



*Sichere E-Mails mit Seahorse und Evolution*

*IRC in der Konsole: WeeChat*



*OpenTTD - Die Wirtschaftssimulation für Linux*

# Vorwort

Und wieder einmal ist ein Monat in die Lande gezogen. Mittlerweile schreiben wir den 15. März und – worauf wir besonders stolz sind – an einem weiteren Kapitel in der Geschichte unseres Projekts.

In den letzten Ausgaben noch vermisst, wurden wir in den vergangenen Wochen förmlich mit erfreulichen Ereignissen überschüttet. Wie man nun bereits erahnen kann, möchten wir euch an einigen dieser Geschehnisse teilhaben lassen. Um diesen Meldungen aber in allem Umfang gerecht zu werden, haben wir uns dazu entschlossen, das Vorwort – der genervte Leser schlage nun die Hände über dem Kopf zusammen – inhaltlich auszudehnen. Bevor aber der nun zusätzlich zur Verfügung stehende Platz vollkommen mit derartigen Hiobsbotschaften ausgefüllt wird, beginnen wir lieber einmal:

An erster Stelle ist es interessant zu wissen, dass nicht nur wir über allerlei Dinge aus der Linux-Welt berichten, sondern andere Persönlichkeiten auch einmal über uns berichten wollen. Daniel Schneider ist eine eben jener Personen und hat im Rahmen eines Berichts über freie und kostenlos verfügbare Linux-Magazine ein Interview mit den Kollegen von freiesMagazin [1], MagDriva [2], ProLinux [3] und – man möge es kaum glauben – auch mit Vertretern der Yalm-Redaktion geführt. Dieses äußerst umfangreiche und vor allem informative Interview, das wissenswerte Themen wie beispielsweise Entstehungsgründe, organisatori-

sche Belange und Ziele der einzelnen Projekte näher beleuchtet, findet ihr auf Daniels treffend betitelter Website »Pinguinzubehör« [4]. Für seine Zeit und seine Mühen möchte sich die Redaktion noch einmal in jeder Form herzlich bedanken.

Doch damit nicht genug, es gab auch etliche interne, schon lange angekündigte und nun endlich eingelebte, Neuerungen. Dazu aber, wie könnte es anders sein, eine kleine Geschichte:

Das offizielle Yalm-Forum [5], zentrale Verwaltungsstelle und Treffpunkt der Redakteure, litt unter einigen technischen »Schwierigkeiten«. Es begann alles mit verhältnismäßig harmlosen MySQL-Fehlermeldungen, die zwar störten, den Arbeitsablauf geringfügig aufhielten, ansonsten aber nicht weiter behinderten. Doch dies war erst der Anfang, das Ganze gipfelte schließlich darin, dass Posts zwar angefertigt und »abgesendet«, im Forum selbst aber nie dargestellt wurden. Zwar trat dieser Fehler nur sporadisch in Erscheinung, und obgleich nichts Verheerendes eintrat gab es doch einige ärgerliche, auf diese Weise verursachte, Verluste.

Der »Fehler« fand sich schließlich an unserem, offenbar vollkommen überlasteten, VServer. Der logische Umkehrschluss legte demnach die Anschaffung eines neuen Servers nahe. Normalerweise dürfte man nun eine sich über Monate ziehende, auch an Punkten wie der Kosten-

frage immer wieder scheiternde Diskussion erwarten, doch bereits binnen weniger Stunden war die Lösung eigentlich schon gefunden. Gleich zwei Redaktionsmitglieder haben ihre Hilfe angeboten; an dieser Stelle ein weiteres Dankeschön an Thomas Rudolph und Peter Majmesku, letzterer nun offizieller Host unserer Server.

Mit diesem neuen Rootserver wurden aber nicht nur die zuvor bezeichneten Fehler ausgemerzt; es hielten, wie bereits angedeutet, auch weitere und bemerkenswert angenehme Innovationen Einzug. Beginnen wir einmal mit unserer Artikelverwaltung:

Eben diese wurde komplett umgestellt und neu strukturiert. Tatsächlich bedienen wir uns nun der freien Software »DokuWiki« [6]. Zwar hatten wir vor einigen Monaten vermeldet, dass sich ein eigenes Redaktionssystem in Entwicklung befände, was so gesehen auch stimmte, aber letzten Endes gab es einige erschwerende Hindernisse. Gewiss, wir hätten die Entwicklung auch weiter vorantreiben können, aber bereits Sergej P. Koroljow sagte:

*»Die Genialität einer Konstruktion liegt in ihrer Einfachheit. Kompliziert bauen kann jeder.«*

Wahre Worte, bedenkt man die einfach zu erlernende Wiki-Syntax und das hervorragende Änderungsprotokoll, welches DokuWiki mit sich bringt. Weiterhin haben unsere Web-Entwickler einige zusätzliche Tools erschaffen, die uns weiter entgegenkommen und den gesamten Ablauf noch einmal automatisierter gestalten und viel Arbeit, insbesondere bei der Einhaltung von einheitlichen Formatierungen, ersparen. Dies sind freilich nur einige Gründe, welche uns letzten Endes zur Nut-

zung von DokuWiki bewegten, aber im Gegensatz zu dessen Vorgänger ist es einfach zu handhaben und spart ergänzend ein großes Maß an Zeit sowie Ressourcen, welche, hätten wir auf die Weiterentwicklung der ursprünglichen YalmDocs bestanden, verbraucht worden wären.

Aber all das hat natürlich auch Vorteile für euch. Ab sofort kann man einzelne Artikel – und damit im Gesamtbild auch die komplette Ausgabe – online in unserem Wiki ansehen. Wir denken, dass den Forderungen nach einer HTML-Ausgabe somit Genüge getan wurde; für Anregungen, Kritik und weitere Ideen sind wir aber selbstverständlich sehr dankbar. Wie immer genügt hier ein Post in unserem Forum oder eine kurze Mail an [redaktion@yalmagazine.org](mailto:redaktion@yalmagazine.org).

Womit wir auch schon beim nächsten Punkt dieser scheinbar nicht enden wollenden Liste angelangt wären: Auch der E-Mail-Verkehr wird nun direkt über unseren Server abgewickelt. Dies gestaltet die Sache nicht nur angenehmer, sondern bietet auch noch aus organisatorischer Perspektive einige Vorteile, auf die genauer auszuführen wir an dieser Stelle aber verzichten möchten.

Damit wären die wichtigsten Punkte abgehandelt. Aber in diesem Monat gab es nicht nur viel zu berichten, nein, auch die Redaktion hat die größtenteils regnerischen Tage effektiv genutzt und dafür gesorgt, dass diese Ausgabe erneut die 40-Seiten-Marke erreichen konnte. Wie man sich infolgedessen bereits denken kann, werden in diesem Monat Themen aus den verschiedensten Bereichen in gewohnter Qualität behandelt.

So, was gäbe es noch? Da wir uns in diesem Monat nicht schon wieder selbst bemitleiden und uns über fehlende Nachrichten beschweren wollen – was in diesem Falle auch schlicht gelogen wäre – könnten wir nun wirklich damit beginnen, Meldungen aus der ganzen Linux-Welt aufzugreifen und uns mit einigen davon genauer auseinanderzusetzen.

Aber da hierfür der noch vorhandene Platz nicht ausreicht, verzichten wir besser darauf und warten ab, welche Überraschungen der April bereithält.

Abschließend möchten wir jedenfalls noch einmal um euer Feedback, insbesondere aber zu unserer HTML-Ausgabe, bitten.

Somit wäre nun auch dieses überdimensionierte Vorwort an seinem Ende angelangt, weshalb uns nicht mehr verbleibt als euch alles Gute und viel Vergnügen mit dieser Ausgabe zu wünschen.

Stefan Zaun  
[sciron@yalmagazine.org](mailto:sciron@yalmagazine.org)

### Informationen

- [1] <http://www.freiesmagazin.de/>
- [2] <http://www.mandrivauser.de/doku/doku.php?id=allgemein:magdriva>
- [3] <http://www.pro-linux.de/>
- [4] <http://www.knetfeder.de/linux/index.php?id=38>
- [5] <http://yalmagazine.org/forum/index.php>
- [6] <http://www.dokuwiki.org/dokuwiki>

### Inhalt

<b>Yalm - Vorwort.....</b>	<b>2</b>
Vorwort.....	2
<b>Yalm - Rückblick.....</b>	<b>4</b>
Rückblick.....	4
<b>Yalm - Magazin.....</b>	<b>5</b>
World Of Goo 1.40.....	5
Medienwiedergabe in der Konsole.....	8
Ubuntu 9.04.....	14
Pidgin – Nachrichtenverschlüsselung mit OTR.....	16
OpenTTD – Das Urgestein der Wirtschaftssimulationen auf dem Linuxsystem.....	18
Verschlüsseln und Signieren von E-Mails mit Seahorse und Evolution.....	23
Arbeiten in der Konsole (II): WeeChat – IRC Client.....	28
AssaultCube.....	33
Kleiner TrueCrypt Guide.....	35
<b>Yalm - Schlussbemerkungen.....</b>	<b>40</b>
Schlussbemerkungen.....	40

# Rückblick

## Gnome 2.26 RC erschienen

Das Gnome-Projekt hat die letzte Entwicklerversion vor der Veröffentlichung freigegeben. Die endgültige Version wird in den nächsten Wochen erscheinen. Neuerungen sind das Brennprogramm Brasero, welches den Nautilus-CD-Brenner ersetzt und Aufräumarbeiten im Code, wodurch der Start mehrerer Programme beschleunigt werden soll; allen voran Nautilus. Ferner wurde Evolution um eine MS-Exchange-Server-Funktion erweitert, die auch Exchange-Server-2007 unterstützt. [1]

## Songbird 1.1.1

Eine neue Version des auf Xulrunner basierenden Media Players ist erschienen. Der Player unterstützt jetzt Cover-Downloads von Last.FM, Normalisierung und vieles mehr. Die wichtigsten Verbesserungen wie das Überwachen von Ordnern sollen aber erst unter Windows richtig funktionieren. [2]

## Vanilla-Kernels in Ubuntu verfügbar

Um eine bessere Hardwareunterstützung auch auf älteren Generationen von Ubuntu zu gewährleisten, veröffentlichen die Ubuntu-Entwickler künftig auch die sogenannten »Vanilla-Kernels« von kernel.org, allerdings ohne Support. Proprietäre Treiber und ubuntu-spezifische Änderungen sind natürlich nicht enthalten. [3]

## Probleme mit Ext4

Nach Berichten mehrere Nutzer gibt es Probleme mit Ext4, welches nach Abstürzen Datenverlust verursachen soll. Die Probleme treten wegen einer Caching-Änderung auf: Während Ext3 alle fünf Sekunden die Daten auf die Festplatte schreibt, lässt sich Ext4 bis zu 60 Sekunden Zeit, was unter anderem einen Performancegewinn mit sich bringt. [4]

## Freier Flashplayer Gnash 0.8.5 erschienen

Die freie Alternative zum proprietären Flashplayer von Adobe unterstützt mittlerweile die Version 7 von SWF und Version 2 von Actionscript. Den Einsatz kann man aber noch nicht empfehlen, da der Player rund 3 Versionen zurück liegt: Die Aktuelle SWF beträgt 10, Actionscript liegt in Version 3 vor. [5]

## Firefox 3.5 statt 3.1

Die Entwickler von Mozilla haben beschlossen, die neue Version von Firefox mit 3.5 anstatt 3.1 zu versehen, um eine umfangreiche Erweiterung und Überarbeitung zu signalisieren. Mit an Bord sollen unter anderem Unterstützung der HTML-5-Elemente <audio> und <video> Tags sein, welche hoffentlich die Vormacht von Flash beim Streamen von Musik und Videos brechen können. Auch die

JavaScript-Engine soll zukünftig noch schneller sein und gemeinsam mit spekulativem Parsen den Seitenaufbau beschleunigen. [6], [7]

Bernhard Posselt  
ray@yalmagazine.org

## Informationen

- [1] Gnome 2.26 RC erschienen: <http://derstandard.at/?url=/?id=1234508757407>
- [2] Songbird 1.1.1: <http://www.pro-linux.de/news/2009/13927.html>
- [3] Vanilla Kernels in Ubuntu verfügbar: <http://derstandard.at/?url=/?id=1234508464160>
- [4] Probleme mit Ext4: <http://derstandard.at/?url=/?id=1234509298539>
- [5] Freier Flashplayer Gnash 0.8.5 erschienen: <http://www.pro-linux.de/news/2009/13896.html>
- [6] Firefox 3.5 statt 3.1: <http://www.pro-linux.de/news/2009/13902.html>
- [7] Firefox 3.5 offiziell bestätigt: <http://www.golem.de/0903/65829.html>

# World Of Goo 1.40

**Kaum jemanden lässt das Spiel mit den klebrigen Schleimbällchen in verschiedenen Variationen unbeeindruckt. Es verbindet erfrischend absurden Humor, Stil, Atmosphäre und Köpfchen. Das derzeit beste Spiel für Linux? Wir haben es uns näher angesehen.**

## Der Ausbruch einer Sucht

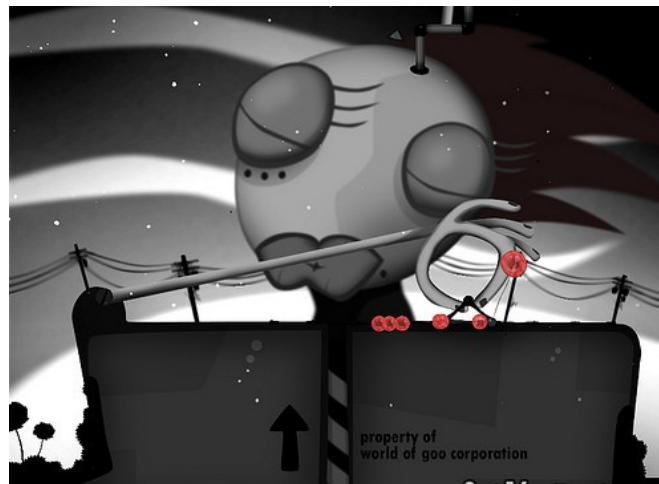
Da sitzt man also mit einem Becher Kaffee vor dem PC und plaudert ein wenig zum Wachwerden im IRC-Channel des Yalmagazines [1] und plötzlich ist da die Rede von »wog«. Was mag dieses Akronym denn bedeuten? Merkwürdigerweise häufen sich daraufhin in kurzen Abständen von mehreren Besuchern, die zuvor das Demo heruntergeladen haben, verräterische Emotionsausbrüche wie »wahaha«, »X-)«, »hrhr« usw. Anschließend lädt man aus konsequenzenreicher Neugier also selbst die Demoversion, welche als Debian-Paket [2] nur 40 MB umfasst. Installiert es in einem Ruck, spielt es und muss aus purer Begeisterung sein eigenes »wahaha« in den Channel posten. Mag es auch herzlich albern sein.

## Spielprinzip

Das Prinzip an sich ist simpel. Wie bei einem Puzzle muss man lustig aussehende »Goo-Bälle« aneinanderkleben und sich in einer liebevoll gezeichneten 2D-Vektorlandschaft zu einem Rohr bewegen. Ist man nahe daran, saugt das Rohr die Goos an, welche in einer vorgegebenen Anzahl durch das Rohr hindurchschießen müssen, damit das Level beendet ist. Zur Abwechslung gibt es ausnahmsweise andere Levelziele. Am Ende des

ersten Kapitels (das Inhalt der Demos ist), muss man sich beispielsweise »zum Himmel« hocharbeiten, eine Anzahl Goos an Luftballons befestigen und diese hochfliegen lassen.

Das war es im Großen und Ganzen gewesen. Selbst pfiffige Kleinkinder sollten das Spielprinzip auf Anhieb verstanden haben. Doch Vorsicht: Als Hindernis haben die Entwickler die Physik eingebaut. So baumelt man oft gefährlich nahe an vernichtenden Stacheln, Feuerzungen oder Abhängen. Mitunter erinnert das Goo-Bauwerk an einen Berg aus Gelee. Oft sieht man sich in der Rolle



*Level mit einem weiblichen Goo*

eines Architekten, der die Statik zu überlisten trachtet.

## Eine knifflige Angelegenheit

In späteren Levels ist das Ziel des Spiels nicht direkt ersichtlich und man arbeitet sich durch Versuche vor. Auch der mysteriöse Schildermaler ist einem vorangegangen und hat scheinbar wahllos in der Landschaft rätselhafte Hinweise hinterlassen, die vom witzigen Schreibstil her an Terry Pratchett erinnern. All das wird von einer gelungenen So-und-kulisse unterstrichen. Die Goos quietschen beim Anfassen, freuen sich und drücken auch sonst bei jedem Anlass wie Äffchen ihre Gefühle aus.

Es gibt verschiedene Goo-Spezies, die man kombinieren muss. Da gibt es die »goo-schwangere Schöne«, die man aufbrechen muss um an weitere Goos zu gelangen, die Totenkopf-Goos, die stachelresistent sind, die Luftballon-Goos usw. Es ploppt. Es wabbelt. Es piept: »Ohje, ein Luftballon weniger und man hätte die Klippe gemeistert. Was solls – neustarten.« Zum Glück ist zu jedem Level auf Youtube eine Lösung vorhanden. Denn manche Levels sind eben knifflig. Doch steigt die Schwierigkeitskurve nicht dröge gleichmäßig an. Zwischendurch kommen erfrischend einfache Levels, die aufatmen lassen und einem die Feststellung eingeben, dass man doch nicht auf den Kopf gefallen ist. Denn räumliches und logisches Denken greifen je nach Level in unterschiedlicher Dosis.



### Entwickler & Veröffentlichung

Kaum zu glauben. Gerade einmal drei Leute waren hauptverantwortlich in die Produktion involviert: Kyle Gabler war für Grafik, Musik und Story zuständig, Ron Carmel, der wie Gabler einst bei Electronic Arts in Lohn und Brot stand, kümmerte sich um Produktion und Programmierung; später ergänzte Allan Blomquist noch das Projekt und machte sich an die Wii-Umsetzung – welche erst im Februar auf den Markt kam. Der Entwickler ist 2D Boy [3] und den Verleger hat im deutschsprachigen Raum RTL-Games inne, der die Schleimbällchen ab dem 26.02. als DVD-Box auf den Markt bringt. Erstmals wurde das Spiel am 13. Oktober 2008 als Downloadvariante herausgegeben. Bis zur Veröffentlichung durch RTL-Games in Videospielläden konnte man sich das Spiel lediglich vom US-Server herunterladen, was wider Erwarten fix von der Stange geht. Sofern man Homebanking betreibt, kann man sich kurzer Hand bei PayPal anmelden und das Spiel per Lastschrift bezahlen.

Mehrere Mitglieder der Yalm-Redaktion haben sich die Software auf diese Weise gekauft, was ausnahmslos ohne Probleme klappte. Das Spiel kostet über die Downloadvariante 20 \$ (umgerechnet ca. 16 €) und man bekommt im Anschluss an die bei PayPal angegebene E-Mail Adresse einen Link zur Downloadseite zugesendet. Dort kann man sich das Spiel für Linux (.deb, .rpm, .tar.gz), Mac (.dmg) und Windows (.exe) herunterladen. Die DVD-Box kostet bei amazon.de 18,97 €. Zwei Tage nach der Veröffentlichung der Linux-Version betrug der Anteil der Downloads für das freie

Betriebssystem 4,6% von den Gesamtdownloads. 12% luden das Spiel als .rpm-, 30% als .tar.gz- und 57% als .deb-Paket. An dem Tag, als die Linux-Ausgabe erschien, wurden über die Website mehr Kopien verkauft, als an jedem anderen Tag. Dieser Tag überschritt das bisher höchste tägliche Downloadvolumen um 40%. Dadurch wird ein lukrativer Markt für Linuxspiele deutlich. Leider gibt es den Level-Editor bisher nur für Windows. Mit WINE bringt man ihn nicht zum Starten. Abhilfe schafft hierbei eine VM.

### Kompletter Verzicht auf DRM

Gegen die Mode besitzt das Spiel keinerlei Kopierschutz. Kyle Gabler errechnete, dass Anfang November 2008 ungefähr 82 Prozent der Goo-Spiele illegale Kopien waren. Er verglich die Verkaufszahlen mit dem Spiel *Ricochet*, das mit Kopierschutz ausgeliefert wurde, und kam zum Ergebnis, dass ein Kopierschutz nur ein tausendstel der jetzigen Besitzer illegaler Kopien erwogen hätte, ein Original zu kaufen. Zunächst ging er von 90 Prozent an illegalen Kopien aus, berechnete nach Zweifeln im Forum jedoch neu. Dabei ging er nun auch davon aus, dass ein Benutzer das Spiel durchschnittlich an 1,25 Computern installiert. Dennoch war World of Goo zeitweilig hinter *World of Warcraft* das am zweitbesten verkaufte Spiel bei amazon.com. Bei den US-WiiWare-Verkäufen lag World of Goo

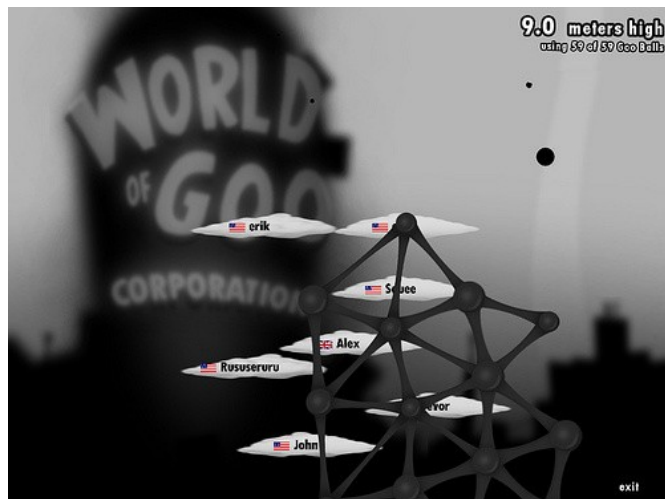
mehrere Wochen lang auf dem ersten Platz. Am 20. Januar 2009 stellte Kyle Gabler den Soundtrack gratis zum Download bereit [4].

Der Publisher Brighter Minds Media musste 2009 einen Antrag auf Restrukturierung stellen. Er stellte jedoch klar, dass die illegalen Kopien bei World of Goo nicht zu den finanziellen Problemen beigetragen hatten, sondern die Wirtschaftskrise, gestiegene Verschuldung und generell gesunkene Verkaufszahlen die Hauptschuld trügen. 2D Boy erklärte, dass es keine Verbindung zum Verzicht auf DRM bei World of Goo gebe und das Experiment fortgesetzt werde. Nach unserer Recherche konnten wir auf Anhieb bei den einschlägigen Torrent- sowie Rapidshareseiten zwar theoretisch die



Hinaus aus dem Maul des Goo-Frosches

Windows-Ausgabe herunterladen, jedoch war der Linux-Ableger nirgends zu finden. Was wohl mit dem kleinen Marktanteil von Linux und der Dominanz von Windows im Spielesektor zu erklären ist. Diese Tatsache wird sich womöglich mit der Verbreitung der DVD-Box durch RTL-Games noch ändern.



*Im Turmbau-Modus kann man sich mit anderen Spielern messen*

### Kritiken

Im deutschsprachigen Raum gab 4players.de [5] dem Spiel eine hohe Wertung von 86%. Ähnlich wertete die Gamestar mit 84%. Auf internationaler Ebene erhielt es bei den Websites MobyGames, Gamerankings und Metacritic, die eine Durchschnittsbewertung aus mehreren Bewertungen durch Fachzeitschriften ermitteln, zum 16. Januar 2009 88% bis 90,8% und die Wii-Fassung 93,7% bis 95%. Von IGN wurde World of Goo in sieben Kategorien ausgezeichnet, darunter Wii Game of

the Year, Best Puzzle Game für PC und Wii sowie Best WiiWare Game für Wii. Bei Gametunnel und Rock Paper Shotgun wurde World of Goo zum Spiel des Jahres, bei Gamasutra nach Fallout 3 zum zweitbesten Spiel des Jahres gewählt.

### Auch ein Topspiel hat Schwachstellen

Nach der Installation passt sich das Spiel den System-Spracheinstellungen an und man kann sofort loslegen. Die eventuell zuvor installierte Demo muss unter Linux nicht deinstalliert werden, denn diese geht in die Vollversion über. Word of Goo besitzt leider kein Konfigurationsmenü für Grafik- oder Soundeinstellungen. Es lässt sich zwar in der Config-Datei `/opt/WorldOfGoo/properties/config.txt` die Auflösung anpassen, der Sichtbarkeitsbereich wird im Spiel aber nicht größer. Die 47 Level sind in etwa 7 Spielstunden durchgespielt. Mittels einer Anwendung von Spielsucht ist diese Zeit jedoch schnell verfliegen. Es bietet sich nur noch ein Turmbaumodus an, bei dem man mit den Goos, welche über das Sammelziel hinaus eingeheimst wurden, ein Bauwerk in Konkurrenz zu Statistiken anderer Spieler errichten kann. Dieser Modus gestaltet sich aber auf nur einer Landschaft, die nicht sonderlich einladend in dunklen Farben gehalten ist. Außerdem kann man versuchen, das ZKV (zwingendes Kriterium für Vollständigkeit) zu knacken, was durchaus anspruchsvoll sein kann.

In der Wii-Version gibt es einen Spielmodus für vier Spieler, und die Entwickler haben Planungen zu einem Mehrspielermodus für den Computer bekannt gegeben, der in Partnerschaft mit Steam

Raubkopierer fernhalten soll. Sollte man das Spiel über die Downloadvariante erstehen, so gelangt man zu einer Seite mit den jeweils aktuellen Versionen. Zum Zeitpunkt der Niederschrift dieses Artikels war das die Version 1.40. Die Besitzer der DVD-Box dürften sicherlich auch Zugang zu Updates erhalten. Somit dürfte man sich in kommender Zeit auf weitere Neuerungen freuen. Mehr Levels, mehr Spielmodi, ein größerer Sichtbereich mit Zoom-Möglichkeiten und ein Konfigurationsmenü. Wenn das umgesetzt werden kann, wird sich das gut angefangene Spielejahr für Linuxer positiv fortsetzen.

Peter Majmesku  
pe@yalmagazine.org

### Informationen

- [1] [irc.freenode.net #yalmagazine](http://irc.freenode.net/#yalmagazine)
- [2] Debian-Paket:  
<http://worldofgoo.com/dl2.php?lk=demo>
- [3] Homepage der Entwickler:  
<http://2dboy.com/>
- [4] Gratisdownload des Soundtracks:  
<http://kylegabler.com/WorldOfGooSoundtrack/>
- [5] Test bei 4players.de:  
[http://www.4players.de/4players.php/disbericht/P-C-CDROM/Test/9550/60678/0/World\\_of\\_Goo.html](http://www.4players.de/4players.php/disbericht/P-C-CDROM/Test/9550/60678/0/World_of_Goo.html)

# Medienwiedergabe in der Konsole

**Effizienz, Beschränkung auf das wesentliche und eine Spur Extravaganz. So könnte man viele Konsolenprogramme umschreiben. Programme zur Wiedergabe von Audio und Video unter Linux werden immer hungriger, was Speicher und CPU Auslastung anbelangt. Einige Alternativen werden in diesem Artikel vorgestellt.**

Wenn man es genau betrachtet, wären Programme wie z. B. Amarok [1] ohne die Konsole zum Teil nicht möglich. Aber das kann man auf viele grafische Programme beziehen. Alle Anwendungen, die grafisch dargestellt werden, setzen zwingend einen laufenden X-Server in Verbindung mit einem Window- oder Desktop-Manager voraus. Doch was machen, wenn man genau diese Voraussetzungen nicht erfüllen kann oder möchte?

## Da »rockt« die Kommandozeile

Um seine Musik abspielen zu können oder um Internetradio bzw. Musikstreams zu empfangen und wiederzugeben, braucht es nur die Konsole. Wiedergabeprogramme dafür gibt es wie den sprichwörtlichen Sand am Meer.

Ein altes Vorurteil zur Arbeit in der Konsole bzw. auf der Kommandozeile ist, dass man teils ellenlange Befehlsketten eingeben muss. Das mag für manche Programme stimmen, aber auch die Konsole bietet dank ncurses [2] eine semi-graphische Oberfläche für diverse Programme. Bekanntester Vertreter dürfte der Midnight Commander [3] sein. Dieser Dateimanager, der dem Norton Commander® nachempfunden wurde, gehört wohl zu den

beliebtesten Vertretern der ncurses-Bibliotheken. Doch auch andere Programme nutzen diese, um dem Benutzer eine Oberfläche zu bieten, die einem grafischem X-Programm in keiner Weise nachstehen soll. – Aber Achtung: Führt man Kon-

solenprogramme in einem Terminalemulator wie z. B. gnome-terminal aus, so stehen einige Funktionstasten nicht zur Verfügung. So führt z. B. der Druck auf die [F1]-Taste dazu, dass die Hilfefunktion des verwendeten Desktop- oder Window-Managers aufgerufen wird.

## mp3blaster

Um mp3blaster zu installieren, genügt es, den Paketmanager seiner Distribution zu starten und nach dem Programm zu suchen. Nach der Installation startet man das Programm mit dem Befehl:

```
jan@ubuntu-netbook: ~/Dokumente/Programmierung/Testdateien
Datei Bearbeiten Ansicht Terminal Reiter Hilfe

jan@ubuntu-netbook: /media/disk/Splinter-Jens/Madagascar... X jan@ubuntu-netbook: ~/Dokumente/Programmierung/Testdat... X

[F 1] Add Files To List [F 2] Invert Selection [F 3] Recurs. Select All
[F 4] Enter New Path [F 5] Add Dirs As Groups [F 6] Convert MP3 To WAV
[F 7] Add URL(shoutcast) [ / ] Start Search [ s ] Toggle File Sort
[ f ] Toggle File Display [bsp] Go Up One Dir [spc] Select File

Sorting mode : Sort alphabetically, case-insensitive
Next Song :

./
bin/
boot/
cdrom/
dev/
etc/
home/
lib/
media/
mnt/
opt/
proc/

|>
<Unknown Album> (no comments)

[ ] shuffle
[ ] repeat
0:00
0:00

[ < ] [ > ] [ > ]
4 5 6

[ << ] [ ] [ >> ]
1 2 3

[ t ] Mixer
Vol
[ < ] +064% [ > ]

1 2 3 4 5 6 7 ACPI: 40 °C / AC-Strom / CPU: 800 MHz / Wetter: -3 °C / Freitag: 20.02.2009 10:49 KW-08 / 1.10, 0.97, 0.82 / MemFree: 27476 kB
```

*mp3blaster in Aktion*



## mp3blaster

Man befindet sich unmittelbar nach dem Start in einer Oberfläche wieder, die auch als CLI [4] bezeichnet wird. Da es im Normalfall keine Mausunterstützung in der Konsole gibt, steuert man das Programm bequem per Tastatur.

Im oberen Teil der Oberfläche findet man diverse Funktionen zusammen mit der jeweiligen Taste. Um sich einen groben Überblick zu verschaffen, drückt man die Taste [+], um durch die verschiedenen Funktionen zu »scrollen«. Am rechten Rand befinden sich die bekannten Symbole für Play, Stop usw. Gesteuert werden diese über die Zahlen auf der Tastatur. Unterhalb der Symbole befindet sich der Lautstärkeregler. Mittels der Taste [T] schaltet man die diversen Mixer-Devices des Soundservers durch und reguliert diese mit den Tasten [<] und [>] jeweils nach rechts (lauter) oder links (leiser).

In der Mitte von mp3blaster befindet sich eine große freie Fläche. Diese dient zum Navigieren durch die Verzeichnisse und Playlisten. Mittels [F1] kann man nach einzelnen Dateien suchen. Wer gleich eine ganze Playlist einlesen lassen möchte, drückt stattdessen [F3].

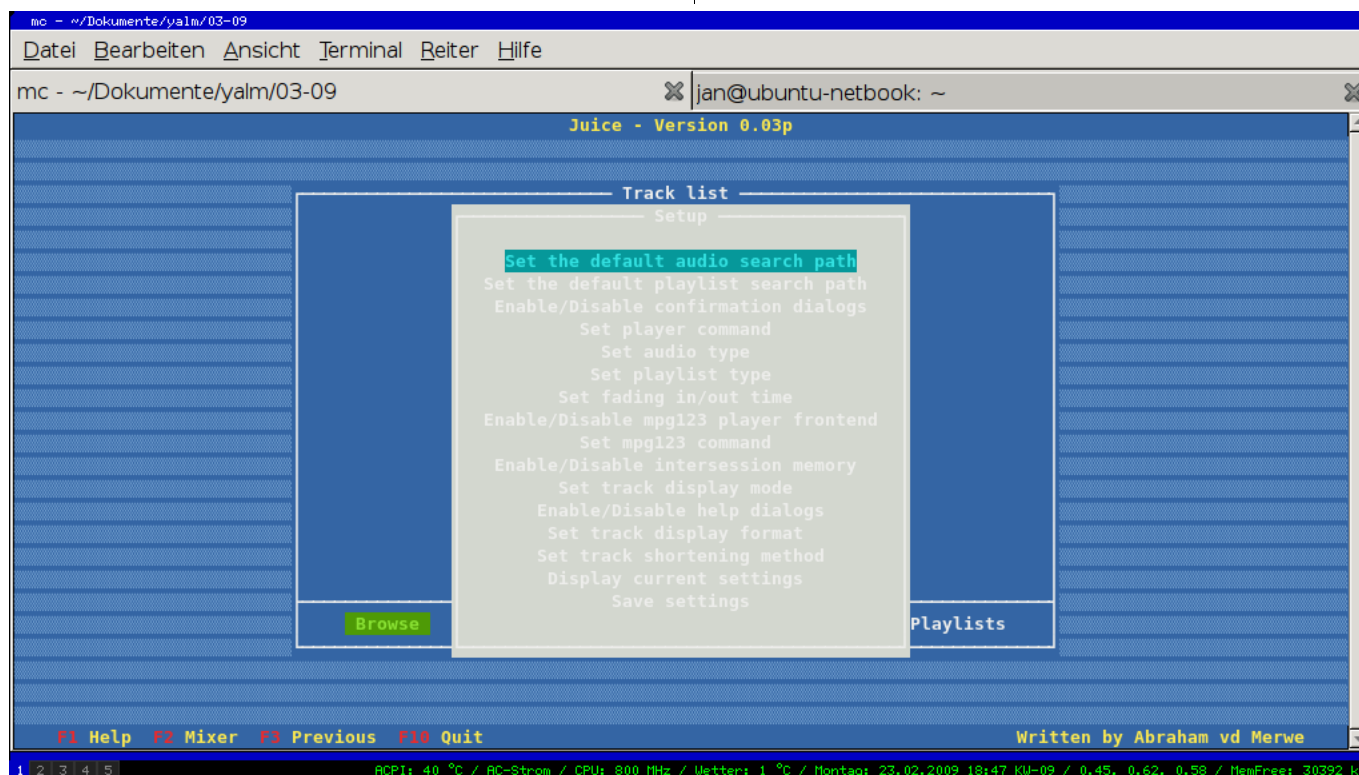
Doch mp3blaster kann, anders als der Name vermuten lässt, nicht nur MP3-Formate wiedergeben. Auch OGG Vorbis [5] und WAV gehören zum Wiedergabefundus des Programms. Ferner kann man

einzelne Dateien oder auch ganze Playlisten von MP3 nach WAV konvertieren lassen, um sie später gleich auf CD brennen zu können. Wenn man keine Lust auf seine eigene Musik hat, kann man auch Internetradio hören. Auch Wiedergabemöglichkeiten für den Endlosbetrieb sind mit an Board (*shuffle* und *repeat*). Durch diverse Scripte kann man den Funktionsumfang von mp3blaster noch erhöhen. So gibt es Scripte für die Anbindung an den Online-Dienst last.fm oder auch Scripte für die Anzeige des Titels der gespielt wird, z. B. in weechat.

## Ein saftiges Erlebnis – Juice

Beim Programm Juice handelt es sich um eine ncurses-Oberfläche für Abspielprogramme wie z. B. mpg123. Ähnlich wie bei mp3blaster installiert man beide Programme über den Paketmanager seiner Distribution.

Wer Juice aus einem Terminalemulator wie z. B. xterm aufruft, sollte sicherstellen, dass das Fenster mindestens 80×25 Pixel groß ist. Sollte dies nicht der Fall sein, quittiert Juice seinen Dienst mit einer Fehlermeldung.



Das Setup-Menü von JUICE

## Das Setup-Menü von JUICE

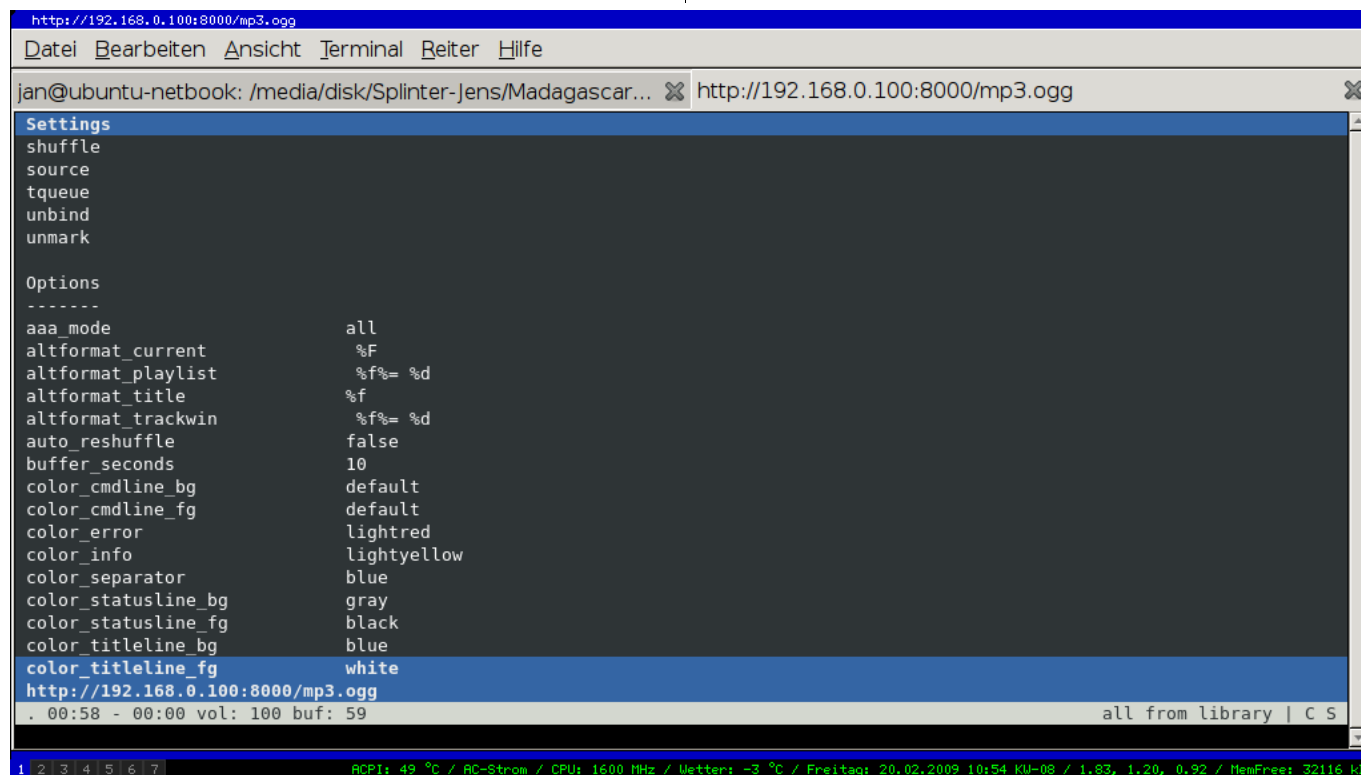
Nachdem man das Programm gestartet hat, findet man sich auf einer ziemlich leeren blauen Oberfläche wieder. Am unterem Rand des Programms sind vier »Schaltflächen« die man per [TAB]-Taste erreicht. Weiter unten sind die Funktionen der verfügbaren Funktionstasten ersichtlich. Beim ersten Start sollte man mittels [F3] das Setup besuchen. Dort kann man u. a. festlegen, in welchem Verzeichnis standardmäßig nach Musikdateien gesucht werden soll. Auch Angaben zur späteren

Anzeige der ID3-Daten kann man hier festlegen. Nach erfolgreichem Setup sollte man die Einstellungen speichern.

Die Bedienung ist weitgehend selbsterklärend. Beendet man sich in einem Verzeichnis, aus welchem man gern seine Musik zur Playlist hinzufügen möchte, geht man per [TAB]-Taste zum Befehl *ADD*, um einzelne Dateien zu übertragen oder zu *ADD all*, um alle vorhandenen Dateien in die Playlist zu überstellen.

Hat man auf diese Weise seine persönliche Playlist zusammengestellt, so kann man diese natürlich speichern, um sie beim nächsten Mal problemlos wieder laden zu können. Leider unterstützen weder Juice noch mpg123 den Import von M3U- oder PLS-Playlisten, obwohl man im Setup den Typ der zu speichernden Playlisten angeben kann.

Ob diese Unterstützung in folgenden Versionen von Juice erfolgen wird, bleibt unklar, da der Programmierer leider nicht mehr unter der auf der Homepage angegebenen E-Mail erreichbar ist.



```
http://192.168.0.100:8000/mp3.ogg
Datei Bearbeiten Ansicht Terminal Reiter Hilfe
jan@ubuntu-netbook: /media/disk/Splinter-Jens/Madagascar... http://192.168.0.100:8000/mp3.ogg
Settings
shuffle
source
tqueue
unbind
unmark

Options
-----
aaa_mode          all
altformat_current %F
altformat_playlist %f% = %d
altformat_title   %f
altformat_trackwin %f% = %d
auto_resuffle     false
buffer_seconds    10
color_cmdline_bg  default
color_cmdline_fg  default
color_error       lightred
color_info        lightyellow
color_separator   blue
color_statusline_bg gray
color_statusline_fg black
color_titleline_bg blue
color_titleline_fg white
http://192.168.0.100:8000/mp3.ogg
. 00:58 - 00:00 vol: 100 buf: 59
all from library | C S
1 2 3 4 5 6 7
ACPI: 49 °C / AC-Strom / CPU: 1600 MHz / Wetter: -3 °C / Freitag: 20.02.2009 10:54 KW-08 / 1.03, 1.20, 0.92 / MemFree: 32116 kB
```

*Konfigurationseinstellungen von cmus*

## Leichtgewicht cmus

cmus gehört wohl zu den bekanntesten Musikwiedergabeprogrammen auf der Konsole. Das mag daran liegen, dass der Player nicht nur unter Linux, sondern auch unter anderen UNIX-artigen Betriebssystemen läuft. Zum anderen kann es auch daran liegen, dass man, je nach Plugin, von AAC bis WV (WavePack) alles wiedergeben kann, was an Formaten für Musik existiert.

Bevor man sich cmus über seinen Paketmanager herunterlädt und installiert, sollte man sich kurz Gedanken machen, welche Formate man abspielen und über welchen Soundserver man später seine Musik hören möchte. Die entsprechenden Bibliotheken sollte man im Vorfeld installieren wie z. B. vorbis für die Wiedergabe von OGG Musikdateien.

Unter den meisten Distributionen sind die Unterstützungen für die gängigen Musikformate bereits

enthalten. Einzig MP3 muss man vereinzelt nachinstallieren. Um nun cmus zu installieren, markiert man das Programm einfach in seinem Paketmanager.

Nach erfolgreicher Installation schaut man am besten mit dem Befehl:

```
cmus --plugins
```

nach, welche Formatunterstützung aktiviert ist.

Die Oberfläche des Programms gliedert sich in zwei Hälften. Die linke kümmert sich um die Darstellung des Dateisystems und die rechte um die Anzeige der Playlist.

### Konfigurationseinstellungen von cmus

Zu bedienen ist cmus über sogenannte Keybindings, also vorgegebene Tastaturkürzel. Stellenweise kann man die Befehle auch eingeben. Der Stil ähnelt dabei dem von vi(m). Die benutzbaren Befehle und Tastaturbefehle zeigt ein Blick in die man-Page von cmus, oder man drückt im laufenden Betrieb die Zifferntaste [7].

Den Reiz und die Bekanntheit von cmus verdankt das Programm nicht zuletzt den umfangreichen Konfigurationsmöglichkeiten. Hat man die Zifferntaste [7] gedrückt, offenbart sich einem nicht nur eine Liste über die Tastaturkürzel und Eingabebefehle, sondern auch noch Angaben zu Hintergrundfarbe, Darstellungsoptionen, verwendeter

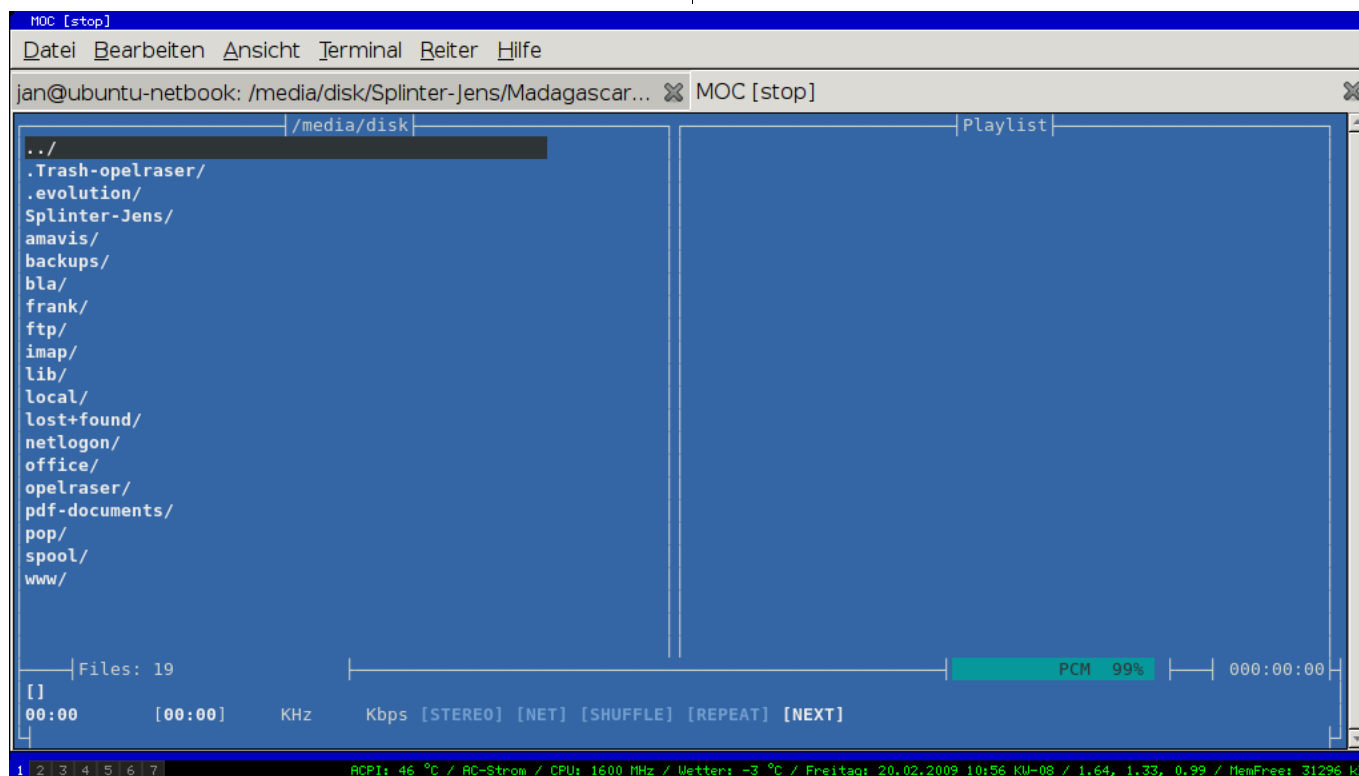
Soundserver etc. Möchte man etwas ändern, wählt man per Pfeiltasten den jeweiligen Eintrag an und drückt [Enter] und ändert die Standardangabe entsprechend seinen Bedürfnissen ab. Beim Beenden merkt sich cmus die Einstellungen.

### Music On Console – Der Player moc

Ein weiterer sehr bekannter Player ist der moc, wobei es sich bei der Bezeichnung mehr um eine Beschreibung handelt. Das Ziel ist einfach: Wiedergabe von Musik auf der Konsole verpackt in eine ncurses-Oberfläche.

Wer sich moc über seinen Paketmanager installiert, wird sich wundern, dass der anschließende Aufruf von moc am Prompt eine Fehlermeldung produziert. Da es sich bei dem Programmnamen mehr um eine Bezeichnung handelt, wurde dem Player der Mame mocp gegeben, wobei das »p« für »Player« steht. Gibt man diesen Befehl ein, findet man sich in einer (gewohnten) ncurses Oberfläche wieder.

Linker Hand ist der Dateibrowser und rechts die Playlistverwaltung zu finden. Unten noch eine



Die Oberfläche von moc(p)

Lautstärkeanzeige und einige Statusinformationen. Soweit, so gut, aber genauso bekannt. Die Stärke von moc liegt auch hier in seiner vielfältigen Konfigurationsmöglichkeit. Diesmal aber wieder über eine ausgelagerte config-Datei.

Diese sollte man sich aus dem Verzeichnis `/usr/share/doc/moc (config.example.gz)` in sein Home-Verzeichnis kopieren. Wenn man vorhat, auch vorhandene Tastaturkürzel zu ändern, kopiert man zusätzlich noch die Datei `keymaps.example`. Beide kann man nun nach Herzenslust bearbeiten und beim nächsten Aufruf von mocp angeben, um seine Einstellungen zu aktivieren.

Zu den großen Stärken von moc zählen auch das schnelle Verzeichniswechseln (*Fastdir*) und die Möglichkeit, eigene Befehle (*execCommand*) anzulegen. Weiterhin bietet das Programm die Option, beim Verlassen der ncurses-Oberfläche weiterhin Musik zu spielen oder auch mocp gleich ohne Oberfläche und nur mit der Angabe einer Playlist starten zu lassen. Über Tastatureingaben wie z. B.

```
mocp -f
```

für »nächster Titel« lässt sich das Programm sozusagen fernsteuern. Aufgrund seiner Popularität hat sich eine große Community um moc gebildet. Somit stehen für verschiedene Aufgaben auch entsprechende Skripts [6] zu Verfügung, die den Funktionsumfang sinnvoll erweitern.

Wer nun denkt, dass sich die Medienwiedergabe auf der Konsole nur auf Musik beschränkt, dass sogar die Ausgabe von Videosignalen möglich ist.

### Videowiedergabe auf der Konsole

Obgleich es für Musikwiedergabe einen reichhaltigen Fundus an Programmen gibt, ist bei der Videowiedergabe die Auswahl eher beschränkt. Aber die Programme, die zur Auswahl stehen, sind wohl die bekanntesten und umfangreichsten Player unter Linux – der mplayer und vlc.

Damit beide in der Konsole bewegte Bilder abspielen können, braucht es den Framebuffer.

Der Framebuffer ist eine Option des Kernels, mit der Grafikkarte auch ohne spezielle Treiber zu kommunizieren. Der Kernel benutzt dazu den VESA-Standard [7] und stellt zur Benutzung u.a. die Schnittstelle `/dev/fb0` zur Verfügung.

Bei aktuellen Distributionen ist meist der Kernel mit Framebuffer-Option aktiviert. Kompiliert man seinen Kernel selbst oder ist die Option deaktiviert, so sollte man die Framebuffer Unterstützung aktivieren, bevor man den Kernel mit *make* übersetzt. Wer sich nicht sicher ist, der kann das Ganze wie folgt überprüfen:

```
less /boot/config-`uname -r` | grep → CONFIG_FRAMEBUFFER_CONSOLE
```

Ist der Framebuffer bereits aktiviert, steht hinter dem Parameter `CONFIG_FRAMEBUFFER_CONSOLE` ein »m«. Dieses »m« steht für Modul und wird bei Bedarf in den Kernel eingebunden. Damit ist die halbe Arbeit schon getan.

Um den Framebuffer zu aktivieren gibt es zwei Wege. Weg eins ist ein direktes Editieren der Datei `menu.lst` unterhalb von `/boot/grub`. Dort trägt man bei seinem Kernel die Option `vga=0xXXX` ein. Weg zwei ist die temporäre Lösung. Startet man sein System, kann man in der GRUB-Auswahl per Taste [E] in den Editormodus schalten. Nun kann man die Option `vga=0xXXX` direkt in die Kerneloptionen eintragen und startet den Kernel dann mit der Taste [B]. Nun hat man den Framebuffer bis zum nächsten Reboot.

Wie bereits vermutet, gibt man nicht wirklich XXX ein, sondern einen Zahlencode. Dieser Zahlencode variiert je nach verwendeter Auflösung (s. Tabelle).

Auflösung	640 × 480	800 × 600	1024 × 768	1280 × 1024
256	0x301	0x303	0x305	0x307
32k	0x310	0x313	0x316	0x319
64k	0x311	0x314	0x317	0x31A
16M	0x312	0x315	0x318	0x31B

Zahlencodes für die VGA-Option im Kernel



Nicht immer unterstützt der Framebuffer die volle Auflösung des Monitors. In diesem Falle bietet der Kernel beim Booten eine Übersicht der verwendbaren Modi an. Auch ein 640×480 reicht für die Videoausgabe auf der Konsole völlig aus.

Nachdem man nun den Framebuffer aktiviert hat, möchte man natürlich auch damit arbeiten und endlich seine Filme/Videos anschauen.

Verwendet man den mplayer, so muss man das Programm nun mit dem Parameter `-vo fbdev` aufrufen. Doch Achtung, auf das Device `/dev/fb0` darf im Normalfall nur ein Benutzer mit Root-Rechten zugreifen. Jetzt sollte mplayer das Video oder den Film brav mit Bild wiedergeben. Optionale Parameter beim Programmaufruf können auch `-fs` für Vollbild und `-vf scale` für eine neue Skalierung der Videoausgabe sein. Wobei `-vf scale` dafür sorgt, dass die Videoausgabe mittig auf dem Bildschirm platziert wird. Meist macht das der MPlayer aber auch von sich aus.

Entscheidet man sich für vlc zur Wiedergabe von bewegten Bildern, so ruft man das Programm wie folgt auf:

```
cvlc /dev/fb0 <datei>
```

Das »c« vor vlc steht für *console* und ruft vlc ohne Oberfläche auf. Nun sollte auch vlc bewegte Bilder zeigen.

Die Möglichkeiten des Framebuffer sind mit der Wiedergabe von Videos aber nicht erschöpft. Wer gern seine Bilder auf der Konsole betrachten möchte, der greift zum Programm *fb*. Nennt man einen DVB-T Stick oder eine PCI Karte sein eigen, schaut man einfach TV auf der Konsole im Framebuffer. Laut der Internetseite *directfb* [8] ist es auch möglich, Anwendungen wie GIMP oder Firefox über den Framebuffer laufen zu lassen.

### Fazit

Um Musik zu genießen, gibt es auch in der Konsole genug Programme. Egal ob man es einfach (mp3blaster) oder etwas individueller (cmus, mocp) mag, für jeden ist etwas dabei. Und funktioniert der X-Server mal nicht, auf der Konsole läuft immer Musik. Durch den Framebuffer gibt es auch eine Möglichkeit, seine Bilder und Videos anzuschauen. Und das ist alles keine Hexerei, auch braucht man sich keine kilometerlangen Parameter zu merken oder endlos kryptische Angaben in Konfigurations-Dateien zu machen. Da fragt man sich manchmal, warum man den X-Server überhaupt anwerfen soll. Wer noch mehr über die Arbeit in der Konsole erfahren möchte, der sei auf die Artikelreihe »Arbeiten in der Konsole« verwiesen. Hier werden u.a. auch Themen wie E-Mail oder Kommunikation via IRC und Co. behandelt.

Jan Radecker

[cyclame@yalmagazine.org](mailto:cyclame@yalmagazine.org)

### Informationen

- [1] Amarok Homepage: <http://amarok.kde.org/>
- [2] Ncurses in Wikipedia: <http://de.wikipedia.org/wiki/Ncurses>
- [3] Midnight Commander Projektseite: <http://www.midnight-commander.org/>
- [4] Kommandozeile in Wikipedia: <http://de.wikipedia.org/wiki/Kommandozeile>
- [5] Ogg Vorbis Projekt Seite: <http://www.vorbis.com/>
- [6] MOC Skripte: <http://moc.daper.net/contrib>
- [7] Vesa im Linux Kernel: <http://lxr.linux.no/linux/Documentation/fb/vesafb.txt>
- [8] Directfb Projekt Seite: <http://www.directfb.org/>

## Ubuntu 9.04

Jedes Jahr gibt Canonical zum 23. April eine neue Ausgabe der Linux-Distribution Ubuntu heraus, deren Schwerpunkt auf Neuheit und Einsteigerfreundlichkeit liegt. Auch diesmal führt die gewollte Reise in Richtung Fortschritt.

Trotz der Tatsache, dass Linux im Bereich der Desktop-PCs einen optimistisch geschätzten Marktanteil von 1,2 % besitzt, kommt in knapp zwei Monaten also wieder eine neue Version der statistisch beliebtesten Linux-Distribution heraus. Nachdem bereits die Installationsroutine der ersten Alphas bei vielen Testern fehl schlug, ist »Jaunty Jackalope« ab der Alpha 4 ohne Schwierigkeiten sogar mit dem neuen Ext4-Dateisystem installierbar. Die einschlägigen Programmversionen sind teils neu, teils alt. Zuerst das Neue:

- Kernel 2.6.28
- OpenOffice 3.0.1
- GTK 2.15.3
- Gnome 2.25.90

Zudem kommen aber auch Programme, die es aktueller gibt:

- Pidgin 2.5.3
- GIMP 2.6.3

Im Instant-Messaging Bereich hat sich Empathy, wider einiger Unkenrufe, bei 8.10 nicht gegen den bewährten Pidgin durchgesetzt. Mit Notify-OSD gibt es einen neuen Weg zur Benachrichtigung. Nachrichten können darüber z. B. aus Pidgin direkt

auf den Bildschirm befördert werden und nach einer kurzen Anzeige automatisch verschwinden. Ebenso verhält es sich mit einem kritischen Akkustand und anderem. Eine ausführliche Beschreibung dessen, gibt es auf dem Blog von Mark



*Notify-OSD auf dem Desktop von Mark Shuttleworth*

Shuttleworth [1] (dem südafrikanischen Gründer des Ubuntu-Unternehmens, welcher schon als Astronaut unterwegs war). Der Bootvorgang ist trotz der gepriesenen Ankündigungen, ebenso wie das Dateisystem, nur unmerklich schneller geworden. Bei Letzterem kann es allenfalls bei massiven Datenmengen zum Aha-Effekt kommen. Im Serverbereich macht es auch mehr Sinn, denn da bietet Ext4 großzügigere Verwaltungskapazitäten

(einen Vergleich mit Benchmarks gibt es bei Pro-Linux [2]). Zudem wird bei »Jaunty Jackalope« das Versionsverwaltungssystem Bazaar [3] und die Infrastruktur für die Entwicklergemeinschaft weiter ausgebaut.

Auf Notebooks sollte Ext4 bis zum Kernel 2.6.30 (derzeit aktueller Kernel ist die Version 2.6.28) möglichst nicht als Dateisystem benutzt werden, da es bei Abstürzen mehr Datenverlust verursachen kann als der Vorgänger. Das Absturzrisiko ist insbesondere bei kritischen Akkuständen gegeben. Auf Desktoprechnern treten solche Totalabstürze wegen dem Netzstrom seltener auf, wodurch man im Hinblick auf die Vorteile und das vergleichsweise kleine Risiko jenen Makel in Kauf nehmen kann. Hintergrund ist die Verzögerung beim Schreiben auf die Festplatte, wodurch nach einem Absturz Daten verloren gehen können, die zu diesem Zeitpunkt in Bearbeitung waren. Effektiv bedeutet dies, dass Daten, die eine Anwendung speichert, bei Ext4 tatsächlich erst einige Sekunden nach dem Benutzerbefehl (bis zu 60 Sekunden) auf den Datenträger geschrieben werden und solange nur im Arbeitsspeicher vorliegen. Dies ist auf Entwicklungen im Bereich der Energieeinsparung zurückzuführen, die noch Fehler mit sich bringen [4].

Mark Shuttleworth kündigte an, dass das bewährte Ext3-Dateisystem bis zu Ubuntu 9.10 Standard bleibt. Fedora 10, welche insbesondere in den USA beliebt ist und auch sonst (als Puffer von möglichen Innovationen für das kommerzielle Redhat-Linux) Neuerungen früher als andere Distributionen übernimmt, setzt jetzt schon standardmäßig



### Desktop in Jaunty Alpha

auf Ext4. Nächste Veränderungen des Oberflächendesigns sollen bei Ubuntu 9.10 kommen.

Interessant sind zudem die Bugfixes. Viele Alpha-Tester beklagen sich über die fehlerhafte Unterstützung der proprietären Treiber von GeForce- sowie ATI-Grafikkarten. Seit dem 14. Februar konzentriert sich das Entwicklerteam ausschließlich auf das Schließen von Fehlern und bringt keine weiteren Neuerungen in den »lebhaften Wolpertinger« (eine der umstrittenen deutschen Überset-

zungen von »Jaunty Jackalope«). Sicherlich wird 9.04 aber weiterhin altbackene Bugs enthalten, die im Ubuntu Launchpad [5] von den Entwicklern mit niedriger Priorität eingestuft wurden. So gibt es in Ubuntu 8.10 zum Beispiel den GTK-Bug, in dessen Zuge Dialogfenster im Zusammenspiel mit Compiz in minimaler Größe angezeigt werden, bereits seit Ubuntu 6.06 [6]. Wer will, kann sich Näheres über die Veröffentlichungszeiten der Vorversionen beim Jaunty Release Schedule [7] ansehen.

### Fazit

Wer weniger Wert auf neuste Software, jedoch mehr Wert auf längerfristig erprobte Fehlerfreiheit legt, sollte sich Debian Lenny [8] ansehen. Von der Neuheit der Software liegt diese zwar etwa ein Jahr zurück, ist hingegen ebenfalls ein Universalbetriebssystem und bezüglich Stabilität seit jeher bekannt. Zudem geht Ubuntu daraus hervor und bietet seit der vor kurzem erschienenen stabilen Version auch eine durchdachte und einsteigerfreundliche grafische Oberfläche. Für Abenteuerlustige mit einem gewissen Zeitfenster, Geduld und dem Wunsch nach Neuem, aber nicht zwingend Besserem, ist die neue Version von Ubuntu mit Sicherheit eine runde Sache.

Peter Majmesku

pe@yalmagazine.org

### Informationen

- [1] Mark Shuttleworth beschreibt Notify OSD: <http://www.markshuttleworth.com/archives/265>
- [2] Ext4 im Vergleich: <http://www.pro-linux.de/berichte/ext4/ext4.html>
- [3] Offizielle Homepage von Bazaar: <http://bazaar-vcs.org/>
- [4] Blogartikel »Ext4: So jung und schon vergesslich«: <http://www.menzer.net/de/content/20090311-ext4-so-jung-und-schon-vergesslich>
- [5] Ubuntu Launchpad: <https://launchpad.net/ubuntu>
- [6] GTK+ Darstellungs Bug: <https://bugs.launchpad.net/ubuntu/+source/gtk+2.0/+bug/75324>
- [7] Jaunty Release Schedule: <https://wiki.ubuntu.com/JauntyReleaseSchedule>
- [8] Debian Homepage: <http://www.debian.org>



# Pidgin – Nachrichtenverschlüsselung mit OTR

**Verschlüsselung für deine Gespräche, einfach und schnell. Wir erklären, wie man Pidgin abhörsicher macht.**

Für den heutigen User ist die Kommunikation durch einen Instant Messenger wohl die meistgenutzte Kommunikation über Internet. Da man auf diese Art die meisten Informationen über sich preisgibt, sollte man sich eventuell Gedanken darüber machen, diese zu verschlüsseln.

## Warum sollte man verschlüsseln?

Erstaunlicherweise ist nicht nur die Privatsphäre ein Argument für die Verschlüsselung, sondern auch die dreisten Konditionen der meisten populären Anbieter. Werfen wir hierzu einen Blick auf einige der weitestverbreiteten Messenger und ihre AGBs:

### AIM

»AIM or AOL may use your AIM information to present offers to you on behalf of business partners and advertisers. ... Your AIM information, including the contents of your online communications, may be accessed and disclosed in response to legal process (for example, a court order, search warrant or subpoena), or in other circumstances in which AOL has a good faith belief that AIM or AOL are being used for unlawful purposes. AOL may also access or disclose your AIM information when necessary to protect the rights or

property of AIM or AOL, or in special cases such as a threat to your safety or that of others.« [1]

AIM verwendet also nicht nur eure Informationen, um sie an Partner und Werbeagenturen weiterzuverkaufen, die euch dann personalisierte Werbung schicken, sondern gibt auch freizügig eure Kommunikationsdaten im Falle eines Prozesses heraus.

### ICQ

»You agree that by posting any material or information anywhere on the ICQ Services and Information you surrender your copyright and any other proprietary right in the posted material or information. You further agree that ICQ LLC. is entitled to use at its own discretion any of the posted material or information in any manner it deems fit, including, but not limited to, publishing the material or distributing it.« [2]

Das bedeutet, dass alles, was ihr über ICQ verschickt oder postet, nun ICQ gehört und sie damit machen kön-

nen, was sie wollen. Verschickt ihr eigene Bilder oder die Musik eurer Band über ICQ, tretet ihr somit sämtliche Urheberrechte ab. ICQ behält sich sogar das Recht vor, das Material zu verkaufen!

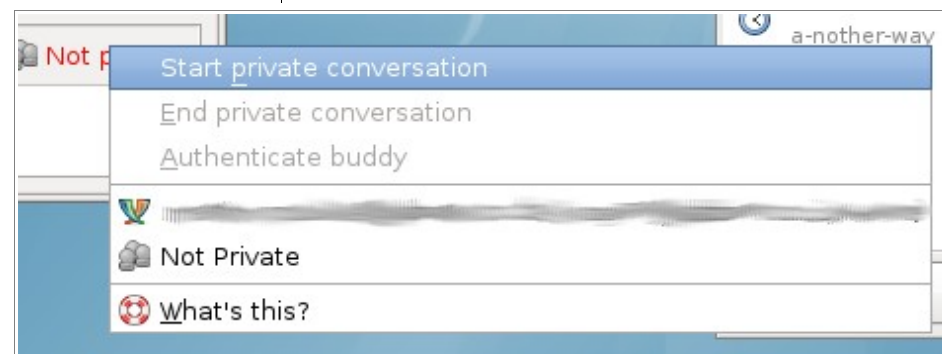
Doch ICQ lizenziert nicht nur euren Datenverkehr, sondern auch eure hinaufgeladenen Avatare. Das zeigt ein Fall, indem sich ICQ geweigert hat, Avatare eines Nutzers zu löschen, da dieser nun Eigentum von ICQ sei [3].

## Verschlüsseln mit OTR

Für Pidgin kann man das OTR-Plugin (Off-The-Record Messaging) bequem über den Paketmanager nachrüsten. Das Paket nennt sich auf den meisten Systemen:

pidgin-otr

Wer Pidgin auf Windows verwendet, muss das Paket dazu manuell herunterladen und installieren [4].



Starten einer verschlüsselten Sitzung



Ist das Plugin installiert, muss man dieses mit einem Haken bei *Off-The-Record Messaging* unter *Werkzeuge – Plugins* aktivieren. Von nun an sehen wir über unserem Nachrichtenfenster einen Button mit der Aufschrift *Not private*. Dies mag bei

anderen Versionen variieren: bei manchen Versionen finden man den Button rechts vom Eingabefeld und gelangt in dessen Menü mit einem Rechtsklick.

Hat nun auch euer Gegenüber ein OTR-Plugin installiert, könnt ihr die Kommunikation über das Menü des Buttons verschlüsseln.

Wird das Plugin zum ersten Mal gestartet, muss dieser erst ein Schlüsselpaar generieren, da OTR wie PGP auf asymmetrische Verschlüsselung aufbaut. Hier sollte man geduldig das Ende abwarten, da die Prozedur auf schwächeren Systemen einige Minuten in Anspruch nehmen kann. Von nun an kann man jederzeit auf Knopfdruck mit seinem Gegenüber schnell eine verschlüsselte Kommunikation starten.

### Verifizieren des Gegenübers

Um sich sicher sein zu können, dass der Kommunikationspartner auch der ist, für den man ihn hält, kann man seinen öffentlichen Schlüssel noch verifizieren. Dazu ruft man im Menü den Punkt *Authenticate buddy* auf, wo die Art der Verifikation eingestellt werden kann. Am einfachsten und schnellsten geht dies über die manuelle Verifikation des Fingerabdrucks.

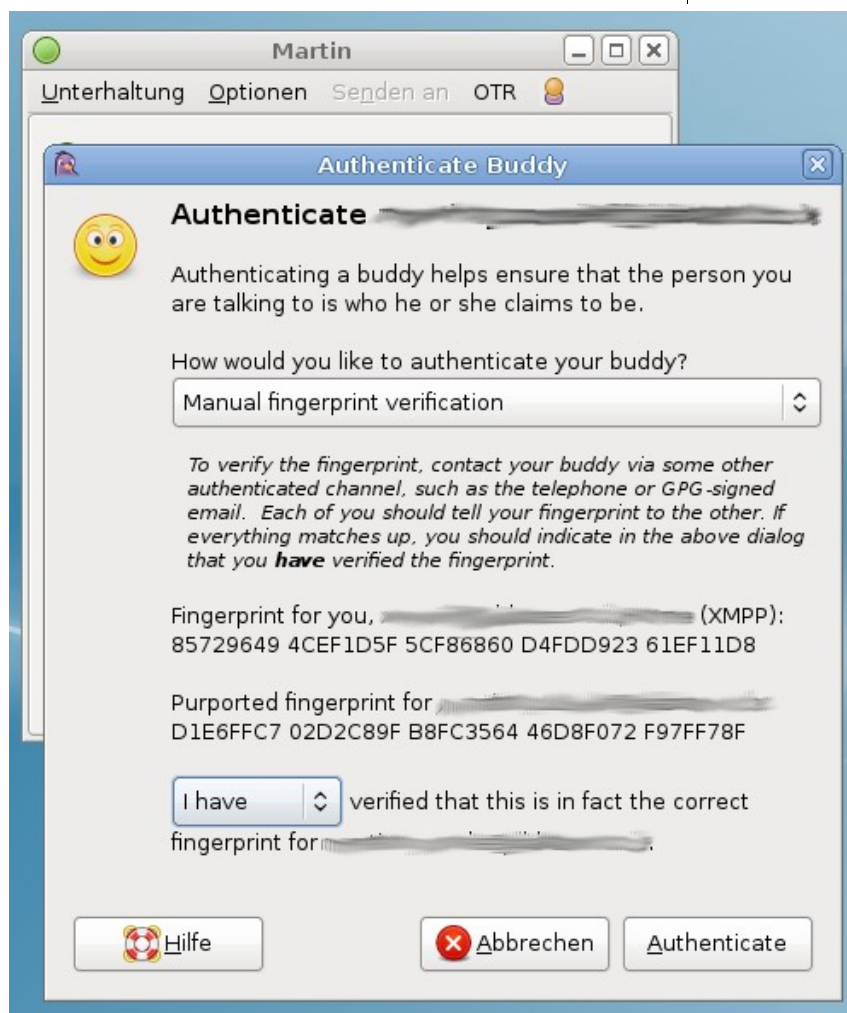
### Fazit

Besonders die schnelle und einfache Möglichkeit, seine Kommunikation zu verschlüsseln, dürfte ein schlagendes Argument für die Verbindung von Pidgin und OTR sein. Da Pidgin sowohl unter Windows [5] als auch unter Mac OS [6] verwendet werden kann, kann man sicher einen Großteil seiner Kollegen zum Verschlüsseln überreden.

Bernhard Posselt  
ray@yalmagazine.org

### Informationen

- [1] AIM Privatsphäre: [http://www.aim.com/tos/privacy\\_policy.adp?aolp=0](http://www.aim.com/tos/privacy_policy.adp?aolp=0)
- [2] ICQ AGB: <http://www.icq.com/legal/policy.html>
- [3] ICQ-Nutzer kann seinen Avatar nicht löschen: <http://iq.lycos.de/qa/show/1139062/Darf-ICQ-das-rechtlich-machen/>
- [4] OTR für Windows: <http://www.cypherpunks.ca/otr/index.php#downloads>
- [5] Pidgin für Windows: <http://pidgin.im/download/windows/>
- [6] Pidgin Alternative Adium für Mac OS X: <http://www.adiumx.com/>



Die einfachste und schnellste Methode: Manuelle Verifizierung des Fingerabdruckes

# OpenTTD – Das Urgestein der Wirtschaftssimulationen auf dem Linuxsystem

Einige unserer Leser werden sich vielleicht noch an das Urgestein unter den Wirtschaftssimulationen erinnern können. Transport Tycoon Deluxe war Mitte der 90iger das erste von vielen Tycoon-Spielen, in dem der Spieler seine eigene Transportfirma gründet und mit Bussen, LKWs, Zügen, Schiffen und Flugzeugen sein Geld verdienen muss.

Gefolgt von vielen anderen Wirtschaftssimulationen, wie z. B. »Transport Gigant« oder »Railroad Tycoon«, machte Transport Tycoon sich auf vielen Windowsrechnern breit und sorgte für lang anhaltenden Spielspaß. Das OpenSource-Projekt »OpenTTD« macht es möglich, Transport Tycoon als Klon auf dem Linuxrechner zu spielen. Yalm zeigt, wie man den Klassiker auf Linux zum Laufen bekommt.

## Die Installation

OpenTTD lässt sich über die Paketverwaltung installieren. Dazu einfach, z. B. bei Ubuntu, in die Synaptic-Paketverwaltung gehen und über die Suchfunktion das Paket »openttd« suchen und zum Installieren markieren. Anschließend findet man OpenTTD unter *Anwendungen – Spiele*.

Wichtig: Um OpenTTD spielen zu können, benötigt man die Grafikdateien vom Originalspiel.

Diese lassen sich bei *Transport Tycoon Main Station* [1], einer deutschen Projektseite zum Transport Tycoon Deluxe, kostenlos herunterladen. [2]

Ist das Originalspiel heruntergeladen, entpackt man die Dateien in einen beliebigen Ordner auf



Das Menü zur Welterstellung in OpenTTD

dem System. Im nächsten Schritt werden die Spieldaten in den Datenordner von OpenTTD (*/usr/share/games/openttd/data*) kopiert. Dabei muss man alle Rechte für diesen Ordner besitzen, da es sonst nicht möglich ist, die Datei in diesen Ordner zu kopieren. In einigen Spielversionen kann es sein, dass diese Datei groß geschrieben ist (Beispiel: *SAMPLE.CAT*). In solch einem Fall muss diese Datei in *sample.cat* (Kleinschreibung) umbenannt werden, da Linux zwischen Groß- und Kleinschreibung unterscheidet.

Nun kann es mit dem Spiel losgehen!

## Das Spiel

OpenTTD kann wie im Original im Singleplayer- sowie im Mehrspielermodus gespielt werden.

Über *Neues Spiel* startet man den Singleplayermodus. Zunächst wird die Karte erstellt, auf der die Simulation gestartet werden soll.

Der Spieler hat in der Welterstellung die Option, die Art der Landschaft auszuwählen. Dabei gibt es vier Typen zur Auswahl: Eine grüne Landschaft mit Flüssen, Seen, Wäldern und Hügeln, eine Winter-, eine Wüsten- sowie eine Fantasielandschaft á la Alice im Wunderland.

Des weiteren können die Spielfeldgröße, die Anzahl der Städte, die Dichte der Industrie, das Startdatum und einige weitere Landschaftseigenschaf-



ten wie zum Beispiel der Baum-Algorithmus eingestellt werden.

Startet man das Spiel mit einem frühen Startdatum, so stehen Fahrzeuge dieser Zeit zur Verfügung. Das Startdatum 1950 beinhaltet beispielsweise Dampflok und Propellerflugzeuge. Wählt man ein frühes Startdatum, so durchläuft man alle technologischen Epochen während des Spiels. Von der Dampflok zur Magnetschwebebahn, von Propellermaschinen zu Düsenjets. Es lohnt sich also recht früh zu starten, um alle Fahrzeuge einmal durchzuspielen. Außerdem bleibt das Spiel so länger interessant.

### Die ersten Jahre sind hart

Im Spiel angekommen, sollte man sich nun erst mal in aller Ruhe die Karte ansehen um herauszufinden, wo es sich lohnt sein Geschäft zu starten. Da die Anschaffung von Transportmitteln sowie das Bauen von Straßen, Gleisen, Bahnhöfen und Flughäfen teuer und der Geldbeutel zu Beginn des Spiels eher schmal ist, sollte man sich wirklich gut überlegen, mit welchem Geschäft man anfängt, da die eigene Firma sonst ruck, zuck pleite ist. Es besteht zwar die Möglichkeit, einen Kredit aufzunehmen, jedoch wird das Kreditlimit anhand der eigenen Liquidität festgelegt und so kann diese Möglichkeit, an Geld zu kommen, auch schnell ausgeschöpft sein. Es empfiehlt sich, erst einmal klein anzufangen, wie bei vielen Dingen im Leben. Die in der Anschaffung günstigsten Fahrzeuge sind Busse und LKWs. Straßen sind in der Regel

schon viele vorhanden, jedoch müssen Städte in der Regel noch miteinander verbunden werden. Busbahnhöfe sind im Vergleich zu anderen Bahnhöfen noch erschwinglich. Sucht man sich also zwei relativ große Städte, die viele Passagiere produzieren, und verbindet diese miteinander, lässt sich mit der Hilfe von Bussen und Busbahnhöfen

das erste Geld verdienen. Wie viele Passagiere oder Waren Städte bzw. Fabriken produzieren, kann man herausfinden, indem man auf die Stadt oder Fabrik klickt. Ein Infofenster öffnet sich, in dem man das Potenzial der Stadt oder Fabrik nachlesen kann.



*OpenTTD - schon das Startmenü erinnert sehr stark an das Original Transport Tycoon*



Transportiert man Waren von Produktionsstädten zu Fabriken, bedeutet dies meist nicht nur Geld durch diese erbrachte Transportleistung, sondern es kann im Anschluss auch Geld am Transport der Waren, welche Fabriken produzieren, verdient werden. Befördert man beispielsweise Getreide und Vieh von einem Bauernhof zu einer Fabrik mit

einigen LKWs oder mit der Bahn, produziert diese Fabrik wiederum Waren, welche man mit dem LKW an einem Warenterminal in einer Stadt anliefern kann.

Während des Spiels wird man feststellen, dass sich Städte in denen man Passagiere befördert,

mit der Zeit wachsen. Dies bedeutet, dass damit auch die Passagierzahlen mit wachsen und man somit noch mehr Fahrzeuge zum Transport einsetzen kann, wodurch Bahnhöfe und Flughäfen noch profitabler werden.

### Ist der Grundstein gelegt ...

... und die eigene Transportfirma steht finanziell auf eigenen Beinen und der Anfangskredit ist zurückbezahlt, kann man nun etwas größere Investitionen in Flughäfen und Flugzeugen, Häfen und Schiffen tätigen und somit noch mehr Geld verdienen. In frühen Jahren steht ein kleiner Flughafen mit einer Start- und Landebahn zur Verfügung. Verbindet man zwei Städte mit Flughäfen bzw. Flugzeugen mit einander, wird man merken, dass die Erträge bei Flugzeugen wesentlich höher sind als bei Bussen oder Zügen. Damit verbunden ist jedoch ein höherer Anschaffungswert und auch ein gewisses Risiko, da Flugzeuge auch abstürzen können. Nach einigen Jahren Spielzeit, stehen auch größere Flughäfen mit mehreren Start- und Landebahnen zur Verfügung, welche die Abwicklung von Starts und Ladungen beschleunigen. Größere Flughäfen rentieren sich zum Beispiel bei Städten, die gewachsen sind und eine hohe Passagierzahl ausweisen.

Da in OpenTTD die Beförderung von Passagieren und Fracht nicht nur auf dem Land- oder Luftweg möglich ist, sondern auch auf dem Wasserweg, lassen sich auch Häfen bauen, um Schiffe welche Fracht oder Passagiere anliefern möchten, anle-



*Aller Anfang ist schwer, jedoch am einfachsten mit einer einfachen Buslinie wie in dieser Abbildung*



gen zu lassen. Sind zwei Städte beispielsweise durch einen Fluss oder See getrennt, ist der einfachste Weg, beide miteinander zu verbinden, einen Fährdienst einzurichten. Mit Fähren lassen sich einfach und schnell mehr Passagiere als mit dem Bus befördern und es ist nicht extra erforderlich, vorher eine Trasse zu bauen, da diese bereits durch die natürliche Umgebung vorhanden ist.

Des Weiteren lassen sich einige Güter am effektivsten mit dem Schiff befördern, wie zum Beispiel Öl. Ölquellen oder Ölbohrinseln werfen eine Menge Öl ab, für welche man große Transportkapazitäten benötigt, um diese Mengen zu befördern. Ein LKW oder ein Zug reichen da in der Regel nicht aus. Da helfen große Öltanker, mit welchen sich diese Mengen am besten befördern lassen. Zwar sind Öltanker langsam, weisen aber bei einer langen Transportstrecke einen hohen Gewinn aus.

### Warte und erweitere deine Flotte

Wie in der Realität, gehen Fahrzeuge auch kaputt und werden alt. Um zu gewährleisten, dass Bus-, Flug- oder Schifflinienverkehre nicht von Pannen dominiert werden, müssen die Verkehrsmittel mit der Zeit ausgewechselt werden. Dadurch rüstet man seine Flotte auch immer mit der neuesten und effektivsten Technik aus. Alte langsame Busse werden gegen neue schnellere, welche sogar mehr Passagiere befördern können, ausgetauscht. Mit schnelleren und größeren Fahrzeugen lässt sich automatisch auch mehr Geld verdienen. Es empfiehlt sich also, die Fahrzeuge nicht nur fahren



*Eine Großstadt mit einem internationalen Flughafen mit vier Start- und Landebahnen*

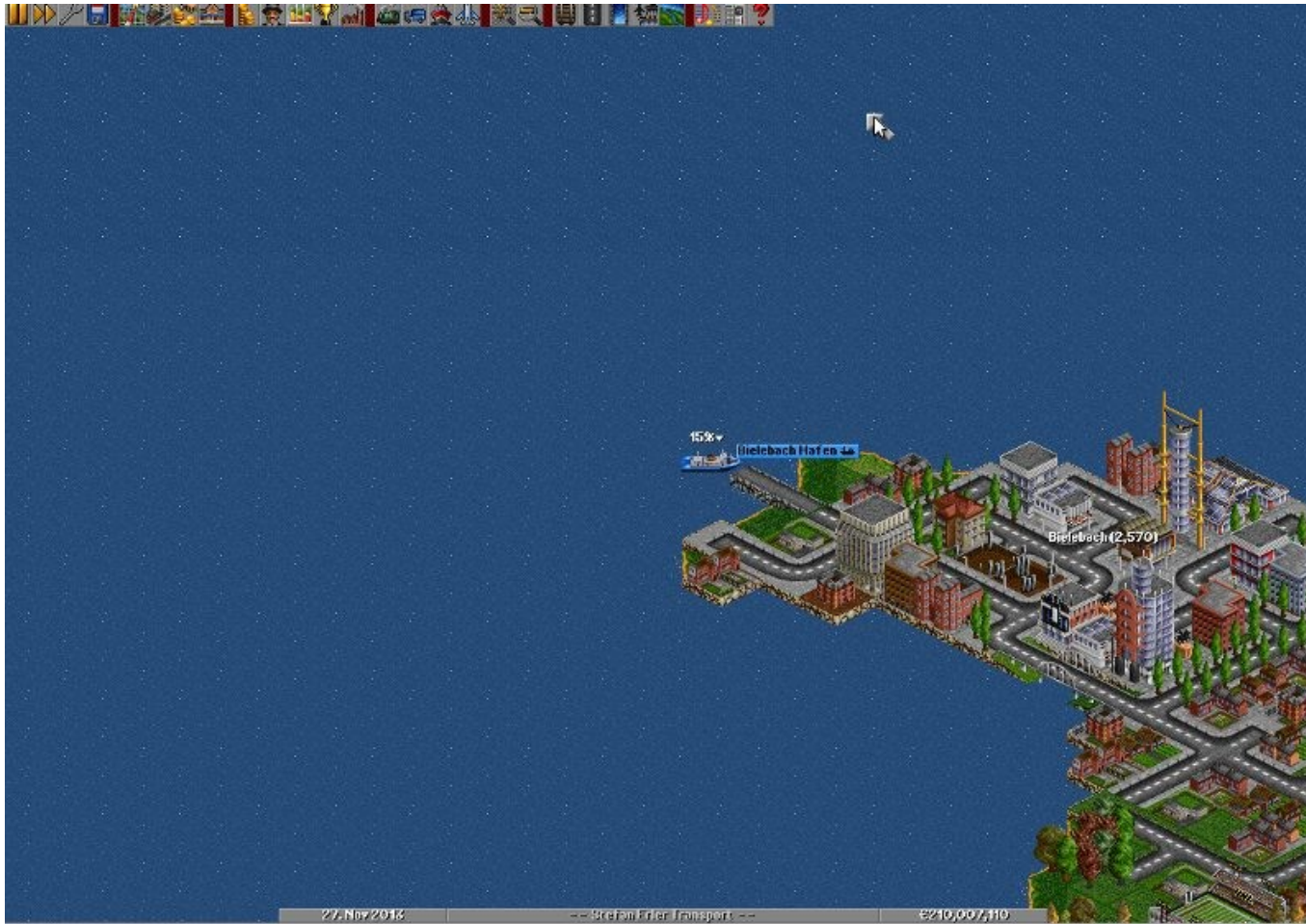
oder fliegen zu lassen, sondern diese auch öfter mal zu überprüfen, ob diese vielleicht zu alt sind und ausgetauscht werden müssen. Dies ist in der Regel nach 30 Jahren der Fall.

### Der Wettbewerb ist groß – schalte deine Mitbewerber aus

In den Einstellungen des Spieles kann man zwar die Anzahl der Mitbewerber auf null setzen, jedoch wird das Spiel ohne Mitbewerber mit der Zeit lang-

weilig. Spannend wird es erst dann, wenn man seine Gegner ausschalten kann, wobei man jedoch auch aufpassen muss, dass man nicht selber ausgeschaltet wird. Die einfachste Methode einen Mitbewerber auszuschalten wäre, diesen einfach aufzukaufen. Die etwas spannendere Methode wäre jedoch, dem Gegner das Geschäft zu vermiesen, indem man einfach eigene Bahnhöfe oder Flughäfen neben denen des Gegners baut oder die exklusiven Transportrechte von Städten kauft, in denen





*Eine Fähre macht im Hafen fest*

der Mitbewerber Bahnhöfe oder Flughäfen betreibt. So wäre der Gegner gezwungen, seine Aktivitäten in diesen Städten einzustellen und die eigenen Gebäude abzureißen, der er damit keine Möglichkeit mehr hat, Geld zu verdienen.

### Fazit

Die Grafik und der Sound von OpenTTD sind veraltet. Für Spieler, die besonderen Wert auf diese beiden Eigenschaften legen, ist OpenTTD sicherlich nichts. Jedoch merkt man bei OpenTTD nicht, wie schnell die Zeit vergeht, und wer Wirtschaftssi-

mulationen mag, für den ist dieses Spiel sicherlich der richtige Zeitvertreib. Da OpenTTD grafisch nicht besonders aufwändig ist, läuft dieses Spiel auch auf älterer Hardware und Netbooks. Auf der Projektseite von OpenTTD [2] erhält man Hilfe sowie Karten und Erweiterungen zum Download.

Stefan Erler

[der-captain@yalmagazine.org](mailto:der-captain@yalmagazine.org)

### Informationen

- [1] TTD-Homepage: <http://www.tt-ms.de>
- [2] Direktdownload-Link von TTD: <http://www.tt-ms.de/downloads/ttdos201119.rar>
- [3] Projektseite von OpenTTD: <http://www.openttd.org>

# Verschlüsseln und Signieren von E-Mails mit Seahorse und Evolution

Wenn es ums Signieren und Verschlüsseln von E-Mails geht, bilden die beiden Gnome-Standardprogramme Evolution und Seahorse ein effizientes und komfortables Paar. Wir haben uns die Funktionsweise genauer angeschaut und erklären die Nutzung.

Wenn es ums Signieren und Verschlüsseln von E-Mails geht, bilden die beiden Gnome-Standardprogramme Evolution und Seahorse ein effizientes und komfortables Paar. Wir haben uns die Funktionsweise genauer angeschaut und erklären die Nutzung.

In Zeiten medialer und staatlicher Überwachung wird es immer wichtiger, durch Verschlüsselung der Kommunikation seine Privatsphäre zu wahren. Um dieses Ziel zu erreichen, ist sowohl die Verschlüsselung des Instant Messengers mit OTR [1], als auch die Verschlüsselung des E-Mail-Verkehrs mit PGP (Pretty Good Privacy), wichtig. Beide Methoden setzen auf asymmetrische Verschlüsselung.

## PGP

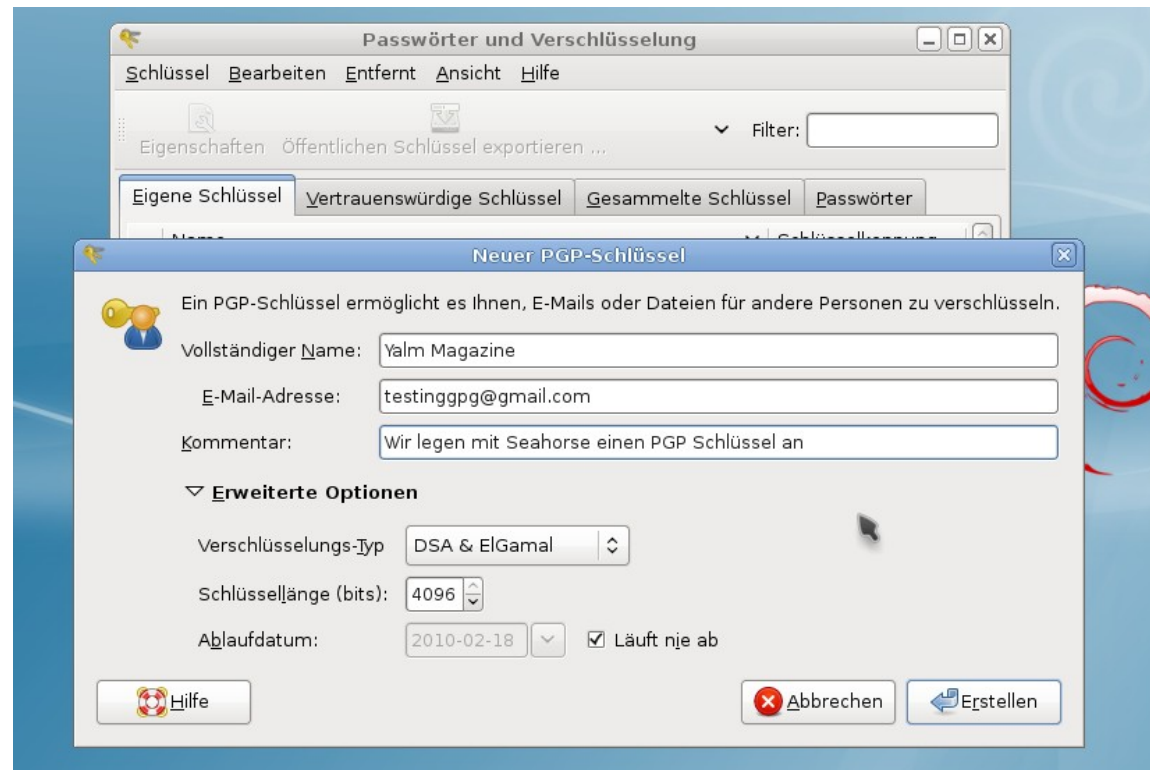
Folgendes Beispiel soll die Funktionsweise der asymmetrischen Verschlüsselung besser veranschaulichen:

Stell dir vor, du und dein Freund haben zwei Schatzkisten und diese wollt ihr hin und her schicken.

## Symmetrische Verschlüsselung

Ihr habt beide den gleichen Schlüssel und die gleiche Kette, mit der ihr die Kisten verschließt. Der Sender schließt die Kiste mit seiner Kette ab und der Empfänger öffnet sie mit seinem Schlüssel. Solange nur ihr zwei eure Kisten untereinander austauscht, funktioniert diese Art der Verschlüsselung hervorragend.

Stell dir jedoch vor es kommt ein Dritter dazu, dem du eine abgeschlossene Kiste schickst. Damit dieser deine Kiste öffnen kann, braucht er exakt den gleichen Schlüssel wie du und dein Freund ihn be-



Anlegen eines PGP Schlüsselpaares

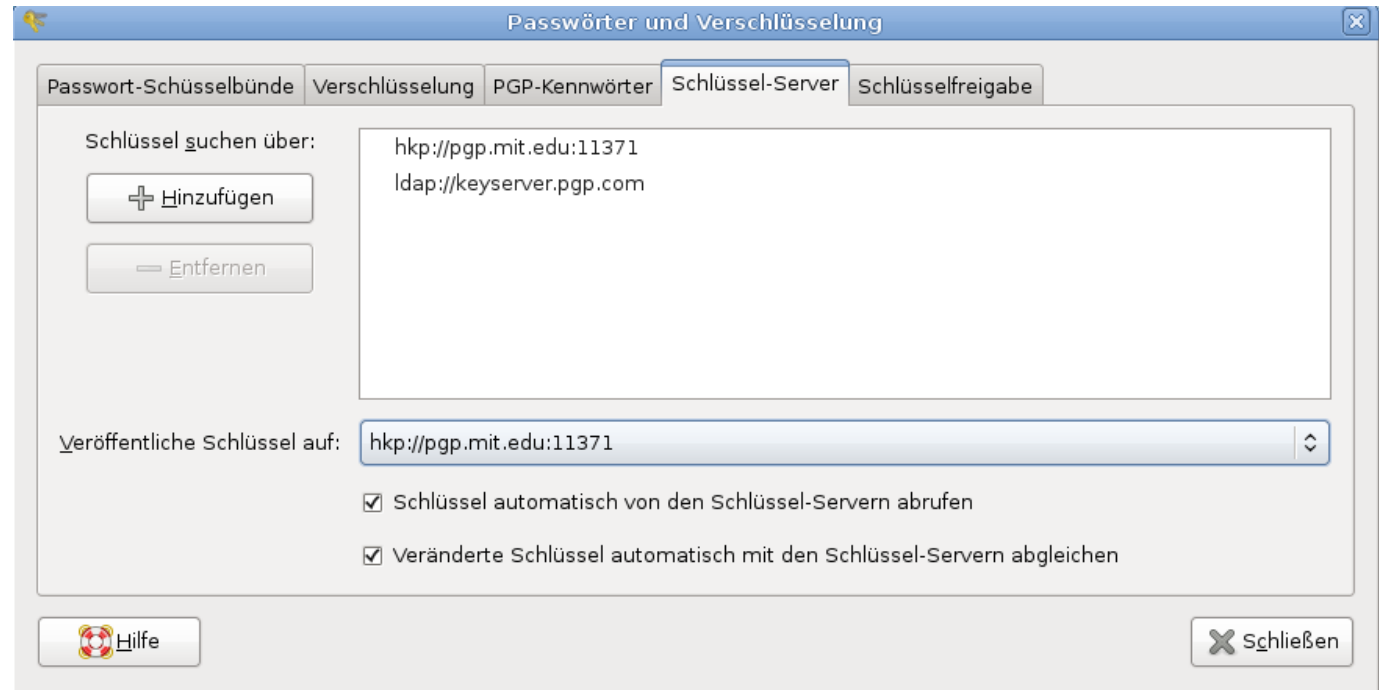
sitzen. Das hat zur Folge, dass er nun auch in der Lage wäre, alle Kisten zu öffnen, die du deinem Freund schickst. Somit muss nur jemand euer »Web-Of-Trust« [2] infiltrieren, um alle ausgetauschten Kisten öffnen zu können – keine besonders schöne Vorstellung.

### Asymmetrische Verschlüsselung

Ihr habt beide einen einzigartigen, »privaten« Schlüssel. Die »öffentliche« Kette, die dein privater Schlüssel öffnet, schickst du nun deinem Freund. Wenn dein Freund dir nun eine Kiste schicken will, nimmt er deine Kette und verschließt damit die Kiste. Kein anderer ist nun in der Lage, dein Schloss zu öffnen außer dir; es gibt ja nur einen Schlüssel; und den besitzt du. Andersrum läuft es gleich. Wenn du deinem Freund eine Kiste schicken willst, holst du dir seine Kette und verschließt damit die Kiste. Nur er kann jetzt die Kiste wieder öffnen.

Kommt nun ein Dritter dazu, kann dieser – unter genau den gleichen Konditionen wie dein Freund – Kisten verschicken und empfangen. Jedoch kann er keine Kisten mehr öffnen, die nicht an ihn adressiert sind.

Grundsätzlich gilt: Symmetrische Verschlüsselung setzt man beim Verschlüsseln lokaler Daten auf der Festplatte ein, da nur einer einen Schlüssel haben muss. Sobald man diese Daten aber an mehrere Leute verschicken will, wird man zur asymmetrischen Verschlüsselung greifen müssen.



#### Auswahl eines Keyserver

PGP ist eine Methode für asymmetrische Verschlüsselung.

#### Ein PGP Schlüsselpaar generieren

Damit man nun seine Mails mit PGP verschlüsseln und signieren kann, braucht man zwei Schlüsselpaare: den öffentlichen Schlüssel (die Kette) und den privaten Schlüssel (den Schlüssel). Beide werden mit dem Tool Seahorse generiert, welches sich normalerweise unter *Anwendungen – Zubehör – Passwörter und Verschlüsselung* befindet.

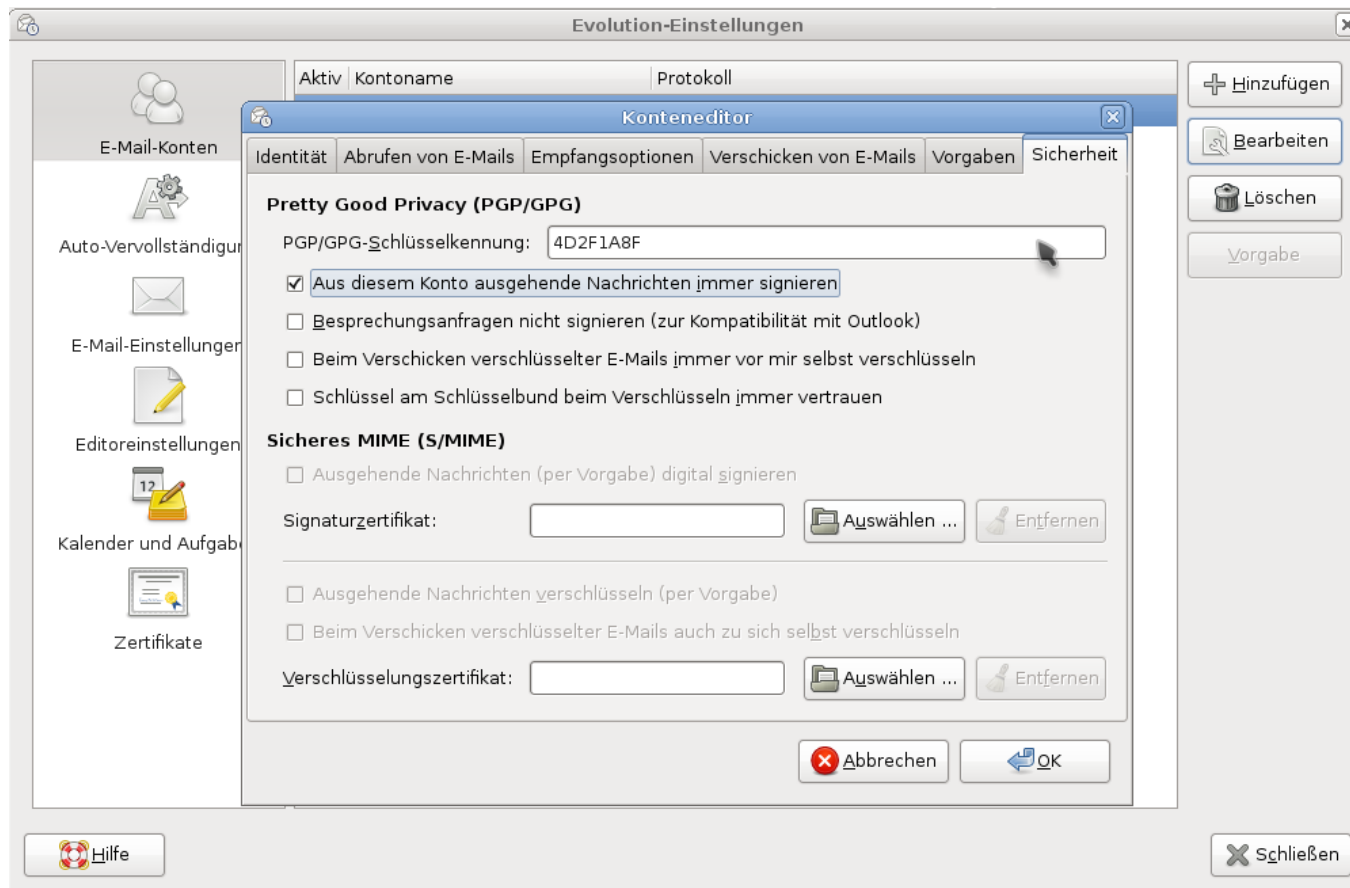
Dort angekommen rufen wir mit *Schlüssel – Neuen Schlüssel erzeugen* den Assistenten auf, der

uns nun, gefüllt mit unseren Daten, ein neues Schlüsselpaar generiert. Als E-Mail-Adresse muss man diejenige wählen, bei der man später seine E-Mails signieren und verschlüsseln will. Um die Verschlüsselung besonders stark zu machen, verwenden wir einen 4 kByte langen Schlüssel. Danach werden wir nach einer Passphrase gefragt. Diese wird später immer benötigt, wenn wir unseren privaten Schlüssel zum Entschlüsseln benutzen wollen.

#### Backup des Schlüsselpaares

Da in unserer Version der Export beider Paare ein wenig fehlerbehaftet war, raten wir dringend, das





### Konfiguration des gewünschten E-Mail-Kontos

Verzeichnis `~/gnupg` zu sichern. Bei einem verlorenen privaten Schlüssel kann der Empfänger die an ihn adressierten Nachrichten nicht mehr lesen und muss ihn widerrufen, was mit einem erheblichen Aufwand für alle Sender verbunden ist: Diese müssen sich dann den neuen öffentlichen Schlüssel noch einmal herunterladen.

### Öffentlichen Schlüssel publizieren

Damit andere Leute uns verschlüsselte Nachrichten schicken können, brauchen sie den öffentlichen Schlüssel. Diesen können wir nun mit einem Rechtsklick auf den Schlüssel und *Öffentlichen Schlüssel exportieren* in eine Textdatei exportieren und verschicken. Auf keinen Fall sollte man seinen privaten Schlüssel veröffentlichen!

Eine wesentlich komfortablere Methode bietet jedoch die Veröffentlichung des Schlüssels auf einem Keyserver.

Um den Schlüssel auf einen Keyserver zu laden, macht man einen Rechtsklick auf den Schlüssel und wählt *synchronisiere und veröffentliche Schlüssel*. Mit einem Klick auf *Schlüsselserver* spezifizieren wir unser Ziel. Standardmäßig ist es am Feinsten, auf dem MIT-Server [3] zu veröffentlichen, da pgp.com eine Authentifizierung per Mail verlangt. Brauchen wir einen anderen, lässt sich dieser komfortabel über den Hinzufügen-Button ergänzen.

Aus Komfortgründen sollte man noch die beiden Optionen *Schlüssel automatisch von den Schlüssel-Servern abrufen* und *Veränderte Schlüssel automatisch mit den Schlüssel-Servern abgleichen* setzen.

### Auswahl eines Keyserver

Ist das erledigt, kann man das Fenster schließen und mit einem Klick auf *synchronisieren* den Upload starten.

### Evolution einrichten

Nach dem Einrichten und Hochladen des Schlüsselpaares muss unsere E-Mail Software konfiguriert werden.

Dazu Bearbeiten wir unser E-Mail-Konto, welches wir unter *Bearbeiten – Einstellungen – E-Mail-Konten* finden. Unter dem Reiter *Sicherheit* geben wir als Erstes unsere Schlüsselkennung ein. Diese kann in Seahorse unter dem Reiter *Eigene*

*Schlüssel*, Spalte Schlüsselkennung, nachgeschaut werden. Außerdem können wir die Option *Aus diesem Konto ausgehende Nachrichten immer signieren* gefahrlos aktivieren.

### Konfiguration des gewünschten E-Mail-Kontos

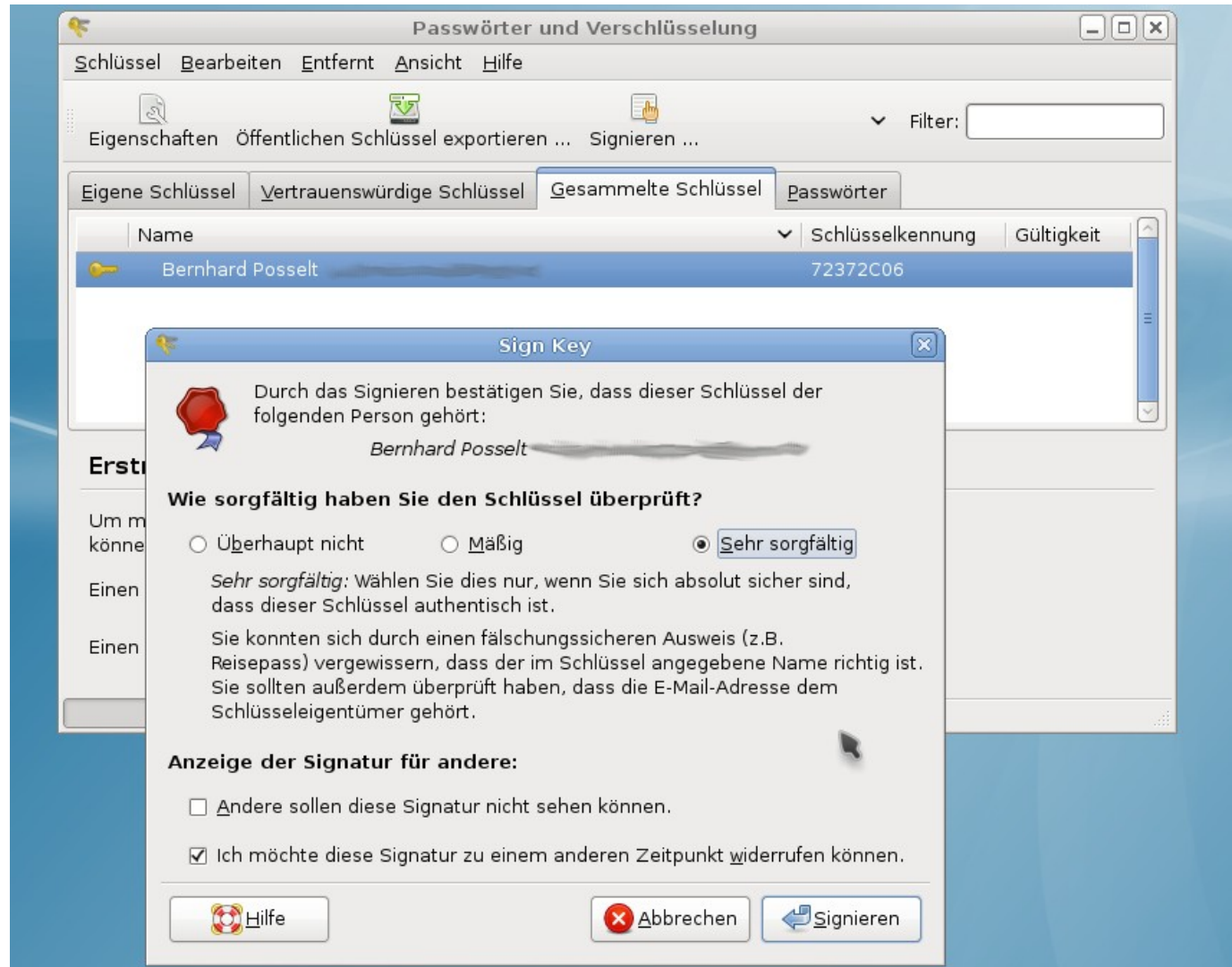
Nach diesen Schritten sind wir bereits in der Lage, unsere E-Mails zu signieren. Wollen wir sie aber verschlüsseln, müssen wir uns zuerst den öffentlichen Schlüssel des Empfängers holen.

### Importieren öffentlicher Schlüssel

Neben dem Verschlüsseln von E-Mails werden öffentliche Schlüssel auch zur Verifikation von fremden Signaturen benötigt. Hat man einen öffentlichen Schlüssel zugeschickt bekommen, kann man diesen in Seahorse über *Schlüssel – Importieren* zu den gesammelten Schlüsseln hinzufügen.

Die komfortablere Methode beinhaltet wieder den Keyserver. Über *Entfernt – Entfernte Schlüssel suchen* können wir nun nach dem Schlüssel suchen. Als Suchterme kommen die Schlüsselkennung oder E-Mail-Adresse des Eigentümers in Frage. Müssen wir auf anderen Servern suchen als den vorgegebenen, können wir diese über *Bearbeiten – Voreinstellungen – Schlüssel-Server* hinzufügen. Hat man den gewünschten Schlüssel gefunden, kann man diesen nun importieren.

Alle importierten Schlüssel befinden sich zunächst unter dem Reiter *Gesammelte Schlüssel* und müssen erst signiert werden. Mit einem Klick auf




### Öffentliche Schlüssel signieren um ein Web-Of-Trust aufzubauen

*Signieren* kann der Schlüssel je nach Überprüfung signiert werden. Signierte Schlüssel wandern unter den Reiter *Vertrauenswürdige Schlüssel*. Damit nun auch andere Leute von der Verifikation profi-

tieren können, sollte man den Schlüssel, wie in *Öffentlichen Schlüssel publizieren* beschrieben, synchronisieren.

Von: Yalm <testingpgp@gmail.com>  
Antwort an: testingpgp@gmail.com  
An: [REDACTED]  
Betreff: test  
Datum: Thu, 19 Feb 2009 03:33:48 +0100 (02:33 GMT)  
2 Anlagen  Alle speichern

test  
  
hihi

 PNG-Bild-Anlage (Bildschirmfoto.png)  
 einfaches Textdokument-Anlage (howto)

 Gültige Signatur  
Verschlüsselt

*Geschafft! Sowohl die Signatur, als auch die Verschlüsselung funktionieren*

Nach dieser Prozedur können nun verschlüsselte E-Mails an den Empfänger gesendet und fremde Signaturen verifiziert werden.

### Eine verschlüsselte Mail senden

Nachdem man sich den öffentlichen Schlüssel des Empfängers »geschnappt« hat, schreibt man eine E-Mail an ihn. Beim Erstellen der E-Mail setzt man unter *Sicherheit – Mit PGP verschlüsseln* einen Haken und kann die Mail so verschlüsselt losschicken. Etwaige Anhänge werden mit verschlüsselt.

Hat alles funktioniert, muss der Empfänger beim Anschauen der E-Mail noch seine Passphrase eingeben und kann nun die E-Mail entschlüsseln.

### Fazit

Verschlüsselung leicht gemacht: Hat man erst einmal die Schlüssel seiner Kontakte zusammen, erlaubt es Evolution, bequem verschlüsselte E-Mails auszutauschen. Gegen Identitätsdiebstahl schützt eine Signatur.

Verschlüsselung von E-Mails ist nicht nur in kritischen Bereichen wie Krankenhäusern und großen Firmen sinnvoll: Sollte man einen gratis E-Mail-Account besitzen (GMX, GoogleMail, WEB.de...), sollte man es durchaus in Erwägung ziehen, die Datensammelwut der Provider durch Verschlüsselung privater E-Mails einzuschränken.

Wem Evolution zu überladen ist und seine Mails mit Thunderbird verwaltet, sollte zum Thunderbird-Plugin »Enigmail« greifen [4].

Bernhard Posselt  
ray@yalmagazine.org

### Informationen

- [1] Off-The-Record Messaging:  
[http://wiki.ubuntuusers.de/Off-the-Record\\_Messaging](http://wiki.ubuntuusers.de/Off-the-Record_Messaging)
- [2] Web-Of-Trust:  
[http://de.wikipedia.org/wiki/Web\\_of\\_trust](http://de.wikipedia.org/wiki/Web_of_trust)
- [3] MIT-Server: <http://pgp.mit.edu/>
- [4] Enigmail & Thunderbird: <http://wiki.ubuntuusers.de/Thunderbird/Tipps>



# Arbeiten in der Konsole (II): WeeChat – IRC Client

**Das IRC-Netzwerk baut auf einem ganz simplen Protokoll auf, das viele Menschen in Verbindung bringt. Dazu braucht man nur noch einen einfach zu bedienenden Client.**

Wie bei so vielen anderen Programmen in der Unix-Welt auch, gibt es eine große Auswahl an IRC-Clients. Allein die Liste der Konsolencients [1] macht es so manchem Nutzer schwer, die richtige Wahl zu treffen. Fragt man einmal herum, wer denn welchen Client auf der Konsole benutzt, bekommt sehr oft die Antwort »irssi« [2]. Es gibt allerdings einen weiteren ausgefeilten Client, der die Konsole unsicher macht, und dieser soll jetzt vorgestellt werden. Die Rede ist von WeeChat [3].

## Warum WeeChat und was kann es?

Das noch recht junge Projekt von FlashTux [4] startete am 27.09.2003 mit der Version 0.0.1. Schon damals war klar, dass man einen schnellen und leichten IRC-Client schaffen wollte, der es dem Benutzer leicht macht, sich im IRC zu unterhalten und auf gewisse Dinge zu reagieren. Die aktuelle Version 0.2.6.1 ist in mehreren Sprachen verfügbar, hat eine vollständige UTF-8 Unterstützung und ist ohne Ausnahme frei verfügbar. Man kann sich mit beliebig vielen Servern verbinden und hat die Möglichkeit, IPv6, SSL sowie einen Proxy-Server und eine automatische Wiederverbindung zu benutzen. Interessant ist WeeChat allerdings nicht nur für Benutzer der Konsole, denn es gibt auch eine Gtk- sowie demnächst eine Qt-

Version des Clients. Dieser Artikel beschränkt sich allerdings auf die curses-Version des Clients, mit der man auf der Konsole arbeitet.

Damit man alles im Blick hat, verfügt der Client standardmäßig über eine Benutzerliste für den jeweiligen Channel. Wenn der Benutzer angeschrieben wird, was als »highlighting« bezeichnet wird, so sieht man dies, egal in welchem Channel man sich gerade befindet. Falls mal mehr als ein Channel gleichzeitig eingesehen werden soll, so kann man neue Fenster erzeugen, die horizontal und vertikal im Programm aufgeteilt werden können. Wer sich nicht mehr genau an den Tag und die Stunde erinnert, an dem etwas bestimmtes geschrieben wurde, der hat die Möglichkeit in seinen gepufferten Nachrichten zu suchen. Neu ist neben der Suche auch eine Rechtschreibprüfung mittels aspell. Das immer wieder auftretende Problem der (De-)Kodierung löst WeeChat, indem der Nutzer die Zeichenkodierung global, für jeden Server oder auch jeden einzelnen Channel getrennt einstellen kann. Über eine sogenannte »FIFO pipe« ist es außerdem möglich, Nachrichten über diesen Tunnel an den Client zu schicken, die somit auch im IRC ankommen.

Wem das alles nicht genug ist, der kann WeeChat mittels der integrierten Plugin-API zusätzlich erweitern. Dies kann mit Perl, Python, Ruby oder auch Lua geschehen. Auf der Website gibt es eine Liste [5] veröffentlichter Plugins, die zum Download bereitstehen. Damit aber noch nicht genug der Anpassungsmöglichkeiten, denn der Benutzer kann sämtliche Befehle mit einem Alias versehen und Funktionen auf alle verfügbaren Tasten legen. Alles ist veränderbar, so wie man es selbst gern haben möchte.

## Installation und Konfiguration

Die Installation geht wie gewohnt über die gebräuchlichen Wege. Unter Ubuntu kann man WeeChat mittels Paketmanager/Synaptic installieren. Damit die Plugins benutzt werden können, braucht man noch das Paket *weechat-plugins*. Um einige Plugins gleich mitzuinstallieren, gibt es das Paket *weechat-scripts*. Somit kann man sich sein Riesenpaket unter Ubuntu mit folgendem Befehl installieren:

```
sudo aptitude install weechat-curses →  
weechat-plugins weechat-scripts
```

Bei anderen Distributionen hilft eine Suche in der Paketliste nach *weechat*, oder man kompiliert sich die aktuelle Version selbst. Der Quelltext ist von der Projektseite herunterladbar.

Um WeeChat seinen Wünschen entsprechend zu konfigurieren, hat man nun zwei Möglichkeiten zur Auswahl. Die erste Variante wäre der übliche Weg des Editierens der Konfigurationsdatei. Diese liegt standardmäßig im Heimverzeichnis des Benutzers unter *~/.weechat/weechatrc*. Dort kann jede Konfi-

gurationsvariable mit ihrem gewünschten Wert eingetragen werden und man braucht nur noch zu speichern, damit der IRC-Client beim nächsten Start die Einstellungen verwendet. Alle Variablen [6], die das Programm kennt, sind in der Dokumentation [7] von WeeChat aufgelistet. Hier muss positiv erwähnt werden, dass es für die aktuelle Version auch eine deutsche Übersetzung gibt.

Einen viel eleganteren Weg bietet allerdings die zweite Variante. Zumal vor dem ersten Start des Programms noch keine Konfigurationsdatei existiert, macht es wenig Sinn, dort nun alle wichtigen Werte per Hand einzutragen. Wird WeeChat gestartet, erzeugt es automatisch eine Datei mit den Standardeinstellungen, die rundum auch alle gebräuchlich sind. Die angesprochene zweite Variante ermöglicht es dem Benutzer, alle Einstellungen über einen integrierten Befehl zu verändern. Sämt-

liche Werte, die »on the fly« eingestellt wurden, sind auch sofort im Programm aktiv. Beim Beenden speichert WeeChat dann alle veränderten Werte in die Konfigurationsdatei. Daraus folgt auch, dass es nicht sinnvoll ist, die Datei per Hand zu editieren, wenn das Programm noch läuft; beim Beenden werden alle Werte mit denen überschrieben, die der Client zum Schluss hatte. Näheres zu dieser Variante folgt in einem späteren Abschnitt des Artikels.

### Server, Channel, Benutzer

Startet man WeeChat auf der Konsole mit dem Befehl

```
weechat-curses
```

wird man zuerst vom Programm freundlich begrüßt, das dann alle Plugins lädt und den Benutzer, wenn dies der erste Programmstart war, zum Freenode [8] IRC-Netzwerk verbindet. Der Benutzername wird anhand des Unix-Benutzernamens ausgelesen. Sobald die Verbindung steht, rast auch gleich eine Menge Text herunter. Um sich diesen von vorne bis hinten durchlesen zu können, bedient man sich der Tasten [Bild hoch] um hoch zu scrollen, sowie [Bild runter], damit man im Textpuffer wieder dem Ende näher kommt.

Da nicht jeder Benutzer auf freenode (oder nur dort) chattet, gibt es die Serververwaltung in WeeChat. Mit-

tels des Befehls `/server` erhält man eine kleine Übersicht aller gespeicherten Server. In der Kurzansicht der Liste sieht man bei jedem Einzelnen, ob man mit diesem verbunden ist, in wie vielen Channels man aktiv ist und wie viele private Chats derzeit offen sind. Gibt man stattdessen noch den Parameter `listfull` mit an, so bekommt man mit dem Befehl `/server listfull` von allen Servern die Einstellungen. Wer nun einen neuen Server hinzufügen möchte, gibt als Parameter `add` an, sowie weitere Informationen über den Server. Als Beispiel für das InsiderZ.DE-Netzwerk [9] sieht der entsprechende Befehl folgendermaßen aus:

```
/server add insiderz irc.insiderz.de →
-auto -nicks holloway holloway_ →
holloway__ -realname Holloway -autojoin →
#meinchannel
```

Somit wurde der insiderz.de Server mit dem Alias »insiderz« hinzugefügt. Im gleichen Schritt wurde festgelegt, dass man mit dem Benutzernamen »holloway« und dem realen Namen »Holloway«, sowie den Ersatzbenutzernamen »holloway\_« und »holloway\_\_« verbunden sein wird. Der Parameter `-auto` bewirkt einerseits, dass man automatisch mit dem Server »insiderz« verbunden wird; andererseits wird diese Information von WeeChat gespeichert. Beim nächsten Programmstart verbindet sich der Client zu allen Servern, die diese Einstellung haben. Dasselbe gilt für den Parameter `-autojoin`, allerdings für die Channel, in die man automatisch dazustößt.

```
WeeChat 0.2.6 (c) 2003-2007 - http://weechat.flashtux.org
16:36:44 Willkommen in WeeChat, the geekiest IRC client!
16:36:44 WeeChat 0.2.6, kompiliert am Oct 28 2008 03:00:19
16:36:44 -----
16:36:44 -P- Initialisiere Plugin "Ruby" 0.1
16:36:44 -P- Loading Ruby module "weechat"
16:36:44 -P- Plugin "Ruby" (/usr/lib/weechat/plugins/ruby.so) geladen.
16:36:44 -P- Initialisiere Plugin "Aspell" 0.1
16:36:44 -P- [Aspell] [LOAD] options loaded
16:36:44 -P- Plugin "Aspell" (/usr/lib/weechat/plugins/aspell.so) geladen.
16:36:44 -P- Initialisiere Plugin "charset" 0.1
16:36:44 -P- Charset plugin starting, terminal charset: UTF-8 (WeeChat
internal: UTF-8)
16:36:44 -P- Charset: setting "charset.global.decode" to UTF-8
16:36:44 -P- Plugin "charset" (/usr/lib/weechat/plugins/charset.so) geladen.
16:36:44 -P- Initialisiere Plugin "Python" 0.1
16:36:44 [1] [freenode] 1:[freenode]
16:37:47 März, Sonntag 01 2009
holloway1()
```

Willkommensgruß von WeeChat

Nicht jeder kann sich immer alle Parameter merken, deshalb gibt es einen Hilfebefehl. Wird `/help` ohne Parameter aufgerufen, listet der IRC Client alle Funktionen auf, die verfügbar sind. Gibt man nun als Parameter einen dieser Befehle an, so zeigt es die Hilfe zum angegebenen Befehl an. Als Beispiel kann nun einmal `/help server` eingegeben werden. Das Gegenstück zum Hinzufügen von Servern ist das Löschen selbiger. Dies geschieht ganz simpel mit dem Parameter `del` und dem Alias vom gewünschten Server.

Mittels

```
/server del freenode
```

kann also z. B. der von WeeChat voreingestellte Server entfernt werden. Beachtet werden muss hierbei lediglich, dass man nicht mit diesem Server verbunden ist. Da man beim ersten Start vom Client noch mit dem freenode-Netzwerk verbunden ist, muss man sich zuerst mit dem Befehl `/disconnect freenode` von diesem trennen. Auch hier benutzt man wieder den Alias. An dieser Stelle wird auf die Tab-Completion hingewiesen, die unter anderen bei Befehlen, Parametern, Aliase und Benutzernamen funktioniert. Es reicht also aus, lediglich `/dis` einzutippen und dann die [Tab] Taste zu drücken, damit der disconnect-Befehl vervollständigt wird. Wer keine automatische Verbindung eingestellt hat, muss sich manuell mit dem Befehl `/connect` und dem Serveralias verbinden.

```
[18:30:47] -> holloway_
(weechat@iZ-9E95F68D.versanet.de) ist in
den Channel #blablubb gekommen
[18:30:47] - Nicks #blablubb: [holloway_]
[18:30:47] - Channel #blablubb: 1 Nick (1 Operator, 0
Halb-Operator, 0 Gevoiceter, 0 normal)
[18:30:47] - Channel erstellt am Sun Mar 1 18:29:53
2009
[18:31:16] holloway_ | Hier ist ziemlich wenig los. :)

[3] [insiderZ] 2: #blablubb()
[18:33:08] März, Sonntag 01 2009
[holloway_(x)]

Willkommen im Netzwerk-Channel #insiderZ ]-[ Themen: Chatten, Lifestyle & Hilfe
rapunzel Ratboy redrum !Velines^
redrum^mindcontrolled !alphaloff
RitterRostlabschnur !Boronloff
rill[x]la sF silversurfer !byteinterceptor
Sita Sk8er[OFF] !Cat
SkullSplitter !ChuckY
Skyscraper[BNC] !Cpt-Future|BNC
sockenschuss|bnc sozjo !darklord
spielkind2k Stanloff !HELPLBot
SteveHH[BNC] stone !herzdame
StonedStorm stylus740 !hex^irssi
Sweety t3rr4n !Markus
TheD|OFFLINE TheFox !Seelenjaegerin
TheReaper theexception !Spirit[AW]
Thoki Timecop|besuch !svenissimo
Titania tomtomgradhedda !Galeader
unbehagen ungeliebt vampy !JimBoblaway
Watzmann|onAir Werderaner !ReinerZufall
wonderfull wXwZocker !Saint'off
x-Dieu Zero zickchen|off !Ent
174min !Gratulator
[18:31:04] - Channel #insiderZ: 168
Nicks (15 Operatoren, 4
Halb-Operatoren, 6
Gevoicete, 143 normal)
[18:31:04] - Channel erstellt am Fri
Apr 1 00:01:21 2005
[18:31:28] - gigahansi ist nun bekannt
als gig|alansi
[18:31:33] - zickchen|off ist nun
bekannt als Zickchen
[18:32:15] - killerbees19 ist nun
bekannt als KB19|offline
[18:32:40] - Sweety ist nun bekannt
als Sweetyl|ng
[3] [insiderZ] 3: #insiderZ +ntrSCTGF [8j,5m^m1,5t]:3
[18:33:08] März, Sonntag 01 2009
[holloway_(x)]
```

### Vertikal geteilte Chatfenster

Das Hauptaugenmerk beim IRC-Netzwerk liegt darauf, dass sich mehrere Personen gleichzeitig unterhalten können, weshalb es auf einem Server Channels gibt. Damit man einem dieser Räume beitreten kann, muss man den Namen wissen und den Befehl `/join` benutzen. Um beispielsweise dem Channel `#yalmagazine` beizutreten, gibt man `/join #yalmagazine` ein. (Hinweis: Der Channel von Yalm befindet sich im freenode-Netzwerk.) Alle in diesem Channel befindlichen Personen werden nun rechts in einer Liste angezeigt. Um in der Benutzerliste zu scrollen, falls mehr Personen vor-

handen sind als Zeilen, benutzt man die Tasten [F11] und [F12].

Gelegentlich kann es vorkommen, dass man mit einer einzigen Person in Kontakt treten will. Hierfür gibt es den Befehl `/query`, welcher in Verbindung mit einem auf dem Server befindlichem Benutzer-namen einen neuen Puffer, in WeeChat Buffer genannt, öffnet.

### Buffer und Windows

Langsam wird der eine oder andere sich fragen, wie kommt man nun wieder zurück zum Channel,



oder sogar zur Serverausgabe? WeeChat arbeitet mit sogenannten Buffern. In jedem Buffer ist entweder eine Serverausgabe, ein Channel, ein Dateitransfer oder aber ein Privatchat, der oft als Query bezeichnet wird. Diese sind in der Reihenfolge, wie sie erstellt wurden, nummeriert. Welche Nummer der aktuell angezeigte Buffer hat, wird in der Statusleiste unten an dritter Stelle angezeigt. An erster Stelle steht in eckigen Klammern die Gesamtanzahl aller Buffer, danach kommt, wieder in eckigen Klammern, der Serveralias. Die Verwaltung dieser Buffer erfolgt mittels des Befehls `/buffer`. Als erste Variante kann man die Nummer des Buffers anfügen, zu welchem gewechselt werden soll. Mittlerweile gibt es auch die Möglichkeit, die Namen der Buffer zu verwenden, welche direkt hinter der Buffernummer zu finden sind. Kleiner Tipp: Wieder kann mit der [Tab] Taste durch alle Namen »getablt« werden. Drückt man stattdessen [Shift] + [Tab], so geht WeeChat die Auswahl rückwärts durch. Wird der aktuell angezeigt Buffer nicht mehr benötigt, verschwindet er auf Befehl mittels `/buffer close`. Sitzt man in diesem Buffer noch in einem Channel, kann alternativ eine Nachricht hinten angefügt werden, die dann als Meldung beim Verlassen angezeigt wird.

```
WeeChat 0.2.6 (c) 2003-2007 - http://weechat.flashtux.org
[20:37:49] insiderz.server_realname = "Holloway"
[20:37:49] insiderz.server_hostname = ""
[20:37:49] insiderz.server_command = ""
[20:37:49] insiderz.server_command_delay = 1
[20:37:49] insiderz.server_autojoin = ""
[20:37:49] insiderz.server_autorejoin = ON
[20:37:49] insiderz.server_notify_levels = ""
[20:37:49] 183 Konfigurationsoption(en) gefunden
[20:37:54] [log]
[20:37:54]   log_auto_server = OFF
[20:37:54]
[20:37:54] Detail:
[20:37:54]   . boolesche Werte ('on' or 'off')
[20:37:54]   . Standardwert: 'off'
[20:37:54]   . Beschreibung: Automatisches Logging von Servermessages
[20:38:47] [log]
[20:38:47]   log_auto_server = ON
[1] 1:[nicht verbunden]
[20:39:07] März, Dienstag 03 2009
[-cmd-()]
```

### Einstellungen in WeeChat

Wer bei mehreren Buffern gleichzeitig Ausschau nach neuen Nachrichten halten will, kann sich die Fläche horizontal sowie vertikal teilen. Hierfür gibt es technisch auch keine Grenze, so könnte man sich theoretisch alle Buffer gleichzeitig in allen möglichen Variationen anzeigen lassen. Das Ganze wird dann nur etwas unübersichtlich. Alles, was mit Fenstern zusammen hängt, wird mit dem Befehl `/window` gesteuert. Geteilt wird die Fläche horizontal mit dem Parameter `splitw` und vertikal mittels `splitv`. Beispielsweise könnte man sich 2 Fenster nebeneinander anzeigen lassen, wenn man den Befehl `/window splitv` eingibt. Zu guter

Letzt muss man sich auch wieder zwischen den einzelnen Fenstern bewegen können. Hierfür hat der `window`-Befehl die Parameter `+1`, `-1`, `up`, `down`, `left` und `right`, womit, der Reihenfolge entsprechend, in das nächste, letzte, darüber liegende, darunter liegende, links liegende, sowie rechts liegende Fenster gewechselt wird.

### Suchen und Einstellungen

Bei mehreren hundert bis tausend Zeilen Verlauf kann es manchmal vorkommen, dass man nicht mehr genau weiß, wo über eine bestimmte Sache gesprochen wurde. Für solche Fälle hat WeeChat eine Suche integriert, die den gesamten Verlauf des aktuellen Buffers durchsucht. Aktiviert wird diese standard-

mäßig mit der Tastenkombination [Strg] + [r]. Alle nun eingegeben Zeichen werden als Suchwort interpretiert. Findet der Client eine passende Stelle, wird diese in der obersten Zeile angezeigt. An allen Zeilen, in der das Suchwort vorhanden ist, wird links daneben ein farbiges Kästchen angezeigt. Darunter folgen alle Zeilen, die im Verlauf des Gesprächs als nächstes geschrieben wurden. Mit den Tasten [Pfeil hoch] und [Pfeil runter] wird jeweils eine Fundstelle hoch, sowie eine nach unten gescrollt, immer mit der aktuellen Fundstelle in der ersten Zeile. Über die Tasten [Bild hoch] und [Bild runter] kann weiterhin normal im Verlauf gescrollt

werden um so per Hand nach Fundstellen, die mit dem Kästchen markiert sind, zu suchen. Zum Abschluss, um die Suche zu beenden, betätigt man die [Enter] Taste.

Im Abschnitt *Installation und Konfiguration* wurde angesprochen, dass alle Einstellungen direkt im Programm verändert werden können. Wie bei anderen großen Anlaufstellen, gibt es auch hierfür einen zentralen Befehl. Füttert man WeeChat mit `/set`, so rast mal wieder eine lange Liste herunter. In dieser sind, kategorisiert, alle Einstellungen aufgeführt, die der Client kennt und somit im Programmverlauf benutzt. Eine Verbindung mit der eingebauten Suche hilft hier, um eine Einstellung zu finden, nach der in etwa gesucht wird. Ebenfalls eine Hilfe ist wieder einmal die Vervollständigung mittels der [Tab] Taste. Weiß man allerdings genau wonach man sucht, so gibt man die Einstellung einfach als Parameter hinter den Befehl mit an. Da hier noch keine Wertzuweisung stattfindet, gibt WeeChat den aktuellen Wert und eine Kurzhilfe zur angeforderten Einstellung. Beispielsweise können mit dem Befehl `/set log_auto_server` die besagten Informationen aus dem Client gekitzelt werden. Für spätere Einsichten in die Meldungen des IRC Servers kann man nun WeeChat mit der Einstellung dazu bringen, dass alle Nachrichten in einer Log-Datei gespeichert werden. Nach der Eingabe des Befehls

```
/set log_auto_server on
```

sind im Konfigurationsordner vom Client in einem Unterverzeichnis die erzeugten Log-Dateien zu fin-

den, in der Standardeinstellung also in `~/.weechat/logs/`.

### Aliase und Tastaturkürzel

Manchmal, beziehungsweise auch mal öfters, ist man etwas faul und möchte nicht immer diese langen Befehle eintippen, damit WeeChat die dazugehörige Funktion aufruft. Dessen Abhilfe zu schaffen, gibt es zwei Wege, um sich die lästige Schreiarbeit zu verkürzen. Über eine Aliassteuerung kann man sich lange Befehle inklusive Parameter, die man häufig benutzt, mit einem anderen, und vor allem kurzen, Namen versehen. Eine Abwesenheit wird über den Befehl `/away` erzeugt, die in Verbindung mit dem Parameter `-all` und einer nachfolgenden Nachricht auf allen verbundenen Server gesetzt wird. Erzeugt man mit

```
/alias AFT away -all aft – away from →  
terminal :)
```

den Alias, so genügt ab sofort der Befehl `/AFT`, um sich auf allen Servern vorerst zu verabschieden.

Weitaus effektiver ist der Einsatz von Tastaturkürzeln, die Funktionen von WeeChat aufrufen. Voreingestellt sind im Client schon so einige, die man sich mit dem Befehl `/key` allesamt auflisten lassen kann. Laut der Liste kann man standardmäßig zum Beispiel schon mittels [Alt] + [1] zum Buffer ersten wechseln, oder mit [Alt] + [3] zum dritten Buffer. Will man nun eine neue Kombination hinzufügen, folgt zuerst die Tastenkombinationen, danach die Funktion, oder auch ein kompletter Be-

fehl inklusive Parameter. Zu Beginn wird man nicht gleich wissen, wie die richtige Tastenkombination in WeeChat geschrieben werden muss, doch gibt es auch für dieses Problem eine Lösung vom IRC-Client. Drückt man [Alt] + [k], ist ein Modus aktiviert, der die nächste Tastenkombination vom Benutzer in der Art und Weise in die Eingabezeile schreibt, wie sie das Programm akzeptiert. Aus dieser Information heraus bildet sich zum Beispiel der Befehl

```
/key ctrl-Q /quit
```

um dem wundervollen Client auch einmal eine Auszeit mit den Tasten [Strg] + [q] zu gönnen.

Thomas Rudolph  
[holloway@yalmagazine.org](mailto:holloway@yalmagazine.org)

### Informationen

- [1] <http://www.ircreviews.org/clients/platforms-unix.html>
- [2] <http://irssi.org/>
- [3] <http://weechat.flashtux.org/>
- [4] <http://flashtux.org/>
- [5] <http://weechat.flashtux.org/plugins.php>
- [6] <http://weechat.flashtux.org/doc/de/ch03s05.html>
- [7] <http://weechat.flashtux.org/doc/de/index.html>
- [8] <http://freenode.net/>
- [9] <http://insiderz.de/>

# AssaultCube

Heute stellen wir einen freien Ego-Shooter vor, der auf der von Wouter van Oortmerson geschriebenen Cube-Engine basiert.

Nach dem Projektstart am 17. November 2007 – damals noch unter dem Namen ActionCube – und einer längeren Beta-Phase wurde er vor kurzem als stabiles 1.0-Release [1] ausgeliefert. Informationen aus einer E-Mail-Korrespondenz mit Markus Bekel, der als Deutscher einer der neun Mitglieder des Entwicklerteams ist, bilden das Fundament des Artikels.

Im Gegensatz zu Counter-Strike, das auf den Strategieaspekt drückt und lediglich mit WindowsSystemen nativ läuft, ist AssaultCube schneller, auf allen gängigen Betriebssystemen spielbar und buhlt um den Spaßfaktor.

## Spielprinzip

Die Einfachheit von ActionCube sollte in eine realistischere Umgebung übertragen werden, was mehr oder weniger realisiert wurde. In den Spielmodi Deathmatch und Team Deathmatch kann man als Erschossener nach knapp 5 Sekunden wieder aktiv am Spiel teilnehmen. Dann ist es oft noch möglich denselben Gegner anzugreifen, der einen zuvor getötet hat. Den Ernst nehmen zudem sich häufende Situationen, bei denen man im selben Moment stirbt, in welchem man den Gegner erschossen hat,

der einem selbst »das Leben nahm«. Auch sind die sogenannten Hit-Boxen nicht auf Präzision ausgelegt. Außer beim Scharfschützengewehr, ist der Treffer ins Bein gleichbedeutend mit einem Treffer in die Herzgegend. Beim Scharfschützengewehr gibt es hingegen noch den Head-Shot, der den Gegner beim ersten Treffer erledigt.

Die Teams im Spiel spalten sich in die »Cubers Liberations Army (CLA)« und die »Rapid Viper

Special Forces (RVSF)«. In AssaultCube ist das sogenannte Straferunning möglich, eine Art der Bewegung, die es dem Spieler erlaubt durch gleichzeitige Vorwärts- und Seitwärtsbewegung schneller zu werden. Straferunning wurde aus der Cube-Engine übernommen, obwohl es nicht sehr realistisch ist; aber den Entwicklern zufolge macht es Spaß.

Eine weitere unrealistische Bewegungsmöglichkeit in AssaultCube ist ein dem Raketensprung vergleichbarer Tricksprung, bei dem der Rückstoß einer Waffe ausgenutzt wird, um höher springen und schneller laufen zu können. Diese Bewegungsmöglichkeit ist ebenso aus dem Spiel Quake3 Arena bekannt. AssaultCubes Waffen sind alle fiktional und typisch für das Genre Ego-Shooter: Assault Rifle, Sub-machine Gun, Sniper Rifle, Pistol, Knife und Shotgun. Zudem gibt es dreizehn verschiedene Mehrspielermodi:

- Deathmatch und Team Deathmatch
- One Shot One Kill und Team One Shot One Kill (nur Sniper Rifle und Messer)
- Last Swiss Standing (nur Messer und Granaten, benannt nach dem Schweizer Messer, da einer der Entwickler Schweizer ist)
- Survivor und Team Survivor
- Pistol Frenzy (nur Pistole, Messer und Granaten)
- Capture the Flag



Eine Nahkampfsituation



- Keep The Flag und Team Keep The Flag
- Hunt The Flag
- Coop Edit (gemeinsames Erstellen oder Verändern einer Map)

### Entwicklung

Mit den Grundeinstellungen ist das Spiel als brutal zu erachten. Sobald man getötet wurde, besteht der Torso aus in einer Blutlache liegenden Fleischfetzen. Blut und anderes lässt sich allerdings bei den Spieleinstellungen abwählen [2]. Da das Spiel in C++ geschrieben wurde, läuft es auch auf betagteren PCs flüssig. Zudem können bei den Grafikeinstellungen die obligatorischen, individuellen Regelungen vorgenommen werden. Obwohl Python eine leicht zu erlernende Sprache ist, wird C++ wegen seiner Schnelligkeit und der vorhandenen Engine verwendet. Die Windows-, Mac- und Linux-Versionen sind gleich, da sie auf OpenGL-, OpenAL- und SDL-Bibliotheken basieren [3][4].

Im weiteren Verlauf der Entwicklung sind lediglich Bugfixes geplant. Auch will man die Sprachdateien in .cfg-Dateien auslagern und den UTF-8 Zeichensatz unterstützen, damit man das Spiel vereinfacht in weitere Sprachen aus dem Englischen übersetzen kann. Für einen Hostage- bzw. Bomb-Mode, bei dem man also Geiseln befreien oder Bomben entschärfen muss, was das andere Team zu ver-



*Der Gesundheitsstatus in Form eines blutigen Bildschirmrandes*

hindern trachtet, ist die Cube-Engine aufgrund ihrer Einschränkungen ungeeignet.

Das Entwicklerteam ist über den gesamten Globus verstreut. Sie kommen etwa aus USA, Deutschland, Schweiz, Neuseeland, Polen und Australien. Das jüngste Mitglied ist 19 und die ältesten liegen in den 30ern. Ein Unterstützer, welcher Maps herstellt, ist erstaunlicherweise über 50 Jahre alt. Weitere Mitglieder sind derzeit jedoch nicht gewünscht. Gelegentlich werden Patches angenommen.

Falls doch ein neues Glied in die Kette des Teams Einzug erhält, passiert das über das Internetforum. Dort muss ein Interessent erst unter Beweis stellen, dass er weiß was er tut und sympathisch ist. Mittlerweile stellt die Fangemeinde [5] ungefähr ein Dutzend an Servern zur Verfügung. Es gibt AssaultCube-Clans, die Turniere organisieren. Selbst die E-Sport Liga ESL hat einen Cup ins Leben gerufen. Für Abwechslung und den Frusterguss für zwischendurch ist Assaultcube zu empfehlen, und obwohl das Spiel manche süchtig macht, werden es andere sicherlich als monoton erachten.

Peter Majmesku  
pe@yalmagazine.org

### Informationen

- [1] Spielhomepage: <http://assault.cubers.net/>
- [2] Wiki zum Spiel: [http://assault.cubers.net/wiki/Main\\_Page/](http://assault.cubers.net/wiki/Main_Page/)
- [3] Wikipediaeintrag: <http://de.wikipedia.org/wiki/AssaultCube/>
- [4] AssaultCube bei SourceForge.net: <http://sourceforge.net/projects/actiongame/>
- [5] Das offizielle Forum: <http://assault.cubers.net/forum/>

# Kleiner TrueCrypt Guide

**Geheime Daten nicht nur verschlüsseln, sondern auch noch verstecken, sie nicht nur mit einem Passwort absichern, sondern zusätzlich mit Bildern oder MP3-Songs schützen und auch noch einen Fingerabdruck-Scanner verwenden – wer wissen möchte wie das mit Linux funktioniert, sollte weiter lesen.**

Bereits in Yalm Ausgabe 04/2008 [1] wurde TrueCrypt [2] mit grafischer Oberfläche vorgestellt und der Vorgang des Verschlüssels anhand eines USB-Sticks demonstriert. Wer bisher noch keine Berührung mit dieser Software hatte, dem sei empfohlen, zunächst diesen Artikel zu lesen.

## Hidden Volumes

Seit der Version 6.0 ist es auch unter Linux möglich sogenannte »Hidden Volumes« zu erstellen. Es handelt sich hierbei um einen verschlüsselten Bereich innerhalb eines bereits verschlüsselten Bereichs. Der Grundgedanke hierbei ist, besonders schützenswerte Daten so zu verstecken, dass für einen Fremden nicht einmal deren Existenz erkennbar ist. Genannt wird dieses Prinzip »plausible deniability« [3], zu deutsch etwa glaubhafte Abstreitbarkeit. Gemeint ist damit die Existenz versteckter Daten auf dem Datenträger negieren zu können, da die Gegenseite deren Vorhandensein nicht beweisen kann. Zu verschlüsseln sind hiermit alle üblichen Datenträger wie Festplatten, USB-Sticks usw.

Vater dieser Idee war die Überlegung, dass man gezwungen sein könnte, das Passwort für einen

verschlüsselten Datenträger zu nennen, und somit einem Unbefugten Zugang zu seinen Daten gewähren muss. Für diesen Fall gibt man das Passwort für den Bereich heraus, den TrueCrypt als »outer Volume« bezeichnet. Hier werden weniger sensible Daten abgelegt, die jedoch schon eine Verschlüsselung rechtfertigen. Da die Existenz des »inner Volume« genannten Containers, der die wirklich schützenswerten Daten enthält, jedoch weder sichtbar noch nachweisbar ist, ist dieser für Unbefugte ohne das notwendige zweite Passwort nicht einsehbar.

## Keyfiles

Wer den Schutz seiner Daten nicht nur einem Passwort anvertrauen möchte, kann seine Daten zusätzlich mit sogenannten Keyfiles absichern. Hierbei handelt es sich um normale Dateien, deren Extension keine Rolle spielt. So kann z. B. ein verschlüsselter USB-Stick neben dem Passwort auch noch mit *BildvonOma.jpg*, *meinLieblingssong.mp3* und *Brief.odt* gesichert werden. Verwendet man dieses zusätzliche Feature, muss man unbedingt darauf achten, dass auf diese Dateien zum Öffnen der Partition oder des Volumes auch zugegriffen

werden kann. Wenn also verschlüsselte USB-Sticks auf einem fremden Rechner gemountet werden sollen, müssen auch dort diese Keyfiles verfügbar sein. Hat man seinen *Lieblingssong.mp3* durch einen *NeuerLieblingssong.mp3* ersetzt, so kann TrueCrypt ihn nicht mehr als Bestandteil des Schlüssels erkennen und das Mounten ist nicht möglich. Zumindest die ersten 1024 Byte des Keyfiles müssen unverändert bleiben, denn die benötigt das Programm zu dessen Identifizierung und damit zur Öffnung des verschlüsselten Datenträgers.

## Security Token

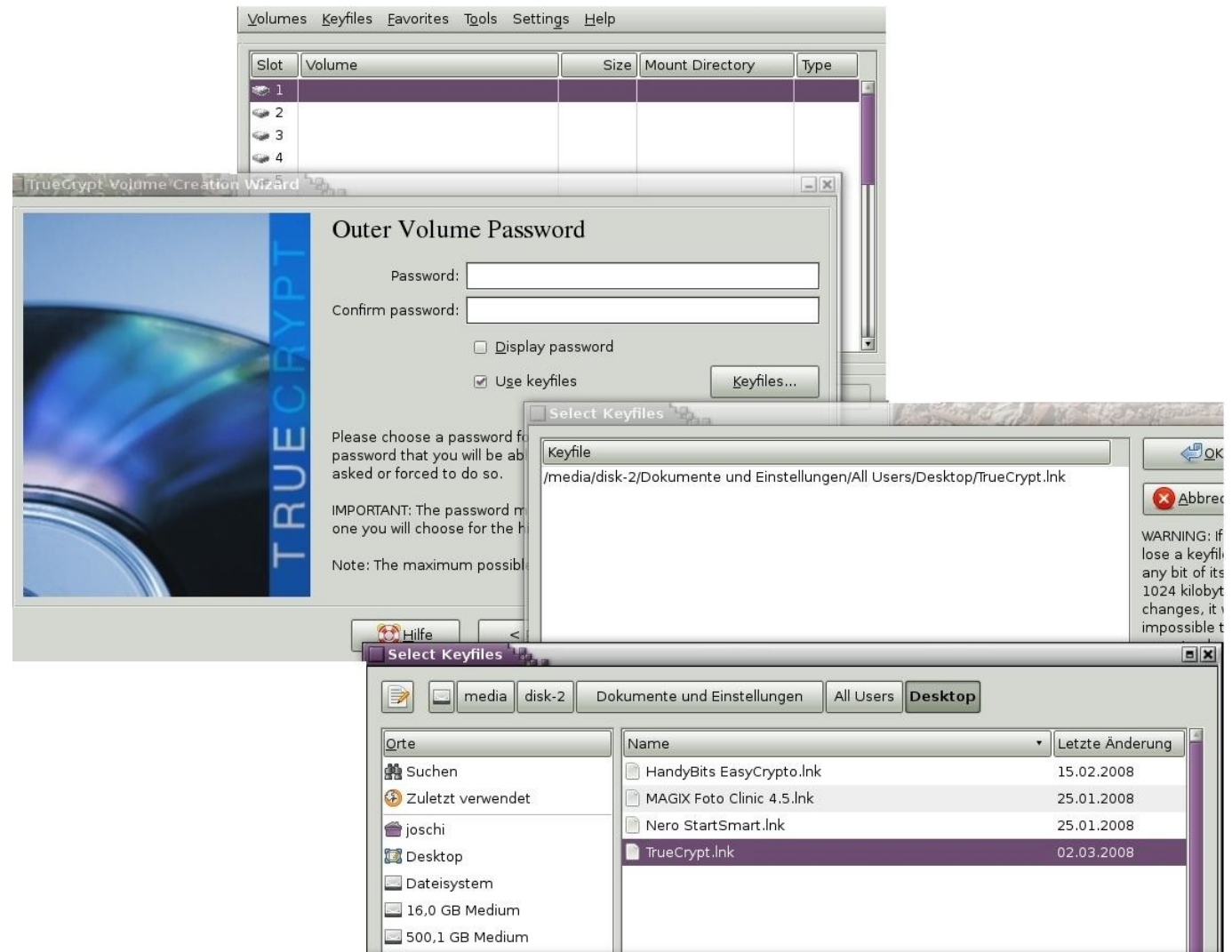
Auch hardwareseitig gibt es Möglichkeiten, den Zugriff auf seine Daten zu steuern. TrueCrypt kann direkt auf Keyfiles zugreifen, die auf einem Security Token [4] oder auf Smart Cards, die den PKCS #11 Standard erfüllen, gespeichert sind.

Mit Token wird in diesem Falle sämtliche Hardware bezeichnet, die es erlaubt, von TrueCrypt verschlüsselte Daten oder Datenträger einzubinden, zu mounten. Hierbei kann es sich um Smart Cards, USB-Sticks oder andere beliebige Speichermedien, Scanner für Fingerabdrücke oder speziell für diesen Zweck hergestellte Medien handeln. Bedingung für deren Nutzung sind die Installation einer PKCS #11 Softwarebibliothek und die Manipulierbarkeit des Mediums durch den Nutzer. TrueCrypt erlaubt den Schutz der Daten mit Hilfe eines Passwortes, Keyfiles und eines Tokens gemeinsam.

## Die Verschlüsselungs-Algorithmen

Eingangs muss gesagt werden, dass eine ausführliche Behandlung dieser Thematik leicht eine Ausgabe unseres Magazins füllen würde. Interessierte werden deswegen auf die weiterführenden Links verwiesen.

Im Jahre 1997 suchte das National Institute of Standards and Technology (NIST), USA, nach einem Nachfolger des bisherigen Verschlüsselungssystems Data Encryption Standard (DES), denn durch die Steigerung der Rechnerleistung war das DES-System nicht mehr ausreichend sicher und wurde letztendlich auch geknackt. Abhilfe schaffte vorübergehend die Verdreifachung der DES-Verschlüsselung, bekannt als 3DES. Da dies jedoch zu Geschwindigkeitseinbußen bei der Datenverarbeitung führte, hat man sich für eine offene Ausschreibung zur Entwicklung des AES (Advanced Encryption Standard) entschieden. Dieser Standard ist in den USA zur Verschlüsselung von Dokumenten mit der höchsten Geheimhaltungsstufe zugelassen. TrueCrypt bietet uns die Algorithmen AES [5], Serpent [6] und Twofish [7] an. Alle drei kamen in die Endausscheidung dieser Ausschreibung und wurden bisher praktisch noch nie geknackt. Kryptographen haben bisher lediglich theoretische Ansätze erarbeitet, um diese Verschlüsselungen zu durchbrechen. Ob ihre Lösungsansätze in der Praxis funktionieren würden ist unklar, denn die hierfür notwendige Rechenpower ist momentan (noch) nicht vorhanden. Die Benutzung der Algorithmen ist frei und damit jedermann gestattet.



### Einsatz von Keyfiles beim Verschlüsselungsvorgang

Als Sieger ging der in Belgien entwickelte Rijndael-Algorithmus aus diesem Wettbewerb hervor. Den Ausschlag gab letztendlich nicht dessen Sicherheit, die war bei seinen härtesten Konkurrenten

genauso hoch oder gar höher, sondern der im Vergleich einfachere Aufbau und die höhere Geschwindigkeit mit der er arbeitet.



### Der Hash-Algorithmus, der Wächter unserer Daten

Um sicherzustellen, dass sich Daten im Originalzustand befinden und nicht verändert wurden, werden sie von einem Hash-Algorithmus [8] ausgelesen und zertifiziert. Bekannt ist dieses Verfahren durch die so genannte Digitale Signatur oder die MD5-Prüfsumme, die beispielsweise abgleicht, ob aus dem Internet heruntergeladene Daten dem Original auf dem Server entsprechen und während des Downloads nicht verändert wurden.

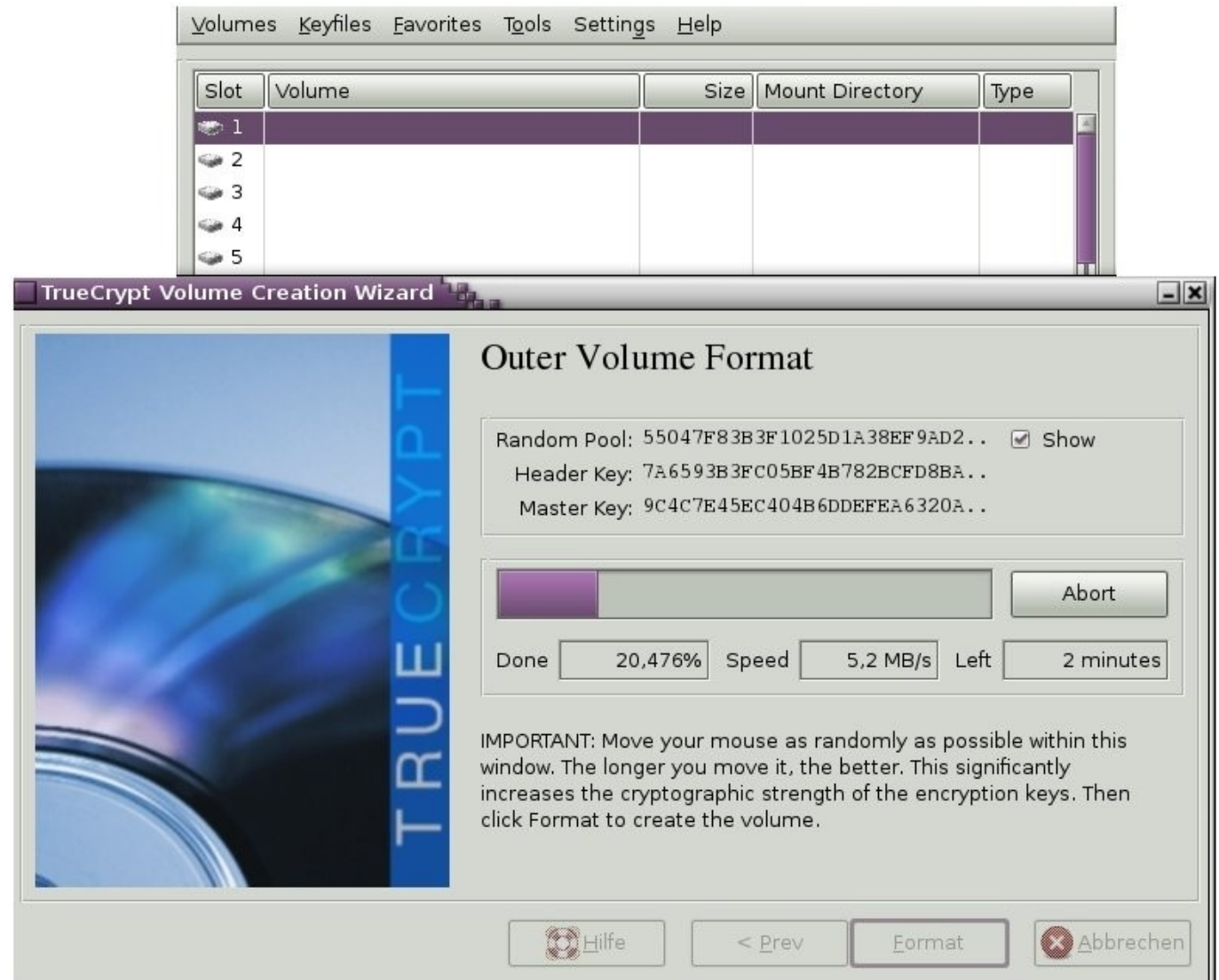
Ein weiteres Einsatzgebiet ist das Speichern von Passwörtern als Hash-Wert.

TrueCrypt bietet drei Hash-Algorithmen an. Ob nun RIPEMD-160, SHA-512 oder Whirlpool sicherer sind, darüber streiten wie auch bei den Verschlüsselungs-Algorithmen die Gelehrten.

### Einrichten eines Hidden Volumes auf einem USB-Stick

Sollten sich auf dem zu verschlüsselnden Stick wichtige Daten befinden, so sind sie vor dem Verschlüsseln zu sichern, da während des Vorganges alle Daten des Volumes gelöscht werden.

Nach dem Start des Programmes klickt man den Button *Create Volume* und belassen die Vorgabe *Create a volume within a partition/drive*. Im nächsten Fenster wählt man *Hidden TrueCrypt volume*. Per *Select Device* wählt man aus der Liste der vorhandenen Datenträger den zu verschlüsselnden USB-Stick aus. Anschließend warnt TrueCrypt un-



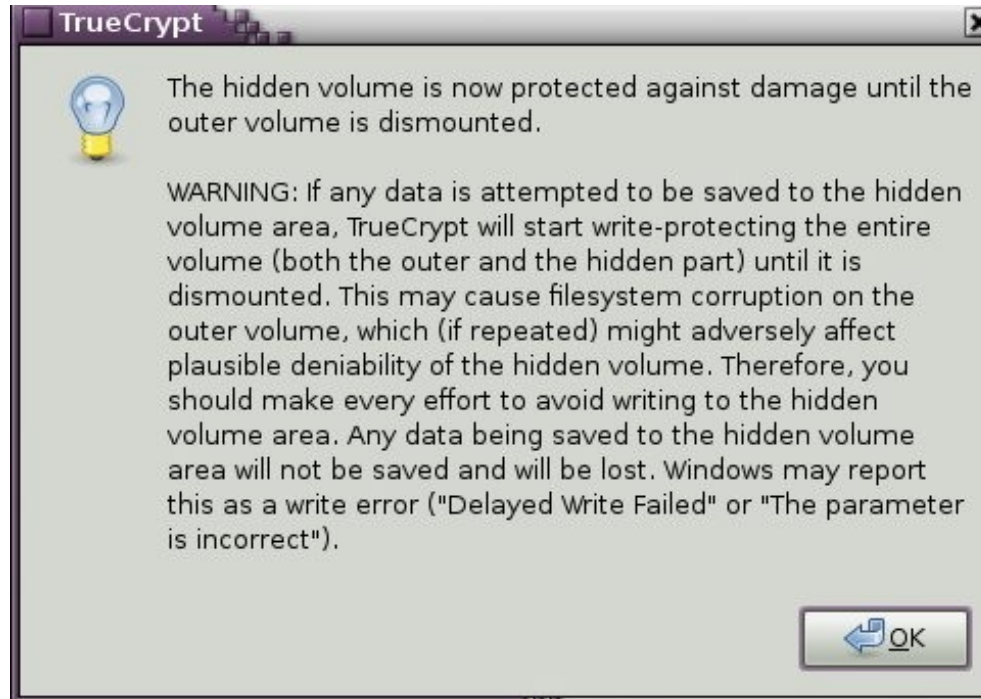
### Der Formatierungsvorgang des Outer Volume

erfahrene Anwender davor, einen gesamten Datenträger zu verschlüsseln. Man bestätigt diese Meldung mit Ja. Auch den nächsten Hinweis, dass

das Formatieren des USB-Sticks alle darauf befindlichen Daten zerstört, quittiert man mit Ja. Nun wird man aufgefordert, den Verschlüsselungs-Al-

gorithmus für das outer Volume zu wählen. Da sich hier lediglich Pseudo-Geheimdaten verbergen, belässt man die Voreinstellung AES. Nach der Wahl eines Passwortes (TrueCrypt empfiehlt mindestens 20 Zeichen) wird man aufgefordert, die Maus innerhalb eines Fensters zu bewegen. Je länger, je lieber – wir verstärken so die Intensität der Verschlüsselung. Nach einem Klick auf *Format* beginnt die Formatierung des Datenträgers. Während des Vorgangs wird man über den Status der Formatierung informiert. Nach dessen Beendigung fordert das Programm auf, das soeben erstellte outer Volume zu öffnen und sensibel wirkende Daten darauf abzulegen. Ist das geschehen, so klickt man auf *Next* und TrueCrypt weist darauf hin, dass man sich jetzt im Abschnitt inner Volume befindet.

Wieder wählt man einen Verschlüsselungs-Algorithmus aus, der dieses Mal aber etwas komplizierter sein darf. Eine Kombination von mehreren Algorithmen ist hier erste Wahl. Nachdem man den Hash-Algorithmus bestimmt hat, bestätigen man mit *Next* und sollte nun die Größe des versteckten Bereiches festlegen. Hierbei ist zu berücksichtigen, ob man zukünftig in beiden Bereichen Daten hinzufügen möchte oder ob man sich damit auf ei-



*Dem Hidden Volume bitte später keine Daten mehr hinzufügen!*

nes der beiden Volumes beschränkt. Anschließend wird man wieder aufgefordert, ein Passwort einzugeben. Dieses muss sich selbstverständlich von dem für das outer Volume gewählte unterscheiden und sollte ausreichend sicher sein. Es ist unsinnig, hohen Wert auf sichere Verschlüsselung zu legen, aber ein Passwort zu wählen, das bei einer Attacke in kurzer Zeit geknackt werden kann [9].

Um die Sicherheit der Verschlüsselung zu erhöhen, setzen wir ein Häkchen vor *use Keyfiles*. Der Klick auf *Keyfiles...* öffnet ein Fenster, in dem uns zunächst der Button *Add Files...* interessiert.

Klicken wir ihn an, so öffnet sich unser Dateimanager und zeigt uns den Inhalt unserer Festplatte. Auf dieser, oder einem anderen gemounteten Datenträger, wählen wir nun die Dateien aus, die wir zu unseren Keyfiles bestimmen möchten. Der Button *Add Path* ermöglicht es, ganze Verzeichnisse nebst Unterverzeichnissen als Keyfiles zu benennen. Die Anzahl der Dateien ist beliebig, die Dateiendungen spielen keine Rolle.

Soll zusätzlich noch ein Token eingesetzt werden, so gelangt man über *Add Token Files* in den Auswahlbereich.

Hat man die Verschlüsselung vervollständigt, verlässt man das Fenster mit OK und wird dann nach dem Dateiformat gefragt, in dem der USB-Stick formatiert werden soll. Hier sollte man, wenn er auch unter Windows genutzt werden soll, FAT verwenden. Wieder bewegt man den Mauszeiger im Fenster, diesmal darf es ruhig etwas länger sein.

Der nun folgende zweite Formatierungsvorgang geht sehr schnell vonstatten und TrueCrypt meldet, dass das Hidden Volume erfolgreich erstellt wurde. Nun können die wirklich schützenswerten Daten hierin abgelegt werden.

### Wichtig zu Wissen

Möchte man weitere Daten in das outer Volume schreiben, so kann es passieren, dass man damit

Daten im inner Volume überschreibt. Um dies zu vermeiden, klickt man beim Mounten des Datenträgers auf den Button *Options* und setzt ein Häkchen vor *Protect hidden volume when mounting outer volume*. Nun wird zunächst das Passwort für das hidden Volume abgefragt. Nach dessen Eingabe folgt das Passwort für das outer Volume. Mit Klick auf OK verlässt man das Fenster und bekommt die Meldung, dass das hidden Volume nun gegen Schäden bis zum Aushängen des outer Volume geschützt ist. Es folgt der Hinweis, dass zukünftig keine weiteren Daten mehr in das inner Volume geschrieben werden sollen. Falls doch, kann sich die Dateistruktur verändern und die Existenz des hidden Volume wird sichtbar! Und das sollte man natürlich unbedingt vermeiden!

### Sichern der Volume Header

Da es auf dieser Welt nichts gibt, was nicht kaputt gehen kann, ist es sinnvoll, den Vorspann (Header) der verschlüsselten Dateien zu sichern. Sollte dieser auf unserem USB-Stick beschädigt werden, so ist ein Backup des Headers die einzige Möglichkeit, um wieder an die eigenen Daten zu gelangen.

Zunächst muss man den Datenträger aushängen (*Dismount*). Über *Tools – Backup Volume Header* öffnet sich ein Fenster, das die Reihenfolge der Passwort-Eingabe erläutert. Zunächst gibt man das Passwort für das outer Volume ein. Die Frage: *Does the volume contain a hidden volume?* beantwortet man, indem man *The volume contains a hidden volume* anklickt. Nachdem man mit *OK* das

Fenster verlassen hat, wird man zur Eingabe des Passworts für das hidden volume aufgefordert. Danach setzt man wieder ein Häkchen in *Use keyfiles*, klickt auf *Keyfiles* und nennt dem System die von uns verwendeten. Die Frage, ob der die Header nun gesichert werden soll bestätigt man mit *OK* und wird aufgefordert, einen Speicherort und den Namen, unter dem der Header gespeichert werden soll, zu benennen. Anschließend ein Klick auf *OK* und man ist fertig.

### Besonderheiten

Wer ganz geheim unterwegs ist, sollte wissen, dass, auch wenn man einen verschlüsselten Datenträger bereits ausgehängt hat, sich die zuletzt aufgerufenen Daten noch im Arbeitsspeicher respektive im Swap-Speicher befinden können.

Selbst wenn man den PC ausgeschaltet hat, bleiben die Daten noch für einige Zeit im Arbeitsspeicher erhalten und sind von dort noch auszulesen.

### Die Zukunftsaussichten

Es steht zu hoffen, dass TrueCrypt in absehbarer Zeit auch komplette Systempartitionen – wie unter Windows bereits möglich – verschlüsseln kann. Dies erfolgt dort im laufenden Betrieb [10]. Zum Systemstart wird ein Bootloader vorgeschaltet, der eine Pre-Boot Authentication (Identifizierung vor dem Hochfahren des Computers) fordert; ohne diese ist das Betriebssystem nicht zu starten. Sehr wichtig ist in diesem Falle die Erstellung einer bootfähigen Rettungs-CD, die bei Beschädigung des Bootloaders dazu dient den Rechner zu starten.

Auch über den Traveller-Mode würde sich die Linux Gemeinde sicherlich freuen. Dieser ermöglicht es, mit TrueCrypt verschlüsselte Datenträger auf fremden Rechnern zu öffnen, ohne dass das Programm dort installiert sein muss.

Jürgen Weidner

[joschi@yalmagazine.org](mailto:joschi@yalmagazine.org)

### Informationen

- [1] <http://www.yalmagazine.org/homepage/yalm/download>
- [2] <http://www.truecrypt.org/>
- [3] <http://www.truecrypt.org/docs/>
- [4] <http://de.wikipedia.org/wiki/Security-Token>
- [5] <http://www.korelstar.de/informatik/aes.html>
- [6] <http://www.repges.net/AES-Kandidaten/Serpent/serpent.htm>
- [7] <http://www.repges.net/AES-Kandidaten/Twofish/twofish.htm>
- [8] <http://www.heise.de/security/Konsequenzen-der-erfolgreichen-Angriffe-auf-SHA-1-/artikel/56555>
- [9] <http://www.techsupportforum.de/howto-allgemein/10043-sicheres-passwort.html>
- [10] [http://www.heise.de/software/download/special/windows\\_verschluesseln/26\\_1](http://www.heise.de/software/download/special/windows_verschluesseln/26_1)



# Schlussbemerkingen

Yalm ist ein privates, nichtkommerzielles Projekt. Die Zeitschrift erscheint am dritten Sonntag eines Monats.

Rückmeldungen zu unserem Magazin – seien es Artikelwünsche, Verbesserungsvorschläge, Lob oder auch Kritik – sind herzlich willkommen. Schreibt einfach an [redaktion@yalmagazine.org](mailto:redaktion@yalmagazine.org) oder postet in unserem Forum auf <http://www.yalmagazine.org/forum>.

Wir suchen immer engagierte und zuverlässige Helfer, die bei unserem Magazin mitarbeiten wollen. Nicht nur Layouter mit guten OpenOffice-Kenntnissen und natürlich Autoren sind gerne gesehen, sondern auch Programmierer und Entwickler sind herzlich eingeladen, bei Yalm mitzumachen. Schreibt uns bei Interesse bitte eine E-Mail an [redaktion@yalmagazine.org](mailto:redaktion@yalmagazine.org) oder seht euch für weitere Details die Rubrik »Mitmachen« auf unserer Homepage an.

## Layout

Yalm wird mit OpenOffice erstellt; die Bearbeitung und Korrektur der Texte erfolgt jetzt in unserem Dokuwiki. Die jeweils gültige Dokumentvorlage kann von der Yalm-Homepage (Rubrik »Extras«) [heruntergeladen](#) werden.

## Listings und weiterführende Informationen

Layoutbedingte Zeilenumbrüche werden mit einem Pfeil → dargestellt. Eventuell notwendige Leerzeichen stehen vor diesem Pfeil.

Weiterführende Informationen, Listings und Dateien zu einzelnen Artikeln werden in der Rubrik »Extras« der Yalm-Homepage zum Download angeboten.

## An dieser Ausgabe haben mitgewirkt:

Bernhard Posselt (Autor, Korrektur)  
 Frank Brungräber (Layout, Korrektur)  
 Heiko Andresen (Korrektur)  
 Jan Guth (Korrektur)  
 Jan Radecker (Autor, Korrektur)  
 Jürgen Weidner (Autor, Korrektur)  
 Mario Fuest (Layout, Korrektur)  
 Matthias Haupt (Korrektur)  
 Peter Majmesku (Autor, Korrektur)  
 Stefan Zaun (Autor, Korrektur)  
 Thomas Rudolph (Autor, Korrektur)

## Lizenz

Yalm wird unter der [Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 3.0 Deutschland Lizenz](#) veröffentlicht.



Kurz: Yalm-Ausgaben oder einzelne Artikel dürfen kopiert, verbreitet und öffentlich zugänglich gemacht werden; die Inhalte dürfen abgewandelt und bearbeitet werden. Voraussetzung hierfür ist, dass sowohl der Autor als

auch Yalm genannt werden und die Weitergabe unter den gleichen Lizenzbedingungen erfolgt.

## Redaktion und Homepage

Kontakt: [redaktion@yalmagazine.org](mailto:redaktion@yalmagazine.org)

Yalm-Homepage: <http://www.yalmagazine.org>

V.i.S.d.P.: Tobias Kündig

Sagenblickweg 6

CH-6030 Ebikon

[tobias@yalmagazine.org](mailto:tobias@yalmagazine.org)

## Bildquellen

Die Inhaber der Bildrechte werden in den Bildunterschriften oder in den Artikelinformationen genannt. Für den Fall, dass die Verwendung eines Bildes nicht zulässig oder gewünscht ist, bitten wir um eine kurze Information; wir werden es dann umgehend entfernen.

Die Verwendung des [WeeChat-Logos](#) wurde von [FlashCode](#), Initiator und Entwickler des Projekts, genehmigt. Das [Evolution-Icon](#) wurde dem »[Tango Desktop Project](#)« (Version 0.3.1) entnommen und unterliegt den [CC-BY-SA 2.5](#). Das [OpenTTD-Logo](#) unterliegt der GPL v.2 und höher.

*Yalm 04/2009 erscheint  
am 19. April 2009*

Yalmagazine.org wird von [NETzor.de](#) gehostet.