TRAINING COURSE

ON

BASIC COMPUTER SKILLS

(UNDER WORLD BANK AIDED HYDROLOGY PROJECT)

October 15 - 25, 1997

MODULE - 8

SOFTWARE AND FILE PROBLEMS

by

Mrs. Archana Sarkar

NATIONAL INSTITUTE OF HYDROLOGY
ROORKEE - 247 667 (U.P.)
INDIA

SOFTWARE AND FILE PROBLEMS

INTRODUCTION

Over the past decades, computer software has become the pivotal element of computer based systems. Software, as a sequence of commands(programme) used to achieve the desired output, is not limited to one particular jobor application. Advanced categories of software tools include operating systems, language compilers, application packages and user written programmes.

It is software that determines the success of entire systems. Software provides function by tapping the potential hardware provides. This in turn leads to the intelligence associated with computer based products. Unfortunately, development and/or application of software has its problems. Some of the problems faced by users in file handling are presented in this lecture.

1.0 LOST FILES

Inspite of all precautions, everyone deletes the wrong files occasionally or changes his or her mind after deleting a file. Similarly, user may accidently format the wrong disk. Using just the tools included with DOS and Norton Utilities (NU), user can do much to protect and recover his data from all the things that can go wrong in his system.

1.1 Protection Utilities

The tool that provides the best protection against data loss of any kind is MSBACKUP. This program helps user keep up-to-date backups of all his important files so that he can recover from any kind of loss. As far as deleting and formatting the wrong files or disks, the following Norton utilities provide the protection.

♬ Protecting data with Image
♬ Preserving deleted files with Smartcan
♬ Formatting disks with safe format

1.1.1 Protecting Data With Image

Image saves PC's boot record, file allocation table (FAT), and root directory information to a file named IMAGE.DAT. Unformat and Unerase both use this file to recover data.

Image command can be specified in AUTOEXEC.BAT to run it every time. When computer is turned ON or it can be typed on DOS prompt.

```
IMAGE [drive :] [/NOBACKUP] [/OUT]
```

Where,

drive : specifies save information on current drive. If omitted, save information for the current drive only.

/NOBACKUP : Overwrite the current IMAGE.DAT file without creating the backup file, IMAGE.BAK

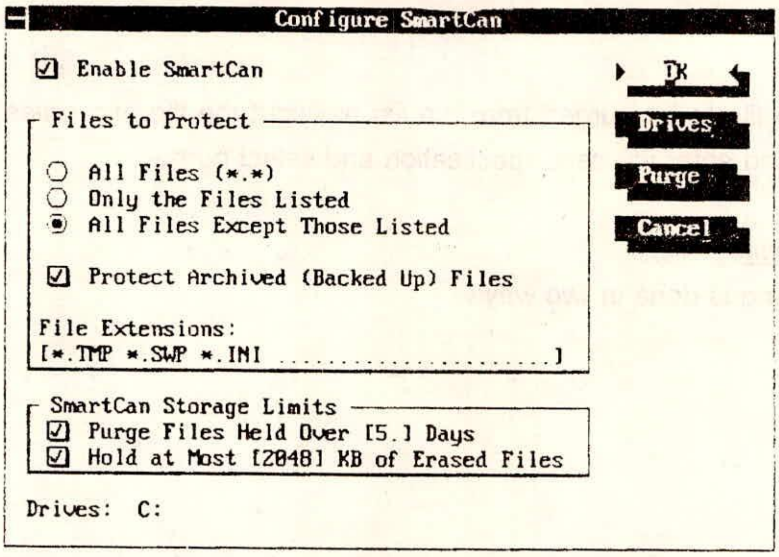
/OUT: Display no update messages.

Whenever Image runs, it creates a new IMAGE.DAT file and renames the old one IMAGE.BAK. Image also creates a file called IMAGE.IDX which is an Index file pointing to the locations of the DAT and BAK files

1.1.2 Preventing Deleted Files With Smartcan

Smartcan protects deleted files from being overwritten. As the disk space is limited it purges the protected files after a specified number of days or when protected data reaches a specified size.

- Select Smartcan in command list in NU main screen or type SMARTCAN at DOS prompt. Figure -1 shows default settings.
- To enable Smartcan : Enable Smartcan check box.
- Protecting other Drives : Select the floppy, local or Network drive to protect by clicking on Drives option.
- Files to Protect : Specify which files to protect it may be all or specified files by giving their extension. Eg. *.DBF & *.DOC.
- Protect Archived : (Backed up) Files Check the Protect Archived (Backed up) Files check box.
- Changing Storage Limits : It can be done by two ways :
    - Specifying number of Ways for which deleted files be kept and not overwritten,default is 5 days.
    - Specifying the space limit in kilobytes i.e. number of files be kept till memory is full, default is 16k.



☑ Enable SmartCan

Files to Protect

○ All Files (*.*)
○ Only the Files Listed
● All Files Except Those Listed

☑ Protect Archived (Backed Up) Files

File Extensions:
[*.TMP *.SWP *.INI ....]

SmartCan Storage Limits

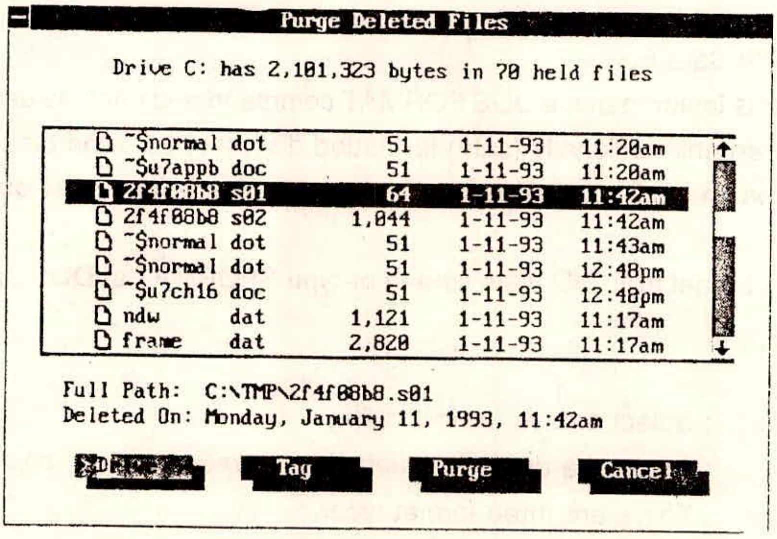
☑ Purge Files Held Over [5.] Days
☑ Hold at Most [2048] KB of Erased Files

Drives: C:

Figure 1 - Configure Smartcan dialog box

➡ Purging Files Manually

Select Purge Command button. It gives list of deleted files. If these files are not necessary to save protection can be removed for these file types.



Drive C: has 2,101,323 bytes in 70 held files

```
~$normal  dot       51   1-11-93   11:20am
~$u7appb  doc       51   1-11-93   11:20am
2f4f08b8  s01       64   1-11-93   11:42am
2f4f08b8  s02    1,044   1-11-93   11:42am
~$normal  dot       51   1-11-93   11:43am
~$normal  dot       51   1-11-93   12:48pm
~$u7ch16  doc       51   1-11-93   12:48pm
ndw       dat    1,121   1-11-93   11:17am
frame     dat    2,820   1-11-93   11:17am
```

Full Path: C:\TMP\2f4f08b8.s01
Deleted On: Monday, January 11, 1993, 11:42am

Figure 2 - Purge Deleted files dialog box

To mark the file to be purged from the list highlight the file and press Spacebar or select Tag and enter wildcard specfication and select purge.

1.1.3 Formating Disk

Disk formatting is done in two ways

- High level
- Low level

High Level Format :

High Level format only resets the information in the system area, making the disk available for new data, it does not overwrite data. Even though the disk appears empty, the file data is still there. Safe format & Quick formatting mode perform high level format.

Low Level Format :

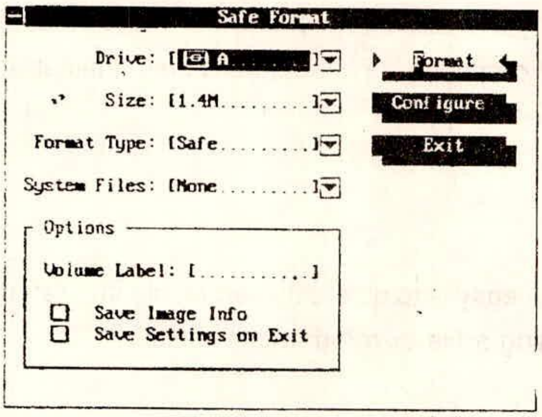
Low level format destroys all the data on the floppy disk (hard disk only receive high level formats). Formatting a floppy disk with the DOS FORMAT Command from earlier DOS Versions perform only a low level format.

Formatting Disk with Safe Format :

Safe format is faster than the DOS FORMAT command and enables user to completely recover data from an unintentionally (safe) formatted disk. It checks the disk surface, marks bad sectors, creates Image files, and reforms bad sectors. It provides more options than DOS format.

Select safe format from NU main screen or type SFORMAT at DOS prompt as shown in the next figure.

- ➨ Drive : Select a drive for formatting.
- ➨ Size : Select the drive size, default is drives maximum capacity.
- ➨ Format type : There are three format types :
  - Safe Format : It uses its own formatting algorithm, checks the disk surface, marks sectors, creates image files and reforms bad tracks.



```
Safe Format

Drive: [A..........]
Size: [1.4M.........]
Format Type: [Safe.........]
System Files: [None.........]

Options
Volume Label: [..........]
□ Save Image Info
□ Save Settings on Exit
```

Figure 3 - Safe Format dialog box

  - Quick format : It places a new system area on a previously formatted disk and creates Image files. It is faster than safe format and is good for quickly removing a large directory tree from a disk.
  - DOS Format : It duplicates the DOS FORMAT command from DOS version before 5.0. It completely erases all data. User cannot recover data that existed before formating.
- System Files : Specify whether or not to put system files on the disk to make it bootable, or to leave space for system files & make it bootable later.
- Options :
  - Volume label : Enter a name of upto eleven characters for disk.
  - Save Image Info : Specify whether to save the disks system area to the file IMAGE.DAT, which enables user to unformat data. Not available for DOS format mode.
  - Save settings on Exit : Save current settings so the same could be used for next time.
- Format : Select to begin formatting. A warning box displays any files currently on the disk.

- Configure : When configure command button is selected safe format automatically determines the number, types and highest capacity of the floppy drive attached to computer. There are two options :
  - Prompt for Missing Diskettes : checks disk in drive when selected.
  - Allow hard Disk Formatting : Protects hard disk against accidental formatting when in unselected mode.

1.2 Recovery Utilities

User probably knows how easy is to delete the wrong file and reformat the wrong disks or change your mind after deleting a file or reformatting a disk.

1.2.1 Recovery of Deleted/Erased files

When user wants to recover a deleted file, the best possible method is to restore it from its backup. But if user need to recover a file that hasn't been backed up, DOS's UNDELETE and NU's UNERASE may be his best recourse.

1.2.1.1 DOS UNDELETE Command

UNDELETE restores files that were previously deleted by using the <DEL> command. It offers three levels of protecting files against accidental deletion: Delete Sentry, Delete Tracker, and Standard

- Delete Sentry

Delete Sentry provides the highest level of protection to ensure that user can recover deleted files. This level of protection creates a hidden directory named SENTRY. When user deletes a file, UNDELETE moves the file from its current location to the SENTRY directory without changing the record of the file's location in the file allocation table (FAT). If user undeletes the file, MS-DOS moves the file back to its original location.

The size of the SENTRY directory and its files is limited to approximately 7 percent of hard disk space. If user deletes a file and the directory and its files exceed this limit, UNDELETE purges the oldest files until enough space has been freed to accommodate the newly deleted file.

In addition to the disk space needed for the SENTRY directory, Delete Sentry requires 13.5K of memory for the memory-resident portion of the UNDELETE program.

♫ Delete Tracker

Delete Tracker provides an intermediate level of protection. It uses a hidden file named PCTRACKER.DEL to record the location of deleted files. When user deletes a file, MS-DOS changes the file allocation table (FAT) to indicate that the location of the file is now available for another file. User can recover the deleted file provided that another file has not been placed in that location. If another file has been placed there, user is able to partially recover the deleted file.

Delete Tracker requires 13.5K of memory for the memory-resident portion of the UNDELETE program and a minimal amount of disk space for the PCTRACKER.DEL file.

♫ Standard

The standard level of protection is automatically available when you switch on your computer. Of the three levels of guarding against accidental file protection, it provides the lowest level of protection. However, it does not require user to load a memory-resident program. It also has the advantage of requiring neither memory nor disk space.

Using this level of protection, user can recover a deleted file, provided MS-DOS has not placed another file in the deleted file's location. If a file has been placed there, user may be unable to recover all or part of the deleted file.

Method used to recover files

Use any one of the following switches : /DOS, /DT, or /DS. If user do not specify a switch, UNDELETE uses Delete Sentry, if it is available. If Delete Sentry is not available, UNDELETE uses the Delete Tracker file if available. If a deletion-tracking file is not available, UNDELETE attempts to recover files by using MS-DOS.

The UNDELETE.INI file

UNDELETE uses the UNDELETE.INI file to define values when UNDELETE is loaded into memory. If the file does not exist when you load UNDELETE into memory. Undelete creates an UNDELETE.INI file.

The UNDELETE.INI file has five sections : [sentry.drives], [sentry.files], [mirror.drives], [configuration], and [defaults].

The [sentry.drives] section specifies the drives protected by the Delete Sentry method, if used.

The [sentry.files] section specifies the files protected from deletion using either Delete Tracker or Delete Sentry. A hypen (-) before a filename indicates that the file is not saved. The default values defined in the [sentry.files] section are as follows :

```
[sentry.files]
*.*  -*.TMP  -*.VM?  -*.WOA  -*.SWP  -*.SPL  -*.RMG  -*.IMG  -*.THM  -*.DOV
```

The [mirror.drives] section specifies the drives protected by the Delete Tracker method, if used.

The [configuration] section defines the following values :

Whether files with the archive bit set are protected. If files with the archive bit set are not protected (the default value), the entry is as follows :

```
archive=FALSE
```

A TRUE value saves files with the archive bit set.

The number of days files are saved. The default value is days= 7.

The amount of total disk space reserved for deleted files. The default value is: percentage = 20

The [defaults] section specifies the method of file tracking. The following defines the default Delete Sentry method :

```
[defaults]
d.sentry=TRUE
d.tracker=FALSE
```

Syntax of UNDELETE

```
UNDELETE [ [drive:][path]filename][DT¦/DS¦/DOS]
UNDELETE[/LIST¦/ALL¦/PURGE[drive]¦/STATUS¦/LOAD¦/UNLOAD
¦/S[drive]¦/Tdrive[-entries]]
```

Parameter

[drive:][path]filename

Specifies the location and name of the file or set of files user want to recover. By default, UNDELETE restores all deleted files in the current directory.

Switches

/LIST

Lists the deleted files that are available to be recofered, but does not recover any files. The [drive][path]filename parameter and the /DT,

/ALL

Recovers deleted files without prompting for configuration on each file. UNDELETE uses the Delete Sentry method, if it is present. If Delete Sentry is not, UNDELETE uses Delete Tracker, if present. Otherwise, UNDELETE recovers files from the DOS directory, supplying a number sign (#) for the missing first character in the filename. If a duplicate filename already exists, this switch next tries each of the following characters, in the order listed, until the result is a unique filename:

/DOS

Recovers only those files that are internally listed as deleted by MS-DOS, prompting for confirmation on each file. If a deletion-tracking file exists, this switch causes UNDELETE to ignore it.

/DT

Recovers only those files listed in the deletion-tracking file, prompting for confirmation on each file.

/DS

Recovers only those files listed in the SENTRY directory, prompting for confirmation on each file.

/LOAD

Loads the Undelete memory-resident program into memory using information defined in the UNDELETE.INI file. If the UNDELETE.INI file does not exist, UNDELETE uses default values.

/UNLOAD

Unloads the memory-resident portion of the Undelete program from memory, turning off the capability to restore deleted files.

/PURGE[drive]

Deletes the contents of the SENTRY directory. If no drive is specified. UNDELETE searches the current drive for the directory.

/STATUS

Displays the type of delete protection in effect for each drive.

/S[drive]

Enables the Delete Sentry level of protection and loads the memory-resident portion of the UNDELETE program. The program records information used to recover deleted files on the specified drive. If user do not specify a drive, using this switch enables the Delete Sentry level of protection on the current drive. Specifying the /S switch loads the memory-resident program into memory using the information defined in the UNDELETE.INI file.

/Tdrive [-entries]

Enables the Delete Tracker level of protection and loads the memory-resident portion of the UNDELETE program. The program records information used to recover deleted files. The required drive parameter specifies the drive containing the disk for which you want UNDELETE to save information about deleted files. The optional entries parameter, which must be a value in the range 1 through 999, specifies the maximum number of entries in the deletion-tracking file (PCTRACKR.DEL). The default value for entries depends upon the type of disk being tracked. The following list shows each disk size, its default number of entries, and its corresponding file size:

Disk size	Entries	File size
360 K	25	5 K
720 K	50	9 K
1.2 MB	75	14 K
1.44 MB	75	14 K
20 MB	101	18 K
32 MB	202	36 K
>32 MB	303	55 K

Limitations of UNDELETE

UNDELETE cannot restore a directory that has been removed, and it cannot retrieve a file if user has removed the directory that contained the file. If the directory was an immediate subdirectory of the root directory, user may be able to retrieve the directory and its files if he first use the UNFORMAT command to restore the directory and then use UNDELETE to retrieve the files. He must use caution because he can lose data if he use UNFORMAT incorrectly. Usually, UNFORMAT can restore only immediate subdirectories of the root directory. However, when he use UNFORMAT to recover an accidentally formatted disk, UNFORMAT reocvers all root-level files and subdirectory names.

Examples of UNDELETE

The following command loads the memory-resident portion of the UNDELETE program into memory, creates a hidden directory named SENTRY, and specifies that UNDELETE move files user deletes on drive C to that directory :

```
undelete /sc
```

The following command loads the memory-resident portion of the UNDELETE program into memory and creates a PCTRACKER.DEL file to track up to 400 deleted files on drive C:

```
undelete /tc-400
```

1.2.1.2 NU's UNERASE Command

There are three methods of recovering files with UnErase :

♬ By Emergency Disk

♬ Recovering automatically

♬ Manual Unerase

1.2.1.2.1 Emergency Disk

If Norton Utilities are not installed in Hard Disk and user need to restore files then he should not install N.U. on his hard disk as it may overwrite erased files, preventing full recovery in that case. Emergency Disk is used to recover file.

➡ Place Emergency Disk in drive A.

➡ Type A: UNERASE at DOS prompt.

Then select the option Recovering Automatically.

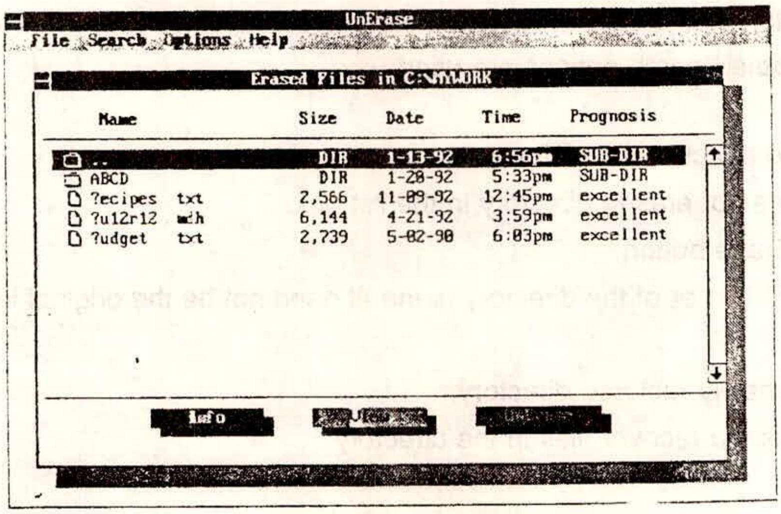
1.2.1.2.2 Recovering file Automatically

➡ Choose UNERASE in the command list on the Norton Utilities main screen.

➡ Unerase then checks for files protected with Smartcan or Erase Protect. If both protections are used it asks the user to select the utility he used to protect the file he wants to recover.

➡ Unerase then displays erased files directories in the current directory and names of existing subdirectories. For each erased file, UNERASE displays the name, size, date and time and prognosis for recovery.

Prognosis is excellent for file protected with Smartcan. Unless user protected the erased file with Smartcan a question mark appears in place of first letter of the file name. Where user erases a file, DOS overwrites the first letter of the filename.



Name	Size	Date	Time	Prognosis
..	DIR	1-13-92	6:56pm	SUB-DIR
ABCD	DIR	1-28-92	5:33pm	SUB-DIR
?ecipes txt	2,566	11-09-92	12:45pm	excellent
?u12r12 wch	6,144	4-21-92	3:59pm	excellent
?udget txt	2,739	5-02-90	6:03pm	excellent

Figure 4 - Unerase Screen

Recovering file/files from a directory

- ➡ Select the Drive and Directory from file menu and select the file to be recovered. Select most important or smaller file first.

- ➡ If number of files are to be recovered they can be marked with arrows by highlighting them and pressing space bar.

- ➡ If the contents of the file to be recovered are to be viewed, choose VIEW ALL DIRECTORIES from File menu. Select the file and View command.

- ➡ Select UnErase Command enter first letter of file name if ? mark dialog box appears. It need not be the original letter any letter will do. If the file was protected with Smartcan first letter is preserved and Unerase the file.

Recovering files in Erased Directories

Each file on disk has a directory entry that stores important information about the file. If the directory containing the erased file is itself erased, the files directory entry remains intact until overwritten.

If the directory name exist in list box it can be recovered directly but if it is overwritten and it is not traceable Search options are used.

Recovering Erased directory and Files in it

- ➨ Select Names of erased directory in the list box.
- ➨ Select UnErase button.
- ➨ Enter the first letter of the directory name. It need not be the original letter. Any letter will do.
- ➨ Change to newly restored directory.
- ➨ Use UnErase to recover files in the directory.

To recover a file in an erased directory that user could not automatically recover

- ➨ Choose FOR LOST NAMES from the Search Menu. UnErase begins searching for Lost names and you can view the found files and use unerase to recover.
- ➨ If the file is not found use UnErase Search Options. It searches for erased files containing specific type of data you want to recover for a specific text string.

1.2.1.2.3. Recovering with Manual UnErase

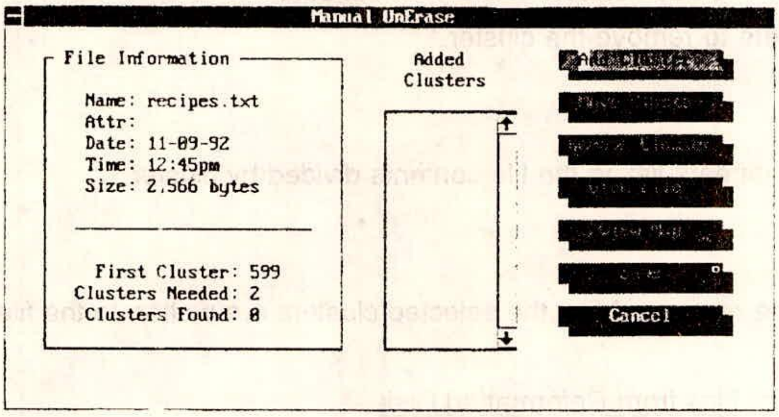
If automatic recovery was unsuccessful, or the data recovered is not in right order, then Manual UnErase is used.

- ➨ Select file you want to recover
- ➨ Choose Manual Unerase from file Menu
- ➨ Enter first letter of file name. It need not be the original letter any letter will do.
- ➨ Manual Unerase dialog box appears as shown in Figure below:

File Information

It lists the first cluster, the cluster needed, and the clusters found for this file. User should use found cluster as a base that he can add to and subtract from to reconstruct the file.

In reconstructing the file user should try to get the clusters found as close as possible to the clusters needed.



Name: recipes.txt
Attr:
Date: 11-09-92
Time: 12:45pm
Size: 2,566 bytes

First Cluster: 599
Clusters Needed: 2
Clusters Found: 0

Figure 5 - Manual Unerase dialog box

Add Clusters

It adds cluster not in use by existing file. It has five options :

♬	All clusters	: Add all of the most likely clusters.
♬	Next probable	: Add the next most likely cluster.
♬	Data Search	: Find the cluster containing key text.
♬	Browse	: Browse for clusters to add.
♬	Cluster number	: Enter the cluster number directly.
♬	Cancel	: Do not add any clusters.

Move Cluster

➨ Select the cluster to move in the added cluster list box Press Spacebar to mark it with arrows.

➨ Press UpArrow or Down Arrow to reposition the selected cluster.

➨ Press Enter to drop the cluster in the new location.

Remove Cluster

➨ Select the number of the cluster to delete in adeded cluster list. Cluster number appears above each cluster in the view list box.

➨ Press Delete to remove the cluster.

View File

➨ A screen appears listing the file contents divided by cluster.

Save

➨ It saves the recovered file, the selected clusters are written to the file.

1.2.2 Recovery of files from Reformatted Disk

Suppose that user has formatted a disk. As he take it out of the drive and see the label - uh oh! Its the wrong disk. No fear, he can use the UNFORMAT command.

Unformat Command restores a disk that was erased by using the FORMAT command.

Background

The information on disk is stored in two areas :

♬ System area

♬ Data area

System area : It contains book keeping information - the boot record, the file allocation table (FAT), and the root directory that DOS uses to find files on disk.

Data area : It contains the actual data in files.

The FORMAT command reinitializes the system area but does not overwrite the data area. Even though the disk appears to be empty when user uses DIR command.

Application

♬ It recovers a hard disk that has been accidently reformatted.

- It restores a floppy disk that has been formatted with safe format or DOS versions 5.0 or later.
- Rebuild a disk that has been corrupted due to a power failure.
- Rebuild a disk that has been damaged by a virus.

Unformat can be done either by

- DOS Unformat Command
- Norton Utilities Unformat Command

When Unformat command is run it searches the disk for lost book keeping information stored in file called IMAGE.DAT created by Norton Utilities Image Program or MIRROR.FIL created by DOS Mirror program. These programs take a snapshot of the critical system information area of Hard Disk. Recovery process is faster with Image or Mirror file. However, Unformat can recover data without either of these files but it may not completely recover all files. At a minimum root directory will be lost. In some cases user might not get any useful data.

1.2.2.1 DOS UNFORMAT Command

➡ Type UNFORMAT Command at DOS prompt. Its syntax is as follows :

```
UNFORMAT drive : [/L][TEST][/P]
```

Parameter
drive : specifies the drive that contains disk on which to recover files

Switches
/L
List every file and subdirectory found by Unformat.
If this switch is not specified it lists subdirectories and files that are fragmented. To suspend scrolling of displayed list press CTRL+S; to resume scrolling press any key.

/Test
Shows how UNFORMAT would recreate the information on the disk, but does not actually unformat the disk.

/P
Sends output message to the printer connected to LPT1.

Example of DOS UNFORMAT

UNFORMAT a:/test
Determines whether unformat can restore a disk in drive A.

UNFORMAT a:/L
To restore a formatted disk in drive A, listing all files and subdirectories.

1.2.2.2 Norton Utilities UNFORMAT Command

- Choose Unformat in the command list on Norton Utilities Main screen
- Select the drive to recover from the drives list box.
- UNFORMAT asks if user has used Image or the DOS Mirror program to create a copy of system and of disk. If user is sure select YES, if he is not sure a list of files currently stored in the root directory on selected drive is displayed along with a message.

  "Are you sure you want to Unformat it ? Select Yes to continue.

- Unformat finds two copies of Image file user can select most recent version or the previous version depending upon requirement.

e.g. If disk damage had occurred late in the day and it is noticed next day when computer is booted. If Image is included in AUTOEXEC.BAT file, Image automatically updates a copy of damaged system area when user started his computer, thus making the most recent version of IMAGE.DAT unusable. Thus in this case select previous to restore the previous version.

➨ Select Full or Partial restoration. Select Partial restoration when user knows what exactly the problem is.

When Unformat finishes reconstructing disk, the program advises user to run Norton Disk Doctor to clean up any disk problem that might have occurred due to changes made on the disk after IMAGE.DAT file was created.

To start system with recovered disk but if it does not work use Disk tools to make the disk bootable.

Limitations of UnFormat

♫ If the Format command was used with the /U switch UnFormat cannot restore the disk to its previous condition.

♫ If Unformat finds a file that appears to be fragmented it cannot recover the file because it cannot locate the remaining portions of the file.

♫ If UnFormat does not prompt you for a specific file, that file is most likely intact. In certain circumstances Unformat may not recognize that a file is fragmented, even though it has located a portion of the file, hence information is lost.

♫ In some older versions of DOS, including COMPAQ 3.1 and AT&T DOS version 2.11, actually overwrite the existing information when they format a Hard Disk so UnFormat will not work under these operating systems.

♫ Floppy disk formatted with safe format or DOS versions 5.0 or later can only be restored.

1.2.3 Other Recovery Utilities

Some more recovery utility programs in NU are described briefly in the following section :

1.2.3.1 File Fix

File Fix diagnosis problems in damaged or unopenable dBASE, clipper, Excel, Lotus 1-2-3, Quattro Pro, Symphony, Word Perfect, or data files compatable with these applications.

File Fix examines the file, rebuilds an error-free copy and recovers as much data as possible. It checks disk for cross-linked files or any other errors in the fle allocation table and directory area. If the disk is damaged an error message appears when user attempt to fix a file and recommends user to run Norton Disk Doctor on the disk that contains the file.

1.2.3.2 Disk Tool

Disk tool is a set of four utilities that perform disk management and recovery operations.

- Make a Disk Bootable
- Recover from DOS's Recover
- Revive a Defective Diskette
- Mark a cluster

1.2.3.3 Norton Disk Doctor (NDD)

NDD for DOS runs numerous tests to determine the health of disk. It warns user if problems are found and give options of correcting them. Test and corrections are performed automatically. When test is complete a report is generated about disk. User can print report and undo any changes NDD performs.

1.2.3.4 Rescue Disk

Rescue Disk creates a rescue disk unique to user computer. If the user losses his system configuration stored in CMOS RAM (Complementry Metal-Oxide Semiconductor RAM) it can be restored from rescue disk. In absence of system configuration computer when booted will give error message "Hard drive not fund", "Missing operating system" or "Non-DOS disk error" and user cannot access his hard disk.

2. UNTRACEABLE FILES

There might be a situation when user need to access file but he doesn't know where they are located or he knows some of the text it contains but can't remember its filename. In order to trace such untraceable files DOS and NU both provide some utilities.

2.1 Tracing files with DOS DIR command

User can give the following command at the root directory or any other desired directory prompt to trace a particular file.

```
C:\[filename]/s/p
```

The filename could be the full file name of the file that you want to trace. In case user don't remember the exact filename, he can still search the file by using the wildcard characters * and ? with one probable alphabet of the file or with the extension. The command will search all the files having that particular alphabet in the name or that particular extension.

The switch /s lists every occurrence, in the specified directory and all subdirectories, of the specified file except the system and hidden files.

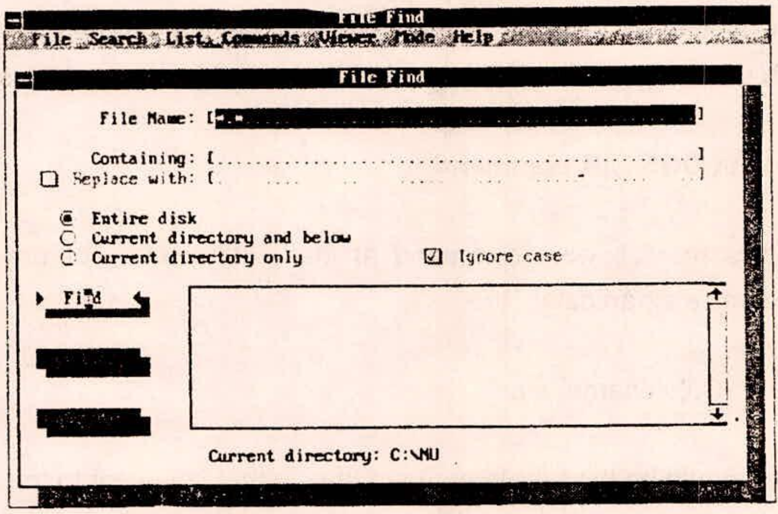
The switch /p displays one screen of the listing at a time. To see the next screen, press any key.

2.2 Tracing files with NU FILE FIND command

File Find (FILE FIND) locates files by searching through all the drives and directories on one or more disks. File Find also finds hidden or system files not displayed by the DOS DIR Command, and creates batch files that operate on the files it finds. With File Find, user can perform a simple filesearch using the Standard DOS wildcard characters * and ? User can also perform an advanced search by specifying a files data, size and attributes.

Once File Find locates a group of files, user can change their attributes, data stamps or time stamps. File Find also includes a search and replace feature that lets user replace text contained in one or more files.

➡ Choose File Find from Norton Utilities main screen or type FILEFIND at the DOS prompt. The File Find screen appears as shown in Figure below:



File Name: [ ]

Containing: [...]

□ Replace with: [ ]

● Entire disk
○ Current directory and below
○ Current directory only

☑ Ignore case

Current directory: C:\NU

Figure 6 - The File Find screen

File Name

- Enter the file name in file name text box. If the user does'nt know the file name but knows some of the file contents, enter text string. User can uncheck the Ignore case check box to make text search case-sensitive.

Replace text within a file or group of files

- Enter the text to search for in the containing text box.
- Check the Replace with Check box and
- Enter the replacement text string in the Replace with text box.
- The view command button changes to Replace.
- Select Find to begin the search.

Specify Scope

- Specify appropriate, option button to specify where File Find should search for the file.

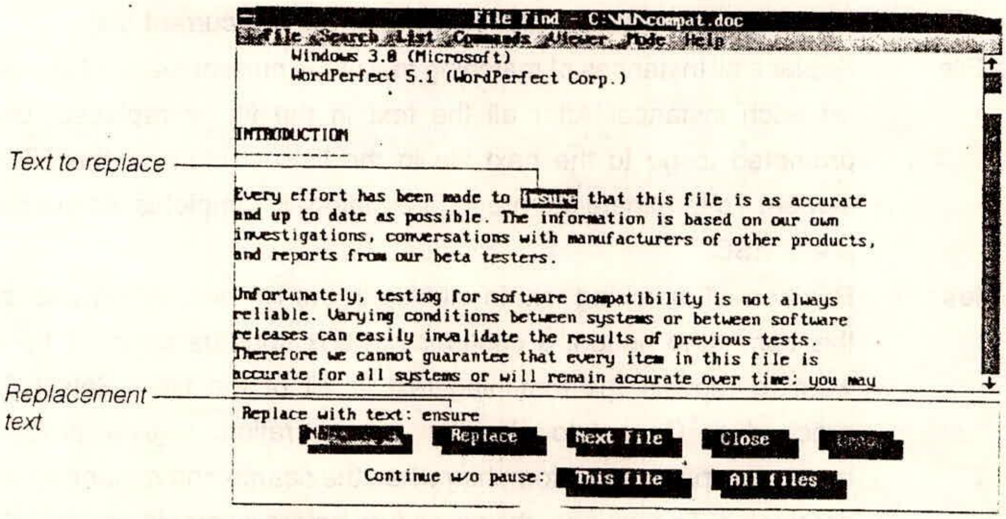
♫ Entire disk

♫ Current directory and below

♫ Current directory only

To view the contents of a file

Co ntents of file can be viewed by highlighting the file in list box and select view. The view screen appears as follows :



File Find - C:\MI\compat.doc
File Search List Commands Viewer Mode Help
Replace
Next File
Close
This file
All files

```
     Windows 3.0 (Microsoft)
     WordPerfect 5.1 (WordPerfect Corp.)

INTRODUCTION
------------

Every effort has been made to ensure that this file is as accurate
and up to date as possible. The information is based on our own
investigations, conversations with manufacturers of other products,
and reports from our beta testers.

Unfortunately, testing for software compatibility is not always
reliable. Varying conditions between systems or between software
releases can easily invalidate the results of previous tests.
Therefore we cannot guarantee that every item in this file is
accurate for all systems or will remain accurate over time: you may

Replace with text: ensure
Continue w/o pause:
```

Text to replace

Replacement text

Figure 7 - The File Find search and replace display

The file displayed is in ASCII format by default and can be changed to HEX from the Mode menu.

➨ No Change : Move to the next instance of matching text without changing the current one. This button changes to Stop when user perform a search and replace operation on a file or files using This File or All Files command button.

- Replace : Change the currently highlighted matching text and move to the next instance.
- Next File : Move to the first instance of matching text in the next file in the list, without changing any remaining matching text in the current file.
- Undo : Change the last instance of replaced text back to the original search text. User can undo up to 1000 replacements for each file in the list this command button.
- Close : Terminate the replace operation and return to the File Find screen. If user has replaced any text in the current file, a confirmation message appears asking if he wants to save the changes. Select OK to save the file with all changes, or Cancel to return to the current file.
- This File : Replace all instances of matching text in the current file without pausing at each instance. After all the text in the file is replaced, user is prompted to go to the next file in the list or return to the File Find screen. To terminate the procedure before it completes, select Stop or press ESC.
- All Files : Replace all matching text in all files in the list box. When user select this command button, a confirmation box appears asking if he really want to replace the matching text in all of the files. Select OK to proceed or Cancel to abandon the operation. If user proceed, a message appears to inform him when the search and replace operation completes. To terminate the procedure before it completes, select Stop or press ESC.

File Pull Down Menu

For more control both during and after a search, use the commands in the File Find pull-down menus.

The File Menu

- Drive : Change to a specified drive.
- Directory : Change the current directory.
- Exit : Quit File Find

The Search Menu

- ➡ Search Drives : Select multiple drives to search.
- ➡ Advanced Search: Specify multiple search criteria. Searches can be performed by file date, size, attribute, or, for network searches, owner. User can also narrow a text search by specifying how much of a search string to look for : all matching text (including partial words), the full search string only, or prefixes or suffixes only.
- ➡ Hex Strings : Search for (and optionally replace) hexadecimal strings within a file.
- ➡ MAKE BACKUP FILES : Make backup copies of all files changed during a search and replace. The backup files retain the original filenames, but the file extensions are preceded by a curly brace ({). For example, the backup file for WORK.DOC would be named WORK.{DO.

The List Menu

- ➡ Set List Display : Specify how to display found files, including the amount of file information shown, the sort criterion, and the sort order.
- ➡ Print List : Print the list of found files to a printer or file after a search completes. User can specify the amount of file and summary information to print, including the number of occurrences of search text in each file, the total number of files listed per directory and the total disk space they use, and the totals for the entire list.
- ➡ Create Batch : Create a batch file to perform selected operations on the list of found files after a search completes. specify the name of the batch file, the commands to be performed on the files, and additional parameters for those commands (for example, the COPY command before the found files and A: after them would copy them all to a floppy disk). User can also specify which commands to perform on the listed directories.

The Commands Menu

- ➡ Set Attributes : Set or clear a combination of file attributes for the selected file or group of files.
- ➡ Set Date/Time : Set the date and/or time stamp for the selected file or list of files. The current date and time is the default.
- ➡ Target Fit : Determine if the found files will fit onto a target drive.

The Viewer Menu

- ➡ Previous Match : Find the previous instance of matching text (search and replace only).
- ➡ Next Match : Find the next instance of matching text (search and replace only).
- ➡ Previous File : View the previous matching file. This command is available only after files have been found.
- ➡ Next File : View the next matching file. This command is available only after files have been found.

The Mode Menu

- ➡ Search : Return to the File Find screen.
- ➡ View ASCII : View a file's contents in ASCII text format.
- ➡ View HEX : View a file's contents in hexadecimal format.

3. VIRUSES

3.1 What is a Computer Virus ?

A computer virus is a software program. Like all programs, it runs in memory and is stored in a file. A computer virus can be part of an existing file or a file on its own, or it can hide in system areas of the disk. The instruction in a virus program serve two purposes : to modify the files or system configuration in some way and to enable the file to copy itself onto another disk or computer.

3.2 Types of computer virus

Computer viruses found under DOS can be classified as :

- ♬ BOOT or PARTITION infecting viruses
- ♬ Executable FILE infecting viruses
- ♬ MULTI-PART viruses
- ♬ DIRECTORY infecting viruses

All the above virus types can be further classified into two types :

♬ Resident, and

♬ Non resident

Resident viruses are those which on execution install their code in memory and infect other programs or disks from there. The other, non-resident viruses, do not install themselves in memory but spread when an infected program is run or an infected disk is used to BOOT the system.The resident viruses normally infect program files after they are installed in memory and hence are termed as Indirect Action viruses. On the other hand, the Non-Resident viruses infect other program files the moment they get control and are therefore called Direction Action viruses.

3.2.1 BOOT/PARTITION Viruses

The boot sector in the first physical sector of a floppy disk that contains the code (program) to load and start the operating system when user turns on his computer. For any hard disk, the first physical sector contains the PARTITION TABLE also called as the Master Boot. The Master Boot interprets the partition information, locates the normal BOOT sector, reads the normal BOOT into system memory and transfer control to it which in turn starts up its specific operating system.

A BOOT/PARTITION virus replaces the disks original BOOT sector with its own, and loads the virus into memory.

3.2.2 File Viruses

All viruses that modify executable (program) files to replicate are classified as file infecting viruses. Under the DOS environment, any file which has an extension of BAT.COM or EXE in executable and can be infected by the file viruses.

3.2.3 Multi-Part Viruses

Multi-Part viruses have the ability to infect both the executable files as well as the BOOT. These viruses are slightly more dangerous because they require user to check for, and to remove, them from both the places they have the capability of infecting. If user forgets to remove the virus from the infected files, it will come back to the BOOT as well and vice-versa.

3.2.4 Directory Viruses

The directory infecting viruses using undocumented DOS structures and peculiarities manages to point the start of every executable file (based on the COM or EXE extension) to an area of the disk where the virus code is written.

The moment user tris to run any program, the virus gets control first, does whatever it is programmed to do and then loads the original programs and lets it execute in a normal fashion.

The net result is that the virus in no way modifies the actual program files or the BOOT and yet manages to infect entire drives within seconds and the time taken is merged with normal DOS activities making it almost un-noticeable.

3.3 Phases of Virus Infection

Computer viruses can be considered to have different phases of infection. Initially, it remains dormant and does nothing to arouse the users suspicion. For example, if user uses an infected program, and nothing abnormal happens, then he would feel safe using the infected program and the virus gets a chance to propagate. During the propagation phase, the virus infects other programs and has a chance to spread onto other systems via diskettes, communication links, etc. After this comes the triggering phase. The trigger in some condition which can be tested logically by the virus code. It could be a particular date or time or number of infections performed or any other logical condition. After the virus has been triggered, it causes the desired damage it was meant for.

3.3.1 How do Viruses Infect ?

♫ BOOT

♫ EXE & COM Files

♫ DIRECTORY

3.3.1.1 Infecting the BOOT

Most BOOT viruses infect the BOOT Sector of floppy diskettes and the MASTER BOOT sector (PARTITION) of hard disks. Infection of the BOOT is normally a very simple process. Generally, the virus will copy the original BOOT Sector to some other predefined area of the disk and copy itself over the actual BOOT. This predefined area could be anywhere. It could be a sector in the directory area which would destroy any file entries in that area, or it could be a sector in the FAT (File Allocation Table) effectively destroying any file linkage chains in that area. The reason behind keeping a copy of the original BOOT sector is to preserve the original functionality of the disk in order to avoid early detection and eradication of the virus.

An important point to be noted here is that a BOOT Virus can spread infection only if it is active in the system memory or when user attempts to BOOT off a diskette or a hard drive which is already infected by a BOOT virus. He cannot get a BOOT virus infection just by looking at the infected diskette's Directory.

3.3.1.2 Infecting the Files

There are two basic formats for executable programs, that is, the COM and EXE format as per the extensions of the programs.

♫ COM Format Programs

The COM format for programs is quite simple as it is a direct binary image of the program in memory. All that the OS (operating system) has to do is, load the COM format program into memory and transfer control to the Start of the file image in memory.

The virus infecting a COM file usually saves the original program size and the first 3 or more bytes of the start of the original program. The virus saves only the first 3 bytes (or more) because it attaches its code to the end of the original program and changes the first 3 bytes to a JUMP instruction which transfers control to the virus code first whenever the inected program is run. The virus, after doing whatever it was programmed to do, replaces these three bytes back to the start of the original program in memory and JUMPS right back to it. This preserves the original functionality of the infected program and makes it more difficult to detect the virus at an early stage.

This is the most general technique that computer viruses use while infecting COM format programs. There could be other possibilities also but the general idea remains the same, and that is to modify the program in such a manner that after infection, the virus code gets a chance to execute first.

♫ EXE Format Programs

The EXE format programs contain a HEADER called the EXE Header at the start of the program file. This header contains all the information required by DOS to load and execute the program.

The EXE Header is basically a variable size record which is attached to the start of an EXE format program by the LINK program based on the information contained in the different OBJECT MODULES and LIBRARIES.

Any virus which infects an EXE file attaches its code after the end of the EXE file and changes the information in the EXE header to reflect the new starting position of the program which would transfer control to the virus code whenever the infected program is run. The virus preserves the original values from the EXE header which were modified in order to maintain the original program functionality.

3.3.1.3 Infecting the Directory

The directory infecting virus infects the directory entries of executable files.

For any DOS formatted disk, there is a predefined area set aside for the directory entries. This area is put aside when user first formats any disk under DOS. These entries are updated as and when required. A directory entry under DOS consists of 32 bytes a piece. These 32 bytes contain all the information required by DOS as far as starting point for any file is concerned. The structure of a directory entry is tabulated in the following table.

As seen in the table, the start of all the files is also stored in the directory entry for that file. What the directory infecting virus has to do is to modify this entry so that it points to the start of the Virus code and infection would take place.

As in the previous cases, the virus has to somehow preserve the original start of the file so that it can maintain the original functionality of the infected program. One place which might seem to be an obvious choice for storing the original start of the file would be the reserved (unused) 10 bytes in the directory entry.

Offset	Size	Contents
00	8 BYTES	File name
08	3 BYTE S	File extension
11	1 BYTE	File attribute. This is the byte which is used for special marking of a directory entry. This marks out the normal files, hidden files, the volume label file, read only files, directory entries or a system file.
12	10 BYTES	Reserved (Undocumented) by DOS
22	2 BYTES	File time stamp
24	2 BYTES	File date stamp
26	2 BYTES	file start point. This is actually the cluster number of the first cluster of the file, and this is what the virus will have to modify to point to its own code.
28	4 BYTES	File size

3.3.2 Damages a Virus can do.

A list of some possible damages by computer viruses is given below :

♬ Corrupt file allocation table

♬ Erase or corrupt file

♬ Format disk

♬ Redefine keys

♬ Change data in programs or files

♬ Damage hardware

♬ Display a message

♬ Change the screen display

♫ Make sounds through the PC speaker

♫ Copy data elsewhere

♫ Reset the computer

♫ Change file attributes

♫ Encrypt program or data files

♫ Interfere with printing to the parallel port

♫ Print messages on the printer

♫ Lock the keyboard

♫ Cause type errors

♫ Hide data or program files

♫ Selectively delete data

♫ Corrupt directories

♫ Transpose digits in numerical data

3.4 Detection of virus from symptoms.

The damage done by various viruses could be prevented if it is detected at an early stage. In practice, most of the viruses leave tell-tale signs of infections. These signs can either be very obvious or a little involved.

Here some general virus symptoms are presented that user can check for using plain DOS utilities (DOS version 5.0 or higher and a PC having a full BASE RAM of 640 KB).

3.4.1. Memory loss

Base memory error is a common symptom of both BOOT as well as File infecting virus. Most BOOT viruses usually use between 1 to 4 KB of BASE RAM for their own use. For example, if user knows that his system has 640 KB of BASE RAM, and when he looks at the amount of BASE RAM reported by any utility program such as the DOS check disk (CHKDSK) he would see a display like the following :

```
Volume G Drive          created 07-30-1996 3:40p

    310,509,568  bytes total disk space
     30,728,192  bytes in two hidden files
      1,196,032  bytes in 138 directories
    207,052,800  bytes in 4,200 user files
     71,532,544  bytes available on disk

          8,192  bytes in each allocation unit
         53,645  total allocation units on disk
         24,473  available allocation units on disk

        655,360 total bytes memory
        626,384 bytes free
```

Although the exact display and the various numbers and details may vary on account of different systems and DOS versions, the last two lines of interest remain the same. The first line tells the total amount of BASE RAM as seen by DOS and the second line tells the amount of memory left free for programs after DOS has loaded all required device drives etc.

Look carefully at the total bytes of memory. If this number is less than 655360 bytes, then in all probability the system is infected with a BOOT virus.

Now, to detect a file virus, the first step is to BOOT off the hard disk using a minimal or bare configuration.This means that user should not load any device drivers or TSRs from the CONFIG.SYS or the AUTOEXEC.BAT respectively. After the BOOT run the DOS CHKDSK program and note the amount of free memory. Now BOOT off the clean DOS diskette using the same minimal configuration and run CHKDSK, again. Now compare the amount of free memory available. If the free memory count does not match then, in all probability, there is a resident (indirect action) file infecting virus on the system's hard disk.

3.4.2 Diskette Activity

The other factor to watch out for is when any floppy diskette is accessed. Consider seeing a DIRectory of a diskette. When user gives a DIR A: or B: command, the DIRectory listing appears after a perceptible pause. In other words, the DIRectory listing itself will display as quickly as before, but the time between the DIR command and the DIRectory listing start, will be slightly longer than normal. In some cases, the DIRectory listing itself will appear slowly and will take a longer time to complete the display. These symptoms may point to a BOOT virus being resident in the system. One may also occasionally notice the floppy disk drive going on even when the drive is not accessed. For example, one might suddenly see the floppy disk drive light turn on for no apparent reason. This is almost certainly an indication of a BOOT virus infection.

3.4.3 Sluggish System Speed

Yet another symptom that user could watch out for is a sluggish hard disk activity. The hard drive may appear to be unusually slow when a BOOT virus is resident. This system may not be of much use to those who have fast computer systems, but on most of the older and slower systems the speed degradation may be perceptible.

3.4.4 Funny File Names in Directory

This is one of the most common indications of a BOOT virus infection.There are two basic reasons for funny or odd looking file names appearing in directories :

- The presence of a BOOT virus that has already been triggered and caused some damage. The hard disk or floppy disk could be permanently damaged in this case but in some cases, the data present on the drive could be recovered.
- The second reason is when an older BOOT virus infect disk formats that the virus was not programmed for.This generally result in the original BOOT record or a part of the virus code being written to the DIRectory area of the disk. When DOS looks at this DIRectory information, it attempts to interpret and display it in a usable format. This results in the funny or odd looking file names in the DIRectory listing.

3.4.5 Abnormal Program Behaviour or System Crashes

This could be an indication of a BOOT as well as FILE Virus. Normal programs, which were functioning properly (before the virus infection) either start exhibiting abnormal behaviour or tend to crash when you try to run them. This behaviour could be there due to some other reasons also but one should just play safe and check for the virus infection possibility first.

3.4.6 Directory Listing

One of the oldest and most common symptoms of file infecting viruses is found in the DIRectory listing itself. Usually the virus infected files will have either a different file size (larger size) or a different date and time stamp, or both.

The catch here is that user must be familiar with the actual (original) size of the program file or the date and time stamp or both. For example, one of the most commonly found viruses adds 1800 bytes to the size of the infected files .

3.4.7 Program Load Failure

Another visual indication that has a direct link with a lot of file infecting viruses, is displayed by DOS itself. When user tries to run the infected file, he will see a message similar to the one below :

```
Program too big to fit in memory
               or
         invalid format
```

This generally occurs when a virus infects a COM format program file, and the combined size of the original un-infected program plus the virus exceeds the 64KB limit or when a COM infecting virus infects an EXE format file and the size exceeds 64KB or when an over writing virus infects any EXE file which is larger than the 64KB COM format file.

3.4.8 Out of Disk Space

This is not a very uncommon phenomena. A lot of known computer virus today repeatedly infect files. The result is that user runs out of hard disk space for no apparent reason. Of course, it is quite possible that one has actually run out of disk space. But just make sure that this is not caused by any virus.

Although such virus will eventually fill out all available disk space, the DIRectory information will almost always provide a positive identification of this possibility.

3.5 Virus Scanning and Removal

Virus scanners are programs which search system areas as well as program files for known virus infections. Initially, virus scanners used to contain virus signatures consisting of a portion of a virus code which was constant in all infections for that particular virus. If this code sequence was found in the system areas or an executable file, it was flagged as being infected by that particular virus. But this technique sometimes gives false alarm when a program's normal code matches that of a particular signature code. The better virus scanners have graduated to virus pattern matching and fuzzy-logic techniques for detection of virus.The virus scanners are of two types :

- Stand-alone
- Resident

The stand-alone virus scanners are those which are normally run from the DOS command line whenever required to scan a particular disk for virus infection. The resident virus scanners normally would be loaded from the DOS command line or as a DOS device from CONFIG.SYS file.

3.5.1 DOS Anti-Virus Programs

DOS 6's anti-virus programs protect computer systems in two ways : first, they scan memory and disks for resident viruses : second, they monitor all system activity for virus like behaviour. Both procedures take up time in the system and one can tailor anti-virus options to minimize the time or maximize the protection.

3.5.1.1 DOS MSAV Program

The MSAV (Micro Soft Anti Virus) program scans the computer for known viruses. A known virus is one that has already been discovered and analysed by anti-virus specialists. It has a name, such as Stoned or Michelangelo. It also has a signature-a series of bytes contained in the virus program that serve to uniquely identify it. The virus may have several known strains-slight variations of the same basic program. More than a thousand viruses have been identified so far. Many of them haven't been seen for a while and are probably extinct, but there's no way of predicting when or where one will crop up again.

MSAV scans for known viruses by examining memory and disks for the thousand or so known virus signatures. This may take several minutes on a large hard drive. The search could be limited to those areas most likely to be infected by a virus : the partition tables of hard drives, the boot records of disks and program files. Very few viruses hide themselves in other places.

The scanner can remove many known viruses from a disk without damaging the infected files or system areas; this is called cleaning a virus. However, some viruses damage files or system areas when they invade them, and of course, the scanner can't undo the damage. Such files need to be deleted; user can restore them from a backup or reinstall them from their original program disks.

MSAV can clean viruses automatically, warning user when a virus can't be cleaned. It also can notify user when encountering an unknown virus. It detects unknown viruses by looking for changes in program files indicating that they may have been infected by a virus. Most program files don't change after they are installed, so any change at all could indicate a virus infection.

The first time user uses a Microsoft anti-virus scanner on a drive, it creates a file named CHKLIST.MS in each directory, recording the size, attributes, and date/time stamps for all the program files in that directory. It also records a checksum-a unique value calculated from the contents of the file: if the contents change, the checksum changes, and the virus scanner knows that the file has changed, even if the size, attributes, and date/time stamp remain unchanged.

Each subsequent scan compares the recorded data in CHKLIST.MS against the program files. Any difference causes the scanner to report a verify error, and user must decide what to do. User could choose to ignore the change, update CHKLIST.MS with the new data, delete the infected file, or stop scanning.

Many program changes are legitimate. Some programs write in their own program files when user does such things as changing the program options or reconfiguring its screens. User can ignore verify errors for them.

If user updates an application to a new version, the next scan produces verify errors for the changed program files. Because user knows that the program is updated he can ask the scanner to update CHKLIST.MS with its new values.

When user gets a verify error for a program that he has not upgraded or reconfigured, he should pay serious attention to it. User may choose to delete the file right away, or choose to stop the scan while doing some additional investigation and decide what action to take.

Here it must be noted that if an unknown virus already exists in the system when the scanner records the CHKLIST.MS data, it will not be identified. Fortunately, Microsoft's virus monitor (VSAFE), which is described next, can block it from doing any damage.

Syntax of MSAV

```
MSAV [drive:] [/S ¦ /C] [/R] [/A ¦ /L] [/N] [/P] [/F] [/VIDEO]
```

Parameter

drive : Specifies the drive that MSAV scans for viruses. If user does not specify a drive, MSAV scans the current drive.

Switches

/S

Scans the specified drive, but does not remove viruses that MSAV finds.

/C

Scans the specified drive, and removes viruses that MSAV finds.

/R

Creates an MSAV.RPT file that lists the number of files MSAV checked for viruses, the number of viruses it found, and the number of viruses it removed. By default, MSAV does not create a report. When it does create MSAV.RPT, the file is placed in the root directory.

/A

Scans all drives except drive A and drive B.

/B

Scans all local drives except network drives.

/N

Displays the contents of an MSAV.TXT file, if it exists and it is located in the directory that contains the MSAV.EXE file. MSAV then scans the current drive or the drive you specify. MSAV does not use the graphical interface. If MSAV detects a virus, it returns exit code 86 instead of displaying a message on your screen.

/P

Displays a command-line interface instead of the graphical interface.

/F

Turns off the display of filenames that have been scanned. use this switch only with the /N or /P switch.

/VIDEO

Displays a list of the switches that affect how MSAV is displayed.

Example of MSAV

To start MSAV using a black and white color scheme, and to specify that MSAV check all drives except drives A and B, type the following command :

```
msav /bw /a
```

To write a simple batch program named VIRUS that supports the MSAV exit code and the /S switch to scan the current drive, type the following commands by using MS-DOS Editor:

```
echo off
        rem msav command
        if error level 86 go to virus
        if not error level 86 go to none
        :virus
```

```
echo MSAV has detected a virus on your current drive :
go to exit
:none
echo MSAV found no viruses on your current drive.
go to exit
:exit
```

3.5.1. DOS VSAFE Program

Microsoft's anti-virus monitor, called VSAFE, must be loaded as a memory-resident program. VSAFE runs under DOS and uses 22K of memory. It monitors all system activity looking for viruses. Consequently, it slows down the entire system and when security over speed is chosen to load VSAFE. User can compromise by monitoring only activities most likely to be undertaken by a virus, such as modifying a hard disk partition table or doing a physical format on a hard disk.

When VSAFE identifies a suspicious behavior, it blocks the activity and displays an alert box asking user whether to continue or stop. If user knows that the activity is safe-if one is using FDISK to rework the hard disk partition table, for example-user can tell VSAFE to let the activity continue. If not, stop the activity, reboot to remove the potential virus from memory, and run the virus scanner immediately to locate the virus.

Here, it is to be noted that the VSAFE command should not be used when windows is running.

Syntax of VSAFE

```
VSAFE [/options[+ ¦ -]_ _ _ ] [/NE] [/NX] [/Ax ¦ /Cx] [/N] [/D] [/U]
```

Switches

Option

Specifies how VSAFE monitors for viruses. Use a plus or minus sign (+ or -) after the number to turn an option on or off. The following list describes the options user can choose.

1: Warns of formatting that could completely erase the hard disk.The default setting is "on".

2: Warns of an attempt by a program to stay in memory.The default setting is "off".

3: Prevents programs from writing to disk.The default setting is "off".

4: Checks executable files that MS-DOS opens. The default setting is "on".

5: Checks all disks for boot sector viruses.The default setting is "on".

6: Warns of attempts to write to the boot sector or partition table of the hard disk. The default setting is "on".

7: Warns of attempts to write to the boot sector of a floppy disk.The default setting is "off".

8: Warns of attempts to modify executable files. The default setting is "off".

/NE

Prevents VSafe from loading into expanded memory.

/NX

Prevents VSafe from loading into extended memory.

/Ax

Sets the hot key as ALT plus the key specified by x.

/Cx

Sets the hot key as CTRL plus the key specified by x.

/N

Allows VSAFE to monitor for possible viruses on network drives.

/D

Turns off checksumming.

/U

Remove VSAFE from memory.

Using VSAFE with Microsoft Windows

Before installing Windows, turn off VSAFE. If VSAFE is running, user may not be able to complete the Windows installation. If one uses VSAFE with Windows, run the MWAVTSR.EXE memory-resident program by adding the following command to the WIN.INI file :

```
load=mwavtsr.exe
```

MWAVTSR.EXE enables VSAFE messages to be displayed in Windows

Example of VSAFE

To specify that VSAFE not check for formatting that could erase all data on the hard disk, that VSAFE warn of attempts to write to the boot sector of a floppy disk, and that ALT+T be assigned as the hot key to display the VSAFE screen, type the following command :

```
vsafe /1- /7+ /At
```

3.5.1.3 Other Virus Scanners/Cleaners

Some other Anti virus programs which scan as well as clean viruses are listed below:

♬ Mcaffee

♬ Nashot

♬ f-prot

♬ Smartdog

3.6 Virus Prevention Techniques

Prevention is better than cure.

This age old saying still has considerable weight especially when applied to computer viruses.

The ideal protection from virus attacks would be to have a closed system, i.e. a computer system that does not communicate via any means with any other computer system and does not allow any external media for transfer of data or programs.

This situation, although 100% safe, is just not practical.

For any computer system to be of any practical use, it has to communicate with the outside world in some way. The moment a computer system talks to any other system or media like diskettes, the chances of virus infection are always there. The best way to prevent any virus infection is to monitor (scanning) all incoming data into a computer system.

Viruses often travel in the boot sectors of floppy disks. When a disk that comes from another system-whether it's new software or just an old disk borrowed from a friend-one should scan it before booting from it, copying from it, installing a program from it, starting up a program that is on it, or using it in any other way.

Scan new or rented computers as soon as received, because a dealer may not scan a computer before delivering it. It could have been infected in the shop, or in the case of a rental, by the previous user.

One also should rescan the system when exposed to the possibility of a virus invasion.

- If one signs on to a bulletin board service (even a nationally known one such as CompuServe or Prodigy) or any type of on-line service, especially if one downloads something from it.
- If one links the computer to another one via INTERLNK or similar software.
- If one signs on to a network and copy anything from a network drive to one of the local drives or run a program located on a network drive.
- If one restores a file from its backup after deleting an infected version of the file (the backup also may have been infected).
- If one installs or upgrades any software, especially software not sealed in its original package.

***