chapter 19

Troubleshooting Windows

"Chaos is inherent in all compounded things. Strive on with diligence."

—Buddha

In this chapter, you will learn how to

- **Troubleshoot Windows boot problems**
- **Troubleshoot Windows GUI problems**
- **Troubleshoot Windows application problems**

This chapter looks at Windows problems from the ground up. It starts with catastrophic failure—a PC that won't boot—and then discusses ways to get past that problem. The next section covers the causes and workarounds when the Windows GUI fails to load. Once you can access the Windows GUI, the many Windows diagnostic and troubleshooting tools that you've spent so much time learning about come to your fingertips. The chapter finishes with a discussion on application problems.

Failure to Boot

When Windows fails to boot, you need to determine whether the problem relates to hardware or software. You'll recall from Chapter 12 that a hard drive needs proper connectivity and power, and that CMOS must be configured correctly. If not, you'll get an error like the one in Figure 19.1. We'll look more closely at these sorts of scenarios in the first part of this section as a refresher.

But after the drive powers on and the POST completes successfully, the computer tries to boot to an OS. Failure at *this* point gives you an entirely different set of errors such as *NTLDR is Missing* or *BOOTMGR is missing* (see Figure 19.2). You need a totally different set of tools from the ones used to troubleshoot hardware or CMOS issues. Windows XP and Windows Vista/7 boot differently, so to troubleshoot these failures to boot you need to know both processes and the tools available. We'll look at this type of scenario in the second part of this section.

• **Figure 19.1** If you see this screen, the problem is with hardware. Windows hasn't even started trying to boot.

• **Figure 19.2** Scary error

Failure to Boot: Hardware or Configuration

Most failed boot scenarios require you to determine where the fault occurred: with the hardware and configuration, or in Windows. This is a pretty straightforward problem. Imagine that a user calls and says "My PC won't boot" or "My computer is dead." At this point, your best tools are knowledge of the boot process and asking lots of questions. Here are some I use regularly:

"What displays on the screen—if anything—after you press the power button on the case?"

"What do you hear—if anything—after you press the power button on the case?"

"Is the PC plugged in?"

"Do you smell anything weird?"

Hardware problems can give you a blank screen on bootup, so follow the tried and true troubleshooting methodology for hardware. Make sure everything is plugged in and turned on. If the PC is new, as in less than 30 days old, you know it might have suffered a burn-in failure. If the customer smells something, one of the components might have fried. Try replacing with known good devices: RAM, power supply, CPU, hard drive, motherboard.

If the user says that the screen says "No boot device detected" and the system worked fine before, it *could* mean something as simple as the computer has attempted to boot to an incorrect device, such as to something other than the primary hard drive. This scenario happens all the time. Someone plugs a thumb drive into a USB port and CMOS is configured to boot to removable media before hard drives. The first few times it happened to me, I nearly took my machine apart before experiencing that head-slapping moment. I removed the thumb drive and then watched Windows boot normally.

The CompTIA A+ 802 exam objectives list "Invalid boot disk" as a symptom of a Windows problem, but it's more typical of a CMOS or hardware issue.

Failure to Boot: Windows XP

Windows boot errors take place in those short moments between the time POST ends and the *Loading Windows* screen begins. For Windows XP to start loading the main operating system, the critical system files ntldr, ntdetect.com, and boot.ini must reside in the root directory of the C: drive, and boot.ini must point to the Windows boot files. In a scenario where any of these requirements isn't in place, the system won't get past this step. Here are some of the common error messages you see at this point:

No Boot Device Present

NTLDR Bad or Missing

Invalid BOOT.INI

The CompTIA A+ 802 exam objectives describe these error messages as "Missing NTLDR" and "Missing Boot.ini." The intent is the same, so don't be surprised by the slight difference in wording.

These text errors take place very early in the startup process. That's your big clue that you have a boot issue. If you get to the Windows splash screen and then the computer locks up, that's a whole different game, so know the difference.

If you are in a failure to boot scenario where you get one of the catastrophic error messages with a Windows XP system, you have a three-level

process to get back up and running. You first should attempt to repair. If that fails, attempt to restore from a backup copy of Windows. If restore either is not available or fails, your only recourse is to rebuild. You will lose data at the restore and rebuild phases, so you definitely want to spend a lot of energy on the repair effort first! Follow this process when faced with a corrupted system files or missing operating system scenario.

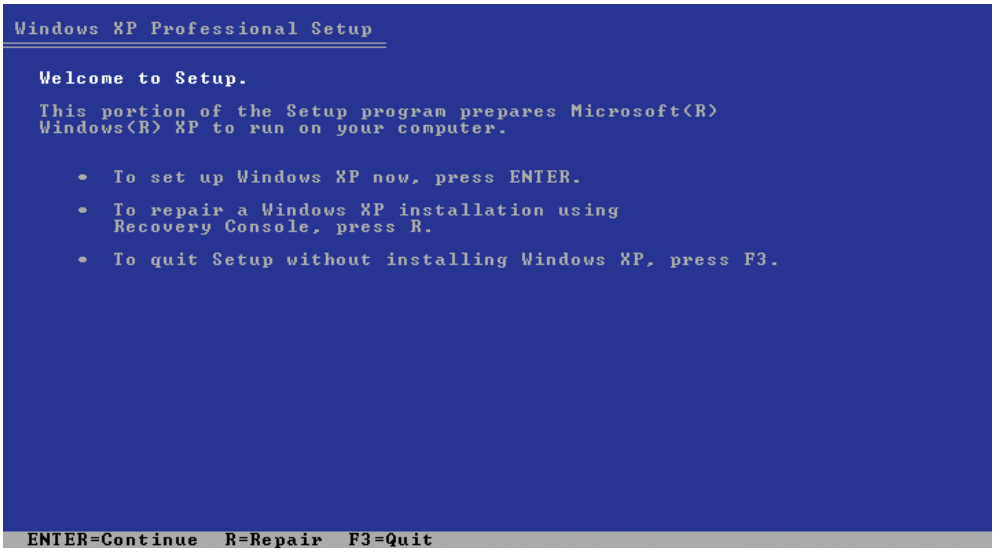
Attempt to Repair by Using the Recovery Console

To begin troubleshooting one of these errors, boot from the installation CD-ROM. You have three options from the initial screen: set up Windows XP, repair using the Recovery Console, and quit Setup (see Figure 19.3). The **Recovery Console**, as you'll recall from earlier chapters, provides a command-line interface for working with Windows before the GUI starts. Press R to start the Recovery Console.

When you select the Recovery Console, you will see a message about ntdetect, another message that the Recovery Console is starting up, and then you are greeted with the following message and command prompt:

```
Microsoft Windows XP<TM> Recovery Console.
The Recovery Console provides system repair and recovery
functionality.
Type Exit to quit the Recovery Console and restart the computer.

1: C:\WINDOWS
Which Windows XP installation would you like to log onto
<To cancel, press ENTER>?
```

The cursor is a small, white rectangle sitting to the right of the question mark on the last line. If you are not accustomed to working at the command prompt, this may be disorienting. If there is only one installation of Windows XP on your computer, type the number **1** at the prompt and press the ENTER key. If you press ENTER before typing in a valid selection, the Recovery Console will cancel and the computer will reboot. The only choice you can



• **Figure 19.3** Initial Windows XP Setup screen

Try This!

Installing the Recovery Console

If you like to be proactive, you can install the Recovery Console on your hard drive so that it is one of your startup options and does not require the Windows XP CD-ROM to run. First, you need to log on to the system with the administrator account. Next, grab a Windows XP installation CD-ROM and drop it in your system. If the Autorun function kicks in, just click the No button. To install the Recovery Console and make it a part of your startup options, click the Start button, select Run, and type the following (if your CD-ROM drive uses a different drive letter, substitute it for the D: drive):

d:\i386\winnt32 /cmdcons

Then just follow the instructions on the screen. If you are connected to the Internet, allow the Setup program to download updated files. From now on, every time the system boots, the OS selection menu will show your Windows OS and the Microsoft Windows Recovery Console. It may also show other choices if yours is a multiboot computer.

make in this example is 1. Having made that choice, the screen displays a new line, followed by the cursor:

```
Type the Administrator password:
```

Enter the Administrator password for that computer and press ENTER. The password does not display on the screen; you see asterisks in place of the password. The screen still shows everything that has happened so far, unless something has happened to cause an error message. It now looks like this:

```
Microsoft Windows XP<TM> Recovery Console.
The Recovery Console provides system repair and recovery
functionality.
Type Exit to quit the Recovery Console and restart the computer.

1: C:\WINDOWS
Which Windows XP installation would you like to log onto
<To cancel, press ENTER>? 1
Type the Administrator password: ********
C:\Windows>
```

By now, you've caught on and know that there is a rectangular prompt immediately after the last line. Now what do you do? Use the Recovery Console commands, of course. The Recovery Console uses many of the commands that work in the Windows command-line interface that you explored in Chapter 18, as well as some commands uniquely its own. Table 19.1 lists common Recovery Console commands.

The Recovery Console shines in the business of manually restoring Registries, stopping problem services, rebuilding partitions (other than the system partition), and using the expand program to extract copies of corrupted files from an optical disc or floppy disk.

Table 19.1 Common Recovery Console Commands

Command	Description
attrib	Changes attributes of selected file or folder
cd (or chdir)	Displays current directory or changes directories
chkdsk	Runs CheckDisk utility
cls	Clears screen
copy	Copies from removable media to system folders on hard disk. No wildcards
del (or delete)	Deletes service or folder
dir	Lists contents of selected directory on system partition only
disable	Disables service or driver
diskpart	Creates/deletes partitions
enable	Enables service or driver
extract	Extracts components from .cab files
fixboot	Writes new partition boot sector on system partition
fixmbr	Writes new master boot record (MBR) for partition boot sector
format	Formats selected disk
listsvc	Lists all services on system
logon	Enables you to choose which Windows installation to log on to if you have more than one
map	Displays current drive letter mappings
md (or mkdir)	Creates a directory
more (or type)	Displays contents of a text file
rd (or rmdir)	Removes a directory
ren (or rename)	Renames a single file
systemroot	Makes current directory system root of drive you're logged on to
type	Displays contents of a text file

Using the Recovery Console, you can reconfigure a service so that it starts with different settings, format partitions on the hard drive, read and write on local FAT or NTFS partitions, and copy replacement files from a floppy or optical disc. The Recovery Console enables you to access the file system and is still constrained by the file and folder security of NTFS, which makes it a more secure tool to use than some third-party solutions.

The Recovery Console also works great for fixing three items: repairing the MBR, reinstalling the boot files, and rebuilding boot.ini. Let's look at each of these.

A bad boot sector usually shows up as a No Boot Device error. If it turns out that this isn't the problem, using the Recovery Console command to fix it won't hurt anything. At the Recovery Console prompt, just type

fixmbr

This fixes the master boot record.

Missing system files are usually indicated by the error *NTLDR bad or missing*. Odds are good that if ntdlr is missing, so are the rest of the system files. To fix this, get to the root directory (cd\—remember that from

Chapter 18?) and type the following line (substituting the drive letter of the optical drive for *d:* in the example):

copy d:\i386\ntldr

Then type this line:

copy d:\i386\ntdetect.com

This takes care of two of the big three and leads us to the last issue, rebuilding boot.ini. If the boot.ini file is gone or corrupted, run this command from the Recovery Console:

bootcfg /rebuild

The Recovery Console will try to locate all installed copies of Windows and ask you if you want to add them to the new boot.ini file it's about to create. Say yes to the ones you want.

If all goes well with the Recovery Console, do a thorough backup as soon as possible (just in case something else goes wrong). If the Recovery Console does not do the trick, the next step is to restore Windows XP.

To use the Windows XP System Restore, you need to be able to get into Windows. "Restore" in the context used here means to give you an option to get into Windows.

Attempt to Restore

If you've been diligent about backing up, you can attempt to restore to an earlier, working copy of Windows. Assuming you made an Automated System Recovery (ASR) backup, this will restore your system to a previously installed state, but you should use it as a last resort. You lose everything on the system that was installed or added after you created the ASR disk. If that's the best option, though, follow the steps outlined in Chapter 17.

Rebuild

If faced with a full system rebuild, you have several options, depending on the particular system. You could simply reboot to the Windows CD-ROM and install right on top of the existing system, what's called a *repair installation*. To avoid losing anything important, though, you'd be better off swapping the C: drive for a blank hard drive and installing a clean version of Windows.

Most OEM systems come with a misleadingly named *Recovery CD* or *recovery partition*. The Recovery CD is a CD-ROM that you boot to and run. The recovery partition is a hidden partition on the hard drive that you activate at boot by holding down a key combination specific to the manufacturer of that system. (See the motherboard manual or users' guide for the key combination and other details.) Both "recovery" options do the same thing—restore your computer to the factory-installed state. If you run one of these tools, *you will wipe everything off your system*—all personal files, folders, and programs will go away! Before running either tool, make sure all important files and folders are backed up on an optical disc or spare hard drive.

When you attempt to install Windows XP onto a system with Windows XP already installed, the setup process will detect the previous OS and prompt you to repair or install a fresh copy of Windows.

Failure to Boot: Windows Vista and Windows 7

Two critical boot files risk corruption in Windows Vista and Windows 7, bootmgr and bcd, both of which you can fix with one tool, bcdedit. You can use this tool in the Windows Recovery Environment.

WinPE and the Death of the Recovery Console

With Windows Vista, Microsoft upgraded the installation environment from the 16-bit text mode environment used in every previous version of Windows to 32- and 64-bit. This upgrade enabled the Windows installation process to go graphical and support features such as a mouse pointer and clickable elements, rather than relying on command-line tools. Microsoft calls the installation environment the **Windows Preinstallation Environment** (**WinPE** or *Windows PE*).

With Windows PE, you can boot directly to the Windows DVD. This loads a limited-function graphical operating system that contains both troubleshooting and diagnostic tools, along with installation options. The Windows installation media is called a **Live DVD** because WinPE loads directly from disc into memory and doesn't access or modify the hard drive.

When you access Windows PE and opt for the troubleshooting and repair features, you open a special set of tools called the **Windows Recovery Environment** (**WinRE** or *Windows RE*). The terms can get a little confusing because of the similarity of letters, so mark this: Windows RE is the repair tools that run within Windows PE. WinPE powers WinRE. Got it? Let's tackle WinRE.

Although here I discuss only how WinPE helps boot repair, know that WinPE goes much further. WinPE can assist unattended installations, network installations, and even booting diskless workstations on a network.

Microsoft also refers to the Windows Recovery Environment as the *System Recovery Options menu*. It's unclear as of this writing which label CompTIA will use.

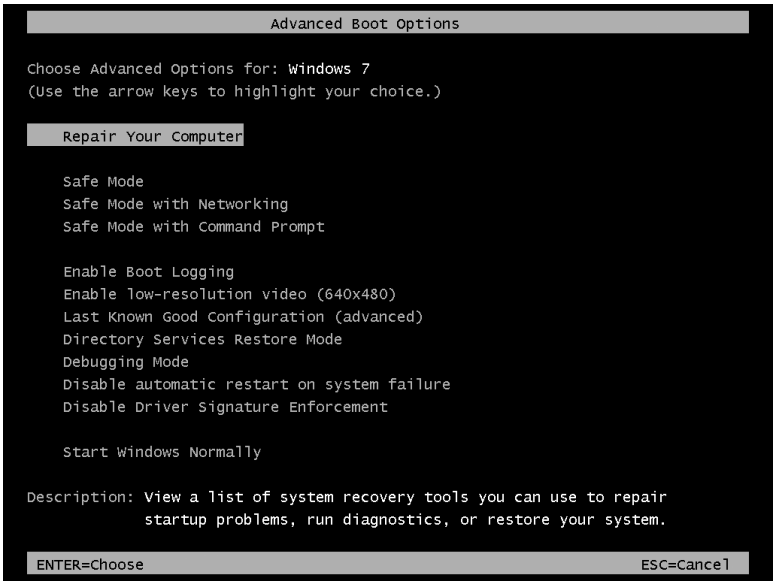
Enter Windows RE

It would be unfair to say that the Windows Recovery Environment only replaces the Recovery Console. WinRE includes an impressive, powerful set of both automated and manual utilities that collectively diagnoses and fixes all but the most serious of Windows boot problems. Although WinRE does all the hard work for you, you still need to know how to access and use it. When faced with a failure to boot scenario in Windows Vista or Windows 7, WinRE is one of your primary tools.

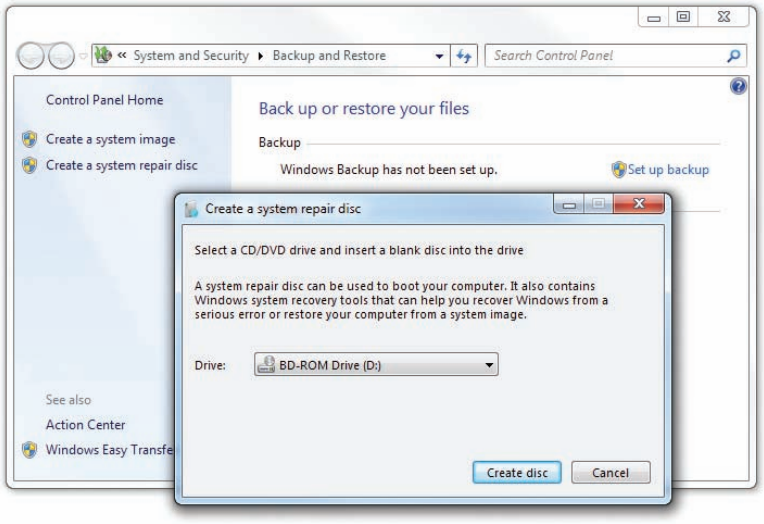
Getting to Windows RE

In Windows 7, you can access WinRE in three ways. (See the Exam Tip for Windows Vista options.) First, you can boot from the Windows installation media and select *Repair*. Second, you can use the *Repair Your Computer* option on the Advanced Boot Options (F8) menu (see Figure 19.4). Third, you can create a system repair disc before you have problems. Go to Control Panel | System and Security | Backup and Restore and select *Create a system repair disc*, which opens the dialog box shown in Figure 19.5.

Windows Vista does not have the Repair Your Computer option on the Advanced Boot Options menu. You can either use a Windows installation media or, if you have SP1 or later, make a bootable system repair disc.



• **Figure 19.4** Selecting Repair Your Computer in the Advanced Boot Options menu



• **Figure 19.5** Making a system repair disc in Windows 7

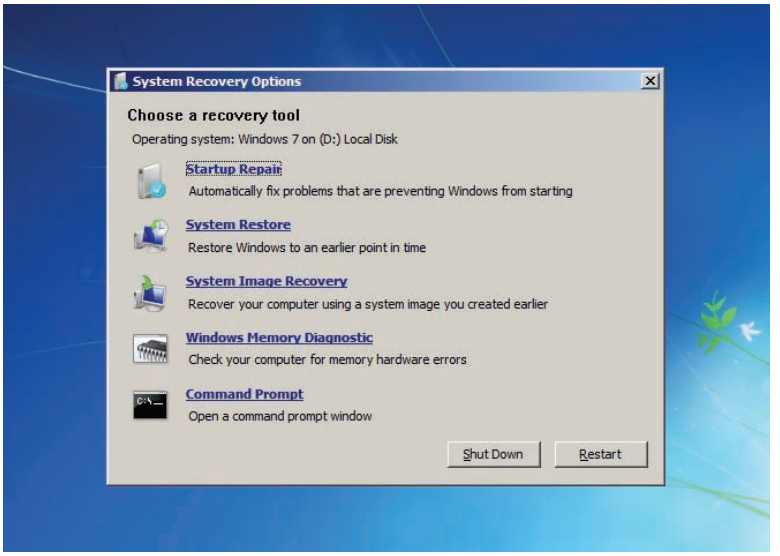
Although any of these methods works fine, I recommend that you access WinRE from the Windows installation media for three reasons:

- The hard drive can be so messed up that you won't make it to the Advanced Boot Options menu.
- Accessing WinRE using the Repair Your Computer option in the Advanced Boot Options menu requires a local administrator password.
- Using a bootable disc enables you to avoid any malware that might be on the system.

Using Windows RE

No matter how you choose to access the Windows Recovery Environment, the main menu looks the same (see Figure 19.6). You have five options in WinRE:

- Startup Repair
- System Restore
- System Image Recovery (Windows 7) or Windows Complete PC Restore (Vista)
- Windows Memory Diagnostics (Tool) (only Vista includes "Tool" in the name)
- Command Prompt



• **Figure 19.6** Recovery Environment main screen

The name of the third option differs between Windows 7 and Windows Vista, though the intent—rebuilding from a backup—is the same. I'll talk about how these options differ a little later in the chapter.

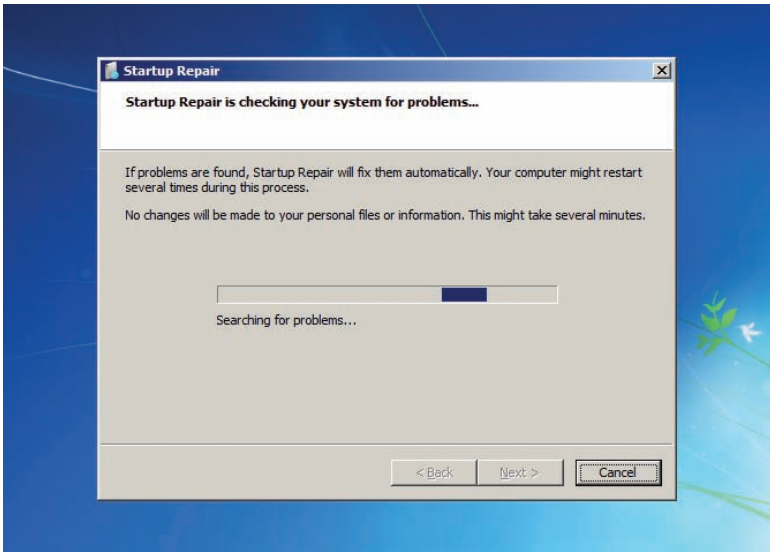
Make sure you know how to access the Windows Recovery Environment and what each of the available tools does.

Startup Repair The **Startup Repair** utility serves as a one-stop, do-it-all option (see Figure 19.7). When run, it performs a number of repairs, including:

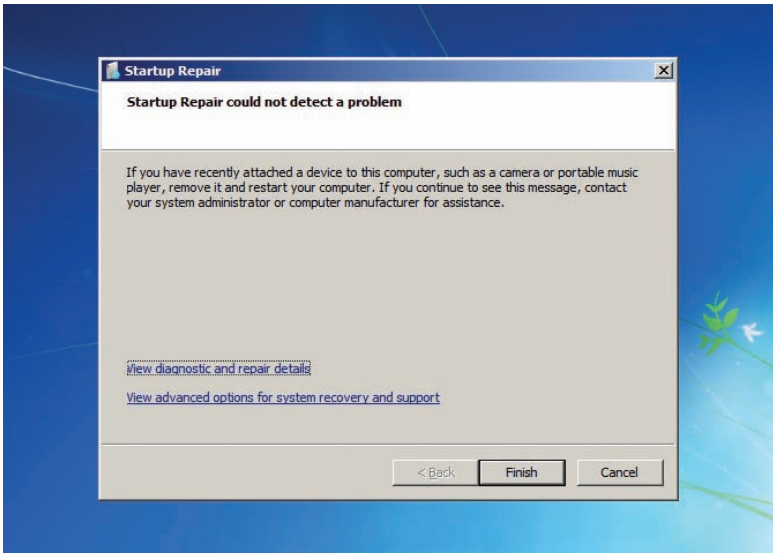
- Repairs a corrupted Registry by accessing the backup copy on your hard drive
- Restores critical system and driver files
- Runs the equivalent of the Recovery Console's fixboot and fixmbr
- Rolls back any non-working drivers
- Uninstalls any incompatible service packs and patches
- Runs chkdsk
- Runs a memory test to check your RAM

Startup Repair fixes almost any Windows boot problem. In fact, if you have a system with one hard drive containing a single partition with Windows Vista or Windows 7 installed, you'd have trouble finding something it *couldn't* fix. Upon completion, Startup Repair shows the screen shown in Figure 19.8.

Note the link in Figure 19.8 that says *View diagnostic and repair details*. This opens a text file called srttrail.txt that lists exactly what



• **Figure 19.7** Startup Repair in action



• **Figure 19.8** Startup Repair complete; no problems found

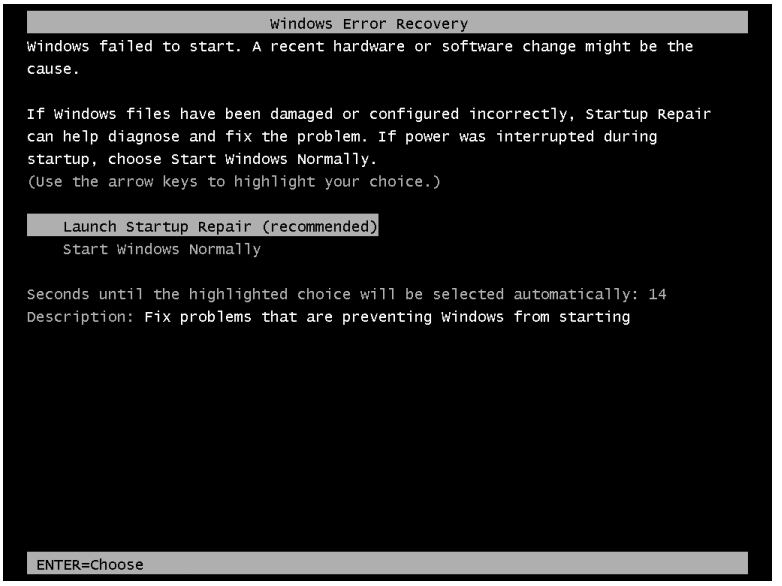
The *View advanced options for system recovery and support* link simply returns you to the main screen.

the program found, what it fixed, and what it failed to do. It may look cryptic, but you can type anything you find into Google for more information. I've reproduced the beginning of the (very long) srttrail.txt file here:

```
Startup Repair diagnosis and repair log
---------------------------
Last successful boot time: 7/14/2012 2:37:43 AM (GMT)
Number of repair attempts: 6

Session details
---------------------------
System Disk = \Device\Harddisk0
Windows directory = C:\Windows
AutoChk Run = 0
Number of root causes = 1

Test Performed:
---------------------------
Name: Check for updates
Result: Completed successfully. Error code =  0x0
Time taken = 32 ms

Test Performed:
---------------------------
Name: System disk test
Result: Completed successfully. Error code =  0x0
Time taken = 0 ms
```

In Windows 7, Startup Repair starts automatically if your system detects a boot problem. If you power up a Windows system and see the screen shown in Figure 19.9, Windows has detected a problem in the startup process.

Personally, I think this menu pops up way too often. If you fail to shut down your computer properly, for example, this menu appears. In this case,



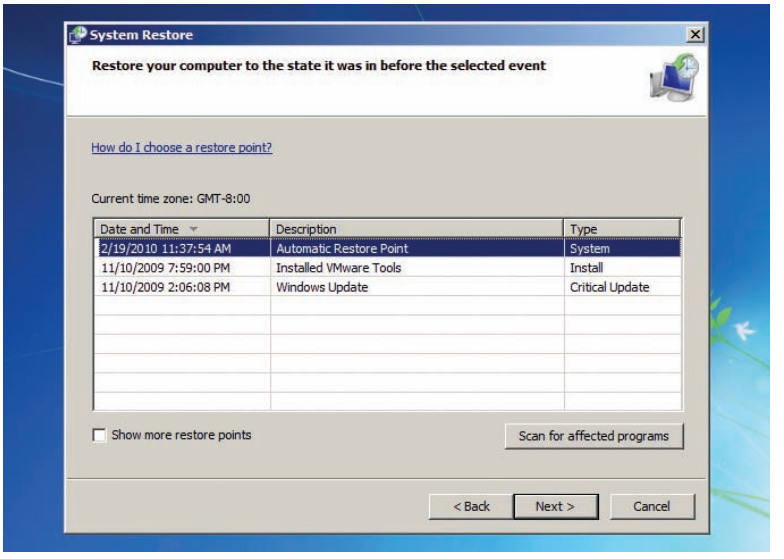
• **Figure 19.9** Windows Error Recovery

you can save time by booting normally. When in doubt, however, go ahead and run Startup Repair. It can't hurt anything.

A powerful tool like Startup Repair still doesn't cover everything. You may have specific needs that require more finesse than a single, do-it-all approach. In many cases, you've already discovered the problem and simply want to make a single fix. You might want to perform a system restoration or check the memory. For this, we'll need to explore the other four options available in WinRE.

If you have trouble booting your computer, you should try Startup Repair first.

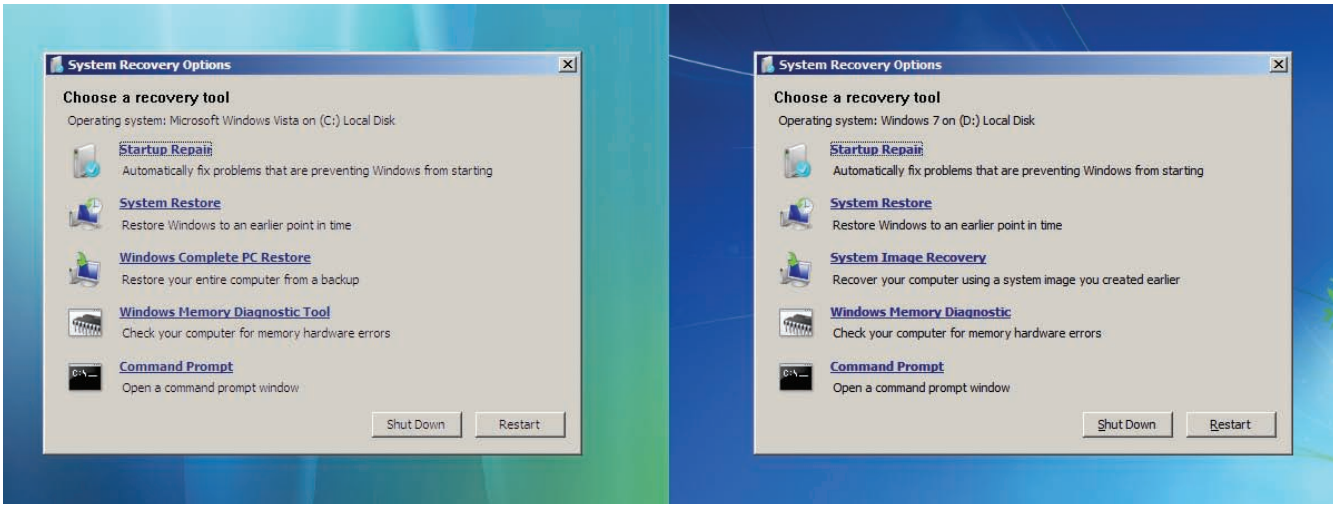
System Restore **System Restore** does the same job here it has done since Microsoft first introduced it in Windows Me, enabling you to go back to a time when your computer worked properly. Placing this option in Windows RE gives those of us who make many **restore points**—snapshots of a system at a given point of time—a quick and handy way to return our systems to a previous state (see Figure 19.10).



• **Figure 19.10** System Restore points

System Image Recovery/Windows Complete PC Restore Windows 7's backup tools differ from Windows Vista's. Note Figure 19.11, which shows the Windows Vista Recovery Environment menu on the left next to the Windows 7 Recovery Environment on the right. The third WinRE option differs. Windows Vista uses the Windows Complete PC Restore utility, whereas Windows 7 includes the System Image Recovery tool.

With an image in hand, you can use the Windows Complete PC Restore/System Image Recovery tool to restore your system after a catastrophe.



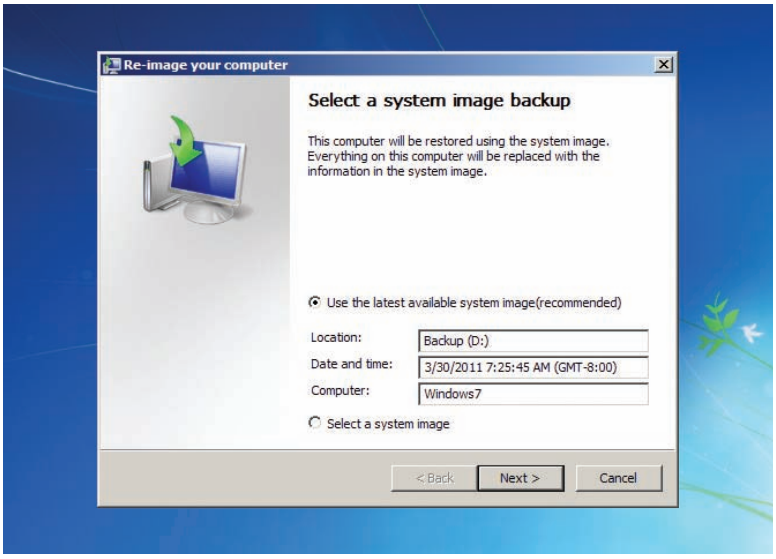
• **Figure 19.11** The WinRE options in Windows Vista (left) and Windows 7 (right)

The CompTIA A+ 802 exam objectives use the phrase *recovery image*, which conflates separate tools in Windows 7. You can use Backup and Restore to create a system image and a system repair disc. You can use the system repair disc to get to the System Image Recovery that uses the system image on the second disc to write a "fixed" or previously working version of Windows 7 to the hard drive. Got all that?

If you have the drive containing the system image plugged in when you first run the wizard, it should detect your latest backup and present you with the dialog box shown in Figure 19.12. If it doesn't list a system image or it lists the wrong one, you can select an image from another date on the same disk or even a remote network share.

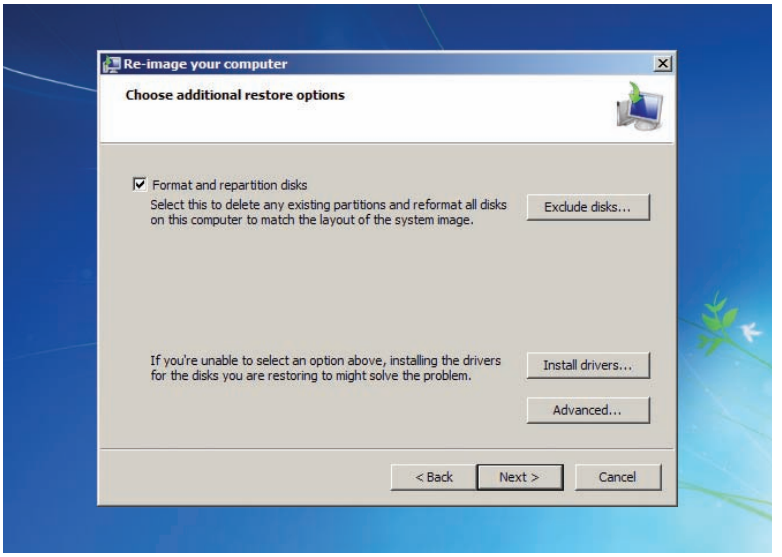
After you select the image you want to restore, the utility presents you with a few more options, as shown in Figure 19.13. Most importantly, you can choose to format and repartition disks. With this option selected, the utility wipes out the existing partitions and data on all disks so the restored system will get the same partitions that the backed-up system had.

After you click Finish on the confirmation screen (see Figure 19.14), which also contains a final warning, the restore process begins (see Figure 19.15). The utility removes the old system data and then copies the backed-up system image to the hard drive(s). Once the process completes, your system reboots and should start up again with all of your data and programs just where you left them when you last backed up.

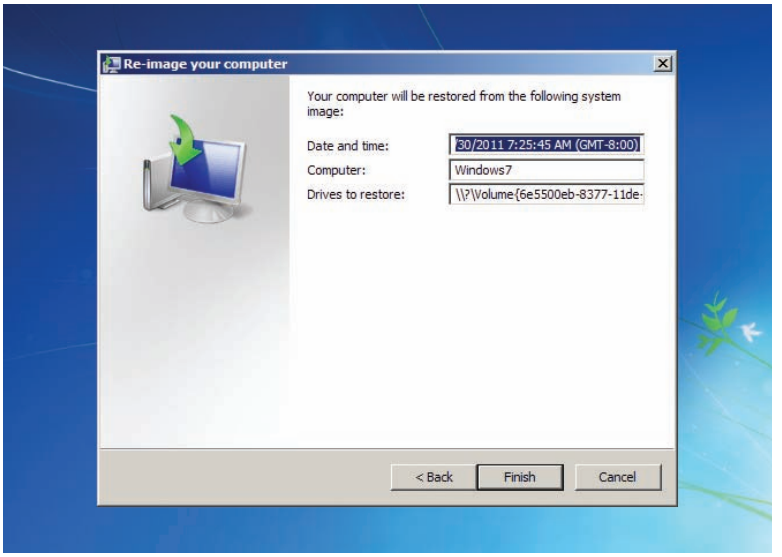


• **Figure 19.12** Selecting a system image

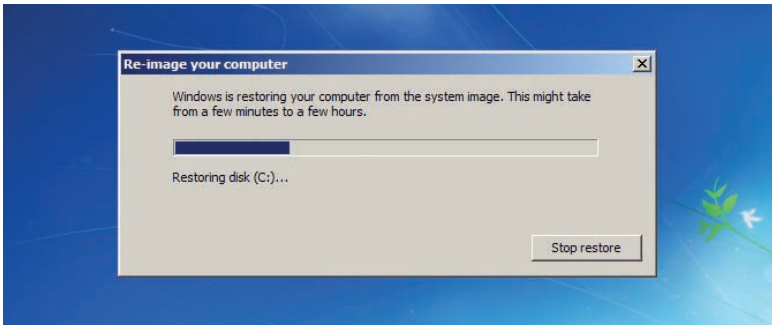
Windows Memory Diagnostics (Tool) Bad RAM causes huge problems for any operating system, creating scenarios where computers get Blue Screens of Death (BSoDs), system lockups, and continuous reboots. Starting with Windows Vista, Microsoft added a memory tester to the Windows Recovery Environment. When you click the Windows Memory Diagnostic (Tool) link from the main WinRE screen, it prompts you to *Restart now and check for problems (recommended)* or *Check for problems the next time I start my*



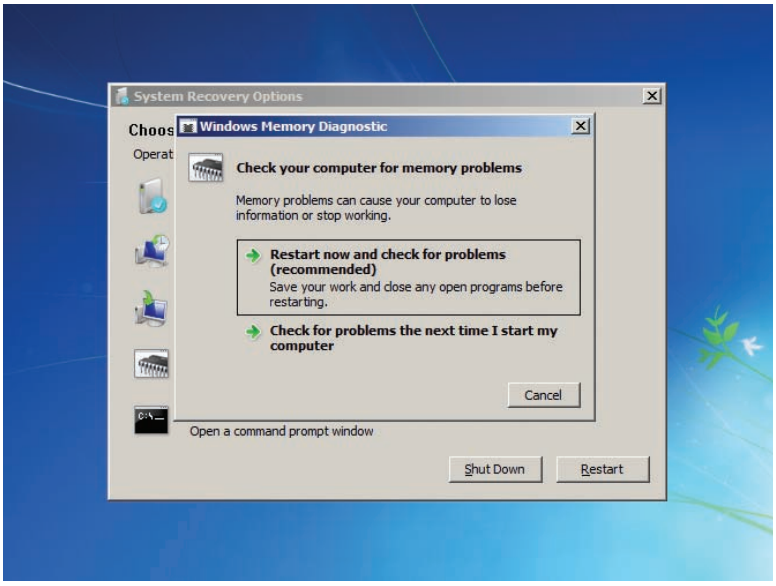
• **Figure 19.13** Additional restore options



• **Figure 19.14** Confirming your settings



• **Figure 19.15** Restoring your computer



• **Figure 19.16** Windows Memory Diagnostic screen

computer (see Figure 19.16). It doesn't really matter which option you choose, but if you think you need to test the system's RAM, that probably means you should do it now.

Once you restart, your system immediately starts running the Windows Memory Diagnostics Tool, as shown in Figure 19.17. While the program runs, you can press F1 to see the Memory Tester options (see Figure 19.18).

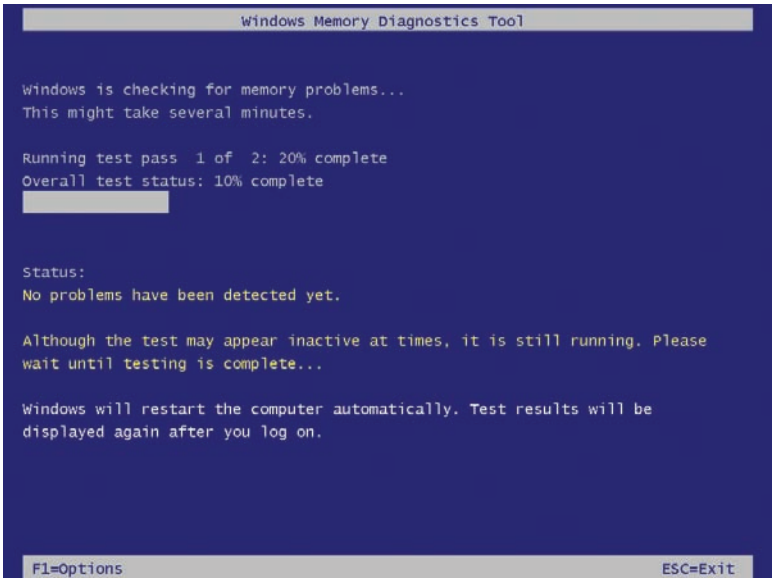
The tool lists three important Test Mix options at the top of the screen: Basic, Standard, and Extended. *Basic* runs quickly (about one minute) but performs only light testing. *Standard*, the default choice, takes a few minutes and tests more aggressively. *Extended* takes hours (you should let it run overnight), but it will very aggressively test your RAM.

This tool includes two other options: Cache and Pass Count. The *Cache* option enables you to set whether the tests use the CPU's built-in cache as well as override the default cache settings for each test type. Simply leave Cache set at Default and never touch it. *Pass Count* sets the number of times each set of tests will run. This option defaults to 2.

After the tool runs, your computer reboots normally. You can open Event Viewer to see the results (see Figure 19.19).

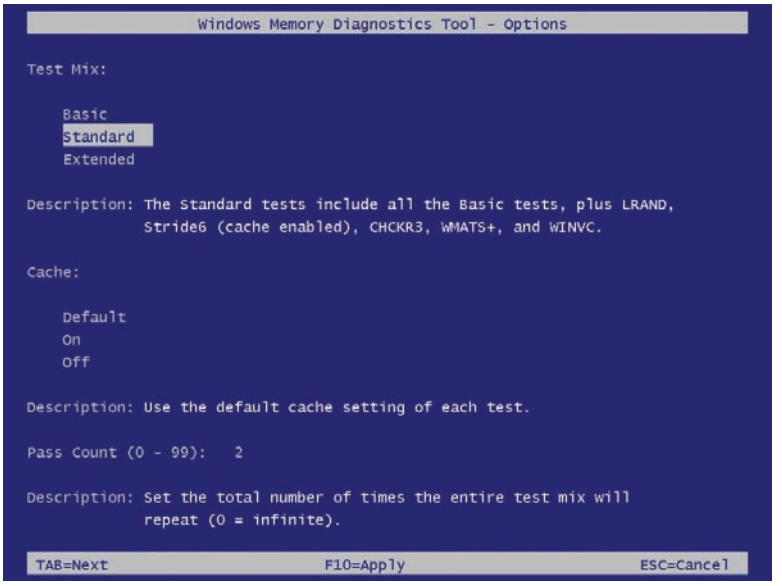
Sadly, I've had rather poor results with the Windows Memory Diagnostics Tool. We keep lots of bad RAM around the labs here at Total Seminars, and, when put to the test, we were unable to get this tool to do anything other than give us a BSoD or lock up the system. We still turn to tried-and-tested tools such as the free Memtest86+ when we're worried about bad RAM.

You can also find the Windows Memory Diagnostics Tool in the Control Panel under System and Security | Administrative Tools, or start it from an administrative command prompt using the **mdsched** command.



• **Figure 19.17** Windows Memory Diagnostics Tool running

Command Prompt The last, most interesting, and easily nerdiest option in the WinRE menu is Command Prompt. Unlike the Recovery Console, the WinRE command prompt is a true 32- or 64-bit prompt that functions similarly to the regular command prompt. WinRE's command prompt, however, includes an important utility (bootrec) that you can't find in the regular command prompt. The WinRE command prompt also lacks a large number of the command-prompt tools you'd have in a regular Windows command prompt (though all the important ones remain). Let's begin by looking at the bootrec command. After that, we'll look at some other utilities that the WinRE command prompt offers.



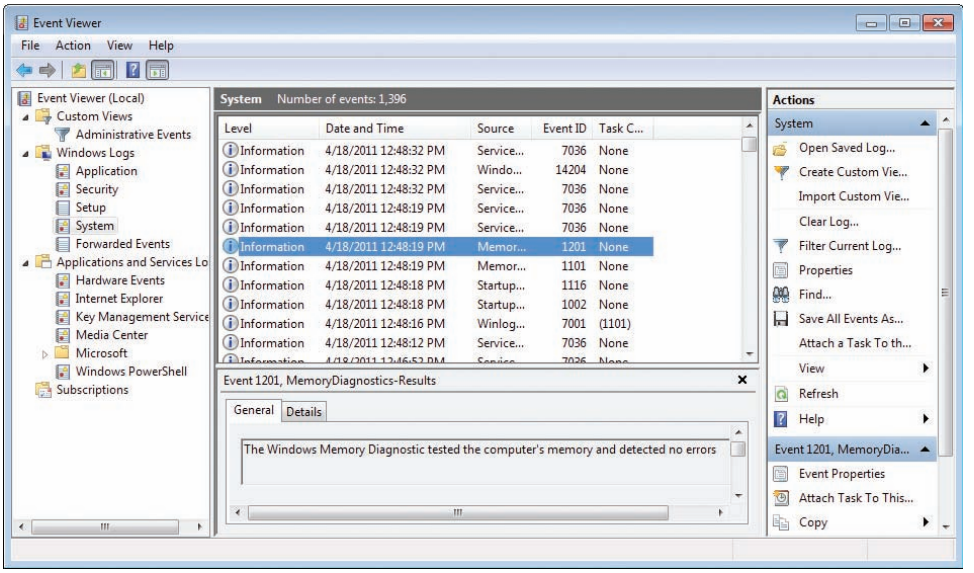
• **Figure 19.18** Windows Memory Diagnostics Tool options

You can find out more about Memtest86+ here: www.memtest.org.

It's important for you to understand that the CompTIA A+ exams do not expect you to know everything about all these command-prompt utilities. The CompTIA A+ exams expect that you do know these things, however:

- Which utilities are available and their names
- How to access these utilities (WinRE, regular command prompt)
- What these utilities basically do
- Some of the basic switches used for these utilities
- With higher-level support, that you can fix computers using these tools (being led by a specialist tech over the phone, for example)

The Startup Repair tool runs many of these command-prompt utilities automatically. You need to use the WinRE command prompt only for unique situations where the Startup Repair tool fails.



• **Figure 19.19** Event Viewer results

The **bootrec** command is a Windows Recovery Environment troubleshooting and repair tool that repairs the master boot record, boot sector, or BCD store. It replaces the old fixboot and fixmbr Recovery Console commands and adds two more repair features:

- **bootrec /fixboot** Rebuilds the boot sector for the active system partition
- **bootrec /fixmbr** Rebuilds the master boot record for the system partition
- **bootrec /scanos** Looks for Windows installations not currently in the BCD store and shows you the results without doing anything
- **bootrec /rebuildmbr** Looks for Windows installations not currently in the BCD store and gives you the choice to add them to the BCD store

With ntldr, you could access the boot.ini text file to see the Windows boot order. With boot.ini replaced by the BCD store, you can use a tool called **bcdedit** to see how Windows boots. Running bcdedit by itself (without switches) shows the boot options. The following boot information comes from a system with a single copy of Windows installed. Note there are two sections: the *Windows Boot Manager* section describes the location of bootmgr and the *Windows Boot Loader* section describes the location of the winload.exe file.

```
Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=\Device\HarddiskVolume1
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
default                 {current}
resumeobject            {d4539c9b-481a-11df-a981-
a17cb98be35c}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             Windows 7
locale                  en-US
inherit                 {bootloadersettings}
recoverysequence        {d4539c9d-481a-11df-a981-
a17cb98be35c}
recoveryenabled         Yes
osdevice                partition=C:
systemroot              \Windows
resumeobject            {d4539c9b-481a-11df-a981-
a17cb98be35c}
nx                      OptIn
```

Tech Tip

BCD Store

Boot configuration data (BCD) files contain information about operating systems installed on a computer. In Microsoft speak, that information is called a store *or* BCD store. *This applies to Windows Vista and Windows 7 only.*

Instead of editing the boot .ini text file, Windows Vista/7 includes the bcdedit program for editing the BCD store.

To make changes to the BCD store, you need to use switches:

- **bcdedit /export <filename>** exports a copy of the BCD store to a file. This is a very good idea whenever you use bcdedit!
- **bcdedit /import <filename>** imports a copy of the BCD store back into the store.

If you look carefully at the previous bcdedit output, you'll notice that each section has an identifier such as {bootmgr} or {current}. You can use these identifiers to make changes to the BCD store using the /set switch. Here's an example:

```
BCDEDIT /SET {current} path \BackupWindows\system32\winload.exe
```

This changes the path of the {current} identifier to point to an alternative winload.exe.

The bcdedit command supports multiple OSs. Notice how this BCD store has three identifiers: {bootmgr}, {current}, and {ntldr}—a fairly common dual-boot scenario.

```
Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=D:
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
default                 {current}
resumeobject            {60b80a52-8267-11e0-ad8a-
bdb414c1bf84}
displayorder            {ntldr}
                        {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Legacy OS Loader
------------------------
identifier              {ntldr}
device                  partition=D:
path                    \ntldr
description             Earlier Version of Windows

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             Windows 7
locale                  en-US
inherit                 {bootloadersettings}
recoverysequence        {60b80a54-8267-11e0-ad8a-
bdb414c1bf84}
recoveryenabled         Yes
osdevice                partition=C:
systemroot              \Windows
resumeobject            {60b80a52-8267-11e0-ad8a-
bdb414c1bf84}
nx                      OptIn
```

A BCD store like this will cause the following menu to pop up at boot (see Figure 19.20).

You can use the bcdedit command to change the display order of the menu. If you wanted to add Windows XP to the beginning of the list, type this command:

bcdedit /displayorder [WindowsXP} /addfirst

You can also use bcdedit to set the default OS:

bcdedit /default {current}

You can even remove one of the identifiers, preventing others from booting to that OS:

bcdedit /delete {WindowsXP}

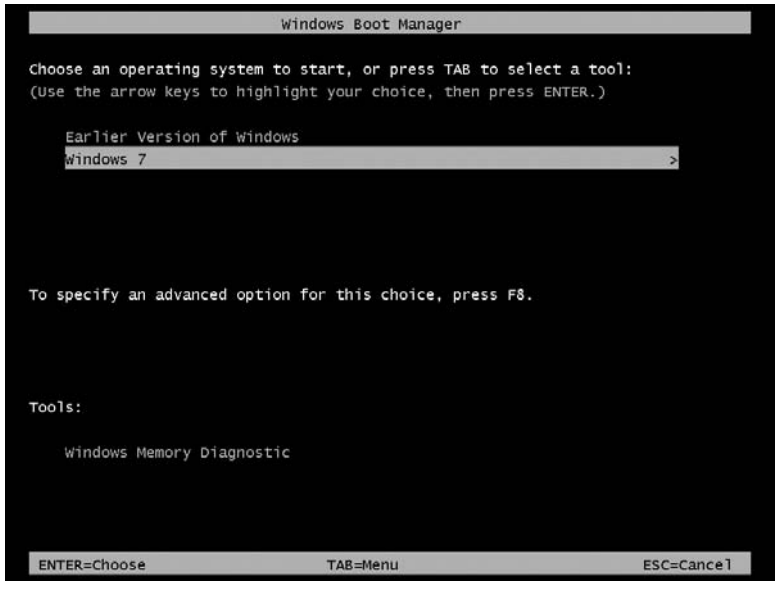
You can find EasyBCD at www.neosmart.net.

The bcdedit command is a tricky tool to use. To make your life easier, consider using the popular EasyBCD program from NeoSmart Technologies. You can run EasyBCD only from within a normal Windows boot, not the WinRE, but it provides more power and safety than bcdedit (see Figure 19.21).

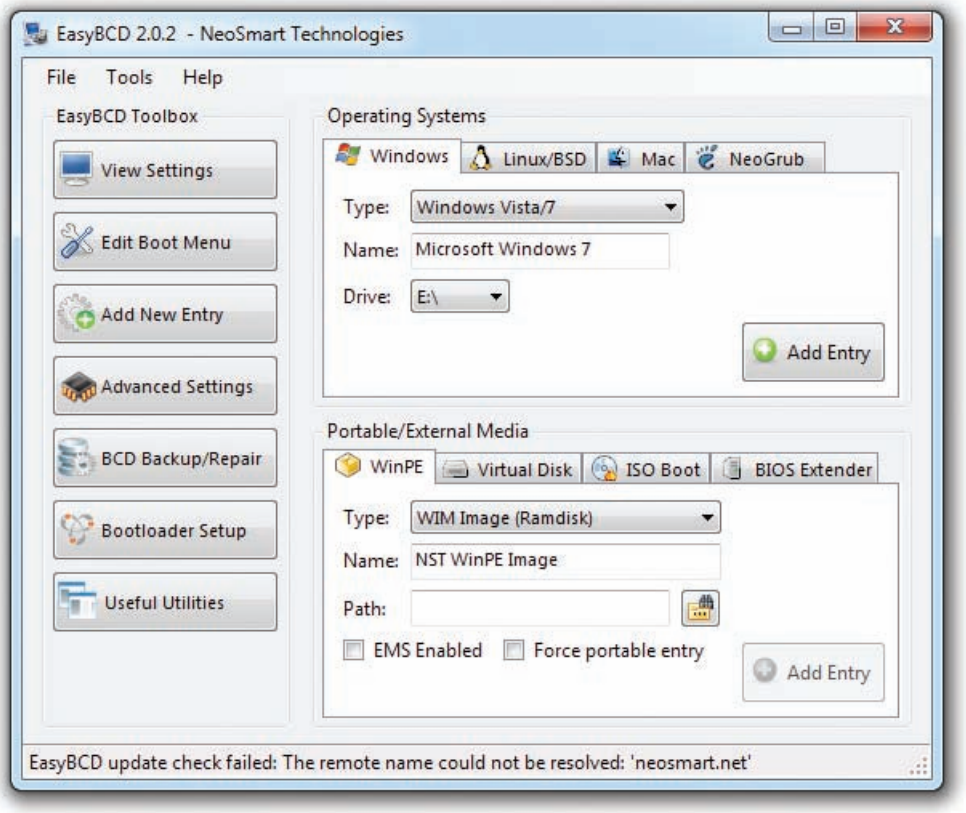
The command prompt also includes **diskpart**, a fully featured partitioning tool. This tool lacks many of the safety features built into Disk Management, so proceed with caution. You can, for example, delete any partition of any type at any time. Starting diskpart opens a special command prompt as shown here:

```
C:\Windows\system32>diskpart
Microsoft DiskPart version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: MIKESPC
DISKPART>
```

You can list volumes (or partitions on Basic disks):



• **Figure 19.20** bootmgr showing available versions of Windows



• **Figure 19.21** EasyBCD at work

```
DISKPART> list volume
  Volume ###  Ltr  Label       Fs     Type        Size     Status    Info
  ----------  ---  ----------  -----  ----------  -------  --------  -----
  Volume 0     D                       DVD-ROM         0 B  No Media
  Volume 1     C   New Volume  NTFS   Partition  1397 GB  Healthy   System

DISKPART>
```

Select a volume to manipulate (you may also select an entire drive):

```
DISKPART> select volume 1
Volume 1 is the selected volume.
DISKPART>
```

You can run commands at the diskpart prompt to add, change, or delete volumes and partitions on drives, mount or dismount volumes, and even manipulate software-level RAID arrays.

Run the **clean** command at the diskpart prompt to wipe all partition and volume information off the currently selected disk. This tool handles nasty corruptions that simply won't let Windows boot and serves as my last-ditch step before I toss a drive.

Commands available at the diskpart prompt handle volumes and partitions, but you still need a tool for handling file systems. Both WinRE and the regular command prompt provide all of the typical utilities such as

copy, move, del, and format. One tool, however—fsutil—does a few more interesting jobs:

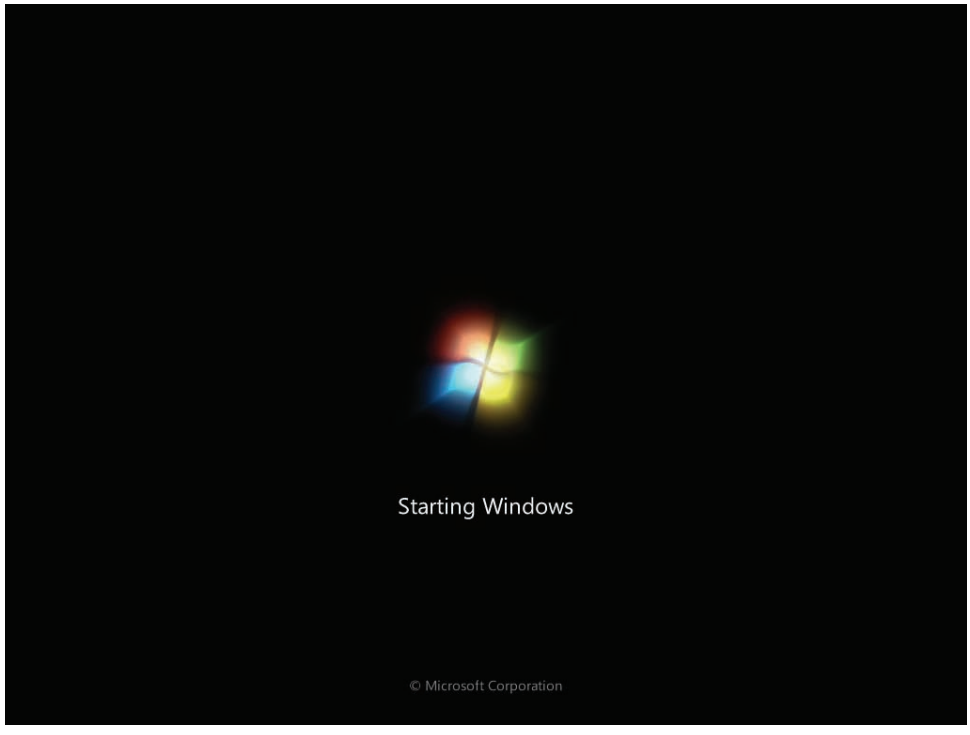
- Typing **fsinfo** provides a detailed query about the drives and volumes.
- Typing **fsutil dirty <drivename>** tells you if Windows considers the drive to be "dirty"—meaning you need to run autochk at the next reboot. When Windows detects an error in the file system for a drive, it flags that drive as a *dirty drive* or *dirty volume*. The disk checking utility autochk runs after a reboot and before Windows loads and will correct errors in the file system of a drive.
- Typing **fsutil repair initiate <drive letter>** runs a basic version of chkdsk without rebooting.

Failure to Load the GUI

If faced with a scenario where the GUI files have become corrupted, what CompTIA calls a "Missing Graphical Interface" problem, your only choices are to restore from backup or rebuild from the installation media.

Assuming that Windows gets past the boot part of the startup, it then begins to load the graphical Windows OS. You will see the Windows startup image on the screen, hiding everything until Windows loads the desktop (see Figure 19.22).

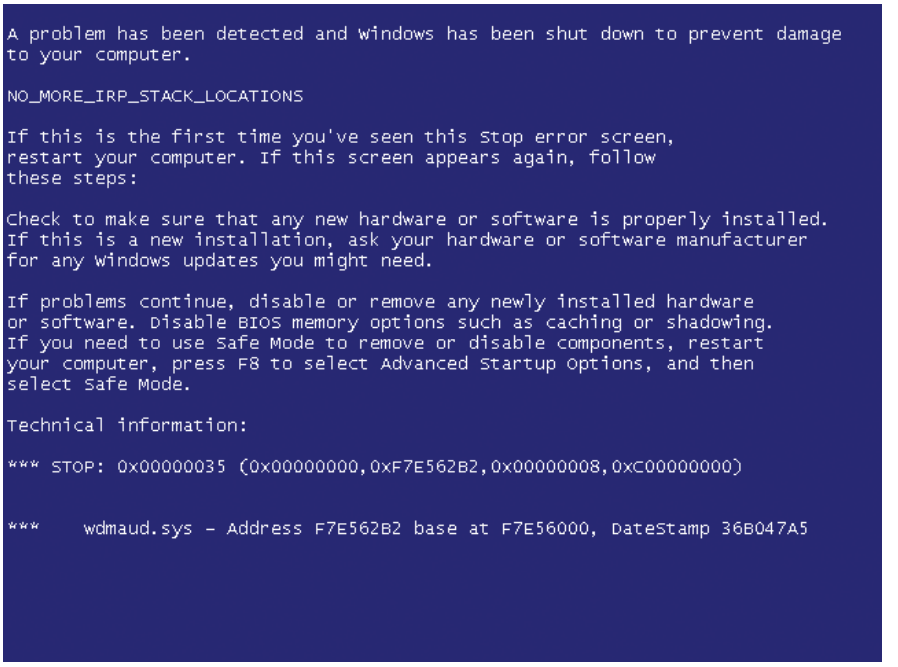
Several issues can create a scenario where the graphical interface fails to load. Windows can hang during the GUI-loading phase because of buggy device drivers or Registry problems. Even autoloading programs can cause the GUI to hang on load. The first step in troubleshooting these sorts of scenarios is to use one of the Advanced Startup options (covered later in the chapter) to try to get past the hang spot and into Windows.



• **Figure 19.22** GUI time!

Device Drivers

Device driver problems that stop Windows GUI from loading look pretty scary. Figure 19.23 shows the infamous Windows *Stop error*, better known as the **Blue Screen of Death (BSoD)**. The BSoD only appears when something causes an error from which Windows cannot recover. The BSoD is not limited to device driver problems, but device drivers are one of the reasons you'll see the BSoD.



• **Figure 19.23** BSoD

Whenever faced with a scenario where you get a BSoD, read what it says. Windows BSoDs tell you the name of the file that caused the problem and usually suggests a recommended action. Once in a while these are helpful.

BSoD problems due to device drivers almost always take place immediately after you've installed a new device and rebooted. Take out the device and reboot. If Windows loads properly, head over to the manufacturer's Web site. A new device producing this type of problem is a serious issue that should have been caught before the device was released. In many cases, the manufacturer will have updated drivers available for download or will recommend a replacement device.

The second indication of a device problem that shows up during the GUI part of startup is a freeze-up: the Windows startup screen just stays there and you never get a chance to log on. If this happens, try one of the Advanced Startup Options, covered following the Registry.

Viruses can cause the GUI to fail or make it appear to be missing. One nasty one running around recently, for example, caused what appeared to be a BSoD warning of imminent hard drive controller failure. Even after getting rid of the virus, Windows appeared devoid of any graphical elements at all: no Start button, icons, or files even in Computer. That's because the virus had changed the attributes of every file and folder on the hard drive to hidden! See Chapter 18 for the attrib command; see Chapter 29 for recovery techniques for virus-attacked computers.

Registry

The Registry files load every time the computer boots. Windows does a pretty good job of protecting your Registry files from corruption, but from time to time something may slip by Windows and it will attempt to load a bad Registry. These errors may show up as BSoDs that say "Registry File Failure" or text errors that say "Windows could not start." Whatever the case, when you run into these sorts of scenarios, you need to restore a good Registry copy. The best way to do this is the Last Known Good Configuration boot option (see the upcoming section). If that fails, you can restore an earlier version of the Registry through the Recovery Console in Windows XP or through Windows RE in Windows Vista/7.

Replacing the Registry in Windows XP

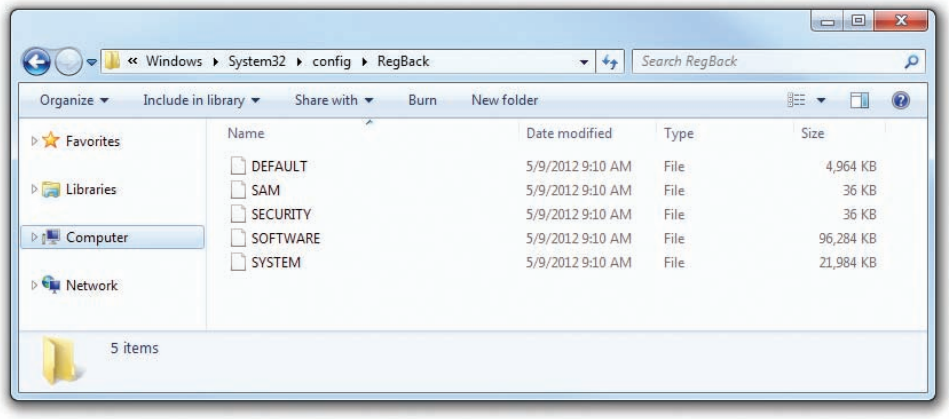
Boot to the Windows installation CD-ROM, get to the Recovery Console, and type these commands to restore a Registry. Notice I didn't say "your"

Registry in the previous sentence. Your Registry is corrupted and gone, so you need to rebuild.

```
delete c:\windows\system32\config\system
delete c:\windows\system32\config\software
delete c:\windows\system32\config\sam
delete c:\windows\system32\config\security
delete c:\windows\system32\config\default

copy c:\windows\repair\system c:\windows\system32\config\system
copy c:\windows\repair\software c:\windows\system32\config\software
copy c:\windows\repair\sam c:\windows\system32\config\sam
copy c:\windows\repair\security c:\windows\system32\config\security
copy c:\windows\repair\default c:\windows\system32\config\default
```

Replacing the Registry in Windows Vista/7

Windows Vista and Windows 7 keep a regular backup of the Registry handy in case you need to overwrite a corrupted Registry. By default, the RegIdleBackup task runs every 10 days, so that's as far back as you would lose if you replaced the current Registry with the automatically backed-up files. Of course, it would be better if you kept regular backups too, but at least the damage would be limited. You can find the backed-up Registry files in \Windows\System32\config\RegBack (see Figure 19.24).



• **Figure 19.24** The backed-up Registry files located in the RegBack folder

To replace the Registry, boot to the Windows DVD to access Windows RE and get to the Command Prompt shell. Run the **reg** command to get to a reg prompt. From there, you have numerous commands to deal with the Registry. The simplest is probably the *copy* command. You know the location of the backed-up Registry files. Just copy the files to the location of the main Registry files—up one level in the tree under the \config folder.

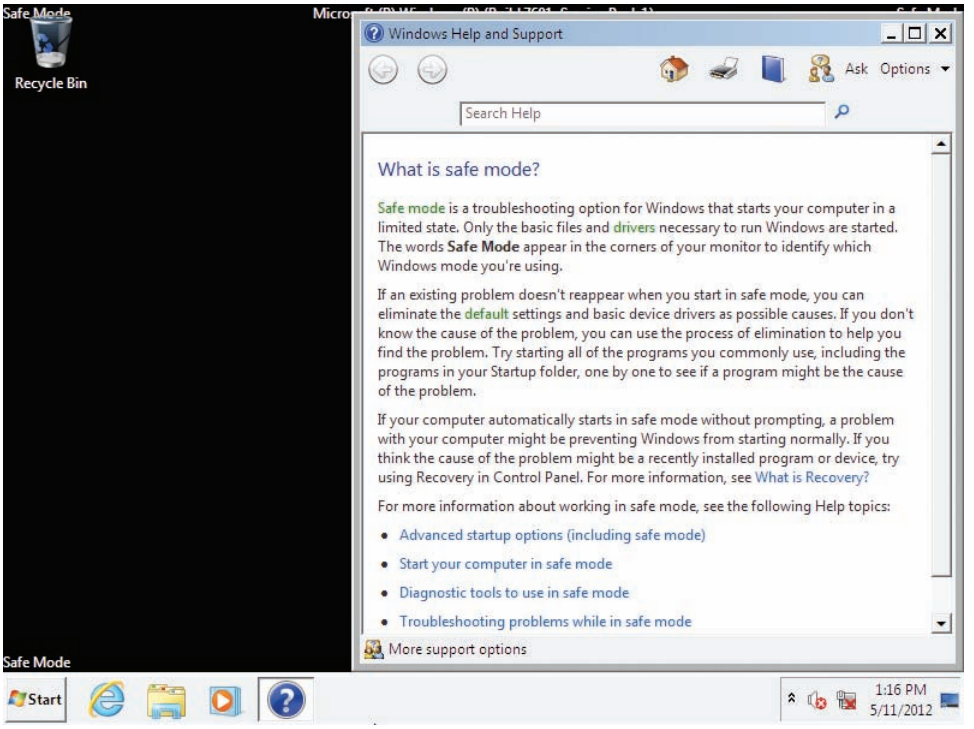
Advanced Startup Options

Windows 9*x* had an option for step-by-step confirmation, but that is not a choice in Windows XP/Vista/7. Look for it as a wrong answer on the exams!

If Windows fails to start up, use the Windows **Advanced Startup Options** menu to discover the cause. To get to this menu, restart the computer and press F8 after the POST messages but before the Windows logo screen appears. Windows XP's Startup options are a tad different from Windows Vista's and Windows 7's. Central to these advanced options are Safe Mode and Last Known Good Configuration. Here's a rundown of the menu options.

Safe Mode (All Versions)

Safe Mode starts up Windows but loads only very basic, non–vendor-specific drivers for mouse, 640 × 480 resolution monitor (in XP) and 800 ×



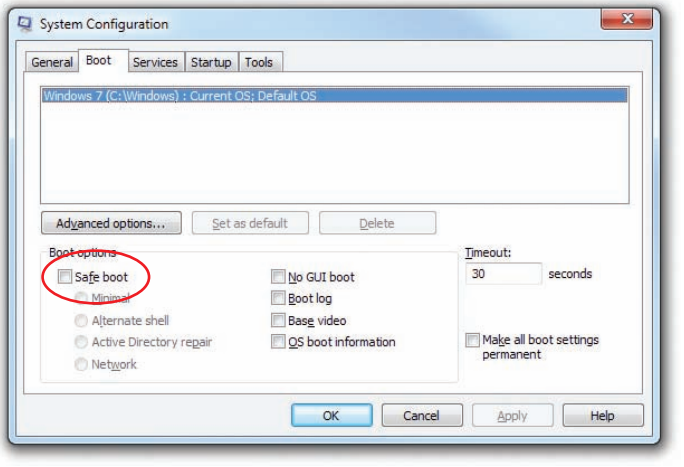
• **Figure 19.25** Safe Mode

600 resolution monitor (Vista and 7), keyboard, mass storage, and system services (see Figure 19.25).

Once in Safe Mode, you can use tools such as Device Manager to locate and correct the source of the problem. When you use Device Manager in Safe Mode, you can access the properties for all the devices, even those that are not working in Safe Mode. The status displayed for the device is the status for a normal startup. Even the network card will show as enabled. You can disable any suspect device or perform other tasks, such as removing or updating drivers. If a problem with a device driver is preventing the operating system from starting normally, check Device Manager for warning icons that indicate an unknown device.

There is no safety or repair feature in any version of Windows that makes the OS boot to Safe Mode automatically. In most cases, Windows automatically booting to Safe Mode indicates that someone has set the System Configuration utility to force Windows to do so. Type **msconfig** at the Start | Search or Start | Run option and press ENTER to open the System Configuration utility, and then deselect the Safe boot or Boot to Safe Mode check box (see Figure 19.26).

The CompTIA A+ 802 exam objectives mention a scenario where Windows boots directly to Safe Mode. This can only happen if a tech specifically makes a change to the System Configuration utility.



• **Figure 19.26** Uncheck Safe boot

Safe Mode with Networking (All Versions)

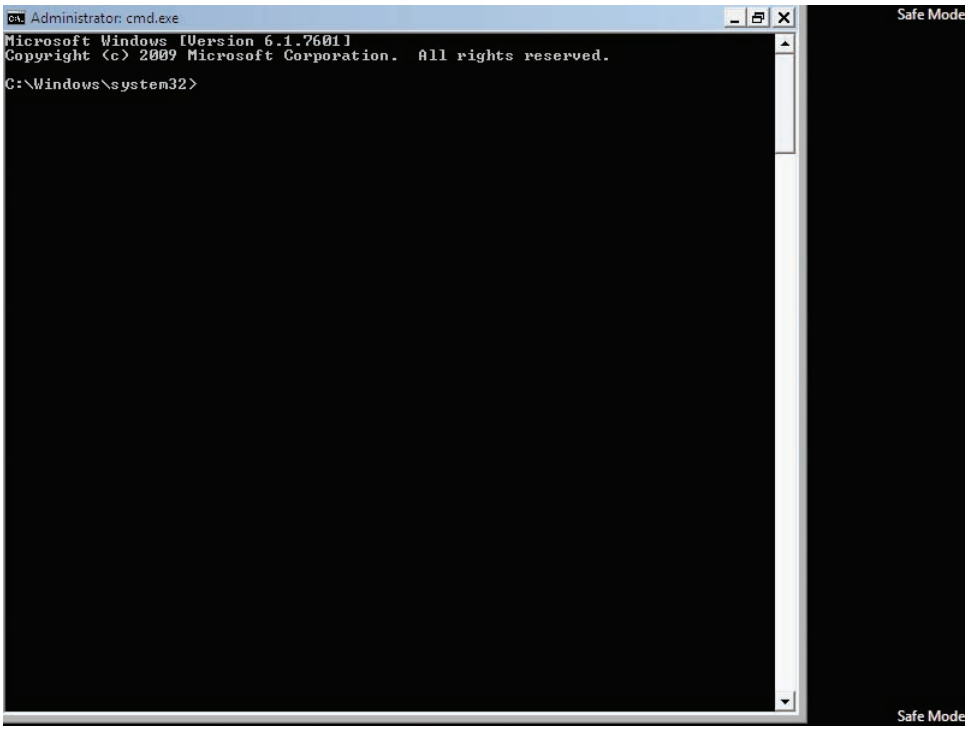
This mode is identical to plain Safe Mode except that you get network support. I use this mode to test for

a problem with network drivers. If Windows won't start up normally but does start up in Safe Mode, I reboot into Safe Mode with Networking. If it fails to start up with Networking, the problem is a network driver. I reboot back to Safe Mode, open Device Manager, and start disabling network components, beginning with the network adapter.

Safe Mode with Command Prompt (All Versions)

When you start Windows in this mode, rather than loading the GUI desktop, it loads the command prompt (cmd.exe) as the shell to the operating system after you log on, as shown in Figure 19.27. From here you can run any of the commands you learned about in Chapter 18, plus a lot of utilities as well. Error-checking runs fine as chkdsk, for example. Disk Defragmenter probably runs even faster when you type **defrag** followed by a drive letter at the command prompt than it does from the graphical version of the tool.

Safe Mode with Command Prompt is a handy option to remember if the desktop does not display at all, which, after you have eliminated video drivers, can be caused by corruption of the explorer.exe program. From the command prompt, you can delete the corrupted version of explorer.exe and copy in an undamaged version. This requires knowing the command-line commands for navigating the directory structure, as well as knowing the location of the file you are replacing. Although Explorer is not loaded, you can load other GUI tools that don't depend on Explorer. All you have to do is enter the correct command. For instance, to load Event Viewer, type **eventvwr.msc** at the command line and press ENTER.



• **Figure 19.27** Safe Mode with Command Prompt

Enable Boot Logging (All Versions)

This option starts Windows normally and creates a log file of the drivers as they load into memory. The file is named Ntbtlog.txt and is saved in the %SystemRoot% folder. If the startup failed because of a bad driver, the last entry in this file may be the driver the OS was initializing when it failed.

Reboot and go into the Recovery Console or WinRE. Use the tools there to read the boot log (**type ntbtlog.txt**) and disable or enable problematic devices or services.

Enable VGA Mode (XP)/Enable Low-Resolution Mode (Vista and 7)

Enable VGA Mode/Enable Low-Resolution Mode starts Windows normally, but only loads a default VGA driver. If this mode works, it may mean you have a bad driver, or it may mean you are using the correct video driver but it is configured incorrectly (perhaps with the wrong refresh rate and/or resolution). Whereas Safe Mode loads a generic VGA driver, this mode loads the driver Windows is configured to use but starts it up in standard VGA mode rather than using the settings for which it is configured. After successfully starting in this mode, open the Display applet and change the settings.

Last Known Good Configuration (All Versions)

When Windows' startup fails immediately after installing a new driver but before you have logged on again, try the **Last Known Good Configuration** option. This option applies specifically to new device drivers that cause failures on reboot.

Directory Services Restore Mode (All Versions)

The title says it all here; this option only applies to Active Directory domain controllers, and only Windows Server versions can be domain controllers. I have no idea why Microsoft includes this option. If you choose it, you simply boot into Safe Mode.

Debugging Mode (All Versions)

If you select this choice, Windows starts in kernel debug mode. It's a super-techie thing to do, and I doubt that even über techs do debug mode anymore. To do this, you have to connect the computer you are debugging to another computer via a serial connection, and as Windows starts up, a debug of the kernel is sent to the second computer, which must also be running a debugger program.

Disable Automatic Restart on System Failure (All Versions)

Sometimes a BSoD will appear at startup, causing your computer to spontaneously reboot. That's all well and good, but if it happens too quickly, you might not be able to read the BSoD to see what caused the problem. Selecting *Disable automatic restart on system failure* from the Advanced Startup Options menu stops the computer from rebooting on Stop errors. This gives you the opportunity to write down the error and hopefully find a fix.

Disable Driver Signature Enforcement (Vista and 7)

Windows Vista and 7 require that all very low-level drivers (kernel drivers) must have a Microsoft driver signature. If you are using an older driver to connect to your hard drive controller or some other low-level feature, you must use this option to get Windows to load the driver. Hopefully you will always check your motherboard and hard drives for Windows compatibility and never have to use this option.

Start Windows Normally (All Versions)

This choice will simply start Windows normally, without rebooting. You already rebooted to get to this menu. Select this if you changed your mind about using any of the other exotic choices.

Reboot (All Versions)

This choice will actually do a soft reboot of the computer.

Return to OS Choices Menu (All Versions)

On computers with multiple operating systems, you get an OS Choices menu to select which OS to load. If you load Windows and press F8 to get the Advanced Startup Options menu, you'll see this option. Choosing it returns you to the OS Choices menu, from which you can select the operating system to load.

Troubleshooting Tools in the GUI

Once you're able to load into Windows, whether through Safe Mode or one of the other options, the whole gamut of Windows tools is available for you. In the previous scenario where a bad device driver caused the startup problems, for example, you can open Device Manager and begin troubleshooting just as you've learned in previous chapters. If you suspect some service or Registry issue caused the problem, head on over to Event Viewer and see what sort of logon events have happened recently. Let's go there first.

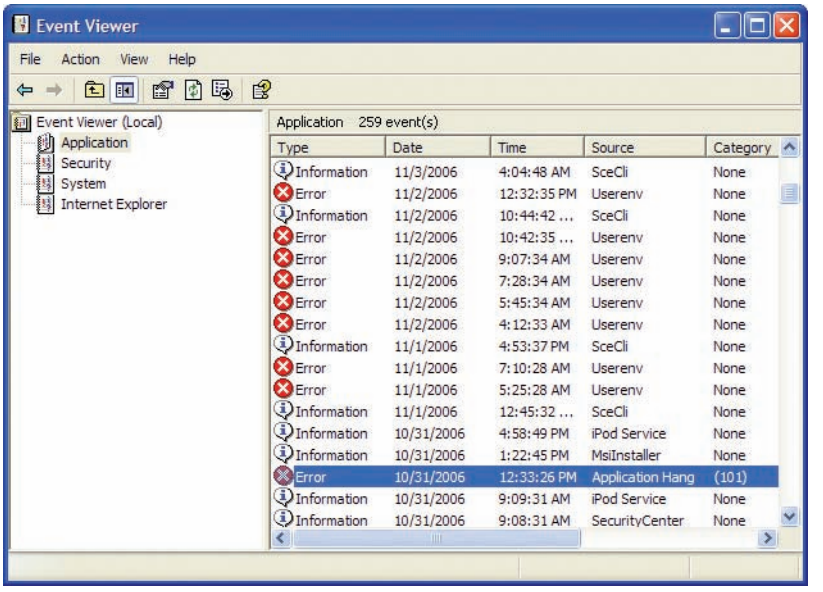
Event Viewer

When you get into the GUI, one of the first tools you should use is Event Viewer to see what's causing the problems on your computer. **Event Viewer** is Windows' default tattletale program, spilling the beans about a number of interesting happenings on the system. With a little tweaking, Event Viewer turns into a virtual recording of anything you might ever want to know about on your system.

Keep in mind that Event Viewer is a powerful tool for more than just troubleshooting Windows—it's a powerful tool for security as well, as you'll see in Chapter 29. But for now let's examine Event Viewer, both in Windows XP and in Windows 7 (the Vista version of Event Viewer is almost identical to the version in Windows 7), to see what we can do with this amazing utility.

Windows XP Event Viewer You can find Event Viewer in the Administrative Tools applet in the Control Panel. By default, Event Viewer has

three sections: Application, Security, and System. If you've downloaded Internet Explorer 7 or later, you'll see a fourth option for the browser, Internet Explorer (see Figure 19.28). Each of these sections stores certain types of events, as described next.

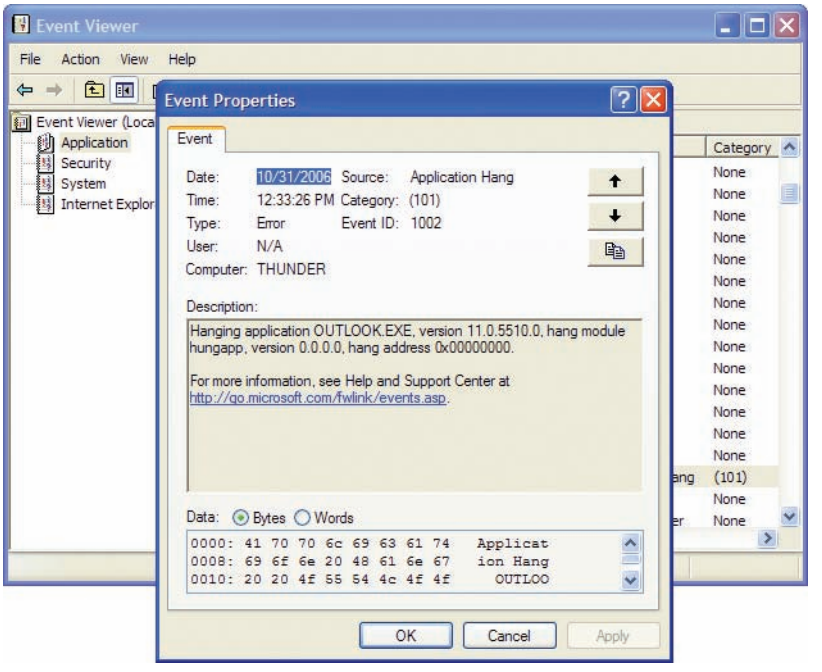


• **Figure 19.28** Event Viewer

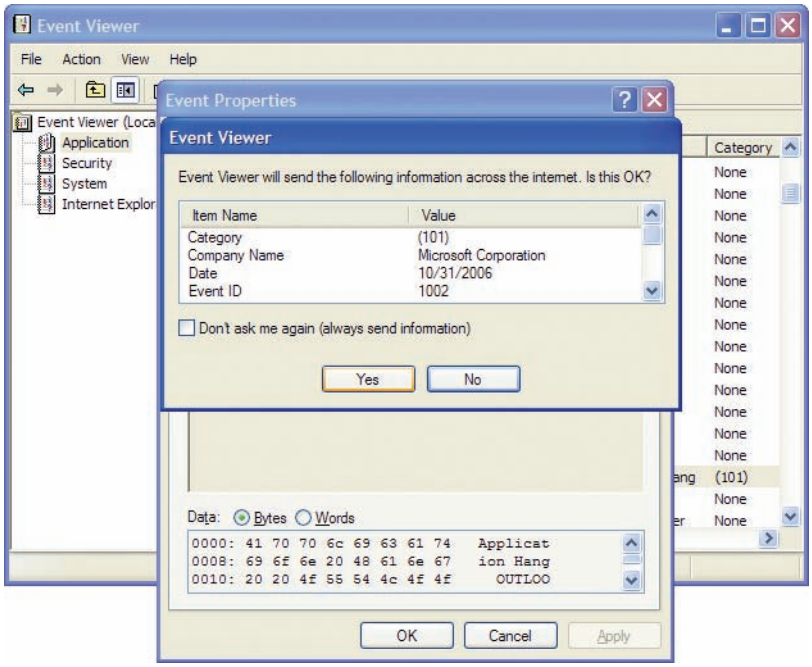
- **Application** As the name implies, the Application section stores events specific to applications. There are three types of events recorded: Errors, Warnings, and Information. Errors, marked with a red *X*, are the most serious, reflecting events that prevent the application from working properly. Warnings, marked with an exclamation point over a triangle, are for events that aren't preventing the application from running but may do so in the future. Information events are merely record keeping, letting you know that a program, driver, or service ran successfully.
- **Security** Security records events that Microsoft calls *audits*. Audits record anything to do with security, such as the number of logon events. All audits are listed as either successful or failed. There a thousands of audits available on a Windows system, the vast majority of which are turned off by default but can be turned on in Administrative Tools | Local Security Policy. Since these are security issues, we'll cover the Security section as well as auditing in Chapter 29.
- **System** The System section is similar to the Application section in that you have Errors, Warnings, and Information, but the events listed here are specific only to the operating system.

When something goes wrong with Windows, it's common for techs to turn to Event Viewer first. Let's say an application fails to load. A common use for Event Viewer is to view the application to see what happened (see Figure 19.29).

One very cool feature of Event Viewer is that you can click the link to take you



• **Figure 19.29** Typical application error message

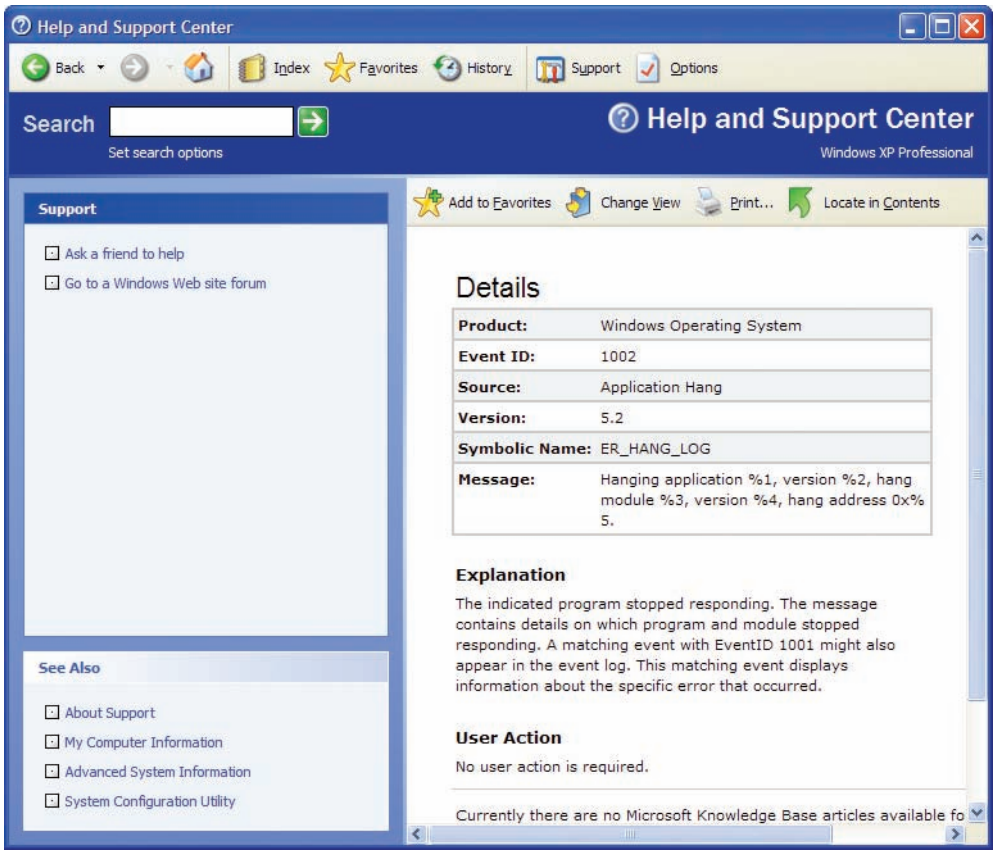


• **Figure 19.30** Details about to be sent

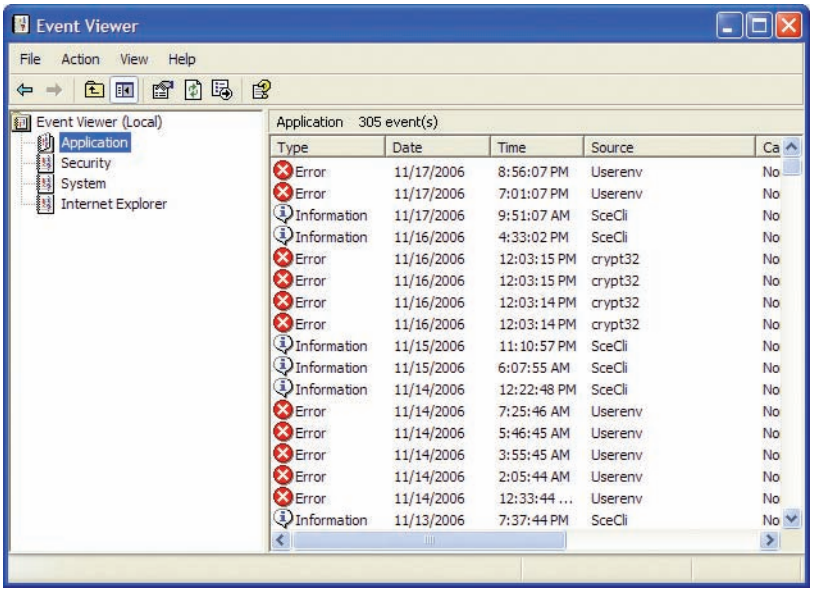
to the online Help and Support Center at Microsoft.com, and the software reports your error (see Figure 19.30), checks the online database, and comes back with a more or less useful explanation (see Figure 19.31).

Event Viewer might reveal problems with applications failing to load, a big cause of Windows loading problems (see Figure 19.32). It might also reveal problems with services failing to start. Finally, Windows might run into problems loading DLLs. You can troubleshoot these issues individually or you can use System Restore to load a restore point that predates the bugginess.

Windows Vista/7 Event Viewer Windows Vista/7 adds an easy-to-use interface to Event Viewer (while retaining the old Windows XP style if you prefer it). Opening Event Viewer (System and Security | Administrative Tools | Event Viewer)



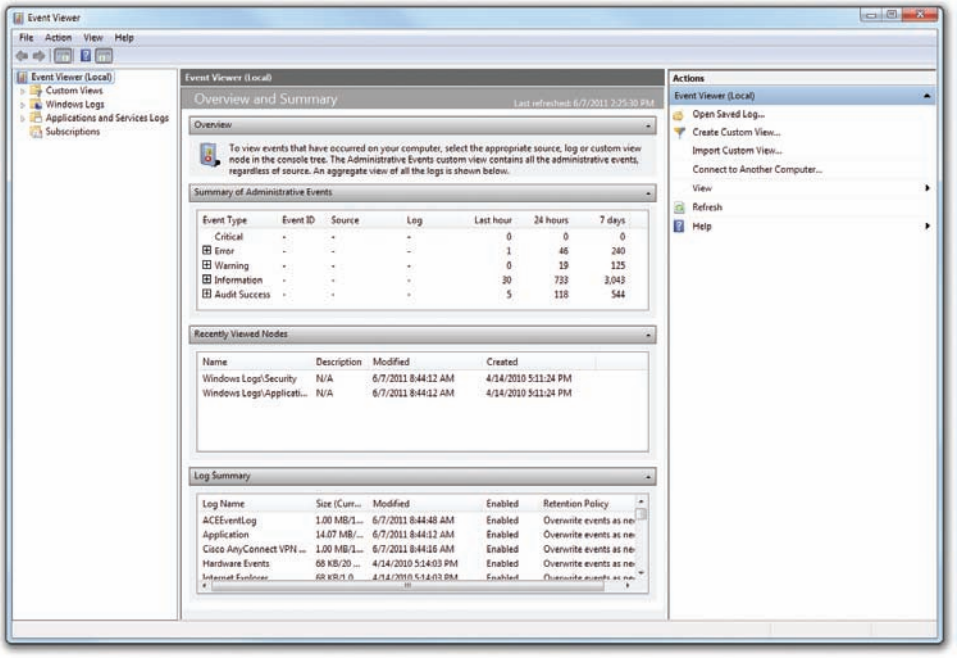
• **Figure 19.31** Help and Support Center being helpful



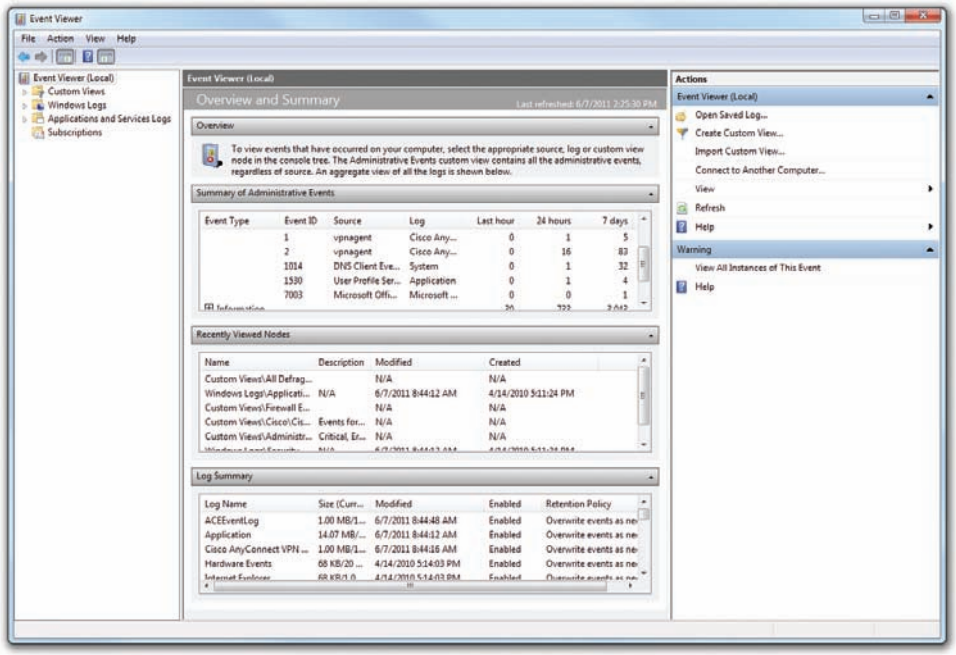
• **Figure 19.32** Event Viewer in Windows XP showing some serious application errors!

shows you a very different interface from the one you've seen in Windows XP (see Figure 19.33).

Note the four main bars in the center pane: Overview, Summary of Administrative Events, Recently Viewed Nodes, and Log Summary. Pay special attention to the Summary of Administrative Events. It breaks down the events into different levels: Critical, Error, Warning, Information, Audit Success, and Audit Failure. Figure 19.34 shows a typical Summary with the Warning Events opened. You can then click any event to see a dialog box describing the event in detail. Microsoft refers to these as *Views*.



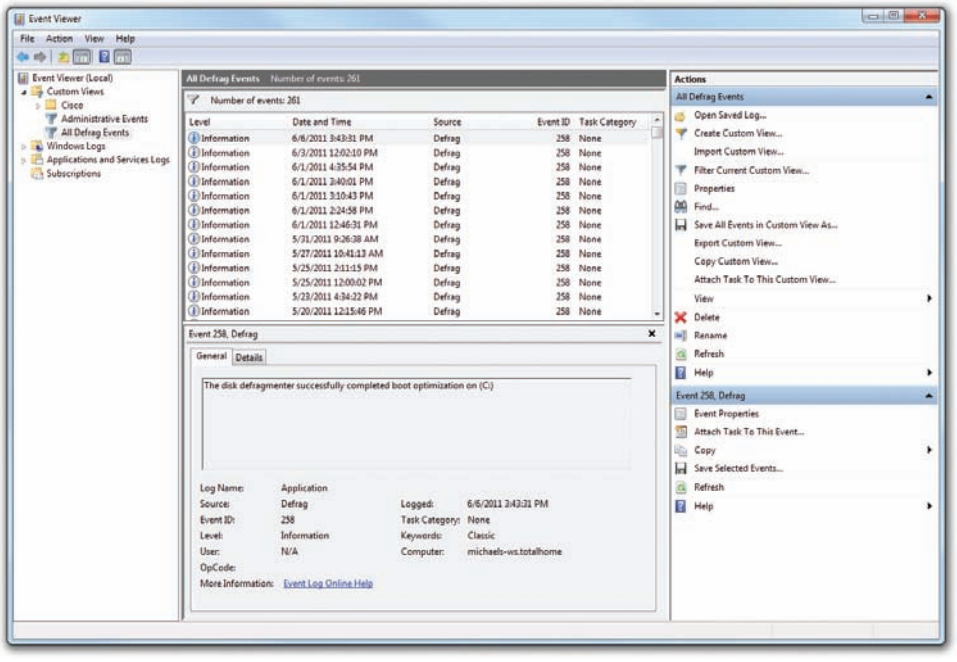
• **Figure 19.33** Windows 7 Event Viewer default screen



• **Figure 19.34** Warning Events open

By default, Event Viewer stores logs as .evtx files in the C:\windows\system32\winevt\ logs folder.

Windows 7's Event Viewer still includes the classic logs you saw in Windows XP (Application, Security, and System) but leans heavily on Views to show you the contents of the logs. Views filter existing log files, making them great for custom reports using beginning/end times, levels of errors, and more. You can use the built-in Views or easily create custom Views, as shown in Figure 19.35.



• **Figure 19.35** Created custom Views

Remember, you still record all data to logs. Logs in Windows 7 still have the same limitations that logs in earlier versions of Windows had. They have a maximum size, a location, and a behavior for when they get too big (such as overwrite the log or make an error). Figure 19.36 shows a typical Log Properties dialog box in Windows 7.

Windows 7's Event Viewer remains largely untouched in terms of the data collected, but Microsoft did a great job of making that data much easier to understand and use.

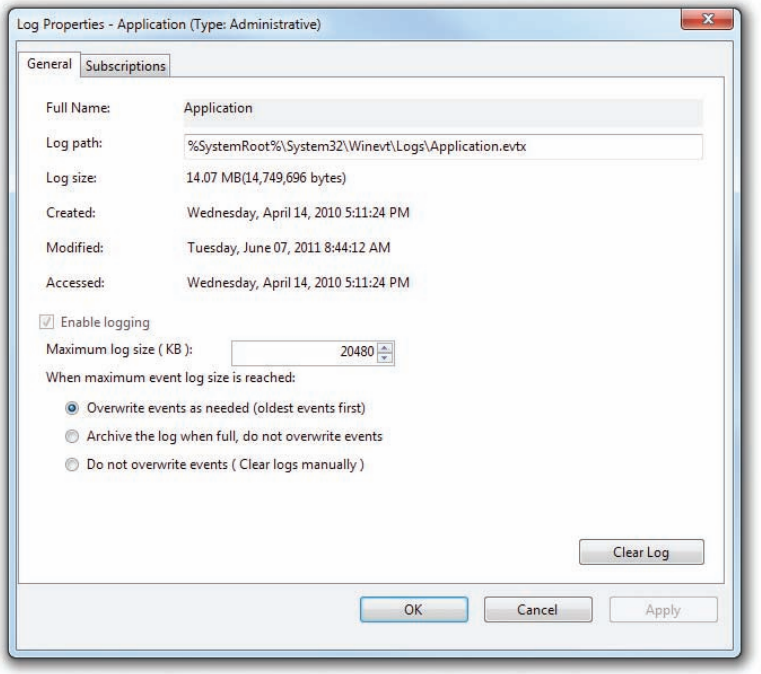


Figure 19.36 Log Properties dialog box in Windows 7

Only users with Administrator privileges can make changes to log files in Event Viewer.

If you run into a scenario where a device has failed and this created problems with Windows' startup, you would turn to the primary Windows tool for hardware issues: Device Manager. We've covered Device Manager in chapters specific to hardware, so there's no need to go into it yet again here.

Autoloading Programs

Windows loves to autoload programs so they start at boot. Most of the time this is an incredibly handy option, used by every Windows PC in existence. The problem with autoloading programs is that when one of them starts behaving badly, you need to shut off that program! Use the System Configuration utility to temporarily stop programs from autoloading. If you want to make the program stop forever, go into the program and find a load on startup option (see Figure 19.37).

If you can't find a load on startup option in your application, run the Registry Editor and go to where most applications autoload: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Services

Windows loads a number of services as it starts. In a scenario where any critical service fails to load, Windows tells you at this point with an error message. The important word here is *critical*. Windows will not report *all* service failures at this point. If a service that is less than critical to Windows doesn't start, the OS usually waits until you try to use a program that needs that

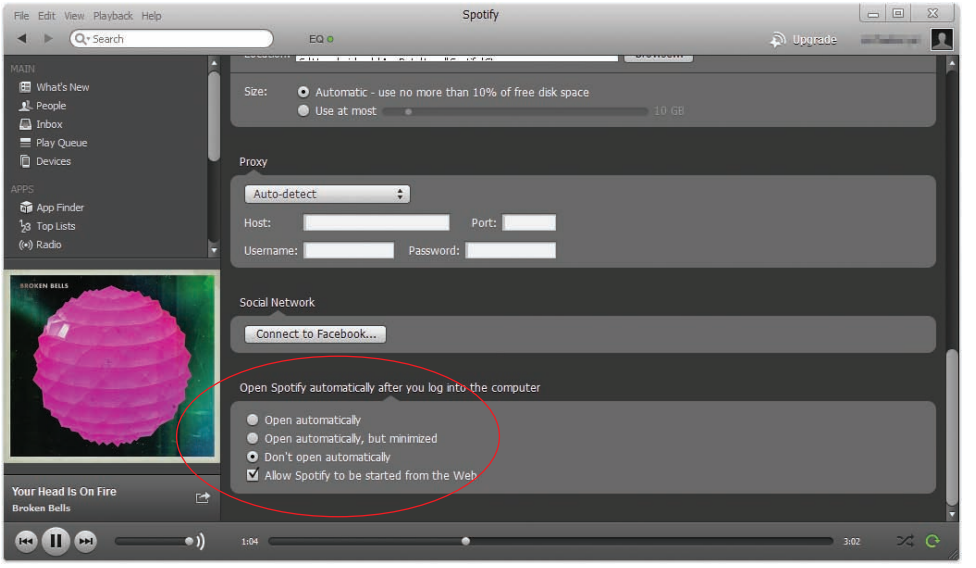
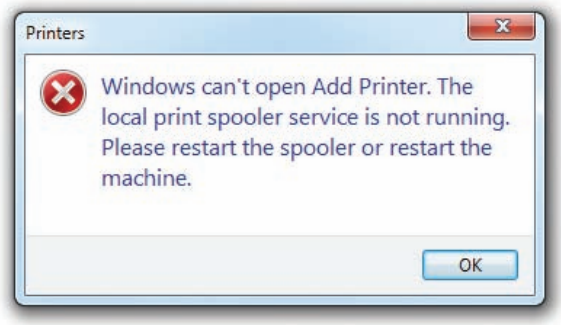
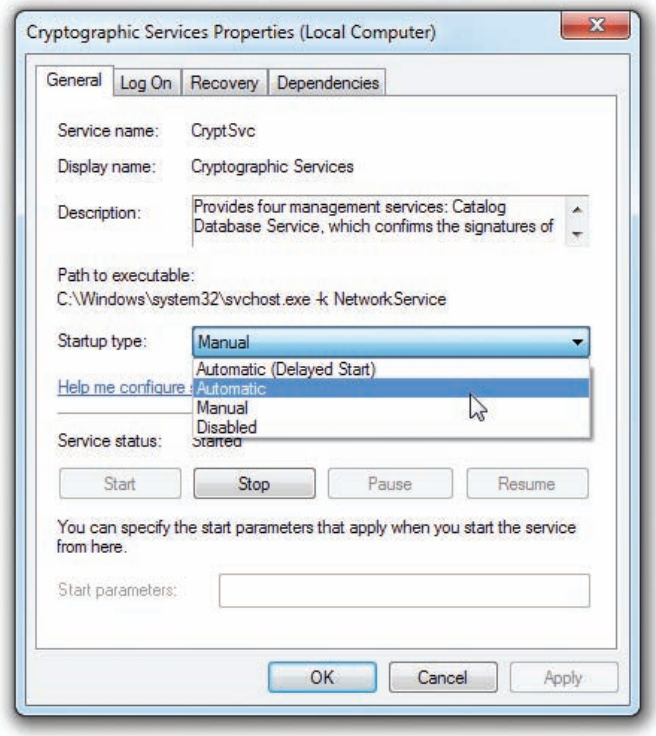


Figure 19.37 Typical load on startup option



• **Figure 19.38** Service error



• **Figure 19.39** Autostarting a service

Newly installed DLLs must be entered into the Registry via a process cleverly called *registration*. In most cases DLLs will register themselves, but on rare occasions you might need to manually register a DLL using the command-line tool regsvr32 that you learned about in Chapter 15.

service before it prompts you with an error message (see Figure 19.38).

To work with your system's services, go to the Control Panel | Administrative Tools | Services and verify that the service you need is running. If not, turn it on. Also notice that each service has a Startup Type—Automatic, Manual, or Disabled—that defines when it starts. It's very common to find that a service has been set to Manual when it needs to be set to Automatic so that it starts when Windows boots (see Figure 19.39).

Task Manager and Command-Line Options

Task Manager is a great place to go to shut down errant processes that won't otherwise close properly. Task Manager enables you to see all applications or programs currently running or to close an application that has stopped working. You remember how to get to it, right? Press CTRL-SHIFT-ESC to open it directly or CTRL-ALT-DELETE to get to a list of action items, one of which opens Task Manager.

If you're unable to get to Task Manager or are comfortable with the command line, you can get to a command prompt (like in the Recovery Console or Windows Recovery Environment) and type the command **tasklist** to find the names and process IDs of all the running processes. You can then run **taskkill** to end any process either by filename or by process ID. If you're in the Windows PowerShell, the commands are *tasklist* and *kill*.

System Files

Windows lives on dynamic link library (DLL) files. Almost every program used by Windows—and certainly all of the important ones—call on DLL files to do most of the heavy lifting that makes Windows work.

Windows protects all of the critical DLL files very carefully, but once in a while you may get an error saying Windows can't load a particular DLL. Although rare, the core system files that make up Windows itself may become corrupted, preventing Windows from starting properly. You usually see something like "Error loading XXXX.DLL," or sometimes a program you need simply won't start when you double-click its icon. In these cases, the tool you need is the **System File Checker** that you learned about in Chapter 18. Use it to check and replace a number of critical files, including the ever-important DLL cache.

System Restore

System Restore is the final step in recovering from a major Windows meltdown. Earlier in the chapter, you learned that you can use System Restore from the Windows Recovery Environment, but don't forget that you can

also use restore points from within Windows. Follow the process explained in Chapter 17.

Troubleshooting Tools in Windows Vista and Windows 7

Windows Vista and Windows 7 include amazing utilities designed to help you support your system. Many of these tools first appeared in Windows Vista, but Windows 7 either refined them or made them easily accessible. These Control Panel tools perform a number of different jobs, from telling you what's happening on the system to showing you how well a system's performance stacks up to other computers.

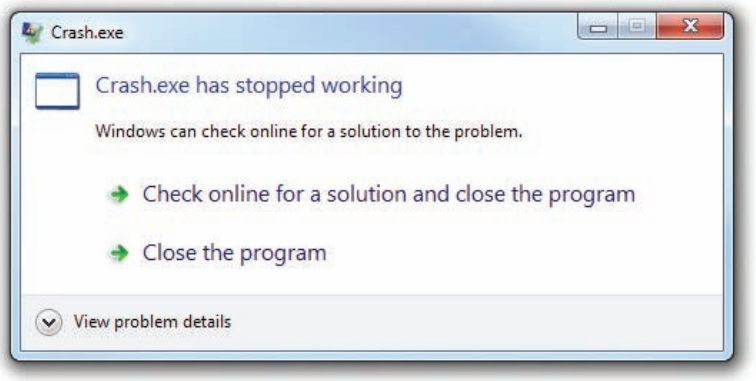
Problem Reports and Solutions (Windows Vista) and Action Center (Windows 7) centralize a lot of useful information about the status of your computer. The Performance and Information Tools applet tells you just how powerful your computer really is. Let's take a look at this crazy mixture of utilities in alphabetical order and explore the scenarios appropriate for their use.

Problem Reports and Solutions

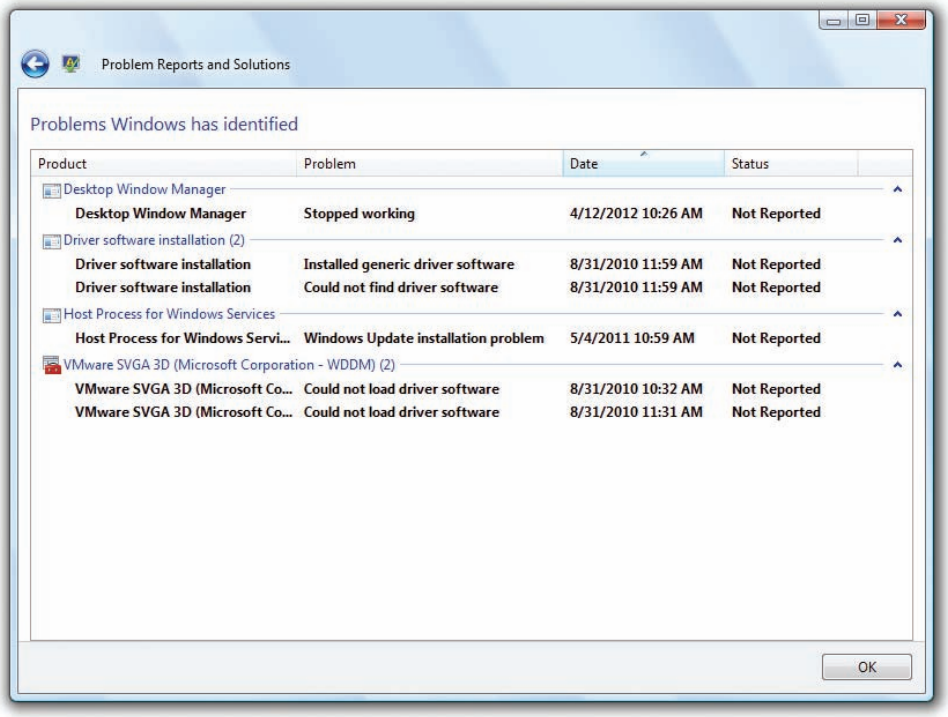
If a computer is having a problem, wouldn't it be great to tell the people who are in charge of the program you're having that problem so they can fix it? That's the idea behind *Windows Error Reporting*. There's a good chance that, like many users, you've run into errors that look something like Figure 19.40.

The problem with these errors is that, while they might help Microsoft, they traditionally do little to help us fix the computer. Windows Error Reporting was a one-way tool, until Microsoft upgraded it with Vista to a much more powerful, two-way tool that gives developers a way to give you ways to fix computers.

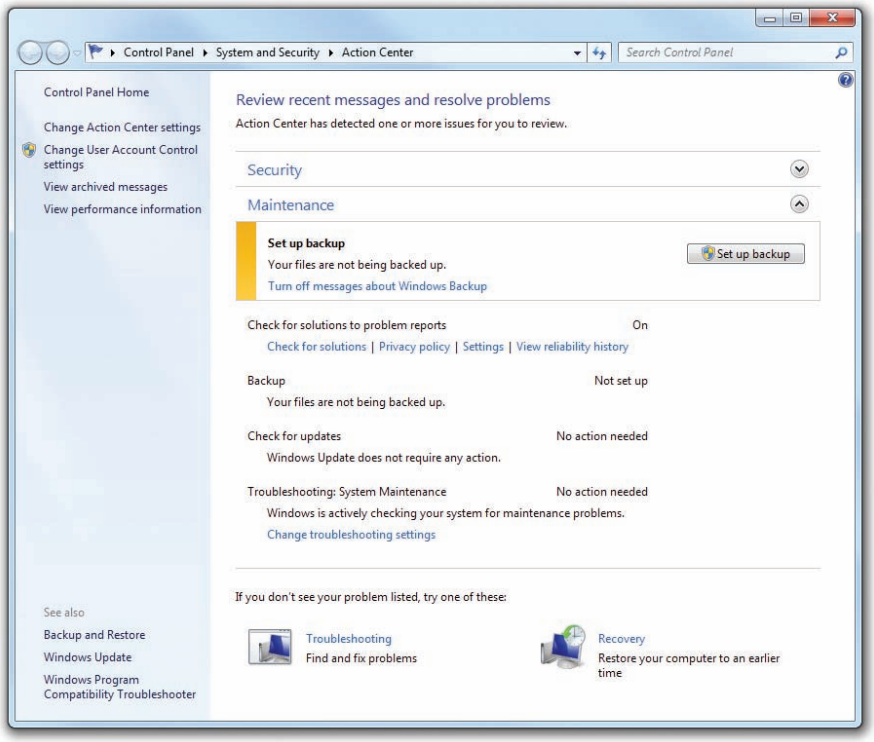
The **Problem Reports and Solutions** Control Panel applet in Windows Vista lists all Windows Error Reporting issues (plus a few easy-to-check items like firewall and antimalware status), as shown in Figure 19.41. You click on the solution and, in many cases, the problem is fixed.



• **Figure 19.40** Crash.exe has stopped working.



• **Figure 19.41** Problem Reports and Solutions



• **Figure 19.42** Action Center

Action Center

Problem Reports and Solutions is a good tool but lacks some refinements. For example, once you fix a problem, you have to delete the problem from the list manually. Also, there are a number of issues that don't have anything to do with Windows Error Reporting that just make sense to combine, such as Microsoft Troubleshooter and System Restore. Microsoft realized that they could organize the solutions to make it easier for you to choose what you wanted to do. **Action Center** in Windows 7 provides a one-page aggregation of event messages, warnings, and maintenance messages that, for many techs, might quickly replace Event Viewer as the first place to look for problems. Unlike Event Viewer, Action Center separates issues into two sections, Security and Maintenance, making it easier to scan a system quickly (see Figure 19.42).

Action Center only compiles the information, taking data from well-known utilities such as Event Viewer, Windows Update, Windows Firewall, and UAC and placing it into an easy-to-read format. If you wish, you can tell Action Center where to look for information by selecting *Change Action Center settings* (see Figure 19.43).

If you see a problem, Action Center includes plenty of links to get you to the utility you need. From the Action Center applet, you get direct links to the following tools:

- UAC settings
- Performance Information and Tools
- Backup and Restore
- Windows Update
- Troubleshooting Wizard
- System Restore

Although Action Center does little more than reproduce information from other utilities, it makes finding problems quick and easy. Combined with quick links to most of the utilities you'll need, Action Center should become your base of operations when something goes wrong on your Windows 7 PC.

Performance Information and Tools

Techs must often answer difficult questions like "Why is my machine running so slowly?" Before Windows Vista, we could only use Performance Monitor baselines or third-party tools. Neither of these options worked very well. Baselines required you to choose the right counters—choosing

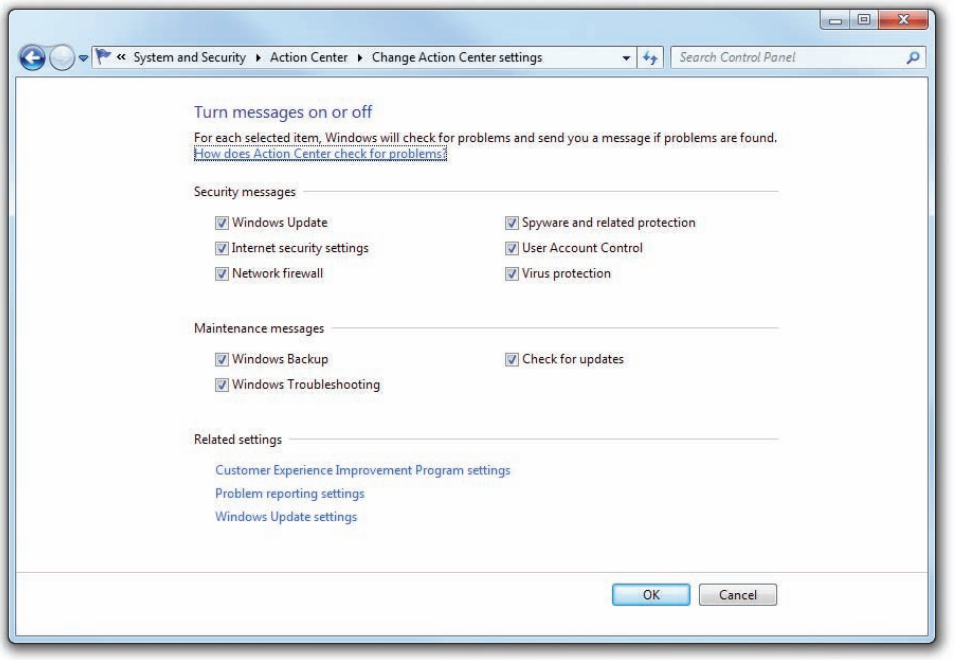
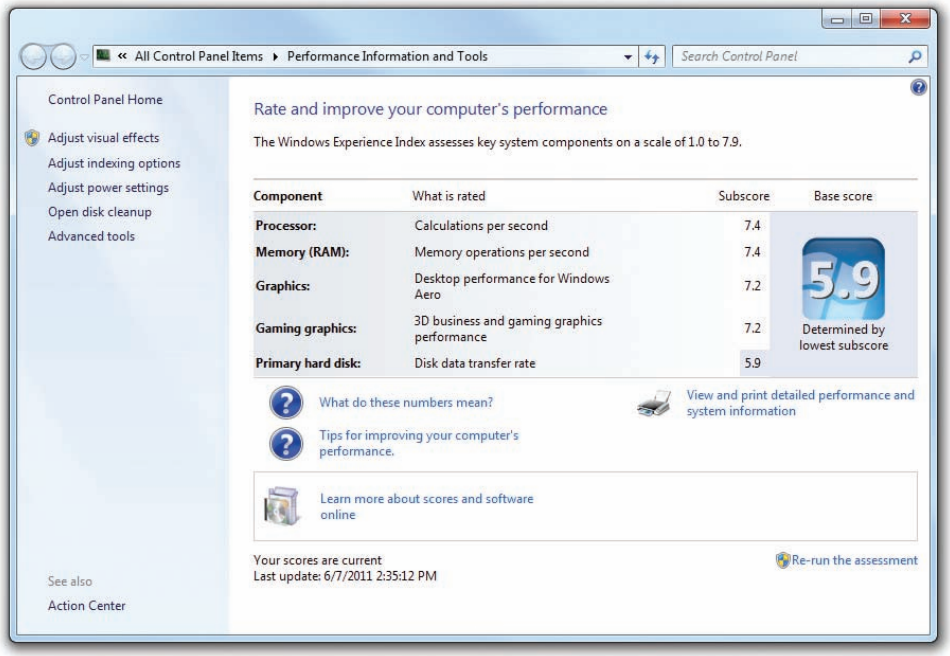


Figure 19.43 Change Action Center settings



• **Figure 19.44** Performance Information and Tools

the wrong counters made useless and sometimes even distracting logs. Third-party tools often measured one aspect of a system (like video quality) very well but didn't help much when you wanted an overview of your system.

This changed with Microsoft's introduction of the Performance Information and Tools Control Panel applet (see Figure 19.44).

The **Performance Information and Tools** applet doesn't fix anything. It just provides a relative feel for how your computer stacks up against other systems using the Windows Experience Index. Windows bases this on five components:

- **Processor** Calculations per second
- **Memory (RAM)** Memory operations per second
- **Graphics** Desktop performance for Windows Aero
- **Gaming graphics** 3-D business and gaming graphics performance
- **Primary hard disk** Disk data transfer rate

Each component generates a subscore. These values range from 1 to 5.9 for Windows Vista and 1 to 7.9 for Windows 7. Microsoft determines the calculations that generate these numbers, so I don't know exactly what it takes to give, for example, a CPU a score of 6.1. Your system's Base score is based on the lowest subscore.

The Performance Information and Tools applet won't fix anything, but tells you which component is the weakest link in overall performance.

You can't change a subscore in the Windows Experience Index without making some kind of hardware change.

Every once in a while you'll get an application that reports an error if the clock settings in Windows don't match. This can cause the application not to run. Likewise, if a computer has a failing battery and is offline for a while, the BIOS time and settings will be off. You'll get a brief "error" noting the change when you connect that computer to a network timeserver. This is both a hardware issue (failing battery) and an application issue. When the Windows clock resets, so does the BIOS time and settings.

Application Problems

Programmers want to write applications that work well, enable you to accomplish a specific task, and be good enough to earn your money. But PCs are complicated and programmers can't get it right every time with every combination of hardware and software.

Application problems show up in several ways. The typical scenario has the application failing to install or uninstall. Operating system version issues can cause compatibility problems. Another typical scenario is where an application tries to access a file and that file is either missing or won't open. The least common problems come from sloppy or poorly written

code that causes the application or the operating system to crash. Finally, corrupted applications can corrupt data too, but Windows has tools for recovering previous versions of files and folders.

Application Installation Problems

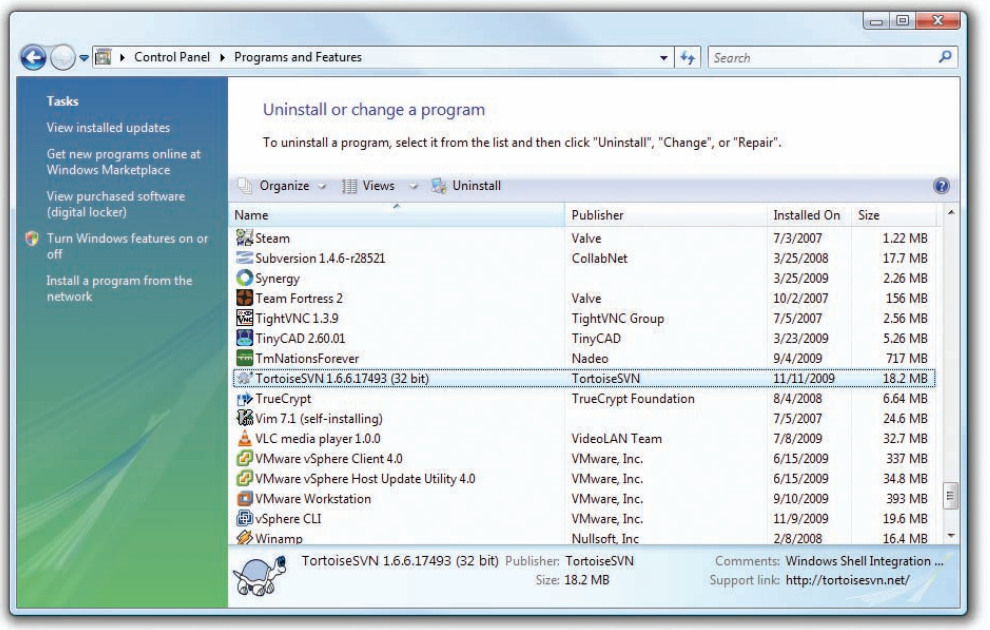
Almost all Windows programs come with some form of handy installer. When you insert the disc, Windows knows to look for a text file called autorun.inf that tells it which file to run off the disc, usually setup.exe. If you download the application, you'll need to double-click it to start the installation. Either way, you run the installer and the program runs. It almost couldn't be simpler.

A well-behaved program should always make itself easy to uninstall as well. In most cases, you should see an uninstallation option in the program's Start menu area; and in all cases (unless you have an application with a badly configured installer), the application should appear in either the Add/Remove Programs applet or the Programs and Features applet (see Figure 19.45) in the Control Panel.

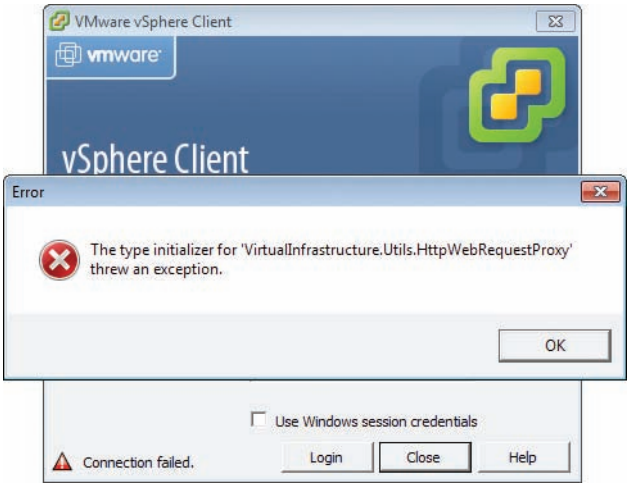
Programs that fail to install usually aren't to blame in and of themselves. In most cases, a problem with Windows prevents them from installing, most notably the lack of some other program that the application needs so it can operate. One of the best examples of this is the popular Microsoft .NET Framework. .NET is an extension to the Windows operating system that includes support for a number of features, particularly powerful interface tools and flexible database access. Programs written to incorporate .NET require the proper version of the framework installed to function. Many such programs attempt to install the .NET framework when you install the program, but this doesn't always work. If .NET is missing or if the version of .NET you are using is too old (there have been a number of .NET versions since it came

The fact that Windows looks for the autorun.inf file by default when you insert a disc creates a security issue. Someone could put a malicious program on a disc and write an autorun.inf file to point to the virus. Insert the disc and boom! There goes your clean PC. Of course, if someone has access to your computer and is fully logged on with administrator privileges, then you've already lost everything, with or without a disc-born program, so this "big" security issue is pretty much not an issue at all. Nevertheless, you should know that to turn off this behavior in Windows requires opening the Registry Editor and changing up to six different settings.

Remember that you need local administrator privileges to install applications in all versions of Windows.



• **Figure 19.45** Programs and Features Control Panel applet



• **Figure 19.46** .NET error

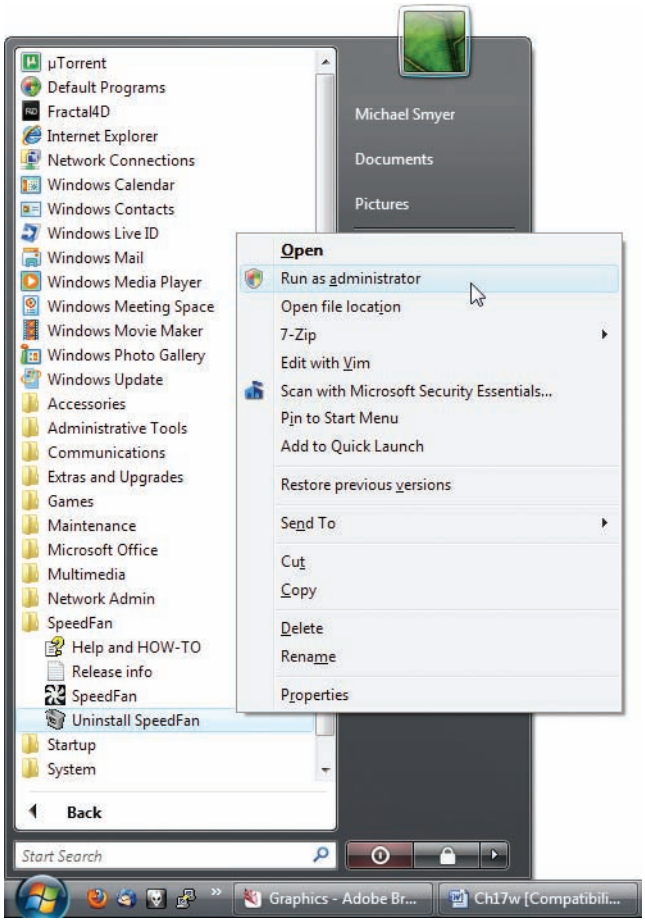
out in 2002), you can get some of the most indecipherable errors in the history of Windows applications.

Figure 19.46 shows one such example in Windows 7 where the VMware vSphere client fails due to the wrong .NET version. Too bad the error doesn't give you any clues!

These types of errors invariably require you to go online and do Web searches, using the application name and the error. No matter how bad the error, someone else has already suffered from the same problem. The trick is to find out what they did to get around it.

Problems with Uninstalling

The single biggest problem with uninstalling is that people try to uninstall without administrator privileges. If you try to uninstall and get an error, log back on as an administrator and you should be fine. Don't forget you can right-click on most uninstallation menu options on the Programs menu and select *Run as administrator* to switch to administrator privileges (see Figure 19.47).



• **Figure 19.47** Selecting Run as administrator from the context menu

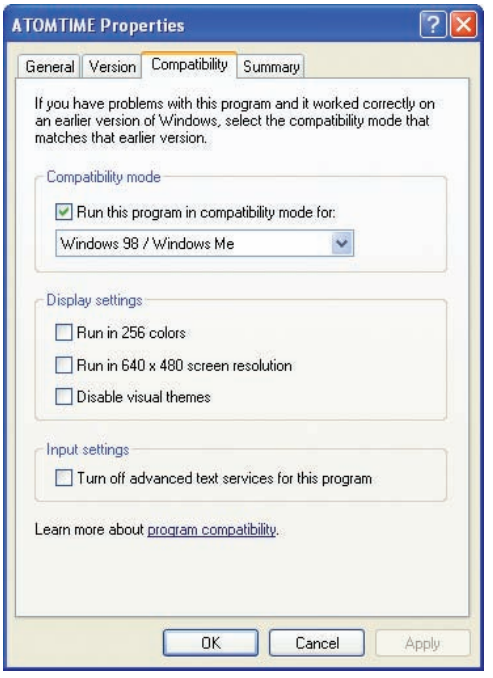
Compatibility

Most applications are written with the most recent version of Windows in mind, but as Windows versions change over time, older programs have difficulty running in more recent Windows versions. In some cases, such as the jump from Windows Vista to Windows 7, the changes are generally minor enough to cause few if any compatibility problems. In other cases, say a program written back when Windows 98 was around, the underpinnings of the OS differ so much that you have to perform certain steps to ensure that the older programs run. Windows XP, Windows Vista, and Windows 7 provide different forms of **compatibility modes** to support older applications.

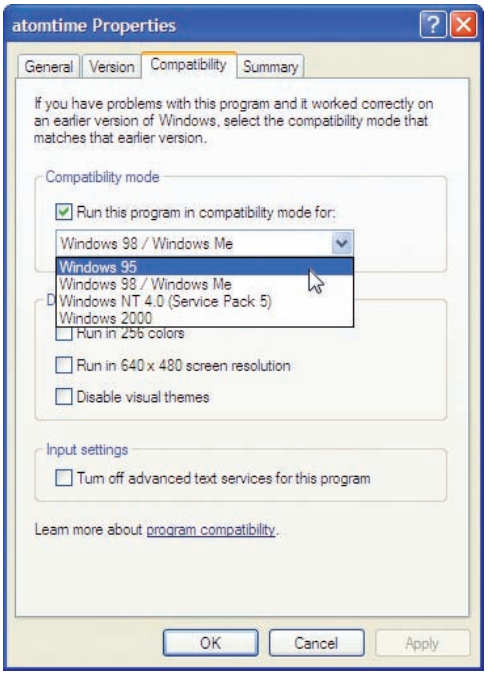
Windows XP handles compatibility using the aptly named Compatibility tab (see Figure 19.48) in every executable program's Properties dialog box (right-click on the executable file and click Properties). Select the version of Windows you want Windows XP to emulate, and in many cases that is all you need to do to make that older program work (see Figure 19.49).

You can also set other settings on the Compatibility tab, such as the following located under Display settings:

- **Run in 256 colors** Many old Windows programs were designed to run in 256 colors. Later versions of Windows that support more colors can confuse these older programs.
- **Run in 640 × 480 screen resolution** A few (badly written) older programs assume the screen to be at 640 × 480 resolution. This setting enables them to work.
- **Disable visual themes** Windows themes change a program window's title bar, fonts, and menus, which might make problems for some programs.



• **Figure 19.48** XP Compatibility tab



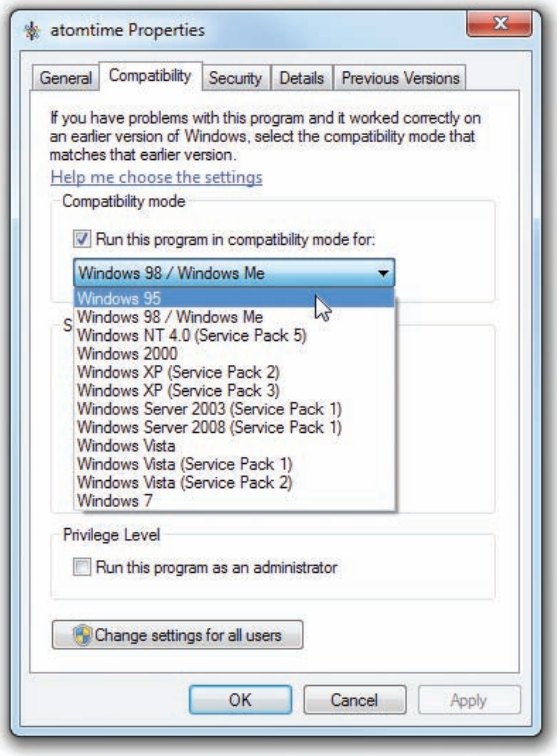
• **Figure 19.49** Compatibility mode options in Windows XP

Windows Vista and Windows 7 add some important improvements to the Compatibility tab. Both add more recent OS options to the Compatibility mode drop-down menu. Figure 19.50 shows the many options available in Windows 7.

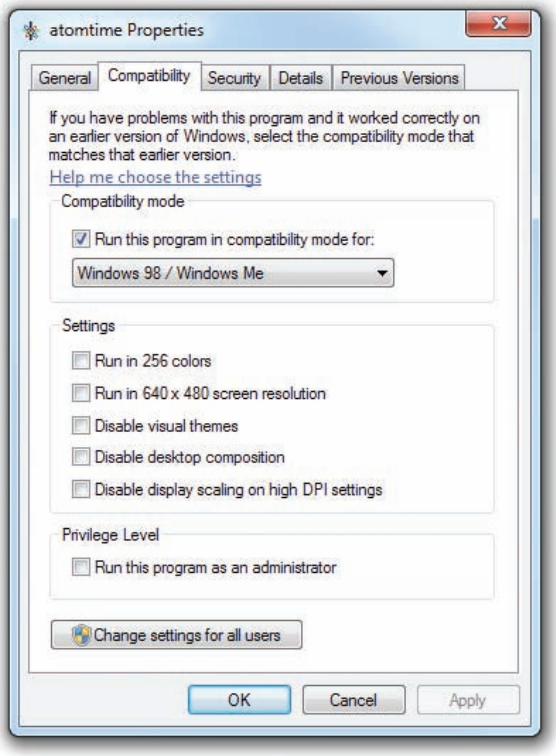
The newer Compatibility tab also adds some new options (see Figure 19.51) to help older programs run:

- **Disable desktop composition** Disables all display features such as Aero. More advanced Windows display features often bog down older programs.
- **Disable display scaling on high DPI settings** Turns off automatic resizing of a program's windows if you're using any high DPI (dots per inch) font. This was added because many programs with large fonts would look bizarre if resized.
- **Run this program as an administrator** As stated, enables you to run the program as an administrator. If this option isn't available, log on as an administrator to see it.
- **Change settings for all users** Clicking this button applies compatibility changes made to a program to every user account on the machine. Otherwise, the settings are only for the current user.

If you need to make things 100 percent compatible with Windows XP and you have Windows 7 (Professional, Ultimate, and Enterprise only)



• **Figure 19.50** Compatibility mode options in Windows 7



• **Figure 19.51** Windows 7 Compatibility tab

installed on your system, you can download Windows XP Mode. **Windows XP Mode** is nothing more than a premade Windows XP SP3 virtual machine that runs under Microsoft's popular (and free) virtualization program, Windows Virtual PC (see Figure 19.52).

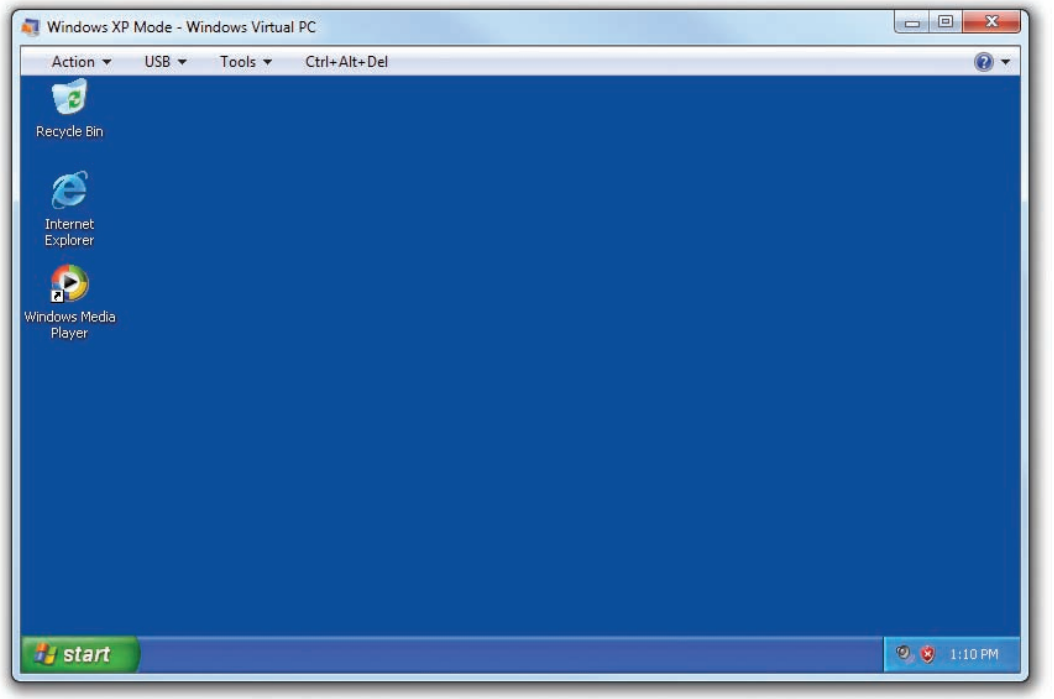
We'll wait until Chapter 30 for a complete discussion of virtualization and how it works, but for now it's important to appreciate that Windows XP Mode is nothing more than a copy of Windows XP. You can install programs in this virtual machine, access the Internet, print to your printers—everything that you can do with a real computer.

The secret to using compatibility mode isn't much of a secret at all: if the program doesn't run, try a compatibly mode. If you want to be really careful, do a Web search on your application before you try to run it. Compatibility mode is a handy tool to get older applications running.

Missing File or Incorrect File Version

An application may rely on other files, in particular DLL files. Sometimes the application installer will bring specially formatted versions of common DLL or other files to Windows, overwriting the previous versions. Later applications might look for the earlier version of the DLL and fail when it's not found.

You'll experience this sort of scenario with error messages such as "missing DLL" or "cannot open file *xyz*." The usual fix for either issue is to perform an Internet search for the missing DLL or file that fails to open, along with the name of the program you're trying to use.



• **Figure 19.52** Windows XP Mode

Crashing Programs

Occasionally, a program gets released that isn't ready for prime time and the error-prone code causes the application to crash or even causes the operating system to crash. I've seen this most often with games rushed to market near the winter holidays. The results of this rushed code can be pretty spectacular. You're right in the middle of a thrilling fight with the bad guy and then what happens? A crash to desktop (CTD).

Poorly written or buggy programs can have awful effects on you and your clients. Some of the scenarios caused by such programs are the computer locking up or unexpectedly shutting down. The system might spontaneously shut down and restart. That kind of improper shutdown can cause problems, especially to open files and folders.

The problem here is that all this crashing can be caused by hardware and driver problems, not just application problems. You've got to keep in mind all of these things as you approach troubleshooting a crash.

One error common on older systems, still mentioned on the CompTIA A+ exams but largely absent or invisible on modern systems, is a *general protection fault* (*GPF*). A GPF occurs when a program tries to do something not permitted, like writing to protected memory or something else Windows doesn't like. This can cause an error message to appear or can even crash the computer. You are very unlikely to encounter a GPF today.

Here's a typical scenario where you need to troubleshoot broadly first. If you're playing a graphically intensive game that happens to be huge and takes up a lot of RAM, what could the problem be if the screen locks up and Windows locks up too? It could be that the program ran a routine that clashed with some other application or used a Windows feature improperly. It could be that the video card was marginal and failed when taxed too much. It could be that the system accessed a section of RAM that had gone bad.

In that same scenario, though, where the game runs but degrades the overall performance of Windows, what could cause that problem? That points more squarely at the application side of things rather than the hardware or drivers, especially if the computer successfully runs other programs. The bottom line with crash issues is to keep an open mind and not rule out anything without testing it first.

Volume Shadow Copy Service and System Protection

One of the big headaches to a failure with an application isn't so much the application itself but any data it may have corrupted. Sure, a good backup or a restore point might save you, but these can be a hassle. Unless the data was specifically saved (in the backup), there's a chance you don't have a backup in the first place. Microsoft came to your rescue in Windows Vista (Business, Ultimate, and Enterprise only) and Windows 7 (all editions) with a feature called System Protection.

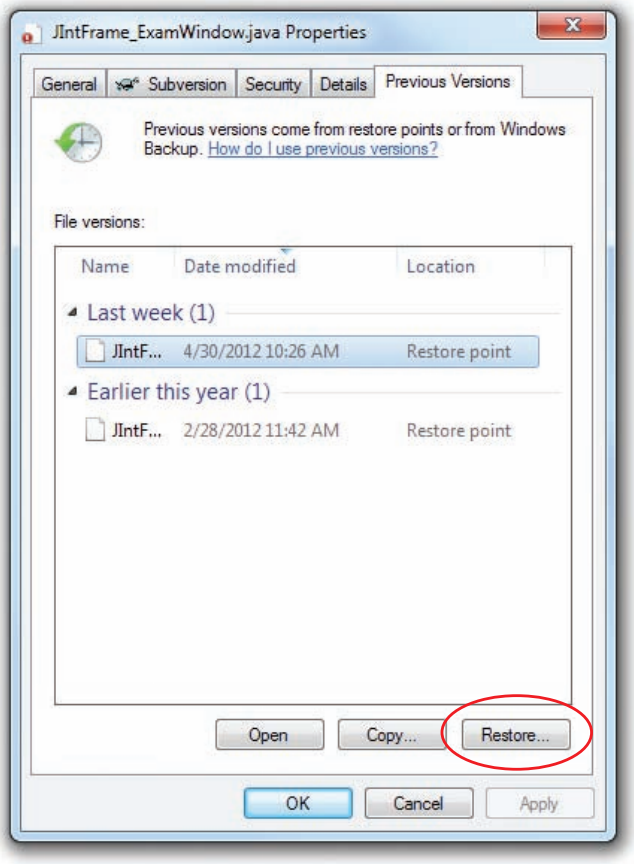
This amazing feature is powered by Volume Shadow Copy Service (VSS), a feature introduced in Windows XP and used by ntbackup. VSS enables the operating system to make backups of any file, even one that is in use. In Windows Vista and 7, VSS is also used by **System Protection**, enabling you to access previous versions of any data file or folder. Try right-clicking on any data file and selecting *Restore previous versions*, which opens the file's Properties dialog box with the Previous Versions tab displayed, as shown in Figure 19.53.

If any of the following criteria are met, you will have at least one previous version in the list:

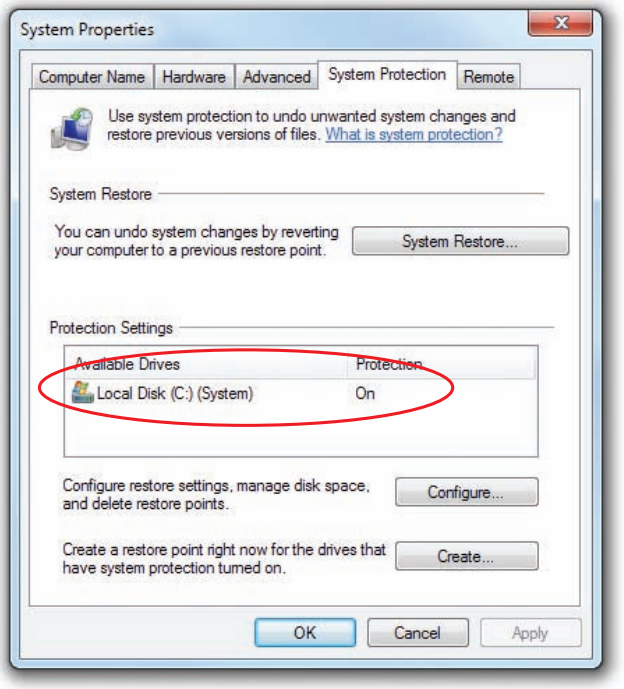
- The file or folder was backed up using the backup program.
- You created a restore point.
- The file or folder was changed.

You must make sure System Protection is enabled as well. Go to the System Protection tab in the System Properties dialog box (see Figure 19.54) to see if the feature is enabled (it should be running by default).

System Protection falls in the category generically called *file recovery software*, and does an outstanding job. You can also get many third-party utilities that accomplish general file recovery. I've used Recuva from Piriform many times, for example, to get "deleted" data off a hard drive or RAID array.



• **Figure 19.53** Previous Versions tab



• **Figure 19.54** System Protection tab

Keep in mind that System Protection doesn't have to be only for recovery of corrupted data files caused by bad applications. It's also a great tool to recover previous versions of files that users accidently overwrite.

The System Protection tab also enables you to load a restore point and to create restore points manually, very handy features.

Chapter 19 Review

Chapter Summary

After reading this chapter and completing the exercises, you should understand the following about troubleshooting Windows.

Troubleshoot Windows boot problems

- If you see an "NTLDR is Missing" or "BOOTMGR is missing" error, you first want to check your hardware configuration. Check the screen—what do you see? Is the PC plugged in? These are all common problems. If that doesn't work, you should use either Windows XP's Recovery Console or Windows Vista/7's Recovery Environment (also known as the System Recovery Options menu).
- The Recovery Console works as a command-line utility. Many of its commands are those familiar to DOS users, but some new commands have also been added. Because the file for the Recovery Console is on the system partition in a folder called cmdcons, this program is useless for system partition crashes, but it is excellent for restoring Registries, stopping problem services, or using the expand program to extract copies of files from an optical disc or floppy disk. You can also use it to partition and format hard drives and read and write on local FAT or NTFS volumes. It's also good for repairing the MBR, reinstalling the boot files, and rebuilding boot.ini.
- A bad boot sector usually shows up as a No Boot Device error. If it turns out that this isn't the problem, the Recovery Console command to fix it won't hurt anything. At the Recovery Console prompt, just type **fixmbr**, which fixes the master boot record.
- The second problem the Recovery Console is best at fixing is missing system files, usually indicated by the error "NTLDR bad or missing." To fix this, get to the root directory (**cd**) and type the following line: **copy d:\i386\ntldr**. Then type **copy d:\i386\ntdetect.com**. To rebuild the boot.ini file, type **bootcfg /rebuild**.
- Automated System Recovery can restore your system to a previously installed state, but you should use it as a last resort. You lose everything on the system that was installed or added after you created the ASR disk.
- When rebuilding your Windows installation, you're best off swapping the C: drive for a blank hard drive and installing a clean version of Windows. You may also have a Recovery CD or recovery partition that came with your computer. These tools can restore your PC to its factory settings.
- Windows Vista/7 do not use the Recovery Console. Instead, you boot to the Windows Preinstallation Environment (Windows PE). Here, you can boot directly to the Windows installation disc or access a set of repair tools known as the Windows Recovery Environment (Windows RE). Windows RE is also called the System Recovery Options menu.
- From Windows RE, you can access Startup Repair, System Restore, System Image Recovery/Windows Complete PC Restore, Windows Memory Diagnostics (Tool), and the Command Prompt.
- The Startup Repair utility enables you to repair a corrupted Registry, restore critical system files, roll back nonfunctioning drivers, uninstall incompatible service packs and patches, and more. In Windows 7, Startup Repair runs automatically if the system detects a boot problem.
- System Restore enables you to return your system to a previous state.
- The System Image Recovery/Windows Complete PC Restore tools use a system image to restore the files, applications, and settings for your PC. You will need to use the Backup and Restore Center/Backup and Restore applet in Control Panel to make a system image first.
- The Windows Memory Diagnostics (Tool) checks for bad RAM that may be causing BSoDs, system lockups, or continuous reboots. This tool isn't perfect, and can sometimes cause more problems than it fixes. Check out Memtest86+ for another solution.
- Unlike the Recovery Console in Windows XP, the Command Prompt in Windows RE is fully featured. It also adds an important utility called bootrec, which enables you to troubleshoot the master boot record, boot sector, and BCD store. You can also work with the boot configuration data using the bcdedit command.

Troubleshoot Windows GUI problems

- Several issues can cause Windows to hang during the GUI-loading phase, such as buggy device drivers, Registry problems, and even autoloading programs.
- If you get errors like "Registry File Failure" or "Windows could not start," you should try restoring a good copy of the Registry. You can do this manually or by using the Last Known Good Configuration boot option from the Advanced Startup Options menu. To get to the Advanced Startup Options menu, restart the computer and press F8 after the POST messages but before the Windows logo screen appears. From here, you can start your computer into Safe Mode or into the Last Known Good Configuration.
- From the Advanced Startup Options menu, you can boot your computer into Safe Mode. Safe Mode uses basic, non–vendor-specific drivers for mouse, display, keyboard, storage, and system services. You can also use Safe Mode with Networking and Safe Mode with Command Prompt, which enable networking and the command prompt, respectively.
- Enable Boot Logging creates a log of the boot process as the drivers are loaded into memory. The file is named Ntbtlog.txt and is saved in the %SystemRoot% folder.
- Enable VGA Mode in Windows XP and Enable Low-Resolution Mode in Windows Vista/7 boot into Windows normally but disable your normal display driver and use a standard one instead.
- Last Known Good Configuration loads the configuration of Windows that existed immediately before you installed the most recent device driver.
- Directory Services Restore Mode is designed for use with Active Directory domain controllers. Debugging Mode sends a debug of the kernel to a second computer. Both of these tools are only used in very specific circumstances.
- With the Disable Automatic Restart on System Failure mode, you can prevent Windows from automatically rebooting after a BSoD. You can also use the Disable Driver Signature Enforcement mode to use devices without signed drivers that Windows Vista/7 would otherwise prevent you from using. You can also start Windows normally, reboot, or return to the OS Choices menu.
- Event Viewer in Window shows you all sorts of interesting happenings on the system. You can record application events, security events, and system events. One of these recorded events may be able to tell you why the system crashed, locked up, or otherwise failed.
- The System Configuration utility enables you to keep individual programs and services from autoloading, but it does not actually remove the programs/services.
- Windows loads a number of services as it starts. If any critical service fails to load, Windows will tell you at this point with an error message.
- Task Manager is a great place to go to shut down errant processes that won't otherwise close properly. If you're unable to get to Task Manager or are comfortable with the command line, you can use the tasklist and taskkill commands to do the same thing.
- Windows protects all of its critical DLL files very carefully, but once in a while you may get an error saying Windows can't load a particular DLL. In these cases, the tool you need is the System File Checker. Use it to check a number of critical files, including the ever-important DLL cache, and replace any corrupted ones.
- The Problem Reports and Solutions Control Panel applet in Windows Vista lists all Windows Error Reporting issues and shows the status of your firewall and antimalware software. In Windows 7, Microsoft enhanced this tool and created the Action Center. The Action Center performs all of the same functions as the Problem Reports and Solutions applet, but adds the Microsoft Troubleshooter, System Restore, and several other messages and warnings.
- While the Performance Information and Tools applet doesn't fix anything, it does provide you a relative feel for how your machine stacks up against other systems. Using the Windows Experience Index, the applet ranks your processor, RAM, graphics, and hard disk on a scale of 1 to 5.9 for Windows Vista and on a scale of 1 to 7.9 for Windows 7.

Troubleshoot Windows application problems

- Programs that fail to install usually aren't to blame in and of themselves. In most cases, a problem with Windows prevents them from installing, most notably the lack of some other program that the application needs so it can operate. If you get an error while trying to uninstall a program, log back on as an administrator and try again.
- Most applications are written with the most recent version of Windows in mind, but as Windows versions change over time, older programs have difficulty running in more recent Windows versions. You can use compatibility modes to emulate older versions of Windows. Other compatibility settings include lowering the resolution, lowering the number of colors, disabling themes, and so on.
- If you see an error message about a missing DLL file, use the Internet to search for the missing file and find the popular solution.
- If your applications crash repeatedly, it could be bad programming. It could also be a hardware or driver problem that causes the application to crash. You'll need to check both software and hardware to find out why applications crash to desktop.
- Windows Vista Business, Ultimate, and Enterprise and all editions of Windows 7 use Volume Shadow Copy Service, which enables the OS to make backups of any files, even one that is in use. Windows Vista/7 also use System Protection, which enables you to access previous versions of any data file or folder.

Key Terms

Action Center *(714)*
Advanced Startup Options *(702)*
bcdedit *(696)*
Blue Screen of Death (BSoD) *(701)*
bootrec *(696)*
compatibility mode *(719)*
diskpart *(698)*
Event Viewer *(706)*
Last Known Good Configuration *(705)*
Live DVD *(687)*
Performance Information and Tools *(716)*
Problem Reports and Solutions *(713)*
Recovery Console *(683)*
restore point *(691)*
Safe Mode *(702)*
Startup Repair *(689)*
System File Checker *(712)*
System Protection *(722)*
System Restore *(691)*
Task Manager *(712)*
Windows Preinstallation Environment (WinPE) *(687)*
Windows Recovery Environment (WinRE) *(687)*
Windows XP Mode *(721)*

Key Term Quiz

Use the Key Terms list to complete the sentences that follow. Not all terms will be used.

1. The _____ tool enables you to view and modify the BCD store.
2. Use the _____ to check and replace any corrupted critical Windows files, such as DLLs.
3. If Windows fails but you have *not* logged on, you can select _____ to restore the computer to the way it was the last time a user logged on.
4. To start Windows using only the most basic and essential drivers and services, use _____.
5. The _____, accessed by pressing CTRL-SHIFT-ESC once, enables you to see all applications or programs currently running or to close an application that has stopped working.
6. Use the _____ in Windows 7 to see an aggregation of event messages, warnings, and maintenance messages.

7. In Windows Vista and Windows 7, you can use the _____ feature to recover previous versions of corrupted or deleted files.
8. To run a program written for Windows XP in a Windows 7 computer, use _____ if you encounter problems.
9. The _____ applet provides a relative feel for how your computer stacks up against other systems using the Windows Experience Index.
10. While Windows XP provides the Recovery Console troubleshooting environment, Windows Vista and Windows 7 include the _____.

Multiple-Choice Quiz

1. Mark loaded a new video card on his system, but now everything looks very bad. What should he do first?
   - **A.** Go to Event Viewer and check the log
   - **B.** Go to Device Manager
   - **C.** Go to the printed manual
   - **D.** Call tech support
2. Which utility is useful in identifying a program that is hogging the processor?
   - **A.** Task Manager
   - **B.** Device Manager
   - **C.** System Monitor
   - **D.** System Information
3. You've just installed a software update, rebooted, and now your system experiences random crashes. Which utility should you use first to try to fix the problem?
   - **A.** Automated System Restore
   - **B.** Device Manager
   - **C.** System Restore
   - **D.** Recovery Console
4. You suspect your system is failing to boot because of a corrupt master boot record. Which utility is the best to fix this?
   - **A.** Automated System Restore
   - **B.** Device Manager
   - **C.** System Restore
   - **D.** Recovery Console
5. What command should you run to check and fix corrupt system files, DLLs, and other critical files?
   - **A.** cmdcons /fixboot
   - **B.** sfc /scannow
   - **C.** chkdsk /r
   - **D.** defrag –a
6. You get a tech call from a distraught Windows XP user who can't get into Windows. He says he has a Recovery CD from the manufacturer and plans to run it. What would you suggest?
   - **A.** Run the Recovery CD to restore the system
   - **B.** Run the Recovery CD to return the system to the factory-installed state
   - **C.** Try to get the computer to boot into Safe Mode
   - **D.** Reinstall Windows by using a Windows XP disc
7. Which of the following points to a hardware or CMOS problem rather than an OS problem with a PC that won't boot.
   - **A.** A black screen with the error message "invalid boot disk"
   - **B.** A black screen with the error message "NTLDR Bad or Missing"
   - **C.** A black screen with the error message "Invalid BOOT.INI"
   - **D.** A black screen with the error message "Invalid BCD"
8. John's computer has an error that says bootmgr is corrupted. What tool can he use to fix this problem?
   - **A.** bcdedit
   - **B.** chkdsk
   - **C.** config.sys
   - **D.** regedit

9. What does Microsoft call the 32- or 64-bit installation environment in Windows 7?
   - **A.** WinEE
   - **B.** WinPE
   - **C.** WinRE
   - **D.** Recovery Console
10. Ralph suspects a bad RAM stick is causing Windows to fail to boot. What default Windows tool can he use to check the RAM?
   - **A.** MEMMAKER
   - **B.** Memtest86+
   - **C.** Windows RAM Diagnostic Tool
   - **D.** Windows Memory Diagnostics Tool
11. If you create a system image from Windows 7's Backup and Restore applet, what gets backed up?
   - **A.** Everything
   - **B.** Essential system files and personal information for all users
   - **C.** Personal information for all users
   - **D.** Personal information for all users and a full system image
12. Which of the following commands will repair a damaged master boot record in a Windows 7 PC?
   - **A.** bootrec /fixboot
   - **B.** bootrec /fixmbr
   - **C.** fixboot
   - **D.** fixmbr
13. Ellen tries to boot into Windows but the computer crashes at the logon screen. What tool should she use first to try to fix the problem?
   - **A.** Boot to the Windows DVD, get to WinRE, and type **clean** at the diskpart prompt
   - **B.** Boot to the Windows DVD, get to WinRE, and run Startup Repair
   - **C.** Reboot the PC, press F8 to open the Advanced Startup Options menu, and select Safe Mode
   - **D.** Reboot the PC, press F8 to open WinRE, and select Safe Mode
14. Which feature in Windows 7 enables you to right-click a file or folder and restore previous versions of that file or folder?
   - **A.** Reversion
   - **B.** System Protection
   - **C.** System Revert
   - **D.** Undelete
15. Which of the following can cause a computer to lock up or unexpectedly shut down? (Select two.)
   - **A.** Bad RAM
   - **B.** Poorly written application
   - **C.** Windows Installer
   - **D.** Windows remote shutdown

Essay Quiz

1. Your team needs to present a case for updating the primary company computers from Windows XP to Windows 7. Your role is to discuss and contrast the recovery tools in case of system crashes. Write an essay on how the recovery tools work in Windows 7 compared to how the recovery tools work in Windows XP.
2. The Registry Editor is the universal tool for editing the Registry in all versions of Windows (covered on the CompTIA A+ exams). Your boss needs an explanation of the Registry and how the Registry Editor can be used to back up and restore the Registry files. Explain these things to your boss (you can draw from Chapter 8 and Chapter 15 as well). Don't forget to tell the boss how to load the Registry Editor!
3. Write an essay that contrasts the three Safe Mode options available in the Advanced Startup Options menu. Why would you use anything but straight-up Safe Mode? Provide a scenario in your answer for why Safe Mode with Command Prompt might offer better troubleshooting options than Safe Mode with Networking.

Lab Projects

• Lab Project 19.1

On your test system, put the Windows recovery tools to the test. You can do this project in any of the relevant versions of Windows. Back up the system. Create a system image if you're using Windows 7. Create a system repair disc. Make some catastrophic change to Windows, then boot to the system repair disc and run through the recovery process.

• Lab Project 19.2

Similar to Lab Project 19.1, put the System Protection tool in Windows 7 to the test. Delete some files. Right-click on the folder they were deleted from and select *Restore previous version*. What happens? Go further. Delete a whole folder, then select *Restore previous version* from the folder in which that deleted folder resided. What happens? Try both exercises again, but this time empty the Recycle Bin before trying to restore. What happens now?