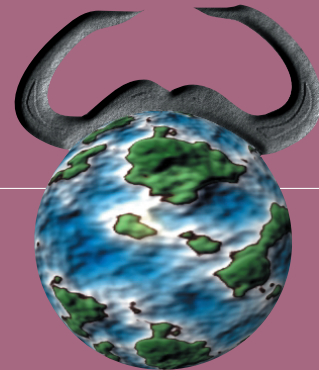


Die monatliche GNU-Kolumne

# Brave GNU World



Diese Kolumne berichtet aus der Perspektive des GNU-Projekts und der FSF über Projekte und aktuelle Geschehnisse aus dem Umfeld freier Software. In dieser Ausgabe: Das E-Mail-Programm Balsa, Spam: Kur gelungen - Patient tot, sicher chatten mit Silky, Agnula und die Agnula Trademark License. Georg C.F. Greve

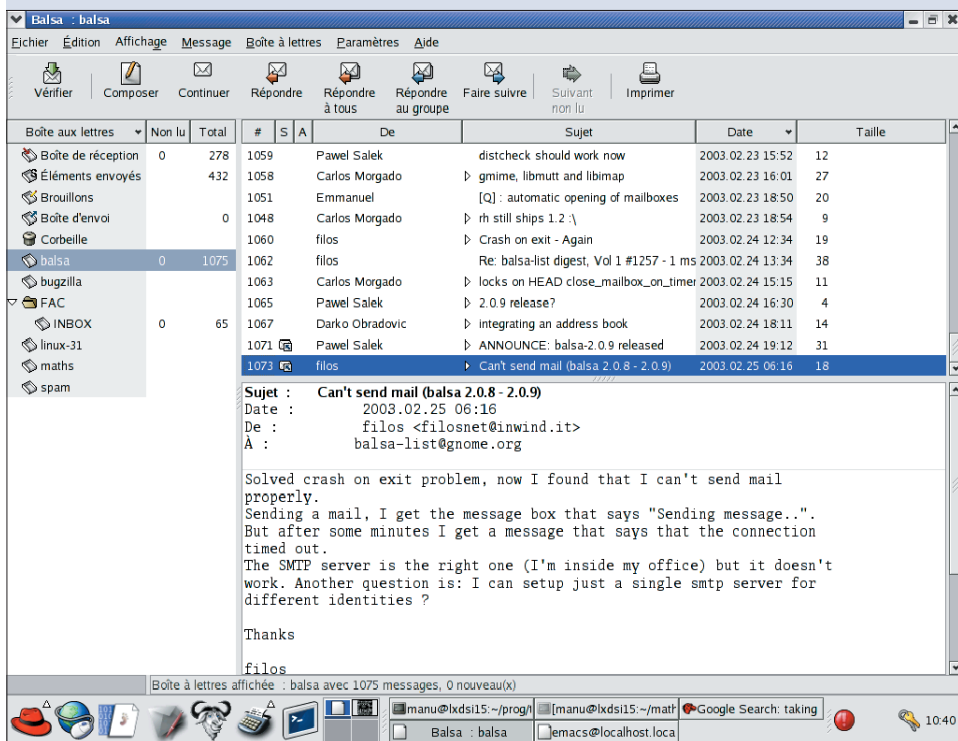


Abbildung 1: Das Programm Balsa ist eine von vielen E-Mail-Applikationen für Linux. Balsa ist in den Gnome-Desktop integriert, läuft aber auch in anderen Umgebungen.

**Willkommen** zu einer weiteren Ausgabe der Brave GNU World, diesmal mit einem Schwerpunkt Kommunikation und dem glücklichen Abschluss eines der ersten freien Softwareprojekte der europäischen Kommission.

## E-Mail

Unter Linux gibt es unzählige E-Mail-Programme. Viele enthalten Funktionen, die nichts oder nur indirekt etwas mit E-Mail zu tun haben. Das auf Gnome basierende Ximian Evolution [5] ist eine dieser umfangreichen Lösungen. Es richtet sich an Umsteiger von Microsoft Outlook, die in dem Programm eine sehr ähnliche Umgebung wiederfinden wie

auf dem Windows-System. Daher bringt Evolution auch einige Nachteile mit sich. Da es den kompletten Funktionsumfang von Microsoft Outlook abbilden muss, ist die Applikation entsprechend groß. Unter Linux hat sich jedoch das alte Unix-Paradigma der schlanken Anwendungen bis heute erhalten, was unter anderem ein Grund für den Erfolg von Ascii-Mailreadern wie Mutt [6] ist.

## Balsa

Doch es ist nicht nötig, gleich bis zu purem Ascii zurückzukehren, um einen schlanken und schnellen Mailreader zu erhalten, wie das Programm Balsa zeigt. Im Jahr 1997 begann Stuart Parmenter

mit der Arbeit an Balsa [7]. Dieses Mailprogramm ist in die Gnome-Oberfläche [8] integriert und benutzt GTK. Es ist komplett in die Gnome-Oberfläche integriert, funktioniert aber auch unabhängig von Gnome.

Ab Version 0.7 übernahm Pawel Salek die Koordination des Projekts, Balsa 1.0 kam im Jahr 2001 heraus. Diese Version verfügte bereits über die wichtigsten Funktionen wie das Verwalten mehrerer Identitäten und HTML-Mails. In 1.2 kam Unterstützung für die Libesmtplib von Brian Stafford hinzu, Version 1.4 unterstützte dank Albrecht Dreß erstmals GnuPG [9]. Obwohl es mittlerweile einen 2.x-Zweig gibt, ist Balsa 1.4.4 immer noch sehr verbreitet.

Mit Version 2.0 stellten die Entwickler auf GTK 2 um und die weitere Planung sieht für die 2.2-Release eine komplett neue Mime-Anbindung mittels GMime vor sowie verbesserte IMAP-Unterstützung, S/Mime und den GTK-2.4-Dateidialog. Daran arbeiten zurzeit vor allem Pawel Salek, Carlos Morgado, Peter Bloomfield, Emmanuel Allaud und Albrecht Dreß, natürlich mit der Unterstützung anderer Freiwilliger.

Es gibt bei der Programmierung von Balsa einige zentrale Design-Entscheidungen: Den Entwicklern ist vor allem eine möglichst genaue Einhaltung der E-Mail-Standards wichtig. Daher setzte Balsa bis Version 2.0 auf die Libmutter von Alan Cox. Erst ab Version 2.0 benutzt Balsa GMime von Jeffrey Steadfast, da diese Bibliothek besser mit einem grafischen Programm mit multiplen Threads zusammenarbeitet.

Was die Qualität des Codes angeht, sind die Balsa-Maintainer nach Aussage von Carlos Morgado schon fast übermäßig

konservativ. Außerdem legen die Programmierer viel Wert auf die Kompatibilität zu anderen Mail-Programmen, die entweder lokal auf dem eigenen Rechner oder auf anderen Computern in einem Netzwerk laufen. Zu guter Letzt soll Balsa sich auf die wesentlichen Funktionen – und ein paar coole Features – beschränken und nicht überladen oder langsam werden.

Auf Backend-Seite unterstützt Balsa verschiedenste lokale Mailbox-Formate sowie POP3 und IMAP. In den Augen von Steffen Klemer, einem der Entwickler, sind der flexible Mailfilter, die Kryptographie- und LDAP-Unterstützung, die integrierte Rechtschreibprüfung und die vielen Möglichkeiten zur Anpassung an persönliche Präferenzen spezielle Stärken von Balsa. Als Teil von Gnome überrascht es nicht, dass Balsa unter der GNU General Public License (GPL) als freie Software vertrieben wird.

## Spam: Kur gelungen – Patient tot

Es ist allgemein bekannt, dass Spam mehr als nur lästig ist. Manche Computernutzer ziehen es sogar vor, ihre E-Mails gar nicht mehr zu lesen. Viele

Gegenmaßnahmen erweisen sich nämlich nur kurzfristig als effektiv. Es findet ein Wettrüsten statt, das zunehmend Ressourcen bindet, die sonst für sinnvolle Aufgaben zur Verfügung ständen, und einige Methoden zur Spam-Abwehr sind geradezu dumm.

So erhielt ich kürzlich eine automatisch generierte Mail von einer unbekannt Person, die mich darauf hinwies, dass eine Mail von meiner Adresse eingegangen sei und wenn diese tatsächlich kein Spam sei, solle ich dies doch bitte per E-Mail-Antwort bestätigen. Andernfalls lande meine Adresse auf einer Blacklist und es würde ohne Nachfrage und Warnung jegliche künftige Korrespondenz mit meiner Adresse gelöscht.

Da der Absender dieser E-Mail offensichtlich zuvor eine Spam-Mail erhalten hatte, in der meine Adresse als Absender eingetragen war, hatte ich zwei Möglichkeiten: Ich konnte darauf antworten, was nicht verhindert hätte, dass der Betroffene weiterhin Spam mit meiner gefälschten Adresse bekommt. Oder ich konnte nichts tun – und nie mehr in der Lage sein, mit der Person zu kommunizieren. Dieser ineffektive Spamfilter wird über kurz oder lang für himmlische Ruhe bei diesem Nutzer führen.

Im E-Mail-System ist es möglich, eine Fehlermeldung an den Absender zu schicken, falls er eine Mail an eine Adresse geschickt hat, die es nicht gibt. Dummerweise fälschen Spammer ihre Mails mit existierenden Adressen, die sie vorher aus dem Web oder Usenet geholt haben. Die Fehlermeldung erreicht damit einen Dritten, der gar nichts mit den beiden anderen zu tun hat. Eine einzige Spam-Mail verstopft also indirekt die Postfächer von zwei Internet-Nutzern gleichzeitig.

Viele Anwender konfigurieren ihr System gleich so, dass Spam-verdächtige E-Mails ohne Rückmeldung gelöscht werden. So erfährt der Spammer nichts darüber, ob hinter dieser E-Mail-Adresse tatsächlich eine Person steckt oder ob es die Adresse überhaupt gibt.

Das Diagnosesystem, das vor der Spamflut sinnvoll und nützlich war, ist also nun dank der Spammer nicht mehr benutzbar. Denn viele Internet-Nutzer löschen mittlerweile derartige Diagnosemeldungen ungelesen. Es ist nämlich

sehr aufwändig, aus tausenden Diagnosesmeldungen eine herauszufinden, die vielleicht tatsächlich für den Benutzer relevant sind.

Funktionierte das Internet lange Zeit nach dem Prinzip „Keine Rückmeldung = vermutlich angekommen“, ist es dank der Wechselwirkung von Spam und Gegenmaßnahmen zu einem „Keine Rückmeldung = vermutlich gelöscht“-Netz geworden. Die Mail-Programme könnten zwar über Verwendung der Message-IDs unter den Rückläufern nach selbst verschickten Mails suchen, um das Diagnosesystem wieder benutzbar zu machen. Allerdings ist mir zurzeit kein Programm bekannt, dass diese Funktion implementiert. Hinzu kommt, dass es nur einen Teil des Problems lösen würde.

## Blacklists sind böse

Die wohl destruktivste und zweifelhafteste Form der Antispam-Maßnahmen sind Blacklists, die die Annahme von E-Mails bestimmter IP-Adressen verweigern. Da die meisten Internet-Nutzer ihre IP-Adressen dynamisch zugewiesen bekommen, bedeutet dies zum einen, dass Menschen willkürlich und ohne vorheriges Fehlverhalten ihrer Kommunikationsmöglichkeiten beraubt werden. Eine Vorgehensweise, die nicht zuletzt gegen die universelle Erklärung der Menschenrechte verstößt.

Zum anderen nutzen Spammer geackelte Rechner nichts ahnender Anwender für die Auslieferung ihrer Nachrichten. Die Besitzer derartiger missbrauchter Computer sehen sich plötzlich mit der Tatsache konfrontiert, dass sie niemanden mehr warnen können, da ihre Kommunikationsverbindung durch die Blacklists gekappt wurde.

Blacklists sind ein Instrument der willkürlichen Zensur, gemeinsam mit anderen Filtermechanismen gewöhnen sie uns als Internet-Nutzer daran, dass manche normale E-Mail nie ihr Ziel erreicht. Sollte irgendwann und irgendwo tatsächlich politische Zensur stattfinden, würden wir diese nicht einmal mehr als solche wahrnehmen.

Eine sehr viel ausführlichere Beschreibung des Problems gibt es auf der Website von Colin P. Fahey [10]. Er be-



**Abbildung 2: Das Wettrüsten zwischen Spammern und Antispam-Techniken nimmt ungeahnte Ausmaße an, doch neue Technologien könnten helfen, dem Spam-Problem ein Ende zu setzen.**

schreibt dort einen Lösungsvorschlag, der es vorsieht, ein Codesystem zur Authentifizierung von E-Mail einzuführen, das zusätzlich zu vorhandenen Mechanismen implementiert wird und keine Modifikation der vorhandenen Infrastruktur erfordert.

Zwei Parteien, die E-Mails austauschen wollen, verständigen sich bei diesem System vorher auf einen gemeinsamen Schlüssel, mit dem später ein bestimmter Code generiert wird, den Spammer nicht erraten können, wenn sie den Schlüssel nicht kennen. Diesen Code muss der Mail-Client des Absenders in die E-Mail einfügen. Der Client des Empfängers checkt, ob der Code stimmt, und weiß dann, ob die E-Mail vertrauenswürdig ist oder nicht.

Das klingt zunächst nicht schlecht, doch die Nachteile der Methode sind erheblich: Vor dem ersten Mail-Austausch müssen Anwender ihre Schlüssel über einen sicheren Mechanismus wie Telefon oder Fax austauschen, was eine große Umstellung bei den Nutzern erfordert. Außerdem ist es nötig, die E-Mail-Programme anzupassen.

Die Verwendung von OpenPGP [11] zur Mail-Signierung scheint hier angebrachter. Sie bringt die gleichen Vorteile (die automatische Unterscheidung zwischen Spam und Nicht-Spam), ist aber um einiges sicherer und ermöglicht auch digitale Unterschriften sowie die Verschlüsselung des gesamten Mailverkehrs.

## Provider in der Pflicht?

Die treuen Leser dieser Kolumne erinnern sich vielleicht noch an Ausgabe 54 [12], in der es auch um den Provider UK Free Software Network (UKFSN) ging. Dessen Kunden müssen laut Vertragsbedingungen damit rechnen, eine Gebühr von 150 britischen Pfund pro Empfänger zu zahlen, falls sie Spam versenden. Den Hauptgrund für den Versand von Spam, die sehr niedrigen Kosten, eliminiert UKFSN also. Daher haben mehrere Spammer schnell ihr Interesse an dem Provider verloren.

Würden mehr Provider diesem Beispiel folgen und so helfen, die Kosten der Spammer zu erhöhen, wäre dies zwar nicht die ultimative Lösung des Problems, doch derartige Maßnahmen sind

nützlich. Ebenso wie die Abkehr von harten Black- und Whitelists zugunsten von Greylists, bei denen Provider einen Wert für ihre Freundlichkeit gegenüber Spammern erhalten.

Der Einsatz von digitalen Signaturen, zum Beispiel mittels GnuPG [9] ist ebenfalls sehr effektiv. Dafür muss sich aber der Umgang mit diesen Technologien ändern, denn absurderweise bevorzugten in letzter Zeit gerade die großen Unternehmen E-Mails ohne Signaturen. Das ist so, als würde die Post handgeschriebene Briefe nicht mehr ausliefern. Letztlich ist es aber auch möglich, dass nur die Einführung eines neuen Protokolls zur E-Mail-Übertragung das Spam-Problem wirklich löst. Genau diesen Vorschlag hat D. J. Bernstein, der Autor des Mailserver QMail, gemacht.

Bis zu einer (endgültigen?) Lösung wird wohl noch etwas Zeit vergehen. Bis dahin bieten Erfolge wie die Durchsetzung des Antispam-Haikus von Habeas [13] zumindest kleine Lichtblicke. Für Anwender, die statt per E-Mail lieber direkt und in Echtzeit miteinander kommunizieren, ist der SILC-Client Silky sicherlich interessant.

## Silky

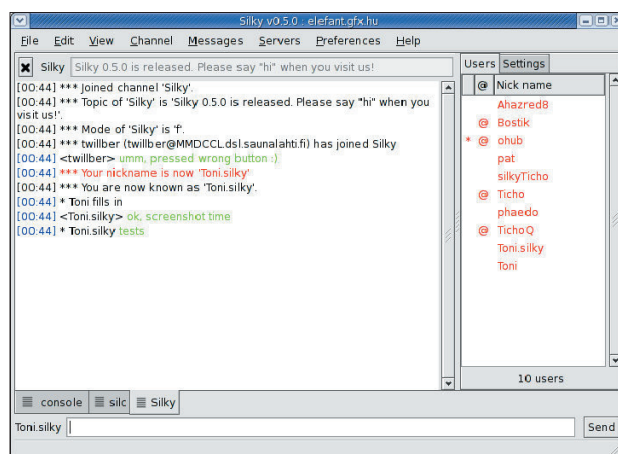
Das IRC (Internet Relay Chat) gehört zu den Oldies der Internet-Technologien, erfreut sich aber großer Beliebtheit. Und das trotz der großen Verbreitung sehr ähnlicher Anwendungen wie der Instant-Messenger ICQ & Co. Genauso wie bei anderen alten Internet-Protokollen wie TCP/IP oder SMTP haben sich die Erfinder auch beim IRC nicht sehr um die Sicherheit ihrer Entwicklung gekümmert. Ihnen ging es mehr um möglichst gute Funktionalität und Performance.

Vor allem in Ländern, in denen unbedachte Worte zu Repressalien führen können, sind aber unverschlüs-

selte Chatsysteme ein nicht zu vernachlässigendes Risiko. Kryptographie ist eine Möglichkeit, die Privatsphäre im Internet zu gewährleisten. Das mit Kryptographie ausgestattete Pendant zum IRC nennt sich SILC (Secure Internet Live Conferencing) [14]. Mit diesem Protokoll lassen sich Chatsysteme ähnlich dem IRC und auch Instant-Messenger-Lösungen entwickeln.

Der GUI-Client Silky [15] implementiert den SILC-Standard und steht unter der GPL. Die Oberfläche unterscheidet sich kaum von denen gängiger IRC-Programme. Im Sommer 2003 gründete Toni Willberg das Silky-Projekt, da es bis dato keine grafischen SILC-Clients gab. Bis jetzt haben es freiwillige Entwickler schon in acht Sprachen übersetzt. Das Programm ist bereits teilweise einsetzbar, auch wenn noch die eine oder andere Funktion fehlt. Toni Willberg bezeichnet den aktuellen Status als „zwischen Alpha- und Betastadium“ und rechnet mit Version 1.0 noch vor dem Ende des Sommers 2004.

Dafür sucht er noch Hilfe von interessierten Entwicklern, die Erfahrung in C-Programmierung mit den Bibliotheken Glib und GTK+ haben, auf denen Silky basiert. Das Programm integriert sich daher besonders gut in Gnome, ist allerdings auch unter anderen Environments lauffähig, da es keine höheren Gnome-Bibliotheken benutzt. Bisher haben Anwender Silky erfolgreich unter GNU/Linux, \*BSD, Mac OS X und Windows getestet. Laut Toni sind die wesentlichen Stärken des Projekts die starke Krypto-



**Abbildung 3:** Das Echtzeit-Protokoll SILC ist ähnlich aufgebaut wie das IRC, es bietet jedoch zusätzlich starke Kryptographie. Der SILC-Client Silky ist das erste SILC-Programm mit grafischer Oberfläche.

graphie sowie die ausdrückliche Orientierung auf Benutzerfreundlichkeit nach dem Motto „Wenn es deine Mutter benutzen kann, ist es einfach genug“. Die Kryptographie zwischen den Clients sorgt sogar dafür, dass selbst die Administratoren der Server Nachrichten nicht lesen können.

## Linux für Audio-Anwender: Agnula

Das Agnula-Projekt [16] hat es sich zum Ziel gesetzt, eine professionelle GNU/Linux-Distribution für professionelle Audio-Anwender zusammenzustellen. Das geschieht wahlweise auf Basis von Debian (Demudi) oder Red Hat (Rehmudi). Um dieses Projekt ging es zwar bereits vor einer Weile in Ausgabe 49 [17] der Brave GNU World, doch es gibt inzwischen einige Neuerungen.

Agnula hatte die Unterstützung der Europäischen Kommission und Ende März 2004 fand das offizielle Abschlussmeeting in Brüssel statt, bei dem die Entwickler die neue Version 1.0 vorstellten. Von Seiten der Kommission ist Agnula also beendet, auch wenn das Projekt selber keinesfalls am Ende ist, vielmehr hat sich im Laufe der Jahre eine Community gebildet, die das Projekt weiter aktiv betreiben wird.

Dennoch ist dies ein guter Zeitpunkt, um sich die aktuelle Ausgabe zu be-

schaffen, zumal Agnula als eine der wenigen Distributionen Wert darauf legt, ausschließlich freie Software zu enthalten. Anwender können also sicher sein, sich beim Installieren von Agnula keine versteckten Abhängigkeiten zu proprietärer Software einzufangen.

Damit dies auch so bleibt, gibt es die Agnula Trademark License [18] der Free Software Foundation Europe, die im Auftrag des ehemaligen Agnula-Konsortiums die Agnula Trademark in der EU registriert und die Lizenz dafür entwickelt hat. Grundgedanke der Lizenz ist es, im Sinne freier Software allen Interessenten die Verwendung der Marke zu gestatten, solange diese den Prinzipien des Projekts und des ehemaligen Agnula-Konsortiums treu bleiben und nur freie Software vertreiben.

## Agnula Trademark License

Das gibt den Anwendern die Sicherheit, dass Agnula-Distributionen oder Produkte – egal von welchem Distributor – immer frei von proprietärer Software sind. Jeder kommerzielle Distributor ist herzlich willkommen, eigene Agnula-Distributionen und Produktlinien herauszubringen. Anstatt mit Hilfe der Trademark den Wettbewerb einzuengen, verwenden die Entwickler sie, um ihn allgemein zu erlauben – solange alle die Spielregeln einhalten.

Das soll es für diesen Monat gewesen sein. Wie immer bitte ich um zahlreiche Ideen, Anregungen, Kommentare, Vorschläge und Fragen per E-Mail an die übliche Adresse [1]. (mwe) ■

### Infos

- [1] Ideen, Anregungen, Kommentare an die Brave GNU World: [\[column@brave-gnu-world.org\]](mailto:column@brave-gnu-world.org)
- [2] Homepage des GNU-Projekts: [\[http://www.gnu.org/\]](http://www.gnu.org/)
- [3] Homepage von Georgs Brave GNU World: [\[http://brave-gnu-world.org\]](http://brave-gnu-world.org)
- [4] „We run GNU“-Initiative: [\[http://www.gnu.org/brave-gnu-world/rungnu/rungnu.de.html\]](http://www.gnu.org/brave-gnu-world/rungnu/rungnu.de.html)
- [5] Ximian Evolution: [\[http://www.ximian.com/products/evolution/\]](http://www.ximian.com/products/evolution/)
- [6] Der Mail-Client Mutt: [\[http://www.mutt.org\]](http://www.mutt.org)
- [7] Gnome Balsa: [\[http://balsa.gnome.org\]](http://balsa.gnome.org)
- [8] Gnome: [\[http://www.gnome.org\]](http://www.gnome.org)
- [9] GNU Privacy Guard (GnuPG): [\[http://www.gnupg.org\]](http://www.gnupg.org)
- [10] Artikel „Spam: The Phenomenon“: [\[http://www.colinfahey.com/spam\\_topics/spam\\_the\\_phenomenon.htm\]](http://www.colinfahey.com/spam_topics/spam_the_phenomenon.htm)
- [11] OpenPGP: [\[http://www.openpgp.org\]](http://www.openpgp.org)
- [12] Georg C.F. Greve, „Brave GNU World“: Linux-Magazin 11/03, S. 78
- [13] „Habeas win \$100k judgement against spammer“: [\[http://www.theregister.co.uk/2004/04/07/habeas\\_spam\\_lawsuit/\]](http://www.theregister.co.uk/2004/04/07/habeas_spam_lawsuit/)
- [14] Secure Internet Live Conferencing (SILC): [\[http://www.silcnet.org\]](http://www.silcnet.org)
- [15] Silky: [\[http://silky.sf.net/\]](http://silky.sf.net/)
- [16] Das Agnula-Projekt: [\[http://www.agnula.org\]](http://www.agnula.org)
- [17] Georg C.F. Greve, „Brave GNU World“: Linux-Magazin 06/03, S. 82
- [18] Agnula Trademark License: [\[http://www.germany.fsfeurope.org/projects/agnula/license.html\]](http://www.germany.fsfeurope.org/projects/agnula/license.html)

### Der Autor

Dipl.-Phys. Georg C. F. Greve beschäftigt sich seit etlichen Jahren mit freier Software und kam früh zu GNU/Linux. Nach Mitarbeit im GNU-Projekt und seiner Aktivität als dessen europä-



ischer Sprecher hat er die Free Software Foundation Europe initiiert, deren Präsident er ist. Mehr Informationen finden sich unter: [\[http://www.gnuhh.org\]](http://www.gnuhh.org)

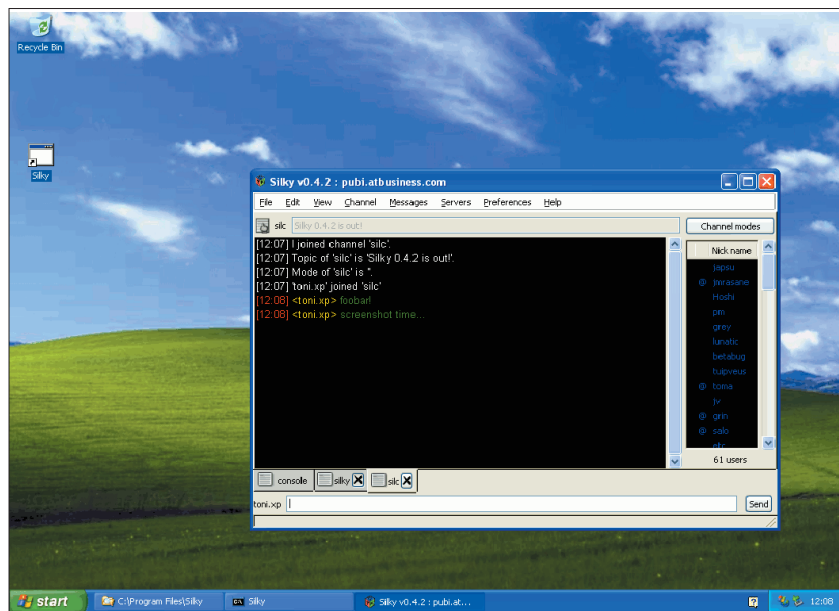


Abbildung 4: Das Chatprogramm Silky bietet verschlüsselte Verbindungen nicht nur unter Linux an, es läuft auch auf Windows und Mac OS X.