The PCLinuxOS magazine

Volume 111

April, 2016

Secure File Deletion: Going, Going, Gone ... You Hope!

Inkscape Tutorial: How To Create Melted Text

Testimonial: I Always Stay Close To PCLinuxOS

Inkscape Tutorial: Easy Patterns Using The Stamping Tool

And more inside ...

In This Issue ...

The PCLinuxOS magazine

The PCLinuxOS name, logo and colors are the trademark of Texstar.

The PCLinuxOS Magazine is a monthly online publication containing PCLinuxOS-related materials. It is published primarily for members of the PCLinuxOS community. The magazine staff is comprised of volunteers from the PCLinuxOS community.

Visit us online at http://www.pclosmag.com

This release was made possible by the following volunteers:

Chief Editor: Paul Arnote (parnote)
Assistant Editor: Meemaw
Artwork: ms_meme, Meemaw
Magazine Layout: Paul Arnote, Meemaw, ms_meme
HTML Layout: YouCanToo

Staff:
ms_meme
Meemaw
Gary L. Ratliff, Sr.
Daniel Meiß-Wilhelm
daiashi
Alessandro Ebersol
loudog
YouCanToo
Pete Kelly
Antonis Komis
Khadis Thok
Smileeb

Contributors:
everstart
mr-roboto

Welcome From The Chief Editor

In my heart, I knew this day was coming. The only question was “when?” I kept hoping that it would continue to be “put off,” as it had been for quite some time. But now, it looks like my beloved 32-bit versions of PCLinuxOS are approaching end-of-life status (EOL), and I am sad.

I have ***always*** ran the 32-bit versions of PCLinuxOS, even on my 64-bit computers. Until now, I couldn’t justify running the 64-bit versions. The 32-bit versions ran perfectly and efficiently, even on my 64-bit computers. Need to access more than 3.2 GiB of memory? No problem! Just use the PAE kernel, which made up to 64 GiB of RAM accessible to the 32-bit version. And up until recently, the 32-bit repository had more packages available, with certain things missing from the 64-bit repository. Plus, the “speed gains” of the 64-bit version over the 32-bit version are negligible. I really don’t have an idea of what I would possibly do with that extra 0.01 seconds I might gain every day by running the 64-bit version over the 32-bit version.

Yes, I have an eclectic mix of older computers, some utilizing the 64-bit architecture, and others utilizing the 32-bit architecture. To keep things simple, it made sense to use only the 32-bit version of PCLinuxOS. It prevented me from having to remember which computer was capable of what, and having to remember the adjustments I might have to make for each.

Now, I have no choice but to “upgrade” (I put that in quotes because the 32-bit version runs so perfectly on all of my computers) to the 64-bit version of PCLinuxOS. If I don’t, I’ll eventually lose access to updates, with software that is forever frozen in time. My back is up against the wall, so to speak.

I won’t be able to “upgrade” any time soon. Yes, I have the 64-bit Live CD ISOs downloaded (my wife’s computer went completely wonky, and a reinstallation will be easier and faster than trying to fix the current xorg issues). But with a remodeling project that MUST be done relatively soon, due to the new baby coming in August, I just don’t have the time currently to sit down and do anything but the periodic updates via Synaptic.

In short, the EOL status of the 32-bit version could not have possibly come at a worse time for me. The three computers in my possession that I use the most are 64-bit. But with every ounce of free time being dedicated to getting my long delayed remodeling project finished (when I had the money, I

Disclaimer

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

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

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

4. No representations, warranties or guarantees whatsoever are made as to the accuracy, adequacy, reliability, completeness, suitability, or applicability of the information to a particular situation. All trademarks are the property of their respective owners.

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

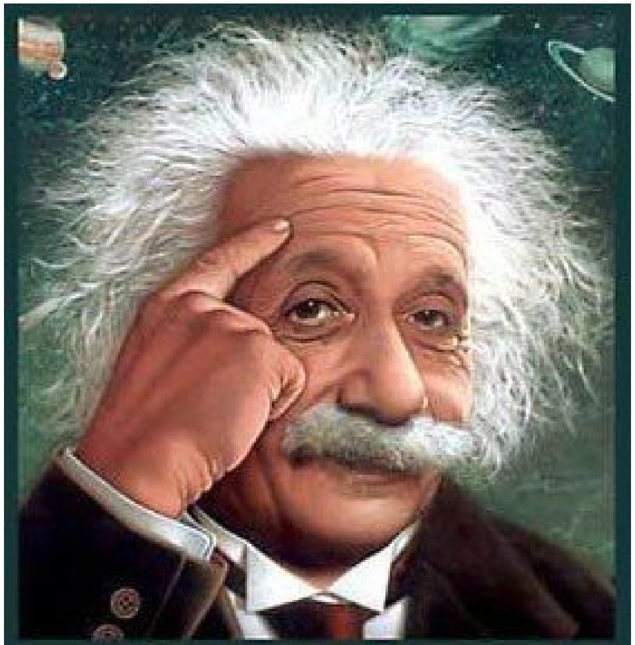
Material Submitted by Users
A majority of sections in the magazine contain materials submitted by users. The PCLinuxOS Magazine accepts no responsibility for the content, accuracy, conformity to applicable laws of such material.

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

didn’t have the time, and when I had the time, I didn’t have the money … a real Catch 22!), coupled with trying to maintain and run this magazine, there isn’t any leftover time in the month to sit down and deal with this “upgrade.” Plus, all of my computers – 32 and 64 bit – purr happily along on the 32-bit version of PCLinuxOS that is currently installed on every single one of my computers.

What I hate the most is the wanton waste of my computers with 32-bit architecture. These are perfectly fine computers, even if they are “old” by modern standards. They purr happily along, performing their tasks reliably. These computers are not yet ready for the trash heap. They have plenty of life still left inside them, and are still useful. Woe is me!

Until next month, and still from the 32-bit version of PCLinuxOS, I bid you peace, happiness, serenity and prosperity.

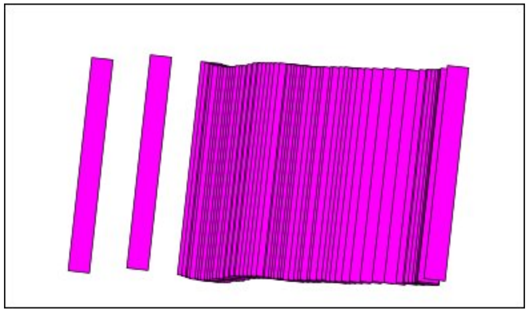


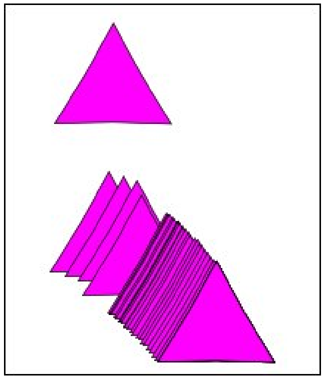
Inkscape Tutorial: Easy Patterns Using The Stamping Tool

by Meemaw

We have created loads of really fun things over the past several years. Sometimes the creation design is something that repeats or something that copies a certain shape. We can duplicate or multiple duplicate to get what we want, but maybe that's too slow. I found this tutorial not too long ago, and it discusses the stamping tool. Let's experiment!

Create a rectangle with a border. To use the stamping tool, click on the rectangle like you are moving it, start dragging your rectangle, then press and hold down the spacebar. As you are moving your object, you will see it multiplying before your eyes. Cool, right?

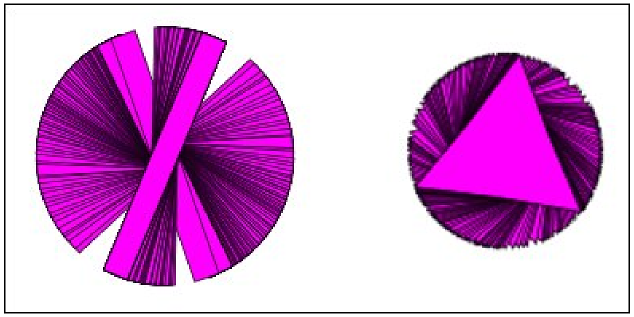




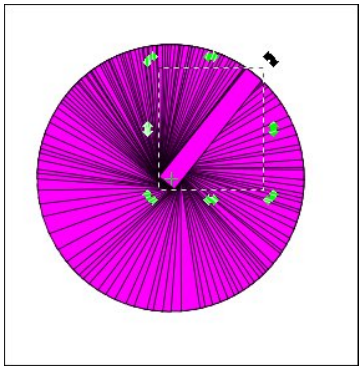
You can do this, naturally, with any object - rectangle, square, triangle, star….

We can expand on this. Remember that when you select your object, and click a second time, the rotate arrows appear, along with a little plus sign on the center of your object. Depending on where the plus sign appears, since it serves as the center of rotation, you can make all sorts of different designs just by changing the center of rotation.

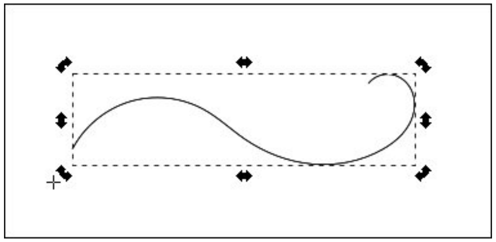
If we leave it in the center, we get the following:



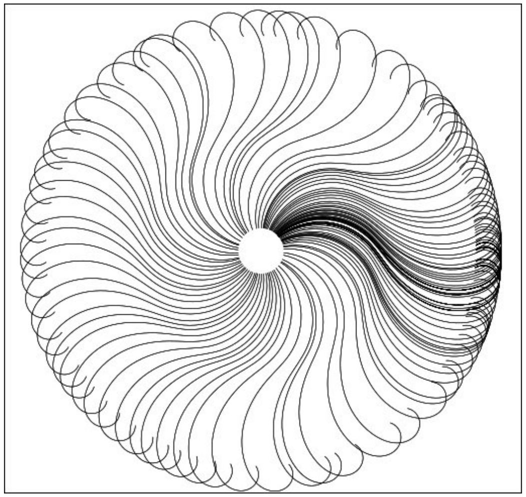
However, using the rectangle, move the plus sign to the end, then grab the other end to rotate it:



Let's try that with a simple curved line. Using the draw tool, draw a line (top, right).

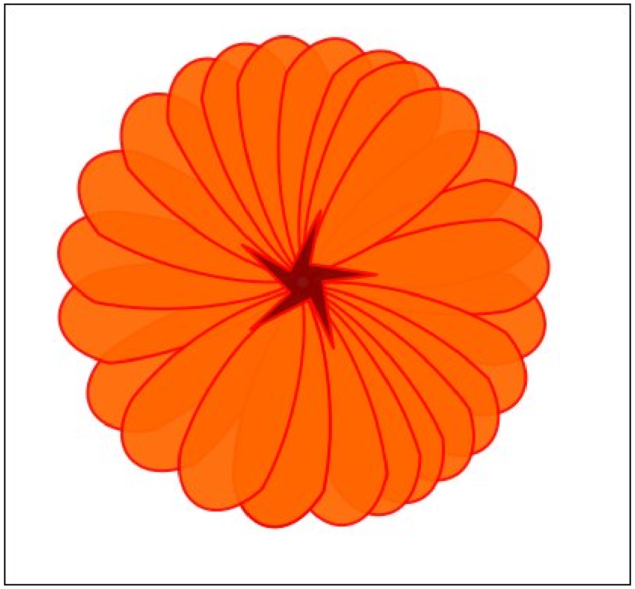


Using the selection tool, move the plus sign to one end (I actually moved it past the line end, as you can see), then grab the other end to rotate it. I used the corner arrow closest to the curly end.



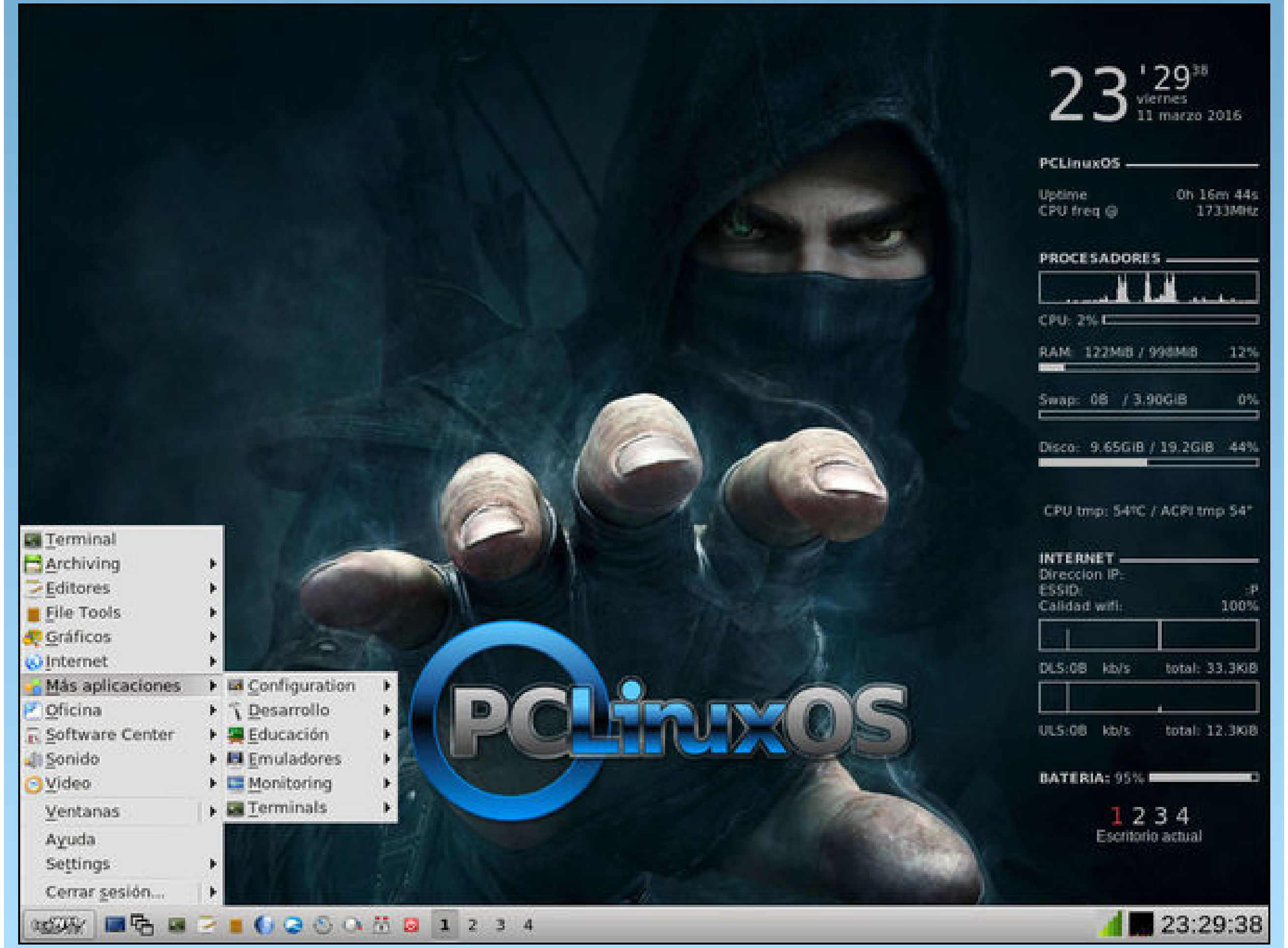
You will have to keep your motion smooth and at a constant speed to make your copies even all the way around the rotation. It takes a bit of practice.

This expands the items we can make and makes our job easier. I made this simple flower (next page, top right) by drawing one petal, then using the stamping tool to duplicate the petals, after which I created the center by itself.



This was a 2 minute creation. I also went back and chose individual flowers to move to make it more even. You could always edit individual flowers so each of them is not identical. With a little practice, I'm sure you can do something spectacular!

Screenshot Showcase



Posted by Aleph, March 11, 2016, running Ice WM.

Game Zone: American Truck Simulator

by daiashi

About The Game

Experience legendary American trucks and deliver various cargoes across sunny California and sandy Nevada. **American Truck Simulator** takes you on a journey through the breathtaking landscapes and widely recognized landmarks around the states.

Game mechanics are based on the highly successful model from Euro Truck Simulator 2 and have been expanded with new features, creating the most captivating game experience from SCS Software.

American Truck Simulator puts you in the seat of a driver for hire entering the local freight market, making you work your way up to become an owner-operator, and go on to create one of the largest transportation companies in the United States.

Features

* Drive highly detailed truck models officially licensed from iconic truck manufacturers.
* Your truck is your new home. Make it yours by changing cabins, chassis, paint jobs, adding tuning accessories or more powerful engines.
* Lots of different cargoes to choose: From food to machinery to hazard cargoes.
* Multiple types of trailers – from reefers to flatbeds, from dumpers to lowboys and goosenecks.
* The longest trailers (up to 53 ft) will challenge your skills and patience while hauling and during parking.
* Deliver your cargoes to a rich variety of companies and locations like refineries, oil storage, gas stations, car factories, or roadworks.
* Various simulation settings for trucking enthusiasts: Air brake simulation; different types of brakes: retarder, Jake brake, trailer brake; multiple types of transmissions straight from real trucks, brake intensity, and more.
* Feel like inside a real cabin: Adjust your seat, mirrors and position your head to get the best view of the road.
* Drive safely, follow the rules and speed limits – police will fine you if you aren't careful!
* Ensure that you are not delivering overweight cargo – you may be checked at the weigh scales.
* Use the route adviser as your personal assistant during the travels.
* Try the life of a truck driver for hire. By delivering the cargoes safely and improving your skills, become the owner of your own, successful company!
* Build your own fleet of trucks, buy garages, hire drivers, manage your company for maximum profits.
* Make your trucking time better by listening to your favorite songs via built-in music player or streaming your favorite radio stations.
* Capture your favorite moments with a photo mode offering rich set of editing options.
* Great support for steering wheels, gamepads and other input devices.
* Long-time support of the game, including new features.
* Obtain challenging Steam achievements and collect all hand-painted Steam trading cards.

System requirements:

Fully updated PCLinuxOS and Steam

Hardware:

Minimum:

OS: PCLinuxOS

Processor: Dual core CPU 2.4 GHz

Memory: 4 GB RAM

Graphics: GeForce GTS 450-class (Intel HD 4000)

Storage: 3 GB available space

Recommended:

OS: PCLinuxOS

Processor: Quad core CPU 3.0 GHz

Memory: 6 GB RAM

Graphics: GeForce GTX 760-class (2 GB)

Storage: 3 GB available space

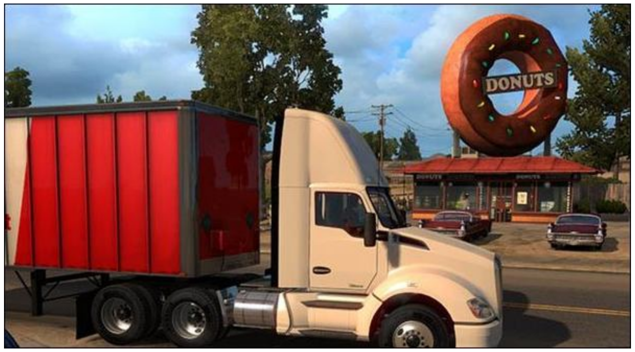
About The Company

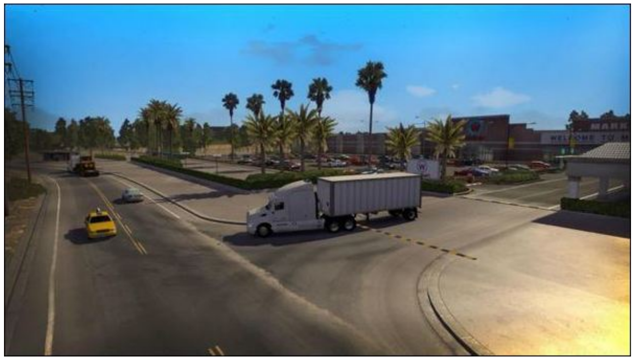
SCS Software is a privately owned game and 3D software development company located in Prague, Czech Republic.

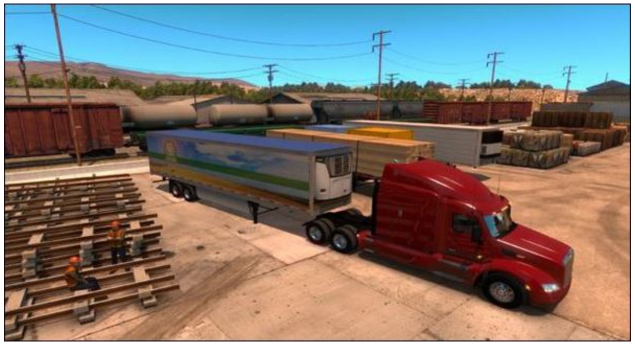
Since its founding in 1997, the company has concentrated on creating licensable 3D engine technology. Their game engines powered over a dozen commercially successful games, including best selling games Deer Hunter II and Deer Hunter III, or the critically acclaimed Duke Nukem: Manhattan Project.

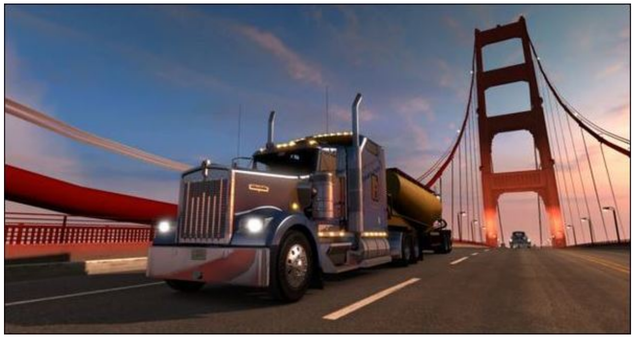
Starting in 1999, they began offering full-scale game development services as a third party developer/contractor. With eight finished games under their belt, they now have a very experienced team capable of building games in a variety of genres. Using their own game engine technology as a base, they can guarantee very competitive prices, state of the art visuals, solid game design and passion and dedication to make your game stand out.

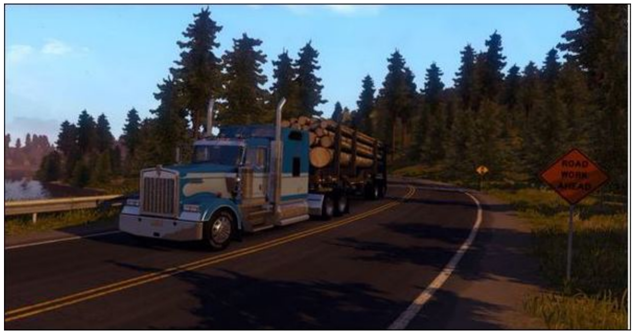
Some Gameplay Screenshots







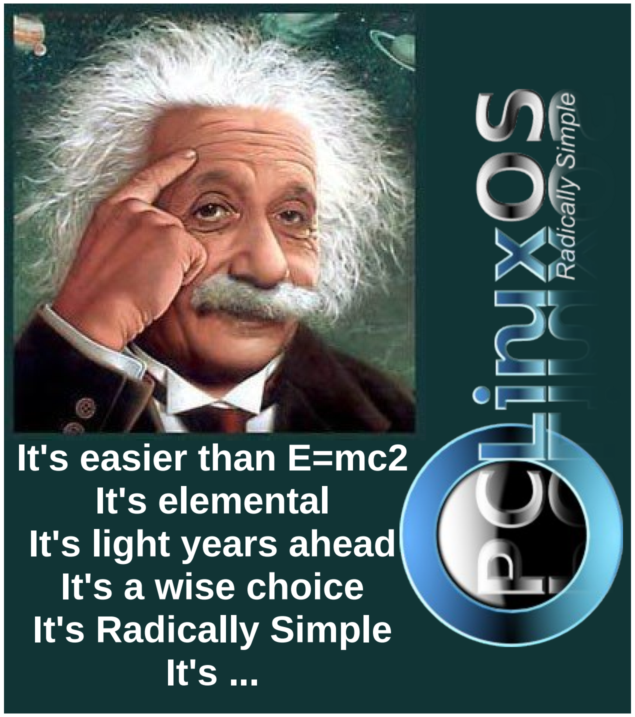




Getting It To Run

Install Steam (if you don't have it installed already), then start it. You will need to create a new account, if you do not already have one. Once you have Steam up and running, go to the store tab. Click on the Linux tab if you wish and search for. Click on and download the demo. If you have updated your system, including graphics drivers, you should be good to go.

American Truck



International Community PCLinuxOS Sites

PCLinuxOS.nl
Netherlands

PCLinuxOS
Daykonun mekanı
Turkey

PC Linux OS
Denmark

Czechoslovakia
PCLinuxOS
síla jednoduchosti

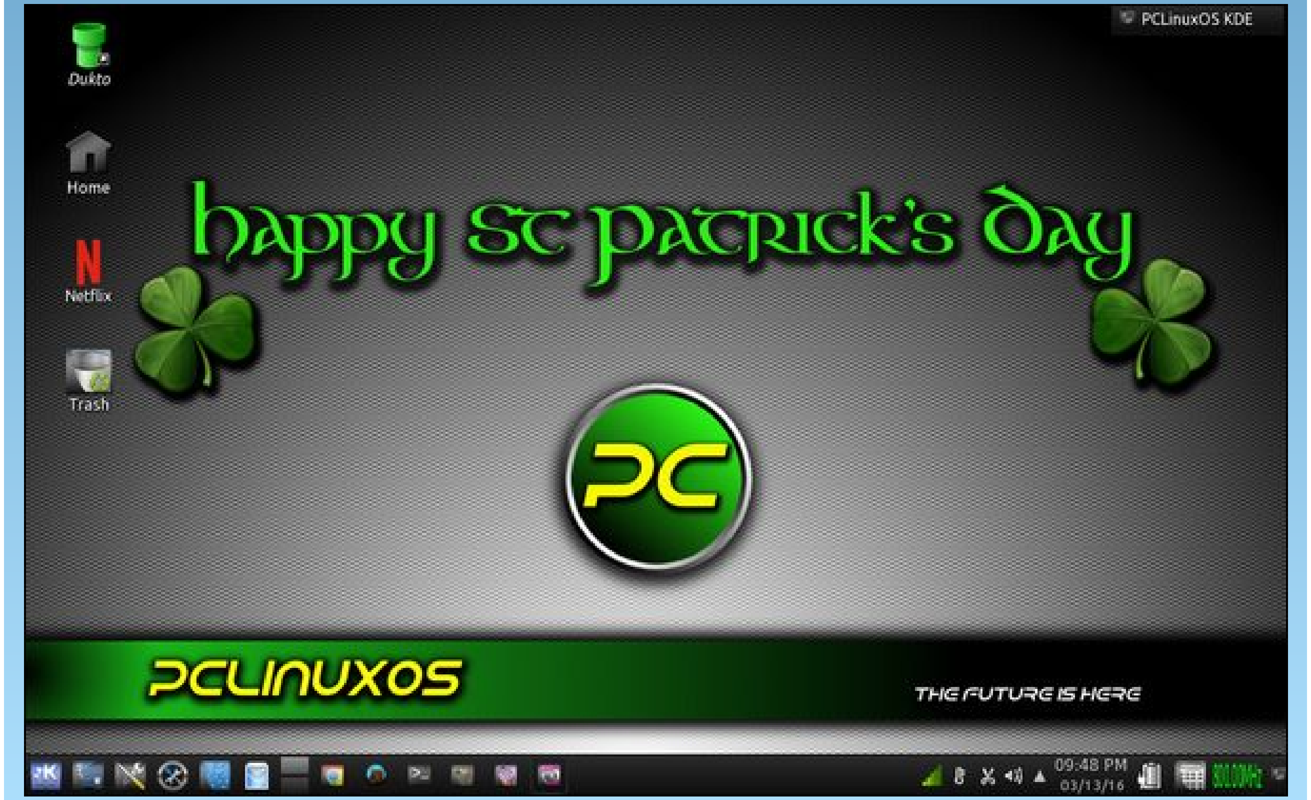
PCLinuxOS.it
Italy

PCLinuxOS
Polskie Centrum
Poland

PCLinuxOS FINLAND

PCLinuxOS
Brazil

Screenshot Showcase



Posted by tuxlink, March 13, 2016, running KDE.

Secure File Deletion: Going, Going, Gone ... You Hope!

by Paul Arnote (parnote)

Last month, we talked about how to recover files that you might have mistakenly deleted. But what if you want to delete a file, and make sure that no one – you and no one else – is able to recover those files? What if you are donating one of your computers to your local computer user group, or if you are selling it/giving it away? Most assuredly, you don't want your private information in the hands of others. You need a way to securely delete those files.

As you might recall from last month's article, I was literally SHOCKED by how many of my "deleted" files were recoverable, in some cases months after I deleted them using normal deletion methods. I thought those files were long gone, never to be seen again. Boy, oh boy, was I ever wrong! The data was rather benign in nature, but should I sell, give away or otherwise dispose of this laptop (or any of my computers), other subsequent "owners" of it don't need to know what I'm up to or what I use my computer(s) for. In short, it is MY data, and they are not entitled to it.

Before I get too far into this, I need to give a shout out to Not_yet_16, Jonesy, Linadian and a few other PCLinuxOS forum users. Their work in helping to spread the word about how to securely delete files and how to securely wipe disks laid the groundwork and basis for this article. I coupled my own research with the message they delivered in the PCLinuxOS forum. You can view Not_yet_16's post on this topic here, Jonesy's post here, and Linadian's post here. There are others, but these are the ones that started me on my journey to write this article.

I also have to admit that as I dug deeper and deeper into this matter, several alternative headlines for this article came to mind. Some of those were "Secure File Deletion: Rotsa Ruck!", "Secure File Deletion: Don't Count On It", "Secure File Deletion: Fuhgeddaboudit", and "Secure File Deletion: Not Easy For Linux Users".

There are a couple of things we also need to keep in mind. First, we need to divide the tools into two categories: secure file deletion, and securely wiping magnetic hard drives. Second, make a backup of your files and data if you're tempted to try these methods. Short of a forensic computer lab with very expensive computers, tools, a knowledgeable technician or operator, and a LOT of time – there will be no way to recover your files or data. At the very least, your data should be safe from the prying eyes of the user level recovery tools we discussed in last month's column. In fact, there is an exceptionally miniscule chance of your data being recovered, especially if you use the tools discussed here for securely wiping your magnetic media.

It might be worth noting, too, that this information ONLY applies to magnetic media, like traditional hard drives. Solid state drives (SSDs) are a whole other animal, and trim (in the PCLinuxOS repository) will – or should – take care of any lingering data. You are using trim with your SSDs, right? Never mind. That's another article for another time.

Also, if you're a user who avoids the command line like forgotten three week old leftovers in the refrigerator, all but two of these utilities – for secure file deletion and for securely wiping drive – are command line only. Even then, installing one of the GUI versions also installs the command line version of the very same utility. To add insult to injury, the GUI version of this tool works imperfectly at times, so always double check to insure the file(s) you wanted to be gone really are gone. The other GUI tool should be already installed on PCLinuxOS users' computers, provided that you installed a full version, as opposed to a "Mini" version. If you are a member of the latter club, this other tool is easily installed, via Synaptic.

If you've been around the command line much, then you probably already know this next bit of wisdom, but I repeat it here for those who don't use the command line much. If the filename and/or path has spaces in it, you will need to place the filename/path in double quotes. Linux uses spaces as delimiters to separate different command line switches and the different parts of the command, so the spaces in filenames/paths will confuse the command line tools. Just be sure to place the entire filename/path in quotes. Alternatively, you can escape the spaces with a backslash ("\"), but it's way easier to just place the filename/path in double quotes – and much more readable. If you avoid using spaces in your filenames and paths (I'm totally anal about avoiding them, since they can cause so many problems), then you avoid this problem entirely. I've even created a short bash script that I can call from a custom action in Thunar that will convert spaces in a filename to dashes. I use it promptly and religiously for files that I've downloaded that contain spaces in the filename.

Historical Foundation

Much of the basis for understanding secure deletion of files and media comes from a 1996 paper by Dr. Peter Gutmann, called “Secure Deletion of Data from Magnetic Media and Solid-State Memory.” His paper was first published in the Sixth USENIX Security Symposium Proceedings, San Jose, California, July 22-25, 1996. It is published under the Creative Commons license. There were some key differences 20 years ago. First, the hard drives in existence were smaller, and they operated a bit differently. Second, journaled file systems were not yet in widespread use, like they are today.

Dr. Gutmann has added three epilogues to his original paper over the years, mostly in an attempt to set the record straight, and to address advances that magnetic storage media has made in the past 20 years.

If you want to know more information about securely deleting magnetic media, I recommend reading over his paper. It’s not as “dry” as you might expect. Plus, if you’re a charter member of the local paranoia club, or if you have a real need (or desire) to prevent sensitive data from falling into the wrong hands, Dr. Gutmann’s paper should be high on your “must read” list. In security circles, it’s almost as if Dr. Gutmann has been elevated to godlike status, with even secure deletion “routines” named after him.

Secure File Deletion

Most of the tools for secure file deletion were written and created before the journaled file systems we use today came about, namely EXT3 and EXT4. In fact, I’m betting that the vast majority of PCLinuxOS users are using the EXT4 file system. Therein lies the problem. The journaled file systems are a tough nut to crack. You may be able to eliminate the actual data, but information about the file(s) may still exist in the file system’s journal entry. That information could include block IDs for the data, aiding a forensic lab in retrieving the information that you’d rather not be retrieved. That data may or may not have been overwritten, and if not, is easily retrieved. It can also go the other way, too, where the journal entry in the file system is deleted, but the data remains intact. In fact, the latter is the most likely case, from what I can decipher about the whole matter.

If you are using EXT3 as your file system, there is a good chance that the secure file deletion utilities will work as described, provided you haven’t changed the “data=something” flag for your drive in your /etc/fstab line (or someone else hasn’t changed it). EXT3 defaults to the “data=ordered” setting, which allows most of the secure file deletion utilities to work as they should. EXT3 will use the default setting if no other setting is specified. The other settings for the data flag are journal and writeback.

If you are using EXT4, Btrfs, ReiserFS (now known as Reiser4), or some other journaled file system, things won’t be as certain. Use of the secure file deletion utilities MAY leave sensitive data on your drive, or stored in the filesystem’s journal. According to Wikipedia’s page about the EXT4 file system, “the ext4 file system does not honor the "secure deletion" file attribute, which is supposed to cause overwriting of files upon deletion. A patch to implement secure deletion was proposed in 2011, but did not solve the problem of sensitive data ending up in the file system journal.” The EXT4 wiki entry about “new features” shows that this feature appears to be stalled and is not currently being worked on – unfortunately.

Still, most secure file deletion utilities work well enough to prevent others with access to and knowledgeable use of user level file recovery tools from gaining access to your data. If you are paranoid about the possibility of others gaining access to your data, then securely wiping the magnetic media will be your best bet, short of physical destruction of the drive.

That doesn’t mean, though, that the secure file deletion utilities are without merit or use. They definitely deserve your consideration. There may be times when you want or need to securely delete only a few files. If it’s just a few files you’re needing to securely delete, wiping the hard drive, then having to reinstall your operating system and the other data you want to keep is just a LOT of work.

With all of the secure file deletion utilities below, I have tested them. The yardstick I used to determine success or failure was if I could see the file(s) with testdisk, which we discussed in last month’s article on how to undelete files, after performing the file deletion with each utility. In every case, none of the file(s) were visible using testdisk after using the secure file deletion utility. If testdisk could no longer see the file, then the secure file deletion was considered to be a success.

While it’s not the most scientific test and is far from perfect, I feel that if the user level file recovery utilities cannot see them, then you have had at least some degree of success. Short of securely wiping the drive contents, I think this is the best we can do, given what we have to work with. Will their use protect you from the prying eyes of a forensic computer lab? Probably not, but it’s better than nothing. The only two things that have any level of success against the probing by a forensic computer lab are securely wiping the drive (probably multiple times, just to be sure), and physical destruction of the drive.

srm

The name srm is short for **S**ecure **R**e**M**ove. Its use is very much like the use of the remove (rm) command. Currently, at the time I wrote this article, srm is NOT in the PCLinuxOS repository. Still, it is easily installed and is a self contained, benign addition to your PCLinuxOS installation. I am mostly including it here because of the rather large number of references to it when you search the internet for information about securely deleting files.

While I have made a package request for the addition of srm to the PCLinuxOS repository, there is no guarantee that it will be added (just as with any package request). If you want to install srm yourself from the source code, it’s relatively easy to do.

First, download the source code, and extract the tar.gz archive file to a folder somewhere in your /home directory. The current version is 1.2.15. Then, as the root user, navigate to the folder where you extracted the tar.gz file, and enter the following commands, one at a time on the command line:

```
./configure
make
make install
```

Your terminal window will whirl and purr at each stage of the installation. When all three commands have been executed, srm will be sitting in the /usr/local/bin directory, ready to use. It really is that simple.

Using srm is fairly straightforward. Executing the command **srm --help** at the command line will give you this:

```
[parnote-toshiba@parnote-toshiba srm-1.2.15]$ srm --help
Usage: srm [OPTION]... [FILE]...
Overwrite and remove (unlink) the files. By default use the 35-
pass Gutmann method to overwrite files.

-d, --directory          ignored (for compatibility with rm(1))
-f, --force              ignore nonexistent files, never prompt
-i, --interactive        prompt before any removal
-x, --one-file-system    do not cross filesystem boundaries
-s, --simple             overwrite with single pass using 0x00
                         (default)
-P, --openbsd            overwrite with three passes like OpenBSD
                         rm
-D, --dod                overwrite with 7 US DoD compliant passes
-E, --doe                overwrite with 3 US DoE compliant passes
-G, --gutmann            overwrite with 35-pass Gutmann method
-C, --rcmp               overwrite with Royal Canadian Mounted
                         Police passes
-r, -R, --recursive      remove the contents of directories
-v, --verbose            explain what is being done
-h, --help               display this help and exit
-V, --version            display version information and exit
```

By default, srm uses the Gutmann method to overwrite data in a series of 35 passes. But, if you want to vary that default setting, then use one of the other methods. Those are known as the simple method, the OpenBSD method, the DoD method, the DoE method, and the RCMP method. Contrary to what the on screen help information says, the simple method is NOT the default setting. Just keep in mind that the more passes a method uses, the slower the file deletion will be. The simple method is the fastest, since it overwrites the data just once with zeros. The Gutmann method is the slowest, since it overwrites the data 35 times.

Minimally, the command for srm looks like this:

```
srm path/to/file
```

Or, if you are already in the directory where the file you want to delete resides:

```
srm filename
```

Of course, it’s nice to have a little feedback from the program about what it’s doing, so something like this will most likely be the best implementation:

```
srm -v -s filename
```

This turns on verbose output and uses the simple method. If you want to securely delete entire directories, their subdirectories, and all the files contained therein, add the -r command line switch. It might look something like this:

```
srm -v -s -r path/to/directory/
```

There is a lot of information about srm out there on the internet, including its man page. Most Linux distributions have it available to install from their repos. But do keep in mind that srm works best with non-journaled file systems (e.g., FAT16, FAT32, exFAT, EXT2, etc.). Dr. Gutmann acknowledges this, and makes the suggestion to use the simple method of file deletion with srm, rather than any of the other methods.

Is it perfect? Nope. Does it work? Mostly. It’s certainly far better than just using the standard rm command. Does it securely delete your files? Maybe. Maybe not. Will your files still be recoverable in a forensic computer lab? Most likely, since there’s no guarantee that the file contents are obfuscated or overwritten on a journaled file system.

wipe

This is another utility that isn't in the PCLinuxOS repository – and probably for good reason. The wipe program hasn't been updated since 2009, and is most likely being abandoned. I include it here because there are numerous references to it when you seek information on the internet about securely deleting files on Linux.

Just as with srm, wipe is reported to not work well with journaled file systems. Also, just like with srm, you can download the source code and compile it yourself. The steps are the same as for downloading and compiling the srm source code. So, instead of repeating all of that again here, refer to the earlier directions when we were talking about srm. It is also a self-contained and benign program, just like srm.

Once you have it installed, enter wipe -h at the command line. You should see this information in your terminal session:

```
[parnote-toshiba@parnote-toshiba Test]$ wipe -h
Wipe v2.3.1 - released November 1st, 2009
by Tom Vier <nester@users.sf.net>

Usage is wipe [options] [file-list]

Options:                Default: wipe -ZdNTVEAkO -S512 -C4096 -l1 -x1
-p1

-h               --   help - display this screen
-u               --   usage
-c               --   show copyright and license
-w               --   show warranty information
-i  and  -I       --   enable (-i) or disable (-I) interaction -
                      overrides force
-f               --   force file wiping and override interaction
-r  and  -R      --   recursion - traverse subdirectories
-s               --   silent - disable percentage and error
                      reporting
-v               --   force verbose - always show percentage
-V               --   verbose - show percentage if file is >= 25K
-e  and  -E      --   enhance (-e) percentage accuracy or faster
                      writes (-E)
-d  and  -D      --   delete (-d) or keep (-D) after wiping
-n  and  -N      --   delete (-n) or skip (-N) special files
-k  and  -K      --   lock (-k) or don't lock (-K) files
-z               --   zero-out file - single pass of zeroes
-Z               --   perform normal wipe passes
-t  and  -T      --   enable (-t) or disable (-T) static passes
-a  and  -A      --   write until out of space (-a) or don't (-A)
-o[size] -O      --   write to stdout (-o) or use files (-O)
-B(count)        --   block device sector count
-S(size)         --   block device sector size - default 512 bytes
                      or stdout write length when used with -A
-C(size)         --   chunk size - maximum file buffer size in
                      kilobytes (2^10)
-l[0-2]          --   sets wipe secure level
-x[1-32] -X      --   sets number of random passes per wipe or
                      disables
-p(1-32)         --   wipe file x number of times
-b(0-255)        --   overwrite file with this value byte
```

When you look at the command line switches, it's hard to not notice that a lot of them are the same as with srm – so much so, that wipe looks like srm on steroids with all the extra options.

The command for wipe will most likely look like this:

```
wipe filename
```

If you want to change up any of the default values (see at the beginning of the list of command line parameters in the help listing above), your command might look like this:

```
wipe -v -z -p 7 filename
```

Just as with srm, add the -r command line switch to recurse directories and delete all subdirectories, along with the files in them.

Your results using wipe will be similar to the results using srm. Definitely no guarantees, but it's better than the standard rm command, and definitely better than nothing.

shred and shred_GUI

Shred and shred_GUI are in the PCLinuxOS repository. You will only find shred_GUI listed, as the command line version is installed along with the GUI version. So, if you're looking to install just the command line tool, you will have to install the GUI version just to get the command line version.

Here's what Synaptic says about Shred_GUI:

shred_GUI - overwrite a file to hide its contents, and optionally delete it

Simple GUI for shred.

Overwrite the specified FILE(s) repeatedly, in order to make it harder for even very expensive hardware probing to recover the data.

Delete FILE(s) if --remove (-u) is specified. The default is not to remove the files because it is common to operate on device files like /dev/hda, and those files usually should not be removed. When operating on regular files, most people use the --remove option.

CAUTION: Note that shred relies on a very important assumption: that the file system overwrites data in place. This is the traditional way to do things, but many modern file system designs do not satisfy this assumption. The following are examples of file systems on which shred is not effective, or is not guaranteed to be effective in all file system modes:

* log-structured or journaled file systems, such as those supplied with AIX and Solaris (and JFS, ReiserFS, XFS, Ext3, etc.)

* file systems that write redundant data and carry on even if some writes fail, such as RAID-based file systems

* file systems that make snapshots, such as Network Appliance's NFS server

* file systems that cache in temporary locations, such as NFS version 3 clients

* compressed file systems

In the case of ext3 file systems, the above disclaimer applies (and shred is thus of limited effectiveness) only in data=journal mode, which journals file data in addition to just metadata. In both the data=ordered (default) and data=writeback modes, shred works as usual. Ext3 journaling modes can be changed by adding the data=something option to the mount options for a particular file system in the /etc/fstab file, as documented in the mount man page (man mount).

In addition, file system backups and remote mirrors may contain copies of the file that cannot be removed, and that will allow a shredded file to be recovered later.

Let's take a look at the help text for the shred command line utility.

```
[parnote-toshiba@parnote-toshiba ~]$ shred --help
Usage: shred [OPTION]... FILE...
Overwrite the specified FILE(s) repeatedly, in order to make it
harder for even very expensive hardware probing to recover the
data.

If FILE is -, shred standard output.

Mandatory arguments to long options are mandatory for short
options too.

  -f, --force          change permissions to allow writing if
                       necessary
  -n, --iterations=N   overwrite N times instead of the default (3)
      --random-source=FILE  get random bytes from FILE
  -s, --size=N         shred this many bytes (suffixes like K, M, G
                       accepted)
  -u, --remove[=HOW]   truncate and remove file after overwriting;
                       See below
  -v, --verbose        show progress
  -x, --exact          do not round file sizes up to the next full
                       block; this is the default for non-regular
                       files
  -z, --zero           add a final overwrite with zeros to hide
                       shredding
      --help           display this help and exit
      --version        output version information and exit

Delete FILE(s) if --remove (-u) is specified. The default is not
to remove the files because it is common to operate on device
files like /dev/hda, and those files usually should not be removed.
The optional HOW parameter indicates how to remove a directory
entry:
'unlink' => use a standard unlink call.
'wipe' => also first obfuscate bytes in the name.
'wipesync' => also sync each obfuscated byte to disk.
The default mode is 'wipesync', but note it can be expensive.

CAUTION: Note that shred relies on a very important assumption:
that the file system overwrites data in place. This is the
traditional way to do things, but many modern file system designs
do not satisfy this assumption. The following are examples of file
systems on which shred is not effective, or is not guaranteed to be
effective in all file system modes:

* log-structured or journaled file systems, such as those supplied
with AIX and Solaris (and JFS, ReiserFS, XFS, Ext3, etc.)

* file systems that write redundant data and carry on even if some
writes fail, such as RAID-based file systems
```

```
* file systems that make snapshots, such as Network Appliance's
NFS server

* file systems that cache in temporary locations, such as NFS
version 3 clients

* compressed file systems

In the case of ext3 file systems, the above disclaimer applies
(and shred is thus of limited effectiveness) only in data=journal
mode, which journals file data in addition to just metadata. In
both the data=ordered (default) and data=writeback modes, shred
works as usual. Ext3 journaling modes can be changed by adding the
data=something option to the mount options for a particular file
system in the /etc/fstab file, as documented in the mount man page
(man mount).

In addition, file system backups and remote mirrors may contain
copies of the file that cannot be removed, and that will allow a
shredded file to be recovered later.

GNU coreutils online help:
<http://www.gnu.org/software/coreutils/>
Full documentation at:
<http://www.gnu.org/software/coreutils/shred>
or available locally via: info '(coreutils) shred invocation'
```

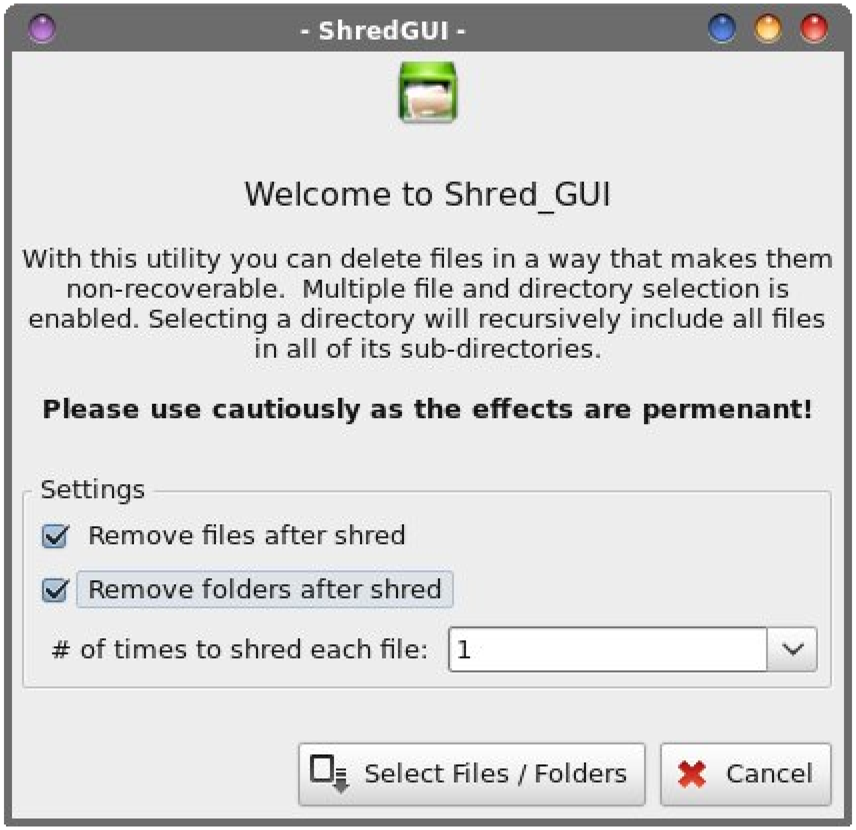
Hmmm … yet another secure file deletion utility that doesn't play well with journaled file systems. As a result, the previous warnings about sensitive data being left behind do apply. The emphasis with the **red text** is mine, by the way.

Stringing together all the necessary command line options, you might use shred like this:

```
shred -v -u -z -n 1 path/to/some.file
```

The **-v** switch turns on verbose output, so you have some indication of progress. The **-u** switch truncates and removes the file after overwriting. The **-z** switch performs a final overwrite of the file with zeros. The **-n 1** switch tells shred to overwrite the data with random data in one pass. If you want more passes, change the "1" to the number of passes you want to perform. Finally, there is the path and filename of the file you want to securely delete.

Contrary to the popular belief in some paranoia filled circles that more passes equals greater security, one pass is generally sufficient to obfuscate files. After making one pass with random data and then overwriting that data with zeros, your data will not be recoverable on a modern hard drive. Multiple passes, however, will increase wear and tear on your hard drive, and it will take longer to complete the process. Remember … we're talking about magnetic media here, not SSDs, which are a whole different creature.



- ShredGUI -

Welcome to Shred_GUI

With this utility you can delete files in a way that makes them non-recoverable. Multiple file and directory selection is enabled. Selecting a directory will recursively include all files in all of its sub-directories.

Please use cautiously as the effects are permenant!

Settings

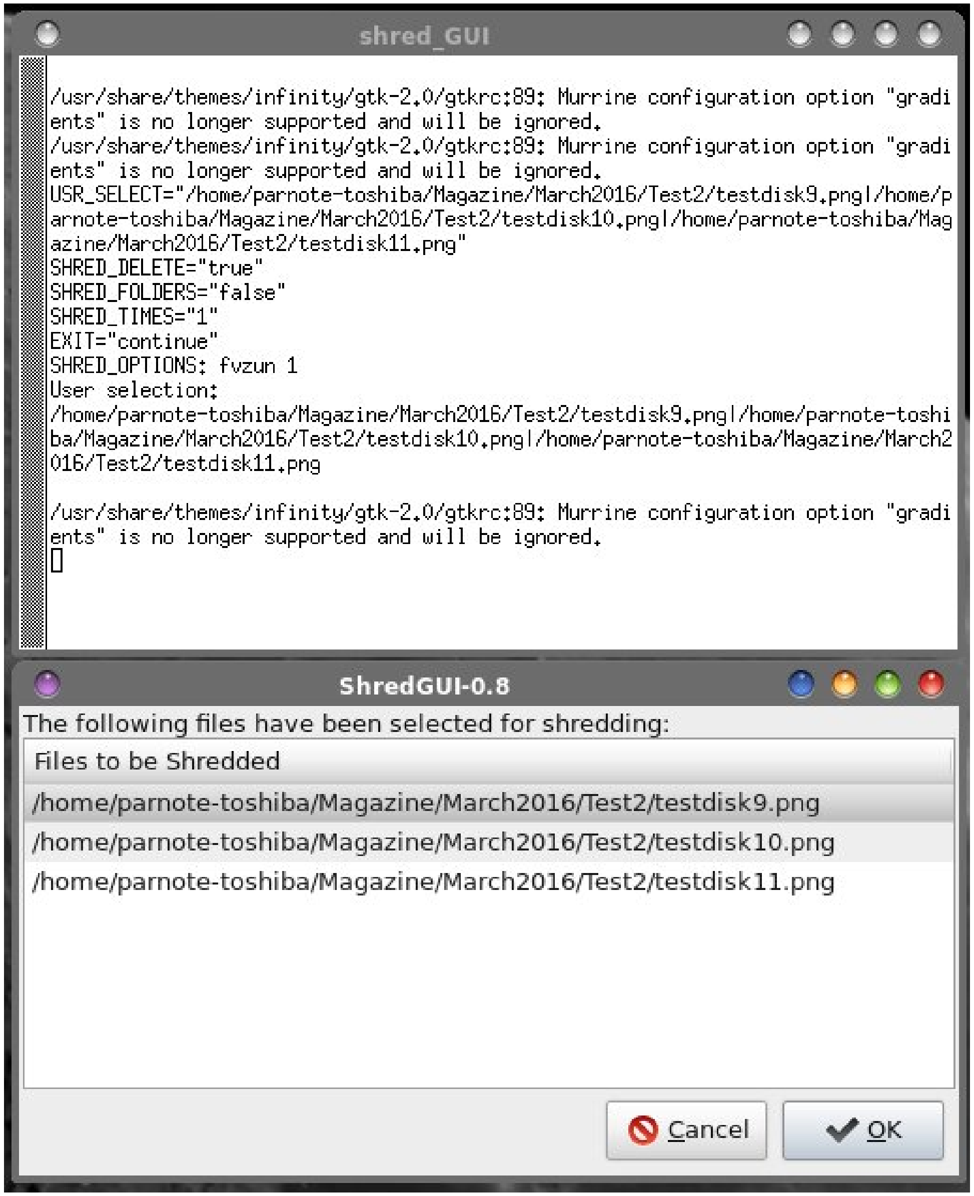
☑ Remove files after shred

☑ Remove folders after shred

# of times to shred each file: 1

When you launch Shred_GUI, you should see something like the image above. You would do well to read the text in the program's main window. By default, the checkboxes are unchecked, so you will need to check the relevant boxes that pertain to what you are wanting to delete. You will also need to select how many times to "shred" each file. Shredding them once should be sufficient, but you can select to shred each file up to 50 times, which is probably way beyond overkill.

Next, select the "Select Files/Folders" button, and you can select the files and folders (directories) you want to shred.



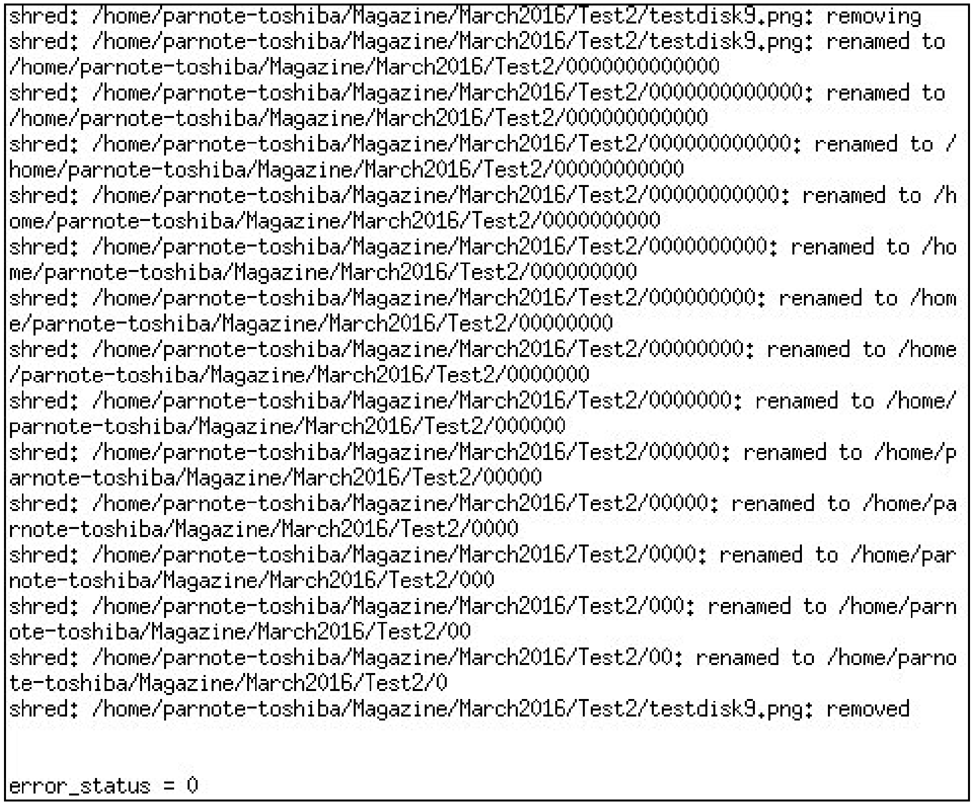
```
/usr/share/themes/infinity/gtk-2.0/gtkrc:89: Murrine configuration option "gradi
ents" is no longer supported and will be ignored.
/usr/share/themes/infinity/gtk-2.0/gtkrc:89: Murrine configuration option "gradi
ents" is no longer supported and will be ignored.
USR_SELECT="/home/parnote-toshiba/Magazine/March2016/Test2/testdisk9.png|/home/p
arnote-toshiba/Magazine/March2016/Test2/testdisk10.png|/home/parnote-toshiba/Mag
azine/March2016/Test2/testdisk11.png"
SHRED_DELETE="true"
SHRED_FOLDERS="false"
SHRED_TIMES="1"
EXIT="continue"
SHRED_OPTIONS: fvzun 1
User selection:
/home/parnote-toshiba/Magazine/March2016/Test2/testdisk9.png|/home/parnote-toshi
ba/Magazine/March2016/Test2/testdisk10.png|/home/parnote-toshiba/Magazine/March2
016/Test2/testdisk11.png

/usr/share/themes/infinity/gtk-2.0/gtkrc:89: Murrine configuration option "gradi
ents" is no longer supported and will be ignored.
```

The following files have been selected for shredding:

Files to be Shredded
/home/parnote-toshiba/Magazine/March2016/Test2/testdisk9.png
/home/parnote-toshiba/Magazine/March2016/Test2/testdisk10.png
/home/parnote-toshiba/Magazine/March2016/Test2/testdisk11.png

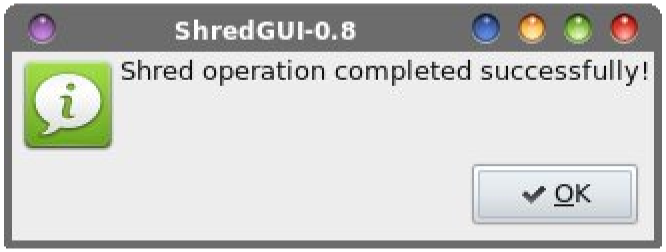
In the above image is a window that shows the three files I asked Shred_GUI to delete. The Xterm window typically opens behind the Shred_GUI window, but I repositioned the windows so you can see them in one screenshot. Shred_GUI simply runs the shred command line utility. Notice in the Xterm window that the SHRED_OPTIONS parameter (about halfway down the Xterm window) shows "fvzun 1" being passed to the shred command line program. These options are the command line switches that are then used by the shred command line program to delete your files.



```
shred: /home/parnote-toshiba/Magazine/March2016/Test2/testdisk9.png: removing
shred: /home/parnote-toshiba/Magazine/March2016/Test2/testdisk9.png: renamed to
/home/parnote-toshiba/Magazine/March2016/Test2/0000000000000
shred: /home/parnote-toshiba/Magazine/March2016/Test2/0000000000000: renamed to
/home/parnote-toshiba/Magazine/March2016/Test2/000000000000
shred: /home/parnote-toshiba/Magazine/March2016/Test2/000000000000: renamed to /
home/parnote-toshiba/Magazine/March2016/Test2/00000000000
shred: /home/parnote-toshiba/Magazine/March2016/Test2/00000000000: renamed to /h
ome/parnote-toshiba/Magazine/March2016/Test2/0000000000
shred: /home/parnote-toshiba/Magazine/March2016/Test2/0000000000: renamed to /ho
me/parnote-toshiba/Magazine/March2016/Test2/000000000
shred: /home/parnote-toshiba/Magazine/March2016/Test2/000000000: renamed to /hom
e/parnote-toshiba/Magazine/March2016/Test2/00000000
shred: /home/parnote-toshiba/Magazine/March2016/Test2/00000000: renamed to /home
/parnote-toshiba/Magazine/March2016/Test2/0000000
shred: /home/parnote-toshiba/Magazine/March2016/Test2/0000000: renamed to /home/
parnote-toshiba/Magazine/March2016/Test2/000000
shred: /home/parnote-toshiba/Magazine/March2016/Test2/000000: renamed to /home/p
arnote-toshiba/Magazine/March2016/Test2/00000
shred: /home/parnote-toshiba/Magazine/March2016/Test2/00000: renamed to /home/pa
rnote-toshiba/Magazine/March2016/Test2/0000
shred: /home/parnote-toshiba/Magazine/March2016/Test2/0000: renamed to /home/par
note-toshiba/Magazine/March2016/Test2/000
shred: /home/parnote-toshiba/Magazine/March2016/Test2/000: renamed to /home/parn
ote-toshiba/Magazine/March2016/Test2/00
shred: /home/parnote-toshiba/Magazine/March2016/Test2/00: renamed to /home/parno
te-toshiba/Magazine/March2016/Test2/0
shred: /home/parnote-toshiba/Magazine/March2016/Test2/testdisk9.png: removed


error_status = 0
```

The image above shows the output from the shred command line tool running in Xterm. Shred_GUI will show you the output so that you can follow the progress of the file deletion.



Shred operation completed successfully!

Finally, Shred_GUI will give you a confirmation dialog box when the operation is complete. If there were problems or errors, a slightly different dialog box will be displayed that details any problems that were encountered. Also, the green icon at the left of the confirmation dialog box is changed to a red “X” icon, if problems or errors were encountered.

Like with the other secure file deletion utilities we’ve discussed, your results using shred or Shred_GUI with a journaled filesystem (e.g., EXT4, Reiser4, etc.) won’t be a guarantee, but it’s better than the basic rm command, and definitely better than nothing.

bcwipe

This utility definitely is in the PCLinuxOS repository. So, installing it on your system is as simple as installing any other program from the repository onto your computer, via Synaptic.

BCwipe is a command line program, and (as far as I know or can discern) there is no GUI front end for the free version in the repository. There is indication that the paid, commercial version (available for just under $40 (USD) from http://www.jetico.com) does have a GUI.

Here’s the description for bcwipe from Synaptic:

> Securely erase data from magnetic and solid-state memory.

So, that’s not much to go on. Let’s see if the help text for bcwipe helps.

```
[parnote-toshiba@parnote-toshiba Test]$ bcwipe -h
bcwipe version 1.9-8 rev 319 2010-10-04  Copyright 1994-2010
Jetico, Inc.
Usage: bcwipe [OPTIONS]... FILE...
Remove FILE(s) with wiping.
OPTIONS:
  -mb           German BCI/VISTR 7-pass wiping
  -md           U.S. DoD 5220-22M 7-pass extended character
                rotation wiping
  -me           U.S. DoE 3-pass wiping
  -mf<file>     read wiping scheme from file. See *notes below
  -mg           (default) 35-pass wiping by Peter Gutmann
  -ms           7-pass wiping by Bruce Schneier
  -mt           1-pass test mode: fill the start of 512-byte block
                with block number
  -mz           1-pass zero wiping
  -m N          U.S. DoD 5220-22M N-pass extended character
                rotation wiping
  -w            disable verification
  -n sec        NAS mode: wait sec seconds between wiping passes.
                See **notes below
  -s            use ISAAC random instead of SHA-1
  -p            use random pattern instead of full random
  -r            process the contents directories recursively
  -f            force wiping, never prompt (use with caution)
  -d            do not delete file(s) after wiping
  -b            wipe contents of block devices (use with caution)
  -B            disable direct IO access mode for block devices
  -t N          use N threads to wipe block devices. Useful for
                multiple disk devices.
  -S            wipe file slacks
  -F            wipe free space on mounted file system
  -i            prompt before any removal (y/[n]/a)
                  y - yes, n - no(default), a - yes for all
  -I            disable interactive prompt
  -v            verbose mode
  -l[file]      write log to file. Log to console if file name is
                omitted
  -V            output version information and exit
  -h            display this help and exit


 *         scheme file line format: pass_number.
{random|complementary|hex[,hex[,hex[,hex]]][, verify]}
           Example:
           1. random, verify
           2. AA,00,55
 **        modern enterprise level storage systems (NAS, disk
           arrays etc.) employ powerful caches. To avoid
           undesirable caching effects use this option to insert
           delay before file deleting.

Report bugs to support@jetico.com
```

The bcwipe man page at FreeBSD is somewhat helpful, but really doesn’t shed much more light on things than the online help text. I didn’t find a typical Linux man page, but was able to track this one down. Jetico also has an online command line reference page here.

I actually have this one set up as a custom action in Thunar to securely delete files from my hard drive. From what I’ve been able to ascertain from the scattered commentary and documentation about bcwipe is that it doesn’t care much about the file system that it is scanning. Rather, it goes after the actual data itself.

Most commentary and documentation is positive about bcwipe. By default (without specifying otherwise), bcwipe uses the “Gutmann” method of wiping files, by overwriting the data 35 times. You can speed things up considerably by specifying the use of the U.S. DoD 5220-22M 7-pass extended character rotation wiping scheme, with the -md command line switch. Hey, it's only seven passes of random characters, but if it's good enough for the U.S. DoD and their sensitive data, then it ought to be good enough for the rest of us.

Your bcwipe command line might look something like this:

```
bcwipe -md -r -v -I path/to/some.file
```

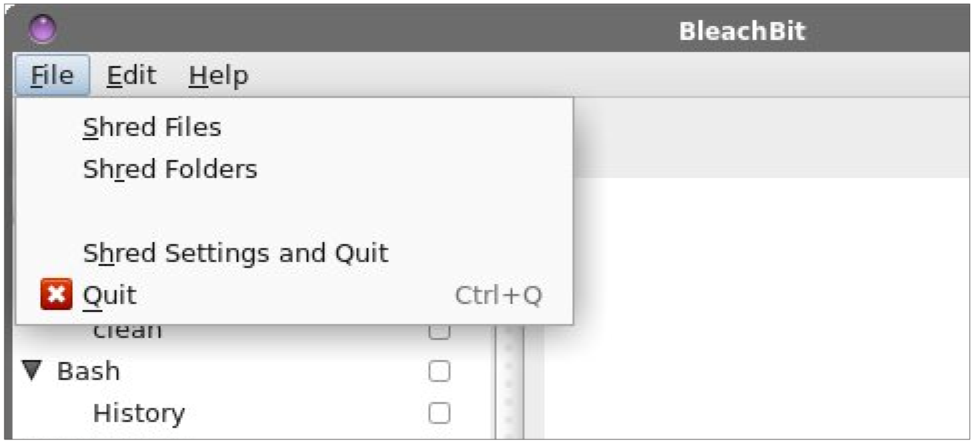
The **-md** command line switch tells bcwipe to use the U.S. DoD seven pass method. The **-r** command line switch tells bcwipe to recurse directories, deleting all files and subdirectories, along with all the content of those subdirectories. The **-v** turns on verbose mode, so you have some feedback and progress notification. The **-I** turns off interactive mode, and just goes straight after the data. If "path/to/some.file" is a directory, instead of a file, then that directory and all of its contents, including subdirectories and their contents, will be wiped from your hard drive.

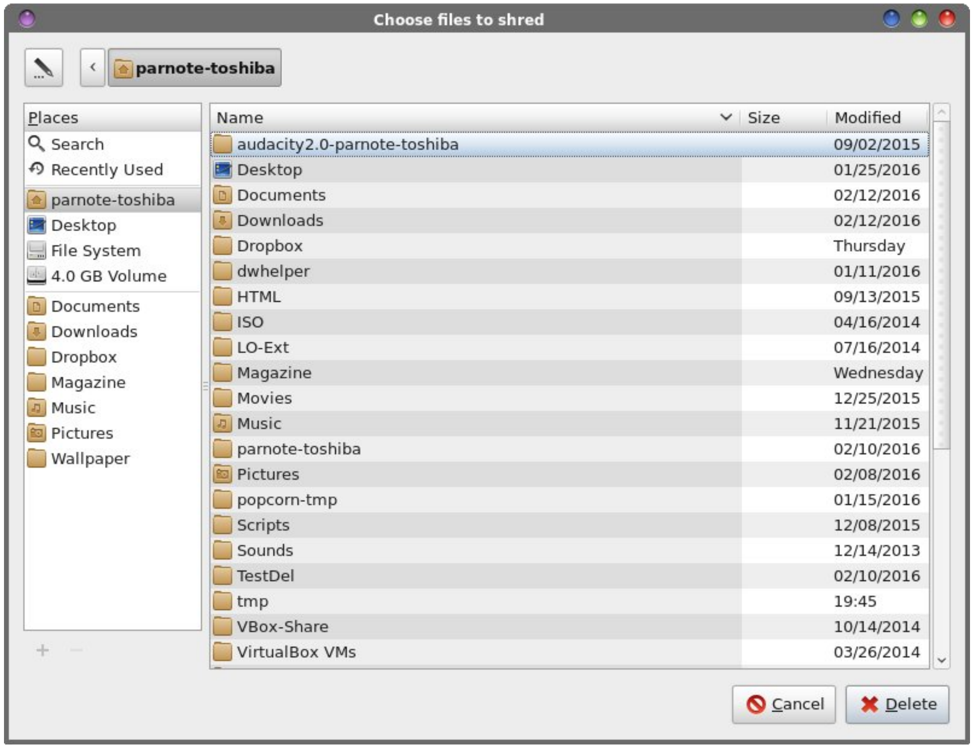
If I were going to choose just one secure file deletion program to install on my computer, bcwipe would be it. Not only is it easy to use, especially after I've set it up as a custom action in Thunar (KDE users can do something similar by setting it up as a service menu in Dolphin and Konqueror … refer to here for how to set up a KDE service menu), but it has a fairly good reputation. Plus, Jetico has a pretty impressive list of clients (U.S. DoD, U.S. DoE, etc.) who rely on being able to cover their tracks completely and be able to wipe magnetic media of very sensitive material. If it meets their needs, it ought to be able to meet yours and mine.

BleachBit

If this one sounds familiar, it should. It has been a staple of every full PCLinuxOS installation for nearly as long as I can remember. Most users use BleachBit to periodically clean their computers of old browser cookies, old log files, and a whole host of remnant files that are no longer necessary. Believe it or not, many users may not be aware that BleachBit also has the ability to securely delete files and directories from your computer.

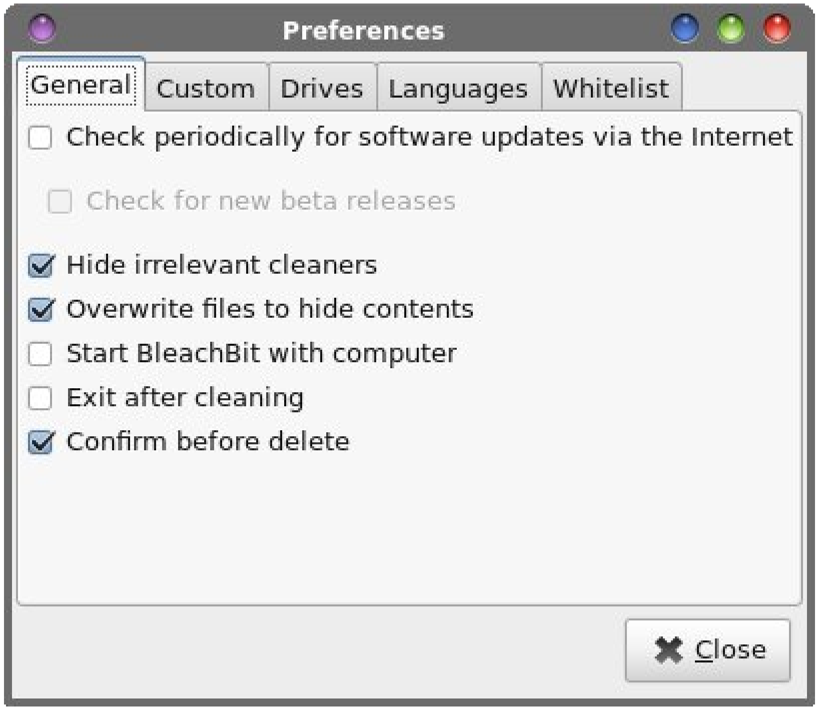
Just take a look at the first two items listed in the "File" menu: Shred Files and Shred Folders. I wasn't even aware that BleachBit offered these "services" until I found a couple of passing comments about using BleachBit to securely delete files, while I was searching out more information for this article. Lo and behold, there those features are, hiding right under my nose all this time. I suspect I'm not the only user who simply went down the list of option in the left pane, selecting the things I wanted cleaned from my computer, and never paying any mind or attention to the menu options.





Name	Size	Modified
audacity2.0-parnote-toshiba		09/02/2015
Desktop		01/25/2016
Documents		02/12/2016
Downloads		02/12/2016
Dropbox		Thursday
dwhelper		01/11/2016
HTML		09/13/2015
ISO		04/16/2014
LO-Ext		07/16/2014
Magazine		Wednesday
Movies		12/25/2015
Music		11/21/2015
parnote-toshiba		02/10/2016
Pictures		02/08/2016
popcorn-tmp		01/15/2016
Scripts		12/08/2015
Sounds		12/14/2013
TestDel		02/10/2016
tmp		19:45
VBox-Share		10/14/2014
VirtualBox VMs		03/26/2014

Selecting the "Shred Files" option opens up a file selection dialog box to allow you to select which files you want to get rid of. The same file selection dialog box opens when you select the “Shred Folders” option, allowing you to delete entire directories. It’s really that simple.



□ Check periodically for software updates via the Internet

□ Check for new beta releases

☑ Hide irrelevant cleaners

☑ Overwrite files to hide contents

□ Start BleachBit with computer

□ Exit after cleaning

☑ Confirm before delete

When you select the Edit > Preferences menu option, you should see the window shown above. You will want to select the second and fifth option under the “General” tab to insure secure deletion of your files and directories. On my Xfce installation of PCLinuxOS, these options were already selected (I had never changed or even checked them before). However, you will want to insure they are selected prior to using BleachBit to securely delete files and directories on your computer.

I never knew that I already had a secure file deletion option installed this whole time. I wonder how many others don’t realize it, either.

Secure File Deletion Summary

At this point in time, secure file deletion that can be relied on is an unrealized dream for those of us who use journaled file systems. There simply are no guarantees that sensitive data cannot be recovered. Believe me when I say that I’m not faulting the use of journaled file systems. They are a natural and necessary evolution that needed to happen. Before they came along, data loss was a very real risk, especially if the computer crashed or lost power in the middle of writing a file. I can remember the computer crashing in the middle of saving a file years ago (when I was using Windows, and it happened more than once), and the results were corrupted files and even corrupted file systems. For some users, the results were catastrophic, necessitating a full reinstallation and resulting in loss of LOTS of data. Journaled file systems have helped to mostly resolve and at least lessen that risk.

Are the secure file deletion tools helpful? Yes. Most assuredly, all of them are far better than the normal file deletion accomplished with the rm command. Do they hide or eliminate data? That depends on who you ask. To at least some extent, they prevent data from being recovered when using user level file recovery tools. But, they may not prevent a forensic computer lab from doing the same.

As a case in point, in the article Digital Forensics: In-depth analysis of SRM and BCWipe (for unix) blog article on the SANS Digital Forensics and Incident Response website, author Juan Leaniz deleted files from a *nix system using srm, shred and bcwipe. He then tried to recover the data using the open source command line tools collectively known as “The Sleuth Kit.” You can check out the tools here, where they may be downloaded for free. There is also a companion tool called “Autopsy,” which expands/harnesses the capabilities of The Sleuth Kit. Both tools can be downloaded for free, but you will have to compile them from source to install them on your system.

At any rate, I’m getting a bit off topic. In every case where he attempted to do a secure file deletion with srm, shred and bcwipe, the tools in The Sleuth Kit were able to completely recover/view the “deleted” data from the hard drive.

Such revelations don’t make me rest easy about “secure file deletion” on my computers. Not that I have anything to hide, but if I did, I sure wouldn’t be relying on these tools to cover my tracks or obfuscate sensitive data.

Securely Wiping Magnetic Media

Probably the MORE secure way to get rid of sensitive data (or cover your tracks) from magnetic media would be to completely wipe the hard drive. Fortunately, there are three tools you can install from the PCLinuxOS repository to help you accomplish this.

Before we proceed, I feel that it’s **very important** to issue a very, very terse and necessary warning. ***CAUTION:*** These actions are irreversible, and will result in total data loss! DO NOT try this on a drive that contains data you want to keep, at least until you’ve made a backup of any data/files you might want to retain.

With that out of the way, I also have to come forward and state that I have not yet tried any of these methods that follow. Even with all the computers I have (each one is dedicated to a specific purpose), I am not in a position where I can wipe the hard drive of any of them. Instead, I must rely on the knowledge and attempts by others. In this respect, I am merely the messenger of what others have divulged. For much of this, we can thank PCLinuxOS forum member (and Super Hero) Not_yet_16 for his tireless and unselfish work in showing us how to securely wipe magnetic media.

bcwipe

Say what? Didn't I already cover this one?

Well, yes I did. But there is an option with bcwipe that allows a user to wipe an entire hard drive, or hard drive partition. I'll spare you from having to read a repeat of everything else I've already written about bcwipe. Instead, let's focus on this one option.

The command you will need is as follows:

```
bcwipe -b -v /dev/sdX
```

This will completely wipe the specified drive. The **-b** command line switch tells bcwipe to delete the contents of the block device specified at the end of the command line. The **-v** option specifies verbose output, so you have some indication of what is happening and so you can monitor the progress. The /dev/sdX is the drive/partition designation that you want to wipe. By default, bcwipe will use the Gutmann method to wipe the hard drive using 35 passes. If you wanted to use the DoD seven pass method, add in the -md command line switch after the -v option (it will save you a whole lot of time, and will most likely be just as effective).

You can also enter the command as follows, if you want to zero out the **free space** of the specified target:

```
bcwipe -F -v -mz [target]
```

Doing this, you will overwrite all of the free space on the specified target with one pass of zeros. So, on the laptop I'm using to write this article, I could enter "bcwipe -F -v -mz /home" to zero out all the free space in my /home directory, which exists on its own drive partition. That free space should also include any data from files that have been "deleted," but not yet overwritten.

This is why I said earlier that if I had to choose one tool for securely deleting files, bcwipe would be it. It's flexible to use for individual files (with no guarantees, obviously) and to use for wiping magnetic media, it's easy to use, and it appears to do the job.

dd & dcfldd

I combine both of these tools under the same section because they both use the exact same command line syntax. At one time, and until very recently, dd lacked any progress indicators to let you know that it was even doing anything. You'd execute a command and just sit back and wonder. So, since dcfldd did offer progress indicators, some users transitioned to using it in place of dd, especially for tasks that took a bit of time to complete. In fact, dcfldd uses dd as its basis. Lately though, users have reported that dd now has progress indicators. To "activate" the progress indicator with the dd command, add the **status=progress** option to the end of the dd command. So the choice is yours about which one to use. They will both accomplish the task we aim to complete.

To completely wipe a hard drive, you will need to use this command:

```
dd if=/dev/zero of=/dev/sdX

dcfldd if=/dev/zero of=/dev/sdX
```

The **if=/dev/zero** sets the input file to all zeros. The **of=/dev/sdX** writes those zeros out to fill up the drive identified as /dev/sdX. On the laptop I'm writing this article on, that would be sda.

To completely wipe a hard drive **partition**, you will need to alter the command a bit, like this:

```
dd if=/dev/zero of=/dev/sdXY

dcfldd if=/dev/zero of=/dev/sdXY
```

The first part of the command remains the same. Only the last part of the command, the **of** part, needs to change. Notice how we now have sdXY. The X represents the drive that contains the partition, Y, that I want to wipe. On the laptop I'm writing this article on, that would be sda5 for the /root partition, and sda6 for my /home partition.

To completely wipe the **free space** on a hard drive (which should include deleted files), you will need to enter the command like this:

```
dd if=/dev/zero of=/dev/sdXY/wiped

dcfldd if=/dev/zero of=/dev/sdXY/wiped
```

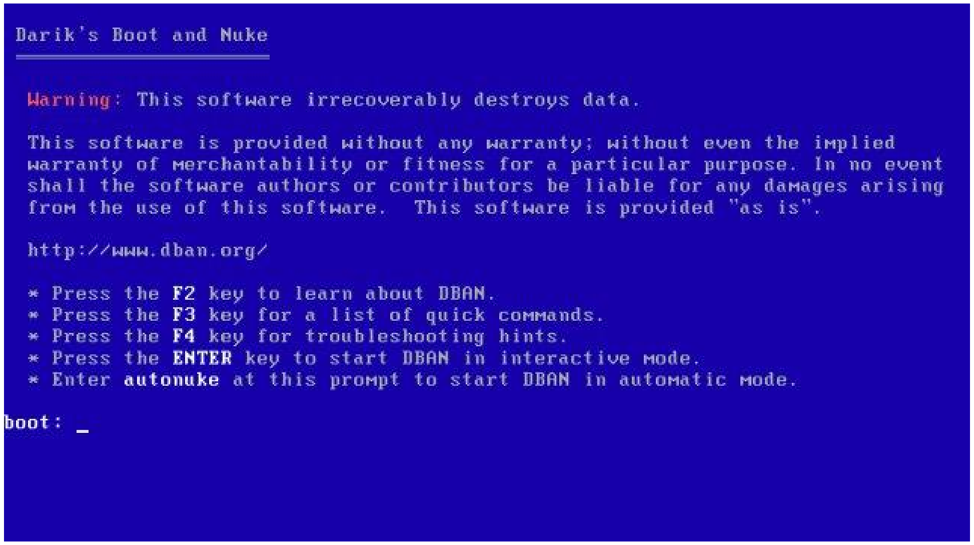
The command remains the same as the previous one, with one addition. With this version of the command, we write out the zeros to the file named “wiped.” This will create one huge file that consumes the free space on the designated partition, full of zeros. Then, just go in and delete the file named “wiped” and the free space will be reclaimed.

If your /home directory is on a separate partition, this is a very effective way to wipe the free space. If you want to do this on your /root partition, however, it would be best to do this from a different operating system (another installation on the same computer), or from a LiveCD/LiveDVD/LiveUSB. Otherwise, you will run out of space on your /root partition.

As you can see, wiping an entire hard drive, wiping a partition, or wiping the free space on a drive all require slightly different approaches. But these are also probably one of the most effective ways of eliminating any traces of sensitive data.

Darik’s Boot and Nuke

Informally known as DBAN, Darik’s Boot and Nuke is a 16.7 MB LiveCD ISO file that you burn to a CD. You can download the ISO from SourceForge.



```
Darik's Boot and Nuke

 Warning: This software irrecoverably destroys data.

 This software is provided without any warranty; without even the implied
 warranty of merchantability or fitness for a particular purpose. In no event
 shall the software authors or contributors be liable for any damages arising
 from the use of this software.  This software is provided "as is".

 http://www.dban.org/

 * Press the F2 key to learn about DBAN.
 * Press the F3 key for a list of quick commands.
 * Press the F4 key for troubleshooting hints.
 * Press the ENTER key to start DBAN in interactive mode.
 * Enter autonuke at this prompt to start DBAN in automatic mode.

boot: _
```

Since you boot DBAN from a LiveCD session, it doesn’t care what the installed operating system is. Your mouse won’t be needed (or recognized) since it’s menu driven via the keyboard.

From the SourceForge download page:

“Darik's Boot and Nuke ("DBAN") is a self-contained boot floppy that securely wipes the hard disks of most computers. DBAN is appropriate for bulk or emergency data destruction.”

Insert the LiveCD and reboot your computer to run off of the LiveCD. Once it has booted, follow the onscreen menu prompts. Don’t expect it to be particularly fast, though. Some of the comments on SourceForge tell of it running for almost two days to finish wiping large hard drives. Also, DBAN will ignore SSDs, and will not work on them … and I suspect you wouldn’t want it to, anyways.

Secure Wiping Magnetic Media Summary

Without a doubt, wiping magnetic media is WAY more certain to eliminate any traces of sensitive data that you don’t want anyone else to recover. In an age when privacy is under attack from all directions, and more and more criminals are using more sophisticated methods to gain access to your private and personal data, you can’t be too careful.

Back in 2008, there was a challenge posted to three different professional data recovery firms to see if they could recover data from a drive that was overwritten with one pass of zeros. The challenger (System16) divulged that the dd command was used to wipe the drive with a single pass of zeros. Upon hearing that dd was used, two firms immediately declined to review the drive. The third was willing to try, but admitted that their Unix team stated a “less than zero percent chance” of retrieving any data from a drive overwritten with a single pass of zeros using the dd command. You can read more information about the challenge, which lasted one year, here.

If it were me, I’d certainly trust the results from using the dd and dcfldd commands. If professional data recovery firms won’t even look at a drive that was wiped with these commands, then I shouldn’t expect anyone to be able to retrieve any sensitive, private or personal data.

When all else fails …

If none of the above methods give you enough peace of mind, then you can always physically destroy a hard drive. There are several methods you can use, and some are more fun than others. Yes, I said fun.

First of all, you can take the tried and true route and drill holes in the hard drive. There are a lot of YouTube videos with folks doing just this. If you choose this route, please be sure to clamp the hard drive in a vise or to your work surface. You DO NOT want to hold the hard drive in one hand and attack it with a drill in your other hand. The hard drive could spin uncontrollably as it breaks free from your grip (yes, the risk is very high here), or you could drill through your hard drive and straight into your hand that's supporting the hard drive. In either case, you're most likely going to (at least) be paying a visit to the Emergency Department of your local hospital. Unfortunately, there are some "less than bright" individuals showing you how to do it the dangerous way in some of these videos. Please … do NOT follow their lead. Use proper tool safety, and wear proper protection (goggles anyone?) to prevent injury to yourself.

Another way of putting holes in your hard drive (and rendering it inoperable, and thus rendering your data unretrievable) is to shoot holes in it at the shooting range (if that's an option for you). There are a lot of YouTube videos showing people doing just this. I will caution you that not all of the videos are produced by the brightest of individuals. So, if you decide on this route to literally obliterate your data, please practice firearm safety. Some of the clowns in the videos just have way more testosterone than common sense.

Yet another way to dispose of your hard drive is to smash it with a hammer. Just as with the previous two methods, there are several YouTube videos showing you how to go about it. And, just as with the previous methods, not everyone follows common sense safety rules … like wearing eye protection. Even the so-called "pros" employ unsafe practices in their videos (think Geek Squad). A lot of newer hard drives have glass platters that are coated with iron oxide. This makes their destruction very easy: just a couple of good, powerful whacks with a hammer and the glass platters are shattered, rendering your data unretrievable. For older hard drives, their platters are made of aluminum or steel, so they will require a much more severe "beating" to render the data on them unretrievable.

You can also utilize machines that are especially made for the physical destruction of hard drives. These machines typically are quite expensive (thousands of U.S. dollars), but the costs associated with them are far less than the theft of your personal information and data. You can watch some YouTube videos showing these machines in action. While you may not want to purchase your own “Disk Destroya” machine, there may be companies in your area that will put your used hard drive through the machine. They will most likely charge a modest fee.

If you work in a machine shop or automotive shop and have access to a hydraulic press, it’s highly doubtful that your used hard drive will survive a few trips through the press with tons of pressure applied to your hard drive. Just be sure you clear it with your boss or shop foreman first. We don’t want anyone losing their job over this. Also, it would be wise to alter the compression point with each pass through the press.

Finally, you can open up the hard drive and physically scrape the iron oxide coating from the platters. Or, you can cut up the platters with a cutoff wheel grinder or power hack saw. At any rate, you will rest assured that there is NO chance of ever retrieving the data on those drives … ever.

Consider environmental issues when you dispose of your destroyed hard drive’s carcass. Many electronic devices contain dangerous and poisonous compounds, like lead and mercury, and you will want to insure that your hard drive is disposed of properly. Improper disposal could risk those dangerous and poisonous compounds leaching into surrounding soil and groundwater. They may not affect you today, but these compounds can affect your children and your grandchildren in the future. In some jurisdictions, you can be fined or charged with a crime for improperly disposing of such items.

Also, keep in mind that trying to sell a computer without a hard drive will cause you to get a significantly lower price for your used computer. If you’re giving it away, the person (or entity) receiving your discarded computer may not have the money or knowledge to replace the hard drive. Despite your good and/or charitable intentions, they will end up with a computer that they cannot use. Both situations can be remedied by you buying a new hard drive and installing it (and the OS) before selling or giving away your old computer. Even an inexpensive new hard drive is better than no hard drive at all.

Overall Summary

Thanks to the widespread use of journaled file systems, secure file deletion by itself is no guarantee, except for preventing recovery by user level file recovery tools. They do a fairly decent job at preventing the average Joe from gaining

The PCLinuxOS magazine
Windows Migration Guide
September 2013
The PCLinuxOS magazine
Enlightenment Special Edition
May, 2011
The NEW PCLinuxOS Magazine
Fall 2010
The KDE 4 SC Special Edition
The NEW PCLinuxOS Magazine
Gtk Lightweight Desktops: Xfce & LXDE Special Edition
November, 2010
The NEW PCLinuxOS Magazine
Command Line Interface Intro Special Edition
October, 2010
The PCLinuxOS magazine
Openbox Special Edition
March, 2012

access to your files and data. But, a forensic computer lab or professional data recovery firm will probably have no problem – whatsoever – retrieving the data that was deleted with one of these tools.

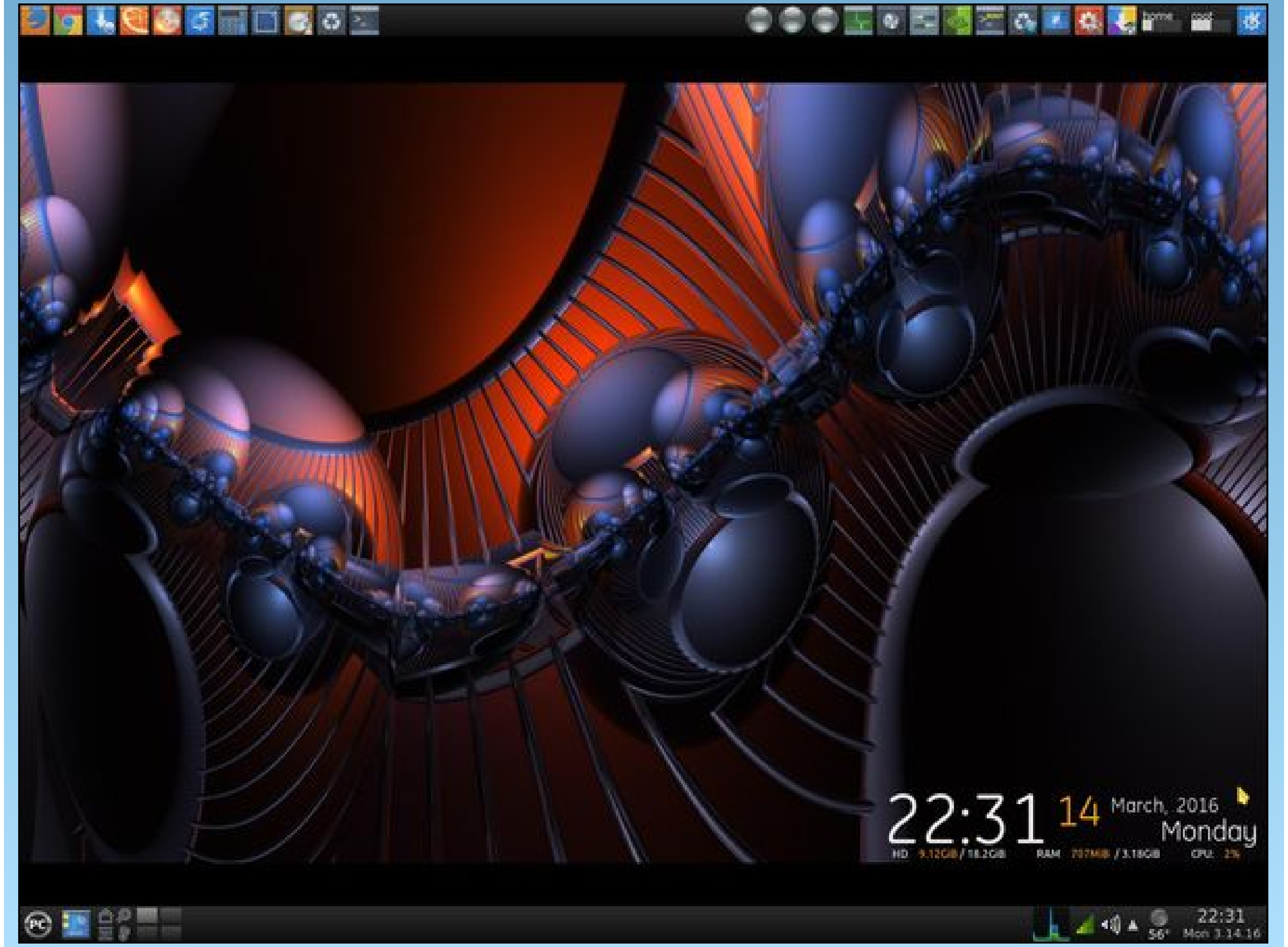
If you can do it, wiping the entire hard drive is your best bet, short of physical destruction of the hard drive. There are many different methods you can use to physically destroy the hard drive: degaussing with a strong magnetic field, drilling holes through the hard drive platters, sledge hammers, incineration, and physical shredding … just to name a few. There are even companies that make machines dedicated to the destruction of data storage media. Costs for such machines run in the thousands of U.S. dollars.

Just as much as privacy has catapulted itself to the forefront of our consciousness, ecological concerns also remain. The gross, physical destruction of hard drives leaves them as nothing more than landfill fodder. With that remains concerns about toxic chemicals used in the production of hard drives and their components leaching into the soil and possibly making their way into our groundwater systems. Still, for some users, this remains the most certain way to destroy any traces of sensitive, personal or private data.

But, given that professional data recovery firms won't accept the challenge to attempt recovery of files/drives zeroed with the dd command, there are definitely options other than the physically destruction of a hard drive that may still give several years of useful service.

Perhaps the ideal solution lies with a combination of the two methods. First, delete your sensitive/personal/private files with one of the secure file deletion commands. Second, follow that up with the wiping of the free space on that drive. After that, you should be able to sleep well at night, safe in the knowledge that no one can ever get their hands on your data ever again.

Screenshot Showcase



Posted by trytip, March 15, 2016, running KDE.

PCLinuxOS Recipe Corner

Slow Cooker Cheesy Mexican Chicken

Ingredients:

Chicken

1 lb boneless skinless chicken breasts, cut into bite-size pieces
1 package mild taco seasoning mix
1 can (10 oz) mild enchilada sauce
1 can (14.5 oz) diced tomatoes, undrained
1 cup shredded Cheddar cheese (4 oz)

Accompaniment

2 packages (8.2 oz each) Old El Paso™ fiesta rice

Optional Toppings

1/4 cup chopped fresh cilantro

Directions:

1. Spray 4-quart slow cooker with cooking spray.

2. Place cubed chicken in slow cooker. Sprinkle taco seasoning mix over chicken; stir, making sure all pieces are well coated. Stir in enchilada sauce and tomatoes. Stir once again until well combined.

3. Cover; cook on Low heat setting 6 hours.

4. Uncover; sprinkle cheese over chicken. Cover; cook on Low heat setting 10 minutes longer.

5. Meanwhile, cook rice as directed on packages.

6. Serve chicken over rice. Top with cilantro if desired.

Tips:

Make a double batch of this recipe and pack leftovers for an excellent lunch the next day.

Not only does this cheesy Mexican chicken taste great on rice, it also is great in wraps or as a salad topper.

ms_meme's Nook: Putting On The Ritz With PCLinuxOS

Are you caught in Window's rat race
Need an OS to take its place

Though it's famous everywhere
It has flaws so beware

It cost a lot of dollars
No longer be one of its followers

Don't spend your last cent
Leave Window's torment

MP3 **OGG**

If Windows makes you blue
Why don't you get something new
Without stress
PCLinuxOS

Runs so smooth download it now
You will find it is highbrow
The very best
PCLinuxOS

You will like its easy updating
Get it now why are you waiting
Never frustrating

Come now mix in our forum
Find new friends with decorum
What a success
PCLinuxOS

If Windows makes you blue
Why don't you get something new
Without stress
PCLinuxOS

Runs so smooth download it now
You will find it is highbrow
The very best
PCLinuxOS

You will like Texstar's creation
Don't forget to give a donation
No hesitation

Come now mix in our forum
Find new friends with decorum
What a success
PCLinuxOS

If Windows makes you blue
Why don't you get something new
Without stress
PCLinuxOS

Runs so smooth download it now
You will find it is highbrow
The very best
PCLinuxOS

Never have to do that defraggin'
About this OS tongues are waggin'
Always braggin'

Come now mix in our forum
Find new friends with decorum
What a success
PCLinuxOS

PCLinuxOS Family Member Spotlight: Bill Grubbs

As told in his own words

What is your name/username?
Bill Grubbs/Bill Grubbs

How old are you?
The body is 66, the mind is 26. It's a bad combination.

Are you married, single?
Never married

How about Kids, Grandkids ?
None that I am aware of.

Do you have pets, what is your favorite?
I love animals and especially dogs. I own a 15 year old cat. I hate cats.

Are you retired, still working and if working, what do you do?
I am a retired steam boiler plant operator for Atlanta Water Works. 28 years service. I could start the plant up from a cold start and shut it down completely without assistance.

Where do you call home? What is it like? IE: weather, scenery
I am a native of Atlanta Georgia USA. It is a rather crowded place but there is lots to do in and around the area.

I tend to stay on the fringes of it. The suburbs are wooded with pines, oaks, dogwoods, maples and so on. It is lovely here in the fall. We have four distinct seasons. Winters are tolerable and generally there are only a few episodes of snow. Spring is lovely with lots of things blooming. Expect summer highs to be around 95F during the day with 80 at night. For the last few summers we have had lots and lots of rain. My lawn has never looked so good.

Cartecay Vineyard in North GA

Urban scenery is minutes away. Mountains are an hour or so to the North. The coastal plain is a few hours to the East. Florida's sandy beaches are a day's drive away. We have our own river, the Chattahoochee. And our own big lake, Lake Lanier, that provides water sports of all kinds.

Where did you go to school and what is your education level?
I attended Reinhardt University and Georgia State University. I have a BBA degree. My roommate at Rinehardt had a '68 Road Runner 383 that provided a lot of fun. This was in '68-'70. I met my Ellijay friend at Rinehart and we rode all over creation in his Olds 442. Those were good days.

What kind of things you like doing? hobbies, travel, fishing, camping?
Currently, I travel to Ellijay, GA about once a month where an old college buddy has a band named Downtown Roy. Ellijay is also the heart of Georgia apple country and you can buy all kinds of good things to eat at the apple houses. I like cars and planes. There is a good USAF museum in Warner Robins, GA and I visit it when I can.

I love to type and honed my typing skills in chat rooms back during the BBS days. In the late 90's I was big into IRC chat. I started and ran a successful group on Facebook that is still going strong today although I finally lost interest and left it. Then the PCLinuxOS Fan Club group sort of fell in my lap and I was administrating that until I had to go to dial up.

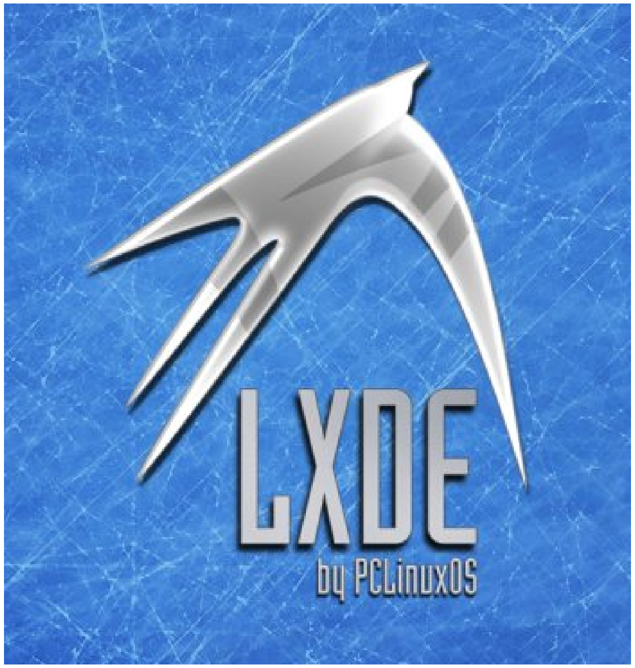
From the mid 80's to the early 90's I was a part of the Chattahoochee river rafting scene. I went every available weekend during the warm season and spent many enjoyable hours floating along as traffic raced across the bridges that crossed the river. It was the in thing to do back then and the river could be very crowded with rafts on the weekends. On Fridays, I would take the raft to work and would be on the river watching rush hour traffic go by.

Why and when did you start using Linux?
I probably got my first computer in 1984, an 8088 machine. It was really slow but subsequent machines got faster and faster. DOS was the operating system I used and I was able to do pretty well with it and eventually got online with it which opened up a new world. Windows followed and I went with the flow but realized their business practices did not conform to what I thought was ethical. I finally got fed up. I had heard of Linux and it seemed like the only viable alternative. I don't

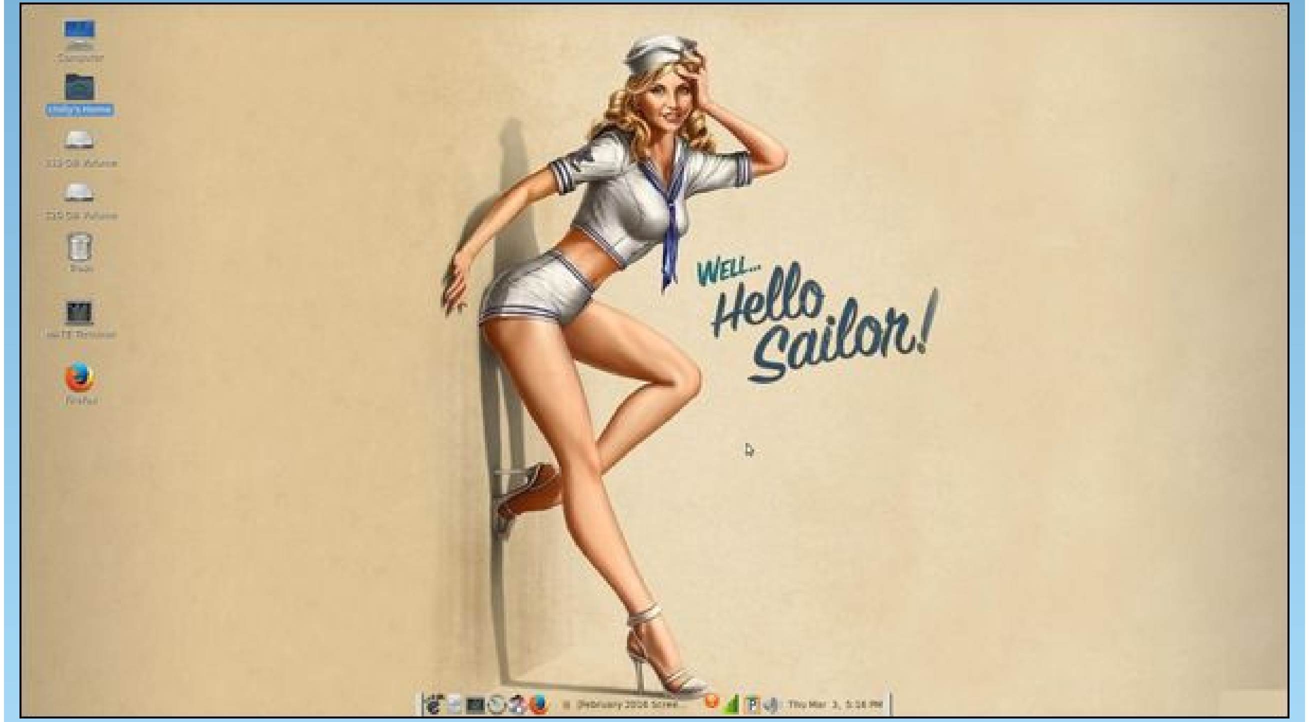
recall the exact year, maybe 7 or 8 years ago. I quickly found Ubuntu and about as quickly found I didn't like it. I tried a few others. When I got to PCLinuxOS, I found what I wanted and have been with it pretty much ever since.

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, parnote or Meemaw in the PCLinuxOS forum expressing your interest.



Screenshot Showcase



Posted by chilly, March 3, 2016, running KDE.

Inkscape Tutorial: How To Create Melted Text

By Khadis

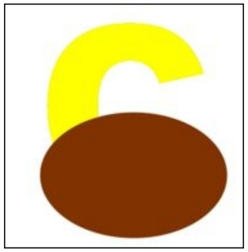
There are various nice text effects we can create manually in Inkscape. You can create scattered effect, bubble effect, 3D effect, etc. In this article, I want to show you a simple technique to create a melted text effect. It might be suitable to be put in a food package :)

Here we go!

* Create a text. I choose to type “Cokelat”, that means “chocolate” with yellow as the fill color. For this text, I simply use Arial Black 180 pt.

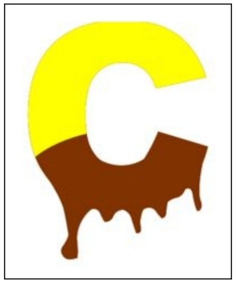
* Duplicate the text (**Ctrl + D**) and convert it into path from **Path – Object to Path** menu (**Shift + Ctrl + C**). Un-group this duplicated text (**Ctrl + Shift + G**). This action will break the text into single letters.

* Create an ellipse above each letter, started from letter “C”.

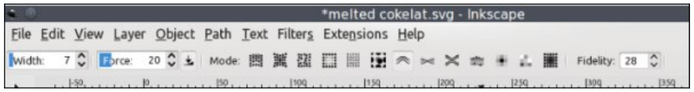


* Do the division operation. Click the letter, hold your Shift button, then click the ellipse. Go to **Path – Division**. Click outside your choices, then select the bottom part of the letter to see the division. Give it brown as the fill color.

* Modify the new modified ellipse using Tweaking tool (**Shift + F2**) by clicking and dragging the bottom part of the ellipse several times in different spots.



* For the tweaking setting, I use **Width = 7, Force = 20, and Fidelity = 28**. The selected mode is “Push parts of paths in any direction”. Your setting could be different, depending on the font size.



*melted cokelat.svg - Inkscape

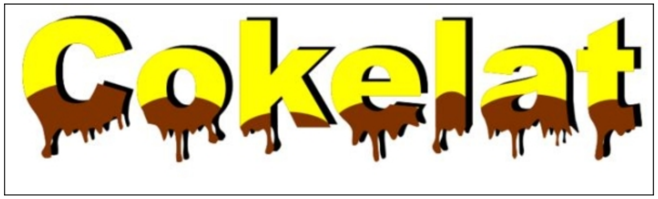
File Edit View Layer Object Path Text Filters Extensions Help

Width: 7 Force: 20 Mode: Fidelity: 28

* Do the same steps for other letters.

* You can add a 3D effect to the text by grouping all objects, then duplicate the group and color it with black. Then, send it to back by pressing Page Down button. Place it little bit higher or lower than the main “Cokelat” text (depends on your preference). And also move it little bit to right or left.

Your final result might be similar to this:



Playing Eldevin In PCLinuxOS

by Alessandro Ebersol (Agent Smith)

Eldevin is an award winning MMORPG (Massively Multiplayer Online Role Playing Game) indie free to play game from Hunted Cow Studios. Join thousands of other players, explore the mystical land of Eldevin, with over 160 kingdoms, each inhabited by unique creatures and characters to interact.

Explore vast plains or descend into underground caves and hidden dungeons, make friends or enemies of various factions in an epic quest to defend the kingdom of Eldevin.

The story

The kingdom of Eldevin, for generations, has been a green and peaceful land. That all changed ten years ago with the discovery of the Elemental Spheres. It was thought that they were mere legend, but these powerful magical artifacts had an immediate effect on the kingdom, plunging it into confusion and chaos.

The royal family decreed that the Spheres should be scattered to the four corners of the world in order to not cause more destruction. It was too late. The presence of the Spheres corrupted their guardians. Now Tristan, ruler of the Infernal Empire, plans to conquer the spheres. Only the Kingdom of Eldevin is in its way.

With this epic story begins Eldevin, a wonderful RPG game, F2P, from the company above, Hunted Cow.

You start the game in a battle 10 years ago, when giant Orcs tried to steal the spheres and destroyed the kingdom of Eldevin. The battle was so intense, that it created an interdimensional vortex, sucking several soldiers into it, including you.

Now, magicians of the order of light are managing to rescue the exiled of the great battle, and so you reappear in the mystical tower, clothesless, without memory and not knowing who you are.

A very interesting point: the game has no defined classes. At first, you are a normal person, without many attributes. While developing your skill tree, you will start to learn more skills of one class than others, as you see fit. It is a very interesting feature, as it allows an immense flexibility when developing your character.

The classes

There are six classes:

* Warrior: (Melee Damage)
* Templar: (Tank) One who serves as a target and shield for his teammates
* Assassin: (Melee Damage) Master rapid attacks and attacks over time ..
* Ranger: (Ranged Damage) Specializing in archery.
* Mage: (Magic Damage) You can use powerful spells to attack.
* Prophet: (Healer) Heals party members with healing spells and resurrection.

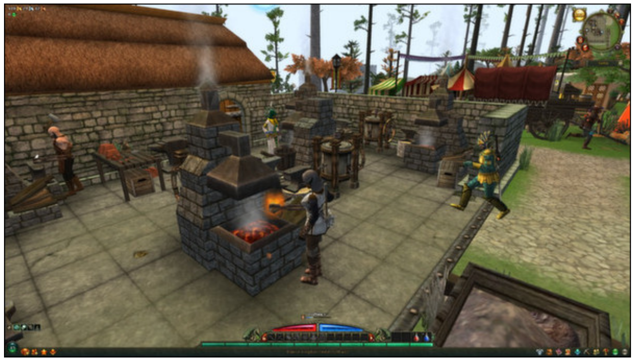
The professions

You will learn from 14 different professions (mining, metallurgy, woodworking, crafts, etc.) and be able to create your own weapons, armor, shields, rings and talismans. You will also learn to fish, cook, skin and tan the leather of slaughtered animals. It's really interesting.

My opinion

This is a very good game, immersive, rich with a whole society (of which the player becomes part) and, with full interaction. Not only the game changes depending on the outcome of quests, but also changes if some quests are ignored. Graphically, it is beautiful. The staff of Hunted Cow worked hard, creating a rich set of details. Sometimes it is interesting to play it just to wander through the vast plains, or go fishing in lakes, or take a stroll on Eldevin beaches.

Ahh, one more detail: The game represents the passage of time, there’s morning time, noon and nighttime. The weather, however, does not change.



Features

* Rich storyline involving hundreds of epic adventures.
* Huge world to explore, with many cities, areas, dungeons, and secrets.
* Six talent trees with more than 200 talents.
* Real-time combat system.
* Use strategy and tactics to defeat epic enemies and bosses.
* Enter PvP combat with your friends and enemies.
* Your decisions and actions will affect meetings and future possibilities.
* Classless system of combat; Eldevin players are free to learn more than 100 unique skills.
* Train in 14 professions to create your own weapons, armor, items and talismans.
* 16 general dungeons and dozens of small individual dungeons based on stories, both solo and in groups.
* Hundreds of items, including over 40 unique sets, to obtain and collect.
* Maximum level 45, to enjoy fantastic game content and consistent updates with seasonal events.

Requirements

* Updated Java virtual machine
* Computer capable of displaying OpenGL 2.1 graphics
* It works well even with Dual Core machines.

Sign in here:
https://www.huntedcow.com/auth/create?game=11

Tip Top Tips: Changing The GRUB Menu For ANY PCLinuxOS Media

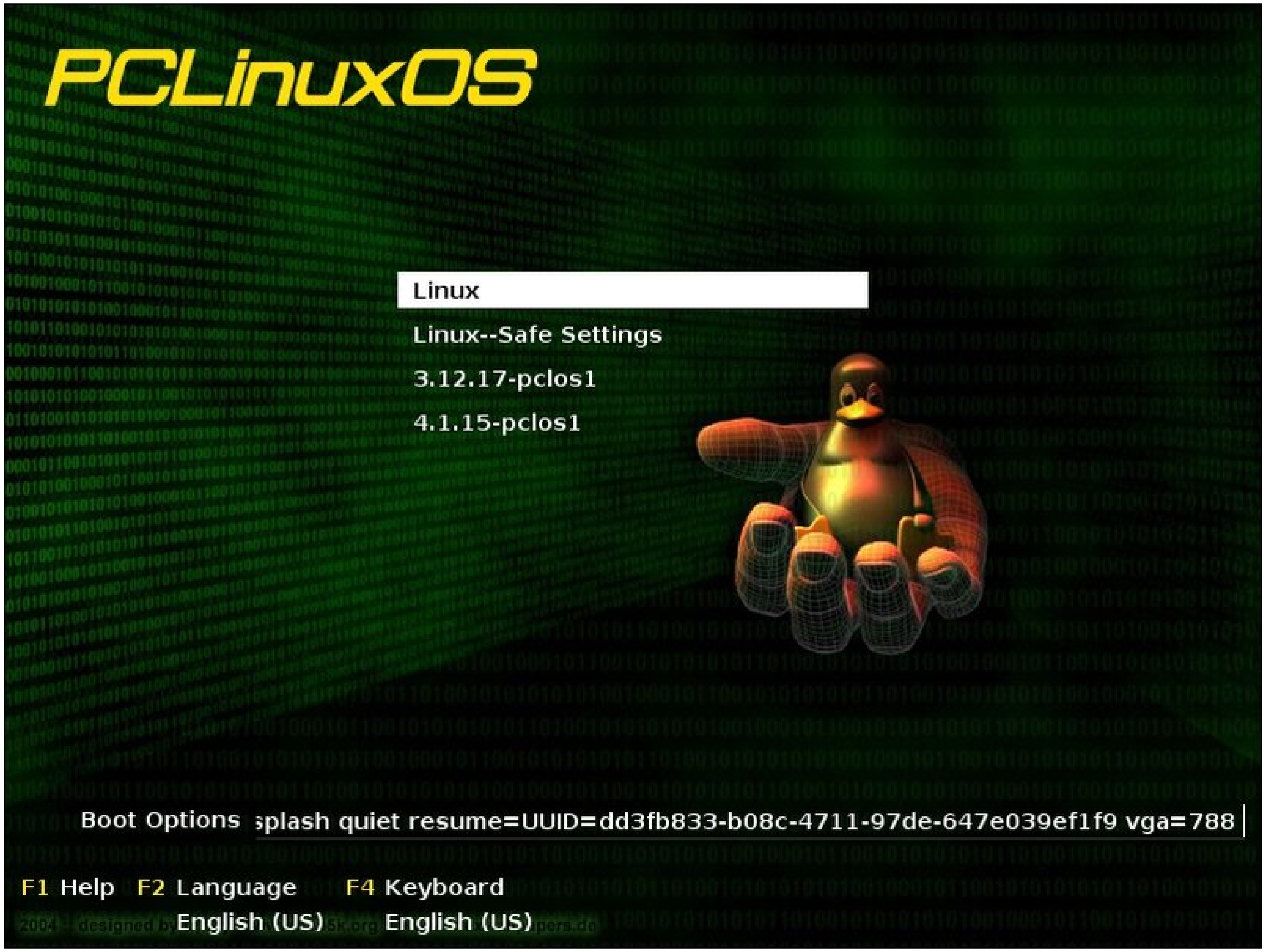
Editor’s Note: *Tip Top Tips is a new monthly column in The PCLinuxOS Magazine. Each month, we will feature – and possibly even expand upon – one tip from the PCLinuxOS forum. The magazine will not accept independent tip submissions specifically intended for inclusion in the Tip Top Tips column. Rather, if you have a tip, share it in the PCLinuxOS forum’s “Tips & Tricks” section. Your tip just may be selected for publication in The PCLinuxOS Magazine.*

This month’s tip comes from PCLinuxOS forum member **mr-roboto**.

If you've ever wanted a custom GRUB menu background for your customized PCLinuxOS media, especially for a USB flash, but couldn't find the info on doing it, look no further. I've made three new backgrounds, all of which have worked across more than ten trials and I look forward to others trying this quickie HOWTO, to get some feedback.

Before you start, choose a straightforward JPEG file, probably not a photo, for size reasons, but some illustration that suits your tastes. From my reading, which never had a truly authoritative source, an image should be no more than 150KB for this exercise. Your image must also have dimensions of 800x600, or it won't display correctly. The background graphic supplied by the PCLinuxOS developers is only 50KB.

Next, open a terminal window and make an empty working folder apart from your other documents and activities. You can name it anything you want and place it anywhere you'd like, but for the sake of these instructions, create and make current a subdirectory called **grubmenu** in your home directory, as shown below:



Boot Options splash quiet resume=UUID=dd3fb833-b08c-4711-97de-647e039ef1f9 vga=788

```
mkdir ~/grubmenu
cd ~/grubmenu
```

As some of the files are located in privileged areas, go superuser for the remainder of these instructions. The source archive file for the exercise is **/boot/gfxmenu**, which we will expand into our **grubmenu** working folder:

```
cpio -i </boot/gfxmenu
```

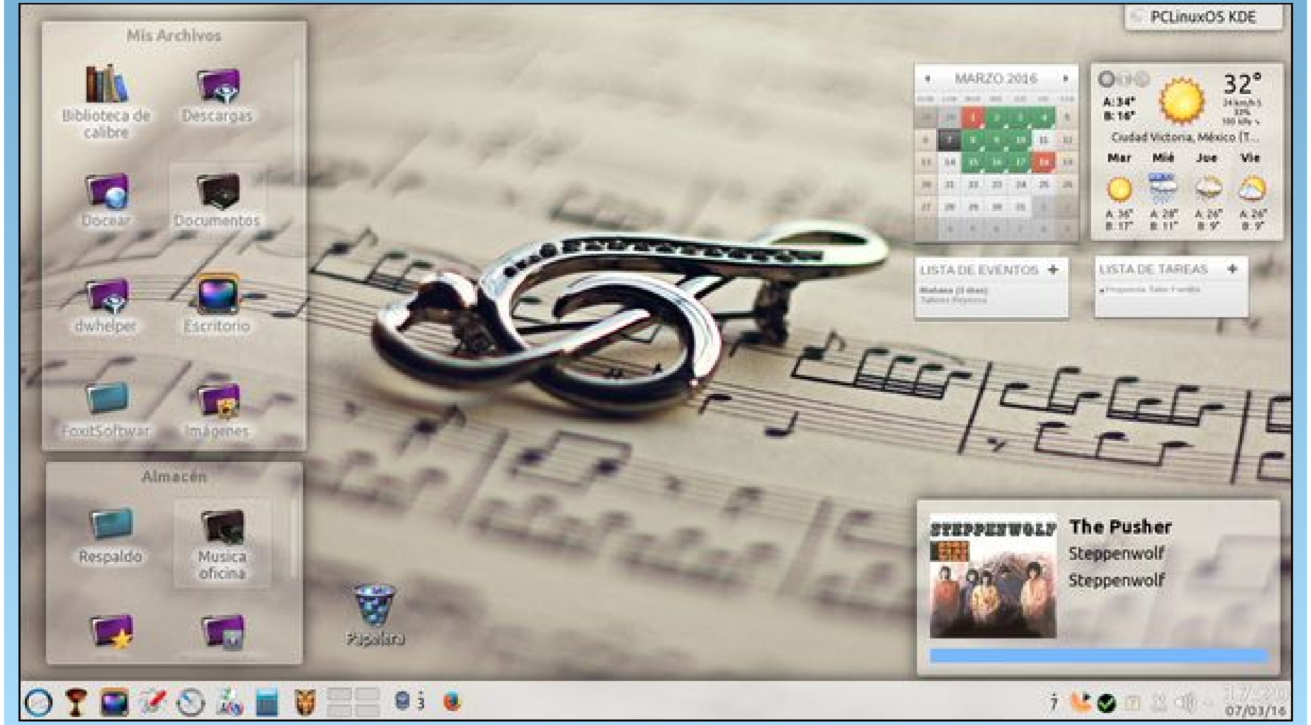
Replace **back.jpg** from the cpio archive you just dumped, with your new GRUB menu background graphic. That is, delete the existing **back.jpg** and replace it with your JPEG called **back.jpg**. Next, backup the old archive and create a new one containing your new graphic, like so:

```
cp /boot/gfxmenu /boot/gfxmenu.orig
ls | cpio -o >/boot/gfxmenu
```

Now, reboot your media at your first opportunity and see your new GRUB menu background. It's that simple. I did have one hiccup playing with the privilege mask once. I fixed a graphic that didn't want to display, using a 0644 mask and all was well. Included (previous page) is a sample of one my successful experiments.

Finally, I wanted all of my remastered live media to have this menu background, so I changed **/boot/gfxmenu** on my development machine prior to my media remaster. In fact, I held up the job all day yesterday, until I figured out what I just presented above. Actually, I worked on it recently and started the script to generate a new ISO, just before going to sleep. When I awoke, I copied the new ISO, and made ready to test it in a virtual machine. What did I see ? Our colleague and PCLinuxOS's master maintainer **Texstar** has switched the live media's boot manager to SYSLINUX/ISOLINUX! Anyway, you might still find this handy, at some point. You might also find my HOWTO more direct than this link, which was helpful, but as I said less direct. If it isn't, your feedback is welcome.

Screenshot Showcase



Posted by Crow, March 7, 2016, running KDE.

Testimonial: I Always Stay Close To PCLinuxOS

by everstart

Sometimes you see applications that because perhaps the author is associated with, or more familiar with, another distribution, you are drawn to it imagining it might be best at doing that really neat thing being described.

But it doesn't take long, not even hours, before I head into the relative sanity of the PCLinuxOS environment, and may I say culture.

It blows my mind (a little) that every distro does not have interchangeable fstab configurations. The form and function is particular to the distribution. It seems obvious but sometimes it's tempting to copy-paste what works for one distro, but which you know really is a “gamble at a casino”, meaning you're gonna lose.

I am not learning Linux just as a hobbyist and yet I am, so I don't have to defend what may sound condescending to hobbyists – we are all serious about this. I think my special twist is that I mostly stopped advancing in CSC after the 90’s, and now two decades later, I am that far behind. It means I have to get priority and perspective and be serious about advancing in ability to administrate what I need and learning things that can wait for later.

It has been and is like a giant jigsaw puzzle, but part if not all of the whole picture is not there. It comes together – learning some here and there, finding out days or weeks later that it's good you picked up that bit, because you've come upon at least one reason you needed to know which way to go, and you did know. Still for me, the puzzle has lots of holes.

I have been working with the fstab and wow, is it important. I have had help from forum members with great detail made for me at great pains, and I have printed them out. I am now printing them out again, as they are so marked up with colored pen, I need fresh copies. Members have pointed me to links, told me the one book I must read. It's all very good and really perfect, but I am not perfect, and I don't have the time that a disciplined, diligent, on the ball person has.

I see the BSD work, which is admirable and top notch, but at the same time, I think it's important to realize that a NAS by whatever name can be well implemented with software such as ownCloud and Unison and sync from the Synaptic repo, and by learning it at that level, as they say, 'you own it.'

Yes, I have looked through other repositories and they are very lofty. But when I look through the PCLinuxOS repo, I am just as overwhelmed by what is really amazing. If this had existed when I was in 9th grade, well over 2 decades ago, then I would loved it and never thought anything of it because it was just there. But it wasn't always like this. Many of you know how far – how far we were from where we are now and most of us couldn't imagine anything like all this.

When I went to college, I could program and well. But we never opened a computer box, we never spoke of Unix, but we did have a class on operating systems. The closest I came was hacking terrible code at the technical college on a burroughs mainframe/mini. It was so cold in there you had to wear 10 layers, and the box sat on top of the air conditioner blowing into it. It was the size of two washing machines – big ones. All we did was COBOL, and I did that while a high school senior, as they let me sign up for that class at the tech college.

I want to do it on my own. I want to find the answers. But it isn't possible. I see the hardware, I know what it can do, I just can't yet put it together and anticipate what the Orico box that runs the 4TB NAS drive. I use it because I don't think the workstation T1600 board will support that large of a drive, and we are Linux, so the support is for Windows or Mac. We have only our own to lean on and within that, the varied distros sometimes competing for attention, and they are not compatible to the level necessary. Even the damn syntax changes among the fstab implementation. I have it connected via USB3 (it's faster) or esata. It hangs. I chip away and correct, but I am really in a hurry, but not just for the sake of rushing. I need to gain the skills and I am just me – late, behind, and there are so many puzzle pieces.

Anyway, PCLinuxOS is not a baby step. It is a real, full size, exceedingly capable, liberal distribution. It's no mistake I came to it and stick with it.

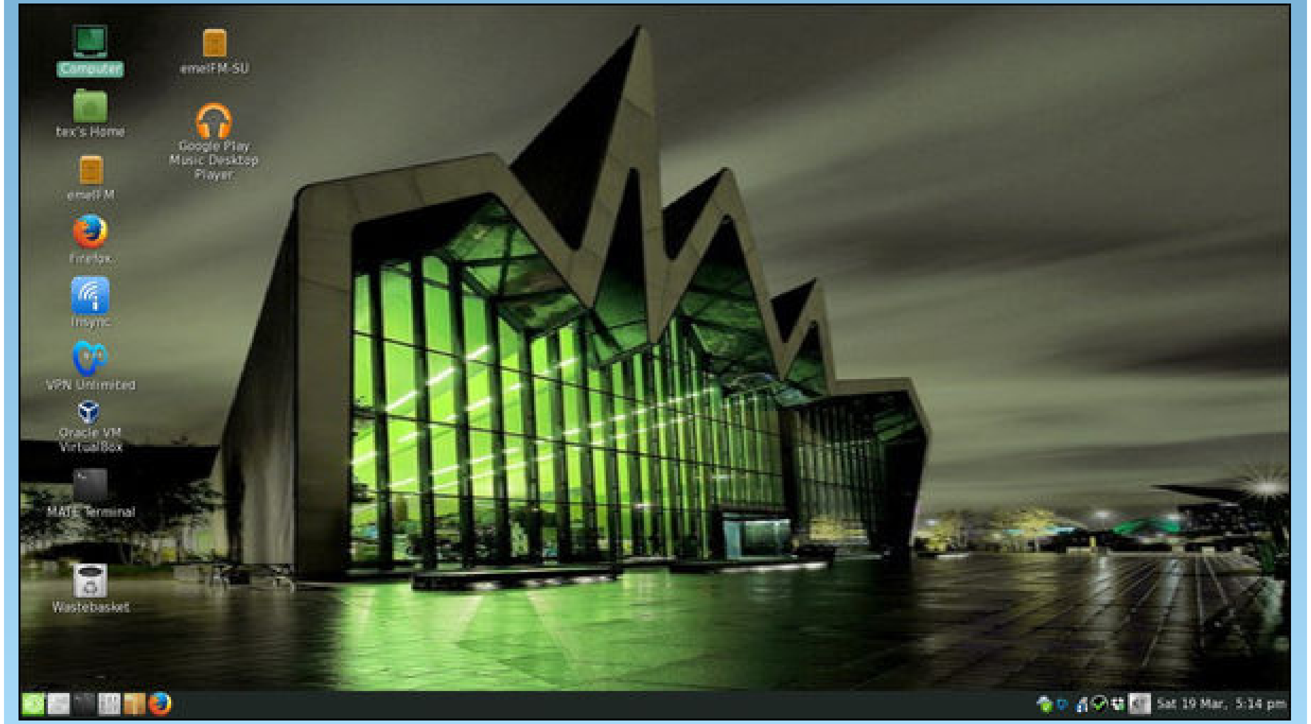
To you, it is so easy; you see the whole picture. I see more and maybe right around the corner I'll see enough. I admit it is late, but I believe it is not too late to catch up to where I need to be.

I can't make this into a testimonial, altogether now, but I believe a little longer with PCLinuxOS tunnel vision, I will get where I'm going. Believe me, I have learned a lot. This is a good place. It is a noble thing that has happened in 20 years, like the grand experiment of limited democracy and escaping the tyranny of kings and all tyrannies that might try to take their place. It is open source, free, unthinkable and unheard of back in the IBM cloning, Xerox, Palo Alto Park, walking away from the 'mouse' and windowing OS.

The best I can do is say thank you to all that have chosen to help me out (so sappy but so true).

Keep being good, resist tyranny.

Screenshot Showcase



Posted by Texstar, March 29, 2016, running Mate.

PCLinuxOS Puzzled Partitions

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

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 a 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!

Download Puzzle Solutions Here

X	E	T	U	R	E	T
8	1	1	1	1	1	1

_ _ _ _ _ _ _

T	E	S	R	N	I	P
1	1	1	1	1	1	3

_ _ _ _ _ _ _

Double Word

H	U	K	Z	E	C	C
4	1	5	10	1	3	3

_ _ _ _ _ _ _

Triple Word

O	L	O	T	R	I	N
1	1	1	1	1	1	1

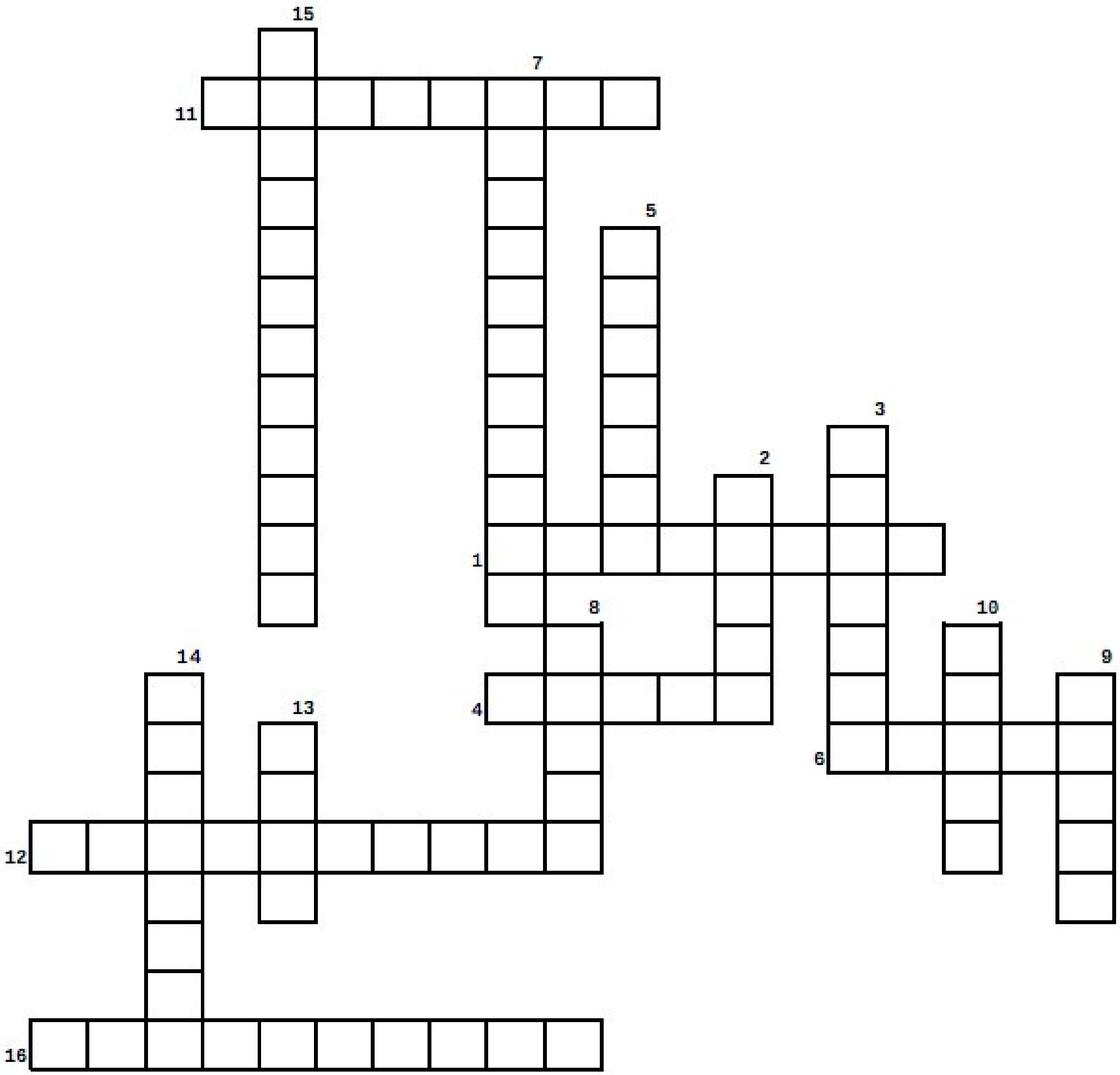
_ _ _ _ _ _ _

O	T	L	S	C	E	H
1	1	1	1	3	1	4

_ _ _ _ _ _ _

Possible score 246, average score 172.

PCLinuxOS Crossword Puzzle: April 2016 Agriculture



1. animal caretakers
2. the main ingredient in many loaves of bread
3. tillers of the soil
4. apples and oranges
5. the gradual destruction of something by natural forces
6. pig
7. the practice of growing crops or raising animals
8. many are nice and shady in the summer
9. a great way to season your food
10. products made from milk
11. a very versatile plant whose beans can be used for many things
12. beautiful flowers and seeds to snack on
13. another name is sorghum
14. placing seed into the ground to grow a crop
15. saving the natural resources
16. a very healthy part of your diet

Download Puzzle Solutions Here

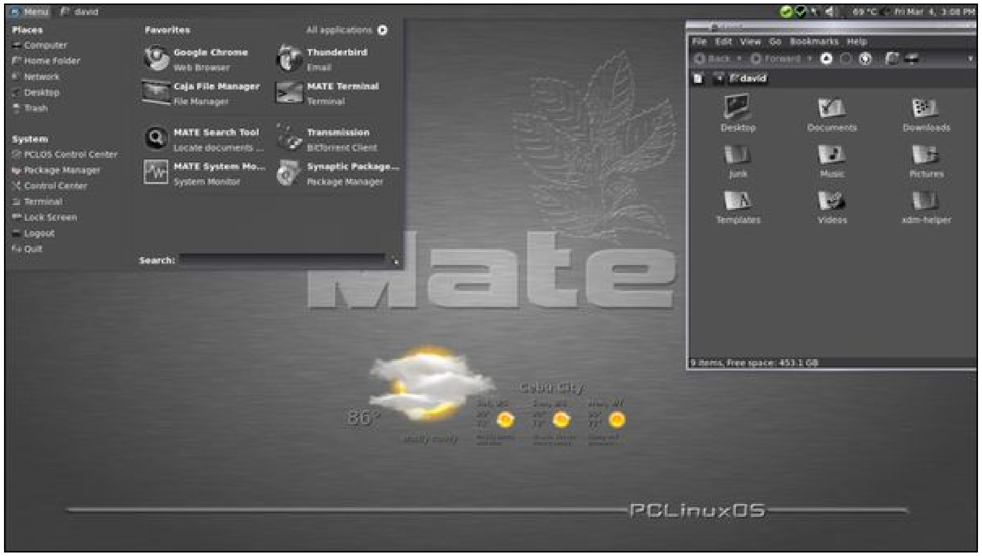
Agriculture Word Find

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

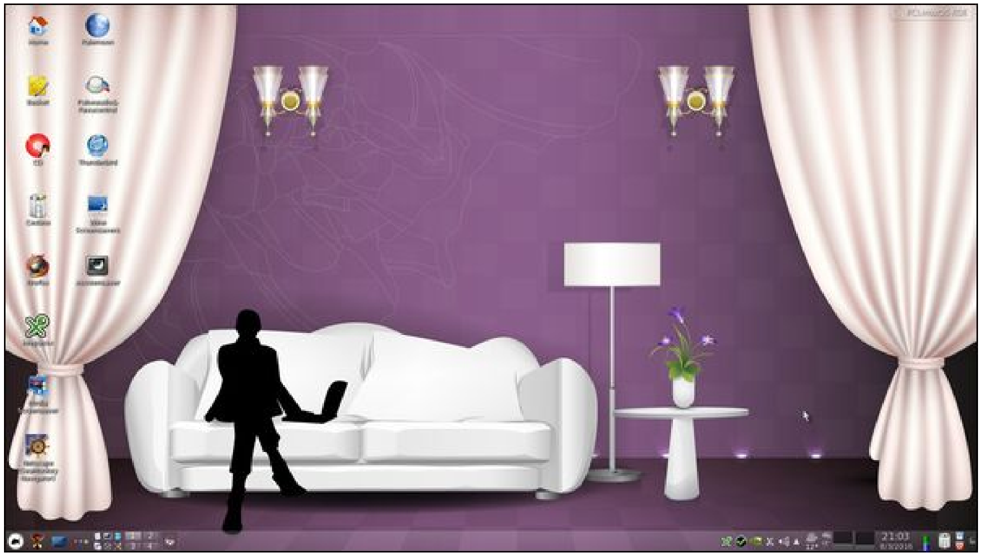
Agriculture
Cattle
Conservation
Corn
Dairy
Erosion
Farmers
Fruit
Gardeners
Goats
Herbs
Horses
Milo
Planting
Ranchers
Sheep
Soil
Sorghum
Soybeans
Sunflowers
Swine
Trees
Vegetables
Wheat
Wildlife

Download Puzzle Solutions Here

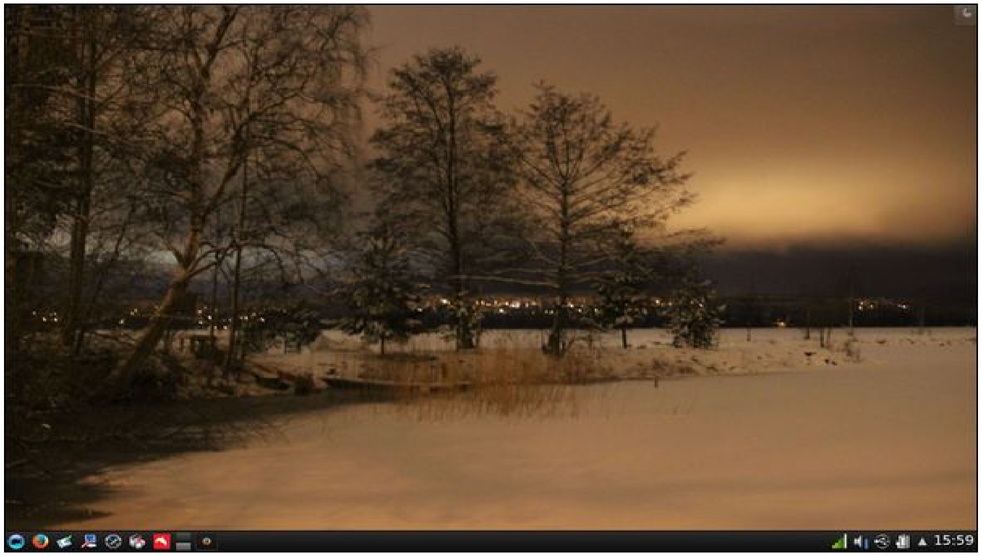
More Screenshot Showcase



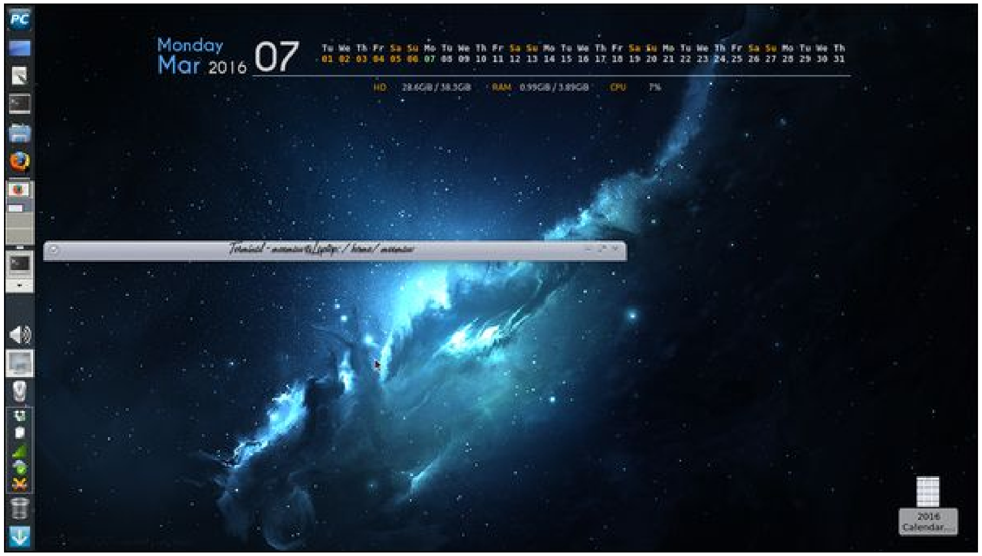
Posted by daspicer, March 4, 2016, running Mate.



Posted by francesco bat, March 8, 2016, running KDE.



Posted by luikki, March 3, 2016, running KDE.



Posted by Meemaw, March 7, 2016, running Xfce.