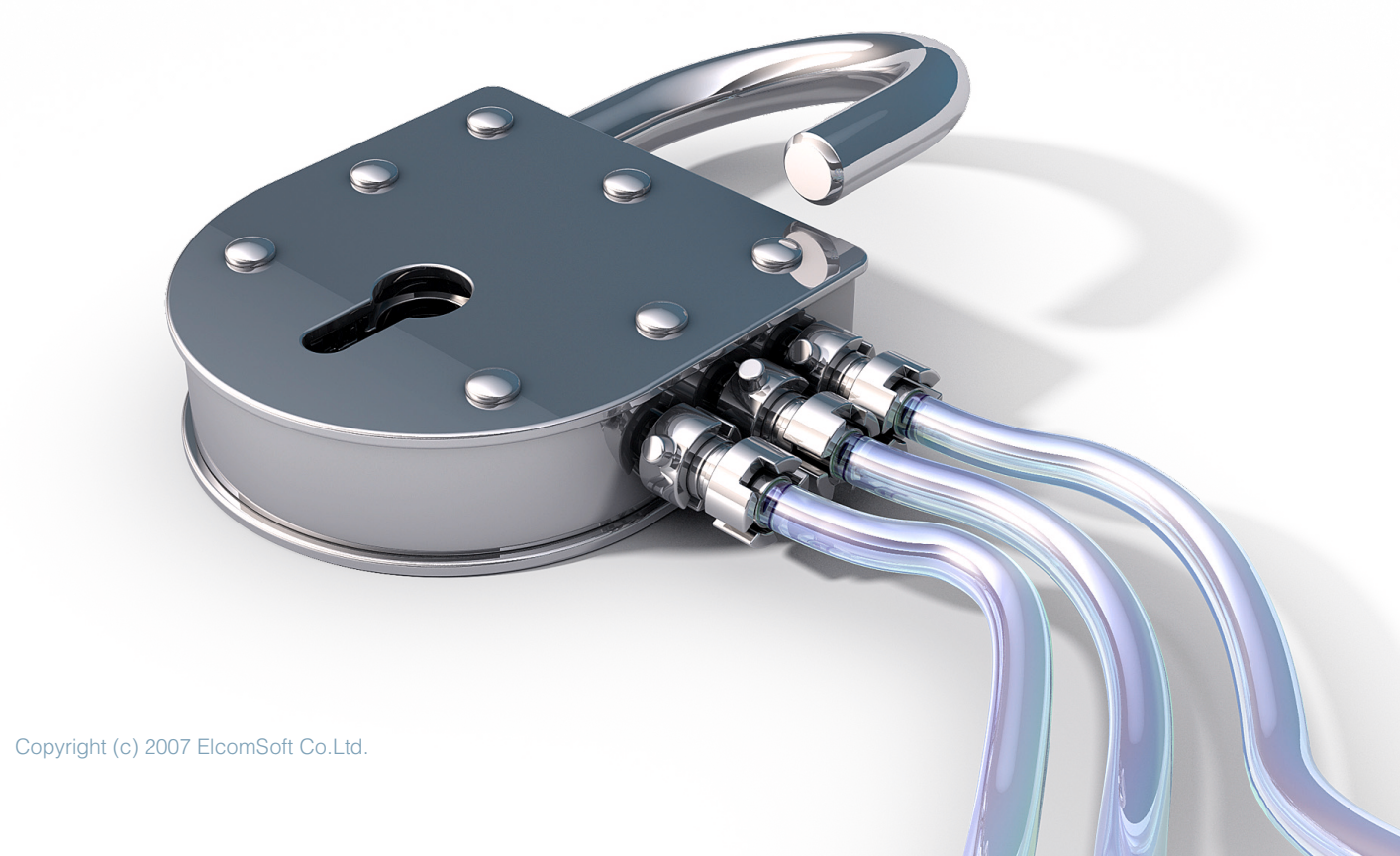
ELCOMSOFT
PROACTIVE SOFTWARE

UNLOCKING PDF

GUARANTEED PASSWORD RECOVERY FOR ADOBE ACROBAT



ELCOMSOFT
PROACTIVE SOFTWARE

CONTENTS

GOING DIGITAL

Rapid development of digital technologies and electronic communication, availability of mobile PCs and smart phones, abundance of tools for creating documents or high-quality presentations coupled with constantly growing volumes of information and yearning for doing business more effectively leads to switching to electronic exchange of information.

Not only enterprises, but state organizations are introducing new electronic systems of documents circulation. Online-readers of e-newspapers and e-magazines outnumber those, who still read print media. Some titles exist on the net only. Those who own PDAs prefer e-books and e-magazines over paper ones. For instance, more than 80,000 e-books can be bought at the Amazon[1] online store.

Exchanging e-documents means compatible platforms, applications and software versions. Everyone has faced a "can't open the file" situation. What does a file recipient use – PC or Mac, Windows Vista or Windows XP, Microsoft Word or Corel WordPerfect? The solution is using a universal format, which depends neither on software nor on hardware.

[1] PDF books and documents. Data of 12.09.07

WHAT'S GOOD ABOUT PDF?

Such format does exist. This is an immensely popular PDF (Portable Document Format) — cross-platform format for e-documents, designed by Adobe.

Documents saved as PDF files can be viewed on virtually any system. Though platform, operating system, installed fonts or software may vary, a document with original text formatting, font settings, pictures or layout can still be opened, read or printed correctly.

PDF is widely used in publishing and printing, distributing e-versions of media, publishing reports, reference information or documents, and exchanging data. Google search results for PDF files amounts to 2 360 000 pages!

It is really important that the software needed to open a PDF is **free** (from Adobe or a third party). These figures show the popularity of PDF format: Acrobat Reader is downloaded from CNET Downloads for nearly 35 billion times per month[2].

Versatile PDF format has quite a number of extra features: easy browsing of large documents with a help of a cross-reference system; proper viewing of a document with handheld devices running Palm OS, Symbian OS etc; text availability for search engines; compact files (small file size) and – the feature we are most interested in – **wide range of document protection methods**.

[2] Over a period 08.08.07-13.09.07

PDF DOCUMENTS PROTECTION

CUI BONO?

Let's see who needs to protect a PDF document and why. Today's world assumes that possessing information is a competitive edge. Leak of confidential data may cause direct financial harm to an enterprise, indirect losses of opportunities and other unfavorable or unpredictable effects.

Obviously, much attention is paid to data protection. IT Security is a rapidly developing branch of Information Technology industry. The easiest method of data protection is locking with a password. One has an ability to set the password (to open and/or edit the document, or use particular features like hi-resolution printing) in most desktop applications, including Adobe Acrobat.

Proper document password protection should keep the balance between security and usability. When setting a protection to a PDF document, one should keep the following points in mind:

1. target audience (all users, or just a certain group);
2. version of Adobe Acrobat / Acrobat Reader available;
3. storage location or publishing location of the document (company web site, intranet, or printing-house);
4. data type (text, graphics, multimedia);
5. presumable usage of the document (viewing, filling forms, sending by mail, editing or reviewing).

PDF DOCUMENTS PROTECTION METHODS

Adobe Acrobat features two levels of PDF password protection. Protecting the 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). Also, there are "open" (so-called "user") passwords. If one is set, the file is encrypted with strong algorithm, and cannot be opened at all, if the password or encryption key is not known.

Adobe Acrobat uses RC4 encryption algorithm (stream cipher, widely-used by various data protection systems), while Adobe Acrobat 7.0 and upwards can also use AES (Advanced Encryption Standard). Originally, 40-bit encryption has been used, but version 5.0 and above uses 128-bitencryption, which makes it much more difficult to find a password (40-bit encryption involves 240 values, while 128-bit encryption involves 2128 values).

In addition, using security certificates allows creating different access/usage rights for different user groups. For instance, some users will be allowed to fill in the forms, while users from another group will be able to edit the document as well.

Certificate-based protection for Adobe Acrobat is based on two keys: public key and private key. The former one is used to decrypt the file, and the last one is used for document encryption and/or signing a document.

DATA ACCESS LOSS

Good document protection is a double-edged weapon. Why?

Confidential data, such as sales reports, market research results or analytic reports, is stored in PDF files, and all operations (editing, printing and even opening a file) could be password-protected.

Obviously, the weakest link of any protection technology is a human. Password protection is a subject of various “flaws”. How many times have you forgotten a password? Once you may need to access a document created by your colleague or partner, but that person could have quitted the job or taken a leave. What should be done? You can’t cease a project because of such a hindrance.

And another problem is more likely to occur when working with PDF files. Imagine you need to extract a piece of information from a report to prepare tender documents, but you fail to select and copy some text from a file. You obey copyright and always refer to a source of information, but you have to prepare the documents for tomorrow’s tender as soon as possible.

And here is the rub: you need to remove restrictions set for a PDF file, or decrypt it (if it requires password at opening) to get access to the information and solve current business tasks.

SOLVING A PUZZLE

A FEW WORDS ABOUT PASSWORDS

Since the problem of password loss first occurred the day password protection was invented, software developers have considered a way of tackling it. As the result, a number of password recovery technologies are available now.

Putting aside the issue of nowadays password recovery methods, let's start with basic knowledge about passwords, password types and information, which may assist you in finding a password.

English language passwords generally use the following symbols: 26 lowercase letters (a…z), 26 uppercase letters (A…Z), 10 digits (0…9) and 33 specific characters (!@#$%^ etc), which makes 95 symbols for any combinations. Sometimes specific symbols are excluded from the group, which decreases the number of possible combinations. Moreover, password may be short or long, which is crucial when one cannot retrieve or reset a password, but has to use the brute-force attack.

Understanding human mind also counts on a quest for a password. In spite of numerous restrictions forced on users to secure password protection, some users still neglect the most simple security tips. Such phenomenon proves that human is a weak link, a dangerous breach in system security.

The majority of popular passwords are nothing but words, derived from a mother tongue of a user. Sometimes words, used as passwords, can be found in user's daily life: birth year, pet name, phone number, credit card number etc. A new password can be a slightly modified previous password. This is the way most users solve the problem of regular password changing, prescribed by security policy. And the most important hint, people tend to keep a password note right at a work desk or in a file on a PC. Though, such a remedy undermines the whole idea of password protection.

Thus, being aware of basic password security requirements (such as password structure or length) or having some information about a user may help finding a password. Technologies, applied by specific software to recover passwords, enable using such kind of information.

PASSWORD RECOVERY METHODS

The basic methods of password recovery are brute force, mask attack, dictionary search, encryption key search (less possible combinations in comparison with brute force) and so-called "rainbow attack". Sometimes other methods of restoring access to a file are used, for example, known-plaintext attack. Let's review some of the methods briefly.

Brute force attack

Brute force attack is simple: in search for a password a program tries every possible combination of symbols. The search may be restricted to a certain length and character set (letters, digits and other symbols).

But how much time does the brute force attack need to recover a password? It depends on the factors mentioned above (password length, character set), performance of the PC used for password recovery task, and the file type.

Of course, a correct password may be found quickly and a program won't have to try all the possible combinations. But you shouldn't count on that. The task can take years, if ran on an average PC. The brute force attack, as the most time-consuming method, may be resorted to, when no other methods are at the hand.

Mask attack

In the case you created a password by yourself, you may try to recover a password with a help of mask attack by limiting the search range. You might remember the length of a password or some of the symbols. Any information may be of use to you.

For example, you are quite sure, that you used only digits and lowercase Latin letters. Then, when setting search parameters, you may exclude specific symbols and uppercase letters. That would be great if you also knew a certain position of a symbol in a password. For example, a password consists of 10 symbols, starts with a letter "a" and ends with "2007", than you can use a "a?????2007" search pattern. Unknown symbols are designated with questions marks in the pattern.

Mask attack is making sense: a program has to try fewer combinations, so a password will be found in less time.

It's a pity, but any details about a password are rarely known, thus mask attack cannot be used generally. Fortunately, there is one more efficient password recovery method.

Dictionary attack

Let's assume that you possess some information about possible words or names that could be used in a password. In this case you may use the dictionary attack.

Users tend resort to common words for creating passwords. Generally, these are English words like "open", "access" or "letmein". In comparison with chaotic combinations of letters and digits such passwords are easier to remember. In fact, such passwords are as easily forgotten as any other passwords, but they are easier to recover.

Where the dictionary (or the word list) should be taken from? First, it may be included into password recovery program package. Second, you may search for it on the Internet. Various lists of common words, thematic lists (fauna, football teams etc), abbreviation lists are commonly available. Third, you can create a dictionary manually.

The method has a number of apparent advantages. The list of common words, generally used in passwords, is limited; it never contains more than a hundred thousand words. Trying hundred thousand combinations is an easy task for a modern PC. It turns out that dictionary attack method should be implemented in the first place. It may do well.

Rainbow table attack

Obviously, the most important criterion of password search is the criterion of time, consumed by the search. Brute force attack tries all possible combinations, and recovery of complex passwords may take too much time. If the search may take up months or years, than its practical use is zero.

A method employing rainbow tables (rainbow attack) is used to eliminate the problem. The basis of the method is using precomputations of password variants for a certain set of symbols.

The idea of replacing resource-intensive computations with a search by a lookup table, that was prepared beforehand, is not brand new. Lookup tables are used when data is easier extracted from the memory, rather than created. The main drawback of a lookup table is its size: not every enterprise can afford storing terabytes of data. That's why rainbow tables, or optimized lookup tables, came into being. The size of a rainbow table is much less, than of a lookup one.

Generating rainbow tables may have preset probability of password or key recovery, suggested time of attack, and time of table's generation. Adjusting the settings and finding a good balance between the attack time and probability of password/key recovery should be considered separately. As a result, the tables that help to quickly find the password/key from a certain range with a high probability are created in a reasonable time.

In comparison with simple lookup tables, the probability of password recovery using rainbow attack is slightly lower than 100%, but the result is still worth trying. For example, rainbow attack based on a table for 7 alphanumeric symbols (built within a week) allows recovering any password consisting of seven alphanumeric symbols within 20-30 seconds. Brute force attack would take up more than 24 hours. The advantage is obvious.

CHOOSING A SOLUTION

Thus there're no more doubts in buying password recovery tool (for PDF files) or not. Obviously, every system administrator should have such tool at hand. The expenses will be repaid a hundredfold when the first password is missed.

What points should be considered in this case?

First, the probability of password recovery claimed by a software provider. The criterion is crucial for estimating solution efficiency. This is why you buy it. Of course, 100% probability may be guaranteed in the absence of time constraints, but this picture is not good enough for you. As a general rule, access to a document has to be restored as soon as possible: time counts.

Second, the next point to consider is a range of supported operating systems, application versions, file formats, languages and encodings. It's hard to tell what version of Adobe Acrobat you'll have to deal with when recovering a password. Make sure you know how to get an upgrade with support of newer versions, and what timeframe such upgrade will be available in.

Third, consider the time needed for password recovery. Of course, it may depend on performance of your PC, but a software provider usually gives some "average" data.

And the last point is whether distributed computing is ever possible. This method of solving complex (CPU-hungry) problems suggests using the united performance of a computer group, for example, computers connected locally or remotely. The method is employed when hacking a password. Some passwords for documents or applications may be recovered in a short period of time with a help of a single computer (for example, ICQ password saved locally, or a password to WordPerfect document), but for many others, the recovery has much higher requirements. For example, PGP passwords are so safe that hacking them could be possible using distributed computing only.

"ELCOMSOFT" SOLUTION – SECURE ACCESS TO PDF-FILES

Russian company ElcomSoft offers a wide range of password-recovery solutions for virtually any system and file format: from applications and instant messengers to archives and Windows logon passwords.

ElcomSoft takes advantage of unique technologies and staff experienced in the field of cryptography. It allows creating high-quality password recovery software. Depending on password length, complexity and encryption method the probability of password recovery amounts into nearly 80%. But in most cases, 100% success rate is guaranteed.

ElcomSoft has developed special software to restore access to Adobe Acrobat files – Advanced PDF Password Recovery. Moreover, you can get Elcomsoft Distributed Password Recovery, which allows to take advantage of distributed computing if the password is long and well selected.

ADVANCED PDF PASSWORD RECOVERY

Advanced PDF Password Recovery supports all versions and encryption methods used by Adobe Acrobat 3.0 – 8.0, allowing to unlocking PDF files and remove restrictions.

Features provided by the program depend on the version: Standard, Professional, and Enterprise. Standard edition allows to removing editing and printing restrictions. Professional edition can find a password to open a file. Enterprise edition finds an encryption key (DVD with rainbow tables is supplied) with a help of improved rainbow attack.

Let's review basic features of the product.

A "user" password (required to open the file) is often known or not set. So the only thing to search for is an "owner" password, which restricts editing and printing options. Advanced PDF Password Recovery uses unique technology to solve this problem: it does not have to try password combinations at all, but allows to decrypting the document regardless of encryption algorithm and key length (see pic 1).

If "user" is set but unknown, Advanced PDF Password Recovery uses a number of methods: brute force attack, mask attack, dictionary search and exclusive technology of key search (see pic 2). The probability of password recovery by common methods (brute force attack or dictionary search) generally amounts to 80%. In the meantime, the key search attack provides 100% success rate, but can be applied only to files with 40-bit protection.

ADVANCED PDF PASSWORD RECOVERY

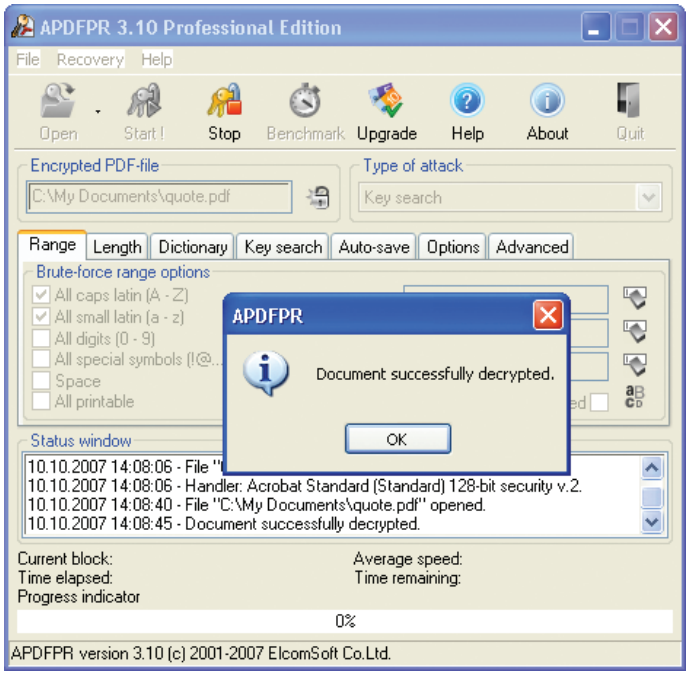
Advanced PDF Password Recovery supports all versions and encryption methods used by Adobe Acrobat 3.0 – 8.0, allowing to unlocking PDF files and remove restrictions.

Features provided by the program depend on the version: Standard, Professional, and Enterprise. Standard edition allows to removing editing and printing restrictions. Professional edition can find a password to open a file. Enterprise edition finds an encryption key (DVD with rainbow tables is supplied) with a help of improved rainbow attack.

Let's review basic features of the product.

A "user" password (required to open the file) is often known or not set. So the only thing to search for is an "owner" password, which restricts editing and printing options. Advanced PDF Password Recovery uses unique technology to solve this problem: it does not have to try password combinations at all, but allows to decrypting the document regardless of encryption algorithm and key length (see pic 1).

If "user" is set but unknown, Advanced PDF Password Recovery uses a number of methods: brute force attack, mask attack, dictionary search and exclusive technology of key search (see pic 2). The probability of password recovery by common methods (brute force attack or dictionary search) generally amounts to 80%. In the meantime, the key search attack provides 100% success rate, but can be applied only to files with 40-bit protection.



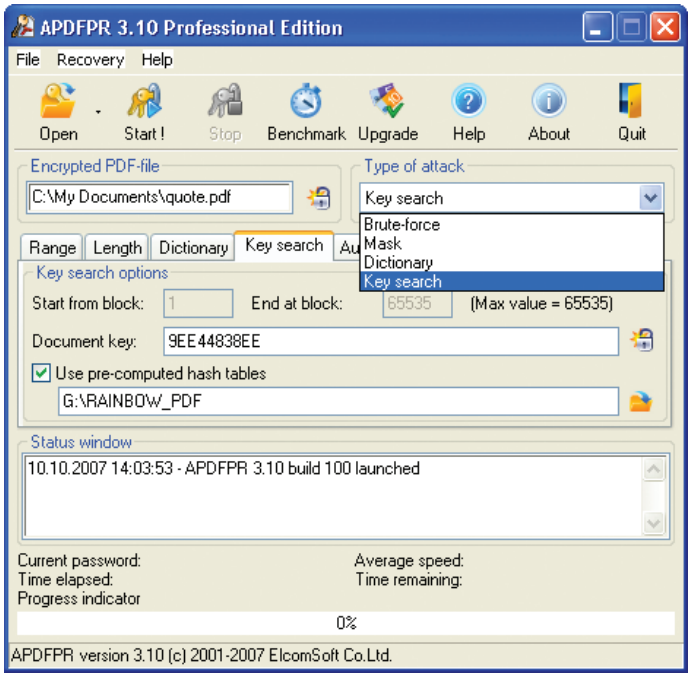
Picture 1. Removing restrictions from a PDF file.

If “user” is set but unknown, Advanced PDF Password Recovery uses a number of methods: brute force attack, mask attack, dictionary search and exclusive technology of key search (see pic 2). The probability of password recovery by common methods (brute force attack or dictionary search) generally amounts to 80%. In the meantime, the key search attack provides 100% success rate, but can be applied only to files with 40-bit protection.

Apart from probability of password recovery, the speed of recovery process counts as well. Advanced PDF Password Recovery has the best results: an average PC needs only several days to restore access to documents protected by user-password and encrypted with 40-bit RC4.

Enterprise edition employs rainbow attack to solve the problem in just a few minutes. Program uses pre-computed hash tables (supplied on a DVD). Thunder Tables™ [3] technology, developed by ElcomSoft, allows reaching 100% probability of finding the key (and so decrypting the file). The technology uses lookup tables and rainbow tables jointly, which, on one hand, guarantees success (as when using simple lookup tables) and, on the other hand, takes only a few minutes to complete. Other parties may guarantee such results only when using full search for an encryption key (takes several days) or using bulky lookup tables (a few terabytes).

[3] Patent technology has been claimed



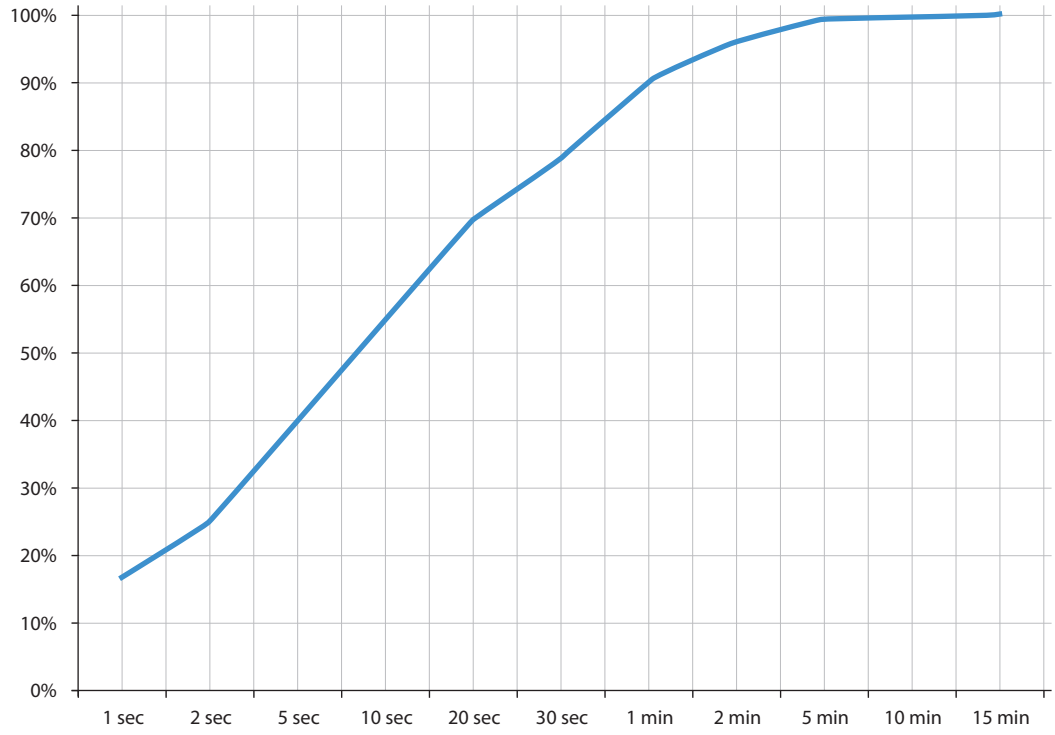
Picture 2. Selecting file decryption method.

The amount of decrypted files depends on attack period (see pic 3). Half of the files are opened within 10 seconds. The maximum attack time is 15 minutes, and the minimum is a fraction of a second; 25 seconds on an average. Using modern computer with multi-core processor (for example, Intel® Core™ 2 Duo) and reading tables from a USB flash card (instead of DVD) is recommended.

The program also allows to restore access to PDF documents protected by 128-bit encryption (including Advanced Encryption Standard) with a help of brute force attack, mask attack and dictionary search. The technology of key search is not applied to files of this type.

The program offers the best working pattern depending on a configuration of your processor (Non-MMX processors, Intel PII/PIII/Celeron, AMD Athlon, Intel P4 SSE2 are enlisted). The highest performance for Core, Core Duo or Core 2 Duo processors is gained by selecting Intel PII/PIII/Celeron from the list.

Trial version of the program can help to estimate its features. Though the functionality is limited (recovery of 4-symbol password and decrypting first 10% of document pages), it still gives a complete image of the product.

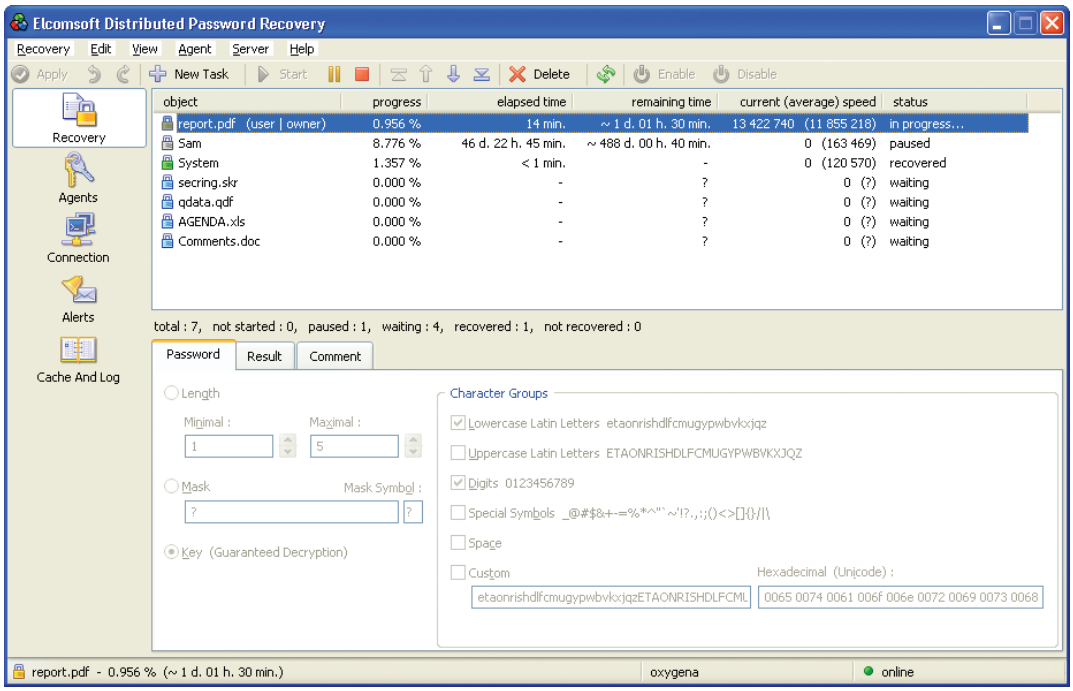


Picture 3. The amount of decrypted PDF files Vs period of attack.

ELCOMSOFT DISTRIBUTED PASSWORD RECOVERY

The advantages of using distributed computing when solving complex tasks have been discussed earlier. When talking about PDF documents, you may also face such tasks, especially if you deal with considerable amount of paperwork, safe passwords and advanced encryption algorithms.

A program consists of three components: server, agent and console. Server (see pic 4), installed on the computer in the local network, controls the brute force attack. Agents, which try certain sets of password combinations sent by the Server, may be installed on all computers in the net. Console may be launched from any computer and allows driving the Server, adding new tasks and viewing statistics. Server and Agent have trial versions.



Picture 4. Main window of Elcomsoft Distributed Password Recovery (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