ERD Commander 2003

User's Guide

Winternals Software LP
3101 Bee Caves Road, Suite 150
Austin, Texas 78746
(512) 330-9130
(512) 330-9131 Fax
www.winternals.com

Table of Contents

1 Introduction

When your Windows NT, Windows 2000, Windows XP or Server 2003 system becomes unbootable and you've exhausted the recovery options available with the operating system, you can rely on ERD Commander 2003 to provide full access to your dead system with a familiar Windows-like environment. ERD Commander 2003 provides the tools you need to help you quickly diagnose and repair the problem that is preventing your system from booting.

Like the Recovery Console of Windows 2000 and Windows XP, as well as the previous versions of ERD Commander, ERD Commander 2003 makes any Windows NT/2000/XP/Server 2003 file system accessible, including FAT, NTFS and CDFS. Unlike those other utilities, ERD Commander 2003 offers both a graphical windowing environment and a command-line console. In addition, ERD Commander 2003 includes a service and driver manager, Registry editor, Explorer-like file system browser, Notepad-like text editor, Event Viewer, and local password changer so that you can gain access to accounts to locked accounts. And when you need to save files to another system on the network or to copy files from another system as part of the repair process, ERD Commander 2003 gives you full access to network file shares.

With ERD Commander 2003, repairing your dead systems has never been easier or more intuitive.

1.1 Overview of Use

ERD Commander's built-in tools allow you to perform many different types of system diagnosis and repair. A few of the ways that ERD Commander 2003 helps you solve problems include:

Removing or Replacing Buggy Drivers

You can use ERD Commander 2003 to delete or replace the image files of drivers or services that, because of a bug or misconfiguration, prevent Windows NT/2000 from booting.

Updating Out-of-Date System Files

Incorrectly applying service packs or system software updates can cause system DLLs to become out of sync with each other. In many cases this can prevent Windows NT/2000 from booting successfully. ERD Commander 2003 can copy up-to-date versions of old files from floppy disks, CD-ROMs, or other computers on your network.

Correcting Misconfigured NTFS or Registry Security

If excessively restrictive security attributes are applied to certain system files or directories on NTFS boot drives, or to some Registry keys, Windows will become unbootable. Using ERD Commander 2003's Explorer and Regedit you can reset permissions on files, directories and Registry keys to regain access.

Updating Locked Files

Once Windows NT/2000/XP/Server 2003 is up and running many system files cannot be replaced because the system keeps them locked. ERD Commander 2003 makes it possible to update such files because it runs when Windows NT/2000/XP/Server 2003 is off-line and the files are not open.

Correcting Registry Problems

A significant number of Windows NT/2000/XP/Server 2003 boot problems are the result of misconfigured Registry values. The ERD Commander 2003 Registry editor has all the capabilities and the same interface as the Windows NT/2000/XP/Server 2003 Registry editor, making it easy for you to inspect and change Registry settings.

Recovering Deleted Files

ERD Commander 2003 includes FileRestore, a utility that you can use to find and restore deleted files from any supported Windows NT/2000/XP/Server 2003 file system format, including FAT, FAT32, and NTFS.

Copying Important Files off of a Dead System

ERD Commander 2003 enables you to access files on a Windows NT/2000/XP/Server 2003 system that fails to boot. You can copy files to removable media such as floppy disks, Zip drives, or Jaz drives, or use ERD Commander 2003's network capabilities to copy them to another system on your network.

Regaining Access to a System That You've Been Locked Out Of

ERD Commander 2003's Locksmith utility allows you to list the accounts for a Windows NT/2000/XP/Server 2003 system and to change their passwords, including Administrator accounts.

Viewing Event Logs

Since the Event Logs of a system often contain clues that can help you diagnose a boot problem, ERD Commander 2003 includes an Event Log Viewer with the same interface as the Windows 2000/XP Event Log Viewer MMC snap-in, allowing you to inspect logs for relevant records.

Running CHKDSK on Corrupt Drives

ERD Commander 2003 will let you check the consistency of hard drives.

Enabling and Disabling Services and Drivers

You can list and modify the start types of a system's drivers and services with ERD Commander 2003's Service and Driver Manager utility. The utility implements an interface similar to the Windows 2000/XP Services MMC snap-in, which makes it easy to identify services and drivers and to disable those that are preventing a system from booting.

Restoring Windows XP Restore Points

Windows XP's Restore Point feature periodically creates snapshots of a system's state that includes system files and Registry data. Overcoming a deficiency of Windows XP's Restore Point functionality, ERD Commander 2003 allows you to restore unbootable systems to a previous Restore Point.

Comparing a Working System with a Dead System

ERD Commander 2003's System Compare utility let's you compare service and driver configuration and the system files of a dead system with that of a live system or a Windows installation media to which you direct it. This enables you to identify differences between working systems and one that doesn't boot in order to guide your repair process.

Partitioning and Formatting Disks

The Disk Management MMC snap-in that ERD Commander 2003 includes in its Computer Management utility has many of the features of the Windows 2000/XP Disk Management MMC snap-in, allowing you to delete, format, and create partitions and volumes. If you prefer a command-line environment you can use the corresponding command-line tool, DiskPart, to accomplish the same tasks.

Scanning a Dead System for Viruses

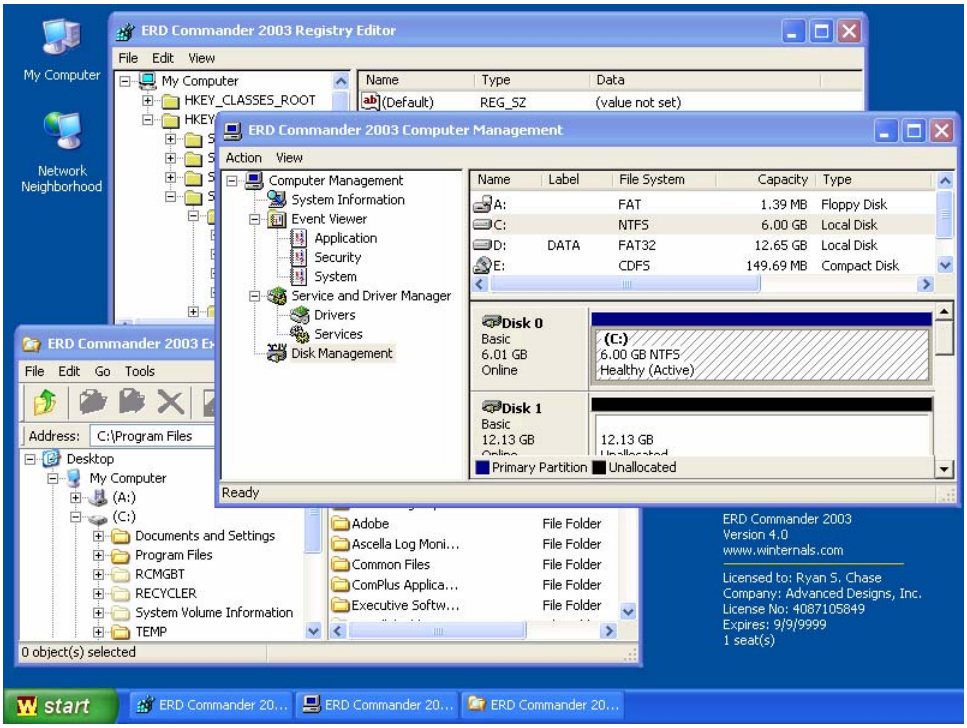
With ERD Commander 2003 you can share the drives of a system on the network so that you can access them from another computer. This allows you to use tools installed on other systems to aid in the repair process. For example, if you suspect a virus has attacked a computer you can shut it down, boot into ERD Commander 2003, share its drives, and then run a virus scanner on the drives from a different system.

Registering COM/DCOM Server DLLs

A system may become unstable if COM or DCOM registration information is corrupted or deleted. The standard Windows COM/DCOM server DLL registration utility, Regsvr32, requires that you be logged into a system into which you are registering DLLs, but ERD Commander 2003's Regsvr32 utility enables you to register COM/DCOM server DLLs into an installation that's offline.

1.2 Sample Screen

This screenshot demonstrates a typical session using ERD Commander 2003 to access the Registry and service configuration of an unbootable system.



2 ERD Commander 2003 Setup

2.1 System Requirements

ERD Commander 2003 requires that the target system have a bootable CD-ROM, and one of the following operating systems:

- Windows NT 4
- Windows 2000
- Windows XP
- Windows Server 2003

Regardless of operating system, ERD Commander 2003 requires a minimum of 64MB of system memory and an x86 233MHz processor.

Note that ERD Commander 2003 also gives you access to the drives of Windows 95, 98 and Me systems, although many utilities, such as the password changer, Registry editor and Event Log viewer do not function when accessing installations of those operating systems.

The ERD Commander 2003 Boot CD-ROM Wizard runs on Windows 95, 98, Me, NT, 2000, XP and Server 2003.

2.2 Booting with ERD Commander 2003

There are two delivery methods for ERD Commander 2003: as a Boot-CD Wizard and as a bootable CD-ROM. You receive the Boot CD-ROM Wizard as an executable file when you download ERD Commander 2003 after an on-line purchase; the version of ERD Commander 2003 that ships as physical media is a bootable image that also includes an installer for the Boot-CD Wizard.

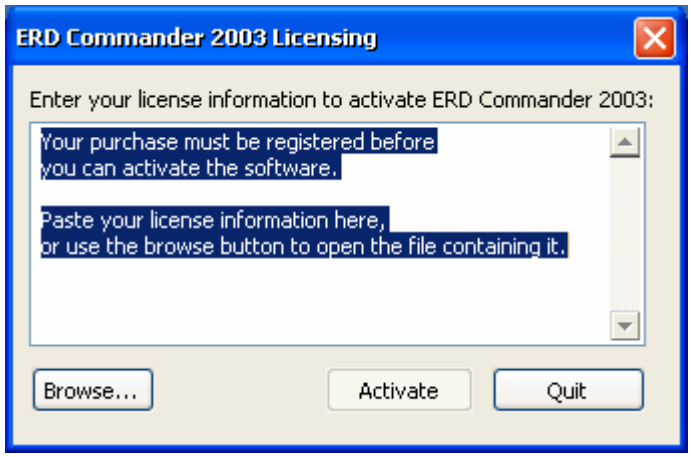
Use the Boot CD-ROM Wizard to create a bootable CD-ROM ISO image. A CD-ROM ISO image is a file that represents the raw contents of a CD-ROM that you can burn onto a writable CD-ROM with most popular CD-ROM burning software. You will need several items in addition to successfully create a bootable CD-ROM from the ISO image the Boot CD-ROM Wizard creates:

- CD-ROM burner
- CDR or CDRW disk
- CD-ROM burning software that supports the formatting of CD-ROMs from CD-ROM ISO images

This section guides you through the use of the wizard to create a CD-ROM ISO image using the Boot CD-ROM Wizard.

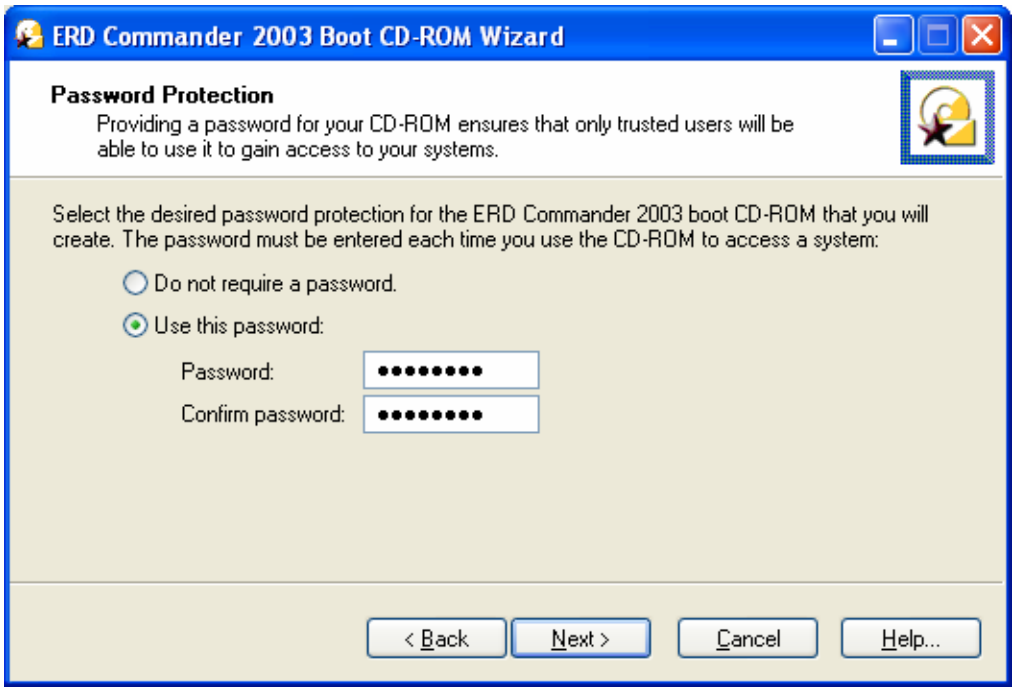
2.3 License

After you start the Boot CD-ROM Wizard you will be presented with a page that requests your licensing information. On-line purchasers receive the licensing information as an e-mail attachment that you can import into the Wizard. The Boot CD-ROM Wizard verifies the license information and embeds it into the ISO image so that, after you create a bootable CD-ROM from the image and start ERD Commander 2003 from the resultant CD-ROM, ERD Commander 2003 presents the licensing information when it starts.



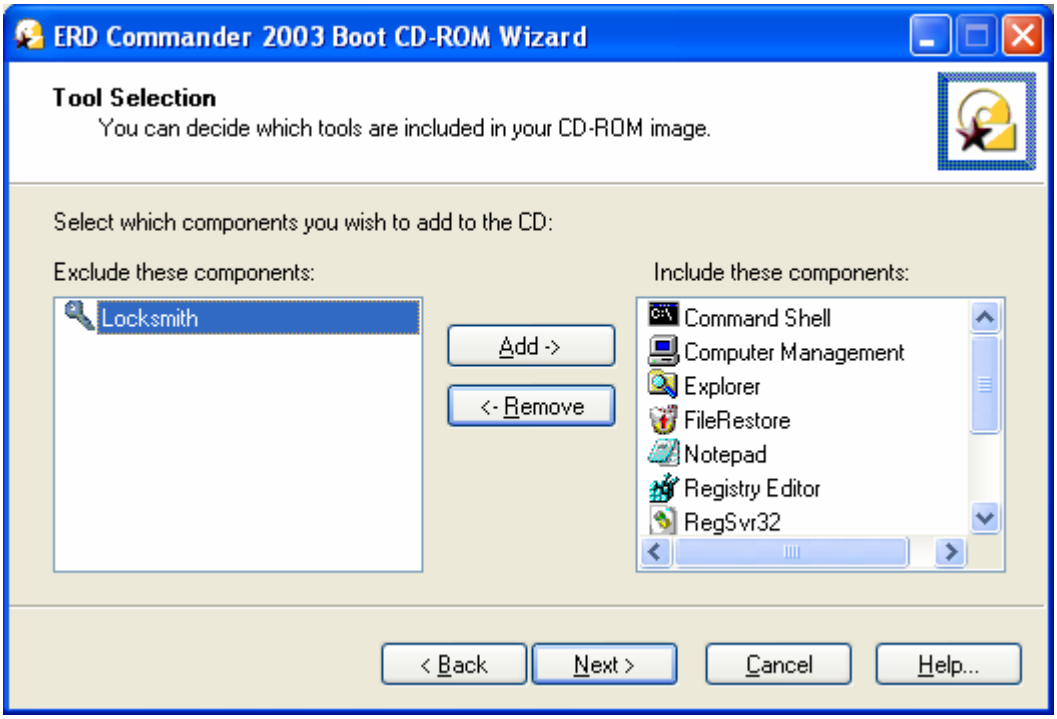
2.4 Password Protection

The Boot CD-ROM Wizard offers you the option to password protect the ERD Commander 2003 CD-ROM that you create. This is useful if you wish to restrict use of the ERD Commander 2003 boot CD-ROM to authorized individuals.



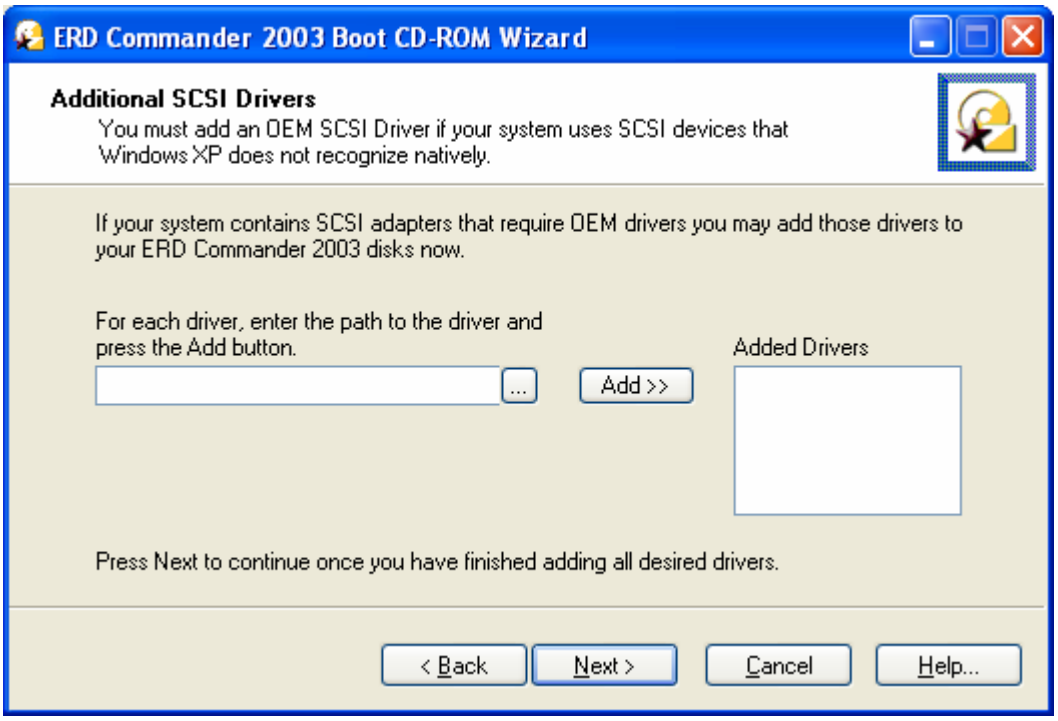
2.5 Selecting the Installed Applications

You can customize the set of tools included on the ERD Commander 2003 CD. For some deployments you may wish to restrict the power of an ERD Commander boot CD by omitting certain tools, for example. Tools that you omit are not included on that instance of the CD-ROM image.



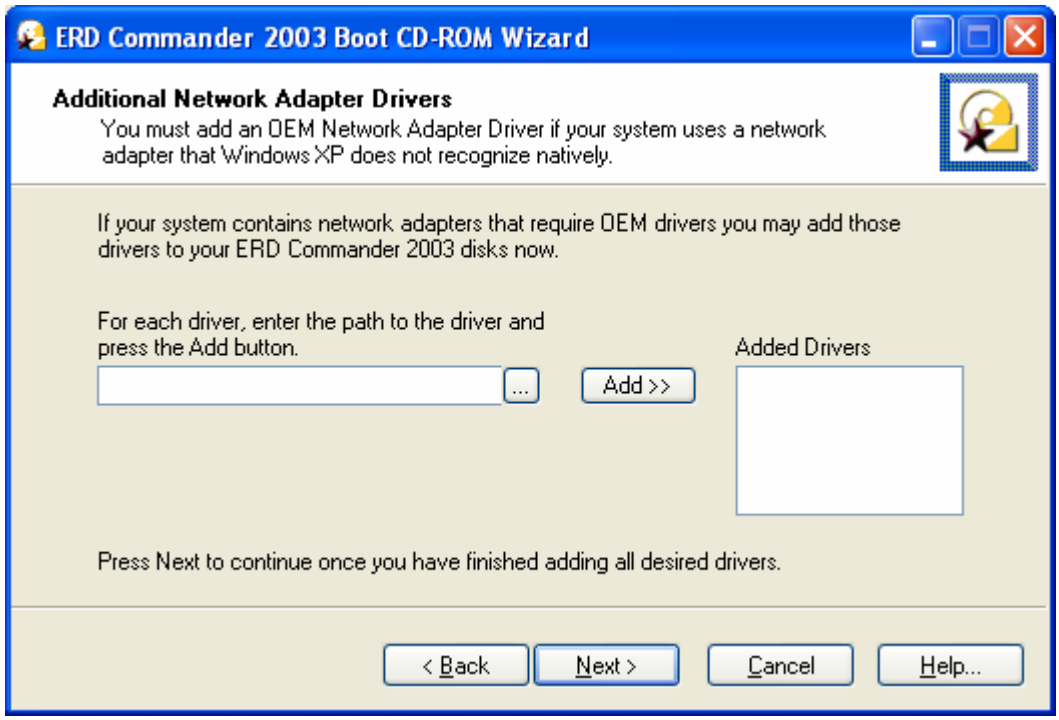
2.6 Adding OEM SCSI Drivers

If you work with systems that use SCSI adapters that Windows XP does not natively support (i.e., hardware that requires additional drivers to be added for Windows XP to use it) then you can add those OEM drivers to ERD Commander 2003. To add an OEM driver, simply enter the path to the driver (the driver file should end in .SYS) or browse to it, and click the **Add** button.



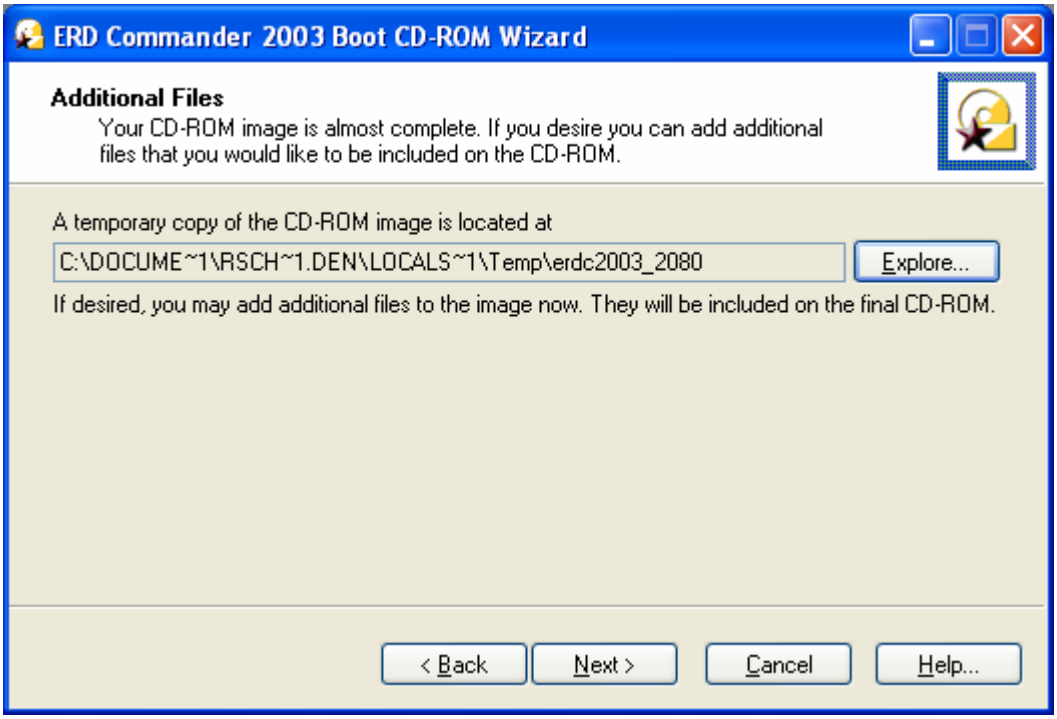
2.7 Adding OEM Network Drivers

If you work with systems that have network drivers that Windows XP does not natively support (i.e., hardware that requires additional drivers to be added for Windows XP to use it) then you can add those OEM drivers to ERD Commander 2003. To add an OEM driver, simply enter the path to the driver's installation file (the installation file should end in .INF) or browse to it, and the **Add** button.



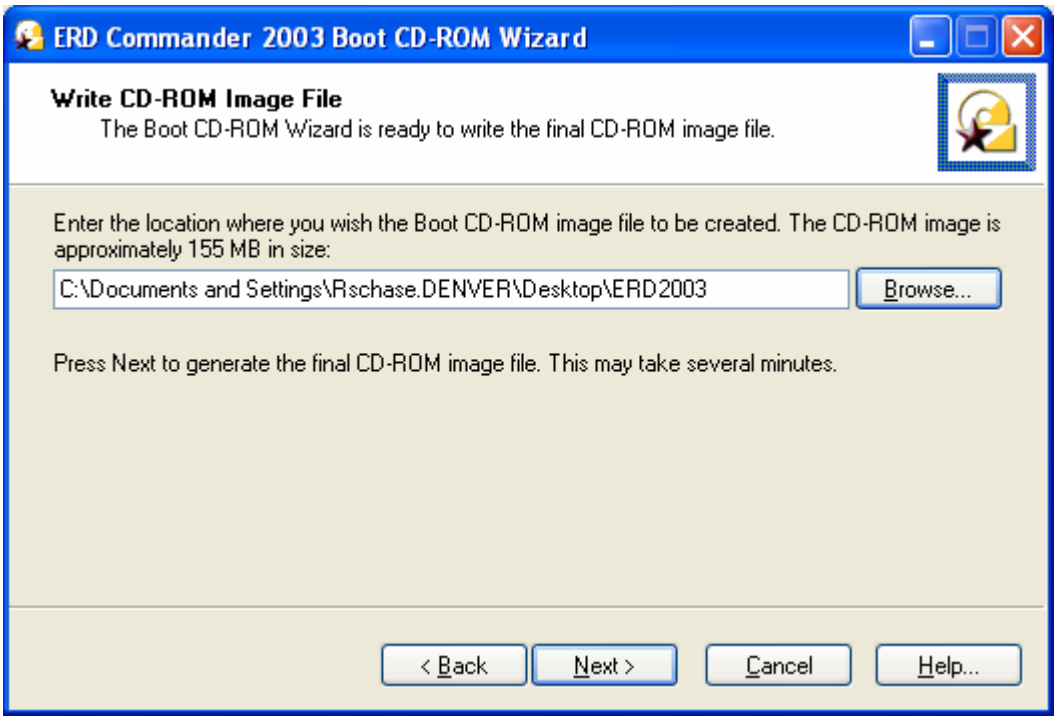
2.8 Adding Files to the CD-ROM Image

Before creating the final ISO image, ERD Commander 2003 gives you the opportunity to add your own files to the image. The Boot CD-ROM Wizard informs you of the location of the ERD Commander 2003 directory tree. Files you add to the tree will be present in the final CD-ROM image.



2.9 Image Location

The Boot CD-ROM Wizard's final interactive step prompts you to specify the destination of the generated ISO image. The image requires approximately 150 MB of disk storage, and because most CD-ROM burning software requires ISO images to have a .iso file extension, the Boot CD-ROM Wizard also requires that extension.



2.10 Burning the ERD Commander 2003 CD-ROM

Most popular CD-ROM burning applications offer the option to write a CD-ROM from a CD-ROM ISO file. Check with your software's documentation for information on how to do this. For additional tips, please check the Winternals Product Knowledge Base:

http://www.winternals.com/support/kbfiles/ISOtoCD.pdf

3 Using ERD Commander 2003

Once ERD Commander 2003 boots, a stripped-down version of Windows XP will start and run the ERD Commander 2003 windowing environment. It's important to keep in mind that, although this graphical environment looks like Windows and even has similar utilities, it is not Windows code and therefore behaves slightly differently. Also note that your end-user license agreement prohibits use of ERD Commander 2003 as a general-purpose operating system, and the environment is designed to reboot automatically 24 hours after starting.

NOTE: *it is important that you do not remove the ERD Commander 2003 CD-ROM from the system while ERD Commander 2003 is running. Doing so could result in a lock-up of ERD Commander 2003, requiring a reboot.*

The ERD Commander 2003 environment provides a number of powerful utilities that help you identify and repair problems that are preventing a system from booting. These include:

- Logon
- Windowing Shell
- System Information
- Explorer
- File Search
- FileRestore
- Command Prompt
- Chkdsk
- Regsvr32
- Notepad
- Regedit

- Service and Driver Manager
- Event Log Viewer
- TCP/IP Configuration
- Disk Management
- Locksmith
- File Sharing
- System Restore
- System Compare
- Disk Commander (available if ERD Commander 2003 is purchased as part of the Administrator's Pak)

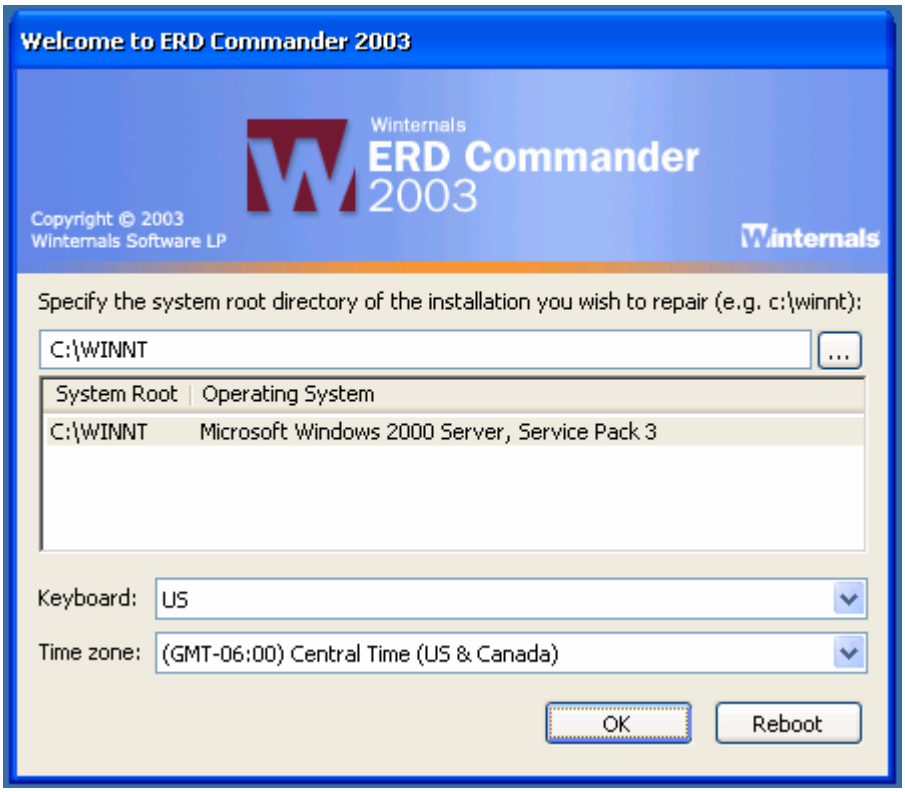
This section describes the functionality and use of each of these tools. In addition, you can execute Win32 applications other than those that are part of the ERD Commander 2003 environment.

3.1 Logon

When ERD Commander 2003 boots it executes the Winternals Logon application. The first step performed by the Logon application is to start the networking services. These services assume that a DHCP server is present on your network and attempt to obtain an IP address. If your network uses static IP addresses rather than DHCP you can use the TCP/IP Configuration utility after logging in to specify a static IP address.

If the ERD Commander 2003 CD was generated by the Boot CD-ROM Wizard, the Logon application next displays the licensing information entered during execution of the wizard. Otherwise it will prompt you to enter ERD Commander 2003 license text or specify a file containing an ERD Commander 2003 license.

Next, the Logon application scans the system's hard-disk volumes for Windows NT, 2000, XP, and Server 2003 installations. It displays the system root directory of located installations, the type of operating system installed, and service pack information. It also allows you to specify the language layout of your keyboard. The default language selection is the one specified by the operating system installation entered in the edit box of the Logon application.



If the system you wish to repair is not in the list or the operating system is displayed as "unknown", then some or all of the Registry hives for that installation are damaged, missing, or have restrictive permissions that do not allow the System account access. Registry hives are the Registry's on-disk storage files and are stored under \SystemRoot\System32\Config (where SystemRoot is the system root directory of a Windows NT, 2000, XP, or Server 2003 installation).

Choose the installation you wish to repair from the list, by manually entering the system root path, or by browsing to the system root directory. When you make a selection the Logon application validates the SYSTEM, SOFTWARE, SAM and SECURITY Registry hives and notifies you if any of them are corrupt or missing. Note that in this event the corresponding portions of the Registry will be inaccessible by the Winternals Registry editor and other ERD Commander 2003 utilities also have limited functionality.

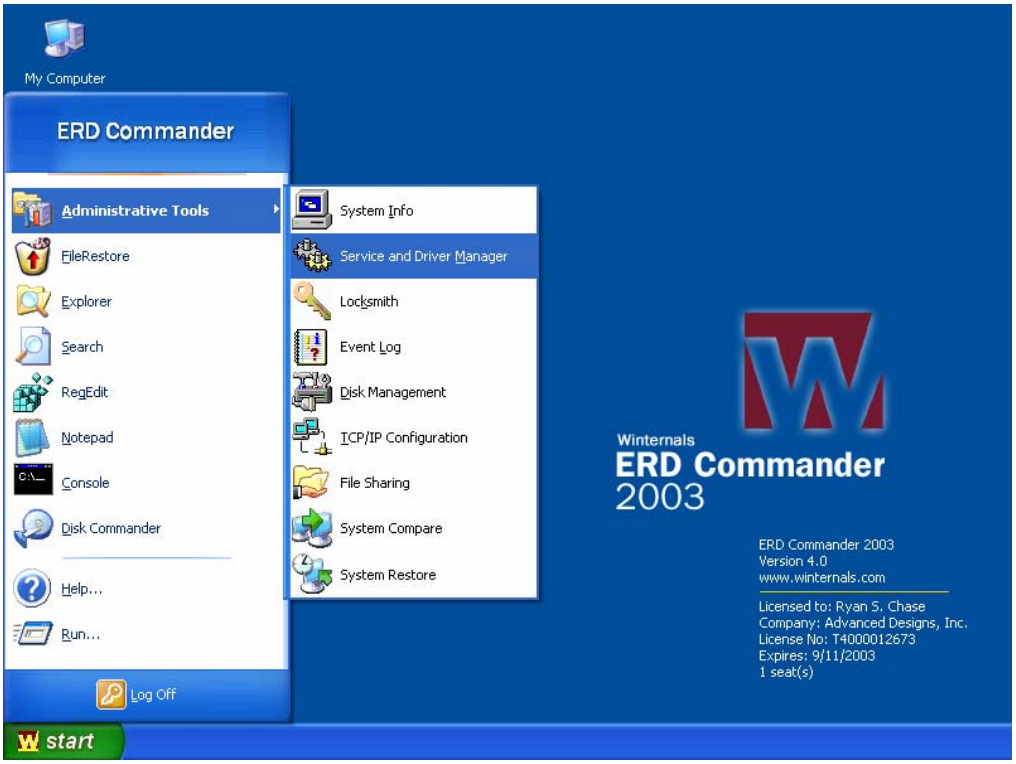
The Logon application allows you to choose a keyboard layout and time zone using the drop down controls. The default selections for keyboard layout and time zone are taken from the installation you have currently entered into the installation selection field if the Registry of that installation is accessible.

Clicking the **OK** button selects the specified installation and starts the ERD Commander 2003 Windowing Shell, described in the next section. After you have completed work on an installation and log off the Windowing Shell you return to this **Logon** dialog. Clicking the **Reboot** button performs a clean shutdown and reboot of the computer.

3.2 Windowing Shell

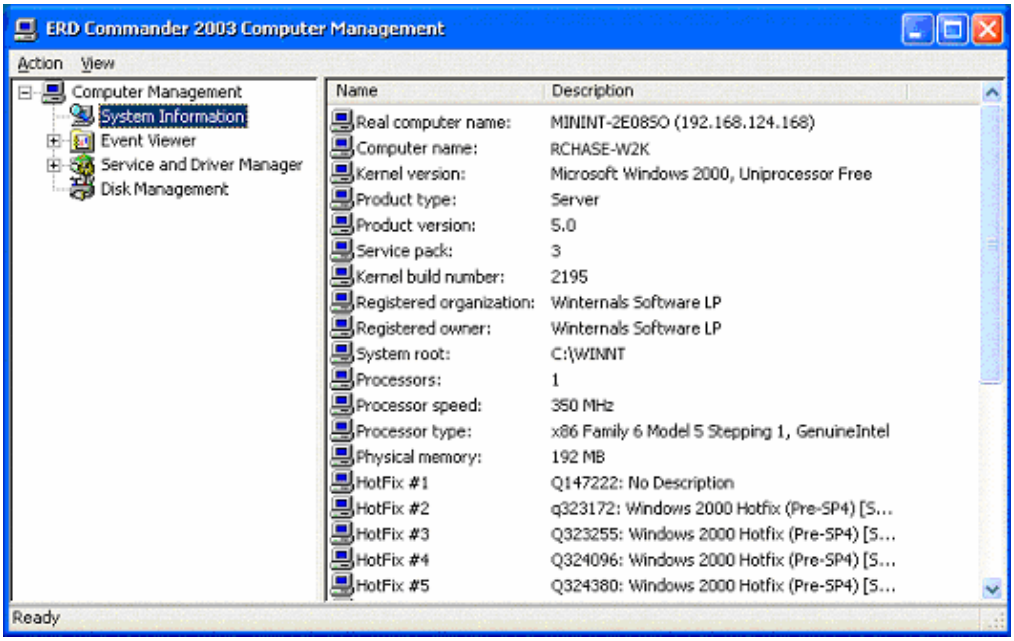
The ERD Commander 2003 Windowing Shell closely resembles Microsoft's Explorer shell. It has a task bar, **Start** menu, and desktop shortcuts. However, you cannot move the Windowing Shell's task bar, edit the items on the **Start** Menu, move or modify existing desktop shortcuts, or create new desktop shortcuts. The Windowing Shell provides the familiar desktop motif and allows you to easily access ERD Commander 2003 applications and manage multiple running applications with taskbar buttons.

NOTE: *a limitation in the ERD Commander 2003 operating environment prevents concurrent execution of more than approximately 4 applications. ERD Commander 2003 will inform you when starting another application might exceed the limit.*



3.3 System Information

The ERD Commander 2003 System Information utility is accessed via the Administrative Tools folder of the **Start** menu. The utility reports extensive information about the system you are repairing, including the operating system version, service pack, hotfixes, registered owner and organization and more. It also displays the installation's computer name as well as the computer name (listed as the "Real computer name") that ERD Commander 2003 randomly assigns while it is running. The value of the System root, which represents the root folder of the installation, can be useful to determine where key system files, such as service and driver files and Registry hives, reside.



3.4 Explorer

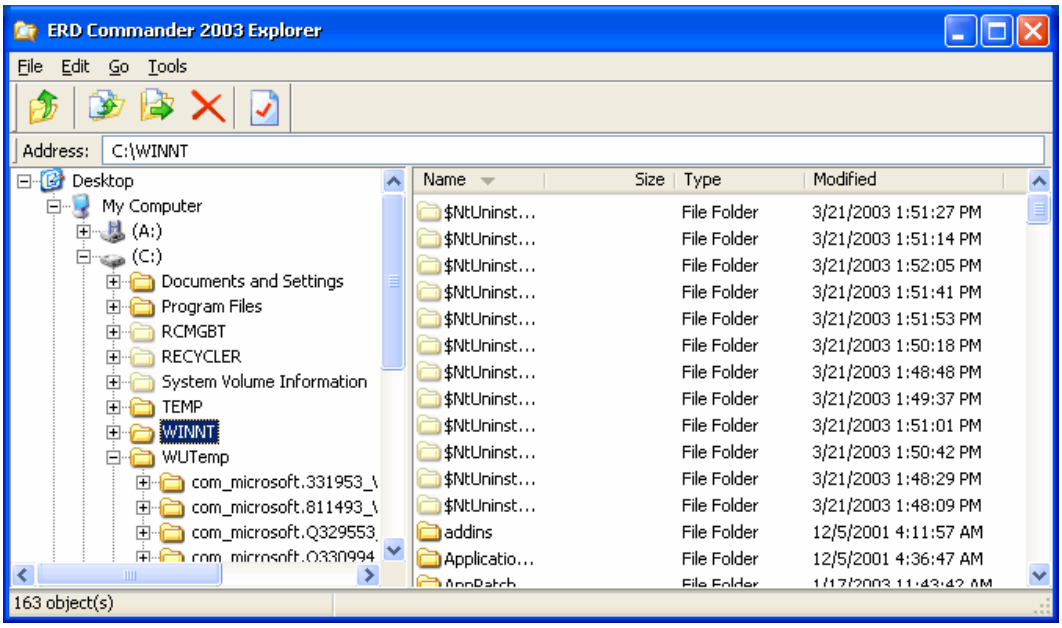
ERD Commander 2003 Explorer, which is accessible from the **Start** menu, allows you to browse the system's volumes as well as the NetBIOS network neighborhood. Active Directory browsing is not supported. The Explorer window has a tree view on the left and a list view on the right that displays the contents of the folder selected in the tree view. The My Computer and Network Neighborhood desktop shortcuts open instances of Explorer that select the associated folder.

ERD Commander 2003 Explorer supports many of the operations supported by the Windows Explorer, including drag-and-drop, the up-directory button, in-place rename, new-folder creation, delete, and property viewing for most items. It also provides for mapping file shares exported by other systems on the network to local drive letters, and includes built-in support for cabinet (.CAB) and ZIP files.

ERD Commander 2003 Explorer obtains icon information for file extensions from the Software Registry hive of the system you are repairing. If the Software hive is corrupt or missing Explorer displays only basic icons.

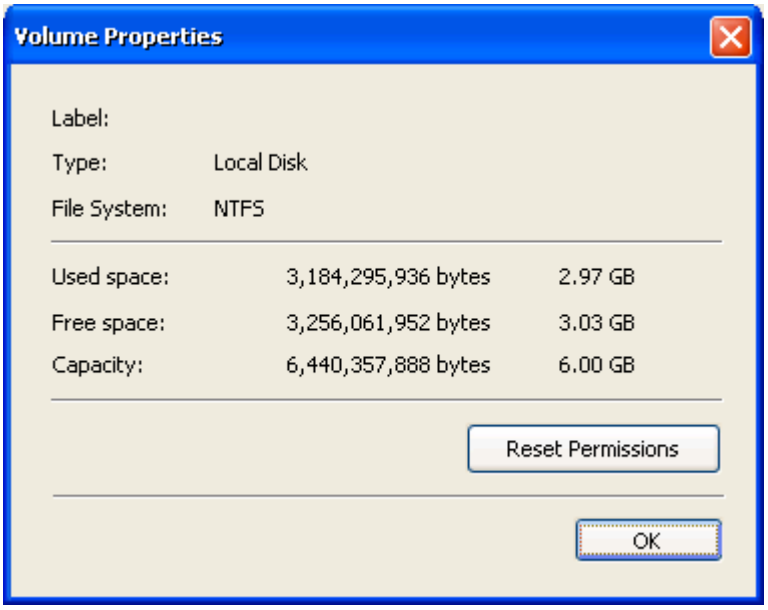
Note that, unlike the default behavior of Windows Explorer, ERD Commander 2003 Explorer displays hidden folders and files (those with the hidden attribute set), displaying them with faded icons. Also unlike Windows Explorer, you cannot drag-and-drop items between different Explorer windows; use the **Copy To** button on the toolbar for this purpose.

The following sections describe the **Property** dialogs associated with different items, as well as how to map network shares to local drive letters.


ERD Commander 2003 Explorer
File Edit Go Tools
Address: C:\WINNT
Desktop
My Computer
(A:)
(C:)
Documents and Settings
Program Files
RCMGBT
RECYCLER
System Volume Information
TEMP
WINNT
WUTemp
com_microsoft.331953_\
com_microsoft.811493_\
com_microsoft.Q329553_
com_microsoft.Q330994
Name Size Type Modified
$NtUninst... File Folder 3/21/2003 1:51:27 PM
$NtUninst... File Folder 3/21/2003 1:51:14 PM
$NtUninst... File Folder 3/21/2003 1:52:05 PM
$NtUninst... File Folder 3/21/2003 1:51:41 PM
$NtUninst... File Folder 3/21/2003 1:51:53 PM
$NtUninst... File Folder 3/21/2003 1:50:18 PM
$NtUninst... File Folder 3/21/2003 1:48:48 PM
$NtUninst... File Folder 3/21/2003 1:49:37 PM
$NtUninst... File Folder 3/21/2003 1:51:01 PM
$NtUninst... File Folder 3/21/2003 1:50:42 PM
$NtUninst... File Folder 3/21/2003 1:48:29 PM
$NtUninst... File Folder 3/21/2003 1:48:09 PM
addins File Folder 12/5/2001 4:11:57 AM
Applicatio... File Folder 12/5/2001 4:36:47 AM
163 object(s)

3.5 Volume Properties

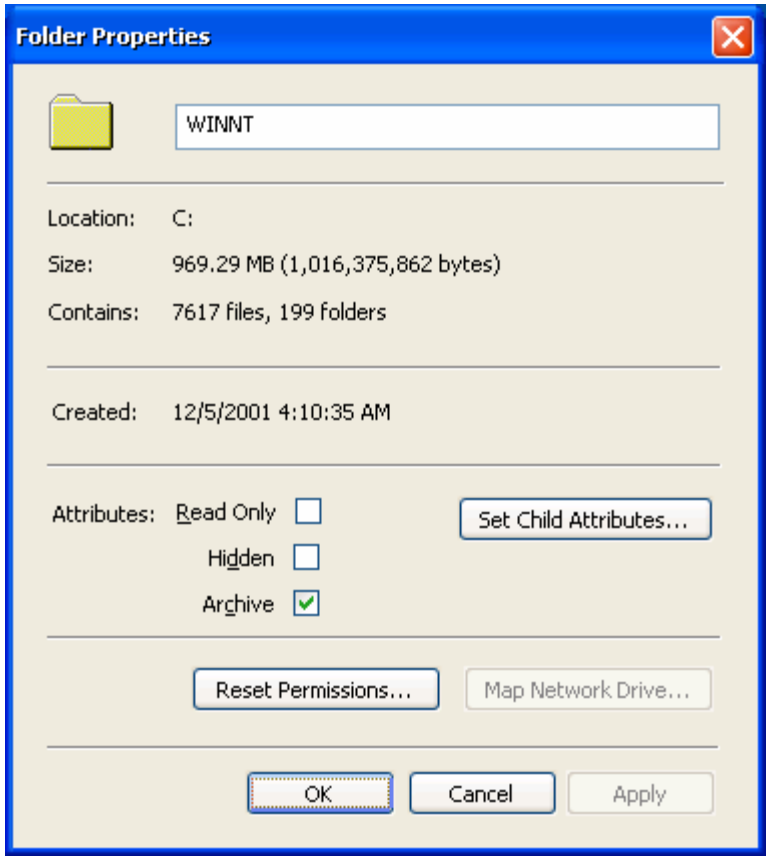
Selecting **Properties** from a volume's context menu (accessible by right-clicking on a volume) or selecting **Properties** from the File menu launches a dialog that displays information about a volume, including statistics on total size and free space. See section 3.7, *Resetting Permissions*, for a description of the **Reset Permissions** button.



3.6 Folder Properties

You can view detailed information about a folder by choosing **Properties** from the folder's context menu or selecting **Properties** from the **File** menu when the folder selected. The **Map Network Drive** button enables when you select a folder that represents a network share, allowing you to map the share to a local drive letter. Find more information in section 3.8, *Mapping Network Drives*. See section 3.7, *Resetting Permissions*, for a description of the **Reset Permissions** button.

Editing a folder's name in the **Properties** dialog and then applying the change renames the folder. Similarly, you can change the attributes of the folder in the **Attributes** area of the dialog, and use the **Set Child Attributes** to apply a set of attributes to all of the files and folders contained within the selected folder.



3.7 Resetting Permissions

A system can become unbootable if permissions are set on NTFS folders or directories that prevent the operating system from accessing the files required for the boot process. The **Reset Permissions** button on a volume or folder **Properties** dialog changes the permissions on the volume folder, and optionally on child folders, to a security descriptor that gives the Everyone group (all users) full access.

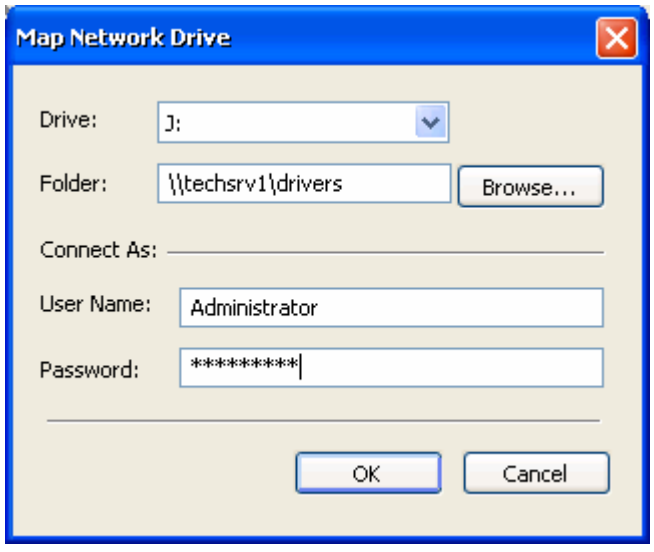
***NOTE**: Because resetting permissions makes folders and directories fully accessible to any user, you should lock down the appropriate folders and directories after the system is booted normally to close potential security holes.*

3.8 Mapping Network Drives

ERD Commander 2003 Explorer provides a Network Neighborhood folder for you to navigate to file shares. However, in some cases it is more convenient to access a file share through a mapped drive letter. To map a share to a drive letter use the **Map Network Drive** menu item in the **Tools** menu or the **Map Network Drive** button on a file share's **Properties** dialog. This method allows you to map shares on networks without NetBIOS and thus not visible in Network Neighborhood.

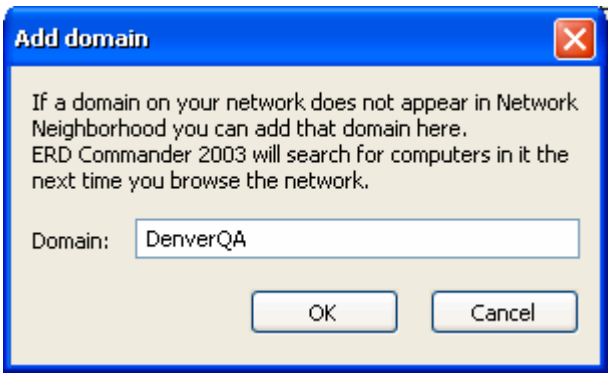
The **Map Network Drives** dialog requires that you specify a free local drive letter, the path to the network file share that you want to map, and optionally the username and password information that Explorer should use to connect to the share. The network share path can consist of DNS (e.g. \\system.mydomain.com), NetBIOS (\\System) or TCP/IP (\\192.168.3.101) computer addresses.

Disconnect a mapped drive either by selecting the drive you wish to disconnect and selecting **Disconnect** from its context menu, or by selecting the drive in the **Disconnect Network Drive** dialog, accessed from the **Tools** menu.



3.9 Adding a Domain

If a domain is not visible within ERD Commander 2003's Network Neighborhood you can add it with the **Add Domain** dialog, which you activate from the **Tools** menu of ERD Commander 2003 Explorer.



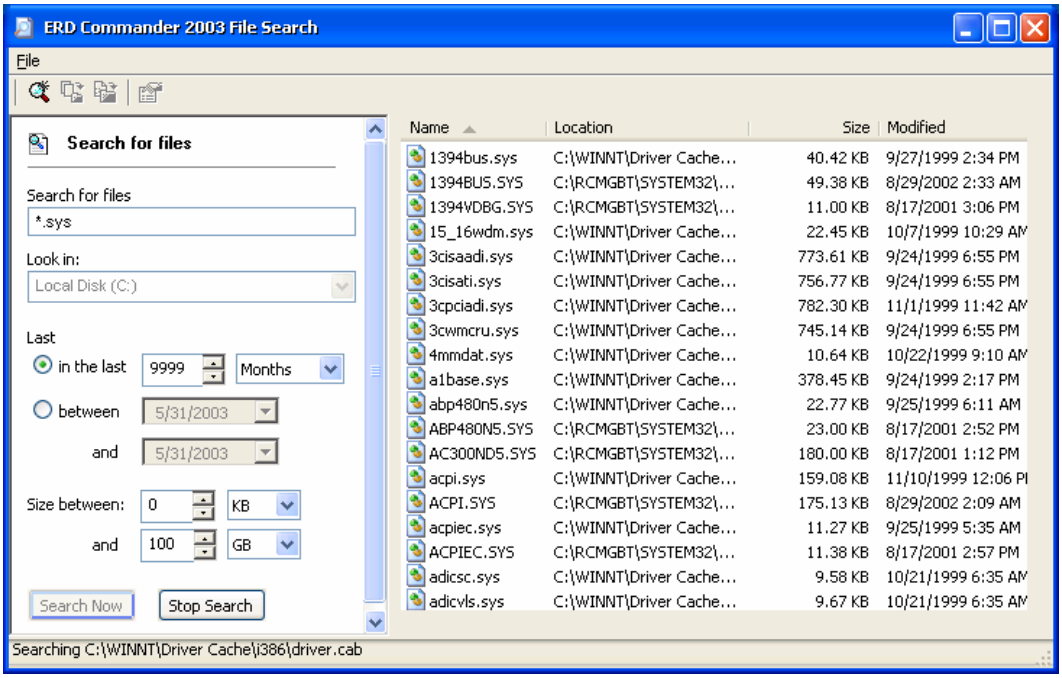
3.10 Using File Search

You can search for files on the hard disks of the system that you are repairing using ERD Commander 2003 File Search. ERD Commander 2003 File Search has an interface nearly identical to that of the Windows 2000 File Search utility, and is accessible via the **Start** menu and from the context menu of folders within ERD Commander 2003 Explorer. As with Windows 2000 File Search, the search pattern you enter can contain any subset of the file or path names for which you wish to search, and can include the asterisk (*) wild-card character. You can also optionally modify your search to include only results with modifications within a certain time period, or of a particular size.

File Search displays the result of a search as a list in its right pane. After selecting one or more entries in the list you can perform the following operations, all of which are accessible via menu items in the **File** menu, the context menu (display the context menu by right clicking), and the toolbar:

- **Copy**
- **Move**
- **View properties**
- **Explore** (opens an instance of ERD Commander 2003 Explorer with the target location opened)
- **Open** (opens documents and executes executable images)

Double-clicking on a result also displays the properties file or folder for that item.


ERD Commander 2003 File Search
File
Search for files
Search for files
*.sys
Look in:
Local Disk (C:)
Last
in the last
9999
Months
between
5/31/2003
and
5/31/2003
Size between:
0
KB
and
100
GB
Search Now
Stop Search
Name
Location
Size
Modified
1394bus.sys C:\WINNT\Driver Cache... 40.42 KB 9/27/1999 2:34 PM
1394BUS.SYS C:\RCMGBT\SYSTEM32\... 49.38 KB 8/29/2002 2:33 AM
1394VDBG.SYS C:\RCMGBT\SYSTEM32\... 11.00 KB 8/17/2001 3:06 PM
15_16wdm.sys C:\WINNT\Driver Cache... 22.45 KB 10/7/1999 10:29 AM
3cisaadi.sys C:\WINNT\Driver Cache... 773.61 KB 9/24/1999 6:55 PM
3cisati.sys C:\WINNT\Driver Cache... 756.77 KB 9/24/1999 6:55 PM
3cpciadi.sys C:\WINNT\Driver Cache... 782.30 KB 11/1/1999 11:42 AM
3cwmcru.sys C:\WINNT\Driver Cache... 745.14 KB 9/24/1999 6:55 PM
4mmdat.sys C:\WINNT\Driver Cache... 10.64 KB 10/22/1999 9:10 AM
a1base.sys C:\WINNT\Driver Cache... 378.45 KB 9/24/1999 2:17 PM
abp480n5.sys C:\WINNT\Driver Cache... 22.77 KB 9/25/1999 6:11 AM
ABP480N5.SYS C:\RCMGBT\SYSTEM32\... 23.00 KB 8/17/2001 2:52 PM
AC300ND5.SYS C:\RCMGBT\SYSTEM32\... 180.00 KB 8/17/2001 1:12 PM
acpi.sys C:\WINNT\Driver Cache... 159.08 KB 11/10/1999 12:06 PM
ACPI.SYS C:\RCMGBT\SYSTEM32\... 175.13 KB 8/29/2002 2:09 AM
acpiec.sys C:\WINNT\Driver Cache... 11.27 KB 9/25/1999 5:35 AM
ACPIEC.SYS C:\RCMGBT\SYSTEM32\... 11.38 KB 8/17/2001 2:57 PM
adicsc.sys C:\WINNT\Driver Cache... 9.58 KB 10/21/1999 6:35 AM
adicvls.sys C:\WINNT\Driver Cache... 9.67 KB 10/21/1999 6:35 AM
Searching C:\WINNT\Driver Cache\i386\driver.cab

3.11 Using FileRestore

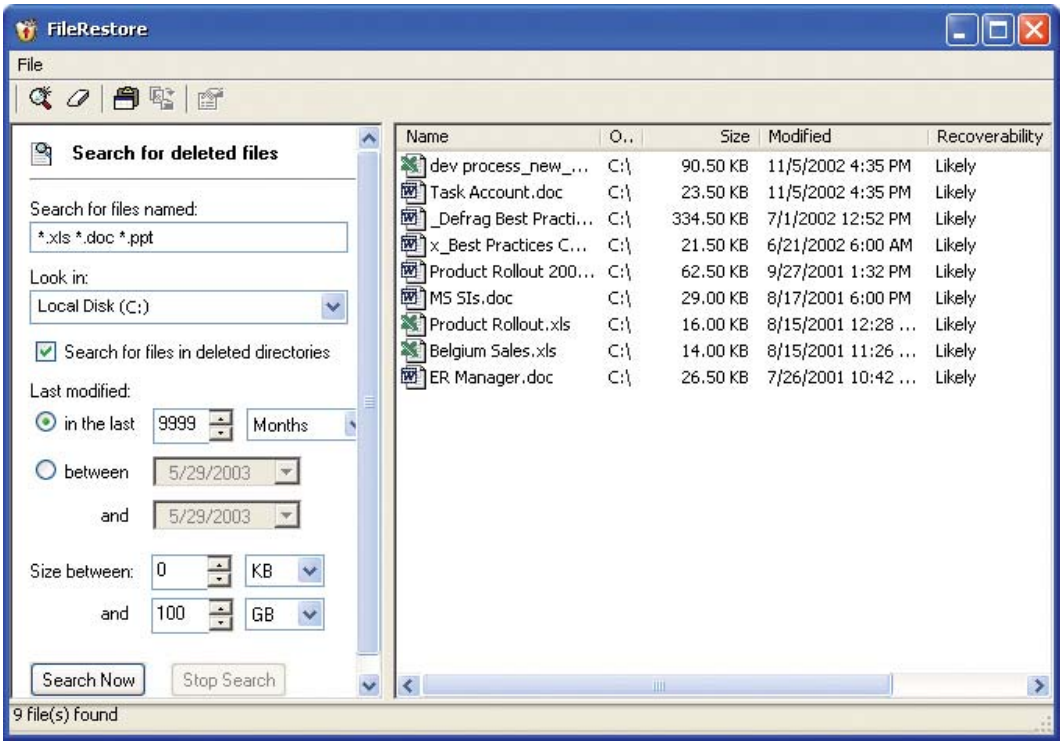
Use ERD Commander's FileRestore utility to recover deleted files from the system you are repairing. Its interface, like that of ERD Commander 2003 File Search, is similar to that of the Windows 2000 File Search utility. The search pattern you enter can contain any subset of the file or path names for which you wish to search, and can include the asterisk (*) wild-card character. Optionally, you can modify your search to only include results with modifications within a certain time period, or of a particular size. When you Click the **Search** button FileRestore searches the locations you specified and displays found items in the right pane of its window.

FileRestore attempts to determine whether each deleted file is recoverable and reports the result in the Recoverability column. If a file is marked Likely it means that none of the file's data is known to be overwritten by other files. However, this is only an estimate of the file's condition, and it is possible that even a file marked Likely will contain corrupt data. In general the longer the time since a file has been deleted the less likely that it can be recovered.

When searching for files on FAT or FAT32 volumes the first letter of the file name cannot always be retrieved. For this reason FileRestore displays files that match all characters entered in Search for files named, as well as those matching all characters but the first. Whenever the first letter cannot be retrieved it is replaced by the question mark character ('?') when displayed and by an underscore ('_') when the file is copied to a new location.

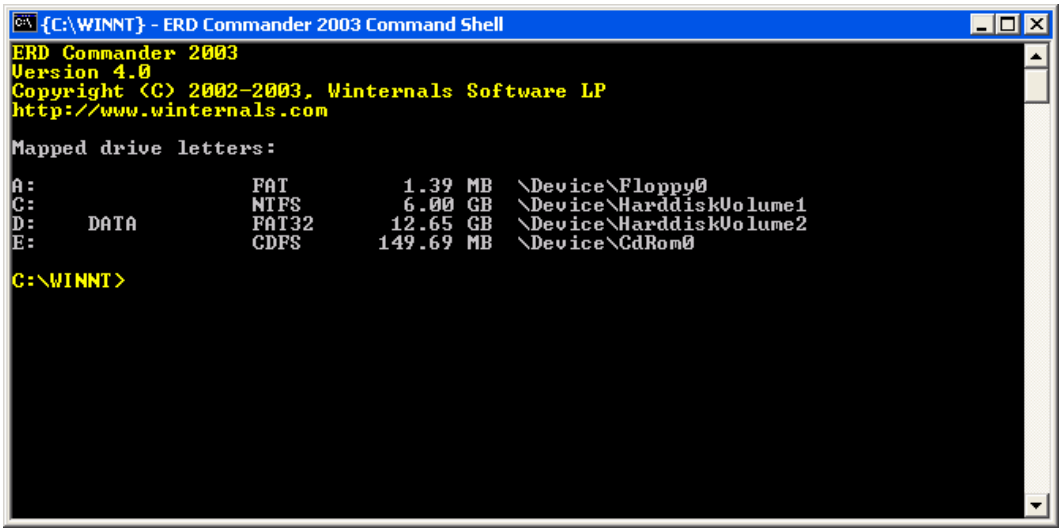
If a file is found but it cannot be determined which directory it belongs to (usually because the parent directory is also deleted) then it is placed in a directory labeled "...Unknown Folder #...". It is possible for there to be multiple orphan directories, each corresponding to a different directory that no longer exists.

***NOTE**: To reduce the possibility of overwriting data that you may wish to recover, whenever practical you should restore files to a location other than the source volume.*



3.12 Command Prompt

ERD Commander 2003 Command Prompt presents a subset of the functionality implemented by the Windows XP command-prompt that includes most built-in commands, the ability to execute external applications, and batch file capabilities. This section serves as reference for the Command Prompt's built-in commands.



3.12.1 The Command Set

ATTRIB	Displays or changes file attributes.
BUFFER	Sets console screen buffer information.
CALL	Calls one batch program from another.
CD	Displays the name of or changes the current directory.
CHDIR	Displays the name of or changes the current directory.
CHKDSK	Checks a disk and displays a status report.
CLS	Clears the screen.
COPY	Copies one or more files to another location.
DATE	Displays the current date.

DEL	Deletes one or more files.
DIR	Displays a list of files and subdirectories in a directory.
DISKPART	Partitions disks.
ECHO	Displays messages, or turns command echoing on or off.
ERASE	Deletes one or more files.
EXIT	Exits the command prompt.
HELP	Provides Help information for ERD Commander 2003 commands.
MAP	Displays drive letter to partition mapping.
MD	Creates a directory.
MKDIR	Creates a directory.
MOVE	Moves or renames a file or directory.
RD	Removes a directory.
REGSVR32	Registers COM/DCOM DLLs.
RMDIR	Removes a directory.
SCREEN	Sets console screen information.
SET	Sets, displays, or removes environment variables.
START	Starts a program in a new command prompt window.
TIME	Displays the current time.
TYPE	Displays the contents of a file.
VER	Displays ERD Commander 2003 version number.
VERSION	Displays ERD Commander 2003 version number.
XCOPY	Copies files and directory trees.

3.12.2 Attrib

Displays or changes file attributes.

```
ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [[drive:][path]filename]
[/S]

  +   Sets an attribute.
  -   Clears an attribute.
  R   Read-only file attribute.
  A   Archive file attribute.
  S   System file attribute.
  H   Hidden file attribute.
  /S  Processes files in all directories in the specified path.
```

3.12.3 Buffer

Sets console screen buffer information.

```
BUFFER [width height]

  width   Specifies width of the console buffer.
  height  Specifies height of the console buffer.
```

3.12.4 Call

Calls one batch program from another.

```
CALL [drive:][path]filename [batch-parameters]

  batch-parameters   Specifies any command-line
                     information required by the batch
                     program.
```

3.12.5 Cd/Chdir

Displays the name of or changes the current directory.

```
CHDIR [drive:][path]
CHDIR[..]
CD [drive:][path]
CD[..]
```

".." specifies that you want to change to the parent directory.

Type CD drive: to display the current directory in the specified drive.

Type CD without parameters to display the current drive and directory.

3.12.6 Cls

Clears the screen.

```
CLS
```

3.12.7 Copy

Copies one or more files to another location.

```
COPY source [destination]

  source        Specifies the file or files to be copied.
  destination   Specifies the directory and/or filename for
                  the new file(s).
```

Wildcards can be used in both the source and destination file name specifications.

3.12.8 Date

Displays the current date.

```
DATE
```

3.12.9 Del/Erase

Deletes one or more files.

```
DEL [/P] [/F] [/S] [/Q] [/A[[:]attributes]] [[drive:][path]filename
ERASE [/P] [/F] [/S] [/Q] [/A[[:]attributes]] [[drive:][path]filename

  [drive:][path]filename
              Specifies the file(s) to delete.
              Specify multiple files by using wildcards.
  /P          Prompts for confirmation before deleting each file.
  /F          Force deleting of read-only files.
  /S          Delete specified files from all subdirectories.
  /Q          Quiet mode, do not ask if ok to delete on global
              wildcard
  /A          Selects files to delete based on attributes
  attributes  R  Read-only files     S  System files
              H  Hidden files        A  Files ready for archiving
              - Prefix meaning not
```

The display semantics of the /S switch are reversed in that it shows you only the files that are deleted, not the ones it could not find.

3.12.10 Dir

Displays a list of files and subdirectories in a directory.

```
DIR [drive:][path][filename] [/P] [/W] [/A[[:]attributes]]
  [/O[[:]sortorder]] [/S] [/X]

  [drive:][path][filename]

Specifies drive, directory, and/or files to list.

  /P          Don't pause after each screen of information.
  /W          Uses wide list format.
  /A          Displays files with specified attributes.
  Attributes  D  Directories        R  Read-only files
              H  Hidden files       A  Files ready for archiving
              S  System files       -  Prefix meaning not
  /O          List by files in sorted order.
  Sortorder   N  By name (alphabetic)
              S  By size (smallest first)
              D  By date & time (earliest first)
              -  Prefix to reverse order
  /S          Displays files in specified directory and all
              subdirectories.
  /X          This displays the short names generated for
              non-8dot3 file names. If no short name is
              present, blanks are displayed in its place.
```

3.12.11 Echo

Displays messages or turns command echoing on or off.

```
ECHO [message] [on | off]

   message    Message to display.
   on         Turns command echoing on.
   off        Turns command echoing off.
```

3.12.12 Exit

Exits the command prompt

```
EXIT
```

3.12.13 Help

Provides Help information for ERD Commander 2003 built-in Command Prompt commands.

```
HELP [command]

  Command        Displays specific information on the specified command.
```

3.12.14 Map

Displays drive letter to partition mappings.

This command displays the drive letter assignments made by ERD Commander 2003. For each drive you will see the device name, volume label, file system type and drive size.

If the System account or Administrators group is denied access to an NTFS drive because of the security settings applied to the drive's root directory, the file system type will be <?>. Use the **Volume Properties** dialog for the volume to unlock the drive.

An example mapping is shown below:

```
Mapped drive letters:
A:                                      \Device\Floppy0
C:    WINXP         NTFS        7.81 GB  \Device\HarddiskVolume2
D:    DEV           NTFS       10.69 GB  \Device\HarddiskVolume3
E:    SRC           NTFS        4.48 GB  \Device\HarddiskVolume4
F:    MSDN          NTFS        2.41 GB  \Device\HarddiskVolume5
G:    GAMES         NTFS        8.50 GB  \Device\HarddiskVolume6
H:                                       \Device\CdRom0
I:    Audio CD      CDFS        0.00 MB  \Device\CdRom1
```

3.12.15 Mkdir/Md

Creates a directory.

```
MKDIR [drive:]path
MD [drive:]path
```

MKDIR creates any intermediate directories in the path, if needed. For example, assume \a does not exist then:

```
mkdir \a\b\c
```

is the same as:

```
mkdir \a
mkdir \a\b
mkdir \a\b\c
```

3.12.16 Move

Moves or renames a file or directory.

```
MOVE Source [Target]

  Source      Specifies the path and name of the file(s) to move.
  Target      Specifies the path and name to move file(s) to.
```

3.12.17 Rmdir/Rd

Removes (deletes) a directory.

```
RMDIR [/S] [/Q] [drive:]path
RD [/S] [/Q] [drive:]path

  /S      Removes all directories and files in the
          specified directory in addition to the
          directory itself.  Used to remove a
          directory tree.
  /Q      Quiet mode, do not ask if ok to remove a
          directory tree with /S
```

3.12.18 Screen

Sets console screen information.

```
SCREEN [width height]

  width   Specifies width of the console window.
  height  Specifies height of the console window.
```

3.12.19 Set

Displays, sets, or removes command prompt environment variables.

```
SET [variable=[string]]

  variable    Specifies the environment-variable name.
  string      Specifies a series of characters to
              assign to the variable.
```

Type SET without parameters to display the current environment variables.

3.12.20 Start

Starts a program in a new command prompt window.

```
START [program] [parameters]

  program      Specifies the program.
  parameters   Specifies the parameters for the
               program.
```

3.12.21 Time

Displays the current time.

```
TIME
```

3.12.22 Type

Displays the ASCII contents of a file.

```
TYPE filename
```

The TYPE command displays the contents of a file. You can pause the output at any time by pressing CTRL-S, and abort the output by pressing CTRL-C.

3.12.23 Ver/Version

Displays ERD Commander 2003's version number.

```
VERSION
VER
```

3.12.24 Xcopy

Copies files and directory trees.

```
XCOPY source [destination] [/A | /M] [/P] [/S] [/W]
                           [/C] [/E] [/I] [/Q] [/F] [/H] [/R] [/T] [/U]
[/K]

 source       Specifies the file(s) to copy.
 destination  Specifies the location and/or name of new files.
 /A           Copies files with the archive attribute set,
              doesn't change the attribute.
 /M           Copies files with the archive attribute set,
              turns off the archive attribute.
 /P           Prompts you before creating each destination
              file.
 /S           Copies directories and subdirectories except
              empty ones.
 /W           Prompts you to press a key before copying.
 /C           Continues copying even if errors occur.
 /E           Copies empty subdirectories.
 /I           If destination does not exist and copying more
              than one file, assumes that destination must be a
              directory.
 /Q           Does not display file names while copying.
 /F           Displays full source and destination file names
              while copying.
 /H           Copies hidden and system files also.
 /R           Overwrites read-only files.
 /T           Creates directory structure, but does not copy
              files.  Includes empty directories or
              subdirectories.
 /U           Copies only files that already exist in
              destination.
 /K           Copies attributes. Normal Xcopy will reset
              read-only attributes.
```

3.13 Chkdsk

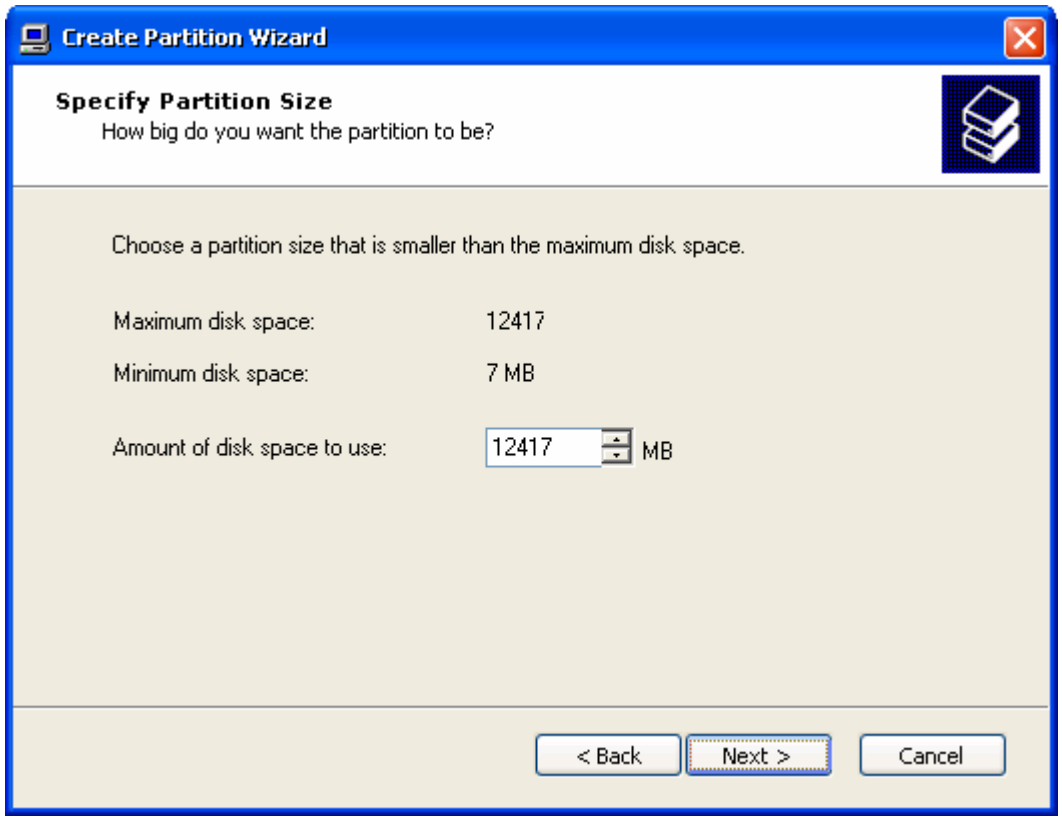
ERD Commander 2003 includes a clone of the Windows 2000/XP Chkdsk utility for analyzing and correcting file system corruption. Run Chkdsk, which is located in the system32 directory of the ERD Commander 2003 CD-ROM, from a command prompt window. The ERD Commander 2003 Chkdsk supports a subset of the Windows Chkdsk command-line options:

```
Usage: chkdsk [/F] [/X] [/R] [drive:]
    /F      Fixes errors on the disk.
    /X      Forces the volume to dismount first if necessary.
    /R      Locates bad sectors and recovers readable
            information (implies /f)
```

If you specify a drive that has open files, for instance because you are running an application from the drive, you must use the /X switch. However, the /X switch does not work on the system drive of an installation you are repairing if you are running any utilities that access the Registry of that installation. The ERD Commander 2003 utilities that access the Registry include Regedit, Explorer, Service and Driver Manager, System Information, and Event Log Viewer. Make sure that you close these applications before running Chkdsk against the system drive.

3.14 Diskpart

Diskpart, Microsoft's command-line disk partitioning utility, ships with ERD Commander 2003. The ERD Commander 2003 Disk Management snap-in that you access with the Computer Management utility provides a graphical interface to Diskpart's functionality, but Diskpart has interactive as well as script-driven modes. For help on Diskpart's commands, run it and enter the Help command. Microsoft's web site also has information on using Diskpart.



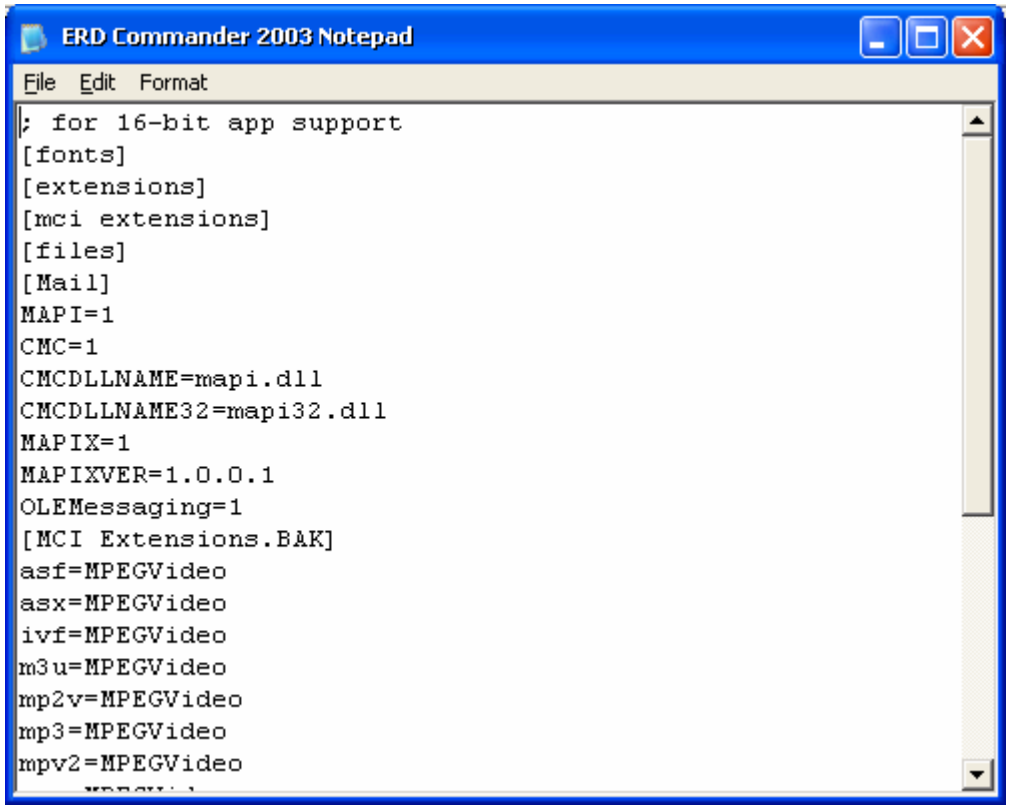
3.15 Regsvr32

ERD Commander 2003 Regsvr32 has an interface identical to that of the Windows Regsvr32 utility. The Windows Regsvr32 utility does not function properly in the ERD Commander 2003 environment because it cannot register DLLs into an installation you are repairing, so use ERD Commander 2003 Regsvr32 to register COM/DCOM server DLLs.

```
Usage: regsvr32 [/u] [/s] [/n] [/i[:cmdline]] dllname
    /U      Unregister server
    /S      Silent; display no message boxes
    /L      Call DllInstall passing it an optional [cmdline];
              when used with /u calls dll uninstall
    /N      Do not call DllRegisterServer; this option must be used with /l
```

3.16 Notepad

ERD Commander 2003 Notepad is essentially a clone of the Windows Notepad application, allowing you to edit existing text files and create new ones.



3.17 Regedit

ERD Commander 2003 Regedit is similar to the Windows XP Regedit utility, but enables you to edit the Registry of the system you are repairing. Unlike with Windows Regedit, you will only see two top-level keys in ERD Commander 2003 Regedit: HKEY_CLASSES_ROOT and HKEY_LOCAL_MACHINE. This is because there are no users actually logged on to the system you are repairing with ERD Commander 2003, obviating the need for the HKEY_USERS and HKEY_CURRENT_USER root keys. Since ERD Commander 2003 (not the system) is booted, there is no current hardware configuration loaded, obviating the need for HKEY_CURRENT_CONFIG (the root key that links to the part of the Registry representing the active hardware profile) and there is no HARDWARE subkey under HKEY_LOCAL_MACHINE, since the system creates the HARDWARE key for an installation when it boots.

If any of the Registry hives (the files that store Registry data) of the system that you are repairing are missing or corrupt one or more subkeys under HKEY_LOCAL_MACHINE will not be available. See Chapter 4, *Frequently Asked Questions*, for a description of the correspondence between Registry hives and the keys that represent them.

ERD Commander 2003 Regedit understands the following Registry value types:

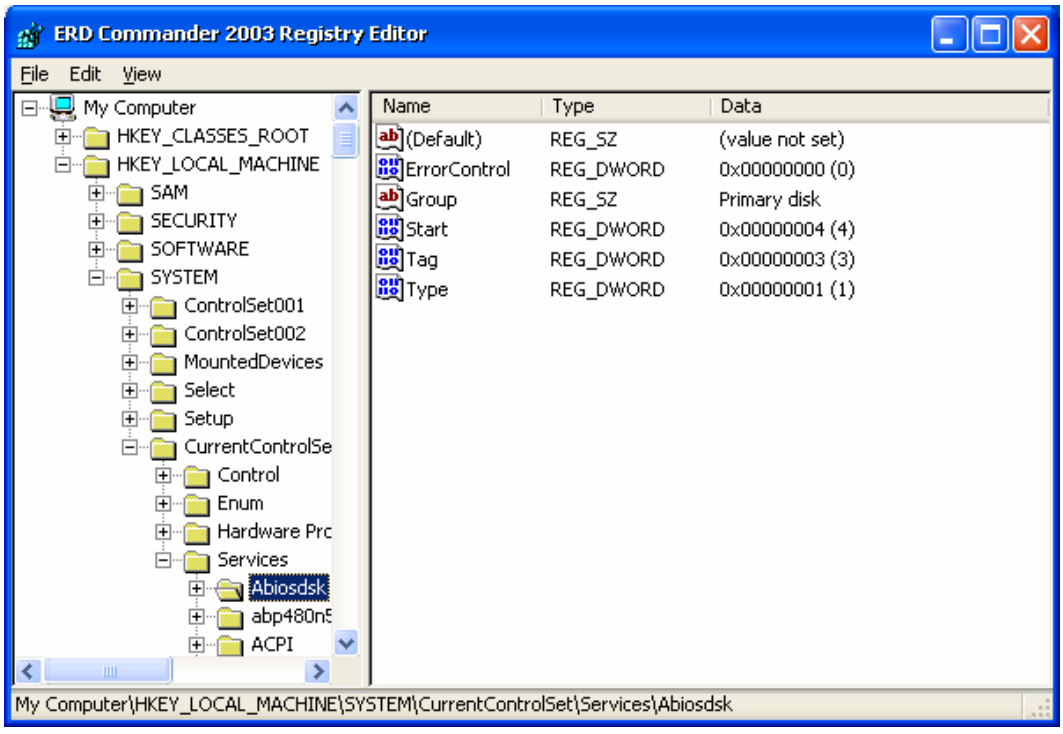
- String
- Multi-String
- Expandable String
- Binary
- DWORD

Like the Windows Regedit, ERD Commander 2003 Regedit supports Registry key import and export, allowing you to save Registry key information to a text

file and to incorporate Registry key information of the same format into the Registry. The file format used by ERD Commander 2003 Regedit is the same as that used by the Windows 2000, XP, and Server 2003 Registry editors.

Use ERD Commander 2003 Regedit's permissions reset functionality when a system becomes unbootable because security permissions on keys prevent the system from accessing critical areas of the Registry. Select the key whose permissions you wish to reset and chose the **Reset Permissions** menu entry. You can reset the permissions on a specific key or a key and all its subkeys.

***NOTE*:** Because resetting permissions makes objects fully accessible to any user, you should lock down the appropriate objects after the system is booted normally to close potential security holes.

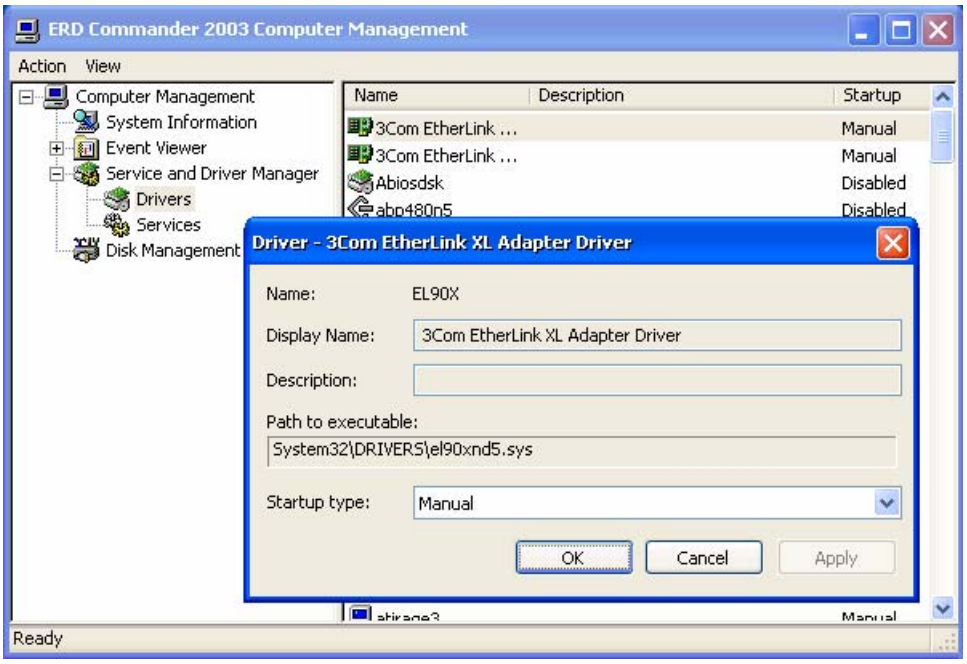


3.18 Using Service and Driver Manager

The ERD Commander 2003 Service and Driver Manager, accessible in the Administrative Tools folder of the **Start** menu, is an ERD Commander 2003 Computer Management utility snap-in. The Service and Driver Manager is actually an interface to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services part of the Registry where service and driver configuration subkeys are located for the system you are repairing.

Every service and driver has a subkey that includes values that specify its start type, and an optional description and display name. The Service and Driver Manager shows this information and allows you to edit the start type when you view the properties of a selected service or driver. You can access the **Properties** dialog by selecting the service or driver and double-clicking, or by choosing **Properties** from the **Action** menu or from the context menu that appears when you right-click.

Typical repair operations involve disabling a service or driver that is preventing a system from booting, or replacing a corrupt service or driver file. To disable a service or driver, display its properties and change the startup type to Disabled. The **Properties** dialog also reports the path to the service or driver's executable image.

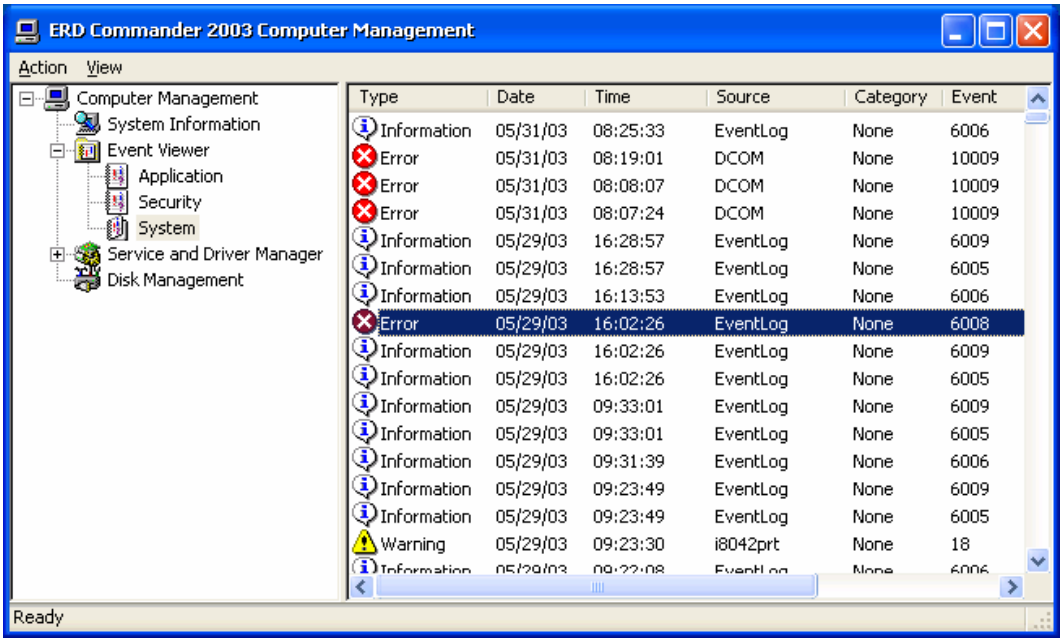

ERD Commander 2003 Computer Management
Action View
Computer Management
System Information
Event Viewer
Service and Driver Manager
Drivers
Services
Disk Management
Name
Description
Startup
3Com EtherLink ...
Manual
3Com EtherLink ...
Manual
Abiosdsk
Disabled
abp480n5
Disabled
Driver - 3Com EtherLink XL Adapter Driver
Name:
EL90X
Display Name:
3Com EtherLink XL Adapter Driver
Description:
Path to executable:
System32\DRIVERS\el90xnd5.sys
Startup type:
Manual
OK
Cancel
Apply
Ready

3.19 Using Event Log Viewer

ERD Commander 2003 Event Log Viewer enables you to examine the System, Application, and Security event logs of the system you are repairing. It functions like the Windows Event Viewer, allowing you to look for entries that might help you diagnose a problem that is preventing a system from booting. Examples include blue-screen crash errors and errors or warnings that indicate problems with particular services or drivers.

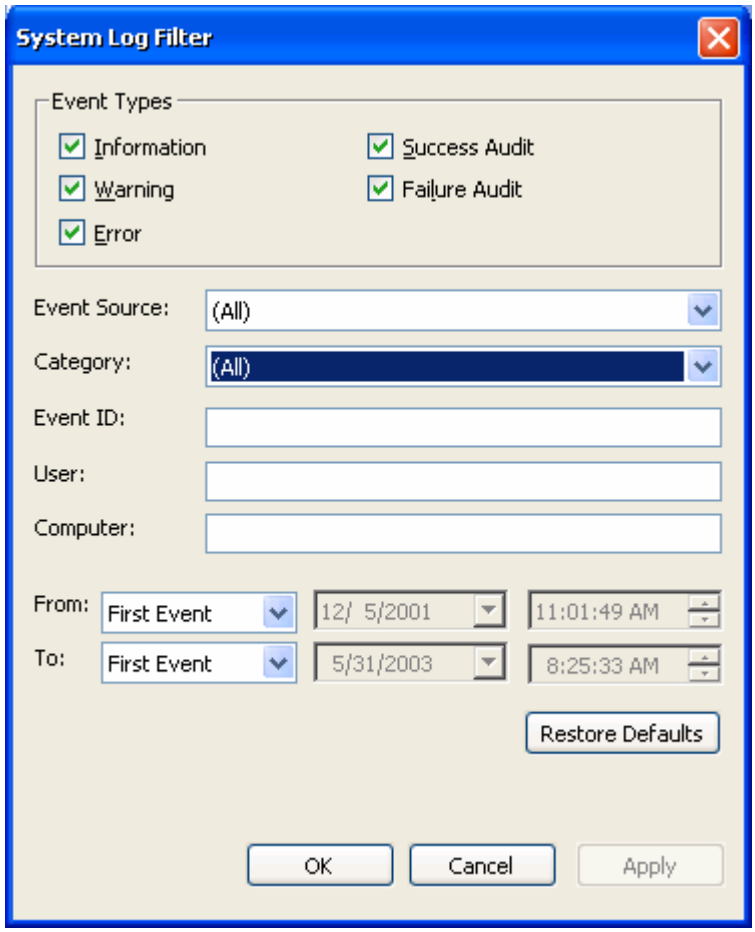
Event Log Viewer is a snap-in to the ERD Commander 2003 Computer Management utility that you access via the Administrative Tools folder in the **Start** menu. The three event logs displayed by ERD Commander 2003 Event Log Viewer are stored in the system's SystemRoot\System32\Config folder. If any of these files are missing or corrupt, you will see no entries in the corresponding node.

To view detailed information about the entry, choose **Properties** from the **Action** menu or an event log entry's context menu, or double-click on the entry. Use the up and down arrows in the **Properties** dialog to move between different event entries.



3.20 Filtering Events

You can filter the events that you want to see by selecting the **Filter** menu entry from the **Action** menu of Computer Management. The **Filter** dialog, shown below, allows you to filter based on the event severity, source, category, date, and other attributes.

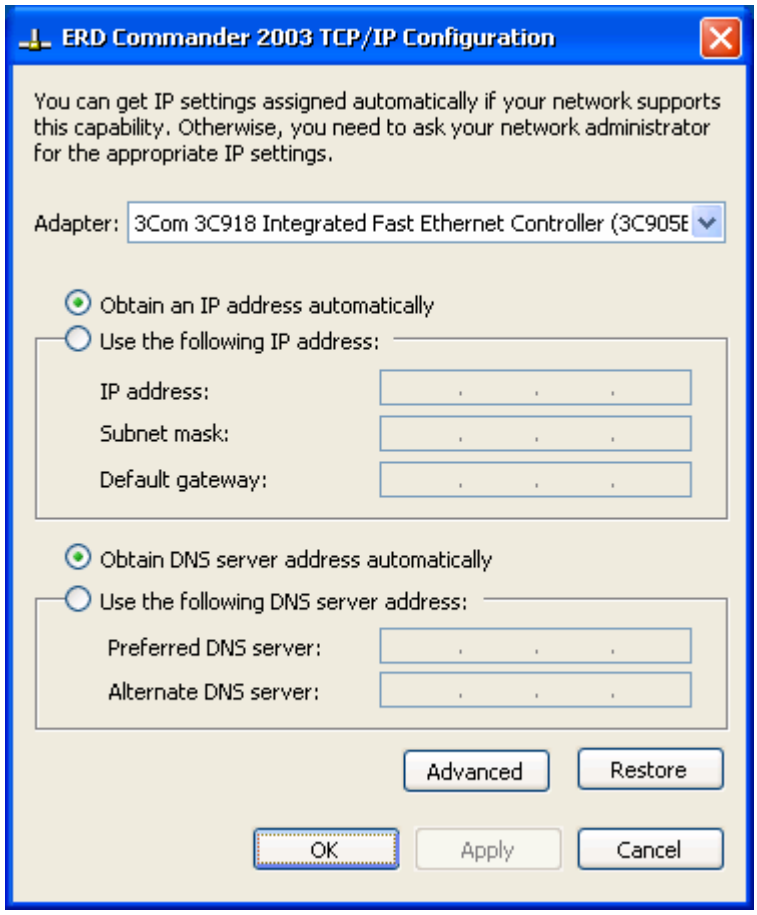


3.21 Using TCP/IP Configuration

When you boot a computer with ERD Commander 2003, network adapters on the system are started using a default configuration that assumes that you have a DHCP server on your network from which an IP address, gateway, and DNS servers can be obtained. If your network requires explicit configuration of any of these values, use the ERD Commander 2003 TCP/IP Configuration utility after logging on to the system you wish to repair. The TCP/IP Configuration utility, accessible in the Administrative Tools folder of the **Start** menu, lets you select the network adapter for which you want to make changes and to enter explicit TCP/IP settings for that adapter. The settings that you enter become active immediately when applied.

The advanced page of the TCP/IP Configuration utility shows the currently enabled settings for IP address, DNS server, gateways, WINS servers, and, if DHCP is configured, DHCP server and lease time.

Note that ERD Commander 2003 assigns a random name to the computer being accessed for repair. If you wish to access the volumes of the computer from another system you must enable file sharing by running the File Sharing utility.


ERD Commander 2003 TCP/IP Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Adapter:
3Com 3C918 Integrated Fast Ethernet Controller (3C905E
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server address:
Preferred DNS server:
Alternate DNS server:
Advanced
Restore
OK
Apply
Cancel

3.22 Using Disk Management

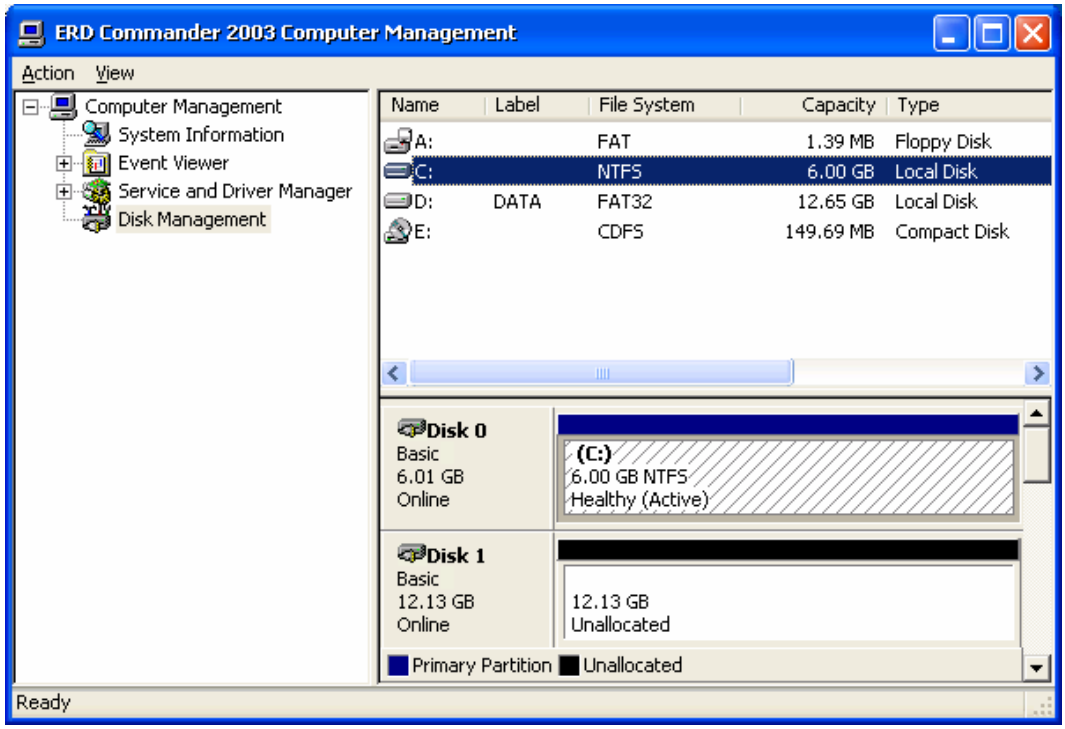
The Disk Management utility is a snap-in to the ERD Commander 2003 Computer Management utility that is located in the Administrative Tools folder of the **Start** menu. It provides information on drive-letter to volume mappings as well as a graphical disk partitioning and formatting interface.

The drive letters that ERD Commander 2003 assigns to volumes may not be the same as those made when you boot normally into the system you are repairing. To aid in identifying volumes, two ways are provided to view detailed drive letter mapping information. The first is with the map command in the ERD Commander 2003 Command prompt, and the second is accessed from the ERD Commander Disk Management utility.

The bottom portion of ERD Commander 2003 Disk Management's window shows a graphical view of the system's disks and partitions. A context menu specific to the selected object appears in the **All Actions** submenu of the **Action** menu; you can also right-click on an object to access the same menu. You can create new partitions or volumes within free space, format, delete and explore existing volumes, and for partitions on Basic Disks (disks that use Master Boot Record – MBR – partitioning), mark a partition as Active (bootable). Most of the operations available in ERD Commander 2003 Disk Management are also available in Diskpart, a command-line disk partition tool with scripting capability.

If a volume does not have an assigned drive letter in the ERD Commander 2003 environment, you can assign one for that session so that you can explore the volume, run Chkdsk, and perform other operations on it.

Note Microsoft licensing does not allow you to create multipartition volumes - including spanned volumes, mirrored volumes, striped volumes, and RAID-5 volumes - using either Diskpart or ERD Commander 2003 Disk Management.


ERD Commander 2003 Computer Management
Action View
Computer Management
System Information
Event Viewer
Service and Driver Manager
Disk Management
Name Label File System Capacity Type
A: FAT 1.39 MB Floppy Disk
C: NTFS 6.00 GB Local Disk
D: DATA FAT32 12.65 GB Local Disk
E: CDFS 149.69 MB Compact Disk
Disk 0
Basic
6.01 GB
Online
(C:)
6.00 GB NTFS
Healthy (Active)
Disk 1
Basic
12.13 GB
Online
12.13 GB
Unallocated
Primary Partition
Unallocated
Ready

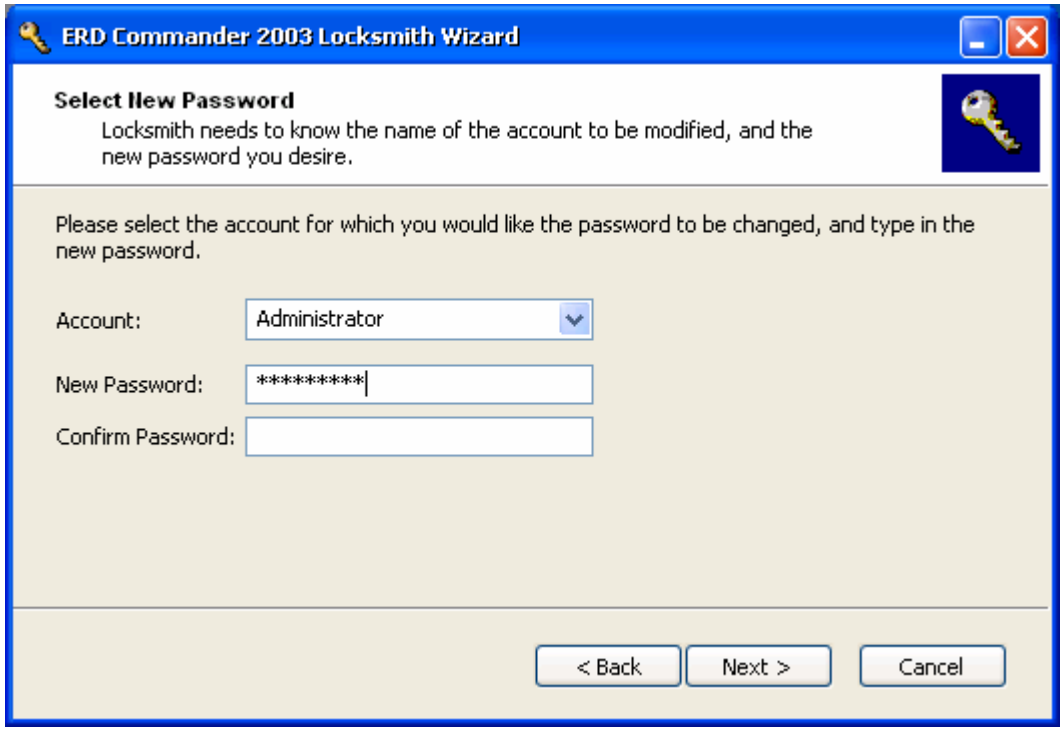
3.23 Locksmith

If you are unable to logon to a system because you have lost the local administrator password or because the administrative password has been locked out, use the ERD Commander 2003 Locksmith utility to reset the password to a known value and unlock the account. The Locksmith wizard, located in the Administrative Tools folder of the **Start** menu, guides you through the process of selecting the account for which you want to change the password and entering the new password. The account will have the new password and be unlocked the next time you boot normally into the system you are repairing.

***NOTES**: You will lose a previous change if you rerun Locksmith to change another password before booting the system normally.*

Locksmith requires the System Registry hive to be intact.

If you have a local policy on the system that enforces password length and/ or complexity, the new password must comply with this policy to take effect.



3.24 File Sharing

To export the volumes of a system booted with ERD Commander 2003, use the ERD Commander 2003 File Sharing utility located in the Administrative Tools folder of the **Start** menu. The utility requires that you enter a workgroup name and password for the ERD Commander 2003 administrator account. Note that ERD Commander 2003 File Sharing sets the password of the ERD Commander 2003 administrator account that is in effect during the current ERD Commander 2003 session, not the administrative account of an installation that you may be repairing.

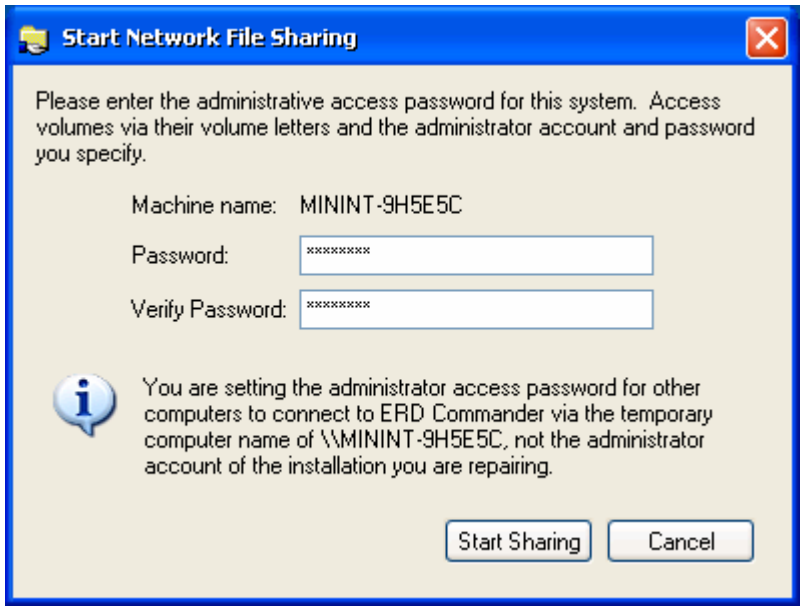
When you enable file sharing each volume of the system is exposed with a share name corresponding to the volume's drive letter. Access the volumes of the ERD Commander 2003 system using its temporary computer name and administrative account. For example, if the system's temporary name is MININT-LX423P and you had set the administrative account password to "allaccess" execute the following command on another computer to gain access to the volume of the dead system:

```
net use \\minint-lx423p\ipc$ /user:minint-lx423p allaccess
```

After executing the command access to the volumes using their drive letters e.g.:

```
dir \\minint-lx423p\c
```

Disable file sharing by rebooting the system.


Start Network File Sharing
Please enter the administrative access password for this system. Access volumes via their volume letters and the administrator account and password you specify.
Machine name: MININT-9H5E5C
Password:
Verify Password:
You are setting the administrator access password for other computers to connect to ERD Commander via the temporary computer name of \\MININT-9H5E5C, not the administrator account of the installation you are repairing.
Start Sharing
Cancel

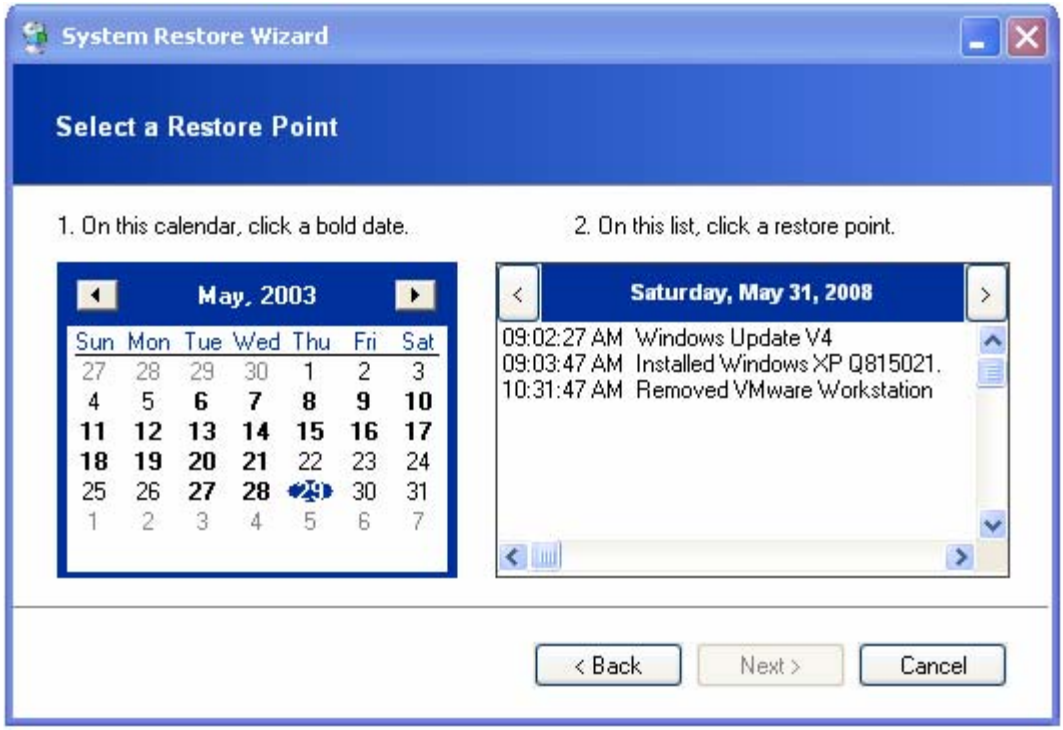
3.25 System Restore

Windows XP's System Restore feature can be configured to periodically create snapshots, called restore points, of operating system files, the Registry, and various Windows component configuration databases such as COM+ and WMI (Windows Management Instrumentation). In order to undo damage caused by user error, system updates, or an application installation, an end-user can run Windows XP's System Restore Wizard and roll back the state of these files and settings to a previous restore point. However, the Windows XP System Restore Wizard is only accessible when a system is booted, making it unavailable when a system is rendered unbootable. ERD Commander 2003's System Restore Wizard provides access to the restore points of Windows XP System Restore, enabling you to apply a restore point even when a system cannot boot.

The ERD Commander 2003 System Restore Wizard, which resides in the Administrative Tools folder of the **Start** menu, is similar to the Windows XP System Restore Wizard. Use the wizard's restore point calendar to select a restore point that you wish to apply. The wizard applies the system files, configuration databases and Registry of the selected restore point, making backups of any files it changes within root-directory folders named ErdUndoCache on the volumes on which replaced files reside.

If you apply a restore point and later wish to restore the previous state, run the ERD Commander 2003 System Restore Wizard and chose the undo option. When you decide that you no longer require the option to undo a restore point's application, use ERD Commander 2003 System Restore Wizard to delete the undo cache directories from the installation's volumes.

NOTE: In order to ensure that subsequent use of Windows XP's System Restore Wizard does not corrupt the system's state, ERD Commander 2003 System Restore Wizard deletes the restore point that you apply and any that follow it chronologically from the Windows XP System Restore database.


System Restore Wizard
Select a Restore Point
1. On this calendar, click a bold date.
2. On this list, click a restore point.
May, 2003
Sun Mon Tue Wed Thu Fri Sat
27 28 29 30 1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 31
1 2 3 4 5 6 7
Saturday, May 31, 2008
09:02:27 AM Windows Update V4
09:03:47 AM Installed Windows XP Q815021.
10:31:47 AM Removed VMware Workstation
< Back
Next >
Cancel

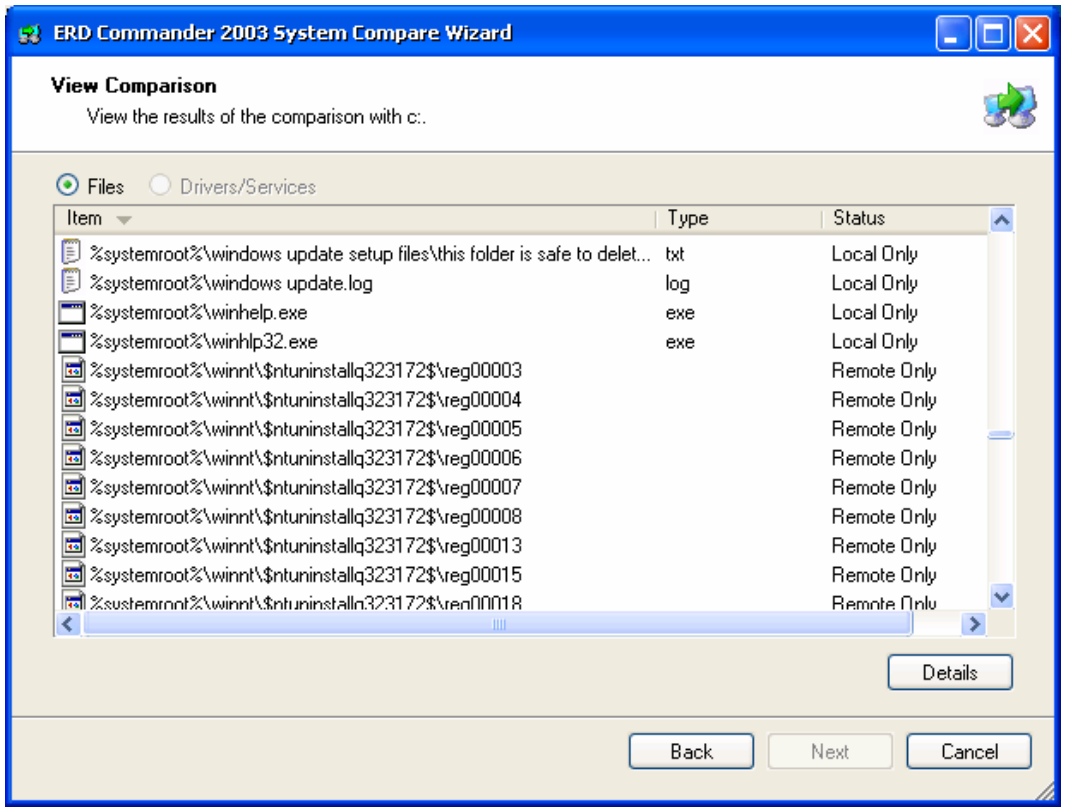
3.26 System Compare

If you have an unbootable system that was configured similarly to another installation on your network or to an on-disk image (such as an installation CD), use the ERD Commander 2003 System Compare utility to identify file, service and driver differences between the system and a reference image to help guide the repair process.

The ERD Commander 2003 System Compare utility starts by asking you to select the local installation directory. By default, this is the system directory of the installation that you logged into. However, if corruption or other issues prevent ERD Commander 2003 from finding the installation directory you can also specify a directory.

You can specify the reference installation in one of two ways: either as a computer name or as a path to an installation directory or Windows installation media root directory. You must enter computer names with a "\\" prefix e.g. "\\ref-comp". If you designate a computer or a remote path the wizard requires you to enter an account name and password with which to access the remote location. You should enter a computer name if you want to compare both file and service and driver configuration, since only file information is available for comparison if you enter a directory path.

After making your selections the ERD Commander 2003 System Compare utility performs the requested comparison and presents the results in a list. If the reference location is a computer then you have the option to see either file or driver and service differences. For files, the **Details** button or right-click context menu selection displays a dialog box with additional information about the selected file.



3.27 Running External Commands

The ERD Commander 2003 operating environment allows you to run Win32 applications other than those included on your product CD. Such External Commands may be found on the volumes of the computer that you wish to repair, or on the network. However, because the ERD Commander 2003 environment is different than that of Windows, many applications launched within it either behave incorrectly or fail to run. It should also be noted that different Windows installations provide different versions of many commands, so a particular External Command found on one system may work, while that found on another system may not. For these reasons Winternals Software does not warrant or support use of commands other than those found on your ERD Commander 2003 product CD, and a warning is displayed whenever you launch an external command from the ERD Commander 2003 Windowing Shell or an ERD Commander 2003 command prompt.

If you wish to suppress the external command dialog for commands launched from within the ERD Commander 2003 command prompt (for example, when you execute batch files that spawn them) you can set the AllowExternalCommand environment variable to a value of "yes". If you do not want to allow the execution of any external commands set the AllowExternalCommand environment variable to "no". The default value of the variable is "warn".

4 Disk Commander

Disk Commander is an advanced partition, volume, file and master boot record (MBR) salvage and repair tool that ERD Commander 2003 includes when you purchase it as part of the Winternals Administrator's Pak. You can use Disk Commander to:

- Salvage files from a volume that your operating system is having trouble accessing.
- Salvage files from a volume that your operating system does not recognize or provide a drive letter for.
- Recover deleted files.
- Repair volumes that have been damaged by a virus or been accidentally deleted by FDISK or the Windows Disk Administrator.

Disk Commander consists of a Wizard that guides you through the recovery process.

***Warning**: Some features of Disk Commander allow you to modify your disk in ways that can potentially damage or render your volumes inaccessible. Because all volumes on a disk share the same partition table it is possible that changes to one volume can impact other volumes on the disk. It is highly recommended that you use a conventional back up program to preserve as much of your data as possible before using Disk Commander to perform repairs.*

4.1 Selecting a Drive Letter to Recover

If the data you wish to recover is on a volume that is relatively intact and has a drive letter assigned to it, then you can select that drive letter and go directly to recovering files. If it does not have a drive letter assigned then there are several additional step needed for Disk Commander to locate the partition.

The version of Disk Commander you are running impacts which volumes may be recognized, since drive letter assignments are performed by the underlying operating system rather than Disk Commander. Therefore, if you

are running the DOS version of Disk Commander, or the Win32 version on a Windows 9x/Me system, you will not be able to directly select NTFS volumes. Similarly a Windows NT 4.0 system will not normally recognize FAT32 volumes.

Warning: *The drive letter assignments you see in Disk Commander may be different than what Windows assigns. Please carefully examine the sizes and labels of all of the drives before making a selection.*

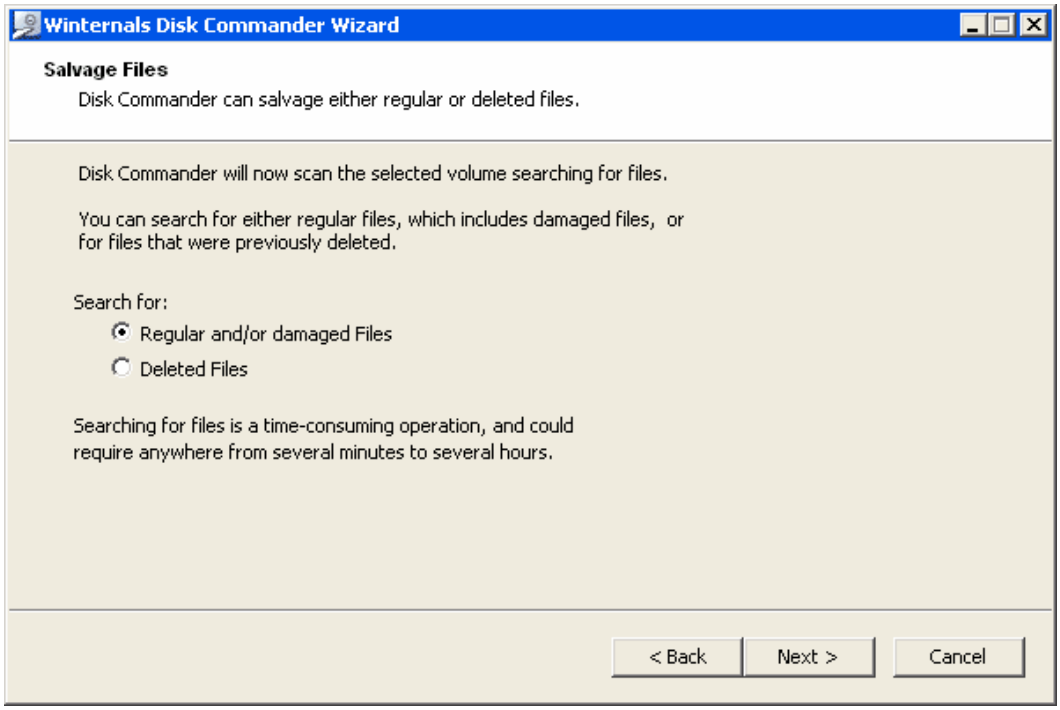
If you select a drive letter then you will be able to salvage files from the volume, but not make any kinds of repairs (normally if the volume is assigned a drive letter than there are no further repairs that Disk Commander can perform). If you wish to make repairs to the partition then indicate the volume does not have a drive letter.

By selecting a drive letter here you advance straight to the Salvaging Files screen.

4.2 Selecting a Target Disk

If the volume you are interested in was not assigned a drive letter, or you elected not to use the letter assigned, then you must help Disk Commander to locate the volume.

Select which physical hard disk that contains the volume you need to recover files from.



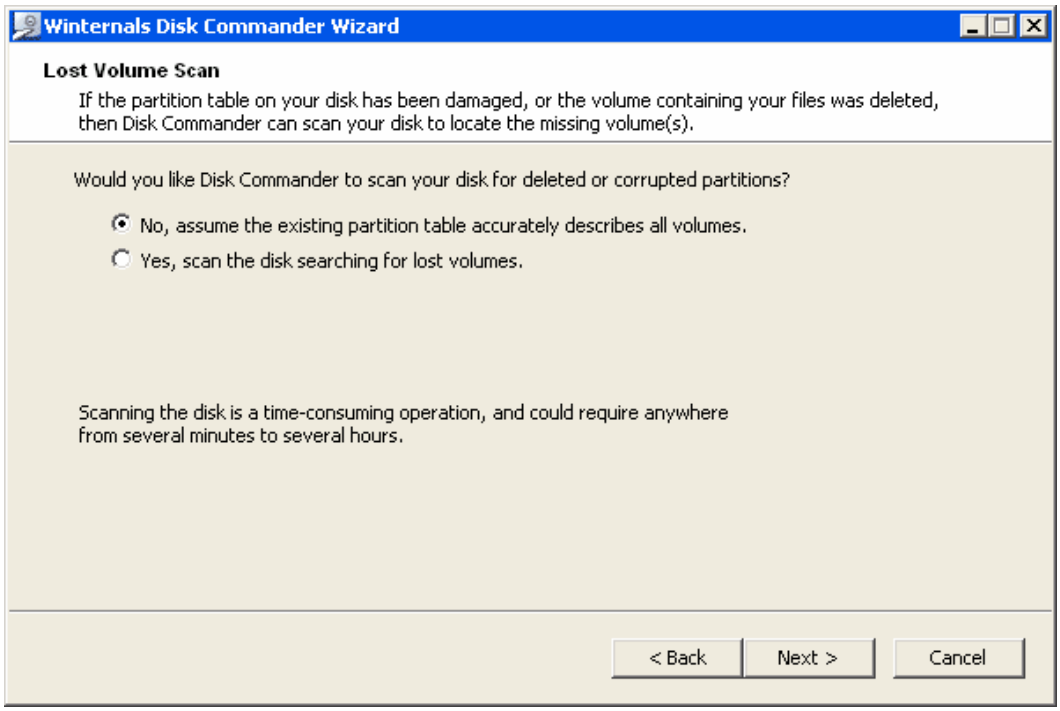
4.3 Lost Volume Scan

The next page in the wizard gives you the opportunity to scan for lost volumes. Disk Commander will always look at the partitions defined in the partition table for the disk you have selected, but it can also perform an exhaustive scan of your disk attempting to locate volumes that do not appear in your partition table.

The exhaustive scan takes a long time to perform and is usually not necessary to recover your data. You may want to skip the scan initially and

see if Disk Commander can locate your volume without it. If it cannot then back up and perform the scan.

After you perform a scan Disk Commander will save the results in a file so you do not have to perform the scan again, even if you exit and restart the program.

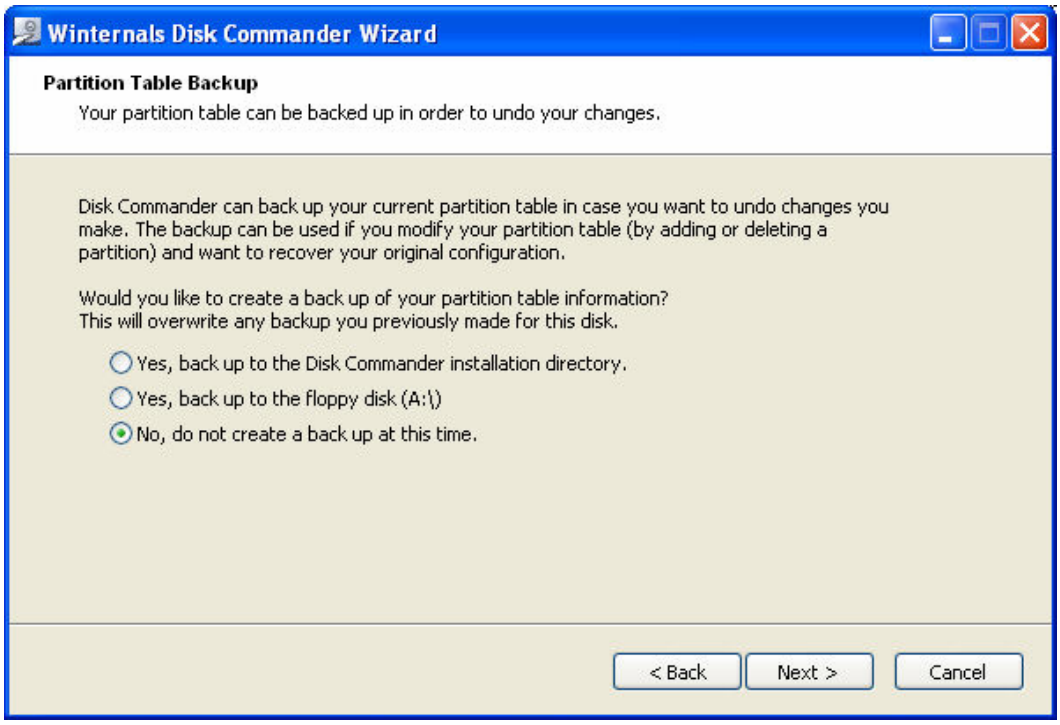


4.4 Partition Table Backup

Because Disk Commander allows you to modify your partition table, you may want to create a back up of the information stored there. Disk Commander allows you to back up the partition table entries, as well as the boot sectors of each of your partitions, and save them to a file.

The backup file can be stored in the Disk Commander installation directory (if running from a floppy disk it will be stored on the floppy disk) or on a floppy disk you designate.

You can use the back up to restore your partition table and boot sectors in the event that your changes cause additional problems with your system.



4.5 Volume Recovery

The Recover Volume screen is the main screen for analyzing and modifying your disk.

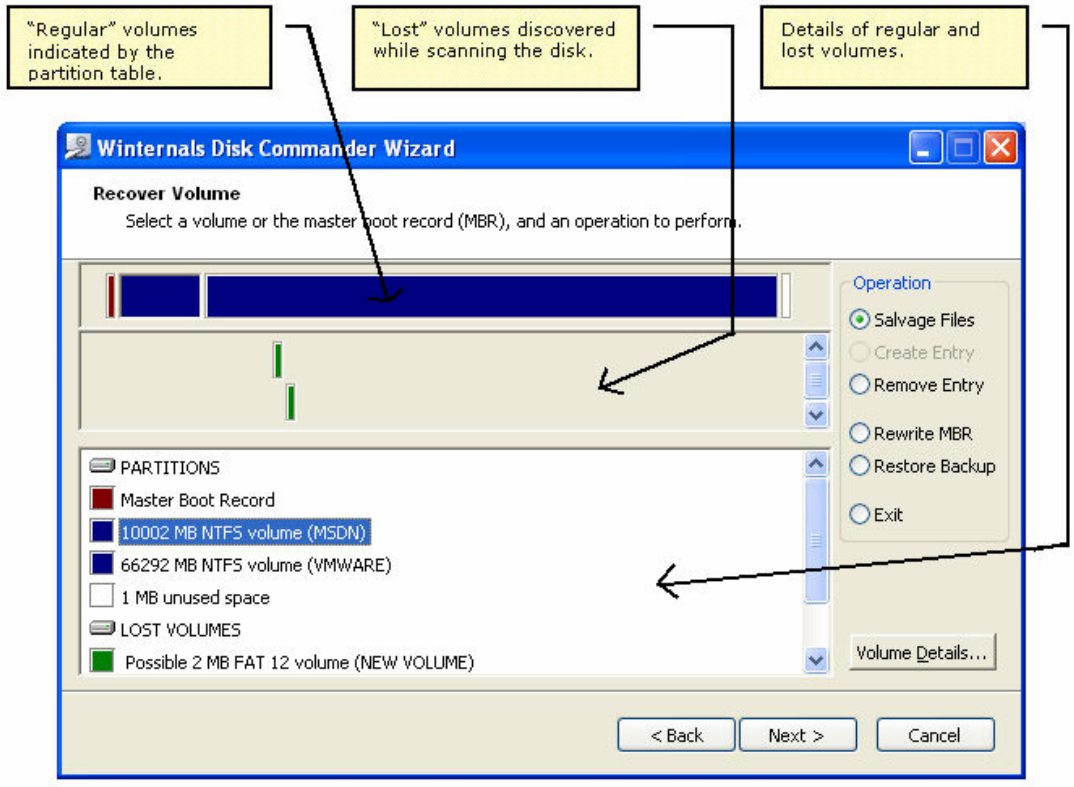
The screen displays information about your disk in several ways. The top most pane shows the layout of partitions on your disk. Every disk starts with a Master Boot Record (MBR) shown in red, followed by one or more partitions and extended partitions. NTFS volumes are shown in blue, while FAT volumes are shown in green. Extended boot records (used to delineate logical volumes) are shown in yellow.

The middle pane shows volumes that were discovered by Disk Commander while scanning your disk. (If you elected not to perform a disk scan on the **Lost Volume Scan** screen then this area will not be shown.) Some of the

volumes in this area may overlap your regular volumes; these may be remnants of volumes created and then deleted at some point in the past. You may also see volumes that seem to be identical to existing volumes, but there is a slight difference: these volumes are shown because they can be mounted using an alternate boot sector. If the regular boot sector for a volume has been corrupted you can use this "backup" version of the partition to repair or salvage data in the original.

The bottom pane provides a summary of all the displayed volumes. It first lists the regular volumes, followed by lost volumes. Clicking an entry in the top or middle pane will automatically select the corresponding entry in the bottom pane, and vice versa.

You can select a volume and click the **Details** button to obtain additional information about the volume you've selected.



4.6 Salvaging Files

Use the Salvage Files option to scan a partition for files that reside on it, and to copy those files to a safe location.

Disk Commander allows you to scan for either regular files (including files that have been damaged or rendered inaccessible by disk corruption), or for files that have been accidentally deleted.

After you select the type of files you wish Disk Commander to look for it may take several minutes to scan the volume.

Once Disk Commander has finished scanning your volume for files it presents an Explorer-like view of the files and directories it has found.

In order to copy one or more files off of the corrupt volume:

- Click on a file or directory icon.
- Click the **(De)Select** button to mark the file/directory. A black check mark on a file or directory icon indicates that it is marked to be salvaged. A gray check mark on a directory icon indicates that some of the files it contains are marked to be salvaged. Mark all files and directories you wish to salvage. You can unmark a marked file/directory by clicking the **(De)Select** button again.
- Type the path of a directory on an intact volume to which you wish to copy the marked files/directories, or use the **Browse** button to select one.
- If you wish for Disk Commander to preserve the directory structure of the files being copied then ensure that **Preserve paths** is checked. Otherwise no directories will be created when the files are copied.
- Click **Next** to begin copying files.

Once you have copied files off the volume you can exit Disk Commander, or return to this screen to copy additional files.

Even though a file appears to successfully copy, it does not necessarily mean that its contents are those it originally had. Files that are deleted may have been overwritten with other file data, and corrupt files may contain invalid data. In addition, Disk Commander reports copy errors when the amount of file data it can salvage for a file is smaller than the apparent size of the file. For these reasons you should examine salvaged data carefully to ensure that it is intact and complete.

NOTES:

- The percentage value shown next to files indicates Disk Commander's estimate as to how much of a deleted file is intact. The value is based on heuristics and is not definitive, however you can use it as guide for selecting the best candidate for a restore when there a number of deleted copies of the same file.

- After copying files and returning to this screen your selections are not automatically cleared. Select the root folder and pre **(De)Select** twice to clear all of you selections.

- Use the **Search** button to search for files or directories by name. Disk Commander will search for any file or directory whose name contains the text you enter. The use of wild cards in your search is not supported by Disk Commander.

- If a file is deleted it will be marked with a red **X.**

- If a file or directory is found but it cannot be determined which directory it belongs to (possibly because the parent directory is destroyed) then it is placed in a directory labeled "<orphan>" and marked with **X**. It is possible for there to be multiple orphan directories, each corresponding to a different directory that no longer exists.

5 Frequently Asked Questions

Why do I get access denied errors when I try to replace a system's Registry hives?

If you are running a utility that accesses the Registry of the system being repaired you will be unable to replace the Registry hives. Utilities that access the Registry include Regedit, Explorer, Service and Driver Manager, System Information, and Event Log Viewer.

Why didn't you use the Windows versions of the tools instead of writing your own?

ERD Commander 2003 includes special versions of several utilities to comply with Microsoft licensing requirements, and to provide interfaces that are intuitive in its repair environment. For example, the Windows Regedit utility would only allow you to edit the ERD Commander 2003 Registry, whereas ERD Commander 2003 Regedit allows you to edit the Registry of the installation that you wish to repair.

Why can't I have more than 4 applications active at the same time?

This limit results from the restricted environment in which ERD Commander 2003 executes.

Why are some Registry keys empty when I know I should see subkeys?

When you use Regedit, ERD Commander 2003 attempts to load the Registry hives (files) that make up the Registry keys that you are familiar with. The Logon application informs you if it cannot load a hive, and those that it cannot load result in empty Registry keys within Regedit and possibly limitations to the functionality of other ERD Commander 2003 applications. Registry hives reside in

%systemroot%\system32\config and cannot be loaded if they are either missing or corrupt. The correspondence between hives and their Registry keys is as follows:

Hive Name	Registry Key(s)
SAM	HKLM\SAM
SECURITY	HKLM\SECURITY
SOFTWARE	HKLM\SOFTWARE
SYSTEM	HKLM\SYSTEM, HKCR

Why does ERD Commander 2003 freeze when I eject the ERD Commander 2003 CD-ROM?

Individual ERD Commander 2003 applications are loaded into memory on demand. If you remove the ERD Commander 2003 CD the system cannot read any items not already in memory, potentially causing a fatal error within the ERD Commander 2003 environment. In this event the system must be rebooted to continue running ERD Commander 2003.

Why does my application behave strangely or fail to execute when I run it inside of ERD Commander 2003?

The ERD Commander 2003 environment is a stripped-down version of the standard Windows XP environment and is missing many non-core system files, services, and run-time support.

6 Sales

Order Winternals products online at www.winternals.com, or by fax, phone or email:

Phone: (800) 408-8415
(512) 330-9130
Fax: (512) 330-9131

Email: sales@winternals.com

Mail: Winternals Software LP
3101 Bee Caves Road
Suite 150
Austin, TX 78746
USA

7 Technical Support

To view Online Help, press F1 or select Help from the ERD Commander 2003 **Start** Menu.

To access the ERD Commander 2003 Support Knowledge Base, visit our support web site at:
www.winternals.com/support

You may also request help by email for issues not covered in the Online Help or Support Knowledge Base. Please visit:
www.winternals.com/support/getsupport.asp or send email to:
support@winternals.com

Customers who have purchased Product Assurance may receive phone support by calling 512-330-9861.

Before contacting support, please determine if the problem is reproducible, and if so, record the steps necessary to reproduce it. In addition, please have the following information about your system ready:

- Windows version (including Service Pack) of the system being repaired,
- Memory size, disk types, and file system types
- Version of ERD Commander 2003
- The License Number shown on the lower right of your ERD Commander 2003 desktop

8 Index