USER GUIDE

Recover Lost or Forgotten Passwords

Password Recovery Toolkit™
Recover Passwords Quickly & Easily

AccessData®
Legal Notices
AccessData Corp. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Corp. reserves the right to revise this publication and to make changes to its content at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Corp. makes no representations or warranties with respect to any software and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Corp. reserves the right to make changes to any and all parts of AccessData software at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

© 2003–2007 AccessData Corp. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

PRTK 6.1 User Guide, revision 1, July 2005
PRTK 6.2 User Guide, revision 1, July 2006
AccessData Trademarks
AccessData is a registered trademark of AccessData Corp.
Distributed Network Attack is a registered trademark of AccessData Corp.
DNA is a registered trademark of AccessData Corp.
Forensic Toolkit is a registered trademark of AccessData Corp.
FTK is a trademark of AccessData Corp.
FTK Imager is a trademark of AccessData Corp.
Known File Filter is a trademark of AccessData Corp.
KFF is a trademark of AccessData Corp.
Password Recovery Toolkit is a trademark of AccessData Corp.
PRTK is a trademark of AccessData Corp.
Registry Viewer is a trademark of AccessData Corp.
Ultimate Toolkit is a trademark of AccessData Corp.

Third-party Trademarks
All third-party trademarks are the property of their respective owners.

This product includes the following third-party components:


XercesImpl.jar for the parsing of XML (http://apache.org/licenses).

TeeChart Pro ActiveX version 6 (http://www.steema.com).


Libxslt (http://xmlsoft.org/XSLT). Copyright © 2001–2002 Daniel Veillard. All rights reserved.


dtSearch Full Text Search Engine (http://www.dtsearch.com). Copyright © 1991–2004 dtSearch Corp. All rights reserved.

Boost Software (http://www.boost.org).


This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). Copyright (c) 1998–2004 The OpenSSL Project. All rights reserved.

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
   THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Copyright (C) 1995–1998 Eric Young (eay@cryptsoft.com)
All rights reserved.

1. Redistributions of source code must retain the copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)."

The word "cryptographic" can be left out if the routines from the library being used are not cryptographically related.

4. If you include any Windows-specific code (or a derivative thereof) from the APPS directory (application code), you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
CONTENTS

Preface
- Forensic Analysis Software ............................................. 3
- Registry Viewer Software ............................................. 4
- Distributed Network Attack ........................................... 4
- Secure Deletion Tools ................................................ 4
- Ultimate Toolkit .......................................................... 4
- Password Recovery Software ......................................... 5

Chapter 1 Password Recovery Toolkit Overview ...................... 7
- Password Recovery Toolkit ........................................... 7
- Features Overview ..................................................... 8
- PRTK Additional Tools ................................................ 9
  - LicenseManager ..................................................... 9
  - Language Selector ................................................ 9
  - Passphrase Generator ............................................. 9

Chapter 2 Installing Password Recovery Toolkit ...................... 11
- System Requirements .................................................. 12
- Supervisor Requirements ........................................... 13
- DNA Worker Requirements ......................................... 14
- PRTK Installation from CD ......................................... 16
- Basic Supervisor Installation ....................................... 24
- Sharing the Supervisor Directory .................................. 25
- Basic Worker Installation on a Windows Workstation .......... 26
- Basic Worker Installation on a Macintosh Workstation ........ 26
- Basic Worker Installation on a Linux Machine ................. 29
- Stealth Worker Installation .......................................... 32
- Licensing ................................................................. 33
- Uninstalling PRTK ........................................................ 34
  - Uninstalling the DNA Supervisor ................................ 34
  - Uninstalling the DNA Worker ................................... 35
Chapter 9 Using the Dictionary Utility ........................................ 149
  Dictionary Basics .................................................. 149
  AccessData Dictionary Utility ...................................... 151
      Starting the Dictionary Utility ................................ 151
  Dictionary Information ............................................... 152
  Browse Dictionaries .................................................. 153
  Standard Dictionary Generator ..................................... 153
  Biographical Dictionary ............................................. 155
      Biographical Dictionary Data ................................... 155
  Pass-phrase Dictionary Generator ................................. 159
  Permutation Dictionary Generator ................................. 160
  Merging Golden Dictionaries ....................................... 161

Chapter 10 Specialized Password Recoveries .......................... 163
  Recovering Login Passwords ....................................... 164
      Accessing the SAM file and the system file ................... 164
  Recovering Login Passwords on Windows NT ..................... 165
  Recovering Passwords from Win 9x Files ......................... 165
  Recovering Login Passwords on Windows 2000 and XP Systems . 166
  Recovering Passwords from the Current Registry ............... 168
  Recovering Passwords from the Registry Protected Storage Area . 168
  Windows 95/98/ME ................................................ 172
  Windows 2000 ..................................................... 172

Chapter 11 Using Recovered Passwords to Open Files .......... 175
  Copying a Recovered Password to the Clipboard ................. 175
  Opening a File with a Recovered Password ....................... 176
  Opening Files with Multiple Passwords, Spare Passwords, or International Characters ...................................... 176
      Multiple Passwords ............................................. 176
      Spare Passwords ............................................... 176
      International Passwords ........................................ 177
  Modifying a Job ..................................................... 178
      Changing Job Name or Adding Comments ....................... 178
      Pausing a Job .................................................. 178
      Resuming a Job ............................................... 178
      Deleting a Job ................................................ 179
      Deleting All Jobs .............................................. 179
  Manually Decrypting Files with a Password or Key ........... 179
      Decrypting with a Key ........................................ 179
Welcome to AccessData® Password Recovery Toolkit™ (PRTK®). PRTK is used in many different environments to provide specific, password-related functions. For example, law enforcement and corporate security professionals can use PRTK in computer forensic investigations to access password-protected files. IT administrators can use PRTK to recover system passwords, while individual users can use PRTK to recover lost passwords to personal files. PRTK provides access to passwords for most available applications in the industry.

This chapter contains the following sections:

- “Audience” on page 1
- “Handling Evidence” on page 2
- “Other AccessData Products” on page 3

**Audience**

PRTK is intended for law enforcement officials and corporate security professionals who need access to password-protected files that might provide case evidence. PRTK is also available for any individual, such as an administrator or user, who needs to recover a lost or forgotten password.

PRTK allows law enforcement officials who are involved in the acquisition of digital evidence that is intended for use in court to recover passwords and access computer files that might contain critical evidence.

PRTK allows IT administrators to use PRTK to recover system passwords and allows users to recover lost passwords to personal files. Administrators can also use PRTK as a security
risk assessment tool to identify the weakest links in an organization’s security profile.

Anyone using PRTK needs to possess the following competencies:

- Basic knowledge of and experience with personal computers
- Understanding of file protection through passwords and cryptographic standards
- Familiarity with the Microsoft Windows environment

In addition, law enforcement and corporate security professionals need to possess the following competencies:

- Basic knowledge of and training in forensic policies and procedures
- Familiarity with the fundamentals of collecting digital evidence and ensuring the legal validity of the evidence
- Understanding of forensic images and how to acquire forensically sound images
- Experience with case studies and reports

## Handling Evidence

Law enforcement officials using PRTK to gather evidence need to understand the basics of computer forensics. Computer forensics involves the acquisition, preservation, analysis, and presentation of computer evidence. This type of evidence is fragile and can easily, even inadvertently, be altered, destroyed, or rendered inadmissible as evidence. Computer evidence must be properly obtained, preserved, and analyzed to be accepted as reliable and valid in a court of law.

To preserve the integrity of case evidence, forensic investigators do not work on the original files themselves. Instead, they create an exact replica of the files and work on this image to ensure that the original files remain intact.

To verify the files they are working on have not been altered, investigators can compare a hash of the original files at the time they were seized with a hash of the imaged files used in
the investigation. Hashing provides mathematical validation that a forensic image exactly matches the contents of the original computer.

Another important legal element in computer forensics is the continuity, or chain of custody, of computer evidence. The chain of custody deals with who has supervised, acquired, analyzed, and controlled the evidence. Forensic investigators must be able to account for all that has happened to the evidence between its point of acquisition or seizure and its eventual appearance in court.

There are many cases in which personnel trained in information technology have rendered incriminating computer evidence legally inadmissible because of reckless or ill-conceived examinations. Only properly trained computer forensics specialists should obtain and examine computer evidence.

Other AccessData Products

AccessData has developed other industry-leading products to assist in forensic analysis and password recovery. The following sections offer a brief introduction to these products:

Forensic Analysis Software

AccessData Forensic Toolkit® (FTK™) provides award-winning technology that can be used by law enforcement and corporate security professionals to filter and investigate evidence.

FTK provides users with the ability to perform complete and thorough computer forensic examinations. FTK features powerful file filtering and search functionality. FTK customized filters allow you to sort through thousands of files so you can quickly find the evidence you need. FTK is recognized as the leading forensic tool for performing e-mail analysis.

For more information about FTK, see the AccessData website at http://www.accessdata.com/Product04_Overview.htm .
Registry Viewer Software

AccessData Registry Viewer™ allows you to view the contents of Windows operating system registry files. Unlike Windows Registry Editor, which only displays the registry of the current system, Registry Viewer lets you examine registry files from any system. Registry Viewer also provides access to a registry’s protected storage, which contains passwords, usernames, and other information not accessible in Windows Registry Editor.

For more information about Registry Viewer, see the AccessData website http://www.accessdata.com/Product01_Overview.htm.

Distributed Network Attack

In addition to PRTK, AccessData offers another tool for password recovery. Distributed Network Attack® (DNA®) provides a new approach to recovering password-protected files. Rather than using a single machine, DNA uses machines across the network or across the world to conduct key space and dictionary attacks.

For more information about DNA, see the AccessData website at http://www.accessdata.com/Product03_Overview.htm.

Secure Deletion Tools

AccessData provides tools for a complete drive wipe in DOS. WipeDrive™ is ideal when you want to perform a complete Department of Defense (DoD)-compliant wipe of a drive. With a rate of 1 GB every three minutes, it is one of the fastest cleaning tools available and complies with DoD standards.

For more information about WipeDrive, see the AccessData website at http://www.accessdata.com/Product07_Overview.htm.

Ultimate Toolkit

The most comprehensive AccessData product for forensic investigation is the Ultimate Toolkit™, which includes all the PRTK recovery modules, a 100-client license for DNA, the
Forensic Toolkit, WipeDrive, Registry Viewer, and a one-year upgrade subscription for all of the included products.

For more information about the Ultimate Toolkit, see the AccessData website at http://www.accessdata.com/ultimate_overview.htm.

Password Recovery Software

AccessData has been the leader in the field of commercial software decryption since 1987. In addition to DNA, accessData has also developed Password Recovery Toolkit® (PRTK®).

PRTK has a wide variety of individual password-breaking modules that can help you recover lost passwords.

For more information about PRTK, see the AccessData website (http://www.accessdata.com/Product00_Overview.htm).
Password Recovery Toolkit Overview

This chapter contains the following sections:

- “Password Recovery Toolkit” on page 7
- “How PRTK Works” on page 7
- “Features Overview” on page 8
- “PRTK Additional Tools” on page 9

Password Recovery Toolkit

Password Recovery Toolkit™ (PRTK®) is a software solution that provides the tools you need to recover passwords and gain access to critical information in computer files. The critical information to recover might include vital personal files protected by a forgotten password or password-protected files that an administrator needs to recover or that a law enforcement officer needs to evaluate for evidence.

PRTK provides password-breaking modules for most industry applications you might use or encounter.

How PRTK Works

PRTK analyzes files to find encrypted files to recover using password recovery modules for supported applications. See “Understanding Encrypted Files” on page 254.

Before recovering passwords for protected files, PRTK creates hash values that can be used to determine whether the content of a file changed during the password recovery.
PRTK performs recoveries on protected files using various methods, including decryption and dictionary attacks. For more information on attack types, see “Understanding the PRTK Decryption Process” on page 255. For difficult password key values, PRTK performs dictionary attacks using levels of dictionaries, including Golden (containing previously recovered passwords), Biographical, custom User, and Default dictionaries.

PRTK displays file information for files or “jobs” in the recovery window.

After recovering passwords, PRTK lets you verify hashes, print reports, and open recovered files.

**Features Overview**

PRTK performs the following functions:

- **Hashes files**
  
  Hashing a file provides a unique algorithm that verifies the identity of a file. When you recover the password of a file, PRTK automatically hashes that file. This is particularly helpful to law enforcement personnel who need to verify that a file has not been changed while recovering a password.

- **Recovers passwords**
  
  PRTK can recover the password to any file created in most popular industry applications by using a variety of methods, including the dictionary attack, which recovers a password using different dictionaries and word combinations. PRTK can also recover multi-lingual passwords.

- **Generates reports**
  
  You can print file information for password recovery jobs.

- **Opens recovered files**
  
  You can open recovered files, if the applications where the files originated are available on the computer.
PRTK Additional Tools

PRTK includes the following tools:

LicenseManager

Lets you manage product and license subscriptions using a dongle or dongle packet file.

Language Selector

Lets you select the language to use when using PRTK.

Passphrase Generator

Lets you build dictionaries based on phrases from imported documents.
Installing Password Recovery Toolkit

This chapter describes how to install and uninstall Password Recovery Toolkit (PRTK).

This chapter contains the following sections:

- “System Requirements” on page 12
- “Before Installing PRTK” on page 14
- “Installing PRTK” on page 15
- “Basic DNA Installation” on page 24
- “Uninstalling PRTK” on page 34
- “Uninstalling the DNA Worker” on page 35
System Requirements

To run PRTK, the computer you install PRTK on must meet minimum system requirements.

The following table identifies the system requirements for installing PRTK:

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum</th>
<th>Suggested</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer CPU</td>
<td>Pentium III (500 MHz)</td>
<td>Pentium 4 (1 GHz or faster)</td>
</tr>
<tr>
<td>Memory</td>
<td>256 Megabytes (MB)</td>
<td>256 MB – 512 MB</td>
</tr>
<tr>
<td>Hard Disk Space</td>
<td>195 MB for program only</td>
<td>Additional dictionaries require more space</td>
</tr>
<tr>
<td>Monitor Display</td>
<td>VGA compatible</td>
<td>SVGA compatible</td>
</tr>
<tr>
<td>Ports</td>
<td>USB or parallel port</td>
<td>USB or parallel port</td>
</tr>
<tr>
<td>Security-compliance</td>
<td>USB or parallel port</td>
<td>USB or parallel port</td>
</tr>
<tr>
<td>Dongle</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP/IP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Password recovery processing is affected by processor speed and available memory.

The DNA system can consist of these components:

- At least one supervisor
- At least one or more workers

AccessData recommends that each component run on its own machine. The following table outlines the recommended and maximum DNA system numbers. The recommended numbers are dependent on the hardware available on each machine:
### Supervisor Requirements

The supervisor requirements are the same. The requirements are listed below according to the number of supervisors or workers that are supported.

<table>
<thead>
<tr>
<th>DNA Component</th>
<th>Recommended Number</th>
<th>Maximum Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor</td>
<td>50 in a DNA system</td>
<td>100 in a DNA system</td>
</tr>
<tr>
<td>Worker</td>
<td>500 workers per supervisor; 25,000 total workers in a DNA system</td>
<td>3,000 workers per supervisor; 100,000 total workers in a DNA system</td>
</tr>
</tbody>
</table>

##### Hardware or Software

<table>
<thead>
<tr>
<th>Hardware or Software</th>
<th>Less than 5 supervisors or Less than 50 workers</th>
<th>6 or more supervisors or More than 50 workers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows 2000, XP, or Server 2003</td>
<td>At least one processor that is 2 GHz or higher</td>
</tr>
<tr>
<td>Processor</td>
<td>Processor that is 1.5 GHz</td>
<td>At least one processor that is 2 GHz or higher</td>
</tr>
<tr>
<td>RAM</td>
<td>1 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Available Hardware Space</td>
<td>1 GB</td>
<td>1 GB</td>
</tr>
<tr>
<td>Network Card</td>
<td>100 MB or gigabyte network card The network card must support TCP/IP communications.</td>
<td>At least one 100 MB or gigabyte network card The network card must support TCP/IP communications.</td>
</tr>
<tr>
<td>CD-ROM Drive</td>
<td>4x speed</td>
<td>4x speed</td>
</tr>
<tr>
<td>USB or Parallel Port</td>
<td>Dongle that ships with DNA</td>
<td>Dongle that ships with DNA</td>
</tr>
<tr>
<td>Additional Software</td>
<td>AccessData recommends that DNA, Worker, and Forensic Toolkit run on separate machines.</td>
<td>AccessData recommends that DNA, Worker, and Forensic Toolkit run on separate machines.</td>
</tr>
</tbody>
</table>
DNA Worker Requirements

The DNA Worker requirements are listed below:

<table>
<thead>
<tr>
<th>Hardware or Software</th>
<th>Requirements</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Hard Drive Space</td>
<td>256 MB</td>
<td>1 GB</td>
</tr>
<tr>
<td>Network card</td>
<td>10/100 MB or gigabyte network card</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The network card must support TCP/IP communications.</td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td>Widows 2000</td>
<td>Windows XP Pro</td>
</tr>
<tr>
<td></td>
<td>Mac OS 10.3.9 (Power PC), OS 10.4 (Intel)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Linux Fedora Core 4, Redhat, Gentoo, SUSE, and Mandrake</td>
<td></td>
</tr>
</tbody>
</table>

Before Installing PRTK

Before installing PRTK, you should evaluate the workstation and its current software according to your investigational needs. A good understanding of the workstation and its configured devices can help ensure that PRTK runs efficiently.

Before installing PRTK, you must consider the following:

- **Role of the workstation**
  Determine if it is used as a regular user workstation, a forensic analysis workstation, or a password recovery machine.

- **Access policy**
  Identify where the system is located, who can access the information, and when the cases can be worked on.

- **Hardware and software requirements**
  For the hardware and software requirements, see “System Requirements” on page 12.
Installing Password Recovery Toolkit

- Application relationships
  Verify that the applications can work simultaneously. Do not run so many applications that you compromise overall performance.

- Network and Internet issues
  Determine if the workstation should be connected to a network or the Internet. Under normal circumstances, the forensic analysis workstation is not connected to the Internet to avoid the possibility of tainting evidence.

- System policies and procedures
  Check with your system administrator about any specific policies and procedures that might exist.

- Administrator rights
  To run PRTK successfully, you must be logged in as an administrator with sufficient rights.

**Installing PRTK**

The PRTK installation consists of the following parts:

- PRTK program files, password recovery modules, and additional tools (LicenseManager, Language Selector, and Passphrase Generator)

- Dongle and Dongle drivers
  A USB or parallel port dongle and the dongle drivers are required to run PRTK unless you are running PRTK in Demo mode.

  **Note:** To run PRTK to its fullest, you must have a dongle. For more information, see “Using the Dongle” on page 41.

  The dongle should be stored in a secure location when not in use.

You can install PRTK and the dongle drivers from a CD or from downloadable files available on the AccessData website at http://www.accessdata.com.

For solutions to commonly asked installation questions, see “Troubleshooting” on page 195.
PRTK Installation from CD

Using the Password Recovery Toolkit CD, you can install PRTK components, view this PRTK User Guide (requires Adobe Reader), and demo other AccessData products.

The following sections review how to install the PRTK components available on the CD:

- “Installing the Dongle Drivers from CD” on page 17
- “Installing PRTK from CD” on page 19
Installing the Dongle Drivers from CD

Before you can install the dongle drivers, you must have a dongle. The dongle is a security-compliance device that maintains your PRTK licensing and subscription information and is required to use a full PRTK session.

If you purchase the full PRTK package, AccessData provides a parallel or USB dongle with the product package.

If you do not have a dongle, you can demo PRTK. See “Running PRTK in Demo Mode” on page 42.

Note: Insert the dongle into the parallel or USB port only when prompted during installation of the dongle drivers.

To install the dongle drivers from CD:

1. Insert the CD into the CD-ROM drive and click Install the Dongle Drivers.
   If auto-run is not enabled, select Start and then Run. Browse to the CD-ROM drive and select Autorun.exe.
2. Click Next on the Welcome screen.
3. Select the type of dongle drivers you want to install; then click Next.
4. Depending on your dongle, do one of the following:
If you have a USB dongle, verify that it is not plugged in, and then click **Next**.

If you have a parallel port dongle, verify that it is plugged in, and then click **Next**.

5 Choose the dongle driver directory.

6 If you have a USB dongle, plug it in.

7 Click **Finish**.
**Important:** If the Windows Found New Hardware wizard appears, complete the wizard.

Once you have installed the dongle and the dongle drivers, you can use LicenseManager to manage product licenses. For more information about LicenseManager, see “Managing Licenses” on page 181.

**Installing PRTK from CD**

Although you can install PRTK from the product CD, you cannot fully use the product until you install a security dongle from AccessData. You can, however, install and demo the product without a security dongle.

- If you have a dongle, you must install the dongle drivers and the dongle before installing PRTK. See “If you have a USB dongle, plug it in.” on page 18.
- If you do not have a dongle, you can demo PRTK. See “Running PRTK in Demo Mode” on page 42.

To install PRTK from CD, complete the following:

1. Insert the CD into the CD-ROM drive and click **Install Password Recovery Toolkit**.
   
   If auto-run is not enabled, select **Start** and then **Run**. Browse to the CD-ROM drive and select **Autorun.exe**.

2. Click **Next** on the Welcome screen.

3. Select **Next** to accept the license agreement.

   If you choose not to accept the terms of the license agreement, you cannot continue with the installation.

   If you want, you can print the license agreement by clicking **Print**.

   - Click **Complete** to install all components to the default directory. The default directory is \drive\Program Files\AccessData.

   or
Click **Custom** to specify a different location or to select which components to install.

4 Click **Install** to begin installing the product. A progress bar shows the status of the installation.

To run PRTK after completing the installation, select **Run PRTK 6**.

To run PRTK with a dongle, you must have already installed the dongle drivers. For more information, see “If you have a USB dongle, plug it in.” on page 18.

If you have installed the dongle and the dongle drivers, select **Run PRTK 6** to run PRTK after completing the installation.

If you have not installed the dongle and the dongle drivers, uncheck **Run PRTK 6**, click **Finish**, run the **Autorun.exe**, and then click **Install the Dongle Drivers**.

You can start PRTK later by selecting **Start** then **Programs** then **AccessData** then **Password Recovery Toolkit 6** and then **PRTK 6**.

5 Click **Finish** to complete the installation.

The following sections provide information on downloading the PRTK components available on the AccessData website.

- “Installing PRTK from Downloadable Files” on page 21
- “Installing the Dongle Drivers from Downloadable Files” on page 21
- “Installing LicenseManager from Downloadable Files” on page 22

Installing PRTK from Downloadable Files

Although you can download PRTK from the AccessData website, you cannot fully use the product until you receive a security dongle from AccessData. You can, however, download and demo the product without a security dongle.

- If you have a dongle, we recommend installing the dongle drivers and the dongle before installing PRTK. See “Installing the Dongle Drivers from Downloadable Files” on page 21.
- If you do not have a dongle, you can demo PRTK. See “Running PRTK in Demo Mode” on page 42.

Installing the Dongle Drivers from Downloadable Files

Before you can install the dongle drivers, you must have a dongle. The dongle is a security-compliance device that maintains your PRTK licensing and subscription information and is required to use PRTK fully.

If you purchase the full PRTK package, AccessData provides a parallel or USB dongle with the product package.

If you do not have a dongle, you can demo PRTK. See “Running PRTK in Demo Mode” on page 42.

To install the dongle drivers from downloadable files:

2 On the download page, click the **Dongle Drivers** link.

3 Save the dongle installation file to a temporary directory on your drive.

4 To launch the installation program, go to the temporary directory and double-click the dongle installation file.

5 Click **Install**.

   **Note:** Insert the dongle into the parallel or USB port only when prompted during installation of the dongle drivers.

6 Follow the same instructions for installing from CD, beginning with Step 2 on page 17.

### Installing LicenseManager from Downloadable Files

LicenseManager lets you manage product and license subscriptions using a dongle or dongle packet file. For more information, see “Managing Licenses” on page 181.

**Note:** LicenseManager is installed when running the installation program for PRTK. If you need to install LicenseManager on a machine without PRTK, perhaps to manage licenses remotely, you can install LicenseManager standalone.

To install LicenseManager standalone:


2 On the download page, click the **LicenseManager** link.

3 Save the installation file (Licensemanager.exe) to a temporary directory on your drive.

4 To launch the installation program, go to the temporary directory and double-click the installation file (Licensemanager.exe).

5 Click **Next** on the Welcome screen.

6 Click **Yes** to accept the license agreement.
7 Choose the destination.

8 If you want to launch LicenseManager after completing the installation, select **Run LicenseManager**.

You can start LicenseManager later by selecting **Start** then **Programs** then **AccessData** then **LicenseManager** and then **LicenseManager**. You can also start LicenseManager in PRTK by selecting **Help** and then **Launch LicenseManager**.
Basic DNA Installation

You can install DNA from a CD or from downloadable files available on the AccessData website (http://www.accessdata.com).

You need to install the DNA Supervisor, the dongle driver, and the DNA Worker.

You can also choose to install the Passphrase Generator.

- **DNA Supervisor**: A machine in the DNA system that controls worker machines beneath it and the jobs that they process. Install the supervisor before you install the DNA Workers.

- **Dongle Driver**: The dongle enables you to use DNA; the dongle drivers must be installed on the machines of the supervisors.

- **DNA Worker**: You must run the appropriate DNA Worker installation program on each participating machine in the system.

The installation copies the files to the Program Files\AccessData\ directory.

Basic Supervisor Installation

Run the supervisor installation on the machine that you want to be a DNA Supervisor. Complete the supervisor installation before installing the DNA Worker on any machine.

1. Turn off all firewalls, virus scanners, and spyware.

2. Insert the CD into the CD-ROM drive.

   If auto-run is not enabled, select **Start**, and then **Run**. Browse to the CD ROM drive. In the Setup folder, double-click **Autorun.exe**.

   If you are installing from downloadable files, double-click **DNAversion_number.exe**.

3. Click **Supervisor** on the DNA Installation screen.

4. Click **Next** on the Supervisor form.

5. Select **I Accept the Terms of the License Agreement**.
If you choose not to accept the terms of the license agreement, you cannot continue with the installation.

6 Click **Print** to print the license agreement.

7 Click **Next** to accept the default folder location in the Choose Destination Location field.

To specify a different location, click **Browse**, select the location, and click **OK**; then click **Next**.

8 (Conditional) If you have already completed a partial uninstall and want to re-install the supervisor using your saved keys, click **Yes**; then browse to and select the **Supervisor.ini** file.

9 Click **Finish** to complete the installation on the Supervisor Installation Complete form.

If you want to run the Supervisor, check the **Run Supervisor** box.

10 Check the box for either the server or the interface.

**Basic DNA Worker Installation**

The DNA Worker installation programs are available in the Supervisor directory. You can install the DNA Worker on Windows, Macintosh, or Linux machines. For more information about the worker system requirements, see “System Requirements” on page 20.

This section contains the following information:

- “Basic Worker Installation on a Windows Workstation” on page 39
- “Basic Worker Installation on a Macintosh Workstation” on page 41
- “Basic Worker Installation on a Linux Machine” on page 44

**Sharing the Supervisor Directory**

You need to share the Supervisor directory so that worker machines can remotely access this directory to run the DNA Worker installation.
If the directory isn’t already shared, complete the following:

1. In Windows Explorer, right-click the AccessData\DNA 3\Supervisor\ directory and select Sharing.
2. In the Sharing tab, select Shared As.
3. (Optional) Enter any additional information in the fields in the Sharing tab that you want to require of the client workstations before they can access the directory.

Basic Worker Installation on a Windows Workstation

1. On the Windows workstation, browse to the shared Supervisor directory and double-click WorkerInstall.exe.
2. Click Next on the Worker screen.
3. Click Yes to accept the license agreement.
4. Click Next to accept the default folder location in the Choose Destination Location field.
   
   To specify a different location, click Browse, select the location, then click OK, and then click Next.
5. Click Finish to complete the installation of the worker.

   If you want to run the DNA Interface, then check the box. After the installation is completed, the Worker Status icon, shown below, appears in the Taskbar.

   Clicking the icon opens the DNA Worker Status screen. For more information about the DNA Worker Status screen, see “DNA Worker Interface” on page 67.

Basic Worker Installation on a Macintosh Workstation

You can install the DNA Worker at the local machine or from the DNA Supervisor machine.

Installing Locally

To install the DNA Worker locally, complete the following steps as user root at a terminal on the target Macintosh machine.
Sometimes the SSH service on a Mac needs to be started. To execute the command, start a terminal on the Mac, log in as root user and run: /sbin/service ssh start. This will start the service and allow access to the Mac using SSH.

Sometimes the Mac requires the Root user to install/uninstall the program. If the error: operation not permitted comes up, type: “login root” at the cmd line and provide the root password. Then proceed with the following commands:

1 Copy worker-powerpc-install.sh from the Windows Supervisor folder to a folder on the Mac box using a command prompt:

   scp worker-powerpc-install.sh <Mac box name>:

   You will be prompted for your user password. By default, the folder is copied to the /users/<username> folder.

2 Once copied, logon to the box by typing ssh user@box_name and switch to the root user:

   Login root (prompts for password).

3 Change directory to the folder you copied worker-powerpc-install.sh to: cd /users/<user_name> and run:

   ./worker-powerpc-install.sh.

4 When prompted to install Java, answer no. Mac already has java installed.

5 Once the worker is installed, go to the /opt/Accessdata/DNA3/Worker folder by typing:

   cd /opt/AccessData/DNA3/Worker.

6 Run the following command to start the worker service:

   ./dna3workerd start

7 Once running, the worker on this Mac box should display with the IP address and name of the machine on the Supervisor.

8 Run the following command to stop the worker service: ./ dna3workerd stop to stop the worker.
Installing Remotely

Before you remotely install the DNA Worker on a Macintosh workstation, verify the following:

- The DNA Supervisor is already installed on a Windows machine.
- Scl and ssh command files are available on the supervisor machine.
- You have a user account on the Macintosh workstation.

To remotely install the DNA Worker from the supervisor machine:

1. Modify the Hosts file in C:\windows\system32\drivers\etc to include the IP address of the worker machine.

2. Using a terminal, copy worker-powerpc-install.sh from the Supervisor directory to a directory on the Macintosh machine:

   scp worker-powerpc-install.sh <Macintosh machine name>:

   By default, the file is copied to the /users/<username> directory.

**Note:** You might need to be logged in as root to complete this step.

   Type `login root` at the terminal and provide the root password.

1. Enter the user password for the Macintosh workstation.

2. Log in to the Macintosh workstation:

   `ssh user@machine_name`

**Note:** You might need to start the ssh service. Start a terminal on the Macintosh, log in as root user, and run `sbin/service ssh start`.

3. Switch to the root user: Login root

4. Enter the root password.

5. Go to the directory in which you copied `worker-powerpcinstall.sh`; type the following:

   `./worker-powerpc-install.sh`
6 When prompted to install Java, enter No. The machine already has Java installed.

7 Go to the /opt/Accessdata/DNA3/Worker folder:
   cd /opt/AccessData/DNA3/Worker

8 To start the worker service, run the following command:
   ./dna3workerd start

   The worker on the Macintosh workstation displays the IP address and machine name of the supervisor.

   If you get a library error when trying to start the worker, then go to the /opt/Accessdata/DNA3/Worker directory and type the following:
   DYLD_LIBRARY_PATH=. sh ./dna3worker-powerpc start

9 To stop the worker service, run the following command:
   ./dna3workerd stop

Basic Worker Installation on a Linux Machine

You can install the DNA Worker at the local machine or from the DNA Supervisor machine. Modify the hosts file under C:\windows\system32\drivers\etc to include the IP addresses of the worker machines so you can log on to the correct box and use the SCP and SSH commands for file transfer.

Installing Locally

To install the DNA Worker locally, complete the following steps as user root at the command line on the target Linux machine:

1 Copy worker-i386-install.sh from the Windows Supervisor folder to a folder on the Linux box using a command prompt:
   scp worker-i386-install.sh <Linux box name>:

   You will be prompted for your user password. By default, the folder is copied to the /home/<username> folder.
2 Once copied, logon to the box by typing ssh user@box_name and switch to the root user:
   su (prompts for password, if applicable).
3 Change directory to the folder you copied worker-i386-install.sh to: cd /home/<user_name> and run:
   ./worker-i386-install.sh.
4 When prompted to install Java, answer Yes.
5 Once Java is installed, go to the /opt/Accessdata/DNA3/Worker folder by typing:
   cd /opt/AccessData/DNA3/Worker.
6 Run the following command to start the worker service:
   ./dna3workerd start to start the worker.
7 Once running, the worker on this Linux box should display with the IP address and name of the machine on
   the Supervisor.
8 Run the following command from the AccessData folder to stop the worker service:
   ./dna3workerd stop to stop the worker.

Installing Remotely

Before you remotely install the DNA Worker on a Linux machine, verify the following:
   • The DNA Supervisor is already installed on a Windows machine.
   • Scp and ssh command files are available on the supervisor machine.
   • You have a user account on the Linux machine.
To remotely install the DNA Worker from the supervisor machine:
1 Modify the Hosts file in C:\windows\system32\drivers\etc to include the IP address of the worker machine.
2 Using a command prompt, copy `worker-i386-install.sh` from the Supervisor directory to a directory on the Linux machine:

```
scp worker-i386-install.sh <Linux machine_name>:
```

By default, the folder is copied to the `/home/<username>` directory.

3 Enter the user password for the Linux machine.

4 Log in to the Linux machine:

```
ssh user@machine_name
```

5 Switch to the root user:

```
su
```

6 (Conditional) Enter the root user password.

7 Go to the directory in which you copied `worker-i386-install.sh`; type the following:

```
./worker-i386-install.sh
```

8 When prompted to install Java, answer **Yes**.

9 After Java is installed, go to the `/opt/Accessdata/DNA3/Worker` directory:

```
cd /opt/AccessData/DNA3/Worker
```

10 To start the worker service, run the following command:

```
./dna3workerd start
```

The worker on the Linux machine displays the IP address and machine name of the supervisor.

If you get a library error when trying to start the worker, then go to the `/opt/Accessdata/DNA3/Worker` directory and type the following:

```
LD_LIBRARY_PATH=. ./dna3worker-i386 start
```

11 To stop the worker service, run the following command:

```
./dna3workerd stop
```
Stealth Worker Installation

A “Stealth” install involves installing a DNA worker to a computer where the user does not know it is installed. The only difference between a normal and “Stealth” install is the fact that the worker.exe is not started and therefore, the key icon on the taskbar does not display.

You can perform a stealth DNA Worker installation so that the users of the Windows workstations are not aware of the install or the program itself. You cannot perform a stealth installation on Macintosh, or Linux machines.

Before you perform a stealth DNA Worker installation, be sure to first install the DNA Supervisor to which the workers will be assigned.

To perform a stealth client installation, enter the following in a command prompt:

`WorkerInstall.exe /s /f1<path to WorkerInstall.iss filename>`

By default, WorkerInstall.iss is installed in the `C:\Program Files\AccessData\DNA 3\Supervisor` directory.

For example:

`WorkerInstall.exe /s /f1"C:\Program Files\AccessData\DNA 3\Supervisor\WorkerInstall.iss"`

Or you can use third-party applications, such as ZENworks or Windows 2003 Server to push out the installation. Refer to the individual product documentation for more information.

If you perform a stealth DNA Client installation, the DNA Worker Status icon does not appear in the Taskbar.

A Stealth install is accomplished in two ways:

1. By installing a worker on any given machine and using a 3rd party product to ‘push’ the installed worker out to the worker computers.

or

2. Copy the files, the installation file: WorkerInstall.exe, and the response file: WorkerInstall.iss, to the worker
computer, and then run the install with the command below. Once installed, both the install & response files can be deleted.

For example, to install a stealth worker on a user’s computer, copy the files listed above to a temporary folder and then run the following command from the temp folder:

WorkerInstall.exe /s /f1"C:\temp\WorkerInstall.iss"

Verify you use the quotes around the path of the response file. Wait until the command prompt returns. Once it returns, the worker should be listed on the supervisor and the worker is ready to process jobs.

**After Installing PRTK**

Before running the full package of PRTK, you must install a dongle and the dongle drivers, and add licenses to the dongle.

**Licensing**

You can manage product licenses on a dongle using LicenseManager.

For information about installing LicenseManager, see “Installing LicenseManager from Downloadable Files” on page 22.

For information about starting LicenseManager, see “Managing Licenses” on page 181.

For information about password modules, see “Viewing Module Information” on page 42.
Uninstalling PRTK

You can uninstall PRTK just as you would typically remove other programs from the Windows Control Panel.

To uninstall the PRTK program:

1. Under the Start menu, select Control Panel > Add or Remove Programs.
2. Select AccessData PRTK 6; then click Remove.
3. Select Uninstall PRTK 6; then click Next.
4. Click Yes to proceed with the uninstallation.
5. Click Finish to complete the uninstallation.

To uninstall the dongle drivers:

1. Under the Start menu, select Control Panel and then Add or Remove Programs.
2. Select the Dongle Driver; then click Change/Remove.
3. Click OK to proceed with the uninstallation.
4. Click Finish to complete the uninstallation.

Uninstalling the DNA Supervisor

You can uninstall the DNA Supervisor from the Windows Control Panel. You can perform one of the following:

- Partial uninstall: Removes the DNA program files. You can select a partial uninstall if a program file becomes corrupted. You can then re-install the supervisor without losing your customized DNA files, such as profiles, levels, and the communication keys. For more information, see “Basic Supervisor Installation” on page 27.
- Full uninstall: Removes all files in the Supervisor directory, including program files and customized files. If you perform a full uninstall, the workers subordinate to the supervisor stop processing jobs.

To uninstall the DNA Supervisor:
1 Under the Start menu, select Control Panel and then Add/Remove Programs.

2 Select AccessData DNA 3 Supervisor and click Change/Remove.

3 Select the desired type of uninstall and click Next.

4 Click Finish.

Uninstalling the DNA Worker

You can uninstall the DNA Worker on Windows workstations and Linux machines. You can also use a stealth removal to uninstall the DNA Worker on many Windows workstations.

This section contains the following information:
- “Uninstalling the DNA Worker on a Windows Workstation” on page 55
- “Uninstalling the DNA Worker on a Macintosh, or Linux Machine” on page 55
- “Performing a Stealth Removal of the DNA Worker” on page 56

Uninstalling the DNA Worker on a Windows Workstation

You can uninstall the DNA Worker from the Windows Control Panel.

To uninstall the DNA Worker:

1 Under the Start menu, select Control Panel and then Add/Remove Programs.

2 Select AccessData DNA 3 Worker and click Change/Remove.

   If you are prompted that the application is still running, right-click the key icon in the Taskbar and select Exit.

3 Click OK to remove DNA and all its components.

4 Click Finish.
Uninstalling the DNA Worker on a Macintosh, or Linux Machine

To uninstall the DNA Worker on a Linux machine, complete the following steps as user root at the command line:

1. Go to the /opt/Accessdata/DNA3/Worker directory.
2. Stop the worker service by typing the following:
   ./dna3workerd stop
3. Using the additional uninstall switch, run the appropriate install file from the directory you copied it to during installation:
   - On a Macintosh workstation, type sh ./workerpowerpc-install.sh uninstall
   - On a Linux machine, type ./worker-i386-install.sh uninstall

The AccessData/DNA3/Worker directory and the related symbolic links are removed.

Performing a Stealth Removal of the DNA Worker

You can perform a stealth DNA Worker removal so that the users of the Windows workstations are not aware of the uninstall. You cannot perform a stealth uninstallation on Macintosh and Linux machines.

You can use several third-party applications, such as ZENworks or Windows 2003 Server, to remove the application from individual workstations. Refer to the individual product documentation for more information.

To perform a stealth uninstall:

1. Copy the files: (WorkerInstall.exe and the response file: WorkerUninstall.iss) to a temp folder and run:
   WorkerInstall.exe /s /f "C:\temp\WorkerUninstall.iss"
2. Verify you use the quotes around the path of the response file. Wait until the command prompt returns.
The worker is now successfully removed from the user’s computer.

Uninstalling the Dongle Driver

You can uninstall the dongle driver from the Windows Control Panel.

To uninstall the dongle driver:

1. On the machine the dongle driver is installed on, select Control Panel and then Add/Remove Programs.
2. Select AccessData Dongle Driver and click Change/Remove.
3. Click OK to remove the dongle driver and all its components.
4. Click Finish.
Getting Started

This section acquaints you with Password Recovery Toolkit (PRTK).

This chapter contains the following sections:

- “Starting PRTK” on page 40
- “Touring the Interface” on page 43
- “Customizing the Interface” on page 49
- “Managing the PRTK Services” on page 51
- “Starting DNA” on page 54
- “DNA Management Interface” on page 55
- “DNA Worker Interface” on page 59
Starting PRTK

To start PRTK, select **Start**, then **Programs**, then **AccessData**, then **Password Recovery Toolkit 6**, and then **PRTK 6**.

PRTK uses services to handle password recovery functions. The services must be running for PRTK to run successfully. Typically, the services are started when PRTK is started, and the services are stopped when PRTK is stopped.

**Note:** To run the services and PRTK successfully, you must be logged in as an administrator with sufficient rights.

For more information, refer to “Managing the PRTK Services” on page 51.

When starting, PRTK searches for a dongle, which is a security-compliance device. If you do not have a dongle or if the dongle drivers are not installed correctly, then the product runs in demo mode.

The full version of PRTK requires a dongle for security management. Consequently, when you run PRTK without a dongle, you can only use the demo version of the product.

When starting, PRTK attempts to establish communication with PRTK services. If PRTK cannot successfully communicate with the services, then the product displays the following dialog:

![Password Recovery Toolkit](image)

`Unable to connect to the PRTK Engine. Verify the service is started and retry.`

In this case, you must start or restart the PRTK services. See “Starting, Stopping, or Restarting a Service” on page 54.
Using the Dongle

To prevent unauthorized use of your software and to operate fully, PRTK requires a dongle. If you purchase the full PRTK package, AccessData provides a parallel or USB dongle with the product package.

The dongle is a security-compliance device that you insert into a parallel or USB port only when prompted during the installation of the dongle drivers. It maintains your PRTK licensing and subscription information and is required to use PRTK fully.

**Note:** AccessData supports USB dongles, but will support parallel dongles on request.

For information on installing the dongle drivers, see “If you have a USB dongle, plug it in.” on page 18 or “Installing the Dongle Drivers from Downloadable Files” on page 21.

Typically, FTK, PRTK, and the Registry Viewer reside on the same dongle. This configuration assumes that you are running the products on a single machine. (You can only use one security-compliance device on a computer.) If you prefer to run the products on separate machines, you can order an additional dongle for a nominal fee. For more information, contact AccessData at http://www.accessdata.com.

**Note:** Running FTK, PRTK, and the Registry Viewer on a single machine facilitates interaction between the products. For example, FTK 1.50b and above has an option to automatically decrypt EFS files using PRTK. As long as FTK and PRTK are on the same dongle on the same machine, PRTK automatically decrypts these files for FTK. If you run the products on different machines, you lose this integrated functionality.

Once you install the dongle and the dongle drivers, you can use LicenseManager to manage your product licenses. For more information, see “Managing Licenses” on page 181.
Running PRTK in Demo Mode

The full version of PRTK requires a dongle for security management. Consequently, when you run PRTK without a dongle, you can only use the demo version of the product.

If you do not use a dongle, you cannot use licensed password recovery modules to recover passwords.

The demo version includes the following:

- Executable File (Zip Self-extractor) Dictionary Attack
- Old Format PGP Secret Key Ring Dictionary Attack
- PGP Disk 4.0/5.0/6.0 Dictionary Attack
- PGP Secret Key Ring Dictionary Attack
- Win95/98 Screensaver Settings
- Zip Archive Dictionary Attack

Viewing Module Information

You can view information about password recovery modules, including information about module names, display names, attack types, and supported products and versions.

To view module information, click Help, and then Recovery Modules.
Touring the Interface

The PRTK interface consists of the PRTK Window, the Menu bar, the Toolbar, the Status bar, and the Properties bar.

The following sections discuss elements of the PRTK interface:

- “The Menu Bar” on page 44
- “The Toolbar” on page 46
- “The Status Bar” on page 47
- “The Properties Bar” on page 47
- “Right-click Menus” on page 49

The PRTK Window

The PRTK Window displays the files that are being processed in the current session, along with some of their individual file attributes.

The following table describes the file attributes listed in the PRTK window:

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>Path and filename of the file</td>
</tr>
</tbody>
</table>
PRTK allows you to select which file attributes you want to appear in the PRTK window and the order in which they appear. You can also change the file sort order. For more information, see “Changing the Sort Order in the PRTK Window” on page 49.

### The Menu Bar

The Menu bar in the PRTK window lets you access product features.

The following table provides descriptions of the items found in the Menu bar:

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Menu</td>
<td>Print, Print Preview, and Exit. Print a report of the files in the password recovery. Preview the report page by page and zoom in or out to view details. Close the PRTK program.</td>
</tr>
<tr>
<td>Edit Menu</td>
<td>Dictionaries, Levels, Profiles, Find, Find Next, Select All, and Preferences. Customize dictionaries, levels, and profiles. Find specific information in password recoveries. Edit preferences for recovery options, thresholds, and logging.</td>
</tr>
<tr>
<td>Menu Item</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| View Menu   | Toolbar, Status Bar, Properties Bar, Reset Positions, and File Properties.  
Hide or show the Toolbar, Status Bar, and Properties Bar. View file properties, including job and progress information. |
| Analyze Menu| Select Files, Select Drives or Folders, Verify Hashes, Pause All, Resume All, and Delete All.  
Select all files to control the recovery progress (pause all, resume all, delete all) and to view file properties. Verify hashes of files. Manage the password recovery process of all files. |
| Tools Menu  | Passphrase Generator.  
Use tools included with PRTK to create phrases based on websites or content of a specified document. |
View online help. Link to support on the web, Start LicenseManager. Select a language to use when using PRTK. View information for Password Recovery Modules. View information about PRTK (including product version, copyright, subscription renewal date, dongle number, and AccessData support contact information). |
The Toolbar

The Toolbar provides easy access to various functions in PRTK.

The following table shows each Toolbar icon and describes its function:

<table>
<thead>
<tr>
<th>Toolbar Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Print file information</td>
<td>Print the file information for files in the recovery session.</td>
</tr>
<tr>
<td>Select files to add</td>
<td>Select files to add to the recovery session.</td>
</tr>
<tr>
<td>Select drives/folders</td>
<td>Select drives/folders to add to the recovery session.</td>
</tr>
<tr>
<td>Pause recoveries</td>
<td>Pause all active recoveries.</td>
</tr>
<tr>
<td>Resume recoveries</td>
<td>Resume all paused or waiting recoveries.</td>
</tr>
<tr>
<td>Delete recoveries</td>
<td>Delete all active recoveries.</td>
</tr>
<tr>
<td>Manage profiles</td>
<td>Manage profiles.</td>
</tr>
<tr>
<td>Manage dictionaries</td>
<td>Manage dictionaries to use in profiles.</td>
</tr>
<tr>
<td>Verify hash values</td>
<td>Verify hash values of files.</td>
</tr>
<tr>
<td>View recovery details</td>
<td>View file recovery details.</td>
</tr>
<tr>
<td>Access Help</td>
<td>Access Help information.</td>
</tr>
</tbody>
</table>
The Status Bar

The Status bar at the bottom of the PRTK window shows descriptions for the Toolbar icons (when hovering the mouse cursor over them), thresholds for the password recovery process, and the number of files in the PRTK window.

The Properties Bar

The Properties bar shows some attributes of the selected file in the PRTK window.

The following table describes the file attributes listed in the Properties bar for a selected file:

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Attribute Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>Path and filename of the file</td>
</tr>
<tr>
<td>Attack Type</td>
<td>Attack type based on password recovery or decryption method (decryption or dictionary)</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Attribute Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Module</td>
<td>Name of password recovery module</td>
</tr>
<tr>
<td>Profile</td>
<td>Name of profile used with job</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the password recovery process (finished, running, depends on, paused, waiting)</td>
</tr>
<tr>
<td>Difficulty</td>
<td>Easy, moderate, or difficult password recovery</td>
</tr>
<tr>
<td>Begin Time</td>
<td>Start time of recovery process</td>
</tr>
<tr>
<td>End Time</td>
<td>End time of recovery process</td>
</tr>
<tr>
<td>Decryptable</td>
<td>Decryption method can be used on file</td>
</tr>
<tr>
<td>Result Type</td>
<td>Type of result</td>
</tr>
<tr>
<td>Results</td>
<td>Results of the password recovery</td>
</tr>
<tr>
<td>Comments</td>
<td>Specific comments you entered about the file</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Adding Comments to a Job” on page 94.</td>
</tr>
<tr>
<td>Filename</td>
<td>Path and filename of the file</td>
</tr>
<tr>
<td>Type</td>
<td>File type based on analysis of file</td>
</tr>
<tr>
<td>Version</td>
<td>Version of source application based on analysis of file</td>
</tr>
<tr>
<td>Size</td>
<td>File size</td>
</tr>
<tr>
<td>MD5</td>
<td>MD5 (128-bit) hash of the file contents</td>
</tr>
<tr>
<td>SHA-1</td>
<td>SHA (160-bit) hash of the file contents</td>
</tr>
<tr>
<td>Created</td>
<td>Date and time file was created</td>
</tr>
<tr>
<td>Modified</td>
<td>Date and time file was last modified</td>
</tr>
</tbody>
</table>

To view more attributes, double-click the selected file. See “Monitoring Jobs” on page 85.
Right-click Menus

Throughout the interface you can right-click the mouse to see features specific to the tasks you are performing.

Customizing the Interface

You can customize several aspects of the interface to fit your needs or preferences.

Changing the Sort Order in the PRTK Window

PRTK lets you sort files by their file properties.

To change the sort order, click the file property heading of the column you want to sort by.

Sizing Column Headings in the PRTK Window

You can resize the columns in the PRTK Window.

To resize a column heading, click and drag a column heading separator. The mouse cursor changes when you hover it over the separator between column headings.

Showing or Hiding the Bars

You can show or hide the Toolbar, Status bar, and Properties Bar.

To show or hide a bar, click View, and then Toolbar or Status Bar or Properties Bar.

Reset the Bars’ Positions

You can return the Toolbar, Status bar, and Properties Bar to their default positions.

To reset the positions, click View, and then Reset Positions.
Docking the Toolbar

You can position or dock the Toolbar to any side of the PRTK window or you can float the Toolbar.

To position the Toolbar, click the background area of the Toolbar; then drag the Toolbar where you want it.

Docking the Properties Bar

You can position or “dock” the Properties bar to any side of the PRTK window or you can float the Properties bar.

To position the Properties bar, click the background area of the Properties bar; then drag the Properties bar where you want it.

Selecting a Language with Language Selector

Using Language Selector, you can specify the language you want PRTK to display in its interface.

To select a language:

1. Select Help, and then Select Language or select Start, then Programs, then AccessData, then LanguageSelector, and then LanguageSelector.

2. From the list of supported languages, select the language you want.

3. Click Save Settings.

4. Click File, and then Exit to close Language Selector.
Managing the PRTK Services

PRTK uses services to handle password recovery functions. The PRTK services run as Windows services in the background. The services must be running for PRTK to run successfully.

**Note:** To run the services and PRTK successfully, you must be logged in as an administrator with sufficient rights.

The following table lists the PRTK services and describes what the services do:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessData PRTK 6 Database</td>
<td>Communicates with the database to persistently store session jobs and passwords. Communicates passwords with Worker service.</td>
</tr>
<tr>
<td>AccessData PRTK 6 Supervisor</td>
<td>Establishes connection between the PRTK program and the database. Supervises processes assigned to Worker service.</td>
</tr>
<tr>
<td>AccessData PRTK 6 Worker</td>
<td>Performs PRTK tasks assigned by Supervisor service.</td>
</tr>
</tbody>
</table>

For PRTK to function successfully, the services must be started and properly configured. You can use the Windows Services tool to manage and troubleshoot the PRTK services. See “Using the Windows Services Tool” on page 52.

**Note:** To manage the PRTK services, you must be logged in as an administrator.

For information about opening the Windows Services tool, see “Opening Services” on page 53.
Using the Windows Services Tool

Using the Windows Services tool, you can manage the services in the following ways:

- Start, stop, or restart a service.
  See “Starting, Stopping, or Restarting a Service” on page 54.

- Configure the account used by a service.
  The PRTK services are installed to log on using the Local System account. If necessary, you can change the logon account and specify a password.

- Set up recovery actions to take place if a service fails to start.
  For example, you can restart a service automatically or restart the computer (on computers running Windows XP or Windows 2000 only).

- Check the Windows Event Viewer
  The Windows Event Viewer displays messages regarding programs in Windows.

- Verify that a service is starting without user intervention when running PRTK
  The PRTK services are configured to start and stop when PRTK is started and stopped.
  See “Starting, Stopping, or Restarting a Service” on page 54.

- Use caution when changing default settings for a service.
  Changing the default settings for services might prevent key services from running correctly. It is especially important to use caution when changing the Startup Type and Log On As settings of services that are configured to start automatically.

  Changing the default service properties might prevent the program from running correctly. In particular, use caution when changing the default Startup type and Log On settings for any of the PRTK services—they are configured to start and (typically) log on only when running PRTK.
Check the Log file.

If you are directed by Customer Support to log recovery information, check the log file for indications of problems with a service.

Opening Services

You can use several methods to open Services.

To open Services:

1. Do one of the following:
   - From the Start menu on the Windows 2000 desktop, select Settings, then Control Panel, then Administrative Tools, and then Services.
   - From Windows XP, select Start, then Control Panel, then Performance and Maintenance, then Administrative Tools; then double-click Services.
   - From the Start menu on the Windows desktop, click Run. In the Open text field, type services.msc; then click OK.

2. Scroll the list of services until you see an AccessData service under the Name column.

   See “Starting, Stopping, or Restarting a Service” on page 54.
Starting, Stopping, or Restarting a Service

To start, stop, or restart a service, you must be logged in as an administrator. (If your computer is connected to a network, network policy settings might prevent you from completing these tasks.)

Some instances of when you might need to start, stop, or restart a service include the following:

- **Start or Restart**: If the program is unable to authenticate or connect.
- **Restart**: You have just changed login settings to a service, or the program has stopped working.
- **Stop**: You believe a service might be causing a problem on the computer, or you want to temporarily free memory resources.

**Important**: Stopping a service prevents PRTK from processing recovery jobs in the PRTK window.

To start, stop, or restart a service:

1. From a Services window, under the Name column, select an AccessData service. See “Opening Services” on page 53.
2. Select one of the following:
   - **Action**, then **Start**
   - **Action**, then **Stop**
   - **Action**, then **Restart**

Starting DNA

To start DNA after you complete the installation:

1. Select **Start**, then **Programs**, then **AccessData**, then **DNA 3**, and then **Supervisor**.
   
   By default, DNA starts automatically when the computer is started. If DNA does not start, complete this step.
2. In the Login form, complete the following:
2a Leave the Password field blank.

By default, there is no password to log in. To change the password, see “Changing the Administrator and User Passwords” on page 160.

2b In the Server drop-down list, select the desired server connection. If you are on a supervisor machine and want to authenticate to the machine itself, select the name of the supervisor from the drop-down list.

In the Port field, enter the desired port number connection. The default port for the supervisor is 49170.

**DNA Management Interface**

With the management interface, you can monitor each job and each worker in the system.

The default management interface is divided into Priority Groups, a job queue, and a Worker List, which are discussed in the following sections. The bottom row of the interface, shown below, displays information about the current status of the server.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNA Version</td>
<td>The version of DNA that the supervisor is currently running.</td>
</tr>
<tr>
<td>Connection</td>
<td>The status of the connection to the DNA database.</td>
</tr>
<tr>
<td>Refresh</td>
<td>The time in seconds until the statistics are updated on the management interface.</td>
</tr>
</tbody>
</table>

To change the refresh rate, see “Changing the Management Interface Refresh Rate” on page 154.
Priority Groups

The Priority Groups list is used to rank jobs by importance. The list displays the priority groups in DNA and the percentage of all available resources working on each priority. The following table describes all groups in the Priority Groups list.

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>The most urgent priority group for jobs in DNA. Jobs classified in this priority group are processed according to the order they are added to the group.</td>
</tr>
<tr>
<td>Normal</td>
<td>The basic priority group in DNA. Jobs classified in this priority group are processed according to the order they are added to the group. By default, 10% of all available resources in the group or DNA system process jobs in the Normal group.</td>
</tr>
<tr>
<td>Waiting</td>
<td>The group for jobs that are paused or waiting for another job to complete, or that have timed out. Jobs move out of this group after their processing is resumed.</td>
</tr>
<tr>
<td>Finished</td>
<td>The group that displays all processed jobs.</td>
</tr>
</tbody>
</table>

Job Queue

The job queue is the section of the management interface that displays varying levels of information about each job that is decrypted. You can select the following different views for the job queue:

- Small icons: Displays each job as a small icon with the icons reading left to right.
- Large icons: Displays each job as a large icon with the icons reading left to right.
- List: Displays each job as small icons with the icons reading top to bottom.
Details: Displays nine categories of information about each job.

The following table describes all columns in the Details view:

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the job in DNA. The job name can be different than the filename of the job. Each job is listed once for each type of attack that is performed on the job.</td>
</tr>
<tr>
<td>Attack Type</td>
<td>The attack type used to decrypt the file. The following are the possible attack types:</td>
</tr>
<tr>
<td></td>
<td>• Dictionary</td>
</tr>
<tr>
<td></td>
<td>• Decryption</td>
</tr>
<tr>
<td></td>
<td>• Keyspace</td>
</tr>
<tr>
<td></td>
<td>• Reset</td>
</tr>
<tr>
<td></td>
<td>If DNA is using either the dictionary or keyspace attack, more specific information is listed about the type of attack being used.</td>
</tr>
<tr>
<td></td>
<td>For more information on the attack types, see “Understanding the DNA Decryption Process” on page 11.</td>
</tr>
<tr>
<td>Filename</td>
<td>The complete name of the encrypted file, including the full path to the file and the file extension.</td>
</tr>
<tr>
<td>File Type</td>
<td>The application in which the encrypted file was created.</td>
</tr>
<tr>
<td>Begin Time</td>
<td>The date and time that the DNA system started working on the job. If you specify a timeout value during the job wizard, an asterisk (*) appears in this column for the first password attack on a file. For more information, see “Adding a Job” on page 80.</td>
</tr>
<tr>
<td>End Time</td>
<td>The date and time that the DNA system finished working on the job.</td>
</tr>
</tbody>
</table>
Worker Summary

The Work Summary displays information about each supervisor or worker in the DNA system. If you are on a supervisor machine, you only see the workers assigned to that supervisor.

The top row of the summary, shown below, displays filtering options that you can use to filter the machines listed in the

<table>
<thead>
<tr>
<th>Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the job. The following are the possible statuses:</td>
</tr>
<tr>
<td></td>
<td>• Depends On: The job is dependent upon the completion and results of another job before it can start its processing.</td>
</tr>
<tr>
<td></td>
<td>• Expired: The job timed out, according to the time limit you specified when you added the job.</td>
</tr>
<tr>
<td></td>
<td>• Finished No Passwords Found: The job is completed and no passwords were found.</td>
</tr>
<tr>
<td></td>
<td>• Finished password: The job is completed and the password is displayed. If the password contains a space, &lt;space&gt; displays in the appropriate location, for example, AccessData&lt;space&gt;Corporation.</td>
</tr>
<tr>
<td></td>
<td>• Paused: The job is paused on the DNA management interface.</td>
</tr>
<tr>
<td></td>
<td>• Queued: The job is not yet assigned to a group.</td>
</tr>
<tr>
<td></td>
<td>• Running: The job is being processed by DNA.</td>
</tr>
<tr>
<td></td>
<td>• Waiting On: The job is dependent upon the completion or timeout of another job before it can start its processing.</td>
</tr>
<tr>
<td>Priority Group</td>
<td>The priority group that the job is assigned to. If the job has been processed, then this column lists the priority group in which the job was processed.</td>
</tr>
<tr>
<td>Priority (%)</td>
<td>The percentage of available resources in the DNA system that processed the job.</td>
</tr>
</tbody>
</table>
queue. For more information on filtering, see “Filtering the Worker List” on page 108.

The bottom row of the queue, shown below, displays a button to manage groups and connection information about the supervisors or workers. For more information about groups, see “Managing Supervisors, Workers, and Groups” on page 107.

The following table describes all columns in the queue:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The computer name of the DNA Supervisor or Worker.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP Address IP address of the DNA Supervisor or Worker. It might be a static address that has</td>
</tr>
<tr>
<td></td>
<td>been previously assigned or a dynamic address from a DHCP server.</td>
</tr>
<tr>
<td>Processors</td>
<td>The total number of physical processors on the DNA Supervisor or Worker machine.</td>
</tr>
<tr>
<td>Connected</td>
<td>Y or N, depending on whether the DNA Supervisor or Worker is connected to the Supervisor. Green</td>
</tr>
<tr>
<td></td>
<td>indicates a connection, while red indicates that the worker is disconnected or unavailable.</td>
</tr>
<tr>
<td>Last Contact Time</td>
<td>The last time the DNA Supervisor contacted the Worker.</td>
</tr>
<tr>
<td>Working On</td>
<td>The job and attack type that the DNA Supervisor or Worker is currently processing. If DNA is</td>
</tr>
<tr>
<td></td>
<td>using either the dictionary or keyspace attack, more specific information is listed about the</td>
</tr>
<tr>
<td></td>
<td>type of attack being used.</td>
</tr>
<tr>
<td>Groups</td>
<td>Names of groups that the DNA Supervisor or Worker belongs to.</td>
</tr>
</tbody>
</table>

**DNA Worker Interface**

You can track DNA Worker statistics on each worker machine. A graphic-based interface is available on Windows.
workstations. A text-based interface is available on Macintosh and Linux machines. This section contains the following information:

- “DNA Worker Interface on a Windows Workstation” on page 67
- “DNA Worker on a Macintosh or Linux Machine” on page 69

To access more statistics about each worker, see “Monitoring a DNA Supervisor or Worker” on page 109.

DNA Worker Interface on a Windows Workstation

On Windows workstations, you can access the DNA Worker interface by clicking the DNA Worker icon in the Taskbar.

If you have performed a stealth installation of the worker, you can access the DNA Worker interface by double-clicking **Worker.exe** in the DNA \Worker\ directory. The following table describes each component of the DNA Worker interface:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>Yes or No, depending on whether the DNA Worker is connected to the supervisor.</td>
</tr>
<tr>
<td>Supervisor Hostname</td>
<td>The computer name of the DNA Supervisor to which the DNA Worker is subordinate.</td>
</tr>
</tbody>
</table>
DNA Worker on a Macintosh or Linux Machine

To access a text-based DNA Worker interface on a Macintosh or Linux machine, complete the following:

1. At the command line of the machine, go to the `/opt/Accessdata DNA3/Worker` directory.

2. Type `. /dna3workerd status`

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supervisor IP Address</td>
<td>IP address of the DNA Supervisor to which the DNA Worker is subordinate. It might be a static address that has been previously assigned or a dynamic address from a DHCP server.</td>
</tr>
<tr>
<td>Working Processors</td>
<td>The number of physical processors on the DNA Worker machine that are working on DNA jobs.</td>
</tr>
<tr>
<td>Idle Processors</td>
<td>The number of physical processors on the DNA Worker machine that are not working on DNA jobs.</td>
</tr>
<tr>
<td>Power</td>
<td>The speed of the machine’s physical processors.</td>
</tr>
<tr>
<td>Last Contact Time</td>
<td>The last date and time the supervisor contacted the DNA Worker.</td>
</tr>
</tbody>
</table>
| Elapsed Idle or Running Time | For Elapsed Idle Time, the amount of time (minutes and seconds) that has passed since the DNA Worker processed its last job.  
                          | For Elapsed Running Time, the amount of time (minutes and seconds) that the DNA Worker has been processing its job. |
| Release                  | The version of the DNA Worker that the machine is running.                                       |
| Restart                  | Prompts to either restart the DNA Worker or cancel restarting. You might restart the DNA Worker if the supervisor has lost connection with it. |
| About                    | Displays the version of DNA that the machine is running.                                         |
| Close                    | Closes the DNA Worker interface.                                                                |
The following table describes each component of the DNA Worker interface:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>Yes or No, depending on whether the DNA Worker is connected to the supervisor. Green indicates a connection, while red indicates that the worker is unavailable or disconnected.</td>
</tr>
<tr>
<td>Supervisor Hostname</td>
<td>The computer name of the DNA Supervisor to which the DNA Worker is subordinate.</td>
</tr>
<tr>
<td>Supervisor IP Address</td>
<td>IP address of the DNA Supervisor to which the DNA Worker is subordinate. It might be a static address that has been previously assigned or a dynamic address from a DHCP server.</td>
</tr>
<tr>
<td>Working Processors</td>
<td>The number of physical processors on the DNA Worker machine that are working on DNA jobs.</td>
</tr>
<tr>
<td>Idle Processors</td>
<td>The number of physical processors on the DNA Worker machine that are not working on DNA jobs.</td>
</tr>
<tr>
<td>Power</td>
<td>The speed of the machine’s physical processors.</td>
</tr>
<tr>
<td>Last Contact Time</td>
<td>The last date and time the supervisor contacted the DNA Worker.</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Elapsed Idle or Running Time</td>
<td>For Elapsed Idle Time, the amount of time (minutes and seconds) that has passed since the DNA Worker processed its last job.</td>
</tr>
<tr>
<td></td>
<td>For Elapsed Running Time, the amount of time (minutes and seconds) that the DNA Worker has been processing its job.</td>
</tr>
<tr>
<td>Release</td>
<td>The version of the DNA Worker that the machine is running.</td>
</tr>
<tr>
<td>Restart</td>
<td>Prompts to either restart the DNA Worker or cancel restarting. You might restart the DNA Worker if the supervisor has lost connection with it.</td>
</tr>
</tbody>
</table>
Managing System Configurations

In DNA, management tasks include backing up the keys used for communication, customizing the DNA management interface, and changing passwords to access the interface.

This chapter contains the following sections:

- “Customizing the Management Interface” on page 152
- “Changing the Management Interface Refresh Rate” on page 154
- “Disconnecting from and Connecting to the DNA Database” on page 154
- “Restarting the Worker” on page 156
- “Backing Up and Restoring Keys” on page 157
- “Changing the Administrator and User Passwords” on page 160
- “Selecting a Language for AccessData Products” on page 161

Customizing the Management Interface

You can customize both the look and content of the management interface.

For example, you might change the look and content of the interface if you want to focus on specific information, such as detailed information on all jobs in the DNA system.
The management interface is divided into three panes: Priority Groups, the job queue, and the Worker List.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View: Small Icons</td>
<td>Displays each job as a small icon, with the icons reading left to right.</td>
</tr>
<tr>
<td>View: Large Icons</td>
<td>Displays each job as a large icon, with the icons reading left to right.</td>
</tr>
<tr>
<td>View: List</td>
<td>Displays each job as a small icon, with the icons reading top to bottom.</td>
</tr>
<tr>
<td>View: Details</td>
<td>Displays nine categories of information about each job on the DNA system.</td>
</tr>
<tr>
<td></td>
<td>For more information about each column in the Details view, see “Job Queue” on page 64.</td>
</tr>
</tbody>
</table>
By default, the interface automatically displays Priority Groups, Details, and Workers.

To customize the content of the management interface:

1. Click View and select the options that you want to display in the interface. The settings that you select are saved even after the DNA management interface is closed.

2. If you want to return the dockable frames to the default positions, select Reset Positions.

Changing the Management Interface Refresh Rate

By default, the DNA management interface refreshes itself every 10 seconds. You can either increase or decrease the refresh rate.

You might increase the refresh rate if changes to the jobs or workers on the DNA system are minimal. You might decrease the refresh rate if you want to closely monitor the progress of jobs or workers.

To change the interface refresh rate:

1. Select Edit, and then Preferences.

2. In the Default Refresh Time field, click the arrows to increase or decrease the refresh rate. The shortest refresh rate is five seconds. The longest refresh rate is 30 seconds.

3. Click OK.
Note: Refreshing a large amount of workers may take longer than the time selected.

Disconnecting from and Connecting to the DNA Database

You might want to temporarily disconnect from the DNA database to run maintenance procedures either on DNA or the machine itself.

To disconnect from the DNA database, select File, and then Disconnect.

After you finish the maintenance procedures, you must reconnect to the DNA database.

To connect to the DNA database:

1. Select File, and then Connect.

2. In the Login form, complete the following:
   2a. In the Password field, enter the password. By default, the password is blank. To change the password, see “Changing the Administrator and User Passwords” on page 160.
   2b. In the Server drop-down list, select the name of the machine that you are using. Re-connect to the DNA database that is on the local machine.
   2c. In the Port field, enter the desired port number connection. The default port for the supervisor is 49170.

Restarting the Supervisor

You can restart the supervisor connection. You might restart the supervisor to refresh the connection with it.

To restart the supervisor:

1. Select File, then Restart, and then Yes. DNA attempts to connect to the DNA database for 10 seconds.

2. In the Login form, enter the authentication information to log in to the supervisor; then click Login.
You are prompted to authenticate only if DNA cannot automatically establish a connection with the DNA database.

Restarting the Worker

You can restart a DNA Worker to re-establish its connection. You might need to restart a worker if current statistics are not available in the Workers queue.

**WARNING!** Do not restart the worker if you know it is currently processing jobs. If you restart the worker while it is processing a DNA job, then the work already completed on the job will be lost.

To restart a DNA Worker from the management interface:

1. In the Workers queue, select the worker you want to restart.
2. Right-click and select Restart. If the DNA Worker no longer displays in the Workers queue and you know that the worker machine is running, you need to restart the DNA Worker on its machine.

To restart a DNA Worker from its machine:

1. On a Windows workstation, complete the following:
   1a. In the Taskbar, right-click the DNA Worker icon and select Open.
   1b. Click **Restart**.
2. On a Macintosh or Linux machine, complete the following:
   2a. At the command line of the machine, go to the `/opt/Accessdata/DNA3/Worker` directory.
   2b. Type `/dna3workerd restart`

Backing Up and Restoring Keys

During the DNA Supervisor installation, a public and private key pair is generated. This key pair is used when a communications session is initiated between the DNA Supervisor and a DNA Worker. After the initial
communication, a session key is created and used to secure communication for the rest of that session.

Backing Up Keys

You can back up the key pair on the supervisor as a preventive measure against data loss. Backing up keys is also useful if you need to re-install either the supervisor.

The backup keys can be restored to maintain communication with the current supervisors. The User Guide backup keys can be restored to a supervisor to maintain the communication with the current DNA Workers. For information on restoring keys, see “Restoring Keys” on page 159.

If you re-install the supervisor without backing up and then restoring keys, the supervisor will lose communication with its workers.

Note: You can use the backup keys for a partial installation of DNA. Before you start the installation, you must complete a partial un-install. If you perform a completely new install, new keys are created.

To back up the keys:

1. Select Tools, and then Backup Keys.
2. Browse to and select the location for the backup; then click OK, and then OK. The file supervisor.ini is saved to the selected location.

Restoring Keys

You can restore the key pair to the supervisor if you experience a loss of data. For example, if the entire system or a hard drive is lost on the DNA Supervisor, you can install a new version of DNA and restore the backup keys. As long as the hostname or IP address of the supervisor remains the same, the supervisors and workers do not have to change any configuration to work with the restored system.

To restore the keys:

1. Select Tools, and then Restore Keys.
2 Browse to and select the location of mastercontroller.ini or supervisor.ini; then click OK, and then OK.

Changing the Administrator and User Passwords

You can change both the administrator and user passwords on the Change Password form. The administrator password grants full administrative rights to the DNA system. The user password grants full administrative rights to the DNA system with the following exception: A user cannot change the administrator or user passwords.

By default, both the administrator password and the user password are blank. You might want to define passwords to maintain the security of the DNA system.

To change the administrator and user passwords:

1 Select Edit, then Preferences, and then Change Password.

2 Enter the administrator password for the machine. You must enter the password in this field in order to authenticate to DNA and make any subsequent password changes.

3 To change the administrator password:
   3a In Admin Password, check the Change box.
   3b Enter the new administrator password in both fields.

4 To change the user password:
   4a In User Password, check the Change box.
   4b Enter the new user password in both fields.

5 Click Submit.

Selecting a Language for AccessData Products

You can select the default language for all AccessData products. The default language is displayed in the product interfaces as long as you already have the associated language DLLs on the machine.

To select a default language:
1 Select **Help**, and then **Select Language**. Or select **Start**, then **Programs**, then **AccessData**, and then **LanguageSelector**.

2 In the Language drop down list, select the language that you want.

3 Click **Save Settings**.

4 Click **File**, and then **Exit**.

5 Restart the AccessData application.
Recovering Passwords

Password Recovery Toolkit (PRTK) lets you add files you want to recover, monitor recovery jobs, view recovery results, verify hashes, and print recovery reports.

This chapter contains the following sections:

- “Recovery Process Overview” on page 74
- “Adding Jobs” on page 76
- “Add Job Processing Results” on page 79
- “Managing the Recovery Process” on page 79
- “Specifying Recovery Preferences” on page 81
- “Monitoring Jobs” on page 85
- “Verifying Hashes” on page 94
- “Printing Recovery Reports” on page 95
Recovery Process Overview

You can add files to be recovered by selecting files, dragging and dropping files, or searching drives or folders.

When you add a file or a group of files to PRTK, a “job” is started. For each job, PRTK analyzes the files to verify whether the files can be recovered and to identify the modules to use and the attack types to perform.

For certain files, a Module Options dialog displays the options you can select to define the recovery settings to use based on the type of file, its version, and the attacks available to be performed on the file. If necessary, you can deselect the attacks you don’t want performed on each job.

Note: Some password recoveries are specialized and require additional steps. See “Specialized Password Recoveries” on page 163.

Each job must be associated with a profile, which will be used during the recovery process. A profile contains the dictionaries and levels to use for the recovery process. You can associate your job with the default profile, or you can create your own
customized profile. For more information, see “Setting a Default Profile” on page 124.

Note: When adding multiple jobs, you can select or define only one profile. If you want the files to be processed with different profiles, add each job individually.

After you select a profile, PRTK generates the job process, adds the file to the list of jobs in the PRTK window, and displays the processing results. See “Add Job Processing Results” on page 79.

Important: After you start a job, do not move the files PRTK is working on. While PRTK works on jobs, you can continue to add files.
Best Practices for Adding Jobs

To maintain system performance, AccessData recommends the following:

- Do not add more than 50 files at one time.
- If a desired file on the network is larger than 10 MB, copy the file to the local machine and then add it locally.
- Do not run a job on network drives or folders. Processing files across the network generates a large amount of network traffic.
- Set default recovery threshold preferences in accordance with the processing capability and memory of the computer. See “Specifying Recovery Thresholds” on page 83.

**WARNING!** Never set the recovery threshold preference to zero (0). When set to zero, the jobs are queued but never processed.

Adding Jobs

You can add files to be recovered by selecting files, dragging and dropping files, or searching drives or folders. The following sections describe how to add recovery jobs.

Selecting Files

You can add files to be recovered by selecting files.

For recommendations about adding files, see “Best Practices for Adding Jobs” on page 76.

To select files as a recovery job:

1. From the menu bar, select **Analyze**, and then **Select Files**.
2. Select the file or files you want to add as a job.
   - Press **Shift+click** to select multiple contiguous files. Press **Ctrl+click** to select multiple discontiguous files.
3. Click **Open**.
   - PRTK analyzes the files.

---

76 Password Recovery Toolkit User Guide
4 (Conditional) In the Module Options dialog, specify the module options you want for each file; then click **OK**.

5 Select the profile you want to use on files in the password recovery job; then click **OK**.

PRTK generates the recovery process settings for the job and displays the processing results. See “Add Job Processing Results” on page 79.

**Dragging and Dropping Files**

You can add files to be recovered by dragging and dropping files into PRTK.

For recommendations about adding files, see “Best Practices for Adding Jobs” on page 76.

To drag and drop files as a recovery job:

1 In Windows Explorer, select the file or files you want to add as a job.

   Press **Shift+click** to select multiple contiguous files. Press **Ctrl+click** to select multiple discontiguous files.

2 Drag and drop the selected file or files into PRTK.

   PRTK analyzes the files.

3 (Conditional) In the Module Options dialog, specify the module options you want for each file; then click **OK**.

4 Select the profile you want to use on files in the password recovery job; then click **OK**.

   PRTK generates the recovery process settings for the job and displays the processing results. See “Add Job Processing Results” on page 79.
Searching Drives or Folders

You can add files to be recovered by searching drives or folders for files to add to PRTK.

For recommendations about adding files, see “Best Practices for Adding Jobs” on page 76.

To search for files to add as a recovery job:

1. From the menu bar, select Analyze, and then Select Drives/Folders.
2. Select the drives or folders you want to add as a job.
   - Click “+” or “−” to expand or collapse drives.
3. Select the profile you want to use on files in the password recovery job; then click OK.
   - PRTK analyzes the files.
PRTK generates the recovery process settings for the job and displays the processing results. See “Add Job Processing Results” on page 79.

**Add Job Processing Results**

After processing jobs to be added, PRTK displays results in the Processing results dialog. The following are possible results:

- **Cancelled**: You canceled the processing of the job.
- **Corrupted**: The file is corrupted.
- **Failed to Process**: The file cannot be added to the system. This result is a general tag used for any file that cannot be classified as any other result.
- **File in Use**: The file is locked by another program.
- **Successfully Added**: The file is added to the job queue.
- **Timed Out**: The file cannot be identified by PRTK in five minutes. This result usually appears when PRTK is busy processing other jobs.
- **Unencrypted**: The file doesn’t need to be added because the file isn’t encrypted.
- **Unidentifiable**: PRTK cannot recognize the file and its source application.
- **Unsupported Version**: The file was created in an unsupported version of a supported application.

**Managing the Recovery Process**

PRTK lets you manage the recovery process of the jobs in the recovery session. This section reviews the tools you can use to manage the recovery session:

**Stopping and Starting the Recovery Session**

You can stop or start the recovery session by exiting or opening PRTK.
To close the session, select **File**, and then **Exit**.

When you run PRTK again, the recovery jobs in the session appear in the PRTK window.

**Note:** When recovering passwords, PRTK independently analyzes and tracks the progress of each file. Consequently, you can close a session before all of the password recoveries are completed and then open the session later to have PRTK resume the password recoveries.

### Pausing Job Processing

You can pause recovery processes for all jobs in the recovery session or for selected jobs only.

To pause recoveries for all jobs, select **Analyze**, and then **Pause All**.

To pause recoveries for selected jobs:

1. Select the jobs you want to pause.
2. Right-click a job; then click **Pause**.

### Resuming Job Processing

You can resume recovery processes for all jobs in the recovery session or for selected jobs only.

To resume recoveries for all jobs, select **Analyze**, and then **Resume All**.

To resume recoveries for selected jobs:

1. Select the jobs you want to resume.
2. Right-click a job; then click **Resume**.

### Removing Jobs

You can remove all jobs in the recovery session or selected jobs only.

To remove all jobs, select **Analyze**, and then **Delete All**.

To remove selected jobs:

1. Select the jobs you want to remove.
2 Right-click a job; then click **Delete**, or select the job and press the Delete key.

**Specifying Recovery Preferences**

You can set default recovery settings to use when processing jobs in the recovery session.

![Preferences](image)

To set default recovery settings, select **Edit**, and then **Preferences**.

The following table describes the default preference settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrypt file when key is found</td>
<td>Automatically decrypts files using a key when the key is recovered. Saves decrypted files in either the same directory as the encrypted file or in a specified directory. For an explanation of encrypted files, see “Understanding Encrypted Files” on page 254.</td>
</tr>
</tbody>
</table>
Saving Decrypted Files

You can specify that files are decrypted and saved automatically after PRTK recovers the decrypt key of a file.

To set recovery options:

1. Select **Edit**, and then **Preferences**.
2. Select **Decrypt file when key is found**.
3. Specify where to save decrypted files.
4. When finished, click **OK**.

For an explanation of encrypted files, see “Understanding Encrypted Files” on page 254.

Saving Decrypted Files Manually

After PRTK recovers the decrypt key of a file, you can manually decrypt and save the file.

To decrypt a file after recovering the key:

1. In the PRTK window, right-click a job that has a recovered decrypt key.
2. Select **Decrypt** from the menu.
3. Specify where to save the decrypted file.
For an explanation of encrypted files, see “Understanding Encrypted Files” on page 254.

Setting Up E-mail Notification

You can send an e-mail to an address using SMTP after the recovery process for a job is completed.

To set up e-mail notification:

1. Select Edit, and then Preferences.
2. Click Send an e-mail when a job has been completed.
3. Specify an e-mail address to send messages to.
   - Use a valid e-mail address such as someone@somewhere.com.
   - Send messages to multiple e-mail addresses by separating addresses with a comma.
4. Specify theSMTP server and port to use. Use a valid server name or IP address such as smtp.somewhere.com.
5. Click Test to verify the e-mail settings.
6. When finished, click OK.

Specifying Recovery Thresholds

You can specify how many easy, moderate, and difficult recoveries you want PRTK to perform at the same time.

If a threshold for a type is reached as jobs are being added, PRTK waits to process other jobs of that type until it completes processing current jobs of that type.

The settings apply to files when jobs are added to the session.

To set recovery thresholds:

1. Select Edit, and then Preferences.
2. Specify the number threshold for Easy, Moderate, and Difficult recovery levels.
3. When finished, click OK.
Playing Sounds for Recoveries

You can specify the sounds to play when a recovery is successful or unsuccessful.

To set sounds to play for recoveries:

1. Select **Edit**, and then **Preferences**.

2. Specify the sounds you want to use for successful or failed recoveries.
   
   Enter the path and file name of the .wav file, or click the browse button (…) to select the .wav file you want to use.
   
   For example, on Windows XP, you could play `drive:\Windows_directory\Media\tada.wav` for a successful recovery.

3. Test the sounds by clicking the **Play** button.

4. When finished, click **OK**.

Logging Recovery Progress Information

When troubleshooting PRTK, you can log recovery progress information to a log file when directed by customer support.

**Important:** Enable logging only when tracking recovery progress is essential and when sufficient space is available for the log file to increase in size. The log file can become very large.

To set up logging progress information:

1. Select **Edit**, and then **Preferences**.

2. Click **Logging**.

3. Click **Enable Logging**.

4. Specify the location, name, and extension of the log file.
   
   By default, if you only specify a filename, then the file is located in `drive:\Program Files\AccessData\PRTK 6`.

5. When finished, click **OK**.
To stop logging progress information, select Edit, then Preferences, then Logging, uncheck Enable Logging, and then click OK.

Monitoring Jobs

You can monitor jobs in several ways, including monitoring the password attacks or looking at statistics and graphical analysis of one job or selected jobs.

You can view some properties for jobs using the Properties Bar. See “The Properties Bar” on page 47.

Displaying Job Properties

You can view detailed statistical and graphical analysis of the jobs in the recovery session.

To view the properties for one job, do one of the following:

- Double-click the job you want.
- Select a job and press Enter.
- Right-click a job and select Properties.
- Select a job and click View, and then File Properties.

To view the properties for multiple jobs, do one of the following:

- Select the jobs and press Enter.
- Select the jobs, right-click a job, and select Properties.
- Select the jobs and click View, and then File Properties.

The Job Properties screen contains four windows organized as tabs, each with a particular focus or function. Each tab is discussed in the following sections. You can resize the Job Properties screen if desired.

Note: When viewing properties for multiple jobs, you can switch to view the properties of another file by clicking another file from the Name pull-down menu in either the Information tab or the Levels tab.

To close the Job Properties screen, click OK or Cancel.
The Information window displays basic job information and the results of the job processing.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The job name. If you selected multiple jobs in the job queue, select the job in the drop-down list that you want to view.</td>
</tr>
<tr>
<td>Comments</td>
<td>Any comments you entered in the Add Job Wizard, or any commands from the Job Properties screen.</td>
</tr>
</tbody>
</table>

The window is divided into four categories. Each category is discussed in the following sections.

**Basic Information**

The following table describes the Basic Information section:
**File Information**

The following table describes the File Information section:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>Filename of the job, including the full path to the file.</td>
</tr>
<tr>
<td>Type</td>
<td>Application that the file was created in.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the file format recognized by PRTK modules.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the file in bytes.</td>
</tr>
<tr>
<td>Created</td>
<td>Date and time that the file was originally created.</td>
</tr>
<tr>
<td>Modified</td>
<td>Date and time that the file was last modified.</td>
</tr>
<tr>
<td>MD5</td>
<td>MD5 (128-bit) hash of the file data.</td>
</tr>
<tr>
<td>SHA-1</td>
<td>SHA (160-bit) hash of the file data.</td>
</tr>
</tbody>
</table>

**Properties**

The following table describes the Properties section:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Type</td>
<td>Attack type used for this particular instance of the job.</td>
</tr>
<tr>
<td>Module</td>
<td>Recovery module used for the attack. The module is based on the file type, such as Word, and the attack type.</td>
</tr>
<tr>
<td>Profile</td>
<td>The profile assigned to the job during the Add Job Wizard.</td>
</tr>
</tbody>
</table>
Status  The status of the job.

The following are the possible states:

- **Depends On**: The job is dependent upon the completion and results of another job before it can start its processing.

- **Finished No Passwords Found**: The job is completed and no passwords were found.

- **Finished password**: The job is completed and the password is displayed. If the password contains a space, `<space>` displays in the appropriate location, for example, `AccessData<space>Corporation`.

- **Paused**: The job is paused.

- **Queued**: The job is not yet assigned for processing.

- **Running**: The job is being processed.

- **Waiting On**: The job is dependent upon the completion or timeout of another job before it can start its processing.

Begin Time  The date and time that PRTK begins processing the job.

End Time  The date and time that PRTK finishes processing the job.

Time Out  How long PRTK/DNA performs the dictionary attack before it times out and begins a different attack.

Groups  The groups to which the job is assigned.
**Results**

The Results section displays the passwords and keys that PRTK discovers during the decryption process.

The Results section might have multiple entries even if a password is discovered in the first entry. Some files, such as PDF documents, have multiple passwords. Even though one password is discovered, more tests might still be running on lower levels because PRTK is searching for the other passwords in the document.

The following table describes the Results section:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Either password or key, depending upon what PRTK decrypts first.</td>
</tr>
<tr>
<td>Data</td>
<td>The actual password or key that decrypts the file. If the password contains a space, <code>&lt;space&gt;</code> displays in the appropriate location; for example, <code>AccessData&lt;space&gt;Corporation</code>.</td>
</tr>
<tr>
<td>Description</td>
<td>The type of password or key that is found. The type is defined by the specific application that the file is encrypted in. The following are possible types: File, User, Owner, Administrator, Assistant, Reader, Definer, Supervisor, Spare, Possible, Read-Write, Service Website, Field, Write Reservation, Option Protect, Sheet, Save As, Title, Protection, Transaction, Data Entry, Payroll, Spare User, Pass Key, and Zip Key.</td>
</tr>
<tr>
<td>Found In</td>
<td>The level and corresponding dictionary that the password or key was discovered in.</td>
</tr>
</tbody>
</table>

**Levels**

The Levels window displays information about the recovery levels for a job. It also displays a graph that illustrates the
number of decryption attempts per recovery level and the progress of the attack.

You can zoom in on the graph to display a greater level of detail. Click the desired region and drag the mouse to create a rectangle that covers the area you want to see.
The following table describes the Levels window:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the job about which recovery level information is displayed. If you selected multiple jobs in the job queue, select the job in the drop-down list that you want to view.</td>
</tr>
<tr>
<td>Legend</td>
<td>A color key for the levels displayed in the graph. The following list describes each level:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unassigned</strong>: A level is not assigned until the previous level is completed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Assigned</strong>: The level is allocated to be processed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Completed</strong>: The level has been processed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Unassignable</strong>: The level has been allocated to another resource.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Failed</strong>: The level was assigned, but the program did not return the results.</td>
</tr>
<tr>
<td>ID</td>
<td>A number assigned by PRTK to each level.</td>
</tr>
<tr>
<td>Description</td>
<td>The level and corresponding dictionary that the level is run on.</td>
</tr>
<tr>
<td></td>
<td>If you do not want to display a level in the graph, right-click the level and select <strong>Skip</strong>. A skipped level is not processed by PRTK; PRTK immediately marks the skipped levels as completed.</td>
</tr>
<tr>
<td>Number Completed</td>
<td>The number and percentage of possible passwords or keys that have been tried in the particular level.</td>
</tr>
<tr>
<td>Size</td>
<td>The total number of possible passwords or keys in the particular level.</td>
</tr>
</tbody>
</table>

The Levels window graph can be displayed two different ways. By default, PRTK displays the graph with the **Logarithmic** box.
checked. The graph, shown above, displays great detail about how many tries are attempted at each recovery level. The graph reduces the number of tries that are shown so that you can see each attempt in greater detail.

If you uncheck the Logarithmic box, PRTK displays a larger-scale graph that displays a more general view of the level progress. An example of this type of graph is shown below. The non-logarithmic graphic displays the last few levels much larger than all the others. This type of graph displays the relationships between the levels more accurately.

Passwords/Second

The Passwords/Second window displays a graph of the number of passwords per second that are tested for validity over a given amount of time on the selected job. The bottom
of the window displays the average number of passwords per second for the selected time interval.

Password statistics can be misleading because some types of encryption, such as PGP, require more effort to test passwords than other types of encryption, such as a Zip file. Also, the same encryption type can contain options that take longer to test.

For example, one machine performing 1,000 password tests per second on a PGP disk file is working much harder (or much faster) than another machine performing 1,000,000 password tests per second on a Zip file.

To customize the Passwords/Second graph:

1. In the Interval drop-down list, select the time interval that you want displayed on the Seconds axis of the graph.
2. In the Precision field, enter the number of data points that you want displayed on the Seconds axis of the graph.
The default number of data points is 100. If you want a more detailed graph, enter a larger number of points. The graph takes more time to display with a larger number of points. If you want the graph to quickly display, enter a smaller number of points.

Adding Comments to a Job

To add comments about a job:
1 Double-click a job.
2 In the Information window, add comments for the job.
3 Click OK.

These comments appear in the Properties Bar and in the job Information window.

Verifying Hashes

Before PRTK begins a password recovery, it automatically creates two different hash values: a Secure Hash Algorithm (SHA) hash and a Message Digest 5 (MD5) hash.

These hash values can be used to verify that the contents of a file have not changed during recovery of the password.

For more information about hashing methods, see “Current Encryption Standards” on page 257.

Verify Hashes Option

The Verify Hashes option is used to verify that the contents of files have not changed during the password recovery.
To verify hash values for files in the PRTK Window, select **Analyze**, and then **Verify Hashes**.

If the current hash values for files are identical to the hash value created before the password recovery jobs, PRTK returns the message “No files have changed.”

**Printing Recovery Reports**

You can print reports containing file information for jobs in the PRTK window.

Reports contain file attributes information, including filename, registered type, identified type, size, file version, created, modified, and hash values (SHA and MD5). For information on attributes, see “Displaying Job Properties” on page 85.

To print a recovery report, select **File**, and then **Print**.

To preview the file before printing, select **File**, and then **Print Preview**.

**Note:** You must have a printer driver installed to print or view files in Print Preview.

Print Preview has the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Print</td>
<td>Print the report.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Next Page</td>
<td>View the next page of the report.</td>
</tr>
<tr>
<td>Previous Page</td>
<td>View the previous page of the report.</td>
</tr>
<tr>
<td>One Page</td>
<td>View the report one page at a time.</td>
</tr>
<tr>
<td>Two Page</td>
<td>View the report two pages at a time.</td>
</tr>
<tr>
<td>Zoom In</td>
<td>Magnify the view of a report.</td>
</tr>
<tr>
<td>Zoom Out</td>
<td>Minimize the view of a report.</td>
</tr>
<tr>
<td>Close</td>
<td>Close Print Preview.</td>
</tr>
</tbody>
</table>

**Note:** You can click the mouse repeatedly in Print Preview to change the zoom or page view.
Managing Jobs in DNA

After you complete the installation of Distributed Network Attack (DNA), you are ready to add and work with encrypted files, or jobs, in the DNA system.

This chapter contains the following sections:
- “Adding a Job” on page 80
- “Allocating Resources for a Job” on page 85
- “Monitoring a Job” on page 89
- “Modifying a Job” on page 101
- “Manually Decrypting Files with a Password or Key” on page 104

Adding a Job

You add a job to the DNA system so that DNA can decrypt it. When you add a job to the DNA system, the job must be associated with a profile. The file application doesn’t have to be installed on the machine in order for DNA to process the job.

By default, DNA includes one profile for English files. You can associate your job with the default profile, or you can create your own profile that is more specific to the file that you are working with. For more information, see “Creating a Profile” on page 72.
Entering Basic Job Information

On the Add Job Wizard Page 1 form, you specify how DNA processes the job.

For example, you select the profile for the job and specify the priority of the job.

The following table describes the Add Job Wizard Page 1 form:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the job. By default, DNA displays the filename. You can change the name so that the job name is different than the filename.</td>
</tr>
<tr>
<td>Profile</td>
<td>The profile that you want to apply to the file. If you select Other, you can create a profile that is used only on this job and is not saved for future use.</td>
</tr>
</tbody>
</table>
### Item Description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>Any information about the job. The comments can include anything you want to record, including information concerning the file or notes to others working on the files.</td>
</tr>
<tr>
<td>Files</td>
<td>The full directory path to the encrypted file.</td>
</tr>
<tr>
<td>Groups</td>
<td>The groups that you want to process this file. By default, the Trusted group processes files handled by sensitive modules. For a list of the sensitive modules, see “Creating a Group” on page 116. If you add multiple files and only some of the files are handled by sensitive modules, the sensitive files are processed by the Trusted group and the remaining files are processed by the other checked, non-trusted groups. This default status is indicated by a gray check in the Trusted group box. If you add multiple files and want all files to be processed by the Trusted group, even files handled by non-sensitive modules, check the Trusted group box and uncheck all other group boxes. All files are only processed in this Trusted group. This status is indicated by a black check in the Trusted group box. If you uncheck the Trusted group, all files, including those handled by sensitive modules, are processed by available, non-trusted workers. <strong>WARNING!</strong> If you uncheck the Trusted group, you might be compromising the integrity of the files because they might be processed throughout the entire DNA network. For more information about groups, see “Creating a Group” on page 116. For more information about adding resources to the Trusted group, see “Changing the Group Membership of a DNA Supervisor or Worker” on page 118.</td>
</tr>
<tr>
<td>Priority Group</td>
<td>The importance of the job, either High or Normal. By default, 90% of all available resources in groups or DNA systems process jobs in the High group; 10% of all available resources process jobs in the Normal group.</td>
</tr>
</tbody>
</table>
To enter basic job information:

1. Select **File**, and then **Add Job**. Or right-click in the job queue and then select **Add**.
2. Browse to and select the encrypted file to recover; click **Open**.
   
   You can select multiple files if you want them to be processed with the same profile. For faster performance, AccessData recommends that you only add multiple files of the same file type, such as Microsoft Word documents. If you want to add multiple files for several file types, run the Add Job Wizard for each file type.

   You cannot add more than 50 files at one time. If you have a network file that is larger than 10 MB, you need to copy it to the local machine before adding it in the wizard.

3. Specify the job information on the Add Job Wizard Page 1 form.
   
   When you add ZIP, ARJ, RAR, PPG, Invisible Secrets, or EMF files, DNA automatically adds them to the Trusted group. For more information, see “Understanding the DNA Decryption Process” on page 11 and “Creating a Group” on page 116.

   **WARNING!** You must assign workers to the Trusted group before the group can process jobs.
4 Click **Next**.

**Selecting the Password and Key Attacks**

The File Information form lists the full filename, file type, and application version of the job. It also lists the various attacks that can be performed on the job.

![Add Job Wizard (Page 2 of 2)](image)

The listed attacks are based on the file type. The attacks run in the order listed in this form.

To enter file information:

1. Choose the attacks that you want DNA to run on the encrypted file.

   You might choose to not run an attack because you don’t want some of the information, such as a spare password.

   In some of the attacks, you must enter a key. The key is a numeric value obtained from running a decryption or key-space attack.
2 To change any of the items listed in the form, click **Back**.

If you do not want to add the job to the DNA system, click **Cancel**. To finish the wizard, click **Finish**.

After DNA processes the jobs, the Processing Results window, shown below, displays the results of the wizard.

Possible results could be:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancelled</td>
<td>You cancelled the processing of the job.</td>
</tr>
<tr>
<td>Corrupted</td>
<td>The file is corrupted.</td>
</tr>
<tr>
<td>Failed to Process</td>
<td>The file cannot be added to the system. This result is a general tag used for any file that cannot be classified as any other result.</td>
</tr>
<tr>
<td>File in Use</td>
<td>The file is locked by another program.</td>
</tr>
<tr>
<td>Successfully Added</td>
<td>The file is added to the job queue.</td>
</tr>
<tr>
<td>Timed Out</td>
<td>The file cannot be identified by DNA in one minute, or you specified to have the job time out after a certain amount of time. This result usually appears when the supervisor is busy processing other jobs.</td>
</tr>
<tr>
<td>Unencrypted</td>
<td>The file does not need to be added to the DNA system because the file isn’t encrypted.</td>
</tr>
<tr>
<td>Unidentifiable</td>
<td>DNA cannot recognize the file and its source application. The module might not exist.</td>
</tr>
</tbody>
</table>
Allocating Resources for a Job

You can allocate the percentage of DNA Workers in a supervisor group that works on a particular job. By default, DNA automatically divides the number of jobs between the available processors on all the machines in the supervisor group.

Determining How Workers Process Jobs

You can determine the amount of data sent to each worker so that the worker machines don’t receive more than they can handle.

After the DNA Worker program is installed on a machine, DNA detects its processing power. DNA sends appropriate amounts of data based on the power of each machine. You can specify the chunk size for sending jobs, to a worker.

By default, DNA Workers always use a low-priority thread on the machine to process jobs. However, you can choose to have workers only process jobs when the machines are idle. DNA determines a machine is idle if the mouse and the keyboard aren’t being used on the machine.

You can change the job processing method for all workers in the DNA system or only for workers subordinate to a particular supervisor. You cannot change the job processing method for DNA Workers running on Windows 98 or ME machines.

To specify how workers process jobs:

1. Select Edit, and then Preferences.

Chunk size is the amount of passwords the Supervisor can process in the amount of time allotted. To change the

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsupported Version</td>
<td>The file was created in an unsupported version of a supported application. For more information about the supported applications and versions, see “Supported Applications and File Formats” on page 201.</td>
</tr>
</tbody>
</table>
process duration, slide the bar up or down to increase or decrease the minutes.

**Important:** To change when the workers process jobs, check the **Stop Workers on Mouse or Keyboard Input** box.

2 Click **OK**.

**Changing the Priority Group of a Job**

You can change the priority group assigned to a job. The priority group determines which jobs are processed with greater resources.

DNA has two priority groups: High and Normal. You might change the assigned priority group to High if you want the job to be processed more quickly.

To change the priority group of a job:

1 In the Priority Groups list, select the job that you want to change.

2 Right-click and select **Priority Group**, and then **High** or **Normal**.

**Changing the Priority of a Job**

You can change the priority of a job on the Change Job Priority form. The job priority determines the percentage of available resources within a DNA Supervisor’s control that can work on a particular job.

To change the priority of a job:

1 In the Priority Groups list, select the job that you want to change.

2 Right-click and select **Change Priority**.

3 In the New Priority field, click the up or down arrows until you reach the desired priority.

4 Click **OK**.
**Monitoring a Job**

After you add a job to the job queue, you can monitor the job in several ways, including monitoring the password attacks or looking at statistics and graphical analyses of that job or all jobs.

**Displaying Job Status**

You can view detailed statistical and graphical analyses of the jobs that the program works on.

To view the job status:

1. Select the jobs in the job queue.
2. Press **Enter** or right-click the job and select **Properties**. The Job Properties screen contains three windows organized as tabs, each with a particular focus or function. Each tab is discussed in the following sections. You can resize the Job Properties screen if desired.

   To close the Job Properties screen, click **OK** or **Cancel**.

**Information**

The Information window displays basic job information and the results of the DNA processing.
The window is divided into four categories:

- Basic Information
- File Information
- Properties
- Results
### Basic Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The job name. If you select multiple jobs in the job queue, select the job that you want to view from the drop-down list.</td>
</tr>
<tr>
<td>Comments</td>
<td>Any comments you entered about the job in the Add Job Wizard.</td>
</tr>
</tbody>
</table>

### File Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>Filename of the job, including the full path to the file.</td>
</tr>
<tr>
<td>Type</td>
<td>Application in which the file was created.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the application recognized by the module.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the file in bytes.</td>
</tr>
<tr>
<td>Created</td>
<td>Date and time that the file was originally created.</td>
</tr>
<tr>
<td>Modified</td>
<td>Date and time that the file was last modified.</td>
</tr>
<tr>
<td>MD5</td>
<td>MD5 (128-bit) hash of the file data.</td>
</tr>
<tr>
<td>SHA-1</td>
<td>SHA (160-bit) hash of the file data.</td>
</tr>
</tbody>
</table>

### Properties

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack Type</td>
<td>Attack type used by DNA for this particular instance of the job. If DNA is using either the keyspace or dictionary attack, then more specific information is listed about the type of attack being used. For more information about attack types, see “Understanding the DNA Decryption Process” on page 11.</td>
</tr>
<tr>
<td>Module</td>
<td>DNA module used for the attack. The module is based on the file type, such as Word, and the attack type.</td>
</tr>
</tbody>
</table>
The Results section displays the passwords and keys that DNA discovers during the decryption process.

Multiple entries in the Results section may occur even if a password is discovered in the first entry. Some files, such as PDF documents, have multiple passwords. Even though one password is discovered, more tests might still be running on
lower levels because DNA is searching for the other passwords in the document.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Either password or key, depending upon what DNA decrypts first.</td>
</tr>
<tr>
<td>Description</td>
<td>The type of password or key that is found. The type is defined by the specific application that encrypted the file. Possible types could be: File, User, Owner, Administrator, Assistant, Reader, Definer, Supervisor, Spare, Possible, Read-write, Service Website, Field, Write Reservation, Option Protect, Sheet, Save As, Title, Protection, Transaction, Data Entry, Payroll, Spare User, Pass Key, and Zip Key.</td>
</tr>
<tr>
<td>Found In</td>
<td>The level and corresponding dictionary that the password or key are discovered in.</td>
</tr>
<tr>
<td>Timeout After (minutes)</td>
<td>The number of minutes that DNA processes the first password attack in a job before it stops that attack and moves on to dependent password attacks.</td>
</tr>
<tr>
<td>Groups</td>
<td>The names of the groups that are assigned to process the job.</td>
</tr>
<tr>
<td>Begin Time</td>
<td>The date and time that DNA begins processing the job.</td>
</tr>
<tr>
<td>End Time</td>
<td>The date and time that DNA finishes processing the job.</td>
</tr>
</tbody>
</table>

Levels

The Levels window displays information about the recovery levels for a job. It also displays a graph that illustrates the number of decryption attempts per recovery level.
You can zoom in on the graph to display a greater level of detail. Click the desired region and drag the mouse to create a rectangle that covers the area you want to see. To reset the graph, close the Job Properties screen and then re-open the Levels window.

The following table describes the components of the Levels window:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the job about which the recovery level information is displayed.</td>
</tr>
</tbody>
</table>
The Levels window graph can be displayed two different ways. By default, DNA displays the graph with the Logarithmic box checked. The graph, shown above, displays great detail about how many tries are attempted at each recovery level. The graph reduces the number of tries that are shown so that you can see each attempt in greater detail.

If you uncheck the Logarithmic box, DNA displays a larger scale graph that displays a more general view of the level progress. An example of this type of graph is shown below. In the non-logarithmic graphic, the last two levels appear much larger than all the others. This type of graph displays the relationships between the levels more accurately.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legend</td>
<td>A color key for the levels displayed in the graph. The following list describes each color:</td>
</tr>
<tr>
<td></td>
<td>• Unassigned: The level is not assigned to any workers. A level is not assigned to workers until the previous level is completed.</td>
</tr>
<tr>
<td></td>
<td>• Assigned: The level is assigned to workers.</td>
</tr>
<tr>
<td></td>
<td>• Completed: The level is completed.</td>
</tr>
<tr>
<td></td>
<td>• Unassignable: The level cannot be assigned by supervisors.</td>
</tr>
<tr>
<td></td>
<td>• Failed: The level was assigned to the workers, but the workers did not return the results.</td>
</tr>
<tr>
<td>ID</td>
<td>A number assigned by DNA to each level and corresponding dictionary that the level is run on.</td>
</tr>
<tr>
<td>Description</td>
<td>The level and corresponding dictionary that the level is run on. If you do not want to display a level in the graph, right-click the level and select Skip. A skipped level is not processed by DNA; DNA immediately marks the skipped levels as completed.</td>
</tr>
<tr>
<td>Number Completed</td>
<td>The number and percentage of possible passwords or keys tried in a particular level.</td>
</tr>
<tr>
<td>Size</td>
<td>The total number of possible passwords or keys in a particular level.</td>
</tr>
</tbody>
</table>
Passwords/Second

The Passwords/Second window displays a graph of the number of passwords per second that are tested for validity over a given amount of time on the selected job. The bottom of the window displays the average number of passwords per second for the selected time interval.

Password statistics can be misleading because some types of encryption, such as PGP, take more effort to test passwords than other types of encryption, such as a Zip file. Also, the same encryption type can contain options that take longer to test.

For example, one machine performing 1,000 password tests per second on a PGP disk file is working much harder (or much faster) than another machine performing 1,000,000 password tests per second on a Zip file.

To customize the Passwords/Second graph:

1. In the Interval drop-down list, select the time interval that you want displayed on the Seconds axis of the graph.
2. In the Precision field, enter the number of data points that you want displayed on the Seconds axis of the graph.

The default number of data points is 100. If you want a more detailed graph, enter a larger number of points. The graph takes more time to display with a larger number of points. If you want the graph to quickly display, enter a smaller number of points.

Creating the Log File

The program can create a log file that contains information about all the processes that run on jobs. Enable Logging by AccessData’s request Customer Support solve any problems you might encounter.

To enable logging (by request of AccessData Support only):

1. Select **Edit**, then **Preferences**, and then **Logging**.
2. Check the **Enable Logging** box.
3 In the field, enter the name and extension of the log file that you want, such as log.txt or log.htm.

The program puts the log file in the Supervisor directory. Data is automatically added to the log until you disable logging.

**Important:** Disregarded logs will continue to grow and consume disk space over time. Enable logging only at the request of an AccessData’s Customer Support representative.

**Recovery Options**

By default, the program does not automatically decrypt a file after a key is discovered. You can choose to have the key automatically applied to the file, and you can receive an e-mail when the job is completed. You can configure both these features in the Recovery Options section of the Preferences form.

To automatically decrypt the file after a key is found:

1. Select **Edit**, and then **Preferences**.
2. Check the **Decrypt File When Key Is Found** box.
3. Select **Save in Same Directory as the Encrypted File**, or select **Save In** and browse to and select the desired directory.

   The directory of the encrypted file is the directory that you added the encrypted file from during the Add Job Wizard. You might want to specify a different directory if you want to keep all decrypted files in one location.

   After a file is decrypted with a key, the filename is appended with `-decrypted` for example, file1-decrypted.xls.

4. Click **OK**.

To receive an e-mail after a job is completed:

1. Select **Edit**, and then **Preferences**.
2. Check the **Send an Email When a Job Has Been Completed** box.
3 In the E-mail Address field, enter the recipient’s e-mail address.

4 In the SMTP Server field, enter the name of the SMTP server for the specified e-mail address.

5 In the Port field, enter the port number.

6 Click Test to send a test e-mail to verify that the e-mail address and SMTP server information is working.

7 Click OK.

Note: Works only with servers not requiring SMTP authentication.

Managing Workers and Groups

You can manage the DNA Workers in the DNA system in the system or by creating groups.

This chapter contains the following sections:
- “Filtering the Resource Queue” on page 108
- “Monitoring a DNA Supervisor or Worker” on page 109
- “Creating a Group” on page 116
- “Editing a Group” on page 117
- “Removing a Group” on page 118
- “Changing the Group Membership of a DNA Supervisor or Worker” on page 118
- “Changing the Supervisor of a DNA Worker” on page 120

Filtering the Resource Queue

You can filter the resource queue. You might filter them to see only the machines within a certain subnet.
You can update the resource queue on the Apply Filter form. The following table describes the Apply Filter form:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Field     | A drop-down list that contains the following columns to sort by:  
- Name: The computer name of the worker.  
- IP Address: IP address of the worker.  
- Processors: The total number of physical processors on the supervisor or worker machine. |
| Expression| Enter any regular expression, including the following:  
- Period (.) to match any character.  
- Asterisk (*) to repeat the last character.  
- Plus Sign (+) to repeat the previous character.  
- [x–y] to signify the OR operation, and to specify a range of letters. |
| Access    | A drop-down list of Allow or Deny that corresponds to the entry in the Expression field. |

To filter the resource queue:

1. In the resource queue, click **Filter**.
2. Enter the information in the form.
3. Click **Apply**. The resource queue is updated according to the filter specifications.
To clear the filter, click **Clear**. The current filter will be cleared, but not removed from the list.

**Monitoring a DNA Worker**

You can view detailed statistical and graphical analyses of the performance of each DNA worker.

To view the worker status:

1. Select the workers in the resource queue.
2. Right-click the selection and choose **Properties**.

   The Properties screen contains three windows organized as tabs, each with a particular focus or function. Each tab is discussed in the following sections. You can resize the Worker Properties screen if desired.

To close the Properties screen, click **OK** or **Cancel**.

**Information**

The Information window displays basic supervisor or worker information.

The window is divided into one category about the supervisor or worker and one category about the groups that the supervisor or worker belongs to. Each category is discussed in the following sections.

**Worker Information**

The following table describes the Basic Information section:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worker</td>
<td>The worker name.</td>
</tr>
<tr>
<td></td>
<td>If you select multiple resources in the resource queue, then select the resource in the drop-down list that you want to view.</td>
</tr>
<tr>
<td>Connected</td>
<td>Yes or No, depending on whether the worker is connected to the supervisor.</td>
</tr>
</tbody>
</table>
Group Information

The following table describes the Group Information section:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>The total number of physical processors on the worker machine.</td>
</tr>
<tr>
<td>Power</td>
<td>The processor speed of the machine’s physical processors. The program will average the processing speed of multiple processors selected.</td>
</tr>
<tr>
<td>Last Contact Time</td>
<td>The last date and time the supervisor contacted the worker.</td>
</tr>
<tr>
<td>Release</td>
<td>The version of the DNA that the machine is running.</td>
</tr>
<tr>
<td>Working On</td>
<td>The job name and attack type that the worker is processing. This field might be blank if the worker is not currently processing a job.</td>
</tr>
<tr>
<td>Group List</td>
<td>Names of groups that the worker belongs to.</td>
</tr>
<tr>
<td>Change Group</td>
<td>Opens the Change Group Membership form so that you can quickly add or remove the worker from the listed groups.</td>
</tr>
<tr>
<td>Membership</td>
<td>For more information about this form, see “Changing the Group Membership of a DNA Worker” on page 118.</td>
</tr>
<tr>
<td>Restart</td>
<td>Prompts to either restart the supervisor or worker or cancel restarting. You might restart the resource to update its group membership in the DNA management interface.</td>
</tr>
</tbody>
</table>

Passwords/Second

The Passwords/Second window displays a graph of the number of passwords per second that are tested for validity over a given amount of time on the selected worker.

If you are viewing the properties of an individual worker, then this graph displays the passwords per second of the worker for the specified interval. The bottom of the window displays the average number of passwords per second for the selected time interval.
Password statistics can be misleading because some types of encryption, such as Pretty Good Privacy (PGP), take more effort to test passwords on than other types of encryption, such as a Zip file. Also, the same encryption type can contain options that take longer to test. For example, one machine performing 1,000 password tests per second on a PGP disk file is working much harder (or much faster) than another machine performing 1,000,000 password tests per second on a Zip file.

To customize the Passwords/Second graph:

1. In the Interval drop-down list, select the time interval that you want displayed on the Seconds axis of the graph.

2. In the Precision field, enter the number of data points that you want displayed on the Seconds axis of the graph.

   The default number of data points is 100. If you want a more detailed graph, enter a larger number of points. The graph takes more time to display with a larger number of points. If you want the graph to quickly display, enter a smaller number of points.

Availability

The Availability window displays a graph of the time when the worker is available. The Availability axis simply depicts if the resource is available or not; the range of numbers along the axis is purely for computational purposes. The bottom of the window displays the approximate availability for the selected time interval. The Availability statistics are useful metrics in understanding when the worker is most or least available to process jobs.

To customize the Availability graph:

1. In the Interval drop-down list, select the time interval that you want displayed on the Time axis of the graph.

2. In the Precision field, enter the number of data points that you want displayed on the Time axis of the graph.
The default number of data points is 100. If you want a more detailed graph, enter a larger number of points. The graph takes more time to display with a larger number of points. If you want the graph to quickly display, enter a smaller number of points.

Creating a Group

You can create a group to manage DNA workers. For example, if a DNA supervisor manages 30 worker machines, you might create three groups of ten workers, each based on location or processing power. If you have a job that requires a quicker decryption rate, you can assign it to the most powerful group.

By default, DNA creates three groups:

- Default: Use to process the majority of files. All workers are assigned to this group.
- Trusted: Use to process ZIP, ARJ, RAR, PGP, Invisible Secrets, and EMF files. You must assign workers to the Trusted group before DNA can process jobs with the group. For more information, see “Changing the Group Membership of a DNA Worker” on page 118.
- Dictionary: Use to process files that only require a dictionary attack.

You use the Manage Groups form to create a group. To create a group:

1. Click Manage Groups in the resource queue, or select Edit, and then Manage Groups.
2. Click Add on the Manage Groups form.
3. In the Group Name field, enter the name of the group and click OK. You might enter a name based on the location or power of the workers. After you create a group, you can then assign workers to the group.

Editing a Group

You can edit an existing group of workers to better suit your needs.
To edit a group:

1. Click **Manage Groups** in the resource queue, or select **Edit**, and then **Manage Groups**.

2. Select the group that you want to edit from the **Manage Groups** list and click **Edit**.
   - To change the group name, enter the new group name in the field.
   - To specify the speed at which DNA downloads dictionaries to the workers, select the type of network connection for the group and the percentage of connection bandwidth to use.
   - To apply a filter to the group, click **Add** and complete the Apply Filter form.

3. After the changes are complete, click **OK**.

Removing a Group

To remove a group:

1. In the resource queue, click **Manage Groups**, or select **Edit**, and then **Manage Groups**.

2. In the **Manage Groups** list, select the group that you want to delete and click **Remove**.

3. Click **Close**.

Changing the Group Membership of a DNA Worker

After you create a group, you can then assign workers to the group. You might assign a worker to become a member of a group because you need the machine’s processing power in a group. A worker can be a member of more than one group. A powerful machine can be part of several groups to help process jobs more quickly.

If you want to use the default Trusted group for sensitive files, you need to first assign workers to the group. You can change group membership on the Change Group Membership form.
To assign group membership to a worker: In the Resource queue, right-click the worker you want to assign and click Change Group Membership.

To add the supervisor or worker to a group:

1. In the Available list, select the group to host the supervisor or worker.
2. Click the left-arrow button.

To remove the supervisor or worker from a group:

1. In the Current Membership list, select the group you want to remove from the supervisor or worker.
2. Click the right-arrow button.
3. Click OK.

Changing the Supervisor of a DNA Worker

Change the supervisor assignment for a particular worker if you install a newer supervisor.

To change the supervisor of a DNA Worker:

1. In the resource queue, right-click the worker you want to re-assign and click Change Supervisor.
2. In the drop-down list, enter or select the computer name or IP address of the new supervisor.
3. Click OK.
Managing Profiles

Before a job can be processed in Password Recovery Toolkit (PRTK), it must be added to an existing profile. A profile is a collection of specific levels and dictionaries that are pertinent to a category of encrypted files.

PRTK contains one default profile for files written in English. This chapter contains the following sections:

- “Default Profiles” on page 123
- “Setting a Default Profile” on page 124
- “Creating a Profile” on page 125
- “Editing a Profile” on page 128
- “Deleting a Profile” on page 129

Default Profiles

DNA and PRTK share the same profile names:

- English (default): This profile begins by searching for simple passwords, followed by, dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. All default English dictionaries and character sets are used.

- Arabic: This profile begins by searching for simple passwords, followed by, dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. All default Arabic dictionaries and character sets are used.
European: This profile begins by searching for simple passwords, followed by dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. All default German, French, Italian and Spanish dictionaries and character sets are used.

Russian: This profile begins by searching for simple passwords, followed by, dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. All default Russian dictionaries and character sets are used.

English Transitional: This profile follows the same order of the DNA 3.1 and PRTK 6.1 English Profile.

Pass-phrase: This profile uses all pass-phrase levels in English

FTK Import: This profile is used as a template for FTK imported wordlists

PRTK (DNA only): Levels in this profile are ordered by research conducted on recovered passwords. Each level completes in 24 hours or less based on a job processing 200,000 passwords/second.

DNA (DNA only): Levels in this profile are ordered by research conducted on recovered passwords. Levels that can complete in five days or less are processed first, followed by levels that take longer than five days to process (based on a job processing 200,000 passwords/second on one worker).

Setting a Default Profile

You can set a profile as the default profile. Every job added to the PRTK system is assigned to the default profile unless you select a different profile for the job.
To set a default profile:

1. Select Edit, and then Profiles.
2. In the Manage Profiles list, select the profile that you want to set as the default, and then click Set As Default.

Creating a Profile

You can create profiles that are specific to the files with which you are working.
For example, if you have a collection of encrypted files from a case that has documents in both English and Arabic, then you can create a profile that includes only English and Arabic dictionaries. When PRTK processes the files, it only runs the levels on the selected dictionaries. This limiting process speeds up the decryption process for your files.

You can use the New Profile form to name the profile and select the languages, character groups, dictionaries, and levels to include in the profile.

The following table describes the Profile window:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Information about the profile, including the name and any comments about the specific profile you are creating.</td>
</tr>
</tbody>
</table>
Languages

PRTK can process encrypted files in the following languages:
- Arabic
- English
- French
- German
- Italian
- Russian
- Spanish

Character Groups

By default, Lowercase Letters, Uppercase Letters, Digits, Symbols, and Diacritics are checked.

**Note:** The character selections do not affect the dictionaries.
- Lowercase Letters: uses only lowercase letters to generate passwords.
- Uppercase Letters: uses only uppercase letters to generate passwords.
- Digits: Searches for numbers.
- Symbols (Standard): Searches for symbols from the keyboard, such as the plus sign (+) or the dollar sign ($).
- Symbols (Extended): Searches for symbols from the character tables, such as the Em dash (—) or the Yen (¥).
- Diacritics: Searches for symbols, such as the tilde (~) or the circumflex (^) combines with letters.
- All 7-bit Characters (ASCII): Searches for any ASCII characters. This box includes all characters listed above it.
- All 8-bit Characters: Searches for any ASCII and Extended ASCII characters. This box includes all characters listed above it and the Extended ASCII characters.

Dictionaries

The following dictionaries are included in PRTK. Dictionaries end with the .adf or .xml extensions. Each dictionary includes both a code page (-c.adf) and a Unicode (-u.adf) version.

You can also create additional dictionaries from a forensic image. For example, you can create dictionaries from the word list from FTK.

Levels

The password levels that PRTK applies to dictionaries. The levels are run in the order you list.
To create a profile:

1. Select **Edit**, then **Profiles**, and then **New**.

2. In the Name field, enter the name of the profile. Without a profile name, the profile will not be saved.

3. (Optional) In the Comments field, enter any comments that might be helpful to others working on the case, such as “Use this profile for files in Case 1.”

4. Check the languages to include.

5. Check the character groups to include.

6. Check the dictionaries to include.

   The dictionaries are checked by default according to the languages that you specify in Step 4. You might add more dictionaries that are relevant to your encrypted files.

   To aid in the selection process, click **Select All** or **Deselect All**.

7. Check the levels to include.

   To change the order of a level, select the level; then click **Move Up** or **Move Down**.

   To aid in the selection process, click **Select All** or **Deselect All**.

8. Click **Save**, and then **Yes**.

9. The *.profile file must be saved to the PRTK\Profiles\ folder.

---

**Editing a Profile**

You can edit any of the information that you originally specified when you created a profile. You might edit a profile if you want to change the order of the password levels or add another dictionary that you have recently created. You can edit a profile on the Manage Profiles screen.

To edit a profile:

1. Select **Edit**, and then **Profiles**.
In the Manage Profiles list, select the profile that you want to edit and then click **Edit**.

Modify the desired options in the profile form.

Click **OK**, and then **Yes**.

Select the profile file to update and click **Save**, and then **Yes**.

You cannot change the name of the profile on this screen. If you enter a new profile name, then another profile with the same name as the profile that you are editing is added to the Manage Profiles list.

For more information about each option, see “Creating a Profile” on page 125.

**Deleting a Profile**

You might delete a profile if you no longer need its specific collection of levels and dictionaries. You can delete a profile on the Manage Profiles screen.

To delete a profile:

1. Select **Edit**, and then **Profiles**.

2. In the Manage Profiles list, select the profile that you want to delete and then click **Delete**.

3. Click **Yes** to confirm the deletion.
Managing Password Levels

You can customize the password recovery levels that Password Recovery Toolkit (PRTK) uses in its file decryption. You can customize the levels either by creating a new level or changing the level order so that the time required to decrypt a file is decreased.

This chapter contains the following sections:

- “Understanding Level Categories” on page 131
- “Modifying the Password Level Order” on page 138
- “Understanding a User-defined Level” on page 140
- “Editing a User-defined Level” on page 148
- “Removing a User-defined Level” on page 148

Understanding Level Categories

Level ordering (the arrangement of levels when creating new profiles) started with levels of the fewest amounts of password tests and ended with levels of the greatest amount. Profiles were then created to reflect the level order, with the idea that levels with the fewest tests (attempts) would complete first, in the least amount of time for each of the profiles created.

Several levels use the Markov permutation. These levels include words with phonemes that sound like English words; the words themselves, however, are actually meaningless.

If you select a level that is language-specific and the profile contains a dictionary that cannot use the specific level, PRTK
simply does not generate any words from that level. For example, if you have a profile that contains an Arabic dictionary and you select the Markov level, PRTK does not apply the Markov levels to the Arabic dictionary because the Markov levels currently support only the English language.

Levels are ordered by a combination of the number of password tests and the types of password attacks. The label Basic (BAS), Advanced (ADV), or Pass-phrase (PP) is prefixed to the level name according to the number of tests they perform. Some Language-specific levels may fall into Basic levels according to size, but are labeled as Advanced because of the choice of character groups that can be applied to a given profile. Each level has a prefix composed of a category, followed by an intensity, followed by an ID. For example, the level (BAS-1-01) represents:

<table>
<thead>
<tr>
<th>Attempt Category</th>
<th>Attempt Intensity</th>
<th>Attempt ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>1</td>
<td>01</td>
</tr>
</tbody>
</table>

**Default Level Order**

PRTK and DNA levels are arranged in this order:

- (BAS-1-01) One digit search
- (BAS-1-02) One letter, language specific search
- (BAS-1-03) Two digit search
- (BAS-1-04) Two letter, language specific search
- (BAS-1-05) Three digit search
- (BAS-1-06) Three letter, language specific search
- (BAS-1-07) Four digit search
- (BAS-1-08) Five digit search
### Default Level Order

<p>| (BAS-1-09) | Five Markov characters within a threshold of one hundred with two characters uppercased search |
| (BAS-1-10) | Six digit search |
| (BAS-1-11) | Four Markov characters with a threshold of one primary search |
| (BAS-2-01) | Four letter, language specific search |
| (BAS-2-02) | Five letter, language specific search |
| (BAS-2-03) | Five Markov characters with a threshold of one primary search |
| (BAS-2-04) | Five Markov characters with a threshold of one primary reverse search |
| (BAS-2-05) | Six Markov characters with a threshold of one primary search |
| (BAS-2-06) | Six Markov characters with a threshold of one hundred with two characters uppercased search |
| (BAS-2-07) | Six Markov characters with a threshold of one primary reverse search |
| (BAS-2-08) | Seven digit search |
| (BAS-2-09) | Seven Markov characters with a threshold of fifty primary search |
| (BAS-2-10) | Seven Markov characters with a threshold of fifty primary reverse search |
| (BAS-2-11) | Seven Markov characters with a threshold of one hundred with two characters uppercased search |
| (BAS-2-12) | Seven-digit telephone number search |
| (BAS-2-13) | Eight digit search |
| (BAS-2-14) | Eight Markov characters with a threshold of fifty primary search |
| (BAS-2-15) | Eight Markov characters with a threshold of fifty primary reverse search |
| (BAS-2-16) | Eight Markov characters with a threshold of one hundred with two characters uppercased search |
| (BAS-2-17) | Dictionary primary search |</p>
<table>
<thead>
<tr>
<th>Default Level Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>(BAS-2-18) Dictionary primary reverse search</td>
</tr>
<tr>
<td>(BAS-2-19) Dictionary with two characters uppercased search</td>
</tr>
<tr>
<td>(BAS-2-20) Dictionary primary character replacements search</td>
</tr>
<tr>
<td>(BAS-2-21) Dictionary primary followed by common postfixes search</td>
</tr>
<tr>
<td>(BAS-2-22) Dictionary primary preceded by common prefixes search</td>
</tr>
<tr>
<td>(BAS-2-23) Dictionary primary followed by a one digit search</td>
</tr>
<tr>
<td>(BAS-2-24) Dictionary primary preceded by a one digit search</td>
</tr>
<tr>
<td>(BAS-2-25) Dictionary primary followed by a one letter, language specific search</td>
</tr>
<tr>
<td>(BAS-2-26) Dictionary primary preceded by a one letter, language specific search</td>
</tr>
<tr>
<td>(BAS-2-27) Dictionary primary followed by a non-alphanumeric symbol search</td>
</tr>
<tr>
<td>(BAS-2-28) Dictionary primary preceded by a language-specific non-alphanumeric symbol search</td>
</tr>
<tr>
<td>(BAS-2-29) Dictionary primary character replacement, followed by a one digit search</td>
</tr>
<tr>
<td>(BAS-2-30) Dictionary primary character replacement, preceded by a one digit search</td>
</tr>
<tr>
<td>(BAS-2-31) Dictionary primary preceded and followed by a one digit search</td>
</tr>
<tr>
<td>(BAS-2-32) Dictionary primary followed by a two digits search</td>
</tr>
<tr>
<td>(BAS-2-33) Dictionary primary preceded by a two digits search</td>
</tr>
<tr>
<td>(BAS-2-34) Dictionary primary preceded by common prefixes and followed by a one digit search</td>
</tr>
<tr>
<td>(BAS-2-35) Dictionary primary preceded by one digit followed by common postfixes</td>
</tr>
<tr>
<td>(BAS-2-36) Date Search (2 digit year)</td>
</tr>
<tr>
<td>(BAS-2-37) Three letter, language specific characters followed by common postfixes</td>
</tr>
<tr>
<td>(BAS-2-38) Three letter, language specific characters preceded by common prefixes</td>
</tr>
</tbody>
</table>
Default Level Order

(BAS-2-39) Five Markov Characters with a threshold of one followed by common postfixes
(BAS-2-40) Five Markov Characters with a threshold of one preceded by common prefixes
(BAS-2-41) Six Markov Characters with a threshold of fifty followed by common postfixes
(BAS-2-42) Six Markov Characters with a threshold of fifty preceded by common prefixes
(BAS-2-43) Nine Markov characters with a threshold of one hundred search
(BAS-3-06) Social Security Number search
(BAS-3-01) Dictionary primary with a non-alphanumeric symbol inserted search
(BAS-3-02) Dictionary primary character replacement, followed by a two digit search
(BAS-3-03) Dictionary primary character replacement, preceded by a two digit search
(BAS-3-04) Dictionary primary followed by a three digit search
(BAS-3-05) Dictionary primary preceded by a three digit search
(BAS-3-06) Four letter, language specific characters followed by common postfixes
(BAS-3-07) Four letter, language specific characters preceded by common prefixes
(ADV-1-01) All one-character, language-specific search
(ADV-1-02) All two character, language-specific search
(ADV-1-03) All three-character, language-specific search
(ADV-1-04) All four-character, language-specific search
(ADV-1-05) One digit followed by three language-specific characters search
(ADV-1-06) Three language-specific characters followed by one digit search
(ADV-1-07) One language-specific character followed by a four digit search
(ADV-1-08) One digit followed by four language-specific characters search
<table>
<thead>
<tr>
<th>Default Level Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ADV-1-09) Two language-specific characters followed by a three digit search</td>
</tr>
<tr>
<td>(ADV-1-10) Two digits followed by three language-specific characters search</td>
</tr>
<tr>
<td>(ADV-1-11) Three language-specific characters followed by a two digit search</td>
</tr>
<tr>
<td>(ADV-1-12) Four language-specific characters followed by a one digit search</td>
</tr>
<tr>
<td>(ADV-1-13) Four language-specific characters followed by a non-alphanumeric symbol search</td>
</tr>
<tr>
<td>(ADV-1-14) Four language-specific characters preceded by a non-alphanumeric symbol search</td>
</tr>
<tr>
<td>(ADV-1-15) Six letter, language specific search</td>
</tr>
<tr>
<td>(ADV-1-16) Two digits followed by four language-specific characters search</td>
</tr>
<tr>
<td>(ADV-1-17) Two language-specific characters followed by four digits search</td>
</tr>
<tr>
<td>(ADV-1-18) Three language-specific characters followed by a three digit search</td>
</tr>
<tr>
<td>(ADV-1-19) Four language-specific characters followed by a two digit search</td>
</tr>
<tr>
<td>(ADV-1-20) Dictionary primary followed by a two letter, language specific search</td>
</tr>
<tr>
<td>(ADV-1-21) Dictionary primary preceded by a two letter, language specific search</td>
</tr>
<tr>
<td>(ADV-1-22) Dictionary primary preceded by a two digit followed by common postfixes</td>
</tr>
<tr>
<td>(ADV-1-23) Dictionary primary preceded by common prefixes and followed by a two digit search</td>
</tr>
<tr>
<td>(ADV-1-24) Dictionary primary preceded and followed by a two digit search</td>
</tr>
<tr>
<td>(ADV-1-25) Dictionary primary followed by a four digit search</td>
</tr>
<tr>
<td>(ADV-1-26) Dictionary primary preceded by a four digit search</td>
</tr>
<tr>
<td>(ADV-1-27) Ten-digit telephone number search</td>
</tr>
<tr>
<td>(ADV-2-01) All five-character, language-specific search</td>
</tr>
</tbody>
</table>
### Default Level Order

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADV-3-01</td>
<td>Four language-specific characters with a non-alphanumeric symbol inserted search</td>
</tr>
<tr>
<td>ADV-3-02</td>
<td>Four language-specific characters followed by a three digit search</td>
</tr>
<tr>
<td>ADV-4-01</td>
<td>All six-character, language-specific search</td>
</tr>
<tr>
<td>ADV-4-02</td>
<td>Seven letter search</td>
</tr>
<tr>
<td>ADV-4-03</td>
<td>All seven-character, language-specific search</td>
</tr>
<tr>
<td>ADV-4-04</td>
<td>Eight letter search</td>
</tr>
<tr>
<td>ADV-4-05</td>
<td>All eight-character, language-specific search</td>
</tr>
<tr>
<td>ADV-4-06</td>
<td>Nine letter, language specific search</td>
</tr>
<tr>
<td>ADV-4-07</td>
<td>All nine-character, language-specific search</td>
</tr>
<tr>
<td>ADV-4-08</td>
<td>Ten letter, language specific search</td>
</tr>
<tr>
<td>ADV-4-09</td>
<td>All ten-character, language-specific search</td>
</tr>
<tr>
<td>ADV-4-10</td>
<td>All eleven-character, language-specific search</td>
</tr>
<tr>
<td>ADV-4-11</td>
<td>All twelve-character, language-specific search</td>
</tr>
<tr>
<td>PP-1-01</td>
<td>Two word concatenation without spaces search</td>
</tr>
<tr>
<td>PP-1-02</td>
<td>Two word concatenation with spaces search</td>
</tr>
<tr>
<td>PP-1-03</td>
<td>Dictionary preceded by a verb or prepositional phrase search</td>
</tr>
<tr>
<td>PP-1-04</td>
<td>The common English dictionary preceded by a verb or prepositional phrase search</td>
</tr>
<tr>
<td>PP-2-01</td>
<td>Word inserted into another word search</td>
</tr>
<tr>
<td>PP-2-02</td>
<td>Dictionary followed by a verb or prepositional phrase followed by a Dictionary search</td>
</tr>
<tr>
<td>PP-2-03</td>
<td>Two word passphrase using the common English dictionary</td>
</tr>
<tr>
<td>PP-3-01</td>
<td>Three word concatenation without spaces search</td>
</tr>
</tbody>
</table>
Modifying the Password Level Order

PRTK uses many different password levels to filter potential passwords through various permutations. The levels progress through the Golden Dictionary automatically, and subsequently all other selected dictionaries from the top of the list to the bottom. For a table that contains all password levels, see “Password Recovery Attacks” on page 219.

Default Level Order

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(PP-3-02)</td>
<td>Three word concatenation with spaces search</td>
</tr>
<tr>
<td>(PP-3-03)</td>
<td>Four word concatenation without spaces search</td>
</tr>
<tr>
<td>(PP-3-04)</td>
<td>Four word concatenation with spaces search</td>
</tr>
</tbody>
</table>

You can change the order of the password levels to increase the speed of password recovery. For example, if you know the password is English and contains three characters, you can move up the “All Three-letter Language-specific Passwords Search” level to the beginning of the execution order.
You change the order of the password levels within a profile. You cannot automatically change the password level order for all profiles.

To change the password level execution order for a profile:

1. Select **Edit**, and then **Profiles**.
2. In the Manage Profiles list, select the profile that you want to change, then click **Edit**.
3. In the Levels list, select the levels that you want to move, then click either **Move Up** or **Move Down**.

   One click moves the level one place. Click the button as many times as needed to set the level order.

   **Note:** If you change the properties of a profile, such as modifying the level order, the new changes are not applied to current jobs in the PRTK system. The changes are applied only to new jobs that are added.

4. Click **OK**, and then **Yes**.

5. Replace the original profile file with the modified file you created.
Understanding a User-defined Level

You can create a user-defined level to facilitate the decryption process for a file or set of files. You might create a password level that combines dictionaries or adds certain prefixes or postfixes that might be relevant to the files. To use the password level, you must then add it to a profile.

You can use the Level Editor form to create a level. The types listed in the applicable drop-down list on the Level Editor form are the building blocks for creating a level. Types are different ways that characters or words are permuted. Types and the information that you specify about the types are used to create levels.

One level can have multiple types. For example, you can create a level that combines words created by two different types, as seen in the graphic above.

In this example, the Lowercase type creates a lowercase word set of an English dictionary (en-u.adf). The Romanize type uses the words in an Arabic dictionary (ar-u.adf) to create a word set of Arabic words re-written with English letters. The
Concatenate type then combines the two word sets created by the Lowercase and Romanize types to create a single word set.

**Important:** A word set is any series of words. Some word sets are stored in dictionaries, which are saved in (.adf) files to your hard drive. It's available for use in multiple profiles and multiple sessions. Other words sets are not saved. For example, the Lowercase word set is generated by PRTK when the level is applied, but the resulting word set is stored just in memory as the level is being used.

Although you can combine types to create one level, each type within the level must ultimately point to a word set. The type uses the word set as its source to create a derivative word set.

In the example above, the Lowercase type uses an English dictionary as its source of words. The type applies its function of displaying all letters in the dictionary in lowercase letters. It then creates a new word set of lowercase English words.

The example above uses only English and Arabic dictionaries. However, you should generally create a user-defined level that contains all dictionaries to increase the versatility of the user-defined level. You can then specify the appropriate dictionaries in each profile.
The available basic word sets are:

- Characters
- Dictionary
- Golden Dictionary
- Markov

Each word set and all available types can function either as sources or source modifiers.

A source is a word set or dictionary from which PRTK draws words.

A modifier is a word set that affects the source word set.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arabicize (modifier)</td>
<td>Uses a word from any non-Arabic language and replaces the letters in the word with the corresponding letters in the Arabic alphabet; “alif” replaces “a” for example. If you select this type, you must create a modifier.</td>
</tr>
<tr>
<td>Arabic on English Keyboard (modifier)</td>
<td>Transforms Arabic words typed on an English keyboard into English words that might be passwords. The words are created according to the key location on the keyboard. For example, this type replaces the letter “shin” in Arabic with the letter “a” in English because they have the same location on a keyboard. The new English words are completely meaningless. If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.</td>
</tr>
</tbody>
</table>
Character (source)  A word set based on a fixed-length sequence of characters. The character word sets are created from the languages specified in the profile.

For example, you have created a profile that only uses the Spanish language. If you create a user-defined level that contains the Character type, the character word set consists of only Spanish characters.

If you select the Character type, you must enter the desired number of characters in the appropriate field, and you must check the character groups that you want to include.

Concatenate (modifier)  Combines words from different word sets. This type takes one word from one word set and places it next to one word from another word set.

For example, if one word set consists of dog and the other word set consists of cat, the Concatenate type creates “dogcat” and “catdog.”

If you select this type, you must create two subordinate Character, Dictionary, Golden Dictionary, or Markov types.

Dictionary (source)  A word set that is associated with a language. The entire set is tagged as codepage or UTF16-LE.

Typically, when you create a user-defined level, you only select this type when you need to specify a word set. This type doesn’t perform any permutations of characters or words.

If you select this type, you must select the dictionary from the Dictionary drop-down list.

Generally you should create a user-defined level that contains all dictionaries to increase the versatility of the user-defined level. You can then specify the appropriate dictionaries in each profile.

English on Arabic Keyboard (modifier)  Transforms English words typed on an Arabic keyboard into Arabic words that might be passwords. The words are created according to the key location on the keyboard.

For example, if you’ve memorized a password by keystroke, the password will be the same between different keyboards.
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| English on Russian Keyboard (modifier) | Transforms English words typed on an Russian keyboard into Russian words that might be passwords. The words are created according to the key location on the keyboard.  
For example, if you've memorized a password by keystroke, the password will be the same between different keyboards. |
| Golden Dictionary (source) | A word set that is not associated with a language and consists of previously discovered passwords. Each password is included in both code page and UTF16-LE.  
Typically, when you create a user-defined level, you only select this type when you need to specify a word set. This type doesn’t perform any permutations of characters or words. |
| Group (modifier)         | A collection of types and their descriptions.  
In the future, you can use the Group type to save a collection of types to apply to other user-defined levels. |
| Insert (modifier)        | Places each word of one word set into all possible positions for each word in another word set. For example, if the word set consists of dog and cat, the Insert type creates cdogat, cadogt, catdog, and so on.  
If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type. |
| Lowercase (modifier)     | Uses an existing word set to create another word set that is all lowercase letters.  
If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type. |
| Markov (source)          | The word set uses statistical Markov methods to create words with phonemes that sound like English words; however, the words themselves are actually meaningless.  
This is the only type that uses the Threshold field. The threshold number determines how many times any combination of letters must appear in a database table of all English words. If the combination of letters meets the threshold, then the letters are used to create words in the word set.  
A high threshold generates a relatively small number of words. A low threshold generates a large number of words. |
Multi-slot (modifier) | Allows multiple passwords on one file. This type is only used for the DriveCrypt and DriveCrypt Plus Pack.  
If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.

Primary (modifier) | Uses a word set and performs the following for each word in that set:  
• Lowercased  
• Uppercased  
• Lowercased with the first letter uppercased  
• Uppercased with the first letter lowercased  
If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.

Reverse (modifier) | Uses a word set and reverses each word in the set.  
If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.

Romanize (modifier) | Uses Arabic words and replaces letters according to the sounds of English letters.  
If you select this type, you must create a subordinate Character or Dictionary type. If you select the Character type, the profile must include the Arabic language. If you select the Dictionary type, you must select an Arabic dictionary.

Russian on English Keyboard (modifier) | Transforms Russian words typed on an English keyboard into English words that might be passwords. The words are created according to the key location on the keyboard.  
For example, if you’ve memorized a password by keystroke, the password will be the same between different keyboards.

Secondary (modifier) | Uses a word set to create another word set of both lower- and uppercased words.  
If you select this type, you must create a subordinate Character, Dictionary, Golden Dictionary, or Markov type.
Creating a User-defined Level

You can use the Level Editor form to create a user-defined level.

The following table describes the Level Editor form:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hierarchy</td>
<td>The structure of the level that you create. The top level of the structure is the name that you give the level.</td>
</tr>
<tr>
<td>Type</td>
<td>The basic unit of a user-defined level. You can select multiple equal or subordinate types per level.</td>
</tr>
</tbody>
</table>
To create a user-defined level:

1. Select **Edit**, then **Levels**, and then **New**.
2. Click **New Level** and enter the name of the user-defined level.

You might name the level according to its function, such as Combine Arabic/English words.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary</td>
<td>The available dictionaries. You only use this drop-down list when you select a Dictionary type. Generally you should create a user-defined level that contains all dictionaries to increase the versatility of the user-defined level. You can then specify the appropriate dictionaries in each profile.</td>
</tr>
<tr>
<td>Number of Characters</td>
<td>The number of characters to include in a character word set. You only use this field when you select a Character or Markov type.</td>
</tr>
<tr>
<td>Threshold</td>
<td>The number of times a combination of letters must be found to include it in the Markov word set. You use this field only when you select the Markov type.</td>
</tr>
</tbody>
</table>
| Character Groups| The following specific character groups to use in the Character word set:  
  - Lowercase Letters: Searches for lowercase letters.  
  - Uppercase Letters: Searches for uppercase letters.  
  - Digits: Searches for numbers.  
  - Symbols: Searches for symbols, such as the plus sign (+) or the dollar sign ($).  
  - Diacritics: Searches for diacritics, such as the tilde (~) or the circumflex (^).  
  - All 7-bit Characters (ASCII): Searches for any ASCII characters. This box includes all characters listed above it.  
  - All 8-bit Characters: Searches for any ASCII and Extended ASCII characters. This box includes all characters listed above it and the Extended ASCII characters. |

You only use this list if you select the Character type.
3 Enter the necessary information in the form.
4 To add an additional type at the root level, select the level name and then click **Add**.
5 To remove any type in the hierarchy, select the type in the Hierarchy window and click **Remove**.
6 Click **OK**. Click **Cancel** if you do not want to save the information you entered on the form.

**Editing a User-defined Level**

You might want to edit a user-defined level to increase the effectiveness of the level. You can modify any of the information that you specify when you create a new level, such as the level name and the types used in the level.

To edit a user-defined level:

1 Select **Edit**, and then **Levels**.
2 In the User-defined Levels screen, select the level that you want to modify and then click **Edit**.
3 Enter the new information in the Level Editor form.
4 Click **OK**.
   Click **Cancel** if you do not want to save the information you entered on the form.

**Removing a User-defined Level**

You might delete a user-defined level if you no longer need its functionality in the files that you are processing.

You delete a level on the User-defined Levels form. To delete a user-defined level:

1 Select **Edit**, and then **Levels**.
2 In the User-defined Levels screen, select the level that you want to delete.
3 Click **Remove**, and then **Yes**.
Using the Dictionary Utility

Password Recovery Toolkit (PRTK) uses dictionaries to create possible passwords. You can create, import, and browse the dictionaries in PRTK.

Note: After you create or import any dictionary, you must add the dictionary to a profile. For more information, see “Editing a Profile” on page 128.

This chapter contains the following sections:

- “Dictionary Basics” on page 149
- “AccessData Dictionary Utility” on page 151
- “Dictionary Information” on page 152
- “Standard Dictionary Generator” on page 153
- “Biographical Dictionary” on page 155
- “Pass-phrase Dictionary Generator” on page 159
- “Permutation Dictionary Generator” on page 160
- “Merging Golden Dictionaries” on page 161

Dictionary Basics

PRTK uses dictionaries to discover the passwords that decrypt files. The dictionary attacks employ the default dictionaries included with the product as well as biographical and custom user dictionaries.
PRTK supports dictionaries in Arabic, English, French, German, Italian, Russian, and Spanish. All dictionaries are stored in the PRTK directory.

PRTK automatically stores all recovered passwords in a single file referred to as the Golden Dictionary. This file contains all recovered passwords (in both code page and Unicode) from all PRTK jobs. The Golden Dictionary is automatically created after PRTK recovers its first successful password.

Biographical dictionaries contain personal data, such as dates or phrases, significant to the person who created the password. Most passwords used with general applications contain some information about the person who locked the file; therefore, creating a dictionary that contains personal data on the person in question increases the probability that you can recover the password.

User dictionaries contain key phrases or words that are associated with the investigation but not with the person who locked a particular file.

Note: To create a user dictionary, enter one word per line in a standard text editor such as Notepad. Each term must be separated with a hard return.

During a dictionary attack, PRTK creates variations, permutations, and combinations of the biographical and user dictionaries. Additionally, it uses phonetic alterations, adds prefixes or suffixes, and substitutes characters.
By default, PRTK uses the following dictionaries in this order:
1. The Golden Dictionary
2. Biographical dictionary/As-is dictionaries
3. Those specified in the profile

**AccessData Dictionary Utility**

Dictionaries are an optimization used for password recovery. By using dictionaries, target specific candidate passwords are tested before the more general ones. This utility creates a variety of custom dictionaries for use with the Password Recovery Toolkit (PRTK™) and Distributed Network Attack (DNA™).

**Warning!** Make backup copies of word lists and dictionaries before using this utility. Once a dictionary has been modified or deleted, there may be no way to recover it.

**Starting the Dictionary Utility**

The AccessData Dictionary Utility allows you to create and manage the dictionaries of the Password Recovery Toolkit™ (PRTK) and Distributed Network Attack® (DNA) will use to help you find passwords.

To start the Dictionary Utility:

1. Start either PRTK or DNA.

2. From the **Tools** menu, click **Dictionary Tools**.

The following tools can be accessed from the Dictionary Tools menu:

<table>
<thead>
<tr>
<th>Tool</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionary Browser</td>
<td>This utility provides a way to view the words in each dictionary, or to delete a particular dictionary or dictionaries.</td>
</tr>
<tr>
<td>Dictionary Info</td>
<td>This utility provides a way to see the specific details about a dictionary, such as the dictionary type, encoding, language, word count, and a description.</td>
</tr>
</tbody>
</table>
If the tools complete successfully, they will generate multiple dictionaries that you will need to copy into the following directories:

- PRTK: Program Files/AccessData/PRTK 6/Dictionaries

**Dictionary Information**

The Dictionary Information tool provides a way to view details about an AccessData dictionary. The interface is divided into two different areas: the navigation controls and the details panel.

The navigation controls allow you to navigate your hard disk to the dictionaries that you have. Selecting a dictionary in the navigator displays the details for that dictionary in the details panel below. The navigator window shows only dictionary files and directories. Each dictionary file entry shows the filename, type, and the date the file was last modified.
The Details Panel shows the following information:

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encoding:</td>
<td>Codepage indicates a standard 8-bit character encoding; UTF-16LE indicates a 16-bit little-endian encoding. Only these encodings are supported at this time.</td>
</tr>
<tr>
<td>Language:</td>
<td>The special vocabulary and usages of a scientific, professional, or national group.</td>
</tr>
<tr>
<td>Word Count:</td>
<td>The number of words that the dictionary is supposed to have as indicated by its header.</td>
</tr>
<tr>
<td>Actual Count:</td>
<td>The number of words the dictionary actually has as counted by the Dictionary info tool.</td>
</tr>
<tr>
<td>Description:</td>
<td>An explanation of the dictionaries contents.</td>
</tr>
</tbody>
</table>

**Browse Dictionaries**

The Browse Dictionaries tool provides a way to view the contents of a dictionary, or to delete a dictionary. Use the mouse to select a dictionary file from the list of those found in the current directory.

- When you select a dictionary, click the View button to see a window containing a scrollable list of the dictionaries entries.
- Scroll by dragging the thumb up or down. When you select a dictionary and click the Delete button, a confirmation dialog opens to make sure you really want to delete the file.

**Warning!** You cannot recover a deleted dictionary. Be careful when deleting!

**Standard Dictionary Generator**

The Standard Dictionary Generator tool provides a way to create standard dictionaries from a source list of words. You can enter the full path or browse to the source word list file.
Once a file has been selected, the remainder of the controls will become available.

A source word list is provided in a text file where each word is separated from the others by a carriage return. You can use a phrase in place of a word since the tool does not try to separate the provided text, except at carriage returns.

Under the dictionary settings the language for the dictionary as well as the type of characters that occur in the dictionary can be specified. By unchecking one of the character types, that character type will be filtered from the phrases added to the dictionary.

The tool filters these character types:

<table>
<thead>
<tr>
<th>Character Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Letters</td>
<td>Alphabetic characters used to compose words. These include letters with diacritic marks and any other type of composed character used to construct words.</td>
</tr>
</tbody>
</table>
If the checkbox to restrict the length is checked, then the maximum length of each word, in characters can be specified. The permutation will be truncated to the specified length regardless of the resulting number of words that will remain in the generated permutation.

If the tool completes successfully, two dictionaries will have been created, one each for Unicode and Codepage encodings.

### Biographical Dictionary

The Biographical Dictionary tool creates dictionaries using personal data such as dates or phrases about the password creator.

### Biographical Dictionary Data

Since people use passwords that are easy to remember, the passwords often take the form of something meaningful to the person creating the password.

Just as a homeowner might invest in a high-quality door lock and then hide a key under the doormat, a computer user might install sophisticated encryption technology and then use glaringly obvious passwords:

- Names, dates, phone numbers, and addresses
- Birthdays, anniversaries, or other significant dates
- Interests and hobbies
- Pets, celebrities, family

<table>
<thead>
<tr>
<th>Character Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digits</td>
<td>Numeral characters (0–9).</td>
</tr>
<tr>
<td>Symbols</td>
<td>Symbol characters. These include punctuation and non-alpha or digit characters, but do not include the diacritic marks used for composed characters.</td>
</tr>
<tr>
<td>Diacritics</td>
<td>The special characters used in composed characters. If letters are included but diacritics are not, then the base letter will be preserved.</td>
</tr>
</tbody>
</table>
You can also glean valuable personal details for the biographical and user dictionaries by evaluating the physical evidence at an investigation site. Often the routine clues—sticky notes, phone number lists, date books, electronic lists (perhaps in a file named “passwords” on a hard drive or floppy disk), entries on a Palm Pilot/Pocket PC, or even a file on a thumb drive or the Compact Flash card in a digital camera—offer valuable information. Hiding places can range from the most ingenious to right out in plain sight. Be careful not to overlook the obvious.

The following can provide valuable clues at a crime scene:

- Books and magazines
- Photographs
- Calendars, day planners, and personal organizers
- Notes and mail, including e-mail
- Paraphernalia

In addition, reconstructing the alleged crime or using related evidence found at the scene can give the investigator clues which can be leveraged in the biographical dictionary. Additional clues can be observed by how the evidence interacts, how the suspect uses digital media, or how the times are related to evidence and events.

To understand how evidence relates to the crime, the investigator must evaluate the geographic location of people and computers as well as any communication or transactions that occurred between them. For example, in a fraud investigation involving thousands of people and computers, understanding where each party was located and how they interacted can reveal important information about the biography of the criminal. Sorting the financial transactions of individuals or organizations can also reveal patterns of behavior.
By observing the evidence at a scene and reconstructing the actions performed by the subject, you can create a more effective.

You can enter words or numbers in the Word field, such as the name of the individual that you are creating the dictionary about and the birthdate.

The Data drop-down menu lists the following types of personal information:

- Name
- Address
- City
- State
- ZIP Code
- Country
- Phone Number
- Number
- Word
- Phrase
- Date

Any combination and arrangement of the information you can think of will make your biographical dictionary more effective. Make every guess you can at a subject’s password, and enter as many versions of the guess as you can.

You can use a variety of different formats to enter numeric information, such as phone number and date. For example,
you can enter a phone number as 111.222.3334 or 111–222–3334. Enter as many different formats as you can think of.

To create a biographical dictionary:

1. Select **Dictionary Tools**, then **Biographical Dictionary Generator**.
2. Click the **Biographical Data** tab.
3. In the Data drop-down list, select the type of personal data to enter.
4. Type the personal data into the Word field, then click the **Add** button, or hit the Enter key.

   To remove a word and its type from the Word list, select the word and click the **Remove** button.

5. Click the **Generator** tab to create a dictionary based on the Word list, then specify your dictionary and word settings.

6. Click **Generate** and enter the name of the biographical dictionary.
The biographical dictionary is automatically added to the list of dictionaries in PRTK in codepage (-c), Unicode (-u), and as-is (-xml) formats.

**Pass-phrase Dictionary Generator**

A pass-phrase is a sub-phrase composed of some number of consecutive words from a provided source phrase. The tool generates all phrases from two words up to the configuration length specified in the user interface by sliding through the source phrase from start to finish. Source phrases are provided to the tool in a text file where each phrase is separated from the others by a carriage return.

Under the dictionary settings, you can specify the language as well as the type of characters that occur. By unchecking one of the character types, that character type will be filtered from the phrases added to the dictionary.

You can specify the number of words to use in each phrase as well as the maximum phrase length. By default, the maximum phrase restriction is disabled.
The phrase composition is the maximum number of consecutive words to use for each generated phrase. If the requested number of words is more than the total number of words in the source phrase, then the entire source phrase will be used. If the checkbox to restrict the phrase length is checked, you can specify the maximum length of the phrase in characters. The generated phrase will be truncated to the specified length regardless of the resulting number of words that will remain in the generated phrase.

If the checkbox to rotate the phrase is checked, each resultant phrase is rotated through all of the characters they contain.

**Permutation Dictionary Generator**

A permutation is simply some combination of words from a specified source list where each word is used once in the resultant sequence. This tool will generate all possible permutations from one to the number of words specified as the configuration in the user interface.

This tool provides a way to create dictionaries of the various permutations of a source list of words. You can enter the full path or browse to the source word list file. Once a file has been selected, the remainder of the controls will become available.
You can use a phrase in place of a word since the tool does not try to separate the provided text, except at carriage returns. A source word list where each word is separated from the others by a carriage return is provided in a text file.

You can specify the language for the dictionary as well as the type of characters that occur in the dictionary under the dictionary settings. By unchecking one of the character types, that character type will be filtered from the phrases added to the dictionary.

**Merging Golden Dictionaries**

Two dictionaries are needed in order to perform a merge: a source and a target.

The source dictionary can be either a 5.x or 6.x golden dictionary, while the target dictionary must be a 6.x golden dictionary.

When you click the merge button, the contents of the source dictionary are written into the target dictionary. The utility will display the following information:

- **Passwords Merged:** the number of passwords added from the source dictionary to the target dictionary to create the new golden dictionary

  **Note:** The Merge Golden Dictionary tools does not add duplicate passwords to the new dictionary.

- **Total Passwords:** the number of passwords contained in the new golden dictionary
Specialized Password Recoveries

This chapter reviews the steps required to perform the following specialized password recoveries:

- “Recovering Login Passwords” on page 164
- “Recovering Passwords from the Windows Registry” on page 168
- “Recovering AOL Communicator Account Passwords” on page 170
- “Recovering AOL Instant Messenger Passwords” on page 170
- “Recovering AOL Sign-on Passwords” on page 171
- “Recovering MSN Messenger Login Passwords” on page 171
- “Recovering Netscape .W and .S Files” on page 173
- “Recovering QuickBooks Passwords” on page 173
- “PRTK uses a decryption attack to recover the file passwords for QuickBooks 2002 or earlier. To open a recovered file, open it in QuickBooks and enter the recovered password when prompted. Recovering Yahoo! Messenger Login Passwords” on page 173
- “Recovering WinZip Archive Files” on page 174
Recovering Login Passwords

PRTK can recover the user login password from Windows NT 4.x, 2000, and XP systems. These passwords are located in the SAM file and system file found in the `drive:\Windows_directory\system32\config\` directory. Windows locks the SAM file and system file, it cannot be directly accessed through the operating system. Use FTK Imager to access these files.

Accessing the SAM file and the system file

To access the SAM file and system file, you must do one of the following:

- If you are using FTK Imager, copy the SAM file and system file.
  FTK Imager bypasses the Windows operating system, allowing you to copy the file underneath the Windows file lock. The only potential problem is that if the SAM file and system file are being written to during the copy operation, you might get a corrupted copy.

- If you have an image, extract the SAM file and system file from the `drive:\Windows_directory\system32\config\` directory.

- If you are not using FTK Imager or if you do not have an image, boot your computer from a boot disk and copy the SAM file and system file from the system drive.

To boot your computer from a boot disk and copy the SAM file and system file:

1. Restart the computer with a boot disk that is able to read your system drive.

   If the system drive is a FAT partition, you can use a Windows 98 boot disk. If the system drive is an NTFS partition, you must use a Linux or NTFS/OS boot disk.

2. After booting to the boot disk, go to the `drive:\Windows_directory\System32\config` directory.
3 Copy the SAM file and system file to another location, such as a floppy disk or a network directory.
4 Restart the computer normally.

Recovering Login Passwords on Windows NT

On Windows NT (not NT 4 SP3 or later), you can perform the password recovery after you obtain the SAM file and system file:

1 Start the recovery.
2 In PRTK, select Analyze, then Select Files, and then select the SAM file and system file, or drag and drop the SAM file and system file into the PRTK Window.
3 Specify the module options.
4 Select the profile to use.

PRTK analyzes the SAM file and system file and recovers the login password. Since there can be multiple users in the SAM file and system file, each with a unique password, the SAM file and system file are added to the file list multiple times—once for each recovered user password.

Recovering Passwords from Win 9x Files

PRTK can recover passwords from PWL files. PWL files are specific to Windows 9.x systems and are typically located in the drive:\Windows directory. They contain user-specific passwords such as the following:

- Mapped drive passwords
- Dial-up networking passwords
- Secure Website login passwords

Important: PRTK does not run on Windows 9.x systems. You cannot recover PWL files in their native environment. You must copy them to a Windows NT, 2000, or XP system.
A separate PWL file exists for each user on the current system. The actual filename is an 8.3 derivative of the user’s login name (for example, roy.pwl or elizabet.pwl).

To determine the user’s login name, check the system.ini folder in the Windows directory. The system.ini folder lists the login names of every user on the current system.

After you have determined the user’s login name, you can drag and drop the PWL file into the PRTK Window. When PRTK attempts to recover the passwords in the PWL file, it prompts you for the user’s login name. PRTK then retrieves the passwords within the file.

Recovering Login Passwords on Windows 2000 and XP Systems

On Windows NT 4 SP3 and later, Windows 2000, and Windows XP systems, PRTK must first have the SAM file and the appropriate system file before it can crack the login passwords in the SAM file and system file.

By default, the syskey is stored locally in the System registry file located in the drive:\Windows_directory\system32\config\ directory. The syskey is a utility that encrypts the hashed password information in a SAM database using a 128-bit encryption key.

**Important:** If the syskey is stored in the System registry file, it cannot be directly accessed because, like the SAM file and system file, Windows keeps it locked. Otherwise, the syskey could be stored on a floppy disk.

To access the system file on a computer that is not running PRTK, you must do one of the following:

- If you are using FTK Imager, copy the system file. Click the Obtain Restricted Files button and save the files to any location.
- If you have an image, extract the SAM file and system file from the drive:\Windows_directory\system32\config\ directory.
If you are not using FTK Imager or if you do not have an image, boot your computer from a boot disk and copy the SAM and system registry file from the hard drive.

To boot your computer from a boot disk and copy the System registry file:

1. Restart the computer with a boot disk that is able to read your system drive.

   If the system drive is a FAT partition, you can use a Windows 98 boot disk. If the system drive is an NTFS partition, you must use a Linux or NTFS-DOS boot disk.

2. After booting to the boot disk, go to the `drive:\Windows_directory\System32\config` directory.

3. Copy the SAM file and system file to another location, such as a floppy disk or a network directory.

4. Restart the computer normally.

To enter the SAM file and system file after obtaining it:

1. Add the SAM file and system file to PRTK.

2. Specify the module options.

   ![Module Options](image)

3. Specify the system file.

   - If the system file is on a hard drive or a network drive, browse to the system file.
If the computer requires a floppy disk to authenticate, select the startkey.key file from the floppy. If you do not specify the syskey, the syskey for the local machine is used.

**Important:** Without a valid system file or startkey.key file, the password will not be generated.

### Recovering Passwords from the Windows Registry

The Windows registry is essentially a set of data files that allows the Windows operating system to control hardware, software, user information, and the overall functionality of the Windows interface. Registry files are particularly useful for password recovery because they contain usernames and passwords for programs, e-mail, and Internet sites. For recovering login passwords, see “Accessing the SAM file and the system file” on page 164.

### Recovering Passwords from the Current Registry

PRTK can retrieve passwords for the following from the current machine’s live Windows registry:

- Internet Explorer Content Advisor
- Windows 9x/Me Screen Saver

To recover the password, copy the system.dat file to a machine running PRTK.

**Note:** PRTK does not recover screen saver passwords on Windows 2000 or XP systems. However, you can recover screen saver passwords on these systems using the SAM file and system file attack, because the screen saver password is the same as the user’s login password. For more information, see “Accessing the SAM file and the system file” on page 164.

### Recovering Passwords from the Registry Protected Storage Area

PRTK can recover the following from the protected storage area on the registry:

- Outlook and Outlook Express passwords
• Internet Explorer text fields, such as passwords, e-mails, and user names submitted online in text fields

The following table identifies the registry files required to recover these passwords on each operating system:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows NT/2000/XP</td>
<td>drive\Documents and Settings\user\ntuser.dat</td>
</tr>
<tr>
<td>Windows 9.x system with one configured user</td>
<td>drive\Windows_directory\system.dat</td>
</tr>
<tr>
<td>Windows 9.x systems with multiple configured users</td>
<td>drive\Windows_directory\Profiles\user\user.dat</td>
</tr>
</tbody>
</table>

Unfortunately, Windows locks these registry files; therefore, they cannot be directly accessed through the operating system.

To access these files, you must do one of the following:

• If you are using FTK Imager, copy the file.
  
  FTK Imager bypasses the Windows operating system, allowing you to copy the file underneath the Windows file lock. The only potential problem is that if the file is being written to during the copy operation, you might get a corrupted copy.

• If you have an image, extract the file from the file directory.

• If you are not using FTK Imager or if you do not have an image, boot your computer from a boot disk and copy the file from the system drive.
  
  To boot your computer from a boot disk and copy the ntuser.dat or user.dat file:

1. Restart the computer with a boot disk that is able to read your system drive.
If the system drive is a FAT partition, you can use a Windows 98 boot disk. If the system drive is an NTFS partition, you must use a Linux or NTFS-DOS boot disk.

2 After booting to the boot disk, go to the associated file directory.

3 Copy the file to another location, such as a floppy disk or a network directory.

4 Restart the computer normally.

After you obtain the ntuser.dat, system.dat, or user.dat file, you can perform the password recovery as follows:

1 Start the recovery job. In PRTK, select Analyze, then Select Files and then select the file, or drag and drop the file into the PRTK Window.

2 Specify the module options.

3 Select the profile to use.

PRTK analyzes the file and recovers the Outlook or Outlook Express password and the Internet Explorer text fields.

### Recovering AOL Communicator Account Passwords

AOL Communicator Account Passwords are encrypted in .pref files. The keys needed to decrypt the .pref files are contained in the keyS.db file, which is protected by the master password. To recover these passwords, PRTK does a dictionary attack on the keyS.db file. After the master password is recovered, the .pref files can be decrypted.

To recover an AOL Communicator Account Password, first recover the master password from keyS.db in `drive:\Documents and Settings\username\Application Data\NSS PKI Store\AOL;` then recover the .pref files in `drive:\Documents and Settings\username\Application Data\AOL Communicator`.

### Recovering AOL Instant Messenger Passwords

AOL Instant Messenger Passwords are stored in the storage area of the registry, located in the user’s ntuser.dat file.
To recover an AOL Instant Messenger Password:

1. Obtain the user’s ntuser.dat file.

To access the protected storage area of the registry, see “Recovering Passwords from the Registry Protected Storage Area” on page 168.

2. Add the ntuser.dat file to the PRTK job queu.

**Recovering AOL Sign-on Passwords**

For AOL versions 8.0 and 9.0, sign-on passwords (including guest logins) are encrypted in the main.idx file (`C:\Documents and Settings\All Users\Application Data\AOL\C_America Online \version\idb\main.idx`).

For AOL 9.0 Security Edition, sign-on passwords are encrypted in SNMaster.idx (`C:\Documents and Settings\All Users\Application Data\AOL\C_America Online \version\idb\SNMaster.idx`).

To recover an AOL Sign-on Password, you need the volume serial number of the C: drive. If there is no C: drive, AOL does not use the volume serial number and PRTK can immediately recover the sign-on passwords.

- If you are running PRTK on the original computer, PRTK automatically finds the serial number.
- If you are using FTK Imager, you can find the serial number in the Properties window. Once you know the volume serial number, enter it in the Module Options dialog in PRTK.
- If no volume serial number is supplied, PRTK begins a keyspace attack.

**Recovering MSN Messenger Login Passwords**

MSN Messenger Login passwords are recovered differently, depending on the Windows operating system.

**Note:** To recover an MSN Messenger Login password, the user must have selected the Remember Password option for the system to store this information.
Windows 95/98/ME

On Windows 95/98/Me systems, the password is obscured in the registry.

**Important:** PRTK does not run on Windows 9.x systems. Therefore, you cannot recover these passwords in their native environment. You must copy them to a Windows NT, 2000, or XP system.

To recover an MSN Messenger Login password:

1. Obtain the user’s ntuser.dat file.
   - To access the protected storage area of the registry, see “Recovering Passwords from the Registry Protected Storage Area” on page 168.
2. Copy the file to a machine running PRTK.
3. Add the ntuser.dat file to the PRTK job queue.

Windows 2000

On Windows 2000 systems, the password is encrypted in the registry. Before the password can be decrypted, the EFS master key files must be cracked.

To recover an MSN Messenger Login Password:

1. Recover the Windows login password from the SAM file and system file.
2. Copy the EFS master key files from `drive\Documents and Settings\username\Application Data\Microsoft\Protect\user_SID`.
3. Add the ntuser.dat file to the PRTK job queue.

**Note:** When used in conjunction with PRTK, FTK sends PRTK the EFS master key file, along with any other EFS-related keys. PRTK then performs an EFS attack to obtain the login password. FTK and PRTK must be running on the same dongle on the same machine to support this integrated functionality.
Windows XP

On Windows XP systems, the password is encrypted in the user’s credential file. The credential file cannot be decrypted until the EFS master key files are cracked.

To recover an MSN Messenger Login Password:

1. Recover the Windows login password from the SAM file and system file.
2. Copy the EFS master key files from `C:\Documents and Settings\username\Application Data\Microsoft\Protect\user_SID`.
3. Perform the password recovery on the credential file in `C:\Documents and Settings\username\Application Data\Microsoft\Credentials\user_SID\Credentials`.

Note: When used in conjunction with PRTK, FTK sends PRTK the EFS master key file, along with any other EFS-related keys. PRTK then performs an EFS attack to obtain the login password. FTK and PRTK must be running on the same dongle on the same machine to support this integrated functionality.

Recovering Netscape .W and .S Files

Netscape .W and .S files store sensitive user information such as credit card numbers and Website passwords. They are encrypted with a key stored in the `key3.db` file in the same directory (`C:\Documents and Settings\username\Application Data\Mozilla\Profiles\default\directory.slt`).

To recover Netscape .W and .S files, first recover the master password from `key3.db`, then recover the Netscape .W and .S files.

Recovering QuickBooks Passwords

PRTK resets the file passwords for QuickBooks 2003 or later. To open a recovered file, open it in QuickBooks and enter a blank password when prompted.

PRTK uses a decryption attack to recover the file passwords for QuickBooks 2002 or earlier. To open a recovered file, open it in QuickBooks and enter the recovered password when prompted.

Recovering Yahoo! Messenger Login Passwords
Yahoo! Messenger Login Passwords are stored in the protected storage area of the registry located in the user’s ntuser.dat file.

To recover a Yahoo! Messenger Login Password:

1. Obtain the user’s ntuser.dat file.
   - To access the protected storage area of the registry, see “Recovering Passwords from the Registry Protected Storage Area” on page 168.

2. Perform the password recovery.

   Note: You can use FTK to recover Yahoo! Messenger chat logs.

---

Recovering WinZip Archive Files

WinZip versions 6.0 through 8.1 have a security flaw in their encryption algorithm. By using a divide-and-conquer attack called the “WinZip Superfast Attack,” AccessData is able to exploit this flaw to recover files from archives created with these versions of WinZip.

Note: WinZip 9.0 files are encrypted with the AES (Advanced Encryption Standard) algorithm and therefore cannot be recovered using the WinZip Superfast Attack.

The WinZip Superfast Attack is not a standard key space attack. It breaks the key space down much more quickly than a linear key space because it intelligently narrows down the zip keys, effectively processing a trillion keys per second.

After the WinZip Superfast Attack recovers the zip keys, it attempts to recover the original password by performing a dictionary attack of passwords up to seven characters.

If Decrypt file when key is found is marked in the Preferences dialog, PRTK decrypts the file using the zip key. It then saves the file as filenameRecovered.zip in the directory designated in the Preferences dialog. The recovered file can be opened without a password. For more information on configuring the PRTK decryption options, see “Specifying Recovery Preferences” on page 81.
Using Recovered Passwords to Open Files

The following information details the methods you can use to open files from PRTK:

- “Copying a Recovered Password to the Clipboard” on page 175
- “Opening a File with a Recovered Password” on page 176
- “Opening Files with Multiple Passwords, Spare Passwords, or International Characters” on page 176

Copying a Recovered Password to the Clipboard

After PRTK recovers a password, you can copy the password to the clipboard to use when opening the file in its original application.

To copy a recovered password to the clipboard:

1. In the PRTK window, right-click a job that has a recovered password (listed in the Results column).
2. Select Copy password to clipboard from the menu.
Opening a File with a Recovered Password

After PRTK recovers a password, you can open the file in its original application from within PRTK.

**Note:** To open a file, the application in which the file was created must be available. For example, to open an Excel file, you must have Microsoft Excel installed on the computer.

To open a file with a recovered password:

1. In the PRTK window, right-click a job that has a recovered password (listed in the Results column).
2. Select **Open with default Application** from the menu.
3. When prompted for a password, paste the recovered password from the clipboard.

Opening Files with Multiple Passwords, Spare Passwords, or International Characters

In some recoveries, PRTK recovers multiple passwords, spare passwords, or passwords with international characters.

**Multiple Passwords**

In some recoveries, PRTK might recover multiple passwords. For example, for system files, PRTK might recover the access passwords for multiple users. For FTP program files, PRTK might recover the login passwords for multiple FTP sites. In some cases, a single file might have multiple passwords with different rights associated with them. For example, one password might be the open password and another might be the modify password.

**Spare Passwords**

In some recoveries, PRTK might not recover the original password that was used to lock the file, but might recover a “spare.” The spare password can consist of a string of numbers or a combination of alphanumeric characters.

For example, when performing a password recovery using the Paradox module, PRTK recovers a password that is a string of
numbers. This string of numbers acts just like a spare key to your car or home; it unlocks the document even though it is not the original password.

While they are not the original password, these spare passwords can be used to open the file.

To open a file that has a spare password, type the recovered password. If the recovered password does not unlock the file, please contact AccessData support.

International Passwords

PRTK has been used successfully to recover passwords for documents created in other languages, including Arabic, French, German, Italian, and Spanish.

When recovering passwords containing Extended ASCII or Unicode characters, PRTK displays password characters using the Microsoft Sans Serif font. Before opening a file, you need to determine the Alt keystrokes to enter for the password when opening the file.

To recover a password that has international characters:

1 After PRTK recovers a password with international characters, open the **Windows Character Map** (Start, then Programs, then Accessories, then System Tools, and then Character Map).

2 Select the **Microsoft Sans Serif** font.

   **Important:** Make sure you are using the correct font. PRTK uses Microsoft Sans Serif, and not MS Sans Serif.

3 In the lower-right corner of the window, find the Alt keystrokes necessary to enter the character code.

4 Open the file and, when prompted for the password, enter the Alt keystrokes for the character code displayed in the Microsoft Sans Serif character set.

   **Note:** When entering Alt keystrokes, make sure NUM LOCK is on. Hold down ALT, then, using the numeric keypad, type 0 (zero) followed by the character code.
Modifying a Job

After the program starts processing a job, you can rename a job, modify the status of a job, or delete a job.

Changing Job Name or Adding Comments

After you add a job to the jobs queue, you can change the name of the job or add comments about the job.

To change the job name or add comments:
1. In the job queue, select the job that you want to change.
2. Right-click the job and select Properties.
3. In the Information window, enter the new name or add comments.
4. Click Apply.

Pausing a Job

You might pause a job (or multiple jobs) if you want the DNA Workers to focus on decrypting a particular job. You also might pause a job if you want to delay decrypting the file for some other reason.

To pause a job:
1. In the job queue, select the file or files that you want to pause.
2. Right-click the job and then select Pause.

Resuming a Job

You can resume a job (or multiple jobs) after you suspend it. You might resume a job if you are ready for DNA to resume processing it.

To resume a job:
1. In the job queue, select the file or files that you want to resume processing.
2. Right-click and select Resume.
DNA continues to process the job after a DNA Worker becomes available.

Deleting a Job

Delete jobs if you no longer want the file decrypted or if you no longer need its decryption information. You can delete a job of any Status, such as Running or Finished.

If you delete a job that has other jobs dependent on its results, all the dependent jobs are deleted as well.

To delete a job:

1. In the job queue, select the file or files that you want to delete.
2. Right-click and select Delete.

Deleting All Jobs

Delete all jobs if you want to permanently clear the job queue to start decrypting a set of new files.

Warning: Do not select Delete All Jobs unless you want to permanently remove all jobs listed. This operation cannot be undone.

To delete all jobs, select Edit, and then Delete All Jobs.

Manually Decrypting Files with a Password or Key

After DNA discovers a password or key for an encrypted file, it displays the password or key in the Results section of the job Properties screen, shown below. You must then apply the password or key to decrypt the file.

Decrypting with a Key

You can choose to decrypt an encrypted file with a key on a file-by-file basis. You might decrypt a file individually because you want to closely manage the content of the decrypted file.

You can also choose to have DNA automatically decrypt the file after the key is discovered. For more information, see “Recovery Options” on page 100.
CHAPTER 12

Managing Licenses

This chapter acquaints you with the LicenseManager interface and describes how to manage licenses and update products using LicenseManager.

Note: While LicenseManager requires having an Internet connection to use some features, you can manage licenses in a dongle packet file for a dongle that resides on a machine not connected to the Internet.

For information about installing LicenseManager, see “Installing LicenseManager from Downloadable Files” on page 22. For information about starting LicenseManager, see “Starting LicenseManager” on page 182.

This chapter is divided into the following sections:
- “Managing Licenses with LicenseManager” on page 181
- “LicenseManager Interface” on page 184
- “Opening and Saving Dongle Packet Files” on page 188
- “Viewing Product Licenses” on page 188
- “Adding and Removing Product Licenses” on page 188
- “Updating Products” on page 192
- “Purchasing Product Licenses” on page 193
- “Sending a Dongle Packet File to Support” on page 194

Managing Licenses with LicenseManager

LicenseManager lets you manage product licenses on a dongle or in a dongle packet file.
With LicenseManager, you can view license information, add or remove existing licenses for a dongle or dongle packet file, renew your subscription, purchase licenses, and send a dongle packet file to AccessData support. You can also check for product updates and download the latest product versions.

LicenseManager displays dongle information (including packet version and serial number) and licensing information for such products as FTK, PRTK, DNA, and Registry Viewer. The licensing information provides the following:

- Name of the program
- Subscription expiration date
- Number of DNA clients, if any
- Latest version of the program

Starting LicenseManager

To start LicenseManager, select Help, then Launch LicenseManager or select Start, then Programs, then AccessData, then LicenseManager, and then LicenseManager.

Note: LicenseManager.exe is located in the drive:\Program Files\AccessData\Common Files\AccessData LicenseManager directory.
When you start LicenseManager, it reads licensing and subscription information from the dongle.

If you are using a dongle, and LicenseManager either does not open or display the message “Dongle not found.”
- Make sure the dongle drivers are installed.
  
  For more information, see “If you have a USB dongle, plug it in.” on page 18 or “Installing the Dongle Drivers from Downloadable Files” on page 21.
- Make sure the dongle is connected to the USB or parallel port.
- In LicenseManager, select File, and then Reload from Dongle.

If you do not have a dongle installed, LicenseManager lets you manage licenses using a dongle packet file.

To open LicenseManager without a dongle installed:

1. Run LicenseManager by selecting Help, and then Launch LicenseManager or by selecting Start, then Programs, then AccessData, then LicenseManager, and then LicenseManager.
   
   LicenseManager displays the message “Dongle not found.”

2. Click OK; then browse for a dongle packet file to open.

When you start LicenseManager, you are prompted to check the update site for the latest product versions. You can also choose not to be prompted to check for updates when starting LicenseManager.

Important: If you disable the option to display this prompt at startup, you cannot turn it back on. However, you can still check the update site for the latest product versions by selecting AccessData, and then Check for Updates within LicenseManager.
LicenseManager Interface

The LicenseManager interface consists of the menu bar, toolbar, and options in the LicenseManager window. The following sections discuss each of these elements.

The Menu Bar

The menu bar in the LicenseManager interface lets you access product features.

The following table describes the items found in the LicenseManager menu bar:

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Menu</strong></td>
<td>Reload from Dongle, Read from File, Save to File, and Exit. The File menu lets you get license information on the dongle, open or save a dongle packet file (with a .pkt extension), or exit LicenseManager.</td>
</tr>
<tr>
<td><strong>View Menu</strong></td>
<td>Registration Info, Toolbar, and Status Bar. The View menu lets you view product subscriptions associated with the dongle or dongle packet file and subscriptions available to be associated with a dongle or dongle packet file (when connected to the Internet), and show or hide the toolbar and status bar.</td>
</tr>
</tbody>
</table>
| **AccessData Menu** | Add Existing License, Purchase Licenses, Check for Updates, and Finalize Removal. These pages all require an Internet connection.  
Add Existing License opens Webpages where you can add an unassociated license to the dongle or dongle packet file. For more information, see “Adding and Removing Product Licenses” on page 188.  
Purchase Licenses allows you to purchase new products and add them to your current dongle or dongle packet file. For more information, see “Purchasing Product Licenses” on page 193.  
The Check for Updates feature checks the AccessData Website and returns the current version numbers for each product. If there is a new version of License Manager, the Check for Updates feature also prompts you to update LicenseManager.  
Finalize Removal removes a license from a dongle packet file for a dongle that resides on a machine that is not connected to the Internet. For more information, see “Adding and Removing Product Licenses Remotely” on page 189. |
The Toolbar

The LicenseManager toolbar, shown below, provides easy access to various functions in LicenseManager.

The following table shows each toolbar icon and describes its associated function:

<table>
<thead>
<tr>
<th>Toolbar Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Open an existing dongle packet file.</td>
</tr>
<tr>
<td></td>
<td>Save the current dongle packet file.</td>
</tr>
</tbody>
</table>

Menu Item | Description
---|-------------------------------------------------|
Help Menu | About LicenseManager. The Help menu lets you view information about LicenseManager.
The LicenseManager Window

The LicenseManager window displays dongle information for the current dongle packet file and licensing information for available AccessData products.

The dongle information provides the following:

- Packet Version
- Serial Number
- Company Name (subscriber)

The licensing information provides the following:

- Name of the program
- Subscription expiration date
- Number of DNA clients, if applicable
- Latest version of the program
The following table describes the items in the LicenseManager window:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Version</td>
<td>Displays the version of the dongle packet.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Displays the unique number assigned to each dongle.</td>
</tr>
<tr>
<td>Company Name</td>
<td>Displays the name of the company for the subscription.</td>
</tr>
<tr>
<td>UTK Dongle or Beta</td>
<td>Indicates whether the dongle is an Ultimate Toolkit (UTK) or a beta version. A UTK dongle is one where all products in the Ultimate Toolkit are on the dongle.</td>
</tr>
<tr>
<td>Dongle</td>
<td></td>
</tr>
<tr>
<td>Licensing Information</td>
<td>Displays product name, subscription expiration date, number of DNA clients, and product version for listed items.</td>
</tr>
<tr>
<td></td>
<td>The Expiration Date displays expiration dates for product licenses associated with the dongle or dongle packet file.</td>
</tr>
<tr>
<td></td>
<td>When connected to the Internet, clicking a listed version number under Latest Version prompts whether to download the installation program for the latest product version.</td>
</tr>
<tr>
<td>Install Newest Versions</td>
<td>Prompts whether to download the latest product installation program for the selected products.</td>
</tr>
</tbody>
</table>
| Remove from Dongle      | Lets you remove selected product licenses from the dongle or dongle packet file when connected to the Internet. (Clicking Remove from Dongle does not cancel product subscriptions.) You can register available (but unassociated) product licenses with another dongle or dongle packet file.
|                         | To finalize the removal of a license in a dongle packet file for a dongle on another machine (where you cannot or do not want to connect to the Internet), select AccessData, and then Finalize Removal. |
| Refresh Dongle          | When connected to the Internet, lets you update the dongle with the product license information in the AccessData Website database.       |
|                         | Conversely, to display license information currently stored on the dongle, select File, and then Reload from Dongle.                    |
Opening and Saving Dongle Packet Files

You can open or save dongle packet files using LicenseManager. When started, LicenseManager attempts to read licensing and subscription information from the dongle. If you do not have a dongle installed, LicenseManager lets you browse to open a dongle packet file.

To open a dongle packet file:
1. Select File, and then Read from File.
2. Browse for a dongle packet file to open; then click Open.

To save a dongle packet file:
1. Select File, and then Save to File.
2. Specify the folder and name of the .pkt file; then click Save.

Viewing Product Licenses

LicenseManager lets you view product license information for products registered (or associated) with the dongle or dongle packet file.

To view product licenses that are associated with a dongle, select File, and then Reload from Dongle.

To view all available product licenses that are or can be associated with a dongle (according to Website database), select View, and then Registration Info.

Note: To synchronize the dongle with the product license information in the AccessData Website database, click Refresh Dongle.

Adding and Removing Product Licenses

On a computer with an Internet connection, LicenseManager lets you add available product licenses to or remove them from a dongle.

To move a product license from one dongle to another dongle, first remove the product license from a dongle; then add the product license to another dongle.

To add (associate) a product license:
1 Select AccessData, and then Add Existing License.

2 On the Website page, select the product license you want to add; after an update file downloads and installs, then click OK.

3 Click Yes when the LicenseManager prompts, “Were you able to associate a new product with this dongle?”

To remove (unassociate) a product license:

1 Mark the program whose license you want to remove, and then click Remove from Dongle.

2 When prompted to remove the selected license from the dongle, click Yes.

3 After an update file downloads and installs, click OK. The message, “Your license was successfully removed!” appears.

Adding and Removing Product Licenses Remotely

While LicenseManager requires an Internet connection to use some features, you can add or remove licenses from a dongle packet file for a dongle that resides on a computer, such as a forensic lab computer, that does not have an Internet connection.

If you cannot connect to the Internet, the easiest way to move licenses from one dongle to another is to physically move the dongle to a computer with an Internet connection, add or remove product licenses as necessary using LicenseManager, and then physically move the dongle back to the original computer. However, if you cannot move the dongle—due to organization policies or a need for forensic soundness—then transfer the packet files and update files remotely.

To remotely add or remove product licenses, you must transfer the dongle packet file to a computer with an Internet connection so you can open the dongle packet file and add or remove product licenses. You must then copy and run the update file on the original computer where the dongle resides.

To remotely move a product license from one dongle to another dongle, first remove the product license from the
Adding a Product License Remotely

To remotely add (associate) a product license:

1 On the computer where the dongle resides:
   1a Select File, and then Reload from Dongle in LicenseManager to read the dongle license information.
   1b Save the dongle packet file to the local machine.

2 Copy the dongle packet file to a computer with an Internet connection.

3 On the computer with an Internet connection:
   3a Open the copied dongle packet file in LicenseManager.
   3b Select AccessData, and then Add Existing License.
   3c Complete the process to add a product license on the Website page.
   3d Click Yes when the LicenseManager prompts, “Were you able to associate a new product with this dongle?”

When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted to save the update file.

   3e Save the update file to the local machine.

4 After the update file is downloaded, copy the update file to the computer where the dongle resides:

5 On the computer where the dongle resides:
   5a Run the update file.
   5b After an update file downloads and installs, click OK.
5c Select **File**, and then **Reload from Dongle** in LicenseManager to verify the product license has been added to the dongle.

6 On the computer with an Internet connection, select **View**, and then **Registration Info** in LicenseManager to see license information for associated and unassociated product licenses.

Removing a Product License Remotely

To remotely remove (unassociate) a product license:

1 On the computer where the dongle resides:
   1a Select **File**, and then **Reload from Dongle** in LicenseManager to read the dongle license information.
   1b Save the dongle packet file to the local machine.

2 Copy the file to a computer with an Internet connection.

3 On the computer with an Internet connection:
   3a Open the copied dongle packet file in LicenseManager.
   3b Select the product license you want to unassociate; then click **Remove from Dongle**.
   3c When prompted to remove the selected license from the dongle, click **Yes**.

   When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted save the update file.
   3d Click **Yes** to save the update file to the local computer.

   The Step 1 of 2 dialog details how to use the dongle packet file to remove the license from a dongle on another computer.

   3e Save the update file to the local machine.
4 After the update file is downloaded, copy the update file to the computer where the dongle resides.

5 On the computer where the dongle resides:
   5a Run the update file.
   5b Select File, and then Reload from Dongle in LicenseManager to verify the product license is removed from the dongle.
   5c Save the dongle packet file to the local machine.

6 Copy the file to a computer with an Internet connection.

7 On the computer with an Internet connection:
   7a Open the copied dongle packet file in LicenseManager.
   7b Select AccessData, and then Finalize Removal.

   Note: On the computer with an Internet connection, click View, and then Registration Info in License Manager to see license information for associated and unassociated product licenses.

**Updating Products**

You can use LicenseManager to check for product updates and download the latest product versions.

For more information on the general features of the subscription service, see the AccessData Website at http://www.accessdata.com/subscription_renewal.htm.

**Checking for Product Updates**

To check for product updates, select AccessData, and then Check for Updates.

When checking for updates, LicenseManager checks for an updated version of LicenseManager. If there is one, a prompt appears. When prompted whether to update LicenseManager, click Yes to download and install the latest product version, or click No to update product version information for the products listed in the LicenseManager window.
To determine whether you have the latest version of a product:

1. Check for updates.
2. In the product you want to verify, select **Help**
3. Select **About**, and compare the product version with the latest version number listed in the LicenseManager window.

### Downloading Product Updates

To download a product update:

1. Ensure that LicenseManager displays the latest product information by selecting **AccessData**, and then **Check for Updates**.
2. Select a program you want to download; then click **Install Newest Versions**.
   
   You can also click a version number in the Latest Version column.
3. When prompted, click **Yes** to download the latest install program of the product.
4. Save the product update file.
5. If installing the update on a remote computer, copy the product update file to another computer.
6. Install the product update.

   For information about installing the product update, refer to the installation information for the product.

### Purchasing Product Licenses

You can use LicenseManager to link to the AccessData Website where you can purchase products.

To purchase a product, select **AccessData**, and then **Purchase Licenses**.

**Note:** Once a product has been purchased and appears in the AccessData Website database, you can add the product license to a dongle or dongle packet file by clicking **Refresh Dongle**.
Sending a Dongle Packet File to Support

Send a dongle packet file only when specifically directed by AccessData Support.

To send a dongle packet file, e-mail it to:
support@accessdata.com.
CHAPTER 13

Troubleshooting

This chapter explains how to troubleshoot Password Recovery Toolkit (PRTK) in the following areas:

- “Installation” on page 196
- “Password Recovery” on page 197
- “Password Recovery” on page 197
- “Troubleshooting DNA” on page 198
## Installation

This section contains solutions to common PRTK installation and upgrade issues and questions.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>I installed PRTK on a new machine, and my dongle is not working.</td>
<td>Dongle isn’t installed properly.</td>
<td>If you do not install the dongle driver correctly, then the product displays “A dongle was not detected. PRTK is now running in DEMO Mode. You will be able to run only jobs with the free modules” message at startup. To make sure you installed the driver correctly, check the following: Make sure the dongle security hardware is plugged in to the correct port during installation of the dongle driver. If you do not use the dongle, you cannot access licensed versions of the application modules or use those applications to recover passwords.</td>
</tr>
</tbody>
</table>

How can I download the full version of PRTK from the AccessData Website so that I can use the product immediately? The full version of PRTK requires a dongle driver for security management. When you download PRTK from the Web. You cannot use the full version of PRTK until the dongle has been shipped an installed.
## Password Recovery

This section contains solutions to the most common PRTK password recovery issues and questions.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When I try to recover a password-protected file, PRTK returns the message “Finished. Password not found” What should I do now?</td>
<td>If the recovery failed, then the password could not be located in your custom or default dictionaries. You need to re-evaluate the evidence and create a more detailed custom dictionary.</td>
<td>When running a dictionary attack, provide as much information as possible about the person who locked the file. This information can be defined in a biographical dictionary or a custom user dictionary.</td>
</tr>
<tr>
<td>I know that my Excel/Word password is made up of all letters or all numbers. Can this information help me recover my password more quickly?</td>
<td>Create a specific profile for this case.</td>
<td></td>
</tr>
<tr>
<td>Why can’t I recover my Zip file?</td>
<td>Attack needs more time.</td>
<td>The program uses SuperFast Zip Attack if your archive contains five or more files and was created with WinZip 8.0 or an earlier version. This attack generally takes around 2 to 3 hours.</td>
</tr>
<tr>
<td>Why don’t the Quicken 2002, QuickBooks 2002, WinZip, or VBA files appear in the clipboard after I recover the password?</td>
<td>You did not recover the password for these files; instead, you decrypted the file using the key.</td>
<td>You can access the decrypted version of your file at the location you specified when setting up.</td>
</tr>
</tbody>
</table>
## Troubleshooting DNA

This chapter contains solutions to the following commonly asked questions.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRTK has been running a dictionary attack for a very long time. Is this normal?</td>
<td>Yes.</td>
<td>Double-click the file in PRTK to see the progress. If the number of passwords tested is still increasing, then the recovery is still running.</td>
</tr>
<tr>
<td>If my computer crashes during a lengthy password recovery, how do I recover the work that was already performed?</td>
<td>Restart the program.</td>
<td>PRTK continues the password recovery process for jobs in the session when you restart PRTK.</td>
</tr>
</tbody>
</table>
| I cannot add a file to the jobs queue from a different network machine. Why? | Although you might be able to see the file in Windows Explorer, the SYSTEM account, which DNA uses, does not have adequate permissions to access the network file. | You must have administrator rights to access the file so that the Distributed Network Attack (DNA) Server, which runs as a System service, can also access the file.  
1. Copy the network file to the local machine.  
2. Add the file to DNA. |
<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why is a DNA Worker not responding?</td>
<td>The DNA Worker lost its connection to the network or is turned off.</td>
<td>1. Try to ping the DNA Worker machine from the DNA Supervisor machine.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. If you can ping the Worker machine, but the DNA Worker is still not responding, then reboot the computer that is running the DNA Worker.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. If you cannot ping the Worker machine, verify that the worker machine is turned on, and try to access network services on it, such as the Internet or printing.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. If the DNA Worker is still not responding, see the system administrator or call AccessData.</td>
</tr>
<tr>
<td>The Stop Worker on User Input option has been selected.</td>
<td></td>
<td>Uncheck the option.</td>
</tr>
<tr>
<td>After I added a job and DNA worked on it, the Password/User Password column read “Empty Password.” Why?</td>
<td>The file is encrypted, but the password is empty or contains no characters.</td>
<td>To unlock the file, press Enter when you are prompted for a password.</td>
</tr>
<tr>
<td>I added a job, and DNA has still not located the password. Why?</td>
<td>Finding passwords can take a long time. Also, recovery isn’t guaranteed for applications that use stronger than 40-bit encryption.</td>
<td>Install more DNA Workers with at least the recommended processor requirements. The more machines that DNA can use, the faster it can run its tests.</td>
</tr>
</tbody>
</table>
Add Job Processing Results

After processing jobs to be added, PRTK displays results in the Processing results dialog. The following are possible results:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancelled</td>
<td>You canceled the processing of the job.</td>
</tr>
<tr>
<td>Corrupted</td>
<td>The file is corrupted.</td>
</tr>
<tr>
<td>Failed to Process</td>
<td>The file cannot be added to the system. This result is a general tag used for any file that cannot be classified as any other result.</td>
</tr>
<tr>
<td>File in Use</td>
<td>The file is locked by another program.</td>
</tr>
<tr>
<td>Successfully Added</td>
<td>The file is added to the job queue.</td>
</tr>
<tr>
<td>Timed Out</td>
<td>The file cannot be identified by PRTK in five minutes. This result usually appears when PRTK is busy processing other jobs.</td>
</tr>
<tr>
<td>Unencrypted</td>
<td>The file doesn’t need to be added because the file isn’t encrypted.</td>
</tr>
<tr>
<td>Unidentifiable</td>
<td>PRTK cannot recognize the file and its source application.</td>
</tr>
</tbody>
</table>

What is the difference between the owner keys and passwords and the user keys and passwords?

PDF documents have both owner and user passwords. The owner password is used to open and edit the file. The user password is used to open and read the file.

Use either the owner or user password to unlock the PDF document. Generally, you use the user password to unlock the document. However, in some instances you might use the owner password to modify the file.

For example, if the file creator has forgotten the password, you might create a new password for the file.

Problem Possible Cause Solution

What is the difference between the owner keys and passwords and the user keys and passwords? PDF documents have both owner and user passwords. The owner password is used to open and edit the file. The user password is used to open and read the file. Use either the owner or user password to unlock the PDF document. Generally, you use the user password to unlock the document. However, in some instances you might use the owner password to modify the file.

For example, if the file creator has forgotten the password, you might create a new password for the file.

Add Job Processing Results

After processing jobs to be added, PRTK displays results in the Processing results dialog. The following are possible results:

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancelled</td>
<td>You canceled the processing of the job.</td>
</tr>
<tr>
<td>Corrupted</td>
<td>The file is corrupted.</td>
</tr>
<tr>
<td>Failed to Process</td>
<td>The file cannot be added to the system. This result is a general tag used for any file that cannot be classified as any other result.</td>
</tr>
<tr>
<td>File in Use</td>
<td>The file is locked by another program.</td>
</tr>
<tr>
<td>Successfully Added</td>
<td>The file is added to the job queue.</td>
</tr>
<tr>
<td>Timed Out</td>
<td>The file cannot be identified by PRTK in five minutes. This result usually appears when PRTK is busy processing other jobs.</td>
</tr>
<tr>
<td>Unencrypted</td>
<td>The file doesn’t need to be added because the file isn’t encrypted.</td>
</tr>
<tr>
<td>Unidentifiable</td>
<td>PRTK cannot recognize the file and its source application.</td>
</tr>
</tbody>
</table>

200 Password Recovery Toolkit User Guide

<table>
<thead>
<tr>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsupported Version</td>
<td>The file was created in an unsupported version of a supported application.</td>
</tr>
</tbody>
</table>
Supported Applications and File Formats

This appendix lists the applications and file formats that Password Recovery Toolkit (PRTK) supports and their corresponding PRTK modules.

The appendix is divided into sections based on the attack type that PRTK uses to decrypt the file. The last section lists applications that use multiple attack types.

- “Decryption Attack” on page 204
- “Dictionary Attack” on page 208
- “Keyspace Attacks” on page 212
- “Reset attack is the least common attack type used by PRTK because few applications are susceptible to it.” on page 213
**Decryption Attack**

The decryption attack decrypts the password that locks the file. PRTK uses the decryption attack on the applications listed in the following table.

<table>
<thead>
<tr>
<th>Supported Application</th>
<th>PRTK Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT! 1–4, 2000, 5–6</td>
<td>ACT! Password Module</td>
</tr>
<tr>
<td>AOL Instant Messenger through 5.9, AIM</td>
<td>AIM Password Module</td>
</tr>
<tr>
<td>Triton through 1.0.4</td>
<td></td>
</tr>
<tr>
<td>AOL 8.0–9.0 Security Edition</td>
<td>AOL Password Module</td>
</tr>
<tr>
<td>Ascend</td>
<td>Ascend Password Module</td>
</tr>
<tr>
<td>BulletProof FTP 1.03–2.45</td>
<td>BPFTP Password Module</td>
</tr>
<tr>
<td>CuteFTP 2–5, 7x</td>
<td>CuteFTP Password Module</td>
</tr>
<tr>
<td>DataPerfect</td>
<td>DataPerfect Password Module</td>
</tr>
<tr>
<td>dBASE 2.x–3.x</td>
<td>dBASE Password Module</td>
</tr>
<tr>
<td>EasyCrypto 5.5</td>
<td>EasyCrypto Password Module</td>
</tr>
<tr>
<td>FileMaker 3.x, 5.x</td>
<td>FileMaker Password Module</td>
</tr>
<tr>
<td>Hello 1.0</td>
<td>Hello Password Module</td>
</tr>
<tr>
<td>ICQ 2003b–5.04</td>
<td>ICQ Password Module</td>
</tr>
<tr>
<td>Internet Explorer 5.0–6.0 AutoComplete database</td>
<td>Protected Registry Module</td>
</tr>
<tr>
<td>Note: This module is also used for Outlook Express.</td>
<td></td>
</tr>
</tbody>
</table>

Kaikei through 05                        | Kaikei Password Module|

---

204  Password Recovery Toolkit User Guide
### Supported Applications and File Formats

<table>
<thead>
<tr>
<th>Supported Application</th>
<th>PRTK Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lotus 1-2-3 of the following versions:</td>
<td>Lotus 123 Password Module</td>
</tr>
<tr>
<td>• 1A–4</td>
<td>Note: This module is also used</td>
</tr>
<tr>
<td>• 9</td>
<td>for Lotus Symphony 1–2 and Lotus</td>
</tr>
<tr>
<td>• 97</td>
<td>1-2-3 seal passwords.</td>
</tr>
<tr>
<td>• FRM</td>
<td></td>
</tr>
<tr>
<td>• Japanese</td>
<td></td>
</tr>
<tr>
<td>Lotus 1-2-3 seal passwords</td>
<td>Lotus 123 Password Module</td>
</tr>
<tr>
<td>Note: This module is also used for Lotus</td>
<td>Symphony and Lotus 1-2-3.</td>
</tr>
<tr>
<td>Lotus Approach through 97</td>
<td>Lotus Approach Password Module</td>
</tr>
<tr>
<td>Lotus Organizer 1–4</td>
<td>Lotus Organizer Password Module</td>
</tr>
<tr>
<td>Lotus Symphony 1–2</td>
<td>Lotus 123 Password Module</td>
</tr>
<tr>
<td>Note: This module is also used for Lotus 1-2-3 and Lotus 1-2-3 seal passwords.</td>
<td></td>
</tr>
<tr>
<td>Lotus WordPro 96, 97, or Millenium</td>
<td>WordPro Password Module</td>
</tr>
<tr>
<td>Messenger Plus! 3.50–3.61</td>
<td>MessengerPlus Password Module</td>
</tr>
<tr>
<td>Microsoft Access</td>
<td>MS Access Encryption Module</td>
</tr>
<tr>
<td>Microsoft Money 2002–2006</td>
<td>MS Money Password Module</td>
</tr>
<tr>
<td>Microsoft Office Data (PST) files 2003 or earlier</td>
<td>MS Outlook PST Password Module</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>Microsoft Office Encryption</td>
</tr>
<tr>
<td>• Excell 2–7, 97, 2000, XP, 2003</td>
<td>Module</td>
</tr>
<tr>
<td>• Word 2–6, 97, 2000, XP, 2003</td>
<td></td>
</tr>
<tr>
<td>• PowerPoint XP, 2003</td>
<td></td>
</tr>
<tr>
<td>Microsoft Project 98–2003</td>
<td>MS Project Password Module</td>
</tr>
<tr>
<td>Microsoft Schedule+ 7.x</td>
<td>Scheduler Password Module</td>
</tr>
</tbody>
</table>

---

**Supported Applications and File Formats** 205
<table>
<thead>
<tr>
<th>Supported Application</th>
<th>PRTK Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SourceSafe 6x</td>
<td>SourceSafe Password Module</td>
</tr>
<tr>
<td>Microsoft Visual SourceSafe 6.x</td>
<td>SourceSafe Password Module</td>
</tr>
<tr>
<td>Mozilla ProtectedData</td>
<td>Mozilla Protected Data Module</td>
</tr>
<tr>
<td>• Mozilla 1.7x</td>
<td></td>
</tr>
<tr>
<td>• AOL Communicator through 20030919.3</td>
<td></td>
</tr>
<tr>
<td>• Mozilla Firefox through 1.5</td>
<td></td>
</tr>
<tr>
<td>• Netscape 7.x–8.0</td>
<td></td>
</tr>
<tr>
<td>MS Backup</td>
<td>MS Backup Password Module</td>
</tr>
<tr>
<td>MS Mail</td>
<td>MS Mail Password Module</td>
</tr>
<tr>
<td>MSN Messenger through 7.0</td>
<td>MSN Messenger Password Module</td>
</tr>
<tr>
<td>MYOB</td>
<td>MYOB Password Module</td>
</tr>
<tr>
<td>• Plus 3.x</td>
<td></td>
</tr>
<tr>
<td>• Premier Accounting 2005–2006</td>
<td></td>
</tr>
<tr>
<td>• Business Basics 2</td>
<td></td>
</tr>
<tr>
<td>Netscape Mail through 6.x</td>
<td>Netscape Mail Password Module</td>
</tr>
<tr>
<td>Outlook Express 5.0–6.0, SMTP password</td>
<td>Protected Registry Module</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This module is also used for Internet Explorer.</td>
</tr>
<tr>
<td>Palm Pilot User File</td>
<td>Palm Password Module</td>
</tr>
<tr>
<td>Paradox 4.x, 5.x, or 7.x</td>
<td>Paradox Password Module</td>
</tr>
<tr>
<td>PasswordPal through 2.0</td>
<td>PasswordPal Password Module</td>
</tr>
<tr>
<td>Protected Registry</td>
<td>Protected Registry Module</td>
</tr>
<tr>
<td>• Microsoft Internet Explorer 5.0–6.0</td>
<td></td>
</tr>
<tr>
<td>• Microsoft Outlook Express 5.0–6.0</td>
<td></td>
</tr>
<tr>
<td>ProWrite</td>
<td>ProWrite Password Module</td>
</tr>
<tr>
<td>Supported Application</td>
<td>PRTK Module</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>PC Encrypt through 9.11</td>
<td>PC Encryption Encryption Module</td>
</tr>
<tr>
<td>PST through 2003</td>
<td>MS Outlook PST Password Module</td>
</tr>
<tr>
<td>PWL</td>
<td>PWL Password Module</td>
</tr>
<tr>
<td>Quattro Pro 1–12, X3</td>
<td>Quattro Pro Password Module</td>
</tr>
<tr>
<td>Quickbooks through 2002</td>
<td>Quickbooks Password Module</td>
</tr>
<tr>
<td>Quicken through 2001</td>
<td>Quicken Password Module</td>
</tr>
<tr>
<td>SAMFile</td>
<td>SAM File Module</td>
</tr>
<tr>
<td>• SAM Files LAN Hash, NT Hash (MD4)</td>
<td></td>
</tr>
<tr>
<td>• Active Directory</td>
<td></td>
</tr>
<tr>
<td>Steganos</td>
<td>Steganos Password Module</td>
</tr>
<tr>
<td>• Security Suite</td>
<td></td>
</tr>
<tr>
<td>• LockNote</td>
<td></td>
</tr>
<tr>
<td>Symantec QA 4.x–5.x</td>
<td>SymantecQA Password Module</td>
</tr>
<tr>
<td>VBA</td>
<td>VBA Password Module</td>
</tr>
<tr>
<td>VersaCheck</td>
<td>VersaCheck Password Module</td>
</tr>
<tr>
<td>• VersaCheck 2001 Home and Pro</td>
<td></td>
</tr>
<tr>
<td>• VersaCheck Platinum 2004–2007</td>
<td></td>
</tr>
<tr>
<td>• VersaCheck Enterprise 2004–2007</td>
<td></td>
</tr>
<tr>
<td>Whisper 32 1.16 or earlier</td>
<td>Whisper Password Module</td>
</tr>
<tr>
<td>Windows 95 Screen Saver</td>
<td>Screen Saver Password Module</td>
</tr>
<tr>
<td>Windows XP Credential Files in Windows XP</td>
<td>XP Credentials Module</td>
</tr>
<tr>
<td>through Service Pack 2</td>
<td></td>
</tr>
<tr>
<td>WordPerfect 5.0–12, X3</td>
<td>WordPerfect Password Module</td>
</tr>
<tr>
<td>WS_FTP 5.0x, 2006</td>
<td>WS_FTP Encryption Module</td>
</tr>
<tr>
<td>Yahoo! Messenger 3.0–7.0</td>
<td>Yahoo! Messenger Password Module</td>
</tr>
</tbody>
</table>
Dictionary Attack

The dictionary attack uses the words in a dictionary, applies levels to the words, and applies the password to the files. PRTK uses the dictionary attack on the applications listed in the following table.

<table>
<thead>
<tr>
<th>Supported Application</th>
<th>PRTK Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yayoi Kaikei 05 or earlier</td>
<td>Kaikei Password Module</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supported Application</th>
<th>PRTK Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABI Coder 3.5.7.4–3.6.1.4</td>
<td>ABI Coder Password Module</td>
</tr>
<tr>
<td>Adobe Acrobat 3.0–6.0 and Adobe PDF 1.2–1.6</td>
<td>PDF Encryption Module</td>
</tr>
<tr>
<td>AOL Instant Messanger through 5.9, AIM Triton through 1.0.4</td>
<td>AIM Password Module</td>
</tr>
<tr>
<td>Ami Pro</td>
<td>AmiPro Password Module</td>
</tr>
<tr>
<td>ARJ 2.82</td>
<td>ARJ Password Module</td>
</tr>
<tr>
<td>Ashampoo</td>
<td>Ashampoo Password Module</td>
</tr>
<tr>
<td>• Security Manager 99</td>
<td></td>
</tr>
<tr>
<td>• Power Encrypt</td>
<td></td>
</tr>
<tr>
<td>• Privacy Protector through 2005</td>
<td></td>
</tr>
<tr>
<td>• Magic Security</td>
<td></td>
</tr>
<tr>
<td>BestCrypt 4.x–7.20, BCArchive 1.06</td>
<td>BestCrypt Password Module</td>
</tr>
<tr>
<td>CheckWriter 5.x</td>
<td>CheckWriter Password Module</td>
</tr>
<tr>
<td>CodedDrag 2.4</td>
<td>CodedDrag Password Module</td>
</tr>
<tr>
<td>crypt</td>
<td>*nix crypt Password Module</td>
</tr>
<tr>
<td>• htpasswd</td>
<td></td>
</tr>
<tr>
<td>• passwd MD5-based, SHA-based, fcrypt</td>
<td></td>
</tr>
<tr>
<td>Cryptainer LE 5–6</td>
<td>Cryptainer Password Module</td>
</tr>
<tr>
<td>Supported Application</td>
<td>PRTK Module</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>CryptaXix</td>
<td>CryptaXix Password Module</td>
</tr>
<tr>
<td>• CryptaPix 2.00–2.24</td>
<td></td>
</tr>
<tr>
<td>• CryptaFlix 1.00–1.10</td>
<td></td>
</tr>
<tr>
<td>CryptText 2.30–3.40</td>
<td>CryptText Password Module</td>
</tr>
<tr>
<td>CuteFTP 2–5, 7x</td>
<td>CuteFTP Password Module</td>
</tr>
<tr>
<td>CD-Lock 5.08–6.02</td>
<td>CDLock Password Module</td>
</tr>
<tr>
<td>DriveCrypt 4.2</td>
<td>DriveCrypt Password Module</td>
</tr>
<tr>
<td>DriveCrypt Plus Pack 3.0</td>
<td>DriveCrypt Plus Pack Password Module</td>
</tr>
<tr>
<td>Encrypted Magic Folders 3.x</td>
<td>EMF Password Module</td>
</tr>
<tr>
<td>GnuPG 1.4.0 or earlier</td>
<td>PGP Password Module</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This module is also used for PGP.</td>
</tr>
<tr>
<td>HandyBits EasyCrypto Deluxe 5.5</td>
<td>EasyCrypto Password Module</td>
</tr>
<tr>
<td>htpasswd</td>
<td>*nix crypt Password Module</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This module is also used for passwd.</td>
</tr>
<tr>
<td>Icon Lock-IT XP</td>
<td>Lockit Password Module</td>
</tr>
<tr>
<td>Internet Explorer Content Advisor</td>
<td>IEContent Password Module</td>
</tr>
<tr>
<td>Justsystem</td>
<td>Justsystem Password Module</td>
</tr>
<tr>
<td>• Ichitaro 5–2004</td>
<td></td>
</tr>
<tr>
<td>• Hanako 3.1–2004</td>
<td></td>
</tr>
<tr>
<td>KeePass Password Safe 8–1.04</td>
<td>KeePass Password Module</td>
</tr>
<tr>
<td>Kremlin</td>
<td>Kremlin Password Module</td>
</tr>
<tr>
<td>• Encrypt 3.0</td>
<td></td>
</tr>
<tr>
<td>• Text 3.0</td>
<td></td>
</tr>
<tr>
<td>MaxCrypt 1.0–1.10</td>
<td>MaxCrypt Password Module</td>
</tr>
<tr>
<td>Supported Application</td>
<td>PRTK Module</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Messenger Plus! 3.50–3.61</td>
<td>MessengerPlus Password Module</td>
</tr>
<tr>
<td>Microsoft Encrypted File System (EFS), Windows 2000–XP Support Pack 2</td>
<td>EFS Module</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>Microsoft Office Encryption Module</td>
</tr>
<tr>
<td>• Excell 2–7, 97,2000, XP, 2003</td>
<td></td>
</tr>
<tr>
<td>• Word 2–6, 97,2000, XP, 2003</td>
<td></td>
</tr>
<tr>
<td>• PowerPoint XP, 2003</td>
<td></td>
</tr>
<tr>
<td>Microsoft Money 2002–2006</td>
<td>MS Money Password Module</td>
</tr>
<tr>
<td>Mozilla</td>
<td>Mozilla Master Password Module</td>
</tr>
<tr>
<td>• Mozilla 1.7x</td>
<td></td>
</tr>
<tr>
<td>• AOL Communicator 20030919.3</td>
<td></td>
</tr>
<tr>
<td>• FireFox through 1.5</td>
<td></td>
</tr>
<tr>
<td>• Netscape 7.x–8.0</td>
<td></td>
</tr>
<tr>
<td>MYOB</td>
<td>MYOB Password Module</td>
</tr>
<tr>
<td>• Plus 3.x</td>
<td></td>
</tr>
<tr>
<td>• Premier Accounting 2005–2006</td>
<td></td>
</tr>
<tr>
<td>• Business Basics 2</td>
<td></td>
</tr>
<tr>
<td>Norton Secret Stuff 1.0</td>
<td>SecretStuff Encryption Module</td>
</tr>
<tr>
<td>Omziff 1.0–3.0.4</td>
<td>Omziff Password Module</td>
</tr>
<tr>
<td>OpenOffice.org</td>
<td>OpenOffice Password Module</td>
</tr>
<tr>
<td>• Office 1.0–2.0</td>
<td></td>
</tr>
<tr>
<td>• StarOffice</td>
<td></td>
</tr>
<tr>
<td>passwd, MD5- and SHA-based encryption and fcrept</td>
<td>*nix crypt Password Module</td>
</tr>
<tr>
<td>PasswordPal through 2.0</td>
<td>PasswordPal Password Module</td>
</tr>
<tr>
<td>PasswordSafe 1–3</td>
<td>PasswordSafe Password Module</td>
</tr>
</tbody>
</table>

*Note: This module is also used for htpasswd.*
<table>
<thead>
<tr>
<th>Supported Application</th>
<th>PRTK Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC-Encrypt through 9.11</td>
<td>PCEncrypt Encryption Module</td>
</tr>
<tr>
<td>PDF</td>
<td>PDF Encryption Module</td>
</tr>
<tr>
<td>• Acrobat 3.0–6.0</td>
<td></td>
</tr>
<tr>
<td>• PDF 1.2–1.6</td>
<td></td>
</tr>
<tr>
<td>PFX</td>
<td>PFX Password Module</td>
</tr>
<tr>
<td>• Microsoft PFX</td>
<td></td>
</tr>
<tr>
<td>• P12 Private Key Format</td>
<td></td>
</tr>
<tr>
<td>PGP</td>
<td>PGP Password Module</td>
</tr>
<tr>
<td>• PGP 9.0.2</td>
<td></td>
</tr>
<tr>
<td>• gnupg 1.4.0</td>
<td></td>
</tr>
<tr>
<td>PGP Disk</td>
<td>PGP Disk Password Module</td>
</tr>
<tr>
<td>• PGP 8.1 or earlier</td>
<td></td>
</tr>
<tr>
<td>• PGP Disk 4.0–6.0</td>
<td></td>
</tr>
<tr>
<td>• PGP SDA</td>
<td></td>
</tr>
<tr>
<td>• Whole Disk Encryption 9.0</td>
<td></td>
</tr>
<tr>
<td>PKZIP</td>
<td>ZIP Password Module</td>
</tr>
<tr>
<td>PWL</td>
<td>PWL Password Module</td>
</tr>
<tr>
<td>Quickbooks 2003–2005</td>
<td>Quickbooks Password Module</td>
</tr>
<tr>
<td>Quicken 2003–2006</td>
<td>Quicken Password Module</td>
</tr>
<tr>
<td>RAR 1.x–3.x</td>
<td>RAR Password Module</td>
</tr>
<tr>
<td>SafeHouse Personal Privacy 2</td>
<td>SafeHouse Password Module</td>
</tr>
<tr>
<td>SAM files</td>
<td>SAM File Module</td>
</tr>
<tr>
<td>• SAM files NT (MD4) hash, LAN hash</td>
<td></td>
</tr>
<tr>
<td>• Active Directory</td>
<td></td>
</tr>
</tbody>
</table>

Note: This module is also used for WinZip 8 or earlier.
**Keyspace Attacks**

The keyspace attack is used on applications that use 40-bit encryption or less. Because of the relatively small number of possible keys, DNA tries every possible key until it finds the one that decrypts the file.

Some applications use the keyspace attack in conjunction with another attack. For more information, see “Multiple Attacks.”
## Supported Application PRTK Module

<table>
<thead>
<tr>
<th>Supported Application</th>
<th>PRTK Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>CryptaXix</td>
<td>CryptaXix Password Module</td>
</tr>
<tr>
<td>• CryptaPix 2.00–2.24</td>
<td></td>
</tr>
<tr>
<td>• CryptaFix 1.00–1.10</td>
<td></td>
</tr>
<tr>
<td>ICQ 2003b–5.04</td>
<td>ICQ Password Module</td>
</tr>
<tr>
<td>Microsoft Office</td>
<td>Microsoft Office Encryption Module</td>
</tr>
<tr>
<td>• Excell 2–7, 97,2000, XP, 2003</td>
<td></td>
</tr>
<tr>
<td>• Word 2–6, 97,2000, XP, 2003</td>
<td></td>
</tr>
<tr>
<td>• PowerPoint XP, 2003</td>
<td></td>
</tr>
<tr>
<td>PDF</td>
<td>PDF Encryption Module</td>
</tr>
<tr>
<td>• Acrobat 3.0–6.0</td>
<td></td>
</tr>
<tr>
<td>• PDF 1.2–1.6</td>
<td></td>
</tr>
<tr>
<td>PWL</td>
<td>PWL Password Module</td>
</tr>
<tr>
<td>SAM files</td>
<td>SAM File Module</td>
</tr>
<tr>
<td>• SAM files NT (MD4) hash, LAN hash</td>
<td></td>
</tr>
<tr>
<td>• Active Directory</td>
<td></td>
</tr>
<tr>
<td>SecretStuff 1.0</td>
<td>SecretStuff Encryption Module</td>
</tr>
<tr>
<td>ZIP</td>
<td>ZIP Password Module</td>
</tr>
<tr>
<td>• WinZip</td>
<td></td>
</tr>
<tr>
<td>• PKZIP 8</td>
<td></td>
</tr>
</tbody>
</table>

## Reset Attacks

Reset attack is the least common attack type used by PRTK because few applications are susceptible to it.
**Multiple Attacks**

Some applications are susceptible to more than one attack type. Multiple attacks can be used to decrease the time necessary to decrypt a file. For applications where multiple attack types can be used, PRTK starts with the least time-consuming attack type.

For example, PRTK might use a dictionary attack first on a PowerPoint spreadsheet and then use the key space attack if the file isn’t decrypted during the dictionary attack.

---

**Supported Application** | **PRTK Module**
---|---
Ashampoo | Ashampoo Password Module
• Security Manager 99
• Power Encrypt
• Privacy Protector through 2005
• Magic Security
DriveCrypt 4.2 | DriveCrypt Password Module
MSN Messenger through 7.0 | MSN Messenger Password Module
MYOB | MYOB Password Module
• Plus 3.x
• Premier Accounting 2005–2006
• Business Basics 2
Quickbooks 2003–2005 | Quickbooks Password Module
Quicken 2003–2006 | Quicken Password Module
VBA | VBA Password Module
PRTK uses multiple attack types on the applications listed in the following table. The order in which the attack types are listed in the table is the order that PRTK uses.

<table>
<thead>
<tr>
<th>Supported Application</th>
<th>Attack Types</th>
<th>PRTK Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>AOL 8.0–9.0 Security Edition</td>
<td>1. Decryption</td>
<td>AOL Password Module</td>
</tr>
<tr>
<td></td>
<td>2. Keyspace</td>
<td></td>
</tr>
<tr>
<td>AOL Communicator</td>
<td>1. Dictionary</td>
<td></td>
</tr>
<tr>
<td>20030919.3 or earlier</td>
<td>2. Decryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This module is also used for Mozilla, Mozilla Firefox, and Netscape.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This module is also used for Mozilla, Mozilla Firefox, and Netscape.</td>
</tr>
<tr>
<td>ARJ 2.82 or earlier</td>
<td>1. Keyspace</td>
<td>ARJ Password Module</td>
</tr>
<tr>
<td></td>
<td>2. Dictionary</td>
<td></td>
</tr>
<tr>
<td>DriveCrypt 4.2</td>
<td>1. Dictionary</td>
<td>DriveCrypt Password Module</td>
</tr>
<tr>
<td></td>
<td>2. Reset</td>
<td></td>
</tr>
<tr>
<td>HandyBits EasyCrypto Deluxe 5.5</td>
<td>1. Dictionary</td>
<td>EasyCrypto Password Module</td>
</tr>
<tr>
<td></td>
<td>2. Decryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Decryption</td>
<td>Note: This module is also used for Microsoft Word and Microsoft PowerPoint.</td>
</tr>
<tr>
<td>Supported Application</td>
<td>Attack Types</td>
<td>PRTK Module</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>Microsoft Money 97–2004,</td>
<td>1. Dictionary</td>
<td>MS Money Password Module</td>
</tr>
<tr>
<td>backup files</td>
<td>2. Decryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Versions of Microsoft Money</td>
<td></td>
</tr>
<tr>
<td></td>
<td>before 2002 use the decryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>attack. Microsoft Money 2002–04 uses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the dictionary attack.</td>
<td></td>
</tr>
<tr>
<td>Microsoft PowerPoint XP</td>
<td>1. Dictionary</td>
<td>Microsoft Office Encryption Module</td>
</tr>
<tr>
<td>and 2003</td>
<td>2. Decryption</td>
<td><strong>Note:</strong> This module is also used for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Microsoft Excel and Microsoft PowerPoint.</td>
</tr>
<tr>
<td>Microsoft Word 2–6, 97,</td>
<td>1. Dictionary</td>
<td>Microsoft Office Encryption Module</td>
</tr>
<tr>
<td>2000, XP, and 2003</td>
<td>2. Decryption</td>
<td><strong>Note:</strong> This module is also used for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Microsoft Excel and Microsoft PowerPoint.</td>
</tr>
<tr>
<td>Mozilla 1.7.x</td>
<td>1. Dictionary</td>
<td>1. The dictionary attack uses the Mozilla</td>
</tr>
<tr>
<td></td>
<td>2. Decryption</td>
<td>Master Password Module.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This module is also used for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AOL Communicator, Mozilla Firefox, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Netscape.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. The decryption attack uses the Mozilla</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protected Data Module.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> This module is also used for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AOL Communicator, Mozilla Firefox, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Netscape.</td>
</tr>
<tr>
<td>Supported Application</td>
<td>Attack Types</td>
<td>PRTK Module</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Mozilla Firefox 1.0.4 or earlier | 1. Dictionary  2. Decryption | 1. The dictionary attack uses the Mozilla Master Password Module.  
  Note: This module is also used for AOL Communicator, Mozilla, and Netscape.  
  2. The decryption attack uses the Mozilla Protected Data Module.  
  Note: This module is also used for AOL Communicator, Mozilla, and Netscape. |
  Note: This module is also used for AOL Communicator, Mozilla, and Mozilla Firefox.  
  2. The decryption attack uses the Mozilla Protected Data Module.  
  Note: This module is also used for AOL Communicator, Mozilla, and Mozilla Firefox. |
<p>| Password Pal 2.0 or earlier     | 1. Dictionary  2. Decryption | PasswordPal Password Module                                                    |
| QuickBooks 2001 or earlier     | PRTK uses a decryption attack to recover the file passwords for QuickBooks 2001 or earlier. To open a recovered file, open it in QuickBooks and enter the recovered password when prompted. | QuickBooks Password Module                                                    |</p>
<table>
<thead>
<tr>
<th>Supported Application</th>
<th>Attack Types</th>
<th>PRTK Module</th>
</tr>
</thead>
</table>
| Quicken 2004 or earlier    | 1. Dictionary  
2. Decryption  
3. Reset  
**Note:** PRTK uses a dictionary attack to recover the file passwords for Quicken 2003–2004. A decryption attack is used for Quicken 2001 or earlier. PRTK resets the password to a blank password for Quicken 2002. | Quicken Password Module |
| Visual Basic for Applications (VBA) | 1. Dictionary  
2. Decryption  
3. Reset  | VBA Password Module |
| Windows PWL files          | 1. Decryption  
2. Dictionary  | PWL Password Module |
| WinZip 8 or earlier        | 1. Keyspace  
2. Dictionary  
**Note:** This module is also used for PKZIP. | ZIP Password Module |
Password Recovery Attacks

A profile is the combination of four individual components: Languages, Character Groups, Dictionaries, and Levels, each described below.

Languages

Language selection affects two aspects of password recovery: the dictionaries selected for dictionary attacks (which can also be independently selected and deselected), and the character sets that will be used in levels that use computer generated characters as opposed to reading words from a dictionary. PRTK currently supports the following character sets: Arabic, English, French, German, Italian, Russian and Spanish.

Character Groups

Character groups allow a profile to refine and expand the set of characters that will be used in levels that generate characters. The following character groups can be selected or deselected for the given profile:

<table>
<thead>
<tr>
<th>Character Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All 7-bit Characters (ASCII)</td>
<td>Character represented by a value from 0 to 127 encoded as a byte.</td>
</tr>
<tr>
<td>All 8-bit Characters</td>
<td>Character represented by a value from 0 to 255 encoded as a byte.</td>
</tr>
</tbody>
</table>
Dictionaries

Dictionaries are word list groupings that have been complied in several different languages in both a codepage and Unicode format. PRTK will select the correct format depending on whether a module uses codepage or Unicode. Once a dictionary has reached 500,000 entries, a new codepage and Unicode dictionary is created.

PRTK ships with the following dictionaries:

<table>
<thead>
<tr>
<th>Character Group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uppercase Letters</td>
<td>Characters represented as uppercase for the selected languages in the profile (for languages that support uppercase and lowercase characters).</td>
</tr>
<tr>
<td>Lowercase Letters</td>
<td>Characters represented as lowercase for the selected languages in the profile (for languages that support uppercase and lowercase characters).</td>
</tr>
<tr>
<td>Diacritics</td>
<td>The combination of a character and an additional mark sometimes referred to as an accent.</td>
</tr>
<tr>
<td>Digits</td>
<td>Characters represented as numbers for the selected languages in the profile (for languages that support digit characters).</td>
</tr>
<tr>
<td>Symbols (Standard)</td>
<td>Non-Alphanumeric characters that can be found on a keyboard.</td>
</tr>
<tr>
<td>Symbols (Extended)</td>
<td>Non-Alphanumeric characters that cannot be found on a keyboard. Characters selected from the character map utility provided in Microsoft Windows, for example.</td>
</tr>
</tbody>
</table>

See AccessData’s “Languages and Character Sets” whitepaper for more details on languages and character sets.
<table>
<thead>
<tr>
<th>Language</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arabic</td>
<td>[AR-1] Names-ar-c.adf: Arabic Names (codepage)</td>
</tr>
<tr>
<td></td>
<td>[AR-1] Names-ar-u.adf: Arabic Names (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[AR-2] Quran-ar-c.adf: Arabic words from the Quran (codepage)</td>
</tr>
<tr>
<td></td>
<td>[AR-2] Quran-ar-u.adf: Arabic words from the Quran (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[AR-3] General-ar-u.adf: General Arabic words (Unicode)</td>
</tr>
<tr>
<td>German</td>
<td>[DE-1] General-1-de-c.adf: General German words – List 1 (codepage)</td>
</tr>
<tr>
<td></td>
<td>[DE-1] General-1-de-u.adf: General German words – List 1 (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[DE-1] General-2-de-c.adf: General German words – List 2 (codepage)</td>
</tr>
<tr>
<td></td>
<td>[DE-1] General-2-de-u.adf: General German words – List 2 (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[DE-1] General-3-de-c.adf: General German words – List 3 (codepage)</td>
</tr>
<tr>
<td></td>
<td>[DE-1] General-3-de-u.adf: General German words – List 3 (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[DE-1] General-4-de-c.adf: General German words – List 4 (codepage)</td>
</tr>
<tr>
<td></td>
<td>[DE-1] General-4-de-u.adf: General German words – List 4 (Unicode)</td>
</tr>
<tr>
<td>Language</td>
<td>Format</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td>[EN-1] Common-en-u.adf: Common English words and passwords (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[EN-2] Miscellaneous-en-c.adf: Crime related, keyboard sequences and words that may not be found in normal dictionaries (codepage)</td>
</tr>
<tr>
<td></td>
<td>[EN-2] Miscellaneous-en-u.adf: Crime related, keyboard sequences and words that may not be found in normal dictionaries (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[EN-3] Names-en-c.adf: Common English first names, last names and business names (Codepage)</td>
</tr>
<tr>
<td></td>
<td>[EN-3] Names-en-u.adf: Common English first names, last names and business names (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[EN-4] General-1-en-c.adf: General English words, not found in the other English dictionaries – List 1 (codepage)</td>
</tr>
<tr>
<td></td>
<td>[EN-4] General-1-en-u.adf: General English words, not found in the other English dictionaries – List 1 (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[EN-4] General-2-en-c.adf: General English words, not found in the other English dictionaries – List 2 (codepage)</td>
</tr>
<tr>
<td></td>
<td>[EN-4] General-2-en-u.adf: General English words, not found in the other English dictionaries – List 2 (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[ES-1] General-es-u.adf: General Spanish words (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[FR-1] General-fr-u.adf: General French words (Unicode)</td>
</tr>
</tbody>
</table>
Levels create password tests that:

- Are words that are read from dictionaries
- Characters that are computer generated
- A combination of both.

<table>
<thead>
<tr>
<th>Language</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Italian</td>
<td>[IT-1] General-it-c.adf: General Italian words (codepage)</td>
</tr>
<tr>
<td></td>
<td>[IT-1] General-it-u.adf: General Italian words (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[JA-2] Kanji-ja-u.adf: Japanese words from the Kanji dialect (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[JA-3] Katakana-ja-c.adf: Japanese words from the Katakana dialect (codepage)</td>
</tr>
<tr>
<td></td>
<td>[JA-3] Katakana-ja-u.adf: Japanese words from the Katakana dialect (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[RU-1] General-1-ru-u.adf: General Russian words – list 1 (Unicode)</td>
</tr>
<tr>
<td></td>
<td>[RU-1] General-2-ru-u.adf: General Russian words – list 2 (Unicode)</td>
</tr>
<tr>
<td>Slovak</td>
<td>[SK-1] General-sk-c.adf: General Slovak words (codepage)</td>
</tr>
<tr>
<td></td>
<td>[SK-1] General-sk-u.adf: General Slovak words (Unicode)</td>
</tr>
</tbody>
</table>
This table lists the intensity of each level:

<table>
<thead>
<tr>
<th>Attempt Category</th>
<th>Attempt Intensity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic (BAS)</td>
<td>1—Less than one-million tests</td>
</tr>
<tr>
<td></td>
<td>2—One-million to one-billion tests</td>
</tr>
<tr>
<td></td>
<td>3—One-billion to ten-billion tests</td>
</tr>
<tr>
<td>Advanced (ADV)</td>
<td>1—Ten-billion to 25-billion tests</td>
</tr>
<tr>
<td></td>
<td>2—25-billion to 50-billion tests</td>
</tr>
<tr>
<td></td>
<td>3—50-billion to 100-billion tests</td>
</tr>
<tr>
<td></td>
<td>4—More than 100-billion tests</td>
</tr>
<tr>
<td>Pass Phrase (PP)</td>
<td>1—Less than 100-billion tests</td>
</tr>
<tr>
<td></td>
<td>2—100-billion to one-trillion tests</td>
</tr>
<tr>
<td></td>
<td>3—More than one-trillion tests</td>
</tr>
</tbody>
</table>

**Default Level Order**

This table show the default level order for new profiles:
<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>(BAS-1-01)</td>
<td>One digit search</td>
<td>9</td>
</tr>
<tr>
<td>(BAS-1-02)</td>
<td>One letter, language specific search</td>
<td>b</td>
</tr>
<tr>
<td>(BAS-1-03)</td>
<td>Two digit search</td>
<td>33</td>
</tr>
<tr>
<td>(BAS-1-04)</td>
<td>Two letter, language specific search</td>
<td>XP</td>
</tr>
<tr>
<td>(BAS-1-05)</td>
<td>Three digit search</td>
<td>456</td>
</tr>
<tr>
<td>(BAS-1-06)</td>
<td>Three letter, language specific search</td>
<td>aBc</td>
</tr>
<tr>
<td>(BAS-1-07)</td>
<td>Four digit search</td>
<td>9876</td>
</tr>
<tr>
<td>(BAS-1-08)</td>
<td>Five digit search</td>
<td>15935</td>
</tr>
<tr>
<td>(BAS-1-09)</td>
<td>Five Markov characters within a threshold of one hundred</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with two characters uppercased search</td>
<td></td>
</tr>
<tr>
<td>(BAS-1-10)</td>
<td>Six digit search</td>
<td>123456</td>
</tr>
<tr>
<td>(BAS-1-11)</td>
<td>Four Markov characters with a threshold of one primary search</td>
<td></td>
</tr>
<tr>
<td>(BAS-2-01)</td>
<td>Four letter, language specific search</td>
<td>ZXcv</td>
</tr>
<tr>
<td>(BAS-2-02)</td>
<td>Five letter, language specific search</td>
<td>LKJh</td>
</tr>
<tr>
<td>(BAS-2-03)</td>
<td>Five Markov characters with a threshold of one primary</td>
<td>revid</td>
</tr>
<tr>
<td></td>
<td>search</td>
<td></td>
</tr>
<tr>
<td>(BAS-2-04)</td>
<td>Five Markov characters with a threshold of one primary</td>
<td>elpa</td>
</tr>
<tr>
<td></td>
<td>reverse search</td>
<td></td>
</tr>
<tr>
<td>(BAS-2-05)</td>
<td>Six Markov characters with a threshold of one primary</td>
<td>clorne</td>
</tr>
<tr>
<td></td>
<td>search</td>
<td></td>
</tr>
<tr>
<td>(BAS-2-06)</td>
<td>Six Markov characters with a threshold of one hundred</td>
<td>enrolc</td>
</tr>
<tr>
<td></td>
<td>with two characters uppercased search</td>
<td></td>
</tr>
<tr>
<td>(BAS-2-07)</td>
<td>Six Markov characters with a threshold of one primary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reverse search</td>
<td></td>
</tr>
<tr>
<td>(BAS-2-08)</td>
<td>Seven digit search</td>
<td>77777777</td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>(BAS-2-09)</td>
<td>Seven Markov characters with a threshold of fifty primary search</td>
<td>drotune</td>
</tr>
<tr>
<td>(BAS-2-10)</td>
<td>Seven Markov characters with a threshold of fifty primary reverse search</td>
<td>enutord</td>
</tr>
<tr>
<td>(BAS-2-11)</td>
<td>Seven Markov characters with a threshold of one hundred with two characters uppercased search</td>
<td></td>
</tr>
<tr>
<td>(BAS-2-12)</td>
<td>Seven digit telephone number search</td>
<td>555-1234</td>
</tr>
<tr>
<td>(BAS-2-13)</td>
<td>Eight digit search</td>
<td>98765432</td>
</tr>
<tr>
<td>(BAS-2-14)</td>
<td>Eight Markov characters with a threshold of fifty primary search</td>
<td>schroten</td>
</tr>
<tr>
<td>(BAS-2-15)</td>
<td>Eight Markov characters with a threshold of fifty primary reverse search</td>
<td>netorhcs</td>
</tr>
<tr>
<td>(BAS-2-16)</td>
<td>Eight Markov characters with a threshold of one hundred with two characters uppercased search</td>
<td></td>
</tr>
<tr>
<td>(BAS-2-17)</td>
<td>Dictionary primary search</td>
<td>Apple</td>
</tr>
<tr>
<td>(BAS-2-18)</td>
<td>Dictionary primary reverse search</td>
<td>llabesab</td>
</tr>
<tr>
<td>(BAS-2-19)</td>
<td>Dictionary with two characters uppercased search</td>
<td>peACH</td>
</tr>
<tr>
<td>(BAS-2-20)</td>
<td>Dictionary primary character replacements search</td>
<td>b@n@n@</td>
</tr>
<tr>
<td>(BAS-2-21)</td>
<td>Dictionary primary followed by common postfixes search</td>
<td>jazz#1</td>
</tr>
<tr>
<td>(BAS-2-22)</td>
<td>Dictionary primary preceded by common prefixes search</td>
<td>drBob</td>
</tr>
<tr>
<td>(BAS-2-23)</td>
<td>Dictionary primary followed by a one digit search</td>
<td>orange2</td>
</tr>
<tr>
<td>(BAS-2-24)</td>
<td>Dictionary primary preceded by a one digit search</td>
<td>1pear</td>
</tr>
<tr>
<td>(BAS-2-25)</td>
<td>Dictionary primary followed by a one letter, language specific search</td>
<td>strawberryQ</td>
</tr>
<tr>
<td>(BAS-2-26)</td>
<td>Dictionary primary preceded by a one letter, language specific search</td>
<td>xCherry</td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>(BAS-2-27)</td>
<td>Dictionary primary followed by a non-alphanumeric symbol search</td>
<td>plum$</td>
</tr>
<tr>
<td>(BAS-2-28)</td>
<td>Dictionary primary preceded by a language-specific non-alphanumeric symbol search</td>
<td>^raspberry</td>
</tr>
<tr>
<td>(BAS-2-29)</td>
<td>Dictionary primary character replacement, followed by a one digit search</td>
<td>@pple5</td>
</tr>
<tr>
<td>(BAS-2-30)</td>
<td>Dictionary primary character replacement, preceded by a one digit search</td>
<td>3Pea[h</td>
</tr>
<tr>
<td>(BAS-2-31)</td>
<td>Dictionary primary preceded and followed by a one digit search</td>
<td>4orange4</td>
</tr>
<tr>
<td>(BAS-2-32)</td>
<td>Dictionary primary followed by a two digits search</td>
<td>bANANA55</td>
</tr>
<tr>
<td>(BAS-2-33)</td>
<td>Dictionary primary preceded by a two digits search</td>
<td>12CHERRY</td>
</tr>
<tr>
<td>(BAS-2-34)</td>
<td>Dictionary primary preceded by common prefixes and followed by a one digit search</td>
<td>mrAnderson1</td>
</tr>
<tr>
<td>(BAS-2-35)</td>
<td>Dictionary primary preceded by one digit followed by common postfixes</td>
<td>3cat’s</td>
</tr>
<tr>
<td>(BAS-2-36)</td>
<td>Date Search (Two digit year)</td>
<td>12-17-83</td>
</tr>
<tr>
<td>(BAS-2-37)</td>
<td>Three letter, language specific characters followed by common postfixes</td>
<td>trw123</td>
</tr>
<tr>
<td>(BAS-2-38)</td>
<td>Three letter, language specific characters preceded by common prefixes</td>
<td>abcMgh</td>
</tr>
<tr>
<td>(BAS-2-39)</td>
<td>Five Markov Characters with a threshold of one followed by common postfixes</td>
<td>revid123</td>
</tr>
<tr>
<td>(BAS-2-40)</td>
<td>Five Markov Characters with a threshold of one preceded by common prefixes</td>
<td>abcrevid</td>
</tr>
<tr>
<td>(BAS-2-41)</td>
<td>Six Markov Characters with a threshold of fifty followed by common postfixes</td>
<td></td>
</tr>
<tr>
<td>(BAS-2-42)</td>
<td>Six Markov Characters with a threshold of fifty preceded by common prefixes</td>
<td></td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>(BAS-2-43)</td>
<td>Nine Markov characters with a threshold of one hundred search</td>
<td></td>
</tr>
<tr>
<td>(BAS-3-01)</td>
<td>Dictionary primary with a non-alphanumeric symbol inserted search</td>
<td>app&amp;le</td>
</tr>
<tr>
<td>(BAS-3-02)</td>
<td>Dictionary primary character replacement, followed by a two digit search</td>
<td>@apple23</td>
</tr>
<tr>
<td>(BAS-3-03)</td>
<td>Dictionary primary character replacement, preceded by a two digit search</td>
<td>76app</td>
</tr>
<tr>
<td>(BAS-3-04)</td>
<td>Dictionary primary followed by a three digit search</td>
<td>apple258</td>
</tr>
<tr>
<td>(BAS-3-05)</td>
<td>Dictionary primary preceded by a three digit search</td>
<td>987apple</td>
</tr>
<tr>
<td>(BAS-3-06)</td>
<td>Social Security Number Search</td>
<td>123-45-6789</td>
</tr>
<tr>
<td>(BAS-3-07)</td>
<td>Four letter, language specific characters preceded by common prefixes</td>
<td>abcPoUy</td>
</tr>
<tr>
<td>(BAS-3-08)</td>
<td>Four letter, language specific characters followed by common postfixes</td>
<td>Asdf123</td>
</tr>
<tr>
<td>(ADV-1-01)</td>
<td>All one-character, language-specific search</td>
<td>a</td>
</tr>
<tr>
<td>(ADV-1-02)</td>
<td>All two character, language-specific search</td>
<td>1a</td>
</tr>
<tr>
<td>(ADV-1-03)</td>
<td>All three-character, language-specific search</td>
<td>!1a</td>
</tr>
<tr>
<td>(ADV-1-04)</td>
<td>All four-character, language-specific search</td>
<td>1a%</td>
</tr>
<tr>
<td>(ADV-1-05)</td>
<td>One digit followed by three language-specific characters search</td>
<td>7!qy</td>
</tr>
<tr>
<td>(ADV-1-06)</td>
<td>Three language-specific characters followed by one digit search</td>
<td>tuh5</td>
</tr>
<tr>
<td>(ADV-1-07)</td>
<td>One language-specific character followed by a four digit search</td>
<td>*1234</td>
</tr>
<tr>
<td>(ADV-1-08)</td>
<td>One digit followed by four language-specific characters search</td>
<td>5wert</td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>(ADV-1-09)</td>
<td>Two language-specific characters followed by a three digit search</td>
<td>xx333</td>
</tr>
<tr>
<td>(ADV-1-10)</td>
<td>Two digits followed by three language-specific characters search</td>
<td>93!Q2</td>
</tr>
<tr>
<td>(ADV-1-11)</td>
<td>Three language-specific characters followed by a two digit search</td>
<td>!@d56</td>
</tr>
<tr>
<td>(ADV-1-12)</td>
<td>Four language-specific characters followed by a one digit search</td>
<td>A$Df6</td>
</tr>
<tr>
<td>(ADV-1-13)</td>
<td>Four language-specific characters followed by a non-alphanumeric symbol search</td>
<td>P0&amp;6@</td>
</tr>
<tr>
<td>(ADV-1-14)</td>
<td>Four language-specific characters preceded by a non-alphanumeric symbol search</td>
<td>$t7^3</td>
</tr>
<tr>
<td>(ADV-1-15)</td>
<td>Six letter, language specific search</td>
<td>QwErTy</td>
</tr>
<tr>
<td>(ADV-1-16)</td>
<td>Two digits followed by four language-specific characters search</td>
<td>22asD%</td>
</tr>
<tr>
<td>(ADV-1-17)</td>
<td>Two language-specific characters followed by four digits search</td>
<td>$%1234</td>
</tr>
<tr>
<td>(ADV-1-18)</td>
<td>Three language-specific characters followed by a three digit search</td>
<td>4%$123</td>
</tr>
<tr>
<td>(ADV-1-19)</td>
<td>Four language-specific characters followed by a two digit search</td>
<td>Aa$77</td>
</tr>
<tr>
<td>(ADV-1-20)</td>
<td>Dictionary primary followed by a two letter, language specific search</td>
<td>Appleff</td>
</tr>
<tr>
<td>(ADV-1-21)</td>
<td>Dictionary primary preceded by a two letter, language specific search</td>
<td>quapple</td>
</tr>
<tr>
<td>(ADV-1-22)</td>
<td>Dictionary primary preceded by a two digit followed by common postfixes</td>
<td>12applebc</td>
</tr>
<tr>
<td>(ADV-1-23)</td>
<td>Dictionary primary preceded by common prefixes and followed by a two digit search</td>
<td>abcapple12</td>
</tr>
<tr>
<td>Level</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>(ADV-1-24)</td>
<td>Dictionary primary preceded and followed by a two digit search</td>
<td>12apple34</td>
</tr>
<tr>
<td>(ADV-1-25)</td>
<td>Dictionary primary followed by a four digit search</td>
<td>apple4567</td>
</tr>
<tr>
<td>(ADV-1-26)</td>
<td>Dictionary primary preceded by a four digit search</td>
<td>2468apple</td>
</tr>
<tr>
<td>(ADV-1-27)</td>
<td>Ten digit telephone number search</td>
<td>800-555-8888</td>
</tr>
<tr>
<td>(ADV-2-01)</td>
<td>All five-character, language-specific search</td>
<td>Hg^s</td>
</tr>
<tr>
<td>(ADV-3-01)</td>
<td>Four language-specific characters with a non-alphanumeric symbol inserted search</td>
<td>a3&amp;c8</td>
</tr>
<tr>
<td>(ADV-3-02)</td>
<td>Four language-specific characters followed by a three digit search</td>
<td>rfizg555</td>
</tr>
<tr>
<td>(ADV-4-01)</td>
<td>All six-character, language-specific search</td>
<td>Dg*4g&amp;</td>
</tr>
<tr>
<td>(ADV-4-02)</td>
<td>Seven letter search</td>
<td>aAbBeCd</td>
</tr>
<tr>
<td>(ADV-4-03)</td>
<td>All seven-character, language-specific search</td>
<td>a1!c$7</td>
</tr>
<tr>
<td>(ADV-4-04)</td>
<td>Eight letter search</td>
<td>sLdKlenD</td>
</tr>
<tr>
<td>(ADV-4-05)</td>
<td>All eight-character, language-specific search</td>
<td>!#@$12we</td>
</tr>
<tr>
<td>(ADV-4-06)</td>
<td>Nine letter, language specific search</td>
<td>aISODheKg</td>
</tr>
<tr>
<td>(ADV-4-07)</td>
<td>All nine-character, language-specific search</td>
<td>*&amp;g1234</td>
</tr>
<tr>
<td>(ADV-4-08)</td>
<td>Ten letter, language specific search</td>
<td>SOdkghdlSJ</td>
</tr>
<tr>
<td>(ADV-4-09)</td>
<td>All ten-character, language-specific search</td>
<td>1a!2b@3c#4</td>
</tr>
<tr>
<td>(ADV-4-10)</td>
<td>All eleven-character, language-specific search</td>
<td>1a!2b@3c#4D</td>
</tr>
<tr>
<td>(ADV-4-11)</td>
<td>All twelve-character, language-specific search</td>
<td>1a!2b@3c#4D$</td>
</tr>
<tr>
<td>(PP-1-01)</td>
<td>Two word concatenation without spaces search</td>
<td>dogcat</td>
</tr>
<tr>
<td>(PP-1-02)</td>
<td>Two word concatenation with spaces search</td>
<td>cat dog</td>
</tr>
</tbody>
</table>
If you create additional levels, more levels are added to the password attacks. If you select Customized Dictionaries, more levels will be added to the attack.

Profiles

DNA and PRTK share the same profile names, though the DNA Profiles use additional levels (suggested for distributed processing only).

- English (default)
- English Transitional
- Arabic
- European
- Russian
- Pass-phrase
- FTK Import

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>(PP-1-03)</td>
<td>Dictionary preceded by a verb or prepositional phrase search</td>
<td>in the house</td>
</tr>
<tr>
<td>(PP-1-04)</td>
<td>The common English dictionary preceded by a verb or prepositional phrase search</td>
<td>is a dog</td>
</tr>
<tr>
<td>(PP-2-01)</td>
<td>Word inserted into another word search</td>
<td>inswordert</td>
</tr>
<tr>
<td>(PP-2-02)</td>
<td>Dictionary followed by a verb or prepositional phrase followed by a Dictionary search</td>
<td>he is a cook</td>
</tr>
<tr>
<td>(PP-2-03)</td>
<td>Two word passphrase using the common english dictionary</td>
<td>able about</td>
</tr>
<tr>
<td>(PP-3-01)</td>
<td>Three word concatenation without spaces search</td>
<td>catdogbird</td>
</tr>
<tr>
<td>(PP-3-02)</td>
<td>Three word concatenation with spaces search</td>
<td>pig goat owl</td>
</tr>
<tr>
<td>(PP-3-03)</td>
<td>Four word concatenation without spaces search</td>
<td>onetwothreefour</td>
</tr>
<tr>
<td>(PP-3-04)</td>
<td>Four word concatenation with spaces search</td>
<td>five six seven eight</td>
</tr>
</tbody>
</table>
The English profile begins by searching for simple passwords, followed by, dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. The program uses all default English dictionaries and character sets.

**Dictionaries:**
- [EN-1] Common-en-c.adf
- [EN-1] Common-en-u.adf
- [EN-2] Miscellaneous-en-u.adf
- [EN-3] Names-en-c.adf
- [EN-3] Names-en-u.adf

**Levels (in order):**
1. (BAS-1-01) One digit search
2. (BAS-1-03) Two digit search
3. (BAS-1-05) Three digit search
4. (BAS-1-07) Four digit search
5. (BAS-1-08) Five digit search
6. (BAS-1-02) One letter, language specific search
7. (BAS-1-04) Two letter, language specific search
8. (BAS-1-06) Three letter, language specific search
9. (ADV-1-01) All one-character, language-specific search
10. (BAS-1-11) Four Markov characters with a threshold of one primary search
11. (BAS-2-03) Five Markov characters with a threshold of one primary search
12. (BAS-2-17) Dictionary primary search
13. (BAS-2-01) Four letter, language specific search
14. (BAS-2-04) Five Markov characters with a threshold of one primary reverse search
15. (ADV-1-07) One language-specific character followed by a four digit search
16. (BAS-1-10) Six digit search
17. (BAS-2-36) Date Search (two digit year)
18. (ADV-1-03) All three-character, language-specific search
19. (BAS-2-05) Six Markov characters with a threshold of one primary search
20. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
21. (BAS-2-21) Dictionary primary followed by common postfixes search
22. (BAS-2-22) Dictionary primary preceded by common prefixes search
23. (BAS-2-23) Dictionary primary followed by a one digit search
24. (BAS-2-24) Dictionary primary preceded by a one digit search
25. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
26. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search
27. (BAS-2-20) Dictionary primary character replacements search
28. (BAS-2-13) Eight digit search
29. (BAS-2-12) Seven digit telephone number search
30. (ADV-1-05) One digit followed by three language-specific characters search
31. (ADV-1-06) Three language-specific characters followed by one digit search
32. (BAS-2-10) Seven Markov characters with a threshold of fifty primary reverse search
33. (BAS-2-02) Five letter, language specific search
34. (ADV-1-17) Two language-specific characters followed by four digits search
35. (BAS-2-14) Eight Markov characters with a threshold of fifty primary search
36. (BAS-2-15) Eight Markov characters with a threshold of fifty primary reverse search
37. (BAS-2-27) Dictionary primary followed by a non-alphanumeric symbol search
38. (BAS-2-28) Dictionary primary preceded by a language-specific non-alphanumeric symbol search
39. (BAS-2-32) Dictionary primary followed by a two digits search
40. (BAS-2-33) Dictionary primary preceded by a two digits search
41. (BAS-2-31) Dictionary primary preceded and followed by a one digit search
42. (BAS-2-19) Dictionary with two characters uppercased search
43. (BAS-2-43) Nine Markov characters with a threshold of one hundred search
44. (ADV-1-10) Two digits followed by three language-specific characters search
45. (ADV-1-11) Three language-specific characters followed by a two digit search
46. (ADV-1-04) All four-character, language-specific search
47. (BAS-3-01) Dictionary primary with a non-alphanumeric symbol inserted search

48. (BAS-3-04) Dictionary primary followed by a three digit search

49. (BAS-3-05) Dictionary primary preceded by a three digit search

50. (BAS-3-06) Social Security Number Search

51. (ADV-1-18) Three language-specific characters followed by a three digit search

52. (ADV-1-08) One digit followed by four language-specific characters search

53. (ADV-1-12) Four language-specific characters followed by a one digit search

54. (ADV-1-20) Dictionary primary followed by a two letter, language specific search

55. (ADV-1-21) Dictionary primary preceded by a two letter, language specific search

56. (ADV-1-15) Six letter, language specific search

English Transitional

English Transitional follows the same order of the DNA 3.1 and PRTK 6.1 English profile. It is useful for re-submitting unfinished jobs.

Arabic

The Arabic profile begins by searching for simple passwords, followed by dictionary and permutated dictionary searches, and ends with complex searches for dictionary and computed password. All default Arabic dictionaries and character sets are used.

Character Groups

- Uppercase Letters
- Lowercase Letters
- Diacritics
- Digits
- Symbols (Standard)

**Dictionaries:**
- [AR-1] Names-ar-c.adf
- [AR-1] Names-ar-u.adf
- [AR-2] Quran-ar-c.adf
- [AR-2] Quran-ar-u.adf
- [AR-3] General-ar-c.adf
- [AR-3] General-ar-u.adf

**Levels (order):**
1. (BAS-1-01) One digit search
2. (BAS-1-03) Two digit search
3. (BAS-1-05) Three digit search
4. (BAS-1-07) Four digit search
5. (BAS-1-08) Five digit search
6. (BAS-1-02) One letter, language specific search
7. (BAS-1-04) Two letter, language specific search
8. (BAS-1-06) Three letter, language specific search
9. (ADV-1-01) All one-character, language-specific search
10. (ADV-1-02) All two character, language-specific search
11. (BAS-1-11) Four Markov characters with a threshold of one primary search
12. (BAS-2-03) Five Markov characters with a threshold of one primary search
13. (BAS-2-17) Dictionary primary search
14. (BAS-2-01) Four letter, language specific search
15. (BAS-2-04) Five Markov characters with a threshold of one primary reverse search
16. (ADV-1-07) One language-specific character followed by a four digit search
17. (BAS-1-10) Six digit search
18. (BAS-2-36) Date Search (two digit year)
19. (ADV-1-03) All three-character, language-specific search
20. BAS-2-18) Dictionary primary reverse search
21. (BAS-2-05) Six Markov characters with a threshold of one primary search
22. (BAS-2-07) Six Markov characters with a threshold of one primary reverse search
23. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
24. (BAS-2-21) Dictionary primary followed by common postfixes search
25. (BAS-2-22) Dictionary primary preceded by common prefixes search
26. (BAS-2-23) Dictionary primary followed by a one digit search
27. (BAS-2-24) Dictionary primary preceded by a one digit search
28. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
29. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search
30. (BAS-2-20) Dictionary primary character replacements search
31. (BAS-2-13) Eight digit search
32. (BAS-2-12) 7-digit telephone number search
33. (ADV-1-05) One digit followed by three language-specific characters search
34. (BAS-2-10) Seven Markov characters with a threshold of fifty primary reverse search
35. (BAS-2-02) Five letter, language specific search
36. (ADV-1-17) Two language-specific characters followed by four digits search
37. (BAS-2-14) Eight Markov characters with a threshold of fifty primary search
38. (BAS-2-15) Eight Markov characters with a threshold of fifty primary reverse search
39. (BAS-2-27) Dictionary primary followed by a non-alphanumeric symbol search
40. (BAS-2-28) Dictionary primary preceded by a language-specific non-alphanumeric symbol search
41. (BAS-2-32) Dictionary primary followed by a two digits search
42. (BAS-2-33) Dictionary primary preceded by a two digits search
43. (BAS-2-31) Dictionary primary preceded and followed by a one digit search
44. (BAS-2-19) Dictionary with two characters uppercased search
45. (ADV-1-10) Two digits followed by three language-specific characters search
46. (ADV-1-11) Three language-specific characters followed by a two digit search
47. (ADV-1-04) All four-character, language-specific search
48. (BAS-3-04) Dictionary primary followed by a three digit search
49. (BAS-3-05) Dictionary primary preceded by a three digit search
50. (BAS-3-06) Social Security Number Search
51. (ADV-1-18) Three language-specific characters followed by a three digit search
52. (ADV-1-08) One digit followed by four language-specific characters search
53. (ADV-1-12) Four language-specific characters followed by a one digit search
54. (ADV-1-20) Dictionary primary followed by a two letter, language specific search
55. (ADV-1-21) Dictionary primary preceded by a two letter, language specific search
56. (ADV-1-15) Six letter, language specific search

European

The European profile begins by searching for simple passwords, followed by dictionary and permuted dictionary searches, and ends with complex searches for dictionary and computed password. All default German, French, Italian, and Spanish dictionaries and character sets are used.

**Dictionaries**
- [DE-1] General-1-de-c.adf
- [DE-1] General-1-de-u.adf
- [DE-1] General-2-de-c.adf
- [DE-1] General-2-de-u.adf
- [DE-1] General-3-de-c.adf
- [DE-1] General-3-de-u.adf
- [DE-1] General-4-de-c.adf
- [DE-1] General-4-de-u.adf
- [ES-1] General-es-c.adf
- [ES-1] General-es-u.adf
- [FR-1] General-fr-c.adf
- [FR-1] General-fr-u.adf
- [IT-1] General-it-c.adf
- [IT-1] General-it-u.adf
Levels:
1. (BAS-1-01) One digit search
2. (BAS-1-03) Two digit search
3. (BAS-1-05) Three digit search
4. (BAS-1-07) Four digit search
5. (BAS-1-08) Five digit search
6. (BAS-1-02) One letter, language specific search
7. (BAS-1-04) Two letter, language specific search
8. (BAS-1-06) Three letter, language specific search
9. (ADV-1-01) All one-character, language-specific search
10. (ADV-1-02) All two character, language-specific search
11. (BAS-1-11) Four Markov characters with a threshold of one primary search
12. (BAS-2-03) Five Markov characters with a threshold of one primary search
13. (BAS-2-17) Dictionary primary search
14. (BAS-2-01) Four letter, language specific search
15. (BAS-2-04) Five Markov characters with a threshold of one primary reverse search
16. (ADV-1-07) One language-specific character followed by a four digit search
17. (BAS-1-10) Six digit search
18. (BAS-2-36) Date Search (two digit year)
19. (ADV-1-03) All three-character, language-specific search
20. (BAS-2-18) Dictionary primary reverse search
21. (BAS-2-05) Six Markov characters with a threshold of one primary search
22. (BAS-2-07) Six Markov characters with a threshold of one primary reverse search
23. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
24. (BAS-2-21) Dictionary primary followed by common postfixes search
25. (BAS-2-22) Dictionary primary preceded by common prefixes search
26. (BAS-2-23) Dictionary primary followed by a one digit search
27. (BAS-2-24) Dictionary primary preceded by a one digit search
28. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
29. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search
30. (BAS-2-20) Dictionary primary character replacements search
31. (BAS-2-13) Eight digit search
32. (BAS-2-12) Seven digit telephone number search
33. (ADV-1-05) One digit followed by three language-specific characters search
34. (BAS-2-10) Seven Markov characters with a threshold of fifty primary reverse search
35. (BAS-2-02) Five letter, language specific search
36. (ADV-1-17) Two language-specific characters followed by four digits search
37. (BAS-2-14) Eight Markov characters with a threshold of fifty primary search
38. (BAS-2-15) Eight Markov characters with a threshold of fifty primary reverse search
39. (BAS-2-27) Dictionary primary followed by a non-alphanumeric symbol search
40. (BAS-2-28) Dictionary primary preceded by a language-specific non-alphanumeric symbol search
41. (BAS-2-32) Dictionary primary followed by a two digits search
42. (BAS-2-33) Dictionary primary preceded by a two digits search
43. (BAS-2-31) Dictionary primary preceded and followed by a one digit search
44. (BAS-2-19) Dictionary with two characters uppercased search
45. (ADV-1-10) Two digits followed by three language-specific characters search
46. (ADV-1-11) Three language-specific characters followed by a two digit search
47. (ADV-1-04) All four-character, language-specific search
48. (BAS-3-04) Dictionary primary followed by a three digit search
49. (BAS-3-05) Dictionary primary preceded by a three digit search
50. (BAS-3-06) Social Security Number Search
51. (ADV-1-18) Three language-specific characters followed by a three digit search
52. (ADV-1-08) One digit followed by four language-specific characters search
53. (ADV-1-12) Four language-specific characters followed by a one digit search
54. (ADV-1-20) Dictionary primary followed by a two letter, language specific search
55. (ADV-1-21) Dictionary primary preceded by a two letter, language specific search
56. (ADV-1-15) Six letter, language specific search

**Russian**

The Russian profile begins by searching for simple passwords, followed by, dictionary and permuted dictionary searches, and ends with complex searches for dictionary and computed password. All default Russian dictionaries and character sets are used.
Dictionaries:
- [RU-1] General-1-ru-c.adf
- [RU-1] General-1-ru-u.adf
- [RU-1] General-2-ru-c.adf
- [RU-1] General-2-ru-u.adf

Levels:
1. (BAS-1-01) One digit search
2. (BAS-1-03) Two digit search
3. (BAS-1-05) Three digit search
4. (BAS-1-07) Four digit search
5. (BAS-1-08) Five digit search
6. (BAS-1-02) One letter, language specific search
7. (BAS-1-04) Two letter, language specific search
8. (BAS-1-06) Three letter, language specific search
9. (ADV-1-01) All one-character, language-specific search
10. (ADV-1-02) All two character, language-specific search
11. (BAS-1-11) Four Markov characters with a threshold of one primary search
12. (BAS-2-03) Five Markov characters with a threshold of one primary search
13. (BAS-2-17) Dictionary primary search
14. (BAS-2-01) Four letter, language specific search
15. (BAS-2-04) Five Markov characters with a threshold of one primary reverse search
16. (ADV-1-07) One language-specific character followed by a four digit search
17. (BAS-1-10) Six digit search
18. (BAS-2-36) Date Search (Two digit year)
19. (ADV-1-03) All three-character, language-specific search
20. (BAS-2-18) Dictionary primary reverse search
21. (BAS-2-05) Six Markov characters with a threshold of one primary search
22. (BAS-2-07) Six Markov characters with a threshold of one primary reverse search
23. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
24. (BAS-2-21) Dictionary primary followed by common postfixes search
25. (BAS-2-22) Dictionary primary preceded by common prefixes search
26. (BAS-2-23) Dictionary primary followed by a one digit search
27. (BAS-2-24) Dictionary primary preceded by a one digit search
28. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
29. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search
30. (BAS-2-20) Dictionary primary character replacements search
31. (BAS-2-13) Eight digit search
32. (BAS-2-12) Seven digit telephone number search
33. (ADV-1-05) One digit followed by three language-specific characters search
34. (BAS-2-10) Seven Markov characters with a threshold of fifty primary reverse search
35. (BAS-2-02) Five letter, language specific search
36. (ADV-1-17) Two language-specific characters followed by four digits search
37. (BAS-2-14) Eight Markov characters with a threshold of fifty primary search
38. (BAS-2-15) Eight Markov characters with a threshold of fifty primary reverse search
39. (BAS-2-27) Dictionary primary followed by a non-alphanumeric symbol search
40. (BAS-2-28) Dictionary primary preceded by a language-specific non-alphanumeric symbol search
41. (BAS-2-32) Dictionary primary followed by a two digits search
42. (BAS-2-33) Dictionary primary preceded by a two digits search
43. (BAS-2-31) Dictionary primary preceded and followed by a one digit search
44. (BAS-2-19) Dictionary with two characters uppercased search
45. (ADV-1-10) Two digits followed by three language-specific characters search
46. (ADV-1-11) Three language-specific characters followed by a two digit search
47. (ADV-1-04) All four-character, language-specific search
48. (BAS-3-04) Dictionary primary followed by a three digit search
49. (BAS-3-05) Dictionary primary preceded by a three digit search
50. (BAS-3-06) Social Security Number Search
51. (ADV-1-18) Three language-specific characters followed by a three digit search
52. (ADV-1-08) One digit followed by four language-specific characters search
53. (ADV-1-12) Four language-specific characters followed by a one digit search
54. (ADV-1-20) Dictionary primary followed by a two letter, language specific search
55. (ADV-1-21) Dictionary primary preceded by a two letter, language specific search
56. (ADV-1-15) Six letter, language specific search

Pass-phrase

All Pass-phrase levels in English

Dictionaries:

- [EN-1] Common-en-c.adf
- [EN-1] Common-en-u.adf
- [EN-2] Miscellaneous-en-u.adf
- [EN-3] Names-en-c.adf
- [EN-3] Names-en-u.adf

Levels:

1. (PP-1-03) Dictionary preceded by a verb or prepositional phrase search
2. (PP-1-04) The common English dictionary preceded by a verb or prepositional phrase search
3. (PP-2-01) Word inserted into another word search
4. (PP-2-02) Dictionary followed by a verb or prepositional phrase followed by a Dictionary search
5. (PP-2-03) Two word pass-phrase using the common English dictionary
6. (PP-3-01) Three word concatenation without spaces search
7. (PP-3-02) Three word concatenation with spaces search
8. (PP-3-03) Four word concatenation without spaces search
9. (PP-3-04) Four word concatenation with spaces search
FTK Import

Used as a template for FTK imported wordlists

**Dictionaries:**

None Defined. Intended for user to select FTK imported dictionaries

**Levels:**

Dictionary normalized, lowercase search

PRTK

Levels in this profile are ordered by research conducted on recovered passwords.

**Dictionaries:**

- [EN-1] Common-en-c.adf
- [EN-1] Common-en-u.adf
- [EN-2] Miscellaneous-en-u.adf
- [EN-3] Names-en-c.adf
- [EN-3] Names-en-u.adf

**Levels:**

1. (BAS-1-01) One digit search
2. (BAS-1-07) Four digit search
3. (BAS-1-03) Two digit search
4. (BAS-2-17) Dictionary primary search
5. (BAS-1-02) One letter, language specific search
6. (BAS-1-05) Three digit search
7. (ADV-1-01) All one-character, language-specific search
8. (BAS-1-04) Two letter, language specific search
9. (BAS-2-23) Dictionary primary followed by a one digit search
10. (BAS-1-08) Five digit search
11. (ADV-1-02) All two character, language-specific search
12. (BAS-1-06) Three letter, language specific search
13. (BAS-1-10) Six digit search
14. (BAS-2-01) Four letter, language specific search
15. (ADV-1-03) All three-character, language-specific search
16. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
17. (BAS-2-08) Seven digit search
18. (ADV-1-04) All four character, language-specific search
19. (ADV-1-09) Two language-specific characters followed by a three digit search
20. (BAS-2-20) Dictionary primary character replacements search
21. (BAS-2-03) Five Markov characters with a threshold of one primary search
22. (BAS-2-13) Eight digit search
23. (BAS-2-02) Five letter, language specific search
24. (BAS-2-32) Dictionary primary followed by a two digits search
25. (ADV-1-20) Dictionary primary followed by a two letter, language specific search
26. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
27. (ADV-1-07) One language-specific character followed by a four digit search
28. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search

29. (BAS-2-18) Dictionary primary reverse search

30. (ADV-1-05) One digit followed by three language-specific characters search

31. (ADV-1-15) Six letter, language specific search

32. (ADV-2-01) All five-character, language-specific search

DNA

Levels in this profile are ordered by research conducted on recovered passwords.

**Dictionaries:**
- [EN-1] Common-en-c.adf
- [EN-1] Common-en-u.adf
- [EN-2] Miscellaneous-en-u.adf
- [EN-3] Names-en-c.adf
- [EN-3] Names-en-u.adf

**Levels (in order):**
1. (BAS-1-01) One digit search
2. (BAS-1-07) Four digit search
3. (BAS-1-03) Two digit search
4. (BAS-2-17) Dictionary primary search
5. (BAS-1-02) One letter, language specific search
6. (BAS-1-05) Three digit search
7. (ADV-1-01) All one-character, language-specific search
8. (BAS-1-04) Two letter, language specific search
9. (BAS-2-23) Dictionary primary followed by a one digit search
10. (BAS-1-08) Five digit search
11. (ADV-1-02) All two character, language-specific search
12. (BAS-1-06) Three letter, language specific search
13. (BAS-1-10) Six digit search
14. (BAS-2-01) Four letter, language specific search
15. (ADV-1-03) All three-character, language-specific search
16. (BAS-2-25) Dictionary primary followed by a one letter, language specific search
17. (BAS-2-08) Seven digit search
18. (ADV-1-04) All four-character, language-specific search
19. (ADV-1-09) Two language-specific characters followed by a three digit search
20. (BAS-2-20) Dictionary primary character replacements search
21. (BAS-2-03) Five Markov characters with a threshold of one primary search
22. (BAS-2-13) Eight digit search
23. (BAS-2-02) Five letter, language specific search
24. (BAS-2-32) Dictionary primary followed by a two digits search
25. (ADV-1-20) Dictionary primary followed by a two letter, language specific search
26. (BAS-2-09) Seven Markov characters with a threshold of fifty primary search
27. (ADV-1-07) One language-specific character followed by a four digit search
28. (BAS-2-26) Dictionary primary preceded by a one letter, language specific search
29. (BAS-2-18) Dictionary primary reverse search

**Character Replacements**

This list shows characters commonly replaced for each other:

- Replace 1 with L
- Replace 1 with i
- Replace 3 with \[
- Replace 3 with \]
- Replace a with @
- Replace a with 4
- Replace b with 3
- Replace c with (}
- Replace e with 3
- Replace e with [ Replace 1 with | Replace 1 with ! Replace L with 1 Replace o with 0 Replace o with () Replace ph with f Replace s with 5 Replace s with $ Replace z with 5 Replace i with |
Common Prefixes

123   !@#   2u   de   con   net   pro
abc   4u   dr   in   dis   non   sub
mr    4u2  re   un   mac   out   anti
mrs   2b   co   bio   mis   pre   non-
over  poly  post  semi  tele  #1

Common Suffixes (a.k.a. postfixes)

#1    dr   s   ly   ers
123   !@#   's   er   ity
abc   4u   es   ing   ness
mr    4u2  ed   ies   ites
mrs   2b   en   ism   isms

Prepositional and Verb Phrases

in     in the    into the    is a    is the
was a  was the   has a    has the   had a
for a  for the   of a    of the   with a
going to going to the is in the should be would be
and    not      could    can      had the
with the
Encryption Technology

To understand how Password Recovery Toolkit (PRTK) searches for the different password combinations available for application files, you need to be familiar with the underlying elements and classifications of encryption and password technology.

Encryption is explained in the following sections:

- “Understanding Encrypted Files” on page 254
- “Understanding the PRTK Decryption Process” on page 255
- “Current Encryption Standards” on page 257
- “Hashing” on page 259
Understanding Encrypted Files

An encrypted file is digitally altered so the file’s data cannot be read without the key. In a binary editor, the data within an encrypted file appears as unintelligible characters. The only way to access an encrypted file is to open the file in its native application using the file’s password.

When you password protect and encrypt a file, the program you are using applies an algorithm to the password to create a digital key which is used to lock the file. This is the first line of defense. The program then uses the key and a different algorithm to encrypt the file. The file is locked and encrypted so both the file and its data are protected. To access the file, you must open the file in its native program and enter a password that produces the identical key. The program uses the key and a reverse algorithm to decrypt the file.
Understanding the PRTK Decryption Process

To recover an encrypted document, you need a password or a “key,” a long series of binary data.

Typically applications use a transformation function that allows a user to enter a password to encrypt or decrypt a file. So, if you create an encrypted document in Microsoft Word, you only use a password. Microsoft Word then transforms that password into a key, without you even knowing it. The same password generates the same key every time.

To obtain either a password or a key, PRTK uses the following attack types. Each attack type is discussed in more detail in the following sections.

• **Decryption Attack**: Decrypts the password that locks the file.

• **Dictionary Attack**: Uses the words in a dictionary, applies levels to the words, and converts the possible words into keys.

• **Keyspace Attack**: Tries every possible key because there is a finite number of keys for the file.

  **Note**: The possible number of keys can be very large, but with enough computing power, it is possible to try every key.

• **Reset**: Rewrites the key that opens the file to a key that comes from a password that you specify.

Decryption Attack

The decryption attack looks for the password that locks the file. In the files that PRTK uses the decryption attack on, the password is protected or scrambled with a known key. The password is then stored in the file itself.

PRTK knows the key that encrypts the password because the application uses the same key each time. (Each application in the decryption attack category uses a different key.) PRTK knows the location of the encrypted password in the file, applies the key to it, and then decrypts the password.
Dictionary Attack

PRTK tries to find the passwords of these documents, because an exhaustive key search takes an unreasonable amount of time.

Most people use passwords that they can remember. If you limit a set of passwords to a language they speak or other biographical data of the people, there is a good chance of finding the password in a reasonable time frame.

The language, biographical data, and other information is stored in dictionaries. PRTK uses dictionaries to try to find a password. Levels are applied to the words in a dictionary to further attempt password recovery.

For example, one level is a primary search using the dictionaries. The primary search includes the words with all lower-case letters, all capital letters, one capital letter followed by all lower-case letters, and one lower-case letter followed by all capital letters, such as hello, Hello, HELLO, hELLO etc.

When PRTK discovers a password, it adds it automatically to a Golden Dictionary. Each time a new password is added, the updated Golden Dictionary is applied to the jobs in the job queue. If there are jobs with duplicate passwords, PRTK automatically discovers them by using the Golden Dictionary.

Keyspace Attack

The keyspace attack is typically used on applications that use 40-bit encryption or less. In 32-bit encryption applications, such as WinZip 6.0–8.1, there is a limit to the number of keys that can be stored. The limit is the largest number that can be represented with 32 bits.

This number might seem extremely large; but it is actually small enough that, with enough computing power, you can decrypt an encrypted document in a reasonable amount of time.

So with certain applications, PRTK generally finds the key for an encrypted document rather than the password because
there are a relatively small number of keys that can be created, and key recovery is guaranteed.

**Reset Attack**

In the reset attack, two types of keys are associated with an encrypted file: one key that encrypts the password for the file and one key that actually encrypts the file. The reset attack usually rewrites the key that encrypts the file to a key that comes from a known password.

**Current Encryption Standards**

Although it is helpful to understand the methods by which documents are encrypted, PRTK actually deciphers this information for you when you recover a password and does not require any user input.

**Symmetric Encryption**

In *symmetric encryption*, the encryption and decryption keys are the same. Some common symmetric encryption systems are:

- Data Encryption Standard (DES) is a 56-bit standard that is considered weak by current standards. It can easily be broken by a special hardware device known as “deep crack,” and it can be broken with a distributed network of computers. For more information, see “Distributed Network Attack” on page 4.

- Triple-DES (3DES) can be used with two keys (EDE2 112-bit) or three keys (EDE3 168-bit).

- Pretty Good Privacy (PGP) is used for sending secure e-mail. It provides both confidentiality and authentication.

- BestCrypt can be used with any of the following Hash functions and encryption algorithms: GOST and SHA Hash; GOST, DES, Blowfish, IDEA, Twofish, CAST, AES, RC6, and 3DES encryption.

- Advanced Encryption Standard (AES) has replaced DES as the encryption standard. It uses a 128-, 192-, or 256-bit key.
RC4

RC4 is a variable key-length stream cipher designed by RSA. Microsoft Word and Excel use RC4 and a 40-bit key to encrypt their files. Keys this small can be easily broken by governments, criminals, and amateurs.

Asymmetric Encryption

In asymmetric encryption, the encryption and decryption keys are different. Asymmetric encryption uses a public key (which can be posted on an Internet site or made “public” through other means) and a private key, which remains secret.

In this system, something that has been encrypted with the private key can only be decrypted by the public key, and vice versa.

Asymmetric algorithms are slower than symmetric algorithms, but can nonetheless be very useful. They are often used in combination with symmetric algorithms.

The number of possible key values refers to the actual number of different key words or passwords that can exist, based on the particular algorithm used to create the key value in question. This number can be calculated as follows: an $n$-bit key has $2^n$ possible values. For example, a 40-bit key has $2^{40}$ possible values, or approximately one trillion possibilities.

The security of an algorithm should rely on the secrecy of the key only, not the secrecy of the algorithm.
Hashing

Hashing is used to determine whether a file has changed. Producing two different items with the same hash value is computationally improbable since changing a single bit in a file results in a completely different hash. Therefore, hashes can function as a type of digital fingerprint that can be used to verify data integrity.

Before PRTK begins a password recovery, it automatically creates SHA and MD5 hash values for the files to be recovered. After a password is recovered, you can verify the hash values of a file providing proof that the contents of the file were not changed during the recovery of the file’s password.

PRTK uses two different hashing methods.

Secure Hash Algorithm (SHA)

The National Institute of Standards and Technology (NIST) designed the Secure Hash Algorithm (SHA). SHA takes as input an arbitrary-length file and outputs a fixed-length number referred to as a “hash” or “digest.” SHA-1 produces a 160-bit (20 byte) digest. SHA hashes take longer to generate than MD5 hashes.

Message Digest 5 (MD5)

Message Digest 5 (MD5) was developed by Professor Ronald L. Rivest. MD5 takes as input an arbitrary-length file and outputs a fixed-length number referred to as a “hash” or “digest.” MD5 produces a 128-bit (16-byte) digest. MD5 is a faster implementation than SHA.
Program Files

The following tables identify key program files, their locations, and their functions for Password Recovery Toolkit (PRTK).

- “PRTK Files” on page 262

The following tables identify key program files, their locations, and their functions for the Distributed Network Attack (DNA) system.

- “DNA Supervisor Files” on page 263
- “DNA Worker Files” on page 266
## PRTK Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Directory Location</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.adf</td>
<td>\AccessData\PRTK 6\Dictionaries</td>
<td>A dictionary file. Codepage dictionaries have -c appended to the filename. Unicode dictionaries have -u appended to the filename.</td>
</tr>
<tr>
<td>*.profile</td>
<td>\AccessData\PRTK 6\Profiles</td>
<td>A profile file, which contains information about the dictionaries and levels used to decrypt files.</td>
</tr>
<tr>
<td>\bin directory</td>
<td>\AccessData\PRTK 6</td>
<td>A directory containing a portion of the Java Runtime Environment, which runs PRTK.</td>
</tr>
<tr>
<td>\data directory</td>
<td>\AccessData\PRTK 6</td>
<td>The directory that contains the PRTK database files.</td>
</tr>
<tr>
<td>\Dictionaries directory</td>
<td>\AccessData\PRTK 6</td>
<td>The directory that contains the dictionaries used by PRTK.</td>
</tr>
<tr>
<td>GoldenDictionary</td>
<td>\AccessData\PRTK 6\Dictionaries</td>
<td>A file added after the installation that contains all passwords recovered by PRTK.</td>
</tr>
<tr>
<td>\Levels directory</td>
<td>\AccessData\PRTK 6</td>
<td>The directory that contains the password recovery levels used by PRTK.</td>
</tr>
<tr>
<td>\lib directory</td>
<td>\AccessData\PRTK 6</td>
<td>A directory containing a portion of the Java Runtime Environment, which runs PRTK.</td>
</tr>
<tr>
<td>\Modules directory</td>
<td>\AccessData\PRTK 6</td>
<td>The directory that contains the application modules supported by PRTK.</td>
</tr>
</tbody>
</table>
### Additional PRTK Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Directory Location</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ad_dictionaryutility.jar</td>
<td>\AccessData\PRTK6</td>
<td>The Dictionary Utility program.</td>
</tr>
</tbody>
</table>

### DNA Supervisor Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Directory Location</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ADF</em></td>
<td>\AccessData\DNA 3\Supervisor\Dictionaries</td>
<td>A dictionary file. Codepage dictionaries have -c appended to the filename. Unicode dictionaries have -U appended to the filename.</td>
</tr>
<tr>
<td><em>Profile</em></td>
<td>\AccessData\DNA 3\Supervisor\Profiles</td>
<td>A profile file, which contains information about the dictionaries and levels used to decrypt files.</td>
</tr>
<tr>
<td>Bin directory</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>A directory used by the JavaVirtual Machine, which runs DNA.</td>
</tr>
<tr>
<td>Data directory</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>The directory that contains the DNA database files.</td>
</tr>
<tr>
<td>Dictionaries directory</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>The directory that contains the dictionaries used by DNA.</td>
</tr>
<tr>
<td>Filename</td>
<td>Directory Location</td>
<td>Function</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>generate_keys</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>A file used by the DNA installation program to create encrypted communication between the supervisor and worker.</td>
</tr>
<tr>
<td>generate_worker_install</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>A file used by the DNA installation program to create the DNA Worker installation files available in the Supervisor directory.</td>
</tr>
<tr>
<td>GoldenDictionary</td>
<td>\AccessData\DNA 3\Supervisor \Dictionaries</td>
<td>A file added after the installation that contains all passwords recovered by the DNA Supervisor.</td>
</tr>
<tr>
<td>Levels directory</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>The directory that contains the password recovery levels used by DNA.</td>
</tr>
<tr>
<td>lib directory</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>A directory used by the Java Virtual Machine, which runs DNA.</td>
</tr>
<tr>
<td>Modules directory</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>The directory that contains the application modules supported by DNA.</td>
</tr>
<tr>
<td>Profiles directory</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>The directory that contains the profiles used by DNA.</td>
</tr>
<tr>
<td>postgres</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>A DNA database executable. This process must be running in order for DNA to work.</td>
</tr>
<tr>
<td>postmaster</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>A DNA database executable. This process must be running in order for DNA to work.</td>
</tr>
<tr>
<td>Filename</td>
<td>Directory Location</td>
<td>Function</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>prefs</td>
<td>\AccessData\DNA3\Supervisor</td>
<td>A file added after the installation that holds preferences, including the option to decrypt the file after key recovery and the dimensions of the DNA management interface.</td>
</tr>
<tr>
<td>Supervisor</td>
<td>\AccessData\DNA3\Supervisor</td>
<td>The DNA Supervisor program. You manage the DNA Supervisor from the management interface.</td>
</tr>
<tr>
<td>user_defined</td>
<td>\AccessData\DNA3\Supervisor\Levels</td>
<td>The file that contains information about each level that you have created.</td>
</tr>
<tr>
<td>worker</td>
<td>\AccessData\DNA3\Supervisor</td>
<td>The DNA Worker program. This file is only added to this directory if the DNA Worker is installed on the same machine as the supervisor.</td>
</tr>
<tr>
<td>worker-i386-install.sh</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>The DNA Worker installation program for Linux machines.</td>
</tr>
<tr>
<td>worker_service</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>A file used by the DNA installation program to create the services needed by the DNA Worker installation files available in the Supervisor directory.</td>
</tr>
<tr>
<td>worker-mac-install.sh</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>The DNA Worker installation program for Macintosh machines.</td>
</tr>
<tr>
<td>WorkerInstall</td>
<td>\AccessData\DNA 3\Supervisor</td>
<td>The DNA Worker installation program for Windows workstations.</td>
</tr>
</tbody>
</table>
## DNA Worker Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Directory Location</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.adf</td>
<td>\AccessData\DNA 3\Worker</td>
<td>A dictionary file that the worker receives from the supervisor when it processes jobs. Codepage dictionaries have -c appended to the filename. Unicode dictionaries have -u appended to the filename.</td>
</tr>
<tr>
<td>\bin directory</td>
<td>\AccessData\DNA 3\Worker</td>
<td>A directory used by the Java Virtual Machine, which runs DNA Worker.</td>
</tr>
<tr>
<td>\lib directory</td>
<td>\AccessData\DNA 3\Worker</td>
<td>A directory used by the Java Virtual Machine, which runs DNA Worker.</td>
</tr>
<tr>
<td>worker.exe</td>
<td>\AccessData\DNA 3\Worker</td>
<td>The DNA Worker program. On the DNA Worker machine, you manage the worker from the DNA Worker interface.</td>
</tr>
<tr>
<td>Worker.ini</td>
<td>\AccessData\DNA 3\Worker</td>
<td>The file that contains configuration information about the worker, including its supervisor hostname and IP address.</td>
</tr>
<tr>
<td>worker_service</td>
<td>\AccessData\DNA 3\Worker</td>
<td>A service needed by the DNA Worker. This service must be running in order to process jobs on the DNA Worker.</td>
</tr>
</tbody>
</table>
## Additional DNA Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Directory Location</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>ad_dictionaryutility.jar</td>
<td>\AccessData\DNA3\</td>
<td>The Dictionary Utility program.</td>
</tr>
</tbody>
</table>
Recovering EFS Files

On Windows 200 and Windows XP systems, Microsoft’s encrypted file system (EFS) allows you to encrypt a single file or to automatically encrypt all files saved to a particular folder. You don’t have to remember passwords because Windows encrypts the data using your login password.

You must use FTK to decrypt EFS-encrypted files. PRTK recovers EFS files by retrieving your login password from the EFS master key file (drive\Documents and Settings\user\Application Data\Protect\user_SID).

Ultimately, this recovery performs the same function as the SAM file attack. Recovering the user login password from the SAM file can be faster than recovering the login password from the EFS master key file. Use the SAM file to recover the user’s login password.

Note: When used in conjunction with PRTK, FTK1.50b and above has an option to automatically decrypt EFS files. Essentially, FTK sends PRTK the EFS master key file along with any other EFS-related keys. PRTK then performs an EFS attack to obtain the user login password. FTK and PRTK must be running on the same machine to support this integrated functionality.

Recovering EFS on Windows XP Service Pack 1 or Later

If you are using Windows XP Service Pack 1 or later, you must export the SAM and SYSTEM file using FTK Imager or FTK and import the files into PRTK to obtain the login password. After PRTK has obtained the password, you can provide the
password to FTK so that FTK can continue decrypting the EFS files.

To recover EFS files:

1. Start PRTK.
2. In PRTK, add the SAM file and system file and browse to the SYSTEM file when the syskey is requested.
3. After obtaining the login password, start FTK.
4. In FTK, select **Tools**, then **Enter EFS Password**, and then click **OK**.
5. Enter the password.

FTK decrypts the EFS passwords if the login password obtained from the SAM and SYSTEM files is valid. If FTK cannot decrypt the EFS passwords, either the login password has been changed after the SAM and SYSTEM files were obtained or the EFS file was encrypted by another user.

**Important:** If there are multiple users on a workstation, you must have all user login passwords to increase chances of decrypting the files. EFS files could have been encrypted by more than one of the users. FTK and PRTK must be running on the same dongle on the same machine to support this integrated functionality.

**Other Notes**

In Windows 2000, every file is also encrypted with the Recovery Agent's EFS public key. The Administrator user is the default Recovery Agent for computers that are not a part of a domain. If the computer is joined to a Windows 2000 domain, the Domain Administrator user is the default Recovery Agent. In Windows XP, the Recovery Agent is optional.

Certain files cannot be encrypted:

- System files
- NTFS compressed files
- Files in `%Systemroot%` and its subdirectories
Corporate Information

This appendix contains the following corporate information about AccessData and its products:

- “Registration” on page 272
- “License Agreement” on page 272
- “Subscriptions” on page 275
- “Technical Support” on page 276
Registration

The AccessData product registration is tracked by the dongle included with your purchase, and managed by AccessData. To view your current registration, use the AccessData LicenseManager interface. For more information, see Managing Licenses.

License Agreement

BEFORE OPENING THE SEAL ON THIS PACKAGE, CAREFULLY READ THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE ("LICENSE") TO USE THE PASSWORD RECOVERY TOOLKIT SOFTWARE (PRTK) DISKETTES ("DISKETTES") AND ACCOMPANYING PRTK USER DOCUMENTATION ("DOCUMENTATION") CONTAINED IN THIS PACKAGE (COLLECTIVELY REFERRED TO AS "YOU OR YOUR") AND ACCESSDATA, INCLUDING ITS SUCCESSORS OR ASSIGNS (REFERRED TO AS "LICENSOR"), AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES. IF YOU DO NOT WISH TO ENTER INTO THIS LICENSE, RETURN TO THE PLACE OF PURCHASE, ALONG WITH NONE OF THE SEALS BROKEN, FOR A REFUND OF THE PURCHASE PRICE LESS ANY APPLICABLE RETAILER HANDLING, RESTOCKING, OR SERVICE CHARGES.

LICENSE GRANT. Licensor hereby grants to You, and You accept, a nonexclusive license to use the Diskettes, including the forensic investigation software contained therein in object-code-only from ("Software"), and Documentation, only as authorized in this License. The Software may be used only on a single computer owned, leased, or otherwise controlled by You; or, in the event of the inoperability of that system, on a backup system selected by You. Concurrent use of the program on two or more systems is not authorized without the advance written consent of Licensor and the payment of additional license fees. You agree that You will not assign, sublicense, transfer, pledge, lease, rent, or share Your rights under this License.
Upon loading the Software into Your system, You may retain the media for backup purposes. In addition, You may make one copy of the Software on a second set of media for the purpose of backup in the event that the original media is damaged or destroyed. Any such copies of the Software shall include Licensor’s copyright and other proprietary notices.

Except as authorized under this paragraph, no copies of the Program or any portions thereof may be made by You or any person under Your authority or control.

LICENSOR’S RIGHTS. You acknowledge and agree that the Program consists of proprietary, published and unpublished property of Licensor, protected under United States copyright law and trade secret laws of general applicability. You further acknowledge and agree that all right, title, and interest in and to the Program are and shall remain with Licensor. This License does not convey to you an interest in or to the Program, but only a limited right of use revocable in accordance with the terms of this License.

LICENSE FEES. The license fees paid by You are paid in consideration of the licenses granted under this License.

SOFTWARE INSTALLATION. It shall be Your sole responsibility to install and make operational the Software on Your system. In the event you need installation assistance, such services may be available from Licensor at an additional cost to You.

TERM. This License is effective upon Your breaking of any of the seals on the package containing the Program, and shall continue until terminated. You may terminate this License at any time by returning the entire Program, including the Media, Software and Documentation, and other paraphernalia and all copies thereof and extracts therefrom, to Licensor and by erasing all copies of the software that may be located on any systems owned or controlled by You or upon which You know a copy of the Software has been placed. Licensor may terminate this License upon the breach by You of any term hereof. Upon such termination by Licensor, You agree to immediately return to Licensor the entire Program, including the Diskettes, Software and Documentation, and all copies thereof and extracts therefrom, and to erase all copies of the
Software that may be located on any systems owned or controlled by You or upon which You know a copy of the Software has been placed.

LIMITED WARRANTY. Licensor warrants, for Your benefit alone, that the Diskettes in which the Software is embedded shall, for a period of sixty (60) days from the date of Your purchase of the Program (referred to as the “Warranty Period”), be free from defects in material and workmanship. Licensor further warrants, for Your benefit alone, that during the Warranty Period the software shall operate substantially in accordance with the Documentation.

If, during the Warranty Period, a defect in the Program diskettes or Software appears, You may return the Program to Licensor personally or by mail to AccessData, 1317 East 750 North, Orem, Utah 84097, with written instructions for replacement.

YOU AGREE THAT THE FOREGOING CONSTITUTES YOUR SOLE AND EXCLUSIVE REMEDY FOR BREACH BY LICENSOR OF ANY WARRANTIES MADE UNDER THIS LICENSE. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE PROGRAM, DISKETTES, SOFTWARE AND DOCUMENTATION ARE LICENSED “AS IS,” AND LICENSOR DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

LIMITATION OF LIABILITY. LICENSOR’S CUMULATIVE LIABILITY TO YOU OR ANY OTHER PARTY FOR ANY LOSS OR DAMAGES RESULTING FROM ANY CLAIMS, DEMANDS, OR ACTIONS ARISING OUT OF OR RELATING TO THIS LICENSE OR THE USE OF THE PROGRAM SHALL BE LIMITED TO REPLACEMENT OF THE PROGRAM AND, IN ANY EVENT, SHALL NOT EXCEED THE LICENSE FEE PAID TO LICENSOR FOR THE USE OF THE PROGRAM. IN NO EVENT SHALL LICENSOR BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES.
OR LOST PROFITS OR ANY SIMILAR CLAIMS, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

INDEMNIFICATION. You accept full legal responsibility for all forensic investigations performed through Your use of the Program. You agree to hold harmless and indemnify Licensor for any and all demands, claims, legal action and damages, including all attorney’s fees and costs, against Licensor, which arise out of Your use of the Program.

In any legal action regarding the indemnification contained in paragraph 7, the prevailing party shall be entitled to recover from the nonprevailing party all of its attorney’s fees and costs.

GOVERNING LAW. This License shall be construed and governed in accordance with the laws of the State of Utah. Any dispute arising out of or with respect to this License between You and Licensor shall be solely adjudicated by the competent Federal or State court situated in Salt Lake City, Utah. You and Licensor consent to the venue and jurisdiction of such court for purposes of any such dispute.

SEVERABILITY. Should any court of competent jurisdiction declare any term of this License void or unenforceable, such declaration shall have no effect on the remaining terms hereof.

NO WAIVER. The failure of either you or Licensor to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breach.

Subscriptions

A yearly subscription is now offered on all AccessData software. A subscription is good for one year from the date of purchase.

The AccessData subscription service allows you to download updates from the AccessData Website during the subscription period.
You can use LicenseManager to check for product updates and to download the latest product versions. For more information, see “Managing Licenses” on page 181.

For more information on the general features of the subscription service, see the AccessData Website at http://www.accessdata.com/products/subscriptions.

**Technical Support**

AccessData offers free technical support on all of its software from 8:00 a.m. to 5:30 p.m. MST.

You can get technical support in these ways:

- **Phone** Long distance: 1–800–658–5199
- **Fax** 1–801–377–5426
- **Website** http://www.accessdata.com
  - Product-specific FAQs that list common questions and their quick fixes.
  - Online Support Form to submit for support at http://www.accessdata.com/support. All support inquiries are typically answered within 24 hours. If there is an urgent need for support, contact AccessData via phone.
  - Forensic Bulletin Board provides a forum to share questions and answers with other AccessData users.

- **E-mail** support@accessdata.com

**Documentation**

Please e-mail any typos, inaccuracies, or other problems you find with the documentation to:

documentation@accessdata.com
ADR Session
In PRTK, selecting one or more files and starting the password recovery process is called an ADR (AccessData Recovery) session. Typically, each case has one session unless you have a large number of encrypted files.

Address
A location of data, usually in main memory or on a disk. You can think of computer memory as an array of storage boxes, each of which is one byte in length. Each box has an address (a unique number) assigned to it. By specifying a memory address, programmers can access a particular byte of data. Disks are divided into tracks and sectors, each of which has a unique address.

Advanced Encryption Standard
A common symmetric encryption system that has replaced Data Encryption Standard as the encryption standard. It uses a 128, 192, or 256-bit key.

Asymmetric Encryption
A type of encryption in which the encryption and decryption keys are different. Asymmetric encryption uses a public key (which can be posted on an Internet site or made “public” through other means) and a private key, which remains secret. In this system, something that has been encrypted with the private key can be decrypted only by the public key, and vice versa. Asymmetric algorithms are slower than symmetric algorithms, but can nonetheless be very useful. They are often used in combination with symmetric algorithms, as with EFS Encryption.

The number of possible key values refers to the actual number of different key words or passwords that can exist, based on the
particular algorithm used to create the key value in question. This number can be calculated as follows: an n-bit key has $2^n$ possible values. For example, a 40-bit key has 240 possible values, or 1,099,511,627,776 possibilities.

The security of an algorithm should rely on the secrecy of the key only, not the secrecy of the algorithm.

You shouldn’t compare key sizes between symmetric and asymmetric algorithms. For example, a 128-bit symmetric key is approximately as strong as a 512-bit asymmetric key.

**BestCrypt**

A common symmetric encryption system that can be used with any of the following hash functions and encryption algorithms:

- GOST
- SHA1 Hash
- Blowfish
- IDEA
- Twofish
- CAST
- AES
- RC6
- 3DES encryption

**Binary**

Pertaining to a number system that has just two unique digits. Computers are based on the binary numbering system, which consists of just two unique numbers, 0 and 1. All operations that are possible in the decimal system (addition, subtraction, multiplication, and division) are equally possible in the binary system.

**BIOS**

Acronym for Basic Input/Output System. The BIOS is built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code
required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

**Bit-stream Image**

*(See Forensic Image)*

**Bookmark**

A menu entry or icon on a computer that is most often created by the user and that serves as a shortcut to a previously viewed location (as an Internet address). The term “bookmark” as used in a Computer Crimes Unit report refers to locating a file, folder or specific item of interest to the examiner or to the investigator. The location of the data (file name, file location, relative path, and hardware address) is identified. Other data can be addressed as well.

**Boot**

To load the first piece of software that starts a computer. Because the operating system is essential for running all other programs, it is usually the first piece of software loaded during the boot process.

**Boot Record**

All the three types of FAT have a boot record, which is located within an area of reserved sectors. The DOS format program reserves 1 sector for FAT12 and FAT16 and usually 32 sectors for FAT32.

**Chunk Size**

The number of passwords the supervisor machine can process in the amount of time specified.

**Cluster**

Fixed-length blocks that store files on the FAT media. Each cluster is assigned a unique number by the computer operating system. Only the part of the partition called the “data area” is divided into clusters. The rest of the partition is simply sectors. Files and directories store their data in these clusters. The size of one cluster is specified in a structure called the Boot Record, and can range from a single sector to 128 sectors. The operating system assigns a unique number to each cluster and the keeps track of files according to which cluster they use.
CMOS

Short for Complementary Metal Oxide Semiconductor. Pronounced SEE-moss, CMOS is a widely used type of semiconductor. CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor. This makes them particularly attractive for use in battery-powered devices, such as portable computers. Personal computers also contain a small amount of battery-powered CMOS memory to hold the date, time, and system setup parameters.

CRC

Short for Cyclical Redundancy Check. It performs a complex calculation on every byte in the file, generating a unique number for the file in question. If so much as a single byte in the file being checked were to change, the cyclical redundancy check value for that file would also change. If you know the CRC value for a file before it is downloaded, you can compare it with the CRC value generated by this software after the file has been downloaded to ascertain whether the file was damaged in transit. The odds of two files having the same CRC value are even longer than the odds of winning a state-run lottery—along the lines of one in 4,294,967,296.

Cylinder

A single-track location on all the platters making up a hard disk. For example, if a hard disk has four platters, each with 600 tracks, then there will be 600 cylinders, and each cylinder will consist of 8 tracks (assuming that each platter has tracks on both sides).

dd

(\text{Linux}) \text{ Makes a copy of a input file (STDIN) using the specified conditions, and sends the results to the output file (STDOUT).}

Data Encryption Standard

A 56-bit symmetric encryption system that is considered weak by current standards. It has been broken in a distributed environment.

Device

Any machine or component that attaches to a computer. Examples of devices include disk drives, printers, mice, and modems. These
particular devices fall into the category of peripheral devices because they are separate from the main computer.

Most devices, whether peripheral or not, require a program called a device driver that acts as a translator, converting general commands from an application into specific commands that the device understands.

**Disk**

A round plate on which data can be encoded. There are two basic types of disks: magnetic disks and optical disks.

**EnScript (also "e script")**

EnScript is a language and APT that has been designed to operate within the EnCase environment. EnScript is compatible with the ANSI C++ standard for expression evaluation and operator meanings but contains only a small subset of C++ features. In other words, EnScript uses the same operators and general syntax as C++ but classes and functions are organized differently.

**Evidence Item**

A physical drive, a logical drive or partition, or drive space not included in any partitioned virtual drive.

**File Allocation Table (FAT)**

A table that the operating system uses to locate files on a disk. A file may be divided into many sections that are scattered around the disk. The FAT keeps track of all these pieces.

There is a field in the Boot Record that specifies the number of FAT copies. With FAT12 and FAT16, MS-DOS uses only the first copy, but the other copies are kept in sync. FAT32 was enhanced to specify which FAT copy is the active one in a 4-bit value part of a Flags field.

Think of the FAT as a singly linked list. Each of the chains in the FAT specify which parts of the disk belong to a given file or directory.

A file allocation table is a simple array of 12-bit, 16-bit or 32-bit data elements. Usually there will be two identical copies of the FAT.

**FAT12:** The oldest type of FAT uses a 12-bit binary number to hold the cluster number. A volume formatted using FAT12 can hold a
maximum of 4,086 clusters, which is $2^{12}$ minus a few values (to allow for reserved values to be used in the FAT). FAT12 is most suitable for very small volumes, and is used on floppy disks and hard disk partitions smaller than about 16 MB (the latter being rare today.)

**FAT16:** The FAT used for older systems, and for small partitions on modern systems, uses a 16-bit binary number to hold cluster numbers. When you see someone refer to a FAT volume generically, they are usually referring to FAT16, because it is the de facto standard for hard disks, even with FAT32 now more popular than FAT16. A volume using FAT16 can hold a maximum of 65,526 clusters, which is $2^{16}$ less a few values (again for reserved values in the FAT). FAT16 is used for hard disk volumes ranging in size from 16 MB to 2,048 MB. VFAT is a variant of FAT16.

**FAT32:** The newest FAT type, FAT32 is supported by newer versions of Windows, including Windows 95's OEM SR2 release, as well as Windows 98, Windows ME and Windows 2000. FAT32 uses a 28-bit binary cluster number—not 32 because 4 of the 32 bits are reserved. 28 bits is still enough to permit ridiculously huge volumes—FAT32 can theoretically handle volumes with over 268 million clusters, and will theoretically support drives up to 2 TB in size. To do this, however, the size of the FAT grows very large; see here for details on FAT32’s limitations.

VFAT has several key features and improvements compared to FAT12 and FAT16:

- **Long File Name Support:** One of the most annoying limitations of operating systems prior to Windows 95 was the eleven-character file name restriction. For most people, VFAT’s most important accomplishment was enabling the use of long file names by the Windows 95 operating system and applications written for it, while maintaining compatibility with older software that had been written before VFAT was implemented.

- **Improved Performance:** The disk access and file system management routines for VFAT were rewritten using 32-bit protected-mode code to improve performance. At the same time, 16-bit code was maintained, for use when required for compatibility.
Better Management Capabilities: Special support was added for techniques like disk locking, to allow utilities to access a disk in exclusive mode without fear of other programs using it in the meantime.

**File Header**

The data at the beginning of a file that identifies the file type: .gif, .doc .txt etc.

**File Footer**

The data at the end of the file signifying the file is complete and allows the file to be understood by the operating system.

**File Item**

Any item FTK can parse from the evidence. This includes complete files as well as sub-elements such as graphics, files, or OLE objects embedded in other files; deleted items recovered from unallocated space; and so forth.

**File Slack**

Unused space. Operating systems store files in fixed-length blocks called clusters. Because few files are a size that is an exact multiple of the cluster size, there is typically unused space between the end of the file and the end of the last cluster used by that file.

**Forensic Image**

A process where all areas of a physical disk are copied, sector by sector, to storage media. This image may be a raw file, as in the case of the Linux utility DD, or it may be a forensically correct copy, such as SPADA provides. These images replicate exactly all sectors on a given storage device. All files, unallocated data areas, and areas not normally accessible to a user are copied.

**Forensically Prepared Media**

Digital media (such as a diskette, tape, CD, hard drive) that is sanitized (wiped clean) of all data. This means computer media that may be sanitized up to the Department of Defense standards 5220.22-M (National Industrial Security Program Operating Manual Supplement) using software wipe utilities such as Dan Mares (Maresware) Declassify, New Technologies Inc (NTI) Disk Scrub or M-Sweep Pro or Symantec (Norton) WipeInfo to remove
all data by overwriting the existing data with random or pre-defined characters. The Linux OS may also be used to write out a value of zero (0) to a device.

The media is then examined using tools to determine that no data exists (MD5, SHA1 or Diskedit). The partition information is removed and the media is sanitized from the physical address of (cylinder/head/sector) 0/0/1 to the physical (versus logical) end of the media.

The partition information is removed and the media is sanitized from the physical address of (cylinder/head/sector) 0/0/1 to the physical (versus logical) end of the media. This process involves using a program such as I-wipe, Encase, Linux, Drivespy, SPADA or any program capable of writing multiple passes of a single character over the entire drive.

Checksum is a form of redundancy check, a very simple measure for protecting the integrity of data by detecting errors in data that. It works by adding up the basic components of a message, typically the bytes, and storing the resulting value. Later, anyone can perform the same operation on the data, compare the result to the authentic checksum and (assuming that the sums match) conclude that the message was probably not corrupted.

Redundancy check is extra data added to a message for the purposes of error detection and error correction.

The value of the checksum of forensically prepared media will be zero (0) provided the write process is done using zeros.

**Graphic Image Files**

Computer graphic image files such as photos; drawings, etc. Come in various standard formats. Some of the most common file types include but are not limited to Joint Photographic Experts Group (JPEG, JPG), Bitmap (BMP), Graphics Interchange Format (GIF, JFIF) and AOL image file (ART).

**Golden Dictionary**

The Golden Dictionary file, ADPasswords.dat, contains all recovered passwords for all PRTK sessions on the current computer. It is stored in the AccessData program directory (drive:\Program Files\AccessData\Recovery\). Recovered passwords are used as the first level of attack in all password
recovery sessions. Most people use the same password for different files, so recovering the password for a simple file often opens the door to more difficult files.

**Graphic Interchange Format (GIF)**

A common graphics format that can be displayed on almost all Web browsers. GIFs typically display in 256 colors and have built-in compression. Static or animated GIF images are the most common form of banner creative.

**Hard Disk (Drive)**

A magnetic disk on which you can store computer data. The term hard is used to distinguish it from a soft or floppy, disk. Hard disks hold more data and are faster than floppy disks. A hard disk, for example, can store anywhere from 10 megabytes to several gigabytes, whereas most floppies have a maximum storage capacity of 1.4 megabytes.

**Hashing**

Generating a unique alphanumeric value based on a file’s contents. The alphanumeric value can be used to prove that a file copy has not been altered in any way from the original. It is statistically impossible for an altered file to generate the same hash number.

**Head**

The mechanism that reads data from or writes data to a magnetic disk or tape. Hard disk drives have many heads, usually two for each platter.

**Hexadecimal**

The base-16 number system, which consists of 16 unique symbols: the numbers zero through nine and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (eight bits) as two consecutive hexadecimal digits. It is easier for humans to read hexadecimal numbers than binary numbers.

**Markov Permutation**

The Markov permutation records the times certain words, letters, punctuation, and spaces occur together in a given amount of text,
then generates random output that has the same distribution of groups.

For example: if you were to scan through the text and create a huge frequency table of what words come after the words “up the,” you might find “tree,” “ladder,” and “creek” most often. You would then generate output from the words “up the,” and get the results “up the tree,” “up the creek,” and “up the ladder” randomly.

If the words “up the” were followed most frequently by the word “creek” in your sample text, the phrase “up the creek” would occur most frequently in your random output.

Andrey Andreyevich Markov (June 14, 1856–July 20, 1922) was a Russian mathematician.

**Message Digest 5 (MD5)**

An algorithm created in 1991 by Professor Ronald Rivest that is used to create digital signatures, or a 128-bit digital fingerprint based on a file's content. Message Digest 5 (MD5) takes as input an arbitrary-length file and outputs a fixed-length number referred to as a hash or digest. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest. When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn’t been changed. This comparison is called a hash check.

**Memory**

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips; the word storage is used for memory that exists on tapes or disks. Moreover, the term memory is usually used as shorthand for physical memory, which refers to the actual chips capable of holding data.

**Message Digest 5**

A 128-bit digital fingerprint based on a file's content that was designed by Ron Rivest of RSA. Message Digest 5 (MD5) takes as input an arbitrary-length file and outputs a fixed-length number referred to as a hash or digest. The number is derived from the input in such a way that it is computationally infeasible to derive
any information about the input from the hash. It is also computationally infeasible to find another file that will produce the same output.

MD5 hashes are used by the KFF to identify known files.

**Metadata**

Literally data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted. Metadata is essential for understanding information stored in data warehouses and has become increasingly important in XML-based Web applications.

**Mount**

To make a mass storage device available to the OS, or to a user or user group. In may also mean to make a device physically accessible. In a Unix environment, the mount command attaches discs or directories logically rather than physically. The Unix mount command makes a directory accessible by attaching a root directory of one file system to another directory, which makes all the file systems usable as if they were subdirectories of the file system they are attached to. Unix recognizes devices by their location, while Windows recognizes them by their names (C: drive, for example). Unix organizes directories in a tree-like structure, in which directories are attached by mounting them on the branches of the tree. The file system location where the device is attached is called a mount point. Mounts may be local or remote. A local mount connects disk drives on one machine so that they behave as one logical system. A remote mount uses Network File System (NFS) to connect to directories on other machines so that they can be used as if they were all part of the user’s file system.

**NT File System (NTFS)**

One of the file systems for the Windows NT operating system (Windows NT also supports the FAT file system). NTFS has features to improve reliability, such as transaction logs to help recover from disk failures. To control access to files, you can set permissions for directories or individual files. NTFS files are not accessible from other operating systems, such as DOS. For large applications, NTFS supports spanning volumes, which means files and directories, can be spread out across several physical disks.
Pagefile (.sys)

The paging file is the area on the hard disk that Windows uses as if it were random access memory (RAM). This is sometimes known as virtual memory. By default, Windows stores this file on the same partition as the Windows system files.

Pretty Good Privacy

A common symmetric encryption system used for exchanging files and e-mail. It provides both privacy and authentication.

RC4

RC4, or ARC4, is a variable key-length stream cipher designed by RSA. Stream ciphers are key-dependent, pseudo-random number generators whose output is XORed with the data: \( \text{plaintext} \oplus \text{random-looking stream} = \text{random-looking ciphertext} \). Because XOR is symmetric (in other words, \( \text{A} \oplus \text{B} \oplus \text{B} = \text{A} \)), XORing the ciphertext with the stream again returns the plaintext. Microsoft Word and Excel use RC4 and a 40-bit key to encrypt their files. An exhaustive key space attack has a much better chance at succeeding with a 40-bit key space.

Sector

A sector is a group of bytes within a track and is the smallest group of bytes that can be addressed on a drive. There are normally tens or hundreds of sectors within each track. The number of bytes in a sector can vary, but is almost always 512. The maximum number of sectors in a cluster is 64. CDROMS normally have 2048 bytes per sector. Sectors are numbered sequentially within a track, starting at 1. The numbering restarts on every track, so that “track 0, sector 1” and “track 5, sector 1” refer to different sectors. Modern drives use a system known as Logical Block Addressing (LBA) instead of CHS to track sectors.

During a low-level format, hard disks are divided into tracks and sectors. The tracks are concentric circles around the disk and the sectors are segments within each circle. For example, a formatted disk might have 40 tracks, with each track divided into ten sectors.

Physical sectors are relative to the entire drive. Logical sectors are relative to the partition.
Secure Hash Algorithm

A 160-bit digital fingerprint based on a file’s content. Designed by the National Institute of Standards and Technology (NIST), Secure Hash Algorithm (SHA) takes as input an arbitrary-length file and outputs a fixed-length number referred to as a hash or digest. The number is derived from the input in such a way that it is computationally impossible to derive any information about the input from the hash. It is also computationally impossible to find another file that will produce the same output. SHA1 hashes are used by the KFF to identify known files.

FTK uses SHA-1. The KFF library contains some A hashes.

SHA1

The SHA (Secure Hash Algorithm) family is a set of related cryptographic hash functions. The most commonly used function in the family, SHA-1, is employed in a large variety of popular security applications and protocols, including TLS, SSL, PGP, SSH, S/MIME, and IPSec. SHA-1 is considered to be the successor to MD5, an earlier, widely-used hash function. The SHA algorithms were designed by the National Security Agency (NSA) and published as a US government standard.

The first member of the family, published in 1993, is officially called SHA; however, it is often called SHA-0 to avoid confusion with its successors. Two years later, SHA-1, the first successor to SHA, was published. Four more variants have since been issued with increased output ranges and a slightly different design: SHA-224, SHA-256, SHA-384, and SHA-512—sometimes collectively referred to as SHA-2.

Attacks have been found for both SHA-0 and SHA-1. No attacks have yet been reported on the SHA-2 variants, but since they are similar to SHA-1, researchers are worried, and are developing candidates for a new, better hashing standard.

Spool (spooling, print spool)

Acronym for Simultaneous Peripheral Operations On-Line, spooling refers to putting jobs in a buffer, a special area in memory or on a disk where a device can access them when it is ready. Spooling is useful because devices access data at different rates. The buffer provides a waiting station where data can rest while the slower device catches up.
The most common spooling application is print spooling. In print spooling, documents are loaded into a buffer (usually an area on a disk), and then the printer pulls them off the buffer at its own rate. Because the documents are in a buffer where they can be accessed by the printer, you can perform other operations on the computer while printing takes place in the background. Spooling also lets you place a number of print jobs on a queue instead of waiting for each one to finish before specifying the next one.

(File and RAM) Slack

Files are created in varying lengths depending on their contents. DOS, Windows and Windows NT-based computers store files in fixed length blocks of data called clusters. Rarely do file sizes exactly match the size of one or multiple clusters perfectly. The data storage space that exists from the end of the file to the end of the last cluster assigned to the file is called file slack. Cluster sizes vary in length depending on the operating system involved and, in the case of Windows 95, the size of the logical partition involved. Larger cluster sizes mean more file slack and also the waste of storage space when Windows 95 systems are involved.

File slack potentially contains randomly selected bytes of data from computer memory. This happens because DOS/Windows normally writes in 512 byte blocks called sectors. Clusters are made up of blocks of sectors. If there is not enough data in the file to fill the last sector in a file, DOS/Windows makes up the difference by padding the remaining space with data from the memory buffers of the operating system. This randomly selected data from memory is called RAM Slack because it comes from the memory of the computer.

RAM Slack can contain any information that may have been created, viewed, modified, downloaded or copied during work sessions that have occurred since the computer was last booted. Thus, if the computer has not been shut down for several days, the data stored in file slack can come from work sessions that occurred in the past.

RAM slack pertains only to the last sector of a file. If additional sectors are needed to round out the block size for the last cluster assigned to the file, then a different type of slack is created. It is called drive slack and it is stored in the remaining sectors which might be needed by the operating system to derive the size needed.
to create the last cluster assigned to the file. Unlike RAM slack, which comes from memory, drive slack is padded with what was stored on the storage device before. Such data could contain remnants of previously deleted files or data from the format pattern associated with disk storage space that has yet to be used by the computer.

For example, take a file that is created by writing the word “Hello.” Assuming that this is the only data written in the file and assuming a two sector cluster size for the file, the data stored to disk and written in file slack could be represented as follows:

Hello+++++++|————(EOC)

RAM Slack is indicated by “+”
Drive Slack is indicated by “–”

File Slack is created at the time a file is saved to disk. When a file is deleted under DOS, Windows, Windows 95, Windows 98 and Windows NT/2000/XP, the data associated with RAM slack and drive slack remains in the cluster that was previously assigned to the end of the deleted file. The clusters which made up the deleted file are released by the operating system and they remain on the disk in the form of unallocated storage space until the space is overwritten with data from a new file.

File slack potentially contains data dumped randomly from the computer’s memory, it is possible to identify network logon names, passwords and other sensitive information associated with computer usage. File slack can also be analyzed to identify prior uses of the subject computer and such legacy data can help the computer forensics investigator. File slack is not a trivial item. On large hard disk drives, file slack can involve several hundred megabytes of data. Fragments of prior E-Mail messages and word processing documents can be found in file slack. From a computer forensic standpoint, file slack is very important as both a source of computer evidence and security risks.
String Searches
A string search is a data string containing standard text or non-text data. The term may be a word, phrase or an expression. Keyword searches are designed to aid in the identification of potentially relevant data on the examined media.

Symmetric Encryption
A type of encryption in which the encryption and decryption keys are the same. Some common symmetric encryption systems are: Data Encryption Standard, Triple-DES, Pretty Good Privacy, BestCrypt, and Advanced Encryption Standard.

Thumbnail
Smaller size version of graphics image.

Unallocated Space
Also called free space, it consists of all the clusters on a drive that are not currently assigned to a file. Some of these clusters may still contain data from files that have been deleted but not yet overwritten by other files.

Until the first file is written to the data storage area of a computer storage device, the clusters are unallocated by the operating system in the File Allocation Table (FAT). These unallocated clusters are padded with format pattern characters and the unallocated clusters are not of interest to the computer forensics specialist until data is written to the clusters. As the computer user creates files, clusters are allocated in the File Allocation Table (FAT) to store the data. When the file is deleted by the computer user, the clusters allocated to the file are released by the operating system so new files and data can be stored in the clusters when needed. However, the data associated with the deleted file remains behind. This data storage area is referred to as unallocated storage space and it is fragile from an evidence preservation standpoint. However, until the unallocated storage space is reassigned by the operating system, the data remains behind for easy discovery and extraction by the computer forensics specialist. Unallocated file space potentially contains intact files, remnants of files and subdirectories and temporary files, which were transparently created and deleted by computer applications and also the operating system. All of such files and data fragments can be sources of computer evidence and also security leakage of sensitive data and information.
URL

Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located.

Volume

A volume refers to a mounted partition. There may be only one volume on a disk, such as a floppy disk or a zip disk. There may be several volumes on a disk as on a partitioned hard drive. A volume is a logical structure, not a physical device. There can be any number (up to 24) of these logical volumes on a disk and they show up as drive “c,” “d,” or “e” in DOS.

Volume Boot Sector

Since every partition may contain a different file system, each partition contains a volume boot sector which is used to describe the type of file system on the partition and usually contains boot code necessary to mount the file system.
A
AOL Communicator Account, password recovery 170
AOL Instant Messenger, password recovery 170
AOL Sign-On, password recovery 171
applications, supported 203
ASCII password 177
Asymmetric Encryption 258
attack
decryption 255
dictionary 256
keyspace 256
reset 257

B
bars, showing or hiding 49
biographical dictionary 150

C
computer forensic
handling evidence 2

D
decrypted files 81
saving 82
saving manually 82
troubleshooting 197
decryption
attack 255
understanding 255
demo mode 42
dictionary
attack 256
biographical 150
creating 150
creating biographical 155
Markov 131
understanding 149
user 150
Distributed Network Attack 4
dongle 41
installing from CD 18
installing from downloadable files 21
troubleshooting 196
using 41
dongle packet file
opening and saving 188
sending to support 192, 194

E
e-mail
send 82
setup 83
Encrypted Files 254
Encryption Standards 257

F
Forensic Toolkit 3

G
Golden Dictionary 150, 256
permutation 256

Password Recovery
AOL Communicator Account 170
AOL Instant Messenger 170
AOL Sign-On 171
copying to the clipboard 175
drag and drop 77, 78
drives 78
files 76
folders 78
Internet Explorer Content Advisor 168
MSN Messenger Login 171
Netscape .W and .S Files 173
NTUSER.DAT files 168, 171, 172, 174
PWL files 165
QuickBooks 173
screen saver 168
USER.DAT files 168, 171, 172, 174
Windows login passwords 164
Windows registry 168
WinZip Archive Files 174
Yahoo! Messenger Login 173
Password Recovery Toolkit 1, 7
download 196
installation of 11, 19
starting an analysis 81
trial version 21
troubleshooting installation 196
uninstalling 34
passwords
copying 175
permutation, password 256
Preferences 81
product
updating 192
profile
creating 125
default 124
deleting 129
editing 128
managing 123
properties
jobs 85
properties bar
attributes 47
docking 50
PRTK
program files 261
PRTK Window
column headings 49
sort order 49
PWL files, password recovery 165
Q
QuickBooks, password recovery 173
R
RC4 258
recoveries
logging 84
sounds 84
specialized 163
Recovery Failed 197
recovery process
password 74
pause 80
resume 80
Recovery Reports, printing 95
Recovery Threshold 82
Registration 272
registration card 272
Registry Viewer 4
reset attack 257
results
job processing 79, 200
S
Screen Saver, password recovery 168
services 51
opening 53
start, stop, restart 54
Session
opening 79
starting 79
sounds 82
specialized recoveries 163
starting
PRTK 40
status bar 47
Subscriptions 275
SuperFast Zip Attack 197
Support 276
supported applications and formats 203
Symmetric Encryption 257
System Requirements 12

T
Technical Support 276
The PRTK Window 43
thresholds, recovery 83
Toolbar
attributes 46
docking 50
troubleshooting
installation 196
password recovery 197

U
Ultimate Toolkit 4
understanding
file decryption 255
understanding, dictionaries 149
Unicode password 177
user interface 43
user, dictionary 150
USER.DAT, password recovery 168, 171,
172, 174
user-defined level
creating 146
editing 148

W
Windows Registry, recovering passwords from
168
WinZip Archive Files, password recovery 174
WinZip SuperFast Attacks 174
WipeDrive 4

Y
Yahoo! Messenger Login, password recovery
173