



# PDF ENTBLOCKEN

GARANTIERTE PASSWORT-WIEDERHERSTELLUNG FÜR ADOBE ACROBAT

## INHALTE

<b>Digitalboom</b> .....	<b>3</b>
<b>Was ist das gute an pdf?</b> .....	<b>4</b>
<b>Schutz der pdf-dokumente</b> .....	<b>5</b>
Cui bono? Schutzmöglichkeiten der pdf-dokumente	
<b>Verlust des datenzugriffs</b> .....	<b>7</b>
<b>Ein puzzle lösen</b> .....	<b>8</b>
Paar wörter über passwörter Methoden zur passwort-wiederherstellung Lösung wählen	
<b>“ElcomSoft” - lösung – sicherer zugriff auf pdf-dateien</b> .....	<b>12</b>
Advanced pdf password recovery ElcomSoft distributed password recovery	
<b>Über ElcomSoft</b> .....	<b>17</b>

## DIGITALBOOM

Eine rasante Entwicklung der Digitaltechnologien und Datenkommunikationen, die Verfügbarkeit der mobilen PCs und Smartphones, die Menge der Tools für das Erstellen der Dokumente oder hochqualitativen Präsentationen, zusammen mit dem immer weiter wachsenden Informationsvolumen und Anzahl der Mitarbeiter, die Ihre Jobs immer effektiver ausführen, führt dazu, dass die Informationen elektronisch ausgetauscht werden.

Nicht nur Firmen, sondern auch die staatlichen Organisationen führen neue elektronische Systeme für die Dokumentenverbreitung ein. Die Anzahl der Online-Leser, die Onlinezeitungen und –magazine lesen, überschreitet die Anzahl jener, die die Printmedien bevorzugen. Einige Ausgaben existieren nur im Web. Die, die PDAs besitzen, bevorzugen elektronische Bücher und Magazine anstatt der gedruckten Versionen. Zum Beispiel, können über 80,000 E-Books im Amazon<sup>1</sup> - Onlineshop gekauft werden.

Der Austausch der E-Dokumente bedeutet kompatible Plattformen, Anwendungen und Software-Versionen. Jeder hat schon mal die "Datei konnte nicht geöffnet werden"-Situation erlebt. Was nutzt der Dateiempfänger - PC oder Mac, Windows Vista oder Windows XP, Microsoft Word oder Corel WordPerfect? Die Lösung ist das Benutzen eines universellen Formates, das weder von Software, noch von Hardware abhängig ist.

<sup>1</sup> PDF – Bücher und -dokumente. 12.09.07

## WAS IST DAS GUTE AN PDF?

Solch ein Format existiert. Es ist das ungemein populäre PDF (Portable Document Format) — Crossplattform-Format für E-Dokumente, das von Adobe entwickelt wurde.

Dokumente, die als PDF-Dateien gespeichert werden, können auf jedem System geöffnet werden. Auch wenn Plattformen, Betriebssysteme, installierte Schriften oder Software variieren können, wird das Dokument trotzdem im unveränderten Textformat - mit alten Schrifteinstellungen, Bildern oder Layout - geöffnet, gelesen und gedruckt.

PDF wird viel in Veröffentlichungen und Druck, Vertrieb der Medien-E-Versionen, Verlagsberichten, Informationshinweisen, sowohl Dokumenten und Datenaustausch benutzt. Google-Suchergebnisse für PDF-Dateien betragen bis 2 360 000 Seiten!

Es ist wirklich wichtig, daß die Software zum Öffnen der PDF-Dateien kostenlos ist. (von Adobe oder Drittprogramm). Diese Zahl zeugt von der Popularität des PDF-Formats: Acrobat Reader wurde etwa 35 Milliarden Mal pro Monat von CNET Downloads heruntergeladen<sup>2</sup>.

Das vielseitige PDF-Format hat eine Anzahl von Extrafeatures: leichtes Durchsuchen großer Dokumente mithilfe des Cross-Reference-Systems; angemessenes Betrachten der Dokumente auf den tragbaren Geräten (Palm OS, Symbian OS etc); Textverfügbarkeit für Such-Engines; kompakte Dateien (kleine Dateigröße) und – das Feature, das uns am meisten interessiert – **viele Methoden zum Dokumentenschutz**.

<sup>2</sup> Im Zeitablauf 08.08.07-13.09.07

## SCHUTZ DER PDF-DOKUMENTE

### CUI BONO?

Lasst uns sehen, wer und warum die PDF-Dokumente schützen sollte. Die heutige Welt geht davon aus, dass das Besitzen der Informationen vom Wettbewerbsvorteil ist. Der Verlust der vertraulichen Daten kann direkten finanziellen Schaden für eine Firma haben, sowohl indirekte Möglichkeitsverluste und andere ungünstige oder unberechenbare Effekte.

Der Datensicherheit wird heute viel Beachtung geschenkt. IT-Sicherheit ist eine sich rasch entwickelnde Branche der IT-Industrie. Die leichteste Methode des Datenschutzes ist die Passwortsperrung. Man kann das Passwort (zum Öffnen und/oder Bearbeiten der Dokumente oder Features, wie hochauflösendes Drucken) in den meisten Anwendungen, einschließlich Adobe Acrobat, festlegen.

Entsprechender Dokumenten-Passwortschutz sollte die Balance zwischen Sicherheit und Bedienbarkeit aushalten. Wenn man den Schutz für ein PDF-Dokument festlegt, sollte einer folgende Punkte berücksichtigen:

1. Zielpublikum (alle Nutzer oder nur eine bestimmte Gruppe);
2. Adobe Acrobat- / Acrobat Reader- Version vorhanden;
3. Speicherplatz oder Veröffentlichungsplatz des Dokumentes (Firmen-Webseite, Intranet, oder Druckverlag);
4. Datentyp (Text, Grafiken, Multimedia);
5. Mutmaßliche Nutzung des Dokumentes (Betrachten, Formular ausfüllen, per E-Mail senden, Bearbeiten oder Prüfung).

## SCHUTZMÖGLICHKEITEN DER PDF-DOKUMENTE

Adobe Acrobat bietet zwei Levels des PDF - Passwortschutzes. Das Dokument mit dem Passwort zur Zugriffseinschränkung zu schützen („Inhaber“, so genanntes „Sicherheits“ oder „Master“-Passwort) beeinflusst nicht die Möglichkeiten des Nutzers, die PDF-Datei zu öffnen und anzusehen, macht es jedoch unmöglich, die Datei zu bearbeiten (zu ändern), diese zu drucken, Text und Grafiken auszuwählen (und diese in die Zwischenablage zu kopieren), Hinweise und Formfelder hinzuzufügen/zu ändern etc (in jeder Kombination). Es gibt auch „offene“ (so genannte „Nutzer“-) - Passwörter. Falls eines gesetzt ist, ist die Datei mit stabilem Algorithmus verschlüsselt und kann überhaupt nicht geöffnet werden, und der Passwortschlüssel ist nicht bekannt.

Adobe Acrobat nutzt RC4 - Verschlüsselungsalgorithmus (Stromchiffre, die oft von verschiedenen Datenschutz-Systemen benutzt wird); Adobe Acrobat 7.0 und höher können auch AES (Advanced Encryption Standard) nutzen. Ursprünglich wurde die 40-Bit-Verschlüsselung genutzt, doch ab der Version 5.0 wird 128-Bit-Verschlüsselung benutzt, was das Finden des Passwortes erheblich erschwert. (40-Bit-Verschlüsselung umfasst 240 - Werte, 128-Bit- Verschlüsselung umfasst 2<sup>128</sup> - Werte).

Zusätzlich ermöglicht die Nutzung der Sicherheitszertifikate das Erstellen unterschiedlicher Zugangs-/Nutzungsrechte für verschiedene Nutzergruppen. So werden, zum Beispiel, einige Nutzer dazu berechtigt, die Formulare auszufüllen, während andere Nutzer aus einer anderen Gruppe auch das Recht haben, die Dokumente zu bearbeiten.

Zertifikatbasierter Schutz für Adobe Acrobat basiert auf 2 Schlüsseln: öffentlicher Schlüssel und privater Schlüssel. Der erste wird benutzt, um die Datei zu entschlüsseln, und der zweite wird für Dokument-Verschlüsselung und/oder Zeichnen des Dokumentes benutzt.

## VERLUST DES DATENZUGRIFFS

Guter Dokumentenschutz ist eine zweiseitige Waffe. Warum?

Vertrauliche Daten, wie Verkaufsberichte, Marktuntersuchungs-Ergebnisse oder analytische Berichte werden in PDF-Dateien gespeichert, und alle Vorgänge (Bearbeiten, Drucken und sogar Öffnen der Datei) könnten passwortgeschützt sein.

Offensichtlich ist der Mensch das schwache Glied in der Sicherheitskette. Passwortschutz ist vielen Fehlern unterworfen. Wie viele Male haben Sie das Passwort vergessen? Vielleicht brauchen Sie irgendwann Zugang zum Dokument, der von Ihrem Kollegen oder Partner erstellt wurde, doch diese Person hat bereits gekündigt. Was soll man machen? Sie können das Projekt wegen solches Hindernisses nicht beenden.

Ein anderes Problem tritt eher bei der Arbeit mit PDF-Dateien auf. Stellen Sie sich vor, Sie brauchen einen Informationsteil aus dem Bericht, um Ausschreibungsdokumente vorzubereiten, doch Sie können den Text aus der Datei weder auswählen, noch kopieren. Sie halten immer die Copyright-Rechte ein und geben immer die Quellen an, doch Sie brauchen schlicht diese Dokumente so schnell wie möglich.

Und hier ist der Hacken: Sie müssen die Einschränkungen, die für PDF-Datei gesetzt wurden, beseitigen oder diese entschlüsseln (falls das Passwort zum Öffnen notwendig ist), um den Zugang zu Informationen zu bekommen und aktuelle Geschäftsaufgaben zu lösen.

## EIN PUZZLE LÖSEN

### PAAR WÖRTER ÜBER PASSWÖRTER

Seit der Passwortschutz erfunden und somit das Problem eines Passwort-Verlustes allgegenwärtig wurde, haben die Software-Entwickler nach einer Möglichkeit gesucht, dieses Problem zu lösen. Als Ergebnis bietet der Markt heutzutage eine weite Reihe der Passwort-Wiederherstellungs-Technologien.

Lasst uns erstmal die Informationen über die Passwort-Wiederherstellungs-Methoden zur Seite legen und die Grundinfos über Passwörter, Passwort-Typen und Infos, die Sie brauchen, um ein Passwort zu finden, ausdiskutieren.

Englischsprachige Passwörter nutzen generell folgende Symbole: 26 Kleinbuchstaben (a...z), 26 Grossbuchstaben (A...Z), 10 Zahlen (0...9) und 33 Sonderzeichen (!@#\$%^ etc); somit ergeben sich 95 Symbole für beliebige Kombinationen. Manchmal werden die Sonderzeichen aus der Gruppe ausgeschlossen, was die Anzahl der möglichen Kombinationen erhöht. Außerdem kann ein Passwort lang oder kurz sein, was von großer Wichtigkeit ist, wenn jemand ein Passwort nicht abrufen oder rücksetzen kann und Brute-Force-Angriff auszuführen hat.

Trotz mehrerer Aufrufe, das Passwort sicher zu verwalten, vermeiden viele Nutzer die einfachsten Schutztricks. Solche Erscheinung erweist, daß ein Mensch ein schwaches Glied in der Kette und eine gefährliche Lücke im Sicherheitssystem ist.

Die Mehrheit der populären Passwörter sind einfach nur Wörter, aus der Muttersprache des Nutzers abgeleitet. Manchmal können die Wörter, die als Passwörter benutzt werden, im Alltagsleben gefunden werden: Geburtsjahr, Telefonnummer, Tiername, Kreditkarten-Nummer etc. Ein neues Passwort kann eine leicht modifizierte Variante des vorherigen Passwortes sein. Dies ist ein Weg, wie die meisten Nutzer die Situation mit regelmäßiger Passwort-Änderung lösen, die von den Sicherheitsvorschriften vorgegeben wird. Doch die offensichtlichste Spur ist, dass die Menschen dazu tendieren, das Passwort auf dem Arbeitsplatz zu behalten oder in der PC-Datei zu speichern. Solch eine Situation untergräbt die Idee des Passwortschutzes komplett.

Demnach kann ein Passwort leicht gefunden werden, wenn man, zum Beispiel, die Passwort-Struktur oder -länge kennt oder einige Informationen über den Nutzer hat. Technologien, die spezifische Software zur Passwort-Wiederherstellung benutzen, ermöglichen die Nutzung solcher Informationen.

## WEGE ZUR PASSWORT-WIEDERHERSTELLUNG

Die Grundmethoden der Passwort-Wiederherstellung sind Brute-Force, Masken-Angriff, Wörterbuch-Suche, verschlüsselte Begriffssuche (weniger mögliche Kombinationen im Vergleich mit Brute-Force) und so genannter Rainbow-Entschlüsselung. Manchmal werden andere Methoden zur Wiederherstellung des Zugriffs auf die Datei benutzt, wie zum Beispiel Known-Plaintext-Angriff. Lasst uns einige Methoden ausführlicher betrachten.

### Brute-Force-Angriff

Brute-Force-Angriff ist einfach: bei der Suche nach einem Passwort probiert ein Programm jede mögliche Symbolkombination aus. Die Suche kann auf bestimmte Länge, Symboltyp (Buchstaben, Zahlen oder anderes) eingeschränkt werden, beziehungsweise auf Symbole, die als erstes ausprobiert werden müssen.

Wie viel Zeit ist jedoch nötig, damit eine Brute-Force-Attacke ein Passwort wiederherstellt? Es hängt von der Passwort-Länge, Symbolreihe und PC-Leistung, sowohl dem passwortgeschützten Dateityp ab.

Natürlich kann ein Passwort sehr schnell gefunden werden, und das Programm muss nicht alle möglichen Kombinationen ausführen. Jedoch sollten Sie darauf nicht zählen. Die Aufgabe kann Jahre dauern, falls sie auf einem Durchschnitts-PC ausgeführt wird. Da die Brute-Force-Technologie die zeitaufwendigste Methode ist, kann darauf nur dann zurückgegriffen werden, wenn keine anderen Methoden vorhanden sind.

### Masken-Attacke

Falls Sie das Passwort selbst erstellt haben, können Sie es mithilfe des Masken-Angriffs wiederherstellen, indem Sie die Suchreihe eingrenzen. Vielleicht wissen Sie noch die Länge des Passwortes oder einiger Symbole? Jede Information könnte vom Nutzen sein.

Sie wissen, zum Beispiel, dass Sie nur Zahlen und kleingeschriebene lateinische Buchstaben benutzt haben. Somit können Sie bei der Suche bestimmte Symbole und Großbuchstaben ausschließen. Es ist auch günstig, wenn Sie eine bestimmte Reihenfolge eines Zeichens im Passwort wissen. Falls zum Beispiel, ein Passwort aus 10 Zeichen besteht, mit „a“ anfängt und mit „2007“ endet, können Sie die Suchvorlage „a?????2007“ nutzen. Unbekannte Zeichen werden in der Vorlage mit Fragezeichen markiert.

Masken-Angriff macht Sinn: ein Programm muss weniger Kombinationen ausprobieren, so dass das Passwort in kürzerer Zeit gefunden wird.

Wenn allerdings keine Details über ein Passwort bekannt sind, kann die Masken-Attacke generell nicht ausgeführt werden. Es gibt aber zum Glück noch eine weitere effiziente Passwort-Wiederherstellungs-Methode.

## Wörterbuch-Suche

Lasst uns annehmen, Sie kennen die Wörter und Namen, die im Passwort vorkommen könnten. In diesem Fall können Sie die Wörterbuch-Suche benutzen.

Die Nutzer neigen oft zur Benutzung allgemeiner Wörter bei der Erstellung der Passwörter. Allgemein könnten es Wörter, wie "öffnen", "Zugriff" oder "Passwort" sein. Im Vergleich zu den chaotischen Kombinationen der Zeichen und Zahlen sind solche Passwörter schneller einzuprägen. Tatsächlich sind solche Passwörter genauso leicht, wie die anderen, zu vergessen, doch leichter wiederherzustellen.

Woher nimmt man aber das Wörterbuch (oder die Wortliste)? Als erstes könnte es in das Passwort-Wiederherstellungs-Programm eingeschlossen sein. Als zweites können Sie danach im Internet suchen. Verschiedene Listen allgemeiner Wörter, thematische Listen (Natur, Fussball-Teams etc), Kurzwort-Listen sind allgegenwärtig. Als drittes können Sie solches Wörterbuch selbst erstellen.

Diese Methode hat offensichtliche Vorteile. Die Liste der allgemeinen Wörter, die in den Passwörtern benutzt werden, ist begrenzt; sie enthält nie mehr als 100 000 Wörter. Das Ausprobieren von 100 000 Kombinationen ist eine leichte Aufgabe für die modernen PCs. Somit ist es ratsam, diese Suchmethode als erste anzuwenden. Es könnte funktionieren.

## Rainbow-Angriff

Offensichtlich ist das wichtigste Kriterium bei der Passwortsuche die Zeit, die man für die Suche braucht. Brute-Force-Angriff probiert alle möglichen Kombinationen aus, und die Wiederherstellung komplexer Passwörter braucht zu viel Zeit. Falls die Suche Monate oder Jahre dauert, ist der praktische Wert gleich Null.

Die Methode der Rainbow-Tabellen („Regenbogen-Angriff“) kann das Problem eliminieren. Der Grundgedanke dieser Methode ist die Nutzung der Vorberechnung von Passwort-Varianten für eine bestimmte Symbolreihe. Die Idee des Ersetzens der ressourcenintensiven Berechnungen durch eine Nachschlagetabelle, die zuvor vorbereitet wurde, ist nicht neu. Nachschlagetabellen werden benutzt, wenn es leichter ist, die Daten aus dem Speicher zu extrahieren, als zu erstellen. Das einzige Manko an der Nachschlagetabelle ist deren Größe: nicht jedes Unternehmen kann sich erlauben, Terabytes von Daten zu speichern. Deswegen wurden die Rainbow-Tabellen (oder optimierte Nachschlagetabellen) ins Leben gerufen. Die Größe der Rainbow -Tabelle ist viel kleiner, als die von der Nachschlagetabelle.

Generieren der Rainbow-Tabelle bestimmt die Wahrscheinlichkeit der Passwort- oder Schlüssel – Wiederherstellung, vorgeschlagene Angriffszeit und Zeit für die Tabellengenerierung im Voraus. Das Abstimmen der Einstellungen und Finden der passenden Balance zwischen der Angriffszeit und Wahrscheinlichkeit der Passwort-/Schlüssel-Wiederherstellung müsste separat behandelt werden. Als Ergebnis werden die Tabellen, die helfen, schnell das Passwort/den Schlüssel aus einer bestimmten Reihe mit hoher Wahrscheinlichkeit zu finden, in einer angemessenen Zeit erstellt.

Im Vergleich zu den einfachen Nachschlagetabellen ist die Wahrscheinlichkeit der Passwort-Wiederherstellung mithilfe des Rainbow-Angriffs niedriger als 100%, doch das Ergebnis ist es wert. So ermöglicht, zum Beispiel, die Rainbow-Attacke, die auf der Tabelle mit 7 alphanumerischen Symbolen (innerhalb einer Woche aufgebaut) basiert, die Wiederherstellung eines Passwortes mit 7 alphanumerischen Symbolen innerhalb der 20-30 Sekunden. Beim Brute-Force-Angriff würden Sie dafür über 24 Stunden brauchen. Der Vorteil ist offensichtlich.

## LÖSUNG AUSWÄHLEN

Somit bestehen nun keine Zweifel, ob das Passwort-Wiederherstellungs-Tool (für PDF-Dateien) gekauft werden müsste. Es ist offensichtlich, dass jeder Systemadministrator solch ein Tool bei sich haben müsste. Die Ausgaben sind spätestens dann zurückgezahlt, wenn das erste Passwort verloren ist.

Was muss in diesem Fall betrachtet werden?

Als Erstes, die Wahrscheinlichkeit der Passwort-Wiederherstellung, die vom Software-Anbieter angegeben wird. Das Kriterium ist für die Bewertung der Lösungs-Effizienz entscheidend. Deswegen kaufen Sie es doch, oder? Natürlich kann die 100%-tige Wahrscheinlichkeit nur in Abwesenheit der Zeiteinschränkungen garantiert werden, doch dieses Bild ist nicht gut genug für Sie. Als Allgemeinregel muss der Zugriff auf das Dokument so schnell wie möglich wiederhergestellt werden: die Zeit geht.

Zweitens ist die Reihe der unterstützten Betriebssysteme, Anwendungs-Versionen, Dateiformate, Sprachen und Dekodierungen zu beachten. Es ist schwer zu sagen, mit welcher Adobe Acrobat – Version Sie sich befassen werden, wenn Sie das Passwort wiederherstellen. Erkundigen Sie sich, wie man die neueren Versionen bekommt, sowohl über die Zeitspanne, in der dieses Upgrade vorhanden sein wird.

Drittens müssen Sie die Zeit beachten, die zur Passwort-Wiederherstellung nötig ist. Natürlich hängt vieles von der Leistung Ihres PCs ab, doch der Software-Anbieter gibt normalerweise die „durchschnittlichen“ Daten.

Der letzte Punkt ist, ob die verteilte Datenverarbeitung überhaupt möglich ist. Diese Methode zur Lösung komplexer (CPU-hungriger) Probleme verlangt nach der Arbeitsleistung einer PC-Gruppe, zum Beispiel, PCs, die lokal oder entfernt miteinander verbunden sind. Die Methode wird beim Passwort-Hacken benutzt. Einige Passwörter für Dokumente und Anwendungen können mithilfe eines einzelnen PCs in kurzer Zeit wiederhergestellt werden (zum Beispiel, lokal gespeichertes ICQ-Passwort oder Passwort für das WordPerfect - Dokument). Doch für viele anderen verlangt die Wiederherstellung größere Ressourcen. So sind, zum Beispiel, die PGP-Passwörter so sicher, daß das Passwort-Hacken nur mithilfe der verteilten Datenverarbeitung möglich ist.

## **“ELCOMSOFT” - LÖSUNG – SICHERER ZUGRIFF AUF DIE PDF-DATEIEN**

Die russische Firma ElcomSoft bietet eine weite Reihe der Passwort-Wiederherstellungs-Lösungen für virtuell jedes System und Dateiformat: von Anwendungen und Instant Messengers bis hin zu Archiven und Windows-Anmeldungs-Passwörtern.

ElcomSoft unterscheidet sich durch einzigartige Technologien und erfahrene Mitarbeiter, die Experten auf dem Kryptographie-Feld sind. Es ermöglicht das Erstellen der hochqualitativen Passwort-Wiederherstellungs-Software. Je nach Passwort-Länge, -komplexität und Verschlüsselungsmethode beträgt die Wahrscheinlichkeit der Passwort-Wiederherstellung bis zu 80%. Doch in vielen Fällen ist ein 100%-ger Erfolg garantiert.

ElcomSoft entwickelte spezielle Software, um den Zugang zu Adobe Acrobat – Dateien wiederherzustellen – Advanced PDF Password Recovery. Mehr noch können Sie Elcomsoft Distributed Password Recovery bekommen, das die Vorteile der verteilten Datenverarbeitung bietet, falls das Passwort zu lang und zu kompliziert ist.

## ADVANCED PDF PASSWORD RECOVERY

Advanced PDF Password Recovery unterstützt alle Versionen und Verschlüsselungsmethoden, die von Adobe Acrobat 3.0 – 8.0 benutzt werden, und ermöglicht das Entlocken der PDF-Dateien und Entfernen der Einschränkungen.

Programmfeatures unterscheiden sich je nach Version: Standard, Professional und Enterprise. Standard – Ausgabe ermöglicht das Entfernen der Bearbeitungs- und Druckeinschränkungen. Professional – Ausgabe kann ein Passwort finden, um die Datei zu öffnen. Enterprise – Ausgabe findet den Verschlüsselungs-Schlüssel (auf DVD mit Regenbogen-Tabellen geliefert) mithilfe des verbesserten Regenbogen-Angriffs.

Lasst uns die Grundfeatures des Produktes betrachten.

Ein "Nutzer"-Passwort (nötig, um die Datei zu öffnen) ist oft bekannt oder nicht gesetzt. So können wir nur nach dem "Inhaber"-Passwort suchen, was die Bearbeitungs- und Druckoptionen einschränkt. Advanced PDF Password Recovery nutzt eine einzigartige Technologie, um das Problem zu lösen: es probiert keine Passwort-Kombinationen aus, erlaubt allerdings das Entschlüsseln des Dokumentes, unabhängig vom Verschlüsselungs-Algorithmus und Schlüssellänge (Bild 1).

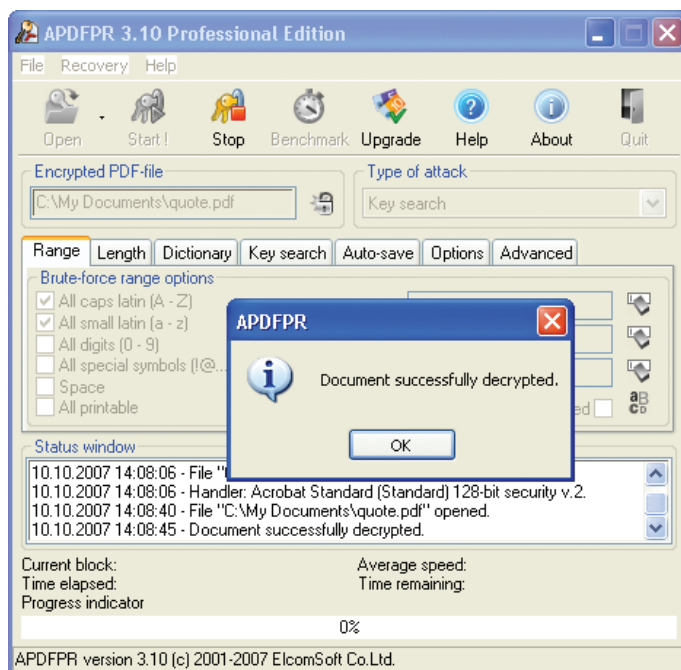


Bild 1. Datei-Entschlüsselungsmethode wählen.

Falls der "Nutzer" festgelegt, aber nicht bekannt ist, nutzt Advanced PDF Password Recovery einige Methoden: Brute-Force-Angriff, Masken-Angriff, Wörterbuch-Suche und exklusive Technologie der Schlüsselsuche (Bild 2). Die Wahrscheinlichkeit der Passwort-Wiederherstellung mit gebräuchlichen Methoden (Brute-Force-Angriff oder Wörterbuch-Suche) beträgt normalerweise bis 80%. Dabei bietet die Schlüsselsuche-Attacke 100% Erfolgsrate, kann allerdings nur auf die Dateien mit 40-Bit-Schutz angewendet werden.

Neben der Wahrscheinlichkeit der Passwort-Wiederherstellung zählt auch die Geschwindigkeit des Suchvorganges. Advanced PDF Password Recovery liefert beste Ergebnisse: ein Durchschnitts-PC braucht nur einige Tage, um den Zugang zu den Dokumenten, die durch das Nutzerpasswort geschützt und mit 40-Bit RC4 verschlüsselt sind, wiederherzustellen.

Enterprise-Ausgabe wendet die Rainbow-Entschlüsselung an, um das Problem in nur wenigen Minuten zu lösen. Das Programm nutzt die Vorberechnungs-Hashtabellen (auf DVD geliefert). Thunder Tables™<sup>3</sup> - Technologie, die von ElcomSoft entwickelt wurde, bietet eine 100%-ge Wahrscheinlichkeit, den Schlüssel zu finden (und somit die Datei zu entschlüsseln). Die Technologie nutzt gemeinsam die Nachschlag- und Rainbow-Tabellen, die auf einer Hand den Erfolg garantieren (als wenn man einfache Nachschlag-Tabellen nutzt) und auf der anderen Hand nur wenige Minuten zum Abschließen brauchen. Andere Firmen garantieren normalerweise solche Ergebnisse nur dann, wenn Vollsuche für den Verschlüsselungsschlüssel (dauert einige Tage) oder umfangreiche Nachschlag-Tabellen (einige Terabytes) benutzt werden.

<sup>3</sup> Patent-Technologie wurde beansprucht

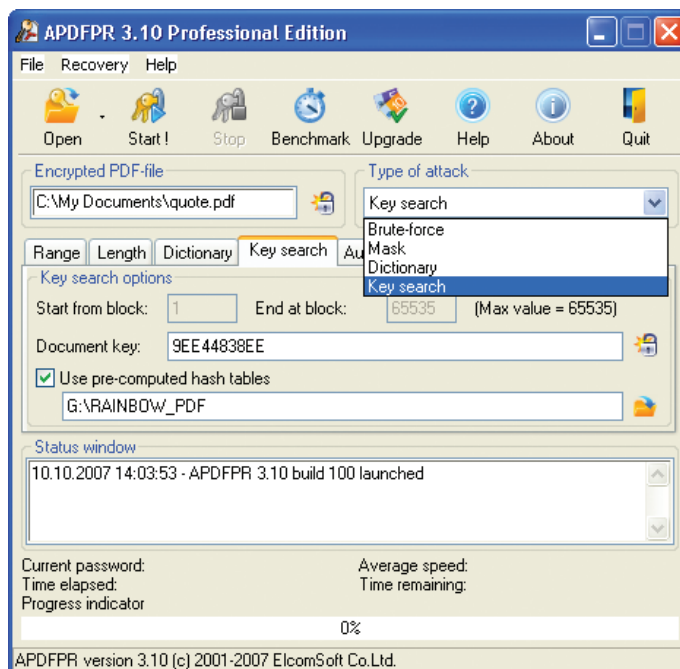


Bild 2. Datei-Entschlüsselungsmethode wählen.

Der Umfang der entschlüsselten Dateien ist von der Angriffsperiode abhängig (siehe Bild 3). Die Hälfte der Dateien werden innerhalb von 10 Sekunden geöffnet. Die maximale Angriffszeit ist 15 Minuten, und das Minimum ist der Bruchteil einer Sekunde; 25 Sekunden im Durchschnitt. Die Nutzung moderner PCs mit Multicore-Prozessoren (zum Beispiel, Intel® Core™ 2 Duo) und das Lesen der Tabellen von der USB-Flashkarte (statt DVD) wird empfohlen.

Das Programm erlaubt auch die Wiederherstellung des Zugriffs auf die PDF-Dokumente, die von der 128-Bit-Verschlüsselung geschützt sind (einschließlich Advanced Encryption Standard), indem Brute-Force-Angriffe, Masken-Angriff und Wörterbuch-Suche benutzt werden. Die Technologie der Schlüsselsuche wird nicht für die Dateien dieses Typs angewendet.

Das Programm bietet das beste Arbeitsmuster, je nach Prozessor-Konfiguration (Nicht-MMX-Prozessoren, Intel PII/PIII/Celeron, AMD Athlon, Intel P4 SSE2 sind aufgeführt). Die höchste Leistung für Core, Core Duo oder Core 2 Duo – Prozessoren ist vorhanden, indem Intel PII/PIII/Celeron aus der Liste ausgewählt wird.

Testversion des Programms hilft beim Aufprobieren dessen Features. Obwohl die Funktionalität beschränkt ist (Wiederherstellung eines 4-stelligen Passwortes und Entschlüsselung der ersten 10% von Dokumentseiten), liefert sie immer noch das komplette Produktbild.

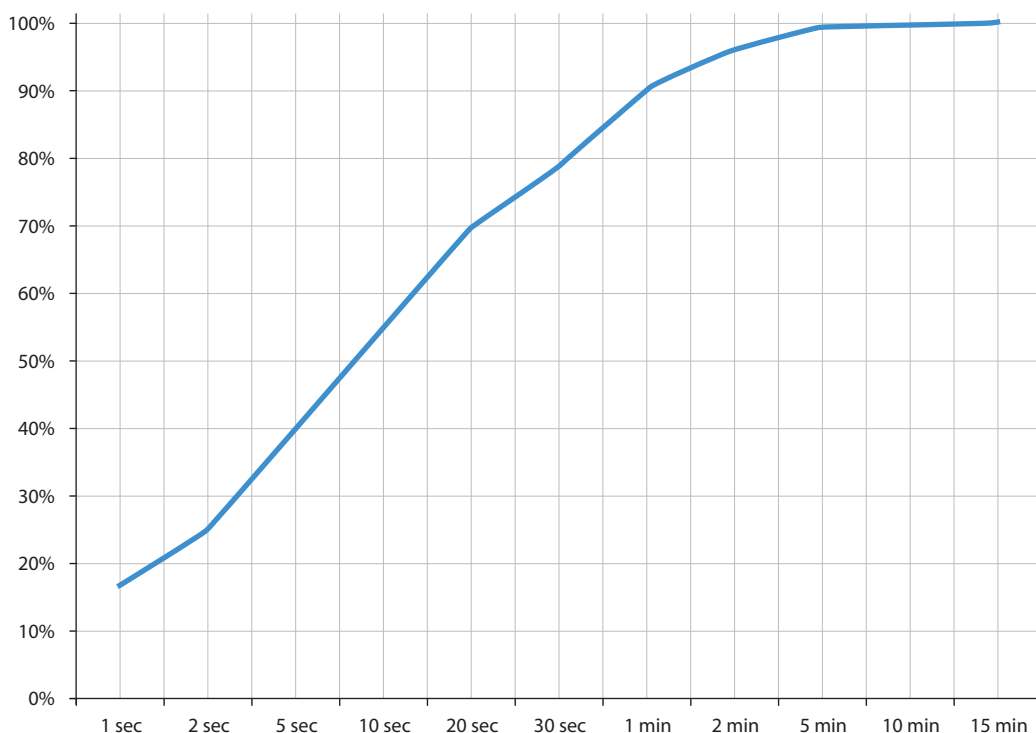


Bild 3. Die Anzahl der entschlüsselten PDF-Dateien vs. Angriffszeit.

## ELCOMSOFT DISTRIBUTED PASSWORD RECOVERY

Die Vorteile des Nutzens von verteilter Datenverarbeitung beim Lösen der komplexen Aufgaben haben wir bereits vorher ausdiskutiert. Bei der Arbeit mit den PDF-Dokumenten können Sie diesen Aufgaben auch begegnen, vor allem, wenn Sie mit großen Dokumentenmengen, Passwörtern und Verschlüsselungsalgorithmen arbeiten.

Das Programm besteht aus 3 Komponenten: Server, Agent und Konsole. Server (s. Bild 4), der auf dem PC im lokalen Netzwerk installiert ist, kontrolliert die Brute-Force-Angriffe. Agenten, die verschiedene Reihen von Passwort-Kombinationen, die vom Server geschickt werden, ausprobieren, können auf allen PCs im Netz installiert werden. Konsole kann von jedem PC gestartet werden und ermöglicht den Serverantrieb, Hinzufügen neuer Aufgaben und Betrachten der Statistiken. Server und Agent haben Testversionen.

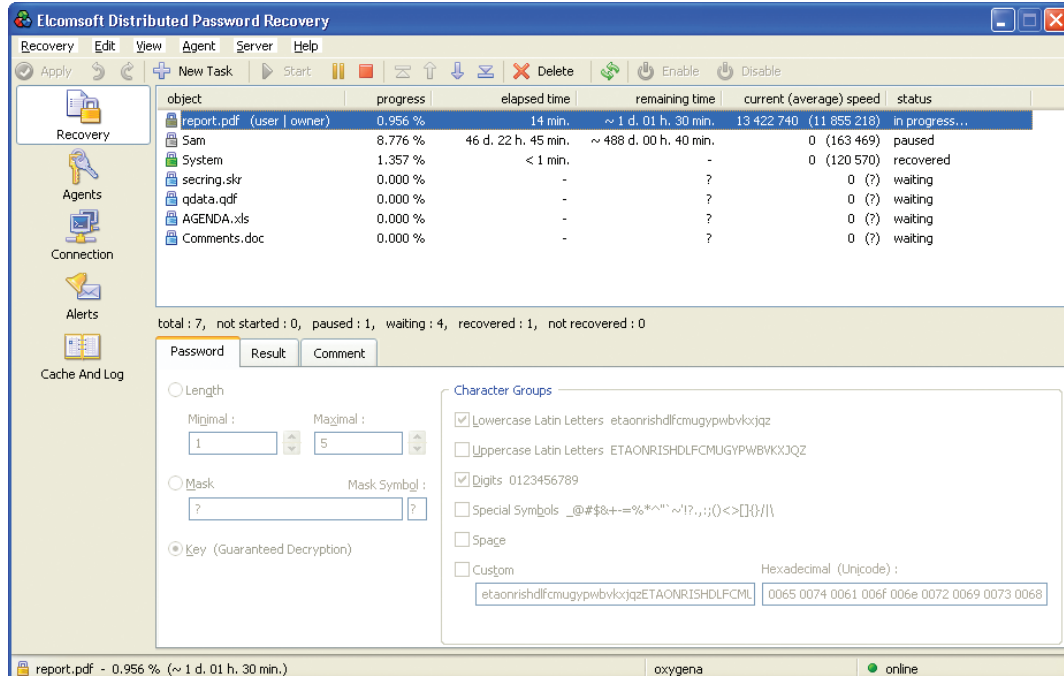
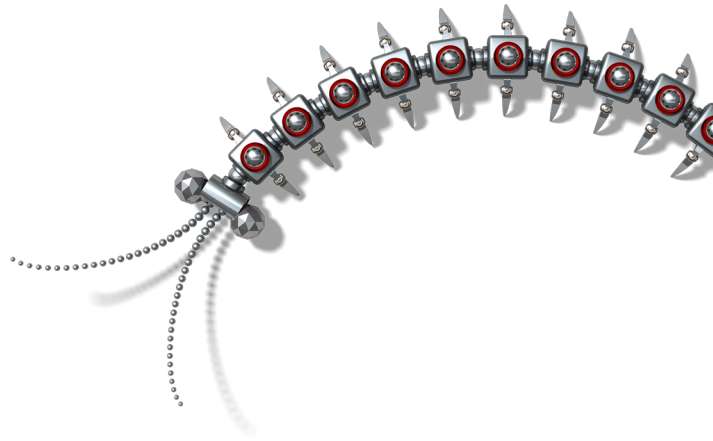


Bild 4. Hauptfenster von Elcomsoft Distributed Password Recovery (Komponente "Server").





Copyright © 2007 ElcomSoft Co.Ltd.  
Alle Rechte vorbehalten

Das vorliegende Dokument ist ausschließlich für Informationszwecke vorgesehen. Sein Inhalt kann ohne vorherige Benachrichtigung verändert werden. Das Dokument garantiert keine Fehlerfreiheit und schließt weder Garantien noch Bedingungen ein, die explizit genannt werden oder vom Gesetz festgelegt sind, einschließlich der indirekten Garantien und Rentabilitätsbedingungen sowie die Eignung des Programms für die Lösung der konkreten Aufgabe. Wir verwehren jegliche Übernahme von Verantwortung, die mit diesem Dokument in Zusammenhang steht. Auf Grundlage dieses Dokumentes können weder direkte noch indirekte vertragliche Verpflichtungen abgeleitet werden. Das Dokument darf ohne schriftliche Genehmigung des Unternehmens Elcomsoft weder reproduziert noch in irgendeiner Form oder mit beliebigen elektronischen oder mechanischen Mitteln für andere Zwecke weitergegeben werden.

Die in diesem Dokument verwendeten Namen sind die Warenzeichen ihrer entsprechenden Eigentümer.