

Handbuch ArchiCrypt Shredder 5

Dok.-Nr.: ACSHR-HB-0003

Ausgabedatum: Mittwoch, 10. November 2010

Ausgabe-Nr.: 5.0

Alle Rechte vorbehalten Weitergabe sowie Vervielfältigung dieser Unterlage, Verwertung und Mitteilung ihres Inhalts sind nur mit ausdrücklicher Zustimmung von Dipl.-Ing. Patric Remus erlaubt. Zuwiderhandlungen verpflichten zum Schadenersatz.

Inhalt

Teil I Hilfe zur Hilfe	1
Teil II Bestellen und Registrieren	2
Teil III Einleitung	5
1 Willkommen	5
2 Neu in Version 5	7
Teil IV Allgemeine Informationen	10
1 Installationshinweise	10
2 Systemvoraussetzungen	10
3 ArchiCrypt Shredder unter Windows Vista und Windows 7	11
Teil V Bedienung ArchiCrypt Shredder	13
1 Überblick	13
2 Gemeinsame Bedienoberfläche	17
3 Dateimanager	19
4 Laufwerksbelegung	20
5 Duplikat Finder	25
Analyse	25
Quarantäne	27
6 ADS Scanner	28
7 Datenträger	31
Bereiche & Strukturen	31
Löschen von Datenpartitionen	33
Boot CD & Löschen des Betriebssystems	35
Hartnäckige Dateien	36
8 Verzeichnisse	37
9 Online-Spuren	41
Online-Spuren	41
Funktionen für Internet Explorer	45
10 Plugins	46

11 Sichere Löschezonen	51
Überblick	52
Sichere Löschezonen	54
ArchiCrypt Shredder - Sichere Löschezone	57
12 Mobile Nutzung	59
13 Kontextmenü	60
14 LogBuch	65
Teil VI Aufgaben-Planer	66
1 Aufgaben planen	67
2 Zeitüberwachung	71
Teil VII Einstellungen	73
1 Allgemeines	73
2 Sicherheit	75
3 Hotkeys	78
4 Duplikat Finder	79
5 ADS Scanner	82
Teil VIII Plugin Editor	84
1 Einleitung Plugin Editor	84
Willkommen	84
2 Plugin Aufbau	84
Überblick	84
Vordefinierte Pfade	85
Variablen	87
Indikatoren	88
Aktionen	89
Überblick.....	89
Registry	90
File	91
Path	91
Process	92
Service	93
Inifiles	93
COM	94
Layered Service Provider.....	94
RegExport.....	95
Teil IX Pro Script Editor	95

1	Hilfe zur Hilfe	95
2	Einleitung	96
	Willkommen	96
3	Kurze Einführung	97
	Voraussetzungen	97
	Sprachelemente	98
	Erweiterung der Script Sprache.....	103
	Sonderfunktionen Shredder.....	105
 Teil X Technischer Teil		 108
1	Verschiedene Betriebs- und Dateisysteme	108
2	Wichtige Begriffe	109
3	Schnelles Überschreiben	111
4	DoD 5220.22-M	111
5	VSITR	112
6	Peter Gutman	112
7	Schwachstellen/Tipps	112
	 Index	 116

1 Hilfe zur Hilfe

Nutzen Sie die Hilfe

Sie sollten sich etwas Zeit nehmen, und die wichtigsten Kapitel zumindest überfliegen.

Als Anwender sollten Sie die folgenden Kapitel lesen.

- [Installationshinweise](#)
- [Systemvoraussetzungen](#)
- [Bedienung](#)

Grundsätzlich gilt.

Wenn man sich über die Auswirkung einer Aktion nicht sicher ist, sollte der Blick in das Handbuch erfolgen.

Symbole

Innerhalb der Hilfe sind besondere Textstellen durch bestimmte Symbole hervorgehoben.



UNBEDINGT LESEN

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, sollten Sie unbedingt lesen. Sie weisen häufig auf Gefahrenquellen, Fehlerfallen oder Einschränkungen hin oder beschreiben wichtige Sachverhalte.



WICHTIGE HINWEISE

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, enthalten wichtige Informationen über Verhaltensweisen der Software und technische Hintergründe.



TIPP

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, geben Ihnen wertvolle weiterführende Hinweise.



EXPERTENTIPP

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, enthalten Hinweise für fortgeschrittene Anwender. Sie weisen weitergehende Möglichkeiten der Software auf oder beschreiben technische Hintergründe.

2 Bestellen und Registrieren



Bestellen bei ArchiCrypt

<http://www.ArchiCrypt.com>

[Weitere Bestellmöglichkeiten >>](#)

So schalten Sie ArchiCrypt Shredder frei

Nach Erhalt der **Seriennummer** starten Sie bitte das Programm. Klicken Sie auf **Kaufen - Registrieren** in der Titelleiste.

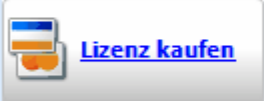






Es erscheint der folgende Dialog:

Registrieren

Registrierungsname: **E-Mail:**

Seriennummer:


So geht das Registrieren ganz einfach!

Sie können die Angaben manuell in die jeweiligen Eingabefelder übertragen. Achten Sie dabei darauf, dass Sie die Daten exakt eingeben!

Nach erfolgter Eingabe klicken Sie auf die Schaltfläche Registrieren

1. In den meisten Fällen wurden Ihnen die Daten per E-Mail zugestellt. Für diesen Fall gibt es eine sehr einfache Methode, die Software zu aktivieren.
2. Öffnen Sie die E-Mail mit den Daten zum Programm.
3. Markieren Sie die Daten des Programms mit der linken Maustaste.
4. Der Markierte Text muss dabei unbedingt die Begriffe Registrierungsname und Download enthalten. Es sollte in etwa wie folgt aussehen:

Registrierungsname:
Mustermann9876

E-Mail:
Max.Mustermann@MaxMustermannsSeite.de

Seriennummer:
2424-C569-8354-A7A1-A1AF-8663-B777-12BB-C3FB-C797-DA71-6D

Download:
http://www.ArchiCrypt.com/files/Shredder5_Vollversion.zip

5. Klicken Sie jetzt auf Registrieren!
6. Die Daten werden jetzt in das Registrierungsformular übertragen und die Registrierung abgeschlossen.

 Weitere Bestellmöglichkeiten

<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: yellow; padding: 5px;">Online-Shop</td> <td style="background-color: yellow; padding: 5px; text-align: center;">zum Online-Shop</td> <td style="background-color: yellow; padding: 5px;">Sobald Sie den Bestellvorgang starten, wird</td> </tr> </table>	Online-Shop	zum Online-Shop	Sobald Sie den Bestellvorgang starten, wird
Online-Shop	zum Online-Shop	Sobald Sie den Bestellvorgang starten, wird	

		eine verschlüsselte SSL-Verbindung aufgebaut. Alle Daten, die zwischen Ihrem Rechner und unserem Bestellsystem übertragen werden, sind dadurch gegen fremden Zugriff geschützt. Internet-Shopping auf sichere Art!
Telefon	(089) 66000-893 Montag - Freitag 09.00 - 17.00 Uhr	Teilen Sie uns die Rechnungsanschrift mit und halten Sie einen Stift und ein Stück Papier bereit. Der Bearbeiter teilt Ihnen das Passwort zur Freischaltung sofort am Telefon mit, das Produkt kann sofort produktiv eingesetzt werden. Gerne beantworten wir auf diesem Wege auch offene Fragen.
FAX	(089) 66000-875	Bestellformular PDF Bestellformular Word Laden Sie sich zu diesem Zweck das von uns vorbereitete Formular von unserer Internetseite. Füllen Sie die entsprechenden Felder bitte leserlich aus und FAXen uns die Bestellung. Falls Sie die Versandart "Nur Passwort" gewählt haben, senden wir Ihnen das Passwort an die angegebene Emailadresse, oder teilen Ihnen das Passwort telefonisch unter der angegebenen Rufnummer mit. Während unserer Geschäftszeiten (Montag - Freitag 09.00 - 17.00 Uhr), erhalten Sie nach dem Bestelleingang umgehend das zur Freischaltung notwendige Passwort.
Brief	<u>Anschrift:</u> Softwareentwicklung Dipl.-Ing. Patric Remus Am Brunneck 6 85521 Ottobrunn	Bestellformular PDF Bestellformular Word Laden Sie sich zu diesem Zweck das von uns vorbereitete Formular von unserer Internetseite. Füllen Sie die entsprechenden Felder bitte leserlich aus und senden uns die Bestellung. Falls Sie die Versandart "Nur Passwort" gewählt haben, senden wir Ihnen das Passwort an die angegebene Emailadresse, oder teilen Ihnen das Passwort telefonisch unter der angegebenen Rufnummer mit.
Anonym	<u>Anschrift:</u> Softwareentwicklung Dipl.-Ing. Patric Remus Am Brunneck 6 85521 Ottobrunn	Voraussetzung für den anonymen Bezug der Software ist ein Email-Zugang bei einem Anbieter, der ihre persönlichen Angaben nicht überprüft. Senden Sie uns einen Brief mit Bargeld in EURO in Höhe des Produktpreises. Fügen Sie dem Brief die Email-Adresse bei. Sie erhalten Ihren Key dann an diese Mailadresse.

3 Einleitung

3.1 Willkommen



Vielen Dank, dass Sie sich für ArchiCrypt Shredder© entschieden haben.

Mit ArchiCrypt Shredder beseitigen Sie unnötigen Ballast und sorgen dafür, dass gelöschte Daten wirklich unwiderruflich gelöscht werden.

Löschen von Dateien

Sicher haben auch Sie Dateien deren Inhalt nur ausgewählten Personen zugänglich sein sollte. Sensible Daten fallen ständig an. Seien es TAN-Listen für Ihr Online-Banking, Passwortdateien, vertraulich oder höher eingestufte Dokumente aus Ihrem Arbeitsumfeld oder schlicht die Spuren Ihres letzten Internetbesuchs. Man kann die Liste beliebig fortsetzen. Wenn es schließlich um das Löschen dieser Dateien geht, ist die Sache nicht ganz so einfach, wie sie zunächst scheint.

Löschen mit Betriebssystemmitteln ist unsicher

Falls Sie Dateien mit den Methoden des Betriebssystems löschen, sind die Daten nicht wirklich gelöscht. Lediglich der Verweis auf die Datei wird entfernt, die Inhalte sind noch vorhanden, bis eine andere Datei deren Platz einnimmt. Jeder, der ein entsprechendes Softwaretool einsetzt, kann Daten, die auf diese Art gelöscht wurden, wieder herstellen. Gelegentlich werden auch nur Teile einer Datei überschrieben. Die verbleibenden Fragmente enthalten oft große Teile der Ursprünglichen Dateien.

Falls Sie nach dem Surfen die Funktionen Ihres Browsers nutzen, um Ihre Spuren zu beseitigen, fühlen Sie sich nicht zu sicher. Die Dateien können einfach wiederhergestellt werden. Um sicherzustellen, dass die Dateien tatsächlich gelöscht sind, müssen die Daten vor dem eigentlichen Löschen überschrieben werden.

Anwendungen sind unsicher

Auch wenn Sie ab sofort alle Dateien mit ArchiCrypt Shredder löschen, werden sensible Daten durch Anwendungen ungefragt im s.g. Freispeicher abgelegt und anschließen mit unsicheren Methoden gelöscht. Gute Beispiele finden sich im Bereich aller Office Produkte, die meist nicht auf der Originaldatei arbeiten, sondern auf einer zuvor angelegten Kopie. Nach Abschluss des Bearbeitungsvorganges wird die ehemalige Originaldatei gelöscht und die Arbeitskopie umbenannt. Diese Daten können einfach betrachtet und wiederhergestellt werden, bis sie zufällig überschrieben werden.

Platzfresser sind schwer zu finden

Mit der Zeit sammeln sich unzählige Dateien an. Der freie Festplattenplatz schwindet zusehends. Wo genau befinden sich diese Dateien? Eine Frage die nicht ganz so leicht zu beantworten ist. Die Analyse der Laufwerksbelegung gibt schnell Auskunft darüber, wo sich

die wirklich großen Dateien verbergen.

Unnötige Doppelgänger

Oft rauben identische Dateien, die an unterschiedlichen Stellen im System abgelegt sind, wertvollen Festplattenspeicher. Das Auffinden solcher Dateien ist schwierig, wenn sie unterschiedliche Dateinamen tragen, sogar nahezu unmöglich. Der Duplikat Finder analysiert Ihr System und unterstützt Sie beim sinnvollen Entfernen der überflüssigen Dateien. Es ist äußerst schwierig zu entscheiden, welches der Duplikate gelöscht wird, und welche Datei unangetastet bleiben soll. Hier hilft die intelligente Auswahl und, für den Fall aller Fälle, eine Quarantäne Funktion, mit der Sie entfernte Duplikate wieder zurückspielen können.

ADS Scanner (Alternative Datenströme)

Alternative Datenströme sind Bereiche, in denen, verborgen vor den Augen eines normalen Anwenders, beliebige Daten gespeichert werden können. Diese so genannten alternativen Datenströme belegen Platz und bieten aufgrund ihrer Eigenschaften Schadprogrammen (Viren/Trojanern) ideale Versteckmöglichkeiten. ArchiCrypt Shredder spürt solche Daten nicht nur auf, sondern kann sie anzeigen und natürlich sicher entfernen!

Mobile Nutzung

Wer ist heute nicht in der Situation, dass er seine Arbeit an verschiedenen Rechnern erledigt. Wer ist heute nicht im Besitz eines USB- oder U3-Sticks, mit dem Daten von einem Rechner zum anderen transportiert werden. Da kommen die neuen Funktionen von ArchiCrypt Shredder genau richtig. Ab sofort können Sie sich mit der normalen PC-Version von ArchiCrypt Shredder eine Installation auf USB-Stick oder U3-Stick erzeugen, die Ihnen auch unterwegs sichere Löschfunktionen für Dateien, Surfspuren und Co. anbietet.

Plug-ins

Plug-ins sind kleine Programm Module, mit denen die Funktionen des Shredders nahezu beliebig erweitert werden können. Dabei gibt es zwei Arten von Plug-ins. An erster Stelle zu nennen sind die Plug-ins, die sich um Überreste von Anwendungen kümmern und diese beseitigen. Noch leistungsfähiger sind die so genannten Pro Scripte. Dabei handelt es sich um richtige kleine Programm mit denen Sie nahezu beliebige Aufgaben erledigen können. Die Vollversion von ArchiCrypt Shredder bringt ca. 130 Plug-ins mit, darunter ca. 10 Pro-Scripte. Diese erledigen Aufgaben wie Backup, Verschlüsselung, Dateidown- und -upload, Dateisuche, Löschen der Spuren von unzähligen Windows Anwendungen, Platz schaffen durch Beseitigen überflüssiger Daten und vieles mehr.

Natürlich bringt ArchiCrypt Shredder auch zwei unterschiedliche Editoren, mit denen Sie Ihre eigenen Plug-ins und Pro-Scripte erstellen können.

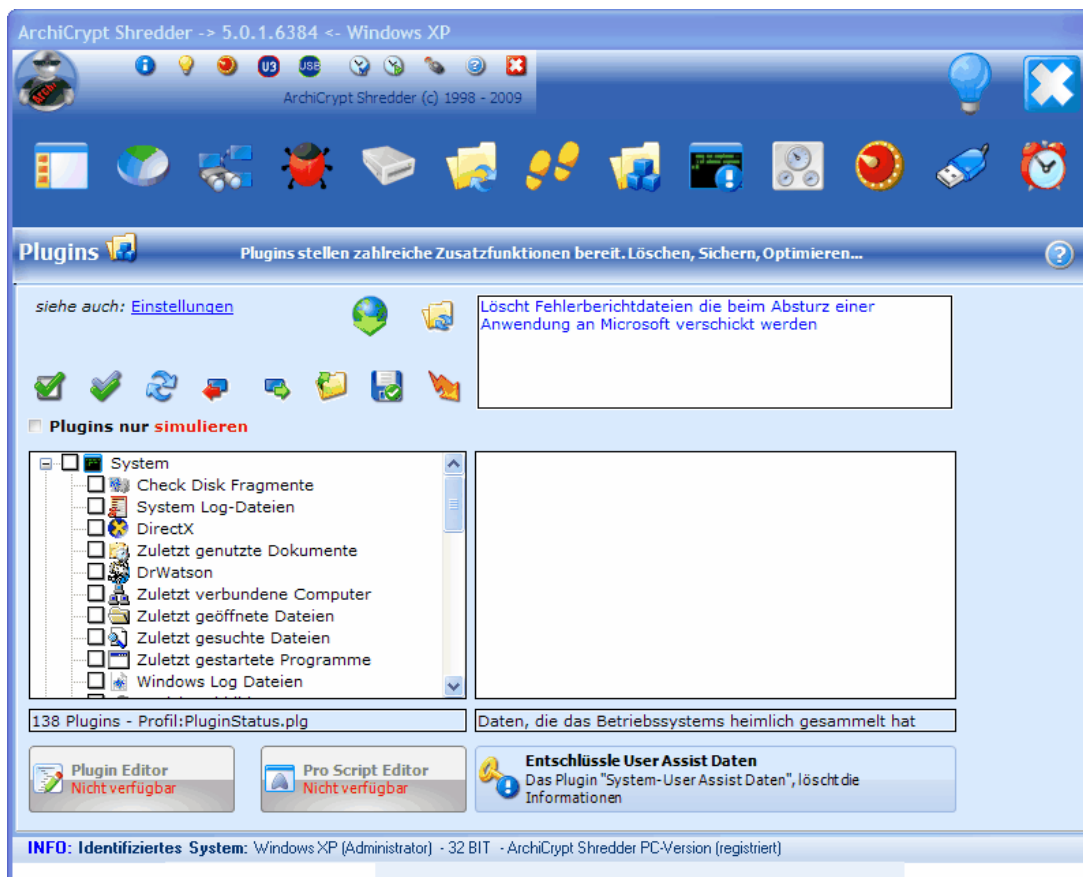
Die neusten Entwicklungen können Sie wie gewohnt unter www.ArchiCrypt.com einsehen.

Dipl.-Ing. Patric Remus

3.2 Neu in Version 5

[Zur History >>>](#)

Die Top Highlights



Moderne Nutzeroberfläche

Das bewährte Konzept der Unterteilung der Funktionen in verschiedene Kategorien wurde beibehalten. Nutzer älterer Versionen werden sich sofort zurechtfinden. An vielen Stellen werden Sie Veränderungen entdecken, die Ihnen die Arbeit mit ArchiCrypt Shredder jetzt noch einfacher machen.

Sie können Listen durch Eingabe von Wortfragmenten einschränken und rasch filtern, sich auf die Angaben der deutlich verbesserten Zeitabschätzung für zeitintensive Aufgaben verlassen, an vielen Stellen schneller auf integrierte Zusatzprogramme wie Aufgabenplaner und Plug-in Editoren zugreifen, insbesondere unter Windows Vista und Windows 7 schnell den ArchiCrypt Shredder mit Administratorrechten neu starten u.v.a.m.

Windows 7

Windows 7 stellt in vielerlei Hinsicht ganz besondere Anforderungen an Programme, die

sehr systemnah arbeiten. Große Teile des Shredders und viele Plug-ins mussten an diese neuen Konzepte und Anforderungen angepasst werden.

Google Chrome

Die neue Version von ArchiCrypt Shredder unterstützt erstmals den Browser Google Chrome. Neben dem normalen Löschen von Spuren die im Zusammenhang mit der Arbeit mit Google Chrome entstehen, bringt ArchiCrypt Shredder eine ganze Kategorie an Plug-ins mit, die die Spionagefunktionen des ansonsten gelungenen Browsers deaktivieren.

Plug-ins

Sie werden viele neue Plug-ins entdecken, die jetzt die Spuren von noch mehr Programmen sauber und bequem von Ihrem System entfernen. Neu ist auch die Funktion, mit der Sie sich via Download mit neuen Plug-ins versorgen (nur Vollversion) können. Eine der weitreichendsten Änderungen befindet sich ebenfalls bei den Plug-ins. Gänzlich unscheinbar finden Sie bei den Plug-ins jetzt die Rubrik Pro Scripte. Dahinter verbergen sich sehr leistungsfähige kleine Programme, mit denen Sie nahezu beliebige Aufgaben erledigen können. Die Vollversion von ArchiCrypt Shredder bringt ca. 130 Plug-ins mit, darunter 10 Pro-Scripte. Diese erledigen Aufgaben wie Backup, Verschlüsselung, Dateidown- und -upload, Dateisuche, Löschen der Spuren von unzähligen Windows Anwendungen, Platz schaffen durch Beseitigen überflüssiger Daten und vieles mehr.

Natürlich bringt ArchiCrypt Shredder auch zwei unterschiedliche Editoren, mit denen Sie, Vorwissen vorausgesetzt, Ihre eigenen Plug-ins und Pro Scripte erstellen können.

Noch mehr Platz schaffen und Ballast beseitigen

In der Kategorie Verzeichnisse finden Sie neben den alt bewährten Funktionen zum Beseitigen von unnützen Dateien aus dem **temporären Verzeichnis** und dem **Windows Prefetch** Ordner jetzt eine weitere Funktion die unter Umständen ordentlich Platz schafft.

Wir haben uns inzwischen alle an den Microsoft Patch Datei gewöhnt, an dem uns Microsoft mit Bug fixes für sein Betriebssystem versorgt. Den wenigsten ist wahrscheinlich bekannt, dass mit vielen Bug fixes Daten installiert werden, mit denen man den Bug fix im Fehlerfall wieder zurücknehmen kann. Sofern bei einem Updaten jedoch alles gut geht, brauchen wir diese Daten nicht mehr. ArchiCrypt Shredder kümmert sich mit seiner neuen **Hotfix Dateien** Funktion um diesen Umstand.

Auch bei den Plug-ins finden Sie unter System neue Funktionen, die ordentlich Platz schaffen können

- Check Disk Fragmente
- System Log-Dateien
- Windows Log Dateien
- Speicherabbilder
- und
- Windows Fehlerberichte.

Platz und Sicherheit

Mit dem Begriff "Alternativen Datenströme" können sicher nur wenige etwas

anfangen. Es handelt sich dabei um Bereiche, in denen, verborgen vor den Augen eines normalen Anwenders, beliebige Daten gespeichert werden können. Diese so genannten alternativen Datenströme belegen Platz und bieten aufgrund ihrer Eigenschaften Schadprogrammen (Viren/Trojanern) ideale Versteckmöglichkeiten. ArchiCrypt Shredder spürt solche Daten nicht nur auf, sondern kann sie anzeigen und natürlich sicher entfernen!

Mobile Nutzung von U3- und USB-Sticks

Wer ist heute nicht im Besitz eines USB- oder U3-Sticks, mit dem Daten von einem Rechner zum anderen transportiert werden. Da kommen die neuen Funktionen von ArchiCrypt Shredder genau richtig. Ab sofort können Sie sich mit der normalen PC-Version von ArchiCrypt Shredder eine Installation auf USB-Stick oder U3-Stick erzeugen, die Ihnen auch unterwegs sichere Löschfunktionen für Dateien, Surfspuren und Co. anbietet.

Steigerung der Geschwindigkeit

Die Löschfunktionen arbeiten gegenüber den Vorversionen um bis zu 30% schneller, ohne dass dabei Abstriche an der Sicherheit der eingesetzten Lösungsverfahren gemacht werden müssen.

Automatische Bereinigung der Quarantäne

Das der mächtige Duplikat Finder mehrfach vorhandene Dateien aufspürt, die man selbst niemals entdecken würde, ist sicher bekannt. Auch die Quarantäne Funktion, mit deren Hilfe man im Falle eines Falles ein Duplikat wieder herstellen kann, ist bekannt und beliebt. Musste man bisher Daten manuell aus der Quarantäne entfernen, kann man jetzt festlegen, nach wie vielen Tagen ArchiCrypt Shredder die Sicherungen automatisch aus der Quarantäne löschen soll.

Sichere Löschezonen

Noch immer gibt es kein anderes Löschprogramm, welches eine ähnlich ausgefeilte Funktion zum sicheren Löschen der Dateien anbietet, die nicht Sie, sondern das Betriebssystem oder andere Anwendungen löschen. Solche Löschoperationen finden tausendfach statt, wobei Sie als Anwender davon nichts mitbekommen und folglich auch nicht eingreifen können. Dateien, die so gelöscht wurden, können mit Recovery Software wieder hergestellt und ausgewertet werden. Die neuen Sicheren Löschezonen sind flexibler und mit nahezu allen Windows Anwendungen kompatibel und erlauben tiefe Einblicke in Vorgänge in Ihrem System.

Unzählige Verbesserungen

Integration von DBAN 2 zum Löschen der Betriebssystem Partition, Aufgaben-Planer zum einfachen erstellen von 1-Klick Löschaufgaben, Feedback und automatischer Neustart, falls ArchiCrypt für eine ausgewählte Funktion keine ausreichenden Rechte besitzt, vereinfachte Registrierung der Vollversion, u.a.m.

4 Allgemeine Informationen

4.1 Installationshinweise

Das Programm wird mit einer eigens entwickelten Installationsroutine geliefert, die Ihnen die Arbeit abnimmt. Die Installation erfolgt automatisch so, dass Sie für jeden Nutzer eingerichtet wird.

Achten Sie darauf, dass Sie unter den Betriebssystemen Windows XP, Windows Vista und Windows 7 **Administratorrechte** besitzen müssen.

Bei der Installation werden keine Systemdateien ersetzt oder geändert.

4.2 Systemvoraussetzungen

Um ArchiCrypt Shredder verwenden zu können, muss Ihr System folgende Voraussetzungen erfüllen:

Unterstützte Betriebssysteme

32 BIT und 64 BIT Versionen - Windows XP, Windows Vista, Windows 7

Minimale Systemanforderungen

Microsoft Windows XP

Bildschirmauflösung 800x600 mit 256 Farben

ca. 35 MB freier Festplattenplatz

Intel Pentium oder AMD K5 Prozessor mit mindestens 200 MHz

1024 MB RAM

CD-ROM oder DVD-ROM-Laufwerk

Empfohlene Systemkonfiguration

Microsoft Windows XP

Bildschirmauflösung 1024x768, true color

50 MB freier Festplattenplatz

2048 MB RAM

CD-ROM oder DVD-ROM-Laufwerk

Falls Sie ArchiCrypt Shredder unter **Windows Vista oder Windows 7** einsetzen möchten, sollten Sie sich unbedingt das Kapitel [ArchiCrypt Shredder unter Vista und Windows 7](#) ansehen.

➔ACHTUNG:

Zur Ausführung bestimmter Funktionen benötigen Sie **Administratorrechte**. Bestimmte Löschaufgaben können Sie insbesondere unter Windows Vista und Windows 7 ausschließlich mit Administratorrechten ausführen.

Systemvoraussetzungen für DBAN (Darik's Boot and Nuke)

Hardware

- DBAN arbeitet mit den meisten SCSI und IDE Festplatten zusammen.

- DBAN arbeitet mit allen 32-bit x86 Computern (Athlon, Pentium, und andere) mit mindestens 8 Megabyte Hauptspeicher zusammen.

Software

- DBAN unterstützt alle Microsoft Windows Plattformen und löscht Daten auf den Dateisystemen FAT, FAT32, VFAT, und NTFS.
 - MS-DOS, Windows 3.1
 - Windows 95, Windows 98, Windows ME
 - Windows NT 3.0, Windows NT 3.1, Windows NT 3.5, Windows NT 4.0
 - Windows 2000, Windows XP, Vista
- DBAN unterstützt alle Unix Systeme und zerstört Daten auf den Dateisystemen ReiserFS, EXT und UFS.
 - FreeBSD, NetBSD, OpenBSD
 - Linux
 - BeOS
 - QNX

4.3 ArchiCrypt Shredder unter Windows Vista und Windows 7

Eingeloggt als Administrator

Windows Vista und Windows 7 bieten mit der s.g. **Benutzerkontensteuerung** (UAC; User Access Control) ein Mittel an, welches Schadprogramme daran hindern soll, sich auf Ihrem System einzunisten und dort Schaden anzurichten.

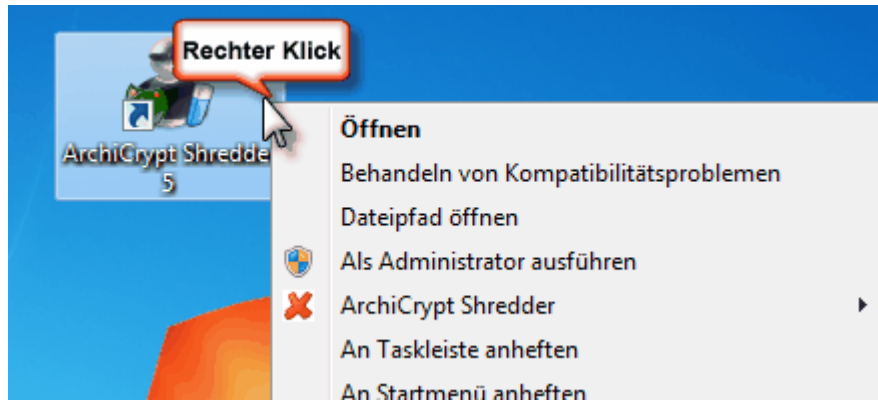
Ein Anteil dieser Benutzerkontensteuerung sorgt dafür, dass Programme selbst dann mit eingeschränkten Nutzerrechten ausgeführt werden, wenn Sie als Administrator eingeloggt sind. Als Hersteller von Software kann man sich dazu entschließen, die Software grundsätzlich mit Administratorrechten starten zu lassen. Eine Rückfrage beim Anwender erfolgt jedoch leider immer, auch wenn man die Software mit einem Digitalen Zertifikat signiert hat. Zudem ist es Programmen, die mit Administratorrechten gestartet werden müssen, nicht gestattet, als Autostart-Eintrag mit dem System zu starten. Auch hier erfolgt eine Rückfrage, bevor das Programm letztlich gestartet wird.

ArchiCrypt Shredder startet grundsätzlich mit eingeschränkten Nutzerrechten und versucht Sie, trotz der eingeschränkten Rechte, möglichst gut zu unterstützen. Auch ein Start über die Autostart-Funktion ist so möglich, insbesondere die oft genutzte Funktion zum automatischen Löschen von Surfspuren ist möglich.

Den Zugriff auf alle Funktionen des Shredders erhalten Sie nur dann, wenn der Shredder als Administrator ausgeführt wird.

So starten Sie ArchiCrypt Shredder als Administrator

Rechte Maustaste über dem Programm-Symbol des Shredders betätigen. Anschließend Als Administrator ausführen wählen.



Unter Windows Vista und Windows 7 finden Sie in der Titelleiste des Shredders ein Schildsymbol, falls der Shredder keine Administratorrechte besitzt. In diesem Fall genügt ein Klick auf das Schildsymbol um den Shredder mit Administratorrechten neu zu starten.



Löschen unter Vista und Windows 7

Vista/Windows 7 legt in einigen Versionen (Ultimate, Business, Enterprise Version bei Vista; zusätzlich bei Windows 7 auch in Home und Premium) s.g. **Schattenkopien** an. Schattenkopien sind Dateien, die Dateien in einem älteren Zustand repräsentieren. Wenn Sie zum Beispiel ein Worddokument speichern und plötzlich feststellen, dass Sie doch lieber wieder die Version von vor zwei Tagen möchten, können Sie über die Schattenkopien ggf. auf diese Sicherung zurückgreifen. Diese an sich nützliche Funktion steht leider in völligem Widerspruch zu unserer Absicht, Daten so zu löschen, dass sie nicht mehr wieder herzustellen sind. Es bleibt nur der Weg, die Schattenkopien zumindest kurzzeitig zu deaktivieren.

So deaktivieren Sie die Schattenkopie-Funktion

Vista: Gehen Sie zu **Systemsteuerung-System und Wartung**. Klicken Sie bei den Aufgaben links auf **Computerschutz**.

Windows 7: Gehen Sie zu **Systemsteuerung-System und Sicherheit - System**. Klicken Sie links auf **Erweiterte Systemeinstellungen** jetzt wechseln Sie bitte auf die Seite **Computerschutz**.



Im Dialog **Systemeigenschaften** wird die Registerseite **Computerschutz** angezeigt. Hier können Sie die Einstellungen für jedes Laufwerk ändern.

Welche Folgen hat das Deaktivieren der Schattenkopie-Funktion

Vorhandene Wiederherstellungspunkte und Schattenkopien gehen verloren. Der blockierte Speicherplatz wird durch das System freigegeben. Die Daten, die bisher in den Schattenkopien und Wiederherstellungspunkten vorhanden waren, sind nicht sicher gelöscht. Um solche Daten sicher zu löschen, müssen Sie z.B. mit dem Shredder den Freispeicher bereinigen. Einmal deaktiviert, werden keine Schattenkopien oder Wiederherstellungspunkte mehr erstellt.

Sie können auch das Plugin Volumenschattenkopie unter Tweak des Shredders nutzen und den zuständigen Systemdienst deaktivieren oder bei Bedarf aktivieren.

Unlöschbare Dateien

In Windows Vista und Windows 7 gibt es Dateien und Bereiche in der Registry, auf die man auch als Administrator keinen Zugriff hat. Hier helfen auch keine ausgefeilten Methoden des Shredders. Einzig das Booten von einem anderen Medium mit Zugriffsmöglichkeit auf NTFS könnte dies beheben. Dieser zunächst kritisch anmutende Umstand ist in der Praxis ohne Belang, da solche Dateien elementare Komponenten des Betriebssystems darstellen, nicht gelöscht werden dürfen und auch keine sensiblen Daten beinhalten.

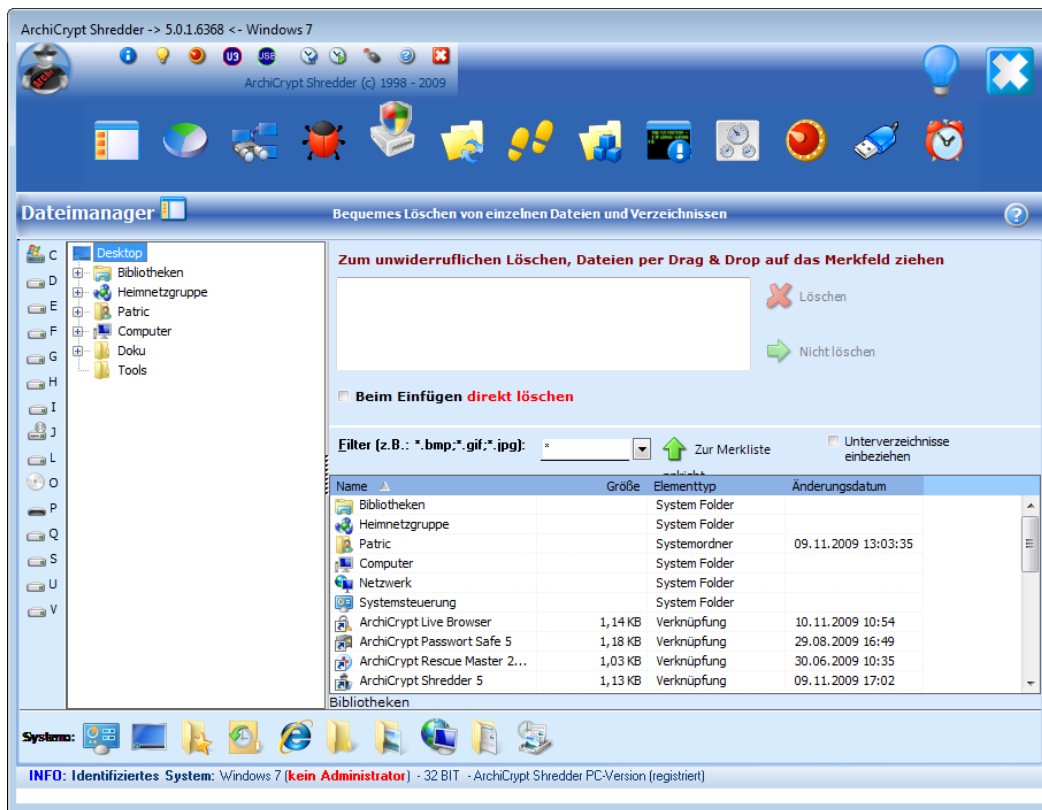
5 Bedienung ArchiCrypt Shredder

5.1 Überblick

Überblick



Mit **ArchiCrypt Shredder** befreien Sie Ihr Betriebssystem von unnötigem Ballast und löschen Sie Daten so, dass diese mit softwaretechnischen Mitteln nicht wieder hergestellt werden können.





➔ ACHTUNG: Um umfänglichen Zugriff auf die leistungsstärksten Funktionen zu erhalten, sollten Sie den Shredder mit **Administratorrechten ausführen!**



Die 9 Hauptkategorien

Alle Funktionen des Shredders sind zentral aus einer gemeinsamen Oberfläche heraus aufrufbar. Der Shredder bietet die folgenden **Hauptkategorien** an:

Hauptkategorien	Beschreibung
 Dateimanager	Verwalten Sie Ihre Dateien und Ordner mit dem Dateimanager. Ziehen Sie Dateien, die sicher gelöscht werden sollen, einfach per Drag & Drop auf das Merkfeld. Greifen Sie rasch auf wichtige Komponenten der Systemsteuerung zu.
 Laufwerksbelegung	Wer kennt das Problem nicht. Gleich wie groß die Festplatte in Ihrem Computer ist, der verfügbare Speicherplatz schwindet zusehends. Lassen Sie ArchiCrypt Shredder Ihre Laufwerke analysieren und die wahren Platzfresser aufspüren. Sowohl grafisch als auch in einer TOP 100 Liste finden Sie die Dateien und Ordner, die den meisten Platz belegen.

 <p>Duplikat Finder</p>	<p>Mit der Zeit sammeln sich auf einem Windowssystem immer mehr Dateien an. Dabei handelt es sich relativ häufig um Duplikate, die nicht nötig sind und unnötig Platz belegen. ArchiCrypt Shredder spürt diese Duplikate auf und unterstützt Sie dabei, die richtige Datei zu löschen. Um Sie im Falle eines Falles zu unterstützen, legt ArchiCrypt Shredder die Duplikate vor dem Löschen in der Quarantäne ab, aus der man sie bei Bedarf wieder einspielen kann.</p>
 <p>ADS Scanner</p>	<p>Auf Laufwerken mit dem NTFS Dateisystem kann man an beliebige Dateien so genannte Alternative Datenströme (Alternate Data Streams; ADS) anhängen. Diese Anhänge belegen Platz und werden sehr häufig missbraucht um Viren und Trojaner auf Ihrem System zu verstecken. Der Shredder spürt diese Daten auf, kann die Inhalte anzeigen und selbstverständlich auch löschen.</p>
 <p>Datenträger</p>	<p>Bereiche und Strukturen Hier können Sie den vermeintlich freien Bereich (Freispeicher) Ihrer Festplatten säubern, s.g. Clustertips und Dateinamen bereinigen.</p> <p>Löschen von Datenpartitionen Oft möchte man die Daten eines ganzen Laufwerks oder einer kompletten Festplatte sicher löschen. Es ist ein Irrglaube, man könne durch einfaches Formatieren die Daten eines Laufwerks vernichten. Dem ist definitiv nicht so! Nutzen Sie die spezielle Funktion des Shredders um solche Laufwerke komplett zu bereinigen.</p> <p>Boot CD - Löschen des Betriebssystems Die Partition auf der Ihr Betriebssystem gespeichert ist, können Sie nicht komplett sicher löschen. Schließlich benötigt ArchiCrypt Shredder das Betriebssystem um laufen zu können. Hier muss eine andere Lösung her. Mit DBAN bietet Ihnen der Shredder an, ein bootbares Medium zu erstellen, mit dem Sie sogar Ihre Betriebssystempartition sicher löschen können.</p> <p>Hartnäckige Dateien Einige Dateien sind derart hartnäckig, dass sie im laufenden Betrieb nicht gelöscht werden können. Der Shredder merkt sich solche Dateien und löscht sie beim nächsten Start Ihres Rechners.</p>
 <p>Verzeichnis se</p>	<p>Haben Sie bestimmte Verzeichnisse in denen Sie ständig Daten ablegen, die nach kurzer Zeit nicht mehr von Bedeutung sind? Schwindet der Speicherplatz weil Anwendungen große Datenmengen im temporären Verzeichnis ablegen und nicht wieder löschen. Dann können Sie solche Verzeichnisse hier festlegen und, falls gewünscht, sogar zeitgesteuert oder automatisch beim Beenden des Browsers bereinigen lassen.</p>

 <p>Online-Spuren</p>	<p>Browser zeichnen nahezu jede Aktion im Internet akribisch auf und speichern Texte und Bilder in einem s.g. Cache. Einige der Browser bieten oft in verschlungenen Untermenüs an, dass man diese Dateien löschen kann. Gelegentlich fehlt diese Funktion ganz. Immer werden die Daten bei diesen Aktionen jedoch mit unsicheren Betriebssystemmitteln gelöscht. Mit entsprechender Software kommen diese Daten rasch wieder an das Tageslicht. Der Shredder fasst die verborgenen Funktionen zentral zusammen und löscht die Daten im Gegensatz zu den Browsern sicher.</p>
 <p>Plugins</p>	<p>Das Betriebssystem und viele Anwendungen sammeln ohne Unterlass Informationen und speichern diese ab. Gegen diese Sammelwut ziehen Sie ab sofort mit zahlreichen Plugins zu Felde. Dabei gibt es neben reinen Löschplugins auch Plugins zum sichern von wichtigen Daten und direkten Manipulieren von Systemeinstellungen. Mit Hilfe des Plugin Editors können Sie die Palette der Plugins beliebig erweitern. Eine besondere Sorte von Plugins, die so genannten Pro Scripte stellen richtige kleine Anwendungen dar, die entsprechend leistungsfähig sind. Für Kenner und Fortgeschrittene bringt der Shredder sogar eine komplette Entwicklungsumgebung mit, mit der Sie sich selbst kleine Tools für den Shredder erstellen können.</p>
 <p>Sichere Löschezonen</p>	<p>Viele Anwendungen, darunter Browser, Office-, Grafik- und Multimediaanwendungen erstellen ununterbrochen und, ohne dass Sie davon etwas mitbekommen, Daten und löschen diese wieder. Das Löschen erfolgt jedoch auch hier leider immer mit den unsicheren Betriebssystemmitteln. Die Daten können also wieder hergestellt werden. Sichere Löschezonen sind Orte auf Ihrem Rechner, an denen der Shredder genau diese unsicheren Löschoperationen abfängt und Daten sicher löscht. Lassen Sie sich vom Shredder Sichere Löschezonen vorschlagen oder definieren Sie eigene.</p>
 <p>Mobile Nutzung</p>	<p>Mit Hilfe der PC-Version des Shredders können Sie sich eine spezielle Version auf einem USB-Stick erzeugen lassen. Ihnen stehen so auch unterwegs die wesentlichen Funktionen des Shredders an jedem Rechner zur Verfügung. Falls Sie einen speziellen U3-Stick Ihr eigen nennen, können Sie sich ein Installationspaket für Ihren Stick erzeugen lassen und den Shredder ab Installation ebenfalls bequem an jedem Rechner nutzen.</p>
 <p>Aufgaben-Planer</p>	<p>Manchmal ist es sinnvoll, bestimmte Löschaufgaben automatisch zu einer bestimmten Zeit ausführen zu lassen. Mit Hilfe des Aufgaben-Planers können Sie solche Löschaufgaben definieren und zu bestimmten Zeiten auch ausführen lassen. Als besonders bequem erweist sich hier die Möglichkeit, solche Löschaufgaben als s.g. 1-Klick Löschaufgabe anzulegen. Wie der Name vermuten lässt, genügt ab dann ein Klick auf die entsprechende 1-Klick Löschaufgabe und der Shredder führt die festgelegten Aufgaben aus.</p>

Kontextmenü

ArchiCrypt Shredder bietet Ihnen system weit ein Kontextmenü an, mit dem Sie zum Beispiel auch im Windows Explorer Dateien sicher löschen oder sicher an einen anderen Speicherort verschieben können.

Über die [gemeinsame Bedienoberfläche](#) können Sie die einzelnen Kategorien aufrufen.

5.2 Gemeinsame Bedienoberfläche

Die Bedienoberfläche

Die einzelnen Funktionen des Shredders können Sie bequem aus einer gemeinsamen Oberfläche heraus aufrufen. Dabei sind die einzelnen **Funktionen** in verschiedene **Kategorien** eingeteilt und so einfacher zu finden.

Die einzelnen **Kategorien** können Sie in der oberen Leiste des Fensters auswählen. Die entsprechende Funktion wird durch Klick auf die Schaltfläche aufgerufen.

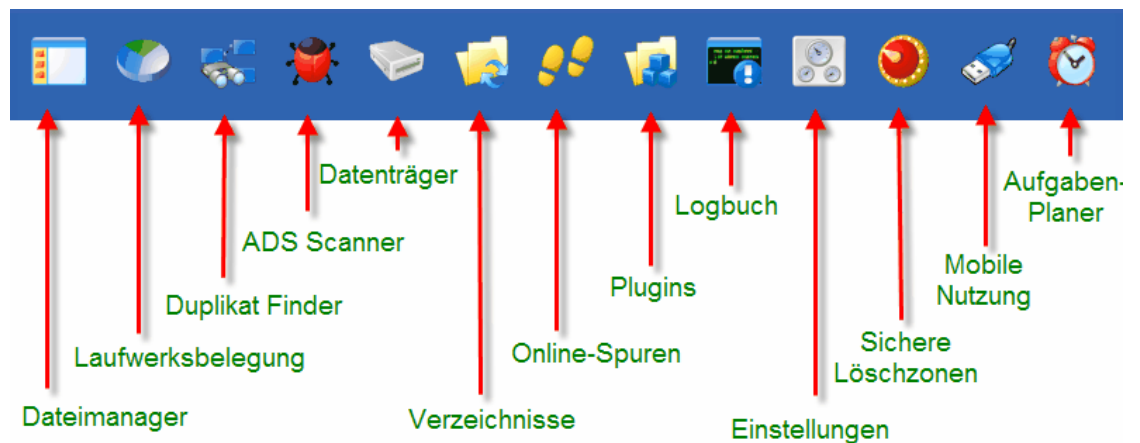


Mini-Menüleiste



Kategorien

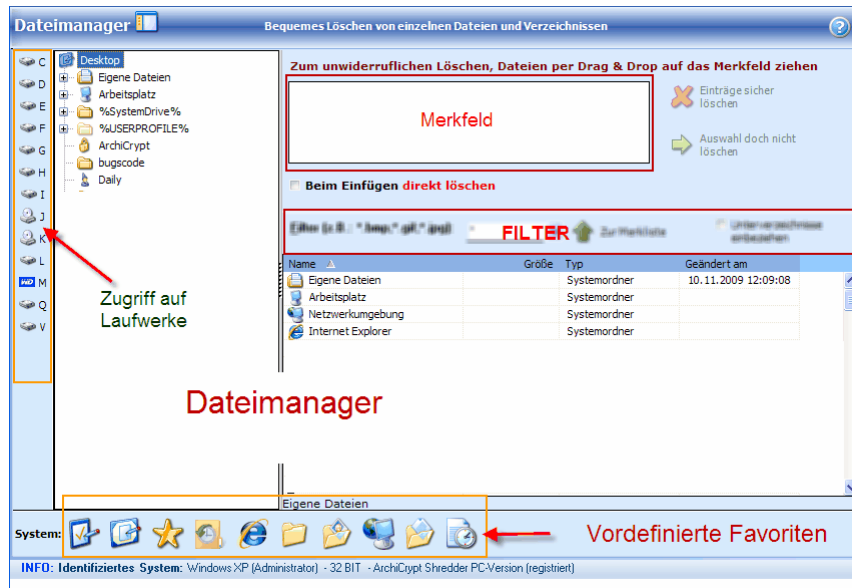
Sie können die Bezeichner mit der Funktion "Text auf Schaltflächen zeigen" (Mini-Menüleiste) dauerhaft ein- und ausblenden. Es genügt jedoch, mit der Maus über ein Element zu fahren, um eine Beschreibung zu sehen.



5.3 Dateimanager

Der Dateimanager

Verwalten Sie Ihre Dateien und Ordner mit dem **Dateimanager**. Ziehen Sie Dateien, die sicher gelöscht werden sollen, einfach per Drag & Drop auf das **Merkfeld**. Greifen Sie über [vordefinierte Favoriten](#) rasch auf wichtige Komponenten der Systemsteuerung zu.



So löschen Sie Dateien und Verzeichnisse mit dem Dateimanager von ArchiCrypt Shredder

Ziehen Sie Dateien und oder Verzeichnisse aus der Datei- oder Verzeichnisansicht des Dateimanagers bei gedrückter linker Maustaste über das **Merkfeld** und lassen Sie die Maustaste los.

Falls Sie die Option Beim Einfügen direkt löschen gewählt haben, beginnt ArchiCrypt Shredder sofort damit, die gewählten Dateien zu shreddern. Falls die Option nicht ausgewählt wurde, werden alle Dateien zunächst im Merkfeld gesammelt. Wenn Sie nur ganz bestimmte Dateitypen in das Merkfeld übernehmen möchten, nutzen Sie die Filterfunktion. Navigieren Sie dazu zunächst in das Verzeichnis, in welchem sich die zu löschenden Dateien befinden. Geben Sie jetzt die Dateitypen als Filter ein, die Sie löschen möchten. Falls mehrere Dateitypen berücksichtigt werden sollen, trennen Sie die einzelnen Einträge mit einem Strichpunkt. Nachdem Sie den Filter festgelegt haben, betätigen Sie die Schaltfläche Zur Merkliste. Wenn Sie die Auswahl Unterverzeichnisse einbeziehen gewählt haben, wird in allen aktuell sichtbaren Verzeichnissen und deren Unterverzeichnissen nach den Dateien gesucht, die die Filterkriterien erfüllen.

Beispiel:

1. Sie möchten in einem Verzeichnis alle Microsoft Word- und Excelldokumente löschen.
Geben Sie dazu als Filter *.doc;*.xls ein.
2. Sie möchten alle Microsoft Worddokumente löschen, deren Dateiname den Begriff

Finanzen enthält. Geben Sie dazu als Filter *Finanzen*.doc ein.

Falls Sie Verzeichnisse über das Merkfeld ziehen, werden alle darin enthaltenen Dateien eingefügt, also auch alle Dateien in eventuell vorhandenen Unterverzeichnissen. Als Funktionen stehen Ihnen das "Einträge sicher löschen" zur Verfügung, durch dessen Aufruf alle im Merkfeld aufgelisteten Dateien unwiderruflich gelöscht werden.

Sind im Merkfeld Dateien enthalten, welche Sie nicht löschen möchten, markieren Sie diese mit der linken Maustaste und Betätigen die Schaltfläche "Auswahl doch nicht löschen". Mehrere Dateien können Sie leicht auswählen, indem Sie die linke Maustaste gedrückt halten, und die Auswahl auf die gewünschten Dateien ausweiten. Falls Sie mehrere Dateien auswählen möchten, die nicht unmittelbar untereinander aufgeführt sind, halten Sie die <STRG> Taste während des Auswahlvorganges gedrückt.

Die Art und Weise des Löschvorganges legen Sie mit den Einstellungen "[Sicherheit](#)" der Kategorie [Einstellungen](#) fest.

Der Fortschritt der aktuellen Aktion wird Ihnen in der Statusleiste am unteren Rand angezeigt. Während des Löschvorganges sollten Sie keine weiteren Funktionen ausführen. Möchten Sie den Vorgang abbrechen, betätigen Sie die "Abbruch" Schaltfläche in der Statusleiste.



TIPP: Wenn Sie alle Dateien die aktuell im Merkfeld aufgelistet sind, nicht löschen möchten, dann klicken Sie doppelt auf das Merkfeld und betätigen die Schaltfläche Auswahl doch nicht löschen.

Vordefinierte Favoriten

Mit den [vordefinierten Favoriten](#) können Sie rasch auf wichtige Ordner oder Funktionen zugreifen.

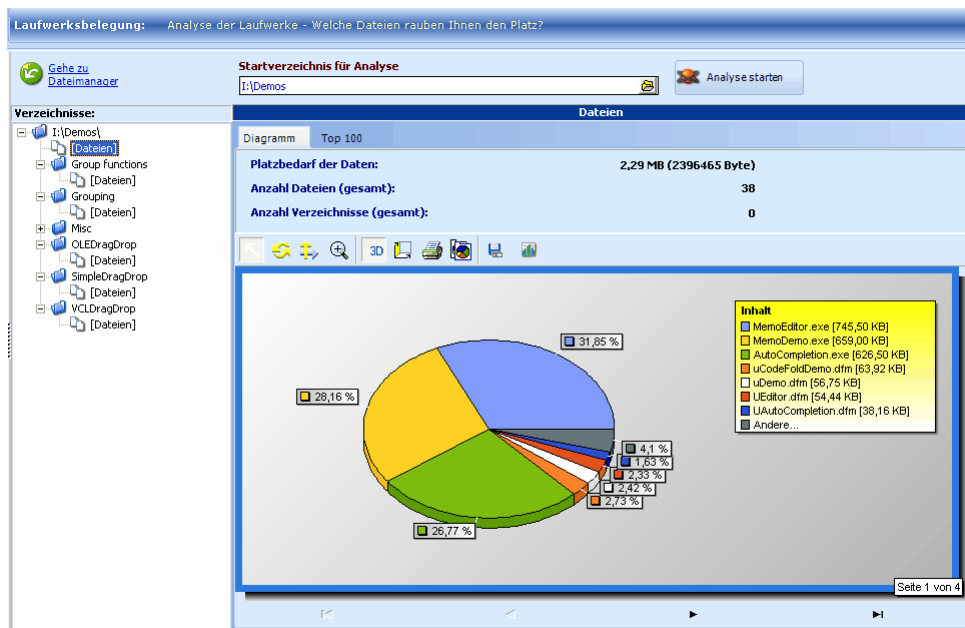
Die Funktionen von links beginnend sind:

- Inhalt der Systemsteuerung
- Inhalt des Desktops wird angezeigt
- Inhalt der Favoriten (Betriebssystem) wird angezeigt
- Verlauf (Internet Explorer) wird angezeigt
- Internet Explorer wird aufgerufen
- Inhalt des Ordners "Anwendungsdaten" wird angezeigt
- Inhalt des Ordners "Eigene Bilder" wird angezeigt
- Netzwerkumgebung
- Inhalt des Ordners "Eigene Dateien" wird angezeigt
- Zuletzt genutzte Dokumente werden angezeigt

5.4 Laufwerksbelegung

Die Laufwerksbelegung

Wer kennt das Problem nicht. Gleich wie groß die Festplatte in Ihrem Computer ist, der verfügbare Speicherplatz schwindet zusehends. Lassen Sie ArchiCrypt Shredder Ihre Laufwerke analysieren und die wahren Platzfresser aufspüren. Sowohl grafisch als auch in einer [TOP 100](#) Liste finden Sie die Dateien und Ordner, die den meisten Platz belegen.



Die Analyse

Um ein Laufwerk oder ein Verzeichnis zu analysieren haben Sie zwei Möglichkeiten:

1. Rufen Sie im Dateimanager des Shredders das Kontextmenü eines beliebigen Verzeichnisses oder Laufwerks auf (mit rechter Maustaste anklicken). Wählen Sie den Eintrag **Analysiere Verzeichnis...**. Die Analyse startet sofort.
2. Geben Sie das zu untersuchende Verzeichnis manuell in das Feld Startverzeichnis für Analyse ein, oder klicken Sie auf das kleine Ordnersymbol im Eingabefeld selbst um im Dialog ein Verzeichnis auswählen zu können. Betätigen Sie die Eingabetaste oder klicken Sie auf die Schaltfläche **Analyse starten**.

Die 3 Phasen der Analyse

In einem ersten Schritt ermittelt ArchiCrypt Shredder alle zu untersuchenden Verzeichnisse. In Phase 2 werden alle Dateien in diesen Verzeichnissen untersucht. Abschließend wird in Phase 3 die TOP 100 Liste erzeugt.

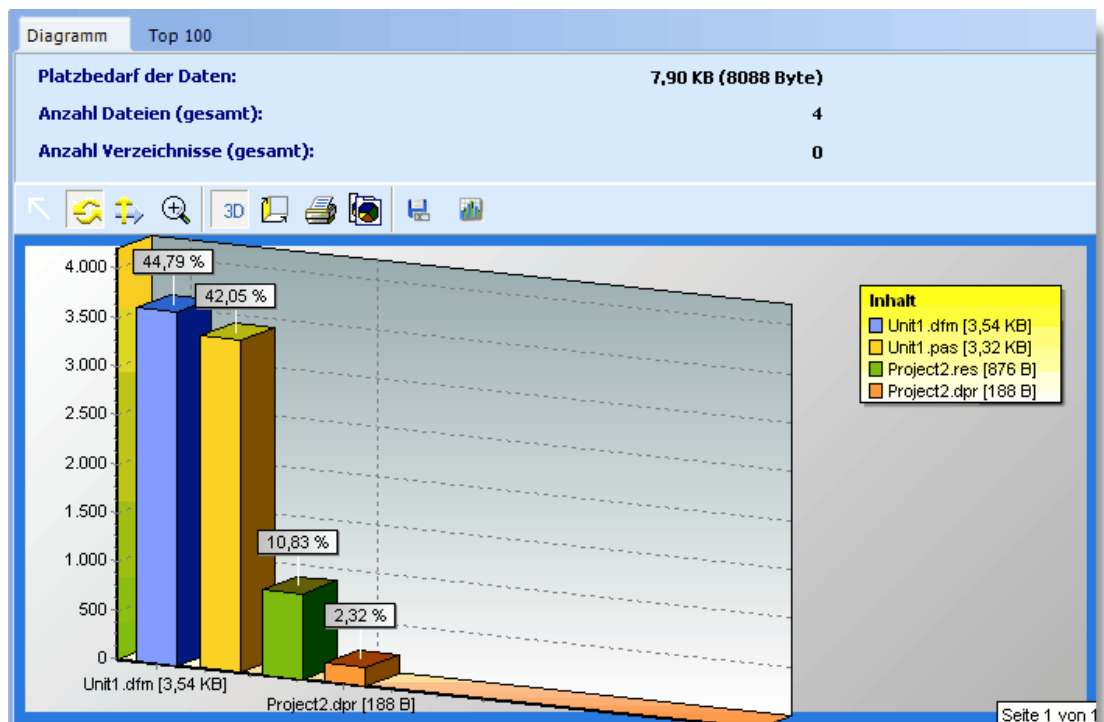
Das Diagramm

Nachdem ArchiCrypt Shredder die Analyse beendet hat, werden die Verzeichnisse links dargestellt. Sie können die Verzeichnisse anwählen wie in einem Dateimanager. Statt in der **Verzeichnisanzeige** Ordner auszuwählen, können Sie direkt auf ein Element der Grafik klicken. Bei dem Element muss es sich um ein Verzeichnis handeln.



TIPP: Wenn Sie einen Ordner mit der rechten Maustaste auswählen, können Sie im Kontextmenü den Eintrag **Zeige in Dateimanager** aufrufen um zum Dateimanager zu wechseln und dort zum entsprechenden Ordner zu wechseln.

Wenn Sie einen Ordner anwählen, dann wird Ihnen eine Grafik angezeigt, die sehr anschaulich zeigt, welche Unterordner oder Dateien den Löwenanteil am Platzbedarf inne haben.



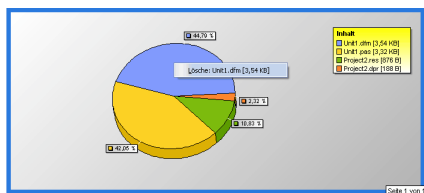
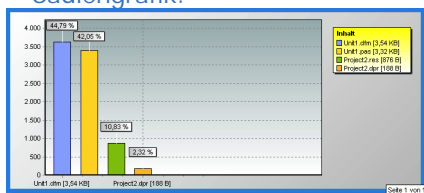
Im oberen Bereich sehen Sie, wie viel Platz enthaltene Ordner bzw. Dateien belegen und, wie viele Dateien und wie viele Ordner enthalten sind.

Anpassen der grafischen Darstellung

Oberhalb der Grafik befindet sich die Menüleiste, die Ihnen von links beginnend folgende

Funktionen zur Verfügung stellt:

- **Normal:** Doppelklick auf ein Element welches ein Verzeichnis repräsentiert, wechselt in dieses Verzeichnis. Rechtsklick auf ein Element öffnet das Kontextmenü.
- **Drehen:** Klicken Sie mit der linken Maustaste in die Grafik und drehen Sie die Grafik bei gedrückter linker Maustaste in die gewünschte Richtung
- **Verschieben:** Klicken Sie mit der linken Maustaste in die Grafik und verschieben Sie die Grafik bei gedrückter linker Maustaste an die gewünschte Position.
- **Zoom:** Bewegen Sie die Maus bei gedrückter linker Maustaste innerhalb der Grafik nach oben um in die Grafik zu zoomen bzw. nach unten, um heraus zu zoomen.
- **3D:** Sie können die 3D Ansicht ein oder ausschalten.
- **Tiefe:** Ändern Sie die Tiefe, indem Sie die Maus bei gedrückter linker Maustaste nach oben oder unten bewegen.
- **Drucken:** Drucken Sie die Grafik aus.
- **Kopieren:** Kopieren Sie die aktuelle Grafik in die Zwischenablage und verwenden Sie sie in beliebigen Anwendungen.
- **Speichern:** Speichern Sie die aktuelle Grafik als Bitmap, PNG, JPEG oder GIF Datei ab.
- **Kuchen-Säulengrafik:** Wechseln Sie zwischen den Darstellungen Kuchen und Säulengrafik.



So löschen Sie Dateien und Verzeichnisse

Wenn Sie einen Platzfresser identifiziert haben und diesen löschen möchten, haben Sie zum einen die Möglichkeit in der Verzeichnisanzeige links ein Verzeichnis mit der rechten Maustaste anzuklicken und das Menü "Zeige in Dateimanager" aufzurufen. Im Dateimanager löschen Sie die Datei dann in gewohnter Weise. Zum anderen können Sie mit der rechten Maustaste auf ein Element in der Grafik klicken, um im Kontextmenü die Funktion Lösche: "Name des Elements" aufzurufen und die Datei direkt zu löschen.

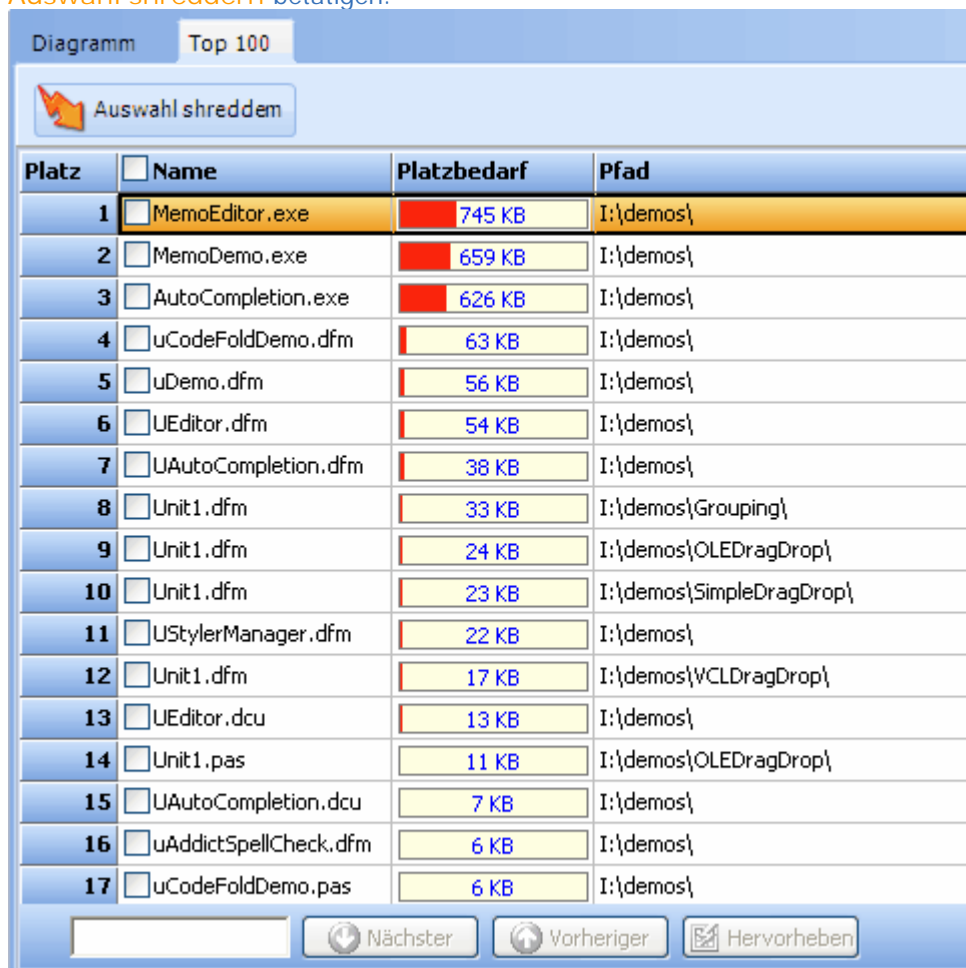
➡ **Anm.:** Das Löschen erfolgt mit den unter [Einstellungen-Sicherheit](#) festgelegten Methoden.

➡ **Warnung:** Sie können grundsätzlich jede Datei auswählen und löschen. Bitte achten Sie darauf, dass Sie ausschließlich Dateien löschen, von denen Sie sicher wissen, dass sie nicht mehr benötigt werden. Dateien, bei denen Sie zweifeln, sollten Sie nie löschen.

TOP 100 Liste

Die Datei mit dem größten Platzbedarf wird Ihnen an Position 1 angezeigt. Setzen Sie ein

Häkchen bei den Dateien, die Sie löschen möchten. Um alle Dateien an oder abzuwählen, klicken Sie bitte in der Spaltenüberschrift auf das Kästchen. Um einen Eintrag aus der Liste zu entfernen oder die Liste zu leeren, rufen Sie das Kontextmenü mit der rechten Maustaste über der Liste auf. Gelöscht werden die ausgewählten Einträge erst dann, wenn Sie die Schaltfläche **Auswahl shreddern** betätigen.



Wenn Sie eine bestimmte Datei suchen, geben Sie im Feld unterhalb der Tabelle Teile des Namens ein. Sie können zu den Treffern springen und oder sich die Treffer hervorheben lassen.

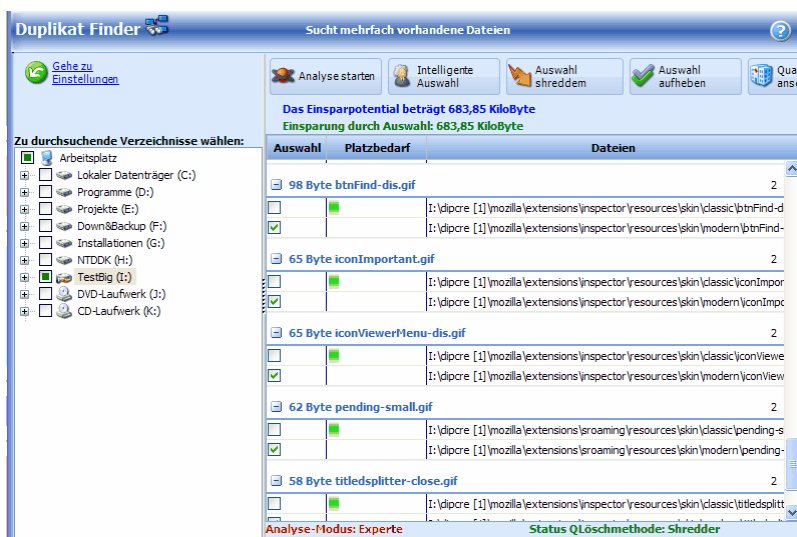
➔HINWEIS: ArchiCrypt Shredder löscht prinzipiell jede Datei, die gelöscht werden kann. Da man in der TOP 100 Liste leicht geneigt ist, alle Dateien auszuwählen und zu löschen, erscheint eine Warnung, wenn es sich um eine für den Betrieb Ihres Rechners mutmaßlich wichtige Datei handelt. Falls Sie sich bei einer Datei nicht sicher sind, löschen Sie diese NICHT!

5.5 Duplikat Finder

5.5.1 Analyse

Duplikat Finder - Analyse

Mit der Zeit sammeln sich auf einem Windows System immer mehr Dateien an. Dabei handelt es sich relativ häufig um **Duplikate** (Dateien, die mehrfach auf Ihrem System gespeichert sind), die nicht nötig sind und unnötig Platz belegen. ArchiCrypt Shredder spürt diese Duplikate auf und unterstützt Sie dabei, die richtige Datei zu löschen. Auch im Fall eines Falles lässt ArchiCrypt Shredder Sie nicht im Stich. Duplikate werden auf Wunsch zunächst in einer **Quarantäne** zwischengespeichert und können von dort bei Bedarf wieder zurückgespielt werden.



So finden Sie Duplikate

Der Duplikat Finder kennt einen Anfänger-, Fortgeschrittenen-, Profi- und nutzerdefinierten Analyse-Modus. Den **Analyse-Modus** können Sie in den [Einstellungen-Duplikat Finder](#) ändern.



Anm.: Zu den Einstellungen für den Duplikat Finder wechseln Sie am schnellsten, indem Sie die Schaltfläche [Gehe zu Einstellungen](#) betätigen. Der Modus wird unterhalb der Tabelle angezeigt. Die Modi unterscheiden sich darin,

welche Dateitypen in die Untersuchung mit einbezogen werden. Der Anfängermodus beschränkt sich zum Beispiel auf reine Datendateien, deren Beseitigung Ihr System nicht instabil machen kann.

Wählen Sie links das zu analysierende Laufwerk oder Verzeichnis aus, indem Sie ein Häkchen setzen (Sie können auch mehrere Laufwerke und Verzeichnisse wählen). Starten Sie die Analyse anschließend mit der Schaltfläche **Analyse starten**. Alle Dateien in den gewählten Verzeichnissen und Unterverzeichnissen werden jetzt analysiert.

Die 2 Phasen der Analyse

Im ersten Schritt sammelt ArchiCrypt Shredder die potentiellen Duplikate. In einem zweiten Schritt werden die in Frage kommenden Dateien dann genauer untersucht. Das Ergebnis der Analyse erhalten Sie in einer **Tabelle**. Duplikate, die den meisten Platz belegen, sind in dieser Tabelle weiter oben zu finden.



TIPP: Deaktivieren Sie in den Einstellungen das Häkchen bei Dateien sind gleich, wenn sie in Inhalt UND Namen übereinstimmen um auch die Duplikate zu finden, die zwar inhaltlich identisch sind, jedoch anders benannt wurden.

Welche Datei soll ich löschen?

Es ist nicht ganz einfach, zu entscheiden, welche der Dateien man löschen soll. Bei Datendateien wie z.B. Word- und Grafik-Dokumenten ist dies noch relativ leicht. Sie selbst wissen, wie Sie die Daten auf Ihrer Festplatte organisiert haben. Schwieriger wird es bei ausgewähltem Profi-Modus, der auch Anwendungen, Services und Treiber auflistet, die das Betriebssystem zwingend benötigt. Hier finden Sie in der Funktion Intelligente Auswahl eine Hilfe. Die Funktion prüft, ob es sich bei der Datei zum Beispiel um eine Systemdatei handelt, oder die Datei in einem für das System oder Anwendungen wichtigen Verzeichnis abgelegt ist. Insgesamt sollten Sie grundsätzlich die Quarantäne aktivieren. Hier können Sie die Duplikate notfalls wieder zurückspielen. Das Löschen aus Systemverzeichnissen sollten Sie unterlassen!

So löschen Sie Duplikate

Nachdem die Analyse abgeschlossen ist und Sie die zu löschenden Dateien gewählt haben, können Sie die überflüssigen Dateien shreddern (Auswahl shreddern). Ob die Dateien sicher gelöscht werden (Löschmethode Shredder) oder aber mit Systemmitteln (Löschmethode System) können Sie in den Einstellungen festlegen. Die Dateien werden bei aktivierter Quarantäne zunächst als Kopie dort abgelegt und erst dann gelöscht.

Was tun, wenn Anwendungen nach der Entfernung eines Duplikates nicht mehr laufen?

Insbesondere der Analyse Modus Profi, ggf. auch der nutzerdefinierte Modus, meldet auch doppelt vorhandene Anwendungen, Systembibliotheken, Treiber etc. Hier kann es in seltenen Fällen vorkommen, dass genau die Datei (das Duplikat) an der falschen Stelle gelöscht wurde. Falls Sie, wie empfohlen und voreingestellt, die Quarantäne aktiviert haben, können Sie die entsprechenden Daten (Quarantäne ansehen) wieder zurückspielen.



WICHTIG: Wenn Sie die Quarantäne aktiviert haben, belegen die darin abgelegten Dateien natürlich weiterhin Speicherplatz. Wenn Ihr System nach dem Beseitigen der Duplikate ohne Probleme läuft, sollten Sie die Quarantäne leeren und damit den Speicherplatz freigeben. In den Einstellungen zum Duplikat Finder können Sie festlegen, nach wie vielen Tagen Einträge automatisch aus der Quarantäne gelöscht werden sollen.

Wie kann ich bestimmte Dateien oder Verzeichnisse von der Analyse ausnehmen?

Nach abgeschlossener Analyse können Sie Einträge mit der rechten Maustaste auswählen und im Kontextmenü die Datei oder das Verzeichnis in die Liste zu ignorierender Dateien/ Verzeichnisse übertragen. Alternativ können Sie in den [Einstellungen](#) manuell Objekte hinzufügen.

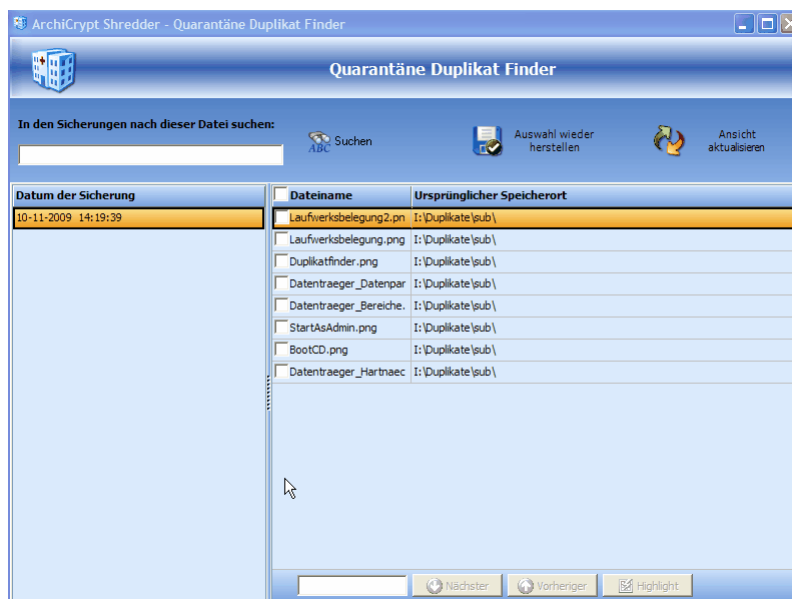
5.5.2 Quarantäne

Duplikat Finder - Quarantäne

Die **Quarantäne** bietet Ihnen eine bequeme Möglichkeit, Dateien die Sie mit dem Duplikat Finder von Ihrem System entfernt haben, wieder herzustellen.

So stellen Sie eine Datei aus der Quarantäne wieder her

Links sehen Sie verschiedene Sicherungen, die nach dem Datum geordnet sind (Datum der Sicherung). Wählen Sie einen Eintrag aus, um rechts in der Tabelle die in der Sicherung enthaltenen Dateien zu sehen. Sie können alle in einer Sicherung enthaltenen Dateien auswählen, indem Sie in der Spaltenüberschrift Dateiname ein Häkchen setzen. Das Entfernen des Häkchens entfernt die Häkchen bei allen Dateien. Einzelne Dateien wählen Sie aus, indem Sie bei der Datei ein Häkchen setzen. Wenn Sie Ihre Auswahl getroffen haben, betätigen Sie die Schaltfläche **Auswahl wieder herstellen**. Die Dateien werden jetzt an Ihren ursprünglichen Ort verschoben und aus der Quarantäne entfernt.



So finden Sie eine bestimmte Datei in der Quarantäne

Geben Sie den Dateinamen oder einen Teil davon in das Eingabefeld **In den Sicherungen nach dieser Datei suchen** ein und betätigen Sie die Suchen Schaltfläche. Falls Sie in einer bestimmten Sicherung suchen möchten, geben Sie den Begriff in das Suchfeld unterhalb der Tabelle ein. Mit den Schaltflächen **Nächster** und **Vorheriger**, wechseln Sie zwischen ggf. mehreren Fundstellen. Die Funktion **Highlight** hebt die gefundenen Stellen in der Tabelle hervor.

So entfernen Sie Dateien aus der Quarantäne

Insbesondere dann, wenn Ihr System nach dem Entfernen der Duplikate einwandfrei arbeitet, sollten Sie den Speicherplatz endgültig freigeben. Dazu können Sie entweder die komplette Sicherung oder einzelne Dateien entfernen. Wählen Sie dazu die Sicherung oder die Datei mit der linken Maustaste aus. Im Kontextmenü können Sie jetzt die Funktion **Entferne aus Quarantäne** aufrufen. Je nach **Einstellung** im Shredder werden die Dateien jetzt sicher gelöscht oder mit Systemmitteln von Ihrem Rechner beseitigt.



TIPP : *In ArchiCrypt Shredder können Sie unter **Einstellungen-Duplikat Finder** festlegen, dass Einträge nach einer bestimmten Zeit automatisch aus der Quarantäne entfernt werden.*

5.6 ADS Scanner

ADS Scanner - Analyse

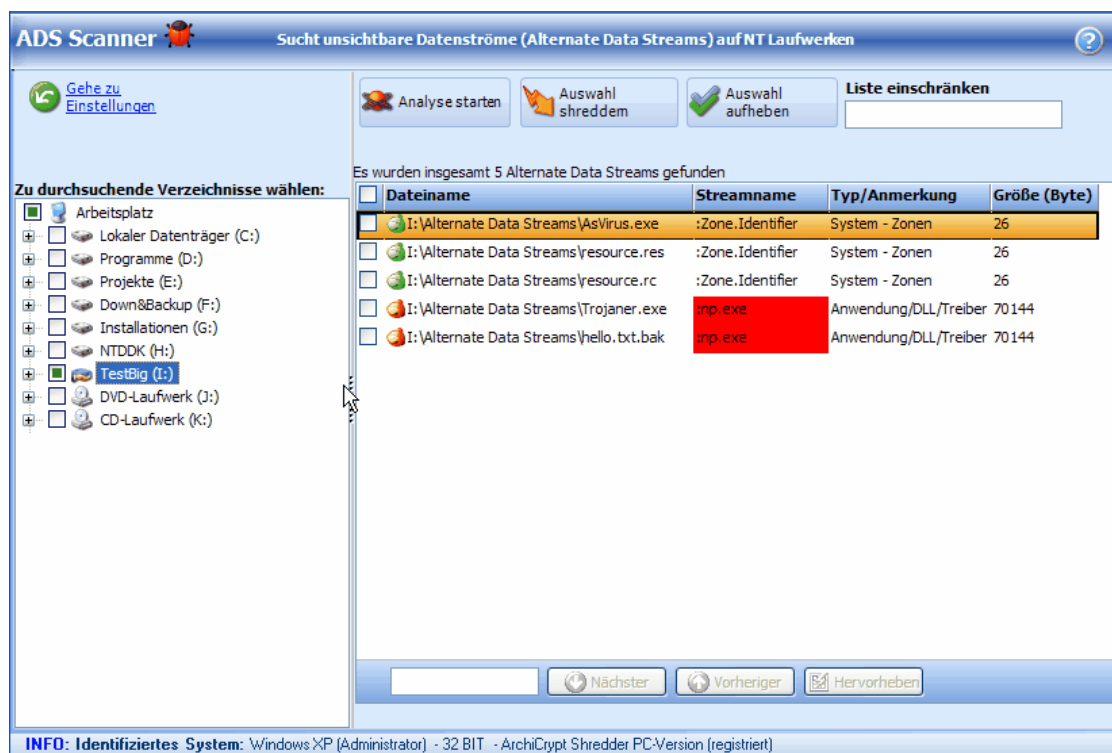
Auf Laufwerken, die mit dem Dateisystem NTFS formatiert wurden, kann man Dateien und Verzeichnissen so genannte Alternative Datenströme (Alternate Data Stream; kurz ADS) anhängen.

Dateien, denen Alternative Datenströme angehängt sind, kann man dies nicht ansehen. Die Dateigröße ist nach dem Anhängen unverändert. Dennoch belegen die Daten Platz und man bequem auf die versteckten Daten zugreifen. Aufgrund dieser Eigenschaften werden ADS häufig genutzt, um Schadprogramme wie **Viren** und **Trojaner** auf Ihrem System einzuschleusen und zu verstecken.

Mit den Bordmitteln, die Windows mitbringt, ist es nahezu und möglich festzustellen, ob einer Datei ein solcher alternativer Datenstrom angehängt wurde.

ADS Scanner

- spürt solche Daten auf,
- kann sie anzeigen
- kann sie löschen
- gibt einen Hinweis auf die potentielle Gefahr
- bietet an, im Internet eine Recherche für Sie durchzuführen.



So finden Sie Alternative Datenströme

Wählen Sie links das zu analysierende Laufwerk oder Verzeichnis aus, indem Sie ein Häkchen setzen (Sie können auch mehrere Laufwerke und Verzeichnisse wählen). Die Analyse dauert bei großen Dateimengen entsprechend lange! Starten Sie die Analyse anschließend mit der Schaltfläche **Analyse starten**. Alle Dateien in den gewählten Verzeichnissen und Unterverzeichnissen werden jetzt analysiert.

Die 2 Phasen der Analyse

Im ersten Schritt ermittelt ArchiCrypt Shredder, welche Dateien zu untersuchen sind. Im zweiten Schritt werden die Daten dann genauer untersucht. Das Ergebnis der Analyse erhalten Sie in einer **Tabelle**.

reinen Text, ist der Datenstrom eher unkritisch. Wenn Sie nicht einschätzen können, wie der Datenstrom zu bewerten ist, halten Sie sich an die automatische Einschätzung durch ArchiCrypt Shredder.

5.7 Datenträger

In der Rubrik Datenträger finden Sie Funktionen, die Strukturen und ganze Partitionen sicher bereinigen können. Um diese Funktionen ausführen zu können, benötigen Sie **Administratorrechte!**

Bereiche und Strukturen

Hier können Sie den vermeintlich freien Bereich (Freispeicher) Ihrer Festplatten säubern, s.g. Clustertips und Dateinamen bereinigen.

Löschen von Datenpartitionen

Oft möchte man die Daten eines ganzen Laufwerks oder einer kompletten Festplatte sicher löschen. Es ist ein Irrglaube, man könne durch einfaches Formatieren die Daten eines Laufwerks vernichten. Dem ist definitiv nicht so! Nutzen Sie die spezielle Funktion des Shredders um solche Laufwerke komplett zu bereinigen.

Boot CD - Löschen des Betriebssystems

Die Partition auf dem Ihr Betriebssystem gespeichert ist, können Sie nicht komplett sicher löschen. Schließlich benötigt ArchiCrypt Shredder das Betriebssystem um laufen zu können. Hier muss eine andere Lösung her. Mit DBAN bietet Ihnen der Shredder an, ein bootbares Medium zu erstellen, mit dem Sie sogar Ihre Betriebssystempartition sicher löschen können.

Hartnäckige Dateien

Einige Dateien sind derart hartnäckig, dass sie im laufenden Betrieb nicht gelöscht werden können. Der Shredder merkt sich solche Dateien und löscht sie beim nächsten Start Ihres Rechners.

5.7.1 Bereiche & Strukturen

Bereiche & Strukturen

Hier können Sie den vermeintlich freien Bereich (Freispeicher) Ihrer Festplatten säubern, s.g.

[Clustertips](#) und [Dateinamen](#) bereinigen.



So bereinigen Sie den Freispeicher, säubern Clustertips und entfernen Spuren alter Dateinamen

Wählen Sie zunächst das oder die Laufwerke aus, indem Sie ein Häkchen vor den Laufwerksbuchstaben setzen. Sie erhalten jetzt eine Übersicht, der Sie entnehmen können, welches **Dateisystem** das gewählte Laufwerk hat und wie viel **freier und belegter Speicher** auf dem Laufwerk vorhanden ist.

Wählen Sie jetzt aus, welche Informationen ArchiCrypt Shredder beseitigen soll, indem Sie die Funktion anhaken.

Freispeicher:

Überschreibt alle Daten die sich in dem Bereich Ihrer Festplatte befinden, der als verfügbar gemeldet wird. Sie sollten diese Funktionen immer dann aufrufen, wenn Sie Dateien ohne die Funktionen von ArchiCrypt Shredder gelöscht haben, die Inhalte jedoch sensibel waren.

Clustertips:

Überschreibt Reste alter Dateien, die sich am Ende von neuen Dateien befinden.

Dateinamen:

Auch Dateinamen können selbst sensible Informationen sein. Schließlich lassen sie Rückschlüsse auf die Inhalte zu. Die Funktion löscht die Dateinamen, die noch ganz oder teilweise in den Strukturen Ihrer Festplatte gespeichert sind.

Die Bereinigung wird gestartet, indem Sie die Schaltfläche Aktion für ausgewählte Festplatte ausführen betätigen.



TIPP: Die Funktion **Freispeicher** und **Clustertips** bereinigen können bei Standarddatenträgern heutiger Größenordnung (300 Gigabyte bis 1 Terabyte), leicht bis zu 24 Stunden und länger in Anspruch nehmen. Nutzen Sie die Funktionen daher eher am Ende eines Arbeitstages und schalten Sie die Funktion "System nach dem Vorgang automatisch herunterfahren" ein. Nach erfolgter Bereinigung wird der Computer dann automatisch heruntergefahren und ausgeschaltet. Die **Rundenzahl** (*Wie oft soll die Methode auf den Freispeicher angewandt werden?*), und die Auswahl der **Methode** unter [Einstellungen Sicherheit](#) wirken sich maßgeblich auf die Dauer des Vorganges aus.

Weiter zu [Löschen von Datenpartitionen](#)

5.7.2 Löschen von Datenpartitionen

Löschen von Datenpartitionen

Oft möchte man die Daten eines ganzen Laufwerks oder einer kompletten Festplatte sicher löschen. Es ist ein **Irrglaube**, man könne durch **einfaches Formatieren** die Daten eines Laufwerks vernichten. Dem ist definitiv nicht so! Nutzen Sie die spezielle Funktion des Shredders um Laufwerke komplett zu bereinigen, auf denen Sie s.g. Nutzdaten ([Datenpartitionen](#)) abgelegt haben.

Falls Sie die Festplatte sicher löschen möchten, die das Betriebssystem enthält, sollten Sie sich das Kapitel [Boot CD & Löschen des Betriebssystems](#) ansehen.



So löschen Sie alle Daten einer Partition

Wählen Sie zunächst das oder die Laufwerke aus, indem Sie ein Häkchen vor den Laufwerksbuchstaben setzen. Betätigen Sie im Anschluss die Schaltfläche **Ausgewählte Festplatte löschen**.

Die Daten der Festplatte und alle enthaltenen Strukturen werden bei diesem Vorgang sicher gelöscht und überschrieben. Um wieder Daten auf der Festplatte speichern zu können, müssen Sie sie mit Systemmitteln formatieren. Nach Abschluss des Löschvorgangs werden Sie von ArchiCrypt Shredder dazu aufgefordert.

Die Funktion **Ausgewählte Festplatte löschen** kann bei Standarddatenträgern heutiger Größenordnung (300 Gigabyte - 1 Terabyte), sehr viel Zeit in Anspruch nehmen. Nutzen Sie die Funktionen daher eher am Ende eines Arbeitstages und schalten Sie die Funktion "System nach dem Vorgang automatisch herunterfahren" ein. Nach erfolgter Bereinigung wird der Computer dann automatisch heruntergefahren und ausgeschaltet. Die **Rundenzahl** (Wie oft soll die Methode auf den Freispeicher angewandt werden?), und die Auswahl der **Methode** unter **Einstellungen Sicherheit** wirken sich maßgeblich auf die Dauer des Vorganges aus.

Bei automatischem Herunterfahren wird der Datenträger nicht wieder neu formatiert. Sie müssen ihn in diesem Fall manuell im Kontextmenü des Windows Explorers neu formatieren!



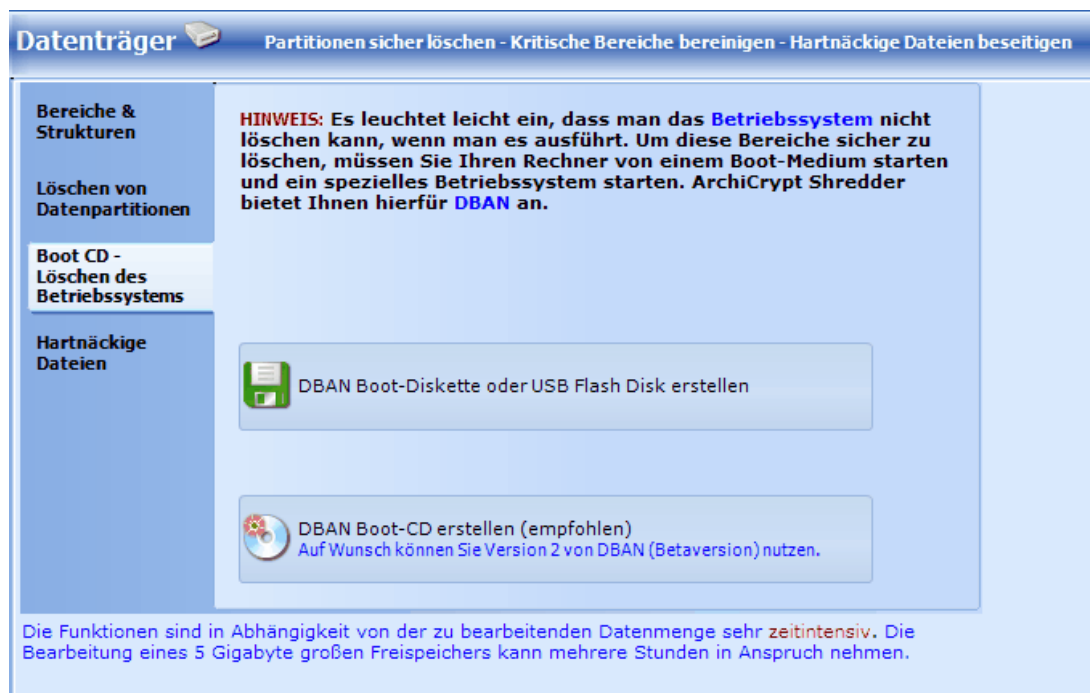
WICHTIG: *Damit Sie die Daten löschen können, darf kein anderes Programm auf Daten dieser Festplatte zugreifen. Schließen Sie solche Anwendungen und achten Sie darauf, dass kein Windows Explorer Fenster den Inhalt des Laufwerks anzeigt. Partitionen, denen aktuell kein Laufwerksbuchstabe zugeordnet ist, können so nicht gelöscht werden. Sie müssen solchen Partitionen in der Datenträgerverwaltung (Systemsteuerung-Computerverwaltung-*

Datenträgermanager) **zunächst einen Laufwerksbuchstaben zuordnen.**

5.7.3 Weiter zu [Boot CD & Löschen des Betriebssystems](#) **Boot CD & Löschen des Betriebssystems**

Boot-Medium - Löschen des Betriebssystems

Die Partition auf dem Ihr Betriebssystem gespeichert ist, können Sie nicht komplett sicher Löschen. Schließlich benötigt ArchiCrypt Shredder das **Betriebssystem** um laufen zu können. Hier muss eine andere Lösung her. Mit DBAN bietet Ihnen der Shredder an, ein bootbares Medium zu erstellen, mit dem Sie sogar Ihre Betriebssystempartition sicher löschen können.



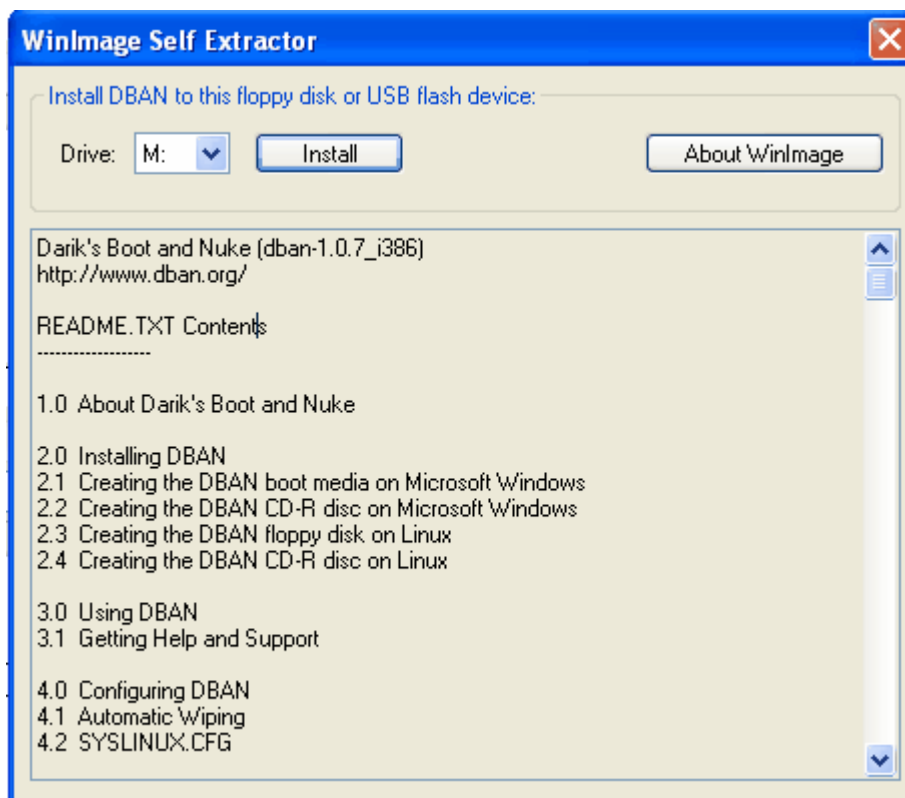
Was ist DBAN?

DBAN (Darik's Darik's Boot and Nuke) ist ein eigenständiges Tool, welches von Herrn Darik Horn entwickelt wurde. DBAN ist kostenlos! ArchiCrypt Shredder bietet lediglich die Funktion, aus dem Programm die Routine aufzurufen, mit der Sie ein **Bootmedium** erstellen können. Alle DBAN betreffenden Nutzer- und Lizenzrechte, sowie Dokumentation entnehmen Sie bitte den mit DBAN gelieferten Originaltexten!

Weitere Informationen über DBAN finden Sie unter:
DBAN.sourceforge.net

Erstellen einer DBAN-Bootdiskette oder eines DBAN-USB Sticks

Legen Sie die **Diskette** ein oder schließen Sie den **USB Stick** an. Alle Daten, die sich auf dem Speichermedium befinden, gehen beim Erstellen verloren!



Wählen Sie das entsprechende Medium (Drives) aus und betätigen Sie die Schaltfläche Install.

Sie werden nochmals gewarnt, dass alle auf dem Medium gespeicherten Daten verloren gehen. Bestätigen Sie, oder brechen Sie den Vorgang ab. Sie sollten sich die Dokumentation zu DBAN ansehen, bevor Sie den Rechner vom Medium booten.

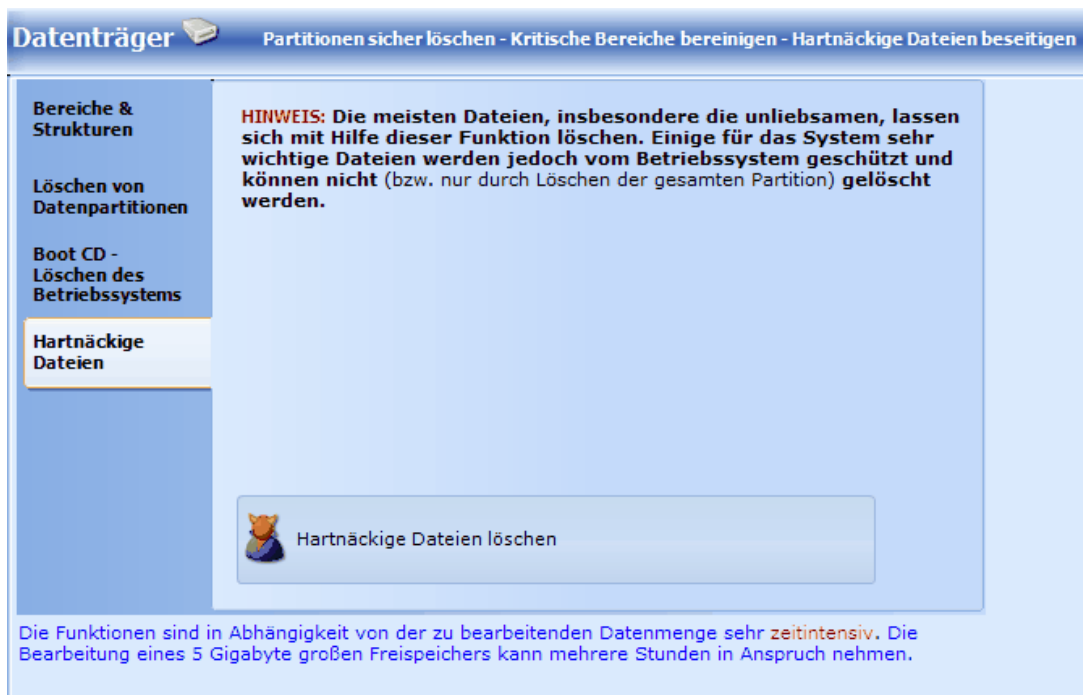
Erstellen einer BOOT-CD

Diese Funktion kopiert eine s.g. **ISO-Image** Datei an den von Ihnen festgelegten Ort. Diese Datei müssen Sie anschließend mit Ihrem CD-Brennprogramm auf CD brennen. Zur Vorgehensweise sollten Sie die Dokumentation Ihres Brennprogramms zu Rate ziehen.

5.7.4 Weiter zu [Hartnäckige Dateien](#) **Hartnäckige Dateien**

Hartnäckige Dateien

Es gibt bestimmte Dateien auf Ihrem Rechner, die man nicht löschen kann, während das Betriebssystem geladen ist. Mit dem Shredder können Sie auch solche Dateien löschen.



So löschen Sie Dateien, die nicht während der Arbeit mit dem Rechner gelöscht werden können

Klicken Sie auf die Schaltfläche Hartnäckige Dateien löschen. Wählen Sie im Dialog die Datei aus, die Sie nicht normal löschen konnten. Die Dateien werden vorgemerkt und beim nächsten **Rechnerstart** gelöscht.



TIPP: *Im Windows Dialog zur Auswahl der Datei können Sie auch mehrere Dateien gleichzeitig auswählen.*

5.8 Verzeichnisse

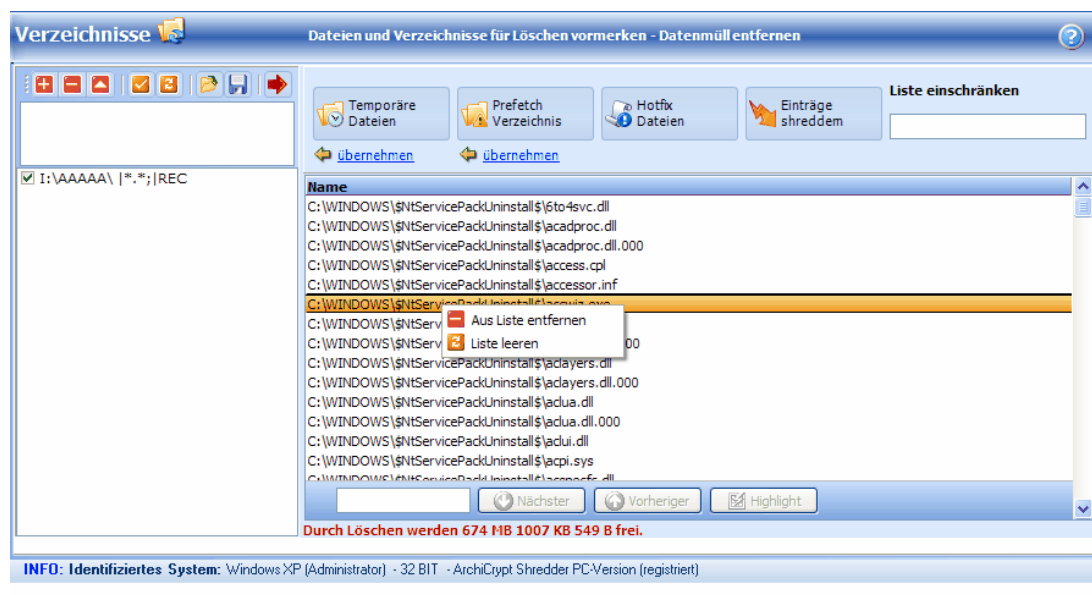
Verzeichnisse

Haben Sie bestimmte Verzeichnisse in denen Sie ständig Daten ablegen, die nach kurzer Zeit nicht mehr von Bedeutung sind? Schwindet der Speicherplatz weil Anwendungen große Datenmengen im temporären Verzeichnis ablegen und nicht wieder löschen. Dann können Sie solche Verzeichnisse hier festlegen und, falls gewünscht, sogar zeitgesteuert oder automatisch beim Beenden des Browsers bereinigen lassen.

Mit den Schaltflächen

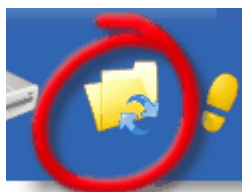
- Temporäre Dateien
- Prefetch Verzeichnis
- Hotfix Dateien

können Sie die Dateien auflisten lassen, die Ihr System vermutlich am stärksten belasten und mit deren Entfernung Sie am meisten Platz zurückgewinnen.



WICHTIGER HINWEIS: *Erst, wenn Sie die Funktion **Einträge shreddern** aufrufen, werden alle in der Tabelle enthaltenen Dateien mit der in den **Einstellungen** festgelegten Methode gelöscht. Vorher werden lediglich die Dateien ermittelt, die für das Löschen in Frage kommen.*

So schaffen Sie sofort eine Menge Platz



Der Shredder bietet für die wichtigen Verzeichnisse **Temporäre Dateien** und **Prefetch Verzeichnis** bereits einen Direktzugriff über die gleichnamigen Schaltflächen in der Kategorie Verzeichnisse. Sie können sich die in diesen Verzeichnissen enthaltenen Dateien in die Tabelle der zu löschenden Einträge übertragen, indem Sie die Schaltfläche betätigen. Die Dateien werden bei diesem Vorgang nur aufgelistet und noch nicht gelöscht.

Durch das Betätigen der Schaltfläche **Hotfix Dateien** werden alle Dateien in die Tabelle übertragen, die durch das Einspielen von Hotfixes und Patches des Betriebssystems noch Speicherplatz belegen. Diese Dateien werden nicht mehr benötigt, sofern Ihr System nach der Installation dieser **Patches** und **Hotfixes** stabil läuft.

Mit den grünen Pfeilen unmittelbar unter den Schaltflächen **Temporäre Dateien** und **Prefetch Verzeichnis** können Sie das zugehörige Verzeichnis dauerhaft in die Liste der Verzeichnisse links übernehmen. Da es sich bei den Hotfixes um viele unterschiedliche Verzeichnisse

handelt, die bei jedem Einspielen solcher Patches anders benannt werden, ist die Übertragung der Verzeichnisnamen in die Liste hier nicht sinnvoll und möglich.

[noch mehr Platz schaffen](#)

Verzeichnisliste

In einer Verzeichnisliste legen Sie Verzeichnisse und Dateitypen fest, die der Shredder berücksichtigen soll.



WICHTIGER HINWEIS: Wenn Sie die Liste nicht speichern, steht sie beim nächsten Start des Shredders nicht mehr zur Verfügung!

[Die Menüleiste zur Bearbeitung der Verzeichnislisten](#)



[Hinzufügen eines neuen Eintrags](#)



Wählen Sie zunächst das gewünschte Verzeichnis aus. Anschließend können Sie im nachfolgenden Dialog festlegen, ob alle Dateien, oder nur Dateien mit bestimmtem Namen berücksichtigt werden sollen. Eine weitere Abfrage ermittelt, ob auch Dateien in ggf. vorhandenen Unterverzeichnissen (rekursiv) berücksichtigt werden sollen.

Beispiel:

Sie möchten in einem Verzeichnis alle Microsoft Word- und Exceldokumente löschen. Geben Sie dazu als Filter **.doc;*.xls* ein.

Sie möchten alle Microsoft Worddokumente löschen, deren Dateiname den Begriff Finanzen enthält. Geben Sie dazu als Filter **Finanzen*.doc* ein.

[Entfernen des/der markierten Einträge](#)



Der markierte Eintrag wird aus der Verzeichnisliste gelöscht

[Bearbeiten des Eintrags](#)



Sie können den aktuell markierten Eintrag bearbeiten.

Alle markieren



Alle Einträge der aktuell geladenen Verzeichnisliste werden aktiviert.

Auswahl komplett aufheben



Alle Einträge der Verzeichnisliste werden deaktiviert.

Gespeicherte Verzeichnisliste laden



Sie können zuvor gespeicherte Verzeichnislisten laden. Beachten Sie, dass der Shredder beim Start immer die zuletzt gespeicherte Verzeichnisliste lädt.

Aktuelle Verzeichnisliste speichern



Sie können die aktuelle Verzeichnisliste mit allen Einstellungen speichern. Diese Liste wird automatisch beim nächsten Start des Shredders geladen. Wurde keine Liste gespeichert, ist die Verzeichnisliste bei nach jedem Start wieder LEER!

Dateien aus Verzeichnisliste in die Tabelle übertragen



Die aktivierten Einträge (Häkchen gesetzt) der aktuellen Verzeichnisliste werden zunächst gesammelt und in die Liste der zu löschenden Dateien aufgenommen.

Die Dateien werden bei dieser Aktion noch nicht gelöscht, sondern nur aufgelistet.



TIPP: So löschen Sie die Inhalte bestimmter Verzeichnisse beim Beenden Ihres Browsers

Oft werden während des Surfens Dateien in bestimmten individuellen Verzeichnissen abgelegt (zum Beispiel bei Downloads) und nach dem Surfen nicht mehr benötigt. Solche Verzeichnisse können Sie automatisch vom Shredder zusammen mit anderen Surfspuren löschen lassen. Definieren Sie einfach eine entsprechende Verzeichnisliste. Speichern Sie diese Liste unbedingt ab. Setzen Sie jetzt bei **Online-Spuren** ein Häkchen bei [Spezielle Verzeichnisse bereinigen](#).



TIPP: So schränken Sie die Liste gefundener Dateien ein

Nachdem Sie die eine Suche durchgeführt haben und die Einträge in der Tabelle aufgelistet wurden, können Sie durch eine Eingabe von Teilen eines Verzeichnis- oder Dateinamens die Liste entsprechend einschränken. Wenn Sie jetzt die Funktion Einträge shreddern aufrufen, werden nur die aktuell in der Tabelle sichtbaren Dateien gelöscht.

5.9 Online-Spuren

5.9.1 Online-Spuren

Online-Spuren

siehe auch [Funktionen für Internet Explorer](#)

Browser zeichnen nahezu jede Aktion im Internet akribisch auf und speichern Texte, Bilder, Videos, Downloads etc. in einem s.g. **Cache** (Zwischenspeicher). Einige der Browser bieten oft in verschlungenen Untermenüs an, dass man diese Dateien löschen kann. Gelegentlich fehlt diese Funktion ganz. Immer werden die Daten bei diesen Aktionen jedoch mit unsicheren Betriebssystemmitteln gelöscht.

Mit entsprechender Software kommen diese Daten rasch wieder ans Tageslicht. Der Shredder fasst die verborgenen Funktionen der Browser zentral zusammen und löscht die Daten im Gegensatz zu den Browsern mit sicheren Methoden so, dass die Daten nicht mehr sichtbar gemacht werden können.

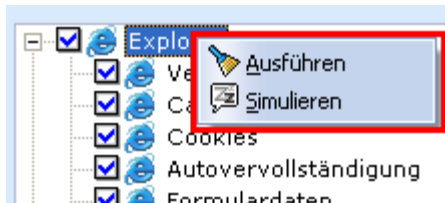


Die **Onlinefunktionen** bieten Ihnen umfassende Möglichkeiten alle Spuren, die eine Internetsitzung auf Ihrem Rechner hinterlässt, zu beseitigen. Im Bereich der Browser-spezifischen Funktionen können Sie festlegen, welche der vom Browser gesammelten Daten

gelöscht werden sollen. Sofern Netscape, Opera, Apple Safari, Google Chrome oder Firefox nicht auf Ihrem Rechner installiert sind, werden die entsprechenden Einträge auch nicht angezeigt!



Die ausgewählten Einträge können Sie über die Blitz Schaltfläche löschen. Wenn Sie einen einzelnen Eintrag auswählen und die rechte Maustaste betätigen, können Sie den Löschvorgang **simulieren** (Simulieren: Bei aktiviertem Logbuch, erhalten Sie Informationen darüber, was gelöscht würde, wenn Sie die Funktion Löschen aufrufen. Sie sollten dazu unbedingt die Funktion [LogBuch führen](#) aktivieren!) oder die dem Eintrag zugeordnete Funktion ausführen.



Um die Liste mit Online Aktionen zu bearbeiten, steht Ihnen eine Menüleiste zur Verfügung:



Alle Einträge auswählen



Auswahl aufheben



Auswahl umkehren



Ansicht reduzieren



Ansicht erweitern (expandieren)



Online-Profil laden und speichern



Sie können sich für verschiedene Situationen und Szenarien jeweils eigene Online-Profile erstellen.



Die **Online-Profile** sind sehr nützlich wenn es darum geht, für verschiedene Situationen unterschiedliche Löschkaktionen vorzusehen. Markieren Sie die gewünschten Löschkaktionen und speichern Sie diese für eine spätere Verwendung. Im [Aufgaben-Planer](#) können Sie den Shredder dann zu bestimmten Zeiten ganz gezielt bestimmte Profile ausführen lassen. Es ist auch möglich, sich mit Hilfe des Aufgaben Planers 1-Klick Löschaufgaben zu erzeugen, die dann bestimmte Online-Profile ausführen.

Funktionen der ausgewählten Einträge ausführen



So löschen Sie Surf Spuren automatisch

Sie können die ausgewählten Aktionen automatisch beim Beenden des zugehörigen Browsers ausführen lassen. Schalten Sie dazu die Funktion "**Daten automatisch löschen**" ein. Ist zum Beispiel eine Funktion für den Internet Explorer ausgewählt überwacht ArchiCrypt Shredder das System. Wenn festgestellt wurde, dass kein Fenster des Internet Explorers mehr aktiv ist, startet der Löschvorgang.

Das Symbol des Shredders im Infobereich (RADAR) zeigt farblich den jeweiligen Status an:

- | | |
|-----------------------|--|
| Rotes Symbol: | Kein automatische Löschen von Online-Spuren |
| Blaues Symbol: | Automatisches Löschen ist aktiviert, es ist jedoch kein Browserfenster geöffnet. |
| Grünes Symbol: | Automatisches Löschen ist aktiv, ein oder mehrere Browserfenster |

sind geöffnet.

Werden diese Fenster geschlossen, startet der Löschvorgang.

Das Löschen der Onlinespuren kann mit Hilfe der Funktionen

[spezielle Verzeichnisse](#)

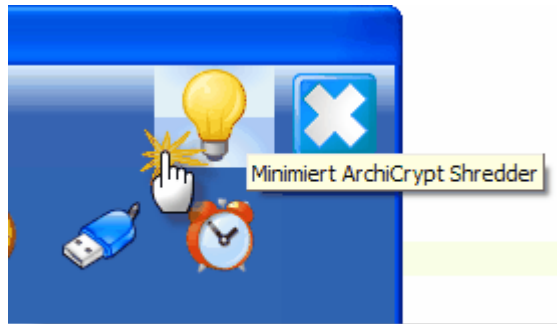
und

[Plugins ausführen](#)

um zusätzliche Aufgaben erweitert werden. Öffnen Sie zum Beispiel während des Surfens im Internet oft ZIP-Archive oder betrachten Videos, können Sie die entsprechenden Plugins zur Beseitigung der Spuren ebenfalls automatisch nach dem Beenden des Browsers ausführen lassen.



TIPP: Insbesondere dann, wenn ArchiCrypt die Online-Spuren automatisch überwachen soll, ist es nicht sinnvoll, das Shredderfenster ständig geöffnet zu haben. Sie können den Shredder in das Systemfach (Infobereich nahe Systemuhr) minimieren und dort über das Symbol per Doppelklick im Bedarfsfall wieder aufrufen. Um den Shredder zu minimieren, klicken Sie in der obersten Menüleiste auf das **Lampensymbol**.



So löschen Sie beim Beenden eines Browsers Dateien in bestimmten Verzeichnissen

Wenn Sie in der Kategorie [Verzeichnisse](#) eine Liste mit Verzeichnissen erstellt UND gespeichert (ohne dass Sie eine Liste gespeichert haben, werden die Einträge bei jedem Start des Shredders leer sein) haben, können Sie die Einträge gleich mit den Surf Spuren beseitigen lassen.

So führen Sie beim Beenden eines Browsers bestimmte Plugins aus

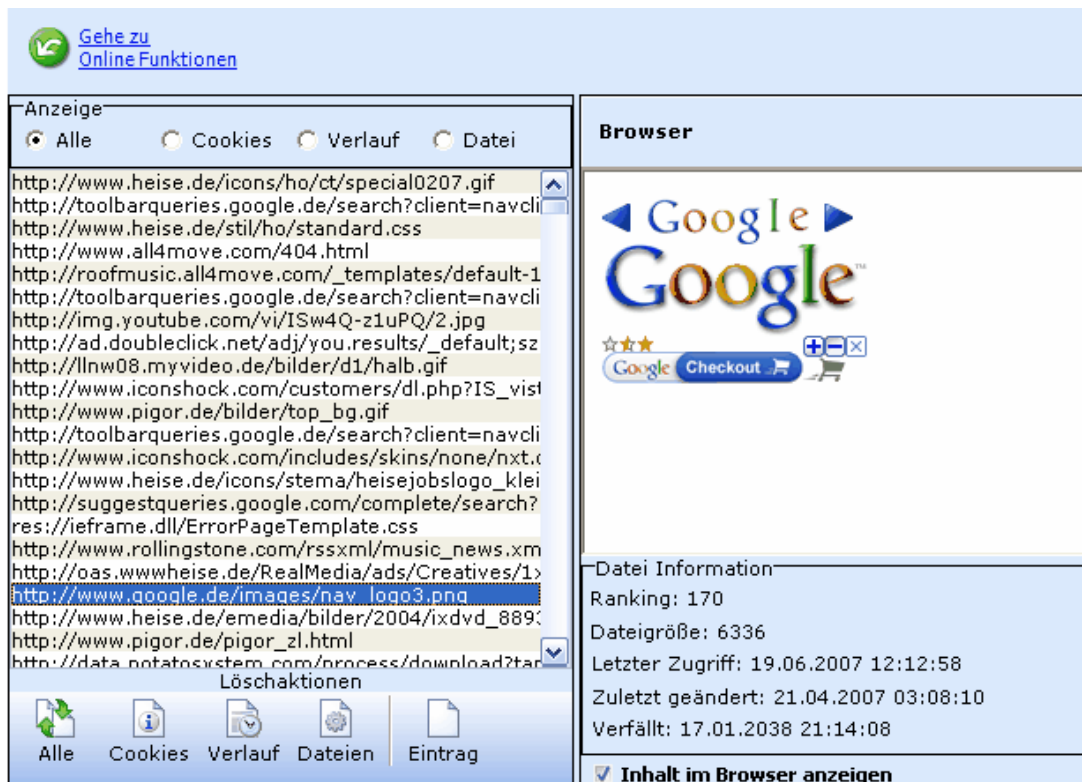
Markieren Sie in der [Kategorie Plugins](#) die Plugins, die beim Beenden des Browsers automatisch ausgeführt werden sollen.

5.9.2 Funktionen für Internet Explorer

Spezielle Funktionen für den Internet Explorer

siehe auch [Online-Spuren](#)

Für die Daten des **Internet Explorers** verfügt ArchiCrypt Shredder über einige **Sonderfunktionen**. Sie können sich den Inhalt des Cache (Zwischenspeichers) ansehen und einzelne Einträge oder Gruppen sicher löschen. Neuere Versionen des Internet Explorers bieten zwar Möglichkeiten, den Zwischenspeicher nach einer Internettour zu löschen, der Löschvorgang basiert jedoch auf Betriebssystemmitteln; so gelöschte Daten können also mühelos rekonstruiert werden.



Anzeige

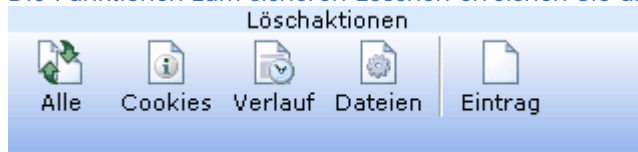


Die auf Ihrem System gespeicherten Einträge zur Auswahl werden in der Auflistung aufgeführt.

Wenn Sie die Option "Inhalt im Browser anzeigen" auswählen, werden Ihnen neben den Detailinformationen (Zwischengespeicherte Webseiten, Bilddateien etc.) in der Inhaltsanzeige (Browser) angezeigt.

Funktionen

Die Funktionen zum sicheren Löschen erreichen Sie über die Menüleiste:



Die Funktion "Alle" löscht alle zwischengespeicherten Daten

Die Funktion "Cookies" löscht alle Cookies

Die Funktion "Verlauf" löscht die Verlaufsdaten (auch History genannt)

Die Funktion "Dateien" löscht alle zwischengespeicherten Webseiten, Bilder etc.

Die Funktion "Eintrag" löscht den aktuell ausgewählten Eintrag

5.10 Plugins

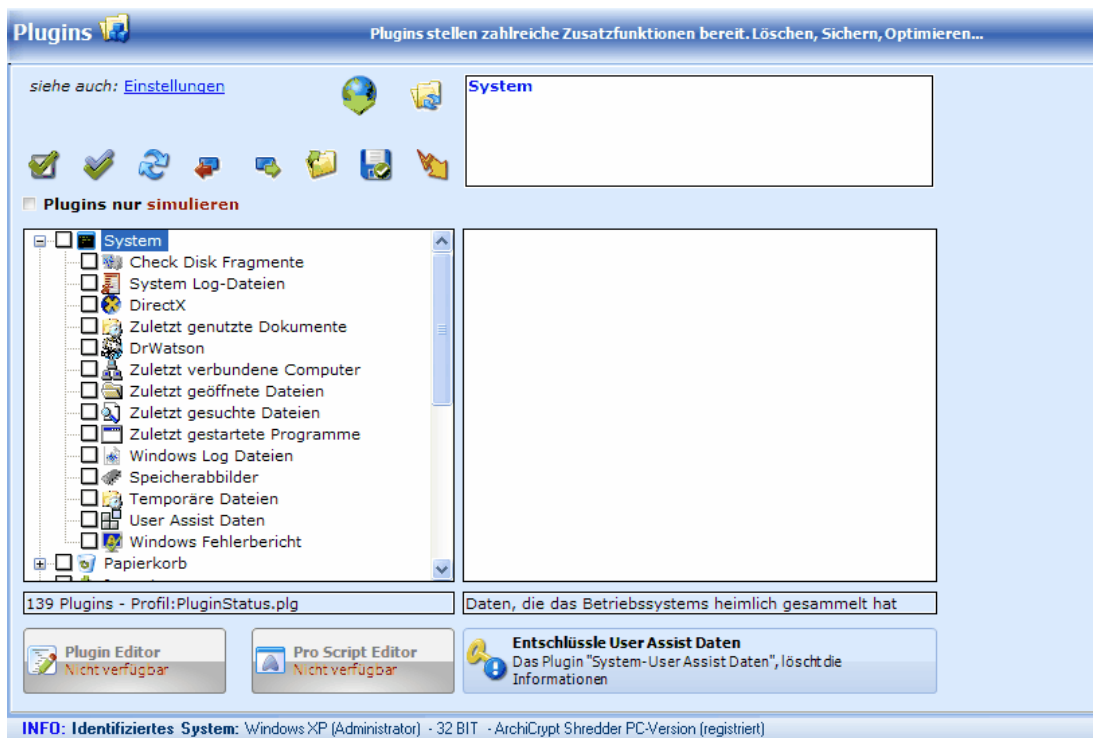
Das Plugin-System

Die **Plugins** bieten die Möglichkeit, ArchiCrypt Shredder in seinen Funktionen nahezu beliebig zu erweitern, ohne dass man Änderungen am Programm selbst vornehmen muss. Dabei beschränken sich die Plugins keinesfalls auf das reine Löschen von Daten. Mit Hilfe der so genannten **Pro Scripte** kann ArchiCrypt Shredder um komplette kleine Anwendungen erweitert werden.

Die Vollversion von ArchiCrypt Shredder bringt ca. 120 Plugins mit, darunter ca. 10 Pro Script Anwendungen (Dateibackup, Ver- und Entschlüsselung, Systemoptimierung, Datei Up- und Download via FTP, Dateisuche, Löschen von E-Mails aus Outlook,...).



EXPERTENTIPP: Die Pro Scripte liegen im Quellcode vor und können von fortgeschrittenen Anwendern mit Programmierkenntnissen mit Hilfe der mitgelieferten Entwicklungsumgebung (Pro Script Editor) für eigene Programmideen verwendet werden.



Plugins für mehr Platz

Einige Plugins in der Rubrik System sorgen dafür, dass Sie sofort wieder einiges mehr an freiem Speicherplatz auf Ihrem Betriebssystem zur Verfügung haben. Sorgen Sie dafür, dass ArchiCrypt Shredder Administratorrechte besitzt. Falls Sie in der Titelleiste eine Schaltfläche mit einem Schildsymbol sehen, betätigen Sie die Schaltfläche um den Shredder mit erweiterten Rechten neu zu starten.



Neustart mit Administratorrechten

Wählen Sie jetzt die folgenden Plugins in der Rubrik System aus:

- Check Disk Fragmente
- System Log-Dateien
- Windows Log Dateien
- Speicherabbilder
- Temporäre Dateien
- Windows Fehlerberichte


Führen Sie die Plugins jetzt aus, indem Sie auf die Blitzschaltfläche klicken.

Ein Pro Script in Aktion:



Um zu sehen, ob und wie ein Plugin arbeitet, können Sie Plugins sogar **simulieren**; Die Funktionen des Plugins werden dann nicht wirklich ausgeführt. (Zum Simulieren sollten Sie unbedingt die Funktion [LogBuch führen](#) aktivieren!).

So führen Sie ein Plugin im Simulationsmodus aus

Wählen Sie das entsprechende Plugin mit der rechten Maustaste aus. Wählen Sie im Kontextmenü jetzt den Eintrag "Simulieren". Alternativ können Sie die Einstellung "Plugins nur **simulieren**" anhaken und die Ausführung des Plugins über die Menüleiste  starten. Das Plugin muss dazu aktiv sein (vorangestelltes Häkchen).

Geheime Aufzeichnungen des Betriebssystems entschlüsseln

Fest in ArchiCrypt Shredder integriert ist die Funktion **Entschlüssele USER ASSIST Daten**. Hier können Sie sich die Daten auflisten lassen, die das Betriebssystem seit der Installation über Ihr Nutzerverhalten gesammelt hat. Um diese Daten von Ihrem System zu entfernen, können Sie das entsprechende Plugin (User Assist Daten) in der Kategorie System ausführen.



ACHTUNG: *Das Plugin User Assist Daten löschen steht wie verschiedene andere Plugins nur in der Vollversion zur Verfügung!*

Wohin sichern Sicherungsplugins meine Daten?

Verschiedene Plugins sichern Daten (z.B. Ihre E-Mails von Outlook Express, Windows Mail oder Thunderbird). Unter Einstellungen Allgemeines [Pfad für Sicherungsplugins](#) sollten Sie daher einen Pfad (Verzeichnis) festlegen, in dem die gesicherten Daten des Plugins dann abgelegt werden.

siehe [Einstellungen-Allgemein](#)

So führen Sie Plugins aus

Um Plugins auszuführen, bestehen grundsätzlich 3 Möglichkeiten.

1. Sie können die Plugins anwählen (Häkchen setzen) und dann über die **Blitzschaltfläche** starten. Sofern Sie nicht den Simulationsmodus aktiviert haben (kein Häkchen bei Plugins nur simulieren), werden die entsprechenden Aktionen ausgeführt.
2. Sie können verschiedene Plugins aktivieren und diese dann automatisch mit dem Beenden des Browsers ausführen lassen, indem Sie unter Online-Spuren die Funktionen Daten automatisch löschen und Plugins ausführen aktivieren. Hierzu müssen Sie die aktuelle Auswahl als **Plugin-Profil** unbedingt abspeichern,
3. Sie können **Löschaufgaben** planen ([Aufgaben-Planner](#)), die zu bestimmten Zeiten ausgeführt werden. Hier können Sie ein Plugin-Profil (sie müssen die Auswahl im Shredder als Plugin-Profil speichern) auswählen und es zu bestimmten Zeiten ausführen lassen.

Um die Liste mit den Plugins zu bearbeiten, steht Ihnen eine Menüleiste zur Verfügung:



Alle Einträge auswählen



Es macht keinen Sinn, alle Plugins zu aktivieren. Einige Plugins fertigen Sicherungen von Dateien an, die andere Plugins wieder zurückspielen. Sie sollten sich daher die Plugins und deren Beschreibung genau ansehen und gezielt an- und abschalten.

Auswahl aufheben



Auswahl umkehren



Ansicht reduzieren



Ansicht erweitern (expandieren)



Plugins neu einlesen



Notwendig, wenn Sie während ArchiCrypt Shredder aktiv ist, neue Plugins installieren.

Im Internet nach neuen Plugins suchen



Setzt Vollversion voraus! Stellen Sie sicher, dass ArchiCrypt Shredder ungehindert auf das Internet zugreifen kann. Sofern im Internet aktualisierte oder neue Plugins bereitstehen, lädt ArchiCrypt Shredder diese auf Ihr System.

Plugin-Profil laden und speichern



Plugin-Profile speichern, welche Plugins aktuell aktiv (Häkchen gesetzt) sind. Sie können sich so für verschiedene Löschaufgaben unterschiedliche Plugins zusammenstellen. Im [Aufgaben-Planner](#) können Sie gezielt einzelne **Plugin-Profile** ausführen lassen oder **1-Klick Löschaufgaben** definieren, die ein bestimmtes Plugin-Profil ausführen.

Funktionen der ausgewählten Einträge ausführen



WICHTIGE HINWEISE:

- Falls Sie bei **Online-Spuren** die Option **Plugins ausführen** gewählt haben, werden die von Ihnen aktivierten Plugins zusammen mit der Beseitigung von **Onlinespuren** ausgeführt!
- Plugins prüfen vor Ihrer Ausführung immer, ob Ihr System bestimmte Voraussetzungen erfüllt. Wenn das Plugin feststellt, dass die Ausführung auf Ihrem System keinen Sinn ergibt (entsprechendes Programm nicht installiert, falsches Betriebssystem, fehlende Nutzerrechte, etc.), bricht es ab. So macht es zum Beispiel keinen Sinn, zwischengespeicherte Werte des Programms WinZIP zu löschen, wenn sich das Programm nicht auf Ihrem Rechner befindet.
- Alle Plugins, die mit ArchiCrypt Shredder ausgeliefert werden, sind verschlüsselt (Ausnahme Pro Scripte). Das Programm bietet die Möglichkeit, **unverschlüsselte Plugins** zu laden. Sie müssen dazu unter Einstellungen **Allgemeines die Funktion " Unautorisierte Plugins zulassen"** aktivieren. Da theoretisch jeder in der Lage ist,

unverschlüsselte Plugins zu erstellen, sollten Sie beim Umgang mit diesen Plugins vorsichtig sein. Achten Sie immer darauf, dass das Plugin aus einer vertrauenswürdigen Quelle stammt.

So erstellen Sie eigene Plugins und Pro Scripts

Mit ArchiCrypt Shredder wird ein [Plugin Editor](#) geliefert. Mit Hilfe dieses Editors können Sie neue Plugins erstellen und den Shredder um eine Vielzahl neuer Funktionen ergänzen.



EXPERTENTIPP: Für fortgeschrittene Anwender mit Programmierkenntnissen steht der Pro Script Editor zur Verfügung. Der Pro Script Editor ist ausschließlich in englischer Sprache verfügbar und ist ähnlich gestaltet, wie die Entwicklungsumgebung für Object Pascal (Delphi). Um Ihnen den Einstieg etwas zu erleichtern stellen wir Ihnen unsere Pro Scripts in unverschlüsselter Form mit Kommentaren (in deutsch) zur Verfügung. Sie finden die Projektdateien im Unterverzeichnis Plugins der Shredderinstallation. Die Projektdateien tragen die Dateieendung `ssproj`, units die Endung `psc` und Formulare die Endung `sfm`. Kopieren Sie sich diese Dateien in ein eigenes Verzeichnis und lassen Sie die eigentlichen Dateien unangetastet. Falls Sie eigene Programme auf Basis der Beispiele anlegen, geben Sie diesen vor dem Kopieren in das Plugins Verzeichnis unbedingt andere Namen. Ansonsten könnten bei einer Aktualisierung der Plugins Ihre Versionen überschrieben werden.

Unterhalb der Plugins finden Sie zwei Schaltflächen, mit denen Sie die entsprechenden Editoren aufrufen können. Voraussetzung ist, dass sich die Anwendungen im gleichen Verzeichnis befinden wie ArchiCrypt Shredder. Wenn Sie sich eine USB- oder U3-Installation erstellen, werden die beiden Editoren nicht mit berücksichtigt und stehen auch nicht zur Verfügung.



EXPERTENTIPP: Um die Editoren auch in den mobilen Versionen nutzen zu können, müssen Sie die Anwendungen (ShredderProScriptEditor.exe und ShredderPlgEditor.exe) aus dem Anwendungsverzeichnis der PC Version in das Shredderverzeichnis auf dem USB-Stick kopieren.

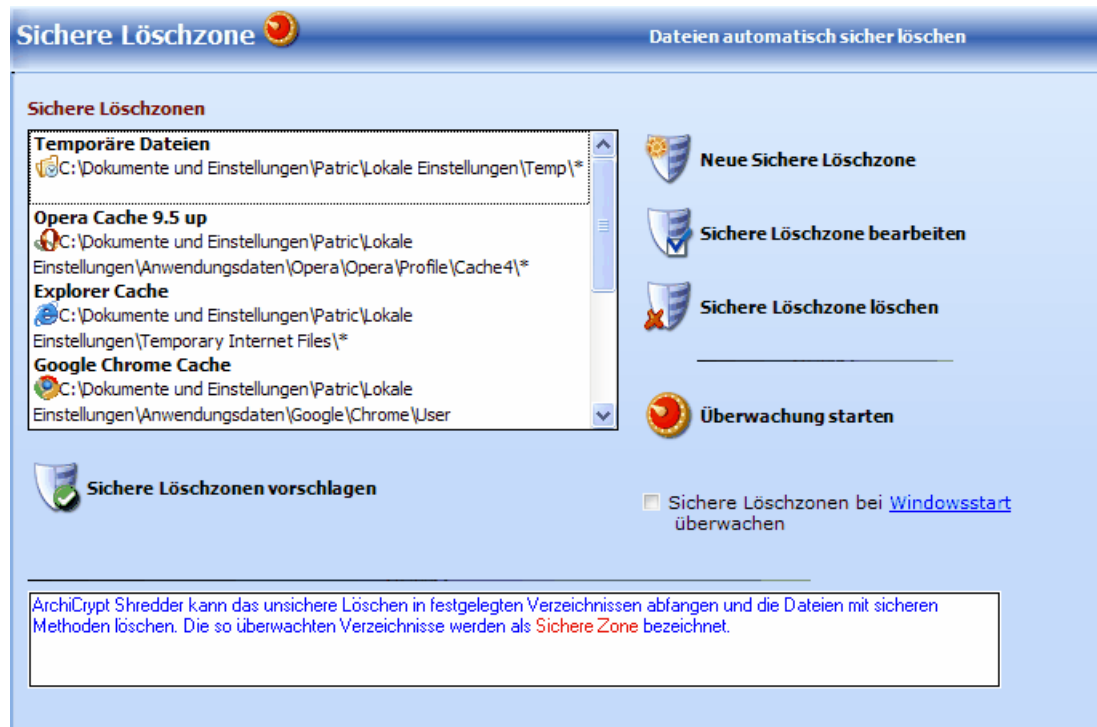
5.11 Sichere Löschezonen

Sichere Löschezonen

Viele Anwendungen, darunter Browser, Office-, Grafik- und Multimediaanwendungen erstellen

on-the-fly Daten und löschen diese wieder. Von diesem Vorgang bekommen Sie als Anwender nichts mit. Das Löschen erfolgt jedoch auch hier leider immer mit den unsicheren Betriebssystemmitteln. Die Daten können also wieder hergestellt werden.

Sichere Löschrzonen sind Orte auf Ihrem Rechner, an denen der Shredder genau diese unsicheren Löschooperationen abfängt und Daten sicher löscht. Lassen Sie sich vom Shredder Sichere Löschrzonen vorschlagen oder definieren Sie eigene.



5.11.1 Überblick

Was sind Sichere Löschrzonen?

Sichere Löschrzonen sind Speicherorte, die von ArchiCrypt Shredder überwacht werden. Wird eine Datei in einer Sicheren Löschrzone gelöscht, übernimmt ArchiCrypt Shredder automatisch die Kontrolle über den Löschrvorgang und sorgt dafür, dass die Dateien mit sicheren Verfahren gelöscht werden.

Warum benötigt man Sichere Löschrzonen?

Es gibt zwei wesentliche Gründe für den Einsatz von Sicheren Löschrzonen

Ein wichtiger Grund ist die Bequemlichkeit. Wenn Sie eine Sichere Löschrzone eingerichtet haben, können Sie darin befindliche Dateien wie gewohnt mit Betriebssystemmitteln löschen. Da ArchiCrypt Shredder die Kontrolle über das Löschr übernimmt, werden die Dateien hier automatisch sicher gelöscht.

Der wichtigste Grund ergibt sich aus dem Verhalten vieler Anwendungen.

Den meisten Anwendern ist nicht bekannt, dass nahezu jedes Programm s.g. temporäre

Dateien (Dateien die Informationen zwischenspeichern, die das jeweilige Programm für die korrekte Arbeit benötigt) erstellt. Viele Anwendungsprogramme erstellen **Sicherungskopien** der Arbeitsdatei. Gearbeitet wird dann mit der Kopie, um im Fehlerfall den Datenverlust so gering wie möglich zu halten. Wird die Anwendung beendet, löscht die Anwendung die Kopie mit Betriebssystemmitteln (unsicher). Sie haben keinerlei Einfluss darauf, wie die Dateien gelöscht werden. Es ist fast überflüssig zu erwähnen, dass die Originalinhalte der mit Betriebssystemmitteln gelöschten Dateien relativ leicht zumindest teilweise wiederherstellbar sind. Fast jedem Nutzer sind in diesem Zusammenhang bereits die berühmten ~\$.doc und mso*. * Dateien von Microsoft Word aufgefallen.

Auch Browser organisieren ihren s.g. **Cache** (Zwischenspeicher, in dem Inhalte aus dem Internet abgelegt werden. Wird eine Seite erneut angefordert, werden die Inhalte aus dem Cache geladen und nicht aus dem Internet. Der Zugriff und Seitenaufbau ist dadurch viel schneller) selbst. Ist eine im Cache befindliche Datei nicht mehr aktuell oder ist das Limit für die Cachegröße erreicht, löscht der Browser mit Betriebssystemmitteln veraltete Dateien.

Die Liste mit Programmen die ähnlich arbeiten, lässt sich nahezu beliebig fortführen. Besonders häufig tritt dieses Phänomen bei Programmen aus den Bereichen Office-Anwendungen, Multimedia, bei Bildbetrachtungs- und -bearbeitungswerkzeugen, Emailclients, Tauschbörsen, Chatprogrammen und Packprogrammen auf. Auch hier haben Sie keine Möglichkeit, den Löschvorgang zu beeinflussen.



Traditionelle Löschprogramme oder Spurenvernichter helfen hier nicht, da diese Tools keine unsicheren Löschaktionen abfangen können.

Besonders heimtückisch sind diese "**Datenlecks**" im Zusammenhang mit verschlüsselten Daten. Gerade dann, wenn es darum geht, sensible Daten vor den Augen Unbefugter zu verbergen, können solche "Datenlecks" verheerend sein. Ein Angreifer kann hier ohne jegliche Kenntnis des Passwortes unter Umständen die Daten einfach aus den Hinterlassenschaften der Anwendungen auslesen, mit denen die Daten bearbeitet oder betrachtet wurden.

ArchiCrypt Shredder 5 ist zur Zeit weltweit das einzige Programm, welches diese unsicheren Löschaktionen in den Sicheren Löschezonen abfangen und durch sichere Methoden ersetzen kann.

➡ ANMERKUNG: *Es soll nicht verschwiegen werden, dass man diese Datenfragmente auch loswerden kann, indem man jedesmal, wenn man mit bestimmten Anwendungen gearbeitet hat, den Freispeicher sicher überschreibt. Allerdings ist der Zeitaufwand für diese Maßnahme je nach Größe des betroffenen Datenträgers gigantisch!*

In [ArchiCrypt Shredder - Sichere Löschzone](#) können Sie sehen, welche Dateien gerade von welcher Anwendung gelöscht wurden. ArchiCrypt Shredder schaltet sich in allen Fällen dazwischen und sorgt dafür, dass die Daten sicher gelöscht werden. Würde ArchiCrypt Shredder sich nicht einschalten, könnten die Daten zum größten Teil wieder hergestellt werden.



HINWEIS:
Wenn Sie selbst z.B. mit dem Windows Explorer Dateien in einer Sicheren Zone löschen,

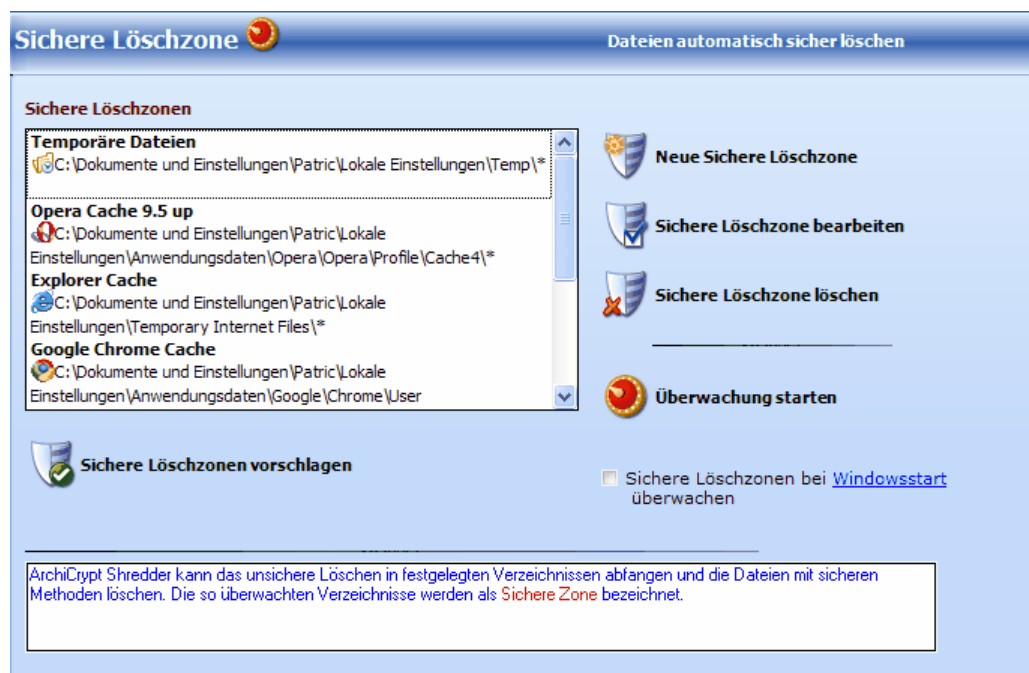
haben Sie 2 Möglichkeiten:

1. Sie können die Datei wie gewohnt in den **Papierkorb** löschen. Die Datei kann dann bei Bedarf wieder hergestellt werden. ArchiCrypt Shredder tastet die Daten der Datei nicht an.
2. Sie können die Datei mit **gehaltener Shift-Taste** löschen. Windows fragt dann, ob Sie die Datei wirklich löschen möchten. Falls Sie mit **JA** antworten, schaltet sich der Shredder ein und löscht die Datei mit sicheren Methoden. Ein Wiederherstellen ist nicht mehr möglich.

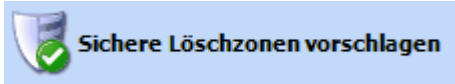
➔ **WICHTIG:** Die Dateinamen von Dateien, die in der sicheren Löschzone gelöscht werden bleiben erhalten. Mit Hilfe s.g. Recovery-Software können Sie so die Dateinamen solcher Datenfragmente ggf. ausmachen, die Inhalte der Dateien sind jedoch nicht wiederherstellbar.

5.11.2 Sichere Löschzonen**Sichere Löschzonen**

siehe auch: [Überblick](#) und [Überwachung der Sicheren Löschzonen](#)

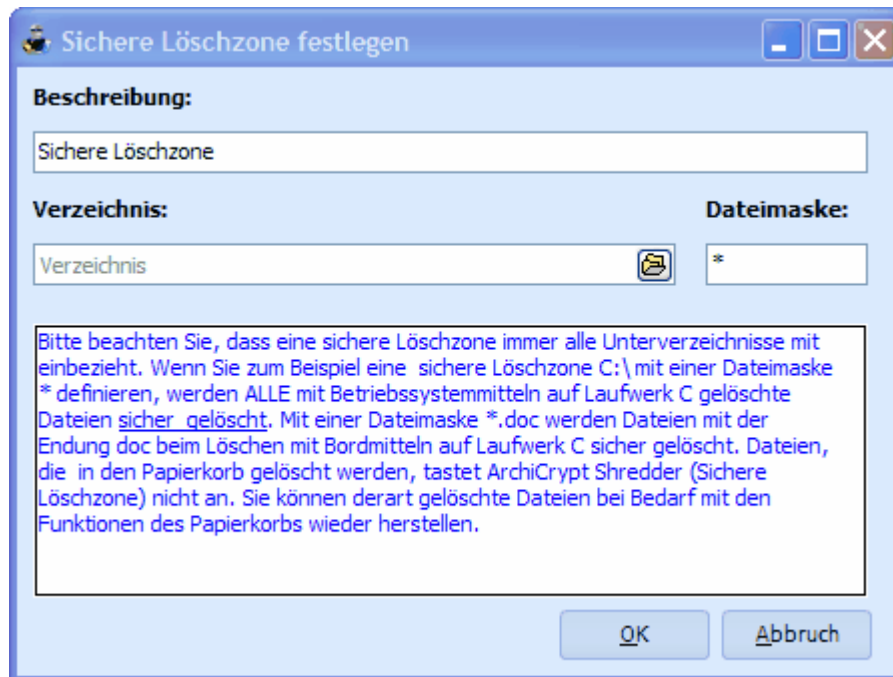
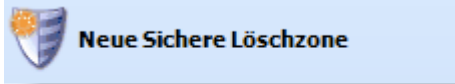



Mit ArchiCrypt Shredder können Sie Sichere Löschzonen definieren und bearbeiten. Um Ihnen den Einstieg zu erleichtern, kann ArchiCrypt Shredder einige Beispielszonen erstellen. Die so erzeugten Sicheren Löschzonen sind in Anzahl und Art je nach Rechner unterschiedlich. Zum Erstellen der Beispielszonen betätigen Sie bitte die Schaltfläche **Sichere Löschzonen vorschlagen** erstellen.



So erstellen Sie eine neue Sichere Löschezone

Betätigen Sie die Schaltfläche "Neue Sichere Löschezone"



Geben Sie eine Beschreibung für die Sichere Löschezone ein und legen Sie das Verzeichnis fest, welches überwacht werden soll (Schaltfläche ) . Damit ArchiCrypt Shredder weiß, bei welchen Dateien er das Löschen übernehmen soll, müssen Sie eine s.g. Dateimasken festlegen. Das * ist ein s.g. **Platzhalter** und steht für eine beliebige Zeichenfolge. Ist als Maske also * angegeben, fängt ArchiCrypt Shredder alle Löschoptionen ab. Wenn Sie z.B. *.txt angeben, fängt ArchiCrypt Shredder das Löschen von Textdateien ab, bei W*.doc alle Löschoptionen von Dateien, deren Name mit W beginnt und deren Dateiendung doc ist.



UNBEDINGT WICHTIG: *Es werden immer auch alle Unterverzeichnisse überwacht! (rekursiv).*

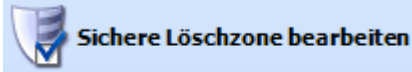
*Vermeiden Sie es möglichst, ein komplettes Laufwerk mit der Maske * als Sichere Löschezone zu definieren. Die Performance Ihres Systems leidet je nach [Einstellung der Löschart](#) unter Umständen erheblich.*

Wenn Sie entgegen dem Ratschlag dennoch ein komplettes Laufwerk als Sichere Löschezone festlegen, sollte dies die einzige Sichere Löschezone für dieses Laufwerk

sein!

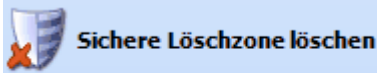
So arbeiten Sie mit den Sicheren Löschezonen

Sichere Löschezone bearbeiten



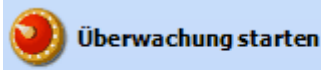
Wählen Sie in der Übersicht die zu ändernde Sichere Löschezone aus und betätigen Sie die Schaltfläche Sichere Löschezone bearbeiten. Nehmen Sie die gewünschten Änderungen vor und betätigen Sie die Schaltfläche OK.

Sichere Löschezone entfernen



Wählen Sie die zu löschenden Sichere Löschezone aus und betätigen Sie die Schaltfläche Sichere Löschezone entfernen.

Überwachung starten



Sichere Löschezonen werden von ArchiCrypt Sichere Löschezone überwacht. Erst wenn ArchiCrypt Sichere Löschezone aktiv ist, werden die Löschezonen in den definierten Sicheren Löschezonen durch ArchiCrypt Shredder überwacht.

(siehe auch [ArchiCrypt Sichere Löschezone](#))

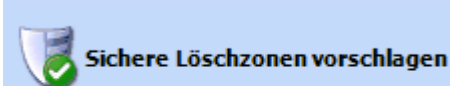
Sichere Löschezonen bei Windowsstart überwachen

Diese Option bewirkt, dass ArchiCrypt Sichere Löschezonen mit Windows gestartet wird und direkt die Sicheren Löschezonen überwacht.



HINWEIS: Verschiedene Antiviren- und Antispyware-Programme verhindern, dass Programme automatisch mit Windows gestartet werden können. Stellen Sie bitte sicher, dass kein solches Programm ArchiCrypt Shredder daran hindert. Notfalls können Sie einen Link auf ArchiCrypt Sichere Löschezone manuell in den Autostart-Ordner kopieren. Hinweise dazu finden Sie in der Hilfe zum Betriebssystem.

Beispielzonen erstellen / Sichere Löschezonen vorschlagen

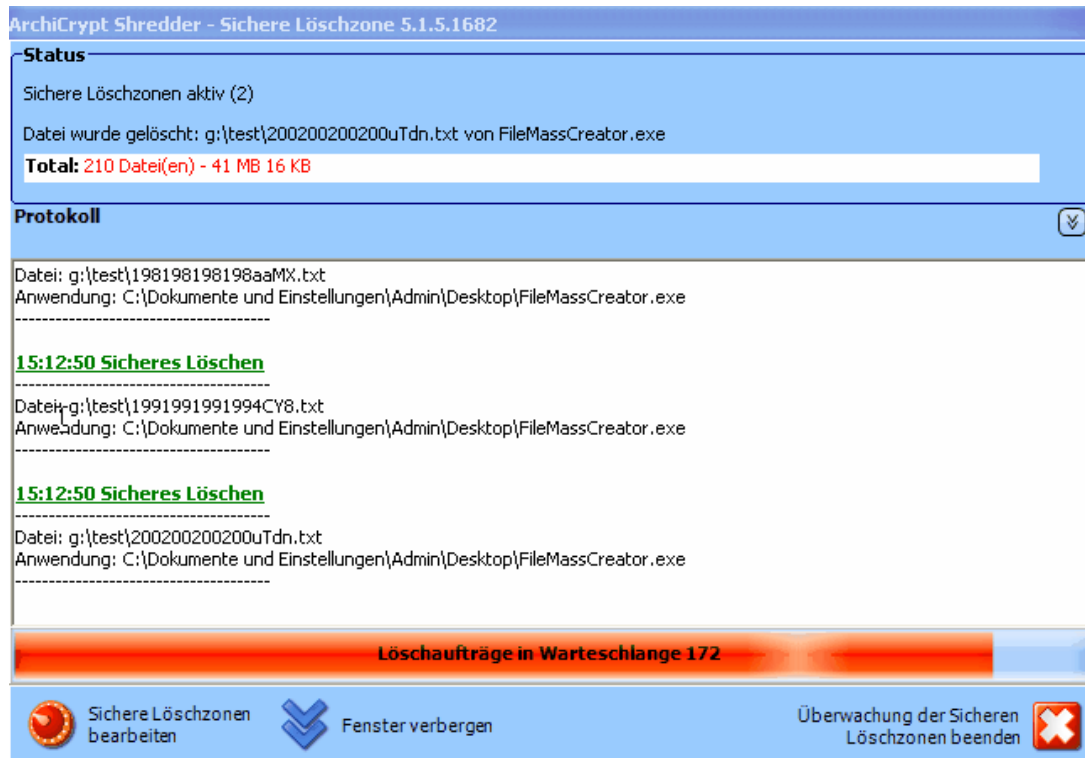


Erstellt auf Ihr System abgestimmte Sichere Löschezonen (hängt davon ab, welche Programme und Verzeichnisse ArchiCrypt Shredder auf Ihrem Rechner findet). Diese Löschezonen können abgeändert und ergänzt werden.

5.11.3 ArchiCrypt Shredder - Sichere Löschrone

Überwachung der Sicheren Löschrone

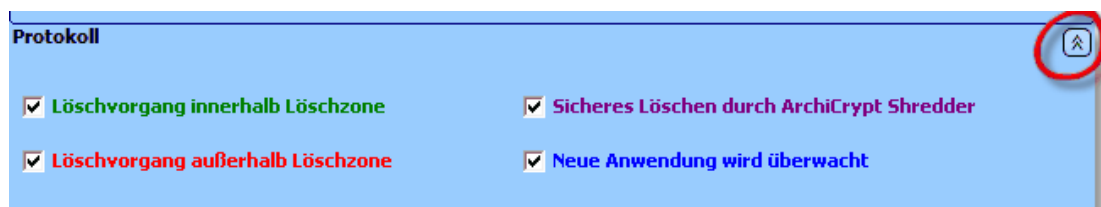
siehe auch: [Überblick](#) und [Sichere Löschrone](#)



ArchiCrypt Sichere Löschrone ist das Programm, welches die eigentliche Überwachung der Sicheren Löschrone vornimmt. Dies bedeutet: Erst, wenn ArchiCrypt Sichere Löschrone gestartet ist, werden die Dateien in den Sicheren Löschrone durch ArchiCrypt Shredder gelöscht. Wird ArchiCrypt Sichere Löschrone beendet, werden die Sicheren Löschrone auch nicht mehr überwacht.

Status und Logbuch der Sicheren Löschrone

Daneben zeigt ArchiCrypt Sichere Löschrone auf Wunsch auch Informationen über durchgeführte Löschkaktionen an.





EXPERTENTIPP

Wenn Sie herausfinden möchten, ob und wo eine Anwendung Dateien temporär speichert, aktivieren Sie die Protokollfunktion **Löschvorgang außerhalb Löscherzone**. Prüfen Sie dann Einträge im Protokoll, bei denen als Anwendung Ihre Anwendung mit auftaucht. Anhand des Namens der gelöschten Datei können Sie evtl. Vorschläge für eine weitere Sichere Löscherzone erhalten.

Beispiel:

```
Anwendung: C:\Programme\Internet Explorer\iexplore.exe
-----
15:21:54 Löschvorgang außerhalb Sicherer Löscherzonen
-----
Datei: C:\Dokumente und Einstellungen\Admin\Cookies\admin@doubleclick[2].txt
Anwendung: C:\Programme\Internet Explorer\iexplore.exe
-----
```

Im obigen Beispiel sehen wir, dass Internet Explorer im Verzeichnis C:\Dokumente und Einstellungen\Admin\Cookies eine Datei gelöscht hat, die nicht in einer sicheren Löscherzone liegt. Wir könnten jetzt eine entsprechende Sichere Löscherzone mit C:\Dokumente und Einstellungen\Admin\Cookies als Verzeichnis und * als Maske anlegen, um auch hier die Löscheroperationen künftig abzufangen!

Das Protokoll bietet ein Kontextmenü, das Sie mit der rechten Maustaste aufrufen können. Im Kontextmenü stehen Ihnen die Funktionen Löschen (setzt das Protokoll zurück) und In Zwischenablage kopieren (Kopiert den aktuellen Inhalt in die Zwischenablage; Sie können den Text in jedem Textprogramm wie z.B. Wordpad oder Word einfügen) zur Verfügung.

Bedienung von ArchiCrypt Sichere Löscherzone

Überwachung der Sicherer Löscherzonen beenden



➔ **WICHTIG: Die Überwachung der Sicherer Löscherzonen wird dadurch ausgeschaltet!**


Sichere Löscherzonen bearbeiten



ArchiCrypt Shredder wird aufgerufen um die Sicherer Löscherzonen zu bearbeiten.

Fenster verbergen



ArchiCrypt Sichere Löscherzone wird minimiert und überwacht im Informationsbereich die Sicherer Löscherzonen weiter. Per Doppelklick auf das Symbol  können Sie ArchiCrypt Sichere Löscherzonen anzeigen lassen. Fängt ArchiCrypt Sichere Löscherzone eine unsichere Löscheroperation ab, werden die Augen im Systemfach für kurze Zeit rot angezeigt.

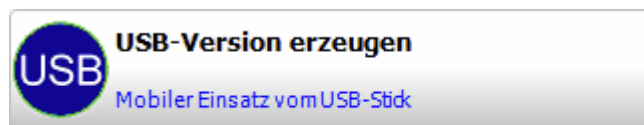
5.12 Mobile Nutzung

Mobile Nutzung

ArchiCrypt Shredder bietet zwei Möglichkeiten, mit denen es Ihnen möglich ist, die wichtigsten Funktionen auch unterwegs zu nutzen, ohne dass Sie ArchiCrypt Shredder auf dem jeweiligen PC installieren müssen und damit ggf. gegen die Lizenzbestimmungen verstoßen.



So installieren Sie ArchiCrypt Shredder auf einem USB-Stick



Diese Methode ist universell und stellt keine besonderen Anforderungen an den verwendeten Stick. Der Stick sollte über ca. 30 Megabyte freien Speicherplatz verfügen.

Wählen Sie nach dem Betätigen der Schaltfläche USB als Ziel Ihren **USB Stick**. ArchiCrypt Shredder legt jetzt automatisch ein Verzeichnis Shredder 5 auf Ihrem Stick an und kopiert eine spezielle Version für die mobile Verwendung auf diesen Stick. Nach Abschluss der Installation können Sie den Shredder durch Aufruf der Datei ACS shredder5.exe im Verzeichnis Shredder 5 starten.

So installieren Sie ArchiCrypt Shredder auf einem U3-Stick



Die U3 Version bietet die gleichen Funktionen, wie die USB-Version. Da ein **U3-Stick** jedoch eine eigene Umgebung mitbringt, aus der heraus man bequem installierte Programme aufrufen kann, ist die Verwendung eines U3-Sticks die bequemste Art, ArchiCrypt Shredder mobil zu nutzen.

Klicken Sie auf die Schaltfläche U3. Sie werden jetzt nach der **Seriennummer Ihres U3-Sticks** (NICHT Seriennummer von ArchiCrypt Shredder!) gefragt. Nachdem Sie die Seriennummer eingetragen haben, müssen Sie einen Speicherort für das U3-Installationspaket angeben. Nachdem das Installationspaket erzeugt wurde, müssen Sie dieses über die [Programmverwaltung Ihres U3-Sticks](#) auf dem Stick installieren. Fortan steht Ihnen ArchiCrypt Shredder auf Ihrem U3-Stick mit den wesentlichen Funktionen zur Verfügung.

Auf welche Funktionen müssen Sie in der mobilen Version verzichten?

Einige Funktionen des Shredders greifen tiefer in das System ein, setzen bestimmte Rechte des Programms voraus und erfordern eine permanente Installation. Andere Funktionen machen mobile keinen oder nur wenig Sinn.

Die mobilen Versionen können selbst keine weiteren mobilen Versionen erzeugen, auf Sichere Löschezonen müssen Sie verzichten. Ebenso kann das Kontextmenü für den Windows Explorer nicht bereitgestellt werden.

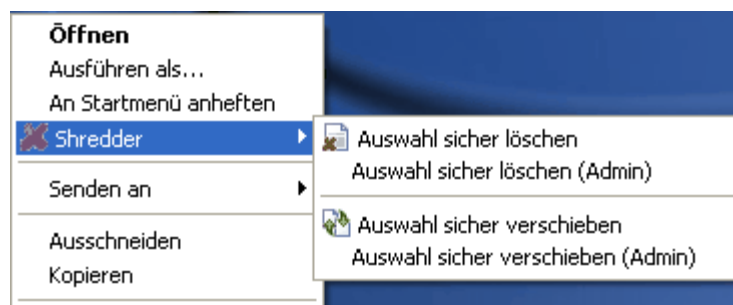
Die Editoren für Plugins und Pro Scripte werden nicht in die mobile Version integriert. Sie können die entsprechenden Dateien bei Bedarf jedoch manuell kopieren. Der Aufgaben-Planer, der zum Verwalten zeitgesteuerter Aufgaben dient, macht mobil ebenfalls keinen Sinn, da nach dem Entfernen des USB- oder U3-Sticks ArchiCrypt Shredder an dem jeweiligen System nicht mehr zur Verfügung stünde.

5.13 Kontextmenü

ArchiCrypt Shredder im Menü des Windows-Explorers

Das Explorer Kontextmenü

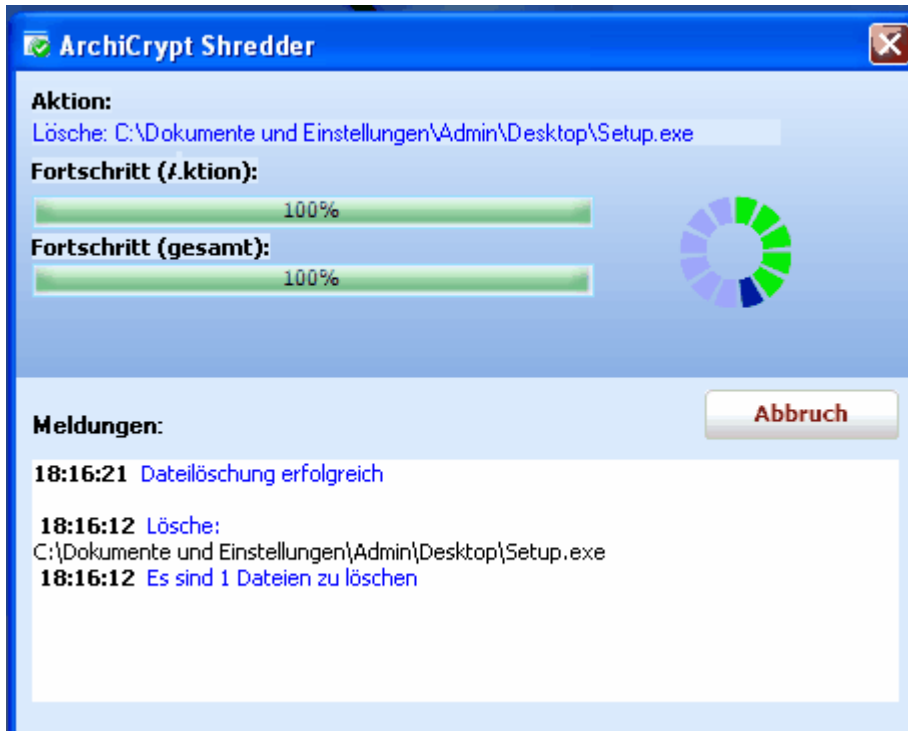
Wenn Sie im Windows Explorer oder einem anderen Dateimanager, der s.g. Shell-Erweiterungen unterstützt, eine Datei oder ein Verzeichnis mit der rechten Maustaste auswählen, erscheint das s.g. **Kontextmenü**. ArchiCrypt Shredder muss NICHT gestartet sein.



Das Kontextmenü bietet Ihnen die folgenden Werkzeuge an:

Auswahl sicher löschen

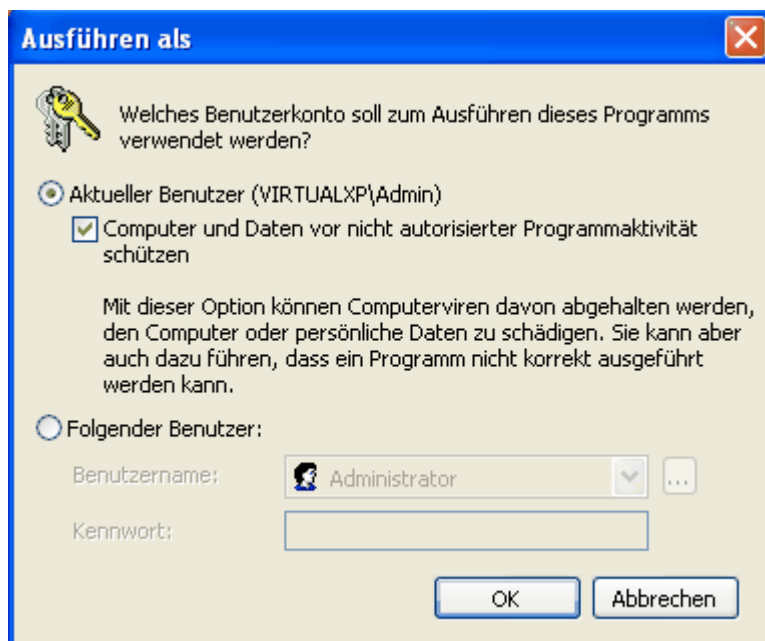
Sie können eine oder mehrere Dateien sowie Verzeichnisse auswählen und so sicher löschen.



Auswahl sicher löschen (Admin)

Es kann vorkommen, dass bestimmte Dateien mit der Funktion Auswahl sicher löschen nicht gelöscht werden können. Hier geht ArchiCrypt Shredder zunächst davon aus, dass Sie nicht über ausreichende Rechte verfügen und schlägt Ihnen den Start von Auswahl sicher löschen (Admin) vor. Hat auch diese Methode keinen Erfolg, wird vorgeschlagen, die Datei zum Löschen **beim nächsten Systemstart** vorzumerken.

Wenn Sie die Admin-Variante wählen, sehen Sie eventuell den folgenden Dialog.



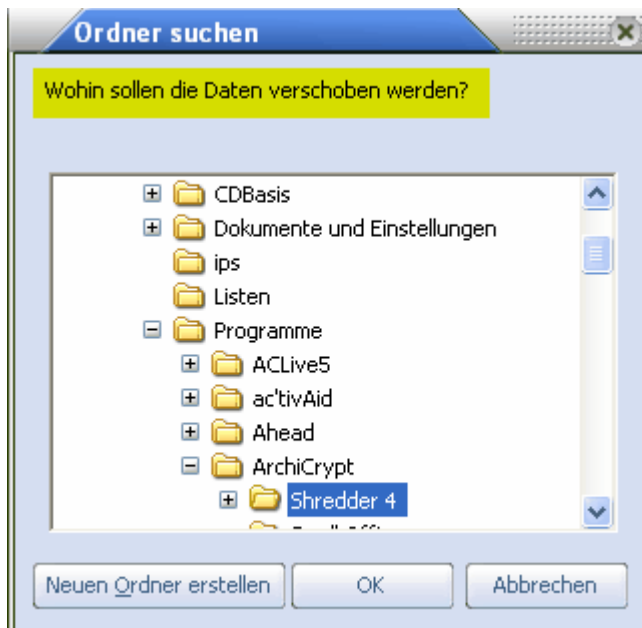
Entfernen Sie auf alle Fälle das Häkchen bei Computer und Daten vor nicht autorisierter Programmaktivität schützen! Entfernen Sie das Häkchen nicht, hat der Shredder keine Administratorrechte. Wenn Sie die Option Folgender Benutzer auswählen, loggen Sie sich bitte als Nutzer mit Administratorrechten ein!

So verschieben Sie Dateien und Verzeichnisse sicher an einen neuen Speicherort

Auswahl sicher verschieben

Wenn Sie Dateien von einem Speicherort an einen anderen verschieben, geschieht bei Nutzung der Betriebssystemfunktionen Folgendes: Zuerst werden die Dateien an den neuen Speicherort kopiert. Nach dem Kopieren werden die Dateien am Ursprungsort gelöscht. Das Löschen erfolgt mit Betriebssystemmitteln und ist unsicher.

ArchiCrypt Shredder hingegen löscht die Dateien sicher.

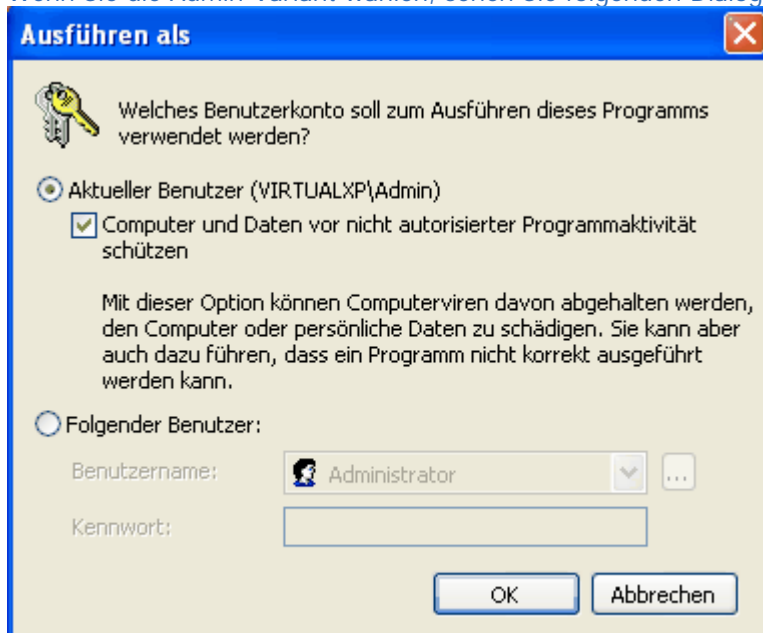


Wählen Sie die Datei(en) oder das Verzeichnis aus, welches Sie **sicher verschieben** möchten. Betätigen Sie die rechte Maustaste und rufen Sie die Funktion **Auswahl sicher verschieben** auf. Legen Sie das Ziel für die Dateien fest und betätigen Sie die **OK** Schaltfläche.

Auswahl sicher verschieben (Admin)

Diese Variante ist angebracht, wenn Sie beim Verschieben mit der normalen Variante eine Fehlermeldung erhalten. Der Verschiebevorgang wird dann ggf. mit höheren Rechten ausgeführt.

Wenn Sie die Admin-Variante wählen, sehen Sie folgenden Dialog.



Entfernen Sie auf alle Fälle das Häkchen bei **Computer und Daten vor nicht autorisierter**

Programmaktivität schützen! Entfernen Sie das Häkchen nicht, hat der Shredder keine Administratorrechte. Wenn Sie die Option Folgender Benutzer auswählen, loggen Sie sich bitte als Nutzer mit Administratorrechten ein!

Was tun, wenn beim Sicheren Verschieben ein Fehler auftritt?

ArchiCrypt Shredder erstellt mit Hilfe des Betriebssystems eine Kopie der ausgewählten Verzeichnisse/Dateien. Meldungen die während dieses Vorganges erscheinen, stammen direkt vom System. Versuchen Sie es im Fehlerfalle mit der (Admin) Variante des Befehls.

In bestimmten Fällen führt ggf. der folgende Weg zum Erfolg:

Kopieren Sie die Dateien wie gewohnt mit Betriebssystemmitteln an den neuen Ort. Wählen Sie dann im Kontextmenü Auswahl sicher löschen (Admin). Hier werden in hartnäckigen Fällen Dateien erst beim nächsten Rechnerstart gelöscht.

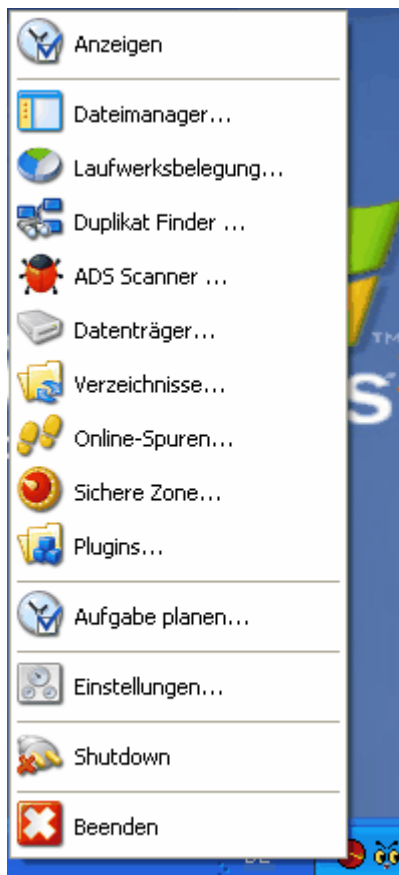
Kontextmenü im Infobereich

Symbol: 

Das Radar Symbol des Shredders im Infobereich zeigt farblich den jeweiligen Status an:

Rotes Symbol:	Kein automatische Löschen von Online-Spuren
Blaues Symbol:	Automatisches Löschen ist aktiviert, es ist jedoch kein Browserfenster geöffnet.
Grünes Symbol:	Automatisches Löschen ist aktiv, ein oder mehrere Browserfenster sind geöffnet.
	Werden diese Fenster geschlossen, startet der Löschvorgang.

Klicken Sie mit der rechten Maustaste auf das Symbol, um das nachfolgende Menü zu erhalten:

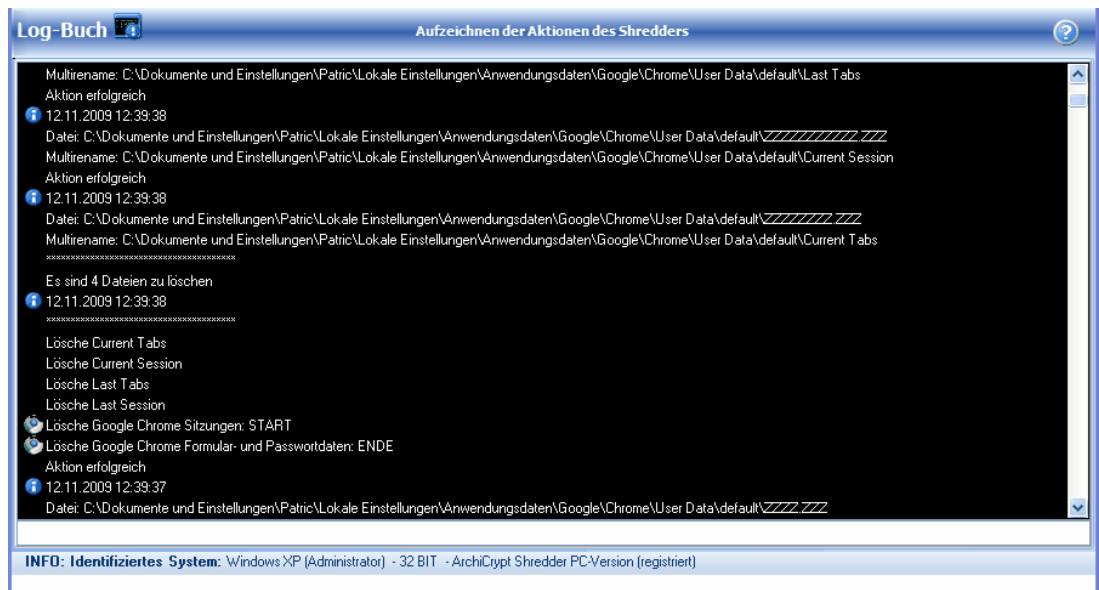


Eine Besonderheit ist die Funktion Shutdown, über die Sie Ihren Rechner sofort herunterfahren können. Die restlichen Funktionen rufen die entsprechenden Kategorien von ArchiCrypt Shredder auf.

5.14 LogBuch

Das Logbuch

Im **Logbuch** werden alle Aktionen mit Uhrzeit und Statusmeldung aufgeführt.



Falls Sie unter [Einstellungen](#) die Option LogBuch führen aktiviert haben, werden die Aktionen von ArchiCrypt Shredder auf dieser Seite protokolliert. Sie sehen immer die letzten 400 Zeilen. Alle Aktionen der aktuellen Sitzung finden Sie in der Protokolldatei ACShreder.log, sofern die Option Logdatei schreiben in den [Einstellungen](#) aktiviert ist. Sie können das LogBuch zurücksetzen, indem Sie die rechte Maustaste betätigen und den Eintrag Löschen wählen.

➔ **HINWEIS:** Eine wichtige Rolle spielt das LogBuch auch im Zusammenhang mit der **Simulation** bei den **Online** und **Plugin-Funktionen**. Hier wird protokolliert, welche Aktionen bei der eigentlichen Ausführung durchgeführt würden.

➔ **ACHTUNG:** Das LogBuch geht verloren, sobald ArchiCrypt Shredder beendet wird.

6

siehe auch [Logdatei](#) unter [Einstellungen Allgemeines](#)
Aufgaben-Planer

Der Aufgaben-Planer

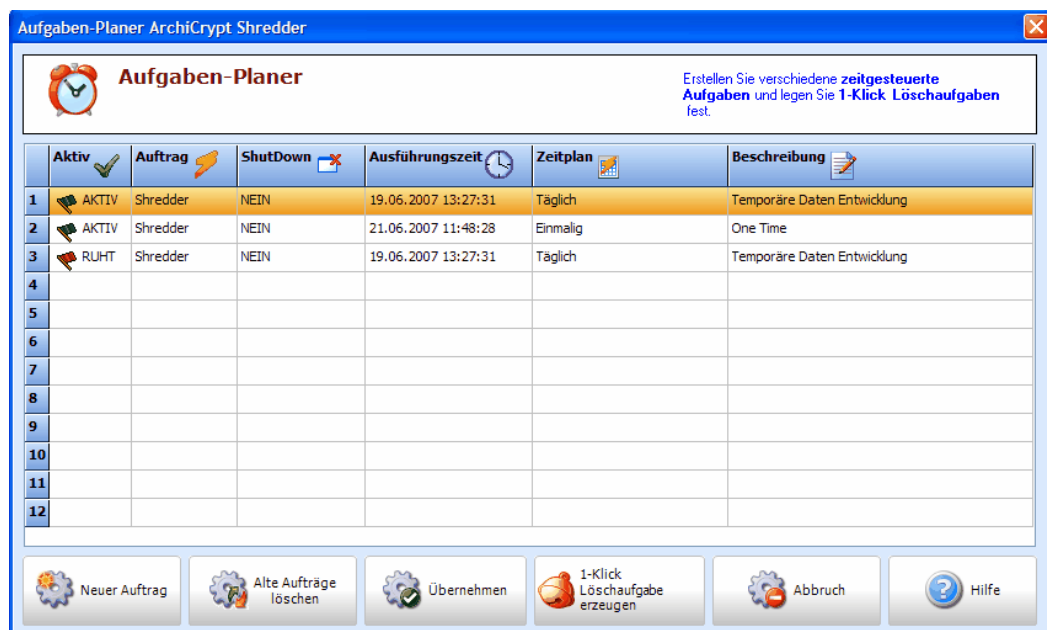
siehe auch [Aufgabe planen](#) und [Zeitüberwachung](#)

Der [Aufgaben Planer](#) dient dazu, bestimmte Aktionen die man normalerweise manuell mit dem Shredder ausführt zusammenzufassen und entweder zu einer bestimmten Zeit oder durch einen einzigen Klick (1-Klick Löschaufgabe) ausführen zu lassen.



Sie starten den Aufgaben-Planer, indem Sie die Schaltfläche Aufgabe planen betätigen.

Die [Zeitüberwachung](#) sorgt dafür, dass geplante Aufgaben auch zum vorgesehenen Zeitpunkt abgearbeitet werden. Sie können die Zeitüberwachung über die Schaltfläche Zeitüberwachung starten aktivieren, oder dafür sorgen, dass die Zeitüberwachung bei jedem Windows Start automatisch gestartet wird. Setzen Sie dazu ein Häkchen bei "Zeitüberwachung mit Windows starten".



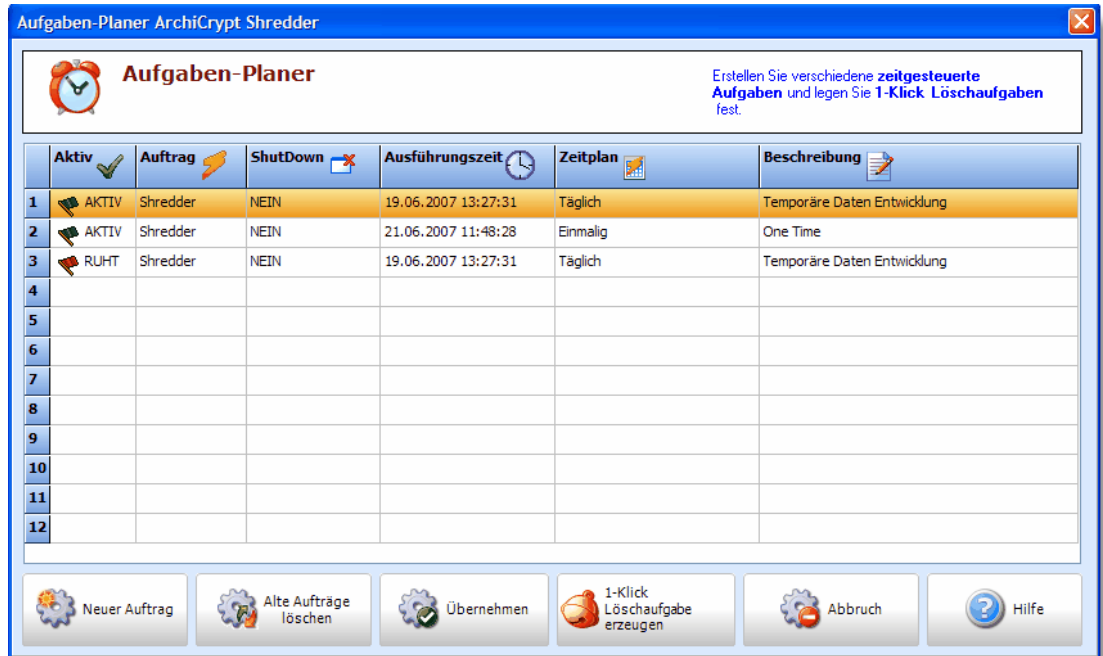
6.1 Aufgaben planen

Der Task-Planer / Aufgabe-Planer

siehe auch: [Zeitüberwachung](#)

Der **Aufgaben-Planer** verwaltet alle Löschaufgaben. Eine **Löschaufgabe** ist eine Zusammenfassung von verschiedenen Aktionen, die ArchiCrypt Shredder dann zu bestimmten Zeiten automatisch ausführen kann.

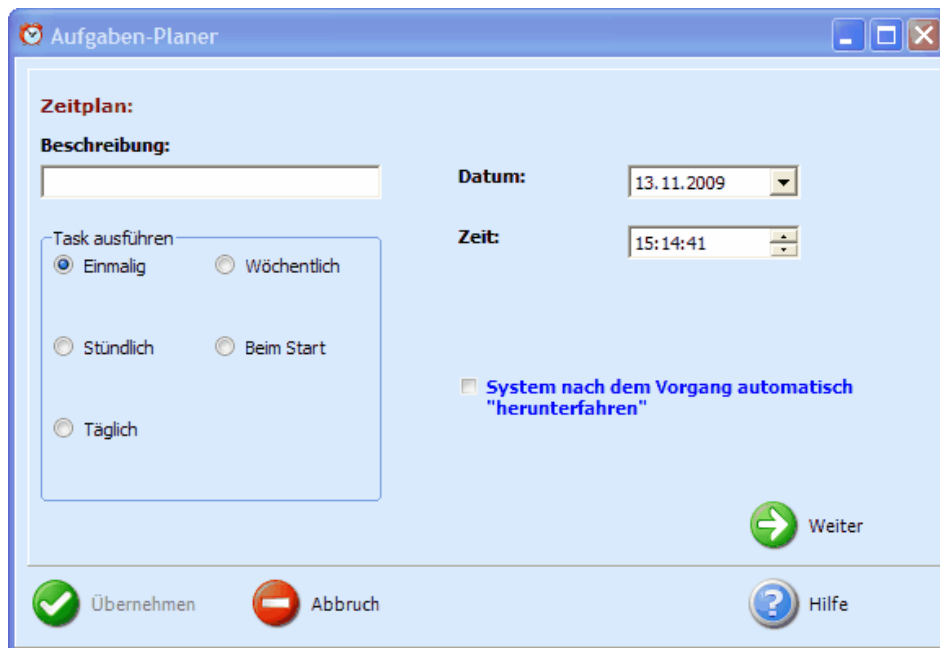
Sie können neue Aufgaben erstellen und bereits vorhandene Aufgaben bearbeiten. Einzelne Aufgaben können Sie direkt starten oder als **1-Klick Löschaufgabe** speichern.



So erstellen Sie einen neuen Löschauftrag

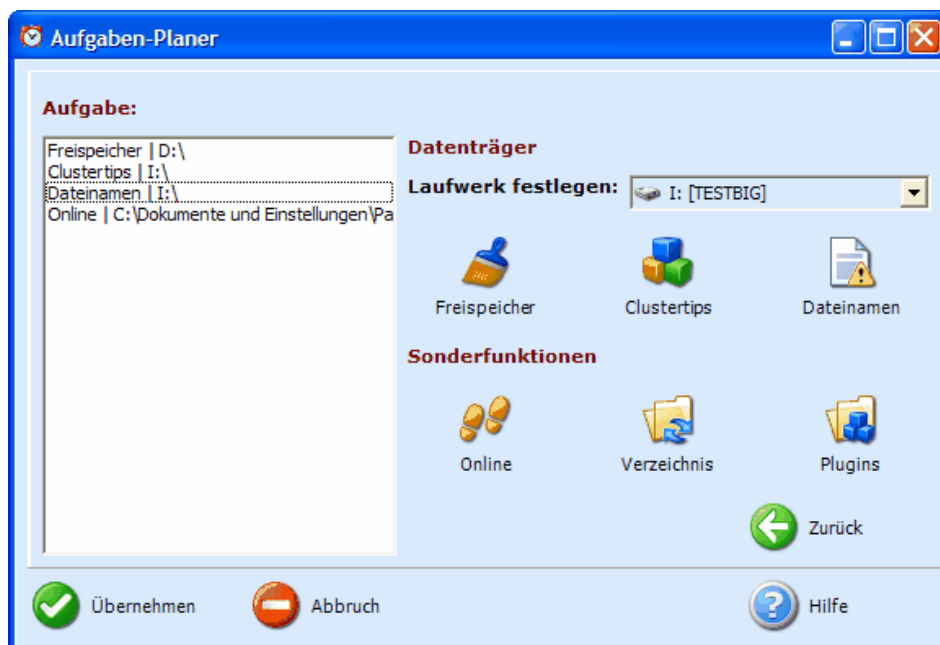
Um eine neue Aufgabe zu erstellen, betätigen Sie bitte die Schaltfläche Neuer Auftrag. Es erscheint ein Wizard, mit dessen Hilfe Sie einen neuen Löschauftrag erstellen können:

1. Schritt:



Geben Sie eine Beschreibung für die neue Aufgabe ein (optional), legen Sie fest, wie häufig und wann die Aufgabe ausgeführt werden soll. Gleichzeitig haben Sie die Möglichkeit, festzulegen, dass der Rechner nach der Bearbeitung der Aufgabe automatisch heruntergefahren werden soll. Dies ist dann nützlich, wenn Sie sehr zeitaufwendige Aufgaben wie zum Beispiel den Freispeicher oder Clustertips bereinigen lassen. Wenn Sie die gewünschten Angaben gemacht haben, betätigen Sie die Schaltfläche Weiter.

2. Schritt



Sie haben die Möglichkeit datenträgerbezogene Aufgaben zu definieren ([Datenträger](#)), oder die [Sonderfunktionen](#) zu wählen. Um eine datenträgerbezogene Aufgabe zu definieren, wählen Sie zunächst das gewünschte Laufwerk aus (Laufwerk festlegen) und betätigen dann die Schaltfläche mit der Funktion Freispeicher, Clustertips oder Dateinamen.

Die Sonderfunktionen:

Online

Beseitigt die Online Spuren, die Sie in ArchiCrypt Shredder unter Online-Spuren festgelegt haben. Hier können Sie, sofern gewünscht ein bereits vorhandenes [Online-Profil](#) ausführen lassen. Wenn Sie kein Online-Profil angeben, werden die aktuell im Shredder aktivierten Löschaufgaben durchgeführt.



ACHTUNG: Die Funktionen [spezielle Verzeichnisse](#) und [Plugins ausführen](#) des Online Profils werden nicht berücksichtigt, können jedoch separat über die anderen Sonderfunktionen Verzeichnis und Plugins nachgebildet werden.

Verzeichnis

Wählen Sie zunächst das gewünschte Verzeichnis aus. Anschließend können Sie im nachfolgenden Dialog festlegen, ob alle Dateien, oder nur Dateien mit bestimmtem Namen berücksichtigt werden sollen. Schließlich können Sie noch festlegen, ob Unterverzeichnisse berücksichtigt werden sollen oder nicht.

Plugins

Hier haben Sie die Möglichkeit, ein bestimmtes [Plugin-Profil](#) ausführen zu lassen. Wenn Sie kein Profil angeben, werden die aktuell in ArchiCrypt Shredder aktiven Plugins ausgeführt.



ACHTUNG: Die Option [Plugins nur simulieren](#) hat keine Wirkung. Alle Plugins werden ausgeführt!

Wenn alle Angaben gemacht sind, können Sie die Schaltfläche Übernehmen betätigen. In der Tabelle sollten Sie jetzt den neuen Eintrag sehen. In der Spalte AKTIV ist eine grüne Fahne zu sehen, die angibt, dass die Aufgabe ausgeführt werden soll. Möchten Sie die Aufgabe ruhen lassen, klicken Sie mit der Maus auf das Flaggensymbol. Um die aktuell [aktiven](#) Aufträge ausführen zu lassen, betätigen Sie die Schaltfläche Übernehmen.

So starten Sie die Zeitüberwachung

Wenn alle Aufgaben Ihren Vorstellungen entsprechen, betätigen Sie die Schaltfläche Übernehmen. Wenn Sie die Schaltfläche Abbruch betätigen wird der Aufgaben-Planer geschlossen und es werden keinerlei Änderungen übernommen! Falls die [Zeitüberwachung](#)

nicht aktiv ist, werden Sie gefragt, ob diese gestartet werden soll. Nur mit aktiver Zeitüberwachung werden die Löschaufgaben auch abgearbeitet!

So starten Sie eine Löschaufgabe direkt aus dem Aufgaben-Planer

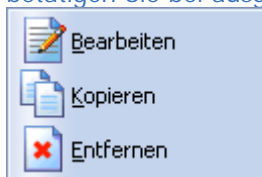
Wählen Sie die entsprechende Löschaufgabe einfach in der Tabelle aus und betätigen Sie die rechte Maustaste. Wählen Sie im Kontextmenü jetzt den Eintrag "Jetzt ausführen". Die Löschaufgabe wird jetzt an den Shredder übertragen. Dabei spielt es keine Rolle, ob die Aufgabe aktiv ist, oder Sie für einen bestimmten Zeitpunkt vorgesehen wird. Die Aufgabe wird sofort ausgeführt.

So speichern Sie Löschaufgaben als 1-Klick Löschaufgabe

Erstellen Sie eine Löschaufgabe wie gewohnt mit dem Aufgaben-Planer. In der Tabelle wählen Sie diesen Eintrag jetzt mit der rechten Maustaste aus. Im Kontextmenü wählen Sie bitte die Funktion Als 1-Klick Löschaufgabe speichern aus. Alternativ klicken Sie auf die Schaltfläche 1-Klick Löschaufgabe erzeugen. Ihr Desktop wird als Speicherort für die Datei vorgegeben. Künftig genügt ein Doppelklick und die definierte Löschaufgabe wird ausgeführt.

So bearbeiten Sie eine Löschaufgabe

Um einen Eintrag zu bearbeiten, führen Sie einen Doppelklick mit der Maus aus, oder betätigen Sie bei ausgewähltem Eintrag die rechte Maustaste.



Sie können einen Eintrag auch kopieren oder aus der Liste der Aufträge löschen.

Aufgaben bereinigen

Nachdem Aufgaben bearbeitet sind, werden sie nicht automatisch aus der Liste gelöscht. Oft ist es sinnvoll, auf die alten Einträge zurückzugreifen und nur z.B. eine Uhrzeit zu ändern. Um abgelaufene Aufgaben aus der Liste zu entfernen, müssen Sie die Schaltfläche Alte Aufträge löschen betätigen.

6.2 Zeitüberwachung

Die Zeitüberwachung

siehe auch [Aufgaben-Planer](#)

Die **Zeitüberwachung** ist ein kleines Programm, welches im Hintergrund dafür sorgt, dass die geplanten Löschaufgaben durch ArchiCrypt Shredder erledigt werden. Sie sollten die Zeitüberwachung mit Windows starten, wenn Sie Aufgaben geplant haben (siehe dazu

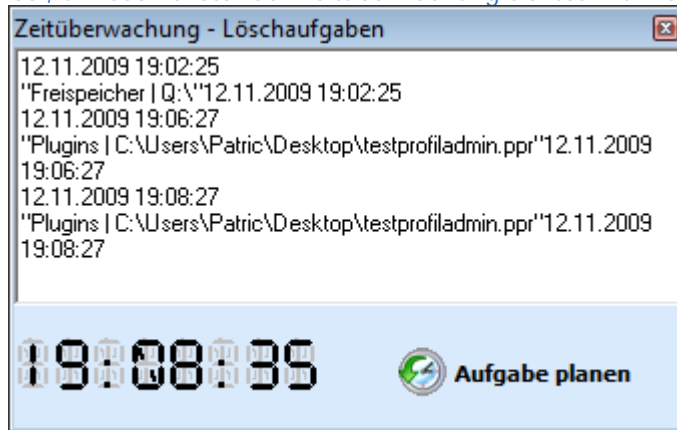
[Aufgaben-Planer](#)

Bedienung Zeitüberwachung

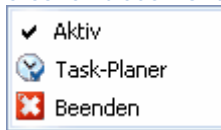
Nach dem Start sehen Sie ein Symbol im Infobereich (Tray)




Das Symbol zeigt dabei an, dass die Zeitüberwachung aktiv ist. Doppelklicken Sie auf das Symbol, um das Fenster der Zeitüberwachung sichtbar zu machen:



Sie sehen die Systemzeit und die Zeiten, zu denen bestimmte Aufgaben zu erfüllen sind. Über die Schaltfläche Aufgabe planen können Sie den Aufgaben-Planer starten. Wenn Sie den Mauszeiger über das Symbol im Infobereich bewegen und die rechte Maustaste betätigen, erscheint das Kontextmenü:



Aktiv

Über die Funktion Aktiv können Sie die Zeitüberwachung De-/Aktivieren. Im deaktivierten Zustand erscheint das Symbol  im Systemtray.

Aufgaben-Planer

Die Funktion Aufgaben-Planer ruft den Aufgaben-Planer auf.

Beenden

Beendet die Zeitüberwachung.



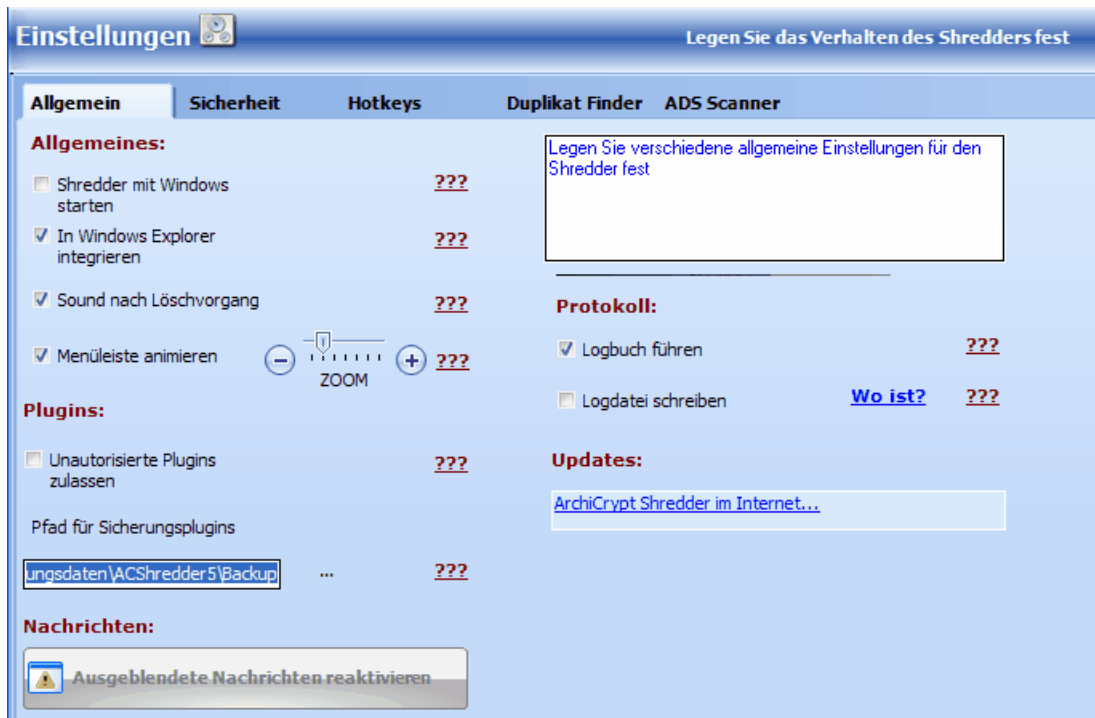
ACHTUNG: Wenn die Zeitüberwachung nicht aktiv ist, werden keine geplanten Aufgaben ausgeführt.

7 Einstellungen

7.1 Allgemeines

Einstellungen Allgemeines

siehe auch [Sicherheit](#) [Hotkeys](#) [Duplikat Finder](#) [ADS Scanner](#)



Allgemeines

Allgemeines

Shredder mit Windows starten

Bei eingeschalteter Option startet ArchiCrypt automatisch bei jedem Systemstart. ArchiCrypt Shredder können Sie nach dem Start per Doppelklick auf das Radar-Symbol im s.g. Infobereich (Systemtray) aufrufen.

siehe auch: [Kontextmenü Infobereich](#)

Symbol:



HINWEIS: *Verschiedene Antiviren- und Antispyware-Programme verhindern, dass sich Programme als Autostart in die Registry schreiben können. Stellen Sie bitte*

sicher, dass kein solches Programm ArchiCrypt Shredder daran hindert. Notfalls können Sie einen Link auf ArchiCrypt Shredder manuell in den Autostart-Ordner kopieren. Hinweise dazu finden Sie in der Hilfe zum Betriebssystem.

In Windows Explorer integrieren

Bei Ausgewählter Option können Sie den Shredder im Kontextmenü des Windows Explorers (Dateimanager) aufrufen.

siehe dazu: [Kontextmenü](#)



WICHTIG: Um die Einstellung ändern zu können, benötigt ArchiCrypt Shredder Administratorrechte!

Sound nach Löschvorgang

Bei ausgewählter Option erklingt nach jedem Löschvorgang ein Sound.

Menüleiste animieren

Bei aktivierter Funktion werden Elemente die Sie in der Menüleiste anklicken animiert (Symbole springen auf und ab). Wer die Animation als lästig empfindet, kann das Häkchen entfernen.

ZOOM:Über den Schieberegler können Sie festlegen, wie die Symbole der Menüleiste beim Überstreichen mit der Maus vergrößert werden.

Plugins

Unautorisierte Plugins zulassen

Unautorisierte Plugins sind Plugins, die nicht durch den ArchiCrypt Shredder Hersteller zur Verfügung gestellt wurden. Per Voreinstellung werden solche Plugins nicht geladen. Um diese Plugins dennoch laden und ausführen zu können, müssen Sie diese Option auswählen.



WICHTIG: Achten Sie darauf, Plugins nur von vertrauenswürdigen Quellen zu beziehen!

Pfad für Sicherungsplugins

Einige Plugins führen eine Datensicherung durch, speichern also wichtige Daten, etwa die Emaildatenbank von MS Outlook Express, in einem bestimmten Verzeichnis. Legen Sie hier das Verzeichnis fest, in dem solche Datensicherungen gespeichert werden sollen.

Nachrichten

Ausgeblendete Nachrichten reaktivieren

Bei einigen Meldungen des Shredders haben Sie die Möglichkeit, auszuwählen, dass diese künftig nicht mehr angezeigt werden sollen. Durch Betätigen dieser Schaltfläche können Sie diese Meldungen wieder reaktivieren.

Protokoll

LogBuch

Das LogBuch sollte nur in Ausnahmefällen ausgeschaltet sein. In ihm werden sämtliche Aktionen, Hinweise und Fehler aufgezeichnet.

siehe dazu [LogBuch](#)

LogDatei

Auf Wunsch können alle Aktionen in einer [Logdatei/Protokolldatei](#) gespeichert werden. Die Datei trägt den Namen [ACShredder.log](#) und wird im Nutzerverzeichnis angelegt. Die Datei wird bei jedem Start mit eingeschalteter Logdatei neu geschrieben. Sie können sich den Inhalt der Logdatei in jedem Texteditor ansehen. Sie können direkt zum Ordner mit der Logdatei springen, indem Sie auf [Wo ist?](#) klicken.



WICHTIG: Bitte beachten Sie, dass die LogDatei je nach Aktion (z.B. bei Bereinigung der Clustertips) sehr groß werden kann. Dabei bremst das Schreiben in die LogDatei den Shredder unter Umständen erheblich aus. Schalten Sie die LogDatei daher nur in Einzelfällen an. Das LogBuch hingegen können und sollten Sie bedenkenlos aktivieren.

Updates

Beim Start prüfen ob es ein Update gibt?

Sofern eine Verbindung zum Internet besteht, prüft der Shredder beim Start automatisch, ob eine neuere Version verfügbar ist.

ArchiCrypt Shredder im Internet...

Ihr Browser wird mit der ArchiCrypt Internetseite aufgerufen

Update suchen

Hier können Sie manuell prüfen, ob eine neuere Version des Shredders verfügbar ist.

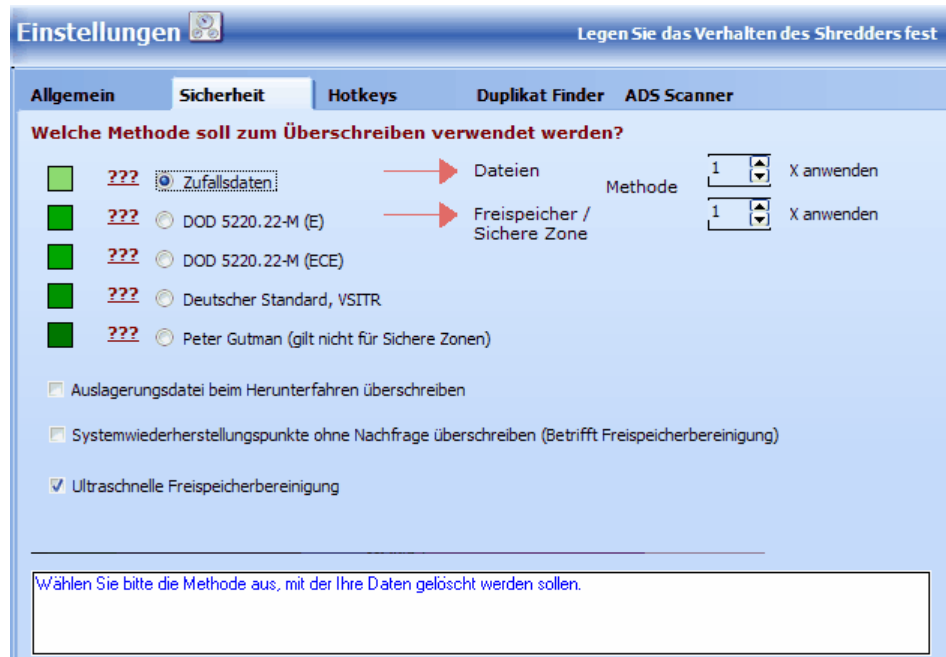


HINWEIS: Die Updatefunktionen stehen Ihnen in der Testversion und in den mobilen Versionen nicht oder nur teilweise zur Verfügung

7.2 Sicherheit

Einstellungen Sicherheit

siehe auch [Allgemeines](#) [Hotkeys](#) [Duplikat Finder](#) [ADS Scanner](#)



WICHTIG: Die Anzahl der Runden und die verwendete Methode entscheiden darüber, wie lange ArchiCrypt Shredder für das Löschen einer Datei, die Bereinigung des Freispeichers und die Säuberung von s.g. Clustertips etc. benötigt. Auf modernen Datenträgern (Baujahr nach 2000) genügt es vollkommen, als Methode Zufallszahlen zu wählen und diese 1 X anwenden zu lassen. Bei der Bereinigung des Freispeichers sollten Sie die Ultraschnelle Freispeicherbereinigung aktivieren. Diese sinnvollen Werte sind bei der Installation des Shredders bereits vorausgewählt!

Welche Methode soll zum Überschreiben verwendet werden?

Zufallsdaten

Ein Durchlauf, bei dem jedes BYTE der Originaldatei mit einem Zufallsbyte überschrieben wird. Diese Methode ist bereits sicher und schützt vor Recovery Software.



TIPP:

Nur mit **ungeheurem technischem und finanziellem Aufwand** ist es **eventuell** möglich **kleine Fragmente** der Ausgangsdaten wieder zu rekonstruieren. Kaum ein Staat dieser Welt kann entsprechende Mittel aufbringen und wird dies nur tun, wenn sich dieser erhebliche Aufwand lohnt.

In der Praxis genügt diese Methode also völlig!

(siehe [Schnelles Überschreiben](#))

DoD 5220.22-M (E)

Insgesamt wird jedes BYTE der Originaldatei 3 MAL mit einem bestimmten BYTE-Wert überschrieben.
(genaue Beschreibung siehe [DoD5220.22-M](#))

DoD 5220.22-M (ECE)

Insgesamt wird jedes BYTE der Originaldatei 7 MAL mit einem bestimmten BYTE-Wert überschrieben.
(genaue Beschreibung siehe [DoD5220.22-M](#))

Der deutsche Standard (VS-IT-Richtlinien - VSITR)

Insgesamt wird jedes BYTE der Originaldatei 7 MAL mit einem bestimmten BYTE-Wert überschrieben.
(genaue Beschreibung siehe [VSITR](#))

Peter Gutman

Jedes BYTE der Originaldatei wird in 35 Durchläufen mit ganz bestimmten BYTE-Werten überschrieben.
(genaue Beschreibung siehe [Gutman](#)). Falls Sie Sichere Zonen überwachen lassen, wird bei ausgewählter Gutman Methode die DoD Methode angewandt. Andernfalls würde die Performance Ihres Systems zu stark herabgesetzt.

Andere Löschmethoden

Andere Methoden unterscheiden sich oft nur anhand der Anzahl an Runden (Wie oft sollen die Daten überschrieben werden) oder stellen eine Kombination aus o.g. Verfahren dar. So zum Beispiel NISPOM (NSA DoD 5220.22-M ECE). Hier wird zunächst der DoD 5220.22-M Standard angewendet, anschließend wird mit Zufallsdaten überschrieben, um in einem letzten Schritt erneut DoD 5220.22-M anzuwenden.

Sofern Sie als Methode Zufallsdaten oder DoD 5220.22 M gewählt haben, können Sie festlegen, wie oft die jeweilige Methode angewendet werden soll. Beachten Sie jedoch, dass der Shredder unter Umständen riesige Datenmengen schreiben muss (Der Shredder schaltet, um wirklich sicher zu löschen den Festplattencache aus). Der Löschvorgang kann daher sehr lange Zeit in Anspruch nehmen.

Stellen Sie z.B. einen Wert bei Dateien von 40 facher Methodenwiederholung ein (nicht empfohlen!) und wählen als Methode DoD 5220.22-M, wird jedes BYTE der Originaldatei insgesamt $3 \times 40 = 120$ fach überschrieben.

Auslagerungsdatei beim Herunterfahren überschreiben

ArchiCrypt Shredder bietet Ihnen an, die Auslagerungsdatei ([pagefile.sys](#)) beim Herunterfahren des Rechners zu überschreiben.
Das Überschreiben erfolgt in einem Durchgang in dem NULLEN geschrieben werden.
Das Herunterfahren des Rechners wird dabei verlangsamt.

(siehe auch [Schwachstellen/Tipps](#))

Systemwiederherstellungspunkte ohne Nachfrage überschreiben (Betrifft XP/Vista/Windows 7 bei Freispeicher)

Die genannten Betriebssysteme speichern Dateien, die wichtig für den fehlerfreien Betrieb des Systems sind in s.g. Wiederherstellungspunkten sobald Sie wesentliche Änderungen am Betriebssystem vornehmen. Dafür reserviert das Betriebssystem Anteile auf Ihrer Festplatte und sperrt den Zugriff für Anwendungsprogramme. Wird beim täglichen Arbeiten der Platz auf dem entsprechenden Datenträger knapp und unterschreitet einen Schwellwert, so löscht das Betriebssystem die Wiederherstellungspunkte ohne Nachfrage. Dies kann im Rahmen eines Downloads, des Speicherns einer Worddatei, oder eben, wie im vorliegenden Fall, durch das Bereinigen des Freispeichers geschehen. Läuft Ihr System zum Zeitpunkt der Bereinigung stabil, können Sie die Wiederherstellungspunkte im Normalfall überschreiben lassen. Beim nächsten Systemstart legt das Betriebssystem wieder einen neuen Wiederherstellungspunkt an.

Falls diese Option ausgeschaltet ist, startet ArchiCrypt Shredder die Bereinigung ohne Rückfrage, ansonsten müssen Sie die Bereinigung zunächst bestätigen.

7.3 Hotkeys

Einstellungen Hotkeys

siehe auch [Allgemeines](#) [Sicherheit](#) [Duplikat Finder](#) [ADS Scanner](#)

Aktion:	Tastaturkürzel:
Sichere Löschzonen	Keine
Online-Spuren	Keine
Verzeichnisliste	Keine
Online-Profil	Keine

HINWEIS: Zur Vergabe eines Tastaturkürzels wählen Sie bitte zunächst eine der Aktionen aus und setzen dann den Eingabecursor in das Eingabefeld Tastaturkürzel. Betätigen Sie jetzt eine Tastenkombination (z.B. STRG + Buchstabentaste). Nach dem Speichern der Einstellungen steht das Tastaturkürzel systemweit zur Verfügung.

Mit den **Hotkeys** haben Sie schnellen Zugriff auf die wichtigsten Funktionen von ArchiCrypt Shredder. Wählen Sie die Aktion aus, die Sie mit einem **Tastaturkürzel** aufrufen möchten, setzen Sie dann den Eingabecursor in das Eingabefeld Tastaturkürzel und betätigen Sie die gewünschte Tastenkombination. Anschließend betätigen Sie bitte die Schaltfläche "Hotkeys

übernehmen".

Hotkey Sichere Löschezonen:

Startet die Überwachung der Sicheren Löschezonen

Hotkey De-/aktivieren:

Minimiert den Shredder in den Infobereich, bzw. holt den Shredder in den Vordergrund

Hotkey Online-Spuren:

Führt aktuelles Online-Profil aus und löscht.

Sofern spezielle Verzeichnisse aktiv, werden die Verzeichnisse in der Verzeichnisliste bereinigt.

Sofern Plugins ausführen aktiv, werden ausgewählte Plugins ausgeführt.

Hotkey Verzeichnisliste:

Aktuelle Verzeichnisliste wird abgearbeitet

Hotkey Online-Profil:

Aktuelles Online-Profil wird abgearbeitet. Verzeichnisliste und Plugins bleiben, anders als bei Hotkey Online-Spuren, unberücksichtigt.

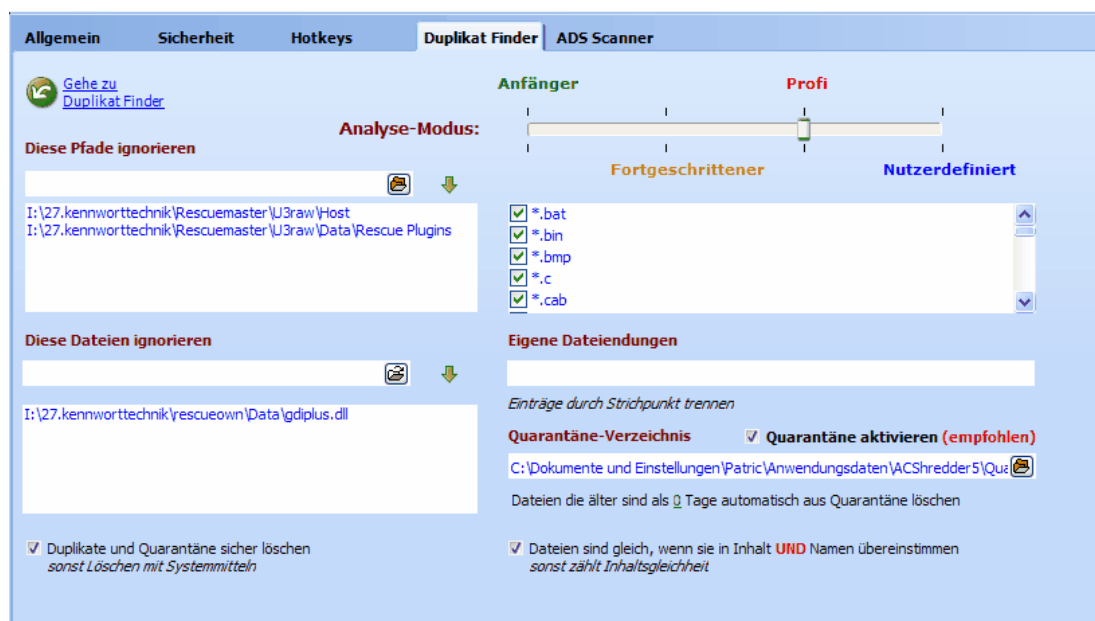
Hotkey Plugin-Profil:

Aktuelles Plugin-Profil wird abgearbeitet

7.4 Duplikat Finder

Einstellungen Duplikat Finder

siehe auch [Allgemeines Sicherheit Hotkeys Duplikat Finder ADS Scanner](#)



Die verschiedenen Analyse-Modi des Duplikat Finders



Analyse Modus

Anfänger

Datendateien mutmaßlich niedriger Bedeutung, deren Entfernung die Stabilität Ihres Systems nicht beeinträchtigen

Fortgeschrittener

Datendateien mit niedriger und hoher Bedeutung, deren Entfernung die Stabilität Ihres Systems nicht beeinträchtigen

Profi

Neben Datendateien hoher und niedriger Bedeutung werden auch Anwendungen, Treiber und andere Dateien berücksichtigt, deren Entfernung sich erheblich auf die Stabilität Ihres Systems auswirken kann.

Nutzerdefiniert

Sie können die vordefinierten Dateitypen beliebig auswählen und eigene Dateimasken/-endungen in das Feld Eigene Dateieindungen eingeben. Wenn Sie mehrere solcher Masken festlegen, trennen Sie diese bitte mittels Strichpunkt.

Sie können eigene Dateieindungen in die Suche mit einbeziehen, oder durch Angabe von * als Maske, einfach alle Dateien mit in die Analyse einbeziehen.

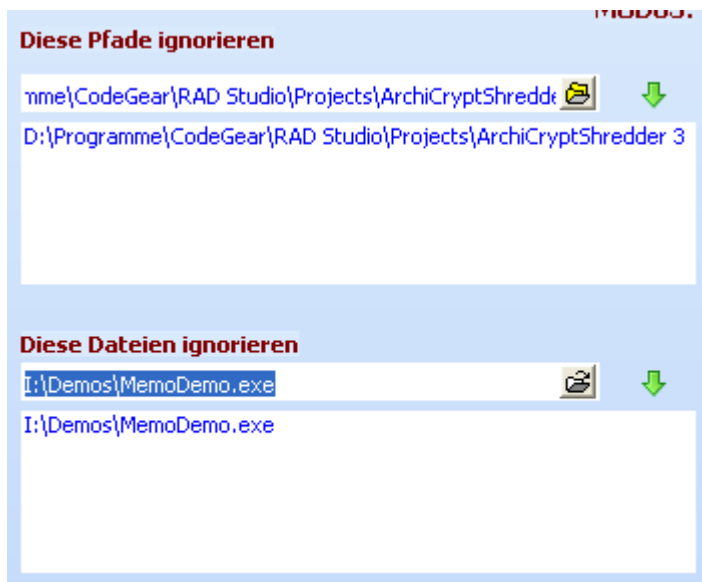
Eigene Dateieindungen

.png;.tiff|

Einträge durch Strichpunkt trennen

So schließen Sie bestimmte Verzeichnisse und Dateien von der Analyse durch den Duplikat Finder aus

Legen Sie Verzeichnisse und Dateien fest, die bei der Analyse nicht berücksichtigt werden sollen. Entweder geben Sie den Verzeichnis- oder Dateinamen direkt in das Eingabefeld ein und betätigen die grüne Pfeil-Nach-Unten Schaltfläche,



oder, Sie rufen mit der rechten Maustaste das Kontextmenü eines Eintrags in der Tabelle mit den Ergebnissen auf und wählen die entsprechende Funktion.



Kontextmenü eines Eintrags in Tabelle Duplikat Finder

Sie können einen Eintrag aus der Liste entfernen, indem Sie ihn mit der rechten Maustaste anklicken und **Löschen** wählen.

Quarantäne und Quarantäneverzeichnis

Duplikate können und **sollten** zunächst in einem **Quarantäneverzeichnis** gesichert werden.

Wenn Sie nach einer gewissen Zeit feststellen, dass das Fehlen dieses Duplikates sich tatsächlich nicht negativ auf Ihr System auswirkt, können Sie die Dateien endgültig löschen. Bei der Option **Quarantäne aktivieren** sollten Sie daher grundsätzlich ein Häkchen setzen. Im Falle eines Falles können Sie das Duplikat so mit der **Quarantäne** wieder an den ursprünglichen Ort zurückspielen.

So bereinigen Sie die Quarantäne automatisch

Dateien die älter sind als Tage automatisch aus Quarantäne löschen

Oft vergisst man, Dateien manuell aus der Quarantäne zu entfernen. Sie können in der Einstellung zum Duplikat Finder einstellen, dass ArchiCrypt Shredder bei jedem Start Einträge automatisch aus der Quarantäne entfernt, die älter als X Tage sind.



TIPP: *In der Praxis hat sich hier ein Wert von 30 als optimal erwiesen.*

Möchten Sie, dass die Duplikate nie automatisch gelöscht werden, stellen Sie den Wert auf 0.

Um den Wert zu ändern, klicken Sie bitte auf den grünen Text, der den aktuellen Wert angibt.

Löschmethode für Duplikate und Dateien in Quarantäne

Duplikate und Dateien der Quarantäne werden in der Voreinstellung sicher gelöscht. Wenn Sie bei Duplikate und Quarantäne sicher löschen kein Häkchen setzen, werden die Daten mit Systemmitteln (schneller, aber ggf. wieder herstellbar) gelöscht.

Wann sind Dateien gleich?

Grundsätzlich identifiziert ArchiCrypt Shredder eine Datei als Duplikat einer anderen Datei, wenn die Dateien inhaltlich exakt übereinstimmen. Dadurch werden auch Dateien gefunden, die andere Namen tragen. Sie können jedoch festlegen, dass nur Dateien als Duplikat gelten, die neben gleichem Inhalt auch den gleichen Dateinamen besitzen (**Dateien sind gleich, wenn sie in Inhalt und Namen übereinstimmen**).

7.5 ADS Scanner

Einstellungen ADS Scanner

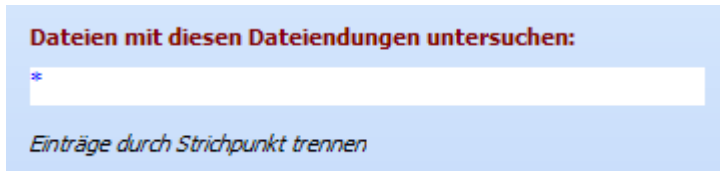
siehe auch [Allgemeines](#) [Sicherheit](#) [Hotkeys](#) [Duplikat Finder](#) [Duplikat Finder](#)

The screenshot shows the 'ADS Scanner' settings window. At the top, there are tabs for 'Allgemein', 'Sicherheit', 'Hotkeys', 'Duplikat Finder', and 'ADS Scanner'. The 'ADS Scanner' tab is selected. Below the tabs, there is a 'Gehe zu ADS Scanner' button with a green arrow icon. The main area is divided into four sections:

- Diese Pfade ignorieren:** A text input field with a green arrow button to its right.
- Diese Dateien ignorieren:** A text input field with a green arrow button to its right.
- Dateien mit diesen Dateieendungen untersuchen:** A text input field containing the character '*'. Below it, the text 'Einträge durch Strichpunkt trennen' is displayed.
- Streams mit diesen Namen ignorieren:** A text input field with a green arrow button to its right.

So legen Sie fest, welche Dateien der ADS Scanner untersuchen soll

In den Einstellungen können Sie unter "Dateien mit diesen Dateieindungen untersuchen" festlegen, welche Dateien ArchiCrypt Shredder auf das Vorhandensein von **Alternativen Datenströmen** untersuchen soll.



Wenn Sie mehrere solcher Masken festlegen, trennen Sie diese bitte mittels Strichpunkt. Durch Angabe von * als Maske werden einfach alle Dateien mit in die Analyse einbezogen.

Beispiel:

Wenn Sie z.B. *.doc und A*.xls angeben, untersucht der ADS Scanner alle Dateien, die die Dateieindung doc tragen und alle Dateien, der Name mit A beginnt und deren Dateieindung xls ist.

So schließen Sie bestimmte Dateien und Verzeichnisse von der Analyse aus

Es kann durchaus sinnvoll sein, bestimmte Dateien und oder Verzeichnisse nicht mit in die Analyse einzubeziehen. Dazu können Sie einen Pfad oder eine Datei gezielt im Windows Dialog in den Einstellungen des ADS Scanners auswählen und anschließen über die grüne Pfeil-nach-unten Schaltfläche in die entsprechende Liste übernehmen, oder Sie betätigen nach einer Analyse die rechte Maustaste über einem Eintrag des Analyseergebnisses und wählen die gewünschte Funktion.

So schließen Sie Datenströme mit bestimmtem Namen aus

Einige Anwendungen, darunter einige Programme aus der Kategorie Antivirus und Antispyware nutzen Alternative Datenströme, um sich zu einer Datei bestimmte Zusatzinformationen zu merken (Ergebnis der letzten Untersuchung, wann zuletzt untersucht etc.). Da diese Alternativen Datenströme dadurch massenhaft auftreten können und so den Blick vom Wichtigen ablenken könnten, kann man solche Dateiströme mit in die Liste übernehmen. Entweder tragen Sie den Namen eines solchen Datenstroms in die Liste manuell ein, oder Sie betätigen nach einer Analyse die rechte Maustaste über einem Eintrag des Analyseergebnisses und wählen die gewünschte Funktion im Kontextmenü aus.



HINWEIS: Sie können Datenströme, die von Antivirensoftware stammt, gefahrlos wieder entfernen. Allerdings dauert der nächste Scanndurchlauf des Virens scanners dann evtl. wieder länger.

8 Plugin Editor

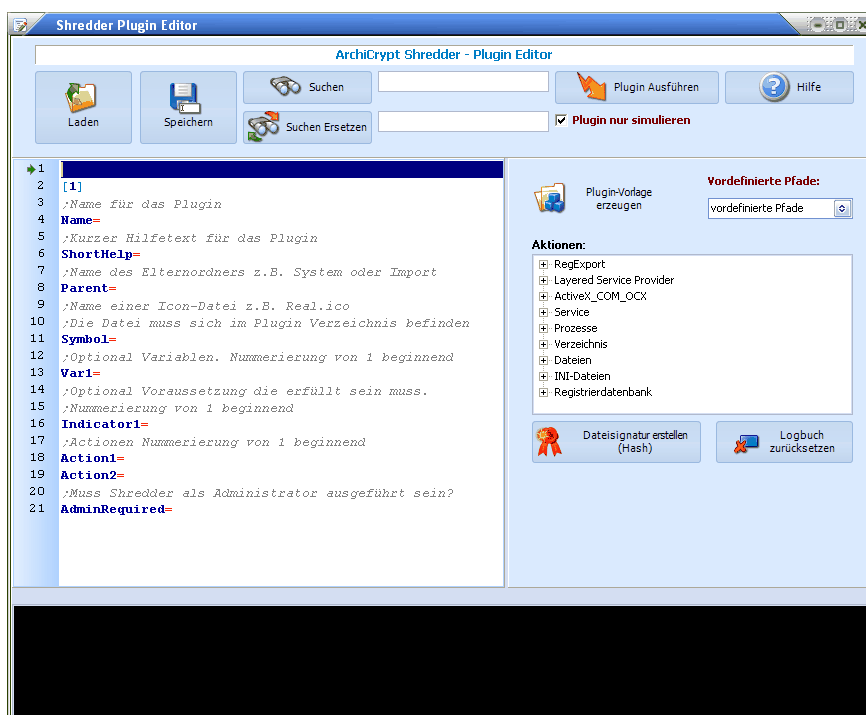
8.1 Einleitung Plugin Editor

8.1.1 Willkommen

Der Plugin-Editor

Den Plugin Editor können Sie in unserer [ArchiCrypt Freeware Zone](#) downloaden!

Dieses Kapitel beschreibt den Aufbau der so genannten ActionScripts/Plugins für ArchiCrypt Shredder. Um die ActionScripts zu erstellen genügt ein einfacher Texteditor. Wesentlich einfacher kann man die Plugins jedoch mit dem kostenlosen Shredder Plugin Editor erstellen.



Plugins sollten Sie nur erstellen, wenn Sie sich mit dem System sehr gut auskennen. Bevor Sie ein Plugin an andere weitergeben, führen Sie bitte ausführliche Tests durch. Bitte beachten Sie, dass Sie ausschließlich s.g. nicht autorisierte Plugins erstellen können. Nutzer von ArchiCrypt Shredder müssen das Laden solcher Plugins ausdrücklich erlauben.

8.2 Plugin Aufbau

8.2.1 Überblick

Nachdem das Plugin fertiggestellt wurde, muss es zusammen mit der Symboldatei (Icondatei) im Pluginverzeichnis des Shredders gespeichert werden. Das Plugin muss die Endung .ukn tragen. Im Shredder muss das Laden unautorisierter Plugins erlaubt sein!

Ein Plugin hat immer folgenden Aufbau:

[1]

Die [1] muss zwingend angegeben werden und ist Bestandteil eines jeden ActionScripts

Name=

Name für das Plugin. Dieser erscheint beim Shredder in der Pluginübersicht

ShortHelp=

Kurzer Hilfetext für das Plugin. Der Hilfetext wird angezeigt, wenn der Nutzer die Maus über das Plugin bewegt.

Parent=

Name des Elternordners z.B. System oder Import. Ihr Plugin wird unterhalb dieses Ordners aufgelistet.

Symbol=

Name einer Icon-Datei z.B. Real.ico. Das Symbol wird neben dem Plugin angezeigt. Die Icondatei muss sich im Plugin Verzeichnis des Shredders befinden.

Var1=

Optional(muss nicht aufgeführt sein). Nummerierung aufsteigend, bei 1 beginnend. In der Nummerierung dürfen sich keine Lücken befinden.

Beispiel:

Var2=Test

Var3=Test2

ist falsch, da nicht bei 1 begonnen wurde.

Var1=test1

var3=test3

falsch, da Lücke in der Nummerierung.

Var3=test3

Var2=test2

Var1=test1

falsch, da nicht auf-, sondern absteigend.

Indicator1=

Optional(muss nicht aufgeführt sein). Für die Nummerierung gelten die gleichen Regeln, wie bei Variablen.

Action1=

Aktionen die ausgeführt werden sollen. Falls Indikatoren aufgeführt sind, werden die Aktionen nur dann ausgeführt, wenn die Indikatoren erfüllt sind.

AdminRequired=

Benötigt man zum Ausführen des Plugins Administratorrechte, müssen Sie true angeben, ansonsten false.

8.2.2 Vordefinierte Pfade

Die vordefinierten Pfade können Sie als Variable an jeder Stelle des ActionScripts einfügen.

%OUTLOOKEXPRESS%

z.B.: C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen
 \Anwendungsdaten\Identities\{1564B27A-C733-44C9-8FEB-ED14A1259380}
 \Microsoft\Outlook Express

%OWN% =Anwendungspfad

z.B.: C:\Programme\ArchiCrypt Live

%APPDATA% = ApplicationData

z.B.: C:\Dokumente und Einstellungen\Schneider\Anwendungsdaten

`%CAPPDATA%` =CommonAppData

z.B.: C:\Dokumente und Einstellungen\All Users\Anwendungsdaten

`%CSTARTUP%` =CommonStartup

z.B.: C:\Dokumente und Einstellungen\All Users\Programme\AutoStart

`%DESKTOP%` =Desktop

z.B.: C:\Dokumente und Einstellungen\Schneider\Desktop

`%FAVORITES%` =Favorites

z.B.: C:\Dokumente und Einstellungen\Schneider\Favoriten

`%FONTS%` =FONTS

z.B. : C:\WINNT\FONTS

`%HISTORY%` =History

z.B.: C:\Dokumente und Einstellungen\Schneider\Lokale Einstellungen\Verlauf

`%NETHOOD%` =NetHood

z.B.: C:\Dokumente und Einstellungen\Schneider\Netzwerkumgebung

`%CACHE%` =Cache

z.B.: C:\Dokumente und Einstellungen\Schneider\Lokale Einstellungen\Temporary Internet Files

`%COOKIES%` =Cookies

z.B.: C:\Dokumente und Einstellungen\Schneider\Cookies

`%RECENT%` =Recent

z.B.: C:\Dokumente und Einstellungen\Schneider\Recent

`%SENDTO%` =SendTo

z.B.: C:\Dokumente und Einstellungen\Schneider\SendTo

`%STARTMENU%` =StartMenu

z.B.: C:\Dokumente und Einstellungen\Schneider\Startmenü

`%STARTUP%` =Startup

z.B.: C:\Dokumente und Einstellungen\Schneider\Startmenü\Programme\Autostart

`%SYSTEM%` =SystemDirectory

z.B.: C:\WINNT\System32

`%WINDIR%` =WindowsDirectory

z.B.: C:\Windows

`%TEMP%` =TempPath

z.B.: C:\Dokumente und Einstellungen\Schneider\Lokale Einstellungen\Temp\

`%PROGRAMS%` =ProgramFiles

z.B.: C:\Programme\

`%OPERAEXE%` =Pfad zu Opera.exe

z.B. C:\Programme\Opera7

%OPERA6% = Pfad zu Opera Nutzerdaten (Cache, History etc.)

z.B.: C:\Dokumente und Einstellungen\Administrator\Anwendungsdaten\Opera\Opera7

%USERDEF% = Nutzerdefinierter Pfad; Wird durch das Programm zur Verfügung gestellt. Sinnvoll, wenn man Plugins realisiert, die zum Beispiel Daten sichern. So kann man die Daten in ein Nutzerdefiniertes Verzeichnis sichern!

%WINMAIL% = Pfad in dem Windows Mail (Windows Vista E-Mail Programm; Nachfolger von Outlook Express) die Daten für das Programm ablegt!

8.2.3 Variablen

Es gibt grundsätzlich 3 Arten von **Variablen**. Eine Art besteht aus reiner Textinformation und wird an der Stelle eingesetzt, an der in der restlichen Definitionsdatei der Platzhalter auftaucht. Sie dient also primär dem Zweck der Schreibbarbeitersparnis.

Die zweite Art dient dazu, Werte auf dem Zielsystem zu ermitteln, die von Rechner zu Rechner verschieden sind. Sie repräsentieren also unbekannte Größen, die erst auf dem Rechner, auf dem das Skript ausgeführt wird, ermittelt werden können. Im Wesentlichen wird es sich um Pfade und Dateinamen handeln, die man aus der Registrierungsdatei oder Initialisierungsdateien ausliest, um anschließend Aktionen in den Verzeichnissen oder mit den Dateien auszuführen.

Die dritte Art sind Größen, die der Nutzer interaktiv angeben kann. Diese werden mit Hilfe von Dialogen ermittelt!

Textvariablen

Variablen werden immer durch das Schlüsselwort VAR mit anschließender Nummer eingeleitet. Die Nummerierung muss immer bei 1 beginnen, muss aufsteigend erfolgen und darf keine Lücken in der Nummerierung enthalten. Die Variablen werden genutzt, wenn man an die Stelle, an der die aufgelöste Variable eingesetzt werden soll, die Nummer der Variablen eingebettet in **%%%** einfügt.

Beispiel:

VAR1=Erste Variable

VAR2=Zweite Variable und %1%

VAR3=Dritte Variable und %2%

%%3% wird also aufgelöst zu Dritte Variable und Zweite Variable und Erste Variable

Werte auf Zielsystem

Mit VAR können Sie Werte aus der Registry oder aus Initialisierungsdateien auslesen und im weiteren ActionScript verwenden.

VAR#=HKEY or IniFilename or Text|VarSpecific

Falls HKEY, dann HKEY=(HKEY_CURRENT_USER|HKEY_LOCAL_MACHINE|HKEY_CLASSES_ROOT|HKEY_CURRENT_CONFIG|HKEY_USERS)

Varspecific=Pfad|KeyName

Beispiel:

```
VAR1 = HKEY_CURRENT_USER | Software\Microsoft\MediaPlayer\Setup
\CreatedLinks|AppName
```

Die Variable VAR1 wird auf einem System zum Beispiel aufgelöst zu C:\PROGRAM~1\WINDOW~2\wmpplayer.exe

Falls IniFileName,

muss der Name der Initialisierungsdatei mit komplettem Pfad angegeben werden. Der Name der Datei muss dabei zwingend die Endung ini besitzen!

VarSpecific=Section|Name

Beispiel:

```
VAR1 = %WINDIR%\win.ini|T-Online Software|browser4
```

Die Variable VAR1 wird auf einem System zum Beispiel aufgelöst zu C:\T-Online\Browser\

Nutzerdefinierte Pfade

VAR#=ASKPATH oder ASKFILE|Dialogüberschrift|Startverzeichnis

Falls ASKPATH, wird der Nutzer aufgefordert, ein Verzeichnis auszuwählen. Das gewählte Verzeichnis steht anschließend als Verzeichnis in der Variablen zur Verfügung. Mit Dialogüberschrift legen Sie den Text fest, der im Dialog als Überschrift angezeigt wird. HINWEIS: Legen Sie eine aussagekräftige Überschrift fest, da der Nutzer ansonsten im Rahmen der Ausführung mehrerer Anfragen nicht erkennen kann, für welche Aktion die Abfrage erfolgt. Mit Startverzeichnis legen Sie fest, welches Verzeichnis der Dialog bei Start anzeigen soll.

Falls ASKFILE, wird der Nutzer aufgefordert, einen Dateinamen auszuwählen oder einzugeben. Weiteres siehe ASKPATH.

Beispiel:

```
VAR1=ASKPATH|Zielverzeichnis für Outlook Express Ordner|C:\
```

8.2.4 Indikatoren

Indikatoren sind Voraussetzungen, die vorliegen müssen, damit die Aktionen ausgeführt werden. Dabei können mehrere Indikatoren angegeben werden.

In einem Indikator können mehrere Voraussetzungen angegeben werden, indem diese durch die Zeichenfolge +or+ getrennt werden. Ein solcher Indikator ist erfüllt, wenn wenigstens einer der durch +or+ getrennten Indikatoren wahr ist. Besonders nützlich ist diese Funktion, wenn die Aktionen nur für bestimmte Betriebssysteme gedacht sind.

Beispiel:

```
Indicator1 = OSW95 +or+ OSW98 +or+ osw98se
```

Dieser Indikator wird mit wahr gewertet, wenn es sich um das Betriebssystem Windows 95, 98 oder 98 Second Edition handelt.

Indikatoren, die in unterschiedlichen Zeilen stehen, werden logisch mit UND verknüpft. D.h. Jeder Indikator muss erfüllt sein.

Beispiel:

```
Indicator1 = OSW95 +or+ OSW98 +or+ osw98se
```

```
Indicator2 = %WINDIR%\Virus.ini
```

Die Aktionen werden nur dann ausgeführt, wenn es sich um eines der aufgeführten Betriebssysteme handelt und die Datei Virus.ini im Windowsverzeichnis vorhanden ist.

Indicator#=

Betriebssystem

OSW95|OSW98|OSW98SE|OSWME|OSWNT|OSW2K|OSWXP

Pfad, Datei

Angabe Pfad oder Dateiname.

Registry

Aufbau:

HKEY|Pfad|[Value]|Refkind|[VALUEREf]

Besonderheit bei Value: Angabe von Standard führt dazu, dass der Wert (Standard) aus der Registry ausgelesen wird.

Refkind: s|n|b

HKEY: HKEY_CURRENT_USER|HKEY_LOCAL_MACHINE|HKEY_CLASSES_ROOT|

HKEY_USERS

Value ist optional. Falls vorhanden, wird geprüft, ob Value existiert. Falls RefKind gesetzt ist, muss auch ValueRef angegeben sein! Bitte beachten, dass jeder Eintrag die Angabe des vorausgehenden voraussetzt! Also HKEY|Pfad|Refkind|VALUEREf keinen Sinn macht und zum Fehler führt!!!

Dabei gilt:

Ist RefKind s, wird ValueRef als String angesehen.

Ist RefKind n, wird ValueRef als Number (Ganzzahl) angesehen.

Ist RefKind b, wird ValueRef als Boolean (Wahrheitswert) angesehen, 0 bedeutet Falsch, 1 bedeutet wahr.

8.2.5 Aktionen

8.2.5.1 Überblick

Mit Aktion werden die Anteile im ActionScript bezeichnet, die etwas auf dem System ausführen. ArchiCrypt Shredder unterstützt eine Vielzahl an unterschiedlichen Aktionen.

Eine Aktion ist grundsätzlich wie folgt aufgebaut:

Action#=actiontype|ActionTypeSPECIFIC

#steht dabei für eine fortlaufende Nummer beginnend bei 1. Bei der Nummerierung darf keine Lücke entstehen.

actiontype steht für einen Aktionstyp,

ActionTypeSpecific für weitere Parameter, deren Aufbau und Bedeutung vom Actiontype abhängen.

8.2.5.2 Registry

Der besseren Übersicht halber sind die Aktionen in verschiedene Rubriken unterteilt.

`actiontype= reg`
`ActionTYPESPECIFIC = (DELKEY|DELVALUE|SETVALUE)`

Falls `DELKEY` dann `HKEY|Pfad|`
 Schlüssel und alle darin befindlichen Einträge werden gelöscht

Beispiel:

`Action1=reg/DELKEY/HKEY_CURRENT_USER/Software\Netscape\Netscape
 \7.01 (de)\Main`

Löscht den Pfad aus der Registry

Falls `DELVALUE` dann `HKEY|PFAD|VALUENAME`
 Valuename wird gelöscht, Valuename und Pfad können Wildcards beinhalten (*,?)

Beispiel:

`Action1=reg/DELVALUE/HKEY_CURRENT_USER/Software\Netscape
 \Netscape\7.01 (de)\Main\Install Directory`

oder

`Action3=reg/DELVALUE/HKEY_CURRENT_USER/Software\RealNetworks
 \RealPlayer\6.0\Preferences\MostRecentClips*/*`

Findet Registryeinträge wie

`Software\RealNetworks\RealPlayer\6.0\Preferences\MostRecentClips1
 Software\RealNetworks\RealPlayer\6.0\Preferences\MostRecentClips2
 Software\RealNetworks\RealPlayer\6.0\Preferences\MostRecentClips3
 Software\RealNetworks\RealPlayer\6.0\Preferences\MostRecentClipsk
 Software\RealNetworks\RealPlayer\6.0\Preferences\MostRecentClipsjkljklj`

*Und löscht in den Registryverzeichnissen wegen * alle Werte!*

Beispiel:

`Action1=reg/DelVALUE/HKEY_CURRENT_USER/Software\Netscape\Netscape
 \7.01 (de)\Main/*`

*Löscht alle Einträge im angegebenen Zweig der Registry. Unterzweige
 werden nicht angetastet!*

Löscht den entsprechenden Eintrag

Falls `SETVALUE`, dann `HKEY|PFAD|VALUENAME|VALUEKIND|VALUE`

Dabei gilt:

Ist `VALUEKIND s`, wird `VALUE` als String angesehen.

Ist `VALUEKIND n`, wird `VALUE` als Number (Ganzzahl) angesehen.

Ist `VALUEKIND b`, wird `VALUE` als Boolean (Wahrheitswert) angesehen, 0 bedeutet
 Falsch, 1 wahr

Es wird notfalls ein komplett neuer Pfad mit entsprechendem Value angelegt. Soll der Eintrag Standard erstellt werden, ist der Wert Standard bei Valuenamen zu übergeben.

Beispiel:

```
Action1=reg/SETVALUE/HKEY_CURRENT_USER/Software\Netscape  
\Netscape\7.01 (de)\Main\Install Directory\s\C:\Programme\Netscape  
\Netscape\
```

setzt den entsprechenden Wert in der Registry.

8.2.5.3 File

`actiontype= file`

`ActionTYPESPECIFIC = (DELETE|REBOOTDELETE|RENAME|MOVE|COPY)`

Falls `DELETE`, dann `DELETE|FILENAME|(++|--)`

++ bedeutet rekursiv

-- bedeutet nur in diesem Verzeichnis

++ oder -- muss zwingend angegeben werden!!

Der Dateiname darf dabei Wildcards enthalten.

Falls `REBOOTDELETE`, dann `REBOOTDELETE|FILENAME|(++|--)`

Dateien werden beim nächsten Booten gelöscht. Wichtig für Dateien, die bereits beim Bootvorgang vom Betriebssystem exklusiv geöffnet werden (Z.B. Index.dat Dateien).

Falls `RENAME`, dann `RENAME|FILENAME|NEWFILENAME`

Newfilename ohne Pfad

Datei wird umbenannt.

Falls `MOVE`, dann `MOVE|FILENAME|TARGETPATH`

FILENAME wird nach TARGETPATH verschoben.

Wildcards bei Dateiname in FILENAME erlaubt

Falls `COPY`, dann `COPY|FILENAME|TARGETPATH`

FILENAME wird nach TARGETPATH kopiert.

Wildcards bei Dateiname in FILENAME erlaubt

8.2.5.4 Path

`actiontype= path`

`ActionTYPESPECIFIC = DELETEPATH|CREATEPATH`

`ACTION#=path|delpath|Path|[INCLUDEPATH]`

Beispiel:

```
Action1=path/delpath/%temp%
```

DELPATH sorgt dafür, dass alle im Verzeichnis Path enthaltenen Dateien und Unterverzeichnisse gelöscht werden.

Wird "`INCLUDEPATH`" angegeben, wird das Verzeichnis Path ebenfalls gelöscht,

ansonsten nur die darin enthaltenen Daten und Verzeichnisse. Dies ist wichtig, wenn man zum Beispiel sicherstellen möchte, dass nur die Inhalte eines Systemverzeichnisses gelöscht werden, nicht aber das Verzeichnis selbst.

8.2.5.5 Process

`actiontype= proc`
`ActionTYPESPECIFIC = KILL|CREATE|CREATEANDWAIT`

Falls `CREATE`, dann `CREATE|FILEPATH`
 Startet den Prozess und führt Folgeaktionen sofort aus

Beispiel:
`ACTION1=proc|CREATE|%OWN% \Signatur.exe`

Startet die Datei Signatur.exe, die sich im Anwendungspfad befinden muss. Eine Folgeaktion wird sofort ausgeführt.

Falls `CREATEANDWAIT`, dann `CREATEANDWAIT|FILEPATH`

Beispiel:
`ACTION1=proc|CREATEANDWAIT|%OWN% \Signatur.exe`

Startet die Datei Signatur.exe, die sich im Anwendungspfad befinden muss. Eine Folgeaktion wird erst ausgeführt, wenn Signatur.exe beendet wurde.

Falls `KILL`, dann `KILL|(HASH|FILENAME|FULLPATH)|(<Hashwert>, <DateinameOhnePfad>, <Dateiname mit Pfad>)`

Beispiel:
`ACTION1=proc|KILL|HASH/4ADCFFBAF057D719E58F3BCF47EACB314ADCFFBAF057D719E58F3BCF47EACB31`

Killt den Prozess, dessen Datei den Hashwert 4ADCFFBAF057D719E58F3BCF47EACB314ADCFFBAF057D719E58F3BCF47EACB31 liefert.

Die Methode HASH ist sehr genau. Sie stellt sicher, dass ein genaues Abbild der Ausgangsdatei berücksichtigt wird. Dabei ist es gleich, wenn die ausführbare Datei umbenannt wurde. Wichtig ist lediglich der Inhalt der ausführbaren Datei.

Beispiel:

Das Beispiel ActionScript:

- Startet Notepad im Windows Verzeichnis, wartet dabei nicht auf das Beenden des Prozesses.
- Startet Calc im Systemverzeichnis und wartet darauf, dass der Taschenrechner beendet wird
- Sobald Calc beendet wird, wird Notepad automatisch beendet

[1]
 Name=Kill Notepad

```

Parent=System
ShortHelp=Kill NotePad
Symbol=Dateisuche.ico
action1=proc/CREATE/% WINDIR% \notepad.exe
action2=proc/CREATEANDWAIT/% SYSTEM% \calc.exe
action3=Proc/KILL/FILENAME/notepad.exe

```

8.2.5.6 Service

```

actiontype=serv
ActionTYPESPECIFIC = (DEACTIVATE|ACTIVATE|DELETE)|Dienstname

```

ACHTUNG: Zur Ausführung werden unter NT Systemen Adminrechte benötigt!
Den Dienstnamen erhält man, indem man im Dienstemanager den Service markiert und im Kontextmenü den Eigenschaftsdialog aufruft. Der Dienstname befindet sich auf der Registerkarte ALLGEMEIN oben.

Beispiel:

```

Action1=serv/DEACTIVATE/wuausev
Der Windows Dienst für Auto-Updates wird angehalten.

```

8.2.5.7 Inifiles

```

ActionType=ini
ActionTYPESPECIFIC=(DELSECTION|DELVALUE|SETVALUE)|ININAME|[SECTIONNAME]|
[VALUEKEYNAME]|[VALUEKIND]|[NEWVALUE]

```

Falls **DELSECTION**, dann DELSECTION|ININAME|SECTIONNAME. Sektion und alle Einträge werden aus der IniDatei entfernt.

Beispiel:

```

ACTION1=ini/DELSECTION/C:\Scanner.ini/ET

```

Falls **DELVALUE**, dann DELVALUE|ININAME|SECTIONNAME|VALUE.

Value darf dabei Wildcards (* und ?) enthalten. Die passenden Werte werden aus der INI-Datei entfernt.

Beispiel:

```

ACTION1=ini/DELVALUE/C:\Scanner.ini/ET2/ein*

```

Entfernt Einträge wie ein, eins, Einhorn, ein Mann, etc. aus der Inidatei C:\Scanner.ini, Sektion ET2.

Falls **SETVALUE**, dann INIFILE|SECTIONNAME|VALUEKEYNAME|VALUEKIND|VALUE

Dabei gilt:

Ist VALUEKIND s, wird VALUE als String angesehen.

Ist VALUEKIND n, wird VALUE als Number (Ganzzahl) angesehen.

Ist VALUEKIND b, wird VALUE als Boolean (Wahrheitswert) angesehen, 0 bedeutet Falsch, 1 wahr.

Es wird notfalls eine komplett INI Datei mit entsprechender Sektion und Value angelegt.

Beispiel:

ACTION1=ini/SETVALUE/C:\Scanner.ini/ET2/drei/s/Dritter Eintrag

8.2.5.8 COM

Active X / COM / OCX

actiontype= COM

ActionTYPESPECIFIC = (REGISTER|UNREGISTER)|FULLPATH

Falls REGISTER, dann REGISTER|FULLPATH

Falls UNREGISTER, dann UNREGISTER|FULLPATH

Es können DLL, TLB und EXE COM registriert und deregistriert werden. Die Dateiendung ist dabei entscheidend, auf welche Art die Engine die Datei behandelt!!

Beispiel:

Action1=com/Register/C:\Programme\Borland\Delphi7\Demos\ActiveX\ShellExt\Contmenu.dll

Action2=com/UnRegister/C:\Programme\Borland\Delphi7\Demos\ActiveX\ShellExt\Contmenu.dll

Action3=com/Unregister/%SYSTEM%\CFX32.ocx

Action4=com/Register/%SYSTEM%\CFX32.ocx

8.2.5.9 Layered Service Provider

Administratorrechte nötig. Gefährlich!!!

actiontype= lsp

ActionTYPESPECIFIC = KILL|(HASH|FILENAME|FULLPATH)|(<Hashwert>, <DateinameOhnePfad>, <Dateiname mit Pfad>)

Falls KILL, dann KILL|(HASH|FILENAME|FULLPATH)|(<Hashwert>, <DateinameOhnePfad>, <Dateiname mit Pfad>)

Beispiel:

ACTION1=lsp/KILL/HASH/

4ADCFFBAF057D719E58F3BCF47EACB314ADCFFBAF057D719E58F3BCF47EACB31

Meist werden Layered Service Provider nur mit dem Namen verzeichnet. Daher sollte man die Methoden FULLPATH und HASH nur verwenden, wenn das entsprechende Programm die Informationen auch in der Registrierung ablegt! Erfolg hat man meist mit dem DLL Namen.

ACHTUNG: Niemals manuell an diesen Werten etwas ändern!!!

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001

Eintrag PackedCatalogItem = Typ REG_BINARY In RegEdit Eintrag auswählen und Ändern aufrufen. Jetzt kann man prüfen, ob der ganze Pfad, oder nur der DLL Name gespeichert werden. Unbedingt auch die Folgeeinträge \000000000002 etc. prüfen. Vor dem DLL Namen darf auf keinen Fall die Bytefolge 00 00 auftauchen!! Es zählt nur das, was vor dieser Bytefolge steht.

8.2.5.10 RegExport

Funktion zum Import und Export von Registryschlüsseln. Beherrscht das Format Regedit 4!

`actiontype= regex`
`ActionTYPESPECIFIC = (EXPORT|IMPORT)`

Falls `EXPORT`, dann

`HKEY|PATH|TARGETFILENAME`

TARGETFILENAME ist dabei die Datei, in der die Schlüssel und Werte aus der Registry abgelegt werden sollen.

Beispiel:

Action1: regex/EXPORT/ HKEY_CLASSES_ROOT /CLSID/% OWN% \CLSID.bup

Falls `IMPORT`, dann

`SOURCEFILENAME`

SOURCEFILENAME ist dabei die Datei, die zuvor über die Exportfunktion erstellt wurde.

Beispiel:

Action1: regex/IMPORT/% OWN% \CLSID.bup

9 Pro Script Editor

9.1 Hilfe zur Hilfe

Symbole

Innerhalb der Hilfe sind besondere Textstellen durch bestimmte Symbole hervorgehoben.



UNBEDINGT LESEN

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, sollten Sie unbedingt lesen. Sie weisen häufig auf Gefahrenquellen, Fehlerfallen oder Einschränkungen hin oder beschreiben wichtige Sachverhalte.



WICHTIGE HINWEISE

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, enthalten wichtige Informationen über Verhaltensweisen der Software und technische Hintergründe.



TIPP

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, geben Ihnen wertvolle weiterführende Hinweise.



EXPERTENTIPP

Textstellen, die mit einem solchen Symbol gekennzeichnet sind, enthalten Hinweise für fortgeschrittene Anwender. Sie weisen weitergehende Möglichkeiten der Software auf oder beschreiben technische Hintergründe.

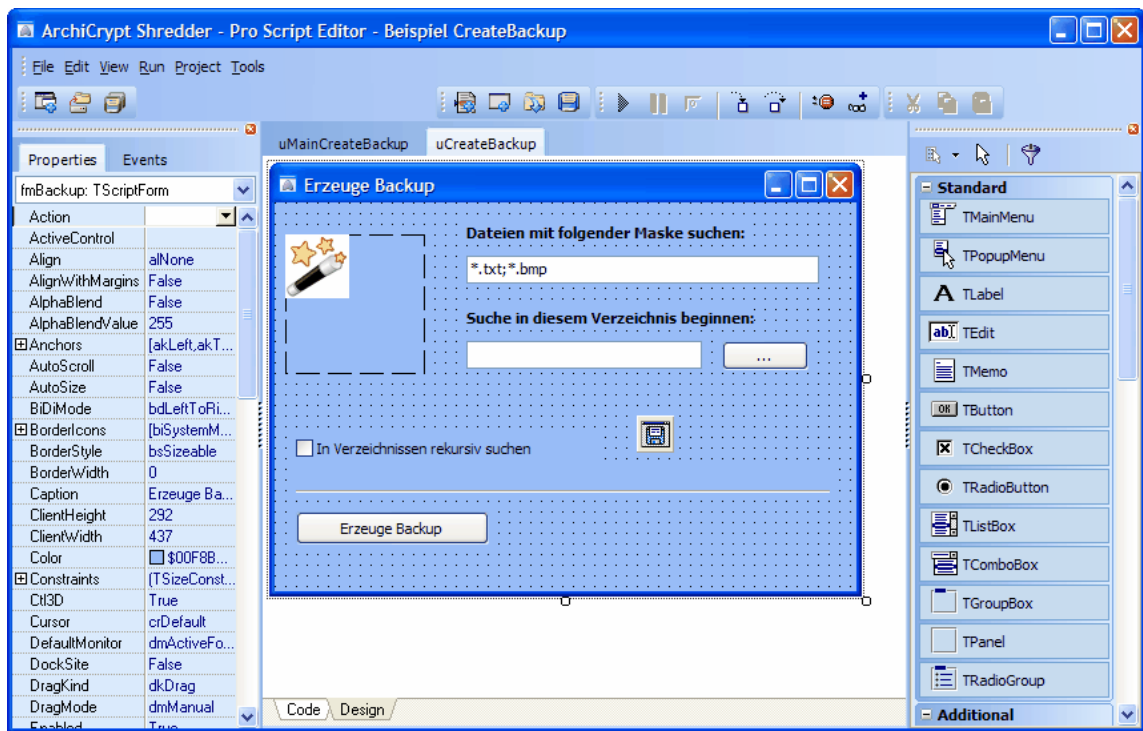
9.2 Einleitung

9.2.1 Willkommen



ArchiCrypt Pro Script Editor ist eine Entwicklungsumgebung für ArchiCrypt Pro Scripte.

Den Pro Script Editor können Sie in unserer [ArchiCrypt Freeware Zone downloaden!](#)



ArchiCrypt Pro Script Editor basiert auf dem TMS Scriter Studio Pro der Firma TMS Software (www.TMSSoftware.com)

Diese kurze Einleitung kann kein Handbuch für angehende Programmierer oder Laien sein. Programmierer finden sich in der Entwicklungsumgebung sicher schnell zurecht. Wer Borland Delphi kennt, wird sich schnell in den Editor einarbeiten können und brauchbare Plugins erzeugen.

9.3 Kurze Einführung

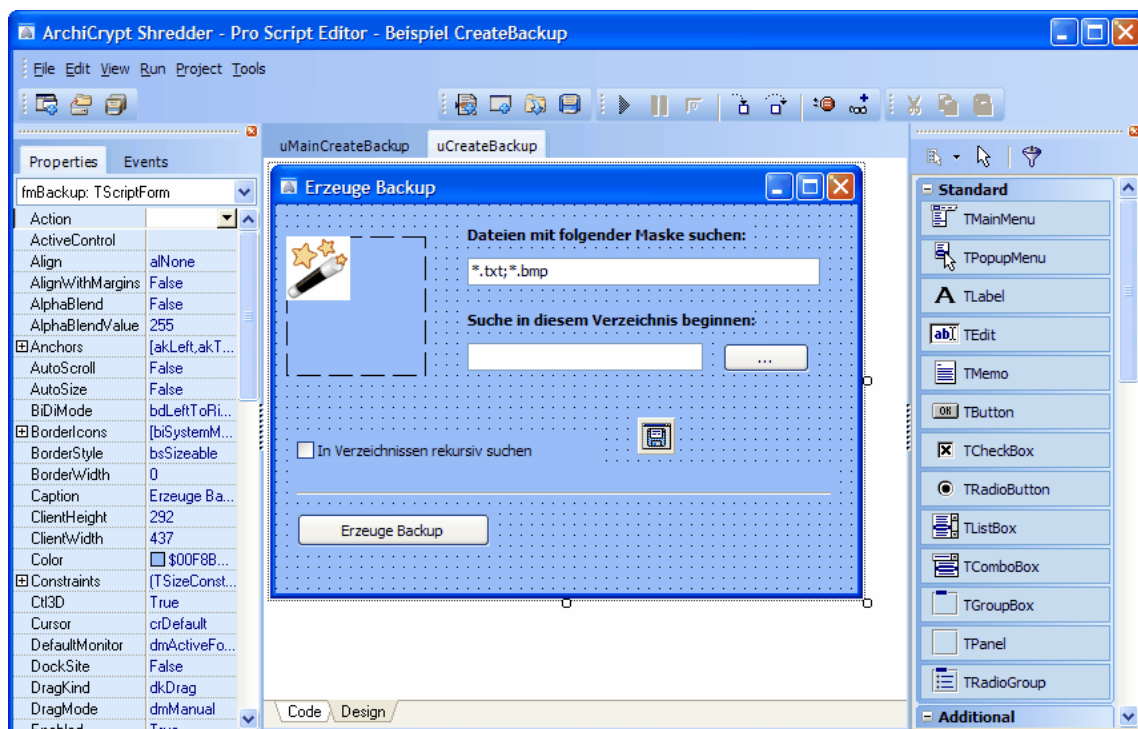
9.3.1 Voraussetzungen

Den Pro Script Editor können Sie in unserer [ArchiCrypt Freeware Zone downloaden!](#)

Um mit ArchiCrypt Pro Script Editor produktiv arbeiten zu können, sollten Sie bereits **Programmiererfahrung** mitbringen und zumindest die **Grundelemente** der Programmiersprache Objekt **Pascal** (Delphi) mitbringen.

Bedienung und Aufbau des **Pro Script Editors** orientiert sich an Borland (inzwischen im Besitz von Embarcadero) Delphi.

So gibt es einen **Objekt Inspektor** (links), eine **Komponentenpalette** (rechts) und Bereiche zum Erstellen von **Units und Formularen** (mitte).



9.3.2 Sprachelemente

siehe auch: [Erweiterung der Scriptsprache](#)

[Sonderfunktionen Shredder](#)

Sprachelemente

Zum Erstellen von Pro Scripten wird die Programmiersprache Pascal genutzt.

Unterstützte Pascal Syntax:

- **begin .. end constructor**
- **procedure and function declarations**
- **if .. then .. else constructor**
- **for .. to .. do .. step constructor**
- **while .. do constructor**
- **repeat .. until constructor**
- **try .. except and try .. finally blocks**
- **case statements**
- **array constructors (x:= [1, 2, 3] ;)**
- **^, *, /, /, and, +, -, or, <>, >=, =, >, <, div, mod, xor, shl, shr operators**
- **access to object properties and methods (ObjectName.SubObject.Property)**

Die Struktur eines Pro Scriptes

```
SCRIPT 1:
procedure DoSomething;
begin
    CallSomething;
end;
begin
    CallSomethingElse;
end;
SCRIPT 2:
begin
    CallSomethingElse;
end;
SCRIPT 3:
function MyFunction;
begin
    result:='Ok!';
end;
```

Wie in Pascal müssen statements mit ";" abgeschlossen werden. Begin..end Blöcke zum Gruppieren von Elementen sind erlaubt.

Identifizierer

Namen von Variablen, Funktionen und Prozeduren müssen mit einem Buchstaben (a..z or A..Z) oder '_' beginnen und können dann alphanumerische Zeichen oder '_' enthalten. Leerzeichen oder andere Zeichen sind nicht erlaubt.

Gültige Identifizierer:

```
VarName
_Some
V1A2
____Some_____
```

Ungültige Identifizierer:

```
2Var
My Name
Some-more
This, is, not, valid
```

Zuweisungsstatements

Zuweisungen erfolgen mittels " := "

```
MyVar := 2;
Button.Caption := 'This ' + 'is ok';
```

Zeichenfolgen

Zeichenfolgen werden in einfache Anführungszeichen eingeschlossen

```
A := 'This is a text';
Str := 'Text '+'concat';
B := 'String with CR and LF char at the end'#13#10;
C := 'String with '#33#34' characters in the middle';
```

Kommentare

Sie können die Zeichen // oder (* *) oder { } Blöcke nutzen um Kommentare in den Code einzufügen.

Falls Sie // Zeichen nutzen, endet der Kommentar in der gleichen Zeile.

Wenn Sie die // Zeichen hinter einer Pascal Anweisung nutzen, lassen Sie bitte hinter ";" ein LEERZEICHEN!!!!

```
//This is a comment before ShowMessage
ShowMessage('Ok');
ShowMessage('Yupp'); //Another comment
(* This is another comment *)
ShowMessage('More ok!');
{ And this is a comment
  with two lines }
ShowMessage('End of okays');
```

Variablen

Auch wenn dies nicht zwingend nötig ist, sollten Sie Variablentypen im Script auch deklarieren. script. Examples:

```
SCRIPT 1:
procedure Msg;
var S:string;
begin
    S:='Hello world!';
    ShowMessage(S);
end;

SCRIPT 2:
var A:integer;
begin
    A:=0;
    A:=A+1;
end;
```

Indizes

Strings, Arrays und Array Eigenschaften können mittels "[" und "]" indiziert werden. Falls str eine Variable vom Typ string ist, gibt der Ausdruck Str[3] das dritte Zeichen des Strings zurück.

```
MyChar:=MyStr[2];
MyStr[1]:='A';
MyArray[1,2]:=1530;
Lines.Strings[2]:='Some text';
```

Arrays

Pro Scripte Scripte unterstützen Array Konstruktoren und Variant Arrays. Um ein Array zu erzeugen benutzt man die Zeichen "[" und "]".

Sie können Mehrdimensionale Array erzeugen, indem Sie Array Konstruktoren verschachteln. Arrays sind 0-basierte Indexe.

```
NewArray := [ 2,4,6,8 ];
Num:=NewArray[1]; //Num receives "4"
```

```
MultiArray := [ ['green', 'red', 'blue'] , ['apple', 'orange', 'lemon'] ];
Str:=MultiArray[0,2]; //Str receives 'blue'
MultiArray[1,1]:='new orange';
```

If Statement

Unterstützt werden die Formen if..then und if..then ... else .

```
if J <> 0 then Result := I/J;

if J = 0 then
  Exit
else
  Result := I/J;

if J <> 0 then
begin
  Result := I/J;
  Count := Count + 1;
end
else
  Done := True;
```

While Statement

```
while Data[I] <> X do I := I + 1;

while I > 0 do
begin
  if Odd(I) then Z := Z * X;
  I := I div 2;
  X := Sqr(X);
end;

while not Eof(InputFile) do
begin
  Readln(InputFile, Line);
  Process(Line);
end;
```

Repeat Statement

```
repeat
  K := I mod J;
  I := J;
  J := K;
until J = 0;

repeat
  Write('Enter a value (0..9): ');
  Readln(I);
until (I >= 0) and (I <= 9);
```

For Statement

```
SCRIPT 1:
for c:=1 to 10 do
  a:=a+c;
SCRIPT 2:
for i:=a to b do
begin
  j:=i^2;
  sum:=sum+j;
end;
```

Case Statement

```

case uppercase(Fruit) of
  'lime': ShowMessage('green');
  'orange': ShowMessage('orange');
  'apple': ShowMessage('red');
else
  ShowMessage('black');
end;

```

Deklaration von Funktionen und Prozeduren

```

procedure HelloWorld;
begin
  ShowMessage('Hello world!');
end;

procedure UpcaseMessage(Msg:string);
begin
  ShowMessage(Uppercase(Msg));
end;

function TodayAsString:string;
begin
  result:=DateToStr(Date);
end;

function Max(A,B:integer):integer;
begin
  if A>B then
    result:=A
  else
    result:=B;
end;

procedure SwapValues(var A, B:integer);
Var Temp:integer;
begin
  Temp:=A;
  A:=B;
  B:=Temp;
end;

```

Import von DLL Funktionen

```

function functionName(arguments): resultType; [callingConvention]; external
'libName.dll' [name ExternalFunctionName];

```

Beispiel:

Die Funktionsdeklaration

```

function MyFunction(arg: integer): integer; external 'CustomLib.dll';

```

importiert eine Funktion namens MyFunction aus der DLL CustomLib.dll mit der Standardaufrufkonvention (register).

Sie können als Aufrufkonvention (stdcall, register, pascal, cdecl oder safecall) nutzen.

Beispiel:

```

function MessageBox(hwnd: pointer; text, caption: string; msgtype:
integer):integer; stdcall; external 'User32.dll' name 'MessageBoxA';

```

importiert 'MessageBoxA' aus User32.dll (Windows API), genannt 'MessageBox'

Unterstützte Datentypen

Integer
Boolean
Char
Extended
String
Pointer
PChar
Object
Class
WideChar
PWideChar
AnsiString
Currency
Variant
Interface
WideString
Int64
Longint
Cardinal
Longword
Single
Byte
Shortint
Word
Smallint
Double
Real
DateTime

Andere Typen wie (records, arrays, etc.) werden nicht unterstützt!

9.3.2.1 Erweiterung der Script Sprache

siehe auch: [Sonderfunktionen Shredder](#)

Erweiterung der Script Sprache

ArchiCrypt Pro Scripte können auf die Funktionen der folgenden Delphi Units zurückgreifen:

Buttons, CheckLst, Classes, clipbrd, ComCtrls, Controls, Dialogs, ExtCtrls, Forms, Graphics, Grids, ImgList, Inifiles, Registry, Menus, Printers, ShellApi, StdCtrls, Strutils, SysUtils, Types, Variants, System, widestrings, widestrutils, Windows, zlib, mask und

math

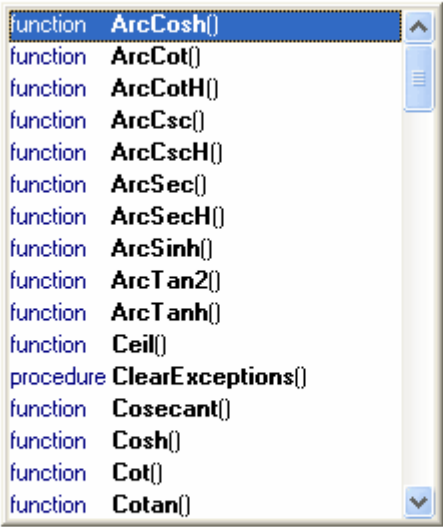


TIPP: Um festzustellen, welche Funktionen konkret zur Verfügung gestellt werden, geben Sie im Pro Script den Unit Namen gefolgt von einem Punkt "." ein und betätigen Sie die Tastenfolge **Strg + Space** (Steuerung + Leerzeichen). Es öffnet sich ein Fenster mit allen durch die Unit bereitgestellten Funktionen. Wählen Sie die gewünschte Funktion aus, um Sie an der aktuellen Stelle in den Quellcode einzufügen. Wenn Sie nicht wissen, welche Parameter die Funktion benötigt, dann suchen Sie im Internet nach "[Delphi Funktionsname](#)" also zum Beispiel [Delphi ArcCosh](#). Sie finden meist schnell ein Beispiel für die Verwendung der entsprechenden Funktion.

Wenn Sie eine Delphi Entwicklungsumgebung besitzen, können Sie dort in den gleichnamigen Units nachsehen.

Wir haben unsere Pro Scripte im Quellcode mit Kommentaren im Plugins Ordner der ArchiCrypt Shredder installation abgelegt. Kopieren Sie sich die Quellcodes ([Projektdatei Dateieindung ssproj](#); [Units Dateieindung psc](#); [Formulare Dateieindung sfm](#)) in einen eigenen Ordner und experimentieren Sie ein wenig mit den Scripten.

```
1 uses
2 math;
3
4 math.
```



9.3.2.2 Sonderfunktionen Shredder

Sonderfunktionen Shredder

Um Ihnen das Erstellen bestimmter Anwendungen erheblich zu erleichtern, stellen Ihnen ArchiCrypt Shredder Pro Scripte die nachfolgenden vordefinierten Funktionen zur Verfügung:

Ausgabe von Informationen im LogBuch des Shredders

```
procedure ACShredderLog(InMessage:string);  
  
Beispiel:  
ACShredderLog('Ich bin eine Nachricht aus einem Script');
```

Anzeige eines Nachrichtenfensters über dem Systemtray

```
procedure ACAlert(AUeberschrift:string;ANachricht:string);  
  
Beispiel:  
ACAlert('Wichtige Nachricht','Ich bin echt wichtig!');
```

Sicheres Löschen einer Datei (einfaches Überschreiben mit Nullen)

```
function ACShredderFile(AFileName:string):Boolean;  
  
Beispiel:  
  
if ACShredderFile('D:\UnnötigeDatei.txt') then  
    ACAlert('Info','Datei gelöscht');
```

Suche nach Dateien mit Maske

```
function ACGetMaskedFileList(StartVerzeichnis: string; DateiMaske: string; var AnzahlGefundenerDateien: integer);  
  
Beispiel siehe Pro Script Unit uCreateReport.psc
```

Sicherstellen, dass Pfad mit \ endet

```
function ACQualifyPath(InPath:string):string;  
  
Beispiel:  
var APath:string;  
  
begin  
    APath := 'C:\Pfad\Unterpfad';  
    APath := ACQualifyPath(APath); //APath sieht jetzt so aus 'C:\Pfad\Unterpfad\  
end;
```

Freien Speicherplatz auf Laufwerk ermitteln

```
function ACDiskFree(ADrive:Byte):int64;  
  
Beispiel:  
var freebytes:int64;  
  
begin  
    freebytes:= ACDiskFree('C');  
end;
```

Größe einer Datei ermitteln

```
function ACGetSizeOfFile(AFileName:string):int64;
```

Auswahldialog für Verzeichnis anzeigen

```
function ACBrowseFolder(AusgewaehltesVerzeichnis:string;DialogTitel:string):boolean;
```

liefert False, falls der Benutzer den Dialog ohne Auswahl eines Verzeichnisses abbricht, true, falls eine Auswahl erfolgt.

Der Name der gewählten Verzeichnisses wird dann in der Variablen AusgewaehltesVerzeichnis zurückgegeben.

Beispiel siehe Pro Script **Unit** uCreateReport.psc

```
var
  StartVerzeichnis:String;
begin
  if ACBrowseFolder(StartVerzeichnis,'Bitte Startverzeichnis wählen') then
  begin
    edtStarteSucheHier.Text := StartVerzeichnis;
  end;
end;
```

Dateien komprimieren und in ZIP Archiv speichern

```
function ACZipFiles(ListeMitDateien:TstringList; //Übergabe der zu komprimierenden Dateien als Liste
  ZIPDateiName:string; //Name inkl. Pfad der zu erzeugenden ZIP-Datei
  bDoLog:Boolean //soll Shredder Informationen im eigenen Logbuch anzeigen
):boolean;
```

Beispiel siehe Pro Script **Unit** uCreateBackup.psc

```
function ACUnZipFiles(ZIPDateiName:string; //Name inkl. Pfad der ZIP-Datei
  TargetPath:string; //Zielpfad für das Entpacken
  bDoLog:Boolean //soll Shredder Informationen im eigenen Logbuch anzeigen
):boolean;
```

Datei per HTTP downloaden

```
function ACDownloadHTTP(url:string, //hier aus dem Internet laden
  Zielverzeichnis:string; //in dieses lokale Verzeichnis speichern
  bDoShowProgress:boolean //Dialog mit Fortschritt anzeigen
):Boolean;
```

Beispiel siehe Pro Script **Unit** uDownloadHTTP.psc

Datei per FTP downloaden

```
function ACDownloadFTP(AHost:string;
  AFilename:string;
  ATargetDir:string;
  AUserName:string;
  APassword:string;
  AFTPPort:integer=21;
  ShowDialog:boolean=true
):Boolean;
```

Beispiel siehe Pro Script **Unit** uDownloadFTP.psc

Datei per FTP Uploaden

```
function ACUploadFTP(AHost:string;  
    ALocalFilename:string;  
    ATargetDir:string;  
    AUserName:string;  
    APassword:string;  
    AFTPPort:integer=21;  
    ShowDialog:boolean=true  
    ):Boolean;
```

Beispiel siehe Pro Script **Unit** uUploadFTP.psc

Datei vom FTP Server löschen

```
function DeleteFTP(AHost:string;  
    AFilename:string;  
    ARemoteDir:string;  
    AUserName:string;  
    APassword:string;  
    AFTPPort:integer=21;  
    ShowDialog:boolean=true  
    ):Boolean;
```

Beispiel siehe Pro Script **Unit** uUploadFTP.psc

Proxy für HTTP und FTP Funktionen festlegen

Muss vor dem Aufruf von HTTP bzw. FTP spezifischen Funktionen erfolgen

```
procedure ACInitProxy(AProxy:string;AProxyUserName:string;AProxyPassword);
```

MD5 Prüfsumme für eine Datei berechnen

```
function ACCalculateFileMD5(AFileName:string):string;
```

MD5 Prüfsumme für eine Zeichenkette berechnen

```
function ACCalculateStringMD5(AString:string):string;
```

Eine Datei verschlüsseln

```
function ACEncryptFile(EingabeDatei:string;AusgabeDatei:string;Passwort:string):Boolean;
```

Beispiel siehe Pro Script **Unit** uEncryptFile.psc

Eine Datei entschlüsseln

```
function ACDecryptFile(EingabeDatei:string;AusgabeDatei:string;Passwort:string):Boolean;
```

Beispiel siehe Pro Script **Unit** uEncryptFile.psc

Eine Zeichenkette verschlüsseln

```
function ACEncryptString(AString:string;Passwort:String):string;
```

Eine Zeichenkette entschlüsseln

```
function ACDecryptString(AString:string;Passwort:String):string;
```

Versionsinformationen von Windows ermitteln

```
function ACSystemInfo(MajorVersion:integer;  
    MinorVersion:integer;  
    BuildNumber:integer;  
    PlattformID:integer): Boolean;
```

Beispiel siehe Pro Script `Unit` `uSystemInfo.psc`

10 Technischer Teil

10.1 Verschiedene Betriebs- und Dateisysteme

ArchiCrypt Shredder wurde konzipiert, um Ihnen die Möglichkeit zu geben, Dateien unter den Betriebssystemen Windows XP, Windows Vista und Windows 7 sicher zu löschen.

Nachfolgend erfahren Sie etwas über die Besonderheiten der Microsoft Betriebssysteme, die im Zusammenhang mit dem Löschen eine Rolle spielen.

Windows XP, Vista und Windows 7 zeichnen sich unter anderem dadurch aus, dass Sie eine ausgefeilte Rechteverwaltung und das transaktionsorientierte Dateisystem NTFS bieten.

Sektoren und Cluster

Die Daten werden bei allen Systemen auf Datenträgern abgelegt, die bestimmte Strukturen aufweisen. Unter Microsoft Betriebssystemen sind diese Strukturen Sektoren und Cluster. In einem Sektor wird jeweils eine bestimmte Anzahl Bytes abgelegt und in einem Cluster wird eine bestimmte Anzahl an Sektoren zusammengefasst.

Inhalte von Dateien werden durch betriebssystemspezifische Funktionen in diesen Strukturen abgelegt. Gleichzeitig führt das Betriebssystem Protokoll darüber, welche Datei wo zu finden ist. Die Art und Weise, wie das Betriebssystem die Informationen ablegt und organisiert, ist für normale Anwendungen unwichtig und teilweise auch undokumentiert. Genau dieses Wissen ist jedoch notwendig, um Dateiinhalte nicht nur scheinbar zu löschen.

Mit Mitteln des Betriebssystems gelöschte Dateien sind nicht wirklich gelöscht

Sie wissen sicher, dass Dateien beim Löschen nicht tatsächlich gelöscht werden. Lediglich der Verweis auf den Inhalt wird entfernt.

Man kann sich das wie folgt vorstellen:

Eine Bibliothek führt eine Kartei, mit Karteikarten für jedes vorhandene Buch. Das Löschen mit Betriebssystemmitteln entfernt lediglich die Karteikarte. Das Buch ist weiterhin vorhanden. ArchiCrypt Shredder kümmert sich um das Buch!

Werden nun neue Daten auf den Datenträger geschrieben, erfolgt dieser Vorgang nicht zwingend an der Stelle, an der zuvor die andere Datei abgelegt war.

Intelligente Cache-Mechanismen (Zwischenspeicher) verhindern auch das sichere Überschreiben. Das Betriebssystem schreibt Daten nicht unmittelbar auf den Datenträger, sondern behält die Daten zunächst im Speicher. Erfolgt der nächste Schreibvorgang, ersetzt das System diese Daten im Arbeitsspeicher. Wird die Datei letztlich gelöscht, wird der Inhalt im Arbeitsspeicher verworfen, da die Datei nicht mehr benötigt wird. Auf dem Datenträger befinden sich immer noch die alten Inhalte, lediglich der Verweis auf diese "Altdaten" (die Karteikarte) wurde entfernt.

Das transaktionsorientierte Dateisystem von Windows NT speichert Informationen über Dateien in Dateien. Man nennt diese Daten **Metadaten**. Dadurch wird man der umfangreichen Rechteverwaltung gerecht, die vorsieht, dass man für jede Datei Zugriffsrechte vergibt. Selbst der Bootsektor (\$BOOT) ist unter diesem Dateisystem als Datei abgelegt. Sehen kann man diese Dateien unter normalen Umständen nicht.

Ein weiteres Konzept von NTFS ist es, die Datei als Ansammlung von Attributen (Eigenschaftswerten) zu sehen. Selbst der eigentliche Dateiinhalt ist ein Attribut. Attribute werden in der Master File Table-Struktur (\$MFT Datei) abgelegt. Ist der Dateiinhalt nicht zu umfangreich, wird auch der eigentliche Inhalt in dieser Struktur abgelegt. Ist der Dateiinhalt zu umfangreich, enthält die MFT-Struktur einen Verweis auf den ersten Cluster, in dem der Inhalt abgelegt ist.

Für das sichere Löschen ist von Interesse, dass man lediglich gezielt auf bestimmte Cluster zugreifen kann, nicht aber auf bestimmte Records (Datensätze) der MFT-Struktur. In der MFT können Dateien bis zu einer Größe von ca. 4 Kilobyte direkt abgelegt werden. Dies bedeutet folglich, dass man Dateien bis zu dieser Größe nicht direkt löschen kann.

Eine weitere Besonderheit des NTFS Dateisystems ist die s.g. Transaktionsorientiertheit. D.h. Änderungen werden ganz oder gar nicht übernommen. Um dies zu bewerkstelligen, führt das Betriebssystem in der Datei \$LogFile alle Dateioperationen auf. In dieser werden dabei auch Inhalte der betroffenen Datei mit aufgeführt. Im Falle eines notwendigen Rollbacks (Rücknahme einer Änderung) dienen diese Informationen dem Wiederherstellen des ursprünglichen Inhalts.

Windows Vista und Windows 7

Darüber hinaus bieten Windows Vista und Windows 7 weitere **Besonderheiten**, die in einem eigenen [Kapitel](#) behandelt werden.

10.2 Wichtige Begriffe

Freispeicher

Der Bereich einer Festplatte, der zum Beispiel im Windows Explorer als verfügbar angegeben wird. In diesem Bereich liegen all die Dateien und Dateifragmente, die Sie mit den Mitteln des Betriebssystems vermeintlich gelöscht haben. Hier können ganze Dateien oder zumindest Dateifragmente wieder hergestellt werden.

Clustertips

Der grobe Aufbau der Datenträgerstruktur unter Microsoft Betriebssystemen wurde unter "[Verschiedene Betriebs- und Dateisysteme](#)" bereits angedeutet.

Wichtig ist, dass im Falle eines Schreibvorganges auf diesen Datenträger immer so viel Speicher auf dem Datenträger belegt wird, dass eine ganzzahlige Anzahl an Clustern blockiert wird.

Nehmen wir an, der Datenträger, auf dem eine Datei gespeichert werden soll hat (die recht verbreitete) Clustergröße 512 Byte.

Wollen Sie jetzt eine Datei speichern, die 723 Byte enthält, werden 2 Cluster reserviert, d.h. 1024 Byte. Von diesen 1024 Byte sind 301 Byte ungenutzt. Diese ungenutzten Anteile, die bei einer Clustergröße K immer nur K-1 Byte groß sein können, bezeichnet man als **Clustertip**.

Warum sollte man Clustertips löschen?

Der ungenutzte Anteil wird nicht überschrieben, und kann auch durch andere Dateien nicht überschrieben werden. Im Betriebssystem ist dieser Cluster als belegt markiert. Nehmen wir an, Sie speichern eine Passwortdatei oder TAN-Datei beliebiger Größe (kein ganzzahliges Vielfaches der Clustergröße). Nach einer bestimmten Zeit löschen Sie die Datei mit Betriebssystemmitteln und speichern andere Daten auf dem Datenträger. Jetzt ist es möglich, dass genau in den s.g. Clustertips wichtige Informationen zu finden sind. Wenn man jetzt noch berücksichtigt, dass die Clustergröße variiert, und bis zu 64 KByte groß sein kann, sieht man, dass es wichtig ist, diesen Anteil zu bereinigen. Insbesondere beim ersten Einsatz des Shredders.

Beispiel:

Geheime Datei:

Dies ist mein geheimes Passwort, es lautet Gustav 23

Datei wird gelöscht, der Verweis aus dem Inhalt des Datenträgers entfernt.
(Dies ist in etwa so, als würde man aus der Inhaltsangabe eines Buches die Seitenzahl eines Kapitels schwärzen, das Kapitel ist dennoch weiterhin vorhanden.)

Nach einer bestimmten Zeit überschreibt das Betriebssystem Anteile der Cluster der geheimen Datei.

Ich bin eine neue Datei

Im s.g. Clustertip, stehen jetzt die vertraulichen Daten "Gustav 23"!!

In dieser Phase sind die Informationen fast komplett erhalten und weiterhin softwaretechnisch leicht zu ermitteln. Falls Sie in dieser Phase einen Dateishredder einsetzen oder den Freispeicher löschen, bleibt dieser Clustertipanteil erhalten, enthält also weiterhin die sensiblen Daten. ArchiCrypt Shredder beherrscht selbstverständlich auch diese Besonderheit und bereinigt auch den Clustertipanteil von Dateien.

So löschen Sie Dateinamen bereits gelöschter Dateien

Dateinamen löschen

Auch Dateinamen sind unter Umständen nicht für die Augen anderer bestimmt. Die Dateinamen bleiben beim Löschen zumindest teilweise, oft sogar komplett erhalten, da sie in speziellen Strukturen des Datenträgers abgelegt werden, die nur schwer zugänglich sind.

So löschen Sie Datenpartitionen und ganze Festplatten

Es gibt eine Betriebssystempartition, auf der Ihr Betriebssystem installiert ist. Alle weiteren Partitionen werden als Datenpartitionen bezeichnet.

Da wir zum Löschen die Hilfe des Betriebssystems benötigen (auch wenn es nur zur Anzeige unseres ArchiCrypt Shredder Programms ist), müssen wir beim Löschen der Partition, auf der sich das Betriebssystem selbst befindet, auf andere Mittel zurückgreifen. [ArchiCrypt Shredder bringt für diesen Zweck DBAN mit.](#)

Datenpartitionen sind alle anderen Partitionen, auf die über einen Laufwerksbuchstaben zugegriffen werden kann und auf denen sich nicht das Betriebssystem befindet. [Hier kann ArchiCrypt Shredder selbst mit Funktionen aufwarten.](#)

Sichere Löschezonen

Sichere Löschezonen sind Orte auf Ihrem Rechner, an denen der Shredder unsichere Löschoperationen beliebiger Anwendungen abfängt und durch sichere Löschmethoden ersetzt. Die so gelöschten Daten sind dann sicher gelöscht.

10.3 Schnelles Überschreiben

Schnelles Überschreiben mit Zufallsdaten

Bei dieser Methode werden die zu löschenden Daten mit Daten aus **Pseudo-Zufallszahlen** in einer Phase überschrieben.

Nur mit **ungeheurem technischem und finanziellem Aufwand** ist es **eventuell** möglich **kleine Fragmente** der Ausgangsdaten wieder zu rekonstruieren. Kaum ein Staat dieser Welt kann entsprechende Mittel aufbringen und wird dies nur tun, wenn sich dieser erhebliche Aufwand lohnt.

In der Praxis genügt diese Methode also völlig!

Mit rein softwaretechnischen Mitteln ist eine Rekonstruktion der Daten NICHT möglich!

(siehe auch [DoD 5220.22-M](#))

10.4 DoD 5220.22-M

DoD 5220.22-M (E)

Die Originaldaten werden durch **dreifaches Überschreiben** nach den Bestimmungen NTSC-TG-025 (Version 2, Sept. 1991) des US-amerikanischen Verteidigungsministeriums vernichtet. Ihre Daten werden hierbei zunächst mit einem fest vorgegebenen Wert überschrieben,

anschließend wird die Datei mit **Pseudo-Zufallszahlen** überschrieben. Abschließend wird in der dritten Runde die Datei mit dem Komplement des Wertes aus Runde 1 überschrieben.

DoD 5220.22-M (ECE)

Diese **Variante von DoD 5220.22-M** arbeitet mit **sieben Durchläufen**, wobei die Daten zunächst mit den drei Durchläufen des DoD 5220.22-M (E) Standards, anschließend mit einem Zufallswert, danach erneut mit den drei Durchläufen des DoD 5220.22-M (E) überschrieben werden.

Falls Sie in der Kategorie **Einstellungen** eine 2 für die Methodenwiederholung angeben, werden die Daten der zu löschenden Datei also insgesamt 14 Mal überschrieben. In dieser Bestimmung wird ausdrücklich darauf hingewiesen, dass das Löschen von Informationen mit der militärischen Einstufung "TOP-Secret" nicht erlaubt ist. Dort hilft nur Type 1 oder 2 Degauss (Entmagnetisierung mit einem sehr starken Magneten) oder Pulverisieren.

Die komplette Rekonstruktion von Daten, die mit ArchiCrypt Shredder gelöscht wurden, ist mit softwaretechnischen Mitteln nicht möglich.

10.5 VSITR

Der deutsche Standard (VS-IT-Richtlinien - VSITR)

Das im **VSITR-Standard** (Richtlinien zum Geheimschutz von Verschlussachen beim Einsatz von Informationstechnik), herausgegeben vom **Bundesamt für Sicherheit in der Informationstechnik** (BSI), beschriebene Verfahren, überschreibt die zu löschenden Daten in insgesamt sieben Durchläufen. In den ersten sechs Durchläufen wird dabei abwechselnd mit den Werten 0x00 und 0xFF und im letzten Durchlauf mit dem Wert 0xAA überschrieben.

Die komplette Rekonstruktion von Daten, die mit ArchiCrypt Shredder gelöscht wurden, ist mit softwaretechnischen Mitteln nicht möglich.

10.6 Peter Gutman

Löschen mit Peter Gutman

In seinem Aufsatz [Secure Deletion of Data from Magnetic and Solid-State Memory](#) erläutert **Peter Gutman** ein Verfahren zum Löschen von Daten auf verschiedenen Medien. Das Verfahren von Peter Gutman ist sehr zeitintensiv, wird jedoch als äußerst sicher angesehen.

Die komplette Rekonstruktion von Daten, die mit ArchiCrypt Shredder gelöscht wurden, ist mit softwaretechnischen Mitteln nicht möglich.

10.7 Schwachstellen/Tipps

Schwachstellen und Tipps

Das sichere Löschen von Dateien hat je nach Betriebssystem einige Schwachstellen. Man kann

grundsätzlich zwischen den Systemen W9x/ME und NT/2000/XP/Vista/Windows 7 unterscheiden. Die erste Gruppe arbeitet grundsätzlich mit dem Dateisystem FAT12/FAT16 und FAT32, während die zweite Gruppe neben diesen Systemen auch das NTFS-Dateisystem unterstützt.

Die zweite Gruppe hat aufgrund ihres Einsatzbereiches in Industrie, Staat und Behörden zahlreiche Mechanismen, die einen sicheren Betrieb der Systeme gewährleisten. Genau diese Mechanismen arbeiten unserer Absicht, sensible Daten sicher zu Löschen, leider entgegen. Das Betriebssystem **Windows Vista und Windows 7** macht mit den s.g. **Schattenkopien** das Löschen besonders schwer. Hier sollten Sie unbedingt die [besonderen Hinweise](#) beachten.

Generell gilt:

Das sichere Löschen von Daten auf **Netzlaufwerken** kann nicht gewährleistet werden. ArchiCrypt Shredder (und kein anderes Löschprogramm der Welt) kann ohne eine Installation auf dem entfernten System feststellen, wie die Daten jenseits des eigenen "Verantwortungsbereichs" organisiert sind. Ohne dieses Wissen ist Sicheres Löschen nicht möglich. Kein Programm vermag dies!

Die s.g. Auslagerungsdatei

ArchiCrypt Shredder bietet Ihnen an, die Auslagerungsdatei (**pagefile.sys**) beim Herunterfahren des Rechners zu überschreiben. Das Überschreiben erfolgt in einem Durchgang in dem NULLEN geschrieben werden. Das Herunterfahren des Rechners wird dabei etwas verlangsamt.

Eingeschränkte Benutzerrechte unter XP, Vista und Windows 7

Windows NT ist ein Betriebssystem für den Mehrbenutzerbetrieb, welches über ein ausgefeiltes **Rechtesystem** verfügt. Nicht jedem Nutzer ist es gestattet, bestimmte Dateien zu Löschen, oder auf bestimmten Datenträgern oder in bestimmten Verzeichnissen Dateien zu erstellen. Ähnlich verhält es sich mit dem Aufruf von systemnahen Funktionen aus Programmen heraus, die der jeweilige Nutzer aufruft. Um Daten tatsächlich zu löschen, arbeitet ArchiCrypt Shredder an einigen Stellen mit Funktionen, die **Administratorrechte** erwarten. Insbesondere dann, wenn Sie mit komprimierten Daten oder verschlüsselten Daten (durch das Betriebssystem verschlüsselte Daten; nicht betroffen sind Dateien, die von externen Programmen verschlüsselt wurden, wie zum Beispiel mit ArchiCrypt) arbeiten. Auch die Bereinigung des Freispeichers und das Löschen von Datenpartitionen setzen bestimmte Privilegien voraus. Sie müssen vollen Zugriff auf den gesamten verfügbaren Festplattenspeicher des zu bereinigenden Datenträgers haben.

ArchiCrypt Shredder gibt Ihnen bei Aufruf entsprechender Funktionen einen Hinweis und bietet Ihnen an, den Shredder mit Administratorrechten neu zu starten.

Systemwiederherstellung und Schattenkopien unter Windows XP, Vista und Windows 7

Windows XP, Vista und Windows 7 schalten die s.g. **Systemwiederherstellung** ab, wenn auf einem Datenträger zu wenig freier Speicher vorhanden ist. Mit dem Abschalten werden auch s.g. **Prüfpunkte / Wiederherstellungspunkte**, mit deren Hilfe man einen älteren Systemzustand wieder herstellen kann, vernichtet.

Beim Bereinigen des s.g. **Freispeichers** wird dieser Umstand künstlich provoziert, mit der Folge, dass die Prüfpunkte verloren gehen. Es handelt sich nicht um einen Fehler von

ArchiCrypt Shredder, sondern um ein Verhalten, welches der Betriebssystemhersteller vorgesehen hat. Den gleichen Effekt würden Sie erhalten, wenn Sie durch "normales Arbeiten" die Kapazität der Festplatte unter einen Schwellwert fallen würde.

Kleine Dateien unter XP, Vista und Windows 7

Unter kleinen Dateien sind Dateien zu verstehen, deren Größe unterhalb 4KByte liegt. Aufgrund der Verwaltung des Datenträgers werden kleine Dateien unter Umständen in der s. g. \$MFT (Master File Table) Datei abgelegt. Die Struktur ist im Wesentlichen dafür verantwortlich, Informationen über Speicherort und Datei- und Sicherheitsattribute aufzunehmen. Allerdings werden die Inhalte kleinerer Dateien ebenfalls in dieser Struktur gespeichert.

Eine weitere, sehr schwierig zu handhabende und zu manipulierende Datei ist die s.g. \$LogFile Struktur. Das Betriebssystem protokolliert in dieser Struktur alle Dateioperationen. Notwendig ist dieses Vorgehen, um ein konsistentes Dateisystem sicherzustellen. Schlägt eine Dateioperation fehl, kann mit Hilfe der im \$LogFile gespeicherten Informationen ein s.g. Rollback durchgeführt werden. D.h. die fehlerhafte Aktion wird zurückgenommen, um den ursprünglichen Zustand wiederherzustellen. Leider hat man keinerlei Einfluss darauf, an welcher Stelle in dieser Struktur Informationen abgelegt werden. Man kann solche Informationen entsprechend nicht überschreiben. In dieser Struktur werden allerdings keine Dateien, sondern Dateiausschnitte abgelegt. Bei Text-basierten Dateien, entstehen dadurch allerdings lesbare Fragmente.

Die Lösung für dieses Problem lautet [Regelmäßige Freispeicherbereinigung!](#)

Internet Explorer ab Version 5

Achten Sie bitte darauf, dass die Funktionen des Shredders nur in Verbindung mit dem Internet Explorer 5.0 aufwärts verfügbar sind. Falls Sie zuvor eine andere Version installiert hatten, kann es vorkommen, dass Reste bleiben. Diese sollten Sie einmalig manuell löschen. Durch die Zwischenspeicherung von Daten im Hauptspeicher Ihres Rechners kann es dazu kommen, dass Inhalte von Seiten, die Sie vor kurzem besucht haben, erst nach dem eigentlichen Löschen mit dem Shredder auf den Datenträger geschrieben werden. Brechen Sie bitte das Löschen im Zusammenhang mit Online-Daten nur im Notfall ab, da ansonsten Inkonsistenzen entstehen, die eine saubere Bereinigung des temporären Speichers behindern. Bitte beachten Sie auch die Hinweise im Kapitel [Sichere Löschezonen](#).

Browser löschen selbst Dateien mit Betriebssystemmitteln. Diese Dateien können dann selbstverständlich wieder hergestellt werden. Wundern Sie sich also bitte nicht, wenn Sie in einem Recovery-Programm trotz des Shredder Einsatzes plötzlich einzelne Dateien aus Ihrem Browsercache als wieder herstellbar angezeigt bekommen. Nutzen Sie also die Sicheren Löschezonen!

Recovery Tools / Tools zur Wiederherstellung von Dateien

Recovery Tools nutzen meist den Umstand, dass Verweise auf die Dateien (Dateiname) beim Löschen einer Datei nicht entfernt werden. Entdecken Sie einen entsprechenden Eintrag, gehen Sie davon aus, dass die Datei noch zu retten ist. In Wahrheit wird beim Durchführen des Recovery eine Datei mit dem ehemals Originaldateinamen und Datenschnitt erzeugt. Um die Dateinamen ebenfalls zu überschreiben wurde eine entsprechende Funktion in der Kategorie [Datenträger](#) realisiert. Wählen Sie den Eintrag **Dateinamen** aus (es ist nicht

nötig, Clustertips oder den Freispeicher zu aktivieren) und bereinigen Sie die Dateinamen.

Index

- 1 -

1-Klick Löschaufgabe 66, 67

- A -

Administratorrechte 10
 ADS Scanner 13
 ADS Scanner - Analyse 28
 Aktion für ausgewählte Festplatte ausführen 31
 Alle 45
 Alle Einträge auswählen 41
 Allgemeines 73
 Alte Aufträge löschen 67
 Analyse starten 25
 Analyse starten 20
 Analyse-Modus 25
 Analysiere Verzeichnis 20
 Andere Löschmethoden 75
 Andere Methoden 75
 Anfänger 79
 Anpassen der grafischen Darstellung 20
 Ansicht erweitern (expandieren) 41
 Ansicht reduzieren 41
 Anzeige eines Nachrichtenfensters über dem Systemtray 105
 APPDATA 85
 ArchiCrypt Shredder im Internet... 73
 ArchiCrypt Shredder im Menü des Windows-Explorers 60
 ArchiCrypt Sichere Löschzone 57
 Arrays 98
 Auf welche Funktionen müssen Sie in der mobilen Version verzichten? 59
 Aufgaben bereinigen 67
 Aufgaben planen 73
 Aufgabenplaner 67
 Aufgaben-Planer 13
 Aufgabe-Planer 67
 Ausgabe von Informationen im LogBuch des Shredders 105
 Ausgeblendete Nachrichten reaktivieren 73
 Ausgewählte Festplatte löschen 33

Auslagerungsdatei 112
 Auslagerungsdatei beim Herunterfahren überschreiben 75
 Auswahl aufheben 41
 Auswahl shreddern 20, 25
 Auswahl sicher löschen 60
 Auswahl sicher löschen (Admin) 60
 Auswahl sicher verschieben 60
 Auswahl sicher verschieben (Admin) 60
 Auswahl umkehren 41
 Auswahl wieder herstellen 27
 Auswahldialog für Verzeichnis anzeigen 105
 Automatische Bereinigung der Quarantäne 7

- B -

Bearbeiten einer Aufgabe 67
 Bedienung von ArchiCrypt Sichere Löschzone 57
 Bedienung Zeitüberwachung 71
 Beenden von ArchiCrypt Sichere Löschzone 57
 Beim Einfügen direkt löschen 19
 Beim Start prüfen ob es ein Update gibt? 73
 Beispielzonen erstellen 54
 Benutzerkontensteuerung 11
 Bereiche und Strukturen 31
 Beschreibung 67
 Boot CD - Löschen des Betriebssystems 31
 Boot-Medium 35
 Boot-Medium - Löschen des Betriebssystems 35
 Browserspuren 41

- C -

CACHE 85
 CAPPDATA 85
 Case Statement 98
 Clustertips 31, 109
 Computer und Daten vor nicht autorisierter Programmaktivität schützen 60
 Computerschutz 11
 COOKIES 45, 85
 CSTARTUP 85

- D -

Das Ergebnis der Analyse einschätzen 28
 Das Explorer Kontextmenü 60

Das Plugin-System 46
 Datei per FTP downloaden 105
 Datei per FTP Uploaden 105
 Datei per HTTP downloaden 105
 Datei vom FTP Server löschen 105
 Dateien 45
 Dateien bequem per Drag&Drop sicher löschen 19
 Dateien komprimieren und in ZIP Archiv speichern 105
 Dateien sind gleich, wenn sie in Inhalt und Namen übereinstimmen 79
 Dateifragmente 109
 Dateimanager 13, 19
 Dateinamen 31
 Daten automatisch löschen 41
 Datenträger 13
 datenträgerbezogene Aufgaben 67
 Datum der Sicherung 27
 Deklaration von Funktionen und Prozeduren 98
 Der Dateimanager 19
 Der deutsche Standard (VS-IT-Richtlinien - VSITR) 75, 112
 DESKTOP 85
 Detailinformationen 45
 Diagramm 20
 Die 2 Phasen der Analyse 28
 Die 3 Phasen der Analyse 20
 Die 9 Hauptkategorien 13
 Die Bedienoberfläche 17
 Die Menüleiste zur Bearbeitung der Verzeichnislisten 37
 Die Sonderfunktionen 67
 Die Struktur eines Pro Scriptes 98
 Die verschiedenen Analyse-Modi 79
 Die verschiedenen Analyse-Modi des Duplikat Finders 79
 Die Zeitüberwachung 71
 DoD 75
 DoD 5220.22-M 111
 DoD 5220.22-M (E) 75
 DoD 5220.22-M (ECE) 75, 111
 Download 2
 Duplikat Finder 13, 25
 Duplikat Finder - Analyse 25
 Duplikat Finder - Quarantäne 27
 Duplikate 25

- E -

Ein Plugin hat immer folgenden Aufbau: 84
 Eine Datei entschlüsseln 105
 Eine Datei verschlüsseln 105
 Eine Zeichenkette entschlüsseln 105
 Eine Zeichenkette verschlüsseln 105
 Eingeloggt als Administrator 11
 Eingeschränkte Benutzerrechte unter XP, Vista und Windows 7 112
 Einstellmöglichkeiten 73
 Einstellungen ADS Scanner 82
 Einstellungen Duplikat Finder 79
 Einstellungen Hotkeys 78
 Eintrag 45
 Einträge automatisch aus der Quarantäne 79
 Empfohlene Systemkonfiguration 10
 Entferne aus Quarantäne 27
 Erstellen einer BOOT-CD 35
 Erstellen einer DBAN-Bootdiskette oder eines DBAN-USB Sticks 35

- F -

FAVORITES 85
 Filterkriterien 19
 Firefox 41
 FONTS 85
 For Statement 98
 Formulare 103
 Fortgeschrittener 79
 Freien Speicherplatz auf Laufwerk ermitteln 105
 Freispeicher 31, 109
 Funktion Shutdown 73
 Funktionen der ausgewählten Einträge ausführen 41

- G -

Geheime Aufzeichnungen des Betriebssystems entschlüsseln 46
 Gleichheit von Dateien 79
 Google Chrome 7
 Größe einer Datei ermitteln 105

- H -

Hartnäckige Dateien 31, 36
 Hartnäckige Dateien löschen 36
 Highlight 27
 Hilfe zur Hilfe 1
 Hinweis für 64 BIT Systeme 10
 HISTORY 7, 85
 Hotkey De-/aktivieren 78
 Hotkey Online-Profil 78
 Hotkey Online-Spuren 78
 Hotkey Plugin-Profil 78
 Hotkey Sichere Löschezonen 78
 Hotkey Verzeichnisliste 78
 Hotkeys 78
 Hotkeys übernehmen 78

- I -

Identifizierer 98
 If Statement 98
 Import von DLL Funktionen 98
 In den Sicherungen nach dieser Datei suchen 27
 In Windows Explorer integrieren 73
 Indikatoren 88
 Indizes 98
 Information über Stream .. 28
 Inhalt im Browser anzeigen 45
 Inhalte von Alternativen Datenströmen ansehen 28
 Inhaltsanzeige 45
 Installation auf einem U3-Stick 59
 Installation auf einem USB-Stick 59
 Installationsroutine 10
 Internet Explorer 112
 Internetexplorer 112
 ISO-Image 35

- K -

Kategorien 17
 Kleine Dateien unter NT/2000/XP 112
 Kleine Dateien unter XP, Vista und Windows 7 112
 Kommentare 98
 Kontextmenü im Infobereich 60
 Kuchen-Säulengrafik 20

- L -

Laufwerksbelegung 13, 20
 Liste zu ignorierender Dateien/Verzeichnisse 25
 LogBuch 73
 LogBuch führen 65
 LogBuch zurücksetzen 65
 Logdatei 73
 Löschen 19, 65
 Löschen des Betriebssystems 35
 Löschen unter Vista und Windows 7 11
 Löschen von Dateien und Verzeichnissen 20
 Löschen von Datenpartitionen 31
 Löschmethode für Duplikate und Dateien in Quarantäne 79
 Löschmethode Shredder 25
 Löschmethode System 25

- M -

MD5 Prüfsumme für eine Datei berechnen 105
 MD5 Prüfsumme für eine Zeichenkette berechnen 105
 Menüleiste animieren 73
 Menüleisten 17
 Merkfeld 19
 Metadaten 108
 Minimale Systemanforderungen 10
 Mini-Menüleiste 17
 Minimieren in Informationsbereich (Tray) 57
 Mit Mitteln des Betriebssystems gelöschte Dateien sind nicht wirklich gelöscht 108
 Mit Windows starten 73
 Mobile Nutzung 13, 59
 Mobile Nutzung von U3- und USB-Sticks 7
 Moderne Nutzeroberfläche 7

- N -

Nachrichten 73
 NETHOOD 85
 Netscape 41
 Neue Sichere Löschezone 54
 Neuer Auftrag 67
 Nicht löschen 19
 NISPOM 75

NISPOM (NSA DoD 5220.22-M ECE) 75

Noch mehr Platz schaffen und Ballast beseitigen 7

Nutzerdefiniert 79

Nutzerdefinierte Pfade 87

- O -

Object Pascal 46

Onlinefunktionen 41

Online-Profil 41

Online-Profil laden und speichern 41

Online-Spuren 13, 41

Opera 41

OPERA6 85

OPERAEXE 85

OUTLOOKEXPRESS 85

OWN 85

- P -

pagefile.sys 75

Peter Gutman 75, 112

Pfad für Sicherungspugins 73

Platz und Sicherheit 7

Platzhalter 54

Plugin-Editor 84

Plugin-Profil 46

Plugin-Profil laden und speichern 46

Plugin-Profile 46

Plugins 13, 46

Plug-ins 7

Plugins neu einlesen 46

Prefetch Verzeichnis 37

Pro Script Anwendungen 46

Pro Script Editor 46

Pro Scripte 46

Profi 79

PROGRAMS 85

Projektdatei 103

Projektdateien 46

Protokoll 73

Protokolldatei 65, 73

Proxy für HTTP und FTP Funktionen festlegen 105

Prüfpunkte 112

psc 103

- Q -

Quarantäne 27

Quarantäne aktivieren 79

Quarantäne ansehen 25

Quarantäne automatisch bereinigen 79

Quarantäne und Quarantäneverzeichnis 79

- R -

Radar 60

Radar Symbol 60

RECENT 85

Recovery Tools 112

Registrieren 2

Registrierungsname 2

Repeat Statement 98

- S -

Schattenkopie 11

Schnelles Überschreiben 111

Schnelles Überschreiben mit Zufallsdaten 111

Secure Deletion of Data from Magnetic and Solid-State Memory 112

Sektoren und Cluster 108

SENDTO 85

Seriennummer 2

sfm 103

Shredder mit Windows starten 73

ShredderPlgEditor.exe 46

ShredderProScriptEditor.exe 46

Shutdown 60, 73

Sichere Löschzone bearbeiten 54

Sichere Löschzone entfernen 54

Sichere Löschzone erstellen 54

Sichere Löschzone überwachen 54

Sichere Löschzonen 7, 13, 51, 109

Sichere Löschzonen bearbeiten 57

Sichere Löschzonen bei Windowsstart überwachen 54

Sichere Löschzonen erstellen 54

Sichere Löschzonen vorschlagen 54

Sichere Zonen 109

Sicheres Löschen einer Datei (einfaches Überschreiben mit Nullen) 105

- Sicherheit 73
- Sicherheit einer Online Session 45
- Sicherstellen, dass Pfad mit \ endet 105
- Sicherungskopien 52
- Simulation 65
- simulieren 41
- So arbeiten Sie mit den Sicheren Löschezonen 54
- So bearbeiten Sie eine Löschaufgabe 67
- So bereinigen Sie den Freispeicher, säubern Clusterips und entfernen Spuren alter Dateinamen 31
- So bereinigen Sie den Freispeicher, säubern Clustertips und entfernen Spuren alter Dateinamen 31
- So bereinigen Sie die Quarantäne automatisch 79
- So deaktivieren Sie die Schattenkopie-Funktion 11
- So entfernen Sie Dateien aus der Quarantäne 27
- So erstellen Sie eigene Plugins 46
- So erstellen Sie eine neue Sichere Löschezone 54
- So erstellen Sie einen neuen Löschauftrag 67
- So finden Sie Alternative Datenströme 28
- So finden Sie Duplikate 25
- So finden Sie eine bestimmte Datei in der Quarantäne 27
- So führen Sie beim Beenden eines Browsers bestimmte Plugins aus 41
- So führen Sie ein Plugin im Simulationsmodus aus 46
- So führen Sie Plugins aus 46
- So installieren Sie ArchiCrypt Shredder auf einem U3-Stick 59
- So installieren Sie ArchiCrypt Shredder auf einem USB-Stick 59
- So legen Sie fest, welche Dateien ArchiCrypt Shredder untersuchen soll 82
- So legen Sie fest, welche Dateien der ADS Scanner untersuchen soll 82
- So löschen Sie alle Daten einer Partition 33
- So löschen Sie beim Beenden eines Browsers Dateien in bestimmten Verzeichnisse 41
- So löschen Sie beim Beenden eines Browsers Dateien in bestimmten Verzeichnissen 41
- So löschen Sie Dateien in bestimmten Verzeichnisse 41
- So löschen Sie Dateien und Verzeichnisse 20
- So löschen Sie Dateien und Verzeichnisse mit dem Dateimanager von ArchiCrypt Shredder 19
- So löschen Sie Dateien, die nicht während der Arbeit mit dem Rechner gelöscht werden können 36
- So löschen Sie die Inhalte bestimmter Verzeichnisse beim Beenden Ihres Browsers 37
- So löschen Sie Duplikate 25
- So löschen Sie Spuren automatisch 41
- So löschen Sie Surf Spuren automatisch 41
- So schaffen Sie sofort eine Menge Platz 37
- So schalten Sie ArchiCrypt Shredder frei 2
- So schließen Sie bestimmte Dateien und Verzeichnisse von der Analyse aus 82
- So schließen Sie bestimmte Verzeichnisse und Dateien von der Analyse durch den Duplikat Finder aus 79
- So schließen Sie Datenströme mit bestimmtem Namen aus 82
- So schränken Sie die Liste gefundener Dateien ein 37
- So speichern Sie Löschaufgaben als 1-Klick Löschaufgabe 67
- So starten Sie ArchiCrypt Shredder als Administrator 11
- So starten Sie die Aufgabenüberwachung 67
- So starten Sie die Zeitüberwachung 67
- So starten Sie eine Löschaufgabe direkt aus dem Aufgaben-Planer 67
- So starten Sie eine Löschaufgabe direkt aus dem Aufgabenplaner heraus 67
- So stellen Sie eine Datei aus der Quarantäne wieder her 27
- So verschieben Sie Dateien und Verzeichnisse sicher an einen neuen Speicherort 60
- Sonderfunktionen 67
- Sound nach Löschvorgang 73
- Spezielle Verzeichnisse bereinigen 41
- ssproj 103
- Starten der Aufgabenüberwachung 67
- STARTMENUE 85
- STARTUP 85
- Status und Logbuch 57
- Status und Logbuch der Sicheren Löschezonen 57
- Steigerung der Geschwindigkeit 7
- Suche mit Google 28
- Suche nach Dateien mit Maske 105
- SYSTEM 85
- System nach dem Vorgang automatisch herunterfahren 31, 33
- Systemsteuerung 11
- Systemtray 73
- Systemvoraussetzungen für DBAN (Darik's Boot and Nuke) 10
- Systemwiederherstellung 112

Systemwiederherstellung und Schattenkopien unter Windows XP und Vista 112

Systemwiederherstellung und Schattenkopien unter Windows XP, Vista und Windows 7 112

Systemwiederherstellung unter Win ME 112

Systemwiederherstellungspunkte 75

Systemwiederherstellungspunkte ohne Nachfrage überschreiben 75

- T -

Task-Planer 67

Tastenkombination 78

TEMP 85

temporäre Dateien 37, 52

Textvariablen 87

Tools zur Wiederherstellung von Dateien 112

TOP 100 Liste 20

- U -

UAC 11

Überblick 13

Überwachung der Sicheren Löschkzonen 57

Überwachung starten 54

Unautorisierte Plugins zulassen 46, 73

Units 103

Unlöschrare Dateien 11

Unterstützte Betriebssysteme 10

Unterstützte Datentypen 98

Unterstützte Pascal Syntax 98

Unterverzeichnisse einbeziehen 19

unverschlüsselte Plugins 46

Unzählige Verbesserungen 7

Update suchen 73

User Access Control 11

USERDEF 85

- V -

Variablen 98

Verlauf 45

Versionsinformationen von Windows ermitteln 105

Verzeichnisliste 37

Verzeichnisse 13, 37

Volumenschattenkopie 11

Vordefinierte Favoriten 19

Vordefinierte Verzeichnisse 37

VSITR 75

- W -

Wann sind Dateien gleich? 79

Warum benötigt man Sichere Löschkzonen? 52

Warum sollte man Clustertips löschen? 109

Was ist DBAN? 35

Was sind Sichere Löschkzonen? 52

Was tun, wenn Anwendungen nach der Entfernung eines Duplikates nicht mehr laufen? 25

Was tun, wenn beim Sicheren Verschieben ein Fehler auftritt? 60

Weitere Bestellmöglichkeiten 3

Welche Datei soll ich löschen? 25

Welche Folgen hat das Deaktivieren der Schattenkopie-Funktion 11

Welche Methode soll zum Überschreiben verwendet werden? 75

Werte auf Zielsystem 87

While Statement 98

Wie kann ich bestimmte Dateien oder Verzeichnisse von der Analyse ausnehmen? 25

Wie oft sollen Dateien überschrieben werden? 73

Wiederherstellungspunkte 11, 112

WINDIR 85

Windows 7 7

Windows Vista 108

Windows Vista und Windows 7 108

WINMAIL 85

Wo ist? 73

Wohin sichern Sicherungsplugins meine Daten? 46

- Z -

Zeichenfolgen 98

Zeitüberwachung 71

Zeitüberwachung mit Windows starten 66

ZOOM 73

ZOOM Menüleistensymbole 73

Zufallsdaten 75, 111

Zur Merkliste 19

Zuweisungsstatements 98

Zwischengespeicherte Webseiten 45