

ACCESSDATA SUPPLEMENTAL APPENDIX

PRTK 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 1
- “Dictionary Attack” on page 3
- “Keyspace Attacks” on page 5
- “Multiple Attacks” on page 6

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.

Supported Application
ACT! 1-4, 2000, 5-6
Ascend
BulletProof FTP 2.3-2.45
CuteFTP 2.x, 4.x
DataPerfect
FileMaker 3.x, 5.x
ICQ 2003b-5.04
Internet Explorer 5.0-6.0 AutoComplete database

Supported Application

Lotus 1-2-3 of the following versions:

- 1A-4
- 9
- 97
- FRM
- Japanese

Lotus 1-2-3 seal passwords

Lotus Approach 2.x-3.x

Lotus Approach 97 or earlier

Lotus Organizer 1-4

Lotus Symphony 1-2

Lotus WordPro 96, 97, or Millenium

Microsoft Access

Microsoft Office Data (PST) files 2003 or earlier

Microsoft Project 98

Microsoft Schedule+ 7.x

Microsoft Visual SourceSafe 6.x

MS Backup

MS Mail

MSN Messenger 7.0 or earlier

MYOB Plus 3.x

Netscape Mail 6.x or earlier

Outlook Express 5.0-6.0, SMTP password

Palm Pilot user file

Paradox 4.x, 5.x, or 7.x

ProWrite

Quattro Pro 1-12

Symantec QA 4.x-5.x

VersaCheck 2001 Home and Business and Professional Editions

Supported Application

Whisper 32 1.16 or earlier

Windows 95 Screen Saver

Windows XP Credential Files in Windows XP Service Pack 2 or earlier

WordPerfect 5.0-12

WS_FTP

Yahoo! Messenger 6.0 or earlier

Yayoi Kaikei 05 or earlier

DICTIONARY ATTACK

The dictionary attack uses the words in a dictionary, applies levels to the words, and converts the possible words into keys. PRTK uses the dictionary attack on the applications listed in the following table.

Supported Application

ABICoder 3.5.7-3.6.1

Adobe Acrobat 3.0-6.0 and Adobe PDF 1.2-1.6

AOL Instant Messenger 5.9 or earlier

Ami Pro

BestCrypt 4.x-7.12

CDLock 5.08

CheckWriter 5.x

Encrypted Magic Folders 3.x

CodedDrag 2.4

CrypText 2.30-3.40

DriveCrypt Plus Pack 3.0

GnuPG 1.4.0 or earlier

htpasswd

Internet Explorer Content Advisor

Invisible Secrets 4.3

Supported Application

Justsystem Ichitaro 5-2004

Justsystem Hanako 3.1-2004

KeePass 0.8-1.03

Kremlin Encrypt 3.0

Kremlin Text 3.0

MaxCrypt 1.0-1.09

Microsoft Encrypted File System (EFS), Windows 2000-XP Support Pack 2

Norton Secret Stuff 1.0

Omziff 1.0

OpenOffice.org 1.1.x or earlier

passwd, MD5- and SHA-based encryption and fcrypt

PasswordSafe 1-2.x

PC-Encrypt 9.11 or earlier

PFX (Windows XP/2000)

PGP 8.1 or earlier

PGP Disk 4.0 or 6.0

PGP SDA

PKZIP

RAR 1.x-3.x

SafeHouse 2.00-2.10

SAM files, NT (MD4) hash

S-Tools 4.0

WinZip 9.x

KEYSPACE ATTACKS

The keyspaces attack is used on applications that use 32-bit encryption or less. Because of the relatively small number of possible keys, PRTK tries every possible key until it finds the one that decrypts the file.

PRTK performs keyspaces attacks for the three following applications:

- AOL 8.0-9.0 Security Edition: PRTK uses a keyspaces attack to recover the sign-on password if you do not enter a volume serial number when adding the file to PRTK.

If you enter a volume serial number, PRTK performs a decryption attack.

- ARJ: PRTK first uses a statistical attack, a non-standard keyspaces attack, to recover the key. If the archive file is larger than 35 KB, the statistical attack is successful approximately 80% of the time.

If the keyspaces attack isn't successful, PRTK then uses a dictionary attack with the dictionaries specified in the profile assigned to the file.

- WinZip versions 6.0 through 8.1: PRTK uses the WinZip Superfast Attack, a non-standard keyspaces attack, to recover the zip key. PRTK then uses a dictionary attack to try to recover the original password for the archive file.

Because the keyspaces attack is used in conjunction with another attack, the applications listed above are included in "Multiple Attacks" on page 6.

For files with encryption that is greater than 32-bit, PRTK performs dictionary and decryption attacks.

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 decryption attack if the file isn't decrypted during the dictionary attack.

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.

Supported Application	Attack Types
AOL 8.0-9.0 Security Edition	1. Decryption 2. Keyspace
AOL Communicator 20030919.3 or earlier	1. Dictionary 2. Decryption
ARJ 2.82 or earlier	1. Keyspace 2. Dictionary
AShampoo Security Manager 99, Ashampoo Power Encrypt, Ashampoo Privacy Protector, Ashampoo Privacy Protector 2005	1. Dictionary 2. Reset Note: A keyspace attack is possible if the CryptaPix file was encrypted with 40-bit RC4 (PC1) or the demo version of the software.
CryptaPix 2.0-2.24 and CryptaFlix 1.00-1.10	1. Dictionary 2. Keyspace
DriveCrypt 4.2	1. Dictionary 2. Reset
HandyBits EasyCrypto Deluxe 5.5	1. Dictionary 2. Decryption
Microsoft Excel 2-7, 97, 2000, XP, 2003	1. Dictionary 2. Decryption
Microsoft Money 97-2004, backup files	1. Dictionary 2. Decryption Versions of Microsoft Money before 2002 use the decryption attack. Microsoft Money 2002-04 uses the dictionary attack.

Supported Application	Attack Types
Microsoft PowerPoint XP and 2003	<ol style="list-style-type: none"> 1. Dictionary 2. Decryption
Microsoft Word 2-6, 97, 2000, XP, and 2003	<ol style="list-style-type: none"> 1. Dictionary 2. Decryption
Mozilla 1.7.x	<ol style="list-style-type: none"> 1. Dictionary 2. Decryption
Mozilla Firefox 1.0.4 or earlier	<ol style="list-style-type: none"> 1. Dictionary 2. Decryption
Netscape 7.x-8.0	<ol style="list-style-type: none"> 1. Dictionary 2. Decryption
Password Pal 2.0 or earlier	<ol style="list-style-type: none"> 1. Dictionary 2. Decryption
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 2003-2004	PRTK resets the file passwords for QuickBooks 2003-2004. To open a recovered file, open it in QuickBooks and enter a blank password when prompted.
Quicken 2004 or earlier	<ol style="list-style-type: none"> 1. Dictionary 2. Decryption 3. Reset <p>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.</p>
Steganos 7.1x-8.0.2	<ol style="list-style-type: none"> 1. Dictionary 2. Decryption <p>Note: All file types are Dictionary jobs, except for files hidden in JPGs.</p>
VBA	<ol style="list-style-type: none"> 1. Dictionary 2. Decryption 3. Reset
Windows PWL files	<ol style="list-style-type: none"> 1. Decryption 2. Dictionary
WinZip 8 or earlier	<ol style="list-style-type: none"> 1. Keyspace 2. Dictionary