

Microsoft®
Desktop Optimization Pack
for Software Assurance

Microsoft®
Diagnostics and
Recovery Toolset

Diagnostics and Recovery Toolset Overview

Technical White Paper

Published: November 2011

By Niamh Coleman, Craig Ashley, and Jeff Gilbert

Microsoft®

CONTENTS

Executive Summary	3
Introduction	4
Creating the DaRT Media	5
Deploying the DaRT Media	7
Exploring the DaRT Tools	9
Registry Editor	9
Locksmith	10
Crash Analyzer	11
File Restore	12
Disk Commander	13
Disk Wipe	14
Computer Management	15
Explorer	16
Solution Wizard	17
TCP/IP Configuration	17
Hotfix Uninstall	18
System File Repair Wizard	19
Search	19
Standalone System Sweeper	20
Using Remote Connection	21
Evaluating DaRT	24
For More Information	25

Situation

Diagnostics and Recovery Toolset (DaRT) reduces time spent and challenges associated with troubleshooting and repairing system failures on Windows-based PCs. DaRT helps IT teams make PCs safer to use, keeps employees productive, and makes desktops easier and less expensive to manage.

Solution

DaRT allows administrators to easily recover unusable PCs, rapidly diagnose probable causes of issues, and quickly repair unbootable or locked-out systems, all without users leaving their PCs—and much faster than the average time it takes to reimagine the machine.

To learn more about how DaRT and MDOP for Software Assurance can help your organization, see: <http://go.microsoft.com/fwlink/?LinkId=160297>.

Benefits

Cost savings through reduced downtime

- Recover instead of reload or reimage Windows
- Boot DaRT remotely removing "in-transit" time lost for users in remote locations
- Recover deleted files, or reset lost or forgotten passwords
- Make PCs safer to use by detecting and removing malware while the PC is offline

Accelerated IT Responsiveness and Streamlined PC Manageability

- Pick the best deployment option : USB, DVD, CD, local drive, network based, and remote boot
- Manage user access rights, allowing the right users to use only the right tools

Products & Technologies

- Microsoft Diagnostics and Recovery Toolset
- Microsoft Desktop Optimization Pack for Software Assurance

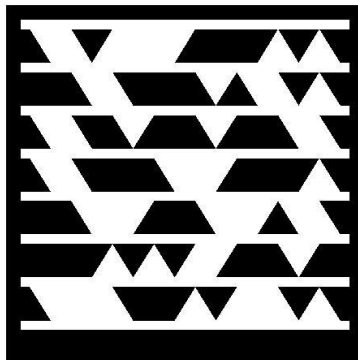
EXECUTIVE SUMMARY

By providing tools that help you quickly troubleshoot and repair Windows-based desktops, Microsoft Diagnostics and Recovery Toolset (DaRT) can reduce the time, cost, and frustration associated with recovering computers that will not boot. DaRT 7.0 includes new features to simplify deployment and troubleshoot systems remotely while limiting local access to the tools. This white paper gives an overview of DaRT—its benefits, its capabilities, and how to evaluate it.

Note: For security reasons, the sample names of forests, domains, internal resources, organizations, and internally developed security file names used in this paper do not represent real resource names used within Microsoft and are for illustration purposes only.

Microsoft Tag 2D barcode symbols, like the one shown here, appear throughout this guide and let you connect to supplemental material online using a mobile phone.

For example, you can use a tag reader application installed on your mobile phone to scan this Microsoft Tag (or go to <http://go.microsoft.com/fwlink/?LinkId=232274>) to connect to the download page for this white paper:



Note: To get the Tag Reader, visit <http://gettag.mobi> on your mobile phone browser. Or, visit <http://tag.microsoft.com/consumer/index.aspx> to send a text message to your phone with a link to the application.

Microsoft Tag is also available for free in most mobile application stores; just search for „Tag Reader“ to get started.

INTRODUCTION

A user frantically calls support, and your manager sends you to fix the problem. At the user's desk, you log on to the Windows operating system and use the variety of tools that are available for troubleshooting. You look in Event Viewer for clues about the problem. You determine that the problem is a faulty device driver, and so you use the Computer Management console to disable that driver. Windows includes many such tools to help you diagnose and fix problems. However, what do you do if you cannot boot the computer into Windows?

The [Microsoft Desktop Optimization Pack](#) (MDOP) for Software Assurance can help organizations reduce the cost of deploying applications, deliver applications as services, and better manage desktop configurations. Together, the MDOP applications that Figure 1 shows can give Software Assurance customers a highly cost-effective and flexible solution for managing desktop computers.






Microsoft Desktop Optimization Pack	
 Microsoft Advanced Group Policy Management	AGPM provides governance and control over Group Policy through robust change management and role-based administration.
 Microsoft Application Virtualization	App-V turns applications into centrally managed services that are never installed, never conflict, and are streamed on demand to end users.
 Microsoft Asset Inventory Service	AIS is a hosted service that collects software inventory data and translates it into business intelligence.
 Microsoft BitLocker Administration and Monitoring	MBAM can help organizations simplify provisioning and deployment, improve compliance and reporting, and reduce support costs for BitLocker Drive Encryption.
 Microsoft Diagnostics and Recovery Toolset	DaRT reduces downtime by accelerating desktop repair, recovery, and troubleshooting of unbootable Windows-based desktops.
 Microsoft Enterprise Desktop Virtualization	MED-V provides deployment and management of virtual PC images to enable key enterprise scenarios, primarily application compatibility with Windows Vista and Windows 7.

Figure 1. Microsoft Desktop Optimization Pack

To help recover Windows-based desktops that will not boot, MDOP offers the Microsoft Diagnostics and Recovery Toolset (DaRT). DaRT is a powerful set of tools that extend the Windows Recovery Environment (Windows RE). With DaRT, you can analyze an issue to determine its source, view the computer's event log for more clues, disable a faulty device driver, and remove hotfixes even when you cannot start the installed Windows operating system. Additionally, DaRT includes tools that enable you to troubleshoot the installed Windows operating system when starting Windows would not be prudent. For example, you can restore deleted files and sweep the computer for malware.

DaRT can help you quickly recover computers running both 32-bit and 64-bit versions of Windows, in less time and with less frustration than reimaging them. Additionally, DaRT 7.0 offers flexible deployment options, and you can troubleshoot computers remotely while limiting local users' access to the tools. This white paper describes the tools that DaRT provides and how you can evaluate DaRT today.

“The cost of not having an effective diagnostics and recovery plan in place was devastating. All of this has been resolved and we reduced overall costs by 10 percent by using a unified tool suite.”

Ram Reddy P.
Manager of IT,
Aurobindo Pharma

CREATING THE DART MEDIA

DaRT provides a wizard that you use to create custom boot media, based on the Windows RE and a set of tools that DaRT provides. This boot media starts the Windows RE, from which you can start the DaRT tools.

You use the DaRT Recovery Image Wizard to create the DaRT boot media. To start the wizard, click Start, All Programs, Microsoft DaRT 7, DaRT Recovery Image. The DaRT Recovery Image Wizard will ask for the following:

- **Boot image.** The Windows 7 or Windows Server 2008 R2 boot image contains the Windows RE. You must use the x86 version of Windows to build 32-bit DaRT boot media. Likewise, use the x64 version of Windows to build 64-bit DaRT boot media.
- **Tool selection.** By default, the wizard enables all DaRT tools for the local user. However, you can disable some or all of the tools for the local user while allowing the help desk full access to them. For example, you can disable potentially destructive tools for the local user, as Figure 2 shows, while the help desk maintains full access to them (see “Connecting to DaRT Remotely”).

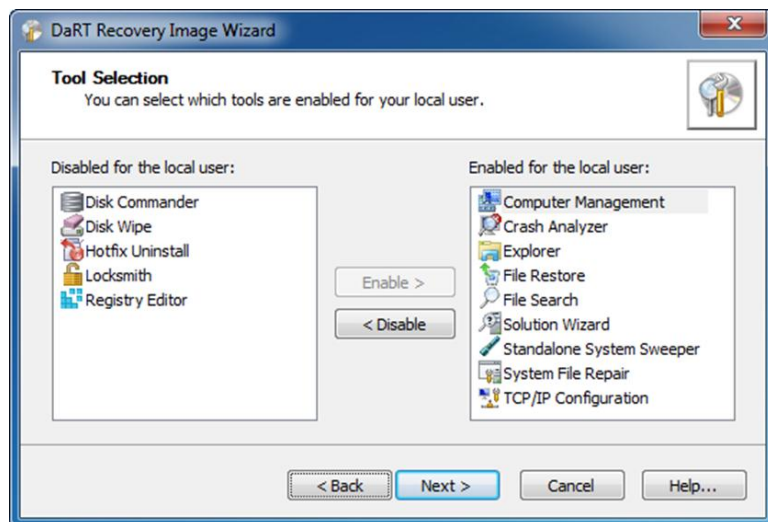


Figure 2. Tool Selection in the DaRT Recovery Image Wizard

- **Remote connections.** Remote Connection is a new feature in DaRT 7.0. Using Remote Connection, the help desk can connect to end users' computers by using Remote Connection Viewer and use the DaRT tools to troubleshoot and repair their computers. As Figure 3 shows, when you enable remote connections, you can also specify a port number and a welcome message. If you do not specify a port number, Remote Connection will assign a random port number. For more information about Remote Connection, see “Connecting to DaRT Remotely,” later in this white paper.

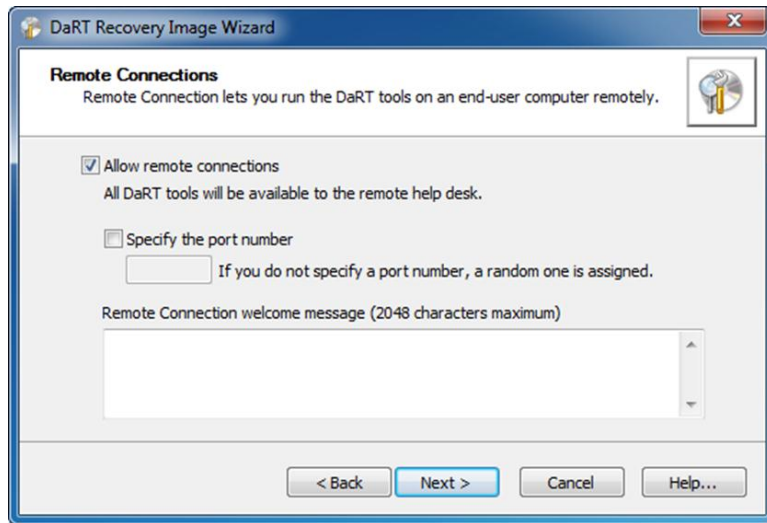


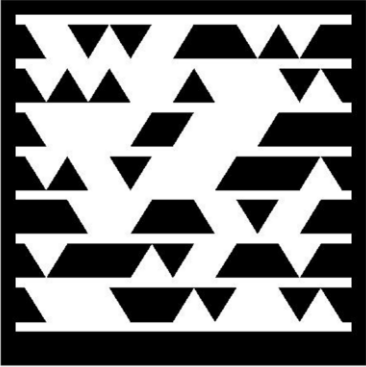
Figure 3. Remote Connections in the DaRT Recovery Image Wizard

- **Debugging Tools for Windows.** The Crash Analyzer in DaRT relies on the Debugging Tools for Windows. (Download them from <http://go.microsoft.com/fwlink/?LinkId=99934>.) You can install these tools on the computer that you are using to create the DaRT boot media, including them on the media, or you can install them on each computer that you repair. Microsoft recommends including the Debugging Tools for Windows on the DaRT boot media.
- **Standalone System Sweeper definitions.** You can download the most recent malware definitions from the Internet, or you can manually download them later. Microsoft recommends downloading the most recent malware definitions from the Internet and including them on the boot media. You can always download updated definitions when you use the media later.
- **Additional drivers.** You can add device drivers that the boot image does not include.
- **Additional files.** You can add additional files to the DaRT boot media by copying them to the image before creating the .iso file. For example, you can add troubleshooting scripts to the media or edit the Windows RE configuration files.

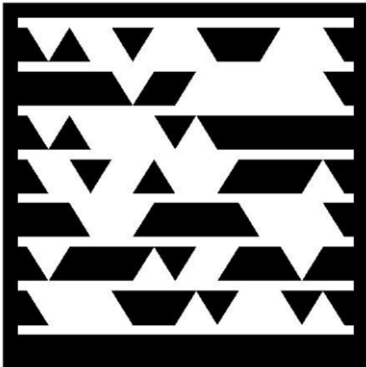
At its completion, the DaRT Recovery Image Wizard prompts you for the location and name of the image file to create. By default, the wizard creates the file DaRT70.iso on your desktop. The wizard also prompts you to burn this image to a CD, but you can deploy it in a variety of ways (see the section titled “Deploying the DaRT Media”).

DaRT supports Windows 7 and Windows Server 2008 R2, and it has minimal hardware requirements. Both x86 and x64 versions are available. However, DaRT does not support cross-platform boot media.

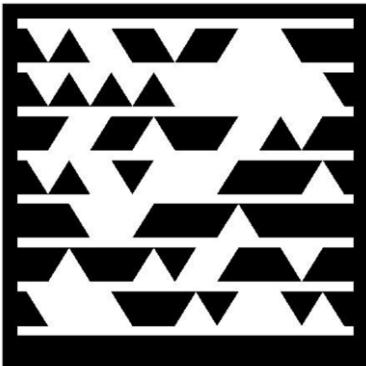
Use your mobile phone to scan the following Microsoft Tag or go to <http://go.microsoft.com/fwlink/?LinkId=232295> to view the Deploying DaRT Locally video:



Use your mobile phone to scan the following Microsoft Tag or go to <http://go.microsoft.com/fwlink/?LinkId=232298> to view the Deploying DaRT with the MDT video:



Use your mobile phone to scan the following Microsoft Tag or go to <http://go.microsoft.com/fwlink/?LinkId=232299> to view the Deploying DaRT with WDS video:

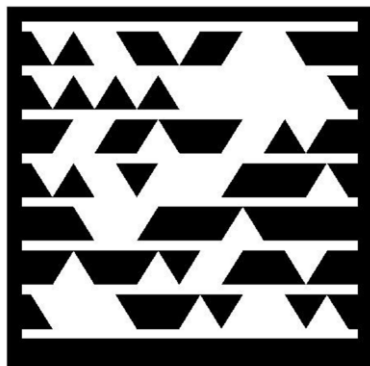


DEPLOYING THE DaRT MEDIA

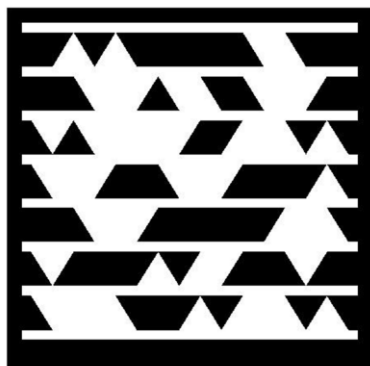
A new capability in DaRT 7.0 is the variety of supported ways you can now deploy the DaRT recovery image. Based on the Windows RE, the DaRT recovery image is a Windows Preinstallation Environment (Windows PE) image. As a result, you can generally deploy the DaRT recovery image using the same tools and techniques you use to deploy Windows RE or Windows PE boot images, including:

- **Local installation.** By installing the DaRT recovery image locally, users can start it by pressing F8 to display the Advanced Boot Options menu, and then choosing Repair Your Computer. Optionally, you can configure a hotkey that users can press to start DaRT when the computer boots. You use the tool Reagentc.exe, which Windows 7 includes in the box, to install DaRT locally.
- **Operating system imaging tools.** You can deploy the DaRT recovery image by using Microsoft System Center Configuration Manager 2007 or the Microsoft Deployment Toolkit 2010 (MDT 2010). The process automates local installation of DaRT tools on each system by using Reagentc.exe.
- **Windows Deployment Services.** To deploy the DaRT recovery image by using Windows Deployment Services (Windows DS), you extract the boot.wim file from the DaRT recovery image and add it to the list of available boot images. Deployment via Windows DS can be the quickest and simplest way to make the DaRT recovery image available to connected users in production.

Use your mobile phone to scan the following Microsoft Tag or go to <http://go.microsoft.com/fwlink/?LinkId=232297> to view the Deploying DaRT on USB Flash Disks video:



Use your mobile phone to scan the following Microsoft Tag or go to <http://go.microsoft.com/fwlink/?LinkId=232296> to view the Deploying DaRT on Disc video:



- **USB flash disks.** Creating a USB flash disk containing the DaRT image is straightforward. You make a bootable flash disk and copy the DaRT recovery image to it. Microsoft offers a free tool called the [Windows 7 USB/DVD Download Tool](#) that can make short work of this process.

- **Removable discs.** Of course, DaRT has always supported burning the recovery image to CDs or DVDs. However, the alternatives now supported are far simpler and more convenient.

After you start a computer by using the DaRT boot media, Windows RE asks a few simple questions to initialize the environment. These include whether to initialize network connectivity in the background by using DHCP (you can manually configure network connectivity later by using the TCP/IP Config tool), which drive letters map to the Windows operating system that you are repairing, and which language and keyboard you want to use. Finally, you choose the Windows operating system to repair.

After preparing the environment, you see the System Recovery Options window, which Figure 4 shows. Clicking **Microsoft Diagnostics and Recovery Toolset** opens DaRT.

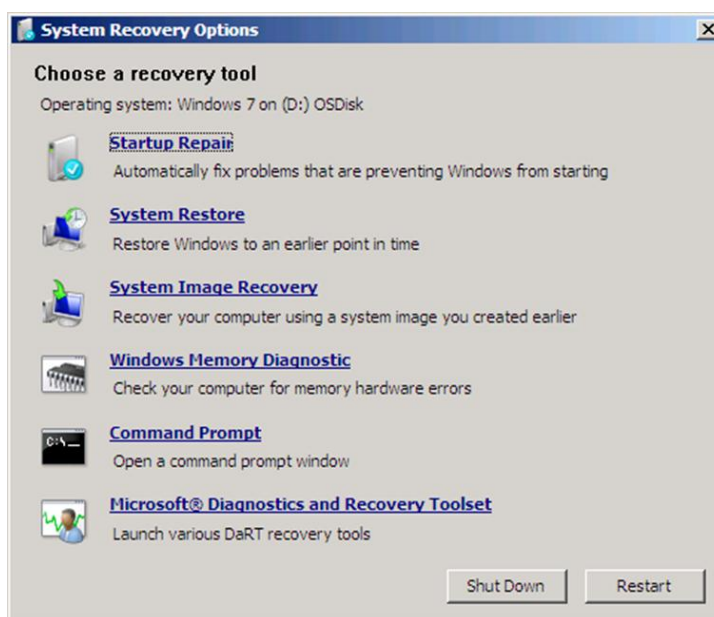


Figure 4. System Recovery Options

EXPLORING THE DART TOOLS

Figure 5 shows DaRT. From this window, you can launch any of the individual tools that you enabled in the DaRT recovery image. You can also use the Solution Wizard to choose the best tool, based on a brief interview. Click Help to see detailed instructions for using each tool. The following sections provide an overview of each tool.

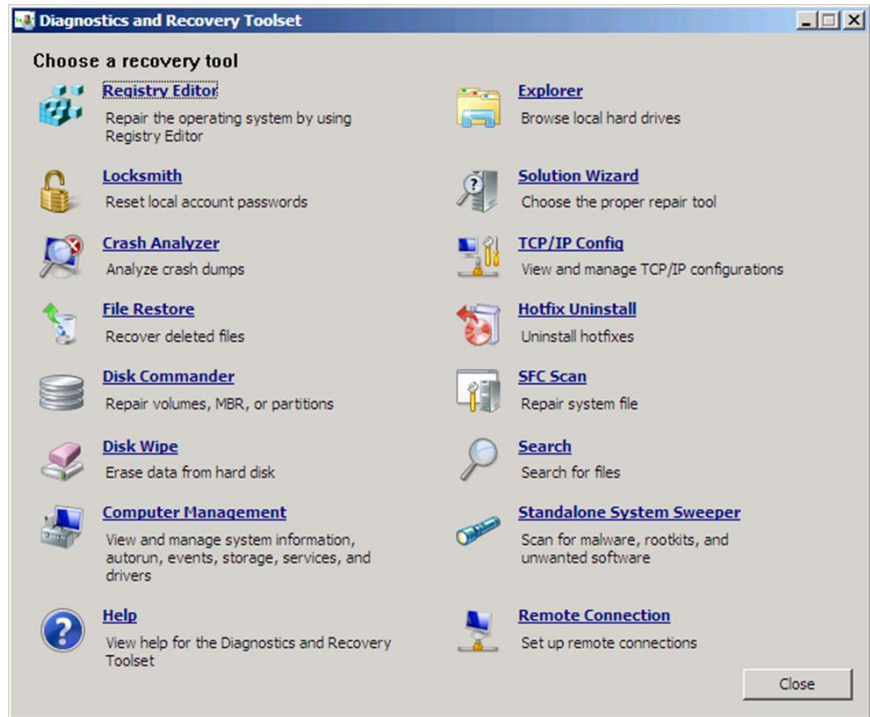


Figure 5. Tools in DaRT

Registry Editor

You can use Registry Editor, which Figure 6 shows, to edit the registry of the Windows operating system that you are repairing. Tasks include adding, removing, and editing keys and values and importing .reg files.

Registry Editor enables you to make registry edits that could help repair a system that will not boot. Additionally, you can use Registry Editor to edit values that the installed Windows operating system locks while it is running.

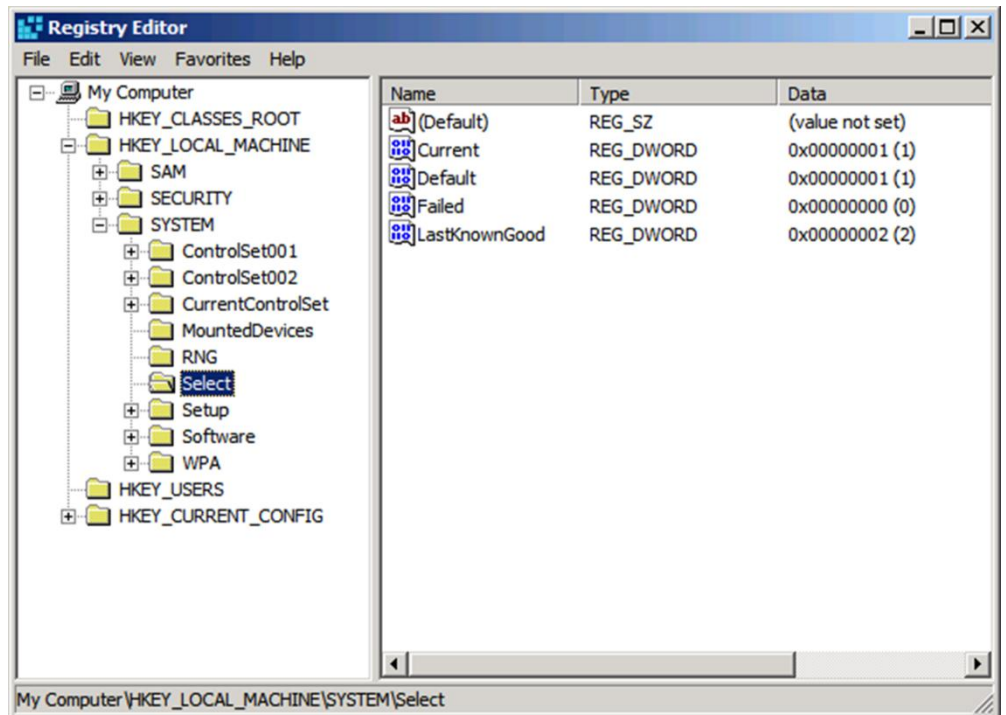


Figure 6. Registry Editor

Notice in Figure 6 that HKEY_CURRENT_USER is missing, because a user did not log on to the installed operating system. Instead, Registry Editor populates HKEY_USERS with all the user hive files found in the target installation. Additionally, HKEY_LOCAL_MACHINE does not contain a HARDWARE key.

Warning: *Serious problems might occur if you modify the registry incorrectly by using Registry Editor. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.*

Locksmith

The Locksmith Wizard is a simple tool that allows you to set the password for any local account on the Windows operating system that you are repairing, as Figure 7 shows. You do not need to know the current password. However, the password you set must comply with any requirements that a local Group Policy object (GPO) defines, including password length and complexity. Use this tool in the event that the password for a local account, such as the local Administrator account, is unknown. This tool cannot set passwords for domain accounts.

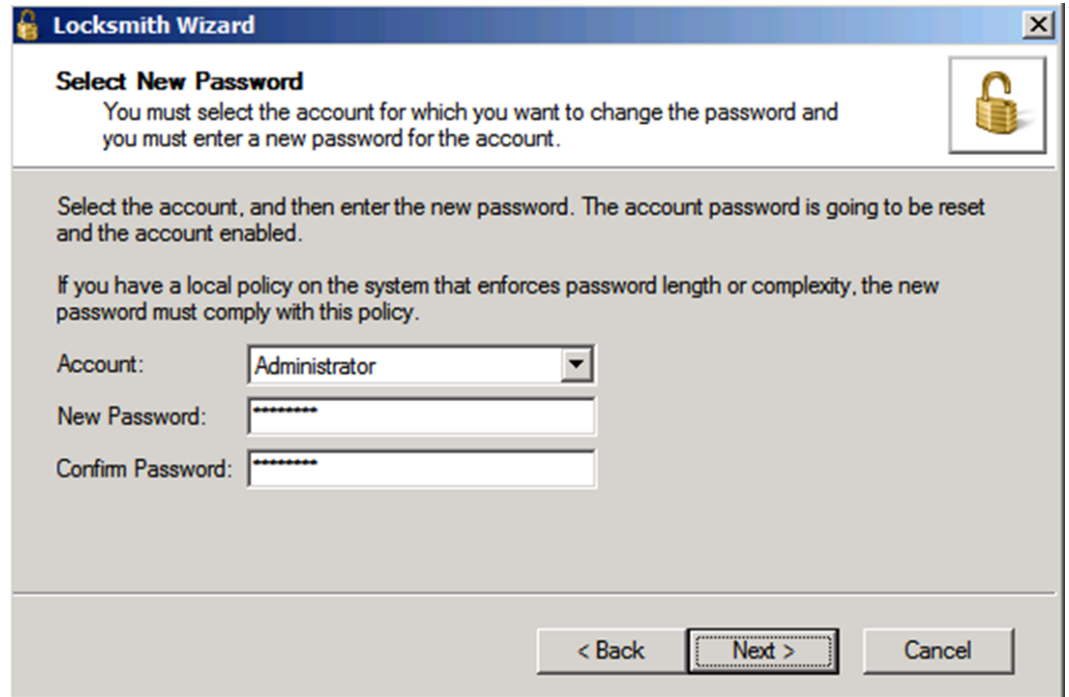


Figure 7. Locksmith Wizard

Crash Analyzer

By using the Crash Analyzer wizard, you can quickly determine the cause of an issue by analyzing the memory dump file on the Windows operating system that you are repairing. Based on this information, you can take corrective action. The Crash Analyzer wizard can eliminate much of the guesswork involved in diagnosing systems that will not boot.

For example, if the Crash Analyzer wizard reports that a device driver called `myfault.sys` is the cause, as Figure 8 shows, you can disable the device driver by using the Services and Drivers item in Computer Management (see the “Computer Management” section). After discovering and disabling the faulty device driver, you can try to start the repaired Windows operating system.

The Crash Analyzer wizard requires the Debugging Tools for Windows. As described in the “Creating the DaRT Media” section, you can include the Debugging Tools for Windows in the DaRT boot media or you can install them on each computer that you are repairing. Microsoft recommends that you include the tools in the DaRT boot media. Otherwise, you must locate the Debugging Tools for Windows each time you use the Crash Analyzer wizard to diagnose a computer that is not responding.

In addition to the Debugging Tools for Windows, the Crash Analyzer wizard requires symbol files for the operating system that you are repairing. Symbol files map memory addresses to names, helping to provide meaningful information for troubleshooting. You can include the symbol files on your DaRT boot media, or you can download the symbol files when you use the Crash Analyzer wizard to repair a computer (in which case, an Internet connection is required while troubleshooting).

Even if you plan to reimage the computer, running the Crash Analyzer wizard to determine the cause of the issue is a good idea. The image might have a bad driver that is causing intermittent problems in your environment, and the Crash Analyzer wizard can help you see these patterns and improve its stability.

Note: *If you do not have access to symbols or the Debugging Tools for Windows on the computer that you are repairing, you can copy the memory dump file to another computer and use the standalone version of the Crash Analyzer wizard to diagnose the issue. By enabling you to analyze memory dump files remotely, this tool is also useful when you are diagnosing an issue that does not prevent Windows from starting. To run the standalone version of the Crash Analyzer wizard on the computer that contains DaRT, click **Start, All Programs, Microsoft DaRT 7, Crash Analyzer**.*

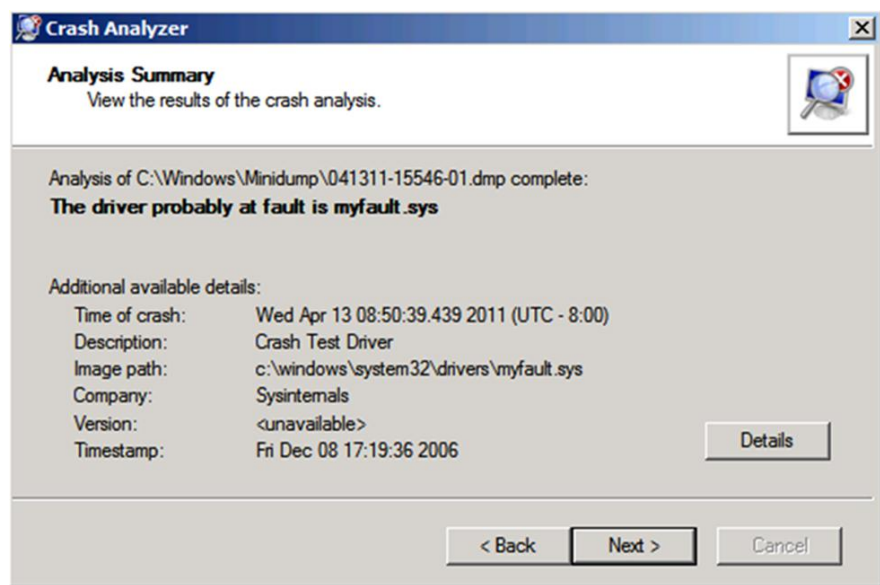


Figure 8. Crash Analyzer

File Restore

In Windows, the Recycle Bin helps prevent users from permanently deleting files by mistake. However, users sometimes realize that they need a particular deleted file only after emptying the Recycle Bin. In other cases, files are too big to fit in the Recycle Bin, or an application deletes the files.

File Restore enables you to attempt to restore such deleted files. Figure 9 shows the File Restore user interface. First, you must find the file you want to restore; File Restore has filtering capabilities to help expedite this process. For instance, you can use a file mask to search for specific file-name patterns. Additionally, you can limit results to a certain path, date range, or size range. File Restore can even find files in deleted directories. For each file that File Restore finds, it indicates whether recovery is likely or unlikely.

File Restore is not limited to regular disk volumes. File Restore can find and restore files on lost volumes or on volumes that are encrypted by Windows [BitLocker Drive Encryption](#). In the

first case, File Restore can scan for and locate lost volumes, which you can then search for deleted files. In the second case, File Restore gives you the ability to unlock BitLocker-encrypted volumes by manually providing the recovery password or loading the recovery key from a file.

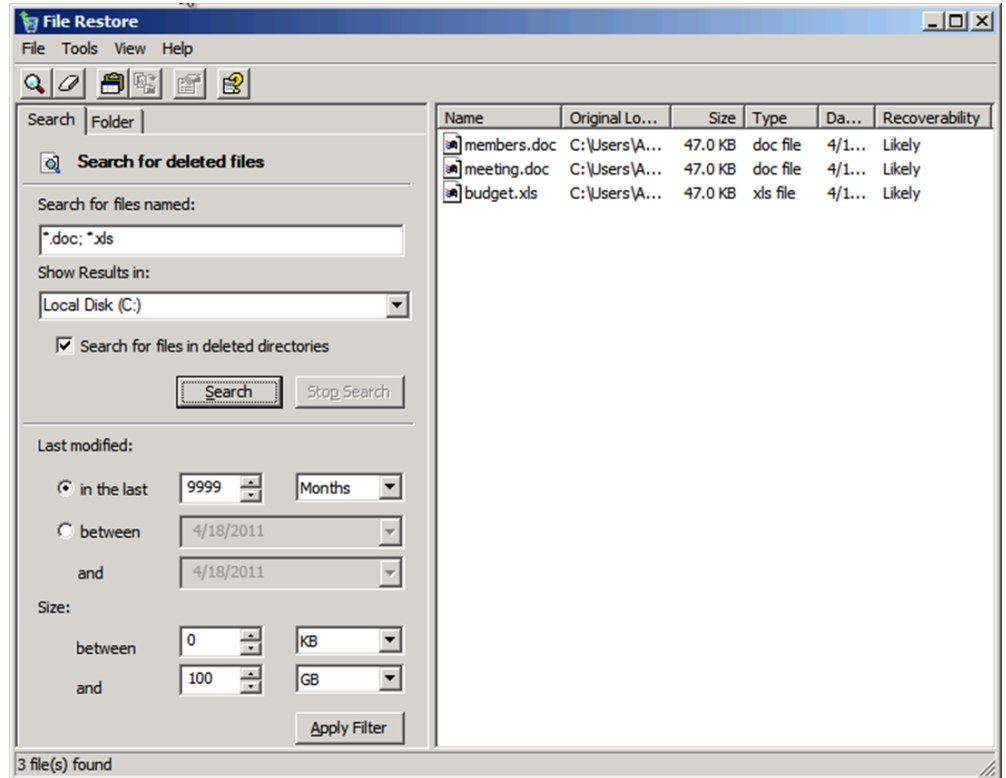


Figure 9. File Restore

Disk Commander

By using Disk Commander, you can recover and repair disk partitions or volumes. As Figure 10 shows, you can choose from the following recovery processes:

- **Restore the Master Boot Record (MBR).** This option repairs damaged boot code in the MBR on a disk, without affecting existing partition tables.
- **Recover one or more lost volumes.** This option scans a disk for lost volumes and allows you to recover them.
- **Restore partition tables from Disk Commander backup.** This option restores partition tables from a backup. Disk Commander gives you the opportunity to back up partition tables before making changes.
- **Save partition tables to Disk Commander backup.** This option backs up partition tables. The backup includes partition table entries and boot sectors for each partition.

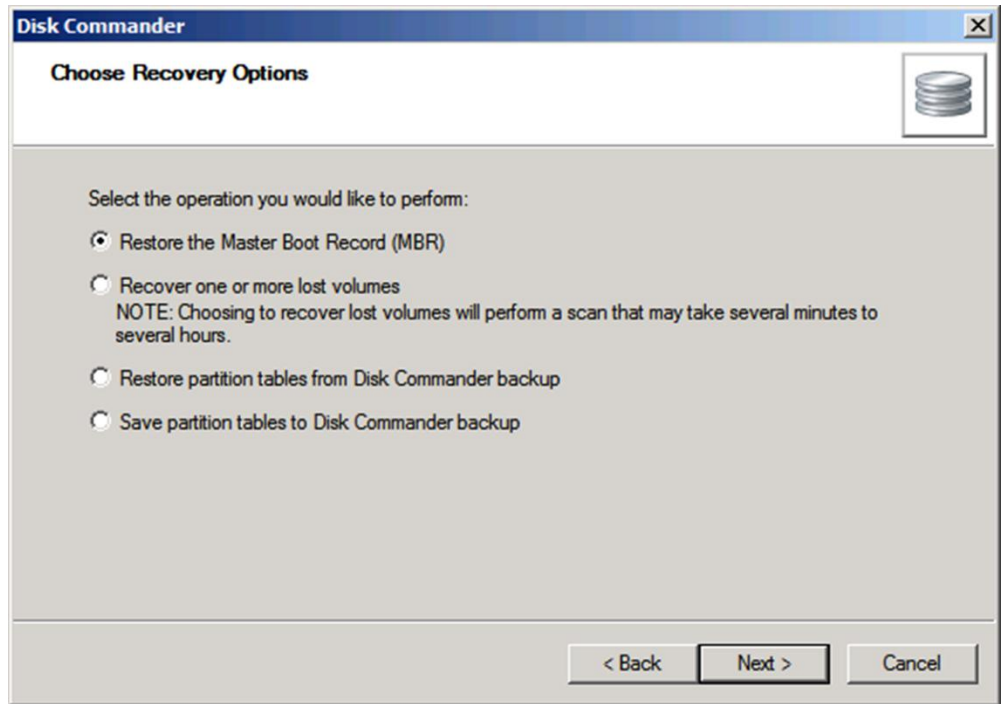


Figure 10. Disk Commander

Warning: *Microsoft recommends that you back up a disk before using Disk Commander to repair it. By using Disk Commander, you can potentially damage volumes and make them inaccessible. Additionally, changes to one volume can affect other volumes because volumes on a disk share a partition table.*

Disk Wipe

Many organizations simply format computers' hard disks when they donate, recycle, or discard them. However, just formatting the hard disk might not destroy sensitive company or personal data on that disk. As various news accounts have shown, malicious users can get their hands on computers that companies discard and can recover sensitive data.

Disk Wipe, which Figure 11 shows, can erase all data from a disk or volume. Two algorithms are available: You can use a single-pass overwrite or four-pass overwrite, the latter of which meets U.S. Department of Defense standards. After wiping a disk or volume, you cannot recover the data. Thus, verify the size and label of a volume before erasing it.

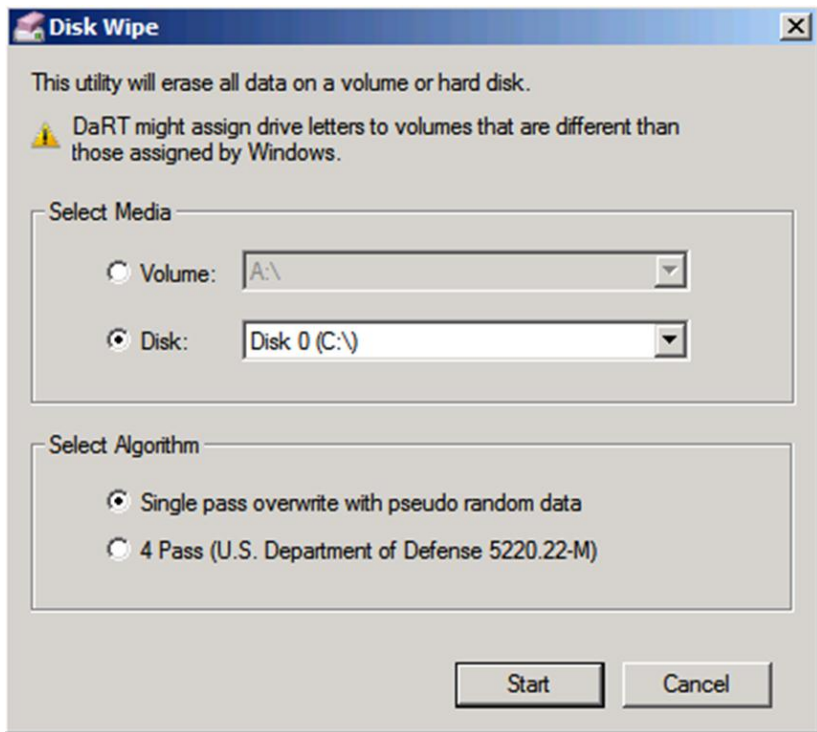


Figure 11. Disk Wipe

Computer Management

The Computer Management console, which Figure 12 shows, is familiar to any information technology (IT) professional. The console is tailored to diagnose and repair problems that can prevent the Windows operating system from booting. The items in this console include the following:

- **System Information.** This item displays information about the system that you are repairing. Information includes the Windows operating system version, registered owner and organization, the computer name as known by the installed operating system, and the computer name that DaRT randomly assigned to the system.
- **Event Viewer.** This item enables you to view the event logs of the Windows operating system that you are repairing. You can use the Event Viewer to look for entries that can help you diagnose the problem.
- **Autoruns.** This item configures the programs that start automatically when the operating system starts. By using Autoruns, you can stop a program from starting automatically when you suspect that the program is preventing the Windows operating system from starting.
- **Services and Drivers.** This item manages the services and device drivers that start when the target Windows operating system starts. For every service and device driver, you see an entry that indicates its startup type, a description, a display name, and so on. You can change the startup type to Boot, System, Automatic, Disabled, or Delayed Auto-start. If you have identified a service or device driver that is preventing the operating system from starting, you can disable it here.
- **Disk Management.** This item displays drive information, creates new partitions or volumes, and formats drives. Disk Management in DaRT is similar to Disk Management in the Windows operating system.

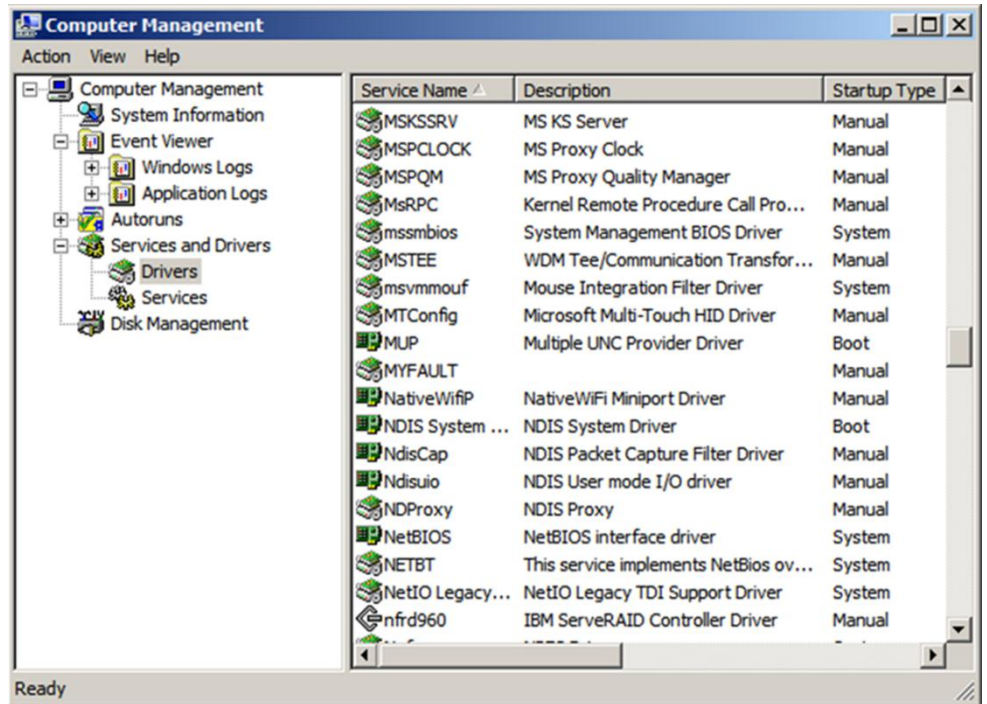


Figure 12. Computer Management

Explorer

Sometimes, before you attempt to repair or reimage a system, you need to remove business-critical information that the user stored on a local drive. In DaRT, you can use Explorer to browse the computer's file system and network shares. Because you can map drive letters to network shares, you can easily copy and move files from the system to the network for safekeeping or from the network to the system to restore them. Figure 13 shows Explorer.

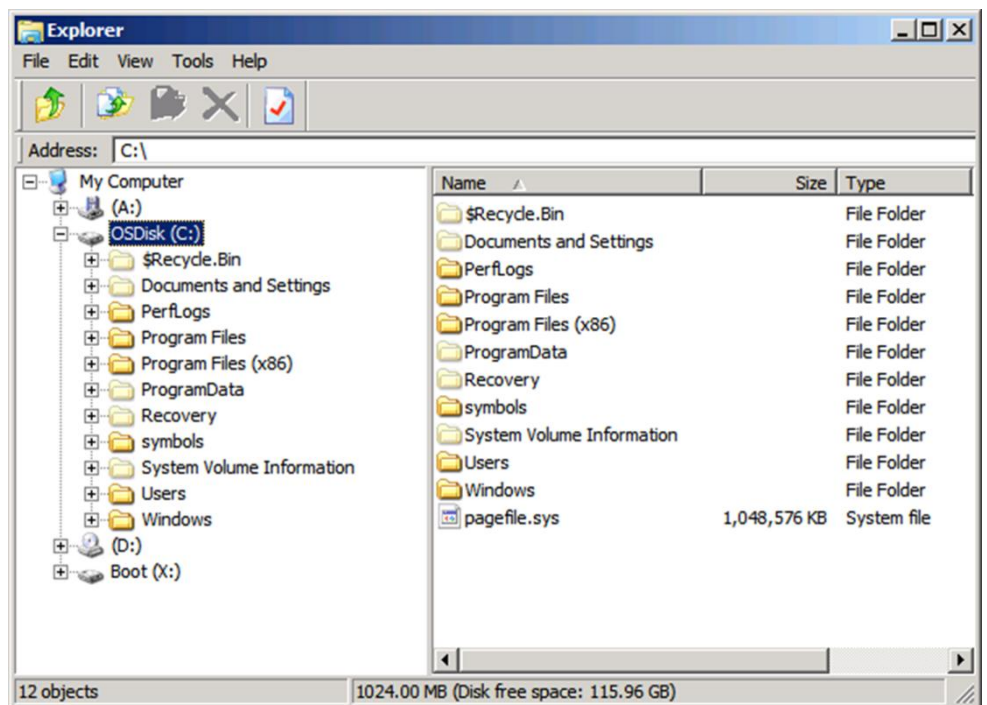


Figure 13. Explorer

Solution Wizard

DaRT has many tools, and figuring out which one to use can sometimes be challenging. The Solution Wizard, which Figure 14 shows, asks you a series of questions and then recommends the best tool for the job, based on your answers. This wizard helps you determine which tool to use when you are not familiar with the tools in DaRT. After becoming familiar with DaRT, you are more likely to start the correct tool for each job, without the help of the Solution Wizard.

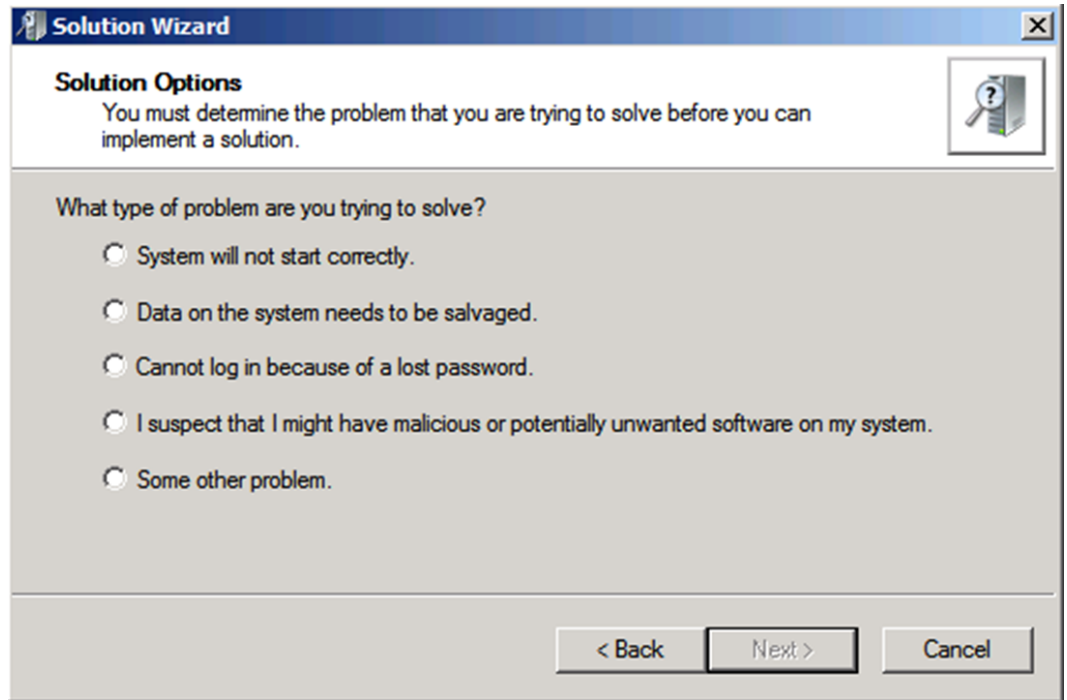


Figure 14. Solution Wizard

TCP/IP Configuration

When you start the DaRT boot media, it optionally obtains its TCP/IP configuration (IP address and DNS server) from DHCP. If DHCP is unavailable, you can manually configure TCP/IP by using the TCP/IP Configuration tool, which Figure 15 shows. First, you choose a network adapter, and then you configure the IP address and DNS server for that adapter. Click Advanced to configure advanced TCP/IP settings.

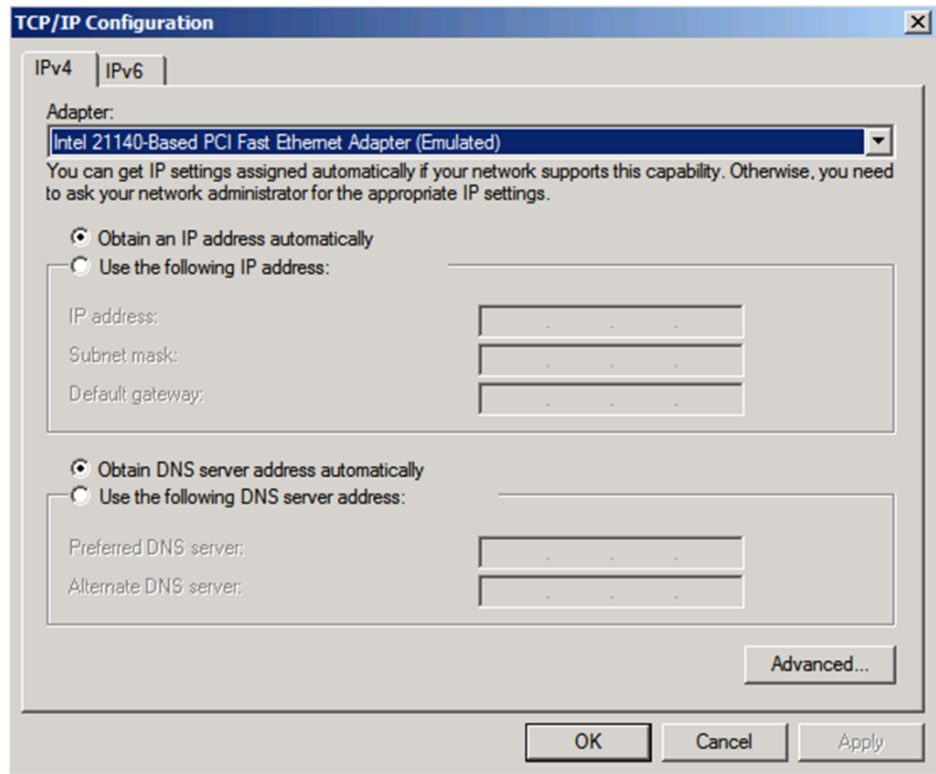


Figure 15. TCP/IP Configuration

Hotfix Uninstall

The Hotfix Uninstall Wizard, which Figure 16 shows, can remove hotfixes or service packs from the Windows operating system that you are repairing. Use this tool when a hotfix or service pack is potentially preventing the operating system from starting. Microsoft recommends that you use this tool to uninstall only one hotfix at a time, even though the tool allows you to uninstall more than one at a time. Be aware that programs that you have installed or updated after installing the hotfix might not work correctly after you uninstall it.

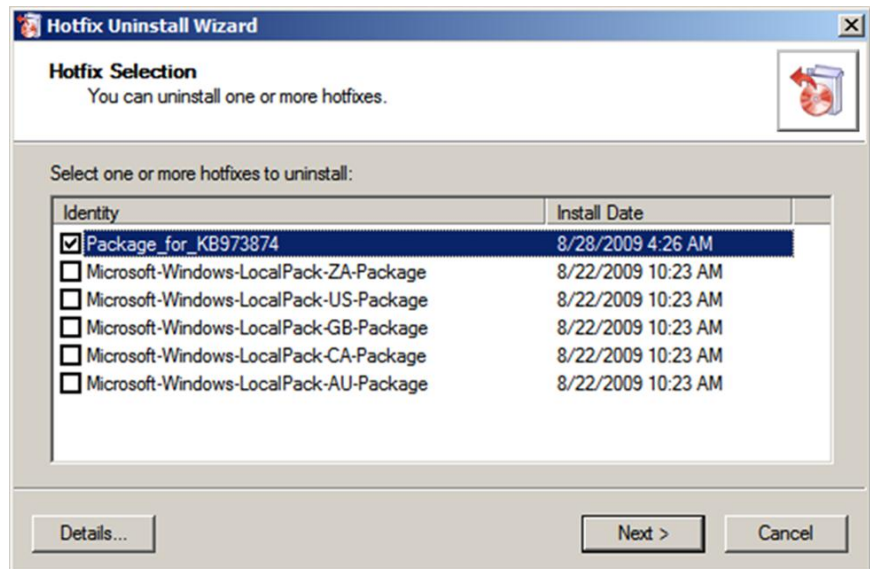


Figure 16. Hotfix Uninstall Wizard

System File Repair Wizard

Use the System File Repair Wizard to repair system files that are preventing the installed Windows operating system from starting. The System File Repair Wizard can automatically repair system files that are corrupted or missing. Alternatively, the wizard can prompt you before performing any repairs.

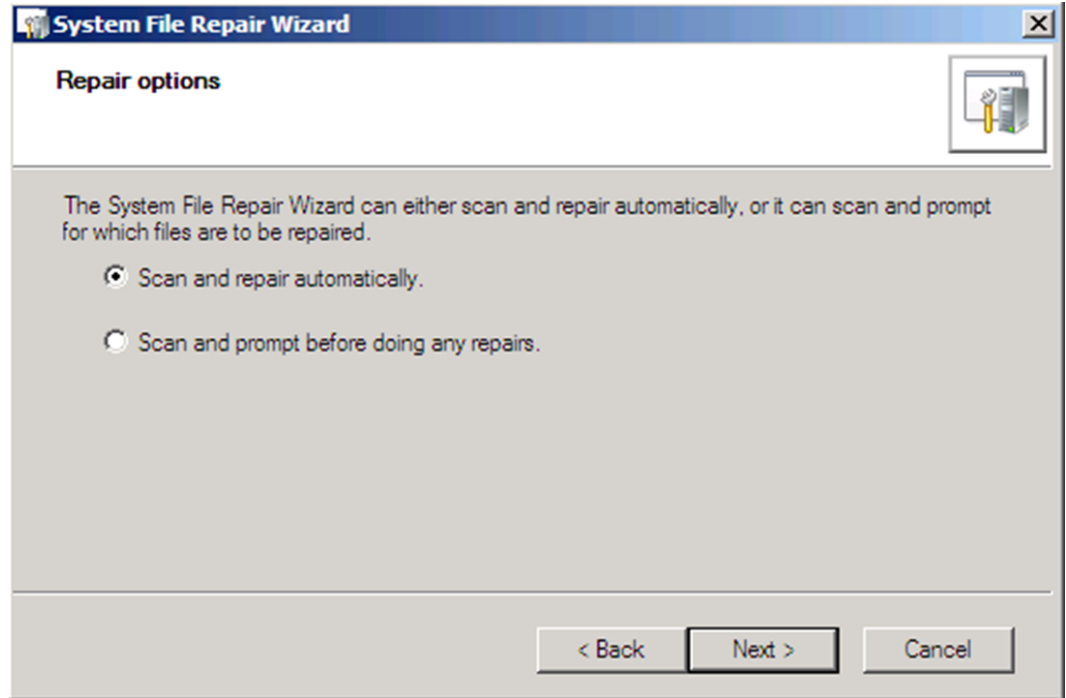


Figure 17. System File Repair Wizard

Search

Before reimaging a computer, recovering files from the local hard disk is important—particularly when the user might not have backed up or stored the files elsewhere. Although the Explorer tool can be helpful, File Search can help you to find documents when you do not know the file path or to search for general types of files across all the local hard disks. File Search, which Figure 18 shows, enables you to search the computer for files. You can search for specific file-name patterns in specific paths. Additionally, you can limit results to a date range or size range. In recovery scenarios, when repairing the installed operating system is not possible, you can use File Search to find users' documents and copy them from the computer.

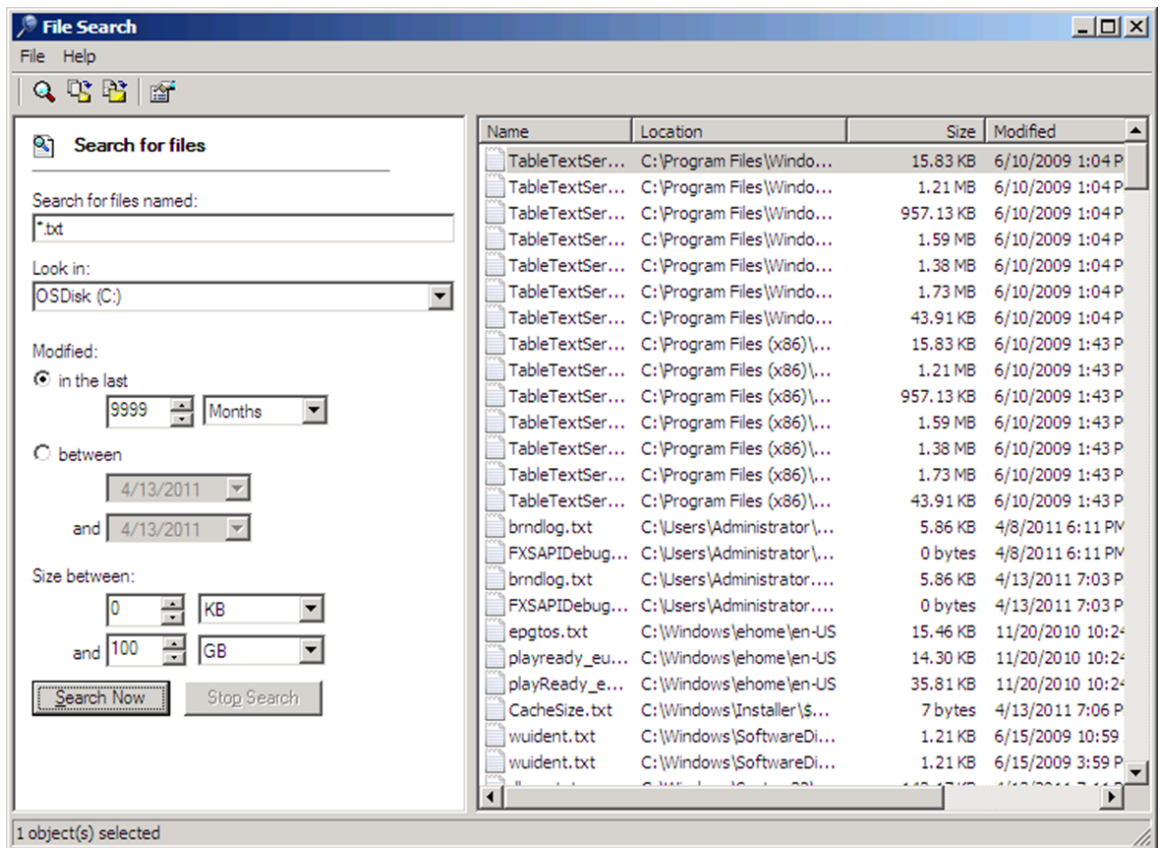


Figure 18. File Search

Standalone System Sweeper

Having a good antivirus and anti-malware strategy in your organization is crucial. Although real-time scanner tools such as Microsoft Forefront Endpoint Protection are vital, today's ever-changing landscape requires many different tools to defend your network.

Malware that uses rootkits can mask itself from the running operating system. If a rootkit-enabled virus or spyware makes its way to the system, most real-time scanning and removal tools can no longer see it or remove it. Because DaRT leaves the installed operating system offline, you can attack the rootkit without it hiding from you.

Figure 19 shows the Standalone System Sweeper. This tool can help detect malware and unwanted software and alert you to security risks. When the Standalone System Sweeper detects malicious or unwanted software, it prompts you to remove, quarantine, or allow each item. You can use this tool to scan a computer for and remove malware while the installed Windows operating system is not running.

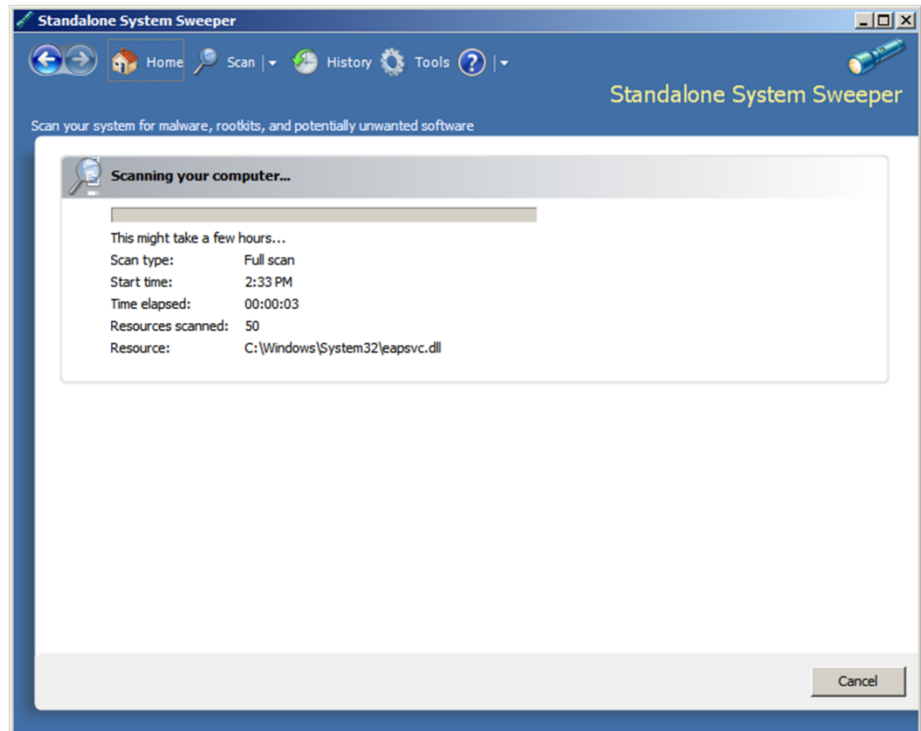


Figure 19. Standalone System Sweeper

Using Remote Connection

DaRT Remote Connection can help reduce the time and effort required to support end users. You can connect to client computers and use the DaRT tools remotely—without visiting users' desks. You enable Remote Connection when you create recovery images by using the DaRT Recovery Image Wizard (see the section titled "Creating the DaRT Media," earlier in this white paper).

When users require remote assistance, you talk them through starting the computer into DaRT. After starting DaRT, they click Remote Connection and confirm that they want to share the DaRT tools; then, as Figure 20 shows, Remote Connection displays a ticket number, IP address, and port number that the user communicates to you.

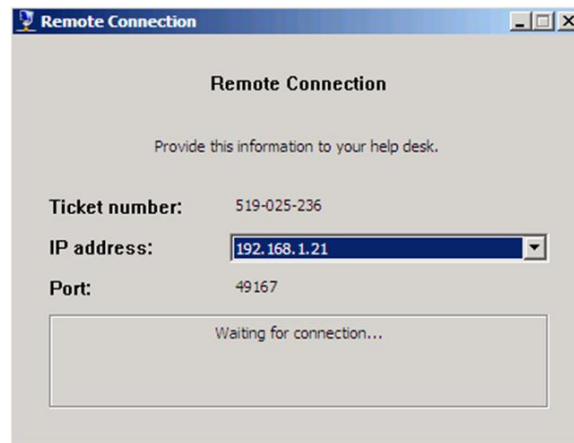


Figure 20. Remote Connection

You then use the Remote Connection Viewer to connect to the DaRT tools remotely, as Figure 21 shows. To simplify the process and reduce the amount of handholding required to get Remote Connection started, you can optionally configure the DaRT recovery image to automatically start Remote Connection whenever users start their computers with the recovery image. See the DaRT 7.0 Help for more information.

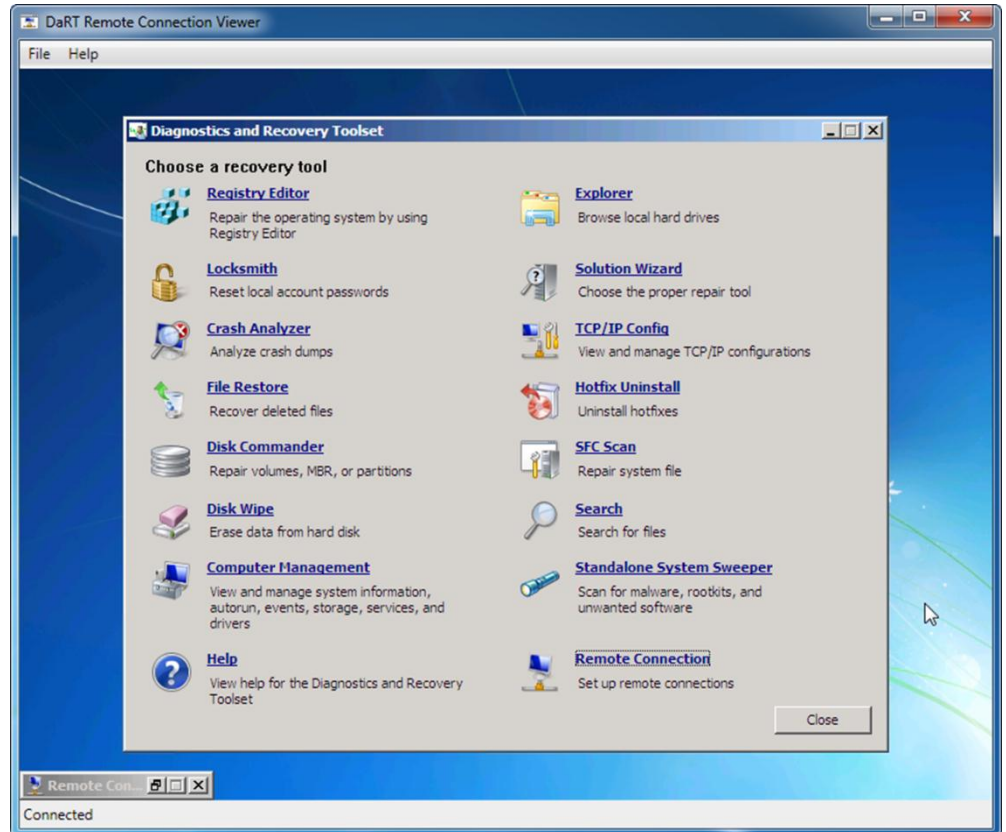


Figure 21. Remote Connection Viewer

You can also restrict local end-user access to the DaRT tools while retaining full access to them through the Remote Connection Viewer. Simply disable all of the tools on the Tool Selection page of the DaRT Recovery Image Wizard. This configuration only disables the tools for the local user. It does not hide them, and it does not disable the Remote Connection tool. When users start the DaRT tools, they see that all of the tools except for Remote Connection are unavailable. However, when you connect to the DaRT tools by using Remote Connection Viewer, you still have unrestricted access to the DaRT tools.

Customizing Remote Connection

Without customization, using Remote Connection requires assistance. Additionally, its default configuration might not match your requirements (you might want to perform actions while the user is away).

You can customize Remote Connection to support advanced options, though. The configuration file `winpeshl.ini` in `\Windows\System32\` on the ISO image allows you to configure custom actions when DaRT starts. For example, you can launch the following applications:

-
- **RemoteRecovery.exe –nomessage.** This initiates the Remote Connection and bypasses the confirmation dialog. Remote Connection continues as if the user had clicked Yes.
 - **WaitForConnection.exe.** This prevents the script from continuing until either Remote Connection is not running or a valid connection is established with the user's computer.

To customize Remote Connection, modify winpeshl.ini on the Add Files page of the DaRT Recovery Image Wizard. The following is an example that starts Remote Connection and waits for the connection before starting the Windows RE (see [Launching DaRT 7 Remote Connection Tool at Startup](#)):

```
[LaunchApps]
"%windir%\system32\netstart.exe -network -remount"
"cmd /C start %windir%\system32\RemoteRecovery.exe -nomessage"
"%windir%\system32\WaitForConnection.exe"
"%SYSTEMDRIVE%\sources\recovery\recenv.exe"
```

When DaRT starts, it creates the file inv32.xml in \Windows\System32\ on the RAM disk. This file contains connection information: IP address, port, and ticket number. You can copy this file to a network share to trigger a helpdesk workflow. For example, a custom program can check the network share for connection files; then, create a support ticket or send email notifications.

EVALUATING DART

DaRT is an add-on license available to Software Assurance customers. Begin your evaluation today:

Download and evaluate DaRT as part of MDOP.

MDOP is available to Volume Licensing customers, Microsoft Development Network (MSDN) subscribers, and Microsoft TechNet subscribers.

See MDOP on Microsoft.com.

To learn how DaRT and MDOP for Software Assurance can help you better troubleshoot and repair computers, see <http://go.microsoft.com/fwlink/?LinkId=160297>.

See MDOP on TechNet.

For technical information about DaRT and MDOP for Software Assurance, see <http://www.microsoft.com/technet/mdop> on TechNet.

Sysinternals Utilities

Mark Russinovich and Bryce Cogswell created the Sysinternals Web site in 1996 to host the advanced Windows utilities and technical information that they built. Microsoft acquired Sysinternals in July 2006.

The Sysinternals utilities are some of the most powerful diagnostic tools available—and they are free. You can download them from <http://technet.microsoft.com/sysinternals/>. They are a perfect complement to DaRT. Whereas DaRT helps you diagnose and recover Windows installations offline, the Sysinternals utilities help you diagnose Windows installations online.

The Sysinternals utilities include dozens of diagnostic tools, but two of the most compelling are Process Monitor and Process Explorer. Process Monitor monitors file-system, registry, process, thread, and DLL activity in real time. Process Explorer displays the files, registry keys, and other objects that processes have open; which DLLs they have loaded; and more.

The combination of DaRT with these utilities can help you troubleshoot problems in a variety of scenarios. See for yourself: Read the case studies that Russinovich posts at <http://blogs.technet.com/markrussinovich/>.

FOR MORE INFORMATION

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada information Centre at (800) 563-9048. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information through the World Wide Web, go to:

<http://www.microsoft.com>

<http://www.microsoft.com/technet/itshowcase>

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

© 2011 Microsoft Corporation. All rights reserved.

Microsoft and Microsoft Diagnostics and Recovery Toolset are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.