Chapter 12

Having Fun with Sysinternals

Solutions in this chapter:

- Generating a Blue Screen of Death on Purpose (BlueScreen)
- Modifying the Behavior of the Keyboard (Ctrl2cap)
- Creating Useful Desktop Backgrounds (BgInfo)
- Bypassing the Login Screen (Autologon)

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

Introduction

This book has dealt with the mundane and pedestrian duties of an administrator, or a programmer acting as an administrator—until now. It is about time we used some of the available tools for "fun and profit," with an emphasis on "fun." The Winternals group has created software that not only makes our administrative tasks easier, but also entertains us.

In this chapter, we will learn about a screensaver with a "perverted" twist to it. We also will find out how to modify the behavior of our keyboards to suit the needs of older users, create an informative desktop background, and finally, bypass the pesky login screen.

Generating a Blue Screen of Death on Purpose (BlueScreen)

The Blue Screen of Death, or BSOD, is one of the most dreaded things that a computer user or administrator can see. Due to various resource conflicts, unstable drivers or dynamic link library (DLL) files, and other system issues, a system crash was once more a probability than a possibility and it always seemed to occur just in time to wipe out hours of work you had not yet saved.

If you look at it from a different point of view, though, the BSOD is a good thing. If the system crashed and just rebooted for no apparent reason, that would be bad. However, Microsoft had the forethought to design the system to display pertinent information about the system crash against a blue background, while dumping the contents of the memory to a file to allow more forensic investigation into the cause of the crash. It is the BSOD that helps the administrator collect the information necessary to get the machine running stable again.

Thanks to the BlueScreen screensaver from Sysinternals, the dreaded BSOD can also be a fun way to protect your computer while you're away, or trick your friends and co-workers.

Installing BlueScreen

To install the BlueScreen screensaver, just copy the **bluescrn.scr** file to the \system32 directory on a Windows NT, 2000, XP, or 2003 machine. If you are using a Windows 9*x* version, copy the file to the \Windows\System directory.

Configuring & Implementing…

Preparing Windows 9*x* to Run BlueScreen

Even though the Blue Screen of Death is no stranger to users of older versions of Windows, the Sysinternals BlueScreen screensaver relies on the ntoskrnl.exe file for some of its functionality.

In order to run the BlueScreen screensaver on a Windows 9*x* computer system, you need to copy the \winnt\system32\ntoskrnl.exe file from a Windows 2000 computer into the \Windows\System directory of your Windows 95, Windows 98, or Windows Me computer.

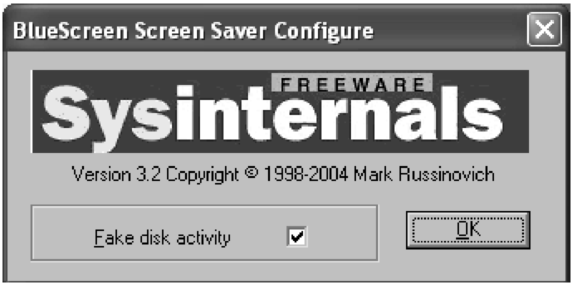
Setting Up the BlueScreen Screensaver

To enable the BlueScreen screensaver once you have installed it, simply right-click on the **Windows desktop** and select **Properties** to bring up the **Display Properties** window. Click the **screensavers** tab and scroll through the drop-down list to find the screensaver called **Sysinternals BlueScreen**.

Like you can with any other screensaver, you can choose how many minutes the computer should be idle before the screensaver is launched, and whether a password should be required to gain access to the system once the screensaver is running.

If you click on the **Settings** button, you can open the BlueScreen configuration options, shown in Figure 12.1. There is really only one option to select. If you want the BlueScreen screensaver to fake disk activity for added realism, check the **Fake disk activity** box and click **OK**.

Figure 12.1 The BlueScreen Screensaver



Version 3.2 Copyright © 1998-2004 Mark Russinovich

Fake disk activity ☑

Let the Fun Begin

After you have installed and configured the screensaver, you can wait for the necessary amount of time to expire so that the screensaver will launch, or you can click on **Preview** from within the **screensaver** tab of the **Display Properties** window. The screensaver will initiate a realistic-looking BSOD crash, complete with a system reboot.

The screensaver will cycle between various blue-screen crashes and simulate a system reboot approximately every 15 seconds. What makes the BlueScreen screensaver more than just a screensaver is the accuracy and realism of the simulated BSOD. The screensaver includes information from the actual computer, including the NT build number, processor revision, currently loaded drivers and addresses, characteristics of the disk drive, and amount of memory on the computer.

The screensaver also includes more-realistic functionality, depending on the operating system on which you run it:

- On Windows NT 4.0 systems, BlueScreen will simulate chkdsk on reboot, complete with finding errors.
- Running BlueScreen on Windows 2000 or 9*x* computers will show a Windows 2000 startup splash screen with an active progress bar and progress control updates to simulate a realistic reboot.
- Windows XP and Windows Server 2003 systems will display the XP/Server 2003 startup splash screen with progress bar activity.

Modifying the Behavior of the Keyboard (Ctrl2cap)

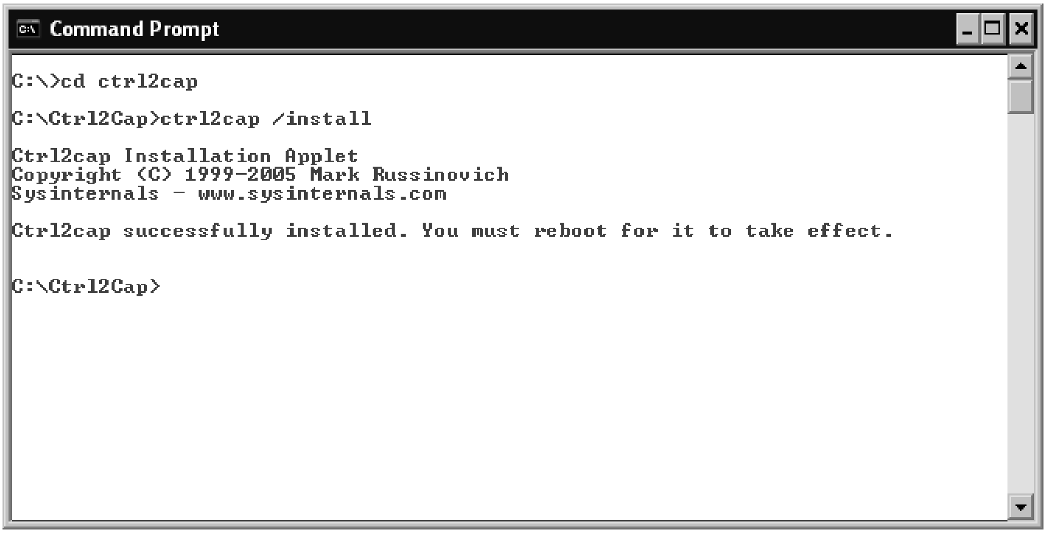
Users who have transitioned from pure Unix machines to a Windows-based system will appreciate this utility. The Unix keyboard generally has a left Ctrl key above the Shift key on the left, where you typically find the Caps Lock key on a Windows keyboard.

The problem is that Unix developers use the left Ctrl key frequently and out of habit may constantly enable and disable the Caps Lock key on the Windows machine. This tool converts the Caps Lock key to a left Ctrl key again so that Unix users and developers can feel at home.

Installing and Using Ctrl2cap

You can download the Ctrl2cap files from Sysinternals at www.sysinternals.com/Utilities/Ctrl2Cap.html. To install the utility, you have to extract the files to a directory on your hard drive. Once you have done that, open a command prompt window and navigate to the directory where you extracted the files. Type **ctrl2cap /install** and press **Enter**. A brief message will appear letting you know that the utility installed successfully, but that you must reboot in order for the changes to take effect (see Figure 12.2).

Figure 12.2 The Command Prompt Window Showing Successful Installation of Ctrl2cap



```
C:\>cd ctrl2cap

C:\Ctrl2Cap>ctrl2cap /install

Ctrl2cap Installation Applet
Copyright (C) 1999-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

Ctrl2cap successfully installed. You must reboot for it to take effect.


C:\Ctrl2Cap>
```

After you reboot, any time you press the Caps Lock key the operating system will treat the key as a Ctrl key. You can then use it in conjunction with other keys to perform Ctrl functions, such as Ctrl+B to enable or disable bold type or Ctrl+V to paste the contents of the clipboard.

Uninstalling Ctrl2cap

If you want to remove the Ctrl2cap utility so that you can use the Caps Lock key to lock the keyboard into using uppercase letters, you have to uninstall Ctrl2cap. Open a command prompt window and navigate to the directory where you have extracted the Ctrl2cap files. Type the following line of code and press the Enter key to remove Ctrl2cap:

```
ctrl2cap /uninstall
```

You must reboot once again in order for the uninstallation to complete and to return the keyboard to normal operation.

How It Works

Ctrl2cap intercepts keyboard requests and determines whether they are calling the Caps Lock function. If so, it redirects the call to the Ctrl function. On Windows 2000 and later systems, the function of the utility is a little more complex. Ctrl2cap installs as a Windows Driver Model (WDM) filter driver that is added to the keyboard class device stack above the keyboard class device.

According to the Sysinternals Web site, this approach has a couple of benefits:

- The Ctrl2cap utility's *IRP_MJ_READ* interception and manipulation code is shared between the NT 4.0 and Windows 2000 versions.
- There is no need to supply an INF file or go through the Device Manager to install the Ctrl2cap utility. Ctrl2cap simply modifies the necessary Registry entry.

NOTE

Because of the way Ctrl2cap interacts with Windows 2000 systems, bypassing the need for an INF file or installation through the Device Manager, you will not receive any warnings that the Ctrl2cap driver has not been digitally signed by Microsoft.

Creating Useful Desktop Backgrounds (BgInfo)

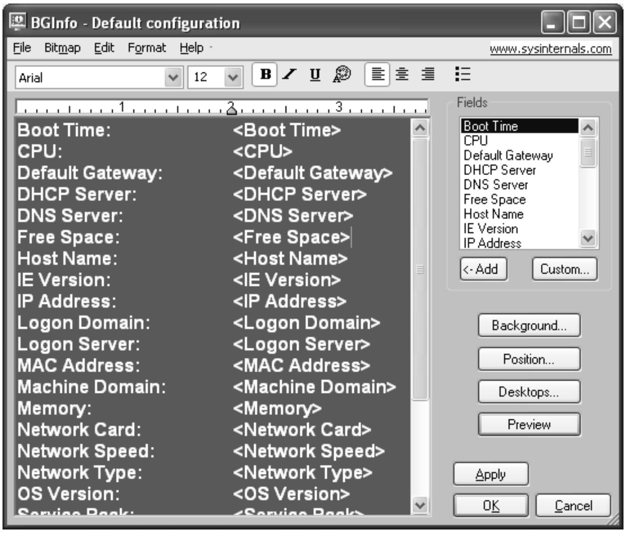
The BgInfo utility from Sysinternals allows you to display useful and relevant information about the computer, right on the desktop. This feature can be very helpful in a corporate network setting to help field technicians quickly identify the attributes of the system they are working on, or for users to have access to this information when placing calls to the help desk.

To run the BgInfo utility, you simply extract the BgInfo.exe file to your computer and copy the file into the Startup folder. Each time the computer boots, the BgInfo program will gather information about the system and display it on the computer's desktop screen. BgInfo does a point-in-time snapshot at the time the system starts, instead of actively displaying live data. This allows BgInfo to display accurate and current information without using up precious system resources while the computer is running.

Customizing Displayed Data

When you launch the BgInfo.exe file the BgInfo Default Configuration screen displays. From this screen (see Figure 12.3), you can customize virtually every aspect of what information BgInfo will display and the look-and-feel of how the data will be displayed on the desktop.

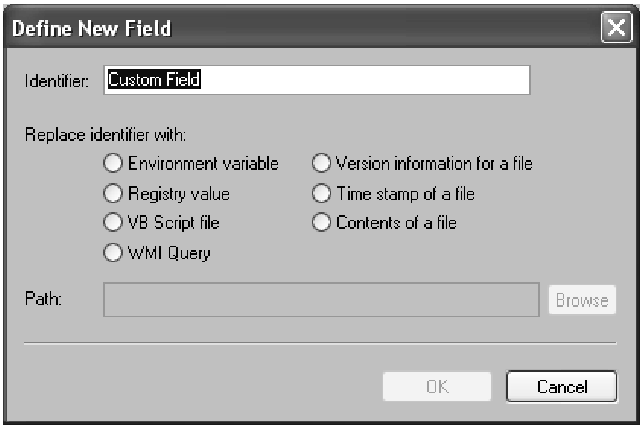
Figure 12.3 The BgInfo Default Configuration Screen



```
Boot Time:         <Boot Time>
CPU:               <CPU>
Default Gateway:   <Default Gateway>
DHCP Server:       <DHCP Server>
DNS Server:        <DNS Server>
Free Space:        <Free Space>
Host Name:         <Host Name>
IE Version:        <IE Version>
IP Address:        <IP Address>
Logon Domain:      <Logon Domain>
Logon Server:      <Logon Server>
MAC Address:       <MAC Address>
Machine Domain:    <Machine Domain>
Memory:            <Memory>
Network Card:      <Network Card>
Network Speed:     <Network Speed>
Network Type:      <Network Type>
OS Version:        <OS Version>
Service Pack:      <Service Pack>
```

You can delete fields from the view in the left pane, or add fields from the pane on the right. If the information you want to display is not defined, BgInfo allows you to define custom fields, as shown in Figure 12.4. With a custom field, you can display just about any piece of system information that is pertinent to you and that you want to have displayed on your Windows desktop for quick reference.

Figure 12.4 Creating a Custom Field



Define New Field

Identifier: Custom Field

Replace identifier with:

○ Environment variable ○ Version information for a file
○ Registry value ○ Time stamp of a file
○ VB Script file ○ Contents of a file
○ WMI Query

Path:

The BgInfo Default Configuration screen contains four buttons on the right-hand side to help you customize the BgInfo output. The first three buttons, Background, Position, and Desktops, allow you to modify BgInfo's various configuration settings. The fourth button, Preview, shows you how the BgInfo output will look with the chosen configuration. Table 12.1 provides more information about the three configuration buttons.

Table 12.1 Customization Options Using BgInfo Configuration Buttons

Option	Function
Background	Allows you to choose the color and/or wallpaper to use as the background for the BgInfo display. You can also select **Copy existing settings** to use the default wallpaper of the currently logged-in user.
Position	Lets you specify where on the screen the BgInfo data should display. It also has options to address issues with overlapping the taskbar, and to address how to handle multiple monitor display configurations.
Desktops	Lets you select which desktops should display the BgInfo data. By default, only the User Desktop wallpaper is affected, but you can also specify that users who log in via Terminal Services will also see the BgInfo display.

Configuring BgInfo Using the Menu Options

At the top of the BgInfo Default Configuration display are a series of menu options: File, Bitmap, Edit, Format, and Help. These options allow you to further configure and modify the way BgInfo works, and save the configuration file for future use.

TIP

By default, BgInfo will open to the BgInfo Default Configuration display each time you run it, and it will display a 10-second countdown timer before shutting down and displaying the BgInfo desktop. To bypass the default configuration, you must specify a configuration file when you launch BgInfo.

For example, instead of placing just **bginfo** into the computer's Startup folder, you would enter **bginfo MyConfig.bgi**.

Refer to Table 12.2 for complete information about the options available via the menu, and for information on how to use the options to configure BgInfo.

Table 12.2 BgInfo Menu Bar Configuration Options

Option	Function
File | Open	Lets you open a BgInfo configuration file (BGI).
File | Save As	Saves the current BgInfo custom configuration to a BGI file.
File | Reset Default Settings	Resets all configuration options to the original default settings.
File | Database	Allows you to specify an XLS, MDB, or TXT file to capture and store the information to which it generates.
Bitmap | 256 Colors	Limits the wallpaper bitmap image to 256 colors.
Bitmap | High Color	Creates a 16-bit color wallpaper image.
Bitmap | True Color	Creates a 24-bit color wallpaper image.
Bitmap | Match Display	Creates the BgInfo wallpaper using the color depth currently in use on the system.
Bitmap | Location	Specifies the location where BgInfo should save the resulting bitmap image.
Edit | Insert Image	Allows you to insert a bitmap image into the BgInfo output.

WARNING

To use the **File | Database** settings you must make sure that all systems that will access the file being used to store the data are using the same version of Microsoft Data Access Components (MDAC), and that JET database support is installed. Sysinternals recommends that you use at least MDAC 2.5 and JET 4.0. Also, note that if you choose XLS as the output type, you must create the XLS file in advance.

The Format button contains standard options for formatting the output of the BgInfo data. You can specify the font, size, and style of the output text, as well as the text color and alignment.

Designing & Planning…

Using BgInfo without Changing the Desktop

You can use BgInfo to display a wide variety of very useful information on the computer desktop. You can capture and display as part of your wallpaper such information as the CPU, host name, default gateway, amount of memory, operating system version, and service pack levels.

You also can capture this information to monitor machines over time, or to maintain a history of various aspects of the computer system. Using the **File | Database** settings, you can specify an output file to store the information BgInfo collects.

You can also use BgInfo for its information-gathering capabilities, without altering the wallpaper or displaying the data on the desktop. Simply customize BgInfo to collect the information you want to monitor, and choose an output file under **File | Desktops**. Then click on the **Desktops** button and deselect all of the desktops so that the BgInfo data will not display as a part of the wallpaper.

Running BgInfo from the Command Line

As great as BgInfo is for capturing and displaying data on the local computer, it provides even more value for network administrators and support technicians. BgInfo includes a number of command-line parameters that you can use to script the execution of BgInfo and customize its functionality and output to suit your needs. Table 12.3 explains the command-line options that you can use with BgInfo.

Table 12.3 Command-Line Options for Customizing the Launch of BgInfo

Option	Function
<path>	Specifies the location of a BGI (BgInfo configuration file) to use when BgInfo executes.
/timer	Sets the countdown timer for displaying the BgInfo Default Configuration screen prior to modifying the desktop. Specifying a time of 0 seconds will automatically update the display; specifying a time of 300 seconds or more will disable the timer.
/popup	Outputs BgInfo to a pop-up window, instead of directly to the desktop wallpaper. BgInfo will not save any information to a database when using the pop-up option.
/taskbar	Executes BgInfo as a button minimized to the taskbar. Clicking the button will display the BgInfo data in a pop-up window. No information is saved to a database when using the taskbar option.
/all	Directs BgInfo to change the desktop wallpaper for all users currently logged on to the system.
/log	Causes BgInfo to write error information to the specified log file, instead of displaying a system warning.
/rtf	Writes the BgInfo output text to an RTF file, retaining the formatting and colors of the actual BgInfo display.

Bypassing the Login Screen (Autologon)

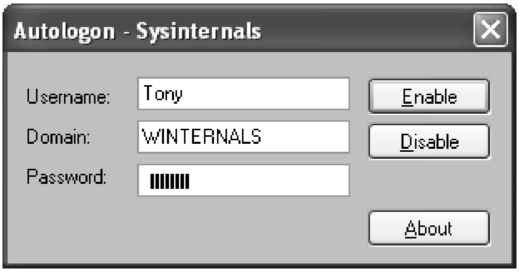
Network and security administrators should probably stop reading right here. From a management or administrator perspective, the Windows login screen provides a valuable and necessary function, ensuring that only those with the proper username and password credentials are able to gain access to the computer or the network resources to which it is attached. So, they probably don't want you to know how to skip right past that trivial annoyance.

The reality is that Windows actually enables users to bypass the login screen. However, doing so requires more knowledge of the Windows operating system and the inner workings of the Registry than most users possess. So, Sysinternals created a tool, called Autologon, which makes the Registry changes for you and allows you to prepopulate the username, domain, and password information to zip right past the login screen and straight to the Windows desktop.

Setting Up Autologon

After you download the Autologon tool from Sysinternals (www.sysinternals.com/Utilities/Autologon.html) and extract the files to a directory on your hard drive, you can double-click the **autologon.exe** file from within a Windows Explorer display or enter it at a command-line prompt to bring up the **Autologon** configuration screen (see Figure 12.5). Running the Autologon utility allows you to enter the necessary credentials and enable or disable the Autologon tool.

Figure 12.5 The Autologon Configuration Screen



Autologon - Sysinternals

Username: Tony

Domain: WINTERNALS

Password: ||||||||

Enabling and Disabling Autologon

As convenient as it may be to use Autologon, there may be times that you need to log in to the computer using different credentials. Regardless of the reason you want to turn Autologon off or on, there are a couple methods for both enabling or disabling the utility.

To enable Autologon and automatically bypass the user login screen, simply start the Autologon tool and enter the appropriate information. You will need to supply a valid username, domain, and password for Autologon to work. Once you enter the information, click **Enable**.

You can also skip the Autologon configuration screen by entering the username, domain, and password information at the command line when you launch Autologon. You simply enter the information in the following order from a command line:

```
autologon user domain password
```

If you want to skip the Autologon for a particular login, but you don't want to turn off the Autologon tool for future logins, you can hold down the **Shift** key while the system is booting to bypass the Autologon sequence. To disable Autologon indefinitely, launch the utility and click on the **Disable** button.

Summary

In this chapter, you learned that you don't have to be all work and no play, and that sometimes you can work and still have fun.

To start with, we talked about using the BlueScreen screensaver tool to embrace the dreaded Blue Screen of Death as a source of both humor and security. Selecting the BlueScreen screensaver produces a realistic-looking BSOD system crash and reboot sequence, while allowing you to password protect your system when you walk away from it.

You then learned about using the Ctrl2cap utility to alter the way the computer interprets the Caps Lock key from the keyboard. This tool mainly benefits classic Unix developers who are used to having a Ctrl key right where the Caps Lock key is located on Windows keyboards. Using Ctrl2cap reduces frustration and increases productivity for users who are in the habit of using that key location for Ctrl functions.

Next we played with a tool that lets you display important information about the computer system, or create custom fields to display virtually any system information you choose, right on the desktop wallpaper. You learned how to customize and configure the BgInfo tool as well as how to use command-line parameters to create scripts that you can use to automate the execution of BgInfo for users throughout a network, and you learned how to use BgInfo to capture and store system information without altering the desktop wallpaper.

The last tool we looked at in this chapter was the Autologon tool. You learned that you could use this handy utility to enter user credentials automatically and bypass the Windows login screen.

Solutions Fast Track

Generating a Blue Screen of Death on Purpose (BlueScreen)

☑ BlueScreen is a screensaver from Sysinternals that accurately mimics a BSOD system crash and reboot.

☑ To run BlueScreen on a Windows 9*x* machine, you have to copy the ntoskrnl.exe file from a Windows 2000 computer.

☑ BlueScreen will display different information depending on the operating system version it is running on, to make it realistic for that specific operating system.

Modifying the Behavior of the Keyboard (Ctrl2cap)

☑ The Ctrl2cap utility from Sysinternals allows you to modify the keyboard to treat the Caps Lock key as though it is a left Ctrl key.

☑ When you install and uninstall Ctrl2cap you must reboot the system reboot for the changes to take effect.

☑ The Ctrl2cap utility is written in a way that bypasses the need for installation through the Device Manager, but also will not warn you that the driver is not digitally signed by Microsoft.

Creating Useful Desktop Backgrounds (BgInfo)

☑ BgInfo is a useful tool that allows you to display a variety of information about the system on the desktop wallpaper.

☑ The BgInfo data is completely customizable.You can choose what information to display, where to display it, and what fonts, colors, and background wallpaper to use.

☑ You can run BgInfo using command-line parameters, allowing you to script BgInfo execution across all user desktops.

☑ You can output BgInfo data to a file for storage and future reference.

☑ You can use command-line options to automate the execution of BgInfo on user desktops using a login script.

Bypassing the Login Screen (Autologon)

☑ Windows contains the capability to bypass the user login screen, but it is buried deep in the Registry.

☑ You can use the Autologon tool from Sysinternals to easily modify the Registry so that you can bypass the user login screen.

☑ You can skip autologon for the current login instance by holding down the **Shift** key before the autologon sequence.

☑ You also can run Autologon from the command line by supplying the necessary information as command-line options.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to www.syngress.com/solutions and click on the "Ask the Author" form.

Q: How can I trick my friends into thinking that my system is crashing?

A: The BlueScreen screensaver from Sysinternals simulates a very realistic Blue Screen of Death system crash, complete with accurate information from the computer on which it is running, and automatic system reboots. Mouse movements will not wake up the screensaver, but clicking any key on the keyboard will stop the screensaver and return it to regular operation.

Q: Can I use BlueScreen with my Windows 98 computer?

A: The BlueScreen screensaver works with Windows 9*x* operating systems, but it requires access to ntoskkrnl.exe in order to run. You have to copy the ntoskrnl.exe file from a Windows 2000 machine into your \Windows\System directory in order for BlueScreen to work on a Windows 9*x* computer.

Q: How can I get my Caps Lock key to work like normal again after installing Ctrl2cap?

A: To remove Ctrl2cap, you just need to open a command prompt window to the directory where the Ctrl2cap files are located, type **ctrl2cap /uninstall**, and then reboot the system.

Q: Can I view information other than the fields to which BgInfo defaults?

A: BgInfo comes with predefined fields that will fit most users' needs. However, BgInfo also allows you to create custom fields to display virtually any piece of information you choose on the BgInfo desktop.

Q: Can I gather information with the BgInfo tool without modifying the wallpaper?

A: Yes. By choosing to output BgInfo information to a database file, but deselecting all desktop display options within BgInfo, you will gather and save the information, but it will not display on any desktop wallpaper.

Q: Is there a way to skip the Windows login screen?

A: Home computer users may be used to their systems going straight to the desktop, or to a Welcome screen with icons to click to log in. However, corporate network users are generally forced to use the three-finger salute (**Ctrl+Alt+Del**) to access the user logon screen, and they must enter a valid domain username and password to gain access. The Autologon tool from Sysinternals lets users preenter the user credential information and log in automatically, bypassing the initial login screen.

Q: Can I use the Autologon tool from a command prompt?

A: Yes. If you launch Autologon from a command line, you can also supply the user credential information as command-line arguments to allow Autologon to run without asking for the user information.