

<<YourApp>> **Hilfeindex**

<< Write a topic here that discusses your application's main dialog.>>

Einführung

Steganos [griechisch]: *geschützt, schützend; verdeckt, verdeckend.*

Vielen Dank, daß Sie Steganos für Windows 95 ausprobieren. Steganos ist eine einfach zu benutzende, dennoch mächtige Assistenten-Anwendung zum Verstecken und Verschlüsseln von Dateien.

Steganos verschlüsselt und versteckt beliebige Dateien in BMP-, DIB-, VOC-, WAV-, ASCII- und HTML-Dateien. (Sämtliche Features.)

Wenn Sie nur Kryptographie benutzen, schützen Sie zwar ihre Daten davor, von Unberechtigten gelesen zu werden, aber es ist dennoch offensichtlich, daß Sie Geheimnisse haben. Wenn Sie Ihre Daten nur verstecken, könnte jemand alle verdächtigen Trägerdateien durchsuchen und möglicherweise sensible Informationen finden.

Steganos kombiniert diese beiden Methoden: Kryptographie - um Ihre Daten für alle unlesbar zu machen, die Ihr Passwort nicht kennen - und Steganographie - um die Existenz Ihrer Daten zu verheimlichen. Dateien, die mit Steganos versteckt und verschlüsselt wurden, können weder gelesen noch leicht gefunden werden.

In Zukunft kann es nötig werden, die Existenz von Informationen zu verschleiern. Sie könnten eines Tages dazu gezwungen werden, Ihre Passwörter preiszugeben. In manchen Ländern ist starke Verschlüsselung schon heute verboten. Kryptographie alleine würde also nicht mehr ausreichen.

Seien Sie vorbereitet - mit Steganos für Windows 95.

Produktinformationen (Features)

Steganos für Windows 95
von Deus Ex Machina Communications

Versteckt alle Arten von Dateien in Bildern (BMP, DIB), Klangdateien (WAV, VOC) und in allen Arten von ASCII Dateien oder HTML Dokumenten.

Einfach zu benutzende Assistentenoberfläche, die für blutige Anfänger und absolute Profis gleichermaßen zweckmäßig ist.

Es besteht die Möglichkeit, Dateien nur zu verschlüsseln und nicht zu verstecken. Die dabei erstellten Steganos-verschlüsselten Dateien (.SEF) können per Doppelklick auf das Datei-Icon wieder entschlüsselt werden.

Starke Kryptographie: Der benutzte Algorithmus (HWY1) generiert einen Ausgabestream, der mit dem "Alleged RC4" ("RC4" ist ein eingetragenes Warenzeichen von RSA Data Securities Inc.), wie er von den Cypherpunks im Usenet gepostet wurde, kompatibel ist. Die Implementation in Windows 95 wurde vollständig aus der Beschreibung von Bruce Schneier (siehe "Applied Cryptography", Wiley, ISBN 0-471-11709-9) entwickelt.

Zu versteckende oder zu verschlüsselnde Dateien werden komprimiert, um die Effizienz zu erhöhen (unter Verwendung der zlib von Jean-loup Gailly und Mark Adler. Sie sind Mitglieder der Info-Zip group und stellen Code für das populäre Programm WinZip zur Verfügung).

Konvertiert Bilder mit zuwenigen Farben in 16,7 Mio.-Farben-Bilder (24-Bit-Format).

Dateien können auch nur versteckt werden (wenn Sie beispielsweise schon verschlüsselt sind).

Versteckt auch in nicht unterstützten Trägerdateien, wenn Sie einige Informationen über die Trägerdatei angeben können.

Erstellt auf Wunsch eine Sicherheitskopie der Trägerdatei, bevor Daten in ihr versteckt werden.

Optional wird die zu versteckende und/oder zu verschlüsselnde Datei nach dem Vorgang unwiderruflich gelöscht.

Verschlüsselte Dateien und Dateien, in denen Daten versteckt wurden, können sofort auf Knopfdruck per E-Mail versandt werden.

Das Dateidatum und die Dateizeit der Trägerdatei bleiben unverändert, um keinen Verdacht zu erregen.

Das Steganos SDK (Software Development Kit) ermöglicht Entwicklern, die Funktionalität der Steganographie in eigene Programme einzubauen. (Bitte lesen Sie dazu die Dokumentation im STE_SDK.ZIP)

Der Steganos Shredder vernichtet Dateien auf ihrer Festplatte unwiderruflich. (Sie müssen nur mit der rechten Maustaste auf das Datei-Icon klicken und "Senden an... Shredder" auswählen.)

Die UpdateNOW! Technologie ermöglicht es, Steganos schnell über das Internet zu aktualisieren.

Steganos für Windows 95 und der Steganos Shredder sind reine 32-Bit-Windows 95-Anwendungen.

Deus Ex Machina Communications ist eine deutsche Softwarefirma mit Sitz in Frankfurt am Main und ein

Mitglied der Association of Shareware Professionals (ASP). Im Mai 1995 veröffentlichte Deus Ex Machina Communications UFO - Universal File Operator, ein von Kunden und Presse hochgelobtes Dateiverwaltungsprogramm für DOS und Windows 95. Weitere Informationen finden Sie auf dem Deus Ex Machina Web Server <http://www.demcom.com>. Oder Sie schicken einfach eine leere E-Mail an info@demcom.com - Sie bekommen dann weitere Informationen per E-Mail zugeschickt.

Haftungsausschluss

(I) BESCHRÄNKTE GARANTIE

OBWOHL DIE AUTOREN UND BETÄTIGTE DIE VORLIEGENDEN PROGRAMME ("SOFTWARE") NACH BESTEM WISSEN UND GEWISSEN GETESTET HABEN, KANN ES DURCHAUS SEIN, DASS NOCH FEHLER ENTHALTEN SIND.

DIE FABIAN HANSMANN/SASCHA WILDGRUBE/GABRIEL YORAN GESELLSCHAFT FÜR EDV-DIENSTLEISTUNGEN UND SOFTWAREENTWICKLUNG GBR, DEUS EX MACHINA COMMUNICATIONS (HANSMANN/WILDGRUBE/YORAN GBR) GARANTIERE NICHT DIE EIGNUNG DES PROGRAMMES FÜR EINEN BESTIMMTEN ANWENDUNGSFALL ODER EINE BESTIMMTE KONFIGURATION.

DIE HANSMANN/WILDGRUBE/YORAN GBR IST NICHT HAFTBAR FÜR SCHÄDEN, DIE SICH AUS DER NUTZUNG ODER UNFÄHIGKEIT ZUR NUTZUNG DES VORLIEGENDEN PRODUKTES ERGEBEN. DIES SCHLIESST DEN VERLUST VON GESCHÄFTSGEWINNEN, DIE UNTERBRECHUNG DER GESCHÄFTLICHEN ABLÄUFE, DEN VERLUST VON DATEN SOWIE ALLE ÜBRIGEN MATERIELLEN UND IDEELLEN VERLUSTE UND DEREN FOLGESCHÄDEN EIN UND GILT SELBST DANN, WENN DIE HANSMANN/WILDGRUBE/YORAN GBR ZUVOR AUSDRÜCKLICH AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WORDEN IST.

FERNER IST DIE HANSMANN/WILDGRUBE/YORAN GBR NICHT HAFTBAR FÜR DURCH VIREN, DIE SICH ÜBER DIE VORLIEGENDEN PROGRAMME VERBREITEN, ENTSTANDENE SCHÄDEN GLEICH WELCHER ART.

(II) KRYPTOGRAPHIE-RESTRIKTIONEN

DIE REGIERUNG DER USA KLASSIFIZIERT VERSCHLÜSSELUNG ALS MUNITION. DER EXPORT SOG. "STARKER KRYPTOGRAPHIE", WIE SIE AUCH IN STEGANOS FÜR WINDOWS 95 VERWENDET WIRD, IST VERBOTEN. SOMIT DARF STEGANOS FÜR WINDOWS 95 NICHT AUS DEN USA EXPORTIERT WERDEN.

IN BESTIMMTEN LÄNDERN IST DAS VERWENDEN VON VERSCHLÜSSELUNG GAR NICHT ERLAUBT.

DEUS EX MACHINA COMMUNICATIONS IST NICHT HAFTBAR FÜR VERBOTENEN EXPORT, IMPORT ODER VERBOTENE NUTZUNG VON STEGANOS FÜR WINDOWS 95.

(III) BESTÄTIGUNG

DURCH DAS BENUTZEN DER SHAREWARE-VERSION VON STEGANOS FÜR WINDOWS 95 UND DES STEGANOS SHREDDER BESTÄTIGEN SIE, DASS SIE DEN HAFTUNGSAUSSCHLUSS GELESEN UND VERSTANDEN HABEN UND DASS SIE MIT DEN DARIN ENTHALTENEN BEDINGUNGEN EINVERSTANDEN SIND.

Copyright

Steganos für Windows 95

Copyright (c) 1996-1997 Fabian Hansmann/Sascha Wildgrube/Gabriel Yoran GbR (Deus Ex Machina Communications). Alle Rechte vorbehalten.

UpdateNOW!, Steganos Shredder

Copyright (c) 1997 Fabian Hansmann/Sascha Wildgrube/Gabriel Yoran GbR (Deus Ex Machina Communications). Alle Rechte vorbehalten.

Kompression

Zlib data compression library 1.0.4, Copyright (c) 1995-1996 Jean-loup Gailly, Mark Adler; DLL-Support von Alessandro Iacopetti.

Alle hier genannten Firmen- und/oder Produktnamen können geschützte Handelsnamen sein, ohne explizit als solche gekennzeichnet zu sein.

Den Haftungsausschluss und Bestimmungen über Kryptographie finden Sie in der Datei readme.txt

Was ist Shareware?

Wenn beim Starten von Steganos für Windows 95 einen Shareware-Hinweis sehen, benutzen Sie eine Shareware-Version. Sie dürfen die Shareware-Version von Steganos für Windows 95 30 Tage lang benutzen. Wenn Sie sie dann nach diesen 30 Tagen weiter benutzen wollen, müssen Sie sich registrieren lassen. Ansonsten müssen Sie die Shareware-Version von Ihrem System entfernen. Wählen Sie *Bestellen* im Startbild von Steganos, um weitere Informationen zu erhalten. In der registrierten Vollversion gibt es keine Shareware-Hinweise. Sie dürfen - Sie sollten sogar - die Shareware-Version an Freunde und Kollegen weitergeben. Das Programm und seine Dokumentation müssen dabei jedoch unverändert in ihrer ursprünglichen Form weitergegeben werden. Das Benutzen dieser Sharewareversion ist in dem Maße erlaubt, das nötig ist, zu entscheiden, ob Sie das Programm kaufen wollen oder nicht.

Bestellformular

Vorname Name : _____
 Tel.: _____
 Strasse u. Nr.: _____
 Fax: _____
 PLZ u. Ort : _____
 K-Nr.: _____
 Datum: _____

JDS-Software
 Jens Driese
 Registrierservice
 Postfach 1269
 D-26302 Varel

Tel.: 04451-959195
 Fax.: 04451-959196
 Box: 04451-959193
 CIS: 100273,2252
 CIS: GO "JDSONLINE"
<http://www.jds-software.com>

Bestellung:

Menge	Produkt	Einzelpreis	Summe
_____	Steganos 95 (1 User private Anwender)	49,00 DM	= _____ DM
_____	Steganos 95 (1 User gewerbliche Anwender)	79,00 DM	= _____ DM
_____	Steganos 95 (2 User gewerbliche Anwender)	110,00 DM	= _____ DM
_____	Steganos 95 (5 User gewerbliche Anwender)	235,00 DM	= _____ DM
_____	Steganos 95 (10 User gewerbliche Anwender)	430,00 DM	= _____ DM
_____	Steganos 95 (25 User gewerbliche Anwender)	890,00 DM	= _____ DM

Versandkosten Inland:

() Post-Versand per Vorkasse (+ 8,-) = _____ DM
 () UPS-Versand per Vorkasse (+ 12,-) = _____ DM
 () Post-Versand per Nachnahme (+ 13,-) = _____ DM
 () UPS-Versand per Nachnahme (+ 15,-) = _____ DM

Versandkosten Ausland:

() Post-Versand per Vorkasse (+ 15,-) = _____ DM
 (Nur per Kreditkarte, Eurocheck in DM oder Bar)

Gesamtbetrag = _____ DM

Zahlungsweise:

() Scheck/Bar liegt bei.
 () Nachnahme
 () Per Kreditkarte

Kartennummer : _____ Gueltig bis: _____

Karteninhaber: _____

Karte : () VISA () DINERS () EURO () MASTER-CARD

Die Allgemeinen Geschaeftsbedingungen erkenne ich an.

Unterschrift

Support

Schreiben Sie uns, wenn Sie eine Frage oder Anregung zum Thema Steganos oder Deus Ex Machina haben!

Internet: steganos-support@demcom.com
WWW: <http://www.demcom.com/deutsch/steganos>
CompuServe: 100735,12
BBS: 05 11/9 50 88 97 (ISDN und analog)
Mail: Deus Ex Machina Communications
Sophienstr. 28
60487 Frankfurt
Deutschland

Wie kann man eine geeignete Trägerdatei auswählen?

Benutzen Sie keine Dateien, die vielen zugänglich sind (wie beispielsweise Bilder auf einer CD-ROM oder auf Webseiten). Da jemand, der die Trägerdatei und das Original besitzt, die Existenz von versteckten Daten durch den Vergleich der Dateien nachweisen kann. Wenn Sie die Option *Verschlüsseln* beim Verstecken gewählt haben, bleiben die Daten trotzdem für alle unlesbar, die das Passwort nicht kennen.

Obwohl Steganos in der Lage ist, Daten in Textdateien zu verstecken, ist diese Methode *nicht zu empfehlen*, da Sie langsam und leicht zu entdecken ist.

Weitere Informationen

Trägerdatei

Wie versteckt Steganos Daten

Wie kann man ein sicheres Passwort wählen?

Die Sicherheit Ihrer Daten ist immer nur so gut wie Ihr Passwort. Das wichtigste bei der Auswahl Ihres Passwortes ist: Benutzen Sie jedes Passwort **immer nur einmal**.

Schlechte Passwörter sind:

- Ihr Name, Ihr Online-Name, Initialen, Telefonnummern und jede Form von persönlichen Daten, die man leicht herausfinden kann.
- Wörter, die in Datenbanken oder Lexika gespeichert sind, besonders Namen von berühmten Personen, Stars, Orte und sogar (Familien)namen im allgemeinen. Das bezieht sich besonders auch auf ausländische und da besonders auf englische Wörter.
- Passwörter, die in Fernsehserien oder Filmen vorkamen (z.B. *War Games*, *Sneakers* und *The X-Files*)
- Kraftausdrücke, Schimpfwörter und Beleidigungen
- Tastaturmuster (wie beispielsweise *QWERTZ*)
- Zeichenketten und einfache Zahlen (wie beispielsweise *AAAAA* oder *123123*)

Gute Passwörter sind:

- Zwei oder mehr Wörter, die durch ein Interpunktionszeichen getrennt sind. Die Wörter sollten keinen Sinn ergeben. Diese Art von Passwörtern werden beispielsweise von Compuserve benötigt.
- Vollständige Sätze (die nicht in schriftlicher Form gefunden werden können - wie beispielsweise in Zitatesammlungen - und nicht leicht geraten werden können)

Beispiele für gute Passwörter:

- *BLOATED:BEAR*
- *2R4e1D117u7#M* (wenn Sie alphanumerische Passwörter wie dieses verwenden, sollten 10 Zeichen genug sein)

HINWEIS: Die o.g. Passwörter sind selbstverständlich keine guten Passwörter mehr. Benutzen Sie sie nicht!

Wie kann man Daten in nicht unterstützten Trägerdateien verstecken?

Was ist eine nicht unterstützte Trägerdatei?

Steganos ist in der Lage, Daten in Dateien zu verstecken, die nicht direkt von Steganos unterstützt sind (Nicht unterstützte Trägerdateien). Diese Methode ist nicht zu empfehlen, da dabei die Trägerdatei beschädigt bzw. funktionsuntüchtig gemacht werden kann. Da Steganos weder die Länge des Dateiheaders noch die Bittiefe der nicht unterstützten Trägerdatei kennt, müssen Sie diese Informationen manuell eingeben (im Schritt 3c des Versteckens von Daten).

Welche Dateien können als nicht unterstützte Trägerdateien benutzt werden?

Um derartige Dateien zu finden, müssen Sie verstehen, wie Steganos Daten in Dateien versteckt. Verwenden Sie keine komprimierten Dateien oder Programmdateien.

Wie kann man Steganos für Windows 95 deinstallieren?

Um Steganos zu deinstallieren, klicken Sie im Startmenü auf *Einstellungen...Systemsteuerung*. Klicken Sie auf *Software* und wählen Sie *Steganos für Windows 95*. Dann klicken Sie auf *Hinzufügen/Entfernen*. Steganos für Windows 95 wird dann deinstalliert.

Verschlüsselung in Steganos (HWY1)

Wie verschlüsselt Steganos Dateien?

Steganos benutzt den HWY1-Verschlüsselungsalgorithmus, der einen Ausgabestream erzeugt, der kompatibel mit dem "Alleged RC4" ("RC4" ist ein eingetragener Handelsname von RSA Data Securities Inc.) ist, wie er von den Cypherpunks im Usenet veröffentlicht wurde. Die Implementation dieses Algorithmus in Steganos wurde vollständig durch die Beschreibung von Bruce Schneier ("Applied Cryptography", siehe [Ressourcen](#)) entwickelt.

Was kann man tun, wenn man sein Passwort vergißt?

Nichts! Einige Sicherheitsmechanismen können durch sog. Backdoors oder Master-Passwords übergangen werden. Nur ein Beispiel: Die meisten Versionen des *Award* BIOS ermöglichen die Eingabe eines Passwortes, um den Computer vor unbefugtem Zugriff zu schützen. Sie können diesen Mechanismus jedoch durch das Benutzen des Master-Passwortes *lkwpeter* und *AWARD_SW* (Groß-Klein-Schreibung beachten) umgehen. Damit ist es völlig irrelevant, welches Passwort Sie benutzen, um Ihren PC zu "schützen". **Steganos hat keine Backdoors oder Master-Passworte.** Selbst Deus Ex Machina kann Ihre Daten ohne das korrekte Passwort nicht entschlüsseln.

Wir können Ihnen nicht helfen, wenn Sie Ihr Passwort vergessen!

Wie Steganos Daten versteckt

Steganos wendet zwei völlig verschiedene Methoden zum verstecken von Daten an:

Verstecken von Daten in Bild- und Tondateien

Steganos benutzt das letzte signifikante Bit eines Datenelementes, um Daten darin zu verstecken. Ein Element sind 8 Bit (1 Byte) in einer 8-Bit-Datei und 16 Bit (2 Byte) in einer 16-Bit-Datei. Beispielsweise benutzt Steganos das niederwertigste Bit aller Bytes in einer 8-Bit-Wav-Klangdatei um Daten in ihr zu verstecken. Da diese Veränderungen vom menschlichen Ohr nicht hörbar sind (wegen Grundrauschens etc.) sind diese Daten tatsächlich *versteckt*. Bei Bildern werden die Farben so geringfügig verändert, daß man die Veränderung nicht sehen kann.

Steganos versteckt keine Daten im Header einer Trägerdatei.

Verstecken von Daten in Textdateien

Um Daten in Textdateien zu verstecken, hängt Steganos Frei- und Tabulatorzeichen an die Zeilenenden an. Steganos versteckt so ein Byte pro Textzeile (die 8 Bit werden durch die Kombination von acht Freizeichen und Tabulatoren dargestellt). Im Unterschied zum Verstecken von Daten in Bildern oder Klängen, kann diese Methode sehr leicht entdeckt werden. Somit ist diese Methode den anderen unterlegen und Sie sollten sie nicht benutzen, wenn Sie die Wahl haben.

Weitere Informationen

Trägerdateien

Warum Steganographie und Kryptographie kombinieren?

Wenn Sie nur Kryptographie benutzen, sind Ihre Daten (hoffentlich) nicht mehr von Unbefugten lesbar, doch es ist offensichtlich, daß Sie ein *Geheimnis* haben.

Wenn Sie nur Steganographie benutzen, wären Ihre Daten versteckt, doch durch simples ausprobieren aller verdächtigen Trägerdateien könnte ein Angreifer (die Person, die versucht, an Ihre Daten zu gelangen) geheime Daten wiederherstellen.

Steganos kombiniert diese beiden mächtigen Technologien. Daten, die mit Steganos versteckt und verschlüsselt worden sind, können weder leicht gefunden, noch ohne weiteres entschlüsselt werden.

Weitere Informationen

[Steganographie](#)

[Kryptographie](#)

Dateien vernichten

Warum Dateien vernichten?

Bei den meisten Betriebssystemen bewirkt das Löschen von Dateien nicht tatsächlich das Entfernen oder Überschreiben von Daten. Oftmals ist nur der erste Buchstabe des Dateinamens mit einem E5h-Zeichen überschrieben - das bedeutet für das Betriebssystem, daß es diese Datei überschreiben kann, wenn der Platz benötigt wird - nicht vorher.

So „löschen“ MS-DOS und Windows 3.1. Unter Windows 95 ist die Sicherheitslücke noch viel größer: Wenn Sie eine Datei mit dem Explorer löschen, wird die Datei lediglich in ein verstecktes Verzeichnis namens „Recycled“ verschoben, besser bekannt als „Papierkorb“. Selbst wenn Sie den Papierkorb leeren, werden die Dateien nicht wirklich gelöscht. Selbst dann können sie noch von diversen Programmen wiederhergestellt werden.

Wie vernichtet Steganos Dateien?

Steganos und der Steganos Shredder überschreiben die Datei drei mal mit pseudo-zufälligen Daten. (Da keine Software wirklich zufällige Daten erzeugen kann, nennt man diese Daten *pseudo-zufällig*.)

Wenn sensible Informationen mit pseudo-zufälligen Daten überschrieben werden, können Laufwerkskomprimierer (wie *DriveSpace* oder *Stacker*) nicht verhindern, daß Ihre Daten wirklich überschrieben werden.

Da sich hinter einer Datei immer noch unbenutzer Speicherplatz („slack“) befindet, der möglicherweise noch geheime Daten enthalten könnte, vernichtet Steganos auch diesen Bereich.

HINWEIS: Da moderne Betriebssysteme (wie Windows 95) Daten auf die Festplatte auslagern, kann das Risiko, daß geheime Daten irgendwo auf der Platte zurückbleiben, nicht vollständig ausgelöscht werden. Bitte vergessen Sie nicht, daß es nicht möglich ist, Daten vollständig von magnetischen Datenträgern zu entfernen. Electron-Tunneling-Mikroskope können sogar Daten, die mehrmals überschrieben wurden, wiederherstellen. Wenn Sie also **wirklich** ein Geheimnis bewahren müssen, könnte es billiger sein, das magnetische Medium nach dem Vernichten von Daten physikalisch zu vernichten, als das Geheimnis an jemanden zu verlieren.

Steganos und der *Steganos Shredder* benutzen dieselbe Funktion zum Vernichten von Dateien. Wählen Sie *Steganos Shredder* in der *Steganos für Windows 95* Programmgruppe oder im entsprechenden Verzeichnis im Startmenü für weitere Informationen zur Anwendung des Steganos Shredders.

Resourcen

Wenn Sie mehr über Steganographie und Kryptographie oder Sicherheitsaspekte im allgemeinen erfahren wollen, sehen Sie sich diese Resourcen an:

sci.crypt

Eine Usenet-Newsgroup zum Thema Kryptographie; enthält viel Nonsense.

National Computer Security Association forum

Ein CompuServe Forum; Das GO-Wort lautet *NCSA*

Steganography Info & Archive

Software, Informationen und Links zum Thema Steganographie
(<http://www.iquest.net/~mrmil/stego.html>)

The Infinite Void

Einiges zum Thema Hacken; zusammengetragen von *Silicon Toad*
(<http://www.vcalpha.com/silicon/episteme.html>)

Snake Oil Warning Signs: Encryption Software to Avoid

Wie man schlechte Kryptographiesoftware erkennt...
(<http://www.research.megasoft.com/people/cmcurtin/snake-oil-faq.html>)

Applied Cryptography

das beste Buch zum Thema Kryptographie - nicht Steganographie; Bruce Schneier, erschienen bei Wiley, ISBN 0-471-11709-9

Electronic Frontier Foundation (EFF)

kämpft für die Bürgerrechte im Netz - und setzt sich gegen Kryptoregulierungen ein (<http://www EFF.org>)

Benutzen des Steganos Shredders

Der Steganos Shredder vernichtet Dateien. Wenn eine Datei durch den Steganos Shredder vernichtet wurde, kann sie nicht mehr durch Programme wie *undelete* oder *unerase* etc. wiederhergestellt werden. Sie können den Steganos Shredder nicht direkt aus der Programmgruppe benutzen. Um eine Datei zu vernichten, klicken Sie mit der rechten Maustaste auf diese Datei und wählen Sie *Senden an...Shredder*.

Einführung

Willkommen zum Steganos Software Development Kit (Steganos SDK). Das Steganos SDK enthält die Funktionen, die Sie benötigen, um Steganographie in Ihren eigenen Programmen zu implementieren.

Die Datei STE_SDK.ZIP ist in jedem Steganos-Paket enthalten, sie enthält das Steganos SDK mit folgenden Dateien:

STE_DLL.h	Headerdatei
STE_SDK.txt	Textdatei
Steganos.lib	Library Datei

Die Steganos Dynamic Link Library, steganos.dll, finden Sie im Steganos Verzeichnis.

Bevor Sie das Steganos SDK benutzen, lesen Sie bitte die [rechtlichen Informationen und Lizenzbestimmungen](#).

Rechtliche Informationen / Lizenzbestimmungen

Das Steganos SDK dürfen Sie kostenlos in Freeware oder Public Domain Anwendungen benutzen. Wenn Sie das Steganos SDK in einer Anwendung benutzen möchten, die nicht kostenlos ist (bzw. registriert werden muß - wenn es sich um Shareware handelt) wenden Sie sich an Deus Ex Machina Communications.

Auf jeden Fall sind Sie dazu verpflichtet, in Ihrer Anwendung zu erwähnen, daß Sie die Steganographiefunktionen des Steganos SDKs benutzen und daß das Copyright 1997 bei Deus Ex Machina Communications liegt.

Beachten Sie bitte, daß Abschnitt I und III des Haftungsausschlusses sich auch auf das Steganos SDK beziehen.

Implementation der Steganographiefunktionen

Verstecken von Daten

Zuerst rufen Sie **IdentifyCarrierFile** auf, um Informationen zur angegebenen Trägerdatei zu erhalten. Überspringen Sie den Header der Trägerdatei mit dem Dateizeiger.

Sie sollten nun die Datendateigröße und andere zusätzliche Informationen über die zu versteckende Datei (wie etwa den Namen der Datei) in der Trägerdatei verstecken, bevor Sie die Datendatei selbst verstecken. Benutzen Sie **HideInBuffer**, um diese Informationen in der Trägerdatei zu verstecken.

Nun lassen Sie eine Schleife durchlaufen, in der Daten aus der Datendatei und aus der Trägerdatei gelesen werden. Verstecken Sie die Daten in den Datendateipuffer in dem Trägerdateipuffer mit **HideInBuffer**. Sie sollten die Daten vor dem Verstecken verschlüsseln und komprimieren. Schreiben Sie den manipulierten Trägerdateipuffer zurück in die Trägerdatei. Die Schleife endet mit dem Ende der Datendatei.

Wiederherstellen von Daten

Wieder rufen Sie als erstes **IdentifyCarrierFile**, um Informationen über die Trägerdatei zu gewinnen, und auf welche Weise Daten wiederhergestellt werden sollen. Überspringen Sie den Header der Trägerdatei. Lesen Sie dann die Informationen wie Datendateigröße und -namen über die Datendatei, die Sie beim Verstecken dort untergebracht haben, durch einen Aufruf von **HnhideFromBuffer** aus.

Dann folgt eine Schleife, in der Daten aus der Trägerdatei gelesen werden, durch **HnhideFromBuffer** wiederhergestellt und in eine neue Datei geschrieben werden. Die Schleife endet, wenn die wiederhergestellten Daten die Größe der ursprünglichen Datei erreicht haben.

IdentifyCarrierFile

int IdentifyCarrierFile(char* fname, tCarrierType* CT);

Rückgabewerte

Es wird IDENTIFY_OK geliefert, wenn die Trägerdatei erfolgreich identifiziert wurde; IDENTIFY_UNIDENTIFIED wenn die Datei nicht als eine gültige WAV, VOC, BMP, DIB oder ASCII-Textdatei identifiziert werden konnte. Es kann jedoch trotzdem möglich sein, Daten in dieser nicht unterstützten Trägerdatei zu verstecken; wenn ein Fehler auftrat, wird einer der folgenden Rückgabewerte geliefert:

IDENTIFY_VOC_NOT_VALID wenn die Dateierdung .voc ist, der Dateiheder aber nicht gültig ist.

IDENTIFY_WAV_NOT_VALID wenn die Dateierdung .wav ist, der Dateiheder aber nicht gültig ist.

IDENTIFY_BMP_OR_DIB_NOT_VALID wenn die Dateierdung .bmp oder .dib ist, der Dateiheder aber nicht gültig ist.

IDENTIFY_BMP_OR_DIB_TOO_FEW_COLORS wenn die Dateierdung .bmp oder .dib ist, die Farbtiefe jedoch nur 4 Bit beträgt. Diese Dateien werden nicht vom Steganos SDK unterstützt. Das Programm sollte diese Bilder in eine höhere Farbtiefe konvertieren.

IDENTIFY_BMP_OR_DIB_NOT_RGB_ENCODED wenn die Dateierdung .bmp oder .dib ist, die Daten jedoch im RLE (run-length-encoded) Format vorliegen. Momentan unterstützt das Steganos SDK keine RLE Bilder.

IDENTIFY_CARRIER_FILE_OPEN_ERR wenn die Datei nicht geöffnet werden konnte.

IDENTIFY_BMP_OR_DIB_ONLY_256_COLORS wenn die Dateierdung .bmp oder .dib ist, das Bild jedoch nur von 8 Bit Farbtiefe ist (256 Farben). Das ist kein wirklicher Fehler. Dieser Rückgabewert sollte als Warnung betrachtet werden. Der Endbenutzer sollte ebenfalls gewarnt werden, da Daten, die in einem derartigen Bild versteckt wurden, unter Umständen leicht vom menschlichen Auge entdeckt werden können.

IDENTIFY_TXT_LINE_TOO_LONG wenn die Datei als Textdatei identifiziert wurde, aber mindestens eine Zeile enthält, die zu lang ist, um vom Steganos SDK benutzt werden zu können (eine Zeile sollte nicht länger als 230 Zeichen lang sein).

IDENTIFY_BMP_OR_DIB_NOT_SUPPORTED wenn die Dateierdung .bmp oder .dib ist, die Datei aber weniger als 4 Bit Farbtiefe hat (weniger als 16 Farben). Diese Dateien sind vom Steganos SDK nicht unterstützt. Das Programm sollte diese Bilder in eine höhere Farbtiefe konvertieren.

Parameter

fname

Zeiger auf einen String, der Pfad und Dateinamen der zu identifizierenden Datei enthält.

CT

Zeiger auf eine tCarrierType Struktur, die die Informationen über die identifizierte Trägerdatei enthalten soll.

Hinweise

Öffnet *fname* und versucht diese Datei zu identifizieren. Wenn *fname* eine ASCII-Textdatei ist, kann dieser Vorgang etwas dauern, da IdentifyCarrierFile die Zeilen der Textdatei zählt.

Weitere Informationen

tCarrierType

HideInBuffer

int HideInBuffer(char* bufCarrier, long sizeBufCarrier, int CarrierType, char* bufDataToHide, long sizeBufDataToHide);

Rückgabewerte

HIDE_OK wenn Daten erfolgreich versteckt werden konnten; einer der folgenden, wenn ein Fehler auftrat:

HIDE_ASCII_BUFSIZE_NOT_1 wenn CarrierType eine ASCII-Textdatei identifiziert und die Pufferlänge nicht 1 beträgt. sizeBufData muß beim verstecken in ASCII-Textdateien 1 sein, da das Steganos SDK pro Aufruf von HideInBuffer immer nur ein Byte in einer Textdatei versteckt.

HIDE_BUF CARRIER_TOO_SMALL wenn sizeBufCarrier < (sizeBufDataToHide * CarrierType).

Parameter

bufCarrier

Beim Verstecken in nicht-Textdateien, zeigt bufCarrier auf einen Puffer, der die Trägerdaten aus der Trägerdatei enthält, in den die Daten versteckt werden sollen (er sollte CarrierType*sizeBufDataToHide lang sein). Andernfalls zeigt es auf den ASCII-Z String, an den die versteckten Daten angehängt werden sollen.

sizeBufCarrier

ist die Länge in Byte von bufCarrier. Beim verstecken in ASCII-Dateien spezifiziert es die Länge des Strings auf den bufCarrier zeigt.

CarrierType

Spezifiziert die Bittiefe der Trägerdatei. Beim verstecken in ASCII-Dateien, muß CARRIERTYPE_ASCII übergeben werden. Sie können einfach den FileType Member der tCarrierType Struktur übergeben.

bufDataToHide

Zeigt auf einen Puffer, der die zu versteckenden Daten enthält. Dieser Puffer kann verschlüsselte und/oder komprimierte Daten enthalten.

sizeBufDataToHide

Spezifiziert die Länge von bufDataToHide. Wenn sizeBufCarrier < (sizeBufDataToHide * CarrierType) wird HideInBuffer einen Fehler zurückliefern.

Hinweise

Versteckt Daten durch Manipulation des niederwertigsten signifikanten Bits der Trägerdaten. Beim Verstecken in ASCII-Textdateien fügt diese Funktion 8 Tabulatorzeichen oder Freizeichen an einen String an.

Weitere Informationen

Implementation der Steganographiefunktionen, tCarrierType, UnhideFromBuffer

UnhideFromBuffer

int UnhideFromBuffer(char* bufCarrier, long sizeBufCarrier, int CarrierType, char* bufUnhiddenData, long sizeBufUnhiddenData);

Rückgabewerte

UNHIDE_OK wenn Daten erfolgreich wiederhergestellt werden konnten; einer der Folgenden, wenn ein Fehler auftrat:

UNHIDE_ASCII_BUFSIZE_NOT_1 wenn CarrierType eine ASCII-Textdatei spezifiziert und sizeBufUnhiddenData ungleich 1 ist. sizeBufUnhiddenData muß 1 sein, wenn Daten aus einer ASCII-Textdatei wiederhergestellt werden, da das Steganos SDK immer nur ein Byte bei jedem Aufruf von UnhideFromBuffer aus einer ASCII-Textdatei wiederherstellen kann..

UNHIDE_BUFUNHIDDENDATA_TOO_SMALL wenn $(\text{sizeBufUnhiddenData} * \text{CarrierType}) > \text{sizeBufCarrier}$ ist.

Parameter

bufCarrier

Beim Wiederherstellen aus einer nicht-Textdatei zeigt bufCarrier auf einen Puffer der die Trägerdaten enthält aus denen Daten wiederhergestellt werden sollen. Andernfalls zeigt bufCarrier auf einen ASCII-Z String, der versteckte Daten enthält.

sizeBufCarrier

ist die Länge von bufCarrier in Byte. Beim Wiederherstellen von Daten aus ASCII-Textdateien spezifiziert sizeBufCarrier die Länge des ASCII-Z Strings, der die versteckten Daten enthält.

CarrierType

Spezifiziert die Bittiefe der Trägerdaten. Beim Wiederherstellen aus ASCII-Textdateien muß dieser Parameter CARRIERTYPE_ASCII sein. Sie können hier einfach den FileType Member der [tCarrierType](#) Struktur übergeben.

bufUnhiddenData

Zeigt auf einen Puffer, der die wiederhergestellten Daten aufnehmen soll.

sizeBufUnhiddenData

Spezifiziert die Länge von bufUnhiddenData in Byte. Wenn $(\text{sizeBufUnhiddenData} * \text{CarrierType}) > \text{sizeBufCarrier}$ ist, liefert HideInBuffer einen Fehler.

Hinweise

Stellt Daten aus einem Puffer mit versteckten Daten wieder her.

Weitere Informationen

[Implementation der Steganographiefunktionen](#), [tCarrierType](#), [HideInBuffer](#)

IsCRLFFile

BOOL IsCRLFFile(const char* clpstrFilename);

Rückgabewerte

TRUE wenn die Datei eine ASCII-Textdatei ist; andernfalls FALSE.

Parameter

clpstrFilename

Zeiger auf einen ASCII-Z String, der Pfad und Dateiname der zu identifizierenden Datei enthält.

Hinweise

Prüft, ob die übergebene Datei eine ASCII-Textdatei ist, oder nicht. Diese Funktion wird von IdentifyCarrierFile benutzt und kann benutzt werden, um zu ermitteln, ob ein Aufruf von **IdentifyCarrierFile** länger dauern könnte.

Weitere Informationen

IdentifyCarrierFile

tCarrierType Struktur

Die tCarrierType struktur wird von [IdentifyCarrierFile](#) benutzt und enthält Informationen über die Trägerdatei.

```
struct tCarrierType { // CT
    char FileType;
    char FileFormatName;
    long FileSize;
    long LongestLine;
    int HeaderSize;
};
```

Member

FileType

Spezifiziert die Bittiefe der Trägerdatei; nicht benutzt bei ASCII-Textdateien

FileFormatName

CARRIERTYPE_VOC wenn die Trägerdatei eine VOC Datei ist.

CARRIERTYPE_WAV wenn die Trägerdatei eine WAV Datei ist.

CARRIERTYPE_BMP_OR_DIB wenn die Trägerdatei eine BMP oder DIB Datei ist.

CARRIERTYPE_TXT wenn die Trägerdatei eine ASCII-Textdatei ist.

CARRIERTYPE_UNIDENTIFIED wenn die Trägersdatei nicht identifiziert werden konnte.

FileSize

Gibt die Länge der Trägerdatei in Byte an. Wenn die Trägerdatei eine ASCII-Textdatei ist, gibt es die Anzahl der Zeilen an.

LongestLine

Wenn die Trägerdatei eine ASCII-Textdatei ist, gibt dieser Member die Anzahl der Zeichen in der längsten Zeile an; wenn die Datei keine ASCII-Textdatei ist, ist dieser Member nicht gesetzt,

HeaderSize

Gibt die Länge des Dateiheaders in Byte an; wenn die Datei eine ASCII-Textdatei ist, ist dieser Member 0.

Wietere Informationen

[IdentifyCarrierFile](#)

SEF-Datei

Was ist eine SEF-Datei?

SEF steht im englischen für *Steganos Encrypted File*. Wenn Sie im ersten Schritt des Versteckens/Verschlüsseln von Dateien *Verschlüsseln* wählen und *Verstecken* abschalten erstellt Steganos eine Steganos-verschlüsselte-Datei (SEF-Datei), die die verschlüsselte Datendatei enthält.

Über das SEF Dateiformat

Steganos-verschlüsselte Dateien sind nicht nur verschlüsselt, sondern auch komprimiert. Erfahren Sie, wie Steganos Daten verschlüsselt.

Wie Sie eine SEF-Datei entschlüsseln können

Sie können Steganos manuell starten und in der Startseite *Daten wiederherstellen und/oder entschlüsseln* wählen, oder Sie klicken doppelt auf das Icon der SEF-Datei.

Trägerdatei

Was ist eine Trägerdatei?

Die Trägerdatei ist die Datei, in der die Datendatei versteckt wird.

Welche Trägerdateien unterstützt Steganos?

Die vorliegende Version von Steganos für Windows 95 unterstützt die folgenden Trägerdateien:

- **Bilddateien (BMP, DIB)**, unkomprimierte (also das RGB-Format, nicht das RLE-Format). Die Bilder können zwischen 16 Farben (4-Bit-Format) und 16,7 Mio. Farben (24-Bit-Format) sein. Wir empfehlen 16,7 Mio.-Farben-Bilder. Wenn Sie ein 16-Farben-Bild oder ein 256-Farben-Bild auswählen, wird Steganos Sie fragen, ob Sie es auf 16,7 Mio. Farben hochkonvertieren lassen wollen. Dies ist zu empfehlen, da es weniger verdächtig ist, Daten in 16,7 Mio-Farben-Bildern zu verstecken.
- **Klangdateien (WAV, VOC)**, und jegliche Unterformate. Klangdateien sind ideal um darin Daten zu verstecken, da Sie leicht sehr große Dateien erstellen können.
- **Textdateien**. Obwohl Steganos das Verstecken von Daten in Textdateien (die nicht einfach nur Textdateien sein müssen, auch HTML-Dokumente oder Stapelverarbeitungsdateien wären geeignet) beherrscht, ist diese Methode nicht zu empfehlen, da sie leicht entdeckt werden kann. Textdateien im Unix- oder Amigaformat werden nicht unterstützt (da sie kein Carriage-Return/Linefeed am Zeilenende haben)
- **Benutzerdefinierte Trägerdateien** (lesen Sie hierzu den Artikel über nicht unterstützte Trägerdateien)

Weitere Informationen

Was ist eine gute Trägerdatei?

Wie Steganos Daten versteckt

Konvertieren von Bildern mit versteckten Daten

Datendatei

Was ist eine Datendatei?

Die *Datendatei* ist die Datei, die in einer Trägerdatei versteckt oder als SEF-Datei verschlüsselt wird. Jede Datei kann eine Datendatei sein. Wenn Sie mehrere Dateien in einer Trägerdatei/SEF-Datei verstecken und/oder verschlüsseln wollen, müssen Sie eine Kompressionssoftware benutzen, um mehrere Dateien zu einer zusammenzufassen.

Nicht unterstützte Trägerdateien

Was ist eine nicht unterstützte Trägerdatei?

Steganos ist in der Lage, Daten in Dateien zu verstecken, die nicht direkt von Steganos unterstützt werden. Diese Methode ist nicht zu empfehlen, da dadurch die Trägerdatei unbrauchbar gemacht werden kann. Da Steganos weder die Länge des Dateiheaders noch die Bittiefe der nicht unterstützten Datei kennt, müssen Sie diese Informationen manuell eingeben (im Schritt 3c des Versteckens von Daten).

Welche Dateien können als nicht unterstützte Trägerdateien benutzt werden?

Um derartige Dateien zu finden, müssen Sie verstehen wie Steganos Daten versteckt. Verwenden Sie keine komprimierten, verschlüsselten oder Programmdateien.

Dateiheader

Die meisten Dateien beginnen mit einem sog. Dateiheader. Dieser Header enthält für gewöhnlich Informationen, die nötig sind, um die gesamte Datei zu bearbeiten. Zum Beispiel enthält der Header einer Bilddatei Informationen über die Farbtiefe, Auflösung etc. Da dieser Teil der Datei meist exakt beschrieben ist, und selbst kleinste Änderungen die Datei unbrauchbar machen können, versteckt Steganos keine Daten im Dateiheader. Einfache ASCII-Textdateien haben normalerweise keinen Header.

Weitere Informationen

[Wie Steganos Daten versteckt](#)

Steganographie

Steganographie ist die Kunst oder Wissenschaft eine Nachricht in einer anderen zu verstecken. So ist z.B. Unsichtbare Tinte auch eine Art der Steganographie.

Weitere Informationen

Wie Steganos Daten versteckt

Warum Steganographie und Kryptographie kombinieren?

Resourcen

Kryptographie

Kryptographie wird verwendet, um Nachrichten (oder eine Datei) für alle unleserlich zu machen, die das Passwort nicht kennen. Kryptographie ist die Kunst oder Wissenschaft Nachrichten geheim zu halten - nicht jedoch ihre Existenz.

Weitere Informationen
[Ressourcen](#)

Kompressionssoftware / Archive

Kompressionsprogramme (auch Packer genannt) werden benutzt, um mehrere Dateien in einer Datei abzulegen und dabei ihre Größe zu verringern. Um Onlinezeit zu sparen sind die meisten Programme aus dem Internet komprimiert. Sie müssen dekomprimiert („ausgepackt“) werden, bevor Sie installiert oder benutzt werden können. *WinZip*, *PkZip für Windows* und *WinRAR* sind Beispiele für Kompressionsprogramme die unter Windows laufen. Archive, die mit ihnen erzeugt wurden, heißen *gepackte* oder *gezippte* Dateien.

Startseite: Verstecken/Verschlüsseln oder Wiederherstellen von Daten

Auf der ersten Seite des Steganos Assistenten müssen Sie entscheiden, was getan werden soll:

Wählen Sie *Daten verstecken und/oder verschlüsseln* um folgendes zu tun:

- Verschlüsseln und Verstecken einer Datei in einer anderen
- Verstecken einer Datei ohne Verschlüsselung
- Verschlüsseln einer Datei (in das SEF Datei-Format)

Wählen Sie *Daten wiederherstellen und/oder entschlüsseln* um folgendes zu tun:

- Wiederherstellen von Daten
- Entschlüsseln einer SEF Datei

Die folgenden Schritte richten sich nach Ihrer Entscheidung. Klicken Sie auf *Weiter* um fortzufahren.

Klicken Sie auf *Info & UpdateNOW!* um Programm- und Copyrightinformationen darzustellen. Sie werden auch gefragt werden, ob Sie UpdateNOW! benutzen wollen - so können Sie Steganos für Windows 95 leicht durch das Internet auf die neueste Version updaten.

Schritt 1: Auswahl der Datendatei

Datendatei

Wählen Sie die Datendatei, die Sie verstecken und/oder verschlüsseln wollen.
Klicken Sie auf *Durchsuchen*, wenn Sie ein Dateiauswahlfenster benötigen.

Datei verstecken

Wählen Sie *Datei verstecken*, um die Datei in einer anderen Datei zu verstecken; z.B. in einer Klangdatei (.WAV). Später werden Sie eine Trägerdatei auswählen, in die Sie die Datendatei verstecken wollen.

Datei verschlüsseln

Wählen Sie *Datei verschlüsseln*, wenn Sie die Datei verschlüsseln wollen. Wenn diese Option ausgewählt ist, wird Sie Steganos später nach einem Passwort fragen. Sie werden dieses Passwort benötigen, wenn Sie die Daten wiederherstellen möchten. Lesen hierzu den Artikel über die in Steganos benutzte Verschlüsselung.

HINWEIS: Sie können beide Optionen anwählen oder nur eine von beiden. Wenn Sie *Datei verschlüsseln* anwählen und *Datei verstecken* abwählen, wird Steganos eine Steganos verschlüsselte Datei (SEF) erstellen. Wenn Sie eine Datei verstecken wollen ist es dringend zu empfehlen, *Datei verschlüsseln* ebenfalls anzuwählen. Lesen Sie hierzu, warum man Steganographie und Kryptographie kombinieren sollte.

Datendatei unwiderruflich löschen

Wählen Sie *Datendatei unwiderruflich löschen* wenn Sie die Datei, die Sie verschlüsseln und/oder verstecken wollen danach unwiderruflich zerstören lassen wollen.

Schritt 2: Eingabe eines Passwortes

Geben Sie ein Passwort ein

Da Sie in der vorherigen Seite *Datei verschlüsseln* angewählt haben, müssen Sie nun ein Passwort eingeben. Da das Passwort auf dem Bildschirm nicht dargestellt wird, müssen Sie es ein zweites mal eingeben um sicherzugehen, daß Sie es korrekt geschrieben haben. Die in Steganos benutzten Passwörter unterscheiden Groß- und Kleinbuchstaben. Sie sind also case - sensitive.

HINWEIS: Sie werden dieses Passwort zum entschlüsseln der verschlüsselten Daten benötigen. Da die in Steganos benutzte Verschlüsselung sehr sicher ist, gibt es praktisch keine Möglichkeit, ohne das Passwort die Daten wiederherzustellen. Wählen Sie kein Passwort, das man leicht herausfinden könnte. Wenn Sie nicht sicher sind, lesen Sie hierzu, wie man ein sicheres Passwort wählt.

Schritt 3a: Auswahl einer Trägerdatei

Trägerdatei

Wählen Sie eine Trägerdatei, in der Sie Daten verstecken wollen. Klicken Sie auf *Durchsuchen* wenn Sie einen Dateiauswahldialog benötigen.

Zeitstempel der Trägerdatei nicht ändern

Wählen Sie diese Option wenn Steganos die Dateizeit und das Dateidatum der Trägerdatei nicht ändern soll. Das ist wichtig, da die Veränderung des Zeitstempels eine offensichtliche Modifikation ist und eventuell einen Verdacht auf diese Datei lenken kann.

HINWEIS: Wenn Sie ein Backupsystem benutzen, daß anhand des Zeitstempels entscheidet, ob eine Datei (wieder) gesichert werden soll, kann das Benutzen dieser Option das Sichern dieser Datei verhindern.

Sicherheitskopie von Trägerdatei anlegen

Wenn diese Option angewählt ist, wird Steganos eine Kopie der Trägerdatei machen bevor Daten in ihr versteckt werden. Das Backup der Datei "bild.bmp" wird als "Kopie von bild.bmp" im selben Verzeichnis erstellt.

HINWEIS: Diese Option ist besonders dann nützlich, wenn Sie Daten in einer nicht unterstützten Trägerdatei verstecken wollen. Seien Sie jedoch vorsichtig mit dieser Option: Wenn jemand die Trägerdatei und ihre Kopie findet, kann er durch Dateivergleich nachweisen, daß die Datei verändert wurde. Wenn Sie *Datei verschlüsseln* angewählt haben, sind die Daten natürlich für alle, die das Passwort nicht kennen, auch nicht zugänglich.

HINWEIS: Wenn Sie die Meldung "Trägerdatei zu klein" erhalten und eine ASCII-Textdatei als Trägerdatei ausgewählt haben, die jedoch lang genug erscheint (genug Zeilen hat), prüfen Sie bitte nach, ob die Textdatei Zeilen enthält, die länger als 230 Zeilen sind, da Steganos nur ASCII-Textdateien unterstützt deren Zeilen nicht länger als 230 Zeichen lang sind.

Schritt 3b: Benennung der SEF-Datei

Steganos-verschlüsselte Datei

Wählen Sie einen Namen für die Steganos-verschlüsselte Datei. Dies ist die Datei, die die verschlüsselte Datendatei enthalten wird. Klicken Sie auf Durchsuchen, wenn Sie einen *Dateiauswahldialog* benötigen.

Schritt 3c: Informationen über nicht unterstützte Trägerdateien

Die Trägerdatei, die Sie angewählt haben, wird von Steganos nicht direkt unterstützt. Steganos kann trotzdem versuchen, Daten in dieser Datei von unbekanntem Format zu verstecken. Diese Methode ist nicht zu empfehlen, da die Datei dadurch leicht unbrauchbar gemacht werden kann. Lesen Sie hierzu den Artikel über nicht unterstützte Trägerdateien. Benutzen Sie keine komprimierten oder verschlüsselten Dateien.

Was ist die Bittiefe der Trägerdatei?

Sie können 8, 16, 24, oder 32 Bit wählen - je nach Format der Trägerdatei, die Sie gewählt haben. Diese Information kann von Steganos nicht selbst ermittelt werden.

Wie groß ist der Dateiheader?

Da die Trägerdatei leicht durch das Überschreiben des Dateiheaders zerstört werden kann, müssen Sie die Größe des Dateiheaders (in Byte) angeben. Steganos wird in diesen Bytes keine Daten verstecken. Manche Dateien haben keinen Header; Geben Sie in diesem Fall einfach 0 an.

HINWEIS: Wenn Sie die exakte Größe des Dateiheaders nicht kennen, seien Sie großzügig. Wenn Sie einen zu kleinen Wert angeben, machen Sie die Datei damit höchstwahrscheinlich unbrauchbar. Wenn Sie einen zu großen Wert angeben ist das zwar nicht sehr effizient, doch es werden dadurch keinen Daten zerstört.

HINWEIS: Steganos erkennt ASCII-Textdateien automatisch. Wenn Sie sicher sind, eine ASCII-Textdatei als Trägerdatei ausgewählt zu haben, und diese Seite des Steganos Assistenten angezeigt wird, ist die Datei womöglich im Unix oder Amiga Format (kein Carriage-Return/Linefeed am Zeilenende). Steganos kann keine Daten in diesen Dateien verstecken.

Schritt 4: Zusammenfassung

Diese Seite faßt zusammen, was passieren wird, wenn Sie auf *Weiter* klicken. Sie sollten die Informationen jedesmal aufmerksam lesen. Sie werden mindestens folgende Informationen bekommen:

- Name der Datendatei
- Name der Trägerdatei und Informationen über ihren Typ (beim Verstecken) oder den Namen der SEF-Datei (beim Verschlüsseln ohne zu Verstecken)
- Kompressionsrate (Steganos komprimiert die Daten, bevor sie versteckt und/oder verschlüsselt werden)

Wenn Sie auf *Weiter* klicken wird Steganos mit dem Verstecken/Verschlüsseln, Komprimieren, Erstellen einer Sicherheitskopie und Vernichten der Daten beginnen, je nach den Optionen, die Sie gewählt haben. Wenn Sie eine der Optionen ändern wollen klicken Sie auf *Zurück*.

Endseite: Explorer starten, Trägerdatei ansehen, E-Mail verschicken

Dies ist die Endseite des Steganos Assistenten. Sie können eine der folgenden Optionen auswählen oder Steganos sofort *schließen*.

Explorer im Zielverzeichnis

Startet den Windows-Explorer im Verzeichnis der Trägerdatei.

Trägerdatei überprüfen

Wenn Sie Option wählen, versucht Steganos die passende Anwendung mit der Trägerdatei zu starten (z.B. die Medienwiedergabe für .wav Dateien). So können Sie überprüfen, ob die modifizierte Trägerdatei wirklich keine signifikanten Veränderungen aufweist. Diese Option ist nicht anwählbar, wenn Sie nur Datei verschlüsseln gewählt haben, da es keinen Sinn macht, eine SEF Datei anzusehen.

Trägerdatei/SEF-Datei verschicken

Wählen Sie diese Option, wenn Sie die Trägerdatei bzw. die verschlüsselte Datei direkt jemandem per E-Mail zusenden wollen. (Die Datei wird an eine E-Mail angehängt, die Sie dann schreiben können).

Schritt 1: Auswählen einer Trägerdatei oder einer SEF-Datei

Trägerdatei oder Steganos-verschlüsselte Datei

Sie können entweder eine Trägerdatei zum Wiederherstellen versteckter Daten oder eine Steganos-verschlüsselte Datei zum Entschlüsseln von Daten auswählen. Wenn Sie einen Dateiauswahldialog benötigen, klicken Sie auf *Durchsuchen*.

Soll die Trägerdatei unwiderruflich gelöscht werden, nachdem die Daten wiederhergestellt wurden?

Wählen Sie diese Option, wenn Steganos die Trägerdatei oder die Steganos-verschlüsselte Datei (SEF) unwiderruflich löschen soll, nachdem die Daten aus dieser Datei erfolgreich wiederhergestellt wurden.

Schritt 1b: Eingabe von Daten über nicht unterstützte Trägerdatei

Die Trägerdatei, die Sie angewählt haben, wird von Steganos nicht direkt unterstützt. Um es Steganos zu ermöglichen, Daten aus dieser Datei wiederherzustellen, müssen Sie ein paar Informationen über die Trägerdatei angeben. Lesen Sie hierzu den Artikel über nicht unterstützte Trägerdateien.

Was ist die Bittiefe der Trägerdatei?

Sie können 8, 16, 24, oder 32 Bit wählen - je nach Format der Trägerdatei, die Sie gewählt haben. Diese Information kann von Steganos nicht selbst ermittelt werden.

Wie groß ist der Dateiheader?

Da die Trägerdatei leicht durch das Überschreiben des Dateiheaders zerstört werden kann, müssen Sie die Größe des Dateiheaders (in Byte) angeben.

HINWEIS: Es ist unbedingt erforderlich, daß Sie die selben Werte eingeben, die beim Verstecken in diese nicht unterstützte Trägerdatei verwandt wurden.

Schritt 2: Passworteingabe

Passwort

Geben Sie das Passwort ein, das zum Verschlüsseln der Datei verwendet wurde. Bei Passwörtern in Steganos muß die Groß-Kleinschreibung beachtet werden. Wenn die Datei nicht verschlüsselt wurde, können Sie kein Passwort eingeben. Klicken Sie einfach auf *Weiter*.

Schritt 3: Benennung der wiederherzustellenden Datei

Wiederhergestellte Datei speichern als

Steganos schlägt den ursprünglichen Dateinamen der verschlüsselten oder versteckten Datei vor. Das aktuelle Verzeichnis wird dabei zum Wiederherstellen verwendet. Sie können das Verzeichnis und den Dateinamen verändern. Wenn Sie einen Dateiauswahldialog benutzen möchten, klicken Sie auf *Durchsuchen*.

Schritt 4: Zusammenfassung

Diese Seite faßt zusammen, was passieren wird, wenn Sie auf *Weiter* klicken. Sie sollten die Informationen jedes mal aufmerksam lesen. Sie werden mindestens folgende Informationen bekommen:

- Name der Trägerdatei und Informationen über ihren Typ (bei versteckten Daten) oder den Namen der SEF-Datei (beim entschlüsseln nicht versteckter Daten)
- Name der Datendatei, die wiederhergestellt wird

Wenn Sie auf *Weiter* klicken wird Steganos mit dem Wiederherstellen/Entschlüsseln, Dekomprimieren und Vernichten der Daten beginnen, je nach den Optionen, die Sie gewählt haben. Wenn Sie eine der Optionen ändern wollen klicken Sie auf *Zurück*.

Endseite: Explorer starten, Datendatei ansehen

Dies ist die Endseite des Steganos Assistenten. Sie können eine der folgenden Optionen wählen oder Steganos sofort *schließen*.

Explorer im Zielverzeichnis

Startet den Windows-Explorer im Zielverzeichnis.

Wiederhergestellte Datei ansehen

Wenn Sie auf diese Option klicken, versucht Steganos die passende Anwendung mit der Trägerdatei zu starten (z.B. die Medienwiedergabe für .wav Dateien). So können Sie die wiederhergestellte Datei sofort benutzen.

Verstecken/Verschlüsseln von Daten...

Während diese Seite gezeigt wird, ist Steganos mit dem Verstecken, Verschlüsseln, Komprimieren und Vernichten von Daten beschäftigt, je nachdem, welche Optionen Sie gewählt haben.

Warten Sie, bis Steganos fertig ist, und klicken Sie dann auf *Weiter* um zur letzten Seite des Assistenten zu gelangen.

Wiederherstellen von Daten...

Während diese Seite gezeigt wird, ist Steganos mit dem Wiederherstellen, Entschlüsseln, Dekomprimieren und Vernichten von Daten beschäftigt, je nachdem, welche Optionen Sie gewählt haben.

Warten Sie, bis Steganos fertig ist, und klicken Sie dann auf *Weiter* um zur letzten Seite des Assistenten zu gelangen.

Wie kann man Steganos durch UpdateNOW! aktualisieren?

UpdateNOW! ist eine von Deus Ex Machina Communications entwickelte Technologie, die es Ihnen ermöglicht, schnell und einfach an die neueste Steganos-Version zu kommen.

Wie funktioniert UpdateNOW!?

UpdateNOW! verbindet Ihren PC mit Deus Ex Machinas Internet Server und findet heraus, ob es eine neue Version von Steganos gibt. Sollte eine neue Shareware-Version verfügbar sein, werden Sie über die neuen Features und Fehlerbehebungen informiert, und gefragt, ob Sie die neue Shareware-Version downloaded möchten. Wenn Sie auf *Ja* klicken, wird eine zip-komprimierte Datei auf Ihren Desktop kopiert.

HINWEIS: Sie benötigen eine bereits konfigurierte DFÜ-Netzwerk Verbindung für dieses Feature. Bitte informieren Sie sich zu diesem Thema in der Windows Hilfe. Um eine zip-komprimierte Datei zu dekomprimieren, benötigen Sie PkZip für Windows, WinZIP oder eine andere Anwendung, die zip-Dateien dekomprimieren kann.

Was kostet UpdateNOW!?

UpdateNOW! ist kostenlos. Selbstverständlich können durch die Telefonverbindung und/oder durch Ihren Internetdienstanbieter (Provider) Gebühren für die Zeit anfallen, in der Sie online sind.

Konvertieren von Bildern, die versteckte Daten enthalten

Es ist möglich, Bilder, die versteckte Informationen enthalten, in andere Formate zu konvertieren (z.B. gif) und nachher zurück zu .bmp oder .dib. Selbst dann wird Steganos in der Lage sein, die versteckten Daten wiederherzustellen. Es ist sehr wichtig, daß Sie keine Kompressionsalgorithmen verwenden, die Informationen zerstören. Das JPEG Format benutzt z.B. den DCT (*Discrete Cosinus Transformation*) Algorithmus, der einzelne Teile des Bildes zerstört, indem er Informationen, die man mit dem Auge so nicht erkennen kann, einfach nicht speichert. Somit würden von Steganos gespeicherte Daten bei der Konvertierung verloren gehen.

HINWEIS: Sie sollten die Konvertierungssoftware vorher unbedingt ausprobieren, da verschiedene Konvertierungsalgorithmen Probleme hervorrufen können.

UpdateNOW!

UpdateNOW! ist eine von Deus Ex Machina Communications entwickelte Technologie, die es Ihnen ermöglicht, schnell und einfach an die neueste Steganos-Version zu kommen.

Wie funktioniert UpdateNOW!?

UpdateNOW! verbindet Ihren PC mit Deus Ex Machinas Internet Server und findet heraus, ob es eine neue Version von Steganos gibt. Sollte eine neue Shareware-Version verfügbar sein, werden Sie über die neuen Features und Fehlerbehebungen informiert, und gefragt, ob Sie die neue Shareware-Version downloaden möchten. Wenn Sie auf *Ja* klicken, wird eine zip-komprimierte Datei auf Ihren Desktop kopiert.

HINWEIS: Sie benötigen eine bereits konfigurierte DFÜ-Netzwerk Verbindung für dieses Feature. Bitte informieren Sie sich zu diesem Thema in der Windows Hilfe. Um eine zip-komprimierte Datei zu dekomprimieren, benötigen Sie PkZip für Windows, WinZIP oder eine andere Anwendung, die zip-Dateien dekomprimieren kann.

Was kostet UpdateNOW!?

UpdateNOW! ist kostenlos. Selbstverständlich können durch die Telefonverbindung und/oder durch Ihren Internetdienstanbieter (Provider) Gebühren für die Zeit anfallen, in der Sie online sind.

Credits

Steganos für Windows 95 wurde entwickelt von
Fabian Hansmann, Sascha Wildgrube und Gabriel Yoran
in Frankfurt, Deutschland.

Besonderer Dank an
Cynthia Ferebee, Siegfried Moersch und Marty Brownell, Frank Tiemann.

Musik, die uns half, die Arbeit zu tun

Apollo Four Fourty: Electro Glide In Blue, Dead Can Dance: Within The Realm Of A Dying Sun, George Michael: Older, Hackers OST, Mark Snow: The Truth And The Light - Music From The X-Files, Dune & The London Session Orchestra: Forever, Stephane Grappelli: Jazz Masters 11, Gustav Holst: The Planets, Rachmaninov: Klavierkonzert No. 2 in C moll, Op. 18, Ravel: La Valse, George Gershwin: Rhapsody in Blue, Judas Priest: Killing Machine, Christopher Franke: Babylon 5 OST, Prodigy: Music For The Jilted Generation/Fire Starter/Breathe, Faithless: Reverence, Underworld: dubnobasswithmyheadman, Trainspotting OST, and techno mixed by various local DJs from Frankfurt (farewell DJ dag).

