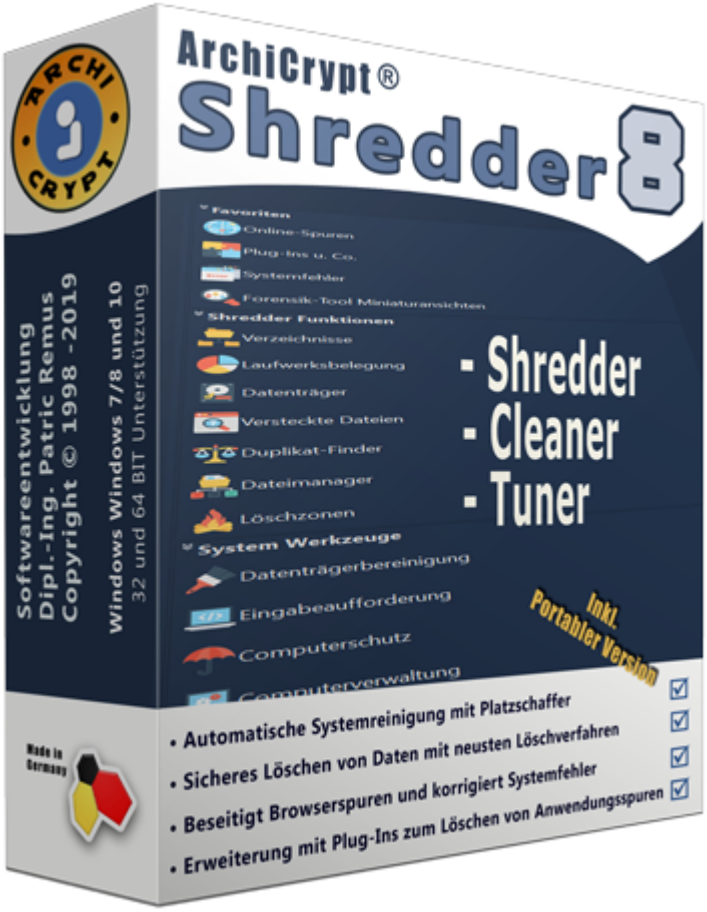
Dok.-Nr.: ACLB-HB-0008

Ausgabedatum: 17.07.2019

Ausgabe-Nr.: 8.0

Handbuch
ArchiCrypt Shredder



D-85521Ottobrunn
Telefon (089) 66000893
E-Mail Anfrage@ArchiCrypt.de

Inhalt

4 Hilfe zur Hilfe

Nutzen Sie die Hilfe

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

Folgende Kapitel sind WICHTIG:

- Installationshinweise 26
- Systemvoraussetzungen 26
- Bedienung 34

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

Symbole in der Hilfe

Innerhalb der Hilfe sind besondere Textstellen *farblich* hervorgehoben.

Hinweise mit roter Hervorhebung sollten Sie unbedingt lesen. Sie weisen häufig auf *Gefahrenquellen*, *Fehlerfallen* oder *Einschränkungen* hin oder beschreiben wichtige Sachverhalte.

Textstellen mit grüner Hervorhebung beinhalten *Tipps* und *Tricks* sowie weiterführende Hinweise.

5 Bestellen und Registrieren

Wer ArchiCrypt Shredder kaufen möchte, der kann dies zum Beispiel über den ArchiCrypt Shop im Internet erledigen. Dort können Sie auch die Pro-Version von Forensik-Tool Miniaturansichten 172 erwerben.

Bestellen bei ArchiCrypt

Informationen zu ArchiCrypt Shredder und weiteren ArchiCrypt Programmen:

https://www.ArchiCrypt.de

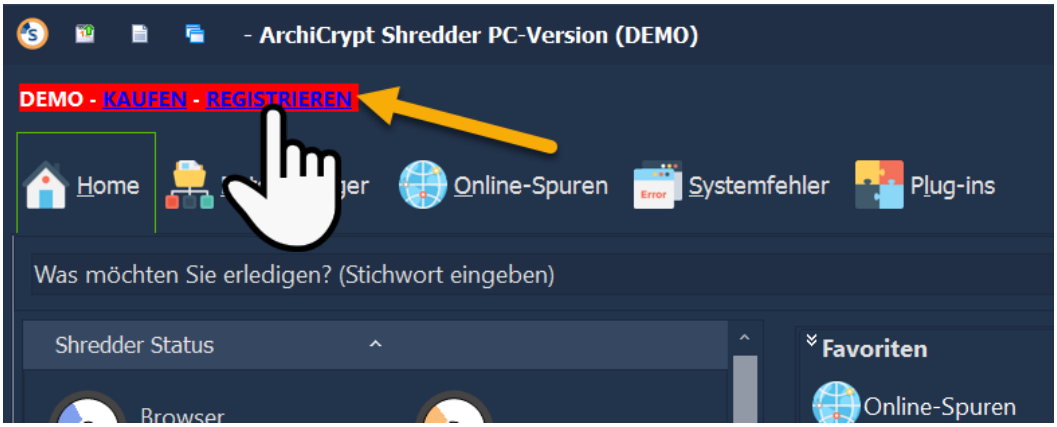
Weitere Bestellmöglichkeiten >>

So schalten Sie ArchiCrypt Software frei

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

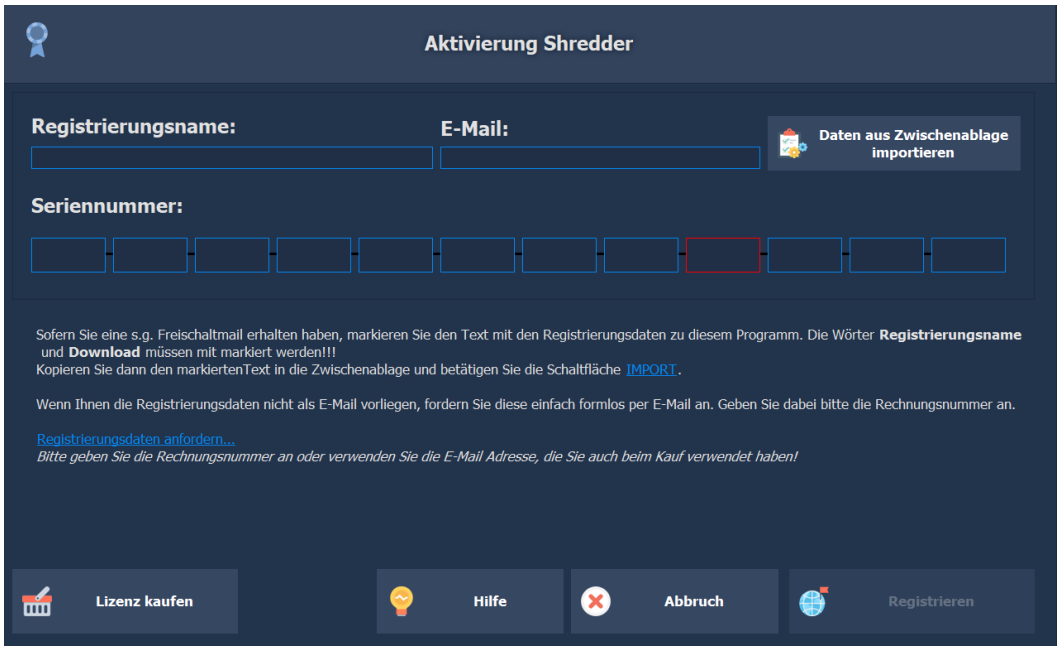
Bei anderen *ArchiCrypt Softwaretiteln* finden Sie einen entsprechenden Link ggf. an anderer Stelle. Dies wird in der jeweiligen Aktivierungsmail beschrieben. Das Vorgehen ist bei allen aktuellen ArchiCrypt Programmen identisch. Sie müssen jedoch unbedingt die Daten verwenden, die für das Programm vorgesehen sind.

Wenn Sie ein Bundle (*mehrere Programme*) erworben haben (*zum Beispiel Allstars oder Shredder + Forensik*), dann haben Sie für JEDES Programm einen eigenen Aktivierungscode erhalten.



So aktivieren Sie ArchiCrypt Shredder 8

Es erscheint der folgende Dialog:



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 mindestens die Begriffe Registrierungsname und Download: (*inklusive Doppelpunkt*) enthalten.
5. Es sollte in etwa wie folgt aussehen:

```
***Ab hier kopieren***
Registrierungsname:
Mustermann9876
E-Mail:
Max.Mustermann@MaxMustermannsSeite.de
Seriennummer:
2424-C569-8354-A7A1-A1AF-8663-B777-12BB-C3FB-C797-
DA71-6D
Download:http://download.ArchiCrypt.de/Shredder.zip
***Bis hier kopieren***
```

6. Kopieren Sie die Daten in die Zwischenablage. Dazu die Tastenkombination Strg + C verwenden oder mit der rechten

Maustaste auf den markierten Text klicken und im Kontextmenü den Eintrag "Kopieren" auswählen.

7. Klicken Sie jetzt im Registrierendialog in ArchiCrypt Shredder auf *IMPORT!*
8. Die Daten werden jetzt in das Registrierungsformular übertragen und die Registrierung wird abgeschlossen.

Manuelle Eingabe

Sie können die Angaben manuell in die jeweiligen Eingabefelder übertragen. Nicht immer stimmen Name und oder E-Mail Adresse der Registrierungsdaten komplett mit Ihren Angaben bei der Bestellung überein. Achten Sie daher darauf, dass Sie die Daten exakt so eingeben, wie in der Freischaltmail angegeben!
Nach erfolgter Eingabe klicken Sie auf die Schaltfläche Registrieren

Weitere Bestellmöglichkeiten

Weitere Bestellmöglichkeiten		
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** Dienstag - Donnerstag 09.00 - 12.00 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**	Bitte Rechnungsanschrift, Produkt, Produktanzahl und Versandart (Postversand, Download/Seriennummer) angeben. Falls Sie die Versandart "Download/Seriennummer“ wählen, geben Sie unbedingt eine E-Mail Adresse an, an die wir dann die Registrierungsdaten senden können.
Brief	**Anschrift:** Softwareentwicklung Dipl.-Ing. Patric Remus Am Brunneck 6 85521 Ottobrunn	Bitte Rechnungsanschrift, Produkt, Produktanzahl und Versandart (Postversand, Download/Seriennummer) angeben. Falls Sie die Versandart "Download/Seriennummer“ wählen, geben Sie unbedingt eine E-Mail Adresse an, an die wir dann die Registrierungsdaten senden können.
Anonym	**Anschrift:** Softwareentwicklung Dipl.-Ing. Patric Remus Am Brunneck 6 85521 Ottobrunn	Voraussetzung für den anonymen Bezug der Software ist ein E-Mail-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 E-Mail Adresse bei. Sie erhalten Ihre Registrierungsdaten dann an diese Mailadresse.

6 Einleitung

6.1 Willkommen

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

Mit ArchiCrypt Shredder beseitigen Sie unnötigen Ballast, bändigen die Datensammelwut von *Browser*, *Betriebssystem* und *Anwendungen* und sorgen dafür, dass vermeintlich gelöschte Daten wirklich unwiderruflich gelöscht werden.
Spüren Sie Systemfehler auf und reparieren Sie diese mit einem Klick. Lahme Rechner werden wieder stabil und arbeiten flott wie am ersten Tag.

Löschen von Dateien

Der Rechner, gleich ob privat oder beruflich verwendet, beherbergt unzählige *sensible Daten*, die *in den falschen Händen* einen immensen Schaden anrichten können. Sensible Daten fallen ständig an, auch dann, wenn Sie dies gar nicht denken. Beim Besuch von Internetseiten oder beim Arbeiten mit fast jeder Anwendung. Das korrekte Löschen solch sensibler Daten ist komplizierter, als es den Anschein hat.

Das Betriebssystem löscht Daten nicht wirklich

Daten, die Sie mit den Mitteln des *Betriebssystems* löschen, werden *nicht wirklich gelöscht*. Diesen Umstand machen sich Rettungswerkzeugen zunutze. Sie machen die vom System verborgenen Daten wieder sichtbar. Windows entfernt lediglich den Verweis auf die Daten. Die mitunter sensiblen Daten bleiben erhalten, bis sie zufällig beim Erstellen einer neuen Datei irgendwann einmal wirklich überschrieben werden. Das kann ein paar Stunden dauern, gerne aber auch Wochen und Monate!

Moderne Browser bieten oft Funktionen an, mit denen man den Verlauf, Cache und Co. (Zwischengespeicherte Dateien, Bilder, besuchte Seiten, Cookies etc.) löschen kann. Wer jetzt denkt, diese Dateien seien wirklich gelöscht, irrt gewaltig. Moderne Browser verteilen Informationen über Ihr Nutzerverhalten, Seiteninhalte, Cookies und unzählige Statistiken quer über das gesamte Windowssystem. In unzähligen Dateien, kleinen Datenbanken und der Registry werden Informationen gesammelt, die genau darüber Auskunft geben, wann Sie welche Inhalte besucht und betrachtet haben. Inklusive der angezeigten Texte und Bilder. Hier selbst den Überblick zu behalten und bei Bedarf die Daten zu entfernen ist äußerst komplex, zeitraubend und nahezu unmöglich. Auch Löschen mit Bordmitteln genügt natürlich nicht. Wer sicher sein will, dass diese Daten entfernt werden, muss spezielle Löschtechniken anwenden.

Anwendungen sind unsicher

Viele Anwendungen erstellen s.g. temporäre Dateien. Es handelt sich dabei um eine exakte Kopie der Arbeitsdatei. Gearbeitet wird mit dieser Kopie. Erst dann, wenn es zu keinem Absturz kommt und Sie die Datei speichern, wird die Kopie wieder entfernt. Das Problem: Diese temporären Dateien werden im besten Fall mit unsicheren Systemmitteln gelöscht. Im ungünstigsten Fall verbleiben diese Dateien mit allen Inhalten als Platzfresser oder Sicherheitsleck auf dem Rechner.

Wo ist der Speicherplatz hin verschwunden?

Egal wie groß eine Festplatte ist, irgendwann ist Sie zu klein. Wo ist der Speicherplatz hin, welche Dateien belegen den ganzen Platz? Wie putze ich das System. Ein manueller Versuch, die Speicherfresser aufzuspüren ist unglaublich zeitintensiv. Einfaches Löschen der mutmaßlich unnötigen Dateien kann sogar das System instabil machen. Shredder hilft mit dem Platzschaffer und Laufwerksanalyse dabei, die Speicherungetüme aufzuspüren und diese so zu löschen, dass das System maximal stabil ist.

Mehrfach vorhandene Dateien

Wer einen PC länger im Einsatz hat, kennt das Phänomen. Man kopiert Dateien von A nach B, von B nach C, benennt um, sichert, verschiebt und verliert so langsam aber ganz sicher den Überblick. Dubletten belegen wertvollen Speicherplatz und sind mit herkömmlichen Methoden nicht mehr auffindbar.
Der Duplikatfinder findet diese *Datei-Dubletten* auch über Datenträger hinweg. Sogar dann, wenn die Dateien umbenannt wurden. Um im Falle einer Fehlentscheidung das Entfernen wieder zurückzunehmen, werden Duplikate zunächst in eine Quarantäne verschoben, aus der Sie die Dateien wieder herstellen können.

Systemfehler aufdecken und beseitigen

Installation und Deinstallation von Programmen, das Einspielen von Updates, Hotfixes und Patches und natürlich das tägliche Arbeiten mit dem Rechner sorgen dafür, dass sich mit der Zeit Fehler in das System einschleichen. Diese wirken sich mal mehr, mal weniger dramatisch aus. Nicht immer muss es sich dabei um einen Fehler handeln, der zu einem Totalabsturz des Rechners führt.

Selbst wenige kleine Fehler genügen, um aus einem leistungsfähigen und schnellen Rechner mit der Zeit eine lahme Krücke zu machen.

Die Systemfehlerbeseitigung stellt verschiedene Fehler-Kategorien zur Verfügung. Entsprechende Fehler werden aufgezeigt und können korrigiert werden. Änderungen, die bei der Fehlerbeseitigung am Rechner vorgenommen werden, werden zunächst in eine Quarantäne verschoben und können bei Bedarf wieder rückgängig gemacht werden.

Versteckte Daten (Alternative Datenströme)

Mit so genannten Alternativen Datenströmen (*Alternate Data streams*) stellt das Windows Betriebssystem eine wenig bekannte Methode bereit, in Bereichen hinter Dateien, verborgen vor den Augen eines normalen Anwenders, beliebige Daten zu speichern. Diese alternativen Datenströme belegen Platz und bieten aufgrund ihrer Eigenschaften Schadprogrammen (*Viren/Trojanern*) ideale Versteckmöglichkeiten. ArchiCrypt Shredder spürt solche Daten nicht nur auf, sondern kann Inhalte anzeigen und natürlich sicher entfernen!

Sammelwut des Betriebssystems bändigen

Die wenigsten Anwender wissen, wie Neugierig das Betriebssystem wirklich ist. Die Absichten des Systemherstellers sind mitunter durchaus gut. Das Arbeiten mit dem Rechner soll durch bestimmte Vorberechnungen flotter werden, das Nutzererlebnis soll verbessert besser werden. Oft erkauft man sich diese meist nicht spürbaren "Verbesserungen" durch eine unglaubliche Menge an Daten die über das eigene Verhalten Auskunft geben. In s.g. *User-Assist Daten* wird minutiös aufgezeichnet, welche Programmen man mit welchen Parametern startet. Das ganze auch noch schlecht verschlüsselt. Bilder und Videos landen in einer speziellen Datenbank, um Vorschaubilder später ein paar Millisekunden schneller anzeigen zu können.

ArchiCrypt Shredder 8 kann die *Nutzer-Assistenzdaten* entschlüsseln und, in der Vollversion mittels Plug-In auch löschen. Das Forensik-Tool Miniaturansichten[172] kann die Bilder und Vorschaubilder der einschlägigen Windows-Datenbanken anzeigen und, in der Vollversion, Bilder daraus als Bilddatei speichern.

Solid State Disk macht sicheres Löschen kompliziert

SSDs sind schnell und inzwischen durchaus zuverlässig. Was vielen Anwendern nicht bekannt ist, ist der Umstand, dass Daten nur sehr schwer verlässlich von einer SSD gelöscht werden können. ArchiCrypt

Shredder hat verschiedene SSD-Funktionen[65] an Bord, mit denen das Löschen

Mobile Nutzung

Mit der *PC-Version von ArchiCrypt Shredder* können Sie sich eine portable ArchiCrypt Shredder Version mit den wichtigsten Funktionen erzeugen, die dann von einem USB-Stick oder einer externen Festplatte verwendet werden kann.

Plug-ins

Plug-ins erweitern die Funktionalität des Shredders. Die Vollversion von ArchiCrypt Shredder bringt unzählige Plug-ins mit, die die Spuren und Hinterlassenschaften zahlreicher Anwendungen beseitigen. Mit *speziellen Plug-Ins für Windows 10* räumt die Vollversion von ArchiCrypt Shredder den Rechner richtig auf.

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

Dipl.-Ing. Patric Remus

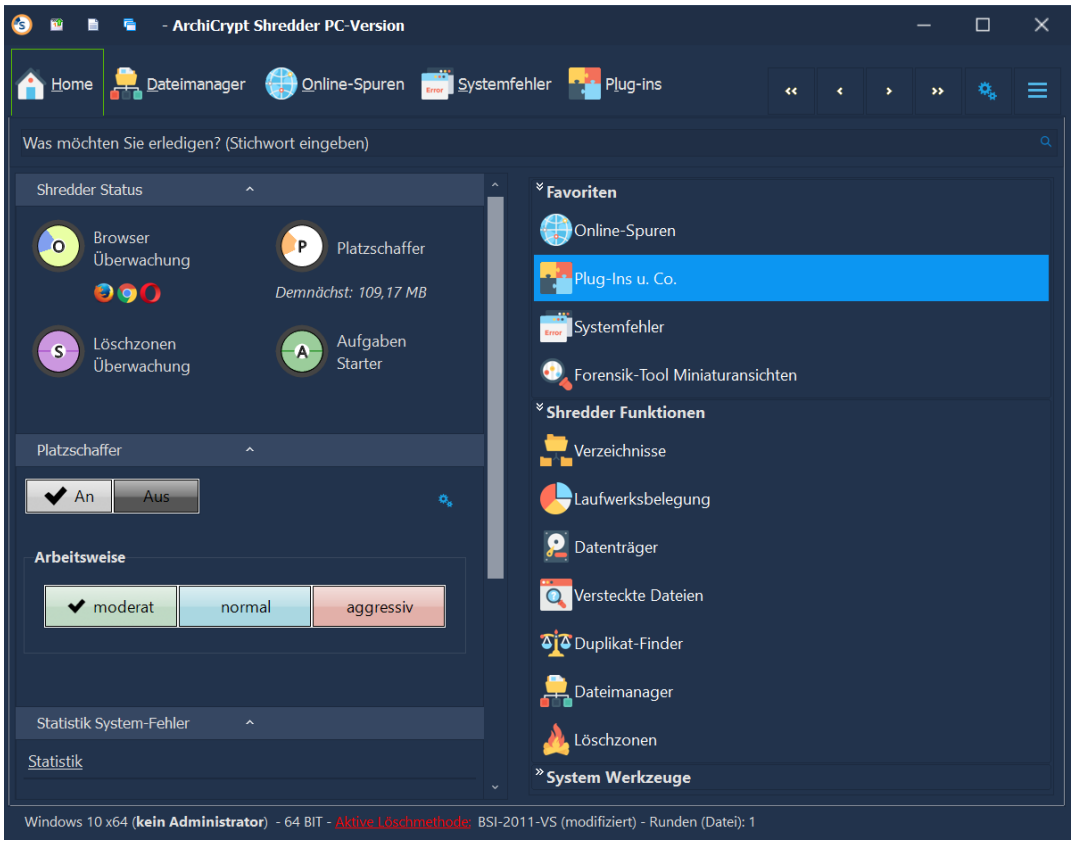
6.2 Neu in Shredder Version 8

History / Changelog

ArchiCrypt Shredder 8 - Neuerungen

Die Top Highlights

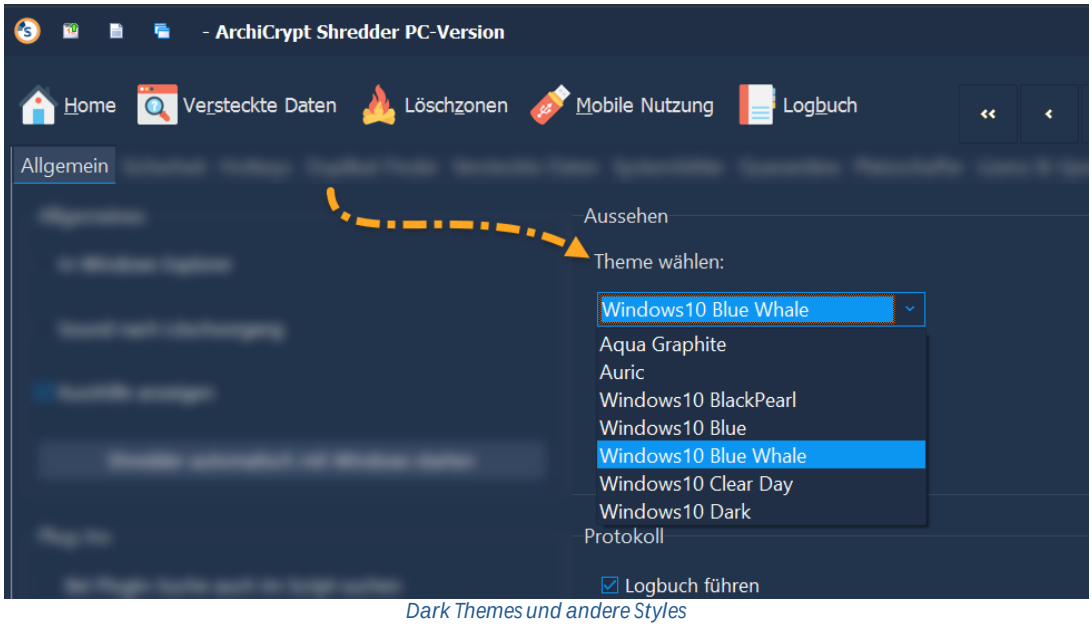
Das einstige Löschwerkzeug ist jetzt ein *unverzichtbares* Schweizer Taschenmesser *für jeden PC Besitzer*.



ArchiCrypt Shredder 8

Dark Theme und andere Styles

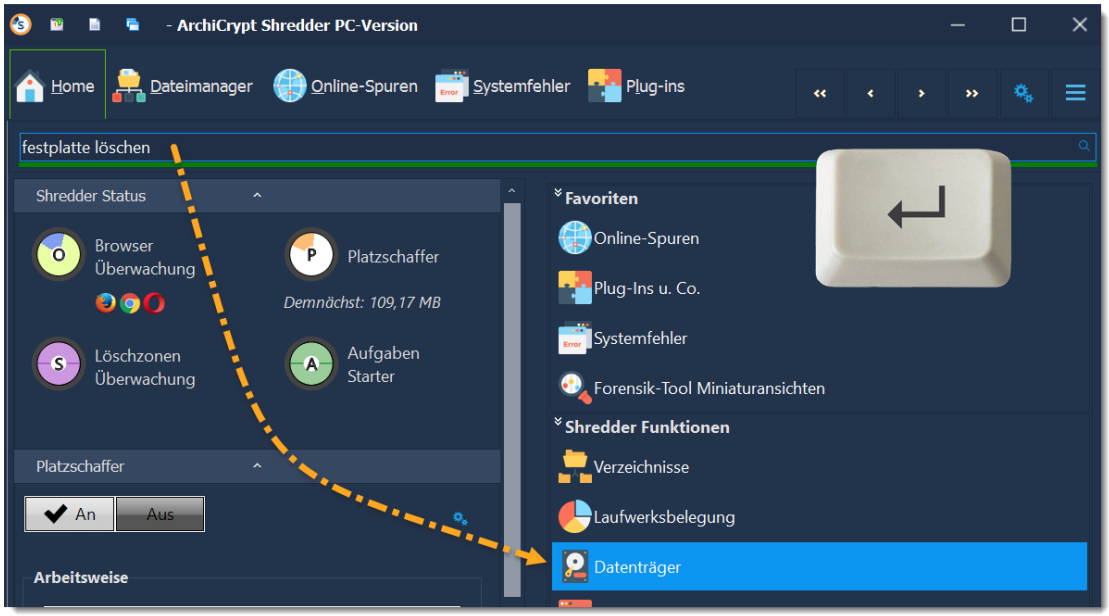
Geschmäcker sind bekanntlich verschieden. Shredder 8 bietet jetzt *Styles* für jeden Geschmack. Insbesondere die Dark Themes sind eine Augenweide. Kontrastreich und ideal für ermüdungsfreies Arbeiten. Die Unterstützung von hochauflösenden 4K Monitor en und Multimonitor-Systemen ist ein weiteres Merkmal der neuen Bedienoberfläche.



Dark Themes und andere Styles

Komplett überarbeitete Home-Ansicht

Die Home-Ansicht ist der Einstieg in die zahlreichen Funktionen des Shredders. Alle wesentlichen Elemente kann man hier rasch auffinden. Geben Sie einfach ein Stichwort wie "*Festplatte löschen*" oder "*Browserspuren*" ein und Sie gelangen mit der Eingabetaste direkt zur Funktion im Shredder.



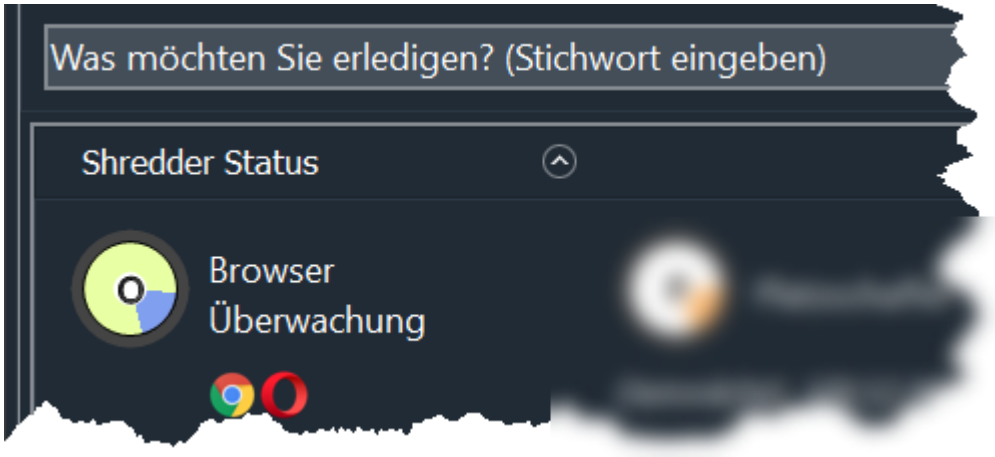
Home-Ansicht von ArchiCrypt Shredder 8

Windows 10

ArchiCrypt Shredder wurde in allen Grundfunktionen auf *Windows 10* ausgerichtet. Spezielle Anpassungen der System-Fehlersuche[110], der Funktionen zum Löschen der Papierkörbe und ganz neue Spezial-Plug-Ins stellen Windows 10 in den Mittelpunkt, ohne dabei Abstriche bei der Unterstützung von Window7 und Windows 8 zu machen.

Unterstützte Browser werden einzeln behandelt

Die weit verbreiteten Browser *Google Chrome*, *Firefox*, *Edge* und *Opera* werden auf der Home Seite angezeigt, sobald die Überwachung einen dieser Browser erkennt. Die Browserspuren werden jetzt nicht mehr komplett nach dem Beenden des letzten aktiven Browsers gelöscht, sondern jeweils für den Browser, der beendet wurde.

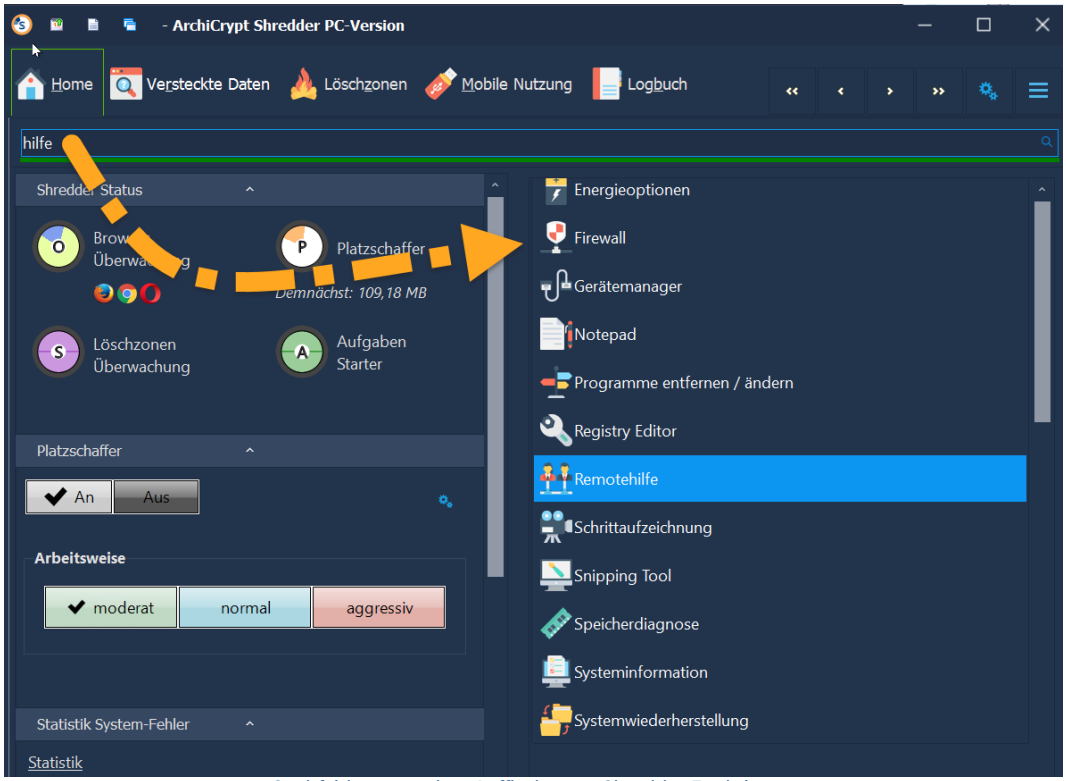


Der *Edge Browser* ist tief im Windows System verankert. Windows behandelt diesen Browser auf eine ganz besondere Weise. So wird Edge zum Beispiel nie ganz beendet, sondern immer wieder gestartet und in eine Art *Tiefschlaf* versetzt. Die Folge dieser Arbeitsweise ist, dass die Spuren des Browsers nicht verlässlich gelöscht werden können. ArchiCrypt Shredder bietet hier die Möglichkeit, die Einstellungen im Windows System so zu ändern, dass der Browser beim Schließen korrekt beendet und die Spuren damit richtig gelöscht werden können.

Edge-Browser zügeln

Schneller Zugriff auf Werkzeuge und Systemeinstellungen

Gleich, ob es um *Energieeinstellungen*, *Systeminformationen*, *Notepad*, die *Firewall* oder die Sicherung handelt, mit der erweiterten Suchfunktion im Shredder haben Sie direkten Zugriff auf die Funktion. Ganz ohne sich durch zahlreiche Systemdialoge oder Verzeichnispfade kämpfen zu müssen. Einfach *Schlagwort eingeben und Eingabetaste* betätigen.

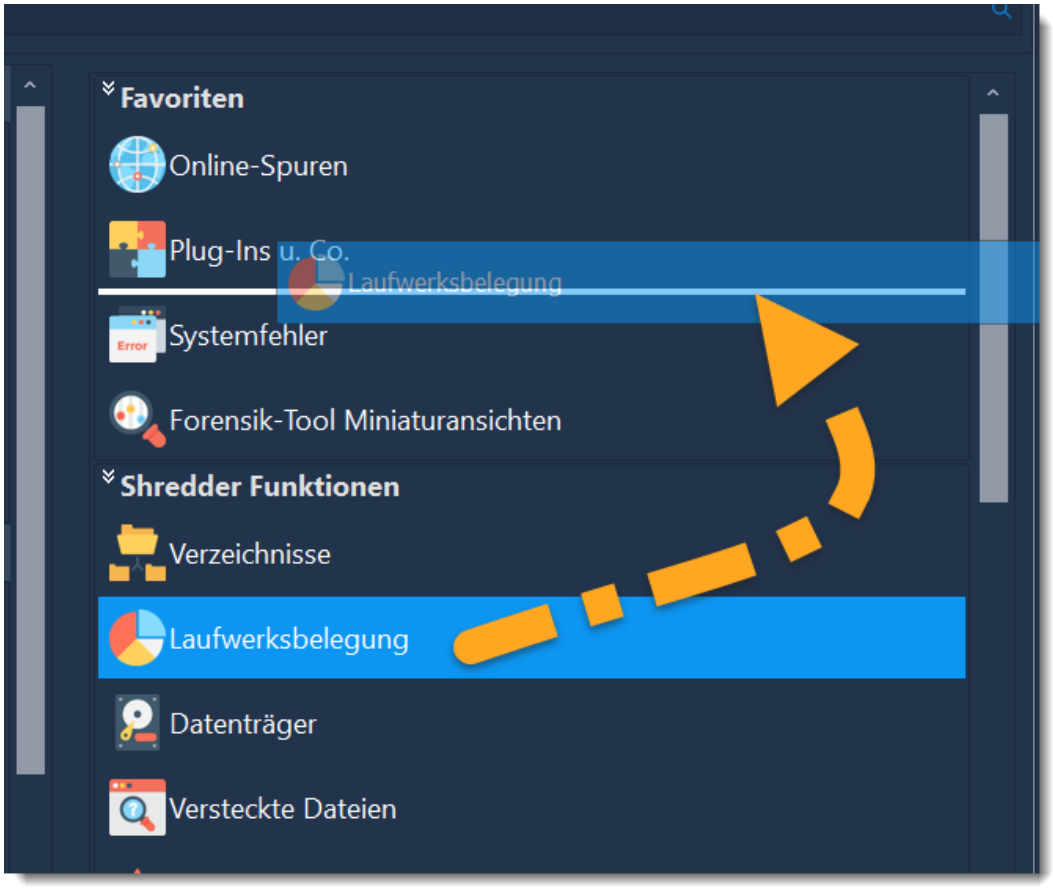


Suchfeld zum raschen Auffinden von Shredder-Funktionen

Favoriten für Funktionen und Werkzeuge

Dynamische Menüs, die sich selbst nach Häufigkeit des Aufrufs anordnen, haben tatsächlich eher zur Verwirrung der Anwender beigetragen. Die Microsoft Office Programme sind hier gute bzw. eben schlechte Beispiele. Viel besser ist es, wenn man als Anwender selbst die Möglichkeit hat, *Funktionen anzuordnen*.

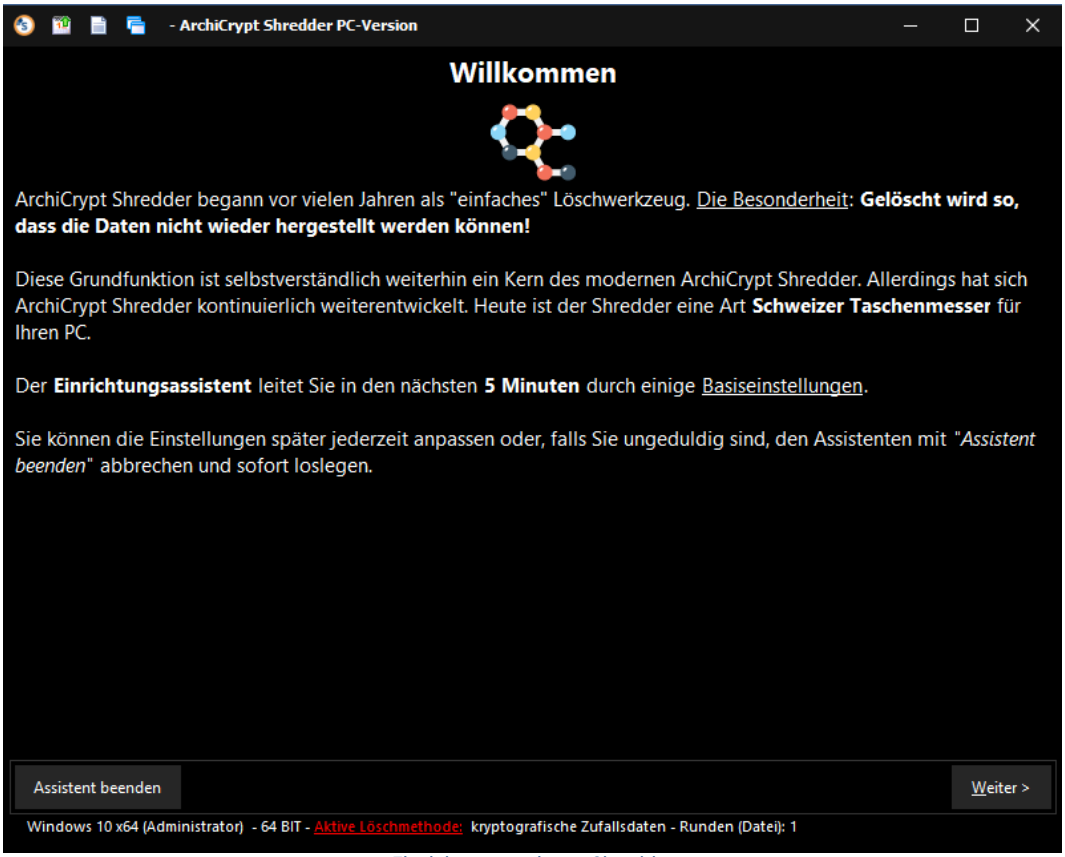
Ziehen Sie die Funktionen in der Home-Ansicht einfach an die Position, an der Sie sie möchten. Machen Sie Funktionen des Shredders oder des Systems einfach zum Favoriten.



Anpassbare Menüs

Einrichtungsassistent

Wer ArchiCrypt Shredder kennt, der wird sich schnell zurecht finden und die wesentlichen Punkte kennen, die es beim Einrichten ggf. zu beachten gilt. Um es Neueinsteigern zu erleichtern, sich in der Vielfalt der Shredder-Funktionen sofort Zuhause zu fühlen, gibt es einen Einrichtungsassistenten, der bei der Ersteinrichtung hilft.

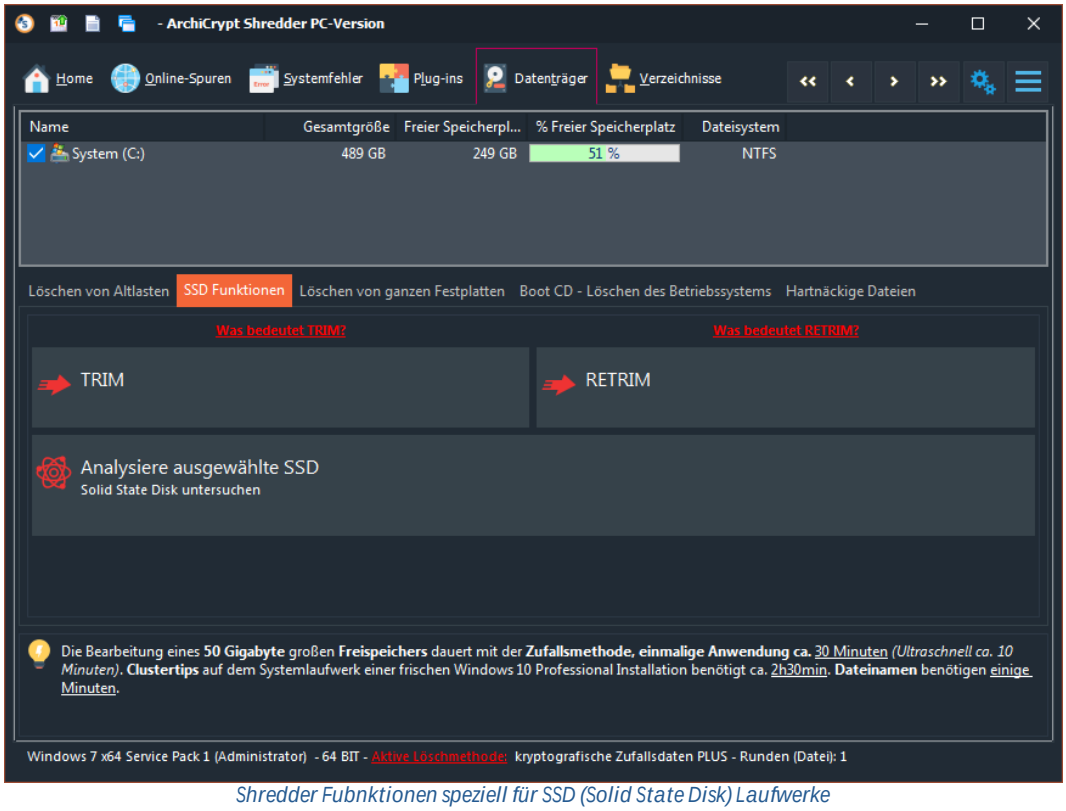


Einrichtungsassistent Shredder

Spezielle Funktionen für SSD (Solid State Disk)

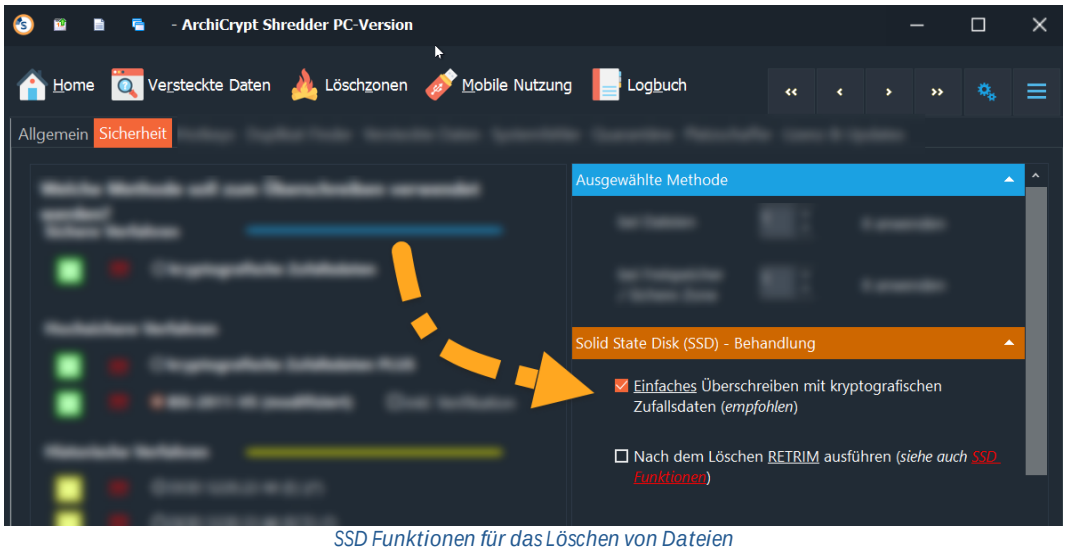
In vielen aktuellen Rechnern kommen s.g. SSDs (*Solid State Disks*) zum Einsatz. Bei dieser Art von Datenträgern handelt es sich um Speichermedien, die gänzlich anders arbeiten als normale, magnetisierbare Medien. Hier wird elektronisch gespeichert, es gibt keine *beweglichen Teile*. Beim *sicheren Löschen von einer SSD* müssen ganz andere Dinge beachtet werden, als bei den Rotationsmedien mit mechanischen Bauteilen.

ArchiCrypt Shredder 8 bietet in der Rubrik Datenträger[60] spezielle Funktionen für SSD Laufwerke an.



Shredder Fubnktionen speziell für SSD (Solid State Disk) Laufwerke

An anderen Stellen kann man das Verhalten des Shredders für den Fall festlegen, dass Daten auf einer SSD gelöscht werden. Bevor Daten künftig gelöscht werden, wird immer dann, wenn es sich um ein *Solid State Drive* handelt, die Löschoperation gemäß Ihren Einstellungen ausgeführt.



SSD Funktionen für das Löschen von Dateien

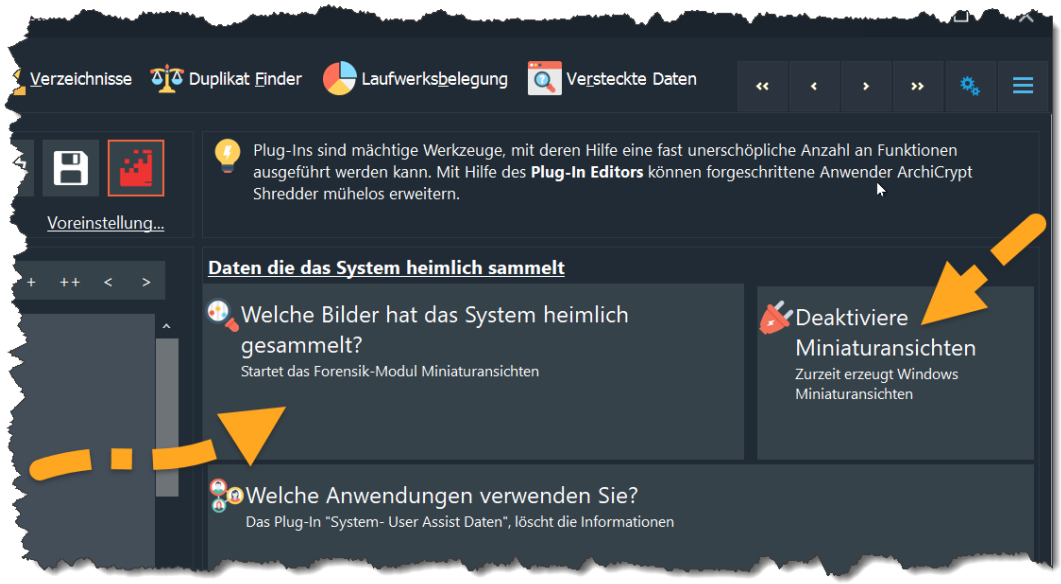
Spezielle Windows 10 Plug-Ins

Die Vollversion von ArchiCrypt Shredder kommt mit einer ganzen Reihe von speziellen *Windows 10 Plug-Ins*.

Spezielle Shredder Plug-Ins für Windows 10

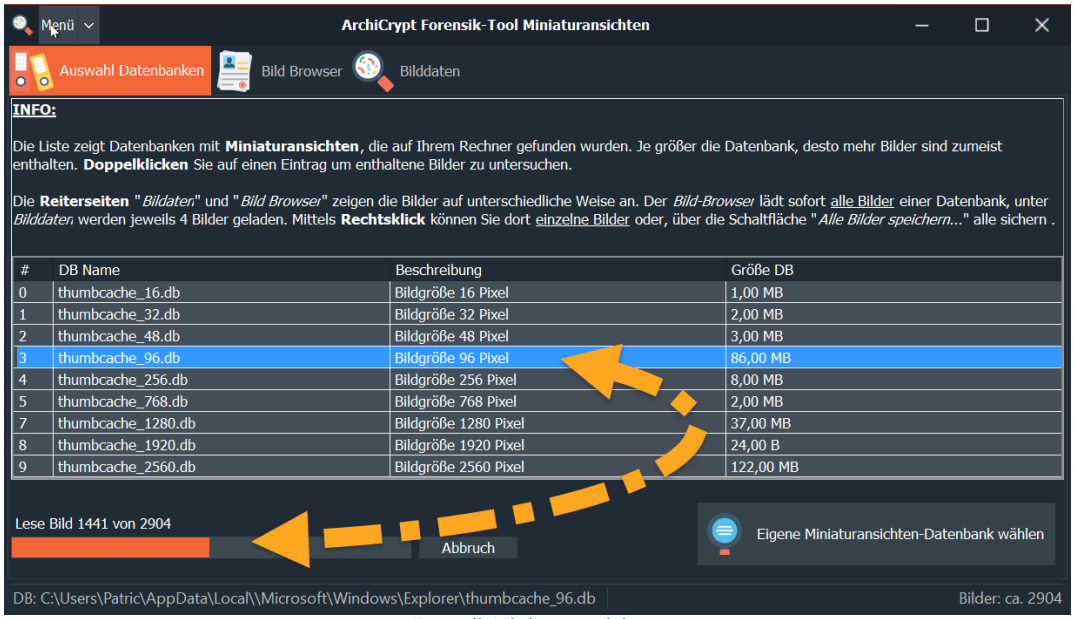
Forensik Werkzeug Miniaturansichten

Es genügt bereits, sich den Inhalt eines Ordners im Windows Explorer (*oder einem anderen Dateimanager*) anzeigen zulassen. Sofort erzeugt Windows eine "Miniaturansicht" der Bilddatei, fertigt ein *Standbild eines Videos* an oder eine *Vorschau für ein Textdokument* (*PDF, Word, etc.*). Diese Bilddaten werden in verschiedenen *Datenbanken in Windows* abgelegt und sind im Normalfall für den Anwender unsichtbar. ArchiCrypt Shredder bringt das Programm Forensik-Modul Miniaturansichten[172] mit.



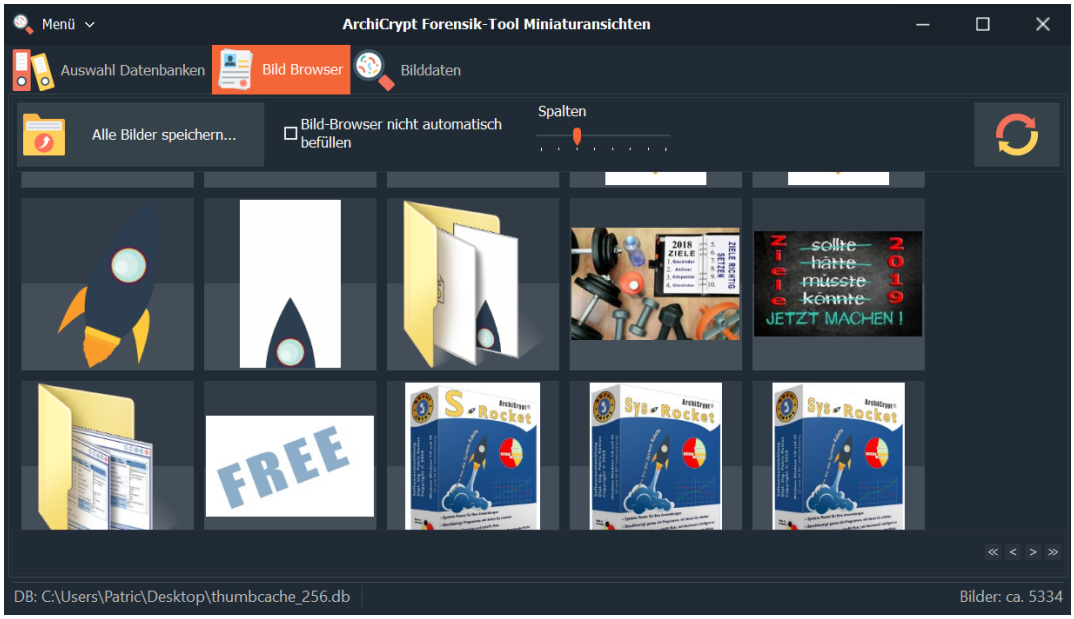
Vorschaubilder Windows 10

Das Programm Forensik-Tool Miniaturansichten ist mindestens in einer **Standard-Version**[174] enthalten. In der Standard-Version kann man sich die *ersten 50 Bilder* in einer Bild Datenbank ansehen. Einige Kauf-Versionen des Shredders enthalten die ggf. *Pro-Version von Forensik-Tool Miniaturansichten*[175]. In Ihrer Freischaltmail ist dann zusätzlich zu den Registrierungsdaten des Shredders der entsprechende Schlüssel zur *Aktivierung von Forensik-Tool Miniaturansichten* enthalten. Sie müssen die Pro-Version also getrennt von ArchiCrypt Shredder aktivieren. Das Forensik-Modul kann auch gesondert im ArchiCrypt Shop erworben und nachträglich aktiviert.



Forensik Miniaturansichten

In der Pro-Version können Sie alle Bilder einer Datenbank laden und betrachten. Zusätzlich besteht die Möglichkeit, *einzelne Bilder oder alle Bilder in ein Verzeichnis zu sichern*.



Bilder aus Vorschaudatenbank extrahieren

In der Vollversion von ArchiCrypt Shredder können Sie Windows komplett davon abhalten, Vorschaubilder zu erzeugen (*Deaktiviere*

Miniaturansichten[108]) oder via Plug-In (*Windows 10*) angelegte Bilddatenbanken zu löschen.

Darüber hinaus werden Sie an unzähligen Stellen Verbesserungen, zusätzliche Funktionen und Optionen finden.

7 Allgemeine Informationen

7.1 Installationshinweise

Das Programm wird mit einer eigens entwickelten Installationsroutine geliefert, die Ihnen die Arbeit abnimmt.

Achten Sie darauf, dass Sie für die Installation Administratorrechte besitzen müssen.

Bei der Installation werden keine Systemdateien ersetzt oder geändert.

7.2 Systemvoraussetzungen

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

Unterstützte Betriebssysteme
32 BIT und 64 BIT Versionen - Windows 7 mit SP1, Windows 8 und Windows 10

Einige Funktionen stehen ausschließlich für Windows 10 zur Verfügung. Darunter die SSD-Funktionen[65] und RETRIM[55], die Windows 10 Spezial-Plug-Ins

Unterstützte WEB-Browser
Edge/Internet Explorer, Opera, Firefox und Google Chrome
mit Versionsstand Juni 2019

Minimale Systemanforderungen

Microsoft Windows 7 mit SP1
Bildschirmauflösung 1024x768 mit 32 BIT Farbtiefe
ca. 80 MB freier Festplattenplatz
Intel Pentium oder AMD K5 Prozessor mit mindestens 200 MHz
2024 MB RAM
CD-ROM oder DVD-ROM-Laufwerk (optional)

Empfohlene Systemkonfiguration

Microsoft Windows 10
Bildschirmauflösung 1024x768, mit 32 BIT Farbtiefe
120 MB freier Festplattenplatz
4048 MB RAM
CD-ROM oder DVD-ROM-Laufwerk

Lesen Sie sich unbedingt das Kapitel Einsatz unter Windows 7, Windows 8 und Windows 10 28 durch.

➡**ACHTUNG:**
Zum Ausführung benötigen Sie grundsätzlich Administratorrechte.

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

7.3 Besonderheiten Windows 7, 8 und 10

Warum erfordert ArchiCrypt Shredder Administratorrechte?

Windows 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 Nutzer Administratorrechte besitzen. Da ArchiCrypt Shredder für die allermeisten Funktionen Administratorrechte benötigt, wird das Programm grundsätzlich mit entsprechenden Rechten gestartet. **Anwender, die nicht der Gruppe der Administratoren angehören (z.B. Gast) können ArchiCrypt Shredder nicht verwenden!**

Edge Browser in Windows 10

Neuere Version des Microsoft Betriebssystems Windows 10 laden Programme sofort mit Systemstart und beenden diese auch nicht mehr. ArchiCrypt Shredder kann so nicht erkennen, wann der Edge Browser beendet wurde. Zudem blockiert der Browser Dateien, die beim Beseitigen von Spuren bearbeitet werden müssen. Der Shredder bietet in der Rubrik Online-Spuren 87 die Funktion **Edge Browser vorbereiten** 90, mit der der Browser passend eingerichtet werden kann.

Löschen unter Windows

Das Windows Betriebssystem kann s.g. Schattenkopien anfertigen. Schattenkopien sind Dateien, die Dateien in einem älteren Zustand repräsentieren.

Neben diesen Schattenkopien gibt es zusätzlich s.g. Wiederherstellungspunkte.

Welche Daten werden in einem Wiederherstellungspunkt gespeichert?

Ein *Wiederherstellungspunkt* wird das aktuelle Treiberabbild gespeichert. Mit diesem Treiberabbild können Sie den Rechner im Falle eines Falles wieder so herstellen, dass das System startet. Dokumente, installierte Programme und andere werden in Wiederherstellungspunkten nicht gesichert. Wiederherstellungspunkte sind also keinesfalls ein Ersatz für eine ordentliche Sicherung Ihrer Daten.

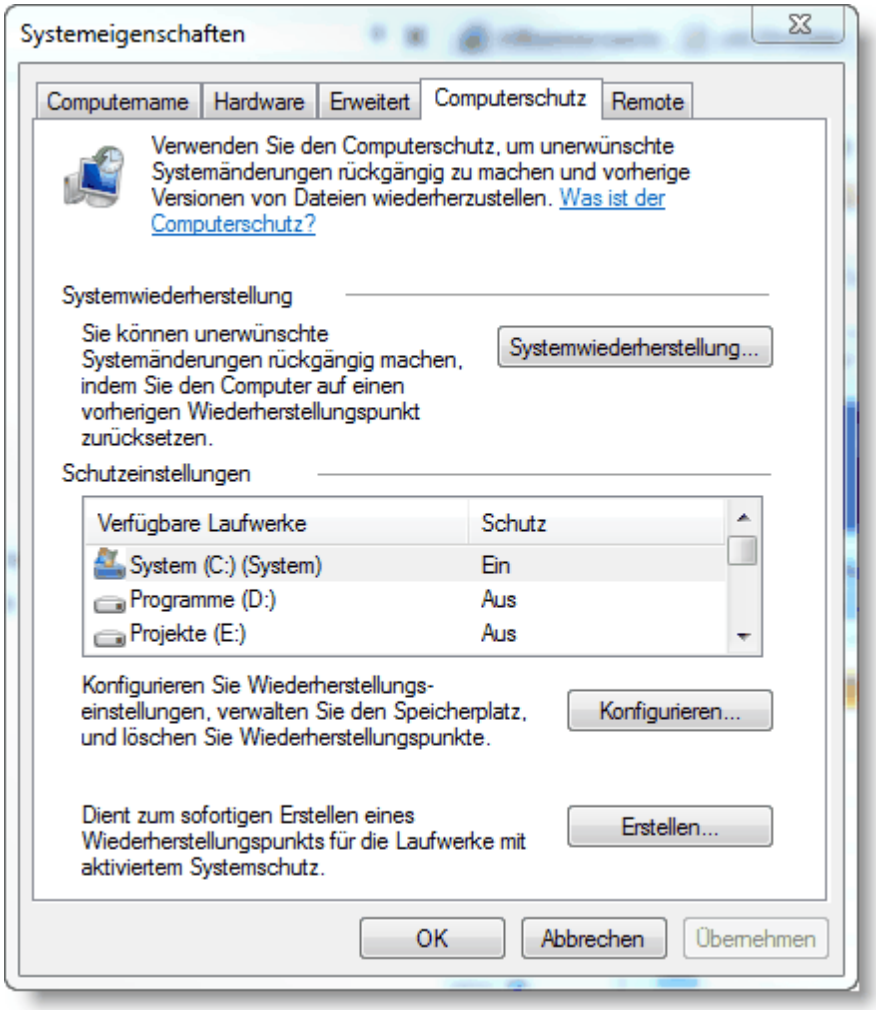
Schattenkopien sind quasi Abbilder der gesamten Festplatte. In ihnen werden also auch Änderungen an Arbeitsdaten festgehalten.
Wenn Sie zum Beispiel ein Word-Dokument speichern und plötzlich feststellen, dass Sie doch lieber wieder die Version von vor zwei Tagen möchten, können Sie über die Schattenkopien eventuell auf diese Sicherung zurückgreifen. Diese an sich nützliche Funktion steht leider in völligem Widerspruch zur Absicht, Daten so zu löschen, dass sie nicht wieder herzustellen sind. Es bleibt nur der Weg, die Schattenkopien zumindest kurzzeitig zu deaktivieren.

Schattenkopie ist kein Backup!

Schattenkopien sind kein Ersatz für eine ordentliche Sicherung der wichtigen Arbeitsdaten. Eine Schattenkopie wird immer auf dem gleichen Datenträger erzeugt, auf dem die Daten selbst liegen. Tritt ein Defekt auf, sind Daten und zugehörige Schattenkopie zerstört. Unter Umständen erkennt das System auch nicht jede Änderung einer Datei.

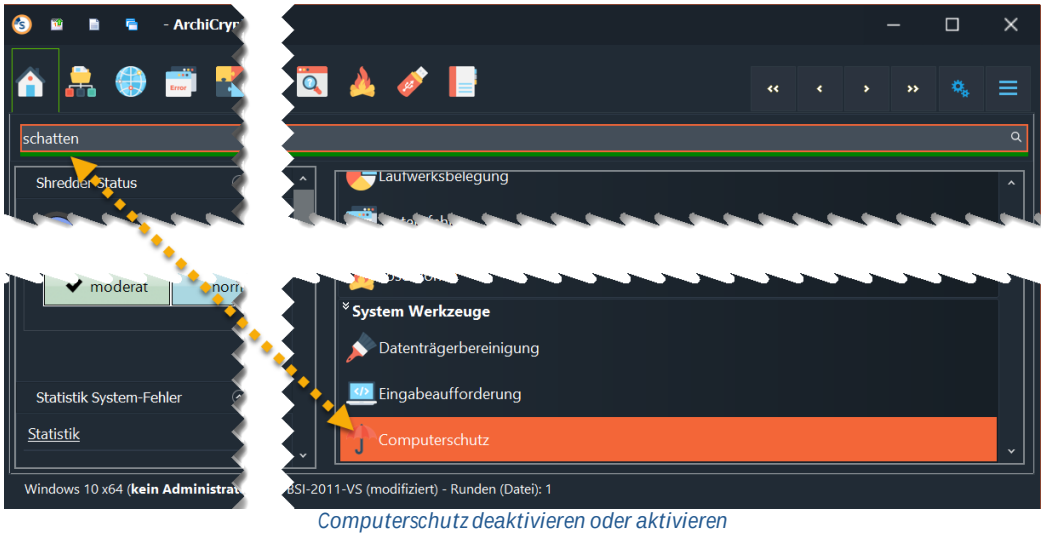
So deaktivieren Sie die Schattenkopie-Funktion

Windows 7, 8: Gehen Sie zu Systemsteuerung-System und Sicherheit - System. Klicken Sie links auf Erweiterte Systemeinstellungen jetzt wechseln Sie bitte auf die Seite Computerschutz.



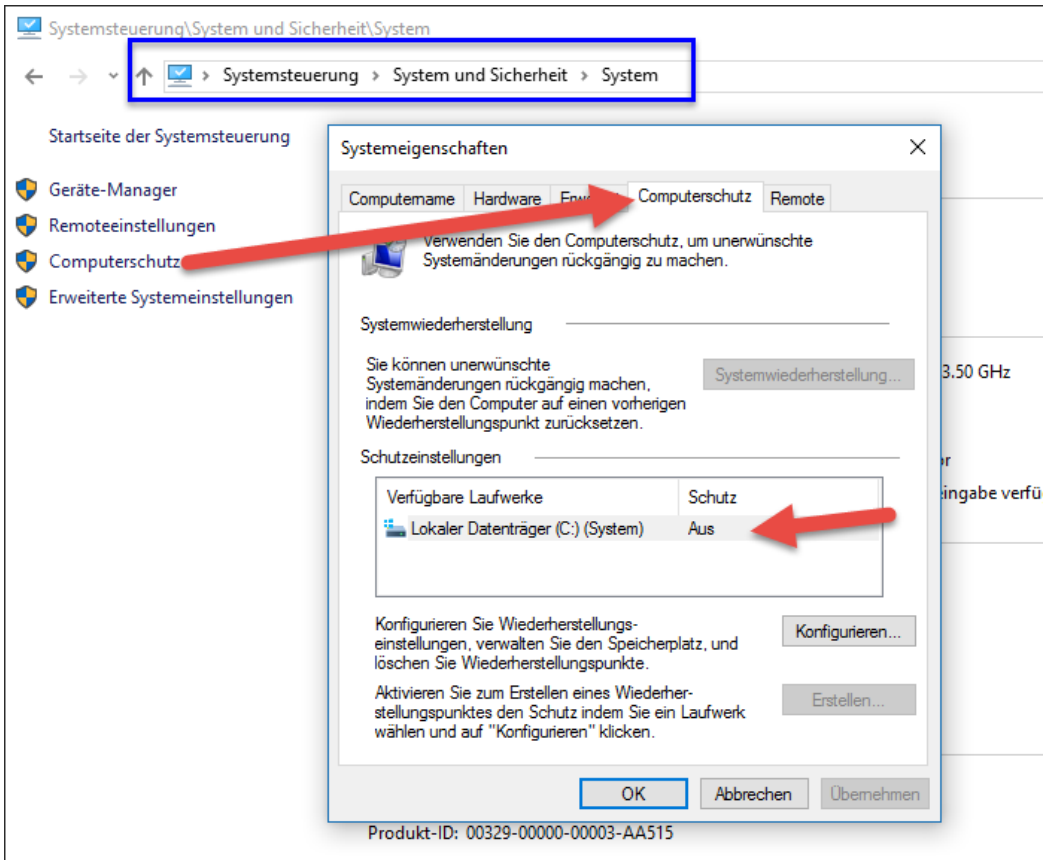
Im Dialog Systemeigenschaften wird die Registerseite Computerschutz angezeigt. Hier können Sie die Einstellungen für jedes Laufwerk ändern.

Alternativ wechseln Sie im Shredder zur Home-Ansicht, geben dort in das Suchfeld🗋44 "*Schatten*" ein und betätigen die Eingabetaste.



Computerschutz deaktivieren oder aktivieren

Windows 10



Computerschutz unter Windows 10

Auch hier können Sie die Funktion direkt über den Shredder aufrufen.[30]

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 62. Einmal deaktiviert, werden keine Schattenkopien oder Wiederherstellungspunkte mehr erstellt.

Überwachter Ordnerzugriff

In Windows 10 wurde mit dem *Fall Creators Update* der s.g. kontrollierte Ordnerzugriff eingeführt. Der kontrollierte Ordnerzugriff in Windows Defender Security Center überprüft Anwendungen, die Änderungen an Dateien in geschützten Ordnern vornehmen können. Gelegentlich wird eine Anwendung, die sicher ist, als schädlich identifiziert. Damit ArchiCrypt Shredder 8 einwandfrei funktioniert, müssen Sie einige Anpassungen vornehmen und bestimmten Anteilen von ArchiCrypt Shredder 8 Zugriff auf geschützte Ordner und Dateien gewähren. Ohne diese Maßnahme ist nicht garantiert, dass Spuren aller Art sicher beseitigt werden.

1. Wählen Sie Start > Einstellungen aus.
2. Wählen Sie Update und Sicherheit > Windows Defender aus.
3. Wählen Sie Windows Defender Security Center öffnen aus.
4. Wählen Sie Viren- & Bedrohungsschutz und dann Einstellungen für Viren- & Bedrohungsschutz aus.
5. Aktivieren oder deaktivieren Sie Überwachter Ordnerzugriff.

Falls der kontrollierte Ordnerzugriff aktiviert ist, fügen Sie bitte folgende Dateien zu der Liste mit Ausnahmen.

Sollte die Datei rundll32-low.exe nicht existieren, warten Sie bitte ab, bis eine Windows Warnung mit dem Hinweis auf diese Datei erscheint. Die Datei wird während der Ausführung bestimmter Aktionen durch ArchiCrypt Shredder 8 erstellt und kann dann eingetragen werden.

Nicht löschbare Dateien

In Windows gibt es *Dateien auf Datenträgern* 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 nur wichtige Komponenten des Betriebssystems so geschützt werden, generell nicht gelöscht werden dürfen und auch keine sensiblen Daten beinhalten.

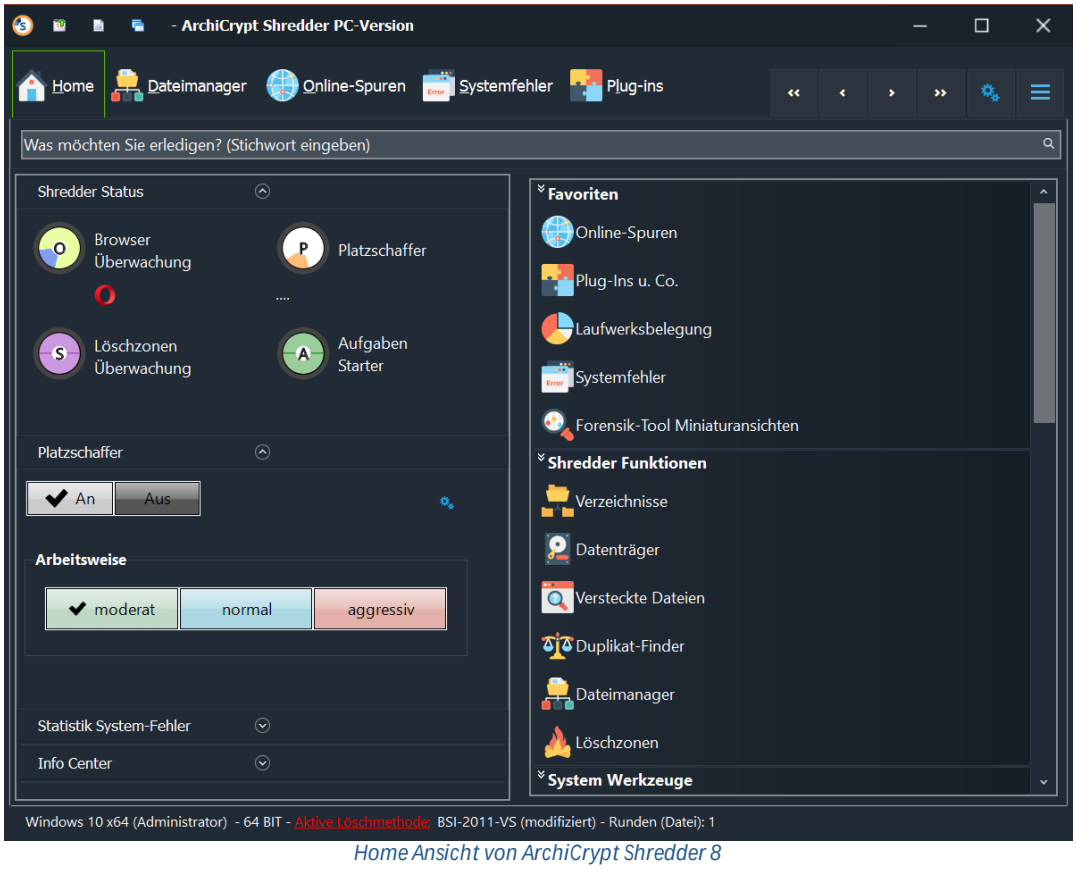
Das Löschen solcher Daten hätte in den meisten Fällen ein nicht mehr funktionierendes System zur Folge!

8 Bedienung ArchiCrypt Shredder

8.1 Ein erster Überblick

Überblick

Mit ArchiCrypt Shredder befreien Sie Ihr Betriebssystem von unnötigem Ballast und löschen Daten so, dass diese mit softwaretechnischen Mitteln nicht wieder hergestellt werden können. Fehler, die das System ausbremsen werden gefunden und können beseitigt werden.



Home Ansicht von ArchiCrypt Shredder 8

Die 12 Hauptkategorien

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

Hauptkategorien	Beschreibung
 Platzschaffer 49	Während Sie mit Windows arbeiten, werden im Hintergrund ununterbrochen Dateien und Daten gesammelt und geschrieben. Dabei verbleiben Reste auf dem Rechner, die man manuell nur mit extremem Aufwand auffinden und beseitigen kann. Meist gibt man nach ein paar Monaten aufgrund eines immer knapper werdenden Speichers und immer

Hauptkategorien	Beschreibung
	langsamerem Rechner auf und installiert das System neu. Der Platzschaffer arbeitet kontinuierlich im Hintergrund, spürt an einschlägigen Stellen im System unnötige Daten auf und beseitigt diese.
 Dateien 51	Verwalten Sie Ihre Dateien und Ordner mit dem Dateimanager. Ziehen Sie Dateien, die sicher gelöscht werden sollen, einfach per Drag & Drop auf das Merkfeld.
 Verzeichnisse 55	Haben Sie bestimmte Verzeichnisse in denen Sie ständig Daten ablegen, die nach kurzer Zeit nicht mehr von Bedeutung sind? Das *Downloadverzeichnis* eines Browsers zum Beispiel? 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.
 Datenträger 60	Löschen von Altlasten 62 Hier können Sie den vermeintlich freien Bereich (Freispeicher 44) Ihrer Festplatten säubern, s.g. Clustertips 44 und Dateinamen 46 bereinigen. SSD Funktionen 65 *Solid State Disks* 52 verwalten Daten auf besondere Weise. Sicheres Löschen ist auf einem Solid State Drive kompliziert. Mit den Funktionen TRIM 55 und RE-TRIM 55 unterstützt Shredder das verlässliche Überschreiben von Daten.

Hauptkategorien	Beschreibung
	Löschen von ganzen Festplatten 66 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. Nutzen Sie die spezielle Funktion des Shredders um solche Laufwerke komplett zu bereinigen. Boot CD - Löschen des Betriebssystems 68 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. Hartnäckige Dateien 71 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.
 Löschzonen 77	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. Löschzonen sind Orte auf Ihrem Rechner, an denen der Shredder genau diese unsicheren Löschoperationen abfängt und Daten

Hauptkategorien	Beschreibung
	sicher löscht. Lassen Sie sich vom Shredder Löschzonen vorschlagen oder definieren Sie eigene.
 Online-Spuren 87	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.
 Plug-Ins 96	Das Betriebssystem und viele Anwendungen sammeln ohne Unterlass Informationen und speichern diese ab. Gegen diese Sammelwut ziehen Sie ab sofort mit zahlreichen Plug-Ins zu Felde. Mit Hilfe des optional erhältlichen Plug-In Editors können Sie die Palette der Plug-Ins beliebig erweitern. Die Vollversion bringt etwa 400 solche Plug-Ins mit. Der Shredder zeigt nur die Plug-Ins an, die sich auf Programme und Einstellungen Ihres Rechners auswirken und blendet unpassende automatisch aus.
 Systemfehler 110	Im Laufe der Zeit schleichen sich auf einem Rechner immer mehr Fehler ein. Das Installieren und Entfernen von Programmen sorgt für ungültige Einträge in der lebenswichtigen Registrierdatenbank (*Registry*) von Windows. Ungültige Verweise auf Dateien, fehlerhafte

Hauptkategorien	Beschreibung
	und inkonsistente Werte und unnötige Reste machen den Computer träge und instabil. Lange Wartezeiten und Abstürze sind die Folge. Unterteilt in Analysefunktionen für Anfänger, Fortgeschrittene und Experten, spürt ArchiCrypt Shredder solche Fehler auf und korrigiert sie.
 Duplikat Finder 124	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. Im Falle eines Falles, können Sie versehentlich entfernte Dubletten aus der Quarantäne wieder herstellen.
 Laufwerksbelegung 131	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.
 Versteckte Daten 138	ADS steht für Alternate Data Stream. Eine Möglichkeit, Daten unsichtbar an andere Dateien anzuhängen. Virenscanner nutzen diese Möglichkeit oft, um sich zu merken, wann eine Datei zuletzt überprüft wurde. Leider verwendet auch Schadsoftware diese verborgenen Bereiche. Viren hängen einfach

Hauptkategorien	Beschreibung
	unsichtbar schädliche Daten an andere, völlig harmlose Dateien an. ArchiCrypt Shredder spürt solche Dateien auf, gewährt Einblick in die Inhalte und kann potentiell schädliche Inhalte natürlich entfernen.
Aufgaben-Planer 145	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.
Mobile Nutzung 160	Mit Hilfe der PC-Version des Shredders können Sie sich eine spezielle portable Shredder Version auf einem USB-Stick oder einer externen Festplatte erzeugen lassen. Ihnen stehen so auch unterwegs die wesentlichen Funktionen des Shredders an jedem Rechner zur Verfügung.
Kontextmenü 165	ArchiCrypt Shredder bietet Ihnen systemweit 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[41] können Sie die einzelnen Kategorien aufrufen.

8.2 Allgemeine Bedienung

Die Bedienoberfläche

Die Home Seite

Die Home Seite wird bei jedem Start von ArchiCrypt Shredder automatisch angezeigt.

Home Ansicht ArchiCrypt Shredder

Unterhalb der Registerkarten[45], finden Sie das Suchfeld[44].

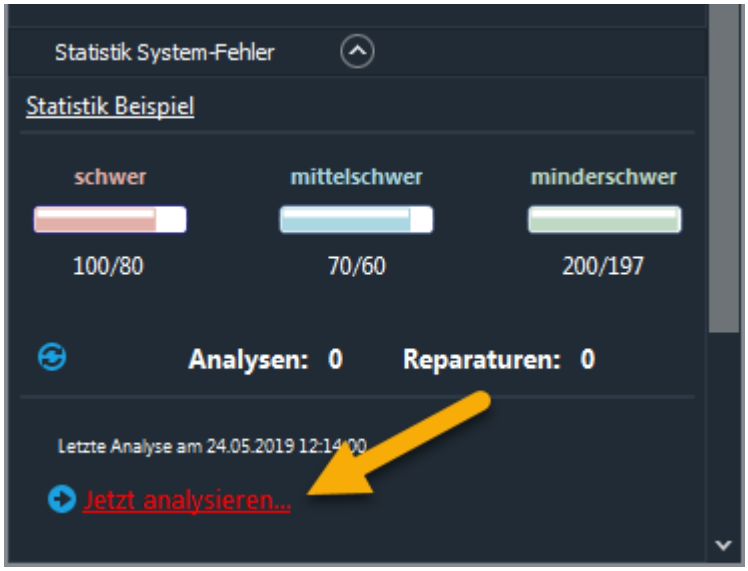
LINKE Seite Home-Ansicht:

Unterhalb der Statusanzeige[44] mit Aktivitätsradar befinden sich die Abschnitte Platzschaffer[49], Statistik System-Fehler[42] und das Info Center[42].

RECHTE Seite Home-Ansicht:

Home Menü[43] *mit allen Kategorien und Werkzeugen des Shredders*

Statistik System-Fehler



Systemfehler Statistik

Die Balken zeigen an, welche Fehler bisher entdeckt und repariert wurden. Über den Link Jetzt analysieren können Sie direkt zur Systemfehler-Analyse[110] springen.

Mit einem Klick auf die Reset-Schaltfläche können Sie die Statistik zurücksetzen. Es wird dann eine Beispielstatistik erzeugt und so lange angezeigt, bis reale Daten anfallen.

Info Center

Im Info-Center können Sie sich den Über-Dialog anzeigen lassen, in dem Sie Informationen zur genauen Version (Versionsnummer) einsehen können, den Einrichtungsassistenten starten können oder

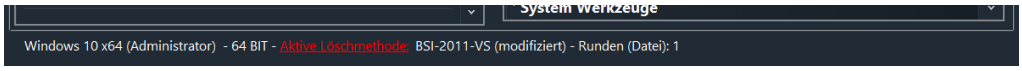
per Link auf die Internetseite von ArchiCrypt kommen.

Home Menü

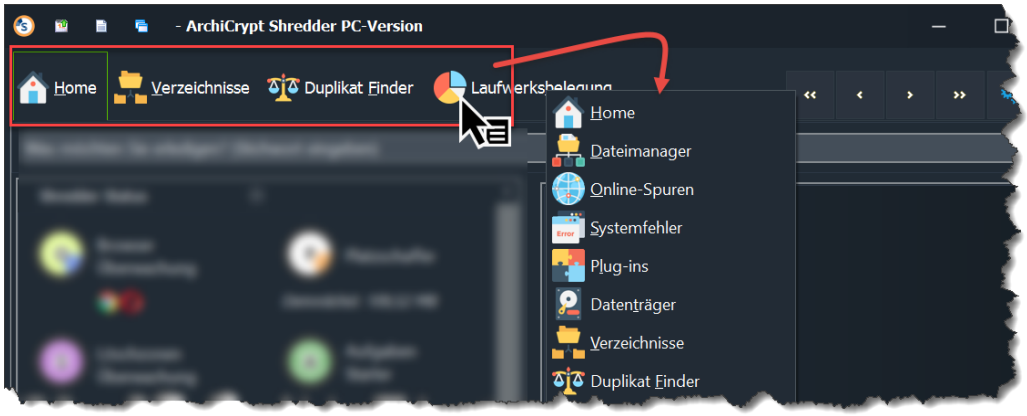
Im Home Menü werden alle Funktionen und Werkzeuge des Shredders in einer Liste angezeigt. Die Elemente können Sie per Drag&Drop gemäß eigenen Wünschen anordnen.

Statusleiste

Die Statusleiste am unteren Rand zeigt Ihnen an, auf welchem *Betriebssystem* mit welchen Rechten ArchiCrypt Shredder aktuell ausgeführt wird. Zudem haben Sie Zugriff auf die aktive Löschmethode[182] . Ein Klick auf den *Link Aktive Löschmethode* bringt Sie zu den Einstellungen für die Löschverfahren[182].

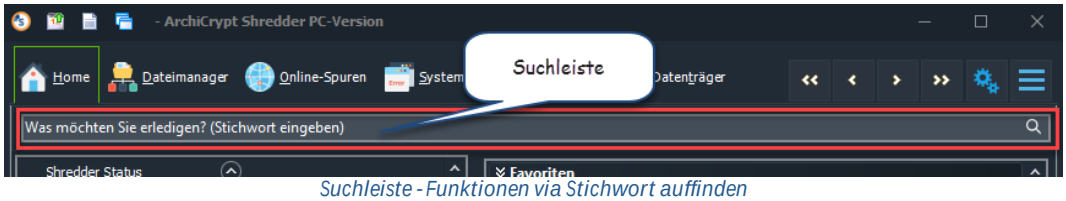


Die einzelnen Kategorien[48] können Sie in der oberen Leiste des Fensters über Registerkarten[45] auswählen. Die entsprechende Funktion wird durch Klick auf die Registerkarte aufgerufen. Sie können auch über jeder Registerseite die rechte Maustaste betätigen, um das Direktmenü[46] aufzurufen. Wenn Sie ein Stichwort in das Suchfeld[44] eingeben (*Was möchten Sie erledigen?*) zeigt ein grüner Balken unter dem Eingabefeld an, dass eine passende Funktion gefunden wurde. Die Funktion wird in der Übersicht markiert, diese kann durch Betätigen durch Eingabetaste oder mittels Linksklick aufgerufen werden.



Wechsel zwischen den Kategorien

Suchfeld



Suchleiste - Funktionen via Stichwort auffinden

Geben Sie in das Suchfeld Begriffe ein wie "Browser, Browserspuren, Festplatte, Duplikate, Dubletten, Support, Datenträger, Fehler, Problem, Backup ..." ein. Kennt ArchiCrypt Shredder eine Funktion, zu der der Begriff passt, wird dies durch eine grüne Linie unterhalb des Eingabefeldes angezeigt, der passende Eintrag wird im Home-Menü[43] markiert. Es kann durchaus mehrere passende Funktionen geben. Um zu den verschiedenen passenden Funktionen zu navigieren, können Sie die Pfeiltasten auf der Tastatur verwenden. Durch das Betätigen der Eingabetaste können Sie die *Funktion sofort aufrufen*.


oder


Shredder Status

Status Anzeige in ArchiCrypt Shredder

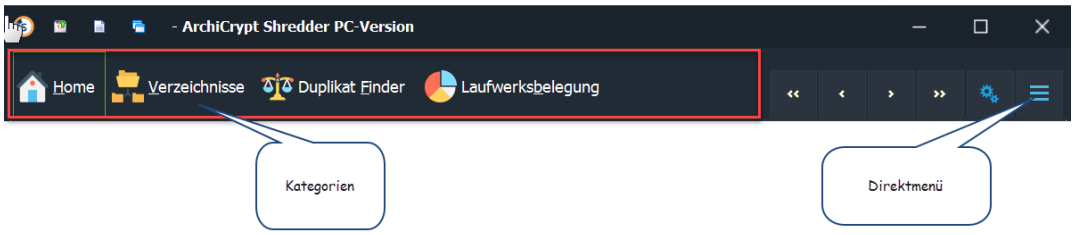
Im Status-Bereich sehen Sie stets, welche *Module* aktiv sind.

Aktiv: Radar-Anzeige oder Segment, falls nicht animiert
Inaktiv: Ausgefüllter Kreis

O ist für die Online-Überwachung[87] (*Browser*) verantwortlich, P zeigt den Status des Platzschaffers[49], S zeigt den Status der Sicheren Löschzonen[72] und A den Status des Aufgabenstarters[156].

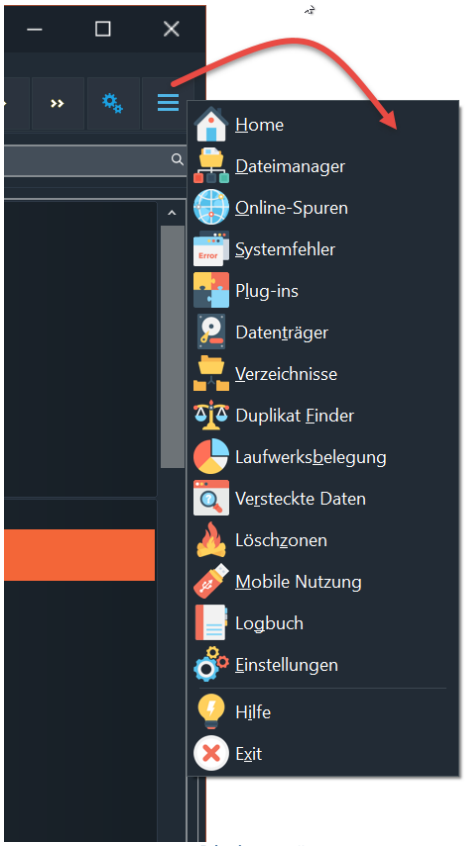
Per Linksklick auf eines der Symbole können Sie die entsprechende Funktion aktivieren bzw. deaktivieren. Per Rechtsklick gelangen Sie zu den spezifischen Einstellungen.

Zugriff auf Funkionen über Registerseiten



Die Registerseiten haben ebenfalls einen dünnen farblichen Rand. Grün steht für Anfängerfunktion, Gelb für Fortgeschrittene und Rot für Profis.

Das Direktmenü können Sie per Rechtsklick über jeder Registerseite aufrufen und damit navigieren.

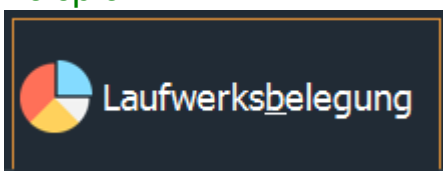


Direktmenü

Zugriff auf Funktionen über Tastaturkürzel

Falls Sie die Bezeichnungen in den Registern anzeigen lassen (*Allgemeines-Kategorie-Bezeichnung anzeigen* 177) , dann können Sie auch durch Betätigen der ALT-Taste zusammen mit dem unterstrichenen Buchstaben zur entsprechenden Kategorie springen.

Beispiel:



Betätigen von ALT + B ruft die Kategorie Systemfehler auf.

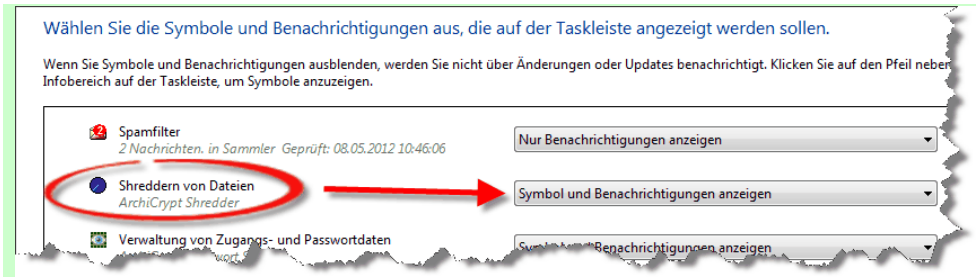
Shredder minimieren und beenden

In der Titelleiste können Sie ArchiCrypt Shredder minimieren. Dies empfiehlt sich insbesondere dann, wenn ArchiCrypt Shredder lang andauernde Aufgaben ausführt oder im Hintergrund auf das Beenden eines Browsers wartet. Beim Minimieren wird ArchiCrypt in den Infobereich verkleinert. Per Doppelklick auf das Symbol im Systemtray holen Sie den Shredder wieder in den Vordergrund.

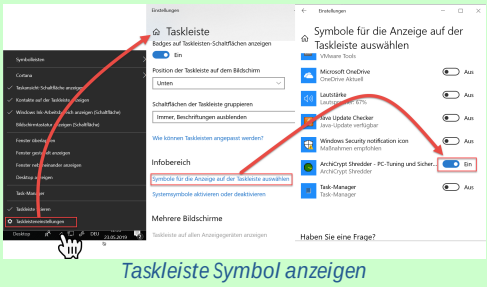
TIPP: Symbol in der Taskleiste

TIPP: Windows blendet die Symbole im Infobereich nach einer Weile aus. Um das Symbol des Shredders sichtbar zu halten, gehen Sie wie folgt vor:
Klicken Sie auf den kleinen Pfeil im Infobereich (Ausgeblendete Symbole einblenden). Klicken Sie dann auf Anpassen... bzw. auf Taskleisteneinstellungen.

Unter Windows 7/8 suchen Sie jetzt den Eintrag zu ArchiCrypt Shredder in der Tabelle und wählen "*Symbol und Benachrichtigung anzeigen*".



Unter Windows 10 sieht der Fluss wie folgt aus:

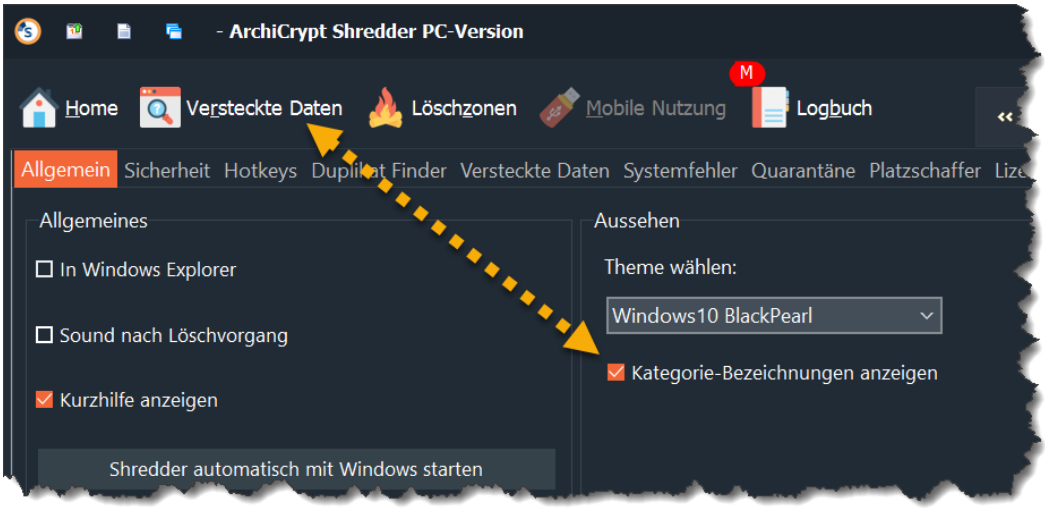


Taskleiste Symbol anzeigen

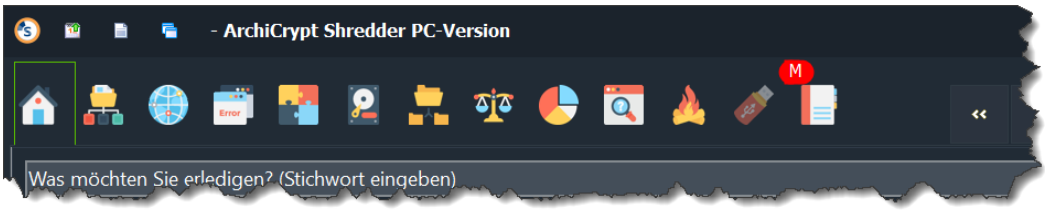
Durch einen Klick auf Beenden werden alle laufenden Aktivitäten des Shredders abgebrochen, bevor die Anwendung selbst beendet wird.

Kategorien und Funktionen

Sie können die Bezeichner auf den Registerkarten[45] in den Einstellungen[177] (*Allgemeines-Kategorie-Bezeichnung anzeigen*) dauerhaft ein- und ausblenden. Wenn Sie die Maus über eine Seite bewegen, wird eine Kurzhilfe angezeigt. Sie können bei eingeblendeter Beschriftung auch mittels Tastaturkürzel[46] zu den Kategorien wechseln.



Registerkarten mit Beschriftung



Registerkarten ohne Beschriftung

Hilfe

Sie können die ausführliche Hilfe Kontext-sensitiv über die F1 Taste aufrufen.

8.3 Platzschaffer

Bereinigung im laufenden Betrieb mit dem Platzschaffer

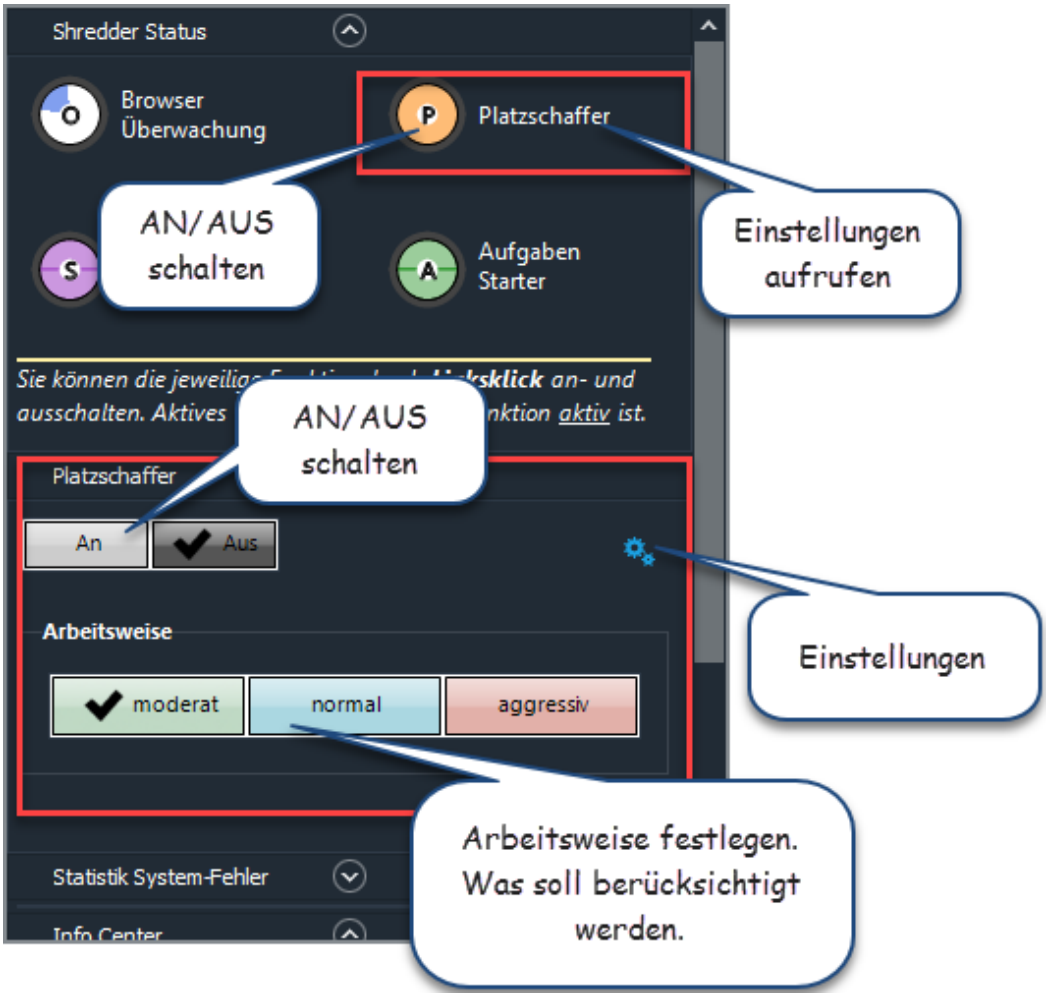
Der Platzschaffer untersucht im Hintergrund Ihren Rechner. Dabei wird an einschlägig bekannten Stellen im System geprüft ob nicht mehr benötigte Daten vorhanden sind. Diese Daten werden dann im laufenden Betrieb in bestimmten Zeitabständen[204] bereinigt.

TIPP: Manche Installationsroutinen müssen Dateien ersetzen, die während des Betriebs durch das System oder andere Anwendungen blockiert sind. In diesem Fall legt das Installationsprogramm (*es kann sich auch um im Hintergrund ablaufende Updates von Windows oder anderen Programmen handeln*) Dateien in temporären Ordnern ab, um

die Ersetzung beim Neustart des Systems durchzuführen. Wurden einfach alle temporären Dateien löscht, kann es mitunter zu Problemen und verwirrenden Fehlermeldungen kommen.

Wenn Sie den Platzschaffer so einrichten, dass Daten erst nach 2 Tagen gelöscht werden, haben Sie stets ein frisches und aufgeräumtes Windows.

Der Platzschaffer kann auf der Home-Seite[41] *gestartet* und *gestoppt* werden. Dazu genügt ein Linksklick auf das Aktivitätssymbol oder das An- oder Ausschalten mittels Schalter.



Platzschaffer über die Home Seite bedienen

Sie können den Platzschaffer[49] direkt auf der Home-Seite[41] bedienen und wesentliche Einstellungen (Arbeitsweise: *moderat, normal, aggressiv*) vornehmen.

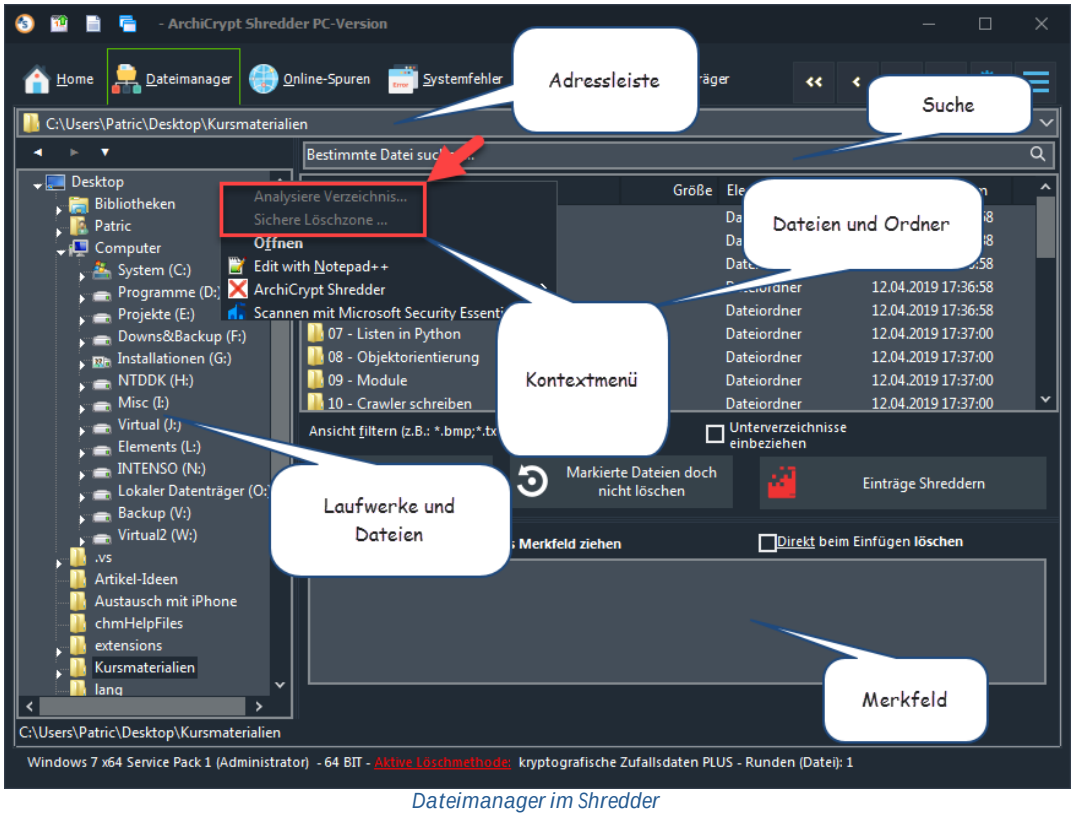
Der Schalter An/Aus *startet* und *stoppt* den Platzschaffer, die *Arbeitsweise* kann ebenfalls ausgewählt werden. In den Einstellungen für den Platzschaffer[204] kann man festlegen und prüfen, welche Verzeichnisse/Plug-ins bei den verschiedenen Arbeitsweisen berücksichtigt werden sollen. Und zu Beispiel festlegen, wie alt Dateien sein müssen, bevor sie gelöscht werden.

8.4 Dateimanager

Der ArchCrypt Shredder Dateimanager will *kein Ersatz für den Windows Explorer* sein. Die Stärke liegt, wie soll es anders sein, in der Fähigkeit, Daten sicher zu löschen und mit verschiedenen anderen Modulen des Shredders (zum Beispiel Laufwerksbelegung[131]) zusammenzuarbeiten.

TIPP: Das sichere Löschen können Sie ebenso über das von ArchiCrypt Shredder im Windows Explorer angebotene Kontextmenü[165] ausführen.

Ziehen Sie Dateien, die sicher gelöscht werden sollen, einfach per Drag & Drop auf das Merkfeld.

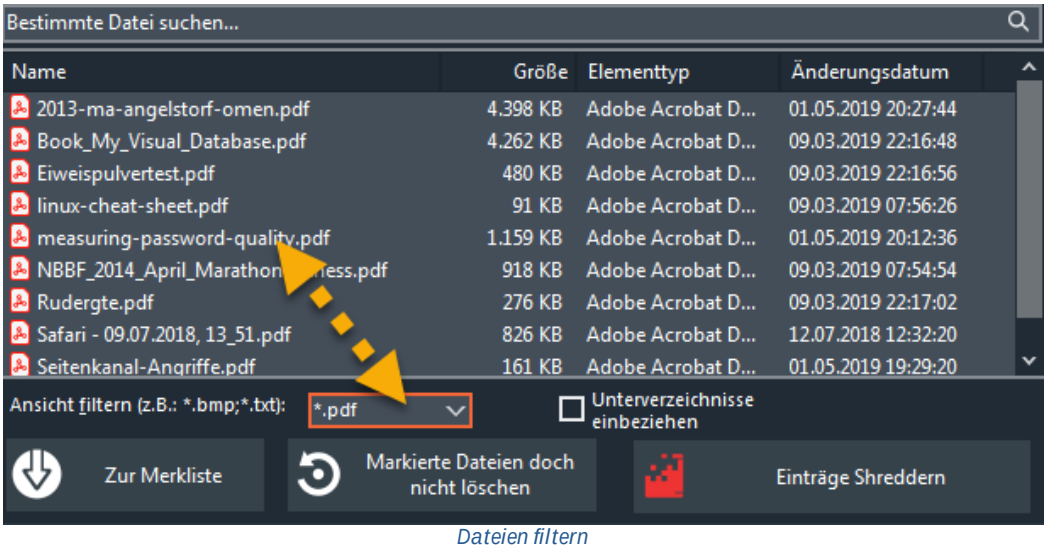


Dateimanager im Shredder

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 **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 gewünschten Dateitypen als Filter ein.



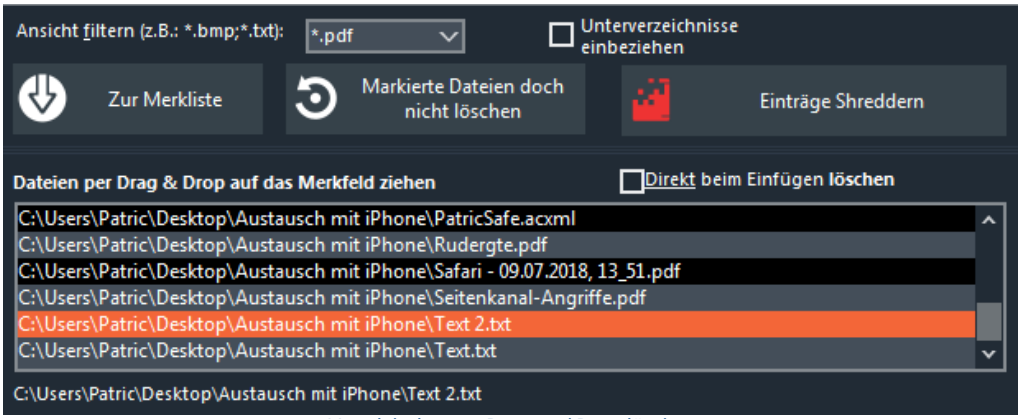
Dateien filtern

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 Excel-Dokumente in die Merkliste übertragen. Geben Sie dazu als Filter *.doc;*.xls ein.
2. Sie möchten alle Microsoft Word-Dokumente in die Merkliste übertragen, 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 (**unabhängig vom eingestellten Filter**), also auch alle Dateien in eventuell vorhandenen Unterverzeichnissen.



Verzeichnisse per Drag and Drop löschen

Sind im Merkfeld Dateien enthalten, welche Sie nicht löschen möchten, markieren Sie diese mit der linken Maustaste und Betätigen die Schaltfläche "Markierte Dateien doch nicht löschen" oder Betätigen Sie die Entf-Taste. 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 gelistet sind, halten Sie die <STRG> Taste während des Auswahlvorganges gedrückt.

TIPP: Wenn Sie *alle Dateien* die aktuell im Merkfeld aufgelistet sind, nicht löschen möchten, dann markieren Sie das oberste Element in der Liste. Betätigen Sie dann die Tastenkombination <STRG>+<Shift> + Ende. Alle Einträge werden jetzt markiert und können per Klick auf Markierte Dateien Auswahl doch nicht löschen entfernt werden.

Sofern Sie nicht die Option **Direkt löschen** aktiviert haben, findet das eigentliche Löschen erst statt, wenn Sie die Schaltfläche Einträge Shreddern betätigen.

Die Art und Weise des Löschvorganges legen Sie mit den Einstellungen "Sicherheit[182] " 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.

siehe auch: Explorer Kontextmenü und Systemtray-Menü 165

8.5 Löschen von Verzeichnissen

Verzeichnisse sicher löschen

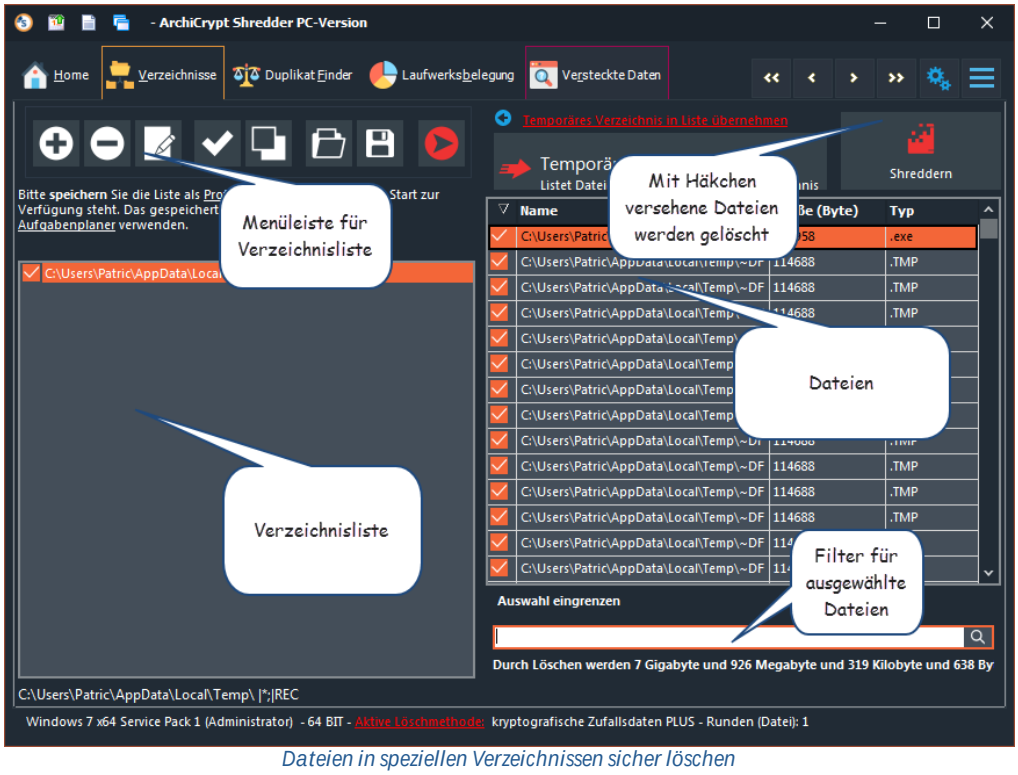
Die spezielle Funktion zum löschen von Verzeichnissen ist insbesondere dann nützlich, wenn man wiederkehrend *Dateien in bestimmten Verzeichnissen löschen* möchte.

Festgelegte Verzeichnisse können sogar zeitgesteuert 142 oder automatisch beim Beenden des Browsers 94 bereinigen lassen. Speichern Sie die Einstellungen als Profil ab und Sie können sich im Aufgabenplaner 142 s.g. 1-Klick Aufgaben 145 erstellen.

Mit der Schaltfläche

- **Temporäre Dateien**

können Sie die Dateien auflisten lassen, die Ihr System vermutlich am stärksten belasten und mit deren Entfernung Sie am meisten Platz zurückgewinnen. Besser ist es jedoch, für die Beseitigung temporärer Dateien den Platzschaffer 49 zu verwenden.



Dateien in speziellen Verzeichnissen sicher löschen

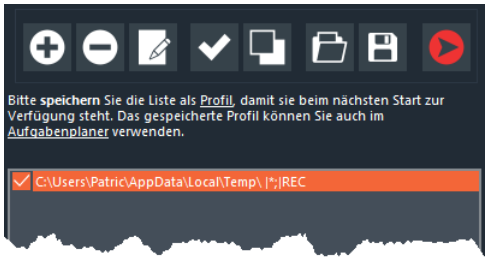
WICHTIGER HINWEIS: Erst, wenn Sie die Funktion Shreddern aufrufen, werden alle mit Häkchen versehenen Einträge in der Tabelle mit der in den Einstellungen 182 festgelegten Methode gelöscht. Vorher werden lediglich die Dateien ermittelt, die für das Löschen in Frage kommen.

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



Menü für 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 Excel-Dokumente löschen. Geben Sie dazu als Filter **.doc;*.xls* ein.

Sie möchten alle Microsoft Word-Dokumente 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 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.

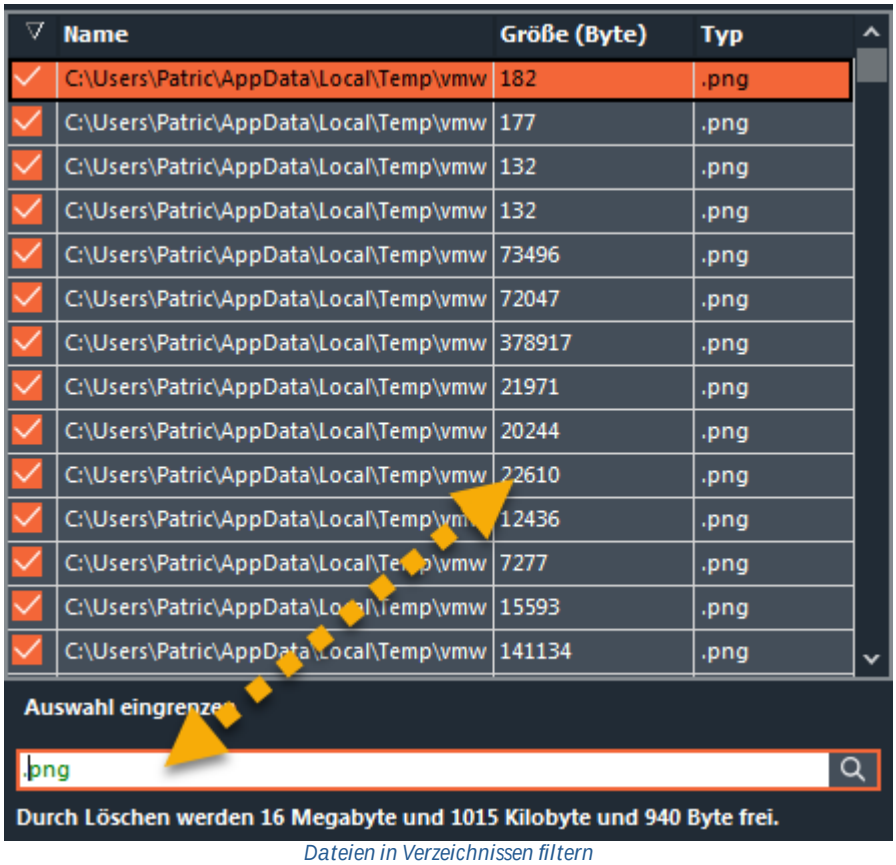
Die Dateien werden bei dieser Aktion noch nicht gelöscht, sondern nur aufgelistet.

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.** Setzen Sie jetzt bei Online-Spuren ein Häkchen bei Spezielle Verzeichnisse bereinigen 94.

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. Nur die Dateien werden mit einem Häkchen versehen, die den eingegebenen Begriff enthalten. Wenn Sie jetzt die Funktion Shreddern aufrufen, werden nur die aktuell in der Tabelle sichtbaren Dateien gelöscht.

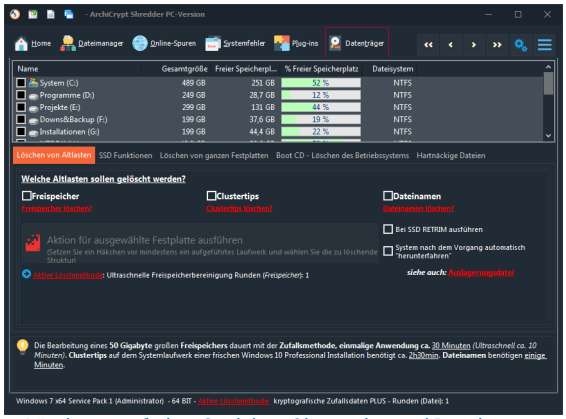


Dateien in Verzeichnissen filtern

8.6 Speichermedien

Speichermedien sicher löschen

In der Rubrik Datenträger finden Sie Funktionen, die ganze Laufwerke und Partitionen sicher bereinigen können.
Aber auch dann, wenn Altlasten (*Dateien die bereits mit unsicheren Verfahren des Betriebssystems gelöscht wurden*) beseitigt werden sollen, finden Sie hier die richtigen Funktionen.



Löschen von freiem Speicher, Clustertips und Dateinamen

Altlasten[62]

Wenn Sie Spuren von Dateien entfernen möchten, die Sie bereits mit unsicheren Mitteln des Betriebssystems "gelöscht" haben, dann finden Sie hier die entsprechenden Funktionen. Hier können Sie den vermeintlich freien Bereich Ihrer Festplatten (Freispeicher[44]) säubern, s.g. Clustertips[44] und Dateinamen[46] bereinigen.

SSD Funktionen[65]

Eine *SSD* (*Solid State Disk*) speichert Daten grundsätzlich anders als ein klassisches, magnetisierbares Speichermedium. In den Einstellungen[183] können Sie das grundsätzliche Verhalten des Shredders beim Löschen von einer SSD festlegen. Zudem bietet der Shredder einige *besondere Funktionen für ein Solid State Drive*[65].

Löschen von ganzen Festplatten[66]

Steht der Verkauf eines Rechners oder eines Datenträgers an, ist man gut beraten, die komplette Festplatte sicher zu überschreiben. Dabei ist es ein weit verbreiteter Irrglaube, man könne durch einfaches Formatieren die Daten eines Laufwerks vernichten. Nutzen Sie die spezielle Funktion des Shredders um solche Laufwerke komplett zu bereinigen.

Boot CD - Löschen des Betriebssystems[68]

Die Partition auf dem Ihr Betriebssystem gespeichert ist, können Sie nicht komplett sicher löschen. Schließlich benötigt ArchiCrypt Shredder das Betriebssystem, um zu arbeiten. 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.

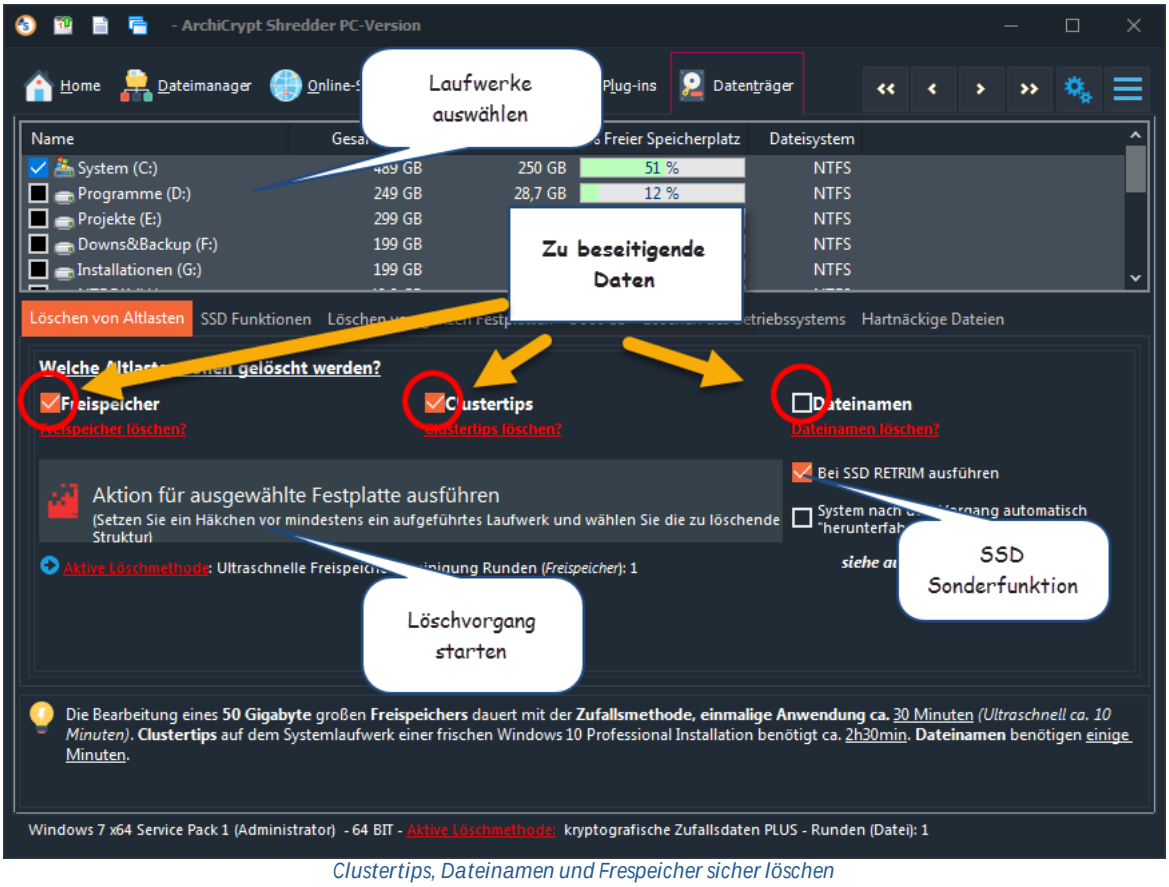
Blockierte Dateien[71]
Einige Dateien sind derart hartnäckig, dass sie im laufenden Betrieb nicht gelöscht werden können. Der Shredder merkt sich solche Dateien und löscht sie beim nächsten Start Ihres Rechners.

8.6.1 Altlasten (Clustertips, Freispeicher und Dateinamen)

Altlasten

Mit Altlasten werden die Daten bezeichnet, die zu mit Betriebssystemmitteln "gelöschten" Dateien gehören.

Hier können Sie den vermeintlich freien Bereich (Freispeicher[44]) Ihrer Festplatten säubern, s.g. Clustertips[44] und Dateinamen[46] bereinigen.



Clustertips, Dateinamen und Frespeicher sicher löschen

So beseitigen Sie Altlasten

Wählen Sie zunächst das oder die Laufwerke aus, indem Sie ein Häkchen vor den Laufwerksbuchstaben setzen.

Wählen Sie jetzt aus, welche Altlasten ArchiCrypt Shredder beseitigen soll, indem Sie die Funktion aktivieren.

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 unsichtbar 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.

Bei SSD RETRIM ausführen

Führt nach dem Löschen der Daten das RETRIM Kommando[55] aus.

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

Erst dann, wenn Sie mindestens ein Laufwerk mit Häkchen versehen und eine "Altlast" ausgewählt ist, können Sie die Schaltfläche "Aktion für ausgewählte Festplatte ausführen" betätigen!

TIPP: Die Funktion *Freispeicher* und *Clustertips bereinigen* können bei Standarddatenträgern heutiger Größenordnung (1 bis 4 Terabyte und mehr), *sehr viel Zeit* in Anspruch nehmen (*24 Stunden und mehr*). Wenn Sie die *BSI Funktion mit Verifikation der Schreibvorgänge* wählen, dauert es extrem lange. 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[182] wirken sich maßgeblich auf die Dauer des Vorganges aus. Manche Löschverfahren erlauben nur eine Rundenzahl von 1. Die dem

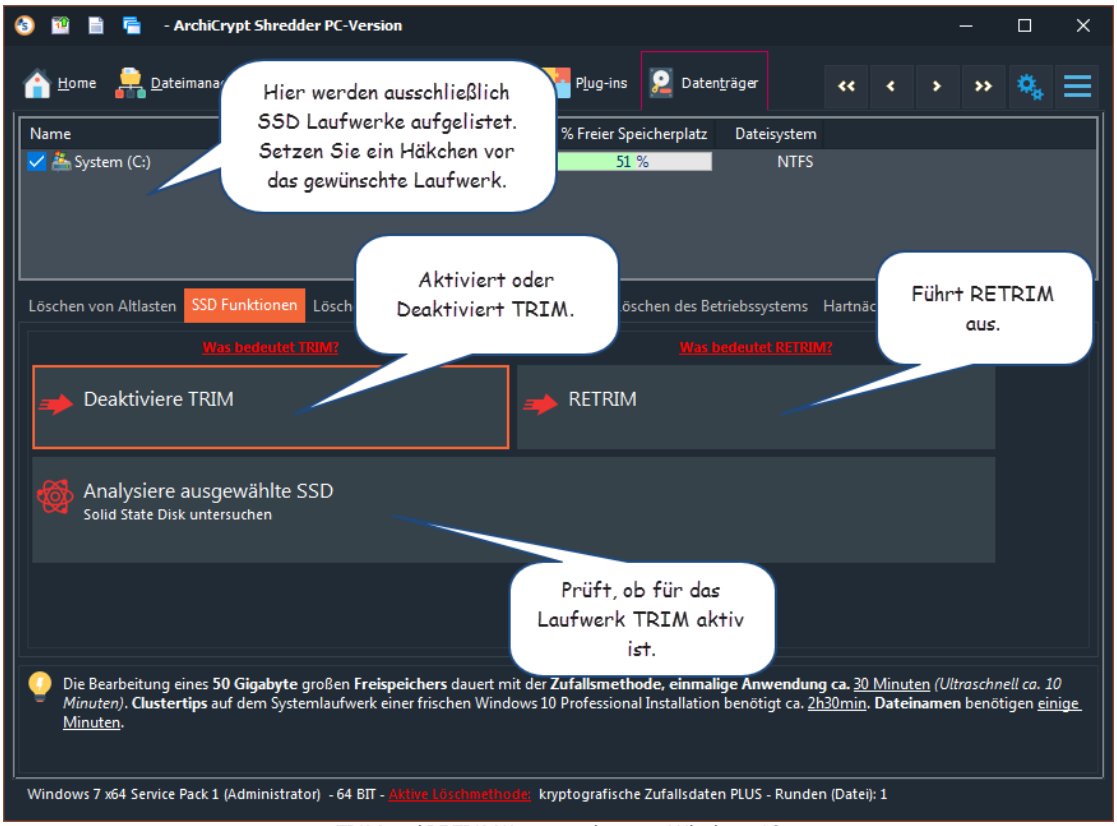
Löschverfahren zugrundelegende Anzahl an Durchläufen bleibt generell unangetastet.

Weiter zu SSD Funktionen[65]

8.6.2 SSD Funktionen

Lesen Sie sich bitte die Hinweise zu Solid State Disk - SSD[52] durch, um etwas über die *Besonderheiten von Solid State Disks* zu erfahren.

SSD Funktionen



TRIM und RETRIM Kommando unter Windows 10

ArchiCrypt Shredder listet hier ausschließlich *erkannte SSD Laufwerke* auf. Setzen Sie bei den zu berücksichtigenden SSD Laufwerke ein Häkchen. Anschließend sollten Sie zunächst die SSD analysieren. Die *Analyse der SSD* zeigt, ob für die *Solid State Disk* TRIM[55] aktiv ist. Je nach Status haben Sie die Möglichkeit, TRIM zu *aktivieren* (**Aktiviere TRIM**) oder TRIM zu *deaktivieren* (**Deaktiviere TRIM**). Mit RETRIM[55]

sorgen Sie dafür, dass sichergestellt ist, dass das System auch wirklich das TRIM Kommando ausführt.

Gibt es einen Grund, TRIM zu deaktivieren?

Sofern das System alle Voraussetzungen für TRIM erfüllt (*dies kann man auf der Herstellerseite der SSD in Erfahrung bringen*), sollte TRIM bereits aktiv sein! Es gibt keinen Grund, ein bereits aktiviertes TRIM, zu deaktivieren. Es bringt im Gegenteil nur Nachteile, TRIM nicht zu aktivieren. So wird die SSD zum Beispiel, wie oben erläutert, mit der Zeit immer langsamer und Daten lassen sich nahezu nicht verlässlich löschen.

Weiter zu Löschen von ganzen Festplatten 66

8.6.3 Löschen von ganzen Festplatten

Löschen einer kompletten Festplatte bzw. Partition

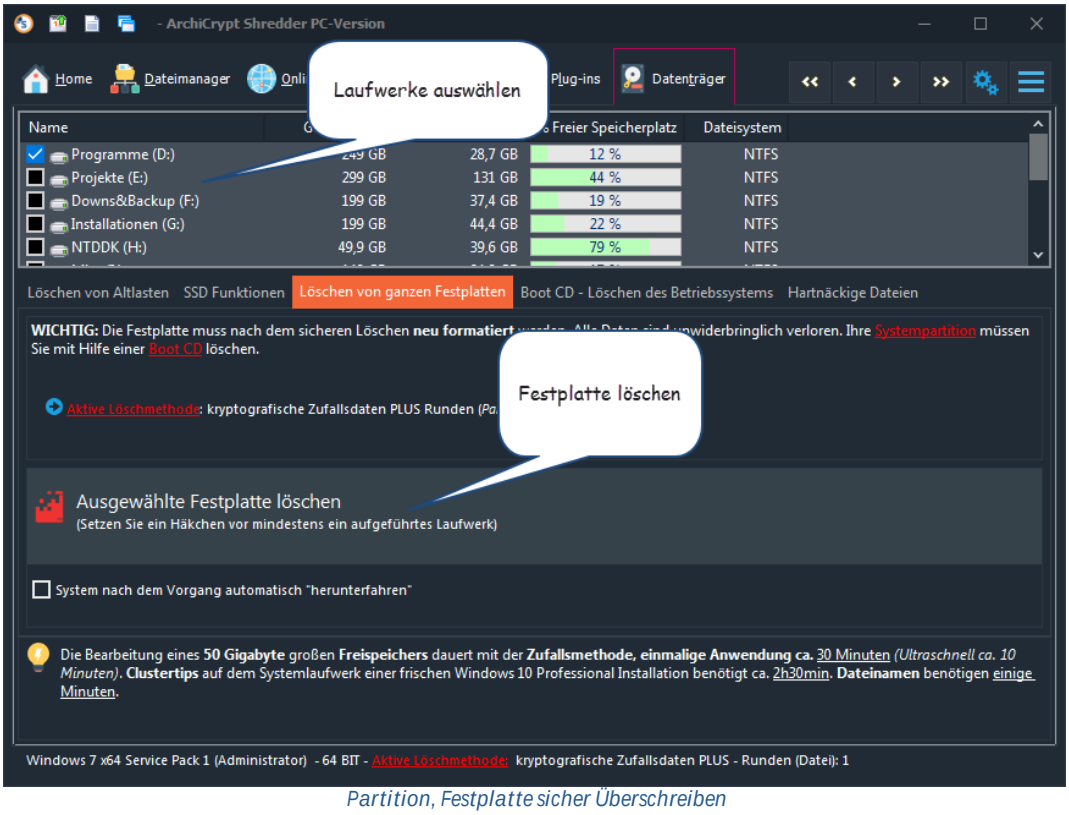
(nicht Betriebssystempartition 68)

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. Beim einfachen Formatieren werden nur die *Strukturen* gelöscht, in denen vermerkt ist, an welcher Stelle der Inhalt einer Datei abgelegt ist. Die Inhalte selbst bleiben erhalten und können mit Spezialsoftware wieder sichtbar gemacht werden.

Nutzen Sie die spezielle Funktion des Shredders, um Laufwerke, auf denen Sie s.g. *Arbeitsdaten* (Datenpartitionen 46) abgelegt haben, komplett zu bereinigen.

Falls Sie das Laufwerk sicher löschen möchten, welches das Betriebssystem enthält, sollten Sie sich das Kapitel Boot CD & Löschen des Betriebssystems 68 ansehen.



Partition, Festplatte sicher Überschreiben

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, sofern Sie die Option "System nach dem Vorgang automatisch herunterfahren" nicht aktiviert haben.

Die Funktion Ausgewählte Festplatte löschen kann bei Standarddatenträgern heutiger Größenordnung (*1 - 4 Terabyte und mehr*), 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 Sicherheit182 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* von Windows (*Systemsteuerung-Computerverwaltung-Datenträgermanager*) zunächst einen Laufwerksbuchstaben zuordnen.

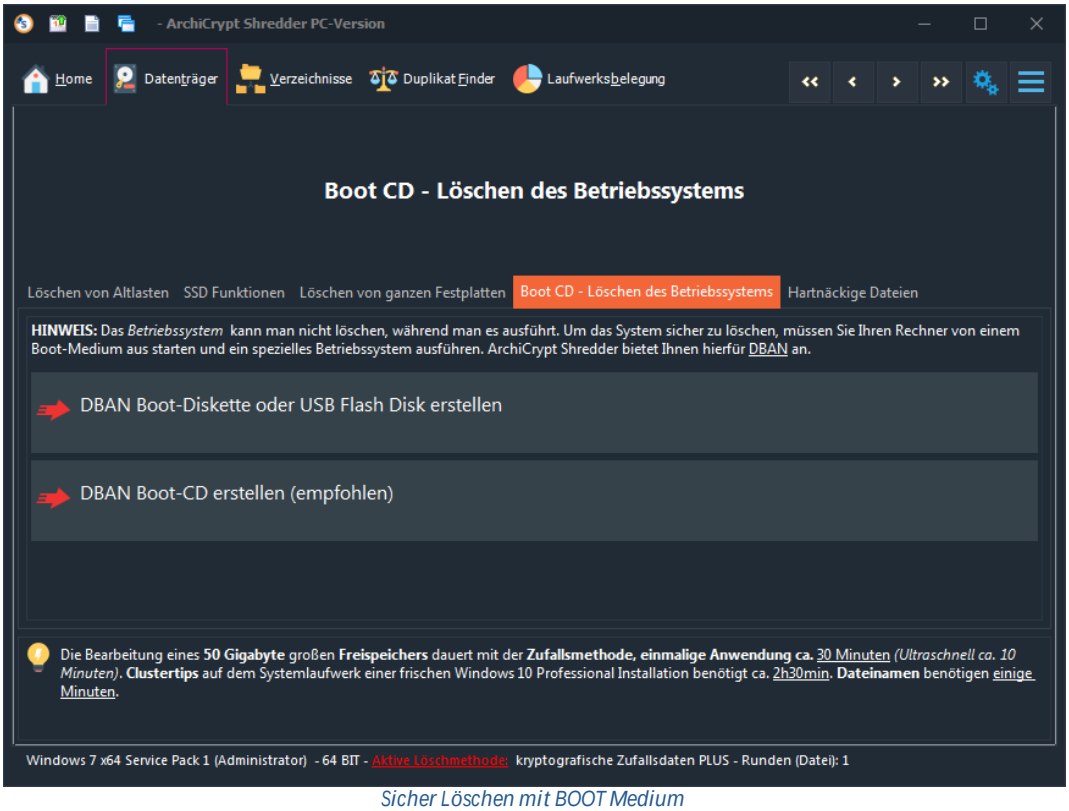
Weiter zu Boot CD & Löschen des Betriebssystems68

8.6.4 Löschen des Betriebssystems

Boot-Medium zum Löschen des Betriebssystems

Die *Partition* auf der Ihr Betriebssystem gespeichert ist, können Sie im laufenden Betrieb nicht komplett sicher Löschen.

Schließlich benötigt ArchiCrypt Shredder das Betriebssystem, um zu arbeiten. ArchiCrypt Shredder bringt daher DBAN mit und gestattet das Erstellen, eines bootfähigen Mediums. Mit diesem Boot-Medium können Sie dann auch die Systempartition sicher löschen.



Sicher Löschen mit BOOT Medium

Was ist DBAN?

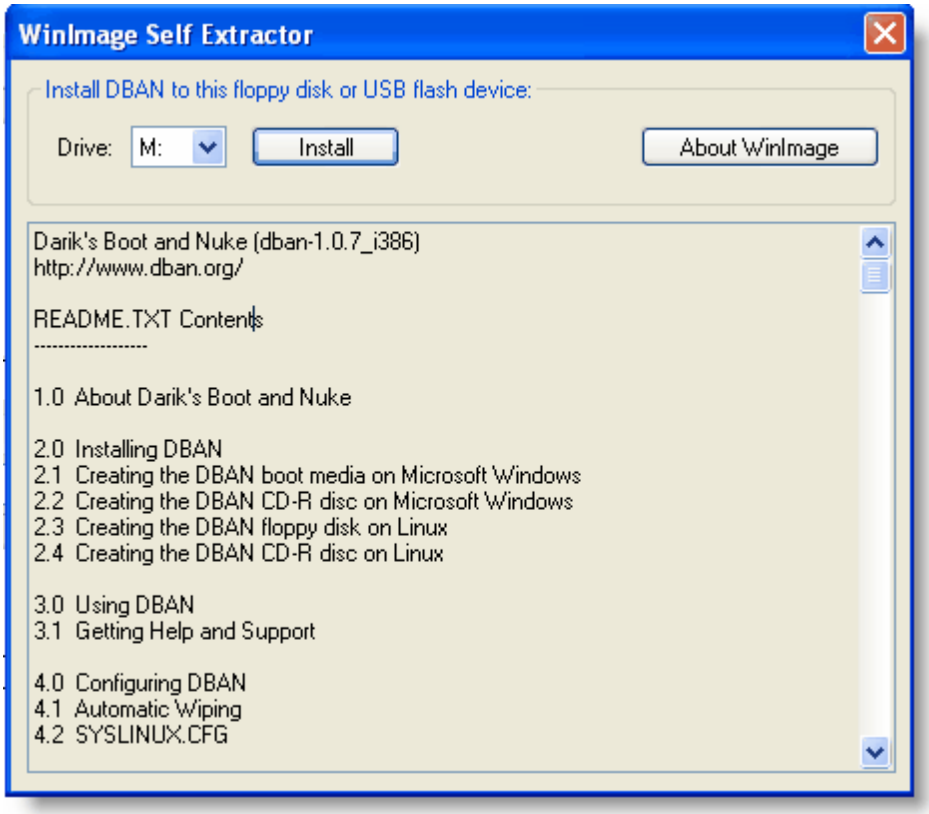
DBAN (*Darik's Darik's Boot and Nuke*) ist ein eigenständiges Tool, welches von Herrn Darik Horn entwickelt wurde. DBAN ist in der mitgelieferten Version kostenlos!

ArchiCrypt Shredder spielt hier lediglich die Rolle, aus dem Programm heraus 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! Auch Support für DBAN können wir nicht leisten.

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

So erstellen Sie ein Boot - Medium

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.

So erstellen Sie eine 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.

Weiter zu Blockierte Dateien 71

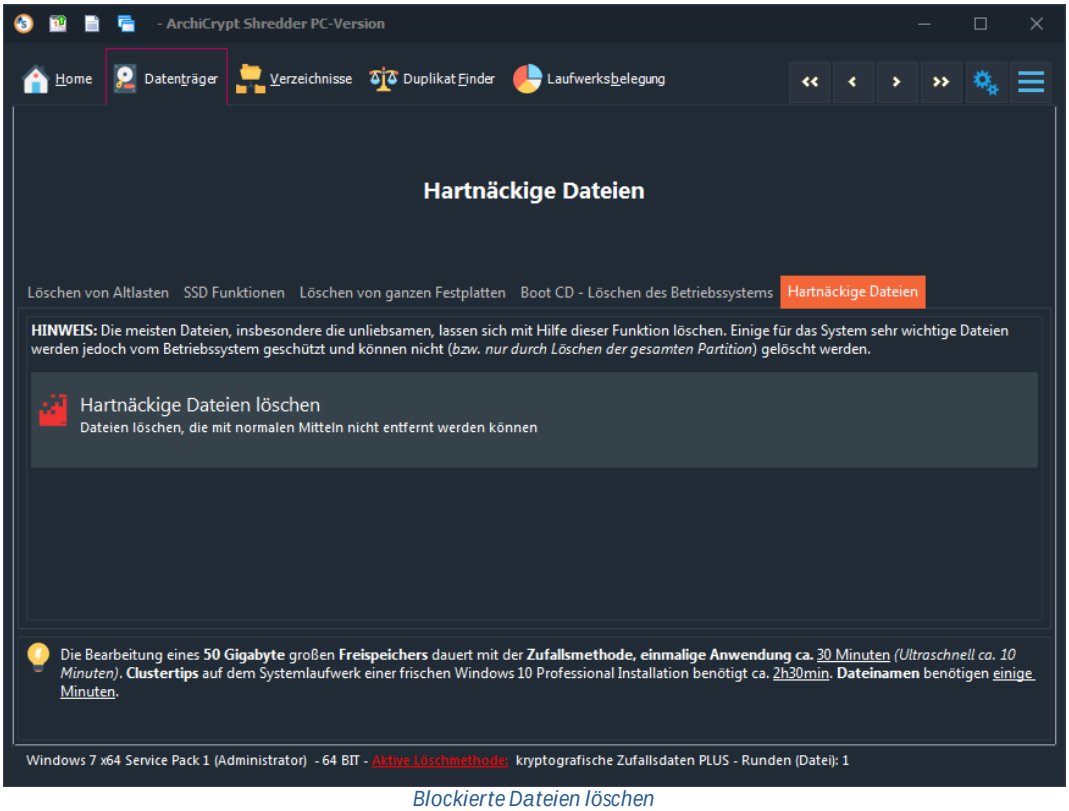
8.6.5 Blockierte Dateien

WARNUNG: Löschen Sie auf diese Weise ausschließlich Dateien, von denen Sie wissen, worum es sich handelt. Ansonsten löschen Sie unter Umständen Dateien, die für das ordnungsgemäße Funktionieren des Betriebssystems erforderlich sind.

Es gibt bestimmte Dateien auf Ihrem Rechner, die man nicht löschen kann, während das Betriebssystem geladen ist. Hier können spezielle Anwendungen oder das Windows System selbst den Zugriff auf eine Datei blockieren.

Mit dem Shredder können Sie auch *blockierte Dateien löschen*. ArchiCrypt Shredder merkt sich diese Dateien und nutzt einen kurzen Moment während des Systemstarts aus, um die ansonsten ***blockierten Dateien*** zu entfernen. Sie müssen also den *Rechner neu starten*, damit die Löschung erfolgt.

HINWEIS: Das Löschen dieser Dateien geschieht mit Systemmitteln, als auf nicht sichere Art. Sollte es sich wieder Erwarten um eine Datei mit potenziell sensiblem Inhalt handeln, dann müssen Sie nach dem Start des Systems den Freispeicher 62 bereinigen.



Blockierte 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 sich nicht normal löschen lässt. Die Dateien werden vorgemerkt und *beim nächsten* Rechnerstart gelöscht.

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

8.7 Sichere Löschzonen

Dateien automatisch sicher löschen mit Löschzonen

Siehe auch:
Überblick 74
Löschzonen 77
Löschzonenüberwachung 82

Was sind (sichere) Löschzonen?

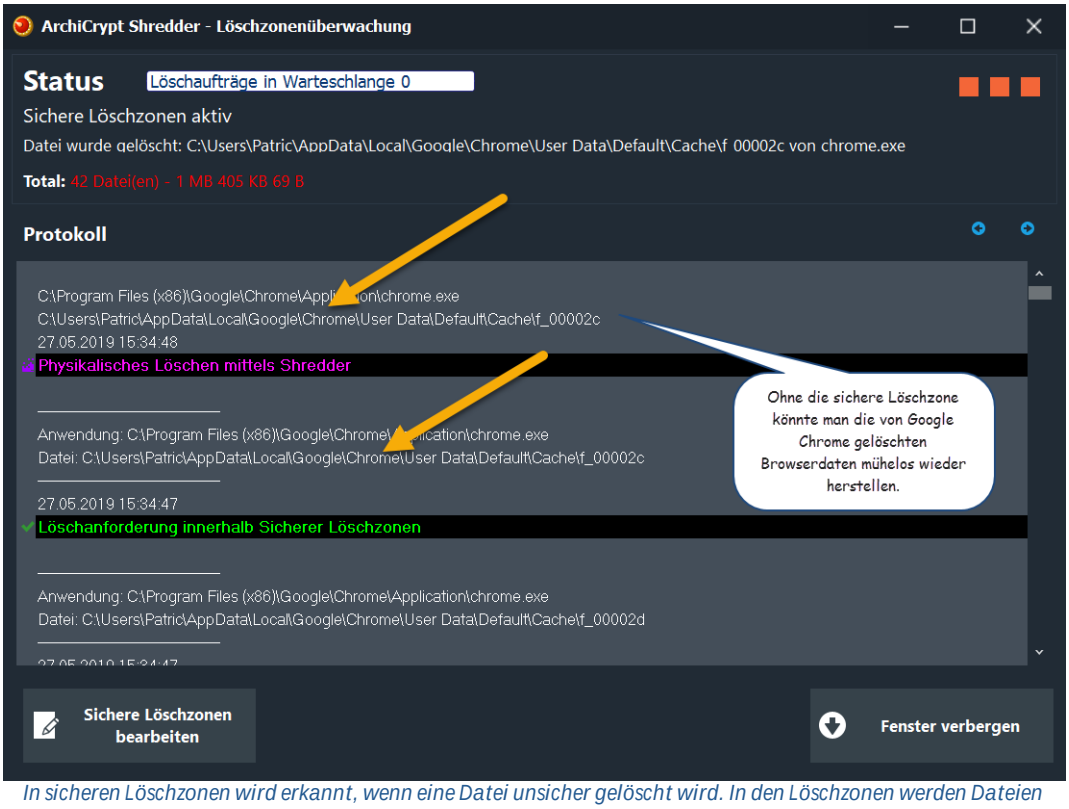
Löschzonen sind Verzeichnisse auf Ihrem Rechner, in denen der Shredder unsichere Löschoperationen abfängt und Daten sicher löscht.

Sie können Shredder zum Beispiel anweisen, dass das temporäre Verzeichnis als sichere Löschzone eingerichtet wird. Löscht eine Anwendung dort erstellte Dateien, greift Shredder ein und stellt sicher, dass Dateien automatisch sicher gelöscht werden. Lassen Sie sich vom Shredder Löschzonen vorschlagen78 oder definieren Sie *eigene Verzeichnisse und Dateifilter* als Sichere Löschzone.

WICHTIG: Dateien, die *Sie selbst* im *Windows Explorer* oder einem anderen *Dateimanager* löschen, werden nicht durch die sicheren Löschmethoden abgefangen. Um solche Dateien sicher zu löschen, müssen Sie das Explorer Kontextmenü165 verwenden.

Nahezu jede Anwendung, darunter natürlich auch *Browser*, *Office-*, *Grafik-* und *Multimediaanwendungen* erstellen und löschen ganz nebenbei unzählige Dateien. Diese Vorgänge finden im Verborgenen statt. Das Löschen erfolgt immer mit *unsicheren Betriebssystemmitteln*.

Die Daten könnten also **wieder hergestellt werden**. Das bedeutet zum Beispiel, dass man mit einem Datenrettungstool zumindest Teile besuchter Internetseiten wiederherstellen kann, auch wenn Sie den Verlauf des Browsers gelöscht haben. Oder man kann Dokumente oder Bilder wieder herstellen, die man in einem Office Programm oder einer Grafikanwendung bearbeitet hat!



In sicheren Löschzonen wird erkannt, wenn eine Datei unsicher gelöscht wird. In den Löschzonen werden Dateien vom Shredder sicher gelöscht.

Weiter zu Überblick über Sichere Löschzonen 74

8.7.1 Überblick über Sichere Löschzonen

Was sind Sichere Löschzonen?

Löschzonen (*auch* sichere Löschzonen *genannt*) sind Speicherorte (*Verzeichnisse ggf. mit Dateifiltern*), die von ArchiCrypt Shredder überwacht werden.

Wird eine Datei in einer Löschzone von einer Anwendung gelöscht, übernimmt ArchiCrypt Shredder automatisch die Kontrolle über den Löschvorgang und sorgt dafür, dass die Dateien mit sicheren Verfahren gelöscht werden.

Anm.: Unter Windows 10 muss es sich um Anwendungen handeln, die im Sicherheitskontext des Anwenders laufen. Also Office Programme, Browser, Mail-Clients, Spiele, Bildbearbeitung und Betrachter, Video-Bearbeiter und Abspieler etc.

Warum benötigt man Sichere Löschzonen?

Der wichtigste Grund für den Einsatz sicherer Löschzonen ergibt sich aus dem Verhalten vieler Anwendungen.

Den meisten Anwendern ist nicht bekannt, dass nahezu jedes Programm s.g. temporäre Dateien (*von Anwendungen für die aktuelle Sitzung zwischengespeicherte Informationen*) erstellt.

Viele Anwendungsprogramme erstellen Sicherungskopien der Arbeitsdatei. Gearbeitet wird dann mit dieser Kopie, um im Fehlerfall den Datenverlust so gering wie möglich zu halten. Wird die Anwendung beendet, löscht die Anwendung die Kopie mit Betriebssystemmitteln (*unsicher*). Oft verbleiben die Dateien aber auch einfach im temporären Ordner und sorgen zusätzlich für stetig sinkenden Speicherplatz.

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 ~$*.doc oder ~$*.docx 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 (*unsicher*) veraltete Dateien.

Besonders häufig tritt dieses Phänomen bei Programmen aus den Bereichen Office-Anwendungen, Multimedia, bei Bildbetrachtungs- und -bearbeitungswerkzeugen, E-Mail Clients, Tauschbörsen, Chatprogrammen und Packprogrammen auf.

Hier haben Sie im Normalfall keine Möglichkeit, den Löschvorgang zu beeinflussen.

Traditionelle Löschprogramme oder Spurenvernichter helfen hier nicht, da diese Tools keine unsicheren Löschaktionen abfangen können. Sie können im Höchstfall vorhandene Dateien sicher löschen, aber nicht die, die zuvor im Hintergrund mit unsicheren Betriebssystemmitteln gelöscht wurden.

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 ist zurzeit weltweit das einzige Programm, welches diese unsicheren Löschaktionen in den Löschzonen abfangen und durch sichere Methoden ersetzen kann.

ANMERKUNG: Es soll nicht verschwiegen werden, dass man diese Datenfragmente auch loswerden kann, indem man jedes Mal, 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 - Löschzonenüberwachung 82 (*einer Art Überwachung für Dateilöschoperationen*) können Sie sehen, welche Dateien gerade von welcher Anwendung gelöscht wurden. ArchiCrypt Shredder schaltet sich in allen Fällen dazwischen, in denen das Löschen in einer definierten Löschzone stattfindet.

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

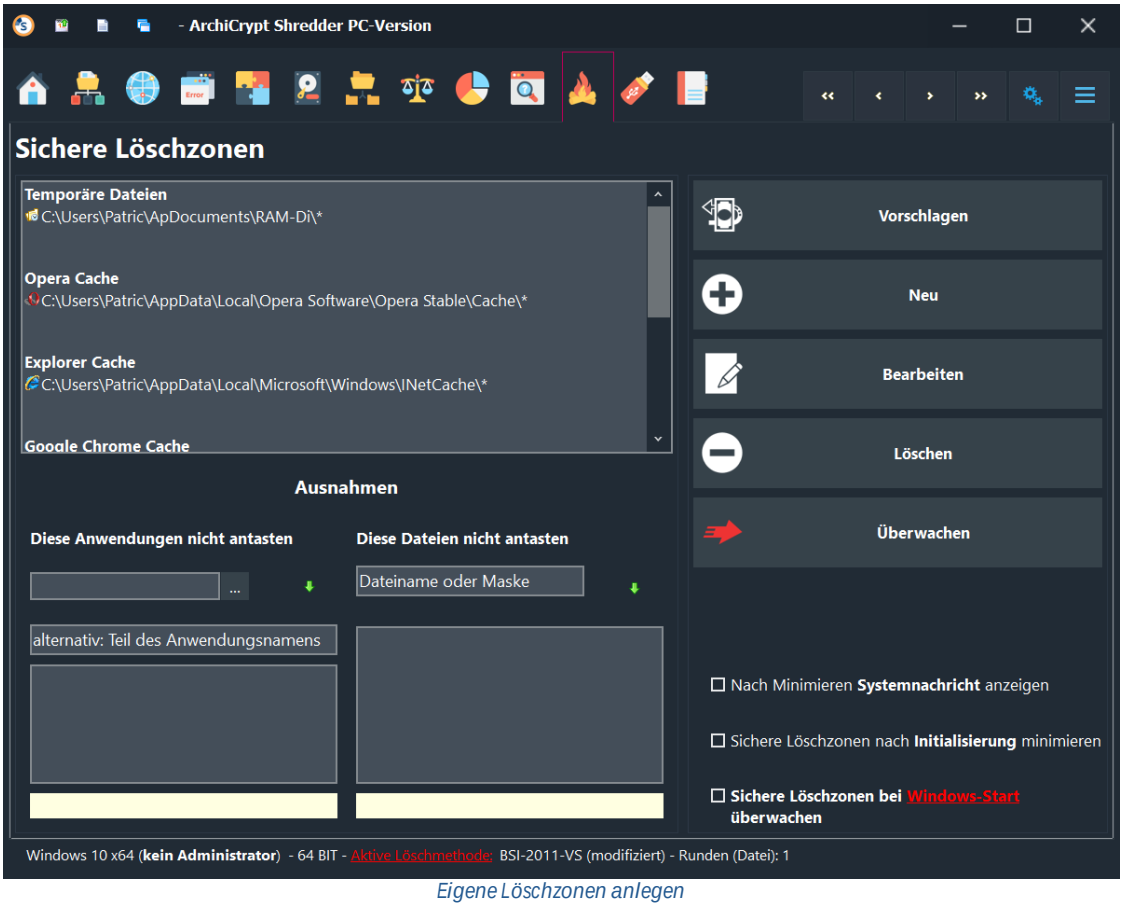
Sollen auch die Dateinamen gelöscht werden, müssen Sie die Altlasten (Dateinamen) 64 ***gesondert über die Funktion im Shredder entfernen.***

8.7.2 Sichere Löschzonen erstellen

Löschzonen erstellen

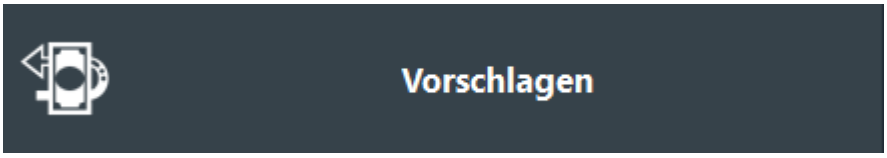
siehe auch: Überblick 74 und Löschzonenüberwachung 82

Lassen Sie sich *Löschzonen vorschlagen* oder definieren Sie eigene Löschzonen.



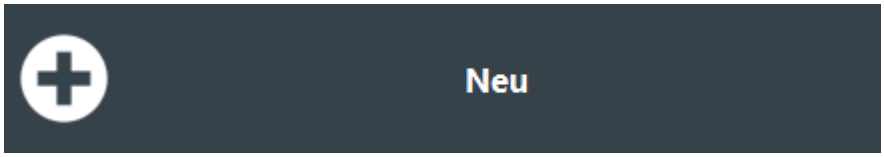
Eigene Löschzonen anlegen

Klick auf die Schaltfläche

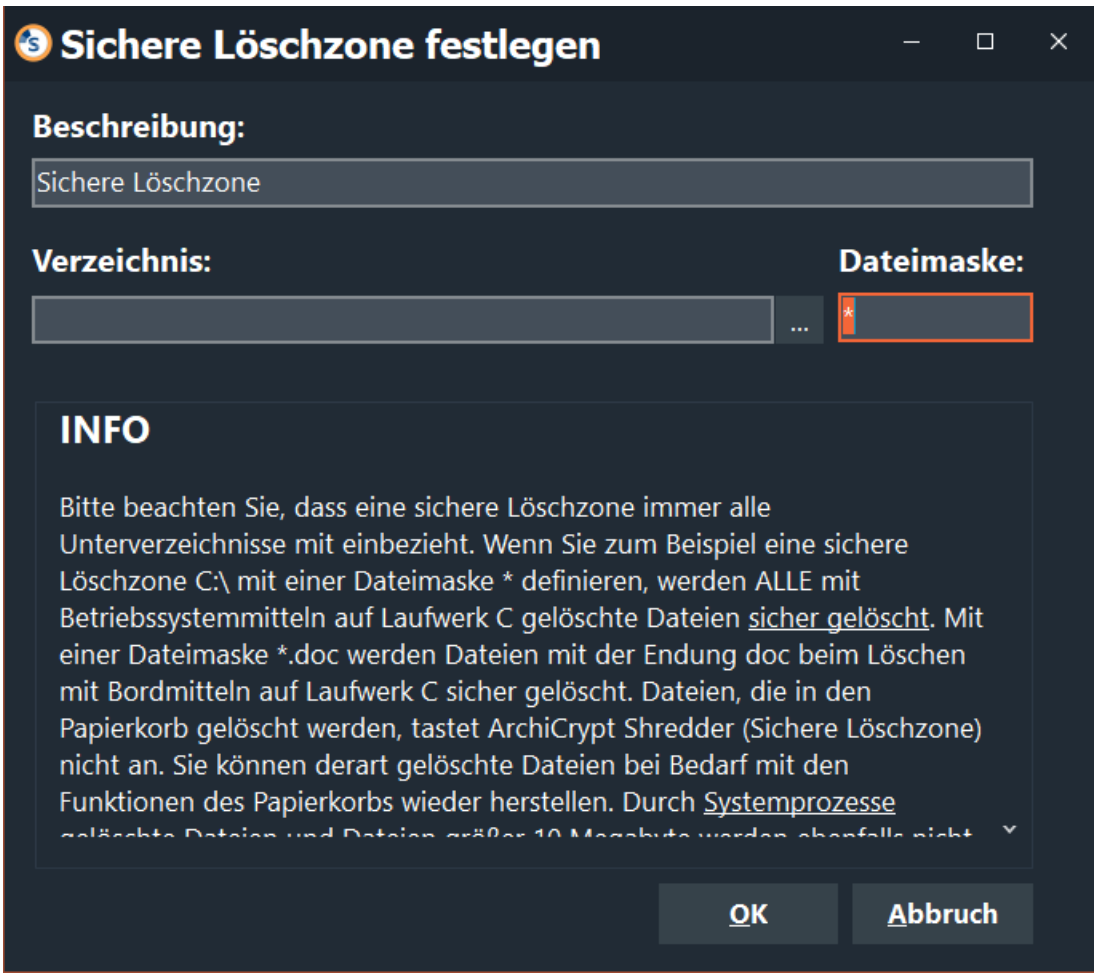


Mit ArchiCrypt Shredder können Sie Löschzonen definieren und bearbeiten. Um Ihnen den Einstieg zu erleichtern, kann ArchiCrypt Shredder einige Beispielzonen erstellen. Die so erzeugten Sicheren Löschzonen sind in Anzahl und Art je nach Rechner unterschiedlich. Zum Erstellen der Beispielzonen betätigen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

So erstellen Sie eine neue Löschzone



Betätigen Sie die Schaltfläche "Neu"



Geben Sie eine Beschreibung für die Löschzone 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. Dateimaske festlegen. Das * ist ein s.g. Platzhalter und steht für eine beliebige Zeichenfolge. Ist als Maske also * angegeben, fängt ArchiCrypt Shredder alle Löschoperationen ab. Wenn Sie z.B. *.txt angeben, fängt ArchiCrypt Shredder das Löschen von Textdateien ab, bei W*.doc alle

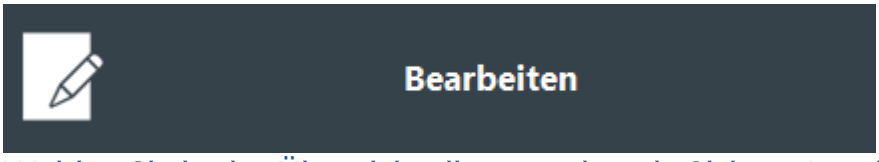
Löschoperationen von Dateien, deren Name mit W beginnt und deren Dateiendung doc ist.

UNBEDINGT LESEN: ***Es werden immer auch alle Unterverzeichnisse überwacht! (rekursiv).***
Vermeiden Sie es möglichst, ein komplettes Laufwerk mit der Maske * als Löschzone zu definieren. Die Performance Ihres Systems leidet je nach Einstellung der Löschart 182 ***unter Umständen erheblich.***

Wenn Sie entgegen dem Ratschlag dennoch ein komplettes Laufwerk als Löschzone festlegen, sollte dies die einzige Löschzone für dieses Laufwerk sein!

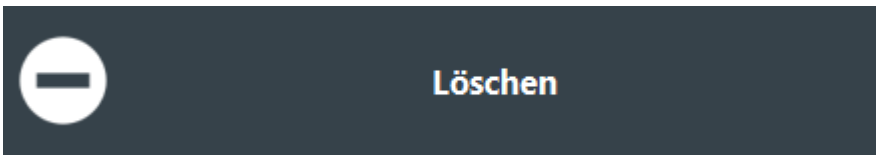
So arbeiten Sie mit den Sicheren Löschzonen

Sichere Löschzone bearbeiten



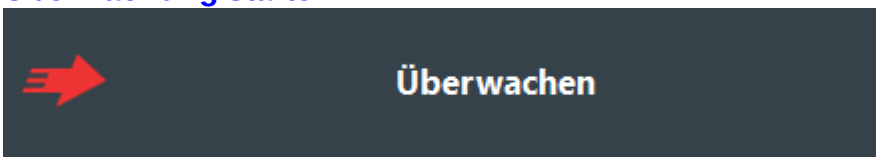
Wählen Sie in der Übersicht die zu ändernde Sichere Löschzone aus und betätigen Sie die Schaltfläche Bearbeiten. Nehmen Sie die gewünschten Änderungen vor und betätigen Sie die **Schaltfläche OK**.

Sichere Löschzone entfernen



Wählen Sie die zu löschenden Löschzone aus und betätigen Sie die **Schaltfläche Löschen**.

Überwachung starten



Löschzonen werden von ArchiCrypt Shredder - Löschzonenüberwachung 82 überwacht. Erst wenn ArchiCrypt Shredder

- Löschzonenüberwachung aktiv ist, werden die Löschaktionen in den definierten Löschzonen durch ArchiCrypt Shredder überwacht.

(siehe auch Löschzonenüberwachung 82)

Optionen und ihre Wirkung

Nach Minimieren Systemnachricht anzeigen

Wenn die Löschzonenüberwachung in den Infobereich der Taskleiste minimiert wird, wird ein kurzes Hinweisfenster angezeigt.

Sichere Löschzonen nach Initialisierung minimieren

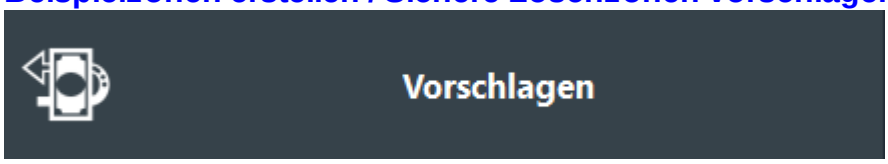
Falls die Löschzonenüberwachung erfolgreich gestartet wird, wird sie automatisch in den *Infobereich der Taskleiste* minimiert.

Sichere Löschzonen bei Windowsstart überwachen

Diese Option bewirkt, dass die Löschzonenüberwachung mit Windows gestartet wird und direkt die Löschzonen überwacht werden.

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 Löschzone manuell in den Autostart-Ordner kopieren. Hinweise dazu finden Sie in der Hilfe zum Betriebssystem.

Beispielzonen erstellen / Sichere Löschzonen vorschlagen



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

Ausnahmen für Sichere Löschzonen

Im Bereich Ausnahmen können Sie Anwendungen festlegen, bei denen ArchiCrypt Shredder nicht eingreifen soll, falls unsicher gelöscht wird. Hier können Sie entweder den kompletten Pfad zur Anwendung oder den Namen der Anwendung eingeben (1). Die Mit der Pfeil Schaltfläche (2) übertragen Sie die Daten in die Liste. Um einen Eintrag wieder aus der Liste zu entfernen, markieren Sie ihn und betätigen Sie die rechte Maustaste. Im Kontextmenü wählen Sie den Menüpunkt Löschen (3).

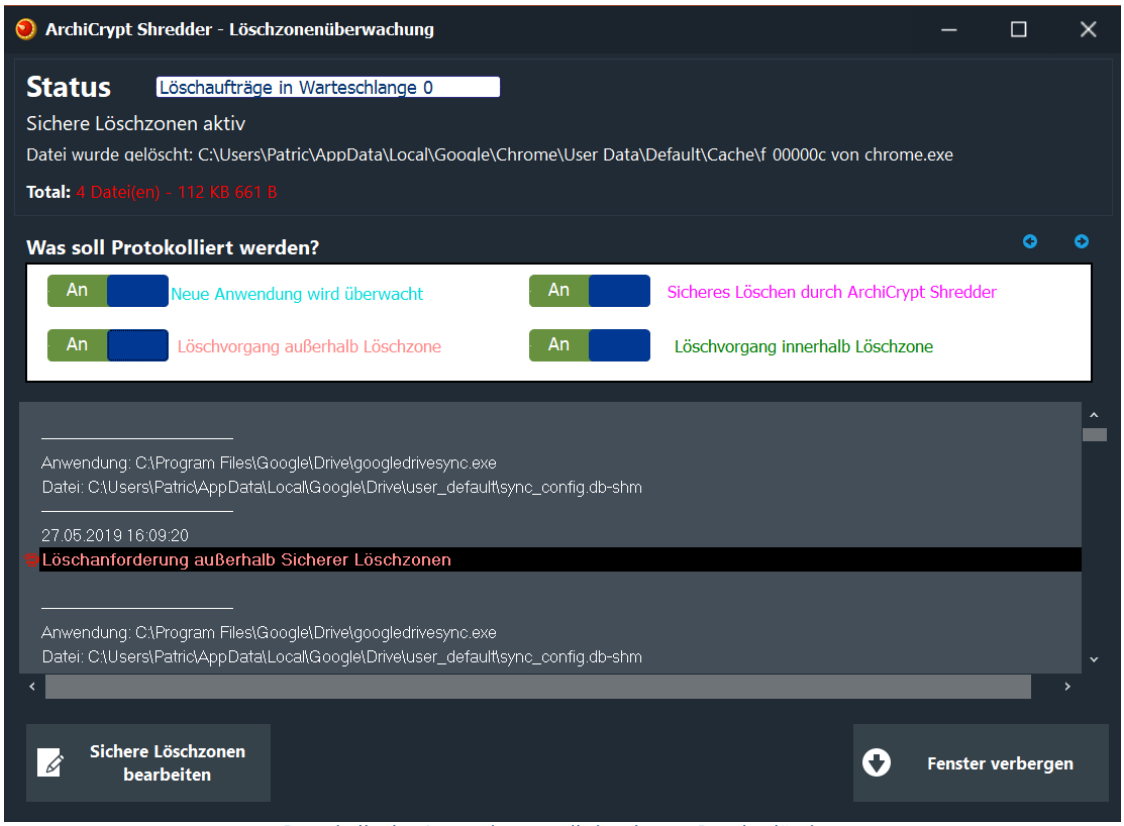
Weiterhin können Sie bestimmte Dateien und Dateitypen als Ausnahme definieren (4). Mit der Pfeil-Schaötfläche (5) übernehmen Sie den Wert. Zum Löschen eines Eintrags (6) rufen Sie das Kontextmenü auf.

Beim Löschen entsprechender Dateien in einer Löschzone greift ArchiCrypt Shredder nicht ein.

8.7.3 Überwachung der Sicheren Löschzonen

Löschzonenüberwachung

siehe auch: Überblick über Sichere Löschzonen 74 und Sichere Löschzonen 77



Protokoll zeigt Anwendungen, die bestimmte Dateien löschen

Die Löschzonenüberwachung ist das Programm, welches die eigentliche Überwachung der Sicheren Löschzonen vornimmt.

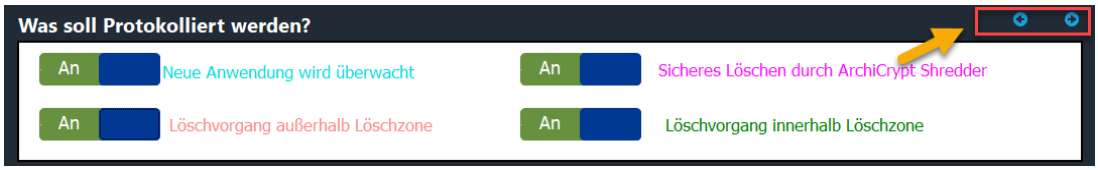
Dies bedeutet:

Erst, wenn die *Löschzonenüberwachung* gestartet ist, werden die Dateien in den Löschzonen durch ArchiCrypt Shredder SICHER gelöscht. Wird die Löschzonenüberwachung beendet, werden die Löschzonen auch nicht mehr überwacht.

Status und Logbuch der Sicheren Löschzonen

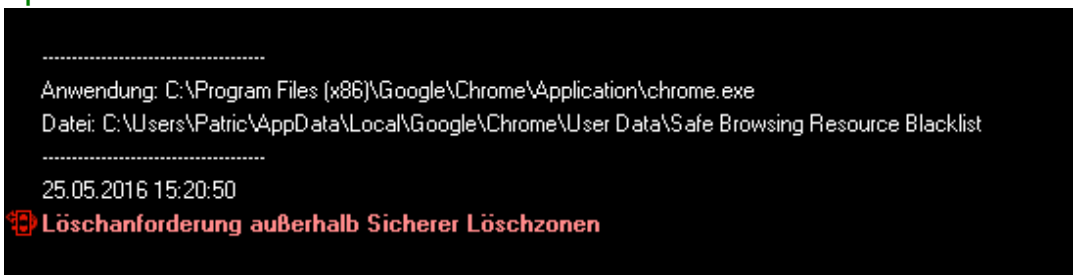
Daneben zeigt die Löschzonenüberwachung auf Wunsch auch Informationen über durchgeführte Löschaktionen an. In einem Protokoll werden Anwendungen angezeigt, die überwacht werden, es

wird protokolliert, wenn eine Datei in oder außerhalb einer Löschzone gelöscht wird.



EXPERTENTIPP: Wenn Sie herausfinden möchten, ob und wo eine Anwendung Dateien temporär speichert, aktivieren Sie die Protokollfunktion Löschvorgang außerhalb Löschzone. 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 Löschzone erhalten.

Beispiel:



Im obigen Beispiel sehen wir, dass Google Chrome im Verzeichnis C:\Users\Patric\AppData\Local\Google\Chrome\User Data\Safe Browsing Resource Blacklist **eine Datei gelöscht hat, die nicht in einer sicheren Löschzone liegt. Wir könnten jetzt eine entsprechende Sichere Löschzone mit** C:\Users\Patric\AppData\Local\Google\Chrome\User Data **als Verzeichnis und * (***Sternchen = alles Dateien***) als Maske anlegen, um auch hier die Löschoperationen künftig abzufangen!**

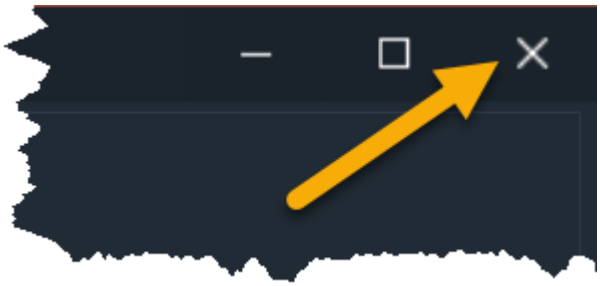
Das Protokoll bietet ein Kontextmenü, das Sie mit der rechten Maustaste aufrufen können. Im Kontextmenü stehen Ihnen die Funktionen Löschen (*setzt das Protokoll zurück*) und In Zwischenablage kopieren (*Kopiert den aktuellen Inhalt in die Zwischenablage; Sie*

können den Text in jedem Textprogramm wie z.B. Wordpad oder Word einfügen) zur Verfügung.

TIPP: Ein doppelter Linksklick auf eine Zeile im Protokoll mit Datei- oder Programmname öffnet den Windows Explorer und navigiert direkt zur Datei.

Bedienung der Löschzonenüberwachung

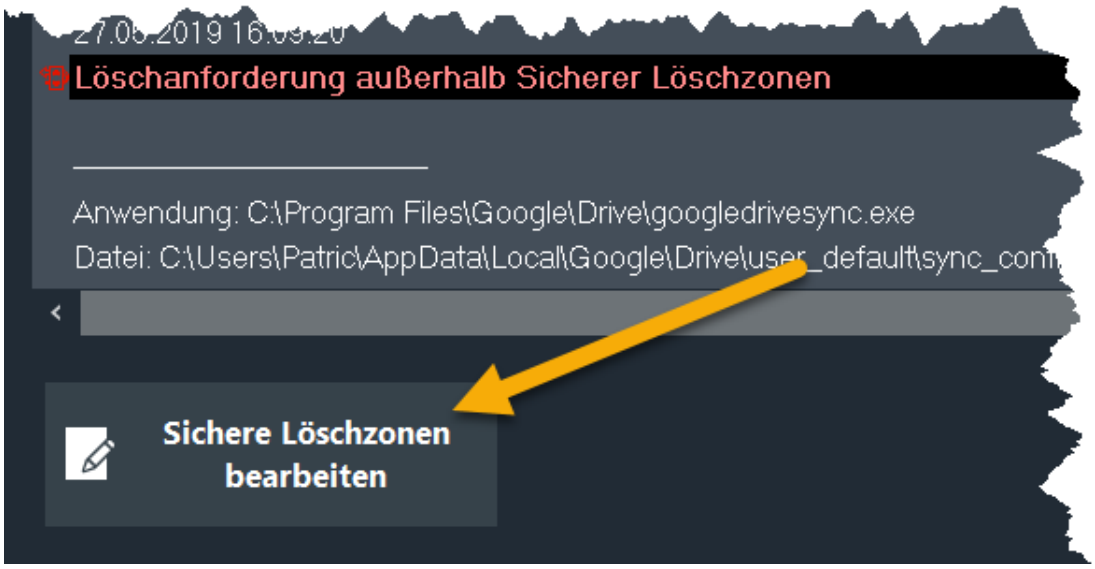
Überwachung der Sicheren Löschzonen beenden



^

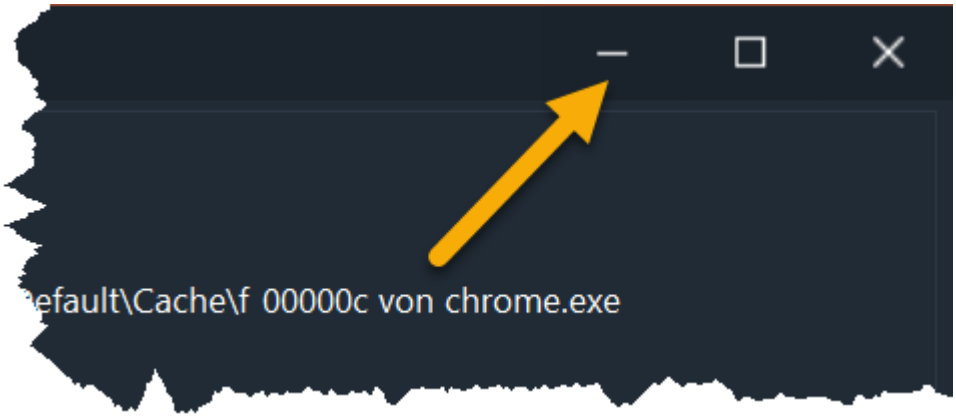
➡ WICHTIG: ***Die Überwachung der Sicheren Löschzonen wird mit dem Beenden ausgeschaltet!***

Sichere Löschzonen bearbeiten

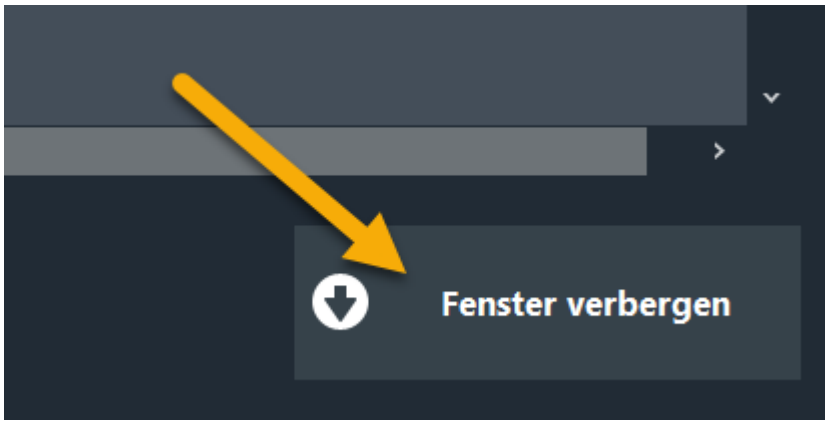


ArchiCrypt Shredder wird aufgerufen um die Löschzonen zu bearbeiten.

Fenster minimieren



oder



ArchiCrypt Sichere Löschzone wird minimiert und überwacht im Informationsbereich die Sicheren Löschzonen weiter. Per Doppelklick auf das Symbol können Sie die Löschzonenüberwachung anzeigen lassen. Falls Sie die Löschzonenüberwachung nicht im Systemtray finden, sehen Sie sich an, wie man Symbole im Infobereich sichtbar[47] macht.

Fängt die Löschzonenüberwachung eine unsichere Löschoperation ab, werden die Augen im Systemfach für kurze Zeit rot angezeigt.

8.8 Online-Spuren

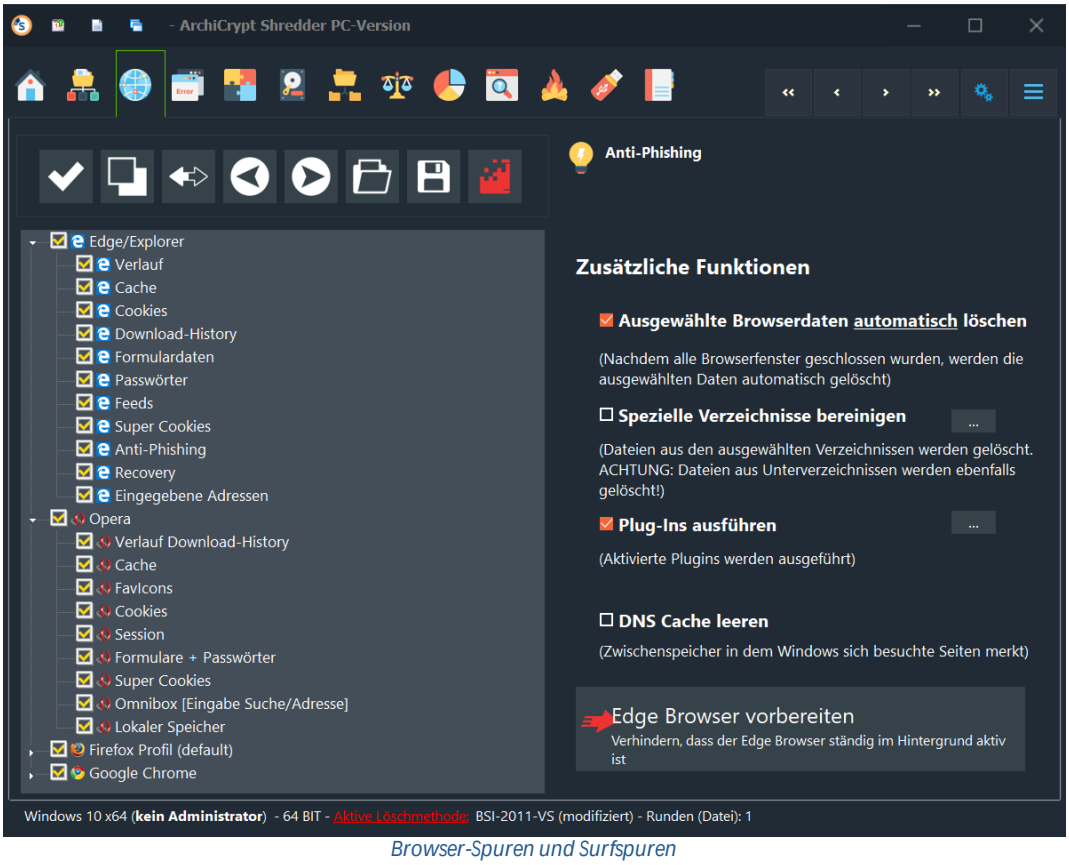
siehe auch:
Plug-Ins erweitern die Funkionalität 96
Löschen von Verzeichnissen 55

Spuren im Internet beseitigen

WEB-Browser zeichnen nahezu jede Aktion im Internet akribisch auf und speichern Texte, Bilder, Videos, Downloads etc. in einem *Zwischenspeicher* auf Ihrem Rechner (*oft* Cache *genannt*).

Einige der Browser bieten, meist tief in Untermenüs verborgen, eine Möglichkeit, diese Dateien zu löschen. Gelegentlich fehlt diese Funktion ganz.

Ist eine solche Funktion vorhanden, werden diese Daten vom Browser IMMER 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 wieder hergestellt werden können.

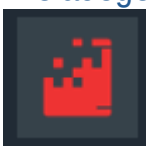


Browser-Spuren und Surfspuren

Online-Funktionen bieten umfassende Möglichkeiten, alle wichtigen Spuren zu beseitigen, die eine Internetsitzung auf Ihrem Rechner hinterlässt. Im Bereich der Browser-spezifischen Funktionen können Sie festlegen, welche der vom Browser gesammelten Daten gelöscht werden sollen.

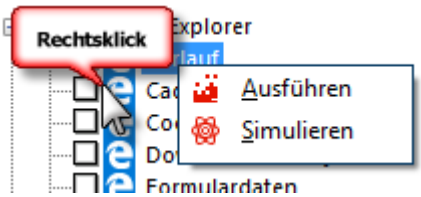
Unterstützte WEB-Browser: *Edge/Internet Explorer, Google Chrome, Firefox und Opera*

Ist ein Browser nicht auf Ihrem Rechner installiert, blendet Shredder diesen Browser aus!

Die ausgewählten Einträge können Sie über die **Shreddern** Schaltfläche  löschen. Wenn Sie einen einzelnen Eintrag auswählen und die

rechte Maustaste betätigen, können Sie den Löschvorgang simulieren oder die dem Eintrag zugeordnete Funktion ausführen.

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[181] aktivieren!)

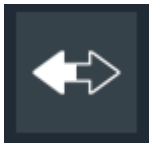


Um die Liste mit Online Aktionen zu bearbeiten, steht Ihnen eine Menüleiste zur Verfügung:

Alle Einträge auswählen

Auswahl aufheben

Auswahl umkehren



Ansicht einklappen

Ansicht ausklappen

Online-Profil laden und speichern

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

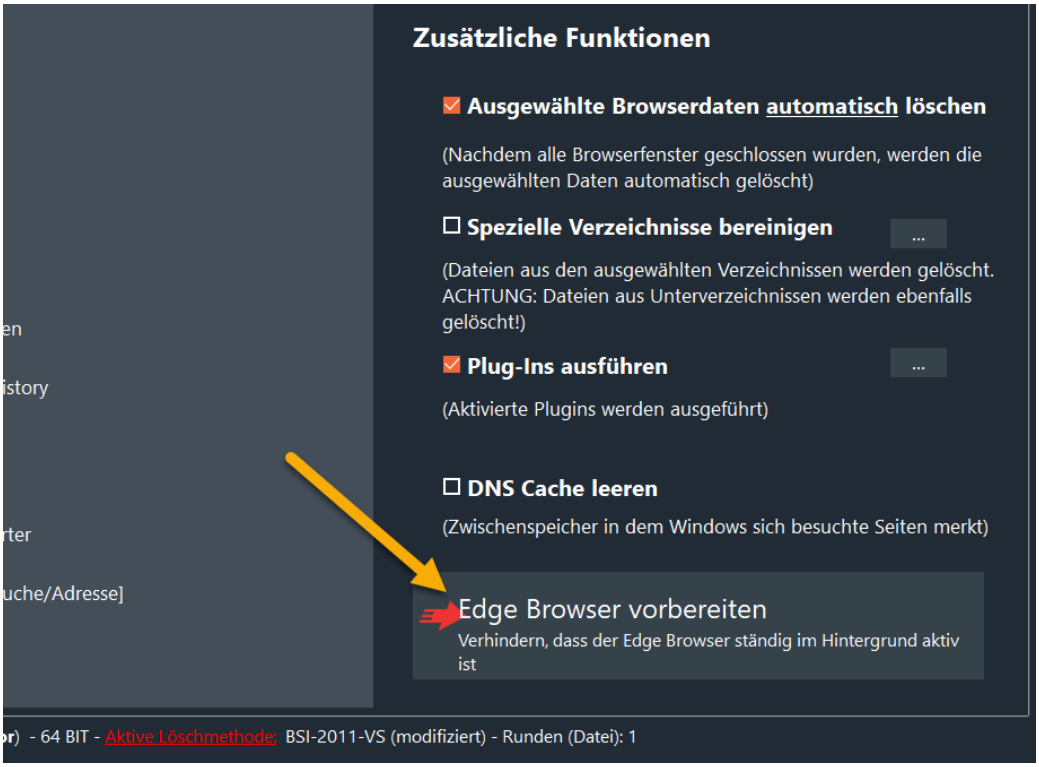
Die Online-Profile sind sehr nützlich wenn es darum geht, für verschiedene Situationen unterschiedliche Löschaktionen vorzusehen. Markieren Sie die gewünschten Löschaktionen und speichern Sie diese für eine spätere Verwendung. Im Aufgaben-Planer[145] können Sie den Shredder dann zu bestimmten Zeiten ganz gezielt bestimmte Profile ausführen lassen. Es ist auch möglich, sich mit Hilfe des Aufgaben Planers 1-Klick Löschaufgaben[153] zu erzeugen, die dann bestimmte Online-Profile ausführen.

Funktionen der ausgewählten Einträge ausführen

Besonderheiten Edge Browser

Der Edge Browser weist einige Besonderheiten auf. Insbesondere in den neueren Build von *Windows 10* (*Oktober Update 2018*; *Build 1809 und später*) wird der *Edge Browser* sofort mit dem System gestartet und *nicht mehr beendet*. Stattdessen versetzt Windows den Browser in eine Art *Schlafmodus*.

Dadurch wird es nicht nur sehr schwer, zu erkennen, wann der Browser beendet wurde. Im Schlafmodus blockiert der Edge Browser auch Datenbanken und Dateien, die beim Beseitigen von Spuren frei verfügbar sein müssen. So kann es mitunter zu Fehlermeldungen kommen, weil Dateien blockiert sind, auf die der Shredder zugreifen muss. Der ständig im Hintergrund laufende Browser belegt zudem dauerhaft Systemressourcen. Der Vorteil des Schlafmodus kommt nur zum Tragen, wenn man den Browser startet. In diesem Fall spart man einige Millisekunden, da die Edge Anwendung nicht vom Datenträger gelesen werden muss, sondern nur "aufgeweckt".



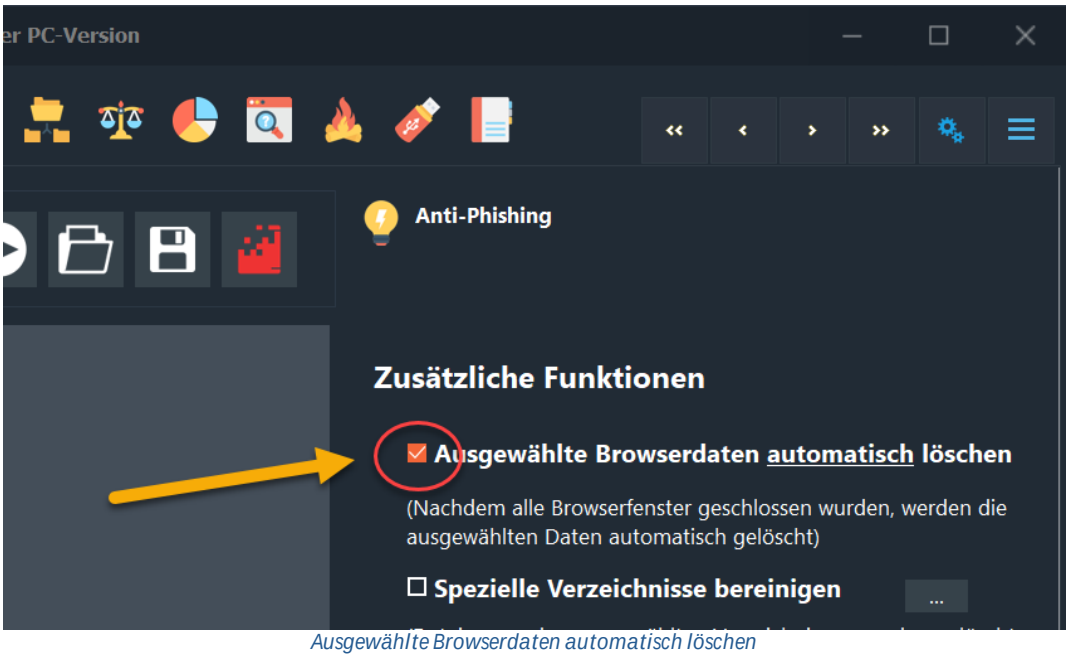
Edge Browser einrichten

Die Schaltfläche **Edge Browser vorbereiten** passt Windows so an, dass der Browser beim Start von Windows *nicht automatisch* geladen und

in den Schlafmodus versetzt wird. Zudem wird sichergestellt, dass der Edge Browser beim Beenden jeweils wirklich beendet wird.

So löschen Sie Surf Spuren automatisch

Sie können ausgewählten Aktionen automatisch beim Beenden des zugehörigen Browsers ausführen lassen. Schalten Sie dazu die Funktion "Ausgewählte Browserdaten automatisch löschen" ein.

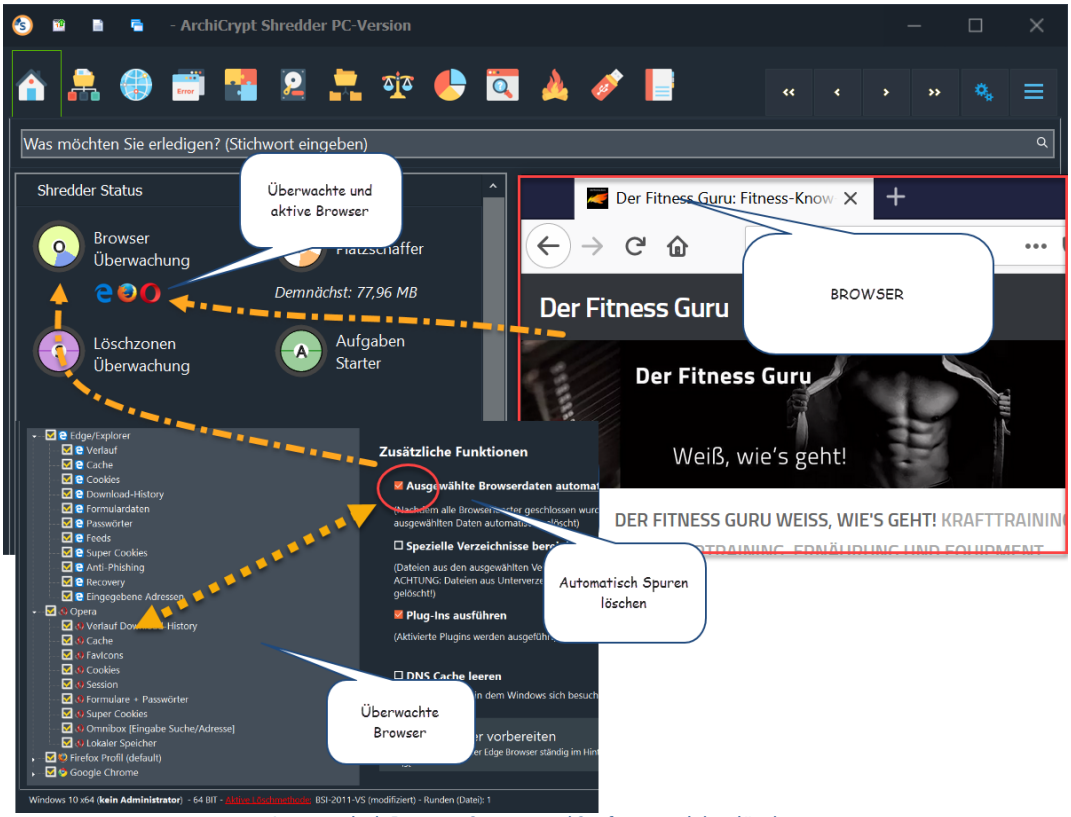


Ausgewählte Browserdaten automatisch löschen

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. Beim Löschen der Browserdaten werden auch die zusätzlich ausgewählten Aufgaben abgearbeitet (*zum Beispiel Spezielle Verzeichnisse bereinigen oder Plug-Ins ausführen*).

WICHTIG: Starten und Beenden Sie zum *Beispiel* den Edge Browser, werden die gewählten Spuren für Edge beseitigt und die zusätzlich ausgewählten Aufgaben abgearbeitet. Schließen Sie anschließend Opera und sind hierfür ebenfalls Spuren ausgewählt, werden auch hier die Spuren von Opera gelöscht und die zusätzlichen Aufgaben bearbeitet. Gerade dann, *wenn Sie oft mit mehreren Browsern arbeiten*, sollten Sie

insbesondere die Plug-Ins lieber manuell oder als 1-Klick Aufgabe[145] gesondert ausführen.



Automatisch Browser Spuren und Surfspuren sicher löschen

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

Rotes Symbol: Kein automatisches Löschen von Online-Spuren
Blaues Symbol: Automatisches Löschen ist aktiviert, es ist jedoch kein zu überwachender Browser geöffnet.
Grünes Symbol: Automatisches Löschen ist aktiv, ein oder mehrere Browserfenster sind geöffnet.
Mit dem Schließen des letzten Browserfensters startet der Löschvorgang.

Das Löschen der Online-Spuren kann mit Hilfe der Funktionen

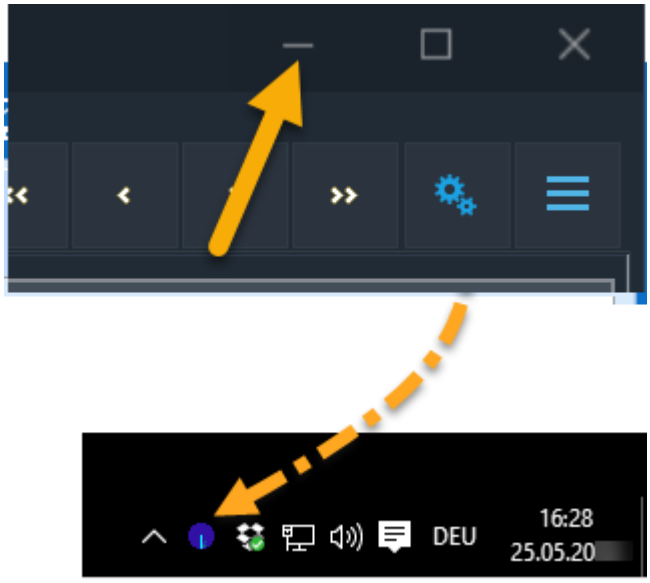
- spezielle Verzeichnisse bereinigen[55]

- Plug-Ins ausführen 96
- DNS Cache leeren

um zusätzliche Aufgaben erweitert werden. Öffnen Sie zum Beispiel während des Surfens im Internet oft ZIP-Archive oder betrachten Videos, können Sie die entsprechenden Plug-Ins 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 minimieren (*Infobereich nähe Systemuhr*) und dort über das Symbol per Doppelklick im Bedarfsfall wieder aufrufen. Wenn das Symbol des Shredders im Systemtray/der Taskleiste nicht sehen, dann lassen Sie sich das Symbol in der Taskleiste anzeigen 47.

Minimieren Sie den Shredder einfach



So löschen Sie beim Beenden eines Browsers Dateien in bestimmten Verzeichnissen

Wenn Sie in der Kategorie Verzeichnisse[55] eine Liste mit Verzeichnissen erstellt UND gespeichert haben (*ohne dass Sie eine Liste gespeichert haben, werden die Einträge bei jedem Start des Shredders leer sein*), können Sie die Einträge gleich mit den Surf Spuren beseitigen lassen.

Bestimmte Verzeichnisse beim Beenden eines Browsers löschen

So führen Sie beim Beenden eines Browsers bestimmte Plug-ins aus

Markieren Sie in der Kategorie Plug-ins[96] die *Plug-Ins*, die beim Beenden des Browsers automatisch ausgeführt werden sollen.

Beim Beenden eines Browsers Plug-Ins ausführen

weiter zu: Plug-Ins erweitern die Funkionalität 96

8.9 Plug-Ins erweitern die Funkionalität

siehe auch: Daten die Windows heimlich sammelt 107

Das Plug-in-System von ArchiCrypt Shredder

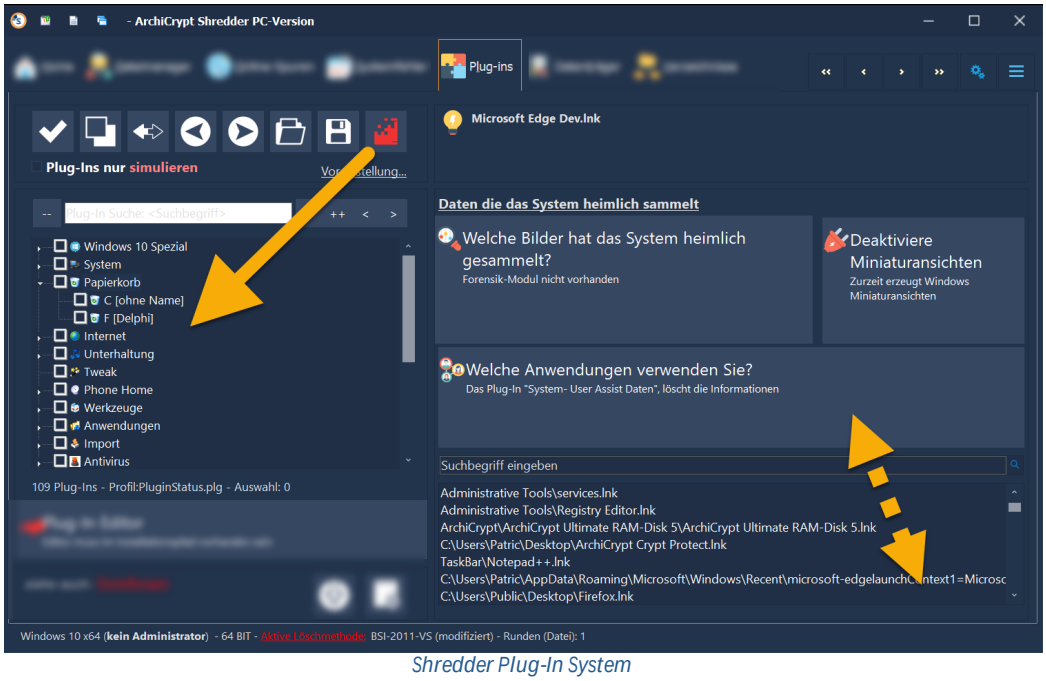
Die Plug-ins bieten die Möglichkeit, ArchiCrypt Shredder zu erweitern, ohne dass man Änderungen am Programm selbst vornehmen muss.

Die Vollversion von ArchiCrypt Shredder bringt bereits zahlreiche Plug-ins mit.

Ein Plug-In für Microsoft Word ist überflüssig, wenn auf dem Rechner kein Word installiert ist. Das Plug-in-System ist "intelligent" und ermittelt beim ersten Start, welche Plug-ins auf Ihrem System Sinn machen.

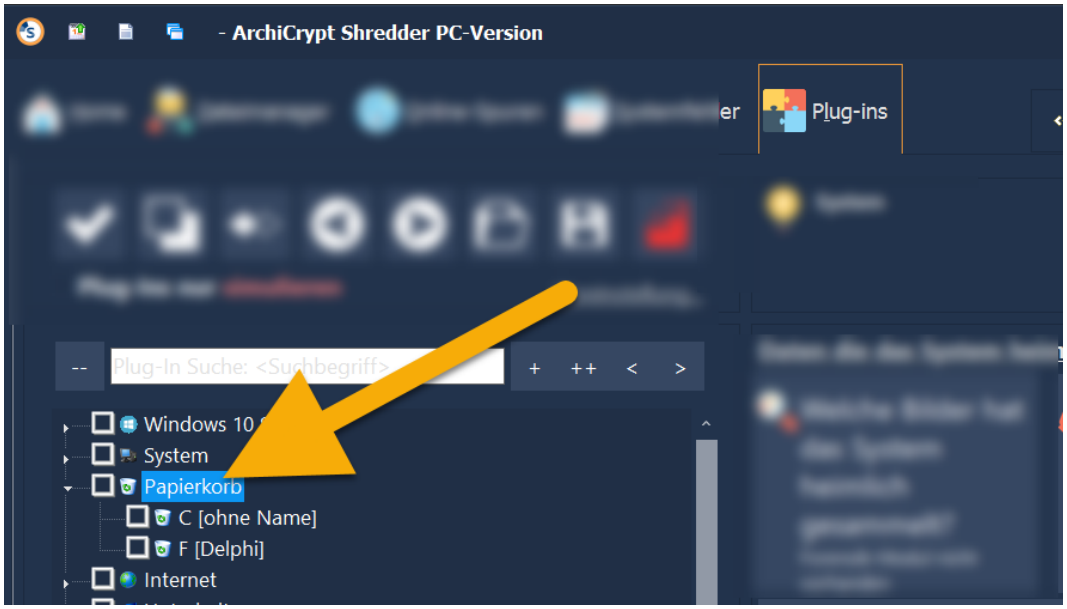
EXPERTENTIPP: Die *Plug-Ins* liegen im Quellcode vor (*Installationsverzeichnis des Shredders, Unterordner plugins*) und

können von fortgeschrittenen Anwendern als Vorlage für eigene Plug-ins verwendet werden.



Shredder Plug-In System

So löschen Sie den Papierkorb



Papierkorb shreddern

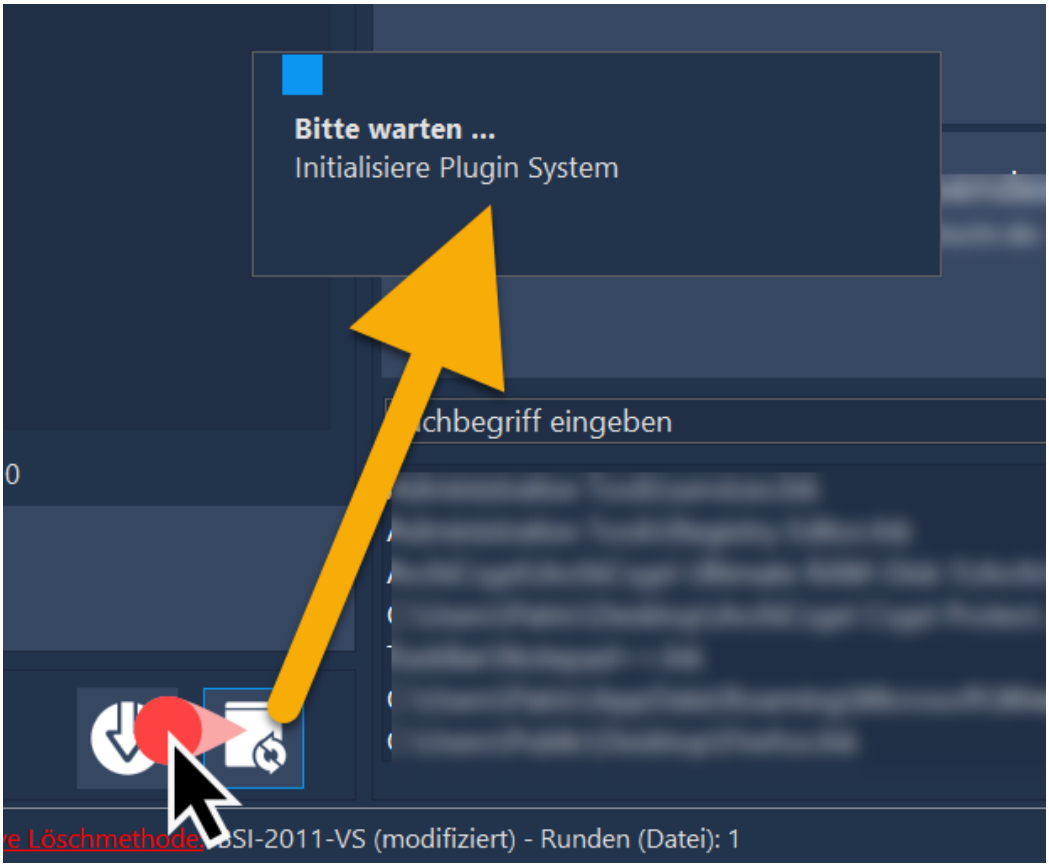
Der Papierkorb, auch *Recycler* oder *Trash Bin* genannt, enthält nicht etwa die tatsächlichen Dateien. Der Papierkorb in Windows ist eine Struktur, in der die Verweise auf eine Datei (*wo liegen die Daten dieser Datei*) und deren Meta-Informationen (*Zeit-Stempel, Name, etc.*) abgelegt sind. Solange eine Datei bzw. deren Positions- und Meta-Daten in der *Papierkorbstruktur* gespeichert sind, blockiert das Windows Betriebssystem den Speicherort der eigentlichen. Entsprechend ändert sich der frei verfügbare Speicher auf einem Datenträger nicht, wenn man eine Datei in den Papierkorb "löscht".

Mit dem speziellen Papierkorb Plug-In löscht ArchiCrypt Shredder die Meta-Daten der Dateien des gewählten Laufwerks und sorgt dafür, dass der Speicher auf dem Datenträger wieder zur Verfügung steht.

So initialisieren Sie das Plug-in System neu

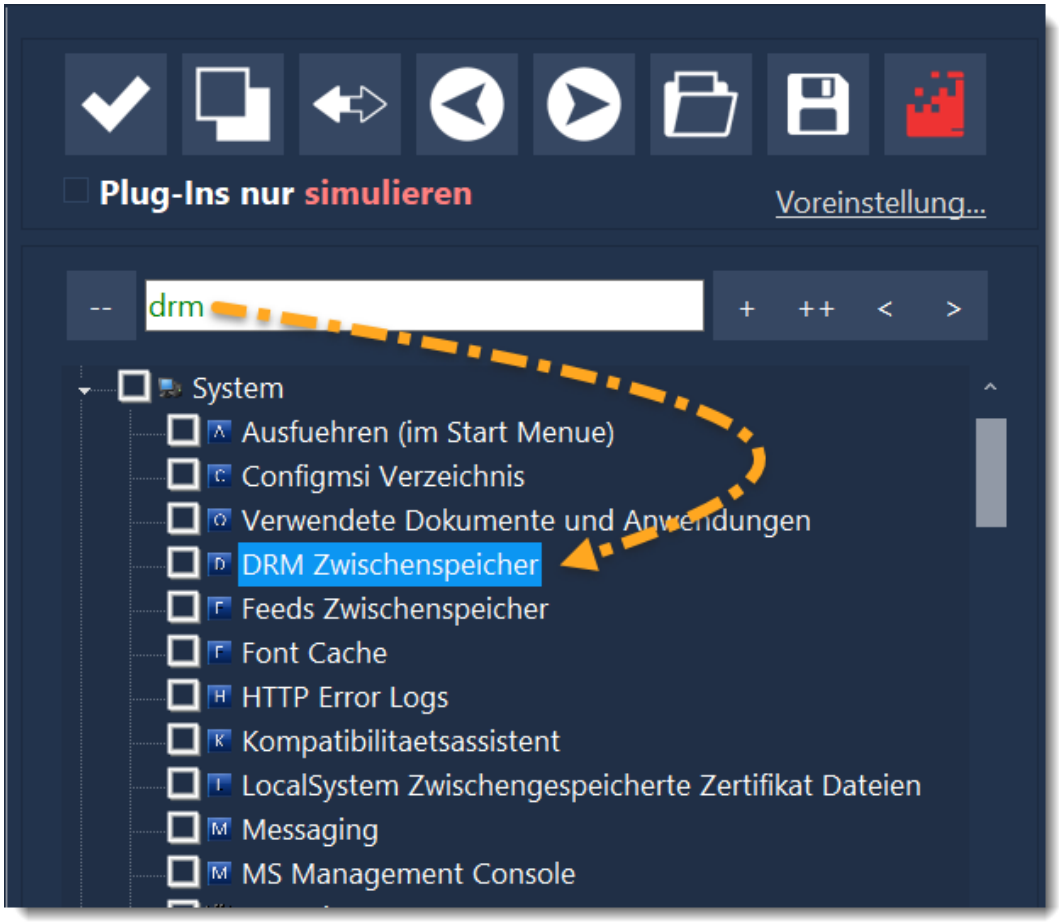
Sollten Sie neue Software installieren, kann es sinnvoll sein, ArchiCrypt Shredder erneut zu veranlassen, das Plug-In System zu initialisieren.

ArchiCrypt Shredder bringt eine ganze Reihe an Plug-Ins mit. Klar ist, dass nicht jedes Plug-In auf jedem Rechner Sinn macht. Wer kein Open Office auf dem Rechner hat, der braucht auch kein Open Office Plug-In. Die Neu-Initialisierung prüft, welche Plug-Ins auf Ihrem Rechner relevant sind. Dieser Vorgang kann einige Minuten in Anspruch nehmen. Im Ergebnis werden jetzt nur noch Plug-Ins aufgeführt, die für Ihren Rechner von Bedeutung sind.



So finden Sie ein bestimmtes Plug-in

Geben Sie einige Zeichen des gesuchten Begriffs in das Suchfeld ein. Mit den Pfeiltasten neben dem Suchfeld können Sie zwischen *verschiedenen Fundstellen* hin und her springen.



Suche nach einem Plug-In

Schnelle an und Abwahl von Plug-Ins

Neben dem Eingabefeld für den Suchbegriff finden Sie verschiedene Schaltflächen mit denen Sie rasch *passende Einträge An- und Abwählen* können.

Deaktiviert alle Plug-Ins die den Suchbegriff beinhalten

Aktiviert ausschließlich die Plug-Ins die den Suchbegriff enthalten

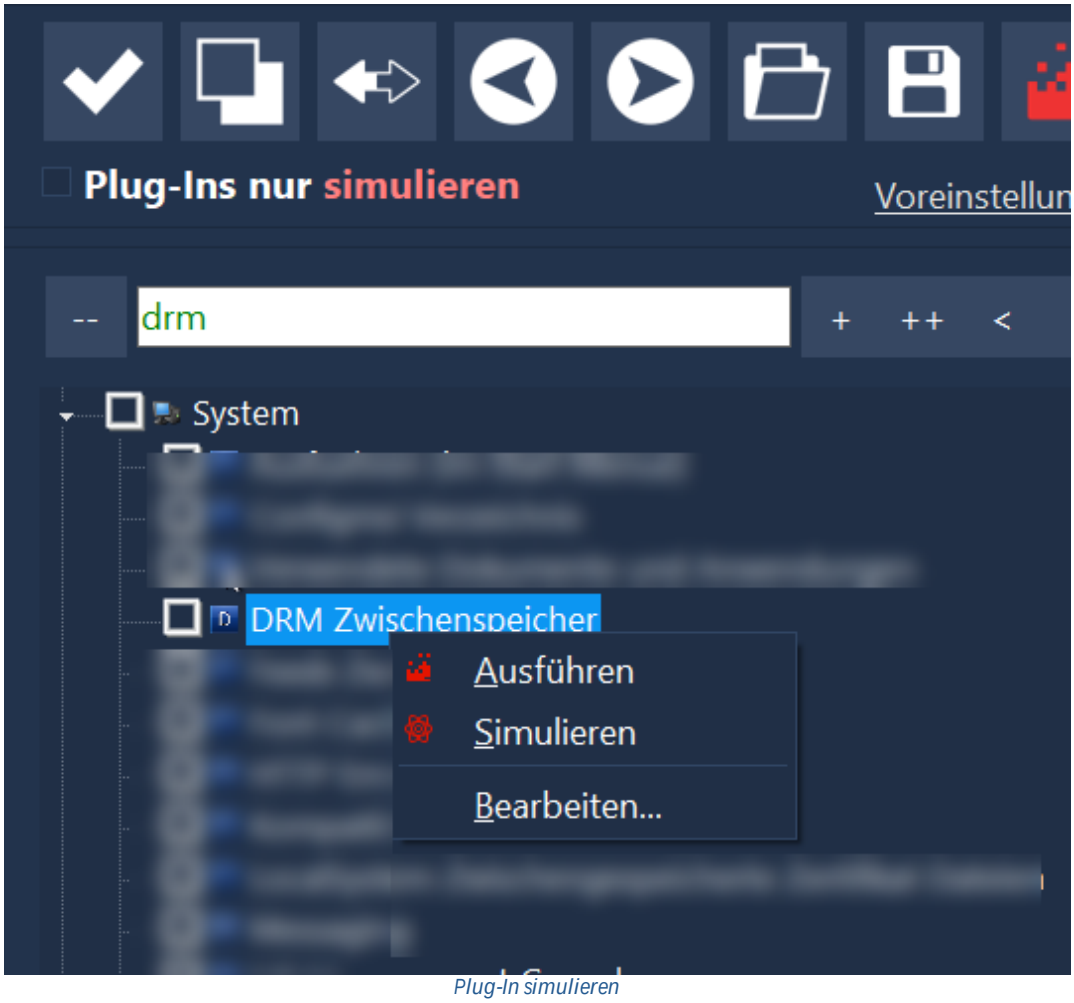
Aktiviert zusätzlich zur aktuellen Auswahl die Plug-Ins, die den Suchbegriff beinhalten

Sie können die Suche auf den Inhalt der Plug-Ins erweitern, indem Sie in den Einstellungen Allgemein - Plugins[179] die Option "Bei Plugin Suche im Script suchen" aktivieren. Damit können Sie dann zum Beispiel nach Plug-Ins suchen, die auf bestimmte *Registryschlüssel* zugreifen.

So führen Sie ein Plug-in im Simulationsmodus aus

Simulieren bedeutet, dass Daten (Dateien, Registryeinträge etc.) nicht wirklich gelöscht oder geändert werden. Es wir lediglich im Logbuch gezeigt, wo und was geändert würde.

Wählen Sie das entsprechende Plug-in mit der rechten Maustaste aus. Wählen Sie im Kontextmenü jetzt den Eintrag "Simulieren". Alternativ können Sie die Option "Plug-Ins nur simulieren" aktivieren und die Ausführung des Plug-ins über die Menüleiste  starten. Das Plug-in muss dazu aktiv sein (*vorangestelltes Häkchen*).



Plug-In simulieren

So löschen Sie Daten, die Windows heimlich sammelt

Siehe Kapitel Daten die Windows heimlich sammelt[107] !

So führen Sie Plug-ins aus

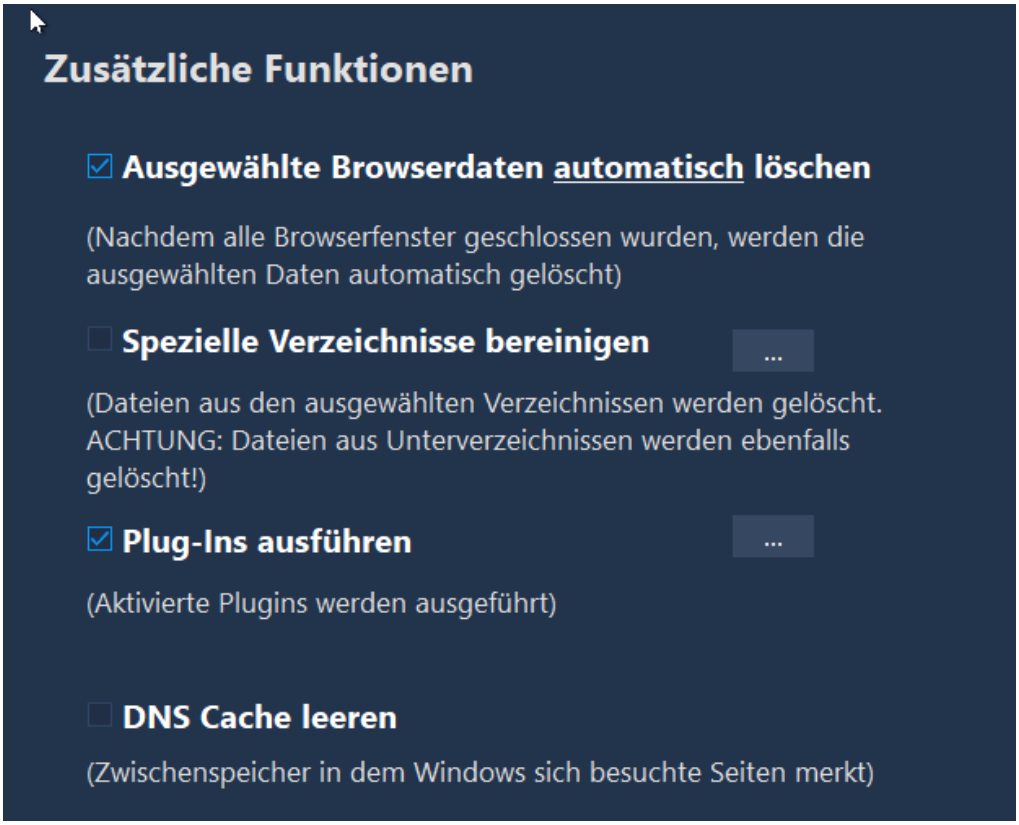
Plug-ins können grundsätzlich auf 4 Weisen ausgeführt werden.

1. Sie können die Plug-ins anwählen (*Häkchen setzen*) und dann über die  starten.

   Sofern Sie nicht den Simulationsmodus aktiviert haben (*kein Häkchen bei Plug-Ins nur simulieren*), werden die entsprechenden Aktionen ausgeführt.

2. Sie können verschiedene Plug-ins aktivieren und diese dann automatisch mit dem Beenden des Browsers ausführen lassen, indem Sie unter Online-Spuren[87] die Funktionen Ausgewählte Browserdaten automatisch löschen und Plug-Ins ausführen aktivieren.

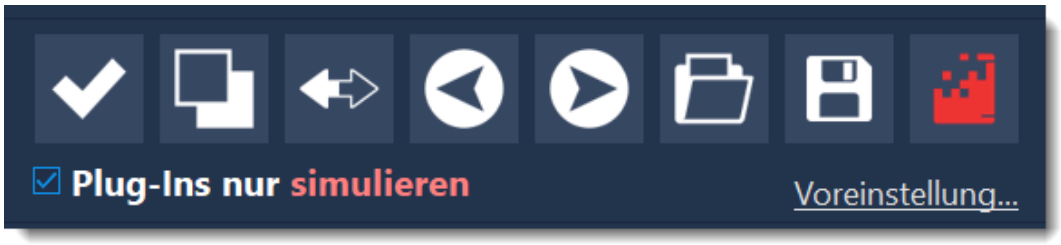
Die aktuelle Auswahl der Plug-ins **müssen** Sie zwingend als Plugin-Profil speichern.



3. Sie können Löschaufgaben planen (Aufgaben-Planer[145]), die zu bestimmten Zeiten ausgeführt werden. Hier können Sie ein Plug-In-Profil auswählen (*sie müssen die Auswahl der Plug-Ins im Shredder als* Plugin-Profil *speichern*) und es zu bestimmten Zeiten ausführen lassen.

4. Aus dem Aufgaben-Planer[145] heraus können Sie einer Löschaufgabe ein Plug-In Profil zuweisen und diese Aufgabe dann als 1-Klick Löschaufgaben[153] speichern

Um die Liste mit den Plug-Ins zu bearbeiten, steht Ihnen eine Menüleiste zur Verfügung:



Alle Einträge auswählen

Es macht keinen Sinn, alle Plug-Ins zu aktivieren. Teilweise heben sich die Aktionen der Plug-Ins gegenseitig auf!

Auswahl aufheben

Auswahl umkehren

Ansicht einklappen

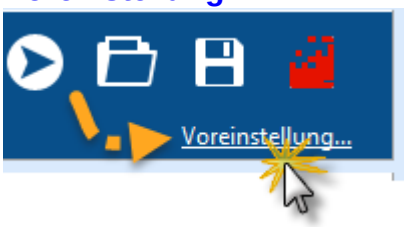
Ansicht ausklappen

Plugin-Profil laden und speichern

Plugin-Profile speichern, welche Plug-Ins aktuell aktiv (*Häkchen gesetzt*) sind. Sie können sich so für verschiedene Löschaufgaben unterschiedliche Plug-Ins zusammenstellen. Im Aufgaben-Planer[145] können Sie gezielt einzelne Plugin-Profile ausführen lassen oder 1-Klick Löschaufgaben[153] definieren, die ein bestimmtes Plugin-Profil ausführen.

Funktionen der ausgewählten Einträge ausführen

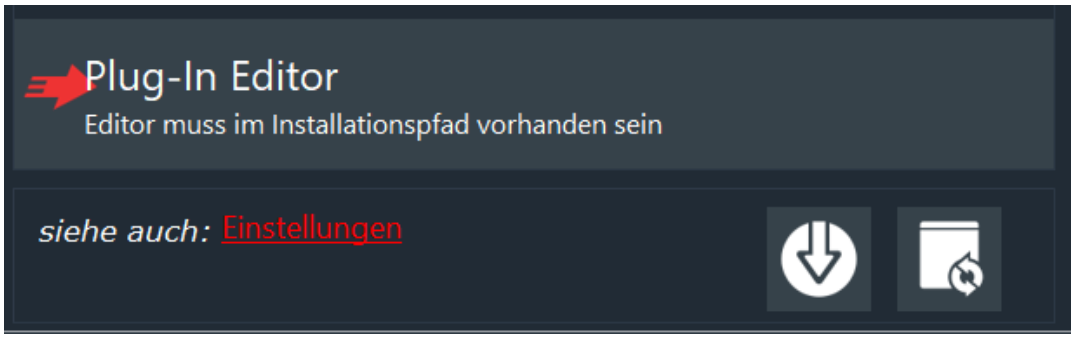
Voreinstellung



Durch Klick auf Voreinstellung werden Plug-Ins mit gängigen Aktionen automatisch aktiviert.

WICHTIGER HINWEIS: Falls Sie bei *Online-Spuren* die *Option Plug-Ins ausführen*[90] gewählt haben, werden die von Ihnen aktivierten Plug-Ins zusammen mit der Beseitigung von Onlinespuren ausgeführt!

Untere Menüleiste



Plug-In Editor

Plug-Ins neu einlesen

- Notwendig, wenn Sie während ArchiCrypt Shredder aktiv ist, neue Plug-Ins installieren.
- Sinnvoll, wenn das Plug-in System neu initialisiert werden soll, weil Sie zum Beispiel *neue Software installiert* haben.

Im Internet nach neuen Plug-Ins suchen

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

So erstellen Sie eigene Plug-ins

Sie können mit einem ganz normalen Texteditor *selbst Plug-ins erstellen*. Einfacher und komfortabler geht dies jedoch mit dem kostenlosen ArchiCrypt Shredder Plug-In Editor.

Den Editor müssen Sie sich ggf. gesondert laden und in das Anwendungsverzeichnis des Shredders kopieren.

Der Editor hat eine eigene Hilfedatei.

Sie können auch ein vorhandenes Plug-In auswählen, mit der rechten Maustaste das Kontextmenü aufrufen und dort auf bearbeiten gehen. Ein Doppelklick mit Links auf ein Plug-In öffnet ebenfalls den Plug-In Editor.

WICHTIG: Sichern Sie eigene Plug-Ins immer unter eigenem Namen und fertigen Sie zusätzlich in einem anderen Verzeichnis eine *Sicherungskopie* an. Im Rahmen eines Updates kann es vorkommen, dass Plug-Ins im Plug-In Verzeichnis überschrieben werden. Ihre Änderungen könnten dabei verloren gehen.

weiter zu: Daten die Windows heimlich sammelt 107

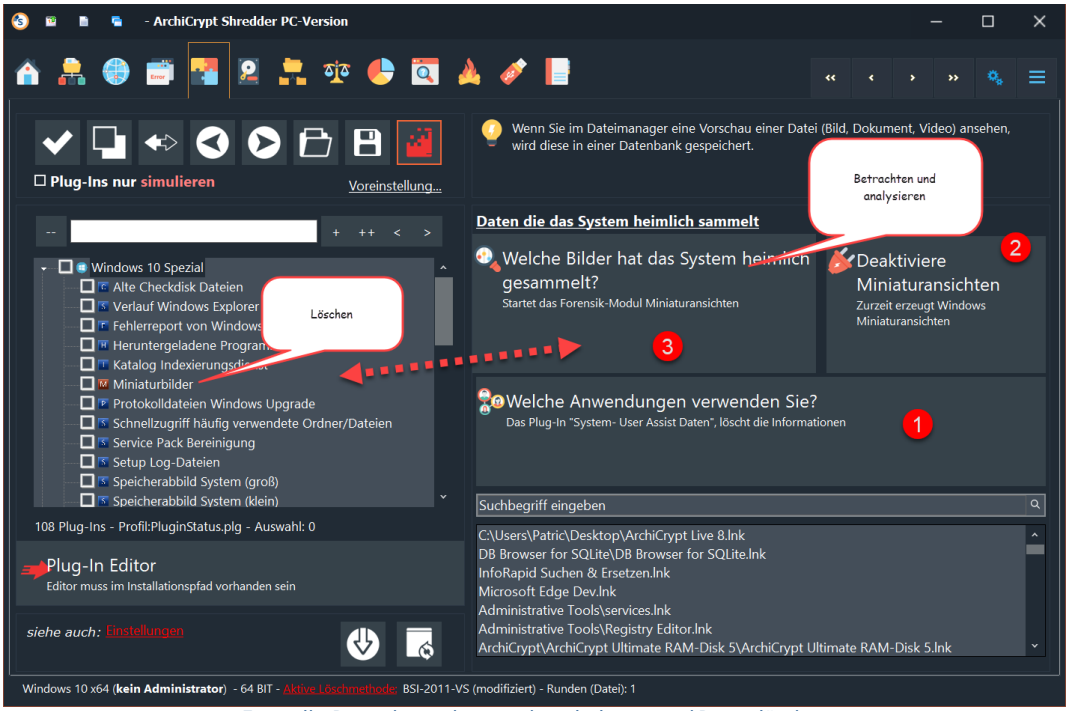
8.10 Daten die Windows heimlich sammelt

Viele wissen, dass das WEB-Browser jeden Schritt eines Anwenders aufzeichnen und Bilder und Texte besuchter Seiten auf den eigenen Rechner laden. Diese Art von Daten kann man bequem - auch automatisch - mit ArchiCrypt Shredder löschen.

Wenige wissen, dass Windows auch Buch darüber führt, welche Anwendungen Sie nutzen.

Kaum jemand weiß, dass Windows von nahezu jedem Symbol, Bild und Foto, von jeder Video- und Dokumentenvorschau eine Kopie in einer für den Anwender nicht zugänglichen Datenbank anlegt.

ArchiCrypt Shredder bringt zwei Module und verschiedene Plug-Ins mit, mit denen diese Daten nicht nur gelöscht, sondern auch eingesehen werden können.



Forensik - Daten betrachten und analysieren - und Daten löschen

ArchiCrypt Shredder ist ein Werkzeug, mit dem man viele Daten und Spuren löschen kann. Für den ein oder anderen ist es aber durchaus interessant, welche Daten gesammelt wurden.

Vorschaubilder und Miniaturansichten

Für die Miniaturansichten (*auch Vorschaubilder*, *Thumbs oder Thumbnails genannt*) gibt es ein eigenes Werkzeug. ArchiCrypt Forensik-Tool für Miniaturansichten ist spezialisiert auf die *Analyse der Datenbanken in denen diese Miniaturansichten* von Windows abgelegt werden.

Die Standardversion von ArchiCrypt Forensik-Tool Miniaturansichten[174] wird automatisch mit ArchiCrypt Shredder installiert.

Mit Klick auf "**Welche Bilder hat das System heimlich gesammelt?**" ③ können Sie das Forensik-Modul aufrufen und so prüfen, ob Windows hier überhaupt Daten ablegt.

Gerne können Sie die Pro Version erwerben[175] und das Forensik Modul erweitern.

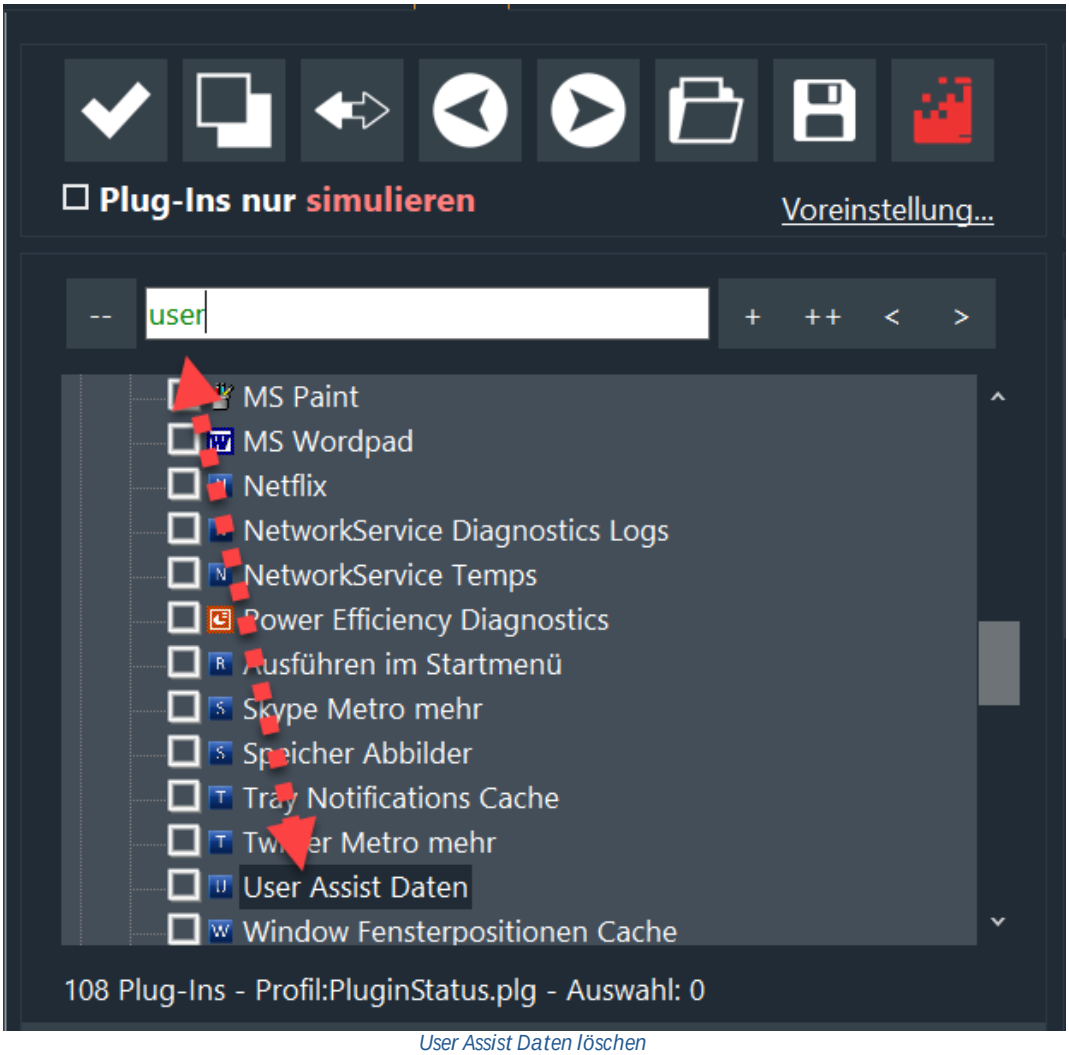
Mit **Deaktiviere Miniaturansichten** (2) können Sie Windows so anpassen, dass keine Vorschaubilder mehr erstellt und in einer Datenbank abgelegt werden.

Mithilfe des *Plug-Ins Miniaturbilder* Sie können die Datenbanken mit den Miniaturbildern leeren. Der Speicherplatz wird freigegeben und die Bilder werden aus den Datenbanken entfernt. Windows beginnt, so Sie nicht das Erstellen der Miniaturansichten deaktiviert[109] haben, beim Betrachten von Dateien, die Datenbank neu zu füllen.

ACHTUNG: *Das Plug-In Miniaturbilder steht, wie verschiedene andere Plug-Ins, nur in der Vollversion des Shredders zur Verfügung! Zusätzlich muss es sich um* Windows 10 *handeln.*

User-Assist Daten - Welche Anwendungen verwenden Sie?

Fest in ArchiCrypt Shredder integriert ist die Funktion **Welche Anwendungen verwenden Sie?** (1). Hier können Sie sich die Daten auflisten lassen, die das Betriebssystem seit der Installation über Ihr Nutzerverhalten (*Telemetrie-Daten*) gesammelt hat. Um diese Daten von Ihrem System zu entfernen, können Sie das entsprechende Plug-In (*User Assist Daten*) in der Kategorie *System* ausführen.



User Assist Daten löschen

ACHTUNG: *Das Plug-In User Assist Daten löschen steht wie verschiedene andere Plug-Ins nur in der Vollversion zur Verfügung!*

8.11 Systemfehler finden und beseitigen

Im Laufe der Zeit schleichen sich auf einem Rechner immer mehr Fehler ein. Das Installieren und Entfernen von Programmen sorgt für ungültige Einträge in der lebenswichtigen Registrierdatenbank (*Registry; Registrierungsdatenbank*) von Windows.

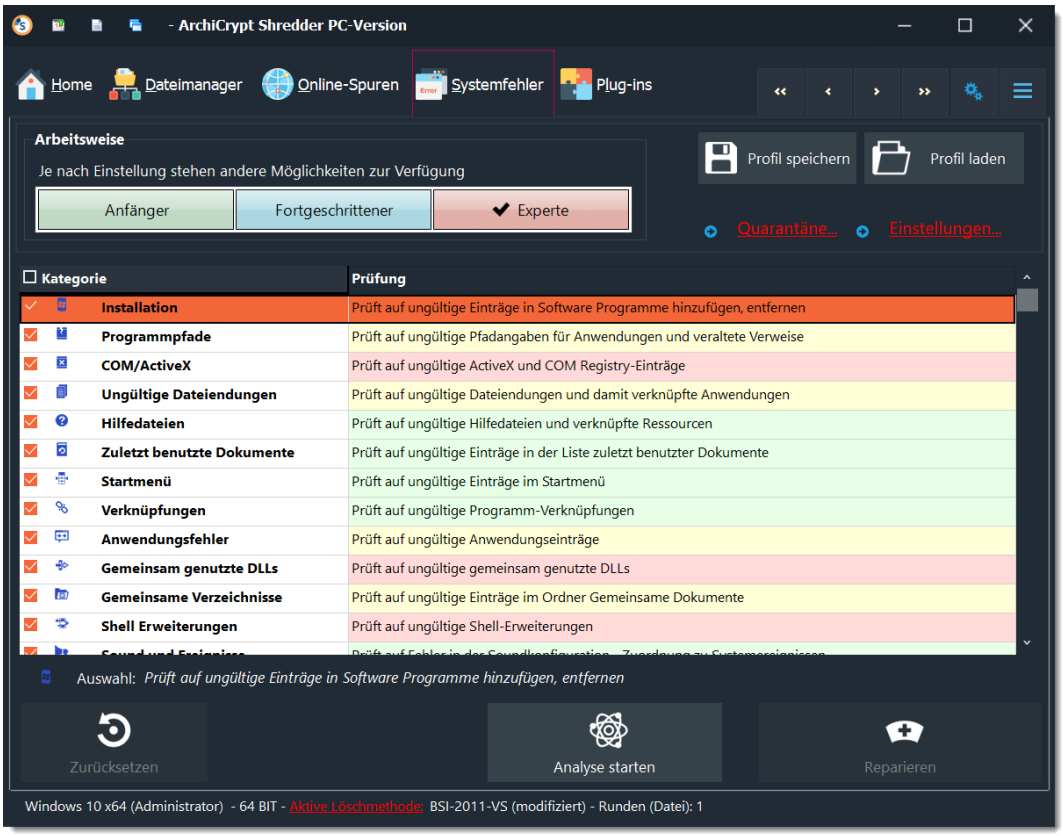
Ungültige Verweise auf Dateien, fehlerhafte und inkonsistente Werte und unnötige Reste führen dazu, dass der Rechner ständig nach nicht vorhandenen Daten und Verweisen sucht und so mit der Zeit träge und

instabil wird. Bei schwerwiegenderen Problemen tauchen störende Fehlermeldungen auf oder das System funktioniert nicht mehr korrekt.

Lange Wartezeiten, Fehlermeldungen und Abstürze sind die Folge.

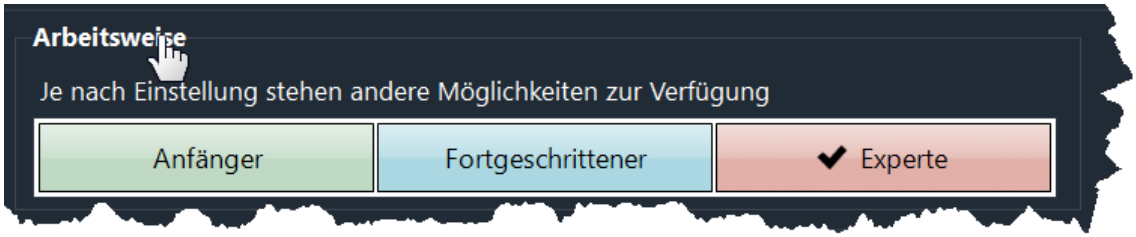
ArchiCrypt Shredder unterteilt die Analysefunktionen in Kategorien für Anfänger, Fortgeschrittene und Experten. Unstimmigkeiten und Fehler werden aufgespürt und können in den meisten Fällen automatisch korrigiert werden.

Sollten durch das *Beseitigen der System-Fehler* Probleme auftreten, kann man Änderungen aus einer Quarantäne[203] heraus rückgängig machen und den ursprünglichen Zustand des Systems wieder herstellen.



Systemfehler aufspüren und reparieren

Die Betriebsmodi der Fehleranalyse



Klicken Sie auf den gewünschten Betriebsmodus, um Kategorien für die Analyse auszuwählen. Die den Modi zugehörigen Einträge in der Tabelle sind farblich markiert.

Grüne Einträge gehören zum Modus *Anfänger*, gelbe Einträge zum Modus *Fortgeschrittener* und rote Einträge zum *Expertenmodus*.

Der Modus für Anfänger

Wählt nur solche Punkte für die Analyse aus, die sich in ihrer Auswirkung auf das System nahezu nicht auswirken. Fehler die hier auftreten, sorgen im Höchstfalle für eine Fehlermeldung in der Art, dass ggf. eine bestimmte Datei nicht gefunden wurde.

Im Anfängermodus können Sie ausschließlich Einträge in der Tabelle anwählen, die grün hinterlegt sind.

Der Modus für Fortgeschrittene

Wählt nur solche Punkte für die Analyse aus, die sich in ihrer Auswirkung auf das System merklich auswirken. Hier analysierte Fehler sorgen im Allgemeinen dafür, dass Anwendungen auch dann nicht mehr korrekt funktionieren, wenn sie neu installiert werden.

Im Fortgeschrittenenmodus können Sie ausschließlich Einträge in der Tabelle anwählen, die grün oder gelb hinterlegt sind.

Der Modus für Experten

Im Expertenmodus können Sie frei festlegen, welche Punkte bei der Analyse berücksichtigt werden sollen. Auch die rot markierten Einträge in der Tabelle sind jetzt aktivierbar. Solche Einträge wirken sich erheblich auf die Stabilität und Zuverlässigkeit von Anwendungen und Betriebssystem aus. Hier gefundene Fehler können dazu führen, dass ein

Rechner öfter abstürzt, träge reagiert und sehr lange zum Starten benötigt.

Im Expertenmodus können Sie *beliebige Einträge* in der Tabelle anwählen.

Beschreibung der Kategorien für die Fehleranalyse

- Installation:
  Untersucht wird, ob Informationen über installierte Programme korrekt sind. Oft gibt es hier Einträge, die auf nicht mehr vorhandene Deinstallationsprogramme verweisen. Diese Einträge funktionieren nicht mehr und sollten entfernt werden.
- Programmpfade:
  Untersucht, ob Werte in der Registry enthalten sind, die auf nicht mehr vorhandene Verzeichnisse verweisen.
- COM/ActiveX:
  Es wird untersucht ob die s.g. COM/ActiveX Objekteinträge in Ihrem System fehlerfrei sind. Bei diesen Objekten handelt es sich um Bausteine mit Funktionen, auf die bestimmte Anwendungen zugreifen. Sind hier Fehler vorhanden, kann dies dazu führen, dass bestimmte Anwendungen nicht mehr funktionieren oder oft abstürzen.
- Ungültige Dateiendungen:
  Es wird untersucht, ob auf Ihrem System Dateiendungen mit Anwendungen verknüpft sind, die sich nicht mehr auf Ihrem System befinden.
- Hilfedateien:
  Es wird untersucht, ob in der Registry Hilfedateien aufgeführt sind, die sich nicht mehr auf dem System befinden.
- Zuletzt benutzte Dokumente:
  Überprüft, ob unter den zuletzt benutzten Dokumenten Einträge vorhanden sind, die auf nicht mehr vorhandene Dateien verweisen.
- Startmenü:
  Untersucht, ob in Ihrem Startmenü auf Programme oder Ordner verwiesen wird, die sich nicht mehr auf Ihrem System befinden.

- Verknüpfungen:
  Überprüft ob Verknüpfungen auf Programme, Dateien oder Ordner verweisen, die sich nicht mehr auf Ihrem System befinden. (siehe auch Einstellungen - Verknüpfungen Einstellungen 202)
- Anwendungsfehler:
  Prüft, ob die Einträge von Anwendungsprogrammen in die Windows Registrierdatenbank Fehlerhaft sind.
- Gemeinsam genutzte DLLs:
  Untersucht, ob Dateien, die für mehrere Anwendungen vorgesehen sind, noch vorhanden sind.
- Gemeinsame Verzeichnisse:
  Untersucht, ob der Ordner gemeinsam genutzte Dokumente ungültige Einträge enthält.
- Shell Erweiterungen:
  Prüft, ob die Registry Verweise auf nicht mehr vorhandene Shell Erweiterungen enthält.
- Sound und Ereignisse:
  Untersucht, ob Systemereignissen oder Anwendungen Klangdateien zugeordnet sind, die nicht mehr auf Ihrem System sind.
- Autostart Programme:
  Untersucht, ob nicht mehr vorhandene Programme als Autostart (sollen beim Starten des Systems geladen werden) eingetragen sind.
- Windows Schriftarten:
  Überprüft, ob auf Ihrem System Schriftarten registriert sind, die nicht mehr vorhanden sind.
- Windows Firewall
  Prüft ob der in Windows integrierte Firewall fehlerhafte Einträge enthält. Dabei handelt es sich um Einträge, die sich auf nicht mehr installierte Software bezieht.
- Browser Hilfsobjekte
  Browser Hilfsobjekte sind zusätzliche Module, die mit älteren Versionen des Microsoft Internet Explorer geladen werden. Fehler die in diesem Bereich auftreten, machen den Browser zumeist völlig instabil. Der Browser lässt sich nicht mehr starten oder stürzt häufig ab.
- Dienste
  Treiber und so genannte Dienst die in der Windows Registry verwaiste

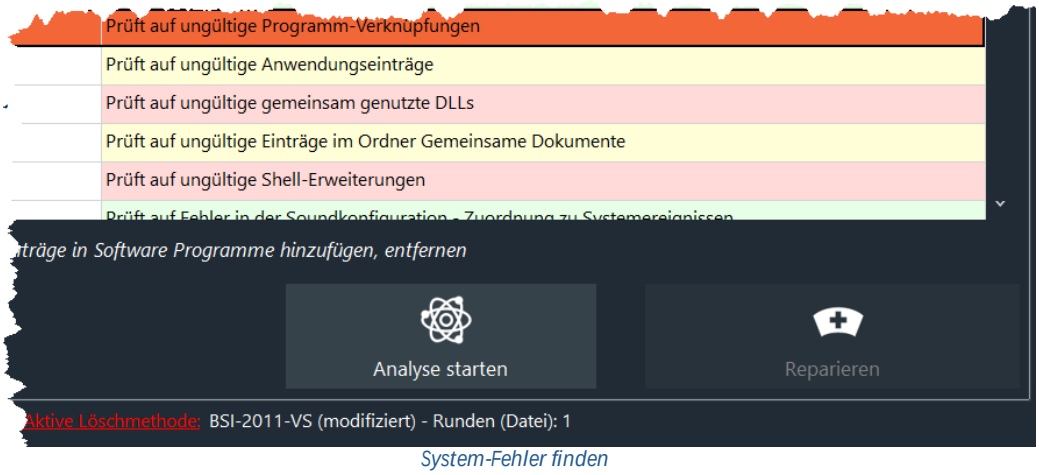
Einträge hinterlassen, machen mindestens den Start des Systems träge, können jedoch auch den Betrieb instabil machen.

So starten Sie die Fehleranalyse

Wählen Sie die zu analysierenden Fehlerquellen in der Tabelle aus und sorgen Sie unbedingt dafür, dass der Virenscanner für die Zeit der Analyse deaktiviert ist.

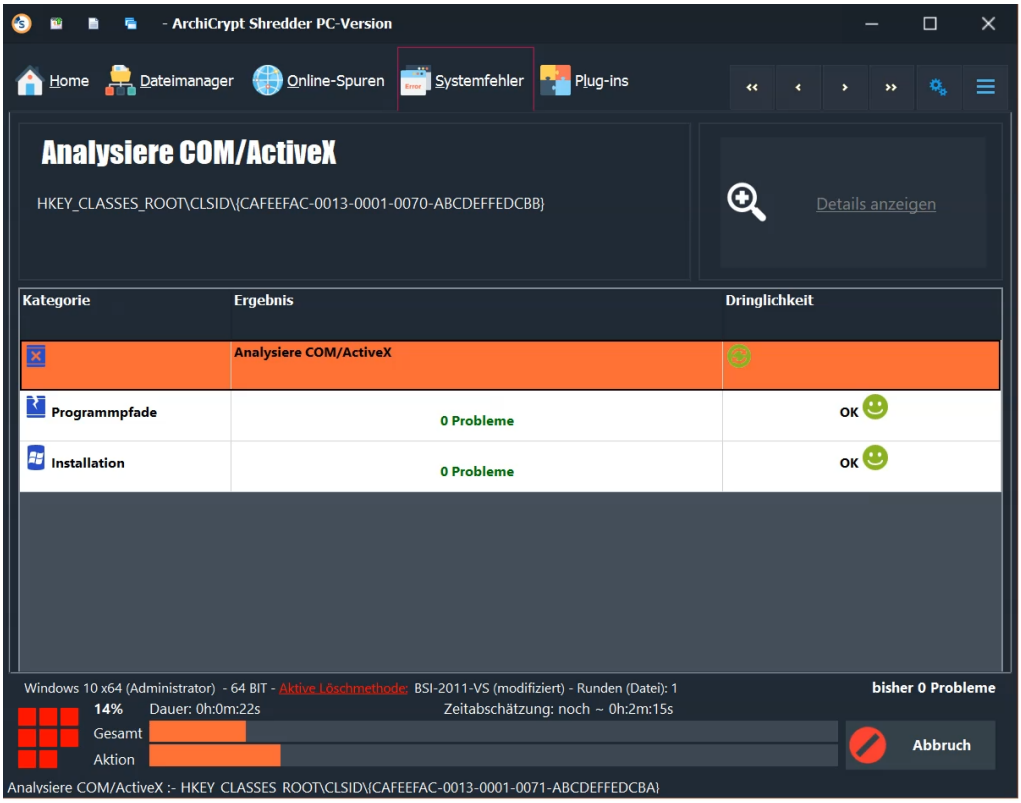
WARNUNG: *Nicht gleich alle Kategorien auswählen*. Starten Sie mit dem *Anfängermodus*, führen Sie dann den *Fortgeschrittenenmodus* aus und anschließend Schritt für Schritt die einzelnen Kategorien im *Expertenmodus*. Warum Sie dies tun sollten, wird hier erklärt 122 .

Klicken Sie dann auf die Schaltfläche Analyse starten.



System-Fehler finden

Die Ansicht schaltet jetzt um. Sie sehen den Fortschritt und die Ergebnisse bei der Analyse der von Ihnen ausgewählten Punkte.

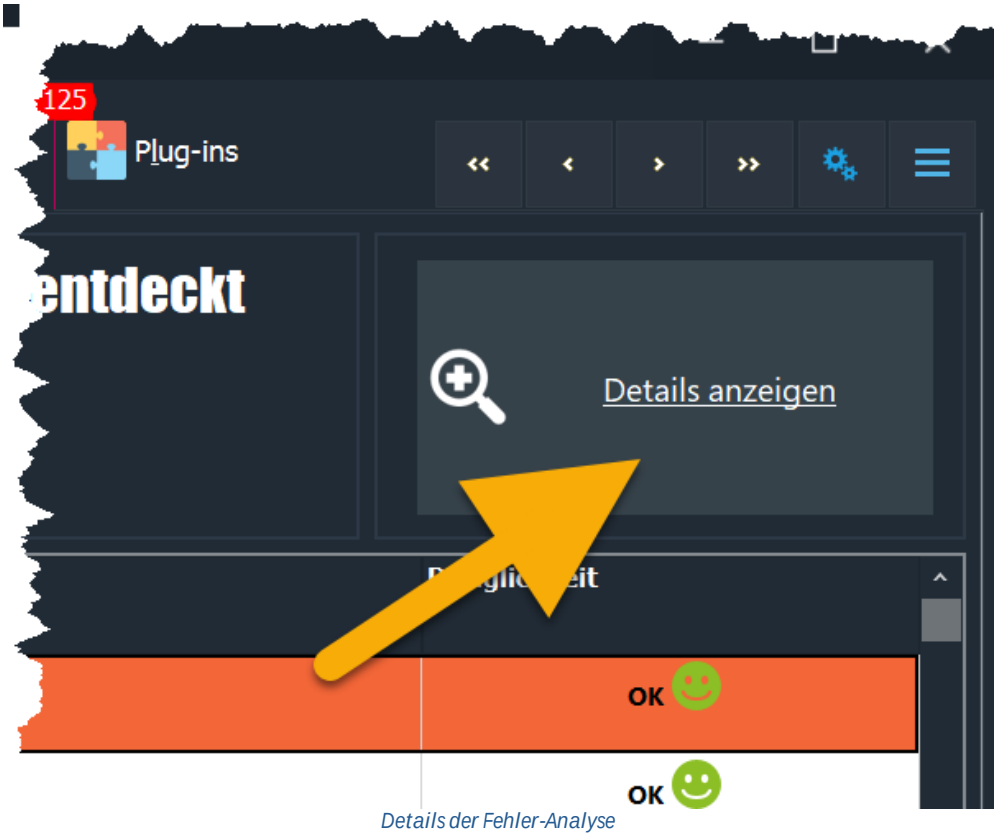


Sobald die Analyse abgeschlossen ist, können Sie die gefundenen Fehler durch einen Klick auf Reparieren beseitigen lassen. Durch diese Aktion werden ALLE gefundenen Fehler beseitigt. Besser ist es, sich die *Details der Analyse* einmal anzusehen. In der Detailansicht[116] kann man einzelne Fehler reparieren oder gezielt von einer Reparatur ausschließen.

So sehen Sie sich Details zu einer Fehleranalyse an

Sobald die Analyse abgeschlossen ist, gelangen Sie

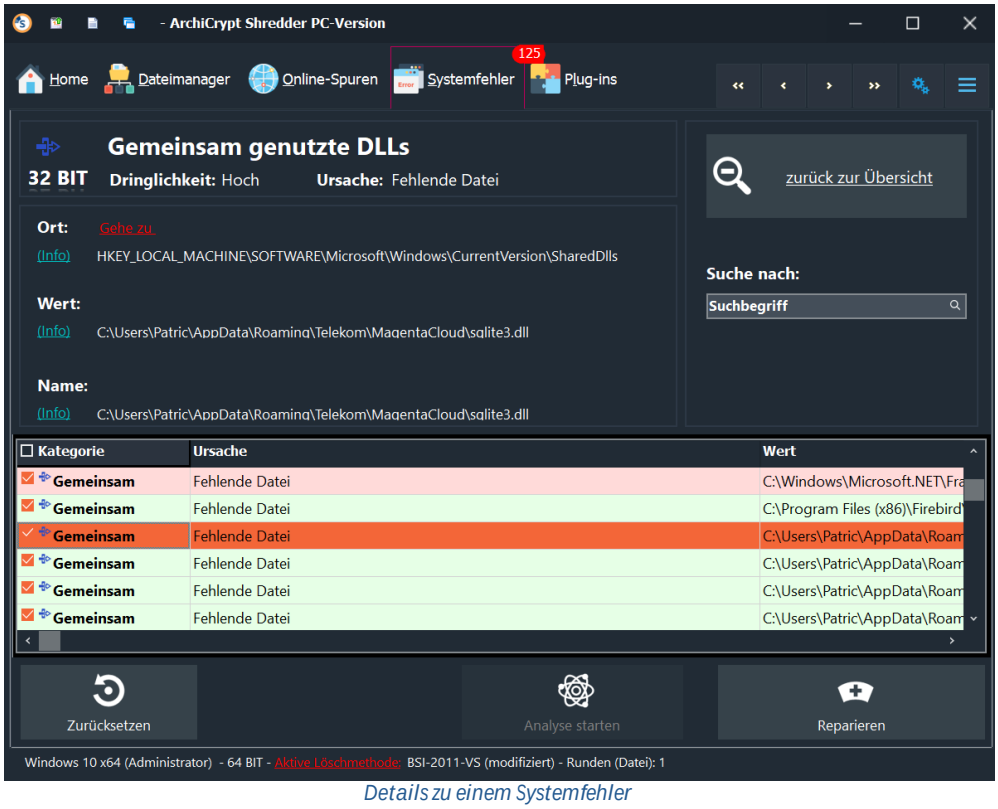
1. durch Klick auf die Schaltfläche Details anzeigen zu einer detaillierten Übersicht.



Details der Fehler-Analyse

In dieser Übersicht werden *ALLE gefundenen Fehler* der ausgewählten Kategorien angezeigt.

2. durch Klick auf eine Zeile in der Tabelle zu den Details, die sich auf diese einzelne Kategorie beziehen.

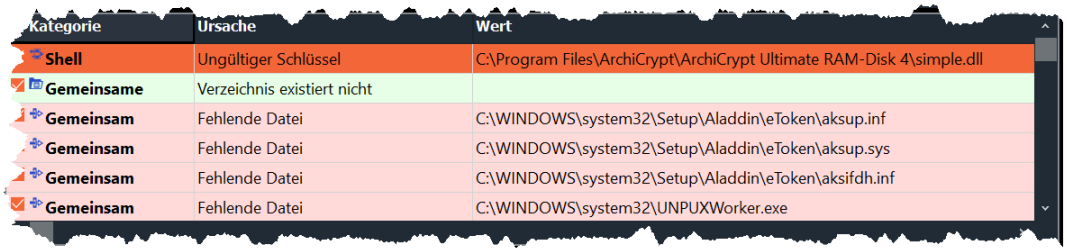


Details zu einem Systemfehler

Von der Detailansicht selbst gelangen Sie zurück zur Übersicht, indem Sie auf die Schaltfläche zurück zur Übersicht klicken.

So interpretieren Sie die Detailansicht

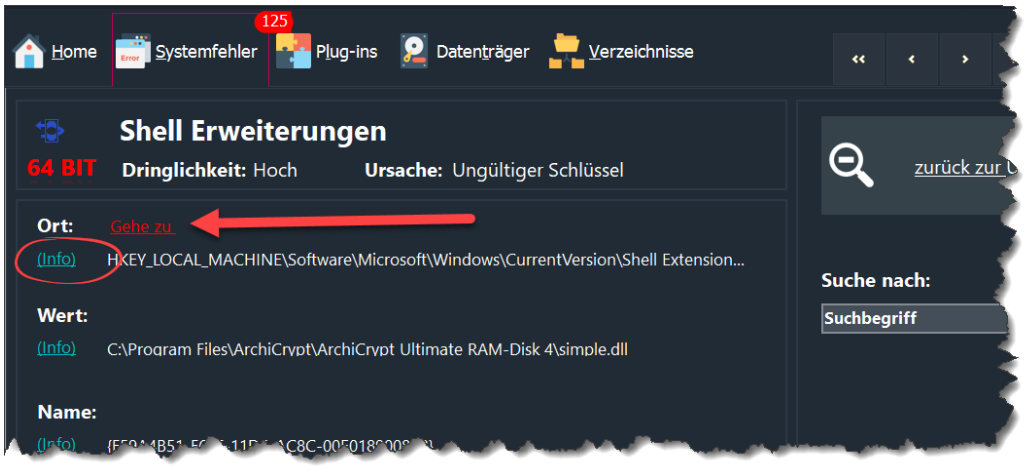
In der Detailansicht werden Ihnen die gefundenen Fehler in einer Tabelle angezeigt. Auf 64 BIT Systemen wird zwischen Fehlern unterschieden, die sich auf 32 BIT und auf 64 BIT Programme beziehen. Einträge mit Bezug zu 32 BIT Programmen sind grün hinterlegt, solche mit Bezug zu 64 BIT Programmen rot.



Kategorie	Ursache	Wert
Shell	Ungültiger Schlüssel	C:\Program Files\ArchiCrypt\ArchiCrypt Ultimate RAM-Disk 4\simple.dll
Gemeinsame	Verzeichnis existiert nicht	
Gemeinsam	Fehlende Datei	C:\WINDOWS\system32\Setup\Aladdin\eToken\aksup.inf
Gemeinsam	Fehlende Datei	C:\WINDOWS\system32\Setup\Aladdin\eToken\aksup.sys
Gemeinsam	Fehlende Datei	C:\WINDOWS\system32\Setup\Aladdin\eToken\aksifdh.inf
Gemeinsam	Fehlende Datei	C:\WINDOWS\system32\UNPUXWorker.exe

Interpretation der System-Fehler

Wenn Sie einen Eintrag in der Tabelle auswählen, wird Ihnen angezeigt, welche Dringlichkeit die Beseitigung des Fehlers hat, was die Ursache für die Meldung des Fehlers hat, an welchem Ort der Fehler gefunden wurde und welchen Wert der gefundene Fehler hat.



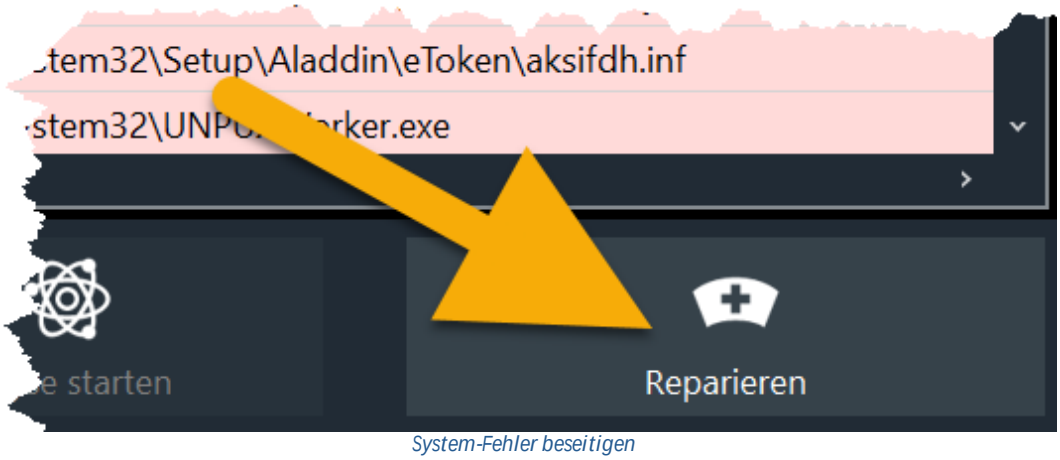
Informationen über System-Fehler im Internet suchen

Durch Klick auf Info wird eine *Internetsuche* zu dem entsprechenden Wert durchgeführt. Meist erhält man bereits mit den ersten Suchergebnissen wertvolle weitere Hinweise. Mit Gehe zu kann man direkt den Registry Editor von Windows aufrufen bzw., wenn die Ursache eine Datei/ein Pfad war, den Windows Explorer starten.

Wenn Sie mit der rechten Maustaste auf eine Zeile in der Tabelle klicken, wird ein Kontextmenü angezeigt. Wenn Sie sich bei einem aufgeführten Problem unsicher sind, nehmen Sie das Häkchen weg oder rufen Sie im Kontextmenü den Punkt Problem künftig ignorieren auf.

Kontextmenü System-Fehler

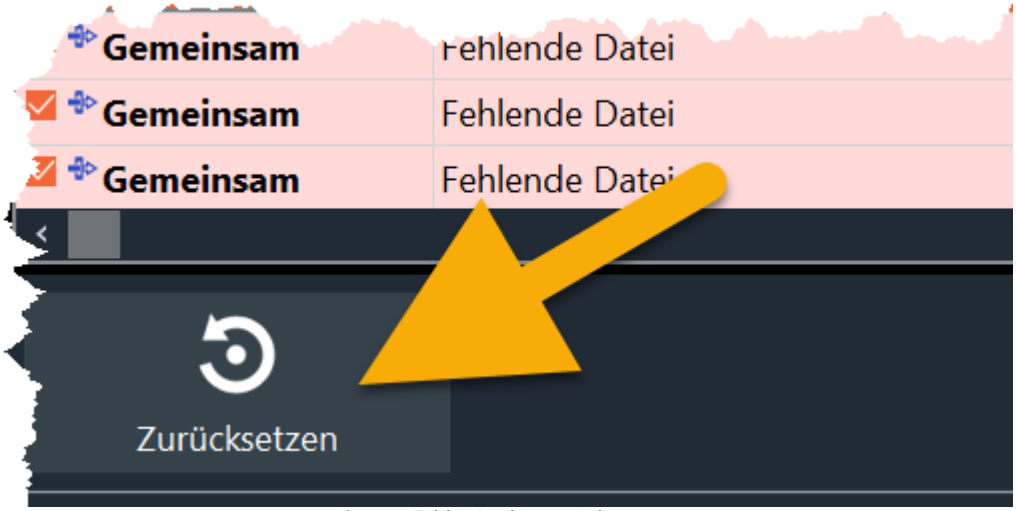
In der Detailansicht können Sie einzelne Fehler gezielt von einer Reparatur ausschließen, indem Sie das entsprechende *Häkchen entfernen*. Die Schaltfläche **Reparieren** enthält auch den Hinweis, dass nur die ausgewählten Fehler beseitigt werden.



System-Fehler beseitigen

Zurücksetzen der aktuellen Fehleranalyse

Möchten Sie das Ergebnis einer Suche zurücksetzen, betätigen Sie bitte die Schaltfläche Zurücksetzen. Alle Suchergebnisse werden gelöscht, Sie gelangen zurück zur Auswahl der Kategorien für die nächste Analyse.

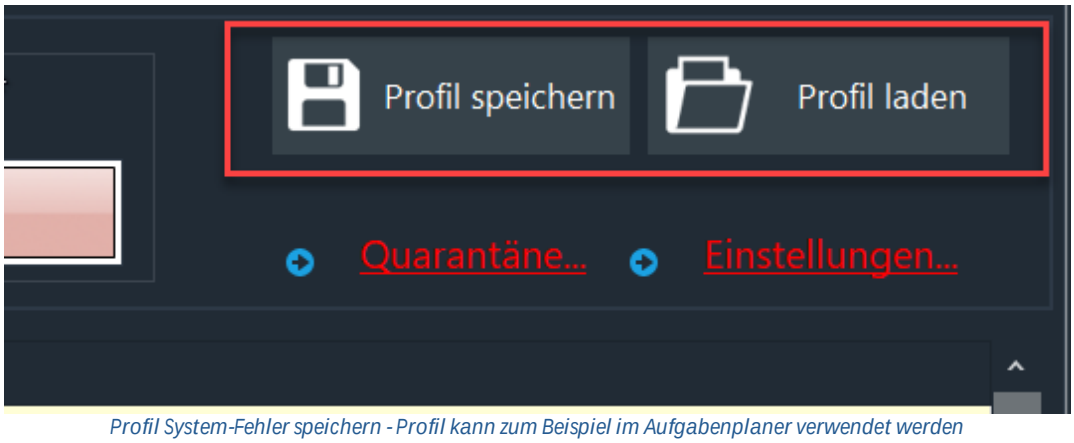


System-Fehler Analyse zurücksetzen

So speichern und laden Sie Profile für die Systemfehler-Bereinigung

Insbesondere dann, wenn Sie zeitgesteuert bestimmte Aufgaben ausführen lassen möchten oder 1-Klick Aufgaben[153] erstellen möchten, ist es angebracht, die zu untersuchenden Kategorien als Profil zu speichern. Dieses gespeicherte Profil können Sie bei Bedarf wieder laden oder im Aufgabenplaner[142] als Vorgabe für eine 1-Klick Aufgabe oder eine zeitgesteuerte Aufgabe nutzen.

Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie bitte auf die Schaltfläche Profil speichern. Wenn Sie ein Profil laden möchten, klicken Sie auf Profil laden.



Profil System-Fehler speichern - Profil kann zum Beispiel im Aufgabenplaner verwendet werden

Warum es zu Fehlern kommen kann, obwohl man doch Fehler reparieren möchte!

Microsoft hat diverse Standards festgelegt, an die sich Hersteller von Anwendungssoftware halten sollten. Diese Standards fließen in die Regeln ein, mit denen ArchiCrypt Shredder's Fehleranalyse arbeitet.

Immer wieder gibt es aber Hersteller, die sich nicht an die Vorgaben halten. Dadurch kann es dazu kommen, dass ArchiCrypt Shredder solche *Nicht-Standardeinträge* als Fehler erkennt und bei der vermeintlichen Korrektur löscht. Will man jetzt die entsprechende Anwendung starten, fehlt der Eintrag und ein Fehler tritt auf.

HINWEIS: ArchiCrypt Shredder verzichtet ganz bewusst darauf, jedes *minimale Abweichen* von Standards als Fehler zu interpretieren. Die Anzahl der gefundenen "Fehler" ist daher unter Umständen geringer, als bei anderen spezialisierten *Reinigungsprogrammen*. Allerdings kommt es durch diese "Zurückhaltung" nur in extrem seltenen Fällen zu Folgeproblemen nach einer vermeintlichen Fehlerkorrektur.

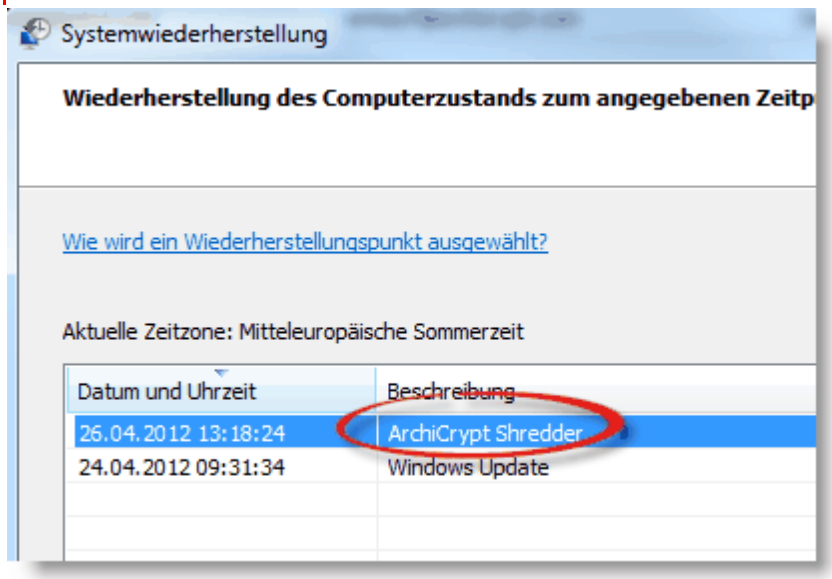
Hinweis: Es kann durchaus vorkommen, dass nach einer Bereinigung bei einer Analyse erneut Fehler angezeigt werden. Dies ist nicht außergewöhnlich! Die Beseitigung des einen Fehlers kann andere Unstimmigkeiten nach sich ziehen. Führen Sie in diesen Fällen die Reparatur so oft durch, bis möglichst keine Fehler mehr angezeigt werden.

Was tun, wenn Sie nach der Reparatur feststellen, dass Anwendungen nicht mehr korrekt funktionieren?

ArchiCrypt Shredder baut zwei Sicherungen ein, auf die Sie im Fehlerfall zurückgreifen können.

1. Windows bietet s.g. Wiederherstellungspunkte an, mit denen man den Zustand des Systems wieder auf den entsprechenden Zeitpunkt zurücksetzen kann. Bei jedem Start des Shredders wird ein solcher Wiederherstellungspunkt erzeugt, wenn Sie die *Reparaturfunktion* aufrufen. Diese Wiederherstellungspunkte erkennen Sie in der Windows Übersicht an der Bezeichnung *ArchiCrypt Shredder*.

   Sie müssen die Systemwiederherstellung in Windows aktiviert haben!



2. ArchiCrypt Shredder sichert jeden Wert bevor er gelöscht wird in der s.g. Quarantäne der Fehlersuche[203] .

   In der Quarantäne können Sie jede Änderung zurücknehmen und so den Zustand vor der Fehlerbeseitigung wieder herstellen.

WICHTIG: Gehen Sie beim *Wiederherstellen* vom *neusten Eintrag zum ältesten* Eintrag vor.

Änderungen können mittels Quarantäne zurückgenommen werden

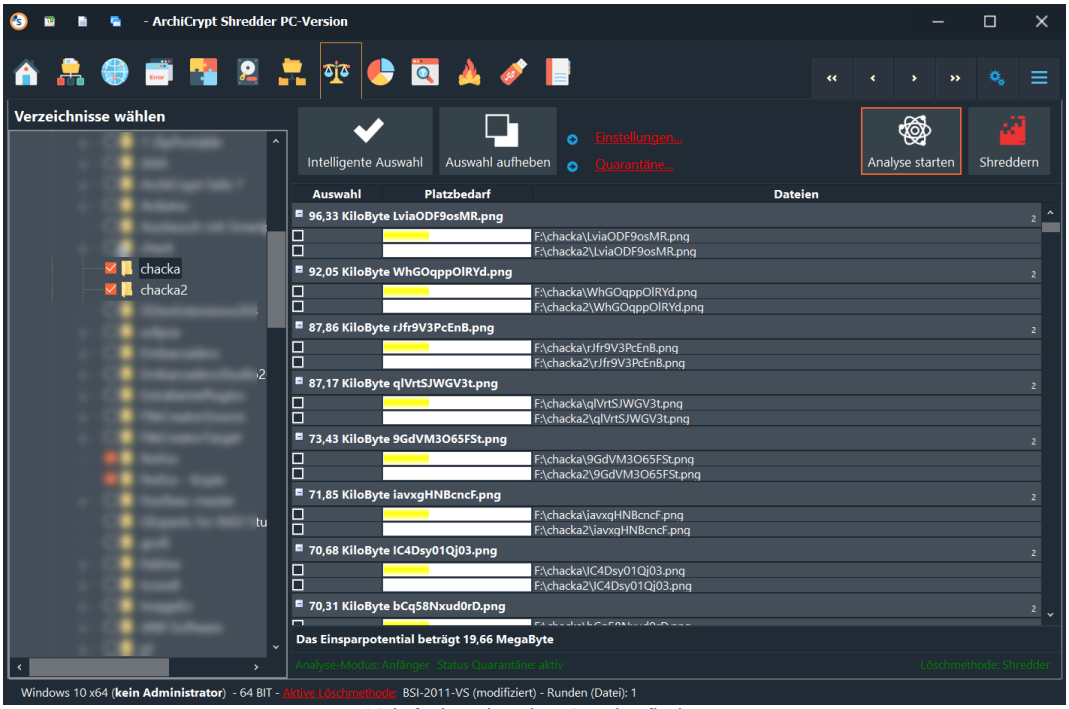
8.12 Duplikat Finder

8.12.1 Duplikate finden und beseitigen

Duplikat Finder - Mehrfach vorhandene Dateien finden und beseitigen

Mit der Zeit sammeln sich auf einem Windows System immer mehr Dateien an. Da kommt es nicht selten vor, dass Dateien plötzlich mehrfach vorhanden sind. Duplikate sind meist überflüssig und belegen unnötig Platz.

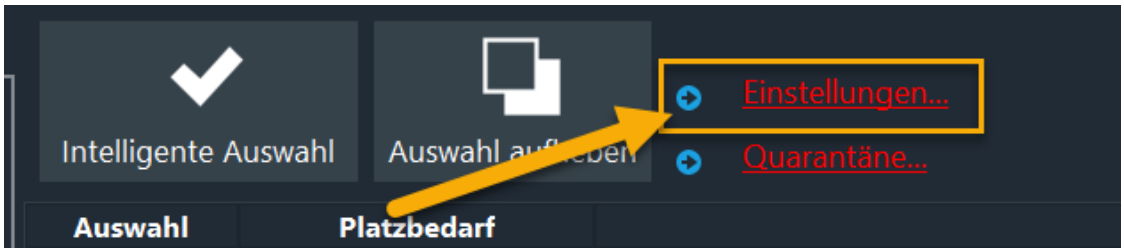
ArchiCrypt Shredder spürt diese mehrfach vorhandenen Dateien auf und unterstützt Sie dabei, die richtige Datei zu löschen. Duplikate werden auf Wunsch zunächst in einer Quarantäne[129] zwischengespeichert und können von dort bei Bedarf wieder zurückgespielt werden.



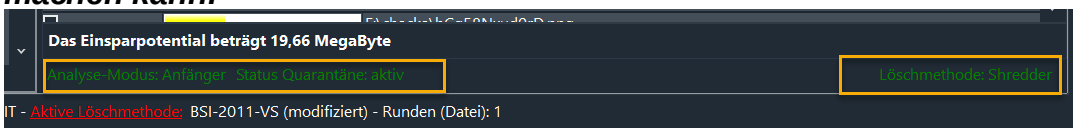
Mehrfach vorhandene Dateien finden

So finden Sie mehrfach vorhandene Dateien

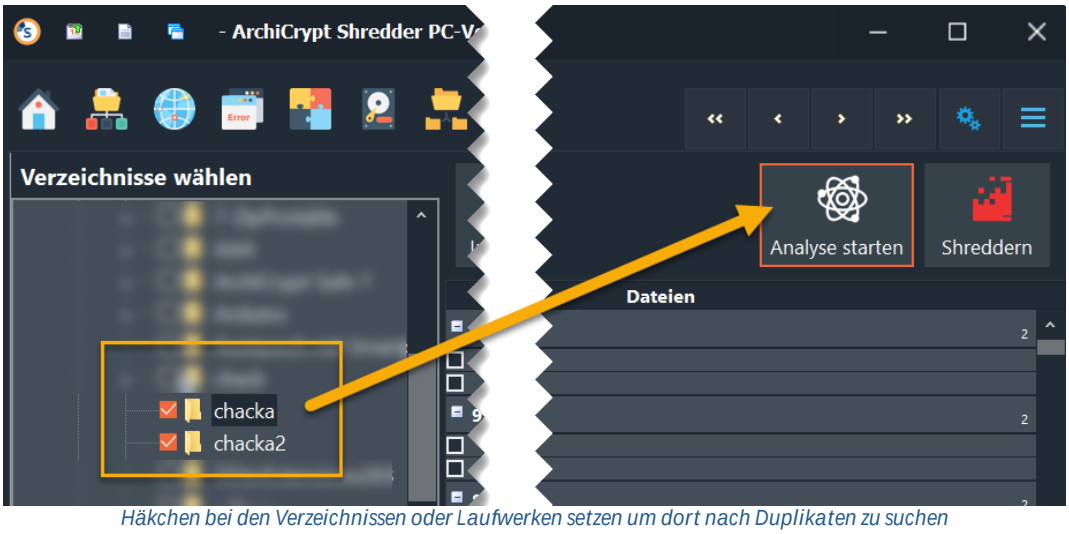
Der Duplikat Finder kennt einen *Anfänger-*, *Fortgeschrittenen-*, *Profi-* und *nutzerdefinierten* Analyse-Modus. Den Analyse-Modus können Sie in den Einstellungen-Duplikat Finder[190] ändern.



Anm.: ***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.



Häkchen bei den Verzeichnissen oder Laufwerken setzen um dort nach Duplikaten zu suchen

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 *potenziellen 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 inhaltlich identisch sind, jedoch anders benannt wurden.

Welche Datei soll ich löschen?

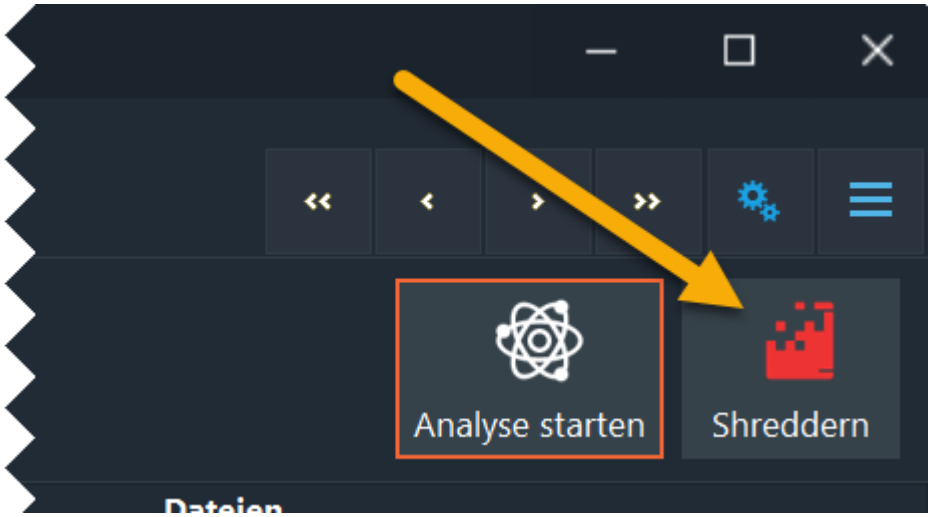
Es ist nicht einfach, zu entscheiden, welche der Dateien man löschen soll. Bei Datendateien wie z.B. Word- und Grafik-Dokumenten ist dies noch relativ leicht. Sie selbst wissen, wie Sie die Daten auf Ihrer Festplatte organisiert haben.

Schwieriger wird es bei ausgewähltem Experten-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 aktivieren190. Hier können Sie die Duplikate notfalls wieder zurückspielen129. **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.

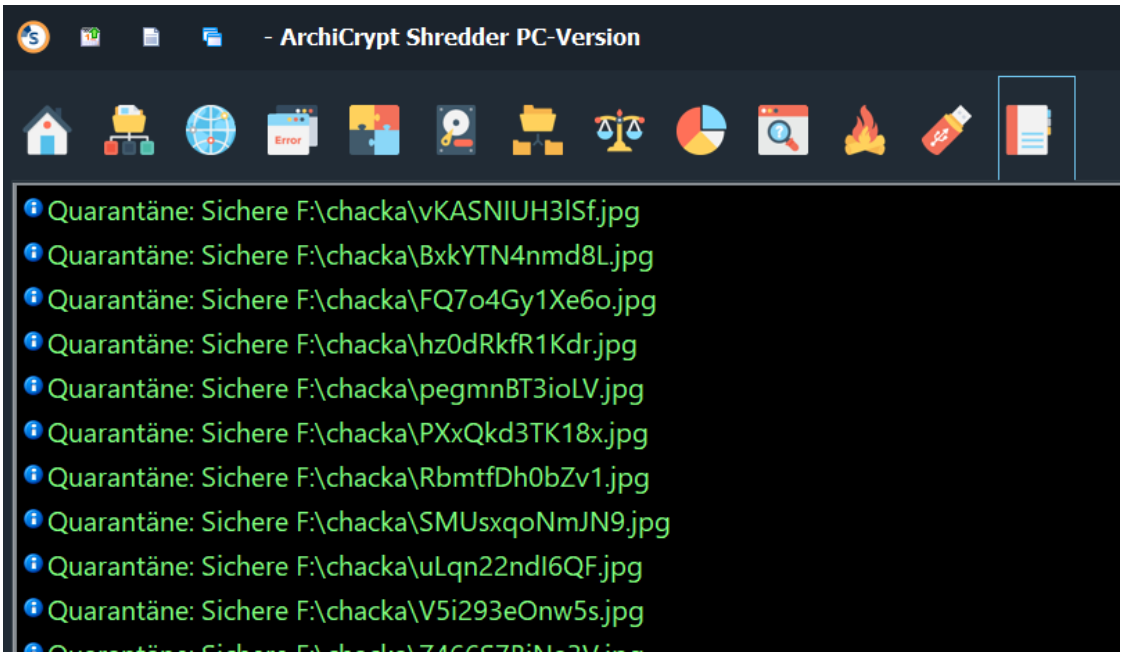


Ob die Dateien sicher gelöscht werden (*Löschmethode Shredder*) oder aber mit Systemmitteln (*Löschmethode System*) können Sie in den

Einstellungen[190] festlegen. Die Dateien werden bei aktivierter Quarantäne[129] zunächst als Kopie dort abgelegt und erst dann gelöscht.

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

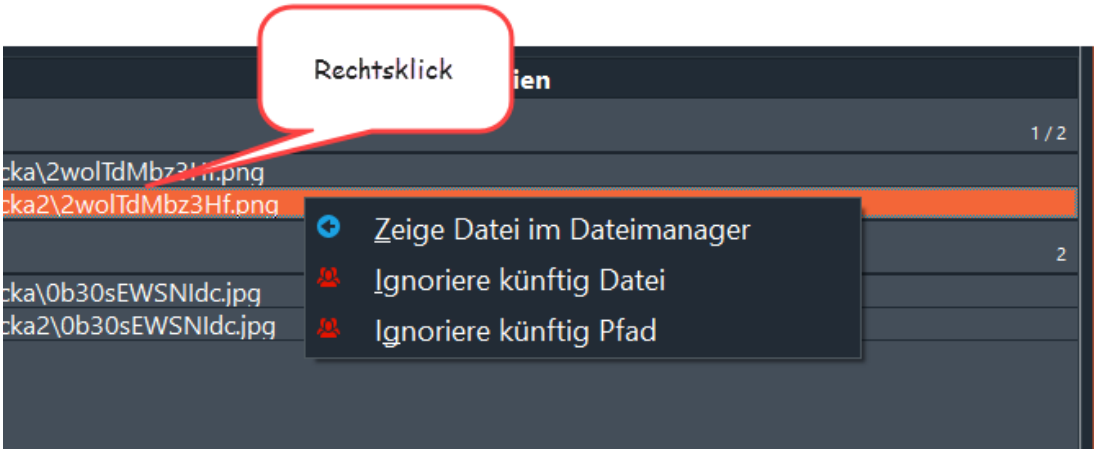
Insbesondere der Analyse Modus *Experte*, ggf. auch der *nutzerdefinierte Modus*, meldet auch doppelt vorhandene Anwendungen, Systembibliotheken, Treiber etc. Hier kann es vorkommen, dass genau die Datei (*das Duplikat*) an der falschen Stelle gelöscht wurde. Falls Sie, wie empfohlen und voreingestellt, die Quarantäne[129] 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[190] 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 190 manuell Objekte hinzufügen.



siehe auch: Quarantäne für Duplikate... 129

8.12.2 Quarantäne für Duplikate

Quarantäne für gelöschte Duplikate

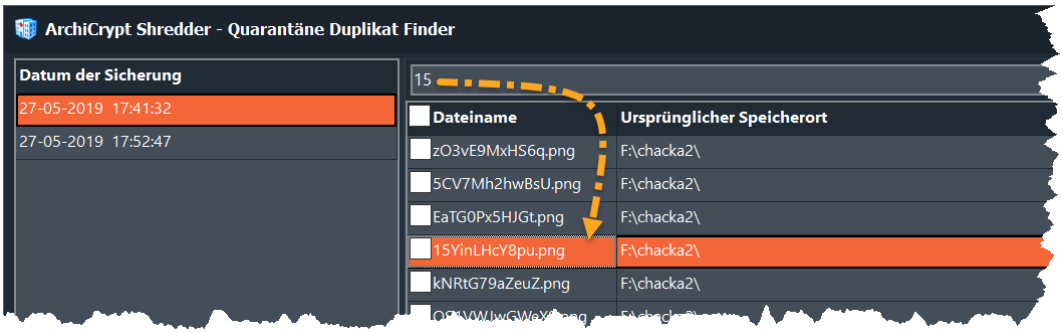
Die Quarantäne bietet Ihnen eine bequeme Möglichkeit, Dateien die Sie versehentlich mit dem Duplikat Finder von Ihrem System entfernt haben, wieder herzustellen.

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.



Dateien in der Duplikat Quarantäne suchen

So finden Sie eine bestimmte Datei in der Quarantäne

Geben Sie den Dateinamen oder einen Teil davon in das Eingabefeld Suchbegriff ein und betätigen Sie die Eingabe Taste.

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[190] 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[190] festlegen, dass Einträge nach einer bestimmten Zeit *automatisch aus der Quarantäne* entfernt werden.

siehe auch: Duplikate finden und beseitigen 124

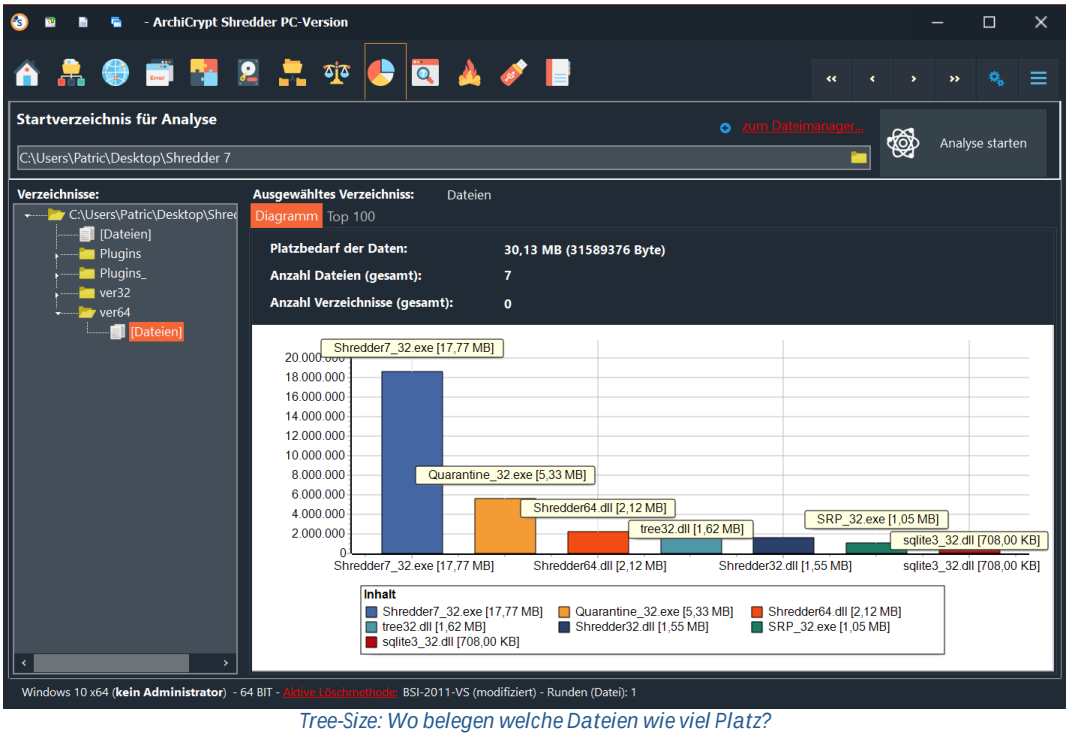
8.13 Laufwerksbelegung - Die größten Dateien finden

Wo ist der wertvolle Speicherplatz geblieben?

Jeder kennt das Problem! Ganz egal wie groß ein Datenträger ist, er kommt früher oder später an seine Grenzen.

Und gerade bei großen Laufwerken ist es nicht leicht, die Dateien zu finden, die den meisten Speicherplatz belegen.

Lassen Sie ArchiCrypt Shredder Ihre *Laufwerke analysieren* und die wahren Platzfresser aufspüren. Sowohl grafisch als auch in einer TOP 100 136 Liste finden Sie die Dateien und Ordner, die den meisten Platz belegen.

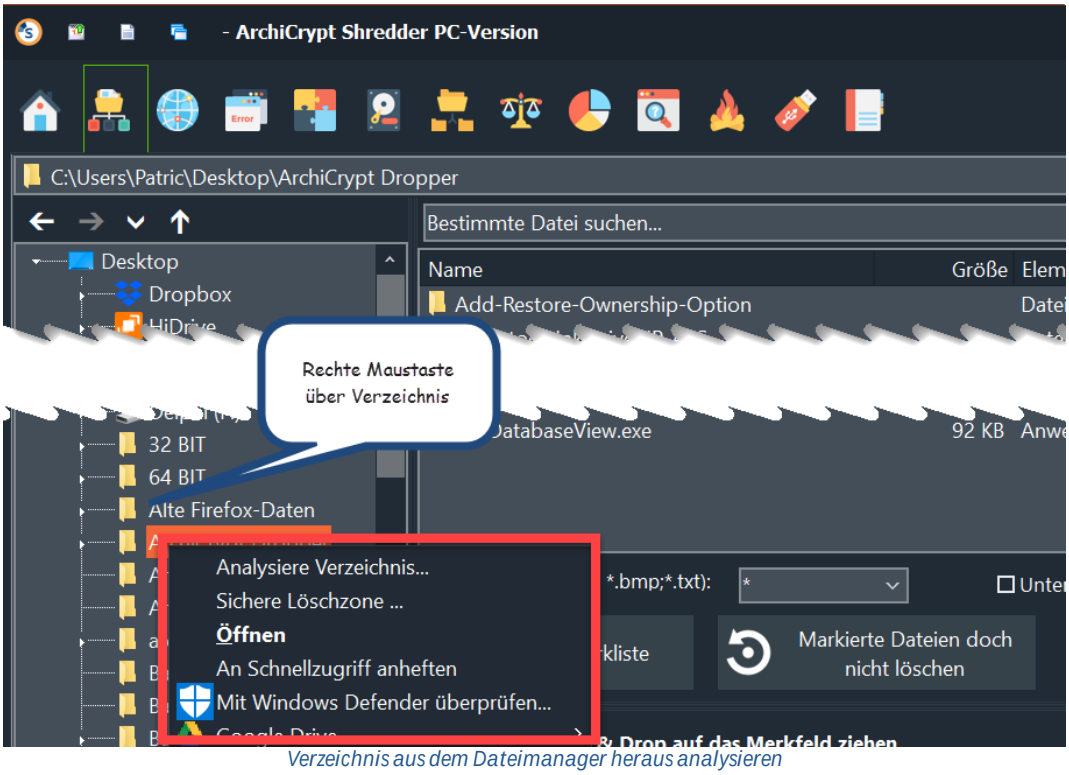


Tree-Size: Wo belegen welche Dateien wie viel Platz?

So finden Sie die Dateien, die den meisten Platz belegen

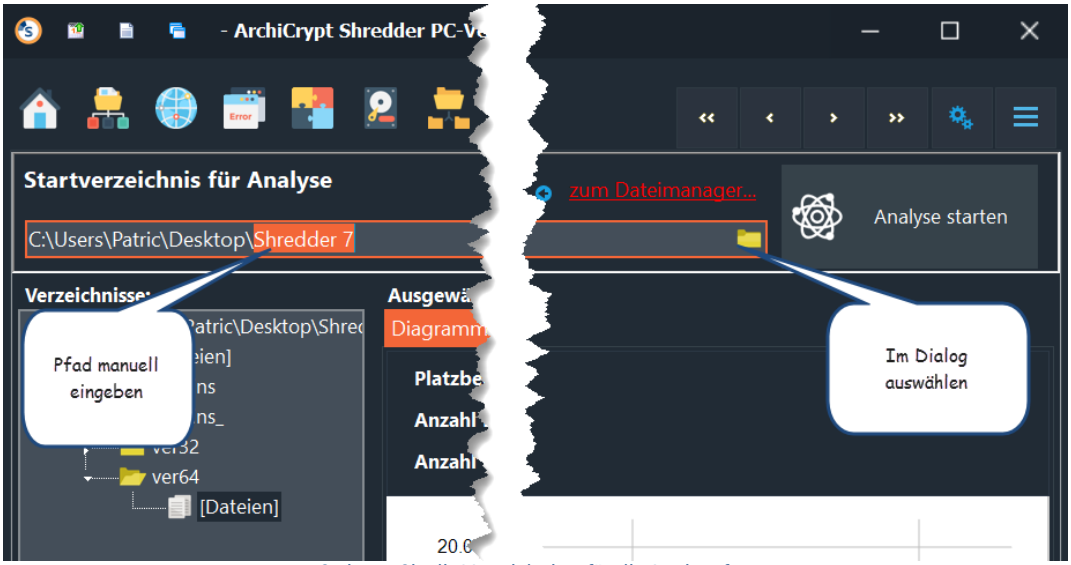
Um ein Laufwerk oder ein Verzeichnis zu analysieren haben Sie zwei Möglichkeiten:

1. Rufen Sie im Dateimanager[51] des Shredders das *Kontextmenü* eines beliebigen Verzeichnisses oder Laufwerks auf (mit rechter Maustaste anklicken). Wählen Sie den Eintrag Analysiere Verzeichnis... Die Analyse startet sofort.



Verzeichnis aus dem Dateimanager heraus analysieren

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.



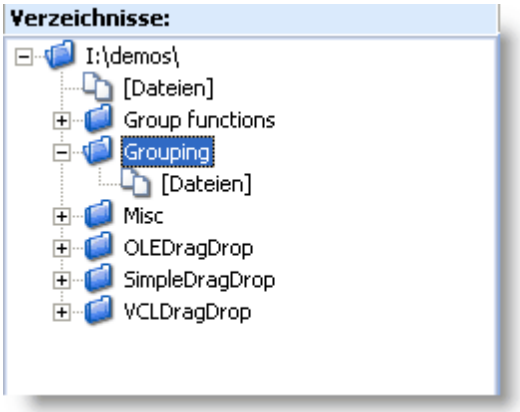
So legen Sie die Verzeichnisse für die Analyse fest

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[136] erzeugt.

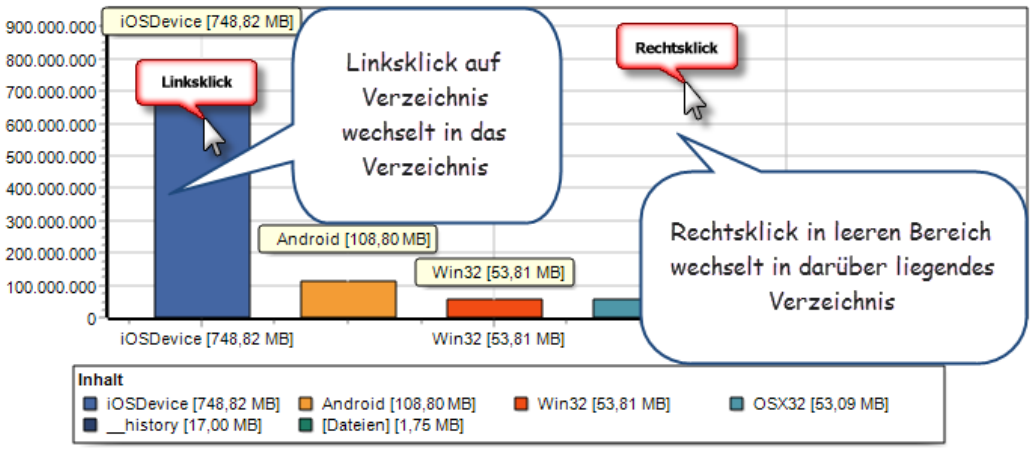
So deuten Sie das Diagramm der Laufwerksbelegung

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



Navigation im Analyse Ergebnis

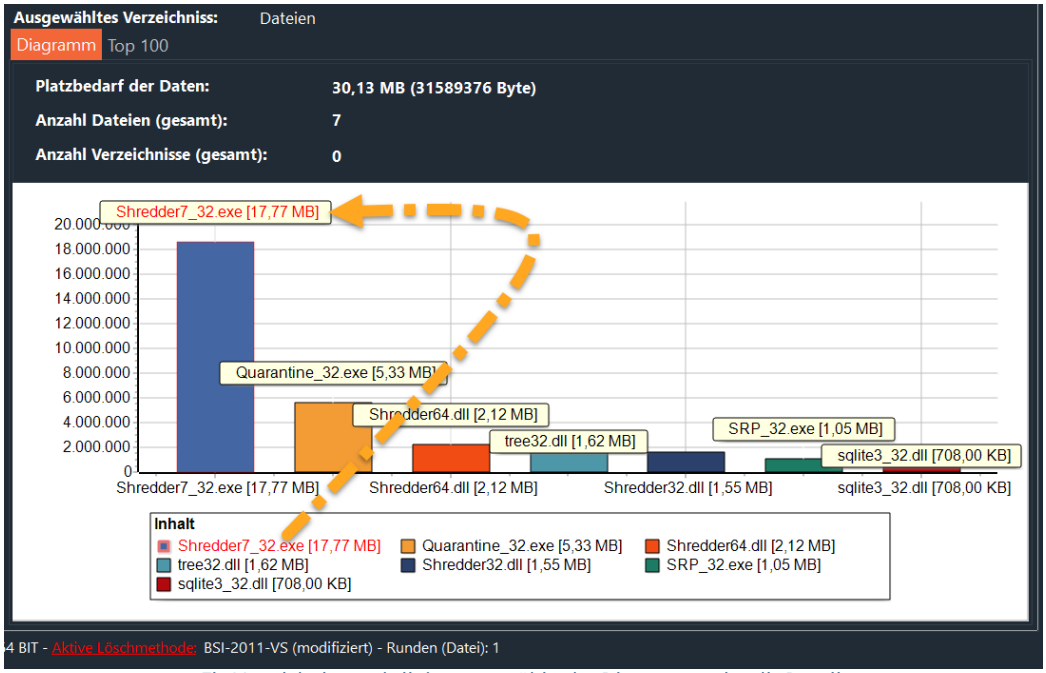
Auswahl eines Ordners in der Übersicht links, zeigt die Details in der Grafik an:



Navigation im Diagramm

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

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

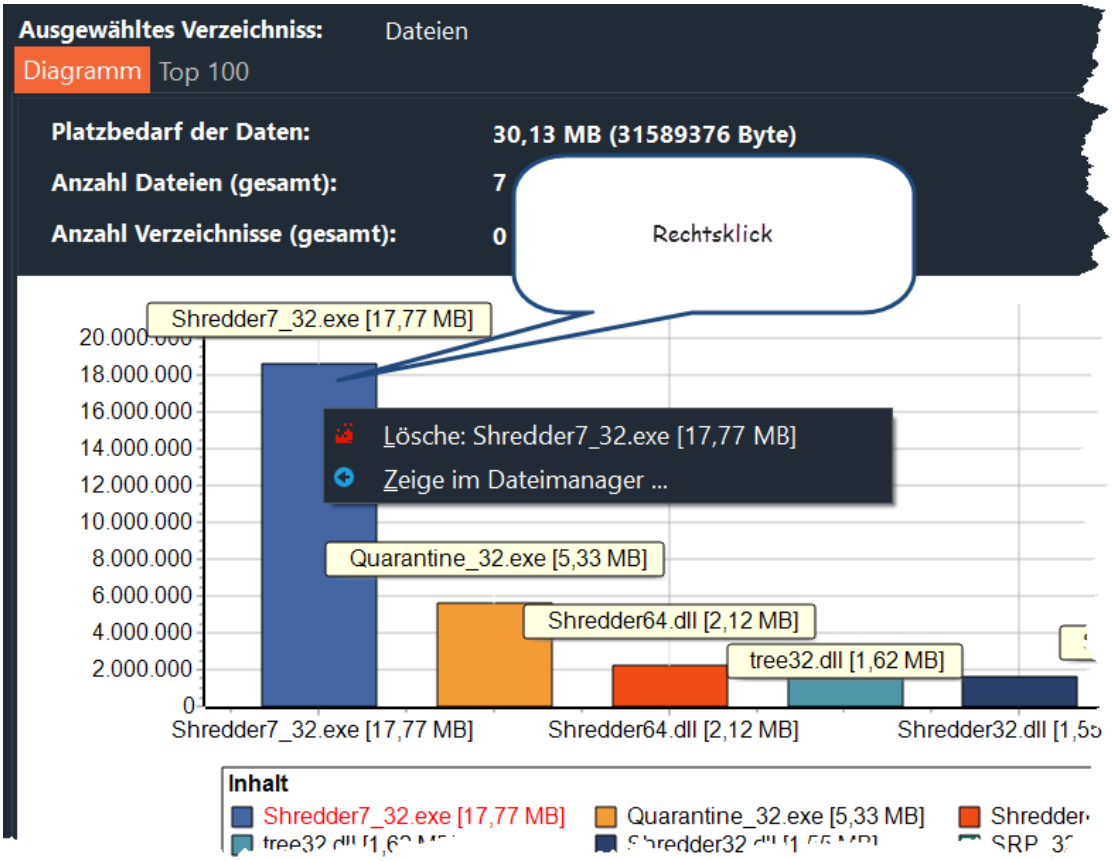


Ein Verzeichnis wurde links ausgewählt, das Diagramm zeigt die Details

Über dem Diagramm sehen Sie, wie viel Platz enthaltene Ordner bzw. Dateien belegen (im Beispiel 30,13 MB) und, wie viele Dateien (7) und wie viele Ordner (0) enthalten sind.

So löschen Sie Dateien und Verzeichnisse

Wenn Sie einen *Platzfresser* identifiziert haben und diesen löschen möchten, haben Sie zum einen die Möglichkeit in der Verzeichnisansicht 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.



Dateien und Verzeichnisse aus Laufwerksanalyse heraus löschen

➡**Anm.:** ***Das Löschen erfolgt mit den unter Einstellungen-Sicherheit*** 182 ***festgelegten Methoden.***

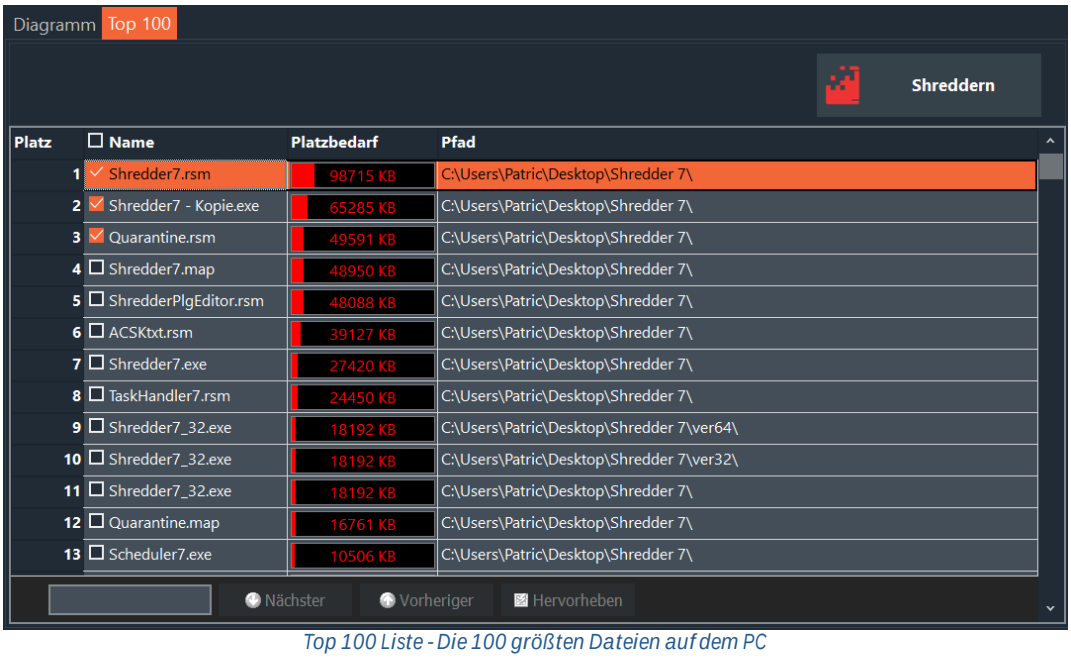
Warnung: Sie können grundsätzlich jede Datei auswählen und löschen. Bitte achten Sie darauf, dass Sie ausschließlich Dateien löschen, von denen Sie sicher wissen, dass sie nicht mehr benötigt werden. Dateien, bei denen Sie zweifeln, sollten Sie nie löschen.

So arbeiten Sie mit der TOP 100 Liste der Laufwerksanalyse

Wechseln Sie von der Diagramm-Ansicht in die Top 100 Ansicht durch **Linksklick** auf die *Registerkarte*.

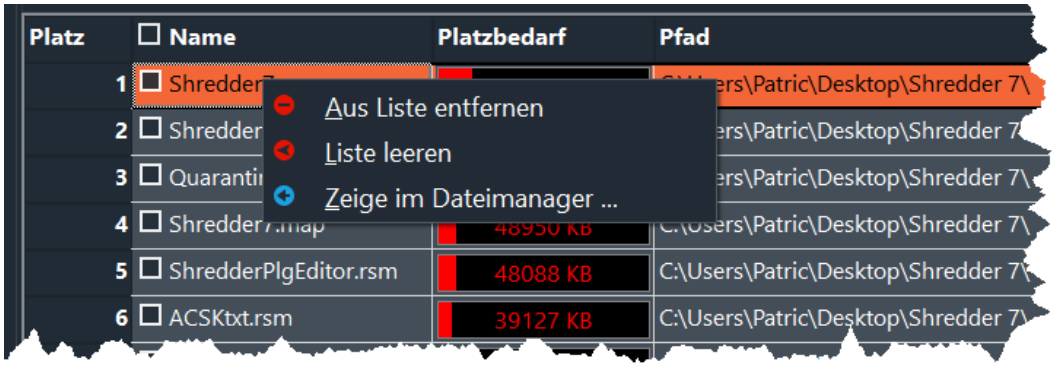
Die Datei mit dem größten Platzbedarf wird Ihnen an Position 1 angezeigt. Setzen Sie ein Häkchen bei den Dateien, die Sie löschen

möchten. Um alle Dateien an oder abzuwählen, klicken Sie bitte in der Spaltenüberschrift NAME auf das Kästchen.



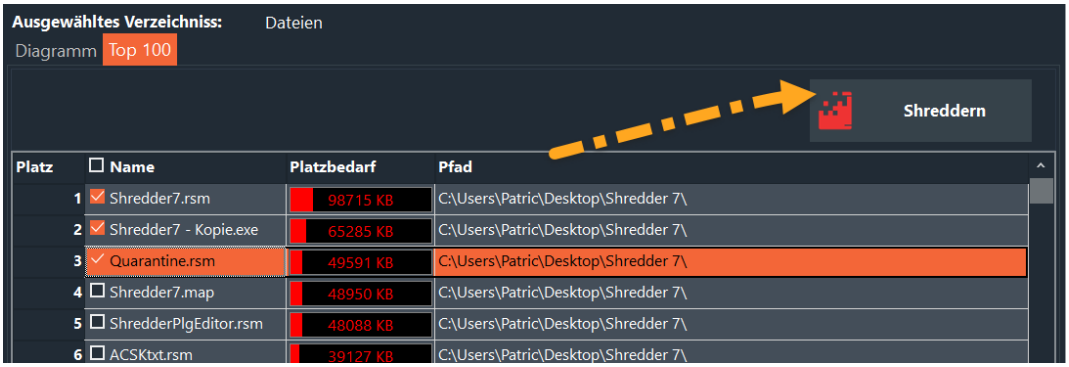
Top 100 Liste - Die 100 größten Dateien auf dem PC

Um einen Eintrag aus der Liste zu entfernen, in also nicht zu löschen, oder die Liste komplett zu leeren, rufen Sie das Kontextmenü mit der rechten Maustaste über der Liste auf. Zudem können Sie sich die Datei im Dateimanager 51 anzeigen lassen.

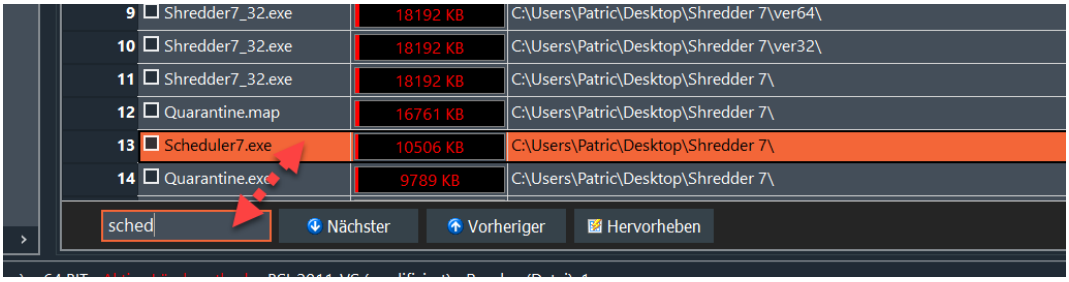


Kontextmenü der TOP 100 Liste

Sicher gelöscht werden die mit Häkchen versehenen Einträge erst dann, wenn Sie die Schaltfläche Shreddern betätigen.



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



8.14 Verborgene Daten finden

Versteckte Daten finden, einsehen und entfernen

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

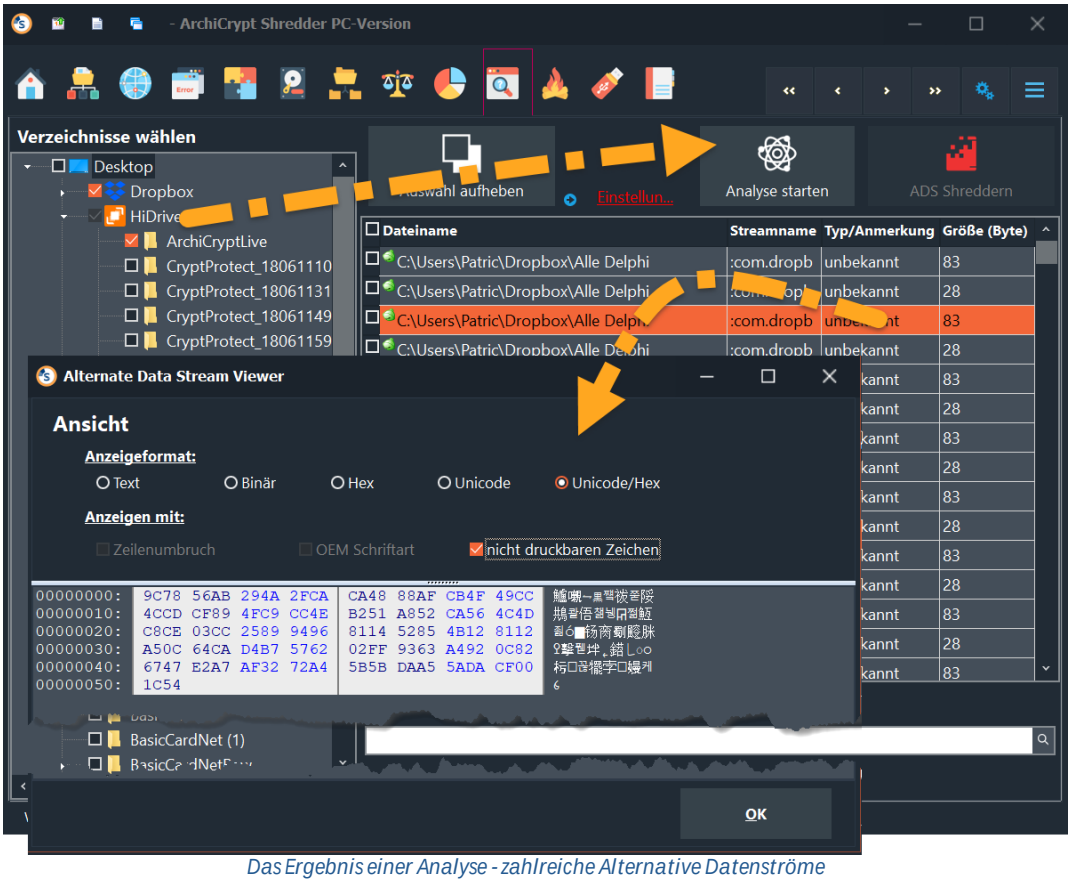
Den Dateien, denen Alternative Datenströme angehängt sind, kann man dies nicht ansehen. Die Dateigröße ist nach dem Anhängen unverändert. Dennoch belegen diese unsichtbaren Daten Platz.

Aufgrund dieser Eigenschaften werden Alternate Data Streams häufig missbraucht, um Schadprogramme wie **Viren** und **Trojaner** auf Ihrem System einzuschleusen und zu verbergen.

Mit den Windows Bordmitteln, ist es nahezu unmöglich, festzustellen, ob einer Datei ein solcher alternativer Datenstrom angehängt wurde.

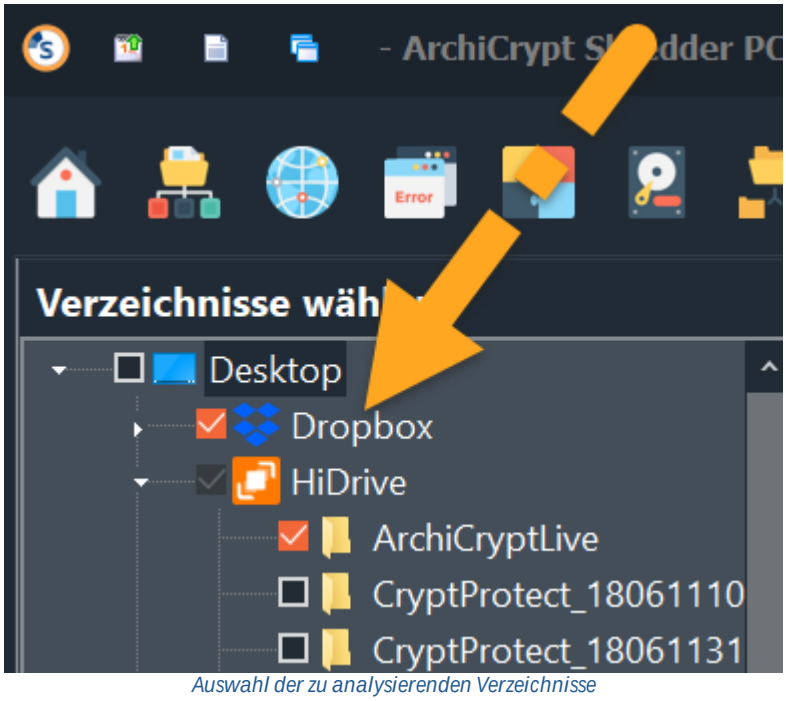
ArchiCrypt Shredder

- findet solche versteckte Daten,
- kann die versteckten Daten anzeigen
- kann die versteckten Daten löschen
- gibt einen Hinweis auf potenzielle Gefahr
- bietet an, im Internet eine Recherche nach Merkmalen des gefundenen Alternativen Datenstroms für Sie durchzuführen.



Das Ergebnis einer Analyse - zahlreiche Alternative Datenströme

So finden Sie versteckte Daten



Auswahl der zu analysierenden Verzeichnisse

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.

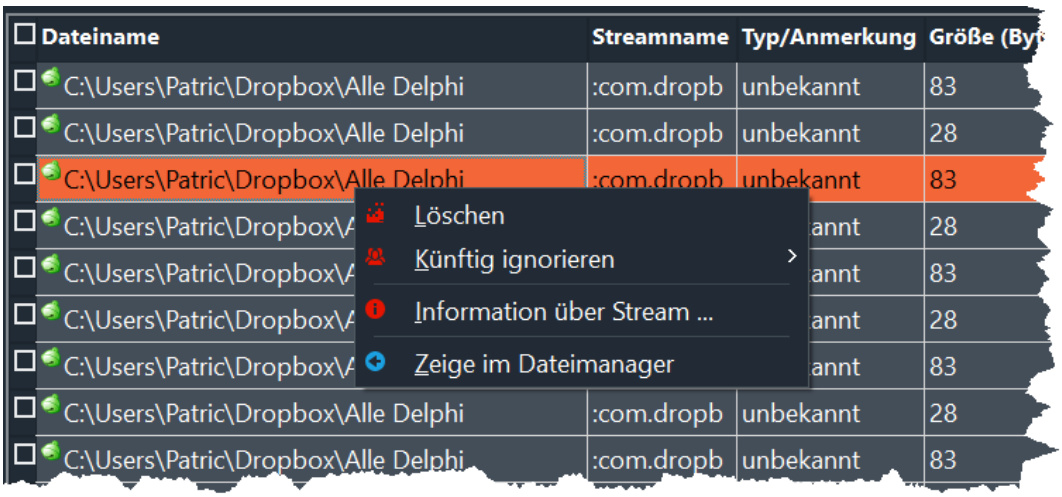
Die 2 Phasen der Analyse

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. ArchiCrypt Shredder versucht abzuschätzen, ob von den versteckten Daten eine Gefahr ausgeht und zeigt ein entsprechendes Symbol.

Das Ergebnis der Analyse einschätzen

Symbol
Von dieser Datei geht vermutlich keine Gefahr aus. Um wirklich sicherzugehen, wählen Sie den entsprechenden Eintrag in der Tabelle aus und betätigen die rechte Maustaste.



Eine Datei mit einem verdächtigen Alternativen Datenstrom

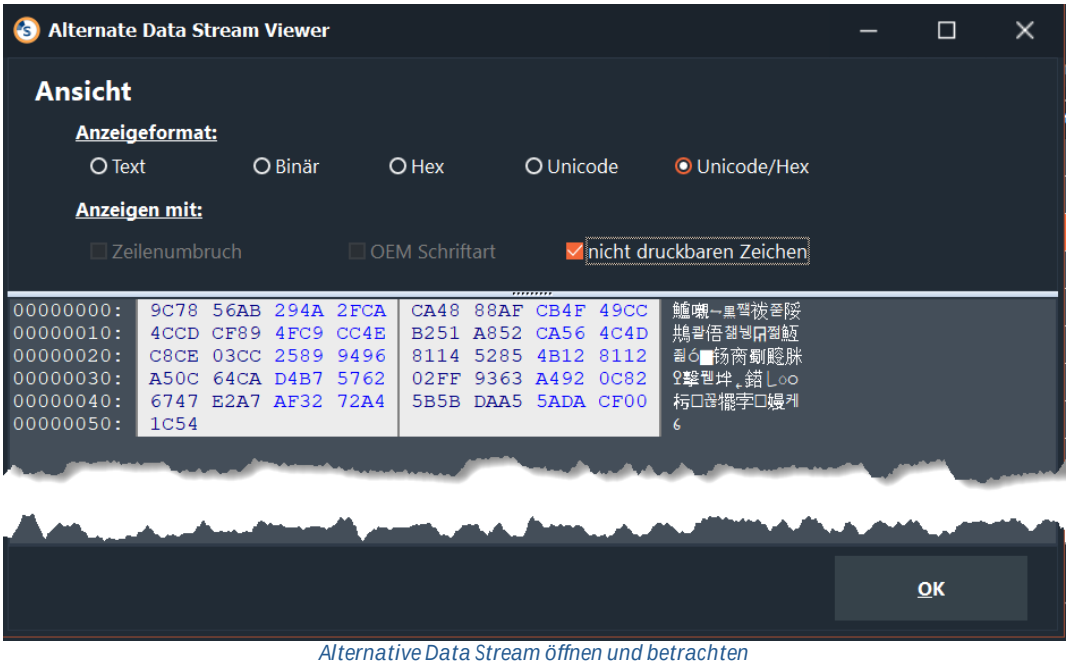
Wählen Sie jetzt im Kontextmenü die Eintrag "Information über Stream ...". ArchiCrypt Shredder zeigt Ihnen jetzt das Ergebnis einer Suche mit Google an. Sie können meist bereits anhand der ersten Suchergebnisse beurteilen, ob es sich um gefährliche Daten handelt.

Symbol

Von diesen Daten geht eine große Gefahr aus. Sie sollten diesen Datenstrom nur dann nicht löschen, wenn Sie genau wissen, um welche Daten es sich handelt und welchen Zweck diese Daten haben.
Auch hier hilft die Funktion "Information über Stream ..." des Kontextmenüs.

So betrachten Sie die Inhalte versteckter Daten

Um sich den Inhalt eines "Streams" anzusehen, klicken Sie bitte doppelt auf den entsprechenden Eintrag in der Tabelle.



Alternative Data Stream öffnen und betrachten

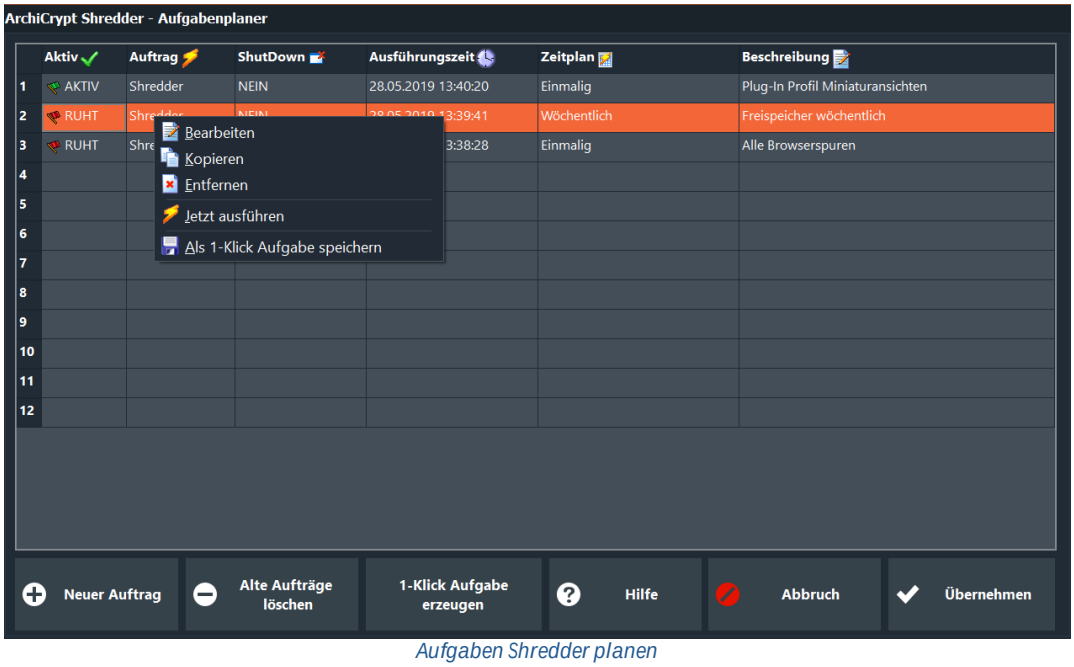
Wenn Sie ein Computerexperte sind, können Sie hier schnell *feststellen*, um welche Art von Datei es sich handelt und was der mutmaßliche Zweck ist. Aber auch als Laie kann man hier bestimmte Rückschlüsse über das Gefahrenpotenzial ziehen. Handelt es sich zum Beispiel um *reinen Text*, ist der Datenstrom *eher unkritisch*. Wenn Sie nicht einschätzen können, wie der Datenstrom zu bewerten ist, halten Sie sich an die automatische Einschätzung durch ArchiCrypt Shredder.

8.15 Aufgaben-Planer

Der Aufgaben-Planer

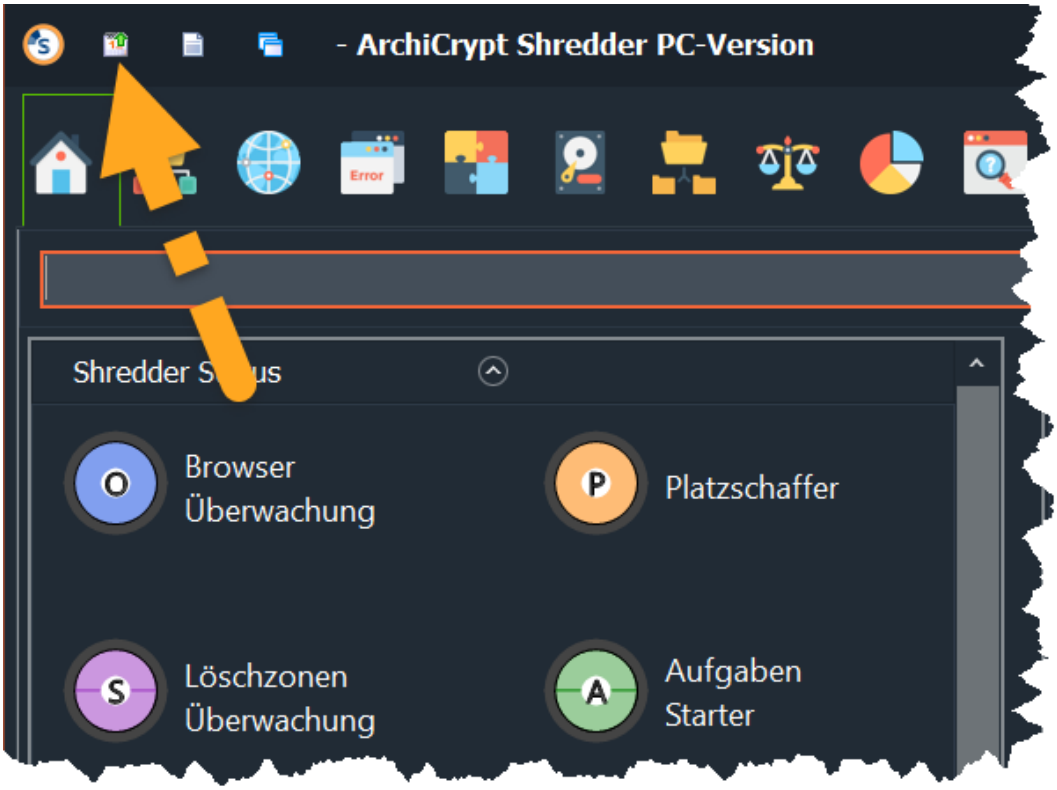
siehe auch Wiederkehrende Löschaufgaben planen[145] (1-Klick Aufgabe) und Löschaufgaben automatisch ausführen[156] (Aufgabenstarter).

Mit dem Aufgabenplaner[145] werden Aktionen definiert, die man entweder zu bestimmten Zeiten automatisch vom Aufgabenstarter[156] ausführen lässt oder als s.g. 1-Klick Aufgabe speichert. 1-Klick Aufgaben[145] führen die Aufgaben aus, sobald man auf die erstellte Datei doppelt linksklickt.



Aufgaben Shredder planen

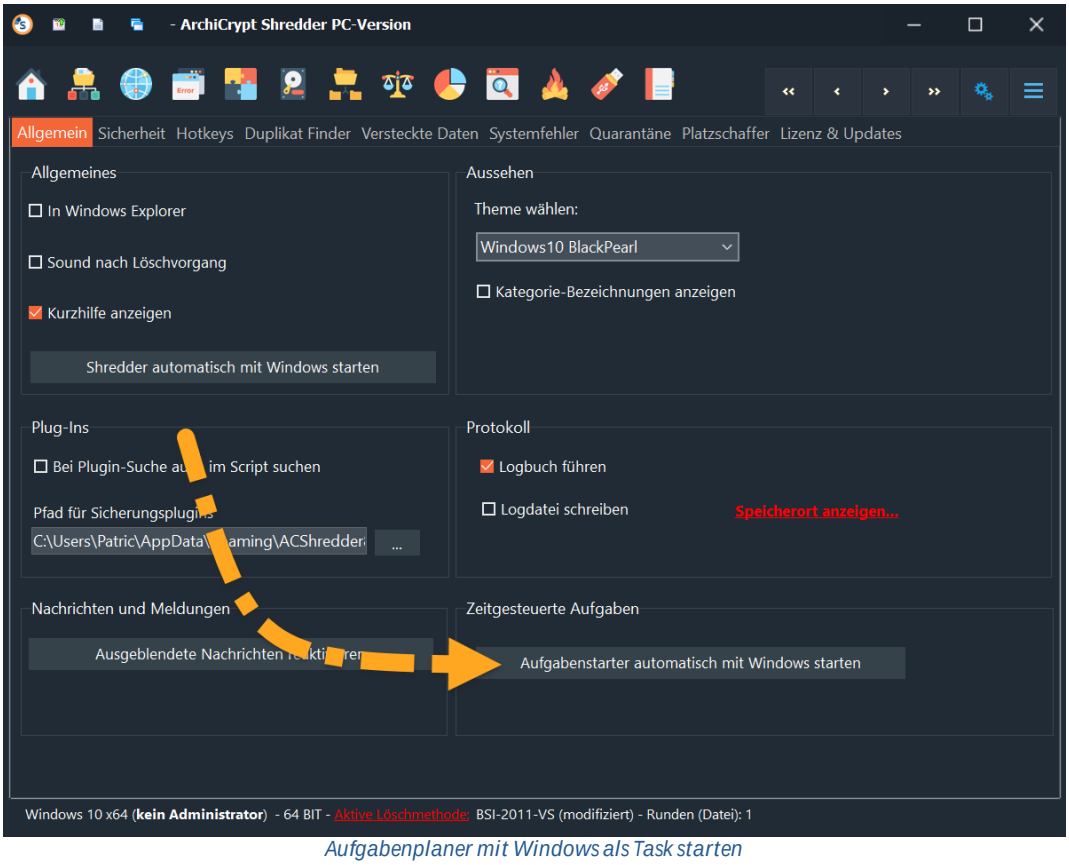
Sie starten den Aufgabenplaner, indem Sie die Schaltfläche Aufgabe planen betätigen.



Zeitgesteuerte Aufgabe erstellen

Der Aufgabenstarter[156] sorgt dafür, dass geplante Aufgaben auch zum vorgesehenen Zeitpunkt abgearbeitet werden. Sie können den Aufgabenstarter über das *Aktivitätssymbol* auf der Home-Seite[44] starten. In den Einstellungen[181] können Sie dafür sorgen, dass der Aufgabenstarter automatisch bei jedem Windows Start ausgeführt wird.

Aktivieren Sie die Funktion "Aufgabenstarter als TASK automatisch mit Windows starten".



Aufgabenplaner mit Windows als Task starten

Weiter zu Wiederkehrende Löschaufgaben planen [145]

Weiter zu Löschaufgaben automatisch ausführen [156]

8.15.1 Wiederkehrende Löschaufgaben planen

Der Aufgaben-Planer

siehe auch: Aufgabenstarter [156]

Der Aufgaben-Planer verwaltet alle Aufgaben.

Eine Aufgabe 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

Aufgabe[153] speichern. Bei einer gespeicherten **1-Klick Aufgabe** genügt es, einen Doppelklick auf das Symbol auszuführen.

Die enthaltenen Aktionen werden dann unmittelbar ausgeführt.

ArchiCrypt Shredder - Aufgabenplaner

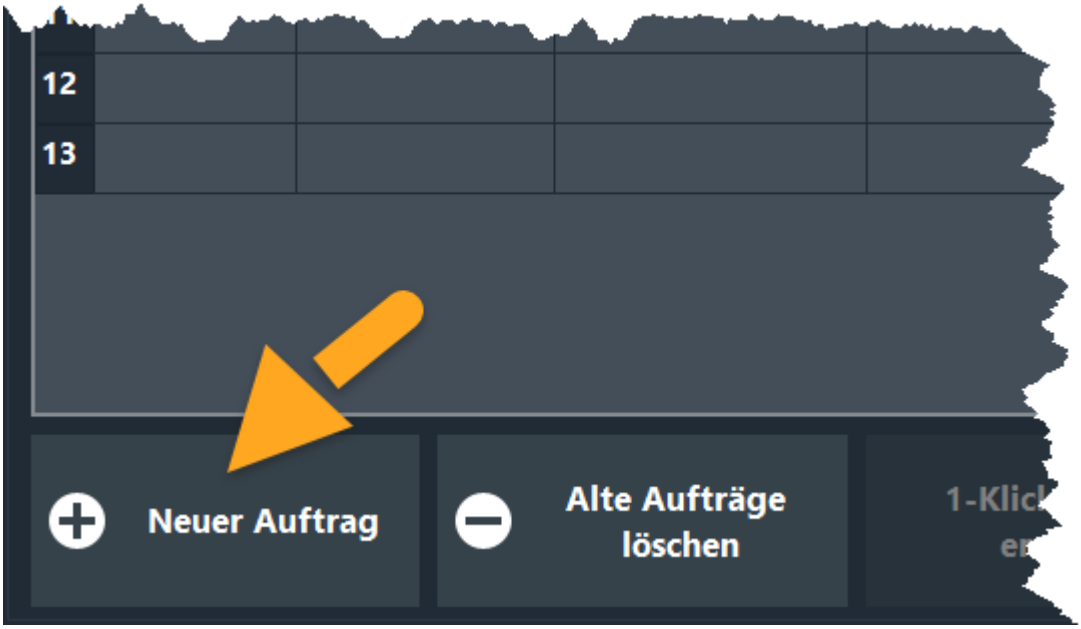
	Aktiv	Auftrag	ShutDown	Ausführungszeit	Zeitplan	Beschreibung
1	RUHT	Shredder	NEIN	28.05.2019 13:38:28	Einmalig	Alle Browserspuren
2	RUHT	Shredder	NEIN	28.05.2019 13:39:41	Wöchentlich	Freispeicher wöchentlich
3	AKTIV	Shredder	NEIN	28.05.2019 13:40:20	Einmalig	Plug-In Profil Miniaturansichten
4						
5						
6						
7						
8						

Zeitgesteuerte Löschaufgaben und 1-Klick Aufgaben erstellen

So erstellen Sie einen neuen Auftrag

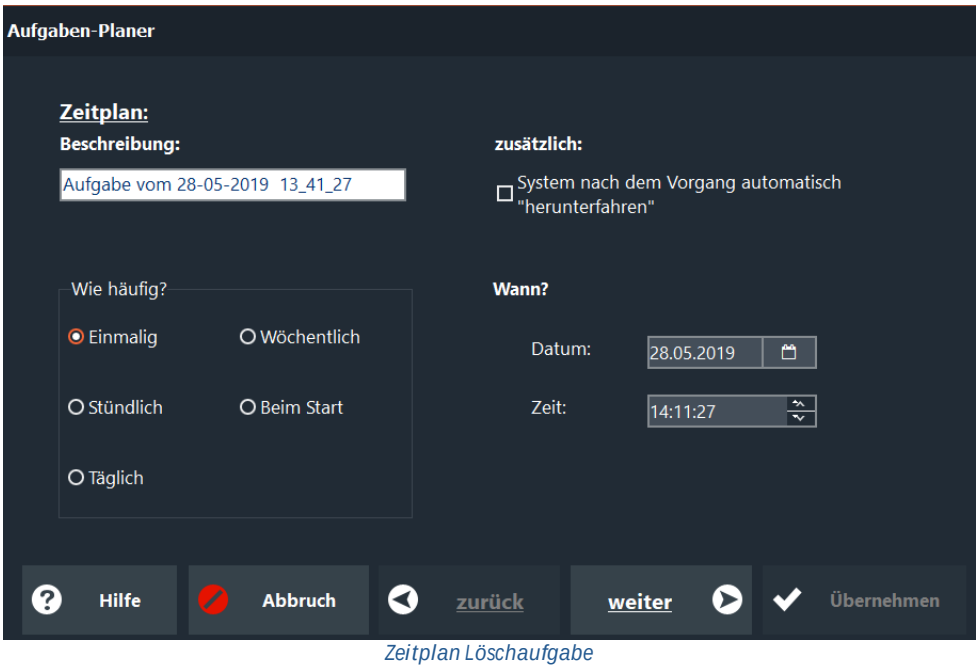
Um einen neuen Auftrag zu erstellen, betätigen Sie bitte die Schaltfläche Neuer Auftrag.

Klick auf Neuer Auftrag



Es erscheint ein Assistent:

1. Schritt:

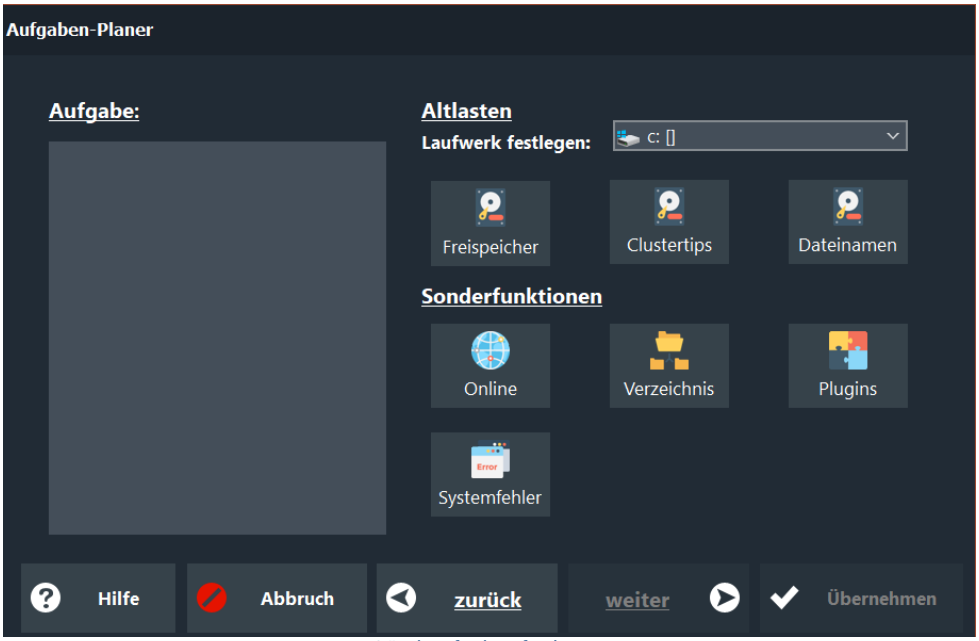


Zeitplan Löschaufgabe

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 (zusätzlich). Dies ist dann nützlich, wenn Sie sehr zeitaufwendige Aufgaben wie zum Beispiel den Freispeicher[44] oder Clustertips[44] bereinigen lassen. Wenn Sie die gewünschten Angaben gemacht haben, betätigen Sie die Schaltfläche Weiter.

2. Schritt



Löschaufgaben festlegen

Sie haben die Möglichkeit Altlasten beseitigen zu lassen (Datenträger[60]), und/oder eine der Sonderfunktionen zu wählen.

Altlasten

Wählen Sie zunächst das gewünschte Laufwerk aus (Laufwerk festlegen) und betätigen dann eine der Schaltflächen Freispeicher, Clustertips oder Dateinamen.

Sonderfunktionen

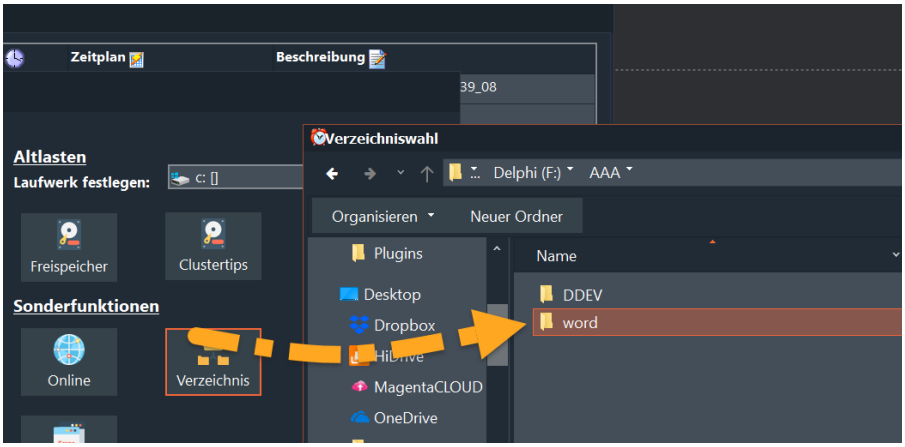
Online

Beseitigt die Online Spuren, die Sie in ArchiCrypt Shredder unter Online-Spuren festgelegt haben. Hier können Sie, sofern gewünscht ein bereits vorhandenes Online-Profil 90 ausführen lassen. Wenn Sie kein Online-Profil angeben, werden die aktuell im Shredder aktivierten Browserspuren beseitigt.

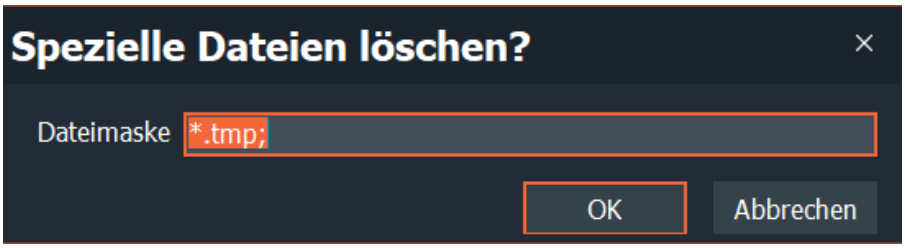
ACHTUNG: Die Funktionen spezielle Verzeichnisse 55 und Plugins ausführen 96 des *Online Profils* werden nicht berücksichtigt, können jedoch separat über die anderen Sonderfunktionen Verzeichnis und Plugins im Aufgabenplaner nachgebildet werden.

Verzeichnis

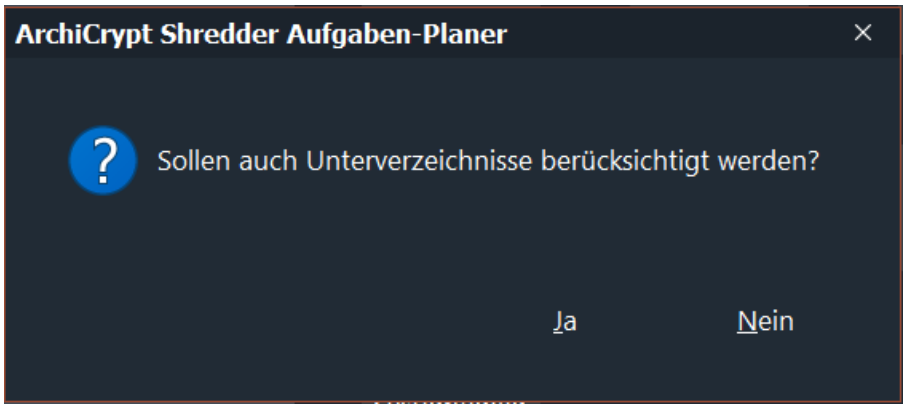
Wählen Sie zunächst das gewünschte Verzeichnis aus.



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

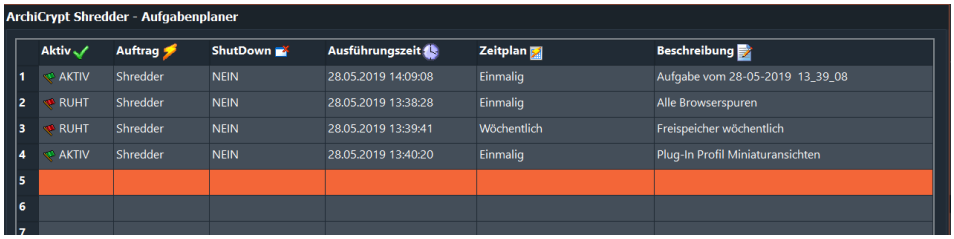
Hier haben Sie die Möglichkeit, ein bestimmtes Plugin-Profil[104] ausführen zu lassen. Wenn Sie kein Profil angeben, werden die aktuell in ArchiCrypt Shredder aktiven Plug-Ins ausgeführt.

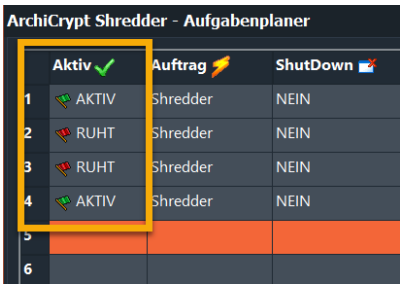
ACHTUNG: Die Option *Plug-Ins nur simulieren* hat keine *Wirkung* wenn Sie eine zeitgesteuert Aufgabe oder eine 1-Klick Aufgabe ausführen. Alle Plugins werden ausgeführt!

Systemfehler

Hier haben Sie die Möglichkeit, ein bestimmtes Systemfehler-Profil[121] ausführen zu lassen. Wenn Sie kein Profil angeben, werden die aktuell in ArchiCrypt Shredder aktiven Kategorien analysiert.

Wenn alle Angaben gemacht sind, können Sie die Schaltfläche Übernehmen betätigen. In der Tabelle sollten Sie jetzt den neuen Eintrag sehen.



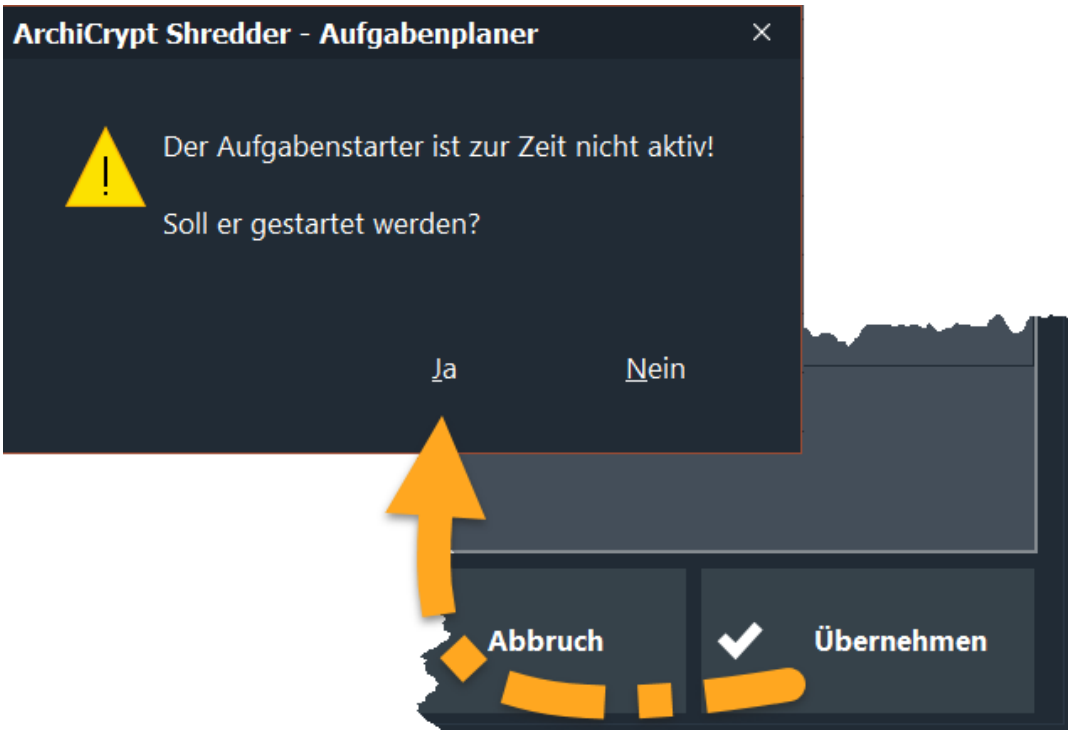


In der Spalte AKTIV ist eine *grüne Fahne* zu sehen, die angibt, dass die Aufgabe ausgeführt werden soll. Möchten Sie die Aufgabe ruhen lassen, klicken Sie mit der Maus auf das Flaggensymbol.

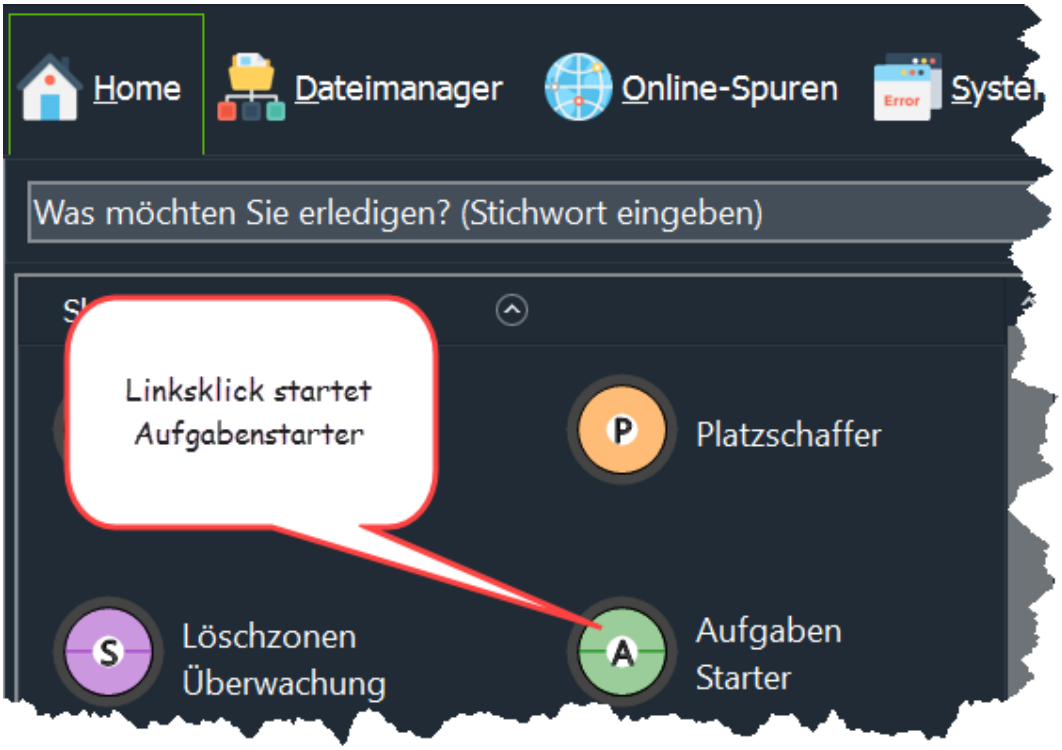
Um die aktuell aktiven Aufträge an den Aufgabenstarter 156 zu übergeben, betätigen Sie die Schaltfläche Übernehmen.

So aktivieren Sie den Aufgabenstarter

Wenn Sie die gewünschten Aufgaben erstellt haben, betätigen Sie die Schaltfläche Übernehmen.



Alternativ kann der Aufgabenstarter direkt aus ArchiCrypt Shredder heraus aufgerufen werden. Dazu können Sie auf der Home-Seite[34] auf das entsprechende *Aktivitätssymbol* klicken.

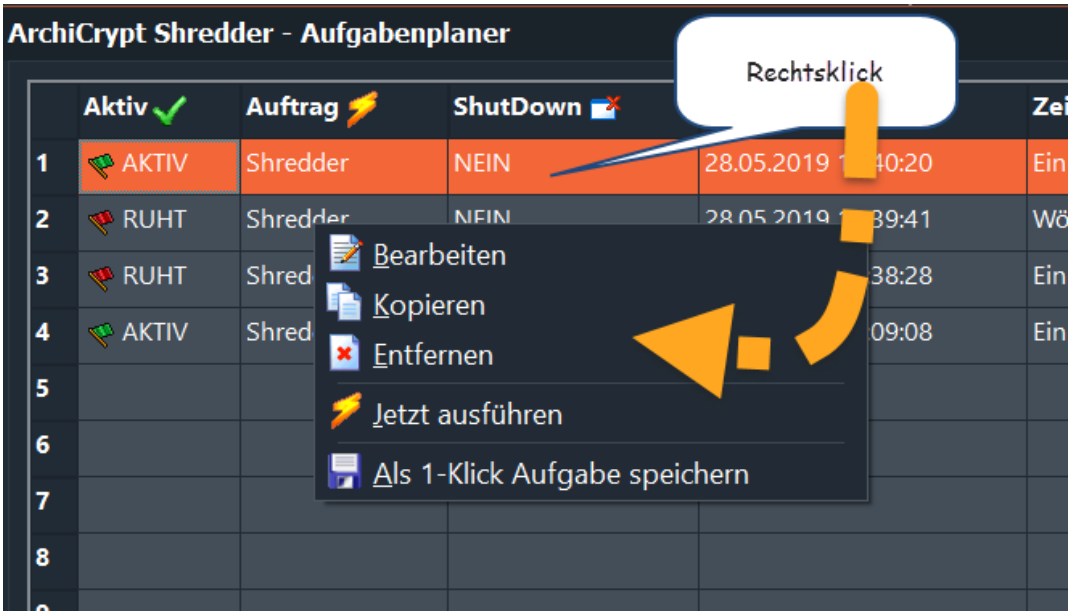


Wenn Sie im Aufgaben-Planer die Schaltfläche Abbruch betätigen wird der *Aufgaben-Planer* **geschlossen** und es werden *keinerlei Änderungen* übernommen!

Falls der Aufgabenstarter[156] nicht aktiv ist, werden Sie gefragt, ob dieser gestartet werden soll. Nur mit aktivem Aufgabenstarter werden die Löschaufgaben auch tatsächlich abgearbeitet!

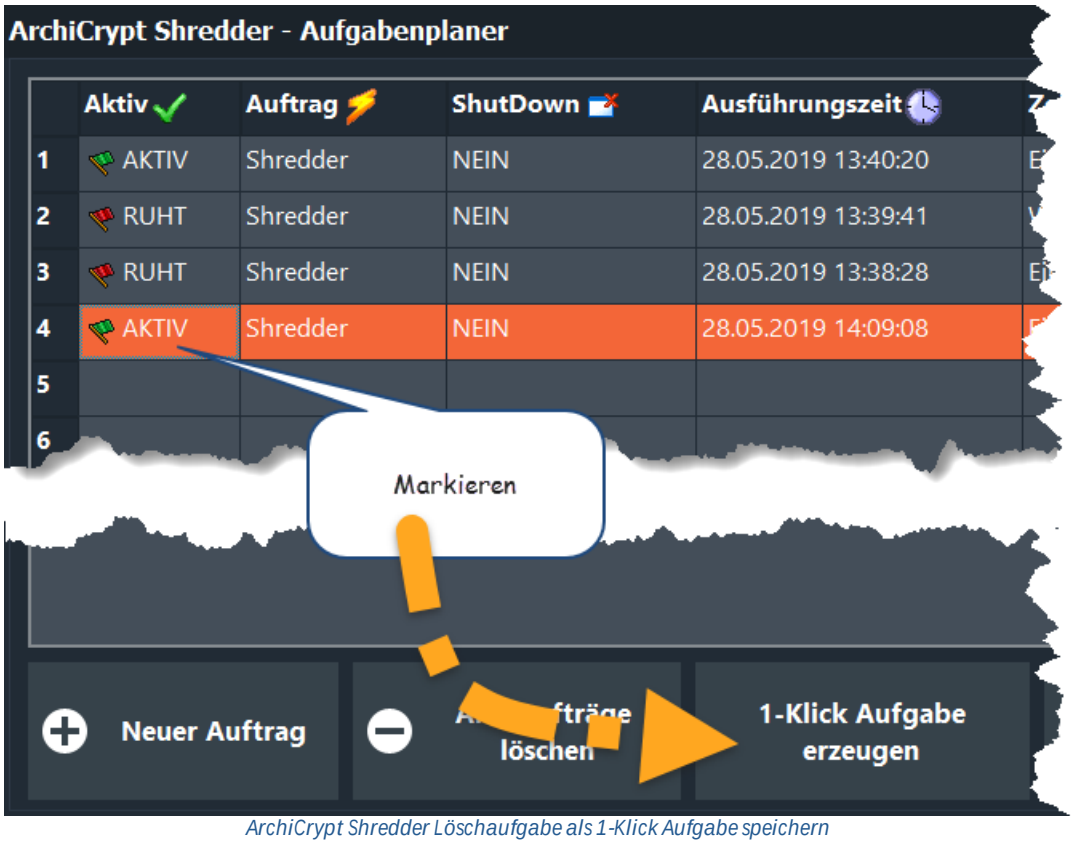
So starten Sie eine Aufgabe direkt aus dem Aufgaben-Planer

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. Ist Shredder mit der Bearbeitung einer anderen Aufgabe beschäftigt, wird die Aufgabe in eine *Warteschlange* übertragen.



So speichern Sie Aufgaben als 1-Klick Aufgabe

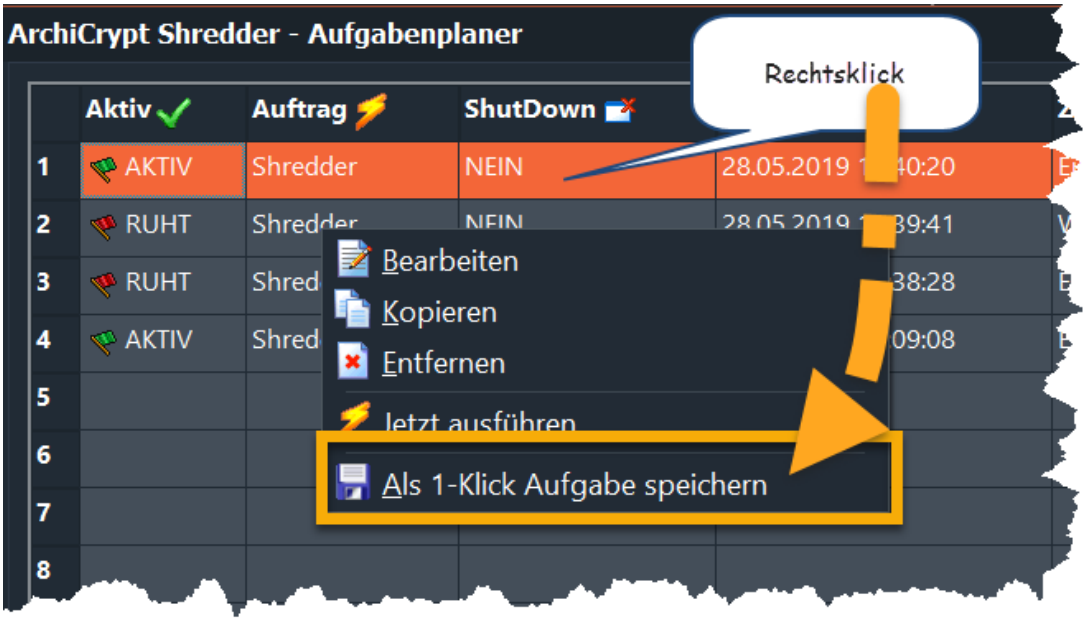
Markieren Sie die Aufgabe im Aufgabenplaner. Betätigen Sie jetzt die Schaltfläche 1-Klick Aufgabe erzeugen. Legen Sie im Windows Dialog Speicherort und Name für die *1-Klick Aufgabe* fest.



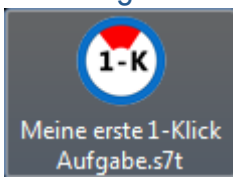
ArchiCrypt Shredder Löschaufgabe als 1-Klick Aufgabe speichern

Alternativ:

In der Tabelle wählen Sie den Eintrag mit der rechten Maustaste aus. Im Kontextmenü wählen Sie bitte die Funktion Als 1-Klick Löschaufgabe speichern aus.



Die Aufgabe wird jetzt mit dem *1-Klick Symbol* des Shredders abgelegt.



Ihr Desktop wird als Speicherort für die Datei vorgegeben. Künftig genügt ein Linksdoppelklick und die 1-Klick Aufgabe wird ausgeführt.

So bearbeiten Sie eine geplante Aufgabe

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

Klick auf Bearbeiten ruft den *Assistenten* mit den Werten der gewählten Aufgabe aus. Sie können jetzt Änderungen an der Aufgabe vornehmen.

Bitte beachten Sie, dass gespeicherte 1-Klick Aufgaben durch diese Maßnahme nicht geändert werden. 1-Klick Aufgaben lassen sich nicht direkt ändern. Löschen Sie einfach die 1-Klick Aufgabe und speichern Sie aus dem Aufgabenplaner heraus die Aufgabe als neue 1-Klick Aufgabe.

Aufgaben bereinigen

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

siehe auch: Löschaufgaben automatisch ausführen 156

8.15.2 Löschaufgaben automatisch ausführen

Der Aufgabenstarter

siehe auch Aufgaben-Planer 145

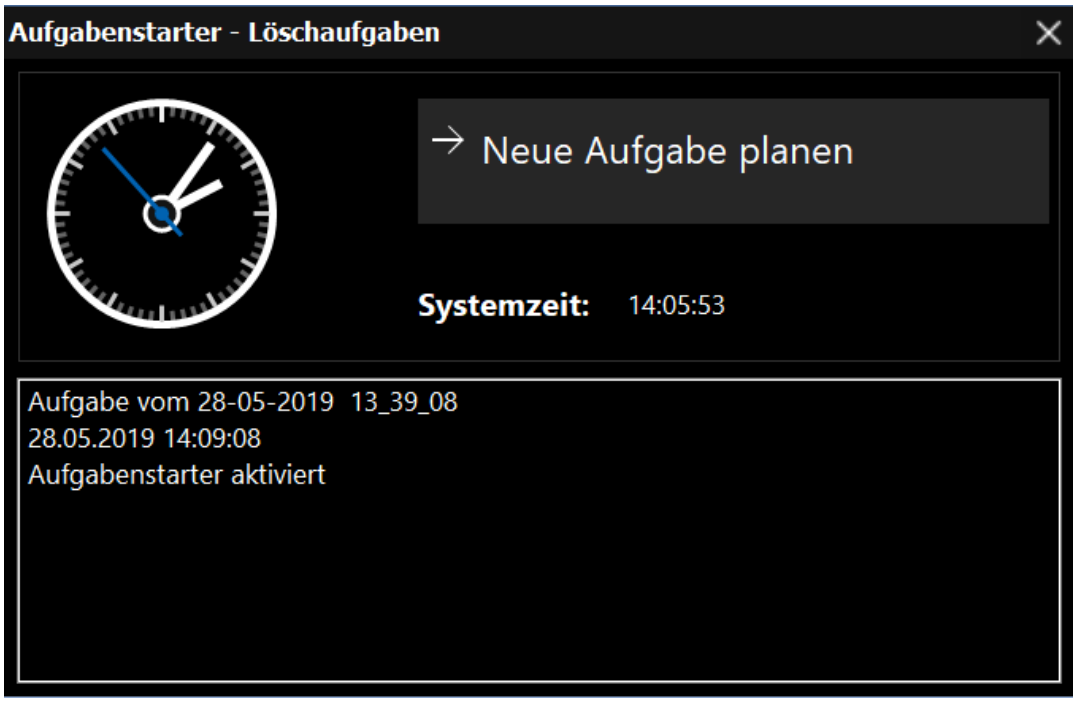
Der Aufgabenstarter ist ein kleines Programm, welches im Hintergrund dafür sorgt, dass die geplanten Aufgaben *durch ArchiCrypt Shredder* erledigt werden. Sie sollten den Aufgabenstarter mit Windows starten lassen, das Programm belegt kaum Ressourcen und sorgt dafür, dass die Aufgaben zur gegebenen Zeit ausgeführt werden.

Bedienung des Aufgabenstarters

Nach dem Start sehen Sie ein Symbol im Infobereich (*Tray*) der Taskleiste.

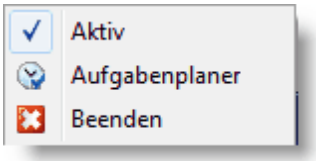
Das Symbol zeigt dabei an, dass die Zeitüberwachung aktiv ist.

Doppelklicken Sie auf das Symbol im Systemtray, um das Fenster das *Aufgabenstartes* sichtbar zu machen:



Sie sehen die Systemzeit und die Zeiten, zu denen bestimmte Aufgaben zu erfüllen sind. Über die Schaltfläche Neue Aufgabe planen können Sie den Aufgaben-Planer[142] starten.

Wenn Sie den Mauszeiger über das Symbol im Infobereich bewegen und die rechte Maustaste betätigen, erscheint ein Kontextmenü:



Aktiv
Über die Funktion Aktiv können Sie die Zeitüberwachung *De-/Aktivieren*. Im deaktivierten Zustand erscheint das Symbol im Systemtray. Aufgaben werden jetzt nicht gestartet.

Aufgaben-Planer
Die Funktion Aufgaben-Planer ruft den Aufgaben-Planer[142] auf.

Beenden
Beenden beendet den Aufgabenstarter.

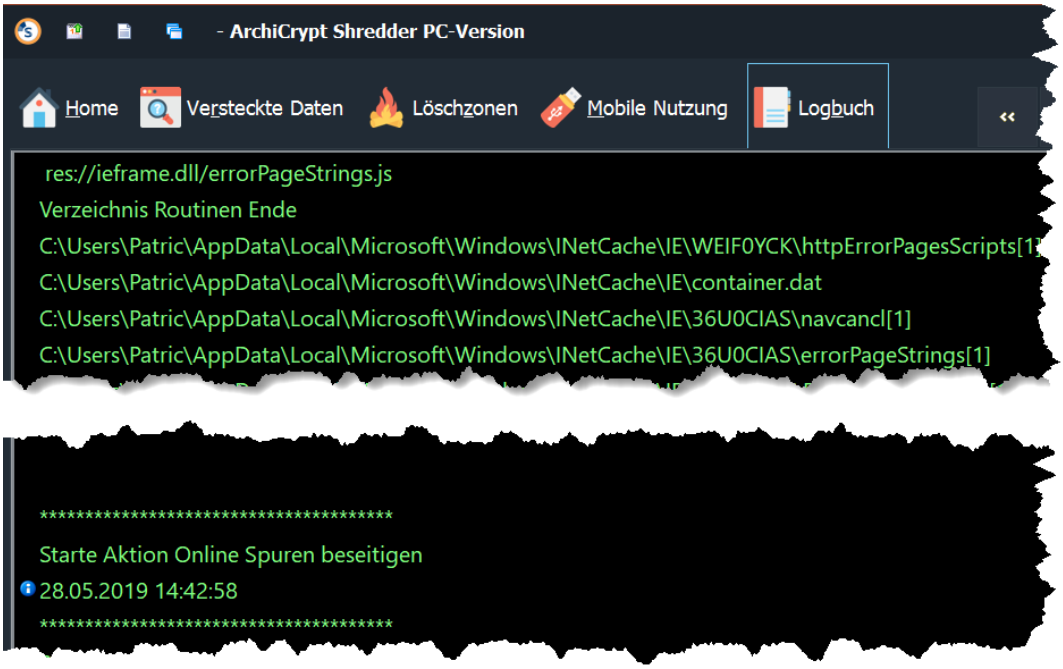
ACHTUNG: Wenn der Aufgabenstarter nicht aktiv ist, werden keine geplanten Aufgaben ausgeführt.

siehe auch: Wiederkehrende Löschaufgaben planen[145]

8.16 LogBuch

Das Logbuch

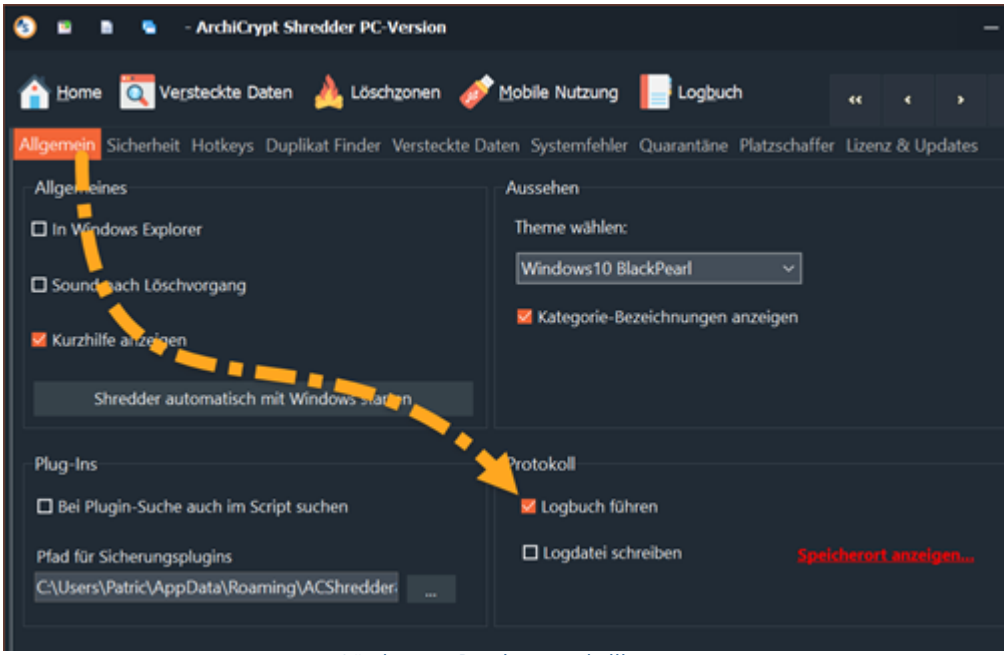
Im Logbuch werden alle Aktionen mit Uhrzeit und Statusmeldung aufgeführt.



Shredder Logbuch - Alle Aktionen des Shredders Protokoll

Falls Sie unter Einstellungen[177] die Option LogBuch führen aktiviert haben (*empfohlen*), werden die Aktionen von ArchiCrypt Shredder auf dieser Seite protokolliert. Sie sehen immer *die letzten 400 Zeilen*. Sie können das LogBuch zurücksetzen, indem Sie die rechte Maustaste betätigen und den Eintrag Löschen wählen.

Falls Sie **zusätzlich** die Option Logdatei schreiben in den Einstellungen[177] aktiviert haben, werden Alle Aktionen der aktuellen Sitzung in der Protokolldatei ACShredder.log gespeichert.



Löschen von Dateien protokollieren

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.

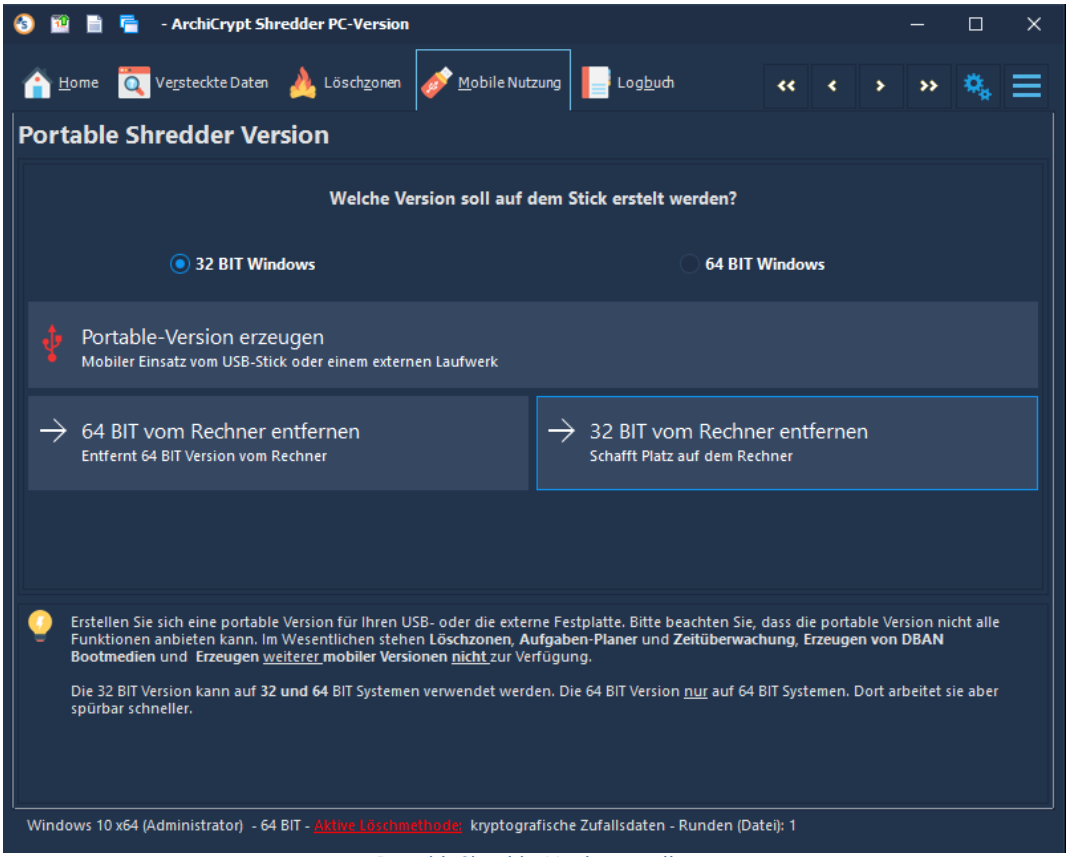
ACHTUNG: Das LogBuch geht verloren, sobald ArchiCrypt Shredder beendet wird.

siehe auch: Logdatei 177 unter Einstellungen Allgemeines

8.17 Shredder Portable

Portable Version von ArchiCrypt Shredder

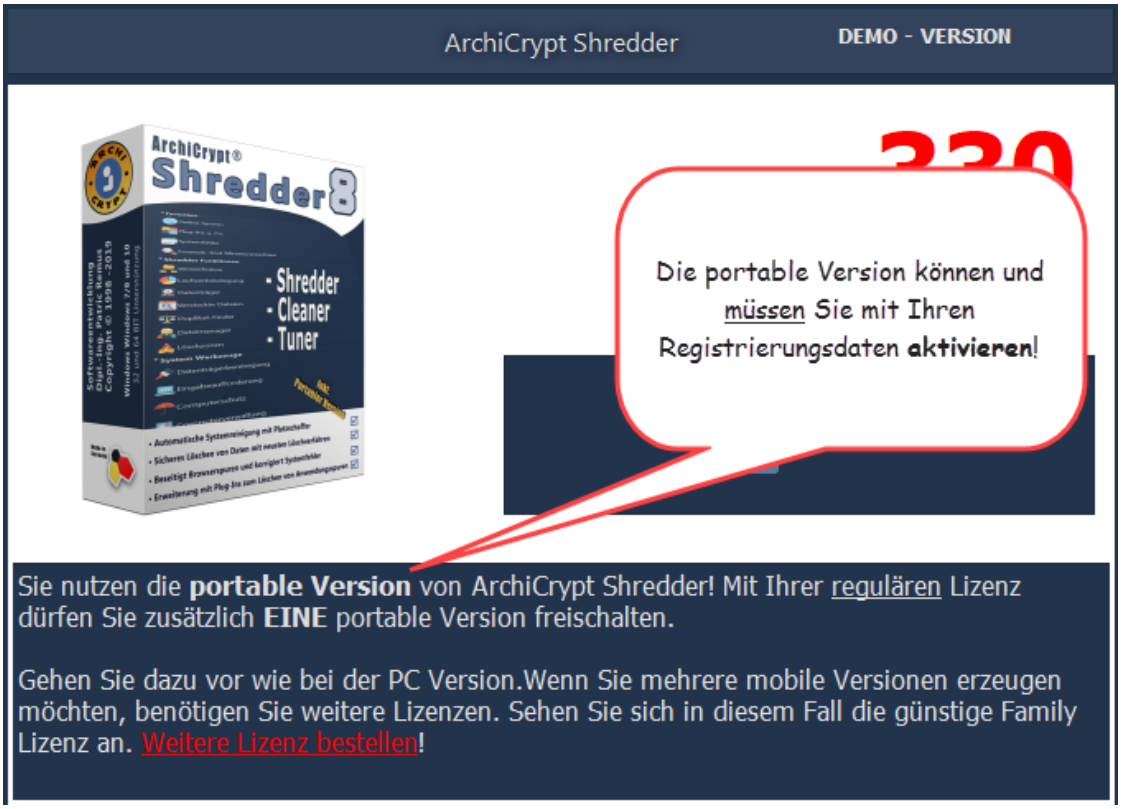
ArchiCrypt Shredder bietet die Möglichkeiten spezielle portable Versionen zu erstellen, die man ohne Installation direkt, *zum Beispiel* von einem *USB-Stick* aus, starten kann.



Portable Shredder Version erstellen

Die Daten für die *portable 32 BIT und 64 BIT* Version des Shredders belegen Speicherplatz auf Ihrem PC. Wenn Sie sich sicher sind, dass sie eine bestimmte Version nicht benötigen, klicken Sie neben der Version auf **ENTFERNEN**. Die Daten werden dann gelöscht und Sie können die entsprechende portable Version nicht mehr erstellen. Wenn Sie sich umentscheiden, müssen Sie ArchiCrypt Shredder neu installieren!

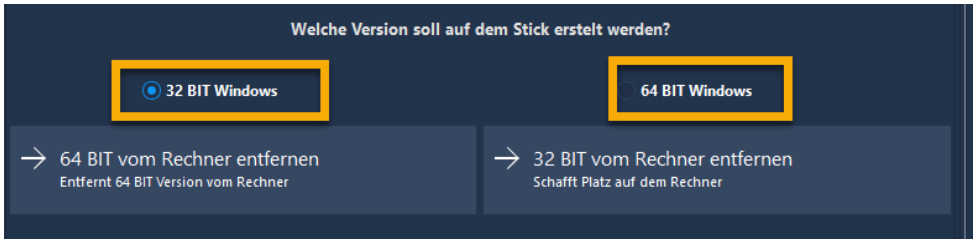
WICHTIG: Die portable Version muss *gesondert aktiviert* werden! Sie sollten die portable Shredder Version möglichst *nicht an einem Rechner* einsetzen, auf dem die *PC Version installiert* ist.



So erstellen Sie eine portable Version von ArchiCrypt Shredders

Die beschrieben Vorgehensweise ist universell und stellt keine besonderen Anforderungen an den verwendeten Datenträger. Da jedoch im Verzeichnis der portablen Version Einstellungen gespeichert werden, darf das Speichermedium nicht schreibgeschützt sein. Der Datenträger sollte über ca. 50 Megabyte freien Speicherplatz verfügen.

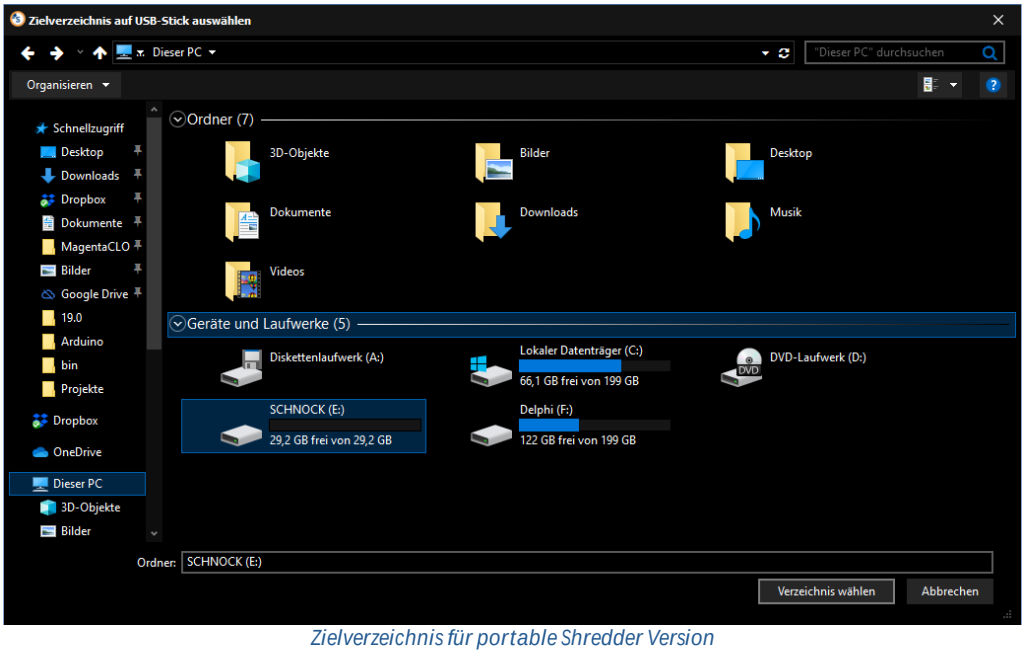
Zunächst entscheiden Sie bitte, ob Sie eine 32 BIT portable Version oder die 64 BIT portable Shredder Version erstellen möchten.



TIPP: Die meisten Systeme sind heute *64 BIT Systeme*. Für diese Systeme ist die 64 BIT Version bestens geeignet und bietet einige Geschwindigkeitsvorteile gegenüber der 32 BIT Version. *Auf reinen 32 BIT Systemen kann die 64-BIT Version nicht eingesetzt werden.* Der 32 BIT portable Shredder hingegen kann auf *64 BIT (mit Einschränkungen) und auf 32 BIT* Systemen eingesetzt werden.

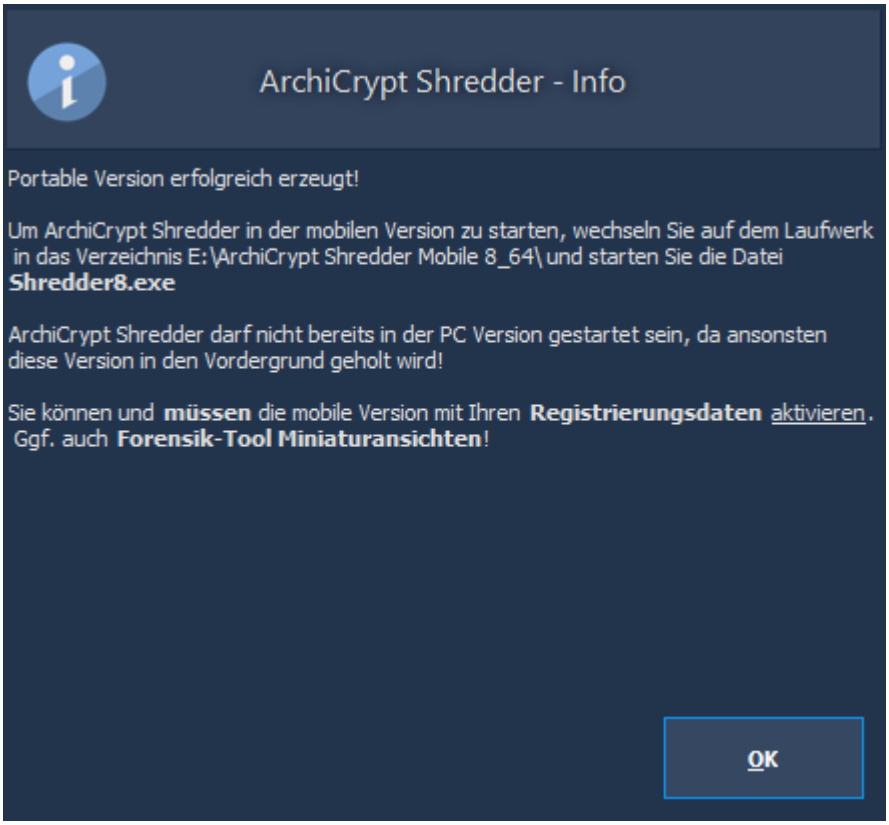
TRICK: Wer *beide Varianten* auf zum Beispiel einem Stick verwenden möchte, kann sich auf dem Stick zwei entsprechende Unterverzeichnisse erstellen und als Ziel dann jeweils das gewünschte Unterverzeichnis angeben.

Wählen Sie nach dem Betätigen der Schaltfläche Portable-Version erzeugen als Ziel das entsprechende Laufwerk oder Verzeichnis aus.



Zielverzeichnis für portable Shredder Version

ArchiCrypt Shredder legt jetzt automatisch ein Verzeichnis ArchiCrypt Shredder Mobile 8_32 bzw. ArchiCrypt Shredder Mobile 8_64 an und kopiert eine spezielle Version für die mobile Verwendung in das Verzeichnis.



HINWEIS: Der *erste Start* der mobilen Version *dauert länger*, da bei jedem ersten Start des Shredders auf einem Rechner das Plug-In System zunächst neu initialisiert werden muss!

Auf welche Funktionen müssen Sie in den mobilen Version verzichten?

Einige Funktionen des Shredders greifen tiefer in das System ein und erfordern eine permanente Installation. Andere Funktionen machen mobil keinen oder nur wenig Sinn.

Die Folgenden Funktionen stehen nicht zur Verfügung:

- Erzeugen weiterer mobiler Versionen
- Sichere Löschzonen
- Kontextmenü für den Windows Explorer
- Editor für Plug-Ins
- Aufgaben-Planer und Zeitüberwachung
- Erzeugen von DBAN BOOT Medien

Welche Daten speichert die mobile Version auf dem PC

Die mobile Version legt ein Verzeichnis im Profil des Nutzers an, der den Shredder startet (%AppData%\Roaming\ACShredderMobile8).

In diesem Verzeichnis werden im Wesentlichen folgende Dateien abgelegt:

- Quarantäne des Duplikatfinders 129
- Quarantäne der Systemfehler Analyse 203
- Liste sinnvoller Plug-Ins
- Liste aktiver Plug-Ins
- Aktives Online-Profil

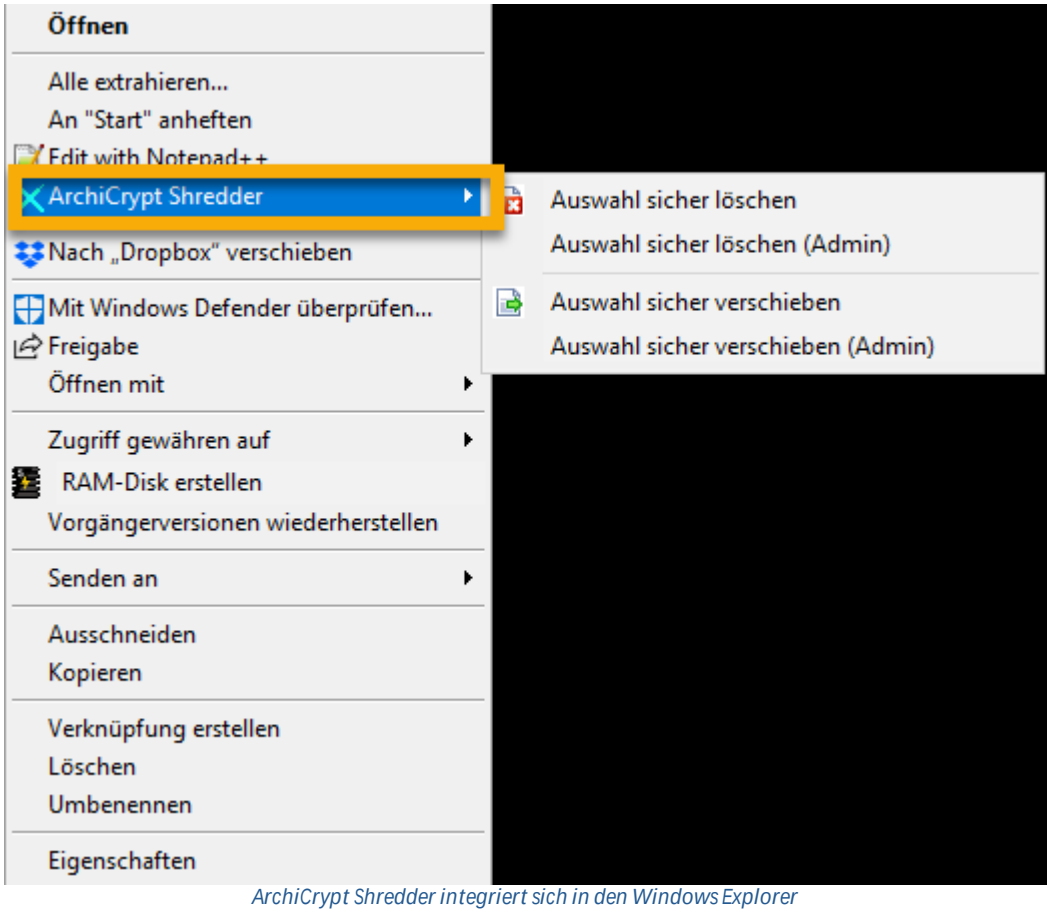
Diese Daten werden auf dem Rechner des Anwenders gespeichert, weil sie NUR auf diesem Rechner Sinn machen.

8.18 Explorer Kontextmenü und Systemtray-Menü

ArchiCrypt Shredder in Kontextmenüs von Windows

Kontextmenü im Windows Explorer

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 dazu NICHT gestartet sein.



ArchiCrypt Shredder integriert sich in den Windows Explorer

Das *Kontextmenü* bietet Ihnen die folgenden Werkzeuge an:

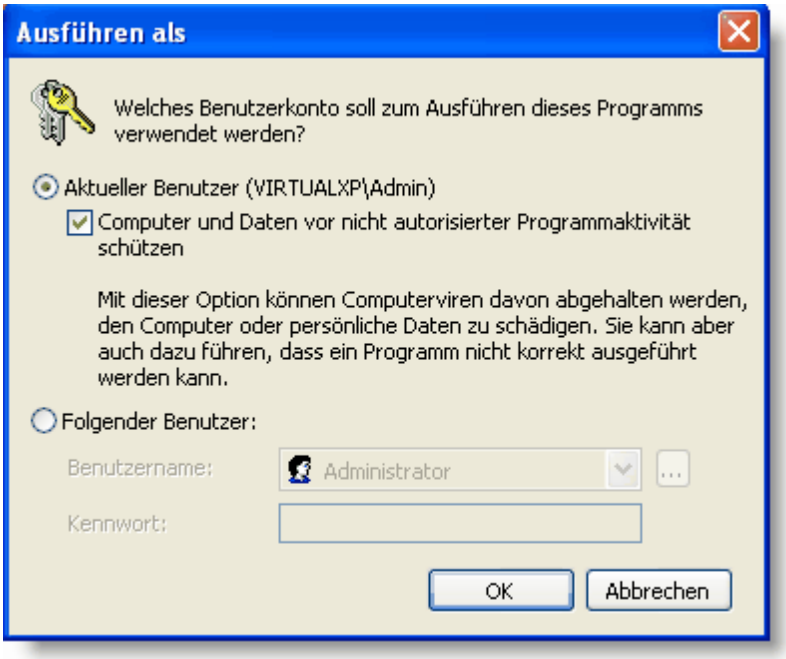
Auswahl sicher löschen

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.



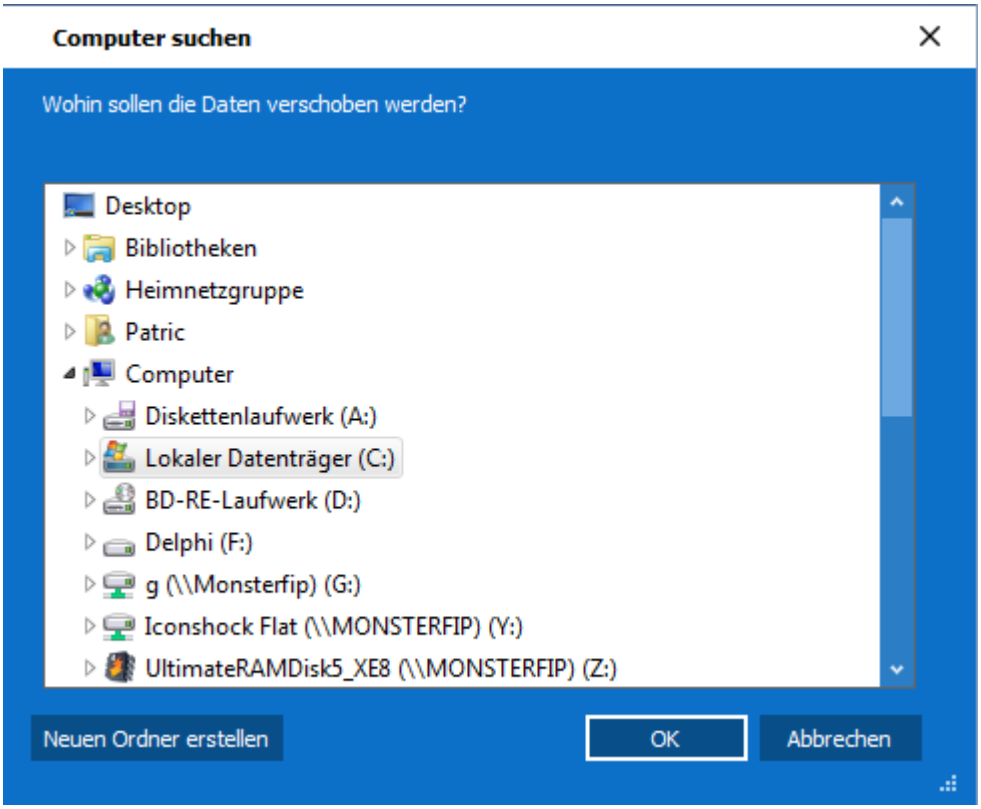
Entfernen Sie auf alle Fälle das Häkchen bei Computer und Daten vor nicht autorisierter Programmaktivität schützen! Entfernen Sie das Häkchen nicht, hat der Shredder keine Administratorrechte. Wenn Sie die Option Folgender Benutzer auswählen, loggen Sie sich bitte als Nutzer mit Administratorrechten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

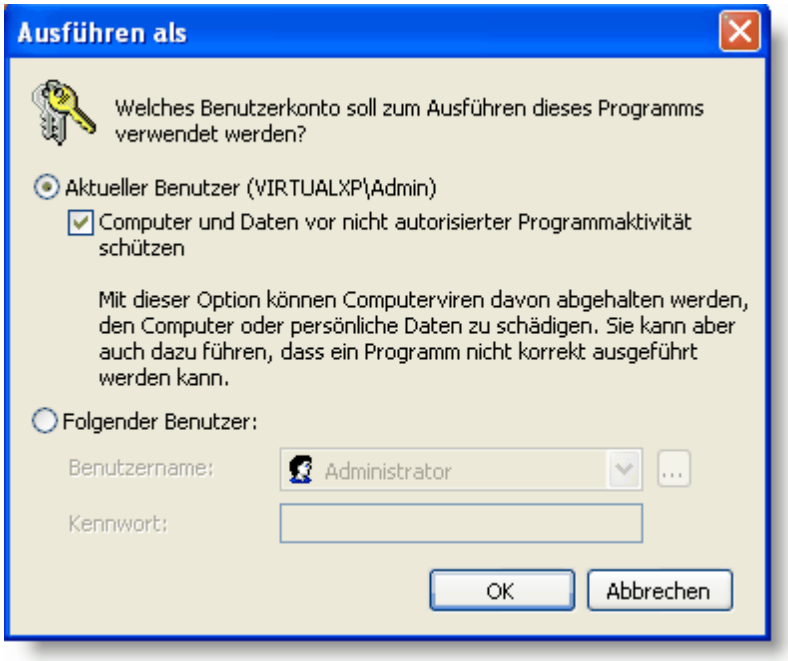


Wählen Sie die Datei(en) oder das Verzeichnis aus, welches Sie sicher verschieben möchten. Betätigen Sie die rechte Maustaste und rufen Sie die Funktion Auswahl sicher verschieben auf. Legen Sie das Ziel für die Dateien fest und betätigen Sie die OK *Schaltfläche*.

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-Variant wählen, sehen Sie ggf. 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!

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) für die Daten an ihrem Ursprungsort. Hier werden in hartnäckigen Fällen Dateien erst beim nächsten Rechnerstart gelöscht.

Kontextmenü im Infobereich (Systemtray)

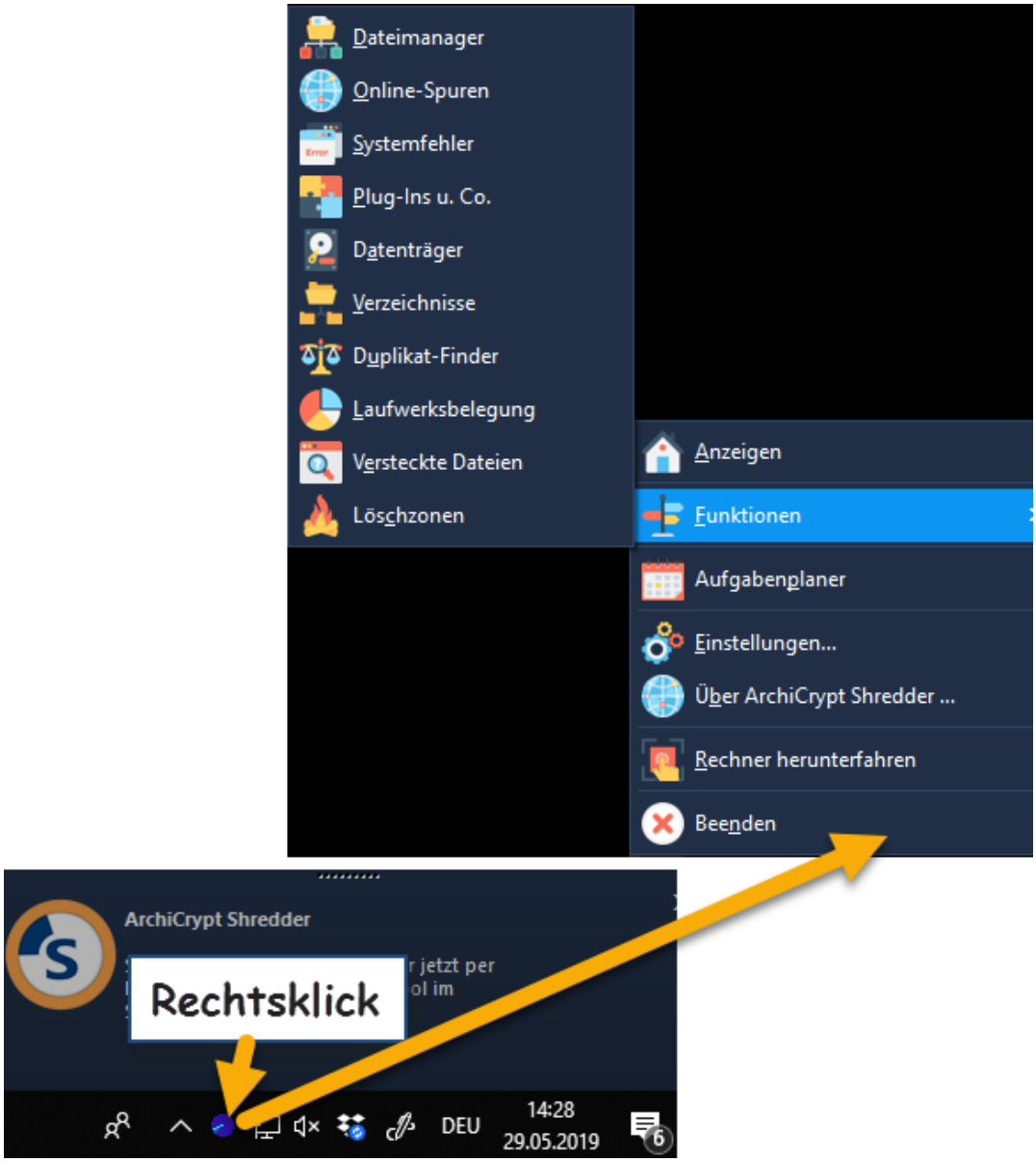
TIPP: Windows blendet das Symbol des Shredders in der Voreinstellung aus. Wenn Sie das Symbol immer sehen möchten, sehen Sie sich den Tipp dazu an[47].

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 System Herunterfahren, über die Sie Ihren *Rechner sofort herunterfahren* und komplett (*kein Energiesparmodus*) herunterfahren können. Die restlichen Funktionen rufen die entsprechenden Kategorien[35] von ArchiCrypt Shredder auf.

9 Forensik-Tool Miniaturansichten

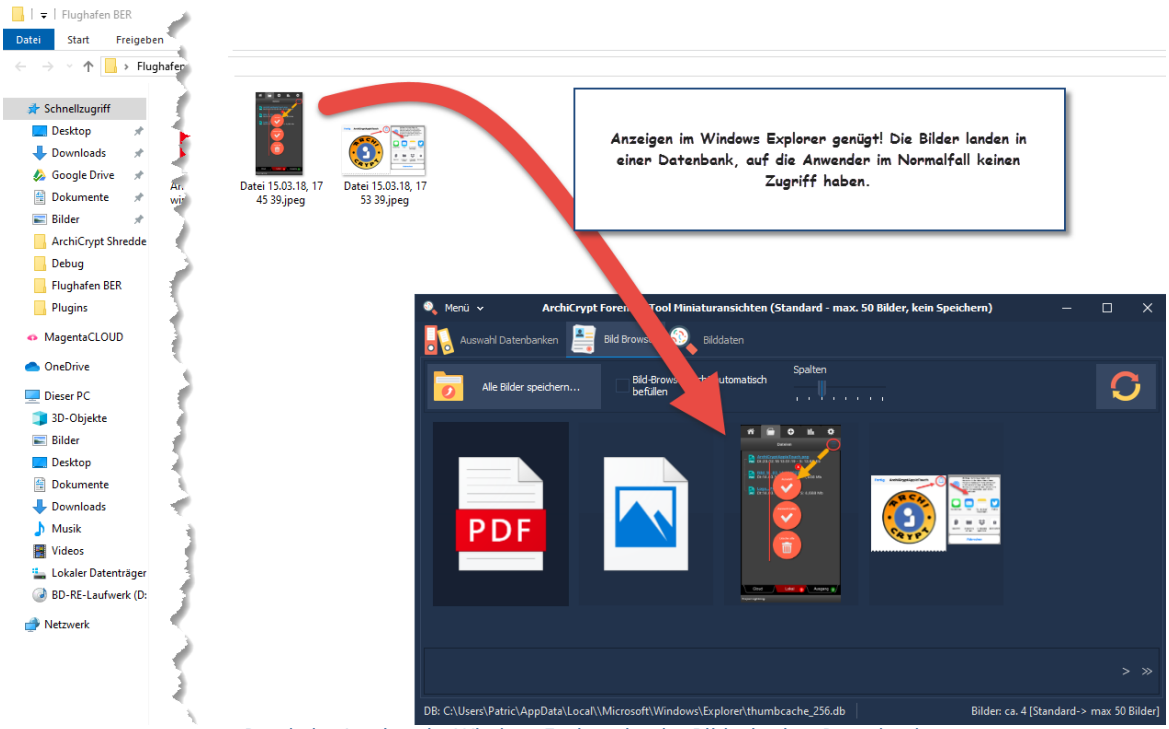
Falls Sie das Forensik-Tool in der Pro Version erworben haben, finden Sie hier eine allgemeine Anleitung[4] , wie Sie das Programm aktivieren

können.

Möchten Sie die Pro Version erwerben?

Die Einzelplatzlizenz finden Sie hier...
Die 3er Lizenz (Family) finden Sie hier...

Sobald in einem *Dateimanager* (zumeist Windows Explorer) der *Inhalt eines Verzeichnisses* angezeigt wird, erzeugt das Betriebssystem Windows Miniaturansichten der dort abgelegten Dateien. Das kann das Programmsymbol (*Icon*) sein, eine verkleinerte Version eines Bildes (*bzw. die skalierte Version*), die Vorschau für ein Video oder die erste Seite eines Dokuments.



Durch das Anzeigen im Windows Explorer landen Bilder in einer Datenbank

Was harmlos klingt und durchaus mit guter Absicht in das Windows Betriebssystem integriert wurde, kann zu einem Datenleck werden. Die Bilder sind mitunter von *sehr hoher Qualität* und lassen selbst Einzelheiten erkennen. Konstruktionszeichnungen, wichtige Listen und andere sensible

Daten werden als Kopie abgelegt, ohne dass der Anwender Einfluss darauf nehmen kann.

Werden die Informationen mit speziellen Werkzeugen wie ArchiCrypt Forensik-Tool Miniaturansichten ausgelesen, gelangen vertrauliche Informationen schnell in falsche Hände.

Forensik-Werkzeug

Die Bilddatenbanken können eine beachtliche Größe einnehmen. Bilder, Videos und Dokumente, die *längst vom Rechner* entfernt wurden, sind, zumeist ohne Wissen des Anwenders, auf unbestimmte Zeit weiter in der Datenbank enthalten. Die Funktionen zum Löschen dieser Datenbanken[108] (*Plug-In*) bietet ArchiCrypt Shredder. Im Shredder (*Vollversion*) kann man das Anlegen von Miniaturansichten sogar komplett stilllegen[108].

Das Forensik Tool Miniaturansichten kann die Inhalte der Miniaturbild-Datenbanken auslesen und anzeigen.

- Das Forensik-Tool gibt es in zwei Varianten.

Standard-Version

Die Standardversion wird grundsätzlich mit ArchiCrypt Shredder ausgeliefert. Mit ihr können Sie feststellen, ob es Bild-Datenbanken auf Ihrem Rechner gibt.

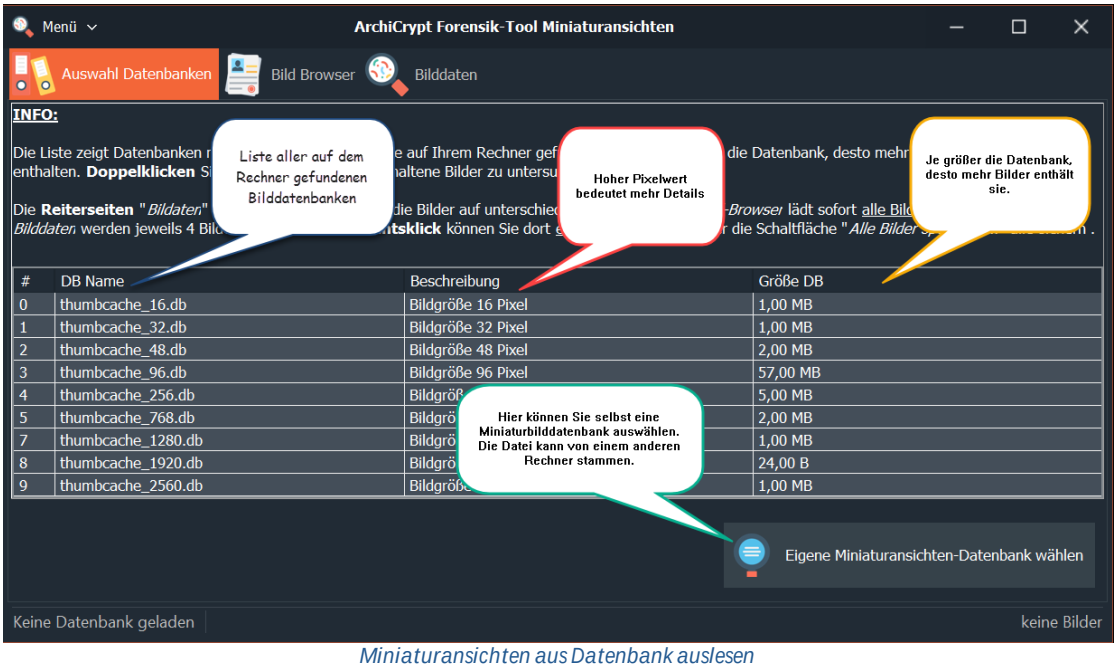
Die ersten 50 Bilder einer Datenbank können Sie sich ansehen. Weitere Bilder werden nicht angezeigt, ein Speichern der Dateien aus der Datenbank heraus ist nicht möglich. Die eingeschränkte Version kann jederzeit in eine registrierte Vollversion umgeformt werden.

Pro-Version

In der Pro Version können Sie sich alle Bilder in einer Datenbanken anzeigen lassen. Zudem können Sie dort abgelegte Bilder wieder *als Bilddatei* auf Ihrem Rechner *sichern*.

Das kann zum Beispiel dann sehr nützlich sein, wenn Sie ein Foto oder ein Bild versehentlich gelöscht haben.

Beim Start listet Forensik-Tool Miniaturansichten alle gefundenen Bild Datenbanken auf. In der Beschreibung sehen Sie die Größe der enthaltenen Bilder in Pixel. Je höher der Pixelwert, desto größer sind die in der Datenbank enthaltenen Bilder und desto mehr Details kann man ihnen entnehmen. Die Größe der Datenbank lässt Rückschlüsse auf die *Zahl der enthaltenen Bilder* zu.



#	DB Name	Beschreibung	Größe DB
0	thumbcache_16.db	Bildgröße 16 Pixel	1,00 MB
1	thumbcache_32.db	Bildgröße 32 Pixel	1,00 MB
2	thumbcache_48.db	Bildgröße 48 Pixel	2,00 MB
3	thumbcache_96.db	Bildgröße 96 Pixel	57,00 MB
4	thumbcache_256.db	Bildgröß	5,00 MB
5	thumbcache_768.db	Bildgrö	2,00 MB
7	thumbcache_1280.db	Bildgrö	1,00 MB
8	thumbcache_1920.db	Bildgrö	24,00 B
9	thumbcache_2560.db	Bildgröß	1,00 MB

Miniaturansichten aus Datenbank auslesen

Laden der Miniaturansichten erfolgt durch Doppellinksklick auf den Namen der Datenbank in der Tabelle.

Wenn Sie eine gültige *Datenbank von einem anderen Rechner* öffnen möchten, dann gehen Sie auf **Eigene Miniaturansichten Datenbank wählen**. Nachdem Sie die Dateiauswahl bestätigt haben, werden die enthaltenen Bilder geladen.

Format: Unterstützt werden Miniaturansichten Datenbanken von *Windows 7 bis Windows 10*.

Sobald die Datenbank geladen wurde, schaltet das Forensik-Tool Miniaturansichten auf die Registerkarte *Bild Browser*.

Bilder aus der Miniaturansichten Datenbank extrahieren und speichern

Bei sehr großen Datenbanken kann man ein Häkchen bei "**Bild-Browser nicht automatisch befüllen**" setzen. Die Bilder werden dann nicht sofort alle geladen, sondern erst dann, wenn man zur entsprechenden Stelle in der Datenbank navigiert. Die Navigation kann entweder über das Mausrad erfolgen oder über die *Pfeiltasten* unterhalb der Bilder.

Mit dem Regler **Spalten**, stellen Sie ein, wie viele Bilder in einer Zeile dargestellt werden sollen.

Die Registerkarte *Bilddaten* stellt die Bilder etwas anders dar und lädt diese grundsätzlich erst dann, wenn die Position in der Datenbank dies erfordert.

Unterhalb der Bildansicht bei Bilddaten können Sie ein *Verzeichnis* angeben, in welches die Bilder auf Befehl gespeichert werden sollen (*Pro Version*).

siehe auch: Daten die Windows heimlich sammelt 107

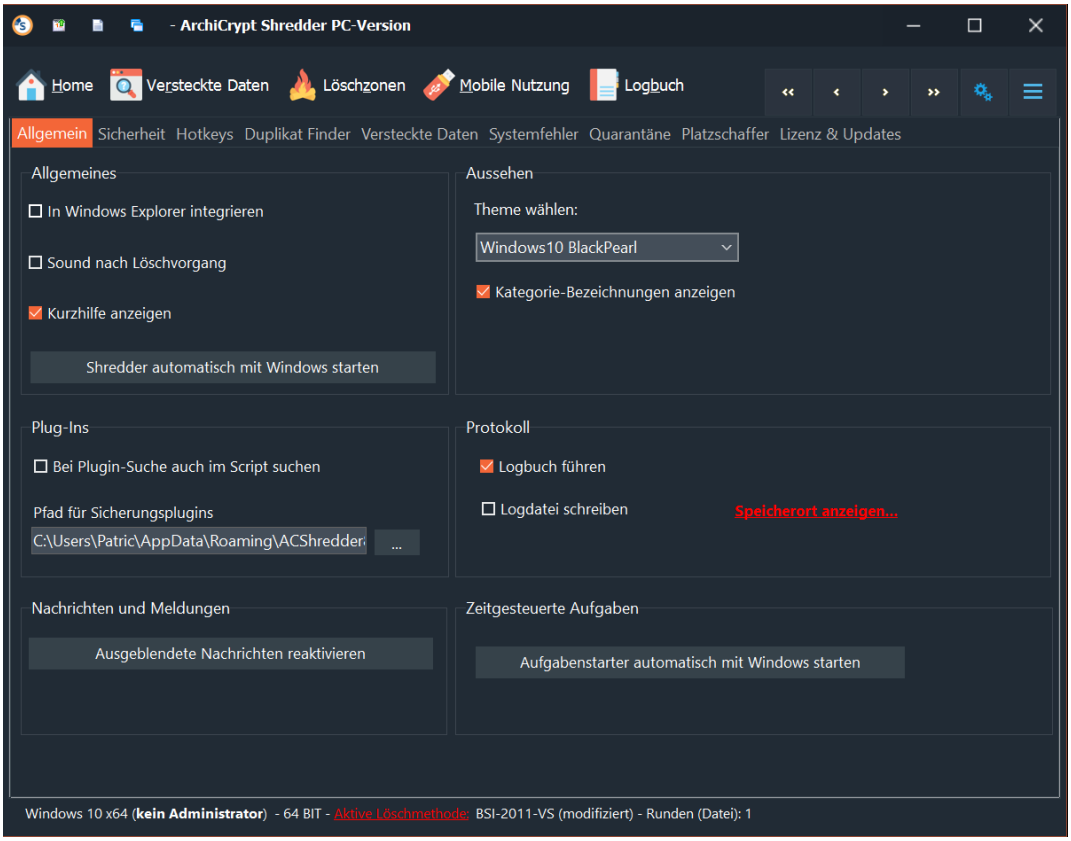
10 Einstellungen

10.1 Allgemeine Einstellungen

Einstellungen Allgemein

siehe auch Einstellungen

- Sicherheit 182
- Hotkeys 189
- Duplikat Finder 190
- Versteckte Daten 197
- System Fehlerbehebung 200
- Quarantäne Systemfehler 203
- Platzschaffer 204
- Lizenz & Updates 210



Allgemein

Allgemeines

In Windows Explorer integrieren

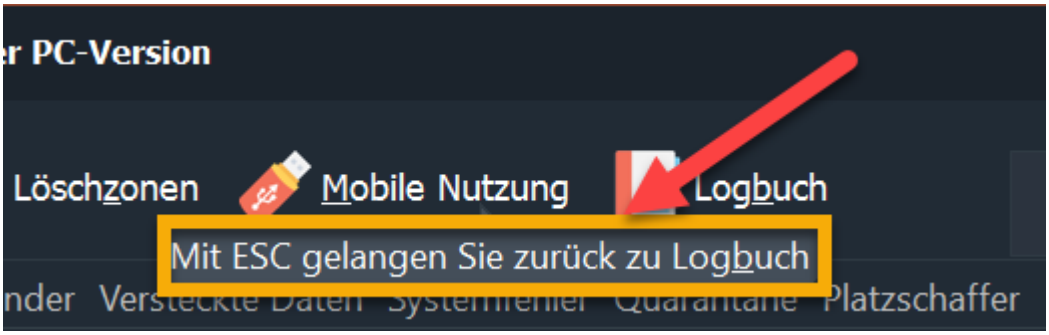
Ist diese Option aktiviert, haben Sie im *Windows Explorer* und alternativen Dateimanagern ein Kontextmenü, mit dem Sie direkt, ohne den Shredder starten zu müssen, Dateien sicher löschen oder von einem Speicherort auf den anderen sicher verschieben können. können Sie den Shredder im Kontextmenü des Windows Explorers (*Dateimanager*) aufrufen.

siehe dazu: Kontextmenü 165

Sound nach Löschvorgang

Bei ausgewählter Option erklingt nach jeder Löschaktion ein *akustisches Signal*.

Kurzhilfe anzeigen



Bei aktiver Option wird am oberen Rand ein Hinweistext eingeblendet, wenn ein Tastenkombination zur Verfügung steht.

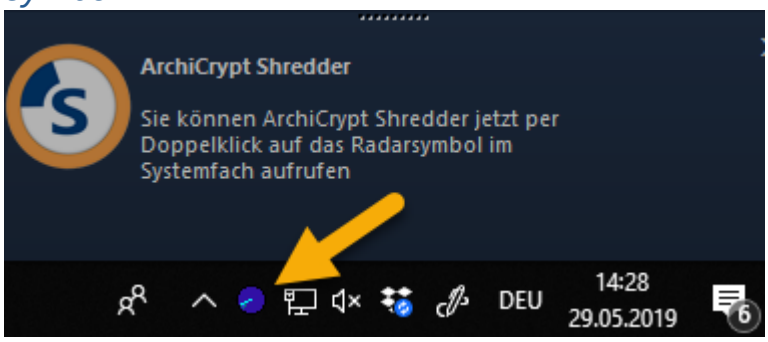
Shredder automatisch mit Windows starten

Bei eingeschalteter Option startet *ArchiCrypt Shredder automatisch bei jedem Anmelden des Nutzers* mit Administratorrechten ohne Rückfrage durch das System.

ArchiCrypt Shredder können Sie nach dem Start von Windows per Doppelklick auf das Radar-Symbol im s.g. Infobereich (*Systemtray*) aufrufen.

siehe auch: Kontextmenü Infobereich 171

Symbol:



Plug-Ins

Bei Plugin-Suche auch im Script suchen

Die Suchfunktion 99 bei den Plug-Ins beschränkt sich im Normalfall auf den Namen des Plug-Ins. Mit aktivierter Option wird die Suche auch im Plug-In (*dem Quelltext*) selbst durchgeführt.

Pfad für Sicherungsplugins
Zur Zeit nicht verwendet!

Nachrichten und Meldungen

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.

Sie können auf diese Weise auch Ihre eigene *Sortierung der Elemente auf der Home-Seite* **zurücksetzen**! Dies geschieht nach vorheriger Rückfrage.

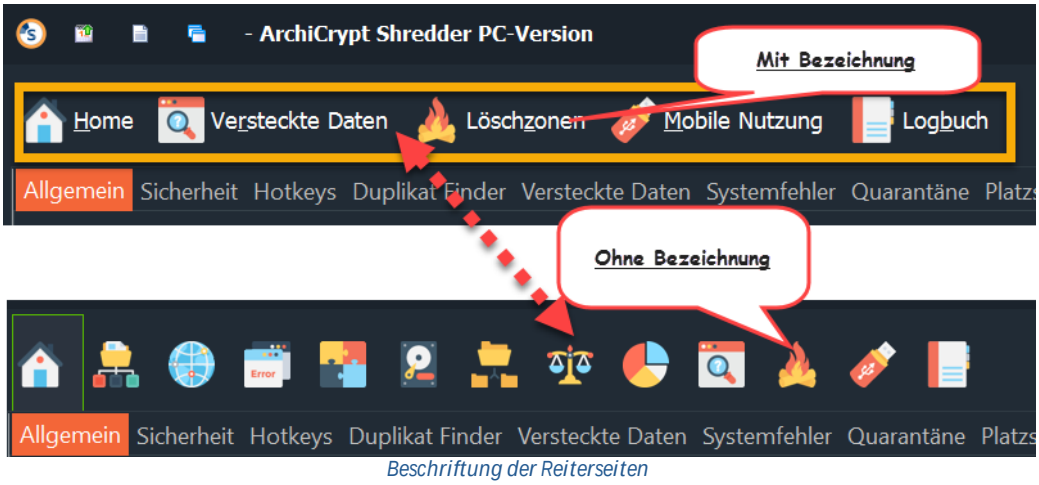
Aussehen

Theme wählen

ArchiCrypt Shredder bringt verschiedene *Styles* mit. Mit den Styles legen Sie das Aussehen von ArchiCrypt Shredder fest.

Einige Anteile von ArchiCrypt Shredder verwenden den *aktuellen Style* erst, wenn ArchiCrypt Shredder neu gestartet wurde.

Kategorie-Bezeichnung anzeigen
Beschriftung auf den Registerkarten ein- oder ausblenden.



Beschriftung der Reiterseiten

Protokoll

LogBuch führen

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

siehe dazu LogBuch 158

LogDatei schreiben

Auf Wunsch können alle Aktionen in einer Logdatei/Protokolldatei gespeichert werden. Die Datei trägt den Namen ACShredder.log. 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 aktivieren.

Zeitgesteuerte Aufgaben

Aufgabenstarter automatisch mit Windows starten

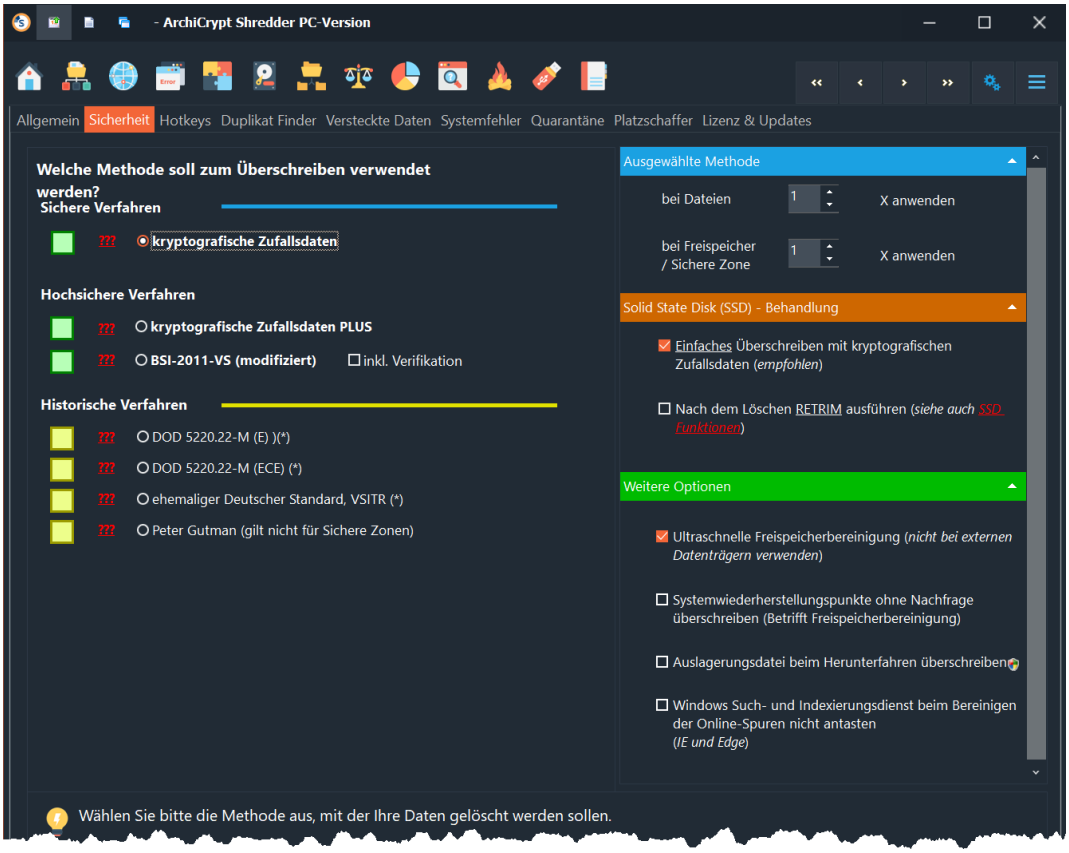
Lassen Sie den Aufgabenstarter mit Windows starten. Der Aufgabenstarter ist nötig, damit ArchiCrypt Shredder zeitgesteuerte Aufgaben[142] ausführen kann.

10.2 Löschverfahren und Sicherheit

Einstellungen Sicherheit

siehe auch Einstellungen

- Allgemein[177]
- Hotkeys[189]
- Duplikat Finder[190]
- Versteckte Daten[197]
- System Fehlerbehebung[200]
- Quarantäne Systemfehler[203]
- Platzschaffer[204]
- Lizenz & Updates[210]



Verfahren Sicheres Löschen - Kryptografische Zufallsdaten, BSI Löscheverfahren, VSITR, Gutman und andere

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 kryptografische Zufallszahlen[47] zu wählen und diese *1 X* anwenden zu lassen. In Hochsicherheitsumgebungen und bei entsprechenden Anforderungen sollten Sie die vom Bundesamt für Sicherheit in der Informationstechnik (*BSI*) empfohlene BSI-2011-VS[48] Methode einsetzen.

Bitte beachten Sie hinsichtlich der Sicherheit die Hinweise zu SSD[53] (Solid State Disk)!

Solid State Disk Behandlung

Hinweise zu den Besonderheiten einer so genannten Solid State Disk (SSD), finden Sie im Kapitel SSD Funktionen[53]. Dort werden auch die Begriffe TRIM[55] und RETRIM[55] erläutert. In den Einstellungen legen Sie bei *Solid State Disk Behandlung* fest, wie ArchiCrypt Shredder immer dann vorgehen soll, wenn eine Datei oder Strukturen auf einer SSD sicher gelöscht werden soll. Es empfiehlt sich grundsätzlich, Daten mit einfachem Überschreiben zu löschen. RETRIM[55] ist optional und kann zum Beispiel über die SSD-Funktionen[65] regelmäßig manuell ausgeführt werden.

Welche Methode soll zum Überschreiben verwendet werden?

Empfehlung:

Wenn Sie auf Nummer Sicher gehen wollen, setzen Sie BSI-2011-VS[48] ein und Berücksichtigen Sie die Besonderheiten bei Daten auf einer SSD[183]. Hier sollten Sie dann auch das RETRIM[55] aktivieren.

Wenn Sie ein hohes Maß an Sicherheit benötigen, setzen Sie kryptografische Zufallszahlen[47] (*Standard Löschverfahren*) ein und wählen Sie eine Rundenzahl von 1. Die historischen Verfahren[185] machen inzwischen keinen Sinn mehr. Sie sind äußerst zeitintensiv und führen in jeder Runde zahlreiche Schreiboperationen auf dem Speichermedium aus, ohne die Sicherheit zu erhöhen. Im Zusammenhang mit den SSD Laufwerken führen die historischen Verfahren oder hohe *Rundenzahlen* zu einem *höheren Verschleiß der SSD*! Die Speicherdichte klassischer Medien, die auf Magnetisierung basieren, sind inzwischen derart hoch, dass man mit s.g. *Rasterkraftmikroskop* keine verwertbaren Informationen mehr extrahieren kann.

Standard Löschverfahren (Sicher)

Kryptografische Zufallsdaten

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

(siehe Überschreiben mit kryptografischen Zufallsdaten[47])

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!

Kryptografische Zufallsdaten Plus

Wie beim Verfahren Kryptografische Zufallsdaten, wird jedes Byte mit einem Zufallsbyte überschrieben. In einem angehängten zweiten Durchlauf werden die Daten mit dem Muster 0xFF überschrieben.

(siehe Überschreiben mit kryptografischen Zufallsdaten 47)

Löschen im Hochsicherheitsumfeld

BSI-2011-VS (modifiziert)

In der im *April 2016* vom Bundesamt für Sicherheit in der Informationstechnik (*BSI*) herausgegebenen Technischen Leitlinie "Anforderung zum Überschreiben von Datenträgern - BSI TL-03423" werden zwei Verfahren zum Überschreiben magnetischer Datenträger beschrieben, von denen das Verfahren BSI-2011 48 in leicht modifizierter Form in ArchiCrypt Shredder umgesetzt ist.

Das Verfahren setzt dabei intern sehr rechenintensive Verfahren ein, wodurch das Überschreiben entsprechend zeitaufwendig ist. Wird zusätzlich Verifikation (*war das Überschreiben erfolgreich?*) eingesetzt, steigt der Zeitbedarf nochmals erheblich an.

Historische Löschverfahren

Bedeutet historisch, dass diese Verfahren unsicher sind?

JEIN!

Die Verfahren setzen oft viele Runden und vor allem meist feste

Muster ein. Die hohe interne Rundenzahl sorgt für erheblichen und, im Zusammenhang mit neueren Festplatten, für unnötigen Zeitbedarf. Nimmt man das *Peter Gutman Verfahren*, sind alleine 35 Runden zu durchlaufen, in denen bestimmte Muster auf den Datenträger übertragen werden.

Aus 100 Megabyte zu überschreibenden Daten werden so 3,5 Gigabyte.

Die *festen Muster* sorgen dafür, dass man theoretisch ein Differenzbild erzeugen kann (*sehr hoher Aufwand*). Man "zieht" sozusagen die Muster vom aktuellen Zustand "ab" und kann so auf die ursprünglichen Daten schließen. Eine potenzielle Sicherheitslücke, die in hochsensiblem Umfeld nicht akzeptabel ist.

DoD 5220.22-M (E) (historisch*) 185

Insgesamt wird jedes BYTE der Originaldatei *3 MAL* mit einem bestimmten BYTE-Wert überschrieben.
(genaue Beschreibung siehe DoD5220.22-M 50)

DoD 5220.22-M (ECE) (historisch*) 185

Insgesamt wird jedes BYTE der Originaldatei *7 MAL* mit einem bestimmten BYTE-Wert überschrieben.
(genaue Beschreibung siehe DoD5220.22-M 50)

Der deutsche Standard (VS-IT-Richtlinien - VSITR) (historisch*) 185

Insgesamt wird jedes BYTE der Originaldatei *7 MAL* mit einem bestimmten BYTE-Wert überschrieben.
(genaue Beschreibung siehe VSITR) 51

Peter Gutman (historisch*) 185

Jedes BYTE der Originaldatei wird in *35 Durchläufen* mit ganz bestimmten BYTE-Werten überschrieben.

(genaue Beschreibung siehe Gutman[51]). 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 historische[185] Löschmethoden

Andere historische 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.

Auslagerungsdatei beim Herunterfahren überschreiben

Sie können die Auslagerungsdatei (pagefile.sys) beim Herunterfahren des Rechners überschreiben lassen.
Das Überschreiben erfolgt in einem Durchgang in dem NULLEN geschrieben werden. Das Herunterfahren des Rechners wird dabei verlangsamt.

(siehe auch Schwachstellen/Tipps[56])

Systemwiederherstellungspunkte ohne Nachfrage überschreiben

Die modernen 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, *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. Wenn Sie die Freispeicherbereinigung zeitgesteuert ausführen lassen, sollten Sie die Option aktivieren, da die Freispeicherbereinigung ansonsten NICHT ausgeführt wird!

Ultraschnelle Freispeicherbereinigung (*nicht bei externen Datenträgern verwenden*)

Falls aktiviert, nutzt ArchiCrypt Shredder einen Trick und "missbraucht" das Betriebssystem dazu, in Leerlaufzeiten den freien Speicher mit NULLEN zu überschreiben. Dies hat den Effekt, dass man viel schneller wieder mit dem Rechner und ArchiCrypt Shredder arbeiten kann. Am Durchsatz und der tatsächlich zu schreibenden Datenmenge, ändert sich natürlich nichts. **Das Verfahren ist jedoch weniger Sicher als einmaliges Überschreiben mit Zufallsdaten.**

Windows Such- und Indexierungsdienst beim Bereinigen der Online-Spuren nicht antasten

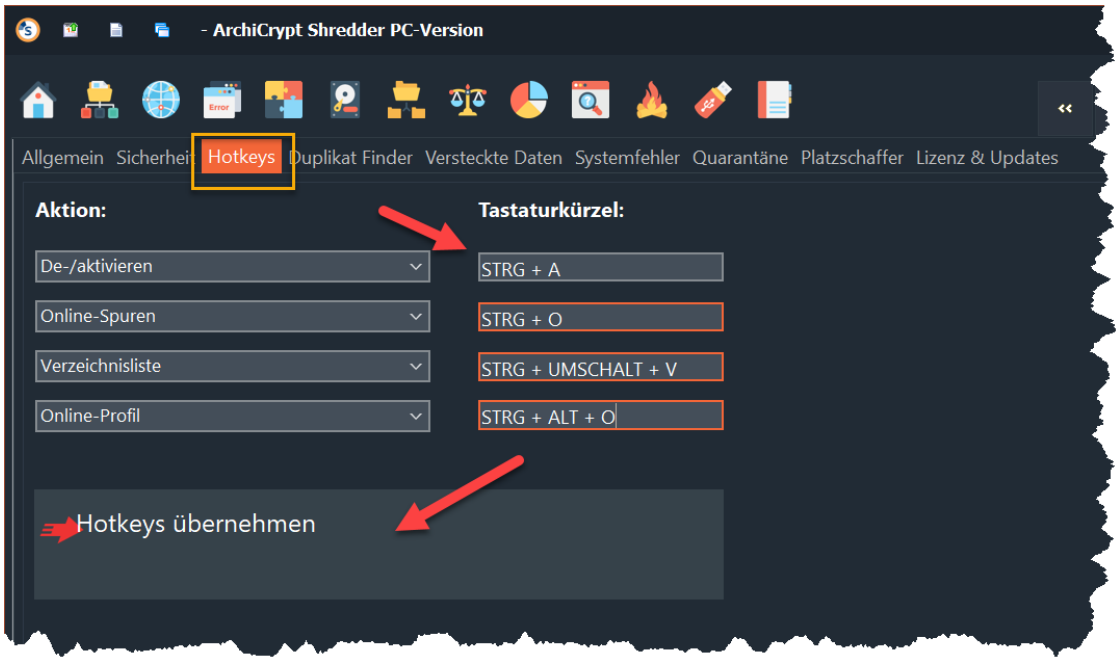
Der Windows Dienst blockiert bestimmte Dateien in den Windows Internet Explorer und der Edge Browser bestimmte Daten ablegen. Der Dienst muss beendet werden, um direkten Zugriff auf die Inhalte zu haben. Wird der Dienst nicht gestoppt, erfolgt der Zugriff indirekt. Dabei kann nicht zu 100% garantiert werden, dass die Daten nicht mehr rekonstruiert werden können. Es können Dateien aus dem Internet und Adressen besuchter Internetseiten auf dem Rechner verbleiben.

10.3 Hotkeys

Einstellungen Hotkeys

siehe auch Einstellungen

- Allgemein 177
- Sicherheit 182
- Duplikat Finder 190
- Versteckte Daten 197
- System Fehlerbehebung 200
- Quarantäne Systemfehler 203
- Platzschaffer 204
- Lizenz & Updates 210



Tastaturkürzel für schnelle Ausführung von Shredder-Kommandos

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 Löschzonen:
Startet die Überwachung der Sicheren Löschzonen

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[55] aktiv, werden die Verzeichnisse in der Verzeichnisliste bereinigt.
Sofern Plugins ausführen[96] aktiv, werden ausgewählte Plugins ausgeführt.

Hotkey Verzeichnisliste:
Aktuelle Verzeichnisliste[55] wird abgearbeitet

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

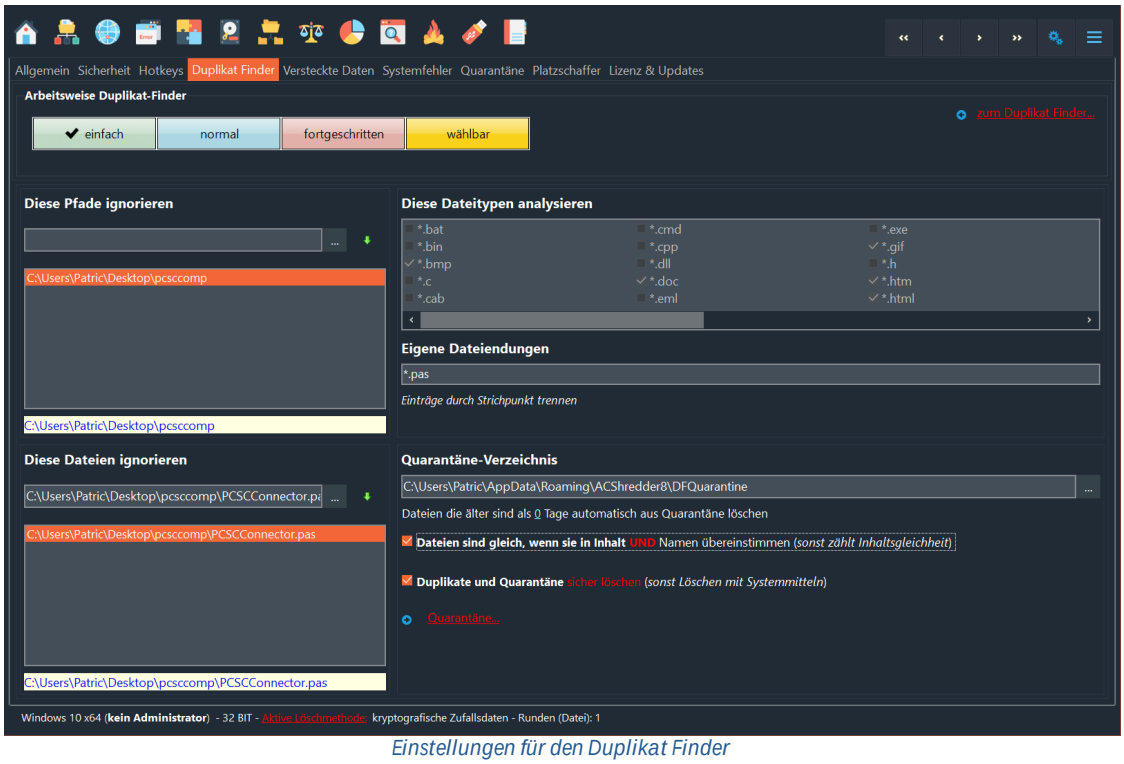
Hotkey Plugin-Profil:
Aktuelles Plugin-Profil[96] wird abgearbeitet

10.4 Duplikat Finder

Einstellungen Duplikat Finder[124]

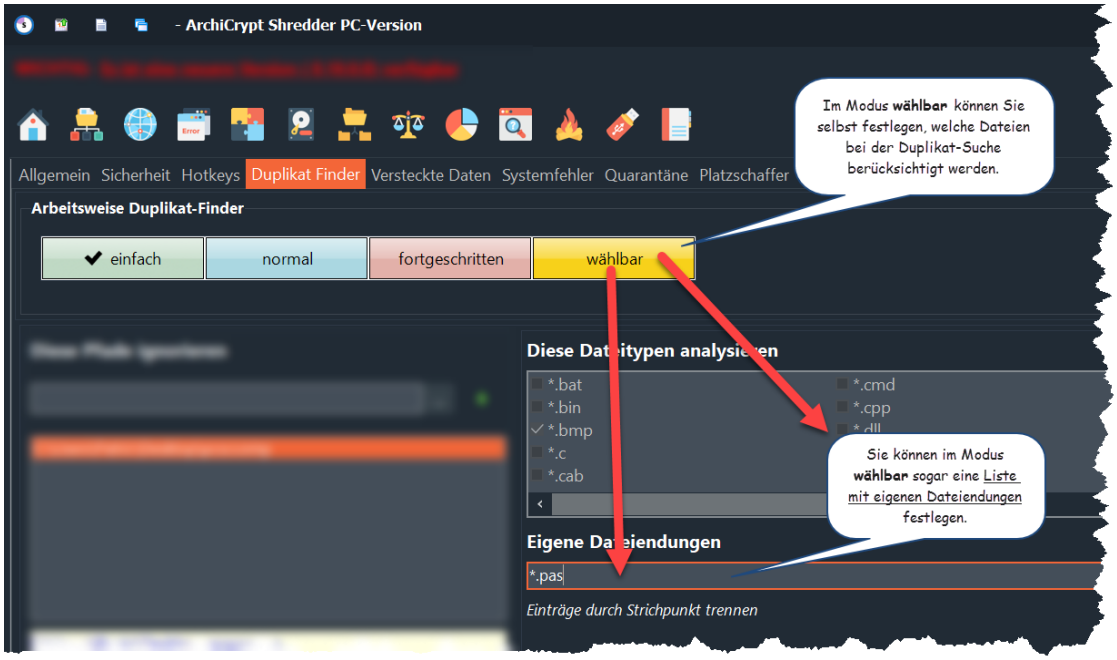
siehe auch Einstellungen

- Allgemein[177]
- Sicherheit[182]
- Hotkeys[189]
- Versteckte Daten[197]
- System Fehlerbehebung[200]
- Quarantäne Systemfehler[203]
- Platzschaffer[204]
- Lizenz & Updates[210]



Einstellungen für den Duplikat Finder

Die verschiedenen Analyse-Modi des Duplikat Finders



Legen Sie fest, welche Dateien der Duplikat-Finder berücksichtigen soll

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

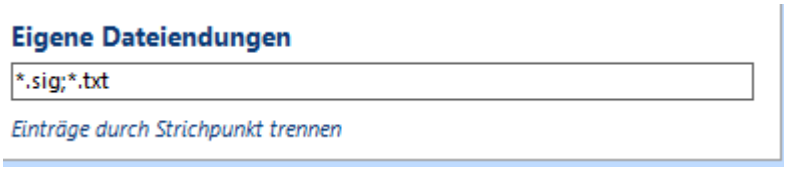
Experte

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.

wählbar

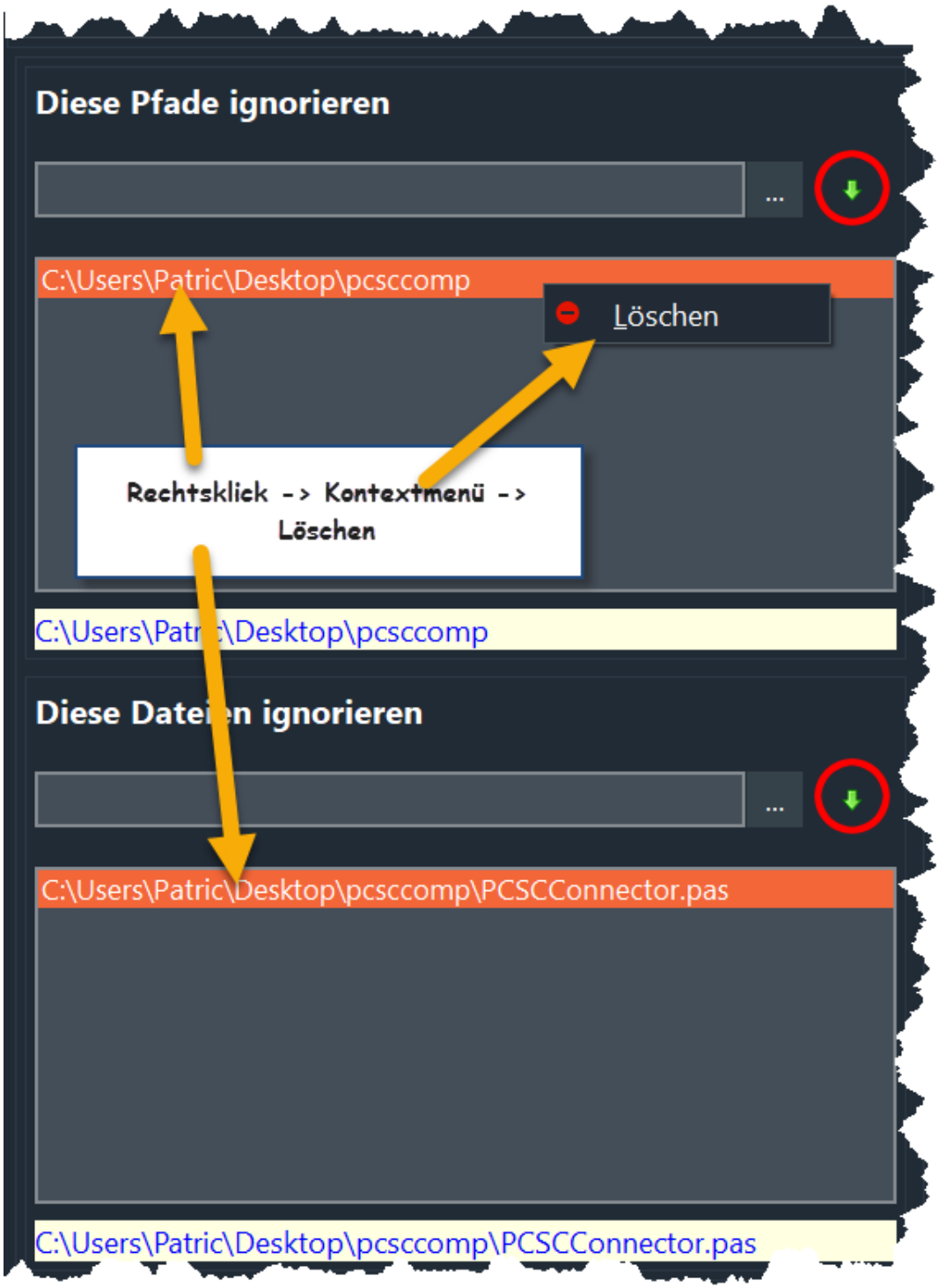
Sie können die vordefinierten Dateitypen *beliebig auswählen* und *eigene Dateimasken/-endungen* in das Feld Eigene Dateiendungen eingeben. Wenn Sie mehrere solcher Masken festlegen, trennen Sie diese bitte mittels Strichpunkt.

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

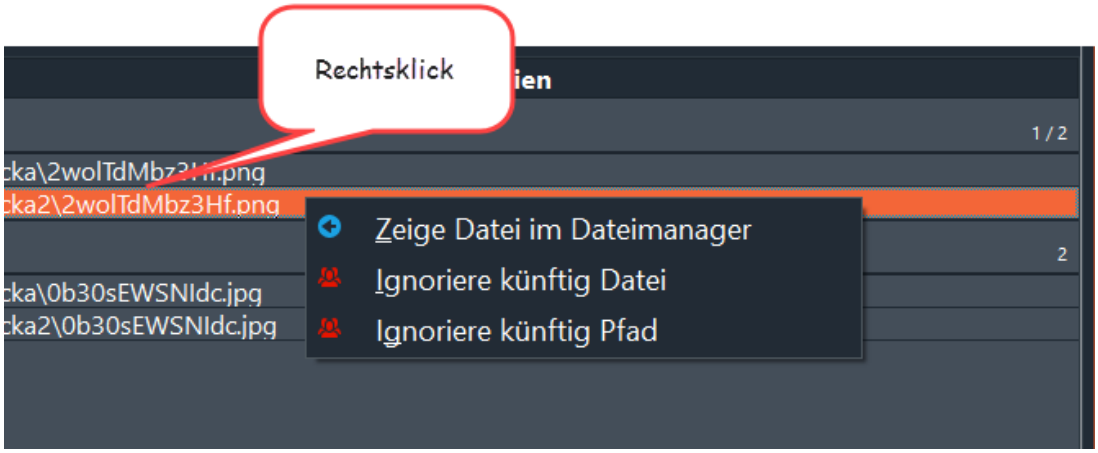


So schließen Sie bestimmte Verzeichnisse und Dateien von der Analyse durch den Duplikat Finder aus

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,



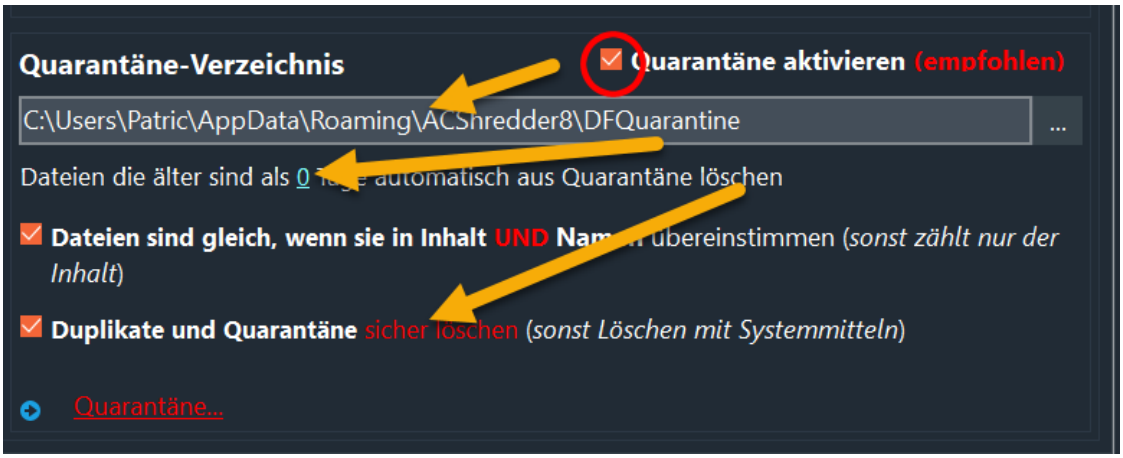
oder, Sie rufen mit der rechten Maustaste das *Kontextmenü* eines Eintrags in der Tabelle mit den Ergebnissen[129] auf und wählen die entsprechende Funktion.



Sie können einen Eintrag aus der Liste zu ignorierender Pfade/Dateien wieder entfernen, indem Sie ihn mit der rechten Maustaste anklicken und Löschen wählen.

Quarantäne und Quarantäneverzeichnis

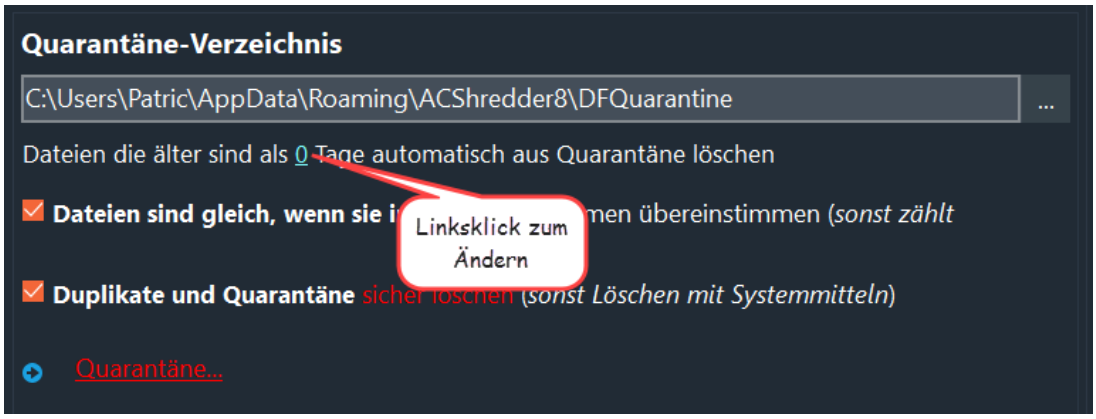
Duplikate können und **sollten** zunächst in einem Quarantäne-Verzeichnis gesichert werden.



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[129] wieder an den ursprünglichen Ort zurückspielen.

So bereinigen Sie die Quarantäne automatisch



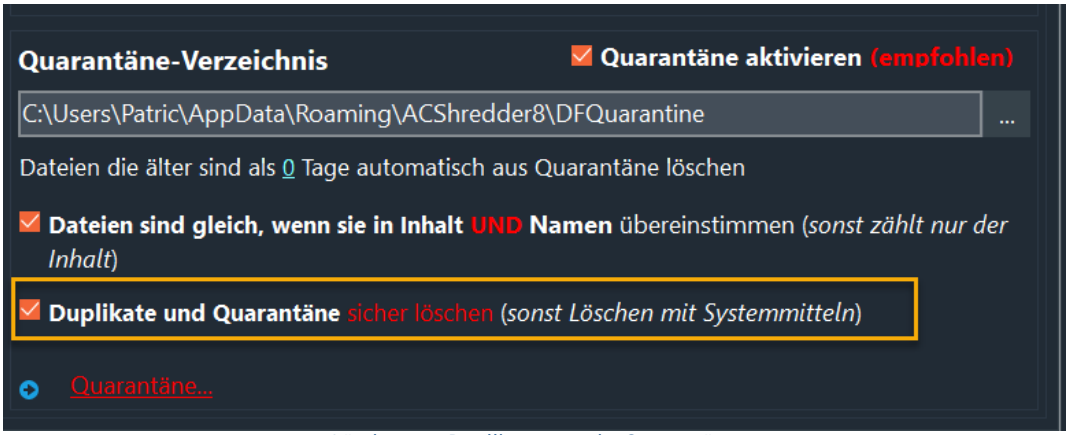
Oft vergisst man, Dateien manuell aus der *Quarantäne* zu *entfernen*. Sie können in der Einstellung zum Duplikat Finder festlegen, dass ArchiCrypt Shredder bei jedem Start Einträge automatisch aus der Quarantäne entfernt, die älter als X Tage sind.

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

Um den Wert zu ändern, klicken Sie bitte auf die Zahl und tragen Sie den neuen Wert ein.

Löschmethode für Duplikate und Dateien in Quarantäne

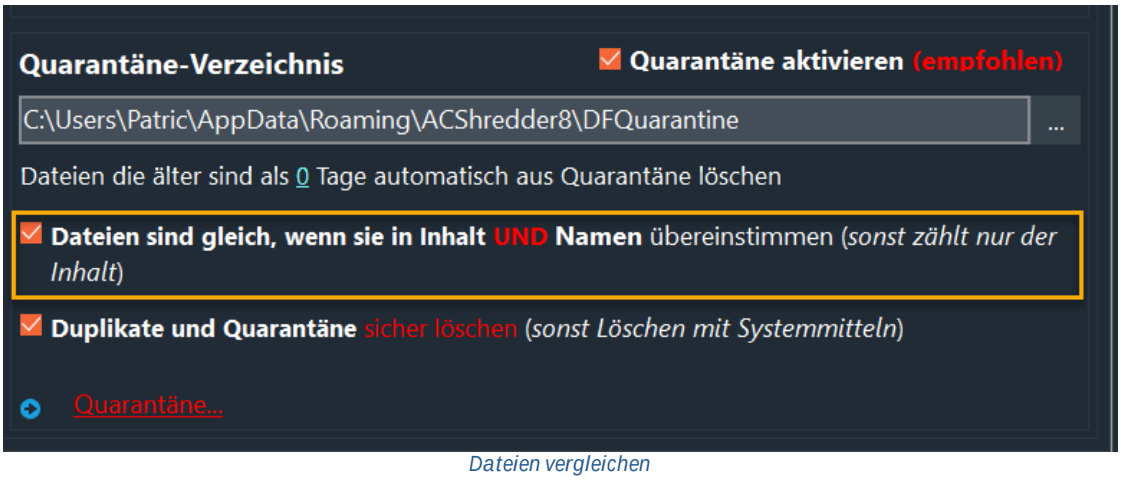
Duplikate und Dateien der Quarantäne werden in der Voreinstellung sicher gelöscht. Wenn Sie bei Duplikate und Quarantäne sicher löschen kein Häkchen setzen, werden die Daten mit Systemmitteln (*schneller, aber ggf. wieder herstellbar*) gelöscht.



Löschen von Duplikaten aus der Quarantäne

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, weil sie nach dem Kopieren umbenannt wurden. Sie können jedoch festlegen, dass *nur die Dateien als Duplikat* gelten, die neben *gleichem Inhalt* auch den *gleichen Dateinamen* besitzen (Dateien sind gleich, wenn sie in Inhalt **und** Namen übereinstimmen).



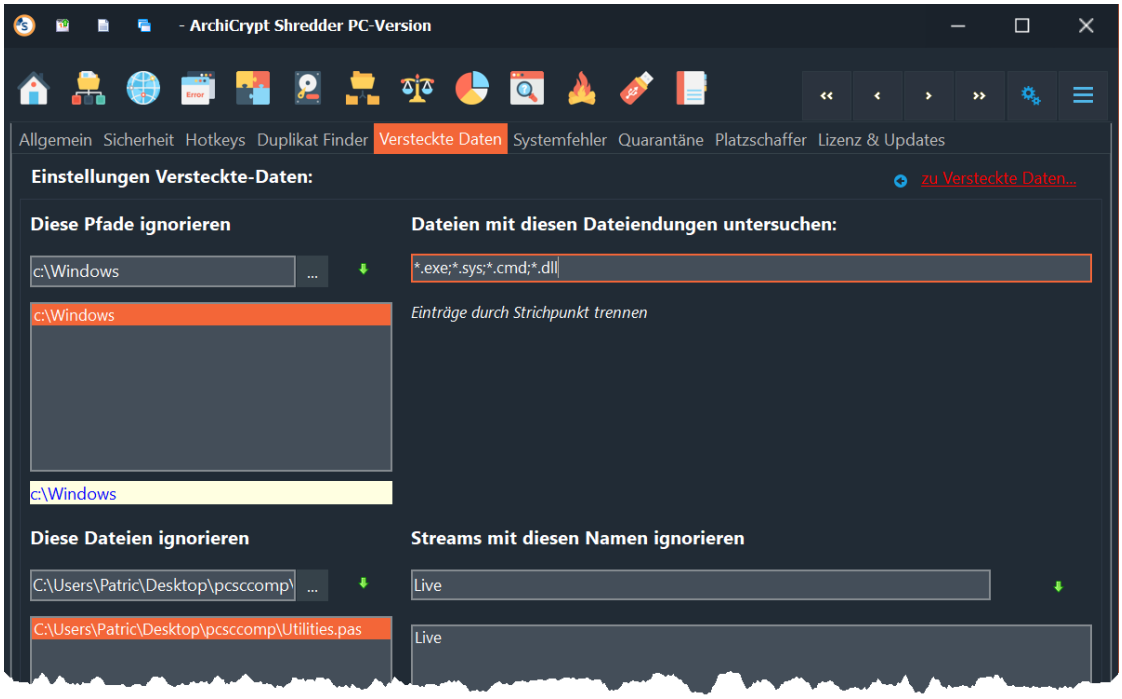
Dateien vergleichen

10.5 Verborgene Daten

Einstellungen Versteckte Daten[138]

siehe auch Einstellungen

- Allgemein[177]
- Sicherheit[182]
- Hotkeys[189]
- Duplikat Finder[190]
- Versteckte Daten[197]
- System Fehlerbehebung[200]
- Quarantäne Systemfehler[203]
- Platzschaffer[204]
- Lizenz & Updates[210]

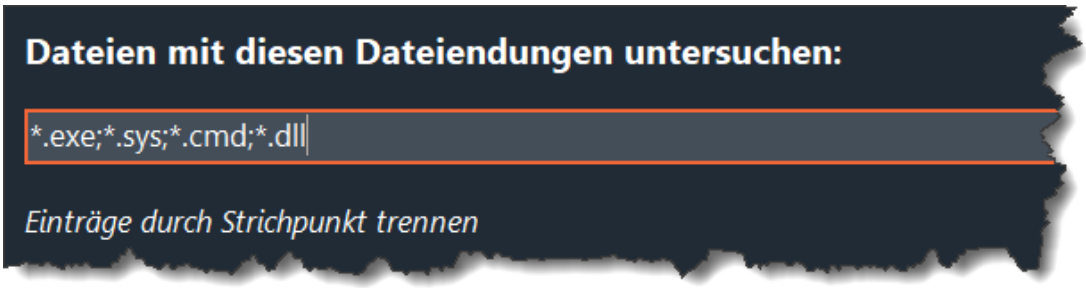


Alternative Datenströme - Alternate Datastreams

So legen Sie fest, welche Dateien untersucht werden sollen

In den Einstellungen können Sie unter "Dateien mit diesen Dateiendungen untersuchen" festlegen, welche Dateien ArchiCrypt

Shredder auf das Vorhandensein von versteckten Daten (*Alternate Data Stream*) untersuchen soll.



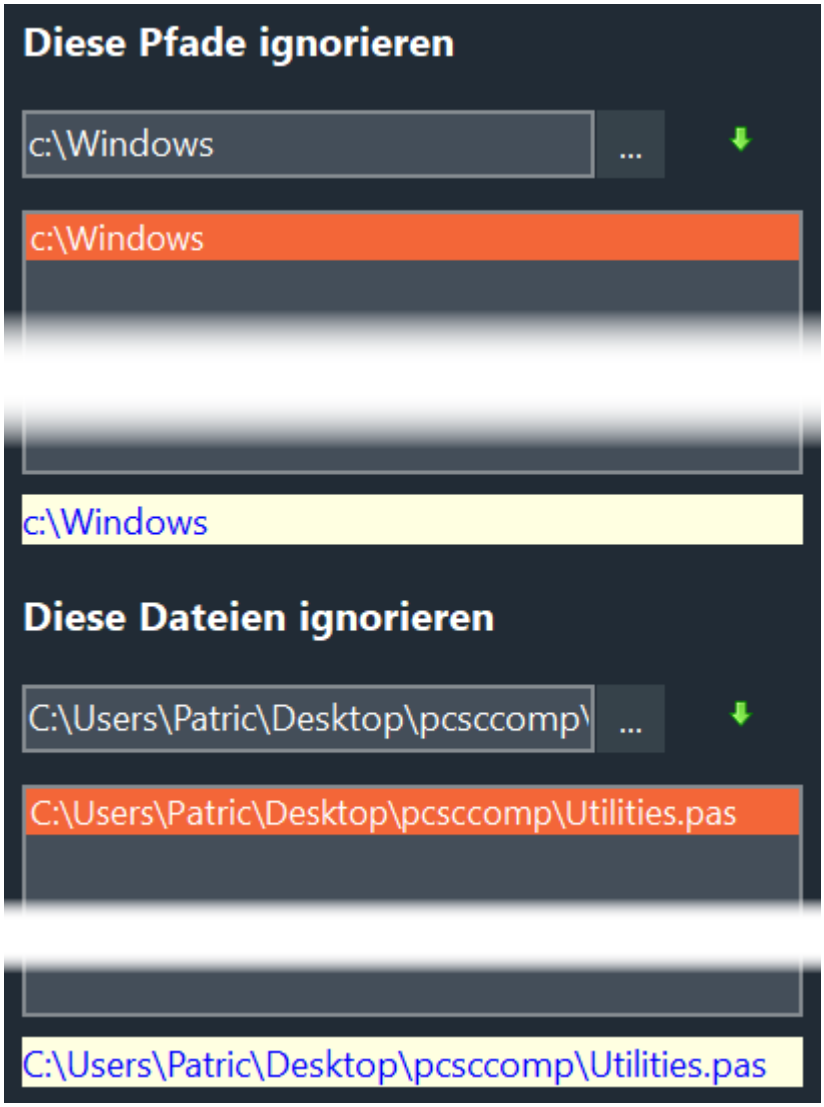
Wenn Sie mehrere solcher Masken festlegen, trennen Sie diese bitte *mittels Strichpunkt*. Durch Angabe von * als Maske werden alle Dateien mit in die *Analyse* einbezogen.

Beispiel:

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

So schließen Sie bestimmte Dateien und Verzeichnisse von der Analyse aus

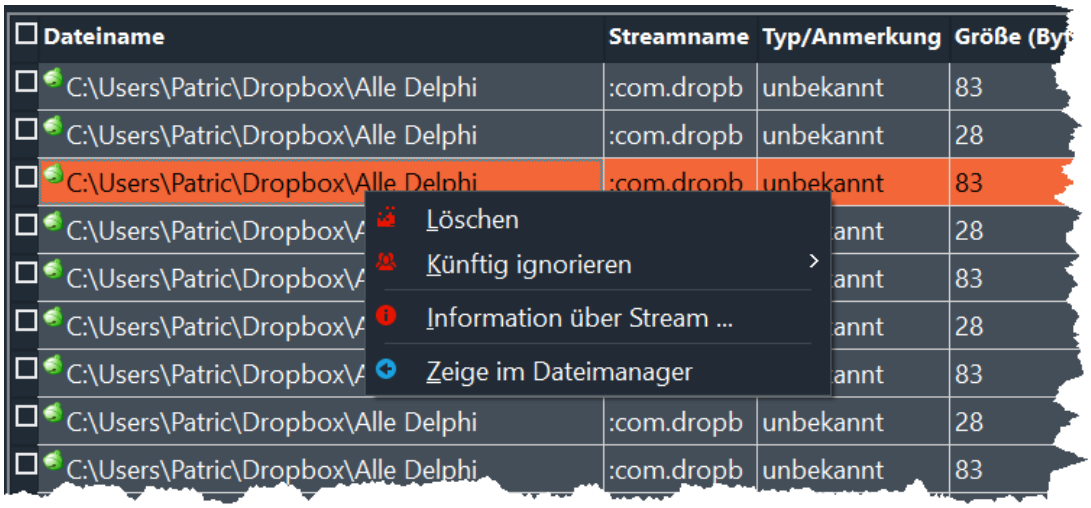
Es kann durchaus sinnvoll sein, bestimmte *Dateien und oder Verzeichnisse* nicht mit in die *Analyse* einzubeziehen. Dazu können Sie einen Pfad oder eine Datei gezielt im Windows Dialog in den Einstellungen auswählen und anschließen über die grüne Pfeil-nach-unten Schaltfläche in die entsprechende Liste 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.



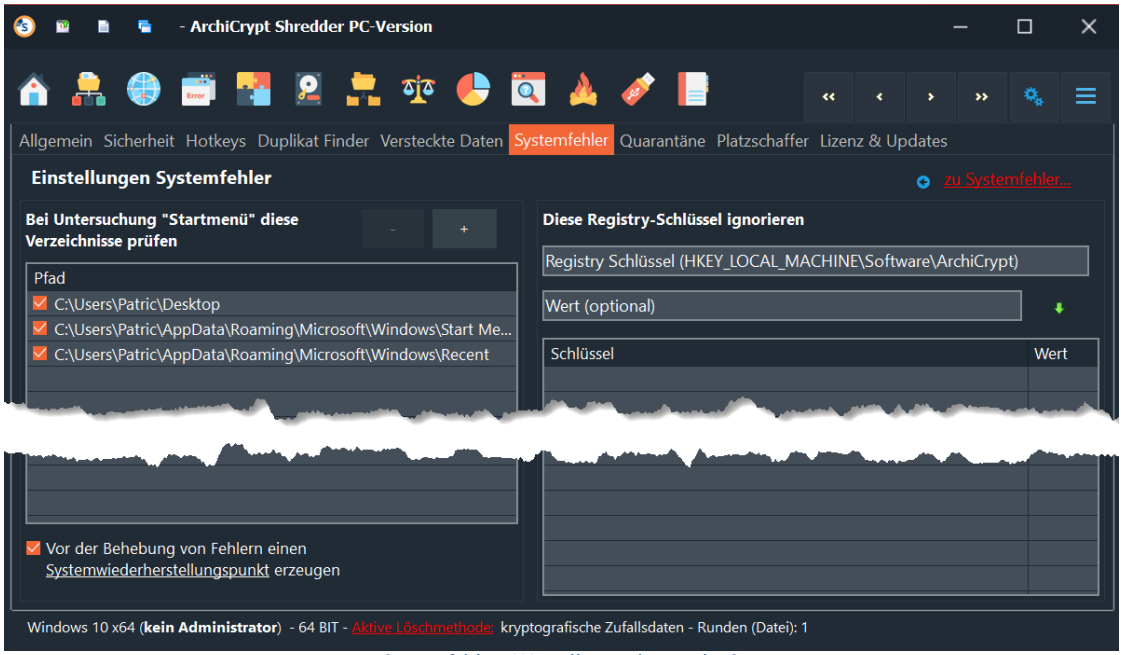
HINWEIS: Sie können Datenströme, die von *Antivirensoftware* stammt, gefahrlos wieder entfernen. Allerdings dauert der nächste Scan-Durchlauf des Virenscanners dann evtl. wieder länger.

10.6 Systemfehler

Einstellungen Systemfehler[110]

siehe auch Einstellungen

- Allgemein[177]
- Sicherheit[182]
- Hotkeys[189]
- Duplikat Finder[190]
- Versteckte Daten[197]
- Quarantäne Systemfehler[203]
- Platzschaffer[204]
- Lizenz & Updates[210]



Systemfehler - Wo soll gesucht werden?

So erstellen Sie vor der Beseitigung von Systemfehlern einen Systemwiederherstellungspunkt

Bei der *Beseitigung* eines mutmaßlichen *Fehlers* kann es in der Folge zu Fehlern beim Arbeiten[122] mit dem Computer kommen.

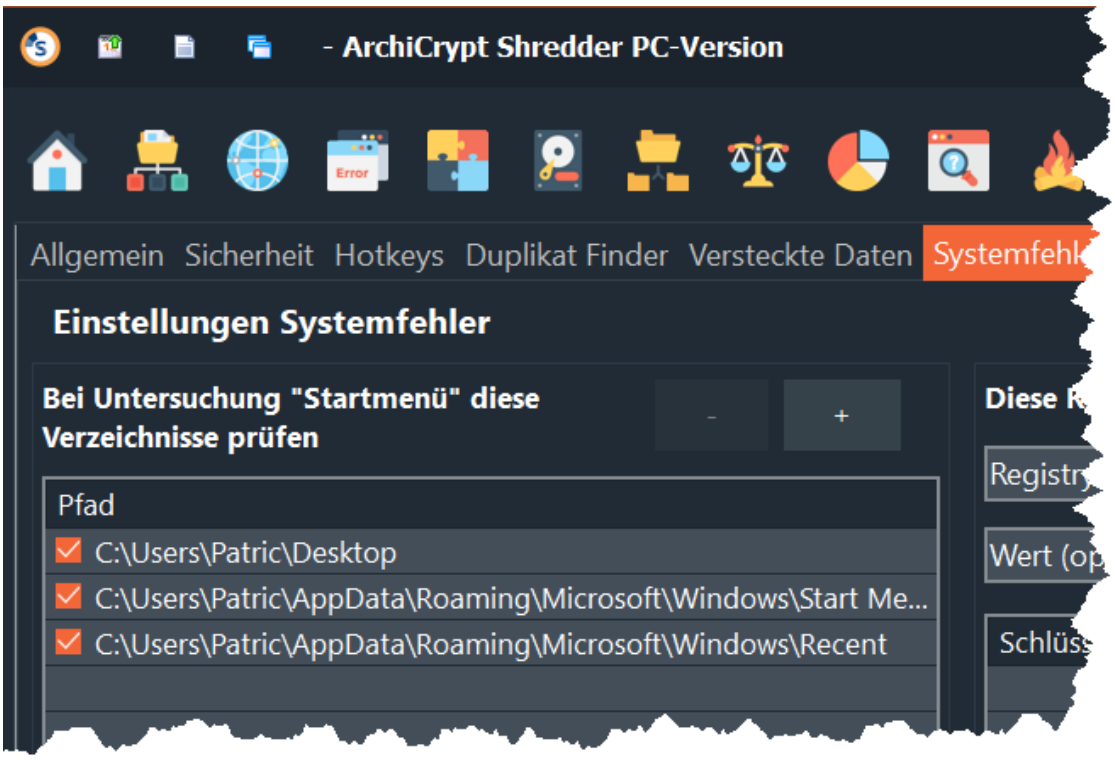
Mit Hilfe des Betriebssystems können Sie so genannten *Wiederherstellungspunkte* erzeugen. Diese Sicherungen helfen Ihnen im schlimmsten Fall weiter. Aktivieren Sie einfach die Option Vor der Behebung von Fehlern einen Systemwiederherstellungspunkt erzeugen.

Bevor tatsächlich Änderungen am Rechner vorgenommen werden (Reparieren) wird ein *Wiederherstellungspunkt* erzeugt. Diesen Wiederherstellungspunkt[122] können Sie in der Systemwiederherstellung (*Windows*) bei Bedarf auswählen.

Die zweite Absicherung bildet die Quarantäne[203] mit deren Hilfe Sie alle Änderungen wieder rückgängig machen können.

Bei Untersuchung Startmenü diese Verzeichnisse prüfen

In den automatisch beim ersten Start des Shredders ermittelten Verzeichnissen wird nach ungültigen *Verknüpfungen* (*Verweise auf Dateien oder Verzeichnisse*) gesucht. Ungültig sind die Verweise dann, wenn sie auf nicht vorhandene Verzeichnisse oder Dateien verweisen. Sie können die *Liste der Verzeichnisse*, in denen die Analyse durchgeführt werden soll *selbst anpassen*.

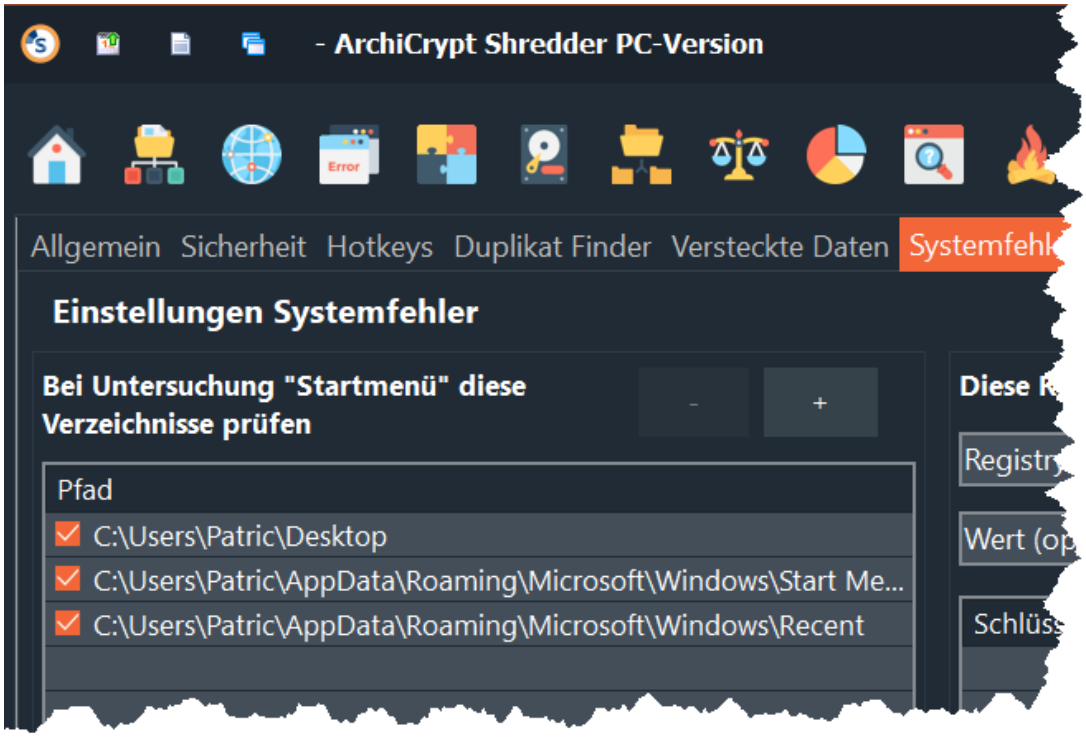


Um *Einträge hinzuzufügen*, betätigen Sie die **+ Schaltfläche**.

Um *Einträge zu entfernen*, markieren Sie den Eintrag und betätigen die **- Schaltfläche**.

Diese Registry-Schlüssel ignorieren

Falls Sie bestimmte Schlüssel oder einzelne Einträge von der Analyse ausschließen möchten, können Sie die entsprechenden Angaben hier machen.



Um einen *Eintrag zu entfernen*, klicken Sie über dem Eintrag mit der rechten Maustaste und wählen **Lösche Eintrag**.

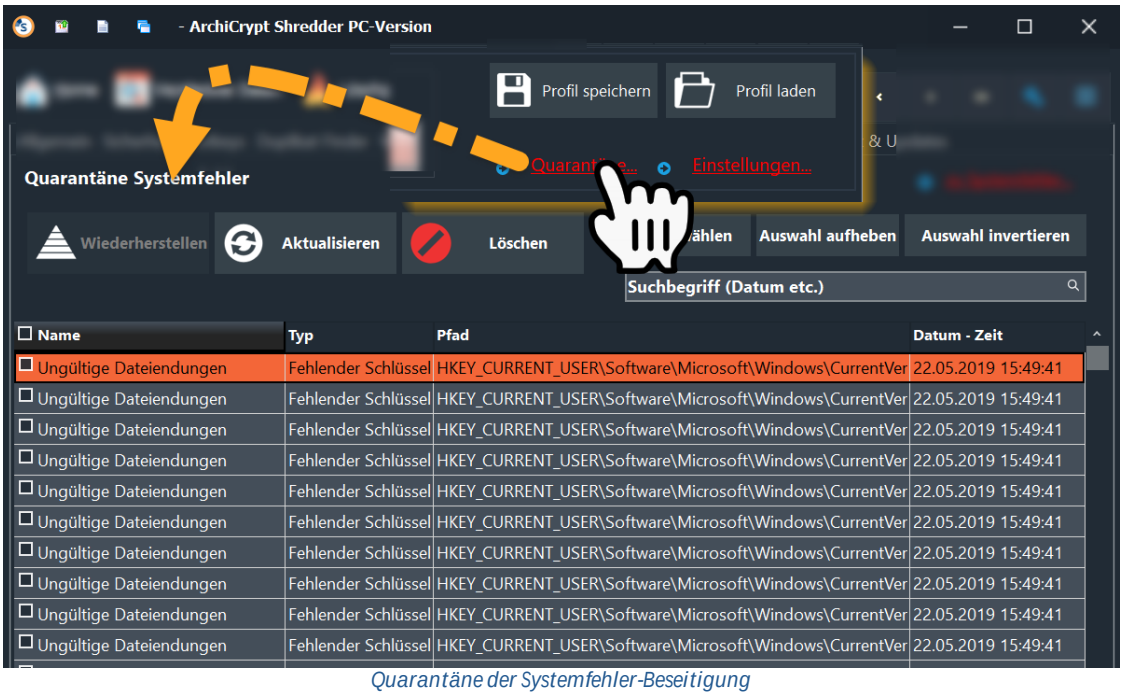
TIPP: Sie können direkt aus der Detailansicht[119] der Analyse Werte in die *Ignorieren Liste* übertragen, indem Sie den Eintrag in der Tabelle mit der rechten Maustaste anklicken und *Problem künftig ignorieren* auswählen.

10.7 Quarantäne Systemfehler

Quarantäne Systemfehler[110]

siehe auch Einstellungen

- Allgemein[177]
- Sicherheit[182]
- Hotkeys[189]
- Duplikat Finder[190]
- Versteckte Daten[197]
- System Fehlerbehebung[200]
- Platzschaffer[204]
- Lizenz & Updates[210]



Quarantäne der Systemfehler-Beseitigung

In der *Quarantäne* der Systemfehler Analyse[110] werden alle *Änderungen mit Datum* aufgelistet. Um eine Änderung rückgängig zu machen, setzen Sie ein *Häkchen vor den Eintrag* und klicken Sie auf Wiederherstellen.

WICHTIG: Wenn Sie mehrere *Analysen* und *Reparaturen* durchgeführt haben und den ursprünglichen Zustand wieder herstellen wollen, dann müssen Sie die *Änderungen von JUNG zu ALT* vornehmen. Also zunächst Änderungen vom 10.08.2020 zurücknehmen, dann die vom 05.07.2020. Nutzen Sie dazu den Filter.

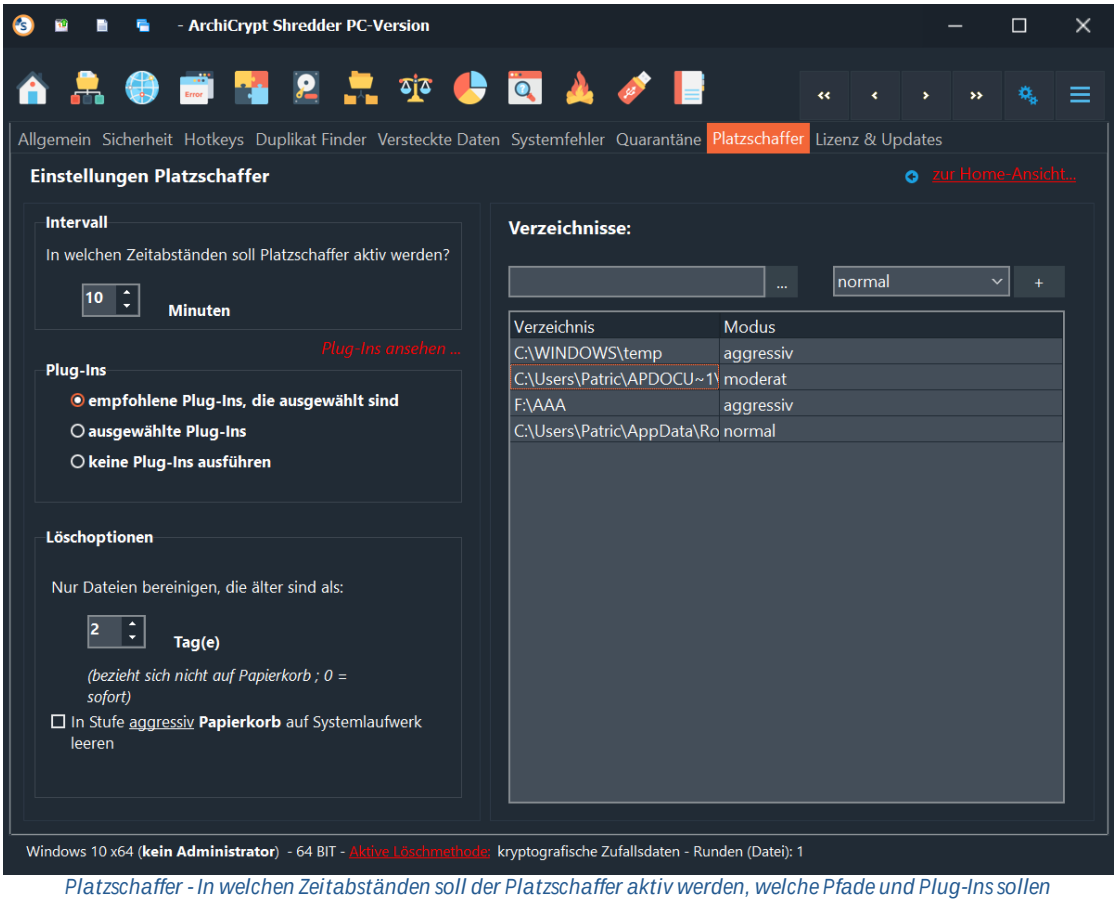
10.8 Platzschaffer

Einstellungen Platzschaffer[49]

siehe auch Einstellungen

- Allgemein[177]
- Sicherheit[182]
- Hotkeys[189]
- Versteckte Daten[197]
- Duplikat Finder[190]

- Versteckte Daten 197
- System Fehlerbehebung 200
- Quarantäne Systemfehler 203
- Lizenz & Updates 210

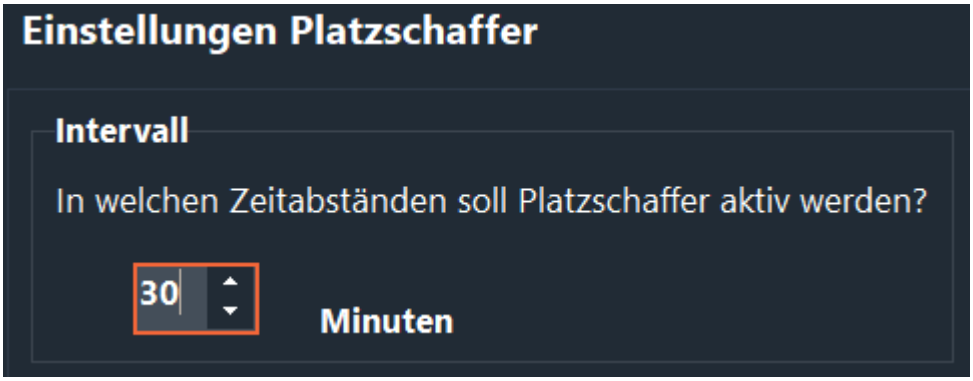


Platzschaffer - In welchen Zeitabständen soll der Platzschaffer aktiv werden, welche Pfade und Plug-Ins sollen berücksichtigt werden?

Das Platzschaffer Intervall

Der Platzschaffer 49 arbeitet zeitgesteuert. In den unter Intervall angegebenen Zeitabständen arbeitet der Platzschaffer die angegebenen Verzeichnisse ab, führt optional bestimmte Plug-Ins aus und leert gegebenenfalls Papierkörbe.

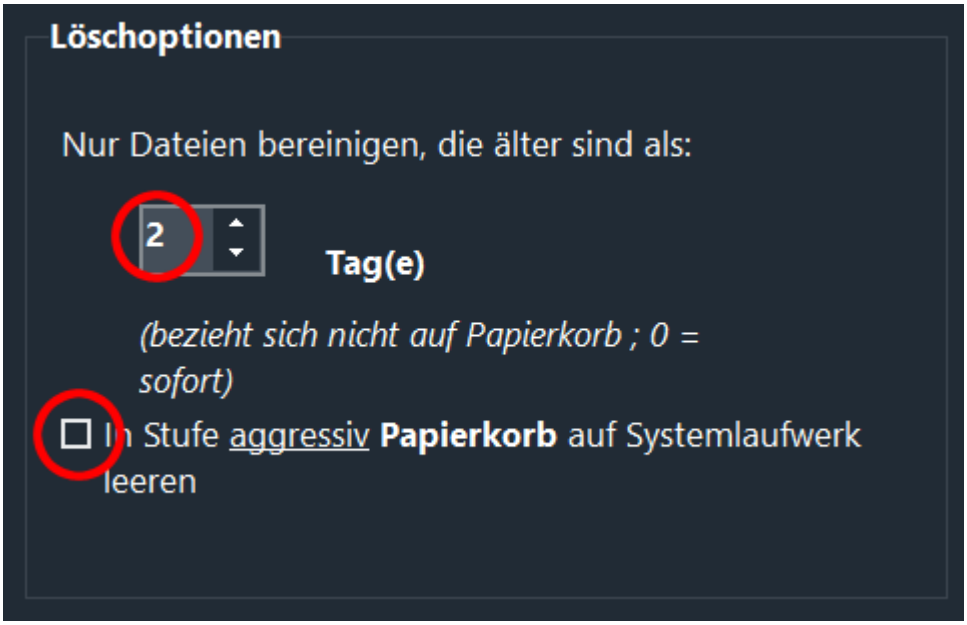
In der Praxis haben sich Werte zwischen 10 und 30 Minuten bewährt.



Das Alter von zu löschenden Dateien

Für die untersuchten Verzeichnisse kann man angeben, dass *nur die Dateien* gelöscht werden, die bereits eine Weile nicht mehr angetastet wurden. So kann es insbesondere bei Installationen vorkommen, dass Anwendungen einige Daten in den temporären Ordner abspeichern um nach einem Rechnerneustart wieder darauf zuzugreifen. Ein sofortiges Löschen hätte also zur Folge, dass die entsprechende Installation fehlschlägt.

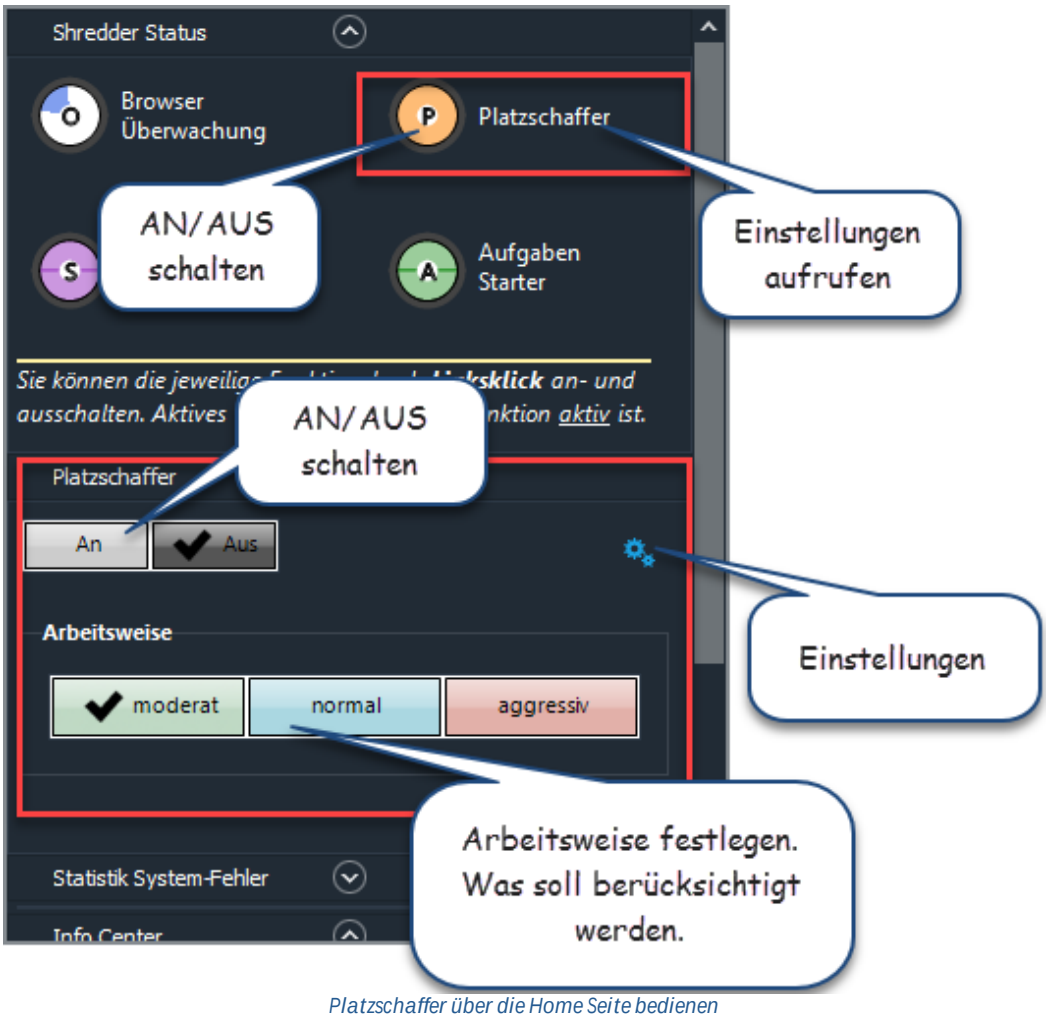
Ein Wert von 2 bis 7 Tagen ist für die tägliche Arbeit geeignet! Wenn Sie 0 Tage als Vorgabe machen, werden alle löschbaren Dateien entfernt. **Ein Wert von 0 wird nicht empfohlen!**



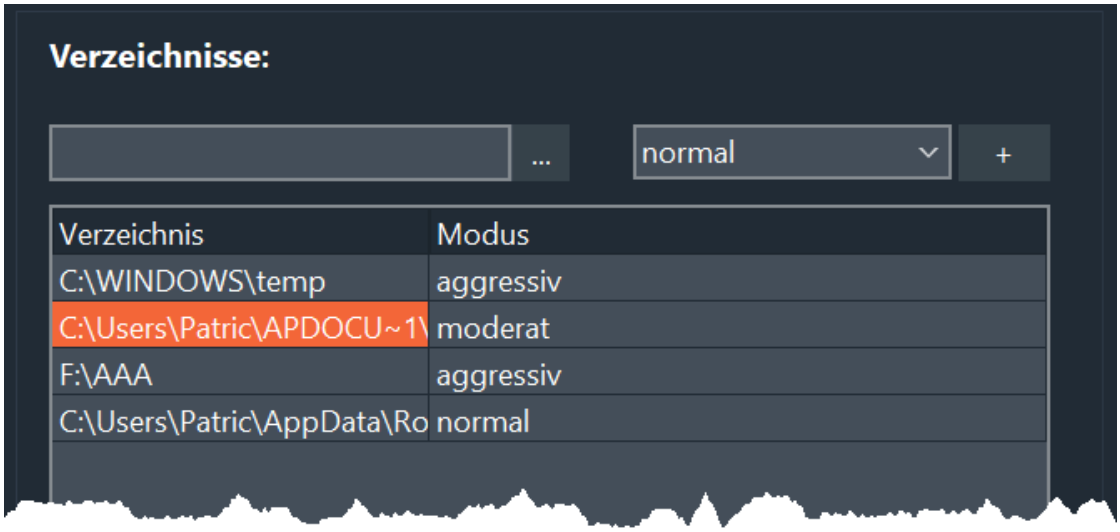
Anm.: Der Wert TAGE gilt nicht für den Papierkorb. Der Papierkorb wird sofort und komplett gelöscht, falls die Option aktiviert und die Stufe auf aggressiv steht.

Die Arbeitsweise des Platzschaffers

Auf der Home-Seite[41] können Sie festlegen, *wie der Platzschaffer*[49] arbeiten soll.



Platzschaffer über die Home Seite bedienen



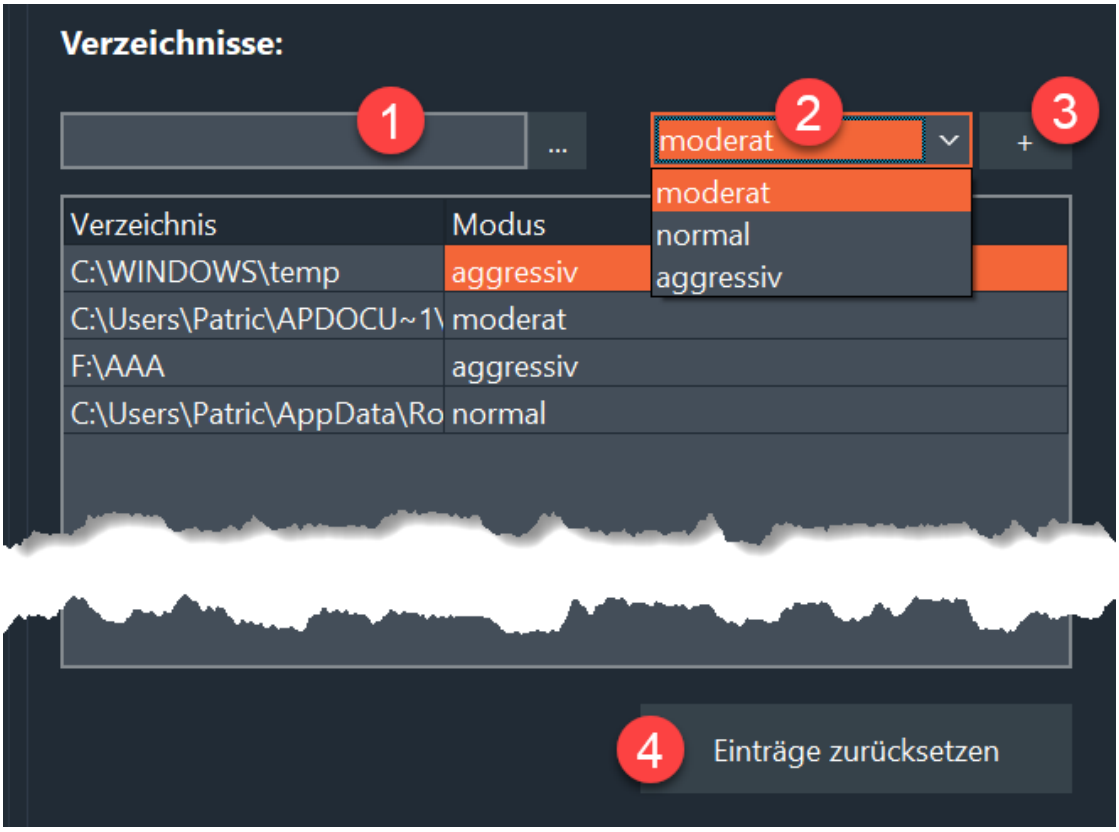
Moderat:
Die in der Verzeichnisliste mit *moderat* gekennzeichneten Einträge werden abgearbeitet

Normal:
Die in der Verzeichnisliste mit *moderat* und *normal* gekennzeichneten Einträge werden abgearbeitet

Aggressiv:
Die in der Verzeichnisliste mit *moderat*, *normal* und *aggressiv* gekennzeichneten Einträge werden abgearbeitet. Zusätzlich wird bei aktiver Option "*Stufe aggressiv leert Papierkorb auf Systemlaufwerk*" auch der Papierkorb geleert.

Allgemein kann man sagen, dass bei steigender Stufe immer mehr Daten berücksichtigt werden, die von Systemprozessen stammen. Niedrigere Stufen hingegen nur solche, die anwenderspezifisch sind.

Verzeichnisse für den Platzschaffer anpassen bzw. erweitern



Wählen Sie ein Verzeichnis (1) aus und legen Sie die Stufe (2) fest, bei der dieses Verzeichnis berücksichtigt werden soll. Klicken Sie dann auf + (3).

Wenn Sie einen Eintrag bearbeiten möchten, klicken Sie ihn links an. Die Werte werden jetzt in die Felder bei 1 und 2 übernommen. Passen Sie den Wert bei 2 an und klicken Sie auf +. Wenn Sie das Verzeichnis (1) ändern und + betätigen, wird der Eintrag als neuer Eintrag gewertet.

Zum Entfernen eines Eintrags wählen Sie ihn aus und betätigen die rechte Maustaste. Wählen Sie **löschen** aus. Die Werte werden auch hier in die Eingabefelder bei 1 und 2 übernommen und können auf Wunsch angepasst mit + übernommen werden.

Bei (4) können Sie mit **Einträge zurücksetzen** alle *Einträge auf Auslieferungszustand* zurücksetzen. Angaben die Sie ergänzt haben, gehen dabei jedoch verloren.

10.9 Lizenz und Updates

Einstellungen Lizenz und Updates

siehe auch Einstellungen

- Allgemein 177
- Sicherheit 182
- Hotkeys 189
- Versteckte Daten 197
- Duplikat Finder 190
- Versteckte Daten 197
- System Fehlerbehebung 200
- Quarantäne Systemfehler 203
- Platzschaffer 204

Lizenzinformationen

Sie können hier die aktuellen Lizenzdaten und die s.g. Rechner ID einsehen. Zudem ist es möglich, die *Lizenz vom aktuellen Rechner* zu entfernen.

Über **Jetzt Update suchen** können Sie manuell prüfen, ob eine neuere Version des Shredders verfügbar ist.

Dabei wird ausschließlich *innerhalb der von Ihnen erworbenen Hauptversion* geprüft. Also zum Beispiel bei Kauf von Version 8 alle 8.x 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. Dabei wird ausschließlich innerhalb der von Ihnen erworbenen *Hauptversion* geprüft. Also zum Beispiel bei Kauf von Version 8 alle 8.x Updates.

11 Plug-In Editor

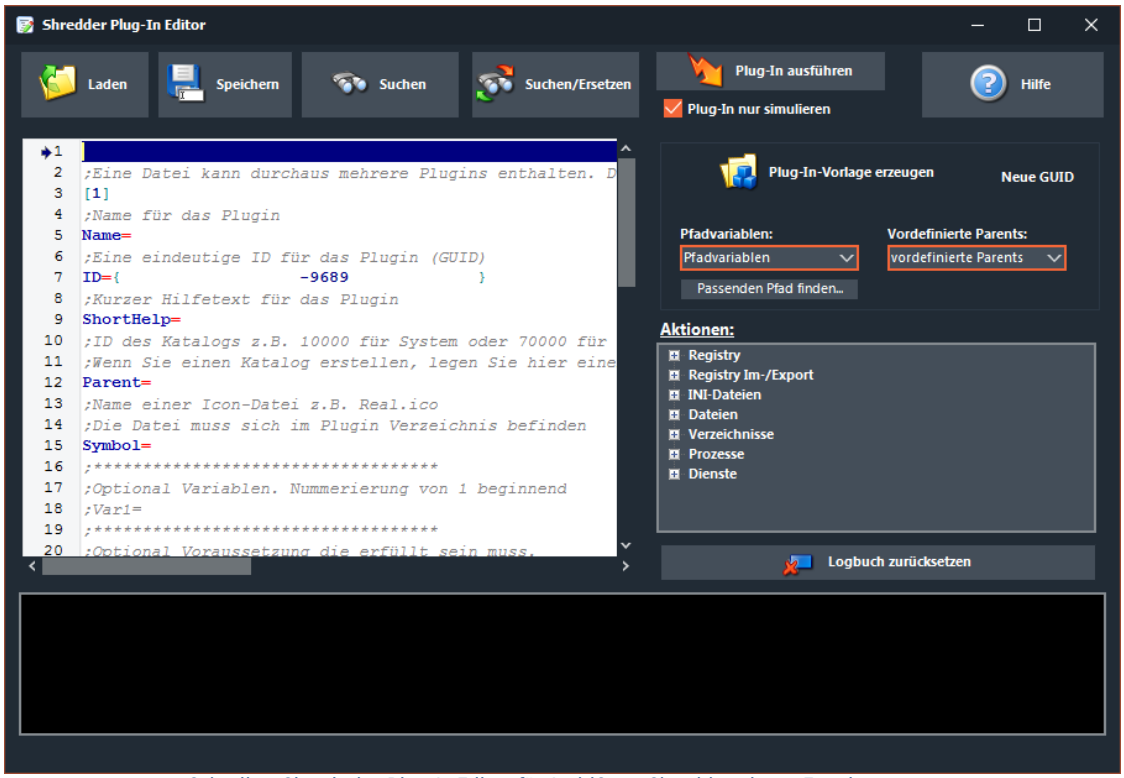
11.1 Einleitung Plugin Editor

11.1.1 Willkommen

Den Plugin Editor können Sie in unserer ArchiCrypt Freeware Zone downloaden!

Um Plug-ins für ArchiCrypt Shredder zu erstellen genügt prinzipiell ein einfacher Texteditor.

Wesentlich einfacher kann man die Plug-ins jedoch mit dem kostenlosen Shredder Plug-in Editor erstellen.



Schreiben Sie mit den Plug-In Editor für ArchiCrypt Shredder eigene Erweiterungen

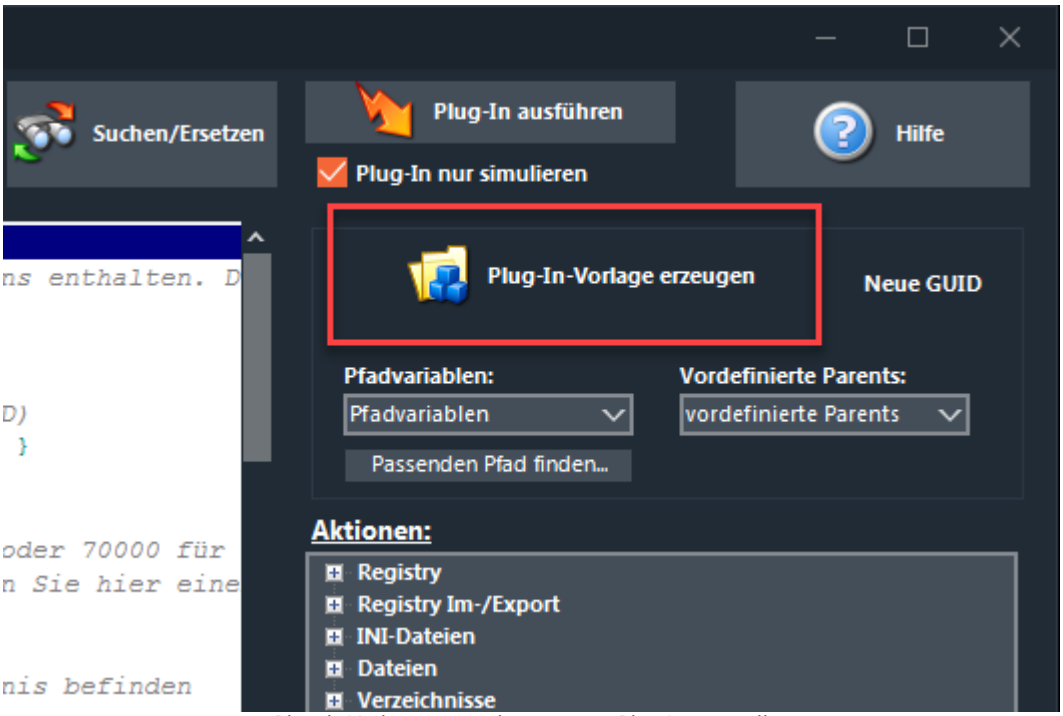
11.2 Shredder Plug-In Aufbau

11.2.1 Allgemeiner Aufbau eines Plug-Ins

THEMEN:

Aufbau eines Plug-ins

Wenn Sie den Plug-in Editor starten, wird Ihnen ein Grundgerüst bereits zur Verfügung gestellt. Sie können sich zu jedem Zeitpunkt ein solches Grundgerüst erzeugen lassen, indem Sie die Schaltfläche Plugin-Vorlage erzeugen betätigen.



Plug_in Vorlage verwenden um neues Plug-In zu erstellen

Ein Plugin ist grundsätzlich wie folgt aufgebaut:

[#]

steht dabei für eine Nummer, die fortlaufend und bei 1 beginnend in eckigen Klammern zwingend angegeben werden muss.
In einer einzelnen Plugin Datei können durchaus mehrere Plugins enthalten sein. Weitere Plugins starten in der Datei dann mit **fortlaufender Nummer** in **eckigen Klammern**.

Name=

Name des Plugins.

ID=

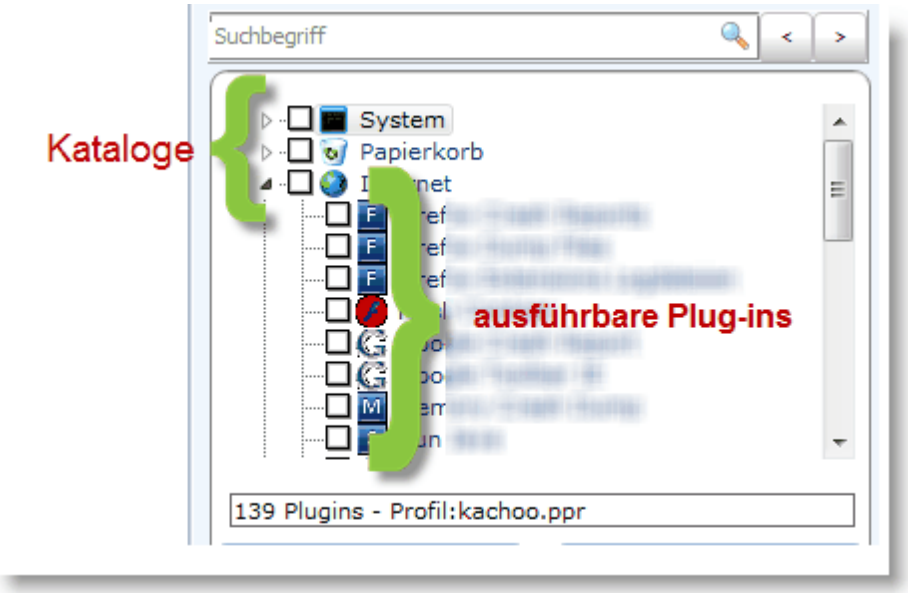
Eindeutige ID für jedes Plug-in. Es handelt sich um eine s.g. GUID, die Sie sich unbedingt durch den Editor (Plugin-Vorlage erzeugen generiert jeweils eine eindeutige GUID) oder ein anderes Werkzeug erzeugen lassen sollten.

ShortHelp=

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

Parent=

Hier gilt es zu unterscheiden, ob man ein ausführbares Plug-in oder einen Katalog (*Eintrag auf oberster Ebene in der Plugin Ansicht im Shredder, der untergeordnete Elemente aufnehmen kann*) erstellt.



falls Katalog

Geben Sie einen Wert an, der **größer als 300000** ist. Verwenden Sie NIEMALS einen Wert unterhalb 300000, da ansonsten die bestehende Struktur in ArchiCrypt Shredder zerstört werden kann.

Beispiel Parent=300010

Wenn Sie später ein ausführbares Plug-in erstellen, können Sie genau diesen Wert angeben, damit das Plug-in unterhalb Ihres Katalogs eingeordnet wird. Das Plug-in müssen Sie unbedingt als **Katalog** (**Dateiendung .kat**) abspeichern!

Katalog=true

Sie **müssen zwingend** angeben, dass es sich bei der Datei um einen Katalog handelt. Die Angabe *Katalog=false* bei ausführbaren Plug-ins kann entfallen.

falls ausführbares Plug-in

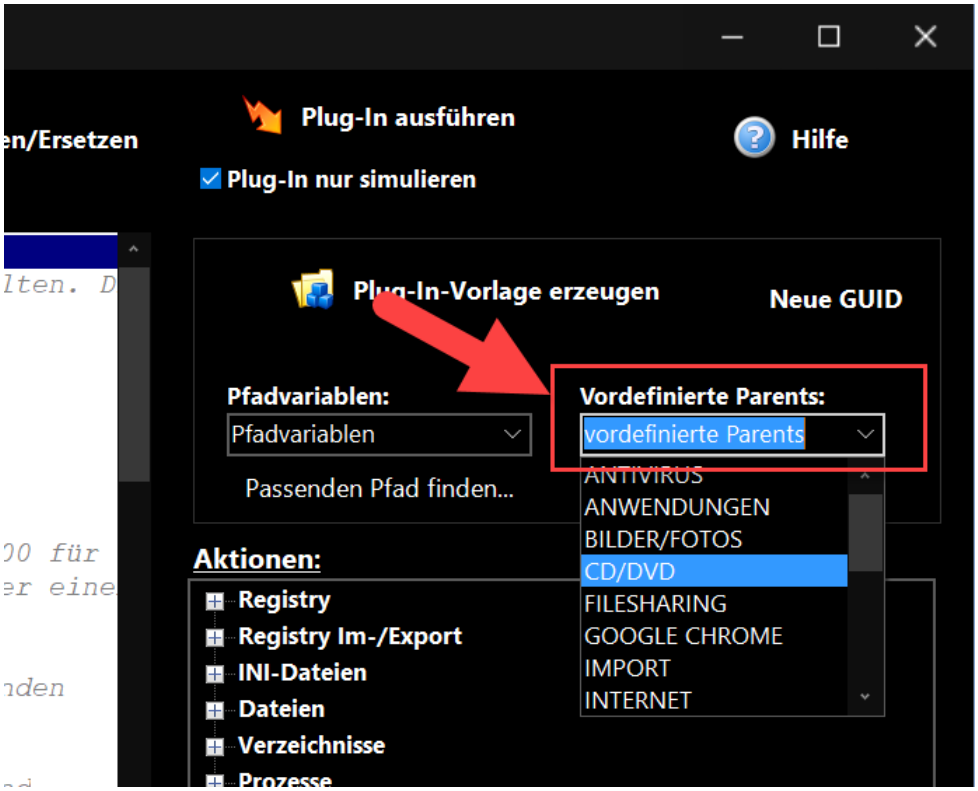
Hier müssen Sie entweder den Parent-Wert eines bestehenden Katalogs (*siehe nachfolgende Auflistung*) oder den Wert angeben, den Sie in der eigenen Katalogdatei festgelegt haben.

Vorgegebene Werte für Parent:

- 10000 für den Katalog System
- 30000 für den Katalog Internet
- 40000 für den Katalog Unterhaltung
- 50000 für den Katalog Tweak
- 60000 für den Katalog Phone Home
- 70000 für den Katalog Import (*Plugins mit unbekanntem Eintrag bei Parent werden automatisch hier eingehängt*)
- 80000 für den Katalog Werkzeuge
- 90000 reserviert für ProScripte (*ProScripte werden automatisch hier eingehängt*)
- 100000 für den Katalog Anwendungen
- 200000 für den Katalog Antivirus
- 200001 für den Katalog Sicherung

- 200002 für den Katalog Bilder/Fotos
- 200003 für den Katalog CD/DVD
- 200004 für den Katalog Google Chrome
- 200005 für den Katalog Filesharing
- 200006 für den Katalog Kompression
- 200007 für den Katalog Office
- 200008 für den Katalog Wiederherstellen

Keine Angst, Sie müssen sich diese vorgegebenen Werte nicht merken. Setzen Sie den Cursor hinter Parent= und wählen Sie in der Auswahl den entsprechenden Parent aus. Der nummerische Wert wird dann eingefügt!



Ausführbare Plug-ins **müssen** mit der **Dateiendung .sig** gespeichert werden!

Beispiele:

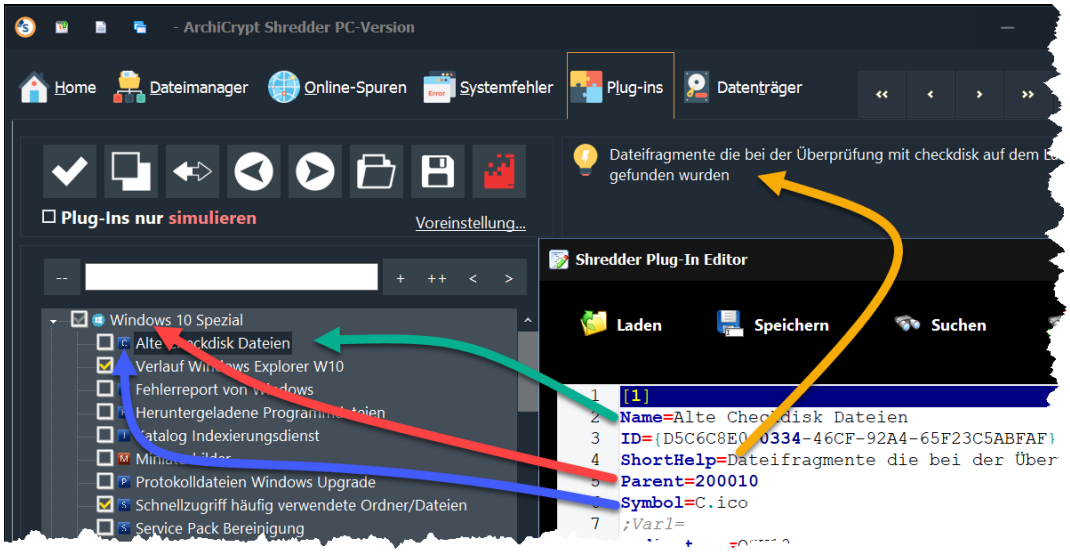
1. Sofern Sie ein ausführbares Plug-in erzeugt haben, welches thematisch in die Kategorie Office passt, geben Sie
   Parent=200007
an.

2. Möchten Sie ein ausführbares Plug-in unterhalb eines selbst angelegten Katalogs ablegen, wobei Sie dem Wert Parent in der Katalogdatei 300010 zugewiesen haben, dann geben Sie im ausführbaren Plugin
   Parent=300010
wie in der Katalogdatei an.

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. Falls Sie hier keinen Namen angeben. Extrahiert ArchiCrypt Shredder den ersten Buchstaben des angegebenen Namens und verwendet dann das entsprechende Buchstaben-Icon.

Zusammenhang zwischen den Angaben im Plug-in und dem Erscheinen in ArchiCrypt Shredder:



Für einen Katalog sind keine weiteren Angaben erforderlich. Die Nachfolgenden Einträge sind ausschließlich für ausführbare Plug-ins vorgesehen.

Var#=

siehe dazu Variablen 12

Optional. # steht dabei für eine Nummer, die bei 1 beginnend, fortlaufend angegeben werden muss.
Mit diesen Einträgen legen Sie sich s.g. Variablen fest, die Sie später im Script mit %var1%, %var2% etc. weiter verwenden können.

Beispiele:

1.
   Var2=Test
   Var3=Test2
   ist **falsch**, da nicht bei 1 begonnen wurde.
2.
   Var1=test1
   var3=test3
   falsch, da Lücke in der Nummerierung.
3.
   Var3=test3
   Var2=test2
   Var1=test1
   falsch, da nicht auf-, sondern absteigend.

4.
   Var1=test1
   Var2=test3
   Var3=test2
   korrekt

Indicator#=

siehe dazu Indikatoren 18

Optional. # steht dabei für eine Nummer, die bei 1 beginnend, fortlaufend angegeben werden muss. Indikatoren bestimmen, welche Voraussetzungen erfüllt sein müssen (*z.B. welche Verzeichnisse, Dateien, Registrywerte, welches Betriebssystem*), damit das Plug-in ausgeführt wird.

ArchiCrypt Shredder lädt nur solche Plug-ins, bei denen die Bedingungen erfüllt sind. Wenn Sie möchten, dass ein Plug-in auf jeden Fall von ArchiCrypt Shredder geladen wird, machen Sie keine Indicator# Angaben.

Action#=

siehe dazu Aktionen[23]
steht dabei für eine Nummer, die bei 1 beginnend, fortlaufend angegeben werden muss. Die Action Angaben enthalten die Anweisungen, die ArchiCrypt Shredder ausführen soll.

Protect#=

Optional. # steht dabei für eine Nummer, die bei 1 beginnend, fortlaufend angegeben werden muss. Schützen Sie bestimmte Dateien, Pfade oder Registry Schlüssel vor dem Löschen. Falls Sie direkt einen Regulären Ausdruck angeben, müssen Sie einen Eintrag "PatternMatching=True" hinzufügen.

Author=

Optional. Angaben über den Autor des Plug-ins.

LastModified=

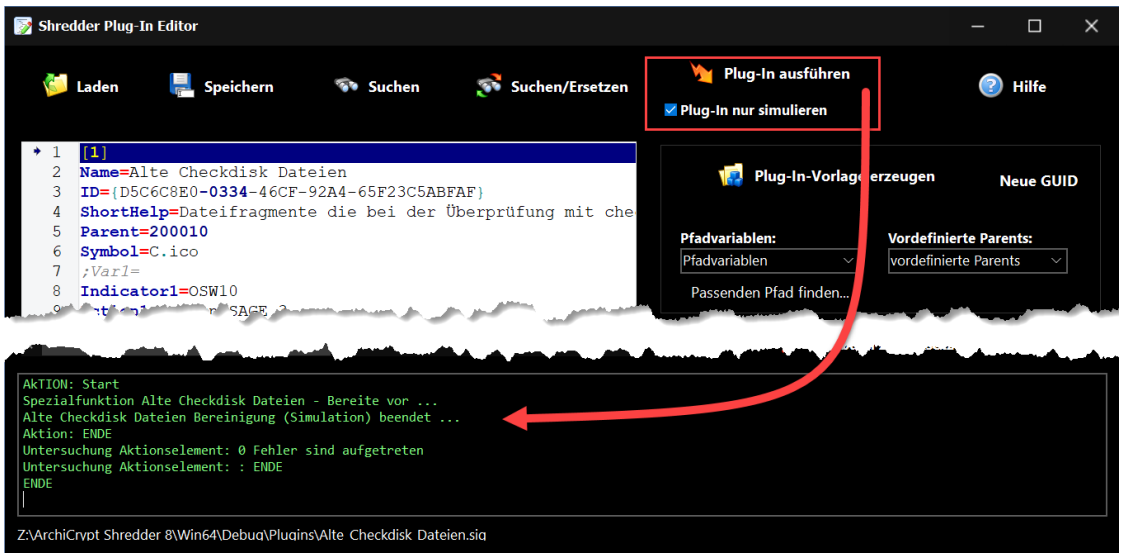
Optional. Datum in dd.mm.yyyy Notation. Gibt an, wann das Plug-in zuletzt bearbeitet wurde.

Plug-in Entwicklung und Test

Während der Entwicklung des Plugins können Sie die die Funktion Plugin ausführen zusammen mit der Option Plugin nur simulieren nutzen, um das Plugin zu testen. Im Logbuch sehen Sie Ausgaben, die der Interpreter der Plugins erzeugt.

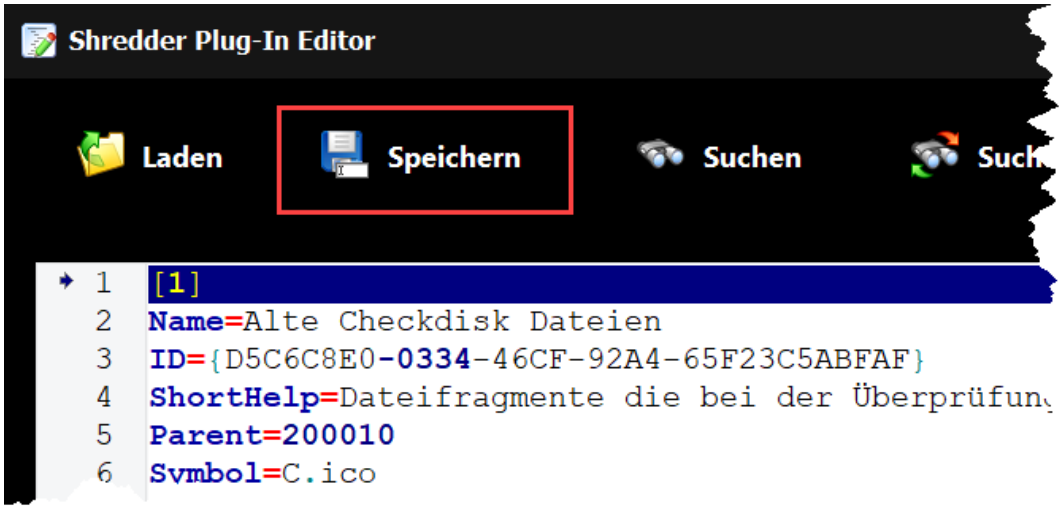
Der Ausgabe können Sie entnehmen, wie Variablen aufgelöst werden, wie Indikatoren ausgewertet werden und welche Aktionen erkannt und wie diese Aktionen auf dem aktuellen Rechner umgesetzt werden.

Wenn Sie ein Plug-in erstellen, beginnen Sie mit eventuellen Variablen. Simulieren Sie dann das Plugin um zu sehen, wie wie Variablen[12] aufgelöst werden.
Erstellen Sie dann ggf. Indikatoren[18] und testen Sie erneut. Zum Schluss erstellen und testen Sie dann die Aktionen[23].



Plug-in speichern

Nachdem das Plug-in fertiggestellt wurde, muss es im Plugin Verzeichnis des Shredders *(Installationsordner, Unterverzeichnis plugins)* gespeichert werden. Falls Sie eine Symboldatei (Symbol) angegeben haben, muss diese ICO Datei ebenfalls in das Plugin Verzeichnis des Shredders kopiert werden.

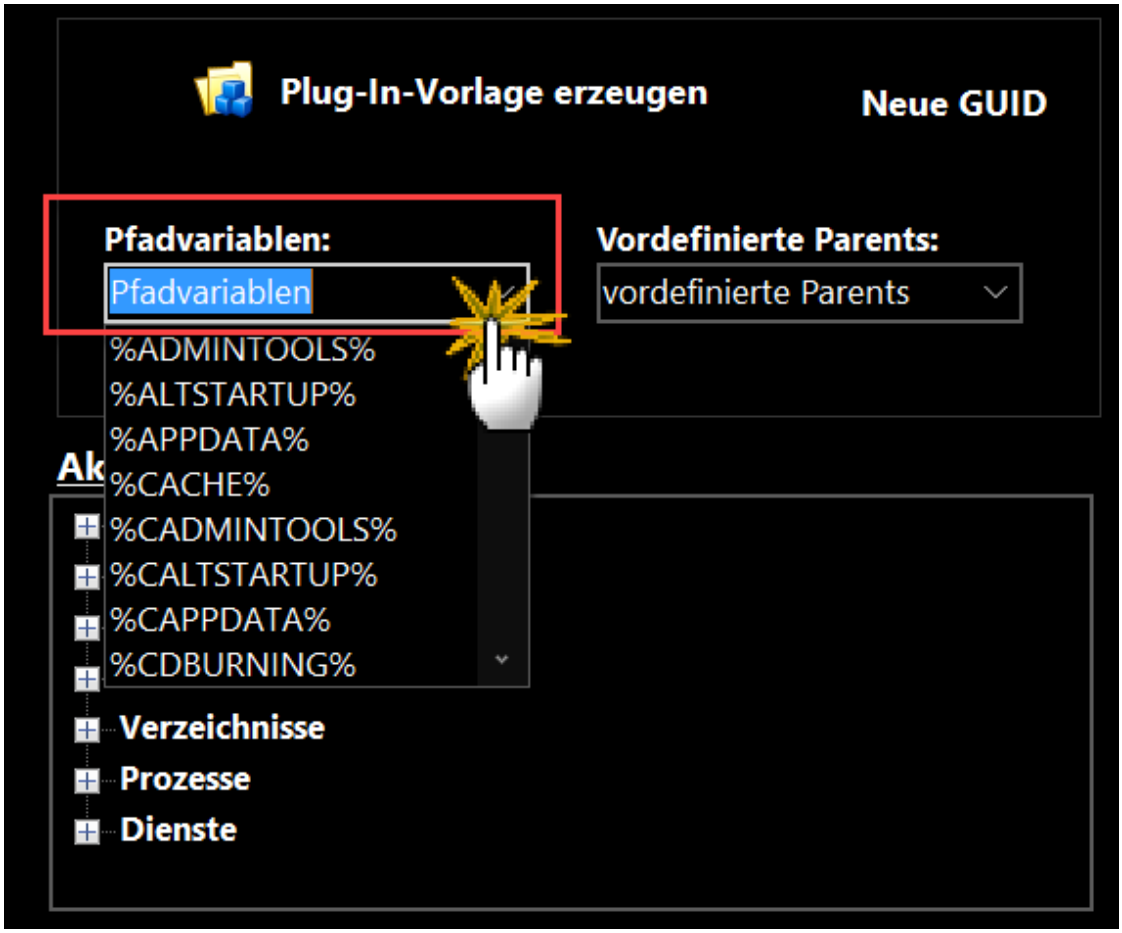


Sie müssen ggf. das Plug-in System des Shredders neu initialisieren[106], damit es geladen wird. Generell wird ein Plugin jedoch **nur** im Shredder angezeigt, wenn angegebene Voraussetzungen (*Indicator#*[7]) erfüllt sind!

11.2.2 Pfadvariablen

Die Verzeichnisstruktur ist auf jedem Rechner eine andere. Daher sollte man mit fest definierten Pfaden in Plug-ins sehr vorsichtig sein.
Der Pfad C:\Dokumente und Einstellungen\Horst\Lokale Einstellungen\Anwendungsdaten\Identities\ mag zwar auf Ihrem Rechner existieren, auf einem anderen Rechner jedoch eher nicht. Das ist nicht weiter tragisch, wenn Sie ein Plug-in nur selbst und nur für einen bestimmten Rechner geschrieben haben.

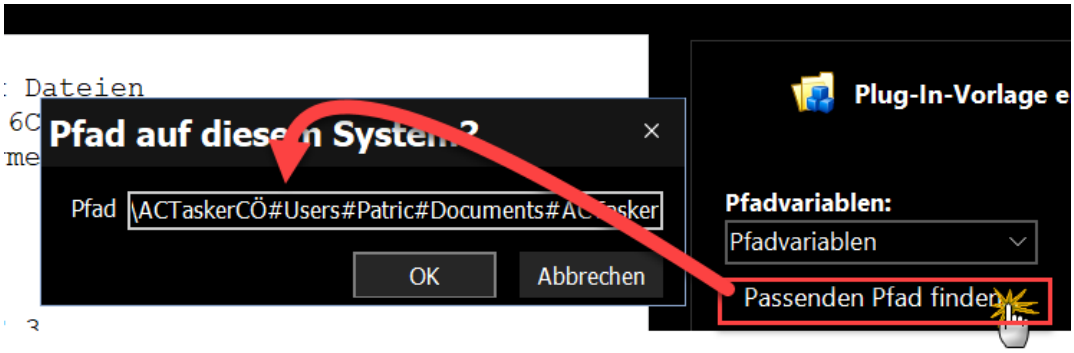
Sobald Sie jedoch ein Plug-in weitergeben möchten oder es auch auf einem anderen Computer nutzen wollen, sollten Sie "Pfadvariablen" verwenden. Diese Verzeichnisse werden auf jedem Rechner zum Zeitpunkt der Plug-in Ausführung berechnet.



Die Pfadvariablen können Sie an jeder Stelle des Plug-ins einfügen. Für den einfacheren Umgang mit den Pfadvariablen haben wir zwei wichtige Werkzeuge in den Plugin Editor integriert.

Umwandlung eines Pfades in einen Pfad mit Pfadvariable

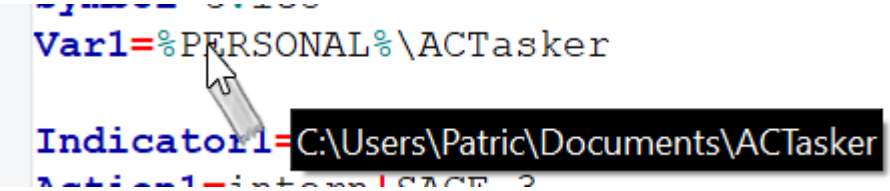
Kopieren Sie den betreffenden Pfad oder Dateinamen (*natürlich inkl. Pfad*) in die Zwischenablage. Rufen Sie jetzt im Editor die Funktion Passenden Pfad finden ... auf. Fügen Sie Ihren Pfad aus der Zwischenablage in den Dialog ein (*z.B. mittels Strg + V*) und klicken Sie auf OK.



Falls eine passende Pfadvariable gefunden wurde, erhalten Sie eine entsprechende Meldung. Sie können den angepassten Pfad jetzt über die Zwischenablage (z.B. Strg + V) an jeder beliebigen Stelle im Plug-in einfügen.

Anzeige des konkreten Pfades auf dem aktuellen System

Wenn Sie ein Plug-in laden, dann können Sie den Mauszeiger kurz über einen Pfad mit Pfadvariable bewegen und Sie erhalten als Hinweis den konkreten Pfad auf dem aktuellen Rechner.



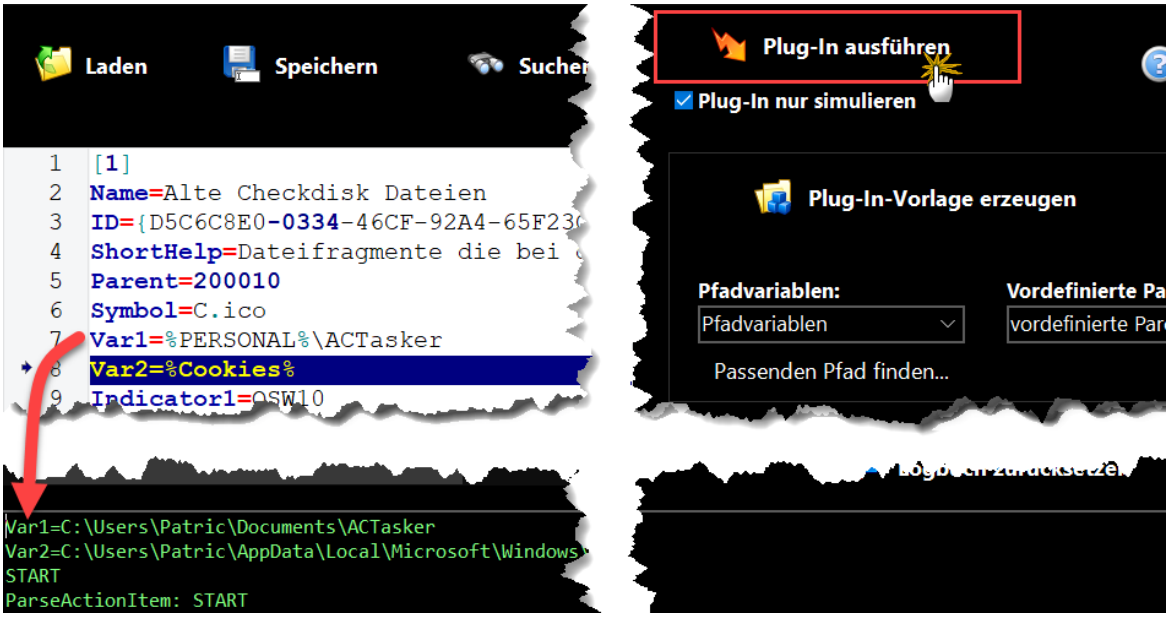
11.2.3 Variablen

In der Beschreibung zum Aufbau eines Plug-ins[2] wurde auf die Möglichkeit hingewiesen, Variablen[7] einzuführen.

Eine Variable kann man im Plug-in dann an beliebiger als Platzhalter verwenden.

TIPP: ***Wenn Sie mit dem Editor ein Plug-in erzeugen, können Sie bei aktivierter Option Plug-in nur simulieren, die Schaltfläche Plugin ausführen betätigen. Im Logbuch erhalten Sie wertvolle Hinweise. So***

können Sie sich zum Beispiel ansehen, welchen Wert die Variablen annehmen.



Für Variablen gelten folgende Regeln:

Definition:

Variablen werden immer durch das Schlüsselwort VAR#=<Wert> definiert. Dabei sind Variablen bei 1 beginnend, fortlaufend zu nummerieren. # steht dabei für die entsprechende Zahl. Hinter dem Gleichheitszeichen wird dann der <Wert> angegeben.

Beispiel:

VAR1=%AppData%\local
VAR2=%Cookies%

Verwendung:

Sobald eine Variable definiert wurde, können Sie sie an beliebiger Stelle verwenden. Dabei wird nur die Nummer, eingebettet in die Zeichen %#% angegeben. Bei der Ausführung des Plug-ins wird dann jedes Vorkommen dieses Platzhalters durch den ermittelten Wert ersetzt.

Beispiel:

VAR1=ArchiCrypt
VAR2=%1% ist cool

Wird das Plug-in ausgeführt, hat VAR2 den Wert "ArchiCrypt ist cool". An jeder Stelle, an der Sie im Plug-in %2% (*Platzhalter für VAR2*) angegeben haben, wird "ArchiCrypt ist cool" eingesetzt.

Es gibt grundsätzlich 3 Arten von Variablen

Reiner Text

Beschreibung: Der Wert wird im Plug-in festgelegt und genau so auf dem Rechner beibehalten, auf dem das Plug-in ausgeführt wird. Es handelt sich also um eine Konstante.

Zweck: Primär Schreibarbeitsersparnis und Möglichkeit, das Plug-in bei Bedarf schneller anpassen zu können.

Syntax: Geben Sie den entsprechenden Text hinter dem Gleichheitszeichen an

Beispiel:
VAR1=Erste Variable
VAR2=Zweite Variable und %1%
VAR3=Dritte Variable und %2%

Im Plug-in wird %3% also aufgelöst zu "Dritte Variable und Zweite Variable und Erste Variable"

Tatsächliche Variablen

Beschreibung: Wert wird erst zur Ausführungszeit des Plug-ins auf dem entsprechenden Rechner ermittelt.

Zweck: Im Wesentlichen wird es sich um Pfade und Dateinamen handeln, die man aus der Registrierungsdatenbank (Registry) oder aus Initialisierungsdateien ausliest, um anschließend Aktionen in den ermittelten Verzeichnissen oder mit den Dateien auszuführen.

So lesen Sie einen Wert aus der Registry aus

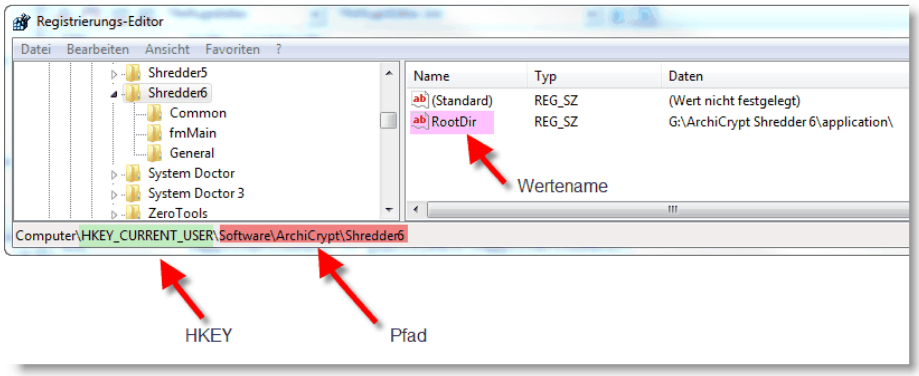
Syntax:

VAR#=HKEY|Pfad|Name

Wobei HKEY einen der folgenden Werte annehmen kann:

- HKEY_CURRENT_USER oder HKCU
- HKEY_LOCAL_MACHINE oder HKLM
- HKEY_CLASSES_ROOT oder HKCR
- HKEY_CURRENT_CONFIG oder HKCC
- HKEY_USERS oder HKUS

Pfad steht für den Pfad in der Registry und Name für den Wertename in der Registry, der ausgelesen werden soll.



Beispiel:

VAR1=HKEY_CURRENT_USER|Software\ArchiCrypt\Shredder6|RootDir

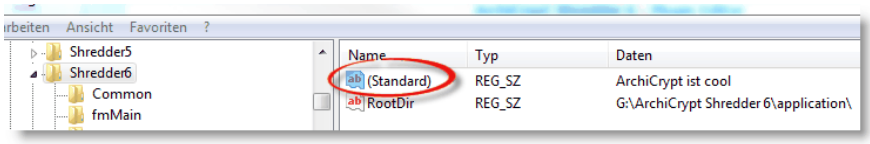
Beim Ausführen des Plug-ins wird der entsprechende Wert (G:\ArchiCrypt Shredder 6\application\) aus der Registry ausgelesen.

Um den Default Wert (Standard) in der Registry auszulesen, geben Sie als Wertename bitte **default** an.

Beispiel:

VAR1=HKEY_CURRENT_USER|
Software\ArchiCrypt\Shredder6|default

Beim Ausführen des Plug-ins wird der entsprechende Wert (*ArchiCrypt ist cool*) aus der Registry ausgelesen.



So lesen Sie einen Wert aus einer Initialisierungsdatei aus (Ini Datei)

Syntax:

VAR#=IniFileName|Section|Name
Dabei muss der komplette Pfad zur Ini Datei angegeben werden.

Section gibt dabei die Sektion an (Sektionen werden in eckigen Klammern in der Ini Datei angegeben)
Name gibt den Wertename an, der ausgelesen werden soll.

Beispiel:

Var1=%APPDATA%\ACShredder6\Shredder.ini|General|
UserDef

Liest aus der Initialisierungsdatei von ArchiCrypt Shredder in der Sektion [General] den Wert von UserDef aus.
Var1 hat dann entsprechend den Wert C:
\Users\Patric\AppData\Roaming\ACShredder6\DataBackup

```
10 [General]
11 Create RP=1
12 PlaySound=1
13 UAPlugins=0
14 Kontext=1
15 XPInfo=0
16 Autostart=0
17 Monitor=0
18 AutoSecureZone=0
19 RoundsFile=1
20 RoundsFReespace=1
21 CleanFreespace=1
22 UltrafastFreespace=1
23 CleanClustertips=0
24 CleanFilenames=0
25 UserDef=C:\Users\Patric\AppData\Roaming\ACShredder6\DataBackup
26 WatchDirs=0
```

%APPDATA%\ACShredder6\Shredder.ini

Interaktive Variablen

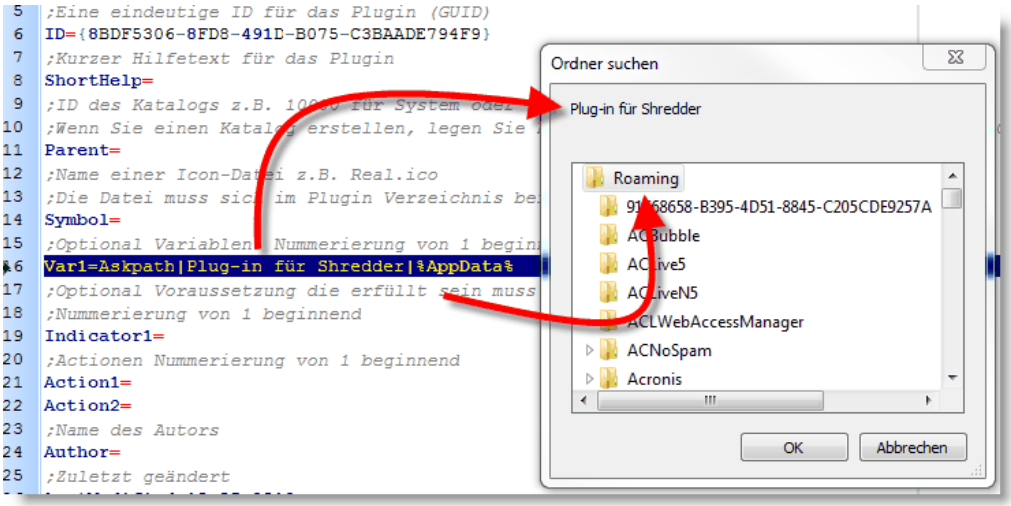
Die Werte werden mit Hilfe von Dialogen ermittelt.
Zweck: Der Nutzer muss ein Verzeichnis oder eine Datei auswählen. Dazu wird ihm der Windows Dialog angezeigt.

So fragen Sie den Anwender nach einem Pfad

Syntax:
VAR#=ASKPATH|Dialogüberschrift|Startverzeichnis

Der Anwender wird 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.

Beispiel:
VAR1=AskPath|Plug-in für Shredder|%AppData%
Der Windows Dialog zur Auswahl eines Verzeichnisses wird angezeigt. Der Titel lautet *Plug-in für Shredder*. Das Verzeichnis *%AppData%* ist vorausgewählt.



So fragen Sie den Anwender nach einer Datei

Syntax:
VAR#=ASKFILE|Dialogüberschrift|Startverzeichnis

Der Anwender wird aufgefordert, einen Dateinamen auszuwählen oder einzugeben.

Beispiel:
VAR1=ASKFILE|Initialisierungsdatei von ArchiCrypt Shredder|%AppData%\ACShredder7
Der Dialog zur Auswahl einer Datei wird mit dem Titel Initialisierungsdatei für ArchiCrypt Shredder angezeigt. Das Verzeichnis %AppData%\Shredder6 ist geöffnet.

11.2.4 Indikatoren

Indikatoren[7] sind Bedingungen, die erfüllt sein müssen, damit das Plug-in von ArchiCrypt Shredder geladen wird. Es können mehrere Indikatoren angegeben werden. Wenn Sie keinen Indikator angeben, wird das Plug-in grundsätzlich geladen. Beim Ausführen wird dann versucht, die Aktionen[23] auszuführen.

Definition von Indikatoren

Indikatoren werden immer durch das Schlüsselwort Indicator#=<Bedingung> definiert. Dabei sind Indikatoren bei 1 beginnend, fortlaufend zu nummerieren. # steht dabei für die entsprechende Zahl. Hinter dem Gleichheitszeichen wird dann die <Bedingung> angegeben.

Verbinden mehrere Bedingungen mittels or (oder)

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 = OSW7 +or+ osw10

Dieser Indikator wird mit wahr gewertet, wenn es sich um das Betriebssystem Windows XP oder Vista oder Windows 7 handelt.

Verbinden mehrerer Bedingungen mittels und

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

Beispiel:

Indicator1 = OSW7 +or+ OSW8 +or+ osw10

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.

Betriebssystem als Indikator

Indicator#=Betriebssystem
Dabei muss der Wert für Betriebssystem einen der folgenden Werte annehmen:

- OSW7
- OSW8
- OSW81
- OSW2012
- OSW2012R2
- OSW10

Beispiel:
Indicator1 = OSW7 +or+ OSW10
Dieser Indikator wird mit wahr gewertet, wenn es sich um das Betriebssystem Windows XP oder Vista oder Windows 7 handelt.

Pfad oder Datei als Indikator

Indicator#=Pfad bzw. Datei

Beispiel:
Indicator1 = %AppData%\ACShredder7
Dieser Indikator wird mit wahr gewertet, wenn der entsprechende Pfad existiert.

Beispiel:
Indicator1 = %AppData%\ACShredder7\Shredder.ini
Dieser Indikator wird mit wahr gewertet, wenn die entsprechende Datei existiert.

Beispiel:
Indicator1 = %AppData%\ACShredder7\Shredder7.ini +or+ %AppData%\ACShredder7\Shredder.ini
Dieser Indikator wird mit wahr gewertet, wenn eine der beiden Dateien existiert

Schlüsselname in Registry als Indikator

Indicator#=HKEY|Pfad

Wobei HKEY einen der folgenden Werte annehmen kann:

- HKEY_CURRENT_USER oder HKCU
- HKEY_LOCAL_MACHINE oder HKLM
- HKEY_CLASSES_ROOT oder HKCR
- HKEY_CURRENT_CONFIG oder HKCC
- HKEY_USERS oder HKUS

Beispiel:

INDICATOR1=HKEY_CURRENT_USER|
Software\ArchiCrypt\Shredder7

Dieser Indikator wird mit wahr gewertet, wenn der Schlüssel HKEY_CURRENT_USER\Software\ArchiCrypt\Shredder7 in der Registry existiert.

Existenz eines Wertes in der Registry als Indikator

Indicator#=HKEY|Pfad|Wert

Wobei HKEY einen der folgenden Werte annehmen kann:

- HKEY_CURRENT_USER oder HKCU
- HKEY_LOCAL_MACHINE oder HKLM
- HKEY_CLASSES_ROOT oder HKCR
- HKEY_CURRENT_CONFIG oder HKCC
- HKEY_USERS oder HKUS

Beispiel:

INDICATOR1=HKEY_CURRENT_USER|
Software\ArchiCrypt\Shredder7|RootDir

Der Indikator wird mit wahr gewertet, falls es den Wert RootDir gibt.

Um den Default Wert (Standard) in der Registry auszulesen, geben Sie als Wertename bitte **default** an.

Beispiel:

INDICATOR1=HKEY_CURRENT_USER|
Software\ArchiCrypt\Shredder7|default

Der Indikator wird mit wahr gewertet, falls es einen default Wert gibt.

Wert in Registry als Indikator

Indicator#=HKEY|Pfad|Wert|Typ|Vorgabe

Wobei HKEY einen der folgenden Werte annehmen kann:

- HKEY_CURRENT_USER oder HKCU
- HKEY_LOCAL_MACHINE oder HKLM
- HKEY_CLASSES_ROOT oder HKCR
- HKEY_CURRENT_CONFIG oder HKCC
- HKEY_USERS oder HKUS

Wobei Typ einen der folgenden Werte annehmen darf:

- s entspricht dem Typ REG_SZ, also Text
- n entspricht Ganzzahl, Typ REG_DWORD
- b entspricht Wahrheitswert, 0 bedeutet falsch, 1 bedeutet wahr

Beispiel:
INDICATOR1=HKCU|Software\ArchiCrypt\Shredder7|default|s|
ArchiCrypt ist cool

Der Indikator wird mit wahr gewertet, falls es den Schlüssel HKEY_CURRENT_USER\Software\ArchiCrypt\Shredder7 mit default Wert (Typ Text) gibt und dieser den Wert "ArchiCrypt ist cool" hat.

Beispiel:
INDICATOR1=HKCU|Software\ArchiCrypt\Shredder7\General|
Create RP|n|1

Der Indikator wird mit wahr gewertet, falls es den Schlüssel HKEY_CURRENT_USER\Software\ArchiCrypt\Shredder7\General mit Name Create RP gibt und dieser den Zahlenwert 1 hat.

Beispiel:

INDICATOR1=HKCU|Software\ArchiCrypt\Shredder7\General|Create RP|b|1

Der Indikator wird mit wahr gewertet, falls es den Schlüssel HKEY_CURRENT_USER\Software\ArchiCrypt\Shredder7\General mit Name Create RP gibt und dieser den Wahrheitswert 1 (entspricht wahr) hat.

11.2.5 Aktionen

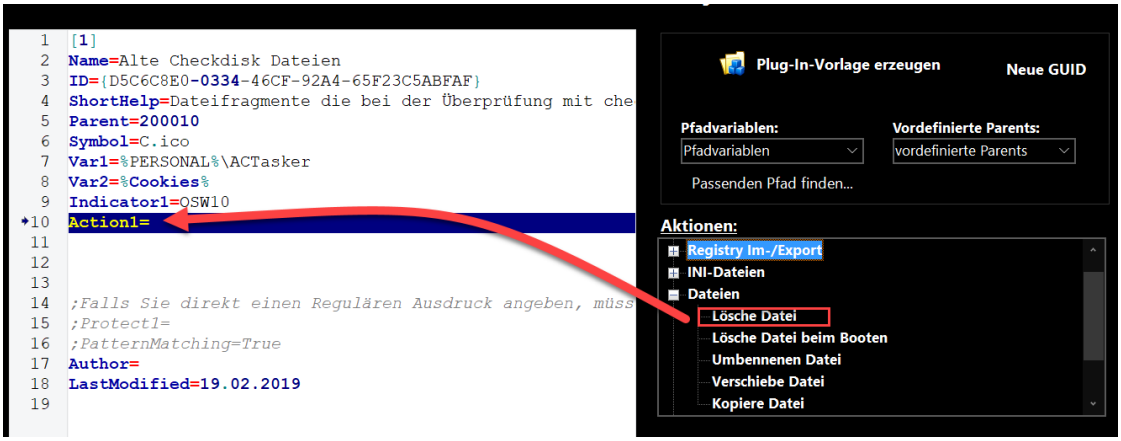
11.2.5.1 Überblick

Aktionen[8] sind die Teile eines Plug-ins, die ArchiCrypt Shredder die Arbeitsanweisungen liefern. ArchiCrypt Shredder unterstützt eine Vielzahl an unterschiedlichen Aktionen.

Aufbau einer Aktion

Syntax:
Action#=Aktionstyp|weitere Daten je nach Aktionstyp
Die Aktionen müssen, beginnend bei 1 fortlaufend nummeriert werden. # steht dabei für die entsprechende Zahl. Hinter dem Gleichheitszeichen wird dann die Aktion näher definiert.

Der Plug-in Editor hält für die meisten Aktionen Vorlagen bereit. Setzen Sie den Eingabecursor hinter das Gleichheitszeichen der Aktion und wählen Sie dann rechts bei den Vorlagen eine passende Aktion durch Doppelklick aus. Die Vorlage wird übertragen. Passen Sie die Vorlage dann bitte an.



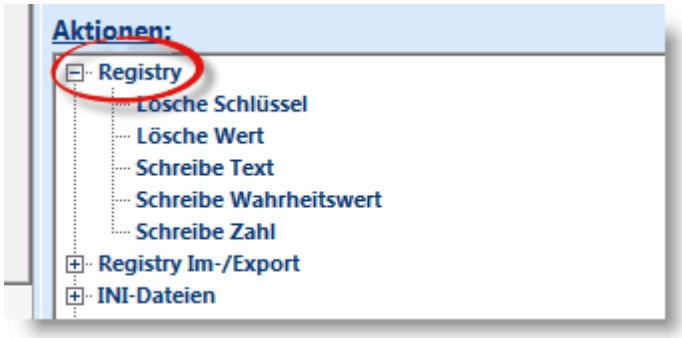
Die Aktionen sind in verschiedene Rubriken unterteilt:

- Registry 24
- Registry Im-/Export 27
- Ini-Dateien 29
- Dateien 32
- Verzeichnisse 34
- Prozesse 36
- Dienste 38

11.2.5.2 Registry

Mit den Aktionen der Kategorie Registry können Sie Registry Schlüssel löschen, Werte in der Registry löschen und Werte in die Registry schreiben.

siehe auch: Registry Im-/Export 27



Aktionen die sich auf die Registry beziehen

Einen Schlüssel in der Registry löschen - Lösche Schlüssel

Syntax:
Action#=**reg|delkey|**HKEY|Pfad

Wobei HKEY einen der folgenden Werte annehmen kann:

- HKEY_CURRENT_USER oder HKCU
- HKEY_LOCAL_MACHINE oder HKLM
- HKEY_CLASSES_ROOT oder HKCR
- HKEY_CURRENT_CONFIG oder HKCC
- HKEY_USERS oder HKUS

Der Pfad darf s.g. Jokerzeichen wie * oder ? enthalten. Seien Sie mit der Verwendung der Joker jedoch **extrem Vorsichtig**
Wenn der Pfad Unterschlüssel und oder Werte enthält, werden diese ebenfalls gelöscht.

Beispiel:
Action1=reg|DELKEY|HKCU|
Software\ArchiCrypt\Shredder6\RegistrationInfo

Löscht den Pfad
HKEY_CURRENT_USER\Software\ArchiCrypt\Shredder6\RegistrationInfo aus der Registry.

Einen Wert in der Registry löschen - Lösche Wert

Syntax:
Action#=**reg|delvalue|**HKEY|Pfad|Wertename

Wobei HKEY einen der folgenden Werte annehmen kann:

- HKEY_CURRENT_USER oder HKCU
- HKEY_LOCAL_MACHINE oder HKLM
- HKEY_CLASSES_ROOT oder HKCR
- HKEY_CURRENT_CONFIG oder HKCC
- HKEY_USERS oder HKUS

Pfad und Wertename können Jokerzeichen wie * und ? enthalten

Beispiel:

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

Löscht der Wert Install Directory aus dem Schlüssel HKEY_CURRENT_USER|Software\Netscape\Netscape\7.01 (de)\Main

Beispiel:

Action1=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\MostRecentClipsjkljkjl
...

und löscht in den Registryverzeichnissen wegen * bei Wertename alle Werte!

Beispiel:

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

Löscht alle Werte im Schlüssel HKEY_CURRENT_USER\Software\Netscape\Netscape\7.01 (de)\Main. Unterschlüssel werden nicht angetastet!

Einen Wert in die Registry schreiben

Syntax:
Action#=**reg|setvalue|**HKEY|Pfad|Wertename|Typ|Wert

Wobei HKEY einen der folgenden Werte annehmen kann:

- HKEY_CURRENT_USER oder HKCU
- HKEY_LOCAL_MACHINE oder HKLM
- HKEY_CLASSES_ROOT oder HKCR
- HKEY_CURRENT_CONFIG oder HKCC
- HKEY_USERS oder HKUS

Wobei Typ einen der folgenden Werte annehmen darf:

- s entspricht dem Typ REG_SZ, also Text
- n entspricht Ganzzahl, Typ REG_DWORD
- b entspricht Wahrheitswert, 0 bedeutet falsch, 1 bedeutet wahr

Es wird notfalls ein komplett neuer Schlüssel mit Wertename und Wert angelegt.
Soll der Eintrag Standard erstellt werden, ist der Wert default bei Wertename zu übergeben.

Beispiel:
Action1=reg|SETVALUE|HKCU|
Software\ArchiCrypt\Shredder6|default|s|ArchiCrypt ist genial

Schreibt in den Schlüssel
HKEY_CURRENT_USER\Software\ArchiCrypt\Shredder6 als Standardwert den Text "ArchiCrypt ist genial".

11.2.5.3 Registry Im-/Export

Mit den Aktionen der Kategorie Registry Im-/Export können ganze Schlüssel der Registry sichern und wieder zurückspielen.

Einen Schlüssel aus der Registry exportieren

Syntax:
Action#=regex|EXPORT|HKEY|Pfad|Zieldatei

Wobei HKEY einen der folgenden Werte annehmen kann:

- HKEY_CURRENT_USER oder HKCU
- HKEY_LOCAL_MACHINE oder HKLM
- HKEY_CLASSES_ROOT oder HKCR
- HKEY_CURRENT_CONFIG oder HKCC
- HKEY_USERS oder HKUS

Beispiel:
Action1=regex|EXPORT|HKEY_CURRENT_USER|
Software\ArchiCrypt\Shredder6|I:\Shredder6.reg

Exportiert den Schlüssel
HKEY_CURRENT_USER\Software\ArchiCrypt\Shredder6 in die
Datei I:\Shredder6.reg

Der Inhalt der Datei sieht in etwa wie folgt aus:

```
1 Windows Registry Editor Version 5.00
2
3 [HKEY_CURRENT_USER\Software\ArchiCrypt\Shredder6]
4 "RootDir"="G:\\ArchiCrypt Shredder 6\\application\\"
5 @="ArchiCrypt ist cool"
6
7 [HKEY_CURRENT_USER\Software\ArchiCrypt\Shredder6\Common
8 "MainForm"="200,0,1,543,207,1343,807"
9
10 [HKEY_CURRENT_USER\Software\ArchiCrypt\Shredder6\fmMai
11 "Left"="-1702"
12 "Top"="112"
13 "Right"="-902"
14 "Bottom"="712"
15 "Maximized"="0"
16
17 [HKEY_CURRENT_USER\Software\ArchiCrypt\Shredder6\Gener
```

Wenn Sie der Datei die Dateiendung reg geben, genügt später ein Doppelklick auf die Datei, um den Inhalt wieder in die Registry zu übernehmen.

Einen Schlüssel aus einer Datei in die Registry importieren

Syntax:
Action#=regex|IMPORT|Quelldatei

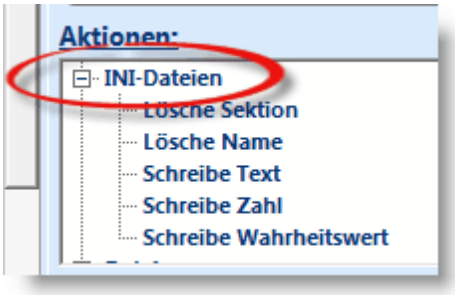
Die Quelldatei muss zuvor über einen Aufruf der regex|Export| Funktion (siehe oben) erstellt worden sein.

Beispiel:
Action1=regex|IMPORT|I:\Shredder6.reg

Importiert alle Inhalte aus der angegebenen Datei in die Registry

11.2.5.4 Ini-Dateien

Mit den Aktionen der Kategorie Ini-Dateien können Sie Initialisierungsdateien manipulieren.



Eine SEKTION aus einer Ini-Datei entfernen

Syntax:
Action#=ini|DELSECTION|INI-Datei|Sektionsname

Beispiel:
Action1=ini|DELSECTION|%AppData%\Shredder6\Shredder.ini|General

Löscht die komplette Sektion General aus der angegebenen Ini Datei.

Einen Wert aus einer Ini-Datei entfernen

Syntax:
Action#=ini|DELVALUE|INI-Datei|Sektionsname|Wertename

Der Wertename darf dabei Jokerzeichen * und ? enthalten.

Beispiel:
Action1=ini|DELVALUE|%AppData%\Shredder6\Shredder.ini|General|Create RP

Löscht den Wert Create RP aus der Sektion General der angegebenen Ini Datei.

Beispiel:

Action1=ini|DELVALUE|%AppData%
\Shredder6\Shredder.ini|SecureDeletionZone|Log*

Löscht aus der Sektion SecureDeletionZone alle Werte die mit Log beginnen.

Einen Wert in eine Ini-Datei schreiben

Syntax:
Action#=ini|setvalue|Ini-Datei|Sektionsname|Wertename|Typ|Wert

Wobei Typ einen der folgenden Werte annehmen darf:

- s entspricht dem Typ Text
- n entspricht Ganzzahl
- b entspricht Wahrheitswert, 0 bedeutet falsch, 1 bedeutet wahr

Existiert die Ini Datei nicht, wird sie erstellt und die Sektion und der Wert werden entsprechend geschrieben.

Beispiel:
Action1=ini|SETVALUE|%AppData%
\Shredder6\Shredder.ini|General|Create RP|n|1

Schreibt den Wert Create RP mit dem Zahlenwert 1 in die Sektion General der angegebenen INI Datei.

Beispiel:
Action1=ini|SETVALUE|%AppData%
\Shredder6\Shredder.ini|DuplicateFinder|QuarantinePath|s|I:\DFQuarantine

Schreibt den Wert QuarantinePath mit dem Wert I:\DFQuarantine als Text in die Sektion DuplicateFinder der angegebenen Ini Datei

11.2.5.5 Dateien

Mit den Aktionen der Kategorie Dateien können Sie Dateien löschen, umbenennen, kopieren und verschieben.

Eine Datei löschen - Lösche Datei und Lösche Datei beim Booten

Syntax:
Action#=file|delete|Dateiname|++ oder --

Der Dateiname darf Jokerzeichen * oder ? enthalten.

++ bedeutet rekursiv
-- bedeutet nur in diesem Verzeichnis
++ oder -- **muss zwingend** angegeben werden!!

Beispiel:
Action1=file|delete|I:\AdvOfficePagerDemo\blog*.php|--

Alle im Verzeichnis I:\AdvOfficePagerDemo\blog*.php gespeicherten Dateien mit der Dateiendung php werden gelöscht. Unterverzeichnisse werden wegen -- nicht angetastet.

Beispiel:
Action1=file|delete|I:\AdvOfficePagerDemo\blog*.php|++

Alle im Verzeichnis I:\AdvOfficePagerDemo\blog*.php gespeicherten Dateien mit der Dateiendung php werden gelöscht. Wegen der Angabe von ++ werden auch in Unterverzeichnissen

von I:\AdvOfficePagerDemo\blog\ Dateien mit der Endung php gelöscht!

Manche Dateien können nicht während des normalen Betriebs gelöscht werden. Sie sind blockiert. Zu diesem Zweck besteht die Möglichkeit, die Dateien zum Löschen beim nächsten Booten des Rechners vorzumerken.

Syntax:
Action#=file|rebootdelete|Dateiname|++ oder --

Beispiel:
Action1=file|rebootdelete|I:\AdvOfficePagerDemo\blog*.php|--

Alle im Verzeichnis I:\AdvOfficePagerDemo\blog*.php gespeicherten Dateien mit der Dateiendung php werden beim nächsten Start des Rechners gelöscht. Unterverzeichnisse werden wegen -- nicht angetastet.

Eine Datei umbenennen

Syntax:
Action#=file|RENAME|Dateiname|Dateiname neu

Es sind KEINE Jokerzeichen erlaubt. Der Dateiname muss mit komplettem Pfad angegeben sein, Dateiname neu darf den Pfad NICHT enthalten!

Beispiel:
Action1=file|rename|I:\Kunden\Daten\Rechnungen.db|Rechnungen2011.db

Benennt die Datei Rechnungen.db im Verzeichnis I:\Kunden\Daten\Rechnungen.db in Rechnungen2011.db um.

Dateien verschieben

Syntax:
Action#=file|MOVE|Dateiname|Zielpfad

Es sind Jokerzeichen im Dateinamen erlaubt.

Beispiel:
Action1=file|move|I:\Kunden\Daten*2010.db|Q:\Datensicherung2010

Verschiebt alle Dateien im Verzeichnis I:\Kunden\Daten\ und der Maske *2010.db in das Verzeichnis Q:\Datensicherung2010

Dateien kopieren

Syntax:
Action#=file|COPY|Dateiname|Zielpfad

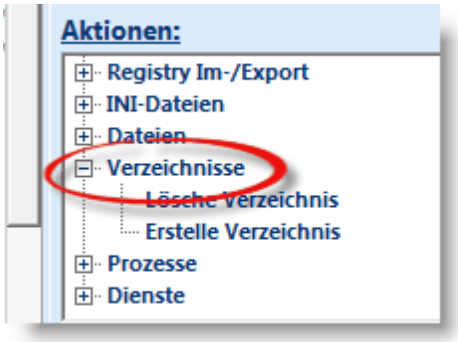
Es sind Jokerzeichen im Dateinamen erlaubt.

Beispiel:
Action1=file|copy|I:\Kunden\Daten*2010.db|Q:\Datensicherung

Kopiert alle Dateien aus dem Verzeichnis I:\Kunden\Daten\ und der Maske *2010.db in das Verzeichnis Q:\Datensicherung2010

11.2.5.6 Verzeichnisse

Mit den Aktionen der Kategorie Verzeichnisse können Sie Verzeichnisse samt Inhalt löschen und neue Verzeichnisse anlegen.



Ein Verzeichnis löschen

Syntax:
Action#=path|deletepath|Verzeichnis

Es sind keine Jokerzeichen erlaubt.

Beispiel:
Action1=path|deletepath|I:\AdvOfficePagerDemo\blog

Alle im Verzeichnis I:\AdvOfficePagerDemo\blog gespeicherten Dateien werden inkl. aller Unterverzeichnisse gelöscht. Das Verzeichnis I:\AdvOfficePagerDemo\blog selbst bleibt erhalten.

Wenn Sie möchten, dass das angegebene Verzeichnis ebenfalls gelöscht wird, geben Sie als letzten Parameter INCLUDEPATH an.

Beispiel:
Action1=path|deletepath|I:\AdvOfficePagerDemo\blog|INCLUDEPATH

Alle im Verzeichnis I:\AdvOfficePagerDemo\blog gespeicherten Dateien werden inkl. aller Unterverzeichnisse gelöscht. Das Verzeichnis I:\AdvOfficePagerDemo\blog wird ebenfalls gelöscht.

Ein Verzeichnis erstellen

Syntax:

Action#=path|createpath|Verzeichnis

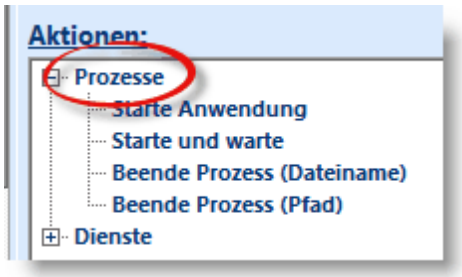
Es sind keine Jokerzeichen erlaubt.

Beispiel:
Action1=path|createpath|I:\AdvOfficePagerDemo\blog\2012\Juni

Erstellt das angegebene Verzeichnis, sofern es nicht bereits existiert.

11.2.5.7 Prozesse

Mit den Aktionen der Kategorie Prozesse können Sie Anwendungen starten und beenden.



Anwendung starten ohne auf Ende zu warten - Starte Anwendung

Syntax:
Action#=proc|CREATE|Pfad

Es sind keine Jokerzeichen erlaubt.

Beispiel:
Action1=proc|CREATE|%WINDIR%\notepad.exe

Startet das Programm Notepad ohne auf das Beenden von Notepad zu warten.

Anwendung starten und auf Ende warten - Starte und warte

Syntax:
Action#=proc|CREATEANDWAIT|Pfad

Es sind keine Jokerzeichen erlaubt.

Beispiel:
action1=proc|CREATEANDWAIT|%WINDIR%\system32\notepad.exe
action2=proc|CREATE|%SYSTEM%\system32\calc.exe

Startet das Programm Notepad und wartet auf das Beenden von Notepad. Startet dann den Taschenrechner.

Eine Anwendung beenden

ACHTUNG: Anwendungen werden beendet, ohne eventuell ungesicherte Daten zu speichern. Entspricht dem Beenden über den Taskmanager des Systems.

Nur mit Dateiname

Syntax:
Action#=proc|KILL|FILENAME|Dateiname

Dateiname enthält keine Pfadangabe

Beispiel:
Action1=proc|KILL|FILENAME|notepad.exe

Sofern eine Instanz von Notepad.exe gefunden wird, wird die Anwendung beendet.

Mit Pfadangabe

Syntax:
Action#=proc|KILL|FULLPATH|Dateiname

Dateiname enthält keine Pfadangabe

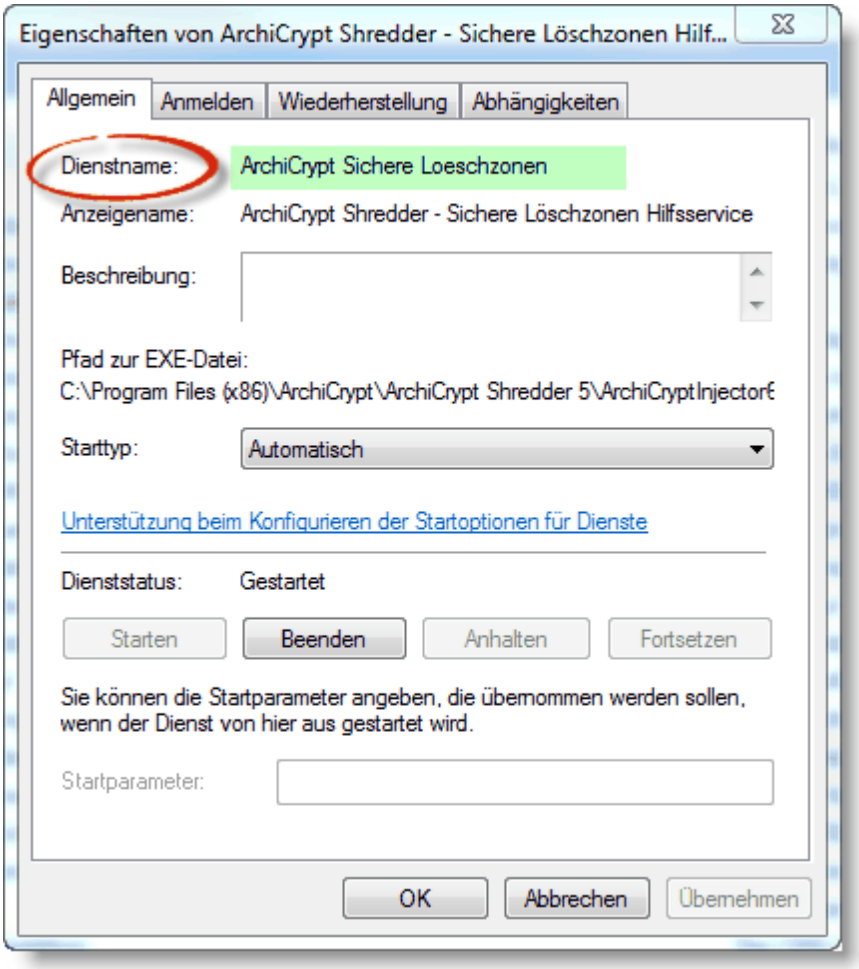
Beispiel:
Action1=proc|KILL|FULLPATH|%WINDIR%\system32\notepad.exe

Sofern eine Instanz von Notepad.exe gefunden wird, die genau der Pfadangabe entspricht, wird die Anwendung beendet.

11.2.5.8 Dienste

Mit den Aktionen der Kategorie Dienste können Sie Dienste aktivieren, deaktivieren und löschen.

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.



Einen Dienst deaktivieren

Syntax:
Action#=serv|DEACTIVATE|Dienstname

Beispiel:
Action1=serv|deactivate|ArchiCrypt Sichere Loeschzonen

Deaktiviert den Dienst mit dem Dienstname ArchiCrypt Sichere Loeschzonen.

Einen Dienst aktivieren

Syntax:
Action#=serv|ACTIVATE|Dienstname

Beispiel:
Action1=serv|activate|ArchiCrypt Sichere Loeschzonen

Aktiviert den Dienst mit dem Dienstname ArchiCrypt Sichere Loeschzonen.

Einen Dienst löschen

Syntax:
Action#=serv|DELETE|Dienstname

Beispiel:
Action1=serv|DELETE|ArchiCrypt Sichere Loeschzonen

Löscht den Dienst mit dem Dienstname ArchiCrypt Sichere Loeschzonen. Der Dienst kann nicht mehr mit activate aktiviert werden!

12 Technischer Teil

12.1 Verschiedene Betriebs- und Dateisysteme

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

Windows zeichnet sich unter anderem dadurch aus, dass es eine ausgefeilte *Rechteverwaltung* und ein *transaktionsorientiertes* Dateisystem NTFS verwendet. Nur in Einzelfällen kommen die Dateisysteme FAT und xFAT auf internen Speichermedien zum Einsatz.

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 verwaltet*. In einer Art *Inhaltsverzeichnis* merkt sich das System, *wo welche Datei abgelegt ist*.

Die Art und Weise, wie das Betriebssystem die Informationen ablegt und organisiert, ist für normale Anwendungen vollkommen unwichtig. Genau dieses Wissen ist jedoch notwendig, wenn es darum geht, Dateiinhalte so zu löschen, dass die Inhalte nicht mit einfachen Mitteln wieder hergestellt werden können.

Das Aufkommen nicht magnetischer Datenträger wirkt dieser Forderung unter Umständen erheblich entgegen. Ist es bei magnetisierbaren Datenträgern noch möglich, die zu löschenden Anteile ganz *gezielt anzusteuern*, ist dies bei neueren Datenträgern wie zum Beispiel SSD (*Solid State Disk*) nicht mehr ohne weiteres möglich. *Die tatsächlichen Gegebenheiten (wo liegen die Daten physikalisch) werden oft hinter der technischen Realisierung verborgen.*

Ein *sicheres Löschen* kann ***nicht mehr zu 100% garantiert*** werden! ArchiCrypt Shredder bringt mit den SSD Funktionen 65 und der Sonderbehandlung von Daten 183, die von einer SSD gelöscht werden, Werkzeuge mit, mit denen man sensible Daten auch von *Solid State Disks* mit hoher Sicherheit löschen kann.

Dateien, die mit Mitteln des Betriebssystems gelöscht wurden, sind nicht wirklich gelöscht

Viele Anwender wissen nicht, dass Dateien, die Sie im Windows Explorer löschen, nicht wirklich gelöscht sind. Daten sind auch dann nicht gelöscht, wenn der Papierkorb geleert wird!

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 und kann, mit etwas Aufwand, weiterhin gefunden werden.

ArchiCrypt Shredder kümmert sich um das Buch!

Werden *neue Daten* auf den Datenträger geschrieben, erfolgt das nicht zwingend an der Stelle, an der die vermeintlich "gelöschte" Datei steht.

Zudem verhindert die *intelligente Speicherverwaltung* des Systems, das Daten sicher überschrieben werden können. Das *Betriebssystem* schreibt Daten nicht unmittelbar auf den Datenträger, sondern *behält die Daten zunächst im Hauptspeicher*.
Erst dann, wenn der Rechner im Leerlauf ist oder das System heruntergefahren wird, werden die Daten dann tatsächlich auf den physikalischen Datenträger geschrieben.

Dadurch entstehen **Probleme**, die sich unmittelbar auf unser Bestreben, Daten sicher zu löschen, auswirken:

1. Man öffnet die Datei, die man sicher löschen möchte.
2. Das System lädt die Datei in den Hauptspeicher.
3. Jetzt schreiben wir Daten in die Datei um den Inhalt zu zerstören.
4. Das System ändert nur den Inhalt im Hauptspeicher, noch nicht auf dem Datenträger.
5. Zum Schluss unserer Löschaktion teilen wir dem System mit, dass wir die Datei löschen möchten.
6. Das System sieht den Löschwunsch und verwirft alle Schreibaktionen, die ja bisher ausschließlich im Hauptspeicher stattfanden. Stattdessen wird einfach der Eintrag aus dem "Inhaltsverzeichnis" auf dem Datenträger entfernt. Auf dem Datenträger befinden sich folglich immer noch die ursprünglichen Daten, die wir ja eigentlich sicher überschreiben wollten.

ArchiCrypt Shredder schaltet diese Mechanismen ab und sorgt so dafür, dass die Daten tatsächlich physikalisch auf den Datenträger geschrieben werden. Die "Intelligenz" des Systems, die sonst sehr

nützlich ist, wird deaktiviert um Daten sicher zu löschen. **Dadurch benötigen Schreibvorgänge deutlich länger!**

Das transaktionsorientierte Dateisystem von Windows NT speichert *Informationen über Dateien* in anderen 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 (*Richtwert bis 4 Kilobyte*), 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.

Im Zusammenhang mit *Sicherem Löschen* ist es wichtig zu wissen, dass man zwar gezielt auf bestimmte Cluster des Datenträgers zugreifen kann, nicht aber *auf Einträge in der MFT-Struktur*. Für uns bedeutet das, dass wir diese kleinen, unmittelbar in der MFT selbst gespeicherten Dateien nicht direkt löschen können!

Eine weitere Besonderheit des NTFS Dateisystems ist die s.g. *Transaktionsorientiertheit*. Änderungen in Dateien 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 7 bis Windows 10

Darüber hinaus bieten Windows 7 bis 10 weitere Besonderheiten, die in einem weiteren Kapitel[28] behandelt werden.

12.2 Wichtige Begriffe

Freispeicher

Definition Freispeicher: Der Freispeicher ist ein *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

Definition Clustertips: Der grobe Aufbau der Datenträgerstruktur unter Microsoft Betriebssystemen wurde unter "Verschiedene Betriebs- und Dateisysteme[40]" 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 *4096 Byte*.
Wollen Sie jetzt eine Datei speichern, die 723 Byte enthält, wird ein *kompletter Cluster* reserviert, d.h. 4096 Byte. Von diesen 4096 Byte sind *3373 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* eines Clusters wird durch den *Inhalt einer Datei* 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 dieser neu geschriebenen Datei 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.

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 mit neuen Daten.

Ich bin eine neue Datei

Das Ergebnis sieht jetzt unter Umständen so aus

Ich bin eine neue Datei es Passwort, es lautet Gustav 23

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

Die sensiblen Informationen sind fast komplett erhalten und weiterhin softwaretechnisch extrem 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 den *Umgang mit Clustertips* und bereinigt auch diesen schwer zugänglichen Anteil.

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.

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 68.

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 66.

Löschzonen 72

Sichere Löschzonen sind Orte auf Ihrem Rechner, an denen der Shredder unsichere Löschoperationen beliebiger Anwendungen abfängt und durch sichere Löschmethoden ersetzt.

12.3 Überschreiben mit kryptografischen Zufallsdaten

Schnelles Überschreiben mit Zufallsdaten

Kryptografische Zufallsdaten

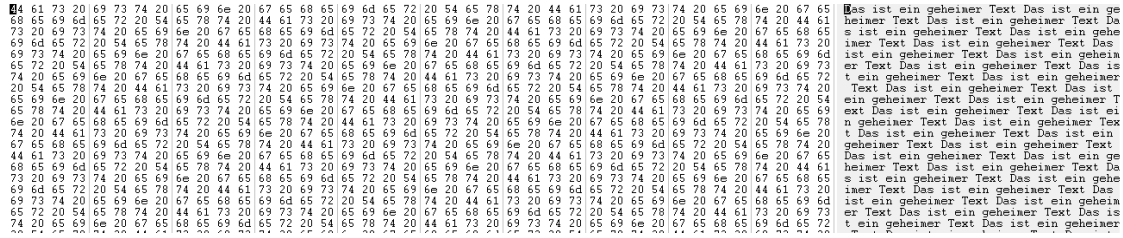
Bei dieser Methode werden die zu löschenden Daten mit Zufallszahlen in einem einzigen *Durchlauf* überschrieben. Die Zufallsdaten werden mit einem Zufallsgenerator basierend auf AES im Counter Mode gemäß NIST Special Publication 800-90 erzeugt.

Kryptografische Zufallsdaten Plus

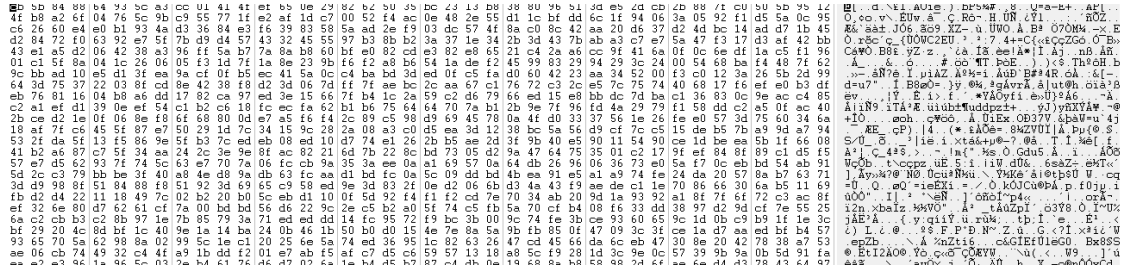
Diese Methode führt *zwei Schritte* aus. Im ersten Schritt werden wie oben beschrieben kryptografische Zufallsdaten über die Daten geschrieben. In einem zweiten Schritt wird abschließend das Muster 0xFF über die Daten geschrieben.

Die so erhaltenen *Zufallsdaten* sind *von sehr hoher Güte* und werden im Normalfall in kryptografischem Kontext (*Schlüssel, Salt-Werte, Initialisierungsvektoren*) verwendet!

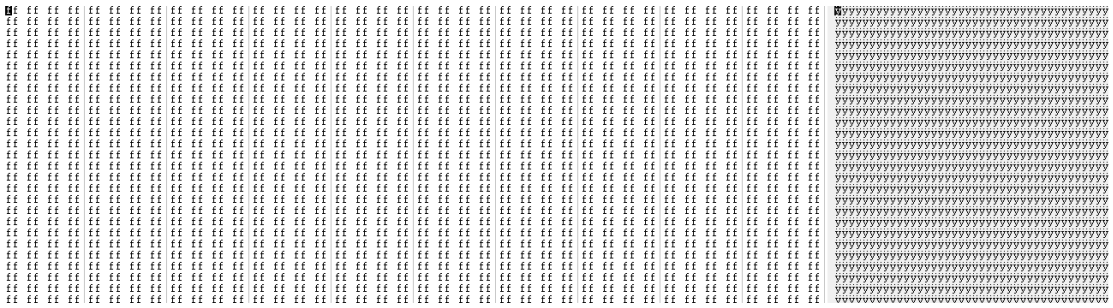
Originaldatei:



Nach dem Überschreiben mit kryptografischen Zufallsdaten:



Nach dem Überschreiben mit Muster FF:



Warum das zusätzliche Überschreiben mit abschließendem Muster?

Wenn die Daten in einem einzigen Arbeitsgang mit Zufallsdaten überschrieben werden, können die geschriebenen Daten natürlich ausgelesen werden. Mit diesen Daten und physikalischen Untersuchungsmethoden kann theoretisch ein Differenzbild (*ursprüngliche Daten und ausgelesene Zufallsdaten*) erzeugt werden, welches Rückschlüsse (*keine komplette Rekonstruktion*) zulassen könnten.

Überschreibt man zusätzlich mit einem Muster, *verschwinden auch die Zufallsdaten* hinter einer *diffusen Nebelwand*. Die Verwendung kryptografischen Zufalls macht eine Rekonstruktion der Zufallsdaten ebenfalls unmöglich. Die Konstruktion eines Differenzbildes ist nicht mehr möglich.

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

siehe auch Einstellungen Löschverfahren und Sicherheit 182

12.4 BSI-2011-VS

Umsetzung der Technischen Leitlinie BSI TL-03423 des *Bundesamtes für Sicherheit in der Informationstechnik* (*BSI*) in der Fassung vom April 2016.

In der *technischen Leitlinie* werden zwei Verfahren definiert. Das Verfahren BSI-2011-VS ist in einer modifizierten Form in ArchiCrypt Shredder 8 umgesetzt.

Beschreibung des Verfahrens und der in ArchiCrypt Shredder vorgenommenen Modifikation

1. Erzeugen eines zufälligen Schlüssels und eines zufälligen Initialisierungsvektors für den Verschlüsselungsalgorithmus AES (*Advanced Encryption Standard*) in der 128 BIT Version.

In Abweichung zur Empfehlung des BSI, wird AES im CBC Modus betrieben. Der CBC Modus kann als gleichwertig angesehen werden und ist im Gegensatz zum empfohlenen OFB Modus in der MS Crypto API vorhanden.

Zur *Erzeugung der Zufallswerte* wird auf diverse *Systemzustände und Nutzeraktionen* zurückgegriffen (*AES counter-mode based PRNG specified in NIST Special Publication 800-90*). Schlüssel und IV werden während der Operationen *im Hauptspeicher* gehalten und *nach der Verwendung sicher gelöscht*. Der Chiffrestrom mit dem die Daten überschrieben werden ist also nicht mehr rekonstruierbar!

2. Die Datenmuster werden jetzt mit AES 128 BIT fortlaufend als 128 BIT Blöcke rekursiv erzeugt.

3. Die Datenmuster werden fortlaufend über die zu überschreibenden Datenblöcke geschrieben, wobei grundsätzlich eventuell zu berücksichtigende Clustertips[44] mit überschrieben werden.

4. Wurde die Verifikation aktiviert, wird für jeden einzelnen 128 BIT Block geprüft, ob der auf dem Datenträger vorhandene Inhalt mit dem entsprechend berechneten Muster übereinstimmt. Schlüssel und Initialisierungsvektor werden in dieser Phase aus dem Speicher entfernt.

5. Die Daten werden jetzt erneut überschrieben. Dabei wird das Muster 0xFF verwendet.

6. Wurde die *Verifikation* aktiviert, wird jetzt eine Stichprobenverifikation vorgenommen, bei der *10% der geschriebenen Daten* überprüft werden. Die Prüfung erfolgt dabei am Anfang der Daten, am Ende der Daten und gleichmäßig verteilt über den Rest.

Anm.: Die Generierung der Zufallsdaten und damit die Berechnung der Blöcke für das Überschreiben werden für jede Löschaktion (jede Datei, Freispeicher, Clustertips, Partition) neu berechnet.

12.5 DoD 5220.22-M

Beide Verfahren werden nicht mehr empfohlen

siehe BSI-2011-VS (modifiziert) 48

und Empfehlungen zu Löschverfahren 184

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 182 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.

12.6 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. Das Verfahren wurde durch eine neue Richtlinie ersetzt und ist nicht mehr gültig.

VSITR in dieser Form wird nicht mehr empfohlen

siehe BSI-2011-VS (modifiziert) 48

und Empfehlungen zu Löschverfahren 184

12.7 Peter Gutman

Peter Gutman wird nicht mehr empfohlen

siehe BSI-2011-VS (modifiziert) 48

und Empfehlungen zu Löschverfahren 184

Löschen mit Peter Gutman

In seinem Aufsatz Secure Deletion of Data from Magnetic and Solid-State Memory erläuterte Peter Gutman ein Verfahren zum Löschen von

Daten auf verschiedenen Medien. Das Verfahren von Peter Gutman ist sehr zeitintensiv, wurde jedoch als äußerst sicher angesehen.

Die *Gefahr*, mit Hilfe der bekannten Muster und einer darauf beruhenden Differenzbildung auf die ursprünglichen Daten zu schließen, lässt die Methode für den Einsatz in einer hochsensiblen Umgebung als nicht mehr geeignet erscheinen.

12.8 Solid State Disk - SSD

- Was Sie über eine SSD wissen sollten

  Eine *Solid-State-Disk* bzw. ein *Solid-State-Drive* (*kurz SSD genannt*), ist ein nichtflüchtiger Datenspeicher. Im Gegensatz zu *magnetisierbaren Laufwerken* (*Hard Disk Drive - HDD*) enthalten SSDs keine mechanischen Teile. Hier gibt es keinen Schreib-/Lesekopf, der beim Lesen oder Schreiben von Daten zunächst an die richtige Stelle bewegt werden muss. Daher sind SSDs zumeist den HDDs in Hinsicht auf Schreib-/Lesegeschwindigkeiten überlegen.

  Wie bereits erwähnt, löscht das Betriebssystem Daten einer Datei nicht, sondern *entfernt den zugehörigen Eintrag aus dem Inhaltsverzeichnis* des Dateisystems. Der Löschvorgang ist damit sehr schnell, gestattet jedoch mit recht einfachen Mitteln ein Wiederherstellen der Datei. Um die Wiederherstellung zu verhindern, steuert ArchiCrypt Shredder die entsprechenden Speicherstellen gezielt an und überschreibt die Daten so, dass ein Wiederherstellen der Inhalte nicht mehr möglich ist.

  Was bei klassischen HDDs sehr gut funktioniert, klappt bei SSDs, die nach einem gänzlich anderen Prinzip arbeiten, nicht mehr so einfach. ArchiCrypt Shredder muss andere Verfahren anwenden.

  Durch die s.g. Nutzungsverteilung werden Schreibvorgänge auf Speicherzellen geleitet, die bisher am wenigsten genutzt wurden. Per Zufall wird dies früher oder später die Speicherzelle sein, in der sich Daten einer ganz bestimmten gelöschten Datei befanden. Gezieltes Löschen ist also nahezu unmöglich bzw. eher Zufall. Diese Umleitung der Schreibvorgänge geschieht im *Controllerchip* der SDD so, dass System und Anwendungen nichts davon mitbekommen.

Nach einer gewissen Einsatzzeit ist quasi jede Speicherzelle der SSD mit Daten belegt. Entweder liegen dort Daten aktueller Dateien oder die *Überreste gelöschter* (*besser: aus dem Inhaltsverzeichnis entfernter Dateien*) - Dateien. Soll jetzt eine Datei neu geschrieben werden, muss die SSD zunächst jede Speicherzelle gelöscht werden, bevor man die neuen Daten schreiben kann. Dies ist natürlich zeitaufwendiger, als der reine Schreibvorgang. Im Prinzip verdoppelt sich die Zeit für einen Schreibvorgang. Die Leistung einer SSD, die sich länger im Einsatz befindet, bricht also nach einer gewissen Zeit dramatisch bei Schreibvorgängen ein.

Hier kommt das s.g. TRIM Kommando zum Einsatz. Das TRIM Kommando ist bei SSDs anwendbar, die seit etwa Mitte 2009 zum Einsatz kommen. TRIM sorgt dafür, dass das SSD Laufwerk im Leerlauf als gelöscht markierte Speicherzellen tatsächlich freigibt. Der Zusatz "im Leerlauf" ist wichtig. Unter Windows 10 kann man mit dem RETRIM Kommando dafür sorgen, dass das SSD Laufwerk vom System entsprechende Leerlaufzeit erhält.

Das TRIM Kommando sorgt für zwei Dinge:

1. Die SSD bleibt dauerhaft schnell
2. Gelöschte Daten können nicht mehr oder nur mit extremem Aufwand wieder hergestellt werden.

Trotz aller Maßnahmen kann man aufgrund der Art, wie SSDs arbeiten, nicht zu 100% garantieren, dass jedes *BIT/Byte* einer Datei tatsächlich überschrieben wird. Lesen Sie sich daher den Nachfolgenden Informationskasten genau durch!

WICHTIG: *Ist sicheres Löschen bei einer SSD überhaupt möglich?*

JEIN! Sollten Sie mit hochbrisanten Daten arbeiten (*geheim, streng geheim - secret, top secret*), dann muss die SSD im Falle eines Falles vernichtet werden. Da derart eingestufte Daten entsprechend wertvoll sind, ist der finanzielle Verlust durch physische Zerstörung der SSD vernachlässigbar!

Warum JEIN? Der *SSD-Controller* legt fest, wann eine Speicherzelle wirklich freigegeben bzw. bei einem Schreibvorgang tatsächlich angesteuert wird. Man kann also nicht verlässlich vorhersagen, wann das SSD-Laufwerk bestimmte Daten tatsächlich löscht. Nur direkte so genannte ATA-Befehle (*AT Attachment, Advanced Technology- ATA-Secure Erase*) erlauben prinzipiell ein zuverlässiges Zurücksetzen einer bestimmten Speicherzelle.

Unter Windows 10 kann man mit dem RETRIM Kommando sehr verlässlich dafür sorgen, dass die Speicherzellen tatsächlich überschrieben werden. Kritischer ist der Umstand dass SSDs während des Abnutzungsausgleichs (*Nutzungsverteilung*) einen kleinen nicht zugewiesenen Speicherplatz als Puffer verwenden (*Spare Area*). Diese Speicherzellen dieses Puffers werden verwendet um Daten darin zu speichern. Andere Zellen, in denen sich noch Nutzdaten befinden, werden einfach elektronisch ausgeblendet. Leider bedeutet dies, dass SSDs für eine Reihe von Datenwiederherstellungstechniken anfällig sind. Die Wiederherstellung von Daten einer SSD ist technisch sehr anspruchsvoll. Hier müssen spezielle Labore ran, die auch nur dann erfolgreich sind, wenn es bei der Wiederherstellung nur um aktuelle Daten (*also nicht um bereits gelöschte Daten*) geht. Mit Software ist ein Auslesen nicht möglich. Erst eine Kombination aus spezieller Software mit einem speziellen Controller, der den *Flash Translation Layer* (*FTL*) [*ordnet der physikalischen Speicherzelle eine Adresse zu*] umgeht, um so verlässlich Flash Speicherzellen anzusteuern und auszulesen, machen das Herstellen von Datenfragmenten möglich.

Wie kann ich die Wiederherstellung von Daten von einer SSD möglichst verhindern?
Wenn man eine SSD also mit TRIM/RETRIM vorbereitet und zusätzlich den Freispeicher[63] bereinigt, ist die Chance, Daten wiederherstellen zu können, nahe NULL. Trotz der beschriebenen Mechanismen (*kein gezieltes Ansteuern einer Speicherzelle aus einer Software heraus, spezielle Arbeitsweise des Controllers*), ist das Auslesen bzw. Wiederherstellen von Daten kein Kinderspiel.

Sind die Spezialwerkzeuge der Hersteller ein Mittel, um Daten auf

einer SSD 100% sicher zu löschen?
NEIN! Diese Werkzeuge bieten das s.g. ATA-*Secure Erase* an. Die Arbeitsweise der Controller und die Umsetzung des *Secure Erase* liegen jedoch im Verborgenen und arbeiten nicht 100% zuverlässig. Das System und Anwendungsprogramme wissen schlicht nicht, wo die Daten in der Hardware selbst liegen. Der Controller verschleiert quasi die physikalischen Gegebenheiten.

FAZIT *Sicheres Löschen* von Daten auf einer SSD ist kompliziert bzw. nicht wirklich möglich. Es bleibt immer ein *Restrisiko*. Und zwar auch dann, wenn der Hersteller vorgibt, dass *Secure Erase ATA* Kommando implementiert zu haben. Andererseits ist die *Wiederherstellung* der Daten ebenso *kompliziert*. Ohne Modifikation/Austausch von Teilen der Steuerelektronik der SSD ist eine Wiederherstellung nicht möglich. Die Aussage, dass ArchiCrypt Shredder Daten so löscht, dass sie mit *Software-technischen Mitteln* nicht wiederhergestellt werden können, gilt also auch für eine SSD.

TRIM
Hat Shredder TRIM auf Ihrem Rechner aktiviert 65, dann sendet das Betriebssystem *beim Löschen einer Datei* eine Information an die SSD, dass die zugehörigen Speicherzellen für ein Überschreiben vorbereitet werden sollen.
Im Klartext: Die SSD überschreibt die Speicherzellen, sobald sie sich im Leerlauf befindet.

RETRIM
RETRIM ist ein spezielles Kommando, welches dafür sorgt, dass die SSD auch genügend Leerlauf hat, um alle ausstehenden TRIM Befehle auszuführen und die Daten in betroffenen Speicherzellen zu überschreiben.
Im Klartext: Retrim ist ein Trim mit *Ausführungsgarantie*!

12.9 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/Windows 8 und Windows 10 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 ausfallsicheren Betrieb der Systeme gewährleisten. Genau diese Mechanismen arbeiten unserer Absicht, sensible Daten sicher zu Löschen, leider entgegen. Die Betriebssysteme Windows Vista, Windows 7, Windows 8 und Windows 10 machen mit den s.g. Schattenkopien das Löschen ggf. besonders schwer. Hier sollten Sie unbedingt die besonderen Hinweise[28] beachten.

Netzlaufwerke

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. Das alleinige Überschreiben mit Nullen bietet keinen 100%igen Schutz gegen fortgeschrittene physikalische *Rekonstruktionsverfahren*. Diese Methoden zur Rekonstruktion sind allerdings äußerst aufwendig, erfordern erhebliche finanzielle Mittel und können im besten Fall nur Fragmente der Ausgangsdaten wieder

herstellen. Mit Rettungssoftware können keine Dateien wieder hergestellt werden.

Systemwiederherstellung und Schattenkopien

Windows schaltet 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 so vorgesehen hat. Den gleichen Effekt würden Sie erhalten, wenn durch "normales Arbeiten" die Kapazität der Festplatte unter einen Schwellwert fallen würde.

Kleine Dateien

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. (siehe Verschiedene Betriebs- und Dateisysteme)[40]. Ein gezieltes Schreiben in diese $MFT-Datei ist nicht möglich.

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 Freispeicherbereinigung62!

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 Löschzonen72.

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 Löschzonen72!

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. Wenn man jedoch eine solche Datei, die zuvor mit dem Shredder gelöscht wurde, wieder herstellt und sich den

Inhalt ansehen möchte, stellt man fest, dass die Datei nur Datenschrott enthält. Um die Dateinamen ebenfalls zu überschreiben wurde eine entsprechende Funktion in der Kategorie Datenträger 60 (Altlasten) realisiert.

13 FAQ-Shredder

Ich erhalte eine Fehlermeldung "Zugriffsverletzung bei Adresse..."

Um einem möglichen Fehler auf die Spur zu kommen, benötigen wir Informationen.

- Was muss man tun, um den Fehler zu reproduzieren?
  Am besten erstellen Sie eine Schritt für Schritt Anleitung.
- Auf welchem System (Betriebssystem, welche Version, 32 oder 64 BIT?) tritt der Fehler auf?

> TIPP: Ab Windows 7 bringt das System einen s.g. Problemrekorder mit. Damit können Sie die Schritte zum Reproduzieren eines Problems aufzeichnen. Suchen Sie dazu in Feld Programme/Dateien durchsuchen den Begriff psr ein. In der Trefferliste rufen Sie dann das Programm psr.exe auf. EXTERNER Link zu Microsoft (*ohne Gewähr, Stand 17.09.2018*):So bedienen Sie das Programm zur Aufzeichnung eines Problems

Optimal ist es, wenn Sie mit einer speziellen Version des Shredders einen Fehler-Report erstellen und uns diesen zusenden:

So geht es:

Laden Sie sich die spezielle Version der Shredder Anwendung über den Link weiter unten. Dabei handelt es sich um keine Installationsdatei, sondern nur um die Kernanwendung Shredder8.exe. Sie müssen das Programm also

bereits über die normale Installationsdatei auf Ihrem Rechner installiert haben.

1. *Beenden* Sie ggf. die ArchiCrypt Shredder Anwendung.

2. Öffnen Sie das *Installationsverzeichnis* der ArchiCrypt Shredder Anwendung im Windows Explorer. Zumeist ist dies der Pfad *C:\Programme\ArchiCrypt\ArchiCrypt Shredder 8*

3. Im Installationsverzeichnis finden Sie die *Originaldatei Shredder8.exe*. Benennen Sie diese Datei temporär um oder sichern Sie sie an einen anderen Ort. Sie können so die Originaldatei später bei Bedarf wieder zurückspielen.

4. Laden Sie sich die *spezielle Version* des Shredders

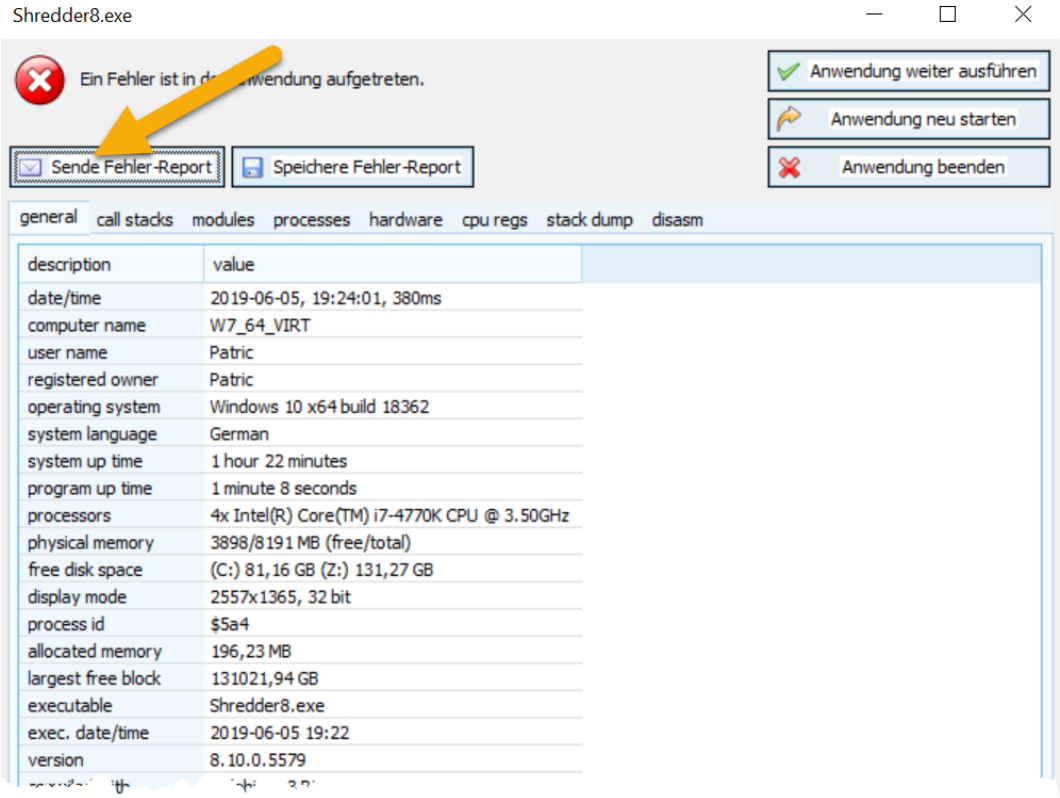
Download spezielle Shredder Version für 64 BIT

Download spezielle Shredder Version für 32 BIT

5. Extrahieren Sie jetzt die Datei *Shredder8.exe* aus der heruntergeladenen ZIP-Datei (*ArchiCryptShredder8_64_Report.zip bzw. ArchiCryptShredder8_32_Report.zip*) in das Installationsverzeichnis.

6. Starten Sie den Shredder und führen Sie die Aktionen durch, die zum Fehler führen.

7. Falls der Fehler tatsächlich innerhalb der Shredder Anwendung auftritt, öffnet sich ein *Fehlerreport-Dialog*.



Fehler-Report Shredder 8 - Support

8. *Senden* Sie uns den Fehlerreport durch Klick auf Sende Fehler-Report per E-Mail zu. Sie haben die Gelegenheit, vor dem Absenden der E-Mail zu prüfen, was uns genau zugesandt wird. Sie können gerne zum Beispiel den Screenshot entfernen, sollte dieser sensible Informationen enthalten.

Index

- - -

- $ -

- (-

- . -

- + -

- 1 -

- 3 -

- 4 -

- 6 -

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- J -

- K -

- L -

- M -

- N -

- O -

- P -

- Q -

- R -

- S -

- T -

- U -

- V -

- W -

- X -

- Z -