The PCLinuxOS magazine

Volume 208 May, 2024

# Inside 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 https://pclosmag.com.

This release was made possible by the following volunteers:

**Chief Editor**: Paul Arnote (parnote)

**Assistant Editor**: Meemaw

**Artwork**: Paul Arnote, Meemaw

**PDF Layout**: Paul Arnote, Meemaw

**HTML Layout**: tbs, horusfalcon

**Staff**:

YouCanToo David Pardue

Alessandro Ebersol

**Contributors**:

# From The Chief Editor's Desk

You might have noticed over the past couple of months that the file size of the magazine's PDF has shrunk a bit. This was intentional. And, that ability to "shrink" the size of the PDF for download from the magazine site is a direct result of some new abilities of Scribus.

"We" use Scribus to create the magazine PDF every month. The newest version of Scribus now (finally!) allows the use of WebP graphics. So, when Meemaw and I create the PDF every month, we have been converting as many of the article images to WebP graphic files. For what it's worth, the ad images are still an eclectic mix of JPG and PNG files.

If you're not familiar with WebP graphics, I'll refer you to this article I wrote in the April 2022 issue of The PCLinuxOS Magazine. All of your major web browsers can now display and use WebP graphics. That means that your web pages can use larger graphics that have smaller file sizes, which means that your web pages load faster. Torsten Schommer, who has taken over the role of laying out the magazine's HTML edition, has also switched to using WebP graphics, whenever and wherever possible (with the exception of the ads).

The file size savings have been astonishing and surprising. We/I always knew that the graphic files were one of the things that contributed to the final size of the PDF generated by Scribus … in a huge way. Some of the WebP graphic files literally are less than half the size of the comparable JPG and PNG files that we used to use. That. Is. Significant.

To be perfectly honest, I was hoping to only shave off one or two MB off of the file size of the final PDF created by Scribus. I *never* expected to see the file size savings that we experienced. For example, for the ***full size*** issue in April to come in at 4.2 MB completely caught me off guard.

*Me and Lexi dyeing Easter eggs*

Over the past 15 years or so of laying out the magazine, I've gotten pretty good at estimating the size of the PDF before it has been laid out. But those estimates were based on the "old" Scribus, coupled with the "tricks" we used to try to keep the final size of the PDF as small as possible for download. All of those estimates are now "out the window," as the new Scribus (with its ability to use WebP graphics) has consistently produced far smaller PDF files than we've ever been able to produce.

By my estimation (and I'm usually pretty close), the April 2024 issue of The PCLinuxOS *should* have been between 8.5 MB and 9.0 MB in file size … using the "old" Scribus. I was EXTREMELY surprised when the final file size of the April PDF came out at 4.2 MB. I was so shocked that I compiled it again, with the exact same results. My surprise turned to elation when I opened up the PDF, and everything was there and functioning as perfectly well as it ever had. Getting the file size of the final PDF down to 4.2 MB was **completely** unexpected, albeit welcomed.

To be perfectly honest, I'm not entirely happy with the changes that the Scribus developers made in the "new" Scribus. Many seem

arbitrary, as if they changed things around "just because they can." And 14+ years of doing it one way are suddenly "upset" because of those seemingly whimsical changes. We've adapted to those changes, begrudgingly. We have no choice but to adapt. But with the most recent iteration of Scribus, I can ***almost*** overlook those niggles, trading them for the remarkably and significantly smaller file sizes.

The file size of the final PDF is very important to me. I've noticed over the years that the more we exceed 10 MB in file size for the final PDF, we have fewer downloads of that PDF. Certainly, this magazine is a great vehicle for communicating with and informing PCLinuxOS users. But I also know that "other people" other than PCLinuxOS users also read the magazine. In that capacity, this magazine also helps "spread the word" about PCLinuxOS. So, the more we can constrain the file size, the more downloads we have, and the more we help spread the word about PCLinuxOS.

We hope that you find the smaller PDF file sizes of The PCLinuxOS Magazine a welcome change. I know we like them … a lot!

**********

This month's cover is based on popular characters from Frank L. Baum's "The Wonderful Wizard of Oz" (its original title). But, in a twist, the characters are all penguins, paying homage to Tux, the Linux mascot. Why Baum? Because he was born on May 15, 1856. This year is the 159th anniversary of his birth. The cover image was created with the Bing AI image creation engine. From left to right in the cover image is the Tin Man, the Scarecrow, Dorothy Gale, the Cowardly Lion, and the Wizard of Oz.

"The Wonderful Wizard of Oz" was first published in 1900, to critical acclaim. The book was the best-selling children's book for two years after its initial publication. Before his death in 1919 from a stroke, Baum wrote a total of 13 novels based on his Oz characters. The last two books of the 13 novels were published after his untimely death at age 62. You can read more about Baum's life here.

**********

Until next month, I bid you peace, happiness, serenity, prosperity, and continued good health!



## 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.

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 UsersA 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.

# PCLinuxOS Debian Edition

**by David Pardue (kalwisti)**

This month's article will highlight the efforts of the PCLinuxOS Debian Project. PCLinuxOS Debian Edition is a variant of PCLinuxOS which is based on the Debian 12 (codename "Bookworm") release, using the Debian Stable repositories as a base with additional software created by the PCLinuxOS community. Another notable feature is the lack of systemd. PCLinuxOS Debian does not allow packages that have hard dependencies on systemd to enter your system.

The project had its genesis about three years ago. It was based on the unstable branch of Devuan and Texstar was involved at first. (He created a series of experimental "Devuan Darkstar" ISOs from December 2021 through January 2022. You can read forum posts detailing its progress in this thread.) However, he had to step aside due to his responsibility for mainline PCLinuxOS and the developers' focus shifted to become a PCLinuxOS / Debian project.

The PCLinuxOS Debian Project is spearheaded by longtime community member Upgreyed, with assistance from tbs (Torsten). Upgreyed has prior experience with PCLinuxOS remasters. He created the first live GNOME .iso in 2005 - 2006, and he led the PCLinuxOS GNOME project until 2010 with the help of two other community members. (By the way, I would like to thank Upgreyed for kindly providing information on the PCLinuxOS Debian Project via e-mail.) Torsten (tbs) has been involved with PCLinuxOS since 2008; he has a background in IT, with significant experience as a systems


analyst and database developer.

Upgreyed has created live ISOs for 64-bit PCs with the following desktop environments: MATE, Xfce, Cinnamon and Budgie. Torsten creates the KDE Plasma and Plasma Mini ISOs. Upgreyed does not plan on offering additional DE releases – such as LXQt or Trinity – because he already has more than enough to keep up with. The ISOs are updated every few days and are date-stamped, so you should not be faced with large updates after a fresh installation.

### Advantages of the Debian Base

Before discussing some of the unique features of PCLinuxOS Debian Edition, we should mention the advantages of such a variant. First, Debian Stable provides a legendary, rock-solid base for PCLinuxOS. Second, Debian's massive software repository relieves Texstar and his small team of helpers from having to package all of the .RPMs that currently go into the repository. Torsten noted that the effort required to ensure that Debian-based flavors of PCLinuxOS remain free of systemd, and to maintain some additional PCLinuxOS-specific packages to make life easier for users, would be far less than the current workload required to keep PCLinuxOS running smoothly. Another factor to consider is the daunting challenges involved with the migration to Qt 6 and KDE Plasma 6.0, then continuing Python updates – this will require recompiling many additional dependent apps.

I installed the PCLinuxOS Debian variants in VirtualBox and have been using them daily for the past couple of weeks. From my perspective as an average PCLinuxOS user, I have not noticed jarring changes due to the OS being .deb-based (rather than .RPM-based). Once I began using them, I was hard-pressed to say that I was not running “regular” PCLinuxOS. As Upgreyed mentioned, it is the same software – albeit a bit older due to Debian Stable's conservatism – just packaged differently. The desktop environments are the same, and you may customize them to suit your needs.

### Unique Features of PCLinuxOS Debian

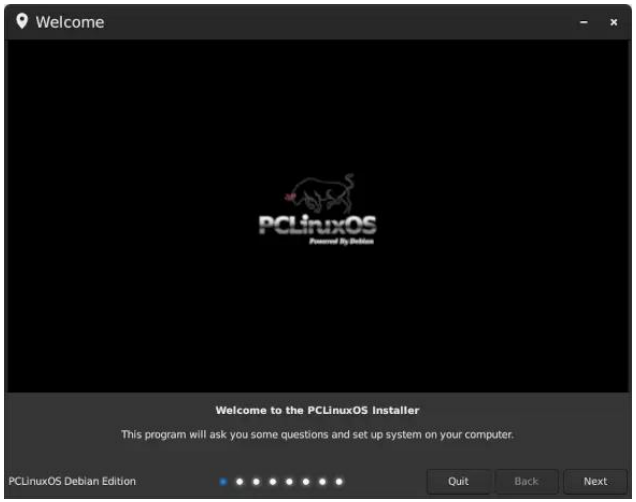
PCLinuxOS Debian is proudly systemd-free. In response to my question about the difficulty of blocking/eliminating systemd elements, Upgreyed wrote that “Not much effort was involved – just some SysVinit packages and pinning out systemd packages. Not much more was required to get around systemd. If I want a systemd-specific package, then I patch and rebuild it for SysVinit.”

PCLinuxOS Debian ships with a more recent kernel than Debian Bookworm's: 6.6.8 (an LTS

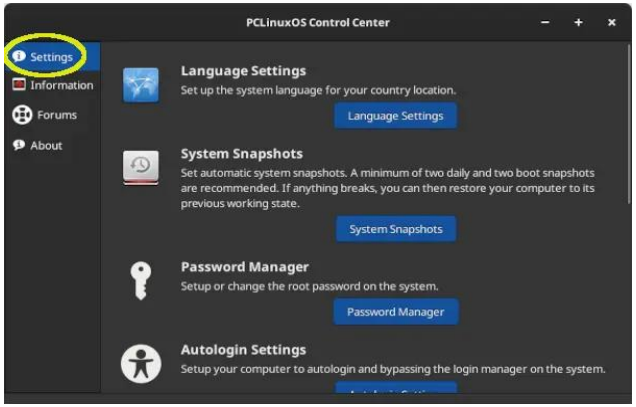
kernel with a projected EOL of December 2026). However, if your hardware requires an older kernel, you can install version 6.1.0-20 [i.e., 6.1.85] from the Debian repository via Synaptic.

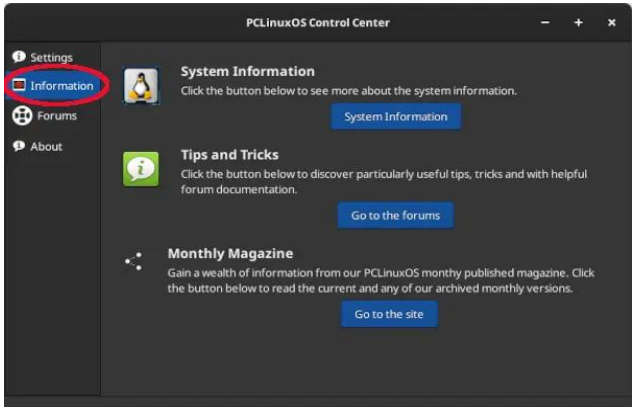
Inspecting the /etc/apt/sources.list file will show that its contents are almost identical to a default Debian Bookworm file – except for the special PCLinuxOS repository maintained by Upgreyed.

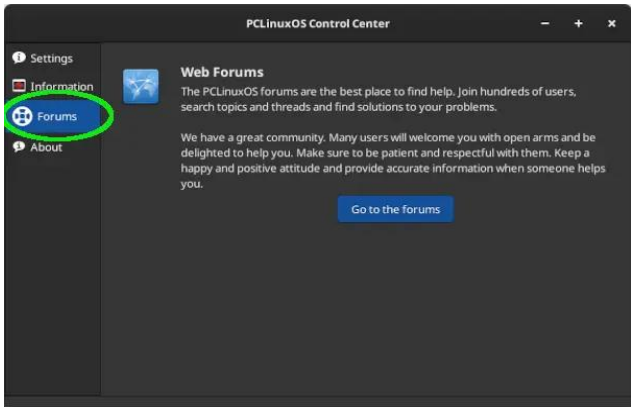

PCLinuxOS Debian uses the new "mylive-install" installer, which became standard with PCLinuxOS ISOs beginning in July 2023. If you are unfamiliar with it and would like an overview, you can read this article in our community magazine and/or consult this thread in the PCLinuxOS Forum.




The PCLinuxOS Control Center (PCC) received a major overhaul in the PCLinuxOS Debian Edition. The three screenshots below give an idea of the functionality which Upgreyed includes in this application:

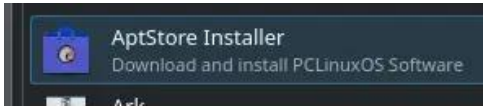


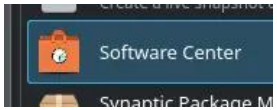



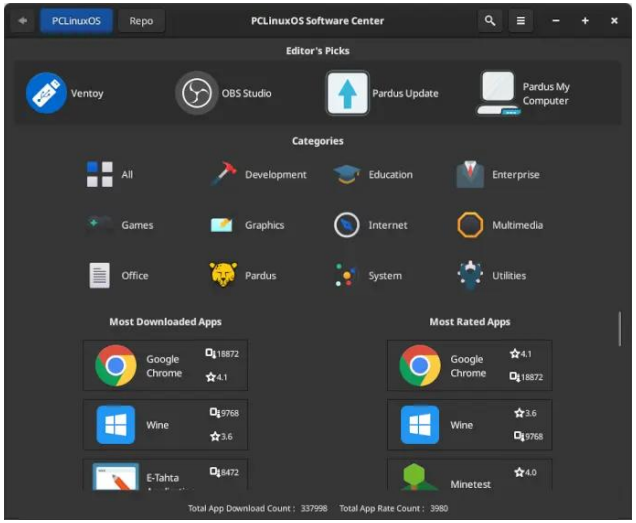

Another unique application is the PCLinuxOS Software Center, and that is an adaptation of the Pardus Software Center which Upgreyed borrowed from Pardus Linux (a Debian-based distribution from Turkey, known for its polished implementation of GNOME). This app functions similarly to Linux Mint's Software Manager or GNOME Software.

You can install the PCLinuxOS Software Center via a simple utility called the AptStore Installer.




After running the installer, the Software Center will appear as an entry under the System (or System Tools) menu.



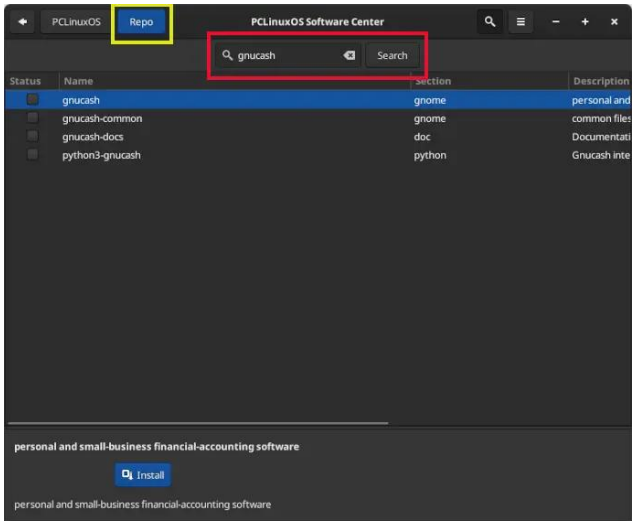




Upgreyed advises users to be patient while the Software Center is initializing; it might take a

minute or longer to start because it is a large app which pulls in many dependencies.

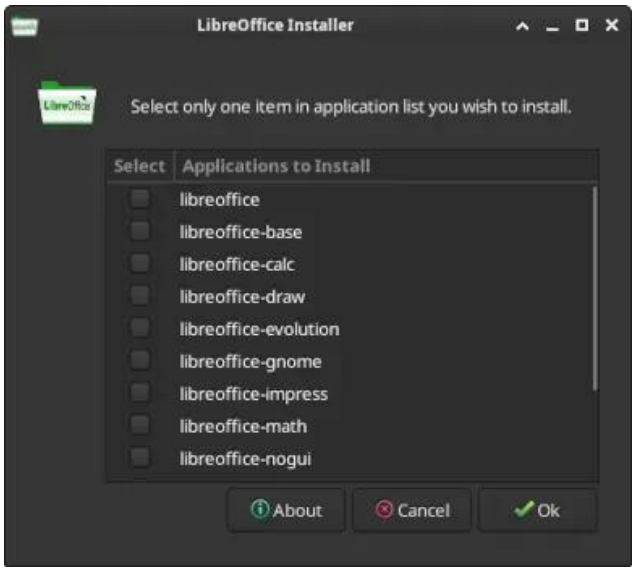
The Software Center is not the only method of installing software in PCLinuxOS Debian. You may also use Synaptic or the traditional apt utility from the Terminal. Based on my testing, the Software Center performed well.

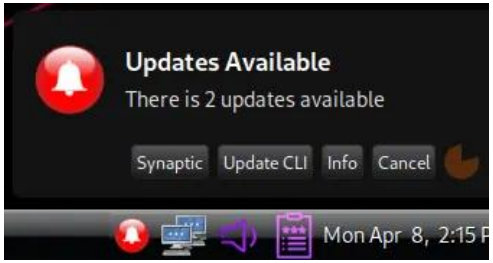
The "boutique" portion of the Software Center does not list every program available in the repositories – only the most popular software. For example, GnuCash does not appear in the Office category. If you do not find your program in the boutique, click on the **Repo** tab and search for the program there.

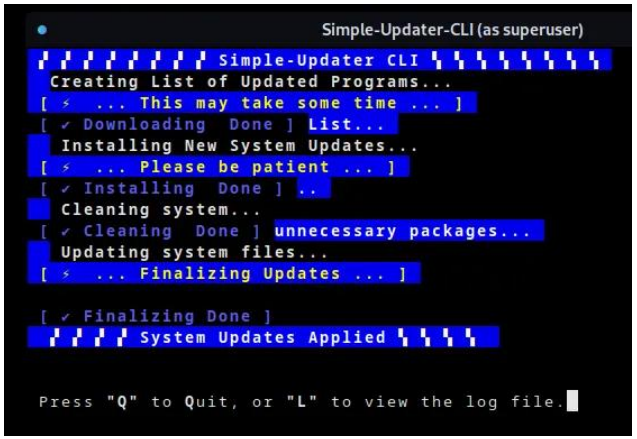



Upgreyed created a LibreOffice Installer utility which is similar to pinoc's LibreOffice Manager (lomanager). (center, top)

Other utilities included are a *printer-installer* and Simple Update Notifier. I appreciate one of the Notifier's options: the ability to update the system via CLI. With a single click, a TUI is invoked; after the update finishes, you can view the log file of the changes that were applied.




All of the PCLinuxOS Debian releases ship with the Mercury browser – a compiler optimized, private Firefox fork. Upgreyed wrote that although he was a longtime user of Firefox, he switched to Mercury because it works without the issues that he was experiencing with Firefox. (If you prefer Firefox, you can easily install Firefox ESR [Extended Support Release] from Debian's repository.)

Upgreyed is the author of several other GUI applications which put a "PCLinuxOS twist" on Debian Bookworm:

- Click Radio – A lightweight and simple GUI interface media app
- CopyCat – Allows you to boot most Debian-based ISOs with persistence and to save changes to USB key
- ddCopy – Creates a bootable Live USB from .iso image
- inxi GUI – Displays system information [package name inxi-gui]
- Installed Info – Gives a list of installed packages on your system [package name installed-info]
- Grub2Splash – Simple Grub2 and Plymouth image changer
- GimpSplasher – Change the GIMP's splash screen
- MATE Random Background
- Speedtest – Runs Speedtest by Ookla without having to open a web browser or use the command line
- Snapshot Tool – Creates a Live CD from your running system
- Change Hostname – Easily change your PC's hostname [package name chghostname]
- Change Root Password – Prompts you to change the root password immediately after first login [package name chpassroot]
- Xrandr GUI – Changes desktop screen resolutions [package name xrandr-gui]

Flatpak is not installed by default in PCLinuxOS Debian (nor in Debian Bookworm). However, you can enable Flatpak support by following the simple Bookworm-specific instructions here.

## Individual Releases

Based on my VirtualBox experiments, all PCLinuxOS Debian releases performed reliably. I updated them daily using Synaptic or the command line (*# apt update && apt upgrade*). I successfully installed additional software via Synaptic, the new PCLinuxOS Software Center and/or the CLI (*# apt install package-name*).

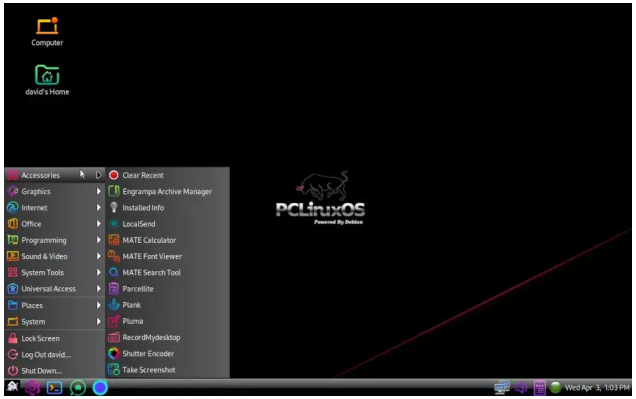
Within PCLOS Debian Cinnamon, I installed a Flatpak without any trouble and verified that it works normally. I also tried customizing the DEs' appearance and briefly experimented with changing the system language / locale.

## MATE

- Kernel 6.6.8
- MATE version 1.26.0
  [The most recent version is 1.28.2.]
- LibreOffice 7.4.7.2

This might be considered the flagship release of PCLinuxOS Debian (my personal opinion, not Upgreyed's). Upgreyed describes himself as a die-hard MATE fan. It is his daily driver, so he has curated a selection of programs and utilities well suited to this desktop environment.

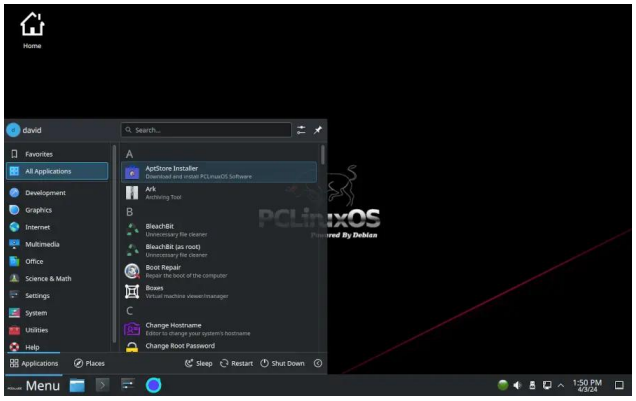
The MATE Edition is visually distinctive due to its use of the neon BeautyLine icon theme. You can further customize the appearance with Plank and/or MATE Tweak (which are installed by default). (center, top)



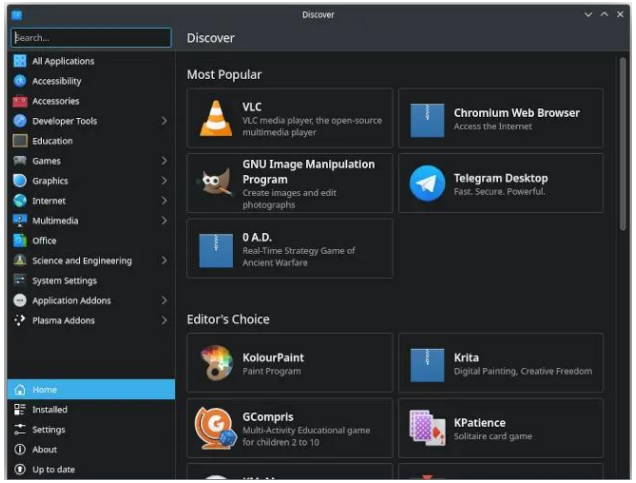
## KDE Plasma

- Kernel 6.6.8
- Plasma version 5.27.5 (LTS)
  [The most recent version is 6.0.3.]
- LibreOffice 7.4.7.2

As mentioned earlier, tbs creates the KDE Plasma and Plasma Mini ISOs. The KDE Plasma Edition includes a nice assortment of programs and utilities which will serve your computing needs.

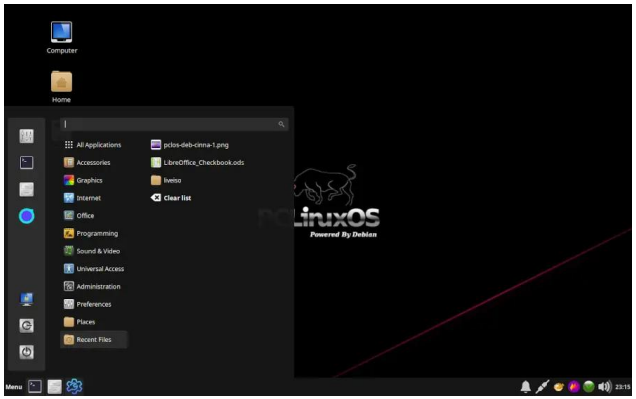


Discover Software Center is also available. This provides users with yet another option for installing software in KDE Plasma. However, Discover is more like an app store than a simple package manager; it is intended for installing programs that have a GUI – not CLI programs or random packages. (In addition, please be aware that Discover cannot install packages from Upgreyed's PCLinuxOS-specific repository.) (top, right)




## Cinnamon

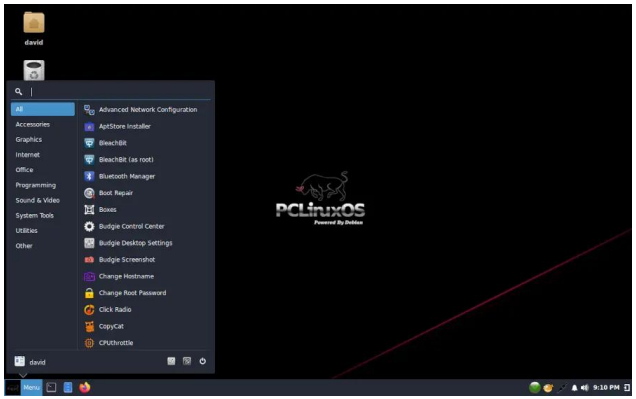
- Kernel 6.6.8
- Cinnamon version 5.6.8
  [The most recent version is 6.0.4.]
- LibreOffice 7.4.7.2



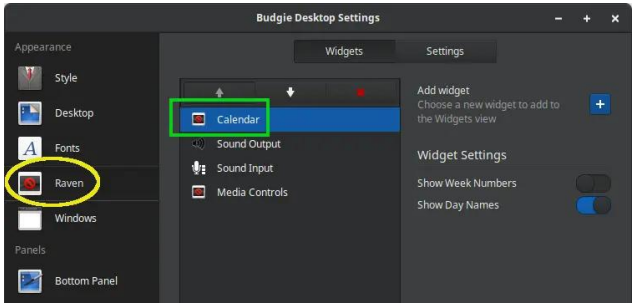
## Budgie

- Kernel 6.6.8
- Budgie version 10.7.1
  [The most recent version is 10.9.1.]
- LibreOffice 7.4.7.2

I was unfamiliar with Budgie, so I devoted some time to learning the DE's layout and basic functionality. Budgie is built from GNOME 3 components but is designed to be easy to use, and is known for not needing much customization. TechHut provides a quick overview in his video "Budgie in 100 Seconds."

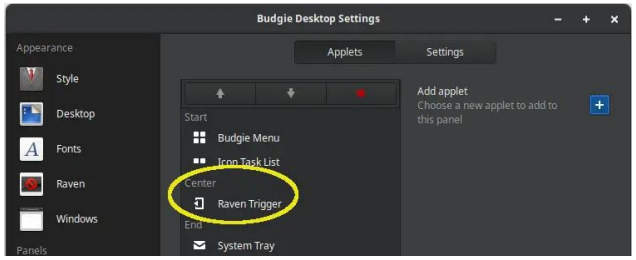


Raven is one of the unique features of the Budgie DE. It is a right-hand panel whose purpose is to display various widgets and notifications, providing quick access. With PCLinuxOS Debian, Raven's Calendar widget is inactive by default.

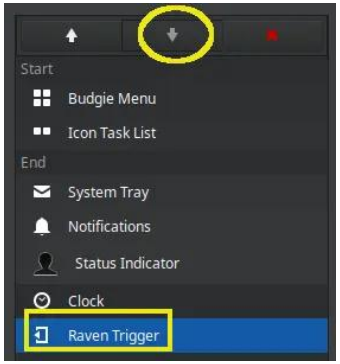



To fix this, go to **Budgie Desktop Settings > Panels > Bottom Panel** and click on the Applets tab to bring it forward.

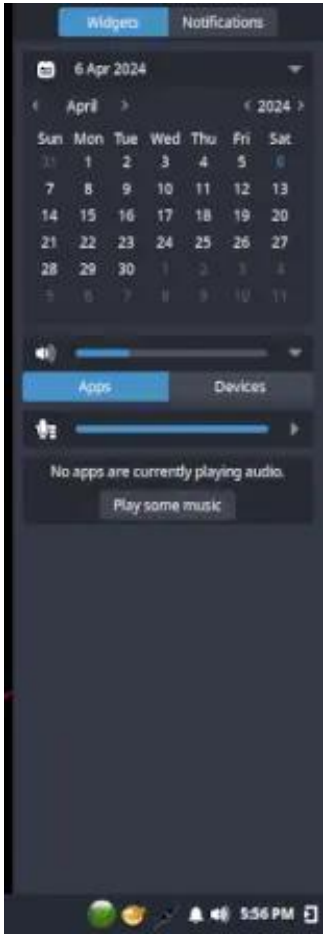
Click the **Add applet** button, then scroll down and choose **Raven Trigger**. Next, click on the Add button.

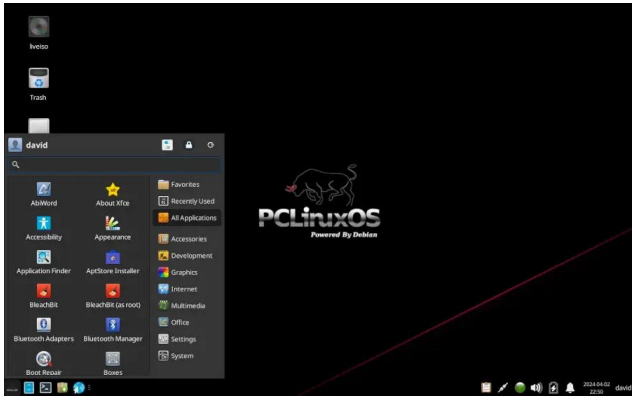



This will add the Raven Trigger applet to the center section of the bottom panel. To shift its location to the far right end of the panel, select the Raven Trigger applet, then click on the Down arrow (↓) until the applet is moved to that location.




The final result should look something like this: (right, top)




## Xfce

- Kernel 6.6.8
- Xfce version 4.18.1
- LibreOffice 7.4.7.2

**Conclusion**

Although it is far from a blatant imitation of Linux Mint Debian Edition (LMDE), PCLinuxOS Debian Edition is a similar concept: a variant of PCLinuxOS that is directly based on Debian Stable [Bookworm] but with user-friendly features and utilities designed to keep it looking like the original PCLinuxOS.

When I asked Upgreyed about his future plans for PCLinuxOS Debian, he wrote that his goal is to make the distribution as user-friendly as possible. More PCLinuxOS-specific packages will be added to the repository. Although he does not know the number of current users, the ISOs have been downloaded hundreds of times. Upgreyed appreciates testers and welcomes feedback, so that he can fix packages or an ISO, if necessary.

PCLinuxOS Debian is a mature project with stable releases, thanks to the dedication of Upgreyed and tbs. If you have been considering the possibility of trying Cinnamon or the Budgie DE but want to stay within the PCLinuxOS family, PCLinuxOS Debian is an attractive option. If you are a MATE fan, I recommend checking out the MATE version due to its rich feature set. Likewise, the KDE Plasma and Xfce Editions are worthy additions to the PCLinuxOS ecosystem

***The PCLinuxOS Magazine***

***Created with Scribus***



# Screenshot Showcase

***Posted by Alistair_Einstein_Izzard, on April 4, 2024, running Openbox.***

# Tip Top Tips: How To Make Pipewire Sound Even Better

**by hunter0one & Paul Arnote**

Recently, **hunter0one** posted a tip in the PCLinuxOS forum about how to improve the sound quality from the recently added PipeWire sound processing system. It's a relatively short tip, but we'll expand it out a little bit.

First, here's the tip that hunter0one posted:

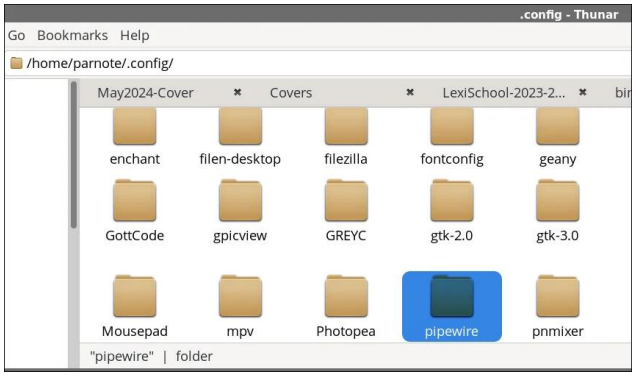
*The sound quality of PipeWire can be improved even more at the cost of more CPU power, or you can lower it to use even less. Here's how.*

*Make a directory within your home .config folder (**~/.config**) called **pipewire** then copy **pipewire-pulse.conf** and **client.conf** from **/usr/share/pipewire** to your new directory **~/.config/pipewire**. Open both of these files in a text editor and somewhere within you will find **resample.quality = 4**.*

*You can change the 4 to a number between 1 and 10. 1 uses the least CPU power but sounds the worst, while 10 sounds the best but uses more processing power. I use 10 on my Ryzen machine, and it sounds great, but you may use whatever you like. Make sure you uncomment it (remove the # at the beginning).*

*Afterwards, restart your machine or log out and log back in. You will now be using the new resample quality. Congrats!*


So, to get started, make the directory in your ~/.config directory, named "pipewire" (without the quotes, of course). Notice that the name for the directory is "pipewire," not "Pipewire." Notice the difference? I hope so, because on Linux, the case (upper or lower) makes a difference. Your "new" directory should be all lowercase letters. Below is mine, as visible in Thunar.




Now, copy the **client.conf** and **pipewire-pulse.conf** files from the /usr/share/pipewire directory to the ~/.config/pipewire directory you just created. You may need to do this as the root user. Doing it this way makes the pipewire settings adjustable on a per-user basis, instead of making them apply to all users on the system. If you have multiple users on your computer, you may need to repeat this step for each user.

The areas of the client.conf and pipewire-pulse.conf files that need to be modified are shown below. Be sure you're editing the files from the ~/.config/pipewire directory. If you mess anything up, you can easily delete them and just start over.

```
72  stream.properties = {
73      #node.latency          = 1024/48000
74      #node.autoconnect      = true
75      #resample.quality      = 4
76      #channelmix.normalize  = false
77      #channelmix.mix-lfe    = true
78      #channelmix.upmix      = true
79      #channelmix.upmix-method = psd  # none, simple
80      #channelmix.lfe-cutoff = 150
81      #channelmix.fc-cutoff  = 12000
82      #channelmix.rear-delay = 12.0
83      #channelmix.stereo-widen = 0.0
84      #channelmix.hilbert-taps = 0
85      #dither.noise = 0
86  }
```

*client.conf*

```
69  stream.properties = {
70      #node.latency          = 1024/48000
71      #node.autoconnect      = true
72      #resample.quality      = 4
73      #channelmix.normalize  = false
74      #channelmix.mix-lfe    = true
75      #channelmix.upmix      = true
76      #channelmix.upmix-method = psd  # none, simple
77      #channelmix.lfe-cutoff = 150
78      #channelmix.fc-cutoff  = 12000
79      #channelmix.rear-delay = 12.0
80      #channelmix.stereo-widen = 0.0
81      #channelmix.hilbert-taps = 0
82      #dither.noise = 0
83  }
```

*pipewire-pulse.conf*

The above images (bottom right column, previous page) are snippets from the files loaded into Geany. In the client.conf file, the line you need to change is line 75. In the pipewire-pulse.conf file, the line you need to change is line 72. Turning on line-numbering in your text editor will help you find the entry quickly. To help make sure you're looking at the right entries, I've pointed them out with red arrows in both images.

Now, remove the "#" symbol from the beginning of that line. Next, change the value from the default value of "4" to whatever quality level suits your needs. Keep in mind that a quality level of "1" will most likely sound like shiitake mushrooms, but will use the least amount of CPU cycles. Likewise, a quality level of "10" will/should provide the highest quality sound, but will also use the most CPU cycles. Make the same change to both files. Don't change one file without changing the other, in a nutshell.

Once you've made your changes, you need to either reboot, or log out and back into your session.

Some users have commented that they haven't seen any (or much) difference with altering the settings. Others, though, have. So, just like with a lot of things, your mileage may vary, depending on the hardware in your computer.





# Screenshot Showcase


***Posted by astronaut, on April 5, 2024, running Openbox.***

# PCLinuxOS Recipe Corner


## Ham & Cheddar Pierogi Bake

Serves: 6

**INGREDIENTS:**

2 tablespoons butter
1 cup diced onions
2 tablespoons all-purpose flour
3/4 cup reduced sodium chicken broth
(from 32-oz carton)
3/4 cup milk *substitute heavy cream
for a richer flavor.
1 1/2 cups shredded Cheddar cheese (6 oz)
1 package (16 oz) frozen potato and
Cheddar pierogies
1 tablespoon water
1 cup cubed ham (6 oz)
2 tablespoons thinly sliced green onions

**DIRECTIONS:**

In a 3-quart saucepan, melt butter over medium heat. Add onions; cook 3 to 4 minutes, stirring occasionally, until just starting to soften. With a whisk, stir in flour until smooth. Cook and stir 1 to 2 minutes or until mixture is bubbly.

In 2-cup glass measuring cup, mix broth and milk. Gradually stir broth mixture into saucepan. Increase heat to medium-high; heat to boiling, stirring constantly. Boil and stir 1 minute; reduce heat to medium. Stir in 1 cup of the Cheddar cheese. Cook until melted, stirring occasionally. Remove from heat.

Meanwhile, place frozen pierogies and water in baking dish; cover with plastic wrap. Microwave on High 2 minutes; stir. Continue microwaving on High 1 1/2 to 2 minutes or until thawed. **** or leave overnight in refrigerator to thaw.*** Pour cheese sauce over pierogies. Top with ham and remaining 1/2 cup cheese.

Bake 20 to 25 minutes, or until cheese is melted and edges are bubbly. Let stand 10 minutes. Top with green onions.

**TIPS:**

Serve with sour cream and applesauce on the side.

Serve with a tossed green salad for a complete meal.

Try pan frying your pierogies first, for a crispy treat.

**NUTRITION:**

Calories: 330 Carbs: 28g Fiber: 1g
Sodium: 870mg Protein: 16g


# How Political Campaigns Use Your Data To Target You

by **Thorin Klosowski**
Electronic Frontier Foundation


Data about potential voters — who they are, where they are, and how to reach them — is an extremely valuable commodity during an election year. And while the right to a secret ballot is a cornerstone of the democratic process, your personal information is gathered, used, and sold along the way. It's not possible to fully shield yourself from all this data processing, but you can take steps to at least minimize and understand it.

Political campaigns use the same invasive tricks that behavioral ads do — pulling in data from a variety of sources online to create a profile — so they can target you. Your digital trail is a critical tool for campaigns, but the process starts in the real world, where longstanding techniques to collect data about you can be useful indicators of how you'll vote. This starts with voter records.

**Your IRL Voting Trail Is Still Valuable**

Politicians have long had access to public data, like voter registration, party registration, address, and participation information (whether or not a voter voted, not who they voted for). Online access to such records has made them easier to get in some states, with unintended consequences, like doxing.

Campaigns can purchase this voter information from most states. These records provide a rough idea of whether that person will vote or not, and—if they're registered to a particular party—who they might lean toward voting for. Campaigns use this to put every voter into broad categories, like "supporter," "non-supporter," or "undecided." Campaigns gather such information at in-person events, too, like door-knocking and rallies, where you might sign up for emails or phone calls.

Campaigns also share information about you with other campaigns, so if you register with a candidate one year, it's likely that information goes to another in the future. For example, the website for Adam's Schiff's campaign to serve as U.S. Senator from California has a privacy policy with this line under "Sharing of Information":

With organizations, candidates, campaigns, groups, or causes that we believe have similar political viewpoints, principles, or objectives or share similar goals and with organizations that facilitate communications and information sharing among such groups.

Similar language can be found on other campaign sites, including those for Elizabeth Warren and Ted Cruz. These candidate lists are valuable, and are often shared within the national party. In 2017, the Hillary Clinton campaign gave its email list to the Democratic National Committee, a contribution valued at $3.5 million.

If you live in a state with citizen initiative ballot measures, data collected from signature sheets might be shared or used as well. Signing a petition doesn't necessarily mean you support the proposed ballot measure—it's just saying you think it deserves to be put on the ballot. But in most states, these signature pages will remain a part of the public record, and the information you provide may get used for mailings or other targeted political ads.

**How Those Voter Records, and Much More, Lead to Targeted Digital Ads**

All that real world information is just one part of the puzzle these days. Political campaigns tap into the same intrusive adtech tracking systems used to deliver online behavioral ads. We saw a glimpse into how this worked after the Cambridge Analytica scandal, and the system has only grown since then.

Specific details are often a mystery, as a political advertising profile may be created by combining disparate information — from consumer scoring data brokers like Acxiom or Experian, smartphone data, and publicly available voter information — into a jumble of data points that's often hard to trace in any meaningful way. A simplified version of the whole process might go something like this:

1. A campaign starts with its voter list, which includes names, addresses, and party affiliation. It may have purchased this from the state or its own national committee, or collected some of it for itself through a website or app.

2. The campaign then turns to a data broker to enhance this list with consumer information. The data broker combines the voter list with its own data, then creates a behavioral profile using inferences based on your shopping, hobbies, demographics, and more. The campaign looks this all over, then chooses some categories of people it thinks will be receptive to its messages in its various targeted ads.

3. Finally, the campaign turns to an ad targeting company to get the ad on your device. Some ad companies might use an IP address to target the ad to you. As The Markup revealed, other companies might target you based on your phone's location, which is particularly useful in reaching voters not in the campaign's files.

In 2020, Open Secrets found political groups paid 37 different data brokers at least $23 million for access to services or data. These data brokers collect information from browser cookies, web beacons, mobile phones, social media platforms, and more. They found that some companies specialize in more general data, while others, like i360, TargetSmart, and Grassroots Analytics, focus on data useful to campaigns or advocacy.

| | | |
|---|---|---|
| **QAnon** | Nonbeliever | |
| **Rightwing Militias** | Oppose | |
| **Right to Repair** | Support | |
| **Inflation Fault** | Corporate America | |
| **Electric Vehicle Buyer** | Likely Buyer | |
| **Climate Change** | Believer | |
| **Amazon Worker Treatment** | Exploitative | |

*A sample of some categories and inferences in a political data broker file that we received through a CCPA request shows the wide variety of assumptions these companies may make.*

These political data brokers make a lot of promises to campaigns. TargetSmart claims to have 171 million highly accurate cell phone numbers, and i360 claims to have data on 220 million voters. They also tend to offer specialized campaign categories that go beyond the offerings of consumer-focused data brokers. Check out data broker L2's "National Models & Predictive Analytics" page, which breaks down interests, demographics, and political ideology—including details like "Voter Fraud Belief," and "Ukraine Continue." The New York Times demonstrated a

particularly novel approach to these sorts of profiles where a voter analytics firm created a "Covid concern score" by analyzing cell phone location, then ranked people based on travel patterns during the pandemic.

Some of these companies target based on location data. For example, El Toro claims to have once "identified over 130,000 IP-matched voter homes that met the client's targeting criteria. El Toro served banner and video advertisements up to 3 times per day, per voter household – across all devices within the home."

That "all devices within the home" claim may prove important in the coming elections: as streaming video services integrate more ad-based subscription tiers, that likely means more political ads this year. One company, AdImpact, projects $1.3 billion in political ad spending on "connected television" ads in 2024. This may be driven in part by the move away from tracking cookies, which makes web browsing data less appealing.

In the case of connected televisions, ads can also integrate data based on what you've watched, using information collected through automated content recognition (ACR). Streaming device maker and service provider Roku's pitch to potential political advertisers is straightforward: "there's an opportunity for campaigns to use their own data like never before, for instance to reach households in a particular district where they need to get out the vote." Roku claims to have at least 80 million users. As a platform for televisions and "streaming sticks," and especially if you opted into ACR (we'll detail how to check below), Roku can collect and use a lot of your viewing data ranging from apps, to broadcast TV, or even to video games.

This is vastly different from traditional broadcast TV ads, which might be targeted broadly based on a city or state, and the show being aired. Now, a campaign can target an ad at one household, but not their neighbor, even if they're watching the same show. Of the main streaming companies, only Amazon and Netflix don't accept political ads.

Finally, there are Facebook and Google, two companies that have amassed a mountain of data points about all their users, and which allow campaigns to target based on some of those factors. According to at least one report, political ad spending on Google (mostly through YouTube) is projected to be $552 million, while Facebook is projected at $568 million. Unlike the data brokers discussed above, most of what you see on Facebook and Google is derived from the data collected by the company from its users. This may make it easier to understand why you're seeing a political ad, for example, if you follow or view content from a specific politician or party, or about a specific political topic.

**What You Can Do to Protect Your Privacy**

Managing the flow of all this data might feel impossible, but you can take a few important steps to minimize what's out there. The chances you'll catch everything is low, but minimizing what is accessible is still a privacy win.

**Install Privacy Badger**

Considering how much data is collected just from your day-to-day web browsing, it's a good idea to protect that first. The simplest way to do so is with our own tracking blocker extension, Privacy Badger.

**Disable Your Phone Advertising ID and Audit Your Location Settings**

Your phone has an ad identifier that makes it simple for advertisers to track and collate everything you do. Thankfully, you can make this much harder for those advertisers by disabling it:

On **iPhone**: Head into ***Settings*** > ***Privacy & Security*** > ***Tracking***, and make sure "Allow Apps to Request to Track" is disabled.

**On Android**: Open ***Settings*** > ***Security & Privacy*** > ***Privacy*** > ***Ads***, and select "Delete advertising ID."

Similarly, as noted above, your location is a valuable asset for campaigns. They can collect your location through data brokers, which usually get it from otherwise unaffiliated apps. This is why it's a good idea to limit what sorts of apps have access to your location:

**On iPhone**: open ***Settings*** > ***Privacy & Security*** > ***Location Services***, and disable access for any apps that do not need it. You can also set location for only "While using," for certain apps where it's helpful, but unnecessary to track you all the time. Also, consider disabling "Precise Location" for any apps that don't need your exact location (for example, your GPS navigation app needs precise location, but no weather app does).

**On Android**: Open ***Settings*** > ***Location*** > ***App location permissions***, and confirm that no apps are accessing your location that you don't want to. As with iOS, you can set it to "Allow only while using the app," for apps that don't need it all the time, and disable "Use precise location," for any apps that don't need exact location access.

**Opt Out of Tracking on Your TV or Streaming Device, and Any Video Streaming Service**

Nearly every brand of TV is connected to the internet these days. Consumer Reports has a guide for disabling what you can on most popular TVs and software platforms. If you use an Apple TV, you can disable the ad identifier following the exact same directions as on your phone.

Since the passage of a number of state privacy laws, streaming services, like other sites, have offered a way for users to opt out of the sale of their info. Many have extended this right outside of states that require it. You'll need to be logged into your streaming service account to take action on most of these, but TechHive has a list of opt out links for popular streaming services to get you started. Select the "Right to Opt Out" option, when offered.

**Don't Click on Links in (or Respond to) Political Text Messages**

You've likely been receiving political texts for much of the past year, and that's not going to let up until election day. It is increasingly difficult to decipher whether they're legitimate or spam, and with links that often use a URL shortener or odd looking domains, it's best not to click them. If there's a campaign you want to donate to, head directly to the site of the candidate or ballot sponsor.

**Create an Alternate Email and Phone Number for Campaign Stuff**

If you want to keep updated on campaign or ballot initiatives, consider setting up an email specifically for that, and nothing else. Since a phone number is also often required, it's a good idea to set up a secondary phone number for these same purposes (you can do so for free through services like Google Voice).

**Keep an Eye Out for Deceptive Check Boxes**

Speaking of signing up for updates, be mindful of when you don't intend to sign up for emails. Campaigns might use pre-selected options for everything from donation amounts to signing up for a newsletter. So, when you sign up with any campaign, keep an eye on any options you might not intend to opt into.

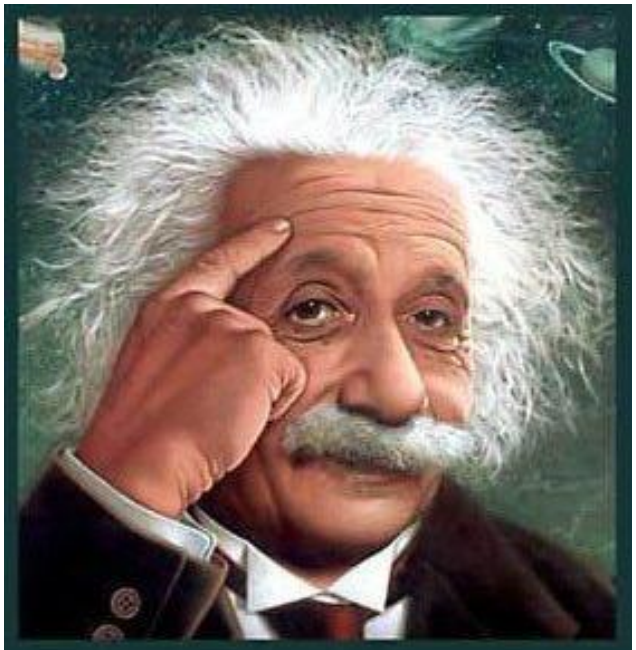
**Mind Your Social Media**

Now's a great time to take any sort of "privacy checkup" available on whatever social media platforms you use to help minimize any accidental data sharing. Even though you can't completely opt out of behavioral advertising on Facebook, review your ad preferences and opt out whatever you can. Also, be sure to disable access to off-site activity. You should also opt out of personalized ads on Google's services. You cannot disable behavioral ads on TikTok, but the company doesn't allow political ads.

If you're curious to learn more about why you're seeing an ad to begin with, on Facebook you can always click the three-dot icon on an ad, then click "Why am I seeing this ad?" to learn more. For ads on YouTube, you can click the "More" button and then "About this advertiser" to see some information about who placed the ad. Anywhere else you see a Google ad, you can click the "AdChoices" button and then "Why this ad?"

You shouldn't need to spend an afternoon jumping through opt out hoops and tweaking privacy settings on every device you own just so you're not bombarded with highly targeted ads. That's why EFF supports comprehensive consumer data privacy legislation, including a ban on online behavioral ads.

Democracy works because we participate, and you should be able to do so without sacrificing your privacy.

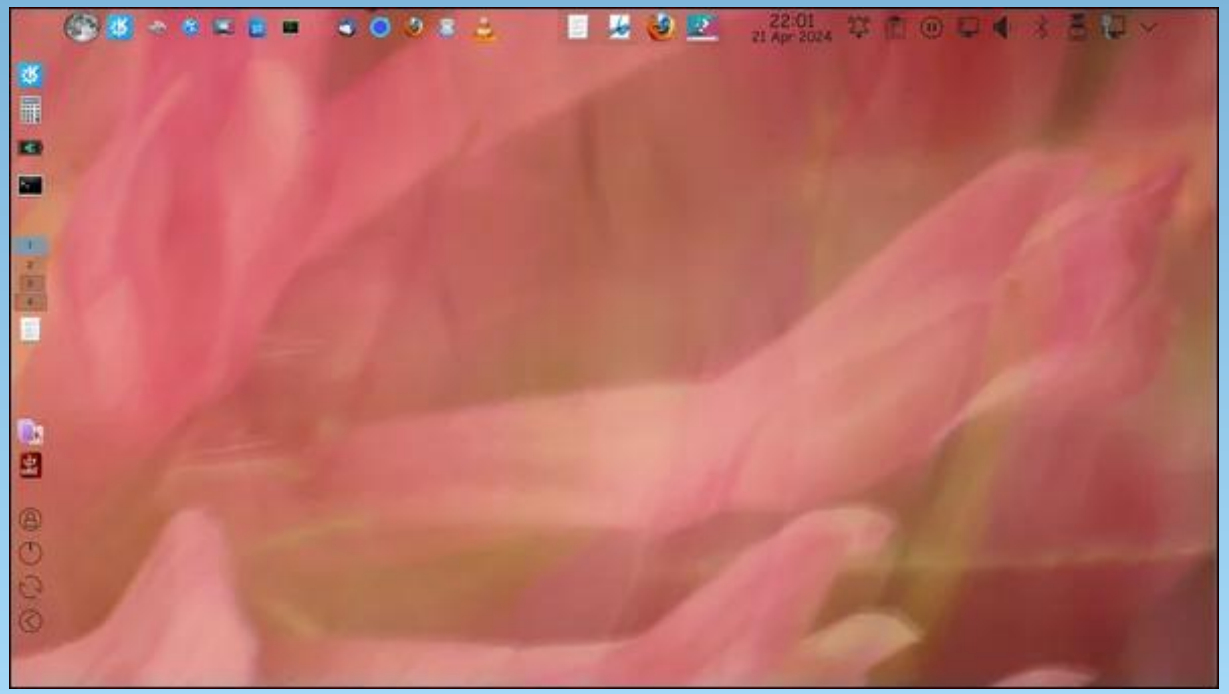


*It's easier than E=mc2*
*It's elemental*
*It's light years ahead*
*It's a wise choice*
*It's Radically Simple*
*It's ...*

PCLinuxOS
Radically Simple



# Screenshot Showcase



*Posted by bliss, on April 24, 2024, running KDE.*

# ICYMI: Google Incognito Mode Settlement Proposed

**by Paul Arnote (parnote)**

*Image by Ralph from Pixabay*

**It appears the European Union is wasting no time enforcing its Digital Markets Act (DMA):** On March 25, 2024, we learned Apple, Google, and Meta will all be investigated for potentially violating the DMA, according to an article from Lifehacker. If found guilty, each company could face up to 10% of their total annual revenue not just in the E.U. but globally —20% for "repeat infringement." Violate the E.U.'s laws, pay with the money you earned everywhere. The DMA is only 18 days old as of the announcement of the investigation: Europe put the law into action March 7, a deadline these big tech companies needed to adhere to. Apple, for example, was required to offer developers the ability to create their own third-party app stores, as well as create true mobile browsers not based on Safari's WebKit platform. Meta, on the other hand, needed to open up WhatsApp and Messenger to third-party messaging services. The European Commission labels six companies as "gatekeepers," identifying them as blocking third-party innovation through their use of specific apps and services. (Interestingly, it did not find Apple's iMessage to be a gatekeeping service.) In addition to Apple, Google, and Meta, the Commission has found Amazon, ByteDance, and Microsoft as gatekeepers.

**Human brains appeared to be getting bigger, temporal trends showed**, according to an article from MedPage Today. From the 1930s to 1970s, brain volumes and cortical surface area of people who had neither dementia nor stroke became progressively larger, reported Charles DeCarli, MD, of the University of California Davis in Sacramento, and co-authors in *JAMA Neurology*. When researchers compared people born in the 1930s with those born in the 1970s and adjusted for age and sex, they found (all P<0.001): intracranial volume was 6.6% greater (1,234 vs. 1,321 mL), white matter volume was 7.7% greater (441.9 vs. 476.3 mL), hippocampal volume had a 5.7% greater value (6.51 vs. 6.89 mL), and cortical surface area had a 14.9% greater value (1,933 vs. 2,222 cm2). Overall gray matter volume did not increase significantly. Cortical thickness was thinner by 20.9% (2.34 mm vs. 1.85 mm) over the same period. The larger brain volumes indicate larger brain development and potentially greater brain reserve that may explain the declining incidence of dementia, the researchers hypothesized. (It's sad, though, that the increased cranial capacity isn't necessarily resulting in smarter people. Just look around.)

**Have you ever thought about where the term Wi-Fi comes from?** That's the question an article from Gizmodo takes a look at. Most people would logically assume it's a shortened version of some highly technical description for the tech that allowed computers to access the internet wirelessly. But those people would be wrong. In reality, the term was created by… Nah! I'm not going to tell you here. Go ahead and go read it for yourself.

**Google agreed to destroy or de-identify billions of records of web browsing data collected when users were in its private browsing "Incognito mode,"** according to a proposed class action settlement filed on April 1, 2024, says an article from The Verge. The proposed settlement in *Brown v. Google* will

also mandate greater disclosure from the company about how it collects information in Incognito mode and put limits on future data collection. If approved by a California federal judge, the settlement could apply to 136 million Google users. The 2020 lawsuit was brought by Google account holders who accused the company of illegally tracking their behavior through the private browsing feature. The proposal is valued at $5 billion, according to Monday's court filing, calculated by determining the value of data Google has stored and would be forced to destroy and the data it would be prevented from collecting. Google would need to address data collected in private browsing mode in December 2023 and earlier. Any data that is not outright deleted must be de-identified.

AT&T is having a rough year. Back in February, customers experienced a massive network outage that lasted about 12 hours. This month, the company has another round of bad news: **AT&T suffered a massive data breach that impacted over 70 million customers** (7.6 million current and 65.4 million former ones), according to an article from Lifehacker. The data made its way to the dark web, a popular destination for bad actors to sell stolen data and information, and the company doesn't exactly know whether the breach occurred through AT&T itself or third-party vendors.

**On March 29, 2024, a lone Microsoft developer rocked the world when he revealed a backdoor had been intentionally planted in xz Utils**, an open source data compression utility available on almost all installations of Linux and other Unix-like operating systems, according to an article from ArsTechnica on April 1, 2024. The person or people behind this project likely spent years on it. They were likely very close to seeing the backdoor update merged into Debian and Red Hat, the two biggest distributions of Linux, when an eagle-eyed software developer spotted something fishy. "This might be the best executed supply chain attack we've seen described in the open, and it's a nightmare scenario: malicious, competent, authorized upstream in a widely used library," software and cryptography engineer Filippo Valsorda said of the effort, which came frightfully close to succeeding. Researchers have spent the weekend (since its discovery) gathering clues. Here's what we know so far. (There's another excellent article over at TechRepublic.)

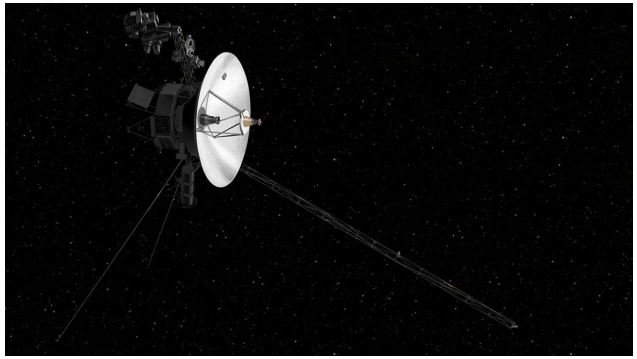
*Image by Lumina Obscura from Pixabay*

On April 4, 2024, **astronomers who are conducting what they describe as the biggest and most precise survey yet of the history of the universe announced that they might have discovered a major flaw in their understanding of dark energy**, the mysterious force that is speeding up the expansion of the cosmos, according to an article from the New York Times. Dark energy was assumed to be a constant force in the universe, both currently and throughout cosmic history. But the new data suggest that it may be more changeable, growing stronger or weaker over time, reversing, or even fading away.

**The U.K. government has formally agreed to work with the U.S. in developing tests for advanced artificial intelligence models**, according to an article from TechRepublic. A Memorandum of Understanding, which is a non-legally binding agreement, was signed on April 1, 2024, by the U.K. Technology Secretary Michelle Donelan and U.S. Commerce Secretary Gina Raimondo. Both countries will now "align their scientific approaches" and work together to "accelerate and rapidly iterate robust suites of evaluations for AI models, systems, and agents." This action is being taken to uphold the commitments established at the first global AI Safety Summit last November, where governments from around the world accepted their role in safety testing the next generation of AI models.

**After more than 9,940 miles (16,000 km) over 352 days across 16 countries, Russ Cook, aka the "Hardest Geezer", has completed the mammoth challenge of running the length of Africa**, according to an article from The Guardian. The 27-year-old endurance athlete from Worthing, West Sussex, crossed the finish line in Tunisia on Sunday afternoon, and planned to celebrate with a party – as well as a

strawberry daiquiri – having raised more than £600,000 for charity. His achievement, believed to be the first person to run tip to tip from southern to northern Africa, was more extraordinary given several setbacks including a robbery at gunpoint in Angola, being held by men with machetes in the Republic of the Congo, health scares and visa complications.



*JPL/Nasa*

**NASA's pioneering Voyager 1 spacecraft has a memory problem. The space agency has been troubleshooting the elderly machine since it began sending back gibberish communications in November**, according to an article from Forbes. NASA hasn't fixed Voyager 1 yet, but engineers now know what's vexing the spacecraft. The glitch paused Voyager 1's science work and kicked off a long-distance diagnosis process. The team traced the issue to the flight data subsystem, a computer that talks to the spacecraft's telemetry modulation unit to send science and engineering data to Earth. The data came back unintelligible. The culprit appears to be a single chip that's part of the FDS. The breakthrough came thanks to a "poke" NASA sent in March that prompted Voyager 1 to send back a readout of its FDS memory. "Using the readout, the team has confirmed that about 3% of the FDS memory has been corrupted, preventing the computer from carrying out normal operations," NASA said in a statement on April 4.

**If life exists on Jupiter's moon Europa, scientists might soon be able to detect it**, according to an article from phys.org. Europa is one of the largest of more than 90 moons in orbit around the planet Jupiter. It is also one of the best places to look for alien life. Often termed an "ocean world" by scientists, observations to date strongly suggest that beneath Europa's icy crust, there could be a liquid saltwater ocean containing twice as much water as Earth's oceans. Now, NASA's Europa Clipper—the largest spacecraft ever developed by the US space agency for a planetary mission—may have the tools to detect it.

**American rescuers found three lost sailors on a tiny uninhabited island in Micronesia with a damaged boat and the word "HELP" spelled out on the beach**, according to an article from the New York Times. The three men were stranded on the remote, uninhabited island (called Pikelot) for more than a week. The men, who were experienced mariners in their 40s, set sail on March 31 from Polowat Atoll, an island that is part of the Federated States of Micronesia, in a 20-foot open skiff powered by an outboard motor. After their unintended delay, the Coast Guard said, the men had been safely returned home Tuesday evening. Pikelot is a tiny dot in the Pacific Ocean covered in palm trees and bushes, measuring less than 2,000 feet (0.61 km) in length. The Micronesian island was part of a search area that the Coast Guard said spanned more than 100,000 square miles.

*Image by Aristal Branson from Pixabay*

**New technology**, which was created at the University of Turku and developed by the company CardioSignal, **uses a smartphone to analyze heart movement and detect heart failure**, according to an article from ScienceDaily. The study involved five organizations from Finland and the United States. Gyrocardiography is a non-invasive technique for measuring cardiac vibrations on the chest. The smartphone's built-in motion sensors can detect and record these vibrations, including those that doctors cannot hear with a stethoscope. The method has been developed over the last 10 years by researchers at the University of Turku and CardioSignal.

**Do you want to learn how to stop your data from being used to train AI?** Well, that's the whole premise of an article from Wired. Some companies let you opt out of allowing your content to be used for generative AI. This article describes how to take back (at least a little) control from ChatGPT, Google's Gemini, and more.

**Is time travel really possible? Here's what physics says**, according to an article from BBC. Answering this question requires understanding how time actually works – something physicists are far from certain about. So far, what we can say with confidence is that traveling into the future is achievable, but traveling into the past is either wildly difficult or absolutely impossible.

*Image by OpenClipart-Vectors from Pixabay*

**Apple sent a threat notification to iPhone users in 92 countries on April 10 informing them that their device was "being targeted by a mercenary spyware attack,"** according to an article from TechRepublic. The alert, sent at 12:00 p.m. Pacific Time, told recipients that the attackers were attempting to "remotely compromise" their phone and that they were likely being targeted specifically "because of who you are or what you do." Apple's notification did not identify the alleged attackers, nor did it specify the locations of its recipients.

**On April 12, 2024, Roku confirmed a cyberattack compromised roughly 576,000 accounts**, according to an article from Lifehacker. It marks the second such cyberattack to affect the company, which compromised a smaller number of accounts earlier this year. As Roku has over 80 million active accounts, the chances of yours being among the fraction of a percent of users affected is small. Still, Roku says it has reset passwords for all users affected in this attack.

In last month's ICYMI article, we told you about how your fancy new car may be spying on you. Well, it seems coverage of this little secret is expanding. According to an article from Lifehacker, **if your car is relatively new, it's been designed as a spying superstar — modern cars typically have microphones, cameras, and tons of sensors collecting data**. But it's not just the sensors built into the car itself — there are also all the apps installed on the car's interface, plus all the apps installed on your phone, which you probably link to the car via Bluetooth, giving away all sorts of privacy in the process. That means car manufacturers can potentially know the music you listen to, things you say inside the car, and the locations you look up on map apps. We're fire hosing private information to a carmaker; we just don't think about it. In fact, some car manufacturers even admitted to tracking your *sexual activity* in relation to your car, along with health data.

*Image by Iuliia Bondarenko from Pixabay*

**Women across the country have been bonding online over their "Ozempic babies" − surprise pregnancies while taking weight loss medications, despite being on birth control or having a history of fertility issues**, according to an article from USA Today. Now, some of them say they're experiencing intense symptoms such as extreme hunger and rapid weight gain after quitting these drugs cold turkey to protect their baby's health. Medications like Ozempic, Mounjaro, WeGovy and Zepbound appear to boost fertility because the weight loss they induce corrects hormonal imbalances caused by obesity and metabolic disorders; some of them

may also reduce the efficacy of birth control pills, increasing chances of pregnancy.

One of the internet's simple pleasures is watching YouTube with an ad blocker. You can watch as many videos as you want without constant interruptions from obnoxious, occasionally unskippable commercials. **But ads are how YouTube makes its money**, so it's not too happy when people use ad blockers to avoid them, according to an article from Lifehacker. Last year, the company started taking a more proactive approach to the situation, showing some ad blocker users a pop-up suggesting they disable their ad blocker or subscribe to YouTube Premium. After that, **the company started blocking video playback entirely**. (That said, even today, I don't see the pop-up on my work profile with uBlock Origin.) YouTube is far from the first site to issue such an anti-ad blocker message, but this was definitely a first for this free video platform. And it won't do you much good to switch to YouTube clients that "skip" the ads, because YouTube is cracking down on those, too. The article goes on to describe how to work around the greedy crackdown.

**Have you ever wondered what really happens when you trade in an iPhone at the Apple Store?** This article from Bloomberg News sheds some light on what happens. Apple touts its network of shredding robots and contractors as a greener way to reuse old gadgets. A lengthy court battle and a Businessweek investigation have cast some light on the recycling industry's dirty secrets.

**Google Chrome is testing a new feature that lets you enable or disable all your extensions by clicking a single button**, according to an article from Lifehacker. Be it debugging or saving resources, there are many reasons why you might want to use this feature, which was first spotted by Gamer Stones. With this new feature, you can quickly disable all extensions and reload the page to determine what's causing the issue. Similarly, if your laptop is low on battery or if your PC is running slow, you could quickly disable all Chrome extensions to improve performance. You might also consider using this feature when you're taking an online test, going through an important application, or in other situations where you're required to turn off browser extensions.



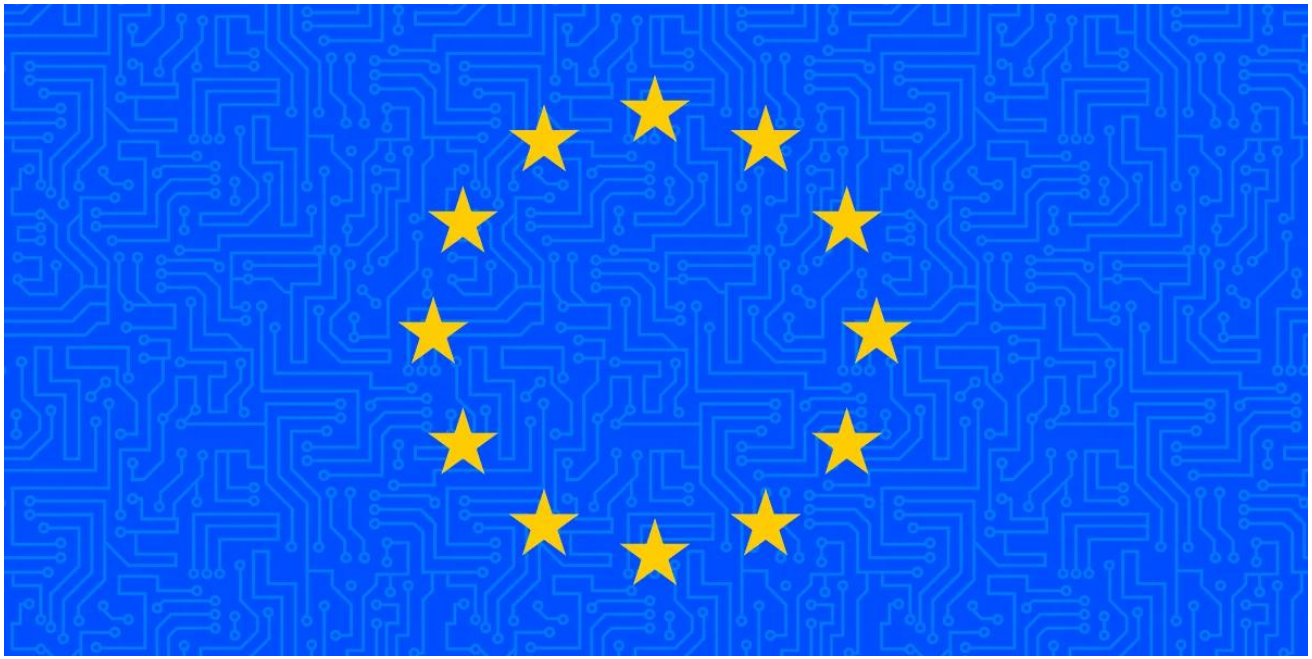
**Like them or hate them, YouTube Shorts are here to stay**, says an article from Lifehacker. If they wish they weren't constantly popping up on your feed, you can do a few things to weaken their pull on your already declining attention span. YouTube's own option lets you temporarily hide them, but you need third-party extensions to banish them forever.

The Guardian takes a look at pesticide levels of common fruits and vegetables in their article **"What's safe to eat? Here is the pesticide risk level for each fruit and vegetable."** I suspect you'll be as surprised as I was. Not to be a spoiler, the fruits and vegetables labeled as "Organic" win hands down with the safest levels of pesticides. So, I guess maybe there is a difference between "conventional" and "organic" foods that justifies their slightly higher price at the checkout after all.

# Making The Law Accessible In Europe & The USA

**by Mitch Stoltz and Cara Gagliano**
Electronic Frontier Foundation
Reprinted under CC-3.0 Attribution License

*Special thanks to EFF legal intern Alissa Johnson, who was the lead author of this post.*



Earlier this month, the European Union Court of Justice ruled that harmonized standards are a part of EU law, and thus must be accessible to EU citizens and residents free of charge.

While it might seem like common sense that the laws that govern us should be freely accessible, this question has been in dispute in the EU for the past five years, and in the U.S. for over a decade. At the center of this debate are technical standards, developed by private organizations and later incorporated into law. Before they were challenged in court, standards-development organizations were able to limit access to these incorporated standards through assertions of copyright. Regulated parties or concerned citizens checking compliance with technical or safety standards had to do so by purchasing these standards, often at significant expense, from private organizations. While free alternatives, like proprietary online "reading rooms," were sometimes available, these options had their own significant downsides, including limited functionality and privacy concerns.

In 2018, two nonprofits, Public.Resource.Org and Right to Know, made a request to the European Commission for access to four harmonized standards—that is, standards that apply across the European Union—pertaining to the safety of toys. The Commission refused to grant them access on the grounds that the standards were copyrighted.

The nonprofits then brought an action before the General Court of the European Union seeking annulment of the Commission's decision. They made two main arguments. First, that copyright couldn't be applicable to the harmonized standards, and that open access to the standards would not harm the commercial interests of the European Committee for Standardization or other standard setting bodies. Second, they argued that the public interest in open access to the law should override whatever copyright interests might exist. The General Court rejected both arguments, finding that the threshold for originality that makes a work eligible for copyright protection had been met, the sale of standards was a vital part of standards bodies' business model, and the public's interest in ensuring the proper functioning of the European standardization system outweighed their interest in free access to harmonized standards.

Last week, the EU Court of Justice overturned the General Court decision, holding that EU citizens and residents have an overriding interest in free access to the laws that govern them.

Article 15(3) of the Treaty on the Functioning of the EU and Article 42 of the Charter of Fundamental Rights of the EU guarantee a right of access to documents of Union institutions, bodies, offices, and agencies. These bodies can refuse access to a document where its disclosure would undermine the protection of commercial interests, including intellectual property, unless there is an overriding public interest in disclosure.

Under the ECJ's ruling, standards written by private companies, but incorporated into legislation, now form part of EU law. People need access to these standards to determine their own compliance. While compliance with harmonized standards is not generally mandatory, it is in the case of the toy safety standards in question here. Even when compliance is not mandatory, products that meet technical standards benefit from a "presumption of conformity," and failure to conform can impose significant administrative difficulties and additional costs.

Given that harmonized standards are a part of EU law, citizens, and residents of member states have an interest in free access that overrides potential copyright concerns. Free access is necessary for economic actors "to ascertain unequivocally what their rights and obligations are," and to allow concerned citizens to examine compliance. As the U.S. Supreme Court noted in 2020, "[e]very citizen is presumed to know the law, and it needs no argument to show that all should have free access" to it.

The Court of Justice's decision has far-reaching effects beyond the four toy safety standards under dispute. Its reasoning classifying these standards as EU law applies more broadly to standards incorporated into law. We're pleased that under this precedent, EU standards-development organizations will be required to disclose standards on request without locking these important parts of the law behind a paywall.

# Screenshot Showcase


***Posted by francesco_bat, on April 5, 2024, running IceWM.***

# GIMP Tutorial: Playing With G'MIC, Part 2

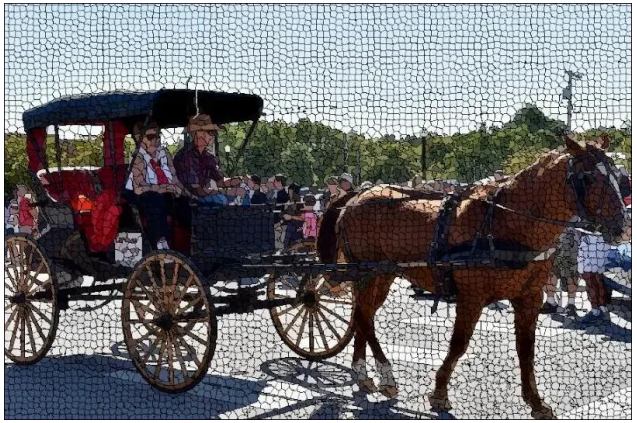
**by Meemaw**

In March, I started on a review of a few of the hundreds of filters you can access in GIMP with G'MIC. I found then that some of the filters in the Windows version aren't available in the Linux version. After the magazine was published I discovered that the Windows version was 3.3 and the version in our repo was 2.9. I'm sure ours will be updated soon!

Anyway, this month I'll review a few more of them that I think might be sort of useful. Of course, it always depends on what you are using them for, but the ones I'll show only do minor changes to your photos. I think you'll like knowing about them.

I used a photo of a horse & buggy I saw in a parade I attended in 2021.

One of the effects I thought was nice is in the **Contours** subcategory. **Super Pixels** makes the photo look like it's been changed to a sort of jigsaw puzzle, but with each piece a certain color, like each is a big pixel. The size can be adjusted, along with the smoothness, iterations (number of different shapes) and the color of the border around each "pixel".



In the subcategory **Deformations**, there is a filter called **Reflection**, which does what you think: puts a reflection under your photo subject. It can be accurate or not, depending on what shadows are in your photo. You have several settings you can change, including height, color, angle and zoom. You might have to play with these and see what works best for your photo (right, top).

Still in Deformations, we have **Textured Glass**, which makes your photo look a little like looking through a frosted window at

your subject. You can edit amplitude, smoothness and noise, and a couple other settings.

The next subcategory is **Degradations**, and one of the filters is **Rain & Snow**. This also does just exactly what you think. Its advantage is that it does it fairly quickly. You can edit Angle,

Speed, Density, Radius, Gamma and Opacity.

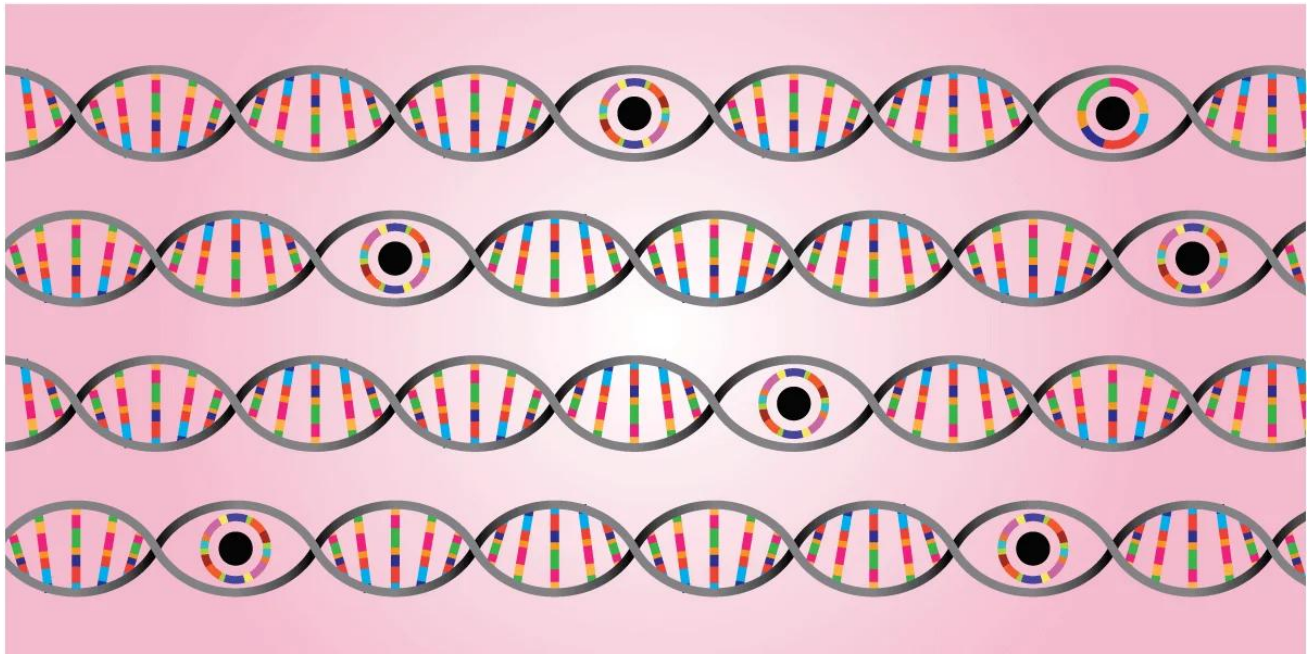
I did an article in the March, 2017 issue about some scripts I got from the GIMP Learn website where I featured a script called Render Snow. This one is similar.

Again from Degradations, another useful filter is called **Visible Watermark**. This one allows you to insert a repeated watermark into your image. You can choose what the watermark says, what angle it's displayed at, its size and its opacity. I haven't, however, seen anything that lets you change it from a pattern all across your image to something less prevalent. If you are trying to keep someone from using your image, though, an all-over watermark is preferred (center, top).

I went on to one called **Details**. One called **Emboss-Relief** looked interesting. It makes your image look embossed. Main settings to change are Angle, Depth and Smoothness (right).

Obviously, you have to play with the settings on each of these to get the best result. I hope you can find some of these useful.

# Cops Running DNA-Manufactured Faces Through Face Recognition Is A Tornado Of Bad Ideas



**by Paige Collings and Matthew Guariglia**
Electronic Frontier Foundation


In keeping with law enforcement's grand tradition of taking antiquated, invasive, and oppressive technologies, making them digital, and then calling it innovation, police in the U.S. recently combined two existing dystopian technologies in a brand new way to violate civil liberties. A police force in California recently employed the new practice of taking a DNA sample from a crime scene, running this through a service provided by US company Parabon NanoLabs that guesses what the perpetrators face looked like, and plugging this rendered image into face recognition software to build a suspect list.

Parts of this process aren't entirely new. On more than one occasion, police forces have been found to have fed images of celebrities into face recognition software to generate suspect lists. In one case from 2017, the New York Police Department decided its suspect looked like Woody Harrelson and ran the actor's image through the software to generate hits. Further, software provided by US company Vigilant Solutions enables law enforcement to create "a proxy image from a sketch artist or artist rendering" to enhance images of potential suspects so that face recognition software can match these more accurately.

Since 2014, law enforcement have also sought the assistance of Parabon NanoLabs — a company that alleges it can create an image of the suspect's face from their DNA. Parabon NanoLabs claim to have built this system by training machine learning models on the DNA data of thousands of volunteers with 3D scans of their faces. It is currently the only company offering phenotyping and only in concert with a forensic genetic genealogy investigation. The process is yet to be independently audited, and scientists have affirmed that predicting face shapes—particularly from DNA samples—is not possible. But this has not stopped law enforcement officers from seeking to use it, or from running these fabricated images through face recognition software.

Simply put: police are using DNA to create a hypothetical and not at all accurate face, then using that face as a clue on which to base investigations into crimes. Not only is this full dice-roll policing, it also threatens the rights, freedom, or even the life of whoever is unlucky enough to look a little bit like that artificial face.

But it gets worse.

In 2020, a detective from the East Bay Regional Park District Police Department in California

asked to have a rendered image from Parabon NanoLabs run through face recognition software. This 3D rendering, called a Snapshot Phenotype Report, predicted that — among other attributes—the suspect was male, had brown eyes, and fair skin. Found in police records published by Distributed Denial of Secrets, this appears to be the first reporting of a detective running an algorithmically-generated rendering based on crime-scene DNA through face recognition software. This puts a second layer of speculation between the actual face of the suspect and the product the police are using to guide investigations and make arrests. Not only is the artificial face a guess, now face recognition (a technology known to misidentify people) will create a "most likely match" for that face.

These technologies, and their reckless use by police forces, are an inherent threat to our individual privacy, free expression, information security, and social justice. Face recognition tech alone has an egregious history of misidentifying people of color, especially Black women, as well as failing to correctly identify trans and nonbinary people. The algorithms are not always reliable, and even if the technology somehow had 100% accuracy, it would still be an unacceptable tool of invasive surveillance capable of identifying and tracking people on a massive scale. Combining this with fabricated 3D renderings from crime-scene DNA exponentially increases the likelihood of false arrests, and exacerbates existing harms on communities that are already disproportionately over-surveilled by face recognition technology and discriminatory policing.

There are no federal rules that prohibit police forces from undertaking these actions. And despite the detective's request violating Parabon NanoLabs' terms of service, there is seemingly no way to ensure compliance. Pulling together criteria like skin tone, hair color, and gender does not give an accurate face of a suspect, and deploying these untested algorithms without any oversight places people at risk of being a suspect for a crime they didn't commit. In one case from Canada, Edmonton Police Service issued an apology over its failure to balance the harms to the Black community with the potential investigative value after using Parabon's DNA phenotyping services to identify a suspect.

EFF continues to call for a complete ban on government use of face recognition—because otherwise these are the results. How much more evidence do law markers need that police cannot be trusted with this dangerous technology? How many more people need to be falsely arrested and how many more reckless schemes like this one need to be perpetrated before legislators realize this is not a sustainable method of law enforcement? Cities across the United States have already taken the step to ban government use of this technology, and Montana has specifically recognized a privacy interest in phenotype data. Other cities and states need to catch up or Congress needs to act before more people are hurt, and our rights are trampled.

# Screenshot Showcase


***Posted by kalwisti, on April 8, 2024, running Debian Mate.***

# The Motion Picture Association Doesn't Get To Decide Who The First Amendment Protects

**by Mitch Stoltz and Katharine Trendacosta**
**Electronic Frontier Foundation**


Twelve years ago, internet users spoke up with one voice to reject a law that would build censorship into the internet at a fundamental level. This week, the Motion Picture Association (MPA), a group that represents six giant movie and TV studios, announced that it hoped we'd all forgotten how dangerous this idea was. The MPA is wrong. We remember, and the internet remembers.

What the MPA wants is the power to block entire websites, everywhere in the U.S., using the same tools as repressive regimes like China and Russia. To it, instances of possible copyright infringement should be played like a trump card to shut off our access to entire websites, regardless of the other legal speech hosted there. It is not simply calling for the ability to take down instances of infringement—a power they already have, without even having to ask a judge—but for the keys to the internet. Building new architectures of censorship would hurt everyone, and doesn't help artists.

The bills known as SOPA/PIPA would have created a new, rapid path for copyright holders like the major studios to use court orders against sites they accuse of infringing copyright. Internet service providers (ISPs) receiving one of those orders would have to block all of their customers from accessing the identified websites. The orders would also apply to domain name registries and registrars, and potentially other companies and organizations that make up the internet's basic infrastructure. To comply, all of those would have to build new infrastructure dedicated to site-blocking, inviting over-blocking and all kinds of abuse that would censor lawful and important speech.

In other words, the right to choose what websites you visit would be taken away from you and given to giant media companies and ISPs. And the very shape of the internet would have to be changed to allow it.

In 2012, it seemed like SOPA/PIPA, backed by major corporations used to getting what they want from Congress, was on the fast track to becoming law. But a grassroots movement of diverse Internet communities came together to fight it. Digital rights groups like EFF, Public Knowledge, and many more joined with editor communities from sites like Reddit and Wikipedia to speak up. Newly formed grassroots groups like Demand Progress and Fight for the Future added their voices to those calling out the dangers of this new form of censorship. In the final days of the campaign, giant tech companies like Google and Facebook (now Meta) joined in opposition as well.

What resulted was one of the biggest protests ever seen against a piece of legislation. Congress was flooded with calls and emails from ordinary people concerned about this steamroller of censorship. Members of Congress raced one another to withdraw their support for the bills. The bills died, and so did site blocking legislation in the US. It was, all told, a success story for the public interest.

Even the MPA, one of the biggest forces behind SOPA/PIPA, claimed to have moved on. But we never believed it, and they proved us right time and time again. The MPA backed site-blocking laws in other countries. Rightsholders continued to ask US courts for site-blocking orders, often winning them without a new law. Even the lobbying of Congress for a new law never really went away. It's just that today, with MPA president Charles Rivkin openly calling on Congress "to enact judicial site-blocking legislation here in the United States," the MPA is taking its mask off.

Things have changed since 2012. Tech platforms that were once seen as innovators have become behemoths, part of the establishment rather than underdogs. The Silicon Valley-based video streamer Netflix illustrated this when it joined MPA in 2019. And the entertainment companies have also tried to pivot into being tech companies. Somehow, they are adopting each other's worst aspects.

But it's important not to let those changes hide the fact that those hurt by this proposal are not Big Tech but regular internet users. Internet platforms big and small are still where ordinary users and creators find their voice, connect with audiences, and participate in politics and culture, mostly in legal—and legally protected—ways. Filmmakers who can't get a distribution deal from a giant movie house still reach audiences on YouTube. Culture critics still reach audiences through zines and newsletters. The typical users of these platforms don't have the giant megaphones of major studios, record labels, or publishers. Site-blocking legislation, whether called SOPA/PIPA, "no fault injunctions," or by any other name, still threatens the free expression of all of these citizens and creators.

No matter what the MPA wants to claim, this does not help artists. Artists want their work seen, not locked away for a tax write-off. They wanted a fair deal, not nearly five months of strikes. They want studios to make more small and midsize films and to take a chance on new voices. They have been incredibly clear about what they want, and this is not it.

Even if Rivkin's claim of an "unflinching commitment to the First Amendment" was credible from a group that seems to think it has a monopoly on free expression—and which just tried to consign the future of its own artists to the gig economy—a site-blocking law would not be used only by Hollywood studios. Anyone with a copyright and the means to hire a lawyer could wield the hammer of site-blocking. And here's the thing: we already know that copyright claims are used as tools of censorship.

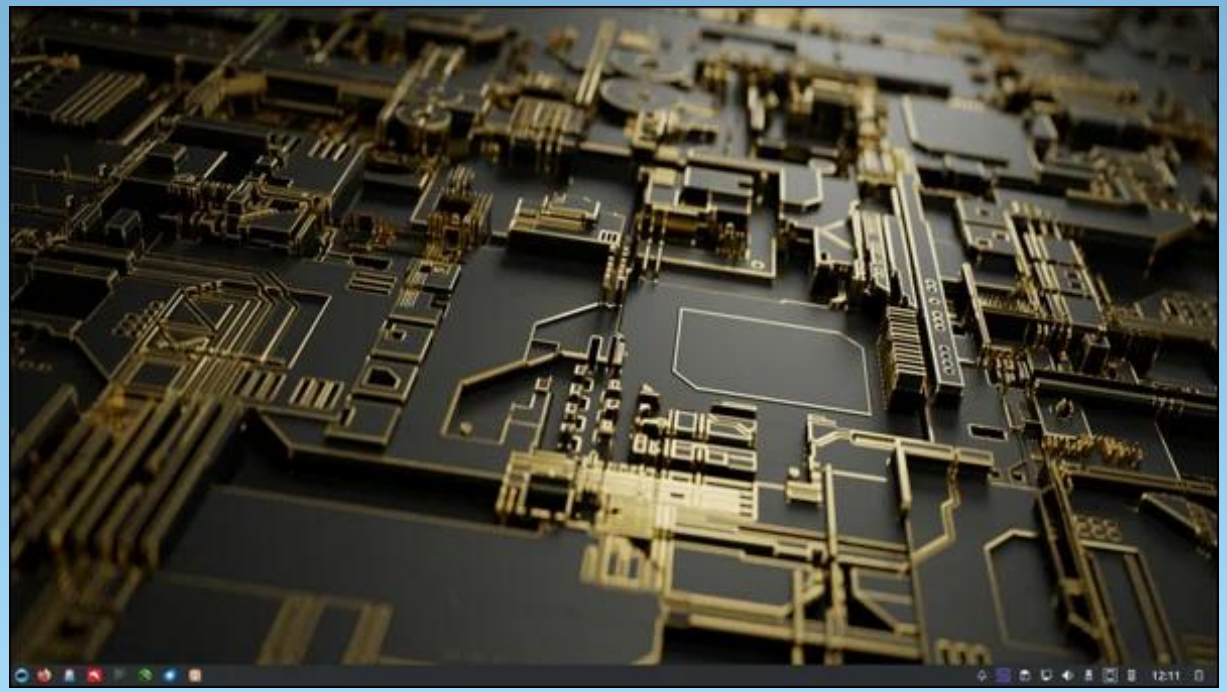
The notice-and-takedown system created by the Digital Millennium Copyright Act, for example, is abused time and again by people who claim to be enforcing their copyrights, and also by folks who simply want to make speech they don't like disappear from the Internet. Even without a site-blocking law, major record labels and US Immigration and Customs Enforcement shut down a popular hip hop music blog and kept it off the internet for over a year without ever showing that it infringed copyright. And unscrupulous characters use accusations of infringement to extort money from website owners, or even force them into carrying spam links.

This censorious abuse, whether intentional or accidental, is far more damaging when it targets the internet's infrastructure. Blocking entire websites or groups of websites is imprecise, inevitably bringing down lawful speech along with whatever was targeted. For example, suits by Microsoft intended to shut down malicious botnets caused thousands of legitimate users to lose access to the domain names they depended on. There is, in short, no effective safeguard on a new censorship power that would be the internet's version of police seizing printing presses.

Even if this didn't endanger free expression on its own, once new tools exist, they can be used for more than copyright. Just as malfunctioning copyright filters were adapted into the malfunctioning filters used for "adult content" on tumblr, so can means of site blocking. The major companies of a single industry should not get to dictate the future of free speech online.

Why the MPA is announcing this now is anyone's guess. They might think no one cares anymore. They're wrong. Internet users rejected site blocking in 2012, and they reject it today.

# Screenshot Showcase



*Posted by luikki, on April 11, 2024, running KDE.*

# PCLinuxOS Recipe Corner Bonus


## Slow-Cooker Whole Orange Chicken

Serves: 4

**INGREDIENTS:**

1 jar (12 oz) sweet orange marmalade
1/2 cup packed brown sugar
1/4 cup soy sauce
2 tablespoons chili garlic sauce
1 teaspoon salt
1 whole chicken (3 1/2 to 4 1/2 lb)
1-inch piece fresh ginger root, peeled
1/4 cup cornstarch
1/4 cup orange juice
6 thin slices of orange, halved
2 tablespoons chopped fresh cilantro leaves
Cooked white rice, if desired

**DIRECTIONS:**

Spray 5-quart oval slow cooker with cooking spray. In a small bowl, mix marmalade, brown sugar, soy sauce, chili garlic sauce and salt. Add chicken and marmalade mixture to slow cooker, spreading marmalade mixture over chicken, inside and out. Place chicken breast side down; add ginger root.

Cover; cook on Low heat setting 4 to 5 hours, until an instant-read thermometer inserted in the thickest part of chicken thigh muscle and not touching bone reads at least 165°F (legs should move easily when lifted or twisted). Do not uncover slow cooker before 4 hours.

Remove ginger root, and discard. Transfer chicken to cutting board; let stand about 5 minutes, or until cool enough to handle. Cut into 8 pieces.

Meanwhile, in a small bowl, mix cornstarch and orange juice; stir into liquid mixture in slow cooker. Cover; cook on High heat setting 10 to 15 minutes, or until sauce thickens.

Position oven rack 4 inches from broiling element. Set oven control to broil. Line a large rimmed baking pan with foil; carefully transfer chicken, skin side up, to pan. Place orange slices around chicken; brush oranges and chicken with sauce. Broil 3 to 5 minutes or until skin is golden brown and crisp; sprinkle with cilantro, and serve with more of the sauce over rice.

**TIPS:**

Trouble getting every last bit of marmalade out of the jar? Submerge the sealed jar in a bowl of very hot water for about 5 minutes.

One large navel orange will provide enough orange slices and juice for this recipe. Cut the thin slices from the center, then squeeze 1/4 cup of fresh orange juice from the remaining ends.

**NUTRITION:**

Calories: 560 Carbs: 28g Sodium: 790mg
Fiber: 1g Protein: 38g

# PCLinuxOS Puzzled Partitions

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

**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.

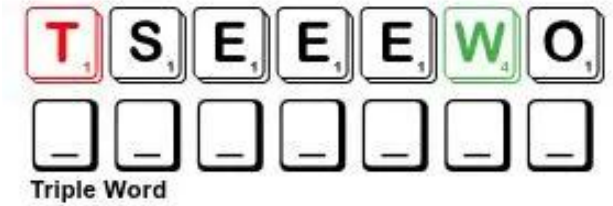
Each column must contain all of the numbers 1 through 9 and no two numbers in the same column of a Sudoku puzzle can be the same. Each row must contain all of the numbers 1 through 9 and no two numbers in the same row of a Sudoku puzzle can be the same.

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.

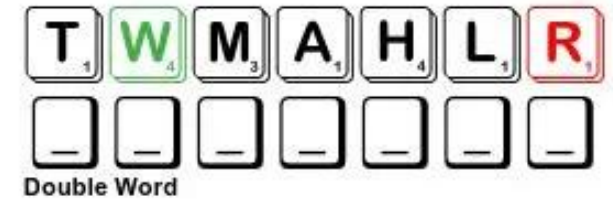
**SCRAPPLER RULES:**

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**







**Possible score 298, average score 209.**

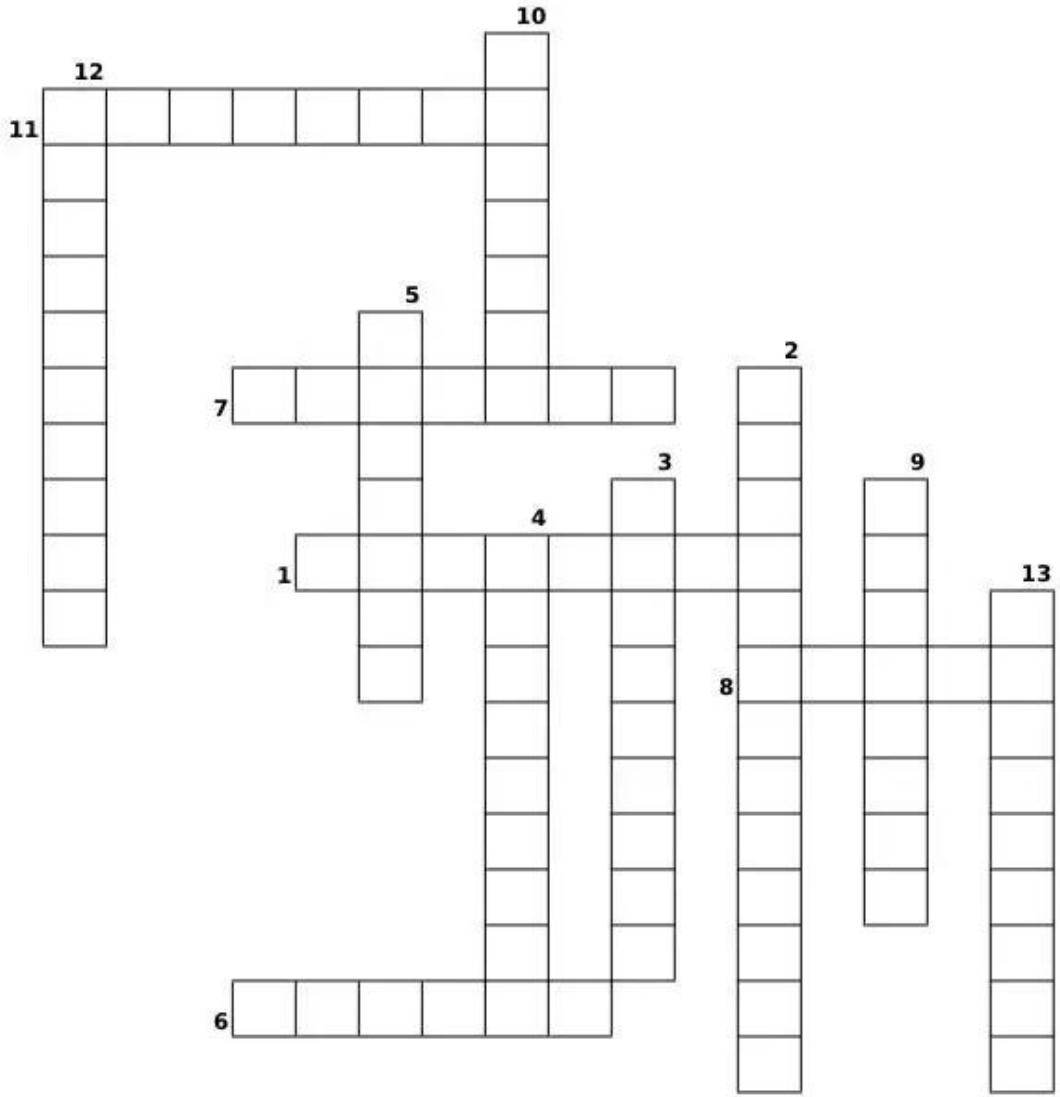
# May 2024 Word Find
# Mother's Day

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

| | |
|---|---|
| ADORE | ANCESTOR |
| APPRECIATE | BIRTH |
| CELEBRATE | CHILD |
| COOKIES | DAISY |
| DOTING | FEELINGS |
| GIFT | GRANDMA |
| GRATEFUL | HUG |
| INHERIT | JEWELS |
| LINEAGE | MAMA |
| MEAL | MEMORIES |
| MOMMY | MOTHER |
| NUCLEAR FAMILY | OFFSPRING |
| PRESENT | SPOUSE |
| SWEET | TRADITION |
| WARMTH | WOMAN |

**Download Puzzle Solutions Here**

# May 2024 Crossword
# Mother's Day




1. Appreciative of benefits received; thankful.
2. A family unit consisting of a mother and father and their children.
3. A child or children of a parent or parents.
4. The passing down of elements of a culture from generation to generation.
5. To receive or take over from a predecessor.
6. Extravagantly or foolishly loving and indulgent.
7. A descending line of offspring.
8. To love (someone) deeply and devotedly.
9. The mental faculty of retaining and recalling past experience.
10. The mother of your father or mother.
11. A person from whom one is descended, especially if more remote than a grandparent.
12. To be thankful or show gratitude for.
13. To observe (a day or event) with ceremonies of respect, festivity, or rejoicing.

**Download Puzzle Solutions Here**

# Mixed-Up-Meme Scrambler

INNEL

SCEHS

NOPPIL

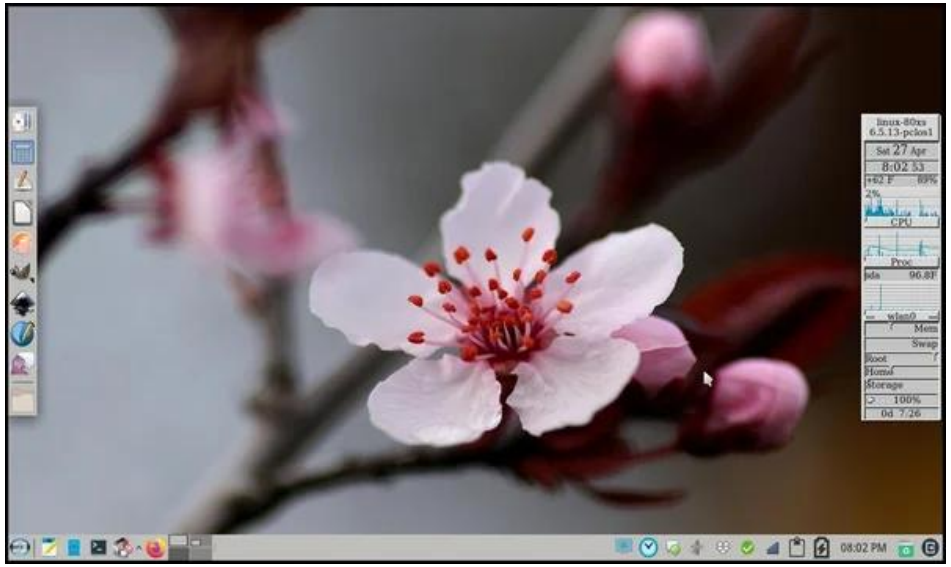
GLEIMN

What a couple of busybodies are good at feeding

_ _ _ _ _ _ _ _ _ _ _ _

Download Puzzle Solutions Here

# More Screenshot Showcase



*Posted by Meemaw, on April 27, 2024, running Xfce.*

*Posted by Nish, on March 31, 2024, running Cinnamon.*

*Posted by onkelho, on April 16, 2024, running Xfce.*

*Posted by parnote, on April 27, 2024, running Xfce.*