



Elcomsoft Desktop Forensic Bundle

USER MANUAL

© 2021 ElcomSoft Co.Ltd.
ElcomSoft Co.Ltd.

1. About Desktop Forensic Bundle	10
2. End-User License Agreement	12
3. Password Recovery Basics	22
3.1 Password Types	23
3.2 Strong Passwords Recovery	23
3.2.1 Brute-force Attack	23
3.2.2 Mask Attack	23
3.2.3 Dictionary Attack	25
3.2.4 Dictionary Mutations	25
3.2.5 Hybrid Attack with Rules	32
4. Password Recovery Programs	35
4.3 Advanced Archive Password Recovery	36
4.3.1 Introduction	36
4.3.2 Requirements	37
4.3.3 How to work with the program	37
4.3.3.1 Passwords and encryption	37
4.3.3.2 Selecting the options	38
4.3.3.2.1 Password-encrypted file	38
4.3.3.2.2 Type of attack	38
4.3.3.2.3 Brute-force range options	39
4.3.3.2.4 Start from password	39
4.3.3.2.5 Password mask	40
4.3.3.2.6 Password length	40
4.3.3.2.7 Dictionary options	40
4.3.3.2.8 Known plaintext attack (ZIP)	42
4.3.3.2.9 Known plaintext attack (ARJ)	45
4.3.3.2.10 Guaranteed WinZip attack	45
4.3.3.2.11 Password from keys	46
4.3.3.2.12 Auto-save	47
4.3.3.2.13 Other options	47
4.3.3.2.14 Advanced options	48
4.3.3.3 Save and Read setup	48
4.3.3.3.1 Save and Read setup	48
4.3.3.4 Benchmarks	49
4.3.3.4.1 Benchmark	49
4.3.3.5 Getting the results	49
4.3.3.5.1 Recovery process	49
4.3.3.5.2 Program status	49
4.3.3.5.3 The password is...	50
4.3.4 Known bugs and limitations	51

4.3.4.1	Known bugs and limitations	51
4.3.5	Tips & tricks	51
4.3.5.1	Files with different passwords	51
4.3.5.2	What to start from	51
4.3.5.3	Command line	52
4.3.6	Acknowledgements	54
4.3.6.1	Acknowledgements	54
4.4	Advanced Intuit Password Recovery	54
4.4.1	Introduction	54
4.4.2	Program information	55
4.4.2.1	System requirements	55
4.4.2.2	Working with AINPR	55
4.4.2.3	Quicken passwords	55
4.4.2.4	QuickBooks passwords	56
4.5	Advanced Lotus Password Recovery	57
4.5.1	Introduction	57
4.5.2	System requirements	58
4.5.3	Working with ALPR	58
4.6	Advanced Mailbox Password Recovery	58
4.6.1	Introduction	58
4.6.2	System requirements	59
4.6.3	Working with AMBPR	59
4.6.3.1	User interface	59
4.6.3.2	Recovery	60
4.6.3.2.1	Search for email clients	60
4.6.3.2.2	Automatic passwords recovery	60
4.6.3.2.3	Manual passwords recovery	60
4.6.3.2.4	Mail server emulator (auto mode)	60
4.6.3.2.5	Mail server emulator (manual mode)	61
4.6.3.3	Options	61
4.6.3.4	Help	62
4.6.3.5	Exit	62
4.7	Advanced Office Password Breaker	62
4.7.1	Introduction	62
4.7.2	Requirements	63
4.7.3	About Word and Excel encryption	63
4.7.4	Files/passwords that are not supported	64
4.7.5	Working with AOPB	64
4.7.5.1	Several words before	64
4.7.5.2	Searching for encryption key	65
4.7.5.3	Decrypting the document	67
4.7.5.4	Program options	68
4.7.5.5	Rainbow attack	70
4.7.5.6	Command line interface	71

4.8	Advanced Office Password Recovery	71
4.8.1	Introduction	71
4.8.2	Getting Started with AOPR	72
4.8.2.1	System requirements	72
4.8.2.2	Supported file types and passwords	73
4.8.2.3	Supported hardware	74
4.8.2.4	Getting Help and Technical Support	75
4.8.2.4.1	Getting Help in AOPR	75
4.8.2.4.2	Contacting us	75
4.8.2.4.3	Where to get the Latest Version	75
4.8.3	Working with AOPR	75
4.8.3.1	Recovering Document Passwords	75
4.8.3.1.1	Selecting a file	75
4.8.3.1.2	Getting results	76
4.8.3.2	Working with Projects	77
4.8.3.2.1	Creating a project	77
4.8.3.2.2	Saving a project	77
4.8.3.3	Outlook E-Mail Accounts	77
4.8.3.3.1	Recovering E-Mail account passwords	77
4.8.3.3.2	Outlook Password Storage Types	78
4.8.3.4	MS Passport stored passwords	79
4.8.3.5	VBA Backdoor	79
4.8.4	Setting AOPR Options	81
4.8.4.1	Type of Attack	81
4.8.4.2	Preliminary Attack	81
4.8.4.3	Customizing the Preliminary Attack	82
4.8.4.4	General Options	83
4.8.4.4.1	Other options	83
4.8.4.5	Password Cache	83
4.8.4.5.1	About Password Cache	83
4.8.4.5.2	Managing Password Cache Files	84
4.8.5	Passwords Manual	84
4.8.5.1	Strong Passwords	85
4.8.5.1.1	Word/Excel Password to Open (Office 97/2000)	85
4.8.5.1.2	Word/Excel/PowerPoint Password to Open (Office XP/2003)	85
4.8.5.1.3	Microsoft OneNote Password to Open	86
4.8.5.1.4	Microsoft Money 2002+ Password to Open	86
4.8.5.1.5	Office 2007 and later: password to open	87
4.8.5.2	Weak Passwords	87
4.8.5.2.1	Word/Excel Password to Open (Weak Encryption)	87
4.8.5.2.2	Visual Basic for Applications (VBA)	87
4.8.5.2.3	Microsoft Access	88
4.8.5.2.3.1	Access Share-Level (Database) Password, Owner Information	88
4.8.5.2.3.2	Access User-Level Passwords	90
4.8.5.2.4	Microsoft Excel	92
4.8.5.2.4.1	Excel Document - all Passwords except the one to Open	92

4.8.5.2.4.2	Excel Add-In (XLA) Protection	93
4.8.5.2.4.3	Pocket Excel	93
4.8.5.2.5	Microsoft Word	93
4.8.5.2.5.1	Word Document - all Passwords except the one to Open	93
4.8.5.2.6	Microsoft Outlook	94
4.8.5.2.6.1	Outlook Personal Storage File Password	94
4.8.5.2.6.2	Outlook E-Mail Accounts Passwords	94
4.8.5.2.7	Microsoft PowerPoint	94
4.8.5.2.8	Microsoft Money	95
4.8.5.2.9	Microsoft Project	95
4.8.6	Troubleshooting	96
4.8.6.1	Creating Debug Log	96
4.8.7	Trial Version of AOPR and Registration	96
4.8.7.1	Limitations of the Trial Version	96
4.8.7.2	Registration	96
4.9	Advanced PDF Password Recovery	97
4.9.1	Introduction	97
4.9.2	Requirements and limitations	97
4.9.3	How to work with the program	98
4.9.3.1	About PDF encryption	98
4.9.3.2	Selecting the options	100
4.9.3.2.1	Encrypted PDF file	100
4.9.3.2.2	Type of attack	101
4.9.3.2.3	Brute-force range options	101
4.9.3.2.4	Start from password	101
4.9.3.2.5	Password mask	102
4.9.3.2.6	Password length	102
4.9.3.2.7	Dictionary options	103
4.9.3.2.8	Key search	104
4.9.3.2.9	Auto-save	105
4.9.3.2.10	Other options	105
4.9.3.2.11	Advanced options	106
4.9.3.3	Save and Read setup	107
4.9.3.3.1	Save and Read setup	107
4.9.3.4	Benchmarks	107
4.9.3.4.1	Benchmark	107
4.9.3.5	Getting the results	108
4.9.3.5.1	Recovering process	108
4.9.3.5.2	Program status	108
4.9.3.5.3	The password is... ..	108
4.9.4	Tips & tricks	110
4.9.4.1	What to start from	110
4.9.4.2	Command line	110
4.9.4.3	Error messages	114
4.10	Advanced Sage Password Recovery	115

4.10.1	Introduction	115
4.10.2	Program information	116
4.10.2.1	System requirements	116
4.10.2.2	ACT! password recovery	116
4.10.2.3	PeachTree/Accounting password recovery	117
4.10.2.4	Other Sage products	118
4.11	Advanced SQL Password Recovery	118
4.11.1	Introduction	118
4.11.2	Program information	119
4.11.2.1	System requirements	119
4.11.2.2	Working with ASQLPR	119
4.12	Advanced WordPerfect Office Password Recovery	120
4.12.1	Introduction	120
4.12.2	System requirements	120
4.12.3	Working with AWOPR	120
4.13	Elcomsoft Internet Password Breaker	122
4.13.1	Introduction	122
4.13.2	Program information	123
4.13.2.1	System requirements	123
4.13.2.2	Outlook PST password	123
4.13.2.3	Internet Explorer passwords	124
4.13.2.4	Other browsers	129
4.13.2.5	Mail and news passwords	129
4.13.2.6	Password storage types	132
4.13.2.7	Options	132
4.13.2.8	Report and Password list	132
4.14	Elcomsoft Wireless Security Auditor	133
4.14.1	Introduction	133
4.14.2	Program information	134
4.14.2.1	System requirements	134
4.14.2.2	About wireless security	134
4.14.2.3	Working with EWSA	134
4.14.2.4	Capturing network packets	136
4.14.2.5	NDIS driver installation	139
4.14.2.6	Hardware acceleration	140
5.	System and Data Recovery Programs	141
5.15	Advanced EFS Data Recovery	142
5.15.1	Introduction	142
5.15.2	Working with AEFSDR	143
5.15.2.1	About EFS (Encrypting File System)	143
5.15.2.2	How AEFSDR works	146
5.15.2.3	Wizard mode	147
5.15.2.4	Scan for encryption keys	148

5.15.2.5	Scan for encrypted files	152
5.15.2.6	Browse for encrypted files	154
5.15.2.7	Decrypting files	155
5.15.2.8	Program options	155
5.15.2.9	System requirements	157
5.16	Elcomsoft Forensic Disk Decryptor	157
5.16.1	Introduction	157
5.16.2	Program information	158
5.16.2.1	System requirements	158
5.16.2.2	Working with the program	158
5.16.2.3	Extract keys	163
5.16.2.4	Decrypt or mount disk	165
5.16.2.5	TrueCrypt and VeraCrypt	168
5.17	Elcomsoft Password Digger	169
5.17.1	Introduction	169
5.17.2	Program information	170
5.17.2.1	System requirements	170
5.17.2.2	Working with the program	170
5.17.2.3	Obtaining keychain files	171
5.17.2.4	Program options	172
5.18	Elcomsoft System Recovery	173
5.18.1	Introduction	173
5.18.2	Program information	175
5.18.2.1	Requirements and limitations	175
5.18.2.2	How to create a bootable UFD	175
5.18.2.3	How to use the program	176
5.18.2.3.1	Bootting from the CD or UFD	176
5.18.2.3.2	Mass-stogare drivers	179
5.18.2.3.3	Database source and working mode	180
5.18.2.3.4	Select operating system or SAM/AD files location	183
5.18.2.3.5	Local user accounts	186
5.18.2.3.6	AD accounts	189
5.18.2.3.7	Domain cached accounts	189
5.18.2.3.8	SAM database editor	190
5.18.2.3.9	Disk tools	191
5.18.2.3.10	Unlock BitLocker drives	194
5.18.2.3.11	Miscellaneous	195
5.19	Proactive Password Auditor	196
5.19.1	Introduction	196
5.19.2	Requirements	197
5.19.3	How to work with the program	198
5.19.3.1	About Windows passwords	198
5.19.3.2	How the program works	199
5.19.3.3	Obtaining password hashes	199

5.19.3.4	Credentials	201
5.19.3.5	Password cracking	202
5.19.3.5.1	Password cracking methods	202
5.19.3.5.2	Rainbow attack	203
5.19.3.5.3	Recovery process and results	205
5.19.3.6	Reports	206
5.19.3.7	Program options	207
5.20	Proactive System Password Recovery	209
5.20.1	Introduction	209
5.20.2	System requirements	209
5.20.3	Working with PSPR	210
5.20.3.1	User interface	210
5.20.3.2	Main menu	212
5.20.3.2.1	Logon password	212
5.20.3.2.2	Cached passwords	212
5.20.3.2.3	RAS entries	213
5.20.3.2.4	Shared info	213
5.20.3.2.5	Recovered hashes	213
5.20.3.2.6	Screensaver password	214
5.20.3.2.7	Domain cached credentials	214
5.20.3.3	Advanced features	215
5.20.3.3.1	Groups and users	215
5.20.3.3.2	NT secrets	215
5.20.3.3.3	Run as	216
5.20.3.3.4	Windows CD key	216
5.20.3.3.5	Net passwords	217
5.20.3.4	Revelation	217
5.20.3.4.1	Behind asterisks	217
5.20.3.4.2	Control reviver	218
5.20.3.4.3	Registry and AD	218
5.20.3.4.4	Password reset disk	219
5.20.3.4.5	Mail/FTP server emulator	219
5.20.3.5	Misc features	220
5.20.3.5.1	Protected storage	220
5.20.3.5.2	Remote assistance	220
5.20.3.5.3	Script decoder	221
5.20.3.5.4	Remote desktop	222
5.20.3.5.5	Wireless network	222
5.20.3.6	Recover PWL	223
5.20.3.6.1	View PWL file	223
5.20.3.7	Options	223
5.20.3.7.1	General options	223
5.20.3.7.2	Attacks options	224
5.20.3.7.3	NT hash options	225

Index

227

About Desktop Forensic Bundle

1 About Desktop Forensic Bundle

All password recovery tools in a single value pack. Unlock documents, decrypt archives, break into encrypted containers with an all-in-one Desktop Forensic Bundle.

- Includes all relevant tools to break passwords to several hundred formats
- Works 25 to 250 times faster with hardware acceleration using conventional video cards for GPU acceleration+
- Distributed attacks with excellent scalability on up to 10,000 computers
- Includes all relevant password recovery tools in a single discounted package

Supports: all versions of Microsoft Office, OpenOffice, NFS Encrypted File System, Windows and macOS passwords, macOS Keychain, ZIP/RAR/RAR5, PDF, BitLocker/PGP/TrueCrypt/VeraCrypt and many more. Instantly extracts passwords from instant messengers, email clients, Web browsers and many other products. Several hundred formats supported.

End-User License Agreement

2 End-User License Agreement

END USER LICENSE AGREEMENT

NOTICE TO USER:

THIS IS AN AGREEMENT GOVERNING YOUR USE OF ELCOMSOFT SOFTWARE, FURTHER DEFINED HEREIN AS "PRODUCT," AND THE LICENSOR OF THE PRODUCT IS WILLING TO PROVIDE YOU WITH Access® TO THE PRODUCT ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT. BELOW, YOU ARE ASKED TO ACCEPT THIS AGREEMENT AND CONTINUE TO INSTALL OR, IF YOU DO NOT WISH TO ACCEPT THIS AGREEMENT, TO DECLINE THIS AGREEMENT, IN WHICH CASE YOU WILL NOT BE ABLE TO INSTALL OR OPERATE THE PRODUCT. BY INSTALLING THIS PRODUCT YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT.

This Electronic End User License Agreement (the "**Agreement**") is a legal agreement between you (either an individual or an entity), the licensee, and Elcomsoft Co. Ltd. and its affiliates (collectively, the "**Licensor**"), regarding the Licensor's software, as applicable pursuant to a valid license, you are about to download and/or other related services, including without limitation a) all of the contents of the files, disk(s), CD-ROM(s) or other media with which this Agreement is provided and including all forms of code, such as source code and object code, (the "**Software**"), b) all successor upgrades, modified versions, modified modules, revisions, patches, enhancements, fixes, modifications, copies, additions or maintenance releases of the Software, if any, licensed to you by the Licensor (collectively, the "**Updates**"), and c) related user documentation and explanatory materials or files provided in written, "online" or electronic form (the "**Documentation**" and together with the Software and Updates, the "**Product**"). You are subject to the terms and conditions of this End User License Agreement whether you Access® or obtain the Product directly from the Licensor, or through any other source. For purposes hereof, "**you**" means the individual person installing or using the Product on his or her own behalf; or, if the Product is being downloaded or installed on behalf of an organization, such as an employer, "**you**" means the organization for which the Product is downloaded or installed, then the person accepting this agreement represents hereby that such organization has authorized such person to accept this agreement on the organization's behalf. For purposes hereof the term "**organization**," without limitation, includes any partnership, limited liability company, corporation, association, joint stock company, trust, joint venture, labor organization, unincorporated organization, or governmental authority.

By accessing, storing, loading, installing, executing, displaying, copying the Product into the memory of a Client Device, as defined below, or otherwise benefiting from using the functionality of the Product ("**Operating**"), you agree to be bound by the terms and conditions of this Agreement. If you do not agree to the terms and conditions of this Agreement, the Licensor is unwilling to license the Product to you. In such event, you may not Operate or use the Product in any way.

BEFORE YOU PUT A CHECKMARK AT THE "I ACCEPT THE AGREEMENT" BUTTON AND PRESS "NEXT," PLEASE CAREFULLY READ THE TERMS AND CONDITIONS OF THIS AGREEMENT, AS SUCH ACTIONS ARE A SYMBOL OF YOUR SIGNATURE AND BY CLICKING ON THE "I ACCEPT THE AGREEMENT" AND "NEXT" BUTTONS, YOU ARE CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS AGREEMENT AND AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "CANCEL" BUTTON AND THE PRODUCT WILL NOT BE

INSTALLED ON YOUR CLIENT DEVICE, AS SUCH TERM IS DEFINED BELOW. For your reference, you may refer to the copy of this Agreement that can be found in the Help for the Software. You may also receive a copy of this Agreement by contacting Licensor at: **info@elcomsoft.com**.

1. Proprietary Rights and Non-Disclosure.

1.1. Ownership Rights. You agree that the Product and the authorship, systems, ideas, methods of operation, documentation and other information contained in the Product, are proprietary intellectual properties and or the valuable trade secrets of the Licensor and are protected by civil and criminal law, and by the law of copyright, trade secret, trademark and patent of the Russian federation, other countries and international treaties. You may use trademarks only insofar as to identify printed output produced by the Product in accordance with accepted trademark practice, including identification of trademark owner's name. Such use of any trademark does not give you any rights of ownership in that trademark. The Licensor and its suppliers own and retain all right, title, and interest in and to the Product, including without limitations any error corrections, enhancements, Updates or other modifications to the Software, whether made by Licensor or any third party, and all copyrights, patents, trade secret rights, trademarks, and other intellectual property rights therein. Your possession, installation or use of the Product does not transfer to you any title to the intellectual property in the Product, and you will not acquire any rights to the Product except as expressly set forth in this Agreement. All copies of the Product made hereunder must contain the same proprietary notices that appear on and in the Product. Except as stated herein, this Agreement does not grant you any intellectual property rights in the Product and you acknowledge that the license granted under this Agreement only provides you with a right of limited use under the terms and conditions of this Agreement.

1.2. Source Code and Modifications. You acknowledge that the source code for the Product is proprietary to the Licensor and constitutes trade secrets of the Licensor. You agree not to modify, or create derivative works based upon the Product in whole or in part nor reverse engineer, decompile, disassemble the source code of the Product in any way.

1.3. Registration Code File and Confidential Information. You agree that, unless otherwise specifically provided herein or agreed by the Licensor in writing, the Product, including the specific design and structure of individual programs and the Product, including without limitation the **Registration Code** File provided to you by the Licensor and/or its authorized resellers or distributors, constitute confidential proprietary information of the Licensor. For purposes hereof, **"Registration Code"** shall mean a unique key identification file or a combination of unique electronic characters provided to you by the Licensor confirming the purchase of the license from the Licensor, which may carry the information about the license and the number of permitted users, and enabling the full functionality of the Product in accordance with the license granted under this Agreement. You agree not to transfer, copy, disclose, provide or otherwise make available such confidential information in any form to any third party without the prior written consent of the Licensor. You agree to implement reasonable security measures to protect such confidential information, but without limitation to the foregoing, shall use best efforts to maintain the security of the **Registration Code** provided to you by the Licensor and/or its authorized resellers or distributors.

2. Grant of License.

2.1. License. The Licensor grants you the following rights ("**License**") and you hereby agree and accept such License:

a). Trial Version. If you have received, downloaded and/or installed a trial version of the Product and are hereby granted an evaluation license for the Software and you may Operate the Product only for evaluation purposes and only during the single applicable evaluation period of thirty (30) days, unless otherwise indicated, from the date of the initial installation. Following this test period of thirty (30) days or less, if you wish to

continue to use the Product, you *must* register. To register you have to pay for the fully functional version. Upon payment we provide the **Registration Code** to you. Any use of the Product for other purposes or beyond the applicable evaluation period is strictly prohibited *provided however* that, subject to the restrictions contained herein, you may copy and distribute a trial version of the Software without any modifications whatsoever to any third party subject to this Agreement and further provided that you have no technical support rights during the trial period. The unregistered (trial) version may be freely distributed, provided that the distribution package is not modified. No person or company may charge a fee for the distribution of the Product without written permission from the copyright holder.

b). Grant of License. Unless otherwise specifically indicated under a valid license (e.g. volume license) granted by the Licensor, once registered you are granted a non-exclusive and non-transferable license to install one (1) copy of the Product and during the term of your license, subject to the payment of the applicable fees and your compliance with the terms hereof, this Agreement permits you or any of your employees to Operate one copy of the specified version of the Product, for internal purposes only, on one computer, workstation, or other electronic device of which the software was designed (each a **"Client Device"**). If you have purchased multiple licenses for the Product, then the number of multiple licenses shall determine the number of copies of the Product you may have and the number of Client Devices on which you may Operate the Product. If the Product is licensed as a suite or bundle with more than one specified software product, this license applies to all such specified software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such software products individually. Additionally, Licensor reserves the right to provide for specific terms and conditions in the purchased licenses and such terms may be embedded in Registration Code specifying other terms, conditions and restrictions of Operating of the Product. The Licensor reserves all rights not expressly granted herein.

c). Limitations on Personal License. With the purchase of a personal License, the Licensee may operate the Product as set forth in the Agreement for non-commercial purposes in a non-business or non-commercial environment. Use of the Product in a corporate, governmental or business environment requires the purchase of a business license.

d). Site License. With the acquisition of a Site License, the Licensee may install and use the Product on an unlimited amount of CPUs within one office in one geographic location. Within these limitations, the Licensee may install the Product as a "Network" Product and run the software from any networked computer on your LAN, provided those computers are located exclusively within one office at one geographic location.

e). Volume Use. If the Product is licensed with volume license terms specified in the applicable product invoicing or packaging for the Product, you may make use and install as many additional copies of the Product on the number of Client Devices as the volume license terms specify. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Product has been installed does not exceed the number of licenses you have obtained.

f). Multiple Environment Product; Multiple Language Product; Dual Media Product; Multiple Copies; Bundles. If the Product supports multiple platforms or languages, if you receive the Product on multiple media, if you otherwise receive multiple copies of the Product, or if you received the Product bundled with other software, the total number of your Client Devices on which all versions of the Product are installed may not exceed the number of licenses you have obtained from the Licensor. You may not rent, lease, sublicense, lend or transfer any versions or copies of the Product you do not use.

2.2. Back-up Copies. You can make one (1) copy the Product for backup and archival purposes *provided, however*, that the original and each copy is kept in your possession or

control, and that your installation and use of the Product does not exceed that which is allowed in this Section 2.

2.3. Prohibitions. You may not use, copy, emulate, clone, rent, lease, sell, modify, decompile, disassemble, otherwise reverse engineer, or transfer the licensed program, or any subset of the licensed program, except as provided for in this Agreement. Any such unauthorized use shall result in immediate and automatic termination of this license and may result in criminal and/or civil prosecution. Neither Elcomsoft binary code nor source may be used or reverse engineered to re-create the program algorithm, which is proprietary, without written permission of Licensor. All rights not expressly granted here are reserved by Elcomsoft Co. Ltd.

2.4. Special Provisions Applicable to Password Recovery Programs. The Licensor has a strict return policy due to the nature of our products. If the software is unable to recover (or remove, or change) a password, a copy of the unrecovered file *must* be sent to the Licensor for evaluation. If the password is recovered, you will be either able to keep the software and receive the password to the file (or unprotected copy of the file), or refund can be made and the end user will need to pay for the in-house recovery in order to receive the password. If the Licensor is unable to recover the password, a full refund will be made. This subsection is applicable only to situations when password recovery or removal is guaranteed without brute-force or dictionary attacks.

2.5. Registration Code. **Registration Code** provided by the Licensor constitutes the confidential proprietary information of the Licensor. Elcomsoft **Registration Code file** may not be distributed, except as stated herein, outside of the area of legal control of the person or persons who purchased the original license, without written permission of the copyright holder. You may not give away, sell or otherwise transfer your **Registration Code** to a third party. Doing so will result in an infringement of copyright. Elcomsoft Co. Ltd retains the right of claims for compensation in respect of damage which occurred by your giving away the registration code. This claim shall also extend to all costs which Elcomsoft Co. Ltd incurs in defending itself.

2.6. Transfers. Under no circumstances shall Licensee sell, rent, lease, license, sublicense, publish, display, distribute, or otherwise transfer to a third party the Software, any copy thereof, in whole or in part, without Licensor's prior written consent, unless otherwise provided for in this Agreement.

2.7. Acceptance of Licensing Terms. Installing and using the Product signifies acceptance of these terms and conditions of the License. If you do not agree with the terms of the license you must remove all Product files from your storage devices, including any back-up or archival copy, and cease to use the Product.

2.8. Material Terms and Conditions. Licensee specifically agrees that each of the terms and conditions of this Section 2 are material and that failure of Licensee to comply with these terms and conditions shall constitute sufficient cause for Licensor to immediately terminate this Agreement and the License granted under this Agreement. The presence of this Section 2.7 shall not be relevant in determining the materiality of any other provision or breach of this Agreement by either party.

2.9. Term and Termination. The term of this Agreement ("**Term**") shall begin when you download, Access® or install the Product or pay the applicable license fees (whichever is earlier) and shall continue for the term specified in your order. Without prejudice to any other rights, this Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately cease use of the Product and destroy all copies of the Product.

2.10. No Rights Upon Termination. Upon termination of this Agreement you will no longer be authorized to Operate or use the Product in any way.

3. Support and Updates.

3.1. Terms of Support. During the one-year period you are entitled to technical services and support for the Product which is provided to you by Licensor during the regular business hours (GMT+ 03:00), except for locally-observed holidays, and includes the support provided through a

special technical support section of the Licensor's site (the "**Site**") and email support@elcomsoft.com. During such period of one year e-mail support is unlimited and includes technical and support questions and patch fixes.

3.2. **Updates.** During the one-year period, you may download Updates to the Product when and as the Licensor publishes them on the Site, or through other online services. If the Product is an Update to a previous version of the Product, you must possess a valid license to such previous version in order to use the Update. You may continue to use the previous version of the Product on your Client Device after you receive the Update to assist you in the transition to the Update, provided that: (i) the Update and the previous version are installed on the same Client Device; (ii) the previous version or copies thereof are not transferred to another party or Client Device unless all copies of the Update are also transferred to such party or Client Device; (iii) you acknowledge that any modification that you made to the Product may be lost, altered, distorted or destroyed rendering such modifications, Product or the part thereof inoperable or non-usable; and (iv) you acknowledge that any obligation the Licensor may have to support the previous version of the Product may be ended upon availability of the Update. Except for the rights to free Updates during the one-year period, as further defined herein, nothing in this Agreement shall be construed as to grant you any rights or licenses with regard to the new releases of the Product or to entitle you to any new release. This Agreement does not obligate the Company to provide any Updates. Notwithstanding the foregoing, any Updates that you may receive become part of the Product and the terms of this Agreement apply to them (unless this Agreement is superseded by a succeeding agreement accompanying such Update or modified version of the Product).

4. **Restrictions.**

4.1. **No Transfer of Rights.** You may not transfer any rights pursuant to this Agreement nor rent, sublicense, lease, loan or resell the Product. You may not permit third parties to benefit from the use or functionality of the Product via a timesharing, service bureau or other arrangement, except to the extent such use is specified in the application price list, purchase order or product packaging for the Product. Except as otherwise provided in Section 1.2 hereof, you may not, without the Licensor's prior written consent, reverse engineer, decompile, disassemble or otherwise reduce any part of the Product to human readable form nor permit any third party to do so, except to the extent the foregoing restriction is expressly prohibited by applicable law. Notwithstanding the foregoing sentence, decompiling the Software is permitted to the extent the laws of your jurisdiction give you the right to do so to obtain information necessary to render the Software interoperable with other software; *provided, however,* that you must first request such information from the Licensor and the Licensor may, in its discretion, either provide such information to you (subject to confidentiality terms) or impose reasonable conditions, including a reasonable fee, on such use of the Software to ensure that the Licensor's and its affiliates' proprietary rights in the Software are protected. Except for the modification permitted under Section 1.2, you may not modify, or create derivative works based upon the Product in whole or in part.

4.2. **Proprietary Notices and Copies.** You may not remove any proprietary notices or labels on the Product. You may not copy the Product except as expressly permitted in Section 2 above.

4.3. **Compliance with Law.** You agree that in Operating the Product and in using any report or information derived as a result of Operating this Product, you will comply with all applicable international, national, state, regional and local laws and regulations, including, without limitation, privacy, trademark, patent, copyright, export control and obscenity law and you shall not use the Product for unethical or illegal business practices or in violation of any obligation to a third party in using, operating, accessing or running any of the Product and shall not knowingly assist any other person or entity to so violate any obligation to a third party.

4.4. **Additional Protection Measures.** Solely for the purpose of preventing unlicensed use of the Product, the Software may install on your Client Device technological measures that are designed to prevent unlicensed use, and the Licensor may use this technology to confirm that you

have a licensed copy of the Product. The update of these technological measures may occur through the installation of the Updates. The Updates will not install on unlicensed copies of the Product. If you are not using a licensed copy of the Product, you are not allowed to install the Updates. The Licensor will not collect any personally identifiable information from your Client Device during this process.

5. WARRANTIES AND DISCLAIMERS.

5.1. Limited Warranty. The Licensor warrants that for 90 days (the "**Warranty Period**") from the date the Registration Code is provided to you by Licensor, the media on which Product has been provided will be free from defects in materials and workmanship and that the Software will perform substantially in accordance with the Documentation or generally conform to the Product's specifications published by the Licensor. Non-substantial variations of performance from the Documentation do not establish a warranty right. THIS LIMITED WARRANTY DOES NOT APPLY TO UPDATES AS APPLIED TO ANY MODIFIED PRODUCT, WHETHER OR NOT SUCH MODIFICATION IS PERMISSIBLE HEREUNDER, TRIAL AND EVALUATION VERSIONS, UPDATES, PRE-RELEASE, TRYOUT, PRODUCT SAMPLER, OR NOT FOR RESALE (NFR) COPIES OF PRODUCT. This limited warranty is void and your support right terminate if the defect has resulted from accident, abuse, or misapplication or any modification, whether or not such modification is permitted hereunder. No warranty is made as to the integrity, protection or safekeeping of any modification to the Products made by you upon installation of any of the Updates. To make a warranty claim, you must return the Product to the location where you obtained it along with proof of purchase within such sixty (60) day period of the license fee you paid for the Product. THE LIMITED WARRANTY SET FORTH IN THIS SECTION GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE ADDITIONAL RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

5.2. Customer Remedies. The Licensor and its suppliers' entire liability and your exclusive remedy for any breach of the foregoing warranty shall be at the Licensor's option: (i) return of the purchase price paid for the license, if any, (ii) replacement of the defective media in which the Product is contained, or (iii) correction of the defects, "bugs" or errors within reasonable period of time. You must return the defective media to the Licensor at your expense with a copy of your receipt. Any replacement media will be warranted for the remainder of the original warranty period.

5.3. NO OTHER WARRANTIES. EXCEPT FOR THE FOREGOING LIMITED WARRANTY, AND FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM TO THE EXTENT TO WHICH THE SAME CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO YOU IN YOUR JURISDICTION, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY WHATSOEVER AND THE LICENSOR MAKES NO PROMISES, REPRESENTATIONS OR WARRANTIES, WHETHER EXPRESSED OR IMPLIED, WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE, REGARDING OR RELATING TO THE PRODUCT OR CONTENT THEREIN OR TO ANY OTHER MATERIAL FURNISHED OR PROVIDED TO YOU PURSUANT TO THIS AGREEMENT OR OTHERWISE. YOU ASSUME ALL RISKS AND RESPONSIBILITIES FOR SELECTION OF THE PRODUCT TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE PRODUCT. THE LICENSOR MAKES NO WARRANTY THAT THE PRODUCT WILL BE ERROR FREE OR FREE FROM INTERRUPTION OR FAILURE, OR THAT IT IS COMPATIBLE WITH ANY PARTICULAR HARDWARE OR SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, LICENSOR DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT OF THIRD PARTY RIGHTS, INTEGRATION, SATISFACTORY QUALITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH RESPECT TO THE PRODUCT AND THE ACCOMPANYING WRITTEN MATERIALS OR THE USE THEREOF. SOME JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU HEREBY ACKNOWLEDGE THAT THE PRODUCT MAY NOT BE OR BECOME AVAILABLE DUE TO ANY NUMBER OF FACTORS INCLUDING WITHOUT LIMITATION PERIODIC SYSTEM MAINTENANCE,

SCHEDULED OR UNSCHEDULED, ACTS OF GOD, TECHNICAL FAILURE OF THE SOFTWARE, TELECOMMUNICATIONS INFRASTRUCTURE, OR DELAY OR DISRUPTION ATTRIBUTABLE TO VIRUSES, DENIAL OF SERVICE ATTACKS, INCREASED OR FLUCTUATING DEMAND, AND ACTIONS AND OMISSIONS OF THIRD PARTIES. THEREFORE, THE LICENSOR EXPRESSLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY REGARDING SYSTEM AND/OR SOFTWARE AVAILABILITY, ACCESSIBILITY, OR PERFORMANCE. THE LICENSOR DISCLAIMS ANY AND ALL LIABILITY FOR THE LOSS OF DATA DURING ANY COMMUNICATIONS AND ANY LIABILITY ARISING FROM OR RELATED TO ANY FAILURE BY THE LICENSOR TO TRANSMIT ACCURATE OR COMPLETE INFORMATION TO YOU.

5.4. LIMITED LIABILITY; NO LIABILITY FOR CONSEQUENTIAL DAMAGES. YOU ASSUME THE ENTIRE COST OF ANY DAMAGE RESULTING FROM YOUR USE OF THE PRODUCT AND THE INFORMATION CONTAINED IN OR COMPILED BY THE PRODUCT, AND THE INTERACTION (OR FAILURE TO INTERACT PROPERLY) WITH ANY OTHER HARDWARE OR SOFTWARE WHETHER PROVIDED BY THE LICENSOR OR A THIRD PARTY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL THE LICENSOR OR ITS SUPPLIERS OR LICENSORS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF DATA, LOSS OF GOODWILL, WORK STOPPAGE, HARDWARE OR SOFTWARE DISRUPTION IMPAIRMENT OR FAILURE, REPAIR COSTS, TIME VALUE OR OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR THE INCOMPATIBILITY OF THE PRODUCT WITH ANY HARDWARE SOFTWARE OR USAGE, EVEN IF SUCH PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LICENSOR'S TOTAL LIABILITY TO YOU FOR ALL DAMAGES IN ANY ONE OR MORE CAUSE OF ACTION, WHETHER IN CONTRACT, TORT OR OTHERWISE EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

6. Indemnification

6.1. Indemnification for Violations. Your Operating of the Product, your accessing your account with Licensor and your entering into this Agreement constitutes your consent and agreement to defend, indemnify and hold harmless Licensor and its affiliated companies, employees, contractors, officers and directors from any claim or demand, including reasonable attorney's fees arising out of your use of the Product in violation of this Agreement.

SPECIAL PROVISION APPLICABLE TO U.S. PERSONS AND ENTITIES.

7. U.S. Government-Restricted Rights.

7.1. Notice to U.S. Government End Users. The Product and accompanying Documentation are deemed to be "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," respectively, as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights, including any use, modification, reproduction, release, performance, display or disclosure of the Product and accompanying Documentation, as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.

7.2. Export Restrictions. You acknowledge and agree that the Product may be subject to restrictions and controls imposed by the Export Administration Act and the Export Administration Regulations of the United States (the "**Acts**"). You agree and certify that neither the Product nor any direct product thereof is being or will be used for any purpose prohibited by the Acts. You

may not Operate, download, export, or re-export the Product (a) into, or to a national or resident of, any country to which the United States has embargoed goods, or (b) to anyone on the United States Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. By downloading or using the Product, you are representing and warranting that you are not located in, under the control of, or a national or resident of any such country or on any such list. You acknowledge that it is your sole responsibility to comply with any and all government export and other applicable laws and that the Licensor has no further responsibility for such after the initial license to you. You warrant and represent that neither the U.S. Commerce Department, Bureau of Export Administration nor any other U.S. federal agency has suspended, revoked or denied your export privileges.

8. Your Information and the Licensor's Privacy Policy

8.1. Privacy Policy. You acknowledge receipt of and agree to the Licensor's privacy statement which is made available to you in connection with installation and is set forth in full at <http://www.elcomsoft.com/privacy.html>. You hereby expressly consent to the Licensor's processing of your personal data (which may be collected by the Licensor or its distributors) according to the Licensor's current privacy policy as of the date of the effectiveness hereof which is incorporated into this Agreement by reference. By entering into this Agreement, you agree that the Licensor may collect and retain information about you, including your name and email address. The Licensor employs other companies and individuals to perform certain functions on its behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, processing credit card payments, and providing customer service. They have Access® only to personal information needed to perform their functions, but may not use it for other purposes. The Licensor publishes a privacy policy on its web site and may amend such policy from time to time in its sole discretion. You should refer to the Licensor's privacy policy prior to agreeing to this Agreement for a more detailed explanation of how your information will be stored and used by the Licensor. If "you" are an organization, you will ensure that each member of your organization (including employees and contractors) about whom personal data may be provided to the Licensor has given his or her express consent to the Licensor's processing of such personal data. Personal data will be processed by the Licensor or its distributors in the country where it was collected.

8.2. Public Announcements. The Licensor may identify you to the public as a customer of the Licensor and describe in a customer case study the services and solutions delivered by the Licensor to you. The Licensor may also issue one or more press releases, containing an announcement of the execution and delivery of this Agreement and/or the implementation of the Product by you. Nothing contained in this Section shall be construed as an obligation by you to disclose any of your proprietary or confidential information to any third party. In addition, you may opt-out from this Section by writing an opt-out request to the Licensor at info@elcomsoft.com.

9. Miscellaneous.

9.1. Governing Law; Jurisdiction and Venue. This Agreement shall be governed by and construed and enforced in accordance with the laws of the Russian Federation without reference to conflicts of law rules and principles. To the extent permitted by law, the provisions of this Agreement shall supersede any provisions of the Uniform Commercial Code as adopted or made applicable to the Products in any competent jurisdiction. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly disclaimed and excluded. The courts within the Russian Federation shall have exclusive jurisdiction to adjudicate any dispute arising out of this Agreement. You agree that this Agreement is to be performed in the Russian Federation and that any action, dispute, controversy, or claim that may be instituted based on this Agreement, or arising out of or related to this Agreement or any alleged breach thereof, shall be prosecuted exclusively in the federal or state courts in of the Russian Federation and you, to the extent

permitted by applicable law, hereby waive the right to change venue to any other state, county, district or jurisdiction; *provided, however,* that the Licensor as claimant shall be entitled to initiate proceedings in any court of competent jurisdiction.

9.2. Period for Bringing Actions. No action, regardless of form, arising out of the transactions under this Agreement, may be brought by either party hereto more than one (1) year after the cause of action has occurred, or was discovered to have occurred, except that an action for infringement of intellectual property rights may be brought within the maximum applicable statutory period.

9.3. Entire Agreement; Severability; No Waiver. This Agreement is the entire agreement between you and Licensor and supersedes any other prior agreements, proposals, communications or advertising, oral or written, with respect to the Product or to subject matter of this Agreement. You acknowledge that you have read this Agreement, understand it and agree to be bound by its terms. If any provision of this Agreement is found by a court of competent jurisdiction to be invalid, void, or unenforceable for any reason, in whole or in part, such provision will be more narrowly construed so that it becomes legal and enforceable, and the entire Agreement will not fail on account thereof and the balance of the Agreement will continue in full force and effect to the maximum extent permitted by law or equity while preserving, to the fullest extent possible, its original intent. No waiver of any provision or condition herein shall be valid unless in writing and signed by you and an authorized representative of Licensor provided that no waiver of any breach of any provisions of this Agreement will constitute a waiver of any prior, concurrent or subsequent breach. Licensor's failure to insist upon or enforce strict performance of any provision of this Agreement or any right shall not be construed as a waiver of any such provision or right.

9.4. Contact Information. Should you have any questions concerning this Agreement contact us at legal@elcomsoft.com.

© 1998-2020 Elcomsoft Co. Ltd. All rights reserved. The Product, including the Software and any accompanying Documentation, are copyrighted and protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

Password Recovery Basics

3 Password Recovery Basics

3.1 Password Types

From the forensic point of view there are two major password types: instant and strong. A password is considered to instant when it can be extracted from the protected entity without trying of all possible passwords. Recovering of all possible instant passwords is a first a necessary step of desktop forensic analysis. Password is called strong if it cannot be recovered instantly. In this case you have to try various attacks to recover it. It may take a lot of time and password recovery success cannot be guaranteed. In our Desktop Forensic Bundle we use all possible methods to speed-up recovery of strong passwords. We support GPU acceleration for all modern graphic adapters. We have powerful and deeply customizable mask and mutation engine. All found instant passwords can be saved as a dictionary that can be used in further recovery of strong passwords.

3.2 Strong Passwords Recovery

Enter topic text here.

3.2.1 Brute-force Attack

Brute-force attack tries all possible password combination in selected range. It consumes a lot of time and therefore this attack should be used as a last resort when all other methods did not find the password. Brute-force has two parameters: password length and character set.

Examples

"a-z, length 3" will try the following passwords:

aaa
aab
aac
...
zzz

"0-9, length 5" will try the following passwords:

00000
00001
00002
...
99999

3.2.2 Mask Attack

If we remember some part of the password, we can use Mask Attack to speed-up the password search. Mask consist of constant and variable parts. In our mask engine you can use

symbols, symbol groups and even dictionary words as variable parts of mask. Variable parts of mask always begin with "?" symbol.

Syntax

- ?? - the '?' symbol itself
- ?c - small Latin character (from 'a' to 'z')
- ?C - large Latin character (from 'A' to 'Z')
- ?\$ - one of the special characters (small set): !@#\$%^&*()-_+= and space
- ?@ - one of the special characters (large/complete set): !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~ and space
- ?# - any printable character with the code from 0x20 to 0x7F
- ?d - one digit (from 0 to 9)
- ?w[*dictionary_name*.udic] - words from dictionary
- ?d(min-max) - a number from min to max.
- ?1..9(min-max) - min..max characters from custom set, min >= 0

Examples

testmask

Only constant part. This mask will try only one word:

testmask

test?d

Constant part is "test", variable part is "?d". This mask will try the following passwords:

test0

test1

test2

...

test9

John?d(1-2)

Will try from 1 to 2 digits after constant part "John":

John0

John1

...

John9

John00

John01

...

John99

Eva?d(1970-2010)

Adds year of birth at the end of constant part "Eva":

Eva1970

Eva1971

Eva1972

...

Eva2010

John?w[last_names.udic]

Contents of last_names.udic:

Smith

Doe

Woo

This mask will try dictionary words from the dictionary last_names.udic after constant part "John":

JohnSmith

JohnDoe

JohnWoo

3.2.3 Dictionary Attack

Dictionary is a simple list of words which maybe used as passwords. Our Desktop Forensic Bundle comes with many dictionaries in various languages. We recommend to run short dictionary attack first, for example with "Top 10000 words" dictionary. Its execution is very fast and there is a high probability that password will be found in dictionary.

3.2.4 Dictionary Mutations

Every user has his own password rules. Password should be strong but easy to remember. That's why most passwords is like "John1979" or "Cindy1990". The name, the birth date and some modification like capitalizing the first letter. That's how the most passwords look. In this attack every dictionary word is tested "as is" and then some mutation rules are applied. Our engine offers many mutation rules and we can set the mutation level for each rule as well. There are three mutation levels: Minimal, Average, Maximal (MIN, AVE, MAX).

Case mutation

Changes the case of symbols.

Level	Description	Word	Result
MIN, AVE, MAX	All lowercase symbols	password	password
MIN, AVE, MAX	All uppercase symbols	password	PASSWORD

MIN, AVE, MAX	First symbol is uppercase	password	Password
MIN, AVE, MAX	All capitals except first symbol	password	pASSWORD
AVE, MAX	First and last symbols are caps	password	PassworD
MAX	Each symbol is capital	password	Password, pAssword, paSsword .. passwordD

Digit mutation

Adds leading and trailing digits to the word.

Level	Description	Word	Result
MIN, AVE, MAX	One digit at the end, all lowercase	password	password0, password1, password2 .. password9
MIN, AVE, MAX	One digit at the end, first symbol is capital	password	Password0, Password1, Password2 .. Password9
AVE, MAX	One digit at the end, all caps	password	PASSWORD0, PASSWORD1, PASSWORD2 .. PASSWORD9
AVE, MAX	One leading digit, all lowercase	password	0password, 1password, 2password .. 9password
AVE, MAX	One leading digit, first letter is capital	password	0Password, 1Password, 2Password .. 9Password
AVE, MAX	One leading digit, all caps	password	0PASSWORD, 1PASSWORD, 2PASSWORD .. 9PASSWORD
MAX	Two digits at the end, all lowercase	password	password00, password01, password02 .. password99
MAX	Two digits at the end, first symbol is capital	password	Password00, Password01, Password02 .. Password99

MAX	Two digits at the end, all caps	password	PASSWORD00, PASSWORD01, PASSWORD02 ... PASSWORD99
-----	---------------------------------	----------	--

Border mutation

Adds frequently used phrases to the word.

Level	Description	Word	Result
MIN, AVE, MAX	Frequent phrase at the end, all small	password	password123, passwordxxx, passwordqwer, password000..
MIN, AVE, MAX	Leading frequent phrase, all small	password	123password, xxxpassword, abcpassword, 000password..
AVE, MAX	Symbols as prefix and suffix, all small	password	#password#, -password-, *password* ..
AVE, MAX	Frequent phrase at the end, first one is capital	password	Password123, Passwordxxx, Passwordqwer, Password000..
AVE, MAX	Leading frequent phrase, first one is capital	password	123Password, xxxPassword, abcPassword, 000Password..
AVE, MAX	Symbols as prefix and suffix, first one is capital	password	#Password#, -Password-, *Password* ..
MAX	Frequent phrase at the end, all caps	password	PASSWORD123, PASSWORDxxx, PASSWORDqwer ...
MAX	Leading frequent phrase, all caps	password	123PASSWORD, xxxPASSWORD, abcPASSWORD ...
MAX	Symbols as prefix and suffix, all caps	password	#PASSWORD#, - PASSWORD-, *PASSWORD* ...

Freak mutation

Changes some symbols to similar ones.

Level	Description	Word	Result
MIN, AVE, MAX	All letters are replaced	password	p@\$\$w0rd
MIN, AVE, MAX	One letter is replaced	password	p@ssword, pa\$sword .. passw0rd
AVE, MAX	All letters except one are replaced	password	pa\$\$w0rd, p@s\$w0rd, p@\$\$word ..
MAX	All possible replacements, one letter is capital	password	P@\$\$w0rd, p@\$\$W0rd, p@\$\$w0rD ..

Abbreviation mutation

Shorten some words by digits.

Level	Description	Word	Result
MIN, AVE, MAX	One word is shortened (hate – h8, you – u etc), all small	ihateyou	ih8you, ihateu
MIN, AVE, MAX	All words are shortened, all small	ihateyou	ih8u
AVE, MAX	One word is shortened, first letter is capital	ihateyou	Ih8you, Ihateu
AVE, MAX	All words are shortened, first letter is capital	ihateyou	Ih8u
MAX	One word is shortened, all caps	ihateyou	IH8YOU, IHATEU
MAX	All words are shortened, all caps	ihateyou	IH8U

Order mutation

Change symbols order, duplicate or triplicate the word.

Level	Description	Word	Result
MIN, AVE, MAX	Reversed letter order, all small	password	drowssap
MIN, AVE, MAX	Word duplication, all small	password	passwordpassword

MIN, AVE, MAX	Duplication with mirroring, all small	password	passworddrowssap
MIN, AVE, MAX	Word triplication, all small	password	passwordpasswordpassword
AVE, MAX	Reversed letter order, first is capital	password	Drowssap
AVE, MAX	Word duplication, first is capital	password	PasswordPassword
AVE, MAX	Duplication with mirroring, first is capital	password	PasswordDrowssap
AVE, MAX	Word triplication, first is capital	password	PasswordPasswordPassword
MAX	Reversed letter order, all caps	password	DROWSSAP
MAX	Word duplication, all caps	password	PASSWORDPASSWORD
MAX	Duplication with mirroring, all caps	password	PASSWORDDROWSSAP
MAX	Word triplication, all caps	password	PASSWORDPASSWORDPASSWORD

Vowel mutation

Play with vowels

Level	Description	Word	Result
MIN, AVE, MAX	Remove all vowels	password	psswrđ
MIN, AVE, MAX	All consonants are uppercase	password	PaSSWoRD
MIN, AVE, MAX	All vowels are uppercase	password	pAsswOrd
AVE, MAX	Remove all vowels, first letter is capital	password	Psswrđ
MAX	Remove all vowels, all caps	password	PSSWRD

Strip mutation

Strip some characters

Level	Description	Word	Result
-------	-------------	------	--------

MIN, AVE, MAX	Remove one letter	password	assword, pssword, pasword ..
AVE, MAX	Remove one letter, first one is capital	password	assword, Pssword, Password ..
MAX	Remove one letter, all caps	password	ASSWORD, PSSWORD, PASSWORD ..

Swap mutation

Swap some characters

Level	Description	Word	Result
MIN, AVE, MAX	Change 2 letters order, all small	password	apssword, psasword, password ..
AVE, MAX	Change 2 letters order, first one is capital	password	Apssword, Psasword, Password ..
MAX	Change 2 letters order, all caps	password	APSSWORD, PSASWORD, PASSWORD ..

Duplication mutation

Duplicate characters

Level	Description	Word	Result
MIN, AVE, MAX	Duplicate one letter, all small	password	ppassword, paassword, passsword ..
MIN, AVE, MAX	Duplicate last letter many times, all small	password	passwordd, passworddd, passwordddd .. passwordddddddddd
AVE, MAX	Duplicate one letter, first one is capital	password	Ppassword, Paassword, Passsword, Passsword ..
MAX	Duplicate one letter, all caps	password	PPASSWORD, PAASSWORD, PASSSSWORD, PASSWWORD ..
MAX	Duplicate first letter many times, all small	password	ppassword, pppassword, pppassword .. ppppppppppassword

Delimiter mutation

Delimit characters by special symbols

Level	Description	Word	Result
MIN, AVE, MAX	Insert symbols between letters, all small	password	p.a.s.s.w.o.r.d, p+a+s+s+w+o+r+d, p*a*s*s*w*o*r*d ..
AVE, MAX	Insert symbols between letters, first one is capital	password	P.a.s.s.w.o.r.d, P+a+s+s+w+o+r+d, P*a*s*s*w*o*r*d ..
MAX	Insert symbols between letters, all caps	password	P.A.S.S.W.O.R.D, P+A+S+S+W+O+R+D, P*A*S*S*W*O*R*D ..

Year mutation

Adding year as prefix of suffix

Level	Description	Word	Result
MIN, AVE, MAX	Using year as a suffix, all small	password	password1990, password1991 .. password 2020
AVE, MAX	Using year as a suffix, first one is capital	password	Password1970, Password1971 .. Password 2020
MAX	Using year as a suffix, all caps	password	PASSWORD1900, PASSWORD1901 .. PASSWORD 2050

Shift mutation

Shift all symbols in the word

Level	Description	Word	Result
MIN, AVE, MAX	Shift all the letters, all small	password	asswordp, dpasswor
AVE, MAX	Shift all the letters, first one is capital	password	Asswordp, Dpasswor
AVE, MAX	Shift all the letters, first initial letter is capital	password	asswordP, dPasswor
MAX	Shift all the letters, all caps	password	ASSWORDP, DPASSWOR

Substitution mutation

Substitute characters with another ones

Level	Description	Word	Result
MIN, AVE, MAX	Replace character to another one, all small	password	oassword, [assword, lassword ..
AVE, MAX	Replace character to another one, first one is capital	password	Oassword, {assword, Lassword ..
MAX	Replace character to another one, all caps	password	OASSWORD, {ASSWORD, LASSWORD ..

Length mutation

Trim the word

Level	Description	Word	Result
MIN, AVE, MAX	Trim right, all small	password	passwor, passwo, passw ..
MIN, AVE, MAX	Trim left, all small	password	assword, ssword, sword ..
AVE, MAX	Trim right, first one is capital	password	Passwor, Passwo, Passw ..
AVE, MAX	Trim left, first one is capital	password	Assword, Ssword, Sword ..
MAX	Trim right, all caps	password	PASSWORD, PASSWO, PASSW ..
MAX	Trim left, all caps	password	ASSWORD, SSWORD, SWORD ..

3.2.5 Hybrid Attack with Rules

In some cases Dictionary Attack with Mutations cannot find password built by "creative" user. If we know some examples of another passwords belong to the same person, we can create our own mutation rules. Hybrid attack can combine up to 2 dictionaries and apply any number of mutation rules. That rules are written in simple language originally used in John the Ripper. We also have some predefined mutation rules that you can use or edit.

Setting number of characters

In hybrid attack number of characters is represented by one symbol. Digits and capital latin letters are used. Digits from 0 to 9 mean corresponding numbers: 0-9. 10 is coded by "A", 11 by "B" etc. Max value is 35 that is represented by "Z".

Hybrid attack mutations syntax

The simplest rule

: Do nothing, use the original input word

Playing with symbols case

- c** Capitalize: password -> Password
- C** Lowercase the first character, uppercase the rest:
password -> pASSWORD
- l** Convert to lowercase
- u** Convert to uppercase
- t** Toggle case of all characters: PassWord -> pASSwORD
- aN** Check all possible symbol cases for the word. N is a maximal length of the word to apply this rule for.
This rule CANNOT be used in conjunction with other ones!
- V** Vowels elite: password -> PaSSWoRD
- v** Vowels noelite: password -> pASSWoRD
- TN** Toggle case of the character at position N.

Rotate, delete, reflect

- {** Rotate left: password -> asswordp
- }** Rotate right: password -> dpasswor
- [** Delete the first character: password -> assword
-]** Delete the last character: password -> password
- DN** Delete the character at position N
- 'N** Truncate the word to N character(s) length
- f** Reflect: password -> passworddrowssap
- r** Reverse: password -> drowssap

Duplicate characters

- d** Duplicate: password -> passwordpassword
- q** Duplicate all symbols: password -> ppaasssswwoorrrd
- zN** Duplicate the first character of the word N times. N = 1 .. 9
- ZN** Duplicate the last character of the word N times. N = 1 .. 9

Reject the word

- <N** Reject the word if it is greater than N characters long.
- >N** Reject the word if it is less than N characters long.
- !X** Reject the word if it contains at least one character X
- /X** Reject the word if it does not contain character X
- (X** Reject the word if the first character is not X
-)X** Reject the word if the last character is not X

- %MX** Reject a word if it does not contain at least M instances of the character X
- =NX** Reject a word if the character at position N is not equal to the X

Insert, remove and copy

- pN** Copy word N times. N = 3 .. 9
- \$X** Add character X to the end of the word
- ^X** Insert character X at the beginning of the word
- @X** Remove all characters X from the word
- iNX** Insert the character X in position N
- oNX** Overwrite a character in position N with the character X
- sXY** Replace all characters X with Y

Substring operations

- xNM** Extract a substring of up to M characters length, starting from position N
- eX** Extract a substring starting at position 0 and ending up before first occurrence of X character. Do nothing if X is not found.
- EX** Extract a substring starting right after the first found X character and till the end of the string. Do nothing if X is not found.

Other

- SLN** Bitwise shift left character at position N
- SRN** Bitwise shift right character at position N

Examples

:c
Password

:
c
password
Password

:soaswv
csOaswv
passvard
Passvard

Password Recovery Programs

4 Password Recovery Programs

4.3 Advanced Archive Password Recovery

4.3.1 Introduction

Advanced Archive Password Recovery (ARCHPR) recovers protection passwords or unlocks encrypted ZIP and RAR archives created with all versions of popular archivers. Recover passwords for plain and self-extracting archives created with PKZip and WinZip, RAR and WinRAR automatically or with your assistance. Guaranteed unlocking of archives created with WinZip 8.0 and earlier in under one hour is possible by exploiting an implementation flaw.

ARCHPR features ultimate compatibility among the various types of archives, knows weaknesses of certain types of protection, and provides best-in-class performance in unlocking all types of archives.

Features and Benefits

- Supports all versions of ZIP/PKZip/WinZip, RAR/WinRAR, as well as ARJ/WinARJ, and ACE/WinACE (1.x)
- Guaranteed recovery of archives in under 1 hour for ZIP archives created with WinZip 8.0 and earlier and containing at least 5 files
- Supports archives over 4 GB and self-extracting archives
- Supports strong AES encryption found in WinRAR and the new versions of WinZip
- Exploits all known vulnerabilities and implementation flaws in the various compression algorithms for faster recovery
- Speedy known-plaintext attack recovers certain ZIP and ARJ archives in minutes (user must supply at least one unprotected file from that archive)
- Interrupt and resume operation at any time
- Supports background operation by utilizing idle CPU cycles only
- Dictionary and brute-force attacks with user-defined masks and advanced templates
- Highly optimized low-level code for optimum performance

Please note, however, that for the password is not stored anywhere in the archive (ZIP/RAR/ARJ/ACE file), and so it cannot be just extracted or decrypted. Instead, ARCHPR can recover it by trying different passwords: all possible combinations in a given range, or from a wordlist, etc. ARCHPR can test as many as ten to thirty million passwords per second (for ZIP archives), and so the likelihood of finding a valid one is very high. There is still no guarantee that the password will be recovered, but here the human factor plays its role: most people use short and/or easy to remember passwords. We estimate the success rate as 90-95%.

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our software or have permission from the legitimate owner to perform these acts. Any illegal use

of our software will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

You further attest that the recovered data, passwords and/or files will not be used for any illegal purpose. Be aware password recovery and the subsequential data decryption of unauthorized or otherwise illegally obtained files may constitute theft or another wrongful action and may result in your civil and (or) criminal prosecution.

4.3.2 Requirements

- Windows 7 - Windows 10
- about 6 megabytes of free space on hard disk
- about 34 megabytes of free memory for ZIP known plaintext attack
- about 260 megabytes of free memory to process RAR 2.9 and 3.x archives

4.3.3 How to work with the program

4.3.3.1 Passwords and encryption

The password encryption in ZIP/ARJ/RAR/ACE is very strong, and if the password is long enough and well selected, there is no way to recover it in a reasonable time. In most cases, only [brute-force](#) and [dictionary](#) attacks are available.

There are also some special notes about every file format.

ZIP

There are a few different encryption algorithms for ZIP archives. ARCHPR supports two of them: the traditional [PKWARE](#) encryption (used in most ZIP-compatible compression utilities; see [Application Notes - ZIP File Format Specification](#)) and [Advanced Encryption Technology](#) (used in [WinZip](#) starting from version 9.0).

For archives that use traditional encryption, ARCHPR recovery speed is about 15 million passwords per second (on Pentium 4 CPU), and so the "practical limit" for brute-force attack is about 10 characters. In addition, the "known-plaintext" attack is available: in most cases, it doesn't recover the password, but allows to get the encryption keys, and the archive can be decrypted so you will not need the password to get in. This attack usually takes 10-15 minutes (and the time does not depend on the password length). Unfortunately, it is not always applicable.

Also, due to the weakness of [WinZip](#) (versions up to 8.0) implementation of ZIP encryption algorithm, guaranteed recovery is available for many WinZip archives (with 5 or more encrypted files). As for known-plaintext attack, ARCHPR finds the decryption keys, so the password don't even needed. This attack is also very fast and takes maximum a few hours (in most cases – 15-20 minutes).

For ZIP files with advanced encryption technology, known-plaintext attack is not available, and brute-force attack works at just a few hundred passwords per second.

ARJ

ARJ encryption is simpler than ZIP one. In addition to brute-force and dictionary attacks, the [known-plaintext attack](#) is also supported; in contrary to ZIP, it allows to get the password instead of just decrypting the file). The practical limit for brute-force attack is 7-8 characters.

RAR

For RAR 2.0..2.8 archives, ARCHPR can try a few thousand passwords per second. RAR 2.9/3.x encryption is even better (see [UnRAR sources](#) for details)– recovery speed is extremely low, just a few passwords per second. So for such archives, brute-force attack is almost useless, and only dictionary attack is more or less effective.

ACE

For ACE 1.x archives, the the speed is just a few hundred passwords per second. ACE 2.x archives are not supported at all. The reason is: ACE 2.x decompression algorithm is proprietary (i.e. source code is not available); we have tried to implement password testing through unacev2.dll shipped with WinACE, but unfortunately, it contains many bugs, causing unexpected crashes – even WinACE itself crashes on some valid archives when particular password is supplied. Please don't ask us to add ACE 2.x support – we will not do that until decompression algorithm will be publically available, or at least the above mentioned DLL will be free of bugs.

4.3.3.2 Selecting the options

4.3.3.2.1 Password-encrypted file

Just enter the name of the ZIP/ARJ/RAR/ACE archive you'd like to get the password for. Use the "Browse" button (or F3 key) to select it, or press the "recent files" button (with a small down arrow) to pick from the list (if you've used ARCHPR on your target archive before). Alternatively, you can use drag'n'drop – just drag the file (with a mouse) from Windows Explorer, and drop it to the ARCHPR window. If all the settings are correct, the attack will be started immediately.

4.3.3.2.2 Type of attack

The way how ARCHPR will try to find the password for a given archive; you can select from [Brute-force](#), Mask, [Dictionary](#) and Plaintext attacks (last one – for [ZIP](#) and [ARJ](#) archives only).

Besides, [Guaranteed WinZip attack](#) is available (for WinZip 8.0 and below archives with 5 or more encrypted files), and there is also the special [Password from keys](#) attack, that could be used in addition to Brute-force and Plaintext attacks on ZIP archives (read the next chapters for details).

4.3.3.2.3 Brute-force range options

Instructs the program what characters have been used in the password. You can choose from all capital letters, all small letters, all digits, all special symbols and the space, or all printable (includes all of the above). The special characters are:

!@#\$%^&*()_+-=<>.,/?[]{}~;`|"\'

Alternatively, you can define your own character set (charset). Just mark the "User-defined" checkbox and click on "Custom charset..." (at the right of the option). In the input window, enter all chars of your password range; for example: if you remember that your password was entered in the bottom keyboard row ("zxcv...") - your password range should be "zxcvbnm,./" (or in caps: "ZXCVBNM<>?"). You can also define both of these: "zxcvbnm,./ZXCVBNM<>?". In addition, you can load and save custom charsets, or combine them using the "Add charset from file..." button.

Just a note about "Convert to OEM encoding" option in the "User Defined Charset" option. Be sure to select it if the password contains any non-English characters, and the archive has been created by a DOS-based compression utility (like PKZIP, for example). Otherwise, the password will not be found.

4.3.3.2.4 Start from password

This option may help, for example, if you know the first character(s) of the password. For example, if you're sure that the small letters have been used (from 'a' to 'z'), the length is 5, and the password definitely starts with 'k', than type 'kaaaa' here. Please also note, that if you press the "Stop" button when ARCHPR is working, the program writes the current password to this window ("Start from password"). It can be used later to restart the program from the same point.

Please note that the program verifies the passwords according to the following character order:

- CAPITAL letters: 'A'..'Z'
- the space
- small letters: 'a'..'z')
- digits: '0'..'9'
- special characters: !@#\$%^&*()_+-=<>.,/?[]{}~;`|"\'

You can also use End at field to set the password ARCHPR should stop at. It might be useful if you attack the same archive on a few computers, and so can split the whole password range onto a few parts.

4.3.3.2.5 Password mask

If you already know some characters in the password, you can specify the mask to decrease the total number of passwords to be verified. At the moment, you can set the mask only for fixed-length passwords, but doing this can still help.

For example, you know that the password contains 8 characters, starts with 'x', and ends with '99'; the other symbols are small or capital letters. So, the mask to be set is "x?????99", and the charset has to be set to All caps and All small. With such options, the total number of the passwords that ARCHPR will try will be the same as if you're working with 5-character passwords which don't contain digits; it is much less than if the length were set to 8 and the All Printable option were selected. In the above example, the '?' chars indicate the unknown symbols.

If you know that the password contains an occurrence of the mask character '?', you can choose a different mask character to avoid having one character, '?', represent both an unknown pattern position and a known character. In this case, you could change the mask symbol from '?' to, for example, '#' or '*', and use a mask pattern of "x#####?" (for mask symbol '#') or "x*****?" (for mask symbol '*'). Select the mask symbol on [Advanced Options](#) page.

4.3.3.2.6 Password length

This is one of the most important options affecting checking time. Usually, you can check all 4-character (and shorter) passwords in a few minutes; but for longer passwords, you have to have patience and/or some knowledge about the password (including the character set which has been used, or even better – the [mask](#)).

The minimum length cannot be set to a value greater than maximum length, of course.

If the minimum and maximum lengths are not the same, the program tries the shorter passwords first. For example, if you set minimum=3 and maximum=7, the program will start from 3-character passwords, then try 4-character ones and so on – up to 7. While ARCHPR is running, it shows the current password length, as well as the current password, average speed, elapsed and remaining time, and total and processed number of passwords ([Program status](#)). All of this information except average speed and elapsed time, which are global, is related only to the current length.

4.3.3.2.7 Dictionary options

Simply select the desired dictionary file. In addition, you can select an option Smart mutations or Try all possible upper/lower case combinations – it may really help if you're not sure about the register the password has been typed in. For example, let's assume that the next word in

dictionary is "PASSword" (the case, actually, doesn't matter here). With the second option enabled, the program will just try all possible combinations, like:

```
password
passworD
passwoRd
passwoRD
passwOrd
...
PASSWORDd
PASSWORD
```

However, checking all such combinations takes a lot of time: in the example above, ARCHPR will check 2^8 words (i.e. 256) instead of one. With smart mutations, you can eliminate a number of "virtually impossible" combinations, and here are all the words which will be checked:

PASSword	(as is)
passWORD	(reversed)
password	(all lower case)
PASSWORD	(all upper case)
Password	(first uppercase, rest lowercase)
pASSWORD	(first lower case, rest uppercase)
PaSSWoRD	(elite: vowels in lc, others in uc)
pAsswOrd	(noelite)
PaSsWoRd	(alt/1)
pAsSwOrD	(alt/2)

So, it makes only 10 combinations for each word.

The Start line # option allows you to start an attack from a given line (in the dictionary); if you interrupt the attack, the "current" line number will be written there (and saved to the project file, of course).

The Convert to OEM encoding option can be used if: the dictionary is in ANSI coding, but the ZIP archive has been created with a DOS archiver (like PKZIP), and so the actual password is in OEM coding. Changing that option doesn't make any difference if all the words in the dictionary contain latin letters only.

The small, but really effective dictionary is included into ARCHPR distribution: english.dic (about 240,000 words).

4.3.3.2.8 Known plaintext attack (ZIP)

Introduction

ZIP files have a strong encryption algorithm. First, the password isn't stored anywhere in a password-protected archive. The ZIP archiver converts the password you've entered into three 32-bit encryption keys, and then uses them to encrypt the whole archive. Because of this, the total complexity of the ZIP attack is 2^{96} , i.e., we would have to try all possible key combinations. This is really a lot – even using all the computers in the world, it is not possible to check all of them, unfortunately... However, this algorithm isn't as strong as the DES, RSA, IDEA, and similar algorithms. One of the ways of breaking ZIP protection is using known-plaintext attack. If you're interested in the details of attack, find the paper "A Known Plaintext Attack on the PKZIP Stream Cipher" by Eli Biham and Paul Kocher. ARCHPR's implementation of plaintext attack is very close to that paper, with some minor modifications.

Having an encrypted file created by the ZIP archiver, and the same file in unencrypted form, we can make some calculations and retrieve the encryption keys used to protect that file. Usually, a ZIP archive contains several files and all of them have the same password (and therefore the same encryption keys). This means that if we get the encryption keys for one of these files, we'll be able to unprotect all the others! Furthermore, it won't take as much time as trying all possible combinations of encryption keys. To perform plaintext attack, all you need is one file from the archive, compressed by the same archiver and by the same method as an encrypted one.

Selecting the correct archiver is a bit complex, however; unfortunately, the ZIP file format doesn't contain any data which might help to identify the archiver. In fact, you may need to try several archivers (of course, only if you don't remember which particular utility you've used). A good check that the plain file is correct is the size difference between it and the encrypted file: the encrypted file must be exactly 12 bytes larger. Also, the files must have the same CRC and uncompressed sizes. ARCHPR automatically checks these conditions for selected files, so all you need to do is to create a "plain" ZIP archive.

Description

To perform plaintext attack you need to:

- Find an unencrypted file which also exists in the password-protected archive.
- Compress it with the same method and the same ZIP archiver as used in the encrypted archive. Note that this is required because ARCHPR checks file sizes and file checksums. (You can, however, use plaintext attack on a partial file; see the description below).

- Run ARCHPR, select encrypted archive, then select "plaintext" attack and browse for archive with unencrypted file.

After that, ARCHPR will check the files, and if there are matching ones, the attack is started.

There are two stages in "plaintext" attack, plus two password search additions (note that timings are estimated for Intel Celeron working at 366 MHz):

1. **Keys reduction cycle.** At this stage, ARCHPR needs about 34 megabytes of (virtual) memory. This cycle takes from one to three minutes (depending on the size of the plaintext). If you haven't got enough physical memory, it may take a bit more time. After this stage, ARCHPR will free most of that memory and work with only 2-4 megabytes. Please also note that the time required to complete this stage cannot be estimated, and so for the first few minutes the progress indicator will read 0%, after that it'll start to increase rapidly.
2. **Searching matching keys.** This is the main stage of "plaintext" attack. Now you can see how much time you need (worst case) to recover the archive. Depending on the size of the plaintext, this stage can take from 5 minutes to several hours. At that stage, you can stop the attack at any time without risk; the program will write a resume value into the Start from field (and save it into the project file, of course). Note that the first stage (keys reduction cycle) will be performed again upon resuming (but it only takes a few minutes).

When ARCHPR finds valid keys, it tries to find the password correlated with them. Due to some reasons, the password search can be easily done for 9 characters long (and shorter) passwords with any symbols, and passwords with up to 10 printable symbols – during a couple of minutes.

If ARCHPR can retrieve the password, it'll display the standard statistics message with it, if it can't – with encryption keys only. Please note that in most cases you don't need the original password because having encryption keys you can easily decrypt the ZIP archive so it will not require the password to unzip it.

Attack on partial file

Sometimes ZIP archives (where the one is password-protected and the second isn't) may differ in size. For example, WinZip can create such ones if the source file almost cannot be compressed. Encrypted files has 12 bytes at least, so when WinZip starts the compression routine, it may select another method to keep compression ratio good. But note that it is very unusual case. However, you can perform plaintext attack on such files anyway – just keep in password-protected archive only one file (that will be attacked); of course, backup your original files first. And keep only one file in "plaintext" archive as well. Run the attack, and ARCHPR will ask for confirmation for "partial" attack. Click 'Yes' and select the number of bytes

to use as plaintext. Because we don't know how many bytes can be the same, it's good idea to start from 1-3Kb (it most cases it's enough) and decrease this number if ARCHPR won't be able to find encryption keys.

Current version notes

1. "Plaintext" file must be at least 12 bytes long.
2. "Plaintext" attack can be saved on the second stage only; after restarting, the first stage will be performed (again) anyway.
3. No time estimation for the first stage. But you can expect that it'll take a few minutes.
4. In any case, you need about 34 megabytes of RAM. If you don't have so much RAM, you need enough space on the for swap file on the disk (and patience – using virtual RAM will greatly decrease the performance). So, we recommend to use the "known plaintext" attack with at least 40-48 megabytes of RAM.

Test results

Here are the results (benchmarks) of "known plaintext" attack for the different files (on Intel Celeron 366MHz with 64MB RAM).

File size (bytes)	Stage #1 time	Stage #2 time
16	20s	2d 12h
32	33s	8h 30m
64	38s	3h 30m
128	45s	1h 45m
256	52s	42m
512	52s	20m
1024	52s	8m
2048	1m 5s	5m 30s
4096	1m 5s	4m
8192	1m 14s	4m
16384	1m 30s	4m
32768	2m 10s	4m

4.3.3.2.9 Known plaintext attack (ARJ)

ARJ files have relatively strong encryption algorithm. The password isn't stored anywhere in password protected archive. However, this algorithm isn't as strong as DES, RSA, IDEA and similar ones, and one of the ways of breaking ARJ protection is using known-plaintext attack.

Having encrypted file created by ARJ archiver, and the same file in unencrypted form, we can make some calculations and retrieve password. Usually, ARJ archive contains several files, and all of them has the same password. To perform plaintext attack, all you need is one file from archive, compressed with the same method as an encrypted one.

To perform plaintext attack you need to:

- Find unencrypted file which also exists in password-protected archive.
- Compress it with the same method as in encrypted archive. Note that this is strongly needed because ARCHPR checks file sizes and checksums of files.
- Run ARCHPR, select encrypted archive, then select "plaintext" attack and browse for archive with unencrypted file.

After that, ARCHPR will check the files, and if there are matching ones, the password will be displayed immediately.

4.3.3.2.10 Guaranteed WinZip attack

That's the most powerful attack available in ARCHPR. It works similarly to [known-plaintext attack](#) described above, but doesn't require you to have any files from the archive. However, the archive itself should have at least 5 encrypted (password-protected) files, and have to be created with [WinZip](#) or any other ZIP archiver based on Info-ZIP sources.

Please note that only WinZip versions 8.0 and below are vulnerable for this particular attack (because of using weak random number generator). In version 8.1, the hole has been fixed, and so for archives created with this version (as well as newer ones) you will not be able to use this attack at all.

Just select the archive file name, Guaranteed WinZip attack from Type of attack drop-down box, and press Run; no other options needed. If the archive has been created with some other archiver, or contains less than 5 files, ARCHPR will show an error message.

The attack consists of three stages: first two are for searching the encrypted keys (needed to decrypt the archive), and the last one searches for the actual password (up to 10 characters).

Usually, first stage takes just a few minutes (the program may show Estimated remaining time as a few hours, but actually, that's the theoretical maximum, and in most cases it is MUCH faster). Second one is from 10 to 30 minutes, and the last stage (where the password itself is being recovered) is 2-3 minutes only. For the second stage, the time estimation is also not

very accurate (to make it better, it would be needed to perform a lot of additional operations, while ARCHPR does its best to recover keys/password as fast as possible).

That attacks works in most cases (as already noted, for WinZip files only), and even if the password is very long (so it could not be found during the 3rd stage), ARCHPR will be able to decrypt the whole archive, so you will not need to supply a password to extract files from it. However, in some very rare cases (the probability is 1/256, i.e. 0,4% only), WinZip may create ZIP archives this attack fails on. ARCHPR identifies such archives and prints a warning message into the log window; actually, this message does not mean that the ARCHPR will definitely fail, but if first stage will be completed but no encryption keys found – sorry, you're out of luck. Just try the other attacks.

4.3.3.2.11 Password from keys

As noted above, Known-plaintext and [Guaranteed WinZip](#) attacks try to recover the encryption keys first. Once they're there, the archive could be decrypted so no password is needed at all. However, they also search for passwords (just in case) that are up to 10 characters long.

If you already have the encryption keys and would like to recover the [longer] password itself, select this attack from drop-down Type of attack box. The keys should be entered on Plain-text tab (if Plain-text attack just finished, they are already there), and other options such as character set (Range tab) and password length (Length tab) – as for Brute-force attack. The recommended minimum password length is 11 (as far as if you have got the keys with ARCHPR and not from any other source, shorter passwords have been already tried), the "practical" maximum value is 14-15, depending on the character set. End at value is not supported for this attack at all; as for Start from – you have to be careful. Actually, there is no need to recover first 6 characters of the password – they're calculated based on the "tail" of the password (7th char and up). So starting password should already start with 6 asterisks, and "meaningful" positions start with 7. The program starts to search for correct combinations from the end; for example, for 11-character passwords containing small letters, the order is:

```
*****aaaaa
*****baaaa
...
*****zaaaa
*****zbaaa
*****zzaaa
...
*****zzzzz
```

Please take that in mind when selecting the starting password manually.

4.3.3.2.12 Auto-save

If you'd like ARCHPR to save its state periodically, please check the appropriate option, and select the time (in minutes) between saves. If you do that, ARCHPR will create and periodically update a restore file named "~archpr.axr" (that's the default – you can change it) in the same folder where your archive is located (also by default; you can select any other folder to save that file to). This file is similar to one created when using the "Save setup" button. Even if your computer stops responding (or if power fails), you'll be able to restore breaking the password from the last saved state. Instead of using the default settings (the name of the file and the folder it will be saved to), you can also select your own settings. Enabling this option is strongly recommended.

4.3.3.2.13 Other options

Priority: background or high.

If you want to start ARCHPR as a "background" process, which will work only when the CPU is in an idle state, you may select "Background". If you want to increase performance, select "High", but be aware that this will decrease the performance of **all other** applications running on your computer.

Minimize to tray:

if this option is enabled, the program window will disappear from the Windows desktop when you press the "minimize" button in the top-right corner of the window (or you select an appropriate item in the system menu). The small icon will be created in the "tray" area of the task bar (near the system clock). Just double-click on that icon to restore the window.

Log to archpr.log:

when enabled, the program saves all information displayed in the status window into the log-file (archpr.log).

Start attack on file select:

when this option is enabled (default), the program analyses the file immediately when you open it.

Progress bar update interval:

allows to set an interval (in milliseconds) between progress bar and status window updates; the default is 500 (a reasonable value). By selecting the higher value (3000, for example), you can get slightly better recovery speed.

Language:

the program has multilingual interface. Just select the appropriate language from the drop-down box. English is the default.

4.3.3.2.14 Advanced options

Use known start of the file for stored archives (hex):

if your archive contains only one encrypted file, and this file is stored (i.e. not compressed), using that option is a solution to get much better recovery speed. But you have to know from 1 to 4 bytes this file starts from. There are a lot of well-known signatures, though: for example, 'MZ' (hex: 4D 5A) for executable files, 'PK' (hex: 50 4B 03 04) for ZIP files, D0 CF 11 E0 (hex) for OLE compound documents (like MS Word/Excel files) etc.

Always use WinZIP optimized attack engine if probability is greater than XX%:

if your archive has been created with WinZIP (or other Windows-based ZIP tool based on the same sources -- there are many such tools) and contains at least five encrypted files, there is some good news: the speed of brute-force attack can be about three times better! ARCHPR tries to recognize such a situation automatically, but unfortunately, a ZIP file doesn't store any information about the archiver. So the program calculates the "probability" value (it depends on the number of files in the archive and other factors). If it is greater than 50%, ARCHPR suggests you to use this (optimized) attack each time you start the recovery process. You can set this option (selecting the appropriate percentage as well) for your convenience, so the optimized engine will (or will not) be used automatically. 85% is the good value to use, but you can set a higher value, if you're not sure.

Mask symbol:

used for [Mask](#) attack.

Use code optimized for:

(Non-MMX processors / Intel PII/PIII/Celeron / AMD Athlon / Intel P4 SSE2 / Intel Core/Core2): force ARCHPR to use the code specially optimized for the given CPUs. The program detects your CPU and tries to select the proper code automatically, but you may want to play with that option if you've got any other CPU.

4.3.3.3 Save and Read setup

4.3.3.3.1 Save and Read setup

You can save your current ARCHPR setup into a specified file (with extension AXR). When you press the "Save setup" button (or F2 key), the "Save file" dialog appears. Just select a file name (e.g. "myarch.axr"), or select an existing AXR-file for overwriting. You can read your setup later – simply press the "Read setup" button.

Alternatively, you can use drag'n'drop – just drag the previously saved axr-file (with a mouse) from Windows Explorer, and drop it onto the ARCHPR window. If all the settings are correct, the attack will be started immediately.

4.3.3.4 Benchmarks

4.3.3.4.1 Benchmark

If you would like to estimate how long the [Brute-force](#) or [Mask](#) attack will take, or test ARCHPR's speed on a particular archive, use the benchmark feature. Just select all the desired options, then press the Benchmark button (next to Stop). The program will work for about 10 seconds, and display some statistics afterwards:

Benchmark result	
Advanced Archive Password Recovery statistics:	
Passwords to process	1 028 071 702 528
Work time	1d 15h 50m 4s 315ms
Average speed (passwords per second)	7 169 043
✓ OK	

Here you can see the total number of passwords (according to the options you set), average program speed, and estimated time. Please note that real time might be slightly different, because the speed of the program depends on how many other applications are running at the same time.

4.3.3.5 Getting the results

4.3.3.5.1 Recovery process

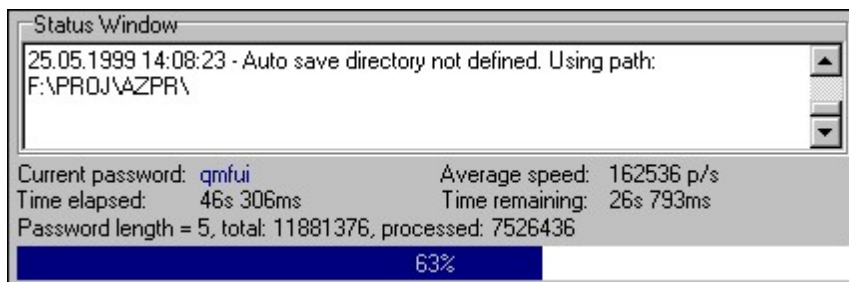
When all of the options are selected, all you have to do is press the Start button on the toolbar (or F9 key) and wait. During the attack, you'll be able to see the [Program status](#) – number of passwords already tried, elapsed and estimated time, etc.

Please note that you can stop the recovering process at any time (Stop button or F10 key), to continue it later (or just save the project). Consult the [Start from password](#) and [Save and Read setup](#) chapters for further details.

In [Known plaintext attack](#), you can stop the process at any time as well, but resuming is possible only if you do that on second stage ("searching for keys") only, but the first stage should be performed again anyway. The first stage takes a few minutes, however (in contrary to the second one, which may take 2-3 days in some cases). Note: resuming known-plaintext attack is available in registered version only.

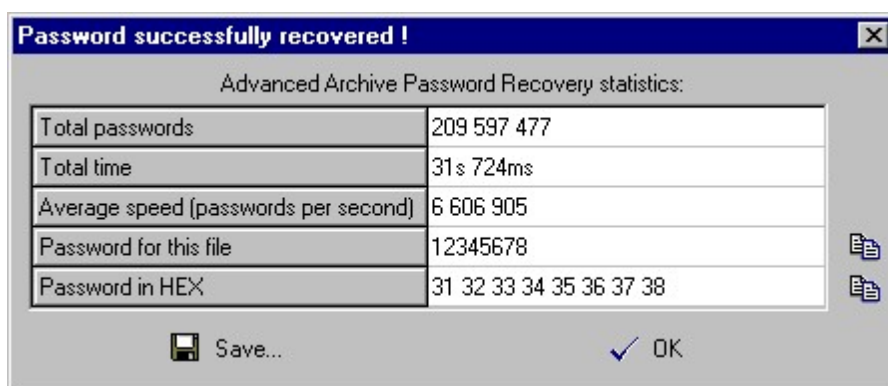
4.3.3.5.2 Program status

When the recovering process is in progress – the current password, average speed, elapsed time, remaining time, total number of password of given length, and number of passwords already processed are displayed:



4.3.3.5.3 The password is...

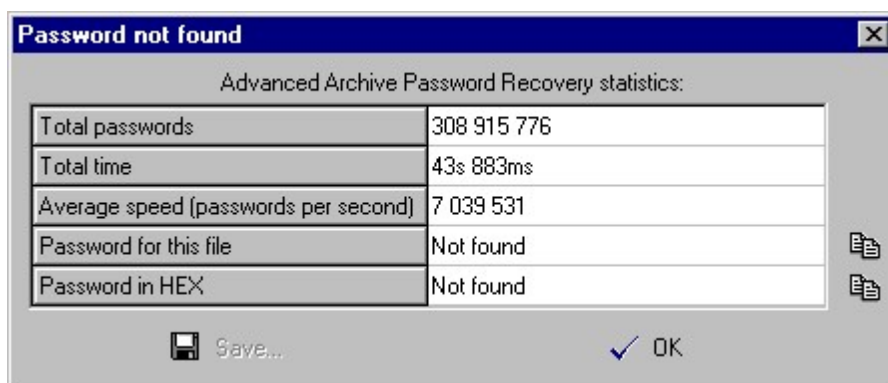
When (if) the password is found, the program shows it, as well as the number of passwords which have been tested, and the program speed:



The last line displays the password in HEX form – it might be useful if the password, for example, contains some non-English characters which cannot be displayed correctly on your system (due to missing fonts, etc.).

Pressing the small button at the right of the password (in "normal" or HEX form) copy the password into the Clipboard. Alternatively, you can save the password to a file.

If all possible passwords in the given range have been tried without success (without finding a valid one), the message looks like:



If you stopped recovery by pressing the "Stop" button, the current step of the brute-force attack is saved in the "Start from" field. Now you can press the "Start" button again. Recovery will be continued from this step.

4.3.4 Known bugs and limitations

4.3.4.1 Known bugs and limitations

- When the files in the archive are stored (without compression, only with encryption), the performance might be lower than expected (especially on large files), because decrypting the whole file is required (unless you know the first few bytes of the encrypted file).
- If the archive contains two or more encrypted files, the program assumes that all of them are encrypted with the same password (see [Files with different passwords](#) topic for a workaround).
- The program does not support ZIP archives that use dclimplode compression method (available in PKWARE Date Compression Library)
- The program does not support Strong Encryption Specification (EFS) (available in PKZip 5 and above)

4.3.5 Tips & tricks

4.3.5.1 Files with different passwords

If the files inside the ZIP archive have been encrypted with different passwords, ARCHPR might not be able to find the correct password. The workaround is to (1) make a backup copy of your archive; (2) remove all files from the archive except those which definitely have the same password (perhaps just one file); and (3) run ARCHPR on the resulting archive. When (if) ARCHPR finds the correct password, create another new archive, keeping the next portion of files which have the same password. If all the files have different passwords, you're in trouble – too much time for recovering them will be required; but that's the only thing you can do.

4.3.5.2 What to start from

If you have no idea how long the password is and what characters it may contain, just run the dictionary-based attack first. If it fails, try brute-force with the following options (character set and password length range):

Charset	Length	Passwords	Time (approx.)
All printable	1..6	742,912,032,768	14 hours
Digits, small/capital, space	7	3,938,980,724,736	3 days
Digits, small letters, space	8	3,512,479,514,624	3 days
Digits, capital letters, space	8	3,512,479,514,624	3 days

Digits	9..11	1,110,999,957,504	1 day
Small letters, space	9	7,625,596,993,536	6 days
Capital letters, space	9	7,625,596,993,536	6 days

The third column shows the total number of possible password combinations (with the given charset and password length); and the last column shows the maximum time required for recovery of the password, assuming that the speed is 15,000,000 passwords per second (the performance of a computer with Pentium 4 3GHz CPU on ZIP archives with three or more files using traditional encryption, and at least one is inflated).

For archives of other types (or ZIP archives that use AES encryption etc. – i.e. when the speed is worse), you will have to run a benchmark in advance, and find the proper options (especially the password range) experimentally.

4.3.5.3 Command line

You can run ARCHPR with command-line parameters. The syntax is:

ARCHPR [switches] [zip/arj/ace/rar-filename]

or

ARCHPR [switches] [axr-filename]

The switches are separated with / or - characters. If the switch is followed by some data (e.g., filename, starting password, etc.) which contains these characters: space, semicolon, slash or dash, it must be enclosed in (single or double) quotes.

Switch	Description	Default
/a:b m d	attack type (brute-force, mask, dictionary)	brute-force
/c:csdepa	character set (caps, small, digits, special, space, all)	caps
/u:chars	user-defined charset	
/oem	convert to OEM (for user-defined charset and dictionary attack)	disabled
/sf:pass	start from password	
/endat:pass	end at password	

/usewz:X	use optimized WinZip attack	
/useknownstart:X X	use known bytes in stored file (from 1 to 4 hex values, no spaces)	
/p[:filename]	plaintext filename	
/m:mask	mask	
/ms:C	mask symbol	?
/min:N	minimum password length	1
/max:N	maximum password length	5
/oem	convert to OEM (for user-defined charset and dictionary attack)	disabled
/useknownstart:X X	use known bytes in stored file (from 1 to 4 hex values, no spaces)	
/d[:filename]	dictionary filename	
/sm	smart mutations	disabled
/ac	try all possible upper/lower case combinations	disabled
/sl:N	start from line N	0
/autosave:N	autosave every N minutes; 0 means disabled	5
/aname:filename	autosave filename	
/adir:dir	autosave directory	
/idle	run at idle priority	enabled
/high	run at high priority	disabled
/dontstart	don't start the attack, just load/set the parameters	
/minimize	minimize the program after starting the attack	
/smartexit[:filena me]	when the attack is completed, write all statistics, including the password (if found) to the given file (default "cmdline_stats.txt"), and close the program	disabled

Examples:

archpr.exe /a:b /c:cs /min:3 /max:7 /smartexit test.zip

(brute-force attack; small and capital letters; length from 3 to 7; save and exit when done)

archpr.exe /a:b /u:12345abcde test.ace

(brute-force attack with "12345abcde" character set; length: from 1 to 5)

archpr.exe /a:m /c:d /m:june???? /sf:june1000 /high test.rar

(mask attack with ""june????" mask; charset: digits; high priority)

archpr.exe /d:english.dic /sm /oem /dontstart test.zip

(dictionary attack; dictionary: "english.dic"; smart mutations; convert words from ANSI to OEM; don't start)

archpr.exe /a:p /p:plain.arj test.arj

(known plaintext attack)

If the parameter is the axr-file, the program will immediately load all the settings from it (ignoring the other settings supplied in the command line, except /dontstart, /minimize and /smartexit), and run the attack.

4.3.6 Acknowledgements

4.3.6.1 Acknowledgements

Many people have helped make ARCHPR what it is, by making suggestions, helping test, reporting bugs, etc., but particular thanks goes to the following individuals: Irina Katalova, Alexander Katalov Jr, Dmitry Sklyarov, Alexander Volok, Marco D'Amato, John Taylor, Paolo Viappiani, Darren Parker, Richard J. Sherin. And the special thanks to Al Anway for correcting the documentation.

This product includes cryptographic software written by [Eric Young](#).

4.4 Advanced Intuit Password Recovery

4.4.1 Introduction

Advanced Intuit Password Recovery, or simply AINPR, is a program to recover passwords to files created in:

- Quicken (*.qdt, *.qdb, *.qdf)
- QuickBooks (*.qba, *.qbw).

Multilingual passwords are supported.

Actual list of supported file formats is available on the [product web page](#).

Legal notice

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our software or have permission from the legitimate owner to perform these acts. Any illegal use

of our software will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

You further attest that the recovered data, passwords and/or files will not be used for any illegal purpose. Be aware password recovery and the subsequential data decryption of unauthorized or otherwise illegally obtained files may constitute theft or another wrongful action and may result in your civil and (or) criminal prosecution.

4.4.2 Program information

4.4.2.1 System requirements

The following requirements must be met to run the program:

- Windows 7 or later
- About 50 megabytes of free space on hard disk

4.4.2.2 Working with AINPR

Simply select the file you want to recover the password for: press the "Open file..." button and browse for it. If the given file is corrupted, or used by another application, or passwords are empty – appropriate error message will be displayed. Otherwise, the program automatically recognizes the file type and works accordingly.

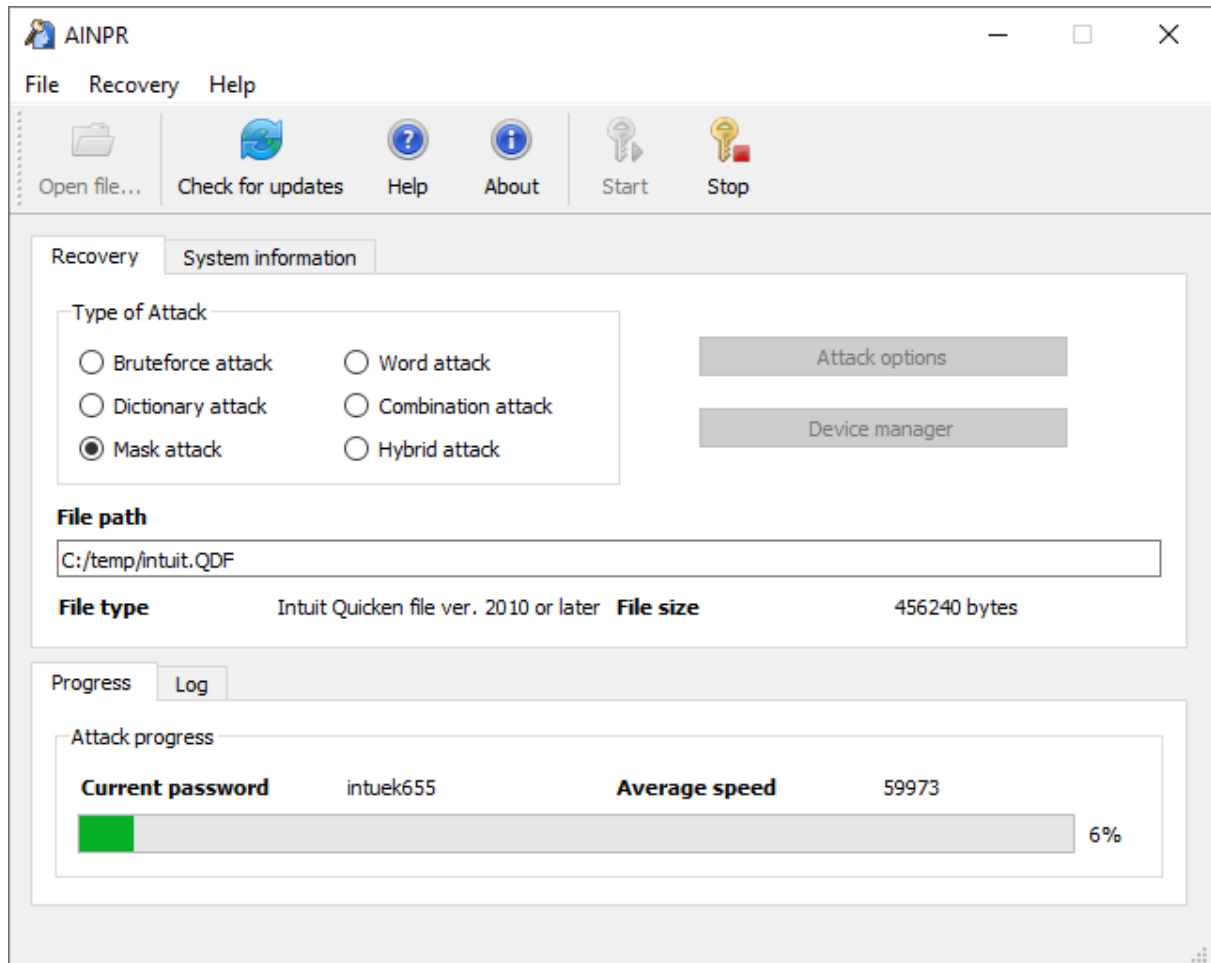
For detailed information on [Quicken](#) and [QuickBooks](#), read the next chapters.

4.4.2.3 Quicken passwords

File password

For the latest versions of Quicken (from 2006 to 2020) "file open" password cannot be found instantly. Only way to recover that password is guessing possible password combinations. This process is called "attack". The simplest attack is "Brute-force" that tries all possible passwords with given character set and length. The program also has more complicated attacks, like Dictionary with mutations or Mask. Please read [this document](#) to learn more information about attacks.

After file opening you have to select attack type and options and then press the Start button to run the attack. You also can select the devices (CPU and GPU) for password recovery using the "Device manager" button. Attack can be stopped anytime using the Stop button.



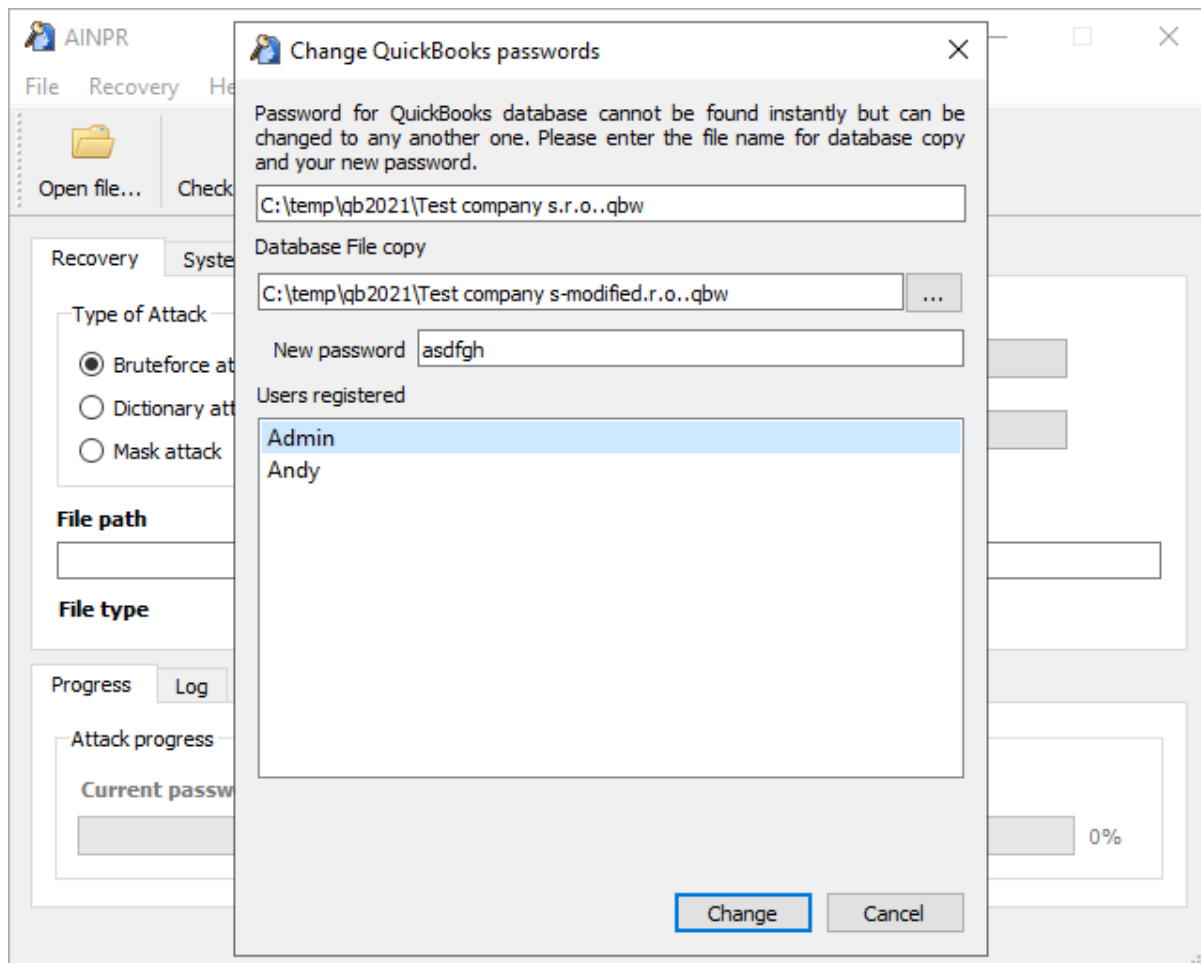
Notes

The program has been tested with all US versions of Quicken as well as some German, Canadian, Australian, New Zealand and Spanish versions. Support for those (non-US) versions is not guaranteed.

4.4.2.4 QuickBooks passwords

File open password

For the latest QuickBooks version (from 2006 to 2021) file open password cannot be recovered instantly. But you can change this password to any other one and use it to open a file. In the password change dialog you can select the new file name, its location and the new password:



By default file with the new password is saved to the same directory, with "-modified" suffix. Passwords for all QuickBooks database users are resetting to the same one, entered in the "New password" field.

4.5 Advanced Lotus Password Recovery

4.5.1 Introduction

Using Lotus SmartSuite? Forgot a password protecting documents created in Lotus Organizer, Lotus WordPro, Lotus 1-2-3, Lotus Approach or Freelance Graphics? Get instant access to password-protected Lotus documents and accounts - guaranteed!

Advanced Lotus Password Recovery allows you regain access to password-protected documents and accounts by instantly revealing passwords protecting documents created with any product and any version of Lotus SmartSuite, as well as FTP account and proxy passwords set in Lotus SmartSuite components. Recover passwords of any length and complexity from Lotus Organizer, Lotus WordPro, Lotus 1-2-3, Lotus Approach and Freelance Graphics. The simple and straightforward user interface allows easy instant recovery of the most complex passwords.

IBM/Lotus provide the ability to protect SmartSuite documents with a password without supplying the tools to recover the protected documents if a password is lost or forgotten. Advanced Lotus Password Recovery fulfills the demand of the many users of Lotus office software by providing a perfect tool to unlock password-protected Lotus documents momentarily. Passwords of any length and complexity can be revealed instantly with no lengthy attacks. Advanced Lotus Password Recovery saves your time and provides you guaranteed instant results.

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our software or have permission from the legitimate owner to perform these acts. Any illegal use of our software will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

You further attest that the recovered data, passwords and/or files will not be used for any illegal purpose. Be aware password recovery and the subsequential data decryption of unauthorized or otherwise illegally obtained files may constitute theft or another wrongful action and may result in your civil and (or) criminal prosecution.

4.5.2 System requirements

Supported operating systems: Windows XP and higher
The program requires less than 1 megabyte of free space on hard disk.

4.5.3 Working with ALPR

Simply select the file you want to recover the password(s) for. Press the Open document button and select an appropriate file; file format will be recognized automatically with corresponding message in the Status window; if the specified file format is not supported by ALPR, or it's corrupted, or used by another application, or not password-protected – appropriate error message will be displayed. Otherwise, the password will be recovered immediately and shown in the message box (and written to the log window, too); for Approach databases, the program shows a new window with the file password, and passwords to all groups – from there, you can copy them to Windows Clipboard.

To recover passwords to ftp and proxy servers (managed from any SmartSuite component and stored in the local system), press the Lotus internet passwords button on the tool bar.

4.6 Advanced Mailbox Password Recovery

4.6.1 Introduction

Advanced Mailbox Password Recovery (or simply AMBPR) is a program to login and password information (stored locally) for most popular email clients: Microsoft Internet Mail And News,

Eudora, TheBat!, TheBat! Voyager, Netscape Navigator/Communicator Mail, Pegasus mail, Calypso mail, FoxMail, Phoenix Mail, IncrediMail, @nyMail, QuickMail Pro, MailThem and MailThem Pro, Opera mail, Kaufman Mail Warrior, Becky! Internet Mail. Also includes POP3 and IMAP server emulator that allows to get POP3/IMAP password from any email client. Passwords are recovered instantly, multilingual ones are supported.

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our software or have permission from the legitimate owner to perform these acts. Any illegal use of our software will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

You further attest that the recovered data, passwords and/or files will not be used for any illegal purpose. Be aware password recovery and the subsequencial data decryption of unauthorized or otherwise illegally obtained files may constitute theft or another wrongful action and may result in your civil and (or) criminal prosecution.

4.6.2 System requirements

- Windows XP or higher
- about one megabyte of free space on hard disk

4.6.3 Working with AMBPR

4.6.3.1 User interface

The program menu is located at the left of the main screen, just like in Microsoft Outlook: contains Recovery ([automatic](#) or [manual](#)), as well as mail server emulator: also [automatic](#) and [manual](#)), [Options](#), [Help](#) and [Exit](#) button (to switch to appropriate pages).

Most interface elements (such as buttons, rows in the "list view" windows etc) have pop-up "tooltips" which gives more details about them – e.g. what action will be performed when pressing the button. "List view" elements also have context-sensitive menus appearing on right button click.

The program also supports keyboard hotkeys. Use CTRL-<digit> to select the high-level menu item, and ALT-<digit> to switch to low-level item under it:

CTRL-1: Recovery

ALT-1: [Search for email clients](#)

ALT-2: [Automatic passwords recovery](#)

ALT-3: [Manual passwords recovery](#)

ALT-4: [Mail server emulator \(auto mode\)](#)

ALT-5: [Mail server emulator \(manual mode\)](#)

CTRL-2: [Options](#)

ALT-1: Register the program

ALT-2: General options

CTRL-3: [Help](#)

ALT-1: Versions and compatibility

ALT-2: About

ALT-3: Help

CTRL-4: [Exit](#)

ALT-1: Minimize to tray

ALT-2: Exit to Windows

4.6.3.2 Recovery

4.6.3.2.1 Search for email clients

Scans your computer (hard disk and Registry) for supported email clients. The full list of clients that are supported by the current version is available on [Help](#) page. For every email client found, the program shows its full name, version and (sometimes) sender's email, name and organization. You can highlight the item you're interested in and press the right mouse button for context menu to get more information about the given client, save/print/copy it, or just refresh the list of the clients.

4.6.3.2.2 Automatic passwords recovery

Tries to recover all kind of passwords for all email clients found on your system. The program shows email client name, password type (POP3, SMTP, IMAP, account etc), mail server address (if available), login and password. Context menu (on right click) is available in that window, too.

4.6.3.2.3 Manual passwords recovery

To be used only when/if requested by our customer support department. Generally, you have to select (from drop-down box) the email client you need to get passwords for; enter the encrypted text (or browse for appropriate file); and press Decrypt.

Please note that TheBat! Voyager is support in this (manual) mode only. You have to supply the Master password in order to get account passwords decrypted.

4.6.3.2.4 Mail server emulator (auto mode)

If you have an email client that is not supported "directly" by the AMBPR, you can try the different approach: Mail server emulator.

In the best scenario, all you have to do is just press Connect button (the program emulates both POP3 and IMAP4 servers simultaneously). Now start your email client (if it was already running, you may need to restart it), and send/receive your mail there (actually, no mail will be received, because the client will connect to AMBPR instead of real mail server). Go back to AMBPR, and login and password (for POP3 or IMAP account) should be there.

There are some limitations, though. First, AMBPR should know what mail servers you connect to. It tries to retrieve the list automatically, but for some clients it may still fail to do that. So if your server is not in the list, press Add server to add it (you will be able to remove it when not needed anymore). Second, you can add servers by either name or IP address, but in the second case, emulation will work properly only if IP can be resolved to the name.

Please also note that this method works for regular authentication only; in other cases (e.g. if MD5 APOP authentication is being used) the password is not passed to the server at all, and so it cannot be captured.

By default, AMBPR uses port 110 for POP3 and port 143 for IMAP4; if your email clients has another port settings, you have to change them in AMBPR, respectively (in [Options](#)).

4.6.3.2.5 Mail server emulator (manual mode)

We'd recommend you to try [Mail server emulator \(auto mode\)](#) first – and only if it fails, use the "standard" one (as described in this topic). Here are the steps to perform:

- Select POP3 or IMAP emulation
- Click Connect button in AMBPR
- Run your email client
- Open account properties in the client
- Remember current incoming mail (POP3 or IMAP) server address
- Replace it with localhost or 127.0.0.1
- Save account properties
- Connect to the Internet (not required for some clients)
- Receive mail (in the client) for your account
- Go back to AMBPR and look at POP3 user/password there

Now go back to AMBPR and look at POP3 or IMAP user/password there. This method works for regular authentication only; in other cases (e.g. if MD5 APOP authentication is being used) the password is not passed to the server at all, and so it cannot be captured.

Unlike the automatic server emulator described above, this (manual) one works for only POP3 or IMAP4 at a time (according to the option selected), so if you're not sure, try both of them separately.

4.6.3.3 Options

Register the program: when/if you have purchased the program, enter your registration code into the input box, and press the Register button.

General options:

Language: select (from drop-down box) an appropriate language to be used for program user interface (menus, messages etc); press Refresh button to update (after changing your selection).

Print entire windows instead of text: when enabled, AMBPR will print the contents of the current window (where the Print button exists) instead of text.

Check for installed e-mail clients at startup: force AMBPR to search (on startup) your computer for [properly] installed email clients the program can recover the passwords for.

POP3 server port and IMAP server port: set port numbers for your email server; defaults are 110 and 143, respectively.

4.6.3.4 Help

Versions and compatibility: contains information of supported email clients, and particular versions AMBPR has been tested on.

About: copyright information, and links to program home page in the Internet.

Help: online help (the one you're reading now).

4.6.3.5 Exit

Minimize to tray: minimizes program to the tray on Windows toolbar (near the system clock). To restore the program to normal state, just double-click on its icon (which looks like an envelope) in the tray.

Exit to Windows: closes current session.

4.7 Advanced Office Password Breaker

4.7.1 Introduction

Break passwords and unlock documents instead of performing lengthy password recovery. Advanced Office Password Breaker (AOPB) unlocks password-protected Microsoft Word documents and Excel spreadsheets within a guaranteed timeframe instead of attacking and recovering the complex passwords.

Due to the implementation of document encryption in Microsoft Word and Microsoft Excel, a weak 40-bit encryption is still the most common method of protecting Office documents. While being strong enough to protect documents against casual curiosity, this encryption can be easily broken with modern computers and appropriate tools. Attacking the 40-bit encryption keys is not just significantly faster than trying all possible combinations of letters and numbers, but guarantees the recovery of your documents within a limited period of time.

Regain access to password-protected documents and spreadsheets by breaking and removing the password with no password-guessing involved. No matter how long and complex your password may be, Advanced Office Password Breaker unlocks your documents in a guaranteed time frame. A modern single-core PC unlocks any document in less than 5 days, while assigning additional processor cores, CPUs and computers reduces this time even further. And with Enterprise Edition, decrypting all Word documents (and most Excel files) takes several minutes only.

4.7.2 Requirements

- Windows XP or higher
- about one megabyte of free space on hard disk (8 gigabytes for Enterprise version; 8Gb USB flash drive recommended)

4.7.3 About Word and Excel encryption

Microsoft Word® and Microsoft Excel® support three levels of document/workbook protection. The user who creates a document or workbook has read/write permission to a document and controls the protection level. The three levels of document protection are:

- File open protection. Word®/Excel® requires the user to enter a password to open a document.
- File modify protection. Word®/Excel® requires the user to enter a password to open the document with read/write permission. If the user clicks Read Only at the prompt, Word®/Excel® opens the document as read-only.
- Read-only recommended protection. Word® prompts the user to open the document as read-only. If the user clicks No at the prompt, Word®/Excel® opens the document with read/write permission, unless the document has other password protection.

In addition to protecting an entire Word® document, you can also protect specific elements (tracked changes, comments and forms) from unauthorized changes. For Excel®, you can protect a worksheet and the contents of locked cells, a structure of a workbook, windows in a workbook and cells or formulas on a worksheet, or items on a chart sheet. Finally, you can prevent users from viewing code by locking VBA project.

All protections but File open one are not secure at all – the password can be either recovered or removed (changed) instantly, and not supported by AOPB at all.

If File open protection is being used, Word® and Excel® encrypt password-protected documents by using the symmetric encryption routine known as [RC4](#). In old versions of Microsoft Office (prior to Office 97 – i.e. Office 95, Office 6.0 etc), however, the implementation was weak and allowed to extract (decrypt) password as well; such files are also not supported by AOPB.

For Word® and Excel® 97/2000 files (and also Word®/Excel® XP/2003, if Office 97/2000 Compatible Encryption is used), File open protection is good enough; at least, password cannot be recovered instantly, and till now, the only methods to break them were brute-force and dictionary attacks. However, these methods fail if password is long enough and well selected (i.e. cannot be found in common dictionary) – it would take years to recover it. This is the only type of protection AOPB supports, by using a new method such as searching for encryption key instead of the password (see [next chapter](#)).

Microsoft Office XP introduces a new encryption, based on [Cryptographic Service Providers](#); for files encrypted that way, AOPB will not help as well.

So if AOPB shows a message that such files are not supported (when you try to start the attack), read the [Files/passwords that are not supported](#) chapter for details what to do.

4.7.4 Files/passwords that are not supported

AOPB does not work with Word® and Excel® file if:

- The file does not use File open protection at all, but only File modify protection, or document/workbook protection, or VBA password.
- The file has been created in Office 95 (or older)
- The file has been created in Office XP/2003, but uses any encryption other than Office 97/2000 Compatible one.
- The file has been created in Office 2007
- The file has been created on a machine with user's locale setting in Regional Settings in Control Panel is set to French (Standard). This is just because strong encryption such as RC4 is banned in France, and Office 97/2000/XP can use only old/weak encryption there.

Instead of AOPB, you should use [Advanced Office Password Recovery](#) (that supports all the types listed above, but doesn't provide 100% recovery rate for File open protection on brute-force and dictionary attacks) instead. AOPB works only with Word®/Excel® 97/2000 (and Word®/Excel® XP/2003 if default, Office 97/2000 Compatible Encryption is used) files, encrypted with password for opening.

4.7.5 Working with AOPB

4.7.5.1 Several words before

As [noted above](#), Word®/Excel® 97/2000 (and Word®/Excel® XP/2003 in Office 97/2000 Compatible mode, which is the default), encrypt files using RC4 encryption routine, if File open protection is used. The simplest way to break the password is running brute-force and dictionary attacks; however, these methods work well only on short and simple passwords only. But if, for example, the password is 10 characters long and contain both small letters,

capital letters and digits – obviously, you will not find it in any dictionary; and for brute-force attack, the appropriate software will have to try the following number of possible passwords:

$$(26 + 26 + 10) ^ 10 = 839,299,365,868,340,224$$

Even assuming that modern PCs with 4 processors can test as much as about a million passwords per second, it will still take more than 26614 years to test them all. Well, only 13307 years in average, but still too much.

This program, AOPB, does not recover the password at all. Because of [U.S. crypto export regulations](#), the key length in RC4 algorithm used for encrypting the document is only 40 bits, and that means that the total number of possible encryption keys is:

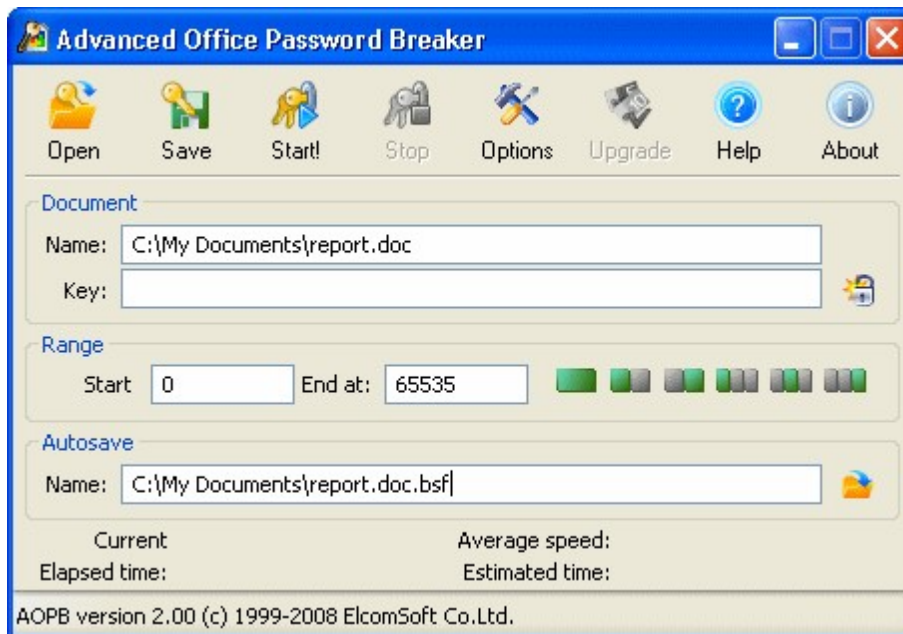
$$2 ^ 40 = 1,099,511,627,776$$

So instead of testing all possible passwords, AOPB test all possible encryption keys. And once the key is found, it decrypts the document, so the password is no longer required to open it. Decryption is still not instant, but recovery time is very reasonable (usually, a few days). Moreover, this method provides 100% success rate regardless the password length. For example, if the speed is one million passwords per second even on old Pentium 4, the program will work about 305 hours or about 13 days – and this is maximum.

For Microsoft Word files, AOPB (Enterprise Edition only) can use pre-computed hash tables, that cut the key search time to several minutes only.

4.7.5.2 Searching for encryption key

To break Word® or Excel® file that uses compatible encryption, open it in AOPB by pressing Open button on toolbar, and browsing for *.doc or *.xls file to be decrypted. The name of file will appear in the Document | Name input box. You can also use Open to load an existing project (*.bsf), which the attack has been partially completed for (to be explained later).



If you have Start the attack immediately after selecting document option enabled (see [Options](#)), this is all you have to do – the attack will be started with default parameters (sufficient for most cases), and now just wait till the key will be found (depending on the speed of your CPU, it may take from a few days and up to two weeks).

Please note that you can interrupt the attack at any time simply by pressing the Stop button. During the attack, the program saves (on a regular basis) intermediate information into the status file (with bsf extension). You can also save this file yourself at any point (using Save button on toolbar), or open previously saved file using Open button (instead of opening Word® or Excel® file here).

If Start the attack immediately after selecting document option is not checked, the parameters will be also set to default values, but you can change them prior to starting the attack. First, you can select an appropriate range. The whole key range (1,099,511,627,776 as defined above) is divided into 65,536 blocks, with 16,777,216 keys in every block. So Start from and End at fields may contain values from 0 to 65535; if you're just starting the attack, select minimum and maximum, accordingly. At the right of these fields, there are small buttons that allow selecting the whole range, or first/second half, or one third – this may help if you split the task across two or three computers. Next, you can select an alternatename for autosave file (with bsf extension).

Now press Start button on the toolbar, and the program will work till it find the encryption key or press the Stop button (you can do that at any time; the Start from field will be automatically set to the number of the current block). During the attack, the program shows some statistics – current block, average speed (in keys per second), elapsed time and estimated time.

Now you just have to be patient till the attack will complete so you will be able to [decrypt your file](#) – as already noted, it usually takes a few days (look at estimated time for more exact time) regardless the password length and complexity.

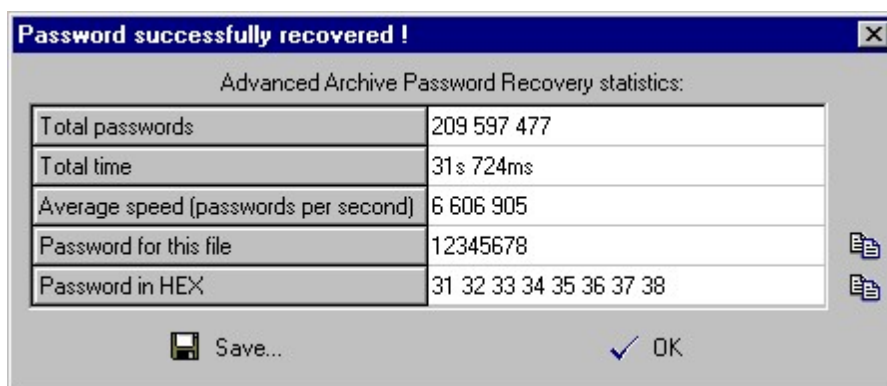
With the Enterprise version of AOPB, you can seriously speed-up this attack by enabling [Use pre-computed hash tables](#) option.

It is NOT recommended to use the tables directly from DVD (shipped with Enterprise version) because of very slow DVD drive performance. You can copy the DVD contents to the hard drive, or even better, to USB flash drive. USB flash drives have relatively low performance when reading files, but much better (than hard drive) random seek time, while this parameter is the most important for this attack.

With hash tables on hard drive, this attack takes from 10 to 30 minutes to complete; on USB flash drives – from just a few seconds and up to 10-15 minutes (worst case; usually much less: up to a minute). This option provides guaranteed recovery for Microsoft Word files, and about 97% success rate for Microsoft Excel files.

4.7.5.3 Decrypting the document

When encryption key is found, the program shows the window like:



Here we have the total number of keys tested, elapsed time, average speed in keys per second, and (the most important) the encryption key itself. You can press Save button so text file with all that information will be created (full path to the file, total keys, total time, average speed, and encryption key). Or just press the Decrypt button to save the decrypted (Word® or Excel®) file (you will be prompted for file name). That file will not have File Open protection at all, i.e. Word®/Excel® will open it without any problems.

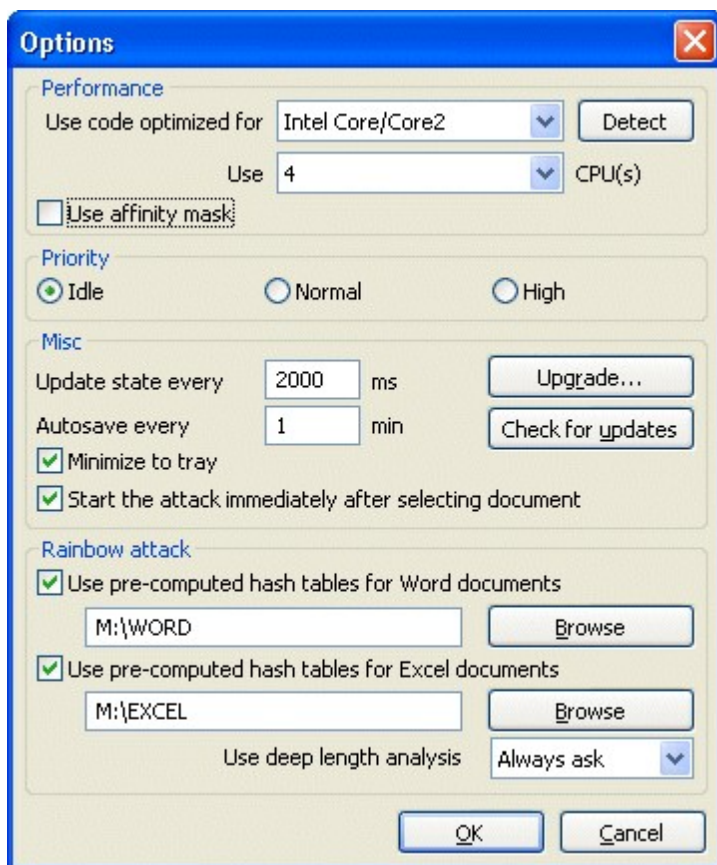
Note: if AOPB already found the encryption key for particular file but you try to start the attack once again (with any settings) on the same computer, you will be informed about that, and the program will ask you would you like to decrypt the file immediately (if yes, the same window as mentioned above will be shown), or start the attack ones again anyway (though there should not be any reason doing that, except for testing purposes). This is just because AOPB

remembers all the keys it has found by storing them in the Windows Registry on your computer. So if you have successfully completed an attack using the trial version of AOPB but have not decrypted the file due to trial version limitations, you will be able to do that just after purchasing the full version.

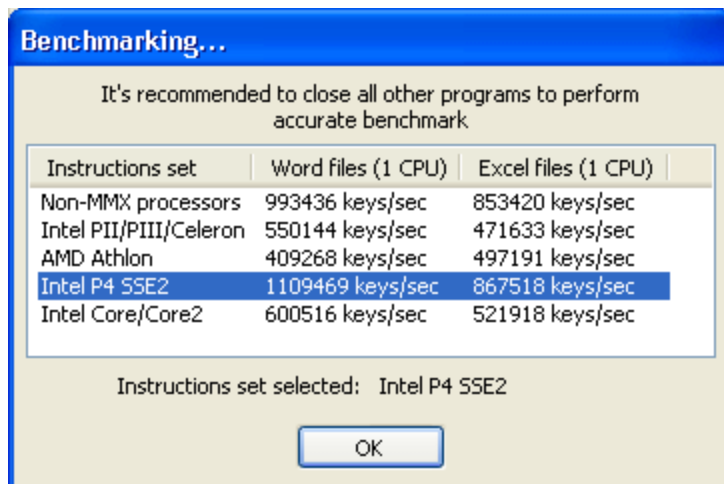
Please also note that if you have two or more documents protected with the same password, their encryption keys are different anyway, because they depend on document-specific information. That means that once the key is found, it can be used for decrypting this particular document only.

4.7.5.4 Program options

Press Options button on program toolbar to tune the program according to your needs. You will see the screen like this:



Use code optimized for (Non-MMX processors / Intel PII/PIII/Celeron / AMD Athlon / Intel P4 SSE2 / Intel Core/Core2): force AOPB to use the code specially optimized for the given CPUs. The program detects your CPU and tries to select the proper code automatically, but you may want to play with that option if you've got any other CPU: press Detect button at the right of this option to get accurate benchmark:



Use XX CPU(s): if you have more than one CPU installed in your system (one multi-core CPU such as Core2 Duo or Athlon MP), AOPB (registered Professional or Enterprise edition only) can use them all – simply select the appropriate number of CPUs from the combo box. Please note, however, that if you have Pentium 4 Northwood processor(s) with HyperThreading (HT) technology enabled, it is recommended to select the number of "physical", not "virtual" CPUs, and check the Use affinity mask option. For Pentium 4 Prescott processors, using HT still improves the performance (on 30-40%).

Priority (Idle / Normal / High): if you want to start AOPB as a "background" process, which will work only when the CPU is in an idle state, you may select Idle. If you want to increase performance, select Normal, but be aware that this will decrease the performance of all other applications running on your computer. If you select High, the program will try to use as many resources as possible (not recommended).

Auto-save every XX min: the program periodically saves all information displayed in the status window into the bsf-file (the path to that file is selected on main program screen) according to the interval selected. **Update state every XX ms:** allows to set an interval (in milliseconds) between status window updates, showing the current block number, recovery speed, elapsed time and estimated time. The default is 2000 (a reasonable value). By selecting the higher value (5000, for example), you can get slightly better recovery speed.

Minimize to tray: if this option is enabled, the program window will disappear from the Windows desktop when you press the "minimize" button in the top-right corner of the window (or you select an appropriate item in the system menu). The small icon will be created in the "tray" area of the task bar (near the system clock). Just double-click on that icon to restore the window.

Start the attack immediately after selecting document: if enabled, AOPB will start searching for document encryption key right after opening the document (if supported). Otherwise, you will have to press Start button yourself (probably after selecting the key range, changing options etc).

Use pre-computed hash tables (Enterprise version only): see [Rainbow attack](#) chapter for details.

Register: press this button to register your copy of AOPB (if you've got the registration code already, of course). If you've already registered AOPB, this button appears as Upgrade, allowing you to register the program using another code – for example, to move from Standard to Professional Edition.

Check for updates: the program connects to AOPB web site to get information about the latest version of the program available for downloading.

4.7.5.5 Rainbow attack

With the Enterprise version of AOPB, you can speed-up the decryption of all Word (and most Excel) documents by enabling Use pre-computed hash tables option. Press Browse button at the right and select the folder where the tables are located (separately for Word and Excel). For Word, the folder should contain the following subfolders/files:

0\t00_I17000.data
0\t00_I17000.index
1\t01_I17000.data
1\t01_I17000.index
2\t02_I17000.data
2\t02_I17000.index
3\t03_I17000.data
3\t03_I17000.index
4\t04_I17000.data
4\t04_I17000.index
5\t05_I17000.data
5\t05_I17000.index
missing.bin

And the list of Excel subfolders/files is:

0x62\0\t00_I12500.data
0x62\0\t00_I12500.index
0x62\1\t01_I12500.data
0x62\1\t01_I12500.index
0x62\2\t02_I12500.data
0x62\2\t02_I12500.index
0x66\0\t00_I12500.data
0x66\0\t00_I12500.index
0x66\1\t01_I12500.data
0x66\1\t01_I12500.index
0x66\2\t02_I12500.data
0x66\2\t02_I12500.index

With hash tables on hard drive, this attack takes from 10 to 30 minutes to complete; on USB flash drives or SSD – from just a few seconds and up to 10-15 minutes (worst case). This option also provides guaranteed recovery for Word files, and about 97% decryption probability for Excel files.

With Use deep length analysis option, you can control the way how Excel files are processed. The problem with Excel is: not all the files contain predictable data (needed for this method of decryption), and the program have to guess some parameters. In most cases, only one or two stages (up to several minutes each) are required to find the correct encryption keys, but there's a chance that the parameters have been selected incorrectly, and some more stages (up to two dozen) are needed, with the other parameters set; the complete process can take an hour or two. So that option instructs the program what to do if the key has not been found at the first/default stages; select Yes to always perform further attacks with the other parameters; Always ask to make the choice only when the first stages will be completed; or No otherwise.

Please note that if the key will not be found using pre-computed Excel tables, you can still decrypt the file by temporary disabling this option, and performing the full key search (which takes about three days).

4.7.5.6 Command line interface

You can execute the program with command line parameters, like:

aopb.exe [options] <filename>

Where the options are:

/minimize OR /m	Minimize the program after starting the attack
/dontstart OR /ds	Don't start the attack, just load/set the parameters from filename

The only mandatory parameter is filename. This is the name of bsf-file that stores the name of attacked Word® or Excel® file, starting block, and block to end at. To create such file, just open Word®/Excel® file in AOPB, select the block range, and press Save button on the toolbar (without starting the attack); look at [Searching for encryption key](#) for details. Or, if you already had the attack running for some time, you can use the auto-save file.

4.8 Advanced Office Password Recovery

4.8.1 Introduction

Advanced Office Password Recovery unlocks documents created with all versions of Microsoft Office from version 2.0 to Office 2019, Office 365 and Microsoft 365. The tool supports many types

of passwords protecting documents in OpenDocument and Hangul Office formats. Advanced Office Password Recovery can recover passwords for Microsoft Word, Excel, Access, Outlook, Project, Money, PowerPoint, Visio, Publisher and OneNote, all OpenOffice applications, and all applications comprising the Hangul/Hancell Office suite.

The features of the product can be divided into two major categories: instant removal of password protection and password recovery via GPU-assisted attacks.

Instant Removal of Document Protection

Certain types of document protection can be removed momentarily and without lengthy attacks. Many types of restrictions such as "password to modify", "VBA password" or "password to print" might be instantly removable.

In addition, certain types of "passwords to open" can be also removed instantly. By carefully analyzing the algorithms and implementations of password protection in different versions of Microsoft Office applications, Elcomsoft developed work-around solutions that allow recovering certain kinds of passwords instantly instead of performing lengthy attacks.

Recovers Passwords to Open

When implemented properly, a password-to-open encrypts the whole content of the document, making instant removal impossible. Advanced Office Password Recovery implements a number of highly sophisticated types of attacks including Dictionary attacks, Mask attacks, Combination and Hybrid attacks. If nothing else helps, a highly optimized, hardware-accelerated Brute-force attack can be used.

4.8.2 Getting Started with AOPR

4.8.2.1 System requirements

Advanced Office Password Recovery requires the following system configuration to run properly:

- Pentium or higher CPU
- Supported operating systems:
 - Windows® XP
 - Windows® Vista
 - Windows® 7
 - Windows® 8
 - Windows® 8.1
 - Windows® 10
 - Windows® Server 2003
 - Windows® Server 2008
 - Windows® Server 2008 R2
 - Windows® Server 2012
 - Windows® Server 2012 R2
 - Windows® Server 2016
 - Windows® Server 2019

- About 100 megabytes of free space on hard disk
- Some features may require Administrative Rights

4.8.2.2 Supported file types and passwords

Advanced Office Password Recovery has three Editions: **Home**, **Standard** and **Professional**. Here is the list of supported file types and passwords:

	AOPR Home	AOPR Standard	AOPR Professional
Microsoft® Word® (versions: 2.0, 6.0, 95, 97, 2000, XP, 2003 - 2019)			
Password to Open	Yes	Yes	Yes
Password to Modify	Yes	Yes	Yes
Document Protection Password	Yes	Yes	Yes
VBA Project Password	No	Yes	Yes
Microsoft® Excel® (versions: 3.0, 4.0, 95, 97, 2000, XP, 2003 - 2019)			
Password to Open	Yes	Yes	Yes
Password to Modify	Yes	Yes	Yes
Workbook Password	Yes	Yes	Yes
Shared Workbook Password	Yes	Yes	Yes
Sheet Passwords	Yes	Yes	Yes
VBA Project Password	No	Yes	Yes
Unlocking XLA Add-In	No	Yes	Yes
Microsoft® Access® (versions: 2.0, 95, 97, 2000, XP, 2003 - 2019)			
Password to Open	Yes	Yes	Yes
User and Group Level Passwords	No	No	Yes
Database Owner and Security ID	No	No	Yes
VBA Project Password (supported through VBA Backdoor feature only)	No	No	Yes
Microsoft® Outlook® (versions: 97, 2000, XP, 2003 - 2019)			
Password to Open (PST-Files)	No	Yes	Yes
VBA Project Password	No	Yes	Yes
E-Mail Accounts stored Passwords	No	Yes	Yes
Microsoft® PowerPoint® (versions: 4.0, 95, 97, 2000, XP, 2003 - 2019)			
Password to Open	No	No	Yes
Password to Modify	No	No	Yes
VBA Project Password	No	No	Yes
Microsoft® OneNote® (versions: 2003 with SP1 and above)			
Password to Open	No	No	Yes
Microsoft® Visio® (versions: 4.0, 5.0, 2000, 2002)			

VBA Project (in some versions supported only through VBA Backdoor)	No	No	Yes
Microsoft® Publisher			
VBA Project Password	No	No	Yes
Microsoft® Project®			
Password to Open	No	No	Yes
Password to Modify	No	No	Yes
VBA Project Password	No	No	Yes
Microsoft® Money (versions: 2.0, 3.0, 4.0, 5.0, 97, 99, 2000, 2002, 2003, 2004, 2005, 2006, 2007, 2008)			
Password to Open	No	No	Yes
Stored MS Passport Passwords	No	No	Yes
Apple iWork (versions: '09 - 2020)			
Password to open	No	Yes	Yes
All Applications with VBA			
VBA Backdoor Feature	No	No	Yes
Hangul/Hancom Office Hanword/Word (versions 2010 - 2020)			
Password to Open	No	No	Yes
Hangul/Hancom Office Hancell/Cell (versions 2010 - 2020)			
Password to Open	No	No	Yes
OpenDocument (OpenOffice, LibreOffice)			
Password to Open	No	Yes	Yes
MyOffice (МойОфис)			
Password to Open (MS Office compatible)	Yes	Yes	Yes
Password to Open (OpenDocument compatible)	No	Yes	Yes

4.8.2.3 Supported hardware

Advanced Office Password Recovery can use **CPU cores** and **graphic cards (GPUs)** to search passwords that cannot be found instantly. The number of CPUs and GPUs that can be used in password recovery process depends on the file format and program edition. Program code is optimized for Intel Core and Intel Xeon processor families.

Detailed actual information about supported GPUs can be found in our [Knowledge Base](#).

Trial version of AOPR supports all available CPUs and one GPU to demonstrate the highest password recovery speed. Registered version supports CPUs and GPUs as follows:

	Home Edition	Standard Edition	Professional Edition
Number of supported CPU cores	1	4	64

Number of supported GPUs	-	1	64
--------------------------	---	---	----

While using of GPU the performance of graphic card can significantly decrease. It may result in the delayed drawing of screen elements.

You can use the Device Manager (located on the "Options" tab) to set up the devices.

4.8.2.4 Getting Help and Technical Support

4.8.2.4.1 Getting Help in AOPR

When **AOPR** is the active window pressing the function key **F1** will give you **AOPR's** comprehensive help file. Alternatively go to the menu bar, select **"Help | Help Contents"**.

Help for particular controls:

Right-click on any control to display a **"What's This?"** menu that leads to a description of the control. This works with menu items as well. This way, if you are uncertain about a control's function or impact help is at hand.

4.8.2.4.2 Contacting us

For **Technical Support** please use the following form:
<https://support.elcomsoft.com>

Please write in **English** language only.

4.8.2.4.3 Where to get the Latest Version

You can download the latest version of **AOPR** from our Website:

<https://www.elcomsoft.com/aopr.html>

4.8.3 Working with AOPR

4.8.3.1 Recovering Document Passwords

4.8.3.1.1 Selecting a file

To select a file you want to recover the password(s) for simply press the **"Open File"** button (or select the **"File | Open File"** menu item) and browse for the appropriate file (or press on a small arrow at the right to load a file you have been working with recently).

File Format will be recognized automatically with corresponding message in the **Log Window**. If the specified File Format is not supported by **AOPR**, or it's corrupted, or used by another application – the appropriate error message will be displayed.

You can clear the Recent Files list selecting the "**File | Clear Files History**" menu item.

4.8.3.1.2 Getting results

After the File selection, the dialog box with results will be displayed automatically. The following situations may occur as the result of the File Processing:

- **All or some Passwords were recovered.** The dialog box with passwords is displayed. Password fields may contain those auxiliary messages:
 - **<none>** - the password is not set;
 - **<cannot be found instantly>** - the password cannot be recovered instantly, you must select the Attack Options and Start the Attack to recover this password. You can [Create a Project](#) to save the Attack parameters to the file.
 - **<can be changed>** - the password cannot be recovered, but can be changed or deleted. In this case a Dialog with results contains two additional buttons: "**Change Password**" and "**Delete Password**". You can change or delete the password simply clicking those buttons. Selected File must not be write-protected to complete this operation successfully.
 - **<not available>** - the Password cannot be recovered by some reason. The possible reasons are:
 - Selected File Format does not have such password
 - Password that decrypts a document is not found yet
 - **<error>** - an error occurred while Password Recovery process. The error message box is displayed to explain the error.
 - **<not supported>** - the Password is not supported by current version of AOPR.
 - **<not displayed in trial version>** - the Password was found but its length exceeds the Trial Version Limitations. You must purchase AOPR License to see that Password.

Any found Password can be copied to the **Clipboard**. Simply press the "**Copy to Clipboard**" button located at the right of the corresponding Password. You can insert the copied Password to any field by pressing the "**Ctrl-V**" buttons combination (usually the Paste menu item is disabled, but the keyboard shortcut always works). Passwords which contains international symbols can be displayed incorrectly on Windows® 95, 98 and Me. These Windows® versions don't support Unicode and therefore we recommend to use Windows® NT, 2000 or XP to recover passwords with international symbols.

Path to the selected File is displayed under "**File Path:**" caption. You can open the File simply clicking the "**Open...**" button.

- **File Format is not supported.** This may occur when you're selecting file which Format is not supported by AOPR. Please see the ["Supported File Types and Passwords"](#) section to learn what File Formats are supported by AOPR.
- **An Error occurred.** The Error message box is displayed.

Please examine the [Passwords Manual](#) to get more information about Document Passwords.

4.8.3.2 Working with Projects

4.8.3.2.1 Creating a project

If you need to recover the "open" password for a document and this password cannot be recovered instantly, you may create a **project**. Project file contains all information about the source File, selected Options and Character Set. You can simply copy the Project File to another computer and you don't need to copy the source File -- **the Project contains all information needed to recover a Password**.

When you open the file for password recovery and this Password cannot be recovered instantly, the program creates a new Project automatically. Project files have an **".AOPR"** extension. By default the Project name is equal to the source File name. For example if you're opening the "test.doc" file, the Project name is "test.opr".

4.8.3.2.2 Saving a project

When the file is loaded, you can save your project -- all the changes you've made will be reflected in the project file. The name for the project is selected automatically based on the name of the file. If you want to give an alternative name – use **"File | Save Project As..."** menu item. If you don't want to change the name, just use the **"File | Save Project"** menu item.

If a Project was created and you're trying to quit AOPR, the **Saving Project Prompt** will be displayed. You can disable this Prompt unchecking the **"Prompt if project was changed"** checkbox at the Options tab.

4.8.3.3 Outlook E-Mail Accounts

4.8.3.3.1 Recovering E-Mail account passwords

Passwords to Microsoft® Outlook® E-Mail Accounts which were stored locally can be easily recovered by clicking the **"MS Outlook®"** button or selecting the **"Internet | Outlook® Mail Accounts..."** menu item.

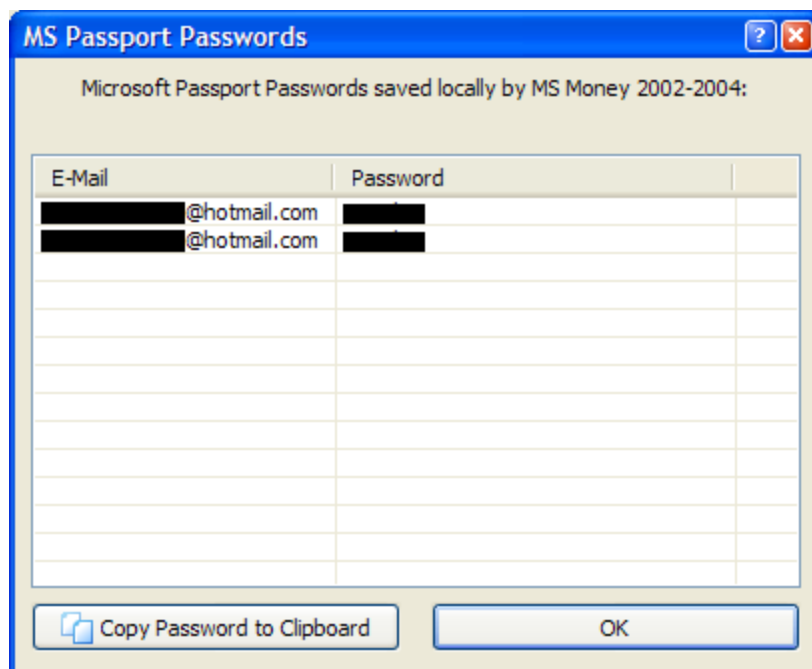
If MS Outlook® has any e-mail accounts configured the following dialog will be displayed:

NO - Password for this account is absent.

If the Storage Type is "UN", "ER" or "NR", please send your [Debug Log](#) to [Elcomsoft Technical Support](#).

4.8.3.4 MS Passport stored passwords

To recover **MS Passport** authentication passwords stored locally by **Microsoft® Money** simply click the "**MS Passport**" button. If the passwords are stored locally on the computer the following dialog is displayed:



Here you can see the user's E-Mail and Passport Password.

You can copy any found Password to the Clipboard.

4.8.3.5 VBA Backdoor

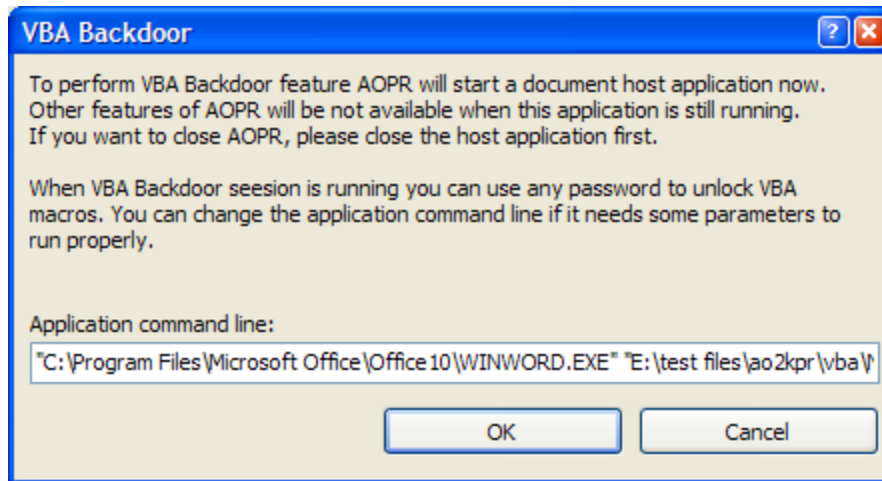
If you have a document with password-protected VBA project, but for some reason the password cannot be recovered, or the password shown by **AOPR** cannot be entered (for example it contains non-English characters that cannot be entered using your keyboard), or **AOPR** only allows to change or remove that password (but you would not like to do that), you can use the "**VBA backdoor**" feature. It works for **all applications** which can create VBA projects in their documents, not only Microsoft® Office (for example, Corel WordPerfect Office and AutoCAD).

With that feature, the password is not being recovered at all. However, you're able to open a VBA project (to view/edit the code). Of course you should have the application (this document has been created with, or later version) installed.

First of all, **please close all running instances of MS Office applications**.

Press the "**VBA Backdoor**" button on **AOPR** toolbar (or select **VBA Backdoor | Open file through backdoor** menu item). The program will prompt you for the document file.

Select the file and the following dialog will be displayed:



Here you set the additional Command Line parameters if needed. **AOPR** will run the application (with a special way) this document has been created with, and load your document into it. Now go into VBA properties (typically, it is under "**Tools | Macro | Visual Basic Editor**" or "**Tools | VBAProject Properties**". You'll be prompted for the Password. Enter **ANY** one (e.g., xyz), and it will be accepted!

If your document has been created in Microsoft® Office 97, you can use Office 2000 or Office XP, too. However, the reverse is not true: if you would like to unprotect Office 2000/XP document, but have only Office 97 installed, **AOPR** will still run it (with a warning message), but Backdoor will not work.

In addition (for example, in the case if the extension of the protected files is not registered in the system, so **AOPR** don't know what program to execute), you can just run the desired application (the one with VBA support: Word®, Excel®, FrontPage, AutoCad etc) using the same technology: select "**VBA Backdoor | Launch application**" menu item. Backdoor will be activated, and for all documents you will open in that application, **any** password will be accepted.

Please note that this backdoor is supported only for a limited number of versions of VBA engine (VBE.DLL, VBE6.DLL, VBE7.DLL) – the ones that were available when current version of **AOPR** has been released (the latest one comes with Microsoft® Office 2013). When the application is executed, **AOPR** prints (into the Log Window) the size and version number of that DLL. If your one is not supported yet, **AOPR** uses "generic" patch, which may fail under certain circumstances.

4.8.4 Setting AOPR Options

4.8.4.1 Type of Attack

If a Password cannot be recovered instantly you must use one of the Attack Types. The detailed description of available attacks can be found in our [Knowledge Base](#).

4.8.4.2 Preliminary Attack

Preliminary Attack is the set of predefined Attacks which are tried when a password cannot be recovered instantly. When this Attack is running the following dialog is displayed:



Preliminary Attack consists of four independent attacks which can be enabled/disabled in program options.

- **Found Passwords Attack.** This attack is always available. It checks all passwords that were found in the document prior to finding the current password. For example Microsoft® Word® files may have a VBA project password. This password is checked first because many users use the same passwords in different places.
- **Password Cache Attack.** This attack checks the [Password Cache](#) (all passwords found in other documents by AOPR). This attack can be enabled/disabled by "**Password Cache Preliminary Attack**" checkbox at the "**Options**" tab.
- **Preliminary Dictionary Attack.** Performs the Dictionary Attack by Default Dictionary. This attack can be enabled/disabled by "**Preliminary Dictionary Attack**" checkbox at the "**Options**" tab.
- **Preliminary Brute-Force Attack.** Performs the Brute-Force Attack by several predefined character sets. This Attack can be enabled/disabled by "**Preliminary Brute-Force Attack**" at the "**Options**" tab.

Preliminary Attack may take several minutes to run. You can stop it at any time clicking the "**Stop**" button.

You can [set your own languages and character sets](#) for Preliminary Attack.

4.8.4.3 Customizing the Preliminary Attack

Every time when you open a document in Advanced Office Password Recovery it performs the preliminary attack in case when the "file open" password is set. This attack tries all passwords that you recovered in past (which are stored in [password cache](#)). After that dictionary attack and finally the brute-force attacks are running.

The brute-force attack consists of two parts:

1. Trying digits and latin letters
2. Trying national characters depending on code page set in Windows.

You can set your own character sets and languages for Preliminary Attack using the **"attacks.xml"** file that is located in the directory where Advanced Office Password Recovery is installed.

The first section of this file is the language map:

```
<LanguageNameMap>
  <x0411>Japanese</x0411>
  <x0419>Russian</x0419>
  <x0422>Russian</x0422>
  <x0423>Russian</x0423>
</LanguageNameMap>
```

The codes are Windows [language identifiers](#). You can link any LID to your custom name.

The next section contains predefined charsets:

```
<Charsets>
  <LatinAllCaps>ABCDEFGHIJKLMNOPQRSTUVWXYZ</LatinAllCaps>
  <LatinAllSmall>abcdefghijklmnopqrstuvwxyz</LatinAllSmall>
  ...
</Charsets>
```

All charsets are in unicode so you can define any national characters here.

And the final section is "documents". All parts of this section have comments about document types. You can define the "common" charsets and charsets that are related to system language. Each "attack" record defines password length and charset.

In this XML file you can simply change the standard preliminary attack and define the custom charsets for your language.

4.8.4.4 General Options

4.8.4.4.1 Other options

AOPR Options can be adjusted at the **"Options"** tab.

The **"Device Manager"** button allows to select a hardware that will be used for password searching. By default AOPR uses all available CPU cores and graphic cards to achieve the best performance. But you can disable some CPUs or GPUs using the Device Manager.

"Enable Debug log" option creates a [separate log file](#) ("**aoxppr_debug_log.txt**") with the detailed information needed for resolving problems. Normally this option must be switched off.

Folder for log files: select the folder where "**aoxppr_debug_log.txt**" and other log files files will be created.

If you select the **Minimize to tray** option, the program will hide itself from the screen when being minimized (so you will not see an appropriate button on Windows® toolbar), but small icon will be created in the tray (near the system tray). Double-click on it to restore.

By disabling the **Prompt if project was changed** option, you instruct **AOPR** not to display the messages like "The project has been changed. Save?", when you've changed some options and open an another project, or creating a new one.

At the **"Options"** tab you can also enable or disable the [Preliminary Attacks](#).

4.8.4.5 Password Cache

4.8.4.5.1 About Password Cache

Password Cache is a storage designed to keep all passwords that were found while **AOPR** worked. These passwords are stored in the Unicode format so passwords which contain international symbols can be stored too. To prevent an unauthorized Access® the Password Cache can be protected by a Password. In this case a Password Cache File is encrypted by RC4 cryptographic algorithm and only SHA-1 Hash is stored in a File to verify a Password.

Password Cache is used in the [Preliminary Attack](#). When a Document Password cannot be recovered instantly AOPR checks the **Password Cache** first. In some cases it helps to recover a password even faster.

At the first Program start a cache File with name "**aopr.pwc**" is created. You can [Manage Password Cache Files](#) at the **"Password Cache"** tab.

4.8.4.5.2 Managing Password Cache Files

All **Password Cache** controls are located at the "**Password Cache**" tab.

To select a **Password Cache** File click the "**Select File...**" button and pick the needed file.

To Protect a Cache File by a Password click the "**Set Password...**" button and enter the Password in the appeared Dialog.

You can also **View** and **Clear** Cache File by clicking the corresponding buttons and disable writing all found passwords to cache by "**Add all found Passwords to the Cache**" option.

4.8.5 Passwords Manual

Strong Passwords

[Word®/Excel® Password to Open \(Office 97/2000\)](#)

[Word®/Excel®/PowerPoint® Password to Open \(Office XP and later\)](#)

[Microsoft® Money 2002 Password to Open](#)

Weak Passwords

[Word®/Excel® Password to Open \(Weak Encryption\)](#)

[Visual Basic for Applications \(VBA\)](#)

Microsoft® Access®

[Access® Share-Level \(Database\) Password, Owner Information](#)

[Access® User-Level Passwords](#)

Microsoft® Excel®

[Excel® Document - all Passwords except the one to Open](#)

[Excel® Add-In \(XLA\) Protection](#)

[Pocket Excel®](#)

Microsoft® Word®

[Word® Document - all Passwords except one to Open](#)

Microsoft® Outlook®

[Outlook® Personal Storage File Password](#)

[Outlook® E-Mail Accounts Passwords](#)

[Microsoft® PowerPoint®](#)

[Microsoft® Money](#)

[Microsoft® Project](#)

4.8.5.1 Strong Passwords

4.8.5.1.1 Word/Excel Password to Open (Office 97/2000)

This Password can be assigned in Microsoft® Word® and Excel®, version 97 or later. To set the password (in English version of Microsoft® Word®) select the **"Tools | Options"** menu item, then select the **"Security"** tab and enter the Password in the **"Password to open"** field.

When you assign the File Opening Password to your Word® or Excel® 97/2000 document (so the user will have to enter it to open the file), Microsoft® Office encrypts the Document using the RC4 cryptographic algorithm. Microsoft® Office uses the MD5 hash to verify a Password. Therefore this Password cannot be recovered instantly.

AOPR can recover a lost Password using the Brute-Force and Dictionary [Attacks](#). For the Brute-Force Attack, you have to set up the password length (it is limited to 15 characters) and password range (which, by the way, can include national symbols). Don't expect to recover long (8+ characters) and complex Passwords in a reasonable time, though.

4.8.5.1.2 Word/Excel/PowerPoint Password to Open (Office XP/2003)

Microsoft® Office XP (2003) and later supports three different levels of Password protection (see Microsoft® Knowledge Base Article - Q290112: [General Information about Microsoft® Office XP Encryption](#)):

Office 97/2000 Compatible Encryption

The default encryption method for Microsoft® Office XP is the *Office 97/2000 Compatible Encryption* method. This is the Office-proprietary [encryption](#) that is supported by Microsoft® Office 97/2000 (Word® and Excel®). Office 97/2000 Compatible continues to be the default Password algorithm to ensure backward compatibility and international document portability.

Weak Encryption (XOR)

This method equates to the Office 95 and older [XOR encryption algorithms](#) that are supported by earlier versions of Word® and Excel® and that are still used in Office 2000 when the system locale is France. This is a fast, simple algorithm, but it does not offer the best security. For files encrypted using this method, all Passwords are being recovered instantly.

Cryptographic Provider

This is a new encryption method introduced in Microsoft® Office XP. Basically, cryptographic service provider (CSP) is an independent software module that actually performs cryptography algorithms for

authentication, encoding, and encryption; for more information, please visit [Cryptographic Service Providers](#) at Microsoft® site.

There are a few different cryptographic service providers developed by Microsoft® (some of them are available with every Windows® installation, while the others are installed only with Microsoft® Internet Explorer upgrades, Service Packs or High Encryption Packs). Office XP Documents can be encrypted using any CSP that supports RC4 (a stream cipher) and SHA-1 (Secure Hash Algorithm). We have successfully tested **AOPR** on documents encrypted using the following CSPs:

Microsoft® Base Cryptographic Provider
Microsoft® Base DSS and Diffie-Hellman Cryptographic Provider
Microsoft® DH SChannel Cryptographic Provider
Microsoft® Enhanced Cryptographic Provider
Microsoft® Enhanced DSS and Diffie-Hellman Cryptographic Provider
Microsoft® RSA SChannel Cryptographic Provider
Microsoft® Strong Cryptographic Provider
Microsoft® Enhanced RSA and AES Cryptographic Provider (Prototype)

For the Documents using that encryption method, **AOPR** can run the same attacks as for [Office 97/2000](#), i.e. Brute-Force and Dictionary – even at better speed. If an unknown CSP has been encountered (other than one from the list provided above), **AOPR** should still recover the password, at least if that CSP follows the Microsoft® specification/standard; otherwise, please [contact technical support](#).

Microsoft® PowerPoint® XP and later uses only "Cryptographic Provider" encryption method.

4.8.5.1.3 Microsoft OneNote Password to Open

Microsoft® OneNote® beginning from version 2003 with Service Pack 1 allows to set a Password to a Notes File. This Password is strong and therefore cannot be recovered instantly.

AOPR can recover this Password using the Brute-Force and Dictionary [Attacks](#).

4.8.5.1.4 Microsoft Money 2002+ Password to Open

This Password can be set selecting the "File | Password Manager" menu item in Microsoft® Money 2002 and later. When you set this Password, the Money Database is encrypted using the RC4 Encryption Algorithm. Only Password Hash is stored in the Database to verify the Password. Therefore this Password cannot be recovered instantly.

AOPR can recover a lost Password using the Brute-Force and Dictionary [Attacks](#). For the Brute-Force Attack, you have to set up the password length and password range (which, by the way, can include national symbols). In Money 2002-2005 all password symbols are capitalized (for example "Aaaa" and "AAAA" are the same Passwords). Therefore the Password Range cannot contain the small latin characters and the "a - z" Charset Option is disabled. In Money 2006, when using the MS Passport login, a password can contain any characters.

Money 2003 and later can use Microsoft® Passport authentication to open a Database. In this case a Password for MS Passport Logon is a Database Password. Money 2003 allows to store MS Passport Passwords locally. [These Passwords can be recovered in AOPR](#).

4.8.5.1.5 Office 2007 and later: password to open

In Office 2007 Microsoft has significantly improved the password protection system.

Now the following applications allow to set the file opening password which is used to encrypt a document:

Word, Excel, PowerPoint, Access.

These programs use AES encryption algorithm and the SHA-1 hash is used in password verification. The password verification is now very slow. Only short and simple passwords can be recovered. In Office 2010 Microsoft doubled the number of SHA-1 hash iterations and therefore password recovery became two times slower.

In Office 2013 SHA-1 was replaced by SHA-512 - more complicated and significantly slower hash algorithm.

We recommend to use graphic cards (GPUs) to recover Office 2007+ passwords. Using of modern graphic card significantly increases the password recovery speed.

4.8.5.2 Weak Passwords

4.8.5.2.1 Word/Excel Password to Open (Weak Encryption)

This type of Encryption is used in the following Applications:

- Word®/Excel® 95 and older
- Word®/Excel® 97/2000 with French Regional Settings
- Word®/Excel® XP and later by selecting the "Weak Encryption (XOR)" Option.

When this Password is set the Document is encrypted by weak algorithm (XOR). It allows to recover the Password instantly. Just [select the Document](#) in **AOPR** and the Password will be [displayed](#).

4.8.5.2.2 Visual Basic for Applications (VBA)

Microsoft® Visual Basic for Applications (VBA) allows to use a Password to protect Macros from reading their source code. When this Password is set a Password Record is appended to the VBA Macro Storage. Nothing is encrypted. In VBA version 5 the Password is stored encrypted by "XOR" logical operation. In VBA version 6 SHA-1 Password Hash is stored and Password cannot be recovered instantly. But we don't need to recover a Password to view the Macro source codes. We can modify or remove the Password Record.

AOPR shows the VBA Password if VBA version is 5 and allows to change or delete the Password if version is 6.

Professional Edition of **AOPR** has a ["VBA Backdoor"](#) Feature that allows to bypass VBA Password checking in any Application.

4.8.5.2.3 Microsoft Access

4.8.5.2.3.1 Access Share-Level (Database) Password, Owner Information

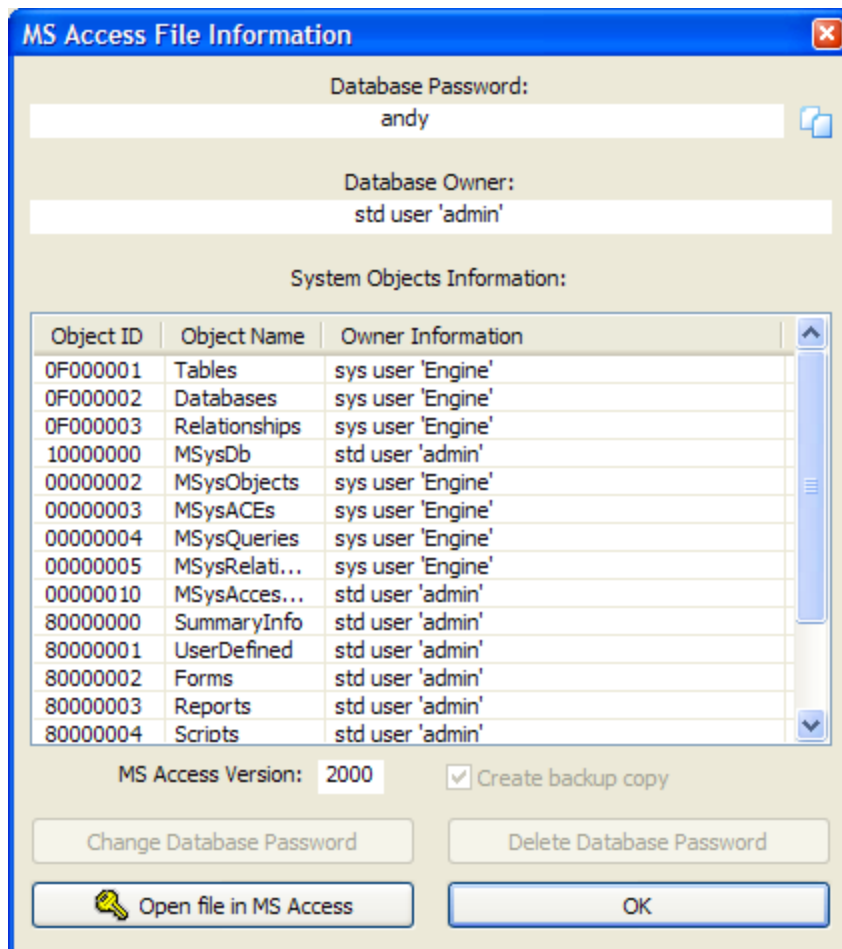
MS Access® **Share-Level (Database) Password** can be set to a Database to prevent unauthorized access. In English version of Access® this Password can be set selecting the **"Tools | Security | Set Database Password..."** menu item. This Password is stored in an Access® File encrypted by weak algorithm (XOR). Therefore it can be recovered instantly by AOPR. In Access 2007 the password protection is improved. Database password can be recovered by brute-force or dictionary attack.

Under [User-Level Security](#), users type a Password when they start Microsoft® Access®. Access® then goes out and reads a workgroup information file, where each user is identified by a unique identification code. Within the workgroup information file, users are identified as authorized individual users, and as members of specific groups, by their personal ID and password.

For Access® Databases (*.mdb) with User-Level Security, the program shows the following information:

- Access® version
- Share-Level (Database) Password
- Database Owner (Name and ID)
- List of Objects and their Owners

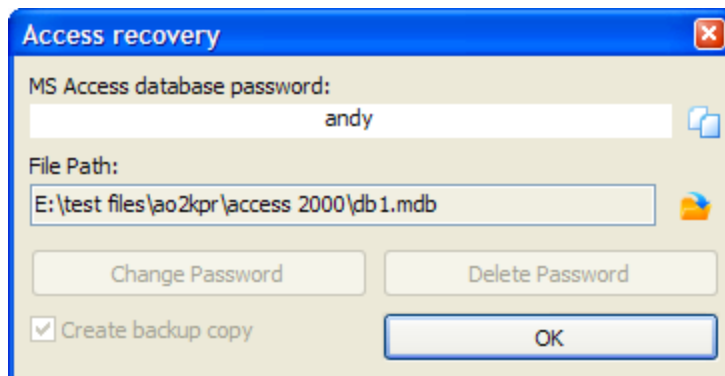
Here is an example:



In most cases, all you need is just the Database password – it is showing at the top of that window (please note that Access® 2.0 supports [User-Level Security](#) only, and so the Database Password will be always empty for Access® 2.0 files). You can use the Password shown by **AOPR**; for Access® 97 files, you're also able to change or delete it (using the appropriate buttons at the bottom), just don't forget to enable "**Create backup copy**" option.

However, if the database has User-Level Security set and workgroup administration file (*system.mda* or *system.mdw*) is not available (if it is there, you can just get all the user names and passwords from it – see **next chapter** for details), you will also need Database Owner information.

Database Owner is showing only in AOPR Professional. Standard Edition just shows the Database Password:



To gain an Access® to a File if User-Level Security Database is absent, you need to do the following:

- Run MS Access® (same version your file has been created with, as shown by **AOPR**).
- Create a new database (or open any existing not protected one).
- Go to **Accounts** setup (usually, it is in **Tools | Security | User And Group Accounts**), **Users** tab.
- Create a new user with name displayed by AOPR (without quotes; just type that name in "Name" drop-down combo box, and press the **New** button). Access® will open a new window with two fields -- Name and "Personal ID". In the second one, type the ID displayed by **AOPR** and press OK.
- Close **Accounts** window with OK and exit from Access®.
- Run Access® from the command line with the '/user' option, i.e.:
MSACCESS.EXE /user
- You'll be prompted for User Name and password. Type the Name you created and empty Password.
- Now open your (protected) database, and you should have all necessary permissions (as Database Owner).

For more information, please see the following Microsoft® articles:

[About user-level security](#)

[Remove user-level security](#)

[Create, join, or fix workgroup information files](#)

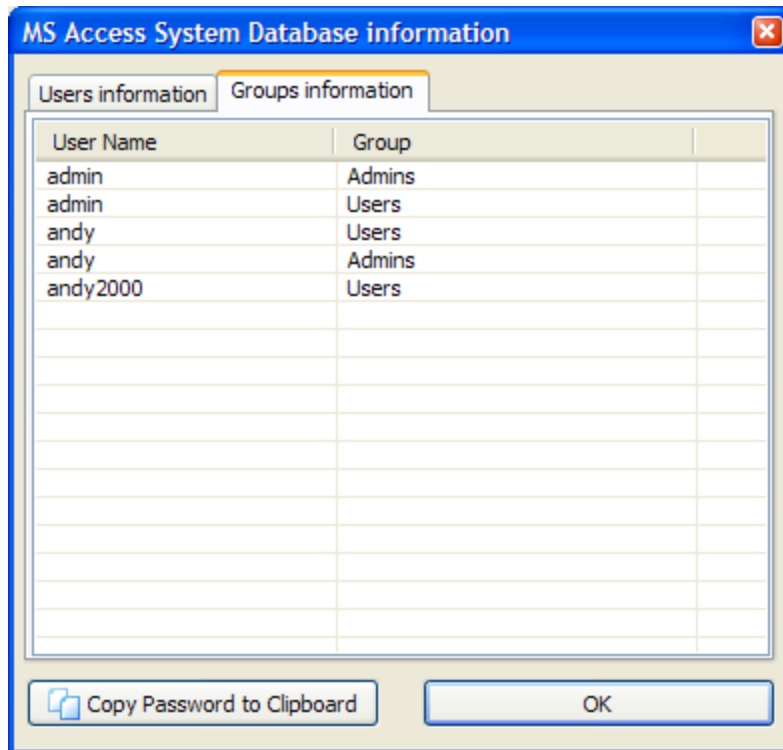
[Manage user and group accounts](#)

[Types of permissions](#)

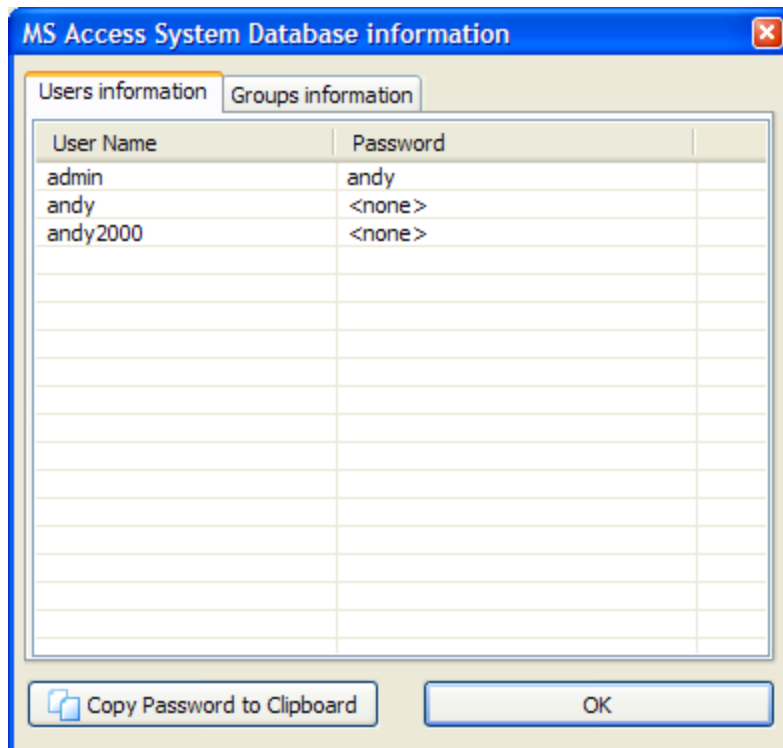
4.8.5.2.3.2 Access User-Level Passwords

Access User-Level Passwords are recovered instantly by **AOPR**.

For System Access® Databases (usually, **system.mda** or **system.mdw**), the program displays a window with two tabs – **Groups information** and **Users information**. The first one displays what groups the users belong to:



The second one displays the Passwords for all users:



4.8.5.2.4 Microsoft Excel

4.8.5.2.4.1 Excel Document - all Passwords except the one to Open

Microsoft® Excel® Document can have the following Passwords:

- Password to Open (can be [Strong](#) or [Weak](#))
- Password to Modify (Write Protection Password)
- Book Password
- Shared Book Password
- Sheet Passwords
- [VBA Project Password](#)

All Excel® Passwords except [Strong Password to Open](#) are recovered instantly. When you open an Excel® Document AOPR shows the following Dialog:

The dialog box titled "Excel Passwords recovery" displays the following information:

- Excel Document Password: <none>
- Excel Write Protection Password: 2b5b5b3b3b1b5
- Excel Book Password: 1b5b5b3b3b1b5
- Excel Shared Book Password: 1b5b5b3b3b1b5
- VBA Password: <none>

#	Sheet name	Sheet password
1	Sheet1	6b1b7b3b3b1b5
2	Sheet2	<none>
3	Sheet3	<none>

All Passwords for the selected File were recovered successfully or can be changed. Please note, in most cases Book and Sheet passwords are different than originally entered ones, but they're still valid for Excel.

File Path: E:\test files\ao2kpr\excel book or sheet\english_all.xls

Buttons: Open..., Change VBA Password, Delete VBA Password, Unlock Excel Add-In, OK

☒ Create backup copy

Please note that some of these Passwords (shown by **AOPR**) may differ from ones originally set in Excel®. However, Excel® will accept them without problems.

You also can change or delete the VBA Password and [Unlock Excel Add-In \(XLA\)](#).

4.8.5.2.4.2 Excel Add-In (XLA) Protection

When you save your Excel® Document as **Add-In** (with XLA extension) the VBA Macros source code cannot be viewed and modified. This Protection is implemented by setting the "XLA Flag" in the Excel® Document. AOPR can simply reset this Flag and after that you can see any VBA Macro source. XLA Add-In can be unlocked in the [Excel® Passwords Dialog](#).

4.8.5.2.4.3 Pocket Excel

Pocket Excel® Files (on Windows® CE and Windows® Mobile) may be protected by File Opening Password. This Password is stored in the File and can be recovered instantly by AOPR. All you need is to transfer the File from Pocket PC by ActiveSync and [open](#) it in the **AOPR**.

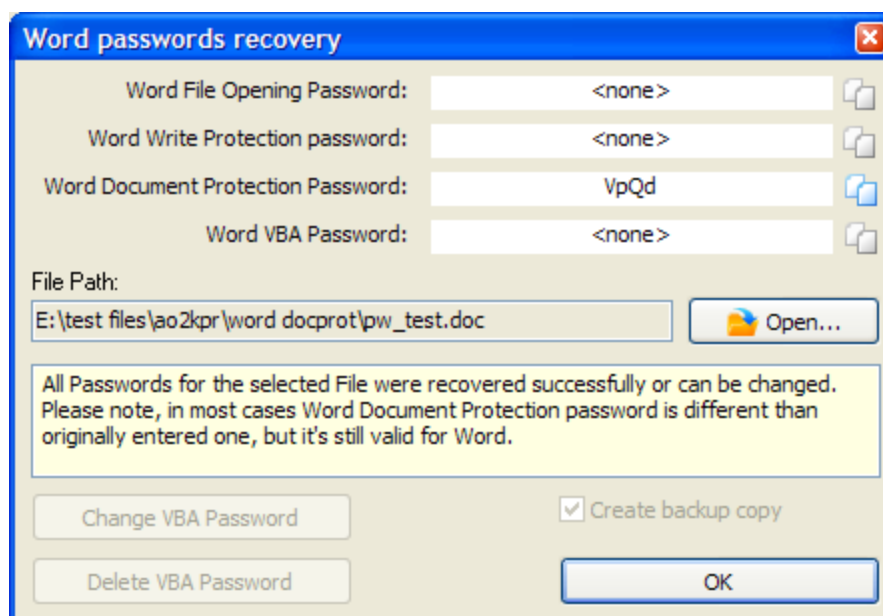
4.8.5.2.5 Microsoft Word

4.8.5.2.5.1 Word Document - all Passwords except the one to Open

Microsoft® Word® Document can have the following Passwords:

- Password to Open ([Strong](#) or [Weak](#))
- Password to Modify (Write Protection Password)
- Document Protection Password
- [VBA Project Password](#)

When you select a Word® Document in **AOPR** the following Dialog appears:



All Passwords except Strong Password to Open are recovered instantly. You can also change or delete the VBA Password.

4.8.5.2.6 Microsoft Outlook

4.8.5.2.6.1 Outlook Personal Storage File Password

Microsoft® Outlook® allows to protect its Personal Storage File (with PST extension) by a password. This password can be set in Outlook® by editing the Personal Folders Properties. Only small Password Hash is stored in the File. Nothing is encrypted. Therefore this password is recovered instantly by **AOPR**.

To get password to **PST** file (all versions of Outlook® are supported: 97, 98, 2000, 2002/XP, 2003, 2007 and 2010), simply open it in **AOPR**. If the given File is corrupted, or used by another application, or not password-protected – appropriate error message will be displayed. Otherwise, the Password will be recovered immediately, shown in the message box and written to the Log Window.

Please note that in some cases, the password recovered by **AOPR** is not the same as the one which has been originally set. That's due to encryption algorithm used in Outlook® – the original Password is not stored in the file. But that password (shown by **AOPR**) will be accepted by Outlook® without problems – just try. And of course, after logging into Outlook®, you'll be able to change that Password to any one, or just remove it.

4.8.5.2.6.2 Outlook E-Mail Accounts Passwords

Microsoft® Outlook® can store Passwords to E-Mail accounts by setting the Option "**Save Password**" in the **Account Properties**. These Passwords are stored in System Registry and can be decrypted by **AOPR**. E-Mail Account Passwords are recovered instantly. Please note the Password can be recovered only in case when it's stored locally by Outlook®. **Passwords which are not stored on local computer cannot be recovered at all.**

[Read more about recovering Outlook® E-Mail Accounts in AOPR](#)

4.8.5.2.7 Microsoft PowerPoint

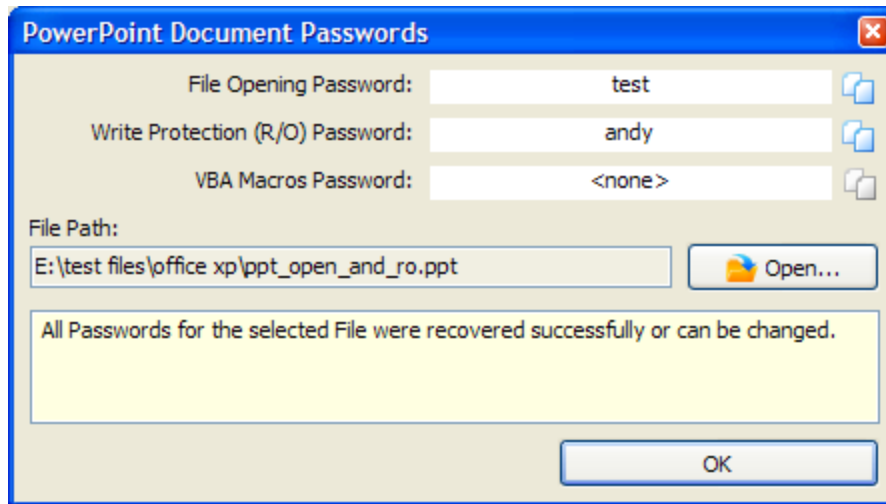
Microsoft® PowerPoint® prior to PowerPoint® XP allows to set only [VBA Project Password](#).

PowerPoint® XP and later allows to set the following Passwords:

- [Password to Open](#)
- Password to Modify (Write-Protection)
- [VBA Project Password](#)

Password to Open is a Strong Password and can be recovered only by Brute-Force or Dictionary [Attack](#). [Read more about this Password](#).

Password to Modify can be recovered instantly. Just [select the Document](#) in **AOPR** and the following Dialog will appear:



You can copy any Password to Clipboard and open the PowerPoint® File.

4.8.5.2.8 Microsoft Money

Microsoft® Money from 3.x to 2000 allows to set the Database Password. This Password is stored in the Database and can be recovered instantly by **AOPR**. Just [select the File](#) in **AOPR**.

Microsoft® Money 2002 and later Database Password cannot be recovered instantly. [Read more about this Password](#).

4.8.5.2.9 Microsoft Project

Microsoft® Project allows to set the following Passwords:

- Password to Open
- Password to Modify
- [VBA Project Password](#)

AOPR recovers these Passwords instantly except VBA Password which can be changed or deleted. To recover Passwords of MS Project File [select the File](#) in **AOPR**.

4.8.6 Troubleshooting

4.8.6.1 Creating Debug Log

While recovering Microsoft® Outlook® Passwords (for E-Mail accounts and PST) there may be some problems which cannot be resolved remotely because all source data is located on the user's computer and we cannot view this data to investigate the problem. We created the "**Debug Log**" feature which collects the needed data during password recovery process.

To create a Debug Log simply do the following:

- Launch AOPR
- Check the "**Enable Debug Log**" checkbox at the "**Options**" tab
- Close AOPR and launch it again
- Do the actions that lead to the Problem
- Close AOPR

The Debug Log will be located at the folder specified in the "**Folder for Log Files**" field at the "**Options**" tab. AOPR Debug Log file name is "**aopr_debug_log.txt**". Please send this file to our [Customer Support](#) and we'll try to resolve the Problem.

4.8.7 Trial Version of AOPR and Registration

4.8.7.1 Limitations of the Trial Version

The Trial version of **Advanced Office Password Recovery** has the following Limitations:

- The maximal length of passwords which are recovered by Brute-Force [Attack](#) is limited to 4 symbols
- Passwords recovered by Dictionary Attack, which are longer than 4 symbols, are not displaying
- The maximal length of passwords, which are recovered instantly, is limited to 3 symbols
- Log File is not created
- [VBA Backdoor](#) feature is not available
- [VBA Passwords](#) cannot be changed or removed
- Excel® Add-Ins (XLA) cannot be unlocked
- [Access® Database Owner Information](#) is not shown
- Only one GPU can be used for password recovery

You can [Purchase the Full Version](#) of **Advanced Office Password Recovery** to withdraw these limitations.

4.8.7.2 Registration

There are three editions of **Advanced Office Password Recovery**: Home, Standard and Professional.

For more information about differences between those editions see the [AOPR Supported File Formats list](#).

You can place an order online using the following order form:

<http://www.elcomsoft.com/purchase/buy.php?product=aopr&ref=DOC>

4.9 Advanced PDF Password Recovery

4.9.1 Introduction

Advanced PDF Password Recovery (APDFPR) unlocks [Adobe Acrobat PDF](#) documents and removes editing, printing and copying restrictions instantly. Get access to encrypted and password-protected PDF documents quickly and efficiently! The unique patented Thunder Tables(tm) technology guarantees the recovery of 40-bit keys in under a minute! GPU acceleration (NVIDIA) is available for the latest Adobe encryption with 256-bit key.

We offer a variety of editions to satisfy the most demanding customer yet affordable to casual users.

The Standard edition is a perfect choice if you have a restricted PDF file that deprives you of getting a hard copy and/or disallows editing and copying of data to clipboard. The Standard edition instantly removes all restrictions and unlocks the protected PDF file.

If you cannot open a PDF file without knowing the password, you need the Professional edition. This edition comes with everything included in the Standard version, and allows retrieving the "owner" and "user" passwords with brute-force and dictionary attacks. The unique Key Search Attack guarantees the recovery of PDF documents protected with 40-bit encryption. Accelerated by GPU and effectively optimized for speed, this attack can recover the protected documents in a matter of days when used on a modern multi-core PC. Removing JScript code, form fields and digital signatures is also an option.

The Enterprise edition extends the features of the Professional version by adding the unique, patent-pending Thunder Tables technology that allows recovering "user" passwords in a minute's time frame instead of days. The Thunder Tables technology uses pre-computed data and supports 40-bit encryption only.

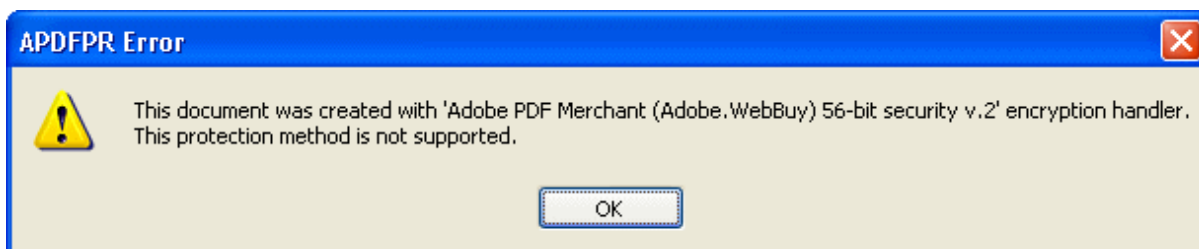
4.9.2 Requirements and limitations

Requirements

- Windows XP or higher
- about 6 megabytes of free space on hard disk (4 gigabytes for Enterprise version)

Limitations

- PDF files protected using [Digital Rights Management \(DRM\) technology](#) or 3rd party plugins such as [FileOpen](#) cannot be decrypted. If you try to start to decrypt such file, APDFPR shows the message like:



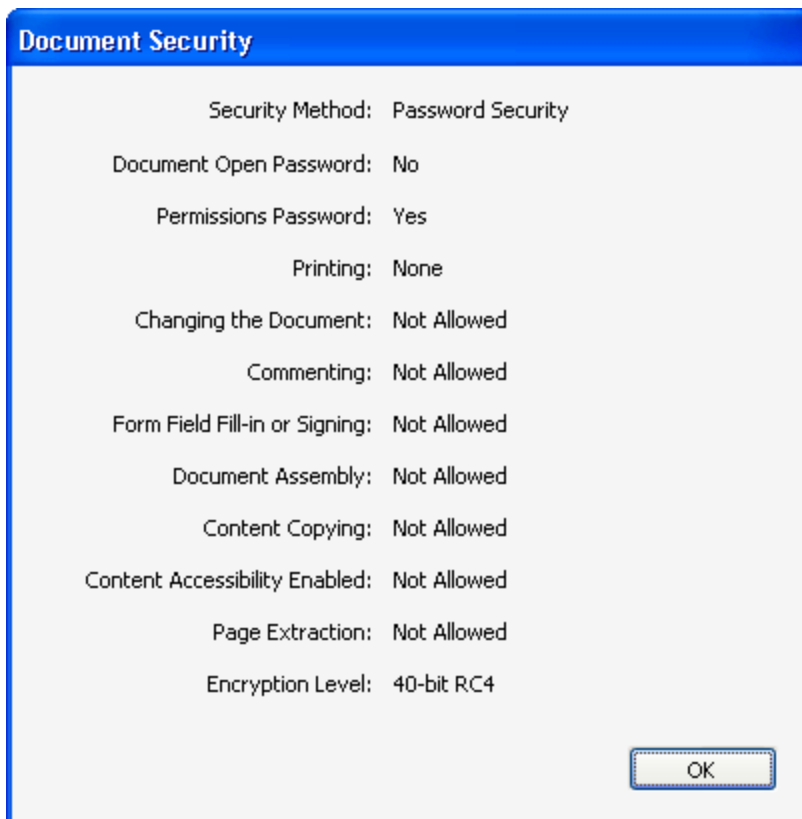
- Brute-force attack is effective for short passwords only, usually up to 7-8 chars. Recovering longer ones will take too much time (months, years) even on a very fast computer. In most cases, dictionary attack really helps (to find long passwords), but if the password is well-selected (e.g. the combination of letters, digits and special chars, or concatenation of two or more words etc), it cannot be recovered at all. Fortunately, if only "owner" password is set, there is no need to recover it at all – the document can be decrypted (instantly) anyway; and for files with "user" password that use 40-bit encryption, you can use [Key search attack](#).
- The program tries to process corrupted files (and on success, shows the number of non-critical errors ignored), but sometimes, it is not possible. You can fix most of such problems simply by opening your file in Adobe Acrobat (full version, not the Reader) and just saving it without making any changes.

4.9.3 How to work with the program

4.9.3.1 About PDF encryption

[Adobe Acrobat](#) features two levels of password protection.

Protecting document with access restriction ("owner", so-called "security" or "master") password does not affect a user's ability to open and view the PDF file, but prevents user from editing (changing) the file, printing it, selecting text and graphics (and copying them into the Clipboard), adding/changing annotations and form fields etc (in any combination). If the file is protected this way, you open it in Adobe Acrobat Reader (again, the password is not required for that) and select File | Properties menu item, Security, Show Details, the following information is shown (for example):



Fortunately, there is no need to recover that password at all: instead, we can remove it (decrypt the file), so the resulting document will not have any restrictions. That's exactly what APDFPR does. However, such decryption possible only if "user" password (see below) is not set or known.

Also, there are "open" (so-called "user") passwords. If one is set, the file is encrypted with strong RC4 algorithm, and cannot be opened at all, if the password or encryption key is not known. APDFPR can recover (try to recover) this password, too, but time-consuming dictionary and brute-force attacks are required. In addition, APDFPR allows to run this attacks to recover "owner" password, because to decrypt the file, either "user" or "owner" password is needed. Even if both passwords are very long and complex, it is still possible to decrypt the file using [Key search](#) attack, which tries all possible 40-bit RC4 keys. It takes a few days to complete, but the success is guaranteed. However, if you have pre-computed hash tables (shipped with APDFPR Enterprise), that process takes just a few minutes.

Note that when the file is being saved in Acrobat and the "user" password is set, the "owner" password is being set automatically to the same value (but can be changed manually, of course). That's because PDF file cannot have only "user" password: in any case, it has either "owner" password, or both "owner" and "user" passwords (which could be the same or different). Please take that in mind when selecting [Advanced options](#).

Finally, PDF files can be protected using [Digital Rights Management \(DRM\) technology](#) or 3rd party plugins such as [FileOpen](#). APDFPR does not support such ones, i.e. cannot decrypt them at all.

Please note that Acrobat versions 5..8 can create PDF files with improved security level: 56..128-bit RC4 or 128-bit AES encryption. For such files, "owner" protection can be recovered instantly as for Adobe Acrobat 4.0 (and older versions), but brute-force and dictionary attacks are much slower; and "key search" attack is not available at all. For Acrobat 9 files with 256-bit AES encryption, "key search" attack is also not available, but brute-force attack speed is much better.

When brute-force or dictionary attack starts, APDFPR provides additional information what kind of security handler is being used; log window will contain a record like:

05.04.2002 13:05:51 - File "C:\My Documents\test.pdf" opened.

05.04.2002 13:06:14 - Handler: Acrobat Standard (Standard) 40-bit security v.1.

or

05.04.2002 13:05:51 - Handler: Acrobat Standard (Standard) 128-bit security v.2.

PDF files (even not encrypted ones) may also contain additional objects such as JScript code, form fields and digital signatures; sometimes they are being used for document protection. APDFPR allows to remove them as well.

4.9.3.2 Selecting the options

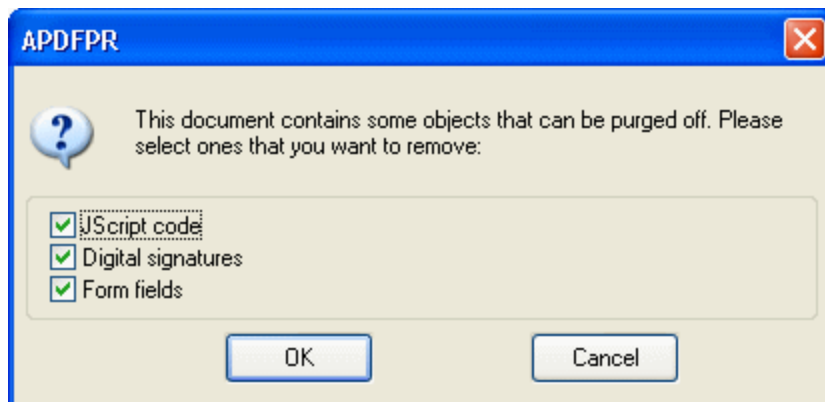
4.9.3.2.1 Encrypted PDF file

Just enter the name of the PDF document you'd like to get the password for. Use the Open button on program toolbar, [File] | [Open File] menu item or F3 key to pick the file from the list. Alternatively, you can use drag'n'drop – just drag the file (with a mouse) from Windows Explorer, and drop it to the APDFPR window.

If Start attack on file select [option](#) is enabled, the program analyses the encryption used. If only "owner" password is set, or any of the passwords ("user" or "owner") is known, and you just need to remove restrictions from the file, you can decrypt the file immediately. If the "user" password is set but now known, you have to select other options and start the attack – consult next chapters for more informations.

If the file is encrypted using any security method other than standard, APDFPR will display an error message (that this kind of encryption is not supported), and write a corresponding record to the log file. If the file is corrupted, or could not be opened for some other reason, an appropriate error message will be shown. For more information, please refer to [Error messages](#) chapter.

If the file is not encrypted at all, but contains JScript code, form fields or digital signatures, the program offers to remove any of these elements:



Please note that if the file is password protected or restricted and contain such elements, it should be processed in two steps: you have to decrypt it first, and then load the file APDFPR again to remove digital signatures and/or other stuff.

4.9.3.2.2 Type of attack

Brute-force or dictionary attack. [Brute-force](#), Mask, [Dictionary](#) and [Key search](#) attacks are available.

4.9.3.2.3 Brute-force range options

Instructs the program what characters have been used in the password. You can choose from all capital letters, all small letters, all digits, all special symbols and the space, or all printable (includes all of the above). The special characters are:

!@#\$\$%^&*()_+-=<>.,/?[]{}~:;`'|"\'

Alternatively, you can define your own character set (charset). Just mark the "User-defined" checkbox and click on "Custom charset..." (at the right of the option). In the input window, enter all chars of your password range; for example: if you remember that your password was entered in the bottom keyboard row ("zxcv...") - your password range should be "zxcvbnm,./" (or in caps: "ZXCVBNM<>?"). You can also define both of these: "zxcvbnm,./ZXCVBNM<>?". In addition, you can load and save custom charsets, or combine them using the "Add charset from file..." button.

4.9.3.2.4 Start from password

This option may help, for example, if you know the first character(s) of the password. For example, if you're sure that the small letters have been used (from 'a' to 'z'), the length is 5, and the password definitely starts with 'k', than type 'kaaaa' here. Please also note, that if you press the "Stop" button when APDFPR is working, the program writes the current password to

this window ("Start from password"). It can be used later to restart the program from the same point.

Please note that the program verifies the passwords according to the following character order:

- CAPITAL letters: 'A'..'Z'
- the space
- small letters: 'a'..'z')
- digits: '0'..'9'
- special characters: !@#\$%^&*()_+-=<>.,/?[]{}~:;`'|"\"

You can also use End at field to set the password APDFPR should stop at. It might be useful if you attack the same document on a few computers, and so can split the whole password range onto a few parts.

4.9.3.2.5 Password mask

If you already know some characters in the password, you can specify the mask to decrease the total number of passwords to be verified. At the moment, you can set the mask only for fixed-length passwords, but doing this can still help.

For example, you know that the password contains 8 characters, starts with 'x', and ends with '99'; the other symbols are small or capital letters. So, the mask to be set is "x?????99", and the charset has to be set to All caps and All small. With such options, the total number of the passwords that APDFPR will try will be the same as if you're working with 5-character passwords which don't contain digits; it is much less than if the length were set to 8 and the All Printable option were selected. In the above example, the '?' chars indicate the unknown symbols.

If you know that the password contains an occurrence of the mask character '?', you can choose a different mask character to avoid having one character, '?', represent both an unknown pattern position and a known character. In this case, you could change the mask symbol from '?' to, for example, '#' or '*', and use a mask pattern of "x#####?" (for mask symbol '#') or "x*****?" (for mask symbol '*'). Select the mask symbol on [Advanced Options](#) page.

4.9.3.2.6 Password length

This is one of the most important options affecting checking time. Usually, you can test all short passwords in just a few minutes; but for longer passwords, you have to have patience and/or some knowledge about the password (including the character set which has been used, or even better – the [mask](#)).

The minimum length cannot be set to a value greater than maximum length, of course.

If the minimum and maximum lengths are not the same, the program tries the shorter passwords first. For example, if you set minimum=3 and maximum=7, the program will start from 3-character passwords, then try 4-character ones and so on – up to 7. While APDFPR is running, it shows the current password length, as well as the current password, average speed, elapsed and remaining time, and total and processed number of passwords ([Program status](#)). All of this information except average speed and elapsed time, which are global, is related only to the current length.

4.9.3.2.7 Dictionary options

Simply select the desired wordlist file. In addition, you can select an option Smart mutations or Try all possible upper/lower case combinations – it may really help if you're not sure about the register the password has been typed in. For example, let's assume that the next word in the wordlist is "PASSword" (the case, actually, doesn't matter here). With the second option enabled, the program will just try all possible combinations, like:

```
password
passworD
passwoRd
passwoRD
passwOrd
...
PASSWORDd
PASSWORD
```

However, checking all such combinations takes a lot of time: in the example above, APDFPR will check 2^8 words (i.e. 256) instead of one. With smart mutations, you can eliminate a number of "virtually impossible" combinations, and here are all the words which will be checked:

PASSword	(as is)
passWORD	(reversed)
password	(all lower case)
PASSWORD	(all upper case)
Password	(first uppercase, rest lowercase)
pASSWORD	(first lower case, rest uppercase)
PaSSWoRD	(elite: vowels in lc, others in uc)
pAsswOrd	(noelite)
PaSsWoRd	(alt/1)
pAsSwOrD	(alt/2)

So, it makes only 10 combinations for each word.

The Start line # option allows you to start an attack from a given line (in the wordlist); if you interrupt the attack, the "current" line number will be written there (and saved to the project file, of course).

A small but very effective wordlist is included into APDFPR distribution: english.dic (about 240,000 words); German and Russian wordlists are also included.

4.9.3.2.8 Key search

If the PDF file has both user and owner passwords and they are long and complex, you have nothing to do but try this attack. It tries all possible RC4 encryption keys until it finds the right one, and allows to decrypt the file using that key – the resulting PDF file will have no security at all. That method gives 100% success.

In PDF 1.2/1.3 files (Acrobat 4.x or older), the key length is 40 bits, and so the total number of keys is 2^{40} , or 1,099,511,627,776. All key space is divided into 65,536 blocks, with 16,777,216 in a block; the whole recovery process takes about 30 days on old and slow PIII-450 computer, and just 3-5 days on modern Intel Core 2 Duo processors.

You have to select the block to start from (Start from block input box) and ending block (End at block box); both values could be from 0 to 65536. During the attack, the program shows the number of the current block, time elapsed, average speed (in keys per second), number of keys already processed and the total number of keys. When the key is found, the program shows it and ask you to decrypt the file; if you already know the key, just put it into the Document key input box and press Decrypt button at the right.

With the Enterprise version of APDFPR, you can seriously speed-up this attack by enabling Use pre-computed hash tables option; press Select user hashes directory button at the right and browse for the folder where the tables are located. This folder should contain the following folders/files (Thunder tablestm):

0\t00_I17000.data
0\t00_I17000.index
1\t01_I17000.data
1\t01_I17000.index
2\t02_I17000.data
2\t02_I17000.index
3\t03_I17000.data
3\t03_I17000.index
4\t04_I17000.data
4\t04_I17000.index

5\t05_I17000.data
5\t05_I17000.index
missing.bin

It is NOT recommended to use the tables directly from DVD (shipped with Enterprise version) because of very slow DVD drive performance. You can copy the DVD contents to the hard drive, or even better, to USB flash drive. USB flash drives have relatively low performance when reading files, but much better (than hard drive) random seek time, while this parameter is the most important for this attack.

With hash tables on hard drive, this attack takes from 10 to 30 minutes to complete; on USB flash drives – from just a few seconds and up to 10-15 minutes (worst case). This option also provides guaranteed recovery.

Finally, please note that Adobe Acrobat 5.0 and later (including the latest version, 8.0) can create PDF files with improved security level: 56..128-bit RC4 encryption (PDF 1.4 specification; look at [New feature highlights](#) document on Adobe server), and so that attack is not applicable to them (you will get an error message).

4.9.3.2.9 Auto-save

If you'd like APDFPR to save its state periodically, please check the appropriate option, and select the time (in minutes) between saves. If you do that, APDFPR will create and periodically update a restore file named "~apdfpr.axr" (that's the default – you can change it) in the same folder where your document is located (also by default; you can select any other folder to save that file to). This file is similar to one created when using the "Save setup" button. Even if your computer stops responding (or if power fails), you'll be able to restore breaking the password from the last saved state. Instead of using the default settings (the name of the file and the folder it will be saved to), you can also select your own settings. Enabling this option is strongly recommended.

4.9.3.2.10 Other options

Priority: background or high. If you want to start APDFPR as a "background" process, which will work only when the CPU is in an idle state, you may select "Background". If you want to increase performance, select "High", but be aware that this will decrease the performance of *all other* applications running on your computer.

Minimize to tray: if this option is enabled, the program window will disappear from the Windows desktop when you press the "minimize" button in the top-right corner of the window (or you select an appropriate item in the system menu). The small icon will be created in the "tray" area of the task bar (near the system clock). Just double-click on that icon to restore the window.

Log to apdfpr.log: when enabled, the program saves all information displayed in the status window into the log-file (apdfprp.log).

Progress bar update interval: allows to set an interval (in milliseconds) between progress bar and status window updates; the default is 500 (a reasonable value). By selecting the higher value (3000, for example), you can get slightly better recovery speed.

Start attack on file select: when this option is enabled (default), the program analyses the file immediately when you open it, and advises what to do next.

Language: the program has multi-language interface. Just select the appropriate language from the drop-down box. English is the default.

4.9.3.2.11 Advanced options

Search for: Any password, User password or Owner password. Select this option to instruct the program which particular password to search for; look at [About PDF encryption](#) chapter first. And here are a few recommendations for different cases:

- Your file is not encrypted at all. It doesn't matter what do you select: when you try to run the attack, the program will note you that it is nothing to do.
- Your file has only "owner" password set. You'll get a notification message that the file can be decrypted now, but you can still search for the original password. Select to search for Owner password only; you can also search for Any password, but the speed will be lower.
- Your file has both "user" and "owner" passwords set, and they're the same (typically, you don't know that in advance, but as noted above, the "owner" password is set to the same value as "user" one just by default). The best solution here is to search for User password only, as far as it is the fastest.
- Both "user" and "owner" passwords are set, but they're different. You can search for any of them, or for both at the same time. Please take in mind that searching for User password is the fastest, for Owner password – almost two time slower, and for Any password – the slowest. So that's up to you what to select. There is a chance that one of these passwords is much shorter/simpler than the other one, but again, you don't know that in advance. We'd recommend to set Any password first (for example, with the [dictionary attack](#), and up to 4-5 chars with [brute-force attack](#)), and then look for User password, but in extended range (e.g. up to 7 chars).

Mask symbol: used for [Mask](#) attack.

Use code optimized for: (Non-MMX processors / Intel PII/PIII/Celeron / AMD Athlon / Intel P4 SSE2 / Intel Core/Core2): force APDFPR to use the code specially optimized for the given CPUs. The program detects your CPU and tries to select the proper code automatically, but you may want to play with that option if you've got any other CPU.

GPU Manager: calls GPU Manager (separate program installed with APDFPR), that allows to set what GPU(s) (graphic processors) the program can run the brute-force attack on, so providing hardware acceleration. The list of compatible video cards is available at [NVIDIA web site](#). Please note that GPU acceleration is available only for PDF files with 256-bit AES encryption.

4.9.3.3 Save and Read setup

4.9.3.3.1 Save and Read setup

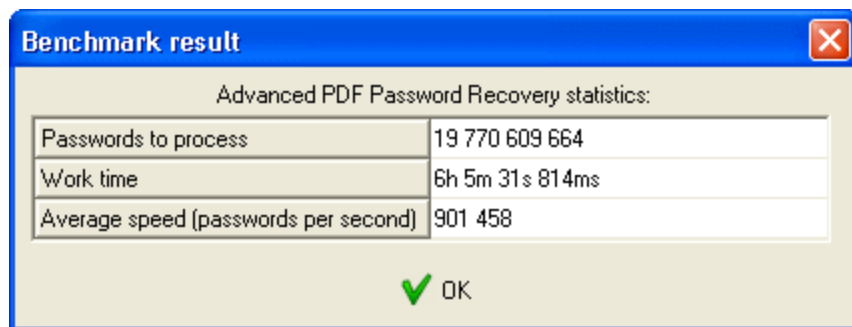
You can save your current APDFPR setup into a specified file (with extension AFR). When you select the [File] | [Save Project] or [Save Project as...] menu item, the "Save file" dialog appears. Just select a file name (e.g. "mydoc.afr"), or select an existing AFR-file for overwriting. You can read your setup later – simply select [File] | [Open Project].

Alternatively, you can use drag'n'drop – just drag the previously saved afr-file (with a mouse) from Windows Explorer, and drop it onto the APDFPR window. If all the settings are correct, the attack will be started immediately.

4.9.3.4 Benchmarks

4.9.3.4.1 Benchmark

If you would like to estimate how long the [Brute-force](#) or [Mask](#) attack will take, or test APDFPR's speed on a particular document, use the benchmark feature. Just select all the desired options, then press the Benchmark button (next to Stop). The program will work for about 10 seconds, and display some statistics afterwards:



Here you can see the total number of passwords (according to the options you set), average program speed, and estimated time. Please note that real time might be slightly different, because the speed of the program depends on how many other applications are running at the same time.

4.9.3.5 Getting the results

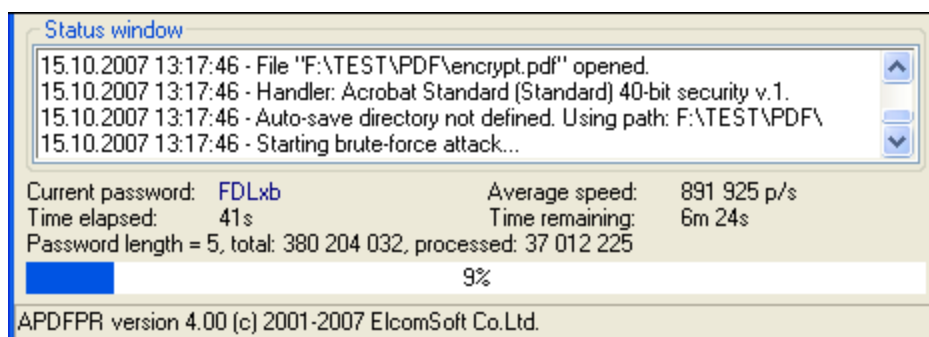
4.9.3.5.1 Recovering process

When all of the options are selected, all you have to do is press the Start button on the toolbar (or F9 key) and wait. During the attack, you'll be able to see the [Program status](#) – number of passwords already tried, elapsed and estimated time, etc.

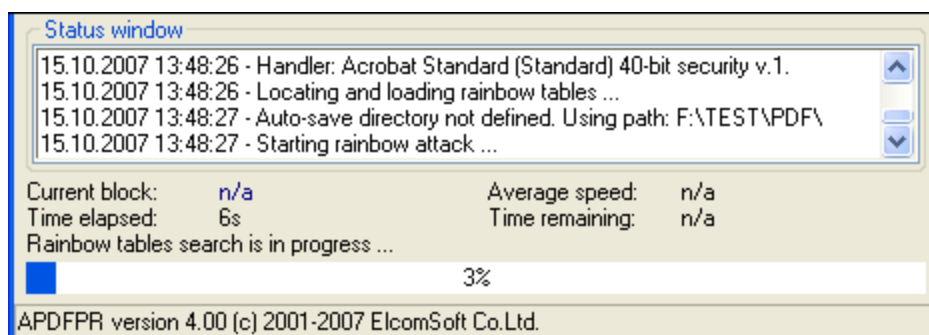
Please note that you can stop the recovering process at any time (Stop button or F10 key), to continue it later (or just save the project). Consult the [Start from password](#) and [Save and Read setup](#) chapters for further details.

4.9.3.5.2 Program status

When the recovering process is in progress – the current password, average speed, elapsed time, remaining time, total number of password of given length, and number of passwords already processed are displayed:

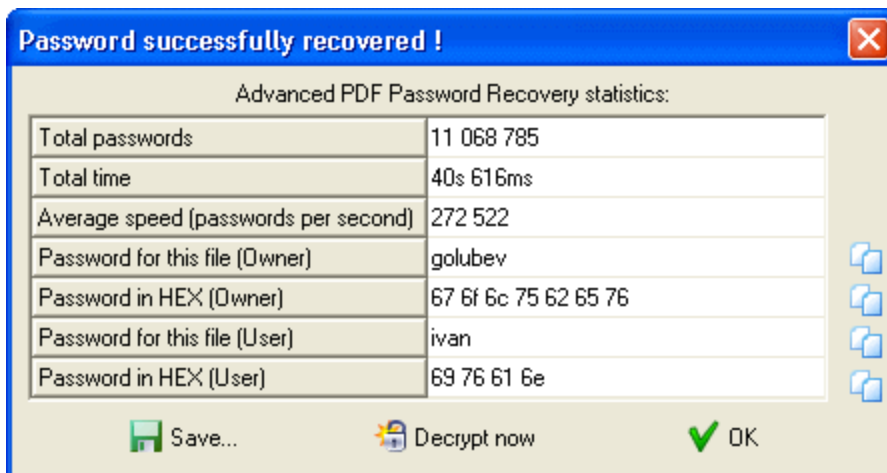


For key search attack using pre-computed hash tables, it is not possible to estimate the time due to the nature of this method, so only elapsed time is shown (however, this attack usually takes a few minutes):



4.9.3.5.3 The password is...

When (if) the password is found, the program shows it, as well as the number of passwords which have been tested, and the program speed:

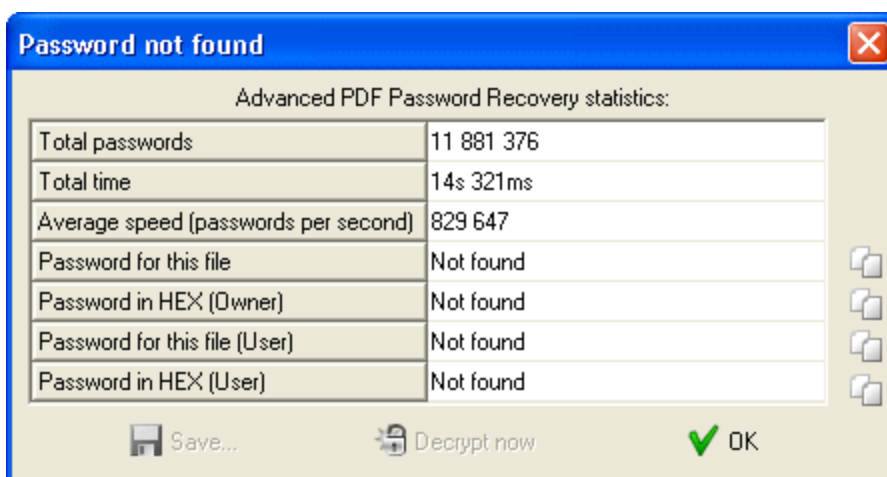


The last line displays the password in HEX form – it might be useful if the password, for example, contains some non-English characters which cannot be displayed correctly on your system (due to missing fonts, etc.).

Pressing the small button at the right of the password (in "normal" or HEX form) copy the password into the Clipboard. Alternatively, you can save the password to a file.

The program also shows the "type" of the password which has been found – "user" or "owner". And from that window, you can decrypt/unprotect the file immediately (using the recovered password, doesn't matter what particular one): press the Decrypt now button for that (you'll be prompted for target file name).

If all possible passwords in the given range have been tried without success (without finding a valid one), the message looks like:



If you stopped recovery by pressing the "Stop" button, the current step of the brute-force attack is saved in the "Start from" field (for key search attack, in "Start block"). Now you can press the "Start" button again. Recovery will be continued from this step.

With the key search attack, the password is not recovered at all, but the program shows the file encryption key – to remove the password (and so the protection) from the given file, simply press Decrypt now button:



4.9.4 Tips & tricks

4.9.4.1 What to start from

If you have no idea how long the password is and what characters it may contain, just run the dictionary-based attack first. If it fails, try brute-force attack up to 5-7 characters (depending on your computer speed, character set, PDF version etc); to estimate the speed of your computer (on your particular PDF file with the given settings), just use the [Benchmark](#) feature.

If brute-force attack also fails, you can try to use other (larger) wordlists and/or play with brute-force attack settings. But if your file uses 40-bit encryption, it is recommended to run the [Key search attack](#) – with it, success (decryption) is guaranteed, though it may take a few days. Using the pre-computer hash tables (available with APDFPR Enterprise), though, decryption is being done in just a few minutes.

4.9.4.2 Command line

You can run APDFPR with command-line parameters. You can use command-line switches for either batch processing (to remove restrictions from PDF files, when 'user' password is empty or known, or to perform attacks on 'user' or 'owner' passwords (for single file).

Batch processing

For batch processing, the command line looks like the following:

apdfpr.exe -batch src_path [dest_path] [options]

Please note that -batch parameter is mandatory here; without it, the command line will be parsed the different way (for user/owner password recovery, see below).

src_path	Path for source file(s); wildcards are allowed.
dest_path	The location of the folder to put decrypted files to (must already exist). If not specified, source path is used.
-b	Create backup copies of files being decrypted. Ignored if dest_path is not equal to src_path.
-p=xxx	If the program encounters the file which is locked from opening (with "user" password set), it tries to decrypt it using the given password ("xxx").
-q	Quiet mode; ignores the files with "user" password, if one specified in -p option doesn't match, or -p option is not supplied at all.
-t	Maintain the decrypted file date/time same as the original.
-l=log_path	Creates a log file ("log_path"; should be a file name).
-w	Close program when all files are processed, main window is not being shown at all; last error is being returned (or just 0 if no errors occurred).

The parameters enclosed in square brackets are optional; the only mandatory parameter is the source path.

If src_file starts with @ character, it is treated as a name of the file that contains a list of PDF documents to be processed (one per line).

If source or destination path contain spaces, it has to be included in double quotes.

The password may contain any special characters, but they have to be represented in hex form with % prefix. For example, the space is represented as 20 in hex, so if the password is "my pass", the appropriate command line option would be:

-p=my%20pass

The % character itself should be replaced with %25.

-w option could be used if you would like to execute APDFPR from your own software, but want the main program window not to appear on the screen (please note that if -p or -q option is not specified, but file with user password will be encountered, the program will still prompt for the password). When all files specified in the command line will be processed, APDFPR terminates with an appropriate [error code](#).

-l option instructs the program to create a log file (describing all the program is doing, error messages etc). If the file already exists, APDFPR appends to it (writes at the information at the

end). If the path to the file contains spaces, it should be shielded with double quotes (see examples below). Please note that if you select src_path as *.* , log file could not be created in the same folder where the source file are, because the name of the log file will also match the given mask, and so APDFPR will try to process it as a PDF file. Just use the mask like *.PDF, and/or create the log file in a different folder.

Examples:

```
apdfpr.exe -batch doc??.pdf
```

```
apdfpr.exe -batch "c:\my documents\manuals\*.pdf" "c:\my documents\decrypted\" -q
```

```
apdfpr.exe -batch @list.txt -b -p=LockSmith -w -l="C:\Program Files\apdfpr_log.txt"
```

User/owner password recovery

Generally, the syntax is:

```
apdfpr.exe [switches] [pdf-filename]
```

If you already have the "project" (e.g. saved from past attack), you can use the project name instead of PDF file name:

```
apdfpr.exe [switches] [afr-filename]
```

The switches are separated with / or - characters. If the switch is followed by some data (e.g., filename, starting password, etc.) which contains these characters: space, semicolon, slash or dash, it must be enclosed in (single or double) quotes.

Switch	Description	Default
/a:b m d	attack type (brute-force, mask, dictionary)	brute-force
/pass:u o a	password to find (user, owner, any)	user
/nommx	don't use MMX instructions	disabled
/c:csdepa	character set (caps, small, digits, special, space, all)	caps
/u:chars	user-defined charset	
/sf:pass	start from password	
/m:mask	mask	

/ms:C	mask symbol	?
/min:N	minimum password length	1
/max:N	maximum password length	5
/d[:filename]	dictionary filename	
/sm	smart mutations	disabled
/ac	try all possible upper/lower case combinations	disabled
/sl:N	start from line N	0
/autosave:N	autosave every N minutes; 0 means disabled	5
/aname:filename	autosave filename	
/adir:dir	autosave directory	
/idle	run at idle priority	enabled
/high	run at high priority	disabled
/dontstart	don't start the attack, just load/set the parameters	
/minimize	minimize the program after starting the attack	
/smartexit[:filename]	when the attack is completed, write all statistics, including the password (if found) to the given file (default "cmdline_stats.txt"), and close the program	disabled

Examples:

apdfpr.exe /a:b /pass:u /c:cs /min:3 /max:7 /smartexit test.pdf

(brute-force attack; user password; small and capital letters; length from 3 to 7; save and exit when done)

apdfpr.exe /a:b /u:12345abcde test.pdf

(brute-force attack with "12345abcde" character set; length: from 1 to 5)

apdfpr.exe /a:m /pass:a /c:d /m:june???? /sf:june1000 /high test.pdf

(mask attack with ""june????" mask; any password; charset: digits; high priority)

apdfpr.exe /d:english.dic /sm /dontstart test.pdf

(dictionary attack; dictionary: "english.dic"; smart mutations; convert words from ANSI to OEM; don't start)

If the parameter is the afr-file, the program will immediately load all the settings from it (ignoring the other settings supplied in the command line, except /dontstart, /minimize and /smartexit), and run the attack.

4.9.4.3 Error messages

When there is a problem with PDF files you're trying to decrypt, APDFPR shows some kind of error message which looks like:

Can't open file C:\My documents\report.pdf. Error 105

Here is the explanation of the error codes:

		Error code	Error description
0		PDFERR_OK	No errors
1		PDFERR_NO_STARTXREF	No reference to objects table
2		PDFERR_BAD_STARTXREF	Invalid reference to objects table
3		PDFERR_NOREF	No objects table
4		PDFERR_BAD_XREF	Invalid objects table
5		PDFERR_NO_TRAILER	No document trailer
6		PDFERR_BAD_TRAILER	Invalid document trailer
7		PDFERR_NO_OBJ	Cannot find object
8		PDFERR_BAD_OBJ	Invalid object format
9		PDFERR_NO_ENDOBJ	Cannot find the end of the object
10		PDFERR_UNEXPECTED_LEX	Unexpected lexem encountered
11		PDFERR_NAME_EXPECTED	No name
12		PDFERR_NO_TRAILER_DICT	No trailer dictionary
13		PDFERR_NO_STREAM_DICT	No stream dictionary
14		PDFERR_NO_STREAM_LEN	No stream length
15		PDFERR_BAD_STREAM_LEN	Invalid format of stream length
16		PDFERR_NO_ENDSTREAM	Cannot find the end of the stream
20		PDFERR_NO_LEX	Lexem not found
21		PDFERR_UNK_LEX	Unknown lexem encountered
30		PDFERR_BAD_NUMBER	Invalid number format
31		PDFERR_BAD_STRING	Invalid string format
32		PDFERR_BAD_HEXSTR	Invalid hexadecimal string format

33		PDFERR_BAD_NAME	Invalid name format
34		PDFERR_BAD_KEYWORD	Invalid keyword format
35		PDFERR_UNK_KEYWORD	Unknown keyword
101		PDFERR_ALREADY_OPENED	Document already loaded
102		PDFERR_CANT_OPEN	Cannot open document
103		PDFERR_CANT_CREATE_MAP	Cannot map file
104		PDFERR_CANT_MAP_VIEW	Cannot view file map
105		PDFERR_NO_HEADER	No PDF file header
1001		PDFERR_NO_ENCRYPT	Document is not encrypted
1002		PDFERR_NO_PDEF	Document is not loaded
1003		PDFERR_BAD_REF	Wrong reference to Encryption Object
1004		PDFERR_BAD_OBJ	Invalid Encryption Object
1005		PDFERR_WRONG_FILTER	Unsupported Encryption Filter
1006		PDFERR_WRONG_VER	Unsupported Encryption Version
1007		PDFERR_WRONG_REV	Unsupported Encryption Revision
1008		PDFERR_WRONG_OWNER	Invalid OwnerKey format
1009		PDFERR_WRONG_USER	Invalid UserKey format
1010		PDFERR_WRONG_PERM	Invalid Permissions format
1011		PDFERR_NO_ID	Cannot find DocumentID
1012		PDFERR_BAD_ID	Invalid DocumentID format

4.10 Advanced Sage Password Recovery

4.10.1 Introduction

Using Sage PeachTree Accounting or ACT! Personal Information Manager manufactured by Symantec, Best Software, Sage or Swiftpage? View user and Admin passwords in Sage PeachTree Accounting and get instant access to password-protected ACT! documents - guaranteed! Advanced Sage Password Recovery works locally and remotely, and does not require local access in order to recover a password. Run Advanced Sage Password Recovery from any networked computer with an access to the password-protected remote database to instantly unlock its password!

Get access to locked Sage PeachTree Accounting databases by retrieving user and administrative passwords in an instant. Advanced Sage Password Recovery displays all user and Admin passwords in all versions and editions of Sage PeachTree Accounting no matter

how long and complex the passwords are. Viewing the passwords in plain text takes just a moment – guaranteed! The program also supports Sage 50 Accounts, Sage Instant Accounts and Sage Simply Accounting.

Recover or replace passwords protecting BLB, MUD and ADF/PAD files created with ACT! software suite locally or remotely. Advanced Sage Password Recovery instantly reveals passwords protecting documents saved by all versions of ACT! including the latest version (v22). Upgrading user accounts from Restricted to Administrator in ACT! Databases by changing user security roles.

Get instant control over password-protected ACT! documents - guaranteed. Advanced Sage Password Recovery will show the passwords in plain text instantly at any time regardless of their length, complexity, or encoding. No lengthy attacks or advanced settings are required! Just open a document with Advanced Sage Password Recovery, and you'll be able to reset or see the password that very moment!

Advanced Sage Password Recovery saves your time and provides guaranteed instant results every time you use it. Act now and get your documents unlocked!

4.10.2 Program information

4.10.2.1 System requirements

- Windows 7 or higher

4.10.2.2 ACT! password recovery

To recover passwords to files created in older versions of ACT! (from [Symantec](#)), press Open file... button on toolbar and select Symantec ACT! menu item, then browse for *.blb or *.mud files you want to get the password(s) for; alternatively, you can drag ACT! file from Explorer and drop it into the ASAPR window). If the given file is corrupted, or used by another application, or no passwords are there – appropriate error message will be displayed. Otherwise, the program will print a list of all users that have the rights to access that file, along with there passwords and security levels/roles (examples: Administrator, Standard, Manager, Browse, Restricted). Here you can highlight the account you need, and press Copy password button at the bottom; password for selected account will be copied into the clipboard, so you can paste it into ACT using Ctrl+V or Shift+Ins button. That might be useful if password is not "printable", i.e. cannot be shown/entered using current character set or keyboard layout. Or press Change Level button to just change the security level for the selected user.

ACT! 2005..2020 (from [Best Software/Sage/Swiftpage](#)) are based on Microsoft SQL Server Engine, and the encryption is much stronger there: passwords cannot be recovered instantly. However, they can be changed or removed. ASAPR provides two ways doing that: through

ACT! itself (more exactly, via MSSQL ODBC drivers used by ACT!), and directly. In order to use the first method, you should have appropriate version of ACT! installed on the local machine, while the *.adf file can be accessed remotely; the second method works even without ACT! , but does not allow to change the security roles.

With the first method, press Open file..., select ACT! 2005-2020 ODBC menu item and browse for *.adf file (ACT! database itself) or *.pad file (that one contains information about ACT! database which may be located on the other computer in the local network). ASAPR shows (like for older versions of ACT!) the list of users with their security roles. Highlight the one you want to change the password for, press Change password button, and enter new password for that user (empty one means that the password will be removed); here you can also change the security role of the selected user.

If you are going to process (with ASAPR) the ACT! database on the computer other than one this database has been accessed the last time at, it is recommended to open it on this (new) computer in ACT! itself first. Don't worry that the password is not known. Simply wait till ACT! asks for password and press Cancel -- so the ACT! will make some changes to configuration files. Now open the database in ASAPR to change the password(s). Otherwise (if you have not opened the database at the new computer before using ASAPR), the program might be confused where the actual database file is located, and so don't work properly.

With the second method, select ACT! 2005-2020 Direct menu item and browse for *.adf file (ACT! database itself). If the file is locked by ACT!, ASAPR allows to stop the SQL service -- without that, the file cannot be accessed/unlocked. Then, the program works almost exactly as with the previous method, but just does not allow you to select the new password (for selected user) yourself; instead, it generates the new password by itself.

Please also note that if you work with ACT! 2005..2020 and change the password to any user, the new passwords is always being converted to the lowercase for compatibility with ACT! 2005 (where the passwords are not case-sensitive), while it is not possible to determine what version of ACT! is used. Also, after changing the password, ACT! will accept it at the first time when you log on to ACT! with that (new) password, but may ask to change it according to the password policy set (which ASAPR does not care about).

Finally, ACT! (most versions) may save the password (last one you used to open the file) in system Registry. ASAPR can extract and decrypt it from there: simply press the Check Registry button on program toolbar. If last password has been saved, it will be shown.

4.10.2.3 PeachTree/Accounting password recovery

Press Open file... button on toolbar and select one of the following items (depending on the specific product):

- 50 Accounting (Peachtree)
- 50 Accounts
- 50 Accounting Canadian Edition (Simply Accounting)

For Peachtree, browse for PERMISS.DAT file from PeachTree database you want to recover the password(s) for. The list of user names and their passwords will be shown.

For Sage 50 Accounts (formerly Sage Line 50) and its simplified version (Sage Instant Accounts), only password to special (built-in) MANAGER user is being recovered; but being logged as this user, you will be able to view or change the passwords for all other users as well. Browse for SETUP.DTA file that is located in appropriate company folder; the password will be recovered instantly.

For Sage Simply Accounting, passwords of all users are being recovered. For versions from 2008 and up, they're stored in ibdata1 file; for older versions -- in *.SDW file. These files are also located in appropriate company folder; browse for the proper one (according to the version), and passwords for all users will be shown.

4.10.2.4 Other Sage products

Sage 50 Accounts (formerly Sage Line 50) and its simplified version: Sage Instant Accounts. Only password to special (built-in) MANAGER user is being recovered; but being logged as this user, you will be able to view or change the passwords for all other users as well. Press Open file... button on toolbar and select 50 Accounts 2004..2019 menu item, then browse for SETUP.DTA file that is located in appropriate company folder; the password will be recovered instantly.

For Sage Simply Accounting, passwords of all users are being recovered. For versions from 2008 to 2011, they're stored in ibdata1 file; for older versions -- in *.SDW file. The files are also located in appropriate company folder; press Open file... button on toolbar and select 50 Accounting (Peachtree) 2002..2020 menu item, then browse for one of the files mentioned above (according to the version). Passwords for all users will be shown.

4.11 Advanced SQL Password Recovery

4.11.1 Introduction

Get instant access to password-protected SQL Server databases - guaranteed! Advanced SQL Password Recovery can change any user or administrative password protecting databases in Microsoft SQL Server 2000-2019 formats. Advanced SQL Password Recovery works with or without SQL Server installed. The password recovery tool accesses the master.mdf file directly, whether or not SQL Server is running or installed.

Advanced SQL Password Recovery offers convenient single-click operation with no configuration or advanced settings to change. If you have MS SQL running, Advanced SQL Password Recovery will automatically detect and stop the service. If you have multiple

instances of MS SQL Server, Advanced SQL Password Recovery will still locate and stop the service.

Advanced SQL Password Recovery is completely safe to operate. The password recovery tool makes a backup of your original database automatically. No matter how long and complex the passwords are, Advanced SQL Password Recovery can replace or reset these passwords in an instant. No lengthy attacks or advanced settings! Advanced SQL Password Recovery will easily replace international passwords in any language and any encoding.

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our software or have permission from the legitimate owner to perform these acts. Any illegal use of our software will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

You further attest that the recovered data, passwords and/or files will not be used for any illegal purpose. Be aware password recovery and the subsequential data decryption of unauthorized or otherwise illegally obtained files may constitute theft or another wrongful action and may result in your civil and (or) criminal prosecution.

4.11.2 Program information

4.11.2.1 System requirements

- Windows 7 or higher

4.11.2.2 Working with ASQLPR

Microsoft SQL Server Engine uses strong encryption, and passwords cannot be recovered instantly. However, they can be changed or removed. Press Open file...and browse for master.mdf file. ASQLPR shows the list of users; highlight the one you want to change the password for, press Change password button, and enter new password for that user (empty one means that the password will be removed).

Important: MSSQL can use two different authentication modes (to be selected during setup): Windows Authentication mode and mixed mode. Windows Authentication mode enables Windows Authentication and disables SQL Server Authentication. Mixed mode enables both Windows Authentication and SQL Server Authentication. When using SQL Server Authentication, logins are created in SQL Server that are not based on Windows user accounts. Both the user name and the password are created by using SQL Server and stored in SQL Server. Users connecting using SQL Server Authentication must provide their credentials (login and password) every time that they connect. Please note that ASQLPR works only with databases that use mixed mode, i.e. SQL Server Authentication.

4.12 Advanced WordPerfect Office Password Recovery

4.12.1 Introduction

Are you a [Corel WordPerfect Office](#) user? Did you password-protect a Paradox database? Did you forget a password from a Quattro Pro spreadsheet? Regain access to password-protected Corel WordPerfect Office documents and accounts in an instant!

Advanced WordPerfect Office Password Recovery (AWOPR) guarantees password recovery by quickly revealing passwords protecting documents created with any version of Corel WordPerfect Office (up to Office X5), as well as Corel WordPerfect Lightning account passwords. Reveal passwords of any length and complexity from WordPerfect, Quattro Pro and Paradox documents instantly. The simple and straightforward user interface provides easy access to the most complex passwords in any language.

Corel provides the ability to protect WordPerfect Office documents with a password, but offers no tools to recover the locked documents when you lose or forget your password. Advanced WordPerfect Office Password Recovery fulfills the demand of the many Corel WordPerfect users, offering a perfectly usable tool to recover password-protected documents and accounts. Save your time and get guaranteed results with Advanced WordPerfect Office Password Recovery!

4.12.2 System requirements

- Windows XP or higher
- about one megabyte of free space on hard disk

4.12.3 Working with AWOPR

Simply select the file you want to recover the password(s) for. Press the Open file button, then select Wordperfect Office menu item and browse for appropriate file (alternatively, you can use drag-and-drop: select the file in Windows Explorer, drag it to AWOPR window holding the left mouse button, and drop there). If the specified file format is not supported by AWOPR, or it's corrupted, or used by another application, or not password-protected – appropriate error message will be displayed. Otherwise, the program will recover and show the password.

WordPerfect

For WordPerfect 5.x files, the password is always being recovered instantly, but only if doesn't contain non-US characters. If it does, it is not possible to recover the password at all, but AWOPR can decrypt (also instantly) the file, so you will be able to open it in WordPerfect without supplying the password. The program will prompt you for file name (to save the new/decrypted file).

For WordPerfect 6.x..13 files, two encryption/protection modes are supported: original and enhanced. For original mode, recovery process are divided into two stages: searching for encryption keys and searching for password. The first one usually takes just a few seconds or sometimes minutes, depending on the character set used. The following character sets are supported (as defined by WordPerfect itself): ASCII, Multinational, Cyrillic, Greek and Hebrew (AWOPR tries them consequently); when/if the appropriate encryption codes are found, the program starts searching for the password, and that (second) stage usually takes more time (up to 10-15 minutes). Sometimes, however, it is not possible to detect what particular character set has been used, and so get the password itself; so AWOPR allows to do about the same as for 5.x files, i.e. find the appropriate encryption key and so decrypt the whole file. Unfortunately, that takes much more time (a few hours maximum), but success is guaranteed. During that process, AWOPR saves its state on a regular basis, and so it is safe to press the Stop button or even close the program – next time when you open the same file, the program will prompt you to resume the recovery process.

For enhanced encryption mode (versions 6.x through X5/15), AWOPR can decrypt passwords of any length, containing any characters (from the character sets mentioned above) in any combination – in most cases, almost instantly. However, if the password is very long and contains symbols from different character sets, recovery process may take more time (but up to 10-15 minutes, as for original encryption mode).

Paradox

In most cases, the password recovered by AWOPR is 8 characters long, and not the same as the original one set in Paradox. That's just to the nature of encryption algorithm used in Paradox, and we cannot do anything with that. However, the password returned by AWOPR will work just fine on your database, i.e. Paradox accepts it as an original one.

Another note: though most passwords are being recovered instantly, there are some ones that AWOPR needs a few seconds to get (up to 20-30 seconds on slow machines). Recovery time doesn't depend on the password length, though.

QuattroPro

QuattroPro encryption is weak, and so the password is being recovered instantly regardless the length and QuattroPro version. Sometimes, however, the passwords contain non-printable characters – they are still being recovered by AWOPR, but cannot be entered from keyboard in QuattroPro. So AWOPR not only shows such passwords, but also allows to decrypt such files (so the password is being removed completely); this step is optional.

WordPerfect Lightning

To get the data associated with your WordPerfect Lightning account (Domain, User name and Password), press Open file button and select WordPerfect Lightning menu item. Then, browse for *.ini file which is located in your user profile at:

%Documents and Settings%\<user name>\Application Data\Corel\WordPerfect Lightning

Please note that password can be recovered only if it is saved (i.e. if Remember my password option in WordPerfect Lightning was checked), and only when you are logged into the system under the same (Windows) user account your WordPerfect Lightning account was accessed from.

4.13 Elcomsoft Internet Password Breaker

4.13.1 Introduction

Elcomsoft Internet Password Breaker instantly reveals passwords to Web sites, identities, and mailboxes stored in a variety of applications. Supporting all versions of Internet Explorer, Microsoft Edge Chromium, Microsoft Edge Legacy, Firefox, Safari, Chrome, Opera, Yandex, QQ Browser, UC Browser, Tor Browser, 360 Safe Browser and all versions of Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail, Elcomsoft Internet Password Breaker helps you retrieve the login and password information to a wide variety of resources.

Get access to hidden information stored in popular Web browsers! Elcomsoft Internet Password Breaker will retrieve logins and passwords to Web sites, reveal AutoComplete information including login forms. Apple Safari, Google Chrome, Mozilla Firefox and Opera passwords are a one-click affair. For Internet Explorer 7+, the tool allows analyzing URL history to identify Web sites last visited and retrieves password information stored for those Web sites. IE password recovery will retrieve stored passwords and AutoComplete information to all Web sites, including webmail clients, Amazon, LinkedIn, LiveJournal, and a variety of social networks.

Elcomsoft Internet Password Breaker extracts stored password information from Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail, including Microsoft Passport passwords. The password recovery tool allows you to access all types of mail account passwords, including passwords protecting POP3, IMAP, SMTP and NNTP accounts, as well as passwords protecting user identities. For all versions of Microsoft Outlook, Elcomsoft Internet Password Breaker will also retrieve passwords to mail accounts and passwords protecting PST files.

If there is more than one product installed on the PC, or more than one user identity exists, Elcomsoft Internet Password Breaker will automatically locate all identities and all PST files and recover all passwords to all installed products automatically.

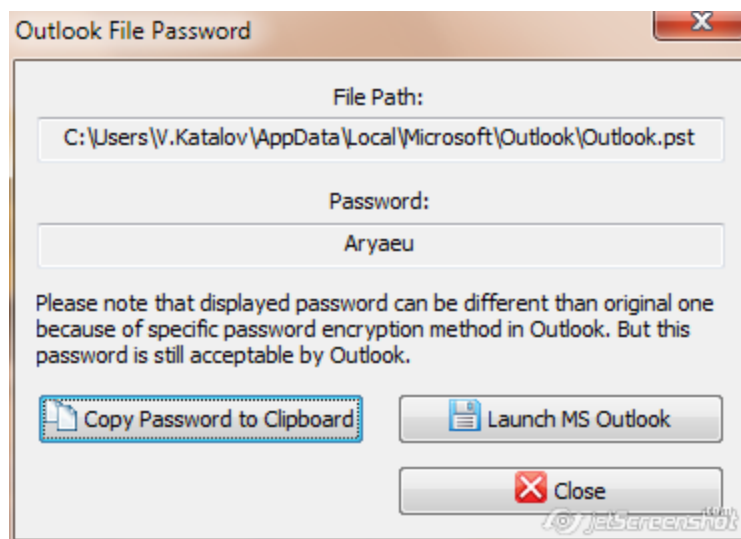
4.13.2 Program information

4.13.2.1 System requirements

- Windows XP or higher
- Internet connection (for Loading web pages from IE history option)

4.13.2.2 Outlook PST password

To get password to PST file (Outlook versions supported: 97, 98, 2000, 2002/XP, 2003, 2007, 2010, 2013, 2016, 2019), simply select the file you want to recover the password(s) for: press the Open PST file button and select an appropriate PST-file. If the given file is corrupted, or used by another application, or not password-protected – appropriate error message will be displayed. Otherwise, the password will be recovered immediately, shown in the message box and written to the log window. You can copy recovered password to Clipboard and run Outlook just from EINPB, put the cursor into the password box, and press Ctrl-V or Ctrl-Ins there to paste the password from the Clipboard (to avoid mistyping).

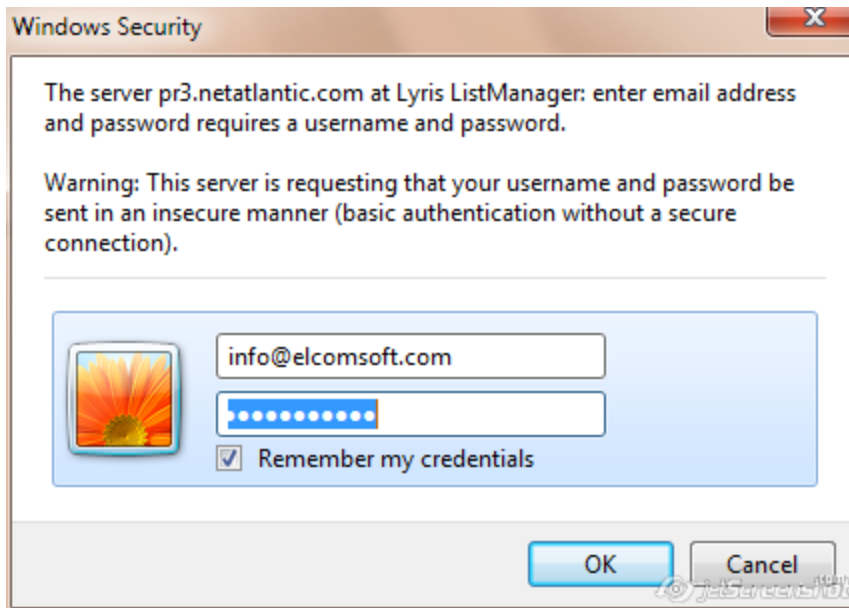


Please note that in some cases, the password recovered by EINPB is not the same as the one which has been originally set. That's due to encryption algorithm used in Outlook – the original password is not stored in the file. But that password (shown by EINPB) will be accepted by Outlook without problems – just try. And of course, after logging into Outlook, you'll be able to change that password to any one, or just remove it.

4.13.2.3 Internet Explorer passwords

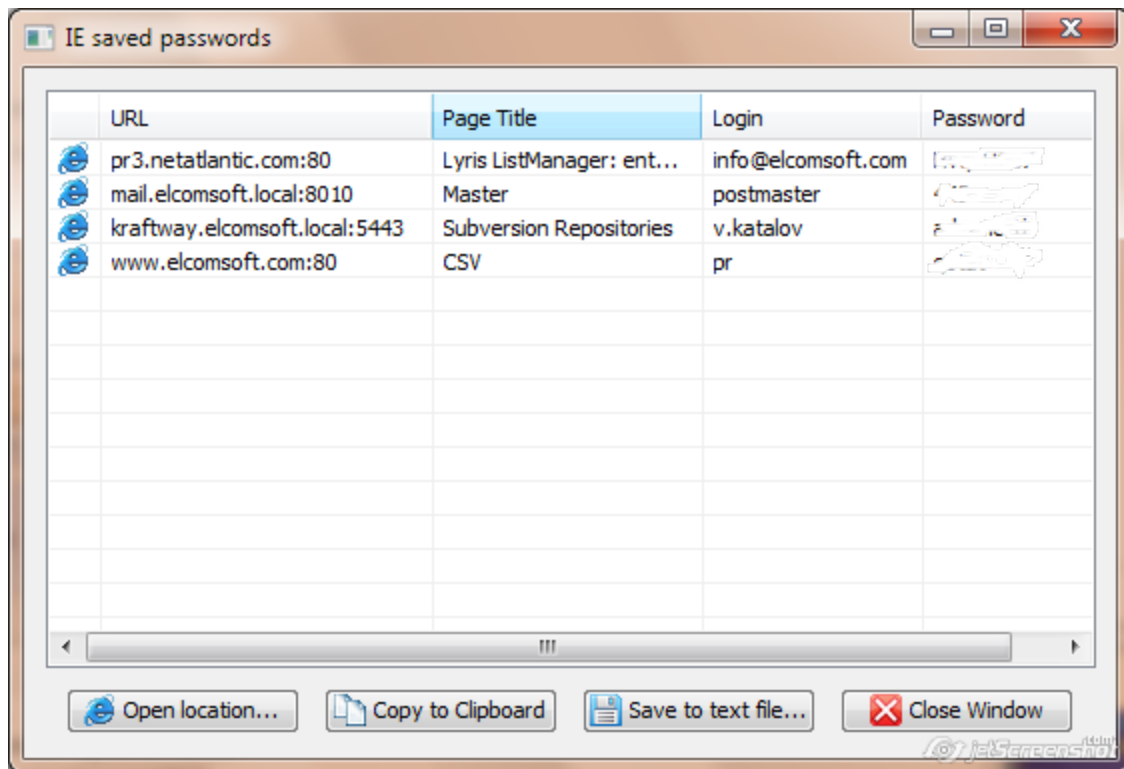
IE Passwords

When you enter to password-protected Internet site (or specific page) using Internet Explorer, it shows the following prompt:



If Remember my credentials option is enabled, and login/password you supplied are correct, the password will be saved (encrypted) in Windows Registry (for older versions of Internet Explorer) or in special files (encrypted) the hard disk (for IE7 and IE8). So next time you will try to access the same page, your login will be already there, but the password will be hidden under the asterisks.

To get a list of all passwords you have saved, press Web Passwords button on the toolbar and IE Password, or select Web Explorer | IE Passwords menu item (actual passwords have been removed from that picture):



That window has the following columns:

URL: just the address of the site. Please note that in most cases it is not the full address, but just the "root" of the site; the actual URL is not saved in the system at all, and so it cannot be retrieved.

Page Title: actually, it is a Realm that is being set by the server. For FTP sites, it is always empty; for web sites it is typically the title of password-protected page, or sometimes the name of HTML file.

Login: just what it says; the name.

Password: the password (for the user shown in Login).

When any of the passwords is selected (highlighted), you can use the buttons at the bottom of that window:

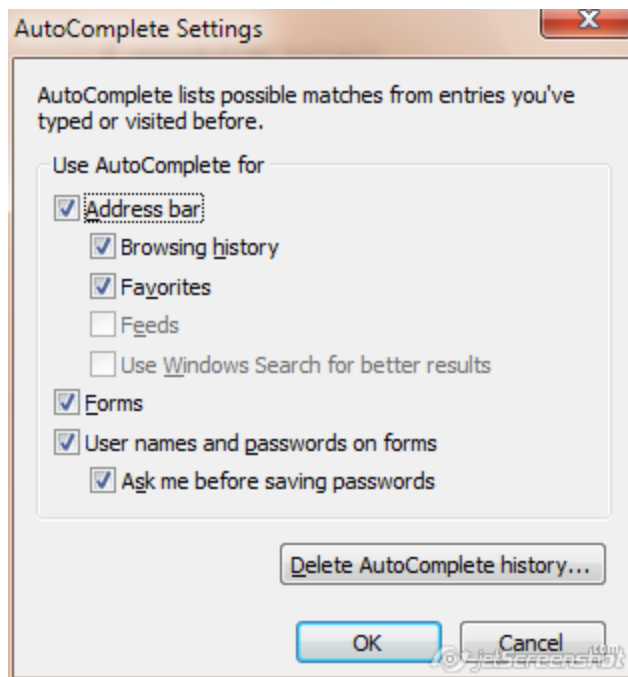
Open location: shows pop-up menu with the type of the connection (FTP, HTTP or HTTPS). Select an appropriate one, and Internet Explorer will go to that page, applying login and password automatically. Please note that sometimes it doesn't work (due to the server problems), so if you fail, type the URL and supply login and password (when prompted) manually.

Copy to Clipboard: copies selected password to the Clipboard; press Ctrl-V to paste it where needed.

Save to text file...: saves the list of all passwords (together with URL and logins) to specified file.

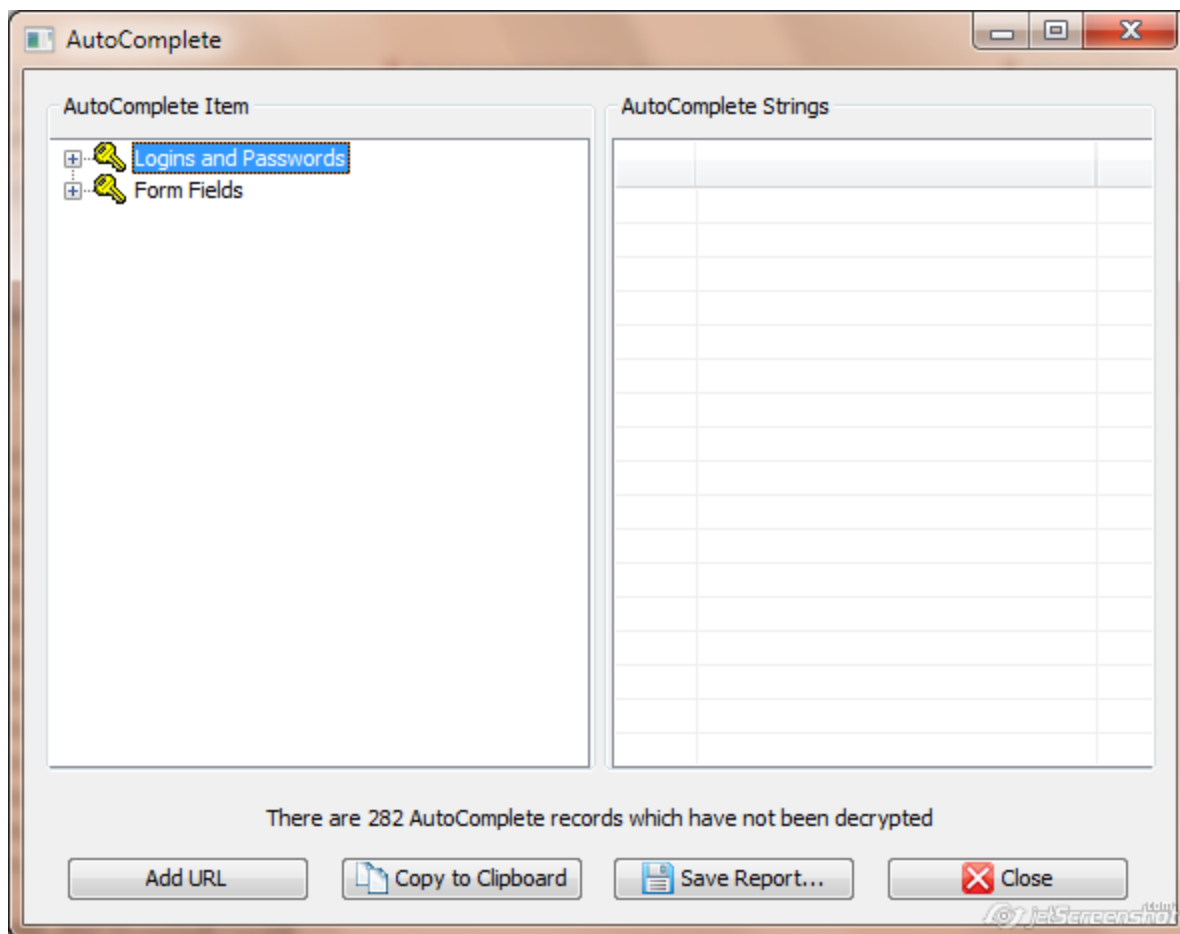
IE AutoComplete

Most versions of Internet Explorer have an AutoComplete feature. To enable it, select Tools | Internet Options menu item, go to Content tab, and Settings button in AutoComplete:



Here you can enable the AutoComplete for Forms and User names and passwords on forms.

EINPB can show all that (saved) information: just press the Web passwords | IE AutoComplete button on the toolbar, or select Web browsers | IE AutoComplete menu item:



Please note that if you have too much saved AutoComplete strings (a few hundred), you may have to wait (usually, for a few seconds) for that window to appear. Note: if Loading web pages from IE history [option](#) is enabled, this process may take much longer (especially on slow Internet connections).

For every entry under Logins and Passwords node, you will see one or two lines in the right window. The first one indicates the login name, and the second one – the password. If there is only one, it means that the password has not been saved.

Under the Form Fields node, field names are shown; for every one, the right window shows the list of strings you ever typed into that field (Internet Explorer saves them all).

Copy to Clipboard button allows copying the selected (at the right) login, password or saved string into the Clipboard.

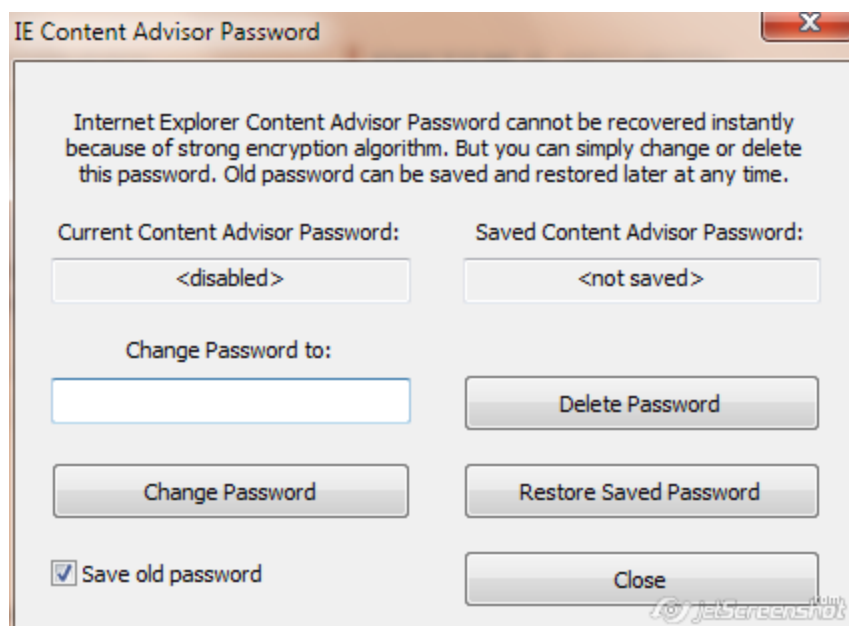
Save Report button could be used for saving all AutoComplete information into the text (UNICODE) file.

If passwords to some web sites have not been shown here (even if Enable loading from web pages [option](#) is enabled), it does not mean that it have not been saved; probably, the URL of these pages just not known to the program (while they should be, for successful decryption). But you can use Add URL button and enter an appropriate link manually; if the password is saved for it, it will be decrypted and shown.

IE Content Advisor

Microsoft Internet Explorer includes Content Advisor that helps to control the Internet content that can be viewed on your computer. To enable it, select Tools | Internet Options, go to Content tab, and press Enable; you will be prompted for supervisor password. Now you can press the Settings button to select ratings, approve or disapprove specific sites, and change the password itself.

If you forgot the supervisor password to IE Content Advisor, it cannot be recovered (because it is not saved at all, just hashed), but EINPB allows to remove or change it. Press Advisor button on toolbar (or Web Browsers | IE Content Advisor menu item):



The Current Content Advisor Password field should be shown as <enabled>. Now you can change the password to your own one, or just delete it. If you want to be able to restore the old password, enable the Save old password option (and use Restore Saved Password later, when/if needed). Once you have the new password, you can go to Content Advisor and disable it completely, or just change its settings.

Please note that the password should be changed and deleted when Internet Explorer is not running; also, in some cases you will have to restart your computer for the changes to take effect.

4.13.2.4 Other browsers

EINPB can recover passwords saved not only in Microsoft Internet Explorer and Edge, but in other browsers as well: Mozilla Firefox, Apple Safari, Opera, Google Chrome, Yandex, QQ Browser, UC Browser, Tor Browser, 360 Safe Browser. Simply select an appropriate item in Web Browsers menu, or from Web Passwords button on the toolbar.

Please note that in order to recover passwords saved in Mozilla Firefox, you should have Firefox itself installed. Also, these passwords should not be protected with the master password; if master password is set, you should remove it in Firefox settings first (or if that password is not known, you can try to recover it with [Elcomsoft Distributed Password Recovery](#)).

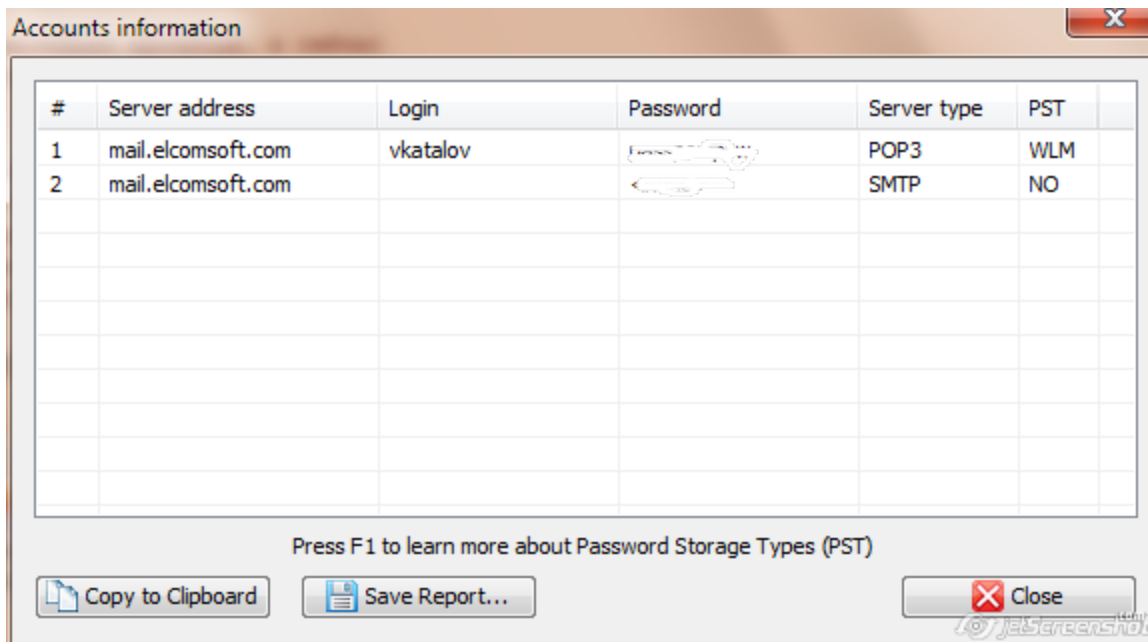
4.13.2.5 Mail and news passwords

There are three mail- and news-related buttons on the program toolbar:

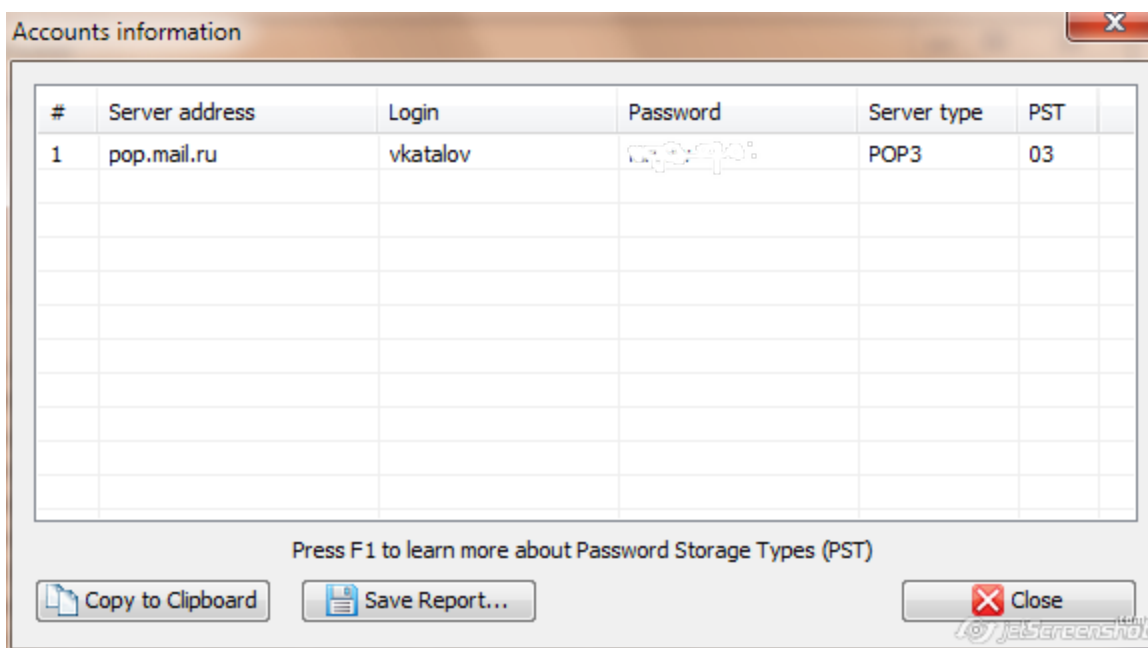
- mail accounts (Outlook Express, Windows Mail and Windows Live Mail, Outlook)
- news accounts (Outlook Express, Windows Mail and Windows Live Mail)
- identities (outlook Express)

Mail accounts

For every mail and news account, EINPB shows the server address, login and password; usually, last two fields are shown as <none> for news, which means that no login/password is required to connect to the given server (however, it might be available only if you connect to the Internet from particular ISP). Also, the program shows the server type (NNTP for news accounts; POP3, IMAP4, HTTP and SMTP for mail accounts) and [Password Storage Type](#). For Outlook Express and Windows [Live] Mail:

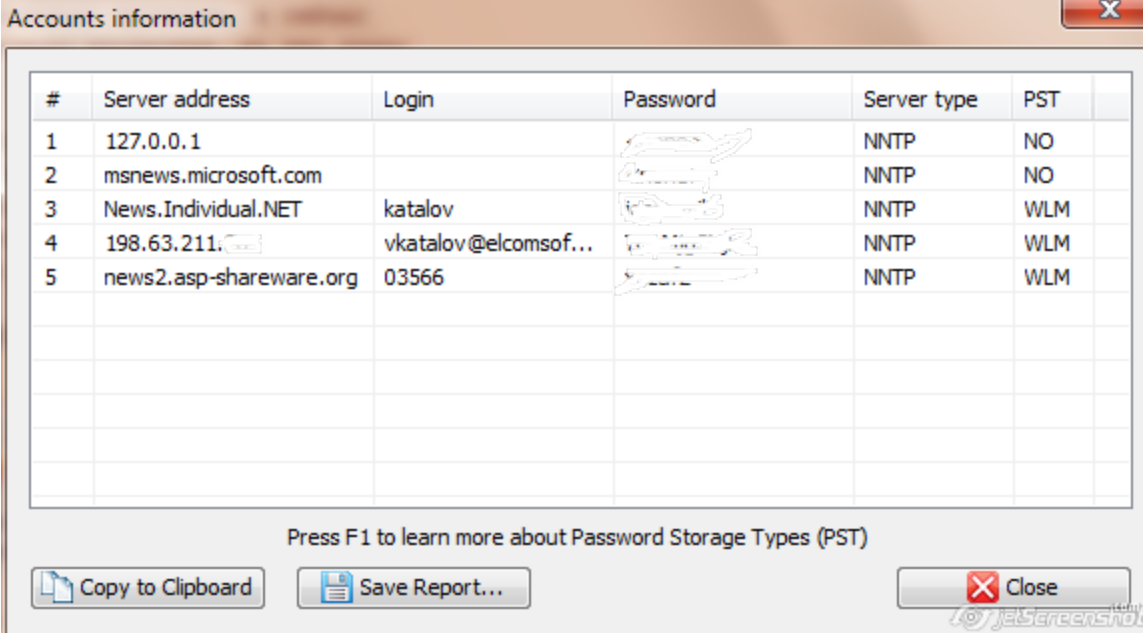


For Outlook 98, 2000, 2002/XP, 2003, 2007, 2010 and 2013 (sorry, Outlook 97 is not supported officially, while EINPB may work for it), you can also recover information about email accounts (server address, login, password and server type) stored in Outlook: press the second button on the toolbar: Outlook Accounts. If Outlook is installed in the system (and there is at least one email account there), EINPB will open new window with appropriate fields (see above). From there, for any account you can copy password to Clipboard by pressing an appropriate button at the bottom:



Also, the program shows the server type (POP3, IMAP4, SMTP or HTTP) and [Password Storage Type](#). Some information (describing what exactly the program is doing) is printed into the log window.

News accounts



The screenshot shows a window titled "Accounts information" with a table of news accounts. The table has columns for #, Server address, Login, Password, Server type, and PST. There are 5 rows of data. Below the table, there is a message "Press F1 to learn more about Password Storage Types (PST)" and three buttons: "Copy to Clipboard", "Save Report...", and "Close".

#	Server address	Login	Password	Server type	PST
1	127.0.0.1			NNTP	NO
2	msnews.microsoft.com			NNTP	NO
3	News.Individual.NET	katalov		NNTP	WLM
4	198.63.211.100	vkatalov@elcomsof...		NNTP	WLM
5	news2.asp-shareware.org	03566		NNTP	WLM

Identities

For Identities, EINPB shows the list of name/password combinations.

Some information (describing what exactly the program is doing) is printed into the log window. You can select (with mouse) some events there, press right mouse button and copy selected lines into the Clipboard using appropriate item in pop-up menu.

All information shown by EINPB (address, login password) can be save into the text file – use Save Report button.

If you experience any troubles when trying to get any passwords (for mail, news or identities), e.g. the program just crashes or does not show the password, you can use debug mode. To enable it, select Options | Settings menu item, check the Enable logging box, and select the path to log file (or just leave the default value). Then, try to recover the passwords again, and send us that log file. It does not contain your passwords, just some technical information (what does the program do: accessing particular Registry keys, reading and decryption data etc). It would really help us to locate and fix a problem.

4.13.2.6 Password storage types

Typically, Microsoft Outlook Express stores all passwords (in encrypted form) in the Protected Storage subsystem, in other Registry areas, or in special credentials files on hard disk). However, some old versions can store account passwords in a plain (unencrypted) form, or encrypted with weak algorithm (logical XOR operation). In some cases, EINPB can show wrong passwords, for example if your system Registry is damaged, or you do not have enough rights (permissions) to access some keys in Registry, or Protected Storage subsystem is not installed on your computer. Displaying of Password Storage Types will help you to identify why some passwords are displayed incorrectly. Here is a brief description of Password Storage Types:

PS	Password is successfully retrieved and stored in Protected Storage.
OL	Password is successfully retrieved and stored in system Registry using "old-style" weak encryption algorithm.
O97	Outlook 97; password is stored with MAPI.
NP	Password was not found in Protected Storage, in some cases it indicates that user name is used as password, or Protected Storage subsystem is damaged.
UN	Unknown Password Storage Type. You may use version of Outlook Express that is not supported by EINPB, or your system Registry is damaged.
ER	Error in password retrieving.
NR	Password was not retrieved. You do not have enough rights to unlock the Protected Storage, or Protected Storage is not installed on your machine.
NO	Password for this account is absent.
WM	Windows Mail
WLM	Windows Live Mail

If Storage Type is "UN", "ER" or "NR", please send your debug log (see Options) to ElcomSoft support.

4.13.2.7 Options

Enable logging option could be used if you experience any troubles when trying to get some passwords, or the program does not work as expected. Send us the log file generated by EINPB, and we will take care.

Enable Loading web pages from IE history option helps to recover contents of form fields (and so passwords) for [Internet Explorer](#). However, it will seriously slow down accessing this feature (parsing all IE history may take several hours), so please use it with care.

4.13.2.8 Report and Password list

If you are not sure what particular browsers are installed and can save everything that can be extracted, click Create Report on the tool bar or select [File] | [Create Report for All] from

menu. The process run completely unattended (just ignoring all errors that may occur), and once it completes, the program only asks for the file name to save address/login/password for all the entries found (from all supported browsers and mail clients found, just except autocomplete strings)

Alternatively, you can extract (also with just one click) all the passwords and generate the wordlist/dictionary from them (sorted, with no duplicates): click Export Passwords on the tool bar or select [File] | [Export Passwords] from menu. Only passwords will be saved, in unicode format, one per line; that wordlist can be used in password recovery software like [Distributed Password Recovery](#).

4.14 Elcomsoft Wireless Security Auditor

4.14.1 Introduction

Audit security of your wireless networks by attacking Wi-Fi passwords. Built-in Wi-Fi sniffer and GPU-accelerated recovery ensure the highest-performance attack on WPA/WPA2-PSK passwords. Elcomsoft Wireless Security Auditor (EWSA) supports dictionary attacks with an advanced variation facility. The built-in wireless sniffer supports general Wi-Fi adapters and AirPCap sticks. The tool can also accept standard tcpdump logs supported by any Wi-Fi sniffer.

Periodic audits of network security policies are necessary to ensure secure production environment. Wireless networks can only provide sufficient security when configured properly. Supporting both WPA and WPA2 security standards, Elcomsoft Wireless Security Auditor can audit all kinds of Wi-Fi networks by attempting to recover WPA-PSK (Pre-Shared Key) and WPA2-PSK passwords.

Elcomsoft Wireless Security Auditor comes with a custom-built Wi-Fi sniffer that can work on ordinary Wi-Fi adapters via a custom NDIS driver (32-bit and 64-bit versions are supplied). AirPCap adapters are also supported. The built-in wireless sniffer intercepts the handshake packet required to start the attack. WinPCap drivers are required to enable Wi-Fi sniffing.

ElcomSoft's patented GPU acceleration makes Wi-Fi password recovery several hundred times faster by using the sheer computational power of today's NVIDIA and AMD video cards. GPU acceleration delivers supercomputer-grade performance with minimum investment. Multiple video cards can be used together for even faster attacks.

Elcomsoft Wireless Security Auditor supports fully automatic and manual operation, allowing to enter password hashes and network's SSID by hand. Retrieving all SSID and password hashes from handshake packets, Elcomsoft Wireless Security Auditor allows selecting which one to recover. In order to test network security from insider attacks, Elcomsoft Wireless Security Auditor can automatically import saved password hashes retrieved by [Elcomsoft Proactive System Password Recovery](#).

4.14.2 Program information

4.14.2.1 System requirements

- Windows Vista or higher
- about 30 megabytes of free space on hard disk
- [AirPcap adapter](#) (recommended; or any compatible 3rd party Wi-Fi adapter), or capture file in 'tcpdump' format with 'handshake' packages (the program can get password hashes from some other sources as well)
- one of [supported NVIDIA or AMD/ATI cards](#) (optional)

4.14.2.2 About wireless security

Wireless security is based on [IEEE 802.1X](#) (IEEE Standard). There are two types of encryption: [WEP](#) and [WPA](#) ([WPA2](#)); besides, there are two WPA/WPA2 modes: pre-shared key mode, and with a [RADIUS](#) server.

Pre-shared key mode (PSK, also known as Personal mode) is designed for home and small office networks; each user must enter a passphrase from 8 to 63 printable characters; a hash function that incorporates the SSID converts the password to a hash value that is being transferred during the 'handshake' process. There is no way to get the plaintext password right from the hash, but the password can be still retrieved (in many cases) by performing various attacks such as trying all words from the dictionary/wordlists ("as is" or modified).

4.14.2.3 Working with EWSA

Input data

EWSA (Professional edition only) includes an integrated network sniffer that supports [AipPCap adapters](#), as well as most modern 'generic' consumer models. If you use AirPCap, you need to install its own drivers; with 3rd party adapters, you need to install the special/custom NDIS drivers bundled with the program.

The program also supports the following input data:

- tcpdump log
- Tamos CommView log
- PSPP log
- Local Registry
- Manual entry

For more details on using the built-in sniffer and importing data from tcpdump and Tamos CommView logs, see [Capturing network packets](#) chapter.

Alternatively, you can import the data from PSPR log, where PSPR stands for [Proactive System Password Recovery](#). When used on the computer with [WZC \(Wireless Zero Configuration\)](#), that program can save WPA-PSK password hash into the text file (press Export button on Misc Features | Wireless network page); EWSA can also dump password hashes from the local Registry itself (use Dump Windows WPAPSK hashes menu item). Please note that neither PSPR nor EWSA cannot extract hashes in the situation when wireless configuration is driven by 3rd party (vendor-supplied) utility instead of WZC.

Finally, you can add the password hash manually.

Program options

CPU Options

Here you can set the number of CPU(s) or cores to run the attack on (Processor utilization option). Press Auto detect to set this option automatically according to the number of processors you have installed. The Summary box shows more information on your operating system, machine name, user name (and whether you have Administrator privileges), CPU(s) name and speed.

Accelerators

Available devices box shows information about "compatible" video cards (or special hardware accelerators) EWSA can run the attack on. If multiple cards are installed, all of them are shown; select the one you want to get more information about, and look at Device info box; press Drivers info to get additional information about video drivers installed. For more information, consult with [Hardware acceleration](#) chapter.

General options

Common: if 'When attack is over, switch to the next hash item and rerun the attack' is checked, then program will start working on the next handshake when current one is processed completely (regardless the result).

Logging: Select what kind of information you want to be printed by the program: regular messages, warnings, error messages. You can also duplicate all log messages to file.

Autosave: set an interval to automatically save attack status. If the program crashes for some reason, next time you start it, you can restore the attack from the last saved point. The status is also saved not just by interval but also when the password is found, the attack is stopper or the new one is set and started etc.

Wireless network sniffer: set wireless sniffing parameters:

- install/reinstall ESNDISMON driver
- minimize program into the tray
- mirror captured packets into .pcap-file (adds program reliability in case it crashes)
- an ability to disable WLAN service when the sniffer starts; helps with some adapters on Windows 7
- deauthentication options (only if two or more adapters are available)

4.14.2.4 Capturing network packets

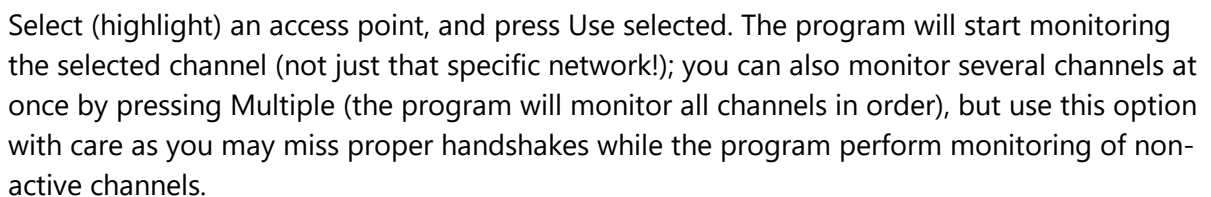
To start capturing network packets, select WiFi sniffer on the tool bar (or AirPCap sniffer if you have the AirPCap adapter). Please note that you should have proper drivers installed; read [NDIS driver installation](#) for more details.

As for adapter compatibility, it actually depends on their drivers' quality. In brief:

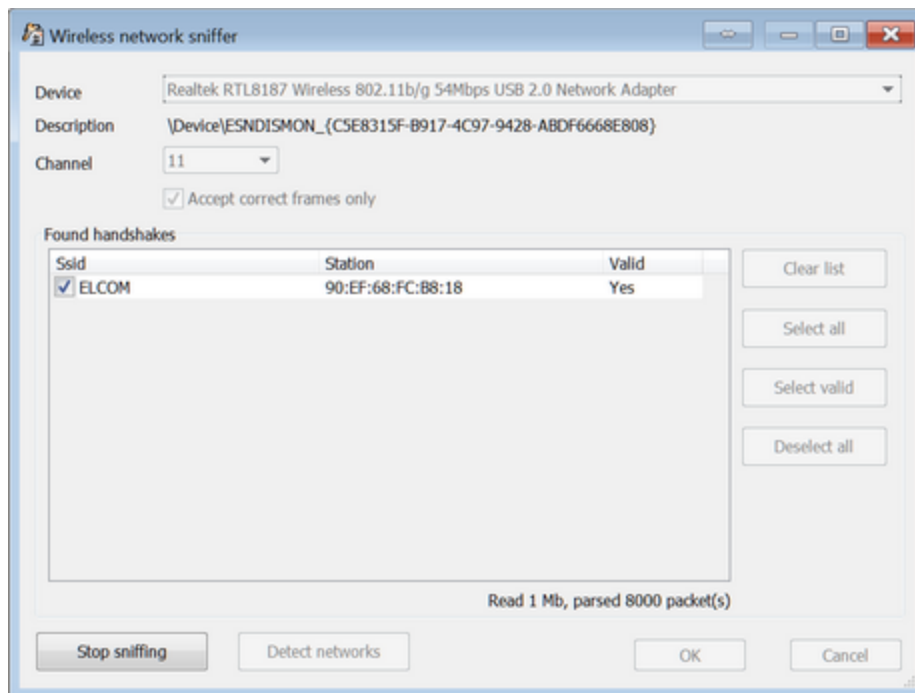
- Most Alfa adapters (like AWUSS036H) usually work correctly
- Intel adapters (used on many laptops) usually do not work at all
- TP-Link adapters: mixed thoughts; usually works best with drivers not from the vendors but for desired chipset; the ones we have tested (and confirmed that everything works correctly) are: TL-WN7200ND, TL-WN822N, TL-WN722
- Atheros: usually work just fine (tested: AR9002WB, AR9485, AR5BW222, AR56x), but there are different problems with some specific ones, from not capturing the packets and up to BSOD

In general, even most 'noname' adapters work correctly, but you may need to spend some time finding proper drivers until you find ones that does not cause program (or system) to fail.

Once all the drivers (adapter ones and NDIS) are installed, select the correct device (for AirPCap adapters, it is typically listed as \\.\airpcap00 device) and channel and press [OK]. If you're not sure about the channel, press [Detect networks] button, and the programs start monitoring all channels; you can press Save at any time to save the list of available networks:



ELCOMSOFT
DESKTOP, MOBILE & CLOUD FORENSICS



All captured packets can be mirrored into the pcap-file (for further analysis in 3rd party software); if that option is enabled, the protection from lost handshake packets is enabled automatically.

Please note that some (fortunately, not many) adapters work correctly only if Accept correct frames only option is turned off.

Once you get the one you need, press Stop sniffing, then OK, and now you can the recovery process. But please note that if you're using trial or standard version of the product, the packets will be still captured, but you will not be able to import them for further password recovery; this feature is available in professional edition only (for more details, see Limitations of unregistered version and Registration chapters).

If you don't have a compatible AirPCap adapter, there are some alternatives. tcpdump is a common packet sniffer that allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. It was originally written by several people working in the Lawrence Berkeley Laboratory; now distributed under a permissive free software licence, and works on most Unix-like operating systems. There are also a few ports of tcpdump for Windows.

Examples of existing packet sniffers can export the packets in tcpdump format: [airodump-ng](#), [OmniPeek](#).

The captured data should contain the full authentication handshake from a real client and the access point. Please note that the program does not work with the packets where linktype is LINKTYPE_ETHERNET (they come from wired, not wireless networks).

4.14.2.5 NDIS driver installation

When you start sniffer at the first time, the program prompts you to install ESNDISMON driver the program cannot perform sniffing without. You can also view the drivers installed (including the installation date) by selecting [Options] | [General options] | [Wireless network sniffer], and install/reinstall driver from there.

To make sure the drivers are properly installed, follow the steps:

1. Make sure that you have compatible adapter.
2. Remove WinPCap and AirPCap drivers if you already have them in the system.
3. Insert the adapter and install the driver provided by the manufacturer. Do NOT use the drivers included with Windows, they are usually not compatible; even better, install the chipset drivers.

In you use AirPCap adapter, install its own drivers from the vendor web site:

<https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html>

4. Restart the system; it is mandatory step for most adapters even if there was no prompt to do so.

5. Install EWSA.

6. Start Wi-Fi or AirPCap sniffer, depending on what adapter you have. EWSA should prompt to install ESSNDISMON driver, and you should confirm.

7. If adapter still does not work, install ESNDISMON manually:

- open Network and sharing center
- select Adapter settings
- right-click on adapter and select Properties
- press Install, select Service, then Add
- press Have disk and select the path to ESNDISMON driver (proper .inf-file, according to system version and 32/64); the drivers are located in "Drivers" folder under the program installation folder

4.14.2.6 Hardware acceleration

EWSA provides hardware acceleration (i.e. runs much faster) on most modern [NVIDIA](#) and [AMD](#) video cards.

You can use NVIDIA [GeForce](#) or [Quadro/Tesla](#) cards. Full list of supported devices can be found [here](#). If you have multiple cards, you need to disable [SLI](#) (either in driver or by physically disconnecting the cards). EWSA also supports acceleration with [AMD Radeon](#) cards. Built-in [Intel HD and Iris graphics](#) is also supported.

Whether you have NVIDIA or AMD card to use with EWSA, you should also have the latest drivers installed. The program is guaranteed to work with up to 8 devices, though may work (by design) with larger systems.

System and Data Recovery Programs

5 System and Data Recovery Programs

5.15 Advanced EFS Data Recovery

5.15.1 Introduction

Decrypt files protected with the Encrypting File System (EFS). Advanced EFS Data Recovery (AEFSDR) decrypts files protected with EFS in Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2012. The recovery is possible even when you transfer a protected disk into a different PC, reformat system partition, or when some encryption keys are tampered with.

Microsoft Encrypting File System (EFS) is a part of NTFS, and is available in many current versions of Windows. The EFS performs transparent encryption of files, enabling the users to effectively protect data against unauthorized access even from those who gain physical access to the hard disk or the computer with the encrypted files.

Losing access to EFS-protected files is as easy as re-installing Windows over the old version, re-formatting system partition, or transferring the disk with encrypted data into a new PC.

Advanced EFS Data Recovery effectively decrypts the EFS-protected files even when all other methods to recover encrypted data fail. Scanning the hard disk in low-level mode and matching the patterns sector by sector allows Advanced EFS Data Recovery to recover the EFS-encrypted files even if some of the encryption keys are lost.

Advanced EFS Data Recovery helps to recover from system administration errors such as deleting user accounts and profiles, missing or misconfigured data recovery authorities, incorrect transfers of user accounts between domains, or moving hard disks with encrypted data between computers.

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our software or have permission from the legitimate owner to perform these acts. Any illegal use of our software will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

You further attest that the recovered data, passwords and/or files will not be used for any illegal purpose. Be aware password recovery and the subsequential data decryption of unauthorized or otherwise illegally obtained files may constitute theft or another wrongful action and may result in your civil and (or) criminal prosecution.

5.15.2 Working with AEFSDR

5.15.2.1 About EFS (Encrypting File System)

The Encrypting File System (EFS) that is included with the Windows 2000 (Professional, all Server editions), Windows XP (Professional), Windows Server 2003/2008/2012, Windows Vista (Business, Ultimate, Enterprise), Windows 7 (Professional, Enterprise, Ultimate), Windows 8 operating systems provides the core file encryption technology to store NTFS files encrypted on disk. EFS particularly addresses security concerns raised by tools available on other operating systems that allow users to physically access files from an NTFS volume without an access check.

More information is available in [Microsoft TechNet documentation](#):

Security features such as logon authentication or file permissions protect network resources from unauthorized access. However, anyone with physical access to a computer such as a stolen laptop can install a new operating system on that computer and bypass the existing operating system's security. In this way, sensitive data can be exposed. Encrypting sensitive files by means of EFS adds another layer of security. When files are encrypted, their data is protected even if an attacker has full access to the computer's data storage.

Only authorized users and designated data recovery agents can decrypt encrypted files. Other system accounts that have permissions for a file — even the Take Ownership permission — cannot open the file without authorization. Even the administrator account cannot open the file if that account is not designated as a data recovery agent. If an unauthorized user tries to open an encrypted file, access is denied.

Benefits of EFS

EFS allows users to store confidential information about a computer when people who have physical access to your computer could otherwise compromise that information, intentionally or unintentionally. EFS is especially useful for securing sensitive data on portable computers or on computers shared by several users. Both kinds of systems are susceptible to attack by techniques that circumvent the restrictions of access control lists (ACLs). In a shared system, an attacker can gain access by starting up a different operating system. An attacker can also steal a computer, remove the hard drive(s), place the drive(s) in another system, and gain access to the stored files. Files encrypted by EFS, however, appear as unintelligible characters when the attacker does not have the decryption key.

Because EFS is tightly integrated with NTFS, file encryption and decryption are transparent. When users open a file, it is decrypted by EFS as data is read from disk. When they save the file, EFS encrypts the data as it is written to disk. Authorized users might not even realize that the files are encrypted because they can work with the files as they normally do.

In its default configuration, EFS enables users to start encrypting files from My Computer with no administrative effort. From the user's point of view, encrypting a file is simply a matter of setting a file attribute. The encryption attribute can also be set for a file folder. This means that any file created in or added to the folder is automatically encrypted.

How EFS Works

1. EFS uses a public-private key pair and a per-file encryption key to encrypt and decrypt data. When a user encrypts a file, EFS generates a file encryption key (FEK) to encrypt the data. The FEK is encrypted with the user's public key, and the encrypted FEK is then stored with the file.
2. Files can be marked for encryption in a variety of ways. The user can set the encryption attribute for a file by using Advanced Properties for the file in My Computer, by storing the file in a file folder set for encryption, or by using the Cipher.exe command-line utility. EFS can also be configured so that users can encrypt or decrypt a file from the shortcut menu accessed by right-clicking the file.
3. To decrypt files, the user opens the file, removes the encryption attribute, or decrypts the file by using the cipher command. EFS decrypts the FEK by using the user's private key, and then decrypts the data by using the FEK.

[...]

Additional information is available at Microsoft site:

- [The Encrypting File System](#)
- [Encrypting File System overview](#)
- [Encrypting File System in Windows XP and Windows Server 2003](#)
- [Protecting Data by Using EFS to Encrypt Hard Drives](#)
- [Encrypting File System best practices](#)
- [Encrypting File System How To ...](#)
- [Encrypting File System Concepts](#)
- [Encrypting File System Troubleshooting](#)

And here is a (partial) list of Microsoft Knowledge Base articles related to the EFS:

- [Best Practice Methods for Windows 2000 Domain Controller Setup](#)
- [Cannot Gain Access to Previously Encrypted Files on Windows 2000](#)
- [Disabling EFS for All Computers in a Windows 2000-Based Domain](#)
- [Encrypting Files in Windows 2000](#)
- [Encrypted Files Cannot Be Compressed](#)
- [Transferring Encrypted Files That Need to Be Recovered](#)
- [Best Practices for Encrypting File System](#)
- [Using a Certificate Authority for the Encrypting File Service](#)
- [Cannot Use Shared Encrypted Files in Windows 2000](#)

- [Default Behavior for Group Policy Extensions with Slow Link](#)
- [Error Message When Attempting to Encrypt Files or Folders](#)
- [Backup Tool Backs Up Files to Which You Do Not Have Read Access](#)
- [The Encrypted Data Recovery Policy for Encrypting File System](#)
- [How to enable the encryption command on the Shortcut menu](#)
- [How to back up the recovery agent Encrypting File System \(EFS\) private key in Windows Server 2003, in Windows 2000, and in Windows XP](#)
- [Using Efsinfo.exe to Determine Information About Encrypted Files](#)
- [How to Disable/Enable EFS on a Standalone Windows 2000 Computer](#)
- [HOWTO: Use Encrypting File System \(EFS\) with IIS](#)
- [Cannot Gain Access to Microsoft Encrypted File Systems](#)
- ["Warning: The Restore Destination Device..." During Restore](#)
- [INFO: Understanding Encrypted Directories](#)
- ["Access Is Denied" Error Message Appears w/ Correct Permissions](#)
- [Encrypted Files Made Available Offline Not Encrypted on Client](#)
- [The Local Administrator Is Not Always the Default Encrypting File System Recovery Agent](#)
- [Selecting Encrypted File Over Network Hangs Client Window](#)
- [Methods for Recovering Encrypted Data Files](#)
- [Cannot Open Encrypted Files with Multiple Windows Installations](#)
- [How to Reinitialize the EDRP on a Workgroup Computer](#)
- [EFS Recovery Agent Cannot Export Private Keys](#)
- [Software Inventory on Encrypted Vol Degrades Performance](#)
- ["Access is Denied" When Encrypting/Decrypting Files or Folders](#)
- [Description of the Windows 2000 Resource Kit Security Tools](#)
- [Logon Process Hangs After Encrypting Files on Windows 2000](#)
- [How to Troubleshoot FRS and DFS](#)
- [Error Message "Access Denied" When Starting a Program\](#)
- [Third-Party Certificate Authority Support for EFS](#)
- [Unable to Recover Encrypted Files After the Domain Controller Is Demoted](#)
- [Recovery of Encrypted Files on a Server](#)
- [Unable to Access Encrypted Files After Using Sysprep.exe](#)
- [Need to Turn Off EFS on a Windows 2000-Based Computer in Windows NT 4.0-Based Domain](#)
- [EFS, Credentials, and Private Keys from Certificates Are Unavailable After a Password Is Reset](#)
- [Sysprep.exe May Re-Enable the Encrypting File System](#)
- [Using the Cipher.exe utility to migrate self-signed certificates to certification authority-issued certificates](#)
- [Cipher.exe Security Tool for the Encrypting File System](#)
- [HOW TO: Prevent Files from Being Encrypted When Copied to a Server](#)
- [How To Encrypt a File in Windows XP](#)
- [How To Encrypt a Folder in Windows XP](#)
- [HOW TO: Share Access to an Encrypted File in Windows XP](#)
- [How To Remove File Encryption in Windows XP](#)

- [Users with Roaming Profiles Cannot Use EFS On Domain Controllers](#)
- [HOW TO: Use Ntbackup to Recover an Encrypted File or Folder in Windows 2000](#)
- [How To Use Cipher.exe to Overwrite Deleted Data in Windows](#)
- [How to encrypt files and folders on a remote Windows 2000 Server](#)
- [HOW TO: Identify Encrypted Files in Windows XP](#)
- [You Cannot Access Protected Data After You Change Your Password](#)
- [Encrypting File System \(EFS\) files appear corrupted when you open them](#)
- [User cannot gain access to certificate functionality after password change or when using a roaming profile](#)
- [HOW TO: Use Cipher.exe to Overwrite Deleted Data in Windows Server 2003](#)
- [You cannot restore encrypted files to a remote computer in Windows 2000](#)
- [A user who has permissions to change the folder attributes can now change the folder encryption attribute](#)
- [The "Encrypt Contents to Secure Data" Check Box Is Unavailable](#)
- [New functionality is available for Cipher.exe in Windows 2000 and Windows XP](#)
- [Computer Stops Responding \(Hangs\) When It Writes Encrypted Data to an NTFS Partition](#)
- [Information about the storage of data files on an encrypted volume in Exchange Server](#)
- [How to add an EFS recovery agent in Windows XP Professional](#)

5.15.2.2 How AEFSDR works

There are three typical scenarios of AEFSDR usage:

- You want to decrypt files from the disk(s) you boot operating system from, and you have Administrator privileges in the system. However, some certificates are corrupted (and so "standard" methods available in the operating system don't work), or some files have been encrypted by other users (and their passwords are not known).
- For some reason, you cannot load operating system, or you don't have Administrator privileges in it.
- You have got a disk (with encrypted files) from an 'alien' system.
- The system has been reinstalled

In the first case, no additional steps (prior to AEFSDR installation and usage) are required. If you cannot boot from the disk with encrypted files, simply install it as an additional one to any system with Windows NT/2000/XP/2003/Vista/2008/7 installed, where you have Administrator privileges (in the second case, you will have to detach the disk from the 'dead' system, of course).

Note: if you start AEFSDR on Windows Vista or Windows 7 under the account with administrator privileges, but not the Administrator itself, you may get the following message:

Cannot get direct access to the logical disk!

You must have Administrator rights to use this program.

Actually, this is the problem of UAC (User Account Control), that does not work correctly in certain circumstances. As a workaround, simply right-click on aefsd.exe and select Run as Administrator from popup menu (you may have to supply Administrator credentials, though). The program will start normally.

Now you can use AEFSDR. The program does the following:

- Search for encryption keys (at the file or sector level)
- Decrypts (tries to decrypt) private keys – all ones that are available in the system.
- Find decrypted files on selected partition(s), and decrypt (try to decrypt) their File Encryption Keys.
- Decrypt files using FEKs using keys received at the previous steps.

If you previously exported the recovery agent EFS private key (see [KB241201](#) for details) but for some reason cannot import it back, AEFSDR can use it directly (so you will not have to search for encryption keys).

All these steps are described in details in the next chapters: [Scan for encryption keys](#), [Scan for encrypted files](#), [Browse for encrypted files](#) and [Decrypting files](#).

The most easy way is to run the [wizard](#). If appropriate [option](#) is enabled, wizard is shown automatically when the program starts; alternatively, you can call it any time by pressing Wizard button on program toolbar.

5.15.2.3 Wizard mode

Wizard mode guides you through all the steps described in [How EFS works](#) section. Typically, they are:

- Select logical disk(s) to scan for keys (by default, all disks are checked)
- Add user name(s) and password(s) to decrypt the keys
- Select logical disk(s) to scan for encrypted files (by default, all NTFS disks are checked)
- Select files to decrypt

At any time, you can switch to Expert mode by pressing the button on wizard screen; your current results (the keys or files that have been found) will not be lost. And/or you can uncheck the Show wizard at startup [option](#) when wizard is already running – that will not terminate the wizard itself, but next time the program will start in Expert mode.

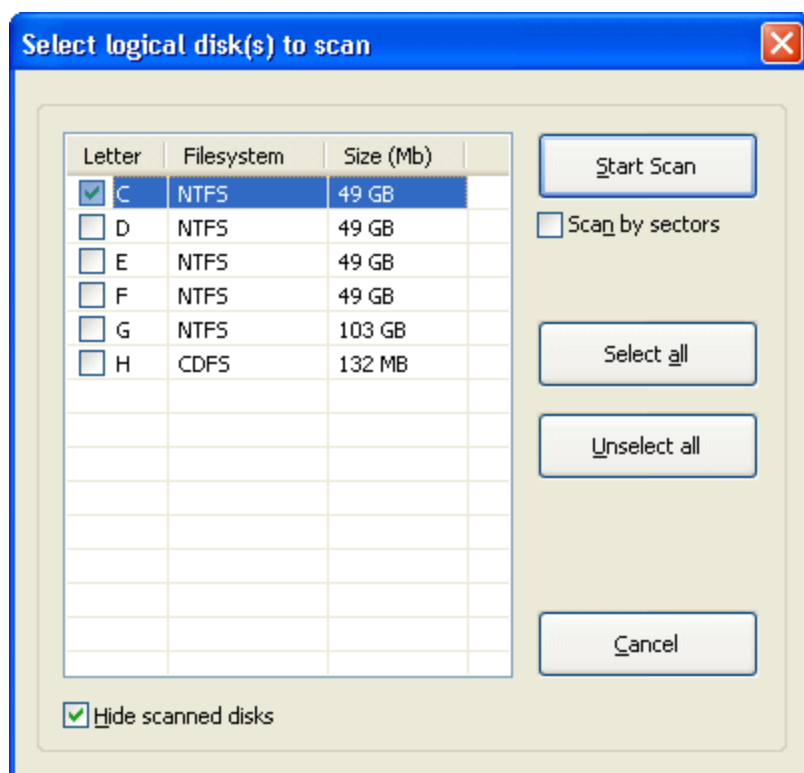
Press Back and Next buttons to navigate through wizard; for example, you may wish to return to one of the previous steps to scan another disk (the one that has not been scanned yet) for keys or files, or add additional passwords if some/all keys have not been decrypted.

5.15.2.4 Scan for encryption keys

Introduction

If you previously exported the recovery agent EFS private key (and have the *.pfx file), just press Add Certificate button, browse for the file, supply its password, and AEFSDR can use it for file recovery/decryption now. In that case, you will not need to scan your disk(s) for encryption keys, as described below. Otherwise, continue reading.

Always start using the program with scanning for encryption keys. At EFS related files tab, press Scan for keys button (or select Scan | Scan for keys menu item; or press Scan for keys button on toolbar); the program will show the list of (local) logical disks, along with their sizes and file systems:



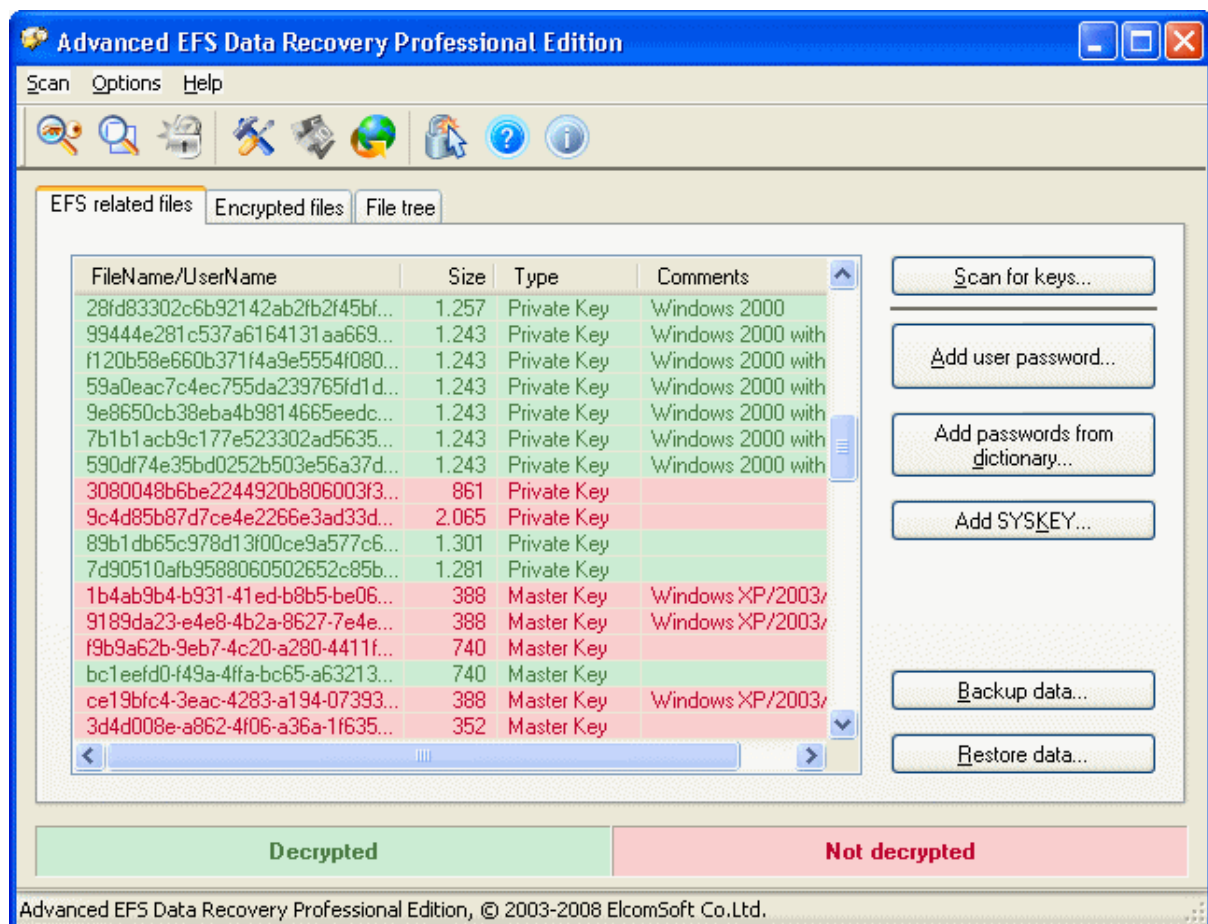
Here, you have to select the boot disk, i.e. the one operating system is (was) loading from, and so where system Registry and encryption keys are located. In some cases, however, encryption keys are located on other disk, so if you're not sure, you can check multiple disks for scanning.

By selecting the Scan by sectors option, you force the program to scan the disk(s) at the lower (sector) level, so it may find the keys that have been deleted, or after re-formatting the disk. Note that such scan is much slower than the 'normal' one, so we recommend to perform the

first scan with this option disabled, and only if the keys (needed for decryption) is not found, re-scan the disks by sectors.

Note the Hide scanning disks option at the bottom – if it is enabled (default) and you already scanned some disk(s) during current program session, these disk(s) will not be shown in that window as far as all keys from there have been already found. If you still wish to see (and select from) all the disks available in the system, uncheck this option.

On pressing the Start Scan button, the program will scan the given disk(s) trying to find all files needed for further decryption of your data:



These files are:

- encryption keys
- SYSTEM Registry
- SAM Registry

Usually, there are a few encryption keys (the actual value may vary depending on the number of users in the system), and a few copies of SYSTEM and SAM Registry (the "active" one, and

two or more backup copies) – but at least one of each. For more information on Registry, look at [Description of the Microsoft Windows Registry](#) article at Microsoft web site.

If any of those components are missing, it means that either you have selected the wrong disk (in that case, simply scan the correct one – or just all of them; the required data, if found, will be appended to the list already created), or they are not available at all (if, for example, they were deleted manually, or the disk has physical errors).

Encryption keys in that list are always in red or green color. Green one means that the key has been decrypted successfully; or if the key is in red – decryption failed.

The last column on this screen, Comments, shows additional information about encryption keys (what particular version of Windows the have been created in), and SYSKEY mode (see below).

Possible problems

If some keys were not decrypted (i.e. they're red), don't panic. Probably, these keys are not needed at all, and you can go directly to the second step – [Scan for encrypted files](#) or [Browse for encrypted files](#). And only if AEFSDR will not be able to decrypt the files you need, return to EFS related files and try to fix the problem as described below.

Password encryption (Windows XP/2003/Vista/2008/7) or SYSKEY protection (Windows 2000)

First, if the files were encrypted on Windows XP or later version, you have to supply the (logon) password of user who encrypted the file(s), or the password of Recovery Agent. Press Add user password button, and enter the user name and password (as text or in hex/UNICODE). User name, actually, does not matter (only password does), so enter it just for the reference. There is no need to add the empty password.

Please note that you can add more than one name/password, and after adding each one, AEFSDR will try to decrypt all keys listed on that tab – on success, the color will change from red to green. Alternatively, you can use Add password from dictionary option, and load the password lists from the text file. That file should contain only the passwords, one per line, without user names (which do not actually matter). It is not recommended to use large wordlists (more than a few hundred entries), especially on Windows XP and later versions, and/or if there are a lot of encryption keys, as far as it takes a lot of time.

In Windows 2000, the password is usually not needed, until advanced SYSKEY protection is being used (for more information, see [How to use the SysKey utility to secure the Windows Security Accounts Manager database](#)). There are three possible SYSKEY options:

- Password Startup: the password is needed to unlock the startup key each time when computer is started.
- Store Startup Key On Floppy Disk: SYSKEY generates a new startup key and stores it on a floppy disk. This floppy disk is inserted each time when you start the computer.
- Store Startup Key Locally: this is the default setting. By storing the startup key on the local hard disk, Windows can access it during startup without further intervention.

AEFSDR should work just fine if last (default) option has been used in a system you're working with, i.e. the keys should be decrypted automatically. But if Startup Key is (was) stored on floppy disk, or Password Startup was selected, the program simply will not be able to decrypt some keys. In that case, you should supply the password (like in Windows XP/2003, see above). Alternatively, if you have the floppy disk with startup key, or know the startup password, you can add them to the program by pressing the Add SYSKEY button. You can add multiple passwords or keys using that feature (but one at a time). Please note, however, that after adding SYSKEY you will have to re-scan for encryption keys.

Password has been changed after encryption

After you change your domain password, you may receive an error message when you try to gain access to protected data. This problem occurs because the protected data is encrypted using a hash that is based on your password. When you change your password on the domain, the data is not re-encrypted with the new password until you first access the data. If you try to access the data for the first time while you are disconnected from the domain, the domain controller cannot be contacted. Therefore, the data cannot be accessed and re-encrypted with the new password.

By design, AEFSDR should be still able to decrypt encryption keys (and so protected data), but if not, use the same trick as for SYSKEY Protection problem, i.e. by adding user password(s). If you don't know them, try the solution described in the following Microsoft Knowledge Base article:

[You Cannot Access Protected Data After You Change Your Password](#)

Computer is a part of domain

The recovery policy provides for a person to be designated as the recovery agent. A default local recovery policy is automatically created when an administrator account logs on to the computer for the first time. When this process occurs, that administrator becomes the default recovery agent. In some situations, the first administrator to log on to Windows 2000 is not the local administrator account. An appropriate Microsoft Knowledge Base article is:

[The Local Administrator Is Not Always the Default Encrypting File System Recovery Agent](#)

If local administrator is the default recovery agent for your data, AEFSDR will work properly. If not (as described in the article mentioned above), you will have to add user passwords to decrypt the keys (see above).

Backup/restore decrypted keys

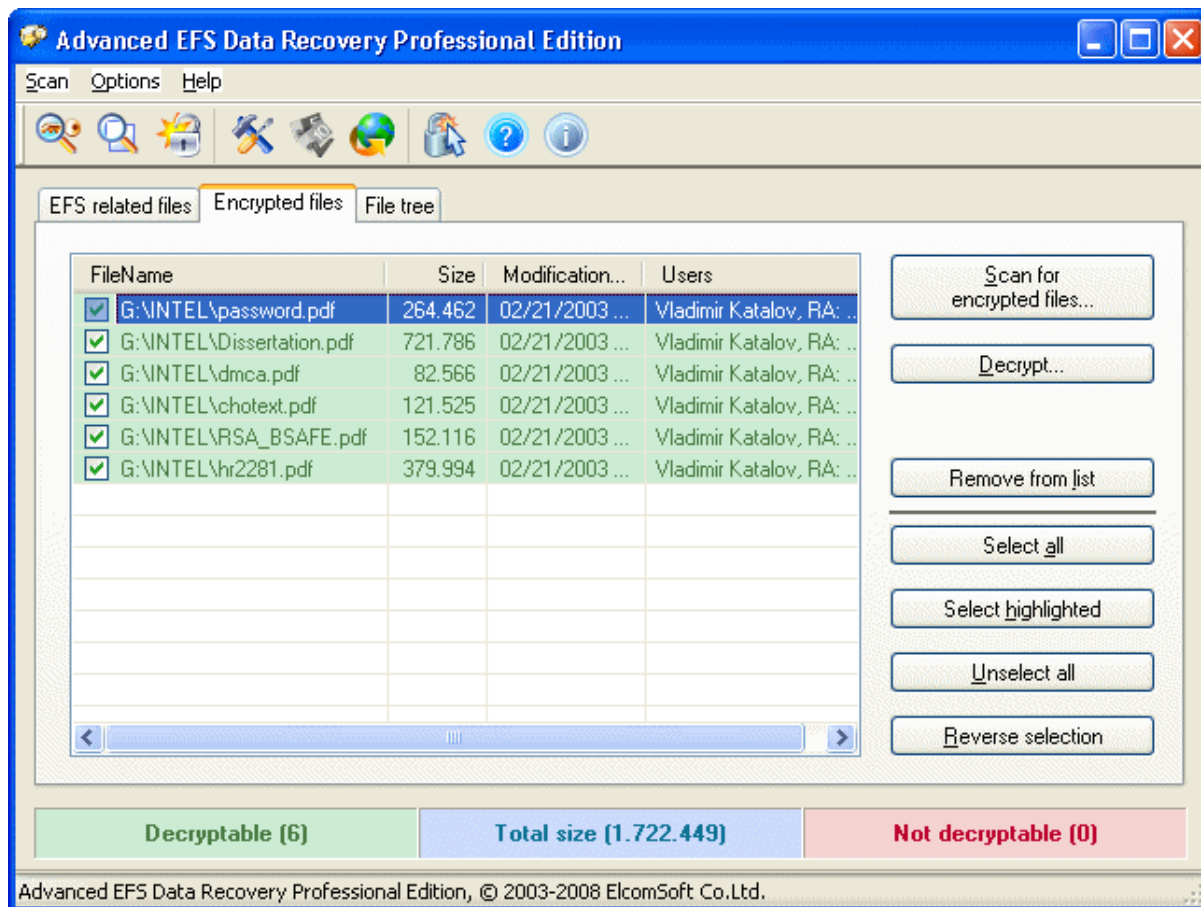
When/if encryption keys (and other EFS-related data) have been found and decrypted by the program, it is recommended to save them for the future use – to avoid scanning the disk again, or just for the case if some data will be tampered. Press Backup data button in AEFSDR, and select the file name to save what you have recovered. When you will use AEFSDR the next time, you'll be able to get all the keys by pressing Restore data button, instead of scanning the disk again, adding user passwords etc.

5.15.2.5 Scan for encrypted files

When all the keys (or at least some of them) have been [found and decrypted](#), you're ready to decrypt your data, i.e. files. If you already know what particular files are encrypted and where they're located, skip this step and go directly to [Browse for encrypted files](#) chapter.

Otherwise, switch to Encrypted files tab in AEFSDR. There, press Scan for encrypted files button (or select Scan | Scan for encrypted files menu item; or press Scan for encrypted files button on toolbar); the program will prompt you to select the disk(s) where to look for encrypted files – about the same way as when you scanned the disk for encryption keys, but only NTFS disks will be listed there (because Encrypting File System is available on NTFS only).

Check all disks you want to scan, and press Start Scan button. Please note that if selected disks is large and there are many files on them, this process may take a several minutes or even hours. Once the program finds the encrypted files, it immediately adds it to the main window, and at the end of scanning, you should get a complete list of encrypted files: file name (with full path), size in bytes, modification date:



The last column (User) looks like the following:

John Doe, RA: Ivan Ivanov

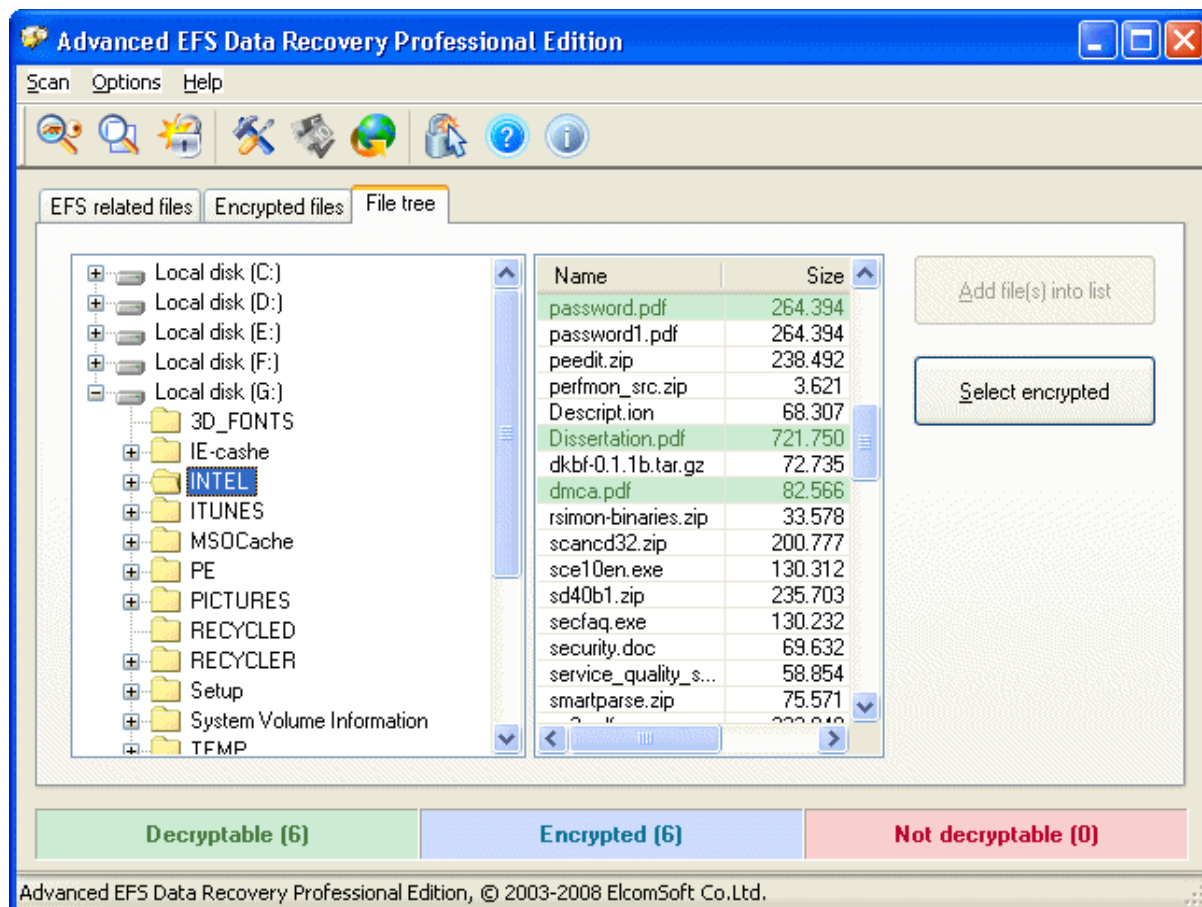
First name ("John Doe" in this example) is the name of the user who encrypted the file; and the names after RA are Recovery Agents ("Ivan Ivanov"), if ones exist.

Same as for encryption keys, all files in this list will be marked with green or red color – depending on whether the file can be decrypted or not (the counter is also there – in brackets). If some files (the ones you need) cannot be decrypted, you have to [scan for encryption keys](#) again (e.g. the different partition; and/or add user passwords or SYSKEY). For files encrypted on Windows XP, you always have to add user passwords – otherwise, the keys (and so the files) cannot be decrypted at all.

When all encrypted files have been found, you can [decrypt](#) them. In addition to number of Decryptable and Not decryptable files, the program also shows the total size of files selected for decryption.

5.15.2.6 Browse for encrypted files

If you already know where the encryption files are (and what are their names), switch to File tree tab in the program. It looks like standard Windows Explorer window: the disk/folder tree is at the left (note: only NTFS partitions are listed), and the right pane shows the list of files in selected folder:



When you change/select the folder at the left, AEFS DR starts to fill the right pane with file names. Encrypted files are being marked with the blue color first, and the program starts analyzing (in the background) whether these files can be decrypted or not using the keys that have been recovered, marks them with green or red color, respectively. Select the files to be decrypted and press Add file into list button (or use Select encrypted to add all encrypted files at once) – and the given files will be added to list at Encrypted files tab. You can also right-click on any folder (in the left pane) and select Scan for encrypted files (recursively) to search for encrypted files only in given folder and all its subfolders. Repeat this steps for all the files you need, and you're ready for [decryption](#).

Note: when you access this tab (File Tree) at the first time after starting the program, the program may "freeze" for a few seconds – this is normal. It just enumerates all logical disks in the system, analyses the file systems and builds the folders/files tree. However, if the program

still will not respond after a few minutes, please terminate it (using Task Manager, called via CTRL-ALT-DEL), restart, turn logging on (see [Program options](#) for details), switch to File Tree tab again and terminate. Log file will be created; send it to us (the log file can be large, so compress it with ZIP or RAR before sending, please) and we'll investigate the problem and do our best to provide you with a quick fix.

5.15.2.7 Decrypting files

Once you have a complete list of encrypted files (created as described in [Scan for encrypted files](#) and [Browse for encrypted files](#) chapters) – of course, after the [keys have been successfully recovered](#) – you can start the decryption process.

First, you have to select the files to be decrypted – at Encrypted files tab. All files listed there have check boxes at the left of the names, and you have to mark ones for further decryption. You can do that one-by-one, or use Select all, Select highlighted, Unselect all and Reverse selection buttons in the right-bottom corner of the window. As noted in the previous chapters, only files with green color can be decrypted, and so the program will not allow you to select the red ones. You can also use Remove from list button to remove selected file(s) from that page.

When files are selected, press Decrypt button at the right (or Decrypt files button on toolbar). AEFSDR will prompt you for the disk/folder to save the file to. Under that folder, the program creates sub-folders with names like AEFSDR_X_DECRYPTED, where 'X' is the drive letter for partition you're decrypting the files from; the complete path (where the source file was located) will be reconstructed under this (AEFSDR) subfolder. Decryption itself is relatively slow process, so please be patient (the program will show the progress bar and the names of the files being decrypted).

It is strongly recommended to save (decrypt) files to NTFS partition only. Simply because FAT and FAT32 partitions have many limitations (compared to NTFS), and so saving some particular files to non-NTFS partition may fail or give unexpected result.

Note: an unregistered (trial) version of AEFSDR decrypts only first 512 bytes of all files, padding the rest of content with zeros (look at Registration to learn how to get the fully functional version). But even in full version, please verify that all files have been decrypted successfully, before deleting the original (encrypted) files.

5.15.2.8 Program options

Log file

Use this option if something goes wrong – e.g. the program fails to scan selected partition, or some files have not been decrypted, etc. Simply type an appropriate file name (you can use the Browse button) to save debug information to, and one of the following options from the combo box:

- Disabled
- Overwrite the existing file
- Overwrite the existing file (Debug)
- Append to the existing file
- Append to the existing file (Debug)

Our technical support may ask you to send us the log file to locate and fix the problems. Debug log is much more detailed (and so more useful when the problem is hard to fix), but it can be really large (up to a few megabytes).

You can also force debug mode by using `-debug_log` command-line switch, by running the program as:

`aefsdrr.exe -debug_log`

In that case, `aefsdrr.log` file will be created in the root folder of disk C. That could be useful if the program does not even start on your machine: run it as described above, and send us the log file so we will be able to locate and fix the problem.

You can also set the maximum size of log file (in megabytes) – on reaching the limit, the program will stop writing to it. Set this option to zero if you don't want any limitations.

Process priority

You can switch between High, Normal, and Low. Recommended setting is Normal, but if you want to run the program as a "background" process, which will work only when the CPU is in an idle state, you can select Low. If you want to increase AEFSDR performance to the maximum, select High, but be aware that this will decrease the performance of *all other* applications running on your computer.

Use simple passwords to decrypt master keys

If this option is enabled, AEFSDR tries to decrypt the master keys using about 100 commonly-used passwords. For files encrypted on Windows 2000, it almost does not affect the performance; for XP/2003 and especially Vista and Windows Server 2008, however, the process of decrypting the keys runs much slower, especially when there are many users in the system, so use this option only as a last resort (when the password is not known).

Show wizard at startup

If enabled (default), the program always starts in [Wizard mode](#). To start the program in Expert mode (and follow all the steps manually: [Scan for Encryption keys](#) etc), uncheck this option.

Analyze deleted files

When this option is enabled, the program also searches for encrypted files that have been deleted.

5.15.2.9 System requirements

- Windows 2000 and higher
- Administrator privileges (for direct disk access)

Known problems and limitations

- The program can decrypt protected files only if encryption keys (at least, some of them) are still exist in the system and have not been tampered.
- Only Basic (but not Dynamic) NTFS partitions are supported.
- For all systems but Windows 2000, the password of user who encrypted the files (or Recovery Agent) is needed for decryption.

5.16 Elcomsoft Forensic Disk Decryptor

5.16.1 Introduction

Elcomsoft Forensic Disk Decryptor (EFDD) offers forensic specialists an easy way to obtain complete real-time access to information stored in popular crypto containers. Supporting desktop and portable versions of most popular disk encryption software, the tool can decrypt all files and folders stored in crypto containers or mount encrypted volumes as new drive letters for instant access. Decryption keys can be acquired by analyzing hibernation files or memory dumps (memory dumping feature is built-in into the product) or obtained via a FireWire attack. The program can also decrypt or mount disks if the password is known, or recovery key is available.

The tool provides near-instant acquisition with two options to access the content of encrypted volumes. With full decryption, the entire content of the protected disk is decrypted, providing investigators with full, unrestricted access to all information stored on encrypted volumes. For fast, real-time access to protected information, the encrypted volume can be mounted as a new drive letter. In this mode, the files will be decrypted on the fly.

Elcomsoft Forensic Disk Decryptor supports three ways to acquire decryption keys used to access the content of encrypted containers. Depending on whether the PC is running or turned off, locked or unlocked, the keys can be obtained by analyzing a memory dump or hibernation file, or by performing an attack via the FireWire protocol in order to obtain a live memory

dump. In order to obtain the decryption keys, the encrypted volume must be mounted on the target PC.

Elcomsoft Forensic Disk Decryptor supports flash drives and removable media encrypted with BitLocker-to-Go, and recognizes encrypted volumes and full disk encryption of all supported types. Raw (DD) and EnCase (.E01) disk images are also supported.

Supported crypto containers:

- BitLocker
- PGP (volume and full-disk encryption)
- TrueCrypt
- VeraCrypt
- LUKS (password hash extraction only)
- BestCrypt (password hash extraction only)

The program that is licensed to you is absolutely legal and you can use it provided that you are the legal owner of all files or data you are going to recover through the use of our software or have permission from the legitimate owner to perform these acts. Any illegal use of our software will be solely your responsibility. Accordingly, you affirm that you have the legal right to access all data, information and files that have been hidden.

You further attest that the recovered data, passwords and/or files will not be used for any illegal purpose. Be aware password recovery and the subsequencial data decryption of unauthorized or otherwise illegally obtained files may constitute theft or another wrongful action and may result in your civil and (or) criminal prosecution.

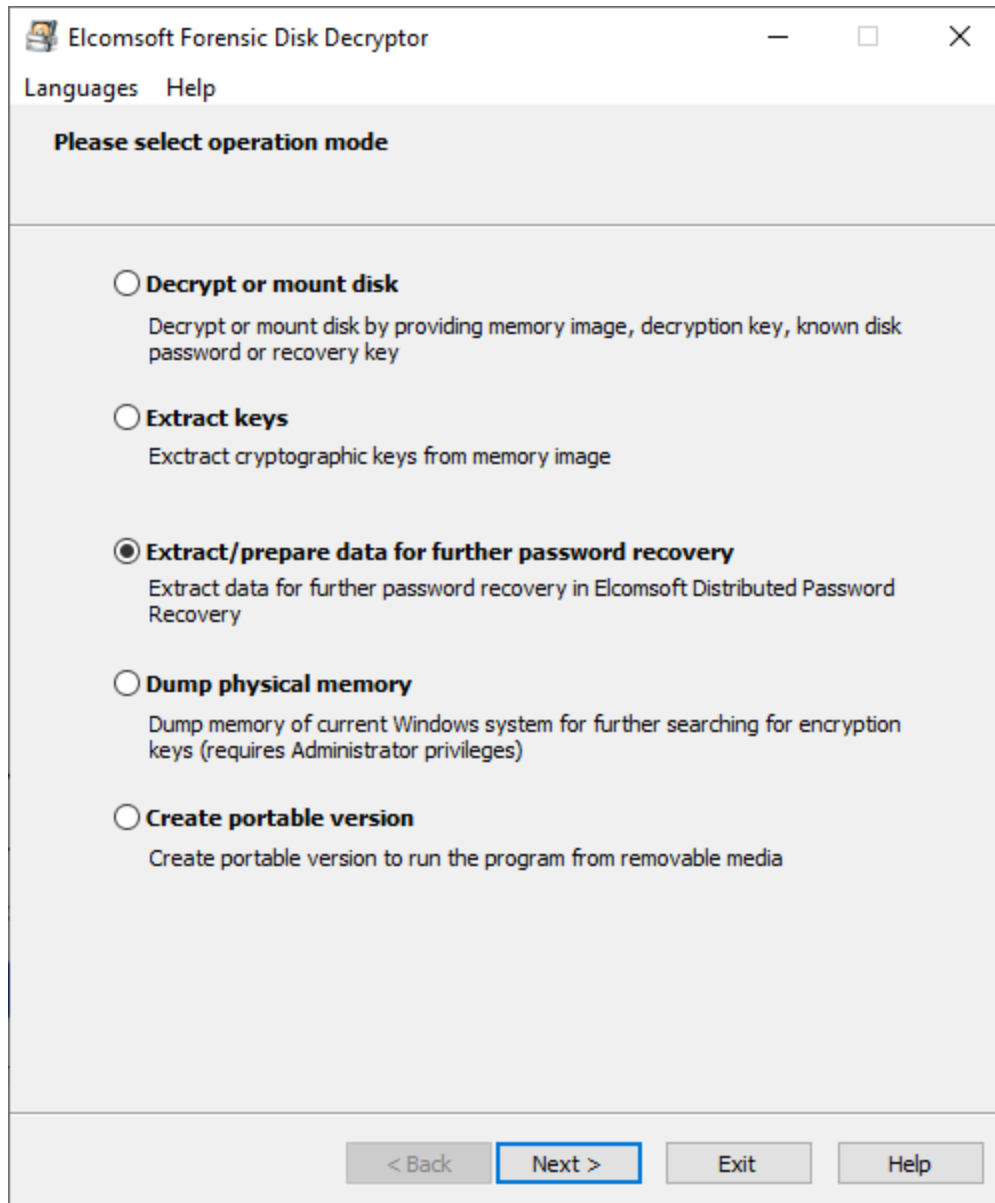
5.16.2 Program information

5.16.2.1 System requirements

- Windows 7 or higher
- about 8 megabytes of free space on hard disk
- for all supported encrypted disks/containers: memory image or hibernation file that contains disk encryption keys (created when encrypted disk was mounted) or password itself
- for BitLocker and PGP: recovery key
- for BitLocker: Active Directory database (ntds.dit)
- for FileVault2-encrypted containers: recovery token from iCloud, or locally saved recovery key, or password (for HFS+ partitions only; for APFS, only generation of data for further password recovery is supported)
- for VHD and VHDX images: Windows 8.1 or higher

5.16.2.2 Working with the program

At the main program screen, the following options are available:



Decrypt or mount disk

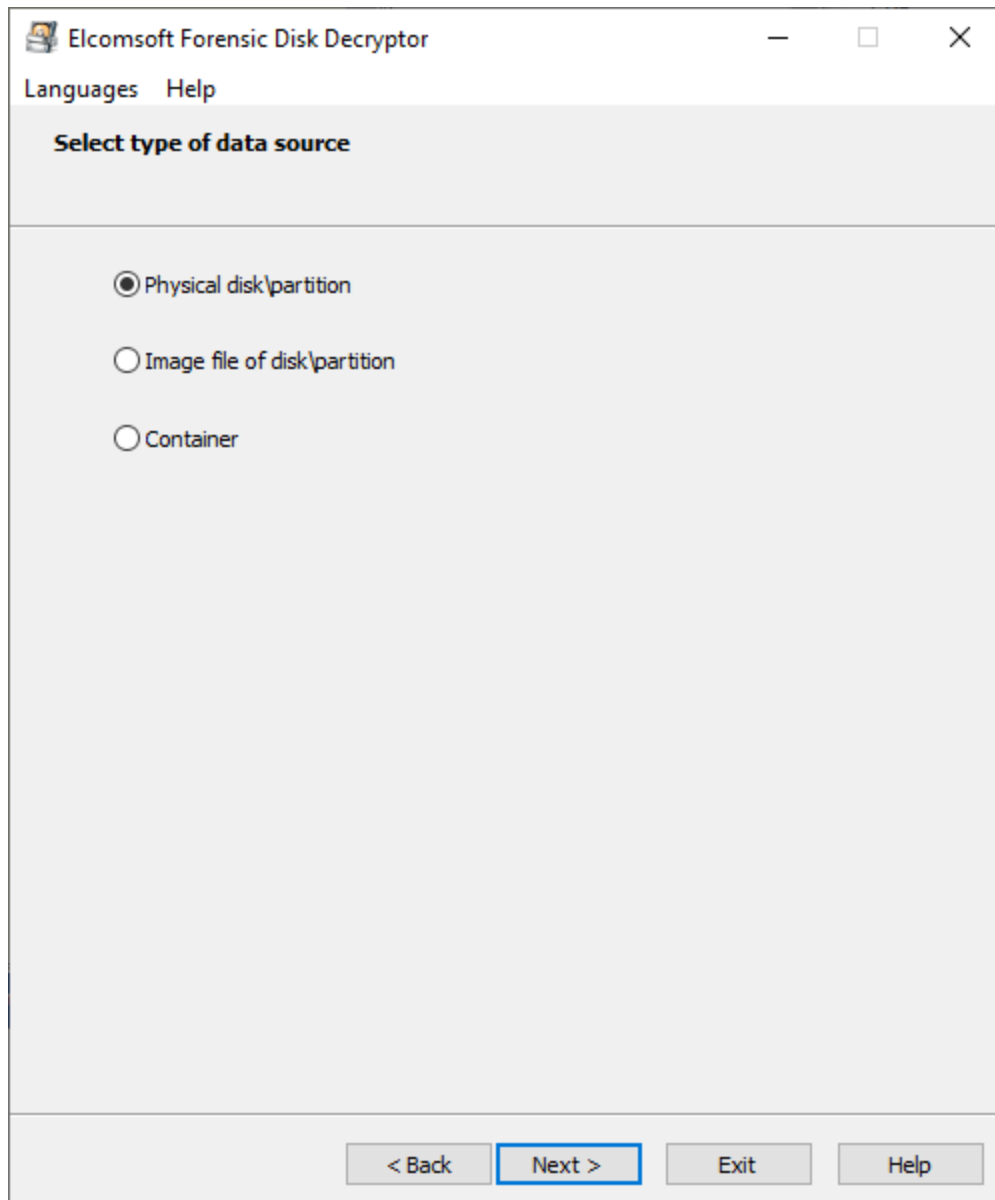
See [Decrypt or mount disk](#) for details.

Extract keys

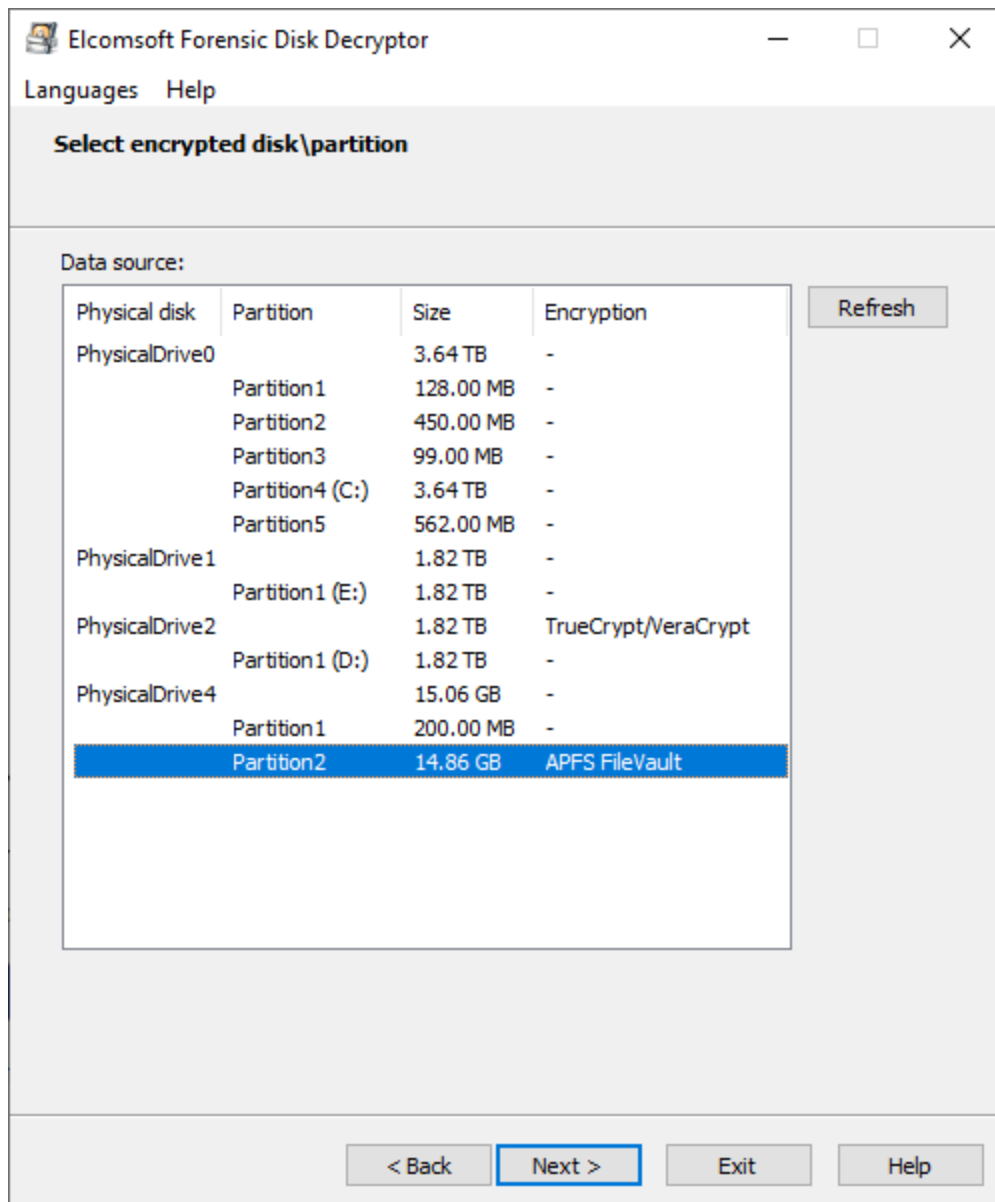
Once the disk is mounted into the system (unlocked), the system keeps the encryption keys in memory, and so can be extracted from there -- from memory dump (keep reading for more information how to get it) or from hibernation file (if the system has been hibernated while the disk was mounted). See [Extract keys](#) for more details.

Extract/prepare data

If password is not known, recovery keys are not available and there is not memory dump or hibernation file, then the only option left is recover the password using time-consuming brute-force or dictionary attack. EFDD allows to extract the data needed for further recovery; then you can use this data in [Distributed Password Recovery](#) for effective password cracking. Like with the first option (Decrypt/mount disk), select the data source first:



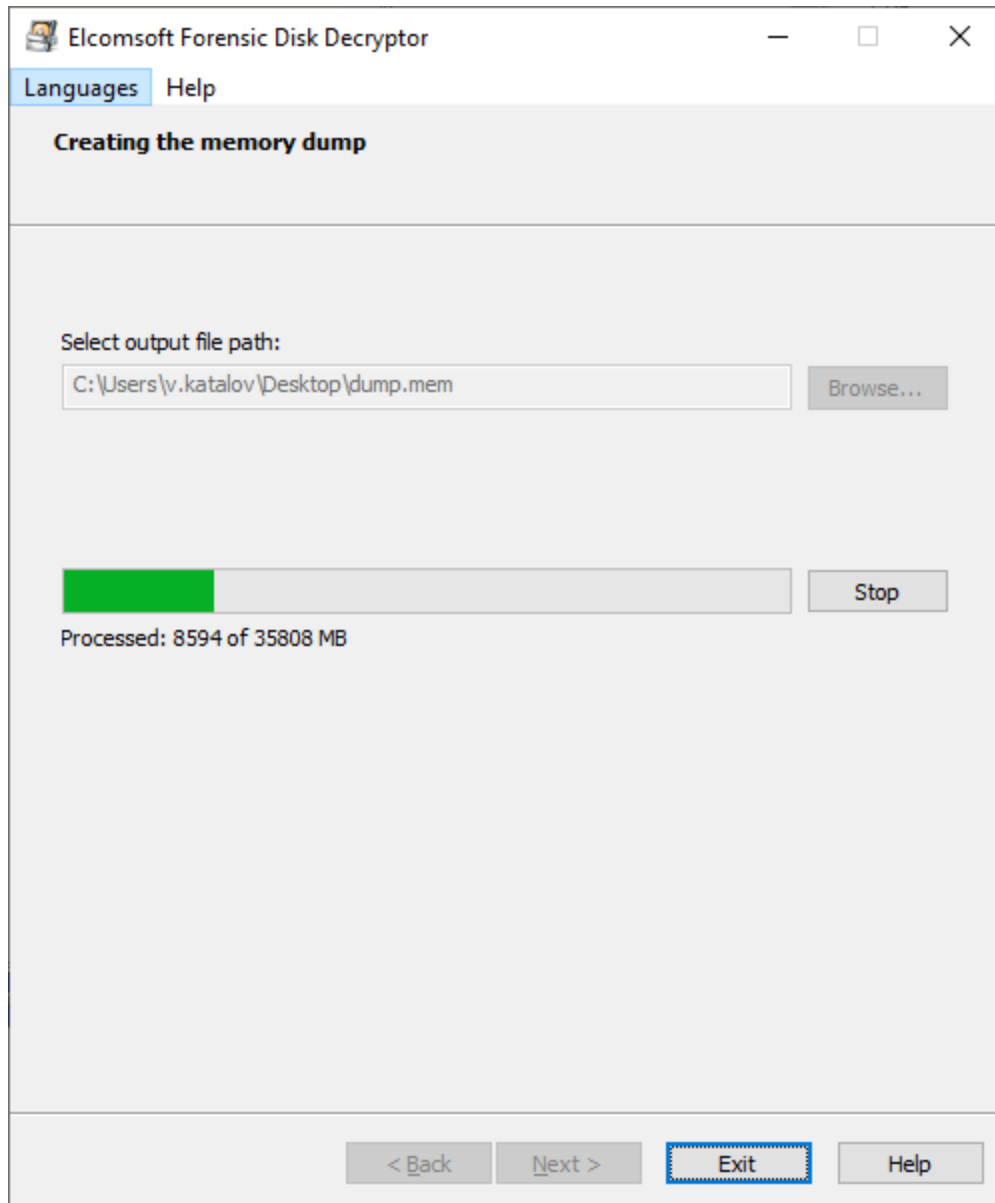
For the first two options, the program lists all partitions available and detects the encryption used there, if any. The last one (container) is for PGP (.pgd) and TrueCrypt/VeraCrypt containers (the latter may have any extension).



The data extracted with EFDD can be further used for password recovery with [Distributed Password Recovery](#).

Dump physical memory

Once the disk is mounted into the system (unlocked), the system keeps the encryption keys in memory, so if you have access to the live system, the keys can be obtained easily. Select the file to dump memory to, and press Start; please note that this operation requires Administrator privileges.



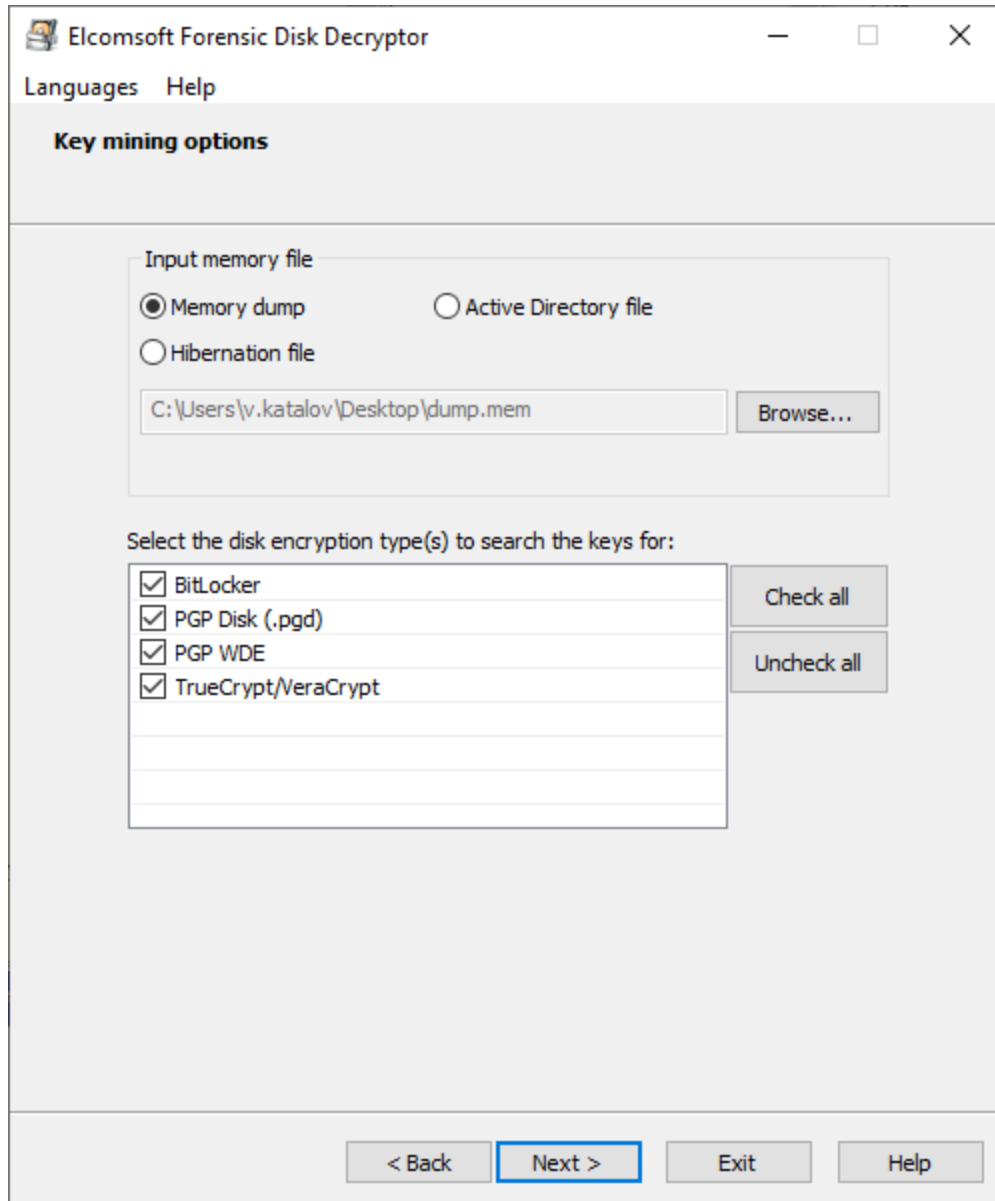
Create portable version

This option allows to create portable version of the program that can run from removable drive (on target's computer?). There are the following differences between normal and portable versions:

- portable version does not require installation; just run 'efdd.exe' to operate
- portable version does not include an option to create another portable version
- portable version cannot mount disks (just decrypt)

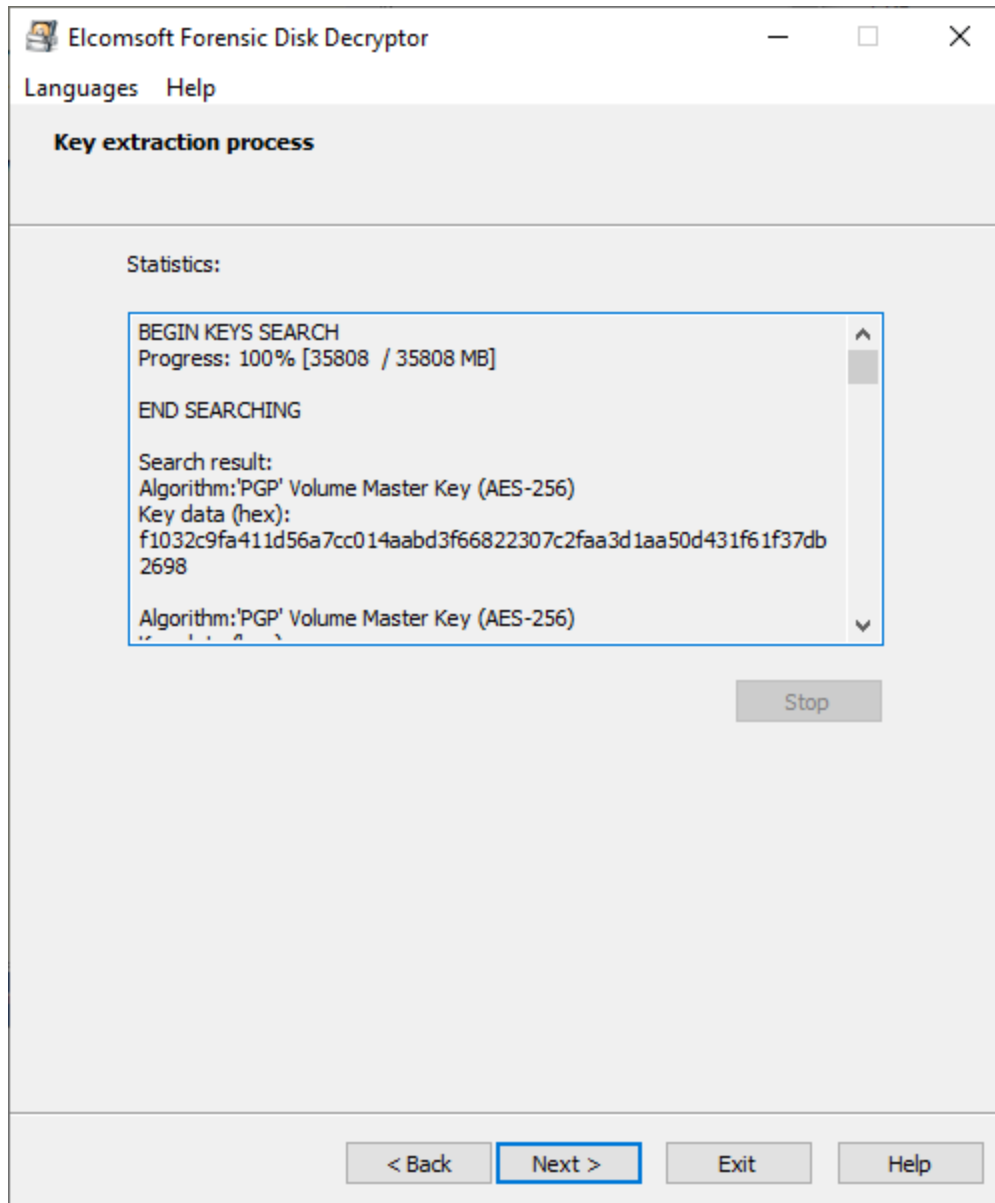
5.16.2.3 Extract keys

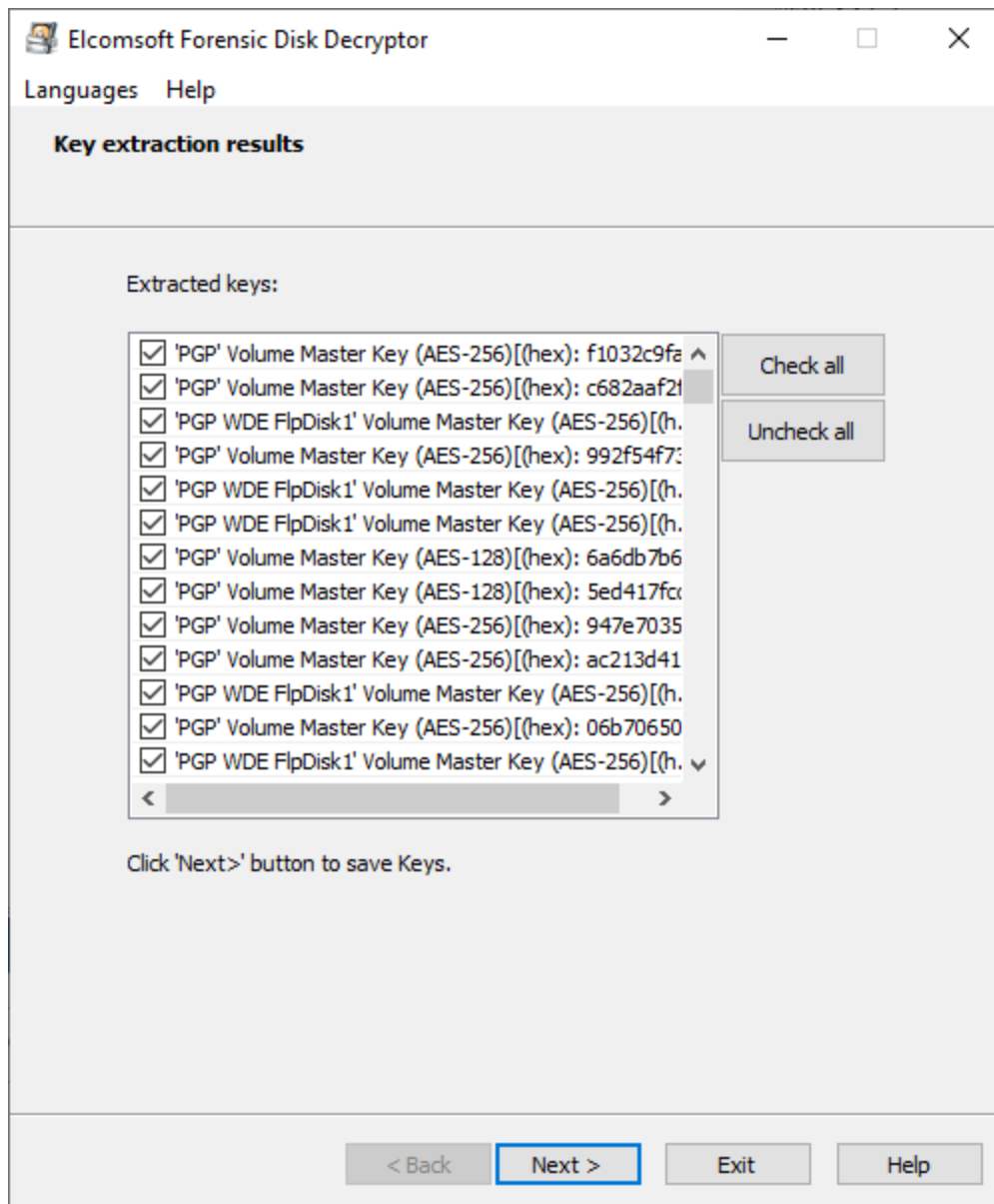
Select proper source (memory dump or hiberfil.sys) and encryption type (BitLocker, PGP or TrueCrypt/VeraCrypt) and press Next:



You can also select Active Directory (ntds.dit file) as a source; at this time, only BitLocker recovery keys are being extracted from there, though.

Once the process is completed, the list of keys found (if any) is shown, and you can save them into the file for further use.





Please note that the encrypted disk should be mounted to the system when you make the dump (or when the computer has been put to the hibernate state); otherwise, the keys are not stored in memory.

Searching for keys is a time-consuming process, so it is recommended to limit the search only to particular types of the keys.

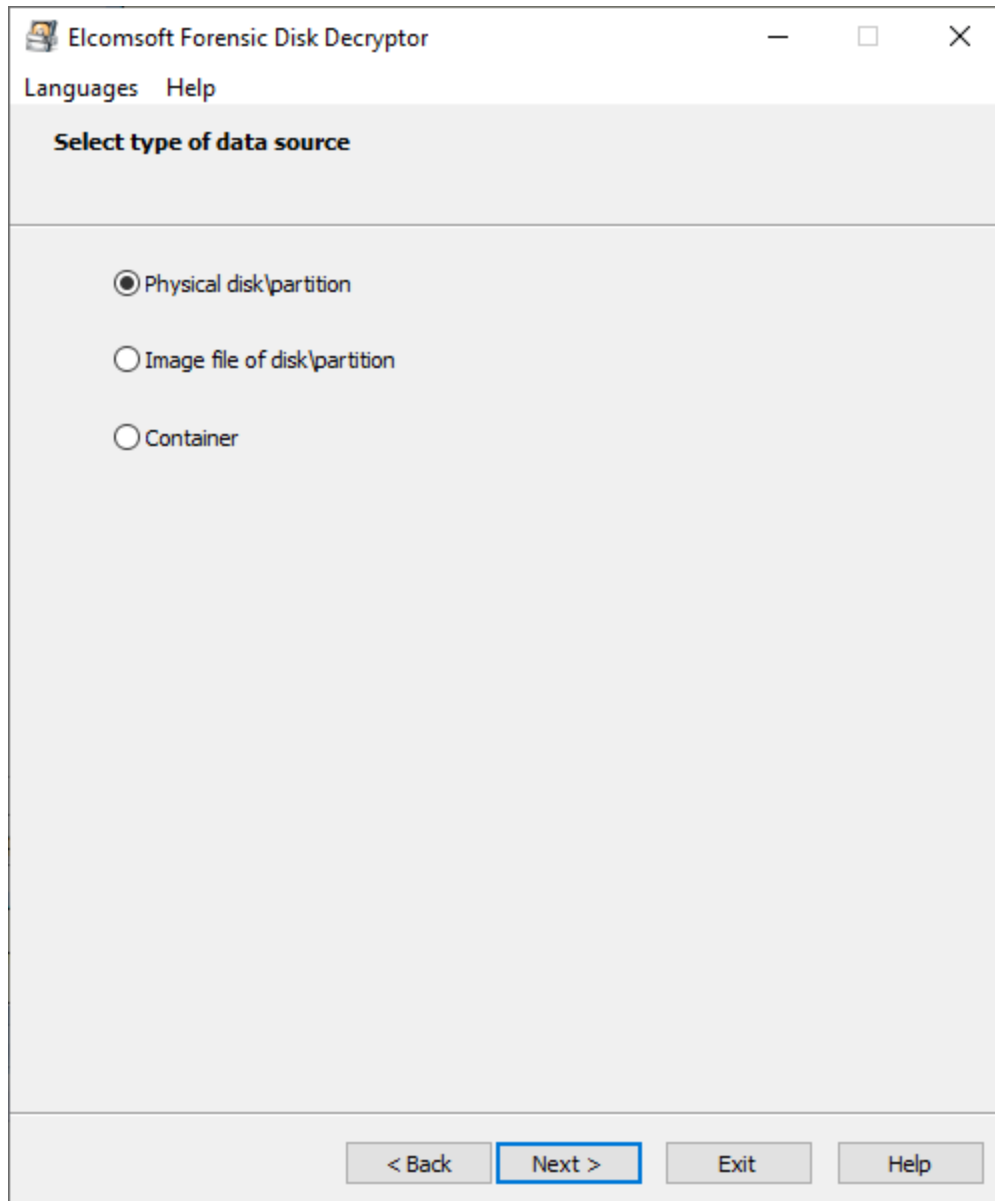
5.16.2.4 Decrypt or mount disk

You can work with actual disk attached to the computer (e.g. via USB interface), with disk images, or with the disk containers (speaking of PGP and TrueCrypt/VeraCrypt).

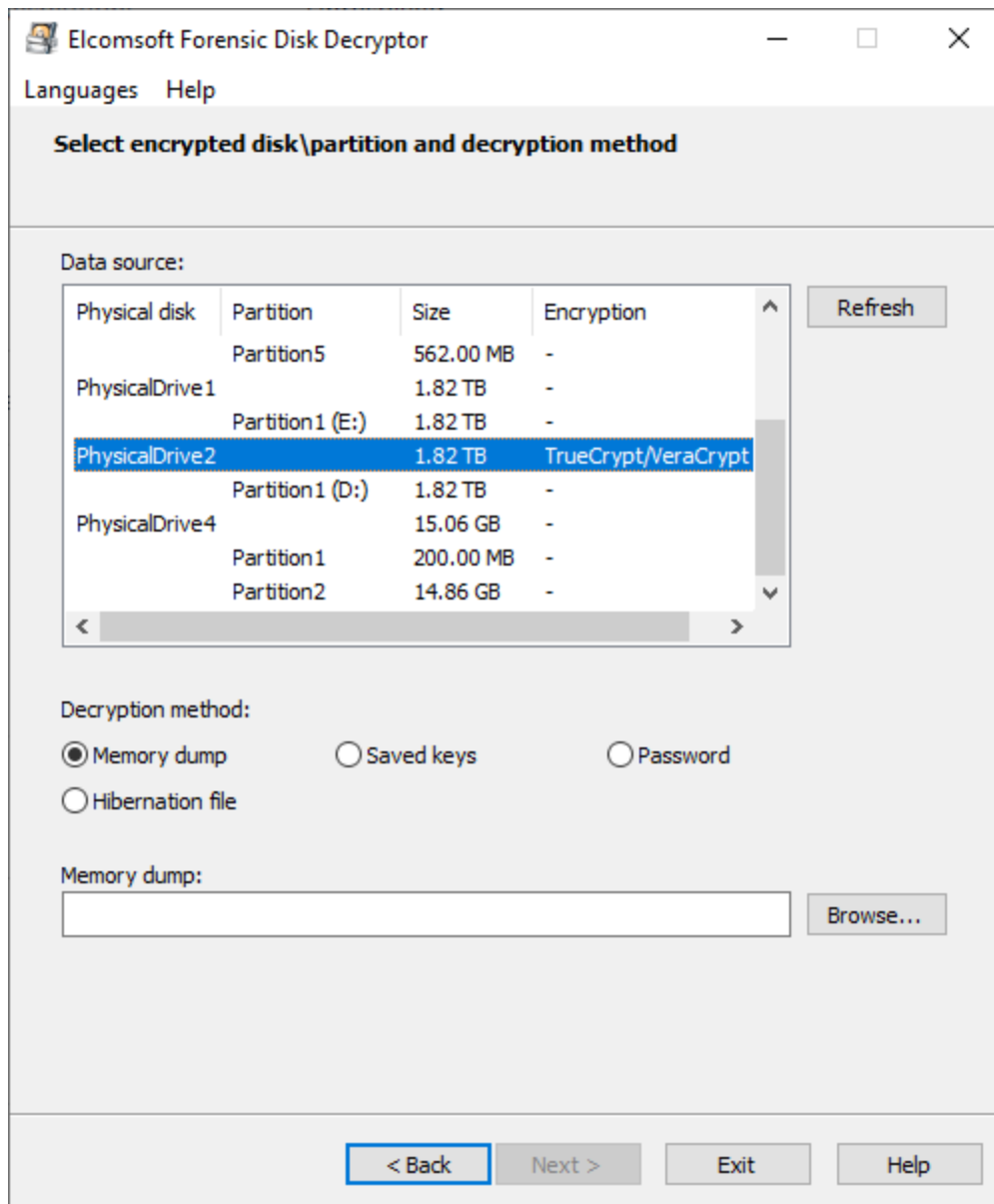
Supported disk images:

- RAW/DD
- EnCase .E01
- VHD/VHDX (Windows 8.1 or higher is required to work with these images)

Select the type of the data first:



Until the disk container is selected, the program parses it, and shows the list of partitions (if there is more than one), detecting the encryption:



Decryption or mounting (the latter is implemented using [ImDisk virtual disk driver](#) installed with EFDD; typically, you don't need to change any settings.

One of the following is required:

- memory dump (see [Extract keys](#))
- saved keys (see [Extract keys](#))
- password
- hibernation file
- active directory file (BitLocker only)
- recovery key (for BitLocker, PGP WDE, FileVault2)

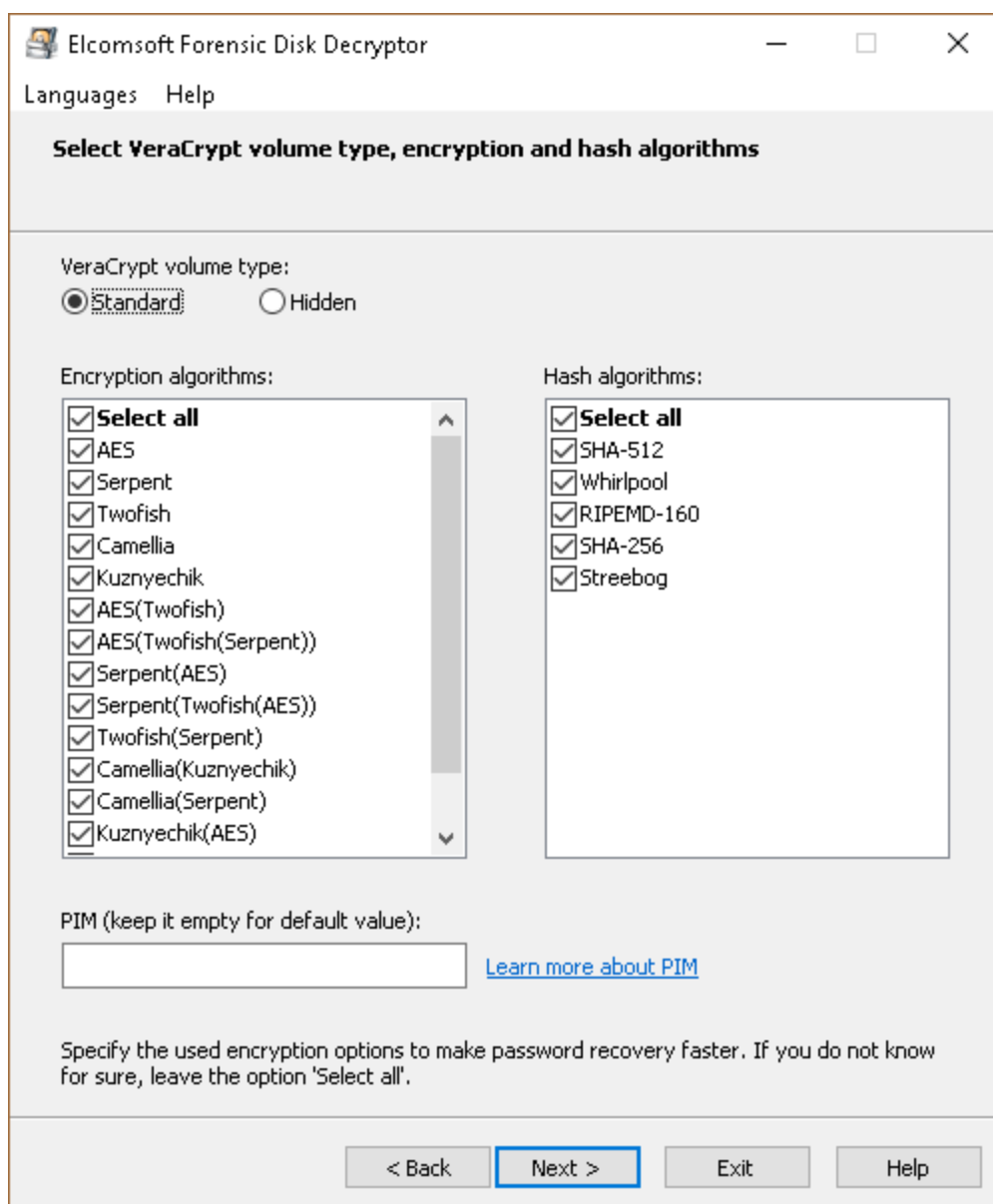
Note that this feature is not yet available for APFS partitions encrypted with FileVault2.

5.16.2.5 TrueCrypt and VeraCrypt

Choosing an encryption algorithm and hash algorithm

When creating a container or image file, the user selects some encryption algorithm and hash algorithm, as well as PIM specifically for VeraCrypt encryption.

If you know the encryption algorithm or hashing algorithm for the selected container or image file, you should specify this data in the window, which will greatly speed up the decryption process.



PIM

PIM (Personal Iterations Multiplier) - a value that specifies the number of iterations used by the header key derivation following the formulas:

To encrypt the system partition, that doesn't use SHA-512 or Whirlpool (faster but less secure):
 $\text{iterations} = \text{PIM} \times 2048$

To encrypt a non-system partition or system encryption that uses SHA-512 or Whirlpool (slower but more secure): $\text{iterations} = 15000 + (\text{PIM} \times 1000)$

It is not mandatory to specify a PIM. If the PIM value is left at zero, the default value will be used:

To encrypt the system partition, that uses SHA-256: $\text{iterations} = 200000$

To encrypt the system partition, that uses RIPEMD-160: $\text{iterations} = 327661$

To encrypt a non-system partition and standard containers, that uses RIPEMD-160: $\text{iterations} = 655331$

To encrypt a non-system partition and standard containers, that uses SHA-256, SHA-512 or Whirlpool: $\text{iterations} = 500000$

PIM is used in VeraCrypt since version 1.12

5.17 Elcomsoft Password Digger

5.17.1 Introduction

Elcomsoft Password Digger (EPD) is a Windows tool to decrypt information stored in macOS keychain. The tool dumps the content of an encrypted keychain into a plain XML file for easy viewing and analysis. One-click dictionary building offers the ability to dump all passwords from the keychain into a plain text file, producing a custom dictionary for password recovery tools. A custom dictionary containing all user passwords can be used to speed up password recovery when breaking encrypted documents or backups. Both system and user keychains can be decrypted.

Mac OS X uses keychain to manage system-wide and user passwords. System passwords are stored in the system keychain and include Wi-Fi passwords.

User keychain can contain highly sensitive authentication information such as passwords to Web sites and accounts (including the user's Apple ID password), VPN, RDP, FTP and SSH passwords, passwords to mail accounts including Gmail and Microsoft Exchange, passwords to network shares, and iWork document passwords. Third-party applications can store sensitive information in the keychain. In addition, the keychain may contain private keys, certificates,

authentication tokens, and secure notes. Information stored in the keychain is securely encrypted.

While Apple provides Keychain Access, a built-in utility for viewing keychain items, using Keychain Access is less than convenient as the user has to re-enter the password for accessing each individual record.

Elcomsoft Password Digger dumps information from Mac OS keychain into a plain, decrypted XML file that can be imported into any XML-enabled tool including Microsoft Excel for easily viewing keychain items.

5.17.2 Program information

5.17.2.1 System requirements

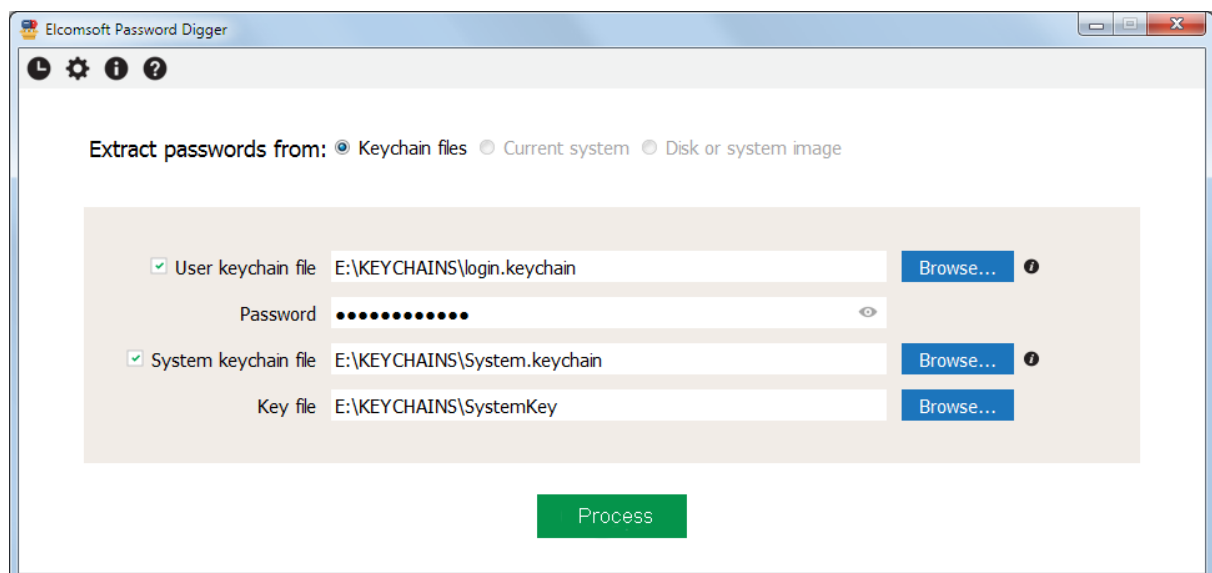
- Windows 7 or above
- about 80 megabytes of free space on hard disk

5.17.2.2 Working with the program

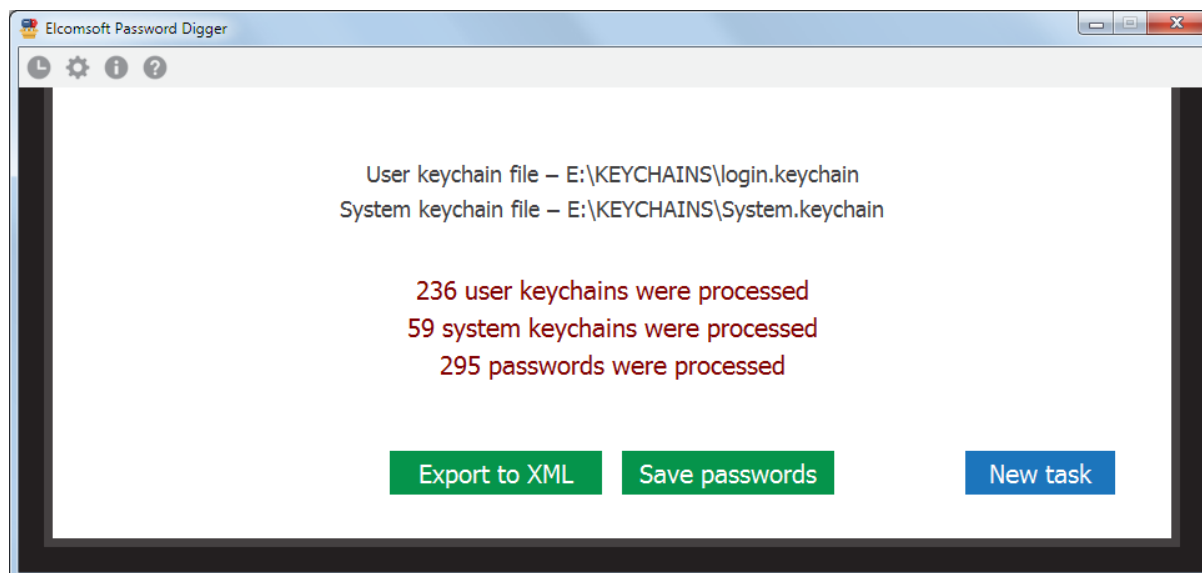
On the main program screen, select the following:

- path to user keychain file (login.keychain or login.keychain-db)
- user's password (if set)
- path to system keychain file
- path to system key file

For more information how/where to get them, please consult [Obtaining keychain files](#) chapter.



Once the files are selected (you can work with just the user's keychain, or system keychain, or both), please Process; if password is not correct, the program will not let you to proceed. The next screen shows how many records are processed in each file:



There you can export all records either to XML file (suitable for further analysis and/or reporting), or save just the passwords, so generating something like a dictionary/wordlist, e.g. to perform dictionary attacks with other software. The text file with password is sorted alphabetically (with the duplicates removed). XML file contains all the records from the keychains, including not just the passwords, but also the encryption keys, tokens etc, until you set the "Ignore non-password data in XML output" [option](#).

5.17.2.3 Obtaining keychain files

In order to decrypt the keychain with EPD, the first thing you'll need is the keychain itself. In macOS, keychain is stored in several physical files. Yet another file holds the decryption key for the system keychain. You'll need all of these in order to gain full access to encrypted information.

If you're acquiring keychain files from a live macOS system, do the following.

- Make a new folder somewhere (e.g. "KEYCHAINS" on the desktop)
- Open Terminal and issue the following command

```
cd Desktop/KEYCHAINS
```

- Copy the following files into the current folder ("KEYCHAINS"):

```
cp /Users/<username>/Library/Keychains/login.keychain .
```

```
cp /Library/Keychains/System.keychain .  
sudo cp /private/var/db/SystemKey .
```

Notes:

- you need superuser access in order to extract SystemKey, a file that contains encryption metadata for decrypting system keychain. You'll be prompted for a password.
- on macOS 10.12 and later, keychain file name (in the first command) is login.keychain-db
- there is a final dot at the end of each "copy" command. This is not a formatting error; the dot means that the file is to be copied into the current folder ("KEYCHAINS" in our case).
- <user name> is the name of the user who's keychain you are about to extract (currently logged in user is displayed before the "\$" sign).
- Transfer the content of the "KEYCHAINS" folder to the Windows PC where you have EPD installed; you may be prompted to enter your Mac administrator's password again (because of special permissions set on SystemKey file).

If you have a disk image instead of the live system, extracting files is easier since you won't need superuser access or admin password. Just mount the disk image and use your favorite file manager to copy the required files to your Windows computer.

Mounting the disk image is normally not a problem. If you're dealing with a DMG image, macOS has built-in tools to mount it. If the disk image is in EnCase .E01 format, you'll need to use third-party tools to mount the image, such as [AccessData FTK Imager](#) or [GetData Forensic Imager](#).

5.17.2.4 Program options

Apart from the program that records just the main steps you perform in the program (and which is visible right from the program interface by clicking the top-left button on the tool bar), you can set the program to create the log file. By default, logging is disabled; you can set this option to Normal (in that case, log will contain just the basic information such as opening/closing the file, decryption started/completed etc) or Debug (so including more information, that may help us to locate and fix the problem in an unlucky case if occurs).

The log file is stored in **%APPDATA%\Elcomsoft\Password Digger** folder.

Ignore non-password data in XML output option allows to filter the items from the keychains that are not actually passwords. That includes encryption keys, certificates, authentication tokens, date/time stamps, and some other data such as UUIDs. Please note that this option affects XML output only; if you export to the text files, the data is always filtered there.

5.18 Elcomsoft System Recovery

5.18.1 Introduction

Restore Access to Locked Windows Accounts

Up to 40% of support calls are related to forgotten passwords and locked logins. Recover or reset Windows system passwords easily and automatically! There is no need to format the disk or reinstall Windows. Just boot from the CD and unlock your system in a matter of minutes! Elcomsoft System Recovery can reset account passwords instantly, while supporting full-scale attacks to recover the original passwords. ESR also unlocks locked and disabled user and administrative accounts in Windows 10 and older version s(incl. Windows NT) and Windows Server (all versions).

Features and Benefits

- Ready to boot with Windows PE (Preinstallation Environment) licensed from Microsoft
- Recovers or resets user and administrative passwords
- Original password recovery may be possible to provide automatic access to EFS-encrypted files
- Unlocks and enables user and administrative accounts
- Assigns administrative privileges to any user account
- Resets or disables password expiry options
- Broad hardware compatibility and genuinely native FAT and NTFS support
- Genuine Windows GUI for convenient operation
- Supports Windows NT 4, Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8/8.1, Windows 10
- Supports Windows Windows Server 2000/2003/2008/2012/2016/2019 (including Domain Administrator password and all users' passwords)
- Supports US and localized versions of Windows and multilingual user names and passwords
- Detects all Windows installations automatically
- An option to dump hashed passwords from SAM/SYSTEM files or Active Directory database for further analysis and off-line password recovery
- An option to dump Domain Cached Credentials
- Dumps encryption keys for protected drives
- Supports Microsoft Live! accounts
- Resets or searches for SYSKEY startup password
- Password reset for Domain Cached accounts
- Dump disk encryption keys
- Unlock BitLocker-encrypted drives
- Locates encrypted virtual machines and extract encryption metadata for subsequent password recovery

- Creates forensic disk or partition images

Ready to Boot, Instant Unlock

Elcomsoft System Recovery comes as a program that makes it easy to create a bootable CD image (ISO) or USB flash drive. No need to create a reach for a Windows setup disks to make one! ElcomSoft has licensed the Windows Preinstallation Environment (Windows PE) directly from Microsoft, allowing the company to distribute the completely working bootable Windows environment based on Windows 10.

If there are no EFS-encrypted files on your Windows account, an instant unlock option is the quickest and easiest way to gain access to user and administrative accounts. Elcomsoft System Recovery resets forgotten passwords with a new password supplied by you, allowing for immediate login without the time-consuming password recovery operations.

Broad Compatibility

Elcomsoft System Recovery bootable environment supports a variety of hardware components, including the most popular hard disk controllers, thanks to Windows drivers. Unlike the various emulation environments, Elcomsoft System Recovery is genuinely compatible with the latest revisions of Microsoft file systems, including the latest versions of the FAT (FAT32, exFAT) and NTFS.

Recovers Original Passwords

In case you must know an original password to a Windows account, Elcomsoft System Recovery is fully equipped with everything needed to recover the password. Common passwords and dictionary attack are attempted first hand, and take only minutes with good chances of retrieving a password.

Elcomsoft System Recovery knows places where system passwords are cached, often allowing for instant password recovery.

Offline password recovery is easily possible by dumping hashed passwords from SAM/SYSTEM files or Active Directory database for further analysis off-line analysis. ElcomSoft recommends [Elcomsoft Distributed Password Recovery](#) for highly scalable, GPU-accelerated recovery of system passwords.

5.18.2 Program information

5.18.2.1 Requirements and limitations

- A minimum of 512 MB of RAM
- The product allows to view/change some properties (Administrator account, Account is locked/disabled, Password expired, Password never expires) for local user accounts only, but not for AD accounts
- Some computers may require 3rd party mass-storage drivers (RAID, SCSI, SerialATA etc). You can load additional drivers right when ESR is already booted (from CD, USB flash drive or floppy disk) or use one that comes with the program
- When you boot from the CD, you cannot save password hashes back to the disk, but only to the hard drive.

There are also some special requirements for booting the computer from UFD (USB Flash Drive), as defined by Microsoft for Windows PE:

- The size of the UFD cannot be smaller than 256 megabytes.
- The size of the UFD cannot be larger than 32 GB.
- The UFD must report a drive type of Removeable, not Fixed.
- The UFD must be first in the list of boot devices in the computer BIOS.
- The computer BIOS must support the extended INT 13h (xINT13) BIOS interrupt for UFDs.
- The computer BIOS must support booting from UFDs.
- The computer's USB controller must support bulk-only transport (BOT).

ESR has been designed for maximum compatibility and should be able to boot even from external hard disk (USB or FireWire) including ones that are larger than 32 GB, but some restrictions still apply.

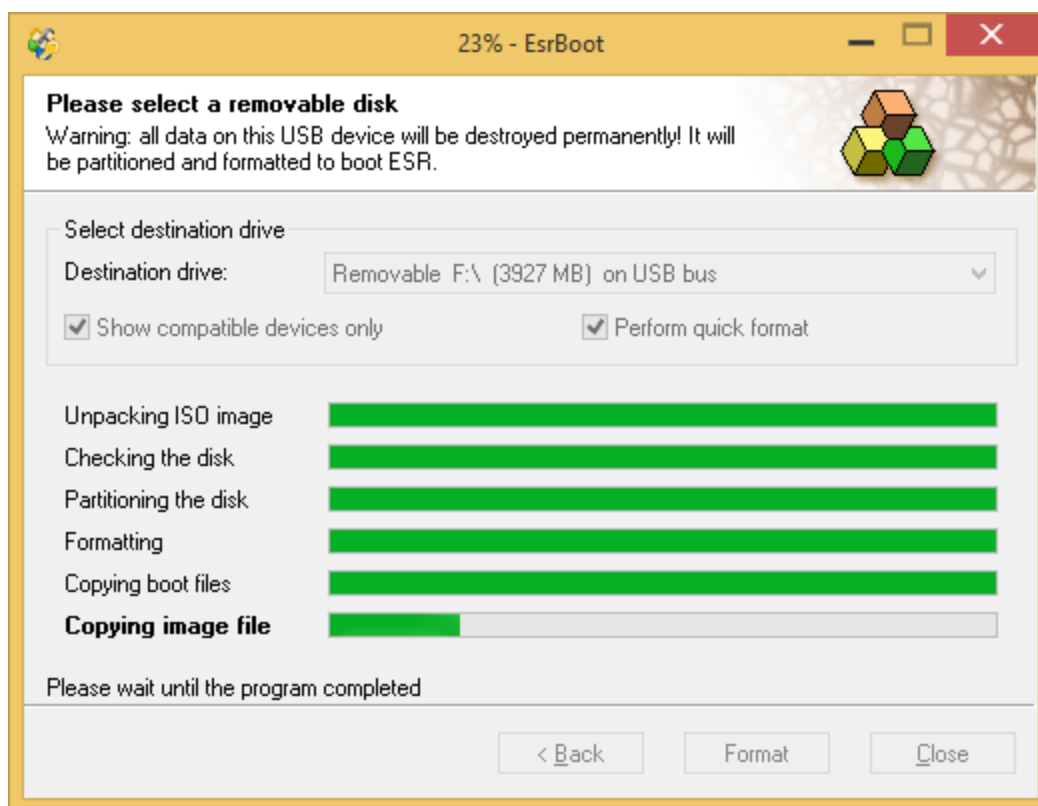
Please note that after you reset the password, you may lose access to the user's: web page credentials, file share credentials, DPAPI encrypted stuff, EFS-encrypted files and certificates with private keys (signed/encrypted e-mail). For more information, please look at Microsoft Knowledgebase article: [KB290260](https://support.microsoft.com/kb/290260).

5.18.2.2 How to create a bootable UFD

Start the ESRBOOT utility and follow a few simple steps to create a bootable UFD:

- Accept the ElcomSoft end user license agreement
- Enter your license key
- Select an option for creating bootable USB drive
- Attach the removable device you would like to format as a bootable disk (warning: all data on this disk will be deleted!)

- Select the disk from the Destination drive drop-down box. It is recommended to have an option Show compatible devices only enabled; you may wish to switch it off only if ESRBOOT does not show your removable disk while you're sure you can boot from it.
- The program verifies that the given disk can be configured to boot ESR; creates a special partition; creates a logical drive; formats the drive; makes this drive bootable; copies the ESR files (Windows PE and the ESR itself):



5.18.2.3 How to use the program

5.18.2.3.1 Booting from the CD or UFD

To boot your computer from ESR CD, you should setup you BIOS to have the CD-ROM drive as the first device in the list:

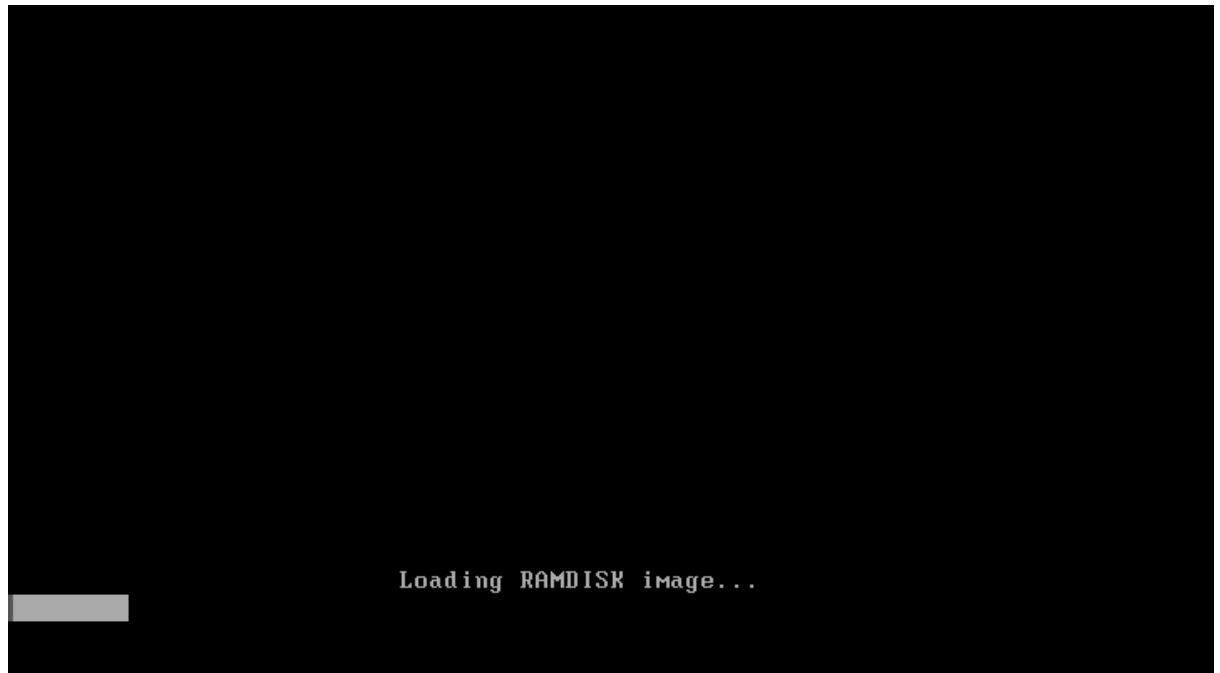
PhoenixBIOS Setup Utility							
Main	Advanced	Security	Power	Boot	Exit		
CD-ROM Drive +Removable Devices +Hard Drive Network boot from AMD Am79C970A						Item Specific Help	
						Keys used to view or configure devices: <Enter> expands or collapses devices with a + or - <Ctrl+Enter> expands all <Shift + 1> enables or disables a device. <+> and <-> moves the device up or down. <n> May move removable device between Hard Disk or Removable Disk <d> Remove a device that is not installed.	
F1	Help	↑↓	Select Item	-/+	Change Values	F9	Setup Defaults
Esc	Exit	↔	Select Menu	Enter	Select ► Sub-Menu	F10	Save and Exit

Then, simply insert the ESR CD and reboot. You will see the Press any key to boot from CD message:



Press any key to boot from CD.._

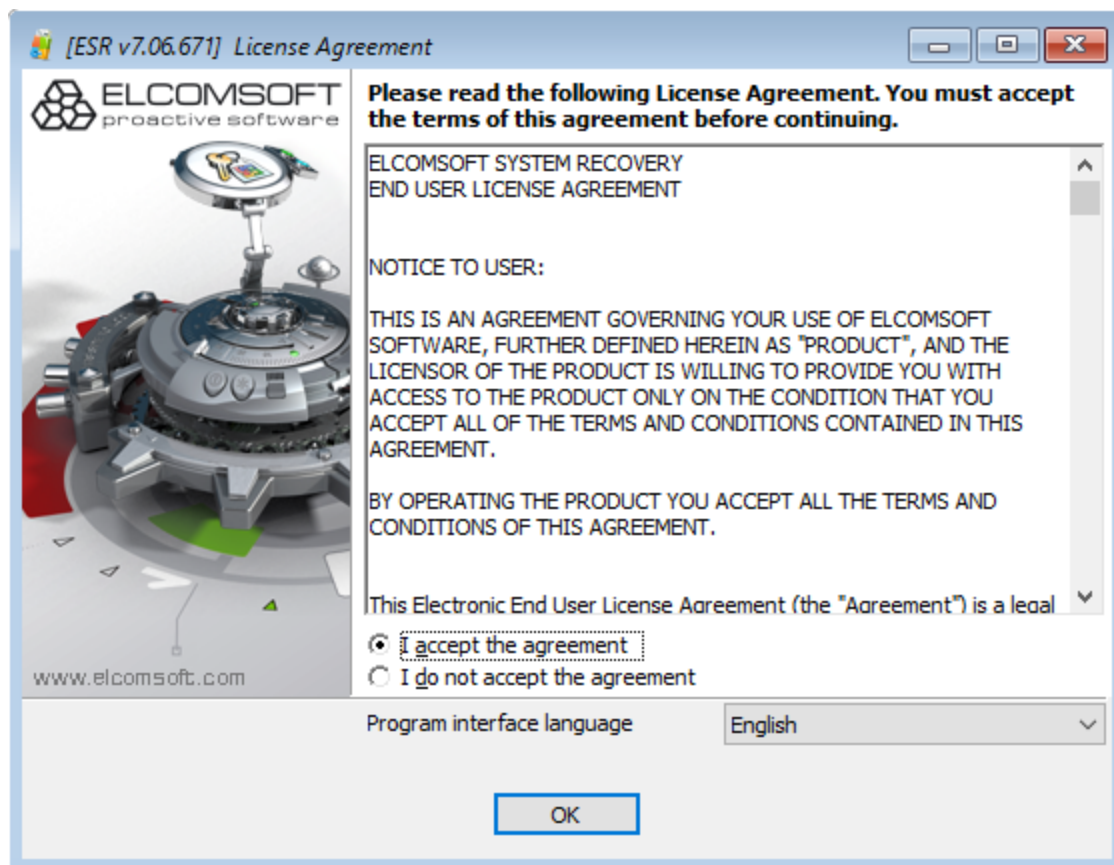
Simply press any key (such as <Space> or <Enter>), and ESR will start booting (creating the RAM drive and loading Windows PE):



Loading RAMDISK image...

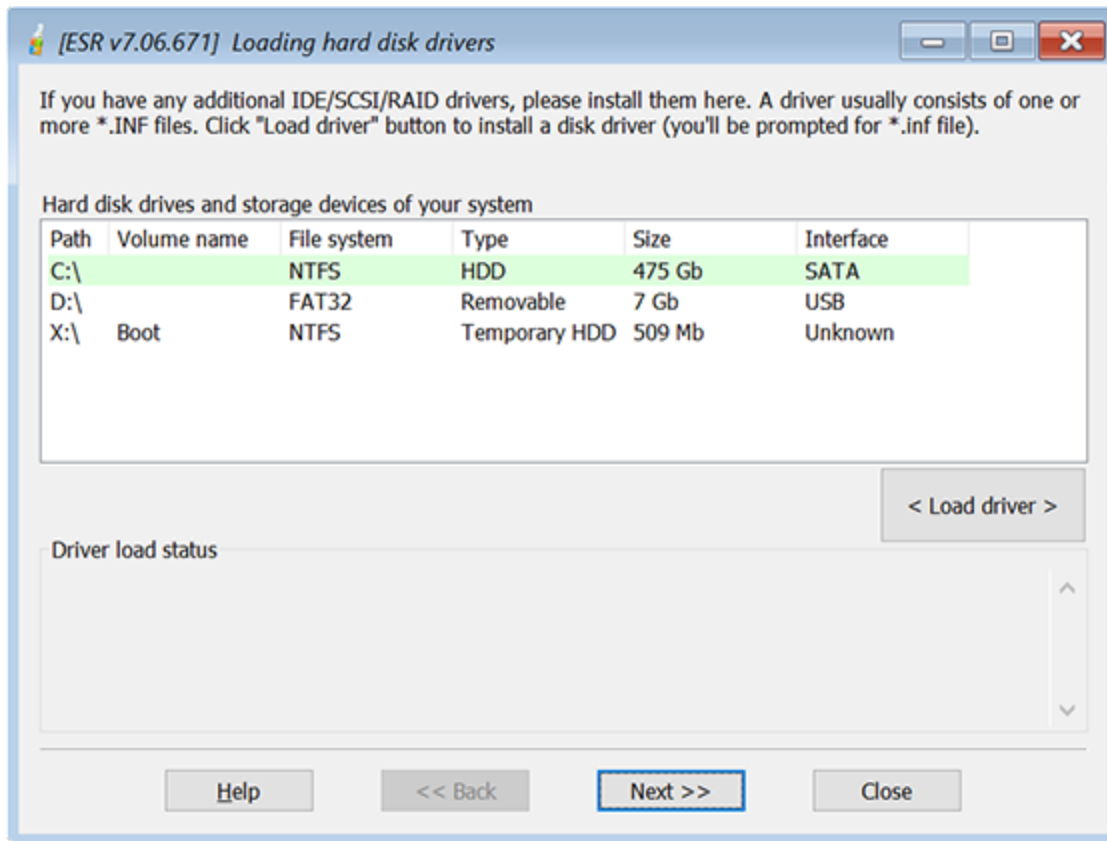
If you boot from the UFD (see [How to create a bootable UFD](#)), the steps are generally the same. You will just have to setup your BIOS to boot from the USB device first (not the CD); also, there will be no Press any key... message during boot process.

When ESR is booted, the first screen shows the license agreement (you have to accept it) and allows to select the program user interface language:



5.18.2.3.2 Mass-storage drivers

If your system uses non-standard mass-storage adapters (such as some SerialATA, SCSI, RAID or SAS), you may need to specify the appropriate drivers:



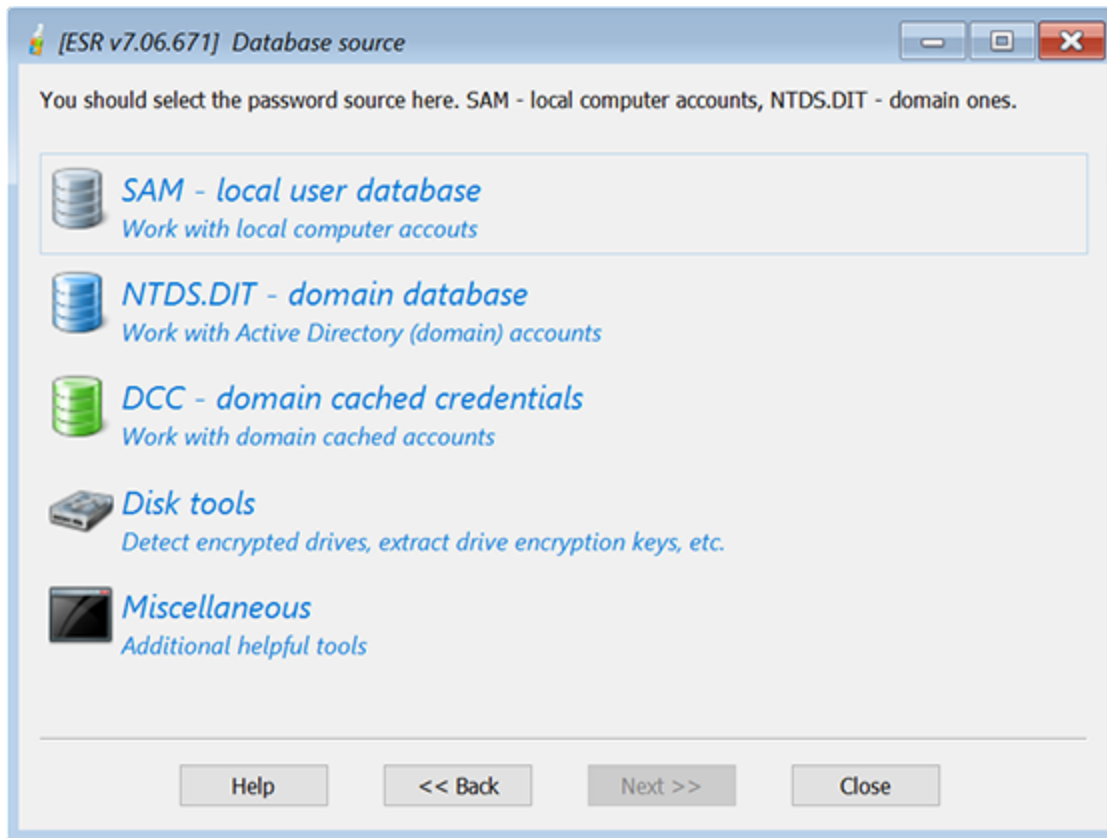
The list of all local drives is shown here; if you cannot see the partition with your operating system, press Load driver button, and browse for the disk (floppy, USB flash disk or CD) that contains the drivers for your disk(s). ESR will load the driver you specified, and update the list of available partitions. The Driver load status window will let you know whether the driver has been loaded successfully.

5.18.2.3.3 Database source and working mode

Database source

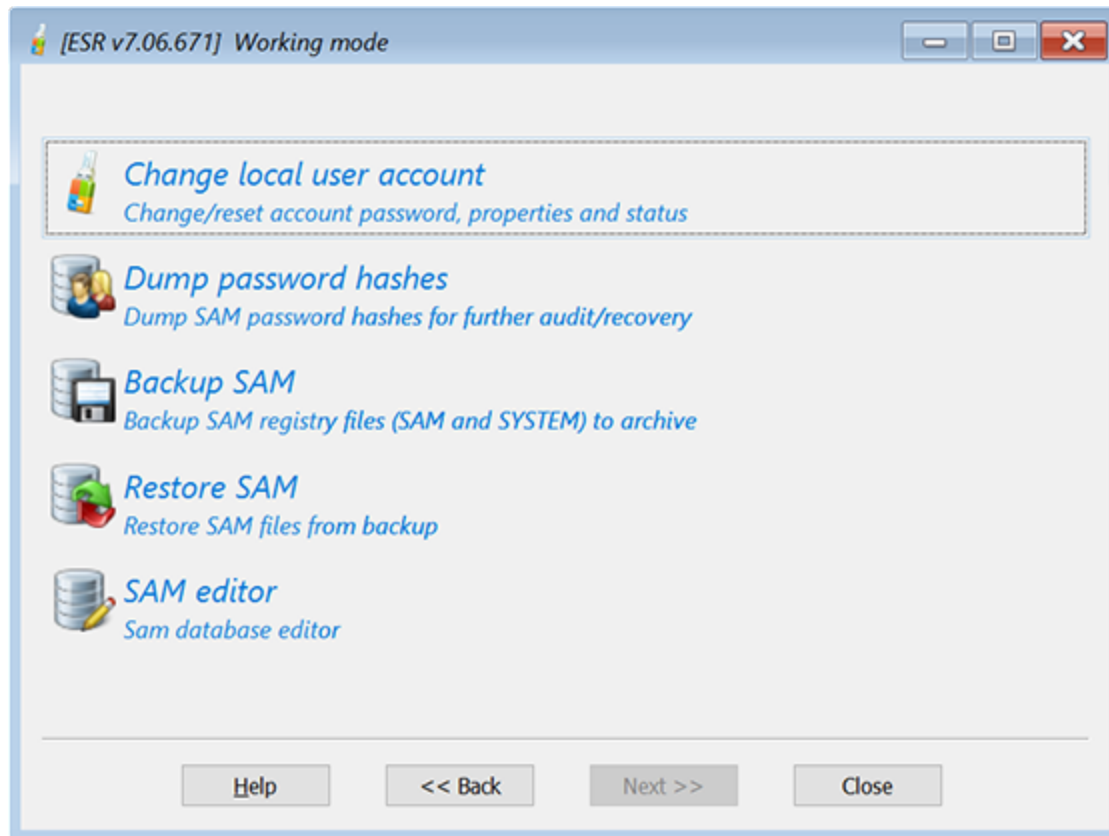
Accounts database source allows to select between local and Active Directory accounts. Please note that to work with AD, you should use ESR on the server (domain controller) running Windows Server 2000/2003/2008/2012/2016/2019.

- Work with local computer accounts (SAM)
- Work with Active Directory accounts (ntds.dit)
- Work with domain cached accounts
- Tools to search for disk encryption keys
- Additional utilities



Working mode

- Change account password and properties
- Dump password hashes for further audit/recovery
- Backup Registry or Active Directory to archive
- Restore Registry or AD from backup
- SAM database editor
- Reset DSRM password



If you already changed some account properties or password(s) and would like to rollback the changes, select the last option: Restore Registry or AD from backup (you will be prompted for locations of backup copy of Windows registry or AD database). Otherwise, select Change account password and properties (to change/reset passwords to user accounts, unlock disabled or locked accounts etc), or Dump password hashes ..., if you would like just to dump password hashes from AD or registry into the text file for further analysis/recovery in other software like [Proactive Password Auditor](#) or [Elcomsoft Distributed Password Recovery](#). Finally, you can backup the Registry (SAM, SECURITY and SYSTEM) or Active Directory database (ntds.dit).

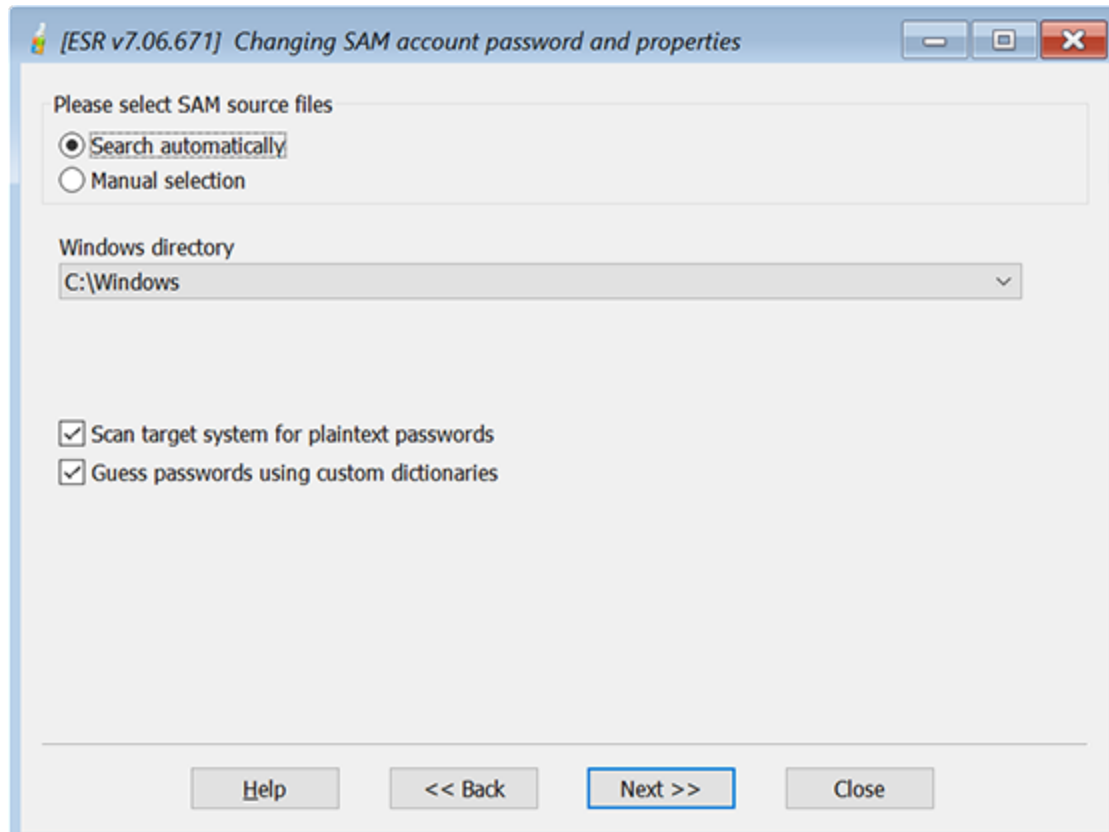
When you dump local password hashes (from SAM), password history hashes are also extracted (and saved into the dump file).

Password hashes can be saved (into the "standard" dump) file in ASCII or UNICODE character set. After dumping, the program asks would you like to open that file in the Notepad; please note that if the user names or comments use non-US alphabet, they will be shown correctly only in UNICODE (and in ASCII dump file, you may see just the asterisks).

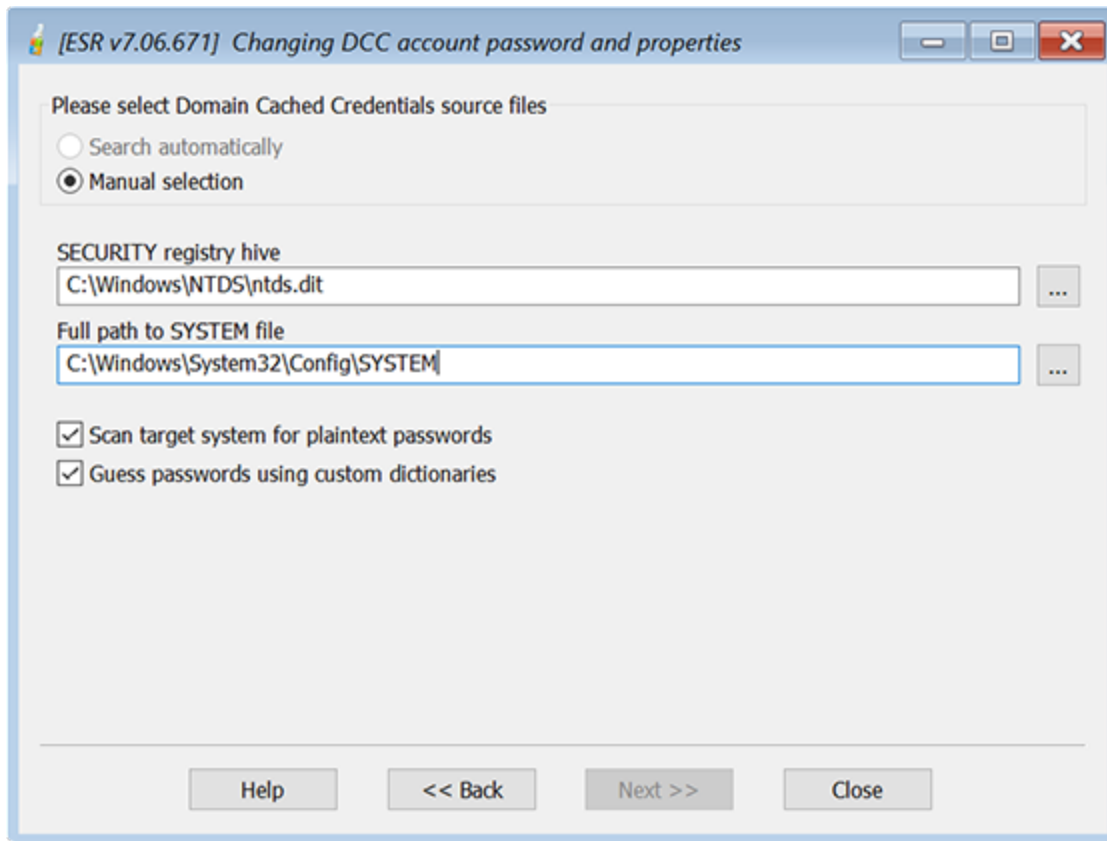
Finally, [SAM database editor](#) allows to edit all the fields in SAM database, that contain the advanced properties of local user accounts.

5.18.2.3.4 Select operating system or SAM/AD files location

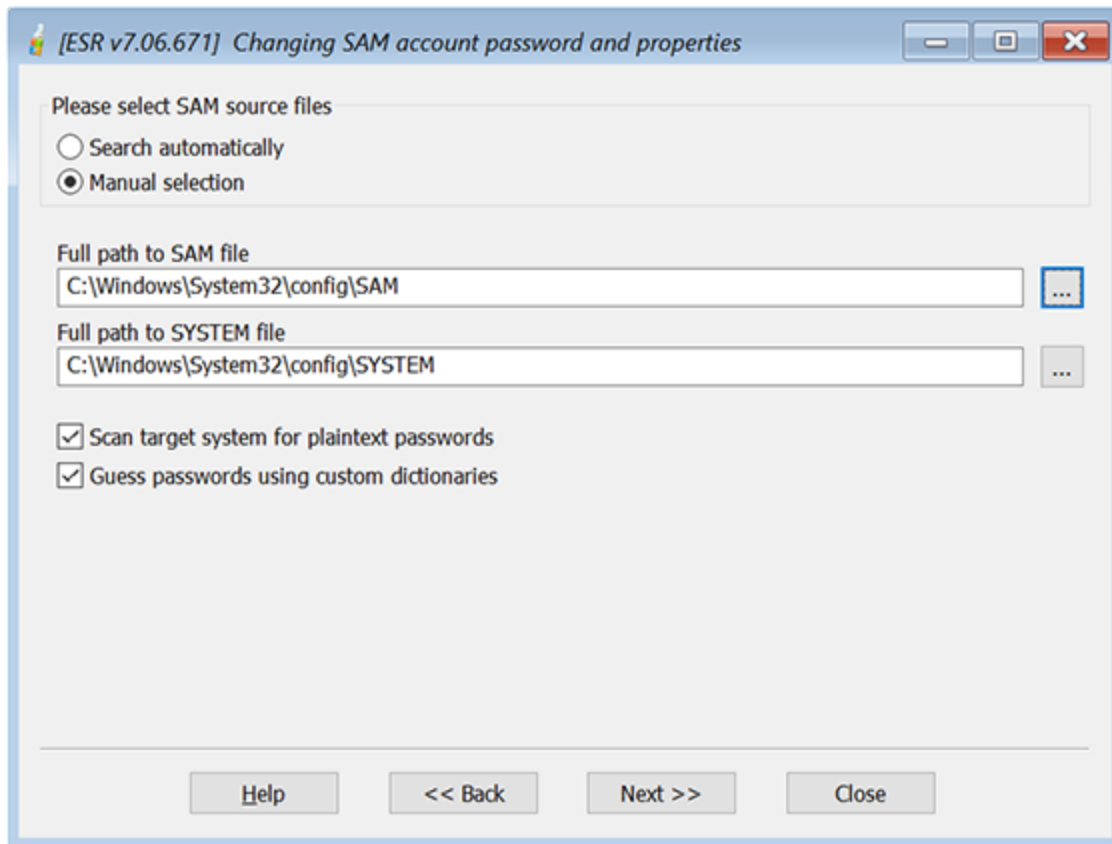
Once you have selected the database source (SAM, DCC or AD) and working mode (task), you will be prompted for the operating system to work with (note: if your system uses non-standard mass-storage adapters such as SCSI or SAS that are not supported by the ESR, you may need to specify additional drivers; see [Mass-storage drivers](#) chapter for details). With the Auto selection, you just select the system folder from the drop-down box:



With Manual selection, you have to select either the location of the AD database and SYSTEM Registry file (using [...] button at the right):



or the location of SAM, SECURITY and SYSTEM files:



In manual mode, it is recommended to select the location of SYSTEM file first, so the location of SAM/SECURITY (or AD database) will be inserted automatically. The default location of SAM, SECURITY and SYSTEM files is:

%WINDOWS%\SYSTEM32\CONFIG\

And AD database (ntds.dit) is usually stored in the following folder:

%WINDOWS%\NTDS\

When browsing for SAM/SECURITY/SYSTEM/AD files, if you don't see the local drive(s), that means that you do not have necessary drivers (such as SerialATA, SCSI, RAID etc) installed. You may need to specify them during boot process (see [Booting from the CD or UFD](#) chapter for details).

Please note that if your system uses non-default SYSKEY mode (i.e. SYSKEY is not stored in the Registry), then the program will prompt you for startup password or SYSKEY floppy disk. If you do not supply them, password hashes cannot be extracted (decrypted), and so you will not be able to change account passwords or properties, or even dump password hashes into the text file.

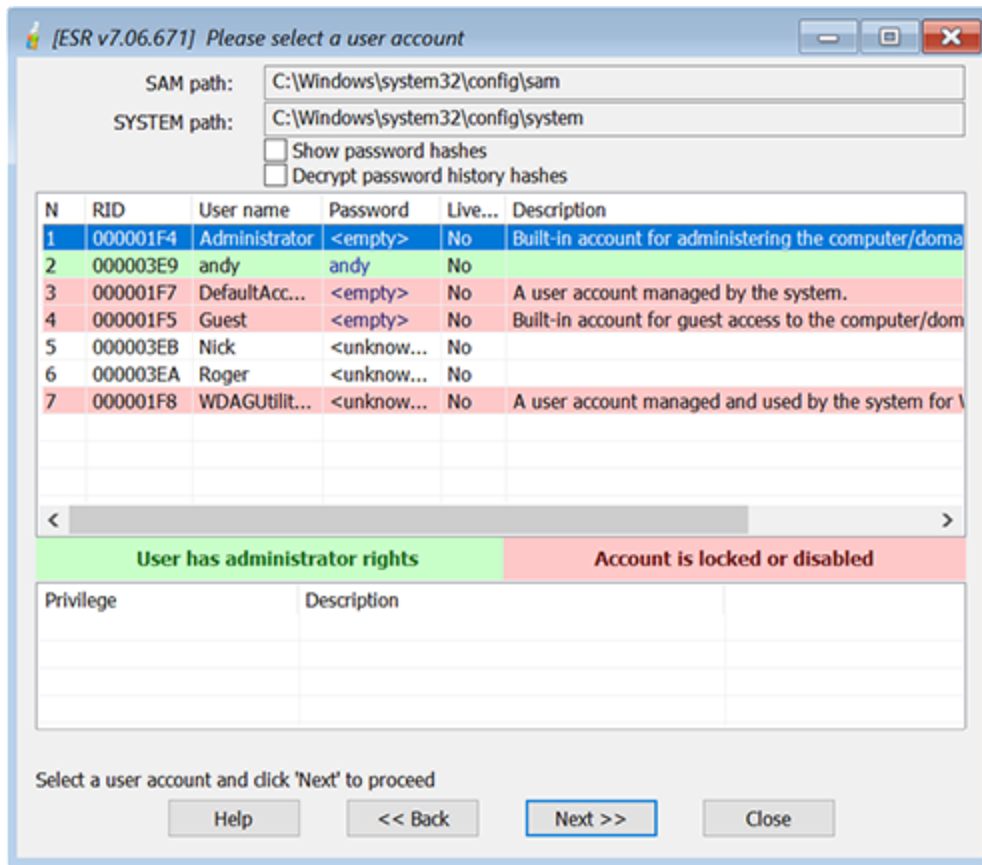
If you have selected Test short and simple passwords option, then ESR will try to recover passwords using several pre-defined built-in dictionary and brute-force attacks, as well as decrypt some passwords that are stored/cached/encrypted in other files. That does not mean that many passwords will be recovered, but takes only a few minutes (may be more on slow computers, so you may wish to disable this option) and really helps to recover short and simple passwords, so you will not need to reset them. Here are the passwords that are being tested:

- obvious combinations like passwords that are equal to login names
- stored dial-up passwords
- passwords from secrets (SECURITY registry file)
- passwords from some browsers that can be decrypted instantly
- LM passwords
 - 4-characters (caps, digits, 16 symbols)
 - passwords from wordlist
 - passwords from wordlist with one digit at the end
- NTLM passwords
 - 4 characters (small, digits, 16 symbols)
 - 4 chars (small, caps)
 - 5 chars (small)
 - 5 chars (caps)
 - 7 chars (digits)
 - 3 chars (all symbols)
 - passwords from wordlist
 - repeatable combinations (like '00000', 'aaa' etc)
 - keyboard combinations (like 'qwerty')
 - keyboard combinations on OEM layout

Then, the program creates a few different 'mutations' for the passwords that have been found at previous steps, and try to apply them to all accounts.

5.18.2.3.5 Local user accounts

If you work with the local (SAM) accounts, you get the list of all local accounts after selecting the operating system or SAM and SYSTEM files:



The accounts that has Administrator rights (privileges) are highlighted with the green color, and the accounts that are locked or disabled are colored with red.

You can also enable Show password hashes option to see the LM and NTLM hashes for all accounts that have non-empty passwords, and Show password history option to see the 'old' records that are available (if saving the password history is enabled in the given system).

Simply select the account you want to change the password or properties for, and press Next; and you will get a detailed information about it:

[ESR v7.06.671] Change account password (SAM)

SAM path: C:\Windows\system32\config\sam
SYSTEM path: C:\Windows\system32\config\system
Account name: Nick RID: 000003EB
Password: Password&094

Administrator flag
☒ Administrator account

Account type
☐ Temporary account ☐ Interdomain trust account
☒ Normal account ☐ Workstation trust account
☐ MNS account ☐ Server trust account

Password flags
☒ Password not required ☐ Encrypted text password allowed
☒ Password never expires ☐ Password expired

Misc flags
☐ Trusted for delegation ☐ Account disabled
☐ Not delegated ☐ Account is locked out
☐ Trusted to auth for delegation ☐ Home directory required
☐ Don't required preauth ☐ Smart card required
☐ Use DES key only

Password policy
Minimum password length: 0 Password history length: 0
Password properties flag:

Items to change: user password, admin status

Help << Back Apply Close

Here you can reset/change the password as well as the following account properties:

- Administrator account
- Password never expires
- Password expired
- Account disabled
- Account is locked out

After you make necessary changes, press Apply. You will be prompted for location and name of backup copy of SAM database.

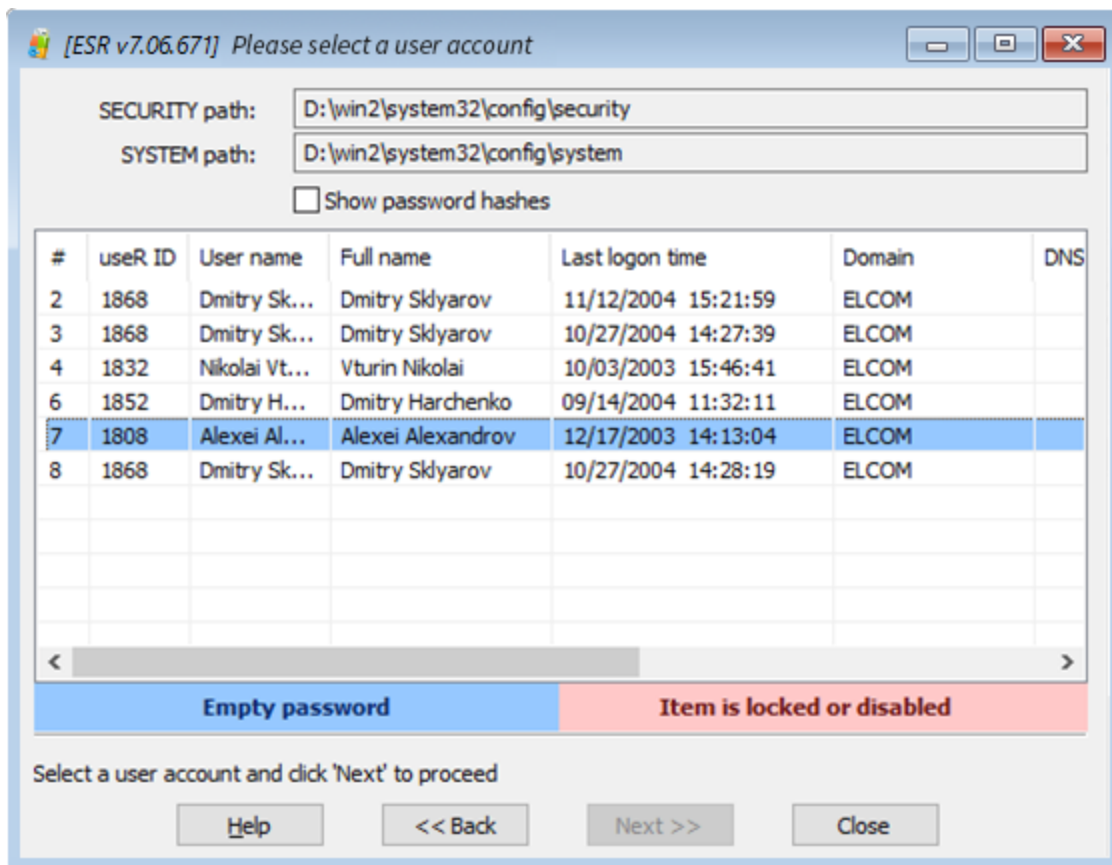
It is NOT recommended to just reset the password (set the empty password as a new one) -- instead, select the new (complex) password for security reasons. Please also note that the local security policy may be applied, and so while you're able to set any (even empty) new password, you might not be able to log on with that new password if it does not comply the password policy. Finally, you cannot give Administrator privileges to built-in accounts such as Guest; it is also not recommended to change the password or any properties for any accounts in Guests user group.

5.18.2.3.6 AD accounts

If you work with Active Directory accounts, you will get a list of all Active Directory accounts along with their properties. Here you can reset the password to any Active Directory user (including Domain Administrator), like for [local user accounts](#). However, you cannot change any of account properties (like Administrator account, Password never expires etc).

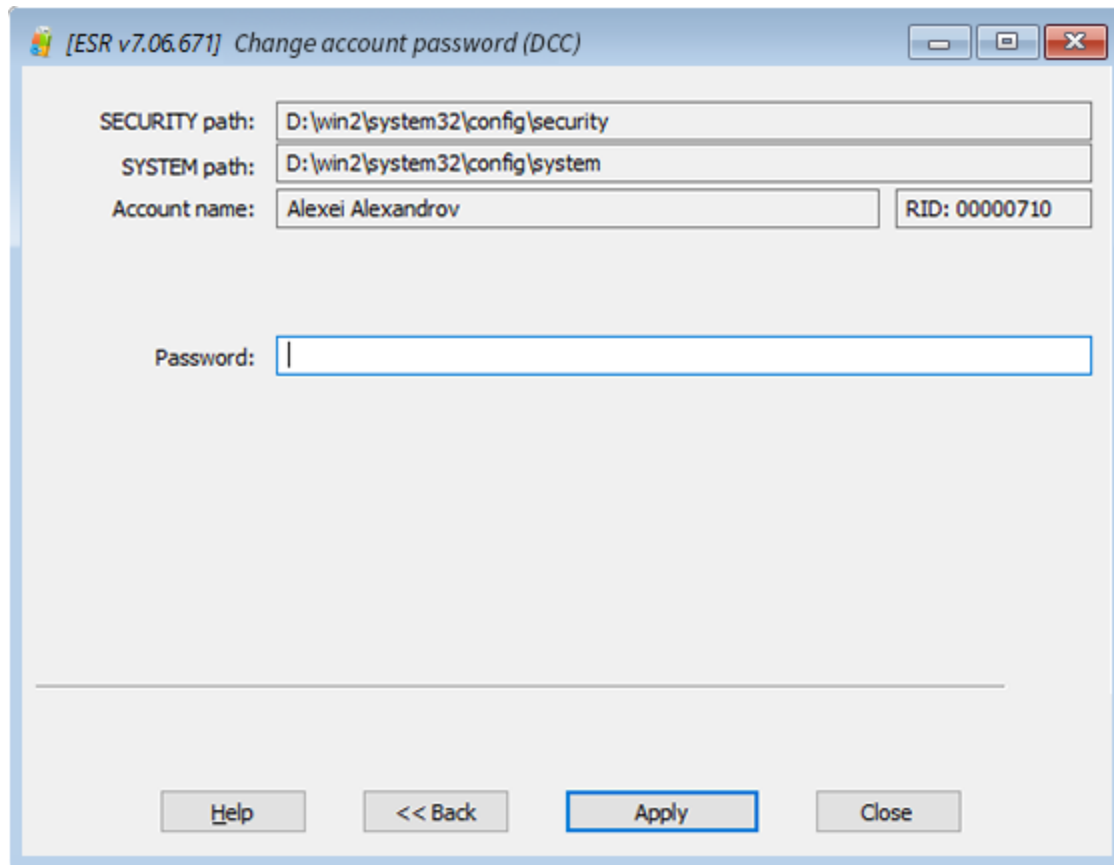
5.18.2.3.7 Domain cached accounts

Once the Windows directory (or SECURITY and SYSTEM files) is selected, the program tries to locate and decrypt domain cached entries and display the list of found cached user accounts.



The accounts with empty passwords are highlighted with the blue color, and the accounts that are locked or disabled are colored with red.

Select the account you want to change the password for, and press Next>> to proceed to the next step.

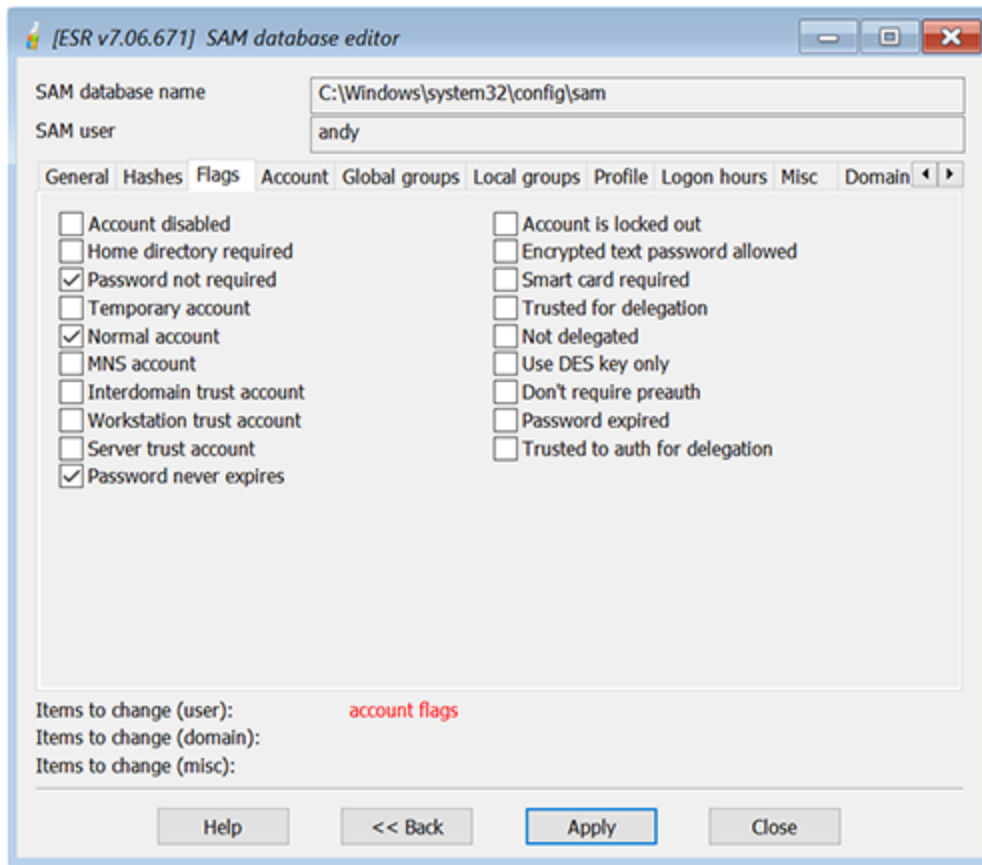


Type in a password or wipe out the appropriate input field then press the Apply button. You will be prompted for backing up the SECURITY file. It is highly recommended to backup the file before applying final changes.

Please note that to log on into the domain account after the password was reset, you will need to disable connection to the domain. Otherwise Windows will not use the cached credentials.

5.18.2.3.8 SAM database editor

SAM database editor allows to view and change most properties of all local user accounts:



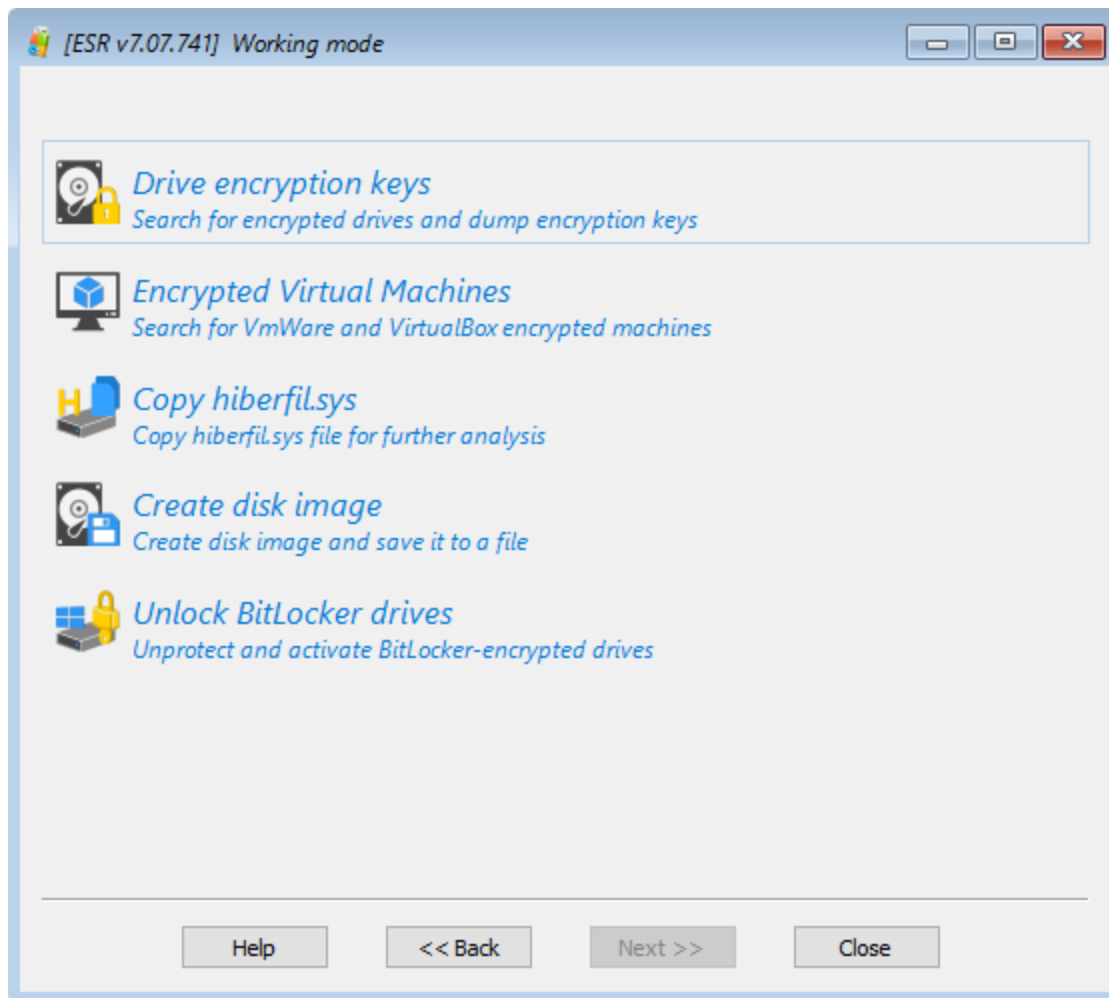
The following information is shown:

- General (user name, full name, comment, user ID)
- Hashes (LM and NTLM)
- Flags (most important user account's properties)
- Account (time of last logon and logoff, password last set, account expiration, last bad password)
- Global and local groups (membership)
- Profile (home directory, script/profile path)
- Logon hours
- Misc (SAM database revision, country code, code page etc)
- Domain information, properties and password properties

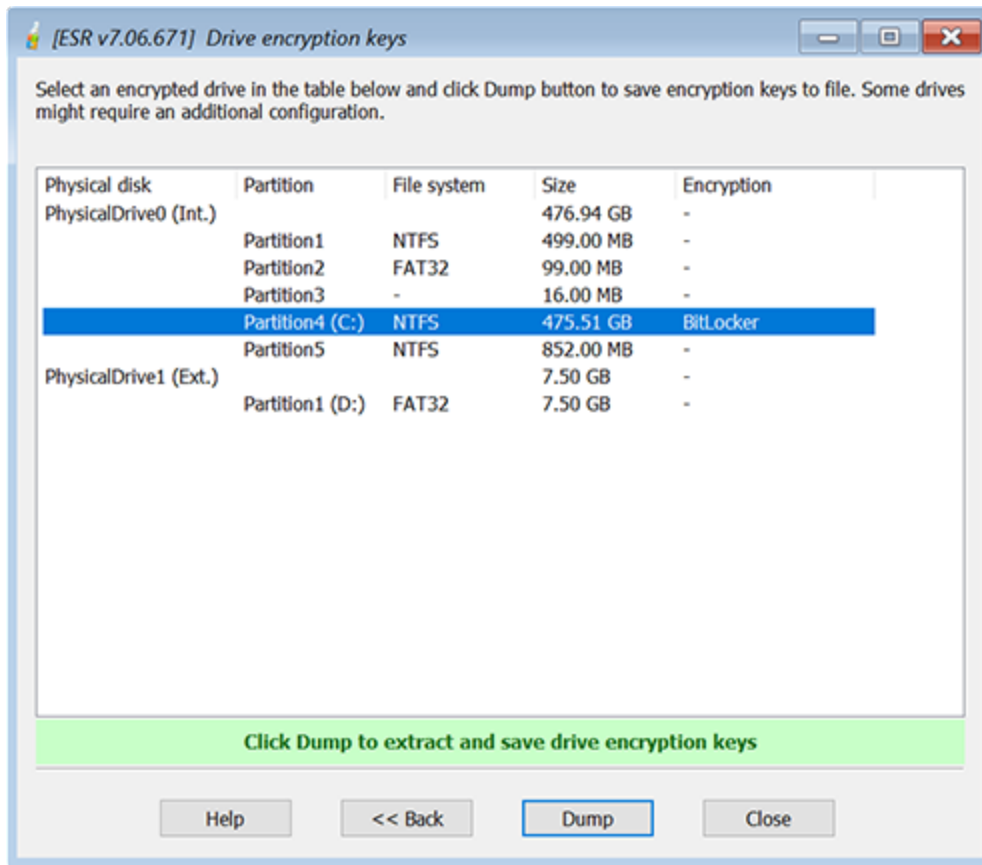
It is not recommended to edit any of SAM database fields until you are absolutely sure what you are doing.

5.18.2.3.9 Disk tools

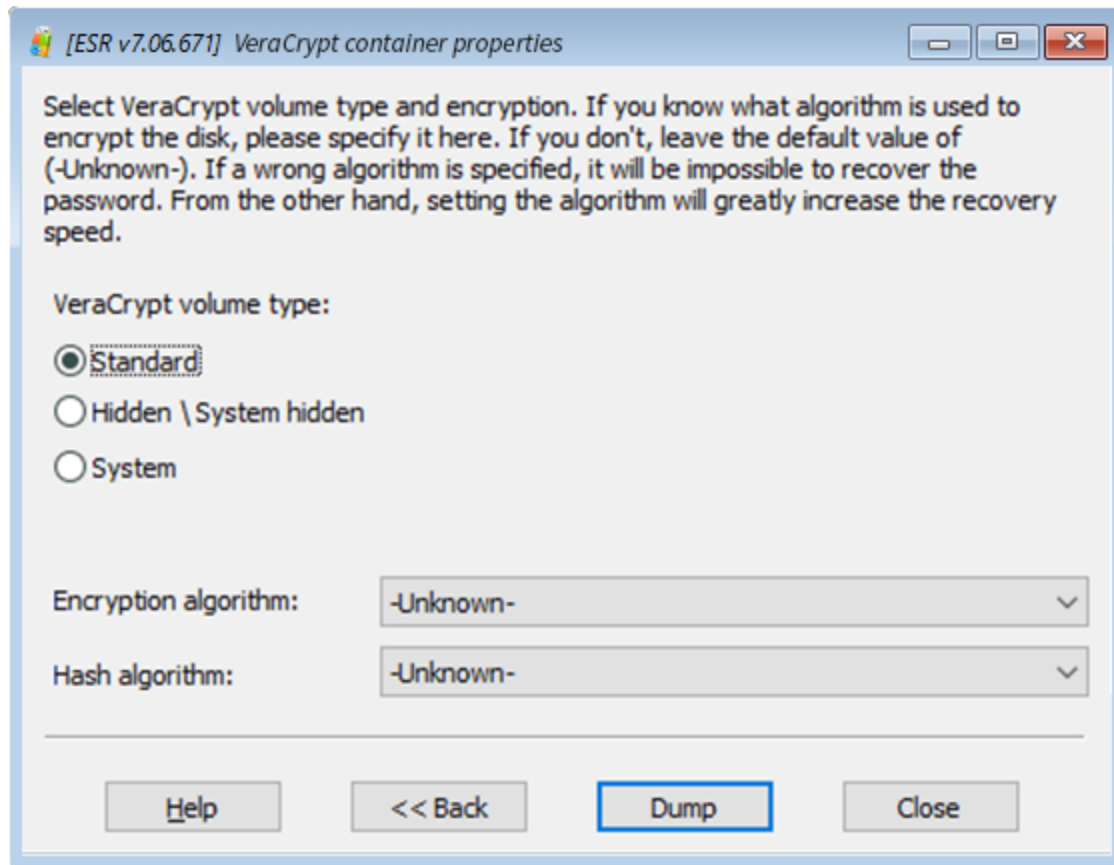
In disk tools dialog you can search for encrypted drives or virtual machines and dump encryption keys for further recovery. For example, in Elcomsoft Distributed Password Recovery. You can also create forensic disk or partion images.



Once the program detects an encrypted drive, select it in the table and click the Dump button to save the disk encryption keys.



TrueCrypt/VeraCrypt disks require additional configuration. You might need to set the encryption algorithms explicitly in order to apply faster recovery.



The program support for the following encryption types:

- BitLocker
- PGP Disk
- PGP WDE
- TrueCrypt
- VeraCrypt
- FileVault
- LUKS

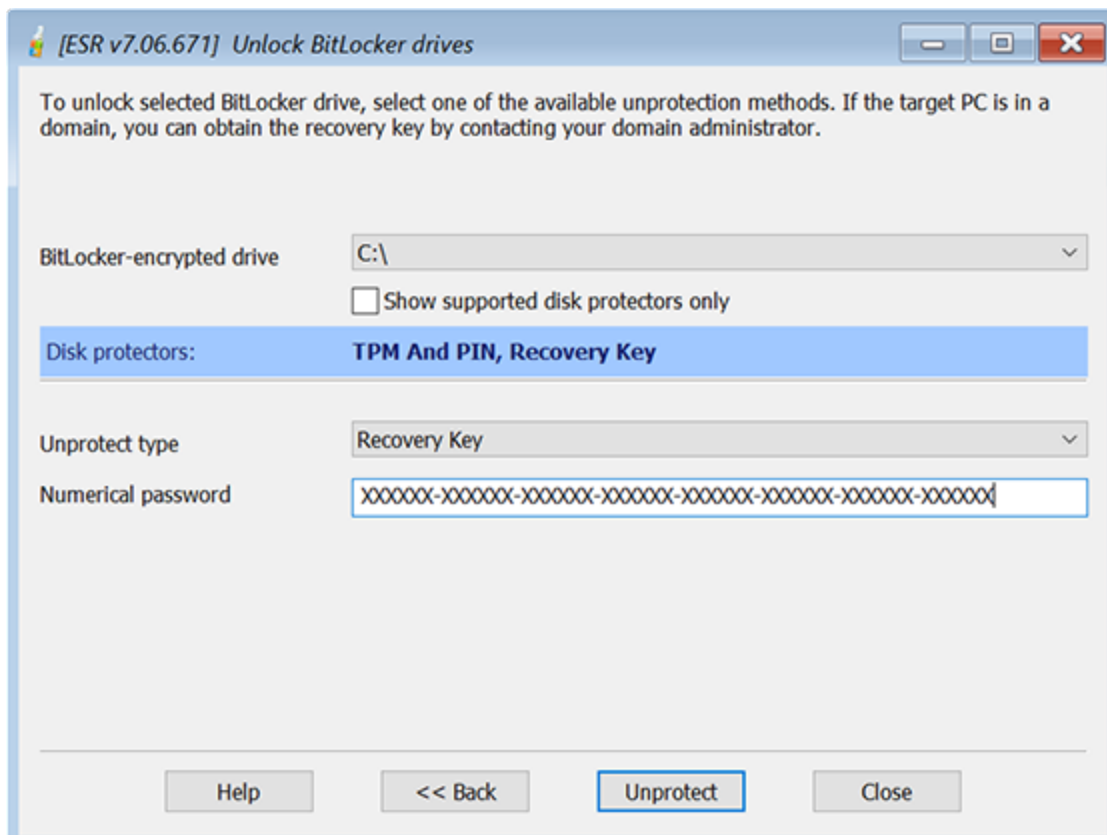
5.18.2.3.10 Unlock BitLocker drives

In order to be able to use a BitLocker-encrypted disk, you will need to unlock and attach it first. The program support for 3 general methods to unlock a BitLocker drive:

- Recovery Key. This method is used by default. Windows generates a 48-digit numeric recovery key every time a user initiates the BitLocker encryption.
- Password. A simple alphanumeric passphrase that is used to unlock BitLocker-encrypted disks in addition to Recovery Key.
- USB Key. A binary file, typically with *.bek extension, that is stored on an external drive (eg. USB).

If the target computer is a part of a domain organization, you can also obtain the Recovery Key by contacting your domain administrator.

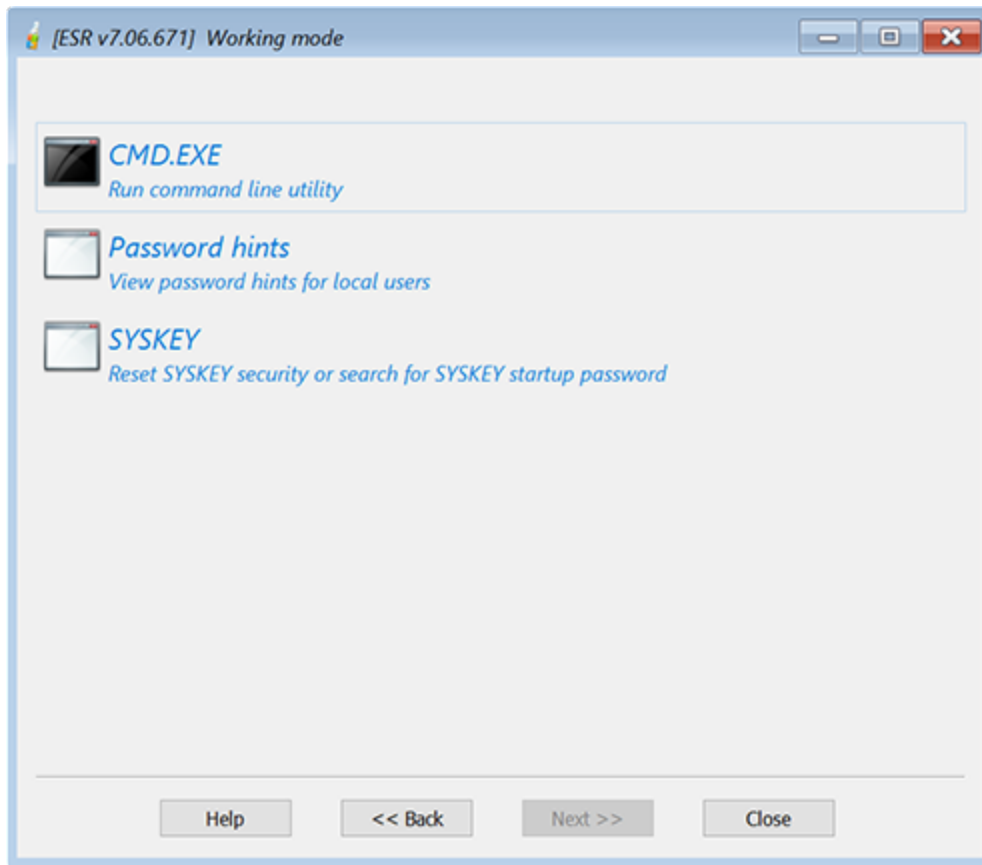
After the selected BitLocker disk is unlocked, the program decrypts and attaches the drive, so you can proceed with any common task for this disk: file copying, password resetting and searching, etc.



5.18.2.3.11 Miscellaneous

Some additional tools can be found here:

- CMD.EXE - command line utility. You can use it to perform additional operations like copying files or launching different built-in WinPE tools.
- Password hints - this feature displays found hints of local users. It is applied to local (SAM) accounts only.
- SYSKEY - it is aimed either to reset or to search for Syskey startup password.



5.19 Proactive Password Auditor

5.19.1 Introduction

Audit security policies, examine network security and recover account passwords with Proactive Password Auditor™ (PPA). Find out exactly how secure your network is by running a full-scale attack on account passwords. By recovering exposing insecure passwords, Proactive Password Auditor determines the security of your network.

Not all security policies are equally secure. A single password that is easy to break becomes the weak link in the chain that compromises security of the entire network. It is common for corporate users to use passwords too short or too simple. These passwords are easy to remember, but essentially insecure.

Proactive Password Auditor™ determines the security of your network by attempting to break into a network by recovering one of the passwords. If just one account is unlocked within certain time, this demonstrates vulnerability of the entire network. If the network withstands the attack for the period of time between password expirations, the password security policy is considered strong enough.

Recovering lost and forgotten passwords to user accounts is another purpose of Proactive Password Auditor™. By analyzing password hashes and recovering plain-text passwords,

Proactive Password Auditor™ makes it possible to access and log in to user accounts, exposing the EFS-encrypted files and folders. A wide range of available attacks from dictionary to brute force makes it possible to recover passwords over the network, while the Rainbow attack recovers up to 95% of passwords in a matter of just minutes. Fortunately, the Rainbow attack cannot be executed from the outside!

Proactive Password Auditor™ can analyze Registry binaries and extracted dump files, allowing for off-line password recovery. Proactive Password Auditor™ runs on Windows 2000, XP, Vista, 7, 8, Windows Server 2003/2008/2012.

5.19.2 Requirements

- Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows Server 2003/2008/2012 (32-bit or 64-bit)
- about 6 megabytes of free space on hard disk

Please note that some features (such as dumping password hashes from memory or registry) are available only with Administrator privileges. If you do not have them, or if Administrator's password is lost, forgotten or expired, or if Administrator's account is locked or disabled, it is suggested to use [Elcomsoft System Recovery](#), a bootable CD or USB flash drive that can reset or change passwords to any user local or Active Directory accounts (including Administrator's one), enable/unlock disabled/locked accounts, dump password hashes into the text file (for further audit/recovery with PPA) and more.

For dumping password hashes from memory, there are some additional requirements:

- 'RestrictAnonymous' value in the following Registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

should be set to 0 or 1; remote access to the registry by domain users also should NOT be restricted using the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

For more information about these keys, see Microsoft Knowledge Base articles [Q143474](#) and [Q246261](#).

- Both the local and remote computers should have File and print sharing (i.e., the Workstation and Server services) enabled.

- Remote system should have Admin\$ share (a hidden share that maps to the \windows directory), or other share with the same properties defined.

If remote machine (you dump password hashes from) is running Windows XP SP2+ or Windows Server 2003+, the Network access: Sharing and security model for local accounts security policy should be set Classic - local users authenticate as themselves there. It can be done using Group Policy Editor (gpedit.msc) under the following branch: Local Computer Policy | Computer Configuration | Windows Settings | Security Settings | Local Policies | Security Options.

If, for some reason, PPA fails to dump from the remote computer, please try to connect to ADMIN\$ resource manually in Windows Explorer: Tools | Map Network Drive (do not forget to disable the Reconnect at logon option and supply the same credentials as in PPA). If connection will be performed successfully, PPA should also work (do not forget to disconnect the network drive after this test); if not, you may also need to check the firewall settings on the remote computer. If manual connection to ADMIN\$ also fails, it means that ADMIN\$ share is not enabled, or security policy described above is set to Guest only - local users authenticate as Guest, or you are supplying the wrong credentials (password is wrong, or the given user does not have administrator privileges on the remote machine).

In the domain environment, it is recommended to start PPA under the domain administrator's account.

5.19.3 How to work with the program

5.19.3.1 About Windows passwords

In Windows operating system, every user has a password. The password is a security measure used to restrict logon names to user accounts and access to computer systems and resources. A password is a string of characters that must be provided before a logon name or an access is authorized. A password can be made up of letters, numbers, and symbols; passwords can also be blank. Microsoft recommends that you require the use of complex passwords to help ensure that passwords provide the best security possible. These complex passwords are much more resistant to attack than blank or simple passwords.

Instead of storing the user account password in clear-text, Windows generates and stores user account passwords by using two different password representations, generally known as "hashes." When you set or change the password for a user account to a password that contains fewer than 15 characters, Windows generates both a LAN Manager hash (LM hash) and a Windows NT hash (NTLM hash) of the password. These hashes are stored in the local Security Accounts Manager (SAM) database or in Active Directory.

The NTLM hash is actually an MD4 hash of the original password (in UNICODE), 16 bytes long. In theory, the password length is limited to 128 chars.

The LM hash is relatively weak compared to the NTLM hash, but it is needed for backward compatibility with Windows 9x clients, and used, typically, to authorize remote connection to a given machine. To generate the LM hash, the system converts the password from UNICODE to ANSI (one byte per character), and translates all characters into uppercase. After that, the password is divided to two chunks (7 chars each, padded with zeros if needed). Each part is used as a DES encryption key, to encrypt the pre-defined constant, and the results of encryption are stored in the system (merged into a single 16-byte value). So, if your system uses LM authentication (and so LM hashes are available), the real password length (complexity) is just 7 characters, and the 14-character password is not much stronger than one of 7 characters.

5.19.3.2 How the program works

Due to the nature of a hashing algorithm (see [About Windows passwords](#)), it is not possible to restore the original password from the hash (whether it is LM or NTLM). However, it is still possible to find the password using brute-force and dictionary attacks, by testing all possible passwords in a given range, or by trying the words from the wordlist, respectively. So, to get the passwords, we just need to:

- [find password hashes](#)
- [find passwords that have the same hashes as the original ones](#)

Because hashing is based on relatively strong algorithms (DES and MD4), finding the right password may take a long time. But because most users prefer passwords that they can easily remember, brute-force and dictionary attacks are often the most effective methods for a malicious user to find a password. So the strength of a password depends on how many characters are in the password, how well the password is protected from being revealed by the owner, and how difficult the password is to guess.

Currently, several [attack methods](#) are based on guessing weak passwords by using dictionary, brute force and rainbow attacks.

5.19.3.3 Obtaining password hashes

PPA supports a few different methods of obtaining password hashes for further attack/audit, as described below.

DUMP file

There are a few 3rd party tools that can generate dump files with password hashes, e.g. pwdump, pwdump2, pwdump3 and samdump. The files generated by these tools have the following format:

user_name:user_id:LM_hash: ntlm_hash:comment:user_home_directory:

The PPA program can open files of this type and read password hashes from them.

Registry of local computer

On all systems that don't use Active Directory, password hashes are stored in the system Registry, and the program can extract them from the Registry, even if they are encrypted using SYSKEY.

Registry files (SAM, SYSTEM)

The program can extract password hashes directly from Registry files: SAM and SYSTEM. You will have to select those two files (or just the SAM file, if the file comes from an old NT system that does not use SYSKEY protection: check the Don't use SYSKEY option in that case). If SYSKEY has been generated from a startup password or stored on a floppy disk, you will have to supply that password or floppy, respectively. Please note that with this feature, you cannot dump from SAM and SYSTEM files that are currently in use (located in WINDOWS\SYSTEM32\config folder), because they're locked by the operating system. You can, however, make copies of these files by booting an alternative operating system such as another Windows installation, or even DOS (though an NTFS driver might be required, such as [NTFS Reader for DOS](#) or [NTFSDOS](#)); another way is to attach the hard disk (where these files are located) as a secondary drive to another Windows workstation.

Memory of local computer

If you have administrator rights on the machine you run PPA on, you can dump password hashes from its memory. This method works regardless of the SYSKEY mode, and gives hashes for all users, including Active Directory users.

Memory of remote computer

This method is similar to the previous one, but allows you to dump hashes from any remote computer in your LAN – server or workstation, with or without Active Directory. Press the Browse button and select the computer(s) you want to get hashes from. Once password hashes are obtained, PPA shows the following information:

- User name
- Computer
- User ID
- Hash type (LM or LM+NTLM)
- LM hash
- NT hash
- Password

- Audit time
- Status (disabled or locked)
- Description

Right-click on any column header to enable/disable visualization for any of those fields in the program interface.

Please note that in order to obtain password hashes from any remote computer, PPA should have administrator privileges there. First, it tries to log on with current credentials (the ones the program was started with) first, then with the [stored credentials](#) (if there is an appropriate record there), and if it still fails, it prompts for user name and password. If the given computer is a domain controller, you should supply the domain administrator credentials (see [Requirements](#) section for more details).

When you dump or open password hashes using any of the methods described above, PPA runs (by default) a fast "preliminary" attack that takes just a few seconds (or a few minutes on slow machines), but recovers many short and simple passwords automatically. Look at [Preliminary attack options](#) for details.

Prior to the attack, when no passwords have been recovered yet, passwords are shown either as <empty> (if no password for the given account is set) or as <unknown>. After the preliminary attack mentioned above, some <unknown> passwords might be recovered and shown.

Now you have to select (check) the user accounts you want to audit, select the attack method and start the attack itself. You will not be able to check the following accounts, though:

- ones that have empty passwords
- ones that are above the limit of the trial version, or according to the license you have purchased (these accounts are also grayed out)

An appropriate message will be printed into the log window (and log file), respectively:

- Password of user "Guest" is empty, recovery for this user is disabled
- Recovery for this user is disabled (number of user 101)

5.19.3.4 Credentials

To simplify access to remote computers, PPA allows you to manage and save the credentials to as many computers as you are auditing. Select the Credentials item from the Options menu, and you will get a list of computers to manage (an empty list if you have just started). Press the Add button, browse for the computer you want to save credentials for, and press Select. On the next screen, you have to enter:

- Domain/computer. You have already selected it at the previous step, but you still can press Select to the right to select another one.
- Resource name. PPA will connect to the given resource to upload the special service (which will dump password hashes) there. Press Select to see the list of shared resources on selected computer (if allowed).
- User name. The name of the user who has Administrator privileges on the given computer. Press Select to get the list of local users, and if needed, the Domain users button on the next screen to select one of the domain user accounts for any selected domain controller.
- Password. The password of the user selected above.

Please note that if you enter a resource name and user name manually, PPA will verify them (as well as the password) only when auditing the given computer. If something goes wrong (resource is not accessible, user not found or password does not match), you will be prompted to correct any/all of these fields, and if the updated information is correct, it will be saved.

5.19.3.5 Password cracking

5.19.3.5.1 Password cracking methods

The program supports different methods of password recovery: Dictionary attack, Brute-force attack and [Rainbow attack](#) (see further chapters for details). Once you select the desired method, the second tab in the main window is modified, reflecting the options that are appropriate for the selected method.

Also, you have to select LM attack or NTLM attack, depending on the authentication method used, i.e., the types of password hashes available. Once the password hashes are obtained, the Hash type field shows either LM+NTLM (which means that both LM and NTLM hashes are present), or NTLM (if LM hash is not available); see [About Windows passwords](#) for explanation.

If most (or even some) users are listed with LM+NTLM hash type, it is recommended to start with the LM attack. Actually, both attacks run at about the same speed (i.e., PPA can try about the same number of passwords per second), but as already noted, an effective password length for LM hash is just 7 characters, and besides, LM passwords are in uppercase. So you can complete a full LM attack (for all 14-character passwords) in a very reasonable time – from a few minutes and up to a few days, depending on the selected character set and the speed of your CPU.

For all users with NTLM hash, however, you will still have to run the NTLM attack.

Please also note that you can perform the attack on as many users as you want (simultaneously). Because of the weak implementation of password hashing (Windows does not add random characters to the password before calculating its hash), it takes almost the

same time to try the same password for 2 users, or for 100 users, or even as many as 10,000 users. So for most effective attack, it is recommended to select all users that have the same hash type (LM or LM+NTLM). To select the user accounts for recovery, simply put the check marks at the left of desired user names; you can also use the context menu (on right mouse click) for easier selection, or hot keys: Ctrl+A to select all users, Ctrl-U to clear selection.

Once the passwords are recovered, the accounts with known/recovered (or empty) passwords are shown in a red color, and Audit time column shows the total time spent on that account/password.

5.19.3.5.2 Rainbow attack

Rainbow attack is an implementation of the [Faster Cryptanalytic Time-Memory Trade-Off](#) method developed by Dr Philippe Oechslin. The idea is to generate the password hash tables in advance (only once), and during the audit/recovery process, simply look up the hash in these pre-computed tables. Such process dramatically reduces the auditing time (especially for complex passwords). Due to the nature of this attack, not all passwords can be found (although with a probability which can be as high as needed).

To access Rainbow attack settings, switch the Attack type to Rainbow, and click on the Rainbow attack tab (second tab, next to the Hashes tab). If you already have the tables, click on the Rainbow tables list button, and you will be able to browse for the tables for further attack (you can add several tables at once), remove the tables from the list, and move them up and down; when completed, press Close, and proceed with the attack itself.

The program also supports indexed rainbow tables that are available at <http://www.freerainbowtables.com>.

To create your own tables, press the Generate tables button. There are a few settings there:

Hash type

LM and NTLM hash tables can be generated; see [About Windows passwords](#) for details on hash types.

Password length

Minimum and Maximum; typically, from 1 to 7 (to cover all password space for LM hashes). However, if you want to audit just 6-character passwords (and second halves of passwords that are from 8 to 15 characters long), you can create more effective and still relatively small tables for length from 1 to 6.

Charset

Available choices:

- alpha: capital letters only (26)
- alpha-space: capital letters plus space character (27)
- alpha-numeric: capital letters plus digits (36)
- alpha-numeric-space: capital letters plus digits and space character (37)
- alpha-numeric-symbol14: capital letters, digits, and 14 most-common symbols: !@#\$%^&*()-_+= (50)
- alpha-numeric-symbol14: capital letters, digits, space and 14 most-common symbols: !@#\$%^&*()-_+= (51)
- all: capital letters, digits and 32 printable symbols including space (69)

Chain length

Typical values are from 1000 to 10000. When this value is increased, you get better probability, but worse generation and cryptanalysis times.

Chain count

Chain count affects the table size (and so disk space), table size, probability and generation time (but not cryptanalysis time).

Number of tables and Indexes

Number of tables to generate, or indexes of tables if you distribute the table generation process across a few computers. More tables you have, the better success rate is achieved. For example, if one table gives a probability of 60% (0,6), two tables will give $1 - (1 - 0,6) * (1 - 0,6) = 0,84$ (84%). With three such tables, the probability is already $1 - (1 - 0,6) ^ 3 = 0,936$ (93,6%). But of course, the total space also increases dramatically.

Output folder

Press Browse to select the folder to save generated tables to (before starting the generation process, please verify that there is enough free space there).

Once all parameters are selected, PPA immediately calculates the key space (the total number of passwords in the given range; actually, it depends only on the character set and password length), disk space (size of each table multiplied by number of tables), and success probability. You can also run the benchmark: press Start, and PPA calculates the speed of your computer

on these operations, and so the table precomputation time, total precomputation time, and maximum cryptanalysis time.

There are some typical configurations (for LM hash type, length from 1 to 7; the time is calculated for Pentium 4 3.0GHz CPU) you can use, for example:

	#1	#2	#3	#4
Charset	alpha	alpha-numeric	alpha-num-sym14	all
Chain length	2,100	2,400	12,000	20,000
Chain count	8,000,000	40,000,000	40,000,000	100,000,000
Tables	5	7	13	20
Success rate	99.9%	99.9%	99.9%	99,3%
Total space	640 Mb	4,480 Mb	8,320 Mb	32,000 Mb
Max gen. time	17h	5d 14h	52d	332d
Max analysis time	7 s	14 s	11 m	48 m

The tables for first three configurations can fit into one CD, DVD (Single Layer) and DVD (Double Layer), respectively. For the last configuration (with a complete character set), they take about 32 gigabytes and need 369 days to generate (so you have to use multiple computers), but with such tables, any password can be recovered in just about an hour with 99,3% probability. Normally, it would take up to 3 weeks to recover such password using a brute-force attack.

5.19.3.5.3 Recovery process and results


When all of the options are selected, all you have to do is press the Start button on the toolbar, or select the Recovery | Start recovery menu item and wait. The program will show the following information during the attack:

- Current password – last checked password (not every one is shown, of course).
- NT passwords found – the number of NT passwords already found. The second number is the total number of users selected for the current attack.
- Passwords checked – the total number of passwords tried since the start of attack.
- Passwords total – the total number of passwords to try, according to the selected options, but for the current length (which is shown in brackets).

- Time elapsed – time elapsed since the attack was started.
- Time left – estimated time left, according to current speed.
- Speed (Cur/Avg) – indicates how many passwords per second the program tries (current, and averaged – since the start of attack).

Once the program finds any passwords for selected users, it immediately shows them in the main window. For LM attack, as already noted, the program will search for password halves independently, and so may find the first or second half only; when both halves have been found, the program recovers the full (NT) password and "unselects" the given user. All information about recovered passwords (and halves) is written (along with a timestamp) into the log window at the bottom, and into the log file (if appropriate option is selected).

Brute-force and dictionary attacks are multi-threaded to use the full power of SMP systems, dual-core CPUs, and processors with HyperThreading technology. By default, PPA runs as many threads as the number of processors (including 'virtual' ones) installed in the system. You can change the number of threads using the command-line parameter (see [Options](#)). If more than one thread is running, you can press Show details to see the status of all threads: current password, total number of passwords, passwords checked, and speed, as well as the total values for all threads together:

Threads	Current	Passwords total	Passwords checked	Speed
 localhost		8.353.082.582	160.439.400	7.063.000
● Thread 0	PPLJIF	4.176.541.291	75.585.343	3.793.000
● Thread 1	QUHEQTM	4.176.541.291	84.853.887	3.270.000

5.19.3.6 Reports

When the attack is running or once it is completed, you can view and save some reports that can be accessed via Reports... button or by selecting Project | Reports... menu item. The following reports are available:

Users passwords

This report is shown (and can be copied to Clipboard or saved) as CSV file (Comma-Separated Values), where every line includes user name, LM password (two halves merged together; if one half of LM password has not been found, it is shown as question marks) and NT password (if available). Such report can be imported into any program that supports CSV format (such as Microsoft Excel) for further analysis or charting.

Press Options button here to set up what particular fields you would like to include into this report: User name, User ID, Computer etc (see Memory of remote computer in [Obtaining password hashes](#) chapter for the full list of available fields).

Passwords by time (running total)

This is a graphical report that shown a number of password recovered (by time); it can be also copied to Clipboard or saved as .BMP file.

You can also save the report as an XML file. In Options, you can set what particular fields you want to print into the output file; you can also ask whether to save all accounts, or only those the passwords have been found for. For every account, PPA writes the following data:

- Password Strength: Weak (recovery is possible in less than one day), Strong (from one day to one week) or Very Strong (more than one week)
- Password Charset: Alpha, Numeric etc
- Password Audit Method: Preliminary attack, Bruteforce attack, Dictionary attack or Rainbow attack
- Password Length Distribution

5.19.3.7 Program options

To access and change program options, select the Options | General menu item, or press the Options button on the toolbar; press Set options password button to set the password required to view or change the options (if password is set, you will be prompted for it every time when accessing the Options).

Save setup every (minutes)

If you'd like PPA to save its state periodically, please check the appropriate option, and select the time (in minutes) between saves. If you do that, PPA will update a project file (with .hdt extension) just as if you use the Save project button, or the Project | Save menu item. Even if your computer stops responding (or if power fails), you'll be able to restore breaking the password from the last saved state. Instead of using the default settings (the name of the file and the folder it will be saved to), you can also select your own settings. If your project does not have a name yet, it will be saved as untitled.hdt. Enabling this option is strongly recommended.

Progress bar update interval (ms)

Allows you to set an interval (in milliseconds) between progress bar and status window updates; the default is 500 (a reasonable value). By selecting the higher value (3000, for example), you can get slightly better recovery speed.

Hide found passwords

If this option is enabled, the password (or half), when found, is not shown in the main program window and in the report (the actual characters are replaced with asterisks).

Log file

When logfile is enabled, the program saves all information displayed in the status window into the logfile (ppa.log).

Minimize to tray

If this option is enabled, the program window will disappear from the Windows desktop when you press the "minimize" button in the top-right corner of the window (or you select an appropriate item in the system menu). The small icon will be created in the "tray" area of the task bar (near the system clock). Just double-click on that icon to restore the window.

Priority

Normal or high. If you want to start PPA as a "background" process, which will work only when the CPU is in an idle state, you may select Normal. If you want to increase performance, select High, but be aware that this will decrease the performance of **all other** applications running on your computer.

Preliminary attack options

Contain the following items:

- User info attack: check for passwords that are equal to user names
- Windows info attack: recover cached passwords (for users HelpAssistant, VUSR_*, IIS_* etc), auto-logon password, and password saved in WinLogon process memory
- Password cache attack: check the passwords against the 'internal' dictionary/wordlist, created from the passwords that were found during previous sessions
- Simple dictionary attack: an attack using the small but effective built-in dictionary
- Simple brute-force attack: brute-force attack on passwords for up to three characters

The first three attacks are extremely fast, and the last one usually takes just a few seconds (up to a few minutes on slow machines with many accounts). But you can still disable any (or all) of them.

Language

Switches the language of program user interface (currently, only English, German and Russian languages are available).

Also, the program can be started with the command line parameters. Currently, the only two supported parameters are project name (.hdt file) and the number of threads (see [Recovery process and results](#)). To start PPA with the given number of threads, use the following command line:

```
ppa.exe -threads N
```

where N is the number of threads.

5.20 Proactive System Password Recovery

5.20.1 Introduction

Proactive System Password Recovery (or simply PSPR; former Advanced Windows Password Recovery) is a program to recover all types of Windows passwords: logon password (when user is logged on and has Admin privileges), screensaver password, .NET Passport password, RAS and dial-up passwords, passwords to shared resources, SYSKEY startup password, passwords stored in cached credentials, Wireless (WEP and WPA-PSK) encryption keys etc. The program also shows all users and groups (with their properties), allows to run any programs in other user's context, show password history hashes, read password hashes from SAM and SYSTEM files, read Protected Storage records, decrypt Windows scripts, reveal passwords hidden under the asterisks, enable disabled controls, and run brute-force and dictionary attacks on PWL files (Windows 9x). Finally, it shows product IDs and CD keys for Windows, Microsoft Office and other Microsoft software installed, and is able to emulate POP3/IMAP/SMTP/FTP servers to retrieve saved email/FTP passwords.

5.20.2 System requirements

- Windows 95 or above
- about 8 megabytes of free space on hard disk

Please note that some program features require Administrator privileges.

5.20.3 Working with PSPR

5.20.3.1 User interface

The program menu is located at the left of the main screen, just as in Microsoft Outlook, and it contains buttons for the Main menu, Advanced features, Revelation, Miscellaneous, Recover PWL, Options, Help and Exit. Click on a button to switch to the appropriate pages.

Most interface elements (such as buttons, rows in the "list view" windows, etc.) have pop-up "tooltips" which give more details about them: e.g., what action will be performed when the button is pressed. "List view" elements also have context-sensitive menus appearing on a right button click.

The program also supports keyboard hotkeys. Use CTRL- <digit> to select the high-level menu item, and ALT- <digit> to switch to the low-level item under it (in order).

Main menu (CTRL-1)

- [Logon password](#)
- [Cached passwords](#)¹
- [RAS entries](#)
- [Shared info](#)
- [Recovered hashes](#)²
- [Screensaver password](#)¹
- [Domain cached credentials](#)³

Advanced features (CTRL-2)

- [Groups and users](#)²
- [NT secrets](#)³
- [Run as](#)²
- [Windows CD key](#)
- [Net passwords](#)⁴

Revelation (CTRL-3)

- [Behind asterisks](#)
- [Control reviver](#)
- [Registry and AD](#)²
- [Password reset disk](#)⁴
- [Mail/FTP server emulator](#)

Misc (CTRL-4)

- [Protected storage](#)
- [Remote assistance](#)⁴
- [Script decoder](#)

- [Remote desktop](#)
- [Wireless network](#)⁵

Recover PWL (CTRL-5)

- [View PWL file](#)
- Bruteforce attack
- Dictionary attack

Options (CTRL-6)

- [General options](#)
- [PWL bruteforce options](#)
- [PWL dictionary options](#)
- [NT hash options](#)

Help (CTRL-7)

- Register the program
- Help
- About
- System information

¹ Available only on Windows 95, Windows 9 and Windows Me

² Available only on Windows NT and up

³ Available only on Windows 2000 and up

⁴ Available only on Windows XP and up

⁵ Available only on Windows XP SP1 and up, when Wireless Zero Configuration service is used

The program also supports a few command-line switches:

-h	Help (shows command line switches)
-c <archive file name> <file or mask>	Compress the given file(s) into CAB archive
-d	Delayed run (starts after 10 seconds)
-u <user name> [-p <password>]	Starts using the credentials of the given user
-v <PWL-file> [-u <user name> [-p <password>]]	Shows PWL file using given user name and password
-noipr	Disables the IPR* feature

*IPR stands for Intelligent Password Recovery, and unique feature of PSPR which works transparent to the user, but really helps to recover long and complex passwords, as well as improves the program performance. When it is enabled, the program collects all passwords from the system when it starts (not every time, but on the first run and then on a regular basis)

- of course, only those ones that can be recovered instantly or in a very short time (from [secrets](#), Internet Explorer and Outlook Express, Mozilla, some network clients, [network credentials](#) etc). Then, all those passwords are compiled into the special internal dictionary/wordlist (saved as passdef.ssd in the program folder), and used in further recovery tasks where the encryption is really strong and requires time-consuming brute-force or dictionary attacks. For example, there is a good chance that some user account (used to log on into the system) has the same password as one of Outlook Express credentials. However, logon passwords are relatively hard to break, while OE passwords are saved in the system; and with IPR, such logon password will be recovered instantly.

However, collecting/updating IPR data may take some time - usually a few minutes, but sometimes more. Also, the program may even 'hang' on that step (i.e. when it starts) on certain circumstances, i.e. on a heavy loaded systems with a lot of accounts. If you encounter such problem, simply terminate PSPR from the Task Manager and restart it with -noipr switch.

5.20.3.2 Main menu

5.20.3.2.1 Logon password

Windows 9x: shows computer name, user name and logon password (for currently logged user), and whether or not auto-logon feature is enabled. Logon password can be changed here. If your machine is configured to log on into Microsoft SQL server, SQL server password (if cached) is shown as well.

Other Windows systems: shows computer name, user name (for currently logged user), auto-logon option state, logon password (Windows NT/2000 only), and cached logon password. Password of current users can be changed here. You can also set auto-logon option (supplying appropriate login and password), but please note that when it is enabled, the password is stored in Windows Registry in plain form (not encrypted).

If [Store password using reversible encryption for all users in the domain](#) policy is set, PSPR also shows the user password saved in Active Directory database.

In addition, password hint (on Windows XP and up), Microsoft SQL server password and Windows 7 HomeGroup password are also shown here (if available).

5.20.3.2.2 Cached passwords

Cached passwords: shows passwords that are cached by the system. If no one is logged on, the program will prompt for a login. Passwords can be added, deleted, and edited here. If password caching is currently disabled, but passwords are still in the system, they will be shown anyway. Please note that if you add a password of type Windows Network Remote Administration, Windows does not always verify the resource name correctly, but PSPR can fix that if Check value of the new cache resource [option](#) is enabled. Please also note that it is not recommended to add cached passwords with user-defined type greater than 127 (some Windows applications may not work correctly if such passwords exist).

5.20.3.2.3 RAS entries

RAS entries: shows remote access entries (connection name, phone number, login name, and password). Can be edited, or new connection can be added. You can also see remote access passwords stored in Windows cache (sometimes these are shown even if the record has already been deleted) by pressing the Cached passwords button.

Also, you can decrypt RAS entries from an alien system: simply check the Manual decryption option, set path to SYSTEM and SECURITY Registry files, browse for phonebook file(s) (or check Use phonebook files of the local computer option), and press the Manual decryption button. The phonebook has .pbk extension and is located in the folder Application Data\Microsoft\Network\Connections\Pbk under All users, or in user's profile directory; typically, only rasphone.pbk (default phonebook) is there.

5.20.3.2.4 Shared info

Shared info: shows shared resources (for both shared level and user level), along with the passwords and/or access rights.

5.20.3.2.5 Recovered hashes

Windows NT/2000XP/2003/2008/Vista/W7 Security Accounts Management Database (SAM) stores hashed copies of user passwords; the hash is a one-way function version of the clear text password. PSPR shows passwords of users that can be recovered instantly (including empty ones), or in a very short time (according to [options](#)). For these users, it is also possible to change the password hashes (and thus the passwords), but that may cause lost access to personal certificates, network passwords, EFS-encrypted files and some other data, so don't use that feature if you don't understand what you're doing.

Password history can be also extracted/decrypted (if appropriate [option](#) is set).

Using that feature, you can also dump (and probably decrypt) password hashes not only from the local system, but also from external (binary) SAM, SYSTEM and SECURITY files, and/or replace or reset the passwords there. Simply check the Manual decryption box, browse for these files, and press the Manual decryption button.

Please note that usually the SAM database is encrypted with a locally stored system key, and PSPR automatically decrypts it, but the SYSKEY utility can be used to additionally secure it by moving the SAM database encryption key off the Windows-based computer. The SYSKEY utility can also be used to configure a start-up password that must be entered to decrypt the system key so that Windows can access the SAM database. If the local machine is configured this way, PSPR can try to recover this start-up password: click on Find SYSKEY startup password link to open a new window where you can set brute-force and dictionary attack options. The same window is opened if you dump password hashes from external SAM and SYSTEM files (in Manual mode), or if the start-up password is known, you can enter it there (or if SYSKEY is

stored on a floppy disk, provide PSPR with it in order to get password hashes decrypted for further attacks).

Password hashes of Active Directory users can be also shown (see [options](#)), and if passwords are stored using reversible encryption, plain-text passwords are recovered instantly regardless their complexity.

In Manual decryption mode (i.e., for password hashes loaded from Registry files taken from another computer), You can also use the SAM database editor feature to see the details of all user accounts (in read-only mode); select the user account you are interested in and press the SAM database editor link (if no account is selected, the first one from the list will be loaded). The following information is available:

- general information (user name, full name, comments, user ID)
- hashes (LM and NTLM, including 'history' ones)
- flags (a lot of)
- date/time of last logon, logoff, password change/set, account expiration, last bad password
- local and global groups
- profile
- logon hours
- misc information
- domain information
- domain properties
- domain password properties (incl. SAM session key and SYSKEY)

Windows logon passwords can be also audited/recovered in [Proactive Password Auditor](#) and [Elcomsoft Distributed Password Recovery](#).

5.20.3.2.6 Screensaver password

Shows the last active password to Windows screensaver (if it was ever set) regardless of the current state (enabled or disabled).

5.20.3.2.7 Domain cached credentials

Operating systems based on the Windows NT series can cache (store) user logon information on users that enter the domain. This feature is designed to bypass the authorization procedure after the server has been unavailable for one reason or another. Additional information is available at:

[Cached Logon Information](#)

[Microsoft Windows XP - Logging On Using Domain Credentials](#)

Along with the general information on a domain user, which includes the actual user information, domain information, and general information (the DCC common record structure will be covered below), DCC contains the user's password hash.

Though these caches are 'stronger' than ones stored in SAM, PSPR is able to recover plaintext passwords from them, too (using dictionary and brute-force attacks).

If you need faster recovery of DCC passwords, have a look at [Elcomsoft Distributed Password Recovery](#) project.

Note: this feature has not been tested on Windows Vista yet.

5.20.3.3 Advanced features

5.20.3.3.1 Groups and users

Shows the tree of users and groups; it can be sorted by users or by groups. The members of Administrators group are marked as green, disabled users as red, and current user with a bold font. Here is what you can do there:

- | add/remove users and groups
- | view available user/group information
- | view/change global system settings (about passwords, server or domain controller, SAM and security)

There are also some password-specific tasks, such as:

- | set new password (typically, for users that have been just added)
- | change password
- | change force to change on next logon password option
- | change password never expires option
- | change user cannot change password option
- | view/change password hashes (use with care)
- | reset password

5.20.3.3.2 NT secrets

Shows passwords cached by the system: RAS passwords, passwords of some users, SQL server passwords, etc. Can be local (for current user only) or global (for all users).

Also, the program can get the secrets from SYSTEM/SECURITY files taken from another system – simply check the Manual decryption option, browse for these files, (optionally) check the Show old secrets option if you'd like to see the secrets that are still stored but not being used anymore, and press Manual decryption.

All secrets (from local machine or external Registry files) can be edited, but use this feature with great care.

5.20.3.3.3 Run as

Allows you to run any program (including PSPR itself) with alternative credentials, or in the context of the SYSTEM account. User name, domain (if the computer is part of a domain) and password have to be supplied.

Note: this feature does not work on Windows Vista.

5.20.3.3.4 Windows CD key

Extracts some valuable information about the current Windows and Office installation, as stored in the system:

- User name
- Computer name
- Platform
- First install date (of operating system)
- Owner
- Organization
- Windows product ID and product (CD) key
- Microsoft Office product ID and product (CD) key
- Microsoft SQL Server product ID and product (CD) key
- IE product ID and product key

PSPR also contains a 'generic' algorithm to extract/decrypt IDs and CD keys to other Microsoft products and server software not listed above; press Retrieve unknown keys to proceed.

The Windows CD key can be changed there, but please use that feature with great care. For Windows XP and Windows Server 2003, you will have to re-activate Windows; if the option Force to activate Windows after the key is changed is enabled, then the activation wizard will be started automatically.

As for Office CD key, please note that PSPR supports only Office 97, Office XP, Office 2003 and Office 2007, but not Office 2000 (it seems that the CD key for this version is not stored in the system at all).

Please also note that if you would like to get the Windows/Office CD key from another machine (remote computer), you should have Administrator privileges there. Using the Manual decryption option, you can also retrieve the CD key from the SYSTEM file (part of Windows Registry) taken from any machine.

Note: for Windows Vista, CD key is saved in the system only till activation. So if Vista is already activated, PSPR is not able to show the key.

5.20.3.3.5 Net passwords

Shows stored user passwords for servers (allowing the user to transparently connect to servers using user names and passwords that are different from those used to log on). These passwords can be managed using the KeyRing; the keyring can be invoked from Control Panel | User Accounts | Advanced | Manage Passwords. .NET Passport passwords are also shown there.

By default, Net passwords are recovered automatically, but if something goes wrong (e.g., some files are located in the wrong folders), you can use Manual decryption. You must at least set the User profile directory and User logon password; if this is not enough, check the Expert options box and select User ID, Credentials, and Master key of the user you want to recover Net and Passport passwords for.

For all items listed here, the program shows additional information such as Server, User, Password, Type, Comment, Alias, Flags, and Last modified.

Here you can also decrypt Credential Backup Files (*.crd) created in Windows Vista and Windows Server Longhorn (for more information, see [Manage stored passwords](#)).

5.20.3.4 Revelation

5.20.3.4.1 Behind asterisks

In many Windows applications (and in the operating system itself), there are some input fields (typically used to enter passwords) that always show their contents as asterisks (*). So when/if your password is saved in the system but you cannot see it because of that feature, you can use PSPR to reveal it, automatically or manually.

The simplest mode is automatic: PSPR scans all visible windows on the desktop, finds the ones where 'asterisked' controls exist, extracts/reveals their contents and prints them into its own window, along with some technical information such as window title, handle, and class. If the Make asterisk field visible [option](#) is set, all such controls will be changed so they will show the actual strings instead of asterisks.

Please note that in this (automatic) mode some controls (used by system services, JAVA applications, those with non-standard Windows class, etc.) will still not be revealed. Edit controls on web pages (opened by Microsoft Internet Explorer), however, are supported.

There is also a manual mode, which may help if there are too many windows on the desktop, and/or if the control you want to reveal has non-standard class. Press the second button and don't release the mouse button; drag the cursor pointer (which will be changed, by the way) to

the field you're interested in, and drop it (release the mouse) there. When dragging, the 'active' window will be 'bordered'.

In manual mode, if you drop the pointer on a control that has Internet Explorer _ Server class, you can get the HTML source of that control. This works for all applications that use IE frames, such as Internet Explorer itself, Windows Explorer, Outlook and Outlook Express, Microsoft Help and many others.

If both automatic and manual modes still fail to do the job, you may need to add a proper class name in [options](#). It is also possible that this control has 'real' asterisks in it, simply indicating that the password is saved (e.g., as for Windows RAS).

Please note that there are some applications that try to detect such (revealing) 'attacks', when another program tries to get the string under the asterisks. For them, automatic mode should still work, but only if Make asterisks fields visible option is not set.

The other options are:

- Stay on top: if enabled, the PSPR window will be always topmost.
- Alternative scanning algorithm (for manual mode only): may help if you cannot locate the proper window to extract the text from – for example, if that control is disabled.
- Transparent window (Windows 2000/XP/2003 only): enable that option to make the PSPR window transparent, so you will be able to see what is behind it.

5.20.3.4.2 Control reviver

Control reviver works almost the same way as the [Behind asterisks](#) feature described above, but instead of revealing hidden passwords, it allows you to activate controls (such as buttons, menu items, check boxes etc.) that are disabled (grayed). You can either activate all disabled controls (that have standard system classes) currently visible using the Automatically revive... button, or use the second mouse button and drag the mouse pointer to the particular control you want to enable, and release the mouse; that control will be enabled.

5.20.3.4.3 Registry and AD

When the operating system is loaded, the key Registry files (SAM, SECURITY, SYSTEM and SOFTWARE) are 'locked': no application running under the operating system itself can access them. However, you may still wish to read from these files yourself, for some password recovery or auditing tasks. This feature of PSPR allows you to create copies of the files, and those copies will not be locked. You can save Registry from the local machine or from the Remote machine (you should have Administrator privileges on that machine, though).

Press the Save Registry button and select (from the popup menu) All Registry, or just the particular Registry branch.

The program also allows you to save Registry files in text format: ANSI (REGEDIT4) or UNICODE (REGEDIT5). Just note that this operation takes much more time than saving in the original (binary) format, especially for the SYSTEM file. Also, you can use the Compress output file(s) option to have the files compressed using Microsoft CAB format.

You can also save the Active Directory database (ntds.dit): select the AD server name, destination folder name (to save database to), Run backup under another security context option (if needed), as well as user name, domain and user password, and press the Backup AD database button. Note: this feature is not compatible with Windows Server Longhorn yet.

5.20.3.4.4 Password reset disk

In Microsoft Windows XP, you can create a special password reset disk:

[HOW TO: Create and Use a Password Reset Disk for a Computer That Is Not a Domain Member in Windows XP](#)

[HOW TO: Create and Use a Password Reset Disk for a Computer in a Domain in Windows XP](#)

If you forget your password, you can log on to the computer with a new password that you create by using the Password Reset Wizard and your password reset disk, as described above.

With PSPR, you can also recover the original password using that disk (the disk, actually, contains just the key used to encrypt the password, while the password itself is stored in the Windows Registry). Just select the Password reset disk path (typically, A:\), file name (userkey.psw by default), and password reset disk owner (from the list).

5.20.3.4.5 Mail/FTP server emulator

If you forgot your password to email account (POP3/SMTP/IMAP) or FTP connection but the password is saved in your mail/FTP client, PSPR is able to get it. Here are the steps to perform:

- Run your email or FTP client
- Open account/connection properties in the client
- Remember current server address (like mail.mydomain.com, pop3.mydomain.com, ftp.mydomain.com etc)
- In PSPR, select POP3, IMAP, SMTP or FTP emulation; the port number will be automatically updated in Server port field, but you may have to change it manually if it is different from the default
- In Server address field, put the proper server address (without prefix) as you got it from the client
- Press Start button
- Send/receive mail (in the client) for your account, or connect to the FTP
- Go back to PSPR and look at login/password there

This method works for regular authentication only, when the plaintext password is being transferred. In other cases (e.g. if CRAM-MD5, NTLM or another authentication is being used) the password is not passed to the server at all, and so it cannot be captured.

5.20.3.5 Misc features

5.20.3.5.1 Protected storage

Protected Storage provides applications with an interface to store user data that must be kept secure or free from modification.

Units of stored data are called Items. The structure and content of the stored data are opaque to the Protected Storage system. Items are uniquely identified by the combination of a Key, Type, Subtype, and Name. The Key is a constant that specifies whether the Item is global to this computer or associated only with this user. The Name is a string, generally chosen by the user. Type and Subtype are GUIDs, generally specified by the application. Additional information about Types and Subtypes is kept in the system registry and include attributes such as Display Name and UI hints. For Subtypes, the parent Type is fixed and included in the system registry as an attribute. The Type group Items is used for a common purpose: for example, Payment or Identification. The Subtype group Items share a common data format.

PSPR shows all information stored in Protected Storage, including (but not limited to):

- passwords to web sites accessed with Internet Explorer
- passwords to ftp sites accessed with Internet Explorer (stored as plaintext in Windows 2000, and encrypted on Windows XP and up; to decrypt, right-click on appropriate Item)
- Internet Explorer AutoComplete information
- passwords to IE items to synchronize
- newsgroup accounts/passwords in Outlook Express
- MSN passwords

It also allows you to edit and remove any items (including binary) in Protected storage, but please use that feature with great care (creating a backup copy of the Registry is strongly recommended).

By default, PSPR shows the Protected Storage that belongs to the current user; to see information available to All users in the system, uncheck the Protected storage of the current user option.

5.20.3.5.2 Remote assistance

Remote Assistance is a technology in Windows XP (and later versions) which enables Windows users to help each other over the Internet. With this tool, one user, called the "Expert," can view the desktop of another user, the "Novice." With the Novice's permission, the Expert can even share control of the Novice's computer to resolve issues remotely. For more information, see:

Overview of Remote Assistance in Windows XP

<http://support.microsoft.com/default.aspx?scid=kb;en-us;300546>

For all Remote Assistance "tickets" created on the local machine (even expired ones), PSPR shows:

- Owner
- Source
- Destination
- Expired

Unfortunately, passwords (if assigned) cannot be extracted instantly because strong encryption is used. However, you can run dictionary and bruteforce attacks to try to recover those passwords.

You may also need to select the proper Profiles folder (C:\Documents and Settings by default).

5.20.3.5.3 Script decoder

Windows Script is a comprehensive scripting infrastructure for the Microsoft Windows platform. Windows Script provides two script engines, Visual Basic Scripting Edition and Microsoft JScript, which can be embedded into Windows Applications. It also provides an extensive array of supporting technologies that makes it easier for script users to script Windows applications. For more information, see:

<http://msdn.microsoft.com/library/en-us/dnanchor/html/Scriptinga.asp>

Script Encoder is a simple command-line tool that enables script designers to encode their final script so that Web hosts and Web clients cannot view or modify their source. See:

<http://msdn.microsoft.com/library/en-us/script56/html/seusingscriptencoder.asp>

Using PSPR, encrypted scripts can be decrypted back to plain source code. The File list to decode window contains the names of the files to be decrypted. Initially, it is empty, but you can add files to it by pressing the Add file(s) to list button, or simply by searching the given disk or folder. Select Files to scan (mask: *.vb*;*.js*;*.htm* by default), Directory to scan and (optionally) Look in subfolders option, then press Start scan. When scanning is in progress, you can press Stop scan at any time.

Once the list contains one or more files, you can highlight the one you wish to decrypt, right-click and select Decode, or press the Decode all button at the bottom to decrypt all the files from the list. Files can be removed from the list by selecting the Remove from list popup menu item. Decrypted files are saved with another extension (set using Output file name option, *.DEC by default). Please also note the Replace existing file(s) option. If the scripts contain text

In that mode, the program may also find previous configurations (not used anymore), and/or ones that are not completed.

If WPA-PSK encryption is being used, the password is not saved in the system, and can be recovered only using dictionary attack (if Dictionary analysis option is enabled), though the speed of recovery is extremely low. You can also save WPA-PSK password hash into the text file (using Export button) to perform brute-force attack in other software such as [Elcomsoft Distributed Password Recovery](#).

Note: this feature has not been tested on Windows Vista yet.

5.20.3.6 Recover PWL

5.20.3.6.1 View PWL file

USERNAME.PWL (where USERNAME is your logon name) is a password list file (PWL) used in Windows 95, Windows 98 and Windows ME. It records passwords to resources on the network and uses them to reconnect to those resources so you don't have to type the password again. Whenever Windows prompts you for a password (except for your logon password, which secures the PWL file itself), the resource name and password are saved in your PWL file for future use. Windows stores passwords for shares on share-level security servers (including Windows for Workgroups machines), passwords for user-level security LAN Manager servers, and LAN Manager domain passwords (used if your logon is validated on a LAN Manager domain).

Because these passwords are sensitive information, the file is encrypted.

To recover the contents of a PWL file with PSPR, type the complete path to PWL file (or browse to this file using [...] button at the right, supply the appropriate login and password, and press View.

If you don't know the password for the PWL file you need to explore, you can try to recover it using brute-force or dictionary attacks.

5.20.3.7 Options

5.20.3.7.1 General options

Program interface language: the program has a multilingual interface, and you can change the language (if supported) on the fly, by selecting the language from the drop-down box and pressing Apply.

User interface options (gradient fill color, caption text color, background color, easily move window, background image): changes the program look and feel.

Custom classes for asterisks revealing: used for [Behind asterisks](#) feature, when the password field has non-standard class.

Print entire window instead of text: when you print passwords and other information recovered by the program, PSPR may print its window (as graphics) instead of text.

Check value of the new cache resource: for Windows 9x cached passwords only; if enabled, PSPR will check (for validity) the resources you are adding.

Modify only enabled screensaver password: if checked, the program will actually change the screensaver password only if the screensaver password protection option is active.

Make asterisks fields visible: used for [Behind asterisks](#) feature; if checked, the program will not only print the passwords into its own window, but also change the style of the controls so the text will become visible in its native application, too.

View html source as text: used for [Behind asterisks](#) feature; if checked, PSPR will show the HTML source code for controls you drop the cursor on.

View only recovered hashes (Windows NT/2000/XP/2003 only): to show only those hashes where the actual passwords have been recovered.

View only recovered secrets (Windows NT/2000/XP/2003 only): same as above, but for [NT secrets](#).

Don't truncate long secrets: if enabled, [NT secrets](#) are being shown as is regardless of the size (otherwise, truncated to fit into the window).

Turn audit off when the program is working: if you want to hide the fact that PSPR was working on the computer, turn this option on, so auditing will be temporarily disabled.

Use fast crypto API: if enabled, PSPR uses its own (fast) implementation of all crypto algorithms (RC4, MD4, MD5, SHA); applicable to all brute-force and dictionary attacks, except attacks on PWL files.

Program startup password: allows to set a password to protect the program itself.

IPR data update period: an interval to update passwords collected by Intelligent Password Recovery engine at (see [User interface](#) chapter for details on IPR feature).

5.20.3.7.2 Attacks options

PWL bruteforce options

Process priority: set idle/normal/high/realtime priority to brute-force attack process

Thread priority: fine-tune the priority of the brute-force attack thread

Refresh time: the interval (in milliseconds) between updates of program state (current password and recovery speed)

Save current position to log: when enabled, the program periodically saves the state of the attack to the disk

PWL dictionary options

Use custom uppercase conversion function: if this option is enabled, the program will translate the characters to uppercase according to strings set in LowCase/Uppercase string symbols above

Convert to ANSI: if you use the dictionary/wordlist that is in OEM codepage, enable this option

5.20.3.7.3 NT hash options

Check short passwords: performs the fast brute-force attack on user's password hashes, using the character set you supply (press >>> button to set the character set and maximum password length, and get a benchmark to estimate the time that attack will be completed in). You can also enable the Fast check method option if LM authentication is being used.

Dictionary analysis: enables a simple dictionary attack on password hashes, using the dictionary you have set the full path to. To set the advanced dictionary options, press >>> button; here you can set the path to dictionary (wordlist) file location, Dictionary file is in OEM format option (if the given dictionary is in OEM codepage) and several SmartDic (Smart Dictionary) settings:

- Case mutation
- Digit mutation
- Border mutation
- Freak mutation
- Abbreviation mutation
- Order mutation
- Vowels mutation
- Strip mutation
- Swap mutation
- Duplicate mutation
- Delimiter mutation
- Year mutation

All those options allow to generate additional combinations from every word from the dictionary (by changing the case, adding prefix or suffix, swap letters etc), and so seriously

increase the probability of finding the password, especially if it has been mistyped when entered. However, please note that if the dictionary is large, and/or the recovery speed is low, that will also increase the time to complete the attack, so you can use Maximize speed and Maximize efficiency for more convenience, Set all to defaults if you are not sure what options would be best (and change them later), or even Disable SmartDic completely.

The same dictionary options are available for all other features of PSPR where dictionary attack is applicable, except just the recovery of PWL passwords.

View only the recovered hashes: if enabled, PSPR will show only those user accounts (in the Recovered hashes page) for which it was able to recover the passwords (using simple attacks mentioned below), including those with empty passwords.

View password history hashes: if password history is enforced (ensuring that old passwords are not continually reused, see [Microsoft documentation](#)), then Windows saves the hashes of previous passwords, so PSPR can show (and analyze) them, too.

Look for passwords stored in Active Directory: when enabled, PSPR extracts password hashes not only from SAM database, but also from Active Directory database.

Don't analyze password hashes: force PSPR not to analyze password hashes using brute-force and/or dictionary attacks, just show them.

- . -

.NET 217

- A -

About PDF encryption 98
 About Windows passwords 198
 About Word and Excel encryption 63
 Access Database Password 88
 Access Owner Information 88
 Access User-Level Passwords 90
 Account disabled 186
 Account is locked out 186
 Accounts database source 180
 Acknowledgements 54
 activation 216
 Active Directory 180, 189, 218
 AD 180, 218
 Administrator account 186
 Advanced options 48, 106
 AOL password 129
 asterisks 217
 Attacks options 224
 Automatic passwords recovery 60
 Auto-save 47, 105

- B -

Benchmark 49, 107
 BIOS 175, 176
 boot 176
 Brute-force attack 224
 Brute-force range options 39, 101
 Buy 96

- C -

cached credentials 214
 CD key 216
 command line 52, 110, 210
 Command line interface 71
 Contacting us 75
 controls 218
 Creating Debug Log 96
 Creating the project 77

credentials 201, 217
 Cryptographic Service Provider 85
 CSP 85

- D -

Debug Log creation 96
 Decrypting files 155
 Decrypting the document 67
 Dictionary attack 224
 Dictionary options 40, 103
 Domain 201
 Domain controller 214
 Download the latest version 75
 drivers 176

- E -

EFS 143
 Elcomsoft System Recovery 173
 Encrypted PDF file 100
 Encrypting File System 143
 Error messages 114
 ESR 173
 Excel Add-In unlocking 93
 Excel Book Password 92
 Excel Document Passwords 92
 Excel Password to Modify 92
 Excel Shared Book Password 92
 Excel Sheet Passwords 92
 Exit 62

- F -

features 209
 Files with different passwords 51
 French versions of Word/Excel 87

- G -

General options 223
 Getting results 76
 groups 215
 Guaranteed WinZip attack 45

- H -

hard disk 209
hard drive 209
Help 62
hotmail password 129
How the program works 199

- I -

identity password 129
IE 124
IE password 124
Internet Explorer 124, 216, 220
Internet Explorer password 124
introduction 36, 54, 57, 58, 62, 71, 97, 115, 118, 120, 122, 133, 142, 157, 169, 173, 196, 209

- K -

Key search 104
Known bugs and limitations 51
Known plaintext attack (ARJ) 45

- L -

LAN manager 223
Language 180
Limitations 175
Limitations of Trial version 96
LM hash 199
local accounts 180

- M -

mail 129
mail password 129
Mail server emulator (auto mode) 60
Mail server emulator (manual mode) 61
Managing Password Cache Files 84
Manual passwords recovery 60
mass-storage 176
menu 210
Microsoft Office 216
Microsoft Outlook 123

Microsoft Passport Passwords 86
Microsoft Policy Regarding Missing or Invalid Passwords 71
Money 2002 Password to Open 86
Money Passwords 95
MS Passport stored Passwords 79
MSN 220

- N -

news 129
NNTP password 129
NT hash options 225
ntds.dit 183
NTFS 143
NTLM hash 199

- O -

Obtaining password hashes 199
Office XP Passwords 85
OneNote 86
Operating system 183
Options 61, 207
organization 216
Other options 47, 83, 105
Outlook E-Mail Account Passwords 94
Outlook E-Mail Accounts 77
Outlook Express 220
Outlook Personal Storage 94
Outlook PST 123
Outlook PST File Password 94
owner 216

- P -

Passport 217
password 186
Password Cache 83
Password cracking methods 202
Password expired 186
Password from keys 46
Password length 40, 102
Password mask 40, 102
Password never expires 186
Password reset disk 219
Password Storage Types (PST) 78

Password-encrypted file 38
Pocket Excel Password 93
PowerPoint Password to Modify 94
PowerPoint Passwords 94
Precompiled hashes 203
Preinstallation Environment 173
Preliminary Attack 81
Price list 96
privileges 209, 216
Proactive System Password Recovery 209
Product ID 216
Program options 68, 83, 155
Program status 49, 108
Project Passwords 95
Protected storage 220
PSPR 209
Purchase 96
PWDUMP 199
PWL file 223
PWL password 223

- Q -

Quicken 2001 and below 55

- R -

RAID 176
Rainbow attack 203
Recovering process 108
Recovery process and results 205
RegEdit 218
Registration 96
Registry 199, 218
Remote Assistance 220
Remote desktop 222
Reports 206
requirements 37, 55, 58, 59, 63, 97, 116, 119, 120, 123, 134, 157, 158, 170, 175, 197, 209
Resource name 201
run as 216

- S -

SAM 183, 199, 218
Save and Read setup 48, 107
Saving your project 77

Scan for encrypted files 152
Scan for encryption keys 148
SCSI 176
Search for email clients 60
Searching for encryption key 65
secrets 215
SECURITY 218
Selecting File 75
SerialATA 176
Several words before 64
shortcut 210
SOFTWARE 218
Start from password 39, 101
Supported File Types 73
Supported Passwords 73
SYSTEM 183, 199, 209, 218
System Requirements 72

- T -

Technical Support 75
The password is 50
Time-Memory Trade-Off 203
Type of attack 38, 81, 101

- U -

UFD 175
USB flash drive 175
user interface 59, 210
users 215

- V -

VBA 87
VBA Backdoor 79
Visual Basic for Applications 87

- W -

Weak Encryption 87
web mail 129
web mail password 129
webmail 129
webmail password 129
What to start from 51, 110
Where to get the latest version 75

Windows 95 223
Windows 98 223
Windows Live Mail password 129
Windows Mail password 129
Windows Me 223
Windows Millennium 223
Windows PE 173
Windows script 221
Wizard 147
Word Document Passwords 93
Word Document Protection Password 93
Word Password to Modify 93
Word/Excel 95 Passwords 87
Word/Excel 97/2000 encryption 85
Word/Excel 97/2000 Password to Open (strong) 85
Word/Excel Password to Open (weak) 87
Word/Excel/PowerPoint XP Password to Open 85
Working mode 180
Working with ACTPR 116
Working with AINPR 55
Working with ALPR 58
Working with ASQLPR 119
Working with AWOPR 120
Working with Password Cache 84

- X -

XLA unlock 93

- Y -

Yahoo password 129