# PCLinuxOS Magazine

Issue 6 • February, 2007 • http://www.pclinuxos.com

**Announcements:**

Test Release 1 is OUT!

**HowTo:**

Change A Lightscribe Label

Use Desktop Shortcuts Effectively

Split (and Rejoin) A File

## Parental Control

by newmikey

## Using Tor Connectivity

by Tim McCormack

## Limewire/Frostwire

by Scooter

## Setting Static IP Address

by Stumpy842

## A Tale Of Too Many Distros

by Wayne Whitman

## Acquiring and Installing VMWare

by vampirefo/Tim Robinson

## Using Fish

by Daiver Pedemonte

# From the Desk of the Chief Editor

*Welcome to the February 2007 issue of PCLinuxOS Magazine. We've had lots of help from people on the main PCLinuxOS forum and the result is a number of excellent how-to articles.*

*There is a review and how-to on Dansguardian for those of you with children whose Internet experience you wish to control. We have an in depth follow-up to my short how-to on using Tor to browse anonymously. There's a step by step tutorial on acquiring and installing VMWare, and much more.*

*As promised last month, this issue contains a "treasure hunt." Last month we placed yellow dots with letters in them on some of the graphics. The key was short and many people figured it out easily. This time, the "keys" are letters, numbers, punctuation, and hidden in plain sight in the text of the articles. Like this. Look for red characters on a yellow background. Be aware that the key is a phrase, not a single word, and may contain punctuation and/or spaces. Note that NONE of the characters on yellow background in this editorial are part of the real key. Remember that capitalization is important.*

*Read the articles, write down the key characters as you find them, then organize them into a phrase. Then visit http://mag.mypclinuxos.com/hunt/script/ and enter your guess. If you guess wrong, you may try as many times as you wish. The first person to get it right wins a copy of PCLinuxOS p.94 from OnDisk.Com. The winner's screen name (only) will be announced in the Magazine's thread on the main forum.*

*While it's all great fun to hunt the key and enter your guess, please take time while you are at the treasure site to provide us some information about yourself. No personally identifiable information is collected at the site (except for your email address if you are the winner). We need the information requested so we can do a better job serving the PCLinuxOS community. Lastly, no members of the Magazine volunteers and their immediate family can join the hunt. Thanks.*

## Late breaking news!

*On January 21, 2007, version p .94 RC1 was released. Your magazine staff was ready and produced an Extra edition in record time. Thanks gang. Next month's issue (released March 1, 2007) will have in depth reviews of all the goodies, screen shots of the cool 3D graphics, explanations of the new menu structure, and all the scoop on this gem. Look for next month's issue. It'll be worth the wait, just as PCLinuxOS p .94 was.*

**Tim Robinson**

PCLinuxOS Magazine is a community project of MyPCLinuxOS.com to provide an additional means of communication to the PCLinuxOS community.

**Project Coordinator:** Derrick Devine
**Publisher:** MyPCLinuxOS.com
**Contact:** mag@mypclinuxos.com

**Chief Editor:** Tim Robinson

**Senior Editor:** Rodney Adkins

**Editors:** Seán Leamy, Neal Brooks, John Paxton

**Proofreaders:** Doug Wilson, Seán Leamy, Jan Allen, Danny Crane, Guy Tayler, James La Rue, Duane Trudeau, DaveDave, MeeMaw, Jared

**Contributors:** newmickey, Tim McCormack, kolosus, johncoom, Scooter, Stumpy 842, Wayne Whitman, vampirefo and Tim Robinson, Ferdi, Daiver Pedemonte

**Treasure Site:** Tim Fielding
**HTML Codes:** Galen

**Page Layout & Graphics:** Archie Arevalo

**Home on the Net:**
http://www.pclinuxos.com/forums/
http://www.mypclinuxos.com

# Announcement: PCLinuxOS 2007 Test Release Out!

Texstar announced the release of PCLinuxOS 2007 Test Release 1 on January 21, 2007.

Disclaimer -This is experimental software. Use at your own risk. PCLinuxOS cannot be held liable under any circumstances for damage to hardware or software, lost data, or other direct or indirect damage resulting from the use of this software. If you do not agree to these terms and conditions, you are not permitted to use or further distribute this software.

## PCLinuxOS 2007 Test Release 1

PCLinuxOS 2007 Test Release 1 is now available for download. Please note this is not the final release. PCLinuxOS 2007 Final will be released at the end of the month.

### Features include:

* Kernel 2.6.18.6-dev3
* KDE 3.5.6
* Mozilla Firefox 2.0.0.1
* Flash 9
* Mozilla Thunderbird 1.5.0.9
* Open Office 2.1.0
* Xorg 7.1
* Beryl, Compiz, Aixgl and Xgl for 3D graphics support
* Gcc 4.1.1 and updated glibc
* Updated bootsplash, icons, and more from the mypclinuxos.com beautification project.
* Xdg Menu system
* Rebuild and update of our entire repository against new gcc and glibc
* Simplified Livecd boot options.

### Livecd boot options:

* Livecd - Default boot options
* Frambuffer - Boot using generic video drivers (Proprietary drivers available after install)
* Safe - Turns off most hardware probing
* Mediacheck - Test the media to determine a good burn to cdr
* Memtest - Test your computer memory

Installation is done through the root account. Login with root as the username and root as the password then click on Install PCLinuxOS to start the installer. Help with installation is also available on the dekstop. PASS users will get a new email on or about February 15th for access to our premium server. 4-5 public software mirrors are currently available for this test release.

### Known Issues:

* Alsa sometimes gives harmless warning at shutdown (fixed with kdebase update from Synaptic)
* Synatpic doesn't allow one to re-install already installed software
* Missing some wireless firmware for various wirelss cards.
* 3D support is still experimental and doesn't work with all video cards yet.
* Missing a lot of applications in the repository. We will be adding more as time allows.
* Menu editor gets wonky from time to time.

The iso you want to get is called livecd.iso

### Download Mirrors:

http://ftp.ch.debian.org/mirror/pclinuxos/live-cd/english/preview/
http://ftp.heanet.ie/pub/pclinuxos/live-cd/english/preview/
http://ftp2.be.freesbie.org/packages/pclinuxos/live-cd/english/preview/
http://ftp.ussg.iu.edu/linux/pclinuxos/pclinuxos/live-cd/english/preview/

Other mirrors were posted on
http://www.pclinuxos.com/forum/index.php?topic=15044.msg119571#msg119571

Please post your bug reports here,
http://www.pclinuxos.com/forum/index.php?topic=15045.0

# Parental Control
## (or how to provide a safe computer environment to your children)

by newmickey

I have two children, aged 10 and 11. Both were introduced to the Internet when they entered primary school. As they advanced through the grades the Internet has changed from a playground into a research source for projects, book reviews, and technical information. From the beginning, my wife and I have wondered how to protect our young children from the inherent dangers of this Global Community, and how to ensure that the content available to them would match their degree of development.

When they were very young, the solution was easy. The various tweaks to system files that enable access to only a few (up to 10) websites were easily executed and did not need to be adjusted too often. As the children grew older, their window on the world widened, and it rapidly became impossible to limit their view without damaging their scholastic advance.

One of the first things always has to be to educate your kids, make them understand how they should behave and, more importantly, how they should definitely NOT behave.

So they have been drilled on the standard, a standard you would be surprised to discover not many parents adhere to. Never give away personal details, use a nickname as an email address, and do not use your friends' real names when chatting or MSN-ing. Keep your password secret; do not let anyone else (even your brother or sister) log in under your name etc, etc. There is a long list of very common sense rules and the kids will gladly follow them if they understand exactly why.

That is why, early in 2005, I started looking at ways to filter unwanted and abusive content, while not limiting the reach and creativity that children need to develop. I found all kinds of programs for Windows, ISP's that offer specific "kids" accounts with server-based filtering and a few Open Source projects.

It so happens that from the beginning I disabled access to the network card in Windows (hardware manager) and taught them that they should use Linux if they wanted to go on the Internet. Therefore, Windows programs like NetNanny were out of the question (and expensive).

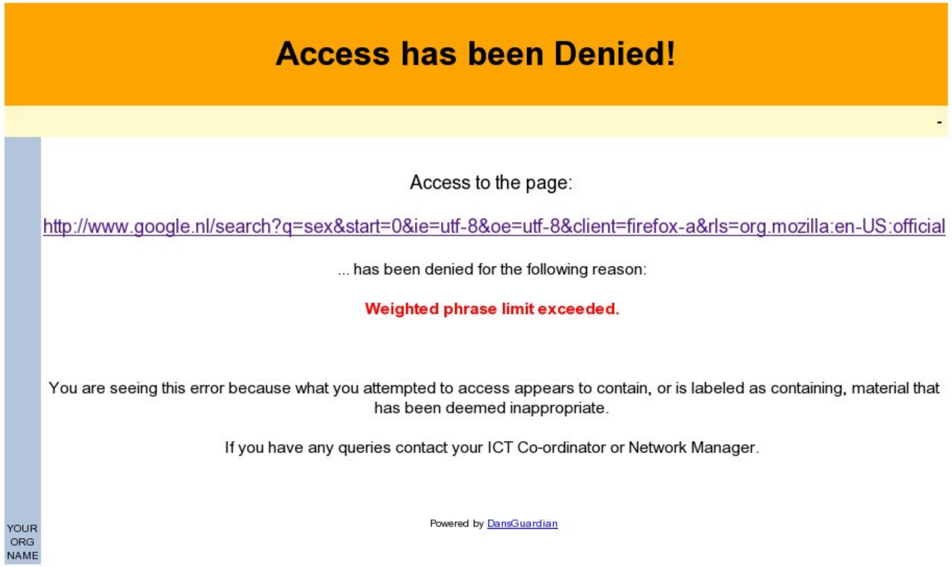
Basing the protection of my children on someone else's opinion of right and wrong seemed not to coincide with our view of limited freedom of information, where "limited" is understood to mean "anything as long as it is not damaging." So letting the ISP decide what my kids would see, was definitely not the way to go either.

I finally settled on DansGuardian, an Internet filter that has multiple ways to avoid presenting unwanted content to your kids. It has blacklists and whitelists, that either completely block or completely allow access to complete domains (websites). It also filters out images that are found to be unfit for children. It has dictionaries for swear words, discriminating phrases, porn, and other categories. Every web page is scanned for these words, before it is rendered on the screen. If one of these "forbidden" words is found, the page is replaced by a message that states that the page is unavailable. This technique is also called "dynamic content filtering".

What impressed me most, however, is the ability of DansGuardian to apply a weighted combination of words and make the resulting score decide whether or not to block a page. What does this mean in practice? Well, let's just say you do not want your children to have access to pages that contain sexually explicit stories or pictures. How does one prevent that? Nowadays, Googling on a subject like Barbie, or pussycat, will land you one result about the famous doll or an adorable feline, and thousands of referrals to websites that would make anyone blush.

So put the word "sex" in the list of forbidden words? That may sound like an easy solution, but, it will also block sites like special children's encyclopedia, school biology lab, and national health department, where information is offered about sex on a level and in a way that is specially targeted at and designed for a healthy sex education. The beauty of DansGuardian is that it offers a way out of this dilemma. DansGuardian allows the school biology lab to educate, national health department to warn and inform, and the encyclopedia to offer its content by comparing a total score of words found, to a maximum set by the parent.

The score can be increased by words or combinations of words, but also decreased by other words. So, just as an example, the word "sex" would add 10 points to the total score, but the combination of the words "health" and "childbirth" would take 10 points off the score. The whole page is scanned this way for several different categories of objectionable content, and if the resulting total is over a certain minimum, the page is blocked.



Access has been Denied!

-

Access to the page:

http://www.google.nl/search?q=sex&start=0&ie=utf-8&oe=utf-8&client=firefox-a&rls=org.mozilla:en-US:official

... has been denied for the following reason:

Weighted phrase limit exceeded.

You are seeing this error because what you attempted to access appears to contain, or is labeled as containing, material that has been deemed inappropriate.

If you have any queries contact your ICT Co-ordinator or Network Manager.

Powered by DansGuardian

YOUR ORG NAME

I hear you say, "my kid is so smart, he will find a way to circumvent this limitation in no time!" I can give you at least some reassurance, my 10 year old son is computer-smart, Linux-smart and technically savvy. He has given up trying. I am sure he will probably break DansGuardian by the time he is 18, but by then, I shouldn't be trying to limit his access anyway.

Is Dansguardian, alone and by itself, capable enough to make sure no access is allowed through other means? No, you need a mechanism that makes sure all Internet access is routed through DansGuardian, regardless of the browser type or settings. The solution to that is to use DansGuardian in combination with Squid, as a so-called "transparent proxy". This will force every attempt to send or receive content over computer port 80 (the http protocol), through DansGuardian's never-sleeping word filter.

Will you have no work at all after that? I would never advise anyone to totally leave the protection of their kids to a piece of software. I tend to review the log files DansGuardian creates once in a while, not to "spy" on the kids, but to make sure nothing is amiss, filtering is adequate, and the "page-score" is adjusted up or down when necessary. I also spend a lot of time with them on the PC, teaching them how to search, what to look for, and how to make sure information retrieved is reliable.

Is it easy to install the above combo? No, at least it wasn't for me. It took me hours, no, nights of puzzling and reading on websites to get it setup the correct way. I hope that the following recipe will allow you to "cook" your kids a wonderful serving with less effort. They will appreciate the extended reach you will be allowing them and you will enjoy the feeling that your kids are protected. The recipe calls for good quality, fresh ingredients. It is therefore advised that you use PCLinuxOS!

**Recipe:**

Take 1 ripe PCLOS installation, and add:
a generous portion of well marinated swap (2GB),
a sniff of games to taste,
two teaspoons of educational packages,
rpm's to taste.
Stir slowly, bring to a boil on a medium heat and...

Make sure your Synaptic is seasoned with the required packages, you need the regular repository and a separate repository called Thac, after its founder, for the Webmin package. For information on how to add Thac as a package source, look here: http://www.pclinuxos.com/forum/index.php?topic=5605.0

**WARNING:** `While the Thac repository is enabled, install` **`ONLY`** `the Webmin package. After it is disabled, install the other packages.`

Add the following packages that are available from Synaptic (keep stirring constantly):

1. Dansguardian
2. Squid
3. perl-Compress-Zlib
4. IpTables

Now lower the flame and download the following package: dg-0.5.10-pr4.wbm (Dansguardian webmin module) from

http://sourceforge.net/projects/dgwebminmodule/

According to the instructions found at:

http://software.newsforge.com/article.pl?sid=04/06/23/1521209&tid=92&tid=2&tid=27&tid=13&tid=31

Edit (as root) /etc/squid/squid.conf and add if needed:

```
http_port 127.0.0.1:3128
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
cache_effective_user squid
cache_effective_group squid
```

Edit (as root) /etc/dansguardian/dansguardian.conf and add if needed:

```
reportinglevel = 3
filterip = 127.0.0.1
filterport = 8080
proxyip = 127.0.0.1
proxyport = 3128
daemonuser = 'squid'
daemongroup = 'squid'
```

Add (as root) the following lines to /etc/rc.d/rc.local:

```
iptables -t nat -A OUTPUT -p tcp --
dport 80 -m owner --uid-owner squid -
j ACCEPT
iptables -t nat -A OUTPUT -p tcp --
dport 3128 -m owner --uid-owner squid
-j ACCEPT
iptables -t nat -A OUTPUT -p tcp --
dport 80 -m owner --uid-owner root -j
ACCEPT
iptables -t nat -A OUTPUT -p tcp --
dport 80 -j REDIRECT --to-ports 8080
iptables -t nat -A OUTPUT -p tcp --
dport 3128 -j REDIRECT --to-ports 8080
```

Start PCLinuxOS Control Center (PCC) and navigate to System Services

1. Set Squid to start at boot
2. Set Dansguardian to start at boot
3. Disable Shorewall
4. Set Webmin to start at boot
5. Set Iptables to start at boot

If you do not wish to turn off Shorewall (firewall), then you need to add the above 5 lines (that start with "iptables") to /etc/shorewall/start and

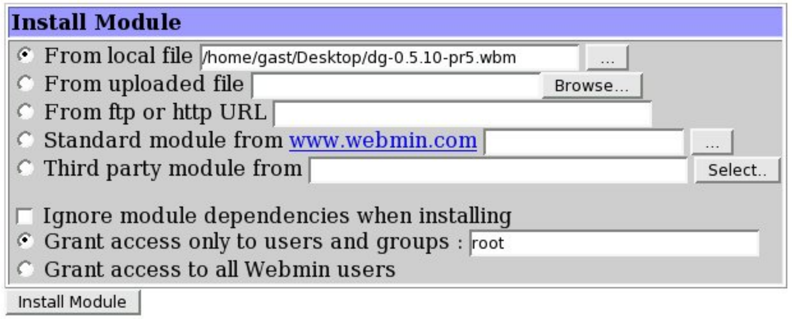
/etc/shorewall/stop, just in case you have to stop Shorewall for some reason, your filters will continue running.

Make sure your PC has a so-called "hostname", otherwise the various ingredients of this recipe will not lead to a satisfactory result and leave a bad taste. You can set the "hostname" by opening the PCLinuxOS Control Center and enter the tab "Networking", section "Configure DNS settings." Set a qualified hostname. You can invent something fancy but "mypc.mynetwork.net" will do fine for now.

You can now install the DansGuardian-webmin-module in Webmin by surfing to

```
https://localhost:10000/webmin/edit_mods.cgi
```

and choosing "Install module from local file." Point at the module you downloaded (probably on your desktop) and click "Install Module."



**Install Module**

● From local file /home/gast/Desktop/dg-0.5.10-pr5.wbm
○ From uploaded file
○ From ftp or http URL
○ Standard module from www.webmin.com
○ Third party module from

□ Ignore module dependencies when installing
● Grant access only to users and groups : root
○ Grant access to all Webmin users

In order to make this dish look more refined, garnish with a Konqueror Desktop link to the DansGuardian module of Webmin by using this URL:

```
https://localhost:10000/dansguardian
```

so that you can examine logfiles and change settings (as root of course!)
You may need to adjust the "forbidden" words lists and scores, depending on where you live. I find the standard settings much too "prudish" for a European taste. On the other hand, I needed to reinforce protection in other categories.

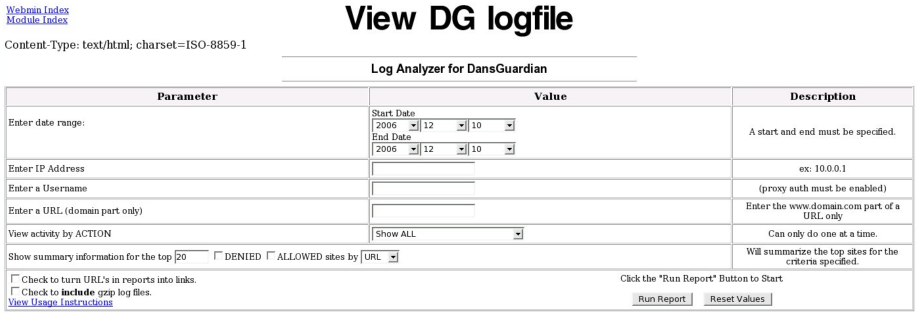
You can either access DansGuardians settings through the Webmin module or edit them with any text editor like Kwrite, Kate or Kedit. You will find all of the blacklists, whitelists, and weighted words in several languages in /etc/dansguardian.
Do remember that you have to restart the services,

after any edit of a DansGuardian file, in order for the changes to take effect. This could be done in a terminal, as superuser:

```
/etc/rc.d/init.d/squid restart
/etc/rc.d/init.d/dansguardian restart
/etc/rc.d/init.d/iptables restart
```

or from the DansGuardian webmin module in your favorite browser with the URL `https://localhost:10000` (Note the extra "s" after http. It indicates a secure connection).

Have a look at some websites, good and bad. Note when you are blocked when you shouldn't be or not blocked when you should be. Now have a look at the logfiles.



Webmin Index
Module Index

View DG logfile

Content-Type: text/html; charset=ISO-8859-1

Log Analyzer for DansGuardian

| Parameter | Value | Description |
|---|---|---|
| Enter date range: | Start Date<br>2006 ▾ 12 ▾ 10 ▾<br>End Date<br>2006 ▾ 12 ▾ 10 ▾ | A start and end must be specified. |
| Enter IP Address | | ex: 10.0.0.1 |
| Enter a Username | | (proxy auth must be enabled) |
| Enter a URL (domain part only) | | Enter the www.domain.com part of a URL only |
| View activity by ACTION | Show ALL ▾ | Can only do one at a time. |
| Show summary information for the top 20 □ DENIED □ ALLOWED sites by URL ▾ | | Will summarize the top sites for the criteria specified. |
| □ Check to turn URL's in reports into links.<br>□ Check to **include** gzip log files.<br>View Usage Instructions | Click the "Run Report" Button to Start<br>Run Report Reset Values | |

They will show you the exact wordscores that led to the above results. I found that increasing the blocking threshold got rid of a lot of false results. You will soon find the perfect combination for your children's age and your local cultural habits. I wish you and your children a healthy, happy and safe 2007.

# Using Tor Connectivity (Anonymous Browsing Edition)

by Tim McCormack

*Reprinted with permission of the author*

*http://www.brainonfire.net/2006/10/21/tor-best-practices-anonymous-browsing/*

Tor is a popular system for sending Internet traffic anonymously. It is mainly used for three purposes: hiding one's identity, hiding the identity of the site one is visiting, and hiding the data that one is sending and receiving. However, using Tor without some basic precautions is worse than not using Tor at all, leading to privacy violations, data theft, and security concerns. Here, I cover browser security with respect to preventing identity and data leakage when using the Tor network. If you are only using it to defeat web filtering, feel free to read only the section called "Locking yourself down."

At the end is an executive summary. Use it as a guideline, but make sure to read this entire article first -- it contains important instructions on how to change your browsing habits.

## Security is a mindset

Anonymity, security, and privacy are not all-or-nothing. Each is a continuum, and the goal of the security-conscious individual is to move a reasonable distance towards the secure end of the spectrum. How far an individual decides to go depends on the specific circumstances: the importance of the data or identity being protected, the consequences of a breach, the likelihood of an attack, the resources of the attacker, and the resources of the individual. In this guide I am concentrating on defeating automated attacks by a casual attacker. Anything  beyond that likely falls outside of the realm of Tor security, and more into the realm of application, data, and physical security. Besides, it would be silly to put in place any security measures more robust than Tor itself -- remember that Tor is experimental software.

I will first discuss the Tor threat model, and only then provide suggestions as to how to alleviate threats. You need to understand the system you are using before you can really rely on it, otherwise you will develop a false sense of security. So hang in there.

## What you need to know about Tor

Tor uses a client-peer model. The client is what you install on your computer. It accepts connections from other programs on your computer (such as web page requests from your browser) and sends the data out to the Tor network. (Any responses also come back through the Tor client.) Note that the Tor client is data-blind, meaning that it does not check the data flowing through it for potential identity leaks or malware.

Any program that wants to use the Tor network has to be configured to do so.

## Simply installing the Tor client is not enough

Each of the peers is a computer like your own, but running an extra part of Tor: the server. These computers are referred to as "nodes" or "onion routers", and your data flows through them. When data leaves the Tor client, it passes through a randomly predetermined chain of these nodes. Due to the Tor algorithms, each node only knows who is immediately before and after it in the chain. Only the first one knows who you are, and only the last one knows where your data is going. Only the last one (the "exit node") can read the data you are sending out. Note that it can also alter the data you are sending and receiving. Therefore, the trustworthiness of the websites you contact is not relevant, since the data you and they send has to pass through an untrusted third party.

## Threat model

Attacks can be launched against the Tor network itself, such as timing attacks, but we're not concerned about that here. The goal is to secure the data that is flowing through the pipes, and let the Tor programmers secure the pipes themselves. Here are the threats you need to be concerned about:

* Personally identifiable information (PII) that you send out,

* Code sent to you that will reveal your identity from inside Tor, and

* Code sent to you that will reveal your identity from outside Tor.

## Locking down Firefox

Make sure you have the latest stable version of Mozilla Firefox installed. Older versions have known security holes.

For several reasons, you should create another Firefox account. (Another reason is to keep you mindful of when you are using Tor and when you are not.) The best way of doing this is to create another user on your computer specifically for Tor browsing. If you can't do that, learn how to use the Firefox profile manager. The rest of these instructions will assume you are using that new Firefox account.

## Locking yourself down

Ultimately, you are the weakest link in the chain of security. Here's the proper mindset for browsing through Tor: Assume that the URLs of the pages you ask for and any data you send or receive is being broadcast to the entire world. Assume that the exit node has secretly altered the page you are looking at, or even altered your request to secretly go to a different website. Since the data you send and receive can be altered and read by an untrusted third party, how can you do anything at all? There's one trick that will defeat a malicious exit node: SSL. When a page's URL begins with https://, that means that SSL is in effect. SSL prevents the exit node from reading the data going back and forth or altering it. (It can only see three things: the site you are talking to, the timing of the data, and the size of the data.) If you visit a site and the browser tells you that the SSL certificate may be invalid, don't trust it! If there is any doubt about the authenticity of the SSL certificate, pretend the site is not using SSL at all, and act accordingly.

This means never log in to a site if the login does not use SSL. Otherwise, your password will be stolen.

Just to be on the safe side, turn on warnings for secure and insecure sites. At the Firefox configuration URL (type `about:config` into the address bar and press Enter), find the keys beginning with `security.warn_`. Set all of them to `true`, except for the ones ending in `.show_once`, which should be set to `false`. Then set `security.warn_entering_secure` to `false` -- you really don't need to be alerted to that.

I recommend installing a theme from mozilla.org that is somewhat different from your usual theme. This will help you remember that you are using Tor (and should therefore browse defensively.)

Additionally, if you are using Tor for anonymity... don't send any information that can identify you. Don't use your real name or email address, for instance.

## Keeping PII out of the data

Now that you have a clean slate to work from, let's make sure it doesn't get dirtied up. In Firefox, open the Preferences window (Mac: `Firefox->Preferences`, Linux: `Edit->Preferences`, Windows: `Tools->Options`.)

Websites are allowed to store bits of information (called "cookies") on your computer, so they know who you are when you come back. This is great for regular browsing, but not when you want to dissociate from your real identity. (A website might notice that your real identity and Tor identity are using the same cookie, meaning you're the same person.) Since you've already created a new Firefox account, you won't need to worry about crossover. However, you do have to worry about cross-site cookies. Under Preferences->Privacy->Cookies, allow cookies for the originating website only, and have them kept only until Firefox is closed. You may wish to disable cookies altogether, and use the Exceptions button to allow specific sites.

## Remove internal leaks

Leaks within the Tor channel are generally caused by plugin technologies such as Java and Flash. These can share information about you across sites, and more importantly they know your real IP address and can communicate this back to their home server. Install the following extensions from mozilla.org:

* FlashBlock: Blocks Flash objects by default.

* NoScript: Block javascript and plugins, allow selectively. In the NoScript options, disallow everything (for now). Disabling Java here is equivalent to disabling Java in the Firefox Preferences window.

## Remove external leaks

Webpage requests are not the only data that are sent out when you visit a URL. Your browser also has to determine what the IP address of the server is, a process called DNS resolution. To force DNS requests into the Tor channel, visit the special URL about:config and find the key `network.proxy.socks_remote_dns`. Set it to `true`.

## Summary

(I sure hope you read all the stuff above this and didn't just skip down here right away.)

1. Create a new Firefox account (use the profile manager or a new user account in your OS)

2. Assume someone is maliciously reading and altering everything not sent through an https:// connection with a good certificate.

3. In `about:config`, turn the `security.warn_*` alerts on, and the one-time options off.

4. Set the `about:config` property `network.proxy.socks_remote_dns` to `true`.

5. Use a different Firefox theme.

6. Allow cookies for the originating site, and only until Firefox is closed. You might turn cookies off.

7. Install the FlashBlock and NoScript extensions, and configure them to disallow everything.

Oh, and now would be a good time to install the TorButton extension, configure it to display the way you like, and turn it on. Once you've done that, go to `Preferences->Privacy` and use the `Clear Private Data` tool.

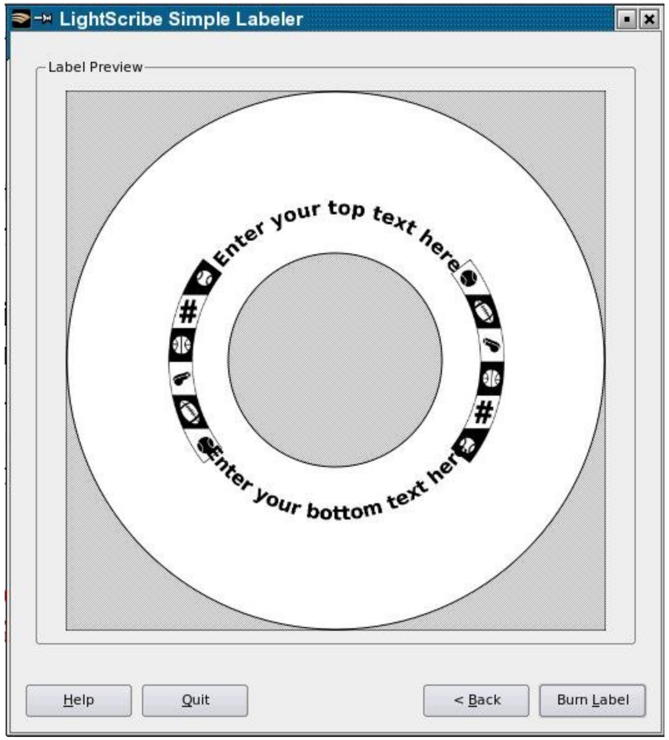
This set of guidelines is not complete, but following it will probably put you ahead of the majority of Tor users. Armed with some knowledge of how the Tor network functions, you will be able to make better choices. Safe browsing!

# How To Change A Lightscribe Label

by kolosus

This article assumes that you have the SimpleLabeler program installed on your computer and know how to open it.

Once SimpleLabeler is opened, you are given a sample of thumbnails to chose from. Click the last one (you could use any other one, but for this example & for convenience we will use the last one) named 'Good Sports'. Click on 'Next'. The program will show 'Generating Preview' and then the preview will be shown. Do not burn the label! This is your template. It will show you how the 'Good Sports' template looks.



Go to folder:

```
/opt/lightscribeApplications/SimpleLabeler/content/images/borders/fullsize
```

That is the folder SimpleLabeler is installed to by default. There you will find an image named 'fs00008.png'. Open it. I used KolourPaint, but you could use any program you want. I'm not familiar with Gimp. It is just overkill for what I had in mind.
Once opened, you will see the label

layout. You will probably have to zoom out to see the image properly. Here you can place any image that you want. I inserted the PCLinuxOS logo. Going back and forth to ● the SimpleLabeler program and to your image manipulator program, you can lay out your label the way you want it. The only limits are your imagination and the program you are using.

Once you have the layout the way you wish, erase the default borders that come with the template (unless you want them to stay). Convert the image to greyscale, if your label is in color. This improves the labeling contrast greatly. Save the image in your `/home` folder as "`fs00008.png`".

Now comes the part where we trick SimpleLabeler. Rename the original file '`fs00008.png`' to something like '`fs00008.bak`'. Place the label that you created in the folder

`/opt/lightscribeApplications/SimpleLabeler/content/images/borders/fullsize`.

It will take the place of the original label.

Go back to SimpleLabeler and do the label selection process again. Be sure to select the 'Good Sports' thumbnail. This time when it shows you the generated preview, it should be of the label you created.

Viola!! Burn it!

If the preview is not of the label you created, then there was a problem. Retrace your steps.

It is quite possible the contrast of the first burn of the label may not be to your liking. The dye used on your media and the intensity (and age) of your burner are usually the cause. If you do successive burns you might want to remove any text, as otherwise they would be darkened too and the contrast of the image will always be trying to catch up to a moving target. On successive burns the images should align perfectly. They did for me and I've done many.

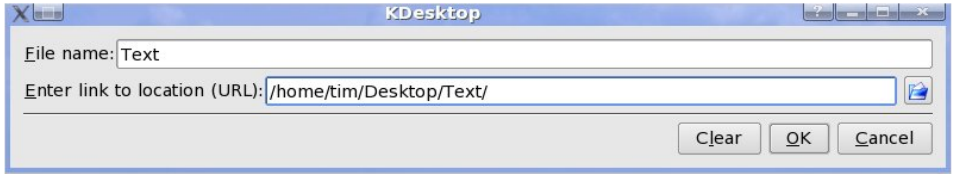
I'm sure Sebastian will soon add LightScribe support right into K3B. Till then we have SimpleLabeler.

# Using Desktop Shortcuts Effectively

by johncoom

Some applications default to saving their files to the desktop. There's nothing technically wrong with storing files there, but after a while, your desktop will become cluttered with files that you probably don't need to access all the time. Here is a tip/trick that you can use to avoid the problems associated with saving to the desktop. It makes it easy to find your files, and requires just one extra click to access them.

First, open the Home directory - "Home" icon on the desktop or "Personal Files" icon on the kickbar (in Windows it's called the taskbar). Next, right click on a blank area of the window that opens and select `Create New >Folder`. Type "Text" or whatever name you wish (without the quotes) and click OK. This creates an empty folder in your home directory. Now close this window so you are back at your normal desktop. Right click on a blank part of the screen and select `Create New>Link to Location` (ignore that it also has URL). In the lower section at the far right, click the little icon for Open File Dialog and then click on the folder that you just made. Then click on OK.



File name: Text

Enter link to location (URL): /home/tim/Desktop/Text/

You can now put any existing text files that you may have on your desktop in this new folder. And when you use your text editor, you put them in this new text folder (its only one more click). When you want to access a text file, it's just one click extra to open the text folder from your desktop.

Doing things this way has several advantages

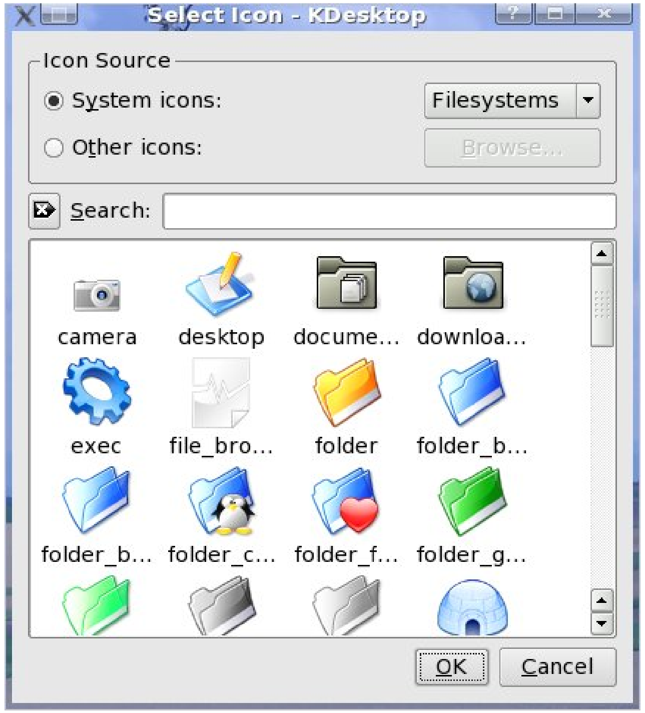
(1) It does not clutter your desktop

(2) You can make similar folders and desktop shortcuts to folders for other things

For example, I made these folders: PDF, ISO, PIC, HTML, Music, and Download. You can create whatever you want, and get to your folders with one click from your desktop.

Now, if you created several such folders, perhaps you've noticed that they all have the same icon. Distinguishing them would be easier if they each had an icon that indicated what type of file you store there.

To change an Icon, right click on your desktop shortcut and select Properties. Then, while in the General tab of the dialog box that opens, left click on the displayed icon symbol, and the "Select Icon" window will open for you.



Select Icon - KDesktop

Icon Source

● System icons: Filesystems

○ Other icons:

Search:

At top left the System Icons will be selected and also at the top right there will be a button with Applications written on it. You should change this to Filesystems as shown above (click the down arrow), and now you will see various icons in the window. Click on the one you want to use for that short cut, and you will be back at the Properties for that icon. Click OK.

That is it, you just changed the icon for that desktop shortcut.

# Limewire/Frostwire

by Scooter

*Found on main PCLinuxOS forum at:*

*http://www.pclinuxos.com/forum/index.php?topic=13742*

I use Frostwire, and it's indistinguishable from Limewire except for the color scheme.

If you choose to use it, you will need to correct a small bug in Frostwire 4.10 . The server list it uses is **outdated/wrong**. You will find that the connection indicator at the bottom left will say "Starting connection...", and it will never connect. To correct this, use this fix from the Frostwire forums: *For full post see:* `http://www.frostwire.com/forum/viewtopic.php?t=678&highlight=starting+connection`

1. Download and install Frostwire from Synaptic.

2. Leave Frostwire CLOSED. Go to your K Menu, select Find > Files and type in "`.frostwire`" (with a dot in front – no quotes). Look for a file called `Gnutella.net` with a "~" in the name - this is a backup file, delete this. Then open the other Gnutella.net file with KWrite. Highlight and delete everything in the file, but leave KWrite open.

3. Go to this link:

```
http://mc3.electronicbox.net/gnutell
a.net
```

This will give you a long list of servers. Copy and paste this list into the Gnutella.net file, save it, and answer "Yes" if you are asked if you want to overwrite the file.

4. Your Frostwire connection should now be excellent. Remember to check your UPnP and port forwarding settings with your firewall/router, if you use one, to make sure the ports are free.

5. Start Frostwire. Enjoy!!

## Plea for Help

The PCLinuxOS Hardware Database project needs your help. For those who may not know, this database is being developed to make it easier for PCLOS users to determine in advance how well a piece of hardware works with PCLOS. It takes a lot of work to sort through all the possible hardware and develop such a wealth of information into usable form.

Jmiahman posted recently that he was not receiving much information from the community. Please take a moment and visit the site and provide what information you can regarding your hardware. We all will benefit in the long run. Thank you.

* Customer: "Hi, I was wondering if you could fix my laptop. It's under warranty."
* Tech Support: "What seems to be the trouble with it?"
* Customer: "My wife got mad and threw it in the pool."

A man purchased a laptop. He called about a week later and said that it would no longer boot up. He brought it in, and it was discovered that sixteen nicely drilled holes were in the bottom of the case. When asked about it, he said the machine was too hot sitting on his lap, so he had drilled these "air holes."

One day a customer called complaining that he just received his computer, but it won't turn on. When he first pushed the power button, the screen flashed and then everything died.

I couldn't do much over the phone, so I went to the customer's office. It was plugged in, everything was hooked up ok, but, sure enough, it refused to turn on. I decided to take it back and promised to deliver a new one as soon as possible. But when I went to pick it up, I couldn't.

Fearful of thieves, the man had fired some 24 inch bolts straight through the box, through the hard drive, motherboard, everything, locking it to his desk.

"Oh," he said, "I thought it was just the TV part that was important. Will my warranty cover this?"

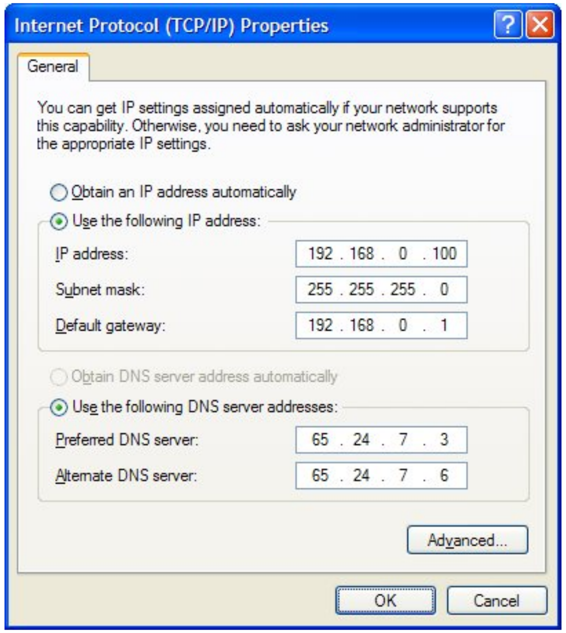
# Setting Static IP Address On Your Network

by Stumpy842

After reading the article "How to Set up a Printer in a Windows Workgroup" in the December issue of PCLinuxOS Magazine, I would like to address an additional consideration. Most Windows machines in a typical home network (that is, several systems connected to a router/Internet gateway) will be set to use DHCP to obtain an IP address on the network automatically. This is the default for Windows unless changed by the administrator. Unfortunately, this means that each time a particular machine is booted up it will possibly get a different IP address, depending on how many other machines are already assigned on the network. The solution is to use static IP addresses for all the machines on your network.

However, trying to set up Windows to use static IP addressing is often a hit or miss situation. Many times when doing this the various machines will not even "see" each other on the network, depending on factors such as which machine has been up and running longer, is acting as the master browser, and so on. I have found it to be a better solution to use the configuration screens in the router to establish a static IP for each machine on the network permanently, and leave DHCP running to catch any other systems which might walk in the door and end up plugged into the network temporarily.

To check your IP settings in Windows XP, open the *Control Panel*. If you are in Category View, click the *Network and Internet Connections* category, then *Network Connections* icon. If you are in Classic View, click the *Network Connections* icon. Right-click on the icon for your adapter and click *Properties*. In the *Properties* dialog double-click on **Internet Protocol (TCP/IP)**. In the *Internet Protocol (TCP/IP) Properties* dialog the default settings are **Obtain an IP address automatically**, and **Obtain DNS server address automatically**. To assign a static IP address to this machine on the network, you would select **Use the following IP address**, and enter appropriate values for **IP address**, **Subnet mask** and **Default gateway**.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

| | |
|---|---|
| IP address: | 192 . 168 . 0 . 100 |
| Subnet mask: | 255 . 255 . 255 . 0 |
| Default gateway: | 192 . 168 . 0 . 1 |

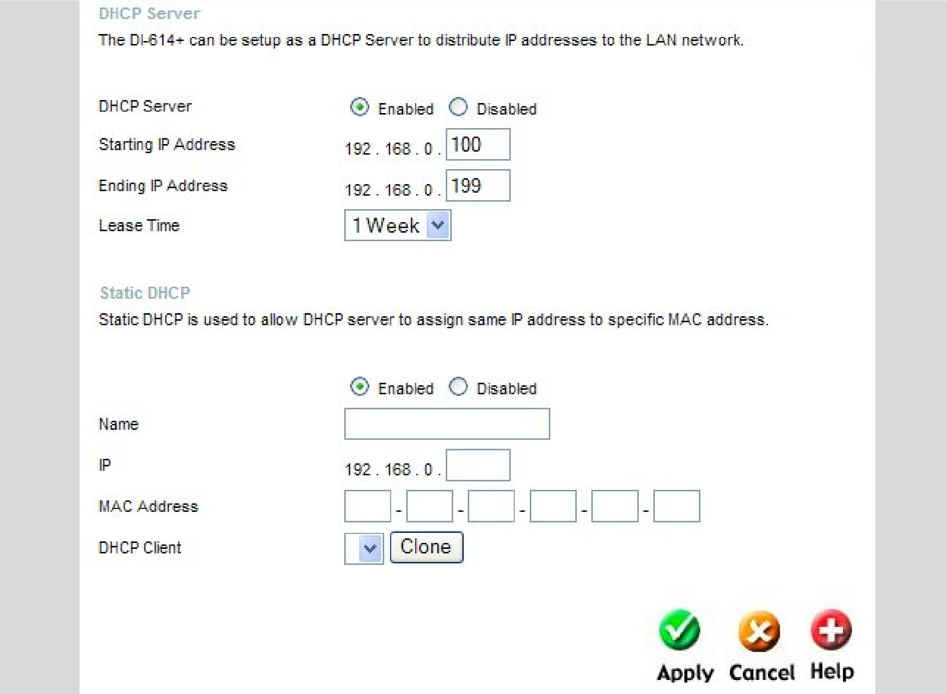
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

| | |
|---|---|
| Preferred DNS server: | 65 . 24 . 7 . 3 |
| Alternate DNS server: | 65 . 24 . 7 . 6 |

Each machine on the network needs a unique IP address, so be sure to change the last number (ie. 100, 101, 102 etc) for subsequent machines when assigning addresses. The *Default gateway* is the IP address of your router, usually 192.168.0.1 or similar. Also, note that selecting **Use the following IP address** automatically selects **Use the following DNS server addresses**. This means you will need to enter a value for **Preferred DNS server** and optionally **Alternate DNS server**. These can be obtained from the Status page of your router's configuration screens, or from your Internet service provider. Along with the possible problems I mentioned with this method earlier is the fact that Internet service providers often change their DNS server numbers, and generally do not tell their customers when they do so. This would mean having to change each machine's DNS server numbers each time this occurred. Failure to do so would result in the machine not being able to access the Internet (unless you entered the actual IP address of the website you want into the address bar in your browser).

A better alternative to this approach is to let the router itself assign static IP addresses to each machine that is a permanent system on your network. This only needs to be done once and avoids the pitfalls of having the DNS servers change. Here is an example of my router, a D-Link DI-604.



DHCP Server

The DI-614+ can be setup as a DHCP Server to distribute IP addresses to the LAN network.

DHCP Server ● Enabled ○ Disabled

Starting IP Address 192 . 168 . 0 . 100

Ending IP Address 192 . 168 . 0 . 199

Lease Time 1 Week

Static DHCP

Static DHCP is used to allow DHCP server to assign same IP address to specific MAC address.

● Enabled ○ Disabled

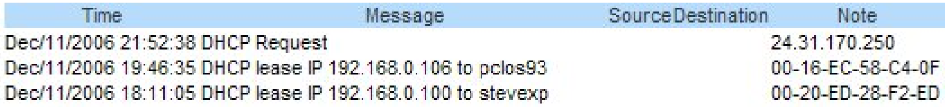
Name

IP 192 . 168 . 0 .

MAC Address - - - - -

DHCP Client

Each machine on the network is identified to the router by its MAC address, a unique string encoded in the Ethernet adapter. So to assign a static IP for a machine, you need the MAC address of its Ethernet adapter and its host name. In the DI-604 you can find this info by viewing the Log pages on the Status screen.



| Time | Message | Source | Destination | Note |
|---|---|---|---|---|
| Dec/11/2006 21:52:38 | DHCP Request | | | 24.31.170.250 |
| Dec/11/2006 19:46:35 | DHCP lease IP 192.168.0.106 to pclos93 | | | 00-16-EC-58-C4-0F |
| Dec/11/2006 18:11:05 | DHCP lease IP 192.168.0.100 to stevexp | | | 00-20-ED-28-F2-ED |

Here we can see the machines *pclos93* and *stevexp* with their corresponding IP and MAC addresses. If your router does not show this information, you can get the MAC address of your Windows machine by Clicking `Start` > `Run` and typing `cmd`, then at the command prompt type `ipconfig /all`. The host name is shown under the *Windows IP Configuration* section and the MAC address is shown as *Physical Address* under the *Ethernet adapter* section. On PCLinuxOS you can get the MAC address by running KDE Control Center, expanding the *Information heading* and selecting *Network Interfaces*. The MAC address is shown under the *HWaddr* column entry of your adapter, typically *eth0*. An alternative method is to run PCLinuxOS Control Center and select *Networking*, then *Reconfigure an existing network interface*. When the *Manage Connections* window opens, select your adapter from the dropdown list and then click the *Information* tab. The host name can be found by opening a terminal and typing `hostname`. If your hostname is *localhost* and you would prefer another name, I refer you to this thread on the PCLinuxOS Forums, "How do I set the machine name?"

`http://www.pclinuxos.com/forum/index.php?topic=12469.0`

See Reply #12 by EvenFlow for info on the changes you need to make.

Armed with this info, you can use your router's configuration screens to assign permanent addresses to the machines on your network. Refer to the documentation for your router to apply this technique. I believe most newer routers support assigning static IP addresses on the network.

I work in a call center for a large cell phone company that sells PDAs with phone functionality. I got a call from a customer who said her stylus had broken. I offered to transfer her to customer care, where they could order her out a pack of styluses. She said no, the phone had gotten "messed up." I asked what was wrong with it, and she said that when the stylus had broken, she'd tried to superglue it back together, then put it back in the slot before the glue had dried, and it got stuck in the phone. So she tried to take it out with a hammer and chisel.

I worked at a photo lab in New Mexico. Part of my job was outputting digital files to a film recorder. Everyone there was friendly, except for one woman who never seemed to like me. After a few months I asked my boss about it. He told me that before I got there, they had tried to train her to do the digital output. They even paid for her to go to a class to learn about computers. She was the only student in the class who managed to get a floppy stuck in the drive upside down and backwards. The teacher had to disassemble the machine to get the disk out. She told him she had to pound it with the heel of her hand to get the disk to go in. After that, the photo lab decided she probably wasn't the one for that position. She always resented the fact that I had 'her' job.

A customer had bought a computer from us about a year ago and a Voodoo 3 card just yesterday. He took it home and tried to install it but couldn't, so he brought them both in this morning. He ranted and raved, etc. He had reboxed the Voodoo 3, expecting a replacement, so we took the computer and the Voodoo 3 in the back and told him we would fit it for free. When we opened the box for the Voodoo 3, it was in a terrible state. The bit of metal that attaches the card to the case was taken off, and a wee heatsink had been scraped off the chip with a screwdriver. I reglued the sink and reattached the backplate. So we opened the machine, and tried to fit the card. Ack. Card is AGP, computer has exactly zero AGP slots. So we went back to the front.

* Me: "Sir, your computer has no AGP slots, and this is an AGP video card."
* Customer: "Yeah, but the card fit perfectly into the little white slot."
* Me: "Which white slot?"
* Guy: "There's five of them -- little white ones. There's a spare one."
* Me: "The PCI slot? Uhh...it shouldn't...let me check."

Sure enough, if you remove the heatsink and backplate, turn the card around, and really hammer it into the only free PCI slot, it will just fit snugly next to the hard disk.

We explained that the AGP card was completely destroyed and he had voided the warranty on it by hacking away at it with a screwdriver. The usual mad customer vs. techie exchange ensued, but he eventually backed down and bought the PCI version instead...and got us to fit it.

# A Tale Of Too Many Distros

by Wayne Whitman

First came Red Hat. If I remember correctly, it was release 3.1. It was archaic by today's standards, but that was back in '96 or so and times have certainly changed. You've come a long way, Penguin! Come to think of it, there wasn't even the Penguin back then.

My reason for loading Linux on my first notebook machine was to learn Unix. I was working on a computer project as a database consultant. The host system was running HPUX and I had never used Unix before. To make matters worse, the network gurus wouldn't let an "outside" PC connect to their network. Ouch! I was stuck with an unfamiliar operating system and vi on a VT50 terminal. What's a newbie to do? Setting up a dual boot on my brand new Windows 95 machine looked like a good opportunity to learn a new OS. Red Hat to the rescue! It was a great learning experience: no X windows, just the command line and vi. It made a wonderful sandbox. I have to admit the experience was painful, but it was also a bit of fun and a good introduction to Linux.

In the years following that project I worked on many different Unix systems. But I had been bitten by the Linux bug. Experimenting with different Linux distributions became an addictive hobby. A few years later I had a used IBM Intellistation purchased online at a cheap price and loaded up with extra disks. Aha! The perfect Linux testbed.

The first guinea pig was Red Hat 6. It was OK, but not everything worked. I was still such a newbie that I even had trouble getting the sound to work. Then it was on to Mandrake, Debian, Xandros, Linspire, SUSE, Progeny, Libranet, Gentoo (never could get it installed), Fedora, Damn Small Linux, and Slackware. I even tried Solaris. By then, I was such an addict, that I had 6 distributions running on one machine. My biggest problem was which one to boot each day. I have to admit, out of all of those, Slackware was my favorite because of its clean file layout and simple approach to things. But all of them seemed to have one problem or another, or there was something I just could not figure out how to get working.

Enter Ubuntu. I really thought this was going to be the one. It looked good. It felt good. But man, did I get tired of sudo. Sometimes I just like to log in as root and do some maintenance. Then there was the bloat and the wireless hassle.

As a true addict, I recently put in yet another order for CDs with ONDisc.com. More new distro releases to try out! Then my order turned up a few dollars short of free shipping. What else to choose? What is this thing called PCLinuxOS on their list? OK, throw it in and get free shipping.

The CD with PCLinuxOS 0.93 Big Daddy sat in the pile on my desk for weeks while I loaded and reloaded new releases of other stuff. I downloaded SLED, and it was interesting, but I had some application install issues that were show-stoppers.

Out of sheer boredom one afternoon, I dug through the pile of CDs and there was PCLinuxOS. Why not give it a try? I had tried almost everything else. Surprised, I discovered everything just worked. Even the wireless  configured itself and came up working. I plugged in the USB printer, and ... wow, I did not even have to configure it with CUPS. I downloaded and installed Firefox 2 and gvim, then added them to the menu. Boy, it is really fun when things just work right. Simplicity and ease of configuration are wonderful things.

I have to admit, I am not a big "more is better" applications fan, so I replaced Big Daddy with MiniMe and just added what I wanted. What a great distribution philosophy: a distro tailored for everyone.

Is this a distribution that could replace Windows for me? Yes, except for one requirement. I need the Oracle development tools for my project work. Unfortunately, Oracle only supports their tools on Windows, Red Hat, and SUSE. My PCLinuxOS now has Vmware installed, and soon I will install the dreaded "W" in a virtual machine just so I can have those tools. But it's a workable solution for me, and it gives me a Linux distribution that works and is a joy to use.

Congratulations to Texstar and the crew for an outstanding piece of work. I can not wait to try out 0.94 with Gnome. Simplicity for me. Donate if you can, send thank you emails or volunteer if you can't.

I work for a major computer retailer and heard a page over the intercom for an available salesman at the customer service desk. Most of the salesmen are a little apprehensive when they hear this, because you never know what you are about to get in the middle of. As I approached the desk, I saw a well-dressed cowboy and a desktop tower on the service desk. One of the customer service reps informed me that the computer he bought today was broken, and he needed a replacement. So I agreed and started toward the tower to take it back. The gentleman stopped me and said he just realized he had forgotten to get his CD out. Before I could say anything, he pulled out a pocket knife and went for it. Luckily, we got him to stop before he did any real damage, and I showed him how to hook it up to a power cord and eject it normally. Never thought I would see somebody try to knife a computer.

A friend of mine (who shall remain nameless) bought a brand new Toshiba laptop computer last year since his "old" one was a model from the year before. He worked in the computer services office on campus here at our university. He decided one night that to impress his co-workers he would make his new laptop more decorative. He bought a can of emerald green Krylon spray paint and sprayed his entire computer (screen, mouse, keyboard, casing, and all) with it. He was shocked to find that his computer wouldn't work afterwards and decided the paint must be at fault. So the next day he bought a can of Goo Gone and a bottle of paint thinner and poured them both on his computer, then rinsed it off in the sink.

Again, he was shocked when his computer wouldn't work. He was even more shocked when Circuit City told him they wouldn't refund his money or exchange his computer for a new one.

I once had a customer whose cdrom drive wasn't working -- I suspect the reason was old or missing drivers, but the customer had tried to fix the problem himself. He thought the problem was that the CD had to sit tightly in the tray, so she took a paper clip, put it through the center hole of the CD, and fastened it to the drive tray. When he tried to use the drive that way, he was greeted with grinding noises caused by the disintegrating drive mechanism.

My mother was visiting one time when I was online. I remarked to her that the computer was running a little slow today. Her solution? Oil it. You can imagine how I wince every time I think of it.

# Acquiring and Installing VMWare

by vampirefo and edited by Tim Robinson

VMWare Server is an application that allows the user to create a complete, separate "virtual machine" that runs within Linux or Windows (the host), providing a method to install a completely separate operating system and use that operating system without exiting the host. For example, one can install a version of Windows or a different Linux distribution for testing purposes or to run an application that does not run in one's existing operating system.

VMWare Server is free – sort of. To acquire a copy, one must visit their site, fill out a form and provide information. Then you will be provided with a serial number that is used during the installation process. This article will walk you through the lengthy, though not complicated process, step by step.

First, visit:

`http://www.vmware.com/download/server/`

and click "Register now to get your free serial number." Provide whatever information you feel is appropriate, being sure to complete all required fields. Once you are given the serial number, be certain you write down the 20-digit result. You will need it later, during the install.

When you arrive at the download page, select `Binary (.tar.gz)`, md5sum: 9846bff6c3c8af97d4e3ae2700f8dd3a. Do NOT select the .rpm version. Downloading will take a while, even with broadband, as this is a 100.6 MB file. Click the Download tab.

Save to a location of your choice. When the download completes, open your favorite file manager and navigate to the location where you saved the file. Right click on the file and extract it. Now open the newly-created folder "vmware-server-distrib."

Open a terminal in that folder. The bulk of what follows will be done within the terminal. Type `su` , then enter your root password so the install can be run. Type "`./vmware-install.pl`" without the quotes to start the process.

Below is the console output, and interspersed with that is what you should do, e.g., "click enter" or "type yes", and so forth. If you follow the instructions exactly you will have no problems.

```
Creating a new installer database
using the tar3 format.
Installing the content of the package.
In which directory do you want to
install the binary files? [/usr/bin]
```

Press enter.

```
What is the directory that contains
the init directories (rc0.d/ to
rc6.d/)?
[/etc/rc.d]
```

Press enter.

```
What is the directory that contains
the init scripts?
[/etc/rc.d/init.d]
```

Press enter.

```
In which directory do you want to
install the daemon files?
[/usr/sbin]
```

Press enter.

```
In which directory do you want to
install the library files?
[/usr/lib/vmware]
```

Press enter.

```
The path "/usr/lib/vmware" does not
exist currently. This program is
going to create it, including needed
```

```
parent directories. Is this what you
want?
[yes]
```

Type "yes", then press enter.

```
In which directory do you want to
install the manual files?
[/usr/share/man]
```

Press enter.

```
In which directory do you want to
install the documentation files?
[/usr/share/doc/vmware]
```

Press enter.

```
The path "/usr/share/doc/vmware" does
not exist currently. This program is
going to create it, including needed
parent directories. Is this what you
want?
[yes]
```

Type "yes", then press enter.

```
Before running VMware Server for the
first time, you need to configure it
by invoking the following command:
"/usr/bin/vmware-config.pl". Do you
want this program to invoke the
command for you now? [yes]
```

Type "yes", then press enter.

```
You must read and accept the End User
License Agreement to continue.
Press enter to display it.
```

Press and hold enter until it reaches 100%

```
Do you accept? (yes/no)
```

Type "yes", then press enter.

```
In which directory do you want to
install the mime type icons?
[/usr/share/icons]
```

Press enter.

```
What directory contains your desktop
menu entry files? These files have a
.desktop file extension.
[/usr/share/applications]
```

Press enter.

```
In which directory do you want to
```

```
install the application's icon?
[/usr/share/pixmaps]
```

Press enter.

```
None of the pre-built vmmon modules
for VMware Server is suitable for
your running kernel.  Do you want
this program to try to build the
vmmon module for your system (you
need to have a C compiler installed
on your system)? [yes]
```

Type "yes", then Press enter.

```
What is the location of the directory
of C header files that match your
running kernel?
[/lib/modules/2.6.16.27.tex1.lve/build
/include]
```

Press enter.

```
Do you want networking for your
virtual machines? (yes/no/help) [yes]
```

Press enter.

```
Do you want to be able to use NAT
networking in your virtual machines?
(yes/no) [yes]
```

Press enter.

```
Do you want this program to probe for
an unused private subnet?
(yes/no/help) [yes]
```

Press enter.

```
Do you wish to configure another NAT
network? (yes/no) [no]
```

Press enter.

```
Do you want to be able to use host-
only networking in your virtual
machines? [yes]
```

Press enter.

```
Do you want this program to probe for
an unused private subnet?
(yes/no/help) [yes]
```

Press enter.

```
Do you wish to configure another host-
only network? (yes/no) [no]
```

Press enter.

```
Please specify a port for remote
console connections to use [902]
```

Press enter.

```
Stopping xinetd:        [FAILED]
Starting xinetd:        [  OK  ]
Configuring the VMware VmPerl
Scripting API.
Could not find necessary components
to build the VMware VmPerl Scripting
API. Look in your Linux distribution
to see if there is a perl-devel
package. Install that package if it
exists and then re-run this
installation program.

********
The VMware VmPerl Scripting API was
not installed.  Errors encountered
during compilation and installation
of the module can be found here:
/root/tmp/vmware-config0

You will not be able to use the
"vmware-cmd" program.

Errors can be found in the log file:
'/root/tmp/vmware-config0/control-
only/make.log'
********

Hit enter to continue.
```

Press enter.

```
In which directory do you want to
keep your virtual machine files?
[/var/lib/vmware/Virtual Machines]
```

A word of warning is in order here. If you have all of your Linux installation residing in one partition, the default above will work fine. If, on the other hand, you have `/home` on a separate partition and your root (/) partition is small, you should specify a different location for the location of your virtual machine files. These files will be quite large (perhaps more than 10Gb), so be sure you specify a location with adequate space. Don't worry whether the location exists or not. If it doesn't, the installation program will create it.

Press enter.

```
The path "/var/lib/vmware/Virtual
Machines" does not exist currently.
This program is going to create it,
including needed parent directories.
Is this what you want? [yes]
```

Press enter.

```
Please enter your 20-character serial
number.
```

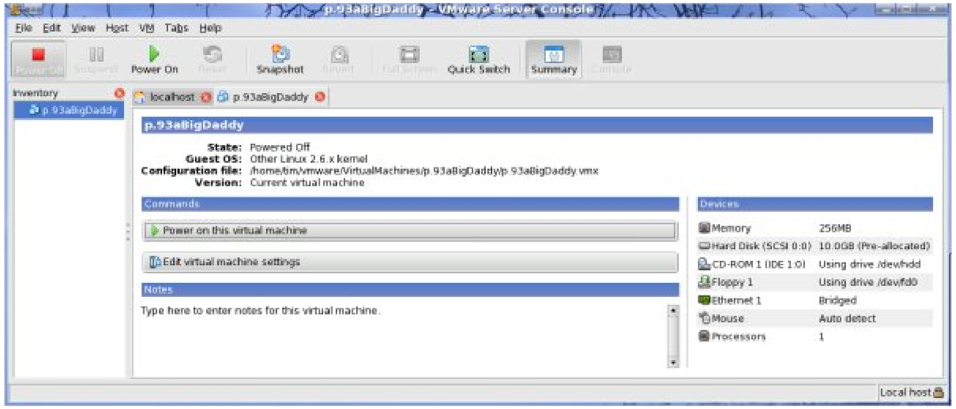
Type XXXXX-XXXXX-XXXXX-XXXXX (the serial number you recorded earlier). Press enter.

```
Starting VMware services:
   Virtual machine monitor    [   OK   ]
   Virtual ethernet           [   OK   ]
   Bridged networking on /dev/vmnet0
                              [   OK   ]
   Host-only networking on
/dev/vmnet1 (background)      [   OK   ]
   Host-only networking on
/dev/vmnet8 (background)      [   OK   ]
   NAT service on /dev/vmnet8
                              [   OK   ]

The configuration of VMware Server
1.0.1 build-29996 for Linux for this
running kernel completed successfully.

[root@localhost vmware-server-
distrib]#
```

Type "`exit`" without the quotes and press enter.

Type "`vmware`" without the quotes. VMWare opens.

Check "`localhost`". Click "`Connect`".



p.93aBigDaddy

**State:** Powered Off
**Guest OS:** Other Linux 2.6.x kernel
**Configuration file:** /home/tim/vmware/VirtualMachines/p.93aBigDaddy/p.93aBigDaddy.vmx
**Version:** Current virtual machine

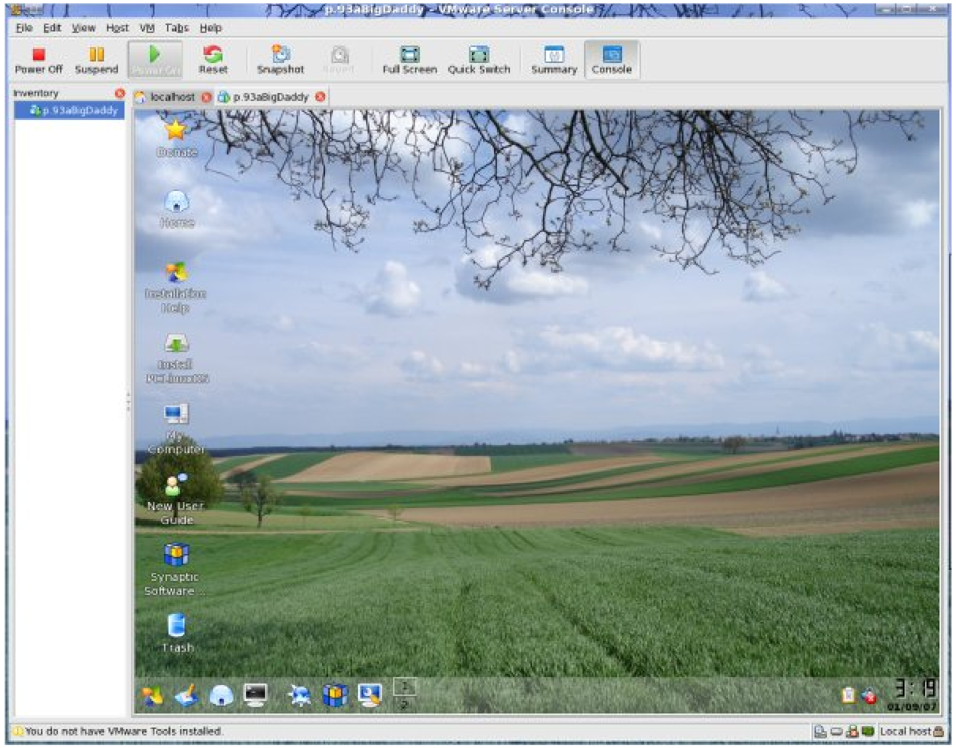
Type here to enter notes for this virtual machine.

| Devices | |
|---|---|
| Memory | 256MB |
| Hard Disk (SCSI 0:0) | 10.0GB (Pre-allocated) |
| CD-ROM 1 (IDE 1:0) | Using drive /dev/hdd |
| Floppy 1 | Using drive /dev/fd0 |
| Ethernet 1 | Bridged |
| Mouse | Auto detect |
| Processors | 1 |

Click "`create a new virtual machine.`" Click `Next`. Click `Next`. Choose the OS you wish to install. Click `Next`. Choose `NAT`. Click `Next`. Choose the size of the virtual hard drive you wish to create. Be sure to make it large enough. Click `Finish`.

Click "`Edit virtual machine settings.`" Adjust RAM, add/remove drives, and so forth.

Put the CD for the OS you wish to install in your new virtual machine in the CDROM or DVD drive, click "Power on this virtual machine," boot and install. Here is a screenshot of PCLinuxOS .93a Big Daddy running inside VMWare, inside PCLinuxOS .93a Big Daddy.



You do not have VMware Tools installed.

The virtual machine will function almost exactly like a real machine would, except it will be running entirely within your "real" OS. Enjoy!

One of our customers bought a scanner with a SCSI card. It wasn't connecting, so she brought it in. It turned out she had pried off one of the blank plates covering an empty ISA slot, then shoved the card through the hole and turned on the system.

My mom had some problems with her system and figured she'd get a new modem. After she installed it, there were more problems than before. It turned out the modem was an ISA modem, and she somehow managed to put it into a PCI slot. How, I have no idea.

While I was at college (back in the days of Archimedes computers), I often helped to teach new users the ropes while the teacher concentrated elsewhere. This one sweet girl was very new, and I didn't mind that she had no concept of the mouse, the screen, and whatnot -- she soon got good enough that I could leave her to do some task and help someone else. Pretty soon, however, she was tugging on my chair, and when I went to see what was going on, she said, "My bracelet is stuck in there."

Eh?

It was wedged into the floppy disk slot. Why? Apparently, the bracelet was annoying her when she typed, so she took it off. She found a small slot on the computer with a happy little door on it and just went ahead and shoved it in. Tech support had to rescue it by taking the thing apart.

When my sister and I were both living in the dorms at college, she would frequently come to me for tech support.

* Her: "Hey, can you look at my laptop? It's having a problem."
* Me: "Yeah, what's the problem?"
* Her: "Every time I try to type a letter, three show up, and none of them are the letter I hit."

I went to check it out. Sure enough, the problem occurred exactly as she stated it. As I was trying to think what the cause might be, I looked down and noticed a noodle under the enter key.

* Me: "There's a noodle in here. How did that get there?"
* Her: "Oh, I spilled soup on my keyboard. Does that make a difference?"

# How To Split (and Rejoin) A File

by author

*Found on main PCLinuxOS forum at:*

*http://www.pclinuxos.com/forum/index.php?topic=14013.msg111147#msg111147*

Sometimes you may wish to split a file, thereby making it easier to email or fit on storage devices. Here is a quick refresher course on splitting and joining.

## Splitting

Open a konsole. (In KDE, this involves either clicking on the icon of the "Konsole Terminal Program" on the KDE menu bar, or using `Main Menu` > `Terminals` > `Terminal Program`.)

CD ( change directory ) to the directory where the file to be split is located. For instance,

```
cd /home/ferdi/mymp3s
```

To split a sample file (filename.mp3) into 2Mb parts with a suffix consisting of 2 numbers do:

```
split -a 2 -b 2m -d filename.mp3 parts
```

The option '-a 2' tells 'split' to use a suffix length of 2.

The option '-b 2m' tells 'split' to make parts of 2Mb size

The option '-d' tells 'split' to use numbers for the suffix instead of the default characters.

'parts' is the first half of the name of the smaller files: parts00 parts01 parts02...

If the new smaller files don't show up immediately in Konqueror, hit F5 to force a screen refresh.

## Joining

To join the smaller parts use the following:

```
cat parts* > filename.mp3
```

The * (wildcard) tells 'cat' to use all files in the current directory that start with 'parts'.

I used to work technical support and account services for a cellular phone company. One day an individual working for a construction company called and asked why we disconnected his service. I informed him that his service was fine and that his account was current, at which time I was informed that we had to have shut off his account because he couldn't power his phone on.

I began asking the usual questions, beginning with the model phone he was using. This often is a huge key to figuring out what the problem is, and it just so happened that he had the most problematic phone we had released due to its emergency yellow and black colors, looking vaguely like one of those water resistant portable cassette players.

We tried plugging it in, switching the battery, but it still wouldn't turn on. I asked him if it had been dropped or damaged before it stopped working. The answer was no.

I asked him if it had been exposed to water, and the answer was, "What does that matter? I have your waterproof model!"

I was sure I had struck the heart of the issue. It turned out that he was showing it off to his work buddies by throwing the "waterproof" phone into a bucket of water while he was joking around on the phone with the foreman.

I informed him that the phone was not actually waterproof, and that he would have to purchase a new phone due to the fact that our insurance policy did not cover damage from intentional misuse.

He explained that he heard a rumor that if you dry the phone out and replace the battery, they will sometimes continue working. This is sometimes true, so I asked him if the phone had been thoroughly dried.

The answer was yes -- he had put the phone into his clothes dryer with a load of laundry, which we then confirmed as the reason the face plate had broken off. He wanted an insurance replacement for his face plate, and I again informed him that our insurance policy did not cover damage from intentional misuse.

# Using Fish

by Daiver Pedemonte

Here's a quick and easy method for setting up a network and accessing remote files. Please note: this works only if SSH is properly enabled in both computers.

## The FISH protocol

I was having a lot of trouble setting up a network using NFS. SMB was out of the question. All I wanted to do was access another computer in my LAN which holds all the media files and acts like a storage room for documents, pictures, etc. without having to use NFS. This is just one of the many ways that you can share files among computers in KDE.

FISH will not allow you to stream audio or video via LAN, but it is probably the easiest way to access your files on another computer. Using FISH, you will be able to copy files locally and store files remotely, assuming the right permissions are set.

**Take FISH for a test drive:**

1)Open Konqueror.

2)In the address bar, type

```
fish://IP_ADDRESS_OF_REMOTE_COMPUTER
```

(In my case, the IP address was 192.168.10.2.)

3)Enter the user and password of the remote computer. (Do not use root.)

This will send you to the home directory of the remote computer's user that you typed in. However, it is possible to view mounted drives in it and, if the permissions are set correctly,  you will also be able to write to the drives.

To view the mounted drives, edit the URL to go to the root filesystem (/) and then navigate to /mnt. Your drives and partitions are there.

The easiest way to set up a quick access is to create a shortcut on the KDE desktop:

1) Right click on the desktop and select `Create new > Link to location`.

2) Put a name to the path to be accessed on the remote computer. If you are going to make the shortcut to access an MP3 directory, then something like MP3 will work or use Docs for documents, etc.

3) Enter the URL to the path to be accessed when you click the shortcut. In my case it was fish://user_name@192.168.10.2/mnt/sdb1/Mp3

(Replace user_name with the username on the computer you want to access.)

Now, any time I want to access my remote storage, I can just click that shortcut and it will take me there. For security reasons, I never save the password, so I just type it in every time.

Best of all, it works using SSH, so everything that goes through FISH is encrypted and secure.

Happy fishing!

I was on a tech support call yesterday, and one of our stores had a crashed server with a bad motherboard. They did not want to transfer the hard drives over to the new server we were going to send them, so I said, ok, mail the hard drives to me, and we would put them in the new server.

So I got the package this morning, and to my surprise I found...the circuit boards from the hard drives. They took the boards off the hard drives and sent them to me.

Grinning, I called the store and asked them to send me "the rest" of the hard drives. I have never ever ever heard of this happening. Now how the heck am I going to find out which hard drive goes with which circuit board, and will there be any way to get them working again?

# DISCLAIMER

1. All the contents of PCLinuxOS Magazine (http://mag.MyPCLinuxOS.com), are intended for general information and/or use only. Such contents do not constitute advice and should not be relied upon in making (or refraining from making) any decision. Any specific advice or replies to queries in any part of the magazine is/are the personal opinion(s) of such experts/consultants/persons and are not subscribed to by PCLinuxOS Magazine.

2. The information in PCLinuxOS Magazine (http://mag.MyPCLinuxOS.com), is provided on an "AS IS" basis, and all warranties expressed or implied, of any kind, regarding any matter pertaining to any information, advice or replies, are disclaimed and excluded.

3. PCLinuxOS Magazine (http://mag.MyPCLinuxOS.com), and its associates shall not be liable, at any time for damages (including, without limitation, damages for loss of any kind) arising in contract, tort, or otherwise from the use of, or inability to use, the magazine or any of its contents, or from any action taken (or refrained from being taken) as a result of using the magazine or any such contents or for failure of performance, error, omission, interruption, deletion, defect, delay in operation or transmission, computer virus, communications line failure, theft or destruction or unauthorized access to, alteration of, or use of, information contained in the magazine.

4. No representation, warranties, or guarantees whatsoever are made as to the accuracy, adequacy, reliability, completeness, suitability, or applicability of the information to a particular situation.

5. Certain links on the magazine lead to resources located on other servers maintained by third parties over whom PCLinuxOS Magazine (http://mag.MyPCLinuxOS.com) has no control or connection, business or otherwise. These sites are external to PCLinuxOS Magazine (http://mag.MyPCLinuxOS.com) and by visiting these, you are doing so of your own accord and assume all responsibility for such action.

## Material Submitted by Users

A majority of sections in the magazine contain materials submitted by users. PCLinuxOS Magazine (http://mag.MyPCLinuxOS.com) accepts no responsibility for the content, accuracy, and conformity to applicable laws of such material.

## Entire Agreement

These items constitute the entire agreement between the parties with respect to the subject matter hereof, and supersedes and replaces all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter.