ontrack/Vcom System Suite	DataRescue Photo Rescue	Ontrack EasyRecovery Professional
Compact Flash 64MB	Deleted selected files in camera	Recovered data back to device when used with Windows 9x/Me only.[1, 2]	Recovered data to user-specified folder.[1, 3]	Recovered data from most recent format and from previous card uses to specified folder.[3, 4]	RawRecovery recovered deleted files from current and previous uses; refer to Table 11.1 for limitations.[3, 4]

Compact Flash 64MB	Deleted selected files with Windows Explorer	Recovered data back to device when used with Windows 9x/Me only.[1, 2]	Recovered data to specified folder when used with any supported version of Windows.[3]	Recovered data from most recent format and from previous card uses to specified folder (files and folders renamed).	DeletedRecovery recovered deleted data from current use (first character of file/folder name lost).
Compact Flash 64MB	Format in camera	Drive could not be unformatted; Disk Edit could retrieve data from current and previous uses to user-specified folder.[3, 5, 6]	Could not locate data. No data was recovered.	Recovered data from most recent format and from previous card uses to user-specified folder.[3, 4]	RawRecovery recovered all readable data, including data from previous card uses to user-specified folder.[3, 4]
Compact Flash 64MB	Format in card reader	Drive could not be unformatted; Disk Edit could retrieve data from current and previous uses.[5, 6]	Could not locate data. No data was recovered.	Recovered data from most recent format and from previous card uses to user-specified folder.[4]	RawRecovery recovered all readable data, including data from previous card uses to user-specified folder.[4]
USB keychain drive (128MB)	Deleted folder with My Computer	Disk Edit can retrieve data from current use.[3, 6]	Partial success: Recovered some files.[3]	Recovered photo files only.[3, 4]	RawRecovery retrieved most files.[3, 4]
USB keychain drive (128MB)	Formatted by Windows Explorer	Disk Edit can retrieve data from current use.[3, 6]	Partial success: Recovered some files (folder names and structure lost).[3]	Recovered photo files only.[3, 4]	RawRecovery retrieved most files.[3, 4]

1. *User supplied first letter of filename during undelete process.*
2. *Norton UnErase doesn't support removable-media drives in Windows NT/2000/XP.*

3. *Program operates in read-only mode on the drive containing the lost data.*
4. *Original file and folder names were not retained; files are numbered sequentially and might need to be renamed after recovery.*
5. *Windows must be used to access flash memory devices, and Norton Unformat can't be used in a multitasking environment such as Windows.*
6. *Disk Edit requires the user to manually locate the starting and ending sectors of each file and write the sectors to another drive with a user-defined filename.*

FAT File System Troubleshooting

Here are some general procedures to follow for troubleshooting drive access, file system, or boot problems:

1. Start the system using a Windows startup disk, or any bootable MS-DOS disk that contains `FDISK. EXE`, `FORMAT. COM`, `SYS .COM`, and `SCANDISK.EXE` (Windows 95B or later versions preferred).
2. If your system can't boot from the floppy, you might have more serious problems with your hardware. Check the floppy drive and the motherboard for proper installation and configuration. On some systems, the BIOS configuration doesn't list the floppy as a boot device or puts it after the hard disk. Reset the BIOS configuration to make the floppy disk the first boot device if necessary and restart your computer.
3. Run FDISK from the Windows startup disk. Select option 4 (Display partition information).
4. If the partitions are listed, make sure that the bootable partition (usually the primary partition) is defined as active (look for an uppercase *A* in the Status column).
5. If no partitions are listed and you do not want to recover any of the data existing on the drive now, use FDISK to create new partitions, and then use `FORMAT` to format the partitions. This overwrites any previously existing data on the drive.
6. If you want to recover the data on the drive and no partitions are being shown, you must use a data recovery program, such as the Norton Utilities or Lost and Found, to recover the data.
7. If all the partitions appear in `FDISK.EXE` and one is defined as active, run the `SYS` command as follows to restore the system files to the hard disk:

   ```
   SYS C:
   ```

8. For this to work properly, it is important that the disk you boot from be a startup disk from the same operating system (or version of Windows) you have on your hard disk.You should receive the message `System Transferred` if the command works properly. Remove the disk from drive A: and restart the system.

9. If you still have the same error before after you restart your computer, your drive might be improperly configured or damaged.
10. Run `SCANDISK` from the Windows startup disk or an aftermarket data-recovery utility, such as the Norton Utilities, to check for problems with the hard disk.
11. Using `SCANDISK`, perform a surface scan. If `SCANDISK` reports any physically damaged sectors on the hard disk, the drive might need to be replaced.

NTFS File System Troubleshooting

The process for file system troubleshooting with Windows 2000/XP is similar to that used for Windows 9x. The major difference is the use of the Windows 2000/XP Recovery Console, which is clarified here:

- If the Recovery Console was added to the boot menu, start the system normally, log in as Administrator if prompted, and select the Recovery Console.
- If the Recovery Console was not previously added to the boot menu, start the system using the Windows CD-ROM or the Windows Setup disks. Select Repair from the Welcome to Setup menu, and then press C to start the Recovery Console when prompted.

If your system can't boot from CD-ROM or the floppy, you might have more serious problems with your hardware. Check your drives, BIOS configuration, and motherboard for proper installation and configuration. Set the floppy disk as the first boot device and the CD-ROM as the second boot device and restart the system.

After you start the Recovery Console do the following:

1. Type `HELP` for a list of Recovery Console commands and assistance.
2. Run `DISKPART` to examine your disk partitions.
3. If the partitions are listed, make sure that the bootable partition (usually the primary partition) is defined as active.
4. If no partitions are listed and you do not want to recover any of the data existing on the drive now, use FDISK to create new partitions, and then use `FORMAT` to format the partitions. This overwrites any previously existing data on the drive.
5. If you want to recover the data on the drive and no partitions are being shown, you must use ata recovery program, such as the Norton Utilities or Lost and Found, to recover the data.

6. If all the partitions appear in `DISKPART` and one is defined as active, run the `FIXBOOT` command as follows to restore the system files to the hard disk:

   ```
   FIXBOOT
   ```

7. Type **EXIT** to restart your system. Remove the disk from drive A: or the Windows 2000 or XP CD-ROM from the CD-ROM drive.
8. If you still have the same error after you restart your computer, your drive might be improperly configured or damaged.

9. Restart the Recovery Console and run `CHKDSK` to check for problems with the hard disk.