ELCOMSOFT
PROACTIVE SOFTWARE

OPEN SESAME!

THE EASY WAY TO RESTORE ACCESS PASSWORDS TO FILES, APPLICATIONS AND DATABASES

CONTENTS

INFORMATION: THE KEY TO EFFECTIVE SOLUTIONS

These days we're always hearing about the "information age," "information technology," and how "information rules the world." We have come to feel that information is everything.

But what does that mean, and is information in itself so important? Not completely. We need information to make decisions – that's what is truly important. A proper decision lights the way to success in any situation. That's why having access to information is a competitive advantage in any business environment.

It's no surprise that a great deal of focus is put on protecting information. The software and hardware market today offers a number of solutions for restricting access to information and preventing information leaks: tools for controlling access and authentication, systems meant to prevent attacks, backup programs, antivirus applications, and more.

But the simplest and most accessible tool for any user is still password protection, which helps prevent unauthorized access to systems, documents and databases. We have all used a password to access our work system and to view databases, etc.

We know that man is the weakest link in the information chain – and problems with password protection are no exception. How many times have you forgotten one password or another. But that's completely understandable, given the number of passwords the average computer user is expected to memorize.

But if a password is lost for any reason, it means access to information is also lost.

ACCESS DENIED...

Data about sales and cash flows, client databases, accounting and management reports, analytical reports and forecasts – all of it is information that is necessary for running a business successfully for taking key strategic decisions about business development.

As a rule, most of this kind of information is not accessible without a password. This is a basic security policy for any company. But what happens when access to certain data is crucial, but the password is unknown? This kind of situation happens all the time.

First of all, you might have forgotten the password. It’s happened to all of us. You’re rational and you didn't write it down on the last page of your calendar – you knew you would remember it with a simple association. For example, your favorite food and the year you were born in. You won’t likely forget your year of birth, but your favorite food is another issue. After that vacation you took in Crete, you can think of nothing but Greek salads. But Greek salads are not getting you authorized in the system.

Sometimes it happens that a certain sales manager leaves the company without giving the password for viewing reports to anyone. There's no way to contact her yet, since she has decided to finally realize her life dream and go on a 90-day tour of Tibet. Counter parties are threatening to terminate your contract if you can't pay them immediately, but you don't have the data behind the deal and you don’t know the details. Sound like a familiar situation?

Employees are sometimes fired for participating in financial schemes or working with a competitor. In these cases, there is no sense in expecting that person to willingly share the password to his documents. But you need to get your hands on the data, urgently.

The problem is clear: in order go gain access to information and take on today's business tasks, you're going to need to be able to restore lost passwords. The good news? In most cases, it can be done.

HOW DO YOU SOLVE THIS PUZZLE?

ALL ABOUT PASSWORDS

Lost passwords have been a problem since the invention of password protection, and software developers have been addressing this problem for some time now. As a result, there are several software password recovery solutions on the market today.

However, let’s take a look at the methods these software programs use to solve the lost password problem. For starters, let's examine the different kinds of passwords that are used and what kind of additional information might be useful when searching for a password.

In general, a password can include the following symbols: 26 lowercase letters (a through z), 26 uppercase letters (A through Z), 10 digits (0 through 9), and 33 other symbols (!@#$%^, etc.) – that gives us a total of 95 symbols that can be used in any combination. In some cases, the other special symbols are excluded, which reduces the number of possible password variations. Passwords can also be different lengths, which can be a crucial factor when a password can only be identified via a scan and cannot be restored or deleted.

Furthermore, knowledge of human psychology can actually be a big help when searching for a password. Despite the many restrictions meant to reinforce password protection (a minimum password length and regular password changes) many users disregard the basic rules of security and once again demonstrate the “weakest link” dynamic mentioned above: the human factor.

Most passwords are comprised of words and symbols in a user’s native language or a language known to him. These worms are often somehow related to the user’s personal life: her year of birth, a pet’s name, a telephone number or bank card number, etc. A new password may be a minor modification of an old password. This is how most users deal with changing passwords, which is often required in a company's security policy. One more important note: people often keep a list of their passwords right on their desks or store them on their computers in a separate file – completely defeating the purpose of password protection.

As a result, just by knowing the basic password requirements (permitted symbols and required length) and knowing a little bit about the user could make it really easy to determine an unknown password. The technologies used by specialized password recovery software involve the application of this kind of information.

WE CAN FIX IT…

Today, the main methods used to search for passwords with software include: a simple scan, a mask scan, a dictionary attack, an encryption key scan (there may be less variations here than in a brute force scan) and the so-called rainbow attack. In some cases, other types of access restoration are applied to a file, such as the sol-called plaintext attack (based on known content). Let's take a look at each of these methods in more detail.

Brute Force

The brute force method is pretty simple: the program tries all of the possible symbol combinations in order to pinpoint the correct password. The search can be limited by some things, such as specifying the number of symbols in the password, defining the type of symbols allowed (letters, digits, other symbols) and even specifying the first symbol in the password.

How long can it take to restore a lost password using brute force? It all depends on the length of the password, the different symbols used, the computer's performance, and the kind of document that is protected by the password.

Of course it can happen that the password is identified quickly, and not all possible combinations will have to be tested. But you shouldn't count on it. Using a regular computer, it could literally take years. The brute force method is the most labor-intensive approach, which is why we recommend resorting to it only when there are no other alternatives.

Mask Scans

If you are the one who created the password, there's always a chance you can restore it using its mask by significantly narrowing the search parameters. You may remember how long the password is or specific symbols used in the password. Any information is helpful.

For example, let's say you know that you used only numbers and lowercase letters. This means you can exclude other special symbols and uppercase letters from the search. It is also helpful if you know which position any symbols took in the password. For example, if you know that there are 10 symbols in the password and that the first symbol is the letter "a" and that the last four symbols are 2007, you can enter "a?????2007" as the search template. The unknown symbols are indicated with a question mark.

Using a mask means that the software will have to try fewer possible combinations, which clearly means that the time it will take to find the right password will be reduced.

Unfortunately, it is a rare case when these kinds of details are known about a password, which is why users are often unable to use mask scans. On the other hand, there is another method used to restore passwords that produces very good results.

Dictionary Attacks

Let's assume that you have some information about the possible words or names that might be used in a password. In this case, you can use a dictionary search.

The fact of the matter is that users often use common words in their passwords. As a rule, these words include: "open," "access," "password," etc., especially because it seems so much easier to remember this kind of password as opposed to a random combination of letters and numbers. The truth is that it is equally easy to forget this kind of password; however, this kind of password is relatively easy to restore.

But where does one get this kind of dictionary (or to be more precise, the list of words)? It might be included in a software program. The next place to look would be a network – FTP servers often host a variety of lists of commonly used words and their modifications, lists of words by topics (animals, football teams, etc.), abbreviations, and others. Another possibility is that a user may have compiled his/her own list.

The advantages of these methods are obvious. A list of words that the user enters as a password is very limited and usually does not exceed 100,000. Modern computers have no problem at all processing 100,000 variations. This method should be attempted before the others – and it might just work.

Rainbow Attacks

As we will see, the most crucial factor in restoring a password is how long it takes. We have already established that using a simple brute force scan will verify every single possible variation, which can be just too time-consuming for complex combinations. If it is going to take months or years to come up with the password, then this method isn't even an option for most.

That's exactly why the rainbow attack was invented. This method is based on using precalculations to search for a password. This isn't the first time someone got the idea to replace CPU-hungry calculations with a typical search with a precomputed and pre-made lookup table. A lookup table is applied in cases where data is much easier to extract from memory than it is to create.

Rainbow attacks use the results of precomputed potential password variations for a particular sequence of symbols. Over the time it takes to break one password using brute force, we can obtain tables that make it thousands of times faster to find any password from the tested range with a very high level of probability.

The size of rainbow tables is considerably smaller than that of a typical lookup table – down from terabytes to gigabytes. The reduced size of the tables is achieved due to their optimization. For the sake of fairness, it should be said that the time required to restore a password using this method is increased, while the probability of password identification is reduced – but the results are worth it. For example, when using a table for seven alphanumeric symbols (it will take about a week to create the table), a rainbow attack can help restore just about any password made up of seven alphanumeric symbols in just 20-30 seconds. Directly entering the different combinations would take more than 24 hours. The advantage is obvious.

Since compiling these tables drives up the prices for these programs considerably, rainbow attacks are applied primarily in corporate solutions. It's also important to keep in mind that the probability of restoring a password using a rainbow attack is lower than using other, more common methods. But that is the price of speed.

MAKING THE RIGHT CHOICE

There's no question that it makes sense to purchase software for quick password recovery – every system administrator should have this kind of tool in his arsenal. The cost of the software is recouped – with interest – the very first time the software is used.

What should you look for when you're in the market for a password recovery solution?

First of all, what is the manufacturer's stated password recovery probability? This is one of the key criteria for determining a solution's effectiveness – after all, that's what you're buying it for. The chances for success depend on the kind of document that is password protected and on the computer's performance. Furthermore, users are becoming increasingly more cautious and are creating better passwords. A probability rate of approximately 80% is what you should expect to see. However, for some kinds of passwords and documents, a software developer may guarantee 99% probability.

Next, make sure you review the product's supported operating systems, application versions, file formats, language support and coding support. It is difficult to predict what version of Microsoft Word or Adobe Acrobat will present you with a password recovery conundrum, not to mention character set (take, for example, Chinese characters or Arabic script). Also find out how quickly support for new versions of applications will be provided. If a software solution does not offer support for Office 2007, it may turn out to be useless. There's no time to wait.

Another thing to look for is the speed of password recovery. Of course, the speed may vary depending on the performance of your computer, but generally manufacturers provide average data. It's important to know what to expect: minutes, days, weeks or months?

Last but not least, does the software allow you to organize Distributed password recovery? This method involves labor-intensive calculation tasks and the utilization of the power of an entire group of computers, both on a local network and remote machines. It is also used in password recovery. While access to some documents and applications can be recovered quickly on a typical computer (such as a password to ICQ or GoogleTalk that is stored locally), the resources of one computer alone will be insufficient to recover other passwords – no matter how long it could take. For example, PGP passwords are so well constructed that they can only be recovered by using Distributed password recovery.

These are the main criteria for selecting a password recovery software solution.

ELCOMSOFT TO THE RESCUE

ElcomSoft, a worldwide leader in password/system recovery, offers clients a full range of solutions for just about any system, from office applications and instant messengers to system passwords for Windows and archives.

One-of-a-kind technologies and team of experts, who have accumulated years of experience in cryptography are what make it possible for ElcomSoft to create high-end password recovery software products. Depending on password length, complexity and encryption technology used in applications, recovery probability never falls below 80%. In most cases 100% recovery is guaranteed.

The selection of products has something to meet the needs of any client, from home users who may need to recover a forgotten ICQ password to major corporate clients who may need to recover system passwords for Windows, restore access to encrypted Microsoft Office documents or remove restrictions from Adobe Acrobat files. Bringing together all of these separate functions in one provides users with access to several products at once, all at a reasonable price.

In order to recover passwords for a large number of documents, including long and complex passwords, in a reasonable amount of time, the distributed calculation function has also been included both for local and remote resources.

Now let’s take a look at ElcomSoft’s main products in order to get an idea about what they can do and the problems they can solve.

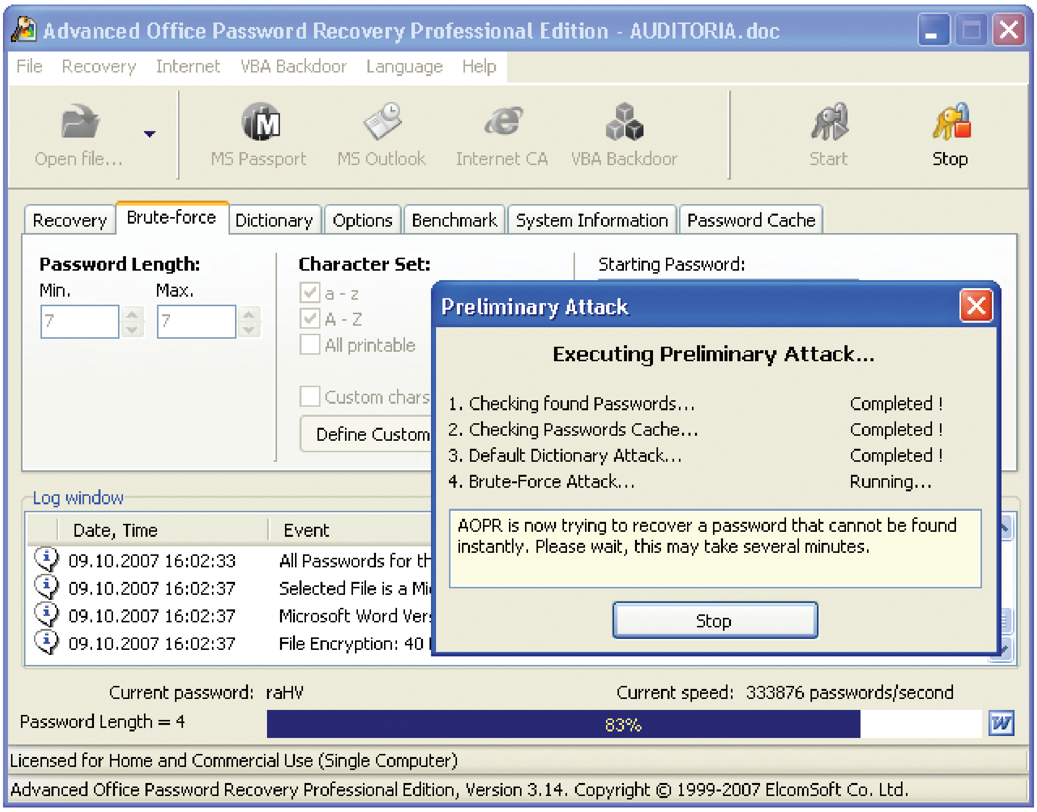
MICROSOFT OFFICE DOCUMENTS

Advanced Office Password Recovery

The majority of passwords are retrieved using instant, direct decoding. It doesn't matter which version of Microsoft Office is being used – Advanced Office Password Recovery can help recover passwords for documents created in any of the versions existing today: Office 95, Office 97, Office 2000, Office XP, Office 2003 Beta, Office 2003, and Office 2007. Moreover, you can find passwords for Microsoft Money, Microsoft Visio, Microsoft Backup and passwords for Internet Explorer Content Advisor.

This software solution is available in three different packages: Home, Standard and Professional. These packages differ based on the software programs they support. The Professional package is meant for major organizations and is capable of retrieving over 30 different kinds of passwords for 14 different applications.

Learn more about Advanced Office Password Recovery and try a demo version at ElcomSoft's website.



Password Length:
Min. 7 Max. 7

Character Set:
☑ a - z
☑ A - Z
□ All printable
□ Custom chars

Starting Password:

Preliminary Attack

Executing Preliminary Attack...

1. Checking found Passwords... Completed !
2. Checking Passwords Cache... Completed !
3. Default Dictionary Attack... Completed !
4. Brute-Force Attack... Running...

AOPR is now trying to recover a password that cannot be found instantly. Please wait, this may take several minutes.

Log window

```
Date, Time            Event
09.10.2007 16:02:33   All Passwords for th
09.10.2007 16:02:37   Selected File is a Mi
09.10.2007 16:02:37   Microsoft Word Vers
09.10.2007 16:02:37   File Encryption: 40 I
```

Current password: raHV
Current speed: 333876 passwords/second
Password Length = 4
83%

Licensed for Home and Commercial Use (Single Computer)
Advanced Office Password Recovery Professional Edition, Version 3.14. Copyright © 1999-2007 ElcomSoft Co. Ltd.

Figure 1. A preliminary attack to retrieve a password needed to open a Microsoft Word 2003 document.

Advanced Office Password Breaker

If you deal with password retrieval for text documents and tables only, you may be interested in Advanced Office Password Breaker, which can be used to decrypt password protected documents created in Word 97/2000 and Excel 97/2000.

Since Microsoft Office 97/2003 uses a 40-bit encryption key, the software guarantees that the document will be decrypted, regardless of the length or the complexity of the password. On an average computer, the time required to recover a password takes roughly two weeks.

Click here to download a demo version of Advanced Office Password Breaker.

Users who need to decrypt Microsoft Office XP documents encrypted with cryptoproviders will need Advanced Office Password Recovery, since only a password scan can be used with these kinds of documents.

EMAIL & INSTANT MESSAGING CLIENTS

Advanced Mailbox Password Recovery

Another common password recovery situation is the loss of access to email. There's an easy, quick solution to this problem: ElcomSoft's Advanced Mailbox Password Recovery. This product can help retrieve locally-stored email account passwords.

The list of supported email clients is exhaustive: Microsoft Internet Mail And News, Eudora, The-Bat!, Netscape Navigator/Communicator Mail, Pegasus mail, Calypso mail, FoxMail, Phoenix Mail, IncrediMail, @nyMail, QuickMail Pro, MailThem, Opera mail, Kaufman Mail Warrior, and Becky! Internet Mail. In addition, this product includes a POP3/IMPA server emulator, which helps recover passwords for any email client.

Click here to download a demo version of Advanced Mailbox Password Recovery.

Advanced Instant Messengers Password Recovery

People are always forgetting their IM passwords, and since this means of communication is first and foremost of a personal nature, the concerns about confidentiality are heightened. No one can hold anyone responsible but themselves for forgetting a password. Most users don't want to lose their easy-to-remember IM numbers or IM histories.

That's why ElcomSoft created Advanced Instant Messengers Password Recovery, a product that helps recover forgotten usernames and passwords for over 30 different instant messengers, including ICQ, Miranda, GoogleTalk, Trillian, Windows Messenger, AOL Instant Messenger.

All passwords are retrieved using instant, direct decoding (which requires that the password be stored locally). A forgotten password may be comprised of Latin letters, or of characters from the alphabets of other languages. The software's demo version has some restrictions, but will show you what the full version is capable of.

ADOBE ACROBAT & INTUIT QUICKEN DOCUMENTS

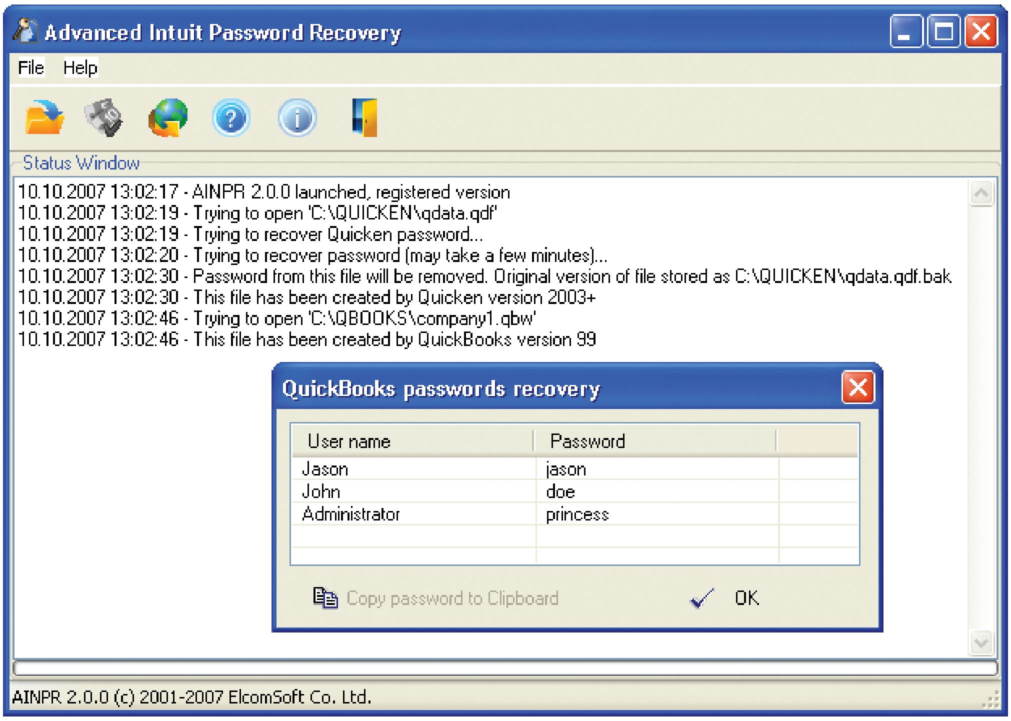
Advanced Intuit Password Recovery

Quicken software was designed by Intuit to process and store data about financial operations. Quicken applications are used by banks, auditors and accounting companies and are useful for calculating taxes and managing personal finances. We can all imagine what a disaster it would be to lose a password to this kind of data.

Advanced Intuit Password Recovery was designed to recover passwords to documents created in Intuit Quicken applications, versions 4 through 2008, as well as Quicken Lawyer (Portfolios, *.PFL) and QuickBooks (*.QBW, *.QBA) versions 3 through 2007 (see figure 2).

For documents created in the 2003 and later versions, Intuit applies enhanced encryption algorithms. Unlike similar products that only use brute force, Advanced Intuit Password Recovery also features instant document decryption.

Click here to download the demo version.



```
10.10.2007 13:02:17 - AINPR 2.0.0 launched, registered version
10.10.2007 13:02:19 - Trying to open 'C:\QUICKEN\qdata.qdf'
10.10.2007 13:02:19 - Trying to recover Quicken password...
10.10.2007 13:02:20 - Trying to recover password (may take a few minutes)...
10.10.2007 13:02:30 - Password from this file will be removed. Original version of file stored as C:\QUICKEN\qdata.qdf.bak
10.10.2007 13:02:30 - This file has been created by Quicken version 2003+
10.10.2007 13:02:46 - Trying to open 'C:\QBOOKS\company1.qbw'
10.10.2007 13:02:46 - This file has been created by QuickBooks version 99
```

User name	Password
Jason	jason
John	doe
Administrator	princess

Copy password to Clipboard
OK
AINPR 2.0.0 (c) 2001-2007 ElcomSoft Co. Ltd.

Figure 2. The results of a search of QuickBooks user passwords.

Advanced PDF Password Recovery

PDF documents are so common that it's probably nearly impossible to find someone who has never worked with Adobe Acrobat documents. Probably just as many people have faced the frustrations of not being able to edit or print PDF documents. Sometimes you need a password just to view the document.

ElcomSoft has developed a special solution to this problem: Advanced PDF Password Recovery. This application supports all Adobe Acrobat versions and all encryption algorithms from 3.x through 8.x and allows users to open files and remove the restrictions applied in the PDF format. Restrictions are removed instantly, regardless of the complexity of the password. In order to retrieve a password to open and view a file, Advanced PDF Password Recovery uses direct brute force scans, dictionary attacks and encryption key searches.

This product is available in three versions: Standard, Professional and Enterprise. The basic editing program makes it easy to remove editing and printing restrictions from PDF documents. The Professional version also features password retrieval for opening and viewing files, while the Enterprise package can be used to find an encryption key using fast-acting rainbow attacks with the help of a DVD disc containing precomputed tables.

Click here to try out a demo version.

ARCHIVES

ElcomSoft provides a number of different solutions for recovering archive passwords: Advanced ZIP Password Recovery, Advanced ARJ Password Recovery, Advanced ACE Password Recovery and Advanced RAR Password Recovery. All of these products are available in the Advanced Archive Password Recovery suite, which can retrieve passwords to all common types of archives:ZIP (PKZIP, WinZIP), ARJ/WinARJ, RAR/WinRAR and ACE/WinACE.

This is the most powerful of all archive password recovery solutions available today. The advantages of the ElcomSoft products include guaranteed recovery of the contents of most password-protected WinZIP archives, regardless of the password's complexity and the fastest brute force scan in the world for ZIP, ARJ and RAR archives (approximately 15 million passwords per second on modern processors). Other features include decryption of WinZIP archives with advanced encryption standards (AES), and known plaintext attack for ZIP and ARJ archives. If the content of at least one of the files in a ZIP archive is known, the password can be retrieved in just a matter of hours, no matter how complex or long the password is.

Click here to try out a demo version.

OTHER OFFICE APPLICATIONS

ElcomSoft's product line includes password retrieval software for other office applications as well.

For example, Advanced Lotus Password Recovery can help recover access to files and documents created in the following IBM Lotus applications: Organizer, WordPro, 1-2-3, Approach and Freelance Graphics. All versions of IBM Lotus applications are supported. Furthermore, the software restores access to FTP and proxy sites. All passwords are found through instant brute force decoding, regardless of the language. Download a 30-day demo version here.

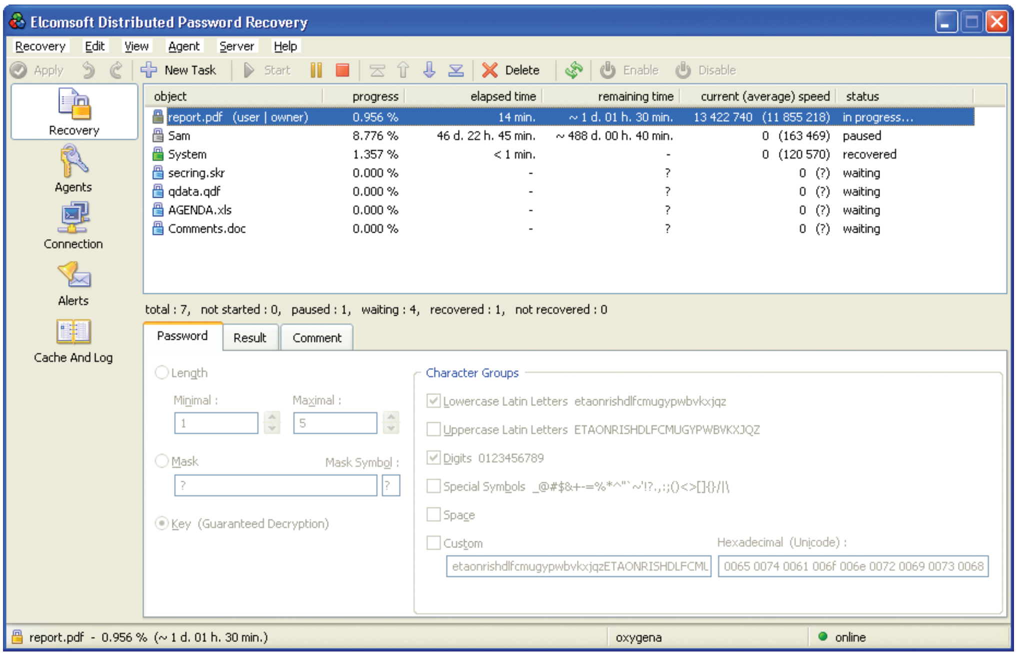
If you work with Corel WordPerfect Office, you should consider using Advanced WordPerfect Office Password Recovery. This solution retrieves lost passwords to Corel WordPerfect Office documents with the following extensions: *.wp, *.wpd, *.qpw, *.wb?, *.wq?, and *.db. All application versions are supported, and all passwords are retrieved in a matter of minutes thanks to direct decoding, regardless of the language. Download a 30-day demo version here.

DISTRIBUTED PASSWORD RECOVERY

We have already mentioned distributed calculations in recovering complex passwords. ElcomSoft's Distributed Password Recovery helps make the most out of any Internet-ready computer's performance, both locally and globally.

This product can be used to retrieve passwords to just about any document created with Microsoft Office, Microsoft Money, Microsoft OneNote, Adobe Acrobat, Intuit Quicken, Lotus Notes, and user passwords for Windows 2000/XP/2003/Visa, PGP private keys (*.skr), PGP Disk (*.pgd) and more.

This software is made up of three components: a server, agent and console. The server (see figure 3) is installed on one of the computers on the network and manages the password recovery process. The agent can be installed on any computer in the network – it tests some of the passwords generated by the server. The console can be launched on any computer and is used to manage the server and the recovery process or add new tasks and review statistics. Demo versions are available for the server and agent components.



object	progress	elapsed time	remaining time	current (average) speed	status
report.pdf (user | owner)	0.956 %	14 min.	~ 1 d. 01 h. 30 min.	13 422 740 (11 855 218)	in progress…
Sam	8.776 %	46 d. 22 h. 45 min.	~ 488 d. 00 h. 40 min.	0 (163 469)	paused
System	1.357 %	< 1 min.	-	0 (120 570)	recovered
secring.skr	0.000 %	-	?	0 (?)	waiting
qdata.qdf	0.000 %	-	?	0 (?)	waiting
AGENDA.xls	0.000 %	-	?	0 (?)	waiting
Comments.doc	0.000 %	-	?	0 (?)	waiting

total : 7, not started : 0, paused : 1, waiting : 4, recovered : 1, not recovered : 0

○ Length
Minimal : 1 Maximal : 5
○ Mask Mask Symbol : ?
?
● Key (Guaranteed Decryption)

Character Groups
☑ Lowercase Latin Letters etaonrishdlfcmugypwbvkxjqz
☐ Uppercase Latin Letters ETAONRISHDLFCMUGYPWBVKXJQZ
☑ Digits 0123456789
☐ Special Symbols _@#$&+-=%*^"`~'!?.,:;()<>[]{}/|\
☐ Space
☐ Custom
etaonrishdlfcmugypwbvkxjqzETAONRISHDLFCML
Hexadecimal (Unicode) : 0065 0074 0061 006f 006e 0072 0069 0073 0068

report.pdf - 0.956 % (~ 1 d. 01 h. 30 min.) oxygena online

Figure 3. The main window in Elcomsoft Distributed Password Recovery (a server component).

ABOUT ELCOMSOFT

Founded in 1990 in Moscow, Russia, ElcomSoft is a leader in the password/system recovery and forensics market. Thanks to one-of-a-kind technologies, ElcomSoft's products have garnered wide recognition both in Russia and abroad.

ElcomSoft's clients include many well known international companies from the following sectors:

High Tech: Microsoft, Adobe, IBM, Cisco
Governmental: FBI, CIA, US Army, US Navy, Department of Defence
Consulting: Andersen Consulting, Deloitte & Touche, Ernst and Young, KPMG, PricewaterhouseCoopers
Finance: Bank of America, Citibank, Equifax, HSBC, Wells Fargo, J.P.Morgan, Credit Suisse
Telecommunications: France Telecom, BT, AT&T
Insurance: Allianz, Mitsui Sumitomo
Retail: Wal-Mart, Best Buy, Woolworth
Media&Entertainment: Sony Entertainment
Manufacturing: Volkswagen, Siemens, Boeing
Energy: Lukoil, Statoil
Pharmaceuticals: Johnson&Johnson, Pfizer, GlaxoSmithKline, Novartis

ElcomSoft is a Microsoft Gold Certified Partner, Intel Software Partner, as well as a member of the Russian Cryptology Association, the Computer Security Institute (CSI), and the Association of Shareware Professionals (ASP).

ElcomSoft is an acknowledged expert in the password/system recovery and forensics market. The company's technological achievements and opinion leadership is quoted in many authoritative publications. For example: “Microsoft Encyclopedia of Security”, “The art of deception” (Kevin Mitnick), “IT Auditing: Using Controls to Protect Information Assets” (Chris Davis), “Hacking exposed” (Stuart McClure).

Visit our website to find out more.

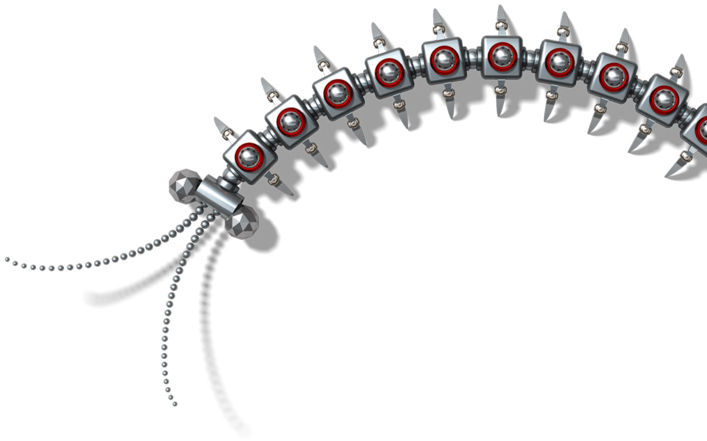
ADDRESS:
Elcomsoft
Zvezdny bulvar 21, office 541
129085 Moscow, Russian Federation

FAX:
US (toll-free): +1 (866) 448-2703
United Kingdom: +44 (870) 831-2983
Germany: +49 18054820050734

WEBSITES:
http://www.elcomsoft.ru
http://www.elcomsoft.com
http://www.elcomsoft.de
http://www.elcomsoft.jp
http://www.elcomsoft.fr

intel Software Partner

Microsoft GOLD CERTIFIED Partner



This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Intel and Intel logo are registered trademarks of Intel Corporation. Elcomsoft and Elcomsoft logo are trademarks or registered trademarks of ElcomSoft Co.Ltd. Other names may be trademarks of their respective owners.