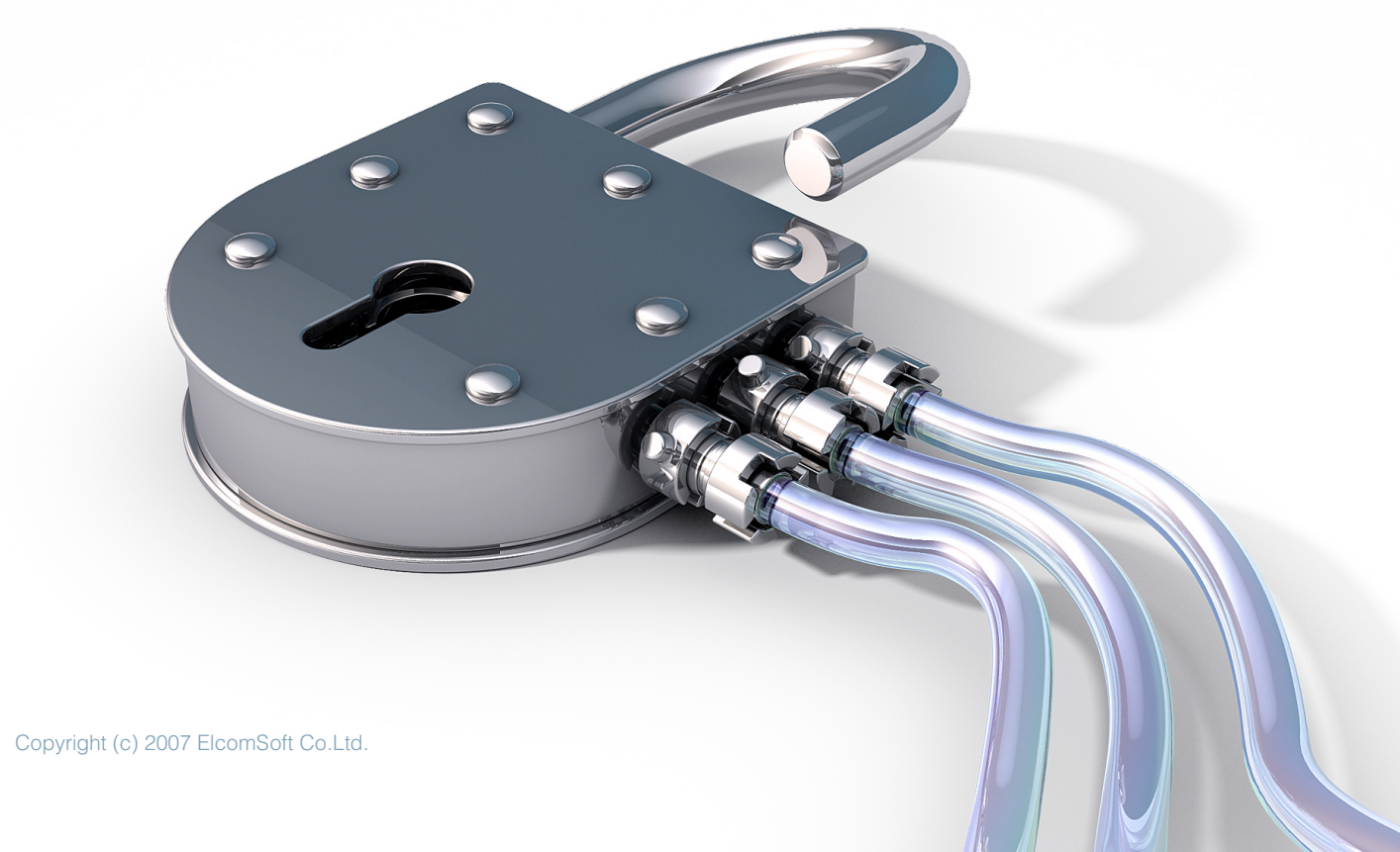
ELCOMSOFT
PROACTIVE SOFTWARE

SIZE DOES MATTER

ADVANTAGES OF DISTRIBUTED PASSWORD RECOVERY



ELCOMSOFT
PROACTIVE SOFTWARE

CONTENTS

INFORMATION IS A KEY TO RIGHT DECISIONS

The words like “information age”, “information technology”, “the one who has the information rules the world” have long since settled in our minds. Everyone knows that information is one of the most precious resources.

Does information itself have any value? No, it doesn’t. Information is crucial in decision making. This is important. Right decision is the key to success in any field. Possessing information is a competitive edge in present business world.

No wonder that protection of information is paid much attention. The most part of information is created and stored digitally (Microsoft Office documents, different databases, and financial data in Intuit Quicken etc). Thus software and hardware means of protecting information are the first to talk about.

PROTECTION IS THE FIRST PRIORITY

IT Security is a rapidly developing branch of Information Technology industry. Market abounds in software products designed to restrict access to information and avoid informational leak, for example, tools for access control and authentication, firewalls, backup systems, antivirus packages and others.

But when speaking about the simplest measures of information protection, the password protection turns out to be the most popular among users.

Data on sales and financial flows, client database, bookkeeping and management accounting, analytic reports and forecasts – all these information is needed to run a company successfully and to make strategic decisions, which influence its growth. Unprotected access to information of these kinds is impossible. This is the simple basis of security policy of a company.

LOSS OF ACCESS – DAILY MATTER

Obviously, the weak link of any informational system is a human. Password protection is subjected to the “flaw”.

In spite of numerous measures been taken to secure password protection, such as limiting minimal password length and complexity, auditing passwords, regular change of passwords, nothing can solve the most common problem – loss of password. It’s hard to find a man, who has worked with a PC, but has never faced this situation.

You may easily forget a password. Being a sensible man you haven’t written it down into your notebook, you’ve chosen to remember it with a help of association. You are sure about the birth year, but your favorite meal has changed and that’s that – you can’t remember it!

Or a sales manager has quitted the job without giving you a password for supply reports. You can’t contact him, counteragents threaten you with breaking a contract, if you won’t pay your bills at once, but you don’t have access to the data.

If employee’s quitting had its roots in financial fraud or working for a rival company, than you shouldn’t even count on his revealing a password. But you still need the access. As soon as possible.

Thus, the problem of password recovery to encrypted data is to be solved. The absurdity of a situation you found yourself in is that the safer a password, the lesser chances you have to break it. Strict password protection policy is hard to intrude. Here is the good news: in most cases the access can be restored.

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 have been presented at the market these days.

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 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 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.

METHODS OF PASSWORD RECOVERY

The basic automatic 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

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, symbol type (letters, digits or other) or symbols, which should be first to be tried.

But how much time does the brute force attack need to recover a password? It depends on password length, set of symbols, and performance of a PC and on password protected 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 SEARCH

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 dictionary search.

Users tend resort to common words for creating passwords. Generally, these are English words like "open", "access" or "password". 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 easy 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 search method should be implemented in the first place. It may do well.

RAINBOW 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 tables 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.

TIME IS MONEY

Having made out what the passwords are and what are the basic methods of password recovery, we can foresee the difficulties of data access recovery: probability of finding a password and period of time needed to find it.

Complexity of finding a password depends on many factors, such as password length, set of symbols, protected document type, encryption algorithm and performance of a PC. As a general rule, probability has direct relation to time: a password can be 100% recovered, if search time is not limited.

These days' users have become more conscious about using passwords: passwords became longer and more complex. For example, about 60% of MySpace[1] users employ passwords, which contain 8 symbols or more, while only 1% of users resort to 5 symbol passwords. 80% of passwords contain letters and digits; passwords, containing a word easily found in a dictionary, make up 3.8%.

As it was said before, a password may be found quickly, so it won't be necessary to try all possible password combinations. But prepare for the worst, because sometimes password search takes up years. Would you still need a password for a file after all this time?

Time factor is crucial when solving a problem of recovering a password, because information loses relevance and becomes obsolete. How can one reduced the password search time?

Encryption algorithm, password length and complexity and document type are constant; these parameters cannot be changed. The only thing we have at our disposal is computing power.

[1] http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300

FINDING PASSWORDS FASTER

DISTRIBUTED COMPUTING

Despite of modern computers processing data at great speed, password recovery with a brute force attack is a stiff task for a single PC, which can take up too much time.

Creating huge computing resource for solving tasks, which occupy many computer-years, is on the world agenda (for example, protein research, mathematic laws, research of human genome, forecasting weather). Only supercomputers, computer of unprecedented performance, can carry out these calculations. Number of supercomputers is constantly increasing, but the price remains very high: not every organization or even not every state can afford a supercomputer[2].

What about uniting a few PCs together? What if they are not few, but there are dozens or even hundreds of them? We will get a totally different kind of a resource. This is how the idea of distributed computing came into being. Distributed computing means carrying out time-consuming calculations with a help of two or more computers, which operate as a network. The task should be divided into parts that could be computed on different computers at the same time. Thus a PC would contribute to a global task by processing a part of data body.

A PC can easily solve such problem in free time. No wonder, that while working with applications (Internet browser, office applications) in Windows a processor stays idle for 99% of work time; it simply awaits new data or tasks to be entered and consumes electricity in vain.

Specialized software, used in distributed computing projects, can load an idle processor with yield. Such software runs in a background mode or starts when processor is idle and terminates at once, when processor is loaded by user, to start again later; running of the software is invisible to a user.

[2] According to http://www.top500.org/ of June 2007, 8 of 10 supercomputers, topping the list of 500 most powerful computers, are located in USA.

BENEFITS OF USING THE METHOD FOR PASSWORD RECOVERY

The task is to try all possible password combinations and to find a lost password or recover access to a document. This is the kind of task that could be easily solved with distributed computing.

Access to some documents or applications may be recovered in a short period of time with a help of a single computer (for example, for IBM® Lotus® SmartSuite®, Corel® WordPerfect® and Office documents regardless of password complexity, or for ICQ or Google talk password, that was saved locally), but other passwords recovery has higher requirements, even if time is not included. High speed search cannot be guaranteed for certain document types or encryption algorithms. For example, Intel® Core™2 Duo can search Microsoft Office 2007 document at guaranteed speed of 100 passwords per second, or it can search RAR-file at speed of not more than 10 passwords per second. RGP password search is time-consuming as well: search speed may vary from dozens to thousands of password per second depending on format and algorithms. Even if search speed is rather high (for example, when using default 40-bit encryption in Word/Excel 97/2000/XP/2003 or Adobe Acrobat PDF documents), distributed computing has a number of advantages. It will take a single PC (even a high-performance one) several days to solve a problem; while a network can manage it within a few hours or even minutes. Moreover, distributed computing is indispensable for searching multiple documents.

Time benefit is not the only advantage of distributed computing. These are a few good points:

- no need to assign a PC (or PCs) to carry out a certain task of password recovery;
- processing of multiple documents;
- using computers at work time or free time (no disturbance to a user);
- using even the slowest PCs of a network – they can also contribute into solving a task;
- modifying the number of engaged PCs depending on number of documents, assumed password complexity and task urgency.

CHOOSING A SOLUTION

Thus there're no more doubts in buying password recovery tool 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 format, 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.

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.

These are the basic criteria of choosing a solution for password recovery.

ELCOMSOFT DISTRIBUTED PASSWORD RECOVERY - PASSWORD AT ONCE

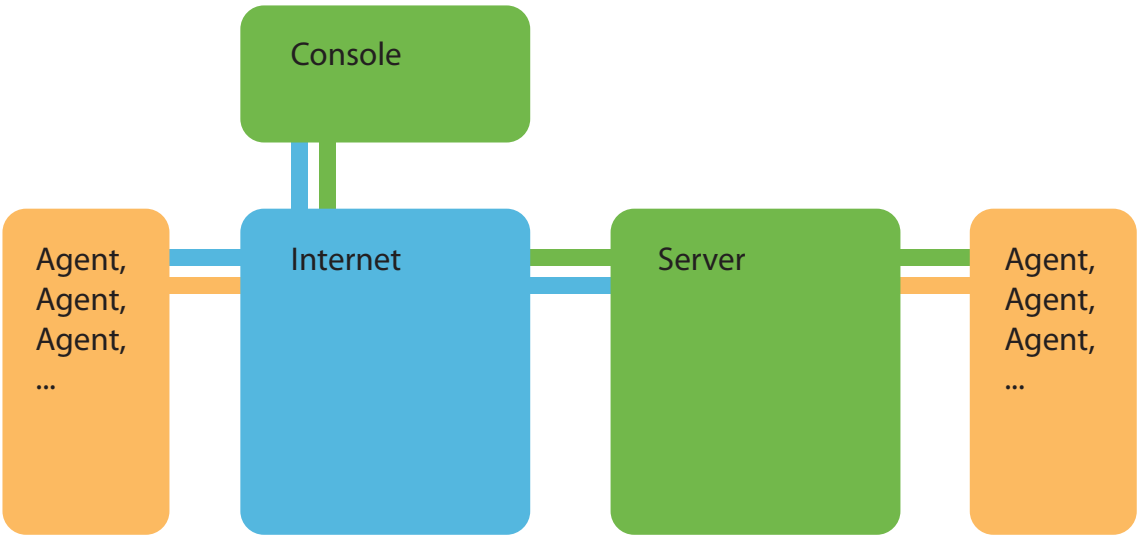
Elcomsoft Distributed Password Recovery allows engaging computing power of all network computers, whether a network is local or global.

This product can recover a password to any Microsoft Office document – Word, Excel, PowerPoint (any edition), passwords for Microsoft Money, Microsoft OneNote, Adobe Acrobat, Intuit Quicken, Lotus Notes (ID files), logon passwords for Windows 2000/XP/2003/Vista, PGP secret keys (*.skr), PGP Disk (*.pgd), PGP Whole Disk Encryption, PGP ZIP archives (*.pgp), PKCS #12 certificates (*.pfx), MD5 hashes.

100% recovery is guaranteed for Word 97-2003 and Excel 97-2003 documents, in case a 40-bit encryption key was used (Microsoft Office default encryption key). Decryption of Adobe Acrobat PDF files with 40-bit encryption is also guaranteed (used in earlier editions of Adobe Acrobat, or selected manually in Acrobat 6/7/8). Elcomsoft Distributed Password Recovery can also find both “user” and “owner” passwords for PDF files with 40-bit or 128-bit encryption.

Well-designed architecture of Elcomsoft Distributed Password Recovery enables constant expanding of supported file formats list.

The program has a “client-server” structure and comprises of three components: server, agent and console (see pic 1).

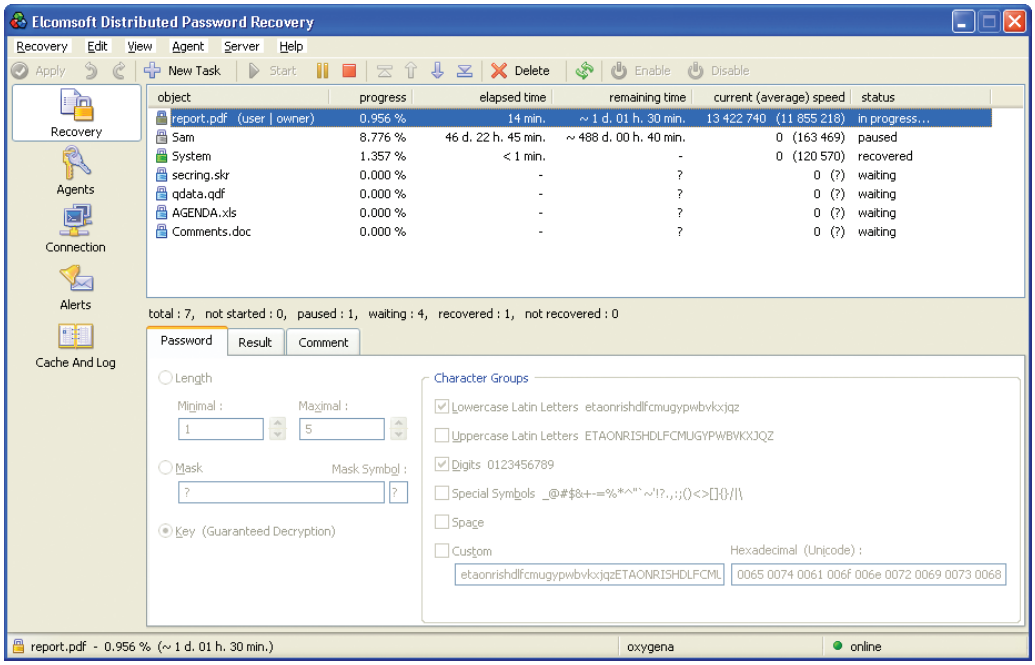


Picture 1: Structure of Elcomsoft Distributed Password Recovery.

The server is started up on one of the computers in the network. Then the previously installed and started up agents (on the workstations) connect to their server, deliver the work done (if they have had any) and receive the next portion of work. The data is transferred in compressed format, so that does not affect the network performance.

Console may be launched from any computer on the Net. It allows controlling the Server, adding new tasks and viewing statistics. Password search server may be controlled either locally or remotely. Work time period (days of week, working hours) and task priority can be set for Agents. A method of password recovery can be chosen when creating a task: search by password length (set minimum and maximum length of a password), mask search (search by minnow part of a password) or guaranteed recovery key search. Set of symbols can be limited as well (lowercase or uppercase letters, digits, specific symbols, space symbols). An administrator can terminate or start a task at any moment.

One of the product advantages is comfortable working with multiple documents. Elcomsoft Distributed Password Recovery allows creating a list of documents; the priority of the search can be edited at any moment. Thus ElcomSoft solution helps to save up computing resources and work time of security service staff.



Picture 2: Main window of Elcomsoft Distributed Password Recovery (server component).

In addition to benefits of using distributed computing for password and key recovery (mentioned above), let's summarize some advantages of Elcomsoft Distributed Password Recovery:

- **Wide range of applications support.** Elcomsoft Distributed Password Recovery can restore access to any documents quickly and efficiently.
- **Scalability.** The product can be used within a network of any size.
- **Minimal network load.** Packed data exchange and minimizing net traffic guarantees minimal overload of a network.
- **Thorough adjustment of agent work.** Work time period (days of week, working hours) and task priority can be set for Agents.
- **Using all available computers.** Even the weakest computers on the net can be used due to setting task priority, setting time of work for agents, minimal software and hardware requirements.
- **Working with multiple documents.** Any number of documents can be enlisted for password search.
- **Choosing an order of document processing.** Every file is given processing priority, which can be edited at any moment.

Server and Agent have trial versions.

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