

PARAGON Encrypted Disk

Anwenderhandbuch

Paragon Technologie, Systemprogrammierung GmbH

Copyright © Paragon Technologie GmbH

Herausgegeben von
Paragon Technologie GmbH, Systemprogrammierung
Pearl-Str. 1
D-79426 Buggingen

Inhalt

Inhalt.....	2
1. Einführung.....	3
2. Installation & Voraussetzungen.....	4
3. Der Hauptbildschirm	5
4. Operationen/Befehle.....	7
4.1. Eine verschlüsselte Imagedatei erstellen	8
4.2. Eine verschlüsselte Imagedatei hinzufügen	12
4.3. Eine verschlüsselte Imagedatei als logisches Laufwerk zuordnen (mounting).....	12
4.4. Zuordnung als logisches Laufwerk aufheben (dismounting).....	12
4.5. Alle verschlüsselten Imagedateien als logische Laufwerke zuordnen	13
4.6. Verschlüsselte Imagedatei entfernen	13
4.7. Eigenschaften.....	13
4.8. Verschlüsseltes Laufwerk neu verschlüsseln.....	14
4.9. Zugriff (share) auf verschlüsseltes Laufwerk regeln	14
4.10. Zugeordnetes verschlüsseltes Laufwerk formatieren.....	14

1. Einführung

Dies ist ein Programm das ihre Daten in Echtzeit verschlüsselt und entschlüsselt. Echtzeit bedeutet das dieses Ver- und Entschlüsseln kontinuierlich bei jedem Lesen und Schreiben von Dateien durchgeführt wird. Die Daten sind somit lediglich bei der Bearbeitung auf dem Bildschirm oder bei Ausgaben auf den Drucker in verständlicher Form vorhanden. Abgespeichert in der Datei sind sie dagegen komplett unlesbar.

Dieses Programm bietet daher den perfekten Schutz vor dem Zugriff durch Unberechtigte. Selbst beim Diebstahl der ganzen Festplatte sind die im verschlüsselten Laufwerk abgelegten Daten somit für den Dieb absolut unerreichbar.

Grundlage des Programms ist eine verschlüsselte Datei, eine Art Imagedatei die zu Beginn als Datei mit einer frei einstellbaren Größe in einem vorhandenen logischen Laufwerk angelegt wird. Diese Datei kann dann dem Betriebssystem als virtuelles logisches Laufwerk zugeordnet und von diesem wie jedes andere logische Laufwerk verwaltet und adressiert werden. Alle in diesem logischen Laufwerk abgelegten Dateien sind verschlüsselt und nicht lesbar.

Diese Datei, die dann als virtuelles logische Laufwerk adressiert wird, kann sich auf einer beliebigen Festplatte oder auf einem ZIP/ Jaz Laufwerken befinden und es sind mehrere solcher Dateien resp. virtueller logischer Laufwerke möglich. Das verschlüsselte virtuelle Laufwerk kann in FAT, FAT32, oder NTFS formatiert werden und die maximale Größe ist nur vom Dateisystem bzw. dem verfügbaren Festplattenspeicher beschränkt.

Bei der Erstellung dieser Imagedatei müssen neben der Größe auch die Verschlüsselungsart und der Zugang festgelegt werden. Als Verschlüsselung kann wahlweise Blowfish (448-bit) oder Triple DES (128 Bit) verwendet werden. Als Zugang kann entweder ein Passwort oder ein spezieller Schlüssel gewählt werden, der auf einer Diskette abgelegt werden sollte.

Begriffe/Hinweise/Empfehlungen:

Verschlüsselte Imagedatei;

Diese Datei kann In einem beliebigen logischen Laufwerk mit einer festen Größe angelegt werden. Diese Datei ist ohne Zuordnung wie eine gewöhnliche Datei in dem logischen Laufwerk sichtbar aber nicht lesbar. Wird diese Datei dem Betriebssystem als logisches Laufwerk zugeordnet so verhält sich diese Datei wie ein echtes logisches Laufwerk.

Logisches Laufwerk:

Diese werden unter Windows durch Buchstaben wie C:, D: usw. adressiert. Das verschlüsselte logische Laufwerk erscheint daher unter Windows wie jedes andere logische Laufwerk und es kann auch in verschiedenen Dateisystemen (FAT, FAT-32 & NTFS) formatiert oder defragmentiert werden. Ebenso kann SCANDISK benutzt werden um eine defekte Dateistruktur zu reparieren.

Verschlüsseltes Laufwerk;

Ein verschlüsseltes Laufwerk ist eine dem Betriebssystem zugeordnete Imagedatei.

Verschlüsselung

a) über Passwort: Nicht zu empfehlen und wenn verwenden Sie sinnlose Buchstaben Kombinationen wie "t4f2i3h1s0" .

b) über einen speziellen Schlüssel der in einer Datei und immer auf einer Diskette gespeichert werden sollte. Diese Verschlüsselung ist zu empfehlen da dieser Schlüssel extrem sicher ist.

Wichtig zu wissen: Gehen Passwort oder Schlüssel verloren so sind auch die Daten im verschlüsselten Laufwerk für immer verloren. Es gibt für niemanden eine Hintertür, auch nicht für die Programmierer dieses Programms.

2. Installation & Voraussetzungen

Das Installationsprogramm kopiert alle benötigten Dateien und installiert die verschiedenen Treiber und erstellt die Programmgruppe in Windows.

Die Hauptkomponenten des Programms sind:

a) Paragon Encrypted Disk Manager – Eine Windows Applikation um die verschlüsselten Laufwerke handhaben zu können. Dieses Modul muß in der Programmgruppe aufgerufen werden.

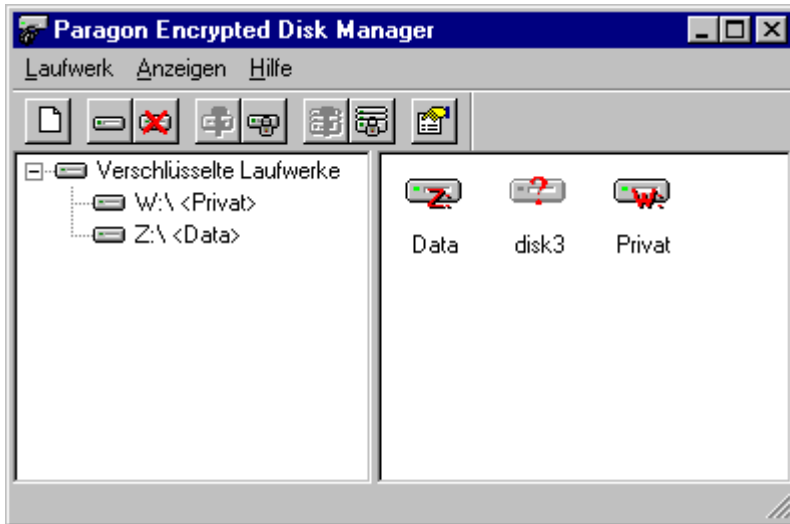
b) Paragon Encrypted Disk Service – Dies sind die für den Anwender nicht sichtbaren Systemtreiber die bei jedem Start von Windows geladen werden.

Voraussetzungen:

Eine beliebige Windows Version (WIN 95, 98 ME WIN NT 4.0 oder WIN 2000.) Für WIN NT wird der Service Pack 3 oder höher empfohlen.

Die Installation erfolgt wie jede andere Programminstallation unter Windows nach Aufruf von SETUP komplett Dialog geführt und bedarf keiner weiteren Beschreibung.

3. Der Hauptbildschirm



Der Hauptbildschirm besteht aus folgenden Elementen:

Pulldown-Menüs, Toolbar und zwei Anzeige-Fenstern. Das linke Fenster zeigt die bereits zugeordneten verschlüsselten Imagedateien als adressierbare logische Laufwerke in Baum-Form an. Das rechte Fenster zeigt alle vorhandenen verschlüsselten Imagedateien/virtuellen Laufwerke als Symbole (Icons) an. Status Anzeige für verschlüsselte Laufwerke:

Zugeordnetes Laufwerk



disk1

Nicht zugeordnetes Laufwerk



disk2

Sobald der Anwender ein neue verschlüsselte Imagedatei anlegt wird diese im rechten Fenster angezeigt. Diese Imagedatei kann nun jederzeit Windows als logisches Laufwerk zugeordnet werden.

Jene Imagedateien die (momentan) nicht gefunden werden können, werden mit einem Fragezeichen angezeigt. Diese Imagedateien befinden sich entweder auf einem beweglichen und momentan nicht eingelegten Datenträger oder auf einem momentan nicht im Zugriff befindlichen Netzwerk Laufwerk. Der Status der angezeigten Symbole kann jederzeit über F5 (Aktualisieren oder refresh) auf den aktuellen Stand gebracht werden.

Werden Imagedateien von einem logischen Laufwerk in ein anderes kopiert oder verschoben so müssen sie im Pulldown-Menü Laufwerke neu aufgenommen werden

Pulldown-Menü "Laufwerke"



Pulldown-Menü "Anzeigen"



Der Aufruf der zur Verfügung stehenden Befehle kann über die Pulldown-Menüs, die Befehlszeile (Toolbar) und teilweise auch über Mausclicks aufgerufen werden.

4. Operationen/Befehle

4.1. Eine verschlüsselte Imagedatei erstellen	8
4.2. Eine verschlüsselte Imagedatei hinzufügen	12
4.3. Eine verschlüsselte Imagedatei als logisches Laufwerk zuordnen (mounting)	12
4.4. Zuordnung als logisches Laufwerk aufheben (dismounting).....	12
4.5. Alle verschlüsselten Imagedateien als logische Laufwerke zuordnen.....	13
4.6. Verschlüsselte Imagedatei entfernen	13
4.7. Eigenschaften	13
4.8. Verschlüsseltes Laufwerk neu verschlüsseln.....	14
4.9. Zugriff (share) auf verschlüsseltes Laufwerk regeln	14
4.10. Zugeordnetes verschlüsseltes Laufwerk formatieren.....	14

Hinweis: Ein Teil der Befehle auf verschlüsselte Laufwerke steht auch von innerhalb des Windows Explorer über Eigenschaften zur Verfügung wenn ein solches verschlüsseltes Laufwerk im Windows Explorer ausgewählt wurde.

4.1. Eine verschlüsselte Imagedatei erstellen

Dieser Befehl kann auf 2 Arten aufgerufen werden:

1. Im Windows Desktop rechten Maus-Klick ausführen und dann "Neu" -> "Encrypted Disk Image" wählen.
2. Im Paragon Encrypted Disk Manager Pulldown-Menü Laufwerk -> "Verschlüsselte Imagedatei erstellen" wählen.

Dies ruft den Wizard zum Erstellen eines verschlüsselten Laufwerks auf.



Abfrage: Speicherplatz und Größe für Imagedatei

Wählen Sie das logische Laufwerk in dem die Laufwerk Imagedatei angelegt werden soll. Die Imagedatei kann in jedem logischen Laufwerk (Festplatte, ZIP/JAZ, etc.) angelegt werden. Stellen Sie sicher das in dem ausgewählten Laufwerk genug freier Speicherplatz für die gewünschte Größe der Imagedatei vorhanden ist. Die hier erforderlichen Angaben sind Größe der Imagedatei und deren Name.



Verschlüsselungsverfahren

Auswahl des Verschlüsselung Algorithmus: Es stehen 2 unterschiedliche Algorithmen zur Auswahl: Blowfish (448 Bit) und Triple DES.



Auswahl des zu verwendeten Zugriffsschlüssels

Möglichkeit 1: Passwort

Hier erfolgt die Verschlüsselung bez. der spätere Zugriff über ein vom Anwender einzugebendes Passwort. Dies Methode ist etwas komfortabler aber auch einfacher zu durchbrechen.

Möglichkeit 2: Vom Programm erzeugter Schlüssel

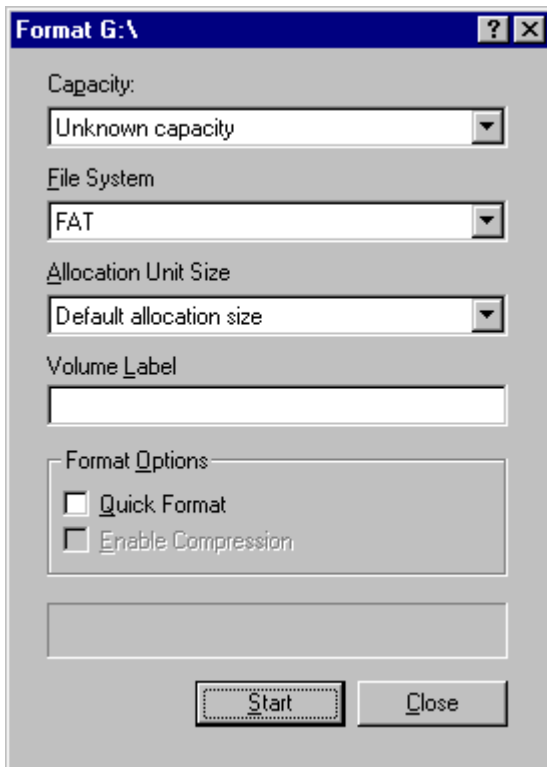
Diese Methode ist sehr sicher da dieser vom Programm erzeugte Schlüssel kaum jemals erraten werden kann. Der Schlüssel wird in einer Datei abgelegt und diese Datei sollte nicht auf der Festplatte sondern auf einer Diskette aufbewahrt werden.

Die Datei in der der Schlüssel abgelegt wird hat den gleichen Namen wie die Imagedatei jedoch mit der Erweiterung .CRK.

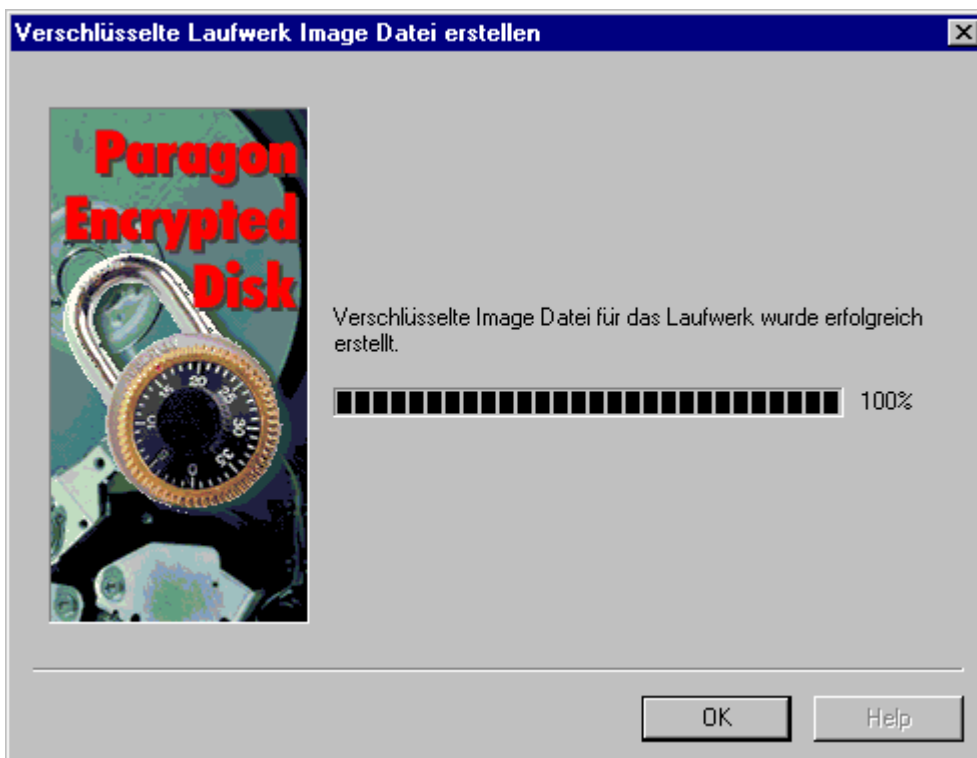


Imagedatei als Laufwerk zuordnen und formatieren

Nach der Erstellung der Imagedatei wird diese dem Betriebssystem als logisches Laufwerk zugeordnet. Die Zuordnung kann über den nächsten freien oder einen beliebigen Laufwerksbuchstaben erfolgen. Damit das Betriebssystem mit diesem Laufwerk auch arbeiten kann müssen Sie es formatieren. Zu diesem Zweck erscheint das Standard "Formatierung" Fenster von Windows in dem Sie das Dateiformat auswählen. Nach Start wird mit der Formatierung begonnen.



Hinweis: Die Warnung von Windows das alle Daten in dem zu formatierenden Laufwerk verloren gehen bezieht sich nur auf das neu erstellte virtuelle verschlüsselte Laufwerk. Das reale Laufwerk, in dem dieses verschlüsselte virtuelle Laufwerk als Datei angelegt wurde, ist natürlich von dieser Formatierung nicht betroffen.

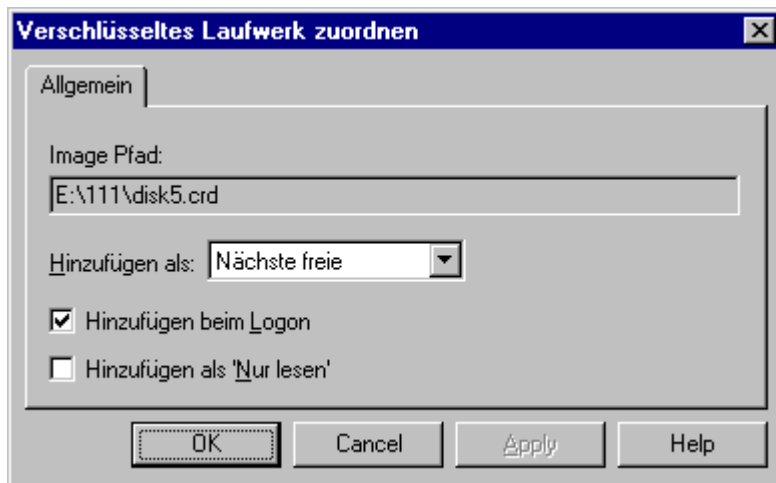


4.2. Eine verschlüsselte Imagedatei hinzufügen

Imagedateien die aus der Verwaltungsdatei gelöscht wurden oder die verschoben oder kopiert wurden, bzw. auf einem beweglichen Datenträger von einem anderen PC kommen können neu in diese Datei aufgenommen werden. Dies geschieht über Paragon Encrypted Disk Manager→Laufwerke→Imagedatei hinzufügen.

4.3. Eine verschlüsselte Imagedatei als logisches Laufwerk zuordnen (mounting)

Nur mit einer als logisches Laufwerk zugeordneten Imagedatei kann gearbeitet werden. Die Zuordnung kann über das Pull-down-Menü→Zuordnung Imagedatei oder über das anklicken der Imagedatei (rechte Maustaste) erfolgen. In beiden Fällen wird das Fenster Zuordnen Imagedatei als logisches Laufwerk angezeigt.



Sie können einen beliebigen freien Laufwerksbuchstaben auswählen oder aber über Wahl "Nächster freier" dem System die Zuordnung des nächsten freien Laufwerksbuchstaben übertragen.

Falls Sie wünschen das die Imagedatei bei jedem Systemstart automatisch als logisches Laufwerk zugeordnet wird so kreuzen Sie dies an. Ebenso kann die Zuordnung mit der Einschränkung "Nur Lesen" erfolgen – in diesem Fall ist der schreibende Zugriff auf dieses Laufwerk nicht möglich.

Nach Drücken der "OK" Schaltfläche wird nach dem Passwort bzw. nach der Schlüsseldatei gefragt. Nur mit dem richtigen Passwort bzw. mit der richtigen Schlüsseldatei wird die Imagedatei als logisches Laufwerk zugeordnet.

4.4. Zuordnung als logisches Laufwerk aufheben (dismounting)

Jede Zuordnung einer Imagedatei als logisches Laufwerk kann jederzeit wieder aufgehoben werden. Sie können das von innerhalb des Windows Explorer oder von innerhalb Paragon Encrypted Disk Manager ausführen.

Wichtig: Die Aufhebung der Zuordnung als logisches Laufwerk kann nur dann erfolgen wenn keine Datei innerhalb dieses logischen Laufwerks geöffnet ist und auch kein Programm gerade das Dateiverzeichnis des logischen Laufwerks verwendet, z.B. Windows Explorer dies gerade anzeigt.

Die Aufhebung der Zuordnung erfolgt außerdem bei jedem Logoff oder Runterfahren des Systems.

4.5. Alle verschlüsselten Imagedateien als logische Laufwerke zuordnen

Sie können pauschal alle vorhandenen verschlüsselten Imagedateien als logische Laufwerke zuordnen (Paragon Encrypted Disk Manager→Laufwerke→Alle zuordnen. Sie werden für jedes Laufwerk nach dessen Schlüssel oder Passwort gefragt.

4.6. Verschlüsselte Imagedatei entfernen

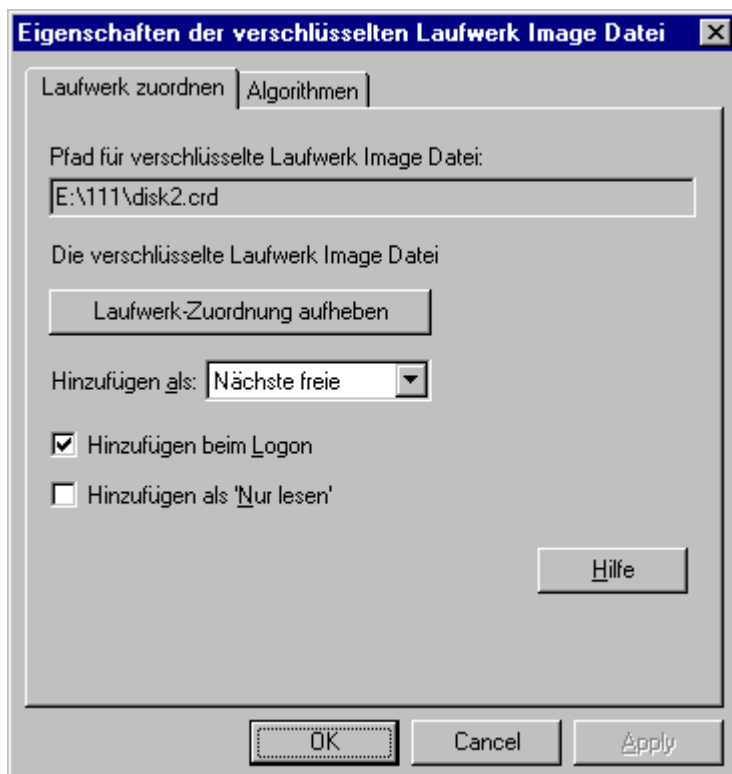
Jede verschlüsselte Imagedatei kann zum einen als Eintrag aus der Dateiverwaltung des ED Managers entfernt als auch komplett von der Festplatte gelöscht werden..

Im Paragon Encrypted Disk Manager→Laufwerk→Laufwerk entfernen wählen. Zuerst wird die Zuordnung als logisches Laufwerk aufgehoben und danach erfolgt die Entfernung des Eintrags aus Dateiverwaltung. Ist auch Löschen von der Festplatte angekreuzt worden so wird auch die verschlüsselte Imagedatei selbst gelöscht.



4.7. Eigenschaften

In Windows Explorer können Sie die Eigenschaften des verschlüsselten Laufwerks einsehen:



Zusätzlich zu den Standardangaben werden Angaben zur Verschlüsselung und zu der logischen Laufwerkszuordnung angezeigt. Desweiteren kann hier eine Neu Verschlüsselung mit neuem Passwort oder neuem Schlüssel vorgenommen werden.

4.8. Verschlüsseltes Laufwerk neu verschlüsseln

Ein verschlüsseltes Laufwerk kann mit einem neuen Passwort oder mit einem neuen Schlüssel neu verschlüsselt werden. Entweder über Windows Explorer→Eigenschaften oder über Paragon Encrypted Disk Manager→Laufwerke→Neu verschlüsseln. Es wird dann zuerst die Zuordnung als Laufwerk aufgehoben und nach Abfrage und Neueingabe eines Passwortes resp. mit einem neuen Schlüssel die Imagedatei mit diesem neuen Passwort resp. Schlüssel neu verschlüsselt.

4.9. Zugriff (share) auf verschlüsseltes Laufwerk regeln

Wie auf jedes andere logische Laufwerk unter Windows kann der Zugriff auf eine verschlüsseltes Laufwerk durch mehrere Anwender geregelt werden.

4.10. Zugeordnetes verschlüsseltes Laufwerk formatieren

Wie bereits mehrfach gesagt verhält sich eine als logisches Laufwerk zugeordnete Imagedatei wie ein normales logisches Laufwerk.. Um es zu formatieren wählen Sie im Windows Explorer die Option Eigenschaften. Die Formatierung löscht wie in einem echten Laufwerk die logische Adressierbarkeit aller dort abgelegten Dateien. .