Computer

Security

Table of Contents

Welcome From The Chief Editor

Q: When does antivirus software become a virus, of sorts, itself?

A: When it marks safe, non-infected software and sites as being infected.

This was the case, not once, but twice during October when the Avast! antivirus software labeled both The PCLinuxOS Magazine and the main PCLinuxOS sites as being infected with malicious software. I suppose since they can't beat Linux with security and quality, the Windows community must resort to falsely reporting software and sites as containing malicious software. Given the flop and joke that Windows has become, it seems that the Windows community is running scared.

Actually, it's Windows users who should be running scared. They should be running to Linux in droves. They should be running away from a corporation who is in bed with the NSA. They should be running scared of the increasingly prevalent incidences of malicious software. They should be running to embrace and adopt the security that Linux offers.

The stories of antivirus-software-gone-awry could fill a book. They go back in time for as long as antivirus software has existed. Virus definition databases would routinely become so large that the antivirus software would further slow an already slow and inefficient operating system to a crawl.

Running antivirus software has become akin to putting a bandage on an arterial bleeder, and then keep applying more bandages on top of blood

soaked bandages as it continues to hemorrhage. Viruses and other malicious software are symptoms of an insecure operating system. Instead of replacing an insecure operating system with a secure one, users keep the bandage companies (the antivirus software vendors) in business by continually buying an ever increasing number of bandages to stop the hemorrhaging.

Why all of this talk about viruses, antivirus software, etc.? Well, besides the "events" in October with Avast! labeling the PCLinuxOS sites as containing malware, much of this month's magazine was already planned to center around computer security issues. The security articles this month revolve around real security for your data and online presence, not plugging an infinite number of leaks in an operating system that looks like Swiss cheese.

I feel fortunate to be running Linux, freed from the frustration of always being on guard for yet another piece of malicious code just waiting to take advantage of yet another vulnerability in an operating system that's an embarrassment to the computing industry. I feel fortunate to be freed from that constant worry, able to devote more of my focus to doing the tasks that I need or want to get done.

Today, the biggest threats to all computer users come from sources no one could have possibly envisioned 15 or 20 years ago. Todays headlines repeatedly ring out with an alphabet soup of governmental agencies – and entire governments – who think it is their business to pry into the most private aspects of our lives. The biggest concern today is the protection of our data, our reputations, and our privacy.

Until next month, I bid you peace, happiness, serenity and prosperity.

Download An Entire Picasa Album

by Paul Arnote (parnote)

OK … it's no secret. Our son was born on August 6, 2013. Being a former professional newspaper photographer, you can only imagine how many photos we have shot of our baby, Ryan. To share with friends and family, we uploaded all of those photos to our Google Picasa account.

Uploading images to Picasa is easy. I used Shotwell to upload the images from one of my laptops equipped with a built-in SD card reader to Picasa. Other users may choose to use DigiKam or Gwenview. The PCLinuxOS Magazine has previously covered uploading images to Picasa in the June 2012 issue, back when Google withdrew support for Linux users. Because I have several computers, I was seeking an easy way to download those images to some of those other computers.

Sure, I could have copied them all to a USB flash drive, but what's the fun in that? I already know how to use a USB flash drive. Since they exist in cyberspace, I figured there must be a way to download them, en masse. That was the challenge I was looking for.

DownThemAll! Firefox Add-On

Perhaps one of the easiest ways to download photos from Picasa is with the Firefox add-on called "DownThemAll!" However, it only works if you do it a certain way.

Log into Picasa in Firefox, and select the album you are interested in downloading.

In the panel on the right side, find and click on the link for the RSS feed.
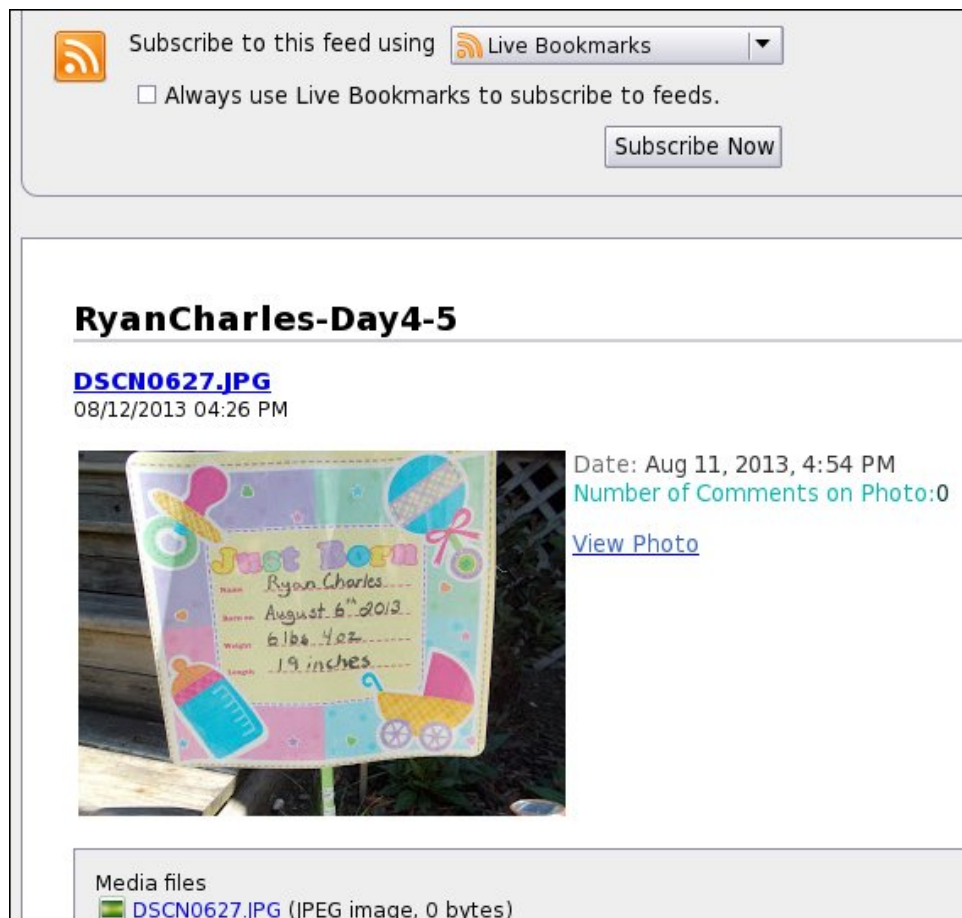
You should see something similar to that shown above. Now, go to the Tools menu, select "DownThemAll! Tools..." and then "DownThemAll!"

You should now see a window similar to the first one below (next page). Select the folder you want to save your images to (below the list of files). Select the Start! button.

The window on the screen will change to something similar to the one shown below (second image, next page). Now, sit back and wait while all of the pictures in the selected album are downloaded to your computer.

Firefox. Then, start up DownThemAll! from the Tools menu, and proceed as previously described.

Another Way (Of Course)

This being Linux, of course there's another way to download your images from your Picasa albums. This method is just as "flexible" as using the DownThemAll! Firefox add-on, and probably even faster. It will download every image you have stored in the specified Picasa album, one after another.

First, install **googlecl** from Synaptic. It has **python-gdata** as a dependency, which will also be installed, if you don't already have it installed. The googlecl utility is a command line utility that allows you to access various Google services from the command line. You can view all of the commands available by going to the online man page for googlecl.

NOTE: Since the upgrade to Python 2.7, you will have a little more to do (at least, until the packagers get around to updating the googlecl package) to make this work. You may get the following message:

File "/usr/bin/google", line 50, in <module>
    import googlecl
ImportError: No module named googlecl

One thing you might want to do is to open the "Preferences" settings for DownThemAll!, and set it to automatically rename dup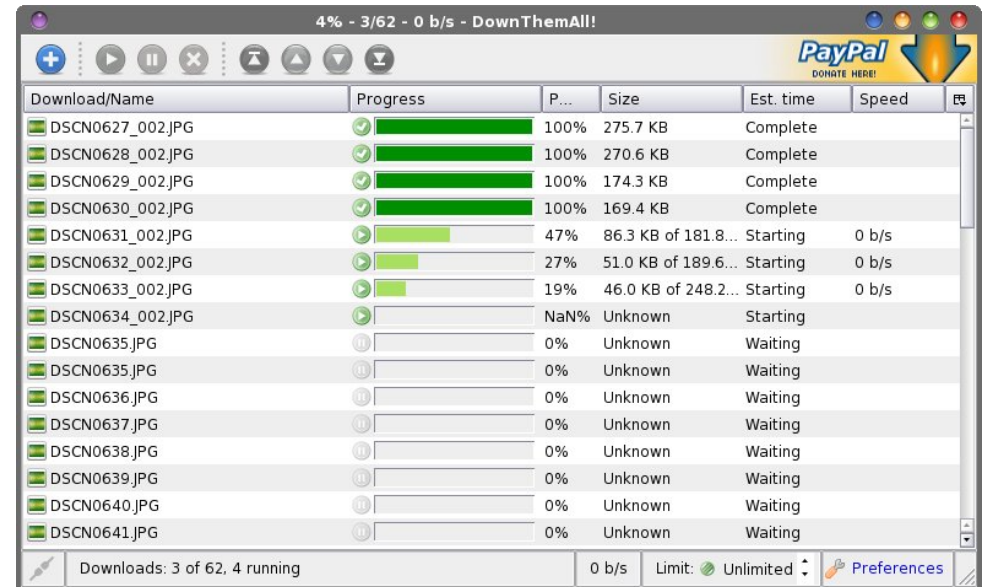licate files. The only problem I encountered with this add-on was that it refused to rename a file when I told it to. It was set to "Ask every time," and I was left with a window on my screen that would not go away, regardless of what I did. To finally rid myself of this window that was stuck in an infinite loop, I had to close Firefox, then open a terminal session and enter pkill firefox at the command line. Once I changed it to automatically rename duplicate files, I never experienced any more problems.

Also take note that this add-on will download twice as many images from Picasa as it lists. This is because it will download both the high resolution and the lower resolution versions of the images.

If you uploaded images to Picasa without specifying that they be resized, you can get your original resolution images back when you download them. To do this, place &imgdl=1 at the end of the RSS feed URL, and reload your Picasa album in

If you see this, open a root session of your file manager and copy the /usr/lib/python2.6/site-packages/googlecl folder to your /usr/lib/python2.7/site-packages/ folder.

To download your Picasa albums, simply enter the following:

google picasa get --title "[Name-of-Album]" path/to/download/folder

For example, I have a Picasa album named RyanCharles-Day1. To make the process ultra easy, I first issued the cd command to travel to my selected destination directory. Then, I entered the following command:

google picasa get --title "RyanCharles-Day1" ./

The first time you access a Google service, you will be redirected to your web browser. There, you will have to grant googlecl access to that particular Google service. You will only have to do this once, the first time you access that particular Google service. In the meantime, googlecl will exit. Don't fear. Just run the command a second time, and it will complete as expected. The other Google services you can access include Blogger, Calendar, Contacts, Docs and YouTube.

Issuing the command as I did above, a new folder will be created in the present working directory, with the same name as the Picasa album you are downloading from.

The benefit of using the googlecl utility is that it doesn't download both the high and low resolution images. Instead, it only downloads the larger resolution images. This is especially beneficial if bandwidth quotas or caps are something that you have to deal with. This method also seems to be a bit quicker than using the DownThemAll! Firefox add-on.

Summary

Anyone who uses Picasa Web Albums knows how relatively simple it is to upload images to the service. What is a pain is downloading your images. Before discovering these two methods of downloading images from Picasa en masse, I've been known to sit and download each individual image, one at a time. To say the least, it's a real pain and a real time waster to have to do it this way. With larger albums, I've been known to take up to an hour to download all of the images to another computer. Now, I can download a copy of an entire Picasa album in far less time than it takes me to download just five images individually.

Screenshot Showcase

Posted by Smileeb on 10/22, running KDE.

Avast! Leaves PCLinuxOS Sites Aghast

by Paul Arnote (parnote)

During the month of October, both the PCLinuxOS Magazine website and the main page of the PCLinuxOS site were marked as containing malware by Avast! antivirus software. As a result, many visits to both sites were blocked (we'll never know exactly how many), and Avast! users were left with a misleading impression that PCLinuxOS and The PCLinuxOS Magazine contains malware and viruses. The damage is unmeasurable, and the reputation of both sites is at peril, thanks to the erroneous label.

Background

Let's start off with this simple, yet accurate, statement: **There are NO viable viruses "in the wild" for Linux.** Certainly, there have been reports of theoretical concept viruses, which exist only in the lab. Yet, when it comes to implementing them in the wild, they have all failed miserably. Most Linux users who have been around for a while already know this. Linux newbies may not realize this, however, since they may still be operating their Linux computers under a "Windows mentality."

As for Windows users … well, part of their daily existence involves running around scared of viruses, malware, spyware, crapware and every other kind of "ware" that infests that so-called operating system. It has become such a huge problem under Windows that an entire segment of the Windows software market has become a multi-billion dollar industry (in U.S. dollars). That one segment is devoted to just creating and marketing software to defend against and protect against the onslaught of malicious software.

Sometime over the first weekend of October 2013, an "updated" Avast! antivirus database flagged the image of the September 2013 issue of The PCLinuxOS Magazine as malware. What was even more odd is that that very same image had been posted to the magazine website for well over a month, without any issues.

The original report came from PCLinuxOS forum member Crow, on October 6, 2013. Meemaw, assistant editor of The PCLinuxOS Magazine, confirmed the problem happened to her on October 4, 2013, when she attempted to bring up the magazine website from her place of employment (as she always does), on a computer running Windows 7, "protected" with – you guessed it – Avast! antivirus. She originally thought it was only her computer and connection that was at fault, until Crow made his report the a few days later. Meemaw subsequently changed to the recently discontinued Microsoft Security Essentials virus scanner, which reported the magazine site as clean and free of malicious software.

Subsequent scanning of all of the files on the magazine website by YouCanToo, using ClamAV (in the PCLinuxOS repository), showed no virus or malware signatures, whatsoever. Additional scanning of the magazine's web page by other PCLinuxOS users, using different virus scanners, also showed that the files in use were, in fact, clean and free of malicious software and signatures.

This is what is known as a "false positive" in the antivirus software world. This is where an otherwise innocent and un-infected file or site is marked as malicious, when it isn't. As a precaution, I (as the website maintainer, one of the duties of the magazine's Chief Editor) took a suggestion from Texstar and opened and resaved the image in Gimp to reset the JPG Exif data with a different filename, re-uploaded the image to the magazine web server, and edited the HTML code to point to the new image.

Meanwhile, PCLinuxOS forum member Tony, returned to one of his old "haunts" in an attempt to help clear up the false positive. Tony, as it turns out, used to be very involved in the Avast! forums, where he seems to still have quite a very good reputation. Tony's post got other Avast! forum members checking out the magazine's web page, and they all gave it an excellent "bill of health" as well. That made the magazine's web page twice vindicated, at least in my eyes.

While there is no certainty or evidence that the Avast! "engineers" actually visit or listen to what's posted on the Avast! forum, it was nonetheless reassuring that the magazine site was found to be free of malicious software – which is something that all of us who work on the magazine and the magazine's website already know with a high level of surety.

Battling Hydra From Ancient Greek Mythology

Just as we thought we were getting a handle on this issue, it raised its ugly head again six days later.
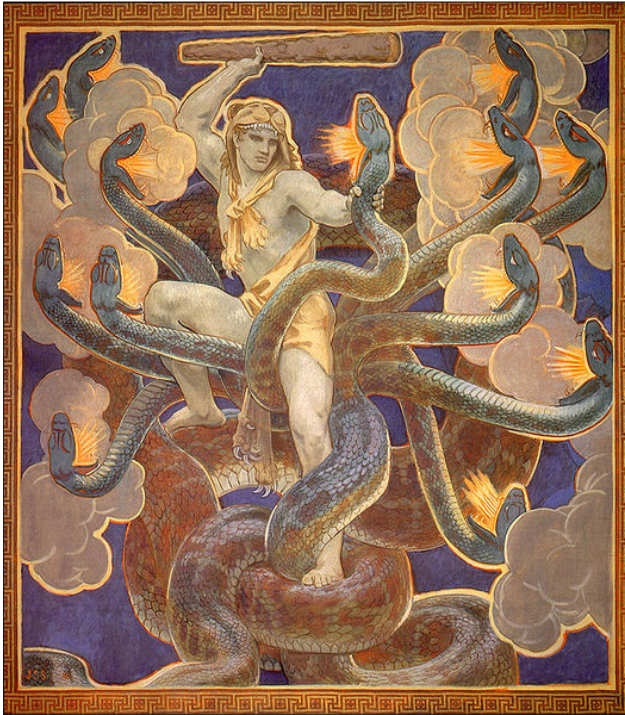
PCLinuxOS forum member BryanC1968 reported on October 12, 2013 that Avast! had flagged the magazine cover image for the October 2013 issue as malware, blocking access to the main PCLinuxOS page where it was displayed. Just as when Hercules battled Hydra in ancient Greek mythology, cutting off one of Hydra's nine heads and two grew back, the Avast! problem resurrected itself in a similar manner.

Once again, YouCanToo and Tony jumped into action to reassure PCLinuxOS users that all was safe, sound and secure.

Then, as if a repeat performance wasn't enough, Avast! flagged all of the websites hosted on YouCanToo's servers as blocked, due to spamming.

YouCanToo has taken the necessary steps to remove his server address, along with all of the sites he hosts, from this list, pointing out that none of the sites or the server itself even hosts a mail server. See? Hydra grew more heads.

How You Can Help

Regardless if you are an Avast! user or not, you can help by filing a "false positive" report on the Avast! site. Simply visit the Avast! form, at least twice. Each time you visit, report a false positive on the pclosmag.com and pclinuxos.com websites (hence, the reason for visiting the form twice). If every member of the PCLinuxOS forum and every reader of The PCLinuxOS Magazine does this, the overwhelming response will force Avast! to act quickly to remove both websites from their blocked sites list. It will also help to quickly restore the reputation of both sites to their rightful status.

Virus Scanner Ratings

If you search for "ratings of windows antivirus software" in Google, you'll get nearly 21,000,000 (yes, million) hits. So, it seems that nearly everyone has an opinion. But, in no instance that I found does Avast! rank in the top five antivirus packages. Even when I was able to find Avast! ranked in the top 10, Avast! ranked low, and even then it was only the paid Avast! Pro version that achieved that status – not the lowly free version that most users tend to use. Even at toptenreviews.com, Avast only ranked ninth out of the top ten. AVG, another popular choice among those feeling the need for antivirus software, was ranked four places higher.

Summary

It's a sad commentary on the computing industry that the most prevalent operating system is the one that is most vulnerable to viruses and other malicious software. What makes the situation even worse is that safer, more stable operating systems exist, such as Linux – and particularly PCLinuxOS. Broader adoption of Linux would literally put the antivirus software vendors out of business, en masse and overnight. Yet, with reality being what it is, we'll be plagued with antivirus software vendors having their programs running wild and rogue, providing false positives at every turn while missing legitimate security concerns. I suspect we'll see more and more of this type of failure for as long as Windows continues to exist.

I remember dual booting my computer with PCLinuxOS and Windows XP. It seems like it was a lifetime ago since I was a participant in that circus. It wasn't very long before I realized that I *never* booted into my WinXP partition. PCLinuxOS met all of my computing needs. I found Linux software to replace my trusty old Windows programs. Most of the time, the Linux software performed better and did more than the Windows counterparts. Sometimes, all it took was to look at the task or problem differently. But I had to take the time to look for alternatives.

The past seven plus years with Linux – over six of them with PCLinuxOS – may have colored my views some. For seven years, I've not found even the smallest need to run antivirus software under Linux. I don't even run antivirus software on my VirtualBox installations of Windows any more (I used to). Instead, I rely (quite aptly) on backups and snapshots of my virtual machine installations. If one of them gets "infected," all I have to do is roll my installation back to an uninfected state.

So, I do have a hard time understanding why users still rely on running software on the most insecure operating system to ever disgrace the computing industry when they are in possession of one of the most secure operating systems ever – Linux. With the Steam client coming to Linux, and thus bringing gaming on Linux to the forefront, there is no longer

any reason to have a full blown, bare metal installation of Windows.

For those other "can't live without" programs (these will vary for every user; I personally cannot think of any, except income tax software – and that is the fault of the software vendors, not the lack of a market), a virtual installation of Windows in VirtualBox or VMWare makes a lot more sense than dual booting, with the virtualized copy of Windows running on a Linux host. It places access of those programs at your fingertips, within the virtual machine, providing access to them without the need to reboot your computer.
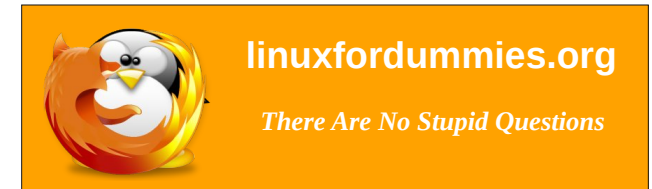
Screenshot Showcase

Posted by Texstar on 10/8, running Windowmaker.

ms_meme's Nook: Take me Home

Almost home now threads a waiting
For the debating in the forum tonight
Life is good there always you will find
Many friends to greet you come there and unwind

PCLOS is my home it's the place I belong
Linux System Texstar Take me home to the Forum

Oh what memories I have gathered
None are strangers no stormy weather
Help you'll find there easy to apply
Everyone needs it give the forum a try

PCLOS is my home it's the place I belong
Linux System Texstar Take me home to the Forum

I boot up in the morning the forum calls me
Happily I go to my home away from home
And as I log in I get the feeling
That I never will be alone be alone

PCLOS is my home it's the place I belong
Linux System Texstar Take me home to the Forum

MP3   **OGG**

Hand Of Thief Trojan: More Linux Virus FUD?

by Paul Arnote (parnote)

To be perfectly honest, I started to write an article about the "new" Linux trojan virus, Hand of Thief, back in August when it was originally announced. I originally had plans to run the article about it in the September issue of The PCLinuxOS Magazine. But something inside of me told me to wait until the dust settled. I am glad that I waited.

Originally touted as one of the first successful banking trojan viruses for Linux, Hand of Thief turns out to be just more FUD (Fear, Uncertainty and Doubt). Back in August the RSA, the security branch of EMC, reported that a group of Russian cybercriminals was looking to offer a new banking trojan that targeted the Linux operating system. That banking trojan is/was called "Hand of Thief," hereinafter referred to as HoT.

Original Claims

The developer of HoT originally claimed that it had been tested on 15 different Linux distributions, including Fedora, Ubuntu and Debian. It isn't clear if PCLinuxOS was one of the distributions that was included in the 15-distribution test group. It was also reported that it was tested on eight different desktop environments, including Gnome and KDE. Original reports also stated that it worked on common web browsers, such as Firefox, Chrome, Chromium, Aurora and Ice Weasel.

HoT was supposed to work as a "form grabber." These work by grabbing information you enter into a

form, such as your identity, any credit card information, the name of the site you are on, a timestamp of when you were on, which websites

you've visited, and possibly any cookies you have stored on your computer. It then sends that information to a command server. Once your information is recorded, it is then sold to crooks, and then you see your credit card bills soar as they go on a shopping spree.

HoT also contains code to block antivirus sites. It does this by manipulating DNS addresses within memory, rather than by doing something as obvious as changing your hosts file. By blocking access to antivirus sites, it enhances HoT's ability to hide on your computer.

HoT was offered up for sale for an initial $2,000, with some prices expected (at the time) to top $3,000 for a copy of the banking trojan. Sounds pretty scary, huh? Well, that's the way things were *supposed* to work.

What really happened

In the end, the only ones who really lost with HoT were those cybercriminals who paid $2,000+ for the banking trojan. After analysis, IT security specialists ended up with the verdict that HoT's bark was way worse than its bite. As malicious software, it failed on many fronts. According to Yotam Gottesman, an RSA Senior Security Researcher, the company

obtained the HoT code builder and created HoT binaries. Gottesman reports that HoT has no real functionality. "Our research and analysis shows that, in reality, HoT's grabbing abilities are very limited if not absent, which would make the malware a prototype that needs a lot more work before it can be considered a commercially viable banking Trojan."

Strike 1: HoT's builder is a Windows application that runs on Linux, under Wine.

Strike 2: HoT ended up not actually affecting all browsers. Instead, it simply exploited a since-patched security vulnerability in the Google Chrome browser.

Strike 3: As malware, HoT fails miserably, and in the most fundamental way: it requires the user to deliberately install it. This might work well under Windows, with its very vulnerable and naive users, but Linux users tend to have a bit more sense than that.

Strike 4: When attempting to run HoT under Firefox, it would simply cause Firefox to crash. Under Google Chrome, HoT simply grabbed useless data.

HoT ended up being nothing more than a prototype. Quite simply, it sucked at gathering data. The HoT virus builder does seem to enable virus makers to make new variants of HoT, and it does create 32 bit Linux ELF (Execute and Linking Format) executable files.

The developer of HoT has stated that he is in the process of finalizing a web injection mechanism, but the RSA doesn't think that it's of any concern – at least at this time. Given how poorly HoT works at gathering data and how the form grabber doesn't seem to work, the RSA doesn't think that his web injection mechanism is anything to fear.

Lessons?

In the end, the responsibility for the security of our computer systems rests with only one person: the end user. We – Linux users – are fortunate to be running an operating system as secure as what we have been given. Still, all the security in the world cannot stop the actions of a naive user.

Opening up suspicious emails is a bad idea. Clicking on unknown links is a bad idea. But we already knew that, now didn't we? Similarly, follow the time honored PCLinuxOS credo of *never installing packages from outside of the official PCLinuxOS repository*, since all of the packages in the PCLinuxOS repository have been built and tested by reputable developers who have nothing but the best interest of PCLinuxOS and its users in mind. You never are quite sure of the quality or reputation of packages from outside of the PCLinuxOS repository, so even packages from supposedly reputable outside sources can be suspect.

Simply applying some common sense and adhering to these simple "rules", PCLinuxOS users can go a long way towards keeping themselves safe from whatever harm cybercriminals might want to send our way.

The PCLinuxOS Magazine

Created with Scribus 1.4.3

Screenshot Showcase

Posted by RobNJ on 10/7, running Enlightenment.

PCLinuxOS Puzzled Partitions

5	9		2			6	3	
4		2				8	9	1
6				8	9			
	4		6					
	8	6		3		9	7	
					7		8	
			3	2				9
3	5	9					1	4
	1	7			5		6	8

SUDOKU RULES: There is only one valid solution to each Sudoku puzzle. The only way the puzzle can be considered solved correctly is when all 81 boxes contain numbers and the other Sudoku rules have been followed.

When you start a game of Sudoku, some blocks will be prefilled for you. You cannot change these numbers in the course of the game.

Each column must contain all of the numbers 1 through 9 and no two numbers in the same column of a Sudoku puzzle can be the same. Each row must contain all of the numbers 1 through 9 and no two numbers in the same row of a Sudoku puzzle can be the same.

Each block must contain all of the numbers 1 through 9 and no two numbers in the same block of a Sudoku puzzle can be the same.

SCRAPPLER RULES:
1. Follow the rules of Scrabble®. You can view them here. You have seven (7) letter tiles with which to make as long of a word as you possibly can. Words are based on the English language. Non-English language words are NOT allowed.
2. Red letters are scored double points. Green letters are scored triple points.
3. Add up the score of all the letters that you used. Unused letters are not scored. For red or green letters, apply the multiplier when tallying up your score. Next, apply any additional scoring multipliers, such as double or triple word score.
4. An additional 50 points is added for using all seven (7) of your tiles in a set to make your word. You will not necessarily be able to use all seven (7) of the letters in your set to form a "legal" word.
5. In case you are having difficulty seeing the point value on the letter tiles, here is list of how they are scored:
  0 points: 2 blank tiles
  1 point: E, A, I, O, N, R, T, L, S, U
  2 points: D, G
  3 points: B, C, M, P
  4 points: F, H, V, W, Y
  5 points: K
  8 points: J, X
  10 points: Q, Z
6. Optionally, a time limit of 60 minutes should apply to the game, averaging to 12 minutes per letter tile set.
7. Have fun! It's only a game!

Tux Scrappler

Download Puzzle Solutions Here!

Points Possible – 214, Average Points - 150

PCLinuxOS Crossword Puzzle: November 2013
CLI Commands

Download Puzzle Solutions Here!
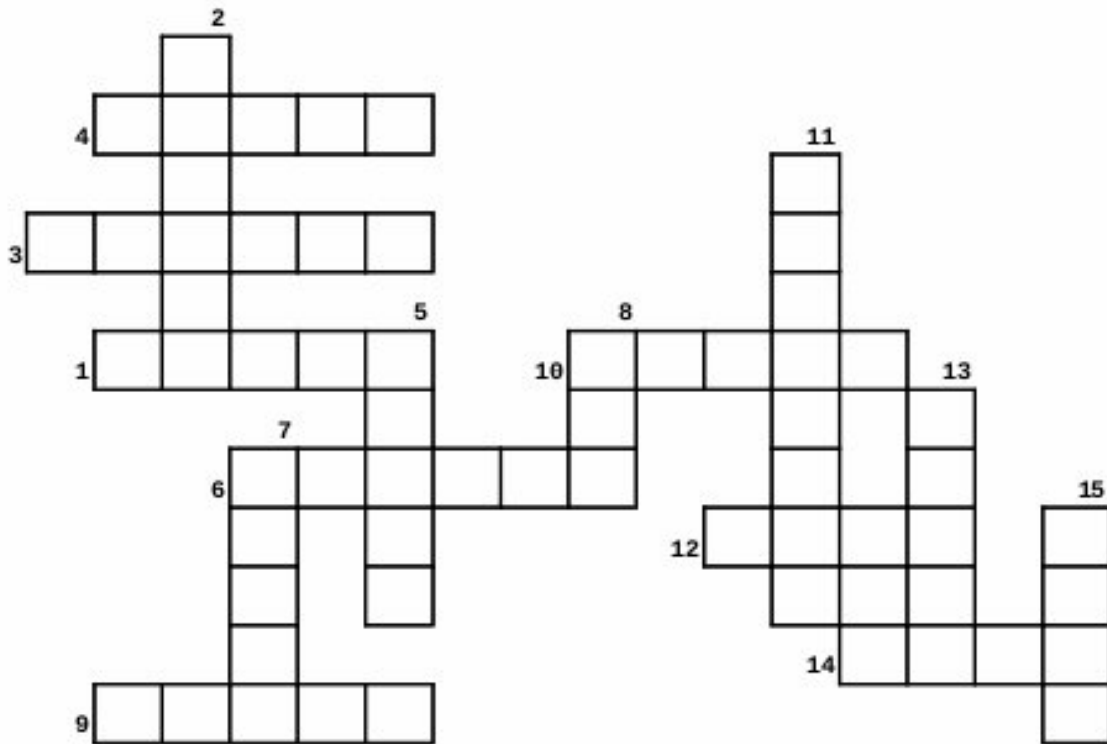
1. synchronize 2 sets of files

2. shows what a certain command does

3. view a process chart

4. change ownership of a file

5. backup an entire file system

6. unmount a file system

7. show information about a machine and OS

8. concatenate

9. empty the terminal screen

10. change permissions on a file or directory

11. wireless configuration information

12. find a data file

13. create a directory

14. show a memory usage chart

15. search a log for a certain pattern

CLI Commands Word Find

```
T E R Q K V N T W U C G W K K D O R B M O B P L M I S V C M
M H F V J N I R J H S Z J W M U N J Z D Y K C S M F S C K K
E H E Q W T W W M Y S C O W R T S U X Q U L C C U N E D H K
F V G U O B N O H D H J B C R S T Q M S R U J G C C I T J N
G I B Y E U D N H R C N Y S R H J P J Z J D M V B R C A T K
Y F L T H P J I Q C S U S W O G F I G E N D D N I O U G V S
H W H E R E I S P K X J E S V E W M U W T L A Z P U Q Q O C
Y U V A W E E G S Y H R Q M O H D T Q U T T U W N O O I M H
P B K U R R G R O L P K T T A Q P U M P E T C W U N H A I X
Y W B W Q T H A V P K H F T Y O Y H A Y S A E P A J L K R P
O X N Z N S A X G C D N I F Y C V W V M Z M Z V X U S B G C
F V K S Y P A Z K O K S T O B Z Y F R Y A G Y C D K M T S A
M H J U O F B Y A S W E N O L C Y Z D N O N C E J U E C S A
C Y C W B W T M S E O A O T H J L W E C E U D R S Y T T X V
S N H O D P T E E Q C K Q H S S F S T E B A C K U P B J A A
Z P P P K D S U B S F W A C O B A P E V J Y C N P I E R Q J
O X Q Q O B J Y C E O C K P N B Z U Z C H E A L L Z S R M L
D C D I G C J I W P T T O Y G J J T T J H M K J Q X I Y G Z
J V S J D Y I O B R M R V J T E Q F F Q E O V A U R K F N P
Y U B J Y E Y J J B P B E R R R K P R C H L E D P Z P U Z A
M P W A G N X J L A H B E N L O C A T E Y I A J T N N K J V
U M O U N T V G Z N R C N P N G I O C J E M C J W X X Q H U
F O K Z G F K R P X H Y V N T R U J V M G R B T R W J F K M
S B N Q F W I H Z G U G V A C L L Y N M E N O H U B Q U K Q
X B S P K H G V U H U Q D S F G I F N O C W I O W C L Z Z W
K H R O L E V X S Q A T L H T Q B A P U C U W H Q S C S T W
X K C E B D S E K Z E J K K J J J X H K J P Z D T N Q B H I
B B P C X R A E L C V A R T U C N F Q P S T I S V F Q G P W
N X W A P A D B T H S M Y Z Q M G Q H Z W W O T O L S U Z E
Z Q O P V H Z Z T P L J W S P E E U Z G K Q I W P W O H H Y
```

cat
locate
whereis
find
uname
mkdir
chmod
chown
pstree
whatis
backup
clone
rsync
umount
iwconfig
grep
echo
apropos
basename
lshw
cksum
clear
file
free
fsck

Xfce Power User Tips, Tricks & Tweaks: Xfce's Built-In Wallpaper Slideshow Made Easy

by Paul Arnote (parnote)

In this, the eighth article in the "Xfce Power User Tips, Tricks & Tweaks" series, we'll take a look at leveraging and tweaking Xfce's built-in desktop wallpaper slideshow capabilities. I actually have two incarnations of this tweak, each approaching the task from different directions.

Desktop Settings

To understand what we're about to do, we first need a basic understanding of Xfce's Desktop Settings applet. This applet is the "control center" for almost everything that pertains to your Xfce desktop – at least, in a visual sense. It's where you set the wallpaper, whether to display a context menu when you right click on the desktop, the brightness of the desktop wallpaper, and what icons to display on the desktop (if any at all), among other settings. Most users' will be most interested in the "Background" tab, which is the first one displayed, and that's what we'll restrict our discussion to for this article.

You can open the Desktop Settings applet by two slightly different ways. The fastest way is to right click on a "blank" area of the Xfce desktop, and select "Desktop Settings" from the context menu. You can also access it from the Xfce Settings Manager.

By default, Xfce is setup to display a single image as the desktop wallpaper. Thumbnails of the images available for use as wallpaper images are shown in the list on the left upper side of the dialog box. On the right upper side of the dialog box, your choices are "Single Image" (the default), "Image List" (what we're going to end up using), and "None" (where
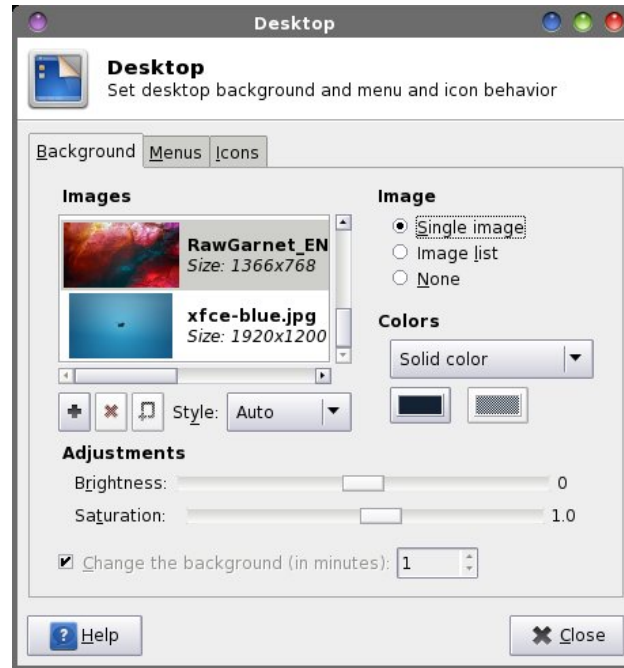
Xfce displays no image and a single color or a gradient between two colors).

Below the thumbnail display list are three buttons, labeled "+", "X" and a square with a + in the lower left corner (hereinafter referred to as the "New List" button). While in the "Single Image" mode, only the + button is active. Clicking on this button will allow you to select another image – like one of your own images – besides the default images, which are stored in /usr/share/backgrounds/xfce and /usr/share/xfce4/backdrops/.

Next to those three buttons is a drop down list button, with "Style" next to it. By default, it is set to "Auto." However, you can also choose from Centered, Tiled, Stretched, Scaled and Zoom. Most of the time, the Auto setting will serve most users

well, setting the wallpaper to fill the desktop dimensions.

At the bottom (grayed out in the image) is another control, called "Change the background (in minutes). This control is **only** available when the "Image List" option is selected. Simply set how long you want to wait before the wallpaper image is changed.

So, let's select "Image List" from the "Image" selection area in the upper right corner of the dialog box. After you do that, the X and New List button to the right of it are activated, as well. The control at the bottom of the dialog box is also now activated and ready for use.

You will notice that once we selected Image List, we don't have any wallpaper displayed. That is because we don't have a wallpaper list yet. Click on the New List button, and select a directory to place the list, and enter a filename for your new image list. You can name it anything (I called mine "Test"), and you don't have to supply a filename extension. Now, click on the + button, and add an image from your hard drive to the list. Keep repeating this procedure for every image you want to add to the image list.

After you add more than three images to the list, you won't see the thumbnail list being updated. Don't worry – the images are being added to the list. If you want to refresh the list, close the Desktop Settings dialog, then reopen it. This process can become a bit arduous, especially if you have a lot of images that you want to put into your image list.
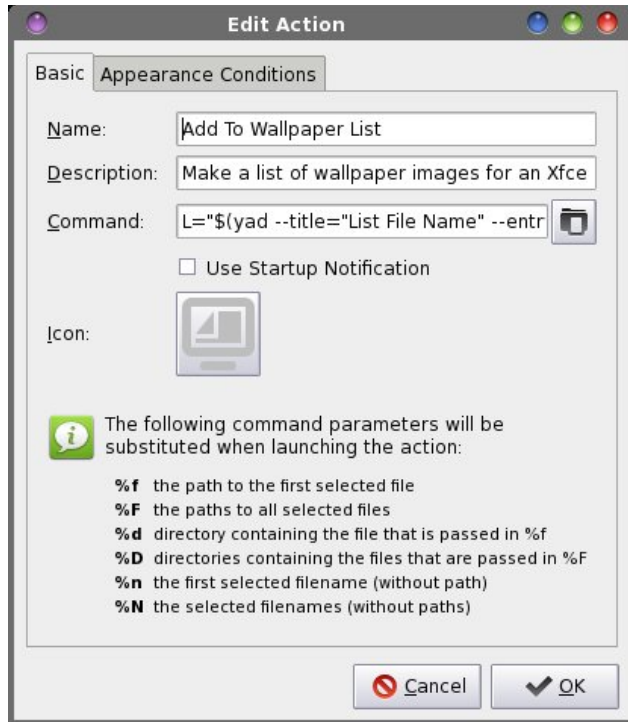
Add To Wallpaper List

If you have wallpaper images scattered around a bit, then this Thunar Custom Action is for you. With it,

you can right click on an image file (*.png or *.jpg), or multiple image files, and add the image(s) to any image list you want/specify.

Enter "Add To Wallpaper List" into the "Name" field, and "Make a list of wallpaper images for an Xfce desktop slideshow" into the "Description" field. Now, enter the following into the "Command" field:

```
L="$(yad --title="Image List Filename" --
entry --entry-label="Please enter the
filename")"; if [ ! -e $L ]; then echo "#
xfce backdrop list" >$L; fi && for file in
%F; do echo $file >>$L; done
```
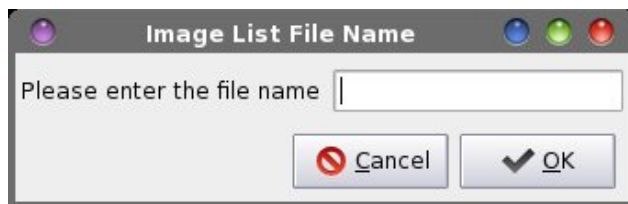

Under the "Appearance Conditions" tab, leave the file pattern set to the default value of *, and place a checkmark in front of "Image Files."

The command allows you to specify the name of the image list file you want to create or add to (remember, you don't need to supply a file extension). If the file doesn't already exist, it is created. The first line of the file, if it doesn't already exist, is written out to the new file. That line is "# xfce backdrop list" and is vital for the file to be recognized for what it is: an image list for the Xfce Desktop Settings. Otherwise, it skips writing that vital first line. Then, the files are appended to that file one at a time, with the redirection command (>>) that tells Linux to append the path and filename of the image to the specified image list file.

Now, whenever you right click on an image (or multiple images), you can select "Add To Wallpaper List" from Thunar's context menu. Be sure to hold down the Ctrl key on the keyboard to select multiple images. The image's (or images') path and filename will be added to the wallpaper list that you specified in the initial dialog box.

Create Wallpaper List From Directory

If you are a bit more organized with how you store your wallpaper files, this Thunar Custom Action is for you. I tend to keep all of my wallpaper images in a folder in my /home directory, called Wallpaper. Within that directory, I have subdirectories with categories of images. I have a subdirectory for images downloaded from National Geographic, others downloaded from Bing, space images, bicycling, architecture, and so on. With this custom action, I can create custom wallpaper image lists for each folder.

Enter "Create A Wallpaper List From Directory" in the "Name" field, and "Make a wallpaper list from a directory of JPG and PNG images" in the
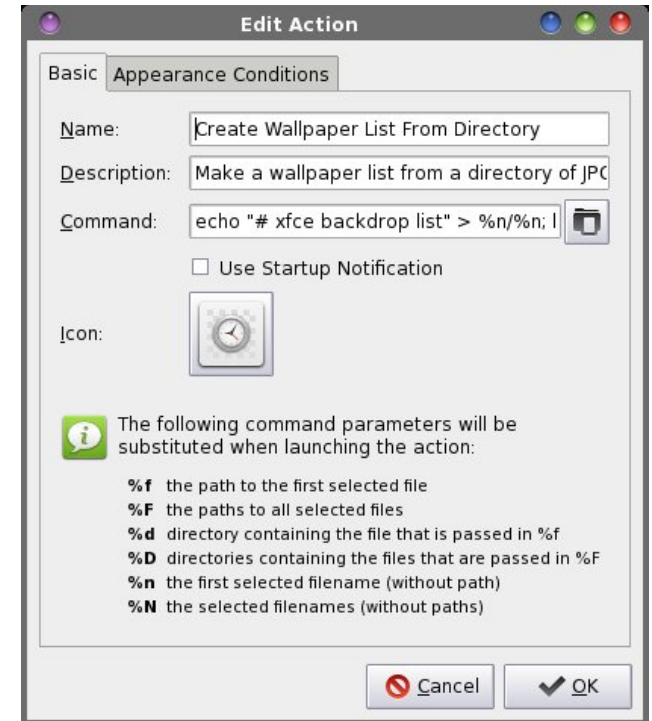
"Description" field. Now, enter the following into the "Command" field:

```
echo "# xfce backdrop list" > %n/%n; ls -1
%f/*.* |egrep
*.'[jJ][pP][eE][gG]|[jJ][pP][gG]|[pP][nN][g
G]' >>%n/%n
```

Under the "Appearance Conditions" tab, leave the file pattern set to the default value of *, and place a checkmark in front of Directories. Now, when you right click on a directory filled with JPG and PNG image files, they will all be added to a new image list file that is placed *inside* the directory directory that we initially selected.

The first echo command writes out the necessary first line (# xfce backdrop list) to the file, and then lists the contents of the directory (ls), one line at a time (-1), and appends each qualifying file (jpg/JPEG/png) to a the image list file.

If you use this custom action to create an image list file from a directory, and you add more files to the directory, you may want to delete any existing image list file before creating a new one. Nothing bad will happen if you don't. But because there is no checking to see if a filename is already listed, all of the previous files will be listed again, appended to the end of the file, along with the new files. Because the previous files will be listed twice and the new ones once, the previous files will be more likely to be displayed than the new ones, due to the random way that Xfce displays images on the image list file. Also, the file will be much larger than it needs to be, if you don't delete the old image list file.

Putting The Image List To Work

Here is an example of the image list file that is created (because of the length of each line, each "line" in the file is separated by a blank line below):

```
# xfce backdrop list

/home/parnote-
t42/Wallpaper/Bing/AustRifleBird_EN-
US11527683146_1366x768.jpg

/home/parnote-
t42/Wallpaper/Bing/ChicagoBeach_EN-
US9395095266_1366x768.jpg

/home/parnote-
t42/Wallpaper/Bing/CrotonDam_EN-
US9172558444_1366x768.jpg

/home/parnote-
t42/Wallpaper/Bing/DenaliSquirrel_EN-
US7652248865_1366x768.jpg

/home/parnote-
t42/Wallpaper/Bing/GiraffesNamibia_EN-
US12247342256_1366x768.jpg

/home/parnote-
t42/Wallpaper/Bing/GreatWallLocks_EN-
US5596619996_1366x768.jpg
```

```
/home/parnote-
t42/Wallpaper/Bing/IcelandTrek_EN-
US10476835436_1366x768.jpg

/home/parnote-
t42/Wallpaper/Bing/KataleKhorCave_EN-
US6707191757_1366x768.jpg

/home/parnote-
t42/Wallpaper/Bing/LakeTiticaca_EN-
US7480201705_1366x768.jpg
```

As you can see, it's nothing more than a list of eligible graphic files, with their complete path and filename listed, one per line. The first line of a Xfce image list file must always be "# xfce backdrop list" or Xfce will not recognize it as such.
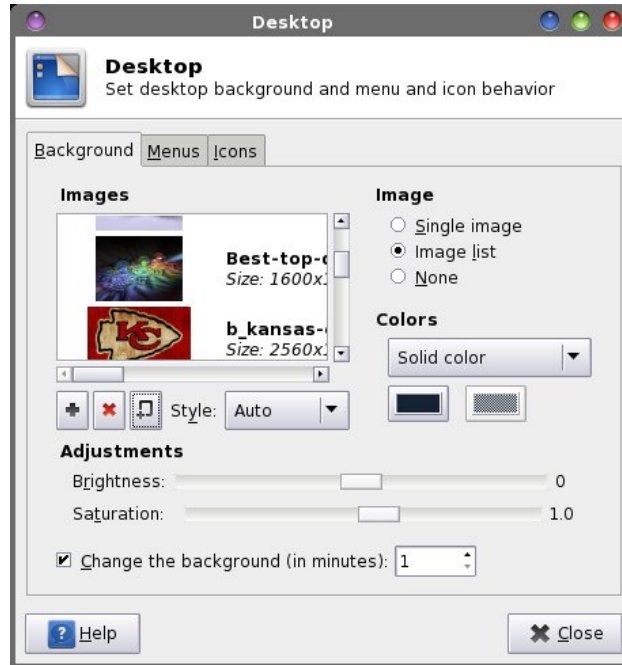
Back in the Desktop Settings window, click on the New List button and select the image list file that you just created. Remember, your new image list file is inside the directory that you chose. Or, you can select the image list file you created with the previous custom action.

You can select to rotate or change the background image by placing a checkmark in front of "Change the background (in minutes)" option, and set the number of minutes you want Xfce to change your wallpaper. Because I was testing, I had the time set to only one minute. More realistically, you'll probably want to set a longer time interval. The default value is 10 minutes.

The selection of which image to display is completely random, selected from the image list. If you choose to not rotate your wallpaper images on a timed basis (by leaving the "Change the background" setting unchecked), Xfce will display a random wallpaper image every time you log into your Xfce desktop, and display that image for the duration of your session.

One word of caution, though. If you use the NatGeo-POD or Bing scripts from the September and October issues of The PCLinuxOS Magazine, respectively, and have them "set" to change your wallpaper, the Desktop Settings will switch back to "Single Image" mode. If you simply download the images with those scripts – without having them set the images as your wallpaper by using the **-d** command line switch – it will not change the Desktop Settings back to "Single Image" mode. But keep in mind your newly downloaded images won't be in the image list file, until you either add that new image to the relevant image list file, or until you delete the old list and rebuild it (if you are keeping all of your NatGeo and Bing images in their own directories and use the custom action that builds the image list file from the directory).

Summary

As you can see from the articles in this series, there are a lot of "extras" you can use to customize Xfce to your liking. These tips, tricks and tweaks can add a lot of extra "horsepower" to your Xfce computing experience.

You are limited only by your imagination. I'm certain that there are Xfce tips, tricks and tweaks that I have missed or not discovered yet. Of course, the better your understanding of the command line, the more you can imagine being done. The ones I've presented to you are the ones that I have found a recurring need for. There are some that are not used frequently, but their presence definitely is appreciated for those times when I do find a need to use them. There are others that I use almost daily.

If you come up with – or come across – additional Xfce tips, tricks and tweaks, I'd love to hear about them. Feel free to send me a PM in the PCLinuxOS forum, or send me an email at pclinuxos.mag@gmail.com. I'll be happy to write them up for The PCLinuxOS Magazine.

Screenshot Showcase

Posted by MerReady on 10/9, running Mate.

PCLinuxOS Family Member Spotlight: Bubba Blues

by Bubba Blues, as told to smileeb
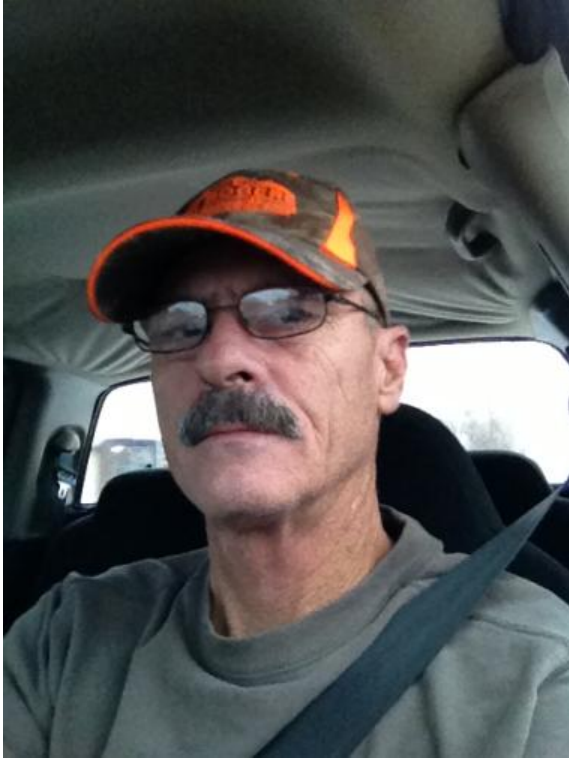
Me in my pick-up on a work day.

How old are you?
I'm 58 years old.

Married, single or what?
Married to my wife for 25 years.

Children, grandchildren?
I have four children ranging from 40 years old to 23 years old. I have three granddaughters, and and one grandson.

Retired or working and for how long and at what?
I'm still working, but not as many hours as I used to. I've been a carpenter/cabinetmaker
for almost thirty five years.

What is the area you live in like? Weather, Quietness, Scenery.
I live in western Oklahoma where the summers are too hot (sometimes up to 115 F) and the winters are too cold. (sometimes 10 below zero F). The wind blows a lot. I've seen straight winds up to 60 mph, and it's also in the middle of Tornado Alley. But the people make up for it. Some of the best folks in the world are right here in Oklahoma. My house is in a rural area where it's a 40 mile drive to the nearest Wal-Mart, but only 12 miles to the nearest small town. My house is about 100 yards off the county road, but a half mile off the main highway so it's nice and quiet. We have lots of deer, coyotes, opossums, raccoons, bobcats, rabbits, squirrels, etc. Rolling hills with mostly cedar, black jack oaks and locust trees.

Are you handy with your hands and have any hobbies?
I've made a living doing woodwork for 35 years. My hobby I suppose is music. I've played guitar even longer than I've been carpentering. I've played in rock, country, blues and Motown bands, but now I'm playing in two different Christian bands. One on Sunday mornings, the other on Sunday nights.

Do you like to travel, go camping?
I love to travel, as long as I'm seeing new countrysides. I love history and nature. I love visiting historical landmarks, monuments, etc., and I love natural wonders. I can't travel as much as I'd like, but I like it when I can.

What caused you to try Linux and join this forum?
I just got fed up with spyware, viruses, malware and Windows in general. My son finally got me to try Linux about five years ago, and I've been a loyal Linux user ever since. I have two or three distros installed on my desktop at all times, and one on my laptop.

Me with my lovely wife one night at a gig I was playing.

PCLinuxOS Family Member Spotlight is an exclusive, monthly column by smileeb, featuring PCLinuxOS forum members. This column will allow "the rest of us" to get to know our forum family members better, and will give those featured an opportunity to share their PCLinuxOS story with the rest of the world.

If you would like to be featured in PCLinuxOS Family Member Spotlight, please send a private message to smileeb in the PCLinuxOS forum expressing your interest.

Game Zone: Arma Tactics

by daiashi

About The Game

Arma Tactics takes the best from the popular strategy genre, and moves across platforms. The finest assets used in the critically acclaimed Arma™ series on PC now come to life on the Android, iOS and Steam platform. Arma Tactics is a turn-based close-combat strategy game, where the player takes control of a four-member Special Forces team. There are no given strategies, rails to move on, or paths to follow; it's up to the player to decide how he will play through both the story-driven missions and generated missions with randomized objectives. Whether using stealth or a more direct approach, players will need to use their strategic thinking and use both basic and advanced weaponry while facing many different opponents - ranging from unorganized local militia to smart and skilled mercenaries. With highly re-playable missions, weapons to unlock and whole campaigns to be regularly added, Arma Tactics offers many hours of intense ever-changing action.

Main Features

Explore highly detailed battlefield environments that come to life with sophisticated particle systems and post-process effects. See your men come to life with realistic animations captured by a powerful motion-capture solution. Lead them through a thrilling single player campaign or improve your skills in generated missions. Gather experience points to level up your characters, upgrade weapons and unlock special equipment. You can choose difficulty level, helping to make sure the game is fun to play for both casual players and hardcore gamers, and take part in challenging special game modes.

For me, the game seemed a lot like Jagged Alliance, if anyone remembers that title. Controls, in my opinion, are not as polished as they should be. Game play is pretty fluid in that you are not jumping all over the place as you play through the story line. Although the minimum system requirements are stated below, and I do exceed these, there was a little lag at times as there are not many graphic changes in the options. I have found that all of the games in the Arma series simply do not run very well on a computer with the minimum specs. It may be the port to Linux or an Nvidia graphics driver issue. Nevertheless, it is still a fun game and I would recommend it if you are into the turn base strategy type games. If you have some time on your hands and like this series, this game may just fill those shoes.

System requirements

Software:
PCLinuxOS and Steam

Hardware:
Minimum:

Processor: Intel Core 2 Duo
or dual core AMD XP or better
Memory: 1 GB RAM
Graphics: Shader Model 2 and higher
graphics card
Hard Drive: 750 MB available space

About The Company

Established in 1999 in Prague, Czech Republic, Bohemia Interactive is an independent game development studio that focuses on developing original, state of the art computer entertainment and simulation software, including the research of proprietary advanced real-time 3D graphics, artificial intelligence and physical simulation technologies for real-time interactive environments.

Operation Flashpoint*, Bohemia Interactive's debut game published by Codemasters in 2001, became the No. 1 best-selling PC game around the world and has won many international awards, including "Game of The Year" and "Best Action Game." It was later renamed to Arma: Cold War Assault.

Bohemia Interactive's second major release, Arma: Armed Assault, followed in 2007, and in the same year, the Arma: Queen's Gambit expansion pack was released.

Arma 2, another hit in the series of tactical military shooters, released worldwide during summer 2009 and was placed in the top positions of official PC charts around the world immediately thereafter. Arma 2 won "Most PC" Game in the 2009 PC Gamer

Awards and is featured 14th in their "Best PC Game of all time".

Following the release of Arma 2, the standalone expansion pack Arma 2: Operation Arrowhead was developed. This massive expansion was strongly received by both critics and fans alike; reviews considered it as surpassing the previous title and building on its strong mil-sim heritage. The 'Armaverse' was then expanded further by the hugely popular British Armed Forces (BAF), Private Military Company (PMC) and the Army of the Czech Republic (ACR) DLCs. To date, the Arma series has sold over 5 million units.

In November 2011, Bohemia Interactive released Take On Helicopters, an authentic civilian helicopter game set in a virtual recreation of Seattle. It was well received, with multiple reviewers praising its refreshing take on the flight sim genre. The game was reinforced shortly after by the Take On Helicopters: Hinds expansion pack and the free Noisecontrollers and Rearm ed DLCs.

About a year later, in October 2012, Bohemia Interactive shipped Carrier Command: Gaea Mission for Windows PC and Xbox 360. Based on the classic game from 1988, it was the first multiplatform title to launch under the Bohemia Interactive flag.

Recently, the studio saw its open attitude towards modding rewarded by the massive success of the DayZ survival mod for Arma 2: Combined Operations. With over a million players, the creator of DayZ - Dean Hall – has announced a partnership with Bohemia Interactive to create a standalone version of DayZ.

This year, on September 12, the most recent instalment in the successful Arma series – Arma 3 - was released. Starting with the Arma 3 Alpha in March, people were invited to participate in the game's development ahead of the game's official release. Building upon the Alpha's massive success,

the game transitioned into Beta in June – bringing along further refinements as well as new playable content. The final game introduced new playable and sandbox content, plus the massive 270 km² Altis terrain. The official single player campaign is scheduled for release across three DLC episodes.

In addition to Arma 3, in 2013, the Arma franchise also moved into the turn-based strategy genre, with the release of Arma Tactics on Android, iOS, PC, Linux and Mac. Holding on to Arma's signature freedom, players take control of a four-member Special Forces team, tasked with a diverse set of missions and no given strategies or rails to move on.

Bohemia Interactive recently expanded its Take On series with the brand new space exploration sim game: Take On Mars. In Take On Mars, players take on the role of a Rover Operator to explore real-life locations on Mars. The game is currently available as an Early Access title on Steam.

Bohemia Interactive won the 2001 Best PC Game Developer award at London's ECTS exhibition and Rookie Studio of the Year award at GDC 2002.

Some Gameplay Screenshots
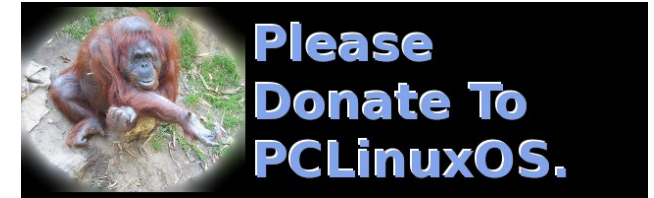
Screenshot Showcase

Getting It To Run

You will require just an updated PCLinuxOS system, the Steam launcher from Synaptic, and a Steam account. There is a demo available, so I would recommend that you grab this first to get an idea if your system can play it.


Posted by jogurtmen on 10/13, running KDE.

KeePassX: Not In The Cloud

by Yankee

With recent events in computer security in the news and cloud services being considered not as reliable as in the past, here's an old, reliable, password program available in the PCLinuxOS repos. It's called KeePassX. The passwords for all your websites are kept locally, encrypted and have a password and/or keyfile for security.

By pressing Ctrl plus a letter into your username/password field, the field(s) are filled in automatically. By putting the site URL into each website entry the program can also act like a website bookmark database, which is another good feature for your most secret websites while using private browsing. Websites needing extra security could be kept separate from your other website bookmarks through KeePassX.
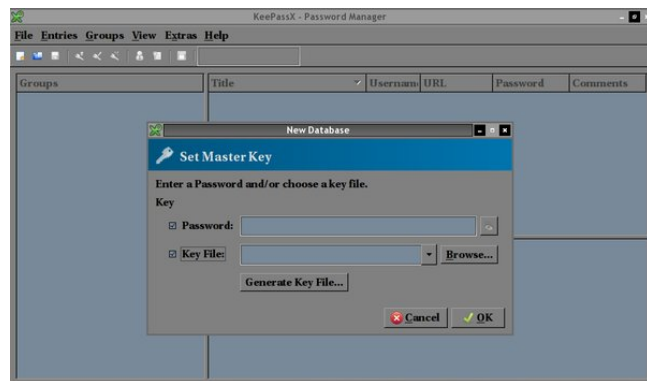
Once installed through Synaptic, click **File > New Database**, and a window similar to the one above appears. I usually just use a password, but either a password, a keyfile, or both can be used. The key

file can be any file on your computer, e.g. a picture or a text document. You can also create a randomly-generated key file by first selecting the key file check box and clicking "Generate Key File..." You can store the key file, for example, on a USB memory stick, to keep it with you everywhere. So, create the database and click **File > Save As** to name it, then save the encrypted database to somewhere you choose.

Next, click **Extras > Settings** and the configuration box appears. The following are reliable default settings. Place a checkmark in front of each of the following items.

General (1): Show system tray icon, Minimize to tray instead of taskbar, Remember last opened file, Start minimized, Save recent directories of file dialogs, and Always ask before deleting entries or groups.

General (2): Save backups of modified entries into the 'Backup' group, Automatically save database after every change.

Appearance: Select the colors you want to use for the gradient that is displayed in the banner, followed by the color of the text that is displayed within that banner. Alternating row colors, Expand all items.

Security: Clear clipboard after **10** seconds, Lock workspace when minimizing the main window, Lock database after inactivity of **30** seconds.

Advanced: Media Root: /media/, Save relative paths (bookmarks and last file), Auto-Type Fine Tuning Pre-Gap 1000ms, Keystroke Delay 100ms, Global Auto-Type shortcut Ctrl + a, Use entries' title to match the window for Global Auto-Type.
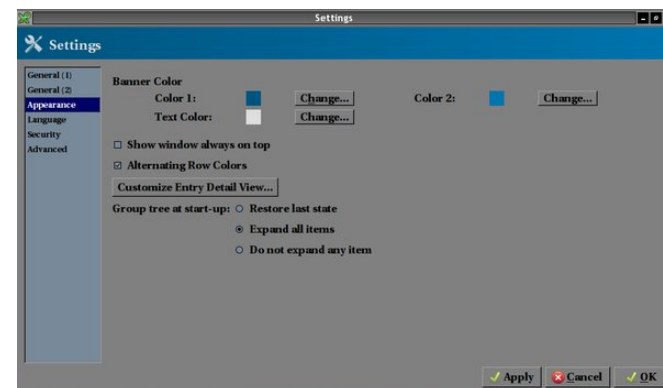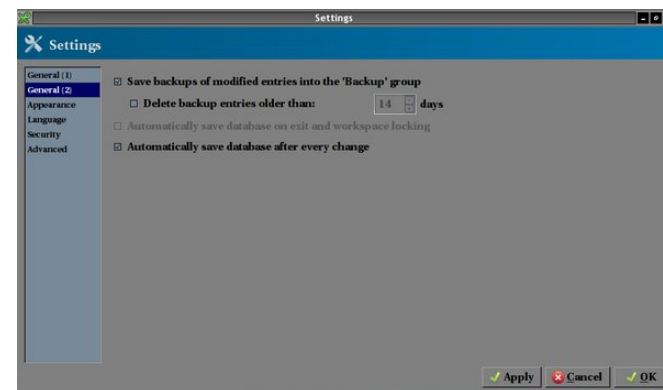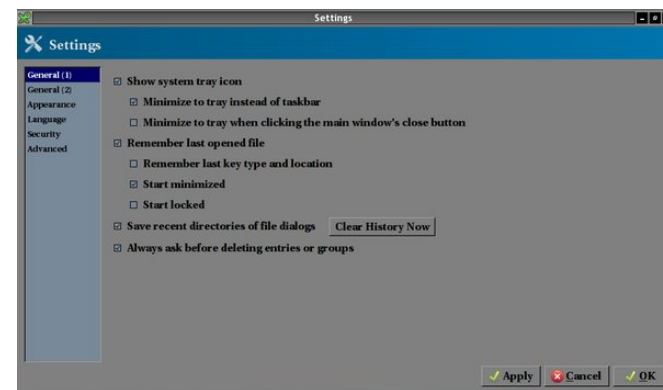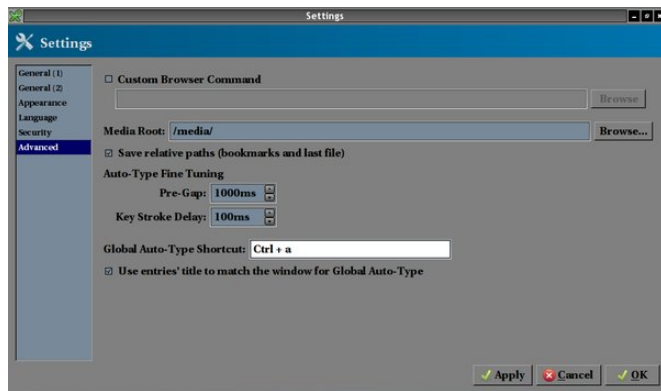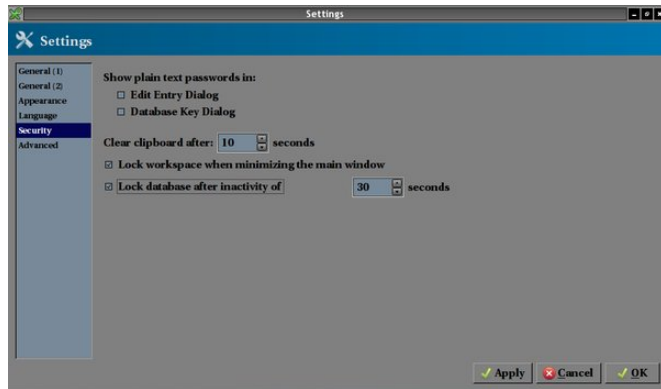
Once you checked the appropriate boxes, click Apply, click OK, click **File > Save** to save the database. These generally do not have to be changed again.

Configuring a website password entry

Now we can select a group in the database tree and click **Entries > Add New Entry**, and the dialog box at center top appears.

Notice the Tools box in the lower left hand corner. Click there to get the Auto-Type line, Customize Sequence, and also click there to select the Auto-Type-Window line which is the Select target window item. Click to select and enter that on the second line above selecting the correct target window title.
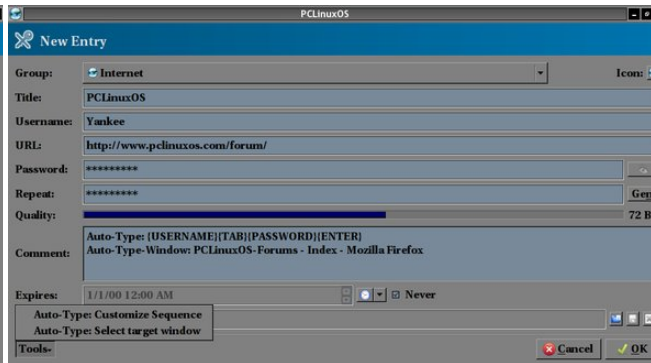
This configures KeePassX to enter the info (username and password) configured in line 1 when **ctrl + a** is used on the webpage title configured on line 2. These can also be adjusted manually if needed.

When creating a custom window/sequence association manually, you need to tell KeePassX how the matching window titles look like. Here, KeePassX supports the use of * as a simple wildcard.

String with Wildcard	Meaning
STRING	Matches all window titles that are named exactly "STRING".
STRING*	Matches all window titles that start with "STRING".
*STRING	Matches all window titles that end with "STRING".
STRING	Matches all window titles that have "STRING" somewhere in the window title. This includes the string being directly at the start or at the end of the window title.

We didn't use these to configure the PCLinuxOS forum entry, but will use them when configuring an entry with multiple windows next. Be sure the database is saved now.

Configuring websites with two login windows :

Overall, there are two methods to configure sites that have two login windows. The first addresses site windows that have different login window titles, the second addresses site windows that have the same login window titles. We will avoid problems with automated methods by just pressing **ctrl + a** twice, once for each window when it appears. Challenge questions randomly appearing during login, and trying to use the URL as window ID when URL's frequently change, can both stop an automated method in the middle of the login. These two methods avoid anything that could stop the auto type from being successful.

Method 1 - different login window titles :

Simply type similar syntax into the lower add/edit entry box for the named website. Otherwise configure the entry in the normal manner, filling in the field information in the usual manner in the upper add/edit entry box.

Auto-Type: {USERNAME}{ENTER}
Auto-Type-Window: Bank of New York — Hello*
Auto-Type-1: {PASSWORD}{ENTER}
Auto-Type-Window-1: Bank of New York - Login*

Pressing ctrl + a once for the first window, wait, and then press
ctrl + a again when the second window appears.

Method 2 - same login window titles :

Two entries need to be created and configured using the add/edit entry box twice. Configure the entries in

the normal manner, filling in the field information in the usual manner in both upper add/edit entry boxes. For entry titles in the upper box use "Bank of New York 1" and "Bank of New York 2," for example, quotes omitted.

For the first entry, type similar syntax into the lower add/edit entry box for the named website. For "Bank of New York 1"

Auto-Type: {USERNAME}{ENTER}
Auto-Type-Window: Bank of New York - Online*

For the second entry type similar syntax into the lower add/edit entry box for the named website. For "Bank of New York 2"

Auto-Type: {PASSWORD}{ENTER}
Auto-Type-Window: Bank of New York - Online*

You can see the website's login Auto-Type-Window's are both titled the same.

Now, when the first login window appears and you use **ctrl + a**, a box will appear allowing you to choose from "Bank of New York 1" or "Bank of New York 2" . Choose "Bank of New York 1" for the username field, wait, then when the second window appears and you use ctrl + a, choose "Bank of New York 2" for the password field in the second window. The pop-up box looks like this.
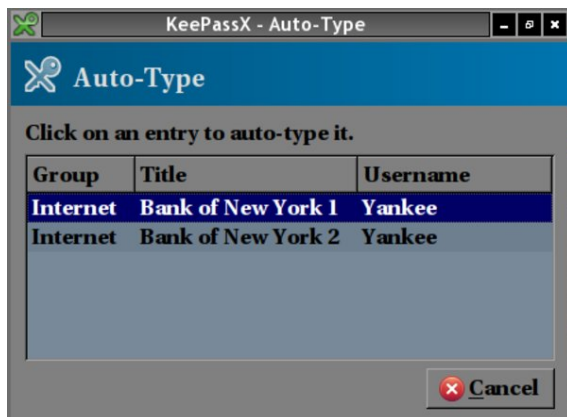
Select the first entry for the username window, and the second entry for the password window.

You should now be able to fly thru multiple login window configurations with one of the two above methods. Once you configure these, you'll be able to configure any website to use KeePassX to securely store its username/password and auto type the username/password into the appropriate window, saving manual keystrokes or copy and paste routines.
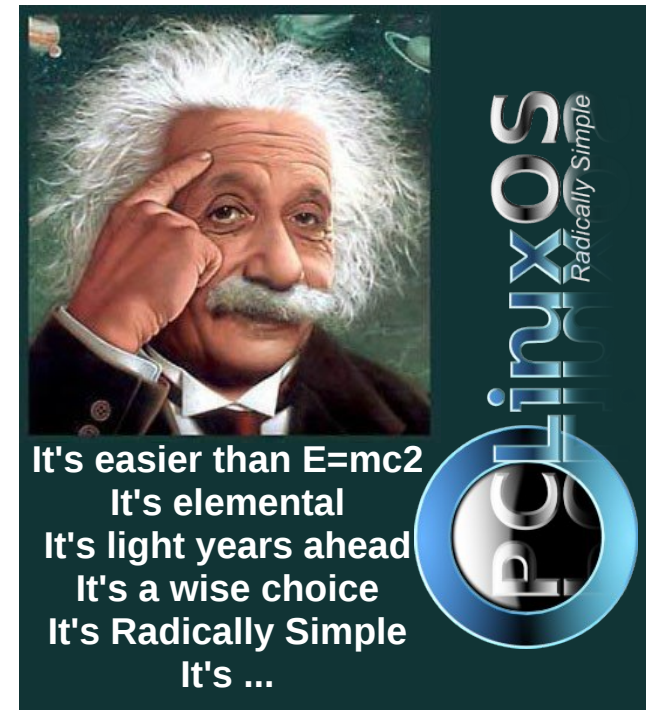
Encrypting Your Email In Thunderbird

by YouCanToo

With *"big brother"* and others snooping more and more into our personal lives, how can we take back some of our privacy?

One way is by encrypting our email and telling others why they should do the same. This article will show you how to setup Thunderbird (Linux, Windows and Mac OS X - 32 or 64 bit) using GnuPG and the enigmail addon.

To get things started we need to open Thunderbird. Once open we want to click on **tools > add-ons**. In the addon search bar we want to search for "enigmail". Select it and then click **Install**.
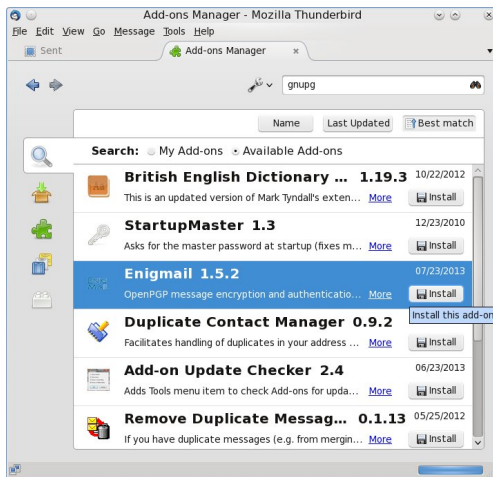
Once this has installed click on "restart now". This will restart Thunderbird with your new Enigmail addon (center, top).

NOTE: The Enigmail addon only works with Thunderbird, IceDove and Seamonkey.
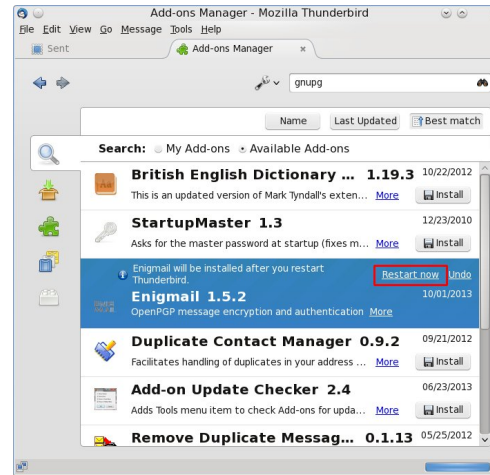
Upon restarting Thunderbird, you should notice a new tab has been added to the top bar called "OpenPGP". Click on "OpenPGP" and then select "Setup Wizard"
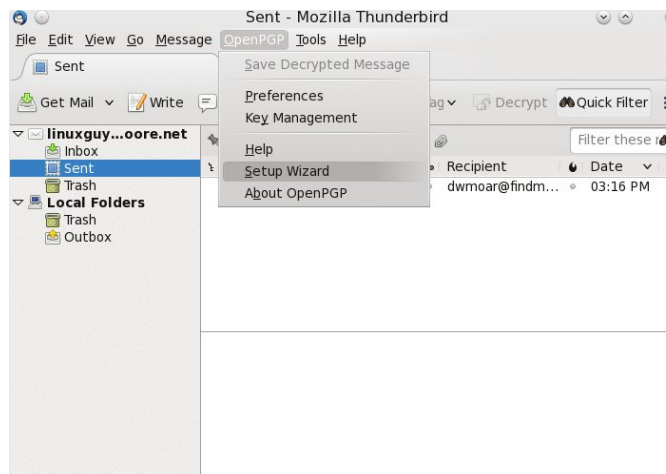
Now we are going to be following most of the prompts.

We will be using the default setting here. Click **NEXT**.

We DO NOT want every email signed, so we want to choose "No". Then click **NEXT**.

On this page we want to allow the setup program to make some needed changes to the Thunderbird preferences, so choose "Yes". I clicked on the "Details" button, to be sure that the "Do not compose HTML messages" box is checked. Click "OK'. The detail window will close. Now click **NEXT**.
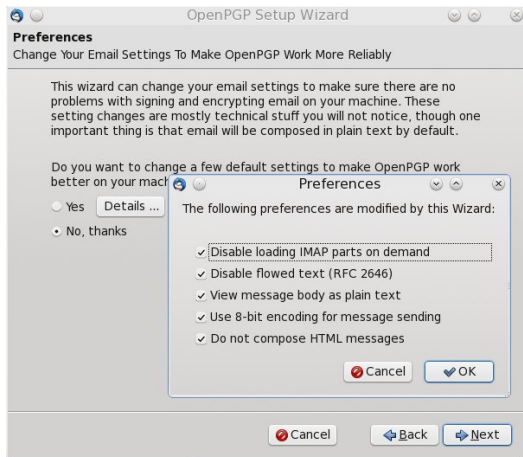
Now we are going to create an OpenPGP key. Make sure the "I want to create a new key pair" line is marked. If you already have a pair of "keys" and would like to use them, then select the second option to import existing keys. When you have made your selection, press **NEXT**.

The first step in creating your key is to set a passphrase. Pick something that you can remember, but can not be easily guessed. When you have entered your passphrase, click **NEXT**.

Now we have a chance to review what we are going to use in the next step. Again, click **NEXT**.

Once the wizard has created your keys, it will popup a window to allow you to generate a revocation certificate. It is suggested that you make this certificate. Click on "Generate Certificate" (center, top).

The file manager will open allowing you to select
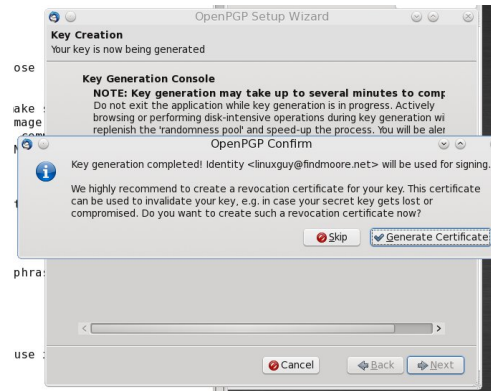
where to save your revocation certificate. When you have selected where to save it, click **save**. A popup will open asking for the passphrase that you chose earlier.
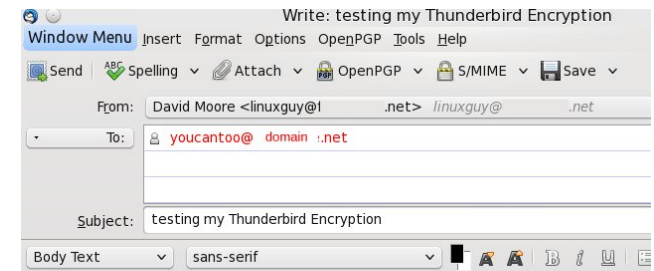
After you have entered your passphrase, click **OK**. The Wizard will close and you will be left at the Thunderbird window.

Now we get to check that everything is working as it should.

Click on the "write" tab to create a new email. From the write dialog window, click on the **OpenPG** tab. Check both the **sign** and **encrypt** boxes.
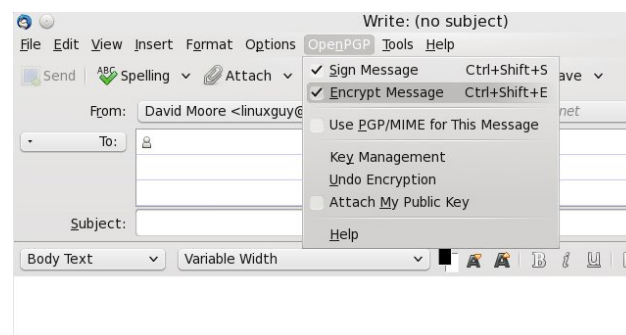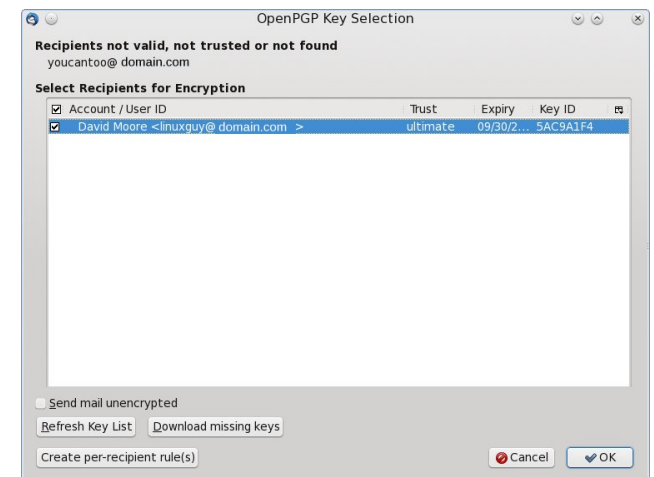
Now go ahead and create your email as normal.

When you have finished creating your email, go ahead and click **send**. You will then be prompted to choose which certificate you want to use. Be sure to select the certificate and then click **OK**.
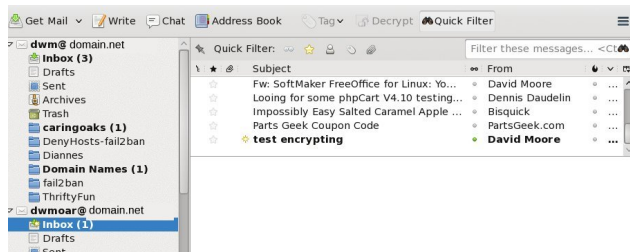
You may be prompted again for your encryption passphrase before sending your email. At this point, you will see your normal text disappear and will then see the encrypted message appear. This part happens *very fast!* (next page, top left)
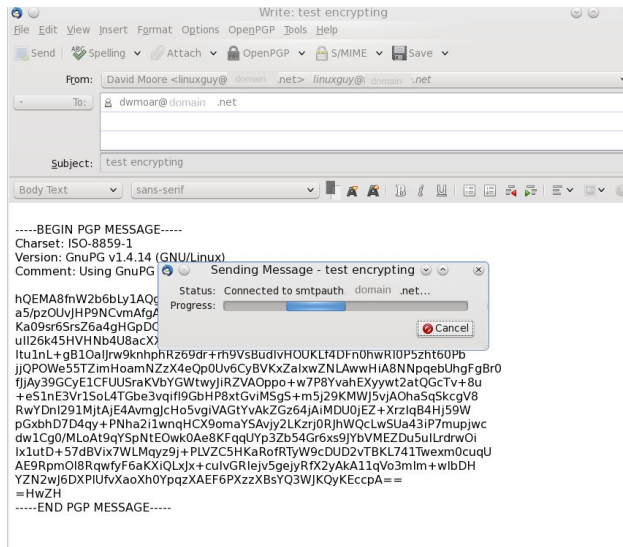
I went and checked the email account that I sent my encrypted message to. Yes, I did receive the message.


and yes, it had indeed been encrypted.

Why is it I can't read it? The reason is above the header of the message "*secret key needed to decrypt message*". It appears that I did not send my public key. I could send the public key in several different ways.

1. send it along with my email
2. export the public key to a file and send it.
3. export it to a keyring server.

In this case, I'm going to send it along with my email. So back I go back to send another email, but this time I will make sure to attach my public key.

Once again I will create a new email. This time when I select the OpenPG tab, I not only select to **sign** and **encrypt** my message, I also selected to **Attach My Public Key** to this email. Clicking send now opens an OpenPGP prompt asking how you want to handle the attachment (your public key). Just choose the default. Then press **OK**.
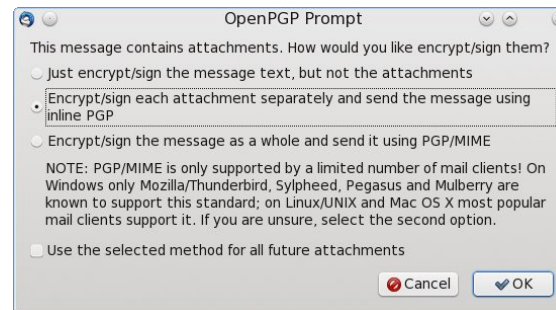
You are then asked for your passphrase. And my email has been sent. Once again I will check my other account to see what I have received. Success….. Thunderbird received and then decrypted the sent email. I have now managed to both send and receive encrypted email.

 Now your little corner of the world is a bit safer from those with prying eyes, thanks to Thunderbird, GnuPG and the Enigmail addon.

You can find more documentation for the Enigmail addon on Enigmail's website.

Support PCLinuxOS! Get Your Official

PCLinuxOS
Merchandise Today!

Mailvelope OpenPGP Encryption For Webmail

by YouCanToo

What is Mailvelope? It is OpenPGP Encryption for Webmail. Mailvelope integrates into the webmail interface. Mailvelope works both with Chrome and Firefox/SeaMonkey. Mailvelope works with the following webmail services.
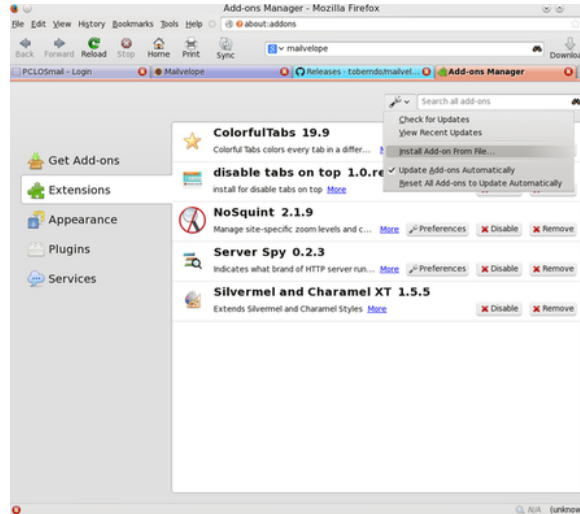
Gmail™
GMX™
Outlook.com™
Yahoo!® Mail

In this article, we will be using Mailvelope with Yahoo!® Mail and Firefox.
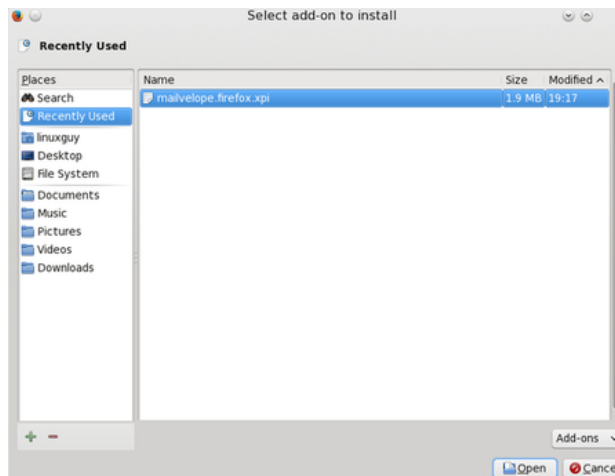
You can get mailvelope from the github website
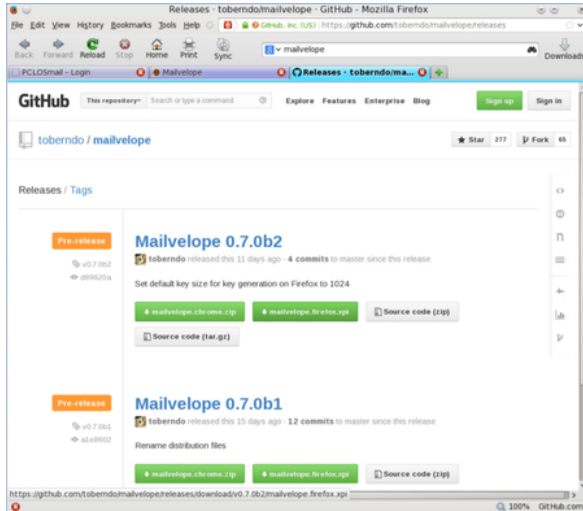
Once downloaded we want to add it to Firefox by going to **Tools > Add-ons**. In the Add-ons window click on the little wrench icon next to the search box. Then select "Install Add-on From File...."
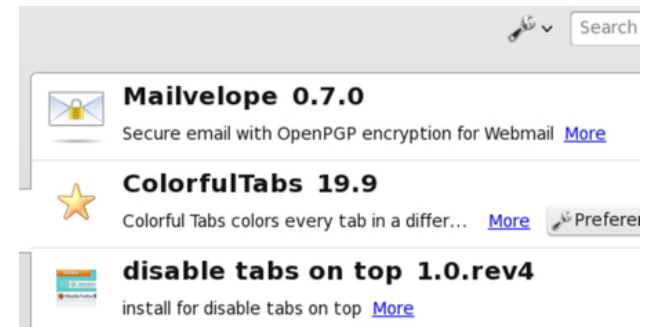

Browse to wherever you downloaded the mailvelope add-on to. Select the mailvelope.firefox.xpi file and then click OPEN.
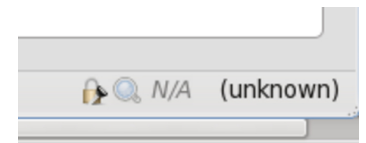

Now we need to install the add-on by clicking Install.
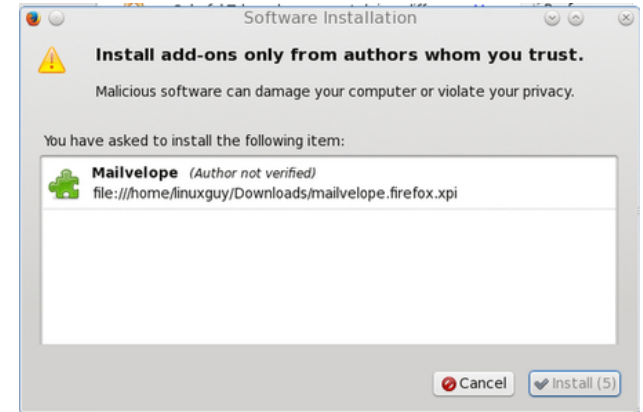
Your Add-on has now been installed.

You can now close the Add-on window. *NOTE*: You DO NOT have to restart Firefox for this extension to work.
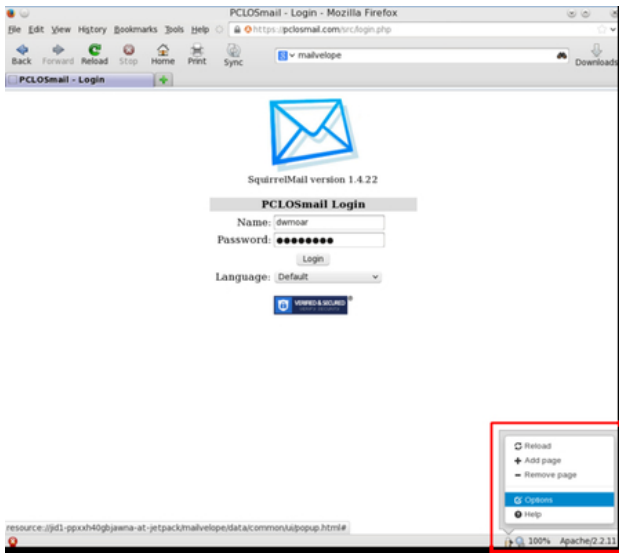
To use mailvelope we need to create a pair of encryption keys. To do this, click on the lock icon at the bottom right of the Firefox screen. Then click on Options (next page, top left).
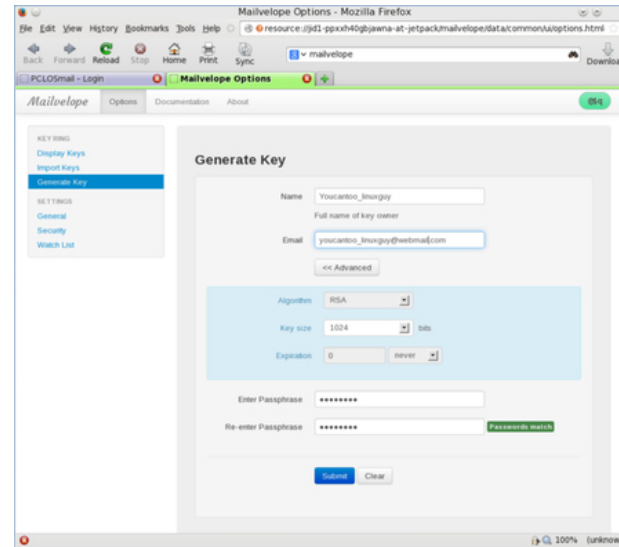
This will open a new tab. Then select "Generate Key"

Fill in the blanks with your information. Remember when choosing a password, use one that is not easily guessed and one that you can easily remember. In the screen shot below, I have clicked

on the advanced tab. You do not need to make any changes under the advanced tab.

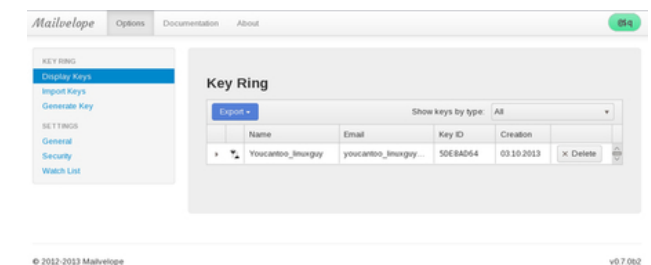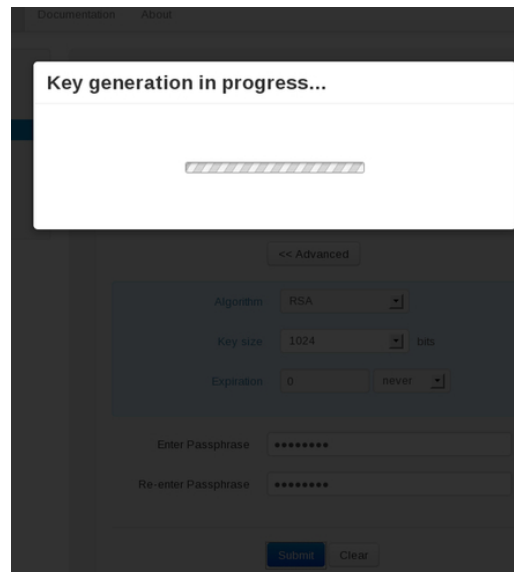If everything is correct, click on the "Submit" button. Your encryption keys are now being generated. Sit back and relax as this can take a few minutes or longer.

If everything went right, you should now see a Success! message.
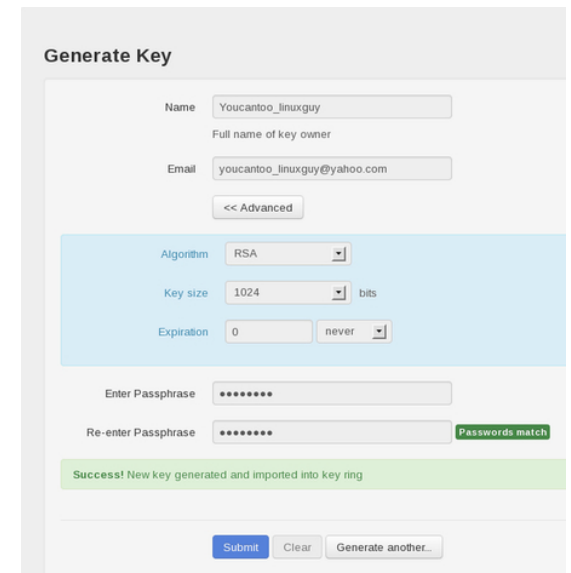
Make sure that you make a backup of your encryption key and put it in a safe spot. Also we need to make a public key. This is the file you give to everyone that you want to send encrypted mail to. To create your public key click on "Display Keys" from the menu on the left hand side of the screen.
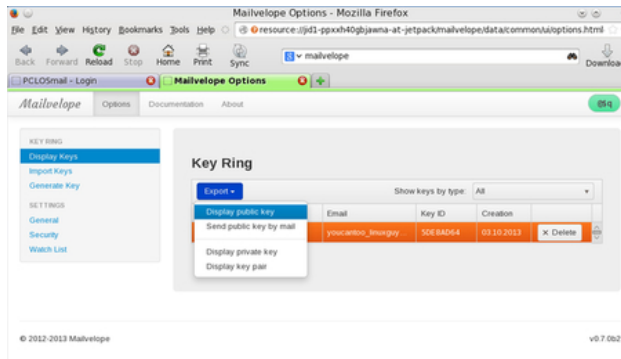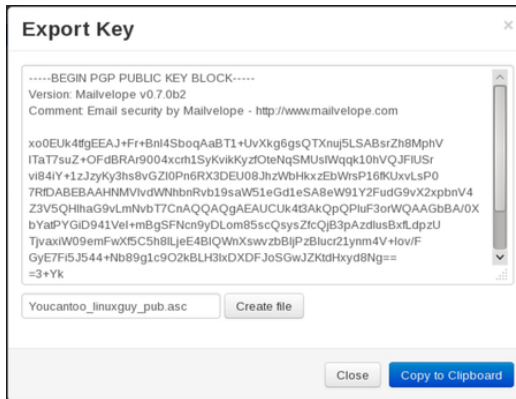

Click on your newly generated encryption to highlight the line and then click on the "Export" button. Then click on "Display public key" (next page, top left).
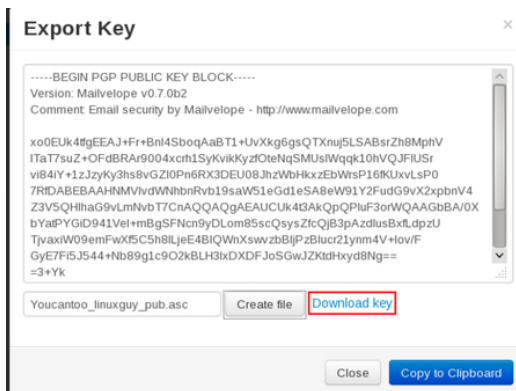
Make sure that you Never NEVER give out your private key. If you do, anyone that has it can read any encrypted mail(s) that you have sent.


To save your public key as a file, click on the "Create file" button.

Then click the "Download Key" link. In the window that opens, be sure to check "Save File" and then click "OK". Be sure that you remember where you downloaded your public key, as you will need it later on.

One last thing, click on the "General" link in the menu to the left and make sure your Primary Private key is being used. If this is blank or is the wrong key then use the drop down arrow and select the correct "Private key". When you selected the right key then press "SAVE".
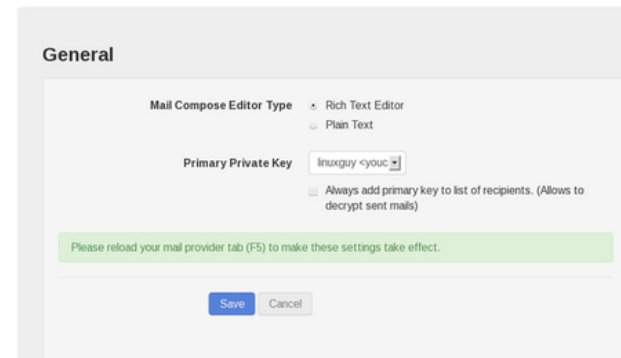
Be sure to refresh (F5 in Firefox) your mail provider's web page.

Now we want to test to see if we can write and send an encrypted email. Since I use Yahoo, I will open my web browser to mail.yahoo.com to log into my account. Once logged into your account click on "Compose". Fill out the "To" and "Subject" fields as you normally would (top, right).

Now click on the little "paper and pencil icon" in the editor window (right, center).

This will open an editor window where we will compose our email to be encrypted (right).

When you have finished composing your email click the little yellow lock in the right corner of the edit window. It will open a small window (next page, top left).
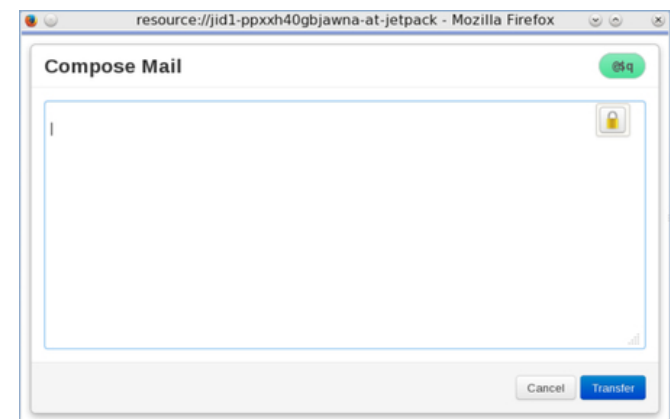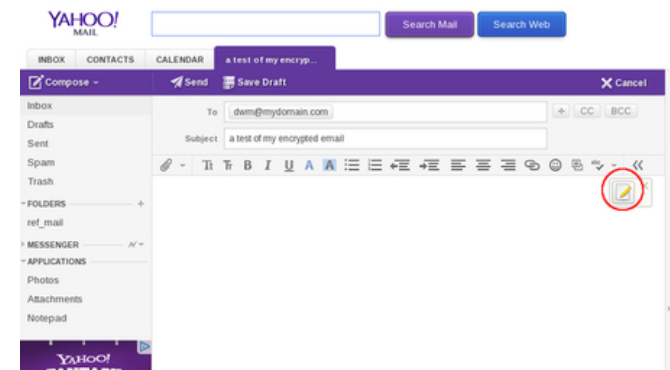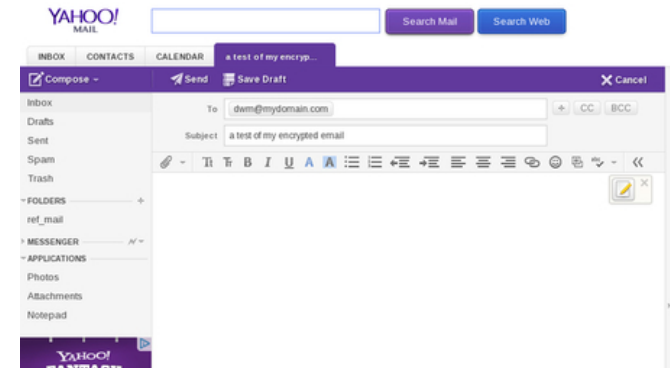
Click "Transfer".   This will now display your encrypted email (next page, bottom left).
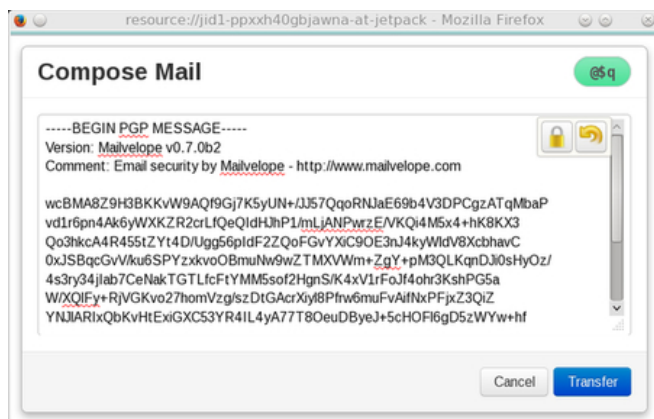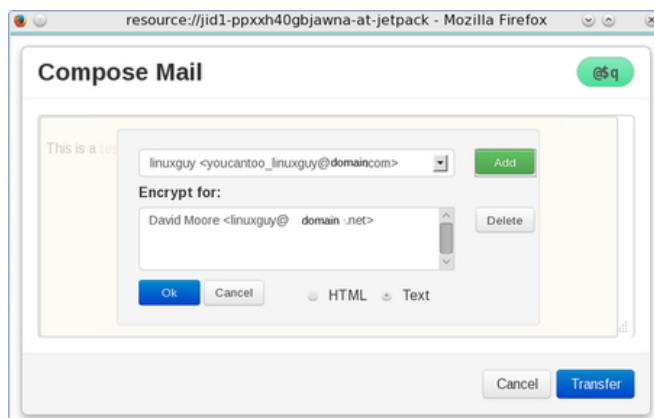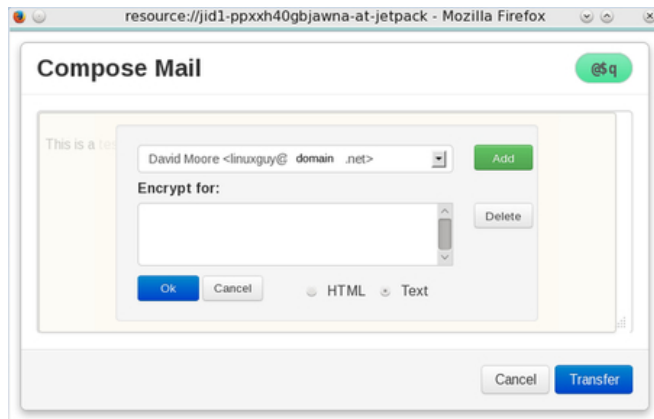
At this point you will be returned back to Yahoo's Compose window and you will see your encrypted message.
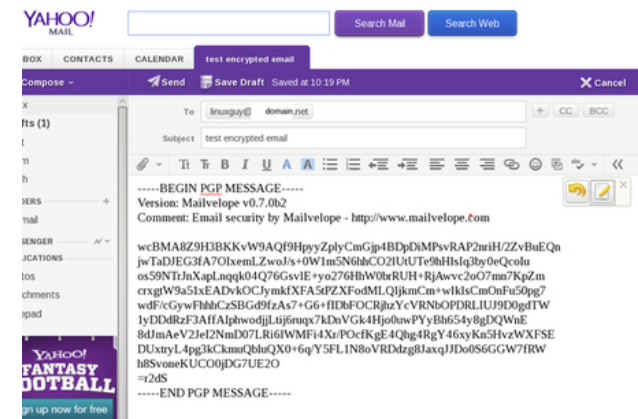
Now click "send" to send your encrypted email.

In my example, I sent the email to one of my test email accounts. I first had to import the public key that we saved earlier into my Thunderbird program. I simply double-clicked on the public key file and told it to open with Kpgp and it imported the key automatically. Kpgp is already installed in PCLinuxOS.

In Thunderbird, I clicked on the "Get Mail" button and lo and behold - I received an email from my Yahoo account.

When I clicked on the new email, I was greeted with a brief flash of the encrypted and then the actual unencrypted email (top, right).

Now I will will try replying to the encrypted email. In this case, I clicked the "Reply" button, filled out my reply and pressed "Send" (center, right).

I watched the program encrypt my reply and send it. The whole process happens very quickly.

Going back to my Yahoo account, I clicked on the
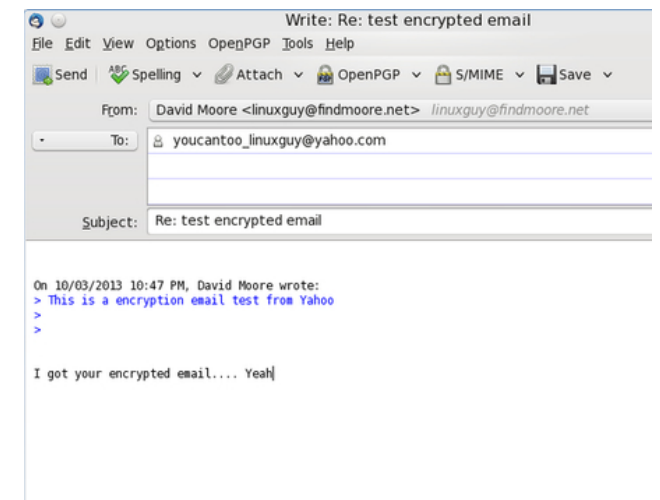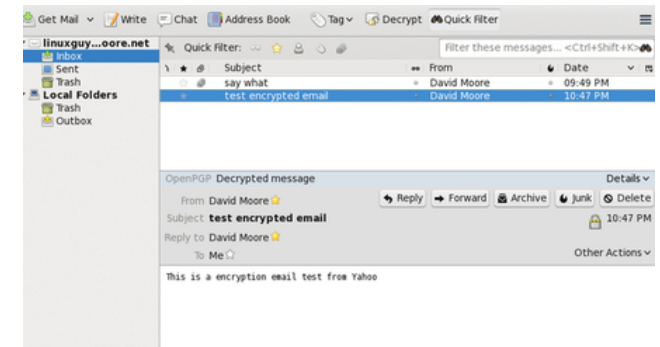
refresh button and low and behold I had an email reply.
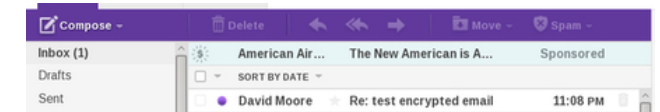
Clicking on the message, I was greeted with an encrypted message (next page, top left).

Moving the mouse pointer in the window and you will notice it appears as a "key". CLick anywhere in the window with the "Lock" icon and a "Key Unlock" will will open asking for your password. Enter your password and press "OK" (next page, left).
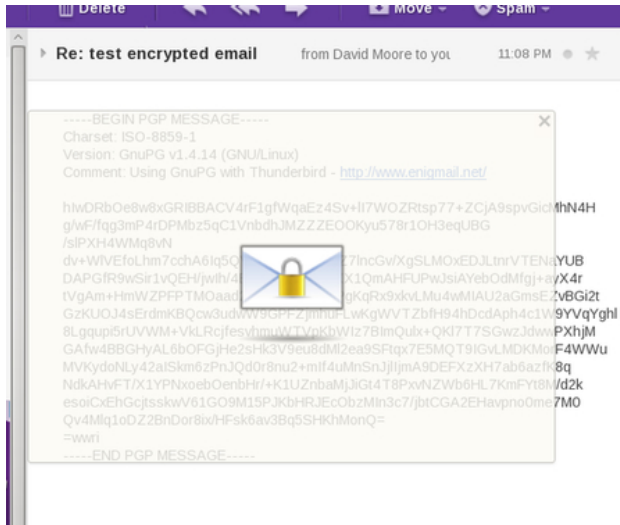
After working for a moment, my message was displayed.
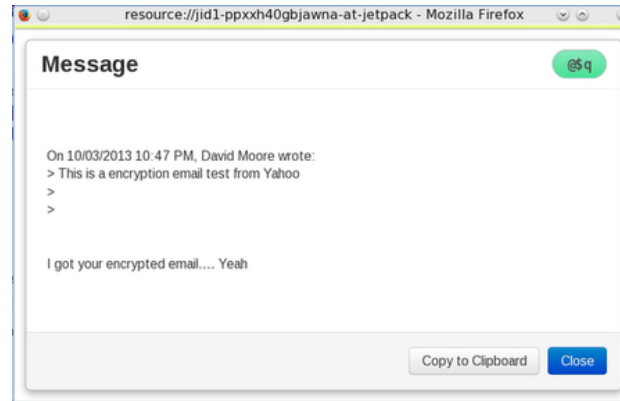
Congratulations, You are now able to send and receive encrypted email from Yahoo!® Mail.
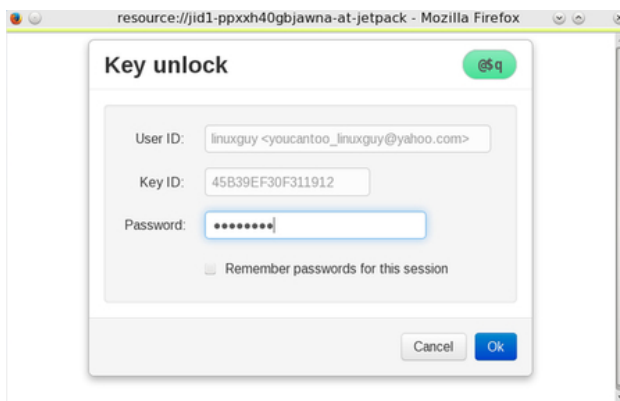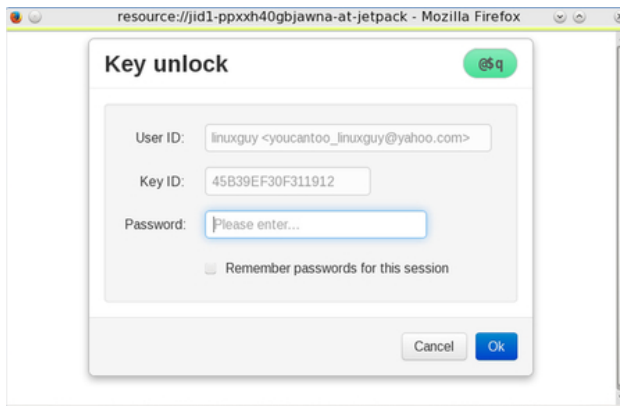
Inkscape: Tree Silhouette in Sunset, Part 2

by Meemaw

Last month we made our tree into a silhouette. We started this project in GIMP, but now we are going to use Inkscape to finish it.

Load your tree into Inkscape. You will always get a window asking if you want to Link or embed the image. With this project it doesn't matter. We are going to do a bitmap trace of the tree. We can use the original image file if we wish, but I also want to experiment. A bitmap trace will enable us to manipulate our drawing easier and do more things with it while keeping the file size smaller. Click on **Path > Trace Bitmap**. The window that opens will have several items from which to choose.

You want to make sure that "Grays" is checked, along with the "Remove Background" checkbox. You can set the number of scans, which will show up as layers in different shades of gray, from 5 to 15. I used 12. Click OK. Inkscape is going to trace over the original drawing we loaded. Depending on your computer hardware, this might take a bit. Just as duplicating an object puts the duplicate on top of the original, Trace bitmap does the same. Click away from your object, and then select it again. Look at the status bar at the bottom. If it says "Group of xx objects" (xx is however many scans you selected), move that to the side. You'll see your tree still there where it was. Click on that one and delete it. Choose your group you moved a minute ago, and click **Object > Ungroup** or just click on the Ungroup button in the upper toolbar. Now move your scans apart so you can see them all.

Using your cursor and drawing a box around them to select them all, change the fill on all of them to black. You might see some that ended up with more detail. Pick the one that looks the best to you. I saw a couple that seemed to have more detail, so I chose one of them. You can move the rest off to the side or delete them. If you just move them off to the side, you can try this tutorial later with another tree.

Place your tree on your drawing where you think it should be located. If you are happy with your work, save your project as a .svg file.
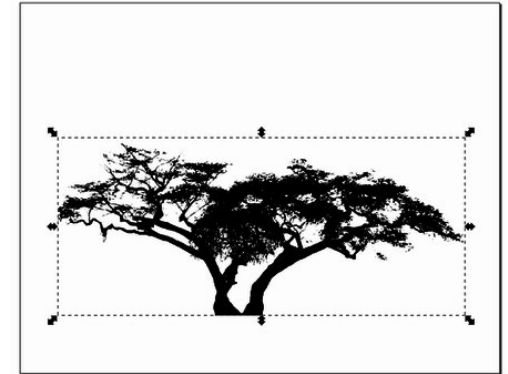
Let's add the ground under the tree. Using the **Bezier Curve and Straight Lines (Pen)** tool, draw the ground however you want it to look. Make sure you click many times and make it the general shape of that you want. With this tool, you should draw a closed curve, even if you have to follow the edges of the page, because you are going to want to fill it with black to match your tree. Don't worry if it doesn't look the way you want it right away - we can remedy that as well. I made my stroke red, so you can see it.
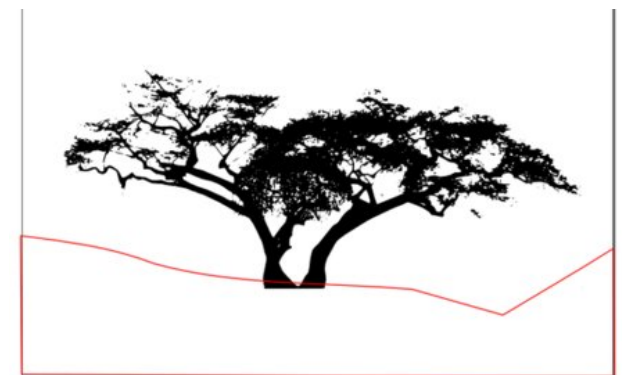
Now we will smooth out our curve. You can click **Path > Simplify**, or use the keystroke for Simplify **<CTRL> + L**, which is much easier. Use this keystroke until your land curve looks relatively smooth.
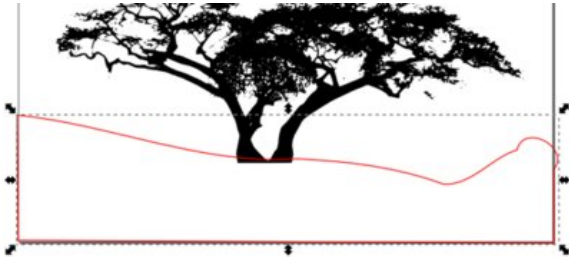
Then click on the Node Editing Tool and finish editing the land. You can pull the nodes or the curves in between until you have it as you want. You can go back and forth between the node tool and the selection tool to see what needs work. Make sure you also square off the corners at the sides and bottom. Add a fill (and I changed my stroke to black as well). When you are satisfied, save your work.

Now we have our tree and ground silhouettes mostly finished. Let's work on our sunset. The first thing you want to do is create a rectangle the same size as your page. Using the **Rectangle / Square Tool**, draw a rectangle. It will be filled with whatever color you used for fill last, and will cover your tree and ground, because all new objects are created on top

of everything else. Edit your rectangle's dimensions so that it is the same size as your page, the using the **Levels** icons above your workspace, send that

rectangle to the bottom of your drawing. You might want to fill it with something besides black so you can see what you're doing. We're going to change it soon anyway.
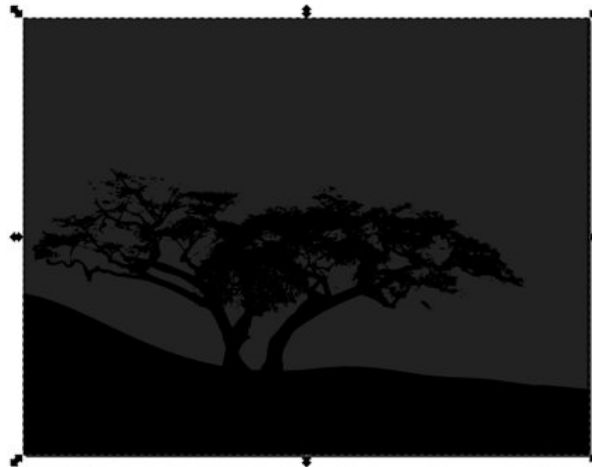
If you don't have the **Fill and Stroke** window open yet, you need it open to set the colors and edit the sunset gradient. Remember the icon in the top row of tools that looks like part of a square with a paintbrush across it. Clicking on it will open the window. If your screen is large enough, you can move your project to the left and put the Fill and Stroke window on the right and see everything you need.

With the Fill tab selected, click on the **Radial Gradient** button. (It's the square at the top that has the round highlight in the center.) When you click on it, your fill will change to a round area in the center of your drawing. In the left side toolbar, pick the **Gradient** tool near the bottom. Now you will see an L-shaped line in your drawing with circles and

diamonds on it. this will allow us to edit this gradient until it looks the way we want. The first thing you want to do is reverse the gradient that's there and add some color. Click on the square in the center and change it to a yellow or gold that reminds you of a sunset. The click on one of the circles at the edge and choose a dark blue or gray. Also, since sunset is usually down on the horizon, you want to move your gradient down lower and lengthen the gradient handles to widen the gradient. You can see what I have now:

While you might think this looks pretty good as it is, we need to add a little more color. Most sunsets have several colors. Double-click on one of the blue gradient lines, and a small diamond should appear in each of the lines. Every time you double-click, another diamond will appear. Each added diamond allows us to add another gradient color. Be careful, though, to double-click over the line in the sky, because double-clicking over your tree or land will create a gradient on one of them. You can create as many as you wish, but I have done only three for now. You can also click on a diamond and move it up or down the gradient line to space them closer together or farther apart.

If your center gradient is a brighter yellow or orange, you want to add a darker colors as you get farther

away from the sunset. Click on the diamond that is closest to the sunset and add a darker yellow or orange.

While I have been adding gradients, I have also moved my gradient around and extended the bottom gradient out so the sunset looks more elliptical than circular. You can also put a gradient right up close to the square in the center and put in a brighter yellow, in case you want your sun to still be up a bit. When you are satisfied, save your work.
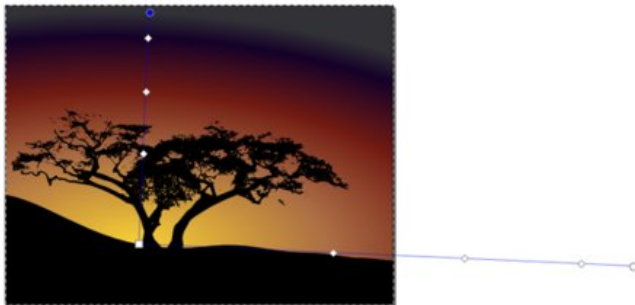
Remember, you can make it as bright or dark as you like - it's your project. So far, mine looks like this:

However, I decided that if the sun hadn't completely set yet, the sky would be a lot brighter. So I removed one of the diamonds and spread the colors out a bit. By the way, the way to remove one of the diamonds is to click on the gradient icon in the Fill & Stroke window, click on **Edit Gradient**, find the one you want to remove in the drop-down list, and choose **Delete Stop**. Now my project looks like this:

We could stop here, but we could also do a couple more things to make our picture look more realistic. The first thing is to put a little gradient on the ground to make a little highlight. Select your ground and choose **Linear Gradient** from the icons. The program will default and show a side-to-side gradient. We are going to edit that. Click on the gradient tool at left, then move your gradient handles so the lighter color is at the top of your ground and the darker color is at the bottom of your picture. Move the handles until you get what you want. Mine looks like this:
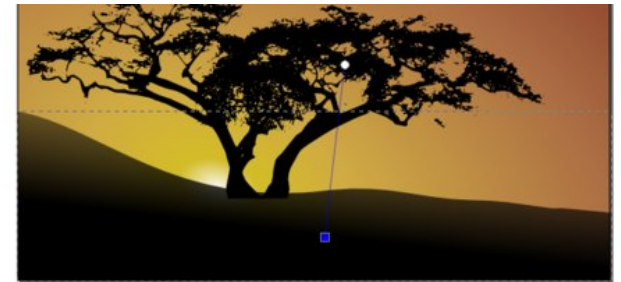
If the sun is going down the tree will cast a shadow, so the last thing I'm going to do is add a shadow. Start by selecting your tree and making a duplicate of it (**<CTRL> + D** or **Edit > Duplicate**). Remember, the program puts the duplicate directly on top of the original. Grab it and move it off to the side. To make the shadow, you need to do a vertical flip on the photo, then stretch it and/or rotate it so it looks the way you think a shadow might look at that time of day. With the sun so low in the sky, your shadow will be rather long, and in the opposite direction from the sunset.
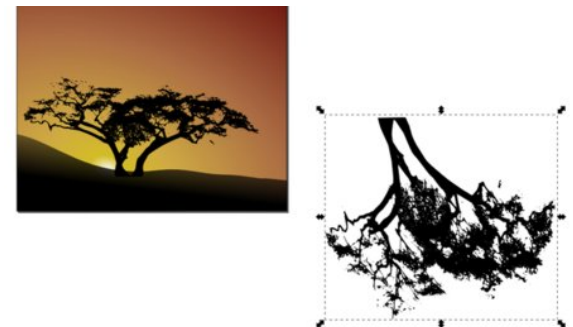
When you get it stretched as you like, place it at the bottom of your original tree, making sure they line up. You may have to zoom in on the tree truck and work on the stretch and rotate a bit.

Before I do anything else, I'm going to blur the shadow a bit, choosing a blur of 2 or 3 from the Stroke & Fill window.
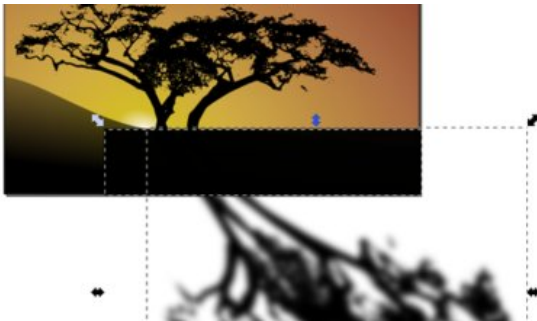
As you see, the shadow extends far out of the picture. I want to get rid of all the excess tree. Choosing the Square & Rectangle tool we drew the background box with, draw a rectangle over the part of the tree you want to keep. Changing to the Selection arrow, select the tree, then holding the shift key down, select the rectangle you just drew.

Now, click on **Object > Clip > Set** and you should have only that part of the shadow that's in your drawing, and the rest should be invisible. Now my drawing looks like this:

Summary

Wow! We've learned quite a few things this time! We have a great tree with the sunset behind it, and we've learned a little bit about bitmap trace and vector drawings. If you made your drawing with the sun farther down, and darker sky at the top, you can also go back in and create a few stars, like we did a couple of months ago for a holiday tree, and scatter them in the darkest part of your sky. When you are satisfied with your work and have saved it, you should also export the drawing to png or jpg.

One great thing about a vector file (svg) is that you can go in and change almost anything in the drawing even after you have saved it. That way you can have different versions of the same design, as long as you don't delete your svg file. Want your gradient brighter or your sunset in a different spot? Change it. Want the land different or the tree smaller? You can change it. Even after you've exported a bitmap of your finished drawing, you can go back and change the svg file again to try something different. Remember, it's your project, and it's finished when <u>you</u> decide it's finished.

PCLinuxOS Recipe Corner

From The Kitchen of YouCanToo
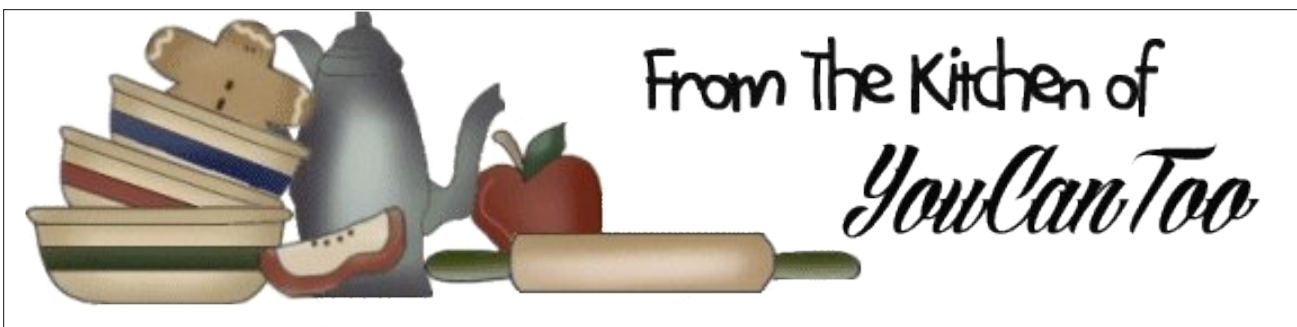
Macaroni and Cheese Ham Pie

Ingredients:

3 cups shredded Cheddar cheese (12 oz)
1 cup cubed cooked ham
1 cup uncooked elbow macaroni (3 1/2 oz)
2 1/4 cups milk
2 eggs
1/2 cup Bisquick® mix
1/4 teaspoon salt
Chopped fresh parsley, if desired

See our recipe for Bisquick type mix here http://recipes.dm-enterprises.net/?p=recipe&recipe=289

Cooking Instructions:

1. Heat oven to 400°F. Spray 10-inch or 9 1/2-inch glass deep-dish pie plate with cooking spray.

2. In large bowl, mix 2 cups of the cheese, the ham and uncooked macaroni. Spread in pie plate.

3. In blender, place milk and eggs. Cover; blend on medium speed until smooth. Add Bisquick mix and salt; blend until smooth. Pour over mixture in pie plate.

4. Bake 35 to 40 minutes or until knife inserted in center comes out clean. Sprinkle with remaining cheese. Bake 1 to 2 minutes longer or until cheese is melted. Sprinkle with parsley. Let stand 10 minutes before serving.

Root Out Root Kits With rkhunter

by Paul Arnote (parnote)

Recent headlines in the news spell out the promotion of computer security and computer spying to the forefront of global consciousness. Edward Snowden. NSA. GCHQ. Google aligning with ALEC. Microsoft intercepting Skype conversations. Microsoft having an "open door" backdoor for the NSA. Canadian spies targeting agricultural interests in Brazil. Chinese hackers stealing defense secrets. There seems to be no end to the spying allegations and revelations in sight.

It became quickly apparent with Avast Antivirus announcing a false positive over the September magazine cover graphic on the magazine's October website (hereafter referred to as the Avast Fiasco), that many users are still concerned about malicious software under Linux. But let's set one thing straight, right up front: *there are no viruses "in the wild" for Linux.* However, this doesn't mean that Linux is immune from malicious software. Linux, as well as every other OS, is still vulnerable to a variety of malicious software known as rootkits. It also illustrates – perfectly – why you should *never* install software from outside the official PCLinuxOS repository.

What is a rootkit? Well, basically, it's a form of malicious software that hides out on your computer that is designed to obtain root level access to a computer. It does this while attempting to hide and prevent detection by antivirus software.

Rootkits can be installed on your computer via a "trojan horse" method, where the software is surreptitiously installed in a "drive-by" fashion. These rootkits can infest your system while browsing nefarious websites, opening suspicious email attachments, or by engaging in password cracking activities.
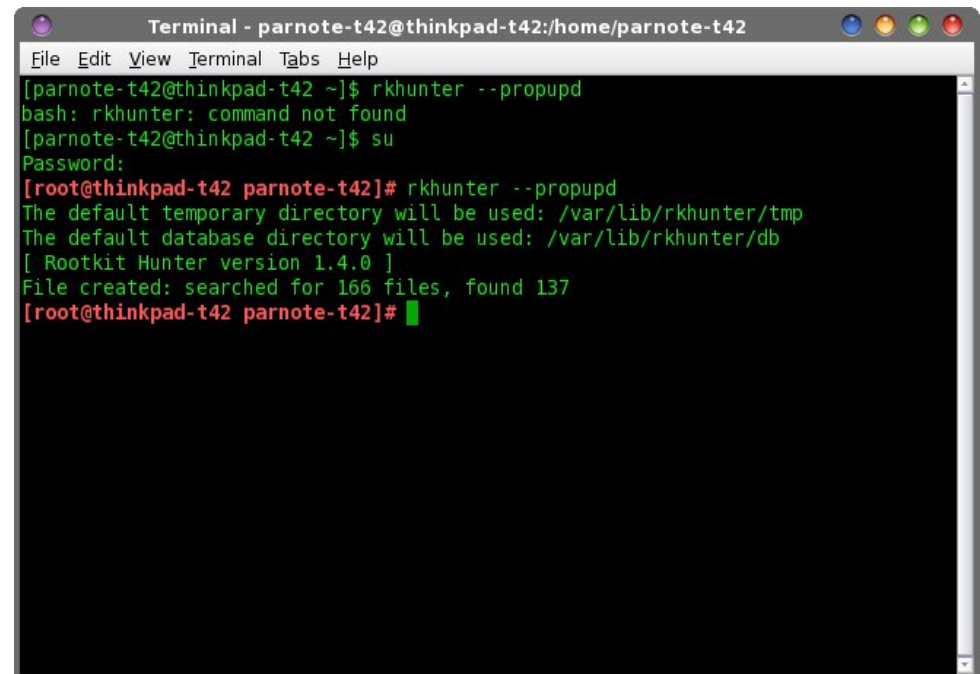
Once installed, they can wreak havoc on a computer. They may stealthily "phone home" with sensitive and private data. Or, they may simply pave the way for other bundled software payloads to steal email contacts, passwords, PIN numbers, credit card information, or conduct activities on your computer that you did not authorize. Today's rootkits don't work so much to elevate privileges to root level access, but instead work mostly to help make the bundled payload software undetectable.

So how do you protect yourself, your computer and your data? The obvious answer is to not surf/browse nefarious websites, open suspicious email attachments, or attempt to crack passwords. Fortunately, the PCLinuxOS repository also includes one of the most popular rootkit detection programs: Root Kit Hunter, also more commonly referred to as **rkhunter.** It is a command line utility that is fairly easy for anyone to run, provided they have root access. It can detect, but not remove, rootkits. More on that later.

To get started with rkhunter, you will need to install it from the PCLinuxOS repository, via Synaptic. Be sure to fully update your system while you've got Synaptic open (it's a very, very bad practice to do selective updates, which *will* lead to you eventually borking your system).

Running rkhunter

Before you get started with rkhunter, you will first need to update its database. First, open a terminal window (any terminal window will work, so choose your favorite). In the above graphic, notice how I first attempted to run rkhunter as a normal user. I was met with a "bash: rkhunter: command not found" error

message. Since you can only run rkhunter as the root user, you will need to **su** to the root user, supplying your root user password when prompted. Once you have root access, enter the following:

rkhunter --propupd

Now, sit back and wait while rkhunter downloads and updates its database.

There are quite a few options you can choose when running rkhunter. Here is a list of them all, with a brief description of what each do:

```
Usage: rkhunter {--check | --unlock | --update | --versioncheck |
            --propupd [{filename | directory | package
            name},...] | --list [{tests | {lang | languages}
            | rootkits | perl | propfiles}] | --config-check
            | --version | --help} [options]


Current options are:
        --append-log            Append to the logfile, do not
                                overwrite
        --bindir <directory>... Use the specified command
                                directories
    -c, --check                 Check the local system
    -C, --config-check          Check the configuration
                                file(s), then exit
        --cs2, --color-set2     Use the second color set for
                                output
        --configfile <file>     Use the specified
                                configuration file
        --cronjob               Run as a cron job
                                (implies -c, --sk and
                                --nocolors options)
        --dbdir <directory>     Use the specified database
                                directory
        --debug                 Debug mode
                                (Do not use unless asked to
                                do so)
        --disable <test>[,<test>...]  Disable specific tests
                                    (Default is to disable
                                     no tests)
        --display-logfile       Display the logfile at the
                                end
        --enable  <test>[,<test>...]  Enable specific tests
                                    (Default is to enable
                                     all tests)
        --hash {MD5 | SHA1 | SHA224 | SHA256 | SHA384 |
            SHA512 | NONE | <command>}  Use the specified
                                         file hash function
                                         (Default is SHA1,
```
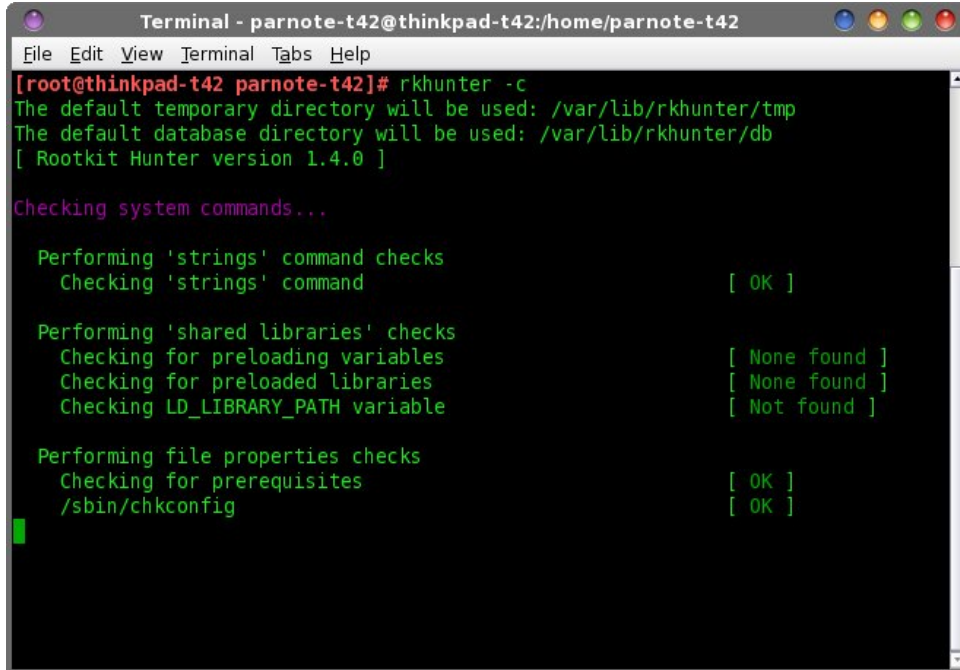
```
                                        then MD5)
    -h, --help                  Display this help menu, then exit
    --lang, --language <language> Specify the language to use
                                    (Default is English)
    --list [tests | languages |   List the available test
                                  names, languages, rootkits
                                  | perl | rootkit names,
                                  perl module status
                                  propfiles] or file
                                  properties database, then
                                  exit
    -l, --logfile [file]        Write to a logfile (Default
                                is /var/log/rkhunter.log)
        --noappend-log          Do not append to the
                                logfile, overwrite it
        --nocf                  Do not use the
                                configuration file entries
                                for disabled tests (only
                                valid with --disable)
        --nocolors              Use black and white output
        --nolog                 Do not write to a logfile
        --nomow, --no-mail-on-warning  Do not send a message
                                        if warnings occur
        --ns, --nosummary       Do not show the summary of
                                check results
        --novl, --no-verbose-logging  No verbose logging
        --pkgmgr {RPM | DPKG | BSD |  Use the specified
                package manager to obtain or SOLARIS |
                NONE}           verify file property values.
                                (Default is NONE)
        --propupd [file | directory | Update the entire file
                properties database, package]...
                    or just for the specified entries
    -q, --quiet    Quiet mode (no output at all)
        --rwo, --report-warnings-only    Show only warning
                                         messages
        --sk, --skip-keypress   Don't wait for a keypress
                                after each test
        --summary               Show the summary of system
                                check results
                                (This is the default)
        --syslog [facility.priority]  Log the check start and
                                      finish times to syslog
                                      (Default level is
                                       authpriv.notice)
        --tmpdir <directory>    Use the specified temporary
                                directory
        --unlock                Unlock (remove) the lock file
        --update                Check for updates to database
                                files
```

```
        --vl, --verbose-logging Use verbose logging (on by
                               default)
  -V, --version       Display the version number, then exit
        --versioncheck  Check for latest version of program
  -x, --autox         Automatically detect if X is in use
  -X, --no-autox      Do not automatically detect if X is
                        in use
```

While the number of options may be overwhelming for some users, we can reduce them down to just those that are more commonly used.

```
Terminal - parnote-t42@thinkpad-t42:/home/parnote-t42
File  Edit  View  Terminal  Tabs  Help

[root@thinkpad-t42 parnote-t42]# rkhunter -c
The default temporary directory will be used: /var/lib/rkhunter/tmp
The default database directory will be used: /var/lib/rkhunter/db
[ Rootkit Hunter version 1.4.0 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                        [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables              [ None found ]
    Checking for preloaded libraries               [ None found ]
    Checking LD_LIBRARY_PATH variable               [ Not found ]


  Performing file properties checks
    Checking for prerequisites                        [ OK ]
    /sbin/chkconfig                                   [ OK ]
```
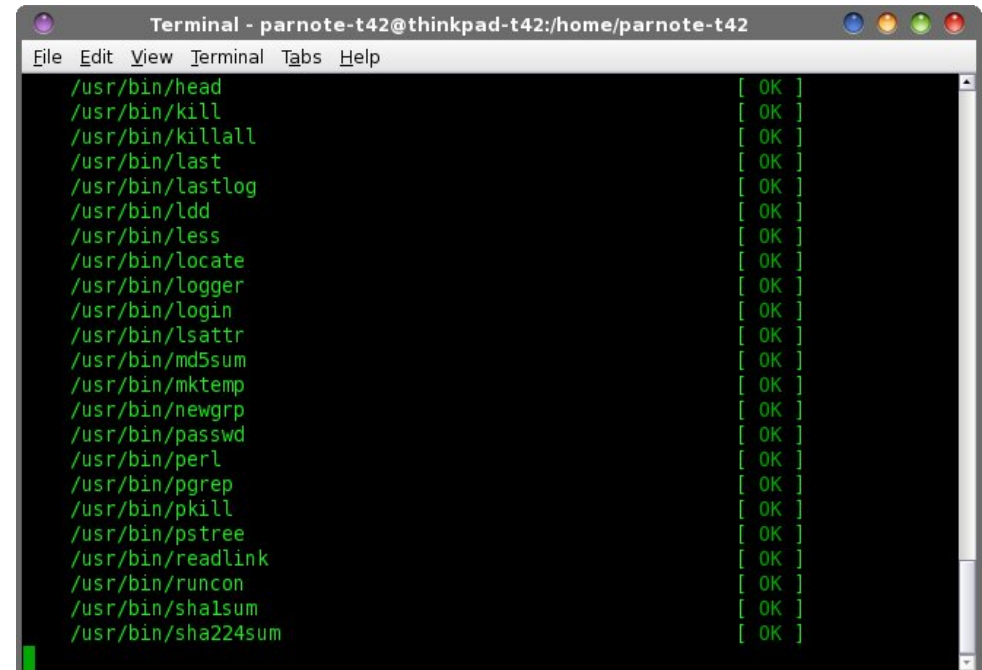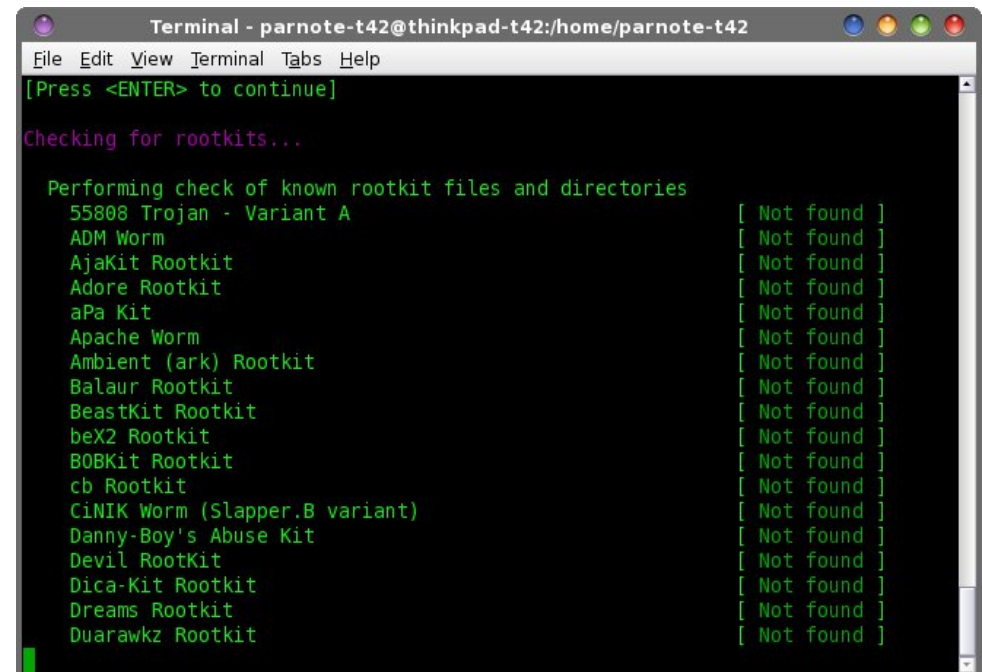
To begin, you will want to simply run rkhunter. Enter **rkhunter -c** on the root command line. Similar to when we performed the initial update to rkhunter, sit back and watch as rkhunter performs its chores. Don't worry … you won't be sitting there long enough for cobwebs to form. The first time I ran rkhunter on my computer, it took just a little over three minutes to complete. But, using the default command line above, it will ask for you to press the Enter key periodically as it performs its various tests. If you prefer it to not wait on your user input, change the command to **rkhunter --sk -c.** The **--sk** command line switch skips the user input (pressing the Enter key), and will allow rkhunter to move straight from one task to the next. However, both commands will still produce the same output in the terminal window.

Below are some random screenshots as rkhunter goes through the process:

```
Terminal - parnote-t42@thinkpad-t42:/home/parnote-t42
File  Edit  View  Terminal  Tabs  Help
/usr/bin/head                                         [ OK ]
/usr/bin/kill                                         [ OK ]
/usr/bin/killall                                      [ OK ]
/usr/bin/last                                         [ OK ]
/usr/bin/lastlog                                      [ OK ]
/usr/bin/ldd                                          [ OK ]
/usr/bin/less                                         [ OK ]
/usr/bin/locate                                       [ OK ]
/usr/bin/logger                                       [ OK ]
/usr/bin/login                                        [ OK ]
/usr/bin/lsattr                                       [ OK ]
/usr/bin/md5sum                                       [ OK ]
/usr/bin/mktemp                                       [ OK ]
/usr/bin/newgrp                                       [ OK ]
/usr/bin/passwd                                       [ OK ]
/usr/bin/perl                                         [ OK ]
/usr/bin/pgrep                                        [ OK ]
/usr/bin/pkill                                        [ OK ]
/usr/bin/pstree                                       [ OK ]
/usr/bin/readlink                                     [ OK ]
/usr/bin/runcon                                       [ OK ]
/usr/bin/sha1sum                                      [ OK ]
/usr/bin/sha224sum                                    [ OK ]
```

```
Terminal - parnote-t42@thinkpad-t42:/home/parnote-t42
File  Edit  View  Terminal  Tabs  Help
[Press <ENTER> to continue]

Checking for rootkits...

  Performing check of known rootkit files and directories
    55808 Trojan - Variant A                        [ Not found ]
    ADM Worm                                        [ Not found ]
    AjaKit Rootkit                                  [ Not found ]
    Adore Rootkit                                   [ Not found ]
    aPa Kit                                         [ Not found ]
    Apache Worm                                     [ Not found ]
    Ambient (ark) Rootkit                           [ Not found ]
    Balaur Rootkit                                  [ Not found ]
    BeastKit Rootkit                                [ Not found ]
    beX2 Rootkit                                    [ Not found ]
    BOBKit Rootkit                                  [ Not found ]
    cb Rootkit                                      [ Not found ]
    CiNIK Worm (Slapper.B variant)                  [ Not found ]
    Danny-Boy's Abuse Kit                           [ Not found ]
    Devil RootKit                                   [ Not found ]
    Dica-Kit Rootkit                                [ Not found ]
    Dreams Rootkit                                  [ Not found ]
    Duarawkz Rootkit                                [ Not found ]
```

```
Terminal - parnote-t42@thinkpad-t42:/home/parnote-t42

File  Edit  View  Terminal  Tabs  Help

[Press <ENTER> to continue]


  Performing additional rootkit checks
    Suckit Rookit additional checks                [ OK ]
    Checking for possible rootkit files and directories    [ None found ]
    Checking for possible rootkit strings          [ None found ]

  Performing malware checks
    Checking running processes for suspicious files   [ Skipped ]
    Checking for login backdoors                   [ None found ]
    Checking for suspicious directories            [ None found ]
    Checking for sniffer log files                 [ None found ]
  Performing trojan specific checks
    Checking for enabled xinetd services           [ None found ]
    Checking for Apache backdoor                   [ Not found ]

  Performing Linux specific checks
    Checking loaded kernel modules                 [ OK ]
    Checking kernel module names                   [ OK ]

[Press <ENTER> to continue]
```

At the end, once rkhunter has run all if its tests, it displays a summary screen:

```
Terminal - parnote-t42@thinkpad-t42:/home/parnote-t42

File  Edit  View  Terminal  Tabs  Help

System checks summary
=====================

File properties checks...
    Files checked: 137
    Suspect files: 0

Rootkit checks...
    Rootkits checked : 315
    Possible rootkits: 0

Applications checks...
    Applications checked: 4
    Suspect applications: 0

The system checks took: 3 minutes and 39 seconds

All results have been written to the log file (/var/log/rkhunter.log)

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

[root@thinkpad-t42 parnote-t42]#
```

Here are the things that rkhunter checks when you run it:

– compare SHA-1 hashes of system binaries against known values in its
    database
– check for known rootkit files and directories
– check for known rootkit strings
– perform malware detection
– check for backdoors, sniffer log files, and other suspicious directories
– perform trojan specific checks, such as examining enabled xinetd services
– check network ports and interfaces
– perform system boot checks
– perform group and account checks
– check system configuration files
– perform file system checks

```
Terminal - parnote-t42@thinkpad-t42:/home/parnote-t42

File  Edit  View  Terminal  Tabs  Help
    Checking for promiscuous in
Checking the local host...

  Performing system boot checks                    [ Found ]
    Checking for local host name files             [ Found ]
    Checking system startup files for malware      [ None found ]

  Performing group and account checks
    Checking for passwd file                       [ None found ]
    Checking for root equivalent (UID 0) accounts  [ None found ]
    Checking for passwordless accounts             [ Warning ]
    Checking for passwd file changes               [ Warning ]
    Checking root account shell history files      [ OK ]

  Performing system configuration file checks
    Checking for SSH configuration file            [ Found ]
    Checking if SSH root access is allowed         [ Allowed ]
    Checking if SSH protocol v1 is allowed         [ Warning ]
    Checking for running syslog daemon             [ Found ]
    Checking for syslog configuration file         [ Found ]
    Checking if syslog remote logging is allowed   [ Not allowed ]


  Performing filesystem checks
```
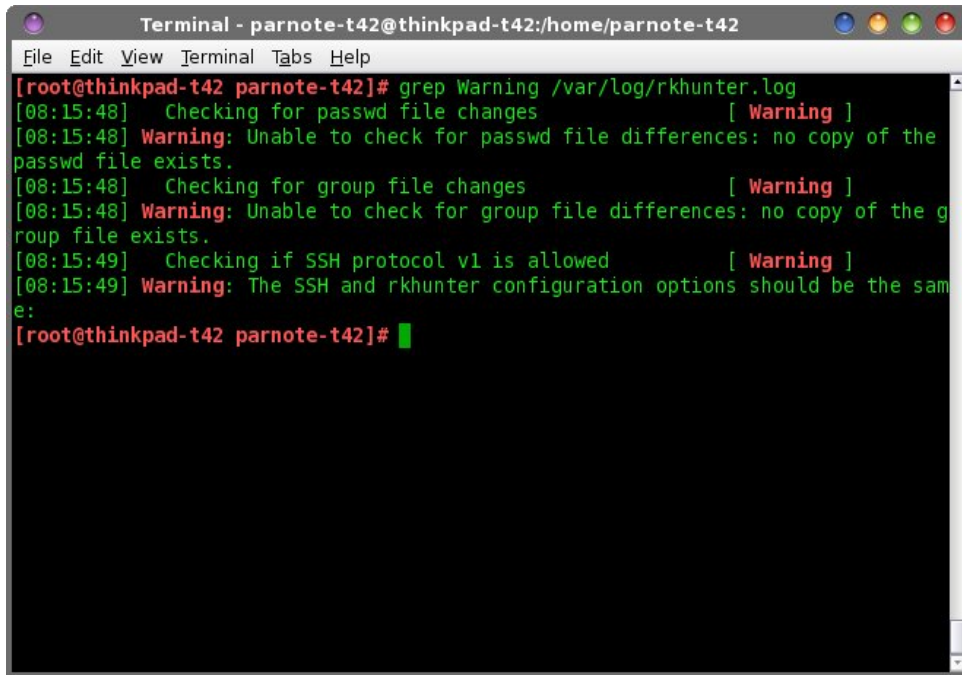
While rkhunter is running, it writes out all of the warnings it finds to the /var/logs/rkhunter.log file. You can easily view those logs from the command line. Still as the root user, enter the following:

grep Warning /var/logs/rkhunter.log

```
Terminal - parnote-t42@thinkpad-t42:/home/parnote-t42
File  Edit  View  Terminal  Tabs  Help
[root@thinkpad-t42 parnote-t42]# grep Warning /var/log/rkhunter.log
[08:15:48]    Checking for passwd file changes                [ Warning ]
[08:15:48] Warning: Unable to check for passwd file differences: no copy of the
passwd file exists.
[08:15:48]    Checking for group file changes                 [ Warning ]
[08:15:48] Warning: Unable to check for group file differences: no copy of the g
roup file exists.
[08:15:49]    Checking if SSH protocol v1 is allowed           [ Warning ]
[08:15:49] Warning: The SSH and rkhunter configuration options should be the sam
e:
[root@thinkpad-t42 parnote-t42]#
```

Every time you run rkhunter, the log file will be overwritten. If you want to keep all of your warnings from every time you run rkhunter, change your command to **rkhunter --append-logs --sk -c** and the new warnings will be appended to the end of the rkhunter.log file.

You should update the rkhunter database periodically. Monthly (or more often) would probably be best. Enter the following command (as the root user) to update the database:

rkhunter --update

You can also set up rkhunter to run on a regular basis, via crontab. Enter the command in crontab (or your favorite crontab GUI program, such as Gnome Schedule or VisualCron) as follows:

rkhunter --cronjob --append-logs

The command above will run as scheduled with crontab, and append any warning information it discovers to the end of the log, stored in /var/logs/rkhunter.log. While you can decide how often to run rkhunter, it would be prudent to run rkhunter at least weekly.

What Are These Warnings?

Keep in mind that rkhunter is merely a rootkit detector. It cannot remove rootkits. Some warnings may occur because you have open ports on your network adapters. On my computers, it usually throws up a warning because of an open SSH port (I use SSH to access files on the various computers around my house). Below is a sample of the warning information from a recent rkhunter session:

```
[12:12:21] Checking if SSH protocol v1 is allowed     [ Warning ]
[12:12:21] Warning: The SSH and rkhunter configuration options
should be the same:
```

Other warning messages may occur because of software upgrades, custom system configurations, or other legitimate system changes. If rkhunter reports a rootkit, you will need to check if it is a false positive. The best thing to do if you get a positive report of a rootkit, or if you get other warning messages, is to re-run rkhunter. Enter the following, as the root user:

rkhunter --propupd (updates database and clears logs)
rkhunter --sk -c

If you still get the warning message, try Googling the specific warning message to see if other folks have received the same warning message. Often times, you'll get your answer. If you still need further assistance, you can sign up for the rkhunter mailing list, and post a question there.

What to do if you have a bonafide rootkit

Fortunately, rootkits under Linux are not a common occurrence, so the chances that you'll need to follow these directions are slim. But if you do, your first step is to immediately take the affected computer offline. Then, backup all of your personal data. Do **not** copy any binary file that you cannot confirm is clean. Remember that rootkits are sneaky little devils, and may masquerade as another file – and often a very innocent looking file.

Unless you are a security expert, attempting to remove a rootkit yourself may not be the best solution. A security expert should be able to diagnose the full mechanism, attack vector, and penetration path of a particular rootkit. Most users do not have this ability.

In this case, your best choice is to reinstall, then move all of your data back onto the computer. Be wary of personal remasters, since the rootkit may have been copied to the personal remaster, as well. It would be best to reinstall from the latest LiveCD version of PCLinuxOS that you prefer. PCLinuxOS users are

spoiled, in a good way, since it only takes 30 minutes (often less) to reinstall the OS. When reinstalling, be sure to format both the / and /home partitions of the drive. This way, you can be more certain that the rootkit isn't hiding out on your hard drive. Sure, it may take some additional time to set everything up the way you like it, as well as reinstalling all of your favorite programs. But in the end, this will be the only way to be certain that you have killed and eliminated the rootkit.

Summary

It's unfortunate that in today's world, we have to be ever vigilant when it comes to computer security. Unlike 15 years ago when the primary concern was malicious hackers releasing a new virus, we must now fear our governments, government agencies, large corporations, in addition to the malicious hackers. The threat level has spread to include groups that we originally – and mistakenly – thought had our security and best interests at heart and in mind. Sad as it is, it seems that we can only trust ourselves. Any user who spends any amount of time online (and who doesn't these days?), we owe it to ourselves to remain vigilant in the protection of our data, identity and reputation.

THE LINUX FOUNDATION

1. Internet

2. Office

3. Games

4. MultiMedia

5. Graphics

6. System

PCLinuxOS *Full Monty...* *Everything you might want or need – plus the kitchen sink!*

Blocking Sites For A More Secure Browsing Experience

by Paul Arnote (parnote)

If you browse the internet (what computer user these days doesn't?), it's a necessity to be vigilant in making your browsing experience secure. Many users don't want their browsing habits to be reported back to online advertisers and other "data mining" sites, like Google, Twitter, Microsoft and Facebook. Most of the time, users are content in just blocking ads from appearing. But given that Facebook has been discovered to be collecting data on all users – not just Facebook members – blocking certain sites is becoming even more and more important to protect our online browsing experience. Let's first take a look at blocking ads.

Everyone and anyone who has browsed the internet has been bombarded with a steady stream of advertisements. Why advertisers continue to subscribe to this intrusive marketing ploy is a mystery. A lot of users feel the same as I do, shunning any advertiser who intrusively thrust their products upon me when I'm trying to be productive doing other tasks.

In my honest opinion, it's a waste of advertising dollars. Sure, it generates revenue for websites (such as the PCLinuxOS website), but it also "turns off" just as many computer users. It's unfathomable that marketing managers would risk alienating and driving away such a large number of potential customers. Browsing the web without some kind of ad blocking software tends to leave me feeling "dirty" and abused.

So, how can a computer user protect themselves from the constant barrage of unwanted and unnecessary advertising? Even more, how can a computer user help protect their data from those companies who ruthlessly mine and collect user data, only to have that information resold to who knows who? Thankfully, there are solutions, and one of them is right under your nose.

Browser Plugins

One of the more common ways to prevent being mauled and molested by unwanted online advertising is to run a browser plugin that blocks the display of ads. Probably one of the most popular ad blocking plugins is Adblock Plus, a.k.a. ABP.

Adblock Plus is available for Firefox, Chrome/Chromium, Opera, Android and Internet Explorer. We've covered Adblock Plus previously in The PCLinuxOS Magazine, as part of a Firefox add-ons article. Setting it up is relatively painless and easy.

Adblock Plus is an open source plugin/add-on, and is the most popular browser extension around. The latter illustrates perfectly how interested internet users are in blocking the annoying and intrusive ads from disrupting their browsing experience.

One advantage of using Adblock Plus is that you can turn it off on websites that you specify. This allows the viewing of ads on a site-by-site basis. The upside of this is that it allows you to help generate ad revenue for sites that you frequent, like the PCLinuxOS website, that rely on that ad revenue to help pay for server space and site administration.

Edit Your /etc/hosts File

The other way to eliminate ads from your browsing experience is to edit your /etc/hosts file to prevent the ads from being displayed. It does this by blocking the server on which the ads reside. Linux, Unix, Windows and OS-X all have a "hosts" file, so this method will work for all of those platforms. Only the details for each individual operating system will differ. We'll focus on how to do this under Linux (of course), and particularly PCLinuxOS.

You could add the server sites, one by one, to the end of your /etc/hosts file. But, that would take a long time, and you're bound to miss a lot of the ad servers. Fortunately, there's someone (Peter Lowe) who has taken the time to not only amass all of these ad servers into one list, but also works tirelessly to maintain that list. You can view or download the entire list from here, on his website. At the time that I wrote this article, there are 2,550 ad servers in the list.

Since the hosts file exists in the /etc directory, you will need root access to edit the file. In a terminal

session, enter the command below that corresponds to your particular desktop environment.

KDE: kdsu kwrite /etc/hosts &
Mate: gksu pluma /etc/hosts &
Xfce: gksu mousepad /etc/hosts &
LXDE: gksu leafpad /etc/hosts &
e17: gksu leafpad /etc/hosts &

The ad server list displayed in Mousepad on Xfce.

After entering the appropriate command in your terminal, hit enter. Supply the root password, and your hosts file should be open and available for editing. **IMPORTANT NOTE:** Before you do anything else, select File > Save As… and save your /etc/hosts file with the file extension of .bak to make a backup copy … just in case something gets messed up, you still have your original hosts file stored, intact. Copy the list above, then move your

cursor to the end of the hosts file, and paste the list.

If there are advertisers you want to allow, place a "# " in front of the line that lists the ad server you want to allow. Let's say, for example, you want to allow ads on the PCLinuxOS site (so that you can help support PCLinuxOS). Look through the list, and if it appears, change the line that reads "127.0.0.1 contextual.media.net" to "# 127.0.0.1 contextual.media.net." (At the time that I wrote this article, contextual.media.net was not in the list). In fact, any line that starts with "# " is treated as a comment and is ignored.

Once you've added "the list" to your hosts file, select File > Save As… and save it as your hosts file (no file extension). You should get a confirmation dialog asking if you want to overwrite your hosts file. Select

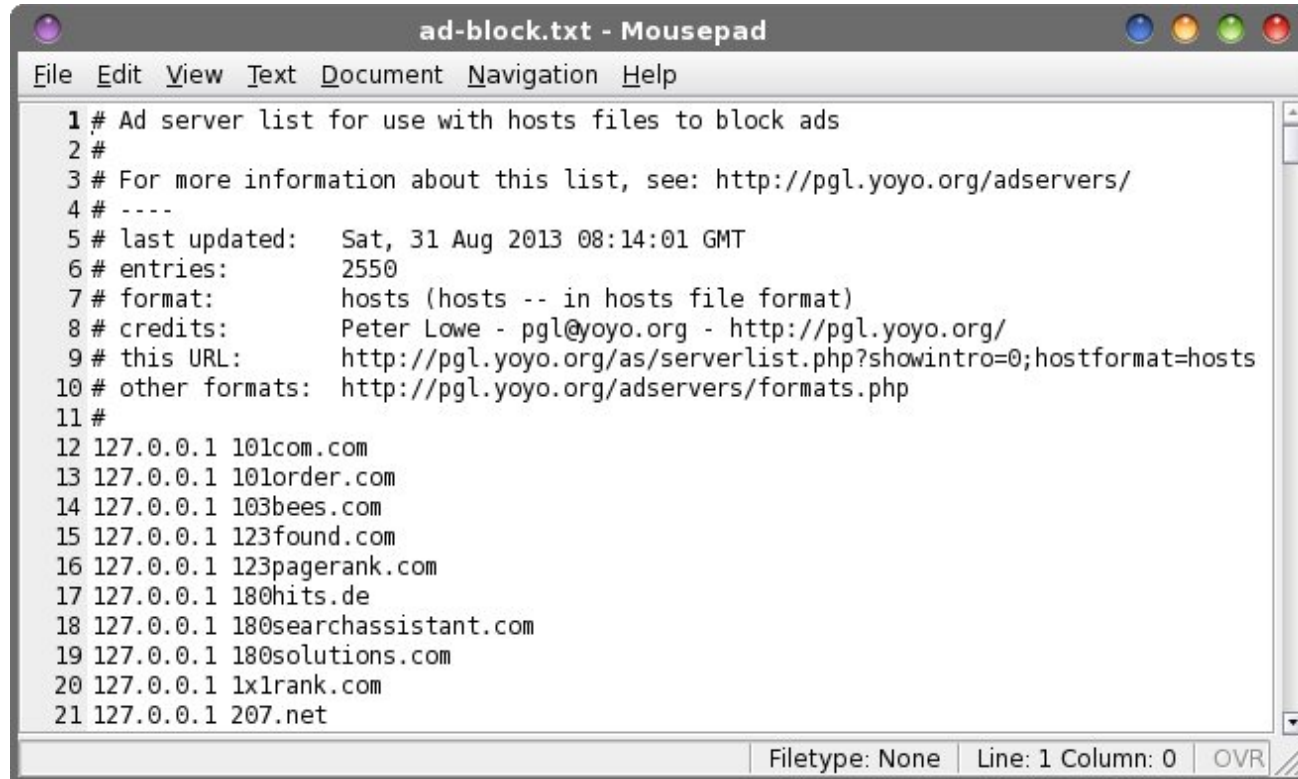to overwrite the original hosts file. Restart your browser.

The benefits of using this method is that it is a universal setting that applies to every user on your computer. The main disadvantage is that you cannot selectively allow ads on some sites but not others, if they originate from the same ad server. Another disadvantage (and an advantage in other aspects) is that you must have root level permissions to add or delete items. Plus, you will also have to make sure that you keep your "block" list updated periodically, as ad servers are added, subtracted and changed. Updating once every three or four months should be sufficient to block most ads.

"Other" Security Concerns

Earlier, we talked about how Facebook (and other sites) amasses and collects data on *all* computer users – not just Facebook members. Recently, the Sandbox section of the PCLinuxOS forum was closed to viewing by guests to the forum. Now, only forum members can see the Sandbox section. Texstar did this after he discovered a Facebook bot crawling over the Sandbox posts, collecting all the data it could. So, whether you have a Facebook account or not, chances are high that Zuckerberg and Co. have collected a LOT of data on you, including your browsing habits, purchasing habits and anything else it thinks it can sell.

Let's explore another scenario. Let's say you have set up a computer for your child in his or her room to help complete school homework. But, being the responsible parent that you are, you don't want your child spending their time on Facebook (let's pick on Facebook here – they are a worthy site to pick on) instead of doing homework.

In either case, you can add Facebook to your "blocked sites" list in your hosts file. Simply add (as root, again) "127.0.0.1 facebook.com" to the end of your hosts file. Now, restart your browser. Try

entering "http://www.facebook.com" into your browser's address bar. Surprise! That computer will no longer be able to connect to Facebook. As an added benefit, Facebook will also not be able to track any of your movements across the web. The latter is an important consideration, especially if you don't have a Facebook account.

You can do this for any site that you a) don't want users visiting, or b) don't want tracking your browsing habits. It's important to use some discretion in what sites you add to the list. For example, Google has become so pervasive that no Google services will be accessible (Google Earth, Picasa, Google +, Gmail, etc.), and sites that you might not think of as having a link to Google may become inaccessible, especially if they use Google's search services to provide a search environment.
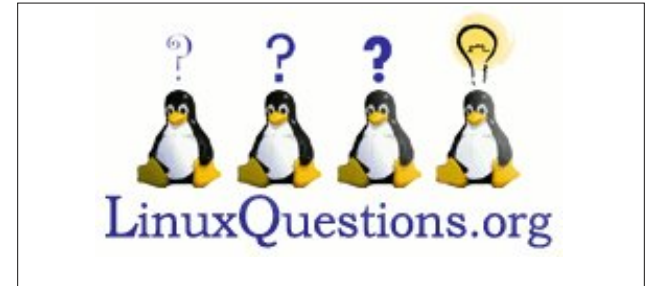
Summary

Users of the web have a few different choices in how to prevent the display of ads, and to help protect their browsing experience. With the current trend of wholesale data collection by nefarious web sites, protecting your data and browsing habits is more important than ever.

Screenshot Showcase

Posted by JohnW_57 on 10/13, running KDE.

# LibreOffice Tips & Tricks: LO Draw

by Meemaw

We have learned many new things in this series. This time we will look at LO Draw. There may be some things you can use to make drawing easier or add a little spark to your creation.

In LO Draw, each page can also be called a slide, just like in LO Impress. The window layout is similar as well, having a page/slide list in the left column and having a workspace with the currently selected slide in the center. You will notice that there are more drawing tools all around your workspace. I'm sure you probably know what most or all of them are, so we won't go into them in any depth. You can always refer to the OpenOffice Draw article I did earlier, since all of the tools are the same. They may not be in the same spot, but you will see them all.

There are some tools that we didn't look at before.

Duplication

Sometimes in your artwork, you create a certain figure, but you find you need several copies, all exactly the same size. Maybe you are creating a cartoon and need callouts, or speech bubbles.
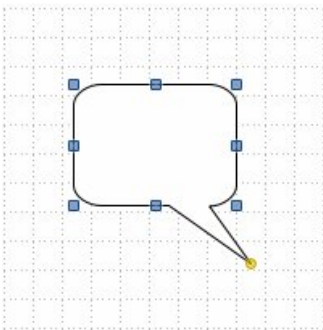
Make sure your shape is the size you desire, then click on **Edit > Duplicate**. A window will pop up asking you how many duplicates you want. You will also be able to designate how they should be spaced out, if necessary.

I finally decided I wanted 5 copies, and left the placement at .20" each, and left everything else the same, although you can make each copy a different size, color and angle.
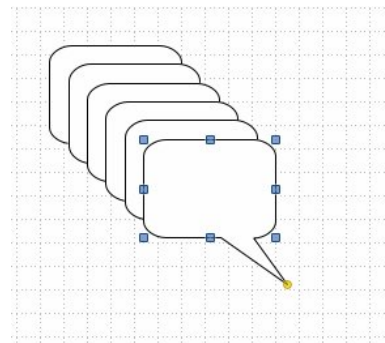
Now you can move these around wherever you want them. They can also be manipulated as usual now, if you have decided you need one bigger, smaller, rotated or flipped.
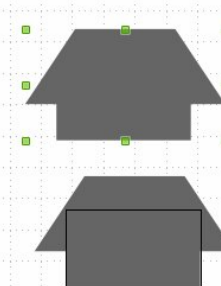
Merge Shapes

Sometimes you want a shape that's more complicated than what is available in the program. For instance, LO Draw can be used as a tool to do a simple floor plan. If you just want to plan your office arrangement, but not build a house, you could use LO Draw rather than SweetHome3D or something similar. But how can you draw the walls and have the shapes stay together if you move the drawing on the page? In the example below, I drew two rectangles, 7" x ¼" and overlapped them at right angles to each other. (I made the borders heavy so they could be seen.)

These can be combined into a single figure by clicking **Modify > Shapes > Merge**.

This figure can now be moved easily. You can merge any number of objects to make your walls, or merge a couple of different shapes to make furniture or something else.

However, if you design an object that needs to remain two different colors, you should *Group* them rather

than *Merge* them. Use **Modify > Group** to be able to move them together easily. I made an image of a computer desk that has a shelf on the lower side for the tower. I wanted both parts to show independently, so I grouped them (see the office plan later in this article). I also made a representation of a swivel chair by placing a circle under one chair and grouping, mainly so the two chairs look different.

Cross-fading

Cross-fading is an interesting effect by which you can "morph" one shape into another. Create two shapes, select them both, then click **Edit > Cross-fading**. You will see a window pop up with three settings: how many steps you want from one shape to the other, whether or not you want the colors (attributes) to cross fade or not, and whether you want the figures to have the same orientation or look twisted.
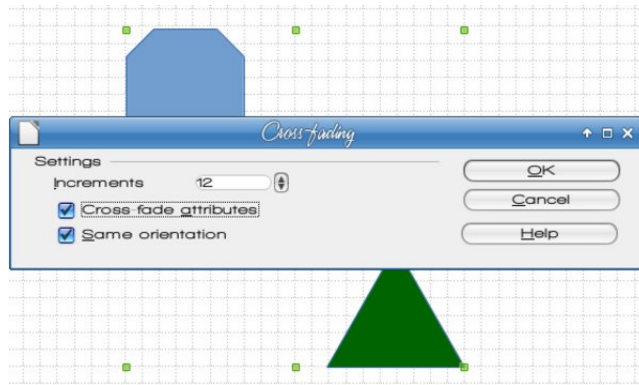
The result of the settings shown is at center top. This results in a group of objects, which can be un-grouped (**Modify > Ungroup**) and can be manipulated one at a time.
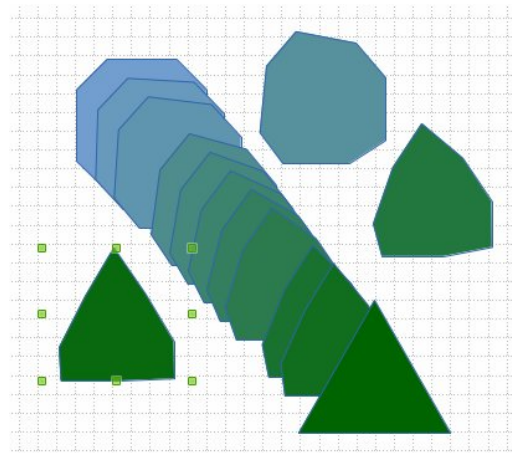

Splitting drawings on multiple layers

Many graphics programs allow you to put objects on more than one layer. LO Draw is no different. This can be very handy if you are working with several objects and want to move them around, but want other objects to stay in one spot. In the case of our room arrangement above, we can put the walls on one layer, then create a new layer for the furniture. In the example below, I have made four walls using the merge command, then filled them with hatching rather than blue. I will then create another layer and switch to it to create the furniture. I have enabled the grid in the background (**View > Grid**) to help me with the scale drawing. My grid has a line every .25 inch (like the old graph paper my math teacher made me use!)

I added a layer named Furniture (top, right). Notice that there are already three layers (they show up as tabs at the bottom of the workspace). The Layout, Controls and Dimension Lines layers are default in the program.

From the LO Help screen, "You cannot delete or rename the default layers. You can add your own layers by **Insert - Layer**.
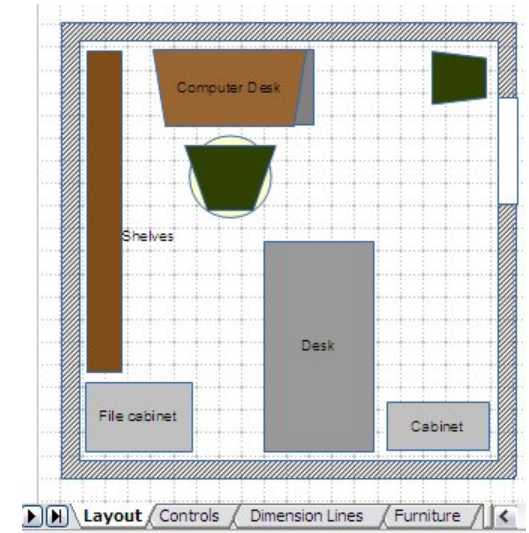
The **Layout** layer is the default workspace. The **Layout** layer determines the location of title, text, and object placeholders on your page.

The **Controls** layer can be used for buttons that have been assigned an action, but that should not be printed. Set the layer's properties to not printable. Objects on the **Controls** layer are always in front of objects on other layers.

The **Dimension Lines** layer is where you draw, for example, the dimension lines. By switching the layer to show or hide, you can easily switch these lines on and off."

You can use those layers or add one or more of your own. I used the Layout layer for my office walls, and added a layer for my furniture. Now I can move furniture around as I desire. To lock a layer, simply right-click on the tab with the layer name and choose **Modify Layer**. You will get a small window with the layer attributes, including a checkbox called "Locked". Simply make sure that box is checked and the layer will be locked. You won't be able to modify or add anything on that layer.

Something else I discovered in my experiments is the ability to add text to any of the figures. Double-clicking inside the gray rectangle, for example, gives you a blinking cursor, and there you can type "Desk" into the center.

3D Text

While we are talking about text, it's fairly easy to create 3D text in LO Draw. Create a text box on your page, and type your text into it. Make sure your spelling is correct because you can't correct the text after it's converted to 3D. Choose the font you desire. When you get it edited as you like, right-click the text box and choose **Convert > To 3D**.
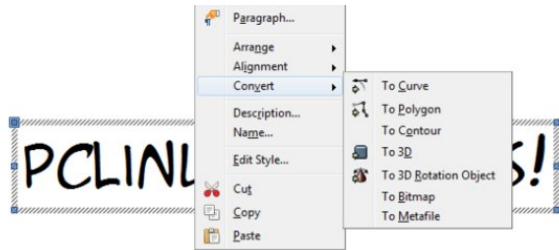
Black text doesn't look real good when converted, so you should probably change the text color if you haven't already. My font is one I downloaded called A.C.M.E. Super Agent.

You can right-click the 3D text and open the 3D Effects window. Play with the settings to get what you want. Also, double-click the text itself for the rotation handles (they are red dots). The corner ones rotate the text, and the other ones change the perspective of the 3D.

We've seen several methods to bring variety to your drawings, and I hope you have learned some new tricks as well.

Visit Us On IRC

• Launch your favorite IRC Chat Client software (xchat, pidgin, kopete, etc.)

• Go to freenode.net

• Type "/join #pclosmag" (without the quotes)

More Screenshot Showcase

Posted by Arctarus5, on 10/7, running Enlightenment.

Posted by agmg, on 10/12, running KDE.

Posted by coffeetime, on 10/20, running Enlightenment.

Posted by Yankee, on 10/2, running LXDE.